



IBM Systems - iSeries

セキュリティー保守ツール
ユーザー ID とパスワード

バージョン 5 リリース 4





IBM Systems - iSeries

**セキュリティー保守ツール
ユーザー ID とパスワード**

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、35 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 (プロダクト番号 5722-SS1) 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
Service tools user IDs and passwords
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

© Copyright International Business Machines Corporation 2003, 2006. All rights reserved.

© Copyright IBM Japan 2006

目次

保守ツール ユーザー ID とパスワード . . . 1	
V5R4 の新機能 1	
トピックの印刷 1	
保守ツール・ユーザー ID とパスワードの概念 . . . 2	
保守ツール・ユーザー ID とパスワードの用語 . . . 2	
DST アクセス方式と SST アクセス方式 3	
保守ツール・ユーザー ID 4	
保守ツール・ユーザー ID のパスワード・ポリシー 6	
保守ツール・サーバー 8	
保守ツール・ユーザー ID とパスワードの管理 . . . 8	
保守ツールへのアクセス 8	

保守ツール・ユーザー ID の管理 11	
保守ツール・サーバーの構成 26	
サービス機能の使用のモニター 29	
保守ツール・ユーザー ID とパスワードのトラブルシューティング 31	
保守ツール・ユーザー ID とパスワードの関連情報 . . . 32	

付録. 特記事項. 35	
プログラミング・インターフェース情報 36	
商標 36	
資料に関するご使用条件 37	

保守ツール ユーザー ID とパスワード

- 保守ツールは、IBM®  iSeries™ モデル 270 または 8xx または論理区画の構成、管理、および保守に使用されます。モデル 8xx 以外のサーバー上の論理区画を管理する場合は、ハードウェア管理コンソール (HMC) を使用する必要があります。

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。

V5R4 の新機能

- V5R4 では、コンソールのテークオーバーという新規保守ツール・ユーザー特権を使用できます。この特権により、別のコンソール装置からオペレーション・コンソールに制御を引き継ぐことが許可されます。
- 詳しくは、『オペレーション・コンソール接続のテークオーバーまたはリカバリー』を参照してください。

新機能や変更点の確認方法

技術的な変更が行われた場所が分かるように、次のマークを使用しています。

- ▶ のマークで、新機能や変更内容の説明が始まる位置を示します。
- ◀ のマークで、新機能や変更内容の説明が終わる位置を示します。

本リリース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、『プログラム資料説明書』を参照してください。

トピックの印刷

この文書の PDF 版を参照用または印刷用にダウンロードし、表示することができます。

この文書の PDF 版をダウンロードし、表示するには、「保守ツール ユーザー ID とパスワード」を選択します。

関連トピック「オペレーション・コンソール」を表示またはダウンロードすることができます。このトピックの PDF は、オペレーション・コンソールの計画、設定、管理およびトラブルシューティングに関する情報を含んでいます。

その他の情報

以下のマニュアルまたはトピックも表示または印刷することができます。

- 「iSeries セキュリティーの手引き」 
- 「iSeries Service Functions」 

- 「iSeries 機密保護解説書」 

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. 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

- PDF ファイルを表示したり印刷したりするには、ご使用のシステムに Adobe Reader がインストールされている必要があります。これは、Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から無料でダウンロードできます。

保守ツール・ユーザー ID とパスワードの概念

次の概念の説明は、保守ツール・ユーザー ID とパスワードを使用する前に必要な基本的な情報です。

保守ツール・ユーザー ID とパスワードの用語

以下の定義は、保守ツール・ユーザー ID とパスワードに関する情報を理解する上で役立ちます。

データ暗号化規格 (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)

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。

省略時パスワード

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、出荷時点では省略時パスワード QSECOFR が設定されている。

使用不可パスワード

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。

有効期限切れパスワード

180 日間以上変更されていないパスワード。有効期限切れ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

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。

1 i5/OS™ ユーザー・プロファイル

ユーザー・プロファイル作成 (CRTUSRPRF) 制御言語 (CL) コマンドまたは iSeries ナビゲーターを使用して作成されたユーザー・プロファイル。オペレーティング・システムへのサインオンに使用される。

ロック 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。

パスワード・レベル

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。省略時のレベルは 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。

保守機能

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

保守ツール

サーバーの運用にかかわる重要な特性を構成、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

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

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

DST、SST、iSeries ナビゲーター (論理区画管理およびディスク装置管理の場合)、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必要なユーザー 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、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)

システム保守ツール (SST) を使用することで、オペレーティング・システムから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、STRSST (SST 開始) CL コマンドを使用してアクセスする。

DST アクセス方式と SST アクセス方式

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、i5/OS がロードされていなくても、ライセンス内部コードが始動している場合、使用可能です。SST はオペレーティング・システムから使用可能です。

1 保守ツールは、以下のアクションを実行するために使用されます。

注: このリストには、すべてが含まれているわけではありませんが、保守ツールにより提供される機能の概念を理解することができます。

- 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) のアクティビティーの管理 (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ー・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・セキュリティーの管理
 - 他の保守ツール・ユーザー ID の管理
- 1 • コンソールのテークオーバー: 別のコンソール装置からオペレーション・コンソールに制御を引き継ぐこと
1 を許可する保守ツール・ユーザー特権。

DST アクセス方式と SST アクセス方式の基本的な違いの概要を、次の表にまとめます。

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、QSECOFR 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"> • STRSST (SST 開始) CL コマンドを使用できる権限 • 保守特殊権限 (*SERVICE) • SST を使用できる機能特権
どんなときに使用可能か	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、i5/OS は必要とされません。	オペレーティング・システムが開始済みの場合に使用可能です。SST へのアクセスには、i5/OS 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。

関連情報

オペレーション・コンソール接続のテークオーバーまたはリカバリー

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)、iSeries ナビゲーター (論理区画管理およびディスク装置管理の場合)、およびオペレーション・コンソールを使用して、保守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あり、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
- 22222222
- 11111111

保守ツール・ユーザー ID QSECOFR、QSRV、および 22222222 のパスワードは、有効期限が切れた状態で提供されます。保守ツール・パスワードはすべて大文字で提供されます。

- 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 には、特定権限が認可されています。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。

注: サーバーが IBM から出荷される時点で、i5/OS ユーザー・プロファイル QSECOFR と保守ツール・ユーザー ID QSECOFR が用意されています。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、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 i5/OS 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。

保守ツール・ユーザー ID を追加作成することにより、セキュリティ管理者は、IBM 提供の保守ツール・ユーザー ID にパスワードを割り当てなくても、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。

重要: すべての i5/OS セキュリティ担当者プロファイルのパスワードおよびすべてのセキュリティ保守ツール・ユーザー ID のパスワードを紛失したり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のインストールおよび初期化が必要になる場合があります。したがって、複数のプロファイルおよびユーザー ID を作成することをお勧めします。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。

保守ツール・ユーザー ID には有効期限を設定でき、これを利用して、サーバーのセキュリティ上のリスクを最小限に抑えることができます。例えば、社員に対し有効期限が切れた保守ツール・ユーザー ID を作成するとします。その社員は、初めて ID を使用するとき、その ID を変更しなければなりません。また、ユーザー ID は、ユーザーが退職した場合に使用不可にすることができるので、退職者に保守ツールを悪用される可能性も最小限に抑えることができます。

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。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の監査ログがあります。

保守ツール・ユーザー ID と同じように、装置 ID にも付与したり取り消したりできる許可を割り当て、機能の実行を制御することができます。装置 ID にアクセスするには SST を使用します。

関連概念

29 ページの『サービス機能の使用のモニター』

DST によりサービス機能の使用をモニターしたり、セキュリティ監査ログにより保守ツールの使用をモニターできます。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。

関連資料

『保守ツール・ユーザー ID のパスワード・ポリシー』

このトピックでは、保守ツール・ユーザー ID のパスワード・ポリシーについて、および Data Encryption Standard (DES) と Secure Hash Algorithm (SHA) による暗号化の変更プロセスについて説明します。

8 ページの『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。

関連情報

iSeries セキュリティの手引き

オペレーション・コンソール

オペレーション・コンソール構成の保護

保守ツール・ユーザー ID のパスワード・ポリシー

このトピックでは、保守ツール・ユーザー ID のパスワード・ポリシーについて、および Data Encryption Standard (DES) と Secure Hash Algorithm (SHA) による暗号化の変更プロセスについて説明します。

注: サインオン時にパスワードを複数回誤って入力すると、保守ツール・ユーザー ID は使用不可になります。その場合、使用不可になったユーザー ID を使用してコンソールからサインオンし、そのユーザー ID をリセットできます。

保守ツール・ユーザー ID は、i5/OS 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。省略時のパスワード・レベルには、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、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 に変更した場合、DES に戻すことはできません。また、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、この関数を使用するすべてのクライアントをアップグレードする必要があります。

DES による暗号化

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。

- 1 • ユーザー ID には、10 桁の英大文字を使用する。
- 1 • パスワードは、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、省略時で有効期限切れに設定されて出荷されます。ただし、ユーザー ID 11111111 は例外です。このユーザー ID は有効期限が切れていません。

SHA による暗号化

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 には、10 桁の英大文字を使用する。
- パスワードは、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、省略時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」画面が表示されます。
2. オプション 5 (DST 環境の処理) を選択し、Enter キーを押す。「DST 環境の処理」画面が表示されず。
3. オプション 6 (保守ツール機密保護データ) 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) 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。

関連概念

9 ページの『DST の使用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。

21 ページの『STRSST または 保守ツール・ユーザー ID 変更 (QSYCHGDS) API 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 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 のパスワードを変更することができます。

22 ページの『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、i5/OS 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。

関連タスク

19 ページの『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』

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ことができます。

20 ページの『SST 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』

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ことができます。

関連資料

4 ページの『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)、iSeries ナビゲータ

ー (論理区画管理およびディスク装置管理の場合)、およびオペレーション・コンソールを使用して、保守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あり、ユーザー・プロファイルとは別のものです。

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・サーバーは、DST 用または i5/OS 用 (あるいはその両方用) に構成することができます。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:

1. 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。
2. サーバー・モデルが 8xx 以外の場合は、ハードウェア管理コンソール (HMC) を使用して i5/OS の区画を管理する必要があります。
3. オペレーション・コンソール (LAN) を使用している場合、保守ツール・サーバーは構成済みです。

関連概念

10 ページの『iSeries ナビゲーターの使用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 i5/OS 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。

関連資料

26 ページの『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 i5/OS 用 (あるいはその両方用) に構成することができます。

関連情報

iSeries ナビゲーターによる区画化

ディスク管理

保守ツール・ユーザー ID とパスワードの管理

保守ツール・ユーザー ID とパスワードの管理と保守に有効な戦略を開発することができます。

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 を管理することができます。

関連資料

4 ページの『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)、iSeries ナビゲーター (論理区画管理およびディスク装置管理の場合)、およびオペレーション・コンソールを使用して、保

守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あり、ユーザー・プロフィールとは別のものです。

11 ページの『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、保守ツール・ユーザー ID の構成と変更、QSECOFR パスワードのリカバリーまたはリセット、および保守ツール機密保護データの保管または復元を行う必要があります。

DST の使用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。

システム・コントロール・パネル から DST の使用による保守ツールへのアクセス

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」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」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 環境の処理) 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 (保守ツールの開始) 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 の使用による保守ツールへのアクセス

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 i5/OS を始動したら、システム電源遮断 (PWRDWN SYS) コマンド、PWRDWN SYS *IMMED RESTART(*YES) を i5/OS コマンド行に入力して、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」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 環境の処理) 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 (保守ツールの開始) 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。

関連資料

6 ページの『保守ツール・ユーザー ID のパスワード・ポリシー』
このトピックでは、保守ツール・ユーザー ID のパスワード・ポリシーについて、 および Data Encryption Standard (DES) と Secure Hash Algorithm (SHA) による暗号化の変更プロセスについて説明します。

SST の使用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。

i5/OS 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。

- SST 開始 (STRSST) CL コマンドを使用できる権限
- 保守特殊権限 (*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. i5/OS コマンド行に STRSST (SST 開始) と入力する。「保守ツールの開始のサインオン」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:** サインオンに使用する保守ツール・ユーザー ID。
 - **パスワード:** 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。

関連資料

11 ページの『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。

iSeries ナビゲーターの使用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 i5/OS 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 が開始済みの場合の iSeries ナビゲーターの使用による保守ツールへのアクセス

注: オペレーション・コンソール (LAN) を使用している場合、保守ツール・サーバーは構成済みです。

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 用に構成され、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 ナビゲーター保守ツール**」ウィンドウをオープンします。」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**」を選択します。
3. 項目「**タスクパッド**」の選択後、接続先サーバーの IP アドレスを入力する必要がある。

i5/OS を稼働中の場合の iSeries ナビゲーターの使用による保守ツールへのアクセス

サーバーにより、i5/OS 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 i5/OS 用に構成され、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。

関連タスク

28 ページの『i5/OS 用保守ツール・サーバーの構成』

i5/OS 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。

関連資料

8 ページの『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。

27 ページの『DST 用保守ツール・サーバーの構成』

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。

関連情報

iSeries ナビゲーター

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、保守ツール・ユーザー ID の構成と変更、QSECOFR パスワードのリカバリーまたはリセット、および保守ツール機密保護データの保管または復元を行う必要があります。

関連資料

8 ページの『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・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 とパスワードを変更できます。

関連タスク

10 ページの『SST の使用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。

27 ページの『DST の使用による保守ツール・サーバーの構成』

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 DST から使用可能にすることができます。

28 ページの『SST の使用による保守ツール・サーバーの構成』

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 SST から使用可能にすることができます。

関連資料

18 ページの『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。

DST の使用による保守ツール・ユーザー ID の構成:

DST から保守ツール・ユーザー ID の作成、変更、表示、使用可能化、使用不可化、または削除を行うことができます。

保守ツール・ユーザー ID を構成した後、DST を使用して保守ツール・ユーザー ID とパスワードを変更できます。

関連タスク

19 ページの『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』

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ことができます。

DST の使用による保守ツール・ユーザー ID の作成:

DST から保守ツール・ユーザー ID を作成することができます。

DST 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 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。
3. 「専用保守ツール (DST) の使用」画面で、オプション 5 (DST 環境の処理) を選択し、Enter キーを押す。「DST 環境の処理」画面が表示されます。
4. 「DST 環境の処理」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) を選択する。「保守ツール・ユーザー ID の処理」画面が表示されます。
5. 「保守ツール・ユーザー ID の処理」画面で 1 (作成) 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」画面が表示されます。

注: ユーザー ID には 1 から 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。

6. 新規ユーザー ID についての情報を入力する。
 - **ユーザー ID 名:** 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:** 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。
 - **記憶域管理の回復処理前の ID のアクセスの許可:** このフィールドの省略時値は 2 (いいえ) です。

- **パスワードの有効期限切れの設定:** このフィールドの省略時値は 1 (はい) です。
- **記述:** 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。

7. ユーザー ID に関する情報の入力をすべて完了したら、次のオプションのいずれかを選択する。

- 省略時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省略時から変更するには、F5 を押して「保守ツール・ユーザー特権の変更」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。機能特権の変更について詳しくは、『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』を参照してください。

関連タスク

19 ページの『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』
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ことができます。

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 から保守ツール・ユーザー ID の機能特権を変更することができます。

DST 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 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。
3. 「専用保守ツール (DST) の使用」画面で、オプション 5 (DST 環境の処理) を選択し、Enter キーを押す。「DST 環境の処理」画面が表示されます。
4. 「DST 環境の処理」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) を選択する。「保守ツール・ユーザー ID の処理」画面が表示されます。
5. 「保守ツール・ユーザー ID の処理」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) と入力する。「保守ツール・ユーザー特権の変更」画面が表示されます。
 - 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) と入力する。
 - 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 (許可) と入力する。
6. 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 (省略時値) を押すと、機能特権は省略時値にリセットされます。

DST の使用による保守ツール・ユーザー ID の記述の変更:

DST から保守ツール・ユーザー ID の記述を変更することができます。

DST から保守ツール・ユーザー ID の記述を変更するには、以下のステップを実行してください。

1. DST 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」画面で、オプション 5 (DST 環境の処理) を選択し、Enter キーを押す。「DST 環境の処理」画面が表示されます。
3. 「DST 環境の処理」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) を選択する。「保守ツール・ユーザー ID の処理」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理」画面で、変更するユーザー ID の記述を選択して「オプション」フィールドに 8 (記述の変更) と入力する。
5. 「記述」フィールドに、ユーザー ID の新しい記述を入力する。ユーザー名、部門、電話番号などを入力できます。

DST の使用による保守ツール・ユーザー ID の表示:

DST から保守ツール・ユーザー ID を表示することができます。

DST から保守ツール・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 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」画面で、オプション 5 (DST 環境の処理) を選択し、Enter キーを押す。「DST 環境の処理」画面が表示されます。
3. 「DST 環境の処理」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) を選択する。「保守ツール・ユーザー ID の処理」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理」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) と入力する。「保守ツール・ユーザー ID の表示」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行回数
 - 状況
 - パスワードが最後に変更された日付
 - 記憶域管理の回復処理前の ID のアクセスの許可 (「YES」または「NO」)
 - パスワードが失効する日付
 - パスワードの有効期限切れの設定 (「YES」または「NO」)
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) を押す。「保守ツール・ユーザー特権の表示」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。

DST の使用による保守ツール・ユーザー ID の使用可能化:

DST から保守ツール・ユーザー ID を使用可能にすることができます。

DST 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 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」画面で、オプション 5 (DST 環境の処理) を選択し、Enter キーを押す。「DST 環境の処理」画面が表示されます。
3. 「DST 環境の処理」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) を選択する。「保守ツール・ユーザー ID の処理」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理」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) と入力する。「保守ツール・ユーザー ID の使用可能」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 の使用による保守ツール・ユーザー ID の使用不可化:

DST から保守ツール・ユーザー ID を使用不可にすることができます。

DST 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 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」画面で、オプション 5 (DST 環境の処理) を選択し、Enter キーを押す。「DST 環境の処理」画面が表示されます。
3. 「DST 環境の処理」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) を選択する。「保守ツール・ユーザー ID の処理」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理」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) と入力する。「保守ツール・ユーザー ID の使用不可」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。

DST の使用による保守ツール・ユーザー ID の削除:

DST から保守ツール・ユーザー ID を削除することができます。

注: IBM 提供の保守ツール・ユーザー ID は削除できません。

DST から保守ツール・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 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」画面で、オプション 5 (DST 環境の処理) を選択し、Enter キーを押す。「DST 環境の処理」画面が表示されます。
3. 「DST 環境の処理」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) を選択する。「保守ツール・ユーザー ID の処理」画面が表示されます。
4. 「保守ツール・ユーザー ID の処理」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」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) を押して、「保守ツール・ユーザー ID の処理」画面に戻る。

SST の使用による保守ツール・ユーザー ID の構成:

SST から保守ツール・ユーザー ID の作成、変更、表示、使用可能化、使用不可化、または削除を行うことができます。

保守ツール・ユーザー ID を構成した後、SST を使用して保守ツール・ユーザー ID とパスワードを変更できます。

関連タスク

20 ページの『SST 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』
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ことができます。

SST の使用による保守ツール・ユーザー ID の作成:

SST から保守ツール・ユーザー ID を作成することができます。

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. 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 SST にサインオンする。

3. 「システム保守ツール (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 および装置の処理) を選択します。
4. 「保守ツール・ユーザー ID および装置の処理」画面で、オプション 1 (保守ツール・ユーザー ID) を選択する。
5. 「保守ツール・ユーザー ID」画面で 1 (作成) 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」画面が表示されません。

注: ユーザー ID には 1 から 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。

6. 新規ユーザー ID についての情報を入力する。
 - **ユーザー ID 名:** 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:** 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。
 - **記憶域管理の回復処理前の ID のアクセスの許可:** このフィールドの省略時値は 2 (いいえ) です。
 - **パスワードの有効期限切れの設定:** このフィールドの省略時値は 1 (はい) です。
 - **記述:** 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。
7. ユーザー ID に関する情報の入力をすべて完了したら、次のオプションのいずれかを選択する。
 - 省略時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省略時から変更するには、F5 を押して「保守ツール・ユーザー特権の変更」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。機能特権の変更について詳しくは、『SST の使用による保守ツール・ユーザー ID の機能特権の変更』を参照してください。

関連タスク

20 ページの『SST 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』
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ことができます。

SST の使用による保守ツール・ユーザー ID の機能特権の変更:

SST から保守ツール・ユーザー ID の機能特権を変更することができます。

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. 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 SST にサインオンする。「システム保守ツール (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 および装置の処理) を選択します。
3. 「保守ツール・ユーザー ID および装置の処理」画面で、オプション 1 (保守ツール・ユーザー ID) を選択する。
4. 「保守ツール・ユーザー ID」画面で、変更するユーザー ID を選択し、「オプション」フィールドに 7 (特権の変更) と入力する。「保守ツール・ユーザー特権の変更」画面が表示されます。
 - 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) と入力する。
 - 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 (許可) 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 キーを押し前に F3 (終了) を押し、変更は有効になりません。F9 (省略時値) を押し、機能特権は省略時値にリセットされます。

SST の使用による保守ツール・ユーザー ID の記述の変更:

SST から保守ツール・ユーザー ID の記述を変更することができます。

SST から保守ツール・ユーザー ID の記述を変更するには、以下のステップを実行してください。

1. 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 SST にサインオンする。「システム保守ツール (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 および装置の処理) を選択します。
3. 「保守ツール・ユーザー ID および装置の処理」画面で、オプション 1 (保守ツール・ユーザー ID) を選択する。
4. 「保守ツール・ユーザー ID」画面で、変更するユーザー ID の記述を選択し、「オプション」フィールドに 8 (記述の変更) と入力する。
5. 「記述」フィールドに、ユーザー ID の新しい記述を入力する。ユーザー名、部門、電話番号などを入力できます。

SST の使用による保守ツール・ユーザー ID の表示:

SST から保守ツール・ユーザー ID を表示することができます。

SST から保守ツール・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. 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 SST にサインオンする。「システム保守ツール (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 および装置の処理) を選択します。
3. 「保守ツール・ユーザー ID および装置の処理」画面で、オプション 1 (保守ツール・ユーザー ID) を選択する。
4. 「保守ツール・ユーザー ID」画面で、表示するユーザー ID を選択し、「オプション」フィールドに 4 (表示) と入力する。「保守ツール・ユーザー ID の表示」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行回数
 - 状況
 - パスワードが最後に変更された日付
 - 記憶域管理の回復処理前の ID のアクセスの許可 (「YES」または「NO」)
 - パスワードが失効する日付
 - パスワードの有効期限切れの設定 (「YES」または「NO」)
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) を押し。「保守ツール・ユーザー特権の表示」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。

SST の使用による保守ツール・ユーザー ID の使用可能化:

SST から保守ツール・ユーザー ID を使用可能にすることができます。

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. 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 SST にサインオンする。「システム保守ツール (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 および装置の処理) を選択します。
3. 「保守ツール・ユーザー ID および装置の処理」画面で、オプション 1 (保守ツール・ユーザー ID) を選択する。
4. 「保守ツール・ユーザー ID」画面で、使用可能にするユーザー ID を選択し、「オプション」フィールドに 5 (使用可能) と入力する。「保守ツール・ユーザー ID の使用可能」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。

SST の使用による保守ツール・ユーザー ID の使用不可化:

SST から保守ツール・ユーザー ID を使用不可にすることができます。

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. 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 SST にサインオンする。「システム保守ツール (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 および装置の処理) を選択します。
3. 「保守ツール・ユーザー ID および装置の処理」画面で、オプション 1 (保守ツール・ユーザー ID) を選択する。
4. 「保守ツール・ユーザー ID」画面で、使用不可にするユーザー ID を選択し、「オプション」フィールドに 6 (使用不可) と入力する。「保守ツール・ユーザー ID の使用不可」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。

SST の使用による保守ツール・ユーザー ID の削除:

SST から保守ツール・ユーザー ID を削除することができます。

注: IBM 提供の保守ツール・ユーザー ID は削除できません。

SST から保守ツール・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. 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 SST にサインオンする。「システム保守ツール (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 および装置の処理) を選択します。
3. 「保守ツール・ユーザー ID および装置の処理」画面で、オプション 1 (保守ツール・ユーザー ID) を選択する。
4. 「保守ツール・ユーザー ID」画面で、削除するユーザー ID を選択し、「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」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) を押して、「保守ツール・ユーザー ID の処理」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前に、保守ツールが構成されている必要があります。また、保守ツール・ユーザー ID の管理についての推奨事項を確認することをお勧めします。

- | **重要:** すべての i5/OS 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すべてのセキュリティー保守ツール・ユーザー ID のパスワードを紛失したり忘れたりした場合、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のインストールおよび初期化が必要になる場合があります。したがって、複数のプロファイルおよびユーザー ID を作成することをお勧めします。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。

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、STRSSST (SST 開始) と F9 を使用するか、または保守ツール・ユーザー ID 変更 (QSYCHGDS) API を使用することができます。

関連概念

22 ページの『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、i5/OS 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。

関連資料

11 ページの『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。

26 ページの『保守ツール・ユーザー ID の管理に関する推奨事項』

ここでは、保守ツール・ユーザー ID の管理に関する推奨事項を示します。

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:

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. 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」画面が表示されます。
3. オプション 5 (DST 環境の処理) を選択し、Enter キーを押す。「DST 環境の処理」画面が表示されず。
4. 「DST 環境の処理」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) を選択する。「保守ツール・ユーザー ID の処理」画面が表示されます。
5. 「保守ツール・ユーザー ID の処理」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 (パスワード変更) 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機密保護特権が自分自身に付与されている場合は、「別のユーザーのための保守ツール・ユーザー・パスワードの変更」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:** 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することはできません。

- パスワードの有効期限切れの設定: 1 (YES) または 2 (NO) を入力します。省略時値は 1 (YES) 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」画面が表示される。確認後、以下のフィールドに入力します。
 - **現行パスワード:** 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:** 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することはできません。
 - **新規パスワード (確認用):** 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。

関連タスク

12 ページの『DST の使用による保守ツール・ユーザー ID の作成』
DST から保守ツール・ユーザー ID を作成することができます。

関連資料

12 ページの『DST の使用による保守ツール・ユーザー ID の構成』
DST から保守ツール・ユーザー ID の作成、変更、表示、使用可能化、使用不可化、または削除を行うことができます。

6 ページの『保守ツール・ユーザー ID のパスワード・ポリシー』
このトピックでは、保守ツール・ユーザー ID のパスワード・ポリシーについて、および Data Encryption Standard (DES) と Secure Hash Algorithm (SHA) による暗号化の変更プロセスについて説明します。

SST 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:

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ことができます。

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には、以下のステップを実行してください。

1. SST を開始する。
2. 保守ツール機密保護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)」メインメニューが表示される。
3. 「システム保守ツール (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 および装置の処理) を選択する。
4. 「保守ツール・ユーザー ID および装置の処理」画面で、オプション 1 (保守ツール・ユーザー ID) を選択する。
5. 「保守ツール・ユーザー ID」画面で、変更するユーザー ID を選択し、「オプション」フィールドに 2 (パスワード変更) と入力する。
6. 「別のユーザーのための保守ツール・ユーザー・パスワードの変更」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:** 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することはできません。
 - **パスワードの有効期限切れの設定:** 1 (YES) または 2 (NO) を入力します。省略時値は 1 (YES) です。
7. 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。

関連タスク

15 ページの『SST の使用による保守ツール・ユーザー ID の作成』
SST から保守ツール・ユーザー ID を作成することができます。

関連資料

15 ページの『SST の使用による保守ツール・ユーザー ID の構成』
SST から保守ツール・ユーザー ID の作成、変更、表示、使用可能化、使用不可化、または削除を行うことができます。

6 ページの『保守ツール・ユーザー ID のパスワード・ポリシー』
このトピックでは、保守ツール・ユーザー ID のパスワード・ポリシーについて、および Data Encryption Standard (DES) と Secure Hash Algorithm (SHA) による暗号化の変更プロセスについて説明します。

STRSST または 保守ツール・ユーザー ID 変更 (QSYCHGDS) API 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 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 のパスワードを変更することができます。

関連資料

6 ページの『保守ツール・ユーザー ID のパスワード・ポリシー』
このトピックでは、保守ツール・ユーザー ID のパスワード・ポリシーについて、および Data Encryption Standard (DES) と Secure Hash Algorithm (SHA) による暗号化の変更プロセスについて説明します。

STRSST の使用による保守ツール・ユーザー ID のパスワードの変更:

STRSST を使用して保守ツール・ユーザー ID のパスワードを変更することができます。

STRSST 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、保守ツール・ユーザー ID を入力し、F9 (パスワード変更) を押す。「パスワード変更」画面が表示されます。
2. 「パスワード変更」画面で、現行パスワードと新規パスワードを入力し、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、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、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。

保守ツール・ユーザー ID 変更 (QSYCHGDS) API 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:

この API を使用すると、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。

複数の iSeries サーバーがあり、それらすべてのサーバーの保守ツール・ユーザー ID を管理する必要がある場合に、保守ツール・ユーザー ID 変更 (QSYCHGDS) API は役立ちます。

関連情報

保守ツール・ユーザー ID 変更 (QSYCHGDS) API

省略時パスワードおよび有効期限が切れたパスワードの変更:

省略時パスワードおよび有効期限が切れた保守ツール・パスワードを変更することができます。

省略時パスワードおよび有効期限が切れた保守ツール・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. 省略時パスワードおよび有効期限が切れたパスワードの変更を許可します。
 - a. SST または DST を開始する。
 - b. 「システム機密保護の処理」を選択する。
 - c. 「システム機密保護の処理」画面で、「省略値で有効期限切れのパスワードを持つ保守ツール・ユーザー ID のパスワードを変更可能」フィールドの設定を「いいえ」から「はい」に変更する。
2. 省略時パスワードおよび有効期限が切れたパスワードを変更します。
 - a. SST を開始する。
 - b. パスワードが省略時および有効期限切れである保守ツール・ユーザー ID を使用して SST にサインオンする。
 - c. メッセージ「パスワードが有効期限切れです」が表示されたら、F9 キーを押してパスワードを変更する。
 - d. 保守ツール・ユーザー ID 名が表示されたら、次のフィールドを設定する。
 - **新規パスワード:** 新規パスワードを入力します。
 - **新規パスワード (確認用):** 新規パスワードをもう一度入力します。
 - e. Enter キーを押す。

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、i5/OS 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、i5/OS 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 i5/OS 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。

i5/OS 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り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・システムの再インストールが必要になる場合があります。したがって、複数のプロファイルおよびユーザー ID を作成することをお勧めします。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。

関連資料

18 ページの『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。

26 ページの『保守ツール・ユーザー ID の管理に関する推奨事項』

ここでは、保守ツール・ユーザー ID の管理に関する推奨事項を示します。

6 ページの『保守ツール・ユーザー ID のパスワード・ポリシー』

このトピックでは、保守ツール・ユーザー ID のパスワード・ポリシーについて、および Data Encryption Standard (DES) と Secure Hash Algorithm (SHA) による暗号化の変更プロセスについて説明します。

i5/OS ユーザー・プロファイル・パスワード QSECOFR 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、i5/OS ユーザー・プロファイル QSECOFR 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。

i5/OS ユーザー・プロファイル QSECOFR 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」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」メニューで、オプション 5 (DST 環境の処理) を選択する。
4. 「DST 環境の処理」メニューで、オプション 6 (保守ツール機密保護データ) を選択する。次のような「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・システムのシステム省略時パスワードのリセット) を選択する。「システム省略時パスワードのリセットの確認」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。

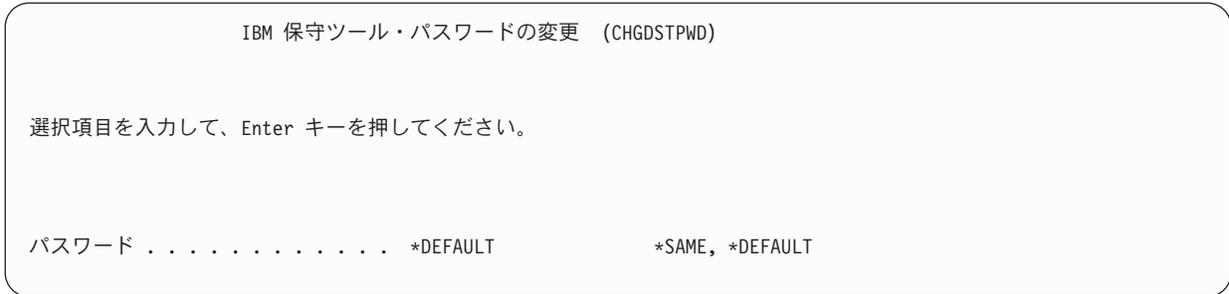
7. 「DST の終了」メニューに戻るまで、F3 (終了) を押す。
 8. オプション 1 (DST の終了) を選択する。「IPL またはシステムの導入」メニューが表示されます。
 9. オプション 1 (IPL の実行) を選択する。システムは、手動 IPL で続行します。IPL の実行に関する追加情報については、トピック『サーバーの開始と停止 (Start and stop the server)』を参照してください。
 10. IPL が完了したら、キーロック・スイッチまたは電子キースティックを自動位置に戻す (これらが存在する場合)。
 11. QSECOFR として i5/OS 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省略時設定のままにしないでください。この値は、すべての iSeries サーバー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。

QSECOFR 保守ツール・ユーザー ID とパスワードのリセット:

i5/OS 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、保守ツール機密保護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 提供の省略時値にリセットすることができます。

QSECOFR 保守ツール・ユーザー ID と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. サーバーを、DST ではなく、通常の操作モードにする。
2. i5/OS 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・パスワードの変更) を入力する。次に、F4 キーを押します (Enter キーは押さないでください)。「IBM 保守ツール・パスワードの変更 (CHGDSTPWD)」画面が表示されます。
4. *DEFAULT と入力し、Enter キーを押す。これにより、保守ツール機密保護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 とパスワードの値を省略時設定のままにしないでください。この値は、すべての iSeries サーバー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・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、(SAVSYS) コマンドを使用してのシステム保管またはライセンス内部コード保管操作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。

保守ツール機密保護データの保管:

DST を使用して保守ツール機密保護データを保管することができます。

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 環境の処理」画面で、オプション 6 (保守ツール機密保護データ) を選択する。
2. 「保守ツール機密保護データの処理」画面で、オプション 5 (保守ツール機密保護データの保管) を選択する。「保守ツール機密保護データの保管」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. データを保管するには、Enter キーを押す。「テープ装置の処理」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
 - a. データを保管するには、Enter キーを押す。「光ディスク装置の処理」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。

保守ツール機密保護データの復元:

DST を使用して保守ツール機密保護データを復元することができます。

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 環境の処理」画面で、オプション 6 (保守ツール機密保護データ) を選択する。
2. 「保守ツール機密保護データの処理」画面で、オプション 4 (保守ツール機密保護データの復元) を選択する。「媒体タイプの選択」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. データを復元するには、Enter キーを押す。「テープ装置の処理」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
 - a. データを復元するには、Enter キーを押す。「光ディスク装置の処理」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. 復元する機密保護データの取り出し元装置を選択する。 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す。
 - 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) と入力する。「保守ツール・ユーザー ID の復元」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」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) 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

ここでは、保守ツール・ユーザー ID の管理に関する推奨事項を示します。

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。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 はすべてのサーバー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、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。

重要: 保守ツール・ユーザー ID QSECOFR とパスワードの値を省略時設定のままにしないでください。この値は、すべての iSeries サーバー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・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 へのみ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。

関連概念

22 ページの『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、i5/OS 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。

関連資料

18 ページの『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。

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 i5/OS 用 (あるいはその両方用) に構成することができます。

注: サーバーでオペレーション・コンソール (LAN) を使用している場合、保守ツール・サーバーは構成済みです。

関連資料

8 ページの『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。

DST 用保守ツール・サーバーの構成

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。

オペレーション・コンソール (LAN) が使用中であるか、事前に構成されている (例えば、LAN コンソールがバックアップ・コンソールとして使用されている) 場合以外は、保守ツール・サーバーには、専用 LAN アダプターが必要です。以下の方法のいずれかにより、ハードウェア要件に適合していることを確認してください。

1. サーバーが論理区画 (LPAR) 環境で実行されていない場合、保守ツール・サーバー・リソースは、ご使用のモデルに基づいて、特定の場所にインストールする必要があります。この場所を確認するには、『オペレーション・コンソールのハードウェア要件を満たす』を参照してください。
2. サーバーが LPAR 環境内で実行されている場合、保守ツール・サーバー・リソース (LAN アダプターの報告先である入出力処理機構 (IOP)) は、コンソールとして、エレクトロニック支援用に (ECS が使用されていない場合でも)、タグ付けされている必要があります。

LAN アダプターを構成してリソースをアクティブにするため、オペレーション・コンソール (LAN) のサーバーを一時的に構成する必要があります。リソースが適切に作動していることを確認した後、元のコンソールを指定することができます。

保守ツール・サーバーを DST または SST を介して使用できるようにするには、1 つのネットワーク・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。

関連概念

10 ページの『iSeries ナビゲーターの使用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 i5/OS 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。

DST の使用による保守ツール・サーバーの構成:

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 DST から使用可能にすることができます。

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 (DST) の使用」画面で、オプション 5 (DST 環境の処理) を選択し、Enter キーを押す。「DST 環境の処理」画面が表示されます。
2. 「DST 環境の処理」画面で、オプション 2 (システム装置) を選択し、Enter キーを押す。「システム装置の処理」画面が表示されます。
3. 「システム装置の処理」画面で、オプション 7 (保守ツール LAN アダプターの構成) を選択し、Enter キーを押す。「保守ツール LAN アダプターの構成」画面が表示されます。

注: 使用可能なリソースがないかタイプが誤っていることを示すメッセージを受け取った場合、保守ツール・サーバーのハードウェア要件に適合していません。『オペレーション・コンソールのハードウェア要件を満たす』を参照してください。

4. 「保守ツール LAN アダプターの構成」画面で、TCP/IP 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) を押します。
5. F7 (保管) を押し、変更を保管する。

6. 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。

関連資料

11 ページの『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。

SST の使用による保守ツール・サーバーの構成:

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 SST から使用可能にすることができます。

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. 「システム保守ツール (SST)」画面で、オプション 8 (保守ツール・ユーザー ID および装置の処理) を選択する。
2. 「保守ツール・ユーザー ID および装置の処理」画面で、オプション 4 (保守ツール LAN アダプターの構成) を選択し、Enter キーを押す。
3. 「保守ツール LAN アダプターの構成」画面で、TCP/IP 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) を押します。
4. F7 (保管) を押し、変更を保管する。
5. 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。

関連資料

11 ページの『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。

i5/OS 用保守ツール・サーバーの構成

i5/OS 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・サーバーは、ローカル・エリア・ネットワーク (LAN) の構成前に追加できます。

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・テーブル項目の追加) と入力し、Enter キーを押す。「サービス・テーブル項目の追加」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' (この項目は小文字で入力し、単一引用符で囲む必要があります。)
 - テキスト記述: 'Service Tools Server' このフィールドはオプションですが、テーブル項目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」フィールドに AS-ST5 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、テーブル項目を追加する。
6. 使用中の環境で TCP/IP の終了が可能であれば、ENDTCP (TCP/IP の終了) と入力して TCP/IP を終了します。追加したサービス・テーブル項目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。
7. STRTCP (TCP/IP の開始) 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」の下で as-st5 を探し、listen の状態値を確認します。

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。

注: サーバー・モデルが 8xx 以外の場合は、ハードウェア管理コンソール (HMC) を使用して i5/OS の区画を管理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、独自の名前を省略時の「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」をクリックする。
3. 「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」をクリックする。「ホスト・アプリケーション」タブをクリックし、「i5/OS」→「保守」を展開します。
4. 保守ツール「ディスク装置」、「QIBM_QYTP_SERVICE_LPARMGMT」、または「サービス追跡」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。
5. 「OK」をクリックする。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。

関連概念

10 ページの『iSeries ナビゲーターの使用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 i5/OS 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。

関連情報

iSeries ナビゲーター

HMC のある論理区画

サービス機能の使用のモニター

DST によりサービス機能の使用をモニターしたり、セキュリティー監査ログにより保守ツールの使用をモニターできます。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ー上のリスクをトレースするのに役立ちます。

関連資料

4 ページの『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)、iSeries ナビゲーター (論理区画管理およびディスク装置管理の場合)、およびオペレーション・コンソールを使用して、保守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あり、ユーザー・プロファイルとは別のものです。

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・セキュリティー・ログに記録されます。DST セキュリティー・ログを使用して、サービス機能をモニターすることができます。

保守ツール・セキュリティー・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」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」メニューで、オプション 5 (DST 環境の処理) を選択する。
4. 「DST 環境の処理」メニューで、オプション 6 (保守ツール機密保護データ) を選択する。次のような「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. 「保守ツール機密保護データの処理」画面で、オプション 3 (保守ツール機密保護ログの処理) を選択し、Enter キーを押す。「保守ツール機密保護ログの処理」画面が表示されます。この画面には、セキュリティーに関するアクティビティーが日時順に表示されます。
6. このログを印刷するには、F6 (印刷) を押す。
7. 詳細を知りたいアクティビティーの「オプション」フィールドに、5 (詳細の表示) と入力する。選択したアクティビティーについての情報を示す「保守ツール機密保護ログの詳細の表示」画面が表示されます。

i5/OS 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

i5/OS セキュリティー監査ログを使用して、保守ツール・アクションを記録することができます。

i5/OS セキュリティー監査ログに保守ツール・アクションが記録されるようにするには、i5/OS セキュリティー監査・ログを使用可能にするサーバーごとに、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、独自の名前が省略時の「**ユーザー接続**」の代わりに使用されている場合がある）。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**」を展開して「**ポリシー**」を選択し、「**監査ポリシー**」をダブルクリックする。
3. 「**システム**」タブをクリックする。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
 - セキュリティ・タスク
 - サービス・タスク
4. 「**OK**」をクリックする。これで、iSeries サーバー上で、選択したセキュリティ監査ログ機能が使用可能になりました。

セキュリティ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、i5/OS コマンド行にジャーナルの表示 (DSPJRN) コマンド、DSPJRN QSYS/QAUDJRN ENTTYP(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・ユーザー ID とパスワードのトラブルシューティング

本トピックでは、保守ツール・ユーザー ID とパスワード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:

- 1 誤ったパスワードを何度も入力したため、保守ツール・ユーザー ID QSECOFR が使用不可になった。パスワードを知っているが、誤って入力したか、小文字で入力した。

- 1 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「パスワード変更」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 のパスワードは変更できません」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 のパスワードが省略時パスワードで、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。
- お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「システム機密保護の処理」オプションにアクセスし、「省略値で有効期限切れのパスワードを持つ保守ツール・ユーザー ID のパスワードを変更可能」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・ユーザー ID とパスワードの関連情報

保守ツール・ユーザー ID とパスワードのトピックに関連する、製品マニュアル、Web サイト、および Information Center トピックを以下に示します。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

- 「保守ツール ユーザー ID とパスワード」
- 「オペレーション・コンソール」

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
- iSeries ナビゲーターによる区画化
- iSeries ナビゲーター

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)。
- 1 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

- | PDF ファイルを表示したり印刷したりするには、ご使用のシステムに Adobe Reader がインストールされている必要があります。これは、Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から無料で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を提供し、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。

- 1 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
- 1 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
- 1 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。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認できません。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をお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

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。 © 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。

プログラミング・インターフェース情報

この「保守ツール ユーザー ID とパスワード」資料には、プログラムを作成するユーザーが IBM i5/OS のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

以下は、IBM Corporation の商標です。

e(ロゴ)server
eServer
i5/OS
IBM
IBM (ロゴ)
iSeries

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。

資料に関するご使用条件

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を提供され、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