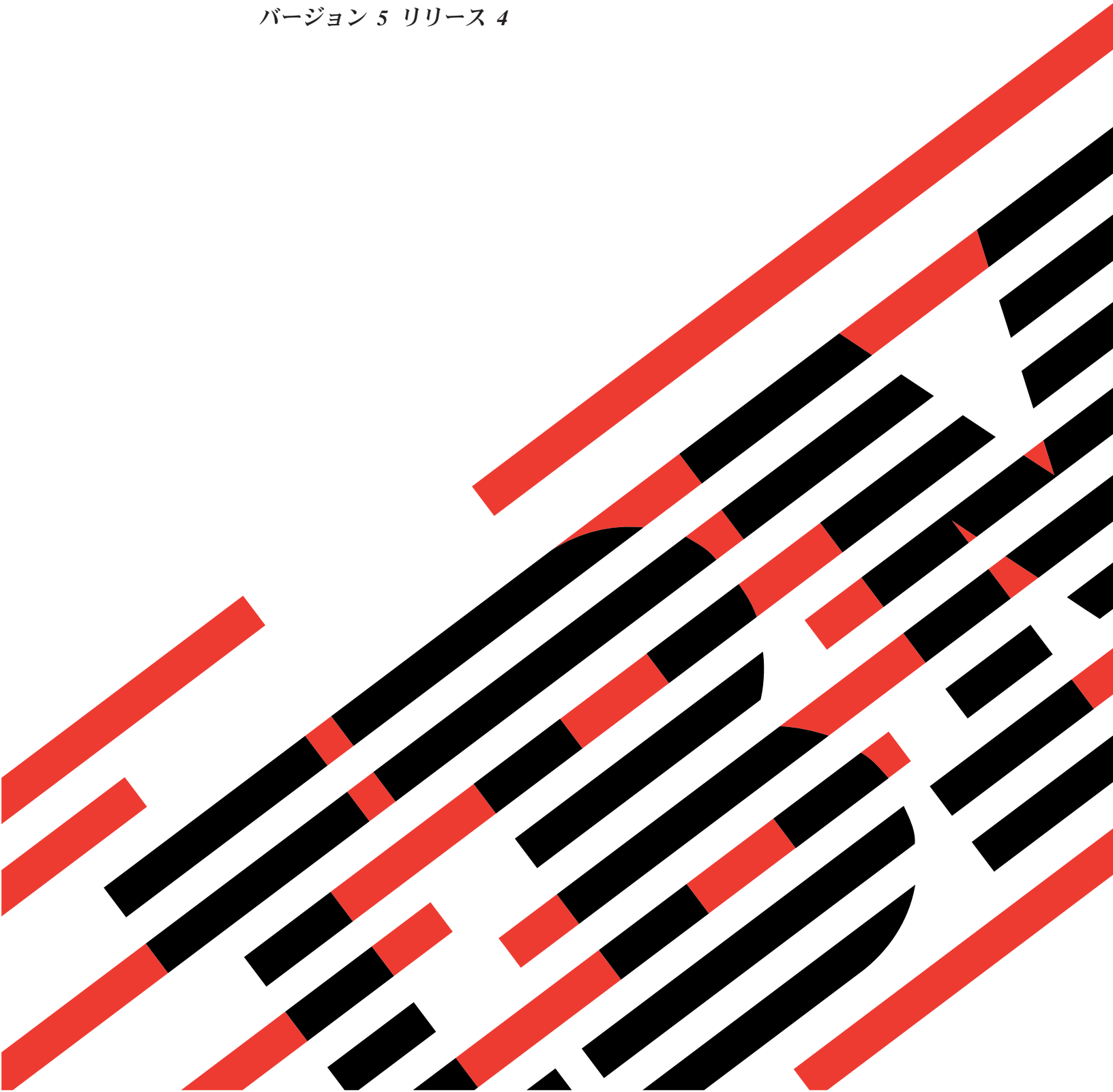
IBM Systems - iSeries

セキュリティー
システム・セキュリティーの計画とセットアップ

バージョン 5 リリース 4



IBM Systems - iSeries

セキュリティー
システム・セキュリティーの計画とセットアップ

バージョン 5 リリース 4

ご注意！

本書および本書で紹介する製品をご使用になる前に、 353 ページの『特記事項』 に記載されている情報をお読みください。

本書は、IBM i5/OS (製品番号 5722-SS1) のバージョン 5、リリース 4モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションに適用されます。 このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原　典： IBM Systems - iSeries
Security Plan and set up system security
Version 5 Release 4

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2006.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、平成角ゴシック体™W7

目次

システム・セキュリティーの計画と設定

この一連のトピックでは、システム・セキュリティーの計画、設定、および使用に関する詳細情報を提供します。これらのトピックは、以前の『基本システム・セキュリティーおよび計画』トピックと「*iSeries*™ セキュリティーの*手引き* 」の情報を結合しています。

貴社のシステム・セキュリティーを判断することは、セキュリティー計画を立てる際に下す最も基本的かつ重要な決定です。システム・セキュリティーにおいては、価値ある情報を保護する必要性と、貴社を首尾よく成長させるためにそうした情報にユーザーがアクセスする必要性との間でバランスを取らなければなりません。このバランスを取るには、貴社の現在の方向性における特定の必要やゴールについて理解するとともに、今後の必要にも注意を払う必要があります。セキュリティー計画は資源を保護するものであると同時に、貴社の成長に合わせて拡張できる十分柔軟な計画でなければなりません。

サーバー上のシステム・レベルのセキュリティーを作成、構成、および管理する際に役立つ幾つかのツールがあります。セキュリティーとは、サーバーを保護して、システムに保管されている資産へのアクセスを管理するだけでは終わらないという点を理解するのは重要なことです。完全なセキュリティーのインプリメンテーションには、システム・レベルのセキュリティーを保護するだけではなく、ネットワーク・レベルのセキュリティーとトランザクション・レベルのセキュリティーも保護する必要があります。このトピックは、システム・レベルのセキュリティーを中心に扱います。

この情報を使用して、貴社の特定のシステム・セキュリティーの必要性に合った独自の計画を作成してください。システム・セキュリティーの計画フェーズが完了したなら、この情報で提供されている説明を使用してシステム・セキュリティーを設定できます。

V5R4 の新機能

「システム・セキュリティーの計画とセットアップ」には、システム・レベルのセキュリティーを効率的かつ体系的に計画および構成する方法が説明されています。

この新しいトピックは、「基本システム・セキュリティーおよび計画」と「*セキュリティーの手引き*」(SD88-5065) 資料を合わせたものです。これら 2 つの古いトピックは、Information Center から除去されました。

新規情報と改訂情報の見つけ方

これは新規トピックのため、リビジョン・バーはありません。

このリリースでの新規情報と改訂情報については、「プログラム資料説明書」の追加情報も参照してください。

印刷可能な PDF

この情報の PDF を表示および印刷するために使用します。

本書の PDF バージョンを表示またはダウンロードするには、「セキュリティー システム・セキュリティーの計画とセットアップ」を選択します。

以下の関連資料を表示またはダウンロードできます。

- iSeries 機密保護解説書

PDF ファイルの保管

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を右マウス・ボタン・クリックする (上部のリンクを右マウス・ボタン・クリック)。
2. Internet Explorer を使用している場合は、「**名前を付けて保存**」をクリックする。Netscape Communicator を使用している場合は、「**名前を付けて保存**」をクリックします。
3. PDF を保管したいディレクトリーに進む。
4. 「**保存**」をクリックする。

Adobe Acrobat Reader のダウンロード

これらの PDF を表示または印刷するには、Adobe Acrobat Reader が必要です。このアプリケーションは、Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) からダウンロードできます。

FAQ

以下は、システム・セキュリティーの設定と使用に関する一般的な質問です。

よく尋ねられる質問

管理者および機密保護担当者には、管理対象のシステムを保護するための多種多様なオプションや解決策があります。考えうるこうした解決策すべてが多いため混乱したり圧倒されたりするかもしれませんが、優れたシステム・セキュリティーには、必要な基本的セキュリティーと貴社においてセキュリティーが果たす役割に関する理解が関係しています。貴社とそのシステムにおけるセキュリティーの価値を理解するには、最も基本的なレベルにおけるセキュリティーの意味合いを把握しておく必要があります。

1. **なぜセキュリティーが重要なのか ?**

   回答: システムに保管される情報は、最も重要なビジネス資産の 1 つです。こうした機密情報としては、顧客アカウント、給与計算ステートメント、決算報告書があります。このような情報を保護する必要性と、従業員がその職責を果たすためにアクセスを許可する必要性との間でバランスを取らなければなりません。情報資産を保護する方法を検討する際、次の 3 つの重要な目的に留意してください。

   - **機密性:** セキュリティー上の適切な対策により、他人が機密情報を見たり、その内容を公表したりすることを防ぐことができます。システムにおいて選ばれた数人のユーザーのみが参照して保守できる、機密性のある情報はどれでしょうか?
   - **保全性:** 適切に設計されたセキュリティー・システムは、コンピューター上の情報の正確さをある程度まで保証することができます。正しいセキュリティーを行えば、許可なくデータが変更されたり、削除されたりすることを防ぐことができます。
   - **可用性:** 誰かが誤ってあるいは故意にシステムのデータに損害を与えた場合、データを回復するまでそれらの資源にはアクセスできなくなります。適切なセキュリティー・システムは、この種の損害を防ぐことができます。

     システム・セキュリティーが検討される場合、大抵は、ビジネス上のライバルなどの外部の人間から組織のシステムを保護することが検討されます。実際のところ、適切に設計されたセキュリティー・システムの最大の効果は、正当なユーザーによる詮索 (せんさく) やシステム事故からシステムを保

護することにあります。適切に設計されたセキュリティーを持たないシステムでは、ユーザーが意図せずに重要なファイルを削除してしまう場合があります。適切なセキュリティー・システムは、この種の事故を防止する上で役立ちます。

2. **システムでのセキュリティーに誰が責任を持つか?**

   回答: セキュリティーへのアプローチは、企業によって異なります。ある場合には、プログラマーが、セキュリティーのすべての局面において責任を持ちます。また、別の場合には、システムを管理する人がセキュリティーも担当することがあります。システムでのセキュリティーに責任を持つべき人を決定するため、以下に提案されているアプローチについて考慮してください。

   - セキュリティーを計画する方法は、会社がアプリケーションを購入するか、あるいは開発するかに応じて異なります。独自のアプリケーションを開発される場合は、開発プロセスで保護の必要を伝えてください。アプリケーションを購入される場合は、アプリケーションの設計担当者と意思の疎通をして、協力して作業してください。いずれの場合にも、アプリケーションの設計者は、設計の一環としてセキュリティーを考慮に入れる必要があります。
   - 資源保護を計画する方法は、会社がアプリケーションを購入するか、あるいは開発するかに応じて異なります。独自のアプリケーションを開発される場合は、開発プロセスで資源保護の必要を伝えてください。アプリケーションを購入される場合は、アプリケーションの設計担当者と意思の疎通をして、協力して作業してください。いずれの場合にも、アプリケーションの設計者は、設計の一環としてセキュリティーを考慮に入れる必要があります。

3. **システムのセキュリティーをなぜカスタマイズすべきか?**

   回答: 小規模なシステムでは 3 人から 5 人程度のユーザーが、2、3 のアプリケーションを実行するものがあります。大規模なシステムでは、多くのアプリケーションを実行する大規模な通信ネットワークで、数千人のユーザーがシステムを使用する場合もあります。ユーザーから見たシステムの外見、またはシステムが実行する方法について、多くの変更を加えることができます。

   システムを最初に導入する際には、おそらく、それほど多くのカスタマイズは必要とされません。IBM® では、多くのオプションにデフォルトと呼ばれる初期設定を施して、システムを出荷します。これらのデフォルトは通常、新規導入に最適な選択肢として使用されます。

   注: 新しいシステムはすべて、デフォルトのセキュリティー・レベル 40 を設定して出荷されます。このセキュリティー・レベルは、定義されたユーザーのみがシステムを使用できるようにします。また、セキュリティーの裏をかこうとするプログラムによる、保全性およびセキュリティーに対する潜在的なリスクを回避することもできます。

   しかし、いくつかのカスタマイズを行うことによって、システムをユーザーにとってより単純で、より効果的なものにすることができます。たとえば、ユーザーがサインオンしたときに、常に正しいメニューが表示されるようにすることができます。また、すべてのユーザーの報告書が適切なプリンターに送られるようにすることができます。いくつかの初期カスタマイズを行って、ユーザー自身のシステムに見栄え (ルック・アンド・フィール) をよりユーザー独自のものにすると、ユーザーはそのシステムをより信頼するでしょう。

自問する必要のある質問

1. **会社のビジネス要件を明確に定義したか?**

   回答: ご使用のシステムに有効なセキュリティーを計画して設定するには、有効かつ効率的に機能するビジネス要件をまず把握する必要があります。会社内におけるシステムの使用方法を理解しなければな

りません。たとえば、会社の会計情報を含むデータベースなどの重要なアプリケーションが含まれるシステムでは、社内での製品テストに使用するシステムに比べて高水準のセキュリティーが必要となります。

2. **保護する対象となる資産とは?**

   回答: ビジネス資産には、管理する物理システムだけでなく、そうしたシステムに保管されているデータや情報も含まれます。盗難やいたずらに遭う可能性を最小限に抑えるため、システムとそこに保管されている情報の目録を作成する必要があります。

   必要なセキュリティーの規模は、システムに保管される情報のタイプ、その情報の機密性、およびそのデータが盗まれたり危険にさらされたりする場合のビジネスに対する影響などに依存します。システムが直面する可能性のあるリスクを理解しておくなら、システムにおけるセキュリティーをより効果的に管理できます。

3. **セキュリティーに関する会社のポリシーはあるか?**

   回答: セキュリティー・ポリシーは、会社の資源を保護するための、またセキュリティーに関連した出来事に対応するための、さらには遠隔地の従業員、ビジネス・パートナー、一般のお客様との安全な商取引を処理するための会社の要件を定義します。このセキュリティー・ポリシーには、システムの物理的セキュリティー、従業員によるインターネット・アクセスなどのネットワーク・セキュリティー問題、およびシステムでのセキュリティーの評価やモニターの指標が関係します。セキュリティー・ポリシーは、セキュリティーに関する判断の基礎と考えてください。セキュリティー・ポリシーは中心となるビジネスを主体にしている必要がありますが、同時に将来のビジネス要求に十分対応できるように柔軟性を持たせる必要もあります。

4. **従業員はインターネットにアクセスしているか、またはその必要があるか?**

   回答: 今日、多くの会社では従業員にインターネットへのアクセスを許可して、調査を行ったり、ビジネス上の日常操作に関連して顧客に応答したりする必要があることを理解しています。システムおよびユーザーがインターネットに接続すると、内部リソースがアタックされるリスクが必ず生じます。インターネットの使用に関連したこうしたリスクからご使用のネットワークを保護するには、許可するネットワーク・サービス、ユーザーがインターネットに接続する方法、およびご使用のネットワークにおいてネットワーク・セキュリティーをモニターする方法を決定する必要があります。インターネットやその使用に関連して下す決定については、従業員に対してセキュリティー・ポリシーとして、明確に定義して伝えなければなりません。こうしたポリシーを全従業員が理解して、承諾契約に署名するのは重要なことです。ネットワーク・セキュリティー・ポリシーの実施はこのトピックの範囲外ですが、セキュリティー・ポリシーのいずれかに、ネットワーク・セキュリティーに関する情報を含めてください。

概念

システムのセキュリティー・ポリシーを効果的に作成し、有効なセキュリティー対策を計画するには、以下のセキュリティー概念を理解する必要があります。一部は一般的な概念ですが、ハードウェア・タイプに特有のものもあります。

小規模なシステムでは 3 人から 5 人程度のユーザー、大規模なシステムでは数千人のユーザーを持つことが考えられます。すべてのワークステーションが 1 か所の比較的安全な区域に置かれるインストール・システムもあれば、ダイヤル・インで接続するユーザーと、パーソナル・コンピューターやシステム・ネットワークを介して接続される間接ユーザーを含む、広範囲に分散したユーザーをサポートするシステムもあります。このシステム上でのセキュリティーは、このように広範囲のユーザーや状況に見合う柔軟性を十分備

えています。使用可能な機能とオプションを固有のセキュリティー要件に適合させるためには、それらの機能とオプションを理解する必要があります。この項では、システム上で使用されるセキュリティー機能を概説します。

システム・セキュリティーには、3 つの重要な目的があります。

機密性:
- 認可のないユーザーに情報が公開されることがないように保護する。
- 機密情報へのアクセスを制限する。
- 好奇心の強いシステム・ユーザーや部外者がアクセスしないように保護する。

保全性:
- 許可なしでデータ変更されることがないように保護する。
- 認可プログラムに対するデータ操作を限定する。
- データの信頼性を保証する。

可用性:
- データが偶発的に変更されたり破壊されたりするのを防止する。
- 部外者がシステム資源を濫用したり破壊したりしないように保護する。

システム・セキュリティーは、ハッカーやライバル企業などの外部との危険とも関係があります。しかしながら、高度なセキュリティー・システムを持つことによって認可ユーザーによるシステム事故からのシステムの保護が最大の効用として得られます。高度なセキュリティー機能を持たないシステムでは、間違ったキーを押したために、重要な情報が削除されてしまう場合があります。システム・セキュリティーを使用すれば、この種の事故を防ぐことができます。

最良のセキュリティー・システム機能を使用していても、よい計画がなければよい結果を生み出すことはできません。計画をせず、一貫性なく設計されたセキュリティーは、混乱を招きます。そのようなセキュリティー設定を保持し監査するのは困難です。計画するとは、あらゆるファイル、プログラム、および装置に対してセキュリティーを事前設計するという意味ではありません。これは、システムのセキュリティーへの全体的なアプローチを確立して、そのアプローチをアプリケーション設計者、プログラマー、およびシステム・ユーザーに伝えることを意味します。

システム上のセキュリティーを計画し、どの程度のセキュリティーが必要かを決定する際には、以下の質問事項を考慮してください。
- 特定のレベルのセキュリティーを求めるような会社の方針や基準が存在するか
- 会社の監査員は特定のレベルのセキュリティーを必要としているか
- システムやそこにあるデータは業務上どれほど重要か
- セキュリティー機能が提供するエラー保護はどれほど重要か
- 企業側は将来的にどの程度のセキュリティーを望んでいるか

導入を円滑に行うために、ユーザーのシステム上のほとんどのセキュリティー機能は、システム出荷時に活動化されていません。このトピックでは、ユーザーのシステムを適切なレベルで保護するために推奨される情報を提供しています。この推奨を評価するときは、導入先固有のシステムのセキュリティー要件を考慮します。

基本用語

このトピックでは、基本的なセキュリティー用語をユーザーに提供します。

オブジェクト

オブジェクトとは、ユーザーまたはアプリケーションが操作可能なシステム上の名前付きスペースのことです。ユーザーまたはアプリケーションが扱うことのできるシステム上のすべてのものが、オブジェクトと見なされます。オブジェクトは、システム構成要素を扱うための共通インターフェースを提供します。最も一般的なオブジェクトの例は、ファイルとプログラムです。別のタイプのオブジェクトには、コマンド、待ち行列、ライブラリー、およびフォルダーなどが含まれます。システム上のオブジェクトは、オブジェクト名、オブジェクト・タイプ、およびオブジェクトの存在するライブラリーによって識別されます。システム上の各オブジェクトを保護することができます。

ライブラリー

ライブラリーは、特殊なタイプのオブジェクトで、他のオブジェクトをグループ化するために使用されます。システム上の多くのオブジェクトは、ライブラリーにあります。ライブラリーは本質的にはコンテナー、つまり他のオブジェクトの組織構造であり、これを使用してシステム上の他のオブジェクトを参照することができます。ライブラリーに多数のオブジェクトを含めることができ、また特定のユーザー・プロファイルやアプリケーションに関連付けることができます。システム上の他のすべてのライブラリーを含む QSYS が、他のライブラリーを含めることのできる唯一のライブラリーです。ライブラリー内のオブジェクトは、サブディレクトリー内のオブジェクトと同様に処理されます。ライブラリーを、ディレクトリー内に置くことはできません。

ディレクトリー

ディレクトリーは特殊なオブジェクトで、システム上のオブジェクトをグループ化するもう 1 つの方法です。オブジェクトはディレクトリー内に存在することができ、ディレクトリーは他のディレクトリーの下に存在して、階層構造を形成することができます。各ファイル・システムは、統合ファイル・システム・ディレクトリー構造内の主要な**サブツリー**です。ディレクトリーはアドレス指定できませんが、各ライブラリーのアドレスは QSYS ライブラリーにマップできるという点が、ディレクトリーとライブラリーの相違点です。ライブラリー名は 10 文字までに制限されますが、ディレクトリーにはより長い名前を付けることができ、大/小文字を区別する場合があります。ディレクトリーへのパスには名前を付けることができ、ディレクトリーそのものではないので、ディレクトリーに複数の名前を付けることができます。ディレクトリーおよびライブラリーを扱う際には、各種のコマンドや権限要件を使用できます。

ユーザー・プロファイル

各システム・ユーザーは、システムにサインオンして使用するにはユーザー ID を有している必要があります。このユーザー ID はユーザー・プロファイルと呼ばれる特殊なオブジェクトで、適切なシステム権限を持つ管理者だけがユーザーのために作成できます。

特殊権限

ユーザー・プロファイルを作成したり他のユーザーのジョブを変更したりするシステム機能の実行を、ユーザーが許可されているかどうかは、特殊権限によって判別します。

物理的セキュリティー

物理的セキュリティーには、システム・ユニット、システム装置、およびバックアップ媒体を事故または配送の損害から保護することが含まれます。システムの物理的セキュリティーを確保するために取るほとんどの手段は、システムに対して外部的なものです。一部のシステム・モデルでは、認可のない機能を防止するキーロックがシステム・ユニットに装備されています。

アプリケーション・セキュリティー

アプリケーション・セキュリティーでは、システムに保管するアプリケーション、およびそれらへのアクセスを複数のユーザーに同時に許可している時にアプリケーションを保護する方法を扱います。

資源保護

システムでの資源保護によって、オブジェクトを使用できるユーザーとそのオブジェクトの使用方法を定義することができます。オブジェクトにアクセスできることを**権限**と呼びます。オブジェクト権限を設定するときは、ユーザーが自分たちの作業を十分に行える権限を与えるとともに、システムの表示や変更を行う能力を与えないように注意してください。オブジェクト権限は、特定のオブジェクトに関する許可をユーザーに与え、そのオブジェクトに対してユーザーは何ができるかを指定できます。オブジェクト資源を特定の詳細なユーザー権限によって、たとえばレコードの追加または変更というように制限することができます。システム資源を使用して、
*ALL、*CHANGE、*USE、*EXCLUDE といった、特定のシステム定義の権限のサブセットへのアクセスをユーザーに与えることができます。システム値とユーザー・プロファイルは、システムにアクセスするユーザーを制御し、許可のないユーザーがサインオンできないようにします。資源保護により、許可されたシステム・ユーザーが正常にサインオンした後に実行できるアクション、およびアクセスできるオブジェクトが制御されます。資源保護は、システム・セキュリティーの主な目的に沿って、以下のものを保護します。

- 情報の機密性
- 情報の正確さ (許可なく変更できないようにする)
- 情報の可用性 (不慮または故意に損傷を与えないようにする)

セキュリティー・ポリシー

セキュリティー・ポリシーを使用すると、i5/OS™ システムにセキュリティーを実装して管理できます。 eServer™ Security Planner を使用すると、サーバーに対する基本的なセキュリティー・ポリシーを計画して実装するのに役立ちます。

関連情報

セキュリティー用語

セキュリティー・レベル

システム・セキュリティーは一連の複数のレベルとして序列化され、レベルが高くなるにつれて、より強固にデータを保護する高水準のセキュリティーを提供します。

セキュリティー・レベル (QSECURITY) システム値を設定することにより、システムで実施するセキュリティーの程度を選択できます。i5/OS では、以下のような完全統合されたシステム・セキュリティー・レベルがサポートされます。

- **レベル 20: パスワード・セキュリティー**

  このセキュリティー・レベルでは、システムにアクセスするユーザーはシステムによって認識されるパスワードとユーザー ID を持っている必要があります。システム管理者がユーザーのユーザー ID と初期パスワードを作成します。このセキュリティー・レベルの場合、ユーザーはシステムに対するあらゆる操作を行う権限を持ちます。つまり、すべてのユーザーに *ALLJOB 特殊権限が与えられるため、システム上のすべてのデータ、ファイル、オブジェクトなどにアクセスできます。

- **レベル 30: パスワードおよび資源保護**

  このセキュリティー・レベルでは、システムの資源保護が施行されます。つまり、ユーザーはデフォルトで何も権限を持っていないため、オブジェクトを使用するための特定権限が必要です。ユーザーはす

べてのシステム・データに対するアクセス権限を自動的に与えられるわけではなく、システム管理者はユーザーのための有効なユーザー ID とパスワードを定義する必要があります。ユーザー・アクセスは、企業のセキュリティー・ポリシーによって制限されます。

- **レベル 40: 保全性保護**

  このセキュリティー・レベルでは、資源保護と保全性保護が施行され、システム自体がユーザーから保護されます。保全性保護機能 (たとえばオペレーティング・システムへのインターフェースのパラメーターの妥当性検査) は、システムに精通しているユーザーがシステムおよびシステム上のオブジェクトを改ざんしないよう保護する上で役立ちます。たとえば、ユーザー作成プログラムは、ポインター操作を介して内部制御ブロックに直接アクセスすることができません。レベル 40 はすべての新規導入で提供されるデフォルトのセキュリティー・レベルであり、ほとんどの導入システムで推奨されるセキュリティー・レベルです。

- **レベル 50: 拡張保全性保護**

  このセキュリティー・レベルでは、資源保護に加えて、レベル 40 の保全性保護よりも拡張された保全性保護が実施されます。拡張保全性保護には、拡張された制限が含まれています (たとえば、システム状態プログラムとユーザー状態プログラムの間のメッセージ処理の制限)。システムがユーザー作成プログラムに対して保護されるだけでなく、ユーザーはシステム上のデータにだけアクセスでき、システム情報自体にはアクセスできません。これにより、セキュリティーがさらに強固になり、システムについて知ろうとするユーザーから保護することができます。レベル 50 は現在可能な範囲で最高水準のセキュリティーを提供するため、ほとんどの企業にとって推奨されるセキュリティー・レベルです。さらに、レベル 50 は C2、FIPS-140、および Common Criteria 認証のための必須レベルです。

関連概念

39 ページの『システム・セキュリティーの計画』
システム・セキュリティーでは、ユーザー・アクセスとその特権の制御、情報の保全性の維持、プロセスとアクセスのモニター、システム機能の監査、およびセキュリティー関連情報のバックアップと回復の提供が必要となります。

ロック可能なセキュリティー・システム値

セキュリティー関連のシステム値をロックして、ユーザーやプログラムがこうした値を変更しないようにできます。

システム保守ツール (SST) および専用保守ツール (DST) には、これらのシステム値をロックするオプションがあります。システム値をロックすることにより、*SECADM 権限と *ALLOBJ 権限を持っている ユーザーでも、CHGSYSVAL コマンドを使ってこれらのシステム値を変更できないように設定できます。これらのシステム値変更の制限のほかに、Add Verifier (妥当性検査の追加) API を使用してディジタル証明書ストアにディジタル署名を追加することを制限したり、ディジタル証明書ストアのパスワードのリセットを制限したりできるようになりました。

システム保守ツール (SST) または専用保守ツール (DST) を使用して、セキュリティー関連のシステム値をロックしたりアンロックしたりできます。ただし、SST は回復モードの間は使用できないため、このモードでは DST を使用する必要があります。それ以外の場合、セキュリティー関連のシステム値をロックまたはアンロックするには、SST を使用します。

関連情報

機密保護関連システム値のロックおよびアンロック

グローバル設定

グローバル設定は、作業内容をシステムに入力する方法と、他のユーザーに対するシステムの表示方法に影響します。

これらのグローバル設定には、以下のものが含まれます。

- セキュリティー・システム値。システムにおけるセキュリティーを制御します。以下の 4 つのグループのいずれかに分類されます。
  - 汎用のセキュリティー・システム値
  - セキュリティー・プロパティーを持つ他のシステム値
  - パスワードを制御するシステム値
  - 監査を制御するシステム値

  システム値は、会社の方針であると考えてください。システム値は、ユーザー・プロファイルなどのより固有なものによってオーバーライドされる場合を除き、システムを使用するすべての人に適用されます。システム値を使用すると、システム・セキュリティーの特性を含め、システムのさまざまな特性のカスタマイズが可能になります。たとえば、1 台の装置でサインオンの試行を許可する人数、非活動のワークステーションをシステムが自動的にサインオフするかどうか、使用できるおよび変更できるパスワードの長さ、さらには他のパスワードの特性について定義できます。
- ネットワーク属性は、システムがほかのシステムが入っているネットワークに参加する (または参加しないことを選択する) 方法を制御します。
- サブシステム記述は、作業内容をシステムへ入力する方法と作業が実行される環境を決定します。多くの実行管理機能値は、セキュリティーに影響があります。
- 通信構成は、作業内容をシステムに入力する方法に影響を与えます。システムとネットワークの他の部分との通信を保護する必要があります。

  関連情報

  実行管理機能

ユーザー・プロファイル

各システム・ユーザーは、システムにサインオンして使用するにはユーザー ID を有している必要があります。このユーザー ID をユーザー・プロファイルといいます。

ユーザー ID は、システムに対してユーザーを一意に識別する文字ストリングです。ユーザー・プロファイルを作成できるのは、適切なシステム権限を持つ管理者だけです。

ユーザー・プロファイルは、ユーザーが実行できる機能を制御し、ユーザーに対するシステム表示をカスタマイズします。ユーザー・プロファイルには、ユーザーがシステム・サインオンし、カスタマイズされた自分のセッション (自分のメッセージ/出力待ち行列を含む) を利用し、自分が権限を持つ機能/オブジェクトにアクセスすることを可能にする、i5/OS で必要とされる情報が含まれます。ユーザー・プロファイルが適切に設計されていれば、システムを保護し、ユーザーに合わせてシステムをカスタマイズするうえで役立ちます。すべてのシステム・ユーザーはユーザー・プロファイルを必要とします。システム管理者が各ユーザーのユーザー・プロファイルを作成する必要があります。

管理者が定義できるユーザー・プロファイル関連パラメーターは多数あります (多数のセキュリティー関連属性を含む)。ユーザー・プロファイルのいくつかの重要なセキュリティー属性について、以下に説明します。

- **特殊権限:** 特殊権限は、ユーザー・プロファイルの作成、他のユーザーのジョブの変更などのシステム機能をユーザーが実行できるかどうかを決定します。
- **初期メニューと初期プログラム:** 初期メニューとプログラムは、システムにサインオンした後にユーザーに対して何を表示するかを決定します。ユーザーの初期メニューを制限することによって、特定のタスク・セットに限定することができます。
- **制限機能:** ユーザー・プロファイルの制限機能フィールドは、サインオン時にユーザーがコマンドを入力して初期メニューや初期プログラムを変更できるかどうかを決定します。

ユーザー・プロファイルをグループ・プロファイルの中に含めることができます。こうすれば、すべてのグループ・メンバーが特定オブジェクトへのアクセスとオブジェクト所有権を共有します。グループ・プロファイルを使用すれば、1 つの変更を複数のユーザーに適用することができ、多数のユーザー管理作業が単純化されます。

ユーザー・プロファイルの詳細については、*「iSeries 機密保護解説書」*の第 4 章『ユーザー・プロファイル』を参照してください。

関連概念

122 ページの『ユーザー・プロファイルの計画』
このトピックでは、ユーザー・プロファイルの目的およびその設計方法について取り上げます。

291 ページの『ユーザー・プロファイルの変更』
このトピックでは、ユーザー・プロファイルの変更方法について取り上げ、ステップバイステップの説明を行います。

291 ページの『使用禁止のユーザー・プロファイルの使用可能化』
このトピックでは、使用禁止のユーザー・プロファイルを使用可能にする方法と、それが重要な理由を取り上げ、段階的な手順を示します。

グループ・プロファイル

グループ・プロファイルは、ユーザーのグループの権限を定義します。

グループ・プロファイルを使用して、以下の作業を実行できます。

- 各ユーザーに個々に権限を与えるのではなく、ユーザー・グループに権限を定義できます。
- システムでオブジェクトを所有できます。
- プロファイル・コピー機能を使用することにより、ユーザー・プロファイルを個別に作成する際にグループ・プロファイルをパターンとして使用できます。

グループ・プロファイルは特別なタイプのユーザー・プロファイルで、システムでオブジェクトを所有できます。一般に、必要なシステム・アクセスや使用法が類似しているユーザーの集合に対してグループ・プロファイルを作成します。たとえば、同じアプリケーションを同じ方法で使用する必要があるユーザーの集合に対してグループ・プロファイルを作成できます。

また、プロファイル・コピー機能を使用するか、iSeries ナビゲーターのセキュリティー・ポリシー・メニューを使用してユーザー権限を編集することにより、ユーザー・プロファイルを個別に作成する際にグループ・プロファイルをパターンとして使用できます。

グループ・プロファイルは、システムにおいて以下の 2 つの目的を果たします。

- **セキュリティー・ツール**: グループ・プロファイルを使用することによって、システム上で特定のオブジェクトを使用できる人 (オブジェクト権限) を簡単に編成することができます。グループの個々のメンバーにではなく、グループ全体に対してオブジェクト権限を定義することができます。

- **カスタマイズ・ツール**: 個々のユーザー・プロファイルを作成する際のパターンとして、グループ・プロファイルを使用することができます。同じグループになるたいていのユーザーは、初期メニューおよびデフォルト・プリンターなど、カスタマイズの要件は同じになります。これらの要件をグループ・プロファイルに定義し、それを個々のユーザー・プロファイルにコピーすることができます。

グループ・プロファイルを使用すると、セキュリティーとカスタマイズの両面において、簡単で、一貫した体系を保持しやすくなります。

グループ・プロファイルを使用した作業について詳しくは、「*iSeries 機密保護解説書*」の以下のセクションを参照してください。

『グループ・プロファイルの計画』。グループ権限の使用について取り上げています。

『オブジェクトのグループ所有権』。グループ・プロファイルが所有する必要のあるオブジェクトについて説明しています。

『オブジェクトの 1 次グループ』。オブジェクトの 1 次グループおよび 1 次グループ権限の使用に関して取り上げています。

『ユーザー・プロファイルのコピー』。ユーザー・プロファイルを個別に作成する場合にグループ・プロファイルをコピーする方法について説明しています。

関連概念

116 ページの『グループ・プロファイルの計画』
このトピックでは、グループ・プロファイルの目的およびその設計方法について取り上げます。グループ・プロファイルを使用して、各ユーザーに個々に権限を与えるのではなく、ユーザーのグループに対して権限を定義します。

215 ページの『グループ・プロファイルの作成』
この項では、グループ・プロファイルの作成方法について説明します。 グループ・プロファイルは、各ユーザーに個々に権限を与えるのではなく、ユーザー・グループに権限を定義する場合に使用できます。

権限リスト

グループ・プロファイルのような権限リストを使用すると、類似したセキュリティー要件を持つオブジェクトをグループ化して、そのグループをユーザーおよびユーザー権限のリストと関連付けることができます。

権限リストは、システム上の類似のオブジェクトに対する権限を管理するための効率的な方法を提供し、セキュリティー情報を回復するのにも役立ちます。

ユーザーが処理する必要のあるあらゆるオブジェクトへのアクセス権をユーザーごとに明示的に規定するには、大量の重複労力が必要になります。多くのユーザーは同じグループのオブジェクトにアクセスする必要があるためです。このアクセス権の規定が容易になる方法として、権限リストを作成します。権限リストの内容は、ユーザーまたはグループのリスト、ユーザーまたはグループごとの権限のタイプ (*USE、*CHANGE、および *EXCLUDE)、およびこのリストでアクセス権を規定するオブジェクトのリストで構成されます。

たとえば、在庫データベースに関連したオブジェクトのリストを含む権限リストを作成することができます。新規在庫品目を注文する責任があるユーザーには、データベース・オブジェクトの内容を見る権限が付与されることになります。また、配送と受け入れを行うユーザー・グループは、部品が在庫から出入りするたびにそのデータベースを更新する必要があります。このグループは、それらのオブジェクトの内容を変更する権限をもつことができます。

権限リストには以下のような利点があります。

- 権限リストは権限の管理を単純化します。ユーザー権限はリスト上の各オブジェクトにではなく、権限リストに定義されます。新しいオブジェクトが権限リストで保護される場合、リスト上のユーザーはオブジェクトに対する権限を獲得できます。
- 1 回の操作で、リスト上のすべてのオブジェクトにユーザー権限を与えることができます。
- 権限リストは、システム上の私用権限の数を減少させます。各ユーザーは 1 つのオブジェクト、つまり権限リストに対して私用権限を持ちます。これによってリスト上のすべてのオブジェクトに対して、ユーザー権限が与えられます。システムの私用権限の数を減らすことには、以下のような利点があります。
  - ユーザー・プロファイルのサイズを小さくできる。
  - システムを保管する (SAVSYS) ときや、 セキュリティー・データを保管する (SAVSECDTA) ときのパフォーマンスを改善できる。
- 権限リストは、ファイルを保護するための有効な手段です。私用権限を使っている場合は、各ユーザーが各ファイル・メンバーに対する私用権限を持っています。権限リストを使用すると、各ユーザーは権限を 1 つだけ持っていればよくなります。また、オープンされているファイルでは、ファイルに対する権限を認可したり、ファイルから権限を取り消したりすることができません。権限リストを使用してファイルを保護する場合は、ファイルがオープンされているときでも、権限を変更することができます。
- 権限リストによって、オブジェクトが保管されたときに権限を記憶する方法が提供されます。権限リストによって保護されたオブジェクトを保管すると、その権限リストの名前がオブジェクトとともに保管されます。オブジェクトが削除されて同じシステムに復元された場合、それは権限リストに再び自動的にリンクされます。オブジェクトが別のシステム上で復元された場合、復元コマンドで ALWOBJDIF(*ALL) が指定されていないと、権限リストはリンクされません。

セキュリティー管理の観点から考えると、権限リストの方が、同じセキュリティー要件のあるオブジェクトを管理するのに良い方法です。リストで保護するオブジェクトが少ししかないときでも、オブジェクトで私用権限を使用するのではなく、権限リストを使用する方がやはり利点があります。1 つの場所 (権限リスト) に権限がまとめて置かれるので、オブジェクトに対し誰を許可するか変更するときに作業が容易になります。また、新規オブジェクトを、既存のオブジェクトと同じセキュリティー・レベル権限で保護することも容易になります。

権限リストを使用する場合は、そのオブジェクトの私用権限を持っていてはなりません。オブジェクトに私用権限があり、しかもそのオブジェクトを権限リストでも保護する場合は、権限検査時に、ユーザーの私用権限についての 2 つの探索が必要になります。最初の探索はオブジェクトの私用権限について探索で、2 番目の探索は権限リストの私用権限についての探索です。 2 つの探索は追加のシステム資源を必要とするので、システム・パフォーマンスに影響することがあります。権限リストだけしか使用しない場合は、1 つの探索だけ実行されます。また、権限リストでは権限キャッシュが使用されるため、権限検査のパフォーマンスは、オブジェクトの私用権限だけを検査する場合と同じになります。

グループ・プロファイルと権限リストの比較

グループ・プロファイルを使用すると、類似したセキュリティー要件を持つユーザーのユーザー・プロファイルの管理が簡単になります。権限リストは、類似したセキュリティー要件のあるオブジェクトを保護するのに役立ちます。 以下の表には、2 つの方法の特性が示されています。

表 1. 権限リストとグループ・プロファイルの比較

使用法に関する考慮事項	権限リスト	グループ・ プロファイル
複数オブジェクトの保護に使用可能。	はい	はい
ユーザーは複数に属することができる	はい	はい

表 1. 権限リストとグループ・プロファイルの比較 (続き)

使用法に関する考慮事項	権限リスト	グループ・ プロファイル
私用権限が他の権限を一時変更する	はい	はい
ユーザーは単独に権限を割り当てられなければならない	はい	いいえ
指定された権限は全オブジェクトに共通	はい	いいえ
オブジェクトは複数で保護される	いいえ	はい
オブジェクト作成時に権限を指定できる	はい	はい
すべてのオブジェクト・タイプを保護できる	いいえ	はい
オブジェクトが削除されるとオブジェクトとの関連も削除される	はい	いいえ
オブジェクトが保管されるとオブジェクトとの関連も保管される	はい	いいえ

権限リストについて詳しくは、「*iSeries 機密保護解説書*」の『グループ・プロファイルと権限リストの比較』を参照してください。

関連概念

164 ページの『権限リストの計画』
権限リストを使用して、類似のセキュリティー要件を持つオブジェクトごとに分類することができます。

230 ページの『権限リストの作成』
この項では、権限リストを作成する作業、およびそれが重要な理由を取り上げ、段階的な手順を示します。

妥当性検査リスト・オブジェクト

妥当性検査リスト・オブジェクトは、 アプリケーションがユーザー認証情報を安全に保管するための方式を提供します。

妥当性検査リスト・オブジェクトを使って次のようなタスクを実行できます。

- アプリケーション用のユーザー認証情報を安全に保管する。
- インターネット・ユーザーのように、i5/OS ユーザー・プロファイルを持たない (必要としない) ユーザー向けの承認メカニズムを提供する。

妥当性検査リスト・オブジェクトは、アプリケーションがユーザー認証情報を安全に保管するための方式を提供します。

たとえば、Internet Connection Server (ICS) は、妥当性検査リストを使用してインターネット・ユーザーの概念をインプリメントします。ICS は妥当性検査リストを使用して、Web ページの表示前に基本認証を実行できます。基本認証では、パスワード、PIN、または顧客番号といった何らかのタイプの認証情報を提供するよう、ユーザーに要求します。ユーザーの名前と認証情報を、妥当性検査リストに中に安全に保管しておくことができます。ICS のすべてのユーザーにシステム・ユーザー ID とパスワードを持たせる代わりに、ICS は妥当性検査リストからこの情報を使用することができます。

インターネット・ユーザーは、Web サーバーからシステムにアクセスすることを許可または拒否されます。しかし、ユーザーはシステム資源に対する権限、またはサインオンしたりジョブを実行する権限を持っていません。システム・ユーザー・プロファイルは、インターネット・ユーザーに対しては決して作成されません。

妥当性検査リスト・オブジェクトはすべてのアプリケーションで使用できます。たとえば、アプリケーションがパスワードを必要とする場合、アプリケーション・パスワードをデータベース・ファイルの中ではなく、妥当性検査リスト・オブジェクトの中に保管しておくことができます。アプリケーションは、自ら妥当性検査を実行する代わりに、妥当性検査リスト API を使って (暗号化された) ユーザー・パスワードを検査することができます。

妥当性検査リスト・オブジェクトの詳細については、*「iSeries 機密保護解説書」*の第 7 章『妥当性検査リスト・オブジェクトの使用の計画』を参照してください。

メニュー・セキュリティー

メニュー・セキュリティーは、ユーザーがどのメニュー機能を実行できるかを制御します。

このシステムは、本来、S/36 や S/38 の後継製品として設計されたものです。現在導入されているシステムの場合、それ以前には S/36 または S/38 が導入されていました。ユーザーの作業を制御するために、これらの初期システムの機密保護管理者は、多くの場合、メニュー・セキュリティーまたはメニュー・アクセス制御と呼ばれる技法を使用していました。

メニュー・アクセス制御とは、ユーザーがサインオンしたときに、メニューを表示するという意味です。ユーザーはメニュー上の機能しか実行できません。ユーザーは、システムのコマンド行を使用しても、メニューに表示されていない機能を実行することはできません。理論上は、メニューやプログラムがユーザーの操作を制御するので、機密保護管理者は、オブジェクトに対する権限について心配する必要はありません。

注: 任意のネットワーク・インターフェースがアクセスすることを許可しているシステムでは、メニューは保護されません。こうしたインターフェースのほとんどは、メニュー・セキュリティーを全く識別しません。

関連概念

234 ページの『メニュー・セキュリティーの設定』
この項では、メニュー・セキュリティーを設定するためのユーザー・プロファイル・パラメーターについて説明します。

ユーザー・セキュリティー

ユーザーの視点から見ると、セキュリティーは、ユーザーがシステム上でタスクを使用および完了する仕方に影響を与えます。

ユーザー・セキュリティーには、ユーザーが自分のタスクを完了するためにどのようにシステムと対話するかという要素が含まれます。このため、セキュリティーがユーザーの視点からどのように見えるかを考慮することが大切です。たとえば、パスワードの有効期限が 5 日ごとに切れるように設定した場合、ユーザーは不満感を持ち、作業の完了が妨げられるかもしれません。一方、パスワード・ポリシーが極端にあいまいな場合は、セキュリティーの問題を引き起こしかねません。

システムに適切なセキュリティーを設けるためには、計画、管理、および監視という 3 つの具体的な部分にセキュリティーを分ける必要があります。ユーザーの視点から見ると、システムのセキュリティーをいくつかの部分に分けることができます。

ユーザー・セキュリティーには、セキュリティーがユーザーに影響を与えるすべての領域、およびユーザーがシステムに影響を与えるすべての領域が含まれます。ユーザー・セキュリティーの主な構成要素は、次のとおりです。

- **システムへの物理的なアクセス**

  物理的セキュリティーは、システム装置、システム上にあるすべての装置、および (ディスケット、テープ、CD などの) バックアップ記憶媒体が、意図されずに、または意図的に失われたり損傷を受けたりするのを防ぎます。システムの物理的セキュリティーを確保するために取るほとんどの手段は、システムに対して外部的なものです。しかし、出荷されるシステムには、システム装置で許可なく機能が使用されるのを防止する、キーロックや電子キースティックが装備されています。

- **ユーザーがサインオンする方法**

  サインオン・セキュリティーは、システム上で未確認のユーザーがサインオンするのを防ぎます。各ユーザーがサインオンするためには、有効な信用証明情報 (たとえばユーザー ID とパスワードの有効な組み合わせ) を提示しなければなりません。サインオン・セキュリティーが侵害されていないかどうかは、システム値と個々のユーザー・プロファイルの両方で確認することができます。たとえば、パスワードを定期的に変更するように指示することができます。また、容易に推測されるパスワードの使用を防止することもできます。

- **ユーザーに許可される操作**

  セキュリティーおよびシステム・カスタマイズの重要な役割は、ユーザーが実行できる操作を定義することです。セキュリティーの視点から言えば、多くの場合、機能制限が使用されます (たとえば、ユーザーが特定の情報を見ることを禁止する)。システムのカスタマイズの視点から言えば、機能許可が使用されます。適切にカスタマイズされたシステムでは、不必要な作業と情報を除去することによって、ユーザーが効率的に作業を行うことができます。ユーザーに許可する操作を定義するには、機密保護担当者が適切な手法を使用する場合もあれば、プログラマーの責任で手法を実装する場合もあります。ここでは主に、機密保護担当者が通常行う事柄に焦点を当てて説明します。システム上でユーザーが実行できる操作を制御するために、個々のユーザー・プロファイル、ジョブ記述、およびクラスでパラメーターを使用することができます。下のリストは、使用可能な手法を簡単に説明しています。

  – 数少ない機能にユーザーを制限する

    ユーザー・プロファイルに基づいて、特定のプログラム、メニューまたはメニューのセット、および少数のシステム・コマンドだけを使用できるようにユーザーを制限することができます。通常は、機密保護担当者がユーザー・プロファイルを作成および制御します。

  – システム機能を制限する

    システム機能を使用すると、情報の保管と復元、プリンター出力の管理、および新しいシステム・ユーザーの設定を行うことができます。各ユーザー・プロファイルは、最も一般的なシステム機能のうち、どの機能をユーザーが実行できるかを指定します。システム機能を実行するために、制御言語 (CL) コマンドおよび API が使用されます。各コマンドおよび API はオブジェクトであるため、誰がそれらを使用してシステム機能を完了することができるかを制御するために、オブジェクト権限を使用できます。

  – ファイルおよびプログラムを使用できるユーザーを決定する

    資源保護には、システム上のすべてのオブジェクトの使用を制御する機能があります。どのオブジェクトにも、それを使用できるユーザーとその使用方法を指定することができます。たとえば、1 人の

ユーザーには、あるファイルの中の情報を見ることのみを許可し、別のユーザーにはファイル内のデータを変更できるように、また 3 番目のユーザーにはファイルを変更したり、ファイル全体を削除したりできるように指定することができます。

– システム資源の乱用を防止する

システムの処理能力は、企業にとって、システムに保管されるデータと同じほど重要な要素になり得ます。ユーザーがジョブを高い優先順位で実行したり、報告書を最初に印刷したり、過度に多くのディスク記憶領域を使用するなど、システム資源を誤用することがないように管理する上で、機密保護担当者は役割を果たします。

- システムを他のコンピューターと通信させる方法

システムが他のコンピューターやプログラム式ワークステーションと通信する場合、付加的なセキュリティーの手段が必要かもしれません。適切なセキュリティー制御を行わない場合、ネットワーク上の他のコンピューターのユーザーが、サインオン・プロセスなしでこのコンピューター上でジョブを開始したり、このコンピューター上の情報にアクセスする可能性があります。システム値とネットワーク属性の両方を使用して、リモート・ジョブ、データのリモート・アクセス、またはシステム上でのリモート PC アクセスを許可するかどうかを制御できます。リモート・アクセスを許可する場合は、どんなセキュリティーを施行するかを指定できます。すべてのシステム値に関する説明は、*「iSeries 機密保護解説書」*の第 3 章『セキュリティー・システム値』にあります。

- セキュリティー情報を保管する方法

システムの情報を定期的にバックアップする必要があります。システム上のデータを保管することに加えて、セキュリティー情報も保管しなければなりません。万一災害が起きた場合は、システム・ユーザー情報、権限情報、および情報そのものを回復する必要があります。

- セキュリティーの計画を監視する方法

システムには、セキュリティーの効果を監視するためのいくつかのツールがあります。

– 特定のセキュリティー違反が起きた場合は、システム操作員にメッセージが送られます。

– さまざまなセキュリティー関連のトランザクションを、特別な監査ジャーナルに記録することができます。

『セキュリティーの監視』には、これらのツールの使用方法がわかりやすく説明されています。セキュリティー監査の詳細については、*「iSeries 機密保護解説書」*の第 9 章『iSeries システムのセキュリティーの監査』を参照してください。

- システムのセキュリティーをカスタマイズする方法

ユーザーが日常の作業を行いやすくするために、システムをカスタマイズすることができます。ユーザーにとって最も使いやすいようにシステムをカスタマイズするには、作業を正常に実行するためにユーザーが何を必要としているかを考えてください。メニューおよびアプリケーションを表示するようにシステムをカスタマイズするには、次のような方法があります。

– ユーザーが必要だと感じるものを表示する

私たちはほとんどの場合、自分の机やオフィスを整理する際に、一番よく使うものを自分の手の届きやすいところに置きます。システムに対するユーザーのアクセスについても、これと同じように考えることができます。ユーザーがシステムにサインオンした後、まずメニューやそのユーザーが最もよく使う画面が最初に表示されなければなりません。このようにするためのユーザー・プロファイルは、容易に設計することができます。

– 不要なアプリケーションを除外する

ほとんどのシステムには、数多くのさまざまなアプリケーションがインストールされています。しかし、ほとんどのユーザーが見たいのは、自分の作業に必要なものだけです。システム上でユーザーが使用する機能をいくつかに制限するなら、ユーザーは作業を実行しやすくなります。ユーザー・プロファイル、ジョブ記述、および適切なメニューを使用して、システムの特定の表示を各ユーザーに提供することができます。

– 適切な場所に出力を送る

どのようにして報告書を適切な印刷装置に送ることができるか、またはどのようにバッチ・ジョブを実行すればよいかを、ユーザーが心配するようなことがあってはなりません。システム値、ユーザー・プロファイル、およびジョブ記述を使って、それらを適切に設定することができます。

– 援助を提供する

どんなに適切にシステムをカスタマイズしても、ユーザーたちは依然として、「私の報告書はどこへ行ったのだろう」、「私のジョブはもう実行されたのだろうか」といった疑問を抱くものです。操作援助機能の画面には、システム機能への簡単なインターフェースがあり、ユーザーがこれらの疑問に対する答えを得る上で役立ちます。操作援助レベルと呼ばれる複数のバージョンのシステム画面は、技術的な経験レベルがさまざまに異なるユーザーを援助します。操作援助機能の画面は、システム導入時にすべてのユーザーに対して自動的に使用可能になります。ただし、アプリケーションの設計によっては、ユーザーが操作援助機能のメニューにアクセスする方法を変更する必要があるかもしれません。提供されているシステム・ツールを使用すれば、ユーザーが資源にアクセスすることを許可しながら資源を保護するよう、システムのセキュリティーをカスタマイズできます。

関連概念

113 ページの『ユーザー・セキュリティーの設定』
ユーザー・セキュリティーの計画には、 セキュリティーがシステム上のユーザーに影響を与えるすべての分野の計画が含まれます。

210 ページの『ユーザー・セキュリティーの設定』
ユーザー・セキュリティーの設定には、アプリケーション・ライブラリーの導入、およびユーザー・グループとプロファイルの設定が含まれます。

276 ページの『セキュリティー情報の保管』
このトピックでは、セキュリティー情報を保管および復元する方法の概要を示します。

関連情報

バックアップおよび回復の手引き (PDF)

資源保護

認証に成功した後に許可ユーザーが行う処置を制御するために、システムの資源保護を使用することができます。

システム値とユーザー・プロファイルは、システムにアクセスするユーザーを制御し、許可のないユーザーがサインオンできないようにします。資源保護は、許可されたシステム・ユーザーが正常にサインオンした後に実行できるアクションを制御します。資源保護は、システム・セキュリティーの主な目的に沿って、以下のものを保護します。

- 情報の機密性
- 情報の正確さ (許可なく変更できないようにする)
- 情報の可用性 (不慮または故意に損傷を与えないようにする)

機密保護担当者は、資源を使用する権限を持つユーザーと、ユーザーが資源にアクセスする方法を決定することにより、システム上の資源 (オブジェクト) を保護します。機密保護担当者は、個々のオブジェクトやオブジェクトのグループに対するオブジェクト権限を設定できます (権限リスト)。保護が必要なオブジェクトとして最も一般的なものは、ファイル、プログラム、ライブラリーですが、システム・セキュリティーでは、システム上のすべてのオブジェクトに対してオブジェクト権限を指定できます。

単純な手法を前もって計画しておけば、資源保護を簡単に、しかも効果的に管理することができます。事前の計画なしで作成された資源保護の体系は、複雑で、効果の無いものになる可能性があります。

システムの資源保護を使用すれば、どんなユーザーがオブジェクトを使用できるか、およびオブジェクトに対してどんな操作を実行できるかを定義できます。オブジェクトにアクセスできることを権限と呼びます。オブジェクト権限を設定するときには、ユーザーが自分たちの作業を十分に実行でき、しかもシステムの表示や変更が不可能な権限を与えるよう、よく考慮してください。オブジェクト権限は、特定のオブジェクトに関する許可をユーザーに与え、そのオブジェクトに対してユーザーは何ができるかを指定できます。具体的で詳細なユーザー権限 (たとえばレコードの追加や変更) を介して、オブジェクト資源を制限できます。システム資源を使用して、*ALL、*CHANGE、*USE、*EXCLUDE といった、特定のシステム定義の権限のサブセットへのアクセスをユーザーに与えることができます。

資源保護を必要とする最も一般的なシステム・オブジェクトはファイル、プログラム、ライブラリー、ディレクトリーですが、システム上のすべてのオブジェクトに対して権限を指定できます。

システムには、単純な資源保護の体系を設計する上で役立つツールがいくつかあります。

グループ・プロファイル
よく似た権限を必要とする複数のユーザーを、1 つのグループ・プロファイルの下にグループ化することができます。すると、グループ内の特定ユーザーに特定権限を定義しない限り、グループ内のすべてのユーザーは同じ権限を共有してオブジェクトを使用できます。

権限リスト
権限リストを使用して、セキュリティー要件の類似した複数のオブジェクトをグループ化することができます。その後、個々のオブジェクトにではなく、このリストに対して権限を与えることができます。権限リストには、ユーザーのリストのほか、権限リストによって保護されるオブジェクトに対するそれらのユーザーの権限が含まれます。また、権限リストを使用して、リスト上のオブジェクトに対する共通権限を定義することもできます。オブジェクトに対する共通権限が *AUTL に設定される場合、オブジェクトは共通権限を権限リストから得ます。ユーザー・プロファイルまたは他の権限リストを保護するために権限リストを使用することはできません。さらに、1 つのオブジェクトに対して 1 つの権限リストだけを指定できます。詳しくは、*「iSeries 機密保護解説書」*の『権限リスト・セキュリティー』を参照してください。

妥当性検査リスト
妥当性検査リスト・オブジェクトは、アプリケーションがユーザー認証情報を安全に保管するための方式を提供します。

ユーザー権限
個々のユーザー・プロファイルに対して、オブジェクトにアクセスし、かつこれを利用する特定権限を定義できます。少数のユーザーのアクセス要件がグループの要件に一致しないような場合には、ユーザー権限を使用すると役立ちます。

オブジェクト所有権
システム上のすべてのオブジェクトには所有者が存在し、所有者は、デフォルトでオブジェクトに対する *ALL 権限を持っています。グループ・プロファイルまたは個々のユーザー・プロファイルがオブジェクトを所有できます。オブジェクトに所有者が存在しない場合、またはオブジェクト

所有権がセキュリティー上のリスクを発生させる可能性がある場合には、システムは IBM 提供のデフォルト所有者 (QDFTOWN) というユーザー・プロファイルにオブジェクト所有権を割り当てます。ユーザーがオブジェクトを作成すると、そのユーザーがオブジェクトの所有者となります。ただし、そのユーザーが、自分の属するグループ・プロファイルをオブジェクト所有者として指定する場合は例外です。オブジェクトに対する所有者の権限を変更または除去することができます。オブジェクト所有権を正しく割り当てておけば、アプリケーションを管理し、情報のセキュリティーの担当を委任する上で役立ちます。詳しくは、「*iSeries 機密保護解説書*」の『オブジェクト所有権』を参照してください。

1 次グループ権限

オブジェクトに 1 次グループを指定し、その 1 次グループの持つ権限をそのオブジェクトに指定することができます。1 次グループ・プロファイルの名前およびオブジェクトに対する 1 次グループの権限は、そのオブジェクトとともにシステムによって保管されます。グループ・プロファイルを使用する場合に比べて、1 次グループ権限を使用すると権限の管理が単純になり、権限検査のパフォーマンスを向上させることができます。グループ識別番号 (*gid*) を持つユーザー・プロファイルだけが、オブジェクトの 1 次グループになれます。オブジェクト所有者とそのオブジェクトの 1 次グループに同じプロファイルを指定することはできません。詳しくは、「*iSeries 機密保護解説書*」の『オブジェクトのグループ所有権』を参照してください。

ライブラリー権限

システム上の多くのオブジェクトは、ライブラリーに存在します。ライブラリー内のオブジェクトにアクセスするには、オブジェクト自体、およびオブジェクトが入っているライブラリーに対する権限が必要です。保護要件が類似している複数のファイルおよびプログラムを 1 つのライブラリーに入れて、そのライブラリーに対するアクセスを制限することができます。ほとんどの場合、このようにした方が、各オブジェクトに対するアクセスを個々に制限するよりも簡単です。ただし、高度なセキュリティーを必要とするデータを保護するには、ライブラリーのセキュリティーは不十分かもしれません。機密性の高い重要なオブジェクトを保護するためには、ライブラリーのセキュリティーだけに依存するのではなく、個々のオブジェクトを保護するか、権限リストを使用するのが適切でしょう。詳しくは、「*iSeries 機密保護解説書*」の『ライブラリー・セキュリティー』を参照してください。

ディレクトリー権限

ディレクトリー内のオブジェクトにアクセスするときには、オブジェクトのパスに含まれるすべてのディレクトリーに対する権限が必要です。さらに、オブジェクトに対して、要求した操作を実行するのに必要な権限も持っていなければなりません。ディレクトリー権限は、ライブラリー権限と同じ方法で使用することができます。1 つのディレクトリー内のオブジェクトをグループ化して、個々のオブジェクトではなくそのディレクトリーを保護することができます。たとえば、ディレクトリーへのアクセスを制限して、ディレクトリー内のオブジェクトに対して共通権限を使用することができます。このように、オブジェクトに対して定義する特定権限の数を少なくすると、権限検査プロセスのパフォーマンスが向上します。

オブジェクト権限

ライブラリーやディレクトリーへのアクセスが十分に特定されていない場合、またはライブラリーやディレクトリーの中の特定のオブジェクトのアクセス要件が一般的なライブラリーやディレクトリーと異なる場合には、個々のオブジェクト (たとえばファイル) に対する権限を制限することができます。オブジェクトに対する権限は、以下の 3 つのカテゴリーに分類されます。

1. オブジェクト権限は、ユーザーまたはプログラムがオブジェクト全体に実行できる操作を定義します。
2. データ権限は、ユーザーまたはプログラムがオブジェクトの内容に対して実行できる操作を定義します。

3. フィールド権限は、ユーザーまたはプログラムがデータ・フィールドに対して実行できる操作を定義します。

オブジェクト権限の種類について、詳しくは「*iSeries 機密保護解説書*」の『情報にアクセスする方法の定義』を参照してください。

共通権限

共通権限は、システムへのサインオン権限を持つすべてのユーザーを対象とし、オブジェクトに対する他の権限を持たないすべてのユーザーがどのようにオブジェクトを利用できるかを定義します。システム上のすべてのオブジェクトに対する共通権限を定義できます。同時に、特定のオブジェクトに対する共通権限を *EXCLUDE にすることもできます。オブジェクトに対するより具体的な権限が見つからない場合、システムは、そのオブジェクトに対する共通権限を使用します。共通権限は、機密性のないオブジェクトを保護する上で効果的な手段であり、システム・パフォーマンスの点でも優れています。

借用権限

借用権限は、プログラムを実行するユーザーの権限に、プログラム所有者の権限を追加します。借用権限は、状況によってユーザーがオブジェクトに対するさまざまな権限を必要とするような場合に便利なツールです。オブジェクトやアプリケーションを処理する状況に応じて、ユーザーがオブジェクトやアプリケーションに対する異なる権限を必要とする場合があります。たとえば、カスタマー・ファイルの情報を変更する機能を持つアプリケーション・プログラムをユーザーが実行するとき、そのような変更を行うことをユーザーに許可するのが適切でしょう。しかし、その同じユーザーが SQL などの意思決定サポート・ツールを使用するときには、顧客情報の表示だけを許可し、情報の変更を許可しないようにすべきです。このような状況を解決するには、顧客情報に対する *USE 権限をユーザーに与えてファイル照会を可能にすると同時に、顧客保守プログラムの中で借用権限を使用して、そのプログラムを実行中のユーザーにファイルの変更を許可することができます。オブジェクト・タイプ *PGM、*SRVPGM、*SQLPKG、および Java™ プログラムが権限を借用できます。詳しくは、「*iSeries 機密保護解説書*」の『所有者の権限を借用するオブジェクト』を参照してください。

権限ホルダー

権限ホルダーは、現在システム上に存在しないプログラム記述データベース・ファイルに対する権限を保持するためのツールです。権限ホルダーは、プログラム記述ファイルの削除と再作成を頻繁に行う System/36™ 環境アプリケーションで主に使用されます。権限ホルダーは、アプリケーションが処理中に削除/作成するプログラム記述データベース・ファイルに対する権限情報を保管します。ユーザーまたはプログラムがオブジェクトを削除すると、そのオブジェクトの権限情報も削除されます。権限ホルダーを使用すれば、プログラムがオブジェクトを削除しても権限情報が確実に保持されます。オブジェクトが削除されると、そのオブジェクトの権限情報も削除されます。権限ホルダーを最もよく使用するのは、System/36 からの変換時です。System/36 アプリケーションはファイルの削除と再作成を頻繁に行うためです。詳しくは、「*iSeries 機密保護解説書*」の『権限ホルダー』を参照してください。

フィールド権限

データベース・ファイル内の個々のフィールドに、「参照」または「更新」のフィールド権限を与えることができます。フィールド権限を使用することにより、データベース・ファイルを保護すると同時に、そのファイル内の特定のフィールドを適切な形で使用可能にすることができます。フィールド権限を管理するには、SQL ステートメント GRANT および REVOKE だけを使用できます。詳しくは、「*iSeries 機密保護解説書*」の『フィールド権限』を参照してください。

関連概念

125 ページの『資源保護の計画』
このトピックでは、それぞれの資源保護の構成要素について、またシステムの情報を保護するためそれ

らすべての構成要素がどのように相互に機能するかについて説明します。また、システム上での資源保護を設定するための、CL コマンドと表示画面の使用方法についても説明します。

224 ページの『資源保護のインプリメント』
以下の情報を参考にすれば、オブジェクトの所有権と共通権限、およびアプリケーションに対する特定権限を設定することにより、ワークステーションとプリンターの資源保護を確立できます。

システム・セキュリティー・ツール

セキュリティー・ツールを使用すれば、システムのセキュリティー環境を管理および監視することができます。

セキュリティー・ツールは i5/OS に含まれています。セキュリティー・ツールはいくつかのコマンドとプログラムから構成され、次のような 2 つのメインメニューを介して管理できます。

- セキュリティー・コマンドを対話式に実行するための「セキュリティー・ツール (SECTOOLS) メニュー
- セキュリティー報告書コマンドをバッチで実行するための「セキュリティー報告書のバッチ処理投入またはスケジュール」(SECBATCH) メニュー

これらのセキュリティー・ツールを使って、ユーザー・プロファイルとの併用、セキュリティー監査の制御、セキュリティー報告書の出力、およびシステム・セキュリティーのカスタマイズを行うことができます。たとえば、セキュリティー・ユーザー・プロファイル・ツールを使用すれば、以下が可能になります。

- デフォルトのパスワードを使用しているユーザー・プロファイルの検出。
- 1 日または 1 週間のうちの特定の時間、ユーザー・プロファイルを使用できないようにするスケジュール。
- 従業員が退職した場合に、そのユーザー・プロファイルを除去するスケジュール。
- 特殊権限を持つユーザー・プロファイルの検出。
- システム上のオブジェクトに対する権限を借用しているユーザーの検出。

オブジェクト・セキュリティー・ツールを使用して、機密オブジェクトに関連付けられた共通権限および私用権限を追跡することができます。これらの報告書を定期的に印刷するよう設定すれば、現在の問題に焦点を絞ったセキュリティー対策を立てる上で役立ちます。また、報告書を前回実行したときからの変更点だけを表示するように報告書を実行することもできます。

他のツールには、次のものを監視する機能があります。

- トリガー・プログラム
- 通信の項目にあるセキュリティー関連の値、サブシステム記述、出力待ち行列、ジョブ待ち行列、およびジョブ記述
- 更新または改ざんされたプログラム

システム・セキュリティー・ツールの使用方法について、詳しくは「*iSeries 機密保護解説書*」の付録 G 『セキュリティー・コマンドのコマンドおよびメニュー』を参照してください。

関連概念

299 ページの『セキュリティー・ツールを使用するためのシステム構成』
この章では、i5/OS の 一部であるセキュリティー・ツールを使用するためのシステムのセットアップ方法について説明します。

セキュリティー監査

このトピックでは、セキュリティー監査の目的について取り上げます。

システムのセキュリティーを監査する必要があるのは、以下のようないくつかの理由のためです。

- セキュリティー計画が完全であるかどうかを評価するため。
- 計画されたセキュリティー管理が適切で機能していることを確認するため。このタイプの監査は、通常、日単位のセキュリティー管理の一部として機密保護担当者によって行われます。さらに、内部または外部の監査員により、定期的なセキュリティーの検討の一部として、より詳細に実行されることもあります。
- システム環境の変更にシステム・セキュリティーが対応しているかどうかを確認するため。セキュリティーに影響する変更には、次のようなものがあります。
  - システム・ユーザーによる新規オブジェクトの作成
  - システムへの新規ユーザーの許可
  - オブジェクト所有権の変更 (権限の調整なし)
  - 責任の変更 (ユーザー・グループの変更あり)
  - 一時的な権限 (適時での取り消しなし)
  - 新しいプロダクトの導入
- 新しいアプリケーションの導入、より高いセキュリティー・レベルへの移動、通信ネットワークの設定など、将来の事象に備えるため。

ここで説明する技法は、これらのすべての状態に当てはまります。監査する対象およびその頻度は、組織のサイズおよびセキュリティーの必要性によって決まります。

セキュリティー監査には、システムにおけるコマンドの使用と、ログ情報およびジャーナル情報へのアクセスが含まれます。システムのセキュリティー監査を行う人が使用する特別なプロファイルを作成することもできます。監査員プロファイルには、システムの監査特性を変更するための *AUDIT 特殊権限が必要です。この章で推奨している監査タスクの中には、*ALLOBJ および *SECADM 特殊権限のあるユーザー・プロファイルを必要とするものがあります。監査期間が終了したら、監査員プロファイルのパスワードを *NONE に設定します。

セキュリティー監査についての詳細は、「*iSeries 機密保護解説書*」の第 9 章『システムのセキュリティーの監査』を参照してください。

関連概念

99 ページの『システム値の監査』
このトピックでは、システム値の監査の詳細について説明します。

315 ページの『セキュリティー監査の計画』
この情報を使用して、ご使用のシステムのセキュリティー監査の計画を立てます。

権限のタイプ

この項では、サーバー上で許可されて使用される権限のタイプについて説明します。

このシステムでは、様々なタイプのユーザーの権限が提供されています。**権限**とは、オブジェクトに対して許可されるアクセスのタイプです。操作に応じて、異なるタイプの権限が必要になります。たとえば、システム上の情報を表示したり変更したりする権限があります。システムには数種類の権限タイプがあります。IBM では、これらの権限タイプを**システム定義の権限**および**特殊権限**というカテゴリーにグループ化しています。

オブジェクトに対するシステム定義の権限は、3 つのカテゴリーに分類できます。

オブジェクト権限
オブジェクト全体に実行できる操作を定義します。

データ権限
オブジェクト内容に対して実行できる操作を定義します。

フィールド権限
データ・フィールドで実行できる操作を定義します。

特殊権限を使用して、ユーザーがシステム資源に実行できる処置のタイプを指定します。ユーザーは 1 つ以上の特殊権限を受けることができます。システム・セキュリティー・レベルは、各ユーザー・クラスに許可されるデフォルトの特殊権限を決定します。ユーザー・プロファイルを作成するとき、ユーザー・クラスに基づいて特殊権限を選択できます。さらに、セキュリティー・レベルの変更時にも、特殊権限がユーザー・プロファイルに追加および除去されます。

資源権限の設定についての詳細は、「*iSeries 機密保護解説書*」の第 5 章『システムによる権限の検査』を参照してください。

システム定義の権限

この表は、ファイル、プログラム、ライブラリーを保護するために、システム定義による権限がどのように適用されるかを示します。

この情報を参考にして、システム定義による権限を計画してください。単純な資源保護を設計するには、ライブラリー全体のセキュリティーの計画を立ててください。以下の表は、ファイル、プログラム、ライブラリーを保護するために、システム定義権限がどのように適用されるかを示します。

表 2. システム定義の権限

	***USE 権限**	***CHANGE 権限**	***ALL 権限**	***EXCLUDE[1] 権限**
許可されているファイル操作	ファイル中の情報の表示。	ファイル中のレコードの表示、変更、および削除。	ファイルの作成および削除。ファイル中のレコードの追加、変更、および削除。他人がファイルを使用する権限。	なし
許可されていないファイル操作	ファイル中の情報の変更または削除。ファイルの削除。	ファイル全体の削除または消去。	なし	ファイルに対するすべてのアクセス。
許可されているプログラム操作	プログラムの実行。	プログラムの記述の変更。	プログラムの作成、変更、および削除。他人がプログラムを使用する権限。	なし
許可されていないプログラム操作	プログラムの変更または削除。	プログラムの変更または削除。	プログラム借用権限の場合は、プログラムの所有者の変更。	プログラムに対するすべてのアクセス。

表 2. システム定義の権限 (続き)

	*USE 権限	*CHANGE 権限	*ALL 権限	*EXCLUDE[1] 権限
許可されているライブラリー操作	• ライブラリー内のオブジェクトの場合、権限によって許可されている、特定のオブジェクトに対するすべての操作。 • ライブラリーの場合、記述情報の表示。	• ライブラリー内のオブジェクトの場合、権限によって許可されている、特定のオブジェクトに対するすべての操作。 • ライブラリーへの新規オブジェクトの追加。 • ライブラリー記述の変更。	• 変更権限によって許可されるすべての処理。 • ライブラリーの削除。 • ライブラリーに対する権限を他のユーザーに付与。	なし
許可されていないライブラリー操作	• ライブラリーへの新規オブジェクトの追加。 • ライブラリー記述の変更。 • ライブラリーの削除。	ライブラリーの削除。	なし	ライブラリーに対するすべてのアクセス。

1 *EXCLUDE は、共通権限やグループ・プロファイルを介して認可された権限をすべてオーバーライドします。

オブジェクト権限とライブラリー権限が協働する仕方についての理解

ライブラリー権限とオブジェクト権限が協働する仕方についても理解する必要があります。以下の表には、オブジェクトとライブラリーの両方に必要な権限の例が示されています。

表 3. ライブラリー権限とオブジェクト権限が協働する仕方

オブジェクト・タイプ	操作	必要なオブジェクト権限	必要なライブラリー権限
ファイル	データの変更	*CHANGE	*EXECUTE
ファイル	ファイルの削除	*OBJOPR、*OBJEXIST	*EXECUTE
ファイル	ファイルの作成	なし	*EXECUTE、*ADD
プログラム	プログラムの実行	*USE	*EXECUTE、*OBJOPR
プログラム	プログラムの再コンパイル	*OBJEXIST、*OBJMGR、*READ	*ADD、*READ
プログラム	プログラムの削除	*OBJEXIST	*EXECUTE

これで、オブジェクト、ディレクトリー、およびライブラリーの特定権限を設定する準備ができました。使用可能な権限の種類、および権限の使用例については、「*iSeries 機密保護解説書*」の第 1 章『資源保護』および付録 D『コマンドで使用するオブジェクトに必要な権限』を参照してください。

関連概念

232 ページの『オブジェクト用およびライブラリー用の特定権限の設定』

オブジェクト権限編集 (EDTOBJAUT) コマンドを使用して、ライブラリーおよびライブラリー内のオブジェクトの特定権限を指定できます。

特殊権限

このトピックでは、ユーザーに対して指定できる特殊権限を説明します。

システム・セキュリティー・レベルは、各ユーザー・クラスに許可されるデフォルトの特殊権限を決定します。ユーザー・プロファイルを作成するとき、ユーザー・クラスに基づいて特殊権限を選択できます。さらに、セキュリティー・レベルの変更時にも、特殊権限がユーザー・プロファイルに追加および除去されます。

以下の特殊権限をユーザーに対して指定できます。

***ALLOBJ**
全オブジェクト特殊権限は、オブジェクトに対するすべての操作を実行する権限をユーザーに与えます。

***AUDIT**
監査特殊権限を使用すれば、システム、オブジェクト、およびシステム・ユーザーの監査特性を定義できます。

***IOSYSCFG**
システム構成特殊権限により、通信、およびシステム上の入出力装置を構成することができます。

***JOBCTL**
ジョブ制御特殊権限は、システムでのバッチ・ジョブおよび印刷の制御を可能にします。

***SAVSYS**
システム保管特殊権限は、オブジェクトの保管および復元を可能にします。

***SECADM**
機密保護管理者特殊権限は、システム上でのユーザー・プロファイルの処理を可能にします。

***SERVICE**
サービス特殊権限は、システム上でソフトウェア・サービス機能を可能にします。

***SPLCTL**
スプール制御特殊権限は、システムでのバッチ・ジョブおよび出力待ち行列の無制限の制御を可能にします。

特殊権限の詳細については、「*iSeries 機密保護解説書*」の『システム・セキュリティー (QSecurity) システム値の使用方法』を参照してください。

関連概念

342 ページの『特殊権限のモニター』
このトピックでは、特殊権限のモニターに使用する SECBATCH メニュー・オプションおよびコマンドについて説明します。

324 ページの『機密保護担当者の処置の監査』
機密保護担当者または機密保護管理者には、 システムのセキュリティーについての責任があります。機密保護担当者には、*ALLOBJ および *SECADM 特殊権限があります。

侵入の検知

侵入の検知には、TCP/IP ネットワークを介して侵入してくる無許可アクセスの試行やハッキングに関する情報を収集することが関係しています。

侵入の検知という語は、iSeries 資料では 2 通りの方法で使用されています。最初の意味としては、侵入の検知とは機密漏れの防止および検出のことを指します。たとえば、ハッカーが無効なユーザー ID を使用

してシステムに入り込もうとする場合や、多くの権限を与えられ過ぎている経験のないユーザーがシステム・ライブラリー内の重要なオブジェクトを変更しようとする場合などがあります。

2 番目の意味としては、侵入の検知はポリシーを使用してシステム上の疑わしいトラフィックをモニターする新しい侵入検知機能について言及しています。TCP/IP ネットワークを介して侵入する疑わしい侵入イベントを監査する侵入検知ポリシーを作成できます。

関連情報

侵入の検知

eServer Security Planner

この情報では、eServer Security Planner と、その価値を説明します。

IBM eServer Security Planner を使用すると、IBM サーバーがサポートしている各オペレーティング・システム (AIX®、Linux®、i5/OS、Microsoft® Windows® 2000、および z/OS® が含まれます) 用の基本的なセキュリティー・ポリシーを計画する上で役立ちます。Security Planner は、お客様のビジネス環境およびセキュリティー・ゴールについて一連の質問を行います。Security Planner は応答を基にして、パスワード規則、資源アクセス規則、ロギング規則および監査規則の各設定、および他の OS 特有のセキュリティー設定に関する推奨事項のリストを提供します。

Security Planner は提案した構成を実行することはできません。その代わりに、Security Planner は IBM サーバーにセキュリティーを計画してインプリメントするためのガイドとなる情報やチェックリストを提供します。場合によっては、Security Planner は推奨ポリシーを適用するために実行できるコマンド付きプログラムを備えることもあります。現在 Security Planner は、各 OS 用のネットワーク・セキュリティー推奨事項を提供します。ネットワーク・セキュリティーの設計の基本概念 (ネットワーク体系、ファイアウォールや他のネットワーク・セキュリティー・テクノロジー、TCP/IP セキュリティー、および侵入の検知が含まれます) について確認してください。

類似したセキュリティー特性と要件を有する e-business 環境のサーバーの各グループごとに、Security Planner を一度ずつ実行する必要があります。実行するたびに、お客様の必要に特有の基本的なセキュリティー・ポリシーが生成されます。たとえば、主幹業務の実動システムで十分に機密保護機能のある環境が必要であるものの、会社の内部開発システムでのリスクに対してはより寛大であるとします。この場合、それぞれで必要なセキュリティー・レベルが異なるため、各システムに対して 1 度ずつ、合計 2 度 Security Planner を実行します。

全体的なセキュリティー戦略の計画

このトピックでは、セキュリティー戦略の計画における種々の面について説明します。

貴社のセキュリティー値をセキュリティー・ポリシーに定義したなら、セキュリティー戦略の作成を開始できます。セキュリティー戦略は、貴社のセキュリティー・ポリシーをインプリメントする上で必要な計画作業すべてに対する体系的なアプローチを提供します。この目標を最善の仕方で成し遂げるには、最も基本的なセキュリティーの必要性から開始して、その後より具体的なセキュリティーについて扱う必要があります。

たとえば、以下の情報で扱う提案されているアプローチでは、ご使用のハードウェアと情報資産の物理的セキュリティーの計画から開始し、その後システム、ユーザー、資源、そしてネットワークの特定のセキュリ

ティーを計画します。ご自分のセキュリティー戦略を作成する際、最も一般的なセキュリティーから開始して、その後他の具体的なセキュリティー・ゴールに移ってください。各計画ステップは、順番に実行するように配置されています。

システムをカスタマイズするためのシステム値の使用

システムは、システム値とネットワーク属性を使用して、セキュリティー以外の数多くの事柄を制御します。システムおよびアプリケーション・プログラマーは、これらのシステム値と属性のほとんどを使用します。機密保護担当者は、システムをカスタマイズするために、いくつかのシステム値とネットワーク属性を設定する必要があります。

システムへの名前の割り当て

システムに名前を割り当てる際は、SYSNAME ネットワーク属性を使用します。システム名は、サインオン画面の右上角とシステムの報告書に表示されます。また、システム名はご使用のシステムが他のシステムと通信したり、iSeries Access for Windows を使用するパーソナル・コンピューターと通信する際にも使用されます。

ご使用のシステムが他のシステムやパーソナル・コンピューターと通信する際、システム名はネットワーク上の他のシステムとご使用のシステムを識別し、区別するものとなります。コンピューターは、通信を行う際にシステム名を交換します。システム名の変更はネットワーク上の他のシステムに影響を与えるため、いったんシステム名を割り当てた後に、それを変更しないでください。

システムには、意味があって、かつ固有な名前を割り当ててください。現在は他のコンピューターと通信していないかもしれませんが、将来通信を行うようになる可能性があります。ご使用のシステムがネットワークに属している場合は、おそらく、ネットワークの管理者から、使用するシステム名を指示されるでしょう。

システムの日付表示形式の選択

システムが日付を印刷または表示する際の、年、月、および日の順番を設定することができます。また、それぞれ年 (Y)、月 (M)、 および日 (D) の間にシステムが使用する文字を指定することができます。システム値 QDATFMT は、日付形式を決定します。次の表は、選択可能な値ごとに、 どのように日付 16 June 2000 が印刷されるかを示しています。

表 4. 日付および時刻の形式

実際の選択	説明	結果
YMD	年、月、日	00/06/16
MDY	月、日、年	06/16/00
DMY	日、月、年	16/06/00
JUL	年間通算日	00/168

注: 上の例では、スラッシュ (/) で日付を区切っています。

システム値 QDATSEP は、システムが年、月、日の間の区切り記号として用いる文字を決定します。下の表は、選択可能な値を示しています。区切り記号は、番号を使って選択します。

表 5. 日付区切り文字

区切り文字	QDATSEP の値	結果
/ (スラッシュ)	1	16/06/00

表 5. 日付区切り文字 (続き)

区切り文字	QDATSEP の値	結果
- (ハイフン)	2	16-06-00
. (ピリオド)	3	16.06.00
, (コンマ)	4	16,06,00
(ブランク)	5	16 06 00

注: 上の例では、DMY 形式を使用しています。

システムの時間表示形式の設定

QTIMSEP システム値は、システムが時間を表示する際に、時、分、および秒の区切り記号として使用する文字を決定します。区切り記号は、番号を使って選択します。下の表は、それぞれの値を選択した場合に、午前 10:30 がどのように表示されるかを示しています。

表 6. 時刻区切り文字

区切り文字	QTIMSEP	結果
: (コロン)	1	10:30:00
. (ピリオド)	2	10.30.00
, (コンマ)	3	10,30,00
(ブランク)	4	10 30 00

システム装置の命名方法の決定

ご使用のシステムでは、付加された新しい表示装置やプリンターを自動的に構成します。システムは、それぞれの新しい装置に名前を付けます。 QDEVNAMING システム値は、名前が割り当てられる方法を決定します。下の表は、システムが、 システムに付加された 3 番目の表示装置と 2 番目のプリンターをどのように命名するかを示しています。

表 7. システム装置の命名

実際の選択	命名形式	表示装置名	プリンター名
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	装置のアドレス	DSP010003	PRT010002

注: 上の例では、表示装置とプリンターが 1 番目のケーブルに接続されています。

推奨事項

S/36 の命名が必要なソフトウェアを実行していない限り、装置アドレスではなく命名規則を使用してください。表示装置とプリンターの名前は、装置のアドレスを使用した名前よりも分かりやすくなっています。表示装置とプリンターの名前は、いくつかの操作援助機能の画面で表示されます。また、プリンター名は、プリンター出力の管理にも使用されます。

システムが新しい装置を構成した後、表示装置の変更 (CHGDEVDSP) コマンドや、印刷装置の変更 (CHGDEVPRT) コマンドを使用して、分かりやすい装置の説明を入力してください。装置の説明には、装置の物理アドレスとロケーションの両方を含めてください。たとえば、John Smith のオフィス、回線 1 アドレス 6 などと入力します。

システム・プリンターの選択

QPRTDEV システム値を使用して、システム・プリンターを割り当てます。特定のジョブで使用するプリンターは、このシステム値、ユーザー・プロファイル、およびジョブ記述によって決定されます。ユーザー・プロファイルかジョブ記述で他のプリンターが指定されていない限り、ジョブはシステム・プリンターを使用します。

推奨事項

通常、システム・プリンターには、システム内で最も速いプリンターを使用します。長い報告書とシステム出力には、システム・プリンターを使用します。

注: プリンターの名前は、システムを導入し、構成するまで分かりません。ここではシステム・プリンターのロケーションをメモしてください。プリンターの名前については後で記入します。

完了したプリンター出力の表示の使用可能化

システムには、ユーザーのプリンター出力を検索する機能があります。「プリンター出力の処理」画面には、現在印刷されている、または印刷を待っているすべての出力が表示されます。また、完了したプリンター出力のリストを、ユーザーが表示できるようにすることもできます。

この画面は、いつ出力が印刷されたのか、およびどのプリンターで印刷されたのかを示します。これは、紛失した報告書を探すときに便利な機能です。ジョブ会計機能および QACGLVL システム値を使用すると、完了したプリンター出力を表示することができます。 QACGLVL システム値に *PRINT オプションを使用すると、完了したプリンター出力に関する情報を保管することができます。

完了したプリンター出力に関する情報を保管すると、システム上のスペースを消費します。ユーザーが多量の報告書を印刷することがなければ、おそらくこの機能は必要はないでしょう。システム値選択用紙には、NO と入力してください。この値は、ジョブ会計レベルを *NONE に設定します。

ユーザー・グループの計画の前に

- JKL Toy Company の例で、Sharon Jones と John Smith が作成したように、お客様の会社で、文章化されたセキュリティー・ポリシーを作成したことを確認してください。
- システム値選択用紙に、選択したシステム値が記入されていることを確認してください。
- セキュリティーのメモに含めたい点を、書き留めてください。

システム値選択用紙にすべてのシステム・オプションを記入し、 セキュリティー・ポリシーを作成したら、ユーザー・グループを計画することができます。

セキュリティー・ポリシーの開発

このトピックでは、セキュリティー・ポリシーを定義し、セキュリティー・ポリシーの作成プロセスについて説明します。

使用または提供する各インターネット・サービスは、システムとそれが接続されているネットワークにリスクを課します。**セキュリティー・ポリシー**とは、組織に所属するコンピューターおよび通信リソースに対す

る操作に適用される規則の集まりです。これらの規則は、物理的セキュリティー、人的セキュリティー、管理セキュリティー、およびネットワーク・セキュリティーなどの領域にわたります。セキュリティー・ポリシーでは、保護したいものと、システム・ユーザーに期待するものを定義しています。セキュリティー・ポリシーは、新規アプリケーションを設計したり、現行のネットワークを拡張する場合に、セキュリティー計画の基盤を提供します。セキュリティー・ポリシーには、機密情報の保護や重要なパスワードの作成など、ユーザーが行わなければならない作業が記述されます。

セキュリティー・ポリシーには、セキュリティー措置の効果をモニターする方法も記述しなければなりません。このようなモニターは、安全防護柵をすり抜けようとする人物がいるかどうかを判別するのに役立ちます。セキュリティー・ポリシーを作成するには、セキュリティーの目的を明確に定義しなければなりません。セキュリティー・ポリシーを立てたならば、そこに含まれる規則を実行に移すためのステップを取らなければなりません。

すべての従業員にセキュリティーの指針を配信すると、物理的な、およびシステムのセキュリティーに関するセキュリティー・ポリシーを強調する上で役に立ちます。これらの指針の中には、ワークステーションのサインオフ、パスワードの適切な使用、および無許可の侵入者からのネットワークの保護など、システム・セキュリティーを保護する方法に関する指示も含める必要があります。さらにセキュリティー・ポリシーでは従業員の訓練や必要なソフトウェアおよびハードウェアの導入に関する手順を説明し、システム・セキュリティーを確保することができます。

セキュリティー・ポリシーは、いつでも変更できることを覚えておいてください。コンピューター環境を変更する場合は、セキュリティー・ポリシーを更新して、変更によって生じる新しいリスクに対処することが必要です。ほとんどの会社では、会社が成長するにつれて、より厳重なセキュリティーが必要であることに気付きます。

セキュリティー・ポリシーを開発するため、以下のステップを実行します

1. セキュリティーの要件をより正しく判別するため、組織内の他のメンバー (セキュリティー監査員など) に相談する。
2. 会社で使用するテクノロジーについて吟味する。たとえば、システムがインターネットに接続される場合には、外部のインターネット・ユーザーからシステムを保護するために、より制限の多いセキュリティー環境が必要になります。
3. 以下のようにして、セキュリティーを保つためのアプローチ全体を決定する。

   厳重 厳重なポリシーは、理解しておくべきセキュリティー機構の一つです。厳重なセキュリティー環境では、ジョブの実行に必要な情報と機能に対してのみ、アクセスすることが許されます。他の情報や機能は除外されます。多くの監査員は、厳重なアプローチを推奨しています。

   平均 平均的なセキュリティー・ポリシーでは、割り当てられている権限に基づいて、オブジェクトに対するユーザーのアクセスを許可します。

   寛容 寛容なセキュリティー環境では、許可を持つユーザーに、システム上のほとんどのオブジェクトに対するアクセスを許可します。機密情報へのアクセスのみを制限します。単一の部門または小規模な会社では、寛容なアプローチをシステムで使用する場合があります。
4. 保護の必要な情報資産を判別する。機密性、競合性、および操作について考慮すると、この判別に役立ちます。

   機密性 社内の人間が一般的に使用できない情報。機密情報の例として、給与計算などが挙げられます。機密情報の別の例としては、まだ公開していない新しい技術情報があります。

   競合性 競争において利益をもたらす情報。製品の仕様書や規格、および価格設定の指針などがあります。

操作　通常のビジネスの作業に不可欠なコンピューター上の情報。顧客レコードや在庫バランスなどがあります。

5. セキュリティーに関する会社のポリシーについての声明文を作成する。これは、お客様と会社の最高責任者との間の協定になります。セキュリティー・ポリシーは、全体的なアプローチと、保護を必要とする資産を定めるものでなければなりません。32 ページの『セキュリティー・ポリシーの例』
6. セキュリティー・ポリシーの草案を作成する。32 ページの『例: 会社のセキュリティーのメモ』
7. 計画プロセスで作業する際、セキュリティー・ポリシーを完成させるために後に使用する補足的なノートを記す。
8. セキュリティー・ポリシーを完成させ、社内の従業員に配布する。システムのセキュリティーをインプリメントしてモニターする際に、それを使用してください。

セキュリティー・ポリシーを作成後、システムの 7 ページの『セキュリティー・レベル』を選択できます。

セキュリティー・ポリシーの例

全体的なアプローチ
寛容: ほとんどのユーザーがほとんどの情報にアクセスできる。

重要な情報
- 契約と価格設定
- 給与計算 (カスタマーに対するクレジットの限度額を設定および変更できるのは、経理の担当者のみです。)
- カスタマーおよび在庫の記録

一般規則
- それぞれのシステム・ユーザーは、ユーザー・プロファイルを持っています。
- ユーザーは、60 日ごとにパスワードを変更しなければならない。
- ユーザーは、最新のセキュリティー・パッチを使用する必要がある。

図 1. 会社のセキュリティー・ポリシー

例: 会社のセキュリティーのメモ

新システムのセキュリティー

すべての社員の皆さんは、我が社の新しいシステムに関してお知らせするための会議に出席されたことと思います。システムを使用する人たちはすでに訓練を開始しており、来週には顧客オーダー処理が開始されます。ご自分のシステムで作業する際、以下のセキュリティー上の指針を守ってください。

- システムを使用する必要のあるすべての人には、ユーザー ID とパスワードが渡されます。システムに最初にサインオンする際に自分のパスワードを変更し、その後は 90 日ごとにパスワードを変更してください。パスワードの長さは 8 文字で、文字と数値の組み合わせを含んでいる必要があります。パスワードには、ご自分の名前、ユーザー ID、または他の個人情報を含めないでください。
- 他の人とパスワードを共有しないでください。パスワードを忘れた場合、パスワードのリセットに関する指示を参照するため、技術サポート Web サイトにアクセスします。
- デスクから離れる際は、スクリーン・セーバー・パスワードを使用してシステムをロックしてください。
- 帰宅する際には、機密情報をロックしてください。機密情報の例として、契約と価格設定情報、および給与計算レコードがあります。

図 2. 会社のセキュリティーのメモ

セキュリティー・ポリシーの変更

iSeries ナビゲーターを使用して、システムのポリシーを表示したり管理したりすることができます。

iSeries ナビゲーターには 5 つのポリシーの分野があります。

監査ポリシー
このポリシーでは、システム上の特定の資源に対する特定のアクションおよびアクセスのモニターをセットアップすることができます。

セキュリティー・ポリシー
このポリシーでは、セキュリティーのレベル、およびシステム・セキュリティーに関連する追加オプションを指定することができます。

パスワード・ポリシー
このポリシーでは、システムのパスワード・セキュリティー・レベルを指定することができます。

復元ポリシー
このポリシーでは、特定のオブジェクトをシステム上で復元する方法を指定することができます。

サインオン・ポリシー
このポリシーでは、ユーザーがシステムにサインオンする方法を指定することができます。

1. iSeries ナビゲーターで、ご使用の「**サーバー**」 → 「**セキュリティー**」と展開します。
2. 「**ポリシー**」を右マウス・ボタンでクリックし、「**探索**」を選択して、作成および管理できるポリシーのリストを表示します。これらのポリシーに固有の情報については、iSeries ナビゲーターのヘルプを参照してください。

物理的セキュリティーの計画

このトピックでは、物理的セキュリティー、および物理的セキュリティーの計画のかぎとなる作業について取り上げ、こうした作業が重要な理由について説明します。

物理的セキュリティーには、事故による (または意図的な) 損傷および盗難からサーバーを保護することが含まれます。サーバーに加えて、これにはすべてのワークステーション、プリンター、および記憶媒体が含まれます。

サーバーの導入の準備をする際に、以下の質問を考慮して、物理的セキュリティーの計画を作成する必要があります。

- システム装置をどこに置くか。
- 各表示装置をどこに配置するか。
- プリンターをどこに配置するか。
- 付加的に必要な装置は何か (配線、電話回線、取り付け器具、または記憶域など)。
- システムを火事や停電などの非常事態から守るために、どのような手段をとるか。

物理的セキュリティーは、全体的なセキュリティーの計画に含めるべき事柄です。システムとその装置を置く場所によっては、保護のために特別な手段が必要になる場合もあります。

システムの物理的セキュリティーに関する決定は、38 ページの『物理的セキュリティー計画ワークシート』を使用して記録することができます。

システム装置の物理的セキュリティーの計画

このトピックでは、物理的位置、制御盤やキーロック、および保守ツールのユーザー ID とパスワードなどの、システム装置の特定の面におけるセキュリティーの重要性について取り上げます。

システム装置は、重要なビジネス資産であり、システムへの入り口となっています。システム内のシステム構成要素の中には、小型で重要なものがあります。システム装置を制御された場所に設置して、他の人物がシステム装置を盗んだり重要なシステム構成要素を除去できないようにする必要があります。最良の手段は、専用の部屋を設けてその部屋をロックしておくことです。システム装置は、通常のビジネス時間前後にはロックできる場所に置いてください。

各システム装置には、ワークステーションを使用しないで基本機能を実行できる機能を備えている制御盤があります。たとえば、制御盤を使用して以下を行うことができます。

- システムの停止
- システムの始動
- オペレーティング・システムのロード
- サービス機能の開始

こうした活動はすべて、システム・ユーザーを混乱させる可能性があります。さらに、システムでの機密漏れの可能性を示すものでもあります。これらのシステム操作が許可なく行われることを防ぐため、 各システム装置には、キーロック・スイッチか電子キースティックがあります。 これらの機能でも、システム装置をある程度保護することはできますが、 キーロック・スイッチや電子キースティックは、 適切な物理的セキュリティーの代わりになるものではありません。 制御盤を使用できないようにするには、「保護」の位置にキーロックをして、 キーを取り外して安全な場所に保管してください。

システム装置へのリスク

システム装置やそのコンポーネントの盗難に加えて、システム装置に対する物理的セキュリティーが不十分なために生じる、いくつかの他のリスクがあります。

システム操作による意図せぬ停止

セキュリティーの問題のほとんどは、許可を持つシステム・ユーザーによって引き起こされます。たとえば、システム上の表示装置の 1 つがロックされたとします。システム操作員は会議で席を離れています。その表示装置を使おうとしたユーザーがシステム装置のところへやってきて、「多分このボタンを押せばいいんだろう」と考えます。そのボタンは、数多くのジョブを実行しているシステムの電源をオフにしたり、再ロードしたりするものかもしれません。部分的に更新されたファイルを回復するには、数時間かかるかもしれません。このような問題が生じるのを避けるために、システム装置のキーロック・スイッチを使用することができます。

専用保守ツール (DST) 機能を使用したセキュリティーの回避

セキュリティーは、システムが実行する保守機能を制御しません。これは、保守機能を実行する必要がある際に、システム・ソフトウェアを正常に操作できない可能性があるためです。システムに関する知識があり保守ツールのユーザー ID とパスワードを知っている、または推測できる人物であれば、使用中のシステムに深刻な損傷を与えることが可能です。

システムを安全に保つために実行できる事柄

以下の情報では、システムを安全に保つ幾つかの方法を提案します。物理的セキュリティー計画ワークシートの『システム装置』セクションに、ご自分の選択を記録してください。 35 ページの『例: 物理的セキュリティー計画用紙 - システム装置』も参照してください。

- 理想的なのは、システム装置をロックされた部屋に置くことです。ご使用の装置がロックされていない部屋に置かれている場合、部外者が使用できない場所に置いてください。加えて、責任のある従業員が監視できる位置に装置を置いてください。次の物理的なセキュリティー機能は、意図しない、または意図的な損傷からシステムを保護する上で役立ちます。
- 電子キースティックまたはキーロックを使用する。
  - キーを使用せずにシステムを開始できるようにするには、操作モードを Normal に設定します。
  - 自動電源オン/オフ機能を使用して、システムを開始および停止するには、操作モードを Auto に設定します。
  - キーを外して安全な場所に保管します。
- システム上でリモート IPL を実行するかまたはリモート診断を実行する必要がある場合には、キーロックに別の設定値を選択する必要がある場合があります。
- システムを導入した後、および保守担当者が保守ツール (DST) を使用した後に、 ただちに保守ツール (DST) のユーザー ID とパスワードを変更する。

例: 物理的セキュリティー計画用紙 - システム装置

表 8. 物理的セキュリティー計画用紙: システム装置

システム装置	
システム装置を保護するためにとったセキュリティー手段 (ロックした部屋の使用など)。	システム装置は経理のエリアに置く。日中は、経理の担当者が常にこのエリアにおり、システム装置を監視することができる。この部屋は、通常のビジネス時間以外にはロックされる。
通常のキーロックの設定位置:	標準。
キーの保管場所:	管理者のオフィスにキーがある。
システム装置に関連したその他の注記。	システム装置のある場所には容易に出入りすることができる。経理のエリアにいる人々については、無許可の人が装置を使用しないようにすることが必要。

システム装置の物理的セキュリティーを計画したなら、システム文書および記憶媒体の物理的セキュリティーを計画することができます。

関連情報

保守ツール・ユーザー ID の構成

システム文書および記憶媒体の物理的セキュリティーの計画

このトピックでは、重要なシステム文書および記憶媒体のセキュリティーの大切さについて取り上げます。こうしたアイテムを 2 つの場所、オンサイトとオフサイトに保管することが強調されます。

システム文書には、IBM がシステムとともにお送りした情報、パスワードの情報、お客様の計画用紙、およびシステムが生成したすべての報告書が含まれています。ご使用のシステムに応じて、バックアップ媒体にはテープ、CD-ROM、ディスケット、または DVD 記憶装置が含まれます。システム文書とバックアップ媒体はいずれも、企業の場所以外に、他の離れた場所にも保管しておく必要があります。万一災害が発生した場合には、システムを回復させるためにこの情報が必要になります。

システム文書を安全に保管する

保守ツールおよび機密保護担当者のパスワードは、システムの運用における重要な情報です。これらのパスワードは書き留めて、機密の場所に安全に保管してください。加えて、災害時にシステムを回復できるよう、これらのパスワードのコピーを離れた別の場所 (オフサイト) に保管してください。

災害時の回復に使用するため、他の重要なシステム文書 (構成の設定やメインのアプリケーション・ライブラリー) については、ビジネスの場所から離れた場所に保管することを考慮してください。

記憶媒体を安全に保管する

システムを導入する際、システム上のすべての情報を、定期的にテープや他の記憶媒体に保管するように計画してください。このようなバックアップを作成することにより、必要な時にシステムを回復することができます。これらのバックアップもやはり、ビジネスの場所から離れた安全な場所 (オフサイト) に保管してください。

バックアップ媒体とパスワード情報に関連したリスク

- バックアップ媒体の損傷: 災害によって、または意図的にバックアップ媒体が破壊された場合、印刷された報告書から情報を復元する以外、システム上にあった情報を回復することはできません。

- バックアップ媒体やパスワードの盗難: バックアップ媒体に機密のビジネス情報が保管されている場合があります。そのことを知っている人物がいると、この情報を他のコンピューターで復元し、印刷したり、処理したりできる恐れがあります。

記憶媒体とパスワードを安全に保つために実行できる事柄

システム文書と記憶媒体を保管する方法として、次に示されている方法を使用することもできます。保管の方法を決定したら、物理的セキュリティー計画ワークシートの、『バックアップ媒体および文書』のセクションに選択事項を記録してください。

- すべてのパスワードおよびバックアップ媒体は、ロックされた、耐火性のキャビネットに保管してください。
- バックアップ媒体のコピーを安全で離れた場所 (オフサイト) に、 定期的に (たとえば、最低でも週に 1 回) 保管するようにしてください。

例: 物理的セキュリティー計画用紙 - バックアップ媒体および文書

表 9. 物理的セキュリティー計画用紙: バックアップ媒体および文書

バックアップ媒体および文書	
バックアップ・テープのビジネスの場所での保管場所:	耐火金庫の中。
バックアップ・テープの別の保管場所:	会社の経理係のオフィスにある耐火金庫の中。
機密保護担当者、保守、および DST パスワードの保管場所:	管理者のオフィス内。
重要なシステム文書 (シリアル番号や構成など) の保管場所:	会社の経理係のオフィスにある耐火金庫の中。

記憶域と文書のセキュリティーの計画が完了したら、ワークステーションに対する物理的セキュリティーを計画することができます。

物理的ワークステーション・セキュリティーの計画

このトピックでは、ワークステーションのセキュリティー・リスクと推奨事項について説明します。

すべてのユーザーが、任意の使用可能なワークステーションにサインオンして、許可されたすべての機能を実行できるようにしたい場合もあります。しかし、あるワークステーションを誰でも使用できるようにしたり、逆に何かの専用に使用する場合は、無許可のユーザーがワークステーションの機能にアクセスしないようにしたいと思われるかもしれません。

ワークステーションに関連したリスク

共用の場所にあるワークステーションが許可されていない目的で使用される
社外の人間が容易に出入りできる場所にワークステーションを置くと、機密情報を見られてしまう可能性があります。システム・ユーザーが、ワークステーションにサインオンしたままにしておくと、社外の人間が入ってきて機密情報にアクセスする恐れがあります。

専用の場所にあるワークステーションが許可されていない目的で使用される
ワークステーションを密閉された場所に置くと、侵入者が長時間誰にも気付かれずにセキュリティーを回避してしまうというリスクがあります。

表示装置のプレイバック機能や PC サインオン・プログラムを使用してセキュリティーが回避される
多くの表示装置には記録およびプレイバックの機能があります。これは、ユーザーが頻繁に使用するキー・ストロークを保管し、1 つのキーを押すだけでそれが繰り返されるようにする機能です。

また、システムでパーソナル・コンピューターをワークステーションとして使用する場合は、プログラムを作成して、サインオン・プロセスが自動的に行われるようにすることができます。ユーザーはサインオン・プロセスを頻繁に行うため、サインオンのたびに入力を行うより、ユーザー ID とパスワードを保管しておくことを考えます。

ワークステーションを安全に保つために実行できる事柄

ワークステーションでセキュリティー・リスクが生じる可能性があるかどうかを識別する必要があります。以下の情報では、ワークステーションを安全に保つ幾つかの方法を提案します。物理的セキュリティー計画ワークシートの『ワークステーションおよびプリンター』セクションに、ご自分の選択を記録してください。『例: 物理的セキュリティー計画用紙 - ワークステーションおよびプリンター』も参照してください。

- ワークステーションを極端に誰でも出入りできる場所や密閉されている場所に配置しないようにします。
- 表示装置や PC プログラムにパスワードを記録することは、システム・セキュリティーに違反することをユーザーに指摘してください。
- ワークステーションから離れる前にサインオフするようユーザーに求めます。
- 非活動タイマー・システム値 (QINACTITV および QINACTMSCQ) などを使用して、ユーザーがシステムをサインオフせずに、共用の場所にあるワークステーションを離れることがないよう、手段を講じてください。
- 無防備なワークステーションに対するアクセスを制限します。
  - 限定された機能を持つユーザー・プロファイルにのみ許可を与えます。
  - QLMTSECOFR システム値を使用して、機密保護担当者権限または保守権限を持つユーザーがサインオンできるワークステーションを制限します。
  - QLMTDEVSSN システム値を使用して、ユーザーが複数のワークステーションに同時にサインオンしないように制限してください。
- プリンターと他の装置に対する *CHANGE 権限を制限します。

例: 物理的セキュリティー計画用紙 - ワークステーションおよびプリンター

表 10. 物理的セキュリティー計画用紙: ワークステーションおよびプリンター

ワークステーションおよびプリンター			
ワークステーション名またはプリンター名	置かれている場所または説明	機密漏れ	実行する保護手段
DSP06	発送センター	極端に誰でも出入りできる場所にある	自動サインオフ。ワークステーションで完了できる機能のみに制限する。
RMT12	離れた場所にある営業所	密閉しすぎている	機密保護担当者がサインオンできないようにする。
PRT01	会計事務所	価格表などの機密情報が目の届く所にある。	プリンターをロックした部屋に配置します。機密出力を 30 分以内に取りに来るようユーザーに伝えてください。

プリンターおよびプリンター出力の物理的セキュリティーの計画

このトピックでは、プリンターおよびプリンター出力のセキュリティーに関するリスクと推奨事項について説明します。

情報の印刷が開始された後は、誰がその情報を見るかを、システム・セキュリティーによって制御することはできません。重要なビジネス情報が誰かによって見られる可能性を最小限にするには、プリンターとプリンター出力を保護する必要があります。また、機密のビジネス情報を印刷することに関して、方針を作成する必要もあります。

プリンターおよびプリンター出力に関連したリスク

プリンターのセキュリティーを計画する際、以下のリスクを念頭に置いてください。

- プリンターの場所。プリンターが共用の場所に置かれていると、許可されていない人々が機密情報を見る恐れがあります。
- プリンター出力。プリンター出力を机の上に放置しておくと、情報が漏れる恐れがあります。
- 機密性のあるプリンター出力。従業員が、給与や製品仕様などの機密情報を印刷する場合もあります。

プリンターおよび出力を安全に保つために実行できる事柄

以下の推奨事項を参考にして、プリンターとその出力に関連した、セキュリティー上のリスクを減らすことができます。

- 機密のプリンター出力を保護することの重要性をシステム・ユーザーに強調してください。ご使用になるセキュリティー・ポリシーに、プリンターおよび出力を保護するための計画を含めます。
- プリンターを公共の場所に置くことは避けてください。プリンターをロックされた部屋に置くことを考慮してください。
- 機密性の高い出力の印刷についてはスケジュールを立て、印刷が行われる間、許可された人がプリンターの所にいるようにするか、機密性のある出力を特定の時間内に持っていくよう従業員に伝えてください。

物理的セキュリティー計画ワークシート

このトピックでは、システム装置、バックアップ媒体、ワークステーション、およびプリンターの物理的セキュリティーを計画するのに使用可能な物理的セキュリティー計画ワークシートを示します。

表 11. 物理的セキュリティー計画ワークシート

物理的セキュリティー計画ワークシート	
作成者:	日付:
指示 • 『物理的セキュリティーの計画』トピックでこのワークシートについて確認してください。 • システム装置および接続装置の物理的な場所に関連したセキュリティーの問題について記述するには、このワークシートを使用します。 • このワークシートの情報は、システムに入力する必要はありません。	
システム装置	
システム装置を保護するためにとったセキュリティー手段(ロックした部屋の使用など)。	
通常のキーロックの設定位置:	

表 11. 物理的セキュリティー計画ワークシート (続き)

物理的セキュリティー計画ワークシート	
キーの保管場所:	
システム装置に関連したその他の注記:	
バックアップ媒体および文書:	
バックアップ・テープのビジネスの場所での保管場所:	
バックアップ・テープの別の保管場所:	
機密保護担当者、保守、および DST パスワードの保管場所:	
重要なシステム文書 (シリアル番号や構成など) の保管場所:	

物理的セキュリティー計画ワークシート			**2 / 2**
第 2 部の追加指示 • 機密漏れを引き起こす可能性のある設置場所のワークステーションまたはプリンターを下にリストします。実行する保護手段を指示します。プリンターの場合は、「機密漏れ」欄に、印刷された機密報告書の例をリストします。 • システムにローカル装置の自動構成を許可する場合は、システムが導入されるまで、ワークステーションおよびプリンターの名前が分からないことがあります。このワークシートを準備する段階で、名前が分からない場合は、説明 (たとえば位置など) を記入し、名前を後で追加します。			
ワークステーションおよびプリンターの物理的セキュリティー			
ワークステーション名またはプリンター名	置かれている場所または説明	機密漏れ	実行する保護手段

システム・セキュリティーの計画

システム・セキュリティーでは、ユーザー・アクセスとその特権の制御、情報の保全性の維持、プロセスとアクセスのモニター、システム機能の監査、およびセキュリティー関連情報のバックアップと回復の提供が必要となります。

i5/OS では、システム・セキュリティーはシステム値を使用してオペレーティング・システムと統合されます。システム値は、その値の定義方法に基づいて指定の機能が実行される方法を制御します。セキュリティー・システム値は、実行する機能に応じて分類されます。たとえば、セキュリティー・システム値はシステムのセキュリティー・レベルや、サインオンおよびパスワード制御を管理できます。

セキュリティー・システム値を使用するには、こうした値を変更および更新するための適切な権限をユーザーまたは管理者が持っていることが必要です。場合によっては、こうしたセキュリティー値の権限が異なることもあります。こうしたセクションで説明されている各セキュリティー・システム値には、必要な権限が備えられています。

セキュリティー・システム値は、i5/OS 文字ベースのインターフェースを使用して、またはほとんどの i5/OS 機能を簡単に管理できるグラフィカル・ユーザー・インターフェースである iSeries ナビゲーターを使用して設定できます。この情報では、iSeries ナビゲーターでのシステム値名、および文字ベースのインターフェースでそれに相当する値の両方を記します。

またこのトピックでは、こうしたセキュリティー・システム値に関する説明や、一般的なインストールでの推奨事項、およびシステム値の決定に関して記録にとどめるための用紙について取り上げます。

システム・セキュリティーの計画を完成させるには、セキュリティー関連のシステム値について検討し、決定した事柄をシステム値選択用紙に記録してください。セキュリティー関連のシステム値に関して、以下のトピックを参照してください。

関連概念

7 ページの『セキュリティー・レベル』
システム・セキュリティーは一連の複数のレベルとして序列化され、レベルが高くなるにつれて、より強固にデータを保護する高水準のセキュリティーを提供します。

汎用のセキュリティー・システム値

汎用のセキュリティー・システム値は、ご使用になるセキュリティー・ポリシーの基礎となります。

汎用のセキュリティー・システム値を使用すると、セキュリティー・ポリシーを作成する際に下した決定をサポートするセキュリティー機能を設定できます。たとえば、顧客アカウントや給与計算インベントリーなどの機密情報が含まれるシステムでは、社内で開発するアプリケーションの検査に使用するシステムよりも厳重なセキュリティー・レベルを必要するということをセキュリティー・ポリシーに記述します。その後、セキュリティー・ポリシーで下した決定に対応するそのようなシステムでのセキュリティー・レベルを計画して設定できます。

セキュリティー・レベル・システム値:

このシステム値を使用すれば、システムのセキュリティー・レベルを設定できます。

システム・セキュリティー・レベルには、5 つの異なるレベルがあります。これらの各セキュリティー・レベルは、それぞれ特定の方法でシステムのセキュリティーを管理します。セキュリティー・ポリシーで決定した内容に応じて、必要を満たすセキュリティー・レベルを選ぶことができます。IBM から出荷される新しいシステムのセキュリティー・レベルはすべて 40 で、これはほとんどの導入システムで必要とされる高水準のセキュリティーを提供します。新しいシステムのセキュリティー・レベルをこの値より低く変更することは、推奨されません。

IBM はシステム・セキュリティー・レベルを 40 のままにすることを推奨しますが、それぞれのセキュリティー・レベルの違いを機能別に比較するために、より低い値についても説明します。

表 12. セキュリティー・レベル・システム値に指定できる値： この表は、セキュリティー・レベルによって可能になるさまざまな設定値と機能を比較します。

セキュリティー・レベル	iSeries ナビゲーターでの記述	使用できる機能	使用できない機能
10 (セキュリティーなし) [1]	パスワードが不要で、ユーザーはすべてのリソースに対する権限を持っています	すべてのオブジェクトに対する *ALLOBJ アクセスをユーザーに与えます。	なし
20 (低く寛容なセキュリティー)	パスワードが必要で、ユーザーはすべてのリソースに対する権限を持っています	• すべてのオブジェクトに対する *ALLOBJ アクセスをユーザーに与えます。 • サインオン時にユーザー名が必要 • サインオン時にパスワードが必要 • パスワード・セキュリティーが活動状態 • メニューおよび初期プログラム・セキュリティーが活動状態 • セキュリティー監査機能を使用できる • 制限された命令を含むプログラムを作成/再コンパイルできない • *USRSPC、*USRIDX、*USRQ オブジェクトは、QALWUSRDMN システム値で指定されているライブラリーでのみ作成できる	• 資源保護が活動状態 • ユーザー・プロファイル自動生成 • サポートされていないインターフェースを使用するプログラムは実行時に失敗する • 拡張ハードウェア記憶保護機構サポートあり • パラメーターで使用されるポインターは、システム状態で実行しているユーザー・ドメイン・プログラムに対して、妥当性が検査される • メッセージ処理規則が、システムおよびユーザー状態プログラム間で実施されている • プログラムの関連スペースを直接変更できない • 内部制御ブロックが保護されている

表 12. セキュリティー・レベル・システム値に指定できる値 (続き): この表は、セキュリティー・レベルによって可能になるさまざまな設定値と機能を比較します。

セキュリティー・レベル	iSeries ナビゲーターでの記述	使用できる機能	使用できない機能
30 (中程度の平均的なセキュリティー)	パスワードが必要であり、ユーザーのアクセスはユーザーの権限に基づきます	• サインオン時にユーザー名が必要 • サインオン時にパスワードが必要 • パスワード・セキュリティーが活動状態 • メニューおよび初期プログラム・セキュリティーが活動状態 • セキュリティー監査機能を使用できる • 制限された命令を含むプログラムを作成/再コンパイルできない • *USRSPC、*USRIDX、*USRQ オブジェクトは、QALWUSRDMN システム値で指定されているライブラリーでのみ作成できる	• すべてのオブジェクトへのアクセスを許可 • 資源保護が活動状態 • ユーザー・プロファイル自動生成 • サポートされていないインターフェースを使用するプログラムは実行時に失敗する • 拡張ハードウェア記憶保護機構サポートあり • パラメーターで使用されるポインターは、システム状態で実行しているユーザー・ドメイン・プログラムに対して、妥当性が検査される • メッセージ処理規則が、システムおよびユーザー状態プログラム間で実施されている • プログラムの関連スペースを直接変更できない • 内部制御ブロックが保護されている

表 12. セキュリティー・レベル・システム値に指定できる値 (続き): この表は、セキュリティー・レベルによって可能になるさまざまな設定値と機能を比較します。

セキュリティー・レベル	iSeries ナビゲーターでの記述	使用できる機能	使用できない機能
40 (高く厳重なセキュリティー) [2]	文書化されていないシステム・インターフェースからの保護	• サインオン時にユーザー名が必要 • サインオン時にパスワードが必要 • パスワード・セキュリティーが活動状態 • メニューおよび初期プログラム・セキュリティーが活動状態 • セキュリティー監査機能を使用できる • 制限された命令を含むプログラムを作成/再コンパイルできない • *USRSPC、*USRIDX、*USRQ オブジェクトは、QALWUSRDMN システム値で指定されているライブラリーでのみ作成できる • パラメーター内で使用されるポインターはユーザー・ドメインに対して検証される • プログラムの関連スペースを直接変更できない • 内部制御ブロックが保護されている	• すべてのオブジェクトへのアクセスを許可 • ユーザー・プロファイル自動生成 • メッセージ処理規則が、システムおよびユーザー状態プログラム間で実施されている

表 12. セキュリティー・レベル・システム値に指定できる値 (続き): この表は、セキュリティー・レベルによって可能になるさまざまな設定値と機能を比較します。

セキュリティー・レベル	iSeries ナビゲーターでの記述	使用できる機能	使用できない機能
50 (高く厳重なセキュリティー) [3]	システム・インターフェースの保護の拡張	• サインオン時にユーザー名が必要 • サインオン時にパスワードが必要 • パスワード・セキュリティーが活動状態 • メニューおよび初期プログラム・セキュリティーが活動状態 • セキュリティー監査機能を使用できる • 制限された命令を含むプログラムを作成/再コンパイルできない • *USRSPC、*USRIDX、*USRQ オブジェクトは、QALWUSRDMN システム値で指定されているライブラリーでのみ作成できる • パラメーター内で使用されるポインターはユーザー・ドメインに対して検証される • プログラムの関連スペースを直接変更できない • 内部制御ブロックが保護されている	• すべてのオブジェクトへのアクセスを許可 • ユーザー・プロファイル自動生成

1. セキュリティー・レベル 10 はサポートされなくなりました。セキュリティー・レベル 10 から 20、30、40、または 50 に変更した場合、レベル 10 に戻せなくなります。
2. IBM は、すべての新しいシステムをセキュリティー・レベル 40 で出荷します。IBM では、セキュリティー・レベルを 40 のままにしておくよう強くお勧めします。
3. セキュリティー・レベル 50 では、システム内部制御ブロックの変更はできません。これに比べて、セキュリティー・レベル 40 では、一部のシステム内部制御ブロックを変更できます。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、資産保護、ユーザー・アクセス、システム・パフォーマンスの 3 要素の間のバランスを維持することを考慮してください。紛失または盗難に遭った場合に企業にとって大きな危険を生じさせる機密性の高い資料や情報がシステムに含まれる場合には、機密性がそれほど高くない情報を含むシステムよりも高いセキュリティー・レベルが必要でしょう。さらに、安全でないネットワーク (たとえばインターネット) にシステムが接続する場合、潜在的に攻撃のターゲットとなり得ます。このようなシステムもまた、高いセキュリティー・レベルによって保護されなければなりません。

注: セキュリティー・レベルだけでは、安全でないネットワークに接続するシステムを攻撃から保護することはできません。インターネットその他の安全でないネットワークへの接続を計画している場合、システムに対するリスクだけでなく、組織のネットワーク全体に対するリスクを分析する必要があります。

表 13. 早見表 : セキュリティー・レベル・システム値の詳細を示します。

iSeries ナビゲーター名	**セキュリティー・レベル**
文字ベースのインターフェース名	QSECURITY
権限	全オブジェクト (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**セキュリティー・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**一般**」ページに、セキュリティー・レベルのオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QSECURITY` と入力します。
変更内容が有効になる時点	サーバーの次回の再始動時
デフォルト値	40 (文書化されていないシステム・インターフェースからの保護)
推奨値	40 (文書化されていないシステム・インターフェースからの保護)
ロック可能	可
特別な考慮事項	セキュリティー・レベル 10 から 20、30、40、または 50 に変更した場合、レベル 10 に戻せなくなります。

このセキュリティー値の詳細については、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

サーバー・セキュリティーの保持:

このシステム値は、クライアント/サーバー・インターフェースを介してサーバーがターゲット・システム上のユーザーを認証するうえで必要なセキュリティー・データを、ホスト・システム上に保持するかどうかを決定します。

このセキュリティー値を使用すると、この機能をオン/オフに切り替えることができます。ただし、これにはシステム・ユーザー・プロファイル・パスワードが含まれません。

「サーバー・セキュリティーの保持」システム値の概要に関する 46 ページの表 15を参照してください。

以下の表は、「セキュリティーの保持」システム値に指定できる値を示しています。

表 14. 「サーバー・セキュリティーの保持」システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
選択解除	0 (いいえ)	サーバーのセキュリティー・データは保持されない。
選択	1 (はい)	サーバーのセキュリティー・データは保持される。

セキュリティー・ポリシーとの関係

表 15. 早見表 : 「サーバー・セキュリティーの保持」システム値の詳細を示します。

iSeries ナビゲーター名	サーバー・セキュリティーの保存の許可 (Allow server security to be retained)
文字ベースのインターフェース名	QRETSVRSEC
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**セキュリティー・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**一般**」ページに、セキュリティー情報保持のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QRETSVRSEC` と入力します。
変更内容が有効になる時点	即時
デフォルト値	選択解除 (0)
推奨値	
ロック可能	可
特別な考慮事項	「サーバー・セキュリティー情報の保持」を許可から不許可に変更した場合、一部のユーザー・アプリケーションが失敗する可能性があります。

このセキュリティー値の詳細については、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

共用メモリーの制御:

このシステム値は、共用メモリーへのアクセスを許可するかどうか、またはマップされたメモリー・ストリーム・ファイルを使用するかどうかを決定します。

これは、メモリーの共用またはマップされたメモリー・ストリーム・ファイルを扱うアプリケーション・プログラミング・インターフェース (API) をユーザー (特にアプリケーション開発者) がどのように使用するかを制御します。環境によっては、それぞれ別のジョブを実行しながらポインターを共用する複数のアプリ

ケーションが存在する場合があります。これらの API を使用すれば、さまざまなアプリケーションおよびジョブの間で共用メモリーとストリーム・ファイルを許可することにより、アプリケーションのパフォーマンスが改善され、アプリケーション開発が簡素化されます。ただし、これらの API を使用すると、システムや資産が危険にさらされる可能性があります。書き込みアクセスを持つプログラマーが、共用メモリーやストリーム・ファイルの中の項目を追加、変更、または削除する可能性があります。

共用メモリー制御システム値の概要に関する表 17を参照してください。

以下の表は、このシステム値として使用できるそれぞれの設定値を説明します。

表 16. 共用メモリー制御システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
選択解除	0 (いいえ)	ユーザーは、共用メモリーまたは書き込み能力を持つマップ・メモリーを使用できません。この値を設定すると、共用メモリー API、または書き込み能力を持つマップ・メモリー・オブジェクトをユーザーやプログラマーが使用することを禁止できます。この値は、セキュリティー要件がより高い環境で使用してください。
選択	1 (はい)	ユーザーは、共用メモリーまたは書き込み能力を持つマップ・メモリーを使用できます。この値を設定すると、ユーザーやプログラマーは共用メモリーやストリーム・ファイルの中の項目を追加、変更、または削除できます。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーに関連して、アプリケーション・パフォーマンスの要件とセキュリティーの要件を比較考量する必要があります。共用メモリーを使用するアプリケーションを企業で使用している場合、プログラマーにこれらの API の使用を許可することを考慮してください。こうすれば、アプリケーション・プログラミングがより簡単かつコスト効率的になります。しかし、より厳重なセキュリティーを必要とする環境では、この能力を制限することをお勧めします。

表 17. 早見表： 共用メモリー制御システム値の概要を示します。

iSeries ナビゲーター名	共用またはマップされたメモリーの書き込み機能による使用の許可
文字ベースのインターフェース名	QSHRMEMCTL
権限	全オブジェクト (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。

表 17. 早見表 (続き)： 共用メモリー制御システム値の概要を示します。

iSeries ナビゲーター名	**共用またはマップされたメモリーの書き込み機能による使用の許可**
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**セキュリティー・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**共用メモリー**」ページに、このオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、WRKSYSVAL QSHRMEMCTL と入力します。
変更内容が有効になる時点	即時
デフォルト値	選択 (1)
推奨値	
ロック可能	可

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

リモート・サービス属性:

このシステム値を使用すれば、システムの設置場所以外のエリアからシステムを分析することができます。

このシステム値を使用することで、サービス専門家はシステムの問題分析をリモートに行い、分析結果に基づいてトラブルシューティングすることができます。リモート・サービス属性はメッセージおよびサービスのシステム値として分類されていますが、セキュリティー上の意味もあります。システムのリモート分析を使用可能にした場合、適切な権限さえあれば、潜在的にはどんなリモート・ユーザーでもシステムにアクセスできます。

リモート・サービス属性システム値の概要に関する 49 ページの表 19を参照してください。

表 18. リモート・サービス属性システム値に指定できる値

iSeries ナビゲーター	**文字ベースのインターフェース**	**説明**
選択解除	0 (オフ)	リモート・サービス属性をオフにする。
選択	1 (オン)	リモート・サービス属性をオンにする。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、システムがサービスを受ける必要がある場合にどうすべきかの概要を示してください。たとえば、実際に必要が生じるまで、リモート・サービスを制限した方がよいかもしれません。サービス専門家によってシステムを分析してもらう必要が生じた場合、サービスを受けている期間中はこの値を設定し直し、トラブルシューティング・タスクがすべて完了した後で元の設定に戻すことができます。

表 19. 早見表： リモート・サービス属性システム値についての詳細を示します。

iSeries ナビゲーター名	**サーバー・セキュリティーの保存の許可 (Allow server security to be retained)**
文字ベースのインターフェース名	QRMTSRVATR
権限	全オブジェクト (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. **「構成とサービス」** → **「システム値」** → **「メッセージおよびサービス」**を展開します。 2. **「リモート」**ページに、リモート・サービス属性のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QRMTSRVATR` と入力します。
変更内容が有効になる時点	即時
デフォルト値	選択解除 (0)
推奨値	
ロック可能	可
特別な考慮事項	推奨値の場合、どんなユーザーもサービス機能をリモートに実行できません。 **注:** 状況によっては、サービス・プロバイダーまたはソフトウェア・プロバイダーから支援を受ける前に、このシステム値を変更する必要があるかもしれません。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

リモート電源オンおよび再始動:

このシステム値は、リモート・ユーザーがシステムを電源オンおよび再始動できるかどうかを決定します。

このシステム値は、電話、モデム、または SPCN 信号を使ってリモート・システムを開始する機能を提供します。つまり、電話をかけるとシステムが再始動します。このシステム値はシステムの再始動オプションを扱いますが、セキュリティー上の意味もあります。明らかに、誰かが不注意にシステムを再始動するような事態は避けるべきです。しかし、リモート・システムを使ってシステムを管理する場合には、リモート再始動を許容する必要があります。

「リモート電源オンおよび再始動」システム値の概要に関する 50 ページの表 21を参照してください。

表 20. 「リモート電源オンおよび再始動」システム値に指定できる値

iSeries ナビゲーター	**文字ベースのインターフェース**	**説明**
選択解除	0 (いいえ)	リモート電源オンおよび再始動を許可しない
選択	1 (はい)	リモート電源オンおよび再始動を許可する

表 21. 早見表 : 「リモート電源オンおよび再始動」システム値の詳細を示します。

iSeries ナビゲーター名	**リモート電源オンおよび再始動**
文字ベースのインターフェース名	QRMTIPL
権限	全オブジェクト (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. **「構成およびサービス」** → **「システム値」** → **「再始動」**を展開します。 2. **「一般」**ページに、リモート電源オンおよび再始動のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QRMTIPL` と入力します。
変更内容が有効になる時点	即時
デフォルト値	選択解除 (0)
推奨値	
ロック可能	いいえ
特別な考慮事項	システムの管理を実施するリモート・システムを使用している場合、リモート電源オンおよび再始動を使用可能にする必要があります。

このセキュリティー値についての詳細情報は、「再始動システム値: 遠隔パワーオンおよび再始動の許可」を参照してください。

借用権限の使用:

借用権限は、プログラムを実行しているユーザーの権限に、プログラム所有者の権限を追加します。

同じユーザーが同じオブジェクトやアプリケーションに対して異なる権限を必要とする場合があるかもしれません。たとえば、顧客情報の更新機能を持つデータ管理アプリケーションを使って顧客情報の更新業務を行う従業員がいるとします。しかし、その同じユーザーが SQL などの意思決定サポート・ツールを使用するときには、顧客情報を表示することはできても、その情報の変更を許可すべきではありません。このような状況の解決策の 1 つは、借用権限を使用することです。借用権限を使用すれば、重要なファイルが承認済みアプリケーション・プログラムの外で変更されないように保護しながら、引き続きそれらのファイルに対する QUERY を許可することができます。

このシステム値の概要については、 52 ページの表 23を参照してください。

表 22. 借用権限使用システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
すべてのユーザー	*NONE [1]	プログラムまたはサービス・プログラムに対する必要な権限を持っているすべてのユーザーは、呼び出し元プログラムの権限を使用するプログラムやサービス・プログラムを作成、変更、または更新できます。
権限リスト	権限リストの名前	ユーザーの権限は、指定された権限リストと比べて検査されます。この権限は、借用権限に由来するものであってはなりません。指定された権限リスト内で、ユーザーに対して少なくとも USE 権限属性が与えられている場合には、そのユーザーは、呼び出し元プログラムの権限を使用するプログラムまたはサービス・プログラムを作成、変更、または更新できます。

1. *NONE は権限リストを使用しないことを意味します。さらに、デフォルトでは、すべてのユーザーは借用権限を使用するプログラムへのアクセスを許可されます。

セキュリティー・ポリシーとの関係

このシステム値は、借用権限を使ってプログラムを利用できるユーザーを決定します。借用権限は、プログラムを実行しているユーザーの権限に、プログラム所有者の権限を追加します。借用権限を持つすべてのユーザーは、そのプログラムに対する権限があれば、プログラムを作成および変更することができます。借用権限を使用するプログラムやユーザーを決定する前に、以下の質問に答えてください。

特定のプログラムまたはアプリケーションに対して、ユーザーにはどれほどの権限が必要ですか ?

プログラムは、過剰な権限を借用するのではなく、必要な機能を実行するのに十分な権限だけを持つユーザー・プロファイルの権限を借用すべきです。*ALLOBJ 特殊権限を持っているユーザー・プロファイル、または重要なオブジェクトを所有するユーザー・プロファイルの権限を借用するプログラムについては、特に注意が必要です。このようなユーザーは、中心的なプログラム機能へのアクセス権限を持つ可能性があり、主要なデータやアプリケーション・パラメーターを変更できるかもしれません。QSECOFR の権限や *ALLOBJ 特殊権限を持つユーザーの権限を借用するよりも、アプリケーション所有者の権限を借用する方法をお勧めします。権限を借用するアプリケーションの所有者が、QSECOFR ユーザー・クラスに属さず、*ALLOBJ 特殊権限も持っていないことを確認してください。

どのプログラムが借用権限を使用すべきですか ?

権限を借用するプログラムは、具体的かつ限定された機能を持っていなければなりません。権限を借用するプログラムによって提供される機能を注意深く監視してください。これらのプログラムにより、コマンド入力機能など、プログラムの制御外のオブジェクトにアクセスする手段がユーザーに提供されないようにしてください。加えて、権限を借用するプログラムを適切に保護する必要があります。借用権限を許可する前に、プログラムがどのように使用されるかを理解しておくことが重要です。借用権限が過度に使用された場合、システム・パフォーマンスがマイナスの影響を受ける可能性があります。「機密保護解説書」の第 5 章「資源保護」には、借用権限の機能を示すフローチャートが含まれています。

表 23. 早見表 : 「借用権限の使用」システム値に関する詳細を示します。

iSeries ナビゲーター名	**プログラムに呼び出し側プログラムからの借用権限を使用させることができるユーザー**
文字ベースのインターフェース名	QUSEADPAUT
権限	*ALLOBJ *SECADM **注:** QSECOFR ユーザー・プロファイルにはこれらの権限が付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**セキュリティー・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**一般**」ページに、借用権限の使用のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QUSEADPAUT` と入力します。
変更内容が有効になる時点	即時
デフォルト値	すべてのユーザー
推奨値	権限リスト
ロック可能	可
特別な考慮事項	このシステム値は、所有者の権限を借用するプログラム/サービス・プログラムをユーザーが作成または変更することを防止するものではありません。このシステム値は「借用権限の使用」(**USEADPAUT**) パラメーターに適用されますが、プログラム/サービス・プログラムのユーザー・プロファイル (**USRPRF**) パラメーターには適用されません。

このセキュリティー値の詳細については、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

ユーザー・ドメイン・オブジェクトの許可:

このシステム値は、ユーザー・ドメイン・オブジェクトを許可するかどうか、およびこうしたオブジェクトが置かれる場所を指定します。

ユーザー・ドメイン・オブジェクト間の移動はモニターできないため、ユーザー・ドメイン・オブジェクトはセキュリティーのリスクを生じさせる可能性があります。ユーザー・ドメイン・オブジェクトのタイプには、以下のものがあります。

- ユーザー・スペース (*USRSPC)
- ユーザー索引 (*USRIDX)
- ユーザー待ち行列 (*USRQ)

セキュリティー要件のレベルの高いシステムでは、これらのユーザー・ドメイン・オブジェクトをシステムの一時ライブラリー (QTEMP) に制限してください。その他のオブジェクト・タイプの、プログラム

(*PGM)、サーバー・プログラム (*SRVPGM)、および SQL パッケージ (*SQLPKG) も、ユーザー・ドメインに含めることができます。しかし、こうしたオブジェクトの内容は直接変更できないので、この制限からは影響を受けません。

このシステム値の概要については、表 25を参照してください。

表 24. 「ユーザー・ドメイン・オブジェクトの許可」システム値に使用可能な値

iSeries ナビゲーター	文字ベースのインターフェース	説明
すべてのライブラリーとディレクトリー	*ALL	すべてのライブラリーとディレクトリーで監査できないオブジェクトを許可します。サーバーには、複数のファイル・システムがあります。ライブラリーは QSYS ファイル・システムの一部で、ディレクトリーは POSIX ファイル・システムの一部です。ディレクトリーは、「root」または「QOpenSys」ファイル・システムの一部として参照されます。
QTEMP ライブラリーおよびすべてのディレクトリー内	*DIR	QTEMP ライブラリーに加え、すべてのディレクトリーで監査できないオブジェクトを許可します。
QTEMP ライブラリーおよび選択済みライブラリー内	ライブラリー名	監査できないオブジェクトを許可するライブラリーを指定できます。このシステム値は、ユーザー・オブジェクトのユーザー・ドメイン・バージョンを入れられる特定のライブラリーを示します。最高 50 個のライブラリーまでリストできます。ライブラリー名のリストを指定した場合、ユーザー・ドメイン・ユーザー・オブジェクトをその時点で処理しているアプリケーションが、リスト内で指定されていないライブラリー内のオブジェクトを使用すると障害が起きる可能性があります。

セキュリティー・ポリシーとの関係

表 25. 早見表 : 「ユーザー・ドメイン・オブジェクト許可」システム値に関する詳細を提供します。

iSeries ナビゲーター名	対象内のオブジェクトを許可します
文字ベースのインターフェース名	QALWUSRDMN
権限	*ALLOBJ *SECADM **注:** QSECOFR ユーザー・プロファイルにはこれらの権限が付属しています。

表 25. 早見表 (続き) : 「ユーザー・ドメイン・オブジェクト許可」システム値に関する詳細を提供します。

アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**セキュリティー・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**ユーザー・ドメイン・オブジェクト**」ページで、このシステム値のオプションを見つけます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、WRKSYSVAL QALWUSRDMN と入力します。
変更内容が有効になる時点	即時。
デフォルト値	すべてのライブラリーとディレクトリー。
推奨値	ほとんどのシステムの場合、推奨値は *ALL です。高いセキュリティー要件を持つシステムの場合、ユーザー・ドメイン・オブジェクトは、 QTEMP ライブラリー内でのみ許可してください。
ロック可能	はい。
特別な考慮事項	システムの中にはユーザー・ドメイン・オブジェクト・タイプ (*USRSPC、*USRIDX、または *USRQ) を必要とするアプリケーション・ソフトウェアを持つものがあります。こうしたシステムでは、このシステム値を設定して、アプリケーションが使用するすべてのライブラリーが含まれるライブラリー・リストを使用します。このシステム値 (QTEMP は例外) で定義されるすべてのライブラリーには、除外 (*EXCLUDE) 共通権限がなければなりません。これにより、これらライブラリーにあるユーザー・ドメイン・オブジェクト内のデータの読み取りまたは変更が可能なユーザー数を制限します。

このセキュリティー値の詳細については、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

新規オブジェクトに対する権限:

このシステム値を使用して、新しく作成されたオブジェクトの共通権限を決定することができます。

この設定は、新しいオブジェクトを作成して権限レベルを指定しない場合に、コマンド作成に対するデフォルトの共通権限としてシステム全体に設定されて使用されます。

このシステム値については、 55 ページの表 27 を参照してください。

表 26. 新しいオブジェクトの権限システム値として指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
変更	*CHANGE	新しく作成されたオブジェクトの変更を共通権限に許可します。
使用	*USE	QTEMP ライブラリーに加え、すべてのディレクトリーで監査できないオブジェクトを許可します。

表 26. 新しいオブジェクトの権限システム値として指定できる値 (続き)

すべて	*ALL	新しく作成されたオブジェクトを完全に制御する許可を、「すべて (ALL)」未満の権限を与えられたユーザーを除き、システムのすべてのユーザーに与えます。こうしたユーザーは、そのようなオブジェクトの読み取り、変更、削除、およびセキュリティーの管理が可能です。
除外	*EXCLUDE	共通権限では、新しいオブジェクトの使用は許可されていない。

セキュリティー・ポリシーとの関係

表 27. 早見表 : 新しいオブジェクトの権限システム値に関する詳細を提供します。

iSeries ナビゲーター名	QSYS.LIB ファイル・システムで新しく作成されたオブジェクトのデフォルト権限
文字ベースのインターフェース名	QCRTAUT
権限	*ALLOBJ *SECADM **注:** QSECOFR ユーザー・プロファイルにはこれらの権限が付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**セキュリティー・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**共通権限**」ページで、このシステム値のオプションを見つけます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QCRTAUT` と入力します。
変更内容が有効になる時点	即時
デフォルト値	変更
推奨値	変更
ロック可能	はい
特別な考慮事項	新しいオブジェクトの権限システム値は、拡張ファイル・システムのディレクトリー内で作成されたオブジェクトには使用されません。 QSYS を含めいくつかの IBM 提供ライブラリーには、システム値 (*SYSVAL) を指し示す作成権限 (CRTAUT) コマンド・セットがあります。

このセキュリティー値の詳細については、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

ファイル・システムのスキャン:

このシステム値を使用すると、統合ファイル・システムのスキャン関連出口プログラムを使ってファイル・システムをスキャンするかどうか指定できます。

出口プログラムの定義方法に応じて、さまざまな理由でスキャンを実行できます。たとえば、特定のテキスト・ストリング、ファイル名、ウィルスを捜すためにスキャンすることができます。統合ファイル・システムのスキャンは、出口プログラムが統合ファイル・システムのスキャン関連の出口点で登録されているときに使用可能です。

このシステム値の詳細に関する表 29を参照してください。

表 28. ファイル・スキャン・システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
選択解除	*NONE	統合ファイル・システムのオブジェクトはスキャンされない。
選択	*ROOTOPNUD	『root』 (/)、QOpenSys、およびユーザー定義ファイル・システム内の *TYPE2 [1] ディレクトリーに保管されたストリーム・ファイル・オブジェクトがスキャンされます。

1. 統合ファイル・システムは、いくつかの異なるファイル・システムから構成されます。ファイル・システムは複数のディレクトリーから成り、ディレクトリーのフォーマットは互いに異なる場合があります。*TYPE2 ディレクトリーの中でファイルを管理すると、パフォーマンス、信頼性、機能性、および能力が改善されます。このようなディレクトリー・タイプについて、詳しくは*TYPE2 ディレクトリーを参照してください。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、ウィルスについて、および疑わしいプログラムを捜すための個人用システムのスキャンについて、明確に記載することが重要です。出口プログラムは、ウィルスに対する保護を提供します。これらのシステム値は、出口プログラムを呼び出すかどうかを指定します。

表 29. 早見表 : 「ファイル・システムのスキャン」システム値に関する詳細を示します。

iSeries ナビゲーター名	**『root』 (/)、QOpenSys、およびユーザー定義ファイル・システムをスキャンするための、登録済み出口プログラムの使用**
文字ベースのインターフェース名	QSCANFS
権限	*ALLOBJ *SECADM **注:** QSECOFR ユーザー・プロファイルにはこれらの権限が付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**セキュリティー・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**スキャン**」ページに、セキュリティー情報保持のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QSCANFS` と入力します。
変更内容が有効になる時点	即時

表 29. 早見表 (続き) : 「ファイル・システムのスキャン」システム値に関する詳細を示します。

iSeries ナビゲーター名	**『root』 (/)、QOpenSys、およびユーザー定義ファイル・システムをスキャンするための、登録済み出口プログラムの使用**
デフォルト値	選択 (*ROOTOPNUD)
ロック可能	可
特別な考慮事項	「ファイル・システム・スキャンの制御」システム値に関連したオプションを使用すれば、スキャン対象ファイルをより細かく制御できます。

このセキュリティー値の詳細については、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

ファイル・システムのスキャンの制御:

「ファイル・システムのスキャン制御」システム値は、出口プログラムが統合ファイル・システムのスキャン関連の出口点で登録されているときに使用可能な、統合ファイル・システムのスキャンを制御します。

このシステム値は「ファイル・システムのスキャン」システム値とともに機能して、統合ファイル・システムでのスキャン対象とスキャン方法をより細かく制御します。別のスキャン・オプションを選択したり、デフォルト・スキャン・オプションの使用を選択することができます (デフォルトの場合、以下のスキャン制御が提供されます)。

- 書き込みアクセス更新の実行
- 閉じる際にスキャンが失敗した場合、クローズ要求が失敗する
- オブジェクトの復元後、次のアクセスの際にスキャン

このシステム値の詳細についての 59 ページの表 31を参照してください。

オプションで、登録済み出口プログラムによるスキャンの対象と方法を制御するいくつかのスキャン・オプションを選択することもできます。これらのオプションについて、以下の表に示します。

表 30. 「ファイル・システムのスキャン制御」システム値に指定できる値

iSeries ナビゲーター	**文字ベースのインターフェース**	**説明**
選択なし	*NONE	統合ファイル・システムのスキャン関連の出口点に対する制御は指定されない。
ファイル・サーバーを通したアクセスのみをスキャン	*FSVRONLY	ファイル・サーバーを介したシステムへのアクセスのみがスキャンされる。システムへのネイティブ接続つまり直接接続はスキャンされません。このオプションを選択しない場合、システムへの直接接続かファイル・サーバーを介した接続かを問わず、すべてのアクセスがスキャンされます。

表 30. 「ファイル・システムのスキャン制御」システム値に指定できる値 (続き)

iSeries ナビゲーター	文字ベースのインターフェース	説明
出口プログラムが失敗した場合は、要求を断念する	*ERRFAIL	このオプションは、出口プログラムの呼び出し中にエラーが発生した場合、出口プログラムを開始した要求または操作を中止することを指定します。その場合、そのオブジェクトのスキャンが失敗したという通知が要求元の操作に送られます。このオプションを選択しない場合、システムは失敗した出口プログラムをスキップして、オブジェクトがその出口プログラムによってスキャンされなかったかのように扱います。
書き込みアクセスの更新を実行する (選択) [1]	なし	このオプションを指定すると、システムは、出口プログラムに渡されるスキャン記述子のアクセスに (可能であれば) 書き込みアクセスを含めるよう更新します。元々は読み取り専用アクセスで開かれた場合でも、出口プログラムがオブジェクトを修正または変更できるようにしたい場合には、このオプションを使用してください。
書き込みアクセスの更新を実行する (選択解除)	*NOWRTUPG	このオプションは、システムが書き込みアクセスを含めるようにアクセスを更新しないことを指定します。
スキャンを制御するために「**オブジェクトが変更された場合のみ**」属性を使用する	*USEOCOATR	このオプションを使用すると、システムはオブジェクトが変更された場合に「オブジェクト変更のみ」スキャン属性を指定します。
閉じる際にスキャンが失敗した場合、クローズ要求が失敗する	*NOFAILCLO	このオプションは、クローズ処理中にオブジェクトのスキャンに失敗した場合、システムがクローズ要求を中止することを指定します。このオプションはクローズ要求だけに適用されます。**「出口プログラムが失敗した場合は、要求を断念する」**オプションを選択し、このオプションを選択しない場合には、クローズ処理中にオブジェクトのスキャンが失敗しても、システムは失敗の通知を送りません。しかし、オブジェクトはスキャン失敗とマークされます。

表 30. 「ファイル・システムのスキャン制御」システム値に指定できる値 (続き)

iSeries ナビゲーター	文字ベースのインターフェース	説明
オブジェクトの復元後、次のアクセスの際にスキャン	*NOPOSTRST	このオプションを指定すると、オブジェクトのスキャン属性の定義にかかわらず、復元後のオブジェクトがスキャンされます。オブジェクトのスキャン属性が「オブジェクトはスキャンされない」であっても、このオプションにより、復元後のオブジェクトが強制的にスキャンされます。オブジェクトのスキャン属性が「最後のスキャン以降に変更された場合のみ、オブジェクトをスキャン」である場合、復元操作はオブジェクト変更操作と見なされるため、復元後のオブジェクトはスキャンされます。

セキュリティー・ポリシーとの関係

スキャン制御オプションは、統合ファイル・システムのスキャン関連出口プログラムの使用に関して、より細かい制御を可能にします。これらのオプションをセキュリティー上の目的で使用すれば、ウィルスを検出するよう設計された出口プログラムを使って、統合ファイル・システム内に潜んでいるコンピューター・ウィルスや疑わしいプログラムをより効率的に検出できます。

表 31. 早見表 : 「ファイル・システムのスキャン制御」システム値の詳細を示します。

iSeries ナビゲーター名	スキャン制御
文字ベースのインターフェース名	QSCANFSCTL
権限	*ALLOBJ *SECADM **注:** QSECOFR ユーザー・プロファイルにはこれらの権限が付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**セキュリティー・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**スキャン**」ページに、スキャン制御のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QSCANFSCTL` と入力します。
変更内容が有効になる時点	即時
デフォルト値	デフォルトのスキャン制御オプションの使用

表 31. 早見表 (続き) : 「ファイル・システムのスキャン制御」システム値の詳細を示します。

iSeries ナビゲーター名	**スキャン制御**
推奨値	**厳格なセキュリティー環境の場合** **「出口プログラムが失敗した場合は、要求を断念する」**オプションを選択して、**「書き込みアクセスの更新を実行する」**を必ず選択解除します。オプションをこのように設定すれば、スキャン出口プログラムが失敗した場合は常に、関連する操作またはスキャン出口プログラムは追加のアクセス・レベルを得られません。 **それほど厳格ではないセキュリティー環境の場合** ほとんどの環境では、これらのオプションを選択しないか、デフォルト・オプションを使用することができます。
ロック可能	可
特別な考慮事項	信頼できるソースから配信されたコードを導入するときは、導入中に**「オブジェクトの復元後、次のアクセス時にスキャンする」**を指定することをお勧めします。

このセキュリティー値の詳細については、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

サインオン・システム値

ユーザーがシステムにサインオンするする方法を決定する必要があります。

サインオンは、システムに対する権限を持つユーザーが資源にアクセスすることを許可します。サインオンは、ユーザー名と、それに関連したパスワードから成ります。システム値は、どのユーザーが、どんな方法で、どの装置にサインオンできるかを制御します。さらに、ユーザーがサインオン規則に違反した場合にシステムが取る処置を制御します。サインオン・システム値は、サインオン環境を設定するシステム値、対話式ジョブのサインオンを処理するシステム値、および特定のユーザーと装置にサインオンを限定するシステム値に分類されます。

サインオン環境

3 つのシステム値を使用して、組織のユーザー用のサインオン環境を作成することができます。これらのシステム値は、サインオン・アクティビティーに関する情報や、システムが処置を取るまでにユーザーに許容されるサインオン試行回数を提供します。ユーザーのサインオン環境を制御するシステム値には、以下のものがあります。

- サインオン情報の表示
- サインオンの最大試行回数
- サインオン最大試行回数処置

対話式ジョブ

対話式ジョブの場合、タスクを実行するために、ユーザーとシステムの間で両方向の通信が継続されなければなりません。対話式ジョブが始まるのは、ユーザーがシステムにサインオンし、要求を入力して、システムが要求を処理することによって応答したときです。このパターンは、ユーザーがシステムからサインオフ

することによって対話式ジョブを終了するまで繰り返されます。以下のような 3 つのサインオン関連システム値が一体的に機能して、対話式ジョブ処理時のセキュリティーを提供します。

- 非活動ジョブのタイムアウト間隔
- タイムアウト間隔処置
- 切り離しジョブのタイムアウト間隔

サインオン制限

場合によっては、システム資源にアクセスできるユーザーと装置を限定する必要があるかもしれません。全オブジェクト (*ALLOBJ) 権限および機密保護担当者 (*SECOFR) 権限を持つユーザーが特定のワークステーションや装置だけを使用できるように、制限するする必要があるかもしれません。さらに、物理的セキュリティーに問題のあるワークステーション (たとえば、人目につかない場所にあり、システムにアクセスするために無許可ユーザーに利用されかねないコンピューター) もまた、制限の対象とすべきでしょう。

- 72 ページの『機密保護担当者の限界』
- 71 ページの『装置セッションの制限』
- 74 ページの『リモート・サインオン制御』

サインオン情報の表示:

このシステム値を使用すると、ユーザーは自分のプロファイルの使用の試行を監視し、新しいパスワードが必要になる時点を知ることができます。

このシステム値は、ユーザーのサインオン時に、前回のサインオンの日時、前回のサインオン以降の無効なサインオン試行の数、(パスワード期限切れまで 7 日以内になった場合) パスワードが期限切れになるまでの日数などの情報を表示するかどうかを制御します。

このシステム値の概要については、表 33を参照してください。

表 32. 「サインオン情報の表示」システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
選択解除	0 (いいえ)	画面は表示されない。
選択	1 (はい)	画面が表示される。

セキュリティー・ポリシーとの関係

企業のセキュリティー・ポリシーの中で、ユーザーのサインオン・アクティビティーをどのように管理すべきかをユーザーに知らせる必要があります。サインオン情報表示システム値を使用すれば、サインオン試行およびパスワード期限切れに関する情報をユーザーに提示することができます。このシステム値によって生成されるタイム・スタンプ情報を使用して、ユーザーはシステムへのサインオン試行を監視することができます。サインオンが不適切に使用された疑いがある場合、ユーザーが何をすべきかをセキュリティー・ポリシーの中に明記する必要があります。

表 33. 早見表 : サインオン情報表示システム値の詳細を示します。

iSeries ナビゲーター名	サインオン情報の表示
文字ベースのインターフェース名	QDSPSGNINF

表 33. 早見表 (続き): サインオン情報表示システム値の詳細を示します。

iSeries ナビゲーター名	**サインオン情報の表示**
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**サインオン・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**一般**」ページに、サインオン情報の表示オプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、WRKSYSVAL QDSPSGNINF と入力します。
変更内容が有効になる時点	即時
デフォルト値	選択解除 (0)
推奨値	選択 (1)
ロック可能	可
特別な考慮事項	なし

このセキュリティー値の詳細については、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

サインオンの最大試行回数:

「サインオンの最大試行回数」システム値は、ローカル・ユーザーおよびリモート・ユーザーが誤ったサインオンを連続して試行できる回数を制限します。

誤ったサインオン試行の原因として、ユーザー ID やパスワードの誤り、または装置に対する不十分な権限が考えられます。「サインオンの最大試行回数」システム値は、サインオン最大試行回数に達した場合にシステムがどんな処置を取るかを指定するシステム値とともに機能します。関連するシステム値については、「サインオン最大試行回数処置」を参照してください。

パスワードを推測してシステムに侵入しようとするハッカーは少なくありません。サインオンを試行できる回数を制限することにより、このような人物によるパスワードの推測を制限できます。「サインオンの最大試行回数」システム値は、サインオン試行が何回まで許容されるかを決定します。通常は、ユーザーが不満に感じない程度の高い値と、侵入者に推測を繰り返させない低い値のバランスを取って値を設定するのが適切でしょう。ほとんどの場合、サインオン試行の回数として 3 から 5 の値を設定すれば、両方の要件を満たすことができます。

「サインオンの最大試行回数」システム値の概要については、早見表を参照してください。

表 34. サインオン最大試行回数システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
最大なし	*NOMAX	システムは、誤ったサインオン試行を無制限に許容する。この値は、潜在的な侵入者に対して、ユーザーID とパスワードの正しい組み合わせを試行するための機会を無制限に与えることになります。
最大数 (Maximum number)	*制限*	1 から 25 までの値を指定。サインオン試行回数の推奨値は 3 です。 通常、試行回数を 3 にすれば、ユーザーは入力ミスを修正することができ、同時に無許可アクセスを防止することもできます。

セキュリティー・ポリシーとの関係

企業のセキュリティー・ポリシーの中で、ユーザーのサインオン・アクティビティーをどのように管理すべきかをユーザーに知らせる必要があります。サインオン試行が何回までユーザーに許されているか、その回数を超えた場合にどんな処置が取られるかを明記することが重要です。

表 35. 早見表 : サインオン最大試行回数システム値についての詳細を示します。

iSeries ナビゲーター名	誤ったサインオンの試行回数
文字ベースのインターフェース名	QMAXSIGN
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**サインオン・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**一般**」ページに、サインオン最大試行回数のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QMAXSIGN` と入力します。
変更内容が有効になる時点	即時
デフォルト値	3
推奨値	3
ロック可能	可
特別な考慮事項	このシステム値の特別な考慮事項については、「サインオン最大試行回数処置」を参照してください。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

サインオン最大回数処置:

「サインオンの最大試行回数処置」システム値は、ワークステーションにおいてサインオンの最大試行回数に達した場合のシステム処置を決定します。

このシステム値は、「サインオンの最大試行回数」システム値とともに機能して、システムへの無許可サインオンを防止します。

「サインオン最大回数処置」システム値の概要に関する 表 37を参照してください。

表 36. サインオン最大試行回数処置システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
ユーザーの使用不可	2	ユーザー・プロファイルのみを使用禁止にする。
装置の使用不可	1	装置のみを使用禁止にする。
ユーザーおよび装置の使用不可	3	ユーザー・プロファイルと装置の両方を使用禁止にする。

セキュリティー・ポリシーとの関係

企業のセキュリティー・ポリシーの中で、ユーザーのサインオン・アクティビティーをどのように管理すべきかをユーザーに知らせる必要があります。サインオン試行が何回までユーザーに許されているか、その回数を超えた場合にどんな処置が取られるかを明記することが重要です。

表 37. 早見表 : サインオン最大回数処置システム値についての詳細を示します。

iSeries ナビゲーター名	最大に達した時
文字ベースのインターフェース名	QMAXSIGNACN
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**サインオン・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**一般**」ページに、サインオン最大試行回数のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QMAXSIGNACN` と入力します。
変更内容が有効になる時点	即時
デフォルト値	ユーザーおよび装置の使用不可 (3)
推奨値	ユーザーおよび装置の使用不可 (3)
ロック可能	可

表 37. 早見表 (続き): サインオン最大回数処置システム値についての詳細を示します。

iSeries ナビゲーター名	最大に達した時
特別な考慮事項	サインオン最大試行回数の推奨値は、ユーザーが正しいユーザー ID とパスワードの組み合わせを使用するまで、連続して 3 回までサインオン試行を許可することです。許容される誤ったサインオン試行回数を超えた場合、システムはそのユーザーのプロファイルを使用不可にして、ユーザーがサインオンしようとした装置をオフに変更します。 再度サインオンするためにユーザー・プロファイルを使用可能にするには、CHGUSRPRF USRPRF(profile-name) STATUS(*ENABLED) というコマンドを使用します。 再度サインオンするためにワークステーションを使用可能にするには、構成状況処理 (WRKCFGSTS) コマンドを使って装置をオンに変更します。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

非活動ジョブのタイムアウト間隔:

「非活動ジョブのタイムアウト間隔」システム値は、ジョブが非活動状態になった場合にシステムが処置をとるまで待つ時間を分単位で指定します。

メニューまたは画面を表示して待機している場合、またはメッセージ入力を待っているがユーザー対話がない場合、ワークステーションは非活動状態と見なされます。ユーザー対話とは、Enter キー、ページング機能、機能キー、およびヘルプ機能を使用することです。

システムは、どのジョブが非活動状態であるかを判別します。たとえば、あるユーザーが同じディスプレイ装置上で 2 番目の対話式ジョブを開始した場合、いずれかのジョブで対話 (たとえば Enter キーを押すこと) が発生すると、両方のジョブが活動状態と見なされます。

「非活動ジョブのタイムアウト間隔」システム値は、ジョブの非活動状態が指定された時間間隔を超えた場合にシステムが取る処置を決定するシステム値とともに機能します。関連するシステム値については、タイムアウト間隔処置を参照してください。システムが始動すると、タイムアウト間隔に達した (または超過した) 非活動ジョブがあるかどうか検査します。システムが午前 9:30 に始動し、タイムアウト間隔が 30 分に設定されている場合、システムは 10:00、10:30、11:00 という間隔で非活動ジョブを検査します。30 分以上にわたって非活動状態であったジョブが検出されると、タイムアウト間隔処置システム値で指定された処置がとられます。これらの 2 つのシステム値により、ユーザーがサインオンしたまま非活動状態のワークステーションを離れるのを防ぐことができ、セキュリティーが保持されます。非活動状態のワークステーションからは、無許可のユーザーがシステムにアクセスする可能性があります。

「非活動ジョブのタイムアウト間隔」システム値の概要については、早見表を参照してください。

表 38. 非活動ジョブ・タイムアウト間隔システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
タイムアウトなし	*NONE	システムは非活動ジョブを検査しない。
5 分から 300 分	*分単位間隔*	5 から 300 までの値を指定。

セキュリティー・ポリシーとの関係

企業のセキュリティー・ポリシーの中で、ユーザーのサインオン・アクティビティーをどのように管理すべきかをユーザーに知らせる必要があります。非活動状態の端末を介して誰かがシステムにアクセスできる可能性があるため、非活動状態のジョブはシステム資源に対するリスクとなる可能性があります。しかし、日常の仕事ではワークステーションの前にいるユーザーの作業がしばしば中断されるため、そのような中断を見込んである程度の柔軟性を持たせる必要があります。対話式ジョブ・システム値を使用すれば、システム資源のセキュリティーを維持し、ユーザーがさまざまな業務を行う上での柔軟性を提供することができます。セキュリティー・ポリシーの中で、ワークステーションおよびアクセス先システムに対するユーザーのサインオン・アクティビティーについて指針を明示する必要があります。たとえば、ユーザーは自分のワークステーションをパスワードで保護し、ワークステーションを離れるたびにパスワード保護を有効にすべきです。システムに対する作業の実行中にユーザーがワークステーションを離れる必要がある場合、いわば第 1 の壁として、ワークステーションをロックすることにより、誰かがそのワークステーションを介してシステムにアクセスするのを防ぐことができます。ただし、パスワード保護は防御の第 1 段階にすぎません。悪意のあるユーザーがシステム資源に決してアクセスできないようにするために、対話式ジョブ・システム値を使用してください。

非活動状態のジョブ用のタイムアウト間隔を超過した場合、システムは指定されたタイムアウト間隔処置を行います。その処置がジョブの切断である場合には、ジョブを切断する前に、システムはタイムアウト間隔の経過を待ちます。その処置がジョブの終了である場合には、ジョブを終了する前に、システムはタイムアウト間隔の経過を待ちます。非活動ジョブ・タイムアウト間隔を 30 分に設定し、非活動ジョブ処置としてジョブの切断を設定したとします。さらに、切り離しジョブのタイムアウト間隔を 300 分 (つまり 5 時間) に設定したとします。あるユーザーが 午前 9:30 にサインオフし忘れた場合、システムは午前 10:00 にそのユーザーのジョブを切断し、午後 3:00 にジョブを終了します。

システムが切り離しジョブを終了すると、システムにまだ入力されていないユーザー画面上のすべてのデータは失われます。切り離しジョブのタイムアウトが経過する前にユーザーが同じワークステーションにサインオンした場合、システムによって切断された時点からジョブが再開します。

表 39. 早見表 : 非活動ジョブ・タイムアウト間隔システム値の詳細を示します。

iSeries ナビゲーター名	**タイムアウト間隔**
文字ベースのインターフェース名	QINACTITV
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**構成およびサービス**」 → 「**システム値**」を展開します。 2. 「**ジョブ**」を右クリックして、「**プロパティー**」を選択します。 3. 「**対話式ジョブ**」ページに、非活動ジョブ用のタイムアウト間隔のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QINACTITV` と入力します。
変更内容が有効になる時点	即時
デフォルト値	タイムアウトなし

表 39. 早見表 (続き)： 非活動ジョブ・タイムアウト間隔システム値の詳細を示します。

iSeries ナビゲーター名	**タイムアウト間隔**
推奨値	60 分
ロック可能	可
特別な考慮事項	このシステム値は、非活動ジョブのタイムアウト間隔処置、および切り離しジョブのタイムアウト間隔システム値とともに使用されます。これらのシステム値をすべて使用すれば、非活動状態かつ切断されたジョブを適切に終了させることができます。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

タイムアウト間隔処置:

タイムアウト間隔処置システム値は、ジョブがタイムアウト間隔に達した場合にシステムが何をするかを指定します。

ジョブの終了を選択した場合、システムは指定されたタイムアウト間隔より長く非活動状態が続いたすべてのジョブを終了します。さらに、非活動ジョブの切断を選択したり、メッセージ待ち行列の名前を指定することができます (ジョブの非活動状態が長く続いた場合、システムはこの待ち行列に警告メッセージを送ります)。対話式ジョブで作業している場合、このシステム値はタイムアウト間隔システム値とともに機能して、指定された時間の経過後に取る処置を決定します。

タイムアウト間隔処置システム値の概要については、早見表を参照してください。

表 40. タイムアウト間隔処置システム値に指定できる値

iSeries ナビゲーター	**文字ベースのインターフェース**	**説明**
ジョブ終了	*ENDJOB	非活動ジョブが終了する。非活動ジョブがグループ・ジョブである場合、そのグループに関連するすべてのジョブも終了します。ジョブが 2 次ジョブの一部である場合は、両方のジョブが終了します。
ジョブの切り離し	*DSCJOB	非活動ジョブは、2 次ジョブまたはそれに関連するグループ・ジョブとともに切り離されます。ジョブを切断できない場合、そのジョブは終了されます。切り離しジョブ・タイムアウト間隔システム値により、システムが最終的に切り離しジョブを終了するかどうかを制御します。
メッセージの送信	*メッセージ待ち行列名*	非活動ジョブ・タイムアウト間隔に達したとき、指定された待ち行列にメッセージ CPI1126 が送信されます。このメッセージは、以下のように表示されます。ジョブ &3/&2/&1 が活動状態になっていない。

セキュリティー・ポリシーとの関係

企業のセキュリティー・ポリシーの中で、ユーザーのサインオン・アクティビティーをどのように管理すべきかをユーザーに知らせる必要があります。非活動状態の端末を介して誰かがシステムにアクセスできる可能性があるため、非活動状態のジョブはシステム資源に対するリスクとなる可能性があります。しかし、日常の仕事ではワークステーションの前にいるユーザーの作業がしばしば中断されるため、そのような中断を見込んである程度の柔軟性を持たせる必要があります。対話式ジョブ・システム値を使用すれば、システム資源のセキュリティーを維持し、ユーザーがさまざまな業務を行う上での柔軟性を提供することができます。セキュリティー・ポリシーの中で、ワークステーションおよびアクセス先システムに対するユーザーのサインオン・アクティビティーについて指針を明示する必要があります。たとえば、ユーザーは自分のワークステーションをパスワードで保護し、ワークステーションを離れるたびにパスワード保護を有効にすべきです。システムに対する作業の実行中にユーザーがワークステーションを離れる必要がある場合、いわば第 1 の壁として、ワークステーションをロックすることにより、誰かがそのワークステーションを介してシステムにアクセスするのを防ぐことができます。ただし、パスワード保護は防御の第 1 段階にすぎません。悪意のあるユーザーがシステム資源に決してアクセスできないようにするために、対話式ジョブ・システム値を使用してください。

非活動ジョブ用のタイムアウト間隔を超過した場合、システムは指定されたタイムアウト間隔処置を行います。さらに、その処置がジョブの切断であれば、ジョブを終了する前に、システムは切り離しジョブ・タイムアウト間隔の経過を待ちます。非活動ジョブ・タイムアウトを 30 分に設定し、切り離しジョブ・タイムアウト間隔を 300 分つまり 5 時間に設定したとします。あるユーザーが 午前 9:30 にサインオフし忘れた場合、システムは午前 10:00 にそのジョブを切断し、午後 3:00 にジョブを終了します。

システムがジョブを終了または切断すると、システムにまだ入力されていないユーザー画面上のすべてのデータは失われます。切り離しジョブのタイムアウトが経過する前にユーザーが同じワークステーションにサインオンした場合、システムによって切断された時点からジョブが再開します。

表 41. 早見表 : タイムアウト間隔処置システム値の詳細を示します。

iSeries ナビゲーター名	**ジョブがタイムアウトに達するとき (When job reaches timeout)**
文字ベースのインターフェース名	QINACTMSGQ
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**構成およびサービス**」 → 「**システム値**」を展開します。 2. 「**ジョブ**」を右クリックして、「**プロパティー**」を選択します。 3. 「**対話式ジョブ**」ページに、タイムアウト間隔処置のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QINACTMSGQ` と入力します。
変更内容が有効になる時点	即時
デフォルト値	ジョブ終了

表 41. 早見表 (続き): タイムアウト間隔処置システム値の詳細を示します。

iSeries ナビゲーター名	**ジョブがタイムアウトに達するとき (When job reaches timeout)**
推奨値	ユーザーが iSeries Access ジョブを実行していない限り、ジョブを使用不可にする値を使用してください。iSeries Access ジョブの実行中にジョブを使用不可にすることは、ジョブを終了することと同等で、多くの情報が失われる可能性があります。iSeries Access ライセンス・プログラムがある場合には、メッセージ待ち行列オプションを使用してください。「CL プログラミング」の第 8 章『メッセージ処理』には、メッセージを処理するプログラムの作成例が記載されています。
ロック可能	可
特別な考慮事項	このシステム値は、非活動ジョブのタイムアウト間隔、および切り離しジョブのタイムアウト間隔システム値とともに使用されます。これらのシステム値をすべて使用すれば、非活動状態かつ切断されたジョブを適切に終了させることができます。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

切り離しジョブのタイムアウト間隔:

「切り離しジョブ・タイムアウト間隔」システム値は、切り離されたジョブが終了される前に非活動状態になる時間の長さ、およびジョブがタイムアウトに達した場合に取る処置を指定します。

非活動状態のジョブを切り離すタイムアウト間隔処置を設定する場合、ジョブを最終的に終了するために、切り離しジョブのタイムアウトを設定する必要があります。

切り離しジョブ (切断されたジョブ) は、システム資源を使い果たすだけでなく、オブジェクトに対するロックをすべて保持します。 2 人のユーザーが同じ情報を同時に変更しようとするのを防ぐため、システムは、情報を更新する前にレコードをロックします。資源に対するロックは、システムがユーザーのジョブを切断しても有効です。ご使用になるアプリケーションの設計、およびシステム上のユーザーの数によっては、ロックがシステムでパフォーマンス上の問題を引き起こす場合があります。プログラマーまたはアプリケーションの提供者に確認して、ロックがパフォーマンスに悪影響を与えるかどうかを判別してください。

「切り離しジョブのタイムアウト間隔」システム値の概要については、早見表を参照してください。

表 42. 切り離しジョブ・タイムアウト間隔システム値に指定できる値

iSeries ナビゲーター	**文字ベースのインターフェース**	**説明**
タイムアウト間隔 (5 分から 1,440 分)	*分単位の時間設定*	5 分から 1,440 分までの値を指定。
タイムアウトなし	*NONE	システムは、切り離しジョブを自動終了しない。システム・パフォーマンスを維持してオブジェクトのロックを解除するために、手動でジョブを終了する必要があるかもしれません。

表 42. 切り離しジョブ・タイムアウト間隔システム値に指定できる値 (続き)

iSeries ナビゲーター	文字ベースのインターフェース	説明
選択なし	240	どのオプションも選択しない場合、システムは切り離しジョブを終了するためにデフォルト値 240 分を使用する。

セキュリティー・ポリシーとの関係

企業のセキュリティー・ポリシーの中で、ユーザーのサインオン・アクティビティーをどのように管理すべきかをユーザーに知らせる必要があります。非活動状態の端末を介して誰かがシステムにアクセスできる可能性があるため、非活動状態のジョブはシステム資源に対するリスクとなる可能性があります。しかし、日常の仕事ではワークステーションの前にいるユーザーの作業がしばしば中断されるため、そのような中断を見込んである程度の柔軟性を持たせる必要があります。対話式ジョブ・システム値を使用すれば、システム資源のセキュリティーを維持し、ユーザーがさまざまな業務を行う上での柔軟性を提供することができます。セキュリティー・ポリシーの中で、ワークステーションおよびアクセス先システムに対するユーザーのサインオン・アクティビティーについて指針を明示する必要があります。たとえば、ユーザーは自分のワークステーションをパスワードで保護し、ワークステーションを離れるたびにパスワード保護を有効にすべきです。システムに対する作業の実行中にユーザーがワークステーションを離れる必要がある場合、いわば第 1 の壁として、ワークステーションをロックすることにより、誰かがそのワークステーションを介してシステムにアクセスするのを防ぐことができます。ただし、パスワード保護は防御の第 1 段階にすぎません。悪意のあるユーザーがシステム資源に決してアクセスできないようにするために、対話式ジョブ・システム値を使用してください。

ジョブが非活動状態のジョブ用のタイムアウト間隔を超過した場合、システムは指定されたタイムアウト間隔処置を行います。その処置がジョブの切断である場合には、ジョブを切断する前に、システムはタイムアウト間隔の経過を待ちます。さらに、切断されたジョブのタイムアウト間隔をも超過した場合には、システムはジョブを終了します。非活動ジョブ・タイムアウト間隔を 30 分に設定し、切り離しジョブ・タイムアウト間隔を 300 分つまり 5 時間に設定したとします。あるユーザーが 午前 9:30 にサインオフし忘れた場合、システムは午前 10:00 にそのユーザーのジョブを切断し、午後 3:00 にジョブを終了します。

システムが切り離しジョブを終了すると、システムにまだ入力されていないユーザー画面上のすべてのデータは失われます。切り離しジョブのタイムアウトが経過する前にユーザーが同じワークステーションにサインオンした場合、システムによって切断された時点からジョブが再開します。

表 43. 早見表 : 切り離しジョブ・タイムアウト間隔システム値の詳細を示します。

iSeries ナビゲーター名	切り離しジョブ
文字ベースのインターフェース名	QDSCJOBITV
権限	なし

表 43. 早見表 (続き)： 切り離しジョブ・タイムアウト間隔システム値の詳細を示します。

iSeries ナビゲーター名	**切り離しジョブ**
アクセス方法	**iSeries ナビゲーター** 1. 「**構成およびサービス**」 → 「**システム値**」を展開します。 2. 「**ジョブ**」を右クリックして、「**プロパティー**」を選択します。 3. 「**対話式ジョブ**」ページに、切り離しジョブ用のタイムアウト間隔のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、WRKSYSVAL QDSCJOBITV と入力します。
変更内容が有効になる時点	即時
デフォルト値	240
推奨値	300
ロック可能	可
特別な考慮事項	このシステム値は、非活動状態のジョブ用のタイムアウト間隔およびタイムアウト間隔処置システム値とともに使用してください。これらのシステム値をすべて使用すれば、非活動状態かつ切断されたジョブを適切に終了させることができます。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

装置セッションの制限:

「装置セッションの制限」システム値は、ユーザーが同時に複数の装置でサインオンすることを許可するかどうかを指定します。

この値によって、システム要求メニューまたはその同じ装置からの 2 番目のサインオンが制限されることはありません。ユーザーに切り離しジョブがある場合、ユーザーは新しい装置セッションでシステムにサインオンできます。ユーザーが同時に 1 つのワークステーションでしかサインオンできないようにすることは、セキュリティーを促進する良い方法です。ユーザーを 1 つの装置に制限する場合は、ユーザー ID とパスワードの共用が行われないようにする必要があります。ユーザー ID が共用されると、制御も責任能力も失われます。システム上で実際に誰がどの機能を使用しているのか分からなくなります。加えて、ユーザーは、他のワークステーションに移る際に、必ずワークステーションをサインオフしなければなりません。ワークステーションを使用しないのにサインオンしたままにしておくと、セキュリティー上のリスクが生じます。すべてのシステム・ユーザーに対して、固有のユーザー ID とパスワード、および適切な権限を与えるとともに、同時に 1 つのワークステーションだけを使用できるように制限してください。また、個別のユーザー・プロファイルを介して、ユーザーを特定の装置に制限することもできます。

装置セッション制限システム値に関する概要を示した 72 ページの表 45を参照してください。

表 44. 装置セッション制限システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
選択解除	0 (いいえ)	システムにより、サインオン・セッションの数が制限なく許可される。
選択	1 (はい)	ユーザーは、1 つの装置セッションに限定される。

セキュリティー・ポリシーとの関係

装置セッション制限システム値を設定すると、ユーザーによるパスワードの共用、およびサインオンしたままワークステーションを離れることが抑制されます。ただし、このシステム値をどのように決定するかにかかわらず、セキュリティー・ポリシーの中でこのような行為を暗黙的に禁止する必要があります。このような不適切な習慣が原因で、アタッカーが企業の資源や重要なビジネス情報にアクセスする可能性があります。セキュリティー・ポリシーの中で、このような行為のリスクおよび考えられる結果をユーザーに明示してください。

表 45. 早見表 : 装置セッション制限システム値の詳細を示します。

iSeries ナビゲーター名	各ユーザーを 1 装置セッションに限定する
文字ベースのインターフェース名	QLMTDEVSSN
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**サインオン・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**一般**」ページに、装置セッション制限のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QLMTDEVSSN` と入力します。
変更内容が有効になる時点	即時
デフォルト値	選択解除
推奨値	選択
ロック可能	可
特別な考慮事項	なし

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

機密保護担当者の限界:

セキュリティーを変更してオブジェクトを制御する権限を持つユーザーを、 特定のワークステーションに制限することができます。

この制限により、把握しにくい離れた場所にあるワークステーションでこれらのユーザーがサインオンするのを防ぐことができます。「機密保護担当者の限界」システム値は、全オブジェクト (*ALLOBJ) 特殊権限またはサービス (*SERVICE) 特殊権限を持つユーザーが任意のワークステーションにサインオンできるかどうかを制御します。強力なユーザー・プロファイルを、適切に制御された特定のワークステーションに限定することにより、セキュリティー保護が可能になります。このシステム値は、機密保護担当者、システム上のすべてのオブジェクトに対する権限を持つユーザー、およびサービス担当員をコンソールに制限します。他の装置へのアクセスをこれらのユーザーに与えるには、GRTOBJAUT コマンドを使用できます。

「機密保護担当者の限界」システム値の概要については、早見表を参照してください。

表 46. 「機密保護担当者の限界」システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
選択解除	0 (いいえ)	*ALLOBJ または *SERVICE 特殊権限を持つユーザーは、変更 (*CHANGE) 権限を持つ任意の表示装置にサインオンできる。ユーザーは、私用権限または共通権限を介して *CHANGE 権限を受け取ることができる。 または、ユーザーは *ALLOBJ 特殊権限を持っているためにこの権限を受け取ることができる。
選択	1 (はい)	*ALLOBJ 特殊権限または *SERVICE 特殊権限を持つユーザーは、表示装置に対して特別に認可を受けている (つまり、*CHANGE 権限を与えられている) か、またはユーザー・プロファイル QSECOFR がその表示装置に対する認可を受けている (*CHANGE 権限を与えられている) 場合にのみ、表示装置でサインオンできる。この権限は、共通権限に由来するものであってはならない。

セキュリティー・ポリシーとの関係

*ALLOBJ および *SERVICE 特殊権限を持つユーザーによるワークステーション・アクセスを制限することにより、これらのユーザーが行うアクティビティーを監視できます。対象となる装置へのユーザー・アクセスを監視して、不審なアクティビティーがあれば即座に対処することができます。このようなユーザーがどんな装置を使用できるか、セキュリティー・ポリシーの中で明記すべきです。

表 47. 早見表 : 「機密保護担当者の限界」システム値の詳細を示します。

iSeries ナビゲーター名	特定の装置への特権ユーザーの制限
文字ベースのインターフェース名	QLMTSECOFR
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。

表 47. 早見表 (続き) : 「機密保護担当者の限界」システム値の詳細を示します。

iSeries ナビゲーター名	**特定の装置への特権ユーザーの制限**
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**サインオン・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**一般**」ページに、特権ユーザー制限のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、WRKSYSVAL QLMTSECOFR と入力します。
変更内容が有効になる時点	即時
デフォルト値	選択解除
推奨値	サインオンを常時表示
ロック可能	可
特別な考慮事項	「機密保護担当者の限界」システム値が機能するためには、システム・セキュリティー・レベルが 30 以上でなければなりません。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

リモート・サインオン制御:

「リモート・サインオン制御」システム値は、ユーザーが別のサーバーからのパススルーまたは Telnet セッションを要求した場合に、システムがユーザーのサインオンを要求するかどうかを決定します。

リモート・サインオン制御システム値の概要については、早見表を参照してください。

表 48. リモート・サインオン制御システム値に指定できる値

iSeries ナビゲーター	**文字ベースのインターフェース**	**説明**
サインオンを常時表示	*FRCSIGNON	リモート・サインオン要求は、通常のサインオン手順に従う必要があります。

表 48. リモート・サインオン制御システム値に指定できる値 (続き)

iSeries ナビゲーター	文字ベースのインターフェース	説明
ソースおよびターゲット・ユーザー ID の一致	*SAMEPRF	ソースおよびターゲット・ユーザー・プロファイル名が同一であるとき、自動サインオンが要求されている場合はサインオン画面をバイパスすることができます。ターゲット・パススルー・プログラムが使用される前にパスワード確認が行われます。自動サインオンの試行時に無効なパスワードが送信されると、パススルー・セッションは必ず終了し、エラー・メッセージがユーザーに送信されます。ただしプロファイル名が異なる場合、この値は、ユーザーがリモート・ユーザー・プロファイルの有効なパスワードを入力しても、セッションがセキュリティー障害で終わることを示します。
ターゲット・システムでユーザー ID を検査	*VERIFY	この値を使用すると、有効なセキュリティー情報が自動サインオン要求によって送信される場合に、ターゲット・システムのサインオン画面をバイパスすることができます。指定されたターゲット・ユーザー・プロファイルのパスワードが無効の場合は、パススルー・セッションはセキュリティー障害のために終了します。
リモート・サインオンを拒否	*REJECT	リモート・サインオンは許可されません。 TELNET アクセスの場合、この値を指定するとどんな処置も行われません。
ユーザー作成の出口プログラムを呼び出す	*プログラム名ライブラリー名*	指定されたプログラムが、すべてのパススルー・セッションの開始時と終了時に実行されます。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーに関連して、このセキュリティー値の設定を決める前に、ユーザーやシステムが資源へのアクセスを要求する方法を知っておく必要があります。たとえば、従業員が iSeries Access for Windows を使用する場合、通常のサインオン手順を要求するか、ソース/ターゲット・システム両方のサインオンを強制的に同じにするようこのシステム値を設定することをお勧めします。iSeries Access を使用しないユーザーに対しては、リモート・サインオンを拒否することができます。

表 49. 早見表 : リモート・サインオン制御システム値の詳細を示します。

iSeries ナビゲーター名	リモート・サインオン
文字ベースのインターフェース名	QRMTSIGN

表 49. 早見表 (続き): リモート・サインオン制御システム値の詳細を示します。

iSeries ナビゲーター名	**リモート・サインオン**
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**サインオン・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**リモート**」ページに、リモート・サインオン制御のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、WRKSYSVAL QRMTSIGN と入力します。
変更内容が有効になる時点	即時
デフォルト値	選択解除
推奨値	選択
ロック可能	可
特別な考慮事項	パススルーまたは iSeries Access へのアクセスを許可したくない場合は、すべてのリモート・サインオンを拒否するようにこの値を設定してください。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

パスワードのシステム値

サインオン・システム値の設定に加えて、ユーザー・パスワードの規則を決定する必要もあります

パスワード・システム値を使用すれば、全般的なセキュリティー環境に適合するようパスワード規則をカスタマイズできます。通常、これらの値は、セキュリティー・ポリシーに文書化された基本的なパスワード要件をサポートします。それぞれのシステム値については、以下の情報を参照してください。

パスワード規則の設定:

以下のステップに従って、ご使用のシステム・サインオンを保護します。

まず以下の事柄を行う必要があります。

- パスワードが単純なものではいけない、またパスワードを共用してはいけないということを表明する方針を設定します。
- その実施に役立てるために、システム値を設定します。表 1 に、推奨システム値の設定を示します。

表の値の組み合わせはかなり制限されたもので、単純なパスワードが作成される可能性を大幅に減らすことを目的としています。しかし、ユーザーは、これらの制限を満たすパスワードの選択が難しく不満を感じる可能性があります。

ユーザーには以下のものを提供することを考えてください。

1. パスワードの基準のリスト
2. 有効パスワードと無効パスワードの例
3. 正しいパスワードの考え方の提案

これらのシステム値の現行設定を印刷するには、 システム機密保護属性印刷 (PRTSYSSECA) コマンドを使用します。

表 50. パスワード用のシステム値

システム値の名前	説明	推奨値
QPWDEXPITV	システム・ユーザーがパスワードを変更しなければならない頻度。ユーザー・プロファイルでは個々のユーザー用に異なる値を指定することができます。	60 (日)
QPWDLMTAJC	システムが同じ文字の連続使用を妨げるかどうか。	1 (はい)
QPWDLMTCHR	パスワードで使用できない文字。	AEIOU#$@
QPWDLMTREP	パスワードに同じ文字が 2 度以上使用されることをシステムが妨げるかどうか。	2 (連続使用は許可されない)
QPWDLVL	ユーザー・プロファイル・パスワードが 10 文字に制限されているか、それとも最大の 128 文字に制限されているか。	0[2]
QPWDMAXLEN	パスワードの文字の最大数。	8
QPWDMINLEN	パスワードの文字の最小数。	6
QPWDPOSDIF	パスワードのそれぞれの文字が、直前のパスワードの同一の位置の文字と違わなければならないか。	1 (はい)
QPWDRQDDGT	パスワードには少なくとも数字を 1 つ含めなければならないか。	1 (はい)
QPWDRQDDIF	ユーザーが再び同じパスワードを使用するまでに待たなければならない期間。	5 またはそれ以下 (満了間隔)[1]
QPWDVLDPGM	新しく割り当てたパスワードの妥当性を検査するために呼び出す出口プログラム。	*NONE

注:

1. QPWDEXPITV システム値は、ユーザーがパスワードを変更しなければならない頻度を指定します。たとえば、60 日ごとなどです。これは満了間隔です。QPWDRQDDIF システム値は、元のパスワードを再び使用できるようになるまでに、ユーザーがパスワードを変更しなければならない回数を指定します。
2. QPWDLMTCHR は、パスワード・レベルが 2 または 3 の場合には施行されません。

パスワードのレベル:

このシステム値は、すべてのユーザー・プロファイル・パスワードの仕様が同じ長さになるような特定のパスワード環境を設定します。

短いパスワード (1 文字から 10 文字)、または長いパスワード (1 文字から 128 文字) になるようにパスワード・レベルを設定できます。パスワード・レベルの設定によっては、パスワード値として「パスフレーズ」を使用できるようになります。「パスフレーズ」とは、非常に長い値を取ることができ、パスワード値として使用可能な文字の制約事項がほとんどないパスワード値です。文字間にブランクを含むパスフレーズを作成できます。こうすれば、1 つの文全体または文の一部をパスワード値として指定できます。パスフレーズの制約事項は、アスタリスク ('*') で開始できないこと、および末尾のブランクは削除されることだけです。

パスワード・レベル・システム値の概要については、早見表を参照してください。

表 51. パスワード・レベルのシステム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
限定文字セットを使用する短いパスワード。(0)	0	パスワード・レベル 0 は、1 から 10 文字の英数字および $、@、#、_ を使用するパスワードをサポートします。ネットワーク内の他のサーバーと通信するシステムの場合、それらのサーバーがパスワード・レベル 0 のパスワードを使用しているか、バージョン V5R1 より前のオペレーティング・システムを実行していれば、パスワード・レベル 0 を使用してください。
限定文字セットを使用する短いパスワード。Windows 95/98/ME クライアント用の NetServer™ パスワードを使用不可にします。(1)	1	パスワード・レベル 1 はパスワード・レベル 0 と同じ文字セットをサポートしますが、すべての NetServer[1] パスワードをシステムから除去するため、セキュリティーが向上します。iSeries NetServer が必要な場合は、パスワード・レベル 1 ではなく 0 または 2 を指定してください。
限定なしの文字セットを使用する長いパスワード。(2)	2	パスワード・レベル 2 は 1 文字から 128 文字までのパスワードをサポートし、大/小文字を区別します。iSeries NetServer と通信するシステムの場合、すべてのユーザー・パスワードが 1 文字から 14 文字までの長さであれば、パスワード・レベル 2 を使用できます。ただし、パスワード・レベル 0 または 1 のパスワードを使用する他のシステム、またはバージョン V5R1 より前のオペレーティング・システムを実行する他のシステムと通信する場合には、パスワード・レベル 2 を使用しないでください。

表 51. パスワード・レベルのシステム値に指定できる値 (続き)

iSeries ナビゲーター	文字ベースのインターフェース	説明
限定なしの文字セットを使用する長いパスワード。Windows 95/98/ME クライアント用の iSeries NetServer パスワードを使用不可にします。(3)	3	パスワード・レベル 3 は 1 文字から 128 文字までのパスワードをサポートし、大/小文字を区別します。システムが以下のものと通信する場合には、このレベルを使用できません。 • パスワード・レベル 0 または 1 を実行する、ネットワーク内の他のシステム • リリース V5R1M0 より前の OS/400® オペレーティング・システムを実行するシステム • パスワードの長さを 1 から 10 文字に制限している他のシステム • iSeries Support for Windows Network Neighborhood (iSeries NetServer) [1] 製品 • OS/400 V5R1 以前のバージョンの iSeries Access を使用するコンピューター

1. パスワード・レベルが 1 または 3 に設定されている場合、Windows 95/98/ME 用 NetServer 製品はシステムに接続できません。NetServer パスワードは弱い暗号化を使用するため、セキュリティー上の理由から、これらのパスワード・レベルを使用するシステムでは NetServer パスワードが除去されます。そのようなパスワードは簡単にデコードできます。

セキュリティー・ポリシーとの関係

これらのオプションは、実際のセキュリティー環境に基づく柔軟なパスワード・セキュリティーを可能にします。短いパスワードを使用する場合、パスワード文字列のつづりを間違えたり忘れたりする可能性が低いため、ユーザーによるパスワード管理が容易になります。ただし、特定のパスワード規則に基づく短いパスワードは、ハッカーによって推測される可能性があります。長く複雑なパスワードまたはパスフレーズを使用する場合、推測は難しくなりますが、ユーザーによるパスワード管理もまた難しくなる可能性があります。セキュリティー環境を厳しくしている場合には、長いパスワードを使用するのが適切かもしれませんが、ユーザーがパスワードを覚えるのに役立つような提案を提供してください。簡単に記憶できるような個人用のパスフレーズを作成することをユーザーに提案してください。

セキュリティー要件をそれほど厳しくしていない環境では、短いパスワードを可能にするパスワード・レベルを選択し、パスワードの管理に関する特定の規則を提供することができます。どのパスワード・レベルを選択する場合にも、ユーザーが独特のパスワード/パスフレーズを作成できるよう、有効なパスワード値の例および提案を提供してください。セキュリティー・ポリシーの提案に含まれるパスワードは単なる例にすぎず、実際のパスワード値として決して使用すべきでないことを強調してください。

表 52. 早見表 : パスワード・レベル・システム値の詳細を提供します。

iSeries ナビゲーター名	パスワード・レベル (次回の再始動時)
文字ベースのインターフェース名	QPWDLVL

表 52. 早見表 (続き) : パスワード・レベル・システム値の詳細を提供します。

iSeries ナビゲーター名	**パスワード・レベル (次回の再始動時)**
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**パスワード・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**一般**」ページに、パスワード・レベルのオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QPWDLVL` と入力します。
変更内容が有効になる時点	次回の再始動時
デフォルト値	限定文字セットを使用する短いパスワード (0)
推奨値	「特別な考慮事項」を参照
ロック可能	可
特別な考慮事項	**パスワード・レベルの変更** パスワード・レベル 3 を 0 または 1 に変更することはできません。パスワード・レベル 0 または 1 で使用されるすべてのパスワードはパスワード・レベル 3 への変更時にシステムから除去されるため、まずパスワード・レベル 3 から 2 に変更した後、1 または 0 に変更する必要があります。 パスワード・レベル 2 では、パスワード・レベル 0 または 1 に変更する前に、パスワード・レベル 0 または 1 で指定される文字長 (10 文字以下) に従うよう、すべてのユーザー・プロファイル・パスワードを変更する必要があります。そうしない場合、ユーザーはシステムにサインオンできなくなります。 このようにパスワードを変更した後、ユーザー・プロファイルのパスワードが変更後のパスワード・レベルに準拠するかどうか検証できます。詳しくは、パスワード・レベルに関するオンライン・ヘルプを参照してください。 詳細な考慮事項、およびパスワード・レベルの変更については、「機密保護解説書」のパスワード・レベル変更の計画に関するセクションを参照してください。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

計画、パスワード・レベルの変更:

パスワード・レベルの変更計画が 適切でないと、他のシステムとの操作が失敗したり、ユーザーがシステムにサインオンできなかったり する可能性があります。

パスワード・レベルの変更は、注意深く計画する必要があります。 QPWDLVL システム値を 変更する前に、必ず、SAVSECDTA または SAVSYS コマンドを使用して、セキュリティーを保管してください。現行のバックアップを保有していれば、下位のパスワード・レベルに戻す必要がある場合に、すべてのユーザーのプロファイルに対するパスワードをリセットできます。

システム、およびそのシステムとインターフェースするクライアント上で使用する製品は、パスワード・レベル (QPWDLVL) システム値が 2 または 3 に設定されている場合には、問題が発生することがあります。システムにパスワードを送信するすべての製品またはクライアントは、ユーザーがサインオン画面で入力する平文形式ではなく、暗号化された形式で、QPWDLVL が 2 または 3 用の新規パスワード暗号化規則を処理できるよう、アップグレードする必要があります。暗号化されたパスワードの送信は、パスワード置換と呼ばれています。

パスワード置換は、ネットワーク上に伝送中のパスワードが読み取られるのを防ぐために使用します。QPWDLVL 2 または 3 の新規アルゴリズムをサポートしていない古いクライアントによって生成されたパスワード置換は、特定の文字が正しい場合でも、受け入れられません。これは、暗号化された値を使用してあるシステムから別のシステムを認証する iSeries 間の対等アクセスにも当てはまります。

影響を受ける一部の製品、たとえば Java Toolbox などがミドルウェアとして使用されている場合には、問題が複雑になります。これらの製品の以前のバージョンを組み込んでいるサード・パーティー製品は、ミドルウェアの更新済みバージョンを使用して再作成しないと、正常に動作しません。この問題とその他のシナリオから、QPWDLVL システム値を変更する前には注意深い計画が必要だということを、容易に理解することができます。

QPWDLVL を 0 から 1 に変更する際の考慮事項:

パスワード・レベルを変更する前に、以下の項目を考慮に入れてください。

パスワード・レベル 1 では、Windows 95/98/ME または AS/400® Client Support for Windows Network Neighborhood (iSeries NetServer) 製品との通信を必要としないシステムは、iSeries NetServer パスワードをシステムから除去することができます。システムから不要な暗号化パスワードを除去すると、システム全体のセキュリティーが向上します。

QPWDLVL 1 では、現行の V5R1 より前のすべてのパスワード置換およびパスワード認証メカニズムは、引き続き作動します。 iSeries NetServer パスワードを必要とする機能またはサービスを除いて、破損する可能性はほとんどありません。

QPWDLVL を 0 または 1 から 2 に変更する際の考慮事項:

パスワード・レベル 2 では、長さが 128 文字までの大/小文字を区別するパスワード (パスフレーズともいう) を使用でき、QPWDLVL 0 または 1 に復帰するための最大限の能力が提供されます。

システムのパスワード・レベルとは無関係に、パスワード・レベル 2 および 3 のパスワードは、パスワード変更時またはユーザーによるシステムへのサインオン時に必ず作成されます。システムのパスワード・レベルがまだ 0 または 1 であるときに、レベル 2 および 3 のパスワードを作成しておくと、パスワード・レベル 2 または 3 への変更の準備として役立ちます。

QPWDLVL を 2 に変更する前に、DSPAUTUSR または PRTUSRPRF TYPE(*PWDINFO) コマンドを使用して、パスワード・レベル 2 で使用可能なパスワードを持っていないユーザー・プロファイルをすべて探

し出す必要があります。どんなプロファイルがコマンドによって検出されたかに応じて、以下のいずれかの方法に従ってパスワード・レベル 2 または 3 のパスワードをプロファイルに追加できます。

- CL コマンド CHGUSRPRF または CHGPWD、あるいは QSYCHGPW API を使用して、そのユーザー・プロファイルのパスワードを変更します。これによって、システムは、パスワード・レベル 0 および 1 で使用可能なパスワードを変更します。さらに、システムは、パスワード・レベル 2 および 3 で使用可能な 2 つの同じパスワードを大/小文字を区別して作成します。パスワード・レベル 2 または 3 で使用できるように、すべて大文字のパスワードとすべて小文字のパスワードが作成されます。

  たとえば、パスワードを C4D2RB4Y に変更すると、システムは C4D2RB4Y および c4d2rb4y というパスワード・レベル 2 のパスワードを生成します。
- パスワードを平文で表示するメカニズムでシステムにサインオンします (パスワード置換は使用しません)。パスワードが有効で、パスワード・レベル 2 および 3 で使用可能なパスワードがユーザー・プロファイルにない場合、システムはパスワード・レベル 2 および 3 で使用可能な 2 つの同じパスワードを大/小文字を区別して作成します。パスワード・レベル 2 または 3 で使用できるように、すべて大文字のパスワードとすべて小文字のパスワードが作成されます。

ユーザー・プロファイルにパスワード・レベル 0 および 1 で使用可能なパスワードがない場合、またはユーザーがパスワード置換を使用する製品を通じてサインオンしようとした場合、パスワード・レベル 2 または 3 で使用可能パスワードがないために問題が発生する可能性があります。このような場合、パスワード・レベルが 2 に変更されると、ユーザーはサインオンできません。

パスワード・レベル 2 および 3 で使用可能なパスワードがユーザー・プロファイルになく、パスワード・レベル 0 および 1 で使用可能なパスワードがユーザー・プロファイルにある場合、平文パスワードを送信する製品を通じてユーザーがサインオンすると、システムはパスワード・レベル 0 のパスワードと比較してユーザーを妥当性検査し、ユーザー・プロファイル用にパスワード・レベル 2 のパスワードを 2 つ (前述のように) 作成します。それ以降のサインオンでは、パスワード・レベル 2 のパスワードと比較して妥当性検査されます。

クライアントまたはサービスが新しいパスワード・パスフレーズ置換方式を使用できるようにアップデートされていない場合には、パスワード置換を使用するクライアントまたはサービスは、QPWDLVL 2 で正しく作動しません。管理者は、新しいパスワード置換方式にアップデートされていないクライアントまたはサービスが必要であるかどうかを調べる必要があります。

パスワード置換を使用するクライアントおよびサービスには、次のものがあります。

- TELNET
- iSeries Access
- iSeries ホスト・サーバー
- QFileSrv.400
- iSeries NetServer 印刷サポート
- DDM
- DRDA®
- SNA LU6.2

QPWDLVL 2 に変更する前に、セキュリティー・データを保管しておくことを強くお勧めします。セキュリティー・データのバックアップがあれば、QPWDLVL 0 または 1 に戻す必要がある場合、遷移が容易になります。

QPWDLVL 2 である程度のテストが完了するまで、QPWDMINLEN および QPWDMAXLEN などの他のパスワード・システム値を変更しないことをお勧めします。こうすれば、QPWDLVL 1 または 0 に戻す必要がある場合、遷移が容易になります。ただし、システムで QPWDLVL を 2 に変更できるようになる前に、QPWDVLDPGM システム値を *REGFAC または *NONE のいずれかに指定する必要があります。

したがって、パスワード妥当性検査プログラムを使用する場合には、ADDEXITPGM コマンドを使用することにより、QIBM_QSY_VLD_PASSWRD 出口点に登録可能な新規プログラムを作成できます。

iSeries NetServer パスワードは QPWDLVL 2 でもサポートされるので、iSeries NetServer パスワードを必要とする機能/サービスは引き続き正しく作動します。管理者がシステムを QPWDLVL 2 で稼働することに慣れてきたら、長いパスワードを活用するために、パスワード・システム値を変更し始めることができます。ただし管理者は、長いパスワードが以下のような影響を与えることを認識しておく必要があります。

- 10 文字より長いパスワードが指定されると、パスワード・レベル 0 および 1 のパスワードはクリアされます。このユーザー・プロファイルは、システムがパスワード・レベル 0 または 1 に戻っても、サインオンできなくなります。
- パスワードに特殊文字が含まれているか、単純オブジェクト名の構成規則に従っていない場合 (大/小文字の区別を除く)、パスワード・レベル 0 および 1 のパスワードはクリアされます。
- 14 文字を超えるパスワードが指定されると、ユーザー・プロファイルの iSeries NetServer パスワードはクリアされます。
- パスワード・システム値は、新しいパスワード・レベル 2 の値にだけ適用され、システムにより生成されたパスワード・レベル 0 および 1 のパスワード、または iSeries NetServer パスワード値 (生成された場合) には適用されません。

QPWDLVL を 2 から 3 に変更する際の考慮事項:

パスワード・レベルを変更する前に、以下の項目を考慮に入れてください。

ある期間、システムを QPWDLVL 2 で稼働した後、管理者は、パスワード・セキュリティー保護を最大化するために QPWDLVL 3 への移行を考慮することができます。

QPWDLVL 3 では、すべての iSeries NetServer パスワードがクリアされるので、 iSeries NetServer パスワードを使用する必要がなくなるまで、システムを QPWDLVL 3 に移行しないでください。

QPWDLVL 3 では、パスワード・レベル 0 および 1 のすべてのパスワードがクリアされます。管理者は DSPAUTUSR または PRTUSRPRF コマンドを使用して、パスワード・レベル 2 または 3 のパスワードが関連付けられていないユーザー・プロファイルを見つけることができます。

割り当て済みパスワードの変更:

ユーザーのシステムに存在している可能性のあるサーバーへの既知の入り口の一部をクローズするため、以下のことを行います。

以下の手順のステップの一部で、これらの表からの情報が必要となります。

表 53. IBM 提供プロファイル用のパスワード

ユーザー識別コード	パスワード	推奨値
QSECOFR	QSECOFR[1]	機密保護管理者だけが知っている単純ではない値。選択したパスワードを書き留め、安全な場所に保管します。
QSYSOPR	QSYSOPR	*NONE[2]

表 53. IBM 提供プロファイル用のパスワード (続き)

ユーザー識別コード	パスワード	推奨値
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2、 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

注:

1. システム出荷時は、 QSECOFR の「パスワードの満了設定」値が *YES に設定されています。新規システムに初めてサインオンしたときに、QSECOFR パスワードを変更しなければなりません。
2. システムはシステム機能のためにこれらのユーザー・プロファイルを必要としますが、ユーザーがこれらのプロファイルを使用してサインオンすることは許可しないでください。 V3R1 またはそれ以降のリリースで導入された新規システムの場合、このパスワードは *NONE として出荷されます。 CFGSYSSEC コマンドを実行すると、システムはこれらのパスワードを *NONE に設定します。
3. TCP/IP を使用して iSeries Access for Windows を実行するには、QUSER ユーザー・プロファイルを使用可能にしておかなければなりません。

表 54. 専用保守ツール用のパスワード

DST レベル 1	ユーザー ID[1]	パスワード	推奨値
基本機能	11111111	11111111	機密保護管理者だけが知っている単純ではない値。[2]
全機能	22222222	22222222[3]	機密保護管理者だけが知っている単純ではない値。[2]
セキュリティー機能	QSECOFR	QSECOFR[3]	機密保護管理者だけが知っている単純ではない値。[2]
サービス機能	QSRV	QSRV[3]	機密保護管理者だけが知っている単純ではない値。[2]

注:

1. ユーザー ID が必要なのは、 オペレーティング・システムの PowerPC® AS (RISC) リリースだけです。
2. サービス技術員がこのユーザー ID とパスワードを使用してサインオンする必要があった場合は、サービス技術員が離れた後で、パスワードを新規の値に変更してください。
3. 保守ツール・ユーザー・プロファイルは、最初に使用されるとすぐに有効期限が切れます。

1. いまだに (ユーザー・プロファイル名と同じ) デフォルト・パスワードを使用しているユーザー・プロファイルがないことを確認する。デフォルト・パスワード分析 (ANZDFTPWD) コマンドを使用することができます。
2. 「IBM 提供プロファイル用のパスワード」という表に示してあるユーザー・プロファイルとパスワードの組み合わせを使用して、システムへのサインオンを試行する。これらのパスワードは公開されているもので、システムに侵入しようとする誰もが最初に選択するものです。サインオンすることができたら、ユーザー・プロファイル変更 (CHGUSRPRF) コマンドを使用して、パスワードを推奨値に変更します。
3. 専用保守ツール (DST) を開始し、表 2 に示すパスワードを使用してサインオンを試行する。
4. これらのパスワードを使用して DST にサインオンできた場合は、パスワードを変更する必要がある。DST パスワードは、認証された装置によってのみ変更することができます。このことは、すべてのパスワードおよび対応する同一のユーザー ID にもあてはまります。認証された装置の詳細については、『オペレーション・コンソール』のセットアップ情報を参照してください。

5. 最後に、ユーザー ID とパスワードを入力しないと、「サインオン」画面で Enter キーを押しただけではサインオンできないことを確認する。各種ディスプレイで試行してみます。「サインオン」画面で情報を入力しなくてもサインオンできる場合には、以下のいずれかを行います。
   a. セキュリティー・レベルを 40 または 50 (QSECURITY システム値) に変更する。 セキュリティー・レベルを 40 または 50 に上げると、アプリケーションの実行動作が変化する場合があります。
   a. 対話式サブシステムに対するすべてのワークステーション項目が USER(*RQD) を指定したジョブ記述を示すように変更する。

デフォルト・パスワードの回避:

新規ユーザー・プロファイルを作成すると、 デフォルトでは、ユーザー・プロファイル名と同一のパスワードが作成されます。

デフォルト・パスワードにより、プロファイル名の割り当ての方針を知っている人物がユーザーの組織に新しい担当者が加わったことを知ると、その人物は、ユーザーのシステムに入り込む機会を得たことになります。

新規ユーザー・プロファイルを作成するときには、デフォルト・パスワードを使用するのではなく、単純ではない固有のパスワードを割り当てるように考えてください。新規ユーザーには、セキュリティー・ポリシーの要点を説明した“システムにようこそ”という題の手紙などの中で、内密にパスワードを知らせてください。ユーザー・プロファイルを PWDEXP(*YES) に設定することにより、初めてユーザーがサインオンするときに、ユーザーにパスワードを変更させる必要があります。

デフォルト・パスワード分析 (ANZDFTPWD) コマンドを使用すると、システムのすべてのユーザー・プロファイルを調べて、デフォルト・パスワードがないかどうかチェックすることができます。報告書を印刷するときには、パスワードがユーザー・プロファイル名と同一の場合に、システムが処置を行う (たとえば、ユーザー・プロファイルを使用不可にする) ことを指定するオプションがあります。ANZDFTPWD コマンドは、検出したプロファイルのリストと行った処置を印刷します。

注: パスワードは、片方向の暗号化形式でシステムに保管されます。パスワードの暗号化を解除することはできません。システムは、指定されたパスワードを暗号化して、ユーザーのサインオン時にパスワードをチェックするように、そのパスワードと保管済みのパスワードを比較します。権限障害 (*AUTFAIL) を監査している場合、システムは、デフォルト・パスワードを持っていないユーザー・プロファイルごとに、PW 監査ジャーナル項目を作成します (V4R1 またはそれより前のリリースで稼働しているシステムの場合)。V4R2 からは、システムは、ANZDFTPWD コマンドの実行時に PW 監査ジャーナル項目を作成しません。

下位パスワード・レベルへの変更:

下位パスワード・レベルに変更する前に、検討すべき考慮事項があります。

下位の QPWDLVL 値に戻ることは、可能ではありますが、全く問題が無いということはありません。一般的に、下位の QPWDLVL 値から上位の QPWDLVL 値への変更は一方通行であると考えるべきです。ただし、下位の QPWDLVL 値の復元が必要な場合があります。

以下のそれぞれの節では、下位のパスワード・レベルに戻すために必要な作業を解説します。

QPWDLVL を 3 から 2 に変更する際の考慮事項

この変更は比較的簡単です。 QPWDLVL を 2 に設定した場合、管理者は、ユーザー・プロファイルが iSeries NetServer パスワードまたはパスワード・レベル 0 あるいは 1 のパスワードを保有する必要があるかどうかを判断しなければなりません。必要がある場合には、ユーザー・プロファイルのパスワードを有効な値に変更してください。

さらに、iSeries NetServer パスワードおよびパスワード・レベル 0 または 1 のパスワードが必要な場合には、パスワード・システム値をこれらと互換性のある値に戻す必要があります。

QPWDLVL 3 を 1 または 0 に変更する際の考慮事項

システムに問題が発生する可能性が非常に高いため、パスワード・レベル 0 および 1 のパスワードがクリアされたために、誰もサインオンできなくなるなど)、この変更は直接にはサポートされていません。 QPWDLVL 3 から QPWDLVL 1 または 0 に変更するには、システムをまず一時的に QPWDLVL 2 に変更する必要があります。

QPWDLVL を 2 から 1 に変更する際の考慮事項

QPWDLVL を 1 に変更する前に、管理者は、DSPAUTUSR または PRTUSRPRF TYPE(*PWDINFO) コマンドを使用して、パスワード・レベル 0 または 1 のパスワードを持っていないユーザー・プロファイルを見付ける必要があります。QPWDLVL の変更後にユーザー・プロファイルがパスワードを必要とする場合には、管理者は、以下のメカニズムのうちのいずれかを使用して、そのユーザー・プロファイルにパスワード・レベル 0 および 1 のパスワードが作成されていることを確認します。

- CHGUSRPRF または CHGPWD CL コマンドか QSYCHGPW API を使用して、ユーザー・プロファイルのパスワードを変更する。これによってシステムは、パスワード・レベル 2 および 3 で使用可能なパスワードを変更します。さらにシステムは、パスワード・レベル 0 および 1 で使用可能な、等価の大文字のパスワードを作成します。システムは、以下の条件に適合する場合のみ、パスワード・レベル 0 または 1 のパスワードを作成することができます。
  - パスワードの長さは 10 文字以下。
  - パスワードは、大文字の EBCDIC 文字 A から Z、0 から 9、@、#、$、および下線に変換可能。
  - パスワードの最初の文字は、数字または下線文字ではない。

  たとえば、パスワードを RainyDay という値に変更すると、システムは、RAINYDAY という、 パスワード・レベル 0 および 1 のパスワードを生成します。しかし、パスワード値を Rainy Days In April に変更すると、システムは、パスワード・レベル 0 および 1 のパスワードをクリアします。パスワードが長すぎて、ブランクが含まれているためです。パスワード・レベル 0 または 1 のパスワードが作成されない場合、メッセージまたは指示は表示されません。
- パスワードを平文で表示するメカニズムでシステムにサインオンします (パスワード置換は使用しません)。パスワードが有効で、さらにユーザー・プロファイルがパスワード・レベル 0 および 1 で使用可能なパスワードを持っていない場合には、システムはパスワード・レベル 0 および 1 で使用可能な等価の大文字パスワードを作成します。システムは、上記条件に適合している場合のみ、パスワード・レベル 0 および 1 のパスワードを作成することができます。

この後、管理者は、QPWDLVL を 1 に変更することができます。QPWDLVL 1 への変更が有効になる (次の IPL) と、 iSeries NetServer パスワードはすべてクリアされます。

QPWDLVL 2 を 0 に変更する際の考慮事項

考慮事項は、変更が有効になっても iSeries NetServer パスワードが保存される点を除いて、QPWDLVL 2 を 1 に変更する場合と同じです。

QPWDLVL 1 を 0 に変更する際の考慮事項

QPWDLVL を 0 に変更した後に、管理者は、DSPAUTUSR または PRTUSRPRF コマンドを使用して、iSeries NetServer パスワードを持っていないユーザー・プロファイルを見つける必要があります。ユーザー・プロファイルが iSeries NetServer パスワードを必要とする場合には、ユーザー・プロファイルを変更するか、またはパスワードを平文で表す方式でサインオンして、作成することができます。これで管理者は、QPWDLVL を 0 に変更できます。

パスワードの満了間隔:

パスワード満了間隔システム値により、次にパスワードを変更するのが必要になるまでの許可日数が制御されます。

ユーザーがパスワード満了後にサインオンを試行すると、システムにより、サインオンの前にパスワードを変更する必要があることを示す画面が表示されます。この値をシステムのすべてのユーザー・プロファイルに全体的に設定したり、個々のユーザー・プロファイルごとにパスワード有効期限をカスタマイズできます。たとえば、機密保護担当者や全オブジェクト (*ALLOBJ) 特殊権限を持つ他のユーザーには、その他のユーザーよりも頻繁にパスワードを変更させたい場合もあります。

パスワード満了間隔システム値の概要については、『早見表』という表を参照してください。

表 55. パスワード満了間隔のシステム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
有効期限なし	*NOMAX	ユーザーにパスワード変更を求めない。
前回の変更後の日数 (1 から 366)	*日数による限界設定*	パスワードの有効期限が切れるまでの日数を指定します。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、パスワード関連のシステム値によって定義されているパスワード規則を説明すべきです。このシステム値では、システムで有効なパスワードの長さ、および有効期限を過ぎた場合に行うべき事柄についてユーザーが分かるようにします。別のいくつかのパスワード・システム値は、システムでパスワード期限切れになるたびに固有のパスワードを作成するよう求めます。また、セキュリティー・ポリシーでもこうした規則を文書化してください。

より厳重なセキュリティー環境においては、パスワード満了間隔が短い方が適切です。ユーザーには定期的にパスワードを変更させる必要があります。そのようにすることによって、ユーザーが他のシステム・ユーザーとパスワードを共有しにくくします。パスワードの満了間隔が長かったり無期限だったりすると、侵入者になり得る人物がシステムへのパスワードを盗んだり入手する場合、長い期間アクセスさせてしまうことになります。侵入者が有効なパスワードを入手した場合には、かなり長期間にわたりシステムの重要データに損害を与えたり盗んだりできます。満了間隔が短ければ、侵入者がお客様のシステムにアクセスする合計時間は限定されます。しかし、正当なユーザーにあまりにも頻繁にパスワードを変更するよう求めると苛立つ可能性もあります。保護とユーザーの必要とのバランスを取るには、30 日から 90 日の間の値を選択してください。ほとんどのインストールでは、この範囲が適切です。パスワード有効期限を、個々のユーザー

やシステムごとにカスタマイズする必要がある場合もあります。おそらく、機密保護管理者や全オブジェクト (*ALLOBJ) 権限を持つユーザーにはより頻繁にパスワードを変更してもらい、誰かにパスワードを盗まれる危険を最小限に抑えたい場合もあります。また、特定のシステムに含まれるデータによっては、そうしたシステムのパスワード満了間隔を短くしたり、長くしたりするかもしれません。

表 56. 早見表 : パスワード満了間隔のシステム値に関する詳細を提供します。

iSeries ナビゲーター名	**有効期限**
文字ベースのインターフェース名	QPWDEXPITV
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**パスワード・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**有効期限**」ページで、パスワード有効期限のオプションを見つけます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QPWDEXPITV` と入力します。
変更内容が有効になる時点	即時
デフォルト値	有効期限なし
推奨値	30 日から 90 日まで
ロック可能	可
特別な考慮事項	なし

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

パスワードの最小文字数:

このシステム値により、パスワード文字の最小数が制御されます。

可能な値は、システムのパスワード・レベルに応じて異なります。パスワード・レベルが 0 または 1 の場合、最小文字数として可能な値は 1 から 10 です。パスワード・レベルが 2 または 3 の場合、最小文字数として可能な値は 1 から 128 です。

「パスワードの最小文字数」システム値の概要については、早見表を参照してください。

表 57. 「パスワードの最小文字数」システム値に指定できる値

iSeries ナビゲーター	**文字ベースのインターフェース**	**説明**
最小文字数	*最小の文字数*	パスワードの最小文字数を指定する。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、パスワード関連のシステム値によって定義されているパスワード規則を説明すべきです。このシステム値に関しては、有効なパスワードの最小文字数をユーザーに知らせてください。このシステム値は、パスワードの最大文字数を指定するシステム値とともに機能して、パスワードの長さの範囲を作成します。有効なパスワードはこの範囲内の長さでなければなりません。なお、パスワードの長さはシステムによって異なります。パスワード・レベルをシステム・ユーザーに開示するのは不適切かもしれませんが、パスワード・レベルによって許容されるパスワード長を明記することは適切です。たとえば、パスワード・レベルを 3 に設定した場合、パスワードの文字数が 1 から 128 文字の範囲でなければならないことをユーザーに知らせる必要があるでしょう。

表 58. 早見表 : 「パスワードの最小文字数」システム値についての詳細を示します。

iSeries ナビゲーター名	**最小文字数**
文字ベースのインターフェース名	QPWDMINLEN
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**パスワード・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**妥当性検査**」ページに、パスワード長のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QPWDMINLEN` と入力します。
変更内容が有効になる時点	即時
デフォルト値	6
推奨値	この値は、選択されたパスワード・レベルに依存します。
ロック可能	可
特別な考慮事項	なし

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

パスワードの最大文字数:

このシステム値により、パスワード文字の最大数が制御されます。

パスワードの最大文字数を制限すると、長すぎて容易に思い出せずどこかに記録しておかなければならないようなパスワードをユーザーが指定するのを防止し、セキュリティーを強化できます。通信ネットワークによっては、8 文字以下のパスワードが必須になっている場合があります。パスワードがネットワークの要件を満たしていることを確認するために、このシステム値を使用できます。

「パスワードの最大文字数」システム値の概要については、早見表を参照してください。

表 59. 「パスワードの最大文字数」システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
最大文字数	最大文字数	パスワードの最大文字数を指定する。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、パスワード関連のシステム値によって定義されているパスワード規則を説明すべきです。このシステム値に関しては、有効なパスワードの最大文字数をユーザーに知らせてください。このシステム値は、パスワードの最小文字数を指定するシステム値とともに機能して、パスワードの長さの範囲を決定します。有効なパスワードはこの範囲内の長さでなければなりません。なお、パスワードの長さはパスワード・レベルを指定するシステム値に依存します。パスワード・レベルをシステム・ユーザーに開示するのは不適切かもしれませんが、パスワード・レベルによって許容されるパスワード長を明記することは適切です。たとえば、パスワード・レベルを 3 に設定した場合、パスワードの文字数が 1 から 128 文字の範囲でなければならないことをユーザーに知らせる必要があるでしょう。

表 60. 早見表 : 「パスワードの最大文字数」システム値についての詳細を示します。

iSeries ナビゲーター名	最大文字数
文字ベースのインターフェース名	QPWDMAXLEN
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**パスワード・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**妥当性検査**」ページに、パスワード長のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QPWDMAXLEN` と入力します。
変更内容が有効になる時点	即時
デフォルト値	6
推奨値	この値は、選択されたパスワード・レベルに依存します。
ロック可能	可
特別な考慮事項	なし

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

パスワード重複の制限:

このシステム値は、パスワードを以前のパスワードと異なるものにしなければならないかどうかを制御します。

このシステム値は、パスワードを以前のパスワードと異なるものにしなければならないかどうかを制御します。この値は、重複しているかどうかの検査対象となる、以前のパスワードの数を設定します。この値を使用すると、ユーザーが以前に使用したパスワードを指定するのを防止することにより、セキュリティーを強化できます。また、この値により、パスワードが満了したユーザーがそれを変更した後、ただちに旧パスワードに戻してしまうことも防止できます。

「パスワード重複の制限」システム値の概要については、早見表を参照してください。

表 61. 「パスワード重複の制限」システム値に指定できる値

iSeries ナビゲーター	**文字ベースのインターフェース**	**説明**
パスワード再使用サイクル	*検査されるパスワード値の数*	重複しているかどうかの検査対象となるパスワードの数を指定する。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、パスワード関連のシステム値によって定義されているパスワード規則を説明すべきです。このシステム値に関しては、この値を超えるまでパスワードを再利用できないことをユーザーに知らせてください。パスワードを再利用すれば、ユーザーは 3 つか 4 つのお気に入りのパスワードの中から選択できますが、システム・セキュリティー上の危険となり得ます。この危険を最小限に抑えるには、このシステム値をパスワード満了システム値とともに使用することにより、同じパスワードが最低 6 カ月は再使用されないようにしてください。たとえば、パスワード満期期間を 30 日、パスワード再使用サイクルを 10 パスワードに選択した場合、システムから警告を受けた時にパスワードを変更する一般のユーザーは、同じパスワードを約 9 カ月間は再使用しません。

表 62. 早見表 : パスワード重複制限システム値の詳細を示します。

iSeries ナビゲーター名	**パスワード再使用サイクル**
文字ベースのインターフェース名	QPWDRQDDIF
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**パスワード・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**妥当性検査**」ページに、パスワード再使用のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QPWDRQDDIF` と入力します。
変更内容が有効になる時点	即時
デフォルト値	1 つのパスワードの後
推奨値	10 個のパスワードの後
ロック可能	可

表 62. 早見表 (続き) : パスワード重複制限システム値の詳細を示します。

iSeries ナビゲーター名	パスワード再使用サイクル
特別な考慮事項	パスワードを繰り返し使用することを防ぐには、10 以上の値を選択してください。パスワードが最低 6 カ月は再使用されないようにするために、「パスワード満了」値と「パスワード再使用サイクル」値を組み合わせて使用することをお勧めします。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

パスワードで制限される文字:

このシステム値により、パスワードで特定の文字を使用することが制限されます。

指定できる文字は、A から Z、0 から 9、およびシャープ (#)、ドル ($)、@ 記号、下線 (_) の特殊文字です。この値を使用すると、ユーザーがパスワードで母音など特定の文字を使用することを防止して、セキュリティーを強化することができます。母音の使用を制限すれば、ユーザーが実際の単語を使ってパスワードを構成することを防ぎます。

「パスワードの文字制限」システム値の概要については、早見表を参照してください。

表 63. 「パスワードの文字制限」システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
なし	*NONE	パスワードでの使用を制限されている文字はなし。
制限される文字	*制限文字*	制限されている文字を最大 10 文字まで指定。 指定できる文字は、A から Z、0 から 9、およびシャープ (#)、ドル ($)、@ 記号、下線 (_) の特殊文字です。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、パスワード関連のシステム値によって定義されているパスワード規則を説明すべきです。このシステム値に関しては、制限される文字をユーザーに知らせてください。このシステム値は、個々のパスワードの構成を指定する他のシステム値とともに機能します。

表 64. 早見表 : 「パスワードで制限される文字」システム値の詳細を示します。

iSeries ナビゲーター名	制限される文字
文字ベースのインターフェース名	QPWDLMTCHR
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。

表 64. 早見表 (続き) : 「パスワードで制限される文字」システム値の詳細を示します。

iSeries ナビゲーター名	**制限される文字**
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**パスワード・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**妥当性検査**」ページに、制限される文字のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、WRKSYSVAL QPWDLMTCHR と入力します。
変更内容が有効になる時点	即時
デフォルト値	なし
推奨値	A、E、I、O、および U。他のシステムとの互換性を保つために、 特殊文字 (#、¥、および @) を制限することもできます。
ロック可能	可
特別な考慮事項	このシステム値は、パスワード・レベル 0 または 1 のときに限って使用できます。パスワード・レベルが 2 または 3 の場合、この値を変更すると、システムは文字制限の設定を無視します。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

パスワード中の連続桁の制限:

このシステム値は、複数の数字を互いに隣接させてパスワードとして使用することを制限します。

この値を使用すると、ユーザーが、誕生日、電話番号、または連続する数字をパスワードとして使用することを防止して、セキュリティーを強化することができます。

「パスワード中の連続桁の制限」システム値の概要については、以下の表を参照してください。

表 65. 「パスワード中の連続桁の制限」システム値に指定できる値

iSeries ナビゲーター	**文字ベースのインターフェース**	**説明**
選択解除	0 (はい)	複数の数字を互いに隣接させてパスワードに使用できる。
選択	1 (いいえ)	複数の数字を互いに隣接させてパスワードに使用できない。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、パスワード関連のシステム値によって定義されているパスワード規則を説明すべきです。このシステム値に関しては、互いに隣接する複数の数字をパスワードに含めてよいかどうか、ユーザーに知らせてください。この値は、同一文字を何回か繰り返すなど、容易に推測できるパスワー

ドをユーザーが指定するのを防ぎ、セキュリティーを強化します。このシステム値は、個々のパスワードの構成を指定する他のシステム値とともに機能します。

表 66. 早見表 : 「パスワード中の連続桁の制限」システム値の詳細を示します。

iSeries ナビゲーター名	**連続する数字の制限**
文字ベースのインターフェース名	QPWDLMTAJC
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**パスワード・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**妥当性検査**」ページに、連続数字の制限のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QPWDLMTAJC` と入力します。
変更内容が有効になる時点	即時
デフォルト値	選択解除
推奨値	選択
ロック可能	可
特別な考慮事項	なし

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

パスワード中の反復文字の制限:

このシステム値により、パスワードで文字の繰り返しを使用することが制限されます。

この値は、同一文字を何回か繰り返すなど、容易に推測できるパスワードをユーザーが指定するのを防ぎ、セキュリティーを強化します。パスワード・レベルが 2 または 3 の場合には、反復文字の検査で大/小文字が区別されます。これは、小文字の「a」は大文字の「A」とは同じではないということです。

「**パスワード中の反復文字の制限**」システム値の概要については、早見表を参照してください。

表 67. 「パスワード中の反復文字の制限」システム値に指定できる値

iSeries ナビゲーター	**文字ベースのインターフェース**	**説明**
文字は複数回使用できます	0	パスワードに同じ文字を 2 回以上使用してもよい。
文字は複数回使用できません	1	パスワードに同じ文字を 2 回以上使用できない。
文字は連続して使用できません	2	パスワードに同じ文字を連続して使用できない。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、パスワード関連のシステム値によって定義されているすべてのパスワード規則を説明すべきです。このシステム値に関しては、パスワード規則で反復文字が許可されているかどうかをユーザーに知らせてください。この値は、同一文字を何回か繰り返すなど、容易に推測できるパスワードをユーザーが指定するのを防ぎ、セキュリティーを強化します。このシステム値は、個々のパスワードの構成を指定する他のシステム値とともに機能します。

表 68. 早見表 : 「**パスワード中の反復文字の制限**」システム値の詳細を示します。

iSeries ナビゲーター名	**反復文字の制限**
文字ベースのインターフェース名	QPWDLMTREP
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**パスワード・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**妥当性検査**」ページに、反復文字の制限のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QPWDLMTREP` と入力します。
変更内容が有効になる時点	即時
デフォルト値	文字は複数回使用できます
推奨値	文字は連続して使用できません
ロック可能	可
特別な考慮事項	パスワード・レベル・システム値が 2 または 3 の場合には、反復文字の検査で大/小文字が区別されます。これは、小文字の「a」は大文字の「A」とは同じではないということです。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

パスワードの各桁に異なる文字が必要:

このシステム値は、新規パスワードの各文字の位置を制御します。

新規パスワードの各文字の位置を制御すると、ユーザーが前のパスワードの対応する位置に同じ文字 (英字または数字) を使用することを防止して、セキュリティーを強化できます。パスワード・レベルが 2 または 3 の場合には、同一文字の検査で大/小文字が区別されます。これは、小文字の「a」は大文字の「A」とは同じではないということです。

「各桁に異なる文字が必要」システム値の概要については、早見表を参照してください。

表 69. 「パスワードの各桁に異なる文字が必要」に使用できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
選択解除	0	前のパスワードの対応する位置に同じ文字を使用できる。
選択	1	パスワードに同じ文字を 2 回以上使用できない。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、パスワード関連のシステム値によって定義されているパスワード規則を説明すべきです。このシステム値に関しては、前のパスワードと同じ位置に同じ文字を再び使用できるかどうかユーザーに知らせてください。このシステム値は、個々のパスワードの構成を指定する他のシステム値とともに機能します。

表 70. 早見表 : 「各桁に異なる文字が必要」の詳細を示します。

iSeries ナビゲーター名	各桁に新規の文字が必要
文字ベースのインターフェース名	QPWDPOSDIF
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**パスワード・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**妥当性検査**」ページに、「各桁に新規の文字が必要」のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QPWDPOSDIF` と入力します。
変更内容が有効になる時点	即時
デフォルト値	選択解除
推奨値	選択
ロック可能	可
特別な考慮事項	パスワード・レベルが 2 または 3 の場合には、反復文字の検査で大/小文字が区別されます。つまり、小文字と大文字は同じと見なされません。

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

パスワードに数字が必要:

このシステム値は、新規パスワードで数字が必要かどうかを決定します。

この値を使用すると、ユーザーがパスワードに英字だけを使用することを防止して、セキュリティーを強化することができます。

「各桁に異なる文字が必要」システム値の概要については、早見表を参照してください。

表 71. 「パスワードに数字が必要」システム値に指定できる値

iSeries ナビゲーター	文字ベースのインターフェース	説明
選択解除	0	新しいパスワードで数字を使用する必要はない。
選択	1	新しいパスワードで 1 文字以上の数字を使用する必要がある。

セキュリティー・ポリシーとの関係

セキュリティー・ポリシーの中で、パスワード関連のシステム値によって定義されているパスワード規則を説明すべきです。このシステム値に関しては、新しいパスワードで 1 文字以上の数字を使用する必要があるかどうか、ユーザーに知らせてください。この値は、個々のパスワードの構成を指定する他のシステム値とともに機能します。

表 72. 早見表 : 「パスワードに数字が必要」システム値の詳細を示します。

iSeries ナビゲーター名	最低 1 桁の数字が必要
文字ベースのインターフェース名	QPWDRQDDGT
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター** 1. 「**セキュリティー**」 → 「**ポリシー**」と展開します。 2. 「**パスワード・ポリシー**」を右クリックして、「**プロパティー**」を選択します。 3. 「**妥当性検査**」ページに、「新規パスワードに数字が必要」のオプションが表示されます。 **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、`WRKSYSVAL QPWDRQDDGT` と入力します。
変更内容が有効になる時点	即時
デフォルト値	選択解除
推奨値	選択
ロック可能	可
特別な考慮事項	なし

このセキュリティー値についての詳細情報は、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

パスワード情報の保管:

いくつかのネットワーク機能と通信要件をサポートするために、iSeries サーバーは、暗号化解除可能なパスワードを保管するための安全な方法を提供します。たとえば、別のシステムとの SLIP 接続を確立するために、システムはこれらのパスワードを使用します。

システムは、どんなユーザー・プログラムやインターフェースからもアクセスできない安全な領域にこれらの特別なパスワードを保管します。明示的に許可されたシステム機能だけが、これらのパスワードの設定と取り出しを行うことができます。

たとえば、ダイヤルアウト SLIP 接続用の保管パスワードを使用するときには、構成プロファイルを作成するシステム・コマンド (WRKTCPPTP) を使用してパスワードを設定します。このコマンドを使用するには、*IOSYSCFG が必要です。特別にコーディングされた接続スクリプトが、ダイヤルアウト手順の際にパスワードを取り出してそのパスワードの暗号化を解除します。暗号化解除されたパスワードはユーザーから見えず、ジョブ・ログにも表示されません。

機密保護管理者は、暗号化解除可能なパスワードをシステムに保管できるようにするかどうか決定する必要があります。これを指定するには、サーバー・セキュリティー・データの保持 (QRETSVRSEC) システム値を使用します。デフォルト値は 0 (なし) です。したがって、明示的にこのシステム値を設定しない限り、システムは暗号化解除可能なパスワードを保管しません。

保管されるパスワードについてのネットワーク要件または通信要件がある場合、適切なポリシーを設定し、通信相手側のポリシーや慣習を理解してください。たとえば、別の iSeries サーバーとの通信に SLIP を使用する場合には、両方のシステムで、セッションを確立するための特別なユーザー・プロファイルのセットアップを考慮する必要があります。特別なプロファイルには、システムに対する制限された権限を与えてください。これにより、保管パスワードがパートナー・システムで危険にさらされた場合に、こちら側のシステムへの影響が抑制されます。

パスワード妥当性検査プログラム:

このシステム値は、パスワードに対する追加の妥当性検査を行うユーザー作成プログラムの使用を可能にします。

現行および新しいパスワードは、暗号化されないまま妥当性検査プログラムに渡されます。妥当性検査プログラムは、パスワードをデータベース・ファイルに保管する可能性があるので、システムのセキュリティーが危険にさらされることになります。

「各桁のパスワード妥当性検査プログラム」システム値の概要については、以下の表を参照してください。

表 73. 「パスワード妥当性検査プログラム」システム値に指定できる値

文字ベースのインターフェース	説明
*NONE	妥当性検査プログラムは実行されない。
*REGFAC	妥当性検査プログラム名が登録機構内で検索される。
プログラム指定	ユーザー作成の妥当性検査プログラムの名前を 1 文字から 10 文字で指定。パスワード・レベル・システム値の現行値または保留値が 2 または 3 の場合には、プログラム名を指定できません。
ライブラリー名	ユーザー作成プログラムが入っているライブラリーの名前を指定。ライブラリー名が指定されない場合は、システム値を変更するユーザーのライブラリー・リストを使用して、プログラムが探索されます。推奨ライブラリーは QSYS です。
注: このシステム値に関しては、iSeries ナビゲーターに同等の機能はありません。	

セキュリティー・ポリシーとの関係

パスワード妥当性検査プログラムは、システムに受け入れられる有効なパスワードをユーザーが作成しているかどうか検査します。ただし、新旧パスワードが妥当性検査プログラムに送られるときに暗号化されないため、システムにとってセキュリティー上の危険が生じます。妥当性検査プログラムがパスワードをデータベース・ファイルに保管する場合には、侵入者がそれにアクセスしてシステム・セキュリティーを損なう可能性があります。したがって、企業にとってパスワード妥当性検査が必要と判断した場合には、設計するすべてのプログラムを機密保護担当者に検査してもらい、そのようなプログラム、および使用される保管ファイルへのアクセスを限定してください。

表 74. 早見表 : パスワード妥当性検査プログラム・システム値についての詳細を示します。

文字ベースのインターフェース名	**QPWDVLDPGM**
権限	全オブジェクト・アクセス (*ALLOBJ) 機密保護管理者 (*SECADM) **注:** これらの権限は機密保護担当者 (QSECOFR) ユーザー・プロファイルに付属しています。
アクセス方法	**iSeries ナビゲーター**: なし **文字ベースのインターフェース** 1. 文字ベースのインターフェースで、WRKSYSVAL QPWDVLDPGM と入力します。
変更内容が有効になる時点	パスワードが次に変更されるとき
デフォルト値	*NONE
推奨値	*NONE
ロック可能	可
特別な考慮事項	パスワード妥当性検査プログラムは、システムの補助記憶域プール (ASP) または基本ユーザーの ASP 内に保管する必要があります。

詳しくは、「機密保護解説書」第 3 章『セキュリティー・システム値』の、パスワード妥当性検査プログラムの使用に関するセクションを参照してください。

関連情報

ディスク・プールのタイプ

システム値の監査

このトピックでは、システム値の監査の詳細について説明します。

システム値を指定し、システム上のセキュリティー監査を制御することができます。

QAUDCTL
監査制御

QAUDENDACN
監査終了処置

QAUDFRCLVL
監査強制実行レベル

QAUDLVL
監査レベル

QAUDLVL2
監査レベル拡張

QCRTOBJAUD
デフォルトの監査の作成

セキュリティー・システム値を印刷するには、WRKSYSVAL *SEC OUTPUT(*PRINT) とタイプします。

関連概念

22 ページの『セキュリティー監査』
このトピックでは、セキュリティー監査の目的について取り上げます。

関連情報

システム値ファインダー

監査制御:

QAUDCTL システム値を使用すれば、監査を行うかどうかを制御できます。

- 文字ベースのインターフェースでの名前: **QAUDCTL**
- iSeries ナビゲーターでの名前: **「アクション監査を活動化」**、**「オブジェクト監査活動化」**、および **「QTEMP 内のオブジェクトを監査しない」**。
- **説明:** QAUDCTL システム値を使用すれば、監査を行うかどうかを制御できます。これは次の項目に対し、オン/オフのスイッチのように機能します。
  - QAUDLVL および QAUDLVL2 システム値
  - オブジェクト監査の変更 (CHGOBJAUD) コマンドと DLO 監査変更 (CHGDLOAUD) コマンドを使ってオブジェクトに定義した監査
  - ユーザー監査変更 (CHGUSRAUD) コマンドを使用して、ユーザーに定義した監査

  *NONE を指定しない限り、QAUDCTL システム値に対して複数の値を指定することができます。
- **推奨値:** QAUDLVL システム値に指定されたイベントをログに記録する (*AUDLVL)、オブジェクト監査が定義されたオブジェクトに関するアクティビティーをログに記録する (*OBJAUD)、QTEMP 内のオブジェクトを監査しない (*NOQTEMP)
-

表 75. 使用できる値

QAUDCTL システム値の使用	
***NONE**	ユーザー処置の監査およびオブジェクトの監査を実行しない。
***OBJAUD**	CHGOBJAUD、CHGDLOAUD、または CHGAUD コマンドを使って選択したオブジェクトに対する監査を実行する。
***AUDLVL**	QAUDLVL と QAUDLVL2 システム値、および個々のユーザー・プロファイルの AUDLVL パラメーターで選択された、任意の機能に対して監査を実行する。ユーザーに対する監査のレベルは、ユーザー監査変更 (CHGUSRAUD) コマンドを使用して変更する。
***NOQTEMP**	オブジェクトが QTEMP ライブラリー内にある場合、ほとんどの処置に対して監査は行われない。*OBJAUD または *AUDLVL では、この値を指定しなければならない。

注: このシステム値は制限付きの値です。セキュリティー・システム値の変更を制限する方法、および制限付きシステム値のリストについては、*「iSeries 機密保護解説書」*の第 3 章『セキュリティー・システム値』を参照してください。

監査レベル:

QAUDLVL システム値を使用すれば、すべてのシステム・ユーザーに関するセキュリティー監査ジャーナル (QAUDJRN) にどんなセキュリティー関連イベントをログとして記録するかを制御できます。

- 文字ベースのインターフェースでの名前: **QAUDLVL**
- iSeries ナビゲーター・インターフェースでの名前: 「**アクション監査を活動化**」
- **説明:** QAUDLVL システム値を使用すれば、すべてのシステム・ユーザーに関するセキュリティー監査ジャーナル (QAUDJRN) にどんなセキュリティー関連イベントをログとして記録するかを制御できます。このシステム値は、QAUDCTL システム値によって制御されます。QAUDLVL システム値が有効になるためには、QAUDCTL システム値に *AUDLVL が含まれている必要があります。*NONE を指定しない限り、QAUDLVL システム値に複数の値を指定できます。
- **推奨値:** 以下の情報をログとしてシステムに記録するのが推奨値です。
  - *AUTFAIL
    - すべてのアクセス失敗 (サインオン、権限、ジョブの実行)
    - 装置から入力された不正なパスワードまたはユーザー ID
  - *PGMFAIL
    - ブロックされた命令
    - 妥当性検査値の障害
    - ドメイン違反
  - *JOBDTA
    - ジョブ開始/停止データ
    - 保留、解放、停止、続行、変更、切断、終了、異常終了、PSR 接続の事前開始ジョブ項目

表 76. QAUDLVL システム値に指定できる値

監査値	説明
*NONE	QAUDLVL または QAUDLVL2 システム値によって制御される事象はログに記録されない。事象はユーザー・プロファイルの AUDLVL 値に基づいて個々のユーザーを対象にログに記録されます。
*ATNEVT	条件のセキュリティー上の重要度を判別するために、さらに評価されなければならない条件を監査する。
*AUDLVL2	QAUDLVL および QAUDLVL2 システム値を使用して、監査対象のセキュリティー処置を決定する。
*AUTFAIL	権限障害の事象がログに記録される。
*CREATE	オブジェクト作成操作がログに記録される。
*DELETE	オブジェクト削除操作がログに記録される。
*JOBDTA	ジョブに影響する処置がログに記録される。
*NETBAS	ネットワーク・ベース機能が監査される。
*NETCLU	クラスターおよびクラスター資源グループ操作が監査される。
*NETCMN	ネットワークおよび通信機能が監査される。 *NETCMN は、監査を適切にカスタマイズするための、いくつかの値で構成されています。 *NETBAS *NETCLU *NETFAIL *NETSCK
*NETFAIL	ネットワーク障害が監査される。

表 76. QAUDLVL システム値に指定できる値 (続き)

監査値	説明
*NETSCK	ソケット・タスクが監査される。
*OBJMGT	オブジェクトの移動および名前変更操作がログに記録される。
*OFCSRV	システム配布ディレクトリーおよびオフィス・メール処置に加えられた変更がログに記録される。
*OPTICAL	光ディスク・ボリュームの使用がログに記録される。
*PGMADP	権限を借用するプログラムからの権限の取得がログに記録される。
*PGMFAIL	システム保全性違反がログに記録される。
*PRTDTA	スプール・ファイルの印刷、出力の印刷装置への直接送信、および出力のリモート印刷装置への送信がログに記録される。
*SAVRST	復元操作がログに記録される。
*SECCFG	セキュリティー構成が監査される。
*SECDIRSRV	ディレクトリー・サービス機能を実行するときの変更または更新が監査される。
*SECIPC	プロセス間通信に対する変更が監査される。
*SECNAS	ネットワーク認証サービス処置が監査される。
*SECRUN	セキュリティー実行時機能が監査される。
*SECSCKD	ソケット記述子が監査される。
*SECURITY	セキュリティー関連機能がログに記録される。 *SECURITY は、監査を適切にカスタマイズするための、いくつかの値で構成されています。 *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECSCKD *SECVFY *SECVLDL
*SECVFY	検査機能の使用が監査される。
*SECVLDL	妥当性検査リスト・オブジェクトに対する変更が監査される。
*SERVICE	保守ツールの使用がログに記録される。
*SPLFDTA	スプール・ファイルに対して実行される処置がログに記録される。
*SYSMGT	システム管理機能の使用がログに記録される。

注: このシステム値は制限付きの値です。セキュリティー・システム値の変更を制限する方法、および制限付きシステム値のリストについては、*「iSeries 機密保護解説書」*の第 3 章『セキュリティー・システム値』を参照してください。

監査レベル拡張:

QAUDLVL2 システム値は、17 個以上の監査値が必要な場合は必須です。

- 文字ベースのインターフェースでの名前: **QAUDLVL2**
- iSeries ナビゲーター・インターフェースでの名前: **「アクション監査を活動化」**

- **説明:** QAUDLVL システム値の 1 つとして *AUDLVL2 を指定すると、システムは、QAUDLVL2 システム値の監査値も探します。*NONE を指定しない限り、QAUDLVL2 システム値に対して複数の値を指定できます。QAUDLVL2 システム値が有効になるには、QAUDCTL システム値に *AUDLVL が含まれている必要があり、QAUDLVL システム値に *AUDLVL2 が含まれている必要があります。

表 77. QAUDLVL2 システム値に指定できる値

監査値	説明
*NONE	このシステム値には監査値は含まれない。
*ATNEVT	条件のセキュリティー上の重要度を判別するために、さらに評価されなければならない条件を監査する。
*AUTFAIL	権限障害の事象がログに記録される。
*CREATE	オブジェクト作成操作がログに記録される。
*DELETE	オブジェクト削除操作がログに記録される。
*JOBDTA	ジョブに影響する処置がログに記録される。
*NETBAS	ネットワーク・ベース機能が監査される。
*NETCLU	クラスターおよびクラスター資源グループ操作が監査される。
*NETCMN	ネットワークおよび通信機能が監査される。 *NETCMN は、監査を適切にカスタマイズするための、いくつかの値で構成されています。 *NETBAS *NETCLU *NETFAIL *NETSCK
*NETFAIL	ネットワーク障害が監査される。
*NETSCK	ソケット・タスクが監査される。
*OBJMGT	オブジェクトの移動および名前変更操作がログに記録される。
*OFCSRV	システム配布ディレクトリーおよびオフィス・メール処置に加えられた変更がログに記録される。
*OPTICAL	光ディスク・ボリュームの使用がログに記録される。
*PGMADP	権限を借用するプログラムからの権限の取得がログに記録される。
*PGMFAIL	システム保全性違反がログに記録される。
*PRTDTA	スプール・ファイルの印刷、出力の印刷装置への直接送信、および出力のリモート印刷装置への送信がログに記録される。
*SAVRST	復元操作がログに記録される。
*SECCFG	セキュリティー構成が監査される。
*SECDIRSRV	ディレクトリー・サービス機能を実行するときの変更または更新が監査される。
*SECIPC	プロセス間通信に対する変更が監査される。
*SECNAS	ネットワーク認証サービス処置が監査される。
*SECRUN	セキュリティー実行時機能が監査される。
*SECSCKD	ソケット記述子が監査される。

表 77. QAUDLVL2 システム値に指定できる値 (続き)

監査値	説明
*SECURITY	セキュリティー関連機能がログに記録される。 *SECURITY は、監査を適切にカスタマイズするための、いくつかの値で構成されています。 *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECSCKD *SECVFY *SECVLDL
*SECVFY	検査機能の使用が監査される。
*SECVLDL	妥当性検査リスト・オブジェクトに対する変更が監査される。
*SERVICE	保守ツールの使用がログに記録される。
*SPLFDTA	スプール・ファイルに対して実行される処置がログに記録される。
*SYSMGT	システム管理機能の使用がログに記録される。

注: このシステム値は制限付きの値です。セキュリティー・システム値の変更を制限する方法、および制限付きシステム値のリストについては、「*iSeries 機密保護解説書*」の第 3 章『セキュリティー・システム値』を参照してください。

監査終了処置:

QAUDENDACN システム値を使用すれば、ジャーナル項目の送信時にエラーが発生したため監査レコードを監査ジャーナルに送れない場合に、システムがどんな処置を行うかを設定できます。

- 文字ベースのインターフェースでの名前: **QAUDENDACN**
- iSeries ナビゲーター・インターフェースでの名前: **「監査ジャーナル・エラー処置」**
- **説明:** このシステム値を使用すれば、ジャーナル項目の送信時にエラーが発生したため監査レコードを監査ジャーナルに送れない場合に、システムがどんな処置を行うかを設定できます。
- **推奨値:** ほとんどのインストール・システムでは、*NOTIFY が推奨値です。セキュリティー・ポリシーにより、監査対象でない処理をシステム上で実行できないようになっている場合、*PWRDWNSYS を選択する必要があります。

  システムが監査ジャーナル項目を書き込めなくなることは、非常にまれです。しかし、これが起きたとき、QAUDENDACN システム値が *PWRDWNSYS であれば、システムは異常終了します。これは、システムの電源を再度オンにしたとき、初期プログラム・ロード (IPL) に時間がかかる原因となります。

表 78. 使用できる値

QAUDENDACN システム値の使用	
*NOTIFY	QSYSOPR メッセージ待ち行列および QSYSMSG メッセージ待ち行列 (存在する場合) に、監査が正常に再開されるまで 1 時間ごとにメッセージ CPI2283 を送信する。システム値 QAUDCTL を *NONE に設定すると、システムが追加の監査ジャーナル項目を書き込むのを防止することができます。システムの処理は続行されます。 監査が再開される前に IPL が実行されると、その IPL の間に メッセージ CPI2284 が QSYSOPR および QSYSMSG メッセージ待ち行列に送信されます。
*PWRDWNSYS	システムは、監査ジャーナル項目を書き込むことができない場合、即時に電源遮断を行う。システム・ユニットには、システム参照コード (SRC) B900 3D10 が表示されます。システムは電力が再度オンになると、制限状態になります。つまり、制御サブシステムが制限状態で、他のサブシステムはすべて非活動状態であり、コンソールでのみサインオンを行うことができます。QAUDCTL システム値は *NONE に設定されます。IPL を完了するためにコンソールにサインオンするユーザーは、 *ALLOBJ および *AUDIT 特殊権限を持っている必要があります。

注: このシステム値は制限付きの値です。セキュリティー・システム値の変更を制限する方法と、制限付きシステム値の完全なリストについては、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。さらに、「システム値ファインダー」も参照してください。

監査強制実行レベル:

QAUDFRCLVL システム値を使用すれば、ジャーナル項目データを補助記憶装置に移動する前に監査ジャーナルに書き込まれるジャーナル項目の数を設定できます。

- 文字ベースのインターフェースでの名前: **QAUDFRCLVL**
- iSeries ナビゲーター・インターフェースでの名前: **「補助記憶装置へ書き込む前の最大ジャーナル項目数」**
- **説明:** このシステム値を使用すれば、ジャーナル項目データを補助記憶装置に移動する前に監査ジャーナルに書き込まれるジャーナル項目の数を設定できます。このシステム値により、システムが異常終了した際に失われる可能性のある監査データの量を制御できます。
- **推奨値:** 最も良い監査パフォーマンスを可能にするのは *SYS です。しかし、システムの異常終了の際に、監査項目が失われることのないようインストール・システムが要求している場合は、1 を指定する必要があります。1 を指定するとパフォーマンスが低下することがあります。

表 79. QAUDFRCLVL システム値に指定できる値

QAUDFRCLVL システム値	使用できる値
*SYS	システムは、内部システム・パフォーマンスに基づいて、ジャーナル項目が補助記憶装置に書き込まれる時を決定する。
レコード数	補助記憶装置に書き込まれる前にメモリーに蓄積できる監査項目の数を、1 から 100 までの数値で指定する。数値が小さいほど、システム・パフォーマンスに与える影響は大きくなります。

注: このシステム値は制限付きの値です。セキュリティー・システム値の変更を制限する方法と、制限付きシステム値の完全なリストについては、「機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。さらに、「システム値ファインダー」も参照してください。

新規オブジェクトの監査:

QCRTOBJAUD システム値を使用すれば、新規オブジェクトがライブラリー内に作成されたときに使用されるデフォルト監査値を設定できます。

- 文字ベースのインターフェースでの名前: **QCRTOBJAUD**
- iSeries ナビゲーター・インターフェースでの名前: **「デフォルト・オブジェクトのデフォルト監査 (default auditing for default object)」**
- **説明:** QCRTOBJAUD システム値を使用すれば、新規オブジェクトがライブラリー内に作成されたときに使用されるデフォルト監査値を設定できます。QCRTOBJAUD システム値は、新しい無フォルダー文書に対するデフォルトのオブジェクト監査値でもあります。
- **推奨値:** 選択する値は、インストール・システムでの監査に対する要件に応じて異なります。また、CRTLIB コマンドと CHGLIB コマンドの CRTOBJAUD パラメーターを使用して、ライブラリー・レベルで監査値を制御することもできます。

表 80. QCRTOBJAUD システム値に指定できる値

QCRTOBJAUD システム値	使用できる値
*NONE	オブジェクトに対する監査は行われない。
*USRPRF	オブジェクトの監査は、オブジェクトにアクセスしているユーザーのプロファイルの値に基づいて行われる。
*CHANGE	オブジェクトに変更が加えられるごとに、監査レコードが記録される。
*ALL	オブジェクトの内容に影響するすべての処置に関する監査レコードが記録される。さらに、オブジェクトの内容が変更されたときにも、監査レコードが記録される。

注: このシステム値は制限付きの値です。セキュリティー・システム値の変更を制限する方法と、制限付きシステム値の完全なリストについては、「iSeries 機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。さらに、「システム値ファインダー」も参照してください。

「セキュリティー関連の復元」システム値

プログラムをシステムに復元すると、機密漏れの可能性が生じます。

復元後のプログラムは、本来意図されない機能を実行するよう変更されているか、強力なユーザー・プロファイルの権限を借用している可能性があります。複数のシステム値から成るセットが一体的に機能して、セキュリティー関連オブジェクトに対するシステムの処置を決定します。復元操作の準備をするとき、以下のような「セキュリティー関連の復元」システム値がどのように連動してオブジェクトを安全に復元するかを理解する必要があります。

- 復元時にオブジェクトの署名を検査
- 復元時の強制変換
- セキュリティーが重要なオブジェクトの復元の許可
- 復元操作後にアクセスされるオブジェクトのスキャン

「復元時にオブジェクトの署名を検査」システム値は、ディジタル署名されたオブジェクトの復元を制御します。ディジタル署名は、システム上のオブジェクトが改変されていないこと、および信頼されたソースから得られたことを保証し、保全性保護を改善します。このシステム値は、署名者が信頼できるかどうか検証することにより、これらのオブジェクトの署名を検証します。オブジェクトがこのシステム値による検査をエラーなく通過した後、システムは「復元時の強制変換」システム値を確認します。

システムが確認するこの 2 番目のシステム値は、復元時にオブジェクトを強制変換するかどうかを決定します。「復元時の強制変換」システム値を使用すれば、プログラム、サービス・プログラム、SQL パッケージ、およびモジュール・オブジェクトを復元時に変換するかどうかを指定できます。さらに、いくつかの

オブジェクトの復元を禁止することもできます。このシステム値に加えて、復元コマンドの発行時にオブジェクト強制変換 (*FRCOBJCVN) パラメーターを指定することができます。最初の 2 つのフィルターを通過したオブジェクトだけが 3 番目のシステム値に進みます。

「セキュリティーが重要なオブジェクトの復元の許可 (QALWOBJRST)」システム値は、機密性の高い属性を持つオブジェクトを復元できるかどうかを指定します。

復元でのオブジェクトの検査:

復元でのオブジェクトの検査 (QVFYOBJRST) システム値は、オブジェクトをシステムに復元するためには、ディジタル署名がそのオブジェクトに必要かどうかを決定します。

オブジェクトに信頼できるソフトウェア・プロバイダーからの適切なディジタル署名がない限り、そのオブジェクトの復元をすべてのユーザーに対して禁止できます。この値は、オブジェクト・タイプ *PGM、*SRVPGM、*SQLPKG、*CMD、および *MODULE に適用されます。また、この値は、Java プログラムを含む *STMF オブジェクトにも適用されます。

システムにオブジェクトを復元しようとすると、 3 つのシステム値が一連のフィルターの働きをして、そのオブジェクトの復元を認めるかどうかを判別します。最初のフィルターは、復元におけるオブジェクトの検査 (QVFYOBJRST) システム値です。これを使用して、ディジタル署名が可能なオブジェクトの復元を制御します。 2 番目のフィルターは、復元時の強制変換 (QFRCCVNRST) システム値です。このシステム値では、プログラム、サービス・プログラム、SQL パッケージ、およびモジュール・オブジェクトを復元時に変換するかどうかを指定することができます。さらに、いくつかのオブジェクトの復元を禁止することもできます。最初の 2 つのフィルターを通過したオブジェクトだけが 3 番目のフィルターに進みます。 3 番目のフィルターは、オブジェクト復元許可 (QALWOBJRST) システム値です。このシステム値は、機密性の高い属性を持つオブジェクトを復元できるかどうかを指定します。

ディジタル証明書マネージャー、(i5/OS オプション 34) がシステムに導入済みでない場合、システムによって信頼されたソースが署名したオブジェクト以外のオブジェクトはすべて、復元操作時に QVFYOBJRST システム値による影響を判別する際に未署名として扱われます。このシステム値への変更は、即時に有効になります。

注:

- このシステム値は制限付きの値です。セキュリティー・システム値の変更を制限する方法と、制限付きシステム値の完全なリストについては、『セキュリティー・システム値』を参照してください。
- システム出荷時は、QVFYOBJRST システム値は 3 に設定されています。QVFYOBJRST 値を変更する場合は、i5/OS オペレーティング・システムの新しいリリースを導入する前に、QVFYOBJRST 値を 3 以下に設定することが大切です。

QVFYOBJRST システム値に指定できる値	
1	復元で署名の検査は行いません。署名とは無関係に、すべてのオブジェクトを復元します。 復元対象の署名付きオブジェクトが妥当な理由で署名検査に失敗してしまう場合を除いて、この値を使用しないでください。
2	復元でオブジェクトの検査を行います。未署名のコマンドおよび未署名のユーザー状態オブジェクトを復元します。署名付きコマンドおよび署名付きユーザー状態オブジェクトは、署名が有効でない場合でも復元されます。 この値は、署名が有効ではない特定のオブジェクトを復元したい場合に限って使用してください。通常は、署名が有効でないオブジェクトをシステムに復元するのは危険です。

QVFYOBJRST システム値に指定できる値	
3	復元で署名の検査を行います。未署名のコマンドおよび未署名のユーザー状態オブジェクトを復元します。署名付きコマンドおよび署名付きユーザー状態オブジェクトは、署名が有効な場合に限って復元されます。 この値は、通常の操作で使用できます。つまり、復元対象の一部のオブジェクトが未署名であることが予想される一方、すべての署名付きオブジェクトに有効な署名が付いていることを確認したいような場合です。ディジタル署名が使用可能になる前に作成または購入したコマンドおよびプログラムは、未署名です。この値では、これらのコマンドおよびプログラムは復元されます。これはデフォルト値です。
4	復元で署名の検査を行います。未署名のコマンドおよび未署名のユーザー状態オブジェクトは復元しません。署名付きコマンドおよび署名付きユーザー状態オブジェクトは、署名が有効でない場合でも復元されます。 この値は、署名が有効ではない特定のオブジェクトを復元したいものの、未署名オブジェクトを復元したくない場合に限って使用してください。通常は、署名が有効でないオブジェクトをシステムに復元するのは危険です。
5	復元で署名の検査を行います。未署名のコマンドおよび未署名のユーザー状態オブジェクトは復元しません。署名付きコマンドおよび署名付きユーザー状態オブジェクトは、署名が有効な場合に限って復元されます。 この値は最も制約の強い値で、信頼できるソースによって署名されたオブジェクトのみを復元したい場合に使用します。

システム状態属性を持つオブジェクト、および継承状態属性を持つオブジェクトは、システムで信頼されたソースの有効な署名を持っている必要があります。有効な署名を持たないシステム状態オブジェクトまたは継承状態オブジェクトの復元を許可する唯一の値は 1 です。有効な署名を持たないこのようなコマンドまたはプログラムを認めると、システム保全性が危険にさらされる可能性が高くなります。 QVFYOBJRST システム値を 1 に変更して、システムにこのようなオブジェクトの復元を許可する場合には、そのオブジェクトの復元後、QVFYOBJRST システム値を元の値に確実に戻してください。

コマンドの中には、オブジェクトの全部分をカバーしない署名を使用するものもあります。コマンドには、署名されない部分と、デフォルト値以外の値が指定された場合にのみ署名される部分があります。このタイプの署名を使用することで、署名を無効にせずにコマンドの内容を変更可能にすることができます。これらのタイプの署名を無効にしない変更の例は、次のとおりです。

- コマンドのデフォルト値の変更
- コマンドへの妥当性検査プログラムの追加 (まだ存在しない場合)
- **where allowed to run** パラメーターの変更
- **allow limited user** パラメーターの変更

必要に応じて、コマンド・オブジェクトのこのような領域が含まれているコマンドにユーザー独自の署名を追加することもできます。

推奨値: 3。

復元時の強制変換:

このシステム値を使用すると、復元時にいくつかのオブジェクト・タイプを変換するかどうかを指定できます。また、いくつかのオブジェクトの復元を禁止することもできます。

このシステム値では、復元時に次のオブジェクト・タイプを変換するかどうかを指定することができます。

- プログラム (*PGM) とサービス・プログラム (*SRVPGM)

- SQL パッケージ (*SQLPKG)
- モジュール (*MODULE)

さらに、いくつかのオブジェクトの復元を禁止することもできます。システム値により変換することが指定されているが、 作成に必要なデータが足りないために変換できなかったオブジェクトは、復元されません。

復元コマンド (RST、RSTLIB、RSTOBJ、RSTLICPGM) の FRCOBJCVN パラメーターの *SYSVAL 値は、 このシステム値の値を使用します。したがって、QFRCCVNRST 値を変更することで、システム全体の変換のオン/オフを切り替えることができます。ただし、FRCOBJCVN パラメーターがシステム値をオーバーライドする場合もあります。 FRCOBJCVN で *YES および *ALL を指定すると、システム値の設定はすべてオーバーライドされます。 FRCOBJCVN パラメーターで *YES および *RQD を指定することは、 このシステム値に 2 を指定することと同じで、 0 または 1 に設定されている場合、システム値はオーバーライドされます。

QFRCCVNRST は一連の 3 つのシステム値の 2 番目です。 これら 3 つのシステム値はフィルターとして機能し、オブジェクトの復元を許可するかどうか、また復元時に変換するかどうかを判別します。 1 番目のフィルター、つまり復元におけるオブジェクトの検査 (QVFYOBJRST) システム値は、ディジタル署名できるオブジェクトの復元を制御します。最初の 2 つのフィルターを通過したオブジェクトだけが、機密性の高い属性を持つオブジェクトの復元を認めるかどうかを指定する 3 番目のフィルター、つまりオブジェクト復元許可 (QALWOBJRST) システム値で処理されます。

出荷時の QFRCCVNRST の値は 1 です。QFRCCVNRST の値にかかわらず、変換が指定されているのに変換できなかったオブジェクトは復元されません。システムで信頼されているソースによってディジタル署名されているオブジェクトは、このシステム値にかかわらず、変換なしで復元されます。

注: このシステム値は制限付きの値です。セキュリティー・システム値の変更を制限する方法と、制限付きシステム値の完全なリストについては、「iSeries 機密保護解説書」の第 3 章『セキュリティー・システム値』を参照してください。

セキュリティーが重要なオブジェクトの復元の許可:

復元におけるオブジェクトの検査 (QVFYOBJRST)、 復元時の強制変換 (QFRCCVNRST)、 およびオブジェクト復元許可 (QALWOBJRST) の 3 つのシステム値が一連のフィルターとして働いて、 プログラムを変更なしで復元するか、 復元時に再作成するか、 またはシステムに復元しないかを判別します。

QVFYOBJRST システム値は、オブジェクトをユーザーのシステムに復元するために、ディジタル署名がそのオブジェクトに必要かどうかを決定します。オブジェクトに信頼できるソフトウェア・プロバイダーからの適切なディジタル署名がない限り、そのオブジェクトの復元をすべてのユーザーに対して禁止できます。

QFRCCVNRST システム値では、復元時に次のオブジェクト・タイプを変換するかどうかを指定することができます。

- プログラム (*PGM)
- サービス・プログラム (*SRVPGM)
- モジュール (*MODULE)
- SQL パッケージ (*SQLPKG)

QALWOBJRST システム値は、セキュリティーが重要なオブジェクトを、システムへ復元するかどうかを決定します。このシステム値を使用すれば、システム状態オブジェクトや権限を借用するオブジェクトを何者かが復元するのを防ぐことができます。

復元操作を実行する前に、どんな復元を実行するか計画する必要があります。次に、必要を満たす適切な設定値にシステム値を構成します。その後、復元操作が実行されるときに、適切な設定値がシステムで指定されます。オブジェクトをシステムに復元する方法を計画するには、それぞれの企業のニーズに応じて以下の質問に答えてください。

- 復元されるものに対して、どれだけ注意が必要ですか ?
- どんなオブジェクトの復元を許可したいですか ?

これらの復元システム値の使用に関する詳細は、「iSeries 機密保護解説書」第 3 章の以下のセクションを参照してください。

- 『復元におけるオブジェクトの検査 (WVFYOBJRST)』
- 『復元時の強制変換 (QFRCCVNRST)』
- 『セキュリティーが重要なオブジェクトの復元の許可 (QALWOBJRST)』

復元操作後にアクセスされるオブジェクトのスキャンを次のように設定します。

システム値 QSCANFSCTL の *NOPOSTRST 値は、復元操作後にオブジェクトをスキャンするかどうかに影響を与えます。復元操作が完了した後、次のアクセス時にオブジェクトをスキャンしたいですか? どんなオブジェクトが復元されるか、スキャンによってパフォーマンスがどのように影響を受けるかを考慮する必要があります。オブジェクトのスキャンを決定する前に、次の点を考慮してください。保管時にオブジェクトをスキャンし、スキャンが失敗したらオブジェクトを保管しないようなオプションを使用した場合には、そのようにして保管された自分のオブジェクトを復元するときにスキャンは必要ないかもしれません。また、信頼されたソースから得られたオブジェクトを復元するときにはスキャンが必要ないかもしれません。

システム値選択ワークシート

このトピックでは、システム値選択ワークシートを紹介します。

表 81. システム値選択ワークシート

汎用のセキュリティー・システム値			
作成者:		日付:	
システム値	**推奨値**	**実際の選択**	
システム名			
日付区切り記号 (QDATSEP)			
日付形式 (QDATFMT)			
QSCANFS			
QSCANFSCTL			
時刻区切り記号 (QTIMSEP)			
新しい装置の装置名形式 (QDEVNAMING)	1 (システム)		
システム印刷装置 (QPRTDEV)			
セキュリティー・レベル (QSECURITY)	40		
機密保護担当者は任意のディスプレイ装置にサインオン可能 (QLMTSECOFR)	N		

表 81. システム値選択ワークシート (続き)

汎用のセキュリティー・システム値			
完了したプリンター出力に関するジョブ会計情報の保管 (QACGLVL)	N (*NONE)		

システム値選択ワークシート		**2 / 2**
第 2 部の追加指示 • システム値処理 (WRKSYSVAL) コマンドを使用して、第 2 部を入力します。		
セキュリティー・システム値		
システム値	**推奨される選択項目**	**実際の選択**
非活動ジョブ・タイムアウト間隔 (QINACTITV)	30 から 60	
非活動ジョブ・メッセージ待ち行列 (QINACTMSGQ)	*DSCJOB	
装置セッション限界 (QLMTDEVSSN)	1 (はい)	
サインオンの試行に失敗したときのアクション (QMAXSGNACN)	3 (どちらも使用不可)	
許可されているサインオンの最大試行回数 (QMAXSIGN)	3 から 5	
パスワード満了間隔 (QPWDEXPITV)	30 から 60	
パスワードの最大文字数 (QPWDMAXLEN)	8	
パスワードの最小文字数 (QPWDMINLEN)	6	
必須の異なるパスワード (QPWDRQDDIF)	7 (6 つの固有のパスワード)	
他のシステム値		
システム値	**推奨される選択項目**	**実際の選択**
切り離しジョブ・タイムアウト間隔 (QDSCJOBITV)	300	
注: 他のセキュリティー関連のシステム値を設定することができます。セキュリティー関連システム値の詳細なリストと推奨事項については、*「機密保護解説書」* (SD88-5027-04) の第 3 章を参照してください。		

インターネット・ブラウザーのセキュリティーに関する考慮事項

インターネット・ブラウザーを使用する場合によく発生するセキュリティー上の危険について、以下の情報を参照してください。

組織の多くの PC ユーザーが、それぞれのワークステーションにブラウザーを導入しています。それらのユーザーはインターネットや組織のサーバーに接続することがあります。PC およびサーバーのセキュリティーに関するより詳しい考慮事項は、システム・インターネット・セキュリティーに関するトピックの「インターネット・セキュリティーの計画」の情報を参照してください。

リスク: ワークステーションの損害:

このトピックでは、ワークステーションに関するセキュリティー上のリスクを説明し、このようなリスクを軽減するための推奨事項を示します。

ユーザーがアクセスする Web ページには、関連する「プログラム」(たとえば、Java アプレット、Active-X コントロール、または他の何らかのタイプのプラグイン) が含まれる可能性があります。このような「プログラム」が PC で実行されると、PC 上の情報が損傷を受ける可能性があります。機密保護管理者は、組織内の PC を保護するために以下の点を考慮してください。

- ユーザーが持っているさまざまなブラウザーのセキュリティー・オプションを理解します。たとえば、Java アプレットが PC データを損なうことを防止するには、Java アプレットからブラウザー外部へのアクセスを制御することができます。
- ユーザーに、ブラウザー設定に関する推奨事項を提供します。設定が不適切な場合のリスクについて、ユーザーに通知しておく必要があります。

リスク: マップされたドライブを介するシステム・ディレクトリーへのアクセス:

このトピックでは、システム・ディレクトリーに関するセキュリティー上のリスクを説明し、このようなリスクを軽減するための推奨事項を示します。

PC が、IBM iSeries Access for Windows セッションでサーバーに接続されているとします。このセッションでは、マップされたドライブを統合ファイル・システムにリンクするようにセットアップされました。たとえば、PC の G ドライブは、ネットワークの SYSTEM1 サーバーの統合ファイル・システムにマップされます。

ここで、同じ PC ユーザーがブラウザーをもち、インターネットにアクセスできるものと仮定します。ユーザーは、Java アプレットや Active-X 制御など害を及ぼす「プログラム」を実行する Web ページを要求します。このプログラムは PC の G ドライブに含まれているすべてのデータを消去する可能性があります。

マップされたドライブに対する損害を防ぐためには、以下のようないくつかの保護処置があります。

- 最も重要な保護処置は、サーバーに関する資源保護です。Java アプレットや Active-X 制御は、サーバーにとって、PC セッションを確立したユーザーのように見えます。サーバーでどの PC ユーザーにどの操作を許可するかについて、個別に注意深く管理する必要があります。
- マップされたドライブへのアクセス試行を防止するようにブラウザーを設定することを、 PC ユーザーに指示しておく必要があります。この方法は Java アプレットに対しては有効ですが、Active-X 制御に対しては機能しません。
- 同一セッションでサーバーとインターネットに接続することの危険性について、ユーザーに通知しておく必要があります。また、iSeries Access セッションが終了したように見えても、ドライブがマップされたままになっていることを PC ユーザーに理解してもらうことも必要です。

リスク: 署名済みアプレットの信頼:

このトピックでは、署名済み Java アプレットに関するセキュリティー上のリスクを説明し、このようなリスクを軽減するための推奨事項を示します。

ユーザーは、指示に従って、アプレットが PC ドライブに書き込まないようにブラウザーをセットアップしているかもしれません。しかし、PC ユーザーは、署名済みアプレットがブラウザーの設定をオーバーライドできるということを知っておく必要があります。

署名済みアプレットには、それを認証するためのディジタル署名が関連付けられています。ユーザーが署名済みアプレットを含む Web ページにアクセスすると、メッセージが出されます。このメッセージには、ア

プレットの署名に加えて、誰がいつそれに署名したかが示されます。ユーザーがアプレットを受け入れるとき、ユーザーはアプレットがブラウザーのセキュリティー設定をオーバーライドするのを認可することになります。署名済みアプレットは、ブラウザーのデフォルト設定によって PC ローカル・ドライブへの書き込みが禁止されていても、書き込みを行うことができます。署名済みアプレットは、サーバー上のマップされたドライブにも書き込むことができます。PC にとって、これらのドライブはローカル・ドライブのように見えるためです。

サーバーから生成された独自の Java アプレットの場合は、署名済みアプレットを使用する必要があるかもしれません。ただし、ソースのはっきりしない署名済みアプレットを受け入れないよう、ユーザーを指導しておく必要があります。

LPAR セキュリティーの計画

この情報を使用して、サーバーでの論理区画 (LPAR) のセキュリティーを計画します。

論理区画を使用すると、単一のサーバー内でリソースを分散させ、それが 2 つ以上の独立したサーバーであるのと同様に機能させることができます。それぞれの論理区画は、独立した論理サーバーとして作動します。しかし各区画は、システムのシリアル番号、システム・モデル、および処理装置のフィーチャー・コードなどのいくつかの物理システム属性を共有します。

区画に分割されたシステムで実行するセキュリティー関連タスクは、論理区画が無いシステムのものと同じです。ただし、論理区画を作成する場合には、複数の独立システムを処理します。そのため、論理区画が無いシステムでは 1 回実行するだけで済むタスクを、各論理区画ごとに実行する必要があります。

『システム管理』の下にある『論理区画のセキュリティー管理』を参照してください。

オペレーション・コンソールのセキュリティーの計画

オペレーション・コンソールでは、PC を使用してシステムにアクセスし制御することができます。 オペレーション・コンソールをセキュリティー計画全体に含めるのは重要なことです。

従来のコンソールからできなかったタスクを、オペレーション・コンソールから行うことができます。たとえば、*SERVICE または *ALLOBJ 特殊権限を持っているユーザー・プロファイルは、オペレーション・コンソール・セッションが使用不可であっても、オペレーション・コンソール・セッションにサインオンすることができます。

オペレーション・コンソールは、保守ツール・ユーザー・プロファイルおよびパスワードを使用して、iSeries サーバーへの接続を可能にします。そのため、保守ツール・ユーザー・プロファイルおよびパスワードの変更が特に重要になります。ハッカーは、デフォルトの保守ツール・ユーザー・プロファイルのユーザー ID およびパスワードをよく知っており、これらを使用して、iSeries サーバーにリモート・コンソール・セッションを確立しようとするかもしれません。パスワードに関するヒントは、『 83 ページの『割り当て済みパスワードの変更』』および『 85 ページの『デフォルト・パスワードの回避』』を参照してください。

ユーザー・セキュリティーの設定

ユーザー・セキュリティーの計画には、 セキュリティーがシステム上のユーザーに影響を与えるすべての分野の計画が含まれます。

ユーザー・セキュリティーを計画する際、次の分野についての記述が必要です。

ユーザー・グループのセキュリティー

ユーザー・グループは、同じアプリケーションを同じ方法で使用する必要があるユーザーのグルー

プです。ユーザー・グループのセキュリティーの計画には、システムの使用を計画するワークグループと、それらのワークグループに必要なアプリケーションの決定が含まれます。

個々のユーザーのセキュリティー
必要なユーザー・グループが決定したら、必要な個々のユーザー・プロファイルを計画することができます。

ユーザー・セキュリティーを計画する際、以下の計画用紙を使用すると役立つ場合があります。

- システム装置および接続装置の物理的な場所に関連したセキュリティーの問題について記述するには、物理的セキュリティー計画ワークシートを使用します。
- ユーザー・グループ ID ワークシートは、同様のアプリケーションを必要としているユーザーのグループを識別するのに使用します。
- ユーザー・グループ記述ワークシートは、各ユーザー・グループの特性を記述するのに使用します。
- *USER 以外のユーザー・クラスを持つ、ご使用のシステムにアクセスするすべてのユーザーのリストを作成するには、システム責任ワークシートを使用します。
- システム上の各ユーザー・グループごとに、個々のシステム・ユーザーに関する情報を記録するユーザー・プロファイル・ワークシートに記入してグループ・プロファイルを作成してください。

ユーザー・セキュリティーの計画が完了したなら、資源保護の計画を開始できます。

関連概念

14 ページの『ユーザー・セキュリティー』
ユーザーの視点から見ると、セキュリティーは、ユーザーがシステム上でタスクを使用および完了する仕方に影響を与えます。

ユーザー・グループの計画

このトピックでは、ユーザー・グループの計画を作成するために行う事柄について取り上げます。

計画のプロセスの最初のステップは、セキュリティー戦略の決定です。これは、会社の方針を設定するのに似ています。次いで、ユーザーのグループを計画することができます。これは、部門の方針を決定するのに似ています。

ユーザー・グループとは ユーザー・グループとは、まさにその名前が示す通り、同じアプリケーションを同じ方法で使用する必要がある人々のグループです。一般的に、ユーザー・グループは、同じ部門で働き、仕事の責任が似ている人同士で構成されます。ユーザー・グループは、グループ・プロファイルを作成することによって定義します。

グループ・プロファイルで何をするか グループ・プロファイルは、システムにおいて以下の 2 つの目的を果たします。

- **セキュリティー・ツール:** グループ・プロファイルを使用することによって、システム上で特定のオブジェクトを使用できる人 (オブジェクト権限) を簡単に編成することができます。グループの個々のメンバーにではなく、グループ全体に対してオブジェクト権限を定義することができます。
- **カスタマイズ・ツール:** 個々のユーザー・プロファイルを作成する際のパターンとして、グループ・プロファイルを使用することができます。同じグループになるたいていのユーザーは、初期メニューおよびデフォルト・プリンターなど、カスタマイズの要件は同じになります。これらの要件をグループ・プロファイルに定義し、それを個々のユーザー・プロファイルにコピーすることができます。

グループ・プロファイルを使用することによって、 セキュリティーとカスタマイズの両面において、 簡単で、一貫した体系を保持しやすくなります。

どのような用紙が必要か

- ユーザー・グループ ID ワークシートを完成させて、システム上で必要なアプリケーションが類似しているユーザーのグループを識別します。
- お客様のシステムを使用する各グループごとに、ユーザー・グループ記述を作成します。

こうした用紙を完成させるには、以下の作業を実行する必要があります。

1. ユーザー・グループの識別
2. グループ・プロファイルの計画
3. サインオンに影響する値の選択
4. ユーザーが実行できる機能を制限する値の選択
5. ユーザーの環境を設定する値の選択

ユーザー・グループの識別

ユーザー・グループを計画する場合、まずシステム上にあるユーザーのグループを識別することが必要です。このようにグループを識別することによって、それらのグループに必要な資源へのアクセスを計画することができます。ユーザー・グループを識別する、1 つの簡単な方法を使ってみましょう。システムを使用する計画がある部署やワークグループについて考えてみてください。前の部分で描いた、使用するアプリケーションのアプリケーション図を見てください。ワークグループとアプリケーションとの間に、自然な関係が存在しているかどうかを調べてください。

- 各ワークグループの 1 次アプリケーションを識別できるか。
- 各グループに必要なアプリケーションを認識しているか。各グループが必要としないアプリケーションは何か。
- 各アプリケーション・ライブラリーに情報を持つべきグループを認識しているか。

これらの質問に「はい」と答えられる場合は、グループ・プロファイルの計画を始めることができます。しかし、「時々」とか、「たぶん」という答えの場合は、系統立ててユーザー・グループを識別するとよいでしょう。

注: 1 人のユーザーが属するグループ・プロファイルを 1 つだけに絞るなら、セキュリティーの管理を単純化することができます。しかし、ある場合には、1 人のユーザーを複数のグループ・プロファイルに属させた方が、役に立つ場合もあります。ユーザーを複数のグループ・プロファイルに属させると、通常は、個々のユーザー・プロファイルに私用権限を与えるよりも、管理が容易になります。

各ユーザー・グループの役割を決定してください。決定においてユーザー・グループ識別用紙が必要であれば、この用紙に記入してください。ユーザー・グループ識別用紙にユーザーを追加したら、グループ・プロファイルを計画することができます。

例: ユーザー・グループの識別

この例では、さまざまなグループが契約と価格設定のアプリケーションを必要とします。

- 販売マーケティングの部門は、価格を設定し、顧客との契約を取り付けます。この部門は、価格設定および契約の情報を所有しています。
- 顧客オーダーの部門は、間接的に契約情報を変更します。この部門で注文が処理されると、契約の数量が変更されます。彼らは、契約と価格設定の情報を変更する必要があります。
- 注文処理の担当者たちは、作業の計画を立てるためにクレジットの限度額を知る必要がありますが、その情報を変更することは許されていません。彼らはクレジットの限度額に関するファイルを表示する必要があります。

表 82. 例: ユーザー・グループ識別用紙

ユーザー・グループ識別用紙					
		アプリケーションに対して必要なアクセス			
ユーザー名	部門	アプリケーション : A	アプリケーション : B	アプリケーション : C	アプリケーション : D
Ken H.	注文処理	O	C	C	C
Karen R.	注文処理	O	C	C	C
Kris T.	経理	V		V	O
Sandy J.	経理	V	C	V	O
Peter D.	経理	C		V	O
Ray W.	倉庫	V	O	V	
Rose Q.	倉庫	V	O	V	
Roger T.	販売マーケティング	C	C	O	C
Sharon J.	管理	C	C	C	C

注:
- アプリケーションの情報を見るだけでよいユーザーについては、V (表示) を使用します。
- アプリケーションの情報を変更する必要もあるユーザーについては、C (変更) を使用します。
- 情報に対して主要な責任を持つユーザーについては、O (所有者) を使用します。

グループ・プロファイルの計画:

このトピックでは、グループ・プロファイルの目的およびその設計方法について取り上げます。グループ・プロファイルを使用して、各ユーザーに個々に権限を与えるのではなく、ユーザーのグループに対して権限を定義します。

1 人のユーザーは、最高で 16 個のグループ・プロファイルのメンバーになれます。個々のユーザー・プロファイルを作成する際は、グループ・プロファイルをパターンとして使用することができます。

ユーザー・グループを識別したら、続いて各グループにプロファイルを計画することができます。下される決定の多くは、セキュリティーとカスタマイズの両方に影響します。たとえば、初期メニューを指定すると、あるユーザーをそのメニューだけに制限することになるでしょう。しかし、その指定は、そのユーザーがサインオンした後に、適切なメニューが表示されるようにすることにもなります。

グループ・プロファイルは、特別なタイプのユーザー・プロファイルです。グループ・プロファイルは、システムにおいて以下の 2 つの目的を果たします。

セキュリティー・ツール
グループ・プロファイルにより、システムでの権限を構成し、それらの権限をユーザー間で共用するための方式が提供されます。それぞれ個々のユーザー・プロファイルごとにではなくグループ・プロファイルごとにオブジェクト権限または特殊権限を定義することができます。1 人のユーザーは、最高で 16 個のグループ・プロファイルのメンバーになれます。

カスタマイズ・ツール
グループ・プロファイルは、個々のユーザー・プロファイルを作成する場合のパターンとして使用できます。同じグループになるたいていのユーザーは、初期メニューおよびデフォルト・プリンタ

ーなど、カスタマイズの要件は同じになります。これらの要件をグループ・プロファイルに定義し、そのグループ・プロファイルをコピーして個々のユーザー・プロファイルを作成することができます。

数人のユーザーが類似したセキュリティー要件を持っている場合、グループ・プロファイルは有用なツールです。それらが特に役立つのは、ジョブ要求とグループ・メンバーシップが変更した場合です。たとえば、ある部門のメンバーがあるアプリケーションに対して責任がある場合、グループ・プロファイルをその部門に対して設定することができます。ユーザーが部門に加わったり離れたりするたびに、そのユーザー・プロファイルのグループ・プロファイル・フィールドは変更することができます。この方がユーザー・プロファイルから個々の権限を除去するよりも管理が簡単です。プロファイルを特にグループ・プロファイルとして作成したり、または既存のプロファイルをグループ・プロファイルとして作成したりすることができます。グループ・プロファイルは単に特殊なタイプのユーザー・プロファイルです。次のいずれかが起きると、それはグループ・プロファイルになります。

- 別のプロファイルがプロファイルをグループ・プロファイルとして指定する。
- それにグループ識別番号 (*gid*) を割り当てる。

たとえば、以下のような場合があります。

1. GRPIC と呼ばれるプロファイルを作成する。 `CRTUSRPRF GRPIC`
2. プロファイルが作成される場合、それは普通のプロファイルであり、グループ・プロファイルではない。
3. GRPIC を別のグループ・プロファイルのために、グループ・プロファイルとして指定する。 `CHGUSRPRF USERA GRPPRF(GRPIC)`
4. システムは GRPIC をグループ・プロファイルとして扱い、それに *gid* を割り当てる。

グループ・プロファイル計画の作成

グループ・プロファイルは、個々のプロファイルを作成するのと同じ方法で作成します。システムは、最初のメンバーをグループ・プロファイルに追加する際に、そのグループ・プロファイルを認識します。この時点で、システムはプロファイルにそれがグループ・プロファイルであることを示す情報を設定します。システムは、プロファイルのグループ識別番号 (*gid*) も生成します。 さらに、GID パラメーターに値を指定してプロファイルを作成する際、そのプロファイルをグループ・プロファイルとして指定することもできます。

グループ・プロファイルを計画するには、以下のステップを実行します。

1. 識別された各グループごとにユーザー・グループ記述ワークシートを準備する。
2. それぞれのグループに一貫した名前を付ける。
3. 命名規則ワークシートを使用して、使用するグループ命名規則を文書化する。
4. 各ユーザー・グループで必要なアプリケーションおよびライブラリーを判別する。アプリケーション記述およびライブラリー記述ワークシートを使用してください。
5. ユーザー・グループごとのジョブ記述を定義する。

オブジェクトの 1 次グループの計画

システム上のすべてのオブジェクトは、1 次グループを持つことができます。 1 次グループが、オブジェクトのほとんどのユーザーに対して最初のグループである場合、1 次グループ権限により、パフォーマンス上の利点が得られます。 ユーザーの 1 つのグループが、顧客情報などの、システムのある種の情報を担当

する場合があります。そのグループには、他のシステム・ユーザーより、その情報に対する高い権限が必要です。 1 次グループ権限を用いると、権限検査のパフォーマンスに影響を与えずに、この種の権限計画を設定することができます。

複数のグループ・プロファイルの計画

1 人のユーザーは、最高 16 個のグループのメンバーになれます。これらは、最初のグループ (ユーザー・ファイル内の GRPPRF パラメーター)、 および 15 個の補足グループ (ユーザー・プロファイル内の SUPGRPPRF パラメーター) です。グループ・プロファイルを用いると、権限をより効果的に管理し、オブジェクトに対する個々の私用権限の数を減らすことができます。しかし、グループ・プロファイルの使用を誤ると、権限検査のパフォーマンスに望ましくない影響を与える可能性があります。

複数のグループ・プロファイルを使用するときは、次の提案に従ってください。

- 複数グループを、1 次グループ権限と組み合わせて用いるようにして、オブジェクトへの私用権限を除去します。
- ユーザーにグループ・プロファイルを割り当てる順序を慎重に計画します。ユーザーの最初のグループは、そのユーザーの 1 次割り当て、および最も頻繁に使用されるオブジェクトに関連させます。たとえば、WAGNERB と呼ばれるユーザーが在庫作業を定期的に行い、注文入力作業を不定期に行うとします。在庫権限 (DPTIC) に必要なプロファイルは、 WAGNERB の最初のグループになります。 注文入力作業 (DPTOE) に必要なプロファイルは、WAGNERB の最初の補足グループになります。オブジェクトに私用権限が指定される順序は、権限検査パフォーマンスには影響しません。
- 複数グループを使用する計画を立てるときは、複数グループを権限リストなどの他の権限手法と組み合わせて使用する場合に、システム・パフォーマンスにどのような影響があるかを理解しておいてください。

ユーザー記述ワークシートの準備

以下の例では、 120 ページの『ユーザー・グループ記述ワークシート』にはグループ・プロファイル名、そのグループが使用するアプリケーションとライブラリーが含まれます。

表 83. 例: ユーザー・グループ記述ワークシート

ユーザー・グループ記述ワークシート
グループ・プロファイル名: DPTWH グループの説明: 倉庫部門
グループの 1 次側アプリケーション: 在庫管理 グループに必要な他のアプリケーションのリスト: なし
グループに必要な各ライブラリーをリストします。グループごとの初期ライブラリー・リストに含める必要のある各ライブラリーには X を付けます。 • X ITEMLIB • X ICPGMLIB

グループ・プロファイルの命名

グループ・プロファイルは、特別なタイプのユーザー・プロファイルとして働くため、リスト上や画面上で識別できるようにすると便利です。そのようにするには、グループ・プロファイルに特別な名前を付ける必要があります。グループ・プロファイルがリスト上にまとめて表示されるようにするには、すべてのグルー

プ・プロファイル名の先頭を、GRP (グループ) や DPT (部門) などの同じ文字で統一する必要があります。ユーザー・グループに名前を付ける際は、以下のガイドラインに従ってください。

- ユーザー・グループ名は最大 10 文字までです。
- 名前には、文字、数字、およびいくつかの特殊文字 (ポンド (#)、ドル ($)、 円 (¥)、下線 (_)、およびアットマーク (@)) を使用することができます。
- 名前を数字で開始することはできません。

注: 各グループ・プロファイルに対して、システムは、グループ識別番号 (*gid*) を割り当てます。通常は、システムに *gid* を生成させることができます。システムをネットワークで使用する場合は、グループ・プロファイルに、固有の *gid* を割り当てなければならない場合があります。ネットワーク管理者に相談して、ID を割り当てる必要があるかどうかを検討してください。

ユーザー・グループに必要なアプリケーションとライブラリーの判別

ユーザー・グループを、先に作成したアプリケーション図とライブラリーにまだ追加していない場合は、追加してください。この視覚的なイメージは、各グループに必要な資源とアプリケーションを決定する上で役立ちます。

120 ページの『ユーザー・グループ記述ワークシート』 の第 1 部では、 グループの 1 次側アプリケーション、つまりそのグループで最も頻繁に使用するアプリケーションを指示します。また、グループに必要な他のアプリケーションをリストしてください。

作成したアプリケーション記述ワークシートを見て、各グループに必要なライブラリーを調べてください。プログラマーやアプリケーションの提供者に相談して、これらのライブラリーへのアクセスを提供する、最良の方法を探してください。ほとんどのアプリケーションでは、次のいずれかの手法を使用します。

- アプリケーションが、ライブラリーをユーザーの初期ライブラリー・リストに組み込む。
- アプリケーションがセットアップ・プログラムを実行して、ライブラリーをユーザーのライブラリー・リストに置く。
- ライブラリーが、ライブラリー・リストに含まれている必要はない。アプリケーション・プログラムは、常にライブラリーを指定します。

システムは、ライブラリー・リストを使用して、アプリケーションが実行される際に必要なファイルとプログラムを検索します。ライブラリー・リストとは、システムがユーザーに必要なオブジェクトを検索するライブラリーのリストです。このリストには、次の 2 つの部分があります。

1. システム部分: QSYSLIBL システム値によって指定された部分。システム部分は i5/OS ライブラリーに使用されます。このシステム値のデフォルトは、変更する必要はありません。
2. ユーザー部分: ライブラリー・リストのうち、ユーザー部分は、QUSRLIBL システム値による部分です。ユーザーのジョブ記述は、初期ライブラリー・リスト、つまりユーザーがサインオンした後のコマンドを指定します。初期ライブラリー・リストがある場合、このリストは QUSRLIBL システム値をオーバーライドします。アプリケーション・ライブラリーは、ライブラリー・リストのユーザー部分に含まれます。

ジョブ記述の定義

ユーザーがシステムにサインオンする際、ユーザーのジョブ記述は、ジョブの印刷方法、バッチ・ジョブの実行方法、および初期ライブラリー・リストを含む、ジョブの多くの特性を定義します。このシステムには QDFTJOBD というジョブ記述がありますが、グループ・プロファイルを作成する際に、このジョブ記述を使用することができます。ただし、QDFTJOBD は、初期ライブラリー・リストとして QUSRLIBL システ

ム値を指定しています。ユーザー・グループによって、サインオンの際にアクセスするライブラリーが異なる場合は、グループごとに固有のジョブ記述を作成する必要があります。

グループに必要な各ライブラリーを、ユーザー・グループ記述用紙にリストしてください。グループのジョブ記述で、初期ライブラリー・リストに加えるライブラリーについては、用紙の各ライブラリー名にマークを付けてください。

関連概念

10 ページの『グループ・プロファイル』
グループ・プロファイルは、ユーザーのグループの権限を定義します。

ユーザー・グループ ID ワークシート:

このトピックでは、「ユーザー・グループ ID」ワークシートについて説明します。

表 84. ユーザー・グループ ID ワークシート

ユーザー・グループ ID ワークシート								
作成者:		日付:						
指示: • このワークシートについては、『ユーザー・グループの計画』を参照してください。 • このワークシートは、アプリケーション要件が類似しているユーザー・グループを識別するのに役立ちます。 1. 主要なアプリケーションをワークシートの上部にリストします。 2. ユーザーを左側の列にリストします。 3. ユーザーごとに、必要なアプリケーションにマークを付けてください。 • このワークシートの情報は、システムに入力する必要はありません。								
		アプリケーションに対して必要なアクセス						
ユーザー名	部門	APP:	APP:	APP:	APP:	APP:	APP:	APP:
注: • *寛容な* セキュリティー環境の場合は、ユーザーが必要とするアプリケーションに **X** を付けます。 • *厳重な* セキュリティー環境の場合は、アプリケーションの使用方法 を指定するために、 **C** (変更) および **V** (表示) のマークを付けます。								

ユーザー・グループ記述ワークシート:

このトピックでは、「ユーザー・グループ記述」ワークシートについて説明します。

表 85. ユーザー・グループ記述ワークシート (1 / 2)

ユーザー・グループ記述ワークシート	**1 / 2**
作成者:	日付:
第 1 部の指示 • このワークシートの作成方法については、『ユーザー・グループの計画』を参照してください。 • このワークシートの入力方法については、『ユーザー・セキュリティーの設定』を参照してください。 • システムを使用するグループごとに別々のワークシートを作成します。 • ジョブ記述作成 (CRTJOBD) コマンドを使用して、グループのジョブ記述を作成します。ジョブ記述には、グループの初期ライブラリー・リストがあります。	
グループ・プロファイル名: グループの記述:	
グループの 1 次アプリケーション: グループが必要とする他のアプリケーションのリスト:	
グループに必要な各ライブラリーをリストします。グループごとの初期ライブラリー・リストに含める必要のある各ライブラリーには、マーク **X** を付けます。	
注: 前の部分にリストされているアプリケーションごとに、 アプリケーション記述ワークシートを調べて、アプリケーションが使用するライブラリーを見つけてください。	

表 86. ユーザー・グループ記述ワークシート (2 / 2)

ユーザー・グループ記述ワークシート		**2 / 2**
第 2 部の追加指示 • 下の表は、「ユーザー・プロファイルの作成」画面に表示されるフィールドをすべてリストしています。フィールドは、自分で選択しなければならないものと、デフォルト値を使用するよう IBM が推奨するフィールドの 2 つのグループに分けられています。 • 「ユーザー・プロファイルの処理」画面またはユーザー・プロファイル作成 (CRTUSRPRF) コマンドを使用して、用紙の第 2 部の情報をシステムに入力します。		
グループ・プロファイル内の次のフィールドでは、値を選択する:		
フィールド名	**推奨される選択項目**	**実際の選択**
グループ・プロファイル名 (ユーザー)		
パスワード	*NONE	
ユーザー・クラス (ユーザーのタイプ)	*USER	
現行ライブラリー (デフォルトのライブラリー)	*グループ・プロファイル名と同じ*	
呼び出す初期プログラム (サインオン・プログラム)		
初期プログラム・ライブラリー		
初期メニュー (第 1 メニュー)		
初期メニュー・ライブラリー		
制限機能 (コマンド行の使用の制限)	*YES	
テキスト (ユーザー記述)		
ジョブ記述	*グループ・プロファイル名と同じ*	

表 86. ユーザー・グループ記述ワークシート (2 / 2) (続き)

ユーザー・グループ記述ワークシート		**2 / 2**
ジョブ記述ライブラリー		
グループ・プロファイル名 (ユーザー・グループ)	*NONE	
印刷装置 (デフォルト・プリンター)		
出力待ち行列	*DEV	
注: フィールドの順番は、「ユーザー・プロファイルの作成」画面 (F4 を使用) で表示される順序と同じです。		
次のフィールドには、システム提供の値 (デフォルト) を使用する:		
会計コード	キーボード・バッファリング	共通権限
操作援助レベル	言語 ID	パスワードの期限満了の設定
アテンション・プログラム	装置セッションの制限	分類順序
コード化文字セット識別コード	最大記憶域	特殊権限
国または地域 ID	メッセージ待ち行列	特殊環境
サインオン情報の表示	パスワードの満了間隔	状況
文書パスワード	優先順位限界	ユーザー・オプション
注: このリストのフィールドは、アルファベット順に配列されています。		

ユーザー・プロファイルの計画

このトピックでは、ユーザー・プロファイルの目的およびその設計方法について取り上げます。

ユーザー・プロファイルには、ユーザーがシステムにサインオンする方法、サインオン後にユーザーに許可されている事柄、ユーザーの活動が監査される方法など制御する、セキュリティーに関連した情報が入っています。

これまでの部分では、全体的なセキュリティー戦略を決定し、ユーザー・グループを計画しました。次に、個々のユーザー・プロファイルを計画することができます。

ユーザー・プロファイルを計画する際には、以下の点を考慮してください。

- ユーザー・プロファイルの命名に関する考慮事項
- 個々のユーザーに割り当てられた責任
- 個々のユーザーの値

ユーザー・プロファイルを計画するために以下のワークシートを完成させてください。

- 「個々のユーザー・プロファイル」ワークシート
- システム責任ワークシート

ユーザー・プロファイルを計画する際、完成した以下のワークシートを参照してください。

- 120 ページの『ユーザー・グループ記述ワークシート』
- 命名規則ワークシート
- ご使用のアプリケーション記述ワークシート

ユーザー・プロファイルの命名

システムは、ユーザー・プロファイル名によってユーザーを識別します。ユーザーは、サインオン画面の「ユーザー ID」フィールドに、自分のユーザー・プロファイル名を入力します。ユーザーが行うすべての作業、およびユーザーが作成するすべてのプリンター出力は、ユーザーのユーザー・プロファイル名と関連付けられます。ユーザー・プロファイルに名前を付ける際は、以下の点を考慮してください。

- ユーザー・プロファイル名は最大 10 文字までです。 一部の通信方式では、ユーザー ID を 8 文字までに制限しています。
- ユーザー・プロファイル名には、文字、数字、およびいくつかの特殊文字 (ポンド (#)、ドル ($)、円 (¥)、下線 (_)、 およびアットマーク (@)) を使用することができます。名前の先頭に数字や下線 (_) を使用することはできません。
- システムでは、ユーザー・プロファイル名の大文字と小文字の区別はされません。英小文字を入力すると、システムはそれらの文字を大文字に変換します。
- ユーザー・プロファイル名を管理するために使用する画面とリストでは、ユーザー・プロファイル名をアルファベット順で示します。
- IBM 提供のプロファイルにはすべて、名前の先頭に文字 Q が付きます。 ユーザーのプロファイルと IBM 提供のプロファイルを区別するため、ユーザー・プロファイル名には、文字 Q で始まる名前を使用しないでください。

要確認: ユーザー・プロファイル名を割り当てる 1 つの技法として、 名字の先頭から 7 文字までと名前の先頭 1 文字を使用する方法があります。この方法を使用すれば、ユーザー・プロファイル名を覚えやすくなります。また、リストや画面にプロファイルを表示する場合にも、ユーザーの名字のアルファベット順で表示することができます。

ユーザー・プロファイルの役割

ユーザー・プロファイルは、システムにおいて以下の役割を担っています。

- ユーザーがシステムにサインオンする方法、サインオン後にユーザーに許可されている事柄、ユーザーの活動が監査される方法などを制御する、セキュリティーに関連した情報が入っています。
- システムをカスタマイズし、ユーザーに適応させるために設計された情報が入っています。
- オペレーティング・システムの管理および回復ツールの役割も担っています。ユーザー・プロファイルには、ユーザーが所有するオブジェクトと、オブジェクトに対するすべての私用権限についての情報も入っています。
- ユーザー・プロファイル名により、ユーザーのジョブとプリンター出力を識別します。

システムにおける QSECURITY システム値が 20 である場合、ユーザー・プロファイルが存在していなければ、ユーザーはサインオンできません。

例: ユーザー・プロファイルの命名規則ワークシート

表 87. 例: 命名規則ワークシート: ユーザー・プロファイル

ユーザー名	**ユーザー・プロファイル名**
Anderson、George	ANDSERSOG
Anderson、Roger	ANDERSOR
Jones、Sharon	JONESS
オブジェクトのタイプ	**命名規則**

表 87. 例: 命名規則ワークシート: ユーザー・プロファイル (続き)

ユーザー名	ユーザー・プロファイル名
ユーザー・プロファイル	名字の先頭から 7 文字までと名前の先頭 1 文字を使用する。ユーザー・プロファイルの説明の項には、名字、名前の順に示す。

命名規則ワークシートに、計画しているユーザー・プロファイルの命名規則を記述したら、システム機能の責任者の決定、および個々のユーザーの値の選択を行うことができます。

ユーザー・プロファイルの詳細については、「iSeries 機密保護解説書」の『ユーザー・プロファイル作成コマンドの使用』を参照してください。

関連概念

9 ページの『ユーザー・プロファイル』
各システム・ユーザーは、システムにサインオンして使用するにはユーザー ID を有している必要があります。このユーザー ID をユーザー・プロファイルといいます。

217 ページの『グループ内のユーザー用のプロファイルの作成』
このトピックでは、個別のユーザーごとのプロファイルの作成方法を取り上げます。

221 ページの『グループに属さないユーザーのプロファイルの作成』
まず最初の個別のユーザー・プロファイルをコピーして、 グループ内に追加メンバーを作成します。コピー方式を使用して個別プロファイルを作成する際には、それぞれの個別プロファイルをよく見てください。

システム責任ワークシート:

このトピックでは、システム責任ワークシートについて説明します。

表 88. システム責任ワークシート

システム責任ワークシート			
作成者:			日付:
指示: • このワークシートについては、『個々のユーザー・プロファイルの計画』を参照してください。 • このワークシートを使用して、*USER 以外のユーザー・クラスを持つ人物をリストします。 • このワークシートの情報を、ユーザー・プロファイル・ワークシートの「ユーザー・クラス」列に入力します。			
セキュリティーの第 1 責任者: 補佐の機密保護担当者:			
プロファイル名	ユーザー名	クラス	コメント

ユーザー・プロファイル・ワークシート:

このトピックでは、個別ユーザー・プロファイル・ワークシートについて説明します。

表 89. 「個々のユーザー・プロファイル」ワークシート

「個々のユーザー・プロファイル」ワークシート						
作成者:			日付:			
指示: • このワークシートの作成方法については、『個々のユーザー・プロファイルの計画』を参照してください。 • このワークシートを使用して、個々のシステム・ユーザーに関する情報を記録します。システム上のユーザー・グループ (グループ・プロファイル) ごとに 1 枚ずつワークシートに記入します。 • 個々のユーザーに指定したい追加フィールドがあれば、右側のブランクの欄を使用します。 • このワークシートの入力方法については、『ユーザー・セキュリティーの設定』を参照してください。						
グループ・プロファイル名:						
作成されたオブジェクトの所有者:			作成されたオブジェクトに対するグループ権限:			
グループ権限タイプ:						
グループのメンバーごとに項目を作成します。						
ユーザー・プロファイル	テキスト (説明)	ユーザー・クラス	制限機能			

資源保護の計画

このトピックでは、それぞれの資源保護の構成要素について、またシステムの情報を保護するためそれらすべての構成要素がどのように相互に機能するかについて説明します。また、システム上での資源保護を設定するための、CL コマンドと表示画面の使用方法についても説明します。

資源保護により、システム上のオブジェクトを使用できるユーザーと、それらのオブジェクト上で実行できる操作が定義されます。

情報にアクセスできるユーザーの定義

個々のユーザー、ユーザーのグループ、および共通ユーザーに対して権限を与えることができます。

注: 環境によっては、ユーザーの権限は特権と呼ばれます。

オブジェクトを使用できるユーザーを定義する方法はいくつかあります。

- 共通権限: 共通ユーザーは、ユーザーのシステムへサインオンが許可されている任意のユーザーで構成されています。システム上のすべてのオブジェクトに対して共通権限を定義できます (あるオブジェクトに対する共通権限を *EXCLUDE にすることができます)。オブジェクトに対する共通権限は、そのオブジェクトに対する他の特定権限が存在しない場合に使用されます。

- 私用権限: オブジェクトを使用する、または使用しない場合に、特定の権限を定義できます。個々のユーザー・プロファイルまたはグループ・プロファイルに対して、権限を認可することができます。共通権限、オブジェクト所有権、または 1 次グループ権限以外の権限がオブジェクトに定義されている場合、そのオブジェクトは私用権限を持ちます。
- ユーザー権限: 個々のユーザー・プロファイルには、システム上のオブジェクトを使用する権限を与えることができます。この権限は、私用権限の 1 つのタイプです。
- グループ権限: グループ・プロファイルには、システム上のオブジェクトを使用する権限を与えることができます。グループ・メンバーに対して特に権限が定義されていない限り、そのユーザーは、グループの権限を得ます。グループ権限もまた、私用権限と考えることができます。
- オブジェクト所有権: システム上の各オブジェクトには、所有者が存在します。所有者は、デフォルトで、オブジェクトに対する *ALL 権限を持っています。しかし、オブジェクトに対する所有者の権限を変更または除去することができます。オブジェクトに対する所有者の権限は私用権限とは見なされません。
- 1 次グループ権限: オブジェクトに 1 次グループを指定し、その 1 次グループの持つ権限をそのオブジェクトに指定することができます。1 次グループ権限はオブジェクトと一緒に保管され、グループ・プロファイルに認可された私用権限を使用するよりもパフォーマンスが向上する可能性があります。グループ識別番号 (*gid*) を持つユーザー・プロファイルだけが、オブジェクトの 1 次グループになれます。1 次グループ権限は、私用権限とは見なされません。

オブジェクト権限について詳しくは、『オブジェクト権限の計画』を参照してください。

資源保護の計画

これで、システム上のユーザーの計画プロセスが完了したので、システム上のオブジェクトを保護するための資源保護の計画を立てることができます。『資源保護』では、システムの資源保護の設定方法について説明されています。

システム値とユーザー・プロファイルは、システムにアクセスするユーザーを制御し、許可のないユーザーがサインオンできないようにします。資源保護は、許可されたシステム・ユーザーが正常にサインオンした後に実行できるアクションを制御します。資源保護は、システム・セキュリティーの主な目的に沿って、以下のものを保護します。

- 情報の機密性
- 情報の正確さ (許可なく変更できないようにする)
- 情報の可用性 (不慮または故意に損傷を与えないようにする)

資源保護の計画は、 お客様の会社でアプリケーションを開発したか、購入したかによって異なる場合があります。 アプリケーションを開発する場合は、 アプリケーションの設計時に、 情報のセキュリティー要件についてプログラマーと話し合う必要があります。 アプリケーションを購入する場合は、 計画したいセキュリティーの必要性を判別し、 それをアプリケーションの提供者が設計した方法に合わせる必要があります。 以下に説明されている手法は、どちらの事例にも役立つはずです。

この情報では、資源保護の計画に関する基本的なアプローチを示します。主要な手法を紹介し、その使用方法を示します。以下に説明されている方式は、必ずしもすべての会社のすべてのアプリケーションに当てはまるとは限りません。資源保護の計画を立てる際には、プログラマーかアプリケーションの提供者と相談してください。

以下のセクションでは、資源保護の計画を立てるのに役立つ情報を取り上げています。[子へのアクティブ・リンクのリスト]

- 資源保護
- 権限のタイプの理解
- アプリケーション・ライブラリーのセキュリティーの計画
- ライブラリーとオブジェクトの 所有権の決定
- オブジェクトのグループ化
- プリンター出力の保護
- ワークステーションの保護
- 資源保護のインプリメント
- アプリケーションの導入の計画

以下の計画用紙は、システム・レベルのセキュリティーを計画する際に役立ちます。

- システム上の各アプリケーションについて、アプリケーション記述ワークシートを完成させます。
- 『オブジェクト権限の計画』を参照して、所有権および共通権限をロードした後でそれらをアプリケーションに設定する方法を計画します。
- 「権限リスト」ワークシートを使用して、リスト、およびリストにアクセスするグループと個人が保護するオブジェクトをリストします。
- 「プリンター出力待ち行列およびワークステーションのセキュリティー」ワークシートを使用して、特別な保護が必要なワークステーションまたは出力待ち行列をリストします。

資源保護の目的の決定: 資源保護の計画に取りかかるには、最初に目的を理解しなければなりません。このシステムでは、柔軟な資源保護を実現しています。重要な資源を希望どおりに保護する機能が備えられています。しかし、資源保護により、ご使用のアプリケーションのオーバーヘッドも増加します。たとえば、あるオブジェクトがアプリケーションで必要になる場合、そのつどシステムはそのオブジェクトに対するユーザー権限を検査する必要があります。機密性の必要を満たすこととコスト・パフォーマンスの間で平衡を取らなければなりません。資源保護について決定する際には、セキュリティーの価値とコストを比較考慮してください。資源保護のためにご使用のアプリケーションのパフォーマンスが低下しないようにするには、以下の指針に従ってください。

- 資源保護の体系を単純にしておく。
- 保護する必要のあるオブジェクトだけを保護する。
- 情報を保護するための他のツールの代わりとしてではなく、補足するものとして、次のように資源保護を使用する。
  - ユーザーを特定のメニューとアプリケーションに制限する。
  - ユーザー・プロファイルの機能を制限して、ユーザーがコマンドを入力できないようにする。

資源保護の計画は、目的を定義することから始めてください。 セキュリティーの目的は、アプリケーション記述用紙かライブラリー記述用紙のどちらかで定義することができます。 使用する用紙は、ライブラリーで情報をどのように編成しているかによって決まります。

ワークステーションのセキュリティーの計画: プリンターおよびプリンター出力の資源保護の計画を立てたら、ワークステーションのセキュリティーの計画を立てることができます。物理的セキュリティーの計画の際に、ロケーションが原因でセキュリティーのリスクが生じるワークステーションをリストしました。この情報を使用して、制限する必要のあるワークステーションを判別してください。

これらのワークステーションを使用するユーザーに、特にセキュリティーに注意するよう促すことができます。これらのユーザーがワークステーションから離れる際には必ずサインオフする必要があります。セキュ

リティー・ポリシーの中に、無防備なワークステーションのサインオフ手順に関する決定事項を記録することもできます。これらのワークステーションで実行できる機能を制限して、リスクを最小限にとどめることもできます。

ワークステーションでの機能を制限する最も簡単な方式は、限定された機能を持つユーザー・プロファイルにしか、その機能を使用できないように制限することです。機密保護担当者権限または保守権限を持つユーザーがサインオンできるワークステーションを制限することもできます。 QLMTSECOFR システム値を使用してこの処理を行うと、機密保護担当者権限を持つユーザーは、特別に許可されたワークステーションだけにサインオンできます。出力待ち行列およびワークステーションのセキュリティー用紙のワークステーションの部分を作成してください。

資源保護に関する推奨事項の要約: ワークステーションのセキュリティーの計画を立てたら、以下の資源保護に関する推奨事項を検討できます。システムは、システム上の情報を保護するためのオプションを多数提供しています。このオプションを使用すると、資源保護の計画を設計する上で融通がきくため、お客様の会社にとって最善の設計にすることができます。しかし、この多数のオプションは複雑でもあります。以下の情報では、これらの指針を使用する資源保護の計画に関する基本的なアプローチを示します。

- 汎用権限から特定権限に移行する。
  - ライブラリーのセキュリティーを計画する。必要な場合のみ個々のオブジェクトを扱ってください。
  - 共通権限を最初に計画し、それからグループ権限と個別権限を計画する。
- ライブラリー内の新しいオブジェクトの作成権限 (CRTAUT) は、ライブラリー内の既存オブジェクトの大多数について定義した共通権限と同じにする。
- 共通権限より低い権限をグループまたは個別に付与しない。付与すると、パフォーマンスが低下し、その後の作業で間違いを犯しやすくなったり、監査も難しくなったりします。全員がオブジェクトに対して共通権限と同等かそれ以上の権限を持っていることが分かっていれば、セキュリティーの計画や監査が行いやすくなります。
- 同じセキュリティー要件を持つグループ・オブジェクトに対して、権限リストを使用する。権限リストは個別権限よりも管理するのが簡単で、セキュリティー情報を回復するのに役立ちます。
- アプリケーション所有者として特別なユーザー・プロファイルを作成する。所有者パスワードを *NONE に設定してください。
- QSECOFR や QPGMR のような IBM 提供のプロファイルにアプリケーションを所有させることは避ける。
- 機密報告書には特別な出力待ち行列を使用する。機密情報が含まれているライブラリーに出力待ち行列も作成してください。
- 機密保護担当者権限を持つユーザーの数を制限する。
- オブジェクトまたはライブラリーに *ALL 権限を認可する際には注意する。 *ALL 権限のあるユーザーはこれらのものを意図せずに削除する可能性があります。

資源保護の設定を正しく計画したことを確認するには、 以下の情報を収集する必要があります。

- すべてのアプリケーション・ライブラリーのライブラリー記述用紙の第 1 部と第 2 部を記入する。
- 個別ユーザー・プロファイル用紙の「作成されたオブジェクトの所有者」フィールドと「作成されたオブジェクトに対するグループ権限」フィールドに記入する。
- 命名規則用紙に、権限リストの命名計画を記述する。
- 権限リスト用紙を作成する。
- ライブラリー記述用紙に権限リスト情報を追加する。
- 出力待ち行列およびワークステーションのセキュリティー用紙を作成する。

これで、 アプリケーションの導入の計画を立てる準備が完了しました。

セキュリティー戦略の計画のステップ 3 が終了しました。次のステップへリンクします。 187 ページの『ネットワーク・セキュリティーの計画』

関連概念

17 ページの『資源保護』
認証に成功した後に許可ユーザーが行う処置を制御するために、システムの資源保護を使用することができます。

ライブラリー・セキュリティーの計画

このトピックでは、システム上のライブラリーのセキュリティーの計画方法について取り上げます。

アプリケーション情報のライブラリーへのグループ化、およびライブラリーの管理は、さまざまな要因によって影響を受けます。このトピックでは、ライブラリー設計に関連したセキュリティーの問題のいくつかについて取り上げます。オブジェクトにアクセスするには、オブジェクトそのものへの権限と、オブジェクトを含んでいるライブラリーへの権限が必要です。オブジェクトへのアクセスの制限は、オブジェクトそのもの、またはそれを含んだライブラリー、あるいはその両方を制限することによって行うことができます。

ライブラリーの計画

ライブラリーは、ライブラリー内にオブジェクトを位置付けるために使用されるディレクトリーに似ています。ライブラリーに対する *USE 権限によって、ディレクトリーを使用してライブラリー内のオブジェクトを探すことが許可されます。オブジェクトそのものに対する権限によって、そのオブジェクトをどのように使用できるかが決まります。ライブラリーへの *USE 権限は、ライブラリー内のオブジェクトに対する操作の多くを実行するのに十分なものです。

オブジェクトに対して共通権限を使用し、ライブラリーへのアクセスを制限するのは、簡単で効果的なセキュリティーの手法です。他のアプリケーションのオブジェクトとは別のライブラリーにプログラムを入れると、セキュリティー計画を単純化できます。ファイルが複数のアプリケーションによって共用される場合は、特にそう言えます。アプリケーション・プログラムを含むライブラリーへの権限を使用して、アプリケーション機能を実行できる人を制御することができます。

ライブラリー・セキュリティーは、以下の規則が守られた場合にのみ有効です。

- ライブラリーが、類似したセキュリティー要件を持つオブジェクトを含む。
- ユーザーは、制限されたライブラリーに新しいオブジェクトを追加することを許可されていない。ライブラリー内のプログラムへの変更は制御される。つまり、ユーザーがオブジェクトを直接ライブラリーに作成する必要がある場合を除いて、アプリケーション・ライブラリーには *USE または *EXCLUDE の共通権限が必要である。
- ライブラリー・リストは制御される。

ライブラリー・セキュリティーの記述

アプリケーションの設計者として、機密保護管理者にライブラリーについての情報を提供する必要があります。機密保護管理者はこの情報を利用して、ライブラリーとそのオブジェクトを保護する方法を決定します。必要とされる一般的な情報は以下のとおりです。

- オブジェクトをライブラリーに追加するアプリケーション機能があるか。
- アプリケーションの処理中に、ライブラリー内のオブジェクトが削除されるかどうか。
- ライブラリーとそのオブジェクトを所有するプロファイルはどれか。

- ライブラリーをライブラリー・リストに含めるべきかどうか。

こうした情報を提供するため、以下の記述形式の例を参照してください。

ライブラリー名: ITEMLIB

ライブラリーへの共通権限: *EXCLUDE

ライブラリー内のオブジェクトへの共通権限: *CHANGE

新しいオブジェクトへの共通権限 (CRTAUT): *CHANGE

ライブラリー所有者: OWNIC ライブラリー・リストに組み込みますか? いいえ。ライブラリーは初期アプリケーション・プログラムまたは初期 QUERY プログラムにより、ライブラリー・リストに追加されます。

ライブラリーに対する *ADD 権限を要求するすべての機能をリストしてください。アプリケーションの通常の処理時には、オブジェクトはライブラリーに追加されません。

*OBJMGT または *OBJEXIST 権限を要求するすべてのオブジェクトおよびその権限が必要な機能をリストしてください。: 文字 ICWRK で開始するすべての作業ファイルは、月末に消去されます。これを行うには、*OBJMGT 権限が必要です。

ライブラリー・セキュリティーの使用によるメニュー・セキュリティーの補足

ライブラリーのオブジェクトにアクセスするには、オブジェクトに対する権限とライブラリーに対する権限のどちらも持っていなければなりません。ほとんどの操作では、ライブラリーに対する *EXECUTE 権限か *USE 権限のどちらかが必要です。状況に応じて、ライブラリー権限をオブジェクト保護のための簡単な手段として使用することができます。たとえば、オーダー・エントリー・メニューの例の場合、オーダー・エントリー・メニューに対する権限を持っているすべてのユーザーは、ORDERPGM ライブラリー内のすべてのプログラムを使用することができます。

個々のプログラムを保護するのではなく、 ORDERPGM ライブラリーに対する共通権限を *EXCLUDE に設定することができます。そうすれば、ライブラリーに対する *USE 権限を特定のユーザー・プロファイルに与えることができ、これにより、ライブラリーのプログラムを使用できるようになりますこの場合、プログラムに対する共通権限が *USE であるか、またはそれより大きいと想定しています。ライブラリー権限を、オブジェクト権限を管理するための単純で効率的な方式として使用することができます。ただし、保護しようとしているライブラリーの内容について熟知していて、オブジェクトを不注意にアクセスしないようにすることが必要です。

アプリケーション・ライブラリーのセキュリティーの計画: 資源保護の目的の決定を終えたら、アプリケーション・ライブラリーのセキュリティーの計画を立てることができます。アプリケーション・ライブラリーの 1 つを選択し、以下に説明されているプロセスに従って作業してください。ファイルとプログラムが別々のライブラリーに保管されている場合は、ファイルを含むライブラリーを選択します。このトピックを終えたら、残りのアプリケーション・ライブラリーにも同じステップを繰り返してください。

ご使用のアプリケーションとライブラリーについて収集した以下の情報を検討してください。

- アプリケーション記述用紙
- ライブラリー記述用紙
- ライブラリーが必要なグループの場合、ユーザー・グループ記述用紙

- アプリケーション、ライブラリー、およびユーザー・グループの図

ライブラリー内の情報を必要とするグループ、必要な理由、およびその情報を使用して行う事柄を考慮します。 アプリケーション・ライブラリーには重要なアプリケーション・ファイルが含まれているので、アプリケーション・ライブラリーの内容を判別してください。またその他のオブジェクトも含まれていることがありますが、 その大部分はアプリケーションを適切に稼働させるためのプログラミング・ツールです。 次のようなものがあります。

- 作業ファイル
- データ域およびメッセージ待ち行列
- プログラム
- メッセージ・ファイル
- コマンド
- 出力待ち行列

ファイルおよび出力待ち行列以外の大部分のオブジェクトは、 セキュリティー上の危険を伴うものではありません。 これらのオブジェクトには通常、少量のアプリケーション・データが含まれており、 多くの場合、プログラムの外側では容易に識別できない形式になっています。 ライブラリー表示コマンドを使用して、ライブラリーにあるすべてのオブジェクトの名前と説明をリストできます。たとえば、CONTRACTS ライブラリーの内容をリストするには、`DSPLIB LIB(CONTRACTS) OUTPUT(*PRINT)` を発行します。次に決定する必要があるのは、アプリケーション・ライブラリーとプログラム・ライブラリーに与える共通権限です。

アプリケーション・ライブラリーに対する共通権限の決定: 資源保護の場合、共通とは誰にでもシステムへのサインオンを認可することを意味します。共通権限があると、ユーザーは、他の特定のアクセス権がなくてもオブジェクトにアクセスできます。ライブラリーにある既存のオブジェクトへの共通権限を決定することに加えて、後でライブラリーに追加される新規オブジェクトへの共通権限も指定することができます。それには、作成権限 (CRTAUT) パラメーターを使用します。通常は、ライブラリー・オブジェクトに対する共通権限と、新規オブジェクトについてのライブラリー作成権限は同じにしてください。

作成権限 (QCRTAUT) システム値により、新規オブジェクトのシステム・レベルの共通権限が決まります。 IBM では、出荷時に QCRTAUT システム値に *CHANGE を指定します。 QCRTAUT は多数のシステム機能で変更されるので、この値を変更しないでください。アプリケーション・ライブラリーの CRTAUT に *SYSVAL を指定すると、 QCRTAUT システム値 (*CHANGE) が使用されます。

作業を単純にし、パフォーマンスを良くするために、できるだけたくさんの共通権限を使用してください。ライブラリーに対する共通権限のタイプを決めるには、以下の質問について検討してください。

- このライブラリーにある大部分の情報に対するアクセス権を、全社員に与える必要があるか。
- このライブラリーにある大部分の情報に対して、どのタイプのアクセス権を与える必要があるか。

大多数のユーザーと大部分の情報に関する決定を綿密に検討してください。 後で、例外を扱う方法について説明します。 資源保護の計画は、循環的なプロセスになることがよくあります。 特定のオブジェクトに関する要件を考慮した後で、共通権限に変更を加えなければならないことがあります。 まずオブジェクトとライブラリーの両方に対していくつかの共通権限と私用権限の組み合わせを試行し、 その中からセキュリティーとパフォーマンスの必要に合ったものを選択してください。

適切な権限の確保: 大部分のアプリケーション機能にとっては、オブジェクトに対する適切な権限は *CHANGE、ライブラリーに対する適切な権限は *USE です。しかし、プログラマーかアプリケーションの提供者に次のような質問をして、特定のアプリケーション機能では権限がさらに必要になるかどうか判別する必要があります。

- 処理中にライブラリーにあるファイルまたは他のオブジェクトを削除するかどうか。すべてのファイルを消去するかどうか。すべてのファイルにメンバーを追加するかどうか。オブジェクトの削除、ファイルの消去、またはファイル・メンバーの追加を行うには、オブジェクトに対する *ALL 権限が必要です。
- 処理中にライブラリーにファイルまたは他のオブジェクトを作成するかどうか。オブジェクトを作成するには、ライブラリーに対する *CHANGE 権限が必要です。

プログラム・ライブラリーへの共通権限の決定: アプリケーション・プログラムが、ファイルや他のオブジェクトとは別のライブラリーに保持されることがよくあります。アプリケーション用に別のライブラリーを使用する必要はありませんが、大勢のプログラマーがアプリケーション設計時にこの手法を使用します。アプリケーション用に別のプログラム・ライブラリーを使用する場合は、これらのライブラリーに対する共通権限を決定する必要があります。

ライブラリーとライブラリーにあるプログラムの両方に *USE 権限を使用すると、プログラムを十分に実行できますが、プログラム・ライブラリーには、追加権限が必要な他のオブジェクトも含まれている場合があります。プログラマーに以下の 2、3 の質問をしてください。

- プログラム間の通信のためにアプリケーションがデータ域またはメッセージ待ち行列を使用するかどうか。これらのものがプログラム・ライブラリーにあるかどうか。データ域やメッセージ待ち行列を処理するには、そのオブジェクトに対する *CHANGE 権限が必要です。
- 処理中に削除されるオブジェクト (データ域など) がプログラム・ライブラリーにあるかどうか。オブジェクトを削除するには、そのオブジェクトに対する *ALL 権限が必要です。
- 処理中に作成されるオブジェクト (データ域など) がプログラム・ライブラリーにあるかどうか。ライブラリー中に新規のオブジェクトを作成するには、そのライブラリーに対する *CHANGE 権限が必要です。

ライブラリー記述用紙の第 1 部と第 2 部の、 ライブラリー所有者と権限リストの列を除くすべての箇所に、 資源保護情報を記入してください。 その後で、ライブラリーとオブジェクトの所有権の決定を行えます。

注: ライブラリーに対するアクセス権を持つ熟練したプログラマーであれば、ライブラリーに対する権限が取り消された後でも、そのライブラリーにあるオブジェクトに対するアクセス権を保持できることがあります。ライブラリーにセキュリティーの必要性が大きいオブジェクトが含まれている場合、オブジェクトとライブラリーを制限して完全に保護されるようにしてください。

ライブラリーとオブジェクトの所有権の決定: アプリケーション・ライブラリーのセキュリティーの計画を立てた後、ライブラリーとオブジェクトの所有権を決めることができます。各オブジェクトには、作成時に所有者が割り当てられます。オブジェクトの所有者には、そのオブジェクトに対するすべての権限が自動的に付与されます。その中には、他の人にオブジェクトの使用を許可する権限、オブジェクトを変更する権限、およびオブジェクトを削除する権限が含まれます。機密保護担当者は、システム上のどのオブジェクトにもこれらの機能を実行できます。

システムでは、オブジェクト所有者のプロファイルを使用して、オブジェクトに対する権限を持つユーザーを追跡します。この機能はシステムで内部的に終了します。ユーザー・プロファイルに直接影響を与えることはありません。しかし、オブジェクト所有権の計画が適切でないと、一部のユーザー・プロファイルが大きくなり過ぎることがあります。

システムにオブジェクトが保管される場合は、所有プロファイルの名前も共に保管されます。この情報は、システムでそのオブジェクトが復元される場合に使用されます。復元されるオブジェクトの所有プロファイルがシステム上にないと、所有権がシステムから QDFTOWN という IBM 提供のプロファイルに転送されます。

推奨事項: 以下の推奨事項は多くの状態に当てはまりますが、すべての状態に当てはまるというわけではありません。推奨事項を検討したら、オブジェクトの所有権についてプログラマーかアプリケーションの提供者と相談してください。アプリケーションを購入した場合は、どのプロファイルがライブラリーやオブジェクトを所有するかを制御できないことがあります。この場合、所有権を変更できないようアプリケーションが設計されていることが考えられます。

- IBM 提供のプロファイル (QSECOFR や QPGMR など) をアプリケーション所有者として使用しないでください。これらのプロファイルは、IBM 提供のライブラリーにある多数のオブジェクトを所有しており、すでにかなり大きくなっています。
- 通常は、グループ・プロファイルにアプリケーションを所有させないでください。さらに低い権限を特別に割り当てない限り、グループ中のすべてのメンバーがグループ・プロファイルと同じ権限を持つことになります。そして、結果的にはアプリケーションに対する完全な権限をグループのメンバー全員に与えていることになってしまいます。
- アプリケーション制御の責任をさまざまな部門の管理者に委任する計画を立てる場合は、それらの管理者をすべてのアプリケーション・オブジェクトの所有者にすることもできます。しかし、アプリケーションの管理者が担当を変更することがあります。このような場合は、すべてのアプリケーション・オブジェクトの所有権を新しい管理者に転送します。
- 多くの場合には、アプリケーションごとにパスワードを *NONE に設定した特別な所有者プロファイルを作成するという手法が使用されます。システムでは、その所有プロファイルを使用してアプリケーションに関する権限が管理されます。機密保護担当者、またはこの権限を持つユーザーは、アプリケーションの実際の管理を実行するか、または特定のアプリケーションに対する *ALL 権限を持つ管理者に委任します。

アプリケーションを所有する必要のあるプロファイルを決めてください。 所有者プロファイルの情報を、個々のライブラリー記述用紙に記入してください。 次に、ユーザー・ライブラリーの所有権とアクセス権の決定を行えます。

ユーザー・ライブラリーの所有権とアクセスの決定: システムに IBM Query for iSeries ライセンス・プログラム、または別の意思決定支援プログラムがある場合、ユーザーには、自分が作成した照会プログラムを保管するためのライブラリーが必要です。通常は、ユーザー・プロファイル内の現行ライブラリーが、このライブラリーの役割を果たします。ユーザーがあるグループに所属している場合は、ユーザー・プロファイル内のフィールドを使用して、そのユーザーが作成したオブジェクトをユーザーかグループのどちらが所有するかを指定します。

ユーザーがオブジェクトを所有している場合は、そのオブジェクトを使用するためにグループ・メンバーにどの権限を付与するかを指定することができます。また、グループの権限が、1 次グループ権限か私用権限のどちらであるかを指定することもできます。 1 次グループ権限を使用する方が、システム・パフォーマンスが向上します。作成されたオブジェクトの所有者がグループである場合は、「作成されたオブジェクトに対するグループ権限」フィールドは使用されません。グループ・メンバーには、作成されたすべてのオブジェクトに対する *ALL 権限が自動的に付与されます。

ユーザー・ライブラリーを所有し、それに対するアクセス権を持つユーザーを決めてください。個別ユーザー・プロファイル用紙の「作成されたオブジェクトの所有者」フィールドと「作成されたオブジェクトに対するグループ権限」フィールドに、選択内容を入力してください。これで、オブジェクトのグループ化を始める準備が完了しました。

オブジェクトのグループ化

ライブラリーとオブジェクトの所有権の決定が終わったら、システム上のオブジェクトのグループ化を始めることができます。権限の管理を単純化するには、権限リストを使用して、同じ要件を持つオブジェクトをグループ化してください。その後、リスト上の個々のオブジェクトに対する権限を付与する代わりに、権限リストに対する共通権限、グループ・プロファイル権限、およびユーザー・プロファイル権限を付与できます。システムは権限リスト別に保護されるすべてのオブジェクトを同じ仕方で処理しますが、リスト全体に対するさまざまな権限をさまざまなユーザーに付与することができます。

権限リストを使用すると、オブジェクトの復元時に権限を再確立しやすくなります。権限リストを使用してオブジェクトを保護すると、復元プロセスの際にオブジェクトは自動的にリストにリンクされます。グループまたはユーザーに対して、権限リスト (*AUTLMGT) を管理する権限を付与することができます。権限リストを使用して管理を行うと、他のユーザーをリストに追加したりリストから除去したりでき、またそれらのユーザーに関する権限を変更できます。

推奨事項:

- 保護する必要があり、セキュリティー要件が同じであるオブジェクトの場合は、権限リストを使用してください。権限リストを使用すると、権限を個別に考慮するのではなくカテゴリーとして考慮できるようになります。また権限リストを使用すると、システム上のオブジェクトの復元や権限の監査を容易に行えます。
- 権限リスト、グループ権限、個別権限を組み合わせて、体系を込み入ったものにすることは避けてください。すべての方式を同時に使用するよりも、要件に最適の方式を選択してください。

また、権限リストの命名規則を命名規則用紙に追加する必要があります。 権限リスト用紙を作成したら、ライブラリー記述用紙に戻ってその情報を追加してください。 プログラマーかアプリケーションの提供者がすでに権限リストを作成している可能性があります。 それらを一緒に調べてください。

ライブラリー・セキュリティー

システム上のほとんどのオブジェクトは、ライブラリーに存在します。オブジェクトにアクセスするには、オブジェクト自体、およびオブジェクトが入っているライブラリーの両方に対する権限が必要です。オブジェクトの削除を含め、ほとんどの操作を行うには、(オブジェクトに必要な権限に加えて) オブジェクト・ライブラリーに対する *USE 権限を持っていれば十分です。新しいオブジェクトを作成するには、オブジェクト・ライブラリーに対する *ADD 権限が必要です。付録 D に、オブジェクト、およびオブジェクト・ライブラリーに対して、CL コマンドで必要となる権限が示されています。

ライブラリー・セキュリティーの使用は、単純なセキュリティー体系を保ちながら情報を保護するための手法の 1 つです。たとえば、アプリケーション・セットに対して機密情報を保護するには、以下のことを行えます。

- ライブラリーを使用して、特定のアプリケーション・グループ用のすべての機密ファイルを保管する。
- アプリケーションで使用される (ライブラリー内の) すべてのオブジェクトに対して、共通権限が十分あることを確認する (*USE または *CHANGE)。
- 共通権限をそのライブラリーだけに制限する (*EXCLUDE)。
- アプリケーションが必要とする場合、*USE または *ADD を使用してライブラリーへの権限を、選択されたグループまたは個々のユーザーに与える。

ライブラリー・セキュリティーは、情報を保護するための簡単で効果的な方法ですが、高いセキュリティーを必要とするデータには適さないかもしれません。重要性が高いオブジェクトは、ライブラリー・セキュリティーに頼るのではなく、個別に、または権限リストを使って保護するべきです。

ライブラリー・セキュリティーとライブラリー・リスト

ユーザーのライブラリー・リストにライブラリーが追加されると、ユーザーがライブラリーに対して持っている権限が、ライブラリー・リスト情報とともに保管されます。ライブラリーに対するユーザーの権限は、たとえばジョブの活動中に取り消されても、ジョブの実行全体で保持されます。オブジェクトにアクセスが要求され、*LIBL がそのオブジェクトに指定されている場合は、ライブラリー・リスト情報が使用されてライブラリーの権限が検査されます。修飾名が指定されると、ユーザーのライブラリー・リストに入っているライブラリーであっても、そのライブラリーの権限が検査されます。

注: ライブラリー・リストにライブラリーが追加される時点でユーザーが借用権限のもとで実行されている場合は、そのユーザーがもはや借用権限のもとで実行されなくなっても、ユーザーにはライブラリーに対する権限が残ります。これは、機密漏れの可能性があることを意味します。借用権限のもとで実行されているプログラムがユーザーのライブラリー・リストに追加したすべての項目は、借用権限のプログラムが終了する前に除去する必要があります。

さらに、修飾されたライブラリー名ではなくライブラリー・リストを使用する アプリケーションは機密漏れの可能性があることになります。ライブラリー・リストを処理するコマンドを許可されたユーザーは、異なるバージョンのプログラムを実行できる可能性があります。

ライブラリー所有者の判別:

アプリケーションの導入の計画を立てる際には、 まずアプリケーションごとにユーザー・プロファイルと導入値を決めなければなりません。

ユーザー・プロファイルとアプリケーションのインストール値の判別: 別のシステム上で作成したアプリケーションを導入する場合、その前に 1 つ以上のユーザー・プロファイルを作成しなければならないことがあります。システムにライブラリーをロードするには、アプリケーション・ライブラリーとオブジェクトを所有するユーザー・プロファイルがシステム上にすでに存在していなければなりません。ライブラリーごとに作成する必要のあるプロファイルと、それらのプロファイルに必要なパラメーターを、アプリケーションの導入用紙に記録してください。

必要な導入値を判別するには、プログラマーかアプリケーションの提供者に以下の質問をして、回答をアプリケーションの導入用紙に記録してください。

- アプリケーション・ライブラリーを所有するプロファイル。
- ライブラリーにあるオブジェクトを所有するプロファイル。
- ライブラリーに対する共通権限 (AUT)。
- 新しいオブジェクト (CRTAUT) への共通権限。
- ライブラリーにあるオブジェクトの共通権限。
- 所有者の権限を借用するプログラム (ある場合)。

プログラマーかアプリケーションの提供者が、 アプリケーションの権限リストを作成しているかどうか調べてください。 作成されている権限リストごとに権限リスト用紙を作成するか、 権限リストに関する情報をプログラマーに尋ねてください。 これで、導入値の変更を行う必要があるかどうかを決めることができます。

アプリケーションのインストール値の変更: アプリケーションの導入用紙の情報と、ライブラリー記述用紙に記録したライブラリーの資源保護計画を比較してください。両者が異なる場合は、アプリケーションの導入後にどのような変更を加えるか決める必要があります。

アプリケーション所有者の変更: プログラマーまたはアプリケーションの提供者が特別なプロファイルを作成して、アプリケーション・ライブラリーとオブジェクトを所有している場合は、命名規則に一致していなくてもそのプロファイルを使用することを考慮してください。

オブジェクトの所有権を転送すると長時間かかることがあるため、避けてください。 QSECOFR や QPGMR などの IBM 提供のグループ・プロファイルの 1 つがアプリケーションを所有する場合は、そのアプリケーションの導入後に別のプロファイルに所有権を転送する必要があります。プログラマーは、オブジェクトの所有権に関する変更を加えなくて済むように、アプリケーションを設計することがあります。制約事項の範囲内で作業しながら、セキュリティーの管理に関する独自の要件を満たしてください。しかし、QSECOFR などの IBM 提供のプロファイルがアプリケーションを所有している場合は、お客様自身とプログラマーまたはアプリケーションの提供者が相談して、所有権を変更する計画を開発する必要があります。理想的には、所有権を変更してからアプリケーションを導入してください。

共通権限の変更: オブジェクトを保管する際には、その共通権限も同時に保管することになります。システムにアプリケーション・ライブラリーを復元すると、ライブラリーとそのすべてのオブジェクトには、保管時に持っていたものと同じ共通権限があります。このことは、別のシステムにライブラリーを保管していた場合にも当てはまります。ライブラリーの CRTAUT 値 (新しいオブジェクトの共通権限) は、復元されるオブジェクトには影響しません。ライブラリーの CRTAUT 値に関係なく、保管時の共通権限を持ったまま復元されます。

ライブラリーとオブジェクトの共通権限に変更を加え、ライブラリー記述用紙での計画と一致させる必要があります。アプリケーションの導入計画が終了していることを確かめるためには、以下の作業が終わっていなければなりません。

- 最初のアプリケーションの導入用紙をすべて記入し終えている。完成していたら、その他のアプリケーションに戻って、それぞれの用紙を作成してください。
- すべての用紙を検討し、完成していることを確認する。用紙をコピーし、システムとライセンス・プログラムの導入が終了するまで、安全な場所に保管してください。

これで、これらの計画作業が完了しました。ユーザー・セキュリティーの設定に進むことができます。

ライブラリー記述ワークシート:

命名規則の記述が完了したら、次にシステム上のライブラリーについて記述しなければなりません。 ライブラリーは、システム上のオブジェクトを識別および編成します。

類似したファイルを 1 つのライブラリーにまとめると、 ユーザーは重要なアプリケーションとファイルにアクセスしやすくなります。 また、ユーザーの権限をカスタマイズして、 ユーザーがアクセスできる情報をライブラリー単位で制限することもできます。 各アプリケーションが使用する、 システム上のすべてのライブラリーについて記述してください。 複数のライブラリー記述用紙を作成しなければならない場合もあります。 ライブラリーに関する記述情報のみを記入してください。 ライブラリーについての資源保護を計画する場合は、 ライブラリー記述用紙のその他の項目についても記述を行います。 後で、ライブラリーに対する権限についての情報を加える必要があります。 ライブラリー記述用紙の残りの部分を完成する際の詳細については、 『アプリケーション・ライブラリーのセキュリティーの計画』を参照してください。続行する前に、命名規則ワークシートのライブラリーとファイルに関する部分、および各アプリケーション・ライブラリーのライブラリー記述ワークシートの記述情報を必ず完成させてください。

表 90. ライブラリー記述ワークシート

ライブラリー記述ワークシート	
作成者:	日付:

表 90. ライブラリー記述ワークシート (続き)

ライブラリー記述ワークシート	
指示: • 『ライブラリー所有権の判別』で、このワークシートに関して確認してください。 • このワークシートを使用して、メインのライブラリーについて説明し、それらの資源保護要件を定義します。 • システム上の主要なアプリケーション・ライブラリーごとに 1 枚ずつワークシートに記入します。	
ライブラリー名:	記述名 (テキスト):
このライブラリーの機能についての簡単な説明:	
ライブラリーに対するセキュリティーの目的の定義 (機密情報を含んでいるかどうかなど):	
ライブラリーへの共通権限:	
ライブラリー内のオブジェクトへの共通権限:	
新しいオブジェクト (CRTAUT) への共通権限:	
ライブラリー所有者:	

命名規則ワークシート:

システムがオブジェクトに名前を付ける方法が分かる場合は、 セキュリティーと問題の解決を計画および監視し、バックアップと回復を計画することができます。

ほとんどのアプリケーションには、ライブラリー、ファイル、 およびプログラムなどのオブジェクトに名前を割り当てる際の規則があります。 ソースの異なるアプリケーションには、おそらく、それぞれ固有の命名システムがあると考えられます。 アプリケーションとオブジェクトの命名規則はすべて、命名規則ワークシートに記録するようにしてください。 ライブラリーやファイルに名前を付ける際にアプリケーションが使用する規則をリストしてください。 プログラムやメニューなどの他の命名規則においては、ブランク行を使用することもできます。 ソースの異なるアプリケーションには、おそらく、それぞれ固有の命名規則があると考えられます。 各アプリケーションの命名規則を記述してください。 複数の命名規則ワークシートを作成しなければならない場合もあります。

表 91. 命名規則ワークシート

命名規則ワークシート		
作成者:		日付:
指示 • 情報は、このワークシートからシステムに直接入力する必要はありません。 • このワークシートを使用して、システム上のオブジェクトに名前を割り当てる方法について説明します。各オブジェクトの例を示します。		
オブジェクトのタイプ	**命名規則**	**例**
グループ・プロファイル		
ユーザー・プロファイル		
権限リスト		
ライブラリー		
ファイル		

表 91. 命名規則ワークシート (続き)

命名規則ワークシート		
カレンダー		
装置		
テープ		

アプリケーションのセキュリティーの計画

このトピックでは、貴社のアプリケーション・セキュリティー計画の作成の概要を示します。

アプリケーションに対して適切なセキュリティーを計画するには、次の情報が必要です。

- どのような情報をシステムに保管する計画を立てているか。
- その情報にアクセスする必要があるのは誰か。
- どのような種類のアクセスが必要なのか。その情報を変更する必要があるのか、それとも表示するだけなのか。

これらのアプリケーションの計画のトピックを進むにあたって、システムに保管しようとする情報について、最初の質問に対する答えが必要です。続くトピックの中では、誰がその情報を必要としており、どのようにその情報にアクセスするのかを決定します。アプリケーションの計画に関する情報をシステムに入力することはありません。しかし、これらの情報はユーザーのセキュリティーおよび資源保護を設定する際に必要になります。

アプリケーションとは

アプリケーションのセキュリティーの最初の計画のステップでは、システムで実行しようとしているアプリケーションについて記述する必要があります。アプリケーションとは、論理的に同じように分類される機能のグループのことです。通常、サーバーでは、次のような 2 つの異なったタイプのアプリケーションが実行されます。

- ビジネス・アプリケーション: 注文処理や在庫管理など、特定のビジネス機能を実行するために、購入または開発されるアプリケーション。
- 特殊アプリケーション: ビジネスのプロセスに固有でないさまざまな活動を実行するために、会社全体で使用されるアプリケーション。

どのような用紙が必要か

- アプリケーション記述用紙
- ライブラリー記述用紙
- 命名規則用紙

アプリケーションの記述

ここで、各ビジネス・アプリケーションについて、いくつかの一般的な情報を集める必要があります。下に説明されているようにして、アプリケーション記述用紙の適当なフィールドに、ご使用になるアプリケーションに関する情報を加えてください。この情報は、後でユーザー・グループとアプリケーションのセキュリティーを計画する際に役立ちます。

アプリケーション名および省略形

アプリケーションに短い名前と省略形を割り当て、用紙上での省略表現として、およびアプリケーションが使用する命名オブジェクトとして使用することができます。

記述情報
アプリケーションが行う業務について簡単に記述します。

1 次メニューおよびライブラリー
どのメニューがアプリケーションにアクセスするための 1 次メニューかを識別します。また、そのメニューが含まれているライブラリーを識別します。通常、特定のアプリケーションの機能を使用するための他のメニューは、1 次メニューから導かれます。ユーザーがシステムにサインオンした直後に、メインで使用するアプリケーションの 1 次メニューが表示されるようにすると、ユーザーにとって便利です。

初期プログラムおよびライブラリー
アプリケーションは、ユーザーのバックグラウンド情報を設定したり、セキュリティーのチェックを行ったりする初期プログラムを起動する場合があります。アプリケーションに初期プログラムや設定プログラムがある場合は、用紙にリストしてください。

アプリケーション・ライブラリー
通常、各アプリケーションには、そのファイルを保管するメインのライブラリーがあります。プログラム・ライブラリーや他のアプリケーションのライブラリーを含め、アプリケーションが使用するライブラリーをすべてここに含めてください。たとえば、JKL Toy Company の顧客オーダー・アプリケーションは、在庫のライブラリーを使用して、品目の残量と記述を確認します。各ライブラリーにアクセスする必要があるユーザーを判別するには、ライブラリーとアプリケーションとの間の関係を使用します。

アプリケーションに関する情報の検索

アプリケーションについてまだ分からない情報がある場合は、プログラマーかアプリケーションの提供者への相談が必要となる場合があります。システム上で実行するアプリケーションについて、この情報にアクセスできない場合は、次の方法を使用して、自分で情報を収集することができます。

- アプリケーションのユーザーに尋ねれば、おそらく 1 次メニューとライブラリーの名前を知ることができます。あるいは、自分でシステムにサインオンして確認することもできます。
- ユーザーがサインオンした後に、すぐそのアプリケーションが表示されるのであれば、そのユーザー・プロファイルの「初期プログラム」のフィールドを見てください。このフィールドには、アプリケーションの初期プログラムが含まれています。 DSPUSRPRF コマンドを使用して、初期プログラムを表示することができます。
- システム上のすべてのライブラリーの名前と記述をリストすることができます。 DSPOBJD *ALL *LIB を使用してください。システム上のすべてのライブラリーが表示されます。
- ユーザーがアプリケーションを実行している間、活動ジョブを監視することができます。対話式ジョブに関する詳細な情報を表示するには、中級操作援助レベルで活動ジョブの処理 (WRKACTJOB) コマンドを使用してください。ジョブを表示してライブラリー・リストとそのオブジェクト・ロックを調べ、使用されているライブラリーを見つけてください。
- ユーザー・ジョブの処理 (WRKUSRJOB) コマンドを使用して、アプリケーション内のバッチ・ジョブを表示することができます。

アプリケーションのセキュリティーを計画するために必要なすべての情報を確実に収集するには、 処理を続ける前に以下の作業を完了する必要があります。

- 各ビジネス・アプリケーションについて、アプリケーション記述用紙を完成させる。セキュリティー要件に関する部分を除いて、用紙のすべての項目を記入してください。セキュリティー要件の部分は、アプリケーションの資源保護を計画する際に使用します。この点については、『資源保護』というトピックで扱います。

- 該当する場合は、システム上の各特殊アプリケーションについて、アプリケーション記述用紙を作成する。用紙を使用すると、アプリケーションへのアクセスの提供方法を判別する際に便利です。

注: IBM Query for iSeries など、IBM が提供している特殊アプリケーションのためのアプリケーション記述用紙の作成はオプションです。これらのアプリケーションが使用する、ライブラリーへのアクセスについては、特別な計画は必要ありません。ただし、これらのアプリケーションについて情報を収集し、用紙を作成すると役立つ場合があります。

アプリケーション図の描画

アプリケーション記述用紙およびライブラリー記述用紙を作成する際に、アプリケーションとライブラリーの関係を示す図を描くと便利です。図は、ユーザー・グループを計画する場合にも、資源保護を計画する場合にも便利です。

アプリケーションとライブラリーについての情報を収集することは、必要な多くのセキュリティー上の決定を下す上で役立ちます。システムとアプリケーションに関する知識を深める機会として、この情報に精通してください。必要としているアプリケーションの情報を確実に収集するには、次のようにします。

- システム上の各ビジネス・アプリケーションについて、アプリケーション記述用紙を完成させる。
- システム上の各特殊アプリケーションについて、アプリケーション記述用紙を作成する。
- 命名規則用紙のライブラリーとファイルに関連する部分を記入する。
- 各アプリケーション・ライブラリーについて、ライブラリー記述用紙を作成する。
- アプリケーションとライブラリーの間の関係を図に描画する。

これらの用紙が完成したら、全体的なセキュリティー戦略の計画を開始することができます。

大きなプロファイルを避けるためのアプリケーション計画

パフォーマンスとセキュリティーに及ぼす影響が懸念されるので、IBM では、プロファイルが大きくなり過ぎないようにするため以下のことを強くお勧めします。

- 1 つのプロファイルに、システム上のすべてのものを所有させない。

  アプリケーションを所有する特殊ユーザー・プロファイルを作成してください。 1 つのアプリケーションに固有な所有者プロファイルがあれば、アプリケーションの回復、および、システム間でのアプリケーションの移動が容易になります。また、私用権限についての情報はいくつかのプロファイル内に渡って存在しており、これによってパフォーマンスが向上します。いくつかの所有者プロファイルを使用することで、オブジェクトが多過ぎるためにプロファイルが大きくなり過ぎるのを避けることができます。また、所有者プロファイルによって、ユーザーは不必要な権限を提供する、より強力なプロファイルではなく、所有者プロファイルの権限を借用することができます。
- QSECOFR や QPGMR のような IBM 提供のユーザー・プロファイルにアプリケーションを所有させることは避ける。

  これらのプロファイルは大量の IBM 提供オブジェクトを所有しているので、管理が困難になります。IBM 提供のユーザー・プロファイルが所有するアプリケーションを 1 つのシステムから他へ移動したときに、セキュリティーの問題が発生することがあります。また、IBM 提供のユーザー・プロファイルで所有されているアプリケーションは、 CHKOBJITG や WRKOBJOWN のようなコマンドのパフォーマンスに影響を与えることもあります。
- 権限リストを使用して、オブジェクトを保護する。

複数のユーザーの多数のオブジェクトに私用権限を与える場合には、権限リストを使用してオブジェクトを保護することを考慮してください。権限リストでは、それぞれのオブジェクトごとに 1 つの私用権限項目ではなく、ユーザーのプロファイルの権限リストごとに 1 つの私用権限項目が使用されます。オブジェクト所有者のプロファイルでは、権限リストは、私用権限が与えられたユーザー数を乗じた、全オブジェクトの認可オブジェクト項目ではなく、権限リストに対し権限を与えられるすべてのユーザーの認可オブジェクト項目が使用されます。

オブジェクト権限の計画:

ここでは、オブジェクト権限を計画する際に役立つ情報を提供します。

機密保護管理者としての重要な仕事は、システムのユーザーに不満を感じさせないで、導入先の情報資産を保護することです。システムをブラウズしたり、無許可の変更を行ったりする権限をユーザーに与えずに、ユーザーが自分のジョブを実行するための十分な権限を持つようにする必要があります。

i5/OS オペレーティング・システムは、統合されたオブジェクト・セキュリティーを提供します。ユーザーは、システムによって提供されるインターフェースを使用してオブジェクトにアクセスします。たとえば、データベース・ファイルをアクセスしたい場合は、データベース・ファイルをアクセスするコマンドやプログラムを使用する必要があります。メッセージ待ち行列やジョブ・ログをアクセスするコマンドは使用できません。

ユーザーがシステム・インターフェースを使用してオブジェクトをアクセスするたびに、システムは、そのインターフェースに必要なオブジェクトに対する権限をユーザーが持っているかどうかを調べます。オブジェクト権限は、システムの資産を保護するための強力かつ柔軟なツールです。機密保護管理者としての重要な仕事は、管理と保守が可能な効果的なオブジェクト・セキュリティー方式をセットアップすることです。

オブジェクト権限の拡張

オブジェクトへのアクセスを試みた場合は常に、オペレーティング・システムがそのオブジェクトに対するユーザー権限を検査します。ただし、システムのセキュリティー・レベル (QSECURITY システム値) を 10 または 20 に設定すると、すべてのユーザー・プロファイルが *ALLOBJ 特殊権限を持つようになるため、すべてのユーザーは自動的にすべてのオブジェクトをアクセスする権限を入手することになります。

オブジェクト権限に関するヒント: オブジェクト・セキュリティーを使用しているかどうか分からない場合は、QSECURITY (セキュリティー・レベル) システム値を 調べてください。QSECURITY が 10 または 20 であれば、ユーザー・セキュリティーを使用していません。セキュリティー・レベルを 30 以上に変更するためには、その前に計画と準備が必要になります。それを行わないと、ユーザーが必要な情報にアクセスできなくなる可能性があります。

システム・コマンドとプログラムに対するオブジェクト権限

次に、権限を IBM 提供オブジェクトに制限する場合の推奨事項をいくつか示します。

- システム上に複数の各国語がある場合は、システムには、複数のシステム (QSYS) ライブラリーがあります。システムでは、各国語ごとに QSYSxxxx ライブラリーがあります。オブジェクト権限を使用してシステム・コマンドへのアクセスを制御する場合は、QSYS ライブラリー およびシステム上のすべての QSYSxxx ライブラリーのコマンドを保護することを忘れないでください。
- System/38™ ライブラリーが、制限したいコマンドと同等の機能を持つコマンドを提供することがあります。 QSYS38 ライブラリー内の同等コマンドを制限するようにしてください。
- System/36™ 環境の場合は、追加プログラムの制限を必要とする場合があります。たとえば、QY2FTML プログラム は System/36 ファイル転送を提供します。

オブジェクトのグループ化

ライブラリーとオブジェクトの所有権の決定が終わったら、システム上のオブジェクトのグループ化を始めることができます。権限の管理を単純化するには、権限リストを使用して、同じ要件を持つオブジェクトをグループ化してください。その後、リスト上の個々のオブジェクトに対する権限を付与する代わりに、権限リストに対する共通権限、グループ・プロファイル権限、およびユーザー・プロファイル権限を付与できます。システムは権限リスト別に保護されるすべてのオブジェクトを同じ仕方で処理しますが、リスト全体に対するさまざまな権限をさまざまなユーザーに付与することができます。

権限リストを使用すると、オブジェクトの復元時に権限を再確立しやすくなります。権限リストを使用してオブジェクトを保護すると、復元プロセスの際にオブジェクトは自動的にリストにリンクされます。グループまたはユーザーに対して、権限リスト (*AUTLMGT) を管理する権限を付与することができます。権限リストを使用して管理を行うと、他のユーザーをリストに追加したりリストから除去したりでき、またそれらのユーザーに関する権限を変更できます。

推奨事項:

- 保護する必要があり、セキュリティー要件が同じであるオブジェクトの場合は、権限リストを使用してください。権限リストを使用すると、権限を個別に考慮するのではなくカテゴリーとして考慮できるようになります。また権限リストを使用すると、システム上のオブジェクトの復元や権限の監査を容易に行えます。
- 権限リスト、グループ権限、個別権限を組み合わせて、体系を込み入ったものにすることは避けてください。すべての方式を同時に使用するよりも、要件に最適の方式を選択してください。

また、権限リストの命名規則を命名規則用紙に追加する必要があります。 権限リスト用紙を作成したら、ライブラリー記述用紙に戻ってその情報を追加してください。 プログラマーかアプリケーションの提供者がすでに権限リストを作成している可能性があります。 それらを一緒に調べてください。

情報にアクセスする方法の定義

権限とは、オブジェクトに対して許可されるアクセスのタイプです。操作に応じて、異なるタイプの権限が必要になります。注: ある環境では、オブジェクトに関連する権限は、オブジェクトのアクセス・モードと呼ばれます。オブジェクトに対する権限は、次の 3 つのカテゴリーに分類できます。

1. オブジェクト権限は、オブジェクト全体に対して実行できる操作を定義します。
2. データ権限は、オブジェクトの内容に対して実行できる操作を定義します。
3. フィールド権限は、データ・フィールドに対して実行できる操作を定義します。

以下の表に、使用可能な権限のタイプと、それらを使用する例を示します。多くの場合、オブジェクトにアクセスするには、 オブジェクト権限、データ権限、フィールド権限の組み合わせが必要です。特定の機能を行うために 必要な権限については、付録 D を参照してください。

権限タイプの説明

権限	名前	使用できる機能
オブジェクト権限		
*OBJOPR	オブジェクト操作可能	オブジェクト記述の参照。ユーザーのデータ権限によって判別されたオブジェクトを使用してください。

権限タイプの説明

権限	名前	使用できる機能
*OBJMGT	オブジェクト管理	オブジェクトに対するセキュリティーの指定。オブジェクトの移動または名前変更。*OBJALTER および *OBJREF に対して定義されたすべての機能。
*OBJEXIST	オブジェクト存在	オブジェクトの削除。オブジェクトの記憶域の解放。オブジェクト 1 の保管/復元操作の実行。オブジェクト所有権の転送。
*OBJALTER	オブジェクト変更	データベース・ファイルのメンバーの追加、消去、初期化、および再編成。データベース・ファイルの属性の変更と追加 (トリガーの追加と除去)。SQL パッケージの属性の変更。
*OBJREF	オブジェクト参照	データベース・ファイルを、参照制約において親として指定します。たとえば、顧客レコードがまず CUSMAS ファイル内に存在していなければその顧客のオーダーを CUSORD ファイルに追加できないという規則を定義するとします。この規則を定義するには、CUSMAS ファイルに対して *OBJREF 権限が必要です。
*AUTLMGT	権限リスト管理	権限リスト 2 上でのユーザーとその権限の追加および除去。
データ権限		
*READ	読み取り	オブジェクトの内容を表示。たとえば、ファイル中のレコードの表示など。
*ADD	追加	オブジェクトに項目を追加。たとえば、メッセージ待ち行列にメッセージを追加したり、ファイルへレコードを追加するなど。
*UPD	更新	オブジェクト中で項目を変更。たとえば、ファイル内でのレコード変更など。
*DLT	削除	オブジェクトから項目を削除。たとえば、メッセージ待ち行列からのメッセージの除去、またはファイルからのレコードの削除など。
*EXECUTE	実行	プログラム、サービス・プログラム、または SQL パッケージを実行。ライブラリーまたはディレクトリー内でのオブジェクトの探索。
フィールド権限		

権限タイプの説明

権限	名前	使用できる機能
*Mgt	管理	フィールドに対するセキュリティーの指定。
*Alter	更新	フィールドの属性の変更。
*Ref	参照情報	フィールドを親キーの一部として参照制約に指定する。
*Read	読み取り	フィールドの内容にアクセスする。たとえば、フィールドの内容を表示する。
*Add	追加	データに項目を追加する。たとえば、情報を特定のフィールドに追加する。
*Update	更新	フィールドにある既存の項目の内容を変更する。
[1] ユーザーがシステム保管 (*SAVSYS) 特殊権限を持っている場合、オブジェクト上での保管/復元操作の実行にオブジェクト存在権限は必要ありません。 [2] 詳しくは、『権限リスト管理』を参照してください。		

一般に使用される権限

オブジェクト権限とデータ権限の特定のセットは、通常オブジェクト上で操作を実行する場合に必要とされます。オブジェクトに必要な権限を個々に定義する代わりに、これらのシステム定義の権限セット (*ALL、*CHANGE、*USE) を指定できます。*EXCLUDE 権限を持っているということは、権限がないこととは異なります。 *EXCLUDE 権限は、オブジェクトへのアクセスを否定します。権限がないということは、オブジェクトに定義されている共通権限を使用することを意味します。以下の表は、オブジェクト権限のコマンドや画面を用いて使用可能な、システム定義の権限を示します。

システム定義の権限

権限	*ALL	*CHANGE	*USE	*EXECUTE
オブジェクト権限				
*OBJOPR	○	○	○	
*OBJMGT	○			
*OBJEXIST	○			
*OBJALTER	○			
*OBJREF	○			
データ権限				
*READ	○	○	○	
*ADD	○	○		
*UPD	○	○		
*DLT	○	○		
*EXECUTE	○	○	○	

以下の表は、WRKAUT および CHGAUT コマンドを用いて使用可能な、追加のシステム定義権限を示します。

システム定義の権限

権限	*RWX	*RW	*RX	*R	*WX	*W
オブジェクト権限						
*OBJOPR	○	○	○	○	○	○
*OBJMGT						
*OBJEXIST						
*OBJALTER						
*OBJREF						
データ権限						
*READ	○	○	○	○		
*ADD	○	○			○	○
*UPD	○	○			○	○
*DLT	○	○			○	○
*EXECUTE	○		○		○	

LAN サーバー・ライセンス・プログラムは、アクセス制御リストを使用して権限を管理します。ユーザーの権限は、許可と呼ばれます。以下の表は、LAN サーバー許可がどのようにオブジェクトおよびデータ権限に対応するかを示します。

LAN サーバー許可

権限	LAN サーバー許可
*EXCLUDE	なし
オブジェクト権限	
*OBJOPR	注 1 を参照
*OBJMGT	許可
*OBJEXIST	作成、削除
*OBJALTER	属性
*OBJREF	等価ではない
データ権限	
*READ	読み取り
*ADD	作成
*UPD	書き込み
*DLT	削除
*EXECUTE	実行
[1] アクセス制御リスト内のユーザーに NONE を指定しない限り、 そのユーザーには暗黙的に *OBJOPR が与えられます。	

アクセス対象となる情報の定義

システム上の個々のオブジェクトに関する資源保護を定義できます。また、ライブラリー・セキュリティーまたは権限リストのいずれかを使用して、オブジェクトのグループ用にセキュリティーを定義することもできます。

- **ライブラリー・セキュリティー:**

システム上のほとんどのオブジェクトは、ライブラリーに存在します。オブジェクトにアクセスするには、オブジェクト自体、およびオブジェクトが入っているライブラリーの両方に対する権限が必要です。オブジェクトの削除を含め、ほとんどの操作を行うには、(オブジェクトに必要な権限に加えて) オブジェクト・ライブラリーに対する *USE 権限を持っていれば十分です。新しいオブジェクトを作成するには、オブジェクト・ライブラリーに対する *ADD 権限が必要です。付録 D に、オブジェクト、およびオブジェクト・ライブラリーに対して、CL コマンドで必要となる権限が示されています。

ライブラリー・セキュリティーの使用は、単純なセキュリティー体系を保ちながら情報を保護するための手法の 1 つです。たとえば、アプリケーション・セットに対して機密情報を保護するには、以下のことを行えます。

- ライブラリーを使用して、特定のアプリケーション・グループ用のすべての機密ファイルを保管する。
- アプリケーションで使用される (ライブラリー内の) すべてのオブジェクトに対して、共通権限が十分あることを確認する (*USE または *CHANGE)。
- 共通権限をそのライブラリーだけに制限する (*EXCLUDE)。
- ライブラリーへの権限を、選択されたグループまたは個々のユーザーに与える (アプリケーションが必要とする場合、*USE または *ADD)。

ライブラリー・セキュリティーは、情報を保護するための簡単で効果的な方法ですが、高いセキュリティーを必要とするデータには適さないかもしれません。重要性が高いオブジェクトは、ライブラリー・セキュリティーに頼るのではなく、個別に、または権限リストを使って保護するべきです。

- **ライブラリー・セキュリティーとライブラリー・リスト:**

  ユーザーのライブラリー・リストにライブラリーが追加されると、ユーザーがライブラリーに対して持っている権限が、ライブラリー・リスト情報とともに保管されます。ライブラリーに対するユーザーの権限は、たとえばジョブの活動中に取り消されても、ジョブの実行全体で保持されます。

  オブジェクトにアクセスが要求され、*LIBL がそのオブジェクトに指定されている場合は、ライブラリー・リスト情報が使用されてライブラリーの権限が検査されます。修飾名が指定されると、ユーザーのライブラリー・リストに入っているライブラリーであっても、そのライブラリーの権限が検査されます。

  ライブラリー・リストにライブラリーが追加される時点でユーザーが借用権限のもとで実行されている場合は、そのユーザーがもはや借用権限のもとで実行されなくなっても、ユーザーにはライブラリーに対する権限が残ります。これは、機密漏れの可能性があることを意味します。借用権限のもとで実行されているプログラムがユーザーのライブラリー・リストに追加したすべての項目は、借用権限のプログラムが終了する前に除去する必要があります。さらに、修飾されたライブラリー名ではなくライブラリー・リストを使用するアプリケーションは機密漏れの可能性があることになります。ライブラリー・リストを処理するコマンドを許可されたユーザーは、異なるバージョンのプログラムを実行できる可能性があります。詳しくは、『ライブラリー・リスト』を参照してください。

- **フィールド権限:**

  データベース・ファイルに対してフィールド権限がサポートされるようになりました。サポートされる権限は、参照 (Reference) および更新 (Update) です。これらの権限だけが、SQL ステートメントの GRANT および REVOKE によって管理できます。 オブジェクト権限表示 (DSPOBJAUT) コマンドおよびオブジェクト権限編集 (EDTOBJAUT) コマンドによって、これらの権限を表示できます。EDTOBJAUT コマンドを使っても、フィールド権限は表示できるだけで、編集することはできません。

  フィールド権限の変更には、以下のことが含まれます。

– 私用権限印刷 (PRTPVTAUT) コマンドに、ファイルがいつフィールド権限を持つかを示す新しいフィールドがあります。
– オブジェクト権限表示 (DSPOBJAUT) コマンドには、オブジェクト権限、フィールド権限、またはすべての権限を表示できる、新しい権限タイプ・パラメーターが加わりました。オブジェクト・タイプが *FILE でない場合、オブジェクト権限しか表示できません。
– オブジェクトに許可されたユーザーのリスト (QSYLUSRA) API によって提供される情報に、あるフィールドがフィールド権限を持つかどうかの指示が含まれるようになりました。
– ユーザー権限認可 (GRTUSRAUT) コマンドでは、ユーザーのフィールド権限は認可しません。
– GRTOBJAUT コマンドを使用して参照オブジェクトで認可が実行され、両方のオブジェクトで (認可されるものと参照されるもの) がデータベース・ファイルである場合は、フィールド名が一致する限りすべてのフィールド権限が許可されます。
– データベース・ファイルに対するユーザーの権限が除去された場合は、そのユーザーのフィールド権限もすべて除去されます。

- **セキュリティーと System/38™ 環境:**

  System/38 環境およびタイプ CLP38 の CL プログラムは、セキュリティーに関して問題となる可能性があります。ライブラリー修飾のないコマンドが、 System/38 のコマンド入力画面に入力されるか、CLP38 CL プログラムから呼び出されると、そのコマンドの探索はまず、ライブラリー QUSER38 (存在する場合) に対して行われます。次に、ライブラリー QSYS38 が探索されます。プログラマーなどの熟練したユーザーは、これらのライブラリーのどちらかに別の CL コマンドを入れることにより、ライブラリー・リストのライブラリーにあるコマンドを使用する代わりに、そのコマンドを使用させるようにすることが可能です。

  ライブラリー QUSER38 は、オペレーティング・システムとともに出荷されませんが、ライブラリーを作成する権限があるユーザーであれば、このライブラリーを作成することができます。 System/38 環境の詳細については、「System/38 Environment Programming」資料を参照してください。

  System/38 環境での推奨事項: System/38 環境とタイプ CLP38 の CL プログラムに対してシステムを保護するには、次のようにしてください。
  – QSYS38 ライブラリーの共通権限を検査し、それが *ALL または *CHANGE になっている場合は、*USE に変更する。
  – QUSER38 ライブラリーの共通権限を検査し、それが *ALL または *CHANGE になっている場合は、*USE に変更する。
  – QUSER38 と QSYS38 が存在しない場合は、それらを作成し、それらに共通 *USE 認可を設定する。こうすることで、後に誰かがそれを作成し、それに対する過剰な権限を自分自身または共通ユーザーに与えることを防ぐことができます。

- **ディレクトリー・セキュリティー:**

  ディレクトリー内のオブジェクトをアクセスするときは、オブジェクトが入ったパス内のすべてのディレクトリーに対する権限を持っていなければなりません。さらに、オブジェクトに対して、要求した操作を実行するのに必要な権限も持っていなければなりません。

  ライブラリー・セキュリティーを使用するのと同じ方法で、ディレクトリー・セキュリティーを使用できます。ディレクトリーへのアクセスを制限し、ディレクトリー内のオブジェクトに共通権限を使用します。オブジェクトに定義される私用権限の数を制限すると、権限検査処理のパフォーマンスが向上します。

- **権限リスト・セキュリティー:**

権限リストを使用して、セキュリティー要件の類似したオブジェクトをグループ化することができます。権限リスト内には、概念として、ユーザーのリストおよびリストによって保護されているオブジェクトに対してそのユーザーが持っている権限が入っています。それぞれのユーザーは、リストが保護するオブジェクトのセットに対して、異なる権限を持つことが可能です。権限リストに対してユーザー権限を与える場合、オペレーティング・システムは実際には、権限リストに対するそのユーザーの私用権限を与えます。

また、権限リストを使用して、リスト上のオブジェクトに対する共通権限を定義することもできます。オブジェクトに対する共通権限が *AUTL に設定される場合、オブジェクトは共通権限を権限リストから得ます。

権限リスト・オブジェクトは、システムによって管理ツールとして使用されます。これには、実際に、権限リストによって保護されたすべてのオブジェクトのリストが含まれます。この情報は、権限リスト・オブジェクトの参照または編集を行うための画面を構築する場合に使用されます。

ユーザー・プロファイルまたは他の権限リストを保護するために権限リストを使用することはできません。1 つのオブジェクトに対しては 1 つの権限リストだけを指定できます。

オブジェクトの権限リストを追加または削除できるのは、オブジェクトの所有者、全オブジェクト (*ALLOBJ) 特殊権限を持つユーザー、またはオブジェクトに対してすべての (*ALL) 権限を持つユーザーだけです。システム・ライブラリー (QSYS) 中のオブジェクトについては、権限リストを使用して保護することができます。しかし、オブジェクトの保護を行う権限リストの名前は、オブジェクトとともに保管されます。

オペレーティング・システムの新しいリリースを導入すると、 QSYS ライブラリーにあるすべてのオブジェクトが置き換えられる場合があります。この場合、オブジェクトと権限リストの関係は失われます。権限リストの使用例は、『権限リストの計画』のトピックを参照してください。

権限リスト管理: 権限リスト管理 (*AUTLMGT) と呼ばれる特殊な操作の権限を権限リストに対し認可することができます。*AUTLMGT 権限のあるユーザーは、権限リストに対するユーザーの権限の追加および除去、およびそれらのユーザーの権限の変更を行うことができます。*AUTLMGT 権限自体は、リストを使用した新しいオブジェクトのセキュリティーやリストからのオブジェクトの除去を行う権限を与えません。

*AUTLMGT 権限を持つユーザーは、他のユーザーに自分と同等かまたはより少ない権限を与えることしかできません。たとえば、USERA が権限リスト CPLIST1 に対して *CHANGE 権限と *AUTLMGT 権限を 持っているとします。USERA は、USERB を CPLIST1 に追加して、USERB に *CHANGE 権限またはより少ない権限を与えることができます。USERA は、*ALL 権限を持たないので、 CPLIST1 に対する *ALL 権限を USERB に与えることはできません。

*AUTLMGT 権限を持つユーザーは、除去するユーザー・プロファイル名と同じかより大きい権限をリストに対して持っている場合にのみ、ユーザーの権限を除去できます。USERC が CPLIST1 に対して *ALL 権限を持っている場合、 USERA は *CHANGE および *AUTLMGT しか持っていないので、USERC をリストから除去することはできません。

IBM 提供のオブジェクトを保護するための権限リストの使用: 権限リストを使用して、IBM 提供のオブジェクトをセキュリティーできます。たとえば、あるユーザーに対して一連のコマンドの使用を制限する場合があるかもしれません。 QUSRSYS および QGPL ライブラリーを除く、IBM 提供のライブラリー内のオブジェクトは、オペレーティング・システムの新しいリリースを導入すると置き換えられます。この場合、IBM 提供のライブラリーのオブジェクトと権限リストとの間の連係は失われます。また、権限リストが QSYS 内のオブジェクトをセキュリティーしているときに完全なシステム復元が必要

な場合は、QSYS 内のオブジェクトと権限リストとの間の連係も失われます。新規リリースを導入した後、またはシステムを復元した後は、EDTOBJAUT または GRTOBJAUT コマンドを使用して、IBM 提供のオブジェクトと権限リストとの連係を確立してください。

レッドブック「Implementation Guide for AS/400Security and Auditing」に、権限リストを復元した後で権限リストをオブジェクトに接続するのに使用する、ALLAUTL および FIXAUTL といったサンプル・プログラムが記載されています。

ライブラリーにある新規オブジェクトに対する権限

すべてのライブラリーには、CRTAUT (権限作成) と呼ばれるパラメーターがあります。このパラメーターにより、そのライブラリー内で作成される任意の新しいオブジェクトに対するデフォルトの共通権限が決定されます。オブジェクト作成時は、作成コマンドの AUT パラメーターによってオブジェクトに対する共通権限が決定されます。作成コマンドの AUT 値がデフォルト値 *LIBCRTAUT である場合、そのオブジェクトに対する共通権限はそのライブラリーに対する CRTAUT 値に設定 されます。

たとえば、ライブラリー CUSTLIB に *USE の CRTAUT 値があるとします。以下の両方のコマンドで、共通権限 *USE がある DTA1 というデータ域が作成されます。

- AUT パラメーターを次のように指定します。 `CRTDTAARA DTAARA(CUSTLIB/DTA1) + TYPE(*CHAR) AUT(*LIBCRTAUT)`
- AUT パラメーターにデフォルト値を許可します。*LIBCRTAUT がデフォルトです。 `CRTDTAARA DTAARA(CUSTLIB/DTA1) + TYPE(*CHAR)`

ライブラリーのデフォルト値 CRTAUT は *SYSVAL です。AUT(*LIBCRTAUT) を 使用してライブラリー内に作成されたすべての新しいオブジェクトは、 共通権限が QCRTAUT システム値の値に設定されます。QCRTAUT システム値は、 *CHANGE で出荷されます。 たとえば、ITEMLIB ライブラリーに *SYSVAL の CRTAUT 値があるとします。 このコマンドで、変更の共通権限を使用して DTA2 データ域を作成します。`CRTDTAARA DTAARA(ITEMLIB/DTA2) + TYPE(*CHAR) AUT(*LIBCRTAUT)`

注: QSYS を含め、いくつかの IBM 提供ライブラリーには、 *SYSVAL を指定した CRTAUT 値が入っています。QCRTAUT を *CHANGE 以外に変更すると、問題が発生する場合があります。たとえば、QSYS ライブラリーに装置が作成されたとします。装置を作成する場合のデフォルト値は、AUT(*LIBCRTAUT) です。

QSYS ライブラリーの CRTAUT 値は *SYSVAL です。QCRTAUT が *USE または *EXCLUDE に設定された場合、共通権限では、新しい装置へのサインオンをすることはできません。

ライブラリーの CRTAUT 値は、権限リスト名に設定することもできます。AUT(*LIBCRTAUT) のあるライブラリー内で作成されたすべての新しいオブジェクトの保護は、権限リストで行います。オブジェクトに対する共通権限は、*AUTL に設定されます。

ライブラリーの CRTAUT 値は、移動 (MOVOBJ)、オブジェクト複製 (CRTDUPOBJ)、またはライブラリーへのオブジェクトの復元を行う場合は使用されません。既存オブジェクトの共通権限が使用されます。

作成コマンド上で REPLACE (*YES) パラメーターを使用すると、既存オブジェクトの権限が、ライブラリーの CRTAUT 値の代わりに使用されます。

作成権限 (CRTAUT) のリスク: アプリケーションがアプリケーションの処理時に作成された新しいオブジェクトに対するデフォルト権限を使用する場合は、だれがライブラリー記述を変更する権限を持つのかを制

御しておくべきです。アプリケーション・ライブラリーに対する CRTAUT 権限を変更すると、ライブラリー内で作成された新しいオブジェクトへの許可されないアクセスが許されてしまうおそれがあります。

ディレクトリーにある新規オブジェクトに対する権限

CRTDIR、MD、または MKDIR コマンドを使用してディレクトリー内に新しいオブジェクトを作成するときは、そのオブジェクトに対して一般ユーザーが受けるデータ権限およびオブジェクト権限を指定します。*INDIR オプションを使用する場合、作成されたディレクトリーの権限に対する権限は、それが作成されているディレクトリーから決定されます。それ以外の場合は、特定の権限を指定できます。

所有者の権限を借用するオブジェクト

ユーザーは、状況に応じて、オブジェクトまたはアプリケーションに対して異なる権限を必要とする場合があります。たとえば、カスタマー・ファイルの情報を変更する機能を提供するアプリケーション・プログラムを使用している場合、そのユーザーはそのような変更を行うことができます。しかし、SQL などの意思決定サポート・ツールを使用している場合は、その同じユーザーが顧客情報を表示することはできても、その情報の変更は許可すべきではありません。

この状況の解決として、 1) 顧客情報に対する *USE 権限をユーザーに与えてファイル照会を可能にし、2) 顧客保守プログラムの借用権限を使用して、ユーザーによるファイル変更を可能にすることができます。

オブジェクトが所有者の権限を使用する場合、これを借用権限といいます。タイプ *PGM、*SRVPGM、*SQLPKG、および Java プログラムのオブジェクトが権限を借用できます。プログラムを作成する場合は、CRTxxxPGM コマンドのユーザー・プロファイル (USRPRF) パラメーターを指定します。このパラメーターにより、そのプログラムを実行しているユーザーの権限に加えて、プログラムの所有者の権限を借用するかどうかが決定されます。

以下の事柄は、借用権限に適用されます。

- 借用権限は、ユーザーのための他のすべての権限に追加されます。
- 借用権限は、ユーザー、ユーザー・グループ、または一般ユーザーがオブジェクトに対して持っている権限が、要求操作での使用に適切でない場合にのみ検査されます。
- 所有者プロファイルにある特殊権限 (*ALLOBJ など) が使用されます。
- 所有者プロファイルがグループ・プロファイルのメンバーである場合、そのグループの権限は、借用権限としては使用されません。
- 共通権限は、借用権限には使用されません。たとえば、USER1 はプログラム LSTCUST を実行しますが、 CUSTMST ファイルに対する *USE 権限を必要とします。
  - CUSTMST ファイルに対する共通権限は *USE です。
  - USER1 の権限は *EXCLUDE です。
  - USER2 は、LSTCUST プログラムを所有しますが、これは所有者権限を借用します。
  - USER2 は、CUSTMST ファイルを所有していないので、そのファイルに対する私用権限がありません。
  - USER2 が CUSTMST ファイルにアクセスするのに十分な共通権限がある場合でも、USER1 はアクセスできません。所有者権限、1 次グループ権限、および私用権限が、借用権限に使用されます。
  - 借用されるのは権限だけです。他のユーザー・プロファイル属性は借用されません。たとえば、限定機能属性は借用されません。

- 借用権限を使用中のプログラムがプログラム・スタックにある限り、借用権限は活動状態です。たとえば、PGMA が借用権限を使用するとします。
  - PGMA が CALL コマンドを使用して PGMB を開始する場合、 CALL コマンドの使用前と使用後はこれらがプログラム・スタックになります。

借用権限および CALL コマンド

CALL コマンド使用前の プログラム・スタック	**CALL コマンド使用後のプログラム・スタック**
QCMD . . . PGMA	QCMD . . . PGMA PGMB

PGMA は PGMB を呼び出した後もプログラム・スタックに残るので、 PGMB は PGMA の借用権限を使用します。(借用権限使用 (USEADPAUT) パラメーターを使用すると、これがオーバーライドされる場合があります。

  - PGMA が制御権転送 (TFRCTL) コマンドを使用して PGMB を開始すると、プログラム・スタックは以下のようになります。

借用権限および TFRCTL コマンド

TFRCTL コマンド使用前のプログラム・スタック	**TFRCTL コマンド使用後のプログラム・スタック**
QCMD . . . PGMA	QCMD . . . PGMB

PGMA は、もはやプログラム・スタック内にないため、PGMA の借用権限を使用しません。

- 借用権限のもとで実行中のプログラムで割り込みが発生すると、借用権限の使用は停止されます。以下の機能は、借用権限を使用しません。
  - システム要求
  - アテンション・キー (グループ・ジョブへの転送 (TFRGRPJOB) コマンドが実行中である場合、借用権限はグループ・ジョブには渡されません。)
  - 中断メッセージ処理プログラム
  - デバッグ機能

注: 借用権限は、アテンション・キーまたはグループ・ジョブ要求によって即時に割り込みされます。ユーザーは、アテンション・キー処理プログラムまたはグループ・ジョブ初期プログラムに対して権限を持っていなければなりません。そうでない場合、試行は失敗します。

たとえば、USERA は、プログラム PGM1 を実行しますが、 その際 USERB の権限を借用します。PGM1 は、SETATNPGM コマンドを使用して、PGM2 を指定します。 USERB は、 PGM2 に対して *USE 権限を持っています。 USERA は、 PGM2 に対して *EXCLUDE 権限を持っています。SETATNPGM 機能は、借用権限を使用して実行されているので、正常に実行されます。 USERB の権限が活動状態でなくなったため、 USERA がアテンション・キーを使用しようとすると、権限エラーが受信されます。

- 借用権限を使用するプログラムがジョブを投入する場合、その投入されたジョブに投入側プログラムの借用権限はありません。

- トリガー・プログラムまたは出口点プログラムが呼び出されると、コール・スタック内の直前のプログラムからの借用権限は、そのトリガー・プログラムまたは出口点プログラムに対する権限のソースとしては使用されません。
- ジョブ変更 (CHGJOB) コマンドを使用してジョブの出力待ち行列を変更するとき、プログラム借用機能は使用されません。変更を行うユーザー・プロファイルは、新しい出力待ち行列に対して権限を持っていなければなりません。
- スプール・ファイルを含む、作成されたオブジェクトはすべて、プログラムのユーザーまたはユーザーのグループ・プロファイルにより所有されています。(プログラムの所有者によっては所有されていません。)
- 借用権限は、プログラムを作成するコマンド (CRTxxxPGM) または プログラム変更 (CHGPGM) コマンドのいずれかで指定できます。
- CRTxxxPGM コマンドで REPLACE(*YES) を使用してプログラムを作成した場合、プログラムの新しいコピーは、置換されたプログラムと同じ USRPRF、 USEADPAUT、および AUT 値を持っています。CRTxxxPGM パラメーターで指定された USRPRF および AUT は無視されます。
- 元のプログラムで USRPRF(*OWNER) が指定されている場合、 CRTxxxPGM コマンドで REPLACE(*YES) を指定できるのはそのプログラムの所有者だけです。
- USRPRF パラメーターの値を変更できるのは、プログラムを所有するユーザーか、 *ALLOBJ および *SECADM 特殊権限を持つユーザーだけです。
- 権限を借用するオブジェクトの所有権を転送するには、 *ALLOBJ および *SECADM 特殊権限を持つユーザーとしてサインオンしなければなりません。
- プログラム所有者、または *ALLOBJ および *SECADM 特殊権限を持つユーザー以外のユーザーが、権限を借用するプログラムを復元すると、セキュリティーがリスクを負わないようにするために、そのプログラムに対するすべての私用権限と共通権限が取り消されます。

プログラム表示 (DSPPGM) およびサービス・プログラム表示 (DSPSRVPGM) コマンドによって、プログラムが権限を借用したか どうか (ユーザー・プロファイル・プロンプト)、およびプログラム・スタックにある、前の借用権限を使用しているか どうか (借用権限使用プロンプト) が示されます。借用プログラム表示 (DSPPGMADP) コマンドによって、 特定のユーザー・プロファイルの権限を使用するすべてのオブジェクトが表示されます。借用オブジェクト印刷 (PRTADPOBJ) コマンドは、権限を借用するオブジェクト の詳細を含む報告書を提供します。 また、このコマンドには、最後にコマンドが実行されたとき以降に変更されたオブジェクトの報告書を印刷するオプションもあります。

借用権限と結合プログラム: ILE* プログラム (*PGM) は、1 つまたは複数のモジュールが入ったオブジェクトです。これは、ILE* コンパイラーによって作成されます。 ILE プログラムは、1 つまたは複数のサービス・プログラム (*SRVPGM) に結合することができます。

ILE プログラムを正常な活動状態にするには、ユーザーは ILE プログラムおよびそれが結合されているすべてのサービス・プログラムに対して *EXECUTE 権限を持っていなければなりません。ILE プログラムが、プログラム呼び出しスタックの上位のプログラムの借用権限を使用する場合、その借用権限は、 ILE プログラムがバインドされているすべてのサービス・プログラムに対する権限を検査するために使用されます。 ILE プログラムが借用権限を使用する場合、プログラム起動時にシステムがサービス・プログラムに対するユーザーの権限を検査するときに、借用権限は検査されません。

借用権限のリスクと推奨事項: 借用権限を使用してプログラム実行を許可することは、制御権を意図的に解放するのと同じです。これは、ユーザーがオブジェクトに対する権限、およびユーザーが通常持つことのない特殊権限を持つことを許可することになります。借用権限は、さまざまな権限要件にかなう重要なツールを提供しますが、使用時には以下のような注意が必要です。

- アプリケーション要件を満たすのに必要とされる最小の権限を借用してください。 QSECOFR の権限や *ALLOBJ 特殊権限を持つユーザーの権限を借用するよりも、アプリケーション所有者の権限を借用する方法をお勧めします。
- 権限を借用するプログラムによって提供される機能を注意深く監視してください。これらのプログラムにより、コマンド入力機能など、プログラムの制御外のオブジェクトにアクセスする手段がユーザーに提供されないようにしてください。
- 権限を借用し、他のプログラムを呼び出すプログラムでは、ライブラリー修飾呼び出しを実行しなければなりません。その呼び出しではライブラリー・リスト (*LIBL) は使用しないでください。
- 権限を借用するプログラムを呼び出すことができるユーザーを制御してください。メニュー・インターフェースとライブラリー・セキュリティーを使用して、これらのプログラムが十分な制御なしで呼び出されることがないようにします。

借用権限を無視するプログラム

いくつかのプログラムでは、プログラム・スタックにある以前のプログラムの借用権限を使用したくない場合があります。たとえば、所有者権限を使用する初期メニュー・プログラムを使用する場合、メニュー・プログラムから呼び出されたプログラムがその権限を使用することを望まないかもしれません。

プログラムの借用権限使用 (USEADPAUT) パラメーターにより、オブジェクトに対する権限の検査時に、システムがスタックにある以前のプログラムの借用権限を使用するかどうかが決定されます。プログラムを作成するとき、デフォルトではスタック内の以前のプログラムから借用権限が使用されます。プログラムに借用権限を使用させたくない場合には、プログラム変更 (CHGPGM) コマンドまたはサービス・プログラム変更 (CHGSRVPGM) コマンドによって、 USEADPAUT パラメーターを *NO に設定してプログラムを変更することができます。 CRTxxxPGM コマンドで REPLACE(*YES) を使用してプログラムを作成した場合、プログラムの新しいコピーは、置換されたプログラムと同じ USRPRF、 USEADPAUT、および AUT 値を持っています。

注: 場合によっては、 MODINVAU MI 命令を使用して、呼び出される機能に借用権限が受け渡されないようにすることができます。MODINVAU 命令を使用すれば、C プログラムおよび C++ プログラムから、別のプログラムまたはサービス・プログラムの呼び出される機能に借用権限を渡さないようにできます。これは、呼び出される機能の USEADPAUT 設定値をユーザーが知らない場合に有用です。

権限ホルダー

権限ホルダーは、現在システム上に存在しないプログラム記述データベース・ファイルに対する権限を保持するためのツールです。これは、主にSystem/36 環境アプリケーションに使用されるもので、プログラム記述ファイルの削除および再作成を行います。権限ホルダーは、すでに存在しているファイル、または存在していないファイル用として、権限ホルダー作成 (CRTAUTHLR) コマンドを使用して作成できます。以下の事柄は、権限ホルダーに適用されます。

- 権限ホルダーは、システムの補助記憶域プール (ASP) または基本ユーザーの ASP 内のファイルしか保護できません。 独立 ASP 内のファイルを保護することはできません。
- 権限ホルダーは、特定のファイルとライブラリーに関連しています。権限ホルダーの名前は、ファイルと同じです。
- 権限ホルダーは、プログラム記述データベース・ファイルおよび S/36 環境で作成された論理ファイルにのみ使用できます。
- 一度権限ホルダーが作成されると、ファイルの場合と同じように私用権限を追加します。このコマンドは、オブジェクト権限の認可、取り消し、表示、またオブジェクト・タイプ *FILE を指定する場合に使

用してください。オブジェクト権限画面上では、権限ホルダーとファイル自体の区別はつきません。画面には、ファイルが存在するか、およびファイルに権限ホルダーがあるかどうかは示されません。

- ファイルが権限ホルダーに関連する場合は、権限ホルダーに対して定義された権限が、権限の検査時に使用されます。ファイルに対して定義された私用権限は無視されます。
- 権限ホルダー表示 (DSPAUTHLR) コマンドは、システム上の任意の権限ホルダーを表示または印刷する場合に使用してください。また、処理用に出力ファイル (アウト・ファイル) を作成する場合に使用することもできます。
- 存在するファイルに対して権限ホルダーを作成する場合、以下の事柄を考慮してください。
  - 権限ホルダーを作成しているユーザーは、ファイルに対して *ALL 権限を持っていなければなりません。
  - ユーザーが権限ホルダーを作成しているかどうかにかかわりなく、ファイルの所有者は、権限ホルダーの所有者になります。
  - 権限ホルダーに対する共通権限は、ファイルから取られます。CRTAUTHLR コマンドの共通権限 (AUT) パラメーターは、無視されます。
  - 既存のファイルの権限は、権限ホルダーにコピーされます。
- ファイルを作成して、そのファイルの権限ホルダーがすでに存在していた場合、以下の事柄を考慮してください。
  - ファイルを作成するユーザーは、権限ホルダーに対して *ALL 権限を持っていなければなりません。
  - ユーザーがファイルを作成するかどうかにかかわりなく、権限ホルダーの所有者は、ファイルの所有者になります。
  - ファイルに対する共通権限は、権限ホルダーから取られます。CRTPF コマンドまたは CRTLF コマンドの 共通権限 (AUT) パラメーターは無視されます。
  - 権限ホルダーはファイルにリンクされています。権限ホルダーに指定された権限は、ファイルのセキュリティーに使用されます。
- 権限ホルダーが削除されると、権限の情報はファイル自体に転送されます。
- ファイル名が変更され、新しいファイル名が既存の権限ホルダーと一致する場合、ファイルの権限と所有権は、権限ホルダーと一致するように変更されます。ファイル名を変更するユーザーには、権限ホルダーに対する *ALL 権限が必要です。
- ファイルが異なるライブラリーに移動され、権限ホルダーがそのファイル名とターゲット・ライブラリー用として存在している場合、そのファイルの権限と所有権は、権限ホルダーと一致するように変更されます。ファイルを移動させるユーザーは、権限ホルダーに対する *ALL 権限を持っていなければなりません。
- 権限ホルダーとファイルの所有権は、常に一致しています。ファイルの所有権を変更する場合は、権限ホルダーの所有権も変更します。
- ファイルの復元時に、そのファイル名およびそのファイルを復元中のライブラリー用に権限ホルダーが存在する場合、このファイルは権限ホルダーにリンクされます。
- ライブラリー QSYS、QRCL、QRECOVERY、QSPL、QTEMP、 および QSPL0002 から QSPL0032 には、ファイル用に権限ホルダーを作成できません。

権限ホルダーと System/36 の移行: System/36 移行援助機能により、移行されるすべてのファイルの権限ホルダーが作成されます。また、System/36 上に対応するファイルが存在しない場合は、この機能を使用して System/36 資源保護ファイルの項目用に権限ホルダーを作成します。権限ホルダーは、アプリケーションが削除および再作成を行うファイルの場合にのみ必要になります。権限ホルダー削除 (DLTAUTHLR) コマンドは、必要のない権限ホルダーを削除する場合に使用してください。

権限ホルダーのリスク: 権限ホルダーにより、ファイルが存在する前にそのファイルの権限を定義する機能が提供されます。特定の状況下でこれを行うと、許可されていないユーザーによる情報へのアクセスを許可する結果になる場合があります。アプリケーションによるファイルの作成、移動、または名前変更についてユーザーが知っている場合、そのユーザーはその新しいファイルの権限ホルダーを作成することができます。このようにして、ユーザーはファイルへのアクセスを得ます。このリスクを少なくするため、出荷時の CRTAUTHLR コマンドの共通権限 は *EXCLUDE に設定されています。権限を他のユーザーに認可しない限り、このコマンドを使用できるのは *ALLOBJ 権限を持つユーザーのみです。

権限の処理

この情報では、システム上での権限の設定、保守、およびシステムに関する権限情報の表示を行う場合の一般的な方法を説明します。『セキュリティー・コマンド』には、権限の処理に使用できるコマンドの詳細なリストが提供されています。以下の説明では、すべてのコマンド・パラメーターまたはすべての画面上のフィールドを取り扱っているわけではありません。

権限表示

次の 4 つの画面がオブジェクト権限を表示します。

- 「オブジェクト権限の表示」画面
- 「オブジェクト権限編集」画面
- 「権限表示」画面
- 「権限処理」画面

注:

- オブジェクトに対して *OBJMGT 権限を持っている場合は、そのオブジェクトのすべての私用権限を表示することができます。*OBJMGT 権限がない場合は、そのオブジェクトの自分固有の権限ソースしか表示できません。
- *ADOPTED 権限は、プログラム所有者から受け取る追加権限しか示しません。

権限報告書

セキュリティーの実施状況を監視するのに役立つ複数の報告書が利用できます。たとえば、以下のコマンドを使用すれば、 *EXCLUDE 以外の *PUBLIC 権限を持つオブジェクト、および私用権限を持つオブジェクトを監視することができます。

- 共通権限印刷 (PRTPUBAUT)
- 私用権限印刷 (PRTPVTAUT)

ライブラリーの処理

ライブラリー作成 (CRTLIB) コマンドの 2 つのパラメーターは、権限に影響を与えます。

- 権限 (AUT): AUT パラメーターを使用すると、次のいずれかを指定することができます。
  - ライブラリーの共通権限
  - ライブラリーを保護する権限リスト

  AUT パラメーターは、ライブラリー自体に適用され、ライブラリーのオブジェクトに対しては適用されません。権限リスト名を指定すると、ライブラリーの共通権限は *AUTL に設定されます。 ライブラリーの作成時に AUT を指定しない場合は、 *LIBCRTAUT がデフォルト値になります。システムは、*SYSVAL で出荷される QSYS ライブラリーから CRTAUT 値を使用しま す。

- 権限作成 (CRTAUT): CRTAUT パラメーターにより、ライブラリーに作成された新しいオブジェクトに対するデフォルト権限が決定されます。 CRTAUT は、システム定義権限 (*ALL、*CHANGE、*USE、または *EXCLUDE) の どれか、*SYSVAL (QCRTAUT システム値)、または権限リストの名前に対する権限のいずれかに設定することができます。

  注: ライブラリー変更 (CHGLIB) コマンドを使用して、ライブラリーの CRTAUT 値を変更することができます。

オブジェクトの作成

新しいオブジェクトを作成する場合は、権限 (AUT) を指定するか、またはデフォルトの *LIBCRTAUT を使用できます。

個々のオブジェクト権限の処理

オブジェクト権限を変更するには、以下のうちいずれかの権限を持っていなければなりません。

- *ALLOBJ 権限、または *ALLOBJ 特殊権限を持つグループ・プロファイルのメンバーシップ。

  注: オブジェクトに対して私用権限を持っている場合、グループの権限は使用されません。
- オブジェクトの所有権。グループ・プロファイルがオブジェクトを所有する場合、オブジェクト権限を変更する要件にかなっていない特定権限がメンバーに与えられているのではない限り、このグループのメンバーはオブジェクト所有者として操作を行うことができます。
- オブジェクトに対する *OBJMGT 権限、および認可または取り消しされているすべての権限 (*EXCLUDE を除く)。オブジェクト権限の処理を認可されているすべてのユーザーは、 *EXCLUDE 権限を認可したり取り消したりすることができます。

個々のオブジェクト権限を変更する最も簡単な方法として、 「オブジェクト権限編集」画面を使用することができます。この画面は、オブジェクト権限編集 (EDTOBJAUT) コマンドを使用して直接呼び出すか、または「所有者によるオブジェクト処理 (WRKOBJOWN)」画面か 「オブジェクト処理 (WRKOBJ)」画面からオプションで選択することができます。 これらのコマンドを使用してオブジェクト権限を変更することもできます。

- 権限変更 (CHGAUT)
- 権限処理 (WRKAUT)
- オブジェクト権限認可 (GRTOBJAUT)
- オブジェクト権限取り消し (RVKOBJAUT)

読み取り/書き込み (*RX) または書き込み/実行 (*WX) などの総称権限サブセットを指定する ときは、CHGAUT コマンドまたは WRKAUT コマンドを使用しなければなりません。

ユーザー定義権限の指定

「オブジェクト権限編集」画面の「オブジェクト権限」欄を使用して、システム定義の権限セット (*ALL、*CHANGE、*USE、*EXCLUDE) を指定することができます。システム定義のセットではない権限を指定したい場合は、 F11 (詳細の表示) を使用してください。

注: ユーザー・プロファイルのユーザー・オプション (USROPT) フィールド を *EXPERT に設定すると、F11 を押さなくてもこの画面の詳細なバージョンを表示することができます。F11 (データ権限の表示) を押すと、データ権限を表示または変更することができます。

追加ユーザーに権限を与えるには、「オブジェクト権限編集」 画面で F6 (新しいユーザーの追加) を押してください。複数ユーザーの権限の定義を可能にする、「新しいユーザーの追加」画面が表示されます。

ユーザーのオブジェクト権限を除去することと、ユーザーに *EXCLUDE 権限を 与えることには相違があります。*EXCLUDE 権限は、ユーザーにはオブジェクトの使用が特に許可されていないことを意味します。 *EXCLUDE 権限をオーバーライドするのは、*ALLOBJ 特殊権限と借用権限のみです。ユーザーの権限を除去することは、ユーザーがオブジェクトに対して特定権限を持っていないことを意味します。ユーザーは、グループ・プロファイル、権限リスト、共通権限、 *ALLOBJ 特殊権限、または借用権限を介してアクセス権を得ることができます。

「オブジェクト権限編集」画面を使用して、ユーザーの権限を除去することができます。ユーザーのオブジェクト権限フィールドにブランクをタイプし、Enter キーを押してください。ユーザーが画面から除去されます。また、オブジェクト権限取り消し (RVKOBJAUT) コマンドを使用することもできます。ユーザーが持つ特定権限を取り消すか、またはユーザーの *ALL 権限を取り消して ください。

注: RVKOBJAUT コマンドでは、指定した権限だけが取り消されます。たとえば、USERB は、ライブラリー LIBB の FILEB に対して *ALL 権限を 持っています。*CHANGE 権限を次のように取り消します。 `RVKOBJAUT OBJ(LIBB/FILEB) OBJTYPE(*FILE) + USER(*USERB) AUT(*CHANGE)`

複数オブジェクトの権限の処理

「**オブジェクト権限編集**」画面を使用すると、一度に 1 つのオブジェクトの権限を対話式に処理することができます。オブジェクト権限認可 (GRTOBJAUT) コマンドを使用すると、 一度に 2 つ以上のオブジェクトに対する権限変更が認可されます。GRTOBJAUT 権限コマンドは、対話式またはバッチで使用できます。また、このコマンドは、プログラムから呼び出すこともできます。以下に、GRTOBJAUT コマンドの使用例とそのプロンプト表示を示します。コマンドが実行されると、変更が行われたかどうかを示す、各オブジェクトに関するメッセージを受信します。権限の変更には、オブジェクトに排他ロックをかける必要があり、オブジェクトの使用中は変更を実行できません。試行され、実行された変更のレコードのジョブ・ログを印刷してください。 TESTLIB ライブラリーのすべてのオブジェクトに *USE の共通権限を与えるには、以下のようにします。

```
オブジェクト権限認可  (GRTOBJAUT)

  選択項目を入力して，実行キーを押してください。
  オブジェクト  . . . . . .  *ALL
    ライブラリー  . . . . . .    TESTLIB
  オブジェクト・タイプ  . . . . .  *ALL
 ASP 装置  . . . . . .  *
  ユーザー  . . . . . .  *PUBLIC
              値の続きは＋
権限 . . . . . .*USE
```

この GRTOBJAUT コマンドの例では、 指定する権限が与えられますが、指定した権限より上位の権限は除去されません。 TESTLIB ライブラリーのいくつかのオブジェクトが共通権限 *CHANGE を 持っている場合、このコマンドでは、*USE に対する共通権限は削除されません。 TESTLIB のすべてのオブジェクトが必ず *USE の共通権限を持つようにするには、 次のように、REPLACE パラメーターを指定した GRTOBJAUT コマンドを使用してください。 `GRTOBJAUT OBJ(TESTLIB/*ALL) OBJTYPE(*ALL) + USER(*PUBLIC) REPLACE(*YES)`

REPLACE パラメーターは、指定する権限が、ユーザーの既存の権限を置き換えるかどうかを指定します。デフォルト値 REPLACE(*NO) により、指定する権限が与えられますが、 *EXCLUDE 権限を認可する場合を除いて、指定した権限より上位の権限は除去されません。これらのコマンドにより、現在ライブラリー

に存在するオブジェクトに対してのみ共通権限が設定されます。後で作成される新しいオブジェクトの共通権限を設定するには、ライブラリー記述上の CRTAUT パラメーターを使用してください。

オブジェクト所有権の処理

オブジェクトの所有権を変更するには、次のいずれかを使用します。

- オブジェクト所有者変更 (CHGOBJOWN) コマンド
- 所有者によるオブジェクト処理 (WRKOBJOWN) コマンド
- 所有者変更 (CHGOWN) コマンド

「所有者によるオブジェクト処理」画面には、プロファイルが所有するすべての オブジェクトが表示されます。個々のオブジェクトを新しい所有者に割り当てることができます。また、画面の最下部にある NEWOWN (新しい所有者) パラメーターを使用して、 一度に 2 つ以上のオブジェクトの所有権を変更することもできます。 いずれかの方法を使用して所有権を変更する場合、 オブジェクトに対する以前の所有者の権限を除去する選択を行うことができます。CUROWNAUT (現在の所有者の権限) パラメーターのデフォルト値は、*REVOKE です。 オブジェクトの所有権を移すには、以下の権限を持っていなければなりません。

- オブジェクトに対するオブジェクト存在権限
- オブジェクトが権限リストである場合、*ALL 権限または所有権
- 新しい所有者のユーザー・プロファイルに対する追加権限。
- 現行所有者のユーザー・プロファイルに対する削除権限。

オブジェクトを所有するユーザー・プロファイルを削除することはできません。「所有者によるオブジェクト処理」画面には、統合ファイル・システム・オブジェクトが含まれます。 これらのオブジェクトの場合、画面のオブジェクト欄に、パス名の最初の 18 文字が示されます。 パス名が 18 文字より長い場合、記号 (>) が、パス名の終わりに表示されます。絶対パス名を表示するときは、カーソルをそのパス名の任意の位置に置いて、F22 キーを押します。

資源保護

システムでの資源保護によって、オブジェクトを使用できるユーザーとそのオブジェクトの使用方法を定義できます。オブジェクトにアクセスできることを権限と呼びます。オブジェクト権限を設定するときには、ユーザーが自分たちの作業を十分に実行でき、しかもシステムの表示や変更が不可能な権限を与えるよう、よく考慮してください。

オブジェクト権限は、特定のオブジェクトに関する許可をユーザーに与え、そのオブジェクトに対してユーザーは何ができるかを指定できます。具体的で詳細なユーザー権限 (たとえばレコードの追加や変更) を介して、オブジェクト資源を制限できます。システム資源を使用して、
*ALL、*CHANGE、*USE、*EXCLUDE といった、特定のシステム定義の権限のサブセットへのアクセスをユーザーに与えることができます。資源保護を必要とする最も一般的なシステム・オブジェクトはファイル、プログラム、ライブラリー、ディレクトリーですが、システム上のどんなオブジェクトに対しても権限を指定できます。

権限のタイプの理解: 資源保護の目的の決定を終え、決定事項をライブラリー記述用紙に記録したら、権限のタイプの計画を立てることができます。資源保護により、ユーザーがシステム上のオブジェクトにどのようにアクセスするかが定義されます。

権限とは、特定のユーザーに与えられているオブジェクトの使用許可のことです。たとえば、システム上の情報を表示したり変更したりする権限があります。システムには数種類の権限タイプがあります。 IBM で

は、これらの権限タイプをシステム定義の権限というカテゴリーにグループ化しています。これは大多数の人々の必要に合ったものです。以下の表に、これらのカテゴリーのリストと、それらがどのようにファイルとプログラムの保護に適用されるかが示されています。

注: 権限の計画を立てる際には以下の表を参照してください。

システム定義の権限

権限名	許可されているファイル操作	許可されていないファイル操作	許可されているプログラム操作	許可されていないプログラム操作
*USE	ファイル中の情報の表示。	ファイル中の情報の変更または削除。ファイルの削除。	プログラムの実行。	プログラムの変更または削除。
*CHANGE	ファイル内のレコードの表示、変更、および削除。	ファイル全体の削除または消去。	プログラムの記述の変更。	プログラムの変更または削除。
*ALL	ファイルの作成および削除。ファイル内のレコードの追加、変更、および削除。他人がファイルを使用する権限。	なし	プログラムの作成、変更および削除。他人がプログラムを使用する権限。	プログラム借用権限の場合は、プログラムの所有者の変更。
*EXCLUDE[1]	なし	ファイルに対するすべてのアクセス。	なし	プログラムに対するすべてのアクセス。
[1] *EXCLUDE では、共通権限やグループ・プロファイルを介して認可された権限はすべて変更されます。				

単純な資源保護を設計するには、 ライブラリー全体のセキュリティーの計画を立ててください。 そのためには、システム定義の権限がライブラリーに適用される方法について理解する必要があります。 以下の表に、その点が示されています。

ライブラリーに関するシステム定義の権限

権限名	許可されている操作	許可されていない操作
*USE	• ライブラリー内のオブジェクトの場合、権限によって許可されている、特定のオブジェクトに対するすべての操作。 • ライブラリーの場合、記述情報の表示。	• ライブラリーへの新規オブジェクトの追加。 • ライブラリー記述の変更。 • ライブラリーの削除。
*CHANGE	• ライブラリー内のオブジェクトの場合、権限によって許可されている、特定のオブジェクトに対するすべての操作。 • ライブラリーへの新規オブジェクトの追加。 • ライブラリー記述の変更。	ライブラリーの削除。
*ALL	• 変更操作によって行えるすべての処理。 • ライブラリーの削除。 • ライブラリーに対する権限を他のユーザーに付与。	なし。

ライブラリー権限とオブジェクト権限が協働する仕方についても理解する必要があります。 以下の表には、オブジェクトとライブラリーの両方に必要な権限の例が示されています。

ライブラリー権限とオブジェクト権限が協働する仕方

オブジェクト・タイプ	操作	必要なオブジェクト権限	必要なライブラリー権限
ファイル	データの変更	*CHANGE	*USE
ファイル	ファイルの削除	*ALL	*USE
ファイル	ファイルの作成	*ALL	*CHANGE
プログラム	プログラムの実行	*USE	*USE
プログラム	プログラムの変更 (再コンパイル)	*ALL	*CHANGE
プログラム	プログラムの削除	*ALL	*USE

ディレクトリー権限はライブラリー権限に似ています。 オブジェクトにアクセスするには、 オブジェクトのパス名のすべてのディレクトリーに対する権限が必要です。

オブジェクト所有権の判別:

システム上のすべてのオブジェクトには、それぞれ所有者がいます。所有者は、デフォルトで、オブジェクトに対する *ALL 権限を持っています。

オブジェクト所有権

各オブジェクトには、作成時に所有者が割り当てられます。所有者になるのは、オブジェクトを作成するユーザーか、あるいはメンバー・ユーザー・プロファイルでグループ・プロファイルをオブジェクトの所有者に指定している場合は、そのグループ・プロファイルです。オブジェクトが作成されると、すべてのオブジェクト権限とオブジェクトに対するすべてのデータ権限が所有者に与えられます。

オブジェクトの所有者は、任意のまたはすべての権限が特に除去されていない限り、常にオブジェクトに対するすべての権限を持つことになります。オブジェクト所有者は、予防策としていくつの特定権限を除去しておくこともできます。たとえば、重要な情報の入っているファイルがあるとして、所有者は不慮の事故でそのファイルを削除してしまわないように、自分のオブジェクト存在権限を除去しておくことができます。しかし、オブジェクト所有者として、いつでも任意のオブジェクト権限を自分自身に認可することができます。

オブジェクトの所有権は、一人のユーザーから他のユーザーに転送できます。所有権は、個々のユーザー・プロファイルまたはグループ・プロファイルに転送できます。グループ・プロファイルは、そのグループにメンバーがあってもなくても、オブジェクトを所有できます。

オブジェクトの所有者を変更する場合は、以前の所有者の権限を保持するかまたは取り消すかを任意に選択できます。*ALLOBJ 権限を持つユーザーは、以下の権限を持つユーザーと同様に、所有権を転送できます。

- オブジェクトに対するオブジェクト存在権限、権限リストは除く。
- オブジェクトが権限リストである場合は、オブジェクトの所有権。
- 新しい所有者のユーザー・プロファイルに対する追加権限。
- 現行所有者のユーザー・プロファイルに対する削除権限。

オブジェクトを所有するプロファイルは削除できません。オブジェクトの所有権を新しい所有者に転送するか、 オブジェクトを削除しないと、プロファイルを削除することはできません。ユーザー・プロファイル削除 (DLTUSRPRF) コマンドを使用して、プロファイルを削除する際に所有されているオブジェクトの処理ができます。

オブジェクト所有権は、システムにより管理ツールとして使用されます。そのオブジェクトの所有者プロファイルには、オブジェクトに対して私用権限を持つすべてのユーザーのリストが入っています。この情報は、オブジェクト権限の編集または検討を行うための画面を構築する場合に使用します。

多くの私用権限を持つオブジェクトを多く所有するプロファイルは、非常に大きくなる可能性があります。所有されているオブジェクトに対する権限の表示または処理、およびプロファイルの保管または復元を行う際に、多くのオブジェクトを所有するプロファイルのサイズがパフォーマンスに影響を与えます。また、システム操作もインパクトを受けます。パフォーマンスまたはシステム操作上のインパクトを抑えるためには、全システムで 1 つの所有者プロファイルだけにオブジェクトを割り当てることは避けてください。各アプリケーションおよびアプリケーション・オブジェクトは、別々のプロファイルで所有させてください。また、IBM 提供のユーザー・プロファイルには、ユーザーのデータまたはオブジェクトを所有させないでください。また、オブジェクトの所有者にもオブジェクトの十分な記憶域が必要です。

デフォルト所有者 (QDFTOWN) ユーザー・プロファイル: デフォルト所有者 (QDFTOWN) ユーザー・プロファイルは、オブジェクト所有者がいない場合、またはオブジェクト所有者がセキュリティーのリスクの原因になる場合に使用される、IBM 提供のユーザー・プロファイルです。オブジェクトの所有権が QDFTOWN プロファイルに割り当てられる、以下のような状況があります。

- 所有しているプロファイルが損傷を受けて削除された場合、そのオブジェクトは、所有者を持たないことになります。記憶域再利用 (RCLSTG) コマンドを使用して、これらのオブジェクトの所有権をデフォルト所有者 (QDFTOWN) ユーザー・プロファイルに割り当てます。
- オブジェクトが復元され、所有者プロファイルが存在しない場合。
- 再作成される必要のあるプログラムが復元されていても、プログラムが正常に作成されなかった場合。
- 移動されるファイル、名前変更されるファイル、またはそのライブラリー名が変更されるファイルと同じ名前の権限ホルダーを所有するユーザー・プロファイルの最大記憶域限界を超過した。

すべてのオブジェクトには所有者が存在しなければならないので、 QDFTOWN ユーザー・プロファイルがシステムによって提供されています。システムが出荷される時点では、*ALLOBJ 特殊権限を持つユーザーだけが、このユーザー・プロファイルを表示してアクセスし、QDFTOWN ユーザー・プロファイルに関連するオブジェクトの所有権を転送すること ができます。また、このユーザーは、他のユーザーに QDFTOWN プロファイルに対する権限を認可することができます。QDFTOWN ユーザー・プロファイルは、システム使用のみを対象としています。したがって、QDFTOWN が定常的にオブジェクトを所有するようなセキュリティーの設計は しないでください。

アプリケーション所有権の変更

プログラマーまたはアプリケーションの提供者が特別なプロファイルを作成して、アプリケーション・ライブラリーとオブジェクトを所有している場合は、命名規則が一致していなくてもそのプロファイルを使用することを考慮してください。オブジェクトの所有権を転送すると長時間かかることがあるため、避けてください。 QSECOFR や QPGMR などの IBM 提供のグループ・プロファイルの 1 つがアプリケーションを所有する場合は、そのアプリケーションの導入後に別のプロファイルに所有権を転送する必要があります。プログラマーは、オブジェクトの所有権に関する変更を加えなくて済むように、アプリケーションを設計することがあります。制約事項の範囲内で作業しながら、セキュリティーの管理に関する独自の要件を満たしてください。しかし、QSECOFR などの IBM 提供のプロファイルがアプリケーションを所有している場合

は、お客様自身とプログラマーまたはアプリケーションの提供者が相談して、所有権を変更する計画を開発する必要があります。理想的には、所有権を変更してからアプリケーションを導入してください。

共通権限の変更

オブジェクトを保管する際には、その共通権限も同時に保管することになります。システムにアプリケーション・ライブラリーを復元すると、ライブラリーとそのすべてのオブジェクトには、保管時に持っていたものと同じ共通権限があります。このことは、別のシステムにライブラリーを保管していた場合にも当てはまります。ライブラリーの CRTAUT 値は、復元されるオブジェクトには影響しません。ライブラリーの CRTAUT 値に関係なく、保管時の共通権限を持ったまま復元されます。ライブラリーとオブジェクトの共通権限に変更を加え、ライブラリー記述用紙での計画と一致させる必要があります。

オブジェクトのグループ所有権:

このトピックでは、オブジェクトが個人ではなくグループによって所有される場合のセキュリティーの相違点について取り上げます。

オブジェクトのグループ所有権: オブジェクトが作成されると、システムは、オブジェクト所有権を決定するためオブジェクトを作成中であるユーザーのプロファイルを調べます。ユーザーがグループ・プロファイルのメンバーである場合、ユーザー・プロファイルにある OWNER フィールドに、ユーザーとグループのどちらが新しいオブジェクトを所有するかが指定されています。

グループがオブジェクトを所有する場合、OWNER は *GRPPRF、オブジェクトを作成しているユーザーに、オブジェクトに対する特定権限が自動的に与えられることはありません。ユーザーは、グループを介して、オブジェクトに対する権限を得ます。ユーザーがオブジェクトを所有する場合、OWNER は *USRPRF、オブジェクトに対するグループの権限は、ユーザー・プロファイルにある GRPAUT フィールドによって決まります。

ユーザー・プロファイル内のグループ権限タイプ GRPAUTTYP フィールドにより、グループがオブジェクトの 1 次グループになるかどうか、またオブジェクトに対する私用権限がグループに与えられるかどうかが判別されます。オブジェクトを所有するユーザーを異なるユーザー・グループに変更した場合、作成元のグループ・プロファイルは、作成されたすべてのオブジェクトに対する権限を保持します。

ユーザー・プロファイルの所有者フィールドが *GRPPRF である場合でも、新しいオブジェクトの作成中、ユーザーはそのオブジェクトを保持するのに十分な大きさの記憶域を持っていなければなりません。新しいオブジェクトが作成された後、所有権はグループ・プロファイルに移されます。ユーザー・プロファイルの MAXSTG パラメーターにより、ユーザーに許可される補助記憶域が決定されます。

グループと個々のユーザー所有権の選択時に、照会プログラムなど、ユーザーが作成するオブジェクトを以下のように評価してください。

- ユーザーが、異なる部門と異なるユーザー・グループに移動する場合、ユーザーは引き続きオブジェクトを所有すべきか。
- オブジェクトの作成者が分かっているかどうかは重要な問題だろうか。オブジェクト権限画面に表示されるのは、オブジェクト所有者で、オブジェクトを作成したユーザーではありません。

注: 「オブジェクト記述表示」画面には、オブジェクト作成者が表示されます。

監査ジャーナル機能が活動状態の場合、オブジェクト作成 (CO) 項目は、オブジェクトの作成時に QAUDJRN 監査ジャーナルに書き込まれます。この項目により、 作成中のユーザー・プロファイルを識別します。 項目が書き込まれるのは、QAUDLVL システム値に *CREATE が指定されており、QAUDCTL システム値に *AUDLVL が含まれている場合だけです。

オブジェクトの 1 次グループ: オブジェクトには 1 次グループを指定することができます。1 次グループ・プロファイルの名前およびオブジェクトに対する 1 次グループの権限は、そのオブジェクトとともに保管されます。オブジェクトへの権限検査を行うときは、1 次グループ権限を使用すると、私用グループ権限を使用するよりパフォーマンスが向上します。

プロファイルをオブジェクトの 1 次グループとして割り当てるには、そのプロファイルをグループ・プロファイル (*gid* を持つ) にしなければなりません。同じプロファイルはそのオブジェクトおよびその 1 次グループの所有者にはなれません。ユーザーが新規オブジェクトを作成するとき、ユーザー・プロファイル内のパラメーターは、ユーザーのグループにオブジェクトに対する権限が与えられるかどうか、および与えられる権限のタイプを制御します。ユーザー・プロファイル内のグループ権限タイプ (GRPAUTTYP) パラメーターを使用すると、ユーザーのグループをそのオブジェクトの 1 次グループにすることができます。

オブジェクト 1 次グループ変更 (CHGOBJPGP) コマンド、 または 1 次グループによるオブジェクト処理 (WRKOBJPGP) コマンドを使用して、オブジェクトの 1 次グループを指定します。「オブジェクト権限編集」画面または権限認可コマンドおよび取り消しコマンドを使用すると、1 次グループの権限を変更できます。

1 次グループ権限の処理

1 次グループまたは 1 次グループのオブジェクトに対する権限を変更するときは、次のいずれかのコマンドを使用します。

- オブジェクト 1 次グループ変更 (CHGOBJPGP)
- 1 次グループによるオブジェクト処理 (WRKOBJPGP)
- 1 次グループ変更 (CHGPGP)

オブジェクトの 1 次グループを変更するときは、新しい 1 次グループが持つ権限を指定します。 さらに、古い 1 次グループの権限を取り消すこともできます。 古い 1 次グループの権限を取り消さない場合は、それが私用権限になります。 新しい 1 次グループは、オブジェクトの所有者になれません。 オブジェクトの 1 次グループを変更するには、次のものをすべて備えていなければなりません。

- オブジェクトに対する *OBJEXIST 権限。
- オブジェクトがファイル、ライブラリー、またはサブシステム記述である場合は、*OBJOPR および *OBJEXIST 権限。
- オブジェクトが権限リストである場合は、*ALLOBJ 特殊権限、または権限リストの所有者であること。
- 古い 1 次グループの権限を取り消す場合は、*OBJMGT 権限。
- *PRIVATE 以外の値を指定する場合は、*OBJMGT 権限および与えられるすべての権限。

参照オブジェクトの使用

「オブジェクト権限編集」画面と GRTOBJAUT コマンドを使用すると、参照オブジェクトの権限に基づく権限をオブジェクト (またはオブジェクトのグループ) に与えることができます。これはある状況においては便利なツールですが、要件を満たすには権限リストの使用を考慮する必要もあります。

アプリケーション記述ワークシート:

システム上の各アプリケーションについて、このワークシートを完成させてください。

表 92. アプリケーション記述ワークシート

アプリケーション記述ワークシート	
作成者:	日付:

表 92. アプリケーション記述ワークシート (続き)

アプリケーション記述ワークシート	
指示 • アプリケーションごとに別々のワークシートを作成します。 • このワークシートの情報は、システムに入力する必要はありません。	
アプリケーション名:	省略形:
アプリケーションについての簡単な説明:	
1 次メニュー名:	ライブラリー:
初期プログラム名:	ライブラリー:
アプリケーションが使用するライブラリーのリスト (ファイル用とプログラム用の両方):	
アプリケーションに対するセキュリティーの目的 (機密情報を含んでいるかどうかなど):	

アプリケーションの導入の計画:

資源保護の計画を終了するには、 アプリケーションを導入する準備を行う必要があります。

以下のトピックは、アプリケーションを導入した後に、そのアプリケーションに対する所有権や権限を計画するのに役立ちます。しかし、ここで説明する方式が当てはまらないアプリケーションもあります。効率的な導入の計画を立てる際には、プログラマーかアプリケーションの提供者と相談してください。

アプリケーションの提供者からアプリケーションを入手する計画であれば、この情報を使用して、アプリケーション・ライブラリーのロード前後に行う必要のあるセキュリティーを計画してください。プログラマーが開発したアプリケーションをご使用のシステムに導入する計画であれば、この情報を使用して、アプリケーションをテスト状況から実動状況に移行するのに必要なセキュリティー活動を計画してください。まず、1 つのアプリケーションで、すべてのステップを実行します。次に、その他のアプリケーションに戻って、アプリケーションの導入用紙を作成します。

以下の用紙をコピーして、この情報の作業を進めながら記入してください。
- アプリケーション記述用紙。アプリケーションごとに 1 つずつ完成させる必要があります。
- ライブラリー記述用紙
- 権限リスト用紙

これで、これらの計画作業が完了しました。ユーザー・セキュリティーの設定に進むことができます。

権限リストの計画

権限リストを使用して、類似のセキュリティー要件を持つオブジェクトごとに分類することができます。

概念的には、権限リストは、ユーザーのリストと、リストによって保護されているオブジェクトに対してユーザーが持っている権限を示しています。権限リストは、システム上の類似のオブジェクトに対する権限を管理するための効率的な方法を提供します。ただし、場合によっては、権限リストがオブジェクトに対する権限の追跡を困難にすることもあります。私用認可オブジェクトの印刷 (PRTPVTAUT) コマンドを使用して、権限リストの権限に関する情報を印刷することができます。

権限リスト・セキュリティー

権限リストを使用して、セキュリティー要件の類似したオブジェクトをグループ化することができます。権限リスト内には、概念として、ユーザーのリストおよびリストによって保護されているオブジェクトに対し

てそのユーザーが持っている権限が入っています。それぞれのユーザーは、リストが保護するオブジェクトのセットに対して、異なる権限を持つことが可能です。権限リストに対してユーザー権限を与える場合、オペレーティング・システムは実際には、権限リストに対するそのユーザーの私用権限を与えます。また、権限リストを使用して、リスト上のオブジェクトに対する共通権限を定義することもできます。オブジェクトに対する共通権限が *AUTL に設定される場合、オブジェクトは共通権限を権限リストから得ます。

権限リスト・オブジェクトは、システムによって管理ツールとして使用されます。これには、実際に、権限リストによって保護されたすべてのオブジェクトのリストが含まれます。この情報は、権限リスト・オブジェクトの参照または編集を行うための画面を構築する場合に使用されます。

ユーザー・プロファイルまたは他の権限リストを保護するために権限リストを使用することはできません。1 つのオブジェクトに対しては 1 つの権限リストだけを指定できます。オブジェクトの権限リストを追加または削除できるのは、オブジェクトの所有者、全オブジェクト (*ALLOBJ) 特殊権限を持つユーザー、またはオブジェクトに対してすべての (*ALL) 権限を持つユーザーだけです。

システム・ライブラリー (QSYS) 中のオブジェクトについては、権限リストを使用して保護することができます。しかし、オブジェクトの保護を行う権限リストの名前は、オブジェクトとともに保管されます。オペレーティング・システムの新しいリリースを導入すると、 QSYS ライブラリーにあるすべてのオブジェクトが置き換えられる場合があります。この場合、オブジェクトと権限リストの関係は失われます。

権限リストの計画

権限リストには以下のような利点があります。

- 権限リストは権限の管理を単純化します。
- ユーザー権限はリスト上の各オブジェクトにではなく、権限リストに定義されます。新しいオブジェクトが権限リストで保護される場合、リスト上のユーザーはオブジェクトに対する権限を獲得できます。
- 1 回の操作で、リスト上のすべてのオブジェクトにユーザー権限を与えることができます。
- 権限リストは、システム上の私用権限の数を減少させます。各ユーザーは 1 つのオブジェクト、つまり権限リストに対して私用権限を持ちます。これによってリスト上のすべてのオブジェクトに対して、ユーザー権限が与えられます。システムの私用権限の数を減らすことには、以下のような利点があります。
  - ユーザー・プロファイルのサイズが小さくなります。
  - システムを保管する (SAVSYS) ときや、セキュリティー・データを保管する (SAVSECDTA) ときのパフォーマンスを改善できます。
- 権限リストは、ファイルを保護するための有効な手段です。私用権限を使っている場合は、各ユーザーが各ファイル・メンバーに対する私用権限を持っています。権限リストを使用すると、各ユーザーは権限を 1 つだけ持っていればよくなります。また、オープンされているファイルでは、ファイルに対する権限を認可したり、ファイルから権限を取り消したりすることができません。権限リストを使用してファイルを保護する場合は、ファイルがオープンされているときでも、権限を変更することができます。
- 権限リストによって、オブジェクトが保管されたときに権限を記憶する方法が提供されます。権限リストによって保護されたオブジェクトを保管すると、その権限リストの名前がオブジェクトとともに保管されます。オブジェクトが削除されて同じシステムに復元された場合、それは権限リストに再び自動的にリンクされます。オブジェクトが別のシステム上で復元された場合、復元コマンドで ALWOBJDIF(*ALL) が指定されていないと、権限リストはリンクされません。

権限リスト使用の利点

セキュリティー管理の観点から考えると、権限リストの方が、同じセキュリティー要件のあるオブジェクトを管理するのに良い方法です。リストで保護するオブジェクトが少ししかないときでも、オブジェクトで私用権限を使用するのではなく、権限リストを使用する方がやはり利点があります。また、新規オブジェクトを、既存のオブジェクトと同じ権限で保護することも容易になります。

権限リストを使用する場合は、そのオブジェクトの私用権限を持っていてはなりません。オブジェクトに私用権限があり、しかもそのオブジェクトを権限リストでも保護する場合は、権限検査時に、ユーザーの私用権限についての 2 つの探索が必要になります。最初の探索はオブジェクトの私用権限について探索で、2 番目の探索は権限リストの私用権限についての探索です。 2 つの探索はシステム資源の使用を必要として、パフォーマンスに影響することがあります。

権限リストだけしか使用しない場合は、1 つの探索だけ実行されます。また、権限リストでは権限キャッシュが使用されるため、権限検査のパフォーマンスは、オブジェクトの私用権限だけを検査する場合と同じになります。アプリケーションの要求が変更されると、より多くの作業ファイルがアプリケーションに追加されます。また、ジョブ担当が変更すると、別のユーザーが月末処理を実行します。

権限リストはこれらの変更の管理を容易にします。以下のステップを使用して、権限リストを設定します。

1. 権限リストを作成します。 `CRTAUTL ICLIST1`
2. 権限リストとともにすべての作業ファイルを保護します。 `GRTOBJAUT OBJ(ITEMLIB/ICWRK*) + OBJTYP(*FILE) AUTL(ICLIST1)`
3. 月末処理を実行するユーザーを追加します。 `ADDAUTLE AUTL(ICLIST1) USER(USERA) AUT(*ALL)`

権限リストの使用

iSeries ナビゲーターは、セキュリティー計画およびセキュリティー・ポリシーの開発を支援し、貴社のニーズに合わせてシステムを構成するために設計されたセキュリティー機能を提供します。使用可能な機能の 1 つに、権限リストの使用があります。権限リストには、次のような機能があります。

- 類似したセキュリティー要件をもつ権限リスト・グループ・オブジェクト。
- 権限リストには、概念的に、ユーザーやグループ、およびリストによって保護されているオブジェクトに対してユーザーおよびグループが持っている権限が含まれている。
- 各ユーザーおよびグループは、リストによって保護されているオブジェクトのセットに対してさまざまな権限を持つことができる。
- 権限を、ユーザーおよびグループに対して個々に付与せずに、リストによって付与することができる。権限リストを使用して行える作業には、次のものがあります。
  - 権限リストの作成
  - 権限リストの変更
  - ユーザーおよびグループの追加
  - ユーザー許可の変更
  - 保護されたオブジェクトの表示

この機能を使用するには、これらのステップを実行します。

1. iSeries ナビゲーターで、ご使用の「サーバー」—>「セキュリティー」と展開する。権限リストおよびポリシーが表示されます。
2. 「権限リスト」を右マウス・ボタンでクリックし、「新規権限リスト」を選択する。「新規権限リスト」で、以下のことができます。
   - 「使用 (Use)」: オブジェクト属性にアクセスして、オブジェクトを使用することができる。共通のものは表示できますが、オブジェクトを変更することはできません。

- 「変更 (Change)」: いくつかの例外がありますが、オブジェクトの内容を変更できる。
- 「すべて (All)」: 所有者に限定されているオブジェクトを除く、オブジェクトに関するすべての操作が行える。ユーザーまたはグループは、オブジェクトの存在の制御、オブジェクトのセキュリティーの指定、オブジェクトの変更、およびオブジェクトに関する基本機能の実行を行うことができます。また、ユーザーまたはグループは、オブジェクトの所有権を変更することもできます。
- 「除外 (Exclude)」: オブジェクトに関するすべての操作が禁止される。この許可タイプを持っているユーザーおよびグループには、オブジェクトへのアクセスまたは操作が許可されません。共通でオブジェクトを使用することができないように指定してください。

権限リストを処理する際に、オブジェクトとデータの両方の認可を認可することになります。 選択できるオブジェクト許可には、以下のものがあります。

- 「操作可能 (Operational)」: オブジェクトの記述を見るための許可と、そのオブジェクトに対してユーザーまたはグループが持っているデータ許可によって決められている通りにオブジェクトを使用するための許可を与える。
- 「管理 (Management)」: オブジェクトのセキュリティーを指定するための許可、オブジェクトを移動またはリネームするための許可、データベース・ファイルにメンバーを追加するための許可を与える。
- 「存在 (Existence)」: オブジェクトの存在および所有権を制御するための許可を与える。ユーザーまたはグループは、オブジェクトの削除、オブジェクトのストレージの解放、オブジェクトに関する保管および復元操作の実行、オブジェクトの所有権の移行を行うことができます。ユーザーまたはグループが特殊な保管許可を持っている場合には、ユーザーまたはグループは、オブジェクトの存在許可を必要としません。
- 「更新 (Alter)」(データベース・ファイルおよび SQL パッケージに限り 使用される): オブジェクトの属性を更新するために必要な許可を与える。ユーザーまたはグループがデータベース・ファイルに関してこの許可を持っている場合には、ユーザーまたはグループは、トリガーの追加および除去、参照制約および固有制約の追加および除去、データベース・ファイルの属性の変更を行うことができます。ユーザーまたはグループが SQL パッケージに関してこの許可を持っている場合には、ユーザーまたはグループは、SQL パッケージの属性を変更することができます。この許可は、現時点では、データベース・ファイルおよび SQL パッケージに限り使用されます。
- 「参照 (Reference)」(データベース・ファイルおよび SQL パッケージに 限り使用される): あるオブジェクトの操作が他のオブジェクトによって制限されている場合などに、他のオブジェクトからあるオブジェクトを参照するために必要な許可を与える。ユーザーまたはグループが物理ファイルに関してこの許可を持っている場合には、ユーザーまたはグループは、物理ファイルが親である参照制約を追加することができます。この許可は、現時点では、データベース・ファイルに限り使用されます。選択できるデータ許可は、次のとおりです。
- 「読み取り (Read)」: オブジェクトの内容を入手および表示する (ファイルのレコードを表示するなど) ために必要な許可を与える。
- 「追加 (Add)」: オブジェクトに項目を追加する (メッセージをメッセージ待ち行列に追加する、レコードをファイルに追加するなど) ための許可を与える。
- 「更新 (Update)」: オブジェクトの項目を変更する (ファイルのレコードを 変更する) ための許可を与える。
- 「削除 (Delete)」: オブジェクトから項目を除去する (メッセージをメッセージ待ち行列から削除する、レコードをファイルから除去するなど) ための許可を与える。
- 「実行 (Execute)」: プログラム (サービス・プログラムまたは SQL パッケージ) を実行するために必要な許可を与える。ユーザーは、ライブラリーまたはディレクトリー内のオブジェクトを見付けることもできます。

権限リストの作成または編集時の各プロセスの詳細については、 iSeries ナビゲーターのオンライン・ヘルプを使用してください。

権限の管理を単純化するには、権限リストを使用して、同じ要件を持つオブジェクトをグループ化してください。その後、リスト上の個々のオブジェクトに対する権限を付与する代わりに、権限リストに対する共通権限、グループ・プロファイル権限、およびユーザー・プロファイル権限を付与できます。システムは権限リスト別に保護されるすべてのオブジェクトを同じ仕方で処理しますが、リスト全体に対するさまざまな権限をさまざまなユーザーに付与することができます。

権限リストを使用すると、オブジェクトの復元時に権限を再確立しやすくなります。権限リストを使用してオブジェクトを保護すると、復元プロセスの際にオブジェクトは自動的にリストにリンクされます。グループまたはユーザーに対して、権限リスト (*AUTLMGT) を管理する権限を付与することができます。権限リストを使用して管理を行うと、他のユーザーをリストに追加したりリストから除去したりでき、またそれらのユーザーに関する権限を変更できます。

推奨事項:

- 保護する必要があり、セキュリティー要件が同じであるオブジェクトの場合は、権限リストを使用してください。権限リストを使用すると、権限を個別に考慮するのではなくカテゴリーとして考慮できるようになります。また権限リストを使用すると、システム上のオブジェクトの復元や権限の監査を容易に行えます。
- 権限リスト、グループ権限、個別権限を組み合わせて、体系を込み入ったものにすることは避けてください。すべての方式を同時に使用するよりも、要件に最適の方式を選択してください。

ライブラリー記述用紙のグループ権限と個別権限を見てください。 それによって、権限リストを使用することが適切かどうか判別します。 適切な場合は、権限リスト用紙を作成し、権限リスト情報を使用してライブラリー記述用紙を更新してください。

関連概念

11 ページの『権限リスト』
グループ・プロファイルのような権限リストを使用すると、類似したセキュリティー要件を持つオブジェクトをグループ化して、そのグループをユーザーおよびユーザー権限のリストと関連付けることができます。

権限リスト・ワークシート:

システム上のアプリケーションの権限リストを作成するために、このワークシートを使用します。

表 93. 権限リスト・ワークシート

権限リスト・ワークシート					
作成者:			日付:		
指示 • 権限リストごとに、このワークシートを 1 枚ずつ作成します。 • このワークシートを使用して、リスト、およびリストにアクセスするグループと個人が保護するオブジェクトをリストします。					
権限リスト名:					
記述:					
リストが保護するオブジェクトをリストします。					
オブジェクト名	オブジェクト・タイプ	オブジェクト・ライブラリー	オブジェクト名	オブジェクト・タイプ	オブジェクト・ライブラリー

表 93. 権限リスト・ワークシート (続き)

権限リスト・ワークシート					
リストにアクセスするグループとユーザーをリストします。					
グループまたはユーザー	許可されているアクセスのタイプ	リストの管理	グループまたはユーザー	許可されているアクセスのタイプ	リストの管理

データベース・ファイルのセキュリティーの計画

このトピックでは、データベース・ファイルのセキュリティー計画を作成するのに必要なステップについて説明します。

構造化照会言語 (SQL) は、相互参照ファイルを使用して、データベース・ファイルおよびそれらの関係の記録を行います。これらのファイルは総称で SQL カタログと呼ばれます。SQL カタログに対する共通権限は *READ です。 これは、SQL インターフェースとアクセスするすべてのユーザーは、システム上のすべてのファイルの名前とテキスト記述を表示できるということです。SQL カタログは、データベース・ファイルの内容にアクセスするために必要な通常の権限には影響を与えません。

SQL または QUERY マネージャーを開始するために権限を借用する CL プログラムを使用するときは、注意が必要です。これらの QUERY プログラムは両方とも、ユーザーにファイル名の指定を許可します。したがってユーザーは、借用されたプロファイルが持つ権限の対象となるすべてのファイルにアクセスできます。

ファイル・セキュリティーの計画

データベース・ファイルにある情報は、ユーザーのシステムにとって通常最も重要な資産です。資源保護によって、ファイル内の情報を表示、変更および削除できる人を管理できます。状況に応じてファイルに対して異なる権限が必要な場合、借用権限を使用できます。システム上の重要なファイルについては、そのファイルに対する権限を持つユーザーを記録してください。

グループ権限および権限リストを使用する場合、これらの方法によって権限を持っているユーザーを、直接許可されたユーザーに加えて記録しておく必要があります。借用権限を使用する場合、借用プログラム表示 (DSPPGMADP) コマンドを使用して、特定のユーザーの権限を借用するプログラムをリストできます。

ユーザーはまた、システム上でジャーナル機能を利用して、重要なファイルに対しての活動を監視することもできます。ジャーナルの主な目的は情報の回復ですが、セキュリティー・ツールとしても使用できます。それにはファイルにアクセスした人とその方法の記録がとられています。ジャーナル表示 (DSPJRN) コマンドを使用して、定期的にジャーナル項目のサンプリングを見ることができます。

論理ファイルのセキュリティー

システム上の資源保護は、ファイルのフィールド・レベルのセキュリティーをサポートします。論理ファイルを使用して、ファイル内の特定のフィールドまたはレコードを保護することもできます。論理ファイルを使用して、ユーザーが (選択および省略ロジックを使用して) アクセスできるレコードのサブセットを指定できます。これによって、特定のユーザーがあるタイプのレコードにアクセスできないようにすることができます。

論理ファイルを使用して、ユーザーがアクセスできるレコード内のフィールドのサブセットを指定することができます。そのため、特定のユーザーがあるタイプのレコードにアクセスできないようにすることができます。論理ファイルはデータを含みません。これは、データを含む 1 つかそれ以上の物理ファイルの特定のビューです。論理ファイルで定義される情報にアクセスできるようにするには、論理ファイルおよびその関連物理ファイルの両方にデータ権限が必要です。

統合ファイル・システムのセキュリティーの計画

統合ファイル・システムは、サーバーに情報を保管し、それを表示する複数の方法を提供します。

統合ファイル・システムは i5/OS オペレーティング・システムの一部であり、ストリーム入出力操作をサポートします。統合ファイル・システムには、パーソナル・コンピューターのオペレーティング・システムや UNIX® オペレーティング・システムと類似した (かつ、互換性のある) 記憶管理方式が装備されています。統合ファイル・システムでは、階層ディレクトリー構造の観点からシステム上のすべてのオブジェクトを表示することができます。しかし、多くの場合、ユーザーにとっては、それぞれのファイル・システムの最も一般的な方法でオブジェクトが表示されます。たとえば、「従来の」オブジェクトは QSYS.LIB ファイル・システムに入っています。通常、ユーザーにとって、これらのオブジェクトはライブラリーとして表示され、QDLS ファイル・システムに含まれるオブジェクトはフォルダー内の文書として表示されます。ルート (/)、QOpenSys、およびユーザー定義のファイル・システムは、階層 (ネストされた) ディレクトリーの構造を提示します。機密保護管理者は、以下のことについて理解していなければなりません。

- システムで使用されるファイル・システム
- 各ファイル・システムに固有なセキュリティー特性

以下の情報では、統合ファイル・システムのセキュリティーに関するいくつかの一般的な考慮事項について説明します。

統合ファイル・システムのセキュリティーへのアプローチ

ルート・ファイル・システムは、他のすべてのサーバー・ファイル・システムのための基盤としての役割を果たします。ルート・ファイル・システムは、高いレベルから、システム上のすべてのオブジェクトに関する総合的な視点を提供します。サーバーに置くことができる他のファイル・システムは、各ファイル・システムの基本的な目的に応じて、オブジェクトの管理と統合に関してそれぞれ異なるアプローチを提供します。例えば、QOPT (光学式) ファイル・システムを使用すると、アプリケーションおよびサーバー (iSeries Access for Windows ファイル・サーバーを含む) は、サーバー上の CD-ROM ドライブにアクセスすることができます。同様に、QFileSvr.400 ファイル・システムを使用すると、アプリケーションはリモートのサーバー上にある統合ファイル・システム・データにアクセスすることができます。

各ファイル・システムのセキュリティー手法は、そのファイル・システムで使用可能なデータによって異なります。たとえば、QOPT ファイル・システムはオブジェクト・レベルのセキュリティーを提供しません。権限情報を CD-ROM に書き込むテクノロジーがないためです。 QFileSvr.400 ファイル・システムの場合は、アクセス制御はファイルが物理的に格納され管理されているリモート・システムで行われます。QLANSrv のようなファイル・システムの場合は、iSeries 統合 xSeries® サーバーがアクセス制御を行います。セキュリティー・モデルに違いはありますが、多くのファイル・システムは、権限変更 (CHGAUT) や所有者変更 (CHGOWN) などの統合ファイル・システム・コマンドを介して、一貫性のあるアクセス制御の管理をサポートします。

ここでは、統合ファイル・システムのセキュリティーで見落としがちないくつかのヒントを挙げます。統合ファイル・システムは POSIX 標準にできる限り近づけるよう設計されています。これにより、サーバーの権限と POSIX の許可が混合された興味深い性質になっています。

1. あるユーザーが共通権限、グループ、または権限リストで許可されている場合でも、そのユーザーが所有しているディレクトリーに対する私用権限は除去してはいけません。標準のサーバー・セキュリティー・モデルのライブラリーまたはフォルダーで処理を行っている時に所有者の私用権限を除去すると、ユーザー・プロファイルのために保管されている権限情報の量は少なくなりますが、他の操作への影響はありません。しかし、POSIX 標準がディレクトリーの許可継承を定義する方法によって、たとえ新しく作成されたディレクトリーの所有者がその親に対して別の私用権限を持っていたとしても、新しく作成されたディレクトリーの所有者はそのディレクトリーに対して、親の所有者がその親に対して持っているのと同じオブジェクト権限を持ちます。

   これは理解しにくいので、例を示します。 USERA がディレクトリー /DIRA を所有していて、USERA の私用権限が除去されたとします。 USERB は /DIRA に対して私用権限を持っています。 USERB がディレクトリー /DIRA/DIRB を作成します。 USERA は /DIRA に対してオブジェクト権限を持っていないので、 USERB は /DIRA/DIRB に対するオブジェクト権限を持ちません。 USERB は、USERB のオブジェクト権限を変更する処置をとらない限り /DIRA/DIRB を名前変更したり、削除することはできません。これは、open() API で O_INHERITMODE フラグを使用してファイルを作成したときにも起こります。 USERB がファイル /DIRA/FILEB を作成したのだとしたら、USERB はそれに対してオブジェクト権限もデータ権限も持ちません。 USERB は新しいファイルに書き込むことができません。
2. 借用権限は、大部分の物理ファイル・システムでサポートされていません。これには、ルート (/)、QOpenSys、QDLS、およびユーザー定義のファイル・システムが含まれます。
3. オブジェクトは、たとえユーザー・プロファイルの OWNER フィールドが *GRPPRF に設定されていても、そのオブジェクトを作成したユーザー・プロファイルによって所有されています。
4. 多くのファイル・システム操作では、ルート (/) ディレクトリーも含めて、パスの各コンポーネントに対して *RX データ権限が必要です。権限の問題が発生したら、ルート自体に対するユーザーの権限を検査してください。
5. 現行作業ディレクトリー (DSPCURDIR、getcwd()、など) を表示または検索するには、パス内の各コンポーネントに対する *RX データ権限が必要です。しかし、現行作業ディレクトリー (CD、chdir()、など) の変更に必要なのは、 各コンポーネントに対する *X データ権限のみです。したがって、現行作業ディレクトリーを特定のパスに変更するとそのパスを表示できないことがあります。
6. COPY コマンドの意図は、オブジェクトを複写することです。新しいファイルでの権限設定は、所有者以外は元のファイルと同じです。しかし、CPYTOSTMF コマンドの意図は、単純にデータを複写することです。新しいファイルでの権限設定は、ユーザーでは制御できません。作成者 / 所有者は *RWX データ権限を持ちますが、グループおよび共通権限は *EXCLUDE です。 ユーザーは別の方法 (CHGAUT、chmod()、など) を使用して、必要な権限を割り当てる必要があります。
7. ユーザーがオブジェクトに関する権限情報を検索するためには、そのユーザーがそのオブジェクトの所有者であるか、またはオブジェクトに対する *OBJMGT オブジェクト権限を持っている必要がありま

す。これにより COPY (ターゲットのオブジェクトに同等の権限を設定するために、ソース・オブジェクトに関する権限情報を検索しなければなりません) などのように、予期しない結果が発生することがあります。

8. オブジェクトの所有者またはグループを変更するときは、ユーザーはそのオブジェクトに対する適切な権限を持っていなければならないのみならず、新しい所有者 / グループのユーザー・プロファイルに対する *ADD データ権限、 および古い所有者 / グループのプロファイルに対する *DELETE データ権限も持っていなければなりません。これらのデータ権限は、ファイル・システムのデータ権限には関係ありません。これらのデータ権限は、DSPOBJAUT コマンドによって表示でき、EDTOBJAUT コマンドによって変更できます。これはまた、新しいオブジェクトのグループ ID を設定しようとするときに、予期せず COPY を発生させます。
9. MOV コマンドでは、特に、ある物理ファイル・システムから別の物理ファイル・システムに移動するとき、あるいはデータ変換を実行するときに、権限エラーが発生することがあります。このような場合、実際には移動はコピーと削除の操作になります。したがって、MOV コマンドは、COPY コマンド (上記の 7 および 8 参照) および RMVLNK コマンドと全く同じ権限に関する考慮事項の影響を受け、さらにその他の MOV に特定の考慮事項もあります。

統合ファイル・システム API を使用すると、データ管理インターフェースを使用する場合と同様にオブジェクトへのアクセスを制限することができます。しかし、借用権限はサポートされないことに注意してください。統合ファイル・システム API は、ジョブが実行されているユーザー・プロファイルの権限を使用します。

各ファイル・システムには、独自の特殊権限要件がある場合があります。NFS サーバー・ジョブだけが、この規則の例外です。NFS (ネットワーク・ファイル・システム) サーバーは、要求時に NFS サーバーがユーザー識別 (UID) 番号を受け取ったユーザー・プロファイルで実行するよう要求します。サーバー上の権限は、UNIX® システム上の許可と同等です。許可のタイプは、(ファイルまたはディレクトリーの) 読み取りと書き込み、および (ファイルの) 実行、または (ディレクトリーの) 検索です。

許可は一組の許可ビットによって表され、ファイルまたはディレクトリーの『アクセス・モード』を構成します。『変更モード』関数である chmod() または fchmod() を使用すると、許可ビットを変更できます。また、umask() 関数を使用すると、ジョブがファイルを作成するたびにどのファイル許可ビットが設定されるかを制御できます。

統合ファイル・システムのセキュリティーに関する考慮事項:

『ルート』 (/) ファイル・システムは、サーバーに存在する 他のすべてのファイル・システムのための基盤としての役割を果たします。 ルート・ファイル・システムは、高いレベルから、 システム上のすべてのオブジェクトに関する総合的な視点を提供します。

iSeries サーバーに置くことができる他のファイル・システムは、各ファイル・システムの基本的な目的に応じて、オブジェクトの管理と統合に関してそれぞれ異なるアプローチを提供します。たとえば、QOPT (光学式) ファイル・システムを使用すると、 iSeries アプリケーションおよびサーバー (iSeries Access for Windows ファイル・サーバーを含む) は iSeries サーバー上の CD-ROM ドライブにアクセスすることができます。同様に、QFileSvr.400 ファイル・システムを使用すると、アプリケーションはリモートのiSeries サーバー上にある統合ファイル・システム・データにアクセスすることができます。QLANSrv ファイル・サーバーを使用すると、iSeries 統合 xSeries サーバーに保管されたファイルや、ネットワーク内の他の接続サーバーに保管されているファイルにアクセスすることができます。

各ファイル・システムのセキュリティー手法は、そのファイル・システムで使用可能なデータによって異なります。たとえば、QOPT ファイル・システムはオブジェクト・レベルのセキュリティーを提供しません。権限情報を CD-ROM に書き込むテクノロジーがないためです。QFileSvr.400 ファイル・システムの場

合は、ファイルが物理的に格納され管理されるリモート・システムでアクセス制御が行われます。QLANSrv のようなファイル・システムの場合は、iSeries 統合 xSeries サーバーがアクセス制御を行います。セキュリティー・モデルに違いはありますが、多くのファイル・システムは、権限変更 (CHGAUT) や所有者変更 (CHGOWN) などの統合ファイル・システム・コマンドを介して、一貫性のあるアクセス制御の管理をサポートします。

ここでは、統合ファイル・システムの複雑なセキュリティーに関連したいくつかのヒントを挙げます。統合ファイル・システムは POSIX 標準にできる限り近づけるよう設計されています。これにより、iSeries サーバーの権限と POSIX の許可が一緒に使用される場合に興味深い性質になっています。

1. あるユーザーが共通権限、グループ、または権限リストで許可されている場合でも、そのユーザーが所有しているディレクトリーに対する私用権限は除去してはいけません。標準の iSeries サーバー・セキュリティー・モデルのライブラリーまたはフォルダーで処理を行っている時に所有者の私用権限を除去すると、ユーザー・プロファイルのために保管されている権限情報の量は少なくなりますが、他の操作への影響はありません。しかし、POSIX 標準がディレクトリーの許可継承を定義する方法によって、たとえ新しく作成されたディレクトリーの所有者がその親に対して別の私用権限を持っていたとしても、新しく作成されたディレクトリーの所有者はそのディレクトリーに対して、親の所有者がその親に対して持っているのと同じオブジェクト権限を持ちます。たとえば、以下のようにすることができます。

   USERA がディレクトリー /DIRA を所有していて、USERA の私用権限が除去されたとします。 USERB は /DIRA に対して私用権限を持っています。 USERB がディレクトリー /DIRA/DIRB を作成します。 USERA は /DIRA に対してオブジェクト権限を持っていないので、 USERB は /DIRA/DIRB に対するオブジェクト権限を持ちません。 USERB は、USERB のオブジェクト権限を変更する処置をとらない限り /DIRA/DIRB を名前変更したり、削除することはできません。これは、open() API で O_INHERITMODE フラグを使用してファイルを作成したときにも起こります。 USERB がファイル /DIRA/FILEB を作成したのだとしたら、USERB はそれに対してオブジェクト権限もデータ権限も持ちません。 USERB は新しいファイルに書き込むことができません。
2. 借用権限は、大部分の物理ファイル・システムでサポートされていません。これには、『ルート』 (/)、QOpenSys、QDLS、およびユーザー定義のファイル・システムが含まれます。
3. オブジェクトは、たとえユーザー・プロファイルの OWNER フィールドが *GRPPRF に設定されていても、そのオブジェクトを作成したユーザー・プロファイルによって所有されています。
4. 多くのファイル・システム操作では、『ルート』 (/) ディレクトリーも含めて、パスの各コンポーネントに対して *RX データ権限が必要です。権限の問題が発生したら、『ルート』 (/) 自体に対するユーザーの権限を検査してください。
5. 現行作業ディレクトリー (DSPCURDIR、getcwd()、など) を表示または検索するには、パス内の各コンポーネントに対する *RX データ権限が必要です。しかし、現行作業ディレクトリー (CD、chdir()、など) の変更に必要なのは、 各コンポーネントに対する *X データ権限のみです。したがって、現行作業ディレクトリーを特定のパスに変更するとそのパスを表示できないことがあります。
6. COPY コマンドの意図は、オブジェクトを複写することです。新しいファイルでの権限設定は、所有者以外は元のファイルと同じです。しかし、CPYTOSTMF コマンドの意図は、単純にデータを複写することです。新しいファイルでの権限設定は、ユーザーでは制御できません。作成者 / 所有者は *RWX データ権限を持ちますが、グループおよび共通権限は *EXCLUDE です。 ユーザーは別の方法 (CHGAUT、chmod()、など) を使用して、必要な権限を割り当てる必要があります。
7. ユーザーがオブジェクトに関する権限情報を検索するためには、そのユーザーがそのオブジェクトの所有者であるか、またはオブジェクトに対する *OBJMGT オブジェクト権限を持っている必要があります。これにより COPY (ターゲット・オブジェクトに同等の権限を設定するために、ソース・オブジェクトに関する権限情報を検索しなければなりません) などのように、予期しない結果が発生することがあります。

8. オブジェクトの所有者またはグループを変更するときは、ユーザーはそのオブジェクトに対する適切な権限を持っていなければならないのみならず、新しい所有者 / グループのユーザー・プロファイルに対する *ADD データ権限、 および古い所有者 / グループのプロファイルに対する *DELETE データ権限も持っていなければなりません。これらのデータ権限は、ファイル・システムのデータ権限には関係ありません。これらのデータ権限は、DSPOBJAUT コマンドによって表示でき、EDTOBJAUT コマンドによって変更できます。これはまた、新しいオブジェクトのグループ ID を設定しようとするときに、予期せず COPY を発生させます。
9. MOV コマンドでは、特に、ある物理ファイル・システムから別の物理ファイル・システムに移動するとき、あるいはデータ変換を実行するときに、権限エラーが発生することがあります。このような場合、実際には移動はコピーと削除の操作になります。したがって、MOV コマンドは、COPY コマンド (上記の 7 および 8 参照) および RMVLNK コマンドと全く同じ権限に関する考慮事項の影響を受け、さらにその他の MOV に特定の考慮事項もあります。

iSeries サーバーの特定のファイル・システムについて詳しくは、当該ファイル・システムを使用するライセンス・プログラムの資料を調べてください。

ルート、QOpenSys、およびユーザー定義のファイル・システム:

ルート、QOpenSys、およびユーザー定義のファイル・システムのセキュリティー考慮事項を以下に示します。

権限の仕組み

ルート、QOpenSys、およびユーザー定義のファイル・システムは、iSeries サーバー、PC、および UNIX** のオブジェクト管理とセキュリティーの両方の機能を組み合わせて提供します。 iSeries サーバー・セッション (WRKAUT および CHGAUT) から統合ファイル・システム・コマンドを使用すると、すべての通常 iSeries サーバー・オブジェクト権限を設定することができます。こうすることにより、Spec 1170 (UNIX タイプのオペレーティング・システム) と互換性のある *R、*W、および *X 権限が組み込まれます。

注: ルート、QOpenSys、およびユーザー定義のファイル・システムは、機能的には同じものです。 QOpenSys ファイル・システムは大文字小文字の区別をします。ルート・ファイル・システムは大文字小文字の区別をしません。ユーザー定義のファイル・システムは、大文字と小文字を区別するように定義することができます。これらのファイル・システムのセキュリティー特性は同じであるため、以下のトピックでは、それらファイル・システムの名前を同じ意味で使用します。

PC セッションからルート・ファイル・システムに管理者としてアクセスすると、 以下のようなオブジェクト属性を設定することができ、PC はこれを使用して 特定のタイプのアクセスを制限することができます。

- システム
- 隠し
- アーカイブ
- 読み取り専用

これらの PC 属性は、iSeries サーバー・オブジェクト権限値に追加されるものであり、それに代わるものではありません。

ユーザーがルート・ファイル・システムのオブジェクトにアクセスしようとすると、OS/400 は、オブジェクト権限がユーザーのインターフェースから「見える」か否かに関係なく、すべてのオブジェクト権限値とオブジェクト属性を強制的に使用します。たとえば、オブジェクトの読み取り専用属性がオンに設定されているとします。PC ユーザーは、iSeries Access インターフェースからこのオブジェクトを削除することは

できません。iSeries サーバー・ユーザーが *ALLOBJ 特殊権限を持っていても、固定機能ワークステーションを持つ iSeries サーバー・ユーザーもこのオブジェクトを削除することはできません。オブジェクトを削除するには、その前に、許可ユーザーが PC 機能を使用して読み取り専用値をオフにリセットしておかなければなりません。同様に、PC ユーザーが、 オブジェクトの PC 関連セキュリティー属性を変更するための十分な OS/400 権限を持っていないことが考えられます。

iSeries サーバーで実行される UNIX タイプのアプリケーションは、 UNIX タイプのアプリケーション・プログラミング・インターフェース (API) を使用して、ルート・ファイル・システムのデータにアクセスします。UNIX タイプの API の場合では、アプリケーションは次のようなセキュリティー情報を認識し、保守することができます。

- オブジェクト所有者
- グループ所有者 (iSeries サーバー 1 次グループ権限)
- 読み取り (ファイル)
- 書き込み (内容の変更)
- 実行 (プログラムの実行またはディレクトリーの検索)
- S_ISVTX モード・ビット (制限付きの名前変更およびリンク解除属性)

システムは、これらのデータ権限を既存の iSeries サーバー・オブジェクトとデータ権限にマップします。

- Read (*R) = *OBJOPR および *READ
- Write (*W) = *OBJOPR、*ADD、*UPD、*DLT
- Execute (*X) = *OBJOPR および *EXECUTE

他のオブジェクト権限 (*OBJMGT、*OBJEXIST、*OBJALTER、および *OBJREF) の概念は、 UNIX タイプの環境には存在しません。

ただし、これらのオブジェクト権限は、ルート・ファイル・システムのすべてのオブジェクトにあるわけではありません。 UNIX スタイルの API を使用してオブジェクトを作成すると、そのオブジェクトはその親ディレクトリーからこれらの権限を継承し、以下のようになります。

- 新規オブジェクトの所有者は、親ディレクトリーの所有者と同じオブジェクト権限を持つ。
- 新規オブジェクトの 1 次グループは、親ディレクトリーの 1 次グループと同じオブジェクト権限を持つ。
- 新規オブジェクトのパブリックは、親ディレクトリーのパブリックと同じオブジェクト権限を持つ。

所有者、1 次グループ、およびパブリックに対する新規オブジェクトのデータ権限は、API のモード・パラメーターで指定されます。 オブジェクト権限のすべてが「オン」に設定されている場合、権限の振る舞いは、UNIX タイプの環境での振る舞いと同じになります。 POSIX タイプの振る舞いにする場合以外は、オブジェクト権限を「オン」にしておくのが最善です。

UNIX タイプの API を使用するアプリケーションを実行すると、システムは、オブジェクト権限が UNIX タイプのアプリケーションから「見える」か否かに関係なく、全オブジェクト権限を強制的に使用します。たとえば、権限リストの概念が UNIX タイプのオペレーティング・システムに存在しなくても、システムは権限リストの権限を強制的に使用します。

混合アプリケーション環境の場合は、1 つの環境で行った権限変更が別の環境のアプリケーションを中断しないことを確認する必要があります。

ルート、QOpenSys、およびユーザー定義のファイル・システムのセキュリティー・コマンド:

IBM は、複数のファイル・システムでオブジェクトを処理するための一組のコマンドを提供しています。

コマンド

以下のコマンドが、システム・セキュリティーに関連しています。

- 監査変更 (CHGAUD)
- 権限変更 (CHGAUT)
- 所有者変更 (CHGOWN)
- 1 次グループ変更 (CHGPGP)
- 権限表示 (DSPAUT)
- 権限処理 (WRKAUT)

さらに、UNIX タイプの API を、セキュリティーを処理するために使用できます。

権限

***RW**
読み取り/書き込み

***R** 読み取り

***WX**
読み取り / 書き込み / 実行

***W**
書き込み

***X** 実行

"ルート"・ディレクトリーに対する共通権限:

システムの出荷時には、『ルート』・ディレクトリーに対する共通権限が *ALL (全オブジェクト権限および全データ権限) になっています。

この設定により、UNIX タイプのアプリケーションが行う操作にも、一般的な iSeries サーバー・ユーザーが行う操作にも融通性と互換性が提供されます。コマンド行機能を使用できる iSeries サーバー・ユーザーは、単に CRTLIB コマンドを使用するだけで、 新規のライブラリーを QSYS.LIB ファイル・システムに作成することができます。通常、標準的な iSeries サーバーでの権限も、これを行うことができます。同様に、出荷時のルート・ファイル・システムの設定により、一般的なユーザーは、新規のディレクトリーをルート・ファイル・システムに作成することができます (これは、新規のディレクトリーを PC に作成できるのと似ています)。

機密保護管理者は、ユーザーが作成したオブジェクトを適切に保護することについてユーザーを教育する必要があります。ユーザーがライブラリーを作成するときは、ライブラリーに対する共通権限はデフォルト値の *CHANGE ではないはずです。ユーザーは、ライブラリーの内容に応じて、共通権限を *USE または *EXCLUDE のいずれかに設定する必要があります。

アプリケーション・ユーザーが、『ルート』 (/)、QOpenSys、またはユーザー定義のファイル・システムに新規ディレクトリーを作成する必要がある場合には、次のようないくつかのセキュリティー・オプションが使用できます。

- 新規ディレクトリーを作成するときに、デフォルトの権限をオーバーライドするようにユーザーを教育することができます。デフォルトでは、その直接の親ディレクトリーから権限を継承します。ルート・ディレクトリーの新規作成ディレクトリーの場合は、デフォルトで共通権限が *ALL になります。
- マスター・サブディレクトリーを『ルート』・ディレクトリーの下に作成できます。そのマスター・ディレクトリーの共通権限を、ユーザーの組織に該当する設定値に設定してください。その後に、任意の新規個人用ディレクトリーをこのマスター・サブディレクトリーに作成するようユーザーに指示します。これらの新規ディレクトリーは、その権限を継承します。
- ユーザーがオブジェクトを『ルート』・ディレクトリーに作成しないようにするために、ルート・ディレクトリーの共通権限を変更することを考えることができます。
  *W、*OBJEXIST、*OBJALTER、*OBJREF、および *OBJMGT 権限を除去して、ユーザーがオブジェクトを作成できないようにします。ただし、この変更によっていずれかのアプリケーションに問題が生じることがないかどうかを評価する必要があります。たとえば、オブジェクトを『ルート』・ディレクトリーから削除できるような UNIX タイプのアプリケーションを持つことができます。

QSYS.LIB ファイル・システムへのアクセスの制限:

この情報を使用して、QSYS.LIB ファイル・システムへのアクセスを制限できます。

ルート・ファイル・システムは傘状のファイル・システムであるため、QSYS.LIB ファイル・システムは、ルート・ディレクトリー内ではサブディレクトリーと見なされます。したがって、サーバーにアクセスするすべての PC ユーザーは、サーバー・ライブラリー (QSYS.LIB ファイル・システム) に格納されているオブジェクトを通常の PC コマンドと処置で操作することができます。たとえば、PC ユーザーは、QSYS.LIB オブジェクト (たとえば、重要なデータ・ファイルが入っているライブラリー) をシュレッダーにドラッグすることができます。

全オブジェクト権限がインターフェースから見えるかどうかに関係なく、システムは全オブジェクト権限を強制的に使用します。したがって、ユーザーは、オブジェクトに対する *OBJEXIST 権限を持っていない限り、 このオブジェクトを廃棄 (削除) することはできません。ただし、システムが、オブジェクト・セキュリティーではなくメニュー・アクセス・セキュリティーに依存している場合は、 PC ユーザーは、シュレッダーにかけることのできるオブジェクトを QSYS.LIB ファイル・システムで見つけることができます。

システムの使用が増え、アクセスに使用する方式が多様化するにつれ、やがてメニュー・アクセスのセキュリティーが十分でないことに気付くようになります。しかし、サーバーでは、ルート・ファイル・システム・ディレクトリー構造を介する QSYS.LIB ファイル・システムへのアクセスを簡単に防止することもできます。 QPWFSERVER 権限リストを使用すれば、どのユーザーが、ルート・ディレクトリーを介して QSYS.LIB ファイル・システムにアクセスできるかを制御することができます。

QPWFSERVER 権限リストに対するユーザーの権限が *EXCLUDE であれば、ユーザーは、ルート・ディレクトリー構造から QSYS.LIB ディレクトリーに入ることはできません。ユーザーの権限が *USE であれば、ユーザーはディレクトリーに入ることができます。ユーザーがディレクトリーに入るための権限を取得すると、ユーザーが QSYS.LIB ファイル・システム内のオブジェクトに対して実行するすべての処置について、通常のオブジェクト権限が適用されます。つまり、QPWFSERVER 権限リストに対する権限 は、QSYS.LIB ファイル・システム全体に対するドアのような働きをします。 *EXCLUDE 権限を持つユーザーに対しては、このドアはロックされています。 *USE 権限 (または、それより範囲の大きい権限) を持つユーザーに対しては、このドアは開いています。

多くの場合、ユーザーは、 QSYS.LIB ファイル・システムのオブジェクトをアクセスするためにディレクトリー・インターフェースを使用する必要はありません。おそらく導入先では、QPWFSERVER 権限リストに対する共通権限を *EXCLUDE に設定したい場合があります。ただし、権限リストに対する権限は、

ユーザー・ライブラリーを含め、 QSYS.LIB ファイル・システム内のすべてのライブラリーに対して、ドアを開けたり閉めたりするということを忘れないでください。このような排他を嫌がるユーザーに出会った場合は、そのユーザーの要件を個々に評価することができます。適格であれば、個々のユーザーを権限リストに明示的に認可することができます。ただし、ユーザーが QSYS.LIB ファイル・システム内のオブジェクトに対する適切な権限を持っていることを確認する必要があります。さもないと、ユーザーが不注意にオブジェクトやライブラリー全体を削除してしまう可能性があります。

注:

1. システムが出荷されるときは、QPWFSERVER 権限リストに対する共通権限は *USE になっています。
2. 個々のユーザーを明示的に認可する場合は、権限リストは、 iSeries Access ファイル・サービス機能、NetServer ファイル・サービス機能、およびサーバー間のファイル・サービス機能でしかアクセスを制御しません。この方法では、FTP、ODBC、およびその他のネットワークを介した同一ディレクトリーへのアクセスは防止されません。

ディレクトリーの保護:

ルート・ファイル・システム内のオブジェクトにアクセスするには、 そのオブジェクトへ至る全パスを読み取ります。

ディレクトリーを検索するには、そのディレクトリーに対する *X (*OBJOPR および *EXECUTE) 権限を持っていなければなりません。たとえば、次のようなオブジェクトにアクセスするとします。/companya/customers/custfile.dat

この場合、companya ディレクトリーと customers ディレクトリーへの *X 権限を持っていなければなりません。

ルート・ファイル・システムの場合は、オブジェクトとのシンボリック・リンクを作成することができます。概念的には、シンボリック・リンクはパス名の別名です。通常、絶対パス名よりも、シンボリック・リンクの方が短くて、記憶するのが容易です。しかしシンボリック・リンクは、オブジェクトへの別の物理パスは作成しません。ユーザーは、依然として、オブジェクトへの物理パスのすべてのディレクトリーとサブディレクトリーに対する *X 権限を必要とします。

ルート・ファイル・システムのオブジェクトの場合は、 QSYS.LIB ファイル・システムでライブラリー・セキュリティーを使用するのとまったく同じように、ディレクトリー・セキュリティーを使用することができます。たとえば、ディレクトリーの共通権限を *EXCLUDE に設定して、共通ユーザーがそのツリー内のオブジェクトにアクセスしないようにすることができます。

新規オブジェクトのためのセキュリティー:

新規オブジェクトを『ルート』 (/) ファイル・システムに作成すると、作成に使用したインターフェースによってそのオブジェクトの権限が決定します。

たとえば、CRTDIR コマンドをそのデフォルトを指定して使用する場合は、新規ディレクトリーは、その親ディレクトリーのすべての権限特性を継承します。その中には、私用権限、基本グループ権限、および権限リスト・アソシエーションが含まれています。以下のセクションでは、インターフェースのタイプごとに権限を決定する方法を説明します。

権限は、その直接の親ディレクトリーから継承されるものであり、ツリー内の高位のディレクトリーから継承されるものではありません。したがって、機密保護管理者としては、階層のディレクトリーに割り当てる権限を、次の 2 つの観点から見る必要があります。

- ツリー内のオブジェクトへのアクセスに対して、ライブラリー権限のような権限がどのような影響を与えているか。
- 新規作成オブジェクトに対して、ライブラリーの CRTAUT 値のような権限がどのような影響を与えているか。

推奨事項: 統合ファイル・システムを利用するユーザーに対して、ホーム・ディレクトリー (たとえば /home/usrxxx) を与えてから、PUBLIC *EXCLUDE などの適切なセキュリティーを設定してください。そうすれば、ユーザーがホーム・ディレクトリーの下に作成したすべてのディレクトリーが、これらの権限を継承するようになります。

ディレクトリー作成コマンドの使用:

CRTDIR コマンドを使用して新規のサブディレクトリーを作成するときは、 権限を指定するための次の 2 つのオプションを使用することができます。

以下は、権限を指定するための 2 つのオプションです。
- 共通権限を指定できます。共通権限は、データ権限、オブジェクト権限、またはその両方に対して付与できます。
- データ権限、オブジェクト権限、またはその両方に対して *INDIR を指定することができます。データ権限とオブジェクト権限の両方に対して *INDIR を指定すると、システムは、親ディレクトリーのすべての権限情報、たとえば、権限リスト、1 次グループ、共通権限、私用権限などを新規オブジェクトにそのままコピーします。システムは、QSYS プロファイルまたは QSECOFR プロファイルがオブジェクトに対して持っている私用権限はコピーしません。

API を使用したディレクトリー作成:

mkdir() API を使用してディレクトリーを作成するときは、 所有者、1 次グループ、および共通に関するデータ権限を指定します (*R、*W、および *X の権限マップを使用)。

システムは、親ディレクトリーの情報を使用して、所有者、1 次グループ、および共通に関するオブジェクト権限を設定します。 UNIX タイプのオペレーティング・システムはオブジェクト権限のコンセプトを持っていないため、mkdir() API は、オブジェクト権限の指定をサポートしません。別のオブジェクト権限が必要な場合は、iSeries サーバー・コマンド CHGAUT を使用することができます。しかし、いくつかのオブジェクト権限を除去すると、 UNIX タイプのアプリケーションは、予期したように機能しないことがあります。

open() または creat() API を使用したストリーム・ファイルの作成:

creat() API を使用してストリーム・ファイルを作成する際には、所有者、1 次グループ、および共通に対するデータ権限を (UNIX タイプの権限 *R、*W、および *X を使用して) 指定することができます。

システムは、親ディレクトリーの情報を使用して、所有者、1 次グループ、および共通に関するオブジェクト権限を設定します。また、open() API を使用してストリーム・ファイルを作成する場合は、これらの権限を指定することもできます。あるいは、open() API を使用する場合は、オブジェクトがその親ディレクトリーからすべての権限を継承するように指定することができます。これは、継承モードと呼ばれています。継承モードを指定すると、システムは、権限リスト、1 次グループ、共通権限、私用権限などが親権限と完全に一致しているものを作成します。このオプションは、CRTDIR コマンドに *INDIR を指定した場合と同じ働きをします。

PC インターフェースを使用したオブジェクトの作成:

creat() API を使用してストリーム・ファイルを作成できます。

creat() API を使用してストリーム・ファイルを作成する際には、所有者、1 次グループ、および共通に対するデータ権限を (UNIX タイプの権限 *R、*W、および *X を使用して) 指定することができます。

QFileSvr.400 ファイル・システム:

QFileSvr.400 ファイル・システムの場合は、ある iSeries システム (SYSTEMA) のユーザー (USERX) は、別の接続 iSeries システム (SYSTEMB) のデータにアクセスすることができます。

USERX は、クライアント・アクセス・インターフェースと類似したインターフェースを持っています。リモート iSeries サーバー (SYSTEMB) は、すべてのファイル・システムをサブディレクトリーとして持つディレクトリーとして表示されます。USERX が、このインターフェースを持つ SYSTEMB にアクセスしようとすると、SYSTEMA は USERX のユーザー・プロファイル名と暗号化されたパスワードを SYSTEMB に送信します。これと同じユーザー・プロファイルとパスワードが、SYSTEMB に存在していなければなりません。そうでない場合は、SYSTEMB がその要求を拒否します。 SYSTEMB が要求を受け入れると、USERX は、SYSTEMB にはクライアント・アクセス・ユーザーのように扱われます。同じ権限検査規則が、USERX が試行するすべての処置に適用されます。

機密保護管理者としては、QFileSvr.400 ファイル・システムが、システムに対する別のドアを表していることを知っておく必要があります。リモート・ユーザーを、ディスプレイ・パススルーによる対話式サインオンに限定することを想定することはできません。 QSERVER サブシステムを実行し、システムを別の iSeries システムに接続すると、リモート・ユーザーは、あたかもクライアント・アクセスを実行するローカル PC のユーザーのように、システムにアクセスすることができます。おそらく、システムが、QSERVER サブシステムを実行する必要のある接続を持つと考えられます。これが、適切なオブジェクト権限体系が重要であるもう 1 つの理由です。

ネットワーク・ファイル・システム:

ネットワーク・ファイル・システム (NFS) は、 NFS インプリメンテーションを持つシステムとのアクセスを行います。

NFS は、ネットワーク・システムのユーザー間で情報を共用するための業界標準方式です。主要なオペレーティング・システム (PC オペレーティング・システムを含む) の多くは、 NFS を提供しています。UNIX システム の場合、NFS は、データへのアクセスの基本方式です。 iSeries サーバーは、NFS クライアントとしても NFS サーバーとしても動作します。

NFS サーバーとして動作する iSeries システムの機密保護管理者は、 NFS のセキュリティー面について理解して管理する必要があります。推奨事項と考慮事項は、次のとおりです。

- STRNFSSVR コマンドを使用して NFS サーバーの機能を明示的に開始する必要があります。このコマンドを使用する権限を誰にもたせるかを制御します。
- NFS クライアントがディレクトリーまたはオブジェクトを使用できるようにするために、それをエクスポートします。このため、ネットワーク内の NFS クライアントがシステムのどの部分を使用できるようにするかについて、非常に個別的な制御を行うことになります。
- エクスポートするときに、どのクライアントがオブジェクトにアクセスできるかを指定することができます。クライアントの識別は、システム名または IP アドレスで行います。クライアントは、 個々の PC でも、iSeries サーバー全体でも、UNIX システムでも可能です。 NFS 用語では、クライアント (IP アドレス) はマシンと呼ばれます。

- エクスポートするとき、エクスポートされるディレクトリーまたはオブジェクトにアクセスする各マシンごとに、読み取り専用アクセスまたは読み取り/書き込みアクセスを指定することができます。多くの場合、読み取り専用アクセスを指定します。
- NFS はパスワード保護を行いません。 NFS は、システムの承認体系の中でデータ共用を行うように設計され、意図されています。ユーザーがアクセスを要求すると、サーバーはユーザーの UID を受け取ります。UID に関する考慮事項には、以下のようなことが含まれます。
  - iSeries サーバーは、同じ UID を使用してユーザー・プロファイルを探し出そうとします。一致する UID が見つかると、iSeries はユーザー・プロファイルの認証を使用します。認証は、ユーザーの権限を使用して記述するための NFS 用語です。これは、 その他の iSeries サーバー・アプリケーションにおけるプロファイル・スワップインと同じです。
  - ディレクトリーまたはオブジェクトをエクスポートするとき、ルート権限を持つプロファイルによるアクセスを許可するかどうかを指定することができます。 iSeries サーバー上の NFS サーバーは、ルート権限を *ALLOBJ 特殊権限と等価にします。ルート権限を許可しないように指定した場合は、*ALLOBJ 特殊権限でユーザー・プロファイルにマップする UID をもつ NFS ユーザーは、そのプロファイルではオブジェクトにアクセスすることができません。その代わりに、匿名アクセスが許可される場合は、要求元は匿名プロファイルにマップされます。
  - ディレクトリーまたはオブジェクトをエクスポートするとき、匿名要求を許可するかどうかを指定することができます。匿名要求は、システム上のどの UID とも一致しない UID を持つ要求です。匿名要求を許可する方を選択すると、システムは匿名ユーザーを IBM 提供の QNFSANON ユーザー・プロファイルにマップします。このユーザー・プロファイルは、特殊権限や明示権限を一切持っていません。エクスポートするとき、必要であれば、別のユーザー・プロファイルを匿名要求に指定することができます。
- システムが NFS ネットワーク、または、UID に依存する UNIX システムを持つ任意のネットワークに加入している場合は、自動的にシステムに UID を割り当てさせるのではなくて、自分でそれを管理しなければならないこともあります。 UID をネットワークの他のシステムと調整する必要があります。

  ネットワークの他のシステムとの互換性を保つために、UID を 変更しなければならないこともあります (IBM 提供のユーザー・プロファイルの場合でも同様です。ユーザー・プロファイルの UID を簡単に変更できるプログラムが使用できるようになりました。UID を変更すると、そのユーザー・プロファイルが、ルート・ディレクトリーまたは QOpenSrv ディレクトリーのいずれかに所有しているすべてのオブジェクトの UID も変更しなければなりません。 QSYCHGID プログラムは、ユーザー・プロファイルおよびすべての所有オブジェクトの中の UID を自動的に変更します。

プリンターとプリンター出力待ち行列のセキュリティーの計画

このトピックでは、プリンターとプリンター出力待ち行列のセキュリティー計画のキーポイント、この計画作業の重要性、およびこの作業を完成させるための推奨事項について取り上げます。

物理的セキュリティーの計画のプリンターの部分を検討してください。このトピックに沿って作業しながら、プリンター出力およびワークステーションのセキュリティー用紙の出力待ち行列の部分を記入してください。さらに、印刷時や印刷待機時に機密情報を保護する計画も必要です。お客様の会社が機密出力用に使用しているプリンターの物理的セキュリティーの計画を調べてください。プリンター出力待ち行列のセキュリティーの計画が完了したら、ワークステーションのセキュリティーを計画することができます。

基本的な印刷プロセスには、以下のキーポイントが関係します。

- 印刷される報告書のコピーが、スプール・ファイルまたはプリンター出力に保留されます。
- スプール・ファイルは、プリンターが使用できるようになるまで、出力待ち行列というオブジェクトに保管されます。

- スプーリングを行うと、印刷ジョブのスケジュールを立てたり、プリンターを共用したりしやすくなります。
- またスプーリングは、機密出力を保護するのにも役立ちます。

1 つまたは複数の特別な出力待ち行列を作成して機密出力を保留し、それらの出力待ち行列を表示したり管理したりできるユーザーを制限することができます。

- この特別な出力待ち行列を保護するため、以下のコマンドを使用できます。
  - 出力待ち行列記述処理 (WRKOUTQD)
  - 出力待ち行列作成 (CRTOUTQ)
  - 出力待ち行列変更 (CHGOUTQ)
- こうしたコマンドで、以下のキー・パラメーターに値を指定できます。
  - DSPDTA
  - AUTCHK
  - OPRCTL

報告書を印刷するプログラムを実行すると、通常、報告書はプリンターに直接送られません。プログラムによって、スプール・ファイルまたはプリンター出力と呼ばれる、報告書のコピーが作成されます。プリンターが使用できるようになるまで、スプール・ファイルはシステムによって出力待ち行列というオブジェクトに保管されます。出力待ち行列にプリンター出力が入っている場合は、ワークステーションで報告書を表示できます。また、出力を保留にしたり、特定のプリンターに宛先指定したりすることもできます。

スプーリングを行うと、印刷ジョブのスケジュールを立てたり、プリンターを共用したりしやすくなります。またスプーリングは、機密出力を保護するのにも役立ちます。1 つまたは複数の特別な出力待ち行列を作成して機密出力を保留し、それらの出力待ち行列を表示したり管理したりできるユーザーを制限することができます。また、機密出力が待ち行列からプリンターにいつ送信されるのか制御できます。このトピックに沿って作業しながら、プリンター出力およびワークステーションのセキュリティー用紙を完成させてください。

特別な出力待ち行列を作成する際には、セキュリティーに関係する以下のパラメーターを指定することができます。

- **ファイルの表示 (DSPDTA) パラメーター**: 出力待ち行列の DSPDTA パラメーターは、あるユーザーが別のユーザーの所有するスプール・ファイルの表示、送信、またはコピーを行えるかどうかを決定します。
- **検査権限 (AUTCHK) パラメーター:** AUTCHK パラメーターは、出力待ち行列に対するどのタイプの権限で、ユーザーが待ち行列上の全ファイルを制御できるようにするかを指定します。一部の特殊権限を有するユーザーもファイルを制御できる場合があります。
  - ***OWNER:** 出力待ち行列権限テストを通過するには、要求元に出力待ち行列に対する所有権権限がなければなりません。要求元は、出力待ち行列の所有権となるか、待ち行列所有者とグループ・プロファイルを共用するか、または所有者の権限を借用するプログラムを実行することにより、所有権権限を持つことができます。
  - ***DTAAUT:** 出力待ち行列に対して追加、読み取り、および削除の権限を持っているユーザーは、待ち行列上のすべてのスプール・ファイルを制御できます。
- **操作員制御 (OPRCTL) パラメーター:** 出力待ち行列の OPRCTL パラメーターは、*JOBCTL 特殊権限または *SYSOPR ユーザー・クラスを持つユーザーが出力待ち行列を制御できるかどうかを決定します。プロファイルが *SYSOPR ユーザー・クラスで作成されたこと、および特殊権限パラメーターが *USRCLS に設定されて変更されていないことが条件です。

ユーザーが出力待ち行列にあるスプール・ファイルに対して実行できる機能を決定するには、出力待ち行列パラメーター、出力待ち行列に対するユーザー権限、およびユーザーの特殊権限を一緒に使用します。スプール・ファイルで以下の印刷機能を実行できます。

- スプール・ファイルを待ち行列に追加する。
- スプール・ファイルのリストを表示する (WRKOUTQ コマンド)。
- スプール・ファイルを表示、コピー、または送信する (DSPSPLF、CPYSPLF、SNDNETSPLF、および SNDTCPSPLF コマンド)。
- スプール・ファイルを変更、削除、保留、および解放する (CHGSPLFA、DLTSPLF、HLDSPLF、および RLSSPLF コマンド)。
- 出力待ち行列を変更、消去、保留、および解放する (CHGOUTQ、CLROUTO、HLDOUTQ、および RLSOUTQ コマンド)。

印刷コマンドに関する詳細は、「*iSeries 機密保護解説書*」の『付録 D』の以下の表を参照してください。

『出力待ち行列コマンド』

『スプール・ファイル・コマンド』

『書き出しプログラム・コマンド』

スプール・ファイルのセキュリティー

スプール・ファイルは、システム上の特殊なタイプのオブジェクトです。スプール・ファイルを表示および操作するための権限を、直接認可したり取り消したりすることはできません。スプール・ファイルに対する権限は、スプール・ファイルを保留している出力待ち行列上のいくつかのパラメーターによって、制御されています。

スプール・ファイルを作成するには、ユーザーはそのファイルの所有者でなければなりません。ユーザーは、出力待ち行列の権限が定義方法には関係なく、所有しているスプール・ファイルを表示および操作することができます。新しい項目を出力待ち行列に追加するには、*READ 権限を持っていなければなりません。出力待ち行列に対する権限が除去されても、スプール・ファイル処理 (WRKSPLF) コマンドを使用して、出力待ち行列上のユーザー所有の項目にアクセスすることができます。

システム上で印刷される情報のほとんどは、印刷を待機している間は出力待ち行列でスプール・ファイルとして保管されます。システム上で出力待ち行列のセキュリティーを制御しないと、許可されていないユーザーが、印刷待ちの機密情報の表示、印刷、およびコピーをする可能性があります。

機密出力を保護する方法の 1 つは、特殊な出力待ち行列を作成することです。機密出力をその出力待ち行列に送信し、出力待ち行列上でスプール・ファイルを表示および操作できる人を制御してください。出力の宛先を決定するために、システムはプリンター・ファイル、ジョブ属性、ユーザー・プロファイル、ワークステーション装置記述、および印刷装置 (QPRTDEV) システム値を調べます。詳しくは、『出力待ち行列またはプリンターへの印刷の制御』を参照してください。

デフォルト値が使用される場合、プリンターで使用されるシステム値 QPRTDEVで指定されたプリンター装置のデフォルト出力待ち行列が使用されます。

出力待ち行列用のセキュリティー・パラメーターは、出力待ち行列作成 (CRTOUTQ) コマンド または出力待ち行列変更 (CHGOUTQ) コマンドを使って指定することができます。出力待ち行列用のセキュリティー・パラメーターは、出力待ち行列記述処理 (WRKOUTQD) コマンドを使用して表示することができます。

重要: *SPLCTL 特殊権限を持つユーザーは、出力待ち行列の定義方法に関係なく、すべての項目のすべての機能を実行できます。出力待ち行列のいくつかのパラメーターによって、*JOBCTL 特殊権限を持つユーザーは、その出力待ち行列上の項目の内容を表示することができます。 *SPLCTL を持つユーザーは、iASP グループに対する権限を持たない場合は iASP 上のスプール・ファイルの操作、表示、または使用ができません。ユーザーは、1 次 iASP 装置記述に対して *EXECUTE 権限が必要です。

以下の題材に関する詳細は、「*iSeries 機密保護解説書*」の第 6 章『印刷』を参照してください。

『出力待ち行列のデータ表示 (DSPDTA) パラメーター』

『出力待ち行列の検査権限 (AUTCHK) パラメーター』

『出力待ち行列の操作員制御 (OPRCTL) パラメーター』

『印刷のために必要な出力待ち行列およびパラメーター権限』

例: 出力待ち行列

以下に、異なる要求を満たすために、出力待ち行列のセキュリティー・パラメーターを設定する例を示します。

- 汎用出力待ち行列を作成してください。すべてのユーザーは、すべてのスプール・ファイルを表示することが許可されます。システム操作員は、待ち行列の管理およびスプール・ファイルの変更が許可されます。`CRTOUTQ OUTQ(QGPL/GPOUTQ) DSPDTA(*YES) OPRCTL(*YES) AUTCHK(*OWNER) AUT(*USE)`
- アプリケーションの出力待ち行列を作成してください。グループ・プロファイルの GRPA メンバーだけが、出力待ち行列の使用を許可されます。出力待ち行列のすべての許可されたユーザーは、すべてのスプール・ファイルの表示が許可されています。システム操作員は出力待ち行列の処理を許可されていません。`CRTOUTQ OUTQ(ARLIB/AROUTQ) DSPDTA(*NO) OPRCTL(*NO) AUTCHK(*OWNER) AUT(*EXCLUDE)CHGOBJOWN OBJ(ARLIB/AROUTQ) OBJTYP(*OUTQ) USER(GRPA) AUT(*CHANGE)`
- ユーザー・プロファイルと権限についての情報を印刷する時に機密保護担当者が使用する、セキュリティー出力待ち行列を作成してください。出力待ち行列は、QSECOFR プロファイルによって作成および所有されます。 `CRTOUTQ OUTQ(QGPL/SECOUTQ) DSPDTA(*OWNER) AUTCHK(*DTAAUT) OPRCTL(*NO) AUT(*EXCLUDE)` システム上の機密保護担当者が、*ALLOBJ 特殊権限を持っていても、SECOUTQ 出力待ち行列上の他のユーザーのファイルを表示、コピー、送信、または移動することはできません。
- 機密ファイルおよび文書を印刷するユーザーによって共用される、出力待ち行列を作成してください。ユーザーは自分のスプール・ファイルのみ処理できます。システム操作員はスプール・ファイルを処理できますが、他のユーザーのスプール・ファイルを表示、コピー、送信、または移動することはできません。 `CRTOUTQ OUTQ(QGPL/CFOUTQ) DSPDTA(*OWNER) AUTCHK(*OWNER) OPRCTL(*YES) AUT(*USE)`

詳しくは、『プリンター出力待ち行列の保護』を参照してください。

必要なワークシート: プリンター出力待ち行列のセキュリティー・ワークシート

プリンター出力待ち行列のセキュリティー・ワークシート:

プリンター出力待ち行列のセキュリティーの一部として、このワークシートを完成させてください。

表 94. プリンター出力待ち行列およびワークステーションのセキュリティー・ワークシート

プリンター出力待ち行列およびワークステーションのセキュリティー・ワークシート	
作成者:	日付:
指示 • 特殊な保護が必要なワークステーションまたは出力待ち行列があれば、このワークシートに項目を作成します。	
制限付き出力待ち行列のパラメーターのリスト	

表 94. プリンター出力待ち行列およびワークステーションのセキュリティー・ワークシート (続き)

プリンター出力待ち行列およびワークステーションのセキュリティー・ワークシート				
出力待ち行列名	出力待ち行列ライブラリー	ファイルの表示 (DSPDTA)	検査する権限 (AUTCHK)	操作員制御 (OPRCTL)
機密保護担当者のワークステーション: システム値 QLMTSECOFR を yes に設定して機密保護担当者を特定のワークステーションに制限する場合は、機密保護担当者と *ALLOBJ 権限を持つすべてのユーザーに許可されたワークステーションを以下にリストする。				
制限されているワークステーションの権限を下にリストする				
ワークステーション名	権限が与えられているグループまたはユーザー (*CHANGE 権限)			
注: 制限されたワークステーションの共通権限は、*EXCLUDE に設定されていなければなりません。				

ワークステーション資源のセキュリティーの計画

プリンターおよびプリンター出力のセキュリティーの計画を立てたら、 このトピックを使用してワークステーションのセキュリティーの計画を立てることができます。

物理的セキュリティーの計画の際に、ロケーションが原因でセキュリティーのリスクが生じるワークステーションをリストしました。この情報を使用して、制限する必要のあるワークステーションを判別してください。

これらのワークステーションを使用するユーザーに、特にセキュリティーに注意するよう促すことができます。これらのユーザーがワークステーションから離れる際には必ずサインオフする必要があります。セキュリティー・ポリシーの中に、無防備なワークステーションのサインオフ手順に関する決定事項を記録することもできます。これらのワークステーションで実行できる機能を制限して、リスクを最小限にとどめることもできます。

ワークステーションでの機能を制限する最も簡単な方式は、限定された機能を持つユーザー・プロファイルにしか、その機能を使用できないように制限することです。機密保護担当者権限または保守権限を持つユーザーがサインオンできるワークステーションを制限することもできます。 QLMTSECOFR システム値を使用してこの処理を行うと、機密保護担当者権限を持つユーザーは、特別に許可されたワークステーションだけにサインオンできます。

出力待ち行列およびワークステーションのセキュリティー用紙のワークステーションの部分を作成してください。また、資源保護の推奨事項のリストを検討して、資源保護の計画を単純かつ完全なものにする必要もあります。例および推奨事項の検討が完了したら、アプリケーションの導入の計画を開始することができます。

「ワークステーションのセキュリティー」ワークシート:

ワークステーションのセキュリティー計画を作成する際には、このワークシートを完成してください。

表 95. 「ワークステーションのセキュリティー」ワークシート

「ワークステーションのセキュリティー」ワークシート	
作成者:	日付:
指示 • このワークシートには、特殊な保護が必要なワークステーションに関する項目を作成します。	
機密保護担当者のワークステーション: 機密保護担当者のワークステーションを特定のものに制限する場合 (システム値 QLMTSECOFR は「はい」)、機密保護担当者および *ALLOBJ 権限を持つすべてのユーザーに許可されるワークステーションを下にリストします。	
制限されているワークステーションの権限を下にリストする:	
ワークステーション名	権限が与えられているグループまたはユーザー (*CHANGE 権限)
注: 制限されたワークステーションの共通権限は、*EXCLUDE に設定されていなければなりません。	

プログラマーのためのセキュリティーの計画

プログラマーの存在は、機密保護担当者にとって問題となります。 プログラマーは持っている知識によって、注意深く設計されなかったセキュリティー手順をバイパスすることができます。

プログラマーはセキュリティーをバイパスして、テストに必要なデータにアクセスできます。また、システム資源を割り当てる通常の手順を無視して、自分のジョブをより良いパフォーマンスで達成できるようにすることもできます。プログラマーにとっては、セキュリティーも、アプリケーション・テストのような、ジョブが要求するタスクを行う上での妨害と思える場合がよくあります。しかし、システム上でプログラマーに多くの権限を与えすぎると、責任分割というセキュリティーの原則から外れることになります。また、プログラマーが許可されていないプログラムを導入することを可能にしてしまいます。

アプリケーション・プログラマーの環境を設定するための指針:

- プログラマーにはすべての特殊権限を与えないでください。しかし、プログラマーに特殊権限を与える必要がある場合には、そのプログラマーに割り当てられたジョブまたはタスクを実行するのに必要な特殊権限のみを与えてください。
- QPGMR ユーザー・プロファイルを、プログラマーのためのグループ・プロファイルとして使用しないでください。テスト・ライブラリーを使用して、プロダクション・ライブラリーへのアクセスを防止してください。
- プログラマー・ライブラリーを作成して、テスト用に、選択したプロダクション・データをプログラマー・ライブラリーにコピーする権限を借用するプログラムを使用してください。
- 対話式パフォーマンスが問題である場合は、プログラムの作成がバッチでのみ行われるようコマンドを変更することを考慮してください。CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM)
- アプリケーションまたはプログラム変更をテスト・ライブラリーからプロダクション・ライブラリーに移動する前に、アプリケーション機能のセキュリティー監査を実行してください。
- アプリケーションを開発する際には、グループ・プロファイル手法を使用してください。すべてのアプリケーション・プログラムをグループ・プロファイルに所有させてください。アプリケーション上で作業するプログラマーをグループのメンバーにし、プログラマー・ユーザー・プロファイルを定義して、グループが新しく作成された任意のオブジェクト (OWNER(*GRPPRF)) を所有できるようにします。プ

ログラマーがあるプロジェクトから別のプロジェクトに移動する場合、プログラマーのプロファイルのグループ情報を更新できます。詳しくは、『オブジェクトのグループ所有権』を参照してください。

- アプリケーションを実行に移す場合は、そのアプリケーションの所有権を割り当てる計画を立ててください。実行するアプリケーションに加えられる変更を制御するには、プログラムを含むすべてのアプリケーション・オブジェクトが、アプリケーションに指定されたユーザー・プロファイルによって所有されていなければなりません。

  アプリケーション・オブジェクトは、プログラマーが所有すべきではありません。実稼働環境においてプログラマーによるオブジェクトへのアクセスが全く制御されなくなってしまうからです。アプリケーションを所有するプロファイルは、そのアプリケーションに責任のある個人のプロファイルであるか、アプリケーションの所有者として特別に作成されたプロファイルです。

ソース・ファイルの管理

ソース・ファイルは、ユーザーのシステム保全性にとって重要です。ユーザーがカスタム作成のアプリケーションを開発または入手した場合、ソース・ファイルは会社の貴重な資産です。ソース・ファイルは、システム上の他の重要ファイルと同様に保護する必要があります。独立したライブラリーにソース・ファイルを入れ、これらのファイルを更新して実行に移すことができるユーザーを管理するようにしてください。

システム上でソース・ファイルが作成されたとき、デフォルトの共通権限は *CHANGE で、これによってすべてのユーザーはすべてのソース・メンバーを更新できるようになります。デフォルトでは、ソース・ファイルの所有者または *ALLOBJ 特殊権限を持つユーザーだけがメンバーの追加や除去を行うことができます。多くの場合、ソース物理ファイルのデフォルトの権限は変更する必要があります。新しいメンバーを追加するには、アプリケーション上で作業するプログラマーは、ソース・ファイルに対する *OBJMGT 権限が必要です。ソース・ファイルが被制御ライブラリーにある場合、共通権限は *USE または *EXCLUDE に引き下げられる場合があります。

システム・プログラマーまたは管理者のセキュリティーの計画

大半のシステムでは、ハウスキーピング機能の責任を持つ人がいます。この責任者はシステム資源、特にディスク記憶装置の使用を監視し、使用していないオブジェクトを定期的に除去してスペースを解放するようにします。システム上のすべてのオブジェクトを監視するために、システム・プログラマーは広範な権限を必要とします。しかし、これらのオブジェクトの内容を見る必要はありません。

借用権限を使用して、システム・プログラマーに (ユーザー・プロファイルで特殊権限を与える代わりに) 画面コマンドのセットを提供することができます。

ネットワーク・セキュリティーの計画

非トラステッド・ネットワークに接続するときは、ネットワーク・レベルで実装するセキュリティー措置も含め、セキュリティー・ポリシーに包括的なセキュリティー機構を記述することが必要です。

ファイアウォールのインストールは、包括的なネットワーク・セキュリティー措置を展開するには、最良の方法の 1 つです。さらに、インターネット・サービス・プロバイダー (ISP) は、ネットワーク・セキュリティー計画において重要な役割を果たすことが可能であり、またそうすべきでもあります。ネットワーク・セキュリティー機構では、ISP ルーター接続のフィルター規則やパブリック・ドメイン・ネーム・サービス (DNS) 対策など、インターネット・サービス・プロバイダー (ISP) が提供するセキュリティー措置の内容について概要を示すことが必要です。ご使用の ISP を定期的に確認して、セキュリティー措置が継続的にアップグレードされていることを確かめます。そのようにすることは、セキュリティー計画を最新のものに保つのにも役立ちます。

ファイアウォールは確かに、総合セキュリティー計画における中心的な防御ラインとなりますが、それが唯一の防御ラインというわけではありません。インターネット上のセキュリティー・リスクはさまざまなレベルで発生するため、これらのリスクに対しては多重階層による防御が可能なセキュリティー措置を講じる必要があります。

ファイアウォールによってある種のアタックからは十分に保護されていても、ファイアウォールはセキュリティー・ソリューション全体の一部でしかありません。たとえば、SMTP メール、FTP、および TELNET のようなアプリケーションを介してインターネット上に送信するデータを、ファイアウォールは必ずしも保護することはできません。このデータを暗号化しない限り、インターネット上の誰でもが、データが宛先に届くまでにこのデータにアクセスすることができます。

ネットワーク・セキュリティー・オプションの選択

一般に、無許可アクセスに対するガードであるネットワーク・セキュリティー・ソリューションは、保護を提供するファイアウォール技術に依存しています。システムを保護するために、フル装備のファイアウォール製品を使用することも、i5/OS TCP/IP インプリメントの一環として、特定のネットワーク・セキュリティー・テクノロジーを有効にすることもできます。この実装は、パケット・ルール機能 (IP フィルター操作と NAT を含む) および HTTP for iSeries Proxy サーバー機能から成り立っています。

パケット・ルール機能とファイアウォールのどちらを使用するかは、ネットワーク環境、アクセス要件、およびセキュリティー・ニーズによって異なります。システムや内部ネットワークをインターネットや非トラステッド・ネットワークに接続する場合は、ファイアウォール製品を中心的な防御ラインとして使用することを真剣に検討すべきです。

一般にファイアウォールは、外部アクセスへのインターフェースの数が限られている、専用ハードウェアとソフトウェアからなる装置であるため、このケースではファイアウォールが望ましいでしょう。インターネットのアクセス保護のために i5/OS TCP/IP テクノロジーを使用するときは、外部アクセスにオープンなインターフェースとアプリケーションを無数にもつ汎用コンピューティング・プラットフォームを使用しています。

この違いの重要な理由はいくつかあります。たとえば、ファイアウォール専用製品は、ファイアウォール自身を構成するもの以外に他にどのような機能もアプリケーションも提供しません。したがって、アタッカーがファイアウォールを逃れてシステムへのアクセスに成功したとしても、アタッカーはたいしたことはできません。一方、システム上の TCP/IP セキュリティー機能を回避できたアタッカーは、さまざまな種類の有用なアプリケーション、サービス、およびデータにアクセスできる可能性があります。アタッカーはそれらを使用して、そのシステム自身で破滅的大破壊を行ったり、内部ネットワークの他のシステムへのアクセスを獲得したりできます。

TCP/IP セキュリティー機能の使用に対応できますか? 行おうとしているすべてのセキュリティーの選択において、コスト対利益のトレードオフに基づいて決定を下さなければなりません。ビジネスのゴールを分析して、リスクを最小化するためのセキュリティーにかけられる費用と、どの程度までそれらのリスクを負えるのかについて、見極める必要があります。次の表では、TCP/IP セキュリティー機能と完全な機能のファイアウォール装置とを比較して、それぞれどのような場合に適しているのかを示しています。この表を使用すると、ネットワークとシステムの保護を提供する際に、ファイアウォールを使用するべきか、TCP/IP セキュリティー機能を使用するべきか、あるいは両方の組み合わせを使用するべきかを判断することができます。

セキュリティー・テクノロジー	i5/OS TCP/IP テクノロジーに最適な使用方法	完全な機能のファイアウォールに最適な使用法
IP パケット・フィルター操作	• 機密データを扱う公衆 Web サーバーやイントラネット・システムなどの単一システム用に、追加の保護を行う。 • 社内イントラネットのサブネットワークを保護する。システムが残りの社内ネットワークに対するゲートウェイ (カジュアル・ルーター) として機能している場合。 • システムがゲートウェイとして機能している VPN (プライベート・ネットワーク) またはエクストラネットを介して、多少信頼性のあるパートナーとの通信を制御する。	• 社内ネットワークが接続しているインターネットまたはその他の非トラステッド・ネットワークから社内ネットワーク全体を保護する。 • トラフィックの多い大規模サブネットワークを、社内ネットワークの残りの部分から保護する。
ネットワーク・アドレス変換 (NAT)	• 非互換のアドレッシング構造を持つ 2 つの VPN (プライベート・ネットワーク) を接続できるようにする。 • 非トラステッド・ネットワークからサブネットワークのアドレスを隠す。	• インターネットまたはその他の非トラステッド・ネットワークにアクセスするクライアントのアドレスを隠す。Proxy と SOCKS サーバーの代わりとして使用する。 • インターネットのクライアントが、プライベート・ネットワークのシステムのサービスを使用できるようにする。
Proxy サーバー	中央ファイアウォールがインターネットへのアクセスを提供するときに、社内ネットワークのリモート・ロケーションで Proxy を行う。	インターネットにアクセスするときに、社内ネットワーク全体の Proxy を行う。

ネットワーク属性の計画

ネットワークに最初から NetWare サーバーがある場合、システム全体でデフォルト値を変更することによってそうしたサーバーの処理を簡単に行うことができます。

DSPNWSUSR および WRKNWSSTS などの多くのネットワーク・サーバー・コマンドを使用すると、指定のパラメーターに *NWSA を指定して、ネットワーク・サーバー属性からの情報をサーバーが使用するように指示できます。

たとえば、同じ NDS ツリーのセットにあるユーザーのほとんどを登録することを計画する場合、最初にこうしたツリーのデフォルト・リストを定義して登録を単純化できます。その後、ユーザーを登録する際に、該当のコマンド・パラメーターに *NWSA を指定して、デフォルト属性のそのリストを参照することが可能です。また、デフォルトのサーバー・リストを参照するすべてのプロファイルを手動で変更するのではなく、そのデフォルトのサーバー・リストを変更するので、ネットワーク・サーバーの追加や除去も簡単になります。

TCP/IP を実行している場合、CHGNWSA コマンドを使用して NetWare サーバーの TCP/IP 名を追加する必要があります。Novell NetWare 拡張導入機能は、この名前のリストを使用して、TCP/IP NetWare サーバ

ーを検出します。この箇所でのみ、NetWare サーバーの TCP/IP 名をサーバーは使用します。このリストで NetWare サーバーを識別すると、NetWare 拡張導入機能は、TCP/IP 名ではなく、NetWare サーバー名でサーバーを認識します。

さらに、TCP/IP ポートのデフォルト値を 20199 から他の値に変更できます。デフォルト・ポート値を変更する場合、NetWare 拡張導入機能 NLM にパラメーター /tcp=*nnnn* を指定してロードする必要があります。ここで、*nnnn* は新しいポート値です。NLM をロードしてからこの値を変更する場合、新しい値を設定した NLM をアンロードしてから再ロードしなければなりません。

こうした方法ではなく個別ユーザー・プロファイルを基礎としてこれらの属性を設定するには、CHGNWSUSRA コマンドを使用できます。Network サーバー属性は、システム保管 (SAVSYS) コマンドで保管します。Network サーバー属性は、オペレーティング・システムがインストールされるとシステムに復元されます。

Network 属性は、ローカル・システム名、デフォルトのローカル・ロケーション名、デフォルトの制御ポイント名、ローカル・ネットワーク ID、およびネットワーク・ノード・タイプについて記述します。マシンがエンド・ノードの場合には、属性にはこのシステムで使用されているネットワーク・サーバーの名前も含まれます。さらに Network 属性は、システムが HPR を使用するかどうか、または APPN に対して仮想制御装置を使用するかどうかも判別します。

ネットワーク属性変更 (CHGNETA) コマンドは、ネットワーク内のシステムの属性を設定するのに使用します。以下の属性が DISTRIB に定義されていて、こうした属性はこのエンド・ノードのネットワーク内のすべての接続に適用されます。

ネットワーク・サーバー・ユーザー属性には、グループまたはユーザー・プロファイルのネットワーク情報が保存されます。多くの管理コマンドでは、デフォルトのサーバー・タイプ、デフォルト・コンテキスト、およびデフォルトの NDS ツリーなどの、保存されている情報の一部を使用します。またネットワーク・サーバー・ユーザー属性には、NDS ツリーのリスト、および NetWare にユーザーまたはグループを登録するのを支援するためユーザー登録によって使用される関連ユーザー情報も含まれます。ネットワーク・サーバー属性変更 (CHGNWSA) コマンドを使用して、システム全体でこうした情報を同じデフォルトに設定することができます。こうした属性を個別プロファイルやグループ・プロファイルに基づいて指定して、サーバー・ユーザーを NetWare サーバーに登録するには、CHGNWSUSRA コマンドを使用します。このような属性を使用して、ユーザーを登録する NDS ツリーを指定します。

ネットワーク印刷サーバー・オブジェクトには属性があります。ネットワーク印刷サーバーは、以下の属性をサポートしています。各オブジェクトと処置のデータ・ストリーム記述を参照して、その組み合わせでサポートされる属性を判別してください。

関連情報

ネットワーク・サーバー属性の定義

ネットワーク属性の変更

ネットワーク属性 (流通) の変更

ネットワーク・サーバー・ユーザー属性

iSeries オブジェクトの属性

APPC セキュリティーの計画

この情報を使用して、拡張プログラム間通信機能 (APPC) の作動方法およびシステムにおいて APPC に適切なセキュリティーを設定する方法を理解します。

APPC を使用すると、i5/OS 上のプログラムは互換性のある通信サポートを有するプログラムと通信できます。ディスプレイ・パススルー、分散データ管理、パーソナル・コンピューター、および iSeries Access for Windows は、APPC 通信を使用できます。

ご使用のシステムが他のシステムとのネットワークに参加する場合、ご使用のシステムへの出入り口が新たに使用できるようになります。機密保護管理者は、APPC 環境におけるシステムへの入り口の制御に使用することができるオプションを知っておく必要があります。

ヒント: PC をシステム・サーバーに接続するための多くの方法は、APPC や TCP/IP などの通信に依存します。他のシステムへの接続と PC への接続の両方に関するセキュリティーの問題を必ず考えてください。ネットワークの保護を計画する際には、ユーザーのシステムに接続している PC に悪い影響を絶対に与えないようにしてください。

以下のリンクでは、追加情報が提供されています。

- APPC プログラミング
- APPC、APPN および HPR

例: 基本 APPC セッション

APPC 環境において、あるシステムのユーザーまたはアプリケーションが別のシステムへのアクセスを要求すると、 これらの 2 つのシステムはセッションをセットアップします。 セッションを確立するために、システムは 2 つの一致する APPC 装置記述をリンクしなければなりません。

SYSTEMA 装置記述のリモート・ロケーション名 (RMTLOCNAME) パラメーターは、SYSTEMB 装置記述のローカル・ロケーション名 (LCLLOCNAME) パラメーターと突き合わせされなければならず、またその逆も突き合わせされなければなりません。 2 つのシステムが APPC セッションを確立するには、SYSTEMA と SYSTEMB の APPC 装置記述におけるロケーション・パスワードが同一でなければなりません。両方で *NONE を指定するか、両方で同一の値を指定しなければなりません。

パスワードが *NONE 以外の値の場合、これらのパスワードは暗号化形式で保管され、送信されます。パスワードが一致した場合、システムはセッションを確立します。パスワードが一致しない場合、ユーザーの要求は拒否されます。

APPC 通信の基本要素

APPC は、あるシステムのユーザーが別のシステムで作業を行えるようにする機能を提供します。

要求の開始元のシステムは、**ソース・システム**、**ローカル・システム**、または**クライアント**のいずれかの名前で呼ばれます。

要求を受け取るシステムは、**ターゲット・システム**、**リモート・システム**、または**サーバー**のいずれかの名前で呼ばれます。

機密保護管理者の観点から、以下のことをしておかないと、あるシステム (SYSTEMA) のユーザーは 別のシステム (SYSTEMB) で意味のある作業を行うことができません。

- ソース・システム (SYSTEMA) にターゲット・システム (SYSTEMB) へのパスを用意しなければならない。このパスは、**APPC セッション**と呼ばれます。
- ターゲット・システムは、ユーザーを識別し、ユーザーとユーザー・プロファイルを関連付けておかなければならない。ターゲット・システムは、ソース・システムの暗号化アルゴリズムをサポートしていなければならない。

- ターゲット・システムは、適切な環境 (実行管理機能値) を持つユーザー用にジョブを開始しておかなければならない。

ターゲット・システムの機密保護管理者は、APPC ユーザーが絶対にセキュリティーに違反しないようにするための主要な責任があります。しかし、両方のシステムの機密保護管理者が一緒に作業することにより、APPC セキュリティー管理の作業はずっと簡単になります。

ターゲット・システムへの APPC ユーザーのアクセス

以降のトピックでは、APPC ユーザーがターゲット・システムに入りこむ方法を決める要素について説明します。

システムが APPC セッションを確立するときに、システムは、要求元のユーザーがターゲット・システムのドアを獲得するためのパスを作成します。 サーバーは、ユーザー ID と APPC セッション用の要求とを関連付けます。その他のいくつかの要素は、ユーザーがほかのシステムに入り込むためにしなければならないことを決定します。

システム間でのユーザー情報の送信方法:

APPC アーキテクチャーは、ユーザーに関するセキュリティー情報をソース・システムからターゲット・システムに送るための方法を 3 つ提供します。

これらの方法は、アーキテクチャー・セキュリティー値と呼ばれます。「APPC プログラミング」には、アーキテクチャー・セキュリティー値について詳しい情報が記載されています。

以下の表には、APPC アーキテクチャーのセキュリティー値が示されています。

表 96. APPC アーキテクチャーのセキュリティー値

アーキテクチャー・セキュリティー値	ターゲット・システムに設定されるユーザー ID	ターゲット・システムへのパスワード送信
None	いいえ	いいえ
Same	はい[1]	注 2 を参照
Program	はい	はい[3]

注:

1. ソース・システムは、ターゲット・システムが SECURELOC(*YES) または SECURELOC(*VFYENCPWD) を指定している場合、ユーザー ID を送信します。
2. パスワードはソース・システムによって検査済みのため、ユーザーは要求時にパスワードを入力しません。SECURELOC(*YES) および SECURELOC(*NO) の場合、ソース・システムはパスワードを送信しません。SECURELOC(*VFYENCPWD) の場合、ソース・システムは保管され暗号化されているパスワードを取り出して、そのパスワードを暗号化された形式で送信します。
3. パスワードが暗号化形式で送信されるのは、ソース・システムとターゲット・システムの両方がパスワードの暗号化をサポートしている場合です。それ以外の場合、パスワードは暗号化されません。

要求するアプリケーションが、アーキテクチャー・セキュリティー値を判別します。たとえば、SNADS は常に SECURITY(NONE) を使用します。DDM は SECURITY(SAME) を使用します。ディスプレイ・パススルーの場合、STRPASTHR コマンドのパラメーターを使用してセキュリティー値を指定します。

どの場合でも、ターゲット・システムは、ソース・システムで指定されたセキュリティー値を使用する要求を受け入れるかどうか選択します。場合によっては、ターゲット・システムが要求を完全に拒否することがあります。また、ターゲット・システムが別のセキュリティー値を強制使用する場合もあります。たとえ

ば、STRPASTHR コマンドでユーザー ID とパスワードの両方を指定すると、 要求は SECURITY(PGM) を使用します。 しかし、QRMTSIGN システム値がターゲット・システムで *FRCSIGNON であると、その場合でも「サインオン」画面が表示されます。 *FRCSIGNON 設定の場合、システムは常に SECURITY(NONE) を使用します。 これは、ユーザーが STRPASTHR コマンドでユーザー ID もパスワードも入力しないのと等価です。

ソース・システムとターゲット・システムは、データの送信前にセキュリティー値を折衝します。たとえば、ターゲット・システムが SECURELOC(*NO) を指定し、要求が SECURITY(SAME) である場合、ターゲット・システムはソース・システムに SECURITY(NONE) を使用するように命令します。ソース・システムはユーザー ID を送信しません。

ターゲット・システムにおけるユーザーのパスワードの有効期限が切れていると、ターゲット・システムはセッション要求を拒否します。これは、パスワードを送信する接続要求にのみ適用されます。以下の要求が含まれています。

- タイプ SECURITY(PROGRAM) のセッション要求。
- SECURELOC 値が *VFYENCPWD であるときの、タイプ SECURITY(SAME) のセッション要求。

ネットワーク・セキュリティーの責任分担のオプション:

ご使用のシステムがネットワークに参加するときに、ご使用のシステムに入ろうとしている ユーザーの正体の妥当性検査を他のシステムに任せるかどうか、決めておかなければなりません。

USERA が本当に USERA である (または QSECOFR が本当に QSECOFR である) ことを保証する SYSTEMA を信用するかどうか、あるいは、ユーザーにユーザー ID とパスワードをもう一度入力してもらう必要があるかどうかを決定します。

ターゲット・システムにおける APPC 装置記述のセキュア・ロケーション (SECURELOC) パラメーターは、 ソース・システムがセキュア (トラステッド) ロケーションであるかどうかを指定します。

両方のシステムが *VFYENCPWD をサポートするリリースを実行しているときに、アプリケーションで SECURITY(SAME) を使用すると、 SECURELOC(*VFYENCPWD) は追加保護を提供します。要求元は要求時にパスワードを入力しませんが、ソース・システムはユーザーのパスワードを取り出して、要求と一緒にそのパスワードを送信します。要求が正常終了するには、ユーザーが両方のシステムで同一のユーザー ID とパスワードを持っていなければなりません。

ターゲット・システムが SECURELOC(*VFYENCPWD) を指定したものの、ソース・システムがこの値をサポートしないときには、ターゲット・システムは要求を SECURITY(NONE) として処理します。

表 97. APPC セキュリティー値と SECURELOC 値を組み合わせた場合の動作方法

ソース・システム	**ターゲット・システム**	
アーキテクチャー・セキュリティー値	**SECURELOC 値**	**ジョブのユーザー・プロファイル**
None	任意の値	デフォルト・ユーザー[1]
Same	*NO	デフォルト・ユーザー[1]
	*YES	ソース・システムの要求元と同じユーザー・プロファイル名
	*VFYENCPWD	ソース・システムの要求元と同じユーザー・プロファイル名。ユーザーは、両方のシステムで同じパスワードを使用しなければなりません。

表 97. APPC セキュリティー値と SECURELOC 値を組み合わせた場合の動作方法 (続き)

ソース・システム	ターゲット・システム	
アーキテクチャー・セキュリティー値	**SECURELOC 値**	**ジョブのユーザー・プロファイル**
Program	任意の値	ソース・システムからの要求で指定されたユーザー・プロファイル。
注: 1. デフォルト・ユーザーは、サブシステム記述の通信項目で判別されます。		

TCP/IP セキュリティーの計画

TCP/IP (伝送制御プロトコル / インターネット・プロトコル) は、 すべてのタイプのコンピューターが互いに通信を行う一般的な方法です。

TCP/IP アプリケーションはインターネットの世界で広く知られ、使用されています。このトピックでは、以下のようなヒントを示します。

- TCP/IP アプリケーションがシステムで稼働しないようにする。
- TCP/IP アプリケーションがシステムで稼働するのを許可したときに、システム資源を保護する。

SecureWay には、iSeries サーバーをインターネット (非常に大規模な TCP/IP ネットワーク) またはイントラネットに接続する際のセキュリティー上の考慮事項が説明されています。iSeries サーバーは多くの TCP/IP アプリケーションをサポートすることに注意してください。システムで 1 つの TCP/IP アプリケーションを許可することを決めると、他の TCP/IP アプリケーションも許可することになるかもしれません。機密保護管理者は、TCP/IP アプリケーションの範囲と、これらのアプリケーションがセキュリティーに与える影響に注意しておく必要があります。

TCP/IP セキュリティー構成要素

ネットワーク・セキュリティーを強化し、柔軟性を向上させるいくつかの TCP/IP セキュリティー構成要素を利用することができます。

これらのテクノロジーの一部はファイアウォール製品にも見られますが、i5/OS の TCP/IP セキュリティー構成要素はファイアウォールとして使用することが目的ではありません。ただし、これらの機能を使用すると、別個のファイアウォール製品が不要になる場合もあります。また、これらの TCP/IP 機能を使用して、すでにファイアウォールを使用している環境に付加的なセキュリティーを提供できる場合もあります。

以下の構成要素を使用して、TCP/IP セキュリティーを拡張することができます。

- パケット・ルール
- HTTP Proxy サーバー
- VPN (仮想プライベート・ネットワーク)
- SSL (Secure Sockets Layer)

パケット・ルールの使用による TCP/IP トラフィックの保護:

パケット・ルールとは、IP フィルター操作とネットワーク・アドレス変換 (NAT) を組み合わせたもので、 侵入者から内部のネットワークを保護するファイアウォールのような働きをします。

IP フィルター操作によって、IP トラフィックのネットワークへの出入りを制御できます。基本的に、定義した規則に従ってパケットをフィルターにかけることでネットワークを保護します。一方、NAT では、一連の登録済み IP アドレスの背後に未登録のプライベート IP アドレスを隠すことができます。これによ

り、外部ネットワークから内部ネットワークを保護することができます。また、NAT を利用すれば、少数の登録済みアドレスで数多くのプライベート・アドレスを表せるため、IP アドレス不足の問題を緩和するのにも役立ちます。

HTTP Proxy サーバー:

HTTP プロキシー・サーバーは、 IBM HTTP Server for iSeries サーバーに付属しています。

HTTP Server は、i5/OS の一部です。プロキシー・サーバーは、Web ブラウザーから HTTP 要求を受け取り、それらの要求を Web サーバーに再送します。要求を受け取る Web サーバーは、プロキシー・サーバーの IP アドレスだけを認知し、それらの要求の発信元である PC の名前やアドレスを判別することはできません。プロキシー・サーバーは、HTTP、FTP、Gopher、および WAIS 用の URL 要求を処理することができます。

プロキシー・サーバーは、すべてのプロキシー・サーバー・ユーザーによって出された要求から戻された Web ページをキャッシュに入れます。その結果、ユーザーがページを要求すると、プロキシー・サーバーは、そのページがキャッシュに入っているかどうかチェックします。そのページがキャッシュ内にあると、プロキシー・サーバーはキャッシュ・ページを戻します。キャッシュ・ページを使用することにより、プロキシー・サーバーは Web ページの提供サービスをより迅速に行うことができます。これにより、時間のかかる可能性がある Web サーバーへの要求の数が削減されます。さらに、プロキシー・サーバーは、トラッキングの目的で、すべての URL 要求をログに記録することもできます。あとでこれらのログを調べれば、ネットワーク資源の使用および誤用をモニターすることができます。

Web アクセスを強化するため、IBM HTTP Server で HTTP プロキシー・サポートを使用することができます。PC クライアントのアドレスは、クライアントのアクセス先の Web サーバーには隠されています。つまり、プロキシー・サーバーの IP アドレスだけが認知されます。さらに、Web ページのキャッシュにより、通信帯域幅要件とファイアウォール作業負荷を減らすこともできます。

VPN (仮想プライベート・ネットワーク):

仮想プライベート・ネットワーク (VPN) を利用すれば、 インターネットなどの公衆ネットワークの既存のフレームワークの上に、専用のイントラネットをセキュアに拡張することができます。

VPN では、ネットワーク・トラフィックを制御できるだけでなく、認証やデータ・プライバシーなどの重要なセキュリティー機能を提供することもできます。 i5/OS VPN は、i5/OSのグラフィカル・ユーザー・インターフェース (GUI) である、iSeries ナビゲーターのオプションで導入可能な構成要素です。さまざまなホストとゲートウェイの組み合わせの間でセキュアなエンドツーエンド・パスを作成することができます。 i5/OS VPN は、認証方式、暗号化アルゴリズムなどの事前対策を使用して、接続の 2 端点間で送信されるデータのセキュリティーを確保します。

VPN は、TCP/IP 階層通信スタック・モデルのネットワーク層で実行されます。とくに VPN は IP セキュリティー・アーキテクチャー (IPSec) オープン・フレームワークを使用します。 IPSec は、インターネットの基本セキュリティー機能だけでなく、堅固でセキュアな仮想プライベート・ネットワークを作成できる柔軟性の高い構築ブロックも提供します。 VPN は、Layer 2 Tunnel Protocol (L2TP) VPN ソリューションもサポートしています。 L2TP 接続は、仮想回線とも呼ばれ、企業ネットワーク・サーバーを使用してリモート・ユーザーに割り当てた IP アドレスを管理できるようにすることで、コスト効率の良いリモート・ユーザー・アクセスを実現します。さらに、L2TP 接続では、システムやネットワークの保護に IPSec を使用していれば、それらへのセキュアなアクセスも提供します。

VPN がネットワーク全体に与える影響を理解することは重要です。 VPN 接続を成功させるためには、適正な計画とインプリメンテーションが欠かせません。 iSeries Information Center の『VPN』トピックを参照し、VPN の動作とその使用方法を確実に習得してください。

Secure Sockets Layer:

Secure Sockets Layer (SSL) は、 インターネットのように保護されていないネットワーク上でアプリケーションがセキュアな通信セッションを実行できるようにするための業界標準になりました。

SSL プロトコルは、通信セッションの一端または両端を認証する、クライアント・アプリケーションとサーバー・アプリケーション間のセキュアな接続を確立します。また、SSL は、クライアント・アプリケーションとサーバー・アプリケーションがやり取りするデータのプライバシーと保全性も確保します。詳しくは、『Secure Sockets Layer』を参照してください。

TCP/IP 環境の保護

このトピックでは、システムの TCP/IP 環境における機密漏れを減らすための手順に関する一般的な提案を示します。

これらのヒントは、これ以降のトピックで説明される特定のアプリケーションに対してではなく、TCP/IP 環境全体に適用されます。

- TCP/IP ポート用のアプリケーションを作成するときには、必ずアプリケーションを適切に保護してください。外部の者がそのポートを介してアプリケーションにアクセスしようと試みることを想定してください。知識のある部外者が、そのアプリケーションに Telnet での接続を試行する可能性もあります。
- システムの TCP/IP ポートの使用法をモニターします。 TCP/IP ポートに関連したユーザー・アプリケーションは、ユーザー ID やパスワードを入力しなくても、「裏口」からシステムに入ることを許してしまう恐れがあります。システムに対する十分な権限を持っている者が、TCP または UDP ポートにアプリケーションを関連付ける可能性があります。
- 機密保護管理者は、ハッカーが使用するIP スプーフィングという技法に注意してください。TCP/IP ネットワークのすべてのシステムには IP アドレスがあります。IP スプーフィングを使用する者は、システム (通常は PC) をセットアップして、既存の IP アドレスまたはトラステッド IP アドレスであるように見せかけます。このため、他の名前をかたって、ユーザーが通常接続しているシステムであるようなふりをして、システムとの接続を確立する可能性があります。

  システムで TCP/IP を実行し、しかも物理的に保護されていないネットワーク (たとえば、すべての非交換回線と事前定義リンク) に参加している場合には、IP スプーフィングに対して無防備になっています。「スプーファー」(送信偽装者)による損傷からシステムを保護するには、まず、この章におけるサインオン保護やオブジェクト・セキュリティーなどの提案を取り入れてください。また、システムに適切な補助記憶装置の制限も必ず設定してください。これにより、スプーファー (送信偽装者) がメールやスプール・ファイルでシステムをあふれさせ、操作不能するのを防ぐことができます。さらに、システムにおける TCP/IP 活動を定期的にモニターしてください。 IP スプーフィングを検出した場合には、TCP/IP のセットアップにおける弱点を発見し、調整するようにしてください。

  イントラネット (外部に直接接続する必要のない、企業のプライベート・ネットワーク・システム) の場合、再使用可能な IP アドレスを使用します。再使用可能アドレスは、プライベート・ネットワーク内での使用を意図したものです。インターネット・バックボーンは、再使用可能 IP アドレスをもつパケットを経路指定しません。このため、再使用可能アドレスは、ファイアウォール内で追加の保護層を提供します。 IP アドレスの割り当て方法と IP アドレスの範囲、および TCP/IP のセキュリティー情報については、『TCP/IP セットアップ』を参照してください。

自動的に開始する TCP/IP サーバーの制御:

機密保護管理者は、TCP/IP の開始時に自動的に 開始する TCP/IP アプリケーションを制御する必要があります。

TCP/IP 開始コマンド

TCP/IP を開始するには、2 つのコマンドを使用できます。それぞれのコマンドごとに、システムは別々の方法を使用して、開始するアプリケーションまたはサーバーを判別します。

STRTCP *TCP/IP 開始*
システムは、AUTOSTART(*YES) が指定されているすべてのサーバーを開始する。セキュリティー上の推奨事項:

- 自動開始設定を変更できるユーザーを制御するために、注意深く *IOSYSCFG 特殊権限を割り当てる。
- STRTCP コマンドを使用できる権限を持つユーザーを注意深く制御する。このコマンドのデフォルトの共通権限は *EXCLUDE です。
- サーバーの AUTOSTART 値を変更しようとするユーザーをモニターするために、サーバー名属性変更コマンド (CHGTELNA など) 用のオブジェクト監査をセットアップする。

STRTCPSVR *TCP/IP サーバー開始*
開始すべきサーバーを指定するためにパラメーターを使用する。このコマンドの出荷時のデフォルトは、全サーバーの開始です。

セキュリティー上の推奨事項:

- コマンド・デフォルト変更 (CHGCMDDFT) コマンドを使用して、特定のサーバーだけを開始するように STRTCPSVR コマンドをセットアップする。これにより、ユーザーが他のサーバーを開始できないようになるわけではありません。しかし、コマンドのデフォルトを変更することにより、ユーザーが誤ってすべてのサーバーを開始してしまう可能性が低くなります。たとえば、`CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')` というコマンドを使用すれば、Telnet サーバーだけが開始するようにデフォルトが設定されます。

  注: デフォルト値を変更するとき、1 つのサーバーだけを指定できます。定期的に使用するサーバー、または機密漏れの原因になる可能性が最も低いサーバー (たとえば TFTP) を選択してください。
- STRTCPSVR コマンドを使用できる権限を持つユーザーの制御を注意深く行う。このコマンドのデフォルトの共通権限は *EXCLUDE です。

表 98.

サーバー	デフォルト値	ユーザーの値
Telnet	AUTOSTART(*YES)	
FTP (ファイル転送プロトコル)	AUTOSTART(*YES)	
BOOTP (ブートストラップ・プロトコル)	AUTOSTART(*NO)	
TFTP (Trivial File Transfer Protocol)	AUTOSTART(*NO)	
REXEC (リモート実行サーバー)	AUTOSTART(*NO)	
RouteD (ルート・デーモン)	AUTOSTART(*NO)	
SMTP (Simple Mail Transfer Protocol)	AUTOSTART(*YES)	
POP (Post Office Protocol)	AUTOSTART(*NO)	
HTTP (Hypertext Transfer Protocol)[1]	AUTOSTART(*NO)	

表 98. (続き)

サーバー	デフォルト値	ユーザーの値
ICS (Internet Connection Server)	AUTOSTART(*NO)	
LPD (ライン・プリンター・デーモン)	AUTOSTART(*YES)	
SNMP (Simple Network Management Protocol)	AUTOSTART(*YES)	
DNS (ドメイン・ネーム・システム)	AUTOSTART(*NO)	
DHCP (動的ホスト構成プロトコル)	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	
注: 1. IBM HTTP Server では、CHGHTTPA コマンドを使って AUTOSTART 値を設定します。		

TCP/IP 処理の防止:

TCP/IP サーバー・ジョブは QSYSWRK サブシステムで実行されます。 システムで TCP/IP を開始するには、TCP/IP 開始 (STRTCP) コマンドを使用します。

どんな TCP/IP 処理または TCP/IP アプリケーションも実行したくない場合は、STRTCP コマンドを使用しないでください。システムは、STRTCP コマンドの共通認可が *EXCLUDE に設定された状態で出荷されます。

(たとえば、稼働率が低い時間帯に) コマンドにアクセスできる何者かが TCP/IP を開始していると思われる場合、STRTCP コマンドに関するオブジェクト監査を設定することができます。ユーザーがコマンドを実行するたびに、システムは監査ジャーナル項目を書き込みます。

アプリケーションを保護するためのセキュア・シェルの使用

セキュア・シェル (SSH) をセットアップすれば、TCP/IPネットワーク上で実行されるアプリケーションのセキュリティーを保護することができます。

TCP/IP 接続アプリケーション (Telnet、FTP など) は、プレーン・テキストでデータやパスワードをネットワークに送信します。つまり、ネットワーク上の他のユーザーによってデータやパスワードがインターセプトされ、読み取られる可能性があります。

セキュア・シェル (SSH) プロトコル・スイートは、Telnet や FTP に代わる安全な手法です。SSH ではクライアントとサーバーの両方の認証性が検証されます。ユーザー ID やパスワードを含むデータ全体が暗号化されてネットワークに伝送されます。

SSH の使用方法について、詳しくは Web サイト『Portable Utilities for i5/OS』を参照してください。

セキュリティー情報のバックアップと回復の計画

この情報では、セキュリティー情報のバックアップと回復の計画の必要性について説明します。

ユーザーのセキュリティー情報を保管することは、データの保管と同様に重要です。場合によっては、システム上にユーザー・プロファイル、オブジェクト権限、およびデータを回復させる必要があります。ユーザーのセキュリティー情報を保管しないと、ユーザー・プロファイルとオブジェクト権限を手動で再構築しなければなりません。これは時間がかかり、エラーを引き起こし、セキュリティーがリスクを負う原因となり

ます。セキュリティー情報のための適切なバックアップと回復の手順を計画するためには、情報の記憶、保管、および復元方法を理解しておく必要があります。

この表には、セキュリティー情報の保管と復元に使用するコマンドが示されています。続く節では、セキュリティー情報の保管および復元について、より詳細に説明しています。

表 99. セキュリティー情報の保管と復元用のコマンド

	使用される保管/復元コマンド				
保管/復元されるセキュリティー情報	**SAVSECDTA SAVESYS**	**SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG**	**RSTUSRPRF**	**RSTOBJ RSTLIB RSTDLO RSTCFG**	**RSTAUT**
ユーザー・プロファイル	○		○		
オブジェクト所有権[1]		○		○	
1 次グループ[1]		○		○	
共通権限[1]		○		○	
私用権限	○				○
権限リスト	○		○		
権限ホルダー	○		○		
権限リストと権限ホルダーとの関連		○		○	
オブジェクト監査値		○		○	`
機能登録情報[2]		○		○	
機能使用法情報	○		○		○

1 SAVSECDTA、SAVSYS、および RSTUSRPRF コマンドは、次のオブジェクト・タイプに対する所有権、1 次グループ、1 次グループ権限、および共通権限を保管および復元します。ユーザー・プロファイル (*USRPRF)、権限リスト (*AUTL)、および権限ホルダー (*AUTHLR) です。

2 保管/復元するオブジェクトは、QUSRSYS ライブラリーのタイプが *EXITRG の QUSEXRGOBJ です。

セキュリティー情報は、保管媒体上では、システム上とは異なる方法で保管されます。ユーザー・プロファイルを保管する際は、ユーザー・プロファイルとともに保管される私用権限情報は、権限テーブルの形式に従います。権限テーブルは、私用権限を持つ各ユーザー・プロファイルに対して構築され保管されます。セキュリティー情報の形式再設定と保管は、システムで多くの私用権限を持っている場合には、時間がかかる可能性があります。

システムを回復するには、データおよび関連したセキュリティー情報の復元が必要な場合があります。回復の通常の順序は以下のとおりです。

1. ユーザー・プロファイルおよび権限リストを復元する (RSTUSRPRF USRPRF(*ALL))。
2. オブジェクトを復元する (RSTLIB、RSTOBJ、または RSTCFG)。
3. オブジェクトに対する私用権限を復元する (RSTAUT)。

関連情報

バックアップおよび回復の手引き (PDF)

セキュリティー戦略のインプリメント

このトピックでは、セキュリティー戦略のインプリメント作業を取り上げ、それが重要な理由について説明すると同時に、インプリメンテーションに関するトピックへのリンクを提供します。

このトピックでは、セキュリティー戦略をインプリメントするのに必要な作業を概説します。新しいシステムを設定する場合は、これらのステップを順番に完了する必要があります。次のステップに進むたびに、各ステップの情報が使用されます。基本的なシステム・セキュリティーの設定には、ユーザー・セキュリティーの定義、システム・レベルのセキュリティーの設定、システム上の資源の保護、およびネットワーク・セキュリティーの設定が含まれます。以下の表は、ユーザー・セキュリティーと資源保護を設定するために、構成しなければならない個々のステップを強調しています。

始める前に

新しいシステムを導入する場合は、まず以下の作業を行ってからセキュリティーの設定を開始してください。

1. ご使用のシステム装置と装置が導入されており、適切に作動しているか確認する。システムの命名規則を使用して装置の名前を指定するよう計画していない場合は、装置の命名規則を決めるシステム値 (QDEVNAMING) を変更するまで、ワークステーションとプリンターとの接続を待ってください。『新しいシステム値の適用』には、装置をいつ接続するべきか説明されています。
2. 使用を計画しているすべてのライセンス・プログラムをロードします。

注: 資源保護およびネットワーク・セキュリティーの設定を始めるには、その前にまずユーザー・セキュリティーを設定するためのステップをすべて完了しなければなりません。

表 100. システム・セキュリティーの設定に関するステップ

ステップ	このステップの内容	使用するワークシート
ユーザー環境の設定	初期システム値とネットワーク属性の設定。	システム値選択
システム・レベルのセキュリティーの設定	追加のシステム値の設定。	 Security planner 

表 101. 資源保護の設定に関するステップ

ステップ	このステップの内容	使用するワークシート
所有権および共通権限の設定	ライブラリーとオブジェクトの所有権と共通権限の確立。	アプリケーションの導入
権限リストの作成	権限リストの作成。	権限リスト
オブジェクトとライブラリーの特定権限の設定	ライブラリーと個別オブジェクトに対するアクセス権の設定。	ライブラリー記述
プリンター出力待ち行列の保護	出力待ち行列の作成および出力の割り当てによるプリンター出力の保護。	出力待ち行列およびワークステーションのセキュリティー
ワークステーションの保護	ワークステーションの保護。	出力待ち行列およびワークステーションのセキュリティー

表 102. ネットワーク・セキュリティーの設定に関するステップ

ステップ	このステップの内容	使用する参照情報
セキュリティー情報の保管	システム値、グループ・プロファイルおよびユーザー・プロファイル、ジョブ記述、さらには資源保護情報の保管。	バックアップおよび回復の手引き
セキュリティー情報の復元	システム値、ユーザー・プロファイル、オブジェクト、権限、プログラム、権限リスト、およびオペレーティング・システムの復元。	バックアップおよび回復の手引き
ネットワーク・セキュリティーの設定	APPC、および TCP/IP アプリケーションのネットワーク・セキュリティーの設定。	 Security Planner

ユーザー環境の設定

このトピックでは、ユーザー環境をセットアップしてシステムにサインオンする方法を説明します。

ユーザー・セキュリティーの設定を始めるには、全体的なユーザー環境を設定する必要があります。SETUP メニューを使ってシステム値を設定し、独自のユーザー・プロファイルを作成します。さらに、専用保守ツール (DST) プロファイルのユーザー ID とパスワードも変更する必要があります。

以下の手順では、これらのステップを示すコマンド行画面の例が載せられています。ただし、これらの例は画面全体を示しているわけではありません。作業を完了するのに必要な情報だけが取り上げられています。

必要な用紙

『全体的なセキュリティー戦略の計画』で作成したシステム値選択ワークシートの情報を入力します。全体的な環境を設定するには、以下の作業を完了する必要があります。

1. 『システムへのサインオン』
2. 202 ページの『正しい操作援助レベルの選択』
3. 202 ページの『他のユーザーがサインオンできないようにする』
4. 203 ページの『セキュリティー用のサインオン・システム値の入力』
5. 205 ページの『新しいシステム値の適用』
6. 205 ページの『機密保護担当者プロファイルの作成』

システムへのサインオン

システム環境の設定を始めるには、システムにサインオンする必要があります。

1. コンソールで、機密保護担当者 (QSECOFR) としてサインオンします。初めてサインオンする場合は、パスワード QSECOFR を使用してください。このパスワードはシステムの出荷時に期限満了に達しているため、このパスワードを変更するようプロンプト指示されます。正常にサインオンするには、このパスワードを変更しなければなりません。
2. サインオン画面の「メニュー」フィールドに、SETUP と入力します。

注: SETUP メニューの名称は「システム、ユーザー、および装置のカスタマイズ」メニューです。この資料では、一貫して SETUP メニューと呼びます。

```
                    サイン・オン
                                        システム . . . . :
                                        サブシステム . . :
                                        表示装置 . . . . :

          ユーザー . . . . . . . . . . . .  QSECOFR
          パスワード . . . . . . . . . . .  _________
          プログラム／プロシージャー . . .  _________
          メニュー . . . . . . . . . . . .  SETUP
          現行ライブラリー . . . . . . . .  _________
```

システムへのサインオンが完了したら、正しい操作援助レベルを選択しなければなりません。

正しい操作援助レベルの選択

システムにサインオンしたら、ユーザーに適した操作援助レベルを選択できます。操作援助レベルにより、表示される画面のバージョンが決まります。多くのシステム画面には、次の 2 種類のバージョンがあります。

- 初級操作援助レベルのバージョン。情報量が少なく、技術用語は使用されていません。
- 中級操作援助レベル・バージョン。情報量が初級より多くなり、技術用語が使用されています。

特定のバージョンの画面だけに表示できるフィールドや機能があります。その場合、どのバージョンを使用するか指示されます。 1 つの操作援助レベルから別のレベルに変更するには、F21 (操作援助レベルの選択) を使用してください。F21 を使用できない画面もあります。操作援助レベルの選択が完了したら、セキュリティーの設定中に他のユーザーがシステムにサインオンできないようにしなければなりません。

他のユーザーがサインオンできないようにする

正しい操作援助レベルを選択したら、システムに他のユーザーがサインオンできないようにしなければなりません。システムの保護が可能になる前に何者かがシステムを改ざんする恐れがある場合は、別のワークステーションで誰もサインオンできないようにすることができます。これはオプションです。この処理は、一時的にセキュリティーが必要だと思う場合にのみ行ってください。

1. SETUP メニューから、F9 を押してコマンド行を表示します。
2. コマンド行で、GO DEVICESTS と入力します。
3. 画面に「装置状況タスク」メニューが表示されます。「構成状況の処理」メニューが表示される場合には、F21 (操作援助レベルの選択) を使用して、初級操作援助レベルに変更してください。
4. オプション 1 (表示装置の処理) を選択します。
5. 「表示装置の処理」画面で、使用中のもの以外のワークステーションをすべて使用不可にします。そうするには、それぞれのワークステーション名の前に 2 と入力して、Enter キーを押します。
6. F3 (終了) を 2 回押して、SETUP メニューに戻ります。
7. F12 (取り消し) を押して、コマンド行を除去します。

```
                          表示装置の処理

下のオプションを入力して，実行キーを押してください。
  1= 使用可能にする    2= 使用不能にする        5= 明細の表示   7=メッセージの表示
  8= 制御装置および回線の処理    9= 名前変更    13= 記述の変更

OPT   装置       タイプ     状況
__    DSP01       3196     使用可能
__    DSP02       3196     使用可能
__    DSP03       3196     使用可能
__    DSP04       3196     使用可能
```

装置を使用不可にすると、電源がオンになっていてもサインオン画面は表示されません。システムを停止して再始動するまでの間だけ、ワークステーションは使用不可のままになります。このステップを繰り返す必要があるかもしれません。

セキュリティー用のサインオン・システム値の入力

他のユーザーがサインオンできないようにしたら、システムにシステム値を入力する必要があります。次の手順を使用して、システム値選択用紙の「第 1 部」の情報を入力してください。

1. SETUP メニューで、オプション 1 (システム・オプションの変更) を選択します。
2. システム値選択用紙の情報を、「システム・オプションの変更」画面に入力します。画面上の選択内容を変更したくない場合は、タブ・キーを使用してスキップできます。
3. システムの開始時に日時を設定していなかった場合は、この画面上で正しい日時を入力します。
4. このページに情報を入力したら、次のページに移ります。
5. 画面の 2 ページ目に選択項目を入力し、ページ送りします。
6. 画面の 3 ページ目に選択項目を入力し、Enter キーを押します。
7. SETUP メニューが再表示されます。画面の下部に表示される次のメッセージに注意してください。 `System options successfully changed. IPL required.` (システムで IPL が必要なのは、セキュリティーのレベルを変更した場合だけです。)

以下の表は、発生し得るエラーと回復手順を示しています。結果が上記の説明と異なる場合には、これらの表を役立ててください。

表 103. 考えられるエラーと回復手順

考えられるエラー	回復手順
MAIN メニューが表示される。	F3 (終了) または F12 (取り消し) を押しました。 `GO SETUP` と入力して、再試行してください。
「終結処理オプションの変更」画面など、別の画面が表示される。	SETUP メニューで間違ったオプションを選択しました。F3 (終了) を押してメニューに戻り、再試行してください。
Enter キーを押すと、「システム・オプションの変更」画面が再表示される。	画面の下部のエラー・メッセージを参照してください。許可されていない値を入力したと思われます。詳しい情報が必要であれば、F1 (ヘルプ) を使用してください。入力する前の状態にすべての値を復元したい場合は、F5 (最新表示) を使用してください。その後、再試行します。
画面に選択項目をすべて入力し終える前に、Enter キーを押した。	システム値を変更するのに必要な回数だけ、何度でもこの画面を使用できます。 SETUP メニューでオプション 1 を選択して、前回に入力し忘れた値を入力してください。 **重要:** システムが作動可能になったら、プログラマーに相談しないままセキュリティー・レベルを変更しないでください。また、iSeries Access の使用中、あるいは他のコンピューターとの通信中には、システム名を変更しないでください。
ページ送りではなく Enter キーを押した。	SETUP メニューでオプション 1 をもう一度選択し、ページ送りを使用して 2 番目のページを表示します。選択項目を入力して、Enter キーを押します。

以下の表は、許可を受けていない者がユーザー・システムにサインオンするのをより難しくするために設定する各種の値を示しています。CFGSYSSEC コマンドを実行すると、これらのシステム値は推奨設定に設定されます。

表 104. システム値の推奨値

システム値の名前	説明	推奨設定
QAUTOCFG	システムが新規装置を自動的に構成するかどうか。	0 (いいえ)
QAUTOVRT	使用できる装置がない場合にシステムが自動的に作成する仮想装置記述の数	0
QDEVRCYACN	エラーの後で装置を再接続するときにシステムが行うこと。[1]	*DSCMSG
QDSCJOBITV	システムが、切断ジョブを終了する前に待機する時間。	120
QDSPSGNINF	ユーザーがサインオンしたときに、システムが前のサインオン活動についての情報を表示するかどうか。	1 (はい)
QINACTITV	対話式ジョブが非活動のときに、システムが処置を起こすまでに待機する時間。	60
QINACTMSGQ	QINACTITV 時間枠に達したときにシステムが行うこと。	*ENDJOB
QLMTDEVSSN	ユーザーが複数のワークステーションから同時にサインオンすることをシステムが妨げるかどうか。	1 (はい)
QLMTSECOFR	*ALLJOB または *SERVICE 特殊権限を持つユーザーは、特定のワークステーションでしかサインオンできないかどうか。	1 (はい)[2]
QMAXSIGN	間違ったサインオンの試行 (ユーザー・プロファイルかパスワードが間違っている) を連続して行うことができる最大回数。	3
QMAXSGNACN	QMAXSIGN 限界に達したときにシステムが行うこと。	3 (ユーザー・プロファイルと装置の両方を使用不可にする)

注:

1. TELNET セッションの装置記述が明示的に割り当てられている場合、システムは TELNET セッションの切断および再接続を行うことができます。
2. システム値を 1 (はい) に設定した場合、*ALLOBJ または *SERVICE 特殊権限を持つユーザーを装置に対して明示的に許可する必要があります。これを最も簡単に行う方法は、特定の装置に対する *CHANGE 権限を QSECOFR ユーザー・プロファイルに与えることです。

システム値の入力が完了したら、新しいシステム値を適用しなければなりません。

詳しくは、「*iSeries 機密保護解説書*」の『システム機密保護の構成コマンドの設定値』を参照してください。

新しいシステム値の適用

システム値を入力したら、これらの値のいくつかを適用する必要があります。システム値に加えた変更の大部分は、直ちに有効になります。しかし、システムのセキュリティー・レベルを変更すると、システムを停止して再始動するまで変更内容は有効になりません。「システム・オプションの変更」画面にすべての値を正しく入力したことを確認してから、新しい値を適用します。

注: ワークステーションをシステムにまだ接続していない場合は、接続します。システムを開始すると、「システム・オプションの変更」画面で選択した命名形式を使用して、これらの装置が自動的に構成されます。

以下の手順を使用して、システムを停止してから再始動してください。システムが始動すると、「システム・オプションの変更」画面に入力した値が有効になります。

1. コンソールにサインオン済みで、他のワークステーションがサインオンしていないことを確認します。
2. プロセッサー装置上のキーロック・スイッチが、通常位置にあることを確認します。
3. SETUP メニューで、「電源オンおよび電源オフ・タスク」オプションを選択します。
4. 「システムの即時電源遮断およびその後の電源投入」オプションを選択します。 Enter キーを押します。
5. 電源遮断要求の確認を要求する画面が表示されます。 F16 (確認) を押します。

これで、システムは自動的に停止してから再始動します。画面には数分間、何も表示されません。続いて、サインオン画面が再表示されます。

新しいシステム値の適用が完了したら、システム上に自分用の機密保護担当者プロファイルを作成しなければなりません。

機密保護担当者プロファイルの作成

システム上の機密保護担当者とは、*SECOFR ユーザー・クラスか、 または *ALLOBJ 特殊権限および *SECADM 特殊権限を持つユーザーのことです。

「システム・オプションの変更」画面のシステム値を適用したら、自分用および代理者用に、機密保護担当者のユーザー・プロファイルを作成します。今後、機密保護担当者機能を実行する際には、QSECOFR プロファイルではなく、自分のプロファイルを使用してください。

1. QSECOFR としてシステムにサインオンし、SETUP メニューを要求します。選択したシステム名がサインオン画面の右上に表示されることに注意してください。
2. SETUP メニューで「ユーザー登録の処理」オプションを選択します。「ユーザー登録の処理」画面に、システム上の現行プロファイルがリストされます。 (「ユーザー・プロファイルの処理」が表示される場合には、F21 (操作援助レベルの選択) を押して、初級操作援助レベルに変更してください。)
3. 新しいプロファイルを作成するには、「Opt」(オプション) 列に 1 (追加) と入力し、「ユーザー」列にプロファイルの名前を入力します。Enter キーを押します。
4. 「ユーザーの追加」画面で、自分にパスワードを割り当てます。
5. サンプル画面に表示されるフィールドに、自分の該当する情報を記入します。
6. 画面の次ページにページ送りします。
7. 画面の 2 ページ目に記入し、Enter キーを押します。
8. 「ユーザー登録の処理」画面の下部にある確認メッセージをチェックします。
9. F3 (終了) を押して、 SETUP メニューに戻ります。

自分用の機密保護担当者プロファイルの作成が完了したら、保守ツール・ユーザーのユーザー ID とパスワードを変更する必要があります。

割り当て済みパスワードの変更

システムを安全な状態に保つため、ユーザー・プロファイルおよび専用保守ツールの既知のパスワードを変更してください。

ユーザーのシステムに存在している可能性のあるサーバーへの既知の入り口の一部をクローズするため、以下のことを行います。

1. いまだに (ユーザー・プロファイル名と同じ) デフォルト・パスワードを使用しているユーザー・プロファイルがないことを確認する。デフォルト・パスワード分析 (ANZDFTPWD) コマンドを使用することができます。
2. 表 105 に示してあるユーザー・プロファイルとパスワードの組み合わせを使用して、システムへのサインオンを試行する。これらのパスワードは公開されているもので、システムに侵入しようとする誰もが最初に選択するものです。サインオンすることができたら、ユーザー・プロファイル変更 (CHGUSRPRF) コマンドを使用して、パスワードを推奨値に変更します。
3. 専用保守ツール (DST) を開始し、 207 ページの表 106 に示すパスワードを使用してサインオンを試行する。
4. これらのパスワードを使用して DST にサインオンできた場合は、パスワードを変更する必要がある。
5. ユーザー ID とパスワードを入力しないと、「サインオン」画面で Enter キーを押しただけではサインオンできないことを確認する。各種ディスプレイで試行してみます。「サインオン」画面で情報を入力しなくてもサインオンできる場合には、以下のいずれかを行います。
   - セキュリティー・レベルを 40 または 50 (QSECURITY システム値) に変更する。 (セキュリティー・レベルを 40 または 50 に上げると、アプリケーションの実行動作が変化する場合があります。)
   - 対話式サブシステムに対するすべてのワークステーション項目が USER(*RQD) を指定したジョブ記述を示すように変更する。

表 105. IBM 提供プロファイル用のパスワード

ユーザー識別コード	パスワード	推奨値
QSECOFR	QSECOFR[1]	機密保護管理者だけが知っている単純ではない値。**選択したパスワードを書き留め、安全な場所に保管します。**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2]、[3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

注:

1. システム出荷時は、 QSECOFR の「*パスワードの満了設定*」値が *YES に設定されています。新規システムに初めてサインオンしたときに、QSECOFR パスワードを変更しなければなりません。
2. システムはシステム機能のためにこれらのユーザー・プロファイルを必要としますが、ユーザーがこれらのプロファイルを使用してサインオンすることは許可しないでください。このパスワードは、出荷時に *NONE に設定されています。CFGSYSSEC コマンドを実行すると、システムはこれらのパスワードを *NONE に設定します。
3. TCP/IP を使用して iSeries Access for Windows を実行するには、QUSER ユーザー・プロファイルを使用可能にしておかなければなりません。

表 106. 専用保守ツール用のパスワード

DST レベル	ユーザー ID[1]	パスワード	推奨値
基本機能	11111111	11111111	機密保護管理者だけが知っている単純ではない値。[2]
全機能	22222222	22222222[3]	機密保護管理者だけが知っている単純ではない値。[2]
セキュリティー機能	QSECOFR	QSECOFR[3]	機密保護管理者だけが知っている単純ではない値。[2]
サービス機能	QSRV	QSRV[3]	機密保護管理者だけが知っている単純ではない値。[2]

注:

1. ユーザー ID が必要なのは、 オペレーティング・システムの PowerPC AS (RISC) リリースだけです。
2. サービス技術員がこのユーザー ID とパスワードを使用してサインオンする必要があった場合は、サービス技術員が離れた後で、パスワードを新規の値に変更してください。
3. 保守ツール・ユーザー・プロファイルは、最初に使用されるとすぐに有効期限が切れます。

重要: DST パスワードは、認証された装置によってのみ変更することができます。このことは、すべてのパスワードおよび対応する同一のユーザー ID にもあてはまります。認証された装置の詳細については、iSeries Information Center の『オペレーション・コンソール』のセットアップ情報を参照してください。

システム保守ツールを使用したパスワード変更

DST ではなくシステム保守ツール (SST) を使用してもパスワード変更できます。

システム保守ツール (SST) の保守ツール・ユーザー ID を管理および作成するには、 メインの SST 画面でオプション 8 (保守ツール・ユーザー ID の処理) を選択します。パスワードのリセット、特権の認可または取り消し、または保守ツール・ユーザー ID の作成に、DST を使う必要はなくなりました。

サーバー出荷時の、デフォルトのパスワードおよび有効期限切れパスワードの変更機能に制限が加えられました。つまり、保守ツール・ユーザー ID 変更 (QSYCHGDS) API から、デフォルトのパスワードや有効期限切れパスワードを持つ保守ツール・ユーザー ID を変更したり、 SST からそれらのパスワードを変更したりできなくなりました。デフォルトのパスワードや有効期限切れパスワードを持つ保守ツール・ユーザー ID は、DST からしか変更できなくなりました。設定を変更すれば、デフォルトのパスワードや有効期限切れパスワードの変更を許可することができます。また、新しい「システム保守ツール開始」(STRSST) 特権を使用して、DST にはアクセスできるが、SST へのアクセスは制限される、 保守ツール・ユーザー ID を作成することもできます。

IBM 提供のユーザー・プロファイルのパスワード変更

IBM 提供のプロファイルのいずれかでサインオンする必要がある場合は、 CHGUSRPRF コマンドを使用してパスワードを変更することができます。また、SETUP メニューのオプションを使用して、これらのパスワードを変更することもできます。システムを保護するためには、QSECOFR 以外のすべての IBM 提供プロファイルに対して、パスワードを *NONE に設定したままにしておいてください。 QSECOFR プロファイルには簡単なパスワードを使用しないでください。

```
                        弊社提供ユーザーのパスワード変更

弊社提供ユーザーの新しいパスワードを下に入力し，変更を確認するためにはもう一
  度パスワードを入力して，実行キーを押してください。

新しい機密保護担当者 (QSECOFR) パスワード  . . . . . .
  新しいパスワード（確認用） . . . . . .

新しいシステム操作員 (QSYSOPR) パスワード  . . . . . .
  新しいパスワード（確認用） . . . . . .

新しいプログラマー (QPGMR) パスワード  . . . . . .
  新しいパスワード（確認用） . . . . . .

新しいユーザー (QUSER) パスワード  . . . . . .
  新しいパスワード（確認用） . . . . . .

新しい保守 (QSRV) パスワード . . . . . .
  新しいパスワード（確認用） . . . . . .
```

追加のパスワードを変更するには、次ページ・キーを押してください。

```
                        弊社提供ユーザーのパスワード変更

弊社提供ユーザーの新しいパスワードを下に入力し，変更を確認するためにはもう一
  度パスワードを入力して，実行キーを押してください。

新しい基本保守 (QSRVBAS) パスワード  . . . . . .
  新しいパスワード（確認用） . . . . . .
```

サインオンのエラー・メッセージの変更

このトピックでは、システムに侵入を試みるハッカーを阻止するため、サインオンのエラー・メッセージを変更する方法について取り上げます。

ハッカーは、システムへの侵入の進行具合を知りたがっています。「サインオン」画面のエラー・メッセージがパスワードが正しくない、であるとハッカーは、ユーザー ID の方は正しいと想定することができます。メッセージ記述変更 (CHGMSGD) コマンドを使用して 2 つのサインオン・エラー・メッセージのテキストを変更すると、ハッカーをいらだたせることができます。下の表に推奨テキストを示します。

表 107. サインオンのエラー・メッセージ

メッセージ ID	出荷時のテキスト	推奨テキスト
CPF1107	CPF1107 – ユーザー・プロファイルのパスワードが正しくない。	サインオン情報が正しくありません。(メッセージ・テキストにメッセージ ID を組み込まないでください。)
CPF1120	CPF1120 – ユーザー *xxxxx* が存在していない。	サインオン情報が正しくありません。(メッセージ・テキストにメッセージ ID を組み込まないでください。)

システム・セキュリティーの設定

以下の情報は、システム・レベルのセキュリティーを設定する手順をガイドしています。

セキュリティー・ウィザードは、企業にとって適切なシステム設定値を使ってシステムを自動的に構成します。

セキュリティー・システム値を使用して、システムのセキュリティーを制御します。

システム値の中には、通常の操作でこれらのユーザーがシステム値を変更できないようにロックできるものもあります。

セキュリティー・ウィザード

このウィザードは、貴社に適したシステム値設定を自動的にシステムに構成できます。

セキュリティー関連のシステム値の適切な設定方法に不安がある場合や、現行のセキュリティー・ポリシーを吟味したい場合には、セキュリティー・ウィザードを実行してください。このウィザードは、貴社に適したシステム値設定を自動的にシステムに構成できます。構成を実行する方法については、多くのオプションが備えられています。

以下は、このウィザードで実行できるオプションの一部です。

- 提供された情報に基づいてご使用のシステムのシステム値を自動構成します。
- 報告書を保管して、後日システムを構成できるようにします。
- 関係するシステムの推奨システム値設定を含む報告書を印刷します。

セキュリティー・ウィザードにアクセスするには、以下のステップを行います。

1. iSeries ナビゲーターで、ご使用のシステムを選択する。
2. 「セキュリティー」を右クリックする。
3. 「構成」を選択する。

その後、セキュリティー・ウィザードを実行します。

セキュリティー・システム値の適用

セキュリティー・システム値を使用して、システムのセキュリティーを制御します。

これらの値は、4 つのグループに分かれます。

1. 汎用のセキュリティー・システム値
2. セキュリティーに関連するその他のシステム値
3. パスワードを制御するシステム値
4. 監査を制御するシステム値

お客様のビジネスに使用するセキュリティー・システム値を決めることは難しい問題です。サーバーへのセキュリティーのインプリメンテーションが初めてだったり、サーバーの稼働環境が最近変わった場合には、セキュリティー・ウィザードが値の決定に役立ちます。

システム値を入力したら、これらの値のいくつかを適用する必要があります。システム値に加えた変更の大部分は、直ちに有効になります。しかし、システムのセキュリティー・レベルを変更すると、システムを停止して再始動するまで変更内容は有効になりません。「システム・オプションの変更」画面にすべての値を正しく入力したことを確認してから、新しい値を適用します。

注: ワークステーションをシステムにまだ接続していない場合は、接続します。システムを開始すると、「システム・オプションの変更」画面で選択した命名形式を使用して、これらの装置が自動的に構成されます。

以下の手順を使用して、システムを停止してから再始動してください。システムが始動すると、「システム・オプションの変更」画面に入力した値が有効になります。

1. コンソールにサインオン済みで、他のワークステーションがサインオンしていないことを確認します。

2. プロセッサー装置上のキーロック・スイッチが、通常位置にあることを確認します。
3. SETUP メニューで、「電源オンおよび電源オフ・タスク」オプションを選択します。
4. 「システムの即時電源遮断およびその後の電源投入」オプションを選択します。
5. Enter キーを押します。電源遮断要求の確認を要求する画面が表示されます。
6. F16、「確認」を押します。これで、システムは自動的に停止してから再始動します。

画面には数分間、何も表示されません。 続いて、サインオン画面が再表示されます。 新しいシステム値の適用が完了したら、 システム上に自分用の機密保護担当者プロファイルを作成しなければなりません。

このトピックでは、以下のリンクが提供されています。
- システム・セキュリティー構成コマンドによって設定される値
- システム値ファインダー

システム値のロック・ダウン
システム値の中には、通常の操作でこれらのユーザーがシステム値を変更できないようにロックできるものもあります。

ほとんどのセキュリティー・システム値は、機密保護管理者 (*SECADM) 権限および全オブジェクト (*ALLOBJ) 特殊権限を持つユーザーのみが変更できます。通常操作の際にこれらのシステム値をこうしたユーザーでさえ変更できないようにするため、システム保守ツール (SST) および専用保守ツール (DST) には、こうしたセキュリティー値をロックするオプションがあります。

ロック・ダウン可能なシステム値のリストについては、『機密保護関連システム値のロック機能』というトピックを参照してください。

ユーザー・セキュリティーの設定
ユーザー・セキュリティーの設定には、アプリケーション・ライブラリーの導入、およびユーザー・グループとプロファイルの設定が含まれます。

このトピックでは、コマンド行インターフェースを使ってシステム上にユーザー・セキュリティーを設定するために必要な作業を概説します。以下の表は、ユーザー・セキュリティーの設定に必要な手順を示しています。

表 108. ユーザー・セキュリティーの設定に関するステップ

ステップ	このステップの内容	使用するワークシート
アプリケーションのロード	所有者プロファイルの作成。アプリケーションのロード。残りのステップを完了するためには、アプリケーション・ライブラリーとオブジェクトがシステム上にすでに存在していなければなりません。	システム値選択 アプリケーション記述
ユーザー・グループの設定	ジョブ記述、グループ・ライブラリー、およびグループ・プロファイルの作成。	ユーザー・グループ記述
グループ内のユーザー用のプロファイルの作成	個々のユーザー・プロファイルの作成	124 ページの『ユーザー・プロファイル・ワークシート』
グループの各メンバー用の個人ライブラリーの作成	個別ライブラリーの作成。	ライブラリー記述

関連概念

14 ページの『ユーザー・セキュリティー』
ユーザーの視点から見ると、セキュリティーは、ユーザーがシステム上でタスクを使用および完了する仕方に影響を与えます。

アプリケーション・ライブラリーの導入

このトピックには、 アプリケーション・ライブラリーをシステムにロードするのに必要なセキュリティー・ステップが記述されています。

システムにアプリケーション・ライブラリーをロードしてから、ユーザー・グループと個別プロファイルを設定してください。ジョブ記述とプロファイルを作成する際には、アプリケーション・オブジェクトを参照する必要があります。グループおよび個別のプロファイルを作成する前にアプリケーションをロードできない場合は、以下のような警告メッセージが表示されることがあります。

- ジョブ記述の作成時、システムで初期ライブラリーが見つかりません。
- プロファイルの作成時、システムで初期プログラムまたはメニューが見つかりません。

アプリケーション・ライブラリーをロードするまでは、ジョブ記述やプロファイルのテストを正常に行えません。

個々のアプリケーションをロードするには、以下の作業をすべて実行してください。

所有者プロファイルの作成:

この項では、ユーザー・グループを設定する前に必要な、所有者プロファイルの作成ステップについて取り上げます。

アプリケーションの所有者プロファイルを作成する前に、システムにサインオンする必要があります。

システムへのサインオン

- 所有者プロファイルを作成するには、以下のようにします。

  プロファイル
  独自のもの (*SECADM 権限が必要)

  メニュー
  MAIN
- アプリケーション・ライブラリーをロードするには、以下のようにします。

  アプリケーション・ライブラリーのロード時に機密保護担当者かアプリケーション所有者のどちらとしてサインオンすればよいか、アプリケーションの提供者に問い合わせてください。サインオンが完了したら、アプリケーションの所有者プロファイルを作成できます。

所有者プロファイルの作成

システムにサインオンしたら、アプリケーション記述を調べて、アプリケーションをロードする前にプロファイルを作成する必要があるか調べてください。プロファイルを作成するには、以下のようにします。

1. CRTUSRPRF (ユーザー・プロファイル作成) と入力して、F4 (プロンプト) を押します。
2. 「ユーザー・プロファイル作成」画面で、プログラマーかアプリケーションの提供者に指示されたとおりにフィールドに記入します。

3. F10 (追加のパラメーター) を使用してページ送りし、追加のフィールドを表示します。
4. 画面の下部のメッセージをチェックしてください。

```
          ユーザー・プロファイル作成 (CRTUSRPRF)
選択項目を入力して、Enter キーを押してください。

ユーザー・プロファイル  . . . .
ユーザー・パスワード  . . . . .  *USRPRF
パスワードを満了にセット  . . .  *NO
状況  . . . . . . . . . . . . .  *ENABLED
ユーザー・クラス  . . . . . . .  *USER
援助レベル  . . . . . . . . . .  *SYSVAL
現行ライブラリー . . . . . . . . *CRTDFT
呼び出す初期プログラム . . . . . *NONE
  ライブラリー  . . . . . .
初期メニュー  . . . . . . . . .  MAIN
  ライブラリー  . . . . . .  *LIBL
制限機能  . . . . . . . . . . .  *NO
テキスト '記述'  . . . . . . . xxxxxx の所有者
```

アプリケーションの所有者の作成が完了したら、アプリケーションのロードを始められます。

追加情報は、『グループ・プロファイルの作成』を参照してください。

アプリケーションのロード:

アプリケーション管理を使用して、アプリケーションをロードできます。

アプリケーション管理は、システムのグラフィカル・ユーザー・インターフェース (GUI) である、iSeries ナビゲーターのオプションで導入可能な構成要素です。アプリケーション管理を使用すると、システム管理者は、特定のサーバー上のユーザーおよびグループが使用できる機能またはアプリケーションを制御できます。これによって、クライアントを介してサーバーにアクセスするユーザーが使用できる機能を制御することもできます。ここで重要なことは、Windows クライアントからサーバーにアクセスする場合に、どの管理機能を使用できるようにするかを決めるのは、サーバーのユーザーであって、Windows のユーザーではない、ということです。

アプリケーションのロード後、『ユーザー・グループの設定』を行えます。

アプリケーション管理には、アプリケーションに関する追加情報があります。

ユーザー・グループの設定

ここでは、ユーザー・グループを設定するためのタスクを説明します。

このタスクでは、グループ・ライブラリー、ジョブ記述、およびグループ・プロファイルを作成します。 1 つのユーザー・グループに対してこのトピック全体の作業を行ったら、最初に戻り、それ以外のグループで同じステップを繰り返してください。

『ユーザー・グループの計画』で作成したユーザー・グループ記述用紙を使用します。

次のトピックでは、ユーザー・グループの設定手順を示します。

グループのライブラリーの作成:

この項では、ユーザー・グループのライブラリーの作成方法について取り上げます。プログラムなどのオブジェクトを保管するためにライブラリーを使用できます。

ユーザー・グループを設定する前に、独自のプロファイルを使用してシステムにサインオンします (*SECADM 権限が必要)。MAIN メニューに進み、修理を検証します。

システムへのサインオンが完了したら、ユーザー・グループのライブラリーを作成する必要があります。オブジェクト (Query プログラムなど) のライブラリーを作成し、それをグループ内で共用するように計画している場合は、まずライブラリーを作成してからグループ・プロファイルを作成してください。

1. CRTLIB (ライブラリー作成) と入力して、F4 (プロンプト) を押します。
2. 画面に入力します。ライブラリー名はグループ・プロファイル名にしてください。
3. F10 (追加のパラメーター) を押します。
4. ライブラリーの共通権限と、そのライブラリーで作成される新しいオブジェクトを記入します。
5. Enter キーを押します。確認メッセージをチェックします。

```
                        ライブラリー作成  (CRTLIB)

選択項目を入力して，実行キーを押してください。

ライブラリー  . . . . . > DPTWH
ライブラリー・タイプ  . . . . .  *PROD
テキスト ' 記述 ' . . . . . > ' 倉庫ライブラリー '


                追加のパラメーター

権限  . . . . . .  *USE
ASP 番号  . . . . . .  1
ASP 装置  . . . . . .  *ASP
作成権限  . . . . . .  *CHANGE
オブジェクト監査の作成  . . . .  *SYSVAL
```

考えられるエラー	回復
ライブラリーの説明を入力し終える前に、Enter キーを押した。	CHGLIB と入力して、F4 (プロンプト) を押します。プロンプト画面にライブラリー名を入力して、Enter キーを押します。そして、「ライブラリー変更」画面に説明を入力します。
ライブラリーに付けた名前が間違っていた。	オブジェクト名前変更 (RNMOBJ) コマンドを使用してください。

グループのジョブ記述を作成します。:

この項では、グループのジョブ記述を作成する方法を説明します。ジョブ記述には、使用するジョブ待ち行列、スケジューリング優先順位、 経路指定データ、メッセージ待ち行列の重大度、ライブラリー・リスト、 および出力情報など、特定のジョブに関連する属性のセットが含まれています。 属性によって、各ジョブをシステム上で実行する方法を決定します。

グループのライブラリーの作成が完了したら、グループごとにジョブ記述を作成することができます。

初期ライブラリー・リストに必要なライブラリーがまだシステム上にない場合は、ジョブ記述を作成する際に警告メッセージが表示されます。

1. CRTJOBD (ジョブ記述作成) と入力して、F4 (プロンプト) を押します。
2. 以下のフィールドに記入します。

ジョブ記述:
グループ・プロファイル名と同じ。

ライブラリー名:

QGPL テキスト: グループ記述

3. F10 (追加のパラメーター) を押します。
4. 「初期ライブラリー・リスト」フィールドにページ送りします。

```
                      ジョブ記述作成  (CRTJOBD)

選択項目を入力して，実行キーを押してください。

ジョブ記述  . . . . . .  DPTSM
ライブラリー  . . . . . .  QGPL
ジョブ待ち行列  . . . . . .  QBATCH
  ライブラリー  . . . . . .  *LIBL
ジョブ優先順位 (JOBQ での ) . .  5
出力優先順位 (OUTQ での ) . . .  5
印刷装置  . . . . . .  *USRPRF
出力待ち行列  . . . . . .  *USRPRF
  ライブラリー  . . . . . .
テキスト ' 記述 ' . . . . . .  販売営業
```

5. 「初期ライブラリー・リスト」フィールドの *SYSVAL の上に + (プラス符号) を入力し、値のリストを入力することを指定します。 Enter キーを押します。

```
会計コード  . . . . . .  *USRPRF
  .
  .
要求データまたはコマンド  . . .  *NONE
初期ライブラリー・リスト  . . .  +
            値の続きは＋
```

6. 「初期ライブラリー・リスト」フィールドに、ユーザー・グループ記述ワークシート内で照合の印を付けたライブラリーの名前を入力します。
   - 1 行に 1 つずつライブラリー名を記入します。
   - QGPL と QTEMP を含めます。 すべてのジョブは QTEMP というライブラリーを使用して一時オブジェクトを保管します。**すべての初期ライブラリー・リストに QTEMP ライブラリーがなければなりません。** ほとんどのアプリケーションの場合、初期ライブラリー・リストに QGPL ライブラリーもなければなりません。
   - ライブラリー・リストに現行 (デフォルト) ライブラリーを含める必要はありません。このライブラリーはサインオン時にシステムによって自動的に追加されます。
7. Enter キーを押します。 メッセージをチェックします。 (すべてのメッセージを調べるには、ページ送りします。)

```
                パラメーターの追加の値の指定     INLLIBL

選択項目を入力して，実行キーを押してください。

初期ライブラリー・リスト  . . .  CUSTLIB
                              ITEMLIB
                              COPGMLIB
                              ICPGMLIB
                              QGPL
                              QTEMP
```

考えられるエラー	回復
F10 ではなく Enter キーを押した。	初期ライブラリー・リストに正しいライブラリーを含めるには、CHGJOBD (ジョブ記述の変更) と入力してから、F4 を押してください。

考えられるエラー	回復
ジョブ記述を作成しようとしたら、エラー・メッセージが表示された。	エラー・メッセージが表示される最も一般的な原因は、システム上にないライブラリーを含めようとすることにあります。このメッセージは警告です。このような場合でも、ジョブ記述は初期ライブラリー・リストにあるライブラリーを使って作成されます。該当するライブラリーがシステム上にないと、このジョブ記述を指定したプロファイルを使ってサインオンできません。 該当するライブラリーがシステム上にある場合は、入力した名前が間違っていた可能性があります。ライブラリー名を調べて、再試行してください。

詳しくは、「*iSeries 機密保護解説書*」の第 4 章にある『ジョブ記述』を参照してください。

グループ・プロファイルの作成:

この項では、グループ・プロファイルの作成方法について説明します。 グループ・プロファイルは、各ユーザーに個々に権限を与えるのではなく、ユーザー・グループに権限を定義する場合に使用できます。

ジョブ記述の作成後、ユーザー・グループ記述用紙の第 2 部の情報を使用してグループ・プロファイルを作成できます。

1. ユーザー・プロファイル処理コマンドを使用します。 WRKUSRPRF *ALL と入力してください。最初に、IBM 提供のプロファイルがリストされます。

   注: 「ユーザー登録の処理」画面が表示される場合、F21 を押して中間操作援助レベルに変更します。
2. 新しいプロファイルを作成するには、「*Opt*」(オプション) 列に 1 と入力し、「ユーザー・プロファイル」列にプロファイルの名前を入力します。Enter キーを押します。

```
                        ユーザー・プロファイルの処理

オプションを入力して，実行キーを押してください。
  1= 作成    2= 変更    3= コピー    4= 削除    5= 表示
  12= 所有者によるオブジェクトの処理

    ユーザー
OPT プロファイル   テキスト
1    DPTSM
     QDOC          内部文書ユーザー・プロファイル
     QSECOFR       機密保護担当者
```

3. ユーザー・グループ記述用紙の情報を、該当するフィールドに入力します。
4. タブ・キーを使用して、デフォルトを使用するフィールドをすべてスキップします。
5. F10 (追加のパラメーター) を押 します。
6. ページ送りをします。

```
            ユーザー・プロファイル作成  (CRTUSRPRF)

選択項目を入力して，実行キーを押してください。

ユーザー・プロファイル  . . . . > DPTSM
ユーザー・パスワード  . . . . .   *USRPRF
パスワードを満了にセット  . . .   *NO
状況  . . . . . . . . . . . . .   *ENABLED
ユーザー・クラス  . . . . . . .   *USER
援助レベル  . . . . . . . . . .   *SYSVAL
現行ライブラリー  . . . . . . .   *CRTDFT
呼び出す初期プログラム  . . . .   CPSETUP
  ライブラリー  . . . . . . . .     CPPGMLIB
初期メニュー  . . . . . . . . .   CPMAIN
  ライブラリー  . . . . . . . .     CPPGMLIB
制限機能  . . . . . . . . . . .   *YES
テキスト ' 記述 ' . . . . . . .    販売営業
```

7. ユーザー・グループ記述用紙の残りのフィールドを画面の追加のページに入力し、Enter キーを押します。

```
                  ユーザー・プロファイル作成  (CRTUSRPRF)

                追加のパラメーター

特殊権限  . . . . . . . . . . .   *USRCLS
・
・
ジョブ記述  . . . . . . . . . .   DPTSM
  ライブラリー  . . . . . . . .     QGPL
```

8. メッセージをチェックします。

```
                  ユーザー・プロファイル作成  (CRTUSRPRF)

グループ権限  . . . . . . . . .   *NONE
・
・
印刷装置  . . . . . . . . . . .   PRT03
```

重要: グループ・プロファイルは単に特殊なタイプのユーザー・プロファイルです。多くのメッセージと画面では、グループ・プロファイルがユーザーまたはユーザー・プロファイルと見なされます。グループ・プロファイルにメンバーを追加したり、グループ識別番号 (gid) を割り当てたりした場合にのみ、システムはグループ・プロファイルが作成されたことを認識します。

考えられるエラー	回復
グループ・プロファイルに値をすべて入力し終える前に、Enter キーを押した。	F5 (最新表示) を押して、作成したプロファイルを「ユーザー・プロファイル処理」画面に追加します。次に、オプション 2 (変更) を使用して、プロファイルを訂正します。
間違った名前を使用してプロファイルを作成した。	プロファイルの名前は変更できません。コピー・オプション (3) を使用して、正しい名前で新しいプロファイルを作成してください。そして、間違った名前のプロファイルを削除します (オプション 4)。

考えられるエラー	回復
ユーザー・グループ記述用紙のフィールドの一部が画面に表示されない。	中間操作援助レベルを使用しているか確認してください。初級操作援助レベル・バージョンの「ユーザー・プロファイル作成」画面は、「ユーザーを追加」画面といいます。操作援助レベルを変更するには、F12 (取り消し) を押して、「ユーザー登録の処理」画面に戻ります。 F21 を使用して、操作援助レベルを変更します。
「ユーザー・プロファイル作成」画面から、デフォルト情報の一部を不慮に消去してしまった。	フィールドをブランクのままにしておくと、ユーザー・プロファイルの作成時にデフォルトが使用されます。デフォルト値を参照したい場合は、F5 (最新表示) を押して、画面全体を復元します。情報を再び入力してください。

結果のリスト

システム上のすべてのプロファイルの名前と記述をリストするには、権限ユーザー表示 (DSPAUTUSR) コマンドを使用します。 DSPAUTUSR OUTPUT(*PRINT) と入力してください。すべてのグループ・プロファイルがパスワード *NONE を持っているか調べてください。

以下の作業を完了してから、個々のユーザーを設定してください。

- ユーザー・グループごとにジョブ記述を作成する。
- グループごとにライブラリーを作成する (オプション)。
- ユーザー・グループごとにグループ・プロファイルを作成する。

グループ・プロファイルおよび IBM 提供のユーザー・プロファイルの詳細については、「*iSeries 機密保護解説書*」の以下のトピックを参照してください。

- 第 7 章の『グループ・プロファイルの計画』
- 第 9 章の『IBM 提供のユーザー・プロファイル』

関連概念

10 ページの『グループ・プロファイル』
グループ・プロファイルは、ユーザーのグループの権限を定義します。

グループ内のユーザー用のプロファイルの作成:

このトピックでは、個別のユーザーごとのプロファイルの作成方法を取り上げます。

ユーザー・グループを設定するとグループ・プロファイルを作成するためのステップを完了したことになります。ここで、グループのメンバーの個別プロファイルを作成します。 1 つのユーザー・グループのメンバーについてトピック全体の作業を行ったら、最初に戻り、それ以外のグループで同じステップを繰り返してください。

122 ページの『ユーザー・プロファイルの計画』で作成した個別ユーザー・プロファイル・ワークシートを使用します。

グループのメンバーの個別プロファイルを作成するには、以下の作業を完了させてください。

1. 個人ライブラリーの作成 (オプション)。
2. グループ・プロファイルのコピー
3. パスワードの期限満了の設定。
4. 追加ユーザーの作成 (オプション)。

5. ユーザー情報の変更 (必要な場合)。
6. 結果の表示。

注: すべてのグループ・メンバー用のユーザー・プロファイルを作成するまで、個人ライブラリーの作成と追加ユーザーの作成を繰り返してください。

詳しくは、「*iSeries 機密保護解説書*」の第 4 章にある『ジョブ記述』を参照してください。

関連概念

122 ページの『ユーザー・プロファイルの計画』
このトピックでは、ユーザー・プロファイルの目的およびその設計方法について取り上げます。

グループの各メンバー用の個人ライブラリーの作成:

この項では、グループの各メンバー用の個人ライブラリーを作成する作業と、それが重要な理由を取り上げ、段階的な手順を示します。

個々のユーザーの設定を開始するには、オブジェクトのメンバーごとに、Query プログラムなどの個人ライブラリーを作成しなければならない場合があります。個人ライブラリーは、個別のユーザー・プロファイルを作成する前に作成してください。

1. CRTLIB と入力して、F4 (プロンプト) を押します。
2. ライブラリーにユーザー・プロファイルと同じ名前を指定します。
3. F10 (追加のパラメーター) を押します。
4. ライブラリーの共通権限と、そのライブラリーで作成される新しいオブジェクトを記入します。
5. Enter キーを押します。確認メッセージをチェックします。

```
                        ライブラリー作成  (CRTLIB)

 選択項目を入力して，実行キーを押してください。

 ライブラリー  . . . . . > DPTSM
 ライブラリー・タイプ  . . . . .  *PROD
 テキスト ' 記述 ' . . . . . > ' 倉庫ライブラリー '


                  追加のパラメーター

  権限  . . . . . .  *EXCLUDE
ASP 番号  . . . . . .  1
ASP 装置  . . . . . .  *ASP
 作成権限  . . . . . .  *CHANGE
 オブジェクト監査の作成  . . . .  *SYSVAL
```

個人ライブラリーを作成したら、グループ・プロファイルをコピーすることにより、個別のプロファイルを作成できます。

ライブラリーに関する詳細は、「iSeries 機密保護解説書」の以下のセクションを参照してください。

- 第 6 章の『ライブラリー・リストのセキュリティー・リスク』
- 第 7 章の『ライブラリーの計画』

グループ・プロファイルのコピー:

この項では、グループ・プロファイルのコピー方法と、それが重要な理由を取り上げ、段階的な手順を示します。

グループ・プロファイルには、次の 2 つの役割があります。

1. システムはグループ・プロファイルを使用して、グループ・メンバーにオブジェクトを使用する許可があるかどうかを判別します。
2. グループ・メンバーを、個別のユーザー・プロファイルを作成するためのパターンとして使用できます。

ユーザー・グループを設定すると、グループ・プロファイルを作成したことになります。ここで、グループ・プロファイルをコピーして個別のプロファイルを作成し、さらに個別のプロファイルをコピーしてグループ内の他のプロファイルを作成することができます。

1. SETUP メニューから「ユーザー登録の処理」オプションを選択します。

   ヒント: 「ユーザー・プロファイルの処理」画面が表示される場合、F21 (操作援助レベルの選択) を使用して初級操作援助レベルに変更します。

2. ユーザー・グループの前にある *Opt* 列に 3 (コピー) を入力します。「ユーザーのコピー」画面が表示されます。 (コピーしたいユーザー・グループが画面に表示されていない場合、見つかるまでページ送りを行ってください。) システムは「ユーザー名」フィールドをブランクのままにし、残りのフィールドには、コピーしたグループ・プロファイルからの情報を記入します。

```
                          ユーザー登録の処理

  下のオプションを入力して、Enter キーを押してください。
     1= 追加   2= 変更   3= コピー   4= 除去   5= 表示

OPT   ユーザー     記述
      DPTSM        SALES AND MARKETING DEPARTMENT
3     DPTWH        WAREHOUSE DEPARTMENT
```

3. 作成しているユーザー・プロファイルの名前と記述を入力します。
4. パスワードはブランクのままにしておきます。システムは、自動的にパスワードを新しいユーザー・プロファイル名と同じものにします。
5. グループ・プロファイル名を「ユーザー・グループ」フィールドに入れます。
6. 個々のユーザー・プロファイル・ワークシートを調べて、ユーザーにグループとは異なる他の値があるかどうかを確認します。それらの値を入力します。
7. ページ送りをします。

```
                            ユーザーのコピー

コピー元ユーザー  . . . :   DPTWH

下の選択項目を入力して，実行キーを押してください。

ユーザー  . . . . . .   WILLISR
ユーザー記述  . . . . .   Willis, Rose
パスワード  . . . . . .
ユーザーのタイプ  . . . .   *SYSOPR
ユーザー・グループ  . . .   DPTWH

コマンド入力行の使用制限    N

省略時のライブラリー  . .   DPTWH
省略時の印刷装置  . . . .   PRT04
サインオン・プログラム. .   *NONE
  ライブラリー  . . . . .

最初のメニュー  . . . . .   ICMAIN
  ライブラリー  . . . . .   ICPGMLIB
```

8. 画面の次のページで、必要な変更をすべて行ってから、Enter キーを押します。

9. 「ユーザー登録の処理」画面の下部にある確認メッセージをチェックします。

```
                          ユーザーのコピー

コピー元ユーザー  . . . :   DPTWH

下の選択項目を入力して，実行キーを押してください。

アテンション・キー・プログラム *SYSVAL
  ライブラリー  . . . . .
```

考えられるエラー	回復
「ユーザーのコピー」画面の代わりに「ユーザー・プロファイル作成」画面が表示される。	F12 (取り消し) を使用して、「ユーザー・プロファイルの処理」画面に戻ります。 F21 を使用して、初級操作援助レベルに変更します。コピー操作を再び開始します。
選択したユーザー・プロファイル名がユーザー・プロンプトに収まりきらない。	ユーザー・プロファイル名は 10 文字までですが、「ユーザーのコピー」および「ユーザーの追加」画面では 8 文字を超える名前はサポートしていません。短いユーザー名を選択するか、または中間操作援助レベルを使用して個別のユーザー・プロファイルを作成してください。

ユーザー・プロファイルのテスト

グループ内に最初の個別プロファイルを作成するときに、そのプロファイルを使用してサインオンすることにより、プロファイルをテストしなければなりません。最初のメニューが正しく表示され、サインオン・プログラムが実行されるかどうか検証します。

そのプロファイルを使用してサインオンが正常に行えない場合、システムは、そのプロファイルで指定されているものを検出できなかった可能性があります。それは、サインオン・プログラム、ジョブ記述、または初期ライブラリー・リストのライブラリーの 1 つであるかもしれません。「プリンター出力の処理」画面を使用して、サインオンの試行時に作成されたジョブ・ログを見つけてください。ジョブ・ログを調べれば、どのようなエラーが起こったのかがわかります。

ユーザー・プロファイルのテストが完了したら、パスワードの期限満了を設定することができます。

個々のプロファイルのグループ・プロファイルとしての使用

プロファイルをグループ・プロファイルとして特定して作成することは、既存のプロファイルをグループ・プロファイルにするよりも良い方法です。ある特定のユーザーが、ユーザー・グループで必要なすべての権限を持っていて、ユーザー・プロファイルをグループ・プロファイルにしようとする場合があるかもしれません。しかし、個人のプロファイルをグループ・プロファイルとして使用すると、将来以下のような問題が起きる原因となります。

- グループ・プロファイルとして使用されるプロファイルを持つユーザーが責任を変更すると、新しいプロファイルをグループ・プロファイルとして指定する必要、権限を変更する必要、およびオブジェクト所有権を移す必要がそれぞれ生じます。
- グループのすべてのメンバーは、グループ・プロファイルで作成されたすべてのオブジェクトに対して自動的に権限を持ちます。自分のプロファイルがグループ・プロファイルであるユーザーは、他のユーザーを特別に排除しないと、私用オブジェクトを所有できなくなります。

前もって、グループ・プロファイルについて計画してください。特定のグループ・プロファイルをパスワード *NONE を指定して作成してください。アプリケーションを実行した後で、あるユーザーがユーザーのグループに所属するべき権限を持っていることがわかった場合、以下のようにしてください。

1. グループ・プロファイルを作成する。
2. GRTUSRAUT コマンドを使用して、グループ・プロファイルへユーザーの権限を与える。
3. ユーザーから私用権限を除去する。これはもう必要ないためです。 RVKOBJAUT または EDTOBJAUT コマンドを使用してください。

グループ・プロファイル・パスワードの期限満了の設定:

ここでは、グループ・プロファイル・パスワードの期限満了を設定する方法について説明します。それがなぜ重要か、および段階的な手順を示します。

ユーザーが初めてサインオンするときにパスワードの変更を求められるよう、個別プロファイルを設定します。「パスワードを満了にセット」フィールドは、初級操作援助レベル・バージョンの「ユーザーのコピー」画面には表示されません。コピー機能を使用してユーザー・プロファイルを作成した後、ユーザー・プロファイルを個別に変更する必要があります。「パスワードを満了にセット」フィールドを変更するには、`CHGUSRPRF profile-name PWDEXP(*YES)` と入力します。

注: ユーザー・プロファイルを使ってサインオンすることによりユーザー・プロファイルをテストしたい場合には、パスワードの期限満了を設定する前にテストを行ってください。

考えられるエラー	回復
プロファイルをテストして、パスワードを変更するように強制された。	CHGUSRPRF *profile-name* と入力して F4 (プロンプト) を押します。パスワードをユーザー・プロファイル名に戻します。 (「パスワード」フィールドにユーザー・プロファイル名を入力します。) 「パスワードを満了にセット」フィールドに、*YES と入力します。これを行うには、中間操作援助レベルが必要です。

最初の個別ユーザー・プロファイルを作成したら、追加のユーザーを作成することができます。

詳しくは、「iSeries 機密保護解説書」の第 4 章『パスワード満了設定』を参照してください。

グループに属さないユーザーのプロファイルの作成

まず最初の個別のユーザー・プロファイルをコピーして、 グループ内に追加メンバーを作成します。 コピー方式を使用して個別プロファイルを作成する際には、それぞれの個別プロファイルをよく見てください。

個々のユーザー・プロファイル用紙を確認して、新しいユーザー・プロファイル用の固有のフィールドを必ず変更してください。

1. 「ユーザー登録の処理」画面で、コピーしたいプロファイルの前に、3 (コピー) と入力します。
2. 「ユーザーのコピー」画面で、プロファイル名と記述を入力します。
3. 新しいユーザー用の固有のフィールドに情報を入力します。

```
                          ユーザー登録の処理

下のオプションを入力して，実行キーを押してください。
  1= 追加    2= 変更    3= コピー    4= 除去    5= 表示

OPT       ユーザー        記述
          DPTSM           販売営業部
          DPTWH           倉庫部
  3       WILLISR         WILLIS, ROSE
```

考えられるエラー	回復
コピーしたいプロファイルが、「ユーザー登録の処理」画面に表示されない。	F5 (最新表示) を押します。ページ戻しおよびページ送りを行います。リストにはプロファイル名がアルファベット順に表示されます。

ユーザー情報の変更

一部のユーザーにとっては、「ユーザーのコピー」画面に表示されない値を設定しなければならないことがあります。たとえば、ユーザーによっては複数のグループ・プロファイルに属していることがあります。コピー方式を使用してユーザー・プロファイルを作成したら、それを変更することができます。

1. 「ユーザー登録の処理」画面で、F21 を押して中間操作援助レベルに変更します。
2. 「ユーザー・プロファイルの処理」画面で、変更したいプロファイルの横にある *Opt* (オプション) 列に 2 (変更) と入力します。 Enter キーを押します。

```
                        ユーザー・プロファイルの処理

オプションを入力して，実行キーを押してください。
  1= 作成    2= 変更    3= コピー    4= 削除    5= 表示
  12= 所有者によるオブジェクトの処理

    ユーザー
OPT プロファイル  テキスト
2    AMESJ        AMES, JANICE
     DPTSM        販売営業部
     QDOC         内部文書ユーザー・プロファイル
     QSECOFR      機密保護担当者
     WAGNERR      WAGNER, RAY
     WILLISR      WILLIS, ROSE
```

3. 「ユーザー・プロファイル変更」画面で、F10 (追加のパラメーター) を押します。
4. 変更したいフィールドが見つかるまでページ送りを行います。たとえば、ユーザーを追加のグループ・プロファイルのメンバーにする場合は、「補足グループ」フィールドが見つかるまでページ送りを行います。
5. 必要な値を入力して、Enter キーを押します。確認メッセージが表示されます。「ユーザー・プロファイルの処理」画面をもう一度ご覧ください。

```
                  ユーザー・プロファイル変更  (CHGUSRPRF)

選択項目を入力して，実行キーを押してください。

最大許容記憶域  . . . . . .   *NOMAX
最高スケジュール優先順位  . . .   3
ジョブ記述  . . . . . .   DPTWH
  ライブラリー  . . . . . .     QGPL
グループ・プロファイル  . . . .   DPTWH
所有者  . . . . . .   *GRPPRF
グループ権限  . . . . . .   *USE
グループ権限タイプ  . . . . . .   *PGP
補足グループ  . . . . . .   DPTIC
            値の続きは+
```

ユーザー情報を変更した後、結果を表示して、プロファイルを検査することができます。

ユーザー・プロファイルの表示

作成したプロファイルを表示するには、次の方法を使用することができます。

1 つのプロファイルの表示

「ユーザー登録の処理」画面または「ユーザー・プロファイルの処理」画面のいずれかで、オプション 5 (表示) を使用します。

1 つのプロファイルのリスト

ユーザー・プロファイル表示コマンド、DSPUSRPRF *profile-name* DETAIL(*BASIC) OUTPUT(*PRINT) を使用します。

グループ・メンバーの表示

DSPUSRPRF *group-profile-name* *GRPMBR と入力します。 OUTPUT(*PRINT) を使用すると、リストを印刷できます。

すべてのプロファイルのリスト

すべてのプロファイルの名前と記述をグループごとに分けてリストするには、許可ユーザーの表示コマンド、DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT) を使用します。

所有権と共通権限を設定する前に、次の作業を完了させてください。

- 個別のユーザー・プロファイルをすべて作成する。
- プロファイルごとにパスワードの期限満了を設定する。
- グループごとに分けられているすべてのプロファイルのリストを印刷し、それをユーザー・グループ記述用紙に保存する。新しいユーザーを追加したら、リストを再び印刷する。

関連概念

122 ページの『ユーザー・プロファイルの計画』
このトピックでは、ユーザー・プロファイルの目的およびその設計方法について取り上げます。

プログラム機能へのアクセスの制限

プログラム機能へのアクセスを制限することで、アプリケーション、 アプリケーションの一部、またはプログラム内の機能を誰が使用できるかを、 定義することができます。

プログラム機能への制限アクセスにより、そのプログラムでは保護するオブジェクトがない場合でも、プログラムにセキュリティーを提供することができます。 iSeries ナビゲーターを使用してアプリケーション機能へのユーザー・アクセスを管理するには 2 つの方法があります。

最初の方法では、以下のようにしてアプリケーション管理を使用します。

1. アクセス設定を変更したい機能が入っているシステムを右マウス・ボタンでクリックする。
2. 「**アプリケーション管理**」を選択する。
3. 管理システム上にいる場合は、「**ローカル設定**」を選択する。それ以外の場合は、次のステップを継続する。
4. 管理可能な機能を選択する。
5. 「**デフォルト・アクセス**」を選択すると、デフォルトですべてのユーザーがこの機能にアクセスすることを許可する。
6. 「**すべてのオブジェクト・アクセス**」を選択すると、全オブジェクト・システム特権を持つすべてのユーザーがこの機能にアクセスすることを許可する。
7. 「**カスタマイズ**」を選択して、「**アクセスのカスタマイズ**」ダイアログ上の「**追加**」ボタンおよび「**除去**」ボタンを使用して、「**アクセス許可**」リスト内および「**Access Denied (アクセス否認)**」リスト内のユーザーまたはグループを追加または除去する。
8. 「**カスタマイズの除去**」を選択すると、選択された機能についてカスタマイズされたアクセスがすべて除去される。

9. 「**OK**」をクリックし、「**アプリケーション管理**」ダイアログを閉じる。

ユーザー・アクセスを管理するための 2 番目の方法は、iSeries ナビゲーターのユーザーおよびグループを使用するものです。

1. iSeries ナビゲーターで、「**ユーザーおよびグループ**」を展開する。
2. 「**すべてのユーザー**」、「**グループ**」、または「**グループに属さないユーザー**」を選択し、ユーザーおよびグループのリストを表示する。
3. ユーザーまたはグループを右マウス・ボタンでクリックし、「**プロパティー**」を選択する。
4. 「**機能**」をクリックする。
5. 「**アプリケーション**」タブをクリックする。
6. このページを使用して、ユーザーまたはグループのアクセス設定を変更する。
7. 「**OK**」を 2 度クリックし、「**プロパティー**」ダイアログを閉じる。

重要: プログラム機能への制限アクセスは、ユーザーが別のインターフェースから資源、ファイルやプログラムなどにアクセスすることを防ぐことはできないからです。引き続き、資源保護を使用する必要があります。

プログラム機能へのアクセス制限のサポートでは、以下のことを行う API が提供されています。

- 機能を登録する
- 機能についての情報を検索する
- 誰が機能を使用できるか、または使用できないかを定義する
- そのユーザーがその機能を使用することを許可されているかどうかを検査する

アプリケーション内でこの機能を使用するには、アプリケーションの導入時に、アプリケーション・プロバイダーが機能を登録しなければなりません。登録済みの機能は、アプリケーションの特定機能のコード・ブロックに対応します。ユーザーがアプリケーションを実行すると、アプリケーションは使用法検査 API を呼び出して、そのユーザーがコード・ブロックに関連付けられている機能を使用することを許可されているかどうかを、コード・ブロックを呼び出す前に検査します。ユーザーがその登録済み機能の使用を許可されていれば、そのコード・ブロックが実行されます。ユーザーが機能の使用を許可されていなければ、ユーザーはそのコード・ブロックを実行できません。

システム管理担当者は、機能へのアクセスを誰に許可するか、誰を拒否するかを指定します。管理者は、プログラム機能へのアクセスを管理する機能使用法処理 (WRKFCNUSG) コマンドを使用するか、もしくは iSeries ナビゲーターを使用することができます。

資源保護のインプリメント

以下の情報を参考にすれば、オブジェクトの所有権と共通権限、およびアプリケーションに対する特定権限を設定することにより、ワークステーションとプリンターの資源保護を確立できます。

最も重要な保護処置は、サーバーに関する資源保護です。システムでの資源保護によって、オブジェクトを使用できるユーザーとそのオブジェクトの使用方法を定義できます。オブジェクトにアクセスできることを権限と呼びます。オブジェクト権限を設定するときには、ユーザーが自分たちの作業を十分に実行でき、しかもシステムの表示や変更が不可能な権限を与えるよう、よく考慮してください。オブジェクト権限は、特定のオブジェクトに関する許可をユーザーに与え、そのオブジェクトに対してユーザーは何ができるかを指定できます。具体的で詳細なユーザー権限 (たとえばレコードの追加や変更) を介して、オブジェクト資源を制限できます。

システム資源を使用して、*ALL、*CHANGE、*USE、*EXCLUDE といった、特定のシステム定義の権限のサブセットへのアクセスをユーザーに与えることができます。資源保護を必要とする最も一般的なシステム・オブジェクトはファイル、プログラム、ライブラリー、ディレクトリーですが、システム上のどんなオブジェクトに対しても権限を指定できます。

情報にアクセスできるユーザーの定義

個々のユーザー、ユーザーのグループ、および共通ユーザーに対して権限を与えることができます。

注: 環境によっては、ユーザーの権限は特権と呼ばれます。

オブジェクトを使用できるユーザーを定義する方法はいくつかあります。

共通権限
共通ユーザーとは、システムへのサインオンを許可されている任意のユーザーです。システム上のすべてのオブジェクトに対して共通権限を定義できます (あるオブジェクトに対する共通権限を *EXCLUDE にすることができます)。オブジェクトに対する共通権限は、そのオブジェクトに対する他の特定権限が存在しない場合に使用されます。

私用権限
オブジェクトを使用する (または使用しない) ための特定権限を定義できます。個々のユーザー・プロファイルまたはグループ・プロファイルに対して、権限を認可することができます。共通権限、オブジェクト所有権、または 1 次グループ権限以外の権限がオブジェクトに定義されている場合、そのオブジェクトは私用権限を持ちます。

ユーザー権限
個々のユーザー・プロファイルに対して、システム上のオブジェクトを使用する権限を与えることができます。この権限は、私用権限の 1 つのタイプです。

グループ権限
グループ・プロファイルに対して、システム上のオブジェクトを使用する権限を与えることができます。グループ・メンバーに対して特に権限が定義されていない限り、そのユーザーは、グループの権限を得ます。グループ権限もまた、私用権限と考えることができます。

オブジェクト所有権
システム上のすべてのオブジェクトには、それぞれ所有者がいます。所有者は、デフォルトで、オブジェクトに対する *ALL 権限を持っています。しかし、オブジェクトに対する所有者の権限を変更または除去することができます。オブジェクトに対する所有者の権限は私用権限とは見なされません。

1 次グループ権限
オブジェクトに 1 次グループを指定し、その 1 次グループの持つ権限をそのオブジェクトに指定することができます。1 次グループ権限はオブジェクトと一緒に保管され、グループ・プロファイルに認可された私用権限を使用するよりもパフォーマンスが向上する可能性があります。グループ識別番号 (gid) を持つユーザー・プロファイルだけが、オブジェクトの 1 次グループになれます。 1 次グループ権限は、私用権限とは見なされません。

情報にアクセスする方法の定義

権限とは、オブジェクトに対して許可されるアクセスのタイプです。操作に応じて、異なるタイプの権限が必要になります。

注: 一部の環境では、オブジェクトに関連する権限は、オブジェクトのアクセス・モードと呼ばれます。

オブジェクトに対する権限は、次の 3 つのカテゴリーに分類できます。

1. オブジェクト権限は、オブジェクト全体に対して実行できる操作を定義します。
2. データ権限は、オブジェクトの内容に対して実行できる操作を定義します。
3. フィールド権限は、データ・フィールドに対して実行できる操作を定義します。

アクセス対象となる情報の定義

システム上の個々のオブジェクトに関する資源保護を定義できます。また、ライブラリー・セキュリティーまたは権限リストのいずれかを使用して、オブジェクトのグループ用にセキュリティーを定義することもできます。

ライブラリー・セキュリティー

システム上の多くのオブジェクトは、ライブラリーに存在します。オブジェクトにアクセスするには、オブジェクト自体、およびオブジェクトが入っているライブラリーの両方に対する権限が必要です。オブジェクトの削除を含め、ほとんどの操作を行うには、(オブジェクトに必要な権限に加えて) オブジェクト・ライブラリーに対する *USE 権限を持っていれば十分です。新しいオブジェクトを作成するには、オブジェクト・ライブラリーに対する *ADD 権限が必要です。オブジェクトおよびオブジェクト・ライブラリーを処理するいくつかの CL コマンドでは、特殊権限が必要とされます。ライブラリー・セキュリティーの使用は、単純なセキュリティー体系を保ちながら情報を保護するための手法の 1 つです。

ライブラリー・セキュリティーは、情報を保護するための簡単で効果的な方法ですが、高いセキュリティーを必要とするデータには適さないかもしれません。ほとんどのオブジェクトはディレクトリーに格納されます。重要性が高いオブジェクトは、ライブラリー・セキュリティーに頼るのではなく、個別に、または権限リストを使って保護するべきです。

このプロセスでは、以下のワークシートが必要になります。

- 『アプリケーションの導入の計画』で作成した「アプリケーションの導入」ワークシート
- 『オブジェクトのグループ化』で作成した権限リスト・ワークシート
- 『ライブラリーとオブジェクトの所有権の決定』で作成したライブラリー記述ワークシート
- 『プリンター出力の保護』および『ワークステーションの保護』で作成した「出力待ち行列およびワークステーションのセキュリティー」ワークシート
- 『全体的なセキュリティー戦略の計画』で作成したシステム責任ワークシート

以下の作業を完了してください。

- 所有権および共通権限のセットアップ
- 権限リストの作成
- 権限リストによるオブジェクトの保護
- 権限リストへのユーザーの追加
- 特定権限のセットアップ
- ワークステーションの保護
- プリンター出力の保護
- システム操作員のメッセージ待ち行列へのアクセスの制限

関連概念

17 ページの『資源保護』
認証に成功した後に許可ユーザーが行う処置を制御するために、システムの資源保護を使用することができます。

所有権および共通権限のセットアップ

このトピックでは、アプリケーション、ライブラリー、および個人ライブラリーの所有権および共通権限を確立します。

この手順を 1 つのアプリケーションに適用した後、最初に戻り、それ以外のアプリケーションで同じステップを繰り返してください。サンプル画面には、『アプリケーションの導入の計画』で Sharon Jones が顧客オーダー・アプリケーション用に作成したアプリケーションの導入用紙が示されています。

新しいアプリケーションをシステムに導入するとき、または既存のアプリケーションにセキュリティーを設定するときには、このトピックの手順を必ず使用してください。『アプリケーションの導入の計画』で作成したアプリケーションの導入用紙を使用します。

所有権と共通権限を設定するには、次の作業を完了させてください。

1. 所有者プロファイルの作成
2. ライブラリー所有権の変更
3. アプリケーション・オブジェクトの所有権の設定
4. ライブラリーへの共通アクセスの設定
5. ライブラリー内のすべてのオブジェクトの共通権限の設定
6. 新しいオブジェクトの共通権限の設定
7. グループおよび個人ライブラリーの処理

システムへのサインオン

プロファイル
独自のもの (*ALLOBJ 権限が必要)

メニュー
MAIN

所有者プロファイルの作成:

このトピックでは、所有者プロファイルの作成プロセスの概略を記します。

所有者プロファイルがまだ存在しない場合は、CRTUSRPRF (ユーザー・プロファイル作成) コマンドを使用して、ユーザー・プロファイルを作成します。パスワードを *NONE に設定します。

所有者プロファイルがすでに存在する場合は、CHGUSRPRF (ユーザー・プロファイル変更) コマンドを使用して、パスワードを *NONE に設定します。

所有者プロファイルを作成したら、 ライブラリー所有権を変更することができます。

ライブラリー所有権の変更:

このステップでは、ライブラリーにあるオブジェクトではなく、 ライブラリーの所有権を変更します。

重要: アプリケーション・オブジェクトの所有権を変更する前に、必ずアプリケーションの提供者に確認してください。アプリケーションによっては、特定のオブジェクト所有権に関係している機能を使用するものがあります。

1. CHGOBJOWN (オブジェクト所有者変更) を入力して、F4 (プロンプト) を押します。
2. ライブラリー名、オブジェクト・タイプ (*LIB)、および新規所有者を記入します。
3. 確認メッセージをチェックします。

ライブラリー所有権の変更が完了したら、アプリケーション・オブジェクトの所有権を設定することができます。

アプリケーション・オブジェクトの所有権のセットアップ:

アプリケーション・オブジェクトの所有権を変更する場合、 各オブジェクトを 1 つずつ変更しなければならないため、手間のかかる作業となります。 可能であれば、プログラマーまたはアプリケーションの提供者に連絡して、 所有権を確立するように依頼してください。

ライブラリー内のオブジェクトのリスト

所有権を変更する前に、ライブラリー表示コマンドを使用して、ライブラリーにあるすべてのオブジェクトのリストを印刷します。これを、チェックリストとして使用できます。 DSPLIB library-name *PRINT と入力してください。

最適な方法の選択

アプリケーション・ライブラリーにあるオブジェクトの所有権を変更するには、次の 2 つの方法のどちらかを選択します。

方法	機能	いつ使用するか
「所有者によるオブジェクトの処理」コマンド	プロファイルが所有するすべてのオブジェクトをリストする画面を表示します。画面上のオプションを使用して、オブジェクトの所有者を変更できます。	この方法は簡単に使用できます。しかし、QPGMR または QSECOFR のどちらかがオブジェクトを所有する場合、 IBM では、この方法の使用をお勧めできません。これらのプロファイルは多くのオブジェクトを所有しており、リストを表示すると非常に大きなものになります。
オブジェクト所有権変更コマンド	オブジェクトごとに別々のコマンドを使用する必要があります。しかし、コマンド複写 (Retrieve) (F9) を使用して直前のコマンドを繰り返し、必要なタイプ入力の量を減らすことができます。	QPGMR または QSECOFR のどちらかがオブジェクトを所有している場合は、この方法を使用した方が速く処理されます。

ライブラリーへの共通アクセスのセットアップ:

アプリケーション・オブジェクトの所有権を設定したら、 オブジェクト権限編集 (EDTOBJAUT) コマンドを使用して、 ライブラリーに対する共通権限を変更することができます。

システム上のライブラリーへの共通アクセスをセットアップするには、以下の手順に従います。

1. EDTOBJAUT library-name *LIB と入力します。

2. *PUBLIC が示されている行にカーソルを移動します。
3. ライブラリーに対して設定したい共通権限を入力して、Enter キーを押します。画面に、新しい権限が示されます。

ライブラリー内のオブジェクトの共通権限の設定:

オブジェクト権限認可 (GRTOBJAUT) コマンドを使用して、 ライブラリーにあるすべてのオブジェクトに対する共通権限を設定します。

注: オブジェクト権限取り消し (RVKOBJAUT) コマンドを使用して、ライブラリーにあるオブジェクトに対する現在の共通権限を除去します。

1. RVKOBJAUT と入力して、F4 (プロンプト) を押します。
2. 表示されているとおりに入力し、実際のアプリケーション・ライブラリーの名前に置き換えて、Enter キーを押します。

   注: ライブラリーにたくさんのオブジェクトがある場合、システムが要求を処理するのに数分かかることがあります。
3. GRTOBJAUT と入力して、F4 (プロンプト) を押します。
4. 表示されているとおりに入力し、実際のアプリケーション・ライブラリーの名前および必要な権限に置き換えて、Enter キーを押します。

   注: ライブラリーにたくさんのオブジェクトがある場合、システムが要求を処理するのに数分かかることがあります。

ライブラリーにあるすべてのオブジェクトの共通権限を設定したら、ジョブ・ログを使用して作業を確認することができます。

新しいオブジェクトの共通権限の設定:

ライブラリー記述には、作成権限 (CRTAUT) というパラメーターがあります。このパラメーターは、ライブラリー内に作成される新しいオブジェクトの共通権限を決定します。オブジェクトを作成するコマンドは、オブジェクト・ライブラリーの CRTAUT 権限をデフォルトとして使用します。 ライブラリーの CRTAUT は、ライブラリー内のほとんどの既存オブジェクトに対する共通権限と同じにしてください。

1. CHGLIB library-name と入力して、F4 (プロンプト) を押します。
2. F10 (追加のパラメーター) を押します。
3. 「作成権限」フィールドに選択項目を入力します。

CRTAUT を *SYSVAL に設定した場合、ライブラリーに新しいオブジェクトを作成するときに、システムは QCRTAUT システム値の現行設定を使用します。ライブラリーごとに特定の CRTAUT 権限を設定すると、今後、QCRTAUT システム値が変更されないように保護されます。

グループおよび個人ライブラリーの処理:

プロファイルは、ユーザー・グループおよび個々のユーザーの設定時に作成されたグループ・ライブラリーおよび個人ライブラリーを所有しています。

グループ・ライブラリーの所有権をグループ・プロファイルに変更し、個人ライブラリーの所有権を個々のユーザー・プロファイルに変更するには、すでに説明した手順を使用します。

グループおよび個人ライブラリーにある新しいオブジェクトの共通権限を判別するには、それらの各ライブラリーごとに作成権限パラメーターを設定します。

権限リストの作成を始める前に、以下のタスクを完了してください。

1. 「アプリケーションの導入」用紙と「ライブラリー記述」用紙を使用して、すべてのアプリケーション・ライブラリーの所有権および共通権限を確立したことを確認します。
2. 作成したすべてのグループ・ライブラリーと個人ライブラリーの所有権を設定して、権限を作成します。

注: システム上のすべてのライブラリーのリストを表示するには、 `DSPOBJD *ALL *LIB *PRINT` と入力してください。

権限リストの作成

この項では、権限リストを作成する作業、およびそれが重要な理由を取り上げ、段階的な手順を示します。

所有権と共通権限を設定したら、権限リストを設定することができます。権限リスト用紙の情報を使用して、ライブラリーを保護するのに必要な権限リストを作成します。

それには、権限リスト作成 (CRTAUTL) コマンドを使用します。

1. CRTAUTL と入力して、F4 (プロンプト) を押します。
2. 権限リスト用紙の情報を記入します。
3. F10 (追加のパラメーター) を押します。
4. 権限パラメーターを使用して、リストによって保護されているオブジェクトの共通権限を指定します。
5. 確認メッセージを検査します。

考えられるエラー	回復
リストの名前が間違って入力されている。	システムでリストの名前を一度作成したら、変更できません。リストを削除 (DLTAUTL) してから、再び行ってください。
リストに共通権限を指定していない。	権限リスト編集 (EDTAUTL) コマンドを使用します。

この機能を使用するには、以下のステップを実行します。

1. iSeries ナビゲーターから、ご使用のサーバーの「セキュリティー」を展開する。権限リストおよびポリシーが表示されます。
2. 「権限リスト」を右マウス・ボタンでクリックし、「新規権限リスト」を選択する。「新規権限リスト」で、次のことを行うことができます。
   - 「使用 (Use)」: オブジェクト属性にアクセスして、オブジェクトを使用することができる。共通のものは表示できますが、オブジェクトを変更することはできません。
   - 「変更 (Change)」: いくつかの例外がありますが、オブジェクトの内容を変更できる。
   - 「すべて (All)」: 所有者に限定されているオブジェクトを除く、オブジェクトに関するすべての操作が行える。ユーザーまたはグループは、オブジェクトの存在の制御、オブジェクトのセキュリティーの指定、オブジェクトの変更、およびオブジェクトに関する基本機能の実行を行うことができます。また、ユーザーまたはグループは、オブジェクトの所有権を変更することもできます。
   - 「除外 (Exclude)」: オブジェクトに関するすべての操作が禁止される。この許可を持っているユーザーおよびグループには、オブジェクトへのアクセスまたは操作が許可されません。共通でオブジェクトを使用することができないように指定してください。

権限リストを処理する際に、オブジェクトとデータの両方の認可を認可することになります。

選択できるオブジェクト許可は、次のとおりです。

- 「操作可能 (Operational)」: オブジェクトの記述を見るための許可と、そのオブジェクトに対してユーザーまたはグループが持っているデータ許可によって決められている通りにオブジェクトを使用するための許可を与える。
- 「管理 (Management)」: オブジェクトのセキュリティーを指定するための許可、オブジェクトを移動またはリネームするための許可、データベース・ファイルにメンバーを追加するための許可を与える。
- 「存在 (Existence)」: オブジェクトの存在および所有権を制御するための許可を与える。ユーザーまたはグループは、オブジェクトの削除、オブジェクトのストレージの解放、オブジェクトに関する保管および復元操作の実行、オブジェクトの所有権の移行を行うことができます。ユーザーまたはグループが特殊な保管許可を持っている場合には、ユーザーまたはグループは、オブジェクトの存在許可を必要としません。
- 「更新 (Alter)」(データベース・ファイルおよび SQL パッケージに限り 使用される): オブジェクトの属性を更新するために必要な許可を与える。ユーザーまたはグループがデータベース・ファイルに関してこの許可を持っている場合には、ユーザーまたはグループは、トリガーの追加および除去、参照制約および固有制約の追加および除去、データベース・ファイルの属性の変更を行うことができます。ユーザーまたはグループが SQL パッケージに関してこの許可を持っている場合には、ユーザーまたはグループは、SQL パッケージの属性を変更することができます。この許可は、現時点では、データベース・ファイルおよび SQL パッケージに限り使用されます。
- 「参照 (Reference)」(データベース・ファイルおよび SQL パッケージに 限り使用される): あるオブジェクトの操作が他のオブジェクトによって制限されている場合などに、他のオブジェクトからあるオブジェクトを参照するために必要な許可を与える。ユーザーまたはグループが物理ファイルに関してこの許可を持っている場合には、ユーザーまたはグループは、物理ファイルが親である参照制約を追加することができます。この許可は、現時点では、データベース・ファイルに限り使用されます。

選択できるデータ許可は、次のとおりです。

- 「読み取り (Read)」: オブジェクトの内容を入手および表示する (ファイルのレコードを表示するなど) ために必要な許可を与える。
- 「追加 (Add)」: オブジェクトに項目を追加する (メッセージをメッセージ待ち行列に追加する、レコードをファイルに追加するなど) ための許可を与える。
- 「更新 (Update)」: オブジェクトの項目を変更する (ファイルのレコードを 変更する) ための許可を与える。
- 「削除 (Delete)」: オブジェクトから項目を除去する (メッセージをメッセージ待ち行列から削除する、レコードをファイルから除去するなど) ための許可を与える。
- 「実行 (Execute)」: プログラム (サービス・プログラムまたは SQL パッケージ) を実行するために必要な許可を与える。ユーザーは、ライブラリーまたはディレクトリー内のオブジェクトを見付けることもできます。

これで、権限リストによるオブジェクトの保護を行うことができます。

関連概念

11 ページの『権限リスト』
グループ・プロファイルのような権限リストを使用すると、類似したセキュリティー要件を持つオブジェクトをグループ化して、そのグループをユーザーおよびユーザー権限のリストと関連付けることができます。

権限リストによるオブジェクトの保護:

権限リストを作成したら、 オブジェクト権限編集 (EDTOBJAUT) コマンドを使用して、 権限リスト用紙にリストされている項目を保護します。

権限リストの作成に必要な手順は、次のとおりです。

1. EDTOBJAUT と入力して、F4 (プロンプト) を押します。
2. プロンプト画面に値を入力して、Enter キーを押します。
3. 「オブジェクト権限編集」画面で、権限リスト名を入力します。
4. オブジェクトの共通権限が権限リストに由来する場合は、共通権限を *AUTL に変更します。これらの手順を、「権限リスト」用紙に含まれるオブジェクトごとに繰り返します。

これで、権限リストにユーザーを追加することができます。

権限リストへのユーザーの追加:

『権限リストによるオブジェクトの保護』を行ったら、 権限リスト編集 (EDTAUTL) コマンドを使用して、 権限リスト用紙にリストされているユーザーを追加します。

1. EDTAUTL authorization-list-name と入力します。
2. 「権限リスト編集」画面で、F6 (新ユーザーの追加) を押します。
3. ユーザーまたはグループ、そしてそのユーザーまたはグループに必要な権限をリストの項目に入力して、 Enter キーを押します。新しいユーザーがリストに表示されます。

考えられるエラー	回復
ユーザーまたはグループに、リストに対する間違った権限を与えた。	「権限リスト編集」画面で、権限を変更できます。
リストに間違ったユーザーまたはグループを追加した。	ユーザーまたはグループを除去するには、権限リスト項目除去 (RMVAUTLE) コマンドを使用するか、または「権限リスト編集」画面でユーザーの権限にブランクを入力します。

作業の確認

- 権限リスト表示 (DSPAUTL) コマンドを使用して、すべてのユーザー権限を権限リストにリストします。
- 権限リストが保護を行っているオブジェクトをすべてリストするには、画面で F15 を使用します。

特定権限を設定する前に、次の作業を完了してください。

1. CRTAUTL コマンドを使用して、アプリケーションに必要な権限リストを作成する。
2. EDTOBJAUT コマンドを使用して、権限リストによるオブジェクトの保護を行う。
3. EDTAUTL コマンドを使用して、ユーザーに権限リストを追加する。

オブジェクト用およびライブラリー用の特定権限の設定

オブジェクト権限編集 (EDTOBJAUT) コマンドを使用して、ライブラリーおよびライブラリー内のオブジェクトの特定権限を指定できます。

『所有権および共通権限の設定』では、GRTOBJAUT コマンドを使用し、「ライブラリー記述」用紙の情報に基づいて、ライブラリー内のすべてのオブジェクトの共通権限を設定する方法を説明しました。次に、EDTOBJAUT と「ライブラリー記述」用紙の情報を使用して、特定のオブジェクト権限およびライブラリー権限を設定します。

関連概念

23 ページの『システム定義の権限』
この表は、ファイル、プログラム、ライブラリーを保護するために、システム定義による権限がどのように適用されるかを示します。

ライブラリーに対する権限の設定:

ライブラリーは実際には特殊なタイプのオブジェクトです。 ライブラリーの権限を設定するには、ライブラリー以外のオブジェクトに権限を設定するときと全く同じように、EDTOBJAUT コマンドを使用します。 すべてのライブラリーは、QSYS という IBM 提供のライブラリーの中にあります。

オブジェクト権限編集 (EDTOBJAUT) コマンドを使用し、「ライブラリー記述」ワークシートの情報に基づいて、ライブラリーおよびライブラリー内のオブジェクトの特定権限を指定します。

1. EDTOBJAUT と入力して、F4 (プロンプト) を押します。
2. プロンプト画面に値を入力して、Enter キーを押します。
3. 「オブジェクト権限編集」画面で F6 (新ユーザーの追加) を押して、画面にリストされていないユーザーに権限を与えます。
4. Enter キーを押します。
5. 「オブジェクト権限編集」画面は、ライブラリー記述用紙の第 1 部と第 2 部の両方と一致しているはずです。

新しいオブジェクトの共通権限 (CRTAUT) は、ライブラリー用の「オブジェクト権限編集」画面には表示されません。ライブラリーの CRTAUT を表示するには、ライブラリー表示 (DSPLIB) コマンドを使用します。また、この手順を使用して、システム上のオブジェクトに対する特定権限を設定することもできます。これで、オブジェクトに対する特定権限を設定することができます。

オブジェクトに対する権限の設定:

アプリケーション・ライブラリー内のオブジェクトに対する特定権限を設定するための手順は、ライブラリーに対する特定権限を設定する場合と同じです。

1. EDTOBJAUT と入力して、F4 (プロンプト) を押します。
2. プロンプト画面に情報を入力して、Enter キーを押します。
3. 「オブジェクト権限編集」画面に権限情報を入力して、Enter キーを押します。

これで、一度に複数のオブジェクトに対する権限を設定することができます。 『複数のオブジェクトの権限の設定』を参照してください。

複数のオブジェクトの権限の設定:

複数のオブジェクトに対するセキュリティーを設定するには、 オブジェクト権限認可 (GRTOBJAUT) コマンドを使用します。

GRTOBJAUT と入力して、F4 (プロンプト) を押します。

注: 多くのコマンドでは、最初のいくつかの文字の後にアスタリスク(*) を続ける形式でパラメーターを指定できます。システムは、それらの文字で始まる名前のすべてのオブジェクトに対して操作を実行します。

ここまでの作業内容を確認し、システムが必要な権限を変更したかどうか検証するために、DSPJOBLOG コマンドを使用します。

『プリンター出力の保護』に進む前に、EDTOBJAUT または GRTOBJAUT コマンドを使用して、ライブラリー記述用紙の特定権限を設定します。

オブジェクト権限の施行:

オブジェクトへのアクセスを試みた場合は常に、 オペレーティング・システムがそのオブジェクトに対するユーザー権限を検査します。

システムのセキュリティー・レベル (QSECURITY システム値) を 10 または 20 に設定すると、すべてのユーザー・プロファイルが *ALLOBJ 特殊権限を持つようになるため、すべてのユーザーは自動的にすべてのオブジェクトをアクセスする権限を入手することになります。

オブジェクト権限に関するヒント: オブジェクト・セキュリティーを使用しているかどうか分からない場合は、QSECURITY (セキュリティー・レベル) システム値を 調べてください。QSECURITY が 10 または 20 であれば、ユーザー・セキュリティーを使用していません。

セキュリティー・レベルを 30 以上に変更するためには、その前に計画と準備が必要になります。それを行わないと、ユーザーが必要な情報にアクセスできなくなる可能性があります。

メニュー・セキュリティーの設定

この項では、メニュー・セキュリティーを設定するためのユーザー・プロファイル・パラメーターについて説明します。

サーバーは、メニュー・アクセス制御のインプリメントに使用できるユーザー・プロファイル・パラメーターを幾つか備えています。

- **初期メニュー** (INLMNU) パラメーターを使用して、ユーザーがサインオンした後でどのメニューを最初に表示するかを制御することができます。
- **初期プログラム** (INLPGM) パラメーターを使用してユーザーがメニューを見る前にセットアップ・プログラムを実行するか、ユーザーがこのパラメーターを使用して単一のプログラムを実行するように制限することができます。
- **機能限定** (LMTCPB) パラメーターを使用して、ユーザーが限定されたコマンド・セットしか使用しないように制限することができます。このパラメーターは、ユーザーがサインオン表示画面で別の初期プログラムやメニューを指定することも防止します。 LMTCPB パラメーターは、コマンド行から入力されたコマンドのみを制限します。

こうしたユーザー・プロファイル・パラメーターの詳細については、「iSeries 機密保護解説書」の『初期メニュー』、『初期プログラム』および『制限機能』を参照してください。

関連概念

14 ページの『メニュー・セキュリティー』
メニュー・セキュリティーは、ユーザーがどのメニュー機能を実行できるかを制御します。

メニュー・アクセス制御の制限:

システムを保護して、ユーザーがシステムを効果的に使用してジョブを実行できるようにするために、単にメニュー・アクセス制御だけに頼ることはできません。

メニュー・アクセス制御に対する制限は数多くあります。コンピューターやユーザーは、この数年間で大きく変わりました。 QUERY プログラムやスプレッドシートなどの多くのツールが使用可能になったため、ユーザーは、一部のプログラムについて自分でプログラミングして、IS 部門の作業負荷を減らすことがで

きるようになりました。SQL や ODBC など、一部のツールには、情報を表示する機能および情報を変更する機能が備わっています。これらのツールをメニュー構造内で使用可能にするのは非常に困難です。

メニュー・アクセス制御を実施しようとする機密保護管理者には、次の 2 つの基本的な問題があります。

- ユーザーをメニューに限定できた場合、最新のツールを使用できる範囲が限定されるため、ユーザーはおそらくこの処置を歓迎しません。
- 限定できなかった場合、メニュー・アクセス制御で保護できると考えていた重要な機密情報が危険にさらされる可能性があります。システムがネットワークに参加していると、メニュー・アクセス制御を実施する能力が減少します。たとえば、LMTCPB パラメーターは、対話式セッションでコマンド行から入力されたコマンドにのみ適用されます。 LMTCPB パラメーターは、PC ファイル転送、FTP、リモート・コマンドなど、通信セッションからの要求には影響を与えません。

オブジェクト・セキュリティーによるメニュー・アクセス制御の拡張:

この項では、メニュー・アクセス制御を補完するオブジェクト・セキュリティー環境を構築する上での提案を示します。

システムとの接続に使用できる多くのオプションが存在するため、今後の実行可能なサーバーのセキュリティー方式ではメニュー・アクセス制御にのみ依存するわけにはいきません。ユーザーがアプリケーションを実行するためにオブジェクトに対して持つ必要のある適切な権限を付与することにより、メニュー・アクセス制御を強化できます。その後で、ユーザーをグループに割り当て、そのグループに適切な権限を与えます。この方法は、道理に合っていて、しかも論理的です。しかし、システムが長年操作され、アプリケーションの数が増えていれば、アプリケーションの分析やオブジェクト権限のセットアップといった作業は大変なものになります。

この問題の解決として、現行メニューを使用して移行環境を設定しながら、アプリケーションとオブジェクトを徐々に分析していくことができます。

ヒント: プログラム所有者の権限を借用するプログラムに現行メニューを組み合わせている場合、メニュー・アクセス制御の移行の枠を超えている場合があります。権限を借用するプログラムと、これらのプログラムを所有するユーザー・プロファイルの両方を保護してください。

例: メニュー制御環境の変更:

この例では、オーダー・エントリー (OEMENU) メニューのメニュー制御環境、および関連するファイルとプログラムを変更します。

この例では、以下の前提事項と要件をもとに開始されます。

- すべてのファイルは ORDERLIB ライブラリーに入っています。
- すべてのファイルの名前が分かっているわけではありません。また、メニュー・オプションがそれぞれのファイルに対してどの権限を必要としているかも分かりません。
- メニューおよびそれによって呼び出されるすべてのプログラムは ORDERPGM というライブラリーに入っています。
- システムにサインオンできるすべてのユーザーが、すべてのオーダー・ファイル、カスタマー・ファイル、および項目ファイル (たとえば、QUERY やスプレッドシート) の情報を表示できるようにします。
- 現行のサインオン・メニューが OEMENU であるユーザーのみが、ファイルを変更できなければなりません。これらのユーザーは、メニュー上のプログラムを使用してこれを行わなければなりません。
- 機密保護管理者以外のシステム・ユーザーは、*ALLOBJ や *SECADM の特殊権限を持っていません。

QUERY の要件を満たすようにこのメニュー・アクセス制御環境を変更するには、次のステップを実行します。

1. 初期メニューが OEMENU であるユーザーのリストを作成します。ユーザー・プロファイル印刷 (PRTUSRPRF *ENVINFO) コマンドを使用して、システム上のすべてのユーザー・プロファイルの環境をリストします。この報告書には、初期メニュー、初期プログラム、および現行ライブラリーが含まれています。
2. OEMENU オブジェクト (これは *PGM オブジェクトまたは *MENU オブジェクト) が、サインオンに使用しないユーザー・プロファイルによって所有されていることを確認します。ユーザー・プロファイルを使用不可にするか、または *NONE のパスワードをもたせます。 この例では、OEOWNER が OEMENU プログラム・オブジェクトを所有していると仮定しています。
3. OEMENU プログラム・オブジェクトを所有するユーザー・プロファイルが、グループ・プロファイルでないことを確認します。次のコマンドを使用することができます。`DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)`
4. OEMENU プログラムが OEOWNER ユーザー・プロファイルの権限を借用するように、これを変更します。 CHGPGM コマンドを使用して、USRPRF パラメーターを *OWNER に変更します。 *MENU オブジェクトは権限を借用できません。 OEMENU が *MENU オブジェクトであれば、以下のいずれかを行ってこの例に当てはめることができます。
   - メニューを表示するプログラムを作成します。
   - ユーザーが OEMENU メニューからオプションを選択するときに実行するプログラムの借用権限を使用します。
5. 次の 2 つのコマンドを入力して、ORDERLIB 内のすべてのファイルの共通権限を *USE に設定します。`RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC) AUT(*ALL)GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC) AUT(*USE)` *USE 権限を選択した場合は、ユーザーは、 PC ファイル転送または FTP を使用してこのファイルをコピーできるということを忘れないでください。
6. 次のコマンドを入力して、メニュー・プログラムを所有するプロファイルに、ファイルに対する *ALL 権限を与えます。`GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER) AUT(*ALL)` 多くのアプリケーションでは、ファイルに対する *CHANGE 権限で十分です。しかし、アプリケーションによっては、*CHANGE よりも大きな権限を必要とする機能 (たとえば、物理ファイル・メンバーの消去など) を実行することもあります。最終的には、導入先が各アプリケーションを分析し、当該アプリケーションに必要な最小権限のみを提供しなければならなくなります。ただし、移行期間にあるときは、*ALL 権限を借用することにより、権限不足が原因で発生するようなアプリケーション障害が回避されます。
7. 次のように入力して、オーダー・ライブラリーのプログラムに対する権限を制限します。`GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC) AUT(*EXCLUDE)`
8. 次のコマンドを入力して、ライブラリーのプログラムに対する権限を OEOWNER プロファイルに与えます。`GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER) AUT(*USE)`
9. 各ユーザーごとに次のコマンドを入力して、ステップ 1 で識別されたユーザーに、メニュー・プログラムに対する権限を与えます。`GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM) USER(user-profile-name) AUT(*USE)`

上記のステップを完了すると、明示的に除外されていないすべてのシステム・ユーザーが、 ORDERLIB ライブラリーのファイルにアクセスできるようになります (しかし変更はできません)。 OEMENU プログラムに対する権限を持っているユーザーは、 メニューに示されているプログラムを使用して、 ORDERLIB ライブラリーのファイルを更新することができます。 これで、OEMENU プログラムに対する権限を持っ

ているユーザーだけが、 このライブラリーのファイルを変更できるようになりました。 オブジェクト・セキュリティーとメニュー・アクセス制御を組み合わせることで、 ファイルが保護されます。

ユーザー・データが含まれているすべてのライブラリーについて上記のステップを完了すると、 データベース更新を制御するための単純な体系が作成されます。この方式により、 システム・ユーザーは、承認されたメニューとプログラムを使用するとき以外に、 データベース・ファイルを更新できなくなります。同時に、意思決定サポート・ツールを持つユーザーや、 他のシステムや PC からのリンクを持つユーザーが、データベース・ファイルを表示、分析、 あるいはコピーしたりできるようになりました。

ヒント: システムがネットワークに参加すると、 *USE 権限が予期以上の権限を発揮することがあります。たとえば、FTP の場合に、あるファイルに対する *USE 権限を持っていれば、 そのファイルを別のシステム (PC を含む) にコピーすることができます。

ライブラリー・セキュリティーの使用によるメニュー・セキュリティーの補足:

この項では、特定のメニューのユーザーにライブラリー権限を設定する方法について説明します。

ライブラリーのオブジェクトにアクセスするには、オブジェクトに対する権限とライブラリーに対する権限のどちらも持っていなければなりません。ほとんどの操作では、ライブラリーに対する *EXECUTE 権限か *USE 権限のどちらかが必要です。

状況に応じて、ライブラリー権限をオブジェクト保護のための簡単な手段として使用することができます。たとえば、オーダー・エントリー・メニューの例の場合、オーダー・エントリー・メニューに対する権限を持っているすべてのユーザーは、ORDERPGM ライブラリー内のすべてのプログラムを使用することができます。個々のプログラムを保護するのではなく、ORDERPGM ライブラリーに対する共通権限を *EXCLUDE に設定することができます。そうすれば、ライブラリーに対する *USE 権限を特定のユーザー・プロファイルに与えることができ、これにより、ライブラリーのプログラムを使用できるようになりますこの場合、プログラムに対する共通権限が *USE であるか、またはそれより大きいと想定しています。

ライブラリー権限を、オブジェクト権限を管理するための単純で効率的な方式として使用することができます。ただし、保護しようとしているライブラリーの内容について熟知していて、オブジェクトを不注意にアクセスしないようにすることが必要です。

統合ファイル・システムの保護

統合ファイル・システムは、システムに情報を保管し、それを表示するための複数の方法を提供します。

統合ファイル・システムは i5/OS オペレーティング・システムの一部であり、ストリーム入出力操作をサポートします。統合ファイル・システムには、パーソナル・コンピューターのオペレーティング・システムや UNIX オペレーティング・システムに類似した (かつ、互換性のある) 記憶管理方式が装備されています。

統合ファイル・システムでは、階層ディレクトリー構造の観点からシステム上のすべてのオブジェクトを表示することができます。しかし、多くの場合、ユーザーにとっては、それぞれのファイル・システムの最も一般的な方法でオブジェクトが表示されます。たとえば、標準的なシステム・オブジェクトは QSYS.LIB ファイル・システムに入っています。通常、ユーザーにとって、これらのオブジェクトはライブラリーとして表示され、QDLS ファイル・システムに含まれるオブジェクトはフォルダー内の文書として表示されます。『ルート』 (/)、QOpenSys、およびユーザー定義のファイル・システムは、階層ディレクトリーの構造を提示します。

機密保護管理者は、次のことを理解していなければなりません。

- システムで使用されるファイル・システム

- 各ファイル・システムに固有なセキュリティー特性

『ルート』 (/) ファイル・システムは、IBM システム上にある他のすべてのファイル・システムの基盤として機能します。ルート・ファイル・システムは、高いレベルから、システム上のすべてのオブジェクトに関する総合的な視点を提供します。IBM システムに常駐可能な他のファイル・システムは、各ファイル・システムの基本的な目的に応じて、オブジェクトの管理と統合に関してそれぞれ異なる方法を提供します。たとえば、QOPT (光学式) ファイル・システムを使用すると、iSeries Access for Windows ファイル・サーバーを含むシステム・アプリケーションおよびサーバーは、システム上の CD-ROM ドライブにアクセスできます。同様に、QFileSvr.400 ファイル・システムを使用すると、アプリケーションはリモート・システム上にある統合ファイル・システム・データにアクセスすることができます。QLANSrv ファイル・サーバーを使用すると、iSeries 統合 xSeries サーバーに保管されたファイルや、ネットワーク内の他の接続サーバーに保管されているファイルにアクセスすることができます。

各ファイル・システムのセキュリティー手法は、そのファイル・システムで使用可能なデータによって異なります。たとえば、QOPT ファイル・システムはオブジェクト・レベルのセキュリティーを提供しません。権限情報を CD-ROM に書き込むテクノロジーがないためです。QFileSvr.400 ファイル・システムの場合は、ファイルが物理的に格納され管理されるリモート・システムでアクセス制御が行われます。QLANSrv のようなファイル・システムの場合は、iSeries 統合 xSeries サーバーがアクセス制御を行います。セキュリティー・モデルに違いはありますが、多くのファイル・システムは、権限変更 (CHGAUT) や所有者変更 (CHGOWN) などの統合ファイル・システム・コマンドを介して、一貫性のあるアクセス制御の管理をサポートします。

プリンター出力待ち行列の保護

ここでは、プリンター出力待ち行列のセットアップ・タスクについて説明し、それがなぜ重要か、および段階的な手順を示します。

1. CRTOUTQ (出力待ち行列作成) を入力して、F4 (プロンプト) を押します。
2. 出力待ち行列およびライブラリーの名前を記入します。
3. F10 (追加のパラメーター) を押します。
4. 出力待ち行列のセキュリティー情報が見つかるまでページ送りを行います。
5. 出力待ち行列を使用および管理できるユーザーを制御するには、「出力待ち行列およびワークステーションのセキュリティー」用紙の情報を入力します。
6. Enter キーを押して、確認メッセージをチェックします。

考えられるエラー	回復
手順 3 で F10 ではなく Enter キーを押した。	出力待ち行列変更 (CHGOUTQ) コマンドを使用して、追加情報を入力します。
出力待ち行列が間違ったライブラリーに作成された。	オブジェクト移動 (MOVOBJ) コマンドを使用して、出力待ち行列を正しいライブラリーに移動します。

これで、プリンター出力を出力待ち行列に割り当てることができます。

ワークステーションの保護

プリンター出力の保護を行った後、ワークステーションの保護を行う必要があります。ワークステーションを許可する方法は、システム上の他のオブジェクトを許可する方法と同じです。ワークステーションに対する権限をユーザーに与えるには、EDTOBJAUT コマンドを使用します。

システム・ユーザーたちは、自分の机の上のパーソナル・コンピューター (PC) をワークステーションとして使用します。システム・ユーザーは PC 上でツールを実行したり、PC を使用してサーバーに接続します。PC を IBM システムに接続するほとんどの方法は、ワークステーション・エミュレーションよりも多くの機能を提供します。PC はシステムにとってディスプレイのように見え、ユーザーに対話式サインオン・セッションを提供します。さらに、PC は IBM システムにとって別のコンピューターのように見え、ファイル転送やリモート・プロシージャー呼び出しなどの機能を提供します。

IBM システム機密保護管理者は、以下のことを認識しておく必要があります。

- システムに接続している PC ユーザーが使用できる機能
- PC ユーザーがアクセスできる IBM システム資源

拡張 PC 機能 (ファイル転送やリモート・プロシージャー呼び出しなど) をまだ処理できないセキュリティー体系の場合には、これらの拡張 PC 機能を使用不可にすることができます。おそらく長期的な目標は、システムの情報を保護しながら、拡張 PC 機能を許可することでしょう。以下のトピックでは、PC アクセスに関連したセキュリティーの問題をいくつか説明します。

ワークステーションからのデータ・アクセスの保護

一部の PC クライアント・ソフトウェアは、サーバーに情報を保管するために共用フォルダーを使用します。システム・データベース・ファイルにアクセスするため、限定され適切に定義されたインターフェースのセットが PC ユーザーに提供されます。ほとんどのクライアント/サーバー・ソフトウェアに含まれるファイル転送機能を使用すると、PC ユーザーはサーバーと PC との間でファイルをコピーすることができます。DDM ファイル、リモート SQL または ODBC ドライバーなどのデータベース・アクセス機能を使用すると、PC ユーザーはサーバーのデータにアクセスすることができます。

この環境では、サーバー資源にアクセスする PC ユーザーの要求をインターセプトして評価するためのプログラムを作成することができます。要求が DDM ファイルを使用するときには、分散データ管理アクセス (DDMACC) ネットワーク属性で出口プログラムを指定します。一部の PC ファイル転送の方法の場合、クライアント要求アクセス (PCSACC) ネットワーク属性で出口プログラムを指定します。あるいは、登録機能を使用するために、PCSACC(*REGFAC) を指定することもできます。要求が他のサーバー機能を使ってデータにアクセスする場合には、それらのサーバー機能に出口プログラムを登録する WRKREGINF コマンドを使用することができます。

しかし、出口プログラムの設計は難しい可能性があり、ほとんどの出口プログラムは誰にでも扱えるものではありません。出口プログラムは、オブジェクト権限に置き換わるものではありません。オブジェクト権限は、あらゆるソースからの無許可アクセスからオブジェクトを保護するように意図されています。

一部のクライアント・ソフトウェア (たとえば IBM iSeries Access for Windows) は、IBM システム上のデータを保管およびアクセスするために統合ファイル・システムを使用します。統合ファイル・システムを使用すると、サーバー全体が PC ユーザーにとってより簡単に使用できるようになります。オブジェクト権限はより一層不可欠になります。十分な権限を持つユーザーは、統合ファイル・システムを通じて、サーバー・ライブラリーを PC ディレクトリーであるかのように表示することができます。単純な移動およびコピー・コマンドを使用して、システム・ライブラリーから PC ディレクトリーに、またはその逆に、データをすぐに移動することができます。システムは、自動的にデータの形式を適切に変更します。

注: QSYS.LIB ファイル・システムのオブジェクトの使用を制御する権限リストを使用することができます。

統合ファイル・システムの長所は、ユーザーと開発者にとって単純であることです。1 つのインターフェースを使って、ユーザーは複数の環境でオブジェクトの作業を行うことができます。PC ユーザーは、オブジ

ェクトにアクセスするのに特別なソフトウェアや API を必要としません。その代わり、PC ユーザーは、使い慣れた PC コマンドや「ポイント・アンド・クリック」を使ってオブジェクトを直接処理することができます。

PC が接続されているすべてのシステムの場合、特に統合ファイル・システムを使用するクライアント・ソフトウェアを使用するシステムの場合、適切なオブジェクト権限構造が重要です。セキュリティーは i5/OS 製品に統合されているため、データにアクセスする要求は、すべて権限検査プロセスを通らなければなりません。権限検査は、すべてのソースからの要求と、あらゆる方法を使用するデータ・アクセスとに適用されます。

ワークステーションからのアクセスについてのオブジェクト権限

オブジェクトの権限をセットアップするときには、その権限が PC ユーザーに何を提供するかを評価する必要があります。たとえば、ユーザーがファイルに対する *USE 権限を持っていると、そのユーザーはファイルのデータを表示したり印刷することができます。ユーザーは、そのファイル内の情報を変更したり、そのファイルを削除することはできません。 PC ユーザーの場合、表示は「読み取り」と同等です。これは、ユーザーがその PC にファイルのコピーを作成するのに十分な権限を提供します。これは、管理者の意図と異なる可能性があります。

重要なファイルの場合、ダウンロードを防止するために、共通認可を *EXCLUDE に設定する必要があるかもしれません。その後、サーバー上のファイルを表示するための別の方法 (たとえば、権限を借用するプログラム・メニュー) を提供することができます。ダウンロードを防止する別の方法は、PC ユーザーが (対話式サインオン以外の) サーバー機能を開始するたびに、出口プログラムを実行することです。

ネットワーク属性変更 (CHGNETA) コマンドを使用すると、PCSACC ネットワーク属性に出口プログラムを指定することができます。あるいは、登録情報処理 (WRKREGINF) コマンドを使って出口プログラムを登録することもできます。使用する方法は、PC がシステムのデータにアクセスする方法と、PC が使用するクライアント・プログラムによって異なります。出口プログラム (QIBM_QPWFS_FILE_SERV) は、統合ファイル・システムへの iSeries Access およびネットサーバーからのアクセスに適用されます。このプログラムは、他のメカニズム (FTP、ODBC など) を使用する PC からのアクセスは防止しません。

ユーザーが PC からサーバー・データベース・ファイルにデータをコピーできるように、PC ソフトウェアは一般的にアップロード機能も提供します。権限体系を正しくセットアップしないと、PC ユーザーは、ファイル内のすべてのデータを PC のデータでオーバーレイする可能性があります。CHANGE 権限の割り当ては注意深く行う必要があります。ファイル操作に必要な権限については、「iSeries 機密保護解説書」の『付録 D』を参照してください。

ユーザーがワークステーションでサインオンするには、*CHANGE 権限を持っていなければなりません。QLMTSECOFR システム値が「no (0)」の場合、機密保護担当者または *ALLOBJ 権限を持っている人であれば誰でも任意のワークステーションでサインオンできます。 QLMTSECOFR システム値が「yes (1)」の場合、次のガイドラインを使用して、ワークステーションに権限を設定します。

ワークステーションでのサインオンを許可されているユーザー	共通権限	QSECOFR 権限	個々のユーザー権限
すべてのユーザー	*CHANGE	*CHANGE	必須ではない
選択されたユーザーのみ	*EXCLUDE	権限なし	*CHANGE
選択されたユーザーおよびすべてのオブジェクトに対する権限を持っているユーザー	*EXCLUDE	*CHANGE	*CHANGE

ワークステーションでのサインオンを許可されているユーザー	共通権限	QSECOFR 権限	個々のユーザー権限
すべてのオブジェクトに対する権限を持っているユーザー以外のすべてのユーザー	*CHANGE	権限なし	必須ではない

IBM システム機密保護管理者は、以下のことを認識しておく必要があります。

- システムに接続している PC ユーザーが使用できる機能
- PC ユーザーがアクセスできる IBM システム資源

拡張 PC 機能 (ファイル転送やリモート・プロシージャー呼び出しなど) をまだ処理できないセキュリティー体系の場合には、これらの拡張 PC 機能を使用不可にすることができます。おそらく長期的な目標は、システムの情報を保護しながら、拡張 PC 機能を許可することでしょう。

システム操作員メッセージ待ち行列へのアクセスを制限する前に、「出力待ち行列およびワークステーションのセキュリティー」用紙に含まれる情報に基づいて、EDTOBJAUT コマンドを使ってワークステーションを保護してください。

ワークステーションからのアクセスについてのオブジェクト権限:

オブジェクトの権限をセットアップするときには、その権限が PC ユーザーに何を提供するかを評価する必要があります。

たとえば、ユーザーがファイルに対する *USE 権限を持っていると、そのユーザーはファイルのデータを表示したり印刷することができます。ユーザーは、そのファイル内の情報を変更したり、そのファイルを削除することはできません。

PC ユーザーの場合、表示権限があれば、ユーザーの PC 上にファイルのコピーを作成することが可能です。これは、管理者の意図と異なる可能性があります。重要なファイルの場合、ダウンロードを防止するために、共通認可を *EXCLUDE に設定する必要があるかもしれません。その後、サーバー上のファイルを表示するための別の方法 (たとえば、権限を借用するメニューおよびプログラム) を提供することができます。

ダウンロードを防止する別の方法は、PC ユーザーが (対話式サインオン以外の) サーバー機能を開始するたびに、出口プログラムを実行することです。ネットワーク属性変更 (CHGNETA) コマンドを使用すると、PCSACC ネットワーク属性に出口プログラムを指定することができます。あるいは、登録情報処理 (WRKREGINF) コマンドを使って出口プログラムを登録することもできます。使用する方法は、PC がシステムのデータにアクセスする方法と、PC が使用するクライアント・プログラムによって異なります。出口プログラム (QIBM_QPWFS_FILE_SERV) は、IFS への iSeries Access およびネットサーバーからのアクセスに適用されます。このプログラムは、他のメカニズム (FTP、ODBC など) を使用する PC からのアクセスは防止しません。

アプリケーション管理:

アプリケーション管理は、iSeries サーバーのグラフィカル・ユーザー・インターフェース (GUI) である iSeries ナビゲーターのオプションの構成要素です。

アプリケーション管理を使用すると、システム管理者は、特定のサーバー上のユーザーおよびグループが使用できる機能またはアプリケーションを制御できます。これによって、クライアントを介してサーバーにア

クセスするユーザーが使用できる機能を制御することもできます。重要な点として、Windows クライアントからサーバーにアクセスする場合、どの管理機能を使用できるかを決定するのは iSeries サーバーのユーザーであって、Windows のユーザーではありません

iSeries ナビゲーターのアプリケーション管理についての詳細は、「アプリケーション管理」を参照してください。

ポリシー管理

ポリシーとは、管理者が自分のクライアント PC 上でソフトウェアを構成するためのツールです。ポリシーによって、ユーザーがアクセスできる PC 上の機能およびアプリケーションを制限できます。また、ポリシーを使用すると、特定のユーザーまたは特定の PC が使用すべき構成を推奨または指示することもできます。

注: ポリシーは、サーバー資源を制御しません。ポリシーは、サーバーのセキュリティーに置き換わるものではありません。ポリシーを使用すれば、特定のユーザー、特定の PC を使って iSeries Access がサーバーにアクセスする方法を制御することができます。ただし、他のメカニズムを介してサーバー資源にアクセスする方法は、変更されません。

ポリシーはファイル・サーバーに保管されます。 ユーザーが Windows ワークステーションにサインオンするたびに、 その Windows ユーザーに適用されるポリシーがファイル・サーバーからダウンロードされます。ユーザーがワークステーション上で作業を始める前に、ポリシーはレジストリーに適用されます。

Microsoft ポリシーとアプリケーション管理の比較

iSeries Access Express は、ネットワーク内に管理制御をインプリメントするために、Microsoft システム・ポリシーと iSeries ナビゲーター・アプリケーション管理の 2 つの異なるストラテジーをサポートします。どちらの方法がお客様のニーズに最も合うかを検討するときは、以下の点を考慮してください。

Microsoft システム・ポリシー:

ポリシーは PC 主導型で、特定の OS/400 リリースに依存しません。 PC と Windows ユーザーの両方にポリシーを適用できます。つまり、ユーザーとはサーバーのユーザー・プロファイルではなく、Windows ユーザー・プロファイルを意味します。ポリシーを使って制限および構成を行うことが可能です。ほとんどの場合、ポリシーはアプリケーション管理に比べて、きめ細かい制御と広範な機能を提供します。その理由は、ユーザーが特定の機能を使用できるか否かを判別するときに、サーバーに接続する必要がないからです。ポリシーのインプリメンテーションは、アプリケーション管理のインプリメンテーションより複雑です。なぜなら、Microsoft システム・ポリシー・エディターを使用する必要があり、ポリシーをダウンロードできるように PC を個別に構成しなければならないためです。

iSeries ナビゲーターのアプリケーション管理:

アプリケーション管理は、ユーザー・プロファイルにデータを関連付けます (これに対して Microsoft システム・ポリシーは Windows プロファイルに関連付けられます)。アプリケーション管理では、iSeries ナビゲーターのグラフィカル・ユーザー・インターフェースを使用して管理を行います。これは、ポリシー・エディターを使用するよりずっと簡単です。アプリケーション管理の情報は、ユーザーがどの PC からサインオンするかに関係なくユーザーに適用されます。 iSeries ナビゲーター内の特定の機能を制限することができます。制限したいすべての機能がアプリケーション管理で処理可能になっており、ご使用の OS/400 のバージョンがアプリケーション管理をサポートしている場合には、アプリケーション管理を使用することをお勧めします。

ODBC アクセスの防止:

Open Database Connectivity (ODBC) ツールを使用すれば、PC アプリケーションは iSeries データに PC データとまったく同じようにアクセスできます。

ODBC プログラマーは、データの物理位置を PC アプリケーションのユーザーに意識されないようにすることができます。ODBC のセキュリティーに関する考慮事項の詳細については、『iSeries Access for Windows ODBC のセキュリティー』を参照してください。

ワークステーション・セッション・パスワードのセキュリティーに関する考慮事項:

このトピックでは、ワークステーションとサーバーの間でやり取りされるパスワードに関するセキュリティー上の考慮事項を説明します。

通常、PC ユーザーは、iSeries Access などの接続ソフトウェアを開始するときに、サーバーに対してユーザー ID とパスワードを一度入力します。パスワードは暗号化されて PC メモリーに保管されます。ユーザーが同じサーバーへの新規セッションを確立するたびに、PC はユーザー ID とパスワードを自動的に送ります。

一部のクライアント/サーバー・ソフトウェアは、対話式セッションで「サインオン」画面をバイパスするオプションも提供します。そのソフトウェアは、ユーザーが対話式 (5250 エミュレーション) セッションを開始するときに、ユーザー ID と暗号化されたパスワードを送ります。このオプションをサポートするには、サーバーの QRMTSIGN システム値を *VERIFY に設定しなければなりません。

「サインオン」画面をバイパスできるように選択する場合、セキュリティーのトレードオフを考慮する必要があります。

機密漏れ: 5250 エミュレーションなどの対話式セッションでは、「サインオン」画面は他の画面と同じです。パスワードの入力時にそのパスワードは画面上に表示されませんが、パスワードはほかのデータ・フィールドと同様に、暗号化されていない形式でリンクを通じて送信されます。特定の種類のリンクの場合、これによって、リンクをモニターしてユーザー ID とパスワードを検出する機会を潜在的な侵入者に与える可能性があります。電子機器を使用してリンクをモニターすることは、しばしば探知と呼ばれます。 V4R4 以降、Secure Sockets Layer (SSL) を使用して、iSeries Access と iSeries サーバー間の通信を暗号化することができます。これにより、パスワードを含むデータは、ハッカーによる探知から保護されます。

「サインオン」画面をバイパスするオプションを選択すると、PC は送信前にパスワードを暗号化します。暗号化により、パスワードが探知によって盗まれる可能性が回避されます。ただし、PC ユーザーが操作上のセキュリティーを必ず実践するようにしなければなりません。 iSeries システムとのセッションが活動中に PC ユーザーが不在であると、ユーザー ID とパスワードを知らなくても別のセッションを開始する機会を他人に与えることになります。システムが長時間非活動のときには PC をロックするようにセットアップし、セッションの再開にはパスワードを必要とするようにしてください。

たとえ「サインオン」画面のバイパスを選択しなくても、セッション活動中に PC ユーザーが不在になると、機密漏れの可能性があります。ユーザー ID とパスワードを知らなくても、他人が PC ソフトウェアを使ってサーバー・セッションを開始し、データにアクセスする可能性があります。5250 エミュレーションの場合、少ない知識しかなくてもセッションを開始してデータ・アクセスを始めることができるため、機密漏れの可能性がやや大きくなります。

また、iSeries Access セッションを切断した場合の影響について、ユーザーに通知することも必要です。多くのユーザーは、切断オプションによってサーバーへの接続が完全に停止するものと、間違って考えています。実際は、ユーザーが切断オプションを選択すると、サーバーはそのユーザーのセッションを別のユーザ

ーが使用できるようにします。しかし、サーバーへのクライアントの接続はまだ開いたままです。別のユーザーが無保護の PC の前に座り、ユーザー ID とパスワードを一度も入力することなく、サーバー資源にアクセスできる可能性もあります。

セッションの切断を必要とするユーザーには、2 つのオプションを提案することができます。

- パスワードを必要とするロック機能を PC に必ず設定する。これにより、パスワードを知らない人がユーザー不在の PC を使用できなくなります。
- Windows をログオフするか、PC を再始動 (リブート) して、セッションを完全に切断する。これにより、iSeries へのセッションが終了します。

また、iSeries Access for Windows を使用する場合に機密漏れの可能性があることについても、ユーザーに通知する必要があります。iSeries 資源を識別するためにユーザーが UNC (汎用命名規則) を指定した場合、Win95 クライアントまたは Windows NT クライアントは、ネットワーク接続を作成してサーバーにリンクします。ユーザーは UNC を指定するため、ユーザーはこれをマップされたネットワーク・ドライブとして考えません。ユーザーがネットワーク接続の存在に気付かないことさえよくあります。しかし、PC のディレクトリー・ツリーにサーバーが表示されるため、このネットワーク接続は、ユーザー不在の PC で機密漏れする可能性があります。ユーザーのセッションに強力なユーザー・プロファイルがある場合、ユーザー不在の PC でサーバー資源が機密漏れする恐れがあります。上記の例と同様に、解決方法は、ユーザーに機密漏れについて必ず理解させ、PC のロック機能を必ず使用させることです。

リモート・コマンドとリモート・プロシージャーからのサーバーの保護:

このトピックでは、リモート・コマンドとリモート・プロシージャーをサーバーで実行する方法をなぜ考慮する必要があるかを説明します。

iSeries Access などのソフトウェアをよく知っている PC ユーザーは、「サインオン」画面を使用せずにサーバー上のコマンドを実行することができます。 PC ユーザーがサーバー・コマンドを実行する方法には、たとえば以下のようなものがあります。PC ユーザーの使用できる方法は、クライアント/サーバー・ソフトウェアに応じて異なります。

- ユーザーは DDM ファイルを開いてリモート・コマンド機能を使用することにより、コマンドを実行できる。
- iSeries Access Optimized Clients などの一部のソフトウェアは、DDM を使用しなくても、分散プログラム呼び出し (DPC) API を通じてリモート・コマンド機能を提供する。
- リモート SQL および ODBC などの一部のソフトウェアは、DDM や DPC を使用しなくても、リモート・コマンド機能を提供する。

リモート・コマンド・サポート用に DDM を使用するクライアント/サーバー・ソフトウェアの場合、リモート・コマンドを完全に防止するために DDMACC ネットワーク属性を使用することができます。 他のサーバー・サポートを使用するクライアント/サーバー・ソフトウェアの場合、サーバー用に出口プログラムを登録することができます。 リモート・コマンドを許可したい場合には、データを適切に保護するオブジェクト権限体系を必ず構築しなければなりません。リモート・コマンド機能は、ユーザーにコマンド行を提供することと同等です。 さらに、iSeries が DDM を通じてリモート・コマンドを受け取るとき、システムはユーザー・プロファイルの制限機能 (LMTCPB) 設定を実施しません。

リモート・コマンドとリモート・プロシージャーからのワークステーションの保護:

IBM iSeries Access for Windows には、PC でリモート・コマンドを受け取る機能があります。

サーバーに対するリモート・コマンド実行 (RUNRMTCMD) コマンドを使用すると、接続した PC でプロシージャーを実行することができます。RUNRMTCMD 機能は、システム管理者とヘルプ・デスク担当者にとって役に立つツールです。しかし、この機能は、故意あるいは偶然に PC データを損傷する機会も与えてしまいます。

PC には、iSeries サーバーと同一のオブジェクト権限機能はありません。RUNRMTCMD コマンドの問題から保護するための最善の方法は、コマンドにアクセスできるシステム・ユーザーを注意深く制限することです。IBM iSeries Access for Windows には、特定の PC でリモート・コマンドを実行できるユーザーを登録する機能があります。 TCP/IP 経由の接続の場合、リモート・コマンド・アクセスを制御するためにクライアントで特性制御パネルを使用することができます。ユーザー ID またはリモート・システム名によって、ユーザーを許可することができます。SNA 経由の接続の場合、一部のクライアント・ソフトウェアは会話のセキュリティーをセットアップする機能を提供します。その他のクライアント・ソフトウェアを使用する場合には、着信コマンド機能をセットアップするかどうか選択するだけです。

クライアント・ソフトウェアと接続タイプ (TCP/IP や SNA など) の組み合わせごとに、接続されている PC への着信コマンドの可能性を検討する必要があります。クライアントの資料で「着信コマンド」または「RUNRMTCMD」を検索して調べてください。この機能を許可または防止するようにクライアントを正しく (セキュアに) 構成する方法について、PC ユーザーとネットワーク管理者にアドバイスできるように準備してください。

ゲートウェイ・サーバー:

iSeries システムと PC の間に中間サーバーやゲートウェイ・サーバーを使用するネットワーク内に、ご使用のシステムが存在する場合があります。

たとえば、iSeries システムが、PC サーバーを使用して LAN (サーバーに接続している複数の PC が含まれている) に接続しているとします。この状況では、ゲートウェイ・サーバーで実行中のソフトウェアの機能によってセキュリティーの問題が異なります。一部のソフトウェアを使用すると、iSeries システムは、ゲートウェイ・サーバーからのダウンストリームであるユーザー (USERA や USERC など) について認識しません。サーバーは、単一ユーザー (USERGTW) としてシステムにサインオンします。サーバーは、ダウンストリーム・ユーザーからのすべての要求を処理するために USERGTW ユーザー ID を使用します。USERA からの要求は、サーバーにはユーザー USERGTW からの要求のように見えます。

これが該当する場合には、セキュリティーを実施するためにゲートウェイ・サーバーに依存しなければなりません。ゲートウェイ・サーバーのセキュリティー機能を理解および管理する必要が生じます。iSeries サーバーから見ると、すべてのユーザーは、ゲートウェイ・サーバーがセッション開始に使用するユーザー ID と同じ権限を持ちます。これは、権限を借用してコマンド行を提供するプログラムを実行するのと同等と考えることができます。

他のソフトウェアを使用する場合、ゲートウェイ・サーバーは個々のユーザーから iSeries サーバーに要求を渡します。iSeries サーバーは、USERA が特定オブジェクトへのアクセスを要求していることを認識します。ゲートウェイは、システムからほとんど意識されません。

ゲートウェイ・サーバーを使用するネットワーク内にシステムが存在する場合、ゲートウェイ・サーバーが使用するユーザー ID にどの程度の権限を提供するかを評価する必要があります。また、以下のことを理解する必要もあります。

- ゲートウェイ・サーバーが実施するセキュリティーのメカニズム。
- ダウンストリーム・ユーザーが iSeries システムにどのように見えるか。

無線 LAN 通信:

一部のクライアントは、iSeries 無線 LAN を使用してシステムと無線で通信します。

システムの無線 LAN は、無線周波数通信技術を使用します。機密保護管理者は、システム無線 LAN 製品の次のようなセキュリティー特性について理解しておく必要があります。

- これらの無線 LAN 製品は、スペクトル拡散技術を使用しています。これと同じテクノロジーは、これまで無線伝送を安全に行うために米国政府によって使用されてきました。データ伝送を電子的にモニターしようとする人にとって、そのデータ伝送は、実際の伝送ではなくノイズのように見えます。
- 無線接続では、次の 3 つのセキュリティー関連の構成パラメーターが使用されます。
  - データ転送率 (2 つのデータ転送率が可能)
  - 周波数 (5 つの周波数が可能)
  - システム識別コード (800 万の識別コードが可能)

  これらの構成要素を組み合わせると 8000 万種類の構成が可能になり、ハッカーが正しい構成を探そうとしてもそれが見つかる可能性は非常に小さくなります。
- 他の通信方式の場合と同様に、無線通信のセキュリティーはクライアント装置のセキュリティーによって影響されます。システム ID 情報およびその他の構成パラメーターがクライアント装置のファイルに格納されるため、これを保護しなければなりません。
- 無線装置を紛失したり盗まれたりした場合、なくなった (または盗まれた) 装置を使って非許可ユーザーがユーザー・システムにアクセスしようとすると、通常のサーバー・セキュリティー手法 (たとえば、サインオン・パスワードやオブジェクト・セキュリティー) によって保護されます。
- 無線クライアント装置を紛失したり盗まれたりした場合には、すべてのユーザー、アクセス・ポイント、およびシステムに関するシステム ID 情報を変更することを考慮してください。これはちょうど、自分の家の鍵が盗まれた場合にドアのロックを変えるようなものです。
- サーバーを、固有なシステム ID を持ついくつかのクライアント・グループに分割することもできます。こうすれば、装置がなくなったり盗まれたりした場合の影響を低く抑えることができます。この方式が機能するのは、導入システムの特定部分に一部のユーザー・グループを限定できる場合のみです。
- 配線式 LAN 技術とは異なり、無線 LAN 技術は、メーカー独自の仕様になっています。したがって、こうした無線 LAN を対象にした探知機は、一般に入手することはできません。探知機とは、伝送を無許可でモニターする電子装置のことです。

ネットワーク・セキュリティーの設定

以下のトピックでは、TCP/IP プロトコル (FTP、BOOTP、VPN など) および APPC に関するセキュリティー上の推奨事項を示します。

APPC セキュリティーの設定

このグループの項では、APPC セッションのセキュリティーの設定の様々な特徴を取り上げます。

APPC および APPN を使用して相互に通信する i5/OS システムのセキュリティーには様々な局面があります。

- **物理的セキュリティー**。構成可能なシステム、通信回線、およびディスプレイ装置に関するセキュリティーです。
- **ロケーション・セキュリティー**。ネットワーク内の他のシステムの正体を検査します。
- **ユーザー・セキュリティー**。APPC 構成の際にロケーション・パスワード (LOCPWD) パラメーターに *NONE を指定する場合、ローカル・システムおよびリモート・システムにコマンドを発行するユーザーの ID と権利を検査します。

- **資源保護**。セッションの確立時に、機密情報を含んだデータベース・リモート・システムなど特定の資源に対するユーザーのアクセスを制御します。
- **セッション・レベル・セキュリティー**。構成時に、LOCPWD パラメーターにパスワードを指定して設定します。i5/OS システムでは、パスワードを使用して、セッションの確立時にリモート・システムの正体を妥当性検査します。

システムでレベル 10 セキュリティーを使用している場合、APPC は非セキュア・システムとしてネットワークに接続します。i5/OS システムはセッションの確立時にはリモート・システムの正体を妥当性検査しませんし、着信プログラム開始要求でのトランザクション・セキュリティーも必要としません。

i5/OS システムがリモート・システムでレベル 20 以上を使用している場合には、APPC はネットワークにセキュア・システムとして接続します。

APPC セッションの制限:

オブジェクト権限を使用して、APPC セッションへのアクセスを制御します。

ソース・システムの機密保護管理者は、ほかのシステムにアクセスを試行することができるユーザーを制御するためにオブジェクト権限を使用することができます。 APPC 装置記述の共通認可を *EXCLUDE に設定し、特定のユーザーに *CHANGE 権限を与えます。 *ALLOBJ 特殊権限を持つユーザーが APPC 通信を使用しないようにするには、QLMTSECOFR システム値を使用します。

ターゲット・システムの機密保護管理者は、APPC 装置に対する権限を使用して、ユーザーがシステム上で APPC セッションを開始できないようにすることもできます。しかし、どのユーザー ID が APPC 装置記述にアクセスしようとしているかを理解する必要があります。

ヒント: システムの装置記述に対して権限を持つユーザーを検出するには、共通認可オブジェクトの印刷 (PRTPUBAUT *DEVD) コマンドと私用認可オブジェクトの印刷 (PRTPVTAUT *DEVD) コマンドを使用することができます。

システムで APPN を使用する際に、システムが選択した経路用に使用できる既存の装置が無いと、APPN は 新規の APPC 装置を自動的に作成します。 APPN を使用しているシステムの APPC 装置へのアクセスを制限する方法の 1 つは、権限リストを作成することです。権限リストには、APPC 装置に許可すべきユーザーのリストが含まれます。次に、コマンド・デフォルト変更 (CHGCMDDFT) コマンドを使用して CRTDEVAPPC コマンドを変更します。 CRTDEVAPPC コマンドの権限 (AUT) パラメーターに関しては、作成した権限リストにデフォルト値を設定します。

ユーザーまたはアプリケーションに代わって、システムでセッションを要求している別のシステムの正体の妥当性を検査するため、APPC 装置記述でロケーション・パスワード (**LOCPWD**) パラメーターを使用します。ロケーション・パスワードは、名前を偽っているシステムの検出に役立ちます。

ロケーション・パスワードを使用するときには、ネットワークのほかのシステムの機密保護管理者と調整しなければなりません。また、APPC 装置記述および構成リストの作成や変更を行えるユーザーの制御をすることも必要です。システムでは、APPC 装置および構成リストを処理するコマンドを使用するために、*IOSYSCFG 特殊権限が必要です。

ヒント: APPN を使用するときに、ロケーション・パスワードは、装置記述ではなく QAPPNRMT 構成リストに保管されます。

ジョブのユーザー・プロファイルのターゲット・システム割り当て:

ユーザーが別のシステムで APPC ジョブを要求するとき、 その要求には、関連したモード名が含まれています。 モード名は、ユーザーの要求に由来する場合もあれば、 ソース・システムのネットワーク属性のデフォルト値である場合もあります。

ターゲット・システムは、ジョブの実行方法を判別するのに、モード名と APPC 装置名を使用します。ターゲット・システムは、活動状態のサブシステムを検索して、APPC 装置名とモード名に最も合った通信項目がないかどうか調べます。

通信項目は、システムが SECURITY(NONE) 要求用に使用するユーザー・プロファイルを指定します。サブシステム記述における通信項目の例。

```
                                通信項目の表示

サブシステム記述 :   QCMN            状況 :     活動

                                ジョブ                          省略時の       最大
 装置            モード         記述          ライブラリー      ユーザー       活動
*ALL             *ANY           *USRPRF                         *SYS           *NOMAX
*ALL             QPCSUPP        *USRPRF                         *NONE          *NOMAX
```

以下の表は、通信項目におけるデフォルトのユーザー・パラメーターに使用できる値を示したものです。

表 109. デフォルトのユーザー・パラメーターに有効な値

値	結果
***NONE**	デフォルト・ユーザーは使用できません。ソース・システムが要求時にユーザー ID を提供しない場合、ジョブは実行されません。
***SYS**	IBM 提供のプログラム (システム・ジョブ) だけが実行されます。ユーザー・アプリケーションは実行されません。
user-name	ソース・システムがユーザー ID を送信しない場合、ジョブはこのユーザー・プロファイルの下で実行されます。

デフォルト・ユーザー・プロファイルが指定された通信項目をもつすべてのサブシステムのリストを印刷するのに、サブシステム記述印刷 (PRTSBSDAUT) コマンドを使用することができます。

ディスプレイ・パススルー・オプション:

ディスプレイ・パススルーは、APPC 通信を使用するアプリケーションの一例です。 ネットワークを通じてご使用のシステムに接続している別のシステムにサインオンするのに、ディスプレイ・パススルーを使用することができます。

次の表は、パススルー要求 (STRPASTHR コマンド) の例と、ターゲット・システムがこれらの要求を処理する方法を示します。ディスプレイ・パススルーの場合、システムは APPC 通信の基本要素とリモート・サインオン (QRMTSIGN) システム値を使用します。

表 110. パススルー・サインオン要求の例

STRPASTHR コマンドの値		**ターゲット・システム**		
ユーザー識別コード	**パスワード**	**SECURELOC 値**	**QRMTSIGN 値**	**結果**
*NONE	*NONE	任意の値	任意の値	ユーザーはターゲット・システムにサインオンしなければなりません。

表 110. パススルー・サインオン要求の例 (続き)

STRPASTHR コマンドの値		**ターゲット・システム**		
ユーザー識別コード	**パスワード**	**SECURELOC 値**	**QRMTSIGN 値**	**結果**
ユーザー・プロファイル名	入力されない	任意の値	任意の値	要求は失敗します。
*CURRENT	入力されない	*NO	任意の値	要求は失敗します。
		*YES	*SAMEPRF	対話式ジョブは、ソース・システム上のユーザー・プロファイルと同じユーザー・プロファイル名で開始します。リモート・システムにはパスワードは渡されません。ターゲット・システムにユーザー・プロファイル名が存在しなければなりません。
			*VERIFY	
			*FRCSIGNON	ユーザーはターゲット・システムにサインオンしなければなりません。
		*VFYENCPWD	*SAMEPRF	対話式ジョブは、ソース・システム上のユーザー・プロファイルと同じユーザー・プロファイル名で開始します。ソース・システムはユーザーのパスワードを検索し、それをリモート・システムに送信します。ターゲット・システムにユーザー・プロファイル名が存在しなければなりません。
			*VERIFY	
			*FRCSIGNON	ユーザーはターゲット・システムにサインオンしなければなりません。

表 110. パススルー・サインオン要求の例 (続き)

STRPASTHR コマンドの値		**ターゲット・システム**		
ユーザー識別コード	**パスワード**	**SECURELOC 値**	**QRMTSIGN 値**	**結果**
*CURRENT (またはジョブ用の現行ユーザー・プロファイルの名前)	入力される	任意の値	*SAMEPRF	対話式ジョブは、ソース・システム上のユーザー・プロファイルと同じユーザー・プロファイル名で開始します。パスワードはリモート・システムに送信されます。ターゲット・システムにユーザー・プロファイル名が存在しなければなりません。
			*VERIFY	
			*FRCSIGNON	ユーザーはターゲット・システムにサインオンしなければなりません。
ユーザー・プロファイル名 (ジョブ用の現行ユーザー・プロファイルとは別の名前)	入力される	任意の値	*SAMEPRF	要求は失敗します。
			*VERIFY	対話式ジョブは、ソース・システム上のユーザー・プロファイルと同じユーザー・プロファイル名で開始します。パスワードはリモート・システムに送信されます。ターゲット・システムにユーザー・プロファイル名が存在しなければなりません。
			*FRCSIGNON	対話式ジョブは、指定されたユーザー・プロファイル名で開始します。パスワードはリモート・システムに送信されます。ターゲット・システムにユーザー・プロファイル名が存在しなければなりません。

予期しない装置割り当ての回避:

活動中の装置で障害が起こると、システムは回復を試みます。 場合によっては、接続が中断されると、 別のユーザーが障害の起こったセッションを意図的にではなく再確立してしまう可能性があります。

たとえば、USERA がサインオフしないでワークステーションの電源を切ったことを想定してください。 USERB はワークステーションの電源を入れて、サインオンせずに USERA のセッションを再始動することができます。このようなことが起こるのを防ぐため、装置の出入力エラー・アクション (QDEVRCYACN) システム値を *DSCMSG に設定します。装置に障害が起こると、システムはユーザーのジョブを終了します。

リモート・コマンドとバッチ・ジョブの制御:

システムで実行できるリモート・コマンドおよびジョブの制御に役立てるため、いくつかのオプションを使用することができます。

ネットワーク・ジョブを投入できないようにしたり、ネットワーク・ジョブを自動的に実行できないようにするために、ネットワーク・ジョブのアクション (JOBACN) ネットワーク属性を使用することができます。

システムで分散データ管理 (DDM) を使用する場合、以下を実行できます。

- ユーザーが別のシステムからリモート・コマンド投入 (SBMRMTCMD) コマンドを使用できないようにするために、DDM ファイルへのアクセスを制限することができます。 SBMRMTCMD を使用するには、ユーザーが DDM ファイルをオープンできなければなりません。また、DDM ファイルを作成する機能を制限する必要もあります。
- DDM 要求アクセス (DDMACC) システム値用に出口プログラムを指定します。出口プログラムでは、DDM 要求を許可する前に、すべての DDM 要求を評価することができます。

サブシステム記述から PGMEVOKE 経路指定項目を除去することによって、通信環境で実行できるプログラム要求を明示的に指定することができます。 PGMEVOKE 経路指定項目により、要求元は実行するプログラムを指定することができます。 QCMN サブシステム記述などのサブシステム記述からこの経路指定項目を取り除くときに、正常に実行する必要のある通信要求用に経路指定項目を追加しなければなりません。

許可したいそれぞれの要求ごとに、プログラム名と同じ比較値とプログラム名をもつ経路指定項目を追加することができます。この方法を使用するときには、システムにおける実行管理機能環境とシステムで発生する通信要求のタイプを理解する必要があります。できれば、通信要求のすべてのタイプをテストして、通信要求が経路指定項目の変更後に正しく作動することを確認してください。通信要求が使用可能な経路指定項目を検出しないと、ユーザーは CPF1269 メッセージを受け取ります。別の方法は、システムで実行させたくないトランザクション・プログラム用に共通認可を *EXCLUDE に設定することです。

APPC 構成の評価:

通信セキュリティー印刷 (PRTCMNSEC) コマンドまたはメニュー・オプションを使用すると、APPC 構成におけるセキュリティー関連の値を印刷することができます。

以降のトピックに、報告書に関する説明があります。

APPC 装置の関連パラメーター:

この項では、装置記述および構成リストの報告書の例を示します。

この表は、装置記述のための通信情報報告書の一例です。

```
                                通信情報（全報告書）
5722SS1 V5R4M0  060210                                                  SYSTEM4
 オブジェクト・タイプ . . . . . :   *DEVD

                                                                                SNUF
オブジェクト  オブジェクト      装置        ロケーション ロケーション              単一      事前確立   プログラム
  名          タイプ          カテゴリー      保護       パスワード  APPN    可能   セション     セション     開始
 CDMDEV1       *DEVD          *APPC          *NO          *NO          *NO          *YES        *NO
 CDMDEV2       *DEVD          *APPC          *NO          *NO          *NO          *YES        *NO
```

図 3. APPC 装置記述 — 報告書の例

この表は、構成リストのための報告書の一例です。

```
              構成リスト表示                                ページ        1

 構成リスト . . . . . . . . . . . . :   CFGD        QAPPNRMT
 構成リスト・タイプ . . . . . . . . :   CFGTYPE     *APPNRMT
 テキスト . . . . . . . . . . . . . :   TEXT
 ----------------APPN リモート・ロケーション ----------------
          リモート            リモート   制御点
リモート ネットワーク ローカル    制御   ネットワーク 保護
ロケーション ID      ロケーション   点      ID      ロケーション
 SYSTEM36  APPN      SYSTEM4   SYSTEM36  APPN      *NO
 SYSTEM32  APPN      SYSTEM4   SYSTEM32  APPN      *NO
 SYSTEMU   APPN      SYSTEM4   SYSTEM33  APPN      *YES
 SYSTEMJ   APPN      SYSTEM4   SYSTEMJ   APPN      *NO
 SYSTEMR2  APPN      SYSTEM4   SYSTEM1   APPN      *NO
------------------APPN リモート・ロケーション ------------------
          リモート                                ローカル
リモート ネットワーク ローカル   単一       会話    制御     事前確立
ロケーション ID     ロケーションセッション の数     点    セッション数
 SYSTEM36  APPN      SYSTEM4    *NO         10     *NO       *NO
 SYSTEM32  APPN      SYSTEM4    *NO         10     *NO       *NO
```

図 4. 構成リスト報告書の例

APPC 制御装置のパラメーター:

この項は、制御装置記述のための通信情報報告書の一例です。

```
                                通信情報（全報告書）

 オブジェクト・タイプ . . . . . :   *CTLD

オブジェクト オブジェクト 制御装置              交換制御                                    CP       切断     自動削除
  名          ・タイプ     カテゴリー  自動作成     装置       呼出方向    APPN 可能 セッション数 タイマー    分数      装置名
 CTL01        *CTLD       *APPC          *YES        *YES        *DIAL        *YES        *YES          0      1440     AARON
 CTL02        *CTLD       *APPC          *YES        *YES        *DIAL        *YES        *YES          0      1440     BASIC
```

図 5. APPC 制御装置記述 — 報告書の例

回線記述のパラメーター:

この項は、回線記述のための通信情報報告書の一例です。

```
                                  通信情報（全報告書）

 オブジェクト・タイプ . . . . . :   *LIND

オブジェクト   オブジェクト      回線                          自動削除                          自動
  名           ・タイプ         カテゴリー      自動作成      分数          自動応答      ダイヤル
 LINE01         *LIND           *SDLC           *NO              0          *NO           *YES
 LINE02         *LIND           *SDLC           *NO              0          *NO           *YES
 LINE03         *LIND           *SDLC           *NO              0          *NO           *YES
 LINE04         *LIND           *SDLC           *NO              0          *NO           *YES
```

図 6. APPC 回線記述 — 報告書の例

TCP/IP セキュリティーの設定

以下の情報は、TCP/IP セキュリティーを設定する手順をガイドしています。

SLIP の使用に関するセキュリティー上の考慮事項

TCP/IP サポートには、Serial Interface Line Protocol (SLIP) が含まれます。

SLIP は、低コストの 2 地点間接続を提供します。 SLIP ユーザーは、LAN または WAN に含まれるシステムと 2 地点間接続を確立することにより、LAN または WAN に接続することができます。 SLIP は非同期接続で稼働します。 iSeries サーバーとの間のダイヤルアップ接続に SLIP を使用することができます。

たとえば、PC から iSeries システムへのダイヤルアップに SLIP を使用できます。接続の確立後、 PC で TELNET アプリケーションを使用することにより、iSeries TELNET サーバーに接続できます。あるいは、FTP アプリケーションを使用して、2 つのシステム間でファイルを転送することができます。

システムの出荷時に、SLIP 構成はシステムに存在しません。このため、システムで SLIP (およびダイヤルアップ TCP/IP) を実行したくない場合は、SLIP 用の構成プロファイルを構成しないでください。 SLIP 構成の作成には、2 地点間 TCP/IP の処理 (WRKTCPPTP) コマンドを使用します。 WRKTCPPTP コマンドを使用するには *IOSYSCFG 特殊権限が必要です。

システムで SLIP を実行したい場合は、1 つ以上の SLIP (2 地点間) 構成プロファイルを作成します。以下の操作モードで構成プロファイルを作成することができます。

- ダイヤルイン (*ANS)
- ダイヤルアウト (*DIAL)

注: ユーザー・プロファイルは、サインオンを可能にするシステム・オブジェクトです。どのシステム・ジョブを実行するにも、ユーザー・プロファイルが必要です。構成プロファイルは、iSeries システムとの SLIP 接続の確立に使用される情報を保管します。iSeries サーバーへの SLIP 接続を開始するときには、単純にリンクを確立しているだけです。ユーザーは、サインオンを済ませていませんし、iSeries サーバーのジョブをまだ開始していません。したがって、iSeries サーバーへの SLIP 接続を開始するためにユーザー・プロファイルは必ずしも必要ありません。しかし、この後で説明するように、SLIP 構成プロファイルは、接続を許可すべきかどうか判別するためにユーザー・プロファイルを必要とする場合があります。

セキュア・ダイヤルイン SLIP 接続:

誰かが SLIP を使ってシステムへのダイヤルイン接続を確立する前に、あらかじめ SLIP *ANS 構成プロファイルを開始しておく必要があります。

SLIP 構成プロファイルを作成または変更するには、2 地点間 TCP/IP の処理 (WRKTCPPTP) コマンドを使用します。 構成プロファイルを開始するには、2 地点間 TCP/IP の開始 (STRTCPPTP) コマンド、 または WRKTCPPTP 画面のオプションを使用します。 システムの出荷時の STRTCPPTP および ENDTCPPTP コマンドの共通権限は *EXCLUDE です。 SLIP 構成プロファイルの追加、変更、および削除を行うオプション を使用できるのは、ユーザーが *IOSYSCFG 特殊権限を持っている場合だけです。機密保護管理者は、コマンド権限と特殊権限の両方を使用して、 ダイヤルイン接続可能なシステムをセットアップできるユーザーを決めることができます。

ご使用のシステムにダイヤルインする相手のシステムを妥当性検査したい場合には、要求元システムにユーザー ID とパスワードを送信するよう要求します。 こうすれば、ご使用のシステムでユーザー ID とパスワードを検証することができます。 ユーザー ID とパスワードが無効であれば、システムはセッション要求を拒否することができます。 ダイヤルイン妥当性検査をセットアップするには、次のようにします。

1. 要求元システムが接続を確立するために使用できるユーザー・プロファイルを作成する。要求元が送信するユーザー ID とパスワードは、このユーザー・プロファイル名とパスワードに一致しなければなりません。**注:** パスワード妥当性検査を実行するシステムの場合、QSECURITY システム値を 20 以上に設定しなければなりません。追加の保護として、SLIP 接続の確立用に特定したユーザー・プロファイルを作成することができます。このユーザー・プロファイルには、システムに対する制限された権限を与えてください。 SLIP 接続の確立以外の機能用のプロファイルを使用しないよう計画している場合には、ユーザー・プロファイルに以下の値を設定することができます。初期メニュー (INLMNU) を *SIGNOFF に、初期プログラム (INLPGM) を *NONE に、機能制限 (LMTCPB) を *YES に。これらの値により、だれもユーザー・プロファイルを使用して対話式にサインオンできなくなります。
2. 要求元が SLIP 接続の確立を試行する際に、システムがその試行をチェックするための権限リストを作成する。**注:** SLIP プロファイルの作成時または変更時に、システム・アクセス許可リスト・フィールドでこの権限リストを指定します。
3. 権限項目の追加 (ADDAUTLE) コマンドを使用して、 ステップ 1 で作成したユーザー・プロファイルを権限リストに追加する。それぞれの 2 地点間構成プロファイルごとに固有の権限リストを作成することができます。あるいは、いくつかの構成プロファイルが共用する権限リストを作成することができます。
4. WRKTCPPTP コマンドを使用して、以下の特性をもつ TCP/IP 2 地点間 *ANS プロファイルをセットアップする。
   a. 構成プロファイルは、ユーザー妥当性検査を組み込んだ接続ダイアログ・スクリプトを使用しなければならない。ユーザー妥当性検査には、要求元からのユーザー ID とパスワードの受け入れと、それらの妥当性検査が含まれます。システムの出荷時には、この機能を提供するいくつかのサンプル・ダイアログ・スクリプトが付属しています。
   b. 構成プロファイルでは、ステップ 2 で作成した権限リストの名前を指定しなければならない。接続ダイアログ・スクリプトが受信するユーザー ID は、権限リストに入っていなければなりません。

ダイヤルイン・セキュリティーの設定値は、ダイヤルインを行う相手側システムのセキュリティーの実施方法および機能の影響を受けることに注意してください。ユーザー ID とパスワードが必要な場合、要求元システムの接続ダイアログ・スクリプトがそのユーザー ID と パスワードを送信しなければなりません。iSeries サーバーなどの一部のシステムは、ユーザー ID とパスワードを保管するめの安全な方法を提供します。その他のシステムは、ユーザー ID とパスワードをスクリプトに保管します。システムのスクリプトの場所を知っているユーザーは、そのスクリプトにアクセスできる可能性があります。

通信相手側のセキュリティーの実施方法および機能の違いのために、異なる要求元環境ごとに、別の構成プロファイルを作成する必要があるかもしれません。 STRTCPPTP コマンドを使用して、特定の構成プロファイル用のセッションを受け入れるようにシステムをセットアップします。たとえば、いくつかの構成プロ

ファイル用のセッションが一日の特定の時間帯にだけ開始されるようにセットアップできます。関連するユーザー・プロファイルの活動をログに記録するために、セキュリティー監査を使用することができます。

ダイヤルイン・ユーザーによる他のシステムへのアクセスの防止:

システムおよびネットワーク構成によっては、SLIP 接続を開始するユーザーは、システム・サインオン操作なしでネットワーク上の別のシステムにアクセスできる可能性があります。

たとえば、あるユーザーがシステムへの SLIP 接続を確立できるとすると、そのユーザーは、ダイヤルインが許可されていないネットワーク内の別のシステムへの FTP 接続を確立できる可能性があります。

構成プロファイルの IP データグラムの転送許可フィールドに N (いいえ) を指定すると、SLIP ユーザーがネットワークの他のシステムにアクセスできないようにすることができます。これにより、ユーザーがシステムにログオンしない限り、そのユーザーはネットワークにアクセスできなくなります。しかし、ユーザーが正常にシステムにログオンした後は、データグラム転送値の効果はありません。この値は、ネットワーク内の別のシステムとの接続を確立する目的で iSeries システムの TCP/IP アプリケーション (FTP や TELNET など) を使用するユーザーの機能を制限することはありません。

ダイヤルアウト・セッションの制御:

誰かが SLIP を使ってシステムからダイヤルアウト接続を確立する前に、あらかじめ SLIP *DIAL 構成プロファイルを開始しておく必要があります。

SLIP 構成プロファイルを作成または変更するには、WRKTCPPTP コマンドを使用します。構成プロファイルを開始するには、2 地点間 TCP/IP の開始 (STRTCPPTP) コマンド、 または WRKTCPPTP 画面のオプションを使用します。システムの出荷時の STRTCPPTP および ENDTCPPTP コマンドの共通権限は *EXCLUDE です。 SLIP 構成プロファイルの追加、変更、および削除を行うオプションを使用できるのは、ユーザーが *IOSYSCFG 特殊権限を持っている場合だけです。機密保護管理者は、コマンド権限と特殊権限の両方を使用して、ダイヤルアウト接続可能なシステムをセットアップできるユーザーを決めることができます。

ダイヤルアウト・セッションの保護:

iSeries システムのユーザーは、ユーザーの妥当性検査を必要とするシステムへのダイヤルアウト接続を確立したい場合があります。

iSeries サーバーの接続ダイアログ・スクリプトは、リモート・システムにユーザー ID とパスワードを送信しなければなりません。iSeries サーバーは、そのパスワードを保管するための安全な方法を提供します。接続ダイアログ・スクリプトにパスワードを保管する必要はありません。

注:

1. システムはパスワードを送信する前に、パスワードを暗号化解除します。SLIP パスワードは、FTP および TELNET パスワードと同様に、暗号化されていない (「平文の」) 状態で送信されます。しかし、FTP や TELNET の場合とは異なり、SLIP パスワードは、 システムが TCP/IP モードを確立する前に送信されます。
2. SLIP は非同期モードで 2 地点間接続を使用するため、暗号化されていないパスワードの送信時の機密漏れは、FTP および TELNET パスワード使用時の機密漏れとは異なります。暗号化されていない FTP および TELNET パスワードは、ネットワークで IP トラフィックとして送信される可能性があるため、電子的な探知に対して無防備です。 SLIP パスワードの伝送は、2 つのシステム間の電話接続と同じ程度に保護されています。 SLIP 接続ダイアログ・スクリプトを保管するデフォ

ルト・ファイルは QUSRSYS/QATOCPPSCR です。このファイルの共通認可は *USE ですが、これにより、共通ユーザーはデフォルトの接続ダイアログ・スクリプトを変更できません。

妥当性検査の必要なリモート・セッション用の接続プロファイルを 作成するときには、以下のことを行います。

1. サーバー・セキュリティー・データの保持 (QRETSVRSEC) システム値を必ず 1 (はい) にする。このシステム値は、暗号化解除できるパスワードをシステム上の保護された領域に保管するかどうかを決定します。
2. WRKTCPPTP コマンドを使用して、以下の特性をもつ構成プロファイルを作成する。
   a. 構成プロファイルのモードには *DIAL を指定する。
   b. リモート・サービス・アクセス名には、リモート・システムが予期するユーザー ID を指定する。たとえば、別の iSeries サーバーに接続する場合には、その iSeries サーバーでのユーザー・プロファイル名を指定します。
   c. リモート・サービス・アクセス・パスワードには、リモート・システムがこのユーザー ID に対して予期するパスワードを指定する。 iSeries サーバーでは、このパスワードは暗号化解除可能な形式で保護領域に保管されます。構成プロファイルに割り当てる名前とパスワードは、QTCP ユーザー・プロファイルに関連付けられます。どのユーザー・コマンドやインターフェースを使用しても、名前とパスワードにアクセスすることはできません。これらのパスワード情報にアクセスできるのは、登録済みシステム・プログラムだけです。

      注: TCP/IP 構成ファイルを保管する際、接続プロファイルのパスワードが保管されないことに注意してください。 SLIP パスワードを保管するには、セキュリティー・データ保管 (SAVSECDTA) コマンドを使用して QTCP ユーザー・プロファイルを保管します。
   d. 接続ダイアログ・スクリプトには、ユーザー ID とパスワードを送信するスクリプトを指定する。システムの出荷時には、この機能を提供するいくつかのサンプル・ダイアログ・スクリプトが付属しています。システムがスクリプトを実行すると、システムはパスワードを取り出してそのパスワードの暗号化を解除し、リモート・システムに送信します。

Point-to-Point プロトコルの使用に関するセキュリティー上の考慮事項

Point-to-Point Protocol (PPP) は、TCP/IP の一部として使用できます。

PPP は、SLIP で使用できる機能を超える追加機能を提供する 2 地点間接続の業界標準です。 PPP を使用すると、iSeries サーバーは、インターネット・サービス・プロバイダー、あるいはイントラネット/エクストラネット上の他のシステムに高速で直接接続することができます。リモート LAN は、iSeries サーバーに実際にダイヤルイン接続を行うことができます。

SLIP と同様に、PPP が iSeries サーバーへのネットワーク接続を提供することに注意してください。PPP 接続は、基本的に、システムのいわばドアまで要求元を導きます。ただし、要求元は依然として、システムに入って TELNET や FTP などの TCP/IP サーバーに接続するためにユーザー ID とパスワードが必要です。この新しい接続機能についてのセキュリティーの考慮事項は、以下のとおりです。

注: PPP を構成するには、IBM iSeries Access for Windows ワークステーション上の iSeries ナビゲーターを使用します。

- PPP は、(同一ユーザーが常に同一の IP アドレスを使用する) 専用接続の機能を提供します。専用アドレスを使用すると、IP スプーフィング (名前を偽ったシステムが、 認知された IP アドレスをもつトラステッド・システムのふりをすること) が起こる可能性があります。 しかし、PPP が提供する拡張認証機能は、IP スプーフィングに対する 保護に役立ちます。

- SLIP と同様に、PPP の場合、ユーザー名と関連パスワードを指定した接続プロファイルを作成します。ただし、SLIP とは異なり、ユーザーは有効なユーザー・プロファイルとパスワードを所有している必要はありません。ユーザー名とパスワードは、ユーザー・プロファイルとは関連付けられません。その代わり、PPP 認証には妥当性検査リストが使用されます。さらに、PPP には接続スクリプトは不要です。認証 (ユーザー名とパスワードの交換) は PPP アーキテクチャーの一部で、SLIP の場合よりも低いレベルで行われます。
- PPP の場合、CHAP (Challenge Handshake Authentication Protocol) を使用するオプションがあります。CHAP はユーザー名とパスワードを暗号化するため、盗み聞きする者がパスワードを探知することについて心配する必要はなくなります。

  PPP 接続が CHAP を使用するのは、接続の両側のマシンで CHAP がサポートされている場合だけです。 2 つのモデム間で通信をセットアップするためシグナルを交換する際に、その 2 つのシステムは折衝します。 たとえば、SYSTEMA は CHAP をサポートするものの SYSTEMB が CHAP をサポートしない場合、SYSTEMA はセッションを否定するか、暗号化されないユーザー名とパスワードの使用に同意します。暗号化されないユーザー名とパスワードの使用に同意することは、低折衝と呼ばれます。

  低折衝を決めるのは、構成オプションです。たとえば、すべてのシステムに CHAP 機能があることがわかっているイントラネットでは、低折衝にならないように接続プロファイルを構成してください。システムでダイヤルアウトを行う公衆接続の場合、低折衝を行いたいかもしれません。 PPP 用の接続プロファイルは、有効な IP アドレスを指定する機能を提供します。たとえば、特定のユーザー用に特定アドレスまたは特定範囲のアドレスを期待することを指示できます。

  暗号化されたパスワードの機能とともに、この機能は、スプーフィングに対する保護をさらに追加します。活動セッションに対するスプーフィングまたは結合処理をさらに保護するものとして、指定の間隔で再要求するように PPP を構成することができます。 たとえば、PPP セッションの活動中に、iSeries サーバーは他のシステムにユーザー ID とパスワードを要求することができます。15 分間隔で要求することにより、同一の接続プロファイルであるかどうかを確認します。

  エンド・ユーザーは、この再要求活動に気付きません。システムは、エンド・ユーザーが分かるレベルよりも下のレベルで名前とパスワードを交換します。 PPP の場合、リモート LAN が iSeries サーバーと拡張ネットワークにダイヤルイン接続を確立するのを期待することが現実的です。この環境では、IP 転送をオンにすることが必要でしょう。IP 転送は、侵入者がネットワーク上を動き回る (ローミングする) ことを許してしまう可能性があります。 しかし、PPP には、より強化された保護 (パスワードの暗号化や IP アドレスの妥当性検査など) があります。これにより、侵入者がそもそもネットワーク接続を確立できる可能性がより低くなります。

ブートストラップ・プロトコル・サーバーの使用に関するセキュリティー上の考慮事項

ブートストラップ・プロトコル (BOOTP) は、ワークステーションをサーバーに関連付け、ワークステーション IP アドレスと初期プログラム・ロード (IPL) ソースを割り当てるための動的な方法を提供します。

BOOTP は TCP/IP プロトコルの 1 つで、無媒体のワークステーション (クライアント) がネットワーク・サーバーから初期コードを含むファイルを要求できるようにします。BOOTP サーバーは、既知の BOOTP サーバー・ポート 67 を listen します。クライアント要求が受信されると、サーバーはクライアント用に定義された IP アドレスをルックアップし、クライアントの IP アドレスとロード・ファイルの名前を使ってクライアントに応答を戻します。次に、クライアントはそのロード・ファイルに関するサーバーへの TFTP 要求を開始します。クライアント・ハードウェア・アドレスと IP アドレス間のマッピングは、システムの BOOTP テーブルに保持されます。

BOOTP アクセスの防止:

ネットワークに接続しているシン・クライアントがない場合は、 システムで BOOTP サーバーを実行する必要はありません。

他の装置用として BOOTP サーバーを使用することもできますが、それらの装置のためのソリューションとしては、DHCP を使用した方がよいでしょう。 BOOTP サーバーの実行を防止するには、以下のようにします。

1. TCP/IP の開始時に BOOTP サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。`CHGBPA AUTOSTART(*NO)`

   注:

   a. AUTOSTART(*NO) はデフォルト値です。

   b. 120 ページの『自動的に開始する TCP/IP サーバーの制御』には、自動的に開始する TCP/IP サーバーを制御する方法が詳しく説明されています。
2. 何者かが (ソケット・アプリケーションなどの) ユーザー・アプリケーションとシステムが通常 BOOTP 用に使用するポートを関連付けるのを防ぐには、以下のようにします。

   注: DHCP と BOOTP は同じポート番号を使用するため、これによって DHCP が使用するポートまで禁止してしまいます。 DHCP を使用したい場合は、ポートを制限しないでください。

   a. 「GO CFGTCP」と入力して「TCP/IP の構成」メニューを表示する。

   b. オプション 4 (TCP/IP ポート制約事項の処理) を選択する。

   c. 「TCP/IP ポート制約事項の処理」画面で、オプション 1 (追加) を指定する。

   d. 低ポート範囲に 67 を指定する。

   e. 高ポート範囲に *ONLY を指定する。

   注:

   a. ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、 TCP/IP を終了させてから、再度開始しなければなりません。

   b. 共通ポート番号割り当てに関する情報は RFC1700 に示されています。
3. プロトコルに *UDP を指定する。
4. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

BOOTP サーバーの保護:

BOOTP サーバーは iSeries システムに対して直接アクセスを行わないため、 機密漏れは限定されたものになります。

機密保護管理者としての第一の関心は、正しい情報を正しいシン・クライアントに関連付けることです。言い換えれば、悪意のある者が BOOTP テーブルを変更し、それによってシン・クライアントが正しく動作しなかったり、まったく動かなくなってしまう可能性があります。

BOOTP サーバーと BOOTP テーブルを管理するには、*IOSYSCFG 特殊権限が必要です。 システムに対する *IOSYSCFG 特殊権限を持つユーザー・プロファイルを、注意深く制御する必要があります。

DHCP サーバーの使用に関するセキュリティー上の考慮事項

以下のトピックでは、許可ユーザーのために DHCP サーバーを保護し、DHCP サーバーへのアクセスを防止する方法について説明します。

動的ホスト構成プロトコル (DHCP) は、TCP/IP ネットワーク上でホストに構成情報を渡すためのフレームワークを提供します。DHCP はクライアント・ワークステーションに対して、自動構成と類似した機能を提供することができます。クライアント・ワークステーション上の DHCP 使用可能プログラムは、構成情報のための要求をブロードキャストします。DHCP サーバーがシステムで実行中の場合、そのサーバーはクライアント・ワークステーションが TCP/IP を正確に構成するのに必要な情報を送ることにより、要求に応答します。

DHCP を使用すると、ユーザーのシステムへの最初の接続がより容易になります。これは、ユーザーが TCP/IP 構成情報を入力する必要がないためです。また、DHCP を使用すれば、サブネットワークで必要な内部 TCP/IP アドレスの数を減らすこともできます。 DHCP サーバーは、活動ユーザーに (IP アドレスのプールから) IP アドレスを一時的に割り振ることができます。

シン・クライアントの場合は、BOOTP の代わりに DHCP を使用することができます。 DHCP は BOOTP よりも多くの機能を提供し、シン・クライアントと PC の両方の動的構成をサポートすることができます。

DHCP アクセスの防止:

ここでは、ユーザーが DHCP サーバーにアクセスできないようにするための手順を説明します。

システム上で第三者に DHCP を使わせたくない場合は、以下を行います。

1. TCP/IP の開始時に DHCP サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。`CHGDHCPA AUTOSTART(*NO)`

   注: AUTOSTART(*NO) はデフォルト値です。
2. 何者かが (ソケット・アプリケーションなどの) ユーザー・アプリケーションとシステムが通常 DHCP 用に使用するポートを関連付けるのを防ぐには、以下のようにします。
   a. 「`GO CFGTCP`」と入力して「**TCP/IP の構成**」メニューを表示する。
   b. オプション **4** (TCP/IP ポート制約事項の処理) を選択する。
   c. 「TCP/IP ポート制約事項の処理」画面で、オプション **1** (追加) を指定する。
   d. 低ポート範囲に `67` を指定する。
   e. 高ポート範囲に `68` を指定する。

      注: ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。
   f. プロトコルに `*UDP` を指定する。
   g. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。 (保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。) 特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

DHCP サーバーの保護:

ここでは、DHCP サーバーを保護するための推奨事項を示します。

システムで DHCP の実行を選択した場合のセキュリティーに関する考慮事項は、以下のとおりです。

- DHCP を管理する権限を持つユーザー数を制限する。 DHCP の管理には、以下の権限が必要です。
  - *IOSYSCFG 特殊権限
  - 以下のファイルに対する *RW 権限

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```
- LAN に対する物理的なアクセス可能状態を評価する。外部の者がラップトップを持ってユーザーのロケーションに楽々と歩いて入ってきて、LAN にそのラップトップを物理的に接続することができるでしょうか ? これが機密漏れと判断されるならば、DHCP は、DHCP サーバーが構成するクライアント (ハードウェア・アドレス) のリストを作成する機能を提供します。この機能を使用すると、DHCP がネットワーク管理者に提供する生産性の利点が部分的になくなります。しかし、システムが未知のワークステーションを構成することは防止されます。
- 可能であれば、再使用可能 (インターネット用に構築されたものではない) の IP アドレスのプールを使用する。これは、ネットワーク外のワークステーションがサーバーから使用可能構成情報を獲得することを防ぐ上で役立ちます。
- 追加のセキュリティー保護が必要な場合には、DHCP 出口点を使用する。出口点とその機能についての概説を以下に示します。

  ポート項目

  システムは、ポート 67 (DHCP ポート) からデータ・パケットを読み取るたびに、出口プログラムを呼び出します。出口プログラムは、完全なデータ・パケットを受け取ります。出口プログラムは、システムがそのパケットを処理すべきか、または廃棄すべきかを判断することができます。既存の DHCP スクリーニング機能が自分のニーズに対して十分でない場合、この出口点を使用することができます。

  アドレス割り当て

  システムは、DHCP がクライアントにアドレスを正式に割り当てるたびに、出口プログラムを呼び出します。

  アドレス解放

  システムは、DHCP がアドレスを正式に解放し、そのアドレスをアドレス・プールに戻すたびに、出口プログラムを呼び出します。

TFTP サーバーの使用に関するセキュリティー上の考慮事項

以下では、許可ユーザーのために TFTP サーバーを保護し、TFTP サーバーへのアクセスを防止する方法について説明します。

Trivial File Transfer Protocol (TFTP) は、ユーザー認証を使用しない基本ファイル転送を提供します。TFTP はブートストラップ・プロトコル (BOOTP) または動的ホスト構成プロトコル (DHCP) とともに機能します。

クライアントは、最初に BOOTP サーバーまたは DHCP サーバーのいずれかに接続します。BOOTP サーバーまたは DHCP サーバーは、クライアントの IP アドレスとロード・ファイル名を使って応答します。次に、クライアントはそのロード・ファイルに関するサーバーへの TFTP 要求を開始します。クライアントがそのロード・ファイルのダウンロードを完了すると、クライアントは TFTP セッションを終了します。

TFTP アクセスの防止:

ここでは、ユーザーが TFTP サーバーにアクセスできないようにするための手順を説明します。

ネットワークに接続しているシン・クライアントがない場合は、 おそらくシステムで TFTP サーバーを実行する必要はありません。 以下のようにして、TFTP サーバーの実行を防止してください。

1. TCP/IP の開始時に TFTP サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。`CHGTFTPA AUTOSTART(*NO)`

   AUTOSTART(*NO) はデフォルト値です。
2. 何者かが (ソケット・アプリケーションなどの) ユーザー・アプリケーションとシステムが通常 TFTP 用に使用するポートを関連付けるのを防ぐには、以下のようにします。
   a. 「`GO CFGTCP`」と入力して「**TCP/IP の構成**」メニューを表示する。
   b. オプション **4** (TCP/IP ポート制約事項の処理) を選択する。
   c. 「TCP/IP ポート制約事項の処理」画面で、オプション **1** (追加) を指定する。
   d. 低ポート範囲に `69` を指定する。
   e. 高ポート範囲に `*ONLY` を指定する。

      注: ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。
   f. プロトコルに `*UDP` を指定する。
   g. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。 (保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。) 特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

TFTP サーバーの保護:

ここでは、TFTP サーバーを保護するための推奨事項を示します。

デフォルトでは、TFTP サーバーは非常に限定されたシステム・アクセスを提供します。特に、シン・クライアント用の初期コードを提供するように構成されています。機密保護管理者は、TFTP サーバーの以下の特性に注意してください。

- TFTP サーバーは認証 (ユーザー ID とパスワード) を必要としません。すべての TFTP ジョブは、QTFTP ユーザー・プロファイルで実行されます。 QTFTP ユーザー・プロファイルにはパスワードがありません。このため、対話式サインオンでは使用できません。QTFTP ユーザー・プロファイルには特殊権限が何もなく、システム資源に対して明示的に許可されてもいません。シン・クライアントに必要な資源へのアクセスには、共通認可を使用します。
- TFTP サーバーは、出荷時には、シン・クライアント情報が入っているディレクトリーにアクセスする構成になっています。 *PUBLIC または QTFTP に対して、そのディレクトリーへの読み書きを許可しなければなりません。ディレクトリーに書き込みを行うには、CHGTFTPA コマンドの「**ファイル書き込みの許可**」パラメーターに *CREATE を指定する必要があります。既存のファイルに書き込みを行うには、CHGTFTPA コマンドの「**ファイル書き込みの許可**」パラメーターに *REPLACE を指定する必要があります。*CREATE は、既存のファイルを置き換えたり、新しいファイルを作成することを可能にします。*REPLACE は、既存のファイルの置き換えだけを可能にします。

  TFTP 属性の変更 (CHGTFTPA) コマンドを使用して明示的にディレクトリーを定義しない限り、TFTP クライアントがその他のディレクトリーにアクセスすることはできません。このため、ローカル・ユーザーまたはリモート・ユーザーがシステムへの TFTP セッションの開始を試行すると、情報にアクセスしたり、損傷を生じさせるようなユーザーの能力は非常に限定されます。

- シン・クライアントの処理だけでなく、他のサービスも提供するように TFTP サーバーを構成することを決定した場合には、すべての TFTP 要求を評価して認可するための出口プログラムを定義することができます。 TFTP サーバーは、FTP サーバーで使用できる出口に類似した要求妥当性検査出口を提供します。

REXEC サーバーの使用に関するセキュリティー上の考慮事項

以下では、許可ユーザーのために REXEC サーバーを保護し、REXEC サーバーへのアクセスを防止する方法について説明します。

リモート実行サーバー (REXEC) は、REXEC クライアントからコマンドを受け取って実行します。通常、REXEC クライアントは、REXEC コマンドの送信をサポートする PC または UNIX アプリケーションです。このサーバーが提供するサポートは、FTP サーバー用に RCMD (リモート・コマンド) サブコマンドを使用するときの機能と類似しています。

REXEC アクセスの防止:

ここでは、ユーザーが REXEC サーバーにアクセスできないようにするための手順を説明します。

REXEC クライアントからのコマンドをシステムに受け入れさせたくない場合、以下のようにして REXEC サーバーの実行を防止します。

1. TCP/IP の開始時に REXEC サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。`CHGRXCA AUTOSTART(*NO)`

   AUTOSTART(*NO) はデフォルト値です。
2. 何者かが (ソケット・アプリケーションなどの) ユーザー・アプリケーションとシステムが通常 REXEC 用に使用するポートを関連付けるのを防ぐには、以下のようにします。
   a. 「`GO CFGTCP`」と入力して「**TCP/IP の構成**」メニューを表示する。
   b. オプション **4** (TCP/IP ポート制約事項の処理) を選択する。
   c. 「TCP/IP ポート制約事項の処理」画面で、オプション **1** (追加) を指定する。
   d. 低ポート範囲に `512` を指定する。
   e. 高ポート範囲に `*ONLY` を指定する。

      注: ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。
   f. プロトコルに `*TCP` を指定する。
   g. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。 (保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。) 特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

REXEC サーバーの保護:

ここでは、REXEC サーバーを保護するための推奨事項を示します。

システムでリモート実行サーバーの実行を選択した場合の考慮事項は、以下のとおりです。

- REXCD 要求には、ユーザー ID、パスワード、および実行されるコマンドが含まれています。以下のような、通常のサーバーの認証および権限検査が適用されます。

– ユーザー・プロファイルとパスワードの組み合わせが有効でなければならない。
– システムはユーザー・プロファイルに機能の制限 (LMTCPB) 値を強制使用する。
– ユーザーは、コマンド、およびコマンドが使用するすべての資源に対して許可されていなければならない。

- REXEC サーバーは、FTP サーバーに使用できる出口点に類似した出口点を提供します。妥当性検査出口点を使用すると、そのコマンドを評価し、許可するかどうかを決めることができます。
- REXEC サーバーの実行を選択する場合、システム上のメニュー・アクセス制御の外側で実行することになります。オブジェクト権限構造が資源保護に適したものであることを必ず確認してください。

DNS サーバーの使用に関するセキュリティー上の考慮事項

以下では、許可ユーザーのために DNS サーバーを保護し、DNS サーバーへのアクセスを防止する方法について説明します。

ドメイン・ネーム・システム (DNS) は、ホスト名とそれに関連したインターネット・プロトコル (IP) アドレスを管理するための分散データベース・システムです。 IBM システムでは、DNS サーバーは、内部のセキュア・ネットワーク (イントラネット) 用のアドレス変換を提供することを意図したものです。DNS を使用すれば、ユーザーは IP アドレス (xxx.xxx.xxx.xxx) ではなく、単純名 (たとえば 『www.ibm.com』) を使ってホストを探し出すことができます。

DNS アクセスの防止:

ここでは、ユーザーが DNS サーバーにアクセスできないようにするための手順を説明します。

システム上で第三者に DNS を使わせたくない場合は、以下を行います。

1. TCP/IP の開始時に DNS サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。`CHGDNSA AUTOSTART(*NO)`

   AUTOSTART(*NO) はデフォルト値です。
2. 何者かが (ソケット・アプリケーションなどの) ユーザー・アプリケーションとシステムが通常 DNS 用に使用するポートを関連付けるのを防ぐには、以下のようにします。
   a. 「`GO CFGTCP`」と入力して「**TCP/IP の構成**」メニューを表示する。
   b. オプション **4** (TCP/IP ポート制約事項の処理) を選択する。
   c. 「TCP/IP ポート制約事項の処理」画面で、オプション **1** (追加) を指定する。
   d. 低ポート範囲に `53` を指定する。
   e. 高ポート範囲に `*ONLY` を指定する。

      注: ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。
   f. プロトコルに `*TCP` を指定する。
   g. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。 (保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。) 特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。
   h. *UDP (ユーザー・データグラム) プロトコルについて、ステップ 2c から 2g を繰り返す。

DNS サーバーの保護:

ここでは、DNS サーバーを保護するための推奨事項を示します。

システムで DNS の実行を選択した場合のセキュリティーに関する考慮事項は、以下のとおりです。

- DNS サーバーが提供する機能は、IP アドレス変換と名前変換です。このサーバーは、システムのオブジェクトへのアクセスは提供しません。外部の者が DNS サーバーにアクセスする際、サーバーがネットワークのトポロジーを簡単に表示させるというリスクがあります。DNS は、潜在的なターゲット・システムのアドレスを判別しようとするハッカーの手間を省くおそれがあります。ただし、DNS は、それらのターゲット・システムに入り込むのに役立つ情報は提供しません。
- 通常は、イントラネット用に DNS サーバーを使用します。このため、DNS を照会する機能を制限する必要はないはずです。しかし、たとえば、イントラネット内にいくつかのサブネットワークが存在する場合があります。その場合、別のサブネットワークのユーザーにシステムの DNS を照会できないようにする必要があるかもしれません。DNS のセキュリティー・オプションを使用して、1 次ドメインへのアクセスを制限します。iSeries ナビゲーターを使用して、DNS サーバーが応答する IP アドレスを指定します。

  別のセキュリティー・オプションにより、1 次 DNS サーバーから情報をコピーできる 2 次サーバーを指定します。このオプションを使用すると、サーバーは、明示的にリストされた 2 次サーバーからのみ、ゾーン転送要求 (コピー情報への要求) を受け入れます。
- DNS サーバーの構成ファイルを変更する機能は、注意深く制限してください。たとえば、悪意のある者が、ネットワーク外の IP アドレスを指すように DNS ファイルを変更するおそれがあります。彼らは、ネットワークのサーバーをシミュレートし、サーバーに入ってきたユーザーから機密情報を得る可能性もあります。

IBM HTTP サーバーの使用に関するセキュリティー上の考慮事項

以下のトピックでは、許可ユーザーのために IBM HTTP サーバーを保護し、HTTP サーバーへのアクセスを防止する方法について説明します。

HTTP サーバーは、HTML (Hypertext Markup Language) 文書などのシステムのマルチメディア・オブジェクトにアクセスする機能を WWW ブラウザー・クライアントに提供します。また、共通ゲートウェイ・インターフェース (CGI) 仕様もサポートします。アプリケーション・プログラマーは、サーバーの機能性を拡張する CGI プログラムを作成することができます。

管理者は、Internet Connection Server または IBM HTTP サーバーを使用して、同じシステム上で複数のサーバーを並行して実行することができます。実行中のそれぞれのサーバーは、サーバー・インスタンスと呼ばれます。それぞれのサーバー・インスタンスには、固有の名前があります。管理者は、どのインスタンスが開始されるか、および各インスタンスが何を実行できるかを制御します。

重要: Web ブラウザーを使って以下のいずれかを構成または管理する場合には、実行中の HTTP サーバーの *ADMIN インスタンスが必要です。
- iSeries 用のファイアウォール
- Internet Connection Server
- Internet Connection Secure Server
- IBM HTTP Server

ユーザー (Web サイトのビジター) には、システムの「サインオン」画面は表示されません。しかし、 システム管理者は、HTTP ディレクティブですべての HTML 文書と CGI プログラムを定義することにより、それらを明示的に認可しなければなりません。さらに、管理者は、要求の一部またはすべてに対して、資源保護とユーザー認証 (ユーザー ID とパスワード) の両方をセットアップすることができます。

ハッカーによるサービス妨害攻撃のために、Web サーバーがサービス拒否状態になることがあり得ます。サーバーは、特定のクライアント要求のタイムアウトを測定することにより、サービス妨害攻撃を検出することができます。サーバーがクライアントからの要求を受け取らない場合は、サーバーはサービス妨害攻撃が進行中であると判断します。これが発生するのは、サーバーに最初にクライアント接続した後です。サーバーのデフォルトは、攻撃の検出です。

HTTP アクセスの防止:

ここでは、ユーザーが HTTP サーバーにアクセスできないようにするための手順を説明します。

システムにアクセスする目的で誰にもプログラムを使わせたくない場合には、HTTP サーバーの実行を防止する必要があります。以下のようにします。

1. TCP/IP の開始時に HTTP サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。`CHGHTTPA AUTOSTART(*NO)`

   AUTOSTART(*NO) はデフォルト値です。
2. デフォルトでは、HTTP サーバー・ジョブは QTMHHTTP ユーザー・プロファイルを使用します。HTTP サーバーが開始しないようにするため、QTMHHTTP ユーザー・プロファイルの状況を *DISABLED に設定します。

HTTP サーバーへのアクセス制御:

ここでは、組織の Web サイトのコンテンツを保護する上での考慮事項を説明します。

HTTP サーバーを実行する第一の目的は、ビジター (利用者) がシステムの Web サイトにアクセスできるようにすることです。Web サイトを訪問するビジターとは、業界刊行物の広告を見る人のようなものと考えることができます。ビジターは、サーバーの種類やサーバーの物理的な設置場所など、Web サイトを実行しているハードウェアやソフトウェアについては知りません。通常、Web サイト提供者は、潜在的なビジターと Web サイトとの間にバリア (サインオン画面など) を設けたいとは考えません。 しかし、Web サイトが提供する文書または CGI プログラムの一部へのアクセスを制限したい場合もあります。

また、1 つのシステムが複数の論理 Web サイトを提供するようにしたい場合もあります。たとえば、システムは、互いに異なる顧客層を持つさまざまな支店をサポートしている可能性があります。これらの支店ごとに、ビジターにとっては完全に独立しているように見える固有の Web サイトが必要です。さらに、企業の機密情報が入っている内部 Web サイト (イントラネット) を提供する必要もあります。

機密保護管理者は、Web サイトの内容を保護する必要がある一方で、セキュリティーの実施が Web サイトの価値にマイナスの影響を与えないようにする必要があります。さらに、HTTP 活動がシステムあるいはネットワークの保全性を危険にさらさないようにする必要があります。これ以降のトピックでは、プログラムを使用する際のセキュリティー上の提案を示します。

管理の考慮事項:

ここでは、インターネット・サーバーを保護するための推奨事項を示します。

インターネット・サーバーを管理する上でのセキュリティー上の考慮事項は、次のとおりです。

- Web ブラウザーと *ADMIN インスタンスを使用して、セットアップおよび構成機能を実行します。一部の機能 (サーバーでの追加インスタンスの作成など) に関しては、*ADMIN サーバーを使用しなければなりません。
- 管理ホーム・ページ (*ADMIN サーバー用のホーム・ページ) のデフォルト URL は、ブラウザー管理機能を提供する製品の資料の中で公開されています。このため、IBM 提供ユーザー・プロファイルのデ

フォルト・パスワードが知られて公開されているように、デフォルト URL はおそらくハッカーに知られ、ハッカー・フォーラムで公開されるでしょう。以下のいくつかの方法で、この公開から保護することができます。

- 管理機能を実行する必要がある場合に限り、HTTP サーバーの *ADMIN インスタンスを実行する。常に *ADMIN インスタンスを実行したままにしないでください。
- (ディジタル証明書マネージャーを使用して) *ADMIN インスタンス用の SSL サポートを活動化する。*ADMIN インスタンスは、ユーザー ID とパスワードを要求するために HTTP 保護ディレクティブを使用します。SSL を使用すると、ユーザー ID とパスワードが (管理書式に表示されるその他のすべての構成情報とともに) 暗号化されます。
- インターネットから *ADMIN サーバーへのアクセスを防ぐとともに、URL の一部であるシステムおよびドメイン名を隠すために、ファイアウォールを使用する。

- 管理機能の実行時に、*IOSYSCFG 特殊権限を持つユーザー・プロファイルを使用して必ずサインオンする。また、システムの以下のような特定オブジェクトに対する権限も必要になるかもしれません。
  - HTML 文書と CGI プログラムが含まれているライブラリーまたはディレクトリー。
  - サーバーのディレクティブの内部でスワップを計画しているすべてのユーザー・プロファイル。
  - ディレクティブが使用するディレクトリー用のアクセス制御リスト (ACL)。
  - ユーザー ID とパスワードを作成し、保守するための妥当性検査リスト・オブジェクト。
- *ADMIN サーバーと TELNET の両方を使用すると、管理機能をリモートで (おそらくインターネット接続を介して) 実行することができます。 公衆リンク (インターネット) を介して管理を行う場合には、強力な権限をもつユーザー ID とパスワードが探知にさらされている可能性に注意してください。「探知者」は、たとえば TELNET や FTP などを使用してシステムにアクセスを試行するために、このユーザー ID とパスワードを使用する可能性があります。
- HTTP ディレクティブは、サーバー上のすべての活動の基礎を提供します。出荷時の構成では、デフォルトのウェルカム・ページを表示することができます。サーバー管理者がそのサーバー用にディレクティブを定義するまで、クライアントはウェルカム・ページ以外の文書を何も表示できません。ディレクティブを定義するには、Web ブラウザーと *ADMIN サーバーを使用するか、HTTP 構成の処理 (WRKHTTPCFG) コマンドを使用します。どちらの方法でも *IOSYSCFG 特殊権限が必要です。システムをインターネットに接続する場合には、*IOSYSCFG 特殊権限を持つ組織内のユーザーの数を評価および制御することがさらに重要になります。

注:

1. TELNET を使用すると、サインオン画面は他の画面と同様に扱われます。パスワードの入力時にそのパスワードは表示されませんが、システムは、暗号化やエンコードを行わないでそのパスワードを送信します。
2. *ADMIN サーバーを使用すると、パスワードは暗号化されませんが、エンコードされます。エンコード体系は業界標準であるため、ハッカー達の間ではよく知られています。エンコード方式は一般の「探知者」によって簡単には理解されませんが、高度な探知者は、そのパスワードのデコードを試行するためのツールを持っている可能性があります。

セキュリティーのヒント: インターネットを介してリモート管理の実行を計画している場合、*ADMIN インスタンスを SSL と一緒に使用してください。こうすれば、伝送が暗号化されます。安全でないアプリケーションを使用しないでください。アクセス承認済みユーザーからなるイントラネットを介して *ADMIN サーバーを使用している場合には、このサーバーを管理用に安全に使用できます。

資源の保護:

IBM HTTP Server には、 サーバーが使用する情報資産を詳細に制御するための HTTP ディレクティブが組み込まれています。 このディレクティブを使用して、Web サーバーがどのディレクトリーから HTML ファイルおよび CGI プログラムの URL を提供するかを制御したり、他のユーザー・プロファイルにスワップしたり、資源の認証を要求したりすることができます。

HTTP ディレクティブを使用するためのいくつかの提案を以下に示します。

- HTTP サーバーは、「明示権限」を基礎として開始します。サーバーは、ディレクティブに要求が明示的に定義されていない限り、その要求を受け入れません。言い換えれば、サーバーは、URL がディレクティブに (名前または総称で) 定義されていない限り、その URL に関するすべての要求を即時に拒否します。
- 資源の一部あるいはすべてに対する要求を受け入れる前に、保護ディレクティブを使用してユーザー ID とパスワードを要求することができます。
  - ユーザー (クライアント) が保護資源を要求すると、サーバーはブラウザーにユーザー ID とパスワードを要求します。ブラウザーは、ユーザー ID とパスワードの入力をユーザーに指示し、次にその情報をサーバーに送信します。一部のブラウザーはユーザー ID とパスワードを保管して、それ以降の要求時にユーザー ID とパスワードを自動的に送信します。これにより、ユーザーは、要求のたびに同じユーザー ID とパスワードを繰り返し入力しなくても済むようになります。

    ブラウザーの中には、ユーザー ID とパスワードを保管するものもあるため、システムの「サインオン」画面またはルーターを介してシステムに入る場合に気を付けなければならないことを、管理者と同じようにユーザーにも指示してください。ブラウザー・セッションを無人のままにしておくと、機密漏れのおそれがあります。
  - システムがユーザー ID とパスワードを処理する方法には、以下の 3 つのオプションがあります (保護ディレクティブで指定)。
    1. 通常のシステム・ユーザー・プロファイルおよびパスワード検証を使用できます。これは、イントラネット (セキュア・ネットワーク) で資源を保護するために、最も一般的に使用される方法です。
    2. 「インターネット・ユーザー」を作成することができます。インターネット・ユーザーとは、妥当性検査の対象となるが、システムにユーザー・プロファイルを持たないユーザーのことです。インターネット・ユーザーは、「妥当性検査リスト」というシステム・オブジェクトを介してインプリメントされます。妥当性検査リスト・オブジェクトには、特定のアプリケーションの使用ごとに定義されたユーザーとパスワードのリストが含まれます。

       管理者は、インターネット・ユーザーの ID とパスワードの提供方法 (たとえば、アプリケーションによって、あるいは管理者が電子メールからの要求に応答することによって)、およびインターネット・ユーザーの管理方法を決定します。これをセットアップするには、HTTP サーバーのブラウザー・ベースのインターフェースを使用してください。

       非セキュア・ネットワーク (つまりインターネット) の場合、インターネット・ユーザーを使用した方が、通常のユーザー・プロファイルとパスワードを使用する場合よりも、全体として優れた保護が提供されます。ユーザー ID とパスワードを一意の組み合わせにすることにより、これらのユーザーが実行できる機能に関する組み込み制限が作成されます。これらのユーザー ID とパスワードは、(TELNET や FTP などを使った) 通常のサインオンでは使用できません。さらに、通常のユーザー ID とパスワードを、ハッカーによる探知にさらすこともありません。
    3. Lightweight Directory Access Protocol (LDAP) は、伝送制御プロトコル (TCP) 上のディレクトリーへのアクセスを提供するディレクトリー・サービス・プロトコルです。このプロトコルを使用すると、そのディレクトリー・サービスに情報を保管し、それを照会することができます。LDAP は、ユーザー認証を行うための選択肢の 1 つとしてサポートされるようになりました。

注:

- ブラウザーがユーザー ID とパスワードを送信する時には (ユーザー・プロファイルかまたはインターネット・ユーザーかにかかわらず) エンコードしますが、暗号化は行いません。エンコード体系は業界標準であるため、ハッカー達の間ではよく知られています。エンコード方式は一般の「探知者」によっては簡単には理解されませんが、高度な探知者は、これらのデコードを試行するためのツールを持っている場合があります。
- システムは保護システム域に妥当性検査オブジェクトを保管します。ここにアクセスできるのは、定義済みのシステム・インターフェース (API) と適切な権限を持っている場合だけです。

– ユーザー固有のイントラネット証明書権限を作成するために、ディジタル証明書マネージャー (DCM) を使用することができます。ディジタル証明書は、証明書と所有者のユーザー・プロファイルとを自動的に関連付けます。証明書の権限と許可は、関連プロファイルの権限および許可と同じです。

- サーバーが要求を受け入れると、通常のシステムの資源保護がこれを引き継ぎます。資源を要求するユーザー・プロファイルは、その資源 (たとえば、HTML 文書が含まれるフォルダーまたはソースの物理ファイル) へのアクセス権限を持っている必要があります。デフォルトでは、ジョブは QTMHHTTP ユーザー・プロファイルの下で実行されます。ディレクティブを使用すると、別のユーザー・プロファイルにスワップすることができます。そして、システムはそのユーザー・プロファイルの権限を使用して、オブジェクトにアクセスします。このサポートに対する考慮事項を以下にいくつか示します。
  – サーバーが複数の論理 Web サイトを提供している場合には、ユーザー・プロファイルのスワッピングが特に役立ちます。別々のユーザー・プロファイルを Web サイトごとにディレクティブと関連付けることができるため、通常のシステムの資源保護を使用してそれぞれのサイトの文書を保護することができます。
  – ユーザー・プロファイルをスワップする機能と、妥当性検査オブジェクトとを組み合わせて使用することができます。サーバーは、初期要求を評価するために、固有のユーザー ID とパスワード (通常のユーザー ID とパスワードとは異なるもの) を使用します。サーバーがユーザーを認証した後、システムは別のユーザー・プロファイルにスワップして、資源保護を利用します。そのため、ユーザーは本当のユーザー・プロファイル名に気付かず、(FTP などの) 他の方法でそのユーザー・プロファイル名の使用を試行することができません。
- HTTP サーバー要求によっては、プログラムを HTTP サーバーで実行する必要があります。たとえば、システムのデータにアクセスするプログラムなどです。プログラムを実行する前に、サーバー管理者は、CGI ユーザー・インターフェース標準に準拠している特定のユーザー定義プログラムにその要求 (URL) をマップしておかなければなりません。CGI プログラムに関する考慮事項は以下のとおりです。
  – HTML 文書に関して使用する場合と同様に、CGI プログラムに関する保護ディレクティブを使用することができます。このため、プログラムの実行前に、ユーザー ID とパスワードが必要になります。
  – デフォルトでは、CGI プログラムは QTMHHTP1 ユーザー・プロファイルの下で実行されます。プログラムを実行する前に、別のユーザー・プロファイルにスワップすることができます。したがって、CGI プログラムがアクセスする資源用に、通常のシステムの資源保護をセットアップすることができます。
  – 機密保護管理者は、システムでの CGI プログラムの使用を認可する前に、セキュリティーを検討するようにしてください。プログラムの出所と CGI プログラムの実行する機能を理解する必要があります。また、CGI プログラムを実行するユーザー・プロファイルの機能もモニターしてください。さらに、たとえばコマンド行にアクセスできるかどうか判別するために、CGI プログラムを使用してテストする必要があります。権限を借用するプログラムを扱うのと場合と同じように、注意深く CGI プログラムを取り扱ってください。

– さらに、機密オブジェクトが不適切な共通認可を持つ可能性も検討してください。まれに、不適切に設計された CGI プログラムは、知識があり悪意のあるユーザーがシステムに入り込むのを許してしまうおそれがあります。
– CGILIB などの特定のユーザー・ライブラリーを使用して、すべての CGI プログラムを保持します。オブジェクト権限を使用して、このライブラリーに新規オブジェクトを配置できるユーザーと、このライブラリーでプログラムを実行できるユーザーを制御します。ディレクティブを使用して、このライブラリーに入っている CGI プログラムを実行する HTTP サーバーを制限します。

ヒント: サーバーが複数の論理 Web サイトを提供する場合、 それぞれのサイトの CGI プログラム用に別のライブラリーをセットアップすることができます。

セキュリティー上のその他の考慮事項

セキュリティーに関するその他の考慮事項は以下のとおりです。

- HTTP は、システムへの読み取り専用アクセスを提供します。HTTP サーバー要求は、システム上のデータを直接更新または直接削除することはできません。しかし、データを更新する CGI プログラムがあるかもしれません。さらに、 Net.Data® CGI プログラムがシステムのデータベースにアクセスできるようにすることもできます。システムは、(出口プログラムに類似した) スクリプトを使用して、Net.Data プログラムへの要求を評価します。そのため、システム管理者は Net.Data プログラムが行える処置を制御することができます。
- HTTP サーバーは、サーバーを介したアクセスおよびアクセス試行をモニターするのに役立つアクセス・ログを提供します。

SSL と HTTP サーバーの使用に関するセキュリティー上の考慮事項

IBM HTTP Server は、システムとのセキュアな Web 接続を提供することができます。

セキュアな Web サイトとは、クライアントとサーバー間の伝送 (両方向) が暗号化されていることを意味します。このように伝送を暗号化することで、探知者の念入りな探査や、伝送の取り込みまたは更新を試行する人たちからの安全が確保されます。

注: セキュア Web サイトは、クライアント・サーバー間で渡される情報のセキュリティーだけに適用されることに注意してください。セキュア Web サイトの目的は、ハッカーに対するサーバーのぜい弱性を減らすことではありません。ただし、これによって、潜在的なハッカーが探知を通じて容易に入手できる情報量は確実に少なくなります。

Information Center の SSL と Web サーバー (HTTP) のトピックには、暗号化プロセスの導入、構成、および管理のための詳しい説明があります。このトピックでは、サーバー機能の概説と、サーバーを使用する際の考慮事項を説明します。

Internet Connection Server は、以下のライセンス・プログラムのいずれかが導入されている場合に、HTTP および HTTPS をサポートします。

- 5722–NC1

これらのオプションが導入されている場合、本プロダクトは Internet Connection Secure Server と呼ばれます。

暗号化に依存するセキュリティーには、いくつかの要件があります。

- 送信側と受信側 (サーバーとクライアント) は両方とも、暗号化メカニズムを理解して、暗号化と暗号化解除を実行できなければなりません。HTTP サーバーには、SSL を使用できるクライアントが必要です。(SSL はほとんどの一般的な Web ブラウザーで使用可能です。) iSeries 暗号化ライセンス・プログ

ラムは、いくつかの業界標準暗号化方式をサポートします。クライアントがセキュアなセッションを確立しようとするときに、サーバーとクライアントは、両者がサポートする最も安全な暗号化方式を見つけるために折衝します。

- 盗み聞きする人に伝送の暗号化解除を許してはなりません。このため、暗号化方式では、送信側と受信側の両者だけが知っている暗号化/暗号化解除の秘密鍵を両者に持たせる必要があります。セキュアな外部 Web サイトが必要な場合、ユーザーとサーバーに対してディジタル証明書を作成して発行するために、独立した認証局 (CA) を使用してください。認証局は、トラステッド・パーティーと呼ばれます。

暗号化は、転送情報の機密性を保護します。しかし、財務情報などの機密情報の場合、機密性だけでなく、保全性と認証性も必要です。クライアントと (オプションで) サーバーは、(独立参照を通じて) もう一方のパーティーを信頼するだけでなく、伝送が決して更新されていないことを確認する必要があります。認証局 (CA) によって提供されるディジタル署名は、認証性と保全性を保証します。 SSL プロトコルは、サーバー証明書 (およびオプションでクライアント証明書) のディジタル署名を検証することにより、認証を行います。

暗号化と暗号化解除には処理時間が必要で、それが伝送のパフォーマンスに影響を与えます。このため、iSeries サーバーでは、セキュアなサービスとそうでないサービスの両方のプログラムを同時に実行することができます。商品カタログなどセキュリティーの必要がない文書を提供する場合には、セキュアでない HTTP サーバーを使用することができます。これらの文書の URL は、http:// で始まります。セキュアな HTTP サーバーは、顧客がクレジット・カードの情報を記入する書式などの機密情報に使用することができます。このプログラムは、URL が http:// または https:// で始まる文書を処理することができます。

注: 特に Web サイトの一部の文書だけのためにセキュア・サーバーを使用する場合には、伝送が機密保護されるようになった時点、および機密保護されなくなった時点をクライアントに知らせることは、正しいインターネットのエチケットです。

暗号化には、セキュア・クライアントとセキュア・サーバーの両方が必要なことに注意してください。セキュア・ブラウザー (HTTP クライアント) はかなり一般的に普及してきました。

LDAP のセキュリティーに関する考慮事項

Lightweight Directory Access Protocol (LDAP) セキュリティー機能には、 Secure Sockets Layer (SSL)、アクセス制御リスト、および CRAM-MD5 パスワード暗号化機能が含まれます。

V5R1 では、Kerberos 接続およびセキュリティー監査のサポートが追加され、 LDAP セキュリティーが拡張されました。これらのトピックに関する詳細情報は、「ディレクトリー・サービス (LDAP)」を参照してください。

LPD のセキュリティーに関する考慮事項

LPD (ライン・プリンター・デーモン) は、プリンター出力をシステムに配布する機能を提供します。 システムは、LPD 用のサインオン処理を何も実行しません。

LPD アクセスの防止:

以下では、LDP アクセスを防止する方法について説明します。

システムにアクセスする目的で誰にも LPD を使わせたくない場合には、LPD サーバーの実行を防止する必要があります。以下のようにします。

1. TCP/IP の開始時に LPD サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。`CHGLPDA AUTOSTART(*NO)`

注:

a. AUTOSTART(*YES) はデフォルト値です。

b. 『自動的に開始する TCP/IP サーバーの制御』には、自動的に開始する TCP/IP サーバーを制御する方法が詳しく説明されています。

2. 何者かが (ソケット・アプリケーションなどの) ユーザー・アプリケーションとシステムが通常 LPD 用に使用するポートとを関連付けるのを防ぐには、以下のようにします。

a. 「GO CFGTCP」と入力して「TCP/IP の構成」メニューを表示する。

b. オプション 4 (TCP/IP ポート制約事項の処理) を選択する。

c. 「TCP/IP ポート制約事項の処理」画面で、オプション 1 (追加) を指定する。

d. 低ポート範囲に 515 を指定する。

e. 高ポート範囲に *ONLY を指定する。

注:

a. ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。

b. 共通ポート番号割り当てに関する情報は RFC1700 に示されています。

3. プロトコルに *TCP を指定する。

4. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

5. *UDP プロトコルについて、ステップ 2c から 2g を繰り返す。

LPD アクセスの制御:

LPD クライアントがシステムにアクセスするのを許可したい場合、 以下のセキュリティー事項について注意してください。

次のようなセキュリティー問題を認識しておくことは重要です。

- ユーザーが不要オブジェクトでシステムをあふれさせないようにするために、補助記憶域プール (ASP) に適切なしきい値を必ず設定してください。システム保守ツール (SST) または専用保守ツール (DST) のいずれかを使用して、ASP のしきい値を表示および設定することができます。 ASP しきい値の詳細については、「バックアップおよび回復」資料を参照してください。
- システムにスプール・ファイルを送信するユーザーを制限するために、出力待ち行列に対する権限を使用することができます。ユーザー ID を持っていない LPD ユーザーは、QTMPLPD ユーザー・プロファイルを使用します。このユーザー・プロファイルに、ごくわずかな数の出力待ち行列に対するアクセス権を与えることができます。

SNMP のセキュリティーに関する考慮事項

SNMP は、ネットワーク環境でゲートウェイ、ルーター、およびホストを管理する手段を提供します。

システムは、ネットワークにおいてシンプル・ネットワーク管理プロトコル (SNMP) エージェントとして機能します。SNMP エージェントは、システムについての情報を収集し、リモート SNMP ネットワーク管理プログラムが要求する機能を実行します。

SNMP アクセスの防止:

以下の指示に従って、システムへの SNMP アクセスを防止することができます。

システムにアクセスする目的で誰にも SNMP を使わせたくない場合には、SNMP サーバーの実行を防止する必要があります。以下のようにします。

1. TCP/IP の開始時に SNMP サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。CHGSNMPA AUTOSTART(*NO)

   注:

   a. AUTOSTART(*YES) はデフォルト値です。
   b. 『自動的に開始する TCP/IP サーバーの制御』には、自動的に開始する TCP/IP サーバーを制御する方法が詳しく説明されています。

2. 何者かが (ソケット・アプリケーションなど) とユーザー・アプリケーションとシステムが通常 SNMP 用に使用するポートを関連付けるのを防ぐには、以下のようにします。
   a. 「GO CFGTCP」と入力して「TCP/IP の構成」メニューを表示する。
   b. オプション 4 (TCP/IP ポート制約事項の処理) を選択する。
   c. 「TCP/IP ポート制約事項の処理」画面で、オプション 1 (追加) を指定する。
   d. 低ポート範囲に 161 を指定する。
   e. 高ポート範囲に *ONLY を指定する。

   注:

   a. ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。
   b. 共通ポート番号割り当てに関する情報は RFC1700 に示されています。

3. プロトコルに *TCP を指定する。
4. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。
5. *UDP プロトコルについて、ステップ 2c から 2g を繰り返す。

SNMP アクセスの制御:

SNMP マネージャーがシステムにアクセスするのを許可したい場合には、以下のセキュリティー事項について注意する必要があります。

次のようなセキュリティー問題を認識しておくことは重要です。

- SNMP を使用してネットワークにアクセスするユーザーは、ネットワークについての情報を集めることができます。別名とドメイン・ネーム・サーバーを使用して隠した情報は、SNMP を介して潜在的な侵入者にとって使用可能になります。さらに、侵入者は SNMP を使ってネットワーク構成を改変し、通信を混乱させるおそれがあります。
- SNMP は、アクセスについてコミュニティー名に依存しています。概念的に、コミュニティー名はパスワードに類似しています。コミュニティー名は暗号化されません。そのため、コミュニティー名は探知に対して無防備です。「SNMP のコミュニティー追加」(ADDCOMSNMP) コマンドを使用して、マネージャー IP アドレス (INTNETADR) パラメーターを、*ANY ではなく 1 つ以上の特定の IP アドレスに設定してください。また、ADDCOMSNMP または CHGCOMSNMP コマンドの OBJACC パラメーター

を *NONE に設定すると、コミュニティー内のマネージャーは MIB オブジェクトにアクセスできなくなります。これは、コミュニティーを削除しないで、一時的にコミュニティー内のマネージャーへのアクセスを拒否することを目的としています。

INETD サーバーに関するセキュリティー上の考慮事項

ほとんどの TCP/IP サーバーとは異なり、INETD サーバーはクライアントに対して単一のサービスを提供しません。

INETD サーバーは、管理者がカスタマイズできる各種サービスの集まりを提供します。そのため、INETD サーバーは、「スーパー・サーバー」と呼ばれることがあります。INETD サーバーには、以下の組み込みサービスがあります。

- Time (時刻)
- Daytime (昼間)
- Echo (エコー)
- Discard (破棄)
- Changed (変更済み)

これらのサービスは TCP と UDP の両方に対してサポートされています。 UDP の場合は、echo、time、daytime、および changed サービスが UDP パケットを受信し、 それを送信元に送り返します。 echo サーバーは、受信したパケットをそのまま送り返します。time サーバーと daytime サーバーは、 指定された形式で時刻を生成し、それを送り返します。changed サーバーは、印刷可能な ASCII 文字からなるパケットを生成し、それを送り返します。

これら UDP サービスの性質上、システムはサービス妨害攻撃に対して無防備になります。たとえば、SYSTEMA と SYSTEMB という 2 つの iSeries サーバーがあったとします。悪意のあるプログラマーは、SYSTEMA のソース・アドレスと time サーバーの UDP ポート番号を持つ IP ヘッダーと UDP ヘッダーを偽造することができます。そのプログラマーは、次に、そのパケットを SYSTEMB の time サーバーに送信します。SYSTEMB の time サーバーは、時刻を SYSTEMA に送信し、SYSTEMA は、SYSTEMB に応答を返します。これが繰り返され、結果として無限ループに陥り、両システムの CPU 資源とネットワーク帯域幅が使い尽くされてしまいます。

したがって、iSeries システムに対するそのような攻撃のリスクがあることを考慮し、これらのサービスをセキュア・ネットワークだけで実行するようにしなければなりません。INETD サーバーは、出荷時には、TCP/IP の開始時に自動開始しないように設定されています。INETD の開始時にこれらのサービスを開始するかどうかを構成することができます。デフォルトでは、INETD サーバーの開始時に TCP と UDP の time サーバーおよび daytime サーバーの両方が開始します。

INETD サーバーには、次の 2 つの構成ファイルがあります。 `/QIBM/UserData/OS400/inetd/inetd.conf` `/QIBM/ProdData/OS400/inetd/inetd.conf`

これらのファイルによって、INETD サーバーの開始時に開始するプログラムが決まります。さらに、これらのファイルは、INETD がプログラムを開始するときにそのプログラムをどのユーザー・プロファイルのもとで実行するかをも決定します。

注: proddata 内の構成ファイルを決して変更しないでください。このファイルは、システムを再ロードするたびに置き換えられます。カスタマイズによる構成変更は、UserData ディレクトリー・ツリー内のこのファイルにだけ格納してください。このファイルは、リリースのアップグレード中に更新されないためです。

悪意のあるプログラマーがこれらのファイルにアクセスした場合、そのプログラマーは INETD 開始時に任意のプログラムを開始するように構成できます。したがって、これらのファイルの保護が非常に重要になります。デフォルトででは、これらのファイルを変更するには、QSECOFR 権限が必要です。これらのファイルへのアクセスに必要な権限を低くしないでください。

注: ProdData ディレクトリーにある構成ファイルは変更しないでください。このファイルは、システムを再ロードするたびに置き換えられます。カスタマイズによる構成変更は、UserData ディレクトリー・ツリー内のこのファイルにだけ格納してください。このファイルは、リリースのアップグレード中に更新されないためです。

TCP/IP ローミング制限のセキュリティーに関する考慮事項

システムがネットワークに接続されている場合、TCP/IP アプリケーションを使ってネットワークを動き回る (ローミングする) ユーザーの機能を制限する必要があるかもしれません。

これを行う 1 つの方法は、以下のクライアント TCP/IP コマンドへのアクセスを制限することです。

注: 以下のコマンドは、システムのいくつかのライブラリーに存在している可能性があります。少なくとも、QSYS ライブラリーと QTCP ライブラリーの両方に入っています。すべての出現を確実に突き止め、保護してください。

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (REXEC クライアント)

ユーザーの到達可能な宛先は、以下によって決定されます。

- TCP/IP ホスト・テーブルの項目。
- TCP/IP 経路テーブルの *DFTROUTE 項目。これにより、不明のネットワークが宛先である場合に、ユーザーはネクスト・ホップ・システムの IP アドレスを入力することができます。ユーザーは、デフォルト経路を使用して、リモート・ネットワークに到達または接続することができます。
- リモート・ネーム・サーバー構成。このサポートにより、ネットワークの別のサーバーは、ユーザー用のホスト名を探し出すことができます。
- リモート・システム・テーブル。

これらのテーブルへの項目追加と構成変更を行うことのできるユーザーを制御する必要があります。 また、テーブル項目と構成の含意を理解することも必要です。

ILE C コンパイラーにアクセスすることのできる知識のあるユーザーが、TCP または UDP ポートに接続できるソケット・プログラムを作成できることに注意してください。QSYSINC ライブラリーの以下のソケット・インターフェース・ファイルへのアクセスを制限すると、このプログラムの作成をより困難にすることができます。

- SYS
- NETINET
- H
- ARPA

- ソケットおよび SSL

サービス・プログラムの場合、以下のサービス・プログラムの使用を制限することにより、すでにコンパイル済みのソケットおよび SSL アプリケーションの使用を制限することができます。

- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

サービス・プログラムは共通認可が *USE で出荷されますが、 その権限は *EXCLUDE (または必要に応じて別の値) に変更することができます。

RouteD の使用に関するセキュリティー上の考慮事項

このトピックでは、ルート・デーモン (RouteD) サーバーの使用に関するセキュリティー上の考慮事項を説明します。RouteD は、システムでの Routing Information Protocol をサポートします。

ルート・デーモン (RouteD) サーバーは、IBM システム上で、 Routing Information Protocol (RIP) へのサポートを提供します。 RIP は、最も広く使用されている経路指定プロトコルです。これは、自律型システム内の IP パケットの経路指定において TCP/IP を援助する Interior Gateway Protocol です。

RouteD の目的は、トラステッド・ネットワーク内のシステムが互いに現行の経路情報を更新できるようにすることで、ネットワーク・トラフィックの効率を上げることです。 RouteD を実行すると、システムは伝送 (パケット) の経路指定方法について、他の参加システムからの更新情報を受け取ることができます。そのため、ハッカーが RouteD サーバーにアクセスできる場合、RouteD サーバーを使ってパケットを探知または変更できるシステムを介して、パケットの経路を変更する恐れがあります。 RouteD のセキュリティーに関する提案は以下のとおりです。

- IBM システムは RIPv1 を使用しますが、RIPv1 はルーターを認証する方法を提供しません。これは、トラステッド・ネットワーク内での使用を意図したものです。ご使用のシステムが「信用」できない他のシステムとともにネットワーク内に存在する場合は、RouteD サーバーを実行しないでください。RouteD サーバーが自動的に開始しないようにするには、以下のように入力します。`CHGRTDA AUTOSTART(*NO)`
- RouteD 構成を変更することのできる (*IOSYSCFG 特殊権限を持つ) ユーザーを必ず制御してください。
- ご使用のシステムが複数のネットワーク (たとえば、イントラネットとインターネット) に参加している場合は、セキュア・ネットワークとの間でのみ変更内容を送受信するように RouteD サーバーを構成することができます。

セキュリティーの管理

セキュリティー戦略を計画してインプリメントしたら、システムのセキュリティーを管理する作業が残されています。

以下のトピックでは、セキュリティー管理計画の設定をガイドします。

- セキュリティー情報のバックアップと回復
- セキュリティー情報の管理
- 保守ツール・ユーザー ID の管理
- コンピューター・ウィルスに対する保護

保管機能と復元機能の制限

セキュリティー・システムの一環として、ユーザーの保管機能と復元機能を制御する必要があります。

大部分のユーザーは、システム上のオブジェクトを保管したり復元したりする必要はありません。保管コマンドを使用すれば、組織の重要な資産を媒体や別のシステムにコピーすることが可能になります。ほとんどの保管コマンドは、媒体や保管/復元装置にアクセスしないで別のシステムに送信できる保管ファイルをサポートします (SNDNETF ファイル・コマンドを使用)。

復元コマンドを使用すれば、プログラム、コマンド、ファイルなど、無許可のオブジェクトをシステムに復元できるようになります。また、保管ファイルを使用することで、媒体や保管/復元装置にアクセスしないで情報を復元することもできます。SNDNETF コマンドや FTP 機能を使用することで、保管ファイルを別のシステムから送信することができます。

システムで保管操作や復元操作を制限するうえでの推奨事項は次のとおりです。

- どのユーザーが *SAVSYS 特殊権限を持つかを制御します。*SAVSYS 特殊権限があれば、ユーザーはオブジェクトに対する必要な権限を持たなくても、オブジェクトの保管や復元を行うことができます。
- 装置を保管および復元するための物理アクセスを制御します。
- 保管コマンドや復元コマンドへのアクセスを制限します。i5/OS ライセンス・プログラムを導入すると、RSTxxx コマンドの共通認可は *EXCLUDE になります。 SAVxxx コマンドの共通認可は *USE です。SAVxxx コマンドの共通認可を *EXCLUDE に変更することを考慮してください。RSTxxx コマンドの使用を許可するユーザーを注意深く制限してください。
- QALWOBJRST システム値を使用して、システム状態プログラム、権限を借用するプログラム、および妥当性検査エラーになったオブジェクトの復元を制限します。
- QVFYOBJRST システム値を使用して、システムにおける署名オブジェクトの復元を制御します。
- QFRCCVNRST システム値を使用して、システムに復元する特定のオブジェクトの再作成を制御します。
- セキュリティー監査機能を使用して復元操作をモニターします。 *SAVRST を QAUDLVL システム値に組み込み、復元操作で作成された監査レコードを定期的に印刷します。

セキュリティー情報の保管

このトピックでは、セキュリティー情報を保管および復元する方法の概要を示します。

システムのバックアップと回復を計画する際には、情報そのものだけでなく、情報のセキュリティーについても考慮する必要があります。バックアップと回復に関する完全な計画を設計する際には、Information Center の『バックアップ、回復、およびシステムの可用性』のトピックが役に立ちます。以下の一連のトピックでは、セキュリティーを設定する際に作成されるセキュリティー情報をバックアップおよび復元する方法について説明します。

関連概念

14 ページの『ユーザー・セキュリティー』
ユーザーの視点から見ると、セキュリティーは、ユーザーがシステム上でタスクを使用および完了する仕方に影響を与えます。

システム値の保管

ここでは、システム値の保管タスクについて説明します。保管することがなぜ重要か、および段階的な手順を示します。

システム値の保管: システム値は、システム・ライブラリー QSYS に保管されます。以下の操作を行うと、QSYS ライブラリーが保管されます。

- システム保管 (SAVSYS) コマンドを使用する。
- 「保管」メニューでオプションを使用して、システム全体を保管する。
- 「保管」メニューでオプションを使用して、システム情報を保管する。
- 「バックアップの実行 (RUNBCKUP)」メニューでオプションを使用して、システム全体のバックアップをとる。

システム全体を回復する必要がある場合に、オペレーティング・システムを復元すると、自動的にシステム値が復元されます。 次に、『グループおよびユーザー・プロファイルの保管』を参照してください。

V5R4 では、システム値を保管する別の方法として SAVSYSINF コマンドがあります。

グループおよびユーザー・プロファイルの保管

グループおよびユーザー・プロファイルは QSYS ライブラリーに保管されます。 これらを保管するには、システム保管 (SAVSYS) コマンドを使用するか、システム全体を保管するメニュー・オプションを選択します。

さらに、グループおよびユーザー・プロファイルを保管する方法として、セキュリティー・データ保管 (SAVSECDTA) コマンドを使用することもできます。ユーザー・プロファイルを復元するには、ユーザー・プロファイル復元 (RSTUSRPRF) コマンドを使用します。通常の手順は次のとおりです。

1. オペレーティング・システムを復元します。これにより、ライブラリー QSYS が復元されます。
2. ユーザー・プロファイルを復元します。
3. 残りのライブラリーを復元します。
4. 権限復元 (RSTAUT) コマンドを使用して、オブジェクトに対する権限を復元します。

ジョブ記述の保管

ジョブ記述を作成する際に、 それを常駐させるライブラリーを指定します。 IBM は、ジョブ記述を QGPL ライブラリーに作成するようお勧めします。

ジョブ記述を保管するには、それが常駐するライブラリーを保管します。これを行うには、ライブラリー保管 (SAVLIB) コマンドを使用します。 さらに、オブジェクト保管 (SAVOBJ) コマンドを使用して、ジョブ記述を保管することもできます。

ライブラリーの内容を復元するには、ライブラリー復元 (RSTLIB) コマンドを使用します。個々のジョブ記述を復元するには、オブジェクト復元 (RSTOBJ) コマンドを使用します。

資源保護情報の保管

資源保護は、ユーザーがオブジェクトを処理する方法を定義します。資源保護はさまざまなタイプの情報で構成され、さまざまな場所に保管されます。

情報のタイプ	保管される場所	保管される方法	復元される方法
共通権限	オブジェクトの保管場所	SAVxxx コマンド[1]	RSTxxx コマンド[2]
オブジェクト監査値	オブジェクトの保管場所	SAVxxx コマンド[1]	RSTxxx コマンド[2]
オブジェクト所有権	オブジェクトの保管場所	SAVxxx コマンド[1]	RSTxxx コマンド[2]
1 次グループ	オブジェクトの保管場所	SAVxxx コマンド[1]	RSTxxx コマンド[2]

情報のタイプ	保管される場所	保管される方法	復元される方法
権限リスト	QSYS ライブラリー	SAVESYS または SAVSECDTA	RSTUSRPRF、USRPRF (*ALL)
オブジェクトと権限リストの間のリンク	オブジェクトの保管場所	SAVxxx コマンド[1]	RSTxxx コマンド[2]
私用権限	ユーザー・プロファイルの保管場所	SAVESYS または SAVSECDTA	RSTAUT

[1] SAVOBJ または SAVLIB コマンドを使用すると、ほとんどのオブジェクト・タイプを保管できます。オブジェクト・タイプ (構成など) によっては、特殊な保管コマンドを持つものがあります。

[2] RSTOBJ または RSTLIB コマンドを使用すると、ほとんどのオブジェクト・タイプを復元できます。オブジェクト・タイプ (構成など) によっては、特殊な復元コマンドを持つものがあります。

アプリケーションまたはシステム全体を復元させる必要がある場合、オブジェクトに対する権限の回復を含む、回復ステップを注意深く計画する必要があります。次に、アプリケーションの資源保護情報を回復するために必要な基本ステップを示します。

1. 必要に応じて、アプリケーションを所有するプロファイルを含む、ユーザー・プロファイルを復元します。 RSTUSRPRF コマンドを使用すれば、特定のプロファイルまたはすべてのプロファイルを復元できます。
2. アプリケーションによって使用される権限リストを復元します。 RSTUSRPRF USRPRF(*ALL) を使用すると、権限リストが復元されます。

   注: これにより、パスワードを含むすべてのユーザー・プロファイル値がバックアップ媒体から復元されます。
3. RSTLIB または RSTOBJ コマンドを使用して、アプリケーション・ライブラリーを復元します。これにより、オブジェクト所有権、共通権限、およびオブジェクトと権限リストの間のリンクが回復されます。
4. RSTAUT コマンドを使用して、オブジェクトに対する私用権限を復元します。 RSTAUT コマンドによって、権限リストに対するユーザー権限も復元されます。特定のユーザーまたはすべてのユーザーの権限を復元することができます。

デフォルト所有者プロファイル (QDFTOWN) の保管

オブジェクトを復元する際に所有者プロファイルがシステム上にない場合、 システムはオブジェクトの所有権を QDFTOWN と呼ばれるデフォルト・プロファイルに転送します。

所有者プロファイルを回復または再作成した後、「所有者によるオブジェクト処理」 (WRKOBJOWN) コマンドを使用して、所有権を元に戻すことができます。

セキュリティー情報の復元

システムを回復するには、データおよび関連したセキュリティー情報の復元が必要な場合があります。

回復の通常の順序は以下のとおりです。

1. ユーザー・プロファイルおよび権限リストを復元する (RSTUSRPRF USRPRF(*ALL))。
2. オブジェクトを復元する (RSTLIB、RSTOBJ、または RSTCFG)。
3. オブジェクトに対する私用権限を復元する (RSTAUT)。

関連するシステム値の復元

この情報を使用して、どんなセキュリティー関連オブジェクトをどんな方法でシステムに復元するかを制御します。

方法: WRKSYSVAL*SEC (システム値処理コマンド)

権限: *ALLOBJ および *SECADM

ジャーナル項目:
SV

注: 変更内容は、即時有効になります。IPL は必要ありません。

次に、オブジェクトを復元するときに同様に考慮すべき、システムへのセキュリティー関連オブジェクトの復元に関連するシステム値を説明します。

QVFYOBJRST
復元でのオブジェクトの検査

QFRCCVNRST
復元時の強制変換

QALWOBJRST
セキュリティーにかかわるオブジェクトの復元許可

ユーザー・プロファイルを復元する。

ユーザー・プロファイルの復元

復元時には、ユーザー・プロファイルに何らかの変更が加えられる場合があります。

以下の事柄が該当します: プロファイルが個別に復元され (RSTUSRPRF USRPRF(*ALL) は指定されていない)、SECDTA(*PWDGRP) が要求されず、さらに復元されるプロファイルがシステムに存在しない場合、以下のフィールドは *NONE に変更されます。

- グループ・プロファイル名 (GRPPRF)
- パスワード (PASSWORD)
- 文書パスワード (DOCPWD)
- 補足グループ・プロファイル (SUPGRPPRF)

製品のパスワードは *NONE に変更されます。このため、システム上に存在していなかった個々のユーザー・プロファイルを復元した後、製品のパスワードは正しくなくなります。

- プロファイルが個別に復元され (RSTUSRPRF USRPRF(*ALL) は指定されていない)、SECDTA(*PWDGRP) が要求されず、さらにプロファイルがシステムに存在する場合、パスワード、文書パスワード、およびグループ・プロファイルは変更されません。 RSTUSRPRF コマンドで SECDTA(*PWDGRP) パラメーターを指定することにより、保管媒体から復元されるパスワード情報とグループ情報を使ってユーザー・プロファイルを個別に復元することができます。個々のプロファイルの復元時には、パスワード情報とグループ情報を復元するために *ALLOBJ および *SECADM 特殊権限が必要です。ユーザー・プロファイルとともに復元される製品パスワードは、RSTUSRPRF コマンドで SECDTA(*PWDGRP) パラメーターを指定しない限り、システムに存在した個々のユーザー・プロファイルの復元後に誤ったパスワードになります。
- すべてのユーザー・プロファイルがシステムに復元される場合、システム上の既存のプロファイルのすべてのフィールドが保管媒体から復元されます (パスワードを含む)。

注:

1. 復元されるシステムとは異なるパスワード・レベル (QPWDLVLシステム値) を持つシステムから保管されたユーザー・プロファイルを使用すると、復元後のシステムでパスワードが有効でなくなる可能性があります。たとえば、パスワード・レベル 2 で実行されていたシステムから保管されたユーザー・プロファイルの場合、ユーザーは ″This is my password″ というパスワードを持つことができます。このパスワードは、パスワード・レベル 0 または 1 で実行されているシステムでは無効になります。
2. セキュリティー情報の各バージョンに関連した機密保護担当者 (QSECOFR) パスワードを記録しておいてください。このパスワードを保管しておけば、完全な復元操作を実行する必要がある場合に、システムに確実にサインオンすることができます。

DST (専用保守ツール) を利用して、QSECOFR プロファイルのパスワードを再設定することができます。詳しくは、Information Center の『保守ツール』トピックを参照してください。 Information Center へのアクセス方法については、xvi ページの『Prerequisite and related information』を参照してください。

- システムにプロファイルが存在する場合、復元操作によって uid または gid は変更されません。
- プロファイルがシステムに存在しない場合、プロファイルの uid および gid が保管媒体から復元されます。 uid または gid のいずれかがシステムにすでに存在する場合、システムは新しい値を生成してメッセージ (CPI3810) を出します。
- 以下のいずれかの場合には、セキュリティー・レベル 30 以上のシステムに復元されるユーザー・プロファイルから *ALLOBJ 特殊権限が除去されます。
  - プロファイルが別のシステムから保管され、RSTUSRPRF を実行するユーザーが *ALLOBJ および *SECADM 特殊権限を持っていない。
  - セキュリティー・レベル 10 または 20 の同じシステムからプロファイルが保管された。

  注: システムはシステム上および保管メディア上の機械製造番号を使って、オブジェクトが同一のシステムに復元されるか、別のシステムに復元されるかを決定します。

  *ALLOBJ 特殊権限は以下の IBM 提供プロファイルからは除去されません。
  - QSYS (システム) ユーザー・プロファイル
  - QSECOFR (機密保護担当者) ユーザー・プロファイル
  - QLPAUTO (ライセンス・プログラム自動導入) ユーザー・プロファイル
  - QLPINSTALL (ライセンス・プログラム導入) ユーザー・プロファイル

オブジェクトの復元

システムにオブジェクトを復元するとき、システムはオブジェクトとともに保管されている権限情報を使用します。

復元されるオブジェクトのセキュリティーは、以下のようになります。

オブジェクト所有権:

- オブジェクトを所有するプロファイルがシステム上にある場合、所有権はそのプロファイルに復元されます。
- 所有者プロファイルがシステム上にない場合、オブジェクトの所有権は QDFTOWN (デフォルトの所有者) ユーザー・プロファイルに与えられます。
- オブジェクトがシステム上に存在し、そのシステム上での所有者が保管媒体上の所有者と異なる場合、オブジェクトは復元されません。ただし ALWOBJDIF(*ALL) が指定されている場合は例外です。その場合、オブジェクトが復元され、システム上の所有者が使用されます。

1 次グループ・オプション:

システム上に存在しないオブジェクトの場合、以下が適用されます。

- オブジェクトの 1 次グループであるプロファイルがシステム上にある場合、そのオブジェクトに対する 1 次グループ値および権限が復元されます。
- 1 次グループであるプロファイルがシステム上に存在しない場合、以下が適用されます。
  - オブジェクトの 1 次グループは、「なし」に設定されます。
  - 1 次グループ権限は「権限なし」に設定されます。

既存のオブジェクトが復元されるとき、そのオブジェクトの 1 次グループは復元操作で変更されません。

共通権限:

- 復元されるオブジェクトがシステム上にない場合、共通権限は保管されたオブジェクトの共通権限に設定されます。
- 復元されるオブジェクトが存在し、置き換えられる場合には、共通権限は変更されません。保管されたオブジェクト・バージョンからの共通権限は使用されません。
- ライブラリーにオブジェクトを復元する際には、ライブラリーに対する CRTAUT は使用されません。

権限リスト:

- 文書またはフォルダー以外のオブジェクトがすでにシステムに存在し、権限リストにリンクされている場合には、ALWOBJDIF パラメーターによって以下の結果が決定されます。
  - ALWOBJDIF(*NONE) が指定されている場合、既存のオブジェクトは保管オブジェクトと同じ権限リストを持たなければなりません。そうでない場合、オブジェクトは復元されません。 –
  - ALWOBJDIF(*ALL) が指定されている場合、そのオブジェクトは復元されます。オブジェクトは既存のオブジェクトと関連する権限リストにリンクされます。
- すでにシステムに存在している文書またはフォルダーが復元される場合、システム上のオブジェクトに関連した権限リストが使用されます。保管された文書またはフォルダーの権限リストは使用されません。
- 権限リストがシステム上にない場合、オブジェクトは権限リストにリンクされずに復元され、共通権限は *EXCLUDE に変更されます。
- 保管元のシステムと同じシステムにオブジェクトを復元する場合、オブジェクトは権限リストに再びリンクされます。
- オブジェクトを別のシステムに復元する場合、復元コマンド上の ALWOBJDIF パラメーターを使用して、オブジェクトを権限リストにリンクさせるかどうかを決定します。
  - ALWOBJDIF(*ALL) が指定される場合、オブジェクトは権限リストにリンクされます。
  - ALWOBJDIF(*NONE) が指定される場合、オブジェクトは権限リストにリンクせず、オブジェクトの共通権限は *EXCLUDE に変更されます。

私用権限:

- 私用権限はオブジェクトとともにではなく、ユーザー・プロファイルとともに保管されます。
- ユーザー・プロファイルが、復元されるオブジェクトに対する私用権限を持っている場合には、通常、これらの私用権限は影響を受けません。いくつかの種類のプログラムを復元すると、私用権限が取り消されることがあります。

- オブジェクトがシステムから削除された後、保管されたバージョンから復元される場合には、オブジェクトの私用権限はもはやシステム上に存在しません。あるオブジェクトが削除されると、そのオブジェクトに対するすべての私用権限はユーザー・プロファイルから除去されます。
- 私用権限を回復する必要がある場合、権限復元 (RSTAUT) コマンドを使用しなければなりません。通常の順序は以下のとおりです。
  1. ユーザー・プロファイルを復元する。
  2. オブジェクトを復元する。
  3. 権限を復元する。

オブジェクト監査:
- 復元されるオブジェクトがシステムに存在しない場合、保管されたオブジェクトのオブジェクト監査 (OBJAUD) 値が復元されます。
- 復元されるオブジェクトが存在し、置き換えられる場合には、オブジェクト監査値は変更されません。保管されたオブジェクト・バージョンの OBJAUD 値は復元されません。
- 復元されるライブラリーがシステムに存在しない場合、ライブラリーのオブジェクト監査作成 (CRTOBJAUD) 値が復元されます。
- 復元されるライブラリーが存在し、置き換えられる場合には、ライブラリーの CRTOBJAUD 値は復元されません。既存のライブラリーの CRTOBJAUD 値が使用されます。

権限ホルダー:
- ファイルが復元され、そのファイル名および復元先のライブラリーに対する権限ホルダーが存在する場合、ファイルはその権限ホルダーとリンクします。
- 権限ホルダーに関連した権限情報は、共通権限およびファイルとともに保管された所有者情報に置き換わります。

ドメイン・オブジェクト: OS/400 ライセンス・プログラムのバージョン 2 リリース 3 以降で実行中のシステムの場合、システムは、ユーザー・ドメイン・オブジェクト (*USRSPC、*USRIDX、および *USRQ) を QALWUSRDMN システム値で指定されたライブラリーに制限します。*USRSPC、*USRIDX、または *USRQ タイプのユーザー・ドメイン・オブジェクトを保管した後にライブラリーが QALWUSRDMN システム値から除去された場合、システムは、オブジェクトが復元されるときにオブジェクトをシステム・ドメインに変更します。

機能登録情報: QUSEXRGOBJ *EXITRG オブジェクトを QUSRSYS に復元することにより、機能登録情報を復元できます。これによって、登録済み機能のすべてが復元されます。機能に関連した使用法情報は、ユーザー・プロファイルおよび権限の復元時に復元されます。

認証登録情報を使用するアプリケーション: QUSEXRGOBJ *EXITRG オブジェクトを QUSRSYS に復元することにより、認証登録情報を使用するアプリケーションを復元できます。これによって、登録済みのすべてのアプリケーションが復元されます。アプリケーションと認証情報の関連は、QYCDCERTI *USRIDX オブジェクトを QUSRSYS に復元することによって復元できます。

詳しくは、「権限の復元」を参照してください。

権限の復元

セキュリティー情報の復元時には、私用権限を再構築する必要があります。権限テーブルを持っているユーザー・プロファイルを復元するときは、 そのプロファイルの権限テーブルもまた復元されます。権限復元 (RSTAUT) コマンドは、権限テーブルからの情報を利用してユーザー・プロファイル内に私用権限を再構築します。

権限認可操作は、権限テーブル内のそれぞれの私用権限に実行されます。多数のプロファイルの権限を復元する場合、権限テーブルに多数の私用権限が存在すれば、処理に時間がかかる可能性があります。単一のプロファイル、プロファイルのリスト、総称プロファイル名、またはすべてのプロファイルに対して RSTUSRPRF および RSTAUT コマンドを実行できます。システムは SAVSECDTA コマンド、SAVSYS コマンド、または QSRSAVO API によって作成された保管媒体または保管ファイルを検索して、復元対象のプロファイルを見つけます。

フィールド権限の復元:

以下は、システム上にまだ存在しないデータベース・ファイルの私用フィールド権限を復元するために必要なステップです。

- 必要なユーザー・プロファイルを復元または作成する。
- ファイルを復元する。
- 権限復元 (RSTAUT) コマンドを実行する。

私用フィールド権限によって制限される私用オブジェクト権限が再び確立されるまでは、私用フィールド権限は完全には復元されません。

詳しくは、「プログラムの復元」を参照してください。

プログラムの復元

不明なソースから入手したプログラムをユーザーのシステムに復元すると、機密漏れが生じる可能性があります。プログラムは、ユーザーのセキュリティー要件を満たさない操作を実行するかもしれません。 特に注意する必要があるのは、制限付きの命令を持つプログラム、所有者権限を借用するプログラム、および改ざんされたプログラムです。

これには、オブジェクト・タイプ *PGM、*SRVPGM、*MODULE、および *CRQD が含まれます。QVFYOBJRST、QFRCCVNRST、および QALWOBJRST のシステム値を使用すると、これらのオブジェクト・タイプをシステムに復元することを防止できます。これらのシステム値の詳細については、「セキュリティー関連の復元」システム値を参照してください。

システムは、プログラムを保護するために妥当性検査値を使用します。この値はプログラムとともに保管され、プログラムが復元される時に再計算されます。システムの処置は、復元コマンドの ALWOBJDIF パラメーター、および復元時の強制変換 (QFRCCVNRST) システム値によって決定されます。

注: バージョン 5 リリース 1 以降の OS/400 または i5/OS を実行するシステム用に作成されたプログラムには、復元時に必要に応じてプログラムの再作成を可能にする情報が含まれています。プログラム再作成に必要な情報は、プログラム識別情報が削除されても、そのプログラムに残ります。プログラムの復元時に、プログラム妥当性検査エラーの存在が判別された場合には、妥当性検査エラーを訂正するためにそのプログラムが再作成されます。復元時にプログラムを再作成する処置は、iSeries バージョン 5 リリース 1 の新機能ではありません。以前のリリースでも、復元時にプログラム妥当性検査エラーが検出されると、可能な場合 (復元されるプログラムにプログラム識別情報が存在する場合) にはプログラムが再作成されました。バージョン 5 リリース 1 以降のプログラムの違いは、プログラム識別情報がプログラムから除去されても、プログラムの再作成に必要な情報が残ることです。

所有者権限を借用するプログラムの復元:

所有者権限を借用するプログラムを復元すると、そのプログラムに対する所有権と権限が変更されることがあります。以下が該当します。

- 復元操作を行うユーザー・プロファイルは、プログラムを所有しているか、*ALLOBJ および *SECADM 特殊権限を持っていなければなりません。
- 復元操作を行うユーザー・プロファイルは、以下の方法により、プログラムを復元するための権限を受け取ることができます。
  - プログラム所有者となる。
  - プログラムを所有するグループ・プロファイルのメンバーとなる (プログラムに私用権限をもっていない場合)。
  - *ALLOBJ および *SECADM 特殊権限を持つ。
  - *ALLOBJ および *SECADM 特殊権限を持つグループ・プロファイルのメンバーになる。
  - リストされているテストの 1 つを満たす借用権限の下で実行する。
- 復元されるプロファイルが適切な権限を持っていない場合、プログラムに対するすべての共通権限および私用権限は取り消され、共通権限は *EXCLUDE に変更されます。
- プログラムの所有者がシステム上に存在しない場合、QDFTOWN ユーザー・プロファイルに所有権が与えられます。共通権限は *EXCLUDE に変更され、権限リストは除去されます。

詳しくは、「ライセンス・プログラム復元」を参照してください。

ライセンス・プログラム復元

ライセンス・プログラム復元 (RSTLICPGM) コマンドを使用して、システム上に IBM 提供プログラムを導入することができます。 また、SystemView* システム・マネージャー/400* ライセンス・プログラムによって作成された、IBM 以外のプログラムを導入することもできます。

システムが出荷された時点では、*ALLOBJ 特殊権限を持つユーザーだけが RSTLICPGM コマンドを使用できます。 RSTLICPGM プロシージャーは、IBM 提供以外のプログラムを導入する出口プログラムを呼び出します。

システムのセキュリティーを保護するためには、*ALLOBJ 特殊権限を持つプロファイルを使って出口プログラムを実行すべきではありません。*ALLOBJ 権限を持つユーザーに RSTLICPGM コマンドを直接実行させるのではなく、*ALLOBJ 特殊権限を借用するプログラムを使ってコマンドを実行してください。

たとえば、次のようにします。RSTLICPGM コマンドを使用して導入されるプログラムを CPAPP (契約および価格設定) と呼びます。

1. アプリケーションを正常に導入するために十分な権限を持ったユーザー・プロファイルを作成します。このプロファイルに *ALLOBJ 特殊権限を与えないでください。たとえば、OWNCP というユーザー・プロファイルにします。
2. アプリケーションを導入するためのプログラムを書きます。たとえば、プログラムに次のように名前を付けます。 CPINST: PGM RSTLICPGM CPAPP ENDPGM
3. CPINST プログラムを作成して、*ALLOBJ 特殊権限 (QSECOFR など) を持つユーザーの権限を借用し、プログラムに対して OWNCP を認可します。

   ```
   CRTCLPGM QGPL/CPINST USRPRF(*OWNER) +
   AUT(*EXCLUDE) GRTOBJAUT OBJ(CPINST) OBJTYP(*PGM) +
            USER(OWNCP)  AUT(*USE)
   ```

4. OWNCP としてサインオンし、CPINST プログラムを呼び出します。 CPINST プログラムが RSTLICPGM コマンドを実行するときには、QSECOFR 権限の下で実行します。 出口プログラムは、CPAPP プログラムの導入を実行するときに借用権限を終了させます。出口プログラムによって呼び出されたプログラムは、OWNCP 権限の下で実行されます。

段階的な手順については、「権限リストの復元」を参照してください。

権限リストの復元

権限リストは、SAVSECDTA コマンドまたは SAVSYS コマンドによって保管されます。

権限リストは RSTUSRPRF USRPRF(*ALL) コマンドによって復元されます。個々の権限リストを復元する方法はありません。権限リストを復元すると、他の復元されたオブジェクトの場合と同様に、権限と所有権が確立されます。

権限リストの後にオブジェクトが復元された場合には、権限リストとオブジェクトの間のリンクが確立されます。リストへのユーザーの私用権限は、RSTAUT コマンドを使用して復元されます。

次に、オペレーティング・システムを復元します。

オペレーティング・システムの復元

システム上で手動の IPL を実行する場合、「IPL / システムの導入」メニューには、オペレーティング・システムを導入するオプションが提供されます。

専用保守ツール (DST) 機能を使用すれば、このメニュー・オプションを使用するすべてのユーザーに対して DST セキュリティー・パスワードを入力するよう要求することができます。これを使用すると、何者かが許可なくオペレーティング・システムのコピーを復元することを防止できます。オペレーティング・システムの導入を保護するには、以下のようにします。

1. 手動で IPL を実行する。
2. 「IPL / システムの導入」メニューから、DST を選択する。
3. 「DST の使用」メニューから、DST 環境処理オプションを選択する。
4. DST パスワード変更オプションを選択する。
5. オペレーティング・システム導入のセキュリティーを変更オプションを選択する。
6. 1 (セキュリティー) を指定する。
7. F3 (終了) を押して、「IPL/ システムの導入」メニューに戻る。
8. 手動 IPL を完了して、キーロックを通常位置に戻す。

注:

1. オペレーティング・システムの導入を保護する必要がなくなった場合、同じステップを実行し、2 (非セキュリティー) を指定してください。
2. また、キーロック・スイッチを通常位置のままにしてそのキーを除去することによっても、オペレーティング・システムの導入を防ぐことができます。

詳しくは、「セキュリティー情報の管理」を参照してください。

セキュリティー情報の管理

この項では、セキュリティー情報の管理に関する作業を説明します。

ご使用のシステムのセキュリティーを計画し終えたので、ここでビジネスで変更の必要が生じたときに、計画が依然として有効であるか確認する必要があります。このトピックでは、セキュリティーを設計する上での基本的な目標として、単純であることを強調しています。ユーザー・グループを個々のユーザーのパターンとして設計しました。また、特定の個別権限ではなく、共通権限、権限リスト、およびライブラリー権限を使用することにしました。セキュリティーを管理する際に、次のようにしてそのアプローチの利点を活用します。

- 新しいユーザー・グループまたは新しいアプリケーションを追加する際には、セキュリティーを計画するために使用した技法を使用します。
- セキュリティーに変更を加える必要がある場合は、特定の問題を解決するための例外を作成するのではなく、一般的なアプローチを使用するようにします。

セキュリティー・コマンド処理

ここでは、セキュリティー・コマンドを使ってセキュリティー情報を表示、変更、および削除する方法について説明します。

下記の表には、システム上のセキュリティー・オブジェクトを処理するために使用するコマンドが示されています。これらのコマンドを使用して、以下の作業を行うことができます。

- セキュリティー情報の表示およびリスト
- セキュリティー情報の変更
- セキュリティー情報の削除

表 111. セキュリティー・コマンド

セキュリティー・オブジェクト	表示方法	変更方法	削除方法
システム値	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	削除できません。
ジョブ記述	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD
グループ・ プロファイル	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1]、[2]
ユーザー・プロファイル	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]
オブジェクト権限	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT
オブジェクト所有権	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN を使用すれば、以前の所有者の権利を取り消すことができます。
1 次グループ	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP は、1 次グループを *NONE に設定します。
オブジェクト監査	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD (*NONE に設定) CHGAUD
権限リスト	DSPAUTL DSPAUTLOBJ	EDTAUTL (リストに対するユーザー権限) EDTOBJAUT (リストによって保護されるオブジェクト) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL (リスト全体)[3] RMVAUTLE (リストに対するユーザー権限の除去) EDTOBJAUT (リストによって保護されるオブジェクト) RVKOBJAUT

表 111. セキュリティー・コマンド (続き)

セキュリティー・オブジェクト	表示方法	変更方法	削除方法
1. IBM は、「ユーザー登録の処理」画面の除去オプションを使ってプロファイルを削除することをお勧めします。このオプションを使用すると、プロファイルが所有しているオブジェクトを削除したり、それらを新規所有者に再割り当てすることができます。特定の DLTUSRPRF コマンド・パラメーターを使用すると、ユーザーが所有しているすべてのオブジェクトを削除したり、それらをすべて新規所有者に割り当てることができます。所有されているオブジェクトを削除するか、再割り当てしない限り、プロファイルを削除することはできません。さらに、プロファイルがいずれかのオブジェクトの 1 次グループである場合は、そのプロファイルを削除できません。 2. メンバーを有しているグループ・プロファイルは削除できません。グループのメンバーをリストするには、DSPUSRPRF コマンドの *GRPMBR オプションを使用します。グループ・プロファイルを削除する前に、それぞれの個別のグループ・プロファイルごとに「グループ・ファイル」フィールドを変更します。 3. 権限リストがオブジェクトの保護に使用されている場合、その権限リストを削除することはできません。リストによって保護されているオブジェクトをリストするには、DSPAUTLOBJ コマンドを使用してください。リストによって保護されているオブジェクトの権限を変更するには、EDTOBJAUT コマンドを使用してください。			

セキュリティー情報の表示およびリスト

セキュリティー情報をリストするには、表示 (DSP) コマンドで印刷 (*PRINT) オプションを指定します。たとえば、MYLIST という権限リストを表示するには、`DSPAUTL MYLIST *PRINT` と入力します。

表示コマンドによっては、さまざまなタイプのリストのオプションを提供するものがあります。たとえば、個別のユーザー・プロファイルの作成時に DSPUSRPRF コマンドで *GRPMBR オプションを指定すると、グループ・プロファイルのすべてのメンバーがリストされます。プロンプト (F4) とオンライン情報を使用して、セキュリティー・オブジェクトに使用可能なリストを見つけてください。

表示コマンドを使用すると、ディスプレイ装置にセキュリティー情報を表示できます。さらに、より多くの機能を提供する「... 処理」(WRK) コマンドを使用することもできます。「... 処理」コマンドによって、リストが画面に表示されます。この画面を使用して、情報の変更、削除、および表示を行うことができます。

さらに、セキュリティー・コマンドでは、総称名を使って情報をリストまたは表示することもできます。`WRKUSRPRF DPT*` と入力した場合、「ユーザー登録の処理」画面または「ユーザー・プロファイル処理」画面には、*DPT* という文字で始まるプロファイルだけが表示されます。総称名の使用を許可しているパラメーターを確認するには、コマンドのオンライン情報を参照してください。

セキュリティー情報の変更

「... 処理」(WRK) または「 ... 編集」(EDT) コマンドを使用して、セキュリティー情報を対話式に変更することができます。情報を表示し、変更した後で、再びその情報を表示できます。

また、「... 変更」(CHG) または「 ... 認可」(GRT) コマンドを使用すれば、変更前と変更後の情報を表示せずにセキュリティー情報を変更することができます。この方法は、一度に複数のオブジェクトを変更する場合に特に便利です。たとえば、GRTOBJAUT コマンドを使用して、ライブラリー内のすべてのオブジェクトの共通権限を設定します。

セキュリティー情報の削除

「... 処理」(WRK) または「 ... 編集」(EDT) コマンドを使用して、特定のタイプのセキュリティー情報を対話式に削除または除去できます。さらに、「... 削除」(DLT)、「... 除去」(RMV)、および「... 取り消

し」(RVK) コマンドを使用して、セキュリティー情報を削除することもできます。セキュリティー情報の削除がシステムによって許可されるには、特定の条件を満たさなければならない場合があります。

システムへの新しいユーザーの追加

この情報では、システムに新しいユーザーを追加する方法について説明します。

次のいくつかの理由のため、新しいユーザー・グループを作成しなければならない場合があります。

- その他の部門で、そのシステムを使用する必要があるとき。
- 資源保護の必要を満たすために、ユーザー・グループをもっと特定する必要があることに気付いたとき。
- 企業が一部の部門を再編成したとき。

システムに新しいユーザーを追加する必要があるときは、次の手順を使用します。

1. 個人をユーザー・グループに割り当てます。ユーザー・グループ記述ワークシートを参考にしてください。
2. 新しいユーザーがシステム機能を実行する必要があるかどうかを決定します。その必要がある場合は、その情報をシステム責任用紙に追加します。
3. 個人を個別ユーザー・プロファイル用紙に追加します。
4. システム責任ワークシートとユーザー・グループ記述ワークシートを検討して、新しいユーザーがそのグループの値とは異なる値を必要とするかどうかを判別します。
5. グループ・プロファイルまたはグループ・メンバーのプロファイルをコピーして、ユーザー・プロファイルを作成します。パスワードの期限満了を必ず設定してください。
6. 新しいユーザーにセキュリティーのメモのコピーを渡します。

新しいアプリケーションの追加

この項では、新しいアプリケーションの追加方法について取り上げ、ステップバイステップの指示を提供します。

新しいアプリケーションのセキュリティーを計画する際には、元となるアプリケーションを計画したときと同じように注意して行う必要があります。手順も同じです。

1. アプリケーションのアプリケーション記述ワークシートとライブラリー記述ワークシートを作成します。
2. アプリケーション、ライブラリー、およびユーザー・グループの図を更新します。
3. 『資源保護の計画』の手順に従って、新しいアプリケーションのセキュリティーを行う方法を選択します。
4. 『アプリケーションの導入の計画』に説明されている方法を使用して、アプリケーションの導入ワークシートを作成します。
5. アプリケーションからのプリンター出力が機密になっており、保護が必要かどうか評価します。必要に応じて、出力待ち行列およびワークステーションのセキュリティー・ワークシートを更新してください。
6. 『所有権および共通権限の設定』、および『資源保護の設定』で説明されているステップに従って、アプリケーションの導入およびセキュリティーを行います。

新しいワークステーションの追加

この項では、新しいワークステーションの追加方法について取り上げ、ステップバイステップの指示を提供します。

新しいワークステーションをシステムに追加する際には、次のセキュリティー要件を考慮してください。

1. 新しいワークステーションの物理的な位置によって、セキュリティーのリスクが生じますか。(詳しくは、『物理的セキュリティーの計画』を参照してください。)
2. ワークステーションでリスクが生じる場合、出力待ち行列およびワークステーションのセキュリティー・ワークシートを更新します。
3. 通常は、共通権限 *CHANGE を使用して新しいワークステーションを作成します。ワークステーションのセキュリティー要件を満たしていない場合は、EDTOBJAUT コマンドを使用して別の権限を指定します。

ユーザー・グループの変更

この項では、ユーザー・グループの変更方法、およびそれが重要な理由を取り上げ、ステップバイステップの説明を行います。

グループの特性に対して変更を加えるには、変更のタイプに応じた方法で処理する必要があります。次に、変更例とそれらを扱う方法について示します。

グループの権限の変更

グループが必要とするオブジェクトに対する権限が、計画の初期の段階では予期していなかったものであることがわかったとします。この場合、以下のことを行ってください。

1. オブジェクト権限編集 (EDTOBJAUT) コマンドを使用して、グループがオブジェクトまたは適切な権限リストに正しくアクセスできるようにします。『オブジェクト用およびライブラリー用の特定権限の設定』には、このことを行う方法の例が示されています。グループ権限を与えると、グループのすべてのメンバーはオブジェクトに対する権限を取得します。
2. グループ権限を機密資源に与える場合、グループの現在のメンバーを調べることができます。ユーザー・プロファイル表示コマンド (DSPUSRPRF group-profile-name *GRPMBR) を使用して、グループ・メンバーをリストしてください。

グループのカスタマイズの変更

グループのメンバーに合ったユーザー環境の設定を変更しなければならないことがあります。たとえば、ある部門に専用のプリンターが設置される場合、その部門のユーザー・グループのメンバーのために、新しいプリンターがデフォルトになるようにしたいと思うことでしょう。あるいは、システムに新しいアプリケーションが導入される際には、ユーザー・グループのメンバーは、サインオン時に別の初期メニューを表示してほしいと思うことでしょう。

グループ・プロファイルでは、グループ・メンバーに個々のプロファイルを作成するためにコピーできるパターンを提供します。しかし、グループ・プロファイルのカスタマイズ値は、個別のユーザー・プロファイルを作成した後は、それらに影響を与えることはありません。たとえば、グループ・プロファイルで「プリンター」などのフィールドを変更しても、グループ・メンバーには影響を与えません。この場合には、個別のユーザー・プロファイルにある「プリンター」フィールドを変更する必要があります。

「ユーザー・プロファイル処理」画面を使用して、一度に複数のユーザーのパラメーターを変更することができます。例では、グループのすべてのメンバーの出力待ち行列を変更します。

1. WRKUSRPRF *ALL と入力して、Enter キーを押します。
2. 「ユーザー登録の処理」画面が表示される場合は、F21 (操作援助レベルの選択) を使用して、「ユーザー・プロファイルの処理」画面に変更します。

```
                        ユーザー・プロファイルの処理

オプションを入力して，実行キーを押してください。
  1= 作成    2= 変更    3= コピー    4= 削除    5= 表示
  12= 所有者によるオブジェクトの処理

     ユーザー・
OPT  プロファイルテキスト
     HARRISOK    HARRISON, KEITH
2    HOGANR      HOGAN, RICHARD
     JONESS      JONES, SHARON
2    WILLISR     WILLIS, ROSE
 .
 .
                                                                  続く ...
オプション 1，2，3，4，5 のパラメーターまたはコマンド
===> PRTDEV(PRT02)
F3= 終了         F5= 最新表示    F12= 取り消し    F16= 位置指定の繰り返し
F17= 位置指定    F21= 援助レベルの選択            F24= キーの続き
```

3. 変更したいそれぞれのプロファイルの横に 2 (変更) と入力します。
4. 画面の下部のパラメーター行に、パラメーター名と新しい値を入力します。パラメーター名がわからない場合は、F4 (プロンプト) を押します。
5. Enter キーを押します。変更したプロファイルごとに確認メッセージが表示されます。グループ・プロファイルにあるカスタマイズ・フィールドを変更してもグループ・メンバーに影響を与えることはありませんが、今後、役に立つことがあるかもしれません。後でグループにメンバーを追加したいときに、グループ・プロファイルはパターンを提供します。また、これはグループの標準フィールド値の記録ともなります。

新しいアプリケーションへのグループ・アクセスの提供

ユーザー・グループが新しいアプリケーションにアクセスする必要があるときに、グループについての情報とアプリケーションについての情報を分析する必要があります。次に推奨される方法を示します。

1. 新しいアプリケーションのアプリケーション記述ワークシートとアプリケーション、ライブラリー、およびユーザー・グループの図を見てアプリケーションが使用するライブラリーを確認します。これらのライブラリーをユーザー・グループ記述ワークシートに追加します。
2. アプリケーション、ライブラリー、およびユーザー・グループの図を更新して、ユーザー・グループとアプリケーションの新しい関係を表示します。
3. グループの初期ライブラリー・リストにライブラリーを含める必要がある場合は、ジョブ記述変更 (CHGJOBD) コマンドを使用して、グループのジョブ記述を変更します。ジョブ記述の処理についてのヘルプが必要な場合は、『ジョブ記述の作成』を参照してください。

   注: ジョブ記述にあるすべてのライブラリーを初期ライブラリー・リストに追加する場合は、そのジョブ記述を使用するユーザー・プロファイルを変更する必要はありません。ユーザーが次にサインオンするときに、初期ライブラリー・リストが自動的にライブラリーを追加します。
4. 新しいアプリケーションにアクセスするために、グループの初期プログラムか初期メニューのどちらかを変更する必要があるかどうか評価します。 CHGUSRPRF コマンドを使用して、各ユーザー・プロファイルの初期メニューまたはプログラムをそれぞれ変更する必要があります。
5. アプリケーションが使用するすべてのライブラリーのライブラリー記述用紙を検討します。ライブラリーで使用可能な共通アクセスが、グループの必要を十分に満たしているかどうか判別します。十分でない場合は、グループ権限をライブラリー、特定のオブジェクト、または権限リストに与えなければならないことがあります。これを行うには、オブジェクト権限編集 (EDTOBJAUT) および権限リストの編集 (EDTAUTL) コマンドを使用します。

ユーザー・プロファイルの変更

このトピックでは、ユーザー・プロファイルの変更方法について取り上げ、ステップバイステップの説明を行います。

システム・ユーザーが社内で新しい仕事または新しい責任を担う際には、ユーザー・プロファイルに与える影響を評価する必要があります。

1. ユーザーは別のユーザー・グループに属さなければならないでしょうか。ユーザー・プロファイルを変更するには、CHGUSRPRF コマンドを使用します。
2. プロファイル内で、プリンターまたは初期メニューなどのカスタマイズ値を変更する必要がありますか。カスタマイズ値を変更する際にも、CHGUSRPRF コマンドを使用します。
3. 新しいユーザー・グループのアプリケーション権限は、その人物にとって十分でしょうか。
   - ユーザー・プロファイル表示 (DSPUSRPRF) コマンドを使用して、古いグループ・プロファイルと新しいグループ・プロファイルの権限を比較します。
   - 個別のユーザー・プロファイルの権限も調べます。
   - EDTOBJAUT コマンドを使用して、必要な変更を加えます。
4. ユーザーは何らかのオブジェクトを所有しますか。それらのオブジェクトの所有権を変更しなければなりませんか。所有者によるオブジェクト処理 (WRKOBJOWN) コマンドを使用します。
5. ユーザーはシステム機能を実行しますか。ユーザーは新しいジョブのシステム機能を実行する必要がありますか。必要に応じて、システム責任ワークシートを更新し、ユーザー・プロファイルを変更します。

ユーザー・プロファイルの変更

オプション 2 (変更) を使用すれば、「ユーザー・プロファイルの処理」画面または「ユーザー登録の処理」画面のどちらからでもユーザー・プロファイルを変更することができます。また、ユーザー・プロファイル変更 (CHGUSRPRF) コマンドも使用できます。

コマンド入力を許可されているユーザーは、プロファイル変更 (CHGPRF) コマンドを使用して、自分のプロファイルのパラメーターの一部を変更することができます。

プロファイルの変更を行うユーザーより多くの特殊権限または機能を持つように、ユーザー・プロファイルを変更することはできません。

関連概念

9 ページの『ユーザー・プロファイル』
各システム・ユーザーは、システムにサインオンして使用するにはユーザー ID を有している必要があります。このユーザー ID をユーザー・プロファイルといいます。

使用禁止のユーザー・プロファイルの使用可能化

このトピックでは、使用禁止のユーザー・プロファイルを使用可能にする方法と、それが重要な理由を取り上げ、段階的な手順を示します。

システムで QMAXSIGN と QMAXSGNACN システム値に、サインオン試行回数が指定回数を超えるユーザー・プロファイルを使用禁止にするように設定されている場合は、システム操作員などに依頼して、状況を *ENABLE に変更してプロファイルを使用可能にしてもらうことができます。しかし、ユーザー・プロファイルを使用可能にするには、そのユーザー・プロファイルに対する *SECADM 特殊権限、 *OBJMGT 権限、および *USE 権限を持っていなければなりません。通常、システム操作員は *SECADM 特殊権限を持っていません。

解決策として、権限を借用する簡単なプログラムを使用することができます。

1. ユーザー・プロファイルに対する *SECADM 特殊権限、 *OBJMGT 権限、および *USE 権限を持つユーザーが所有する CL プログラムをシステム上で作成します。USRPRF(*OWNER) を指定してプログラムが作成される場合には、所有者の権限を借用してください。
2. EDTOBJAUT コマンドを使用して、プログラムに対する共通権限を *EXCLUDE にして、システム操作員に *USE 権限を与えてください。
3. 操作員は、以下のように入力してプロファイルを使用可能にできます。CALL ENABLEPGM *profile-name*
4. ENABLEPGM プログラムの主要な部分は、以下のようになります。

```
PGM &PROFILE
DCL VAR(&PROFILE) TYPE(*CHAR) LEN(10)
CHGUSRPRF USRPRF(&PROFILE) STATUS(*ENABLED)
ENDPGM
```

ユーザー・プロファイルのリスト

ユーザー・プロファイルに関する情報は、さまざまな形式で表示/印刷を行えます。個別プロファイルを表示して個別のユーザー・プロファイルの値を表示するには、「ユーザー登録の処理」画面または「ユーザー・プロファイルの処理」画面のいずれかでオプション **5** (表示) を使用してください。または、ユーザー・プロファイル表示 (DSPUSRPRF) コマンドを使用することもでき ます。

すべてのプロファイルのリスト

認可ユーザー表示 (DSPAUTUSR) コマンドは、システム上のすべてのユーザー・プロファイルを印刷または表示する場合に使用してください。このコマンドで順序 (SEQ) パラメーターを使用すると、プロファイル名またはグループ・プロファイル名に基づいてリストを分類することができます。

```
                          認可ユーザーの表示

                               最終
グループ・    ユーザー・      変更      パスワード
プロファイル プロファイル    パスワード なし      テキスト
 DSTSM
              ANDERSR       0X/08/04            ANDERS, ROGER
              VINCENT       0X/09/15            VINCENT, MARK
 DPTWH
              ANDERSR       0X/08/04            ANDERS, ROGER
              HOGANR        0X/09/06            HOGAN, RICHARD
              QUINN         0X/09/06            QUINN, ROSE
 QSECOFR
              JONESS        0X/09/20            JONES, SHARON
              HARRISON      0X/08/29            HARRISON, KEN
 *NO GROUP
              DPTSM         0X/09/05      X      販売営業
              DPTWH         0X/09/18      X      倉庫
```

F11 を押すと、各ユーザー・プロファイルで、パスワードがどのパスワード・レベルで使用されるように定義されているかを確認できます。

```
                              認可ユーザーの表示

                            最終      レベル     レベル
ユーザー・    ユーザー・    変更      0  か 1    2  か 3   NETSERVER
プロファイル プロファイルパスワードパスワードパスワードパスワード
 ANGELA                   0X/04/21    *YES       *NO        *YES
 ARTHUR                   0X/07/07    *YES       *YES       *YES
 CAROL1                   0X/05/15    *YES       *YES       *YES
 CAROL2                   0X/05/15    *NO        *NO        *NO
 CHUCKE                   0X/05/18    *YES       *NO        *YES
 DENNISS                  0X/04/20    *YES       *NO        *YES
 DPORTER                  0X/03/30    *YES       *NO        *YES
 GARRY                    0X/04/08    *YES       *YES       *YES
 JANNY                    0X/03/16    *YES       *NO        *YES
```

ユーザー・プロファイル画面のタイプ

ユーザー・プロファイル表示 (DSPUSRPRF) コマンドにより、いくつかのタイプの画面とリストを表示できます。

- 一部の画面およびリストは、個別のプロファイル用としてのみ使用できます。その他の画面とリストは、すべてのプロファイルまたは総称プロファイル・セット用に印刷することができます。使用できるタイプの詳細については、オンライン情報を参照してください。
- *出力* (*OUTFILE) を指定すると、複数の画面から出力ファイルを作成できます。 QUERY ツールまたは QUERY プログラムを使用すると、出力ファイルからカスタマイズされた報告書を作成することができます。

関連概念

9 ページの『ユーザー・プロファイル』
各システム・ユーザーは、システムにサインオンして使用するにはユーザー ID を有している必要があります。このユーザー ID をユーザー・プロファイルといいます。

ユーザー・プロファイル名の変更

ここでは、ユーザー・プロファイルの名前を変更する方法について説明します。名前変更することがなぜ重要か、および段階的な手順を示します。

システムは、ユーザー・プロファイル名を変更する直接的な方法を提供していません。

あるユーザーに新しい名前をつけて、同じ権限を持つ新しいユーザー・プロファイルとして作成することができます。ただし、一部の情報は新規プロファイルに転送できません。以下は、転送できない情報の例です。

- スプール・ファイル。
- ユーザーの設定およびユーザーについてのその他の情報を含む内部オブジェクトは、失われます。
- ユーザー名を含むディジタル認証は無効になります。
- 統合化ファイル・システムによって保持されていた uid および gid 情報は変更できません。
- ユーザー名を含んでいる、アプリケーションによって保管された情報を変更することはできません。

ユーザーによって実行されるアプリケーションには、「アプリケーション・プロファイル」が存在することがあります。ユーザー名を変更するために新規のシステム・ユーザー・プロファイルを作成しても、ユーザーが持つアプリケーション・プロファイルは名前変更されません。アプリケーション・プロファイルの一例としては、Lotus Notes® プロファイルがあります。

以下の例は、ユーザーに新しい名前を付けて、同じ権限を持つ新規プロファイルを作成する方法を示しています。前のプロファイル名は SMITHM です。新しいユーザー・プロファイル名は JONESM です。

1. 「ユーザー登録の処理」画面で、コピー・オプションを使用して、前のプロファイル (SMITHM) を新しいプロファイル (JONESM) にコピーします。
2. 次のようにユーザー権限認可 (GRTUSRAUT) コマンドを使用して、JONESM に SMITHM のすべての私用権限を与えます。

   ```
   GRTUSRAUT JONESM REFUSER(SMITHM)
   ```

3. 1 次グループによるオブジェクト処理 (WRKOBJPGP) コマンドを次のように使用して、 SMITHM が 1 次グループになっているすべてのオブジェクトの 1 次グループを変更します。

   ```
   WRKOBJPGP PGP(SMITHM)
   ```

   1 次グループを変更する必要があるすべてのオブジェクトに関してオプション 9 を入力し、コマンド行に NEWPGP (JONESM) と入力します。

   注: ユーザー・プロファイルの作成または変更 (CRTUSRPRF または CHGUSRPRF) コマンドの GID パラメーターを使用して、JONESM に gid を割り当てる必要があります。
4. ユーザー・プロファイル表示 (DSPUSRPRF) コマンドを次のように使用して、SMITHM ユーザー・プロファイルを表示します。 DSPUSRPRF USRPRF(SMITHM) SMITHM の uid および gid を書き留めます。
5. 他のすべての所有されているオブジェクトの所有権を JONESM に転送し、「ユーザー登録の処理」画面でオプション 4 (除去) を使用して、 SMITHM ユーザー・プロファイルを除去します。
6. ユーザー・プロファイル変更 (CHGUSRPRF) コマンドを次のように使用して、JONESM の uid と gid を、SMITHM に属していた uid および gid に変更します。

   ```
   CHGUSRPRF USRPRF(JONESM) UID(uid from SMITHM) GID(gid from SMITHM)
   ```

   JONESM がディレクトリー内にオブジェクトを所有している場合、CHGUSRPRF コマンドを使って uid および gid を変更することはできません。ユーザー・プロファイル JONESM の uid および gid を変更するには、QSYCHGID API を使用します。

ユーザー・プロファイルの可用性のスケジュール

特定のユーザー・プロファイルが、一日のうちの特定の時間帯、または週の特定の曜日にのみサインオンできるように設定したい場合があるかもしれません。

たとえば、セキュリティー監査員用にセットアップしたプロファイルがある場合、その監査員の作業がスケジュールされている時間帯のみ、そのユーザー・プロファイルを使用できるようにすることができます。稼働率が低い時間帯に、*ALLOBJ 特殊権限を持つユーザー・プロファイル (QSECOFR ユーザー・プロファイルを含む) を使用不可にすることもできます。

活動化スケジュール項目変更 (CHGACTSCDE) コマンドを使用すると、ユーザー・プロファイルを自動的に使用可能/使用不可に設定できます。スケジュールしたいユーザー・プロファイルごとに、ユーザー・プロファイルのスケジュールを定義する項目を作成します。

たとえば、朝 7 時から夜 10 時の間でのみ QSECOFR プロファイルを使用できるようにしたい場合、CHGACTSCDE 画面で以下のとおり入力します。

図 7. プロファイル活動化のスケジュール - 表示例

```
                        活動化スケジュール項目の変更  (CHGACTSCDE)

選択項目を入力して，実行キーを押してください。

ユーザー・プロファイル  . . . . > QSECOFR        名前
時刻の活動化  . . . . . . . . . . > '7:00'        時刻 , *NONE
時刻の非活動化  . . . . . . . . . > '22:00'       時刻 , *NONE
日数  . . . . . . . . . . . . . . > *MON          *ALL, *MON, *TUE, *WED...
                                  > *TUE
                                  > *WED
                                  > *THU
                  値の続きは＋    > *FRI
```

実際、一日につき限定された時間数だけ QSECOFR プロファイルを使用できるようにすることもできます。 *SECOFR クラスの別のユーザー・プロファイルを使用して、ほとんどのシステム機能を実行することができます。こうすれば、事前割り当てのユーザー・プロファイルがハッキング試行にさらされるのを防ぐことができます。

監査ジャーナル項目表示 (DSPAUDJRNE) コマンドを定期的に使用すると、CP (プロファイル変更) 監査ジャーナル項目を印刷することができます。これらの項目を使用して、システムが、計画されたスケジュールに応じてユーザー・プロファイルを使用可能/使用不可にしているかどうか検証します。

計画されたスケジュールに従ってユーザー・プロファイルが確実に使用不可にされていることを検査する別の方法として、ユーザー・プロファイル印刷 (PRTUSRPRF) コマンドを使用することができます。報告書タイプに *PWDINFO を指定すると、その報告書には、選択したユーザー・プロファイルそれぞれの状況が記載されます。たとえば、*ALLOBJ 特殊権限を持つすべてのユーザー・プロファイルを定期的に使用不可にしている場合、プロファイルが使用不可にされた直後に以下のコマンドを実行するようにスケジュールすることができます。 `PRTUSRPRF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)`

システムからのユーザーの除去

ここでは、システムからユーザーを除去する方法について説明します。除去することがなぜ重要か、および段階的な手順を示します。

退職者がいる場合、ユーザー・プロファイルをシステムから直ちに除去しなければなりません。ユーザー・プロファイルを削除する前に、そのプロファイルが所有しているオブジェクトの所有権を削除または転送する必要があります。そうするには、WRKOBJOWN コマンドを使用するか、「ユーザー登録の処理」画面でオプション 4 (除去) を使用します。「ユーザー登録の処理」画面でプロファイルに対するオプション 4 (除去) を選択すると、追加の画面が表示され、そこではユーザーが所有しているオブジェクトを処理することができます。次のように、すべてのオブジェクトを新しい所有者に与えるか、またはオブジェクトを個別に処理するかを選択できます。

```
                              ユーザーの除去

ユーザー . . . . . . . . . :   HOGANR
ユーザー記述 . . . . . . . :    販売営業


このユーザーを除去するためには，下に選択項目を入力してから実行キーを押してく
  ださい。

     1. このユーザーが所有するすべてのオブジェクトを新しい所有者に渡します。
     2. このユーザーが所有する特定のオブジェクト所有者を削除または変更します。
```

オブジェクトを個別に処理することを選択した場合 (オプション **2**)、画面にはユーザーが所有するすべてのオブジェクトがリストされます。

```
                              ユーザーの除去

ユーザー . . . . . :   HOGANR
ユーザー記述 . . . . . :    販売営業

新しい所有者 . . . . . .                    名前，リストは F4 キー

このユーザーを除去するためには，すべてのオブジェクトの所有者を削除または変更
  してください。
下のオプションを入力して，実行キーを押してください。
  2= 新しい所有者への変更    4= 削除    5= 明細の表示

OPT   オブジェクト        ライブラリー     記述
 4   HOGNAR               QUSRSYS       HOGAN, RICHARD メッセージ待ち行列
 4   QUERY1               DPTWH          在庫 QUERY
```

オブジェクトの削除を選択した場合には、「オブジェクトの削除の確認」画面が表示されます。オブジェクトがシステムから削除されたら、ユーザー・プロファイルを除去することができます。次に「ユーザー登録の処理」画面が再び表示され、システムがユーザーを除去したことを示すメッセージが表示されます。

ユーザー・プロファイルの削除

オブジェクトを所有するユーザー・プロファイルを削除することはできません。プロファイルが所有しているすべてのオブジェクトを削除するか、それらのオブジェクトの所有権を別のプロファイルに移さなければなりません。初級操作援助レベルと中間操作援助レベルのどちらも、プロファイルの削除の際に、所有されているオブジェクトの処理が可能です。

ユーザー・プロファイルがいずれかのオブジェクトの 1 次グループである場合には、そのプロファイルを削除できません。中間操作援助レベルを使用してユーザー・プロファイルを削除するときには、オブジェクトの 1 次グループを変更または除去できます。*OBJPGP (オブジェクト 1 次グループ) オプションを指定して DSPUSRPRF コマンドを使用すると、プロファイルが 1 次グループであるオブジェクトをすべてリストすることができます。

ユーザー・プロファイルを削除すると、そのユーザーはすべての配布リストおよびシステム・ディレクトリーから除去されます。

ユーザーのメッセージ待ち行列の所有権を変更したり、待ち行列を削除する必要はありません。システムは、プロファイルを削除する際にメッセージ待ち行列を自動的に削除します。

メンバーを有しているグループ・プロファイルは削除できません。グループ・プロファイルのメンバーをリストするには、 DSPUSRPRF *グループ・プロファイル名* *GRPMBR と入力します。グループ・プロファイルを削除する前に、各メンバー・プロファイル内の GRPPRF フィールドを変更してください。

ユーザー・プロファイル削除コマンドの使用

ユーザー・プロファイル削除 (DLTUSRPRF) コマンドを使用するには、コマンドを直接入力するか、「ユーザー・プロファイルの処理」画面でオプション 4 (削除) を使用できます。DLTUSRPRF コマンドには、以下の項目の処理を可能にするパラメーターがあります。

- プロファイルによって所有されるすべてのオブジェクト
- プロファイルが 1 次グループであるすべてのオブジェクト
- EIM の関連

ユーザー除去オプションの使用

「ユーザー登録の処理」画面で、削除したいプロファイルの前に 4 (除去) と入力します。ユーザー除去オプションが表示されます。

```
                              ユーザーの除去

ユーザー . . . . . :   HOGANR
ユーザー記述 . . . . . :    販売営業


このユーザーを除去するためには，下に選択項目を入力してから実行キーを押してく
  ださい。

     1．このユーザーが所有するすべてのオブジェクトを新しい所有者に渡します。
     2．このユーザーが所有する特定のオブジェクト所有者を削除または変更します。
```

プロファイルの削除の前にすべてのオブジェクト所有権を変更するには、オプション 1 を選択してください。新しい所有者の指定を求めるプロンプトが表示されます。

オブジェクトを個々に処理するには、オプション 2 を選択してください。詳細な「ユーザーの除去」画面が表示されます。

```
                              ユーザーの除去

ユーザー . . . . . :   HOGANR
ユーザー記述 . . . . . :    販売営業

新しい所有者 . . . . . .                    名前，リストは F4 キー

このユーザーを除去するためには，すべてのオブジェクトの所有者を削除または変更
  してください。
下のオプションを入力して，実行キーを押してください。
  2= 新しい所有者への変更    4= 削除    5= 明細の表示

OPT   オブジェクト        ライブラリー     記述
 4   HOGNAR               QUSRSYS       HOGAN, RICHARD メッセージ待ち行列
 2   QUERY1               DPTWH          在庫 QUERY
 2   QUERY2               DPTWH          在庫 QUERY
```

画面上のオプションを使って、オブジェクトを削除したり、オブジェクトを新しい所有者に転送します。すべてのオブジェクトが画面から削除されたら、プロファイルを削除できます。

注:

1. F13 キーを使用すれば、ユーザー・プロファイルが所有するすべてのオブジェクトを削除することができます。
2. スプール・ファイルは、「所有者によるオブジェクトの処理」画面には表示されません。ユーザー・プロファイルがスプール・ファイルを所有していても、そのユーザー・プロファイルの削除は可能です。ユーザー・プロファイルを削除した後、ユーザー・プロファイルが所有しているスプール・ファイルが不要になった場合は、スプール・ファイル処理 (WRKSPLF) コマンドを使ってスプール・ファイルを検索および削除できます。
3. 削除されたユーザー・プロファイルが 1 次グループであったすべてのオブジェクトでは、1 次グループが *NONE になります。

ユーザー・プロファイルの自動的な使用不可化:

長期にわたって組織を離れるユーザーがいる場合、 そのユーザーのプロファイルを使用不可 (非活動化) にします。

プロファイル活動分析 (ANZPRFACT) コマンドを使用すると、指定された日数にわたって使用されなかったユーザー・プロファイルを定期的に使用不可にします。ANZPRFACT コマンドを使用するときには、システムに検査させる非活動日数を指定します。システムは、最終使用日付、復元日付、およびユーザー・プロファイルの作成日を調べます。

いったん ANZPRFACT コマンドの値を指定すると、システムは、ジョブが週に一度、午前 1 時に実行されるようにスケジュールします (初めて値を指定した翌日から開始)。ジョブはすべてのプロファイルを調べて、非活動プロファイルを使用不可にします。非活動の日数を変更したい場合を除いて、再び ANZPRFACT コマンドを使用する必要はありません。

活動プロファイル・リスト変更 (CHGACTPRFL) コマンドを使用すると、 一部のプロファイルを ANZPRFACT 処理から外すことができます。 CHGACTPRFL コマンドは、プロファイルがどんなに長い間非活動状態であっても、ANZPRFACT コマンドによって使用不可にされないユーザー・プロファイルのリストを作成します。

システムが ANZPRFACT コマンドを実行するとき、使用不可化される各ユーザー・プロファイルに関する CP 項目が監査ジャーナル内に書き込まれます。DSPAUDJRNE コマンドを使用すると、新しく使用不可になったユーザー・プロファイルをリストすることができます。

要確認: システムが監査項目を書き込むのは、QAUDCTL 値が *AUDLVL、および QAUDLVL システム値が *SECURITY にそれぞれ指定されている場合だけです。

計画されたスケジュールに従ってユーザー・プロファイルが確実に使用不可にされていることを検査する別の方法として、ユーザー・プロファイル印刷 (PRTUSRPRF) コマンドを使用することができます。報告書タイプに *PWDINFO を指定すると、その報告書には、選択したユーザー・プロファイルそれぞれの状況が記載されます。

ユーザー・プロファイルの自動的な除去:

システムには、必要なユーザー・プロファイルだけを含めるようにしてください。 不要なユーザー・プロファイルは、システムに無許可の入り口を提供する恐れがあります。 ユーザーが組織からいなくなったか、組織内の別の仕事の担当になったために、ユーザー・プロファイルがこれ以降必要なくなった場合、ユーザー・プロファイルを除去します。

満了スケジュール項目変更 (CHGEXPSCDE) コマンドを使用すると、ユーザー・プロファイルの除去または使用不可を管理することができます。あるユーザーが長期間不在になることが分かっている場合、そのユーザー・プロファイルの除去または使用不可をスケジュールすることができます。

初めて CHGEXPSCDE コマンドを使用するとき、毎日深夜 12 時 1 分に実行されるジョブ・スケジュール項目が作成されます。このジョブは QASECEXP ファイルを参照して、ユーザー・プロファイルをその日に除去するようにスケジュールされているかどうかを判別します。

CHGEXPSCDE コマンドを使用して、ユーザー・プロファイルを使用不可にするか、あるいは削除します。ユーザー・プロファイルの削除を選択した場合、そのユーザーの所有するオブジェクトをシステムがどう扱うかを指定しなければなりません。ユーザー・プロファイルの削除をスケジュールする前に、ユーザーの所有するオブジェクトを調査しておく必要があります。たとえば、権限を借用するプログラムをユーザーが所有する場合、これらのプログラムに新しい所有者の所有権を借用させたいかどうか、あるいは、新しい所有者が必要以上の権限 (特殊権限など) を持つかどうか、などです。おそらく、権限を借用する必要のあるプログラムを所有するための特定権限を持つ新規ユーザー・プロファイルを作成することが必要でしょう。

また、ユーザー・プロファイルを削除した場合に、アプリケーションに問題が生じるかどうかを調べておく必要もあります。たとえば、いずれかのジョブ記述がデフォルト・ユーザーとしてそのユーザー・プロファイルを指定しているでしょうか。

満了スケジュール表示 (DSPEXPSCD) コマンドを使用すると、使用不可化または除去がスケジュールされているプロファイルのリストを表示することができます。認可ユーザー表示 (DSPAUTUSR) コマンドを使用すると、システム上のすべてのユーザー・プロファイルをリストすることができます。ユーザー・プロファイル削除 (DLTUSRPRF) コマンドを使用して、古くなったプロファイルを削除します。

セキュリティー上の注意事項: ユーザー・プロファイルの状況を *DISABLED に設定すると、そのユーザー・プロファイルは使用不可になります。ユーザー・プロファイルを使用不可にすると、そのユーザー・プロファイルは対話式に使用できなくなります。使用不可のユーザー・プロファイルを使ってサインオンすることも、使用不可のユーザー・プロファイルにジョブを変更することもできません。バッチ・ジョブは、使用不可のユーザー・プロファイル下で実行することができます。

セキュリティー・ツールを使用するためのシステム構成

この章では、i5/OS の 一部であるセキュリティー・ツールを使用するためのシステムのセットアップ方法について説明します。

i5/OS を導入すると、セキュリティー・ツールが使用できるようになります。以下の各トピックでは、セキュリティー・ツールの操作手順に関する推奨事項を示します。

セキュリティー・ツールの安全な使用

i5/OS を導入すると、セキュリティー・ツールに関連するオブジェクトが保護されます。セキュリティー・ツールを安全に操作するには、どのセキュリティー・ツール・オブジェクトの権限も変更しないでください。

次に、セキュリティー・ツール・オブジェクトに関するセキュリティー設定と要件について説明します。

- セキュリティー・ツールのプログラムとコマンドは QSYS プロダクト・ライブラリーに入っています。これらのコマンドとプログラムは、*EXCLUDE 共通権限付きで出荷されます。セキュリティー・ツール・コマンドの多くは、ファイルを QUSRSYS ライブラリーに作成します。システムがこれらのファイルを作成すると、これらのファイルの共通権限は *EXCLUDE になります。変更報告書を生成するための情報を含んでいるファイルの名前は、QSEC で始まります。ユーザー・プロファイルを管理するための情報を含んでいるファイルの名前は、QASEC で始まります。これらのファイルには、システムに関する機密情報が含まれています。したがって、これらのファイルに対する共通権限を変更しないでください。
- セキュリティー・ツールは、印刷出力を送信するために通常のシステム・セットアップを使用します。これらの報告書には、システムに関する機密情報が含まれています。保護された出力待ち行列に出力を送信するには、セキュリティー・ツールを実行するユーザーのユーザー・プロファイルまたはジョブ記述を適切に変更します。
- セキュリティー・ツール・コマンドは、セキュリティー機能を持っているため、またシステム上の多くのオブジェクトにアクセスするため、*ALLOBJ 特殊権限を必要とします。一部のコマンドには、*SECADM、*AUDIT、または *IOSYSCFG 特殊権限も必要です。これらのコマンドを正常に実行するには、セキュリティー・ツールを使用するときに機密保護担当者としてサインオンする必要があります。したがって、どのセキュリティー・ツール・コマンドに対しても私用権限を与える必要はありません。

ファイル競合の防止

セキュリティー・ツール報告書コマンドの多くは、報告書の変更バージョンの印刷に使用できるデータベース・ファイルを作成します。各コマンドのファイル名は、『セキュリティー・コマンドのコマンドおよびメニュー』に示されています。1 つのジョブからは一度に 1 つのコマンドしか実行できません。ほとんどのコマンドは、これを強制するために検査を行います。別のジョブがまだコマンドを完了していない場合、そのコマンドを実行すると、エラー・メッセージが表示されます。

多くの印刷ジョブは、長時間実行されます。報告書をバッチ処理に投入したり、報告書をジョブ・スケジューラーに追加する場合は、注意深くファイル矛盾を回避する必要があります。たとえば、異なる選択基準を持つ 2 つのバージョンの PRTUSRPRF 報告書を印刷したい場合があります。報告書をバッチ処理に投入する場合は、一時点で 1 つのジョブしか実行しないジョブ待ち行列を使用して、報告書ジョブが順次に実行されるようにします。

ジョブ・スケジューラーを使用する場合は、2 つのジョブの間に十分な時間間隔を入れ、最初のバージョンが完了してから 2 番目のジョブを実行するようにスケジュールします。

関連概念

21 ページの『システム・セキュリティー・ツール』
セキュリティー・ツールを使用すれば、システムのセキュリティー環境を管理および監視することができます。

セキュリティー・ツールの保管

システム保管 (SAVSYS) コマンドを実行するたびに、または SAVSYS コマンドを実行する「保管」メニューのオプションを実行するたびに、セキュリティー・ツール・プログラムが保管されます。

セキュリティー・ツール・ファイルは、QUSRSYS ライブラリーに入っています。このライブラリーは、すでに通常操作手順の一環として保管されているはずです。QUSRSYS ライブラリーには、システムで使用する多くのライセンス・プログラム用のデータが含まれています。QUSRSYS ライブラリーを保管するコマンドとオプションの詳細については、Information Center を参照してください。

セキュリティー・カスタマイズ用のコマンド

このセクションでは、セキュリティー・ツールのためのコマンドとメニューについて解説します。

セキュリティー・コマンド用のコマンドとメニュー

ここでは、コマンドの使用例を多数示します。セキュリティー・ツールでは、次の 2 つのメニューを使用することができます。

- SECTOOLS (セキュリティー・ツール) メニュー。コマンドを対話式に実行します。
- SECBATCH (バッチへのセキュリティー報告書の投入またはスケジュール) メニュー。バッチで報告書コマンドを実行します。

SECBATCH メニューは 2 つの部分に分かれています。メニューの最初の部分は、ジョブ投入 (SBMJOB) コマンドを使用して、バッチの即時処理を行うために報告書を投入します。 メニューの 2 番目の部分は、ジョブ・スケジュール項目追加 (ADDJOBSCDE) コマンドを使用します。このコマンドを使用して、指定された日時にセキュリティー報告書が定期的に実行されるようにスケジュールします。

セキュリティー・ツール・メニュー・オプション

表 112. ユーザー・プロファイルのツール・コマンド

メニュー・オプション[1]	コマンド名	説明	使用するデータベース・ファイル
1	ANZDFTPWD	デフォルト・パスワード分析コマンドを使用して、パスワードと名前が同じユーザー・プロファイルについて報告し、処置を行います。	QASECPWD[2]
2	DSPACTPRFL	活動プロファイル・リスト表示コマンドを使用して、ANZPRFACT 処理が免除されているユーザー・プロファイルのリストを表示または印刷します。	QASECIDL[2]
3	CHGACTPRFL	活動プロファイル・リスト変更コマンドを使用して、ANZPRFACT コマンドの免除リストにプロファイル・リストを追加または除去します。活動状態のプロファイル・リストにあるユーザー・プロファイルは、 (リストからこのプロファイルが除去されるまで) 永続的に活動状態です。活動状態のプロファイル・リストにあるプロファイルがどれほどの期間にわたって非活動状態になっても、ANZPRFACT コマンドは、そのプロファイルを使用不可にしません。	QASECIDL[2]
4	ANZPRFACT	プロファイル活動分析コマンドを使用して、指定された日数にわたって使用されなかったユーザー・プロファイルを使用不可にします。ANZPRFACT コマンドを使って日数を指定すると、システムは夜中に ANZPRFACT ジョブを実行します。 CHGACTPRFL コマンドを使用すれば、ユーザー・プロファイルが使用不可にならないようにすることができます。	QASECIDL[2]

表 112. ユーザー・プロファイルのツール・コマンド (続き)

メニュー・オプション[1]	コマンド名	説明	使用するデータベース・ファイル
5	DSPACTSCD	プロファイル活動化スケジュール表示コマンドを使用して、特定のユーザー・プロファイルを使用可能/使用不可にするスケジュールについての情報を表示または印刷します。スケジュールの作成には、CHGACTSCDE コマンドを使用します。	QASECACT[2]
6	CHGACTSCDE	活動化スケジュール項目変更コマンドを使用して、1 日または 1 週のうちの特定の時間しかユーザー・プロファイルをサインオンできないようにします。スケジュールする各ユーザー・プロファイルごとに、システムは、使用可能時間や使用不可時間のためのジョブ・スケジュール項目を作成します。	QASECACT[2]
7	DSPEXPSCD	満了スケジュール表示コマンドを使用して、今後使用不可にする予定、またはシステムから除去する予定のユーザー・プロファイルのリストを表示または印刷します。ユーザー・プロファイルの満了を設定するには、CHGEXPSCDE コマンドを使用します。	QASECEXP[2]

表 112. ユーザー・プロファイルのツール・コマンド (続き)

メニュー・オプション[1]	コマンド名	説明	使用するデータベース・ファイル
8	CHGEXPSCDE	満了スケジュール項目変更コマンドを使用して、ユーザー・プロファイルの除去をスケジュールします。ユーザー・プロファイルを一時的に除去したり (使用不可にすることによって)、あるいはシステムから削除することができます。このコマンドは、毎日 00:01 (深夜 0 時の 1 分後) に実行するジョブ・スケジュール項目を使用します。このジョブは、QASECEXP ファイルを参照して、ユーザー・プロファイルがその日に満了になるように設定されているかどうかを判別します。満了がスケジュールされているユーザー・プロファイルを表示するには、DSPEXPSCD コマンドを使用してください。	QASECEXP[2]
9	PRTPRFINT	プロファイル内部印刷コマンドを使用して、ユーザー・プロファイルの項目数に関する情報が含まれている報告書を印刷します。項目数は、ユーザー・プロファイルのサイズを決定します。	

注:

1. オプションは、SECTOOLS メニューから選択されます。
2. このファイルは、QUSRSYS ライブラリーに入っています。

システム・セキュリティー構成コマンドによって設定される値

この表は、CFGSYSSEC コマンドを実行する際に設定されるシステム値を リストしたものです。CFGSYSSEC コマンドは、 QSYS/QSECCFGS というプログラムを実行します。

CFGSYSSEC コマンドによって設定された値

表 113. CFGSYSSEC コマンドによって設定された値

システム値の名前	設定値	システム値の説明
QALWOBJRST	*NONE	システム状態プログラムおよび権限を借用するプログラムが復元できるかどうか

表 113. CFGSYSSEC コマンドによって設定された値 (続き)

システム値の名前	設定値	システム値の説明
QAUTOCFG	0 (いいえ)	新規装置の自動構成
QAUTOVRT	0	使用できる装置がない場合にシステムが自動的に作成する仮想装置記述の数
QDEVRCYACN	*DSCMSG (メッセージによる切り離し)	通信の再確立時のシステム処置
QDSCJOBITV	120	システムが切り離しジョブに対する処置を行う前の時間間隔
QDSPSGNINF	1 (はい)	ユーザーにサインオン情報画面を表示するかどうか
QINACTITV	60	システムが非活動対話式ジョブに対する処置を行う前の時間枠
QINACTMSGQ	*ENDJOB	システムが非活動ジョブに対して行う処置
QLMTDEVSSN	1 (はい)	ユーザーが一度に 1 つの装置でのサインオンに制限されるかどうか
QLMTSECOFR	1 (はい)	*ALLOBJ および *SERVICE のユーザーが特定の装置に限定されるかどうか
QMAXSIGN	3	連続して何回までサインオンの失敗が認められるか
QMAXSGNACN	3 (両方)	QMAXSIGN 限界に達した場合に、システムがワークステーションまたはユーザー・プロファイルを使用不可にするかどうか
QRMTSIGN	*FRCSIGNON	システムがリモート (パススルーまたは TELNET) サインオンの試行を処理する方法
QRMTSVRATR	0 (オフ)	この値の指定により、遠隔地からシステムを分析することを可能にする
QSECURITY	50	強制されるセキュリティー・レベル
QVFYOBJRST	3 (復元時に署名を検査)	復元でのオブジェクトの検査
QPWDEXPITV	60	ユーザーがパスワードを変更しなければならない頻度
QPWDMINLEN	6	パスワードの最小文字数
QPWDMAXLEN	8	パスワードの最大文字数
QPWDPOSDIF	1 (はい)	新規パスワードのすべての桁が、直前のパスワードの桁と異なっている必要があるかどうか
QPWDLMTCHR		パスワードで使用できない文字
QPWDLMTAJC	1 (はい)	パスワードで数字の隣接が禁止されるかどうか
QPWDLMTREP	2 (連続反復不可)	パスワードで文字の反復が禁止されるかどうか

表 113. CFGSYSSEC コマンドによって設定された値 (続き)

システム値の名前	設定値	システム値の説明
QPWDRQDDGT	1 (はい)	パスワードに 1 つ以上の数字が必要かどうか
QPWDRQDDIF	1 (32 個の固有パスワード)	パスワードが反復できるようになるまでには何個の固有パスワードが必要か
QPWDVLDPGM	*NONE	パスワードの妥当性検査を行うためにシステムが呼び出すユーザー出口プログラム

注:

1. メッセージ・ファイル QSYS/QCPFMSG のメッセージ ID CPXB302 に制限文字が保管されます。 出荷時には AEIOU@$# となっています。メッセージ記述変更 (CHGMSGD) コマンドを使用すれば、制限付き文字を変更することができます。パスワード・レベル 2 または 3 では、QPWDLMTCHR システム値は使用されません。

さらに CFGSYSSEC コマンドは、以下の IBM 提供のユーザー・プロファイルのパスワードを *NONE に設定します。

- QSYSOPR
- QPGMR
- QUSER
- QSRV
- QSRVBAS

最後に、CFGSYSSEC コマンドは、 セキュリティー監査変更 (CHGSECAUD) コマンドを使用してセキュリティー監査をセットアップします。 CFGSYSSEC コマンドは処置とオブジェクト監査をオンにし、CHGSECAUD コマンドでの監査を行うためのデフォルト設定の処置のセットも指定します。

プログラムのカスタマイズ:

いくつかの設定値がインストール・システムには適さない場合、コマンドを処理する独自のバージョンのプログラムを作成することができます。

この場合、以下のことを行ってください。

1. CL ソース検索 (RTVCLSRC) コマンドを使用して、CFGSYSSEC コマンドを使用するときに実行するプログラムのソースをコピーしてください。検索するプログラムは QSYS/QSECCFGS です。それを検索したら、別の名前を指定してください。
2. プログラムを編集して変更を行います。次に、プログラムをコンパイルします。コンパイルするときは、IBM 提供の QSYS/QSECCFGS プログラムを置き換えないようにしてください。プログラムには別の名前を付ける必要があります。
3. コマンド変更 (CHGCMD) コマンドを使用して、CFGSYSSEC コマンドのコマンド (PGM) パラメーターを処理するようにプログラムを変更してください。 PGM 値をプログラムの名前に設定します。たとえば、MYSECCFG と呼ばれる、QGPL ライブラリー内のプログラムを作成する場合は、次のように入力します。`CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MYSECCFG)`

   注: QSYS/QSECCFGS プログラムが変更される場合は、IBM はこのプログラムの信頼性、保守性、パフォーマンス、または機能を保証しません。商品性、特定目的適合性に関する黙示の保証の適用も一切ありません。

共通認可取り消しコマンドの機能

共通認可取り消し (RVKPUBAUT) コマンドを使用して、 コマンドとプログラムのセットの共通認可を *EXCLUDE に設定することができます。

共通認可が RVKPUBAUT コマンドによって設定されるコマンドおよび API

RVKPUBAUT コマンドは、QSYS/QSECRVKP というプログラムを実行します。出荷された時点で QSECRVKP は、下記の表にリストされているコマンドと、表 12 にリストされている アプリケーション・プログラミング・インターフェース (API) の共通認可を取り消します (共通認可を *EXCLUDE に設定することにより)。システムが到着した時点で、これらのコマンドと API の共通権限は *USE に設定されます。

表にリストされているすべてのコマンドと API は、システムに対する悪意のある操作を可能にする機能を実行します。機密保護管理者は、すべてのシステム・ユーザーに権限を与えるのではなく、これらのコマンドとプログラムを実行する権限を特定のユーザーに明示的に与える必要があります。

RVKPUBAUT コマンドを実行する際に、これらのコマンドを含むライブラリーを指定します。デフォルト値は QSYS ライブラリーです。システム上に複数の各国語ががある場合には、それぞれの QSYSxxx ライブラリーに関してこのコマンドを実行する必要があります。

表 114. 共通権限の設定

RVKPUBAUT コマンドを使用する。		
ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

表 115. 共通権限の設定

RVKPUBAUT コマンドを使用する。
QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

RVKPUBAUT コマンドを実行すると、システムはルート・ディレクトリーの共通認可を *USE に設定します (ただし、すでに *USE またはそれより低い権限に設定されている場合を除きます)。

プログラムのカスタマイズ:

いくつかの設定値がインストール・システムには適さない場合、コマンドを処理する独自のバージョンのプログラムを作成することができます。

以下のようにします。

1. CL ソース検索 (RTVCLSRC) コマンドを使用して、RVKPUBAUT コマンド使用時に実行されるプログラムのソースをコピーします。検索対象のプログラムは QSYS/QSECRVKP です。それを検索したら、別の名前を指定してください。
2. プログラムを編集して変更を行います。次に、プログラムをコンパイルします。コンパイルするときは、IBM 提供の QSYS/QSECRVKP プログラムを置き換えないようにしてください。プログラムには別の名前を付ける必要があります。
3. RVKPUBAUT コマンドに関する「コマンドを処理するプログラム」(PGM) パラメーターを変更するために、コマンド変更 (CHGCMD) コマンドを使用します。PGM 値をプログラムの名前に設定します。たとえば、MYRVKPGM という、QGPL ライブラリー内のプログラムを作成する場合は、次のように入力します: `CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)`

   注: QSYS/QSECRVKP プログラムを変更する場合、IBM は、プログラムの信頼性、保守容易性、性能、または機能性をほのめかしたり保証することはできません。商品性、特定目的適合性に関する黙示の保証の適用も一切ありません。

セキュリティー出口プログラムの使用

一部のシステム・サーバー機能には出口が設けられているため、 システムでユーザー作成プログラムを実行して追加の検査と妥当性検査を行うことができます。たとえば、誰かがシステム上で DDM (分散データ管理) ファイルをオープンしようとすると、 そのたびにシステムで出口プログラムを実行するようにセットアップすることができます。

サンプル出口プログラムのソース

登録機能を使用して、特定の条件下で実行する出口プログラムを指定できます。 以下の表は、これらの出口プログラムと例示プログラムの情報源のリストを示しています。

表 116. サンプル出口プログラムのソース

出口プログラムのタイプ	目的	例の入手先
パスワード妥当性検査	QPWDVLDPGM システム値には、プログラム名を指定できます。または、QIBM_QSY_VLD_PASSWRD 出口点用に登録されている妥当性検査プログラムを使用して、QPWDxxx システム値によって処理されない追加要件に関して新規パスワードを検査できることを指定します。このプログラムは暗号化されないパスワードを受け取るので、このプログラムの使用状況を注意深く監視する必要があります。このプログラムでパスワードをファイルに格納したり、他のプログラムにパスワードを渡したりしないでください。	• An Implementation Guide for iSeries Security and Auditing (GG24–4200) • iSeries 機密保護解説書 (SD88-5027-07)

表 116. サンプル出口プログラムのソース (続き)

出口プログラムのタイプ	目的	例の入手先
PC サポート/400 または Client Access のアクセス [1]	このプログラム名をネットワーク属性のクライアント要求アクセス (PCSACC) パラメーターに指定すれば、以下の機能を制御することができます。 • 仮想印刷装置機能 • ファイル転送機能と共用フォルダー・タイプ 2 機能 • クライアント・アクセス・メッセージ機能 • データ待ち行列 • リモート SQL 機能	An Implementation Guide for iSeries Security and Auditing (GG24–4200)
分散データ管理機能 (DDM) アクセス	このプログラム名をネットワーク属性の DDM 要求アクセス (DDMACC) パラメーターに指定すれば、以下の機能を制御することができます。 • 共用フォルダー・タイプ 0 および 1 機能 • リモート・コマンド投入機能	An Implementation Guide for iSeries Security and Auditing (GG24–4200)
リモート・サインオン	プログラムを QRMTSIGN システム値に指定して、 どのユーザーをどこの場所 (パススルー) から自動的にサインオンできるようにするかを制御することができます。	An Implementation Guide for iSeries Security and Auditing (GG24–4200)
iSeries Access で 使用の Open Database Connectivity (ODBC)[1]	次のような ODBC の機能を制御します。 • 少しでも ODBC の使用を許可するかどうか • iSeries データベース・ファイルに対してどの機能を許可するか • どの SQL ステートメントを許可するか • データベース・サーバー・オブジェクトに関するどの情報を検索するか • どの SQL カタログ機能を許可するか	なし
QSYSMSG 中断処理プログラム	QSYSMSG メッセージ待ち行列をモニターするプログラムを作成し、メッセージのタイプに応じて適切な処置を取ることができます (たとえば、機密保護管理者に知らせる)。	An Implementation Guide for iSeries Security and Auditing (GG24–4200)

表 116. サンプル出口プログラムのソース (続き)

出口プログラムのタイプ	目的	例の入手先
TCP/IP	いくつかの TCP/IP サーバー (たとえば、FTP、TFTP、TELNET、REXEC など) には出口点が設けられています。出口プログラムを追加して、ログオンを処理したり、ユーザー要求 (たとえば、特定のファイルの読み取りや書き込み) を妥当性検査したりできます。これらの出口を使用して、システムに匿名の FTP を与えることもできます。	「iSeries System API Reference」の『TCP/IP User Exits』
ユーザー・プロファイルの変更	以下のユーザー・プロファイル・コマンドのための出口プログラムを作成することができます。CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• iSeries 機密保護解説書 (SD88-5027-07) • 「iSeries System API Reference」の『TCP/IP User Exits』

保守ツール・ユーザー ID の管理

この項では、DST、SST、および iSeries ナビゲーターを使用して、保守ツール・ユーザー ID を管理する方法を説明します。

サーバーの構成、管理、サービス提供には、保守ツールを使用します。保守ツールには、専用保守ツール (DST) やシステム保守ツール (SST) からアクセスできます。 DST、SST にアクセスして、論理区画 (LPAR) 管理およびディスク装置管理に iSeries ナビゲーター機能を使用するには、保守ツールのユーザー ID が必要です。 DST は、i5/OS がロードされていない場合でも、ライセンス内部コードが起動されていれば、使用できます。 SST は、i5/OS から利用できます。 次の表に、DST と SST の基本的な違いをまとめます。

特性	DST	SST
アクセス方法	手動 IPL 時に表示されるコンソールの使用、または制御パネルのオプション 21 の選択による物理的なアクセス。	QSRV または次の権限を使用してサインオンする機能を持つ対話式ジョブによるアクセス。 • STRSST (システム保守ツール開始) CL コマンドに対する権限 • サービス特殊権限 (*SERVICE) または全オブジェクト特殊権限 (*ALLOBJ) • SST を使用するための機能特権
使用できる場合	サーバーの機能が制限されている場合でも使用可能。 DST にアクセスするのに i5/OS は必要ない。	i5/OS が起動されている場合に使用可能。 SST にアクセスするのに i5/OS が必要。
認証方法	保守ツールのユーザー ID とパスワードが必要。	保守ツールのユーザー ID とパスワードが必要。

保守ツールを使用して以下のタスクを実行する方法については、「**iSeries Information Center**」 → 「**セキュリティー**」 → 「**保守**ツール」を参照してください。

- DST からの保守ツールへのアクセス
- SST からの保守ツールへのアクセス
- iSeries ナビゲーターからの保守ツールへのアクセス
- DST の使用による保守ツール・ユーザー ID の作成
- DST の使用による保守ツール・ユーザー ID の機能特権の変更
- DST の使用による保守ツール・ユーザー ID の記述の変更
- DST の使用による保守ツール・ユーザー ID の表示
- DST の使用による保守ツール・ユーザーを使用可能にする
- DST の使用による保守ツール・ユーザーを使用不可にする
- DST の使用による保守ツール・ユーザー ID の削除
- SST または DST の使用による保守ツール・ユーザー ID とパスワードの変更
- STRSST または QSYCHGDS の使用による保守ツール・ユーザー ID とパスワードの変更
- QSECOFR ユーザー・プロファイル・パスワードのリセットまたは回復
- QSECOFR 保守ツール・ユーザー ID とパスワードのリセット
- 保守ツール・セキュリティー・データの保管および復元
- DST の保守ツール・サーバーの構成
- i5/OS の保守ツール・サーバーの構成
- DST によるサービス機能使用のモニター
- i5/OS セキュリティー監査ログによる保守ツール使用のモニター

コンピューター・ウィルスに対する保護

この項では、コンピューター・ウィルスおよび疑わしいプログラムから保護するためのヒントを提供します。

最近のコンピューター使用の傾向として、信頼の置けないソースからのプログラムや、不明な機能を実行するプログラムがシステムに含まれるようなケースが増えてきています。次に、いくつかの例を示します。

- パーソナル・コンピューターのユーザーが、他の PC ユーザーからプログラムを入手することがあります。この PC がシステムに接続されている場合は、そのプログラムがサーバーに影響を与える可能性があります。
- ネットワークに接続されたユーザーも、たとえば、電子掲示板からプログラムを入手することができます。
- ハッカーが、ますます活動的になり注目を集めるようになってきています。ハッカーは、しばしば、自分たちの方式とその結果を公開します。このため、普段は良心的なプログラマーでもこれを模倣する可能性があります。

このような傾向により、**コンピューター・ウィルス**と呼ばれるコンピューター・セキュリティー上の問題が生じました。ウィルスとは、ウィルス自体のコピーを含むように他のプログラムを変更することができるプログラムをいいます。このため、他のプログラムはウィルスに感染したと言われます。さらにウィルスは、システム資源を消費したり、データを破壊したりするような他の操作も行うことがあります。

サーバーのアーキテクチャーは、コンピューター・ウィルスの感染特性に対し、ある程度の保護策を備えています。『コンピューター・ウィルスに対する保護』は、この点について取り上げています。サーバーの機密保護管理者は、無許可機能を実行するプログラムについてもっと関心を持つ必要があります。この章の他

のトピックとしては、悪意を持った人物がどのようにして有害プログラムをセットアップして、システムでそれを実行するかについて説明します。このトピックでは、プログラムが無許可機能を実行しないようにするためのヒントを示しています。

ヒント: オブジェクト権限は、常に、第 1 防護線です。オブジェクトを保護するための適切な計画を持っていないと、システムは無防備になります。この章では、許可ユーザーがどのようにして、オブジェクト権限体系の中の抜け穴を利用しようとするかについて説明します。

ウィルスに感染したコンピューターは、他のプログラムを変更できるプログラムを含んでいます。このシステムのオブジェクト・ベースのアーキテクチャーは、他のコンピューター・アーキテクチャーの場合と比べ、いたずらを企てる者がこのようなウィルスを生成したり、まん延させたりするのをより困難にしています。このシステムでは、特定のコマンドや命令を使用して各タイプのオブジェクトを処理します。ファイル命令を使用して、操作可能プログラム・オブジェクトを変更することはできません (多くのウィルス作成者たちがファイル命令を使用して変更を行います)。また、他のプログラム・オブジェクトを変更するプログラムも簡単には作成できません。これを行うには、多くの時間や人手、熟練が必要であり、また、一般には入手できないツールや文書にアクセスする必要があります。

しかし、サーバーの新しい機能がオープン・システム環境で使用できるようになるにつれて、サーバーのオブジェクト・ベースの保護機能のいくつかが適用されなくなりました。例えば、統合ファイル・システム (IFS) の場合、ユーザーはディレクトリーの中のいくつかのオブジェクト (ストリーム・ファイルなど) を直接処理することができます。

また、サーバーのアーキテクチャーにより、ウィルスがサーバーのプログラム間でまん延するのは難しくなりますが、このアーキテクチャーは、システムがウィルス保菌者になるのを防ぐわけではありません。ファイル・サーバーとしてのサーバーは、 多くの PC ユーザーが共用するプログラムを格納することができます。これらのプログラムのいずれにも、サーバーが検出しないウィルスが入っている可能性があります。このタイプのウィルスが、サーバーに接続されている PC に感染しないようにするには、 PC ウィルス・スキャン・ソフトウェアを使用する必要があります。サーバーには、ポインター機能を持つ低水準言語を使用して操作可能オブジェクト・プログラムを変更できないようにするいくつかの機能が用意されています。

- セキュリティー・レベル 40 以上でシステムが稼働しているときは、保全性保護はプログラム・オブジェクトを変更できないようにする保護機能に含まれます。たとえば、ブロックされた (保護された) 機械語命令を含むプログラムを正常に実行することはできません。
- 別のシステムに保管された (および、変更されたことも考えられる) プログラムを復元するときにも、プログラム妥当性検査値がユーザーを保護する目的で使用されます。「*iSeries 機密保護解説書*」の第 2 章では、プログラム妥当性検査値を始め、セキュリティー・レベル 40 以上の場合の保全性保護機能について説明しています。

注: プログラム妥当性検査値は絶対確実なものではなく、またシステムに復元されたプログラムを評価する際に不寝番を代行してくれるものでもありません。

以下のいくつかのツールも、更新されたプログラムがシステムに導入されるのを検出する際の助けになります。

- オブジェクト保全性検査 (CHKOBJITG) コマンドを使用すれば、検索値を満足するオブジェクト (操作可能オブジェクト) をスキャンして、それらのオブジェクトが更新されていないことを確認することができます。これはウィルス・スキャン機能と同じようなものです。また CHKOBJITG コマンドを使用して、統合ファイル・システム・オブジェクトでスキャンを実行するよう要求することもできます。統合ファイル・システムのスキャンに関連した出口プログラムを使用してウィルスのスキャンを行うアプリケーションまたはビジネス・パートナーをユーザーが有している場合には、そうしたプログラムがウィルスのスキャンをトリガーします。

- セキュリティー監査機能を使用すれば、変更または復元されたプログラムをモニターすることができます。権限レベル・システム値としての *PGMFAIL、 *SAVRST、および *SECURITY 値は、監査レコードを提供します。監査レコードは、ウィルス・タイプのプログラムをシステムに導入しようとしているのを検出する際に役立ちます。「*機密保護解説書*」の第 9 章および付録 F では、監査値と監査ジャーナル項目が詳しく説明されています。
- プログラム変更 (CHGPGM) コマンドの強制作成 (FRCCRT) パラメーターを使用すれば、システムに復元された任意のプログラムを再作成することができます。システムは、プログラムの再作成にプログラム・テンプレートを使用します。プログラム・オブジェクトがコンパイルされた後に変更された場合は、システムは変更されたオブジェクトを再作成し、それを置き換えます。ブロックされた (保護されている) 命令がプログラム・テンプレートに含まれていると、プログラムは正しく再作成されません。
- プログラムをシステムに復元したときに再作成するには、QFRCCVNRST (復元時に強制変換) システム値を使用します。システムは、プログラムの再作成にプログラム・テンプレートを使用します。このシステム値は、再作成するプログラムについて複数の選択肢を提供します。
- QVFYOBJRST (オブジェクト復元検査) システム値を使用して、ディジタル署名を持っていないか、あるいはディジタル署名が無効なプログラムを復元しないようにすることができます。ディジタル署名が無効な場合とは、プログラムが、開発者によって署名された後に変更されていることを意味します。所有するプログラム、保管ファイルおよびストリーム・ファイルに署名することができる API があります。

「共通認可オブジェクトの印刷」(PRTPUBAUT) コマンドの使用

ここでは、「共通認可オブジェクトの印刷」(PRTPUBAUT) コマンドの使用方法を説明します。それがなぜ重要か、および段階的な手順を示します。

「共通認可オブジェクトの印刷」(PRTPUBAUT) コマンドを使用すれば、*EXCLUDE 共通権限を持っていない指定されたオブジェクトの報告書を印刷することができます。*PGM オブジェクトの場合、ユーザーが呼び出すことのできる *EXCLUDE 共通権限を持っていないプログラムだけが報告書に含まれます (このプログラムはユーザー・ドメインであるか、システム・セキュリティー・レベル (QSECURITY システム値) が 30 以下)。このようにして、システム上のすべてのユーザーがアクセス権限を持つオブジェクトを確認することができます。

このコマンドは 2 つの報告書を印刷します。最初の報告書 (完全報告書) には、 *EXCLUDE の共通認可を持っていないすべての指定オブジェクトが含まれます。2 番目の報告書 (変更報告書) には、以前に PRTPUBAUT コマンドが実行されたときに *EXCLUDE 共通権限を持っていた (または存在しなかった) ものの、現在は *EXCLUDE 共通権限を持っていないオブジェクトが含まれます。指定したオブジェクトとライブラリー、フォルダー、またはディレクトリーに対して、以前に PRTPUBAUT コマンドが実行されなかった場合は、「変更報告書」は作成されません。以前にこのコマンドが実行されたものの、*EXCLUDE 共通権限を持つオブジェクトが他に存在しない場合には、「変更報告書」は印刷されますが、オブジェクトはリストされません。

制約事項: このコマンドを使用するには、*ALLOBJ 特殊権限を持っていなければなりません。

例: 次のコマンドは、共通認可 *EXCLUDE を持たない GARRY ライブラリー内のすべてのファイル・オブジェクトについて、完全報告書、および変更報告書を作成します。

```
PRTPUBAUT OBJTYPE(*FILE) LIB(GARRY)
```

次のコマンドは、共通認可 *EXCLUDE を持たない GARRY ディレクトリーから開始するサブディレクトリー構造内のすべてのストリーム・ファイル・オブジェクトについて、完全報告書、変更報告書、および削除報告書を作成します。

```
PRTPUBAUT OBJTYPE(*STMF) DIR(GARRY) SCHSUBDIR(*YES)
```

「私用認可の印刷」(PRTPVTAUT) コマンドの使用

ここでは、「私用認可の印刷」(PRTPVTAUT) コマンドの使用方法を説明します。それがなぜ重要か、および段階的な手順を示します。

私用権限の印刷 (PRTPVTAUT) コマンドを使用すれば、指定されたライブラリー、フォルダー、またはディレクトリーに含まれる指定されたタイプのオブジェクトに関するすべての私用権限報告書を印刷することができます。この報告書には、指定されたタイプのすべてのオブジェクトと、このオブジェクトに対する権限を持っているユーザーがリストされます。このようにして、オブジェクトに対する権限のさまざまなソースを確認することができます。

このコマンドは、選択されたオブジェクトに関して 3 つの報告書を印刷します。最初の報告書 (完全報告書) には、選択された各オブジェクトに関するすべての私用権限が含まれます。2 番目の報告書 (変更報告書) には、指定されたライブラリー、フォルダー、またはディレクトリー内の指定されたオブジェクトに関して PRTPVTAUT コマンドが以前に実行された場合、選択されたオブジェクトに対する私用権限の追加や変更内容が格納されます。選択されたタイプのすべての新規オブジェクト、既存のオブジェクトに対する新規の権限、または既存のオブジェクトに対する既存の権限の変更内容が、「変更報告書」にリストされます。指定されたライブラリー、フォルダー、またはディレクトリー内の指定されたオブジェクトに対して、以前に PRTPVTAUT コマンドが実行されなかった場合は、「変更報告書」は作成されません。以前にこのコマンドが実行されたものの、オブジェクトの権限が変更されていない場合は、「変更報告書」は印刷されますが、オブジェクトはリストされません。

3 番目の報告書 (削除報告書) には、以前に PRTPVTAUT コマンドが実行された後に、指定オブジェクトから削除されたすべての私用認可ユーザーが含まれています。削除されたすべてのオブジェクトや除去されたすべての私用認可ユーザーが、「削除報告書」にリストされます。以前に PRTPVTAUT コマンドが実行されなかった場合は、「削除報告書」は作成されません。以前にこのコマンドが実行されたものの、オブジェクトに対する削除操作が行われなかった場合は、「削除報告書」は印刷されますが、オブジェクトはリストされません。

制約事項: このコマンドを使用するには、*ALLOBJ 特殊権限を持っていなければなりません。

例: 次のコマンドは、PAYROLLLIB 内のすべてのファイル・オブジェクトについて、完全報告書、変更報告書、および削除報告書を作成します。

```
PRTPVTAUT OBJTYPE(*FILE) LIB(PAYROLLLIB)
```

次のコマンドは、GARRY ディレクトリー内のすべてのストリーム・ファイル・オブジェクトについて、完全報告書、変更報告書、および削除報告書を作成します。

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*NO)
```

次のコマンドは、GARRY ディレクトリーから開始するサブディレクトリー構造内のすべてのストリーム・ファイル・オブジェクトについて、完全報告書、変更報告書、および削除報告書を作成します。

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*YES)
```

ユーザー・プロファイル報告書

以下のコマンドは、ユーザー・プロファイル報告書を提供します。

- ユーザー・プロファイル印刷 (PRTUSRPRF)

このコマンドを使用すると、システム上のユーザー・プロファイルの情報を記載する報告書を印刷することができます。4 種類の報告書の印刷が可能です。これらは、権限タイプ情報を記載する報告書、環境タイプ情報を記載する報告書、パスワード・タイプ情報を記載する報告書、パスワード・レベルのタイプ情報を記載する報告書です。

- デフォルト・パスワード分析 (ANZDFTPWD)

  このコマンドを使用すると、デフォルト・パスワードを持つシステム上のすべてのユーザー・プロファイルに関する報告書を印刷し、それらのプロファイルに対する処置を取ることができます。ユーザー・プロファイル名がプロファイルのパスワードと一致する場合には、プロファイルにデフォルトのパスワードが存在します。デフォルトのパスワードを持つシステム上のユーザー・プロファイルを使用禁止にして、そのパスワードを満了に設定することができます。

システム・セキュリティー属性印刷コマンド (PRTSYSSECA) の使用

目的

この例は、システム機密保護属性印刷 (PRTSYSSECA) コマンドの出力です。 報告書には、通常のセキュリティー要件をもつシステム に推奨されるセキュリティー関連システム値およびネットワーク属性の設定が示されます。 また、システムにおける現行の設定値も示されます。

注: 報告書の現在の値列は、システムにおける現行の設定値を示しています。この値を推奨値と比較して、機密漏れの箇所がないか調べてください。

システム機密保護属性報告書の例

システム機密保護属性

システム値 名	現在の値	推奨値
QALWOBJRST	*ALL	*NONE
QALWUSRDMN	*ALL	QTEMP
QATNPGM	QEZMAIN QSYS	*NONE
QAUDENDACN	*NOTIFY	*NOTIFY
QAUDFRCLVL	*SYS	*SYS
QAUDCTL	*AUDLVL	*AUDLVL *OBJAUD *NOQTEMP
QAUDLVL	*SECURITY	*AUTFAIL *CREATE *DELETE *SECURITY *SAVRST
QAUTOCFG	0	0
QAUTORMT	1	0
QAUTOVRT	9999	0
QCMNRCYLMT	0 0	0 0
QCRTAUT	*CHANGE	ライブラリー・レベルで制御。
QCRTOBJAUD	*NONE	ライブラリー・レベルで制御。
QDEVRCYACN	*DSCMSG	*DSCMSG
QDSCJOBITV	120	120
QDSPSGNINF	1	1
QINACTITV	60	60
QINACTMSGQ	*ENDJOB	*ENDJOB
QLMTDEVSSN	0	1
QLMTSECOFR	0	1
QMAXSGNACN	2	3
QMAXSIGN	3	3
QPWDEXPITV	60	60
QPWDLMTAJC	1	1
QPWDLMTCHR	*NONE	AEIOU@$#
QPWDLMTREP	1	1
QPWDLVL	0	
QPWDMAXLEN	8	8

```
QPWDMINLEN      6                    6
QPWDPOSDIF      1                    1
QPWDRQDDGT      1                    1
QPWDRQDDIF      0                    1
QPWDVLDPGM      *NONE                *NONE
QRETSVRSEC      0                    0
QRMTIPL         0                    0
QRMTSIGN        *FRCSIGNON           *FRCSIGNON
QSECURITY       50                   50
QSHRMEMCTL      1                    0
QSRVDMP         *DMPUSRJOB           *NONE
QUSEADPAUT      *NONE                CRTAUTL  AUTL(QUSEADPAUT) AUT(*EXCLUDE)
                                     CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL) NEWOWN(QSYS)
                                     CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)
QVFYOBJRST      1                    3
ネットワーク
   属性名          現在の値              推奨値
 DDMACC           *OBJAUT              *REJECT
 JOBACN           *FILE                *REJECT
 PCSACC           *OBJAUT              *REJECT
```

セキュリティーのモニター

このトピックのセットでは、システムにおけるセキュリティーのモニターおよび監査に関する多様な技法について取り上げます。

セキュリティー監査では、データ・セキュリティーおよびデータ正確性に関する手順の妥当性と有効性を検査して、データ処理システムの活動を検討し、かつ検査します。**セキュリティー監査ジャーナル**は、システムの情報を監査するための主な情報源です。組織内外のセキュリティー監査員は、システムの提供する監査機能を使用して、システムで発生するセキュリティー関連事象についての情報を収集できます。

侵入検知システムは、ネットワークやホスト・システムの一部であるモニター対象のリソースで侵入が試みられたり実際に侵入したことを検出するソフトウェアです。

セキュリティーを定期的に監視する基本的な目的は、通常は次の 2 つです。

- 企業の資源を十分に保護する。
- システムや企業の情報に許可なくアクセスしようとすることを検出する。

この一連のトピックでは、システム・セキュリティーの監査とモニターに関する作業について取り上げます。

セキュリティー監査の計画

この情報を使用して、ご使用のシステムのセキュリティー監査の計画を立てます。

セキュリティーの監視の際、オペレーティング・システムは、システムで発生するセキュリティー・イベントを記録することができます。これらのイベントは、ジャーナル・レシーバーと呼ばれる特殊なシステム・オブジェクトに記録されます。システム値やユーザー・プロファイルの変更、オブジェクトへのアクセス試行の失敗など、さまざまなセキュリティー・イベントを記録するようにジャーナル・レシーバーを設定できます。以下の値は、どんなイベントが記録されるかを制御します。

- 監査制御 (QAUDCTL) システム値
- 監査レベル (QAUDLVL) システム値
- ユーザー・プロファイルの監査レベル (AUDLVL)
- ユーザー・プロファイルおよびオブジェクトのオブジェクト監査 (OBJAUD) 値

監査ジャーナルの情報は、次の目的で使用されます。

- 試行されたセキュリティー違反の検出。
- より高いセキュリティー・レベルへの移行の計画。
- 機密ファイルなどの機密オブジェクトの使用の監視。

監査ジャーナルの情報をさまざまな方法で表示するために、いくつかのコマンドを使用できます。

監査の目的は、システムのセキュリティーを危険にさらす可能性のある活動を検出してログに記録することです。システムで生じる処置をログに記録することを選択すると、パフォーマンスのトレードオフを経験することもあり、場合によってはディスク・スペースが消失するかもしれません。システム上のセキュリティー関連のイベントをログに記録することに決めた場合、eServer Security Planner は実行すべき監査のレベルに関する推奨事項を提供します。

システム上でのセキュリティー監査の使用を計画するには、以下のステップを行います。

- eServer Security Planner を使用して、システム構成とユーザー要件に基づいて、実行すべき監査のレベルに関する推奨事項を見極めます。
- すべてのシステム・ユーザーに対し、どのセキュリティーに関する事象を記録するかを決定します。セキュリティーに関連した事象の監査は、**処置監査**と 呼ばれます。
- 特定のユーザーに、追加の監査が必要かどうかを検査します。
- システム上での特定のオブジェクトの使用を監査するかどうかを決定します。
- オブジェクト監査を、すべてのユーザーに使用するか、それとも特定のユーザーに使用するかを決定します。

セキュリティー監査ジャーナルは、システムの情報を監査するための主な情報源です。組織内外のセキュリティー監査員は、システムの提供する監査機能を使用して、システムで発生するセキュリティー関連事象についての情報を収集できます。システム値、ユーザー・プロファイル・パラメーター、およびオブジェクト・パラメーターを使用して監査を定義します。

セキュリティー監査機能はオプションです。セキュリティー監査を設定するには、特定のステップをとる必要があります。

システムでは、監査を以下の 3 つのレベルで定義できます。

- すべてのユーザーを対象としたシステム全体の監査
- 特定のオブジェクトを対象とした監査
- 特定のユーザーを対象とした監査

監査の対象となるセキュリティーに関する事象が生じた場合、システムは、その事象を監査の対象として選択したかどうか検査します。選択してある場合、システムは、セキュリティー監査ジャーナル用の現行のレシーバーに、ジャーナル項目を書き込みます (ライブラリー QSYS の QAUDJRN)。

処置の監査およびオブジェクト・アクセスの監査の計画に関する情報は、「iSeries 機密保護解説書」の第 9 章を参照してください。

関連概念

22 ページの『セキュリティー監査』
このトピックでは、セキュリティー監査の目的について取り上げます。

セキュリティー監査のためのチェックリスト

このチェックリストを使用して、システム・セキュリティーを計画および監査してください。

セキュリティーを計画する際、ユーザーのセキュリティー要件を満たす項目をリストから選択してください。システムのセキュリティーを監査するには、リストを参照することにより、実施中の管理を評価して追加の管理が必要かどうかを判断してください。リストには、各項目の管理方法と、管理されているかどうかの監視方法が簡単に説明されています。

表 117. セキュリティー監査の計画用紙

セキュリティー監査の計画用紙	
作成者:	日付:
物理的セキュリティーの監視	
バックアップ媒体は損傷および盗難から保護されていますか ?	
さまざまな人が利用する場所にあるワークステーションのアクセスは制限されていますか。ワークステーションに対する *CHANGE 権限を持っているユーザーを確認するには、DSPOBJAUT コマンドを使用します。	
システム値の監視:	
システム値の設定が「システム値選択」用紙と一致するかどうか検査します。システム・セキュリティー属性印刷 (PRTSYSSECA) コマンドを使用してください。	
特に新しいアプリケーションの導入時には、決定済みのシステム値を再確認してください。変更されたシステム値がありませんか ?	
グループ・プロファイルの監視:	
グループ・プロファイルにパスワードがないことを検査します。すべてのグループ・プロファイルがパスワード *NONE を持っていることを検査するには、DSPAUTUSR コマンドを使用します。	
正しい人物がグループのメンバーになっていることを検査します。グループのメンバーをリストするには、*GRPMBR オプションを指定して DSPUSRPRF コマンドを使用します。	
DSPUSRPRF コマンドを使用して、各グループ・プロファイルの特殊権限を検査します。セキュリティー・レベル 30、40、または 50 で実行している場合は、グループ・プロファイルに *ALLOBJ 権限を与えないでください。	
ユーザー・プロファイルの監視:	
システム上のユーザー・プロファイルが次のカテゴリーのいずれかに属していることを検査します。 • 現在の従業員のユーザー・プロファイル • グループ・プロファイル • アプリケーションの所有者プロファイル • IBM 提供のプロファイル (Q で始まる)	
企業がユーザーを転勤させるか、またはユーザーが退職したときに、そのユーザー・プロファイルを除去します。ユーザーの退職と同時にプロファイルを自動的に削除または使用不可にするには、満了スケジュール項目変更 (CHGEXPSCDE) コマンドを使用します。	

表 117. セキュリティー監査の計画用紙 (続き)

セキュリティー監査の計画用紙	
非活動状態のプロファイルを探して、それらを除去します。一定時間にわたって非活動になっているプロファイルを自動的に使用不可にするには、プロファイル活動の分析 (ANZPRFACT) コマンドを使用します。	
ユーザー・プロファイル名と同じパスワードを持っているユーザーを判別します。デフォルト・パスワードの分析 (ANZDFTPWD) コマンドを使用します。このコマンドのオプションを使用して、次回ユーザーがシステムにサインオンするときに、パスワードを変更させます。 **重要:** IBM 提供のプロファイルをシステムから削除しないでください。IBM 提供のプロファイルは、Q の文字で始まります。	
*USER 以外のユーザー・クラスを持つ人物とその理由を識別します。すべてのユーザーとそのユーザー・クラス、およびその特殊権限のリストを入手するには、ユーザー・プロファイルの印刷 (PRTUSRPRF) コマンドを使用します。この情報を「システム責任」用紙と突き合わせます。	
どのユーザー・プロファイルの「制限機能」フィールドが *NO に設定されるかを制御します。	
重要なオブジェクトの監視:	
重要なオブジェクトにアクセスできる人物を確認します。オブジェクトを監視するには、私用権限の印刷 (PRTPVTAUT) コマンドと共通権限オブジェクトの印刷 (PRTPUBAUT) コマンドを使用します。グループがアクセスした場合は、DSPUSRPRF コマンドの *GRPMBR オプションを使用して、グループのメンバーを検査します。	
別のセキュリティー方式 (たとえば借用権限) を使ってオブジェクトへのアクセスを提供するアプリケーション・プログラムを使用できるのはどんな人物かを検査します。借用オブジェクトの印刷 (PRTADPOBJ) コマンドを使用します。	
無許可アクセスの監視:	
システム操作員に、QSYSOPR メッセージ待ち行列内のセキュリティー・メッセージに注意するように指示します。特に、サインオンに繰り返し失敗したケースがあれば、機密保護担当者に通知する必要があります。セキュリティー・メッセージは、2200 から 22FF、および 4A00 から 4AFF の範囲です。接頭部は、CPF、CPI、CPC、および CPD です。	
オブジェクトに対する無許可アクセスをログに記録するように、セキュリティー監査を設定します。	

セキュリティー監査チェックリストの詳しい使用方法については、「iSeries 機密保護解説書」の第 9 章を参照してください。

セキュリティー監査の設定

ここでは、セキュリティー監査を設定する方法について説明します。それがなぜ重要か、および段階的な手順を示します。システムは QAUDJRN ジャーナルの中にセキュリティー・イベントを収集します。

監査を設定するには、*AUDIT 特殊権限が必要です。セキュリティー監査を設定するには、以下のステップを実行してください。

1. ジャーナル・レシーバーの作成 (CRTJRNRCV) コマンドを使用して、選択したライブラリーの中にジャーナル・レシーバーを作成します。この例では、JRNLIB というライブラリーをジャーナル・レシーバー用に使用します。

   ```
   CRTJRNRCV  JRNRCV(JRNLIB/AUDRCV0001) +
              TEXT('Auditing Journal Receiver')
   ```

   - ジャーナル・レシーバーを、定期的に保管されるライブラリーの中に入れます。ジャーナルが QSYS ライブラリーに配置される場合でも、ジャーナル・レシーバーを QSYS ライブラリーには入れないでください。
   - 将来のジャーナル・レシーバーの命名規則を作成するために使用できる、(AUDRCV0001 などの) ジャーナル・レシーバー名を選択します。ジャーナル・レシーバーを変更して命名規則を続行する場合、*GEN オプションを使用することができます。この種の命名規則を使用すると、システムに導入先のジャーナル・レシーバーの変更を管理させる場合にも役立ちます。
   - 使用しているシステムのサイズと活動状態に応じたレシーバーしきい値を指定します。導入先システムのトランザクションの数、および監査用に選択する処置の数に基づいて、サイズの大きさを選択してください。システム変更 - ジャーナル管理サポートを使用する場合、ジャーナル・レシーバーしきい値を少なくとも 100 000 KB にしなければなりません。
   - ジャーナルに保管される情報へのアクセスを制限するために、AUT パラメーターに *EXCLUDE を指定します。
2. ジャーナル作成 (CRTJRN) コマンドを使って、 QSYS/QAUDJRN ジャーナルを作成します。

   ```
   CRTJRN  JRN(QSYS/QAUDJRN) +
                 JRNRCV(JRNLIB/AUDRCV0001) +
                 MNGRCV(*SYSTEM) DLTRCV(*NO) +
         AUT(*EXCLUDE) TEXT('Auditing Journal')
   ```

   - 名前 QSYS/QAUDJRN の使用は*必須*です。
   - 前のステップで作成したジャーナル・レシーバーの名前を指定してください。
   - ジャーナルに保管される情報へのアクセスを制限するために、AUT パラメーターに *EXCLUDE を指定します。ジャーナルを作成するには、オブジェクトを QSYS に追加する権限が必要です。
   - レシーバー管理 (MNGRCV) パラメーターを使用します。こうすれば、接続したレシーバーが、ジャーナル・レシーバー作成時に指定されたしきい値を超えた場合に、システムがジャーナル・レシーバーを変更して新しいジャーナル・レシーバーを接続します。このオプションを選択すると、CHGJRN コマンドを使って手動でレシーバーを切断し、それから新しいレシーバーを作成および接続するという手間が省けます。
   - システムに、切断されたレシーバーを削除させないでください。そのためには、DLTRCV(*NO) を指定します。これはデフォルト値です。 QAUDJRN レシーバーは、セキュリティー監査証跡です。これらをシステムから削除する前に、これらが適切に保存されているかどうか確認してください。
3. WRKSYSVAL コマンドを使用して、 監査レベル (QAUDLVL) システム値または監査レベル拡張 (QAUDLVL2) システム値を設定してください。 QAUDLVL および QAUDLVL2 システム値は、システム上のすべてのユーザーを対象とする監査ジャーナルにどんな処置が記録されるかを決定します。
4. 必要であれば、CHGUSRAUD コマンドを使用して、個別のユーザーに対する処置監査を設定してください。

5. 必要であれば、CHGOBJAUD および CHGDLOAUD コマンドを使用して、特定のオブジェクトに対するオブジェクト監査を設定してください。
6. 必要であれば、CHGUSRAUD コマンドを使用して、特定のユーザーに関するオブジェクト監査を設定してください。
7. システムが監査ジャーナルにアクセスできない場合の処置を制御するために、QAUDENDACN システム値を設定します。
8. QAUDFRCLVL システム値を設定して、監査レコードが補助記憶装置に書き込まれる頻度を制御してください。
9. QAUDCTL システム値を *NONE 以外の値に設定することにより、監査を開始してください。

注: QAUDCTL システム値を *NONE 以外の値に変更する前に、 QSYS/QAUDJRN ジャーナルが存在していなければなりません。監査を始動する際に、システムは監査ジャーナルへのレコードの書き込みを試行します。書き込みの試行が失敗した場合、メッセージを受け取り、監査は始動しません。

詳しくは、「iSeries 機密保護解説書」の以下のトピックを参照してください。
『処置の監査の計画』
『オブジェクト・アクセスの監査計画』
『監査終了処置』

セキュリティー監査ジャーナルの使用

セキュリティー監査ジャーナルは、システムの情報を監査するための主な情報源です。組織内外のセキュリティー監査員は、システムの提供する監査機能を使用して、システムで発生するセキュリティー関連事象についての情報を収集できます。

監査ジャーナルの情報は、次の目的で使用されます。

- 試行されたセキュリティー違反の検出。
- より高いセキュリティー・レベルへの移行の計画。
- 機密ファイルなどの機密オブジェクトの使用の監視。

監査ジャーナルの情報をさまざまな方法で表示するために、いくつかのコマンドを使用できます。システムでは、監査を以下の 3 つのレベルで定義できます。

- すべてのユーザーを対象としたシステム全体の監査
- 特定のオブジェクトを対象とした監査
- 特定のユーザーを対象とした監査

セキュリティーの監視の際、オペレーティング・システムは、システムで発生するセキュリティー・イベントを記録することができます。これらのイベントは、**ジャーナル・レシーバー**と呼ばれる特殊なシステム・オブジェクトに記録されます。システム値やユーザー・プロファイルの変更、オブジェクトへのアクセス試行の失敗など、さまざまなセキュリティー・イベントを記録するようにジャーナル・レシーバーを設定できます。以下の値は、どんなイベントが記録されるかを制御します。

- 監査制御 (QAUDCTL) システム値
- 監査レベル (QAUDLVL) システム値
- ユーザー・プロファイルの監査レベル (AUDLVL)
- ユーザー・プロファイルのオブジェクト監査 (OBJAUD)
- オブジェクトのオブジェクト監査 (OBJAUD)

監査ジャーナルとジャーナル・レシーバーの管理

監査ジャーナル QSYS/QAUDJRN は、セキュリティー監査専用です。オブジェクトを監査ジャーナルに記録すべきではありません。コミットメント制御で監査ジャーナルを使用すべきではありません。ジャーナル項目送信 (SNDJRNE) コマンドまたはジャーナル項目送信 (QJOSJRNE) API を使用して、このジャーナルにユーザー項目を送信しないでください。

システムが監査項目を監査ジャーナルに書き込めるようにするには、特別なロック保護を使用します。監査が活動状態である (QAUDCTL システム値が *NONE でない) 場合、 システム仲裁ジョブ (QSYSARB) は、QSYS/QAUDJRN ジャーナルに対するロックを保持します。監査が活動状態の場合、監査ジャーナルに対して次のような操作を実行することはできません。

- DLTJRN コマンド
- ENDJRN*xxx* コマンド
- APYJRNCHG コマンド
- RMVJRNCHG コマンド
- DMPOBJ または DMPSYSOBJ コマンド
- ジャーナルの移動
- ジャーナルの復元
- 権限を処理する操作、たとえば GRTOBJAUT コマンド
- WRKJRN コマンド

セキュリティー・ジャーナル項目に記録される情報は、「機密保護解説書」で説明されています。監査ジャーナルのすべてのセキュリティー項目には、T というジャーナル・コードが付いています。セキュリティー項目のほかに、ジャーナル QAUDJRN には、システム項目もあります。これらの項目にはジャーナル・コード J が付き、初期プログラム・ロード (IPL) およびジャーナル・レシーバーに対して実行される一般操作 (たとえばレシーバー保管) と関係があります。

ジャーナルまたはその現行レシーバーに損傷が生じたために監査項目をジャーナルできない場合、システムが取る処置は、QAUDENDACN システム値によって決定されます。損傷を受けたジャーナルまたはジャーナル・レシーバーの回復は、他のジャーナルの場合と同じです。

システムにジャーナル・レシーバーの変更を管理させることもできます。 QAUDJRN ジャーナルの作成時に MNGRCV(*SYSTEM) を指定するか、またはジャーナルをその値に変更します。 MNGRCV(*SYSTEM) を指定した場合、システムは、しきい値サイズに達すると自動的にレシーバーを切り離し、新規のジャーナル・レシーバーを作成して接続します。これを**システム変更 - ジャーナル管理**といいます。

オブジェクト権限の分析

この項では、オブジェクト権限の分析方法について取り上げ、ステップバイステップの指示を提供します。

以下の方法を使用して、システム上のライブラリーに権限を持つユーザーを決定します。

1. DSPOBJD コマンドを使用して、システム上のすべてのライブラリーをリストします。`DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)`
2. オブジェクト権限表示 (DSPOBJAUT) コマンドを使用して、特定のライブラリーへの権限をリストします。

   ```
   DSPOBJAUT OBJ(QSYS/library-name) OBJTYPE(*LIB) +
             ASPDEV(asp-device-name) OUTPUT(*PRINT)
   ```

3. ライブラリー表示 (DSPLIB) コマンドを使用して、ライブラリー内のオブジェクトをリストします。
   `DSPLIB LIB(QSYS/library-name) ASPDEV(asp-device-name) OUTPUT(*PRINT)`

これらの報告書を使用して、ライブラリー内にあるものと、ライブラリーへのアクセスを持つ人を決定します。必要であれば、DSPOBJAUT コマンドを使用して、ライブラリー内で選択されたオブジェクトについての権限を表示することができます。

権限を借用するプログラムの分析

この項では、権限を借用するプログラムを分析するステップバイステップの手順を説明します。

*ALLOBJ 特殊権限を持つユーザーの権限を借用するプログラムは、セキュリティー漏えい発生の原因になります。以下の方法で、これらのプログラムを検索および検査することができます。

1. *ALLOBJ 特殊権限を持っているそれぞれのユーザーごとに、借用プログラム表示 (DSPPGMADP) コマンドを使用して、ユーザーの権限を借用するプログラムをリストします。

   ```
   DSPPGMADP USRPRF(user-profile-name) +
                     OUTPUT(*PRINT)
   ```

2. DSPOBJAUT コマンドを使用して、各借用プログラムの使用を許可されるユーザーと、プログラムに対する共通権限を決定します。

   ```
   DSPOBJAUT OBJ(library-name/program-name) +
             OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
                     OUTPUT(*PRINT)
   ```

3. ソース・コードおよびプログラム記述を検査して、次のことを検査します。
   - 借用されているプロファイル下で実行中に、コマンド行の使用などの過剰な機能から、プログラムのユーザーが保護されているか。
   - 目的の機能に必要な最小限の権限レベルをプログラムが借用しているか。プログラムの障害を使用するアプリケーションは、オブジェクトとプログラムの所有者プロファイルと同じものを使用するように設計されています。プログラム所有者の権限が借用されている場合、ユーザーはアプリケーション・オブジェクトに対して *ALL 権限を持っています。多くの場合、所有者プロファイルに特殊権限は必要ありません。
4. DSPOBJD コマンドを使用して、プログラムが最後に変更されたのはいつであるかを検査します。

   ```
   DSPOBJD OBJ(library-name/program-name) +
           OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
                   DETAIL(*FULL)
   ```

ユーザー・プロファイルの分析

この項では、ユーザー・プロファイルの分析方法について取り上げ、ステップバイステップの指示を提供します。

システム上のすべてのユーザーの完全なリストを、認可ユーザー表示 (DSPAUTUSR) コマンドで表示または印刷することができます。リストは、プロファイル名またはグループ・プロファイル名の順序を示します。以下にグループ・プロファイルの順序を示します。

```
                              認可ユーザーの表示

                                    最終
グループ・    ユーザー・    変更      パスワード
プロファイル プロファイルパスワード なし     テキスト
 DSTSM
              ANDERSOR    0X/08/04           ROGER ANDERS
              VINCENTM    0X/09/15           MARK VINCENT
 DPTWH
              ANDERSOR    0X/08/04           ROGER ANDERS
              WAGNERR     0X/09/06           ROSE WAGNER
 QSECOFR
              JONESS      0X/09/20           JONES, SHARON
              HARRISON    0X/08/29           HARRISON, KEN
 *NO GROUP
              DPTSM       0X/09/05     X      販売営業
              DPTWH       0X/09/18     X      倉庫
              RICHARDS    0X/09/05           JANET RICHARDS
              SMITHJ      0X/09/18           JOHN SMITH
```

選択されたユーザー・プロファイルの印刷

ユーザー・プロファイル表示 (DSPUSRPRF) コマンドを使用して、出力ファイルを作成することができます。この出力ファイルは、QUERY ツールを使用することにより処理できます。

```
DSPUSRPRF USRPRF(*ALL) +
                    TYPE(*BASIC) OUTPUT(*OUTFILE)
```

QUERY ツールを使用して、以下のような出力ファイルのさまざまな分析報告書を作成することができます。

- *ALLOBJ および *SPLCTL 特殊権限の両方を持つすべてのユーザーのリスト。
- 初期プログラムまたはユーザー・クラスのような、ユーザー・プロファイルによって順序付けされたすべてのユーザーのリスト。

照会プログラムを作成して、ユーザーの出力ファイルから別の報告書を作成することができます。たとえば、以下のようにすることができます。

- フィールド UPSPAU が *NONE でないレコードを選択して、特殊権限を持つすべてのユーザー・プロファイルをリストする。
- Limit capabilities フィールド (モデル・データベース出力ファイル では UPLTCP と呼ばれている) が *NO または *PARTIAL であるレコードを選択して、コマンドの入力を許可されているすべてのユーザーをリストする。
- 特定の初期メニューまたは初期プログラムを持つすべてのユーザーをリストする。
- サインオン・フィールドの最新の日付を見て、非活動のユーザーをリストする。
- レベル 0 または 1 のパスワード表示フィールド (モデル出力ファイルでは UPENPW と呼ばれる) が N になっているレコードを選択して、パスワード・レベル 0 および 1 で使用可能なパスワードを持っていないすべてのユーザーをリストする。
- レベル 2 または 3 のパスワード表示フィールド (モデル出力ファイルでは UPENPH と呼ばれる) が Y になっているレコードを選択して、パスワード・レベル 2 および 3 で使用可能なパスワードを持っているすべてのユーザーをリストする。

大規模なユーザー・プロファイルの検査

多数の権限を持つユーザー・プロファイルの大半がシステム中にランダムに散らばって表示される場合、セキュリティーの計画の欠如を表します。以下に大きいユーザー・プロファイルを発見する方法とそれらを評価する方法が示されています。

1. オブジェクト記述表示 (DSPOBJD) コマンドは、システム上のすべてのユーザー・プロファイルに関する情報が入っている出力ファイルを作成します。

   ```
   DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
                 DETAIL(*BASIC) OUTPUT(*OUTFILE)
   ```

2. 照会プログラムを作成し、サイズによる降順で各ユーザー・プロファイルの名前とサイズをリストします。
3. 最大のユーザー・プロファイルについての詳細な情報を印刷し、権限と所有されているオブジェクトを評価してそれらが適切かどうかを見ます。

   ```
   DSPUSRPRF USRPRF(user-profile-name) +
                       TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(user-profile-name) +
                       TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   IBM 提供のユーザー・プロファイルの中にはかなり大きいものがありますが、これはそれらが所有するオブジェクトの数によるものです。通常、これらをリストおよび分析する必要はありません。ただし、QSECOFR や QSYS のような、*ALLOBJ 特殊権限を持つ IBM 提供ユーザー・プロファイルの権限を借用するプログラムは検査する必要があります。

詳細については、「iSeries 機密保護解説書 の『IBM 提供のユーザー・プロファイル』を参照してください。

機密保護担当者の処置の監査

機密保護担当者または機密保護管理者には、 システムのセキュリティーについての責任があります。 機密保護担当者には、*ALLOBJ および *SECADM 特殊権限があります。

*ALLOBJ と *SECADM 特殊権限を持つユーザーが実行したすべての処置に関して、記録を取っておきたいと思うかもしれません。ユーザー・プロファイルの処置監査値を使用して、以下の作業を実行できます。

1. *ALLOBJ と *SECADM 特殊権限を持つ各ユーザーに対して、CHGUSRAUD コマンドを 使用して、AUDLVL がシステムの QAUDLVL または QAUDLVL2 システム値に含まれていないすべての値を持つように設定します。たとえば、QAUDLVL が、 *AUTFAIL、*PGMFAIL、*PRTDTA、および *SECURITY に設定されている場合、このコマンドを使用して、機密保護担当者ユーザー・プロファイルに対し、 AUDLVL を設定します。

   ```
   CHGUSRAUD USER((SECUSER) +
            AUDLVL(*CMD *CREATE *DELETE +
                   *OBJMGT *OFCSRV *PGMADP +
                   *SAVRST *SERVICE, +
                   *SPLFDTA *SYSMGT)
   ```

2. *ALLOBJ および *SECADM 特殊権限を持つユーザー・プロファイルから、*AUDIT 特殊権限を除去します。これにより、これらのユーザーが自分のプロファイルの監査特性を変更できなくなります。

   注: QSECOFR プロファイルから、特殊権限を除去することはできません。そのため、QSECOFR としてサインオンしたユーザーが、そのプロファイルの監査特性を変更するのを防止することはできません。しかし、QSECOFR としてサインオンしたユーザーが、CHGUSRAUD コマンドを 使用して監査特性を変更している場合、AD 項目タイプが、監査ジャーナルに書き込まれます。

推奨事項: 機密保護担当者 (*ALLOBJ または *SECADM 特殊権限を持つユーザー) が、より良い監査を行うために、自分のプロファイルを使用してください。QSECOFR プロファイルのパスワードは、分散されるべきではありません。

3. *AUDLVL が確実に QAUDCTL システム値に含まれているようにしてください。
4. 監査ジャーナルの項目を見直すには DSPJRN コマンドを使用してください。

詳しくは、「iSeries 機密保護解説書」の『照会またはプログラムでの監査ジャーナル項目の分析』を参照してください。

関連概念

25 ページの『特殊権限』
このトピックでは、ユーザーに対して指定できる特殊権限を説明します。

機密漏れの防止と検出

以下の情報には、発生する可能性のある機密漏れを検出するときに役立つ、いろいろなヒントが示されています。

更新されたオブジェクトの検査

この項では、オブジェクト保全性検査 (CHKOBJITG) コマンドを使用して、更新されたオブジェクトを探す方法について説明します。

オブジェクトが更新されている場合は、通常、誰かがシステムに損傷を与えようとしていることを示しています。以下のようなことが行われた後に、このコマンドを実行してください。

- システムにプログラムが復元された
- 専用保守ツール (DST) が使用された

このコマンドを実行すると、システムは、発生する可能性のある保全性問題の情報が入ったデータベース・ファイルを作成します。1 つのプロファイル、複数の異なるプロファイルによって所有されるオブジェクト、パス名と一致するオブジェクト、またはシステム上のすべてのオブジェクトを検査できます。ドメインが変更されたオブジェクトおよび損傷したオブジェクトを検索することができます。さらに、プログラム妥当性検査値を計算し直して、変更された *PGM、*SRVPGM、*MODULE、および *SQLPKG タイプのオブジェクトを検出することができます。ユーザーは、ディジタル署名できるオブジェクトの署名を検査できます。ライブラリーおよびコマンドが改ざんされたかどうかを検査することができます。統合ファイル・システムのスキャンを開始したり、オブジェクトが以前のファイル・システムのスキャンに失敗したかどうかを検査することもできます。

また、タイプが *PGM、*SRVPGM、*MODULE、および *SQLPKG である更新されたオブジェクトを探すために、プログラム妥当性検査値を再計算することもできます。 CHKOBJITG プログラムを実行するには、*AUDIT 特殊権限が必要です。このコマンドは、スキャンや計算を行うため、長時間かかることがあります。これを実行するのは、システム活動がビジー状態でないときにしてください。

重要: パフォーマンスまたはシステム操作上のインパクトを抑えるために、オブジェクトの所有権を複数のプロファイルに分散させてください。すべての (または、ほとんどすべての) オブジェクトを 1 つの所有者プロファイルのみに割り当てないでください。

登録済み出口プログラムの評価

システム登録機能を使用すれば、 特定のイベントが発生したときに実行する必要のある出口プログラムを登録することができます。 システムの登録情報をリストするには、WRKREGINF OUTPUT(*PRINT) を入力します。

システムの各出口点ごとに、報告書は現在登録されている出口プログラムがあるかを示します。現在登録されているプログラムが出口点に含まれている場合は、 WRKREGINF の表示バージョンからオプション 8 (表示プログラム) を選択して、次のようなプログラムに関する情報を表示することができます。他の出口プログラムやトリガー・プログラムに使用するこれらの出口プログラムの評価には、同じ方式を使用してください。

スケジュールされたプログラムの検査

スケジュールされたプログラムすべてが正規のものであることを確認します。

サーバーでは、ジョブ・スケジューラーのような、後で実行するジョブをスケジュールするための方法がいくつか用意されています。通常、これらの方式にはセキュリティーに関する問題はありません。なぜならば、ジョブをスケジュールするユーザーは、ジョブのバッチ処理を投入するために必要な権限と同じ権限を持っていなければならないからです。ただし、スケジュールされたジョブについては定期的に検査する必要があります。部門から転出した、不満をいだくユーザーが、この方式を使用して障害を起こす可能性があります。

保護ライブラリー内のユーザー・オブジェクトの検査

オブジェクト権限を使用して、誰が保護されたライブラリーにプログラムを追加できるかを制御することができます。プログラム以外のユーザー・オブジェクトは、システム・ライブラリーに入っているときは、機密漏れの問題を提示することがあります。

すべてのサーバーのジョブはライブラリー・リストを持っています。ライブラリー・リストは、ライブラリー名がオブジェクト名と一緒に指定されていない場合に、システムがオブジェクトを探索する順序を決定します。たとえば、プログラムの所在を指定しないでそのプログラムを呼び出すと、システムは、順番にライブラリー・リストを探し、最初に見つけたプログラムのコピーを実行します。

「*iSeries 機密保護解説書*」では、ライブラリー・リストの機密漏れの問題、およびライブラリー名を指定しないでプログラムを呼び出すこと (未修飾呼び出しと呼ばれる) について詳しく説明しています。この資料には、ライブラリー・リストの内容や、システム・ライブラリー・リストの変更機能の制御に関する推奨事項も示されています。

システムを正しく実行するには、QSYS や QGPL など、特定のシステム・ライブラリーが、すべてのジョブに関するライブラリー・リストに入っていなければなりません。オブジェクト権限を使用すれば、誰がプログラムをこれらのライブラリーに追加できるかを制御することができます。これを行えば、後でライブラリー・リストのライブラリーに現れるプログラムと同じ名前を持つこれらのいずれかのライブラリーに、誰かが有害なプログラムを入れるのを防止するのに役立ちます。

また、誰が CHGSYSLIBL コマンドに対する権限を持っているかを評価し、セキュリティー監査ジャーナルの SV レコードをモニターすることもできます。悪賢いユーザーは、ライブラリーをライブラリー・リストの QSYS の前に入れ、 IBM 提供のコマンドと同じ名前を持つ無許可コマンドを他のユーザーに実行させたりします。

ユーザー・オブジェクト印刷 (PRTUSROBJ) コマンドを実行するには、SECBATCH メニュー・オプション 28 (即時に投入) または 67(ジョブ・スケジューラーを使用) を使用します。PRTUSROBJ コマンドは、指定のライブラリー内にある (IBM が作成したものではない) ユーザー・オブジェクトのリストを印刷します。次に、リストのプログラムを評価して、誰がそれを作成したか、それはどのような機能を実行するかを判別することができます。

プログラム以外のユーザー・オブジェクトも、システム・ライブラリーに入っているときは、機密漏れの問題を提示することがあります。たとえば、プログラムが、未修飾の名前を持つファイルに機密データを書き込んだ場合は、そのプログラムは、システム・ライブラリー内のそのファイルの間違ったバージョンをオープンさせられることがあります。

借用権限の使用の制限

プログラムを実行すると、このプログラムは借用権限を使用して、 次のような 2 つの異なる方法でオブジェクトにアクセスすることができます。

- このプログラム自体がその所有者の権限を借用することができます。この指定は、このプログラムまたはサービス・プログラムのユーザー・プロファイル (USRPRF) パラメーターで行います。
- このプログラムは、まだジョブの呼び出しスタックに入っている前のプログラムの借用権限を使用 (継承) します。プログラムは、それ自体が権限を借用しなくても、前のプログラムの借用権限を継承することができます。プログラムまたはサービス・プログラムの借用権限使用 (USEADPAUT) パラメーターは、そのプログラムがプログラム・スタック内の前のプログラムの借用権限を継承するかどうかを制御します。

異常な削除のモニター

私用権限の印刷 (PRTPVTAUT) コマンドを使用すれば、指定されたライブラリー、フォルダー、またはディレクトリーに含まれる指定されたタイプのオブジェクトに関するすべての私用権限報告書を印刷することができます。

この報告書には、指定されたタイプのすべてのオブジェクトと、このオブジェクトに対する権限を持っているユーザーがリストされます。このようにして、オブジェクトに対する権限のさまざまなソースを確認することができます。このコマンドは、選択されたオブジェクトに関して 3 つの報告書を印刷します。最初の報告書 (完全報告書) には、選択された各オブジェクトに関するすべての私用権限が含まれます。2 番目の報告書 (変更報告書) には、指定されたライブラリー、フォルダー、またはディレクトリー内の指定されたオブジェクトに関して PRTPVTAUT コマンドが以前に実行された場合、選択されたオブジェクトに対する私用権限の追加や変更内容が格納されます。選択されたタイプの任意の新規オブジェクト、既存のオブジェクトに対する新規の権限、または既存のオブジェクトに対する既存の権限に行った変更が、変更報告書にリストされています。指定ライブラリー、フォルダー、またはディレクトリーに含まれている指定オブジェクトに対して、前に PRTPVTAUT コマンドが実行されなかった場合は、変更報告書は作成されません。前にこのコマンドは実行されたが、オブジェクトの権限に対する変更が行われなかった場合は、変更報告書は印刷されますが、オブジェクトはリストされません。

3 番目の報告書 (削除報告書) には、以前に PRTPVTAUT コマンドが実行された後に、指定オブジェクトから削除されたすべての私用認可ユーザーが含まれています。削除されたすべてのオブジェクトや私用権限ユーザーとして除去されたすべてのユーザーが、削除報告書にリストされています。前に PRTPVTAUT コマンドが実行されなかった場合は、削除報告書は作成されません。前にこのコマンドは実行されたが、オブジェクトに対する削除操作が行われなかった場合は、削除報告書は印刷されますが、オブジェクトはリストされません。

重要: このコマンドを使用するには、*ALLOBJ 特殊権限を持っていなければなりません。

異常なシステム使用のモニター

この項では、異常なシステム使用をモニターする作業と、それが重要な理由について取り上げ、段階的な手順を示します。

さらに、プロキシー・サーバーは、トラッキングの目的で、すべての URL 要求をログに記録することもできます。あとでこれらのログを調べれば、ネットワーク資源の使用および誤用をモニターすることができます。

悪質なアクセス試行のモニター

出力待ち行列とジョブ待ち行列へのアクセスのモニター

機密保護管理者は、ファイル・アクセスの保護という大きなジョブを行った後で、ファイルの内容を印刷するときに発生した状態について忘れてしまうことがあります。サーバーには、重要な出力待ち行列やジョブ待ち行列を保護するための機能が用意されています。出力待ち行列を保護することで、たとえば、無許可のユーザーが印刷待ちの機密スプール・ファイルを表示したりコピーしたりできないようにします。ジョブ待ち行列を保護することで、無許可のユーザーが機密ジョブを非機密出力待ち行列に宛先変更したり、ジョブ全体を取り消したりできないようにします。

SECBATCH メニュー・オプション

24 は即時に投入する 63 はジョブ・スケジューラーを使用する

Information Center の「基本システム・セキュリティーおよび計画」および「機密保護解説書」には、出力待ち行列とジョブ待ち行列を保護する方法が示されています。待ち行列権限印刷 (PRTQAUT) コマンドを使用して、システム上のジョブ待ち行列と出力待ち行列のセキュリティー設定を印刷することができます。その後で、機密情報を印刷する印刷ジョブを評価し、それらの印刷ジョブが、保護されている出力待ち行列やジョブ待ち行列に進んでいることを確認することができます。

セキュリティーが重要であると考えられる出力待ち行列とジョブ待ち行列については、セキュリティーの設定を「機密保護解説書」の付録 D の情報と比較することができます。「iSeries 機密保護解説書」

システムに導入された新しいオブジェクトのモニター

ユーザーが独自のプログラムを導入しないように、または導入を制限します。

システムのユーザーが不要な特殊権限を持っていると、適切なオブジェクト権限セキュリティー機構を開発しようとする努力が無駄になることがあります。ユーザー・プロファイルが *ALLOBJ 特殊権限を持っていると、オブジェクト権限は無意味になります。出力待ち行列を保護しようとどのように努力しても、*SPLCTL 特殊権限を持つユーザーは、システム上の任意のスプール・ファイルを見ることができます。*JOBCTL 特殊権限を持つユーザーは、システム操作に影響を与え、ジョブを宛先変更することができます。 *SERVICE 特殊権限を持つユーザーは、オペレーティング・システムを介さなくても、保守ツールを使用してデータにアクセスすることができます。

SECBATCH メニュー・オプション: 29 は即時に投入する。68 はジョブ・スケジューラーを使用する。

ユーザー・プロファイル印刷 (PRTUSRPRF) コマンドを使用して、システム上のユーザー・プロファイルの特殊権限とユーザー・クラスに関する情報を印刷することができます。報告書を実行するときは、次のようないくつかのオプションを使用することができます。

- すべてのユーザー・プロファイル
- 特定の特殊権限を持つユーザー・プロファイル
- 特定のユーザー・クラスを持つユーザー・プロファイル
- ユーザー・クラスと特殊権限の間でミス・マッチしているユーザー・プロファイル

これらの報告書を定期的に実行して、ユーザー・プロファイル管理のモニターに役立てることができます。

トリガー・プログラムの使用のモニター

この項では、トリガー・プログラムの使用をモニターする作業と、それが重要な理由について取り上げ、段階的な手順を示します。

DB2® UDB は、トリガー・プログラムをデータベース・ファイルに関連付ける機能を備えています。トリガー・プログラム機能は、この業界では高機能データベース管理プログラムとしてよく使用される機能です。

トリガー・プログラムをデータベース・ファイルに関連付けるときに、トリガー・プログラムをいつ実行するかを指定します。たとえば、新規レコードがファイルに追加されるたびに、トリガー・プログラムを実行するように顧客オーダー・ファイルをセットアップすることができます。顧客の未払い残高が信用限度を超えると、トリガー・プログラムは警告文を顧客あてに印刷し、メッセージを信用管理者に送信することができます。

トリガー・プログラムは、アプリケーション機能を提供するためにも、情報を管理するためにも生産的な方法になります。トリガー・プログラムは、悪意を持つ人間がシステム上に″トロイの木馬″を作成できるようにもします。破壊的なプログラムが、システムのデータベース・ファイルで特定のイベントが発生したときに実行されるのを座して待っていることもあります。

注: 歴史の上では、トロイの木馬は、ギリシャの兵士たちがこもった、中が空洞になった木製の馬のことです。木馬がトロイの城壁内に入ると、兵士たちは木馬から出てトロイ人と闘いました。コンピューターの世界では、破壊的な機能を隠したプログラムが、しばしばトロイの木馬と呼ばれます。

SECBATCH メニュー・オプション

27 は即時に投入する 66 はジョブ・スケジューラーを使用する

システムが出荷されるときは、トリガー・プログラムをデータベース・ファイルに追加する機能は制限付きになっています。オブジェクト権限を注意深く管理する場合は、一般のユーザーは、トリガー・プログラムをデータベース・ファイルに追加するための十分な権限を持っていません。 (「機密保護解説書」の付録 D には、必要な権限と、物理ファイル・トリガー追加 (ADDPFTRG) コマンドを始めとするすべてのコマンドが示されています。)

トリガー・プログラム印刷 (PRTTRGPGM) コマンドを使用して、特定のライブラリーまたはすべてのライブラリーのすべてのトリガー・プログラムのリストを印刷することができます。

初期報告書を基本として使用して、すでにシステムに存在しているすべてのトリガー・プログラム評価することができます。次に、変更報告書を定期的に印刷して、新規のトリガー・プログラムがシステムに追加されたかどうかを調べることができます。

トリガー・プログラムを評価するときは、以下のことを考慮してください。

- 誰がトリガー・プログラムを作成したか。これを判別するには、オブジェクト記述表示 (DSPOBJD) コマンドを使用します。
- プログラムは何を実行するのか。これを判別するには、ソース・プログラムを調べるか、プログラム作成者に尋ねる必要があります。たとえば、トリガー・プログラムは、誰がユーザーであるかを確認しますか。おそらく、トリガー・プログラムは、システム資源にアクセスするために特定のユーザー (QSECOFR) を待っています。

情報の基礎を確立したら、変更報告書を定期的に印刷して、 システムに追加された新規のトリガー・プログラムをモニターすることができます。

新規プログラムによる借用権限の使用の防止

後でスタックに入れられるプログラムに借用権限を渡すと、 知識のあるプログラマーは、トロイの木馬プログラムを作成する機会を得ます。

トロイの木馬プログラムは、スタックに入っている前のプログラムを利用して、危害を加えるために必要な権限を入手します。これを防止するために、前のプログラムの借用権限を使用するプログラムの作成を許可するユーザーを限定することができます。

新規のプログラムを作成すると、システムは自動的に USEADPAUT パラメーターを *YES に設定します。プログラムに借用権限を継承させたくない場合は、プログラム変更 (CHGPGM) コマンドまたはサービス・プログラム変更 (CHGSRVPGM) コマンドを使用して USEADPAUT パラメーターを *NO に設定しなければなりません。

権限リストおよび借用権限使用 (QUSEADPAUT) システム値を使用して、借用権限を継承するプログラムを作成できるユーザーを制御することができます。権限リスト名を QUSEADPAUT システム値に指定すると、システムはこの権限リストを使用して、新規プログラムの作成方法を決定します。

ユーザーがプログラムまたはサービス・プログラムを作成すると、システムは、権限リストに対するユーザーの権限を検査します。ユーザーが *USE 権限を持っていれば、 新規プログラムの USEADPAUT パラメーターが *YES に設定されます。 ユーザーが *USE 権限を持っていなければ、 USEADPAUT パラメーターが *NO に設定されます。権限リストに対するユーザーの権限は、借用権限からは生じません。

QUSEADPAUT システム値に指定した権限リストは、ユーザーが CHGxxx コマンドを使用して、プログラムまたはサービス・プログラムについて USEADPAUT を設定できるかどうかを制御することもできます。

注:

1. 権限リスト QUESADPAUT を呼び出す必要はありません。別の名前で権限リストを作成することができます。次に、QUSEADPAUT システム値にその権限リストを指定してください。この例のコマンドでは、権限リストの名前を取り替えます。
2. QUSEADPAUT システム値は、システム上の既存プログラムに影響を与えることはありません。CHGPGM コマンドまたは CHGSRVPGM コマンドを使用して、既存のプログラムに USEADPAUT パラメーターを設定してください。

より制限のきつい環境: 大部分のユーザーが USEADPAUT パラメーターを *NO に設定して新規プログラムを作成するようにしたい場合は、次のようにします。

1. 権限リストの共通権限を *EXCLUDE に設定するために、次のように入力します。CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC) AUT(*EXCLUDE)
2. 前のプログラムの借用権限を使用するプログラムを作成するように、特定のユーザーをセットアップしたい場合は、次のように入力します。 ADDAUTLE AUTL(QUSEADPAUT) USER(user-name) AUT(*USE)

より制限の緩い環境: 大部分のユーザーが USEADPAUT パラメーターを *YES に設定して新規プログラムを作成するようにしたい場合は、次のようにします。

1. 権限リストの共通権限を *USE に設定しておきます。
2. 特定のユーザーが前のプログラムの借用権限を使用するプログラムを作成しないようにしたい場合は、次のように入力します。ADDAUTLE AUTL(QUSEADPAUT) USER(user-name) AUT(*EXCLUDE)

ソフトウェアの保全性を保護するためのディジタル署名の使用

ディジタル署名を使用することにより、ソフトウェアのシステムへのロードに対する制御がより効果的 に行え、ロードされてからのソフトウェアの変更を検出する際にも役立ちます。

セキュリティー予防措置をとっても、誰かがいたずらしたデータをシステムに介入させることによってその予防措置をバイパスしたら、意味がありません。サーバーには、いたずらされたソフトウェアをシステムにロードしないようにする、あるいはそのようなソフトウェアがすでにある場合にはそれを検出するために使用できる組み込み (標準装備の) 機能が数多くあります。こうした技法の 1 つは、**オブジェクト署名**です。

オブジェクト署名は、**ディジタル署名**として知られている暗号化概念をインプリメントしたものです。この考えは、比較的簡単です。ソフトウェア製作者がソフトウェアをお客様に出荷する用意が整ったら、製作者はソフトウェアに『署名』します。この署名は、ソフトウェアがある特定の機能を行うことを保証するものではありません。しかし、ソフトウェアの出荷元は署名した製作者であること、およびソフトウェアが作成され署名されてから変更されていないことを証明するための手立てとなります。これは、ソフトウェアがインターネットを介して送信される場合、またはソフトウェアが変更された可能性があると思われるメディアに保管されている場合に、特に重要になります。

新しいシステム値であるオブジェクト復元検査 (QVFYOBJRST) は、システムにロードされるすべてのソフトウェアに識別可能なソフトウェアのソースによる署名を要求する、制限的なポリシーを設定するためのメカニズムを提供します。よりオープンなポリシーを選択し、署名されている場合は、単にその署名を検査することもできます。

すべての i5/OS ソフトウェアとそのオプションのソフトウェアおよびライセンス・プログラムは、システムで承認されたソースで署名されています。これらの署名は、システムによる保全性の保護に役立ち、修正適用時に検査されて、修正がシステムで承認されたソースによるものであること、および転送中に変更されていないことが確認されます。これらの署名は、ソフトウェアがシステムにロードされる際にも検査されます。CHKOBJITG (オブジェクト保全性検査) コマンドが、システム上のオブジェクトの署名を検査します。また、ディジタル証明書マネージャーにも、オペレーティング・システム内のオブジェクトを含む、オブジェクトの署名を検査するためのパネルがあります。

オペレーティング・システムが署名されているように、ディジタル署名を使用して、ビジネスに不可欠なソフトウェアの保全性を保護することができます。ユーザーは、ソフトウェア・プロバイダーによって署名されたソフトウェアを購入することもできますし、または作成したソフトウェアに署名することもできます。そして、定期的に CHKOBJITG、またはディジタル証明書マネージャーを使用して、そのソフトウェアの署名がまだ有効であるか、つまり、オブジェクトが署名されてから変更されていないか検査することをセキュリティー・ポリシーの一部とすることができます。さらに、システムに復元するすべてのソフトウェアが、ユーザーまたはユーザーが識別可能なソースにより署名されていることが必要になる場合もあります。しかし、IBM 以外によって作成されているほとんどのサーバー・ソフトウェアは現在署名されていないので、システムによってはこのメソッドが制限されることもあります。ディジタル署名の機能により、ソフトウェアの保全性を保護するために最善の方法を柔軟に決定することができます。

構造化トランザクション・プログラム名の変更

アーキテクチャー・トランザクション・プログラム名をシステムで実行させないようにするための技法について学びます。

一部の通信要求は、特定のタイプのシグナルをシステムに送信します。 この要求は、 **アーキテクチャー・トランザクション・プログラム名 (TPN)** と呼ばれます。それは、このトランザクション・プログラムの名前がシステムの APPC アーキテクチャーの一部だからです。表示装置パススルー要求の要求は、アーキテ

クチャー TPN の例です。 アーキテクチャー TPN は通信を機能させるための通常の方法であり、必ずしも機密漏れの問題を提示するわけではありません。しかし、アーキテクチャー TPN によって、予期しないシステムへの入り口が提供される場合があります。

一部の TPN は、要求されたプロファイルを渡しません。デフォルト・ユーザーが *SYS である通信項目に要求が関連付けられた場合は、この要求をシステムで開始することができます。ただし、*SYS プロファイルはシステム機能のみを実行でき、ユーザー・アプリケーションを実行することはできません。

アーキテクチャー TPN をデフォルト・プロファイルで実行したくない場合は、通信項目のデフォルト・ユーザーを *SYS から *NONE に変更することができます。

システムで特定の TPN を一切実行したくない場合は、以下のステップを実行します。

1. いくつかのパラメーターを受け入れる CL プログラムを作成します。このプログラムはどの機能も実行しないはずです。このプログラムは単に宣言 (DCL) ステートメントをパラメーターとして持っているだけで、その後で終了します。
2. TPN の経路指定項目を、通信項目とリモート・ロケーション名項目を持つ各サブシステムに追加します。経路指定項目は、次のような指定を行わなければなりません。
   - 開始位置が 37 の TPN のプログラム名と等しい 値比較 (CMPVAL) 値。
   - ステップ 1 で作成したプログラムの名前と等しい呼び出し対象プログラム (PGM) 値。 これにより、TPN が他の経路指定項目 (たとえば、*ANY) を突き止めることができないようにします。

アーキテクチャー TPN 要求:

この項では、アーキテクチャー・トランザクション・プログラム名とその関連ユーザー・プロファイルをリストします。

表 118. アーキテクチャー TPN 要求のプログラムおよびユーザー

TPN 要求	プログラム	ユーザー・プロファイル	説明
X'30F0F8F1'	AMQCRC6A	*NONE	メッセージ待ち行列化
X'06F3F0F1'	QACSOTP	QUSER	APPC サインオン・トランザクション・プログラム
X'30F0F2D1'	QANRTP	QADSM	ADSM/400 APPC 構成
X'30F0F1F9'	QCNPCSUP	*NONE	共用フォルダー
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	リモート SQL-DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	DSNX–PC レシーバー
X'30F0F1F3'	QDXPSEND	QUSER	DSNX–PC 送信側
X'30F0F2C4'	QEVYMAIN	QUSER	ENVY**/400 サーバー
X'30F0F6F0'	QHQTRGT	*NONE	PC データ待ち行列
X'30F0F8F0'	QLZPSERV	*NONE	クライアント・アクセス・ライセンス・マネージャー
X'30F0F1F7'	QMFRCVR	*NONE	PC メッセージ・レシーバー
X'30F0F1F8'	QMFSNDR	*NONE	PC メッセージ送信側
X'30F0F6F6'	QND5MAIN	QUSER	APPN 5394 ワークステーション制御装置

表 118. アーキテクチャー TPN 要求のプログラムおよびユーザー (続き)

TPN 要求	プログラム	ユーザー・プロファイル	説明
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X’30F0F5F4’	QNMEVK	QUSER	システム管理ユーティリティー
X’30F0F2C1’	QNPSERVR	*NONE	PWS-I ネットワーク印刷サーバー
X’30F0F7F9’	QOCEVOKE	*NONE	システム間カレンダー
X’30F0F6F1’	QOKCSUP	QDOC	ディレクトリー・シャドーイング
X’20F0F0F7’	QOQSERV	QUSER	DIA バージョン 2
X’20F0F0F8’	QOQSERV	QUSER	DIA バージョン 2
X’30F0F5F1’	QOQSERV	QUSER	DIA バージョン 2
X’20F0F0F0’	QOSAPPC	QUSER	DIA バージョン 1
X’30F0F0F5’	QPAPAST2	QUSER	S/36—S/38 パススルー
X’30F0F0F9’	QPAPAST2	QUSER	プリンター・パススルー
X’30F0F4F6’	QPWFSTP0	*NONE	共用フォルダー・タイプ 2
X’30F0F2C8’	QPWFSTP1	*NONE	クライアント・アクセス・ファイル・サーバー
X30F0F2C9’’	QPWFSTP2	*NONE	Windows クライアント・アクセス・ファイル・サーバー
X’30F0F6F9’	QRQSRVX	*NONE	リモート SQL 変換サーバー
X’30F0F6F5’	QRQSRV0	*NONE	リモート SQL (コミットなし)
X’30F0F6F4’	QRQSRV1	*NONE	リモート SQL (コミットなし)
X’30F0F2D2’	QSVRCI	QUSER	SOC/CT
X’21F0F0F8’	QS2RCVR	QGATE	SNADS FS2 レシーバー
X’21F0F0F7’	QS2STSND	QGATE	SNADS FS2 送信側
X’30F0F1F6’	QTFDWNLD	*NONE	PC 転送機能
X’30F0F2F4’	QT1HNPCS	QUSER	TIE 機能
X’30F0F1F5’	QVPPRINT	*NONE	PC 仮想印刷
X’30F0F2D3’	QWGMTP	QWGM	Ultimedia Mail/400 server
X’30F0F8F3’	QZDAINIT	QUSER	PWS-I データ・アクセス・サーバー
X’21F0F0F2’	QZDRCVR	QSNADS	SNADS 受信機能
X’21F0F0F1’	QZDSTSND	QSNADS	SNADS 送信機能
X’30F0F2C5’	QZHQTRG	*NONE	PWS-I データ待ち行列サーバー
X’30F0F2C6’	QZRCSRVR	*NONE	PWS-I リモート・コマンド・サーバー

表 118. アーキテクチャー TPN 要求のプログラムおよびユーザー (続き)

TPN 要求	プログラム	ユーザー・プロファイル	説明
X30F0F2C7''	QZSCSRVR	*NONE	PWS-I 中央サーバー

出力待ち行列とジョブ待ち行列へのアクセスのモニター

この項では、出力とジョブ待ち行列へのアクセスをモニターする方法と、それが重要な理由を取り上げ、段階的な手順を示します。

機密保護管理者は、ファイル・アクセスの保護という大きなジョブを行った後で、ファイルの内容を印刷するときに発生した状態について忘れてしまうことがあります。サーバーには、重要な出力待ち行列やジョブ待ち行列を保護するための機能が用意されています。出力待ち行列を保護することで、たとえば、無許可のユーザーが印刷待ちの機密スプール・ファイルを表示したりコピーしたりできないようにします。ジョブ待ち行列を保護することで、無許可のユーザーが機密ジョブを非機密出力待ち行列に宛先変更したり、ジョブ全体を取り消したりできないようにします。

SECBATCH メニューの以下のオプションを使用して、システム上のジョブ待ち行列および出力待ち行列のセキュリティー設定を印刷できます。24 はジョブを即時に投入し、63 はジョブ・スケジューラーを使用します。待ち行列権限印刷 (PRTQAUT) コマンドを使用して、システム上のジョブ待ち行列と出力待ち行列のセキュリティー設定を印刷することもできます。その後で、機密情報を印刷する印刷ジョブを評価し、それらの印刷ジョブが、保護されている出力待ち行列やジョブ待ち行列に進んでいることを確認することができます。

PRTQAUT コマンドについて詳しくは付録 A を参照し、セキュリティーが重要であると考えられる出力待ち行列とジョブ待ち行列については、ご自分のセキュリティーの設定を「iSeries 機密保護解説書」の付録 D にある『ジョブ待ち行列コマンド』および『出力待ち行列コマンド』という表にある出力待ち行列とジョブ待ち行列の必須の機能設定と比較することができます。

サブシステム記述のモニター

この項では、現在システムに入っているサブシステム記述を検討するためのいくつかの推奨事項を示します。

サーバーでサブシステムを開始すると、システムは、作業をシステムに入れて実行するための環境を作成します。サブシステム記述は、この環境の体裁を定義します。したがって、サブシステム記述は、悪意を持ったユーザーに機会を提供する可能性があります。いたずらを企てる人間は、サブシステム記述を使用して自動的にプログラムを開始したり、ユーザー・プロファイルなしでサインオンしたりできます。

共通認可取り消し (RVKPUBAUT) コマンドを実行すると、システムは、サブシステム記述に対する共通権限を *EXCLUDE に設定します。こうすることで、明確に許可されていない (かつ *ALLOBJ 特殊権限を持っていない) ユーザーが、サブシステム記述を変更したり作成したりできないようにすることができます。

サブシステム記述処理 (WRKSBSD) コマンドを使用すれば、すべてのサブシステム記述のリストを作成することができます。このリストから **5** (表示) を選択すると、選択したシステム記述に対するメニューが表示されます。このメニューには、サブシステム環境の各部分のリストが示されています。

オプションを選択して各部分の詳細を確認します。サブシステム記述変更 (CHGSBSD) コマンドを使用して、メニューの最初の 2 つの項目を変更します。他の項目を変更するには、項目タイプに該当する追加、

除去、または変更コマンドを使用します。たとえば、ワークステーション項目を変更するには、ワークステーション項目変更 (CHGWSE) コマンドを使用します。

IBM 提供のサブシステム記述の出荷時における値のリストを含め、サブシステム記述での作業に関する追加情報については、『実行管理機能 (Work Management)』というトピックを参照してください。

自動開始ジョブ項目の確認

自動開始ジョブ項目、および関連するジョブ記述を確認します。サブシステムが開始されるときに自動的に実行されるプログラムの機能を理解しておく必要があります。

自動開始ジョブ項目には、ジョブ記述の名前が入っています。ジョブ記述には、プログラムやコマンドを実行させる要求データ (RQSDTA) が含まれる場合があります。たとえば、RQSDTA は `CALL LIB1/PROGRAM1` となります。サブシステムが開始するたびに、システムは LIB1 ライブラリーの PROGRAM1プログラムを実行します。

ワークステーション名とワークステーション・タイプの確認

ワークステーション項目、および関連するジョブ記述を調べます。意図されないプログラムを実行するように誰かが項目を追加/更新していないか確認してください。

サブシステムは、開始時に、ワークステーション名とワークステーション・タイプの項目に (個々に、またはまとめて) リストされているすべての未割り振りワークステーションを割り振ります。ユーザーがサインオンするとき、ワークステーションを割り振ったサブシステムにサインオンすることになります。

ワークステーション項目を見れば、ジョブがそのワークステーションで開始されるときに、どのジョブ記述が使用されるかが分かります。ジョブ記述には、プログラムやコマンドを実行させる要求データが含まれる場合があります。たとえば、RQSDTA パラメーターは `CALL LIB1/PROGRAM1` となります。ユーザーがそのサブシステム内のワークステーションにサインオンするたびに、システムは LIB1 の PROGRAM1 を実行します。

また、ワークステーション項目は、デフォルトのユーザー・プロファイルを指定することもあります。一部のサブシステム構成では、このように指定すると、**Enter**キーを押すだけで誰でもサインオンすることができます。システムのセキュリティー・レベル (QSECURITY システム値) が `40` よりも低い場合は、デフォルト・ユーザー用のワークステーション項目を検討する必要があります。

ジョブ待ち行列項目の確認

サブシステム記述のジョブ待ち行列項目を定期的に調べて、バッチ・ジョブが正しい環境で実行されていることを確認する必要があります。

サブシステムは、開始時に、サブシステム記述にリストされているすべての未割り振りジョブ待ち行列を割り振ります。ジョブ待ち行列項目は、セキュリティーの問題を直接発生させるわけではありません。しかし、意図されない環境でジョブを実行させることにより、誰かがシステム・パフォーマンスを低下させる機会を与える可能性があります。

経路指定項目の確認

経路指定項目を調べて、意図されないプログラムを実行するように誰かが項目を追加/更新していないか確認してください。

経路指定項目は、ジョブがサブシステムに入った後、ジョブに何を実行させるかを定義します。サブシステムは、すべてのジョブ・タイプ (つまり、バッチ・ジョブ、対話式ジョブ、および通信ジョブ) に経路指定項目を使用します。経路指定項目は、次のものを指定します。

- ジョブのクラス。ジョブ待ち行列項目と同様に、ジョブに関連したクラスはパフォーマンスに影響を与えることがありますが、機密漏れは生じさせません。
- ジョブ開始時に実行されるプログラム。

通信項目とリモート・ロケーション名の確認

通信項目が保護されていることを確認します。

通信ジョブがシステムに入ると、システムは活動サブシステムの通信項目およびリモート・ロケーション名項目を使用して、通信ジョブの実行方法を決定します。これらの項目について、次の事柄を確認してください。

- すべてのサブシステムは通信ジョブを実行することができます。通信に使用するサブシステムが活動状態でない場合、システムに入ろうとしているジョブは、自らの必要を満たす別のサブシステム記述の項目を見つける可能性があります。すべてのサブシステム記述の項目を調べる必要があります。
- 通信項目にはジョブ記述が入っています。ジョブ記述には、プログラムやコマンドを実行する要求データが含まれる場合があります。通信項目と関連ジョブ記述を調べて、ジョブがどのように開始されるかを理解してください。
- 通信項目は、システムが特定の状況で使用するデフォルトのユーザー・プロファイルも指定します。デフォルト・プロファイルの役割を理解してください。システムにデフォルト・プロファイルが含まれている場合は、それらが最小の権限を持つプロファイルであることを確認する必要があります。

サブシステム記述印刷 (PRTSBSDAUT) コマンドを使用して、ユーザー・プロファイル名を指定する通信項目を識別することができます。

デフォルトのユーザー・プロファイルに割り当てられる権限について、詳しくは「ジョブのユーザー・プロファイルのターゲット・システム割り当て」を参照してください。

事前開始ジョブ項目の確認

事前開始ジョブ項目が、許可され、意図された機能だけを実行するかどうか確認する必要があります。

事前開始ジョブ項目を使用すれば、サブシステムに特定の種類のジョブの実行準備をさせることにより、ジョブをより迅速に開始することができます。事前開始ジョブは、サブシステムの開始時、またはそのジョブが必要になったときに開始することができます。事前開始ジョブ項目は、機密漏れを生じさせる可能性があります。

事前開始ジョブ項目は、次のものを指定します。

- 実行するプログラム
- デフォルトのユーザー・プロファイル
- ジョブ記述

ジョブ記述の確認

ジョブ記述を定期的に調べて、意図されないプログラムをジョブ記述が実行しないことを確認する必要があります。ジョブ記述が変更されるのを防ぐには、オブジェクト権限を使用します。

ジョブ記述には、そのジョブ記述が使用されるときに特定のプログラムを実行する要求データと経路指定データが含まれています。ジョブ記述の要求データ・パラメーター内にプログラムが指定されている場合、システムはそのプログラムを実行します。ジョブ記述で経路指定データが指定されている場合、システムはその経路指定データと一致する経路指定項目に指定されているプログラムを実行します。

システムは、対話式ジョブとバッチ・ジョブの両方でジョブ記述を使用します。対話式ジョブの場合、ワークステーション項目がジョブ記述を指定します。通常、ワークステーション項目値は *USRPRF であるため、システムはユーザー・プロファイルに指定されたジョブ記述を使用します。バッチ・ジョブの場合は、ジョブを投入するときにジョブ記述を指定します。

また、ジョブ記述では、どのユーザー・プロファイルの下でジョブを実行するかを指定することもできます。セキュリティー・レベル 40 以上の場合は、ジョブ記述に対する *USE 権限と、ジョブ記述で指定されているユーザー・プロファイルに対する *USE 権限を持っていなければなりません。セキュリティー・レベル 40 未満の場合は、ジョブ記述に対する *USE 権限だけが必要です。

ジョブ記述が変更されるのを防ぐには、オブジェクト権限を使用する必要があります。ジョブ記述を持つジョブを実行するには、*USE 権限で十分です。一般のユーザーには、ジョブ記述に対する *CHANGE 権限は必要ありません。

最後に、ジョブ投入 (SBMJOB) コマンドとユーザー・プロファイル作成 (CRTUSRPRF) コマンドのデフォルト値が、意図されないジョブ記述を指すように変更されていないことを確認する必要があります。

PRTJOBDAUT コマンドの使用

ユーザー・プロファイルを指定し *USE 共通認可を持つジョブ記述のリストを印刷するには、ジョブ記述権限印刷 (PRTJOBDAUT) コマンドを使用します。SECBATCH メニューで、オプション **15** (即時に投入) またはオプション **54** (ジョブ・スケジューラーを使用) を指定して PRTJOBDAUT コマンドを実行します。

PRTJOBDAUT コマンドからのレポートは、ジョブ記述に指定されているユーザー・プロファイルの特殊権限を示します。このレポートには、ユーザー・プロファイルが持つすべてのグループ・プロファイルの特殊権限が含まれています。次のコマンドを使用して、ユーザー・プロファイルの私用認可を表示することができます: `DSPUSRPRF USRPRF(profile-name) TYPE(*OBJAUT)`

ジョブ記述には、実行時にジョブが使用するライブラリー・リストが指定されます。誰かがユーザーのライブラリー・リストを変更できる場合は、そのユーザーが、別のライブラリーに入っている意図されないバージョンのプログラムを実行する可能性があります。システムのジョブ記述に指定されているライブラリー・リストを定期的に確認する必要があります。

権限のモニター

このトピックでは、システム上でのセキュリティー保護の効果を監視するための基本的な提案を取り上げます。

一組のセキュリティー報告書が用意されており、システムで権限がどのようにセットアップされているかを追跡するのに役立ちます。これらの報告書を始めに実行しておくと、すべてのこと (たとえば、すべてのファイルやすべてのプログラムに関する権限) を印刷することができます。

情報の基盤を確立したら、定期的に変更バージョンの報告書を実行することができます。変更バージョンを使用すれば、注意が必要なシステム上のセキュリティー関連の変更を識別するのに役立ちます。たとえば、ファイルの共通権限を示す報告書を毎週実行することができます。変更バージョンの報告書のみを要求することができます。この報告書には、すべてのユーザーが使用できるシステム上の新規のファイルと、最終報告書以降に共通権限が変更された既存のファイルの両方が示されます。

次の 2 つのメニューを使用してセキュリティー・ツールを実行することができます。

- プログラムを対話式に実行するために SECTOOLS メニューを使用します。

- プログラムをバッチで実行するために SECBATCH メニューを使用します。SECBATCH メニューは、2 つの部分に分かれています。1 つは、ジョブを即時にジョブ待ち行列に投入するためのメニューであり、もう 1 つは、ジョブをジョブ・スケジューラーに入れるためのメニューです。

iSeries ナビゲーターを使用している場合は、次のステップに従ってセキュリティー・ツールを実行してください。

1. iSeries ナビゲーターで、ご使用の「**サーバー**」 → 「**セキュリティー**」と展開する。
2. 「**ポリシー**」を右マウス・ボタンでクリックし、「**探索**」を選択して、作成および管理できるポリシーのリストを表示する。

どの監視タスクを定期的に実行する必要があるのかを決定する際には、セキュリティー・ポリシーに関する記述と、ユーザーに対するセキュリティーのメモを検討してください。以下のトピックは、権限をモニターする際に注目すべき幾つかの項目について取り上げています。

権限リストのモニター

オブジェクト・グループを編成するために権限リストをどのように使用するかは、セキュリティー要件によって異なります。

権限リストを使用して、類似のセキュリティー要件を持つオブジェクトごとに分類することができます。権限リスト内には、ユーザーのリストおよびリストによって保護されているオブジェクトに対してそのユーザーが持っている権限が入っています。権限リストは、システム上の類似のオブジェクトに対する権限を管理するための効率的な方法を提供します。ただし、場合によっては、権限リストがオブジェクトに対する権限の追跡を困難にすることもあります。私用認可オブジェクトの印刷 (PRTPVTAUT) コマンドを使用して、権限リストの権限に関する情報を印刷することができます。以下の図は、報告書の例です。

私用権限（全報告書）

権限リスト	所有者	1 次グループ	ユーザー	権限	リスト MGT	オブジェクト OPR	オブジェクト MGT	オブジェクト EXIST	オブジェクト ALTER	オブジェクト REF	SYSTEM4 データ READ	データ ADD	データ UPD	データ DLT	データ 実行
LIST1	QSECOFR	*NONE	*PUBLIC	*EXCLUDE											
LIST2	BUDNIKR	*NONE	BUDNIKR	*ALL	X	X	X	X	X	X	X	X	X	X	X
			*PUBLIC	*CHANGE	X	X	X	X	X	X					
LIST3	QSECOFR	*NONE	*PUBLIC	*EXCLUDE											
LIST4	CJWLDR	*NONE	CJWLDR	*ALL	X	X	X	X	X	X	X	X	X	X	X
			GROUP1	*ALL	X	X	X	X	X	X	X	X	X	X	
			*PUBLIC	*EXCLUDE											

図 8. 権限リストに関する私用権限報告書

この報告書は、権限リスト編集 (EDTAUTL) 表示画面に表示されるものと同じ情報を示しています。この報告書の利点は、すべての権限リストに関する情報が 1 ページで示されることです。たとえば、新規のオブジェクト・グループに関するセキュリティーをセットアップする場合は、報告書を素早くスキャンして、既存の権限リストがこれらのオブジェクトに対するニーズを満たしているかどうかを確認することができます。

変更バージョンの報告書を印刷して、新規の権限リストや、報告書を最後に印刷してから権限が変更された権限リストを見ることができます。また、各権限リストによって保護されているオブジェクトのリストを印刷することもできます。以下の図は、1 つの権限リストに関する報告書の例を示しています。

```
                    権限リスト・オブジェクトの表示

権限リスト . . . . . :   CUSTAUTL
  ライブラリー . . . . . :     QSYS
所有者 . . . . . :   AROWNER
1次グループ . . . . . :   *NONE

                                                1次
ｵﾌﾞｼﾞｪｸﾄ    ﾗｲﾌﾞﾗﾘｰ      タイプ    所有者      グループ    テキスト
CUSTMAS     CUSTLIB     *FILE     AROWNER     *NONE
CUSTORD     CUSTORD     *FILE     OEOWNER     *NONE
```

図 9. 権限リスト・オブジェクト表示の報告書

この報告書を使用すれば、たとえば、新規ユーザーを権限リストに追加した場合の効果 (そのユーザーがどの権限を受け取るか) が分かります。

権限リストの使用

iSeries ナビゲーターは、セキュリティー計画およびセキュリティー・ポリシーの開発を支援し、貴社のニーズに合わせてシステムを構成するために設計されたセキュリティー機能を提供します。使用可能な機能の 1 つに、権限リストの使用があります。

権限リストには、次のような機能があります。

- 類似したセキュリティー要件をもつ権限リスト・グループ・オブジェクト。
- 権限リストには、概念的に、ユーザーやグループ、およびリストによって保護されているオブジェクトに対してユーザーおよびグループが持っている権限が含まれている。
- 各ユーザーおよびグループは、リストによって保護されているオブジェクトのセットに対してさまざまな権限を持つことができる。
- 権限を、ユーザーおよびグループに対して個々に付与せずに、リストによって付与することができる。

権限リストを使用して行えるタスクには、次のものがあります。

- 権限リストの作成
- 権限リストの変更
- ユーザーおよびグループの追加
- ユーザー許可の変更
- 保護されたオブジェクトの表示

この機能を使用するには、以下のステップを実行します。

1. iSeries ナビゲーターで、ご使用の「**サーバー**」 → 「**セキュリティー**」と展開する。**権限リストおよびポリシー**が表示されます。
2. 「**権限リスト**」を右マウス・ボタンでクリックし、「**新規権限リスト**」 を選択する。「**新規権限リスト**」で、次のことを行うことができます。
   - 「**使用 (Use)**」: オブジェクト属性にアクセスして、オブジェクトを使用することができる。共通のものは表示できますが、オブジェクトを変更することはできません。
   - 「**変更 (Change)**」: オブジェクトの内容 (いくつかの例外があります) を変更することができる。「すべて (All)」: 所有者に限定されているオブジェクトを除く、オブジェクトに関するすべての操作が行える。ユーザーまたはグループは、オブジェクトの存在の制御、オブジェクトのセキュリティーの指定、オブジェクトの変更、およびオブジェクトに関する基本機能の実行を行うことができます。また、ユーザーまたはグループは、オブジェクトの所有権を変更することもできます。

- 「**除外 (Exclude)**」: オブジェクトに関するすべての操作が禁止される。この許可を持っているユーザーおよびグループには、オブジェクトへのアクセスまたは操作が許可されません。共通でオブジェクトを使用することができないように指定してください。

権限リストを処理する際に、オブジェクトとデータの両方の認可を認可することになります。選択できるオブジェクト許可は、次のとおりです。

- 「**操作可能 (Operational)**」: オブジェクトの記述を見るための許可と、そのオブジェクトに対してユーザーまたはグループが持っているデータ許可によって決められている通りにオブジェクトを使用するための許可を与える。
- 「**管理 (Management)**」: オブジェクトのセキュリティーを指定するための許可、オブジェクトを移動またはリネームするための許可、データベース・ファイルにメンバーを追加するための許可を与える。
- 「**存在 (Existence)**」: オブジェクトの存在および所有権を制御するための許可を与える。ユーザーまたはグループは、オブジェクトの削除、オブジェクトのストレージの解放、オブジェクトに関する保管および復元操作の実行、オブジェクトの所有権の移行を行うことができます。ユーザーまたはグループが特殊な保管許可を持っている場合には、ユーザーまたはグループは、オブジェクトの存在許可を必要としません。
- 「**更新 (Alter)**」**:** データベース・ファイルおよび SQL パッケージに対してのみ、オブジェクトの属性を更新するために必要な許可を与える。ユーザーまたはグループがデータベース・ファイルに関してこの許可を持っている場合には、ユーザーまたはグループは、トリガーの追加および除去、参照制約および固有制約の追加および除去、データベース・ファイルの属性の変更を行うことができます。ユーザーまたはグループが SQL パッケージに関してこの許可を持っている場合には、ユーザーまたはグループは、SQL パッケージの属性を変更することができます。この許可は、現時点では、データベース・ファイルおよび SQL パッケージに限り使用されます。
- 「**参照 (Reference)**」**:** データベース・ファイルおよび SQL パッケージに対してのみ、あるオブジェクトの操作が他のオブジェクトによって制限されている場合などに、他のオブジェクトからあるオブジェクトを参照するために必要な許可を与える。ユーザーまたはグループが物理ファイルに関してこの許可を持っている場合には、ユーザーまたはグループは、物理ファイルが親である参照制約を追加することができます。この許可は、現時点では、データベース・ファイルに限り使用されます。

選択できるデータ許可は、次のとおりです。

- 「**読み取り (Read)**」: オブジェクトの内容を入手および表示する (ファイルのレコードを表示するなど) ために必要な許可を与える。
- 「**追加 (Add)**」: オブジェクトに項目を追加する (メッセージをメッセージ待ち行列に追加する、レコードをファイルに追加するなど) ための許可を与える。
- 「**更新 (Update)**」: オブジェクトの項目を変更する (ファイルのレコードを 変更する) ための許可を与える。 「削除 (Delete)」: オブジェクトから項目を除去する (メッセージをメッセージ待ち行列から削除する、レコードをファイルから除去するなど) ための許可を与える。
- 「**実行 (Execute)**」: プログラム (サービス・プログラムまたは SQL パッケージ) を実行するために必要な許可を与える。ユーザーは、ライブラリーまたはディレクトリー内のオブジェクトを見付けることもできます。

サーバーでの権限のモニターに関する情報は、『オブジェクトに対する私用権限のモニター』を参照してください。

オブジェクトに対する私用権限のモニター

この項では、オブジェクトに対する私用権限をモニターするのに使用できる SECBATCH メニュー・オプションとセキュリティー・コマンドについて取り上げます。

私用権限はユーザーに与えられたオブジェクト用の特別な権限で、ユーザーのグループ・プロファイルや権限リストの権限など、他の権限をオーバーライドします。グループ・プロファイルや権限リストにリストされていないユーザーは、私用権限の設定されたオブジェクトにはアクセスできません。

SECBATCH メニューの以下のオプションを使用して、オブジェクトに対する私用権限をモニターできます。12 は即時に投入し、14 はジョブ・スケジューラーを使用します。SECBATCH メニューには、機密保護管理者が通常関心を持つオブジェクト・タイプに関するオプションが含まれています。汎用オプション (19 および 58) を使用してオブジェクト・タイプを指定します。

さらに、私用認可オブジェクトの印刷 (PRTPVTAUT) コマンドを使用すれば、指定されたライブラリーに含まれている指定されたタイプのオブジェクトに関するすべての私用権限のリストを印刷することができます。この報告書は、オブジェクトに対する新しい権限を検出するのに役立ちます。この報告書は、私用権限体系が複雑になり過ぎて管理不能になるのを防止するのにも役立ちます。

サーバーでの権限のモニターに関する情報は、『オブジェクトに対する共通権限のモニター』を参照してください。

オブジェクトに対する共通権限のモニター

この項では、オブジェクトに対する共通権限をモニターするのに使用できる SECBATCH メニュー・オプションとセキュリティー・コマンドについて取り上げます。

共通権限は、すべてのユーザーに付与されたオブジェクトに対する権限です。

簡明さのためにもパフォーマンスのためにも、大部分のシステムは、大部分のオブジェクトが大部分のユーザーに使用可能になるようにセットアップされます。ユーザーは、すべてのオブジェクトを使用できることを明示的に許可されるのではなく、セキュリティーが重要な特定の機密オブジェクトにアクセスすることを明示的に拒否されます。高いセキュリティー要件を持つ少数のシステムは、これとは反対のアプローチを取り、必要なときにオブジェクトを許可します。これらのシステムでは、大部分のオブジェクトは、共通権限を *EXCLUDE に設定して作成されます。

これは、オブジェクト・ベースのシステムであり、多くの異なるタイプのオブジェクトを持っています。大部分のオブジェクト・タイプは機密情報を持っていないか、セキュリティー関連の機能を実行しません。一般的なセキュリティー・ニーズを持つシステムの機密保護管理者としては、データベース・ファイルやプログラムのような、保護を必要とするオブジェクトに注意を払う必要があります。その他のオブジェクト・タイプの場合は、アプリケーションにとって十分な共通権限だけを設定することができます。大部分のオブジェクト・タイプの共通権限は *USE です。

共通認可印刷 (PRTPUBAUT) コマンドを使用して、共通ユーザーがアクセスできるオブジェクトに関する情報を印刷することができます。(共通ユーザーとは、オブジェクトに対する明示的な権限を所有していない、サインオン権限を持ったユーザーをいいます。) PRTPUBAUT コマンドを使用する場合は、調べたいオブジェクト・タイプ、およびライブラリーまたはディレクトリーを指定することができます。

SECBATCH メニューのオプション 11 または 50 を使用して、セキュリティーに関係する可能性のあるオブジェクト・タイプについての共通権限オブジェクト報告書を印刷できます。汎用オプション (18 および 57) を使用してオブジェクト・タイプを指定します。この報告書の変更バージョンを定期的に印刷して、どのオブジェクトに注意が必要であるか確認することができます。

詳しくは、『特殊権限のモニター』を参照してください。

ユーザー環境のモニター

この項では、ユーザー環境をモニターするための SECBATCH メニューとコマンドの使用法について説明します。

ユーザー・プロファイルの役割の 1 つは、出力待ち行列、初期メニュー、ジョブ記述など、ユーザーに関する環境を定義することです。ユーザーの環境は、ユーザーのシステムの見方に影響を与えるほか、ユーザーが実行を許可される操作にも、ある程度の影響を与えます。ユーザーは、ユーザー・プロファイルに指定されているオブジェクトに対して権限を持っていなければなりません。しかし、権限体系がまだ進行中であるか、またはあまり限定的でない場合は、ユーザー・プロファイルに定義されているユーザー環境が、意図しない結果を生成することがあります。

SECBATCH メニューの以下のオプションを使用して、ユーザー環境をモニターします。29 はジョブを即時に投入し、68 はジョブ・スケジューラーを使用します。

- ユーザーのジョブ記述は、ユーザーよりも多くの権限を持つユーザー・プロファイルを指定することができます。
- ユーザーは、コマンド行のない初期メニューを持つことができます。しかし、ユーザーのアテンション・キー処理プログラムがコマンド行を提供することができます。
- ユーザーを、機密報告書を実行できるように許可することができます。しかし、ユーザーの出力を、報告書を見てはならないユーザーが使用できる出力待ち行列に送信することができます。

ユーザー・プロファイル印刷 (PRTUSRPRF) コマンドの *ENVINFO オプションを使用することで、システム・ユーザーのために定義されている環境のモニターに役立てることができます。以下の図は、報告書の例を示しています。

ユーザー・プロファイル情報

報告書タイプ . . . . . : *ENVINFO
選択ユーザー . . . . . : *USRCLS

ユーザー・プロファイル	現行ライブラリー	初期メニュー/ライブラリー	初期プログラム/ライブラリー	ジョブ記述 /ライブラリー	メッセージQUEUE/ライブラリー	出力QUEUE/ライブラリー	アテンションプログラム/ライブラリー
AUDSECOFR	AUDITOR	MAIN	*NONE	QDFTJOBD	QSYSOPR	*WRKSTN	*SYSVAL
		*LIBL		QGPL	QSYS		
USERA	*CRTDFT	OEMENU	*NONE	QDFTJOBD	USERA	*WRKSTN	*SYSVAL
		*LIBL		QGPL	QUSRSYS		
USERB	*CRTDFT	INVMENU	*NONE	QDFTJOBD	USERB	*WRKSTN	*SYSVAL
		*LIBL		QGPL	QUSRSYS		
USERC	*CRTDFT	PAYROLL	*NONE	QDFTJOBD	USERC	*WRKSTN	*SYSVAL
		*LIBL		QGPL	QUSRSYS		

図 10. ユーザー・プロファイル印刷: ユーザー環境報告書

詳しくは、『セキュリティー・メッセージのモニター』を参照してください。

特殊権限のモニター

このトピックでは、特殊権限のモニターに使用する SECBATCH メニュー・オプションおよびコマンドについて説明します。

特殊権限は、システム機能を実行するためにユーザーが持つことのできる 1 つのタイプの権限で、全オブジェクト権限、システム保管権限、ジョブ制御権限、セキュリティー管理者権限、スプール制御権、保守権限、およびシステム構成権限が含まれます。

システムのユーザーが不要な特殊権限を持っていると、適切なオブジェクト権限体系を開発しようとする努力が無駄になることがあります。ユーザー・プロファイルが *ALLOBJ 特殊権限を持っていると、オブジ

ェクト権限は無意味になります。出力待ち行列を保護しようとどのように努力しても、 *SPLCTL 特殊権限を持つユーザーは、システム上の任意のスプール・ファイルを見ることができます。 *JOBCTL 特殊権限を持つユーザーは、システム操作に影響を与え、ジョブを宛先変更することができます。 *SERVICE 特殊権限を持つユーザーは、オペレーティング・システムを介さなくても、保守ツールを使用してデータにアクセスすることができます。

SECBATCH メニューの以下のオプションを使用して、特殊権限をモニターします。29 はジョブを即時に投入し、68 はジョブ・スケジューラーを使用します。

ユーザー・プロファイル印刷 (PRTUSRPRF) コマンドを使用して、システム上のユーザー・プロファイルの特殊権限とユーザー・クラスに関する情報を印刷することができます。報告書を実行するときは、次のようないくつかのオプションを使用することができます。

- すべてのユーザー・プロファイル
- 特定の特殊権限を持つユーザー・プロファイル
- 特定のユーザー・クラスを持つユーザー・プロファイル
- ユーザー・クラスと特殊権限の間でミス・マッチしているユーザー・プロファイル

以下の図は、すべてのユーザー・プロファイルに関する特殊権限を示す報告書の例を示しています。

```
                                ユーザー・プロファイル情報

報告書タイプ . . . . . :   *AUTINFO
選択ユーザー . . . . . :   *SPCAUT
特殊権限 . . . . . :   *ALL
                    ---------- 特殊権限 ----------
                                    *IO                                                 グループ
ユーザー・    グループ・  *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  ユーザー・              グループ  権限
プロファイル プロファイル OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  クラス       所有者      権限      タイプ      制約機能
 USERA       *NONE        X     X     X    X     X     X     X     X    *SECOFR     *USRPRF     *NONE       *PRIVATE    *NO
 USERB       *NONE                          X     X                       *PGMR       *USRPRF     *NONE       *PRIVATE    *NO
 USERC       *NONE        X     X     X    X     X     X     X     X    *SECOFR     *USRPRF     *NONE       *PRIVATE    *NO
 USERD       *NONE                                                       *USER       *USRPRF     *NONE       *PRIVATE    *NO
```

図 11. ユーザー情報報告書: 例 1

特殊権限のほかに、報告書には次の情報が示されています。

- ユーザー・プロファイルが制約機能を持っているかどうか
- ユーザーまたはユーザーのグループが、ユーザー作成の新規オブジェクトを所有しているかどうか
- ユーザー作成の新規オブジェクトに対して、ユーザーのグループがどの権限を受け取るか

以下の図は、ミスマッチした特殊権限とユーザー・クラスに関する報告書の例を示しています。以下の点に注意してください。

- USERX は、システム操作員 (*SYSOPR) ユーザー・クラスを持っていますが、 *ALLOBJ および *SPLCTL 特殊権限を持っています。
- USERY は、ユーザー (*USER) ユーザー・クラスを持っていますが、 *SECADM 特殊権限を持っています。
- USERZ も、ユーザー (*USER) クラスと *SECADM 特殊権限を持っています。 USERZ が QPGMR グループのメンバーであり、このグループが *JOBCTL および *SAVSYS 特殊権限を持っていることを確認することができます。

```
                                ユーザー・プロファイル情報

 報告書タイプ . . . . . :   *AUTINFO
 選択ユーザー . . . . . :   *MISMATCH
                        ---------- 特殊権限 ----------
                                   *IO                                                  グループ
ユーザー・    グループ・   *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  ユーザー・              グループ  権限
プロファイル プロファイル OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  クラス      所有者      権限      タイプ      制約機能
 USERX       *NONE        X              X     X                    X    *SYSOPR     *USRPRF     *NONE     *PRIVATE    *NO
 USERY       *NONE                                    X               *USER       *USRPRF     *NONE     *PRIVATE    *NO
 USERZ       *NONE                                    X               *USER       *USRPRF     *NONE     *PRIVATE    *NO
             QPGMR                      X     X
```

図 12. ユーザー情報報告書: 例 2

これらの報告書を定期的に実行して、ユーザー・プロファイル管理のモニターに役立てることができます。

詳しくは、『ユーザー環境のモニター』を参照してください。

関連概念

25 ページの『特殊権限』
このトピックでは、ユーザーに対して指定できる特殊権限を説明します。

サインオンおよびパスワード活動のモニター

システムに入ろうとする未許可の試行について懸念する場合、 サインオンおよびパスワード活動のモニターに役立つ PRTUSRPRF コマンドを使用することができます。

この報告書の使用にあたって、いくつかの提案を示します。

- 一部のユーザー・プロファイルのパスワード満了間隔がシステム値よりも長いかどうか、および、長い満了間隔が正当かどうかを判別する。たとえば、この報告書では、USERY のパスワード満了間隔は 120 日です。
- 正常終了しなかったサインオンの試行をモニターするために、この報告書を定期的に実行する。システムに侵入しようしている人は、正常終了しなかった試行が一定回数に達すると、システムが処置を行うことに知っている可能性があります。毎晩、侵入者になるつもりの人は、試行に対して警告を出されないようにするため、使用中の QMAXSIGN 値よりも少ない回数で試そうとする可能性があります。しかし、この報告書を毎朝早くに実行し、一部のプロファイルのサインオン試行が頻繁に正常終了していないことに気付いた場合、問題が生じているのではないかと疑うことができます。
- 長期間使用されていないユーザー・プロファイルや、パスワードが長期間変更されていないユーザー・プロファイルを識別する。

ユーザー・プロファイルのアクティビティーのモニター

機密保護管理者は、システム上のユーザー・プロファイルに対して行われた変更を制御し監査する必要があります。

ユーザー・プロファイルは、システムへの入り口点を備えています。ユーザー・プロファイルのパラメーターは、ユーザーの環境とユーザーのセキュリティー特性を決定します。

システムが変更のレコードをユーザー・プロファイルに書き込むように、セキュリティー監査をセットアップすることができます。 DSPAUDJRNE コマンドを使用してこれらの変更を印刷することができます。出口プログラムを作成して、ユーザー・プロファイルに対する要求処置を評価することができます。

次の表は、ユーザー・プロファイル・コマンドで使用できる出口点を示しています。

表 119. ユーザー・プロファイルのアクティビティーの出口点

ユーザー・プロファイル・コマンド	出口点名
ユーザー・プロファイル作成 (CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
ユーザー・プロファイル変更 (CHGUSRPRF)	QIBM_QSY_CHG_PROFILE
ユーザー・プロファイル削除 (DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
ユーザー・プロファイル復元 (RSTUSRPRF)	QIBM_QSY_RST_PROFILE

たとえば、出口プログラムは、ユーザーに無許可バージョンのプログラムを実行させるような変更を探し出すことができます。このような変更は、異なるジョブ記述や新規の現行ライブラリーを割り当てる可能性があります。出口プログラムは、受け取った情報に基づいて、メッセージ待ち行列を通知したり、何らかの処置 (ユーザー・プロファイルの変更や使用禁止のような) を行ったりする可能性があります。

「*機密保護解説書*」では、ユーザー・プロファイル処置のための出口プログラムについて詳しく説明しています。「iSeries 機密保護解説書」を参照してください。

セキュリティー・メッセージのモニター

セキュリティー・メッセージをモニターする方法およびそれが重要な理由について。

誤ったサインオンの試行など、セキュリティーに関連する事象によって、QSYSOPR メッセージ待ち行列にメッセージが置かれます。 QSYS ライブラリー内に QSYSMSG と呼ばれる独立したメッセージ待ち行列を作成することもできます。

QSYS ライブラリーに QSYSMSG メッセージ待ち行列を作成すると、重大なシステム事象に関するメッセージが、そのメッセージ待ち行列と QSYSOPR に送信されます。プログラムやシステム操作員は、QSYSMSG メッセージ待ち行列を別々に監視できます。これによって、システム資源に対する保護はさらに強化されます。メッセージ待ち行列に送られるメッセージの量があまりに多いと、QSYSOPR の重大なシステム・メッセージが見過ごされてしまうこともあります。

監査情報の消失の防止

この項は、監査情報の消失を防止するための情報について取り上げます。

エラー条件が原因で監査ジャーナル項目が消失した場合に、2 つのシステム値によって、システムがとる処置が制御されます。

監査強制実行レベル: QAUDFRCLVL システム値によって、システムが監査ジャーナル項目をメモリーから補助記憶装置に書き込む頻度が決定されます。 QAUDFRCLVL システム値は、データベース・ファイルに対して強制実行レベルのように作用します。導入の際に正しい強制実行レベルを決定するには、同じ指針に従わなければなりません。

いつ項目を補助記憶装置に書き込むかをシステムに決定させる場合、システムは、停電によって情報が消失する可能性とパフォーマンスへの影響をふまえた決定をします。 *SYS がデフォルト値であり、推奨値です。

強制実行レベルを低く設定すると、監査レコードが消失する可能性は低くなりますが、パフォーマンスに悪い影響があります。インストール・システムで、停電による監査レコードの消失がないように要求している場合、QAUDFRCLVL を 1 に設定する必要があります。

監査終了処置: QAUDENDACN システム値によって、システムが項目を監査ジャーナルに書き込めないときにとるべき処置が決定されます。デフォルト値は *NOTIFY です。システムが監査ジャーナル項目を書き込めず、 QAUDENDACN が *NOTIFY の場合、システムは以下を行います。

1. QAUDCTL システム値を *NONE に設定して、さらに項目を書き込めないようにします。
2. QSYSOPR メッセージ待ち行列および QSYSMSG メッセージ待ち行列 (存在する場合) に、監査が正常に再開されるまで 1 時間ごとにメッセージ CPI2283 を送信する。
3. 通常の処理が続行されます。
4. IPL がシステムに対して実行された場合、IPL 時にメッセージ CPI2284 が、QSYSOPR および QSYSMSG メッセージ待ち行列に送信されます。

注: ほとんどの場合、IPL を実行すれば、監査の失敗の原因である問題は解決します。システムの再始動後、QAUDCTL システム値を正しい値に設定してください。システムは、このシステム値が変更されたときはいつでも、監査ジャーナル・レコードの書き込みを試行します。

監査が失敗したときに、システムの電源を切るように QAUDENDACN を設定できます (*PWRDWNSYS)。この値を使用するのは、ユーザーのインストール・システムが、監査を活動状態にしてシステムを実行する必要がある場合だけにしてください。システムが監査ジャーナル項目を書き込めず、QAUDENDACN システム値が *PWRDWNSYS である場合、以下のことが生じます。

1. システムは、即時に電源遮断される (PWRDWNSYS *IMMED コマンドを出すことと同等)。
2. SRC コード B900 3D10 が表示される。

次に、以下のことを実行しなければなりません。

1. システム・ユニットで IPL を開始する。 システム・コンソール (QCONSOLE) システム値で指定した装置の電源がオンになっていることを確認します。
2. IPL を完了するには、*ALLOBJ および *AUDIT 特殊権限を持つユーザーが、コンソールでサインオンする。
3. 監査エラーのためにシステムが停止したことを示すメッセージが表示された制限状態で、システムが始動する。
4. QAUDCTL システム値は *NONE に設定される。
5. システムを通常の状態に復元するには、QAUDCTL システム値を NONE 以外の値に設定する。

   QAUDCTL システム値を変更したとき、システムは、監査ジャーナル項目の書き込みを試行します。正常に書き込めた場合、システムは通常の状態に戻ります。システムが通常の状態に正常に戻らない場合、ジョブ・ログを使用して、監査の失敗原因を判別してください。問題を訂正し、QAUDCTL 値を再設定しなおしてください。

ジャーナル・レシーバーの管理

ジャーナル・レシーバーを管理する方法について。

ジャーナル・レシーバーを手動で管理する場合は、以下の手順を使用して、 ジャーナル・レシーバーを切断、保管、および削除してください。

1. CHGJRN JRN(QAUDJRN) JRNRCV(*GEN) と入力します。このコマンドは、以下を事柄を行います。
   a. 現在接続されているレシーバーを切断します。
   b. 次の順次番号の新しいレシーバーを作成します。
   c. 新しいレシーバーをジャーナルに接続します。

たとえば、現行レシーバーが AUDRCV0003 である場合、 システムは AUDRCV0004 という新しいレシーバーを作成および接続します。

ジャーナル属性処理 (WRKJRNA) コマンドは、現在接続されているレシーバーを示します。WRKJRNA QAUDJRN と入力します。

2. オブジェクト保管 (SAVOBJ) コマンドを使用して、切断されたジャーナル・レシーバーを保管します。オブジェクト・タイプ *JRNRCV を指定してください。
3. ジャーナル・レシーバー削除 (DLTJRNRCV) コマンドを使用して、レシーバーを削除します。保管せずにレシーバーを削除しようとすると、警告メッセージを受信します。

オブジェクト・アクティビティーを監視するための監査ジャーナルの使用

監査ジャーナルを使用すれば、オブジェクト・アクティビティーを監視し、セキュリティー事象をログに記録することができます。

QAUDJRN ジャーナルに集めた監査情報を分析したい場合、ジャーナル表示 (DSPJRN) コマンドを使用できます。このコマンドにより、QAUDJRN ジャーナルからの情報をデータベース・ファイルに書き込むことができます。アプリケーション・プログラムまたは照会ツールを使用して、データを分析することができます。

システム処置監査 (QAUDLVL システム値) に *AUTFAIL 値を含めた場合、システムは、資源にアクセスしようとして失敗したすべての試行を監査ジャーナル項目に書き込みます。また、重要なオブジェクトの場合には、成功したすべてのアクセスに関する監査ジャーナル項目をシステムが書き込むようにオブジェクト監査を設定することもできます。

監査ジャーナルは、オブジェクトがアクセスされたことだけを記録します。オブジェクトに対する各トランザクションは、ログに記録されません。重要なシステム・オブジェクトの場合、アクセスされ変更された特定のデータに関するより詳細な情報が必要かもしれません。オブジェクト・ジャーナリングは、これらの詳細を提供することができます。オブジェクト・ジャーナリングは、主としてオブジェクトの保全性および回復のために使用されます。また、機密保護担当者または監査員は、これらのジャーナル項目を使用して、オブジェクト変更を確認することができます。QAUDJRN ジャーナルには、どんなオブジェクトも記録しないでください。

ジャーナル項目には次のものを含めることができます。

- ジョブおよびユーザーの識別とアクセスの時間
- すべてのオブジェクト変更の前と後のイメージ
- オブジェクトのオープン、クローズ、変更、および保管などが行われた時点のレコード

どんなユーザーも (たとえ機密保護担当者であっても) ジャーナル項目を変更することはできません。完全なジャーナルまたはジャーナル・レシーバーを削除することは可能ですが、これは簡単に検出されます。

どのジャーナルがシステム上に存在するか確認したい場合、ジャーナル処理 (WRKJRN) コマンドを使用してください。どのオブジェクトが特定のジャーナルによって記録されるか確認したい場合、ジャーナル属性 (WRKJRNA) コマンドを使用してください。

監査ジャーナルとジャーナル・レシーバーの管理

監査ジャーナル QSYS/QAUDJRN は、セキュリティー監査*専用* です。オブジェクトを監査ジャーナルに記録すべきではありません。コミットメント制御で監査ジャーナルを使用すべきではありません。ジャーナル項目送信 (SNDJRNE) コマンドまたはジャーナル項目送信 (QJOSJRNE) API を使用して、このジャーナルにユーザー項目を送信しないでください。

システムが監査項目を監査ジャーナルに書き込めるようにするには、特別なロック保護を使用します。監査が活動状態である (QAUDCTL システム値が *NONE でない) 場合、 システム仲裁ジョブ (QSYSARB) は、QSYS/QAUDJRN ジャーナルに対するロックを保持します。監査が活動状態の場合、監査ジャーナルに対して次のような操作を実行することはできません。

- DLTJRN コマンド
- ENDJRN*xxx* コマンド
- APYJRNCHG コマンド
- RMVJRNCHG コマンド
- DMPOBJ または DMPSYSOBJ コマンド
- ジャーナルの移動
- ジャーナルの復元
- 権限を処理する操作、たとえば GRTOBJAUT コマンド
- WRKJRN コマンド

監査ジャーナルのすべてのセキュリティー項目には、T というジャーナル・コードが付いています。セキュリティー項目のほかに、ジャーナル QAUDJRN には、システム項目もあります。これらの項目にはジャーナル・コード J が付き、初期プログラム・ロード (IPL) およびジャーナル・レシーバーに対して実行される一般操作 (たとえばレシーバー保管) と関係があります。

ジャーナルまたはその現行レシーバーに損傷が生じたために監査項目をジャーナルできない場合、システムが取る処置は、QAUDENDACN システム値によって決定されます。損傷を受けたジャーナルまたはジャーナル・レシーバーの回復は、他のジャーナルの場合と同じです。

システムにジャーナル・レシーバーの変更を管理させることもできます。 QAUDJRN ジャーナルの作成時に MNGRCV(*SYSTEM) を指定するか、またはジャーナルをその値に変更します。 MNGRCV(*SYSTEM) を指定した場合、システムは、しきい値サイズに達すると自動的にレシーバーを切り離し、新規のジャーナル・レシーバーを作成して接続します。これをシステム変更 - ジャーナル管理といいます。

QAUDJRN に MNGRCV(*USER) を指定した場合、ジャーナル・レシーバーが記憶域しきい値に達すると、ジャーナルに関して指定されたしきい値メッセージ待ち行列にメッセージが送信されます。このメッセージは、レシーバーがしきい値に達したことを示します。 CHGJRN コマンドを使用して、レシーバーを切断し、新しいジャーナル・レシーバーに接続します。これにより、「ジャーナルされていない項目」のエラー条件を防げます。メッセージを受け取った場合、セキュリティー監査を継続するには CHGJRN コマンドを使用する必要があります。

ジャーナルのデフォルトのメッセージ待ち行列は、QSYSOPR です。インストール・システムの QSYSOPR メッセージ待ち行列に大量のメッセージがある場合は、AUDMSG などの異なるメッセージ待ち行列を QAUDJRN ジャーナルに関連付けることができます。メッセージ処理プログラムを使用して、AUDMSG メッセージ待ち行列を監視できます。ジャーナルしきい値の警告 (CPF7099) を受信したら、新しいレシーバーに自動的に接続することができます。システム変更 - ジャーナル管理を使用すると、システム変更ジャーナルが完了した時点で、CPF7020 メッセージがジャーナル・メッセージ待ち行列に送信されます。このメッセージをモニターすれば、切断されたジャーナル・レシーバーを保管する時期を決定できます。

重要: 操作援助機能メニューから利用できる自動終結機能は、 QAUDJRN レシーバーを終結処理しません。ディスク・スペースの問題を避けるために、定期的に QAUDJRN レシーバーの切断、保管、および削除を行う必要があります。ジャーナルおよびジャーナル・レシーバーの管理に関する詳細は、トピック『ジャーナル管理』を参照してください。

注: QAUDJRN ジャーナルが存在せず、 QAUDCTL システム値が *NONE 以外の値に設定されている場合、 IPL 時に QAUDJRN ジャーナルが作成されます。この操作が実行されるのは、ディスク装置の置き換えや補助記憶域プールの消去など、例外的な状態が発生した場合だけです。

監査ジャーナル項目の詳細については、「iSeries 機密保護解説書」の『付録 F』を参照してください。

監査ジャーナル・レシーバーの保管および削除

ここでは、監査ジャーナル・レシーバーを保管および削除する方法について説明します。保管/削除することがなぜ重要か、および段階的な手順を示します。

目的: 新しい監査ジャーナル・レシーバーの接続。古いレシーバーの保管および削除。

方法:

- CHGJRN QSYS/QAUDJRN
- JRNRCV(*GEN) SAVOBJ (古いレシーバーを保管する)
- DLTJRNRCV (古いレシーバーを削除する)

権限: ジャーナル・レシーバーに対する *ALL 権限、ジャーナルに対する *USE 権限

注: 監査ジャーナル・レシーバーを保管および削除するには、システムの稼働率が高くない時間帯を選んでください。

以下の 2 つの理由により、定期的に現行の監査ジャーナル・レシーバーを切り離し、新しい監査ジャーナル・レシーバーを接続する必要があります。

- 具体的かつ管理可能な時間枠の項目が各ジャーナル・レシーバーに含まれていれば、ジャーナル項目の分析はより容易になります。
- 大きなジャーナル・レシーバーは、補助記憶域の貴重なスペースを占めてしまうだけでなく、システム・パフォーマンスにも影響を与えます。

システムにレシーバーを自動的に管理させることを推奨します。これを指定するには、ジャーナルを作成するときに、*レシーバー管理* パラメーターを使用します。

処置監査およびオブジェクト監査によって多数の異なる事象をログに記録するよう設定済みの場合は、そのジャーナル・レシーバーに大きなしきい値を指定することが必要かもしれません。レシーバーを手動で管理する場合は、ジャーナル・レシーバーを毎日変更しなければならないかもしれません。少しの事象だけをログに記録するのであれば、ジャーナル・レシーバーを含むライブラリーのバックアップ・スケジュールに合わせてレシーバーを変更することができます。

レシーバーの切断および新しいレシーバーの接続には、CHGJRN コマンドを使用します。

システム管理によるジャーナル・レシーバー: システムにレシーバーを管理させる場合は、以下の手順を使用して、切断された QAUDJRN レシーバーをすべて保管した後、それらを削除します。

1. WRKJRNA QAUDJRN と入力します。画面に、現在接続されているレシーバーが表示されます。このレシーバーは保管または削除しないでください。
2. レシーバー・ディレクトリーを処理するために、F15 を使用します。これにより、ジャーナルに関連付けられているすべてのレシーバーおよびその状況が表示されます。
3. SAVOBJ コマンドを使用して、(まだ保管されていない) 現在接続されているレシーバーを除く各レシーバーを保管します。
4. DLTJRNRCV コマンドを使用して、保管後の各レシーバーを削除します。

注: 上記の手順に代わる方法として、ジャーナル・メッセージ待ち行列を使用し、システム変更ジャーナルが正常に終了したことを示す CPF7020 メッセージをモニターすることもできます。

詳しくは、「バックアップおよび回復」のセクションを参照してください。

監査機能の停止

監査機能をオフにする方法

監査機能を常時使用する代わりに、定期的に使用することもできます。たとえば、新しいアプリケーションのテスト時に使用できます。または、四半期ごとのセキュリティー監査を実行するために使用することもできます。監査機能を停止するには、以下のようにしてください。

1. WRKSYSVAL コマンドを使用して、 QAUDCTL システム値を *NONE に変更します。 これにより、システムによるセキュリティー事象のログを停止します。
2. CHGJRN コマンドを使用して現行ジャーナル・レシーバーを切断します。
3. SAVOBJ および DLTJRNRCV コマンドを使用して、切断されたレシーバーを保管および削除します。
4. QAUDCTL を *NONE に変更すると、QAUDJRN ジャーナルを削除できるようになります。セキュリティー監査をいつか再開する予定であれば、QAUDJRN ジャーナルをシステムに残すこともできます。

しかし、QAUDJRN ジャーナルを MNGRCV(*SYSTEM) で設定した場合、セキュリティー監査が活動状態かどうかにかかわらず、IPL を実行するごとにシステムはレシーバーを切断して新しいレシーバーを接続します。これらのジャーナル・レシーバーを削除する必要があります。これらには監査項目が入っていないので、削除する前に保管する必要はありません。

ヒストリー・ログの使用

ここでは、ヒストリー・ログの使用方法、ヒストリー・ログがなぜ重要か、および段階的なセットアップ手順を示します。

QMAXSIGN システム値に指定されている誤ったサインオン試行回数の超過など、セキュリティー関連のいくつかの事象が発生すると、メッセージが QHST (活動記録) ログに送信されます。セキュリティー・メッセージは、2200 から 22FF の範囲です。 接頭部は CPI、CPF、CPC、CPD、および CPA です。

いくつかの権限障害および保全性違反メッセージは、もはや QHST (活動記録) ログに送信されなくなりました。QHST ログで入手可能であったすべての情報は、セキュリティー監査ジャーナルで入手できます。セキュリティー監査ジャーナルに情報を記録する方が、システム・パフォーマンスが改善されます。しかも、このようなセキュリティー関連事象に関して QHST ログよりも詳細な情報が得られます。 QHST ログを、セキュリティー違反の完全な情報源とは見なさないでください。その代わりにセキュリティー監査機能を使用してください。

以下のメッセージは、QHST ログにはもはや書き込まれません。

- CPF2218。これらの事象は、QAUDLVL システム値に *AUTFAIL を指定することによって、監査ジャーナルで獲得できます。
- CPF2240。これらの事象は、QAUDLVL システム値に *AUTFAIL を指定することによって、監査ジャーナルで獲得できます。

セキュリティー計画の関連情報

システム・セキュリティーの計画とセットアップに関連した製品マニュアル、IBM Redbooks™ (PDF 形式)、Web サイト、および Information Center のトピックを以下にリストします。いずれの PDF も表示または印刷可能です。

資料

iSeries 機密保護解説

その他の情報

- 「侵入検知」には、TCP/IP ネットワークを介した侵入を防止する方法が説明されています。

PDF ファイルの保管

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を右マウス・ボタン・クリックする (上部のリンクを右マウス・ボタン・クリック)。
2. PDF をローカルに保存するオプションをクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「**保存**」をクリックする。

Adobe Reader のダウンロード

これらの PDF を表示または印刷するには、Adobe Reader をシステムにインストールする必要があります。無償版を Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) からダウンロードできます。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品 、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項に基づいて、 IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 (C) Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

以下は、IBM Corporation の商標です。

- AIX
- AS/400
- DRDA
- eServer
- i5/OS
- IBM
- iSeries
- Lotus Notes
- Net.Data

| NetServer
| OS/400
| PowerPC
| Redbooks
| System/36
| System/38
| xSeries
| z/OS

Microsoft、 Windows、 Windows NT®、および Windows ロゴは、 Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは、Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

| Linux は、Linus Torvalds の米国およびその他の国における商標です。

UNIX は、The Open Group の米国およびその他の国における登録商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することは できません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、 IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12