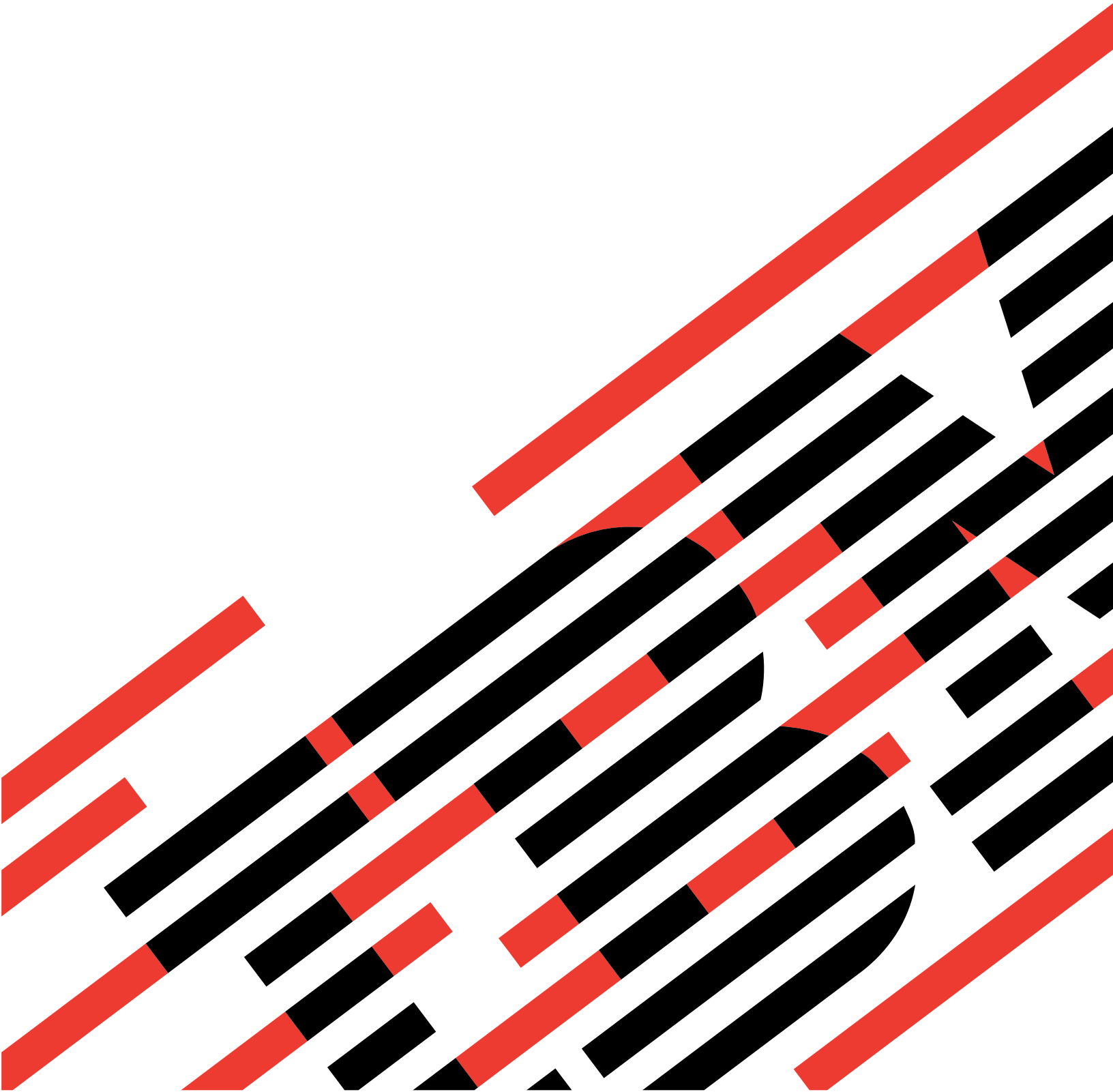
IBM

eserver

iSeries

保守ツール ユーザー ID とパスワード

バージョン 5



IBM

@server

iSeries

保守ツール ユーザー ID とパスワード

バージョン 5

お願い

本書および本書で紹介する製品をご使用になる前に、 39 ページの『特記事項』および資料「*IBM eServer 安全情報*, (GA88-8802)」に記載されている情報をお読みください。

本書は、IBM OS/400 (プロダクト番号 5722-SS1) バージョン 5、リリース 3、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： iSeries
Service tools user IDs and passwords
Version 5

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 2005.8

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, 2004. All rights reserved.

© Copyright IBM Japan 2005

目次

© Copyright IBM Corp. 2003, 2004

第 1 章 保守ツール ユーザー ID とパスワード

保守ツールは、サーバーまたは論理区画の構成、管理、および保守に使用されます。 また、8xx サーバー上の論理区画の管理にも使用されます。モデル 8*xx* 以外のサーバー上の論理区画を管理する場合は、eServer™ 用の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。

以下の情報は、保守ツール・ユーザー ID およびパスワードについて理解し、それらを使用する上で役立ちます。

3 ページの『第 2 章 V5R3 の新機能』
V5R3 での変更点を、最新情報とともに説明します。

5 ページの『第 3 章 トピックの印刷』
本トピック『保守ツール ユーザー ID とパスワード』内の全情報を含む PDF を印刷する方法を説明します。

7 ページの『第 4 章 保守ツール・ユーザー ID とパスワードの概念』
保守ツール・ユーザー ID とパスワード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。

13 ページの『第 5 章 保守ツール・ユーザー ID とパスワードの管理』
サーバー上で保守ツール・ユーザー ID とパスワードを管理する方法を学習します。

トラブルシューティング
保守ツール・ユーザー ID とパスワードに関してよく発生する問題をトラブルシューティングします。

関連情報
本トピック『保守ツール ユーザー ID とパスワード』の関連情報を表示および印刷する方法を説明します。

© Copyright IBM Corp. 2003, 2004

第 2 章 V5R3 の新機能

このトピックでは、保守ツール・ユーザー ID とパスワードの機能上および文書上の変更内容を中心に説明します。

SST の追加メニュー・オプション

「システム保守ツール (SST)」メニューに、「保守ツール・ユーザー ID と装置の処理 (Work with service tools user IDs and Devices)」という新しいオプションが追加されました。このオプションから、保守ツール・ユーザー ID の処理、保守ツール装置 ID の処理、コンソールの処理、および保守ツール LAN アダプターの構成を実行することができます。この新しいオプションを使用するタスクは次のとおりです。

- 19 ページの『SST の使用による保守ツール・ユーザー ID の構成』
- 30 ページの『SST の使用による保守ツール・サーバーの構成』

LPAR の管理

保守ツールは、6xx サーバー上の論理区画の管理に使用されます。 eServer ハードウェア上の論理区画を管理する場合は、 eServer 用の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。

文書上の変更内容

本トピック『保守ツール ユーザー ID とパスワード』は、使いやすさを考えて部分的に再編成されています。 V5R3 のタスクの説明では、タスクの実行に DST、SST のどちらを使用するかに基づいて、手順が分かれています。

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、『最初にお読みください (Memo to Users)』を参照してください。

© Copyright IBM Corp. 2003, 2004

第 3 章 トピックの印刷

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」(約 200 KB) を選択します。

関連トピック「オペレーション・コンソール」(約 1,105 KB) 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

以下のマニュアルはいずれ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」 (約 1856 KB)
- 「iSeries Service Functions」 (約 1780 KB)
- 「iSeries 機密保護解説書」 (約 6382 KB)

PDF ファイルの保管

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

1. ブラウザーで PDF を右マウス・ボタンでクリックする (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。

© Copyright IBM Corp. 2003, 2004

第 4 章 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知っておく必要がある基本的な情報です。

『保守ツール・ユーザー ID とパスワードの用語』
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。

9 ページの『DST アクセス方式と SST アクセス方式』
DST と SST のアクセス方式の違いについて説明します。

10 ページの『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。

11 ページの『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。

12 ページの『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・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。

デフォルト・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
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。

© Copyright IBM Corp. 2003, 2004

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。

ロック 特定の機能へのプログラム的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
ユーザー・プロファイル作成 (CRTUSRPRF) 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。 OS/400 へのサインオンに使用される。

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。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。

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、 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)

システム保守ツール (SST) を使用することで、 OS/400 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、SST 開始 (STRSST) 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、OS/400 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

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。 • 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 を使用できる機能特権

特性	DST	SST
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、 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保守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保守機能にアクセスする場合に必要になるユーザー 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
- 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 に付与されている具体的な権限について詳しくは、

「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、『オペレーション・コンソール』のトピック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、 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。

保守ツール・ユーザー ID を追加作成することにより、セキュリティー管理者は、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。

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ー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 を使用するときに、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ー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 31 ページの『サービス機能の使用のモニター』を行う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。装置 ID およびオペレーション・コンソールを用いた装置 ID について詳しくは、「iSeries セキュリティーの手引き」

 および『オペレーション・コンソール構成のセキュリティー (Secure your Operations Console configuration)』を参照してください。

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ー・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ー・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

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。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 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」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」画面が表示されます。
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。

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ーを実行するには、保守ツール・サーバーを使用可能にする必要があります。 29 ページの『保守ツール・サーバーの構成』は、DST または OS/400 (あるいはその両方) に合わせて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:

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 8*xx* 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 OS/400 の区画を管理する必要があります。

第 5 章 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。

15 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。

29 ページの『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。

31 ページの『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 15 ページの『保守ツール・ユーザー ID の管理』を行うことができます。

保守ツールへのアクセスには、次のいずれかの方法を使用します。

- 『DST の使用による保守ツールへのアクセス』
- 14 ページの『SST の使用による保守ツールへのアクセス』
- 14 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』

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。

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。

© Copyright IBM Corp. 2003, 2004

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 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 PWRDWNSYS *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」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。

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。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
- 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. OS/400 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。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、 15 ページの『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:** 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 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、 12 ページの『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。

サーバーで **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、12 ページの『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。

22 ページの『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。

25 ページの『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。

27 ページの『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。

28 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』
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、 22 ページの『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。

DST または SST の使用による保守ツール・ユーザー ID の構成:

- 『DST の使用による保守ツール・ユーザー ID の構成』
- 19 ページの『SST の使用による保守ツール・ユーザー ID の構成』

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 を構成すると、 22 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』が可能になります。

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、または削除を行います。

- 『DST の使用による保守ツール・ユーザー ID の作成』
- 17 ページの『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』
- 17 ページの『DST の使用による保守ツール・ユーザー ID の記述の変更』
- 17 ページの『DST の使用による保守ツール・ユーザー ID の表示』
- 18 ページの『DST の使用による保守ツール・ユーザー ID の使用可能化』
- 18 ページの『DST の使用による保守ツール・ユーザー ID の使用不可化』
- 18 ページの『DST の使用による保守ツール・ユーザー ID の削除』

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す。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:** このフィールドのデフォルト値は 2 (いいえ) です。
   - **パスワードの有効期限切れの設定:** このフィールドのデフォルト値は 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 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、22 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』を参照してください。

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。
   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) 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 (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、機能特権はデフォルト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。
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 を構成すると、 23 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』が可能になります。

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、または削除を行います。

- 『SST の使用による保守ツール・ユーザー ID の作成』
- 20 ページの『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』
- 20 ページの『SST の使用による保守ツール・ユーザー ID の記述の変更』
- 20 ページの『SST の使用による保守ツール・ユーザー ID の表示』
- 21 ページの『SST の使用による保守ツール・ユーザー ID の使用可能化』
- 21 ページの『SST の使用による保守ツール・ユーザー ID の使用不可化』
- 21 ページの『SST の使用による保守ツール・ユーザー ID の削除』

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 と装置の処理 (Work with service tools user IDs and devices) を選択する。
4. 「保守ツール・ユーザー ID と装置の処理 (Work with Service Tools User IDs and Devices)」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す。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:** このフィールドのデフォルト値は 2 (いいえ) です。
- **パスワードの有効期限切れの設定:** このフィールドのデフォルト値は 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 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、 23 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』を参照してください。

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 と装置の処理 (Work with service tools user IDs and devices) を選択する。
3. 「保守ツール・ユーザー ID と装置の処理 (Work with Service Tools User IDs and Devices)」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。
   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) 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 (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、機能特権はデフォルト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 と装置の処理 (Work with service tools user IDs and devices) を選択する。
3. 「保守ツール・ユーザー ID と装置の処理 (Work with Service Tools User IDs and Devices)」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 と装置の処理 (Work with service tools user IDs and devices) を選択する。
3. 「保守ツール・ユーザー ID と装置の処理 (Work with Service Tools User IDs and Devices)」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。

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 と装置の処理 (Work with service tools user IDs and devices) を選択する。
3. 「保守ツール・ユーザー ID と装置の処理 (Work with Service Tools User IDs and Devices)」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 と装置の処理 (Work with service tools user IDs and devices) を選択する。
3. 「保守ツール・ユーザー ID と装置の処理 (Work with Service Tools User IDs and Devices)」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。
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 と装置の処理 (Work with service tools user IDs and devices) を選択する。
3. 「保守ツール・ユーザー ID と装置の処理 (Work with Service Tools User IDs and Devices)」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、 15 ページの『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、 28 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』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セキュリティー保守ツール・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 25 ページの『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。

保守ツール・ユーザー ID とパスワードを変更します。

- 『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』
- 23 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』
- 24 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』

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」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。デフォルト値は 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。

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 と装置の処理 (Work with service tools user IDs and devices) を選択する。
4. 「保守ツール・ユーザー ID と装置の処理 (Work with Service Tools User IDs and Devices)」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。デフォルト値は 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。

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。

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、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、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

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。

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

デフォルト・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. 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、「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 を許可する (Allow a service tools user ID with a default and expired password)」フィールドの設定を「いいえ」から「はい」に変更する。

2. 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します。
   a. SST を開始する。
   b. パスワードがデフォルト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 (Password has expired)」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、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・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、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」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 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。

QSECOFR 保守ツール・ユーザー ID 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・パスワードの変更) と入力する。次に、F4 キーを押します (Enter キーは押さないでください)。次のような「IBM 保守ツール・パスワードの変更 (CHGDSTPWD)」画面が表示されます。

```
+------------------------------------------------------------------------------+
|                    IBM 保守ツール・パスワードの変更  (CHGDSTPWD)              |
|                                                                              |
| 選択項目を入力して，実行キーを押してください。                               |
|                                                                              |
| パスワード  . . . . . .  *SAME        *SAME, *DEFAULT                        |
|                                                                              |
+------------------------------------------------------------------------------+
```

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、 28 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』を参照してください。

保守ツール・セキュリティー・データの保管と復元

保守ツール・セキュリティー・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・セキュリティー・データは、DST から処理できます。

保守ツール・セキュリティー・データの保管

DST を使用して保守ツール・セキュリティー・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。「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。「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。セキュリティー・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. 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。セキュリティー・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・セキュリティー・データの復元

DST を使用して保守ツール・セキュリティー・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. 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. 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) 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

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。詳しくは、 22 ページの『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)』
- 30 ページの『保守ツール・サーバーの構成 (OS/400 用)』

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 を開始済みにしている場合です。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 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。

- 『DST の使用による保守ツール・サーバーの構成』
- 30 ページの『SST の使用による保守ツール・サーバーの構成』

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・アダプターの構成 (Configure Service Tools Adapter)) を選択し、 Enter キーを押す。「コンソール・タイプの選択」画面が表示されます。
4. 「保守ツール・アダプターの構成 (Configure Service Tools Adapter)」画面で、 LAN アダプター (まだ入力されていない場合) 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) を押します。
5. F7 (保管 (Store)) 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。

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 と装置の処理 (Work
| with Service Tools User IDs and Devices)) を選択する。
| 2. 「保守ツール・ユーザー ID と装置の処理 (Work with Service Tools User IDs and Devices)」画面で、
| オプション 4 (保守ツール LAN アダプターの構成 (Configure service tools LAN adapter)) 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 (Configure Service Tools LAN Adapter)」画面で、 LAN アダプ
| ター (まだ入力されていない場合) と 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 (Store)) 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。

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' (このエントリーは小文字で入力し、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-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、テーブル項目を追加する。
6. 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。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/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-sts 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 8*xx* 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 OS/400 の
| 区画を管理する必要があります。詳しくは、『HMC による区分化 (Partitioning with an HMC)』を参照
| 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「**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。
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ー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・セキュリティー・ログに記録されます。

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係するアクティビティーが日時順に表示されます。
6. (オプション) このログを印刷するには、F6 (印刷) を押す。
7. (オプション) 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が特権の付与または取り消しに関するものである場合、以下の情報を示す「保守ツール機密保護ログの詳細の表示」画面が表示される。
     - アクティビティーの日付/時刻
     - アクティビティーの記述
     - 変更者のユーザー ID
     - 影響を受けたユーザー ID
     - 特権の記述
   - 選択したアクティビティーがユーザー ID の使用可能化または使用禁止に関するものである場合、以下の情報を示す「保守ツール機密保護ログの詳細の表示」画面が表示される。
     - アクティビティーの日付/時刻
     - アクティビティーの記述
     - 変更者のユーザー ID
     - 影響を受けたユーザー ID
   - 選択したアクティビティーがその他のタイプのイベントに関するものである場合、以下の情報を示す「保守ツール機密保護ログの詳細の表示」画面が表示される。
     - アクティビティーの日付/時刻
     - アクティビティーの記述
     - 影響を受けたユーザー 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**」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
   - 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 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。

第 6 章 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: 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「システム機密保護の処理」オプションにアクセスし、「*省略時値で有効期限切れのパスワードをもつ保守ツール・ユーザー ID のパスワードを変更可能*」の設定値を 1 (NO) 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 (YES) に戻します。

© Copyright IBM Corp. 2003, 2004

第 7 章 保守ツール関連情報

以下に、本トピック『保守ツール ユーザー ID とパスワード』に関連する、 iSeries マニュアル、 IBM Redbooks(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 セキュリティーの手引き」 (約 1856 KB)
- 「iSeries Service Functions」 (約 1780 KB)
- 「iSeries 機密保護解説書」 (約 6382 KB)

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分化 (Partitioning with iSeries Navigator)
- iSeries ナビゲーター

PDF ファイルの保管

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

1. ブラウザーで PDF を右マウス・ボタンでクリックする (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。

© Copyright IBM Corp. 2003, 2004

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。 IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

© Copyright IBM Corp. 2003, 2004

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、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

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。

本書に示されている図や仕様は、IBM の書面による許可を得ずにその一部または全部を複製してはいけません。

IBM は、指定された特定のマシンを対象として本書を作成しています。その他の使用および使用結果については、IBM は何ら保証責任を負いません。

IBM のコンピューター・システムには、破壊または損失したデータが検出されない危険性を減少するために設計されたメカニズムが含まれています。しかし、この危険をゼロにすることはできません。不意の停電によるシステムの休止やシステム障害、電力の変動または停電、もしくはコンポーネント障害を経験するユーザーは、停電または障害が起きた時刻もしくはその近辺で行われたシステム操作とセーブまたは転送されたデータの正確性を検証する必要があります。さらに、ユーザーはそのような不安定で危機的な状況で操作されたデータを信頼する前に、独自のデータ検証手順を確立する必要があります。ユーザーはシステムおよび関連ソフトウェアに適用できる更新情報または修正がないか、定期的に IBM の Web サイトをチェックする必要があります。

商標

以下は、IBM Corporation の商標です。

e(ロゴ)server
eServer
i5/OS
IBM
iSeries
Operating System/400
OS/400

電波障害自主規制への適合性

以下のクラス A ステートメントは、IBM eServer i5、eServer p5 サーバー、および IBM eServer OpenPower サーバーに適用されます (ただし、明確にクラス B に識別されるサーバーは除きます)。

以下のクラス B ステートメントは、モデル 9111-520 (スタンドアロン型) に適応されます。

情報処理装置等電波障害自主規制協議会 (VCCI) 表示

電波障害自主規制 届出装置の記述

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

以下の記述は当 IBM 製品に適用されます。当製品と併用されるその他の IBM 製品に関する同様の記述は、それらの製品に関連した資料に記載されています。

情報処理装置等電波障害自主規制協議会 (VCCI) 表示

電波障害自主規制 届出装置の記述

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをしてください。

資料に関するご使用条件

お客様がダウンロードされる資料につきましては、以下の条件にお客様が同意されることを条件にその使用が認められます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。 IBM は、これらの資料の内容についていかなる保証もし

ません。これらの資料は、特定物として現存するままの状態で提供され、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。

これらの資料の著作権はすべて、IBM Corporation に帰属しています。

お客様が、このサイトから資料をダウンロードまたは印刷することにより、これらの条件に同意されたものとさせていただきます。

製品のリサイクルと廃棄

この装置には、使用終了時に特別な処理および廃棄を必要とする、鉛や銅/ベリリウム合金が使われている回路ボード、ケーブル、電磁適合性ガスケットやコネクターなどの材料が含まれています。この装置を廃棄する前に、それらの部品を取り外し、該当する規定に従ってリサイクルするか廃棄する必要があります。IBM では、いくつかの国で製品回収プログラムを提供しています。製品リサイクル・オファリングについては、IBM のインターネット・サイト (http://www.ibm.com/ibm/environment/products/prp.shtml) を参照してください。

IBM では、情報技術 (IT) 機器の所有者に、機器が必要でなくなったときに責任を持って機器のリサイクルを行うことをお勧めしています。 また、機器の所有者による IT 製品のリサイクルを支援するため、さまざまなプログラムとサービスを提供しています。製品リサイクル・オファリングについては、IBM のインターネット・サイト (http://www.ibm.com/ibm/environment/products/prp.shtml) を参照してください。

バッテリー回収プログラム

この製品には、密封された鉛酸、ニッケル・カドミウム、ニッケル水素、リチウム、およびリチウム・イオン・バッテリーが含まれている場合があります。特定のバッテリー情報については、お手元のユーザー・マニュアルまたはサービス・マニュアルを参照してください。バッテリーは、正しくリサイクルするか廃棄する必要があります。リサイクル施設がお客様の地域にない場合があります。米国以外の国におけるバッテリーの廃棄については、http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml を参照するか、またはお客様の地域の廃棄物処理施設にお問い合わせください。

米国では、IBM は、IBM 装置からの使用済みの IBM の密封された鉛酸バッテリー・パック、ニッケル・カドミウム・バッテリー・パック、ニッケル水素バッテリー・パック、その他のバッテリー・パックの再利用、リサイクル、または適切な廃棄のための回収プロセスを確立してあります。これらのバッテリーの正しい廃棄については、IBM 1-800-426-4333 にお問い合せください。お問い合せの前に、バッテリー上に記載されている IBM 部品番号をご用意ください。

オランダでは、次のものが適用されます。

台湾では、以下が適用されます。バッテリーをリサイクルしてください。

IBM 暗号化コプロセッサー・カードの回収プログラム

本マシンには、水銀を含有するポリウレタン材料を組み込んだオプション・フィーチャー、暗号化コプロセッサー・カードが含まれることがあります。このカードの廃棄にあたっては、地方自治体の条例または規則に従ってください。IBM は、特定の IBM 暗号化コプロセッサー・カードの回収プログラムを確立しました。詳しい情報は、http://www.ibm.com/ibm/environment/products/prp.shtml にあります。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12