

IBM

@server

iSeries

保守ツール





@server

iSeries

保守ツール

© Copyright International Business Machines Corporation 2002. All rights reserved.

© Copyright IBM Japan 2002

目次

| | |
|---------------------------|----|
| 保守ツール | 1 |
| V5R2 の新機能 | 1 |
| トピックの印刷 | 2 |
| 保守ツールの概念 | 3 |
| 保守ツール用語集 | 3 |
| DST と SST | 5 |
| 保守ツール・ユーザー ID | 6 |
| 保守ツール・ユーザー ID のパスワード・ポリシー | 7 |
| 保守ツール・サーバー | 8 |
| 保守ツールの管理 | 8 |
| 保守ツールへのアクセス | 9 |
| 保守ツール・ユーザー ID の管理 | 11 |
| 保守ツール・ユーザー ID の構成 | 11 |
| 保守ツール・ユーザー ID とパスワードの変更 | 15 |
| QSECOFR のパスワードのリカバリーとリセット | 19 |
| 保守ツール・セキュリティー・データの保管と復元 | 20 |
| 保守ツール・ユーザー ID の管理に関する推奨事項 | 21 |
| 保守ツール・サーバーの構成 | 21 |
| サービス機能の使用のモニター | 24 |
| 保守ツールのトラブルシューティング | 25 |
| 保守ツール関連情報 | 26 |

保守ツール

保守ツールは、サーバーの構成、管理、および保守に使用されます。保守ツールには、専用保守ツール (DST) またはシステム保守ツール (SST) からアクセスできます。

DST や SST を使用する場合、および iSeries ナビゲーター機能を使用して論理区画 (LPAR) やディスク装置を管理する場合には、保守ツール用のユーザー ID が必要です。

従来、保守ツール用のユーザー ID を指す用語として、DST ユーザー・プロファイル、DST ユーザー ID、保守ツール・ユーザー・プロファイル、またはこれらから派生した用語が使用されていました。本トピックでは、**保守ツール・ユーザー ID** という用語を使用します。

最初に、以下の情報を参照してください。

V5R2 の新機能

V5R2 での変更点を、最新情報とともに説明します。

トピックの印刷

本トピック『保守ツール』内の全情報を含む PDF を印刷する方法を説明します。

保守ツールについて詳しく調べるには、以下からトピックを選択してください。

保守ツールの概念

保守ツールの管理を始める前に理解しておく必要がある一般情報 (本トピックを通じて使用される保守ツール用語の定義など) が含まれています。

保守ツールの管理

サーバー上で保守ツールを管理する方法を学習します。

保守ツールのトラブルシューティング

保守ツールに関する一般的な問題をトラブルシューティングします。

保守ツール関連情報

本トピック『保守ツール』の関連情報を表示または印刷する方法を説明します。

V5R2 の新機能

『保守ツール』は、V5R2 の Information Center で追加された新トピックです。単に情報が新しく追加されただけではありません。V5R2 の保守ツールの機能は、従来より大幅に強化されています。

SST からの保守ツール・ユーザー ID の管理

保守ツール・ユーザー ID が、システム保守ツール (SST) から管理および作成できるようになりました。これにより、パスワードのリセット、特権の付与や取り消し、または保守ツール・ユーザー ID の作成のために、専用保守ツール (DST) を使用しなくてもよくなりました。今後、これらの操作を実行する機能へは、SST のメイン画面でオプション 8 (保守ツール・ユーザー ID の処理 (Work with service tools user IDs)) を選択することでアクセスできます。

SST から保守ツール・ユーザー ID を作成する必要がある場合、または「保守ツール・ユーザー ID の処理 (Work with service tools user IDs)」オプションを使用する必要がある場合、サインオン時に使用する保

守ツール・ユーザー ID のパスワードは、デフォルトのパスワードであってはいけません。パスワードがデフォルト・パスワードの保守ツール・ユーザー ID を使用して SST にサインオンした場合、新規保守ツール・ユーザー ID を作成したり、「保守ツール・ユーザー ID の処理 (Work with service tools user IDs)」オプションを使用したりしようとすると、エラーが発生します。

デフォルト・パスワードおよび有効期限が切れたパスワードの変更機能への制限

iSeries サーバーは、デフォルト・パスワードおよび有効期限が切れたパスワードを変更する機能が制限された状態で出荷されるようになりました。具体的には、パスワードがデフォルトまたは有効期限切れになっている保守ツール・ユーザー ID を保守ツール・ユーザー ID 変更 (QSYCHGDS) API によって変更することはできず、また、それらのユーザー ID のパスワードを SST によって変更することもできません。パスワードがデフォルトまたは有効期限切れになっている保守ツール・ユーザー ID は、DST を使用してのみ変更することができます。

この設定を変更して、デフォルト・パスワードおよび有効期限が切れたパスワードを変更できるようにすることができます。SST または DST で「システム・セキュリティの処理 (Work with System Security)」オプションを選択します。「システム・セキュリティの処理 (Work with System Security)」画面で、「パスワードがデフォルトおよび有効期限切れの保守ツール・ユーザー ID に自己のパスワードの変更を許可する (Allow a service tools user ID with a default and expired password to change its own password)」フィールドを「いいえ」(デフォルト) から「はい」に変更します。


用語の変更

新しい保守ツール用語を反映させるため、テキスト・データやその他の資料が変更されました。具体的には、以前に使用されていた DST ユーザー・プロファイル、DST ユーザー ID、保守ツール・ユーザー・プロファイルなどの用語 (またはこれらから派生した用語) の代わりに、保守ツール・ユーザー ID という用語が使用されるようになりました。

システム保守ツール開始 (STRSST) 特権の追加

システム保守ツール開始 (STRSST) 特権が新しく追加されました。この特権を利用して、DST へのアクセスは許可されても SST へのアクセスは制限される保守ツール・ユーザー ID を作成することができます。

iSeries 最初にお読みください

本リリースでの新機能および変更内容に関するその他の情報については、「iSeries 最初にお読みください」 を参照してください。

トピックの印刷

PDF 版をダウンロードし、表示するには、『保守ツール』 (約 472 KB、36 ページ) を選択します。


PDF ファイルの保存

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・ボタンでクリックする (上記のリンクを右マウス・ボタンでクリックする)。
2. 「リンクを名前を付けて保存」(Netscape Navigator) または「対象をファイルに保存」(Internet Explorer) を選択する。
3. PDF を保管するディレクトリーを指定する。

4. 「保存」をクリックする。

Adobe Acrobat Reader のダウンロード

PDF ファイルを表示したり印刷したりするには、Adobe Acrobat Reader が必要です。これは、Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から、ダウンロードできます。

保守ツールの概念

以下の概念説明には、保守ツールを使用する前に知っておく必要がある基本的な情報が提供されています。

保守ツール用語集

本トピックを通じて使用される保守ツール用語の定義が含まれています。

DST と SST

DST と SST がどのようなものであるか、およびこれらの違いについて説明します。

保守ツール・ユーザー ID

保守ツール・ユーザー ID と機能特権について説明します。

保守ツール・ユーザー ID のパスワード・ポリシー

保守ツール・ユーザー ID のパスワード・ポリシーについて説明します。

保守ツール・サーバー

保守ツール・サーバーについて説明します。

保守ツール用語集

以下の定義は、保守ツール関係の情報を理解する上で役立ちます。

Data Encryption Standard (DES)

可逆暗号化アルゴリズムの一種。DES では、暗号化されるデータと、そのデータの暗号化に使用される鍵の 2 つの情報が使用される。暗号化されたデータと暗号鍵を DES によって処理すれば、データの暗号化を解除して元のデータを取り出すことができる。

専用保守ツール (DST) (dedicated service tools (DST))

専用保守ツール (DST) は、コンソールからのみ使用できるサービス機能である。オペレーション・システムが使用可能な場合だけでなく、使用不能な場合にも実行できる。

デフォルト・パスワード (default password)

パスワードが保守ツール・ユーザー ID と同一である場合のそのパスワード。例えば、IBM 提供の保守ツール・ユーザー ID である QSECOFR には、出荷時点ではデフォルト・パスワード QSECOFR が設定されている。

使用不可パスワード (disabled password)

無効なサインオンが何度も試行されたため、サインオンに使用できないようにされたパスワード。使用不可パスワードを使用してサインオンすることはできない。

有効期限が切れたパスワード (expired password)

180 日間以上変更されていないパスワード。有効期限が切れたパスワードを使用してサインオンすることは引き続き可能であるが、サインオンの際にパスワードを変更しなければならない。

機能特権 (functional privileges)

個別の保守ツール機能へのアクセスを認可または禁止する能力。

ロック (locked)

特定の機能へのプログラムのな変更を制御するために使用されるメカニズム。機能が「ロック」されている場合、その機能は通常のユーザー・インターフェースからは変更できない。そのような機能を変更するには、アンロックする必要がある。

OS/400 ユーザー・プロファイル (OS/400 user profiles)

ユーザー・プロファイル作成 (CRTUSRPRF) CL コマンドを使用して作成されたユーザー・プロファイル。OS/400 へのサインオンに使用される。

パスワード・レベル (password levels)

DST 内では、パスワード・レベルを設定できる。パスワード・レベルによって、パスワード格納の際に Data Encryption Standard (DES) または Secure Hash Algorithm (SHA) のどちらを使用するかが指定される。デフォルトのレベルは DES である。

Secure Hash Algorithm (SHA)

データを数学的に不可逆な方法で暗号化する暗号化方式。異なる複数のデータから同じハッシュ値が生成される可能性があり、ハッシュ値を使用して元のデータを判別することはできない。

サービス機能 (service functions)

保守ツールに備わっている固有の機能。サービス機能は、通常、問題判別および問題解決に使用される (多くの場合、IBM サポートの援助を受けて使用される)。サービス機能の例としては、ライセンス内部コード (LIC) トレース、ライセンス内部コード (LIC) ログ、表示機能、変更機能、ダンプ機能などがある。

保守ツール (service tools)

サーバーの運用にかかわる重要な性質を構成、管理、および保守するために使用される機能。保守ツールを使用すれば、論理区画の構成、ディスク装置の管理、問題のトラブルシューティングなどの作業を行うことができる。保守ツールには、専用保守ツール (DST)、システム保守ツール (SST)、およびその他のサービス関連 CL コマンドを使用してアクセスする。保守ツールを適切に使用しなかった場合、サーバーが損傷する可能性がある。

保守ツール装置 ID (service tools device IDs)

LAN コンソールで、システムへのアクセスを制御するために使用される。

保守ツール・サーバー (service tools server)

保守ツール・サーバーを使用することで、PC からの TCP/IP 経由での保守ツール機能の実行が可能になる。

保守ツール・ユーザー ID (service tools user IDs)

DST や SST にアクセスする場合、iSeries ナビゲーターにアクセスして論理区画やディスク装置を管理する場合、およびオペレーション・コンソールにアクセスする場合に要求されるユーザー ID。保守ツール・ユーザー ID は DST または SST を使用して作成するものであり、OS/400 ユーザー・プロファイルとは別のものである。

システム保守ツール (SST) (system service tools (SST))

システム保守ツール (SST) を使用することで、OS/400 からのサービス機能へのアクセスが可能になる。保守ツールには、SST 開始 (STRSST) CL コマンドを使用してアクセスする。

DST と SST

専用保守ツール (DST) とシステム保守ツール (SST) は、両方とも、保守ツールおよびサービス機能にアクセスするために使用されます。DST は、OS/400 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始動されていれば使用できます。SST は、OS/400 から使用できます。保守ツールは、以下の作業を行うために使用されます。

- サーバーの問題の診断
- サーバーへのハードウェア・リソースの追加
- ディスク装置の管理
- 論理区画 (LPAR) のアクティビティの管理 (メモリー管理を含む)
- ライセンス内部コードおよび製品のアクティビティ・ログの確認
- ライセンス内部コードのトレース
- 主記憶装置のダンプの実行
- システム・セキュリティの管理
- 他の保守ツール・ユーザー ID の管理

DST と SST の基本的な違いの概要を、次のテーブルに示します。

| 特性 | DST | SST |
|--------|---|---|
| アクセス方法 | 手動 IPL 中にコンソールを使用して、またはコントロール・パネルでオプション 21 を選択して、物理的にアクセスします。 | 対話式ジョブを使用してアクセスします。このとき、QSRV または以下の権限を持つユーザーとしてサインオンできることが必要です。 <ul style="list-style-type: none">• SST 開始 (STRSST) CL コマンドを使用できる権限• 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 を使用できる機能特権 |

| 特性 | DST | SST |
|-------|--|--|
| 使用可能時 | サーバーの機能が制限されている場合にも使用できます。DST へのアクセスには、OS/400 は必要とされません。 | OS/400 が始動済みの場合に使用可能です。SST にアクセスするには、OS/400 が必要です。 |
| 認証方法 | 保守ツール・ユーザー ID とパスワードが必要です。 | 保守ツール・ユーザー ID とパスワードが必要です。 |


保守ツール・ユーザー ID

保守ツール・ユーザー ID は、専用保守ツール (DST)、システム保守ツール (SST)、またはオペレーション・コンソールを使用してサービス機能にアクセスする場合、および論理区画管理やディスク装置管理のために iSeries ナビゲーターを使用してサービス機能にアクセスする場合に必要なユーザー ID です。保守ツール・ユーザー ID は DST または SST を使用して作成するもので、OS/400 ユーザー・プロファイルとは別のものです。

IBM からは、以下の保守ツール・ユーザー ID が提供されます。

- QSECOFR
- QSRV
- 11111111
- 22222222

IBM 提供のこれら 4 個のユーザー ID を含めて、最大 100 個の保守ツール・ユーザー ID を作成することができます。IBM 提供の保守ツール・ユーザー ID に付与されている特定の権限の詳細については、

「iSeries セキュリティーの手引き」 を参照してください。IBM 提供の保守ツール・ユーザー ID である 11111111 は、オペレーション・コンソールをアップグレードするときに役立ちます。詳しくは、トピック『オペレーション・コンソール』を参照してください。

注: サーバーが IBM から出荷される時点で、OS/400 ユーザー・プロファイル QSECOFR と保守ツール・ユーザー ID QSECOFR が提供されています。これらは同じものではありません。これらはそれぞれ異なる場所に存在し、異なる機能へのアクセスのために使用されます。保守ツール・ユーザー ID QSECOFR には、OS/400 ユーザー・プロファイル QSECOFR とは異なるパスワードを設定できます。保守ツール・ユーザー ID と OS/400 ユーザー・プロファイルのパスワード・ポリシーは異なります。

また、追加の保守ツール・ユーザー ID を作成する機能も提供されています。セキュリティ管理者は、IBM 提供の保守ツール・ユーザー ID にパスワードを新しく割り当てなくても、追加の保守ツール・ユーザー ID を作成することによって、保守ツールの使用を管理および監査することができます。追加の保守ツール・ユーザー ID は、専用保守ツール (DST) またはシステム保守ツール (SST) を使用して作成できます。

保守ツール・ユーザー ID には有効期限があります。このことを利用して、サーバーのセキュリティ上のリスクを最小化することができます。例えば、サービス技術者に対し、有効期間の短い保守ツール・ユーザー ID を作成し、必要な保守ツールのみアクセスを認可することができます。また、保守ツール・ユーザー ID は、ユーザーが退職した場合には使用不可にすることができるので、退職者が悪意を持って保守ツールにアクセスする可能性を最小化することができます。

保守ツール・ユーザー ID の機能特権

保守ツール・ユーザー ID が個別のサービス機能にアクセスする能力は、認可または取り消すことができます。このような能力を、**機能特権**といいます。機能特権を設定することによって、保守ツール・ユーザー ID がアクセスできるサービス機能を制御することができます。機能特権の使用例を以下に示します。

- あるユーザーに通信およびライセンス内部コードのトレースを許可する一方で、別のユーザーにディスク装置管理のための機能特権を付与することができます。
- 新しい保守ツール・ユーザー ID を作成して、IBM 提供の保守ツール・ユーザー ID である QSECOFR に付与されているのと同じ機能特権を付与します。その後で、IBM 提供の保守ツール・ユーザー ID を使用不可にします。これにより、よく知られているユーザー ID である QSECOFR が使用されないようになるので、サーバーをセキュリティ上のリスクから保護するのに有効です。

機能特権は DST または SST を使用して管理することができます。保守ツール開始特権を利用すると、保守ツール・ユーザー ID に DST へのアクセスを許可する一方で、SST へのアクセスを制限することができます。

ユーザーがサービス機能の使用または実行を許可される前に、機能特権の検査が行われます。ユーザーの特権が十分でない場合、サービス機能へのアクセスは拒否されます。さらに、保守ツール・ユーザーによるサービス機能の使用をモニターするため、監査ログが記録されます。

保守ツール・ユーザー ID のパスワード・ポリシー

保守ツール・ユーザー ID は、OS/400 ユーザー・プロファイルとは別のものです。保守ツール・ユーザー ID のパスワードは、複数のセキュリティ・レベルで暗号化されます。デフォルトのパスワード・レベルでは、Data Encryption Standard (DES) による暗号化が使用されます。iSeries ナビゲーターを使用して論理区画管理やディスク装置管理などのサービス機能に接続する V5R1 以前のバージョンのクライアントが存在する場合は、DES による暗号化を使用する必要があります。

パスワード・レベルを変更して、Secure Hash Algorithm (SHA) による暗号化を使用することもできます。この暗号化方式は、数学的に不可逆であり、より強力な暗号化とより高度なセキュリティ・レベルを実現します。ただし、暗号化方式を SHA に変更した後で、DES に戻すことはできません。暗号化方式を SHA に変更すると、V5R1 以前のバージョンのクライアント (オペレーション・コンソールなど) を使用して保守ツール・サーバーに接続することができなくなります。パスワード・レベルを SHA にアップグレードする場合、そのような機能を使用しているクライアントをすべてアップグレードする必要があります。

DES による暗号化を使用する場合、保守ツール・ユーザー ID とパスワードの特性は次のようになります。

- ユーザー ID は最長 10 桁の英大文字になる。
- パスワードは最長 8 桁で大文字小文字が区別される。ユーザー ID とパスワードを作成する際の最小パスワード長は、1 桁です。パスワードを変更する際には、最低限 6 桁が必要となります。
- ユーザー ID のパスワードは、180 日後も有効期限切れとならない。ただし、IBM 提供の保守ツール・ユーザー ID の初期パスワードは、デフォルトで有効期限切れに設定されて出荷されます。

SHA による暗号化を使用する場合、保守ツール・ユーザー ID とパスワードの特性は次のようになります。

- ユーザー ID は最長 10 桁の英大文字になる。
- パスワードは最長 128 桁で大文字小文字が区別される。ユーザー ID とパスワードを作成する際の最小パスワード長は、1 桁です。パスワードを変更する際には、最低限 6 桁が必要となります。
- ユーザー ID のパスワードは、180 日後に有効期限切れとなる。

- パスワードは、デフォルトで有効期限切れに初期設定される (画面上、明示的に「いいえ」に設定されている場合を除く)。
- パスワードは有効期限切れに設定できる (セキュリティー管理者が設定する)。

使用する暗号化方式を SHA に変更するには、DST にアクセスして、以下のステップを実行してください。

1. 自分の保守ツール・ユーザー ID を使用して DST にサインオンする。「専用保守ツール (DST) の使用 (Use dedicated service tools (DST))」画面が表示されます。
2. オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、Enter キーを押す。「DST 環境処理 (Work with DST Environment)」画面が表示されます。
3. オプション 6 (保守ツール・セキュリティー・データ (Service tools security data)) を選択し、Enter キーを押す。
4. オプション 6 (パスワード・レベル (Password level)) を選択し、Enter キーを押す。新しいパスワード・レベルに変更する準備ができていれば、もう一度 Enter キーを押します。

保守ツール・サーバー

保守ツール・サーバーを使用することで、PC から TCP/IP 経由でサービス機能を実行できるようになります。保守ツール・サーバーを使用して、GUI ベースで論理区画 (LPAR) やディスク管理のアクティビティを実行するには、保守ツール・サーバーを使用可能にする必要があります。保守ツール・サーバーの構成は、DST 用または OS/400 用 (あるいはその両方用) に行うことができます。この構成を行うと、許可ユーザーは、iSeries ナビゲーターから LPAR 管理やディスク管理などの機能を使用することができるようになります。

注: iSeries ナビゲーターのサービス機能は、保守ツール・サーバーを構成および始動せずに使用することはできません。

保守ツールの管理

保守ツールの管理と保守に有効な戦略を開発するには、以下のトピックを参照してください。

保守ツールへのアクセス

DST、SST、および iSeries ナビゲーターを使用して、保守ツールにアクセスします。

保守ツール・ユーザー ID の管理

保守ツール・ユーザー ID の構成、保守ツール・ユーザー ID とパスワードの変更、QSECOFR のパスワードのリカバリーとリセット、および保守ツール・セキュリティー・データの保管と復元を行います。

保守ツール・サーバーの構成

DST 用または OS/400 用 (あるいはその両方用) に保守ツール・サーバーを構成します。

サービス機能の使用のモニター

監査ログを使用して、サービス機能の使用をモニターします。

保守ツールへのアクセス

保守ツールには、DST、SST、および iSeries ナビゲーターを使用してアクセスできます。保守ツールにアクセスした後使用できるサービス機能は、付与されている機能特権によって異なります。適切な機能特権が付与されていれば、SST または DST から保守ツール・ユーザー ID の管理を行うことができます。

以下のセクションでは、保守ツールにアクセスするためのステップを、アクセス手段ごとに示します。

DST による保守ツールへのアクセス

DST を使用して保守ツールにアクセスする際に使用する保守ツール・ユーザー ID には、DST 環境を使用できる機能特権が付与されている必要があります。

DST を開始する方法は 2 つあります。第 1 の方法は、システム・コントロール・パネルの機能 21 を使用して DST にアクセスする方法です。第 2 の方法は、手動 IPL を使用する方法です。

コントロール・パネルから DST を使用して保守ツールにアクセスするには、以下のステップを実行してください。

1. コントロール・パネルを手動モードにする。
2. コントロール・パネルの機能 21 を選択し、Enter キーを押す。「DST サインオン (DST Sign On)」画面がコンソールに表示されます。
3. 自分の保守ツール・ユーザー ID とパスワードを使用して、DST にサインオンする。「専用保守ツール (DST) の使用 (Use dedicated service tools (DST))」画面が表示されます。
4. リストから適切なオプションを選択し、Enter キーを押す。
 - オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、保守ツール・ユーザー ID の処理オプションのメニューに進む。
 - オプション 7 (保守ツール開始 (Start a service tool)) を選択し、DST から使用できる保守ツールのいずれかを開始する。
 - 必要に応じ、その他のオプションを選択する。

手動 IPL から DST を使用して保守ツールにアクセスするには、以下のステップを実行してください。

1. コントロール・パネルを手動モードにする。
2. サーバーの電源がオフになっている場合、オンにする。
3. サーバーの電源をオンにして OS/400 を始動したら、OS/400 コマンド行に `PWRDWN SYS *IMMED RESTART(*YES)` コマンドを入力して、システムの電源の遮断とシステムの再始動を行う。
4. 自分の保守ツール・ユーザー ID とパスワードを使用して、DST にサインオンする。「専用保守ツール (DST) の使用 (Use dedicated service tools (DST))」画面が表示されます。
5. リストから適切なオプションを選択し、Enter キーを押す。
 - オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、保守ツール・ユーザー ID の処理オプションのメニューに進む。
 - オプション 7 (保守ツール開始 (Start a service tool)) を選択し、DST から使用できる保守ツールのいずれかを開始する。
 - 必要に応じ、その他のオプションを選択する。

SST による保守ツールへのアクセス

SST にアクセスする際に使用する保守ツール・ユーザー ID には、SST を使用できる機能特権が付与されている必要があります。OS/400 ユーザー・プロファイルには、以下の権限が付与されている必要があります。

- CL コマンド STRSST を使用できる権限
- サービス特殊権限 (*SERVICE)

SST を使用して保守ツールにアクセスするには、以下のステップを実行してください。

1. OS/400 コマンド行に STRSST (SST 開始) と入力する。「SST 開始のサインオン (Start SST Sign On)」画面が表示されます。
2. 次の情報を入力する。
 - **保守ツール・ユーザー ID (Service Tool User ID):** サインオンに使用する保守ツール・ユーザー ID。保守ツール・ユーザー ID を作成する方法の詳細については、『保守ツール・ユーザー ID の構成』を参照してください。
 - **パスワード (Password):** 上記のユーザー ID に関連付けられたパスワード。
3. Enter キーを押す。

iSeries ナビゲーターによる保守ツールへのアクセス

サーバーの電源がオンで DST が開始済みの場合、または OS/400 が稼働中の場合、iSeries ナビゲーターを使用して保守ツールにアクセスすることができます。

サーバーの電源がオンで DST が開始済みの場合に iSeries ナビゲーターを使用して保守ツールにアクセスするには、保守ツール・サーバーが DST 用に構成済みであり、かつ始動済みであることを確認してから、以下のステップを実行してください。

1. iSeries ナビゲーターで、「**ユーザー接続**」または自分のアクティブな環境を選択する。
2. タスクパッド・ウィンドウで「**iSeries ナビゲーターの保守ツール・ウィンドウのオープン (Open iSeries Navigator service tools window)**」を選択する。タスクパッド・ウィンドウが表示されていない場合は、「**表示**」を選択して「**タスクパッド (Taskpad)**」を選択します。
3. 項目「タスクパッド (Taskpad)」の選択後、接続先サーバーの IP アドレスを入力する。

OS/400 が稼働中の場合に iSeries ナビゲーターを使用して保守ツールにアクセスするには、保守ツール・サーバーが OS/400 用に構成済みであり、かつ始動済みであることを確認してから、以下のステップを実行してください。

1. iSeries ナビゲーターで、「**ユーザー接続**」または自分のアクティブな環境を展開する。
2. 操作対象の iSeries サーバーを選択する。
3. 使用する特定のサービス機能を選択する。
 - 論理区画を管理する場合は、「**構成およびサービス**」を展開する。次に「**論理区画**」を選択します。
 - ディスク装置を管理する場合は、「**構成およびサービス**」を展開する。次に「**ハードウェア**」を展開します。最後に「**ディスク装置**」を展開します。
4. 自分の保守ツール・ユーザー ID を使用してサインオンするよう求めるプロンプトが出される。

保守ツール・ユーザー ID の管理

保守ツール・ユーザー ID の管理と保守に有効な戦略を開発するには、以下を行う必要があります。

保守ツール・ユーザー ID の構成

保守ツール・ユーザー ID の作成、表示、使用可能化、使用禁止、削除、または保守ツール・ユーザー ID の機能特権の変更や説明の変更を行います。

保守ツール・ユーザー ID とパスワードの変更

DST、SST、STRSST (SST 開始)、または保守ツール・ユーザー ID 変更 (QSYCHGDS) API を使用して、保守ツール・ユーザー ID とパスワードを変更します。

QSECOFR のパスワードのリカバリーとリセット

OS/400 ユーザー・プロファイル QSECOFR と保守ツール・ユーザー ID QSECOFR の両方のパスワードをリカバリーまたはリセットします。

保守ツール・セキュリティー・データの保管と復元

重要な保守ツール・セキュリティー・データを保管および復元します。

保守ツール・ユーザー ID の管理に関する推奨事項

保守ツール・ユーザー ID の管理に関する IBM からの推奨事項を学習します。

保守ツール・ユーザー ID の構成

保守ツール・ユーザー ID は、専用保守ツール (DST) またはシステム保守ツール (SST) を使用して、作成、変更、削除、および表示することができます。保守ツール・ユーザー ID を構成すると、保守ツール・ユーザー ID とパスワードの変更が可能になります。

保守ツール・ユーザー ID の作成

DST または SST から保守ツール・ユーザー ID を作成するには、以下のステップを実行してください。

1. DST または SST を開始する。
2. 自分の保守ツール・ユーザー ID とパスワードを使用して、DST または SST にサインオンする。
 - DST では、「専用保守ツール (DST) の使用 (Use dedicated service tools (DST))」画面が表示される。オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、Enter キーを押します。「DST 環境処理 (Work with DST Environment)」画面が表示されます。次に、下記のステップ 3 に進みます。
 - SST では、「システム保守ツール (SST) (System Service Tools (SST))」メインメニューが表示される。オプション 8 (保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)) を選択します。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。次に、下記のステップ 4 に進みます。
3. 「DST 環境処理 (Work with DST Environment)」画面で、保守ツール・ユーザー ID を処理するために、オプション 3 (保守ツール・ユーザー ID (Service tools user IDs)) を選択する。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面で 1 (作成 (Create)) と入力し、表示されたフィールドに新しい保守ツール・ユーザー ID を入力して Enter キーを押す。「保守ツール・ユーザー ID の作成 (Create Service Tools User ID)」画面が表示されます。

注: ユーザー ID には 1 ~ 10 個の文字を使用できます。使用できる文字は、英大文字、数字、および特殊文字 (#, @, \$, または _) です。特殊文字は、ユーザー ID の先頭文字として使用できません。ユーザー ID の文字間にスペースを入れることはできません。

5. 新規ユーザー ID についての情報を入力する。
 - **ユーザー名 (Username):** 新規保守ツール・ユーザー ID の名前が表示されます。
 - **パスワード (Password):** このパスワードは、新規ユーザー ID によって使用されます。1 文字以上の長さが必要です。この他に適用されるパスワード規則はありません。
 - **ストレージ管理 (記憶域管理) のリカバリーの前にユーザー ID のアクセスを許可する (Allow user ID access before storage management recovery):** このフィールドのデフォルト値は 2 (いいえ) です。
 - **パスワードを有効期限切れに設定する (Set password to expired):** このフィールドのデフォルト値は 1 (はい) です。
 - **説明 (Description):** オプションのフィールドです。ユーザー ID の所有者についての詳細情報 (名前、部門、電話番号など) を入力するために使用できます。
6. ユーザー ID に関する情報の入力をすべて完了したら、次の 2 つのオプションのいずれかを選択する。
 - デフォルトの機能特権を持つユーザー ID を作成するには、Enter キーを押す。
 - 付与する機能特権をデフォルトから変更するには、F5 を押して「保守ツール・ユーザー ID の特権の変更 (Change Service Tools User ID Privileges)」画面を表示する。この画面には、特権の対象となる保守ツールのすべてがリスト表示されます。機能特権の変更の詳細については、『保守ツール・ユーザー ID とパスワードの変更』を参照してください。

保守ツール・ユーザー ID の機能特権の変更

DST または SST から保守ツール・ユーザー ID の機能特権を変更するには、以下のステップを実行してください。

1. DST または SST を開始する。
2. 自分の保守ツール・ユーザー ID とパスワードを使用して、DST または SST にサインオンする。
 - DST では、「専用保守ツール (DST) の使用 (Use dedicated service tools (DST))」画面が表示される。オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、Enter キーを押します。「DST 環境処理 (Work with DST Environment)」画面が表示されます。次に、下記のステップ **3** に進みます。
 - SST では、「システム保守ツール (SST) (System Service Tools (SST))」メインメニューが表示される。オプション 8 (保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)) を選択します。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。次に、下記のステップ **4** に進みます。
3. 「DST 環境処理 (Work with DST Environment)」画面で、保守ツール・ユーザー ID を処理するために、オプション 3 (保守ツール・ユーザー ID (Service tools user IDs)) を選択する。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面で、変更するユーザー ID を選択して「オプション」フィールドに 7 (特権の変更 (Change privileges)) と入力する。「保守ツール・ユーザーの特権の変更 (Change Service Tools User Privileges)」画面が表示されます。
 - a. ユーザー ID から除去する機能特権の隣の「オプション」フィールドに、1 (取り消し (Revoke)) と入力する。
 - b. ユーザー ID に追加する機能特権の隣の「オプション」フィールドに、2 (付与 (Grant)) と入力する。
5. Enter キーを押し、これらの変更を有効にする。Enter キーを押す前に F3 (終了) を押すと、変更は有効になりません。F9 (デフォルト (Defaults)) を押すと、機能特権はデフォルト値にリセットされます。

保守ツール・ユーザー ID の説明の変更

DST または SST から保守ツール・ユーザー ID の説明を変更するには、以下のステップを実行してください。

1. DST または SST を開始する。
2. 自分の保守ツール・ユーザー ID とパスワードを使用して、DST または SST にサインオンする。
 - DST では、「専用保守ツール (DST) の使用 (Use dedicated service tools (DST))」画面が表示される。オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、Enter キーを押します。「DST 環境処理 (Work with DST Environment)」画面が表示されます。次に、下記のステップ **3** に進みます。
 - SST では、「システム保守ツール (SST) (System Service Tools (SST))」メインメニューが表示される。オプション 8 (保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)) を選択します。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。次に、下記のステップ **4** に進みます。
3. 「DST 環境処理 (Work with DST Environment)」画面で、保守ツール・ユーザー ID を処理するために、オプション 3 (保守ツール・ユーザー ID (Service tools user IDs)) を選択する。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面で、変更するユーザー ID の説明を選択して「オプション」フィールドに 8 (説明の変更 (Change description)) と入力する。
5. 「説明 (Description)」フィールドに、ユーザー ID の新しい説明を入力する。ユーザー名、部門、電話番号などを入力できます。

保守ツール・ユーザー ID の表示

DST または SST で保守ツール・ユーザー ID を表示するには、以下のステップを実行してください。

1. DST または SST を開始する。
2. 自分の保守ツール・ユーザー ID とパスワードを使用して、DST または SST にサインオンする。
 - DST では、「専用保守ツール (DST) の使用 (Use dedicated service tools (DST))」画面が表示される。オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、Enter キーを押します。「DST 環境処理 (Work with DST Environment)」画面が表示されます。次に、下記のステップ **3** に進みます。
 - SST では、「システム保守ツール (SST) (System Service Tools (SST))」メインメニューが表示される。オプション 8 (保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)) を選択します。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。次に、下記のステップ **4** に進みます。
3. 「DST 環境処理 (Work with DST Environment)」画面で、保守ツール・ユーザー ID を処理するために、オプション 3 (保守ツール・ユーザー ID (Service tools user IDs)) を選択する。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面で、表示するユーザー ID を選択して「オプション」フィールドに 4 (表示 (Display)) と入力する。「保守ツール・ユーザー ID の表示 (Display Service Tools User ID)」画面が表示されます。この画面には、次のようなユーザー ID 関連の情報が表示されます。
 - 直前のサインオン (日時)
 - 無効なサインオンの試み
 - 状況

- パスワードの最終変更日 (Date password last changed)
 - ストレージ管理のリカバリーの前にユーザー ID のアクセスを許可する (Allow user ID access before storage management recovery) (「はい」または「いいえ」)
 - パスワード失効日 (Date password expires)
 - パスワードの有効期限切れ設定 (Password set to expire) (「はい」または「いいえ」)
5. 選択したユーザー ID に関連付けられている機能特権を表示するには、F5 (特権の表示 (Display privileges)) を押す。「保守ツール・ユーザーの特権の表示 (Display Service Tools User Privileges)」画面が表示されます。この画面には、それぞれの機能特権とユーザー状況のすべてがリスト表示されます。この画面から、ユーザー ID に変更を加えることはできません。

保守ツール・ユーザー ID の使用可能化と使用禁止

DST または SST から保守ツール・ユーザー ID を使用可能にするには、以下のステップを実行してください。

1. DST または SST を開始する。
2. 自分の保守ツール・ユーザー ID とパスワードを使用して、DST または SST にサインオンする。
 - DST では、「専用保守ツール (DST) の使用 (Use dedicated service tools (DST))」画面が表示される。オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、Enter キーを押します。「DST 環境処理 (Work with DST Environment)」画面が表示されます。次に、下記のステップ 3 に進みます。
 - SST では、「システム保守ツール (SST) (System Service Tools (SST))」メインメニューが表示される。オプション 8 (保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)) を選択します。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。次に、下記のステップ 4 に進みます。
3. 「DST 環境処理 (Work with DST Environment)」画面で、保守ツール・ユーザー ID を処理するために、オプション 3 (保守ツール・ユーザー ID (Service tools user IDs)) を選択する。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面で、使用可能にするユーザー ID を選択して「オプション」フィールドに 5 (使用可能 (Enable)) と入力する。「保守ツール・ユーザー ID の使用可能 (Enable Service Tools User ID)」画面が表示されます。
5. Enter キーを押して、選択した保守ツール・ユーザー ID を使用可能にすることを確認する。

DST または SST から保守ツール・ユーザー ID を使用不可にするには、以下のステップを実行してください。

1. DST または SST を開始する。
2. 自分の保守ツール・ユーザー ID とパスワードを使用して、DST または SST にサインオンする。
 - DST では、「専用保守ツール (DST) の使用 (Use dedicated service tools (DST))」画面が表示される。オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、Enter キーを押します。「DST 環境処理 (Work with DST Environment)」画面が表示されます。次に、下記のステップ 3 に進みます。
 - SST では、「システム保守ツール (SST) (System Service Tools (SST))」メインメニューが表示される。オプション 8 (保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)) を選択します。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。次に、下記のステップ 4 に進みます。

3. 「DST 環境処理 (Work with DST Environment)」画面で、保守ツール・ユーザー ID を処理するために、オプション 3 (保守ツール・ユーザー ID (Service tools user IDs)) を選択する。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面で、使用不可にするユーザー ID を選択して「オプション」フィールドに 6 (使用不可 (Disable)) と入力する。「保守ツール・ユーザー ID の使用不可 (Disable Service Tools User ID)」画面が表示されます。
5. Enter キーを押して、選択した保守ツール・ユーザー ID を使用不可にすることを確認する。

保守ツール・ユーザー ID の削除

保守ツール・ユーザー ID の削除は、DST または SST から行うことができます。IBM 提供の保守ツール・ユーザー ID は削除できません。保守ツール・ユーザー ID を削除するには、以下のステップを実行してください。

1. DST または SST を開始する。
2. 自分の保守ツール・ユーザー ID とパスワードを使用して、DST または SST にサインオンする。
 - DST では、「専用保守ツール (DST) の使用 (Use dedicated service tools (DST))」画面が表示される。オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、Enter キーを押します。「DST 環境処理 (Work with DST Environment)」画面が表示されます。次に、下記のステップ **3** に進みます。
 - SST では、「システム保守ツール (SST) (System Service Tools (SST))」メインメニューが表示される。オプション 8 (保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)) を選択します。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。次に、下記のステップ **4** に進みます。
3. 「DST 環境処理 (Work with DST Environment)」画面で、保守ツール・ユーザー ID を処理するために、オプション 3 (保守ツール・ユーザー ID (Service tools user IDs)) を選択する。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面で、削除するユーザー ID を選択して「オプション」フィールドに 3 (削除) と入力する。「保守ツール・ユーザー ID の削除 (Delete Service Tools User ID)」画面が表示されます。
5. ユーザー ID の削除を選択したことを確認するプロンプトが出される。
 - 選択したユーザー ID を削除するには、Enter キーを押す。
 - 操作を取り消すには、F12 (取り消し (Cancel)) を押して、「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面に戻る。

保守ツール・ユーザー ID とパスワードの変更

ここでは、保守ツール・ユーザー ID とパスワードの変更方法について説明します。既存の保守ツール・ユーザー ID とパスワードを変更するには、その前に自分の保守ツール・ユーザー ID の構成を済ませておく必要があります。また、保守ツール・ユーザー ID の管理に関する推奨事項を確認しておくことをお勧めします。

重要: 全 OS/400 セキュリティー担当者プロファイルのパスワードおよび全保守ツール・ユーザー ID のパスワードを紛失した場合や忘れてしまった場合、これらのパスワードをリカバリーするには、配布メディアを使用してシステムをインストールおよび初期化しなければならないことがあります。サービス提供元に連絡をとって、援助を依頼してください。OS/400 セキュリティー担当者プロファイルのパスワードまたは保守ツール・ユーザー ID のパスワードのいずれかがわかっている場合は、トピック『QSECOFR のパスワードのリカバリーとリセット』に記載されている、不明なパスワードをリカバリーする方法を参照してください。

保守ツール・ユーザー ID とパスワードを変更する方法はいくつかあります。DST または SST を使用するか、STRSST (SST 開始) と F9 を使用するか、あるいは保守ツール・ユーザー ID 変更 (QSYCHGDS) API を使用することができます。

SST または DST による保守ツール・ユーザー ID とパスワードの変更

保守ツール・ユーザー ID とパスワードの変更は、SST または DST を使用して行うことができます。**DST** を使用して保守ツール・ユーザー ID のパスワードを変更する場合、以下のステップを実行してください。

1. DST を開始する。
2. 自分の保守ツール・ユーザー ID とパスワードを使用して、DST にサインオンする。「専用保守ツール (DST) の使用 (Use dedicated service tools (DST))」画面が表示されます。
3. オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、Enter キーを押す。「DST 環境処理 (Work with DST Environment)」画面が表示されます。
4. 「DST 環境処理 (Work with DST Environment)」画面で、保守ツール・ユーザー ID を処理するために、オプション 3 (保守ツール・ユーザー ID (Service tools user IDs)) を選択する。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。
5. 「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面で、変更するユーザー ID を探して「オプション」フィールドに 2 (パスワードの変更 (Change password)) と入力する。
 - a. 他のユーザーの保守ツール・ユーザー ID を変更できる保守ツール・セキュリティ特権が自分自身に付与されている場合は、「別のユーザーの保守ツール・ユーザー・パスワードの変更 (Change Service Tools User Password for Another User)」画面が表示される。選択した保守ツール・ユーザー ID の名前が表示されます。これが、変更しようとしているユーザー ID の名前であることを確認します。確認後、以下のフィールドに入力します。
 - **新規パスワード (New password):** 新規パスワードを入力します。
 - **パスワードを有効期限切れに設定する (Set Password to expired):** 1 (はい) または 2 (いいえ) を入力します。デフォルト値は 1 (はい) です。
 - b. 他のユーザーの保守ツール・ユーザー ID を変更できるシステム管理特権が自分自身に付与されていない場合は、「保守ツール・ユーザー・パスワードの変更 (Change Service Tools User Password)」画面が表示される。以下のフィールドに入力します。
 - **現行パスワード (Current password):** 選択した保守ツール・ユーザー ID の現在使用されているパスワードを入力します。
 - **新規パスワード (New password):** 新規パスワードを入力します。ここで入力するパスワードは、選択した保守ツール・ユーザー ID の以前のパスワードのうち、直前に使用された 18 個のいずれかと同じものにはできません。
 - **新規パスワード (確認用) (New password (to verify)):** 新規パスワードをもう一度入力します。
6. Enter キーを押して変更を完了する。新規パスワードが受け入れられない場合、そのパスワードは、選択した保守ツール・ユーザー ID のパスワード・ポリシーに適合していない可能性があります。保守ツール・ユーザー ID のパスワードを選択する際には、パスワード・ポリシーを確認し、パスワードがパスワード・ポリシーに適合するようにします。

SST を使用して保守ツール・ユーザー ID のパスワードを変更する場合、以下のステップを実行してください。

1. SST を開始する。

2. 保守ツール・セキュリティー特権を付与されている保守ツール・ユーザー ID とパスワードを使用して、SST にサインオンする。「システム保守ツール (SST) (System Service Tools (SST))」メインメニューが表示される。
3. 「システム保守ツール (SST) (System Service Tools (SST))」メインメニューで、オプション 8 (保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)) を選択する。「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理 (Work with Service Tools User IDs)」画面で、変更するユーザー ID を探して「オプション」フィールドに 2 (パスワードの変更 (Change password)) と入力する。
5. 「別のユーザーの保守ツール・ユーザー・パスワードの変更 (Change Service Tools User Password for Another User)」画面が表示される。選択した保守ツール・ユーザー ID の名前が表示されます。この名前が変更しようとしているユーザー ID の名前であることを確認してから、以下のフィールドに入力します。
 - **新規パスワード (New password):** 新規パスワードを入力します。
 - **パスワードを有効期限切れに設定する (Set Password to expired):** 1 (はい) または 2 (いいえ) を入力します。デフォルト値は 1 (はい) です。
6. Enter キーを押して変更を完了する。新規パスワードが受け入れられない場合、そのパスワードは、選択した保守ツール・ユーザー ID のパスワード・ポリシーに適合していない可能性があります。保守ツール・ユーザー ID のパスワードを選択するには、パスワード・ポリシーを確認し、パスワードがパスワード・ポリシーに適合するようにします。

STRSST による自分の保守ツール・ユーザー ID のパスワードの変更

STRSST を使用して自分の保守ツール・ユーザー ID のパスワードを変更するには、以下のステップを実行してください。

1. STRSST コマンドのサインオン・パネルで自分の保守ツール・ユーザー ID を入力し、F9 (パスワードの変更 (Change Password)) を押す。「パスワードの変更 (Change Password)」画面が表示されます。
2. 「パスワードの変更 (Change Password)」画面で、現行パスワードと新規パスワードを入力し、さらに確認のため新規パスワードをもう一度入力する。ここで入力するパスワードは、直前に使用した 18 個のパスワードのいずれかと同じものにすることはできません。直前に使用したパスワードのいずれかを使用しようとすると、エラー・メッセージが表示されます。Enter キーを押します。

すべてのパスワードが正しく入力され、新規パスワードが受け入れられると、その新規パスワードを使用してサインオンできるようになります。新規パスワードが受け入れられない場合、そのパスワードは、保守ツール・ユーザー ID のパスワード・ポリシーに適合していない可能性があります。保守ツール・ユーザー ID のパスワードを選択するには、パスワード・ポリシーを確認し、パスワードがパスワード・ポリシーに適合するようにします。

保守ツール・ユーザー ID 変更 (QSYCHGDS) API による保守ツール・ユーザー ID とパスワードの変更

保守ツール・ユーザー ID 変更 (QSYCHGDS) API を使用すると、自分の保守ツール・ユーザー ID とパスワードを変更することができます。また、十分な特権が付与されている場合には、別のユーザーの保守ツール・ユーザー ID とパスワードを変更することもできます。さらに、この API は、複数の iSeries サーバーがあり、かつそれらのサーバーのすべてにまたがって保守ツール・ユーザー ID を管理する必要がある場合に役立ちます。

QSECOFR のパスワードのリカバリーとリセット

サーバーが IBM から出荷される時点で、OS/400 ユーザー・プロファイル QSECOFR と、保守ツール・ユーザー ID QSECOFR の両方が提供されています。これらは同じものではありません。これらはそれぞれ

異なる場所に存在し、異なる機能へのアクセスのために使用されます。保守ツール・ユーザー ID QSECOFR には、OS/400 ユーザー・プロファイル QSECOFR とは異なるパスワードを設定できます。保守ツール・ユーザー ID と OS/400 ユーザー・プロファイルのパスワード・ポリシーは異なります。

OS/400 ユーザー・プロファイル QSECOFR のパスワードと保守ツール・ユーザー ID QSECOFR のパスワードの両方を紛失した場合や忘れてしまった場合、これらのパスワードをリカバリーするには、オペレーティング・システムを再インストールしなければならないことがあります。サービス提供元に連絡をとって、援助を依頼してください。これらのパスワードのいずれかがわかっている場合は、ここで説明する、不明なパスワードをリカバリーする方法を参照してください。

OS/400 ユーザー・プロファイル QSECOFR のパスワードのリセット

保守ツール・ユーザー ID QSECOFR のパスワードがわかっている場合、そのパスワードを使用して、OS/400 ユーザー・プロファイル QSECOFR のパスワードを初期値 (QSECOFR) にリセットすることができます。この手順を使用する場合、サーバー上で初期プログラム・ロード (IPL) を実行しなければなりません。ここで行う変更は、IPL の実行が完了するまで、有効になりません。OS/400 ユーザー・プロファイル QSECOFR のパスワードをリセットするには、以下のステップを実行してください。

1. DST を開始する。
2. 「DST サインオン (DST Sign-On)」画面で、保守ツール・ユーザー ID QSECOFR とパスワードを入力する。
3. 「DST の使用 (Use DST)」メニューで、オプション 5 (DST 環境処理 (Work with DST environment)) を選択する。
4. 「DST 環境処理 (Work with DST Environment)」メニューで、オプション 6 (保守ツール・セキュリティー・データの処理 (Work with Service Tools Security Data)) を選択する。次のような「保守ツール・セキュリティー・データの処理 (保守ツール機密保護データの処理)」メニューが表示されます。

```
+-----+
|                保守ツール機密保護データの処理                |
|                                                                |
|                                                                |
|                                                                |
|                システム :                |
|                                                                |
|  次の 1 つを選択してください。                |
|                                                                |
|  1. オペレーティング・システムのシステム省略時パスワードのリセット                |
|  2. オペレーティング・システム導入機密保護の変更                |
|  3. 保守ツール機密保護ログの処理                |
|  4. 保守ツール機密保護データの復元                |
|  5. 保守ツール機密保護データの保管                |
|  6. パスワード・レベル                |
|  選択項目                |
+-----+
```

5. オプション 1 (オペレーティング・システムのデフォルト (省略時) パスワードのリセット) を選択する。「システム・デフォルト・パスワードへのリセットの確認 (Confirm Reset of System Default Password)」画面が表示されます。

6. Enter キーを押してリセットを確認する。システム上でオペレーティング・システムのパスワードのオーバーライドが設定されたことを示す、確認メッセージが表示されます。
7. 「DST の終了 (Exit DST)」メニューに戻るまで、F3 (終了) を押す。
8. オプション 1 (DST の終了 (Exit DST)) を選択する。「IPL/システムのインストール (IPL or Install the System)」メニューが表示されます。
9. オプション 1 (IPL の実行 (Perform an IPL)) を選択する。システムは、手動 IPL で続行します。IPL の実行に関する追加情報については、トピック『iSeries の開始と停止』を参照してください。
10. IPL が完了したら、キーロック・スイッチまたは電子キースティックを自動位置に戻す (これらが存在する場合)。
11. QSECOFR として OS/400 にサインオンする。CHGPWD コマンドを使用して、QSECOFR のパスワードを新しい値に変更します。新しい値を安全な場所に保管します。

重要: QSECOFR のパスワードの値をデフォルト設定のままにしないでください。この値は、どの iSeries サーバーにも出荷時に共通に設定される値であるため一般によく知られており、そのままにすると機密漏れにつながります。

保守ツール・ユーザー ID QSECOFR とそのパスワードのリセット

OS/400 ユーザー・プロファイル QSECOFR のパスワードがわかっている場合、そのパスワードを使用して、保守ツール・セキュリティ特権を付与されている IBM 提供の保守ツール・ユーザー ID (QSECOFR) のパスワードを、IBM 提供のデフォルト値にリセットすることができます。これを行うには、以下のステップを実行してください。

1. サーバーを、DST ではなく、通常の操作モードにする。
2. OS/400 ユーザー・プロファイル QSECOFR を使用して、ワークステーションにサインオンする。
3. コマンド行に、CHGDSTPWD (IBM 保守ツール・パスワード変更) と入力する。次のような「DST パスワード変更 (CHGDSTPWD)」画面が表示されます。

```

+-----+
|                DST パスワード変更 (CHGDSTPWD)                |
|                                                                |
|  選択項目を入力して、実行キーを押してください。            |
|                                                                |
|  DST 機密保護担当者パスワード      *DEFAULT      *SAME, *DEFAULT  |
|                                                                |
+-----+

```

4. *DEFAULT と入力し、Enter (実行) キーを押す。これにより、保守ツール・セキュリティ特権を付与されている IBM 提供の保守ツール・ユーザー ID およびそのパスワードが、QSECOFR に設定されます。

重要: 保守ツール・ユーザー ID QSECOFR とそのパスワードの値をデフォルト設定のままにしないでください。この値は、どの iSeries サーバーにも出荷時に共通に設定される値であるため一般によく知られており、そのままにすると機密漏れにつながります。詳しくは、『保守ツール・ユーザー ID の管理に関する推奨事項』を参照してください。

保守ツール・セキュリティ・データの保管と復元

保守ツール・セキュリティ・データの保管は、システム保管 (SAVSYS) またはライセンス内部コード (LIC) 保管による処理の一部として行われます。DST を使用して手動で行うこともできます。保守ツール・セキュリティ・データは、DST から処理できます。

保守ツール・セキュリティ・データの保管

DST を使用して保守ツール・セキュリティ・データを保管するには、以下のステップを実行してください。

1. 「DST 環境処理 (Work with DST Environment)」画面で、オプション 6 (保守ツール・セキュリティ・データ (Service tools security data)) を選択する。
2. 「保守ツール・セキュリティ・データの処理 (保守ツール機密保護データの処理)」画面で、オプション 5 (保守ツール・セキュリティ・データの保管 (保守ツール機密保護データの保管)) を選択する。「保守ツール・セキュリティ・データの保管 (Save Service Tools Security Data)」画面が表示されます。
3. ストレージ装置が使用可能であることを確認してから、選択可能なオプションのうちのいずれか 1 つを選択する。
 - テープ
 - a. 保管するには、Enter キーを押す。「磁気テープ装置の操作 (Work with Tape Devices)」画面が表示されます。
 - b. 表示された磁気テープ装置のいずれかを選択、選択解除、または詳細表示できる。セキュリティ・データを保管する磁気テープ装置の隣の「オプション」フィールドに、適切な値を入力します。
 - 光ディスク (Optical)
 - a. 保管するには、Enter キーを押す。「光ディスク装置の操作 (Work with Optical Devices)」画面が表示されます。
 - b. 表示された光ディスク装置のいずれかを選択、選択解除、または詳細表示できる。セキュリティ・データを保管する光ディスク装置の隣の「オプション」フィールドに、適切な値を入力します。

保守ツール・セキュリティ・データの復元

DST を使用して保守ツール・セキュリティ・データを復元するには、以下のステップを実行してください。

1. 「DST 環境処理 (Work with DST Environment)」画面で、オプション 6 (保守ツール・セキュリティ・データ (Service tools security data)) を選択する。
2. 「保守ツール・セキュリティ・データの処理 (保守ツール機密保護データの処理)」画面で、オプション 4 (保守ツール・セキュリティ・データの復元 (保守ツール機密保護データの復元)) を選択する。「メディア・タイプの選択 (Select Media Type)」画面が表示されます。
3. ストレージ装置が使用可能であることを確認し、選択可能なオプションのうちのいずれか 1 つを選択する。
 - テープ
 - a. 復元するには、Enter キーを押す。「磁気テープ装置の操作 (Work with Tape Devices)」画面が表示されます。
 - b. 表示された磁気テープ装置のいずれかを選択、選択解除、または詳細表示できる。選択した場合は、ステップ 4 に進みます。

- 光ディスク (Optical)
 - a. 復元するには、Enter キーを押す。「光ディスク装置の操作 (Work with Optical Devices)」画面が表示されます。
 - b. 表示された光ディスク装置のいずれかを選択、選択解除、または詳細表示できる。選択した場合は、ステップ 4 に進みます。
- 4. 復元するセキュリティー・データの取り出し元装置を選択する手順は、磁気テープ装置と光ディスク装置で共通である。
 - a. 操作するリソースの隣のオプション・フィールドに、1 (選択 (Select)) と入力する。「保守ツール・ユーザー ID の復元 (Restore Service Tools User ID)」画面が表示されます。
 - b. 以下のオプションのうちいずれか 1 つを選択する。
 - すべての保守ツール・ユーザー ID を復元する場合
 - 1) 「オプション」フィールドに 1 と入力する。
 - 2) Enter キーを押す。すべての保守ツール・ユーザー ID が復元されます。
 - 復元する保守ツール・ユーザー ID を選択する場合
 - 1) 「オプション」フィールドに 2 と入力し、Enter キーを押す。「復元する保守ツール・ユーザー ID の選択 (Select Service Tools User ID to Restore)」画面が表示されます。
 - 2) 復元するプロファイルの隣の「オプション」フィールドに、1 (選択 (Select)) と入力する。Enter キーを押します。選択した保守ツール・ユーザー ID が復元されます。

保守ツール・ユーザー ID の管理に関する推奨事項

以下は、保守ツール・ユーザー ID の管理に関する推奨事項です。

独自の QSECOFR 保守ツール・ユーザー ID の作成

IBM 提供の保守ツール・ユーザー ID である QSECOFR を使用しないでください。代わりに、QSECOFR に付与されている機能特権を確認し、同じ機能特権を持つユーザー ID を別の名前で複製します。詳しい手順については、『保守ツール・ユーザー ID とパスワードの変更』を参照してください。この新しく作成したユーザー ID を使用して、他の保守ツール・ユーザー ID を管理するようにします。QSECOFR はどのサーバーの出荷時にも共通に設定される値であるため一般によく知られており、QSECOFR の使用は機密漏れにつながりますが、このようにすることで機密漏れを防ぐことができます。

保守ツール・セキュリティー機能特権

保守ツール・セキュリティー機能特権は、ある保守ツール・ユーザー ID に、その他の保守ツール・ユーザー ID の作成と管理を許可する特権です。これは強力な特権なので、QSECOFR と同等の保守ツール・ユーザー ID のみに付与する必要があります。この機能特権をどの相手に付与するかについては、注意して検討してください。

保守ツール・サーバーの構成

保守ツール・サーバーは、DST 用または OS/400 用 (あるいはその両方用) に構成することができます。

保守ツール・サーバーの構成 (DST 用)

保守ツール・サーバーを構成して使用可能にできるのは、あらかじめサーバーの電源をオンにし、DST を開始済みに行っている場合です。LAN に接続可能なオペレーション・コンソールのみを使用して DST アクティビティーを実行している場合は、サーバーの電源がオンにされて DST が開始済みになった時点で保守ツール・サーバーが使用可能になっているので、保守ツール・サーバーを再構成する必要はありません。

保守ツール・サーバーを DST 経由で使用できるようにするには、1 個のネットワーク・インターフェース・カードを保守ツール・サーバー専用にします。専用のネットワーク・インターフェース・カードを持つ保守ツール・サーバーを使用可能にするには、以下のステップを実行してください。

1. 「専用保守ツールの使用 (Use dedicated service tools (DST))」画面で、オプション 5 (DST 環境処理 (Work with DST environment)) を選択し、Enter キーを押す。「DST 環境処理 (Work with DST Environment)」画面が表示されます。
2. 「DST 環境処理 (Work with DST Environment)」画面で、オプション 2 (システム装置 (System devices)) を選択し、Enter キーを押す。「システム装置の操作 (Work with System Devices)」画面が表示されます。
3. 「システム装置の操作 (Work with System Devices)」画面で、オプション 6 (コンソール・モード (Console mode)) を選択し、Enter キーを押す。「コンソール・タイプの選択 (Select Console Type)」画面が表示されます。
4. 「コンソール・タイプの選択 (Select Console Type)」画面で、F11 (構成) を押す。「保守ツール・アダプターの構成 (Configure Service Tools Adapter)」画面が表示されます。
5. 「保守ツール・アダプターの構成 (Service Tools Adapter)」画面で、LAN アダプターと TCP/IP の情報を入力する。各フィールドに必要な情報のタイプを調べるには、F1 (ヘルプ (Help)) を押します。
6. F7 (保管 (Store)) を押し、変更を保管する。
7. F14 (活動化) を押し、アダプターをアクティブにする。

これで、有効な保守ツール・ユーザー ID を使用して、保守ツール・サーバーを使用できるようになりました。

保守ツール・サーバーの構成 (OS/400 用)

OS/400 上の保守ツールに TCP/IP および iSeries ナビゲーターを使用してアクセスするには、サービス・テーブルに保守ツール・サーバーを追加する必要があります。保守ツール・サーバーの追加は、ローカル・エリア・ネットワーク (LAN) を構成する前に行うことができます。サービス・テーブルに保守ツール・サーバーを追加するには、以下のステップを実行してください。

1. コマンド行に ADDSRVTBLE (サービス・テーブル項目追加) と入力し、Enter キーを押す。「サービス・テーブル項目の追加 (Add Service Table Entry)」画面が表示されます。
2. 表示されたフィールドに、以下の情報を入力する。
 - サービス: as-sts
 - ポート: 3000
 - プロトコル: 'tcp' (このエントリーは小文字で入力する必要があります。また前後には単一引用符が必要です。)
 - テキスト記述 (Text description): 'Service Tools Server'
このフィールドはオプションですが、テーブル・エントリーの説明を入力することを強くお勧めします。
3. F10 (追加のパラメーター) を押す。
4. 「別名 (Alias)」フィールドに AS-STs と入力する。テーブル検索には大文字小文字を区別するものがあるので、この別名は、大文字で入力しなければなりません。
5. Enter キーを押し、テーブル・エントリーを追加する。
6. 追加したサービス・テーブル・エントリーを使用可能にするには、TCP/IP を終了して再開する。TCP をここで終了しなければ、保守ツール・サーバーは使用可能になりません。使用中の環境で TCP/IP の終了が可能であれば、ENDTCP (TCP 終了) と入力して TCP/IP を終了します。

7. STRTCP (TCP 開始) と入力する。5250 セッションから NETSTAT OPTION(*CNN) と入力して、保守ツール・サーバーがポート 3000 を listen していることを確認します。見出し「ローカル・ポート (Local Port)」の下で as-sts を探し、listen 状態値 (State value of Listen) を確認します。

iSeries ナビゲーターを使用してディスク装置または論理区画の構成と管理を実行する予定がある場合は、以下のステップをサーバーごとに 1 回ずつ実行する必要があります。

1. iSeries ナビゲーター・セッションの「**ユーザー接続**」の下で、サーバー名を右マウス・ボタンでクリックする (実際の環境では、接続機能の名前として、独自の名前をデフォルトの「**ユーザー接続**」の代わりに使用できます)。
2. 「**アプリケーション管理**」を選択する。「**ホスト・アプリケーション**」タブがあるウィンドウが開かれるまで、「**OK**」を押します。「**ホスト・アプリケーション**」タブを選択して「**オペレーティング・システム/400 (Operating System/400)**」を展開し、「**サービス**」を展開します。
3. 保守ツール「**ディスク装置**」、「**QIBM_QYTP_SERVICE_LPARMGMT**」、または「**サービス・トレース (Service Trace)**」のうち、許可するものを選択する。複数選択することもできます。
4. 「**OK**」を押す。これで、iSeries ナビゲーターのユーザーが、選択された機能を使用できるようになりました (ただし、ユーザーが保守ツール・ユーザー ID を持っていることが条件です)。

サービス・テーブルへの保守ツール・サーバーの追加が完了すると、許可ユーザーは、iSeries ナビゲーターと TCP/IP を使用して、論理区画 (LPAR) 管理サービス機能およびディスク管理サービス機能にアクセスできるようになります。保守ツール・ユーザー ID の場合と同様に、機能特権を使用することによって、ユーザーに特定のサービス機能の使用を選択的に認可または制限することができる点に注意してください。

サービス機能の使用のモニター

DST を使用して、サービス機能の使用をモニターすることができます。また、OS/400 セキュリティー監査ログを使用して、保守ツールの使用をモニターすることができます。このログは、異常アクセス・パターンまたはその他の潜在的なセキュリティ上のリスクをトレースするのに役立ちます。

DST によるサービス機能の使用のモニター

ユーザーが保守ツール・ユーザー ID を使用して DST にサインオンすると、このイベントは必ず保守ツール・セキュリティ・ログに記録されます。

保守ツール・セキュリティ・ログを処理するには、以下のステップを実行してください。

1. DST を開始する。
2. 「DST サインオン (DST Sign-On)」画面で、保守ツール・ユーザー ID QSECOFR とパスワードを入力する。
3. 「DST の使用 (Use DST)」メニューで、オプション 5 (DST 環境処理 (Work with DST environment)) を選択する。
4. 「DST 環境処理 (Work with DST Environment)」メニューで、オプション 6 (保守ツール・セキュリティ・データの処理 (Work with Service Tools Security Data)) を選択する。次のような「保守ツール・セキュリティ・データの処理 (保守ツール機密保護データの処理)」メニューが表示されます。

- アクティビティーの説明 (Activity description)
- 影響を受けたユーザー ID (Affected user ID)

OS/400 セキュリティー監査ログによる保守ツールの使用のモニター

OS/400 セキュリティー監査ログは、保守ツール・アクションの記録に使用できます。OS/400 セキュリティー監査ログに保守ツール・アクションを記録できるようにするには、このログを使用可能にする必要があるサーバーごとに以下のステップを実行してください。

1. iSeries ナビゲーター・セッションの「**ユーザー接続**」の下で、サーバー名を選択する (実際の環境では、接続機能の名前として、独自の名前をデフォルトの「**ユーザー接続**」の代わりに使用できます)。全オブジェクト (*ALLOBJ) 特殊権限と全監査 (*ALLAUDIT) 特殊権限の両方を付与されている ID を使用してサインオンします。
2. 「**セキュリティー**」を展開して「**ポリシー**」を選択し、「**監査ポリシー (Auditing policy)**」をダブルクリックする。
3. 「**システム**」タブを選択する。以下の項目にチェックマークが付いていることを確認します (その他の項目にもチェックマークが付いていることがあります)。
 - アクション監査の活動化 (Activate action auditing)
 - セキュリティー・タスク
 - サービス・タスク
4. 「**OK**」を押す。これで、iSeries サーバー上で、選択したセキュリティー監査ログ機能が使用可能になりました。

セキュリティー監査ログ機能の使用可能化が完了すると、ログ情報がジャーナル・レシーバーに表示されるようになります。ジャーナル・レシーバー内の現在の保守ツール・アクション・エントリーにアクセスするには、OS/400 コマンド行にコマンド `DSPJRN QSYS/QAUDJRN ENTYP(ST)` を入力します。

ジャーナル・レシーバー内の保守ツール・アクション・エントリーにアクセスすると、保守ツール・ユーザー ID ごとの保守ツール監査エントリーを確認することができます。これらの監査エントリーには、SST または DST へのログオン、保守ツール・ユーザー ID のパスワードの変更、保守ツールへのアクセスなどのアクションが含まれます。この監査エントリーの完全なリストと関連情報については、「iSeries 機密保

護解説書」 を参照してください。

保守ツールのトラブルシューティング

本トピックでは、保守ツールに問題が発生した場合の解決方法について説明します。また、サポート・センターへの問題の報告についても説明しています。

問題 1: パスワードが正しくないというエラー・メッセージが表示される。

パスワードの大文字小文字を正しく区別して入力したかどうかを確認してください。IBM 提供の保守ツール・ユーザー ID のパスワードは、英大文字です。パスワードを変更済みの場合は、パスワード変更の際に入力したパスワードと大文字小文字の区別を同一にして、パスワードを入力してください。

問題 2: 保守ツール・ユーザー ID QSECOFR のパスワードを紛失した。

CHGDSTPWD コマンドを使用して、保守ツール・ユーザー ID QSECOFR のパスワードのリセットを行います。

問題 3: 保守ツール・ユーザー ID QSECOFR のパスワードが英大文字であることを忘れていたため、このユーザー ID が使用不可になった。このユーザー ID のパスワードを知っているが、誤って入力してしまった。

保守ツール・ユーザー ID QSECOFR のパスワードが使用不可になっていても、DST には、このユーザー ID を使用していつでもサインオンすることができます。DST にサインオンすれば、DST 内からパスワードをもう一度使用可能にすることができます。

問題 4: STRSST を実行して「パスワードの変更 (Change Password)」画面から自分の保守ツール・ユーザー ID のパスワードを変更しようとした場合、または QSYCHGDS API を使用中に、「保守ツール・ユーザー ID のパスワードを変更できません (Service tools user ID password cannot be changed)」というエラー・メッセージが表示される。




保守ツール・ユーザー ID のパスワードがデフォルト・パスワードで、有効期限が切れているため、そのパスワードを SST または QSYCHGDS API を使用して変更することはできません。以下のオプションのいずれかを使用してください。

- 適切な機能特権を付与されている別の保守ツール・ユーザー ID を使用して、自分の保守ツール・ユーザー ID のパスワードを変更する。次に、自分の保守ツール・ユーザー ID でサインオンし、そのパスワードを自分しか知らない値に変更します。
- DST にアクセスし、自分の保守ツール・ユーザー ID のパスワードを変更する。
- 適切な機能権限を付与されている別の保守ツール・ユーザー ID を使用して DST または SST から「システム・セキュリティの処理 (Work with System Security)」オプションにアクセスし、「パスワードがデフォルトおよび有効期限切れの保守ツール・ユーザー ID に自己のパスワードの変更を許可する (Allow a service tools user ID with a default and expired password to change its own password)」の設定値を 1 (はい) に変更する。自分の保守ツール・ユーザー ID のパスワードを変更してから、この設定をオプション 2 (いいえ) に戻します。

保守ツール関連情報

以下に、本トピック『保守ツール』に関連する、iSeries マニュアル、IBM レッドブック (TM) (PDF 形式)、Web サイト、および Information Center 内の各種トピックを紹介します。PDF 形式の資料は、いずれも表示または印刷することができます。

マニュアル

- **iSeries セキュリティの手引き** (約 1420KB、276 ページ) 
iSeries サーバーのセキュリティ機能の使用、およびセキュリティに配慮した操作手順の確立のための、実践的な提案のセットを示すマニュアル。
- **iSeries Service Functions** (約 1780KB、360 ページ) 
ハードウェア・サービス担当者がよく使用する iSeries のサービス機能についての基本情報を提供する、補足マニュアル CD-ROM 収録のマニュアル。このマニュアルは、ハードウェア・サービス担当者がよくあるハードウェア障害について情報収集する際に役立つよう、記述されています。iSeries サーバー上で使用できるサービス機能のすべてが説明されているわけではありません。
- **iSeries 機密保護解説書** (約 4260KB、688 ページ) 
このマニュアルには、iSeries サーバー上のセキュリティの計画、セットアップ、管理、および監査についての情報が提供されています。システム上のセキュリティ機能のすべてが説明されているほか、


セキュリティー機能が、作業管理、バックアップとリカバリー、アプリケーション設計などのシステムのその他の局面とどのように関係しているかについても説明されています。

その他の情報

- セキュリティー
- オペレーション・コンソール
- 論理区画
- iSeries ナビゲーター

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・ボタンでクリックする (上記のリンクを右マウス・ボタンでクリックする)。
2. 「リンクを名前を付けて保存」(Netscape Navigator) または「対象をファイルに保存」(Internet Explorer) を選択する。
3. PDF を保管するディレクトリーを指定する。
4. 「保存」をクリックする。

PDF ファイルを表示したり印刷したりするには、Adobe Acrobat Reader が必要です。これは、Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から、ダウンロードできます。



Printed in Japan