IBM

eserver

iSeries

iSeries セキュリティーの手引き

バージョン 5

SD88-5065-05
(英文原典：SC41-5300-07)

IBM

@server

iSeries

iSeries セキュリティーの手引き

バージョン 5

SD88-5065-05
(英文原典：SC41-5300-07)

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、 185 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 OS/400 (プロダクト番号 5722-SS1) のバージョン 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： SC41-5300-07
iSeries
Tips and Tools
for Securing Your iSeries
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 2004.4

この文書では、平成明朝体™W3、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™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

目次

図

表

iSeriesセキュリティーの手引き (SD88-5065-05)

組織において、コンピューターの役割は、急速に変化しています。IT (情報技術) 管理者、ソフトウェア・プロバイダー、機密保護管理者、および監査担当者は、これまで通常どおり行ってきた各種業務について、別の角度から見直す必要があります。iSeries セキュリティーも、そうしたものの一つです。

現在のシステムは、従来の会計アプリケーションとは大きく異なる新しい機能を多数提供しています。システムへの入り方も新しくなっており、たとえば、LAN、交換回線 (ダイヤルアップ)、無線などのあらゆるタイプのネットワークが利用されています。サインオン表示を見ることなくシステムへ入ることもよくあります。企業の多くは、その規模を拡大し、やがては、自社仕様のネットワークまたはインターネットを使用した「大企業」へと発展していきます。

システム・セキュリティーを取り巻く環境は、気付いてみるとすっかり変わっているようです。こうした急速に変化している環境の中で、システム管理者と機密保護管理者が情報資産を保護する方法について関心をもつようになったのも当然のことです。

本書では、iSeries のセキュリティー機能の使用のための、およびセキュリティーを考慮した操作手順の確立のための一連の実用的な提案を行います。本書における推奨事項は、平均的なセキュリティーの要件および機密漏れの危険性を伴う導入先に適用されます。本書では、使用可能な iSeries セキュリティー機能のすべてを説明しているわけではありません。その他のオプションについて知りたい場合、あるいはさらに詳しいバックグラウンド情報が必要な場合には、181 ページの『第 17 章 関連情報』に記載されている資料を参照してください。

本書では、OS/400 の一部であるセキュリティー・ツールのセットアップ方法と使用方法についても説明します。31 ページの『第 4 章 セキュリティー・ツールを使用するための iSeries の構成』および 32 ページの『セキュリティー・コマンドのコマンドおよびメニュー』に、セキュリティー・ツールについての参照情報が記載されています。本書では、ツールの使用例を提供します。

本書の対象読者

機密保護担当者または**機密保護管理者**には、システムのセキュリティーについての責任があります。通常、以下のような業務を行います。

- ユーザー・プロファイルのセットアップと管理
- セキュリティーに影響を与えるシステム全般にわたる値の設定
- オブジェクトに対する権限の管理
- セキュリティー・ポリシーの実施とモニター

1 つまたは複数の iSeries システムのセキュリティー管理の担当者が、本書の対象読者です。本書の説明は以下のことを前提にしています。

- サインオンやコマンド使用などの基本的な iSeries 操作手順に精通していること。

- セキュリティー・レベル、セキュリティー・システム値、ユーザー・プロファイル、およびオブジェクト・セキュリティーといった iSeries セキュリティーの基本的な要素について精通していること。

  注: 3 ページの『第 1 章 iSeries セキュリティーの基本要素』では、これらの要素の検討を行います。ユーザーがこれらの基本要素について熟知していない場合には、本書を使用する前に iSeries Information Center の『基本システム・セキュリティーおよび*計画*』をお読みください。詳細は、『前提条件および関連情報』を参照してください。

- セキュリティー・レベル (QSECURITY) のシステム値を最低でも 30 に設定することにより、システムでセキュリティーを活動状態にしていること。

IBM® では、iSeries のセキュリティー機能を絶えず強化しています。これらの機能強化を利用するには、ご使用のリリースに現在使用できる累積修正パッケージを定期的に評価してください。セキュリティーに関係のある修正が含まれているかどうか調べてください。

本書の使用方法

セキュリティー・ツールを使用するようにシステムをセットアップしていない場合、あるいは前のリリース用に Security ToolKit for OS/400 を導入している場合は、以下のことを行ってください。

1. 11 ページの『第 2 章 iSeries セキュリティー・ウィザードおよび eServer セキュリティー・プランナー』から開始してください。ここでは、どのセキュリティー・ツールが推奨されるか選択するためのこれらの機能の使用方法、およびそれらの開始方法が説明されています。
2. さらに基本的なセキュリティー情報については、iSeries™ Information Center のオンライン情報で『機密保護解説書』を参照してください。

ご注意

本書には、iSeries の保護に関するヒントが多数記載されています。ただし、お客様のシステムにそのすべてが必要になるとは限りません。本書を使用して、危険にさらされる可能性のある機密部分とその対応策について学んでください。次に、システムで最も重要な部分について、セキュリティーを適用するようにしてください。

前提条件および関連情報

iSeries Information Center は、iSeries の技術情報検索の開始点として使用します。

Information Center には、次の 2 通りの方法でアクセスすることができます。

- 以下の Web サイトからアクセスする。

  `http://www.ibm.com/eserver/iseries/infocenter`

- 「*iSeries V5R3 Information Center*, SK88-8055-03 CD-ROM からアクセスする。この CD-ROM は、新規 iSeries ハードウェアまたは IBM Operating System/400 ソ

フトウェア・アップグレードをご注文いただくと同梱されています。また、次の Web サイトにアクセスして、IBM Publications Center から CD-ROM を注文することもできます。

http://www.ibm.com/shop/publications/order

iSeries Information Center には、ソフトウェアとハードウェアのインストール、Linux、 WebSphere®、 Java™、高可用性、データベース、論理区画、CL コマンド、およびシステム・アプリケーション・プログラミング・インターフェース (API) など、新規あるいはアップデートされた iSeries 情報が含まれています。また、iSeries ハードウェアとソフトウェアの計画、トラブルシューティング、および構成を支援するためのアドバイザーとファインダーを提供します。

新規のハードウェアをご注文いただくと、「*iSeries セットアップおよびオペレーション*, SK88-8058-02 が提供されます。この CD-ROM には、IBM @server IBM e (ロゴ) server iSeries Access for Windows および EZ セットアップ・ウィザードが含まれています。 iSeries Access ファミリー は、PC を iSeries サーバーに接続するための、強力なクライアントおよびサーバー機能のセットを提供します。 EZ セットアップ・ウィザードは、多数の iSeries セットアップ・タスクを自動化します。

ご意見をお寄せいただく場合

最も正確で高品質な情報を提供する上で、読者のフィードバックは欠かせません。IBM では、本書や他の iSeries の資料に関するご意見をお待ちしております。以下の項目は必ずご記入ください。

- 資料名または iSeries Information Center のトピック
- 資料番号
- ご意見をお寄せいただくページの番号またはトピック

第 1 部 基本 iSeries セキュリティー

第 1 章 iSeries セキュリティーの基本要素

本章では、iSeries セキュリティーを提供するために使用する基本要素について、簡単に説明します。本書の他の部分では、応用編として、こうしたセキュリティー要素を使用して、ユーザーの組織の要件を満たすヒントを記載しています。

セキュリティー・レベル

セキュリティー・レベル (QSECURITY) システム値を設定することにより、システムで実施するセキュリティーの程度を選択できます。システムには、5 つのセキュリティーのレベルがあります。

レベル 10:
システムはセキュリティーを実施しません。パスワードは必要ありません。サインオンしたときに指定のユーザー・プロファイルがシステムに存在しない場合、システムはそのユーザー・プロファイルを作成します。

重要:

V4R3 およびそれ以降のリリースでは、QSECURITY システム値を 10 に設定することはできません。現在、システムがセキュリティー・レベル 10 の場合、バージョン 4 リリース 3 を導入したときに、セキュリティー・レベルはレベル 10 のままになります。セキュリティー・レベルをそれ以外の値に変更すると、レベル 10 に戻すことはできません。レベル 10 ではセキュリティー保護がないため、IBM ではレベル 10 はお勧めしません。**IBM は、セキュリティー・レベル 10 で起こる問題をサポートしません。ただし、その問題がそれより高いセキュリティー・レベルでも生じる場合は除きます。**

レベル 20:
システムへサインオンする際に、ユーザー ID とパスワードが必要になります。セキュリティー・レベル 20 は、多くの場合に**サインオン・セキュリティー**と呼ばれます。デフォルトで、すべてのユーザーが *ALLOBJ 特殊権限をもっているため、すべてのユーザーに全オブジェクトへのアクセス権があります。

レベル 30:
システムへサインオンする際に、ユーザー ID とパスワードが必要になります。ユーザーはデフォルトではなにも権限をもっていないため、オブジェクトを使用するには、そのための権限が必要です。これは、**リソース・セキュリティー**と呼ばれます。

レベル 40:
システムへサインオンする際に、ユーザー ID とパスワードが必要になります。リソース・セキュリティーに加え、システムは**保全性保護**機能を提供します。オペレーティング・システムへのインターフェースのパラメーターの妥当性検査などの保全性保護機能は、システムに精通しているユーザーの攻撃から、システムおよびシステム上のオブジェクトの両方を保護するための

ものです。ほとんどのインストール・システムの場合、レベル 40 が推奨されるセキュリティー・レベルです。V4R5 またはそれ以降のリリースを使用する新規 iSeries システムを受け取った場合、セキュリティー・レベルは 40 に設定されています。

レベル 50:
システムへサインオンする際に、ユーザー ID とパスワードが必要になります。システムは、レベル 40 のリソース・セキュリティーと保全性保護を両方とも実施しますが、システム状態プログラムとユーザー状態プログラムの間のメッセージ処理の制限などの**拡張保全性保護**が追加されます。セキュリティー・レベル 50 は、非常に高いセキュリティー要件がある iSeries システムのためのものです。

注: レベル 50 は、C2 認証 (および FIPS-140 認証) のための必須レベルです。

「*iSeries 機密保護解説書*」の第 2 章には、セキュリティー・レベルについて詳しい情報が記載されています。また、あるセキュリティー・レベルから別のセキュリティー・レベルに変更する方法も記載されています。

グローバル設定

システムには、作業内容をシステムへ入力する方法と、他のシステム・ユーザーに対するシステムの表示方法を制御するためのグローバル設定があります。これらの設定には、以下のものが含まれます。

セキュリティー・システム値:
セキュリティー・システム値を使用して、システムのセキュリティーを制御します。これらの値は、4 つのグループに分かれます。
- 汎用のセキュリティー・システム値
- セキュリティーに関連するその他のシステム値
- パスワードを制御するシステム値
- 監査を制御するシステム値

本書の一部のトピックでは、特定のシステム値のセキュリティーにおける意味について説明します。「*iSeries 機密保護解説書*」の第 3 章では、すべてのセキュリティー関連システム値について説明しています。

ネットワーク属性:
ネットワーク属性は、システムが他のシステムを含むネットワークに参加する (または参加しないことを選択する) 方法を制御します。「*AS/400e シリーズ 実行管理の手引き*」では、ネットワーク属性についてさらに詳しく調べることができます。

サブシステム記述とほかの実行管理機能要素:
実行管理機能要素は、作業内容をシステムへ入力する方法と作業が実行される環境を決定します。本書の一部のトピックでは、一部の実行管理機能値のセキュリティーにおける意味について説明します。「*AS/400e シリーズ 実行管理の手引き*」には、すべての情報が記載されています。

通信構成:
ユーザーの通信構成も作業内容をシステムへ入力する方法に影響を与えます。本書の一部のトピックでは、ユーザーのシステムがネットワークに参加したときにそのシステムを保護するための提案を示します。

ユーザー・プロファイル

すべてのシステム・ユーザーに、ユーザー・プロファイルが**必要です**。ユーザー・プロファイルを作成しておかなければ、ユーザーはサインオンできません。ユーザー・プロファイルを使用して、 DASD ダンプおよび主記憶域ダンプなどの保守ツールへのアクセスを制御することもできます。詳しくは、 69 ページの『保守ツールの管理』を参照してください。

ユーザー・プロファイルは、強力かつ柔軟なツールです。ユーザーが実行可能な事柄を制御し、ユーザーに対するシステムの表示をカスタマイズします。「*iSeries 機密保護解説書*」には、ユーザー・プロファイルのすべてのパラメーターが記載されています。

グループ・プロファイル

グループ・プロファイルは、特別なタイプのユーザー・プロファイルです。グループ・プロファイルは、各ユーザーに個々に権限を与えるのではなく、ユーザー・グループに権限を定義する場合に使用できます。また、プロファイル・コピー機能を使用して、ユーザー・プロファイルを個別に作成するときにグループ・プロファイルをパターン (ひな型) として使用することもできます。あるいは iSeries ナビゲーターを使用する場合、「セキュリティーの方針」メニューを使用してユーザー権限を編集することもできます。

「*iSeries 機密保護解説書*」の第 5 章と第 7 章では、グループ・プロファイルの計画と使用についてさらに詳しい情報を記載しています。

リソース・セキュリティー

システムでのリソース・セキュリティーによって、オブジェクトを使用できるユーザーとそのオブジェクトの使用方法を定義することができます。オブジェクトにアクセスできることを**権限**と呼びます。オブジェクト権限を設定するときは、ユーザーが自分たちの作業を十分に行える権限で、かつシステムの表示や変更はできないような権限を与えるように注意してください。オブジェクト権限によって、ユーザーに特定のオブジェクトに対する許可を与え、そのオブジェクトでユーザーは何ができるかを指定することができます。オブジェクト資源を特定の詳細なユーザー権限によって、たとえばレコードの追加または変更というように制限することができます。システム資源を使用して、*ALL、*CHANGE、*USE、および *EXCLUDE など特定のシステム定義の権限のサブセットへのアクセスをユーザーに与えることができます。

ファイル、プログラム、ライブラリー、およびディレクトリーは、リソース・セキュリティー保護を必要とする最も一般的なシステム・オブジェクトですが、システム上のオブジェクトであればどの個別オブジェクトに対しても権限を指定できます。

『第 5 章 オブジェクト権限による情報資産の保護』では、システムにおけるオブジェクト権限のセットアップの重要性について説明します。「*iSeries 機密保護解説書*」の第 5 章では、リソース・セキュリティーのセットアップのオプションについて説明しています。

プログラム機能への制限アクセス

プログラム機能への制限アクセスにより、そのプログラムでは保護する iSeries のオブジェクトがない場合でも、プログラムにセキュリティーを提供することができます。 プログラム機能への制限アクセスが V4R3 でサポートされる前は、権限リストあるいはその他のオブジェクトを作成し、そのオブジェクトへの権限を検査してプログラム機能へのアクセスを制御していました。 現在ではプログラム機能への制限アクセスを使用して、アプリケーション、アプリケーションの一部、あるいはプログラム内の機能へのアクセスをさらに簡単に制御することができます。

iSeries ナビゲーターを使用してアプリケーション機能へのユーザー・アクセスを管理するには 2 つの方法があります。最初の方法では、以下のようにしてアプリケーション管理サポートを使用します。

1. アクセス設定を変更したい機能が入っているシステムを右マウス・ボタンでクリックする。
2. 「**アプリケーション管理**」を選択する。
3. 管理システム上にいる場合は、「**ローカル設定**」を選択する。それ以外の場合は、次のステップを継続する。
4. 管理可能な機能を選択する。
5. 該当する場合は、「**デフォルト・アクセス**」を選択する。これを選択した場合は、デフォルトですべてのユーザーがこの機能にアクセスすることを許可することになる。
6. 該当する場合は、「**すべてのオブジェクト・アクセス**」を選択する。これを選択した場合は、全オブジェクト・システム特権を持つすべてのユーザーがこの機能にアクセスすることを許可することになる。
7. 該当する場合は、「**カスタマイズ**」を選択する。「**アクセスのカスタマイズ**」ダイアログ上の「**追加**」ボタンおよび「**削除**」ボタンを使用して、「**許可されるアクセス**」リスト内および「**否認されるアクセス**」リスト内のユーザーまたはグループを追加または除去する。
8. 該当する場合は、「**カスタマイズの除去**」を選択する。これを選択すると、選択された機能についてカスタマイズされたアクセスがすべて削除される。
9. 「**OK**」をクリックし、「**アプリケーション管理**」ダイアログを閉じる。

ユーザー・アクセスを管理するための 2 番目の方法は、iSeries ナビゲーターのユーザーおよびグループのサポートに関連するものです。

1. iSeries ナビゲーターで、「**ユーザーおよびグループ**」を展開する。
2. 「**すべてのユーザー**」、「**グループ**」、または「**グループ内にないユーザー**」を選択し、ユーザーおよびグループのリストを表示する。
3. ユーザーまたはグループを右マウス・ボタンでクリックし、「**プロパティー**」を選択する。
4. 「**機能**」をクリックする。
5. 「**アプリケーション**」タブをクリックする。
6. このページを使用して、ユーザーまたはグループのアクセス設定を変更する。
7. 「**OK**」を 2 度クリックし、「**プロパティー**」ダイアログを閉じる。

iSeries ナビゲーターのセキュリティー問題の詳細については、 171 ページの『iSeries ナビゲーター・セキュリティー』を参照してください。

アプリケーション作成者であれば、プログラム機能への制限アクセス API を使用して、以下を行うことができます。

- 機能の登録
- 機能についての情報の取り出し
- 機能を使用できるユーザーと使用できないユーザーの定義
- 機能を使用する許可がユーザーに与えられているかどうかのチェック

注: このサポートは、リソース・セキュリティーの代用とすることは**できません**。プログラム機能への制限アクセスは、ユーザーが別のインターフェースから資源 (ファイルやプログラムなど) にアクセスすることを防ぐことはできないからです。

アプリケーション内でこのサポートを使用するためには、アプリケーション・プロバイダーは、アプリケーションの導入の際に機能を登録しなければなりません。登録された機能は、アプリケーションの特定機能のコード・ブロックに対応します。ユーザーがこのアプリケーションを実行すると、アプリケーションは、コード・ブロックを呼び出す前に API を呼び出します。API は使用チェックの API を呼び出して、機能を使用する許可がそのユーザーに与えられているかどうかを調べます。ユーザーが登録された機能の使用を許可されている場合、コード・ブロックが実行されます。ユーザーが機能の使用を許可されていない場合、そのユーザーはコード・ブロックを実行できません。

注: API では、登録データベース (WRKREGINF) に 30 文字の機能 ID を登録します。機能への制限アクセス API で使用される機能 ID に関連した出口点はありませんが、出口点を持つ必要があります。レジストリーに何かを登録するために、出口点の形式名を提供**しなければなりません**。これを実行するため、機能登録 API はダミーの形式名を作成し、登録するすべての機能にこのダミーの形式名を使用します。これはダミーの形式名なので、出口点プログラムが呼び出されることはありません。

システム管理者は、機能へのアクセスが許可されるユーザーまたは拒否されるユーザーを指定します。管理者は、プログラム機能へのアクセスを管理する API を使用するか、あるいは iSeries ナビゲーターのアプリケーション管理 GUI を使用することができます。プログラム機能へのアクセスを制限する API については、「*iSeries server API Reference*」を参照してください。機能へのアクセスの制御に関する詳細は、 171 ページの『iSeries ナビゲーター・セキュリティー』を参照してください。

セキュリティー監査

システム・セキュリティーの監査は、次のような理由から行われます。

- セキュリティー計画が完全であるかどうかを評価するため。
- 計画したセキュリティー管理が行われているかどうかを確認するため。このタイプの監査は、通常、日単位のセキュリティー管理の一部として機密保護担当者に

よって行われます。また、定期的に行われるセキュリティー・レビューの一部として、さらに綿密に、内部または外部の監査担当者によって行われることもあります。

- システム・セキュリティーが、システム環境に対し行なわれた変更に対応できていることを確認するため。セキュリティーに影響する変更には、次のようなものがあります。
  - システム・ユーザーによる新規オブジェクトの作成
  - システムへの新規ユーザーの許可
  - オブジェクト所有権の変更 (権限が調整されていない)
  - 責任の変更 (ユーザー・グループの変更)
  - 一時的権限 (適時に取り消されていない)
  - 新規プロダクトの導入
- 将来のイベント (新規アプリケーションの導入、上位セキュリティー・レベルへの移行、通信ネットワークの設定など) の準備を行うため。

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

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

セキュリティー監査についての詳細は、「*iSeries 機密保護解説書*」の第 9 章を参照してください。

例: システム機密保護属性報告書

9 ページの図 1 は、システム機密保護属性印刷 (PRTSYSSECA) コマンドの出力例です。報告書には、通常のセキュリティー要件をもつシステムに推奨されるセキュリティー関連システム値およびネットワーク属性の設定が示されます。また、システムにおける現行の設定値も示されます。

注: 報告書の*現在の値* 列は、システムにおける現行の設定値を示しています。これを推奨値と比較して、機密漏れの箇所がないか調べてください。

システム機密保護属性

システム値 名	現在の値	推奨値
QALWOBJRST	*NONE	*NONE
QALWUSRDMN	*ALL	QTEMP
QATNPGM	QEZMAIN QSYS	*NONE
QAUDENDACN	*NOTIFY	*NOTIFY
QAUDFRCLVL	*SYS	*SYS
QAUDCTL	*AUDLVL	*AUDLVL *OBJAUD
QAUDLVL	*SECURITY	*AUTFAIL *CREATE *DELETE *SECURITY *SAVRST *NOQTEMP

図 1. システム機密保護属性報告書 - 例 (1/4)

QAUTOCFG	0	0
QAUTORMT	1	0
QAUTOVRT	9999	0
QCMNRCYLMT	0 0	0 0
QCRTAUT	*CHANGE	ライブラリー・レベルで制御。
QCRTOBJAUD	*NONE	ライブラリー・レベルで制御。
QDEVRCYACN	*DSCMSG	*DSCMSG
QDSCJOBITV	120	120
QDSPSGNINF	1	1
QINACTITV	60	60
QINACTMSGQ	*ENDJOB	*ENDJOB
QLMTDEVSSN	0	1
QLMTSECOFR	0	1
QMAXSGNACN	2	3
QMAXSIGN	3	3

図 1. システム機密保護属性報告書 - 例 (2/4)

QPWDEXPITV	60	60
QPWDLMTAJC	1	1
QPWDLMTCHR	*NONE	AEIOU@$#
QPWDLMTREP	1	2
QPWDLVL	0	
QPWDMAXLEN	8	8
QPWDMINLEN	6	6
QPWDPOSDIF	1	1
QPWDRQDDGT	1	1
QPWDRQDDIF	0	1
QPWDVLDPGM	*NONE	*NONE
QRETSVRSEC	0	0
QRMTIPL	0	0
QRMTSIGN	*FRCSIGNON	*FRCSIGNON
QSECURITY	50	50
QSHRMEMCTL	1	0
QSRVDMP	*DMPUSRJOB	*NONE
QUSEADPAUT	*NONE	CRTAUTL AUTL(QUSEADPAUT) AUT(*EXCLUDE) CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL) CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)
QVFYOBJRST	1	3

図 1. システム機密保護属性報告書 - 例 (3/4)

システム機密保護属性

ネットワーク

属性名	現在の値	推奨値
DDMACC	*OBJAUT	*REJECT
JOBACN	*FILE	*REJECT
PCSACC	*OBJAUT	*REJECT

図 1. システム機密保護属性報告書 - 例 (4/4)

第 2 章 iSeries セキュリティー・ウィザードおよび eServer セキュリティー・プランナー

iSeries サーバーのセキュリティー・ウィザードおよび eServer セキュリティー・プランナー・ツールは、iSeries サーバーで有効にするセキュリティー値の決定に役立ちます。 iSeries ナビゲーターで iSeries サーバーのセキュリティー・ウィザードを使用すれば、お客様が選択した答えに基づいて、お客様のセキュリティー要件を反映した報告書を作成することができます。この報告書を使用して、システム・セキュリティーを構成することができます。

iSeries セキュリティー・ウィザードまたは eServer セキュリティー・プランナーの使用は、 iSeries サーバーの基本セキュリティー・ポリシーの計画およびインプリメンテーションに役立ちます。この 2 つのツールの目的は、システム上でのセキュリティーのインプリメンテーションおよび管理を簡単にすることです。ウィザードは、OS/400® に組み込まれており、サーバー環境に関する高水準の質問をいくつか表示し、お客様の答えに基づいて、一連の推奨値を提供します。またこの推奨値はウィザードがご使用のシステムに直ちに適用することができます。

eServer セキュリティー・プランナーは、セキュリティー・ウィザードのオンライン・バージョンです。お客様のセキュリティー要件に基づいて項目を選択し、サイトを保護するために必要な機能を推奨する報告書を作成できます。

eServer セキュリティー・プランナーは、ウィザードの Web ベース・バージョンです。ウィザードと同じように、システムにセキュリティーをインプリメントする場合の推奨値を提供します。ただし、プランナーは推奨値を適用することはできません。代わりに、プランナーの質問に対するお客様の答えに基づいて、システムに適用する必要があるシステム・セキュリティー値およびその他の属性のリストを出力します。

セキュリティー・ウィザード

お客様のビジネスに使用する iSeries セキュリティー・システム値を決めることは難しい問題です。 iSeries サーバーへのセキュリティーのインプリメンテーションが初めてだったり、iSeries サーバーの稼働環境が最近変わった場合には、セキュリティー・ウィザードが値の決定に役立ちます。

ウィザードとは?

- ウィザードは、初心者ユーザーがシステムで何かを導入または構成する際に使用するために設計されたツールです。
- ウィザードは、質問形式でユーザーから情報を入手します。各質問に対する答えにより、次の質問が決まります。
- ウィザードがすべての質問を終えると、ユーザーに終了パネルが表示されます。そこでユーザーは「**完了**」ボタンを押して、項目を導入および構成します。

セキュリティー・ウィザードの目的

セキュリティー・ウィザードの目的は、ユーザーからの以下の答えに基づいて構成を行うことです。

- セキュリティー関連のシステム値およびネットワーク属性
- セキュリティー関連のシステムの報告およびモニターの報告
- 管理者情報報告書とユーザー情報報告書の生成
  - 管理者情報報告書には、推奨されるセキュリティーの設定および推奨設定を有効にする前にしなければならない手順が含まれています。
  - ユーザー情報報告書には、ビジネス・セキュリティー・ポリシーに使用できる情報が含まれています。たとえば、パスワード構成規則はこの報告書に含まれます。
- システム上のさまざまなセキュリティー関連項目の推奨される設定値

セキュリティー・ウィザードの目的

- セキュリティー・ウィザードの目的は以下のとおりです。
  - ウィザードの質問に対するユーザーの回答に基づいて、どのようなシステム・セキュリティーを設定すべきかを判別し、適切な場合はその設定を行います。
  - ウィザードは、以下が含まれている詳細な情報報告書を作成します。
    - ウィザードの推奨が記載された報告書
    - 設定の前に行うべき手順の詳細が記載された報告書
    - システムのユーザーに伝えるべき関連情報がリストされた報告書
- これらの項目によって、システムで基本的なセキュリティー・ポリシーを実施します。
- ウィザードは、監査ジャーナル報告書をスケジュールを立てて定期的に実行することを推奨します。スケジュールを立てることで、これらの報告書を、以下の点で有効に活用できます。
  - セキュリティー・ポリシーに従っていることを確認できる。
  - 管理者の承認を受けた場合にのみセキュリティー・ポリシーを変更できる。
  - システム上のセキュリティー関連のイベントをモニターするための報告書をスケジュール化できる。
- ウィザードでは、推奨設定を保管したり、推奨の一部またはすべてをシステムに適用することができます。

注: セキュリティー・ウィザードは同じシステムで何度も使用できるので、以前に導入を行ったユーザーが現在のセキュリティーを再検討することができます。セキュリティー・ウィザードは、V3R7 システム (iSeries ナビゲーターが導入されている場合) およびそれ以降のシステムで使用できます。

iSeries ナビゲーターを使用するには、 IBM iSeries Access for Windows® を Windows 95/NT の PC に導入し、その PC から iSeries サーバーとの接続を確立しておかなければなりません。ウィザードのユーザーは、iSeries サーバーに接続されていなければなりません。ユーザーは、*ALLOBJ、*SECADM、*AUDIT、および *IOSYSCFG の特殊権限を持つユーザー ID を持っている必要があります。
Windows 95/NT の PC を iSeries システムに接続する方法については、Information Center の 『IBM iSeries Access for Windows』トピックを参照してください (詳細は、 xii ページの『前提条件および関連情報』を参照してください)。

セキュリティー・ウィザードにアクセスするには、以下を行います。

1. iSeries ナビゲーターで、使用するサーバーを展開します。
2. 「**セキュリティー**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
   - ユーザーが iSeries ナビゲーターの「**セキュリティー**」オプションを開始すると、ユーザーの特殊権限を検査する要求が iSeries サーバーに送信されます。
   - ユーザーが必要な特殊権限 (*ALLOBJ、*AUDIT、*IOSYSCFG、*SECADM) をどれか 1 つでも持っていない場合は、「**構成**」オプションは表示されず、セキュリティー・ウィザードにアクセスできません。
3. ユーザーが、必要な権限を持っている場合には、以下のことが行われます。
   - 直前のウィザードの応答が検索される。
   - 現行のセキュリティー設定が検索される。

セキュリティー・ウィザードは、3 つの起動画面うちの 1 つを表示します。どの画面が表示されるかは、次の条件のどれが当てはまるかによって異なります。

- ウィザードがターゲット iSeries サーバー用に実行されたことがない。
- ウィザードは以前に実行されたことはあるが、セキュリティーの変更は行われなかった。
- ウィザードは以前に実行され、セキュリティーの変更が実施された。

iSeries ナビゲーターを使用していない場合でも、セキュリティー要件の計画を立てるのに役立つ情報を入手できます。eServer セキュリティー・プランナーは、セキュリティー・ウィザードのオンライン・バージョンです。ただし、1 つだけ異なる点があります。セキュリティー・プランナーは、システムを自動的には構成しません。しかし、お客様の回答に基づいて、推奨されるセキュリティー・オプションに関する報告書を生成します。 eServer セキュリティー・プランナーにアクセスするには、次の Web サイトの eServer Information Center にアクセスしてください。

`http://publib.boulder.ibm.com/eserver/`

eServer セキュリティー・プランナー

eServer セキュリティー・プランナーは、セキュリティー・ウィザードのオンライン・バージョンです。セキュリティー・ウィザードと同じ質問をし、質問の回答に基づき同じ推奨値を生成します。これら 2 つのツールの違いは、以下のとおりです。

- eServer セキュリティー・プランナーは、以下のことは**行いません**。
  - 報告書の作成。
  - 現行設定値と推奨設定値との比較。
  - システム値の自動設定。
- eServer セキュリティー・プランナーからの推奨値を適用することはできません。

eServer セキュリティー・プランナーは、CL プログラムを生成します。このプログラムをカット・アンド・ペーストし編集することにより、独自のセキュリティー構成を自動化できます。また、eServer セキュリティー・プランナーから iSeries サーバー文書に直接リンクすることもできます。これは、この設定がユーザー環境に適当であるかどうかを判別するのに役立つシステム値または報告書についての情報を示します。

eServer セキュリティー・プランナーにアクセスするには、インターネット・ブラウザーで次の URL を指定します。

```
http://publib.boulder.ibm.com/eserver/
```

第 3 章 対話式サインオンの制御

システムへの入力の制限を考えるときには、「サインオン」画面から始めます。「サインオン」画面を使用して、侵入者がシステムにサインオンすることは難しくするために使用できるオプションを以下に示します。

パスワード規則の設定

システムのサインオンを保護するには、以下のことを行います。

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

表 1 の値の組み合わせはかなり制限されたもので、単純なパスワードが作成される可能性を大幅に減らすことを目的としています。しかし、ユーザーは、これらの制限を満たすパスワードの選択が難しく不満を感じる可能性があります。

ユーザーに以下のものを提供することを考えてください。

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

これらの値の設定には、システム・セキュリティー構成 (CFGSYSSEC) コマンドを使用します。これらのシステム値の現行設定を印刷するには、システム機密保護属性印刷 (PRTSYSSECA) コマンドを使用します。

「*iSeries 機密保護解説書*」の第 3 章 42 ページの『システム・セキュリティー構成コマンドによって設定される値』に、CFGSYSSEC コマンドの詳しい情報が記載されています。

表 1. パスワード用のシステム値

システム値の名前	説明	推奨値
QPWDEXPITV	システム・ユーザーがパスワードを変更しなければならない頻度。ユーザー・プロファイルで個々のユーザー用に異なる値を指定することができます。	60 (日)
QPWDLMTAJC	システムが同じ文字の連続使用を妨げるかどうか。	1 (はい)
QPWDLMTCHR	パスワードで使用できない文字。[2]	AEIOU#$@
QPWDLMTREP	パスワードに同じ文字が 2 度以上使用されることをシステムが妨げるかどうか。	2 (連続使用は許可されない)
QPWDLVL	ユーザー・プロファイル・パスワードが 10 文字に制限されているか、それとも最大の 128 文字に制限されているか。	0[3]
QPWDMAXLEN	パスワードの文字の最大数。	8
QPWDMINLEN	パスワードの文字の最小数。	6
QPWDPOSDIF	パスワードのそれぞれの文字が、直前に使用していたパスワードの同一の位置の文字と違わなければならないか。	1 (はい)

表 1. パスワード用のシステム値 (続き)

システム値の名前	説明	推奨値
QPWDRQDDGT	パスワードには少なくとも数字を 1 つ含めなければならないか。	1 (はい)
QPWDRQDDIF	ユーザーが再び同じパスワードを使用するまでに待たなければならない期間。[2]	5 またはそれ以下 (満了間隔)[1]
QPWDVLDPGM	新しく割り当てたパスワードの妥当性を検査するために呼び出す出口プログラム。	*NONE

注:

1. QPWDEXPITV システム値は、ユーザーがパスワードを変更しなければならない頻度を指定します。たとえば、60 日ごとなどです。これは**満了間隔**です。QPWDRQDDIF システム値は、ユーザーが再び同じパスワードを使用するまでに、経過しなければならない満了間隔の数を指定します。「*iSeries 機密保護解説書*」の第 3 章には、これらのシステム値が一緒に作動する方法について詳しく記載されています。
2. パスワード・レベル 2 または 3 では、QPWDLMTCHR は使用されません。詳細は、『パスワード・レベル』を参照してください。
3. 要件に合ったパスワード・レベルを決めるには、 17 ページの『パスワード・レベル変更の計画』を参照してください。

パスワード・レベル

V5R1 のオペレーティング・システムより、QPWDLVL システム値によるパスワード・セキュリティーが向上しました。前のリリースでは、パスワードに限られた範囲の文字しか使用できず、長さも 10 文字に制限されていました。新しいリリースでは、システムに設定されているパスワード・レベルに応じて、パスワード (または、パスフレーズ) に使用できる文字が 128 文字になりました。パスワード・レベルは次のとおりです。

- **レベル 0:** システムの出荷時のレベルです。レベル 0 では、パスワードは 10 文字以下で、A ～ Z、0 ～ 9、#、@、$、および _ 文字しか使用できません。レベル 0 のパスワードは、上位のパスワード・レベルよりセキュリティー性が低くなります。
- **レベル 1:** パスワード・レベル 0 と同じ規則が適用されますが、iSeries Support for Windows Network Neighborhood (これ以降、iSeries NetServer とします) のパスワードは保管されません。
- **レベル 2:** このレベルでは、パスワードが保護されます。このレベルはテストの場合に使用することができます。パスワードが 10 文字以下で、レベル 0 または 1 のパスワードの文字セットを使用している場合、レベル 0 または 1 のユーザーのパスワードは保管されます。このレベルのパスワード (またはパスフレーズ) には次のような特性があります。
  - 長さは 128 文字。
  - 使用可能なすべてのキーボード文字で構成される。
  - 全部ブランクにはできない。ブランクは、パスワードの最後から除去される。
  - 大文字小文字の区別がある。

- **レベル 3:** このレベルのパスワードは最もセキュアで、現在最も高機能の暗号化アルゴリズムを使用します。このレベルのパスワードは、レベル 2 のパスワードと同じ特性をもっています。 iSeries のパスワードは、このレベルでは保管されません。

ネットワーク内のすべてのシステムが次の基準を満たしている場合は、パスワード・レベル 2 および 3 のみを使用してください。

- オペレーティング・システムが V5R1 またはそれ以降である
- パスワード・レベルが 2 または 3 に設定されている

同様に、ユーザーは同じパスワード・レベルを使用してログインしなければなりません。パスワード・レベルはグローバルです。保護するパスワードに応じてレベルを選択することはできません。

パスワード・レベル変更の計画

パスワード・レベルの変更は、慎重に計画しなければなりません。パスワード・レベルの変更計画が適切でないと、他のシステムとの操作が失敗したり、ユーザーがシステムにサインオンできなかったりする可能性があります。QPWDLVL システム値を変更する前に、必ず、SAVSECDTA または SAVSYS コマンドを使用して、セキュリティーを保管してください。現行のバックアップを保有していれば、下位のパスワード・レベルに戻す必要がある場合に、すべてのユーザーのプロファイルに対するパスワードをリセットできます。

パスワード・レベル (QPWDLVL) システム値を 2 または 3 に設定すると、システムおよびシステムとのインターフェースがあるクライアントで使用している製品で問題が起こることがあります。ユーザーがサインオン画面で入力するクリア・テキストではなく、暗号化された形式でパスワードをシステムに送信する製品またはクライアントは、QPWDLVL 2 または 3 用の新しいパスワード暗号化規則で作動するように、アップグレードする必要があります。暗号化パスワードの送信は、**パスワード置換**として知られています。

パスワード置換は、パスワードがネットワーク上を伝送される際にキャプチャーされないようにするために使用されます。QPWDLVL 2 または 3 の新規アルゴリズムをサポートしていない古いクライアントによって生成されたパスワード置換は、特定の文字が正しい場合でも、受け入れられません。これは、暗号化された値を使用してあるシステムから別のシステムを認証する iSeries 間の対等アクセスにも当てはまります。

影響を受ける一部の製品 (たとえば、Java Toolbox など) がミドルウェアとして使用されている場合には、問題が複雑になります。これらのいずれかの製品の前のバージョンを組み込んでいるサード・パーティーの製品は、アップデートされたバージョンのミドルウェアを使用して再作成されるまで、正しく作動しません。

これらのことを考えると、QPWDLVL 値を変更する前に、慎重に計画を立てることが必要であるということがおわかりでしょう。

QPWDLVL を 0 から 1 に変更する際の考慮事項

パスワード・レベル 1 では、Windows 95/98/ME AS/400® Client Support for Windows Network Neighborhood (iSeries NetServer) 製品との通信を必要としないシ

ステムは、iSeries NetServer パスワードをシステムから除去することができます。システムから不要な暗号化パスワードを除去すると、システム全体のセキュリティーが増大します。

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

QPWDLVL を 0 または 1 から 2 に変更する際の考慮事項

パスワード・レベル 2 では、128 文字までの大文字小文字を区別したパスワード (パスフレーズとも呼ばれます) を使用でき、QPWDLVL 0 または 1 に復帰するための最大限の能力が提供されます。

システムのパスワード・レベルに関係無く、パスワード・レベル 2 および 3 のパスワードは、パスワード変更時、またはユーザーによるシステムへのサインオン時に作成されます。システムがまだパスワード・レベル 0 または 1 の時にレベル 2 および 3 のパスワードを作成しておくと、パスワード・レベル 2 または 3 への変更の準備に役立ちます。

QPWDLVL を 2 に変更する前に、DSPAUTUSR または PRTUSRPRF TYPE(*PWDINFO) コマンドを使用して、パスワード・レベル 2 で使用可能なパスワードを持っていないユーザー・プロファイルをすべて探し出す必要があります。コマンドが探し出したプロファイルに応じて、以下のいずれかのメカニズムを使用して、パスワード・レベル 2 または 3 をプロファイルに追加します。

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

  たとえば、パスワードを C4D2RB4Y に変更すると、システムは、C4D2RB4Y および c4d2rb4y というパスワード・レベル 2 のパスワードを生成します。
- パスワードをクリア・テキスト (パスワード置換を使用しない) で表示するメカニズムを通じてシステムにサインオンする。パスワードが有効で、ユーザー・プロファイルにパスワード・レベル 2 および 3 で使用可能なパスワードが無い場合、システムはパスワード・レベル 2 および 3 で使用可能な 2 つの同じパスワードを大文字小文字を区別して作成します。パスワード・レベル 2 または 3 で使用できるように、すべて大文字のパスワードとすべて小文字のパスワードが作成されます。

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

ユーザー・プロファイルにパスワード・レベル 2 および 3 で使用可能なパスワードが無く、ユーザー・プロファイルにパスワード・レベル 0 および 1 で使用可能

なパスワードがある場合に、ユーザーが、クリア・テキスト・パスワードを送信する製品を通じてサインオンすると、システムは、ユーザーをパスワード・レベル 0 のパスワードに対して有効にし、ユーザー・プロファイルにパスワード・レベル 2 のパスワードを 2 つ (前述のように) 作成します。置換サインオンは、パスワード・レベル 2 のパスワードに対して有効になります。

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

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

- TELNET
- iSeries Access
- iSeries Host Servers
- QFileSrv.400
- iSeries NetServer 印刷サポート
- DDM
- DRDA®
- SNA LU6.2

QPWDLVL 2 に変更する前に、セキュリティー・データを保管しておくことを強くお勧めします。保管しておくと、必要時に QPWDLVL 0 または 1 に容易に戻ることができます。

QPWDLVL 2 でいくつかのテストが完了するまで、QPWDMINLEN および QPWDMAXLEN などの他のパスワード・システム値を変更しないことをお勧めします。これらの値を変更しなければ、必要時に QPWDLVL 1 または 0 に容易に戻ることができます。ただし、システムが QPWDLVL を 2 に変更する前に、QPWDVLDPGM システム値を *REGFAC または *NONE のいずれかに指定する必要があります。そのため、パスワード妥当性検査プログラムを使用している場合には、ADDEXITPGM コマンドを使用して、QIBM_QSY_VLD_PASSWRD 出口点に登録できる新しいプログラムを作成することもあります。

iSeries NetServer パスワードは QPWDLVL 2 でもサポートされるので、iSeries NetServer パスワードを必要とする機能/サービスは正しく動作します。

管理者がシステムを QPWDLVL 2 で稼働することに慣れてきたら、長いパスワードを活用するために、パスワード・システム値の変更を開始することができます。ただし、管理者は、長いパスワードが以下の影響を及ぼすことを知っておく必要があります。

- 10 文字を超えるパスワードが指定されると、パスワード・レベル 0 および 1 のパスワードはクリアされる。このユーザー・プロファイルは、システムがパスワード・レベル 0 または 1 に戻っても、サインオンできなくなります。

- パスワードに特殊文字が含まれているか、または単純オブジェクト名の構成規則に従っていない場合 (大文字小文字の区別を除く)、パスワード・レベル 0 および 1 のパスワードはクリアされる。
- 14 文字を超えるパスワードが指定されると、ユーザー・プロファイルの iSeries NetServer パスワードはクリアされる。
- パスワード・システム値は、新しいパスワード・レベル 2 の値にだけ適用され、システムにより生成されたパスワード・レベル 0 および 1 のパスワードまたは iSeries NetServer パスワード値 (生成された場合) には適用されない。

QPWDLVL を 2 から 3 に変更する際の考慮事項

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

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

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

下位パスワード・レベルへの変更

下位の QPWDLVL 値に戻ることは、可能ではありますが、全く問題が無いということはありません。一般的に、下位の QPWDLVL 値から上位の QPWDLVL 値への一方向のみであると考えてください。ただし、下位の QPWDLVL 値を復元しなければならない場合があります。

以降の節で、下位のパスワード・レベルに戻すために必要な作業について説明します。

QPWDLVL を 3 から 2 に変更する際の考慮事項: この変更は、比較的容易に行えます。QPWDLVL を 2 に設定した場合、管理者は、どのユーザー・プロファイルが iSeries NetServer パスワードまたはパスワード・レベル 0 あるいは 1 のパスワードを保有する必要があるかどうかを判断しなければなりません。必要がある場合には、ユーザー・プロファイルのパスワードを有効な値に変更してください。

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

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

QPWDLVL 2 を 1 に変更する際の考慮事項: QPWDLVL を 1 に変更する前に、管理者は、DSPAUTUSR または PRTUSRPRF TYPE(*PWDINFO) コマンドを使用し

て、パスワード・レベル 0 または 1 のパスワードを持っていないユーザー・プロファイルを見付ける必要があります。ユーザー・プロファイルが QPWDLVL の変更後もパスワードを必要とする場合には、管理者は、次のいずれかの方式を使用して、そのユーザー・プロファイル用にパスワード・レベル 0 および 1 のパスワードが作成されるようにしなければなりません。

- CHGUSRPRF または CHGPWD CL コマンドか QSYCHGPW API を使用して、ユーザー・プロファイルのパスワードを変更する。これによって、システムは、パスワード・レベル 2 および 3 で使用可能なパスワードを変更します。さらに、システムは、パスワード・レベル 0 および 1 で使用可能な同じ大文字のパスワードを作成します。以下の条件が満たされる場合に限り、システムは、パスワード・レベル 0 および 1 のパスワードを作成できます。
  - パスワードの長さが 10 文字以下である。
  - パスワードを大文字の EBCDIC 文字 A ～ Z、0 ～ 9、@、#、$、および下線に変換できる。
  - パスワードが数値または下線文字で始まっていない。

  たとえば、パスワードを RainyDay という値に変更すると、システムは、パスワード・レベル 0 および 1 の RAINYDAY というパスワードを作成します。しかし、パスワード値を Rainy Days In April に変更すると、システムは、パスワード・レベル 0 および 1 のパスワードをクリアします (パスワードが長すぎて、ブランクが含まれているため)。

  パスワード・レベル 0 または 1 のパスワードを作成できなかった場合、メッセージまたは指示は出されません。
- パスワードをクリア・テキスト (パスワード置換を使用しない) で表示するメカニズムを通じてシステムにサインオンする。パスワードが有効で、ユーザー・プロファイルにパスワード・レベル 0 および 1 で使用可能なパスワードが無い場合、システムはパスワード・レベル 0 および 1 で使用可能な同じ大文字のパスワードを作成します。システムは、上記の条件が満たされている場合に限り、パスワード・レベル 0 および 1 のパスワードを作成できます。

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

QPWDLVL 2 を 0 に変更する際の考慮事項: 考慮事項は、変更が有効になっても iSeries NetServer パスワードが保存される点を除いて、QPWDLVL 2 を 1 に変更する場合と同じです。

QPWDLVL 1 を 0 に変更する際の考慮事項: QPWDLVL を 0 に変更した後に、管理者は、DSPAUTUSR または PRTUSRPRF コマンドを使用して、 iSeries NetServer パスワードを持っていないユーザー・プロファイルを見つける必要があります。ユーザー・プロファイルが iSeries NetServer パスワードを必要とする場合には、ユーザー・プロファイルを変更するか、またはパスワードをクリア・テキストで表す方式でサインオンして、作成することができます。

これで、管理者は、QPWDLVL を 0 に変更することができます。

割り当て済みパスワードの変更

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

__ ステップ 1. いまだに (ユーザー・プロファイル名と同じ) デフォルト・パスワードを使用しているユーザー・プロファイルがないことを確認する。デフォルト・パスワード分析 (ANZDFTPWD) コマンドを使用することができます。 (28 ページの『デフォルト・パスワードの回避』を参照してください。)

__ ステップ 2. 表 2 に示してあるユーザー・プロファイルとパスワードの組み合わせを使用して、システムへのサインオンを試行する。これらのパスワードは公表されているもので、システムに侵入しようとする誰もが最初に選択するものです。サインオンすることができたら、ユーザー・プロファイル変更 (CHGUSRPRF) コマンドを使用して、パスワードを推奨値に変更します。

__ ステップ 3. 専用保守ツール (DST) を開始し、 23 ページの表 3 に示してあるパスワードを使用してサインオンを試行する。「iSeries Information Center」—>「セキュリティー」—>「保守ツール」を参照してください。 iSeries Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。

__ ステップ 4. これらのパスワードを使用して DST にサインオンできた場合は、パスワードを変更する必要がある。保守ツールのユーザー ID およびパスワードの変更方法の詳細については、「iSeries Information Center」—>「セキュリティー」—>「保守ツール」を参照してください。 iSeries Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。

__ ステップ 5. 最後に、ユーザー ID とパスワードを入力しないと、「サインオン」画面で実行キーを押しただけではサインオンできないことを確認する。各種ディスプレイで試行してみます。「サインオン」画面で情報を入力しなくてもサインオンできる場合には、以下のいずれかを行います。

- セキュリティー・レベルを 40 または 50 (QSECURITY システム値) に変更する。

  注: セキュリティー・レベルを 40 または 50 に上げると、アプリケーションの実行動作が変化する場合があります。

- 対話式サブシステムに対するすべてのワークステーション項目が USER(*RQD) を指定したジョブ記述を示すように変更する。

表 2. IBM 提供プロファイル用のパスワード

ユーザー ID	パスワード	推奨値
QSECOFR	QSECOFR[1]	機密保護管理者だけが知っている単純ではない値。**選択したパスワードを書き留め、安全な場所に保管します。**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2、3]

表 2. IBM 提供プロファイル用のパスワード (続き)

ユーザー ID	パスワード	推奨値
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

注:

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

   CFGSYSSEC コマンドを実行すると、システムはこれらのパスワードを *NONE に設定します。
3. TCP/IP を使用して iSeries Access for Windows を実行するには、QUSER ユーザー・プロファイルを使用可能にしておかなければなりません。

表 3. 専用保守ツール用のパスワード

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

注:

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

注: DST パスワードは、認証された装置によってのみ変更することができます。このことは、すべてのパスワードおよび対応する同一のユーザー ID にもあてはまります。認証された装置の詳細については、iSeries Information Center の『オペレーション・コンソール』のセットアップ情報を参照してください。

サインオン値の設定

24 ページの表 4 は、許可を受けていない者がユーザー・システムにサインオンするのをより難しくするために設定する各種の値です。CFGSYSSEC コマンドを実行すると、これらのシステム値は推奨設定に設定されます。「*iSeries 機密保護解説書*」の第 3 章では、これらのシステム値について詳しい情報を得ることができます。

表 4. サインオンのシステム値

システム値の名前	説明	推奨設定
QAUTOCFG	システムが新規装置を自動的に構成するかどうか。	0 (いいえ)
QAUTOVRT	使用できる装置がない場合にシステムが自動的に作成する仮想装置記述の数	0
QDEVRCYACN	エラーの後で装置を再接続するときにシステムが行うこと。[1]	*DSCMSG
QDSCJOBITV	システムが、切断ジョブを終了する前に待機する時間。	120
QDSPSGNINF	ユーザーがサインオンしたときに、システムが前のサインオン活動についての情報を表示するかどうか。	1 (はい)
QINACTITV	対話式ジョブが非活動のときに、システムが処置を起こすまでに待機する時間。	60
QINACTMSGQ	QINACTITV 時間枠に達したときにシステムが行うこと。	*ENDJOB
QLMTDEVSSN	ユーザーが複数のワークステーションから同時にサインオンすることをシステムが妨げるかどうか。	1 (はい)
QLMTSECOFR	*ALLOBJ または *SERVICE 特殊権限を持つユーザーは、特定のワークステーションでしかサインオンできないかどうか。	1 (はい)[2]
QMAXSIGN	間違ったサインオンの試行 (ユーザー・プロファイルかパスワードが間違っている) を連続して行う最大数。	3
QMAXSGNACN	QMAXSIGN 限界に達したときにシステムが行うこと。	3 (ユーザー・プロファイルと装置の両方を使用不可にする)

注:

1. TELNET セッションの装置記述が明示的に割り当てられている場合、システムは、TELNET セッションの切断および再接続を行うことができます。
2. システム値を 1 (はい) に設定した場合、*ALLOBJ または *SERVICE 特殊権限を持つユーザーを装置に対して明示的に許可する必要があります。これを最も単純に行う方法は、特定の装置に対する *CHANGE 権限を QSECOFR ユーザー・プロファイルに与えることです。

サインオンのエラー・メッセージの変更

ハッカーは、システムへの侵入の進行具合を知りたがっています。「サインオン」画面のエラー・メッセージがパスワードが正しくないであると、ハッカーは、ユーザー ID の方は正しいと想定することができます。メッセージ記述変更 (CHGMSGD) コマンドを使用して 2 つのサインオン・エラー・メッセージのテキストを変更すると、ハッカーをいらだたせることができます。 25 ページの表 5 に推奨テキストを示します。

表 5. サインオンのエラー・メッセージ

メッセージ ID	出荷時のテキスト	推奨テキスト
CPF1107	CPF1107 - ユーザー・プロファイルのパスワードが正しくない。	サインオン情報が正しくありません。 **注:** メッセージ・テキストにメッセージ ID を組み込まないでください。
CPF1120	CPF1120 - ユーザー XXXXX が存在していない。	サインオン情報が正しくありません。 **注:** メッセージ・テキストにメッセージ ID を組み込まないでください。

ユーザー・プロファイルの使用可能化のスケジュール

一部のユーザー・プロファイルを、一日のうちの一定の時間、または週の中の一定の曜日にのみサインオンで使用できるようにすることができます。たとえば、セキュリティー監査担当者用にセットアップしたプロファイルがある場合、その監査担当者の作業がスケジュールされている時間帯のみ、そのユーザー・プロファイルを使用できるようにすることができます。オフの時間帯の間は、*ALLOBJ 特殊権限を持つユーザー・プロファイル (QSECOFR ユーザー・プロファイルを含む) を使用不可にすることもできます。

活動化スケジュール項目変更 (CHGACTSCDE) コマンドを使用すると、ユーザー・プロファイルを自動的に使用可/不可にするようにセットアップすることができます。スケジュールしたいユーザー・プロファイルごとに、ユーザー・プロファイルのスケジュールを定義する項目を作成します。

たとえば、朝 7 時から夜 10 時の間でのみ QSECOFR プロファイルを使用できるようにしたい場合、CHGACTSCDE 画面で以下のとおり入力します。

```
                    活動化スケジュール項目の変更  (CHGACTSCDE)

選択項目を入力して，実行キーを押してください。

ユーザー・プロファイル . . . > QSECOFR     名前
時刻の活動化 . . . . . . . . > '7:00'      時刻, *NONE
時刻の非活動化 . . . . . . . > '22:00'     時刻, *NONE
日数 . . . . . . . . . . . . > *MON        *ALL, *MON, *TUE, *WED...
                             > *TUE
                             > *WED
                             > *THU
                  値の続きは＋ > *FRI
```

図 2. プロファイル活動化スケジュール画面の例

実際、毎日の非常に限定された時間でしか QSECOFR プロファイルを使用できないようにすることができます。ほとんどのシステム機能を実行するために、*SECOFR クラスの別のユーザー・プロファイルを使用することができます。こうして、事前割り当てのユーザー・プロファイルが攻撃されることを防ぎます。

監査ジャーナル項目表示 (DSPAUDJRNE) コマンドを定期的に使用すると、CP (プロファイル変更) 監査ジャーナル項目を印刷することができます。これらの項目を

使用して、システムが、計画されたスケジュールに応じてユーザー・プロファイルを使用可 / 不可にしているかどうか検証します。

計画されたスケジュールに応じて、ユーザー・プロファイルが確実に使用不可にされていることをチェックする別の方法に、ユーザー・プロファイル印刷 (PRTUSRPRF) コマンドの使用があります。報告書タイプに *PWDINFO を指定すると、その報告書には、選択したユーザー・プロファイルそれぞれの状況が記載されます。たとえば、*ALLOBJ 特殊権限を持つすべてのユーザー・プロファイルを定期的に使用不可にしている場合、プロファイルが使用不可にされた直後に以下のコマンドを実行するようにスケジュールすることができます。

```
PRTUSRPRF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)
```

非活動ユーザー・プロファイルの除去

ユーザーのシステムには、必要なユーザー・プロファイルだけを置くようにしてください。ユーザーがいなくなった、またはユーザーが組織内部の別の仕事の担当になったため、ユーザー・プロファイルがこれ以降必要なくなった場合、ユーザー・プロファイルを除去します。長期にわたって組織を離れるユーザーがいる場合、そのユーザーのプロファイルを使用不可 (非活動化) にします。不要なユーザー・プロファイルは、ユーザーのシステムに無許可の入り口を提供するおそれがあります。

ユーザー・プロファイルの自動的な使用不可化

プロファイル活動分析 (ANZPRFACT) コマンドを使用すると、指定された日数の間使用されなかったユーザー・プロファイルを定期的に使用不可にします。ANZPRFACT コマンドの使用時に、システムが探す非活動の日数を指定します。システムは、最終使用日付、復元日付、およびユーザー・プロファイルの作成日を調べます。

いったん ANZPRFACT コマンドの値を指定すると、システムは、ジョブが週に一度、午前 1 時に実行されるようにスケジュールします (初めて値を指定した翌日から開始)。ジョブはすべてのプロファイルを調べて、非活動プロファイルを使用不可にします。非活動の日数を変更する必要がなければ再び ANZPRFACT コマンドを使用する必要はありません。

活動プロファイル・リスト変更 (CHGACTPRFL) コマンドを使用すると、一部のプロファイルを ANZPRFACT 処理から外すことができます。 CHGACTPRFL コマンドは、プロファイルがどんなに長い間非活動状態であっても、ANZPRFACT コマンドで使用不可にされないユーザー・プロファイルのリストを作成します。

システムが ANZPRFACT コマンドを実行すると、コマンドは、使用不可のユーザー・プロファイルごとに、監査ジャーナルに CP 項目を書き出します。DSPAUDJRNE コマンドを使用すると、新しく使用不可になったユーザー・プロファイルをリストすることができます。

注: システムが監査項目を書き出すのは、QAUDCTL 値が *AUDLVL を指定し、さらに QAUDLVL システム値が *SECURITY を指定している場合だけです。

計画されたスケジュールに応じて、ユーザー・プロファイルが確実に使用不可にされていることをチェックする別の方法に、ユーザー・プロファイル印刷

(PRTUSRPRF) コマンドの使用があります。報告書タイプに *PWDINFO を指定すると、その報告書には、選択したユーザー・プロファイルそれぞれの状況が記載されます。

ユーザー・プロファイルの自動的な除去

満了スケジュール項目変更 (CHGEXPSCDE) コマンドを使用すると、ユーザー・プロファイルの除去または使用不可を管理することができます。あるユーザーが長期間離れることが分かっている場合、そのユーザー・プロファイルの除去または使用不可をスケジュールすることができます。

初めて CHGEXPSCDE コマンドを使用するときに、このコマンドは、毎日深夜 0 時 1 分に実行するジョブ・スケジュール項目を作成します。このジョブは QASECEXP ファイルを参照して、その日に除去するようにスケジュールされているユーザー・プロファイルを判別します。

CHGEXPSCDE コマンドを使用して、ユーザー・プロファイルを使用不可にするか、あるいは削除します。ユーザー・プロファイルの削除を選択した場合、システムが、ユーザーの所有するオブジェクトで行う作業を指定しなければなりません。ユーザー・プロファイルの削除をスケジュールする前に、ユーザーの所有するオブジェクトを調査しておく必要があります。たとえば、ユーザーが権限を借用するプログラムを所有している場合、これらのプログラムに新規所有者の所有権を借用させたいかどうか。あるいは、新規所有者が必要以上の権限 (特殊権限など) を持つかどうかということなどです。おそらく、権限を借用する必要のあるプログラムを所有するための特定権限を持つ新規ユーザー・プロファイルを作成することが必要です。

ユーザー・プロファイルを削除した場合に、アプリケーションの問題が生じるかどうかを調べておく必要もあります。たとえば、ジョブ記述がデフォルト・ユーザーとしてユーザー・プロファイルを指定するかなどです。

満了スケジュール表示 (DSPEXPSCD) コマンドを使用すると、使用不可または除去がスケジュールされているプロファイルのリストを表示することができます。

認可ユーザー表示 (DSPAUTUSR) コマンドを使用すると、ユーザー・システム上のすべてのユーザー・プロファイルをリストすることができます。ユーザー・プロファイル削除 (DLTUSRPRF) コマンドを使用して、古くなったプロファイルを削除します。

セキュリティーに関する注意事項: ユーザー・プロファイルの状況を *DISABLED に設定して、ユーザー・プロファイルを使用不可にします。ユーザー・プロファイルを使用不可にすると、そのユーザー・プロファイルは対話式使用では使用できなくなります。使用不可のユーザー・プロファイルを使用してサインオンすることも、使用不可のユーザー・プロファイルに対するジョブを変更することもできません。バッチ・ジョブは、使用不可のユーザー・プロファイル下で実行することができます。

デフォルト・パスワードの回避

新規ユーザー・プロファイルを作成すると、デフォルトでは、ユーザー・プロファイル名と同一のパスワードが作成されます。これにより、プロファイル名の割り当てのポリシーを知っている人物がユーザーの組織に新しい担当者が加わったことを知ると、その人物は、ユーザーのシステムに入り込む機会を得ることになります。

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

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

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

サインオン活動とパスワード活動のモニター

システムに入ろうとする未許可の試行について懸念する場合、サインオンおよびパスワード活動のモニターに役立つ PRTUSRPRF コマンドを使用することができます。

この報告書の使用にあたって、いくつかの提案を以下に示します。

- 一部のユーザー・プロファイルのパスワード満了間隔がシステム値よりも長いかどうか、および、長い満了間隔が正当かどうかを判別する。たとえば、この報告書では、USERY のパスワード満了間隔は 120 日です。
- 正常終了しなかったサインオンの試行をモニターするために、この報告書を定期的に実行する。システムに侵入しようしている人は、正常終了しなかった試行が一定回数に達すると、システムが処置を行うことに知っている可能性があります。毎晩、侵入者になるつもりの人は、試行に対して警告を出されないようにするため、使用中の QMAXSIGN 値よりも少ない回数で試そうとする可能性があり

ます。しかし、この報告書を毎朝早くに実行し、一部のプロファイルのサインオン試行が頻繁に正常終了していないことに気付いた場合、問題が生じているのではないかと疑うことができます。

- 長期間使用されていないユーザー・プロファイルや、パスワードが長期間変更されていないユーザー・プロファイルを識別する。

パスワード情報の保管

一部のネットワーク機能と通信要件をサポートするため、iSeries サーバーは、暗号化を解除される可能性のあるパスワードを保管するためのセキュアな方法を提供します。たとえば、別のシステムとの SLIP 接続を確立するのに、システムはこれらのパスワードを使用します。(141 ページの『セキュリティーとダイヤルアウト・セッション』では、この保管パスワードの使用について説明します。)

iSeries サーバーは、どんなユーザー・プログラムやインターフェースからもアクセスすることのできないセキュアな場所にこれらの特別なパスワードを保管します。明示的に許可されたシステム機能だけが、これらのパスワードの設定と取り出しを行うことができます。

たとえば、ダイヤルアウトの SLIP 接続用に保管パスワードを使用するときには、構成プロファイルを作成するシステム・コマンド (WRKTCPPTP) を使用してパスワードを設定します。このコマンドを使用するには、*IOSYSCFG が必要です。特別にコーディングされた接続スクリプトが、ダイヤルアウト手順の際に、パスワードを取り出してそのパスワードの暗号化を解除します。ユーザーは、暗号化解除されたパスワードを見たり、ジョブ・ログにそのパスワードを表示することはできません。

機密保護管理者は、暗号化を解除することができるパスワードをシステムに保管できるようにするかどうかを決める必要があります。これを指定するには、サーバー・セキュリティー・データの保持 (QRETSVRSEC) システム値を使用します。デフォルトは 0 (なし) です。このため、ユーザーが明示的にこのシステム値を設定しない限り、システムは暗号化を解除することができるパスワードを保管しません。

保管パスワードについてネットワークまたは通信要件がある場合、適切なポリシーを設定し、通信相手のポリシーと実施を理解するようにしてください。たとえば、別の iSeries サーバーとの通信に SLIP を使用するときには、両方のシステムで、セッションを確立するための特別なユーザー・プロファイルのセットアップを考えてください。特別なプロファイルには、システムにおける限定権限を持たせるようにしてください。これにより、保管パスワードがパートナー・システムで危険にさらされた場合に、ご使用のシステムへの影響が制限されます。

第 4 章 セキュリティー・ツールを使用するための iSeries の構成

この章では、OS/400 の一部であるセキュリティー・ツールを使用するためのシステムのセットアップ方法について説明します。 OS/400 を導入すると、セキュリティー・ツールが使用できるようになります。以下の各項で、セキュリティー・ツールを使用する操作手順に関する推奨事項を示します。

セキュリティー・ツールのセキュアな操作

OS/400 を導入すると、セキュリティー・ツールに関連するオブジェクトが保護されます。セキュリティー・ツールをセキュアに操作するには、どのセキュリティー・ツール・オブジェクトにも権限の変更を加えないことです。

次に、セキュリティー・ツール・オブジェクトのためのセキュリティー設定と要件について説明します。

- セキュリティー・ツールのプログラムとコマンドは QSYS プロダクト・ライブラリーに入っています。これらのコマンドとプログラムは、*EXCLUDE の共通権限で出荷されます。セキュリティー・ツール・コマンドの多くは、ファイルを QUSRSYS ライブラリーに作成します。システムがこれらのファイルを作成すると、これらのファイルの共通権限は *EXCLUDE になります。

  変更報告書を生成するための情報が含まれているファイルには、QSEC で始まる名前が付けられています。ユーザー・プロファイルを管理するための情報が含まれているファイルには、QASEC で始まる名前が付けられています。これらのファイルには、システムに関する機密情報が含まれています。したがって、これらのファイルに対する共通権限を変更してはなりません。
- セキュリティー・ツールは、印刷出力の送信に通常システム・セットアップを使用します。これらの報告書には、システムに関する機密情報が含まれています。出力を保護出力待ち行列に送信するには、セキュリティー・ツールを実行するユーザーのユーザー・プロファイルまたはジョブ記述に対して該当する変更を行います。
- これらはセキュリティー機能を持っているため、またシステム上の多くのオブジェクトにアクセスするため、セキュリティー・ツールコマンドには *ALLOBJ 特殊権限が必要です。一部のコマンドには、*SECADM、*AUDIT、または *IOSYSCFG 特殊権限も必要です。これらのコマンドを正常に実行するには、セキュリティー・ツールを使用するときに機密保護担当者としてサインオンする必要があります。したがって、どのセキュリティー・ツール・コマンドに対しても私用権限を与える必要はありません。

ファイル矛盾の回避

セキュリティー・ツール報告書コマンドの多くは、変更バージョンの報告書の印刷に使用できるデータベース・ファイルを作成します。32 ページの『セキュリティー・コマンドのコマンドおよびメニュー』では、各コマンドごとのファイル名について説明しています。1 つのジョブからは一度に 1 つのコマンドしか実行できません。コマンドのほとんどには、これを強制する検査があります。別のジョブがコマンドを完了していない場合に、そのコマンドを実行すると、エラー・メッセージが表示されます。

多くの印刷ジョブは、長時間実行ジョブです。報告書をバッチ処理に投入したり、報告書をジョブ・スケジューラーに追加する場合は、注意してファイル矛盾を回避する必要があります。たとえば、異なる選択基準を持つ 2 つのバージョンの PRTUSRPRF 報告書を印刷したい場合があります。報告書をバッチ処理に投入する場合は、一時点で 1 つのジョブしか実行しないジョブ待ち行列を使用して、報告書ジョブが順次に実行されるようにします。

ジョブ・スケジューラーを使用する場合は、2 つのジョブの間に十分な時間間隔をあけ、最初のバージョンが完了してから 2 番目のジョブを実行するようにスケジュールします。

セキュリティー・ツールの保管

システム保管 (SAVSYS) コマンドを実行するたびに、または SAVSYS コマンドを実行する「保管」メニューのオプションを実行するたびに、セキュリティー・ツール・プログラムを保管します。

セキュリティー・ツール・ファイルは QUSRSYS ライブラリーに入っています。このライブラリーは、すでに通常操作手順の一環として保管されているはずです。QUSRSYS ライブラリーには、システムで使用する多くのライセンス・プログラム用のデータが含まれています。QUSRSYS ライブラリーを保管するコマンドとオプションの詳細については、Information Center を参照してください。

セキュリティー・コマンドのコマンドおよびメニュー

このセクションでは、セキュリティー・ツールのためのコマンドとメニューについて解説します。ここでは、これらのコマンドの使用例を随所に示します。

セキュリティー・ツールでは、次の 2 つのメニューを使用することができます。

- SECTOOLS (セキュリティー・ツール) メニュー。これは、コマンドを対話式に実行するためのメニューです。
- SECBATCH (セキュリティー報告書のバッチ処理投入またはスケジュール) メニュー。これは、報告書コマンドをバッチで実行するためのメニューです。SECBATCH メニューは 2 つの部分に分かれています。メニューの最初の部分は、ジョブ投入 (SBMJOB) コマンドを使用して、バッチ即時処理用の報告書を投入します。

  メニューの 2 番目の部分は、ジョブ・スケジュール項目追加 (ADDJOBSCDE) コマンドを使用します。このコマンドを使用して、セキュリティー報告書が指定日時に定期的に実行されるようにスケジュールします。

セキュリティー・ツールのメニュー・オプション

表 6 は、これらのメニュー・オプションと関連コマンドについて説明しています。

表 6. ユーザー・プロファイルのツール・コマンド

メニュー [1] オプション	コマンド名	説明	使用するデータベース・ファイル
1	ANZDFTPWD	デフォルト・パスワード分析コマンドを使用して、パスワードと同じ名前を持つユーザー・プロファイルに関する報告と処置を行います。	QASECPWD [2]
2	DSPACTPRFL	活動プロファイル・リスト表示コマンドを使用して、ANZPRFACT 処理から除外されているユーザー・プロファイルのリストを表示または印刷します。	QASECIDL [2]
3	CHGACTPRFL	活動プロファイル・リスト変更コマンドを使用して、ANZPRFACT コマンドの除外リストにプロファイルを追加したり除去したりします。活動プロファイル・リストに含まれているユーザー・プロファイルは、永続的に活動状態になっています (このプロファイルをリストから除去するまで)。活動プロファイル・リストに含まれているプロファイルが、どれだけの期間非活動状態になっていても、ANZPRFACT コマンドはこのプロファイルを使用不可にすることはありません。	QASECIDL [2]
4	ANZPRFACT	プロファイル活動分析コマンドを使用して、指定された日数使用されなかったユーザー・プロファイルを使用不可にします。 ANZPRFACT コマンドを使用して日数を指定すると、システムは夜中に ANZPRFACT ジョブを実行します。 CHGACTPRFL コマンドを使用して、ユーザー・プロファイルが使用不可にならないようにすることができます。	QASECIDL [2]
5	DSPACTSCD	プロファイル活動化スケジュール表示コマンドを使用して、特定のユーザー・プロファイルを使用可能や使用不可にするスケジュールに関する情報を表示または印刷します。CHGACTSCDE コマンドを使用してスケジュールを作成します。	QASECACT [2]
6	CHGACTSCDE	活動化スケジュール項目変更コマンドを使用して、1 日または 1 週のうちの特定の時間しかユーザー・プロファイルがサインオンできないようにします。スケジュールする各ユーザー・プロファイルごとに、システムは、使用可能時間や使用不可時間のためのジョブ・スケジュール項目を作成します。	QASECACT [2]

表 6. ユーザー・プロファイルのツール・コマンド (続き)

メニュー [1] オプション	コマンド名	説明	使用するデータベース・ファイル
7	DSPEXPSCD	満了スケジュール表示コマンドを使用して、今後使用不可にされるか、またはシステムから除去されるようにスケジュールされたユーザー・プロファイルのリストを表示または印刷します。CHGEXPSCDE を使用して、ユーザー・プロファイルの満了をセットアップします。	QASECEXP [2]
8	CHGEXPSCDE	満了スケジュール項目変更コマンドを使用して、ユーザー・プロファイルの除去をスケジュールします。ユーザー・プロファイルを一時的に除去 (それを使用不可にして) したり、システムから削除することができます。このコマンドは、毎日 00:01 (深夜 0 時の 1 分後) に実行するジョブ・スケジュール項目を使用します。このジョブは、QASECEXP ファイルを調べて、ユーザー・プロファイルがその日に満了になるようにセットアップされているかどうかを判別します。 DSPEXPSCD コマンドを使用して、満了がスケジュールされているユーザー・プロファイルを表示します。	QASECEXP [2]
9	PRTPRFINT	プロファイル内部印刷コマンドを使用して、ユーザー・プロファイルの項目数に関する情報が含まれている報告書を印刷します。項目数は、ユーザー・プロファイルのサイズを決定します。	

注:

1. オプションは、SECTOOLS メニューから選択されます。
2. このファイルは、QUSRSYS ライブラリーに入っています。

メニュー上でページ送りを行うと、その他のオプションを見ることができます。35 ページの表 7 は、セキュリティー監査のメニュー・オプションと関連コマンドについて説明したものです。

表 7. セキュリティー監査のツール・コマンド

メニュー [1] オプション	コマンド名	説明	使用するデータベース・ファイル
10	CHGSECAUD	セキュリティー監査変更コマンドを使用して、セキュリティー監査をセットアップしたり、セキュリティー監査を制御するシステム値を変更します。CHGSECAUD コマンドの実行時に、システムは、セキュリティー監査 (QAUDJRN) ジャーナルが存在しない場合に、これを作成します。 CHGSECAUD コマンドには、QAUDLVL (監査レベル) システム値の設定を簡単にするオプションが用意されています。*ALL を指定すると、指定可能なすべての監査レベル設定値を活動化することができます。あるいは、*DFTSET を指定すれば、最も一般的に使用されている設定 (*AUTFAIL、*CREATE、*DELETE、*SECURITY、および *SAVRST) を活動化することができます。 **注:** このセキュリティー・ツールを使用して監査をセットアップする場合は、監査ジャーナル・レシーバーの管理について計画してください。そうしないと、すぐにディスク使用率の問題が生じるおそれがあります。	
11	DSPSECAUD	セキュリティー監査表示コマンドを使用して、セキュリティー監査ジャーナル、およびセキュリティー監査を制御するシステム値に関する情報を表示します。	

注:

1. オプションは、SECTOOLS メニューから選択されます。

セキュリティー・バッチ・メニューの使用

SECBATCH メニューの最初の部分は、次のとおりです。

```
SECBATCH     バッチへの機密保護報告書の投入またはスケジューリング
                                                          システム:
次の 1 つを選択してください:

  バッチへの報告書の投入
     1. 借用する側のオブジェクト
     2. ジャーナル項目の監査
     3. 認可リスト権限
     4. コマンド権限
     5. コマンド私用権限
     6. 通信保護機能
     7. ディレクトリー権限
     8. ディレクトリー私用権限
     9. 文書権限
    10. 文書私用権限
    11. ファイル権限
    12. ファイル私用権限
    13. フォルダー権限
```

このメニューからオプションを選択すると、「ジョブ投入 (SBMJOB)」画面が表示されます。このコマンドのデフォルト・オプションを変更したい場合は、*実行するコマンド* 行で F4 (プロンプト) を押します。

バッチ・スケジュール報告書を表示するには、SECBATCH メニューをページ送りします。たとえば、メニューのこの部分にあるオプションを使用することで、変更バージョンの報告書を定期的に実行するようにシステムをセットアップすることができます。ページ送りを行うと、その他のメニュー・オプションを表示することができます。メニューのこの部分にあるオプションを選択すると、「ジョブ・スケジュール項目追加 (ADDJOBSCDE)」画面を表示することができます。

実行するコマンド 行にカーソルを置いて F4 (プロンプト) を押すと、報告書の別の設定を選択することができます。分かりやすいジョブ名を割り当てて、ジョブ・スケジュール項目を表示したときにその項目を認識できるようにしておく必要があります。

セキュリティー・バッチ・メニューのオプション

37 ページの表 8 は、セキュリティー報告書のメニュー・オプションと関連コマンドについて説明したものです。

セキュリティー報告書を実行すると、システムは、ユーザーが指定した選択基準とツールの選択基準の両方を満たす情報のみを印刷します。たとえば、ユーザー・プロファイル名を指定するジョブ記述は、セキュリティーに関連するものです。したがって、ジョブ記述 (PRTJOBDAUT) 報告書が指定ライブラリーのジョブ記述を印刷するのは、このジョブ記述の共通権限が *EXCLUDE でなく、かつ このジョブ記述が USER パラメーターにユーザー・プロファイル名を指定している場合だけです。

同様に、サブシステム情報を印刷する (PRTSBSDAUT コマンド) と、システムは、ユーザー・プロファイルを指定する通信項目がサブシステム記述に含まれているときにのみ、サブシステムに関する情報を印刷します。

特定の報告書が印刷する情報が予想していたものより少ない場合は、オンライン・ヘルプ情報を参照して、その報告書のための選択基準を見つけてください。

表 8. セキュリティー報告書のコマンド

メニュー [1] オプション	コマンド名	説明	使用するデータベース・ファイル
1, 40	PRTADPOBJ	借用オブジェクト印刷コマンドを使用して、指定されたユーザー・プロファイルの権限を借用するオブジェクトのリストを印刷します。指定できるのは、単一プロファイル、総称プロファイル (たとえば、Q で始まるすべてのプロファイルなど)、またはシステム上のすべてのユーザー・プロファイルです。 この報告書には 2 つのバージョンがあります。完全報告書には、選択基準を満たすすべての借用オブジェクトがリストされます。変更報告書には、現在システム上にある借用オブジェクトと、最後に報告書を実行したときにシステムにあった借用オブジェクトとの違いがリストされます。	QSECADPOLD[2]
2, 41	DSPAUDJRNE	監査ジャーナル項目表示コマンドを使用して、セキュリティー監査ジャーナル項目に関する情報を表示または印刷します。特定の項目タイプ、特定のユーザー、および時間枠を選択することができます。	QASYxxJ4[3]
3, 42	PRTPVTAUT *AUTL	*AUTL オブジェクトに私用権限オブジェクトの印刷コマンドを使用すると、システム上のすべての権限リストが表示されます。この報告書には、各リストに対して許可されているユーザーと、これらのユーザーがこのリストに対して持っている権限が含まれています。この情報を使用すれば、システム上のオブジェクト権限のソースを分析するのに役立ちます。 この報告書には、3 つのバージョンがあります。完全報告書には、システム上のすべての権限がリストされます。変更報告書には、最後にこの報告書を実行した後に権限に対して行われた追加や変更がリストされます。削除報告書には、最後にこの報告書を実行した後に権限リストに対する権限が削除されたユーザーがリストされます。 完全報告書を印刷する際には、各権限リストが保護するオブジェクトのリストを印刷するためのオプションがあります。システムは、権限リストごとに別々の報告書を作成します。	QSECATLOLD[2]

表 8. セキュリティー報告書のコマンド (続き)

メニュー [1] オプション	コマンド名	説明	使用するデータベース・ファイル
6, 45	PRTCMNSEC	通信セキュリティー印刷コマンドを使用して、システムでの通信に影響を与えるオブジェクトのセキュリティー関連設定を印刷します。これらの設定は、ユーザーやジョブがシステムに入る方法に影響を与えます。 このコマンドは 2 つの報告書を作成します。すなわち、システム上の構成リストの設定を表示する報告書と、回線記述、制御装置、および装置記述のセキュリティー関連パラメーターをリストする報告書です。これらの報告書にはそれぞれ、完全バージョンと変更バージョンがあります。	QSECCMNOLD [2]
15, 54	PRTJOBDAUT	ジョブ記述権限印刷コマンドを使用して、ジョブ記述 (ユーザー・プロファイルが指定され、共通権限が *EXCLUDE でない) のリストを印刷します。この報告書は、ジョブ記述に指定されたユーザー・プロファイルの特殊権限を示しています。 この報告書には 2 つのバージョンがあります。完全報告書には、選択基準を満たすすべてのジョブ記述オブジェクトがリストされます。変更報告書には、現在システム上にあるジョブ記述オブジェクトと、最後にこの報告書を実行したときにシステムにあったジョブ記述オブジェクトとの違いがリストされます。	QSECJBDOLD [2]
注 4 参照	PRTPUBAUT	共通権限オブジェクトの印刷コマンドを使用して、共通権限が *EXCLUDE でないオブジェクトのリストを印刷します。このコマンドを実行するときは、オブジェクトのタイプおよびこの報告書のライブラリー (複数の場合もある) を指定します。PRTPUBAUT コマンドを使用して、システム上のすべてのユーザーがアクセスできるオブジェクトに関する情報を印刷します。 この報告書には 2 つのバージョンがあります。完全報告書には、選択基準を満たすすべてのオブジェクトがリストされます。変更報告書には、現在システム上にある指定オブジェクトと、最後に報告書を実行したときにシステム上にあったオブジェクト (同一ライブラリーの同一タイプのもの) との間の違いがリストされます。	QPBxxxxxx [5]

表 8. セキュリティー報告書のコマンド (続き)

メニュー [1] オプション	コマンド名	説明	使用するデータベース・ファイル
注 5 を参照。	PRTPVTAUT	私用権限の印刷コマンドを使用して、指定ライブラリーに含まれている指定タイプのオブジェクトに対する私用権限のリストを印刷します。この報告書を使用すれば、オブジェクトに対する権限のソースを判別するのに役立ちます。 この報告書には、3 つのバージョンがあります。完全報告書には、選択基準を満たすすべてのオブジェクトがリストされます。変更報告書には、現在システム上にある指定オブジェクトと、最後に報告書を実行したときにシステム上にあったオブジェクト (同一ライブラリーの同一タイプのもの) との間の違いがリストされます。 削除報告書には、最後にこの報告書を実行した後でオブジェクトに対する権限が削除されたユーザーがリストされます。	QPVxxxxxx[5]
24, 63	PRTQAUT	印刷待ち行列報告書を使用して、システム上の出力待ち行列およびジョブ待ち行列に関するセキュリティーの設定を印刷します。これらの設定により、誰が出力待ち行列またはジョブ待ち行列の項目を表示したり変更したりできるかが制御されます。 この報告書には 2 つのバージョンがあります。完全報告書には、選択基準を満たすすべての出力待ち行列とジョブ待ち行列オブジェクトがリストされます。変更報告書には、現在システム上にある出力待ち行列およびジョブ待ち行列オブジェクトと、最後に報告書を実行したときにシステム上にあった出力待ち行列およびジョブ待ち行列オブジェクトとの違いがリストされます。	QSECQOLD[2]
25, 64	PRTSBSDAUT	サブシステム記述印刷コマンドを使用して、システム上のサブシステム記述のセキュリティー関連通信項目を印刷します。これらの設定により、システムに作業を入れる方法とジョブの実行方法が制御されます。報告書がサブシステム記述を印刷するのは、ユーザー・プロファイル名を指定する通信項目がこのサブシステム記述にある場合だけです。 この報告書には 2 つのバージョンがあります。完全報告書には、選択基準を満たすすべてのサブシステム記述オブジェクトがリストされます。変更報告書には、現在システム上にあるサブシステム記述オブジェクトと、最後に報告書を実行したときにシステム上にあったサブシステム記述オブジェクトとの違いがリストされます。	QSECSBDOLD [2]

表 8. セキュリティー報告書のコマンド (続き)

メニュー [1] オプション	コマンド名	説明	使用するデータベース・ファイル
26, 65	PRTSYSSECA	システム機密保護属性印刷コマンドを使用して、セキュリティー関連のシステム値とネットワーク属性のリストを印刷します。この報告書には、現行値および推奨値が示されています。	
27, 66	PRTTRGPGM	トリガー・プログラム印刷コマンドを使用して、システム上のデータベース・ファイルに関連するトリガー・プログラムのリストを印刷します。 この報告書には 2 つのバージョンがあります。完全報告書には、割り当てられていて、しかも選択基準を満たすすべてのトリガー・プログラムがリストされます。変更報告書には、最後に報告書を実行した後で割り当てられたトリガー・プログラムがリストされます。	QSECTRGOLD [2]
28, 67	PRTUSROBJ	ユーザー・オブジェクト印刷コマンドを使用して、ライブラリーに入っているユーザー・オブジェクト (IBM 提供でないオブジェクト) のリストを印刷します。この報告書を使用すれば、ライブラリー・リストのシステム部分に入っているライブラリー (たとえば、QSYS) の中のユーザー・オブジェクトのリストを印刷することができます。 この報告書には 2 つのバージョンがあります。完全報告書には、選択基準を満たすすべてのユーザー・オブジェクトがリストされます。変更報告書には、現在システム上にあるユーザー・オブジェクトと、最後に報告書を実行したときにシステム上にあったユーザー・オブジェクトとの違いがリストされます。	QSECPUOLD [2]
29, 68	PRTUSRPRF	ユーザー・プロファイル印刷コマンドを使用して、指定された基準を満たすユーザー・プロファイルを分析します。ユーザー・プロファイルの選択は、特殊権限、ユーザー・クラス、または特殊権限とユーザー・クラスとの間のミス・マッチに基づいて行うことができます。権限情報、環境情報、パスワード情報、またはパスワード・レベル情報を印刷することができます。	
30, 69	PRTPRFINT	プロファイル内部印刷コマンドを使用して、項目数に関する内部情報の報告書を印刷します。	

表 8. セキュリティー報告書のコマンド (続き)

メニュー [1] オプション	コマンド名	説明	使用するデータベース・ファイル
31, 70	CHKOBJITG	オブジェクト保全性検査コマンドを使用して、操作可能オブジェクト (たとえば、プログラム) がコンパイラーを使用しないで変更されたかどうかを判別します。このコマンドは、ウィルス・プログラムをシステムに導入しようとしたり、無許可命令を実行するためにプログラムを変更しようとするのを検出するのに役立ちます。「*iSeries 機密保護解説書*」では、CHKOBJITG コマンドについて詳しく説明しています。	

注:

1. オプションは、SECBATCH メニューから選択されます。
2. このファイルは、QUSRSYS ライブラリーに入っています。
3. xx は、2 文字のジャーナル項目タイプです。たとえば、 AE ジャーナル項目のモデル出力ファイルは QSYS/QASYAEJ4 です。モデル出力ファイルは、「*iSeries 機密保護解説書*」の付録 F に説明があります。
4. SECBATCH メニューには、機密保護管理者が通常関心を持つオブジェクト・タイプに関するオプションが含まれています。たとえば、オプション 11 または 50 を使用して、*FILE オブジェクトに対して PRTPUBAUT コマンドを実行します。汎用オプション (180 および 57) を使用してオブジェクト・タイプを指定します。
5. SECBATCH メニューには、機密保護管理者が通常関心を持つオブジェクト・タイプに関するオプションが含まれています。たとえば、オプション 12 または 51 は、*FILE オブジェクトに対して PRTPVTAUT コマンドを実行します。汎用オプション (19 および 58) を使用してオブジェクト・タイプを指定します。
6. ファイル名の xxxxxx はオブジェクト・タイプです。たとえば、プログラム・オブジェクトのファイルは、共通権限の場合は QPBPGM と呼ばれ、私用権限の場合は QPVPGM と呼ばれます。これらのファイルは QUSRSYS ライブラリーに入っています。

   ファイルには、報告書が印刷された各ライブラリーごとにメンバーが含まれています。メンバー名は、ライブラリー名と同じです。

セキュリティー・カスタマイズのためのコマンド

42 ページの表 9 は、システム上でセキュリティーをカスタマイズするために使用できるコマンドを説明したものです。これらのコマンドは SECTOOLS メニューにあります。

表 9. システム・カスタマイズ用のコマンド

メニュー オプション [1]	コマンド名	説明	使用するデータベース・ファイル
60	CFGSYSSEC	システム・セキュリティー構成コマンドを使用して、セキュリティー関連のシステム値を推奨値に設定します。このコマンドは、システムのセキュリティー監査もセットアップします。『システム・セキュリティー構成コマンドによって設定される値』は、コマンドの実行内容を説明しています。 **注:** 使用状況に合わせてカスタマイズされたセキュリティー推奨設定値を取得するには、このコマンドではなく、iSeries セキュリティー・ウィザードまたは iSeries セキュリティー・プランナーを実行します。これらのツールの詳細は、11 ページの『第 2 章 iSeries セキュリティー・ウィザードおよび eServer セキュリティー・プランナー』を参照してください。	
61	RVKPUBAUT	共通権限取り消しコマンドを使用して、システム上のセキュリティーに敏感なコマンドに関する共通権限を *EXCLUDE に設定します。44 ページの『共通権限取り消しコマンドの機能』は、RVKPUBAUT コマンドが実行する処置をリストしたものです。	

注:

1. オプションは、SECTOOLS メニューから選択されます。

システム・セキュリティー構成コマンドによって設定される値

表 10 は、CFGSYSSEC コマンドを実行する際に設定されるシステム値をリストしたものです。CFGSYSSEC コマンドは、QSYS/QSECCFGS というプログラムを実行します。

表 10. CFGSYSSEC コマンドによって設定された値

システム値の名前	設定	システム値の説明
QALWOBJRST	*NONE	システム状態プログラムと権限借用プログラムを復元できるかどうか
QAUTOCFG	0 (いいえ)	新規装置の自動構成
QAUTOVRT	0	使用できる装置がない場合にシステムが自動的に作成する仮想装置記述の数
QDEVRCYACN	*DSCMSG (メッセージとの切断)	通信再確立時のシステム処置
QDSCJOBITV	120	システムが切断ジョブに対して処置を行うまでの時間枠
QDSPSGNINF	1 (はい)	ユーザーにサインオン情報画面を表示するかどうか
QINACTITV	60	システムが非活動対話式ジョブに対して処置を行うまでの時間枠
QINACTMSGQ	*ENDJOB	システムが非活動ジョブに対して行う処置
QLMTDEVSSN	1 (はい)	ユーザーを一時点に 1 つの装置でのサインオンに制限するかどうか
QLMTSECOFR	1 (はい)	*ALLOBJ ユーザーおよび *SERVICE ユーザーを特定の装置に限定するかどうか

表 10. CFGSYSSEC コマンドによって設定された値 (続き)

システム値の名前	設定	システム値の説明
QMAXSIGN	3	連続して何回までサインオンの失敗を認めるか
QMAXSGNACN	3 (両方)	QMAXSIGN 限界に達したときに、システムがワークステーションまたはユーザー・プロファイルのいずれを使用不可にするかどうか
QRMTSIGN	*FRCSIGNON	システムがリモート (パススルーまたは TELNET) サインオン試行をどのように処理するか
QRMTSVRATR	0 (オフ)	システムをリモートから分析できるようにする
QSECURITY [1]	50	実施されるセキュリティーのレベル
QVFYOBJRST	3 (復元時に署名を検査)	復元時にオブジェクトを検査
QPWDEXPITV	60	ユーザーがパスワードを変更しなければならない頻度
QPWDMINLEN	6	パスワードの最小文字数
QPWDMAXLEN	8	パスワードの最大文字数
QPWDPOSDIF	1 (はい)	新規パスワードのすべての位置の文字が、直前に使用していたパスワードの位置の文字と異なっている必要があるかどうか
QPWDLMTCHR	注 2 を参照	パスワードに使用できない文字
QPWDLMTAJC	1 (はい)	パスワードに隣接数字が禁止されるかどうか
QPWDLMTREP	2 (連続反復不可)	パスワードに反復文字が禁止されるかどうか
QPWDRQDDGT	1 (はい)	パスワードに少なくとも 1 つの数字が必要かどうか
QPWDRQDDIF	1 (32 個の固有パスワード)	同じパスワードを再度使用できるようになるまでに何個の固有パスワードが必要か
QPWDVLDPGM	*NONE	パスワードの妥当性検査を行うためにシステムが呼び出すユーザー出口プログラム

注:

1. 現在 QSECURITY 値を 40 以下で実行している場合は、より高いセキュリティー・レベルに変更する前に、「*iSeries 機密保護解説書*」の第 2 章に記載されている情報を必ず検討してください。
2. 制限付き文字は、QSYS/QCPFMSG メッセージ・ファイルのメッセージ ID CPXB302 に保管されます。出荷時には AEIOU@$# となっています。メッセージ記述変更 (CHGMSGD) コマンドを使用すれば、制限付き文字を変更することができます。パスワード・レベル 2 または 3 では、QPWDLMTCHR システム値は使用されません。

また、CFGSYSSEC コマンドは、以下の IBM 提供ユーザー・プロファイルのパスワードを *NONE に設定します。

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

最後に、CFGSYSSEC コマンドは、セキュリティー監査変更 (CHGSECAUD) コマンドを使用してセキュリティー監査をセットアップします。 CFGSYSSEC コマンドは処置とオブジェクト監査をオンにし、CHGSECAUD コマンドでの監査を行うためのデフォルトの処置のセットも指定します。

プログラムのカスタマイズ

これらの設定の一部がインストール・システムに適合しない場合は、このコマンドを処理する独自のバージョンのプログラムを作成することができます。この場合は、次のようにします。

__ ステップ 1. CL ソース検索 (RTVCLSRC) コマンドを使用して、CFGSYSSEC コマンドを使用するときに実行するプログラムのソースをコピーします。検索するプログラムは QSYS/QSECCFGS です。プログラムを検索したら、*別の名前* を指定してください。

__ ステップ 2. プログラムを編集して変更を行います。次にそれをコンパイルします。コンパイルするときは、IBM 提供の QSYS/QSECCFGS プログラムを置き換えないようにしてください。プログラムには別の名前が必要です。

__ ステップ 3. コマンド変更 (CHGCMD) コマンドを使用して、CFGSYSSEC コマンドのコマンド (PGM) パラメーターを処理するようにプログラムを変更します。 PGM 値をプログラムの名前に設定します。たとえば、MYSECCFG と呼ばれる、QGPL ライブラリー内のプログラムを作成する場合は、次のように入力します。

```
CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MYSECCFG)
```

注: QSYS/QSECCFGS プログラムを変更する場合、IBM は、プログラムの信頼性、保守容易性、性能、または機能性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。商品性、特定目的適合性に関する黙示の保証も一切ありません。

共通権限取り消しコマンドの機能

共通権限取り消し (RVKPUBAUT) コマンドを使用して、コマンドとプログラムのセットの共通権限を *EXCLUDE に設定することができます。 RVKPUBAUT コマンドは、QSYS/QSECRVKP というプログラムを実行します。出荷された時点で QSECRVKP は、 45 ページの表 11 にリストされているコマンドと、 45 ページの表 12 にリストされているアプリケーション・プログラミング・インターフェース (API) の共通権限を取り消します (共通権限を *EXCLUDE に設定することにより)。システムが到着すると、これらのコマンドと API の共通権限は、*USE に設定されます。

45 ページの表 11 にリストされているコマンドと、 45 ページの表 12 にリストされている API はすべて、攻撃の機会を与える可能性のある機能をシステムで実行します。機密保護管理者としては、これらのコマンドやプログラムをすべてのシステム・ユーザーに開放するのではなく、これらを実行できるユーザーを明示的に許可する必要があります。

RVKPUBAUT コマンドを実行する際に、これらのコマンドが含まれているライブラリーを指定します。デフォルトは QSYS ライブラリーです。システム上に複数の国別言語がある場合は、各 QSYSxxx ライブラリーごとにこのコマンドを実行する必要があります。

表 11. 共通権限が RVKPUBAUT コマンドによって設定されるコマンド

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

表 12 の API はすべて、QSYS ライブラリーに入っています。

表 12. 共通権限が RVKPUBAUT コマンドによって設定されるプログラム

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

RVKPUBAUT コマンドを実行すると、ルート・ディレクトリーの共通権限は *USE に設定されます (ただし、すでに *USE またはそれより低い権限に設定されている場合を除きます)。

プログラムのカスタマイズ

これらの設定の一部がインストール・システムに適合しない場合は、このコマンドを処理する独自のバージョンのプログラムを作成することができます。この場合は、次のようにします。

__ ステップ 1. CL ソース検索 (RTVCLSRC) コマンドを使用して、 RVKPUBAUT コマンドを使用するときに実行するプログラムのソースをコピーします。検索するプログラムは QSYS/QSECRVKP です。プログラムを検索したら、*別の名前* を指定してください。

__ ステップ 2. プログラムを編集して変更を行います。次にそれをコンパイルします。コンパイルするときは、IBM 提供の QSYS/QSECRVKP プログラムを置き換えない ようにしてください。プログラムには別の名前が必要です。

__ ステップ 3. コマンド変更 (CHGCMD) コマンドを使用して、RVKPUBAUT コマンドのコマンド (PGM) パラメーターを処理するようにプログラムを変更します。PGM 値をプログラムの名前に設定します。たとえば、MYRVKPGM と呼ばれる、QGPL ライブラリー内のプログラムを作成する場合は、次のように入力します。

```
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)
```

注: QSYS/QSECRVKP プログラムを変更する場合、IBM は、プログラムの信頼性、保守容易性、性能、または機能性があること

をほのめかしたり保証することはできません。商品性、特定目的適合性に関する黙示の保証も一切ありません。

第 2 部 拡張 iSeries セキュリティー

第 5 章 オブジェクト権限による情報資産の保護

機密保護管理者としての重要な仕事は、システムのユーザーに不満を感じさせないで、導入先の情報資産を保護することです。システムをブラウズしたり無許可の変更を行ったりする権限をユーザーに与えずに、ユーザーが自分のジョブを実行するために十分な権限を持つようにする必要があります。

セキュリティーのヒント

権限の制約が厳しすぎると、逆効果になる場合があります。権限制約が非常に厳しい場合、ユーザー同士が互いにパスワードを共用して対抗することがあります。

OS/400 オペレーティング・システムは、統合されたオブジェクト・セキュリティーを行います。ユーザーは、システムによって提供されるインターフェースを使用してオブジェクトにアクセスします。たとえば、データベース・ファイルをアクセスしたい場合は、データベース・ファイルをアクセスするコマンドやプログラムを使用する必要があります。メッセージ待ち行列やジョブ・ログをアクセスするコマンドは使用できません。

ユーザーがシステム・インターフェースを使用してオブジェクトをアクセスするたびに、システムは、そのインターフェースに必要なオブジェクトに対する権限をユーザーが持っているかどうかを調べます。オブジェクト権限は、システムの資産を保護するための強力かつ柔軟なツールです。機密保護管理者としての重要な仕事は、管理と保守が可能な効果的なオブジェクト・セキュリティー方式をセットアップすることです。

オブジェクト権限の適用

オブジェクトへのアクセスを試みた場合は常に、オペレーティング・システムが、そのオブジェクトに対するユーザー権限を検査します。ただし、システムのセキュリティー・レベル (QSECURITY システム値) を 10 または 20 に設定すると、すべてのユーザー・プロファイルが *ALLOBJ 特殊権限を持つようになるため、すべてのユーザーは自動的にすべてのオブジェクトをアクセスする権限を入手することになります。

オブジェクト権限に関するヒント: オブジェクト・セキュリティーを使用しているかどうか分からない場合は、QSECURITY (セキュリティー・レベル) システム値を調べてください。QSECURITY が 10 または 20 であれば、ユーザー・セキュリティーを使用していません。

セキュリティー・レベルを 30 以上に変更するためには、その前に計画と準備が必要になります。それを行わないと、ユーザーが必要な情報にアクセスできなくなる可能性があります。

Information Center の『**基本システム・セキュリティーおよび計画**』のトピックでは、アプリケーションを分析する方式や、オブジェクト・セキュリティーのセットアップ方法が説明されています。オブジェクト・セキュリティーをまだ使用していない場合、またはセキュリティー方式が古くなったり、複雑になり過ぎている場合は、このトピックを読んでから開始してください。

メニュー・セキュリティー

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

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

iSeries サーバーでは、メニュー・アクセス制御を支援するために、いくつかのユーザー・プロファイル・オプションが用意されています。以下のものを使用できます。

- **初期メニュー** (INLMNU) パラメーターを使用して、ユーザーがサインオンした後でどのメニューを最初に表示するかを制御することができます。
- **初期プログラム** (INLPGM) パラメーターを使用して、ユーザーがメニューを見る前にセットアップ・プログラムを実行することができます。 あるいは、INLPGM パラメーターを使用して、ユーザーが単一のプログラムを実行するように制限することができます。
- **機能限定** (LMTCPB) パラメーターを使用して、ユーザーが限定されたコマンド・セットしか使用しないように制限することができます。 LMTCPB パラメーターは、ユーザーがサインオン表示画面で別の初期プログラムやメニューを指定することも防止します。 (LMTCPB パラメーターは、コマンド行から入力されたコマンドのみを制限します。)

メニュー・アクセス制御の制限

コンピューターやコンピューター・ユーザーは、この数年間で大きく変わりました。 QUERY プログラムやスプレッドシートなどの多くのツールが使用可能になったため、ユーザーは、一部のプログラムについて自分でプログラミングして、IS 部門の作業負荷を減らすことができるようになりました。SQL や ODBC など、一部のツールには、情報を表示する機能および情報を変更する機能が備わっています。これらのツールをメニュー構造内で使用可能にするのは非常に困難です。

固定機能 (「グリーン画面」) ワークステーションは、急速にパーソナル・コンピューターとコンピューター間ネットワークに取って替わられています。システムがネットワークに参加していれば、ユーザーは、サインオン表示やメニューを見ないでシステムに入ることができます。

メニュー・アクセス制御を実施しようとする機密保護管理者には、次の 2 つの問題があります。

- ユーザーをメニューに限定できた場合、最新のツールを使用できる範囲が限定されるため、ユーザーはおそらくこの処置を歓迎しません。
- 限定できなかった場合、メニュー・アクセス制御で保護できると考えていた重要な機密情報が危険にさらされる可能性があります。システムがネットワークに参加していると、メニュー・アクセス制御を実施する能力が減少します。たとえば、LMTCPB パラメーターは、対話式セッションでコマンド行から入力されたコマンドにのみ適用されます。 LMTCPB パラメーターは、PC ファイル転送、FTP、リモート・コマンドなど、通信セッションからの要求には影響を与えません。

オブジェクト・セキュリティーによるメニュー・アクセス制御の拡張

システムとの接続に使用できる多くの新規オプションが存在するため、今後の実行可能な iSeries サーバーのセキュリティー方式ではメニュー・アクセス制御にのみ依存するわけにはいきません。この項では、メニュー・アクセス制御を補完するオブジェクト・セキュリティー環境を構築する上での推奨事項を示します。

Information Center の『*基本システム・セキュリティーおよび計画*』のトピックでは、ユーザーが現行アプリケーションを実行するために必要な、オブジェクトに対する権限を分析する技法について説明しています。その後で、ユーザーをグループに割り当て、そのグループに適切な権限を与えます。この方法は、道理に合っていて、しかも論理的です。しかし、システムが長年操作され、アプリケーションの数が増えていれば、アプリケーションの分析やオブジェクト権限のセットアップといった作業は大変なものになります。

オブジェクト権限に関するヒント: プログラム所有者の権限を借用するプログラムに現行メニューを組み合わせている場合、メニュー・アクセス制御の移行の枠を超えている場合があります。権限を借用するプログラムと、これらのプログラムを所有するユーザー・プロファイルの両方を保護してください。

現行メニューを移行環境のセットアップする際に役立てながら、アプリケーションとオブジェクトを徐々に分析していくことができます。以下、オーダー・エントリー (OEMENU) メニューと関連ファイルおよびプログラム使用する例を示します。

例: 移行環境のセットアップ

この例では、以下の前提事項と要件をもとに開始されます。

- すべてのファイルはライブラリー ORDERLIB に入っています。
- すべてのファイルの名前が分かっているわけではありません。また、メニュー・オプションがそれぞれのファイルに対してどの権限を必要としているかも分かりません。
- メニューおよびそれによって呼び出されるすべてのプログラムは ORDERPGM というライブラリーに入っています。
- システムにサインオンできるすべてのユーザーが、すべてのオーダー・ファイル、カスタマー・ファイル、および項目ファイルの情報を表示できるようにします (たとえば、QUERY やスプレッドシートを使用して)。

- 現行のサインオン・メニューが OEMENU であるユーザーのみが、ファイルを変更できなければなりません。また、これらのユーザーは、メニュー上のプログラムを使用してこれを行わなければなりません。
- 機密保護管理者以外のシステム・ユーザーは、*ALLOBJ や *SECADM の特殊権限を持っていません。

照会の要件を満たすようにこのメニュー・アクセス制御環境を変更するには、次のステップを実行します。

__ ステップ 1. 初期メニューが OEMENU であるユーザーのリストを作成します。

ユーザー・プロファイル印刷 (PRTUSRPRF *ENVINFO) コマンドを使用して、システム上のすべてのユーザー・プロファイルの環境をリストします。この報告書には、初期メニュー、初期プログラム、および現行ライブラリーが含まれています。 69 ページの図 7 は、この報告書の例を示しています。

__ ステップ 2. OEMENU オブジェクト (これは *PGM オブジェクトまたは *MENU オブジェクト) が、サインオンに使用されないユーザー・プロファイルによって所有されていることを確認します。ユーザー・プロファイルを使用不可にするか、または *NONE のパスワードをもたせます。この例では、 OEOWNER が OEMENU プログラム・オブジェクトを所有していると仮定しています。

__ ステップ 3. OEMENU プログラム・オブジェクトを所有するユーザー・プロファイルが、グループ・プロファイルでないことを確認します。次のコマンドを使用することができます。

```
DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)
```

__ ステップ 4. OEMENU プログラムが OEOWNER ユーザー・プロファイルの権限を借用するように、これを変更します。 (CHGPGM コマンドを使用して、USRPRF パラメーターを *OWNER に変更します。)

注: *MENU オブジェクトは権限を借用できません。 OEMENU が *MENU オブジェクトであれば、以下のいずれかを行ってこの例に当てはめることができます。

- メニューを表示するプログラムを作成します。
- ユーザーが OEMENU メニューからオプションを選択するときに実行するプログラムの借用権限を使用します。

__ ステップ 5. 以下の 2 つのコマンドを入力して、 ORDERLIB 内のすべてのファイルに対する共通権限を *USE に設定します。

```
RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*ALL)
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*USE)
```

*USE 権限を選択した場合は、ユーザーは、 PC ファイル転送または FTP を使用してこのファイルをコピーできるということを忘れないでください。

__ ステップ 6. 次のコマンドを入力して、メニュー・プログラムを所有するプロファイルに、ファイルに対する *ALL 権限を与えます。

```
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER)
     AUT(*ALL)
```

多くのアプリケーションでは、ファイルに対する *CHANGE 権限で十分です。しかし、アプリケーションによっては、*CHANGE よりも大きな権限を必要とする機能 (たとえば、物理ファイル・メンバーの消去など) を実行することもあります。最終的には、導入先が各アプリケーションを分析し、当該アプリケーションに必要な最小権限のみを提供すべきです。ただし、移行期間にあるときは、*ALL 権限を借用することにより、権限不足が原因で発生するようなアプリケーション障害が回避されます。

__ ステップ 7. 次のコマンドを入力して、オーダー・ライブラリーのプログラムに対する権限を制限します。

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC)
     AUT(*EXCLUDE)
```

__ ステップ 8. 次のコマンドを入力して、ライブラリーのプログラムに対する権限を OEOWNER プロファイルに与えます。

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER)
     AUT(*USE)
```

__ ステップ 9. ステップ 1 で識別されたユーザーごとに、次のコマンドを入力して、メニュー・プログラムに対する権限を与えます。

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(user-profile-name) AUT(*USE)
```

上記のステップを完了すると、明示的に除外されていないすべてのシステム・ユーザーが、 ORDERLIB ライブラリーのファイルにアクセスできるようになります (しかし変更はできません)。 OEMENU プログラムに対する権限を持っているユーザーは、メニューに示されているプログラムを使用して、 ORDERLIB ライブラリーのファイルを更新することができます。これで、OEMENU プログラムに対する権限を持っているユーザーだけが、このライブラリーのファイルを変更できるようになりました。オブジェクト・セキュリティーとメニュー・アクセス制御を組み合わせることで、ファイルが保護されます。

ユーザー・データが含まれているすべてのライブラリーについて上記のステップを完了すると、データベース更新を制御するための単純な体系が作成されます。この方式により、システム・ユーザーは、承認されたメニューとプログラムを使用しなければ、データベース・ファイルを更新できなくなります。同時に、意思決定サポート・ツールを持つユーザーや、他のシステムや PC からのリンクを持つユーザーが、データベース・ファイルを表示、分析、あるいはコピーしたりできるようになりました。

オブジェクト権限に関するヒント: システムがネットワークに参加すると、 *USE 権限が予期以上の権限を発揮することがあります。たとえば、FTP の場合に、あるファイルに対する *USE 権限を持っていれば、そのファイルを別のシステム (PC を含む) にコピーすることができます。

ライブラリー・セキュリティーの使用によるメニュー・セキュリティーの補足

ライブラリーのオブジェクトにアクセスするには、オブジェクトに対する権限とライブラリーに対する権限のどちらも持っていなければなりません。ほとんどの操作では、ライブラリーに対する *EXECUTE 権限か *USE 権限のどちらかが必要です。

状況に応じて、ライブラリー権限をオブジェクト保護のための簡単な手段として使用することができます。たとえば、オーダー・エントリー・メニューの例の場合、オーダー・エントリー・メニューに対する権限を持っているすべてのユーザーは、ORDERPGM ライブラリー内のすべてのプログラムを使用することができます。 個々のプログラムを保護するのではなく、 ORDERPGM ライブラリーに対する共通権限を *EXCLUDE に設定することができます。そうすれば、ライブラリーに対する *USE 権限を特定のユーザー・プロファイルに与えることができ、これにより、ライブラリーのプログラムを使用できるようになります (この場合、プログラムに対する共通権限が *USE であるか、またはそれより大きいと想定しています。)

ライブラリー権限を、オブジェクト権限を管理するための単純で効率的な方式として使用することができます。ただし、保護しようとしているライブラリーの内容について熟知していて、オブジェクトを不注意にアクセスしないようにすることが必要です。

オブジェクト所有権の構成

システム上のオブジェクトの所有権は、オブジェクト権限体系の重要な部分を占めています。デフォルトで、あるオブジェクトの所有者は、そのオブジェクトに対して *ALL 権限を持っています。「*iSeries 機密保護解説書*」の第 5 章では、オブジェクト所有権を計画するための推奨事項と例が提示されています。次に、いくつかのヒントを示します。

- 一般に、グループ・プロファイルはオブジェクトを所有してはなりません。グループ・プロファイルがオブジェクトを所有すると、グループ・メンバーが明示的に除外されない限り、すべてのグループ・メンバーがそのオブジェクトに対して *ALL 権限をもちます。
- 借用権限を使用する場合は、プログラムを所有するユーザー・プロファイルも、ファイルのような専用のアプリケーション・オブジェクトを所有するかどうかを考慮してください。権限を借用するプログラムを実行するユーザーに、ファイルに対する *ALL 権限をもたせないようにすることができます。

iSeries ナビゲーターを使用している場合、これは、セキュリティー・**ポリシー**機能を使用して変更を完了することによって達成できます。詳しくは、iSeries Information Center を参照してください (詳細は、 xii ページの『前提条件および関連情報』を参照してください)。

システム・コマンドとプログラムに対するオブジェクト権限

次に、IBM 提供オブジェクトに対する権限を制限する場合の推奨事項をいくつか示します。

- システム上に複数の国別言語がある場合は、システムには、複数のシステム (QSYS) ライブラリーがあります。システムでは、各国別言語ごとに QSYSxxxx ライブラリーがあります。オブジェクト権限を使用してシステム・コマンドへのアクセスを制御する場合は、QSYS ライブラリーおよびシステム上のすべての QSYSxxx ライブラリーのコマンドを保護することを忘れないでください。
- System/38™ ライブラリーが、制限したいコマンドと同等の機能を持つコマンドを提供することがあります。 QSYS38 ライブラリー内の同等コマンドも制限するようにしてください。
- System/36™ 環境の場合は、追加プログラムの制限を必要とする場合があります。たとえば、QY2FTML プログラムは System/36 ファイル転送を提供します。

セキュリティー機能の監査

この章では、システムにおけるセキュリティーの有効性を監査する手法について説明します。システム・セキュリティーの監査は、次のような理由から行われます。

- セキュリティー計画が完全であるかどうかを評価するため。
- 計画したセキュリティー管理が行われているかどうかを確認するため。このタイプの監査は、通常、日単位のセキュリティー管理の一部として機密保護担当者によって行われます。また、定期的に行われるセキュリティー・レビューの一部として、さらに綿密に、内部または外部の監査担当者によって行われることもあります。
- システム・セキュリティーが、システム環境に対し行なわれた変更に対応できていることを確認するため。セキュリティーに影響する変更には、次のようなものがあります。
  - システム・ユーザーによる新規オブジェクトの作成
  - システムへの新規ユーザーの許可
  - オブジェクト所有権の変更 (権限が調整されていない)
  - 責任の変更 (ユーザー・グループの変更)
  - 一時的権限 (適時に取り消されていない)
  - 新規プロダクトの導入
- 将来のイベント (新規アプリケーションの導入、上位セキュリティー・レベルへの移行、通信ネットワークの設定など) の準備を行うため。

この章で説明する技法は、これらのすべての状態に当てはまります。監査する対象およびその頻度は、組織のサイズおよびセキュリティーの必要性によって決まります。この章の目的は、監査の頻度についてのガイドラインを示すことではなく、どのような情報が使用可能であるか、その情報をどのようにして入手するか、また、その情報がなぜ必要なのかについて説明することです。

この情報は次の 3 つの部分から成り立ちます。

- 計画および監査できるセキュリティー項目のチェックリスト。
- システムにより提供される監査ジャーナルのセットアップおよび使用に関する情報。
- システムのセキュリティー情報を収集するための、その他の手法。

セキュリティー監査には、iSeries システムにおけるコマンドの使用、システムのログおよびジャーナル情報へのアクセスが含まれます。システムのセキュリティー監査を行う人が使用するために、特別なプロファイルを作成することができます。監査プロファイルは、システムの監査特性を変更することができる *AUDIT 特殊権限を必要とします。この章に記載されている監査タスクの中には、*ALLOBJ および *SECADM 特殊権限があるユーザー・プロファイルを必要とするものもあります。監査期間が終了したら、必ず、監査プロファイルのパスワードを *NONE に設定してください。

セキュリティー監査についての詳細は、「*iSeries 機密保護解説書*」の第 9 章を参照してください。

ユーザー・プロファイルの分析

認可ユーザー表示 (DSPAUTUSR) コマンドを使用して、システムの全ユーザーの完全なリストを表示または印刷することができます。リストは、プロファイル名順またはグループ・プロファイル名順に並べることができます。以下に、グループ・プロファイル順の例を示します。

```
                                認可ユーザーの表示

                                最終
グループ・          ユーザー・   変更          パスワード
プロファイル        プロファイル パスワード      なし      テキスト
DPTSM
                    ANDERSOR     99/08/04                  ROGER ANDERSON
                    VINCENTM     99/09/15                  MARK VINCENT
DPTWH
                    ANDERSOR     99/08/04                  ROGER ANDERSON
                    WAGNERR      99/09/06                  ROSE WAGNER
QSECOFR
                    JONESS       99/09/20                  SHARON JONES
                    HARRISOK     99/08/29                  KEN HARRISON
*NO GROUP
                    DPTSM        99/09/05        X         SALES AND MARKETING
                    DPTWH        99/08/13        X         WAREHOUSE
                    RICHARDS     99/09/05                  JANET RICHARDS
                    SMITHJ       99/09/18                  JOHN SMITH
```

選択されたユーザー・プロファイルの印刷

ユーザー・プロファイル表示 (DSPUSRPRF) コマンドを使用して、照会ツールを使用して処理できる出力ファイルを作成することができます。

```
DSPUSRPRF USRPRF(*ALL) +
          TYPE(*BASIC) OUTPUT(*OUTFILE)
```

照会ツールを使用して、次のような、さまざまな出力ファイルの分析報告書を作成することができます。

- *ALLOBJ と *SPLCTL の両方の特殊権限を持っているすべてのユーザーのリスト。
- 初期プログラムまたはユーザー・クラスなどのユーザー・プロファイル・フィールド順に並べたすべてのユーザーのリスト。

照会プログラムを作成して、出力ファイルとは異なる報告書を作成することができます。たとえば、次のようなことができます。

- UPSPAU フィールドが *NONE でないレコードを選択して、特殊権限を持っているすべてのユーザー・プロファイルをリストする。
- *Limit capabilities* フィールド (モデル・データベース出力ファイルでは UPLTCP と呼ばれている) が *NO または *PARTIAL であるレコードを選択して、コマンドの入力を許可されているすべてのユーザーをリストする。
- 特殊な初期メニューまたは初期プログラムを持っているすべてのユーザーをリストする。
- 最終サインオン日付フィールドを見て、非活動ユーザーをリストする。

大規模なユーザー・プロファイルの検査

非常に多くの権限を持つユーザー・プロファイルがシステムの大部分に点在していると見なされる場合、それはセキュリティー計画の不足を反映している可能性があります。以下に、大規模なユーザー・プロファイルの見付け方および評価のしかたの一例を示します。

1. オブジェクト記述表示 (DSPOBJD) コマンドを使用して、システム上のすべてのユーザー・プロファイルに関する情報が入っている出力ファイルを作成します。

   ```
   DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
           DETAIL(*BASIC) OUTPUT(*OUTFILE)
   ```

2. 照会プログラムを作成して、各ユーザー・プロファイルの名前とサイズを、サイズの大きい順にリストします。
3. 最も大規模なユーザー・プロファイルに関する情報を印刷して、権限および所有オブジェクトが適切かどうかを評価します。

   ```
   DSPUSRPRF USRPRF(user-profile-name) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(user-profile-name) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   IBM 提供のユーザー・プロファイルには、多数のオブジェクトを所有しているために、非常に大規模なユーザー・プロファイルがあります。通常、これらをリストおよび分析する必要はありません。ただし、QSECOFR および QSYS のような、*ALLOBJ 特殊権限を持つ IBM 提供のユーザー・プロファイルの権限を使用しているプログラムについては、調べる必要があります。

セキュリティー監査についての詳細は、「*iSeries 機密保護解説書*」の第 9 章を参照してください。

オブジェクト権限の分析

以下の方法で、誰がシステムのライブラリーに対する権限を持っているかを判別することができます。

1. DSPOBJD コマンドを使用して、システム上のすべてのライブラリーをリストします。

   ```
   DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
   ```

   注: 状況が AVAILABLE ではない独立補助記憶域プール (ASP) 内のライブラリーは、このコマンドでは表示されません。

2. オブジェクト権限表示 (DSPOBJAUT) コマンドを使用して、特定のライブラリーに対する権限をリストします。

```
DSPOBJAUT OBJ(QSYS/library-name) OBJTYPE(*LIB) +
          ASPDEV(asp-device-name) OUTPUT(*PRINT)
```

3. ライブラリー表示 (DSPLIB) コマンドを使用して、ライブラリー内のオブジェクトをリストします。

```
DSPLIB LIB(QSYS/library-name) ASPDEV(asp-device-name) OUTPUT(*PRINT)
```

これらの報告書を使用して、ライブラリー内に何が入っているか、および誰がライブラリーに対するアクセス権限を持っているかを判別することができます。必要であれば、DSPOBJAUT コマンドを使用して、ライブラリー内で選択されたオブジェクトについての権限を表示することもできます。

更新されたオブジェクトの検査

オブジェクト保全性検査 (CHKOBJITG) コマンドを使用して、更新されたオブジェクトを探すことができます。オブジェクトが更新されている場合は、通常、誰かがシステムに損傷を与えようとしていることを示しています。以下のようなことが行われた後に、このコマンドを実行してください。

- システムにプログラムが復元された場合
- 専用保守ツール (DST) が使用された場合

コマンドを実行すると、システムは、考えられる保全性問題の情報を含むデータベース・ファイルを作成します。1 つのプロファイル、多数の異なるプロファイル、またはすべてのプロファイルによって所有されているオブジェクトを検査することができます。ドメインが更新されているオブジェクトを探すことができます。また、タイプが *PGM、*SRVPGM、*MODULE、および *SQLPKG である更新されたオブジェクトを探すために、プログラム妥当性検査値を再計算することもできます。

CHKOBJITG プログラムを実行するには、*AUDIT 特殊権限が必要です。このコマンドは、スキャンや計算を行うため、長時間かかることがあります。このコマンドは、システムがビジーでない時に実行しなければなりません。

注: 多くの専用権限があるオブジェクトを多数所有するプロファイルは、大規模になる可能性があります。所有者プロファイルのサイズは、所有オブジェクトに対する権限を表示および操作する場合や、プロファイルを保管または復元する場合に、パフォーマンスに影響を与えます。システム操作も影響を受ける可能性があります。パフォーマンスまたはシステム操作のいずれにも影響を与えないようにするには、オブジェクトの所有権を複数のプロファイルに分散します。**すべての (または、ほとんどすべての) オブジェクトを 1 つの所有者プロファイルのみに割り当てないでください。**

権限を借用するプログラムの分析

*ALLOBJ 特殊権限を持っているユーザーの権限を借用するプログラムは、機密漏れを表しています。以下の方法で、これらのプログラムを検索および検査することができます。

1. *ALLOBJ 特殊権限を持っているそれぞれのユーザーごとに、借用プログラム表示 (DSPPGMADP) コマンドを使用して、ユーザーの権限を借用するプログラムをリストします。

```
DSPPGMADP USRPRF(user-profile-name) +
          OUTPUT(*PRINT)
```

注: 56 ページの『選択されたユーザー・プロファイルの印刷』に、*ALLOBJ 権限を持っているユーザーをリストする方法が示されています。

2. DSPOBJAUT コマンドを使用して、誰が各借用プログラムを使用する許可を与えられているか、プログラムに対する共通権限は何かを判別します。

```
DSPOBJAUT OBJ(library-name/program-name) +
          OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
          OUTPUT(*PRINT)
```

3. ソース・コードおよびプログラム記述を検査して、次のことを評価します。
   - プログラムのユーザーが過度な機能 (借用プロファイルで実行されているのに、コマンド行を使用するなど) を使用していないかどうか。
   - プログラムが、目的とされた機能に必要な最低レベルの権限を借用しているかどうか。オブジェクトおよびプログラムについて同じ所有者プロファイルを使用して、プログラム障害を使用するアプリケーションを設計できます。プログラム所有者の権限が借用されると、ユーザーは、アプリケーション・オブジェクトに対して *ALL 権限を持ちます。多くの場合、所有者プロファイルに特殊権限は必要ありません。
4. DSPOBJD コマンドを使用して、プログラムが最後に変更されたのはいつであるかを検査します。

```
DSPOBJD OBJ(library-name/program-name) +
        OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
        DETAIL(*FULL)
```

監査ジャーナルとジャーナル・レシーバーの管理

監査ジャーナル QSYS/QAUDJRN は、セキュリティー監査のみを行うためのものです。オブジェクトは、監査ジャーナルに記録されません。コミットメント制御に、監査ジャーナルを使用してはなりません。ジャーナル項目送信 (SNDJRNE) コマンドやジャーナル項目送信 (QJOSJRNE) API を使用して、ユーザー項目をこのジャーナルに送信してはなりません。

システムが監査項目を監査ジャーナルに書き込むことができるように、特殊なロック保護が使用されます。監査が活動状態である場合 (QAUDCTL システム値が *NONE でない場合)、システム・アービトレーター・ジョブ (QSYSARB) は、QSYS/QAUDJRN ジャーナルのロックを保留します。監査が活動状態である場合には、次のような特定の操作を監査ジャーナルで実行することはできません。

- DLTJRN コマンド
- ENDJRNxxx コマンド
- APYJRNCHG コマンド
- RMVJRNCHG コマンド
- DMPOBJ または DMPSYSOBJ コマンド
- ジャーナルの移動
- ジャーナルの復元
- GRTOBJAUT コマンドのような、権限を使用する操作
- WRKJRN コマンド

セキュリティー・ジャーナル項目に記録される情報は、「*iSeries 機密保護解説書*」に記載されています。監査ジャーナルのすべてのセキュリティー項目には、T というジャーナル・コードが付いています。セキュリティー項目の他に、ジャーナル QAUDJRN には、システム項目もあります。これらの項目には J というジャーナル・コードが付いており、初期プログラム・ロード (IPL) およびジャーナル・レシーバーで行われる一般的な操作 (たとえば、レシーバーの保管など) に関連しています。

ジャーナルまたは現行レシーバーが損傷を受けたために監査項目を記録できない場合には、QAUDENDACN システム値によって、システムの処置が決定されます。損傷を受けたジャーナルまたはジャーナル・レシーバーの回復は、他のジャーナルの回復と同じです。

システムにおいて、ジャーナル・レシーバーの変更を管理したい場合があります。QAUDJRN ジャーナルの作成時に MNGRCV(*SYSTEM) を指定するか、またはジャーナルをその値に変更します。 MNGRCV(*SYSTEM) を指定した場合、システムは、しきい値サイズに達すると自動的にレシーバーを切り離し、新規のジャーナル・レシーバーを作成して接続します。これは、**システムのジャーナル変更管理**と呼ばれます。詳細については、「iSeries Information Center」—>「システム管理」->「ジャーナル管理」->「ローカル・ジャーナル管理」->「ジャーナルの管理」を参照してください。 iSeries Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。

第 6 章 権限の管理

システムで権限がどのようにセットアップされているかを追跡するのに役立つ一連の報告書が用意されています。これらの報告書を始めに実行しておくと、すべてのこと (たとえば、すべてのファイルやすべてのプログラムに関する権限) を印刷することができます。

情報の基盤を確立したら、定期的に変更バージョンの報告書を実行することができます。変更バージョンを使用すれば、注意が必要なシステム上のセキュリティー関連の変更を識別するのに役立ちます。たとえば、ファイルの共通権限を示す報告書を毎週実行することができます。変更バージョンの報告書のみを要求することができます。この報告書には、すべてのユーザーが使用できるシステム上の新規のファイルと、最終報告書以降に共通権限が変更された既存のファイルの両方が示されます。

次の 2 つのメニューを使用してセキュリティー・ツールを実行することができます。

- プログラムを対話式に実行するために SECTOOLS メニューを使用します。
- プログラムをバッチで実行するために SECBATCH メニューを使用します。SECBATCH メニューは、 2 つの部分に分かれています。1 つは、ジョブを即時にジョブ待ち行列に投入するためのメニューであり、もう 1 つは、ジョブをジョブ・スケジューラーに入れるためのメニューです。

iSeries ナビゲーターを使用している場合は、次のステップに従ってセキュリティー・ツールを実行してください。

1. iSeries ナビゲーターで、ユーザーのサーバー —>「**セキュリティー**」と展開する。
2. 「**ポリシー**」を右マウス・ボタンでクリックし、「**エクスプローラー**」を選択して、作成および管理できるポリシーのリストを表示する。

オブジェクトに対する共通権限のモニター

簡明さのためにもパフォーマンスのためにも、大部分のシステムは、大部分のオブジェクトが大部分のユーザーに使用可能になるようにセットアップされます。ユーザーは、すべてのオブジェクトを使用できることを明示的に許可されるのではなく、セキュリティーが重要な特定の機密オブジェクトにアクセスすることを明示的に拒否されます。高いセキュリティー要件を持つ少数のシステムは、これとは反対のアプローチを取り、必要に応じてオブジェクトを許可します。これらのシステムでは、大部分のオブジェクトは、共通権限を *EXCLUDE に設定して作成されます。

iSeries は、オブジェクト・ベースのシステムであり、多くの異なるタイプのオブジェクトを持っています。大部分のオブジェクト・タイプは機密情報を持っていないか、セキュリティー関連の機能を実行しません。一般的なセキュリティー・ニーズを持つ iSeries システムの機密保護管理者としては、データベース・ファイルやプロ

グラムのような、保護を必要とするオブジェクトに注意を払う必要があります。その他のオブジェクト・タイプの場合は、アプリケーションにとって十分な共通権限だけを設定することができます。大部分のオブジェクト・タイプの共通権限は *USE です。

共通権限印刷 (PRTPUBAUT) コマンドを使用して、共通ユーザーがアクセスできるオブジェクトに関する情報を印刷することができます。(**共通ユーザー**とは、オブジェクトに対する明示的な権限を所有していない、サインオン権限を持ったユーザーをいいます。) PRTPUBAUT コマンドを使用する場合は、調べたいオブジェクト・タイプ、およびライブラリーまたはディレクトリーを指定することができます。SECBATCH メニューと SECTOOLS メニューのオプションを使用して、通常ほとんどの場合セキュリティーと密接な関係にあるオブジェクト・タイプに関する「共通権限オブジェクト報告書」を印刷することができます。この報告書の変更バージョンを定期的に印刷して、どのオブジェクトに注意が必要であるか確認することができます。

新規オブジェクトに対する権限の管理

OS/400 は、システム上の新規オブジェクトに関する権限と所有権を管理する際に役立つ機能を提供します。ユーザーが新規オブジェクトを作成すると、システムは以下のことを決定します。

- 誰がそのオブジェクトを所有するのか
- そのオブジェクトに関する共通権限は何か
- そのオブジェクトが私用権限を持っているかどうか
- そのオブジェクトをどこに入れるか (どのライブラリーまたはディレクトリーに)
- そのオブジェクトへのアクセスを監査するかどうか

システムは、これらの決定を行うために、システム値、ライブラリー・パラメーター、およびユーザー・プロファイル・パラメーターを使用します。「*iSeries 機密保護解説書*」第 5 章の『新しいオブジェクトへの権限および所有権の割り当て』に、使用可能ないくつかのオプションの例が示されています。

PRTUSRPRF コマンドを使用して、新規オブジェクトの所有権と権限に影響を与えるユーザー・プロファイル・パラメーターを印刷することができます。 67 ページの図 5 は、この報告書の例を示しています。

権限リストのモニター

権限リストを使用して、類似のセキュリティー要件を持つオブジェクトごとに分類することができます。概念的には、権限リストは、ユーザーのリストと、リストによって保護されているオブジェクトに対してユーザーが持っている権限を示しています。権限リストは、システム上の類似のオブジェクトに対する権限を管理するための効率的な方法を提供します。ただし、場合によっては、権限リストがオブジェクトに対する権限の追跡を困難にすることもあります。

私用権限オブジェクトの印刷 (PRTPVTAUT) コマンドを使用して、権限リストの権限に関する情報を印刷することができます。 63 ページの図 3 は、報告書の例を示しています。

```
                                  私用権限 (全報告書)
5722SS1 VXRXMX  000000
  権限                    1 次                          リスト -------オブジェクト--------  ---------データ----------
  リスト       所有者     グループ   ユーザー    権限      MGT  OPR  MGT  EXIST  ALTER  REF  READ  ADD  UPD  DLT   実行
  LIST1        QSECOFR    *NONE      *PUBLIC     *EXCLUDE
  LIST2        BUDNIKR    *NONE      BUDNIKR     *ALL       X    X    X     X      X     X    X     X    X    X     X
                                     *PUBLIC     *CHANGE         X                          X     X    X    X     X
  LIST3        QSECOFR    *NONE      *PUBLIC     *EXCLUDE
  LIST4        CJWLDR     *NONE      CJWLDR      *ALL       X    X    X     X      X     X    X     X    X    X     X
                                     GROUP1      *ALL            X    X     X      X     X    X     X    X    X     X
                                     *PUBLIC     *EXCLUDE
```

図 3. 権限リストに関する私用権限報告書

この報告書は、権限リスト編集 (EDTAUTL) 表示画面に表示されるものと同じ情報を示しています。この報告書の利点は、すべての権限リストに関する情報が 1 ページで示されることです。たとえば、新規のオブジェクト・グループに関するセキュリティーをセットアップする場合は、報告書をす早くスキャンして、既存の権限リストがこれらのオブジェクトに対するニーズを満たしているかどうかを確認することができます。

変更バージョンの報告書を印刷して、新規の権限リストや、報告書を最後に印刷してから権限が変更された権限リストを見ることができます。また、各権限リストによって保護されているオブジェクトのリストを印刷することもできます。 図 4 は、1 つの権限リストに関する報告書の例を示しています。

```
                              権限リスト・オブジェクトの表示
5722SS1 VXRXMX  000000
 権限リスト . . . . . . . . . . . . :   CUSTAUTL
   ライブラリー . . . . . . . . . . :   QSYS
 所有者 . . . . . . . . . . . . . . :   AROWNER
 1 次グループ . . . . . . . . . . . :   *NONE
                                                    1 次
オブジェクト    ライブラリー    タイプ       所有者          グループ       テキスト
 CUSTMAS        CUSTLIB        *FILE        AROWNER         *NONE
 CUSTORD        CUSTORD        *FILE        OEOWNER         *NONE
```

図 4. 権限リスト・オブジェクト報告書の表示

この報告書を使用すれば、たとえば、新規ユーザーを権限リストに追加した場合の効果 (そのユーザーがどの権限を受け取るか) が分かります。

権限リストの使用

iSeries ナビゲーターは、セキュリティー計画およびポリシーの開発を支援し、お客さまの企業のニーズに合わせてシステムを構成するために設計されたセキュリティー機能を提供します。使用可能な機能の 1 つに、権限リストの使用があります。

権限リストには、次のような機能があります。

- 類似したセキュリティー要件をもつ権限リスト・グループ・オブジェクト。
- 権限リストには、概念的に、ユーザーやグループ、およびリストによって保護されているオブジェクトに対してユーザーおよびグループが持っている権限が含まれている。
- 各ユーザーおよびグループは、リストによって保護されているオブジェクトのセットに対してさまざまな権限を持つことができる。
- 権限を、ユーザーおよびグループに対して個々に付与せずに、リストによって付与することができる。

権限リストを使用して行えるタスクには、次のものがあります。

- 権限リストの作成
- 権限リストの変更
- ユーザーおよびグループの追加
- ユーザー許可の変更
- 保護されるオブジェクトの表示

この機能を使用するには、次のステップを実行します。

1. iSeries ナビゲーターで、ユーザーのサーバー —>「セキュリティー」と展開する。「**権限リスト**」および「**ポリシー**」が表示されます。
2. 「**権限リスト**」を右マウス・ボタンでクリックし、「**新規権限リスト**」を選択する。「**新規権限リスト**」で、次のことを行うことができます。
   - 「**使用**」: オブジェクト属性にアクセスして、オブジェクトを使用することができる。共通のものは表示できますが、オブジェクトを変更することはできません。
   - 「**変更**」: オブジェクトの内容 (いくつかの例外があります) を変更することができる。
   - 「**すべて**」: 所有者に限定されているオブジェクトを除く、オブジェクトに関するすべての操作が行える。ユーザーまたはグループは、オブジェクトの存在の制御、オブジェクトのセキュリティーの指定、オブジェクトの変更、およびオブジェクトに関する基本機能の実行を行うことができます。また、ユーザーまたはグループは、オブジェクトの所有権を変更することもできます。
   - 「**除外**」: オブジェクトに関するすべての操作が禁止される。この許可を持っているユーザーおよびグループには、オブジェクトへのアクセスまたは操作が許可されません。共通でオブジェクトを使用することができないように指定してください。

権限リストを処理する際に、オブジェクトとデータの両方の許可を与えることになります。選択できるオブジェクト許可は、次のとおりです。

- 「**作動可能**」: オブジェクトの記述を見るための許可と、そのオブジェクトに対してユーザーまたはグループが持っているデータ許可によって決められている通りにオブジェクトを使用するための許可を与える。
- 「**管理**」: オブジェクトのセキュリティーを指定するための許可、オブジェクトを移動またはリネームするための許可、データベース・ファイルにメンバーを追加するための許可を与える。
- 「**存在**」: オブジェクトの存在および所有権を制御するための許可を与える。ユーザーまたはグループは、オブジェクトの削除、オブジェクトのストレージの解放、オブジェクトに関する保管および復元操作の実行、オブジェクトの所有権の移行を行うことができます。ユーザーまたはグループが特殊な保管許可を持っている場合には、ユーザーまたはグループは、オブジェクトの存在許可を必要としません。
- 「**変更** (データベース・ファイルおよび SQL パッケージに限り使用される)」: オブジェクトの属性を更新するために必要な許可を与える。ユーザーまたはグループがデータベース・ファイルに関してこの許可を持っている場合には、ユーザーまたはグループは、トリガーの追加および除去、参照制約および固有制約の追加および除去、データベース・ファイルの属性の変更を行うことができます。ユーザーまたはグループが SQL パッケージに関してこの許可を持っている場合に

は、ユーザーまたはグループは、SQL パッケージの属性を変更することができます。この許可は、現時点では、データベース・ファイルおよび SQL パッケージに限り使用されます。
- 「**参照** (データベース・ファイルおよび SQL パッケージに限り使用される)」: あるオブジェクトの操作が他のオブジェクトによって制限されている場合などに、他のオブジェクトからあるオブジェクトを参照するために必要な許可を与える。ユーザーまたはグループが物理ファイルに関してこの許可を持っている場合には、ユーザーまたはグループは、物理ファイルが親である参照制約を追加することができます。この許可は、現時点では、データベース・ファイルに限り使用されます。

選択できるデータ許可は、次のとおりです。
- 「**読み取り**」: オブジェクトの内容を入手および表示する (ファイルのレコードを表示するなど) ために必要な許可を与える。
- 「**追加**」: オブジェクトに項目を追加する (メッセージをメッセージ待ち行列に追加する、レコードをファイルに追加するなど) ための許可を与える。
- 「**更新**」: オブジェクトの項目を変更する (ファイルのレコードを変更する) ための許可を与える。
- 「**削除**」: オブジェクトから項目を除去する (メッセージをメッセージ待ち行列から削除する、レコードをファイルから除去するなど) ための許可を与える。
- 「**実行**」: プログラム (サービス・プログラムまたは SQL パッケージ) を実行するために必要な許可を与える。ユーザーは、ライブラリーまたはディレクトリー内のオブジェクトを見付けることもできます。

権限リストの作成または編集時の各プロセスの詳細については、 iSeries ナビゲーターのオンライン・ヘルプを使用してください。

iSeries ナビゲーターでのポリシーへのアクセス

iSeries ナビゲーターを使用して、iSeries サーバーのポリシーを表示したり管理したりすることができます。 iSeries ナビゲーターには 5 つのポリシーの分野があります。

- **監査ポリシー**
  ここでは、システム上の特定の資源に対する特定のアクションおよびアクセスのモニターをセットアップすることができます。
- **セキュリティー・ポリシー**
  ここでは、セキュリティーのレベル、およびシステム・セキュリティーに関連する追加オプションを指定することができます。
- **パスワード・ポリシー**
  ここでは、システムのパスワード・レベルを指定することができます。
- **リストア・ポリシー**
  ここでは、特定のオブジェクトをシステム上で復元する方法を指定することができます。
- **サインオン・ポリシー**
  ここでは、ユーザーがシステムにサインオンする方法を指定することができます。

iSeries ナビゲーターを使用してポリシーを表示または変更する場合は、次のステップに従ってください。

1. iSeries ナビゲーターで、ユーザーのサーバー —>「**セキュリティー**」と展開する。
2. 「**ポリシー**」を右マウス・ボタンでクリックし、「**エクスプローラー**」を選択して、作成および管理できるポリシーのリストを表示する。これらのポリシーに固有の情報については、iSeries ナビゲーターのヘルプを参照してください。

オブジェクトに対する私用権限のモニター

SECBATCH メニュー・オプション:
12 *は即時に投入する、* **41** *はジョブ・スケジューラーを使用する*

私用権限オブジェクトの印刷 (PRTPVTAUT) コマンドを使用すれば、指定したライブラリーに含まれている指定したタイプのオブジェクトに関するすべての私用権限のリストを印刷することができます。

この報告書を使用すると、オブジェクトに対する新規の権限を検出するのに役立ちます。この報告書は、私用権限体系が複雑になり過ぎて管理不能になるのを防止するのにも役立ちます。

出力待ち行列とジョブ待ち行列へのアクセスのモニター

機密保護管理者は、ファイル・アクセスの保護という大きなジョブを行った後で、ファイルの内容を印刷するときに発生した状態について忘れてしまうことがあります。iSeries サーバーには、重要な出力待ち行列やジョブ待ち行列を保護するための機能が用意されています。出力待ち行列を保護することで、たとえば、無許可のユーザーが印刷待ちの機密スプール・ファイルを表示したりコピーしたりできないようにします。ジョブ待ち行列を保護することで、無許可のユーザーが機密ジョブを非機密出力待ち行列に宛先変更したり、ジョブ全体を取り消したりできないようにします。

SECBATCH メニュー・オプション:
24 は即時に投入する、 63 *はジョブ・スケジューラーを使用する*

Information Center の「*基本システム・セキュリティーおよび計画*」および「*iSeries 機密保護解説書*」には、出力待ち行列とジョブ待ち行列を保護する方法が示されています。

待ち行列権限印刷 (PRTQAUT) コマンドを使用して、システム上のジョブ待ち行列と出力待ち行列のセキュリティー設定を印刷することができます。 その後で、機密情報を印刷する印刷ジョブを評価し、それらの印刷ジョブが、保護されている出力待ち行列やジョブ待ち行列に送られることを確認することができます。

セキュリティーが重要であると考えられる出力待ち行列とジョブ待ち行列については、セキュリティーの設定を「*iSeries 機密保護解説書*」の付録 D の情報と比較することができます。付録 D のテーブルには、出力待ち行列とジョブ待ち行列の各種の機能を実行するために必要な設定が示されています。

特殊権限のモニター

システムのユーザーが不要な特殊権限を持っていると、適切なオブジェクト権限体系を開発しようとする努力が無駄になることがあります。ユーザー・プロファイルが *ALLOBJ 特殊権限を持っていると、オブジェクト権限は無意味になります。出力待ち行列を保護しようとどのように努力しても、 *SPLCTL 特殊権限を持つユーザーは、システム上のすべてのスプール・ファイルを見ることができます。
*JOBCTL 特殊権限を持つユーザーは、システム操作に影響を与え、ジョブを宛先変更することができます。 *SERVICE 特殊権限を持つユーザーは、オペレーティング・システムを介さなくても、保守ツールを使用してデータにアクセスすることができます。

SECBATCH メニュー・オプション:
29 は即時に投入する、 68 *はジョブ・スケジューラーを使用する*

ユーザー・プロファイル印刷 (PRTUSRPRF) コマンドを使用して、システム上のユーザー・プロファイルの特殊権限とユーザー・クラスに関する情報を印刷することができます。報告書を実行するときは、次のようないくつかのオプションを使用することができます。
- すべてのユーザー・プロファイル
- 特定の特殊権限を持つユーザー・プロファイル
- 特定のユーザー・クラスを持つユーザー・プロファイル
- ユーザー・クラスと特殊権限の間でミス・マッチしているユーザー・プロファイル

図 5 は、すべてのユーザー・プロファイルに関する特殊権限を示す報告書の例を示しています。

ユーザー・プロファイル情報

5722SS1 VXRXMX 000000
報告書タイプ . . . . . : *AUTINFO
選択ユーザー . . . . . : *SPCAUT
特殊権限 . . . . . : *ALL

		特殊権限												
ユーザー・プロファイル	グループ・プロファイル	*ALL OBJ	*AUD IT	*IO SYS CFG	*JOB CTL	*SAV SYS	*SEC ADM	*SER VICE	*SPL CTL	ユーザー・クラス	所有者	グループ権限	グループ権限タイプ	制約機能
USERA	*NONE	X	X	X	X	X	X	X	X	*SECOFR	*USRPRF	*NONE	*PRIVATE	*NO
USERB	*NONE				X	X				*PGMR	*USRPRF	*NONE	*PRIVATE	*NO
USERC	*NONE	X	X	X	X	X	X	X	X	*SECOFR	*USRPRF	*NONE	*PRIVATE	*NO
USERD	*NONE									*USER	*USRPRF	*NONE	*PRIVATE	*NO

図 5. ユーザー情報報告書: 例 1

特殊権限の他に、報告書には次の情報が示されています。
- ユーザー・プロファイルが制約機能を持っているかどうか

- ユーザーまたはユーザーのグループが、ユーザー作成の新規オブジェクトを所有しているかどうか
- ユーザー作成の新規オブジェクトに対して、ユーザーのグループがどの権限を自動的に受け取るか

図 6 は、ミス・マッチした特殊権限とユーザー・クラスに関する報告書の例を示しています。

ユーザー・プロファイル情報

5722SS1 VXRXMX 000000
報告書タイプ . . . . . : *AUTINFO
選択ユーザー . . . . . : *MISMATCH

		特殊権限												
ユーザー・プロファイル	グループ・プロファイル	*ALL OBJ	*AUD IT	*IO SYS CFG	*JOB CTL	*SAV SYS	*SEC ADM	*SER VICE	*SPL CTL	ユーザー・クラス	所有者	グループ権限	グループ権限タイプ	制約機能
USERX	*NONE	X			X	X			X	*SYSOPR	*USRPRF	*NONE	*PRIVATE	*NO
USERY	*NONE						X			*USER	*USRPRF	*NONE	*PRIVATE	*NO
USERZ	QPGMR				X	X	X			*USER	*USRPRF	*NONE	*PRIVATE	*NO

図 6. ユーザー情報報告書: 例 2

図 6 では、次の点に注目してください。

- USERX は、システム操作員 (*SYSOPR) ユーザー・クラスを持っていますが、*ALLOBJ および *SPLCTL 特殊権限を持っています。
- USERY は、ユーザー (*USER) ユーザー・クラスを持っていますが、 *SECADM 特殊権限を持っています。
- USERZ も、ユーザー (*USER) クラスと *SECADM 特殊権限を持っています。USERZ が QPGMR グループのメンバーであり、このグループが *JOBCTL および *SAVSYS 特殊権限を持っていることを確認することができます。

これらの報告書を定期的に実行して、ユーザー・プロファイル管理のモニターに役立てることができます。

ユーザー環境のモニター

ユーザー・プロファイルの役割の 1 つは、出力待ち行列、初期メニュー、ジョブ記述など、ユーザーに関する環境を定義することです。ユーザーの環境は、ユーザーのシステムの見方に影響を与えるほか、ユーザーが実行を許可される操作にも、ある程度の影響を与えます。ユーザーは、ユーザー・プロファイルに指定されているオブジェクトに対して権限を持っていなければなりません。しかし、権限体系がまだ進行中であるか、またはあまり限定的でない場合は、ユーザー・プロファイルに定義されているユーザー環境が、意図しない結果を生成することがあります。次に、いくつかの例を示します。

SECBATCH メニュー・オプション:

29 *は即時に投入する、* **68** *はジョブ・スケジューラーを使用する*

- ユーザーのジョブ記述は、ユーザーよりも多くの権限を持つユーザー・プロファイルを指定することができます。
- ユーザーは、コマンド行のない初期メニューを持つことができます。しかし、ユーザーのアテンション・キー処理プログラムがコマンド行を提供することができます。
- ユーザーを、機密報告書を実行できるように許可することができます。しかし、ユーザーの出力を、報告書を見てはならないユーザーが使用できる出力待ち行列に送信することができます。

ユーザー・プロファイル印刷 (PRTUSRPRF) コマンドの *ENVINFO オプションを使用することで、システム・ユーザーのために定義されている環境のモニターに役立てることができます。 図 7 は、この報告書の例を示しています。

ユーザー・プロファイル情報

```
5722SS1 VXRXMX  000000
 報告書タイプ . . . . . :   *ENVINFO
 選択ユーザー . . . . . :   *USRCLS
                          初期              初期          ジョブ          メッセージ      出力          アテンション
 ユーザー・     現行       メニュー /        プログラム /  記述 /        QUEUE/          QUEUE/        プログラム /
 プロファイル   ライブラリー ライブラリー     ライブラリー  ライブラリー    ライブラリー    ライブラリー  ライブラリー
 AUDSECOFR      AUDITOR    MAIN              *NONE         QDFTJOBD        QSYSOPR         *WRKSTN       *SYSVAL
                           *LIBL                           QGPL            QSYS
 USERA          *CRTDFT    OEMENU            *NONE         QDFTJOBD        USERA           *WRKSTN       *SYSVAL
                           *LIBL                           QGPL            QUSRSYS
 USERB          *CRTDFT    INVMENU           *NONE         QDFTJOBD        USERB           *WRKSTN       *SYSVAL
                           *LIBL                           QGPL            QUSRSYS
 USERC          *CRTDFT    PAYRPLL           *NONE         QDFTJOBD        USERC           PAYROLL       *SYSVAL
                           *LIBL                           QGPL            QUSRSYS         PRGMLIB
```

図 7. ユーザー・プロファイルの印刷 - ユーザー環境例

保守ツールの管理

サーバーの構成、管理、保守には、保守ツールを使用します。保守ツールは、専用保守ツール (DST) またはシステム保守ツール (SST) からアクセスすることができます。 DST、SST にアクセスして、論理区画 (LPAR) 管理およびディスク装置管理に iSeries ナビゲーター機能を使用するには、保守ツールのユーザー ID が必要です。

DST は、OS/400 がロードされていない場合でも、ライセンス内部コードが起動されていれば、使用できます。 SST は、OS/400 から利用できます。次の表に、DST と SST の基本的な違いをまとめます。

特性	DST	SST
アクセス方法	手動 IPL 時に表示されるコンソールの使用、または制御パネルのオプション 21 の選択による物理的なアクセス。	QSRV または次の権限を使用してサインオンすることができる対話式ジョブによるアクセス。 • STRSST (システム保守ツール開始) CL コマンドに対する権限 • サービス特殊権限 (*SERVICE) または全オブジェクト特殊権限 (*ALLOBJ) • SST を使用するための機能特権
使用できる場合	サーバーの機能が制限されている場合でも使用可能。 DST にアクセスするのに OS/400 は必要ない。	OS/400 が起動されている場合に使用可能。 SST にアクセスするのに OS/400 が必要。
認証方法	保守ツールのユーザー ID とパスワードが必要。	保守ツールのユーザー ID とパスワードが必要。

保守ツールを使用して次のタスクを実行する方法については、「iSeries Information Center」—>「セキュリティー」—>「保守ツール」を参照してください。

- DST からの保守ツールへのアクセス
- SST からの保守ツールへのアクセス
- iSeries ナビゲーターからの保守ツールへのアクセス
- 保守ツール・ユーザー ID の作成
- 保守ツール・ユーザー ID の機能特権の変更
- 保守ツール・ユーザー ID の記述の変更
- 保守ツール・ユーザー ID の表示
- 保守ツール・ユーザー ID の使用可能化または使用不可化
- 保守ツール・ユーザー ID の削除
- SST または DST の使用による保守ツール・ユーザー ID とパスワードの変更
- STRSST 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 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 (QSYCHGDS) API の変更
- QSECOFR OS/400 ユーザー・プロファイル・パスワードのリセット
- QSECOFR 保守ツール・ユーザー ID とパスワードのリセット
- 保守ツール・セキュリティー・データの保管および復元
- 独自バージョンの QSECOFR 保守ツールのユーザー ID の作成
- DST の保守ツール・サーバーの構成
- OS/400 の保守ツール・サーバーの構成
- DST によるサービス機能使用のモニター
- OS/400 セキュリティー監査ログによる保守ツール使用のモニター

iSeries Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。

第 7 章 論理区画 (LPAR) セキュリティーの使用

単一の iSeries サーバーに複数の論理区画を持つことは、次のような点で有益です。

- **独立システムの維持:** それぞれの資源 (ディスク記憶域装置、プロセッサー、メモリー、および入出力装置) の一部を 1 つの区画に専用にすることにより、ソフトウェアの論理独立性が保たれます。また、論理区画が正しく構成されている場合には、ある程度のハードウェア耐障害性もあります。単一のマシンでは一緒にうまく稼働しない対話式とバッチの作業負荷を、別の区画に分離して、効率的に実行することができます。
- **統合:** 1 つのシステムを論理的に区画分割すれば、企業内で必要となる iSeries サーバー・システムの数を削減することができます。多数のシステムを単一の論理的に区画分割された 1 つのシステムに統合することができます。これにより、追加の装置およびそのための費用が不要になります。変更が必要な場合には、ある論理区画から別の論理区画に資源をシフトすることができます。
- **本番とテストの混合環境の作成:** 本番用環境とテスト環境を組み合わせた環境を作成することができます。1 次区画に、単一の本番用区画を作成できます。本番用区画が複数ある場合には、後述の『*複数の本番用区画環境の作成*』を参照してください。

  論理区画は、テスト区画または本番用区画のいずれかです。本番用区画は、主要なビジネス・アプリケーションを実行します。本番用区画での障害は、ビジネス・オペレーションを著しく妨げ、時間と費用を費やします。テスト区画は、ソフトウェアをテストします。テスト区画での障害は、必ずしも計画的なものであるとは限りませんが、通常のビジネス・オペレーションの妨げにはなりません。
- **複数の本番用区画環境の作成:** 複数の本番用区画を作成するのは、2 次区画にしてください。この場合、1 次区画を区画管理専用にします。
- **ホット・バックアップ:** 2 次区画を同じシステム内の別の論理区画に複製しておくと、区画障害時のバックアップへの切り替えの際に起こる問題を最小化することができます。また、この構成は、項目の多い保管ウィンドウの影響を最小化することもできます。他の論理区画が実動作業を継続している間に、バックアップ区画をオフラインにして保管することができます。このホット・バックアップ・ストラテジーを使用するには、特別なソフトウェアが必要です。
- **統合されたクラスター:** 高可用性アプリケーション・ソフトウェアの OptiConnect/400 を使用すると、区画化されたシステムは、統合されたクラスターとして作動します。統合されたクラスターを使用して、2 次区画内の計画外のほとんどの障害からシステムを保護することができます。

注: 2 次区画を設定する際には、カードの位置に注意しなければなりません。コンソールに選んだ入出力プロセッサー (IOP) にも LAN カードがあり、その LAN カードがオペレーション・コンソールと共に使用されるように設計されていない場合、カードはコンソールによって使用されるように活動化され、意図した目的に使用できない可能性があります。オペレーション・コンソールの処理について詳しくは、77 ページの『第 8 章 iSeries のオペレーション・コンソール』を参照してください。

このトピックについての詳細は、iSeries Information Centerの『論理区画』を参照してください。

論理区画のセキュリティー管理

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

次に、論理区画においてセキュリティーを扱う際に覚えておく必要のある基本規則をいくつかリストします。

- ユーザーを一度に 1 つのシステム論理区画に追加する。アクセスするユーザーを各論理区画ごとに追加する必要があります。
- 1 次区画の専用保守ツール (DST) およびシステム保守ツール (SST) にアクセスする権限を持つユーザーの数を制限する。 DST および SST についての詳細は、iSeries Information Centerの『iSeries ナビゲーター、DST、および SST を使用した論理区画の管理』を参照してください。保守ツール・ユーザー・プロファイルを使用した区画へのアクセス制御アクティビティーについては、 69 ページの『保守ツールの管理』を参照してください。

  注: iSeries ナビゲーターを使用して、LPAR 機能にアクセスする前に、保守ツール・サーバー (STS) を初期化しなければなりません。関連情報については、「iSeries Information Center」 —>「セキュリティー」—>「保守ツール」を参照してください。 iSeries Information Center へのアクセス方法については、xii ページの『前提条件および関連情報』を参照してください。
- 2 次区画では、主記憶装置および他の論理区画のディスク装置を見ることまたは使用することはできない。
- 2 次区画では、所有するハードウェア資源しか見ることができない。
- 1 次区画では、DST および SST の「システム区画の処理」で表示されているすべてのシステム・ハードウェアを見ることができる。
- 1 次区画オペレーティング・システムは、依然として、その使用可能な資源だけしか見ることができない。
- システム制御パネルは、1 次区画を制御する。パネル・モードを「保護 (Secure)」に設定している場合には、SST の「区画状況の処理」で処理を実行することはできません。システム制御パネルから DST を強制使用するには、モードを「手動 (Manual)」に変更する必要があります。
- 2 次区画の操作モードを「保護 (Secure)」に設定している場合には、「区画状況の処理」の使用は以下のように制限される。
  - 区画状況を変更する場合、2 次区画では DST しか使用できない。SST を使用して、区画状況を変更することはできません。
  - 2 次区画で DST を強制使用するには、1 次区画の「区画状況の処理」の DST または SST のいずれかしか使用できない。
  - 2 次区画モードを「保護 (Secure)」から他の値に変更する場合、1 次区画の DST しか使用できない。

2 次区画のモードが「保護 (Secure)」でなくなると、2 次区画で DST および SST の両方を使用して、区画状況を変更することができます。

iSeries サーバーにおけるセキュリティーについて詳しくは、「*機密保護解説書*」および iSeries Information Center の『基本システム・セキュリティーおよび計画』のページを参照してください。

第 8 章 iSeries のオペレーション・コンソール

オペレーション・コンソールでは、PC を使用して iSeries サーバーにアクセスし制御することができます。オペレーション・コンソールは、コンソール装置を持たない iSeries サーバーへのリモート PC ダイヤルインをサポートしており、リモート PC をコンソールとして利用することができます。オペレーション・コンソールを使用する際は、次の点に注意してください。

- 従来のコンソールからできなかったタスクを、オペレーション・コンソールから行うことができます。たとえば、*SERVICE または *ALLOBJ 特殊権限を持っているユーザー・プロファイルは、このプロファイルが使用不可であっても、オペレーション・コンソール・セッションにサインオンすることができます。
- オペレーション・コンソールは、保守ツール・ユーザー・プロファイルおよびパスワードを使用して、iSeries サーバーへの接続を可能にします。そのため、保守ツール・ユーザー・プロファイルおよびパスワードの変更が特に重要になります。ハッカーは、デフォルトの保守ツール・ユーザー・プロファイルのユーザー ID およびパスワードをよく知っており、これらを使用して、iSeries サーバーにリモート・コンソール・セッションを確立しようとするかもしれません。パスワードに関するヒントは、 22 ページの『割り当て済みパスワードの変更』および 28 ページの『デフォルト・パスワードの回避』を参照してください。
- リモート・コンソールを使用する場合に情報を保護するには、 Windows ダイヤルアップ・ネットワーキングのコールバック・オプションを使用してください。
- 2 次区画を設定する際には、カードの位置に注意しなければなりません。コンソールに選んだ入出力プロセッサー (IOP) にも LAN カードがあり、その LAN カードがオペレーション・コンソールと共に使用されるように設計されていない場合、カードはコンソールによって使用されるように活動化され、意図した目的に使用できない可能性があります。

V5R1 では、オペレーション・コンソールは拡張されて、コンソール・アクティビティーをローカル・エリア・ネットワーク (LAN) 全体に渡って行えるようになりました。認証およびデータ暗号化が拡張され、コンソール・プロシージャーに関するネットワーク・セキュリティーを提供します。LAN 接続のオペレーション・コンソールを使用する場合には、以下の製品を導入することを強くお勧めします。

- Cryptographic Access Provider (5722-AC2 または 5722-AC3) を iSeries サーバーに導入する
- Client Encryption (5722-CE2 または 5722-CE3) をオペレーション・コンソール PC に導入する

コンソール・データを暗号化するためには、iSeries サーバーに Cryptographic Access Provider 製品の 1 つを導入し、**かつ**、PC に Client Encryption 製品の 1 つを導入しなければなりません。

注: 暗号化製品が導入されていないと、データの暗号化は行われません。

次の表は、使用可能な製品の暗号化の結果を要約したものです。

表 13. 暗号化の結果

iSeries サーバーに導入する Cryptographic Access Provider	オペレーション・コンソール PC に導入する Client Encryption	データ暗号化の結果
None	None	None
5722-AC2	5722-CE2	56 ビット
5722-AC2	5722-CE3	56 ビット
5722-AC3	5722-CE2	56 ビット
5722-AC3	5722-CE3	128 ビット

iSeries オペレーション・コンソールのセットアップおよび管理の詳細については、iSeries Information Center を参照してください。

オペレーション・コンソールのセキュリティーの概要

オペレーション・コンソールのセキュリティーは、次のものから構成されます。

- コンソール装置認証
- ユーザー認証
- データ・プライバシー
- データ保全性

直接接続されているオペレーション・コンソールには、2 地点間接続により、暗黙的な認証、データ・プライバシー、およびデータ保全性があります。コンソール・ディスプレイにサインオンするには、ユーザー認証セキュリティーが必要です。

コンソール装置認証

コンソール装置認証では、物理装置がコンソールであることが保証されます。直接接続されているオペレーション・コンソールは、平衡型コンソールに似た物理接続を使用します。直接接続を使用しているオペレーション・コンソールには、平衡型接続と類似した物理コンソール装置に対するアクセスを制御するための、物理的保護が提供されます。

LAN 接続のオペレーション・コンソールは、証明書を使用せずに装置およびユーザー認証をサポートする Secure Sockets Layer (SSL) のバージョンを使用します。この接続形式の場合、装置認証は、保守ツール装置プロファイルに基づいて行われます。詳細は、79 ページを参照してください。

ユーザー認証

ユーザー認証では、コンソール装置を使用しているユーザーの本人性が保証されます。ユーザー認証に関連する事項は、コンソール・タイプにかかわらず、すべて同じです。

データ・プライバシー

データ・プライバシーでは、意図された受信者だけがコンソール・データを読み取ることができるという確信が与えられます。直接接続のオペレーション・コンソールは、平衡型コンソールまたは LAN 接続用のセキュアなネットワーク接続に類似した物理接続を使用して、コンソール・データを保護します。直接接続を使用するオペレーション・コンソールと、平衡型接続のデータ・プライバシーは同程度のものです。物理接続がセキュアである場合には、コンソール・データは保護されたままです。

LAN 接続のオペレーション・コンソールは、適切な暗号化製品 (ACx および CEx) が導入されている場合、セキュアなネットワーク接続を使用します。コンソール・セッションは、iSeries サーバーに導入されている暗号化製品およびオペレーション・コンソールが稼働している PC に基づいて、可能な限り強力な暗号化を使用します。

注: 暗号化製品が導入されていないと、データの暗号化は行われません。

データ保全性

データ保全性によって、コンソール・データが受信側に到着するまでに変更されないという確信が与えられます。直接接続のオペレーション・コンソールは、平衡型コンソールまたは LAN 接続用のセキュアなネットワーク接続に類似した物理接続を使用して、コンソール・データを保護します。直接接続を使用するオペレーション・コンソールと、平衡型接続のデータ保全性は同程度のものです。物理接続がセキュアである場合には、コンソール・データは保護されたままです。

LAN 接続のオペレーション・コンソールは、適切な暗号化製品 (ACx および CEx) が導入されている場合、セキュアなネットワーク接続を使用します。コンソール・セッションは、iSeries サーバーに導入されている暗号化製品およびオペレーション・コンソールが稼働している PC に基づいて、可能な限り強力な暗号化を使用します。

注: 暗号化製品が導入されていないと、データの暗号化は行われません。

LAN 接続のオペレーション・コンソールの使用

注: どのオペレーション・コンソール装置もコンソールにすることができますが、LAN ベース構成だけが保守ツール・ユーザー・プロファイルを使用します。

iSeries サーバーは、出荷時には、デフォルトの保守ツール装置プロファイル QCONSOLE (デフォルト・パスワードは QCONSOLE) に設定されています。LAN 接続のオペレーション・コンソールは、接続が正常に行われるたびに、パスワードを変更します。詳しくは、80 ページの『オペレーション・コンソールのセットアップ・ウィザードの使用』を参照してください。

iSeries LAN 接続のオペレーション・コンソールの追加情報については、Information Center のトピック『LAN 接続のオペレーション・コンソールの構成』を参照してください。

LAN 接続のオペレーション・コンソールの保護

LAN 接続のオペレーション・コンソールを使用する場合には、以下のことをお勧めします。

- コンソール属性を持つ別の保守ツール装置プロファイルを作成し、プロファイル情報を安全な場所に保管する。
- iSeries サーバーに Cryptographic Access Provider (5722-AC2 または 5722-AC3) を導入し、オペレーション・コンソール PC に Client Encryption (5722-CE2 または 5722-CE3) を導入する。
- 保守装置情報パスワードには、平凡でないものを選ぶ。
- オペレーション・コンソール PC は、平衡型コンソールまたは直接接続されているオペレーション・コンソールと同様の方法で保護する。

オペレーション・コンソールのセットアップ・ウィザードの使用

セットアップ・ウィザードは、LAN 接続のオペレーション・コンソールを使用する場合に、PC に必要な情報を追加します。セットアップ・ウィザードは、保守ツール装置プロファイル、保守ツール装置プロファイル・パスワード、および保守ツール装置プロファイル情報を保護するためのパスワードを必要とします。

注: 保守ツール装置プロファイル情報パスワードは、PC の保守ツール装置プロファイル情報 (保守ツール装置プロファイルおよびパスワード) をロックおよびアンロックするために使用されます。

ネットワーク接続を確立する際に、オペレーション・コンソールのセットアップ・ウィザードは、暗号化された保守ツール装置プロファイルおよびパスワードにアクセスするための保守装置情報パスワードを要求します。また、有効な保守ツール・ユーザー識別およびパスワードも要求します。

第 9 章 不審なプログラムの検出

最近のコンピューター使用の傾向として、信頼の置けないソースからのプログラムや、不明な機能を実行するプログラムがシステムに含まれるようなケースが増えてきています。次に、いくつかの例を示します。

- パーソナル・コンピューターのユーザーが、他の PC ユーザーからプログラムを入手することがあります。この PC が iSeries システムに接続されている場合は、そのプログラムが iSeries サーバーに影響を与える可能性があります。
- ネットワークに接続されたユーザーも、たとえば、電子掲示板からプログラムを入手することができます。
- ハッカーが、ますます活動的になり注目を集めるようになってきています。ハッカーは、しばしば、自分たちの方式とその結果を公開します。このため、普段は良心的なプログラマーでもこれを模倣する可能性があります。

このような傾向により、**コンピューター・ウィルス**と呼ばれるコンピューター・セキュリティー上の問題が生じました。ウィルスとは、ウィルス自体のコピーを含むように他のプログラムを変更することができるプログラムをいいます。このため、他のプログラムはウィルスに感染したと言われます。さらにウィルスは、システム資源を消費したり、データを破壊したりするような他の操作も行うことがあります。

iSeries サーバーのアーキテクチャーは、コンピューター・ウィルスの感染特性に対し、ある程度の保護策を備えています。『コンピューター・ウィルスに対する保護』では、このことについて説明します。 iSeries サーバーの機密保護管理者は、無許可機能を実行するプログラムについてより深い関心を持つ必要があります。この章の他のトピックとしては、悪意を持った人物がどのようにして有害プログラムをセットアップして、システムでそれを実行するかについて説明します。このトピックでは、プログラムが無許可機能を実行しないようにするためのヒントを示しています。

セキュリティーのヒント

オブジェクト権限は、常に、第 1 防護線です。オブジェクトを保護するための適切な計画を行っていないと、システムは無防備になります。この章では、許可ユーザーがどのようにして、オブジェクト権限体系の中の抜け穴を利用しようとするかについて説明します。

コンピューター・ウィルスに対する保護

ウィルスに感染したコンピューターは、他のプログラムを変更できるプログラムを含んでいます。 iSeries のオブジェクト・ベースのアーキテクチャーは、他のコンピューター・アーキテクチャーの場合と比べ、攻撃を企てる者がこのようなウィルスを生成したり、まん延させたりするのをより困難にしています。 iSeries サーバーでは、特定のコマンドや命令を使用して各タイプのオブジェクトを処理します。ファ

イル命令を使用して、操作可能プログラム・オブジェクトを変更することはできません (多くのウィルス作成者たちがファイル命令を使用して変更を行います)。また、他のプログラム・オブジェクトを変更するプログラムも簡単には作成できません。これを行うには、多くの時間や人手、熟練が必要であり、また、一般には入手できないツールや文書にアクセスする必要があります。

しかし、iSeries サーバーの新しい機能がオープン・システム環境で使用できるようになるにつれて、iSeries サーバーのオブジェクト・ベースの保護機能のいくつかが適用されなくなりました。例えば、統合ファイル・システム (IFS) の場合、ユーザーはディレクトリーの中のいくつかのオブジェクト (ストリーム・ファイルなど) を直接処理することができます。

また、iSeries サーバーのアーキテクチャーにより、ウィルスが iSeries サーバーのプログラム間でまん延するのは難しくなりますが、このアーキテクチャーは、iSeries サーバーがウィルス保持者になるのを防ぐわけではありません。ファイル・サーバーとしての iSeries サーバーは、多くの PC ユーザーが共用するプログラムを格納することができます。これらのプログラムのいずれにも、iSeries サーバーが検出しないウィルスが入っている可能性があります。このタイプのウィルスが、iSeries サーバーに接続されている PC に感染しないようにするには、 PC ウィルス・スキャン・ソフトウェアを使用する必要があります。

iSeries サーバーには、ポインター機能を持つ低水準言語を使用して操作可能オブジェクト・プログラムを変更できないようにするいくつかの機能が用意されています。

- セキュリティー・レベル 40 以上でシステムが稼働しているときは、保全性保護はプログラム・オブジェクトを変更できないようにする保護機能に含まれます。たとえば、ブロックされた (保護された) 機械語命令を含むプログラムを正常に実行することはできません。
- 別のシステムに保管された (および、変更された可能性のある) プログラムを復元するときにも、プログラム妥当性検査値がユーザーを保護する目的で使用されます。「*iSeries 機密保護解説書*」の第 2 章では、プログラム妥当性検査値を始め、セキュリティー 40 以上の場合の保全性保護機能について説明しています。

  注: プログラム妥当性検査値は絶対確実なものではなく、またシステムに復元されたプログラムを評価する際に不寝番を代行してくれるものでもありません。

以下のいくつかのツールも、更新されたプログラムがシステムに導入されるのを検出する際の助けになります。

- オブジェクト保全性検査 (CHKOBJITG) コマンドを使用すれば、検索値を満足するオブジェクト (操作可能オブジェクト) をスキャンして、それらのオブジェクトが更新されていないことを確認することができます。これはウィルス・スキャン機能と同じようなものです。
- セキュリティー監査機能を使用すれば、変更または復元されたプログラムをモニターすることができます。 権限レベル・システム値としての *PGMFAIL、*SAVRST、および *SECURITY 値は、監査レコードを提供します。監査レコードは、ウィルス・タイプのプログラムがシステムに導入されることを検出する際に役立ちます。「*iSeries 機密保護解説書*」の第 9 章と付録 F では、監査値と監査ジャーナル項目が詳しく説明されています。

- プログラム変更 (CHGPGM) コマンドの強制作成 (FRCCRT) パラメーターを使用すれば、システムに復元された任意のプログラムを再作成することができます。プログラムの再作成には、プログラム・テンプレートが使用されます。 プログラム・オブジェクトがコンパイルされた後に変更された場合は、システムは変更されたオブジェクトを再作成し、それを置き換えます。ブロックされた (保護されている) 命令がプログラム・テンプレートに含まれていると、プログラムは正しく再作成されません。
- プログラムをシステムに復元したときに再作成するには、QFRCCVNRST (復元時に強制変換) システム値を使用します。システムは、プログラムの再作成にプログラム・テンプレートを使用します。このシステム値は、再作成するプログラムについて複数の選択肢を提供します。
- QVFYOBJRST (オブジェクト復元検査) システム値を使用して、ディジタル署名を持っていないか、あるいはディジタル署名が無効なプログラムを復元しないようにすることができます。ディジタル署名が無効な場合とは、プログラムが、開発者によって署名された後に変更されていることを意味します。所有するプログラム、保管ファイルおよびストリーム・ファイルに署名することができる API があります。

署名について、および署名を使用してシステムを保護する方法について詳しくは、94 ページの『オブジェクト署名』を参照してください。

借用権限の使用のモニター

iSeries サーバーでは、プログラム所有者の権限を借用するプログラムを作成することができます。つまり、プログラムを実行するすべてのユーザーは、プログラムを所有するユーザー・プロファイルと同じ権限 (私用権限および特殊権限) を持っています。

借用権限は、正しく使用すると、貴重なセキュリティー・ツールになります。たとえば、51 ページの『オブジェクト・セキュリティーによるメニュー・アクセス制御の拡張』では、借用権限とメニューをどのように組み合わせれば、メニュー・アクセス制御を超えて拡張する場合に役立つかが説明されています。借用権限を使用すれば、重要なファイルが承認済みアプリケーション・プログラムの外側で変更されないように保護しながら、引き続きそれらのファイルに対して QUERY を許可することができます。

機密保護管理者としては、以下のようにして、借用権限が正しく使用されるようにすることが必要です。

- プログラムは、過剰な権限を借用するのではなく、必要な機能を実行するのに十分な権限のみを持つユーザー・プロファイルの権限を借用しなければなりません。 *ALLOBJ 特殊権限を持っているか、または重要なオブジェクトを所有するユーザー・プロファイルの権限を借用するプログラムについては、特に注意する必要があります。
- 権限を借用するプログラムは、特定の限定機能を持っていなければならず、コマンド入力機能を提供すべきではありません。
- 権限を借用するプログラムは、正しく保護される必要があります。
- 借用権限を過度に使用すると、システム・パフォーマンスに負のインパクトを与えることがあります。パフォーマンス上の問題を回避するためには、権限検査フ

ローチャートを見直すほか、「*iSeries 機密保護解説書*」の第 5 章に示されている借用権限に関する推奨事項を見直してください。

SECBATCH メニュー・オプション:
1 *は即時に投入する、* **40 はジョブ・スケジューラーを使用する**

借用オブジェクト印刷 (PRTADPOBJ) コマンド (SECTOOLS メニューのオプション 21) を使用して、システムにおける借用権限の使用のモニターを援助することができます。

報告書には、指定されたユーザー・プロファイルの特殊権限、ユーザー・プロファイルの権限を借用しているプログラム、およびプロファイルの権限を使用している ASP 装置が表示されます。情報の基礎を確立したら、変更バージョンの借用オブジェクト報告書を定期的に印刷することができます。この報告書には、権限を借用する新規プログラムと、この報告書を最後に実行してから、権限を借用するために変更されたプログラムがリストされます。

借用権限がシステムで誤用されている疑いがある場合は、QAUDLVL システム値を設定して *PGMADP を組み込むことができます。 この値が活動状態になっていると、誰かが権限を借用するプログラムを開始または借用するたびに、システムは監査ジャーナル項目を作成します。この項目には、このプログラムを開始したユーザーの名前とこのプログラムの名前が含まれています。

借用権限の使用の制限

iSeries プログラムを実行すると、このプログラムは借用権限を使用して、次のような 2 つの異なる方法でオブジェクトにアクセスすることができます。

- このプログラム自体がその所有者の権限を借用することができます。この指定は、このプログラムまたはサービス・プログラムのユーザー・プロファイル (USRPRF) パラメーターで行います。
- このプログラムは、まだジョブの呼び出しスタックに入っている前のプログラムの借用権限を使用 (継承) します。プログラムは、それ自体が権限を借用しなくても、前のプログラムの借用権限を継承することができます。プログラムまたはサービス・プログラムの借用権限使用 (USEADPAUT) パラメーターは、そのプログラムがプログラム・スタック内の前のプログラムの借用権限を継承するかどうかを制御します。

次に、前のプログラムの借用権限を使用した場合の効果について例を示します。

ICOWNER ユーザー・プロファイルが ITEM ファイルに対して *CHANGE 権限を持っていて、 ITEM ファイルに対する共通権限が *USE であると仮定します。他のユーザー・プロファイルは、 ITEM ファイルに対して明示的に定義された権限を持っていません。 85 ページの表 14 は、 ITEM ファイルを使用する 3 つのプログラムの属性を示しています。

表 14. 借用権限の使用 (USEADPAUT) の例

プログラム名	プログラム所有者	USRPRF 値	USEADPAUT 値
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

例 1 - 権限の借用:
1. USERA が PGMA プログラムを実行します。
2. PGMA プログラムが更新機能を使用して ITEM ファイルをオープンしようとします。

結果: この試行は成功します。PGMA が ICOWNER の権限を借用するので、USERA は ITEM ファイルへの *CHANGE アクセスを入手します。

例 2 - 借用権限の使用:
1. USERA が PGMA プログラムを実行します。
2. PGMA プログラムが PGMB プログラムを呼び出します。
3. PGMB プログラムが更新機能を使用して ITEM ファイルをオープンしようとします。

結果: この試行は成功します。 PGMB プログラムは権限を借用しませんが (*USRPRF が *USER)、前に借用した権限の使用を許可されています (*USEADPAUT が *YES)。 PGMA プログラムはまだプログラム・スタックに入っています。したがって、 PGMA が ICOWNER の権限を借用するので、 USERA は ITEM ファイルへの *CHANGE アクセスを入手します。

例 3 - 借用権限の不使用
1. USERA が PGMA プログラムを実行します。
2. PGMA プログラムが PGMC プログラムを呼び出します。
3. PGMC プログラムが更新機能を使用して ITEM ファイルをオープンしようとします。

結果: 権限障害が発生します。PGMC プログラムは権限を借用しません。 PGMC プログラムはまた、前のプログラムからの借用権限の使用を許可されていません。PGMA はまだ呼び出しスタックに入っていますが、その借用権限は使用されません。

新規プログラムによる借用権限の使用の防止

後でスタックに入れられるプログラムに借用権限を渡すと、知識のあるプログラマーは、トロイの木馬プログラムを作成する機会を得ます。トロイの木馬プログラムは、スタックに入っている前のプログラムを利用して、危害を加えるために必要な権限を入手します。これを防止するために、前のプログラムの借用権限を使用するプログラムの作成を許可するユーザーを限定することができます。

新規のプログラムを作成すると、システムは自動的に USEADPAUT パラメーターを *YES に設定します。プログラムに借用権限を継承させたくない場合は、プログラム変更 (CHGPGM) コマンドまたは保守プログラム変更 (CHGSRVPGM) コマンドを使用して USEADPAUT パラメーターを *NO に設定しなければなりません。

権限リストおよび借用権限使用 (QUSEADPAUT) システム値を使用して、借用権限を継承するプログラムを作成できるユーザーを制御することができます。権限リスト名を QUSEADPAUT システム値に指定すると、システムはこの権限リストを使用して、新規プログラムの作成方法を決定します。

ユーザーがプログラムまたは保守プログラムを作成すると、システムは、権限リストに対するユーザーの権限を検査します。ユーザーが *USE 権限を持っていれば、新規プログラムの USEADPAUT パラメーターが *YES に設定されます。ユーザーが *USE 権限を持っていなければ、 USEADPAUT パラメーターが *NO に設定されます。権限リストに対するユーザーの権限は、借用権限からは生じません。

QUSEADPAUT システム値に指定した権限リストは、ユーザーが CHGxxx コマンドを使用して、プログラムまたは保守プログラムに対する USEADPAUT を設定できるかどうかを制御することもできます。

注:

1. 権限リスト QUESADPAUT を呼び出す必要はありません。別の名前で権限リストを作成することができます。次に、QUSEADPAUT システム値にその権限リストを指定してください。この例のコマンドでは、権限リストの名前を取り替えます。
2. QUSEADPAUT システム値は、システム上の既存プログラムに影響を与えることはありません。CGHPGM コマンドまたは CHGSRVPGM コマンドを使用して、既存のプログラムに USEADPAUT パラメーターを設定してください。

より制限のきつい環境: 大部分のユーザーが USEADPAUT パラメーターを *NO に設定して新規プログラムを作成するようにしたい場合は、次のようにします。

1. 権限リストの共通権限を *EXCLUDE に設定するために、次のように入力します。

```
CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC)
   AUT(*EXCLUDE)
```

2. 前のプログラムの借用権限を使用するプログラムを作成できるように、特定のユーザーをセットアップしたい場合は、次のように入力します。

```
ADDAUTLE AUTL(QUSEADPAUT) USER(user-name)
   AUT(*USE)
```

より制限の緩い環境: 大部分のユーザーが USEADPAUT パラメーターを *YES に設定して新規プログラムを作成するようにしたい場合は、次のようにします。

1. 権限リストの共通権限を *USE に設定しておきます。
2. 特定のユーザーが前のプログラムの借用権限を使用するプログラムを作成できないようにしたい場合は、次のように入力します。

```
ADDAUTLE AUTL(QUSEADPAUT)
   USER(user-name) AUT(*EXCLUDE)
```

トリガー・プログラムの使用のモニター

DB2® UDB は、トリガー・プログラムをデータベース・ファイルに関連付ける機能を備えています。トリガー・プログラム機能は、この業界では高機能データベース・マネージャーとしてよく使用される機能です。

トリガー・プログラムをデータベース・ファイルに関連付けるときに、トリガー・プログラムをいつ実行するかを指定します。たとえば、新規レコードがファイルに追加されるつど、トリガー・プログラムを実行するように顧客オーダー・ファイルをセットアップすることができます。顧客の未払い残高が信用限度を超えた場合に、トリガー・プログラムは顧客あての警告文を印刷し、メッセージを信用管理者に送信することができます。

トリガー・プログラムは、アプリケーション機能を提供するためにも、情報を管理するためにも生産的な方法になります。トリガー・プログラムは、悪意を持つ人間がシステム上に『トロイの木馬』を作成できるようにもします。破壊的なプログラムが、システムのデータベース・ファイルで特定のイベントが発生したときに実行されるのを座して待っていることもあります。

注: 歴史の上では、トロイの木馬は、ギリシャの兵士たちがこもった、中が空洞になった木製の馬のことです。木馬がトロイの城壁内に入ると、兵士たちは木馬から出てトロイ人と闘いました。コンピューターの世界では、破壊的な機能を隠したプログラムが、しばしばトロイの木馬と呼ばれます。

SECBATCH メニュー・オプション:

27 *は即時に投入する、* **66** *はジョブ・スケジューラーを使用する*

システムが出荷されるときは、トリガー・プログラムをデータベース・ファイルに追加する機能は制限されています。オブジェクト権限を注意深く管理する場合は、一般のユーザーは、トリガー・プログラムをデータベース・ファイルに追加するための十分な権限を持つ必要はないはずです。 (「*iSeries 機密保護解説書*」の付録 D には、必要な権限と、物理ファイル・トリガー追加 (ADDPFTRG) コマンドを始めとするすべてのコマンドが示されています。)

トリガー・プログラム印刷 (PRTTRGPGM) コマンドを使用して、特定のライブラリーまたはすべてのライブラリーのすべてのトリガー・プログラムのリストを印刷することができます。

初期報告書を基本として使用して、すでにシステムに存在しているすべてのトリガー・プログラム評価することができます。次に、変更報告書を定期的に印刷して、新規のトリガー・プログラムがシステムに追加されたかどうかを調べることができます。

トリガー・プログラムを評価するときは、以下のことを考慮してください。

- 誰がトリガー・プログラムを作成したか。これを判別するには、オブジェクト記述表示 (DSPOBJD) コマンドを使用します。
- プログラムは何を実行するのか。これを判別するには、ソース・プログラムを調べるか、プログラム作成者に尋ねる必要があります。たとえば、トリガー・プログラムは、誰がユーザーであるかを確認しますか。おそらく、トリガー・プログラムは、システム資源にアクセスするために特定のユーザー (QSECOFR) を待っています。

情報の基礎を確立したら、変更報告書を定期的に印刷して、システムに追加された新規のトリガー・プログラムをモニターすることができます。

隠れたプログラムの検査

トリガー・プログラムだけが、トロイの木馬をシステムにとり込む方法ではありません。トリガー・プログラムは、**出口プログラム**の一例です。あるイベント、たとえば、トリガー・プログラムの場合のファイル更新が行われると、システムは、そのイベントに関連する出口プログラムを実行します。

表 15 は、システムに置くことができる、その他の出口プログラムの例を示しています。これらの出口プログラムの使用と内容を評価する際には、トリガー・プログラムで使用する方法と同じ方法を使用しなければなりません。

注: 表 15 は、可能なすべての出口プログラムを示しているわけではありません。

表 15. システム提供の出口プログラム

プログラム名	プログラムを実行する時
DDMACC ネットワーク属性のユーザー指定名。	ユーザーがシステムの DDM ファイルをオープンしようとする時、または DRDA 接続を行う時。
PCSACC ネットワーク属性のユーザー指定名。	ユーザーが、オリジナル・クライアントを使用するクライアント・アクセス™機能を使用して、システムのオブジェクトにアクセスしようとする時。
QPWDVLDPGM システム値のユーザー指定名。	ユーザーがパスワード変更機能を実行する時。
QRMTSIGN システム値のユーザー指定名。	ユーザーがリモート・システムから対話式にサインオンしようとする時。
QSYS/QEZUSRCLNP	自動クリーンアップ機能を実行する時。
CHGBCKUP コマンドの EXITPGM パラメーターのユーザー指定名。	操作援助バックアップ機能を使用する時。
CRTPRDLOD コマンドのユーザー指定名。	このコマンドで作成されたプロダクトの保管、復元、または削除を行う前と後。
CHGMSGD コマンドの DFTPGM パラメーターのユーザー指定名。	メッセージについてデフォルト・プログラムを指定した場合は、メッセージが出されたときにシステムがプログラムを実行します。一般のシステムの場合は、メッセージ記述が多過ぎて、デフォルト・プログラムをモニターするのが難しくなります。共通ユーザーがメッセージのためのデフォルト・プログラムを追加できないようにするために、メッセージ・ファイル (*MSGF オブジェクト) の共通権限を *USE に設定することを考えてください。
STREML3270 コマンドの FKEYPGM パラメーターのユーザー指定名。	ユーザーが 3270 装置エミュレーション・セッション時に機能キーを押した時。出口プログラムが終了すると、システムは 3270 装置エミュレーション・セッションに制御を戻します。
パフォーマンス・モニター・コマンドの EXITPGM パラメーターのユーザー指定名。	STRPFRMON、ENDPFRMON、ADDPFRCOL、および CHGPFRCOL コマンドによって収集されたデータを処理するため。データ収集が終了すると、プログラムが実行されます。
RCVJRNE コマンドの EXITPGM パラメーターのユーザー指定名。	指定されたジャーナルおよびジャーナル・レシーバーから読み取られた各ジャーナル項目またはジャーナル項目のグループごとに。
QTNADDCR API のユーザー指定名。	COMMIT または ROLLBACK 操作時。
QHFRGFS API のユーザー指定名。	ファイル・システム機能を実行するため。
印刷装置記述の SEPPGM パラメーターのユーザー指定名。	スプール・ファイルまたは印刷ジョブの前か後で分離ページに何を印刷するかを決定するため。

表 15. システム提供の出口プログラム (続き)

プログラム名	プログラムを実行する時
QGPL/QUSCLSXT	ファイル使用情報を取り込めるようにするためにデータベース・ファイルをクローズするとき。
論理ファイルの FMTSLR パラメーターのユーザー指定名。	レコードがデータベース・ファイルに書き込まれたが、レコード様式名が高水準言語プログラムに組み込まれていないとき。セレクター・プログラムは、このレコードを入力として受け取り、使用されている様式を判別して、それをデータベースに戻します。
QATNPGM システム値、ユーザー・プロファイルの ATNPGM パラメーター、または SETATNPGM ユーザー・プロファイルの PGM パラメーターに指定されたユーザー指定名。	ユーザーがアテンション・キーを押したとき。
TRCJOB コマンドの EXITPGM パラメーターのユーザー指定名。	トレース・ジョブ・プロシージャーを開始する前。

出口プログラムを指定するためのコマンドについては、コマンドのデフォルト設定が出口プログラムを指定するように変更されていないことを確認する必要があります。また、これらのコマンドの共通権限が、コマンドのデフォルト設定を変更するのに十分でないことも確認する必要があります。 CHGCMDDFT コマンドには、コマンドに対する *OBJMGT 権限が必要です。コマンドを実行するためには、*OBJMGT 権限は必要ありません。

登録済み出口プログラムの評価

システム登録機能を使用すれば、特定のイベントが発生したときに実行する必要のある出口プログラムを登録することができます。システムの登録情報をリストするには、WRKREGINF OUTPUT(*PRINT) を入力します。 図 8 は、この報告書の例を示しています。

```
                          登録情報の処理
5722SS1 VXRXMX  000000
 出口点 . . . . . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
 出口点形式 . . . . . . . . . . . . . . :   NJE0100
 登録済み出口点 . . . . . . . . . . . . :   *YES
 登録取消し可能 . . . . . . . . . . . . :   *YES
 出口プログラムの最大数 . . . . . . . . :   *NOMAX
 出口プログラムの現在数 . . . . . . . . :   0
 追加の前処理 . . . . . . . . . . . . . :   *NONE
   ライブラリー . . . . . . . . . . . . :
   様式 . . . . . . . . . . . . . . . . :
 除去の前処理 . . . . . . . . . . . . . :   *NONE
   ライブラリー . . . . . . . . . . . . :
   様式 . . . . . . . . . . . . . . . . :
 検索の前処理 . . . . . . . . . . . . . :   *NONE
   ライブラリー . . . . . . . . . . . . :
```

図 8. 登録情報処理 - 例

システムの各出口点ごとに、報告書は現在登録されている出口プログラムがあるかを示します。現在登録されているプログラムが出口点に含まれている場合は、

WRKREGINF の表示バージョンでオプション 5 (出口点の表示) を選択して、プログラムに関する情報を表示することができます。

```
                              登録情報の処理

オプションを入力して，実行キーを押してください。
  5= 出口点の表示    8= 出口プログラムの処理

                                出口点
OPT   出口点                    の形式     登録済み     テキスト
     QIBM_QGW_NJEOUTBOUND     NJE00100     *YES       ネットワーク・ジョブ項目の
5    QIBM_QHQ_DTAQ            DTAQ0100     *YES       元のデータ待ち行列サーバー
     QIBM_QLZP_LICENSE        LICM0100     *YES       元のライセンス管理サーバー
     QIBM_QMF_MESSAGE         MESS0100     *YES       元のメッセージ・サーバー
     QIBM_QNPS_ENTRY          ENTR0100     *YES       ネットワーク印刷サーバー－項目
     QIBM_QNPS_SPLF           SPLF0100     *YES       ネットワーク印刷サーバー－スプール
     QIBM_QNS_CRADDACT        ADDA0100     *YES       CRQ 記述の追加活動
     QIBM_QNS_CRCHGACT        CHGA0100     *YES       CRQ 記述の変更活動
```

他の出口プログラムやトリガー・プログラムに使用するこれらの出口プログラムの評価には、同じ方式を使用してください。

スケジュールされたプログラムの検査

iSeries では、ジョブ・スケジューラーのような、後で実行するジョブをスケジュールするための方法がいくつか用意されています。通常、これらの方式にはセキュリティーに関する問題はありません。なぜならば、ジョブをスケジュールするユーザーは、ジョブのバッチ処理を投入するために必要な権限を持っていなければならないからです。

ただし、スケジュールされたジョブについては定期的に検査する必要があります。部門から転出した、不満をいだくユーザーが、この方式を使用して障害を起こす可能性があります。

保管機能と復元機能の制限

大部分のユーザーは、システム上のオブジェクトを保管したり復元したりする必要はありません。保管コマンドを使用すれば、部門の重要な資産をメディアや別のシステムにコピーすることができます。ほとんどの保管コマンドは、メディアや保管・復元装置にアクセスしないで別のシステムに送信できる (SNDNETF ファイル・コマンドを使用して) 保管ファイルをサポートします。

復元コマンドを使用すれば、プログラム、コマンド、ファイルなど、無許可のオブジェクトをシステムに復元できるようになります。保管ファイルを使用することで、メディアや保管・復元装置にアクセスしないで情報を復元することもできます。 SNDNETF コマンドを使用したり、FTP 機能を使用することで、保管ファイルを別のシステムから送信することができます。

次に、システムでの保管操作や復元操作を制限する上での推奨事項を示します。

- *SAVSYS 特殊権限を持つユーザーを制御します。*SAVSYS 特殊権限を使用すれば、ユーザーはオブジェクトに対する必須権限を持たなくても、オブジェクトの保管や復元を行うことができます。
- 装置を保管および復元するための物理アクセスを制御します。

- 保管コマンドや復元コマンドへのアクセスを制限します。OS/400 ライセンス・プログラムを導入すると、 RSTxxx コマンドの共通権限は *EXCLUDE になります。 SAVxxx コマンドの共通権限は *USE です。 SAVxxx コマンドの共通権限を *EXCLUDE に変更することを考えてください。 RSTxxx コマンドの使用を許可するユーザーを注意して制限してください。
- QALWOBJRST システム値を使用して、システム状態プログラム、権限を借用するプログラムの復元、および妥当性検査エラーになったオブジェクトの復元を制限します。
- QVFYOBJRST システム値を使用して、システムにおける署名オブジェクトの復元を制御します。
- QFRCCVNRST システム値を使用して、システムに復元する特定のオブジェクトの再作成を制御します。
- セキュリティー監査機能を使用して復元操作をモニターします。 *SAVRST を QAUDLVL システム値に組み込み、復元操作で作成された監査レコードを定期的に印刷します。 (「*iSeries 機密保護解説書*」の第 9 章と付録 F では、監査項目操作が詳しく説明されています。)

保護ライブラリー内のユーザー・オブジェクトの検査

すべての iSeries サーバーのジョブはライブラリー・リストを持っています。ライブラリー・リストは、ライブラリー名がオブジェクト名と一緒に指定されていない場合に、システムがオブジェクトを探索する順序を決定します。たとえば、プログラムの所在を指定しないでそのプログラムを呼び出すと、システムは、順番にライブラリー・リストを探し、最初に見つけたプログラムのコピーを実行します。

「*iSeries 機密保護解説書*」では、ライブラリー・リストの機密漏れの問題、およびライブラリー名を指定しないでプログラムを呼び出す (**未修飾呼び出し**と呼ばれる) ことについて詳しく説明しています。この資料には、ライブラリー・リストの内容や、システム・ライブラリー・リストの変更機能の制御に関する推奨事項も示されています。

システムを正しく実行するには、 QSYS や QGPL など、特定のシステム・ライブラリーが、すべてのジョブに関するライブラリー・リストに入っていなければなりません。オブジェクト権限を使用すれば、誰がプログラムをこれらのライブラリーに追加できるかを制御することができます。これを行えば、ライブラリー・リストの後方にあるライブラリーに置かれたプログラムと同じ名前を持つ有害なプログラムを誰かが置くことを防止するのに役立ちます。

また、誰が CHGSYSLIBL コマンドに対する権限を持っているかを評価し、セキュリティー監査ジャーナルの SV レコードをモニターすることもできます。悪賢いユーザーは、ライブラリーをライブラリー・リストの QSYS の前に入れ、 IBM 提供のコマンドと同じ名前を持つ無許可コマンドを他のユーザーに実行させたりします。

SECBATCH メニュー・オプション:

28 *は即時に投入する、***67** *はジョブ・スケジューラーを使用する*

ユーザー・オブジェクト印刷 (PRTUSROBJ) コマンドを使用して、指定されたライブラリーに入っているユーザー・オブジェクト (IBM によって作成されていないオブジェクト) のリストを印刷することができます。 次に、リストのプログラムを評価して、誰がそれを作成したか、それはどのような機能を実行するかを判別することができます。

プログラム以外のユーザー・オブジェクトも、システム・ライブラリーに入っているときは、機密漏れの問題を提示することがあります。たとえば、プログラムが、未修飾の名前を持つファイルに機密データを書き込んだ場合は、そのプログラムは、システム・ライブラリー内のそのファイルの間違ったバージョンをオープンさせられることがあります。

第 10 章 攻撃の防止と検出

この章では、発生する可能性のあるセキュリティー上の問題や攻撃を企てる者を検出するときに役立つ、いろいろなヒントを示しています。

物理的セキュリティー

システム装置は、重要なビジネス資産であり、システムへの入り口となっています。システム内のシステム構成要素の中には、小型で重要なものがあります。システム装置を制御された場所に設置して、他の人物が重要なシステム構成要素を除去できないようにする必要があります。

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

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

こうした活動はすべて、システム・ユーザーを混乱させる可能性があります。また、システムのセキュリティーを危険にさらす可能性もあります。システムに装備されているキーロックを使用すれば、こうした活動がいつ使用できるかを制御することができます。制御盤を使用できないようにするには、「セキュリティー」の位置にキーロックをして、キーを取り外して安全な場所に保管してください。

注:

1. システム上でリモート IPL を実行するかまたはリモート診断を実行する必要がある場合には、キーロックに別の設定値を選択する必要がある場合があります。iSeries Information Center の『Getting Started』のトピックに、キーロック設定に関する詳しい情報が記載されています (詳細は、 xii ページの『前提条件および関連情報』を参照してください)。
2. すべてのシステム・モデルにキーロックが標準機構として装備されているわけではありません。

ユーザー・プロファイルのアクティビティーのモニター

ユーザー・プロファイルは、システムへの入り口点を備えています。ユーザー・プロファイルのパラメーターは、ユーザーの環境とユーザーのセキュリティー特性を決定します。機密保護管理者は、システム上のユーザー・プロファイルに対して行われた変更を制御し監査する必要があります。

システムがユーザー・プロファイルに対する変更のレコードを書き込むように、セキュリティー監査をセットアップすることができます。 DSPAUDJRNE コマンドを使用してこれらの変更を印刷することができます。

出口プログラムを作成して、ユーザー・プロファイルに対する要求されたアクションを評価することができます。表 16 は、ユーザー・プロファイル・コマンドで使用できる出口点を示しています。

表 16. ユーザー・プロファイルのアクティビティーの出口点

ユーザー・プロファイル・コマンド	出口点名
ユーザー・プロファイル作成 (CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
ユーザー・プロファイル変更 (CHGUSRPRF)	QIBM_QSY_CHG_PROFILE
ユーザー・プロファイル削除 (DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
ユーザー・プロファイル復元 (RSTUSRPRF)	QIBM_QSY_RST_PROFILE

たとえば、出口プログラムは、ユーザーに無許可バージョンのプログラムを実行させるような変更を探し出すことができます。このような変更は、異なるジョブ記述や新規の現行ライブラリーを割り当てる可能性があります。出口プログラムは、受け取った情報に基づいて、メッセージ待ち行列を通知したり、何らかの処置 (ユーザー・プロファイルの変更や使用禁止のような) を行ったりする可能性があります。

「*iSeries 機密保護解説書*」では、ユーザー・プロファイル処置のための出口プログラムについて詳しく説明しています。

オブジェクト署名

セキュリティー予防措置をとっても、誰かが攻撃したデータをシステムに介入させることによってその予防措置をバイパスしたら、意味がありません。 iSeries サーバーには、攻撃されたソフトウェアをシステムにロードしないようにする、あるいはそのようなソフトウェアがすでにある場合にはそれを検出するために使用できる組み込み (標準装備の) 機能が数多くあります。V5R1 で追加された技法の 1 つに、オブジェクト署名があります。

オブジェクト署名は、「ディジタル署名」として知られている暗号化概念を iSeries サーバーにインプリメントしたものです。この考えは、比較的簡単です。ソフトウェア作成者がソフトウェアをお客様に出荷する用意が整ったら、作成者はソフトウェアに「署名」します。この署名は、ソフトウェアがある特定の機能を行うことを保証するものではありません。しかし、ソフトウェアの出荷元は署名した作成者であること、およびソフトウェアが作成され署名されてから変更されていないことを証明するための手立てとなります。これは、ソフトウェアがインターネットを介して送信される場合、またはソフトウェアが変更された可能性があると思われるメディアに保管されている場合に、特に重要になります。

ディジタル署名を使用することにより、ソフトウェアのシステムへのロードに対する制御がより効果的に行え、ロードされてからのソフトウェアの変更を検出する際にも役立ちます。新しいシステム値であるオブジェクト復元検査 (QVFYOBJRST) は、システムにロードされるすべてのソフトウェアに識別可能なソフトウェアのソースによる署名を要求する、制限的なポリシーを設定するためのメカニズムを提供します。よりオープンなポリシーを選択し、署名されている場合は、単にその署名を検査することもできます。

すべての OS/400 ソフトウェアとそのオプションのソフトウェアおよび iSeries サーバー・ライセンス・プログラムは、システムで承認されたソースによって署名されています。これらの署名は、システムによる保全性の保護に役立ち、修正適用時に検査されて、修正がシステムで承認されたソースによるものであること、および転送中に変更されていないことが確認されます。これらの署名は、ソフトウェアがシステムにロードされる際にも検査されます。CHKOBJITG (オブジェクト保全性検査) コマンドが、システム上のオブジェクトの他の保全性機能のほかに、署名も検査するように拡張されました。また、ディジタル証明書マネージャーにも、オペレーティング・システム内のオブジェクトを含む、オブジェクトの署名を検査するためのパネルがあります。

オペレーティング・システムが署名されているように、ディジタル署名を使用して、ビジネスに不可欠なソフトウェアの保全性を保護することができます。ユーザーは、ソフトウェア・プロバイダーによって署名されたソフトウェアを購入することもできますし、または作成したソフトウェアに署名することもできます。そして、定期的に CHKOBJITG またはディジタル証明書マネージャーを使用して、そのソフトウェアの署名がまだ有効であるか、つまり、オブジェクトが署名されてから変更されていないか検査することをセキュリティー・ポリシーに含めることができます。さらに、システムに復元するすべてのソフトウェアが、ユーザーまたはユーザーが識別可能なソースにより署名されていることが必要になる場合もあります。しかし、IBM 以外によって作成されているほとんどの iSeries サーバー・ソフトウェアは現在署名されていないので、システムによってはこの方法が制限されることもあります。新しいディジタル署名のサポートにより、ソフトウェアの保全性を保護するために最善の方法を柔軟に決定することができます。

ソフトウェアを保護するディジタル署名は、ディジタル証明書の使用方法の一例です。ディジタル証明書の管理に関する追加情報は、Information Center の『ディジタル証明書の管理』にあります (詳細は、xii ページの『前提条件および関連情報』を参照してください)。

サブシステム記述のモニター

iSeries サーバーでサブシステムを開始すると、システムは、作業をシステムに入れて実行するための環境を作成します。サブシステム記述は、この環境の体裁を定義します。したがって、サブシステム記述は、悪意を持ったユーザーに機会を提供する可能性があります。攻撃を企てる人間は、サブシステム記述を使用して自動的にプログラムを開始したり、ユーザー・プロファイルなしでサインオンしたりできます。

共通権限取り消し (RVKPUBAUT) コマンドを実行すると、システムは、サブシステム記述に対する共通権限を *EXCLUDE に設定します。こうすることで、明確に許可されていない (かつ *ALLOBJ 特殊権限を持っていない) ユーザーが、サブシステム記述を変更したり作成したりできないようにすることができます。

次に、現在システムにあるサブシステム記述を検討するためのいくつかの推奨事項を示します。サブシステム記述処理 (WRKSBSD) コマンドを使用すれば、すべてのサブシステム記述のリストを作成することができます。このリストで 5 (表示) を選択すると、選択したシステム記述に対するメニューが表示されます。このメニューには、サブシステム環境の各部分のリストが示されています。

オプションを選択して各部分の詳細を確認します。サブシステム記述変更 (CHGSBSD) コマンドを使用して、メニューの最初の 2 つの項目を変更します。他の項目を変更するには、項目タイプに該当する追加、除去、または変更コマンドを使用します。たとえば、ワークステーション項目を変更するには、ワークステーション項目変更 (CHGWSE) コマンドを使用します。

「*AS/400e シリーズ 実行管理の手引き*」では、サブシステム記述の処理について詳しく説明しています。そこでは、IBM 提供サブシステム記述の出荷時の値もリストされています。

自動開始ジョブ項目

自動開始ジョブ項目には、ジョブ記述の名前が入っています。ジョブ記述には、プログラムやコマンドを実行させる要求データ (RQSDTA) が含まれています。たとえば、 RQSDTA は `CALL LIB1/PROGRAM1` になっています。サブシステムを開始するたびに、システムは LIB1 ライブラリーの PROGRAM1 プログラムを実行します。

自動開始ジョブ項目と関連ジョブ記述を見てください。サブシステムが開始されるときに自動的に実行されるプログラムの機能を理解してください。

ワークステーション名とワークステーション・タイプ

サブシステムを開始すると、サブシステムは、ワークステーション名とワークステーション・タイプの項目にリストされている (個々に、またはまとめて) すべての未割り振りワークステーションを割り振ります。ユーザーがサインオンするときは、ワークステーションを割り振ったサブシステムにサインオンします。

ワークステーション項目を見れば、ジョブがそのワークステーションで開始されるときに、どのジョブ記述が使用されるかが分かります。ジョブ記述には、プログラムやコマンドを実行させる要求データが含まれています。たとえば、 RQSDTA パラメーターは `CALL LIB1/PROGRAM1` になっています。ユーザーがそのサブシステムのワークステーションにサインオンするたびに、システムは LIB1 の PROGRAM1 を実行します。

ワークステーション項目と関連ジョブ記述を見てください。認識されていないプログラムを実行するために、誰も項目を追加したり更新したりしていないことを確認してください。

ワークステーション項目には、デフォルトのユーザー・プロファイルを指定することもあります。特定のサブシステム構成の場合は、このように指定されていることにより、実行キーを押すだけで誰でもサインオンすることができます。システムのセキュリティー・レベル (QSECURITY システム値) が 40 よりも低い場合は、デフォルト・ユーザー用のワークステーション項目を検討する必要があります。

ジョブ待ち行列項目

サブシステムを開始すると、サブシステムは、サブシステム記述にリストされているすべての未割り振りジョブ待ち行列を割り振ります。ジョブ待ち行列項目は、直接のセキュリティーの問題はありません。しかしジョブ待ち行列項目は、意図しない環境でジョブを実行させることによって、誰かがシステム・パフォーマンスを低下させるような機会も提供します。

サブシステム記述のジョブ待ち行列項目を定期的に調べて、バッチ・ジョブが正しい環境で実行されていることを確認する必要があります。

経路指定項目

経路指定項目は、ジョブがサブシステムに入った後、ジョブに何を実行させるかを定義しています。サブシステムは、すべてのジョブ・タイプ (つまり、バッチ・ジョブ、対話式ジョブ、および通信ジョブ) に経路指定項目を使用します。経路指定項目は、次のものを指定します。

- ジョブのクラス。ジョブ待ち行列項目と同様に、ジョブと関連するクラスはそのパフォーマンスに影響を与えることがありますが、セキュリティー上の問題はありません。
- ジョブ開始時に実行されるプログラム。経路指定項目を調べ、誰も導入先で認識されていないプログラムを実行するために、誰も項目を追加したり更新したりしていないことを確認してください。

通信項目とリモート・ロケーション名

通信ジョブをシステムに入れると、システムは、活動サブシステムの通信項目とリモート・ロケーション名項目を使用して、通信ジョブをどのように実行するかを決定します。これらの項目について、次のものを調べてください。

- すべてのサブシステムは通信ジョブを実行することができます。通信に使用するサブシステムが活動状態になっていなければ、システムに入ろうとしているジョブは、自分のニーズを満たす別のサブシステム記述の項目を見つけることがあります。すべてのサブシステム記述の項目を調べる必要があります。
- 通信項目にはジョブ記述が入っています。ジョブ記述には、プログラムやコマンドを実行する要求データが含まれています。通信項目と関連ジョブ記述を調べて、ジョブがどのように開始されるかを理解してください。
- 通信項目は、システムが特定の状況の場合に使用するデフォルトのユーザー・プロファイルも指定します。デフォルトのプロファイルの役割を理解してください。システムにデフォルトのプロファイルが含まれている場合は、それらが最小の権限を持つプロファイルであることを確認する必要があります。デフォルトのユーザー・プロファイルの詳細については、『第 12 章 APPC 通信の保護』を参照してください。

  サブシステム記述印刷 (PRTSBSDAUT) コマンドを使用して、ユーザー・プロファイル名を指定する通信項目を識別することができます。

事前開始ジョブ項目

事前開始ジョブ項目を使用すれば、サブシステムが特定の種類のジョブを実行できるようにして、ジョブをより迅速に開始することができます。事前開始ジョブは、サブシステムを開始するとき、またはそのジョブが必要になったときに開始することができます。事前開始ジョブ項目は、次のものを指定します。

- 実行するプログラム

  デフォルトのユーザー・プロファイル

  ジョブ記述

これらはすべて、セキュリティー上の問題を示す可能性を持っています。事前開始ジョブ項目が、目的を持った許可機能しか実行しないことを確認する必要があります。

ジョブとジョブ記述

ジョブ記述には、そのジョブ記述を使用するときに特定のプログラムが実行されるようにする要求データと経路指定データが含まれています。ジョブ記述でプログラムが要求データ・パラメーターに指定されていると、システムはそのプログラムを実行します。ジョブ記述で経路指定データが指定されていると、システムは、その経路指定データと一致する経路指定項目に指定されているプログラムを実行します。

システムは、ジョブ記述を対話式ジョブにもバッチ・ジョブにも使用します。対話式ジョブの場合は、ワークステーション項目にはジョブ記述が指定されます。一般にワークステーション項目値は *USRPRF であるため、システムは、ユーザー・プロファイルに指定されたジョブ記述を使用します。バッチ・ジョブの場合は、ジョブを投入するときにジョブ記述を指定します。

ジョブ記述を定期的に検討して、意図していないプログラムをジョブ記述が実行しないことを確認する必要があります。また、オブジェクト権限を使用して、ジョブ記述が変更されるのを防止する必要があります。ジョブ記述を持つジョブを実行するには、*USE 権限で十分です。一般のユーザーには、ジョブ記述に対する *CHANGE 権限は必要ありません。

SECBATCH メニュー・オプション:
15 *は即時に投入する*、**54** *はジョブ・スケジューラーを使用する*

ジョブ記述には、どのユーザー・プロファイルの下でジョブを実行するかを指定することもできます。セキュリティー・レベル 40 以上の場合は、ジョブ記述に対する *USE 権限と、ジョブ記述に指定されているユーザー・プロファイルに対する *USE 権限を持っていなければなりません。セキュリティー・レベル 40 未満の場合は、ジョブ記述に対する *USE 権限しか必要ありません。

ジョブ記述権限印刷 (PRTJOBDAUT) コマンドを使用して、ユーザー・プロファイルを指定し、かつ *USE の共通権限を持つジョブ記述のリストを印刷することができます。

この報告書は、ジョブ記述に指定されているユーザー・プロファイルの特殊権限を示しています。この報告書には、ユーザー・プロファイルが持つすべてのグループ・プロファイルの特殊権限が含まれています。次のコマンドを使用して、ユーザー・プロファイルの私用権限を表示することができます。

```
DSPUSRPRF USRPRF(profile-name) TYPE(*OBJAUT)
```

ジョブ記述には、実行時にジョブが使用するライブラリー・リストが指定されます。誰かがユーザーのライブラリー・リストを変更できる場合は、そのユーザーが、別のライブラリーに入っている、意図しないバージョンのプログラムを実行する可能性があります。システムのジョブ記述に指定されているライブラリー・リストを定期的に検討する必要があります。

最後に、ジョブ投入 (SBMJOB) コマンドとユーザー・プロファイル作成 (CRTUSRPRF) コマンドのデフォルト値が、意図しないジョブ記述を指すように変更されていないことを確認する必要があります。

アーキテクチャー・トランザクション・プログラム名

一部の通信要求は、特定のタイプのシグナルをシステムに送信します。この要求は、**アーキテクチャー・トランザクション・プログラム名 (TPN)** と呼ばれます。それは、このトランザクション・プログラムの名前がシステムの APPC アーキテクチャーの一部だからです。表示装置パススルー要求の要求は、アーキテクチャー TPN の例です。アーキテクチャー TPN は通信を機能させるための通常の方法であり、必ずしも機密漏れの問題を提示するわけではありません。しかし、アーキテクチャー TPN によって、予期しないシステムへの入り口が提供される場合があります。

一部の TPN は、要求されたプロファイルを渡しません。デフォルト・ユーザーが *SYS である通信項目に要求が関連付けられた場合は、この要求をシステムで開始することができます。ただし、*SYS プロファイルはシステム機能のみを実行でき、ユーザー・アプリケーションを実行することはできません。

アーキテクチャー TPN をデフォルト・プロファイルで実行したくない場合は、通信項目のデフォルト・ユーザーを *SYS から *NONE に変更することができます。100 ページの『構造化 TPN 要求』には、アーキテクチャー TPN と関連ユーザー・プロファイルが示されています。

システムで特定の TPN を一切実行したくない場合は、次のようにします。

1. いくつかのパラメーターを受け入れる CL プログラムを作成します。このプログラムはどの機能も実行しないはずです。このプログラムは単に宣言 (DCL) ステートメントをパラメーターとして持っているだけで、その後で終了します。
2. TPN の経路指定項目を、通信項目とリモート・ロケーション名項目を持つ各サブシステムに追加します。経路指定項目は、次のような指定を行わなければなりません。
   - 開始位置が 37 の TPN のプログラム名 (構造化 TPN 要求を参照) と等しい*値比較* (CMPVAL) 値。
   - ステップ 1 で作成したプログラムの名前と等しい*呼び出し対象プログラム* (PGM) 値。これにより、TPN が他の経路指定項目 (たとえば、*ANY) を突き止めることができないようにします。

いくつかの TPN は、それぞれ独自の経路指定項目を QCMN サブシステムに持っています。これらの TPN は、パフォーマンス上の理由から追加されています。

構造化 TPN 要求

表 17. TPN 要求のプログラムおよびユーザー

TPN 要求	プログラム	ユーザー・プロファイル	説明
X'30F0F8F1'	AMQCRC6A	*NONE	メッセージ待ち行列化
X'06F3F0F1'	QACSOTP	QUSER	APPC サインオン・トランザクション・プログラム
X'30F0F2D1'	QANRTP	QADSM	ADSM/400 APPC 構成
X'30F0F1F9'	QCNPCSUP	*NONE	共用フォルダー
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	リモート SQL-DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	DSNX-PC レシーバー
X'30F0F1F3'	QDXPSEND	QUSER	DSNX-PC 送信側
X'30F0F2C4'	QEVYMAIN	QUSER	ENVY**/400 サーバー
X'30F0F6F0'	QHQTRGT	*NONE	PC データ待ち行列
X'30F0F8F0'	QLZPSERV	*NONE	Client Access ライセンス・マネージャー
X'30F0F1F7'	QMFRCVR	*NONE	PC メッセージ・レシーバー
X'30F0F1F8'	QMFSNDR	*NONE	PC メッセージ送信側
X'30F0F6F6'	QND5MAIN	QUSER	APPN 5394 ワークステーション制御装置
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	システム管理ユーティリティー
X'30F0F2C1'	QNPSERVR	*NONE	PWS-I ネットワーク印刷サーバー
X'30F0F7F9'	QOCEVOKE	*NONE	システム間カレンダー
X'30F0F6F1'	QOKCSUP	QDOC	ディレクトリー・シャドーイング
X'20F0F0F7'	QOQSESRV	QUSER	DIA バージョン 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA バージョン 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA バージョン 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA バージョン 1
X'30F0F0F5'	QPAPAST2	QUSER	S/36—S/38 パススルー
X'30F0F0F9'	QPAPAST2	QUSER	プリンター・パススルー
X'30F0F4F6'	QPWFSTP0	*NONE	共用フォルダー・タイプ 2
X'30F0F2C8'	QPWFSTP1	*NONE	クライアント・アクセス・ファイル・サーバー
X'30F0F2C9'	QPWFSTP2	*NONE	Windows** クライアント・アクセス・ファイル・サーバー
X'30F0F6F9'	QRQSRVX	*NONE	リモート SQL 変換サーバー
X'30F0F6F5'	QRQSRV0	*NONE	リモート SQL (コミットなし)
X'30F0F6F4'	QRQSRV1	*NONE	リモート SQL (コミットなし)

表 17. TPN 要求のプログラムおよびユーザー (続き)

TPN 要求	プログラム	ユーザー・プロファイル	説明
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	SNADS FS2 レシーバー
X'21F0F0F7'	QS2STSND	QGATE	SNADS FS2 送信側
X'30F0F1F6'	QTFDWNLD	*NONE	PC 転送機能
X'30F0F2F4'	QTIHNPCS	QUSER	TIE 機能
X'30F0F1F5'	QVPPRINT	*NONE	PC 仮想印刷
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 Server
X'30F0F8F3'	QZDAINIT	QUSER	PWS-I データ・アクセス・サーバー
X'21F0F0F2'	QZDRCVR	QSNADS	SNADS 受信機能
X'21F0F0F1'	QZDSTSND	QSNADS	SNADS 送信機能
X'30F0F2C5'	QZHQTRG	*NONE	PWS-I データ待ち行列サーバー
X'30F0F2C6'	QZRCSRVR	*NONE	PWS-I リモート・コマンド・サーバー
X'30F0F2C7'	QZSCSRVR	*NONE	PWS-I 中央サーバー

セキュリティー・イベントのモニター方式

セキュリティーの設定は、一回限りの作業ではありません。システムの変更とセキュリティー障害の両方を継続的に評価する必要があります。そして、新たに発生した変更や障害に対応するように、セキュリティー環境を調整する必要があります。

セキュリティー報告書は、システムで発生したセキュリティー関連の変更をモニターするのに役立ちます。以下に、セキュリティーの障害または危険を検出するために役立つその他のシステム機能を挙げます。

- セキュリティー監査は、システムで発生した多様なタイプのセキュリティー関連イベントを監視するための強力なツールです。たとえば、ユーザーが特定のデータベース・ファイルを更新用にオープンするたびに監査レコードを書き込むように、システムを設定できます。システム値のすべての変更を監査することができます。ユーザーがオブジェクトを復元する際の処置を監査することもできます。

  「*iSeries 機密保護解説書*」の第 9 章に、セキュリティー監査機能に関する完全な情報が記載されています。セキュリティー監査変更 (CHGSECAUD) コマンドを使用して、システムのセキュリティー監査を設定することができます。 監査ジャーナル項目表示 (DSPAUDJRNE) コマンドを使用して、セキュリティー監査ジャーナルから選択した情報を印刷することができます。

- QSYSMSG メッセージ待ち行列を作成して、重要なシステム操作員メッセージを取り込むことができます。 QSYSOPR メッセージ待ち行列は、通常の運用日を通してさまざまな重要度のメッセージを数多く受け取ります。 QSYSOPR メッセージ待ち行列内のメッセージは膨大な数となるため、重要なセキュリティー関連メッセージが見落とされてしまう可能性があります。

  システムの QSYS ライブラリーに QSYSMSG メッセージ待ち行列を作成すると、システムは、重要な特定のメッセージを QSYSOPR メッセージ待ち行列ではなく QSYSMSG メッセージ待ち行列に自動的に送信します。

QSYSMSG メッセージ待ち行列をモニターするプログラムを作成することもできますし、あるいはメッセージ待ち行列を自分自身または承認された別のユーザーに中断モードで割り当てることもできます。

第 3 部 アプリケーションとネットワーク通信

第 11 章 統合ファイル・システムの使用によるファイル保護

統合ファイル・システムは、iSeries サーバーに情報を保管し、それを表示する複数の方法を提供します。統合ファイル・システムは OS/400 オペレーティング・システムの一部であり、ストリーム入出力操作をサポートします。統合ファイル・システムには、パーソナル・コンピューターのオペレーティング・システムや UNIX® オペレーティング・システムと類似した (かつ、互換性のある) 記憶管理方式が装備されています。

統合ファイル・システムでは、システム上のすべてのオブジェクトを、階層ディレクトリー構造の観点からとらえることができます。しかし多くの場合、ユーザーは、それぞれのファイル・システムに最も適した方法でオブジェクトをとらえています。たとえば、「従来の」iSeries オブジェクトは QSYS.LIB ファイル・システムに入っています。通常、ユーザーは、これらのオブジェクトをライブラリーの観点からとらえ、QDLS ファイル・システムに含まれているオブジェクトをフォルダーの文書の観点からとらえます。ルート (/)、QOpenSys、およびユーザー定義のファイル・システムは、階層 (ネストされた) ディレクトリーの構造を提示します。

機密保護管理者は、以下のことについて理解していなければなりません。

- システムで使用されるファイル・システム
- 各ファイル・システムに固有な特性

以下、統合ファイル・システムのセキュリティーに関するいくつかの一般的な考慮事項について説明します。

統合ファイル・システムのセキュリティー・アプローチ

ルート・ファイル・システムは、iSeries サーバーに存在する他のすべてのファイル・システムのための基盤としての役割を果たします。ルート・ファイル・システムは、高いレベルから、システム上のすべてのオブジェクトに関する総合的な視点を提供します。 iSeries サーバーに置くことができる他のファイル・システムは、各ファイル・システムの基本的な目的に応じて、オブジェクトの管理と統合に関してそれぞれ異なるアプローチを提供します。例えば、QOPT (光学式) ファイル・システムを使用すると、iSeries アプリケーションおよびサーバー (iSeries Access for Windows ファイル・サーバーを含む) は、iSeries サーバー上の CD-ROM ドライブにアクセスすることができます。同様に、QFileSvr.400 ファイル・システムを使用すると、アプリケーションはリモートの iSeries サーバー上にある統合ファイル・システム・データにアクセスすることができます。 QLANSrv ファイル・サーバーを使用すると、iSeries 統合 xSeries サーバーに保管されたファイルや、ネットワークの他の接続サーバーに保管されているファイルにアクセスすることができます。

各ファイル・システムのセキュリティー・アプローチは、ファイル・システムが使用可能にするデータによって異なります。たとえば、QOPT ファイル・システムはオブジェクト・レベルのセキュリティーを提供しません。それは、権限情報を CD-ROM に書き込むテクノロジーがないからです。 QFileSvr.400 ファイル・システムの場合は、アクセス制御はファイルが物理的に格納され管理されているリモー

ト・システムで行われます。 QLANSrv のようなファイル・システムの場合は、iSeries 統合 xSeries サーバーがアクセス制御を行います。セキュリティー・モデルに違いはありますが、多くのファイル・システムは、権限変更 (CHGAUT) や所有者変更 (CHGOWN) などの統合ファイル・システム・コマンドを使用して、一貫性のあるアクセス制御の管理をサポートします。

ここでは、統合ファイル・システムのセキュリティーで見落としがちないくつかのヒントを挙げます。統合ファイル・システムは POSIX 標準にできる限り近づけるよう設計されています。これにより、iSeries サーバーの権限と POSIX の許可が混合された興味深い性質になっています。

1. あるユーザーが共通権限、グループ、または権限リストで許可されている場合でも、そのユーザーが所有しているディレクトリーに対する私用権限は除去してはなりません。標準の iSeries サーバー・セキュリティー・モデルのライブラリーまたはフォルダーで処理を行っている時に所有者の私用権限を除去すると、ユーザー・プロファイルのために保管されている権限情報の量は少なくなりますが、他の操作への影響はありません。しかし、POSIX 標準がディレクトリーの許可継承を定義する方法によって、たとえ新しく作成されたディレクトリーの所有者がその親に対して別の私用権限を持っていたとしても、新しく作成されたディレクトリーの所有者はそのディレクトリーに対して、親の所有者がその親に対して持っているのと同じオブジェクト権限を持ちます。これは理解しにくいので、例を示します。 USERA がディレクトリー /DIRA を所有していて、USERA の私用権限が除去されたとします。 USERB は /DIRA に対して私用権限を持っています。 USERB がディレクトリー /DIRA/DIRB を作成します。 USERA は /DIRA に対してオブジェクト権限を持っていないので、 USERB は /DIRA/DIRB に対するオブジェクト権限を持ちません。 USERB は、USERB のオブジェクト権限を変更する処置をとらない限り /DIRA/DIRB を名前変更したり、削除することはできません。これは、open() API で O_INHERITMODE フラグを使用してファイルを作成したときにも起こります。 USERB がファイル /DIRA/FILEB を作成したのだとしたら、USERB はそれに対してオブジェクト権限もデータ権限も持ちません。 USERB は新しいファイルに書き込むことができません。
2. 借用権限は、大部分の物理ファイル・システムでサポートされていません。これには、ルート (/)、QOpenSys、QDLS、およびユーザー定義のファイル・システムが含まれます。
3. オブジェクトは、たとえユーザー・プロファイルの OWNER フィールドが *GRPPRF に設定されていても、そのオブジェクトを作成したユーザー・プロファイルによって所有されています。
4. 多くのファイル・システム操作では、ルート (/) ディレクトリーも含めて、パスの各コンポーネントに対して *RX データ権限が必要です。権限の問題が発生したら、ルート自体に対するユーザーの権限を検査してください。
5. 現行作業ディレクトリー (DSPCURDIR、getcwd()、など) を表示または検索するには、パス内の各コンポーネントに対する *RX データ権限が必要です。しかし、現行作業ディレクトリーの変更 (CD、chdir()、など) に必要なのは、各コンポーネントに対する *X データ権限のみです。したがって、現行作業ディレクトリーを特定のパスに変更するとそのパスを表示できないことがあります。
6. COPY コマンドの意図は、オブジェクトを複写することです。新しいファイルでの権限設定は、所有者以外は元のファイルと同じです。しかし、CPYTOSTMF

コマンドの意図は、単純にデータを複写することです。新しいファイルでの権限設定は、ユーザーでは制御できません。作成者 / 所有者は *RWX データ権限を持ちますが、グループ権限および共通権限は *EXCLUDE です。ユーザーは別の方法 (CHGAUT、chmod()、など) を使用して、必要な権限を割り当てる必要があります。

7. ユーザーがオブジェクトに関する権限情報を検索するためには、そのユーザーがそのオブジェクトの所有者であるか、またはオブジェクトに対する *OBJMGT オブジェクト権限を持っている必要があります。これにより COPY (ターゲットのオブジェクトに同等の権限を設定するために、ソース・オブジェクトに関する権限情報を検索しなければなりません) などのように、予期しない結果が発生することがあります。
8. オブジェクトの所有者またはグループを変更するときは、ユーザーはそのオブジェクトに対する適切な権限を持っていなければならず、また、新しい所有者 / グループのユーザー・プロファイルに対する *ADD データ権限、および古い所有者 / グループのプロファイルに対する *DELETE データ権限も持っていなければなりません。これらのデータ権限は、ファイル・システムのデータ権限には関係ありません。これらのデータ権限は、DSPOBJAUT コマンドによって表示でき、EDTOBJAUT コマンドによって変更できます。これはまた、新しいオブジェクトのグループ ID を設定しようとするときに、予期せず COPY を発生させます。
9. MOV コマンドでは、特に、ある物理ファイル・システムから別の物理ファイル・システムに移動するとき、あるいはデータ変換を実行するときに、権限エラーが発生することがあります。この場合、実際には移動はコピーと削除の操作になります。したがって、MOV コマンドは、COPY コマンド (上記の 7 および 8 参照) および RMVLNK コマンドと全く同じ権限に関する考慮事項の影響を受け、さらにその他の MOV に特定の考慮事項もあります。

次のセクションで、いくつかの代表的なファイル・システムに関する考慮事項を示します。 iSeries サーバーの特定のファイル・システムについて詳しくは、当該ファイル・システムを使用するライセンス・プログラムの資料を調べてください。

ルート (/)、QOpenSys、およびユーザー定義のファイル・システム

ルート、QOpenSys、およびユーザー定義のファイル・システムのセキュリティー考慮事項を以下に示します。

権限の仕組み

ルート、QOpenSys、およびユーザー定義のファイル・システムは、iSeries サーバー、PC、および UNIX** のオブジェクト管理とセキュリティーの両方の機能を組み合わせて提供します。 iSeries サーバー・セッションから統合ファイル・システム・コマンド (WRKAUT および CHGAUT) を使用すると、すべての通常の iSeries サーバー・オブジェクト権限を設定することができます。こうすることにより、Spec 1170 (UNIX タイプのオペレーティング・システム) と互換性のある *R、*W、および *X 権限が組み込まれます。

注: ルート、QOpenSys、およびユーザー定義のファイル・システムは、機能的には同じものです。QOpenSys ファイル・システムは大文字小文字の区別をします。ルート・ファイル・システムは大文字小文字の区別をしません。ユーザー定義

のファイル・システムは、大文字と小文字を区別するように定義することができます。これらのファイル・システムのセキュリティー特性は同じであるため、以下のトピックでは、それらファイル・システムの名前を同じ意味で使用します。

PC セッションからルート・ファイル・システムに管理者としてアクセスすると、以下のようなオブジェクト属性を設定することができ、PC はこれを使用して特定のタイプのアクセスを制限することができます。
- システム
- 隠し
- アーカイブ
- 読み取り専用

これらの PC 属性は、iSeries サーバー・オブジェクト権限値に追加されるものであり、それに代わるものではありません。

ユーザーがルート・ファイル・システムのオブジェクトにアクセスしようとすると、OS/400 は、オブジェクト権限がユーザーのインターフェースから「見える」か否かに関係なく、すべてのオブジェクト権限値とオブジェクト属性を強制的に使用します。たとえば、オブジェクトの読み取り専用属性がオンに設定されているとします。 PC ユーザーは、iSeries Access インターフェースからこのオブジェクトを削除することはできません。 iSeries サーバー・ユーザーが *ALLOBJ 特殊権限を持っていても、固定機能ワークステーションを持つ iSeries サーバー・ユーザーはこのオブジェクトを削除することはできません。オブジェクトを削除するには、その前に、許可ユーザーが PC 機能を使用して読み取り専用値を**オフ**にリセットしておかなければなりません。同様に、PC ユーザーが、オブジェクトの PC 関連セキュリティー属性を変更するために十分な OS/400 権限を持っていないことが考えられます。

iSeries サーバーで実行される UNIX タイプのアプリケーションは、 UNIX タイプのアプリケーション・プログラミング・インターフェース (API) を使用して、ルート・ファイル・システムのデータにアクセスします。UNIX タイプの API の場合、アプリケーションは次のようなセキュリティー情報を認識し、保守することができます。
- オブジェクト所有者
- グループ所有者 (iSeries サーバー 1 次グループ権限)
- 読み取り (ファイル)
- 書き込み (内容の変更)
- 実行 (プログラムの実行またはディレクトリーの検索)

システムは、以下のデータ権限を既存の iSeries サーバー・オブジェクト権限とデータ権限にマップします。
- Read (*R) = *OBJOPR および *READ
- Write (*W) = *OBJOPR、*ADD、*UPD、*DLT
- Execute (*X) = *OBJOPR および *EXECUTE

他のオブジェクト権限 (*OBJMGT、*OBJEXIST、*OBJALTER、および *OBJREF) の概念は、 UNIX タイプの環境には存在しません。

ただし、これらのオブジェクト権限は、ルート・ファイル・システムのすべてのオブジェクトにあるわけではありません。 UNIX スタイルの API を使用してオブジェクトを作成すると、そのオブジェクトはその親ディレクトリーからこれらの権限を継承し、以下のようになります。

- 新規オブジェクトの所有者は、親ディレクトリーの所有者と同じオブジェクト権限を持つ。
- 新規オブジェクトの 1 次グループは、親ディレクトリーの 1 次グループと同じオブジェクト権限を持つ。
- 新規オブジェクトの共通は、親ディレクトリーの共通と同じオブジェクト権限を持つ。

所有者、1 次グループ、および共通に対する新規オブジェクトのデータ権限は、API のモード・パラメーターで指定されます。オブジェクト権限のすべてが「オン」に設定されている場合、権限の振る舞いは、UNIX タイプの環境での振る舞いと同じになります。 POSIX タイプの振る舞いにする場合以外は、オブジェクト権限は「オン」にします。

UNIX タイプの API を使用するアプリケーションを実行すると、システムは、オブジェクト権限が UNIX タイプのアプリケーションから「見える」か否かに関係なく、全オブジェクト権限を強制的に使用します。たとえば、権限リストの概念が UNIX タイプのオペレーティング・システムに存在しなくても、システムは権限リストの権限を強制的に使用します。

混合アプリケーション環境の場合は、1 つの環境で行った権限変更が別の環境のアプリケーションに影響を与えないことを確認する必要があります。

ルート (/)、QOpenSys、およびユーザー定義のファイル・システムのセキュリティーの操作

統合ファイル・システムの導入に伴い、iSeries サーバーは、複数ファイル・システムでオブジェクトを処理するための一組の新規のコマンドを提供しました。このコマンド・セットには、セキュリティーを処理するための次のようなコマンドが含まれています。

- 監査変更 (CHGAUD)
- 権限変更 (CHGAUT)
- 所有者変更 (CHGOWN)
- 1 次グループ変更 (CHGPGP)
- 権限表示 (DSPAUT)
- 権限処理 (WRKAUT)

これらのコマンドは、基本データとオブジェクト権限を UNIX タイプの以下の権限サブセットに分類します。

***RWX** 読み取り / 書き込み / 実行
***RW** 読み取り / 書き込み
***R** 読み取り
***WX** 読み取り / 書き込み / 実行
***W** 書き込み
***X** 実行

さらに、UNIX タイプの API は、セキュリティーを処理するためにも使用できます。

ルート・ディレクトリーに対する共通権限

システムが出荷されるときは、ルート・ディレクトリーに対する共通権限が *ALL (すべてのオブジェクト権限およびすべてのデータ権限) になっています。この設定により、UNIX タイプのアプリケーションが行う操作にも、一般的な iSeries サーバー・ユーザーが行う操作にも融通性と互換性が提供されます。コマンド行機能を使用できる iSeries サーバー・ユーザーは、単に CRTLIB コマンドを使用するだけで、新規のライブラリーを QSYS.LIB ファイル・システムに作成することができます。通常、一般的な iSeries サーバーの権限ではこれを行うことができます。同様に、出荷時のルート・ファイル・システムの設定により、一般的なユーザーは、新規のディレクトリーをルート・ファイル・システムに作成することができます (これは、新規のディレクトリーを PC に作成できるのと似ています)。

機密保護管理者は、ユーザーが作成したオブジェクトを適切に保護することについてユーザーを教育する必要があります。ユーザーがライブラリーを作成する場合、ライブラリーに対する共通権限は おそらく *CHANGE (デフォルト) にすべきではありません。ユーザーは、ライブラリーの内容に応じて、共通権限を *USE または *EXCLUDE のいずれかに設定する必要があります。

アプリケーション・ユーザーが、ルート (/)、QOpenSys、またはユーザー定義のファイル・システムに新規ディレクトリーを作成する必要がある場合には、次のようないくつかのセキュリティー・オプションが使用できます。

- 新規ディレクトリーを作成するときに、デフォルトの権限をオーバーライドするようにユーザーを教育することができます。デフォルトでは、その直接の親ディレクトリーから権限を継承します。ルート・ディレクトリーの新規作成ディレクトリーの場合は、デフォルトで共通権限が *ALL になります。
- ルート・ディレクトリーの下に「マスター」サブディレクトリーを作成することができます。そのマスター・ディレクトリーの共通権限を、ユーザーの組織に該当する設定値に設定してください。その後に、任意の新規個人用ディレクトリーをこのマスター・サブディレクトリーに作成するようユーザーに指示します。これらの新規ディレクトリーは、マスター・ディレクトリーの権限を継承します。
- ユーザーがオブジェクトをルート・ディレクトリーに作成しないようにするために、ルート・ディレクトリーの共通権限を変更することを考えることができます。(*W、*OBJEXIST、*OBJALTER、*OBJREF、および *OBJMGT 権限を除去します。) ただし、この変更によっていずれかのアプリケーションに問題が生じることがないかを評価する必要があります。たとえば、オブジェクトをルート・ディレクトリーから削除する可能性のある UNIX タイプのアプリケーションもあるかもしれません。

私用権限オブジェクトの印刷 (PRTPVTAUT) コマンド

私用権限オブジェクトの印刷 (PRTPVTAUT) コマンドを使用すれば、指定されたライブラリー、フォルダー、またはディレクトリーに含まれている指定されたタイプのオブジェクトに関するすべての私用権限報告書を印刷することができます。この報告書には、指定されたタイプのすべてのオブジェクトと、このオブジェクトに対

する権限を持っているユーザーがリストされています。このようにして、オブジェクトに対する権限のさまざまなソースを確認することができます。

このコマンドは、選択されたオブジェクトに関して 3 つの報告書を印刷します。最初の報告書 (完全報告書) には、選択された各オブジェクトに関するすべての私用権限が含まれています。 2 番目の報告書 (変更報告書) には、指定ライブラリー、フォルダー、またはディレクトリーに含まれている指定オブジェクトに対して PRTPVTAUT コマンドが前に実行された場合に、これらのオブジェクトに対する私用権限に行った追加や変更が含まれています。選択されたタイプの任意の新規オブジェクト、既存のオブジェクトに対する新規の権限、または既存のオブジェクトに対する既存の権限に行った変更が、「変更報告書」にリストされています。指定ライブラリー、フォルダー、またはディレクトリーに含まれている指定オブジェクトに対して、前に PRTPVTAUT コマンドが実行されなかった場合は、「変更報告書」は作成されません。前にこのコマンドは実行されたが、オブジェクトの権限に対する変更が行われなかった場合は、「変更報告書」は印刷されますが、オブジェクトはリストされません。

3 番目の報告書 (削除報告書) には、前に PRTPVTAUT コマンドが実行された後に、指定したオブジェクトから削除されたすべての私用権限ユーザーが含まれます。削除されたすべてのオブジェクトや私用権限ユーザーとして除去されたすべてのユーザーが、「削除報告書」にリストされています。前に PRTPVTAUT コマンドが実行されなかった場合は、「削除報告書」は作成されません。前にこのコマンドは実行されたが、オブジェクトに対する削除操作が行われなかった場合は、「削除報告書」は印刷されますが、オブジェクトはリストされません。

制約事項: このコマンドを使用するには、*ALLOBJ 特殊権限を持っていなければなりません。

例:

次のコマンドは、PAYROLLLIB のすべてのファイル・オブジェクトについて、完全報告書、変更報告書、および削除報告書を作成します。

```
PRTPVTAUT OBJTYPE(*FILE) LIB(PAYROLLLIB)
```

次のコマンドは、GARRY ディレクトリーのすべてのストリーム・ファイル・オブジェクトについて、完全報告書、変更報告書、および削除報告書を作成します。

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*NO)
```

次のコマンドは、GARRY ディレクトリーから開始するサブディレクトリー構造のすべてのストリーム・ファイル・オブジェクトについて、完全報告書、変更報告書、および削除報告書を作成します。

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*YES)
```

共通権限オブジェクトの印刷 (PRTPUBAUT) コマンド

共通権限オブジェクトの印刷 (PRTPUBAUT) コマンドを使用すれば、 *EXCLUDE の共通権限を持っていない指定したオブジェクトの報告書を印刷することができます。 *PGM オブジェクトの場合は、ユーザーが呼び出すことのできる *EXCLUDE の共通権限を持っていないプログラム (このプログラムはユーザー・ドメインであるか、またはシステム・セキュリティー・レベル (QSECURITY システム値) が 30

以下) のみが、この報告書に入れられます。このようにして、システム上のすべてのユーザーがアクセスできるオブジェクトを確認することができます。

このコマンドは 2 つの報告書を印刷します。最初の報告書 (完全報告書) には、*EXCLUDE の共通権限を持っていないすべての指定オブジェクトが含まれています。 2 番目の報告書 (変更報告書) には、前に PRTPUBAUT コマンドが実行されたときは *EXCLUDE の共通権限を持っていたか、または存在しなかったが、現在は *EXCLUDE の共通権限を持っていないオブジェクトが入れられます。指定したオブジェクトとライブラリー、フォルダー、またはディレクトリーに対して、前に PRTPUBAUT コマンドが実行されなかった場合は、「変更報告書」は作成されません。前にこのコマンドは実行されたが、追加オブジェクトが *EXCLUDE の共通権限を持っていない場合は、「変更報告書」は印刷されますが、オブジェクトはリストされません。

制約事項: このコマンドを使用するには、 *ALLOBJ 特殊権限を持っていなければなりません。

例:

次のコマンドは、GARRY ライブラリーの共通権限 *EXCLUDE を持たないすべてのファイル・オブジェクトについて、完全報告書、および変更報告書を作成します。

```
PRTPUBAUT OBJTYPE(*FILE) LIB(GARRY)
```

次のコマンドは、GARRY ディレクトリーから開始するサブディレクトリー構造の共通権限 *EXCLUDE を持たないすべてのストリーム・ファイル・オブジェクトについて、完全報告書、変更報告書、および削除報告書を作成します。

```
PRTPUBAUT OBJTYPE(*STMF) DIR(GARRY) SCHSUBDIR(*YES)
```

QSYS.LIB ファイル・システムへのアクセスの制限

ルート・ファイル・システムは傘状のファイル・システムであるため、QSYS.LIB ファイル・システムは、ルート・ディレクトリー内のサブディレクトリーと見なされます。したがって、iSeries サーバーにアクセスするすべての PC ユーザーは、iSeries サーバー・ライブラリー (QSYS.LIB ファイル・システム) に格納されているオブジェクトを通常の PC コマンドと処置で操作することができます。たとえば、PC ユーザーは、 QSYS.LIB オブジェクト (たとえば、重要なデータ・ファイルが入っているライブラリー) をシュレッダーにドラッグすることができます。

107 ページの『ルート (/)、QOpenSys、およびユーザー定義のファイル・システム』に説明されているように、全オブジェクト権限がインターフェースから見えるか否かに関係なく、システムは全オブジェクト権限を強制的に使用します。したがって、ユーザーは、オブジェクトに対する *OBJEXIST 権限を持っていない限り、このオブジェクトを廃棄 (削除) することはできません。ただし、iSeries が、オブジェクト・セキュリティーではなくメニュー・アクセス・セキュリティーに依存している場合、 PC ユーザーが、シュレッダーにかけることのできるオブジェクトが QSYS.LIB ファイル・システムで存在します。

システムの使用が増え、アクセスに使用する方式が多様化するにつれ、やがてメニュー・アクセスのセキュリティーが十分でないことに気付くようになります。

49 ページの『第 5 章 オブジェクト権限による情報資産の保護』では、メニュー・アクセス制御をオブジェクト・セキュリティーで補足するためのストラテジーについて説明しています。しかし、iSeries サーバーでは、ルート・ファイル・システム・ディレクトリー構造を介して QSYS.LIB ファイル・システムへのアクセスを簡単に防止することもできます。 QPWFSERVER 権限リストを使用すれば、どのユーザーが、ルート・ディレクトリーを介して QSYS.LIB ファイル・システムにアクセスできるかを制御することができます。

QPWFSERVER 権限リストに対するユーザーの権限が *EXCLUDE であれば、ユーザーは、ルート・ディレクトリー構造から QSYS.LIB ディレクトリーに入ることはできません。ユーザーの権限が *USE であれば、ユーザーはディレクトリーに入ることができます。ユーザーがディレクトリーに入るための権限を取得すると、ユーザーが QSYS.LIB ファイル・システム内のオブジェクトに対して実行するすべての処置について、通常のオブジェクト権限が適用されます。つまり、QPWFSERVER 権限リストに対する権限は、QSYS.LIB ファイル・システム全体に対するドアのような働きをします。 *EXCLUDE 権限を持つユーザーに対しては、このドアはロックされています。 *USE 権限 (または、それより範囲の大きい権限) を持つユーザーに対しては、このドアは開いています。

多くの場合、ユーザーは、 QSYS.LIB ファイル・システムのオブジェクトにアクセスするためにディレクトリー・インターフェースを使用する必要はありません。おそらく導入先では、QPWFSERVER 権限リストに対する共通権限を *EXCLUDE に設定したい場合があります。ただし、権限リストに対する権限は、ユーザー・ライブラリーを含め、 QSYS.LIB ファイル・システム内のすべてのライブラリーに対して、ドアを開けたり閉めたりするということを忘れないでください。このような排他を嫌がるユーザーがいる場合は、そのユーザーの要件を個々に評価することができます。適格であれば、個々のユーザーを権限リストに明示的に認可することができます。ただし、ユーザーが QSYS.LIB ファイル・システム内のオブジェクトに対する適切な権限を持っていることを確認する必要があります。さもないと、ユーザーが不注意にオブジェクトやライブラリー全体を削除してしまう可能性があります。

注:

1. システムが出荷されるときは、 QPWFSERVER 権限リストに対する共通権限は *USE になっています。
2. 個々のユーザーを明示的に認可する場合は、権限リストは、 iSeries Access ファイル・サービス機能、NetServer ファイル・サービス機能、および iSeries サーバー間のファイル・サービス機能でしかアクセスを制御しません。 この方法では、FTP、ODBC、およびその他のネットワークを介した同一ディレクトリーへのアクセスは防止されません。

ディレクトリーの保護

ルート・ファイル・システム内のオブジェクトにアクセスするには、そのオブジェクトへ至る全パスを読み取ります。ディレクトリーを検索するには、そのディレクトリーに対する *X (*OBJOPR および *EXECUTE) 権限を持っていなければなりません。たとえば、次のようなオブジェクトにアクセスするとします。

```
/companya/customers/custfile.dat
```

この場合、companya ディレクトリーと customers ディレクトリーへの *X 権限を持っていなければなりません。

ルート・ファイル・システムの場合は、オブジェクトのシンボリック・リンクを作成することができます。概念的には、シンボリック・リンクはパス名の別名です。通常、全パス名よりも、シンボリック・リンクの方が短くて、記憶するのが容易です。しかしシンボリック・リンクは、オブジェクトへの別の物理パスを作成するわけではありません。ユーザーは、依然として、オブジェクトへの物理パスのすべてのディレクトリーとサブディレクトリーに対する *X 権限を必要とします。

ルート・ファイル・システムのオブジェクトの場合、 QSYS.LIB ファイル・システムでライブラリー・セキュリティーを使用するのとまったく同じように、ディレクトリー・セキュリティーを使用することができます。たとえば、ディレクトリーの共通権限を *EXCLUDE に設定して、共通ユーザーがそのツリー内のオブジェクトにアクセスしないようにすることができます。

新規オブジェクトのためのセキュリティー

新規オブジェクトをルート・ファイル・システムに作成すると、作成に使用したインターフェースによってそのオブジェクトの権限が決定します。たとえば、CRTDIR コマンドをそのデフォルト値を指定して使用する場合は、新規ディレクトリーは、その親ディレクトリーのすべての権限特性を継承します。その中には、私用権限、基本グループ権限、および権限リスト・アソシエーションが含まれています。以下のセクションでは、インターフェースのタイプごとに権限を決定する方法を説明します。

権限は、その直接の親ディレクトリーから継承されるものであり、ツリー内の高位のディレクトリーから継承されるものではありません。したがって、機密保護管理者としては、階層のディレクトリーに割り当てる権限を、次の 2 つの観点から見る必要があります。

- ツリー内のオブジェクトへのアクセスに対して、権限がどのような影響を与えているか (ライブラリー権限のような)。
- 新規作成オブジェクトに対して、権限がどのような影響を与えているか (ライブラリーの CRTAUT 値のような)。

推奨事項: 統合ファイル・システムを利用するユーザーに対して、ホーム・ディレクトリー (たとえば /home/usrxxx) を与えてから、適切なセキュリティー (たとえば、PUBLIC *EXCLUDE) を設定してください。そうすれば、ユーザーがホーム・ディレクトリーの下に作成したすべてのディレクトリーが、これらの権限を継承するようになります。

次に、各種のインターフェースに関する権限継承について説明します。

ディレクトリー作成コマンドの使用

CRTDIR コマンドを使用して新規のサブディレクトリーを作成するときは、権限を指定するための次の 2 つのオプションを使用することができます。

- 共通権限 (データ権限、オブジェクト権限、またはその両方) を指定することができます。

- データ権限、オブジェクト権限、またはその両方に対して *INDIR を指定することができます。データ権限とオブジェクト権限の両方に対して *INDIR を指定すると、システムは、親ディレクトリーのすべての権限情報、たとえば、権限リスト、1 次グループ、共通権限、私用権限などを、新規オブジェクトにそのままコピーします。 (システムは、QSYS プロファイルまたは QSECOFR プロファイルがオブジェクトに対して持っている私用権限はコピーしません。)

API を使用したディレクトリーの作成

mkdir() API を使用してディレクトリーを作成するときは、所有者、1 次グループ、および共通に関するデータ権限を指定します (*R、*W、および *X の権限マップを使用)。システムは、親ディレクトリーの情報を使用して、所有者、1 次グループ、および共通に関するオブジェクト権限を設定します。

UNIX タイプのオペレーティング・システムはオブジェクト権限のコンセプトを持っていないため、mkdir() API は、オブジェクト権限の指定をサポートしません。別のオブジェクト権限が必要な場合は、iSeries サーバー・コマンド (CHGAUT) を使用することができます。しかし、いくつかのオブジェクト権限を除去すると、UNIX タイプのアプリケーションは、予期したように機能しないことがあります。

open() API または creat() API を使用したストリーム・ファイルの作成

creat() API を使用してストリーム・ファイルを作成する際には、所有者、1 次グループ、および共通に対するデータ権限を (UNIX タイプの権限 *R、*W、および *X を使用して) 指定することができます。システムは、親ディレクトリーの情報を使用して、所有者、1 次グループ、および共通に関するオブジェクト権限を設定します。

また、open() API を使用してストリーム・ファイルを作成する場合は、これらの権限を指定することもできます。あるいは、open() API を使用する場合は、オブジェクトがその親ディレクトリーからすべての権限を継承するように指定することができます。これを**継承モード**と呼びます。継承モードを指定すると、システムは、権限リスト、1 次グループ、共通権限、私用権限などが親権限と完全に一致しているものを作成します。このオプションは、CRTDIR コマンドに *INDIR を指定した場合と同じ働きをします。

PC インターフェースを使用したオブジェクトの作成

PC アプリケーションを使用してオブジェクトをルート・ファイル・システムに作成すると、システムは自動的に全権限を親ディレクトリーから継承します。権限リスト、1 次グループ、共通権限、私用権限などが含まれます。 PC アプリケーションは、オブジェクト作成時の権限指定と同じ操作は行いません。

QFileSvr.400 ファイル・システム

QFileSvr.400 ファイル・システムの場合は、ある iSeries システム (SYSTEMA) のユーザー (USERX) は、別の接続 iSeries システム (SYSTEMB) のデータにアクセスすることができます。USERX は、Client Access インターフェースと類似したインターフェースを持っています。リモート iSeries サーバー (SYSTEMB) は、すべてのファイル・システムをサブディレクトリーとして持つディレクトリーとして表示されます。

USERX がこのインターフェースを持つ SYSTEMB にアクセスしようとすると、SYSTEMA は USERX のユーザー・プロファイル名と暗号化されたパスワードを SYSTEMB に送信します。これと同じユーザー・プロファイルとパスワードが、SYSTEMB に存在していなければなりません。存在しない場合、SYSTEMB がその要求を拒否します。

SYSTEMB が要求を受け入れると、USERX は、SYSTEMB に対する Client Access ユーザーのように扱われます。同じ権限検査規則が、USERX が試行するすべての処置に適用されます。

機密保護管理者としては、QFileSvr.400 ファイル・システムが、システムに対する別のドアを表していることを知っておく必要があります。リモート・ユーザーを、ディスプレイ・パススルーによる対話式サインオンに限定することを想定することはできません。 QSERVER サブシステムを実行し、システムを別の iSeries システムに接続すると、リモート・ユーザーは、あたかも Client Access を実行するローカル PC のユーザーのように、システムにアクセスすることができます。おそらく、システムが、QSERVER サブシステムを実行する必要のある接続を持つと考えられます。これが、適切なオブジェクト権限体系が重要であるもう 1 つの理由です。

ネットワーク・ファイル・システム

ネットワーク・ファイル・システム (NFS) は、 NFS インプリメンテーションを持つシステムとのアクセスを行います。 NFS は、ネットワーク・システムのユーザー間で情報を共用するための業界標準方式です。主要なオペレーティング・システム (PC オペレーティング・システムを含む) の多くは、 NFS を提供しています。UNIX システムの場合、NFS は、データへのアクセスの基本方式です。 iSeries サーバーは、NFS クライアントとしても NFS サーバーとしても動作します。

NFS サーバーとして動作する iSeries システムの機密保護管理者は、 NFS のセキュリティー面について理解して管理する必要があります。推奨事項と考慮事項は、次のとおりです。

- STRNFSSVR コマンドを使用して NFS サーバーの機能を明示的に開始する必要があります。このコマンドを使用する権限を誰にもたせるかを制御します。
- NFS クライアントがディレクトリーまたはオブジェクトを使用できるようにするために、それを**エクスポート**します。このため、ネットワーク内の NFS クライアントがシステムのどの部分を使用できるようにするかについて、非常に個別的な制御を行うことになります。
- エクスポートするときに、どのクライアントがオブジェクトにアクセスできるかを指定することができます。クライアントの識別は、システム名または IP アド

レスで行います。クライアントは、個々の PC でも、iSeries サーバー全体でも、UNIX システムでも可能です。 NFS 用語では、クライアント (IP アドレス) はマシンと呼ばれます。

- エクスポートするとき、エクスポートされるディレクトリーまたはオブジェクトにアクセスする各マシンごとに、読み取り専用アクセスまたは読み取り/書き込みアクセスを指定することができます。多くの場合、読み取り専用アクセスを指定します。
- NFS はパスワード保護を行いません。 NFS は、システムの承認体系の中でデータ共用を行うように設計され、意図されています。ユーザーがアクセスを要求すると、サーバーはユーザーの uid を受け取ります。 uid に関する考慮事項は、次のとおりです。
  - iSeries サーバーは、同じ uid を使用してユーザー・プロファイルを探し出そうとします。一致する uid が見つかると、iSeries はユーザー・プロファイルの認証を使用します。認証は、ユーザーの権限を使用して記述するための NFS 用語です。これは、その他の iSeries サーバー・アプリケーションにおけるプロファイル・スワップインと同じです。
  - ディレクトリーまたはオブジェクトをエクスポートするとき、ルート権限を持つプロファイルによるアクセスを許可するかどうかを指定することができます。 iSeries サーバー上の NFS サーバーは、ルート権限を *ALLOBJ 特殊権限と等価にします。ルート権限を許可しないように指定した場合は、*ALLOBJ 特殊権限でユーザー・プロファイルにマップする uid をもつ NFS ユーザーは、そのプロファイルではオブジェクトにアクセスすることができません。その代わりに、匿名アクセスが許可される場合は、要求元は匿名プロファイルにマップされます。
  - ディレクトリーまたはオブジェクトをエクスポートするとき、匿名要求を許可するかどうかを指定することができます。匿名要求は、システム上のどの uid とも一致しない uid を持つ要求です。匿名要求の許可を選択すると、システムは匿名ユーザーを IBM 提供の QNFSANON ユーザー・プロファイルにマップします。このユーザー・プロファイルは、特殊権限や明示権限を一切持っていません。 (エクスポートするとき、必要であれば、別のユーザー・プロファイルを匿名要求に指定することができます。)
- iSeries サーバーが NFS ネットワーク (または、uid に依存する UNIX システムを持つ任意のネットワーク) に加入している場合は、自動的にシステムに uid を割り当てさせるのではなくて、自分でそれを管理しなければならないこともあります。 uid をネットワークの他のシステムと調整する必要があります。

  ネットワークの他のシステムとの互換性を保つために、uid を変更しなければならないこともあります (IBM 提供のユーザー・プロファイルの場合でも同様です)。ユーザー・プロファイルの uid を簡単に変更できるプログラムが使用できるようになりました。(ユーザー・プロファイルの uid を変更すると、そのユーザー・プロファイルが、ルート・ディレクトリーまたは QOpenSrv ディレクトリーのいずれかに所有しているすべてのオブジェクトの uid も変更しなければなりません。) QSYCHGID プログラムは、ユーザー・プロファイルおよびすべての所有オブジェクトの中の uid を自動的に変更します。このプログラムの使用方法については、「*iSeries System API Reference*」を参照してください。

第 12 章 APPC 通信の保護

ご使用のシステムが他のシステムとのネットワークに参加する場合、ご使用のシステムへの新たなドアが使用できるようになります。機密保護管理者は、APPC 環境におけるシステムへの入り口の制御に使用することができるオプションを知っておく必要があります。

拡張プログラム間通信機能 (APPC) は、パーソナル・コンピューターを含むコンピューターが相互に通信を行う一般的な方法です。ディスプレイ・パススルー、分散データ管理、および iSeries Access for Windows は、すべて APPC 通信を使用します。

この後で説明するトピックでは、APPC の作動方法と適切なセキュリティーのセットアップ方法について、基本的な情報の一部を説明します。これらのトピックは、主に APPC 構成のセキュリティー関連の要素に集中しています。この例をユーザーの状況に適応させるには、通信ネットワークを管理する担当者と (おそらく) アプリケーション・プロバイダーと一緒に作業を行う必要があります。これらの情報を基礎として使用して、セキュリティーの問題と APPC で使用できるオプションの理解に役立ててください。

セキュリティーは決して「自由な」ものではありません。ネットワーク・セキュリティーをより簡単にする提案は、ネットワーク管理をさらに困難にする可能性があります。例えば、ここでは、APPN® (Advanced Peer-to-Peer Networking®) を重視していません。これは、APPN を使用しない方がセキュリティーの理解および管理が簡単だからです。ただし、APPN を使用しない場合、ネットワーク管理者は、APPN が自動的に作成する構成情報を手動で作成しなければなりません。

PC も通信を使用する

PC を iSeries サーバーに接続するための多くの方法は、APPC や TCP/IP などの通信に依存します。以下のトピックを読むときには、他のシステムへの接続と PC への接続の両方に関するセキュリティーの問題を必ず考えてください。ネットワークの保護を計画する際には、ユーザーのシステムに接続している PC に悪い影響を絶対に与えないようにしてください。

APPC 用語

APPC は、あるシステムのユーザーが別のシステムで作業を行えるようにする機能を提供します。要求の開始元のシステムは、以下のいずれかの名前で呼ばれます。

- **ソース・システム**
- **ローカル・システム**
- **クライアント**

要求を受け取るシステムは、以下のいずれかの名前で呼ばれます。

- **ターゲット・システム**

- リモート・システム
- サーバー

APPC 通信の基本要素

機密保護管理者の観点から、以下のことをしておかないと、あるシステム (SYSTEMA) のユーザーは別のシステム (SYSTEMB) で意味のある作業を行うことができません。

- ソース・システム (SYSTEMA) にターゲット・システム (SYSTEMB) へのパスを用意しなければならない。このパスは、**APPC セッション**と呼ばれます。
- ターゲット・システムは、ユーザーを識別し、ユーザーとユーザー・プロファイルを関連付けておかなければならない。ターゲット・システムは、ソース・システムの暗号化アルゴリズムをサポートしていなければならない (詳しくは、 16 ページの『パスワード・レベル』を参照してください)。
- ターゲット・システムは、適切な環境 (実行管理機能値) を持つユーザーのジョブを開始しなければならない。

以降のトピックでは、これらの要素と、セキュリティーにこれらの要素を関連付ける方法について説明します。ターゲット・システムの機密保護管理者は、APPC ユーザーが絶対にセキュリティーに違反しないようにするための主要な責任があります。しかし、両方のシステムの機密保護管理者が一緒に作業することにより、APPC セキュリティー管理の作業はずっと簡単になります。

例: 基本 APPC セッション

APPC 環境において、あるシステムのユーザーまたはアプリケーションが別のシステムへのアクセスを要求すると、これらの 2 つのシステムはセッションをセットアップします。セッションを確立するために、システムは 2 つの一致する APPC 装置記述をリンクしなければなりません。 SYSTEMA 装置記述のリモート・ロケーション名 (RMTLOCNAME) パラメーターは、SYSTEMB 装置記述のローカル・ロケーション名 (LCLLOCNAME) パラメーターと一致しなければならず、またその逆も一致しなければなりません。

2 つのシステムが APPC セッションを確立するには、SYSTEMA と SYSTEMB の APPC 装置記述におけるロケーション・パスワードが同一でなければなりません。両方で *NONE を指定するか、両方で同一の値を指定する必要があります。

パスワードが *NONE 以外の値の場合、これらのパスワードは暗号化形式で保管され、送信されます。パスワードが一致した場合、システムはセッションを確立します。パスワードが一致しない場合、ユーザーの要求は拒否されます。システムがセッションを確立するためのロケーション・パスワードを指定すると、これは**セキュア・バインド**と呼ばれます。

注: すべてのコンピューター・システムがセキュア・バインド機能をサポートするわけではありません。

APPC セッションの制限

ソース・システムの機密保護管理者は、他のシステムへのアクセスを試行することができるユーザーを制御するためにオブジェクト権限を使用することができます。APPC 装置記述の共通権限を *EXCLUDE に設定し、特定のユーザーに *CHANGE 権限を与えます。 *ALLOBJ 特殊権限を持つユーザーが APPC 通信を使用しないようにするには、QLMTSECOFR システム値を使用します。

ターゲット・システムの機密保護管理者も、APPC 装置に対する権限を使用して、ユーザーがシステム上で APPC セッションを開始できないようにすることができます。しかし、どのユーザー ID が APPC 装置記述にアクセスしようとしているかを理解する必要があります。122 ページの『ターゲット・システムへの APPC ユーザーのアクセス』では、iSeries サーバーがユーザー ID と APPC セッション用の要求とを関連付ける方法について説明します。

注: システムの装置記述に対して権限を持つユーザーを検出するには、共通権限オブジェクトの印刷 (PRTPUBAUT *DEVD) コマンドと私用権限オブジェクトの印刷 (PRTPVTAUT *DEVD) コマンドを使用することができます。

システムで APPN を使用する際に、システムが選択した経路用に使用できる既存の装置が無い場合、APPN は新規の APPC 装置を自動的に作成します。 APPN を使用しているシステムの APPC 装置へのアクセスを制限する方法の 1 つは、権限リストを作成することです。権限リストには、APPC 装置に許可すべきユーザーのリストが含まれます。次に、コマンドのデフォルト変更 (CHGCMDDFT) コマンドを使用して CRTDEVAPPC コマンドを変更します。 CRTDEVAPPC コマンドの権限 (AUT) パラメーターに関しては、作成した権限リストにデフォルト値を設定します。

注: ご使用のシステムで英語以外の言語を使用している場合、システムで使用する各国語ごとに、QSYSxxxx ライブラリーでコマンドのデフォルト値を変更する必要があります。

(ユーザーまたはアプリケーションに代わって) システムでセッションを要求している別のシステムの正体の妥当性を検査するため、APPC 装置記述でロケーション・パスワード (LOCPWD) パラメーターを使用します。ロケーション・パスワードは、名前を偽っているシステムの検出に役立ちます。

ロケーション・パスワードを使用するときには、ネットワーク内の他のシステムの機密保護管理者と調整しなければなりません。また、APPC 装置記述および構成リストの作成や変更を行えるユーザーの制御をすることも必要です。システムで、APPC 装置および構成リストを処理するコマンドを使用するためには、*IOSYSCFG 特殊権限が必要です。

注: APPN を使用するときに、ロケーション・パスワードは、装置記述ではなく QAPPNRMT 構成リストに保管されます。

ターゲット・システムへの APPC ユーザーのアクセス

システムが APPC セッションを確立するときに、システムは、要求元のユーザーがターゲット・システムのドアを獲得するためのパスを作成します。その他のいくつかの要素は、ユーザーが他のシステムへの入り口を獲得するためにしなければならないことを決定します。

以降のトピックでは、APPC ユーザーがターゲット・システムへの入り口を獲得する方法を決める要素について説明します。

システム間でのユーザー情報の送信方法

APPC アーキテクチャーは、ユーザーに関するセキュリティー情報をソース・システムからターゲット・システムに送るための方法を 3 つ提供しています。これらの方法は、**アーキテクチャー・セキュリティー値**と呼ばれます。表 18 では、これらの方法を示します。

注: 「*AS/400 アドバンスト・シリーズ APPC プログラミング*」には、アーキテクチャー・セキュリティー値について詳しい情報が記載されています。

表 18. APPC アーキテクチャーのセキュリティー値

アーキテクチャー・セキュリティー値	ターゲット・システムへのユーザー ID 送信	ターゲット・システムへのパスワード送信
None	いいえ	いいえ
Same	はい [1]	注 2 を参照
Program	はい	はい [3]

注:

1. ソース・システムは、ターゲット・システムが SECURELOC(*YES) または SECURELOC(*VFYENCPWD) を指定している場合、ユーザー ID を送信します。
2. パスワードはソース・システムによって検査済みのため、ユーザーは要求時にパスワードを入力しません。 SECURELOC(*YES) および SECURELOC(*NO) の場合、ソース・システムはパスワードを送信しません。 SECURELOC(*VFYENCPWD) の場合、ソース・システムは保管された暗号化パスワードを取り出して、そのパスワードを (暗号化された形式で) 送信します。
3. パスワードが暗号化形式で送信されるのは、ソース・システムとターゲット・システムの両方がパスワードの暗号化をサポートしている場合です。それ以外の場合、パスワードは暗号化されません。

ユーザーが要求するアプリケーションは、アーキテクチャー・セキュリティー値を決定します。たとえば、SNADS は常に SECURITY(NONE) を使用します。 DDM は SECURITY(SAME) を使用します。ディスプレイ・パススルーの場合、ユーザーは、STRPASTHR コマンドのパラメーターを使用してセキュリティー値を指定します。

どの場合でも、ターゲット・システムは、ソース・システムで指定されたセキュリティー値を使用する要求を受け入れるかどうか選択します。場合によっては、ターゲット・システムが要求を完全に拒否することがあります。また、ターゲット・システムが別のセキュリティー値を強制使用する場合もあります。たとえば、ユーザーが STRPASTHR コマンドでユーザー ID とパスワードの両方を指定すると、要求は SECURITY(PGM) を使用します。しかし、ターゲット・システムで QRMTSIGN

システム値が *FRCSIGNON であると、ユーザーには「サインオン」画面が表示されたままになります。 *FRCSIGNON 設定の場合、システムは常に SECURITY(NONE) を使用します。これは、ユーザーが STRPASTHR コマンドでユーザー ID もパスワードも入力しないのと等価です。

注:

1. ソース・システムとターゲット・システムは、データの送信前にセキュリティー値を折衝します。たとえば、ターゲット・システムが SECURELOC(*NO) を指定し、要求が SECURITY(SAME) である場合、ターゲット・システムはソース・システムに SECURITY(NONE) を使用するように命令します。ソース・システムはユーザー ID を送信しません。
2. ターゲット・システムにおけるユーザーのパスワードの有効期限が切れていると、ターゲット・システムはセッション要求を拒否します。これは、パスワードを送信する接続要求にのみ適用されます。以下の要求が含まれています。
   - タイプ SECURITY(PROGRAM) のセッション要求。
   - SECURELOC 値が *VFYENCPWD であるときの、タイプ SECURITY(SAME) のセッション要求。

ネットワーク・セキュリティーの責任分担のオプション

ご使用のシステムがネットワークに参加する場合、ご使用のシステムに入ろうとしているユーザーの正体の妥当性検査を他のシステムに任せるかどうか、決めておかなければなりません。 USERA が本当に USERA である (または QSECOFR が本当に QSECOFR である) ことを保証する SYSTEMA を信用するかどうか、あるいは、ユーザーにユーザー ID とパスワードをもう一度入力してもらう必要があるかどうかを決定します。

ターゲット・システムにおける APPC 装置記述のセキュア・ロケーション (SECURELOC) パラメーターは、ソース・システムがセキュア (トラステッド) ロケーションであるかどうかを指定します。

両方のシステムが *VFYENCPWD をサポートするリリースを実行しているときに、アプリケーションで SECURITY(SAME) を使用すると、SECURELOC(*VFYENCPWD) は追加保護を提供します。要求元は要求時にパスワードを入力しませんが、ソース・システムはユーザーのパスワードを取り出して、要求と一緒にそのパスワードを送信します。要求が正常終了するには、ユーザーが両方のシステムで同一のユーザー ID とパスワードを持っていなければなりません。

ターゲット・システムが SECURELOC(*VFYENCPWD) を指定したものの、ソース・システムがこの値をサポートしないときには、ターゲット・システムは要求を SECURITY(NONE) として処理します。

124 ページの表 19 は、アーキテクチャー・セキュリティー値と SECURELOC 値が一緒に動作する方法を示します。

表 19. APPC セキュリティー値と SECURELOC 値を組み合わせた場合の動作方法

ソース・システム	ターゲット・システム	
アーキテクチャー・セキュリティー値	**SECURELOC 値**	**ジョブのユーザー・プロファイル**
None	任意の値	デフォルト・ユーザー [1]
Same	*NO	デフォルト・ユーザー [1]
	*YES	ソース・システムの要求元と同じユーザー・プロファイル名
	*VFYENCPWD	ソース・システムの要求元と同じユーザー・プロファイル名。ユーザーは、両方のシステムで同じパスワードを使用しなければなりません。
Program	任意の値	ソース・システムからの要求で指定されたユーザー・プロファイル。

注:

1. デフォルト・ユーザーは、サブシステム記述の通信項目で判別されます。『ジョブのユーザー・プロファイルのターゲット・システム割り当て』では、このことについて説明します。

ジョブのユーザー・プロファイルのターゲット・システム割り当て

ユーザーが別のシステムの APPC ジョブを要求するとき、その要求には、関連したモード名が含まれています。モード名は、ユーザーの要求に由来する場合もあれば、ソース・システムのネットワーク属性のデフォルト値である場合もあります。

ターゲット・システムは、ジョブの実行方法を判別するのに、モード名と APPC 装置名を使用します。ターゲット・システムは、活動状態のサブシステムを検索して、APPC 装置名とモード名に最も合った通信項目がないかどうか調べます。

通信項目は、システムが SECURITY(NONE) 要求用に使用するユーザー・プロファイルを指定します。次に、サブシステム記述における通信項目の例を示します。

```
                          通信項目の表示

サブシステム記述:   QCMN            状況:     活動

                                ジョブ                      省略時の      最大
装置          モード            記述          ライブラリー  ユーザー      活動
*ALL          *ANY              *USRPRF                     *SYS          *NOMAX
*ALL          QPCSUPP           *USRPRF                     *NONE         *NOMAX
```

表 20 は、通信項目におけるデフォルト・ユーザー・パラメーターに使用できる値を示したものです。

表 20. デフォルト・ユーザー・パラメーターに有効な値

値	結果
***NONE**	デフォルト・ユーザーは使用できません。ソース・システムが要求時にユーザー ID を提供しないと、ジョブは実行されません。

表 20. デフォルト・ユーザー・パラメーターに有効な値 (続き)

値	結果
***SYS**	IBM 提供のプログラム (システム・ジョブ) だけが実行されます。ユーザー・アプリケーションは実行されません。
USER-NAME	ソース・システムがユーザー ID を送信しない場合、ジョブはこのユーザー・プロファイルの下で実行されます。

デフォルト・ユーザー・プロファイルが指定された通信項目をもつすべてのサブシステムのリストを印刷するのに、サブシステム記述印刷 (PRTSBSDAUT) コマンドを使用することができます。

ディスプレイ・パススルー・オプションの表示

ディスプレイ・パススルーは、APPC 通信を使用するアプリケーションの一例です。ディスプレイ・パススルーを使用して、ネットワークを介してご使用のシステムに接続されている別のシステムにサインオンすることができます。

表 21 は、パススルー要求 (STRPASTHR コマンド) の例と、ターゲット・システムがこれらの要求を処理する方法を示します。ディスプレイ・パススルーの場合、システムは APPC 通信の基本要素とリモート・サインオン (QRMTSIGN) システム値を使用します。

注: ディスプレイ・パススルー要求は、QCMN または QBASE サブシステムに経路指定されなくなりました。 V4R1 からは、QSYSWRK サブシステムに経路指定されています。V4R1 よりも前のリリースでは、QCMD あるいは QBASE サブシステムを開始しないようにすることで、ディスプレイ・パススルーは動作しないものとしていました。現在ではこれは当てはまりません。QPASTHRSVR システム値を 0 に変更することにより、強制的にディスプレイ・パススルーを QCMN (QBASE が活動状態の場合は QBASE) に経路指定できます。

表 21. パススルー・サインオン要求の例

STRPASTHR コマンドの値		ターゲット・システム		
ユーザー ID	**パスワード**	**SECURELOC 値**	**QRMTSIGN 値**	**結果**
*NONE	*NONE	任意の値	任意の値	ユーザーはターゲット・システムにサインオンしなければなりません。
ユーザー・プロファイル名	入力されない	任意の値	任意の値	要求は失敗します。

表 21. パススルー・サインオン要求の例 (続き)

STRPASTHR コマンドの値		ターゲット・システム		
ユーザー ID	**パスワード**	**SECURELOC 値**	**QRMTSIGN 値**	**結果**
*CURRENT	入力されない	*NO	任意の値	要求は失敗します。
		*YES	*SAMEPRF	対話型ジョブは、ソース・システムのユーザー・プロファイルと同じユーザー・プロファイル名を使用して開始します。リモート・システムにはパスワードは渡されません。ターゲット・システムにユーザー・プロファイル名が存在しなければなりません。
			*VERIFY	
			*FRCSIGNON	ユーザーはターゲット・システムにサインオンしなければなりません。
		*VFYENCPWD	*SAMEPRF	対話型ジョブは、ソース・システムのユーザー・プロファイルと同じユーザー・プロファイル名を使用して開始します。ソース・システムはユーザーのパスワードを検索し、それをリモート・システムに送信します。ターゲット・システムにユーザー・プロファイル名が存在しなければなりません。
			*VERIFY	
			*FRCSIGNON	ユーザーはターゲット・システムにサインオンしなければなりません。
*CURRENT (またはジョブ用の現行ユーザー・プロファイルの名前)	入力される	任意の値	*SAMEPRF	対話型ジョブは、ソース・システムのユーザー・プロファイルと同じユーザー・プロファイル名を使用して開始します。パスワードはリモート・システムに送信されます。ターゲット・システムにユーザー・プロファイル名が存在しなければなりません。
			*VERIFY	
			*FRCSIGNON	ユーザーはターゲット・システムにサインオンしなければなりません。

表 21. パススルー・サインオン要求の例 (続き)

STRPASTHR コマンドの値		ターゲット・システム		
ユーザー ID	**パスワード**	**SECURELOC 値**	**QRMTSIGN 値**	**結果**
ユーザー・プロファイル名 (ジョブ用の現行ユーザー・プロファイルとは別の 名前)	入力される	任意の値	*SAMEPRF	要求は失敗します。
			*VERIFY	対話型ジョブは、ソース・システムのユーザー・プロファイルと同じユーザー・プロファイル名を使用して開始します。パスワードはリモート・システムに送信されます。ターゲット・システムにユーザー・プロファイル名が存在しなければなりません。
			*FRCSIGNON	対話式ジョブは、指定されたユーザー・プロファイル名で開始します。パスワードはターゲット・システムに送信されます。ターゲット・システムにユーザー・プロファイル名が存在しなければなりません。

予期しない装置割り当ての回避

活動中の装置で障害が起こると、システムは回復を試みます。場合によっては、接続が中断されると、別のユーザーが障害の起こったセッションを意図的にではなく再確立してしまう可能性があります。たとえば、USERA がサインオフしないでワークステーションの電源を切ったことを想定してください。 USERB はワークステーションの電源を入れて、サインオンせずに USERA のセッションを再始動することができます。

このようなことが起こるのを防ぐため、装置の入出力エラー・アクション (QDEVRCYACN) システム値を *DSCMSG に設定します。装置に障害が起こると、システムはユーザーのジョブを終了します。

リモート・コマンドとバッチ・ジョブの制御

システムで実行することのできるリモート・コマンドおよびジョブの制御に役立てるため、いくつかのオプションを使用することができます。オプションには、以下のものが含まれます。

- システムが DDM を使用する場合、ユーザーが別のシステムからリモート・コマンド投入 (SBMRMTCMD) コマンドを使用できないようにするために、DDM ファイルへのアクセスを制限することができます。 SBMRMTCMD を使用するには、ユーザーは DDM ファイルをオープンできなければなりません。また、DDM ファイルを作成する機能を制限する必要もあります。
- DDM 要求アクセス (DDMACC) システム値用の出口プログラムを指定することができます。出口プログラムでは、DDM 要求を許可する前に、すべての DDM 要求を評価することができます。

- ネットワーク・ジョブを投入できないようにしたり、ネットワーク・ジョブを自動的に実行できないようにするために、ネットワーク・ジョブのアクション (JOBACN) ネットワーク属性を使用することができます。
- サブシステム記述から PGMEVOKE 経路指定項目を除去することによって、通信環境で実行できるプログラム要求を明示的に指定することができます。PGMEVOKE 経路指定項目により、要求元は実行するプログラムを指定することができます。 QCMN サブシステム記述などのサブシステム記述からこの経路指定項目を取り除くときに、正常に実行する必要のある通信要求用の経路指定項目を追加しなければなりません。

  100 ページの『構造化 TPN 要求』は、IBM 提供のアプリケーションによる通信要求用のプログラム名のリストです。許可したいそれぞれの要求ごとに、プログラム名と同じ比較値とプログラム名をもつ経路指定項目を追加することができます。

  この方法を使用するときには、システムにおける実行管理機能環境とシステムで発生する通信要求のタイプを理解する必要があります。できれば、経路指定項目の変更後に通信要求のすべてのタイプをテストして、通信要求が正しく作動することを確認してください。通信要求が使用可能な経路指定項目を検出しないと、ユーザーは CPF1269 メッセージを受け取ります。別の方法 (エラーが起こる可能性は低いが、おそらくは効果がやや薄い) は、システムで実行させたくないトランザクション・プログラムの共通権限を *EXCLUDE に設定することです。

  注: 「*AS/400e シリーズ 実行管理の手引き*」には、経路指定項目と、システムのプログラム開始要求の処理方法とについて詳しく記載してあります。

APPC 構成の評価

通信セキュリティー印刷 (PRTCMNSEC) コマンドまたはメニュー・オプションを使用すると、APPC 構成におけるセキュリティー関連の値を印刷することができます。以降のトピックに、報告書に関する説明があります。

APPC 装置の関連パラメーター

図 9 は、装置記述の通信情報報告書の一例です。 129 ページの図 10 は、構成リストのための報告書の一例です。報告書に続いて、報告書のフィールドの説明を行います。

```
                                通信情報 (全報告書)
5722SS1 VXRXMX  000000                                                  SYSTEM4
 オブジェクト・タイプ . . . . . :   *DEVD

                                                                                SNUF
 オブジェクト   オブジェクト   装置          ロケーション  ロケーション・          単一        事前確立    プログラム
 名             タイプ         カテゴリー    保護          パスワード    APPN 可能  セッション  セッション  開始

 CDMDEV1        *DEVD          *APPC         *NO           *NO           *NO        *YES        *NO
 CDMDEV2        *DEVD          *APPC         *NO           *NO           *NO        *YES        *NO
```

図 9. APPC 装置記述 - 報告書例

```
                        構成リスト表示                                ページ 1
5722SS1 VXRXMX  000000                              SYSTEM4   01/02/07  10:48
 構成リスト . . . . . . . . . . . . :   CFGD        QAPPNRMT
 構成リスト・タイプ . . . . . . . . :   CFGTYPE     *APPNRMT
 テキスト . . . . . . . . . . . . . :   TEXT
 ----------------APPN リモート・ロケーション ----------------
                リモート・                      リモート    制御点
 リモート・     ネットワーク     ローカル・     制御        ネットワーク     保護
 ロケーション   ID               ロケーション   点          ID               ロケーション
 SYSTEM36       APPN             SYSTEM4        SYSTEM36    APPN             *NO
 SYSTEM32       APPN             SYSTEM4        SYSTEM32    APPN             *NO
 SYSTEMU        APPN             SYSTEM4        SYSTEM33    APPN             *YES
 SYSTEMJ        APPN             SYSTEM4        SYSTEMJ     APPN             *NO
 SYSTEMR2       APPN             SYSTEM4        SYSTEM1     APPN             *NO
 ------------------APPN リモート・ロケーション ------------------
                リモート・                                                  ローカル
 リモート・     ネットワーク     ローカル・     単一        会話             制御        事前確立
 ロケーション   ID               ロケーション   セッション  の数             点          セッション数
 SYSTEM36       APPN             SYSTEM4        *NO           10             *NO         *NO
 SYSTEM32       APPN             SYSTEM4        *NO           10             *NO         *NO
```

図 10. 構成リスト報告書 - 例

ロケーション保護フィールド

ロケーション保護 (SECURELOC) フィールドは、リモート・システムがローカル・システムに代わってパスワード検証を行うことを、ローカル・システムが信用するかどうかを指定します。 SECURELOC フィールドは、DDM や CPI 通信 API を使用するアプリケーションなどの SECURITY(SAME) 値を使用するアプリケーションにのみ適用されます。

SECURELOC(*YES) は、リモート・システムに生じる可能性がある欠点に対して、ローカル・システムを無防備な状態にします。両方のシステムに存在するどんなユーザーでも、ローカル・システムのプログラムを呼び出すことができます。これは特に危険です。QSECOFR (機密保護担当者) ユーザー・プロファイルはすべての iSeries システムに存在し、*ALLOBJ 特殊権限を持っているためです。ネットワーク上のあるシステムが QSECOFR パスワード保護の仕事を適切に処理しない場合は、そのシステムをロケーション保護として扱っている他のシステムは危険にさらされます。

SECURELOC(*VFYENCPWD) を使用すると、システムにとって、適切にパスワードを保護しない他のシステムに対する無防備さは弱まります。 SECURITY(SAME) を使用するアプリケーションを要求するユーザーは、両方のシステムで同一のユーザー ID とパスワードを持つ必要があります。 SECURELOC(*VFYENCPWD) では、ユーザーがすべてのシステムで同一のパスワードを持つために、ネットワーク全体のパスワード管理ポリシーが必要です。

注: SECURELOC(*VFYENCPWD) は、V3R2、V3R7、または V4R1 で実行中のシステム間でのみサポートされます。ターゲット・システムが SECURELOC(*VFYENCPWD) を指定しても、ソース・システムがこの機能をサポートしないと、要求は SECURITY(NONE) として扱われます。

システムが SECURELOC(*NO) を指定した場合、SECURITY(SAME) を使用するアプリケーションには、プログラムを実行するためのデフォルト・ユーザーが必要に

なります。デフォルト・ユーザーは、装置記述と要求に関連したモードとに依存します。 (124 ページの『ジョブのユーザー・プロファイルのターゲット・システム割り当て』を参照してください。)

ロケーション・パスワード・フィールド

ロケーション・パスワード・フィールドは、2 つのシステムが、要求元システムが名前を偽っているシステムでないことを検証するためにパスワードを交換するかどうかを決定します。 120 ページの『例: 基本 APPC セッション』で、ロケーション・パスワードについての詳しい説明をします。

APPN 可能フィールド

APPN 可能 (APPN) フィールドは、リモート・システムが拡張ネットワーキング機能をサポートできるか、あるいはホップ 1 回の接続に限定されるかを指定します。APPN(*YES) の意味は以下のとおりです。

- リモート・システムがネットワーク・ノードの場合、リモート・システムはローカル・システムを他のシステムに接続できる。これは、**中間ノード経路指定**と呼ばれます。これは、システムのユーザーがリモート・システムを大規模ネットワークの経路として使用できることを意味します。
- ローカル・システムがネットワーク・ノードの場合、リモート・システムはローカル・システムを使用して、他のシステムに接続することができる。リモート・システムのユーザーは、ローカル・システムを大規模ネットワークの経路として使用できます。

  注: システムがネットワーク・ノードであるか、エンド・ノードであるかを判別するのに、DSPNETA コマンドを使用することができます。

単一セッション・フィールド

単一セッション (SNGSSN) フィールドは、リモート・システムが、同一の APPC 装置記述を使用して同時に複数のセッションを実行できるかどうかを指定します。SNGSSN(*NO) が一般的に使用されますが、これは、リモート・システム用の複数の装置記述を作成する必要をなくすためです。たとえば、PC ユーザーはしばしば、複数の 5250 エミュレーション・セッションと、ファイル・サーバー機能、および印刷サーバー機能用のセッションを必要とします。 SNGSSN(*NO) を指定すると、これらの機能に、iSeries システムの PC 用の 1 つの装置記述を提供することができます。

SNGSSN(*NO) は、PC ユーザーと他の APPC ユーザーのセキュリティーを意識した操作手順に依存しなければならないということです。既存のセッションと同じ装置記述を使用して、システムは、未許可セッションを開始しようとするリモート・システム上のユーザーに対して無防備になります。 (この行為は**結合処理**と呼ばれることがあります。)

事前確立セッション・フィールド

単一セッション装置用の事前確立 (PREESTSSN) セッション・フィールドは、リモート・システムが最初にローカル・システムに接続したときに、ローカル・システムがリモート・システムとのセッションを開始するかどうかを制御します。PREESTSSN(*NO) は、アプリケーションがシステムとのセッションを要求するまで

は、ローカル・システムがセッションを開始するのを待機するということです。 PREESTSSN(*YES) は、アプリケーション・プログラムの接続が完了するまでの所要時間を最短にするのに役立ちます。

PREESTSSN(*YES) は、システムが、使用されていない交換 (ダイヤルアップ) 回線を切断しないようにします。アプリケーションまたはユーザーが、明示的に回線をオフにしなければなりません。 PREESTSSN(*YES) は、ローカル・システムがセッションに伴う結合処理に対して無防備な状態にある時間を延ばす恐れがあります。

SNUF プログラム開始フィールド

SNUF プログラム開始フィールドは、リモート・システムがローカル・システムでプログラムを開始することを、許可するかどうかを指定します。 *YES は、リモート・システムのユーザーがジョブを開始して、ローカル・システムでプログラムを実行するには、ローカル・システムのオブジェクト権限体系がオブジェクトの保護に適している必要があるということです。

APPC 制御装置のパラメーター

図 11 は、制御装置記述の通信情報報告書の一例です。報告書に続いて、報告書のフィールドについての説明があります。

```
                                通信情報 (全報告書)
5722SS1 VXRXMX  000000                                                SYSTEM4
 オブジェクト・タイプ . . . . . :   *CTLD

 オブジェクト  オブジェクト  制御装置                交換制御                                CP          切断      自動削除
 名            ・タイプ      カテゴリー    自動作成  装置      呼出方向  APPN 可能  セッション数  タイマー  分数      装置名
 CTL01         *CTLD         *APPC         *YES      *YES      *DIAL     *YES       *YES              0      1440    AARON
 CTL02         *CTLD         *APPC         *YES      *YES      *DIAL     *YES       *YES              0      1440    BASIC
 CTL03         *CTLD         *APPC         *YES      *YES      *DIAL     *YES       *YES              0      1440    *NONE
```

図 11. APPC 制御装置記述 - 報告書例

自動作成フィールド

回線記述では、自動作成 (AUTOCRTCTL) フィールドは、着信要求が一致する制御装置記述を検出できないときに、ローカル・システムが自動的に制御装置記述を作成するかどうかを指定します。制御装置記述の、装置自動作成 (AUTOCRTDEV) フィールドは、着信要求が一致する装置記述を検出できないときに、ローカル・システムが自動的に装置記述を作成するかどうかを指定します。

APPN 可能の制御装置の場合、自動作成フィールドは効力を持ちません。システムは、自動作成フィールドの設定に関係なく、必要なときに装置記述を自動的に作成します。

回線記述に *YES を指定すると、回線にアクセスしているだれもがユーザーのシステムに接続できるようになります。これには、ブリッジとルーターで接続されるサイトも含まれます。

制御点 (CP) セッション・フィールド

APPN 可能制御装置の場合、制御点セッション (CPSSN) フィールドは、システムがリモート・システムとの APPC 接続を自動的に確立するかどうかを制御します。システムは、ネットワーク情報および状況をリモート・システムと交換するのに CP

セッションを使用します。 APPN ネットワーク・ノード間での最新の情報の交換は、ネットワークが円滑に機能するために特に重要です。

*YES を指定すると、活動停止中の交換回線は自動的には切断されません。これにより、システムは結合処理セッションに対してより無防備な状態になります。

切断タイマー・フィールド

APPC 制御装置の場合、切断タイマー・フィールドは、システムがリモート・システムへの回線を切断するまでに、制御装置を未使用にする (活動セッションがない) 時間を指定します。このフィールドには 2 つの値があります。最初の値は、制御装置が最初に接続されたときから、その制御装置が活動状態のままでいる時間を指定します。 2 番目の値は、制御装置の最後のセッションが終了してからシステムが回線を落とすまでに、システムが待機する時間を決定します。

システムは、交換切断 (SWTDSC) フィールドが *YES のときにのみ切断タイマーを使用します。

これらの値を大きくすると、システムは結合処理セッションに対して、より無防備な状態になります。

回線記述のパラメーター

図 12 は、回線記述の通信情報報告書の一例です。報告書に続いて、報告書のフィールドについての説明があります。

```
                                通信情報 (全報告書)
5722SS1 VXRXMX  000000                                                  SYSTEM4

 オブジェクト・タイプ . . . . . :   *LIND

 オブジェクト    オブジェクト    回線                    自動削除                    自動
 名              ・タイプ        カテゴリー      自動作成  分数          自動応答      ダイヤル
 LINE01          *LIND           *SDLC           *NO             0       *NO           *NO
 LINE02          *LIND           *SDLC           *NO             0       *YES          *NO
 LINE03          *LIND           *SDLC           *NO             0       *NO           *NO
 LINE04          *LIND           *SDLC           *NO             0       *YES          *NO
```

図 12. APPC 回線記述 - 報告書例

自動応答フィールド

自動応答 (AUTOANS) フィールドは、交換回線がオペレーターの介在なしに着呼を受け入れるかどうかを指定します。

*YES を指定すると、システムへより簡単にアクセスできるため、システムの保護は低くなります。 *YES を指定したときの機密漏れを最小化するため、回線が不要になったときに、その回線をオフにしてください。

自動ダイヤル・フィールド

自動ダイヤル (AUTODIAL) フィールドは、交換回線がオペレーターの介在なしに発呼を行えるかどうかを指定します。 *YES を指定すると、通信回線およびモデムに物理的にアクセスしていないローカル・ユーザーが他のシステムに接続できるようになります。

第 13 章 TCP/IP 通信の保護

TCP/IP (伝送制御プロトコル / インターネット・プロトコル) は、すべてのタイプのコンピューターが互いに通信を行う一般的な方法です。 TCP/IP アプリケーションは広く知られているもので、「情報ハイウェイ」を介して広範囲で使用されています。

この章では、以下のことに関するヒントを説明します。

- TCP/IP アプリケーションがシステムで稼働しないようにする。
- TCP/IP アプリケーションのシステムでの稼働を許可したときに、システム資源を保護する。

TCP/IP アプリケーション全般については、「iSeries Information Center」—>「ネットワーキング」—>「TCP/IP」を参照してください。 iSeries サーバーをインターネット (非常に大規模な TCP/IP ネットワーク) またはイントラネットのいずれかに接続する際のセキュリティーの考慮事項については、「*IBM SecureWay®: iSeries とインターネット*」 (「iSeries Information Center」—>「セキュリティー」—>「SecureWay」) を参照してください。 iSeries Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。

iSeries サーバーは多くの TCP/IP アプリケーションをサポートすることを覚えておいてください。システムで 1 つの TCP/IP アプリケーションを許可することを決めると、その他の TCP/IP アプリケーションも使用できるようになります。機密保護管理者は、TCP/IP アプリケーションの範囲と、これらのアプリケーションのセキュリティーへの関与に注意しておく必要があります。

TCP/IP 処理の防止

TCP/IP サーバー・ジョブは QSYSWRK サブシステムで実行されます。システムで TCP/IP を開始するには、TCP/IP 開始 (STRTCP) コマンドを使用します。どのような TCP/IP 処理や TCP/IP アプリケーションも実行したくない場合は、STRTCP コマンドを使用しないでください。システムは、STRTCP コマンドの共通権限が *EXCLUDE に設定された状態で出荷されます。

(たとえば、オフの時間に) コマンドにアクセスできる誰かが TCP/IP を開始していると思われる場合、STRTCP コマンドに関してオブジェクト監査をセットアップすることができます。ユーザーがコマンドを実行するたびに監査ジャーナル項目が作成されます。

TCP/IP セキュリティーの構成要素

ネットワーク・セキュリティーを強化すると同時に、柔軟性を向上させるいくつかの TCP/IP セキュリティー構成要素を利用することができます。これらのテクノロジーの一部はファイアウォール製品にも見られますが、OS/400 の TCP/IP セキュリティー構成要素はファイアウォールとして使用することが目的ではありません。しかし、これらの機能の一部を使用すると、場合によっては、別のファイアウォー

ル・プロダクトが不要になります。また、これらの TCP/IP 機能を使用して、すでにファイアウォールを使用している環境に付加的なセキュリティーを提供できる場合もあります。

以下の構成要素を使用して、TCP/IP セキュリティーを拡張することができます。

- パケット・ルール
- HTTP Proxy サーバー
- VPN (仮想プライベート・ネットワーク)
- SSL (secure sockets layer)

パケット・ルールの使用による TCP/IP トラフィックの保護

パケット・ルールとは、IP フィルター操作とネットワーク・アドレス変換 (NAT) を組み合わせたもので、侵入者から内部のネットワークを保護するファイアウォールのような働きをします。 IP フィルター操作では、IP トラフィックのネットワークへの出入りを制御できます。基本的に、定義した規則に従ってパケットをフィルターにかけることでネットワークを保護します。一方、NAT では、一連の登録済み IP アドレスの後ろに未登録のプライベート IP アドレスを隠すことができます。これにより、外部ネットワークから内部ネットワークを保護することができます。また、NAT を利用すれば、少数の登録済みアドレスで数多くのプライベート・アドレスを表せるため、 IP アドレス不足の緩和にも役立ちます。詳細については、iSeries Information Center を参照してください。

HTTP proxy サーバー

HTTP proxy サーバーは、 IBM HTTP Server for iSeries サーバーに付属しています。 HTTP サーバーは、OS/400 の一部です。proxy サーバーは、Web ブラウザーから HTTP 要求を受け取り、それらの要求を Web サーバーに再送します。要求を受け取る Web サーバーは、proxy サーバーの IP アドレスだけしか認知しないため、それらの要求の発信元である PC の名前やアドレスを判別することはできません。 proxy サーバーは、HTTP、FTP、Gopher、および WAIS 用の URL 要求を処理することができます。

proxy サーバーは、すべての proxy サーバー・ユーザーによって作成された要求から戻された Web ページをキャッシュに入れます。その結果、ユーザーがページを要求すると、proxy サーバーは、そのページがキャッシュに入っているかどうかチェックします。そのページがキャッシュ内にあると、proxy サーバーはキャッシュ・ページを戻します。キャッシュ・ページを使用することにより、proxy サーバーは Web ページのサービスをより迅速に行うことができます。そして、Web サーバーに対して時間のかかる可能性がある要求を取り除きます。

proxy サーバーは、トラッキングの目的で、すべての URL 要求をログに記録することもできます。そして、そのログを検討して、ネットワーク資源の使用および誤用をモニターすることができます。

Web アクセスを強化するため、IBM HTTP SERVER で HTTP proxy サポートを使用することができます。 PC クライアントのアドレスは、クライアントがアクセスする Web サーバーには隠されています。つまり、proxy サーバーの IP アドレスだけが認知されています。 Web ページのキャッシュは、通信帯域幅要件とファイアウォール作業負荷も減らすことができます。詳細については、 IBM HTTP Server

for iSeries のホーム・ページ (http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html) を参照してください。

仮想プライベート・ネットワーク (VPN)

仮想プライベート・ネットワーク (VPN) を利用すれば、インターネットなどの公衆ネットワークの既存のフレームワークの上に、専用のイントラネットをセキュアに拡張することができます。 VPN では、ネットワーク・トラフィックを制御できるだけでなく、認証やデータ・プライバシーなどの重要なセキュリティー機能を提供することもできます。

OS/400 VPN は、 OS/400 のグラフィカル・ユーザー・インターフェース (GUI) である、 iSeries ナビゲーターのオプションで導入可能な構成要素です。さまざまなホストとゲートウェイの組み合わせの間でセキュアなエンドツーエンド・パスを作成することができます。 OS/400 VPN は、認証方式、暗号化アルゴリズムなどの事前対策を使用して、接続の 2 端点間で送信されるデータのセキュリティーを確保します。

VPN は、TCP/IP 階層通信スタック・モデルのネットワーク層で実行されます。特に、VPN は IP セキュリティー・アーキテクチャー (IPSec) オープン・フレームワークを使用します。 IPSec は、インターネットの基本セキュリティー機能だけでなく、堅固でセキュアな仮想プライベート・ネットワークを作成できる柔軟性の高い構築ベースも提供します。

VPN は、Layer 2 Tunnel Protocol (L2TP) VPN ソリューションもサポートしています。 L2TP 接続は、仮想回線とも呼ばれ、企業ネットワーク・サーバーを使用してリモート・ユーザーに割り当てる IP アドレスを管理することで、コスト効率の良いリモート・ユーザー・アクセスを実現します。さらに、L2TP 接続では、システムやネットワークの保護に IPSec を使用していれば、それらへのセキュアなアクセスも提供します。

VPN がネットワーク全体に与える影響を理解することは重要です。 VPN 接続を成功させるために一番大切なことは、適正な計画とインプリメンテーションです。 iSeries Information Center の『VPN』トピックを参照し、VPN の動作とその使用方法を確実に習得してください。詳細については、「iSeries Information Center」—> 「セキュリティー」—>「仮想プライベート・ネットワーク」を参照してください。 iSeries Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) は、非保護ネットワーク (インターネットなど) を介して、アプリケーションでセキュアな通信セッションを行えるようにするための業界標準になっています。SSL プロトコルは、クライアントと通信セッションの一端または両端を認証するサーバー・アプリケーション間でセキュアな接続を確立します。 SSL は、クライアントとサーバー・アプリケーション間でやり取りするデータのプライバシーと保全性も維持します。詳細については、「iSeries Information Center」->「セキュリティー」—>「Secure Sockets Layer (SSL)」を参照してくださ

い。 iSeries Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。

TCP/IP 環境の保護

このトピックでは、システムで TCP/IP 環境における機密漏れを減らすために実行できるステップの一般的な提案を行います。これらのヒントは、以降のトピックで説明を行う特定のアプリケーションに対してというよりも、TCP/IP 環境全体に適用されます。

- TCP/IP ポート用のアプリケーションを作成するときには、必ずアプリケーションを適切に保護してください。部外者がそのポートを通じてそのアプリケーションにアクセスしようとしていることを想定してください。知識のある部外者は、そのアプリケーションに Telnet での接続を試行する可能性もあります。
- システムの TCP/IP ポートの使用法をモニターしてください。 TCP/IP ポートに関連したユーザー・アプリケーションは、ユーザー ID やパスワードを入力しなくても、「裏口」からシステムに入れるようにしてしまうおそれがあります。システムにおける十分な権限を持っている者は、TCP ポートまたは UDP ポートにアプリケーションを関連付ける可能性があります。
  - 機密保護管理者は、ハッカーが使用する *IP スプーフィング* という技法に注意してください。TCP/IP ネットワークのすべてのシステムには IP アドレスがあります。IP スプーフィングを使用する者は、システム (通常は PC) をセットアップして、既存の IP アドレスまたはトラステッド IP アドレスであるように見せかけます。そのため、他の名前をかたって、ユーザーが通常接続している先のシステムであるようなふりをして、システムとの接続を確立する可能性があります。

    システムで TCP/IP を実行し、さらにシステムが物理的に保護されていないネットワーク (すべての非交換回線と事前定義リンク) に参加している場合には、IP のスプーフィングに対して無防備になっています。「スプーファー (送信偽装者)」による損傷からシステムを保護するには、この章におけるサインオン保護やオブジェクト・セキュリティーなどの提案の実行を開始してください。また、システムに適切な補助記憶装置の制限も必ず設定してください。これにより、スプーファー (送信偽装者) がメールやスプール・ファイルで補助記憶域をシステムが操作不能になるまであふれさせないようにします。

    さらに、システムにおける TCP/IP 活動を定期的にモニターしてください。 IP スプーフィングを検出した場合には、TCP/IP のセットアップにおける弱点を発見し、調整するようにしてください。
  - イントラネット (外部に直接接続する必要のないシステムのネットワーク) の場合、再使用可能の IP アドレスを使用します。再使用可能アドレスは、私設ネットワーク内での使用を意図したものです。インターネット・バックボーンは、再使用可能 IP アドレスをもつパケットを経路指定しません。そのため、再使用可能アドレスは、ユーザーのファイアウォール内での保護を追加する層を提供します。

    IP アドレスの割り当て方法と IP アドレスの範囲、および TCP/IP のセキュリティー情報については、「iSeries Information Center」—>「ネットワーキング」—>「TCP/IP」を参照してください。

- インターネットまたはイントラネットにシステムを接続することを考えている場合は、「*IBM SecureWay: iSeries とインターネット*」 (「iSeries Information Center」—>「セキュリティー」—>「SecureWay」) を参照してください。 iSeries Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。

自動的に開始する TCP/IP サーバーの制御

機密保護管理者は、TCP/IP の開始時に自動的に開始する TCP/IP アプリケーションを制御する必要があります。TCP/IP の開始には、2 つのコマンドが使用できます。それぞれのコマンドごとに、システムは別々の方法を使用して、開始するアプリケーション (サーバー) を判別します。

表 22 は、2 つのコマンドと、それらのコマンドに対応したセキュリティーの推奨事項を示します。 138 ページの表 23 は、サーバー用のデフォルトの自動開始値を示します。サーバーの自動開始値を変更するには、そのサーバーに対して CHGxxxA (xxx 属性の変更) コマンドを使用します。たとえば、TELNET に対するコマンドは、CHGTELNA になります。

表 22. TCP/IP コマンドが開始すべきサーバーを判別する方法

コマンド	開始するサーバー	セキュリティーの推奨事項
TCP/IP 開始 (STRTCP)	システムは、AUTOSTART(*YES) が指定されているすべてのサーバーを開始する。 138 ページの表 23 は、それぞれの TCP/IP サーバーごとの出荷時の値を示します。	• 自動開始設定を変更することのできるユーザーを制御するために、注意して *IOSYSCFG 特殊権限を割り当てる。 • STRTCP コマンドを使用できる権限を持つユーザーの制御を注意して行う。このコマンドのデフォルトの共通権限は *EXCLUDE です。 • サーバーの AUTOSTART 値を変更しようとしているユーザーをモニターするために、サーバー名 属性変更コマンド (CHGTELNA など) に対するオブジェクト監査をセットアップする。
TCP/IP サーバー開始 (STRTCPSVR)	開始すべきサーバーを指定するためにパラメーターを使用する。このコマンドの出荷時のデフォルトは、全サーバーの開始です。	• コマンドのデフォルト変更 (CHGCMDDFT) コマンドを使用して、特定のサーバーだけを開始するように STRTCPSVR コマンドをセットアップする。これにより、ユーザーが他のサーバーを開始できなくなるわけではありません。しかし、コマンドのデフォルトを変更することにより、ユーザーが誤ってすべてのサーバーを開始してしまう可能性はほとんどなくなります。たとえば、`CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')` というコマンドを使用して、Telnet サーバーだけが開始するようにデフォルトを設定します。 **注:** デフォルト値を変更するときに、1 つのサーバーだけを指定することができます。定期的に使用するサーバーか、機密漏れの原因には最もなりえない (TFTP などの) サーバーのいずれかを選択してください。 • STRTCPSVR コマンドを使用できる権限を持つユーザーの制御を注意して行う。このコマンドのデフォルトの共通権限は *EXCLUDE です。

次の表に、TCP/IP サーバーの自動開始値を示します。以下の各サーバーの詳細については、iSeries Information Center (「**ネットワーキング**」—>「**TCP/IP**」) を参照してください。 iSeries Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。

表 23. TCP/IP サーバーの自動開始値

サーバー	デフォルト値	ユーザーの値
TELNET	AUTOSTART(*YES)	
FTP (ファイル転送プロトコル)	AUTOSTART(*YES)	
BOOTP (ブートストラップ・プロトコル)	AUTOSTART(*NO)	
TFTP (単純ファイル転送プロトコル)	AUTOSTART(*NO)	
REXEC (リモート実行サーバー)	AUTOSTART(*NO)	
RouteD (ルート・デーモン)	AUTOSTART(*NO)	
SMTP (シンプル・メール転送プロトコル)	AUTOSTART(*YES)	
POP (Post Office Protocol)	AUTOSTART(*NO)	
HTTP (Hypertext Transfer Protocol) [1]	AUTOSTART(*NO)	
ICS (Internet Connection Server)[1]	AUTOSTART(*NO)	
LPD (ライン・プリンター・デーモン)	AUTOSTART(*YES)	
SNMP (シンプル・ネットワーク管理プロトコル)	AUTOSTART(*YES)	
DNS (ドメイン・ネーム・システム)	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP (動的ホスト構成プロトコル)	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	

注:

1. IBM HTTP Server for iSeries サーバーでは、CHGHTTPA コマンドを使用して AUTOSTART 値を設定します。

SLIP を使用する場合のセキュリティーに関する考慮事項

iSeries サーバーの TCP/IP サポートには、Serial Interface Line Protocol (SLIP) が含まれています。 SLIP は、低コストの 2 地点間接続を提供します。 SLIP ユーザーは、LAN または WAN に含まれるシステムと 2 地点間接続を確立することにより、LAN または WAN に接続することができます。

SLIP は非同期接続で稼働します。 iSeries サーバーとの間のダイヤルアップ接続に SLIP を使用することができます。たとえば、PC から iSeries システムへのダイヤルアップに SLIP が使用できます。接続の確立後、 PC で TELNET アプリケーションを使用すると、iSeries TELNET サーバーに接続することができます。あるいは、FTP アプリケーションを使用して、2 つのシステム間でファイルを転送することができます。

システムの出荷時に、SLIP 構成はシステムに存在しません。そのため、システムで SLIP (およびダイヤルアップ TCP/IP) を実行したくない場合は、SLIP 用の構成プロファイルを構成しないでください。 SLIP 構成の作成には、2 地点間 TCP/IP の処理 (WRKTCPPTP) コマンドを使用します。 WRKTCPPTP コマンドの使用には、*IOSYSCFG 特殊権限が必要です。

システムで SLIP を実行したい場合は、1 以上の SLIP (2 地点間) 構成プロファイルを作成します。以下の操作モードで構成プロファイルを作成することができます。
- ダイヤルイン (*ANS)
- ダイヤルアウト (*DIAL)

以降のトピックでは、SLIP 構成プロファイル用にセキュリティーをセットアップする方法を説明します。

注: **ユーザー・プロファイル**は、サインオンを許可する iSeries サーバーのオブジェクトです。すべての iSeries サーバーのジョブには、実行対象のユーザー・プロファイルが必要です。**構成プロファイル**は、iSeries システムとの SLIP 接続の確立に使用される情報を保管します。iSeries サーバーへの SLIP 接続を開始するときには、単純にリンクを確立するだけです。ユーザーは、サインオンを済ませていませんし、iSeries サーバーのジョブをまだ開始していません。そのため、iSeries サーバーへの SLIP 接続を開始する場合、ユーザー・プロファイルは必ずしも必要ありません。しかし、この後の説明にあるように、SLIP 構成プロファイルは、接続を許可すべきかどうか判別するためにユーザー・プロファイルを必要とする場合があります。

ダイヤルイン SLIP 接続の制御

SLIP を使用して、システムへのダイヤルイン接続を確立する前に、あらかじめ SLIP *ANS 構成プロファイルを開始しておかなければなりません。 SLIP 構成プロファイルを作成または変更するには、2 地点間 TCP/IP の処理 (WRKTCPPTP) コマンドを使用します。構成プロファイルを開始するには、2 地点間 TCP/IP の開始 (STRTCPPTP) コマンド、または WRKTCPPTP 画面のオプションを使用します。システムの出荷時の STRTCPPTP および ENDTCPPTP コマンドの共通権限は *EXCLUDE です。 SLIP 構成プロファイルの追加、変更、および削除を行うオプションを使用できるのは、ユーザーが *IOSYSCFG 特殊権限を持っている場合だけです。機密保護管理者は、コマンド権限と特殊権限の両方を使用して、ダイヤルイン接続可能なシステムをセットアップできるユーザーを決めることができます。

ダイヤルイン SLIP 接続の保護

ご使用のシステムへのダイヤルインを行うシステムの妥当性を検査したい場合、要求元システムにユーザー ID とパスワードを送信することを要求します。このようにすると、ご使用のシステムでユーザー ID とパスワードを検証することができます。ユーザー ID とパスワードが無効であると、システムはセッション要求を拒否します。

ダイヤルイン妥当性検査をセットアップするには、以下のことを行います。

__ ステップ 1. 要求元システムが接続を確立するのに使用できるユーザー・プロファイルを作成する。要求元が送信するユーザー ID とパスワードは、このユーザー・プロファイル名とパスワードに一致しなければなりません。

注: パスワード妥当性検査を実行するシステムの場合、QSECURITY システム値を 20 以上に設定しなければなりません。

追加の保護として、SLIP 接続の確立用の特別なユーザー・プロファイルを作成することができます。このユーザー・プロファイルには、システムに対する限定された権限を持たせるようにしてください。 SLIP 接続の確立以外の機能のためのこのプロファイルを使用することを計画しない場合、ユーザー・プロファイルに以下の値を設定することができます。

- 初期メニュー (INLMNU) に *SIGNOFF
- 初期プログラム (INLPGM) に *NONE
- 機能の制限 (LMTCPB) に *YES

これらの値により、このユーザー・プロファイルを使用してだれも対話式にサインオンできなくなります。

__ ステップ 2. 要求元が SLIP 接続の確立を試行する際に、システムがその試行をチェックするための権限リストを作成する。

注: SLIP プロファイルの作成または変更時に、システム・アクセス許可リスト・フィールドでこの権限リストを指定します。 (ステップ 4 を参照してください。)

__ ステップ 3. 権限項目の追加 (ADDAUTLE) コマンドを使用して、ステップ 1 で作成したユーザー・プロファイルを権限リストに追加する。それぞれの 2 地点間構成プロファイルごとに固有の権限リストを作成することができます。あるいは、いくつかの構成プロファイルが共用する権限リストを作成することができます。

__ ステップ 4. WRKTCPPTP コマンドを使用して、以下の特性をもつ TCP/IP 2 地点間 *ANS プロファイルをセットアップする。

- 構成プロファイルは、ユーザー妥当性検査を組み込んだ接続ダイアログ・スクリプトを使用しなければならない。ユーザー妥当性検査には、要求元からのユーザー ID とパスワードの受け入れと、それらの妥当性検査が含まれます。システムは、この機能を提供するいくつかのサンプル・ダイアログ・スクリプト付きで出荷されます。
- 構成プロファイルには、ステップ 2 で作成した権限リストの名前を指定しなければならない。接続ダイアログ・スクリプトが受信するユーザー ID は、権限リストに入っていなければなりません。

ダイヤルイン・セキュリティーのセットアップ値は、ダイヤルインを行うシステムのセキュリティーの実施と機能の影響を受けることに注意してください。ユーザー ID とパスワードが必要な場合、要求元システムの接続ダイアログ・スクリプトがそのユーザー ID とパスワードを送信しなければなりません。 iSeries サーバーなどの一部のシステムは、ユーザー ID とパスワードの保管に関してセキュアな方法を提

供します。(『セキュリティーとダイヤルアウト・セッション』では、この方法について説明します。) その他のシステムは、システムのスクリプトのありかを知っているすべてのユーザーがアクセスできる可能性のあるスクリプトに、ユーザー ID とパスワードを保管します。

通信相手のセキュリティーの実施と機能の違いにより、それぞれの要求元環境ごとに、別の構成プロファイルを作成することができます。 STRTCPPTP コマンドを使用して、特定の構成プロファイル用のセッションを受け入れるようにシステムをセットアップします。たとえば、一部の構成プロファイル用のセッションは、一日の特定の時間にしか開始できません。関連するユーザー・プロファイルの活動をログに記録するのに、セキュリティー監査を使用することができます。

ダイヤルイン・ユーザーによる他のシステムへのアクセスの防止

システムおよびネットワーク構成によっては、SLIP 接続を開始するユーザーは、システムにサインオンしなくてもネットワークの別のシステムにアクセスできる可能性があります。たとえば、あるユーザーがシステムへの SLIP 接続を確立できるとすると、そのユーザーは、ダイヤルインが許可されていないネットワーク内の別のシステムへの FTP 接続を確立できる可能性があります。

構成プロファイルの *IP データグラムの転送許可* フィールドに N (いいえ) を指定すると、SLIP ユーザーがネットワークの他のシステムにアクセスできないようにすることができます。これにより、ユーザーはシステムにログオンせずに、ネットワークにアクセスすることはできなくなります。しかし、ユーザーが正常にシステムにログオンした後では、データグラム転送値の効果はありません。データグラム転送値は、ネットワーク内の別のシステムとの接続を確立するために iSeries システムで TCP/IP アプリケーション (FTP や TELNET など) を使用するユーザーの機能を制限しません。

ダイヤルアウト・セッションの制御

システムからのダイヤルアウト接続を確立するためにだれかが SLIP を使用する前に、あらかじめ SLIP *DIAL 構成プロファイルを開始しておかなければなりません。 SLIP 構成プロファイルを作成または変更するには、WRKTCPPTP コマンドを使用します。構成プロファイルを開始するには、2 地点間 TCP/IP の開始 (STRTCPPTP) コマンド、または WRKTCPPTP 画面のオプションを使用します。システムの出荷時の STRTCPPTP および ENDTCPPTP コマンドの共通権限は *EXCLUDE です。 SLIP 構成プロファイルの追加、変更、および削除を行うオプションを使用できるのは、ユーザーが *IOSYSCFG 特殊権限を持っている場合だけです。機密保護管理者は、コマンド権限と特殊権限の両方を使用して、ダイヤルアウト接続可能なシステムをセットアップできるユーザーを決めることができます。

セキュリティーとダイヤルアウト・セッション

iSeries システムのユーザーが、ユーザーの妥当性検査を必要とするシステムへのダイヤルアウト接続を確立しようとする場合があります。iSeries サーバーの接続ダイアログ・スクリプトは、リモート・システムにユーザー ID とパスワードを送信しなければなりません。iSeries サーバーは、そのパスワードを保管するセキュアな方法を提供します。接続ダイアログ・スクリプトにパスワードを保管する必要はありません。

注:

1. システムで接続パスワードを暗号化形式で保管しても、システムは、そのパスワードの送信前にパスワードの暗号化を解除します。 SLIP パスワードは、FTP および TELNET パスワードと同様に、暗号化されていない (「平文の」) 状態で送信されます。しかし、FTP や TELNET の場合とは異なり、SLIP パスワードは、システムが TCP/IP モードを確立する前に送信されます。

   SLIP は非同期モードで 2 地点間接続を使用するため、暗号化されていないパスワードの送信時の機密漏れは、FTP および TELNET パスワード使用時の機密漏れとは異なります。暗号化されていない FTP および TELNET パスワードは、ネットワークで IP トラフィックとして送信される可能性があるため、電子的な盗聴に対して無防備です。 SLIP パスワードの伝送は、2 つのシステム間の電話接続と同じ程度保護されています。
2. SLIP 接続ダイアログ・スクリプトを保管するデフォルトのファイルは QUSRSYS/QATOCPPSCR です。このファイルの共通権限は *USE ですが、これにより、共通ユーザーはデフォルトの接続ダイアログ・スクリプトを変更できません。

妥当性検査の必要なリモート・セッション用の接続プロファイルを作成するときには、以下のことを行います。

__ ステップ 1. サーバー・セキュリティー・データの保持 (QRETSVRSEC) システム値を必ず 1 (はい) にする。このシステム値は、暗号化を解除することができるパスワードをシステムの記憶保護域に保管できるようにするかどうかを決めます。

__ ステップ 2. WRKTCPPTP コマンドを使用して、以下の特性をもつ構成プロファイルを作成する。

- 構成プロファイルのモードには *DIAL を指定する。
- *リモート・サービス・アクセス名* には、リモート・システムが予期するユーザー ID を指定する。たとえば、別の iSeries サーバーに接続する場合には、その iSeries サーバーのユーザー・プロファイル名を指定します。
- *リモート・サービス・アクセス・パスワード* には、リモート・システムがこのユーザー ID に対して予期するパスワードを指定する。 iSeries サーバーでは、このパスワードは暗号化解除することができる形式で記憶保護域に保管されます。構成プロファイルに割り当てる名前とパスワードは、QTCP ユーザー・プロファイルに関連します。どのユーザー・コマンドやインターフェースを使用しても、名前とパスワードにアクセスすることはできません。これらのパスワード情報にアクセスできるのは、登録済みシステム・プログラムだけです。

  注: TCP/IP 構成ファイルの保管の際に、接続プロファイルのパスワードは保管されないことに注意してください。 SLIP パスワードを保管するには、セキュリティー・データ保管 (SAVSECDTA) コマンドを使用して QTCP ユーザー・プロファイルを保管します。
- 接続ダイアログ・スクリプトには、ユーザー ID とパスワードを送信するスクリプトを指定する。システムは、この機能を提供す

るいくつかのサンプル・ダイアログ・スクリプト付きで出荷されます。システムがスクリプトを実行すると、システムはパスワードを取り出してそのパスワードの暗号化を解除し、リモート・システムに送信します。

Point to Point Protocol のセキュリティーに関する考慮事項

Point-to-Point Protocol (PPP) が TCP/IP の一部として使用できます。 PPP は、SLIP で使用できる機能を超える追加機能を提供する 2 地点間接続の業界標準です。

PPP を使用すると、iSeries サーバーは、インターネット・サービス・プロバイダー、あるいはイントラネットまたはエクストラネット上の他のシステムに、直接高速で接続することができます。リモート LAN は、iSeries サーバーに実際にダイヤルイン接続を行うことができます。

SLIP と同様に、PPP が iSeries サーバーへのネットワーク接続を提供することを覚えておいてください。PPP 接続は、基本的にシステムのドアまで要求元をつなぎます。それでも要求元は、システムに入って TELNET や FTP などの TCP/IP サーバーに接続するためには、ユーザー ID とパスワードが必要です。この新しい接続機能についてのセキュリティーの考慮事項は、以下のとおりです。

注: IBM iSeries Access for Windows ワークステーションの iSeries ナビゲーターを使用して、PPP を構成します。

- PPP は、専用接続 (同一ユーザーが常に同一の IP アドレスを使用) を行う機能を提供します。専用アドレスを使用すると、IP スプーフィング (名前を偽ったシステムが、認知された IP アドレスをもつトラステッド・システムのふりをすること) が起こる可能性があります。しかし、PPP が提供する拡張認証機能は、IP スプーフィングに対する保護に役立ちます。
- SLIP と同様、PPP では、ユーザー名と関連パスワードを指定した接続プロファイルを作成します。ただし、SLIP とは異なり、ユーザーは、有効なユーザー・プロファイルとパスワードを所有している必要はありません。ユーザー名とパスワードは、ユーザー・プロファイルとは関連付けられていません。その代わりに、PPP 認証には妥当性検査リストが使用されます。さらに、PPP には接続スクリプトは不要です。認証 (ユーザー名とパスワードの交換) は PPP アーキテクチャーの一部ですが、SLIP の場合よりも低いレベルで行われます。
- PPP では、CHAP (Challenge Handshake Authentication Protocol) を使用するオプションがあります。 CHAP はユーザー名とパスワードを暗号化するため、盗み聞きする者がパスワードを盗聴することについて心配する必要はなくなります。

  PPP 接続が CHAP を使用するのは、接続の両側のマシンで CHAP がサポートされている場合だけです。 2 つのモデム間で通信をセットアップするためシグナルを交換する際に、その 2 つのシステムは折衝します。たとえば、SYSTEMA は CHAP をサポートするものの SYSTEMB が CHAP をサポートしない場合、SYSTEMA は、セッションを否定するか、あるいは暗号化されていないユーザー名とパスワードの使用に同意することができます。暗号化されていないユーザー名とパスワードの使用に同意することは、低折衝と呼ばれます。低折衝を決めるのは、構成オプションです。たとえば、すべてのシステムに CHAP 機能があることが認識されているイントラネットでは、低折衝にならないように接続プロファ

イルを構成してください。ご使用のシステムがダイヤルアウトを行う公衆接続では、進んで低折衝を行う場合があります。

PPP 用の接続プロファイルは、有効な IP アドレスを指定する機能を提供します。たとえば、特定のユーザー用に特定アドレスまたは特定範囲のアドレスを期待することを示すことができます。暗号化されたパスワードの機能とともに、この機能は、スプーフィングに対する保護をさらに追加します。

活動セッションに関するスプーフィングまたは結合処理からさらに保護するために、指定の間隔で再要求するように PPP を構成することができます。たとえば、PPP セッションの活動中に、iSeries サーバーは他のシステムにユーザー ID とパスワードを要求することができます。15 分間隔で要求して、同一の接続プロファイルであるかどうかを確認します。 (エンド・ユーザーは、この再要求活動に気付きません。システムは、エンド・ユーザーが分かるレベルよりも下のレベルで名前とパスワードを交換します。)

PPP の場合、リモート LAN がご使用の iSeries サーバーと拡張ネットワークにダイヤルイン接続を確立するのを予期することが現実的です。この環境では、IP 転送をオンにすることが必要になるはずです。 IP 転送は、侵入者がネットワークを動き回れるようにしてしまう可能性があります。しかし、PPP には、より強化された保護 (パスワードの暗号化や IP アドレスの妥当性検査など) があります。これにより、侵入者がそもそもネットワーク接続を確立できる可能性がほとんど少なくなります。

PPP の詳細については、iSeries Information Center を参照してください。

ブートストラップ・プロトコル・サーバーを使用する場合のセキュリティーに関する考慮事項

ブートストラップ・プロトコル (BOOTP) は、ワークステーションをサーバーに関連付け、ワークステーション IP アドレスと初期プログラム・ロード (IPL) ソースを割り当てるための、動的な方法を提供します。

BOOTP は、メディアのないワークステーション (クライアント) が、ネットワーク上のサーバーから初期コードを含むファイルを要求できるようにするのに使用される TCP/IP プロトコルです。BOOTP サーバーは、既知の BOOTP サーバー・ポート 67 について listen します。クライアント要求が受信されると、サーバーは、クライアント用に定義された IP アドレスをルックアップし、クライアントの IP アドレスとロード・ファイルの名前を指定してクライアントに応答を戻します。次に、クライアントはそのロード・ファイルに関するサーバーへの TFTP 要求を開始します。クライアント・ハードウェア・アドレスと IP アドレス間のマッピングは、iSeries サーバーの BOOTP テーブルに保持されます。

BOOTP アクセスの防止

ネットワークに接続しているシン・クライアントがない場合は、システムで BOOTP サーバーを実行する必要はありません。 BOOTP サーバーは他の装置に使用できますが、それらの装置のための解決策としては、DHCP を使用した方がよいでしょう。以下のことを行って、BOOTP サーバーが実行されないようにしてください。

__ ステップ 1. TCP/IP の開始時に BOOTP サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。

CHGBPA AUTOSTART(*NO)

注:

a. AUTOSTART(*NO) はデフォルト値です。

b. 137 ページの『自動的に開始する TCP/IP サーバーの制御』では、自動的に開始する TCP/IP サーバーの制御方法について詳しく説明します。

__ ステップ 2. ユーザー・アプリケーション (ソケット・アプリケーションなど) がシステムが通常 BOOTP 用に使用するポートに関連付けられるのを防ぐには、以下のことを行います。

注: DHCP と BOOTP は、同じポート番号を使用するため、これによって、DHCP が使用するポートまで禁止してしまいます。DHCP を使用したい場合は、ポートを制限しないでください。

__ ステップ a. 「GO CFGTCP」と入力して「TCP/IP の構成」メニューを表示する。

__ ステップ b. オプション 4 (TCP/IP ポート制約事項の処理) を選択する。

__ ステップ c. 「TCP/IP ポート制約事項の処理」画面で、オプション 1 (追加) を指定する。

__ ステップ d. 低ポート範囲に 67 を指定する。

__ ステップ e. 高ポート範囲に *ONLY を指定する。

注:

1) ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。

2) 共通ポート番号割り当てに関する情報は RFC1700 に示されています。

__ ステップ f. プロトコルに *UDP を指定する。

__ ステップ g. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。 (保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。) 特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

BOOTP サーバーの保護

BOOTP サーバーは iSeries システムに対して直接アクセスを行わないため、機密漏れは限定されたものになります。機密保護管理者としての第一の関心は、正しい情報を正しいシン・クライアントに関連付けることです。言い換えれば、攻撃を企てる者が BOOTP テーブルを変更し、それによってシン・クライアントが正しく動作しなかったり、まったく動かなくなってしまう可能性があります。

BOOTP サーバーと BOOTP テーブルを管理するには、*IOSYSCFG 特殊権限が必要です。システムで *IOSYSCFG 特殊権限を持つユーザー・プロファイルについては、注意して制御する必要があります。

DHCP サーバーを使用する場合のセキュリティーに関する考慮事項

動的ホスト構成プロトコル (DHCP) は、TCP/IP ネットワークでホストに構成情報を渡すためのフレームワークを提供します。DHCP はクライアント・ワークステーションに対して、自動構成と類似した機能を提供することができます。クライアント・ワークステーションの DHCP 使用可能プログラムは、構成情報のための要求をブロードキャストします。DHCP サーバーが iSeries サーバーで実行中の場合、そのサーバーは、クライアント・ワークステーションが TCP/IP を正確に構成するのに必要な情報を送ることで要求に応答します。

DHCP を使用すると、ユーザーの iSeries サーバーへの最初の接続がより容易になります。これは、ユーザーが TCP/IP 構成情報を入力する必要がないためです。また、DHCP を使用して、サブネットワークで必要な内部 TCP/IP アドレスの数を減らすこともできます。 DHCP サーバーは、活動ユーザーに (IP アドレスのプールから) IP アドレスを一時的に割り振ることができます。

シン・クライアントの場合は、BOOTP の代わりに DHCP を使用することができます。 DHCP は、BOOTP よりも多くの機能を提供し、シン・クライアントと PC の両方の動的構成をサポートすることができます。

DHCP アクセスの防止

システム上で誰にも DHCP を使わせたくない 場合は、以下を行います。

1. TCP/IP の開始時に DHCP サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   注:

   a. AUTOSTART(*NO) はデフォルト値です。

   b. 137 ページの『自動的に開始する TCP/IP サーバーの制御』では、自動的に開始する TCP/IP サーバーの制御方法について詳しく説明します。

2. ユーザー・アプリケーション (ソケット・アプリケーションなど) がシステムが通常 DHCP 用に使用するポートに関連付けられるのを防ぐには、以下のことを行います。

   a. 「GO CFGTCP」と入力して「TCP/IP の構成」メニューを表示する。

   b. オプション 4 (TCP/IP ポート制約事項の処理) を選択する。

   c. 「TCP/IP ポート制約事項の処理」画面で、オプション 1 (追加) を指定する。

   d. 低ポート範囲に 67 を指定する。

   e. 高ポート範囲に 68 を指定する。

注:

1) ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。
2) 共通ポート番号割り当てに関する情報は RFC1700 に示されています。

f. プロトコルに *UDP を指定する。
g. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。 (保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。) 特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

DHCP サーバーの保護

iSeries システムで DHCP の実行を選択したときのセキュリティーに関する考慮事項は、以下のとおりです。

- DHCP を管理する権限を持つユーザー数を制限する。 DHCP の管理には、以下の権限が必要です。
  - *IOSYSCFG 特殊権限
  - 以下のファイルに対する *RW 権限

```
/QIBM/UserData/OS400/DHCP/dhcpsd.cfg
/QIBM/UserData/OS400/DHCP/dhcprd.cfg
```

- LAN に対する物理的なアクセス可能状態を評価する。部外者がラップトップを持ってユーザーのロケーションに楽々と歩いて入ってきて、LAN にそのラップトップを物理的に接続することができるでしょうか? これが発覚した場合、DHCP は、DHCP サーバーが構成するクライアント (ハードウェア・アドレス) のリストを作成する機能を提供します。この機能を使用すると、DHCP がネットワーク管理者に提供する生産性の利点の一部が取り除かれます。しかし、システムが未知のワークステーションを構成することは防止されます。
- 可能であれば、再使用可能 (インターネット用に構築されたものではない) の IP アドレスのプールを使用する。これは、ユーザーのネットワーク外のワークステーションが、サーバーから使用可能な構成情報を獲得しないようにするのに役立ちます。
- さらにセキュリティーが必要な場合には、DHCP 出口点を使用する。出口点とその機能についての概説を以下に示します。「*iSeries System API Reference*」では、これらの出口点の使用方法について説明します。

ポート項目

システムは、ポート 67 (DHCP ポート) からデータ・パケットを読み取るたびに、出口プログラムを呼び出します。出口プログラムは、完全なデータ・パケットを受け取ります。出口プログラムは、システムがそのパケットを処理すべきか、または廃棄すべきかを判断することができます。既存の DHCP スクリーニング機能がユーザーのニーズに対して十分でないときに、この出口点を使用することができます。

アドレス割り当て

システムは、DHCP がクライアントにアドレスを正式に割り当てるたびに、この出口プログラムを呼び出します。

アドレス解放

システムは、DHCP がアドレスを正式に解放し、そのアドレスをアドレス・プールに戻すたびに、この出口プログラムを呼び出します。

TFTP サーバーを使用する場合のセキュリティーに関する考慮事項

単純ファイル転送プロトコル (TFTP) は、ユーザー認証を使用しない基本ファイル転送を提供します。 TFTP は、ブートストラップ・プロトコル (BOOTP) または 動的ホスト構成プロトコル (DHCP) と一緒に動作します。

クライアントは、最初に BOOTP サーバーまたは DHCP サーバーのいずれかに接続します。 BOOTP サーバーまたは DHCP サーバーは、クライアントの IP アドレスとロード・ファイル名で応答します。次に、クライアントはそのロード・ファイルに関するサーバーへの TFTP 要求を開始します。クライアントがそのロード・ファイルのダウンロードを完了すると、クライアントは TFTP セッションを終了します。

TFTP アクセスの防止

ネットワークに接続しているシン・クライアントがない場合は、おそらくシステムで TFTP サーバーを実行する必要はありません。以下のことを行って、TFTP サーバーが実行されないようにしてください。

__ ステップ 1. TCP/IP の開始時に TFTP サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。

```
CHGTFTPA AUTOSTART(*NO)
```

注:

a. AUTOSTART(*NO) はデフォルト値です。

b. 137 ページの『自動的に開始する TCP/IP サーバーの制御』では、自動的に開始する TCP/IP サーバーの制御方法について詳しく説明します。

__ ステップ 2. ユーザー・アプリケーション (ソケット・アプリケーションなど) がシステムが通常 TFTP 用に使用するポートに関連付けられるのを防ぐには、以下のことを行います。

__ ステップ a. 「GO CFGTCP」と入力して「TCP/IP の構成」メニューを表示する。

__ ステップ b. オプション 4 (TCP/IP ポート制約事項の処理) を選択する。

__ ステップ c. 「TCP/IP ポート制約事項の処理」画面で、オプション 1 (追加) を指定する。

__ ステップ d. 低ポート範囲に 69 を指定する。

__ ステップ e. 高ポート範囲に *ONLY を指定する。

注:

1) ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。

2) 共通ポート番号割り当てに関する情報は RFC1700 に示されています。

__ ステップ f. プロトコルに *UDP を指定する。

__ ステップ g. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。 (保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。) 特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

TFTP サーバーの保護

デフォルトでは、TFTP サーバーは、iSeries システムへの非常に限定されたアクセスを行います。これは、特に、シン・クライアント用の初期コードを提供するように構成されています。機密保護管理者は、TFTP サーバーの以下の特性に注意してください。

- TFTP サーバーは認証 (ユーザー ID とパスワード) を必要としません。すべての TFTP ジョブは、QTFTP ユーザー・プロファイルのもとで実行されます。QTFTP ユーザー・プロファイルにはパスワードがありません。そのため、対話式サインオンでは使用できません。QTFTP ユーザー・プロファイルには特殊権限がなにもありませんし、このユーザー・プロファイルはシステム資源に明示的に許可されてもいません。シン・クライアントに必要な資源へのアクセスには、共通権限を使用します。
- TFTP サーバーは、出荷時では、シン・クライアント情報が入っているディレクトリーにアクセスする構成になっています。 *PUBLIC または QTFTP に対して、そのディレクトリーへの読み書きを許可しなければなりません。ディレクトリーに書き込みを行うには、CHGTFTPA コマンドの「ファイル書き込みの許可」パラメーターに *CREATE を指定する必要があります。既存のファイルに書き込みを行うには、CHGTFTPA コマンドの「ファイル書き込みの許可」パラメーターに *REPLACE を指定する必要があります。 *CREATE では、既存のファイルを置き換えたり、新しいファイルを作成したりすることができます。 *REPLACE だけが、既存のファイルを置き換えることができます。

  TFTP 属性の変更 (CHGTFTPA) コマンドを使用して明示的にディレクトリーを定義しない限り、TFTP クライアントがその他のディレクトリーにアクセスすることはできません。そのため、ローカルまたはリモート・ユーザーがシステムへの TFTP セッションの開始を試行すると、情報にアクセスしたり、損傷の原因となるようなユーザーの機能は非常に限定されます。
- シン・クライアントの処理だけでなく、他のサービスも提供するように TFTP サーバーを構成することにした場合は、すべての TFTP 要求を評価して認可するための出口プログラムを定義することができます。 TFTP サーバーは、FTP サーバーで使用できる出口に類似した要求妥当性検査出口を提供します。詳細については、「iSeries Information Center」—>「ネットワーキング」—>「TCP/IP」—>「TFTP」を参照してください。 iSeries Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。

REXEC サーバーを使用する場合のセキュリティーに関する考慮事項

リモート実行サーバー (REXEC) は、REXEC クライアントからコマンドを受け取って実行します。REXEC クライアントは、一般的には、REXEC コマンドの送信をサポートする PC または UNIX アプリケーションです。このサーバーが提供するサポートは、FTP サーバー用に RCMD (リモート・コマンド) サブコマンドを使用するときに使用できる機能と類似しています。

REXEC アクセスの防止

REXEC クライアントからのコマンドを iSeries サーバーに受け入れさせたくない場合、以下のことを行って、REXEC サーバーが実行されないようにします。

__ ステップ 1. TCP/IP の開始時に REXEC サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。

```
CHGRXCA AUTOSTART(*NO)
```

注:

a. AUTOSTART(*NO) はデフォルト値です。

b. 137 ページの『自動的に開始する TCP/IP サーバーの制御』では、自動的に開始する TCP/IP サーバーの制御方法について詳しく説明します。

__ ステップ 2. ユーザー・アプリケーション (ソケット・アプリケーションなど) が、システムが通常 REXEC 用に使用するポートに関連付けられるのを防ぐには、以下のことを行います。

__ ステップ a. 「GO CFGTCP」と入力して「TCP/IP の構成」メニューを表示する。

__ ステップ b. オプション 4 (TCP/IP ポート制約事項の処理) を選択する。

__ ステップ c. 「TCP/IP ポート制約事項の処理」画面で、オプション 1 (追加) を指定する。

__ ステップ d. 低ポート範囲に 512 を指定する。

__ ステップ e. 高ポート範囲に *ONLY を指定する。

__ ステップ f. プロトコルに *TCP を指定する。

__ ステップ g. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。 (保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。) 特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

注:

a. ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。

b. 共通ポート番号割り当てに関する情報は RFC1700 に示されています。

REXEC サーバーの保護

システムでリモート実行サーバーの実行を選択したときの考慮事項は、以下のとおりです。

- REXCD 要求には、ユーザー ID、パスワード、および実行されるコマンドが含まれています。通常の iSeries サーバーの認証および権限検査が適用されます。
  - ユーザー・プロファイルとパスワードの組み合わせが有効でなければならない。
  - システムはユーザー・プロファイルに*機能の制限* (LMTCPB) 値を強制使用する。
  - ユーザーは、コマンド、およびコマンドが使用するすべての資源に対して、許可されていなければならない。
- REXEC サーバーは、FTP サーバーに使用できる出口点に類似した出口点を提供します。妥当性検査出口点を使用すると、そのコマンドを評価し、許可するかどうかを決めることができます。詳細については、「iSeries Information Center」—>「ネットワーキング」—>「TCP/IP」—>「REXEC」を参照してください。iSeries Information Center へのアクセス方法については、xii ページの『前提条件および関連情報』を参照してください。
- REXEC サーバーの実行を選択するときに、ユーザーは、システムにあるメニュー・アクセス制御の外側で実行されます。オブジェクト権限構造が資源を保護するのに適したものであることを必ず確認してください。

RouteD を使用する場合のセキュリティーに関する考慮事項

ルート・デーモン (RouteD) サーバーは、iSeries サーバーで経路指定情報プロトコル (RIP) をサポートします。RIP は、最も広く使用されている経路指定プロトコルです。これは、自律システム内の IP パケットの経路指定で、TCP/IP を援助する Interior Gateway Protocol です。

RouteD の目的は、トラステッド・ネットワーク内のシステムが現行の経路情報を相互に更新することにより、ネットワーク・トラフィックの効率を上げることです。RouteD を実行すると、システムは伝送 (パケット) の経路指定方法について、他の参加システムからの更新情報を受け取ることができます。そのため、ハッカーが RouteD サーバーにアクセス可能であると、 RouteD サーバーを使用してパケットの盗聴または変更を行うことができるシステムを通じて、パケットの経路を変更するおそれがあります。 RouteD のセキュリティーに関する提案は以下のとおりです。

- iSeries サーバーは RIPv1 を使用しますが、RIPv1 はルーターを認証する方法を提供しません。これは、トラステッド・ネットワーク内での使用を意図したものです。ご使用のシステムが「信用」できない他のシステムとともにネットワーク内にいる場合は、RouteD サーバーを実行しないでください。 RouteD サーバーが自動的に開始しないようにするには、以下のように入力します。

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  注:

  1. AUTOSTART(*NO) はデフォルト値です。

2. 137 ページの『自動的に開始する TCP/IP サーバーの制御』では、自動的に開始する TCP/IP サーバーの制御方法について詳しく説明します。

- RouteD 構成を変更することのできる (*IOSYSCFG 特殊権限を持つ) ユーザーを必ず制御してください。
- ご使用のシステムが複数のネットワーク (たとえば、イントラネットとインターネット) に参加している場合は、セキュア・ネットワークとの間でのみ変更内容の送信および受け入れをするように RouteD サーバーを構成することができます。

DNS サーバーを使用する場合のセキュリティーに関する考慮事項

ドメイン・ネーム・システム (DNS) サーバーは、ホスト名と IP アドレス間の相互の変換を行います。iSeries サーバーでは、DNS サーバーは、内部のセキュア・ネットワーク (イントラネット) 用のアドレス変換を提供することを意図しています。

DNS アクセスの防止

システム上のだれにも DNS サーバーを使わせたくない 場合、以下のことを行います。

1. TCP/IP の開始時に DNS サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   注:

   a. AUTOSTART(*NO) はデフォルト値です。

   b. 137 ページの『自動的に開始する TCP/IP サーバーの制御』では、自動的に開始する TCP/IP サーバーの制御方法について詳しく説明します。

2. ユーザー・アプリケーション (ソケット・アプリケーションなど) が、システムが通常 DNS 用に使用するポートに関連付けられるのを防ぐには、以下のことを行います。

   a. 「GO CFGTCP」と入力して「TCP/IP の構成」メニューを表示する。

   b. オプション 4 (TCP/IP ポート制約事項の処理) を選択する。

   c. 「TCP/IP ポート制約事項の処理」画面で、オプション 1 (追加) を指定する。

   d. 低ポート範囲に 53 を指定する。

   e. 高ポート範囲に *ONLY を指定する。

      注:

      1) ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。

      2) 共通ポート番号割り当てに関する情報は RFC1700 に示されています。

   f. プロトコルに *TCP を指定する。

   g. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。 (保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワー

ドを知られていないユーザー・プロファイルです。) 特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

h. *UDP (ユーザー・データグラム) プロトコルについて、ステップ 2c から 2g を繰り返す。

DNS サーバーの保護

iSeries システムで DNS の実行を選択した時のセキュリティーに関する考慮事項は、以下のとおりです。

- DNS サーバーが提供する機能は、IP アドレス変換と名前変換です。このサーバーは、iSeries システムのオブジェクトへのアクセスは提供しません。部外者が DNS サーバーにアクセスする際のリスクは、このサーバーがネットワークのトポロジーを表示するための簡単な方法を提供していることにあります。DNS は、ターゲットになる可能性のあるシステムのアドレスを判別しようとするハッカーの手間を省くおそれがあります。ただし、DNS は、それらのターゲット・システムに入り込むために必要な情報は提供しません。
- 一般的に、イントラネット用に iSeries DNS サーバーを使用します。そのため、DNS を照会する機能を制限する必要はないはずです。しかし、たとえば、イントラネット内にいくつかのサブネットワークが存在する場合があります。その場合、別のサブネットワークのユーザーに iSeries サーバーの DNS を照会できないようにすることができます。DNS のセキュリティー・オプションを使用して、1 次ドメインへのアクセスを制限します。iSeries ナビゲーターを使用して、DNS サーバーが応答する IP アドレスを指定します。

  別のセキュリティー・オプションにより、1 次 DNS サーバーから情報をコピーできる 2 次サーバーを指定します。このオプションを使用すると、サーバーは、ユーザーが明示的にリストした 2 次サーバーからのみゾーン転送要求 (コピー情報への要求) を受け入れます。
- DNS サーバーの構成ファイルを変更する機能は、注意して制限してください。たとえば、悪意のある者が、DNS ファイルをネットワークの外側の IP アドレスを指すように変更するおそれがあります。彼らは、ネットワークのサーバーをシミュレートし、サーバーに入ったユーザーの機密情報にアクセスする可能性もあります。

HTTP Server for iSeries を使用する場合のセキュリティーに関する考慮事項

HTTP サーバーは、HTML (Hypertext Markup Language) 文書などの iSeries サーバーのマルチメディア・オブジェクトにアクセスする機能を WWW ブラウザー・クライアントに提供します。また、これは、*共通ゲートウェイ・インターフェース (CGI)* 仕様もサポートします。アプリケーション・プログラマーは、CGI プログラムを作成してサーバーの機能性を拡張することができます。

管理者は、Internet Connection Server または IBM HTTP Server for iSeries を使用して、同一の iSeries サーバー上で複数のサーバーを並行して実行することができます。実行中のそれぞれのサーバーは、**サーバー・インスタンス**と呼ばれます。それぞれのサーバー・インスタンスには、固有の名前があります。管理者は、開始するインスタンスと、それぞれのインスタンスが行うことを制御します。

注: Web ブラウザーを使用して、以下のいずれかを構成または管理する場合は、実行中の HTTP サーバーの *ADMIN インスタンスが必要です。

- Firewall for iSeries
- Internet Connection Server
- Internet Connection Secure Server
- IBM HTTP Server for iSeries

ユーザー (Web サイトのビジター) には、iSeries サーバーの「サインオン」画面は表示されません。しかし、iSeries サーバーの管理者は、HTTP ディレクティブですべての HTML 文書と CGI プログラムを定義することにより、それらを明示的に認可しなければなりません。さらに、管理者は、要求の一部またはすべてに対して、リソース・セキュリティーとユーザー認証 (ユーザー ID とパスワード) の両方をセットアップすることができます。

ハッカーによる攻撃のために、Web サーバーへのサービスが拒否されることもあります。サーバーは、いくつかのクライアント要求のタイムアウトを測定して、サービス妨害攻撃を検出することができます。サーバーがクライアントからの要求を受け取らない場合は、サーバーはサービス妨害攻撃が進行中であると判断します。このようなことが発生するのは、サーバーに最初にクライアント接続した後です。サーバーのデフォルトでは、攻撃を検出し、ペナルティーを与えます。

HTTP アクセスの防止

システムにアクセスする目的で、だれにもそのプログラムを使わせたくない 場合、HTTP サーバーを実行しないようにしてください。この場合は、次のようにします。

__ ステップ 1. TCP/IP の開始時に HTTP サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。

```
CHGHTTPA AUTOSTART(*NO)
```

注:

a. AUTOSTART(*NO) はデフォルト値です。

b. 137 ページの『自動的に開始する TCP/IP サーバーの制御』では、自動的に開始する TCP/IP サーバーの制御方法について詳しく説明します。

__ ステップ 2. デフォルトでは、HTTP サーバー・ジョブは QTMHHTTP ユーザー・プロファイルを使用します。 HTTP サーバーが開始しないようにするため、QTMHHTTP ユーザー・プロファイルの状況を *DISABLED に設定します。

HTTP サーバーへのアクセスの制御

HTTP サーバーを実行する第一の目的は、ビジターが iSeries システムの Web サイトにアクセスできるようにすることです。Web サイトを訪問するユーザーのことは、業界刊行物の広告を見る人として考えることができます。ビジターは、サーバーの種類やサーバーの物理的な設置場所など、Web サイトを実行しているハードウェアやソフトウェアについては知りません。通常、Web サイトの提供者の側も、潜在的なビジターと Web サイトとの間にバリア (「サインオン」画面など) を設けた

いとは考えません。しかし、Web サイトが提供する文書または CGI プログラムの一部へのアクセスを制限したい場合もあります。

また、1 つの iSeries システムが複数の論理 Web サイトを提供するようにしたい場合もあります。たとえば、iSeries システムは、さまざまな顧客の集合を持つビジネスのさまざまな分野をサポートしている可能性があります。これらのビジネスの各分野ごとに、ビジターにとっては完全に独立しているように見える固有の Web サイトが必要です。さらに、ビジネスについての機密情報が入っている内部 Web サイト (イントラネット) の提供も必要です。

機密保護管理者は、Web サイトの内容を保護する必要がある一方で、同時にセキュリティーの実施が Web サイトの価値にマイナスの影響を与えないようにする必要があります。さらに、HTTP 活動がシステムあるいはネットワークの保全性を危険にさらさないようにする必要があります。以降のトピックでは、プログラムを使用する際のセキュリティーにおける提案を示します。

管理の考慮事項

インターネット・サーバーの管理のためのセキュリティーの考慮事項の一部を以下に示します。

- Web ブラウザーと *ADMIN インスタンスを使用して、セットアップおよび構成機能を実行します。サーバーでの追加のインスタンスの作成などの一部の機能の場合には、*ADMIN サーバーを使用しなければなりません。
- 管理ホーム・ページ (*ADMIN サーバー用のホーム・ページ) のデフォルトの URL は、ブラウザー管理機能を提供するプロダクトの資料の中で公開されています。そのため、IBM 提供ユーザー・プロファイルのデフォルト・パスワードが知られていて、公表されているように、デフォルトの URL は、おそらくハッカーによって知られ、ハッカー・フォーラムで公開されることになります。以下のいくつかの方法で、この公開をされないようにすることができます。
  - 管理機能を実行する必要がある場合は、HTTP サーバーの *ADMIN インスタンスだけを実行する。*ADMIN インスタンスを実行したままにしないでください。
  - (ディジタル証明書マネージャーを使用して) *ADMIN インスタンス用の SSL サポートを活動化する。*ADMIN インスタンスは、ユーザー ID とパスワードを要求するために HTTP 保護ディレクティブを使用します。SSL を使用すると、ユーザー ID とパスワードが (管理書式に表示される構成に関するその他のすべての情報と一緒に) 暗号化されます。
  - インターネットから *ADMIN サーバーへのアクセスを防ぐとともに、URL に含まれるシステム名およびドメイン名を隠すために、ファイアウォールを使用する。
- 管理機能の実行時に、*IOSYSCFG 特殊権限を持つユーザー・プロファイルを使用してサインオンしなければなりません。システムの以下のような特定オブジェクトに対する権限も必要になります。
  - HTML 文書と CGI プログラムが含まれているライブラリーまたはディレクトリー。
  - サーバーのディレクティブの内部でスワップを計画しているすべてのユーザー・プロファイル。
  - ディレクティブが使用するディレクトリー用のアクセス制御リスト (ACL)。

– ユーザー ID とパスワードを作成し、保守するための妥当性検査リスト・オブジェクト。

*ADMIN サーバーと TELNET の両方を使用すると、管理機能をリモートで (おそらくインターネット接続を介して) 実行することができます。公衆リンク (インターネット) を介して管理を行う場合には、強力な権限をもつユーザー ID とパスワードが盗聴にさらされている可能性に注意してください。「盗聴者」は、たとえば TELNET や FTP などを使用してシステムにアクセスを試行するために、このユーザー ID とパスワードを使用する可能性があります。

注:

1. TELNET を使用すると、「サインオン」画面はその他の画面と同様に処理されます。パスワードの入力時にそのパスワードは表示されませんが、システムは、暗号化やエンコードを行わないでそのパスワードを送信します。
2. *ADMIN サーバーを使用すると、パスワードは暗号化されませんが、エンコードされます。コード化体系は業界標準であるため、ハッカー達の間ではよく知られています。エンコード方式は一般の「盗聴者」によって簡単には理解されませんが、高度な盗聴者は、そのパスワードのデコードを試行するためのツールを持っている場合があります。

セキュリティーのヒント

インターネットを介したリモート管理の実行を計画している場合、*ADMIN インスタンスで SSL を使用してください。その結果、伝送が暗号化されます。 V4R4 よりも前のバージョンの TELNET のようなセキュアでないアプリケーションは使用しないでください (TELNET は V4R4 から SSL をサポートしています)。*承認された* ユーザー間でのイントラネットを介して *ADMIN サーバーを使用している場合には、管理用にこのサーバーを安全に使用することができるでしょう。

- HTTP ディレクティブは、サーバー上のすべての活動の基礎を提供します。出荷時の構成では、デフォルト「ウェルカム」ページを表示することができます。サーバー管理者がそのサーバー用にディレクティブを定義するまで、クライアントは「ウェルカム」ページ以外の文書をなにも表示できません。ディレクティブを定義するには、Web ブラウザーと *ADMIN サーバーを使用するか、HTTP 構成の処理 (WRKHTTPCFG) コマンドを使用します。どちらの方法でも *IOSYSCFG 特殊権限が必要です。インターネットに iSeries サーバーを接続する場合は、*IOSYSCFG 特殊権限を持つ組織内のユーザーの数を評価および制御することがさらに重要になります。

資源の保護

IBM HTTP Server for iSeries には、サーバーが使用する情報資産を綿密に制御するための HTTP ディレクティブが組み込まれています。このディレクティブを使用して、Web サーバーがどのディレクトリーから HTML ファイルと CGI プログラムの両方の URL を提供するかを制御したり、他のユーザー・プロファイルにスワップしたり、資源の認証を要求したりすることができます。

注: 使用可能な HTTP ディレクティブとその使い方の詳細については、Information Center の 『Web サービス』を参照してください。このサポートを使用するための提案と考慮事項の一部を以下に示します。

- HTTP サーバーは、「明示権限」をもとに開始します。サーバーは、要求が明示的にディレクティブで定義されていない限り、その要求を受け入れません。言い換えれば、サーバーは、URL がディレクティブに (名前または総称で) 定義されていない限り、その URL についてのすべての要求を即時に拒否します。
- 資源の一部あるいはすべて得るための要求を受け入れる前に、保護ディレクティブを使用してユーザー ID とパスワードを要求することができます。
  - ユーザー (クライアント) が保護資源を要求すると、サーバーはブラウザーにユーザー ID とパスワードを要求します。ブラウザーは、ユーザー ID とパスワードの入力をユーザーに指示し、次にその情報をサーバーに送信します。一部のブラウザーはユーザー ID とパスワードを保管して、それ以降の要求時にユーザー ID とパスワードを自動的に送信します。これにより、ユーザーは、要求のたびに同じユーザー ID とパスワードを繰り返し入力しなくても済むようになります。

    ブラウザーの中には、ユーザー ID とパスワードを保管するものもあるため、iSeries サーバーの「サインオン」画面またはルーターを介してシステムに入る場合に気を付けなければならないことを、管理者と同じようにユーザーにも指示してください。ブラウザー・セッションを無人のままにしておくと、機密漏れのおそれがあるのです。
  - システムがユーザー ID とパスワードを処理する方法には、以下の 3 つのオプションがあります (保護ディレクティブで指定)。
    1. 通常の iSeries サーバーのユーザー・プロファイルおよびパスワードの妥当性検査を使用することができます。これは、イントラネット (セキュア・ネットワーク) で資源を保護するために、最も一般的に使用される方法です。
    2. 「インターネット・ユーザー」を作成することができます。インターネット・ユーザーとは、 iSeries サーバー上でその妥当性検査は行われるが、そのシステムにユーザー・プロファイルを持たないユーザーのことです。インターネット・ユーザーは、「妥当性検査リスト」と呼ばれる iSeries サーバー・オブジェクトを使用してインプリメントされます。妥当性検査リスト・オブジェクトには、特定のアプリケーションの使用するように定義されたユーザーとパスワードのリストが含まれます。

       管理者は、インターネット・ユーザーの ID とパスワードの提供の方法 (たとえば、アプリケーションによって、あるいは管理者が電子メールからの要求に応答することによって) と、インターネット・ユーザーの管理方法を決定します。これを設定するには、HTTP サーバーのブラウザー・ベースのインターフェースを使用します。

       非セキュア・ネットワーク (つまりインターネット) の場合、インターネット・ユーザーを使用した方が、通常のユーザー・プロファイルとパスワードを使用する場合よりも、全体としての保護に優れています。ユーザー ID とパスワードの一意の組み合わせにより、これらのユーザーが行うことができる機能に対する組み込み制限が作成されます。これらのユーザー ID とパスワードは、(TELNET や FTP などを使った) 通常のサインオンでは使用できません。さらに、通常のユーザー ID とパスワードを、ハッカーによる盗聴にさらすこともありません。

3. Lightweight Directory Access Protocol (LDAP) は、伝送制御プロトコル (TCP) 上のディレクトリーへのアクセスを提供するディレクトリー・サービス・プロトコルです。このプロトコルを使用すると、そのディレクトリー・サービスに情報を保管し、それを照会することができます。 LDAP は、ユーザー認証を行うための選択肢の 1 つとしてサポートされています。

注:

1. ブラウザーがユーザー ID とパスワードを送信する時は (ユーザー・プロファイルかまたはインターネット・ユーザーかにかかわらず)、エンコードされますが、暗号化はされません。コード化体系は業界標準であるため、ハッカー達の間ではよく知られています。エンコード方式は一般の盗聴者によっては簡単には理解されませんが、高度な盗聴者は、これらのデコードを試行するためのツールを持っている場合があります。
2. iSeries サーバーは保護システム域に妥当性検査オブジェクトを保管します。ここにアクセスできるのは、定義済みのシステム・インターフェース (API) と適切な権限を持っている場合だけです。

– ユーザー固有のイントラネット認証局を作成するために、ディジタル証明書マネージャー (DCM) を使用することができます。ディジタル証明書は、証明書と所有者のユーザー・プロファイルとを自動的に関連付けます。証明書の権限と許可は、関連プロファイルのものと同一です。

- サーバーが要求を受け入れると、通常の iSeries サーバーの資源保護がこれを引き継ぎます。資源を要求するユーザー・プロファイルは、その資源 (たとえば、HTML 文書が含まれるフォルダーまたはソースの物理ファイル) へのアクセス権限を持っている必要があります。デフォルトでは、ジョブは QTMHHTTP ユーザー・プロファイルで実行されます。ディレクティブを使用すると、別のユーザー・プロファイルにスワップすることができます。そして、システムはそのユーザー・プロファイルの権限を使用して、オブジェクトにアクセスします。このサポートに対する考慮事項を以下にいくつか示します。
  – サーバーが複数の論理 Web サイトを提供していると、ユーザー・プロファイルのスワッピングが特に役立ちます。別々のユーザー・プロファイルをそれぞれの Web サイト用のディレクティブと関連付けることができるため、通常の iSeries サーバーの資源保護を使用してそれぞれのサイトの文書を保護することができます。
  – ユーザー・プロファイルをスワップする機能と妥当性検査オブジェクトとを組み合わせて使用することができます。サーバーは、初期要求を評価するために、固有のユーザー ID とパスワード (通常のユーザー ID とパスワードとは異なるもの) を使用します。サーバーがユーザーを認証してから、システムは別のユーザー・プロファイルにスワップして、資源保護を利用します。そのため、ユーザーは本当のユーザー・プロファイル名に気付かず、(FTP などの) 他の方法でそのユーザー・プロファイル名の使用を試行することができません。
- HTTP サーバー要求によっては、プログラムを HTTP サーバーで実行する必要があります。たとえば、システムのデータにアクセスするプログラムなどです。プログラムを実行する前に、サーバー管理者は、CGI ユーザー・インターフェース標準に準拠している特定のユーザー定義プログラムにその要求 (URL) をマップしておかなければなりません。CGI プログラムのための考慮事項の一部は以下のとおりです。

- HTML 文書の場合と同様に、CGI プログラムに対して保護ディレクティブを使用することができます。このため、プログラムの実行前に、ユーザー ID とパスワードが必要になります。
- デフォルトでは、CGI プログラムは QTMHHTP1 ユーザー・プロファイルで実行されます。プログラムを実行する前に、別のユーザー・プロファイルにスワップすることができます。したがって、CGI プログラムがアクセスする資源用に、通常の iSeries サーバーのリソース・セキュリティーをセットアップすることができます。
- 機密保護管理者は、システムで CGI プログラムの使用を認可する前に、セキュリティーを検討するようにしてください。プログラムの出所と CGI プログラムの実行する機能を認識してください。また、CGI プログラムを実行するユーザー・プロファイルの機能もモニターしてください。また、たとえばコマンド行へのアクセスを得られるかどうかといったことを判別するために、CGI プログラムを使用してテストも行ってください。権限を取り入れたプログラムを扱うのと同じように注意して、CGI プログラムを取り扱います。
- さらに、機密オブジェクトが不適切な共通権限を持つ可能性も検討してください。まれに、設計のよくない CGI プログラムは、知識があり悪意のあるユーザーがシステムに入り込むのを許してしまうおそれがあります。
- CGILIB などの特定のユーザー・ライブラリーを使用して、すべての CGI プログラムを保持します。オブジェクト権限を使用して、このライブラリーに新規オブジェクトを配置できるユーザーと、このライブラリーでプログラムを実行できるユーザーを制御します。ディレクティブを使用して、このライブラリーに入っている CGI プログラムを実行する HTTP サーバーを制限します。

  注: サーバーが複数の論理 Web サイトを提供する場合、それぞれのサイトの CGI プログラム用に別のライブラリーをセットアップすることができます。

セキュリティーに関するその他の考慮事項

セキュリティーに関するその他の考慮事項は以下のとおりです。

- HTTP は、iSeries システムへの読み取り専用アクセスを提供します。HTTP サーバー要求は、直接、システムでデータを更新したり削除することはできません。しかし、CGI プログラムでデータを更新することができる場合があります。さらに、 Net.Data® CGI プログラムが iSeries サーバーのデータベースにアクセスできるようにすることもできます。システムは、スクリプト (出口プログラムに類似している) を使用して、Net.Data プログラムへの要求を検討します。そのため、システム管理者は、Net.Data プログラムが行える処置を制御することができます。
- HTTP サーバーは、サーバーを通じたアクセスとアクセス試行の両方をモニターするのに使用できるアクセス・ログを提供します。

IBM HTTP Server for iSeries で SSL を使用する場合のセキュリティーに関する考慮事項

IBM HTTP Server for iSeries は、iSeries サーバーとのセキュアな Web 接続を提供することができます。**セキュア Web サイト**は、クライアントとサーバー間の伝送

(両方向) が暗号化されていることを意味します。このように伝送を暗号化することで、盗聴者によるせんさくと、伝送の取り込みまたは更新を試行する人たちの両方からの安全が確保されます。

注: セキュア Web サイトは、厳密にクライアント・サーバー間で渡される情報のセキュリティーに適用されることに注意してください。セキュア Web サイトの目的は、ハッカーに対するサーバーの脆弱性を減らすことではありません。しかし、これによって、ハッカー志望の人間が盗聴を通じて容易に入手できる情報を確実に制限します。

Information Center の SSL と Web サーバー (HTTP) のトピックには、暗号化プロセスの導入、構成、および管理のための詳しい説明があります。このトピックでは、サーバー機能の概説とサーバー使用の際の考慮事項を説明します。

Internet Connection Server は、以下のライセンス・プログラムのいずれかが導入されている場合には、HTTP および HTTPS をサポートします。

- 5722-NC1
- 5722-NCE

これらのオプションが導入されている場合は、本プロダクトはインターネット接続セキュア・サーバーと呼ばれます。

IBM HTTP Server for iSeries (5722-DG1) は、HTTP と HTTPS の両方をサポートします。SSL を使用可能にするためには、以下の暗号製品の 1 つを導入しなければなりません。

- 5722-AC2
- 5722-AC3

暗号化に依存するセキュリティーには、いくつかの要件があります。

- 送信側と受信側 (サーバーとクライアント) は両方とも、暗号化メカニズムを「理解」して、暗号化と暗号化解除を実行できなければなりません。HTTP サーバーには、SSL を使用できるクライアントが必要です。(SSL はほとんどの一般的な Web ブラウザーで使用可能です。) iSeries 暗号化ライセンス・プログラムは、いくつかの業界標準暗号化方式をサポートします。クライアントがセキュアなセッションを確立しようとするときに、サーバーとクライアントは、両者がサポートする最もセキュアの度合いが高い暗号化方式を見つけるために折衝します。
- 盗聴者によって、伝送の暗号化が解除できてはなりません。そのため、暗号化方式では、送信側と受信側の両者だけが知っている暗号化 / 暗号化解除の**秘密鍵**を両者に持たせる必要があります。セキュアな外部 Web サイトが必要な場合、ユーザーとサーバーに対してディジタル証明書を作成して発行するために、独立した認証局 (CA) を使用してください。認証局は、トラステッド・パーティー として認識されます。

暗号化は、転送情報の秘密性を保護します。しかし、財務情報などの機密情報の場合、秘密性だけでなく、保全性と認証性も必要です。言い換えると、クライアントと (オプションで) サーバーは、(独立参照を通じて) もう一方のパーティーを信頼しなければなりませんし、さらに伝送が絶対に更新されないようにしなければならないということです。認証局 (CA) によって提供されるディジタル署名は、認証性

と保全性を保証します。 SSL プロトコルは、サーバー証明書 (およびオプションでクライアント証明書) のディジタル署名を検証することにより、認証を行います。

暗号化と暗号化解除には処理時間が必要で、それが伝送のパフォーマンスに影響を与えます。そのため、iSeries サーバーでは、セキュアなサービスとそうでないサービスの両方のプログラムを同時に実行することができます。プロダクト・カタログなどセキュリティーの必要がない文書を提供する場合には、セキュアでない HTTP サーバーを使用することができます。これらの文書の URL は、`http://` で始まります。セキュアな HTTP サーバーは、顧客がクレジット・カードの情報を記入する書式などの機密情報に使用することができます。このプログラムは、URL が `http://` または `https://` で始まる文書を処理することができます。

覚え書き

伝送が機密保護されているかまたは機密保護されていないかをクライアントに知らせることが正しいインターネットのエチケットです (特に Web サイトが一部の文書のためだけにセキュア・サーバーを使用している場合)。

暗号化には、セキュア・クライアントとセキュア・サーバーの両方が必要なことに注意してください。セキュア・ブラウザー (HTTP クライアント) はかなり一般的になってきました。

LDAP のセキュリティーに関する考慮事項

Lightweight Directory Access Protocol (LDAP) セキュリティー機能には、 Secure Sockets Layer (SSL)、アクセス制御リスト、および CRAM-MD5 パスワード暗号化機能が含まれます。 V5R1 では、Kerberos 接続およびセキュリティー監査のサポートが追加され、 LDAP セキュリティーが拡張されました。

これらのトピックについては、「iSeries Information Center」—>「ネットワーキング」->「TCP/IP」->「ディレクトリー・サービス (LDAP)」を参照してください。 iSeries Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。

LPD のセキュリティーに関する考慮事項

LPD (ライン・プリンター・デーモン) は、プリンター出力をシステムに配布する機能を提供します。システムは、LPD 用のサインオン処理を何も実行しません。

LPD アクセスの防止

だれにも、LPD を利用してシステムにアクセスさせたくない 場合、LPD サーバーが実行されないようにしてください。この場合は、次のようにします。

__ ステップ 1. TCP/IP の開始時に LPD サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。

```
CHGLPDA AUTOSTART(*NO)
```

注:

a. AUTOSTART(*YES) はデフォルト値です。

b. 137 ページの『自動的に開始する TCP/IP サーバーの制御』では、自動的に開始する TCP/IP サーバーの制御方法について詳しく説明します。

__ ステップ 2. ユーザー・アプリケーション (ソケット・アプリケーションなど) が、システムが通常 LPD 用に使用するポートに関連付けられるのを防ぐには、以下のことを行います。

__ ステップ a. 「GO CFGTCP」と入力して「TCP/IP の構成」メニューを表示する。

__ ステップ b. オプション 4 (TCP/IP ポート制約事項の処理) を選択する。

__ ステップ c. 「TCP/IP ポート制約事項の処理」画面で、オプション 1 (追加) を指定する。

__ ステップ d. 低ポート範囲に 515 を指定する。

__ ステップ e. 高ポート範囲に *ONLY を指定する。

注:

1) ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。

2) 共通ポート番号割り当てに関する情報は RFC1700 に示されています。

__ ステップ f. プロトコルに *TCP を指定する。

__ ステップ g. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を指定する。 (保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。) 特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

__ ステップ h. *UDP プロトコルについて、ステップ 2c から 2g を繰り返す。

LPD アクセスの制御

LPD クライアントのシステムへのアクセスを許可する場合、以下のセキュリティー事項について注意してください。

- ユーザーが不要なオブジェクトでシステムをあふれさせないようにするために、補助記憶域プール (ASP) に適切な限界値を必ず設定しておいてください。システム保守ツール (SST) または専用保守ツール (DST) のいずれかを使用して、 ASP の限界値を表示および設定することができます。「*バックアップおよび回復の手引き*」には、ASP 限界値についての詳しい説明があります。
- システムにスプール・ファイルを送信するユーザーを制限するために、出力待ち行列に対して権限を使用することができます。ユーザー ID を持っていない LPD

ユーザーは、QTMPLPD ユーザー・プロファイルを使用します。このユーザー・プロファイルに、ほんの少しの出力待ち行列のみに対するアクセス権を与えることができます。

SNMP のセキュリティーに関する考慮事項

iSeries サーバーは、ネットワークにおいてシンプル・ネットワーク管理プロトコル (SNMP) エージェントとして機能します。 SNMP は、ネットワーク環境でゲートウェイ、ルーター、およびホストを管理する手段を提供します。 SNMP エージェントは、システムについての情報を収集し、リモート SNMP ネットワーク管理プログラムが要求する機能を実行します。

SNMP アクセスの防止

だれにも、SNMP を使用してシステムにアクセスさせたくない 場合、SNMP サーバーが実行されないようにしてください。この場合は、次のようにします。

__ ステップ 1. TCP/IP の開始時に SNMP サーバー・ジョブが自動的に開始しないようにするには、以下のとおり入力します。

```
CHGSNMPA AUTOSTART(*NO)
```

注:

a. AUTOSTART(*YES) はデフォルト値です。

b. 137 ページの『自動的に開始する TCP/IP サーバーの制御』では、自動的に開始する TCP/IP サーバーの制御方法について詳しく説明します。

__ ステップ 2. ユーザー・アプリケーション (ソケット・アプリケーションなど) が、システムが通常 SNMP 用に使用するポートに関連付けられるのを防ぐには、以下のことを行います。

__ ステップ a. 「GO CFGTCP」と入力して「TCP/IP の構成」メニューを表示する。

__ ステップ b. オプション 4 (TCP/IP ポート制約事項の処理) を選択する。

__ ステップ c. 「TCP/IP ポート制約事項の処理」画面で、オプション 1 (追加) を指定する。

__ ステップ d. 低ポート範囲に 161 を指定する。

__ ステップ e. 高ポート範囲に *ONLY を指定する。

注:

1) ポートの制限は、次に TCP/IP を開始するときに有効になります。ポートの制限を設定するときに TCP/IP が活動状態である場合、TCP/IP を終了させてから、再度開始しなければなりません。

2) 共通ポート番号割り当てに関する情報は RFC1700 に示されています。

__ ステップ f. プロトコルに *TCP を指定する。

__ ステップ g. ユーザー・プロファイル・フィールドには、システム上で保護されているユーザー・プロファイル名を

指定する。 (保護されているユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーにパスワードを知られていないユーザー・プロファイルです。) 特定のユーザーにポートを制限することによって、他のすべてのユーザーを自動的に除外します。

__ ステップ h. *UDP プロトコルについて、ステップ 2c から 2g を繰り返す。

SNMP アクセスの制御

SNMP マネージャーによるシステムへのアクセスを許可したい場合、以下のセキュリティー事項について注意してください。

- SNMP を使用してネットワークにアクセスするユーザーは、ネットワークについての情報を収集することができます。別名とドメイン・ネーム・サーバーを使用して隠した情報は、SNMP を通じて、侵入するつもりの者が使用できるようになります。さらに、侵入者は SNMP を使用して、ネットワーク構成を更新し、通信を混乱させるおそれがあります。
- SNMP は、アクセスについてコミュニティー名に依存しています。概念的に、コミュニティー名はパスワードに類似しています。コミュニティー名は暗号化されていません。そのため、コミュニティー名は盗聴に対して無防備です。SNMP 用のコミュニティーの追加 (ADDCOMSNMP) コマンドを使用して、マネージャー IP アドレス (INTNETADR) パラメーターを、*ANY ではなく 1 つ以上の特定の IP アドレスに設定します。また、ADDCOMSNMP または CHGCOMSNMP コマンドの OBJACC パラメーターを *NONE に設定すると、コミュニティー内のマネージャーは、MIB オブジェクトにアクセスできなくなります。これは、コミュニティーを削除しないで、一時的にコミュニティー内のマネージャーへのアクセスを拒否することを目的としています。

INETD サーバーのセキュリティーに関する考慮事項

ほとんどの TCP/IP サーバーとは異なり、INETD サーバーはクライアントに対して単一のサービスを提供しません。その代わりに、INETD サーバーは、管理者がカスタマイズできる各種サービスの集合を提供します。そのため、INETD サーバーは、「スーパー・サーバー」と呼ばれることがあります。INETD サーバーには、以下の組み込みサービスがあります。

- time
- daytime
- echo
- discard
- changed

これらのサービスは TCP と UDP の両方に対してサポートされています。 UDP の場合は、echo、time、daytime、および changed サービスが UDP パケットを受信し、それを送信元に送り返します。 echo サーバーは、受信したパケットをそのまま送り返します。time サーバーと daytime サーバーは、指定された形式で時刻を生成し、それを送り返します。changed サーバーは、印刷可能な ASCII 文字からなるパケットを生成し、それを送り返します。

これら UDP サービスの性質上、サービス妨害攻撃に対しては無防備になります。たとえば、SYSTEMA と SYSTEMB という 2 つの iSeries サーバーがあったとします。悪意のあるプログラマーは、SYSTEMA のソース・アドレスと time サーバーの UDP ポート番号を持つ IP ヘッダーと UDP ヘッダーを偽造することができます。それから、そのパケットを SYSTEMB の time サーバーに送信します。SYSTEMB の time サーバーは、時刻を SYSTEMA に送信し、SYSTEMA は、SYSTEMB に応答を返します。これが繰り返され、その結果、無限ループに陥り、両システムの CPU 資源とネットワーク帯域幅が使い尽くされてしまいます。

したがって、iSeries システムではそのような攻撃のリスクがあることを考慮し、これらのサービスはセキュア・ネットワークだけで実行するようにしなければなりません。 INETD サーバーは、出荷時には、TCP/IP の開始時に自動開始されないように設定されています。 INETD の開始時にこれらのサービスを開始するかどうかを構成することができます。デフォルトでは、TCP と UDP の time サーバーと daytime サーバーの両方が開始します。

INETD サーバーには、次の 2 つの構成ファイルがあります。

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

これらのファイルによって、INETD サーバーの開始時に開始するプログラムが決まります。これらのファイルは、 INETD がプログラムを開始したときにそのプログラムをどのユーザー・プロファイルのもとで実行するかということも決定します。

注: proddata 内の構成ファイルは、変更してはいけません。このファイルは、システムを再ロードするたびに置き換えられます。カスタム構成変更は、userdata ディレクトリー・ツリーのこのファイルにだけ加えてください。このファイルは、リリースのアップグレード中は、更新され**ない**ためです。

悪意のあるプログラマーがこれらのファイルにアクセスしたとすると、INETD 開始時に任意のプログラムを開始するように構成することができてしまいます。したがって、これらのファイルの保護が非常に重要になります。デフォルトでは、これらのファイルを変更するには、QSECOFR 権限が必要になります。これらのファイルへのアクセスに必要な権限を落とさないでください。

注: ProdData ディレクトリーにある構成ファイルは変更しないでください。このファイルは、システムを再ロードするたびに置き換えられます。カスタム構成変更は、UserData ディレクトリー・ツリーのこの構成ファイルにだけ加えてください。このファイルは、リリースのアップグレード中は、更新されないためです。

TCP/IP ローミングを制限する場合のセキュリティー考慮事項

システムがネットワークに接続されている場合、TCP/IP アプリケーションを使用してネットワークをうろつくユーザーの機能を制限することができます。これを行う 1 つの方法は、以下のクライアント TCP/IP コマンドへのアクセスを制限することです。

注: 以下のコマンドは、システムのいくつかのライブラリーに存在している可能性があります。少なくとも、QSYS ライブラリーと QTCP ライブラリーの両方に入っています。すべてのオカレンスを確実に突き止め、保護してください。

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (REXEC クライアント)

ユーザーの到達可能な宛先は、以下により決定されます。

- TCP/IP ホスト・テーブルの項目。
- TCP/IP 経路テーブルの *DFTROUTE 項目。これにより、宛先が不明のネットワークの場合に、ユーザーはネクスト・ホップ・システムの IP アドレスを入力することができます。ユーザーは、デフォルト経路を使用して、リモート・ネットワークに到達または接続することができます。
- リモート・ネーム・サーバー構成。このサポートにより、ネットワーク上の別のサーバーは、ユーザー用のホスト名を探し出すことができます。
- リモート・システム・テーブル。

これらのテーブルへの項目の追加と構成の変更を行うことのできるユーザーを制御する必要があります。また、テーブル項目と構成の影響を理解することも必要です。

ILE C コンパイラーにアクセスするための知識のあるユーザーが、TCP ポートまたは UDP ポートに接続するソケット・プログラムを作成できることに注意してください。QSYSINC ライブラリーの以下のソケット・インターフェース・ファイルへのアクセスを制限すると、このプログラムの作成をより困難にすることができます。

- SYS
- NETINET
- H
- ARPA
- ソケットおよび SSL

サービス・プログラムの場合、以下のサービス・プログラムの使用を制限することにより、すでにコンパイル済みのソケット・アプリケーションおよび SSL アプリケーションの使用を制限することができます。

- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

サービス・プログラムは共通権限が *USE で出荷されますが、その権限は *EXCLUDE (または必要に応じて別の値) に変更することができます。

第 14 章 ワークステーションからのアクセスの保護

多くのシステム・ユーザーは、自分のワークステーションとして机の上にパーソナル・コンピューター (PC) を持っています。システム・ユーザーは PC で稼働するツールを使用したり、PC を使用して iSeries サーバーに接続します。

PC を iSeries サーバーに接続するための方法のほとんどは、ワークステーション・エミュレーションよりも多くの機能を提供します。PC は、iSeries のディスプレイ同様ユーザーに対話式サインオン・セッションを提供することができます。さらに PC は、別のコンピューターと同じく、iSeries サーバーに対してファイル転送やリモート・プロシージャー呼び出しなどの機能を提供します。

iSeries サーバー機密保護管理者は、以下のことを認識しておく必要があります。

- システムに接続している PC ユーザーが使用できる機能
- PC ユーザーがアクセスできる iSeries サーバー資源

iSeries サーバー・セキュリティー方式がまだ拡張 PC 機能 (ファイル転送やリモート・プロシージャー呼び出しなど) に対して準備されていない場合、これらの拡張 PC 機能を行えないようにすることができます。管理者の長期的な目標は、システムの情報を保護した上で、拡張 PC 機能を許可することであるはずです。以下のトピックでは、PC アクセスに関連したセキュリティーの問題の一部を説明します。

ワークステーション・ウィルスの防止

ここでは、機密保護管理者が PC ウィルスを防ぐ方法をいくつか説明します。

ワークステーションからのデータ・アクセスの保護

一部の PC クライアント・ソフトウェアは、サーバーに情報を保管するために共用フォルダーを使用します。iSeries データベース・ファイルにアクセスするため、PC ユーザーには、限定され、適切に定義されたインターフェースのセットがあります。ほとんどのクライアント/サーバー・ソフトウェアに含まれるファイル転送機能を使用して、PC ユーザーは、サーバーと PC との間でファイルをコピーすることができます。DDM ファイル、リモート SQL または ODBC ドライバーなどの、データベース・アクセス機能を使用して、PC ユーザーはサーバーのデータにアクセスすることもできます。

この環境では、サーバー資源にアクセスする PC ユーザーの要求をインターセプトして評価するためのプログラムを作成することができます。要求が DDM ファイルを使用するときには、分散データ管理アクセス (DDMACC) ネットワーク属性で出口プログラムを指定します。 一部の PC ファイル転送の方法の場合、クライアント要求アクセス (PCSACC) ネットワーク属性で出口プログラムを指定します。あるいは、登録機能を使用するには、PCSACC(*REGFAC) を指定することができます。要求がデータのアクセスに他のサーバー機能を使用するときには、WRKREGINF コマンドを使用してそれらのサーバー機能に出口プログラムを登録することができます。

しかし、出口プログラムの設計は難しい可能性があり、誰にでも扱えるものではまずありません。出口プログラムは、オブジェクト権限の置き換えではありません。オブジェクト権限は、任意の資源からの無許可アクセスからオブジェクトを保護するように設計します。

IBM iSeries Access for Windows などの一部のクライアント・ソフトウェアは、iSeries サーバー上へのデータの保管とアクセスに統合ファイル・システムを使用します。 統合ファイル・システムを使用すると、サーバー全体が PC ユーザーにとってより簡単に使用できるようになります。オブジェクト権限はさらに絶対不可欠になります。統合ファイル・システムを通じて、十分な権限を持つユーザーは、サーバー・ライブラリーを PC ディレクトリーであるかのように表示することができます。単純な移動およびコピー・コマンドで、iSeries サーバー・ライブラリーから PC ディレクトリーに、また PC ディレクトリーから iSeries ライブラリーにデータをすぐに移動することができます。システムは、自動的にデータの形式を適切に変更します。

注:

1. QSYS.LIB ファイル・システムのオブジェクトの使用を制御する権限リストを使用することができます。詳しくは、 112 ページの『QSYS.LIB ファイル・システムへのアクセスの制限』を参照してください。
2. 105 ページの『第 11 章 統合ファイル・システムの使用によるファイル保護』には、統合ファイル・システム に関連したセキュリティーの問題について詳しい説明があります。

統合ファイル・システムの長所は、ユーザーと開発者にとっての単純さにあります。1 つのインターフェースで、ユーザーは複数の環境のオブジェクトの作業を行うことができます。PC ユーザーは、オブジェクトにアクセスするのに特別なソフトウェアや API を必要としません。その代わり、PC ユーザーは、使い慣れた PC コマンドや「ポイント・アンド・クリック」を使用して直接オブジェクトを処理することができます。

PC が接続されているすべてのシステムの場合、特に統合ファイル・システムを使用するクライアント・ソフトウェアを使用するシステムの場合、正しいオブジェクト権限構造が重要です。セキュリティーは OS/400 製品に統合されているため、データへのアクセス要求は、すべて権限検査プロセスを通らなければなりません。権限検査は、すべての資源からの要求と、あらゆる方法を使用するデータ・アクセスとに適用されます。

ワークステーションからのアクセスについてのオブジェクト権限

オブジェクトの権限をセットアップするときに、その権限により PC ユーザーに提供される事柄を評価する必要があります。たとえば、ユーザーがファイルに対する *USE 権限を持っていると、そのユーザーはファイルのデータを表示したり印刷することができますが、そのファイルの情報を変更したり、そのファイルを削除することはできません。 PC ユーザーの場合、表示は「読み取り」と同等です。これは、ユーザーがその PC でファイルのコピーを作成するのに十分な権限を提供します。これは、管理者の意図したことではない可能性があります。

重要なファイルの中には、ダウンロードを防止するために、共通権限を *EXCLUDE に設定する必要があるものもあります。次に、メニューや、権限を借用するプログラムを使用するなど、サーバー上のファイルを「表示する」ための別の方法を提供することができます。

ダウンロードを防止する別のオプションは、PC ユーザーがサーバー機能を開始する (対話式サインオン以外) たびに実行する出口プログラムを使用することです。ネットワーク属性変更 (CHGNETA) コマンドを使用すると、PCSACC ネットワーク属性に出口プログラムを指定することができます。あるいは、登録情報処理 (WRKREGINF) コマンドを使用すると、出口プログラムを登録することができます。使用する方法は、PC がシステムのデータにアクセスする方法と、PC が使用するクライアント・プログラムによって異なります。出口プログラム (QIBM_QPWFS_FILE_SERV) は、IFS への iSeries Access とネットサーバーからのアクセスに適用されます。このプログラムは、FTP や ODBC などの他のメカニズムを使用した PC からのアクセスは防止しません。

ユーザーが PC からサーバー・データベース・ファイルにデータをコピーできるように、PC ソフトウェアは一般的にアップロード機能も提供します。権限構造を正しくセットアップしていないと、PC ユーザーが、ファイルのデータすべてを PC からのデータでオーバーレイするおそれがあります。*CHANGE 権限の割り当ては注意して行う必要があります。ファイル操作に必要な権限については、「*iSeries 機密保護解説書*」の付録 D を検討してください。

iSeries Information Center には、PC 機能の権限と出口プログラムの使用についての詳しい説明があります。詳細は、 xii ページの『前提条件および関連情報』を参照してください。

アプリケーション管理

アプリケーション管理は、iSeries サーバーのグラフィカル・ユーザー・インターフェース (GUI) である、iSeries ナビゲーターのオプションで導入可能な構成要素です。アプリケーション管理を使用すると、システム管理者は、特定のサーバー上のユーザーおよびグループが使用できる機能またはアプリケーションを制御することができます。これによって、クライアントを介してサーバーにアクセスするユーザーが使用できる機能を制御することもできます。ここで重要なことは、Windows クライアントからサーバーにアクセスする場合に、どの管理機能を使用できるようにするかを決めるのは iSeries サーバーのユーザーであって、Windows のユーザーではない、ということです。

iSeries ナビゲーターのアプリケーション管理の詳細については、「iSeries Information Center」—>「iSeries への接続」—>「接続に使用するアプリケーション」—>「iSeries ナビゲーター」 (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm) を参照してください。

ポリシー管理

ポリシーは、クライアント PC 上でソフトウェアを構成するために使用する管理者のためのツールです。ポリシーによって、ユーザーがアクセスできる PC 上の機能およびアプリケーションを制限できます。また、ポリシーを使用すると、特定のユーザーまたは特定の PC で使用すべき構成を推奨または指示することができます。

注: ポリシーは、サーバーの資源は制御しません。ポリシーは、サーバーのセキュリティーに置き換わるものではありません。ポリシーを使用して、iSeries Access が特定のユーザーによって特定の PC からサーバーにアクセスする方法を制御することができます。しかし、その他のメカニズムによるサーバーの資源へのアクセス方法については変更できません。

ポリシーはファイル・サーバーに保管されます。ユーザーが Windows ワークステーションにサインオンするたびに、その Windows ユーザーに適用されるポリシーがファイル・サーバーからダウンロードされます。ポリシーがレジストリーに適用された後でないと、ユーザーはワークステーション上での作業ができません。

Microsoft® ポリシーとアプリケーション管理の比較

iSeries Access Express は、ネットワーク内に管理制御をインプリメントするために、Microsoft システム・ポリシーと iSeries ナビゲーターのアプリケーション管理の 2 つの異なるストラテジーをサポートします。どちらの方法がお客様のニーズに最も合うかを検討するときは、以下のことを考慮してください。

Microsoft システム・ポリシー

ポリシーは PC 主導型で、特定の OS/400 リリースに依存しません。ポリシーは PC にも、Windows ユーザーにも適用できます。これは、ユーザーがサーバーのユーザー・プロファイルではなく、 Windows ユーザー・プロファイルを参照することを意味します。ポリシーは制限するため、および「構成」するために使用できます。ポリシーは通常、アプリケーション管理と比べて、よりきめ細かい制御とより広範な機能を提供します。これは、ユーザーがある機能を使用できるか否かを判別するときに、サーバーに接続する必要がないからです。ポリシーのインプリメンテーションは、アプリケーション管理のインプリメンテーションより複雑です。なぜなら、Microsoft システム・ポリシー・エディターを使用する必要があり、またそれぞれの PC はポリシーをダウンロードできるように構成されていなければならないためです。

iSeries ナビゲーターのアプリケーション管理

アプリケーション管理は、ユーザー・プロファイルにデータを関連付けます。Windows プロファイルにデータを関連付けるのは、Microsoft システム・ポリシーです。アプリケーション管理を使用するためには、iSeries サーバーで V4R3 以降の OS/400 製品を実行する必要がありますが、機能の中には V4R4 以降でしか提供されないものもあります。アプリケーション管理では、iSeries ナビゲーターのグラフィカル・ユーザー・インターフェースを使用して管理を行います。これは、ポリシー・エディターを使用するよりずっと簡単です。アプリケーション管理の情報は、ユーザーがどの PC からサインオンしたのかに関係なくユーザーに適用されます。iSeries ナビゲーターのうちの特定の機能を制限することができます。制限したい機能のすべてがアプリケーション管理で使用可能で、使用している OS/400 のバージョンがアプリケーション管理をサポートしている場合は、アプリケーション管理を使用することをお勧めします。

iSeries Access for Windows での SSL の使用

iSeries Access Express における SSL の使用については、iSeries Information Center のトピック『*SSL 管理*』、『*iSeries Access Express と iSeries ナビゲーターの保*

護』、『*iSeries Developer Kit for Java*』、および『*iSeries Toolbox* for Java』 (Java メイン・トピックの下) のトピックを参照してください。この情報は、システムで提供されている CD から参照することもできます。

iSeries ナビゲーター・セキュリティー

iSeries ナビゲーターは、iSeries Access を持つユーザー向けの、使いやすいサーバー・インターフェースです。 OS/400 製品の新しいリリースが出されるたびに、iSeries ナビゲーターから利用できるサーバー機能は増えています。使いやすいインターフェースには、技術サポートのコストを削減したり、システムのイメージを改善するといった、多くの利点があります。このインターフェースはまた、セキュリティーのチャレンジももたらします。

機密保護管理者は、もはやユーザーが資源を保護したいという意識を当てにできません。 iSeries ナビゲーターは、ユーザーに対して多くの機能を簡単にそして目に見えるようにします。セキュリティーのニーズを満たすために、ユーザー・プロファイルおよびオブジェクト・セキュリティーに対するセキュリティー・ポリシーの設計、およびインプリメンテーションを確実に行う必要があります。

IBM e (ロゴ) server iSeries Access for Windows の V4R4 以降のバージョンには、ユーザーが iSeries ナビゲーターから実行できる機能を制御する次の方法が用意されています。

- 選択的導入
- アプリケーション管理
- Windows NT® システム・ポリシーのサポート

iSeries ナビゲーターは、複数の構成要素にパッケージされていて、個別に導入することができます。これにより、必要な機能だけを導入することができます。アプリケーション管理により、管理者は、ユーザーまたはグループが iSeries ナビゲーターを介してアクセスできる機能を制御することができます。アプリケーション管理は、アプリケーションを以下のカテゴリーに編成します。

iSeries ナビゲーター
: iSeries ナビゲーターとプラグインが含まれます。

クライアント・アプリケーション
: iSeries Access を含め、アプリケーション管理を介して管理されるクライアント上の機能を提供する、その他のすべてのクライアント・アプリケーションが含まれます。

ホスト・アプリケーション
: サーバーだけに常駐し、アプリケーション管理によって管理される機能を提供するすべてのアプリケーションが含まれます。

選択的導入、アプリケーション管理、およびポリシーを使用して、ユーザーがアクセスできる iSeries ナビゲーターの機能を制限することができます。 ただし、リソース・セキュリティーにこれらを使用しないでください。

V4R4 からは、IBM e (ロゴ) server iSeries Access for Windows で、Windows NT のシステム・ポリシー・エディターを使用して、PC の使用者にかかわらず特定の PC クライアントから実行できる機能を制御できるようになりました。

選択的導入、アプリケーション管理、およびポリシー管理の追加情報については、iSeries Information Center を参照してください。また本書の 6 ページの『プログラム機能への制限アクセス』セクションでもアプリケーション管理について説明しています。

ODBC アクセスの防止

Open Database Connectivity (ODBC) は、PC アプリケーションが iSeries データに PC データと同様にアクセスするために使用できるツールです。 ODBC プログラマーは、このデータの物理位置を PC アプリケーションのユーザーに見えないようにすることができます。 ODBC のセキュリティーに関する考慮事項の詳細については、iSeries Information Center の『iSeries Access for Windows ODBC のセキュリティー』 (/rzaii/rzaiiodbc09.HTM) を参照してください。

ワークステーション・セッション・パスワードのセキュリティーに関する考慮事項

一般に、PC ユーザーは、iSeries Access などの接続ソフトウェアを開始する場合、サーバーに対し、ユーザー ID とパスワードを一度入力します。パスワードは暗号化されて PC メモリーに保管されます。ユーザーが同じサーバーに対して新規セッションを確立するたびに、PC はユーザー ID とパスワードを自動的に送ります。

一部のクライアント/サーバー・ソフトウェアは、対話式セッションで「サインオン」画面をバイパスするオプションも提供します。そのソフトウェアは、ユーザーが対話式 (5250 エミュレーション) セッションを開始したときに、ユーザー ID と暗号化されたパスワードを送ります。このオプションをサポートするには、サーバーの QRMTSIGN システム値を *VERIFY に設定しなければなりません。

「サインオン」画面をバイパスできるように選択する場合、セキュリティーのトレードオフを考慮する必要があります。

機密漏れ: 5250 エミュレーションなどの対話式セッションでは、「サインオン」画面は他の画面と変わりません。パスワードの入力時にそのパスワードは画面上に表示されませんが、パスワードは他のデータ・フィールドと同様に、暗号化されていない形式でリンクを通じて送信されます。リンクのタイプによっては、この送信は、侵入するつもりの者に、リンクをモニターしてユーザー ID とパスワードを検出する機会を与えるおそれがあります。電子機器を使用してリンクをモニターすることは、しばしば**盗聴**と呼ばれます。 V4R4 からは、Secure Sockets Layer (SSL) を使用して、 iSeries Access と iSeries サーバー間の通信を暗号化することができます。これにより、パスワードを含むデータは、ハッカーによる盗聴から保護されます。

「サインオン」画面をバイパスするオプションを選択すると、PC は送信前にパスワードを暗号化します。暗号化は、パスワードが盗聴によって盗まれる可能性を回避します。しかし、PC ユーザーが操作上のセキュリティーを必ず実践するようにしなければなりません。 iSeries システムとのセッションの活動中に PC のユーザーが不在であると、ユーザー ID とパスワードを知らなくても、別のセッションを開始

する機会を他人に与えることになります。システムが長時間非活動のときには PC をロックするようにセットアップし、セッションの再開にはパスワードを必要とするようにしてください。

たとえ「サインオン」画面のバイパスを選択しなくても、セッションの活動中に PC ユーザーが不在になると、機密漏れを意味します。ユーザー ID とパスワードを知らなくても、PC ソフトウェアを使用することにより、他人がサーバー・セッションを開始し、データにアクセスする可能性があります。5250 エミュレーションは、セッションを開始してデータ・アクセスを始めるのにほとんど知識を必要としないので、5250 エミュレーションの場合の機密漏れの可能性はいくぶん大きくなります。

また、iSeries Access セッションを切断した場合の影響について、ユーザーに指示することも必要です。多くのユーザーは、切断オプションがサーバーへの接続を完全に停止すると (論理的に、しかし間違って) 想定しています。実際は、ユーザーが切断のオプションを選択すると、サーバーはそのユーザーのセッション (ライセンス) を別のユーザーが使用できるようにします。しかし、サーバーへのクライアントの接続はまだオープンしたままです。別のユーザーが無保護の PC にきて、ユーザー ID とパスワードを一度も入力しなくても、サーバーの資源にアクセスすることができるのです。

セッションの切断を必要とするユーザーには、2 つのオプションを提案することができます。

- パスワードが必要なロック機能を PC に必ずもたせる。これにより、パスワードを知らない人がユーザー不在の PC を使用できなくなります。
- Windows をログオフするか、PC を再始動 (リブート) して、セッションを完全に切断する。これにより、iSeries へのセッションが終了します。

また、iSeries Access for Windows を使用する場合は、機密漏れの可能性があることについてもユーザーに指示する必要があります。ユーザーが iSeries 資源の識別に UNC (汎用命名規則) を指定すると、Win95 クライアントまたは Windows NT クライアントは、ネットワーク接続を確立してサーバーにリンクします。ユーザーは UNC を指定するため、ユーザーはこれをマップされたネットワーク・ドライブとして考えません。ユーザーがネットワーク接続の存在について気付かないことさえよくあります。しかし、サーバーは PC のディレクトリー・ツリーに表示されるため、このネットワーク接続は、ユーザー不在の PC で機密漏れするのと同じです。ユーザーのセッションに強力なユーザー・プロファイルがある場合、サーバーの資源がユーザー不在の PC で機密漏れするおそれがあります。上記の例の場合、解決方法は、ユーザーに機密漏れについて必ず理解させ、さらに PC のロック機能を必ず使用させることです。

リモート・コマンドとリモート・プロシージャーからのサーバーの保護

知識が豊富な PC ユーザーが iSeries Access などのソフトウェアを使用して、「サインオン」画面を使用せずにサーバー上のコマンドを実行することができます。 PC ユーザーが サーバーのコマンドを実行するのに使用できるいくつかの方法は、以下のとおりです。クライアント/サーバー・ソフトウェアが、PC ユーザーの使用できる方法を決めます。

- ユーザーは、DDM ファイルを開いて、リモート・コマンド機能を使用すると、コマンドを実行することができる。

- iSeries Access Optimized Clients などの一部のソフトウェアは、DDM を使用せずに分散プログラム呼び出し (DPC) API を通じてリモート・コマンド機能を提供する。
- リモート SQL および ODBC などの一部のソフトウェアは、DDM や DPC を使用しなくても、リモート・コマンド機能を提供する。

リモート・コマンド・サポート用に DDM を使用するクライアント/サーバー・ソフトウェアの場合、リモート・コマンドを完全に防止するために DDMACC ネットワーク属性を使用することができます。他のサーバー・サポートを使用するクライアント/サーバー・ソフトウェアの場合、サーバー用に出口プログラムを登録することができます。リモート・コマンドを許可する場合、必ず、オブジェクト権限構造でデータを適切に保護するようにしてください。リモート・コマンド機能は、ユーザーにコマンド行を提供することと同等です。さらに、iSeries が DDM を通じてリモート・コマンドを受け取ると、システムはユーザー・プロファイルの制限機能 (LMTCPB) 設定を実施しません。

リモート・コマンドとリモート・プロシージャーからのワークステーションの保護

IBM iSeries Access for Windows には、PC でリモート・コマンドを受け取る機能があります。サーバーでリモート・コマンドの実行 (RUNRMTCMD) コマンドを使用すると、接続した PC でプロシージャーを実行することができます。RUNRMTCMD 機能は、システム管理者とヘルプ・デスク担当者にとって役に立つツールです。しかし、この機能は、故意あるいは偶然に PC データを損傷する機会も与えてしまいます。

PC には、iSeries サーバーのようなオブジェクト権限機能はありません。RUNRMTCMD コマンドによる問題から保護するための最善の方法は、コマンドにアクセスできるシステム・ユーザーを注意して制限することです。IBM iSeries Access for Windows には、特定の PC でリモート・コマンドを実行できるユーザーを登録する機能があります。接続が TCP/IP 経由のときには、リモート・コマンド・アクセスを制御するためにクライアントで特性制御パネルを使用することができます。ユーザーの許可は、ユーザー ID またはリモート・システム名で行うことができます。接続が SNA 経由のときには、一部のクライアント・ソフトウェアは会話用にセキュリティーをセットアップする機能を提供します。その他のクライアント・ソフトウェアを使用する場合には、着信コマンド機能をセットアップするかどうかを単純に選択します。

クライアント・ソフトウェアと接続タイプ (TCP/IP や SNA など) の組み合わせごとに、接続されている PC への着信コマンドの可能性を検討する必要があります。クライアントの資料で「着信コマンド」または「RUNRMTCMD」を検索して、調べてください。この機能を許可または防止するようにクライアントを構成する正しい (セキュアな) 方法について、PC ユーザーとネットワーク管理者にアドバイスする準備をします。

ゲートウェイ・サーバー

システムは、iSeries システムと PC の間に中間サーバーやゲートウェイ・サーバーがあるネットワーク上に存在する場合があります。たとえば、iSeries システムが、PC サーバーを使用して LAN (サーバーに接続している複数の PC が含まれている) に接続しているとします。この状態のセキュリティーの問題は、ゲートウェイ・サーバーで実行中のソフトウェアの機能によって異なります。 図 13 に、ゲートウェイ・サーバー構成の例を示します。

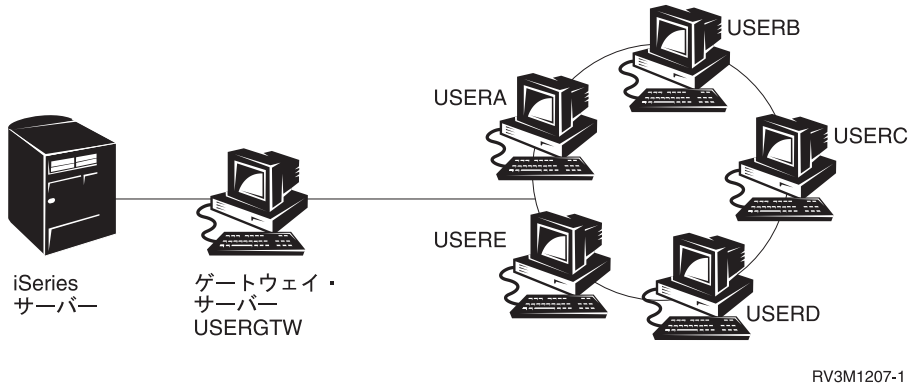

図 13. ゲートウェイ・サーバーを持つ iSeries システム

ソフトウェアによっては、iSeries システムは、ゲートウェイ・サーバーからのダウンストリームであるユーザー (USERA や USERC など) について認識できません。サーバーは、単一ユーザー (USERGTW) としてシステムにサインオンします。サーバーは、ダウンストリーム・ユーザーからのすべての要求を処理するのに、USERGTW ユーザー ID を使用します。 USERA からの要求は、サーバーにはユーザー USERGTW からの要求のように見えます。

この場合、セキュリティーの実施についてゲートウェイ・サーバーに依存しなければなりません。そして、ゲートウェイ・サーバーのセキュリティー機能を理解および管理しなければなりません。 iSeries サーバーから見ると、すべてのユーザーは、ゲートウェイ・サーバーがセッションを開始するのに使用するユーザー ID と同じ権限を持つことになります。このことは、権限を借用し、コマンド行を提供するプログラムを実行するのと同等と考えることができます。

その他のソフトウェアの場合、ゲートウェイ・サーバーは個々のユーザーからの要求を iSeries サーバーに渡します。iSeries サーバーは、USERA が特定オブジェクトへのアクセスを要求していることを認識します。ゲートウェイは、システムに対してほとんど透過的です。

システムが、ゲートウェイ・サーバーのあるネットワーク上に存在する場合、ゲートウェイ・サーバーが使用するユーザー ID にどの程度の権限を提供するかを評価する必要があります。また、以下のことを理解する必要もあります。

- ゲートウェイ・サーバーが実施するセキュリティーのメカニズム。
- ダウンストリーム・ユーザーが iSeries システムにどのように見えるか。

無線 LAN 通信

一部のクライアントは、iSeries 無線 LAN を使用してシステムと無線で通信する場合があります。 iSeries 無線 LAN は、無線周波数通信技術を使用します。機密保護管理者は、iSeries 無線 LAN 製品の次のようなセキュリティー特性について理解しておく必要があります。

- これらの無線 LAN 製品は、スペクトル拡散技術を使用しています。これと同じテクノロジーは、これまで無線伝送を安全に行うために米国政府によって使用されてきました。データ伝送を電子的にモニターしようとする人にとって、そのデータ伝送は、実際の伝送ではなくノイズのように見えます。
- 無線接続では、次の 3 つのセキュリティー関連の構成パラメーターが使用されます。
  - データ転送速度 (2 つのデータ転送速度が可能)
  - 周波数 (5 つの周波数が可能)
  - システム識別コード (800 万の識別コードが可能)

  これらの構成要素を組み合わせると 8000 万種類の構成が可能になり、ハッカーが正しい構成を探そうとしてもそれがみつかる可能性は非常に小さくなります。
- 他の通信方式の場合と同様に、無線通信のセキュリティーはクライアント装置のセキュリティーによって影響されます。システム ID 情報と他の構成パラメーターは、クライアント装置のファイルに入っており、保護されていなければなりません。
- 無線装置がなくなるか盗まれた場合に、非許可ユーザーがこのなくなった装置または盗まれた装置を使用してユーザー・システムにアクセスしようとすると、通常のサーバーのセキュリティー措置 (たとえば、サインオン・パスワードやオブジェクト・セキュリティー) が保護を行います。
- 無線クライアント装置が無くなるか盗まれた場合は、すべてのユーザー、アクセス・ポイント、およびシステムに関するシステム ID 情報を変更することを考えてください。これはちょうど、自分の家の鍵が盗まれた場合にドアのロックを変えるようなものです。
- サーバーを、固有なシステム ID を持ついくつかのクライアント・グループに分割することもできます。こうすれば、装置がなくなったり盗まれたりした場合の影響を低くおさえることができます。この方式が機能するのは、一連のユーザーをインストール・システムの特定部分に限定できる場合のみです。
- 配線式 LAN 技術とは異なり、無線 LAN 技術は、メーカー独自の仕様になっています。したがって、こうした無線 LAN を対象にした盗聴機は、一般に入手することはできません。盗聴機とは、伝送を無許可でモニターする電子装置をいいます。

第 15 章 セキュリティー出口プログラム

一部の iSeries サーバー機能には出口が設けられているため、システムでユーザー作成プログラムを実行して追加の検査と妥当性検査を行うことができます。たとえば、誰かがシステム上で DDM (分散データ管理) ファイルをオープンしようとすると、そのたびにシステムで出口プログラムを実行するようにセットアップすることができます。登録機能を使用して、特定の条件下で実行する出口プログラムを指定できます。

いくつかの iSeries 資料には、セキュリティー機能を実行する出口プログラムの例が示されています。 表 24 は、これらの出口プログラムと例示プログラムの情報源のリストを示しています。

表 24. サンプル出口プログラムのソース

出口プログラムのタイプ	目的	例の入手先
パスワード妥当性検査	QPWDVLDPGM システム値は、プログラム名を指定したり、QPWDxxx システム値によって処理されない追加要件のための新規パスワードを検査するために使用される QIBM_QSY_VLD_PASSWRD 出口点用に登録されている妥当性検査プログラムを示すことができます。このプログラムは暗号化されていないパスワードを受け取るので、このプログラムの使用については慎重にモニターする必要があります。このプログラムでファイルにパスワードを格納したり、他のプログラムにパスワードを渡したり**しないでください。**	• *An Implementation Guide for iSeries Security and Auditing, GG24-4200* • *iSeries 機密保護解説書*, SD88-5027-07
PC サポート /400 または Client Access のアクセス [1]	このプログラム名をネットワーク属性のクライアント要求アクセス (PCSACC) パラメーターに指定して、以下の機能を制御することができます。 • 仮想印刷装置機能 • ファイル転送機能 • 共用フォルダー・タイプ 2 機能 • クライアント・アクセス・メッセージ機能 • データ待ち行列 • リモート SQL 機能	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*
分散データ管理機能 (DDM) アクセス	このプログラム名をネットワーク属性の DDM 要求アクセス (DDMACC) パラメーターに指定して、以下の機能を制御することができます。 • 共用フォルダー・タイプ 0 および 1 機能 • リモート・コマンド投入機能	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*

表 24. サンプル出口プログラムのソース (続き)

出口プログラムのタイプ	目的	例の入手先
リモート・サインオン	プログラムを QRMTSIGN システム値に指定して、どのユーザーをどこの場所 (パススルー) から自動的にサインオンできるようにするかを制御することができます。	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*
iSeries Access で使用の Open Database Connectivity (ODBC)[1]	次のような ODBC の機能を制御します。 • ODBC の全ての使用を許可するかどうか • iSeries データベース・ファイルに対してどの機能を許可するか • どの SQL ステートメントを許可するか • データベース・サーバー・オブジェクトに関するどの情報を検索するか • どの SQL カタログ機能を許可するか	なし
QSYSMSG 中断処理プログラム	QSYSMSG メッセージ待ち行列をモニターするプログラムを作成し、メッセージのタイプに応じて適切な処置 (たとえば、機密保護管理者に知らせる) を取ります。	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*
TCP/IP	いくつかの TCP/IP サーバー (たとえば、FTP、TFTP、TELNET、REXEC など) には出口点が設けられています。出口プログラムを追加して、ログオンを処理したり、ユーザー要求 (たとえば、特定のファイルの読み取りや書き込み) を妥当性検査したりできます。これらの出口を使用して、システムに匿名の FTP を与えることもできます。	『*iSeries System API Reference* の TCP/IP ユーザー出口』
ユーザー・プロファイルの変更	以下のユーザー・プロファイル・コマンドのための出口プログラムを作成することができます。 CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *iSeries 機密保護解説書*, SD88-5027-07 • 『*iSeries System API Reference* の TCP/IP ユーザー出口』

注:

1. このトピックについての追加情報は、iSeries Information Center にあります。詳細は、 xii ページの『前提条件および関連情報』を参照してください。

第 16 章 インターネット・ブラウザーのセキュリティーに関する考慮事項

部門の多くの PC ユーザーが、それぞれのワークステーションにブラウザーを導入しています。これらのユーザーはインターネットに接続することもありますし、サーバーに接続することもあります。以下に、PC およびサーバーの両方のセキュリティーに関する考慮事項について説明します。

リスク: ワークステーションの損傷

ユーザーがアクセスする Web ページは、関連する「プログラム」(たとえば、Java アプレット、Active-X 制御、または他の何らかのタイプのプラグイン) を持っていることがあります。めったにないことですが、このタイプの「プログラム」が PC で実行されると、PC に関する情報が損傷を受けることがあります。機密保護管理者は、組織内の PC を保護するために以下の点を考慮してください。

- ユーザーが持っている各種のブラウザーのセキュリティー・オプションを理解します。たとえば、一部のブラウザーでは、Java アプレットがブラウザーの外部にアクセスするのを制御することができます (Java の制限付き操作環境を *sandbox* と呼びます)。これにより、アプレットが PC データに損傷を与えるのを防止することができます。

  注: Active-X およびその他のプラグインの場合は、sandbox の概念とそれに関連するセキュリティー上の制約事項はありません。
- ユーザーに、ブラウザー設定に関する推奨事項を提供します。ユーザーがこの推奨事項を守っているかどうかを確認する時間や資源はないかもしれません。したがって、設定が不適切な場合のリスクの可能性について、ユーザーを教育しておく必要があります。
- 必要なセキュリティー・オプションを提供する Web ブラウザーの標準化を考えます。
- 特定の Web サイトに関連すると思われるような不審な動作や症状が見られたときは、通知するようにユーザーに指示しておきます。

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

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

ここで、同じ PC ユーザーがブラウザーをもち、インターネットにアクセスできるものと仮定します。ユーザーは、Java アプレットや Active-X 制御など害を及ぼす

「プログラム」を実行する Web ページを要求します。このプログラムは PC の G ドライブに含まれているすべてのデータを消去する可能性があると考えられます。

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

- 最も重要な保護処置は、サーバーに関するリソース・セキュリティーです。Java アプレットや Active-X 制御は、サーバーからは、PC セッションを確立したユーザーのように見えます。サーバーでどの PC ユーザーにどの操作を許可するかについて、注意深く管理する必要があります。
- マップされたドライブへのアクセス試行を防止するようにブラウザーを設定することを、 PC ユーザーに指示しておく必要があります。この方法は Java アプレットには効果がありますが、sandbox 概念をもたない Active-X 制御には効果がありません。
- 同一セッションでサーバーとインターネットに接続することの危険性について、ユーザーに指示しておく必要があります。また、iSeries Access セッションが終了したように見えても、ドライブがマップされたままになっていることを PC (例えば、Windows 95 クライアント) のユーザーに理解してもらうことも必要です。

リスク: 署名済みのアプレットの承認

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

署名済みアプレットには、それを認証するための関連するディジタル署名が付けられています。ユーザーが署名済みアプレットを持つ Web ページにアクセスすると、メッセージが出されます。このメッセージには、アプレットの署名 (誰がいつそれに署名したか) が示されています。アプレットを受け入れると、ユーザーは、アプレットがブラウザーのセキュリティー設定をオーバーライドするのを認可することになります。署名済みのアプレットは、ブラウザーのデフォルト設定によって PC ローカル・ドライブへの書き込みが禁止されていても、それを行うことができます。署名済みアプレットは、サーバー上のマップされたドライブにも書き込むことができます。なぜならば、PC には、これらのドライブがローカル・ドライブのように見えるからです。

サーバーで生成されたユーザー独自の Java アプレットの場合は、署名済みアプレットを使用しなければならないことがあります。ただし、ソースのはっきりしない署名済みアプレットは、通常は受け入れないようユーザーを指導しておく必要があります。

第 17 章 関連情報

マニュアル

- 「*AS/400 アドバンスト・シリーズ APPC プログラミング*, SD88-5032-00」は、iSeries システムの拡張プログラム間通信機能 (APPC) サポートについて説明しています。この資料は、APPC を使用するアプリケーション・プログラムの開発と、APPC 通信のための通信環境の定義について説明しています。この資料には、アプリケーション・プログラムに関する考慮事項、構成要件とコマンド、APPC の問題管理、およびネットワーキングに関する一般的な考慮事項が示されています。iSeries Information Center CD-ROM を参照してください。
- 「*AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet*」レッドブック (SG24-4929) は、セキュリティーに関する問題と、iSeries をインターネットに接続する場合のリスクについて説明しています。この資料には、 TCP/IP アプリケーションに関する例や推奨事項、ヒント、技法などが示されています。
- 「*バックアップおよび回復の手引き*, SD88-5008-07」は、バックアップおよびリカバリーのストラテジーの計画、システムの情報の保管、およびシステムのリカバリーについて説明しています。 iSeries Information Center を参照してください。これらのトピックに関する追加情報は iSeries Information Center にもあります。詳細は、 xii ページの『前提条件および関連情報』を参照してください。
- 「*CL プログラミング*, SD88-5038-06」は、外部記述が可能なファイルのデータ記述仕様 (DDS) をコーディングする方法について詳しく説明しています。このようなファイルとしては、物理、論理、表示、印刷、およびシステム間通信機能 (ICF) ファイルがあります。 iSeries Information Center を参照してください。
- Information Center の『CL』トピック (詳細については、 xii ページの『前提条件および関連情報』を参照) は、すべての iSeries 制御言語 (CL) およびその OS/400 コマンドについて説明しています。 OS/400 コマンドは、OS/400® (5722-SS1) ライセンス・プログラムの機能を要求する場合に使用します。各種言語やユーティリティーを含め、その他のライセンス・プログラムに関連する OS/400 CL 以外のコマンドについては、それらのライセンス・プログラムをサポートするマニュアルを参照してください。
- 「*Implementing iSeries Security, 3rd Edition*」Wayne Madden および Carol Woodbury 著 (Loveland、Colorado: 29th Street Press、a division of Duke Communications International、1998)。この資料は、iSeries セキュリティーの計画、セットアップ、および管理に関するガイダンスと実際的な推奨事項を示しています。

  ISBN オーダー番号:

  1-882419-78-2
- HTTP サーバーの詳細については、次の URL を参照してください。

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- 「*iSeries 機密保護解説書*, SD88-5027-07」は、セキュリティー・システム値、ユーザー・プロファイル、リソース・セキュリティー、およびセキュリティー監査について詳しく説明しています。この資料は、特定のライセンス・プログラム、

言語、およびユーティリティーのセキュリティーについては説明していません。 iSeries Information Center を参照してください。

- Information Center の『システム操作の基本』トピックは、 iSeries の基本操作に必要な主要な概念とタスクを説明しています。詳細は、 xii ページの『前提条件および関連情報』を参照してください。
- Information Center では、TCP/IP と、FTP、SMTP、TELNET などの TCP/IP アプリケーションの使用方法と構成方法を説明しています。詳細は、 xii ページの『前提条件および関連情報』を参照してください。
- 「*TCP/IP File Server Support for OS/400 Installation and User's Guide*」(SC41-0125) には、File Server Support ライセンス・プログラム・オファリングの紹介、導入手順、およびセットアップ手順が示されています。この資料は、製品とともに使用可能になる各機能について説明し、この製品を他のシステムで使用する際の例やヒントを提示しています。
- 「*Trusted Computer Systems Evaluation Criteria*」(DoD 5200.28.STD) は、コンピューター・システムの承認レベルの基準について説明しています。TCSEC は、米国政府の出版物です。この出版物は、以下のアドレスから入手することができます。

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Attention: Chief, Computer Security Standards
- Information Center には、iSeries 上のシステム管理機能および実行管理機能に関するトピックが含まれています。これらのトピックの中には、パフォーマンス・データ収集、システム値管理、ストレージ管理などが含まれます。 Information Center へのアクセス方法については、 xii ページの『前提条件および関連情報』を参照してください。「実行管理の手引き」(SD88-5009) は、実行管理機能環境の作成方法と変更方法について説明しています。 iSeries Information Center を参照してください。

これらの Information Center トピックや補足資料のほかに、次の資料を参考にすることができます。

- **IBM SecureWay**
  IBM SecureWay は、お客様の情報テクノロジーの保護に役立てるために、 IBM が広範囲にわたって蓄積しているセキュリティー・オファリング、つまりハードウェア、ソフトウェア、コンサルティング、およびサービスについて共通のブランドを提供します。個々のニーズを対象とするか、企業全体のソリューションに取り組むのかを問わず、 IBM SecureWay オファリングは、ビジネスのためのセキュアなソリューションの計画や設計、実施、操作などに必要な専門技術を提供します。 IBM SecureWay オファリングの詳細については、次の IBM SecureWay ホーム・ページを参照してください。

  `http://www.ibm.com/secureway`
- **サービス・オファリング**
  新しいハードウェアやソフトウェアを導入すれば、仕事の効率や運営を大幅に向上させることができます。しかし、仕事に支障をきたしたり、ダウン時間が発生する恐れもあり、大切な内部資源に負担がかかることもあります。 IBM グロー

バル・サービスは iSeries セキュリティーに関するサービスを提供しています。iSeries に関する全サービスのリストについては、次の Web サイトを参照してください。

http://www.as.ibm.com/asus

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あり、米国以外の国においては本書で述べる製品、サービス、またはプログラムを提供し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。使用許諾については、下記の宛先に書面にてご照会ください。

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

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

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

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

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

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

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

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

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。

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。

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。お客様は、IBM 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。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

以下は、IBM Corporation の商標です。

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2DRDA
e (ロゴ)
IBM
iSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

Action Media、LANDesk、MMX、Pentium および ProShare は Intel Corporation の米国およびその他の国における商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは、Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

UNIX は、The Open Group の米国およびその他の国における登録商標です。

他の会社名、製品名およびサービス名などはそれぞれ各社の商標または登録商標です。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

［カ行］

[サ行]

[タ行]

[ナ行]

[ハ行]

［マ行］

[ヤ行]

[ラ行]

[ワ行]

[数字]

A

B

C

D

E

F

I

J

L

O

P

Q

R

S

T

U

W

[特殊文字]

Printed in Japan

SD88-5065-05

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