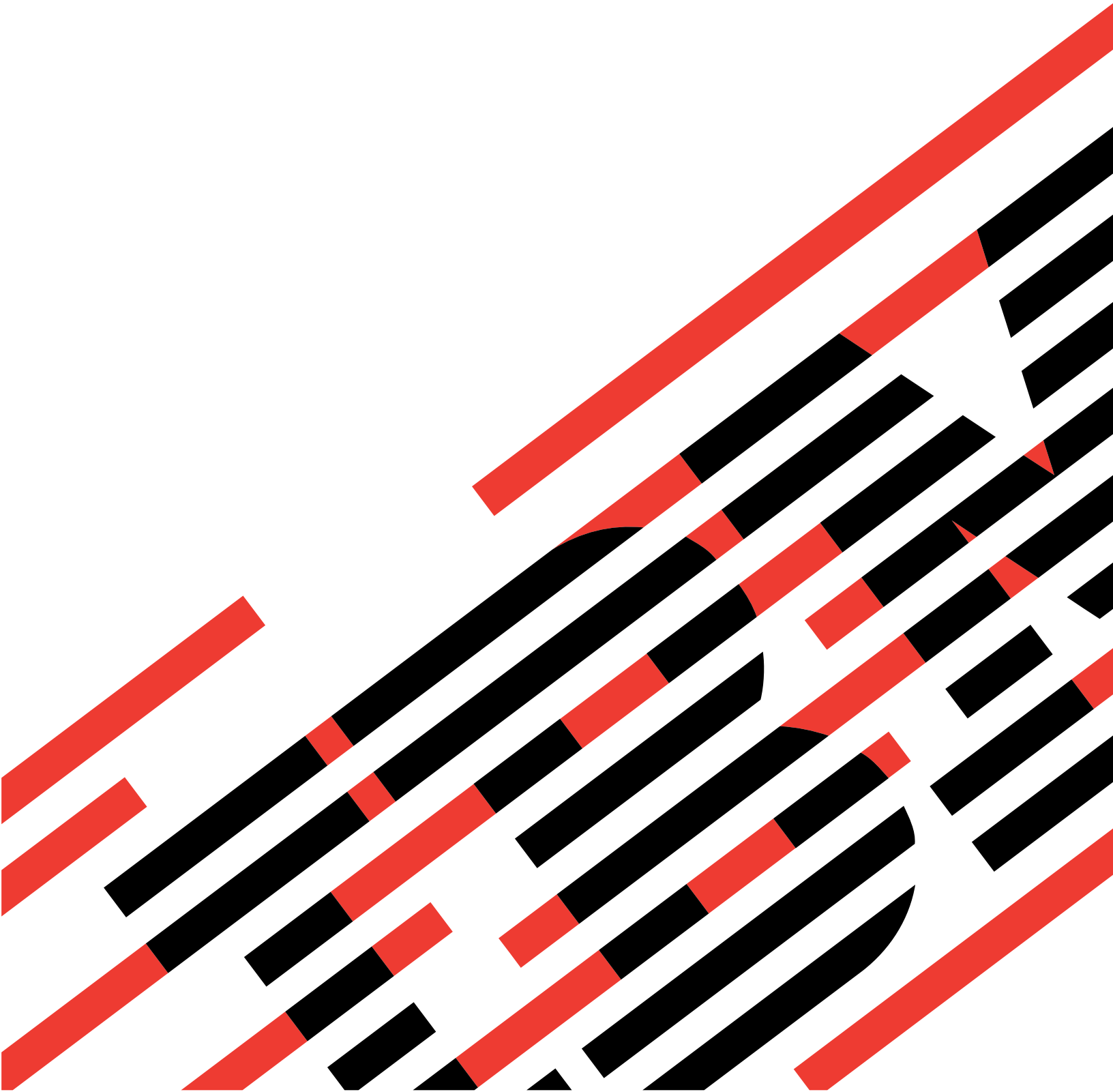
IBM

eserver

iSeries

基本システム セキュリティーおよび計画

バージョン 5 リリース 3



IBM

@server

iSeries

基本システム セキュリティーおよび計画

バージョン 5 リリース 3

お願い

本書および本書で紹介する製品をご使用になる前に、 147 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 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： iSeries
Basic system security and planning
Version 5 Release 3

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2005.8

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

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

目次

基本システム セキュリティーおよび計画

『基本システム セキュリティーおよび計画』では、iSeries™ システムにおけるセキュリティーの計画と設定について、詳細に説明します。このトピックは、セキュリティーの計画に焦点をあてており、セキュリティー上の決定を計画し、記録するための用紙が用意されています。また、基本システム・セキュリティーの設定を段階的に説明しています。このトピックはワークブックのようになっているため、ページを印刷すると、資料をより全体的に概観することができて便利です。

ご使用の iSeries に最適なセキュリティーを設定するには、大きく分けて計画タスクと構成タスクの 2 つの作業が必要です。ビジネスの必要に合ったセキュリティーを設定するため、次のような計画のトピックを検討する必要があります。

- 『基本システム・セキュリティー入門』では、一般的なセキュリティーの概念について概観し、基本システム・セキュリティーに関する疑問に答えています。
- 『ユーザー・セキュリティーの計画』では、ご使用のシステムで作業するユーザーに影響を及ぼすセキュリティーを計画する方法を示します。これには、システムにおける物理的セキュリティー、アプリケーションのセキュリティー、セキュリティーに関するユーザーのすべての戦略、およびユーザー・プロファイルが含まれます。
- 『資源保護の計画』では、システム上でオブジェクトのセキュリティーを計画する方法を示します。これには、オブジェクト内のライブラリーとオブジェクト、印刷装置、印刷装置出力、およびワークステーションなどのセキュリティーが含まれます。

計画が完了した後、以下のトピックを検討して、システムへのセキュリティーの設定に役立てることができます。

- 『ユーザー・セキュリティーの設定』では、ユーザーおよびグループのセキュリティーの設定について説明しています。
- 『資源保護の設定』では、オブジェクトの所有権、オブジェクトに対する共通権限と特定権限、および印刷装置とワークステーションのセキュリティーを設定する方法を示しています。
- 『セキュリティーのテスト』は、セキュリティーのテストについて扱っています。
- 『セキュリティー情報の変更』は、ユーザーおよびグループ・プロファイルの更新と修正、および資源保護の更新と修正について扱っています。
- 『セキュリティー情報の保管』は、セキュリティー情報のバックアップについて扱っています。
- 『セキュリティーの監視』には、セキュリティーを追跡するためのチェックリストがあり、セキュリティーの監査に関する情報が含まれています。

これらのトピックに加え、計画用紙を使用して、計画の戦略とセキュリティー上の決定を文書の形にします。

トピックの印刷

この文書の PDF 版を参照用または印刷用にダウンロードし、表示することができます。PDF ファイルを表示したり印刷したりするには、Adobe® Acrobat® Reader が必要です。これは、Adobe の Web サイト


から、ダウンロードできます。

PDF 版をダウンロードし、表示するには、「基本システム セキュリティーおよび計画」(約 1203 KB、160 ページ) を選択します。

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

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. ブラウザーのメニューから「**ファイル**」をクリックする。
3. 「**名前を付けて保存**」をクリックする。
4. PDF を保管したいディレクトリーに進む。
5. 「**保存**」をクリックする。

基本システム・セキュリティー入門

セキュリティーは、システム管理者からユーザーに至るまで、すべての人が関心を持つべき問題です。システム・セキュリティーは、iSeries およびユーザーが持つ業務上の機密情報を、意図的なセキュリティー違反 (ブリーチ) と意図的ではないセキュリティー違反の両方から保護します。

システム・セキュリティーは、ユーザーのセキュリティー環境やニーズを基にしてカスタマイズすることができます。

セキュリティーはシステムへの入り口であると考えてください。ユーザーはセキュリティー機能を使用して、情報が許可なく使用されないように**キーをかける (ロック)** または保護します。

また、セキュリティー機能を使用してシステムの柔軟性のために**ロック解除**し、各ユーザーに合わせてカスタマイズすることもできます。

優れたセキュリティーの計画はシステムを保護するものの、システム内の装置や情報の安全を保証することはできません。そのため、システムの責任を複数の従業員の間で分割し、1 人のユーザーがシステムを排他的に制御することがないようにする必要があります。

『基本システム・セキュリティーおよび計画』では、基本システム・セキュリティーの計画と設定の段階的なアプローチについて説明しています。このトピックでは、システム・セキュリティーの重要性を強調しており、セキュリティー上の決定を記録するための計画用紙が用意されています。このトピック全体では、セキュリティーに関する決定を容易にするため、セキュリティーを計画する 1 つの企業の例を使用しています。

システム・セキュリティーを確実に成功させるためには、十分に検討された綿密な計画が不可欠です。以下のトピックから、基本的なセキュリティーに必要なものと、セキュリティー計画の重要性について検討してください。

- 基本システム・セキュリティーに関する一般的な質問 (FAQ)
- 基本システム・セキュリティーの概要
- 基本システム・セキュリティーを計画する方法

また、システム上にあるすべての情報のバックアップと回復についても、綿密な計画が必要です。加えて、災害が起きた場合の装置の置き換えについても計画する必要があります。優れたバックアップの計画を立てるための詳細については、Information Center の『バックアップおよび回復』のトピックを参照してください。

ユーザー・セキュリティーに関する詳細な計画の情報

以下のトピックでは、ユーザー・セキュリティーを計画するための手法を示しています。
- アプリケーションのセキュリティーの計画
- セキュリティー戦略の計画
- ユーザー・グループの計画
- 個々のユーザー・プロファイルの計画

資源保護に関する詳細な計画の情報

以下のトピックでは、ユーザー向けの資源保護の計画を系統立てて説明しています。
- 権限のタイプの理解
- アプリケーション・ライブラリーのセキュリティーの計画
- ライブラリーとオブジェクトの所有権の決定
- オブジェクトのグループ化
- 印刷装置出力の保護
- ワークステーションの保護
- アプリケーションの導入の計画

印刷可能な計画用紙

基本システム・セキュリティーおよび計画には印刷可能な計画用紙があり、セキュリティー上のすべての決定を記録することができます。このトピック全体を PDF として印刷することもできるほか、ブラウザーの「印刷」ボタンを使用してそれぞれの計画用紙を個別に印刷することもできます。

基本システム・セキュリティーの段階的な設定の説明

このトピックでは、セキュリティーの計画が完了した後、セキュリティーの計画を実行するための手順を示しています。以下のトピックには、システム・セキュリティーの設定に役立つ情報が含まれています。
- ユーザー・セキュリティーの設定
- 資源保護の設定

基本システム・セキュリティーに関する一般的な質問 (FAQ)

セキュリティーに関する一般的な質問 (FAQ) に対する答えを検討すると、システム・セキュリティーの重要性をさらに理解する上で役立ちます。

なぜセキュリティーが重要なのか ?

システムに保管される情報は、最も重要なビジネス資産の 1 つです。情報資産を保護する方法を検討する場合、次の 3 つの重要な目的に留意してください。
- **機密性:** セキュリティー上の適切な対策により、他人が機密情報を見たり、その内容を公表したりすることを防ぐことができます。
- **保全性:** 適切に設計されたセキュリティー・システムは、コンピューター上の情報の正確さをある程度まで保証することができます。正しいセキュリティーを行えば、許可なくデータが変更されたり、削除されたりすることを防ぐことができます。
- **可用性:** 誰かが誤ってあるいは故意にシステムのデータに損害を与えた場合、データを回復するまでそれらの資源にはアクセスできなくなります。適切なセキュリティー・システムは、この種の損害を防ぐことができます。

システム・セキュリティーが検討される場合、大抵は、ビジネス上のライバルなどの外部の人間から組織のシステムを保護することが検討されます。実際のところ、適切に設計されたセキュリティー・システムの最大の効果は、正当なユーザーによる詮索 (せんさく) やシステム事故からシステムを保護することにあります。適切に設計されたセキュリティーを持たないシステムでは、ユーザーが意図せずに重要なファイルを削除してしまう場合があります。適切なセキュリティー・システムは、この種の事故を防止する上で役立ちます。

ご使用のシステムにどの程度のセキュリティーが必要かを判断するために、次のような質問を考慮してみてください。

- ご使用のコンピューター (およびそこに保管されているデータ) は、ビジネスにおいてどれほど重要ですか ?
- 特定のレベルのセキュリティーを必要とする、会社としての方針をお持ちですか ?
- ご使用のコンピューターに保管されている情報について、監査役には特定のレベルのセキュリティーが必要ですか ?
- 近い将来、ある程度のセキュリティーが必要になるでしょうか ?

なぜシステムをカスタマイズするのか ?

iSeries は幅広い層のユーザーによって使用されます。小規模なシステムでは 3 人から 5 人程度のユーザーが、2、3 のアプリケーションを実行するものがあります。大規模なシステムでは、多くのアプリケーションを実行する大規模な通信ネットワークで、数千人のユーザーがシステムを使用する場合もあります。

iSeries システムは、広範囲のユーザーや状況に対応するため、幅広い柔軟性を提供するように設計されています。ユーザーから見たシステムの外見、またはシステムが実行する方法について、多くの変更を加えることができます。

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

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

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

誰が責任を持つか ?

セキュリティーへのアプローチは、企業によって異なります。ある場合には、プログラマーが、セキュリティーのすべての局面において責任を持ちます。また、別の場合には、システムを管理する人がセキュリティーも担当することがあります。会社で責任を割り当てる方法が明確でない場合は、以下で推奨されている方法を参考にしてください。

- 資源のセキュリティーを計画する方法は、会社がアプリケーションを購入するか、あるいは開発するかに応じて異なります。独自のアプリケーションを開発される場合は、開発プロセスで資源保護の必要を伝えてください。アプリケーションを購入される場合は、アプリケーションの設計担当者と意思の疎通

をして、協力して作業してください。いずれの場合にも、アプリケーションの設計者は、設計の一環としてセキュリティーを考慮に入れる必要があります。

- セキュリティーの設定については、機密保護担当者が責任を持ちます。機密保護担当者はシステムのユーザーと、システムに対するそれらのユーザーのアクセスを定義します。機密保護担当者は、しばしば、情報のバックアップや回復など、システムにかかわる他の事柄にも責任を持ちます。
- また、セキュリティーの多くの要素は、システムのカスタマイズにおいて重要な役割を持つため、システムのカスタマイズも機密保護担当者が行います。

どのような方法を使用してセキュリティーの責任を割り当てる場合でも、**セキュリティーの方針を伝えてください。**会社の幹部役員の方が全社員に、できれば書面で、コンピューターに含まれている情報が重要な資産であることを伝える必要があります。会社の他のいかなる資産と同様に、この情報資源を保護する必要があります。セキュリティー方針の例は、『例: JKL Toy Company のセキュリティー方針』を参照してください。

さて、これまでの部分で、ご使用のシステムにおけるセキュリティーの必要性について理解することができました。続いて、システム・セキュリティーの考慮事項について概要を検討します。

基本システム・セキュリティーの概要

効果的な計画を立てるには、目標の対象が、システムの提供するツールとどのように関係するかを理解する必要があります。目標の達成を容易にするために、ユーザーとシステムの機能がどのように共同作業するのかを把握してください。

以下のトピックでは、セキュリティーとカスタマイズの重要な部分を紹介し、それらがどのように互いに組み合わされるのかを示します。これらのトピックは、計画を始める前にその概要を示すためのものです。ここで紹介されるすべての概念は、計画のプロセスでそれらが必要になるときに、より詳細に説明されます。

- 組み込みシステム・セキュリティー
- 基本用語
- ユーザーの視点から見たセキュリティー
- セキュリティーおよびカスタマイズのためのシステム・ツール

組み込みシステム・セキュリティー

システム側のセキュリティーはすべて、システム内に組み込まれています。これらを別個の製品として購入することはできません。このようにセキュリティーを統合することには、以下のようないくつかの利点があります。

- セキュリティーは、オペレーティング・システムの他の部分との整合性を保ちます。セキュリティーにおいても、同じ画面、コマンド、および用語が使用されます。
- セキュリティーとソフトウェアは分離されていないため、ユーザーはセキュリティーをバイパスできません。
- 適切に設計されたセキュリティーは、パフォーマンスに最小限の影響しか与えません。
- セキュリティーは常に、新しいソフトウェアの開発と歩調を合わせています。新しい機能が使用可能になると、その機能に対するセキュリティーも使用可能になります。

iSeries は、セキュリティー・レベル 40 で出荷されます。このレベルでは、許可されていないユーザーによるシステムへのサインオンを防ぎます。また、セキュリティーの裏をかこうとするプログラムによる、保全性およびセキュリティーに対する潜在的なリスクを回避することもできます。ただし、特定のセキュリティーの設定をカスタマイズしたり、セキュリティーのレベルを変更したりすることもできます。セキュリティー・レベルについては、『セキュリティー・レベルの選択』で説明されています。

これで、組み込みセキュリティーがどのように動作するかについて理解していただけたと思います。続いて、iSeries に共通の用語について説明します。

基本用語

ここで説明する一般用語のセットは、iSeries のセキュリティーを理解する上で非常に重要です。

オブジェクト
オブジェクトとは、システム上の操作可能な名前付きスペースのことです。最も一般的なオブジェクトの例は、ファイルとプログラムです。別のタイプのオブジェクトには、コマンド、待ち行列、ライブラリー、およびフォルダーなどが含まれます。システム上のオブジェクトは、オブジェクト名、オブジェクト・タイプ、およびオブジェクトの存在するライブラリーによって識別されます。システム上の各オブジェクトは保護することができます。

ライブラリー
ライブラリーは、特殊なタイプのオブジェクトで、他のオブジェクトをグループ化するために使用されます。システム上の多くのオブジェクトは、ライブラリーにあります。

ディレクトリー
ディレクトリーは、システム上のオブジェクトをグループ化するもう 1 つの方法です。オブジェクトはディレクトリーに常駐することもできます。ディレクトリーは他のディレクトリーの下に存在して、階層構造を形成することができます。

これで、一般的な iSeries のセキュリティー用語に関する理解を深めることができました。続いて、ユーザーの視点から見たセキュリティーについて検討します。

ユーザーの視点から見たセキュリティー

ユーザーの視点から見ると、セキュリティーは、システム上でのタスクの使用方法や完了の仕方に影響を与えます。また、それらのタスクを完了するために、システムと相互作用する方法にも影響を与えます。そのため、セキュリティーがユーザーの視点からはどのように見えるのかを考慮することが大切です。たとえば、パスワードの有効期限が 5 日ごとに切れるように設定した場合、それはユーザーを失望させ、ユーザーがジョブを完了する際の遅延または妨げの原因となるかもしれません。一方、パスワードの方針が極端にあいまいな場合は、セキュリティーの問題を引き起こしかねません。

システムに適切なセキュリティーを設けるためには、セキュリティーを分割して、計画、管理、および監視が可能な特定の部分に分ける必要があります。ユーザーの視点から見ると、システムのセキュリティーはいくつかの部分に分けることができます。

システムへの物理的なアクセス

物理的セキュリティーは、システム装置、システム上にあるすべての装置、およびディスケットやテープ、または CD などのバックアップ記憶媒体が、意図せずに、あるいは意図的に失われたり損傷を受けたりするのを防ぎます。

システムの物理的セキュリティーを確保するために取るほとんどの手段は、システムに対して外部的なものです。しかし、出荷されるシステムには、システム装置で許可なく機能が使用されるのを防止する、キーロックや電子キースティックが装備されています。

『物理的セキュリティーの計画』では、システムの物理的セキュリティーを計画するために役立つ詳細な情報が提供されています。

ユーザーがサインオンする方法

サインオン・セキュリティーは、システム上で未確認のユーザーがサインオンするのを防ぎます。各ユーザーがサインオンするためには、ユーザー ID とパスワードの有効な組み合わせを入力しなければなりません。

サインオン・セキュリティーが違反されていないかどうかは、システム値と個々のユーザー・プロファイルの両方で確認することができます。たとえば、パスワードを一定の規則に基づいて変更するように指示することができます。また、容易に想像できてしまうパスワードの使用も避けることができます。

ユーザーに許可される操作

セキュリティーとシステムのカスタマイズにおいて重要な役割を果たすのは、ユーザーが実行できる操作を定義することです。セキュリティーの視点から、しばしば使用されるのは、ユーザーが特定の情報を見ることを禁止するなどの、**制限**機能です。システムのカスタマイズの視点から使用されるのは、**許可**機能です。適切にカスタマイズされたシステムでは、不必要な作業と情報を除去することによって、ユーザーがより効率的にジョブを行うことが可能です。

ユーザーが実行できる操作を定義する方法の中には、機密保護担当者が扱うものがあります。また、その他の方法はプログラマーの責任になります。この情報は主に、機密保護担当者が通常行う内容に焦点をあてたものです。「*機密保護解説書*」(SD88-5027) の第 3 章『セキュリティー・システム値』には、すべてのシステム値についての説明があります。

システム上でユーザーが実行できる操作を制御するために、個々のユーザー・プロファイル、ジョブ記述、およびクラスでパラメーターを使用することができます。下のリストは、使用可能な手法を簡単に説明したものです。

いくつかの機能にユーザーを制限する
: そのユーザー・プロファイルに基づいて、特定のプログラム、メニューまたはメニューのセット、およびいくつかのシステム・コマンドに対するユーザーを制限することができます。通常は、機密保護担当者がユーザー・プロファイルを作成および制御します。

システム機能を制限する
: システム機能を使用すると、情報の保管と復元、印刷装置出力の管理、および新しいシステム・ユーザーの設定を行うことができます。各ユーザー・プロファイルは、最も一般的なシステム機能のうち、ユーザーが実行できる機能を指定します。

  iSeries では、制御言語 (CL) コマンド、およびアプリケーション・プログラミング・インターフェース (API) を使用して、システム機能を実行することができます。各コマンドおよび API はオブジェクトであるため、オブジェクト権限を使用して、誰がそれらを使用してシステム機能を完了するかを制御することができます。

ファイルおよびプログラムを使用できるユーザーを決定する
: 資源保護には、システム上のすべてのオブジェクトの使用を制御する機能があります。どのオブジェクトに対してであれ、それを使用できるユーザーとその使用方法を指定することができます。たとえば、1 人のユーザーには、あるファイルの中の情報を見ることのみを許可し、別のユーザーにはファイル内のデータを変更できるように、また 3 番目のユーザーにはファイルを変更したり、ファイル全体を削除したりできるように指定することができます。

システム資源の乱用を防止する
: システム上の処理権限は、ビジネスにとって、システムに保管するデータと同じほど重要な事柄になる場合があります。機密保護担当者は、ユーザーがジョブを高い優先順位で実行したり、報告書を最初に印刷したり、過度に多くのディスク装置を使用するなど、システム資源を誤用することがないように支援します。

システムを他のコンピューターと通信させる方法

システムが他のコンピューターやプログラム式ワークステーションと通信する場合、付加的なセキュリティーの手段が必要になることがあります。適切なセキュリティー制御を行っていない場合、ネットワーク上の他のコンピューターのユーザーが、サインオンのプロセスを行わずにユーザーのマシンでジョブを開始したり、情報にアクセスしたりする場合があります。

システム値とネットワーク属性の両方を使用して、リモート・ジョブ、データのリモート・アクセス、またはシステム上でのリモート PC アクセスを許可するかどうかを制御することができます。リモート・アクセスを許可する場合は、施行するセキュリティーを指定することができます。「*機密保護解説書*」 (SD88-5027)  の第 3 章『セキュリティー・システム値』には、すべてのシステム値についての説明があります。

セキュリティー情報を保管する方法

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

『セキュリティー情報の保管』では、セキュリティー情報を保管する方法について説明します。 Information Center の『バックアップおよび回復』のトピックでは、セキュリティー・データのバックアップと回復について詳細に説明しています。

セキュリティーの計画を監視する方法

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

- 特定のセキュリティー違反が起きた場合は、システム操作員にメッセージが送られます。
- さまざまなセキュリティー関連のトランザクションを、特別な監査ジャーナルに記録することができます。

『セキュリティーの監視』では、これらのツールの使用について一般的な用語で説明しています。「*機密保護解説書*」 (SD88-5027)  の第 9 章『AS/400 システムにおけるセキュリティーの監査』では、セキュリティーの監査についてより詳細に説明しています。

システムをカスタマイズする方法をより理解するためには、ユーザーの視点からカスタマイズを理解する必要があります。

ユーザーの視点から見たシステムのカスタマイズ: ユーザーが日常の作業を行いやすくするために、システムをカスタマイズすることができます。ユーザーにとって最も使いやすいようにシステムをカスタマイズするには、作業を正常に実行するためにユーザーが何を必要としているかを考えてください。次のいくつかの方法でメニューおよびアプリケーションを表示するように、システムをカスタマイズすることができます。

ユーザーに必要なものを表示する

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

不必要なものを除去する

ほとんどのシステムには、数多くのさまざまなアプリケーションがインストールされています。しかし、ほとんどのユーザーが見たいのは、自分のジョブに必要なもののみです。システム上でユーザーが使用する機能をいくつかに制限するなら、ユーザーはジョブを実行しやすくなります。ユーザー・プロファイル、ジョブ記述、および該当するメニューを使用して、各ユーザーがシステムの特定の表示を使用できるようにすることができます。

適切な場所に適切なものを送る

どのようにして報告書を適切な印刷装置に送ることができるか、またはどのようにバッチ・ジョブを実行すればよいかを、ユーザーが心配するようなことがあってはなりません。システム値、ユーザー・プロファイル、およびジョブ記述を使用して、適切な場所に適切なものが確実に送られるようにします。

援助を提供する

システムのカスタマイズがいかに成功したとしても、ユーザーはやはり「私の報告書はどこへ行ったのだろう」とか、「私のジョブはもう実行されたのだろうか」といった疑問を抱くものです。**操作援助機能**の画面には、システム機能への簡単なインターフェースがあり、ユーザーがこれらの疑問に対する答えを得るのを助けます。**操作援助レベル**という、別のバージョンのシステム画面では、さまざまなレベルの技術的な経験を示したユーザーへの援助を提供しています。操作援助機能の画面は、システムを導入する際、すべてのユーザーに対して自動的に使用可能になります。ただし、アプリケーションを設計する際に、操作援助機能のメニューにアクセスする方法を自分で変更する必要があります。

iSeries では、ユーザーによる資源へのアクセスを許可し、一方でシステムのセキュリティーをカスタマイズしてこれらの資源を保護することのできるシステム・ツールが提供されています。

セキュリティーおよびカスタマイズのためのシステム・ツール

効果的な計画を立てるには、セキュリティー上の目標が、システムの提供するツールとどのように関係するかを理解する必要があります。システムのセキュリティーをカスタマイズする際に使用できる、次のようなシステム・ツールがあります。

セキュリティー・レベル

IBM は、すべての新しい iSeries をセキュリティー・レベル 40 で出荷します。セキュリティー・レベル 40 では、パスワード、資源保護、およびシステム保全性が守られます。システムで現在使用中のセキュリティーのレベルは、QSECURITY システム値を変更することによって変えることができます。ただし、IBM では、セキュリティー・レベルを 40 のままにしておくよう強くお勧めしています。セキュリティー・レベルを変更するためには、*SECOFR ユーザー・クラスか、*ALLOBJ および *SECADM 特殊権限が必要です。

システムには、以下の表で示す 4 つのセキュリティー・レベルが備えられています。

表 1. システムで使用可能なセキュリティー・レベル

セキュリティー・レベル	説明
セキュリティー・レベル 20	パスワードのセキュリティーのみ。
セキュリティー・レベル 30	パスワードおよび資源保護。
セキュリティー・レベル 40	パスワードおよび資源保護; 保全性のセキュリティー。
セキュリティー・レベル 50	パスワードおよび資源保護; 拡張された保全性のセキュリティー。

『セキュリティー・レベルの選択』では、必要に最も適したセキュリティー・レベルを決定する方法が説明されています。

システム値

システム値を設定して、ご使用の iSeries でオペレーティング・システムの特定の機能をどのように使用するかを制御することができます。システム値は、会社の方針であると考えてください。システム値は、ユーザー・プロファイルなどのより固有なものによって一時変更される場合を除き、システムを使用するすべての人に適用されます。

システム値は、主印刷装置、システムで日付を表示する方法、およびパスワードを変更する頻度などを決定します。

ネットワーク属性

ネットワーク属性は、システムを他のコンピューター (パーソナル・コンピューターを含む) と通信させる方法に関連した、いくつかの特性を定義します。ネットワーク属性はシステム全体に適用されます。

グループ・プロファイル

グループ・プロファイルは、ユーザーのグループを定義します。グループ・プロファイルは部門の方針であると考えてください。個々のユーザー・プロファイルを作成する際は、グループ・プロファイルをテンプレートとして使用することができます。また、グループ・プロファイルを使用して、システム上にあるオブジェクトに対するアクセスを、グループのメンバーにどのように許可するかを定義することもできます。グループ・プロファイルに関する詳細は、『ユーザー・グループの計画』を参照してください。

ユーザー・プロファイル

ユーザー・プロファイルは、システム上で最も強力で多目的に使用できるオブジェクトの 1 つです。ユーザー・プロファイルには、ユーザーのパスワードや、ユーザーがサインオンした後に表示されるメニューなどが含まれています。ユーザー・プロファイルは、そのユーザーがシステム上でできることとできないことを定義します。また、ユーザー独自のシステムの表示を決定します。『ユーザー・セキュリティーの計画』には、ユーザー・プロファイルを計画するためのヒントが示されています。

ジョブ記述

ジョブ記述は、システム値およびユーザー・プロファイルとともに使用して、システムがユーザーのジョブを処理する方法を決定します。ジョブ記述は、サインオンの後でユーザーが自動的にアクセスを獲得するライブラリーを判別する、初期ライブラリー・リストを設定します。

資源保護

機密保護担当者は、資源を使用する権限を持つユーザーと、ユーザーが資源にアクセスする方法を決定することにより、システム上の資源 (オブジェクト) を保護することができます。機密保護担当者は、個々のオブジェクトやオブジェクトのグループに、オブジェクト権限を設定することができます (権限リスト)。ファイル、プログラム、およびライブラリーは、保護が必要なオブジェクトの中で最も一般的なものですが、権限はシステム上のすべてのオブジェクトに対して指定できます。

一般的で直接的なアプローチを前もって計画しておけば、資源保護を簡単に、しかも効果的に管理することができます。事前の計画をしないで作成されたセキュリティーの構造は、複雑で、効果の無いものになる場合があります。『資源保護の計画』では、資源保護を計画する方法が説明されています。

システムには、直接的な資源保護の構造を設計する上で役に立つ、いくつかのツールがあります。

- **グループ・プロファイル:** 類似したユーザーを、1 つのグループ・プロファイルの下にまとめることができます。ユーザー・グループでは、オブジェクトに対して、すべてのメンバーが同じ権限を共有することができます。
- **権限リスト:** 同じようなセキュリティーを必要とするオブジェクトを、1 つのリストにまとめることができます。権限は、個々のオブジェクトにではなく、このリストに対して与えられます。
- **オブジェクト所有権:** システム上の各オブジェクトには、所有者が存在します。グループ・プロファイルまたは個々のユーザーは、オブジェクトを所有することができます。オブジェクト所有権を正しく割り当てておけば、(1) アプリケーションを管理し、(2) 情報のセキュリティーの担当を委託する際に役立ちます。
- **1 次グループ:** オブジェクトに対して 1 次グループ権限を指定することができます。システムは、オブジェクトとともに 1 次グループ権限を保管します。 1 次グループ権限を使用すると、権限の管理を単純化し、権限検査のパフォーマンスを向上させることができます。
- **ライブラリー権限:** 保護を必要とするファイルとプログラムをライブラリーに入れて、そのライブラリーに対するアクセスを制限することができます。このようにした方が、各オブジェクトに対するアクセスを個々に制限するよりも簡単な場合があります。重要なオブジェクトを保護する場合は、オブジェクトとライブラリーの両方を保護することもできます。
- **オブジェクト権限:** ライブラリーへのアクセスが明確に指定されていない場合は、ファイルなどの個々のオブジェクトに対するアクセスを制限することができます。
- **共通権限:** オブジェクトごとに、そのオブジェクトに対する他の権限をもたないすべてのシステム・ユーザーが使用できるアクセス・タイプを定義できます。共通権限は、機密性のないオブジェクトの保護には効果的な手段であり、システム・パフォーマンスにも優れています。
- **ディレクトリー権限:** ディレクトリー権限は、ライブラリー権限と同じ方法で使用することができます。1 つのディレクトリー内のオブジェクトをグループ化して、個々のオブジェクトではなくそのディレクトリーを保護することができます。
- **権限ホルダー:** オブジェクトを削除する際には、そのオブジェクトの権限情報も削除されます。権限ホルダーは、アプリケーションによって削除され、再作成されるプログラム定義ファイルの権限情報を保守します。権限ホルダーは、System/36™ からの移行を支援するために使用することができます。

セキュリティー・ツール

セキュリティー・ツールは、iSeries のセキュリティー環境を管理および監視する際に役立ちます。また、ユーザー・プロファイル・ツールは、次のような作業を行う場合に役立ちます。

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

オブジェクト・セキュリティー・ツールを変更して、機密オブジェクトに関連付けられた共通権限および私用権限を追跡することができます。これらの報告書を定期的に (たとえば、月 1 回) 印刷すると、目下の問題に対して行ったセキュリティーの成果を考察する上で便利です。報告書を実行して、前回報告書を実行したときからの変更点だけを表示させることができます。

他のツールには、次のものを監視する機能があります。

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

この部分では、システム・セキュリティーの重要性について考慮しました。続いて、このトピックが例として使用している計画方法の説明を検討することができます。

基本システム・セキュリティーを計画する方法

本トピックのこれらの計画トピックでは、外側から内側へ、および一般的な情報から固有の情報へと視点を移していきます。例えば、ユーザー・プロファイルを計画する場合であれば、まず最初に結果 (外側) を考え、その後にどのようにそれを実現するか (内側) を考えます。また、システム値とグループ・プロファイル (一般的な情報) について初めに計画し、次に個々のユーザーに関する例外 (固有の情報) を決定します。トピック『ユーザー・セキュリティーの計画』の計画ステップの手順に沿って実行してください。これらのステップでは、システムの使用を計画する方法に関する説明と、システムを保護およびカスタマイズする方法の決定が論理的な順序で扱われています。

システム・セキュリティーを計画および設計する場合は、基礎から組み立てます。まず最も基本的な形のセキュリティーから始めて、次により複雑なセキュリティーの問題に取り組みます。また、システムの物理的なセキュリティーから始めて、アプリケーションおよびシステム値の説明に進みます。そして最後に、システム上のユーザーとオブジェクトに対するセキュリティーを考慮する必要があります。

これらの計画トピック全体を通して、JKL Toys という会社のシナリオを使用して、このアプローチの例を示します。トピック『例: JKL Toy Company の紹介』で、計画トピック全体を通して使用するサンプル会社について説明します。

トピック『セキュリティー計画プロセスのステップ』で、各ステップとこれらのステップが互いにどう関連しているのかについての簡単な説明を参照してください。

例: JKL Toy Company の紹介

例を使用すると、物事の説明や理解を簡単に行うことができます。そこで、このトピックでは JKL Toy Company を例として使用します。JKL Toy Company は、小さな会社ですが、急成長を遂げている玩具 (がんぐ) 製造業者で、iSeries システム上へのセキュリティーの設定を検討しています。この会社の経営者である John Smith は、新しい iSeries システムを使用することによって、JKL Toy Company の爆発的な成長による負担を軽くしたいと考えています。

John は経理マネージャーの Sharon Jones に、システム管理者および機密保護担当者としての責任を与えています。彼女は、セキュリティーを含む導入全体が円滑に運ぶようにしなければなりません。Sharon は計画の立案が重要であると考えています。現在のところ、会社の規模は小さく、従業員のほとんどが大抵の情報にアクセスすることができます。しかし Sharon は、会社が大きくなるにつれてこの状況が変化することを認識しています。そのため、最初から物事を適切に行いたいと思っています。

まず始めに、JKL Toy Company がシステム上で実行する計画を立てたアプリケーションは、顧客注文、在庫管理、契約と価格設定、および売掛管理です。計画のトピックを一読すると、JKL Toy Company がセキュリティーを処理する方法について、より多くの事柄を知ることができます。

『計画プロセスのステップ』では、システム・セキュリティーの計画に必要な各ステップについて説明しています。

セキュリティー計画プロセスのステップ

次の表は、計画プロセスに含まれる各ステップについて説明し、各ステップがプロセス内の他のステップとどのように関連しているかを示しています。

表 2. セキュリティー計画プロセスのステップ

ステップ	このステップの内容	他のステップとの関連
物理的セキュリティーの計画	システム装置、装置、およびバックアップ媒体の保護を計画する方法について説明します。	このトピックに含まれる情報のほとんどは、プロセス内の他のステップとは関連していません。物理的セキュリティーの計画に関する情報をシステムに入力することはありません。とはいえ、システム値と資源保護を計画する際には、このステップに含まれる情報がいくつか必要になります。
アプリケーションの計画	ご使用になるすべてのアプリケーションの目的、メイン・メニュー、およびライブラリーについて説明します。	このステップの情報は、計画プロセスの残りのステップ、および他のセキュリティー上の決定の基礎になります。この情報をシステムに入力することはありません。
全体的なアプローチの計画	セキュリティーに対する全体的なアプローチを決定します。決定したアプローチに合ったシステム値を選択します。	全体的なアプローチを決定する上で、アプリケーションの計画に関する情報を参照すると便利です。ここで選択するシステム値は、ユーザーおよびグループ・プロファイルの計画方法に影響します。
ユーザー・グループの計画	ユーザーをグループに分ける方法を決定します。どのような特性に基づいてグループを作成するかを決定し、各グループをシステムに定義する方法を決定します。	システム上でグループを決定する際は、アプリケーション記述を使用します。ここで定義するユーザー・グループは、システム上で個々のユーザーを計画する方法に影響します。
個々のユーザー・プロファイルの計画	各システム・ユーザーをグループに割り当てます。各ユーザーを定義し、他のグループと区別するための特性を含めます。たとえば、ユーザーがアプリケーションやライブラリーにアクセスする際に、他のグループとは異なったアクセスを必要とするようにします。	個々のユーザーを定義する際は、アプリケーションの計画の情報、およびユーザー・グループの計画の情報を使用すると便利です。
資源保護の計画	システム上のすべてのユーザーが使用できるアプリケーションを決定します。特定のアプリケーションについて制限が必要な場合は、使用を許可するユーザーやグループを決定します。	資源保護を計画する際は、アプリケーションの計画の情報、およびグループ・プロファイルの計画の情報を使用すると便利です。
アプリケーションの導入の計画	ご使用になるアプリケーション・ライブラリーに対して、所有権と共通権限を確立する方法を決定します。	アプリケーションの導入を計画する場合は、資源保護の計画の情報を使用すると便利です。

セキュリティーの計画プロセスは、ユーザー・セキュリティーの計画から開始することをお勧めします。

ユーザー・セキュリティーの計画

ユーザー・セキュリティーの計画には、セキュリティーがシステム上のユーザーに影響を与えるすべての分野の計画が含まれます。次の分野についての記述が必要です。

物理的セキュリティー

物理的セキュリティーには、iSeries システムを、事故による (または意図的な) 損傷および盗難から保護することが含まれます。加えて、これにはすべてのワークステーション、印刷装置、および記憶媒体が含まれます。『物理的セキュリティーの計画』には、物理的セキュリティーとリスクに関する詳細、および IBM の推奨事項が含まれています。

アプリケーション・セキュリティー

アプリケーション・セキュリティーでは、システムに保管するアプリケーション、およびそれらへのアクセスを複数のユーザーに同時に許可している時にアプリケーションを保護する方法を扱います。『アプリケーションのセキュリティーの計画』では、アプリケーションとその命名規則について詳細に説明しています。

全体的なセキュリティー戦略

全体的なセキュリティーの計画には、ビジネスにおける現在の状況と将来の計画の両方を考慮に入れたセキュリティー計画の開発が含まれます。『全体的なセキュリティー戦略の計画』では、セキュリティー方針、セキュリティー・レベル、パスワードの考慮事項、およびシステム値について詳細に説明しています。

ユーザー・グループのセキュリティー

ユーザー・グループは、同じアプリケーションを同じ方法で使用する必要があるユーザーのグループです。ユーザー・グループのセキュリティーの計画には、システムの使用を計画するワークグループと、それらのワークグループに必要なアプリケーションの決定が含まれます。『ユーザー・グループの計画』では、ユーザー・グループの識別、グループ・プロファイルの計画、システム値の選択、およびユーザー環境の決定について、詳細に説明しています。

個々のユーザーのセキュリティー

必要なユーザー・グループが決定したら、必要な個々のユーザー・プロファイルを計画することができます。『個々のユーザー・プロファイルの計画』では、システム上のユーザーの命名、個々のユーザーが持つ責任の決定、およびシステム値の選択について詳細に説明しています。

これらの計画のトピックには、随所に計画用紙へのリンクがあり、これらを使用して計画上の決定を記録することができます。

物理的セキュリティーの計画

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

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

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

システムの物理的セキュリティーに関する決定は、物理的セキュリティー計画用紙を使用して記録することができます。物理的セキュリティーのすべての局面を確認するには、以下のトピックを検討してください。

- 『システム装置の物理的セキュリティー』では、システムそのもののセキュリティーについて詳細に説明しています。
- 『システム文書および記憶媒体の物理的セキュリティー』では、システム文書と記憶媒体のセキュリティーについて扱っています。
- 『ワークステーションの物理的セキュリティーの計画』では、ワークステーションを保護する方法について説明しています。
- 『印刷装置および印刷装置出力の物理的セキュリティーの計画』では、印刷装置とその出力の物理的な保護について詳細に説明しています。
- 『セキュリティーの方針の計画』では、ユーザー・ガイドラインや、セキュリティー上の方針を準備する方法について説明しています。

各システム装置には、システムを保守するための、または、システムの電源をオン / オフにするなどの特別なシステム操作を行うための制御パネルがあります。これらのシステム操作が許可なく行われることを防ぐため、各システム装置には、キーロック・スイッチか電子キースティックがあります。これらの機能でも、システム装置をある程度保護することはできますが、キーロック・スイッチや電子キースティックは、適切な物理的セキュリティーの代わりになるものではありません。

システム装置の物理的セキュリティー

iSeries には、特別な環境制御の施されたコンピューター・ルームは必要ありません。iSeries 400 のシステム装置は、大勢の人々が出入りするオフィス・エリアの中に置かれることがよくあります。お客様には、iSeries の、小型で保守が簡単であるという特性にご好評いただいております。しかし、これらの特性にはセキュリティー上のリスクも伴います。たとえば、簡単にシステム装置を盗んだり、装置から高価なコンポーネントを取り外したりできてしまう、というリスクがあります。

そのため、システム装置が確実に安全な場所に置かれるように手段を講じる必要があります。最良の手段は、専用の部屋を設けてその部屋をロックしておくことです。最低でも、通常のビジネス時間外にはロックできる場所に、システム装置を置いてください。

システム装置へのリスク

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

システム操作による意図せぬ停止

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

専用保守ツール (DST) 機能を使用したセキュリティーの回避

セキュリティーは、システムが実行する保守機能を制御しません。これは、保守機能を実行する必要がある際に、システム・ソフトウェアを正常に操作できない可能性があるためです。システムに関する知識があり DST ユーザー ID とパスワードを知っている、または推測できる人物であれ

ば、使用中のシステムに深刻な損傷を与えることが可能です。保守ツールの詳細については、Information Center の『保守ツール』のトピックを参照してください。

推奨事項

- 理想的なのは、システム装置をロックされた部屋に置くことです。これが不可能な場合は、装置を外部の人間が出入りできない場所に置いてください。加えて、責任のある従業員が監視できる位置に装置を置いてください。次の物理的なセキュリティー機能は、意図しない、または意図的な損傷からシステムを保護する上で役立ちます。
- 電子キースティックまたはキーロックを使用する。
  - キーを使用せずにシステムを開始できるようにするには、操作モードを Normal に設定します。
  - 自動電源オン/オフ機能を使用して、システムを開始および停止するには、操作モードを Auto に設定します。
  - キーを外して安全な場所に保管します。
- システムを導入した後、および保守担当者が保守ツール (DST) を使用した後に、ただちに保守ツール (DST) のユーザー ID とパスワードを変更する。この作業についての詳細は、Information Center の『保守ツール』のトピックに記載されています。

システム文書および記憶媒体の物理的セキュリティーを計画する前に、装置のセキュリティーについて JKL Toy Company の例を参照することができます。

例: JKL Toy Company の物理的セキュリティー計画用紙 -- システム装置の部分: 下の表は、Sharon Jones が自分のシステムに使用した物理的セキュリティー計画用紙のシステム装置に関する部分の例です。

表 3. JKL Toy Company の物理的セキュリティー計画用紙: システム装置の例

物理的セキュリティー計画用紙	
作成者: Sharon Jones	日付: 9/2/99
システム装置:	
システム装置を保護するためにとったセキュリティー手段 (ロックした部屋の使用など):	システム装置は経理のエリアに置く。日中は、経理の担当者が常にこのエリアにおり、システム装置を監視することができる。経理の担当者は、小額の現金と重要な記録を管理する責任も担っている。この部屋は、通常のビジネス時間外にはロックされる。
通常のキーロックの設定位置:	Normal
キーの保管場所:	Sharon のオフィス内にある小型金庫。
システム装置に関連したその他の注記:	システム装置のある場所には容易に出入りすることができる。経理のエリアにいる人々については、システム装置を不正操作することはないと確信できる。

システム装置の物理的セキュリティーの計画が完了したら、システム文書および記憶媒体に対する物理的セキュリティーを計画することができます。

システム文書および記憶媒体の物理的セキュリティー

他の分野の物理的セキュリティーの計画には、重要なシステム文書と記憶媒体の保管が関係しています。システム文書には、IBM がシステムとともにお送りした情報、パスワードの情報、お客様の計画用紙、およびシステムが生成したすべての報告書が含まれています。

ご使用のシステムに応じて、バックアップ媒体にはテープ、CD-ROM、ディスケット、または DVD 記憶装置が含まれます。システム文書とバックアップ媒体はいずれも、企業の場所以外に、他の離れた場所にも保管しておく必要があります。万一災害が発生した場合には、システムを回復させるためにこの情報が必要になります。システム文書と記憶媒体を保管する方法として、次に示されている方法を使用することもできます。保管の方法を決定したら、物理的セキュリティー計画用紙の、「バックアップ媒体および文書」の部分に選択事項を記録してください。

システム文書を安全に保管する

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

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

記憶媒体を安全に保管する

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

リスク

- バックアップ媒体の損傷: 災害によって、または意図的にバックアップ媒体が破壊された場合、印刷された報告書から情報を復元する以外、システム上にあった情報を回復することはできません。
- バックアップ媒体やパスワードの盗難: バックアップ媒体に機密のビジネス情報が保管されている場合があります。そのことを知っている人物がいると、この情報を他のコンピューターで復元し、印刷したり、処理したりできる恐れがあります。

推奨事項

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

ワークステーションの物理的セキュリティーを計画する前に、システム文書の保管について、JKL Toy Company の例を検討することができます。

例: JKL Toy Company の物理的セキュリティー計画用紙 -- バックアップ媒体および文書の部分: JKL Toy Company の Sharon Jones は、下の表のように、物理的セキュリティー計画用紙の「バックアップ媒体および文書」の部分を完成しました。

表 4. JKL Toy Company の物理的セキュリティー計画用紙: バックアップ媒体および文書の例

物理的セキュリティー計画用紙	
作成者: Sharon Jones	日付: 9/2/99
バックアップ媒体および文書:	
バックアップ・テープのビジネスの場所での保管場所:	大型耐火金庫の中。
バックアップ・テープの別の保管場所:	会社の経理係のオフィスにある耐火金庫の中。

表 4. JKL Toy Company の物理的セキュリティー計画用紙: バックアップ媒体および文書の例 (続き)

機密保護担当者、保守、および DST パスワードの保管場所:	John Smith のオフィスにある二重金庫の中。
重要なシステム文書 (シリアル番号や構成など) の保管場所:	オフィスとは離れた場所にある大型金庫の中。および経理のオフィス。

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

ワークステーションの物理的セキュリティーの計画

ほとんどの場合は、すべてのユーザーが、任意の使用可能なワークステーションにサインオンして、許可されたすべての機能を実行できるようにしたいとお考えになるでしょう。しかし、あるワークステーションを誰でも使用できるようにしたり、逆に何かの専用に使用する場合は、特別な予防策を講じたいと思われるかもしれません。たとえば、パーソナル・コンピューターとキー・ストロークを備えた表示装置には、特別な考慮事項が必要です。次に示すような方法を参考にして、物理的セキュリティー計画用紙の第 2 部 (ワークステーションおよび印刷装置の物理的セキュリティー) を作成することができます。

ワークステーションに関連したリスク

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

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

表示装置のプレーバック機能や PC サインオン・プログラムを使用してセキュリティーが回避される
多くの表示装置には記録およびプレーバックの機能があります。これは、ユーザーが頻繁に使用するキー・ストロークを保管し、1 つのキーを押すだけでそれが繰り返されるようにする機能です。また、iSeries システムで、パーソナル・コンピューターをワークステーションとして使用する場合は、プログラムを作成して、サインオン・プロセスが自動的に行われるようにすることができます。ユーザーはサインオン・プロセスを頻繁に行うため、サインオンのたびに入力を行うより、ユーザー ID とパスワードを保管しておくことを考えます。

推奨事項

ワークステーションに対して物理的なセキュリティーを設定する際は、次の推奨事項を考慮してください。

- 可能であれば、極端に誰でも出入りできる場所や、極端に密閉された場所には、ワークステーションを置かないでください。
- システム・ユーザーには、ワークステーションを離れる際にサインオフすることの重要性を強調してください。セキュリティーの方針の中に、サインオフの手続きを含めるようにお勧めします。
- 表示装置や PC プログラムにパスワードを記録することは、システム・セキュリティーに違反することを強調してください。セキュリティーの方針の中に、パスワードの記録に関する指示を含めるようお勧めします。
- 非活動タイマー・システム値 (QINACTITV および QINACTMSGQ) を使用して、ユーザーがシステムをサインオフせずに、共用の場所にあるワークステーションを離れることがないよう、手段を講じてください。

- 共用のワークステーションに対して、制限された権限を持つユーザーのみを認可することによって、それらのワークステーションでユーザーが実行できる機能を制限してください。
- 専用のワークステーションに対して、セキュリティーや保守の権限を持つユーザーがサインオンすることがないようにしてください。 QLMTSECOFR システム値を使用して、これらの権限でユーザーがサインオンできる場所を制御してください。
- ユーザーが複数のワークステーションに同時にサインオンしないように、制限してください。装置のセッションを制限するシステム値 (QLMTDEVSSN) を使用して、ユーザーがサインオンする場所を制御することができます。

これらの推奨事項を実行するには、『サインオンに影響するシステム値の選択』および『ワークステーションの資源保護の計画』で詳細を参照してください。

物理的セキュリティー計画用紙では、物理的な場所が原因でリスクが生じる可能性のあるワークステーションを識別する必要があります。JKL Toy Company の例では、Sharon Jones がワークステーションに対して計画した物理的セキュリティーを検討することができます。

ワークステーションのセキュリティーの計画が完了したら、印刷装置および印刷装置出力の物理的セキュリティーを計画することができます。

印刷装置および印刷装置出力の物理的セキュリティーの計画

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

印刷装置および印刷装置出力に関連したリスク

ビジネス環境に対して、次のようなリスクが考えられます。ここに挙げられているのは、印刷装置および印刷装置出力に関連する、最も一般的なセキュリティーのリスクです。しかし、ご使用になっている特定のビジネス環境に生じる可能性のある他のリスクについても調査するようお勧めします。

- 印刷装置が共用の場所に置かれていると、許可されていない人々が機密情報を見る恐れがあります。
- 印刷装置出力を机の上に放置しておくと、情報が漏れる恐れがあります。
- システムに、印刷装置が 1 つか 2 つしかない場合は、会社の従業員が、給料支払い小切手などの、価値のある、または機密の情報を見る場合があります。

推奨事項

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

- 機密の印刷装置出力を保護することの重要性をシステム・ユーザーに強調してください。セキュリティーの方針の中に、印刷装置に関連した物理的セキュリティーの決定を含めてください。
- 印刷装置を共用の場所に置くことは避けてください。
- 機密性の高い出力の印刷についてはスケジュールを立て、印刷が行われる間、許可された人が印刷装置の所にいるようにしてください。

『印刷装置および印刷装置出力のセキュリティーの計画』には、機密の印刷装置出力の扱い方について提案が示されています。

セキュリティーの方針の計画を開始する前に、JKL Toy Company による、印刷装置に対するセキュリティーの計画の例を検討することができます。

例: JKL Toy Company の物理的セキュリティー計画用紙 -- ワークステーションおよび印刷装置の部分: 下の表は、Sharon Jones が JKL Toy Company に使用した、物理的セキュリティー計画用紙の第 2 部の例です。

表 5. JKL Toy Company の物理的セキュリティー計画用紙: ワークステーションおよび印刷装置の例

物理的セキュリティー計画用紙			2 / 2
ワークステーションおよび印刷装置の物理的セキュリティー			
ワークステーション名 または印刷装置名	置かれている場所または説明	セキュリティーのエクスポージャー	実行する保護手段
DSP06	発送所	極端に誰でも出入りできる場所にある	自動サインオフ。ワークステーションで完了できる機能のみに制限する。
DSP09	顧客サービス・デスク	極端に誰でも出入りできる場所にある	自動サインオフ。ワークステーションで完了できる機能のみに制限する。
RMT12	離れた場所にある営業所	密閉しすぎている	機密保護担当者がサインオンできないようにする。
PRT02	経理部、システム装置の近く	価格表などの機密情報が目の届く所にある。	誰かが印刷装置出力を監視するようにする。

物理的セキュリティー計画用紙が完成したら、『セキュリティーの方針の計画』に進んでください。

セキュリティーの方針の計画

すべての従業員にセキュリティーの指針を配信すると、物理的な、およびシステムのセキュリティーに関するセキュリティーの方針を強調する上で役に立ちます。システムに後から追加される新しいユーザーにも、同じ指針を送ることができます。

これらの指針の中には、ワークステーションのサインオフおよび共有しないパスワードなど、システム・セキュリティーを保護する方法に関するいくつかの一般的な指示も含める必要があります。さらに、セキュリティーに関してお客様が固有に決定された内容も、この指針に含めてください。

この計画の情報を読む際は、お客様のセキュリティーの指針に含める内容を書き留めてください。また、お客様のセキュリティーの方針についても、メモをお取りになるようお勧めします。

たとえば、JKL Toy Company の Sharon Jones は、彼女がシステムに対して物理的セキュリティーを計画した際、セキュリティーの指針について次のようなメモを作成しました。

```
Make sure to emphasize signing off for loading dock, customer service,
and remote sales office. Accounting people will watch system unit.
```

物理的セキュリティー計画用紙が完成したら、アプリケーションのセキュリティーを計画できます。

アプリケーションのセキュリティーの計画

アプリケーションに対して適切なセキュリティーを計画するには、次の情報が必要です。

- どのような情報をシステムに保管する計画を立てているか。
- その情報にアクセスする必要があるのは誰か。

- どのような種類のアクセスが必要なのか。その情報を変更する必要があるのか、それとも表示するだけなのか。

これらのアプリケーションの計画のトピックを進むにあたって、システムに保管しようとする情報について、最初の質問に対する答えが必要です。続くトピックの中では、誰がその情報を必要としており、どのようにその情報にアクセスするのかを決定します。アプリケーションの計画に関する情報をシステムに入力することはありません。しかし、これらの情報はユーザーおよび資源のセキュリティーを設定する際に必要になります。

アプリケーションとは

アプリケーションのセキュリティーの最初の計画のステップでは、システムで実行しようとしているアプリケーションについて記述する必要があります。アプリケーションとは、論理的に同じように分類される機能のグループのことです。たとえば、JKL Toy Company の例で考えると、注文の入力、注文の出荷、および送り状の印刷は、すべて注文処理というアプリケーションに属しています。

通常、iSeries では、次のような 2 つの異なったタイプのアプリケーションが実行されます。

- **ビジネス・アプリケーション**: 注文処理や在庫管理など、特定のビジネス機能を実行するために、購入または開発されるアプリケーション。
- **特殊アプリケーション**: ビジネスのプロセスに固有でないさまざまな活動を実行するために、会社全体で使用されるアプリケーション。

どのような用紙が必要か

アプリケーションのセキュリティーを計画する際、次のような用紙を使用することができます。

- アプリケーション記述用紙
- ライブラリー記述用紙
- 命名規則用紙

これらの用紙を印刷するには、リンクをクリックし、ブラウザーで適当なフレームを選択して「**印刷**」アイコンをクリックします。

以下の情報を読んで、これらの計画用紙を完成させる際の参考にすることができます。

- アプリケーションの記述
- 命名規則の記述
- ライブラリー情報の記述
- アプリケーション図の描画

アプリケーションの記述

ここで、各ビジネス・アプリケーションについて、いくつかの一般的な情報を集める必要があります。下に説明されているようにして、アプリケーション記述用紙の適当なフィールドに、ご使用になるアプリケーションに関する情報を加えてください。この情報は、後でユーザー・グループとアプリケーションのセキュリティーを計画する際に役立ちます。

アプリケーション名および省略形
: アプリケーションに短い名前と省略形を割り当て、用紙上での省略表現として、およびアプリケーションが使用する命名オブジェクトとして使用することができます。

記述情報
: アプリケーションが行う業務について簡単に記述します。

1 次メニューおよびライブラリー

どのメニューがアプリケーションにアクセスするための 1 次メニューかを識別します。また、そのメニューが含まれているライブラリーを識別します。通常、特定のアプリケーションの機能を使用するための他のメニューは、1 次メニューから導かれます。ユーザーがシステムにサインオンした直後に、メインで使用するアプリケーションの 1 次メニューが表示されるようにすると、ユーザーにとって便利です。

初期プログラムおよびライブラリー

アプリケーションは、ユーザーのバックグラウンド情報を設定したり、セキュリティーのチェックを行ったりする初期プログラムを起動する場合があります。アプリケーションに初期プログラムや設定プログラムがある場合は、用紙にリストしてください。

アプリケーション・ライブラリー

通常、各アプリケーションには、そのファイルを保管するメインのライブラリーがあります。プログラム・ライブラリーや他のアプリケーションのライブラリーを含め、アプリケーションが使用するライブラリーをすべてここに含めてください。たとえば、JKL Toy Company の顧客注文アプリケーションは、在庫のライブラリーを使用して、品目の残量と記述を確認します。

各ライブラリーにアクセスする必要があるユーザーを判別するには、ライブラリーとアプリケーションとの間の関係を使用します。

アプリケーションに関する情報の検索

アプリケーションについてまだ分からない情報がある場合は、プログラマーかアプリケーションの提供者への相談が必要となる場合があります。

システム上で実行するアプリケーションについて、この情報にアクセスできない場合は、次の方法を使用して、自分で情報を収集することができます。

- アプリケーションのユーザーに尋ねれば、おそらく 1 次メニューとライブラリーの名前を知ることができます。あるいは、自分でシステムにサインオンして確認することもできます。
- ユーザーがサインオンした後に、すぐそのアプリケーションが表示されるのであれば、そのユーザー・プロファイルの「**初期プログラム**」のフィールドを見てください。このフィールドには、アプリケーションの初期プログラムが含まれています。 DSPUSRPRF コマンドを使用して、初期プログラムを表示することができます。
- システム上のすべてのライブラリーの名前と記述をリストすることができます。 DSPOBJD *ALL *LIB を使用してください。システム上のすべてのライブラリーが表示されます。
- ユーザーがアプリケーションを実行している間、活動ジョブを監視することができます。対話式ジョブに関する詳細な情報を表示するには、中級操作援助レベルで活動ジョブの処理 (WRKACTJOB) コマンドを使用してください。ジョブを表示してライブラリー・リストとそのオブジェクト・ロックを調べ、使用されているライブラリーを見つけてください。
- ユーザー・ジョブの処理 (WRKUSRJOB) コマンドを使用して、アプリケーション内のバッチ・ジョブを表示することができます。

アプリケーションのセキュリティーを計画するために必要なすべての情報を確実に収集するには、処理を続ける前に以下の作業を完了する必要があります。

- 各ビジネス・アプリケーションについて、アプリケーション記述用紙を完成させる。セキュリティー要件に関する部分を除いて、用紙のすべての項目を記入してください。セキュリティー要件の部分は、アプリケーションの資源保護を計画する際に使用します。この点については、『資源保護の計画』で扱います。

- 該当する場合は、各特殊アプリケーションについて、アプリケーション記述を作成する。用紙を使用すると、アプリケーションへのアクセスの提供方法を判別する際に便利です。

注: IBM Query for iSeries など、IBM が提供している特殊アプリケーションのためのアプリケーション記述用紙の作成はオプションです。これらのアプリケーションが使用する、ライブラリーへのアクセスについては、特別な計画は必要ありません。ただし、これらのアプリケーションについて情報を収集し、用紙を作成すると役立つ場合があります。

命名規則の記述に移る前に、JKL Toy Company が作成したアプリケーション記述用紙の例を見ることができます。

例: JKL Toy Company のアプリケーション記述用紙: Sharon Jones はアプリケーション記述用紙の中で、すべての会社のアプリケーションを省略形でリストしています。また、これらのアプリケーションを使用してユーザーが作業する方法についても、簡単に説明しています。

顧客注文 (CO)
注文の入力、追跡、および出荷。送り状の印刷。

在庫管理 (IC)
完成した製品と材料の両方に関する在庫レベルの管理。すべての在庫変化の処理。

契約と価格設定 (CP)
特殊な価格設定の管理、および顧客との契約の管理。

売掛管理 (AR)
現在の残高の追跡。月ごとの状態の印刷。

下の表には、Sharon Jones が顧客注文について作成した記述が含まれています。彼女は用紙を系統的に作成しており、まず 1 つのアプリケーションについて記述し、次いで残りのアプリケーションについて記述しています。

表 6. JKL Toy Company のアプリケーション記述用紙: 例

アプリケーション記述用紙	
作成者: Sharon Jones	日付: 9/3/99
アプリケーション名: 顧客注文	省略形: CO
アプリケーションについての簡単な説明:	顧客注文の入力、出荷までの注文の追跡、注文の出荷、および送り状と出荷用紙の印刷。
1 次メニュー名: COMAIN	ライブラリー: COPGMLIB
初期プログラム名: NA	ライブラリー: NA
アプリケーションが使用するライブラリーのリスト (ファイル用とプログラム用の両方): • CUSTLIB • ITEMLIB • CONTRACTS • COPGMLIB	
アプリケーションに対するセキュリティーの目的 (機密情報を含んでいるかどうかなど):	

顧客注文アプリケーションに加えて、Sharon Jones は、JKL Toy Company システムの次のアプリケーションについても、アプリケーション記述用紙を作成しました。

- 在庫管理

- 契約と価格設定
- 売掛管理

次に、システム上のオブジェクトに対する命名規則の記述を行うことができます。

命名規則の記述

システムがオブジェクトに名前を付ける方法が分かる場合は、セキュリティーと問題の解決を計画および監視し、バックアップと回復を計画することができます。ほとんどのアプリケーションには、ライブラリー、ファイル、およびプログラムなどのオブジェクトに名前を割り当てる際の規則があります。ソースの異なるアプリケーションには、おそらく、それぞれ固有の命名システムがあると考えられます。

アプリケーションとオブジェクトの命名規則はすべて、命名規則用紙に記録するようにしてください。命名規則用紙では、ライブラリーやファイルに名前を付ける際にアプリケーションが使用する規則をリストしてください。プログラムやメニューなどの他の命名規則においては、ブランク行を使用することもできます。ソースの異なるアプリケーションには、おそらく、それぞれ固有の命名規則があると考えられます。各アプリケーションの命名規則を記述してください。複数の命名規則用紙を作成しなければならない場合もあります。

ライブラリー情報の記述に進む前に、JKL Toy Company システム上のオブジェクトに対して Sharon がどのように命名規則を使用しているか、例を参照することができます。

例: JKL Toy Company の命名規則用紙: 下の表は、ライブラリーとファイルに対する命名規則のみを示しています。ご使用のシステムでは、他のタイプのオブジェクトに対する命名規則についても記述する必要があります。命名規則用紙には、いくつかの一般的なオブジェクトが含まれていますが、オブジェクトによっては別の用紙を作成しなければならない場合があります。

表 7. JKL Toy Company の命名規則用紙: 例

命名規則用紙	
作成者: Sharon Jones	日付: 9/3/99
オブジェクトのタイプ	**命名規則**
ライブラリー	ファイルを含むライブラリーには、CONTRACTS や ITEMLIB のように、意味のある名前を使用する。プログラムを含むライブラリーには、アプリケーションの省略名の後ろに PGMLIB を付けた形式を使用する (例、ICPGMLIB)。
ファイル	主要なファイルには意味のある名前を使用する。たとえば、顧客マスター・ファイルなら CUSTMAST、品目マスター・ファイルなら ITEMMAST のようにする。他のアプリケーション・ファイルには (プログラマーが理解するためにのみ使用される)、アプリケーションの省略名の後ろに FILE を付け、最後に番号を続ける (例、ICFILE14)。

命名規則用紙が完成したら、ライブラリー情報の記述を開始することができます。

ライブラリー情報の記述

命名規則の記述が完了したら、次にシステム上のライブラリーについて記述しなければなりません。ライブラリーは、システム上のオブジェクトを識別および編成します。類似したファイルを 1 つのライブラリーにまとめると、ユーザーは重要なアプリケーションとファイルにアクセスしやすくなります。また、ユーザーの権限をカスタマイズして、ユーザーがアクセスできる情報をライブラリー単位で制限することもできます。各アプリケーションが使用する、システム上のすべてのライブラリーについて記述してください。複数のライブラリー記述用紙を作成しなければならない場合もあります。

注: ライブラリーに関する記述情報のみを記入してください。ライブラリーについての資源保護を計画する場合は、ライブラリー記述用紙のその他の項目についても記述を行います。後で、ライブラリーに対する権限についての情報を加える必要があります。ライブラリー記述用紙の残りの部分を完成する際の詳細については、『アプリケーション・ライブラリーのセキュリティーの計画』を参照してください。

作業を続ける前に、必ず以下の作業を完了してください。

- 命名規則用紙のライブラリーとファイルに関する部分を記入する。
- 各アプリケーション・ライブラリーについて、ライブラリー記述用紙の記述情報を記入する。

アプリケーション図の描画に進む前に、例で、JKL Toy Company の Sharon Jones が作成したライブラリー記述を見ることができます。

例: JKL Toy Company のライブラリー記述用紙: 下の 2 つの表は、JKL Toy Company の顧客注文アプリケーションが使用する 2 つのライブラリーについて記述したものです。 1 つめの表はファイルを含むライブラリーについて、2 つめの表はプログラムを含むライブラリーについて記述しています。

表 8. JKL Toy Company のライブラリー記述用紙: ファイルを含むライブラリーの例

ライブラリー記述用紙	
作成者: Sharon Jones	日付: 9/3/99
ライブラリー名: CUSTLIB	記述名 (テキスト): 顧客レコード・ライブラリー
このライブラリーの機能についての簡単な説明:	注文と売掛管理を含む、すべての顧客ファイルを保持する。

表 9. JKL Toy Company のライブラリー記述用紙: プログラムを含むライブラリーの例

ライブラリー記述用紙	
作成者: Sharon Jones	日付: 9/3/99
ライブラリー名: COPGMLIB	記述名 (テキスト): 顧客注文プログラム・ライブラリー
このライブラリーの機能についての簡単な説明:	顧客注文アプリケーションのすべてのプログラムを保持する

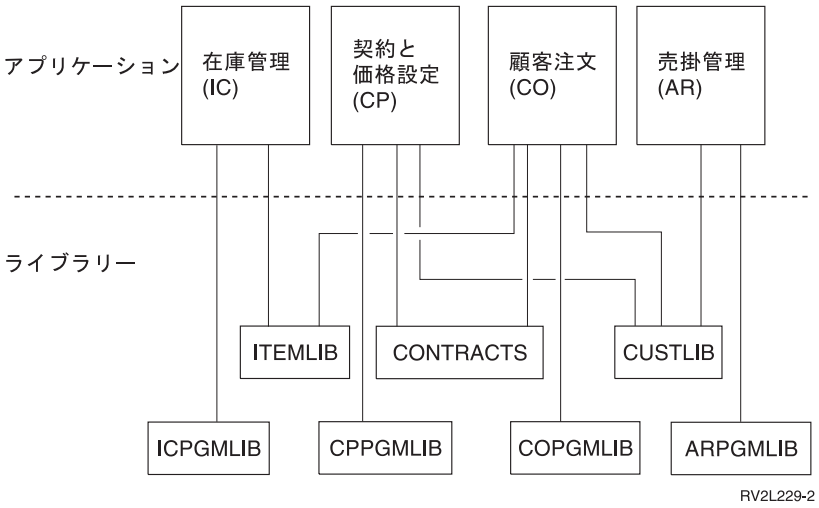
ライブラリーについての記述が完了したら、ご使用のシステムに関するアプリケーション図の描画を行う必要があります。

アプリケーション図の描画

アプリケーション記述用紙およびライブラリー記述用紙を作成する際に、アプリケーションとライブラリーの関係を示す図を描くと便利です。図は、ユーザー・グループを計画する場合にも、資源保護を計画する場合にも便利です。

下の図は、Sharon Jones が描いた、JKL Toy Company のアプリケーションとライブラリーの図です。

JKL Toy Company のアプリケーションおよびライブラリーの図



アプリケーションとライブラリーについての情報を収集することは、必要な多くのセキュリティー上の決定を下す上で役立ちます。システムとアプリケーションに関する知識を深める機会として、この情報に精通してください。

必要としているアプリケーションの情報を確実に収集するには、次のようにします。
- システム上の各ビジネス・アプリケーションについて、アプリケーション記述用紙を完成させる。
- 任意で、システム上の各特殊アプリケーションについて、アプリケーション記述用紙を作成する。
- 命名規則用紙のライブラリーとファイルに関連する部分を完成させる。
- 各アプリケーション・ライブラリーについて、ライブラリー記述用紙を作成する。
- アプリケーションとライブラリーの間の関係を図に描画する。

これらの用紙が完成したら、全体的なセキュリティー戦略の計画を開始することができます。

全体的なセキュリティー戦略の計画

アプリケーションのセキュリティーの計画が完了した後で、全体的なセキュリティー戦略を開始することができます。まず、システムでのセキュリティーに対する、全体的なアプローチを決定しなければなりません。これらの決定を下す際は、現在会社に必要なものと、将来必要になるものとのバランスを取ってください。

ここで決定される内容は、セキュリティーの方針と目標を決定するための計画のプロセス全体で役立ちます。また、この情報は、システム上のすべてのユーザーに影響を与える、基本的なシステム値を選択する際にも役立ちます。

どのような用紙が必要か

アプリケーションの計画を完了するためには、システム値選択用紙を使用します。

システム値に関連した決定を下すために以下のトピックを検討する際は、完成させた物理的セキュリティー計画用紙とアプリケーション記述用紙を使用してください。

セキュリティーの戦略を計画する際は、次のトピックを検討してください。
- セキュリティーの方針の作成
- セキュリティー・レベルの選択

- サインオンに影響するシステム値の選択
- パスワードに影響するシステム値の選択
- システムをカスタマイズするためのシステム値の使用

セキュリティー方針の作成

計画を開始する前に、システムのセキュリティーに関する会社の方針を示すステートメントを作成します。このステートメントは、お客様とお客様の会社の最高責任者との間の協定になります。このステートメントは、重要な問題を決定し、判断する際に役立ちます。セキュリティー方針は、全体的なアプローチと、保護を必要とする情報資産を定めるものでなければなりません。

すべてのシステムがセキュリティーを保持しなければなりません。次のいずれかのアプローチを、お客様のセキュリティーに採用することができます。

- **厳重**: 必須のセキュリティー機構ともいわれます。厳重なセキュリティー環境では、ジョブの実行に必要な情報と機能に対してのみ、アクセスすることが許されます。他の情報や機能は除外されます。多くの監査役は、厳重なアプローチを推奨しています。
- **平均**: 平均的なセキュリティーのアプローチでは、割り当てられている権限に基づいて、オブジェクトに対するユーザーのアクセスを許可します。
- **寛容**: 寛容なセキュリティー環境では、許可を持つユーザーに、システム上のほとんどのオブジェクトに対するアクセスを許可します。特定の重要な資源や機密の資源に対するアクセスを制限します。 1 つの部署の中や小規模な会社のシステムでは、通常、寛容なセキュリティーを使用します。

全体的なアプローチは、特定のセキュリティーの必要について決定する際に役立ちます。システムに対するセキュリティーのアプローチは、会社全体として、情報へのアクセスに対する考え方と一致していなければなりません。どのアプローチを使用したらよいか分からない場合は、次のようにしてみてください。

- 完成させたアプリケーション記述用紙を使用して、それらのアプリケーションにアクセスすべきユーザーと、アクセスすべきでないユーザーを判別する。
- 会社で使用するテクノロジーについて吟味する。たとえば、システムまたはネットワークをインターネットに接続する計画がある場合は、外部のインターネット・ユーザーからシステムを保護するために、より制限の多いセキュリティー環境が必要になります。
- セキュリティーの要件をより正しく判別するため、組織内の他のメンバー (セキュリティーの監査役など) に相談する。

方針は、いつでも変更できることを覚えておいてください。ほとんどの会社では、会社が成長するにつれて、より厳重なセキュリティーが必要であることに気付きます。この情報は、後で多くの変更を加えたり、すべてのアプリケーションをテストし直したりすることなく、より多くのセキュリティーを追加できるセキュリティー機構を設定する際に役立ちます。

保護する対象

セキュリティー方針の中でセキュリティーに対する全体的なアプローチを開始することに加えて、お客様の会社にとって重要な情報資産を識別する必要があります。セキュリティー・システムは、この情報を保護するように設計する必要があります。次のいくつかの要件を使用して、重要な資産を判別することができます。

- **機密性**: 社内の人間が一般的に使用できない情報。機密情報の例として、給与計算などが挙げられます。
- **競合性**: 競争において利益をもたらす情報。製品の仕様書や規格などがあります。
- **作業**: 通常のビジネスの作業に不可欠なコンピューター上の情報。顧客レコードや在庫の残量などがあります。

機密保護担当者の Sharon Jones と会社の経営者である John Smith は、協力してセキュリティー方針を示すステートメントを作成しました。 John Smith は、次のメモを使用して、JKL Toy Company のセキュリティー方針の草案を作成しました。セキュリティーの計画および設定が完了した後、JKL Toy Company が全社員に対して送ったセキュリティー方針を検討することができます。これらの計画のトピックに従って作業する場合は、セキュリティー方針に追加するもののメモを作成するようにしてください。

表 10. JKL Toy Company のセキュリティー方針: 例

全体的なアプローチ

寛容: ほとんどのユーザーがほとんどの情報にアクセスできる。

重要な情報

- 契約と価格設定
- 給与計算
- 顧客および在庫レコードは、社員のみが使用可能

一般規則

- 各システム・ユーザーには、ユーザー・プロファイルを与える。ユーザーは、プロファイルやパスワードを共有できない。
- ユーザーは、60 日ごとにパスワードを変更しなければならない。

セキュリティー方針に関するメモの作成が完了したら、セキュリティー・レベルを選択することができます。

セキュリティー・レベルの選択

QSECURITY システム値を使用すると、システムに設定するセキュリティーのレベルを制御することができます。セキュリティー・レベルがどのように機能するかを理解するには、システムをビルに見立てて、そこに人々が入ろうとしていると考えてみてください。

レベル 20: パスワード・セキュリティー

レベル 20 を選択すると、ある程度機密の保護が得られます。ビルの入り口にいるガードマンが、ID と秘密のパスワードを尋ねてきます。 ID とパスワードの両方を認められた人だけがビルに入ることができます。しかし、一度中に入ってしまえば、好きな場所に行って、好きなことをすることができます。

もし誰かが秘密のパスワードを盗み聞きしてそれを使い、入り口のガードを通過すると、保護手段はなくなってしまいます。

レベル 30: パスワードおよび資源保護

レベル 30 には、レベル 20 の保護がすべて含まれています。加えて、ビルの特定の場所について、出入りする人間を制御し、その場所で行えることを制御することができます。ビルの一部の場所を共用のスペースとして指定し、他の場所については入り口をガードして、そこに入る人を制限することができます。

システムの場合は、制限されたセクションに対するアクセス権を持つ人に、そこで自由に作業することを許可することもできますし、許可された情報のクラーク (プログラム) に対して情報を求めるように要求することもできます。誰かのパスワードを使用して進入した人間は、保護されたセクションに入る際に、内部のガードも通過しなければなりません。

レベル 40: 保全性保護

レベル 40 には、レベル 30 で提供されるすべての保護が含まれますが、このレベルではさらに、

システムがユーザーのアクセスを検証します。ビルの内部にある入り口のガードマンは、パスワードと、その部屋に入室したすべてのユーザーの記録を調べます。

レベル 50: 拡張保全性保護
レベル 50 のセキュリティーになると、特殊な知識を持つ人間が、記録に署名した人の ID を確認して制限された入り口を通過してしまうのを防ぐために、ガードマンはより厳しい一連の規則を適用します。

推奨事項

iSeries は、出荷時にはセキュリティー・レベル 40 に設定されています。セキュリティー・レベル 40 は、セキュリティー方針が厳重、平均、または寛容のいずれであるかにかかわらず、ほとんどの導入に最適なセキュリティー・レベルです。寛容のアプローチを選択している場合は、システム上のほとんどの資源に対して、共通アクセスを設定することができます。最初からセキュリティー・レベル 40 を使用しておくと、将来、多くの変更を加えずにシステムの保護を強化することが可能になります。

アプリケーション・プログラムを購入する場合は、そのプログラムがレベル 40 でテストされていることを、アプリケーションの提供者に確認してください。一部のアプリケーションが使用する操作は、セキュリティー・レベル 40 ではエラーの原因になる場合があります。アプリケーションがレベル 40 か 50 でテストされていない場合は、レベル 30 でアプリケーションを開始してください。監査ジャーナル機能を使用して、アプリケーションが権限の失敗を記録するかどうかを確認してください。記録されない場合は、セキュリティー・レベルを 40 か 50 に変更することができます。

セキュリティー・レベル 50 を選択すると、ほとんどのシステムでは通常発生しないようなイベントを防ぐことができます。システムは、システムでプログラムが実行されるたびに付加的な検査を行います。この付加的な検査は、パフォーマンスを低下させる場合があります。

システム値選択用紙への選択したセキュリティー・レベルの記入が完了したら、サインオンに影響するシステム値を選択することができます。

サインオンに影響するシステム値の選択

セキュリティー・レベルの選択が完了したら、システム値を使用して、表示される画面、および表示される内容とシステムが相互作用する方法をカスタマイズすることができます。これらのシステム値を計画して、システム値選択用紙に選択した値を記録する必要があります。

下の表は、このトピックで使用されるシステム値について説明したものです。

表 11. iSeries のシステム値およびその説明

システム値	説明
QMAXSIGN	連続して行うことができるサインオン試行の回数を制限します。
QMAXSGNACN	連続して行えるサインオン試行回数に達した場合に行うアクションを指定します。
QLMTDEVSSN	同じユーザー・プロファイルを使用して、ユーザーが複数のワークステーションにサインオンできるかどうかを決定します。
QINACTITV	いつシステムが非活動ジョブに対してアクションを行うかを決定します。

表 11. iSeries のシステム値およびその説明 (続き)

システム値	説明
QINACTMSGQ	対話式ジョブが、QINACTITV システム値によって指定された時間、非活動状態にある場合に、システムがとるアクションを決定します。
QDSCJOBITV	システムが一時的に切断されているジョブを終了させるかどうか、およびいつ終了させるかを制御します。
QLMTSECOFR	システム上のすべてのオブジェクトに権限を持つ機密保護担当者を、特定の装置に制限します。

サインオン試行回数の制限 (QMAXSIGN および QMAXSGNACN): 2 つのシステム値によって、誰かがシステム上でサインオンを試行できる回数と、試行回数が制限に達したときにシステムが行うアクションが決定されます。

最大サインオン試行回数 (QMAXSIGN) システム値は、誤ったサインオンを連続して試行できる回数を制限します。この値によって制限された回数を超えると、システムは何らかのアクションを行います。誤ったサインオンの試行とは、誰かが無効なパスワードや不適切なワークステーションへの権限を使用して、特定のユーザー・プロファイルを使おうとすることをいいます。

最大サインオン・アクション (QMAXSGNACN) システム値は、許されている回数を超えて、サインオンが連続して試行された場合に、システムがとるアクションを指定します。可能な値は次のとおりです。

1 装置に対するこれ以上のサインオン試行を禁じます。これを、装置の使用可能化といいます。許可された人が WRKCFGSTS コマンドを使用して装置をオンにしない限り、誰もその装置にサインオンすることはできません。このオプションは通常、十分な保護を与えるものとはなりません。特に、パーソナル・コンピューターやリモート・システムから、システムへのサインオンが試行される場合は、そのように言えます。

システム操作員か、装置に対する *USE 権限を持つ人物であれば、装置を再び使用可能にすることができます。

2 ユーザー・プロファイルに対するこれ以上のサインオン試行を禁じます。これを、ユーザー・プロファイルの使用可能化といいます。許可された人がユーザー・プロファイル変更 (CHGUSRPRF) コマンドを使用してプロファイルを使用可能にするまで、誰もそのプロファイルにサインオンすることはできません。

ユーザー・プロファイルを使用可能 (状況の変更) にできるのは、そのプロファイルに対する権限を持つセキュリティー管理者だけです。

3 ユーザー・プロファイルと装置の両方を使用禁止にします。

リスクと推奨事項

時おり、パスワードを推測して、システムに侵入することを楽しんでいる人々がいます。サインオンを試行できる回数を制限することにより、これらの人々によるパスワードの推測を制限することができます。

無効なサインオンの最大数 (QMAXSIGN) のシステム値は、サインオンを試行できる回数を決定します。ユーザーが不満を抱かない程度に高く、なおかつ、ユーザーが入力ミスに注意するようになり、また侵入者にはあまり多くの推測する機会を与えない程度に低く、この回数を設定してください。適当な値として、最大サインオン試行回数を 3 から 5 に設定されるようお勧めします。

装置もユーザー・プロファイルも使用できなくなると、システム・ユーザーにとっては不便かもしれませんが、最大サインオン・アクション (QMAXSGNACN) は 3 に設定されるようお勧めします。専用の場所に置かれているワークステーションの場合は、さまざまなユーザー・プロファイルとパスワードの組み合わせを試行する機会を、侵入者に与えてしまう恐れがあります。システム上に、設置場所が原因でリスクが生じるようなワークステーションがない場合は、ユーザー・プロファイルを使用不可にするだけで、十分保護できると考えられます。

完成させた物理的セキュリティーの用紙を確認してください。離れた場所にワークステーションを置いている場合、またはリモート・ユーザー (電話回線や VPN 接続を介してシステムにアクセスするユーザー) がいる場合は、サインオンをより厳しく制限する必要があるかもしれません。システム値選択用紙の第 2 部に、選択した QMAXSIGN および QMAXSGNACN の値が追加されていることを確認してください。

ユーザーが一度に使用できるワークステーションを制限するシステム値の選択を始める前に、これらのシステム値が作用し合って、サインオンの試行を制限する方法を実際に示す例を検討する場合に役立ちます。

例: サインオン試行回数の制限: Sharon Jones はサインオン試行回数を 3 回 (QMAXSIGN は 3) に制限し、その制限を超えると、プロファイルと装置の両方が使用不可になるようにシステム値を設定しました (QMAXSGNACN は 3)。設定されたこれらの値に達すると、次のようなアクションが行われます。

1. Roger はパスワードを 2 回間違えて入力しました。
2. 2 回目の試行の後、メッセージが表示されて、もう一度誤ったサインオンを試行すると、ユーザー・プロファイルが使用できなくなることが警告されます。
3. 彼はもう一度間違えました。
4. システムは彼のプロファイルを使用不可にし、そのワークステーションにはサインオンの画面が表示されなくなります。 Roger が他のワークステーションにサインオンしようとすると、エラー・メッセージが表示されます。
5. このような場合、彼はもう一度サインオンを試行するために、Sharon に頼んでプロファイルを使用可能にしてもらわなければなりません。また、Sharon やシステム操作員は、Roger のワークステーションも使用可能にしなければなりません。 Roger がパスワードを忘れてしまったのであれば、Sharon は彼に一時的なパスワードを与えることができます。しかし、次にサインオンするときには変更する必要があります。

続いて、ユーザーが一度に使用できるワークステーションの制限を行うシステム値について検討することができます。

ユーザーが一度に使用できるワークステーションの制限: 装置セッション限界 (QLMTDEVSSN) システム値は、同じユーザーが同時に複数のワークステーションにサインオンできるかどうかを決定します。可能な値は次のとおりです。

0 システムは、同じユーザー・プロファイルを使用するユーザーが、同時にサインオンできるワークステーションの数を制限しません。

1 ユーザー・プロファイルは、一度に 1 つの装置でしか使用できません。同じ装置で複数のセッションを行うことは可能です。

リスクと推奨事項

ユーザーが一度に 1 つのワークステーションにしかサインオンできないようにすることは、優れたセキュリティーの習慣を促進します。怠惰なセキュリティーの習慣は、セキュリティーのリスクを生みます。

- ユーザーを 1 つの装置に制限する場合は、ユーザー ID とパスワードの共有が行われないようにする必要があります。ユーザー ID が共有されると、制御も責任能力も失われます。システム上で実際に誰がどの機能を使用しているのか分からなくなります。

- ユーザーは、他のワークステーションに移る際に、必ずワークステーションをサインオフするようにしなければなりません。ワークステーションを使用していないのにサインオンしたままにしておくと、セキュリティー上のリスクが生じます。

システム値 QLMTDEVSSN は 1 に設定することをお勧めします。1 に設定されていると、ユーザーは 1 つの装置に制限されます。すべてのシステム・ユーザーには、適切な権限とともに、固有のユーザー ID およびパスワードが与えられ、ユーザーは一度に使用できるワークステーションは 1 つに制限されます。システム値選択用紙の第 2 部に、選択した QLMTDEVSSN の値が追加されていることを確認してください。

次に、非活動ジョブに対するシステム値の計画を開始することができます。

非活動ジョブに対するシステム値の計画: ユーザーがワークステーションのサインオフを忘れた場合にシステムが行うアクションは、3 つのシステム値が作用し合って決定されます。

非活動ジョブ・タイムアウト間隔 (QINACTITV)
QINACTITV システム値は、サインオンされている画面で、非活動の状態が指定された時間続いた場合に、システムがアクションを行うかどうかを決定します。

注: 非活動とは、指定された時間、Enter キーや機能キーが押されないことを意味します。

非活動ジョブ・メッセージ待ち行列 (QINACTMSGQ)
QINACTMSGQ システム値の設定は、QINACTITV システム値で指定された時間制限を超えたときに、システムが行うアクションを決定します。 ENDJOB を選択した場合、システムは、QINACTITV で選択したタイムアウト間隔より長く非活動が続いたすべてのジョブを終了します。DSCJOB を選択した場合、システムは、非活動ジョブを切断します。メッセージ待ち行列の名前を指定しておくと、システムは、ジョブの非活動が続いた時、この指定された待ち行列に警告メッセージを送ります。

システムがワークステーションでジョブを**切断**すると、ジョブは一時的に延期されます。ワークステーションはサインオンの画面に戻ります。切断されたジョブは、同じユーザーが同じワークステーションにサインオンすると再開されます。

切断ジョブ・タイムアウト間隔 (QDSCJOBITV)
QDSCJOBITV システム値は、システムが一時的に切断されているジョブを終了させるかどうか、およびいつ終了させるかを制御します。切断されているジョブには、QINACTITV および QINACTMSGQ システム値の設定により、システムが自動的に切断したものが含まれます。また、ユーザーが、操作援助機能メニューやジョブの切断 (DSCJOB) コマンドを使用して、ジョブを一時的にサインオフ (切断) するように要求することもできます。

リスクと推奨事項

Sharon がサインオフするのを忘れたままワークステーションを離れてしまうと、John がそのワークステーションにやってきて、Sharon がシステムに対して持つ権限で、何らかの機能を実行することも可能になります。

次の 2 つの場合には、特に非活動の画面を規制する必要があります。
- システムには機密情報が保管されているため、厳しいセキュリティー環境を設定している。
- 社外の人々が容易に出入りできる場所にワークステーションが置かれている。

日常の仕事においては、ワークステーション上のユーザーの作業が中断されることがしばしばあります。これらの 3 つのシステム値が作用し合う方法を利用して、通常の中断を許可し、なおかつシステムのセキュリティーを保護するようにしてください。

これらのリスクを除くため、IBM では、QINACTITV、QINACTMSGQ、および QDSCJOBITV システム値をともに使用して通常の作業の割り込みを許可し、なおかつシステムのセキュリティーを保護するようにお勧めします。

非活動ジョブ・タイムアウト間隔 (QINACTITV): この間隔は、ワークステーションが無人の状態で放置されないように短くする必要がありますが、ユーザーが不便を感じるほどには短くしないでください。推奨されている設定は、30 分です。ジョブが非活動のまま 30 分が経過すると、システムは、非活動ジョブ・メッセージ待ち行列で指定されたアクションを行います。

非活動ジョブ・メッセージ待ち行列 (QINACTMSGQ): 切断されたジョブを選択します。システムは、非活動ジョブ・タイムアウト間隔で指定された時間、非活動の状態が続いたすべてのジョブを切断します。システムは、ジョブを延期し、画面をサインオフします。同じユーザーが再びサインオンすると、ジョブは切断された時点から再開されます。

この機能の場合、システムはジョブを終了せずに延期するため、ユーザーにとって便利です。非活動ジョブを切断すると、システムは、ジョブを終了する場合と同じように保護されます。

注: システムは、一部のジョブを切断できない場合があります。システムが非活動ジョブを切断できない場合は、代わりにジョブを終了します。ジョブが終了された場合、情報は失われる場合があります。QINACTMSGQ の設定を考慮して、システム操作員メッセージ待ち行列にメッセージが送られるようにしてください。

切断ジョブ・タイムアウト間隔 (QDSCJOBITV): 短い時間ワークステーションを離れる場合はシステムを一時的にサインオフし、長い時間中断しなければならない場合は作業を完了させてからサインオフするように、システム・ユーザーに指示してください。

QDSCJOBITV を使用して、システムが自動クリーンアップなどの夜間処理を開始する前に、切断されているジョブを終了させてください。この間隔は、業務を行っているほとんどの時間に、ユーザーがワークステーションに戻っても使えるよう、十分な長さに設定する必要がありますが、夜間処理が開始される前にはジョブを終了する長さでなければなりません。ユーザーのジョブを妨げることなく夜間処理を完了できる十分な時間を確保するために、300 分 (5 時間) を選択してください。

注: 2 人のユーザーが同じ情報を同時に変更しようとするのを防ぐため、システムは、情報を更新する前にレコードを**ロック**します。資源に対するロックは、システムがユーザーのジョブを切断しても有効です。ご使用になるアプリケーションの設計、およびシステム上のユーザーの数によっては、ロックがシステムでパフォーマンス上の問題を引き起こす場合があります。プログラマーかアプリケーションの提供者に確認して、ロックがパフォーマンスに悪影響を与えるかどうかを判別してください。

これらのシステム値がどのように作用し合って、システムで非活動ジョブを操作するかについて、例を検討することができます。

システム値選択用紙に非活動ジョブに関する決定を記録した後、機密保護担当者がサインオンする場所の制限を決定することができます。

例: QINACTITV、QINACTMSGQ、および QDSCJOBITV システム値による非活動ジョブの操作: 非活動ジョブ・タイムアウト間隔 (QINACTITV) を 30 秒に設定したとします。システムは非活動ジョブを切断します (QINACTMSGQ は DSCJOB)。切り離しジョブ・タイムアウト間隔 (QDSCJOBITV) は 300 分 (5 時間) です。たとえば、Sharon が 午前 9:30 にサインオフを忘れたとします。すると、システムは午前 10:00 にジョブを切断し、午後 3:00 にジョブを終了します。

選択した QINACTITV、QINACTMSGQ、および QDSCJOBITV システム値を、システム値選択用紙の第 2 部に追加してください。

システム値選択用紙に非活動ジョブに関する決定を記録した後、機密保護担当者がサインオンする場所の制限を決定することができます。

機密保護担当者がサインオンする場所の制限: セキュリティーを変更し、オブジェクトを制御する権限を持つユーザーを、特定のワークステーションに制限することができます。この制限により、これらのユーザーが、お客様の知らないところで、離れた場所にあるワークステーションにサインオンすることを防ぐことができます。これは、システム値 QLMTSECOFR (機密保護担当者限界) を使用して行うことができます。QLMTSECOFR を 1 に設定すると、全オブジェクト (*ALLOBJ) 特殊権限、またはサービス (*SERVICE) 特殊権限を持つユーザーは、コンソールか他の指示されたワークステーションにしかアクセスできなくなります。

QLMTSECOFR は、機密保護担当者、システム上のすべてのオブジェクトに対する権限を持つユーザー、およびサービス担当員をコンソールに制限します。オブジェクト権限認可 (GRTOBJAUT) コマンドを使用して、これらのユーザーに他の装置へのアクセスを許可ことができます。

注: QLMTSECOFR システム値を作用させるためには、システム・セキュリティー・レベルが 30 以上でなければなりません。

リスクと推奨事項

QLMTSECOFR システム値は、1 に設定されるようお勧めします。機密保護担当者のプロファイルを使用して、誰かがパスワードを盗んだり、推測したりした場合は、サインオンが許可されている装置へのアクセスも入手しなければなりません。

システム値選択用紙の第 2 部で、選択した QLMTSECOFR の記入が完了したら、パスワードに影響するシステム値を選択することができます。

パスワードに影響するシステム値の選択

ユーザーのパスワードは、機密保護担当者が割り当てるのではなく、ユーザーが自分で割り当てられるようにしなければなりません。ユーザーが自分でパスワードを作成すれば、大抵の場合それを紙に書いて覚える必要はなくなります。紙に書いたパスワードを人目に付く場所に置いたりすれば、セキュリティー上のリスクを生じさせることになります。

パスワードを作成する際のヒント

良いパスワードというのはなかなか思い付かない場合があります。そのような場合は、このような手法を使うこともできます。それは、覚えやすい文を使って想像しにくいパスワードを作る手法です。たとえば、休暇の後であれば、「July 4th fishing was poor (7 月 4 日の釣りはさっぱりだった)」というような文を使えるかもしれません。この場合、J4FWP というパスワードを作ることができます。

システム値によっては、パスワードを規制するものがあります。ユーザーにパスワードの変更を求める頻度を制御することができます。また、多くの規則を設けて、容易に想像できるパスワードが使用されるのを防ぐこともできます。これらのシステム値の大部分は、大規模な組織の場合に必要なシステム値です。また、そのいくつかについては、すべてのユーザーに必要です。

ASSIST メニューのオプション、またはパスワード変更 (CHGPWD) コマンドを使用して、ユーザーは各自のパスワードを割り当てることができます。ユーザーが自分のパスワードを変更する場合、システムは、パ

スワードのシステム値と照らして新しいパスワードをチェックします。ユーザーが CHGUSRPRF コマンドを使用してパスワードを変更した場合は、システムは、セキュリティー・システム値に対して、新しいパスワードをチェックしません。

注: 何らかのパスワード・システム値が設定されている場合、システムは、CHGUSRPRF コマンドを使用してパスワードを設定しない限り、新しいパスワードにユーザー・プロファイル名と同じストリングが使用されることを許しません。

下の表は、パスワードに影響する値とその定義を示しています。

表 12. iSeries のパスワードに関連するシステム値

システム値	説明
QPWDEXPITV	指定された期間を過ぎると、パスワードを変更するようにユーザーに要求します。
QPWDMAXLEN	パスワードの最大文字長を指定することができます。
QPWDMINLEN	パスワードの最小文字長を指定することができます。
QPWDRQDDIF	ユーザーが 2 つの異なるパスワードを交互に使用するのを防ぎます。

以下のトピックでは、これらのパスワード関連のシステム値について、さらに詳細に説明しています。

- パスワード使用期間の決定
- パスワードの長さの決定
- パスワード重複の制限

CL コマンド行で `WRKSYSVAL *SEC` と入力して、QPWD の文字で始まるシステム値のオンライン情報を参照してください。

パスワード使用期間の決定: QPWDEXPITV システム値は、ユーザーにパスワードの変更を求める頻度を決定します。

パスワードの満了日が近づくと、ユーザーにはシステムからの警告が与えられます。パスワードの満了日を過ぎると、システムはプロンプトを出して、次のサインオンの際にパスワードを変更するようユーザーに指示します。

推奨事項

ユーザーには定期的にパスワードを変更させる必要があります。そのようにすることによって、ユーザーが他のシステム・ユーザーとパスワードを共有しにくくします。また、定期的にパスワードを変更していれば、許可を持たないユーザーに誰かのパスワードを盗まれても、そのパスワードは短期間で無効になります。パスワード変更の間隔は、ユーザーを不快にさせない程度に長く、かつ良いセキュリティーを保てる程度に短く設定する必要があります。これらの問題を防ぐため、パスワード変更の間隔を 45 日から 60 日の間に設定します。

システム値選択用紙の第 2 部で、選択した QPWDEXPITV システム値の記入が完了したら、パスワードの長さを決定することができます。

パスワードの長さの決定: ユーザーの中には、入力することが好きではない人がいます。そのような人に自由にパスワードを決めさせると、パスワードを 1 文字にしたり、イニシャルをパスワードにしたりしま

す。しかしながら、パスワードを短く設定すると、侵入者が偶然にパスワードを当ててしまう可能性も高くなります。 QPWDMINLEN システム値では、システム上のすべてのパスワードについて、その最低の長さを設定することができます。

ご使用のシステムが他のシステムと通信を行う場合、ユーザーは 2 つのコンピューターの間でパスワードを交換することができます。通信の方式によっては、パスワードを最大 8 文字に制限している場合があります。 QPWDMAXLEN システム値では、パスワードの最大の長さも指定することができます。

推奨事項

パスワードの最小文字長は 6 文字に設定してください。こうすれば、イニシャルが使用されるのを防ぐことができますし、パスワードの選択に趣向を凝らすようユーザーに促すこともできます。ご使用のシステムで他のシステムと通信を行う場合は、パスワードの最大文字長を 8 文字に設定してください。

システム値選択用紙の第 2 部で、選択した QPWDMINLEN および QPWDMAXLEN システム値の記入が完了したら、パスワード重複の制限を設定することができます。

パスワード重複の制限: パスワード変更 (CHGPWD) コマンドを使用する場合、新規パスワードを旧パスワードと同じものにすることはできません。しかし、QPWDRQDDIF システム値を使用して、2 つの異なるパスワードを禁止しない限り、ユーザーはそれらを交互に使用することができます。下の表は、QPWDRQDDIF システム値に選択できる値を示しています。

表 13. QPDRQDDIF システム値の値

値	重複のチェックの対象となるパスワード数
0	0、すなわち重複パスワードを許可する。
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

推奨事項

パスワード有効期限の間隔とパスワードの重複の値を使用して、パスワードが 1 年間重複しないように要求してください。たとえば、パスワードの有効期限を 60 日にした場合、QPWDRQDDIF システム値には 7 を選択します。

システム値選択用紙の第 2 部で、選択した QPWDRQDDIF システム値の記入が完了したら、システムをカスタマイズするためのシステム値の使用法を決定することができます。

システムをカスタマイズするためのシステム値の使用

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

システムの命名

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

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

推奨事項

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

たとえば、JKL Toy Company の Sharon Jones は、システムの名前を JKLTOY としました。

システムにおける時刻および日付の表示

システムが日付を印刷または表示する際の、年、月、および日の順番を設定することができます。また、それぞれ年 (Y)、月 (M)、および日 (D) の間にシステムが使用する文字を指定することができます。

システム値 QDATFMT は、日付形式を決定します。次の表は、選択可能な値ごとに、どのように日付 16 June 2000 が印刷されるかを示しています。

表 14. QDATFMT (システム日付形式)

選択可能な値	説明	結果
YMD	年、月、日	00/06/16
MDY	月、日、年	06/16/00
DMY	日、月、年	16/06/00
JUL	年間通算日	00/168

注: 上の例では、スラッシュ (/) で日付を区切っています。

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

表 15. QDATSEP (システム日付区切り記号)

区切り文字	QDATSEP の値	結果
/ (スラッシュ)	1	16/06/00
- (ハイフン)	2	16-06-00
. (ピリオド)	3	16.06.00
, (コンマ)	4	16,06,00
(ブランク)	5	16 06 00

注: 上の例では、DMY 形式を使用しています。

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

表 16. QTIMSEP (システム時刻区切り記号)

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

システム装置の命名方法の決定

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

表 17. システム装置の命名

選択可能な値	命名形式	表示装置名	印刷装置名
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	装置のアドレス	DSP010003	PRT010002

注: 上の例では、表示装置と印刷装置が 1 番目のケーブルに接続されています。

推奨事項

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

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

システム印刷装置の選択

QPRTDEV システム値を使用して、システム印刷装置を割り当てます。特定のジョブで使用する印刷装置は、このシステム値、ユーザー・プロファイル、およびジョブ記述によって決定されます。ユーザー・プロファイルかジョブ記述で他の印刷装置が指定されていない限り、ジョブはシステム印刷装置を使用します。

推奨事項

通常、システム印刷装置には、システム内で最も速い印刷装置を使用します。長い報告書とシステム出力には、システム印刷装置を使用します。

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

完了した印刷装置出力の表示の使用可能化

システムには、ユーザーの印刷装置出力を検索する機能があります。「印刷装置出力の処理」画面には、現在印刷されている、または印刷を待っているすべての出力が表示されます。また、完了した印刷装置出力のリストを、ユーザーが表示できるようにすることもできます。この画面は、いつ出力が印刷されたのか、およびどの印刷装置で印刷されたのかを示します。これは、紛失した報告書を探すときに便利な機能です。

ジョブ会計機能および QACGLVL システム値を使用すると、完了した印刷装置出力を表示することができます。 QACGLVL システム値に *PRINT オプションを使用すると、完了した印刷装置出力に関する情報を保管することができます。

推奨事項

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

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

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

例: JKL Toy Company のセキュリティー方針: 下のメモは、JKL Toy Company の代表取締役である John Smith が、セキュリティー方針を実際に示すために、従業員に対して送ったメモです。彼は、自分と Sharon が作成したメモを使用して、このセキュリティーのメモを書き上げました。

表 18. 例: JKL Toy Company のセキュリティーのメモ

送信者: John Smith、代表取締役

JKL Toy Company

宛先: 全 JKL Toy Company 社員

件名: 新システムのセキュリティー

すべての社員の皆さんは、我が社の新しいシステムに関してお知らせするための会議に出席されたことと思います。システムを使用する人たちはすでに訓練を開始しており、来週には顧客注文処理が開始されます。このシステムはすぐに、ビジネスを成功させる上で重要な役割を果たすようになるであろうと思われます。

このたび、我が社のセキュリティーの決定と方針を検討し、その重要性を強調したいと思います。これらの方針は、我が社のビジネスにおいて重要な情報を保護するためのものです。

- 新しいシステムにおいては、Sharon Jones がセキュリティーの責任者となります。また、Ken Harrison が彼女の補佐として働きます。セキュリティーについて何か質問がある場合や、何らかの問題に気付いた場合は、これらの担当者に相談してください。
- システム上で機能を実行するユーザーに関する決定は、情報に関する現在の方針に基づくものです。たとえば、以下のような情報があります。
  - 契約と特別な価格設定の情報は、機密であると考えます。これらの情報は、社外の誰にも漏らしてはなりません。
  - お客様に対するクレジットの限度額を設定および変更できるのは、経理の担当者のみです。
- システムを使用する必要のあるすべての人には、ユーザー ID とパスワードが渡されます。システムに最初にサインオンする際に自分のパスワードを変更し、その後は 60 日ごとにパスワードを変更してください。パスワードは、自分が覚えられるものを選択しますが、分かりやすいパスワードは避けてください。ユーザー ID と一緒に渡される用紙には、パスワード作成に関するいくつかの提案が示されています。
- *他の人とパスワードを共有しないでください。*皆さんが各自のジョブを行うために必要なことは、すべてシステム上で行えるようにする予定です。情報にアクセスする必要がある場合は、Sharon か Ken に連絡してください。パスワードを忘れてしまった場合は、Sharon か Ken がすぐに新しいパスワードを設定してくれます。したがって、他の人のユーザー ID とパスワードを使用してサインオンする理由はありません。
- 皆さんが使用するワークステーションには、入力を保存するための記録およびプレーバック機能がある場合があります。パスワードを保管するためにこの機能を*使用しない* でください。
- デスクを離れる際は、ワークステーションをサインオンしたままにしないでください。訓練の中では、ワークステーションを一時的にサインオフする方法を学ぶことができます。短時間デスクを離れる場合は、この機能を使用してください。長時間デスクに戻らないのであれば、作業を終了して通常のサインオフを使用してください。

  発送所や顧客サービスのエリア、および離れた場所にある営業所など、一般の人々が出入りできる場所の場合は、ワークステーションを離れる際のサインオフが特に重要です。
- システム装置はとても頑丈にできているとはいえ、衝撃を与えたり、上にものを置いたりすることは避けてください。通常、装置の制御パネルは非活動にされていますが、このパネルには触らないでください。経理部門の担当者は、誰もシステム装置に不正操作しないように、責任をもって監視してください。

この新しいシステムは、我が社のすべての仕事をより容易にし、ビジネスのパフォーマンスを向上させるためのものであることを銘記してください。このセキュリティー方針は皆さんを助けるためのものであり、妨害するためのものではありません。質問やご意見は、遠慮なく Sharon、Ken、または私までお知らせください。

セキュリティー方針のドラフトの作成が完了したら、ユーザー・グループの計画を開始することができます。

ユーザー・グループの計画

計画のプロセスの最初のステップは、セキュリティー戦略の決定です。これは、会社の方針を設定するのに似ています。次いで、ユーザーのグループを計画することができます。これは、部門の方針を決定するのに似ています。

ユーザー・グループとは

ユーザー・グループとは、まさにその名前が示す通り、同じアプリケーションを同じ方法で使用する必要がある人々のグループです。一般的に、ユーザー・グループは、同じ部門で働き、仕事の責任が似ている人同士で構成されます。ユーザー・グループは、グループ・プロファイルを作成することによって定義します。

グループ・プロファイルで何をするか

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

- **セキュリティー・ツール**: グループ・プロファイルを使用することによって、システム上で特定のオブジェクトを使用できる人 (オブジェクト権限) を簡単に編成することができます。グループの個々のメンバーにではなく、グループ全体に対してオブジェクト権限を定義することができます。
- **カスタマイズ・ツール**: 個々のユーザー・プロファイルを作成する際のパターンとして、グループ・プロファイルを使用することができます。同じグループになる大抵のユーザーは、初期メニューおよび省略時の印刷装置など、カスタマイズの要件は同じになります。これらの要件をグループ・プロファイルに定義し、それを個々のユーザー・プロファイルにコピーすることができます。

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

どのような用紙が必要か

ユーザー・グループを計画するには、次の用紙が必要です。

- ユーザー・グループ識別用紙
- ユーザー・グループ記述用紙

注: システム上の各ユーザー・グループについて 1 つのユーザー・グループ記述用紙が必要になります。

これらの用紙を完成させる上で、次のトピックを検討することができます。

- ユーザー・グループの識別
- グループ・プロファイルの計画
- サインオンに影響する値の選択
- ユーザーが実行できる機能を制限する値の選択
- ユーザーの環境を設定する値の選択

ユーザー・グループの識別

ユーザー・グループを計画する場合、まずシステム上にあるユーザーのグループを識別することが必要です。このようにグループを識別することによって、それらのグループに必要な資源へのアクセスを計画することができます。ユーザー・グループを識別する、1 つの簡単な方法を使ってみましょう。システムを使用する計画がある部署やワークグループについて考えてみてください。前の部分で描いた、使用するアプリケーションのアプリケーション図を見てください。ワークグループとアプリケーションとの間に、自然な関係が存在しているかどうかを調べてください。

- 各ワークグループの 1 次アプリケーションを識別できるか。
- 各グループに必要なアプリケーションを認識しているか。各グループが必要としないアプリケーションは何か。
- 各アプリケーション・ライブラリーに情報を持つべきグループを認識しているか。

これらの質問に「はい」と答えられる場合は、グループ・プロファイルの計画を始めることができます。しかし、「時々」とか、「たぶん」という答えの場合は、系統立ててユーザー・グループを識別するとよいでしょう。

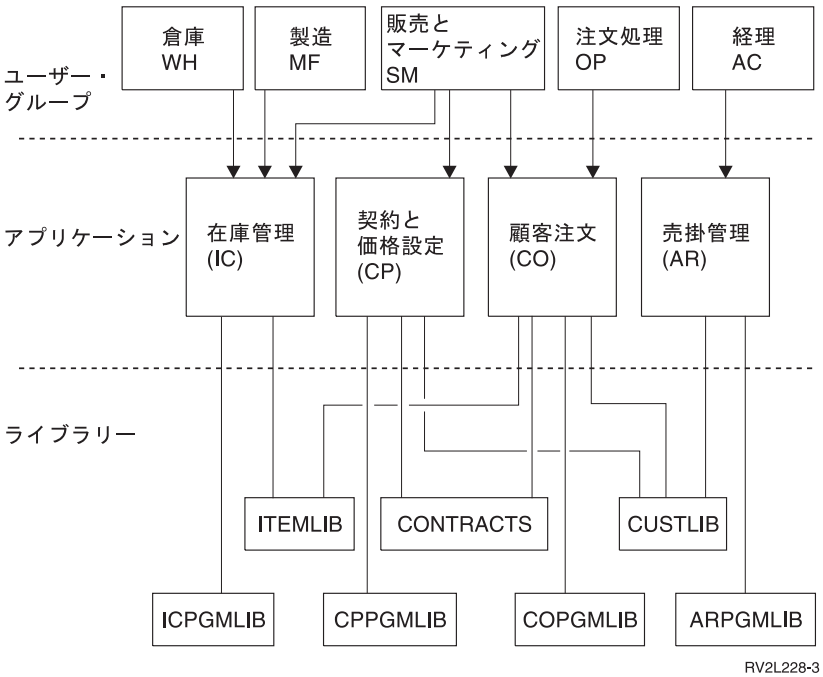
このようなアプローチによるユーザー・グループの識別については、例を検討することができます。

注: 1 人のユーザーが属するグループ・プロファイルを 1 つだけに絞るなら、セキュリティーの管理を単純化することができます。しかし、ある場合には、1 人のユーザーを複数のグループ・プロファイルに属させた方が、役に立つ場合もあります。

ユーザーを複数のグループ・プロファイルに属させると、通常は、個々のユーザー・プロファイルに私用権限を与えるよりも、管理が容易になります。

例: ユーザー・グループの識別: ワークグループとアプリケーションとの関係が分かりにくく思えたり、はっきりしない場合は、ユーザー・グループ識別用紙のようなマトリックス手法を使用すると理解しやすくなります。システム・ユーザーとそれらのユーザーに必要なアプリケーションを、マトリックス上に作図すると、似たようなパターンが浮かび上がってきます。ユーザー・グループ識別用紙の記入に加えて、Sharon Jones は、先に作成したアプリケーション図を使用して、各アプリケーションにアクセスする必要のあるユーザー・グループを識別しました。

下のイラストは、JKL Toy Company のアプリケーション図を示しています。



セキュリティーへのアプローチを「寛容」にしている場合は、アプリケーションを必要とするユーザーを X で示します。セキュリティーへのアプローチを「厳重」にしている場合は、ユーザーがアプリケーションをどのように使用するかについても、考慮しなければなりません。ユーザーに必要なアプリケーションの

使用法が、アプリケーションに含まれる情報を見ることだけであるなら、マトリックスに X とは書かずに V (表示) を使用します。アプリケーションの情報を変更する必要もあるユーザーについては、C (変更) を使用します。情報に対して主要な責任を持つユーザーについては、O (所有者) を使用します。

たとえば、JKL Toy Company では、さまざまなグループが契約と価格設定のアプリケーションを必要とします。

- 販売マーケティングの部門は、価格を設定し、顧客との契約を取り付けます。この部門は、価格設定および契約の情報を*所有* しています。
- 顧客注文の部門は、間接的に契約情報を変更します。この部門で注文が処理されると、契約の数量が変更されます。彼らは、契約と価格設定の情報を*変更* する必要があります。
- 注文処理の担当者たちは、作業の計画を立てるためにクレジットの限度額を知る必要がありますが、その情報を変更することは許されていません。彼らはクレジットの限度額に関するファイルを*表示* する必要があります。

表 19. JKL Toy Company のユーザー・グループ識別用紙: 例

ユーザー・グループ識別用紙					
作成者: Sharon Jones		日付: 9/2/99			
		アプリケーションに対して必要なアクセス			
ユーザー名	部門	アプリケーション: CO	アプリケーション: IC	アプリケーション: PC	アプリケーション: AR
Ken H.	注文処理 (OP)	O	C	C	C
Karen R.	注文処理 (OP)	O	C	C	C
Kris T.	経理 (AC)	V		V	O
Sandy J.	経理 (AC)	V	C	V	O
Peter D.	経理 (AC)	C		V	O
Ray W.	倉庫 (WH)	V	O	V	
Rose Q.	倉庫 (WH)	V	O	V	
Roger T.	販売マーケティング (SM)	C	C	O	C
Sharon J.	マネージャー (MG)	C	C	C	C

注:

- セキュリティー環境が*寛容* の場合は、ユーザーに必要なアプリケーションを X で示す。
- セキュリティー環境が*平均* の場合は、ユーザーが権限を持つアプリケーションを A で示す。
- セキュリティー環境が*厳重* の場合は、C (変更)、V (表示)、および O を使用してアプリケーションの*使用法* を指定する。

Sharon Jones は、マトリックスを作成する際に決定した点について、いくつかのメモを作成しました。

- 注文処理と経理は相互にバックアップを作成する。現在のところ、これらの部門に必要なアプリケーションは類似しているが、将来、人員が増えるにつれてより専門的な働きをするようになるので、グループを分けておいた方が良い。
- 注文処理の担当者には、在庫や契約の情報を直接変更することは許可していないが、彼らが注文を受けたり処理したりすると、品目や契約の数は自動的に変更される。これは、後になってセキュリティーの問題になるだろうか。

- 販売マーケティングの担当者は、ビジネスのすべての部分およびすべてのアプリケーションに関係している。彼らは品目の価格を設定し、品目に関する説明を作成する。クレジットの限度額を設けるのは経理部門だが、販売マーケティング部門が新しい顧客を開拓する。彼らは契約に関連したすべての事項と価格の設定に責任を持つ。

各ユーザー・グループの役割を決定してください。決定においてユーザー・グループ識別用紙が必要であれば、この用紙に記入してください。

ユーザー・グループ識別用紙にユーザーを追加したら、グループ・プロファイルを計画することができます。

グループ・プロファイルの計画

ユーザー・グループを識別したら、続いて各グループにプロファイルを計画することができます。下される決定の多くは、セキュリティーとカスタマイズの両方に影響します。たとえば、初期メニューを指定すると、あるユーザーをそのメニューだけに制限することになるでしょう。しかし、その指定は、そのユーザーがサインオンした後に、適切なメニューが表示されるようにすることにもなります。

例として、1 つのユーザー・グループに対してユーザー・グループ記述用紙を作成します。最初の用紙が完成した後、前に戻って、必要な他のグループについても用紙を完成させます。

iSeries のセキュリティーとカスタマイズは非常に柔軟に設計されています。このトピックの計画方法は、グループ・プロファイルとジョブ記述を設計するのに良い方法ですが、プログラマーやアプリケーションの提供者が他の方法を推奨する場合もあります。

グループ・プロファイルの命名

グループ・プロファイルは、特別なタイプのユーザー・プロファイルとして働くため、リスト上や画面上で簡単に識別できるようにすると便利です。そのようにするには、グループ・プロファイルに特別な名前を付ける必要があります。グループ・プロファイルがリスト上にまとめて表示されるようにするには、すべてのグループ・プロファイル名の先頭を、 GRP (グループ) や DPT (部門) などの同じ文字で統一する必要があります。ユーザー・グループに名前を付ける際は、以下のガイドラインに従ってください。

- ユーザー・グループ名は最大 10 文字までです。
- 名前には、文字、数字、およびいくつかの特殊文字 (ポンド (#)、ドル ($)、円 (¥)、下線 (_)、およびアットマーク (@)) を使用することができます。
- 名前を数字で開始することはできません。

注: 各グループ・プロファイルに対して、システムは、グループ識別番号 (*gid*) を割り当てます。通常は、システムに *gid* を生成させることができます。システムをネットワークで使用する場合は、グループ・プロファイルに、固有の gid を割り当てなければならない場合があります。ネットワーク管理者に相談して、gid を割り当てる必要があるかどうかを検討してください。

命名規則用紙の適当なフィールドに、グループ・プロファイルの命名システムを追加してください。たとえば、Sharon Jones は、グループ・プロファイルの命名規則として DPT を選択しました。彼女は、命名規則用紙の適当な箇所に選択した内容を追加しました。

表 20. JKL Toy Company の命名規則用紙: グループ・プロファイルの例

オブジェクトのタイプ	命名規則
グループ・プロファイル	名前の先頭には DPT の文字を使用し、その後に部門の省略形を付ける。グループ・プロファイルのテキスト記述には、部門名を示す。

ユーザー・グループに必要なアプリケーションおよびライブラリーの判別

ユーザー・グループを、先に作成したアプリケーション図とライブラリーにまだ追加していない場合は、追加してください。この視覚的なイメージは、各グループに必要な資源とアプリケーションを決定する上で役立ちます。

ユーザー・グループ記述用紙の第 1 部では、グループの 1 次側アプリケーション、つまりそのグループで最も頻繁に使用するアプリケーションを指示します。また、グループに必要な他のアプリケーションをリストしてください。

作成したアプリケーション記述用紙とアプリケーション図を見て、各グループに必要なライブラリーを調べてください。プログラマーやアプリケーションの提供者に相談して、これらのライブラリーへのアクセスを提供する、最良の方法を探してください。ほとんどのアプリケーションでは、次のいずれかの手法を使用します。

- アプリケーションが、ライブラリーをユーザーの初期ライブラリー・リストに組み込む。
- アプリケーションがセットアップ・プログラムを実行して、ライブラリーをユーザーのライブラリー・リストに置く。
- ライブラリーが、ライブラリー・リストに含まれている必要はない。アプリケーション・プログラムは、常にライブラリーを指定します。

システムは、ライブラリー・リストを使用して、アプリケーションが実行される際に必要なファイルとプログラムを検索します。**ライブラリー・リスト**とは、システムがユーザーに必要なオブジェクトを検索するライブラリーのリストです。このリストには、次の 2 つの部分があります。

1. **システム部分**: QSYSLIBL システム値によって指定された部分。システム部分は OS/400® ライブラリーに使用されます。このシステム値のデフォルトは、変更する必要はありません。
2. **ユーザー部分**: ライブラリー・リストのうち、ユーザー部分は、QUSRLIBL システム値による部分です。ユーザーのジョブ記述は、初期ライブラリー・リスト、つまりユーザーがサインオンした後のコマンドを指定します。初期ライブラリー・リストがある場合、このリストは QUSRLIBL システム値を一時変更します。アプリケーション・ライブラリーは、ライブラリー・リストのユーザー部分に含まれます。

ジョブ記述の使用

ユーザーがシステムにサインオンする際、ユーザーのジョブ記述は、ジョブの印刷方法、バッチ・ジョブの実行方法、および初期ライブラリー・リストを含む、ジョブの多くの特性を定義します。このシステムには QDFTJOBD というジョブ記述がありますが、グループ・プロファイルを作成する際に、このジョブ記述を使用することができます。ただし、QDFTJOBD は、初期ライブラリー・リストとして QUSRLIBL システム値を指定しています。ユーザー・グループによって、サインオンの際にアクセスするライブラリーが異なる場合は、グループごとに固有のジョブ記述を作成する必要があります。

グループに必要な各ライブラリーを、ユーザー・グループ記述用紙にリストしてください。グループのジョブ記述で、初期ライブラリー・リストに加えるライブラリーについては、用紙の各ライブラリー名にマークを付けてください。

サインオンに影響する値の選択を開始する前に、JKL Toy Company の Sharon Jones が、どのようにユーザー・グループの記述を作成したか、例を検討することができます。

例: JKL Toy Company のユーザー・グループ記述用紙: 1 つ目の表は、Sharon Jones が販売マーケティング部門について作成した、ユーザー・グループ記述用紙の第 1 部を示しています。彼女が、グループの初期ライブラリー・リストに、ライブラリー CONTRACTS および CPPGMLIB を含めていない点に注意し

てください。これらのライブラリーを DPTSM 初期ライブラリー・リストに組み込むのではなく、アプリケーションが自動的にこれらのライブラリーをライブラリー・リストに追加するようにします。すると、ユーザーがアプリケーションを終了したときに、システムはこれらのライブラリーをライブラリー・リストから除去します。これにより、アプリケーション・プログラムを介さなければこれらのライブラリーにアクセスできなくなるため、ライブラリーをより安全に保護することができます。

表 21. JKL Toy Company のユーザー・グループ記述用紙: 記述情報の例

ユーザー・グループ記述用紙	1 / 2
作成者: Sharon Jones	日付: 9/5/99
グループ・プロファイル名: DPTSM グループの説明: 販売マーケティング部門	
グループの 1 次側アプリケーション: 契約と価格設定 グループに必要な他のアプリケーションのリスト: 在庫管理 (品目の説明と価格を入力するため)、顧客注文	
グループに必要な各ライブラリーをリストします。グループの初期ライブラリー・リストに含める必要のある各ライブラリーにはマーク (✔) を付けます。 • ✔CUSTLIB • ✔ITEMLIB • ✔COPGMLIB • ✔ICPGMLIB • CPPGMLIB • CONTRACTS	

加えて、Sharon は、倉庫部門についても、ユーザー・グループ記述用紙の作成を開始しました。

表 22. ユーザー・グループ記述用紙: 記述情報

ユーザー・グループ記述用紙	1 / 2
作成者: Sharon Jones	日付: 9/5/99
グループ・プロファイル名: DPTWH グループの説明: 倉庫部門	
グループの 1 次側アプリケーション: 在庫管理 グループに必要な他のアプリケーションのリスト: なし	
グループに必要な各ライブラリーをリストします。(グループの初期ライブラリー・リストに含める必要のある各ライブラリーにはマーク (✔) を付ける): • ✔ITEMLIB • ✔ICPGMLIB	

ユーザー・グループ記述用紙の第 1 部を完成させたら、サインオンに影響する値の選択を開始することができます。

サインオンに影響する値の選択

システムのグループ・プロファイルを計画したら、サインオンに影響するシステム値を選択する必要があります。選択した値を、ユーザー・グループ記述用紙の第 2 部に記入してください。ここで選択する値は、

グループのメンバーごとの個別プロファイルを作成するために、コピーして使用されることを覚えておいてください。まず初めに、選択したグループ・プロファイル名を入力し、そのグループについての簡単な説明 (テキスト) を入力します。

システムを適切にカスタマイズすると、ユーザーは、サインオン画面で、ユーザー ID とパスワードを入力するように要求されます。ユーザー・プロファイルには、他のサインオン値が含まれています。

パスワード

グループ・プロファイルのパスワードを *NONE に設定します。これによって、だれもグループ・プロファイルでサインオンできないようにすることができます。後でグループ・プロファイルをコピーして、個々のユーザー・プロファイルを作成する際に、各ユーザーのパスワードを設定します。

初期プログラムおよび初期プロシージャー

ユーザーの初期プログラムは、**サインオン・プログラム**とも呼ばれ、システムが最初のメニューを表示する前に実行されます。ライブラリーが初期ライブラリー・リストの一部である場合でも、グループ・プロファイルには、プログラムとそのライブラリーの両方の名前を記入してください。この両方を指定することによって、確実にシステムが適切なプログラムを実行するようになるので、ライブラリー・リストの変更を気にする必要がなくなります。

初期プログラムや初期プロシージャーは、次のいずれかの理由で使用されます。

- アプリケーションによっては、初期プログラムを使用してアプリケーション環境を設定するものがある。
- ユーザーに対してメニューを表示せず、1 つのプログラムだけを使用させる。たとえば、JKL Toy Company の場合、発送所でワークステーションを使用する人々には、在庫状況を受信するプログラムしか実行できないようにします。このようにすることによって、共用の場所にあるワークステーションで、セキュリティーの問題を防ぐことができます。

ユーザーの「**制限機能**」フィールドを *YES または *PARTIAL にしておくと、ユーザーがサインオン画面で初期プログラムを変更できないようすることができます。

プログラマーと相談して、ご使用のアプリケーションに、初期プログラムや初期プロシージャーが必要かどうかを調べてください。

初期メニューおよび初期メニュー・ライブラリー

初期メニューは、**第 1 メニュー**とも呼ばれ、ユーザーがサインオンした後に最初に表示されるメニューです。初期プログラムは、この初期メニューが表示される前に実行されます。初期プログラムが何らかの画面を表示する場合は、システムが初期メニューを表示する前に、それらの画面が表示されます。

通常、グループの初期メニューには、そのグループのメイン・アプリケーションの 1 次メニューを使用します。メニュー名とそのライブラリーの両方を指定してください。

ユーザーの「**制限機能**」フィールドを *YES にしておくと、ユーザーはサインオン画面で初期メニューを変更できなくなります。ユーザーの「*制限機能*」フィールドが *PARTIAL になっていると、ユーザーはサインオン画面で初期メニューを変更することができます。

現行ライブラリー

現行ライブラリーは、**省略時のライブラリー**とも呼ばれます。ユーザーに現行ライブラリーを指定すると、以下のような処置が行われるようになります。

- ユーザーが、Query プログラムなどの何らかのオブジェクトを作成した場合、システムは、ユーザーが別のライブラリーを指定しない限り、これらのオブジェクトを現行ライブラリーに入れます。
- システムは、ライブラリー・リストのユーザー部分に、現行ライブラリーを自動的に追加します。現行ライブラリーは、ジョブ記述の初期ライブラリー・リストに組み込むこともできますが、必ずしもそうする必要はありません。
- 現行ライブラリーは、ライブラリー・リストのユーザー部分で最初のライブラリーになります。システムは、ユーザーのライブラリー・リストでライブラリーを検索する前に、現行ライブラリーでファイルとプログラムを検索します。
- ユーザーに対して現行ライブラリーを割り当てなかった場合、システムは QGPL (汎用) ライブラリーを割り当てます。

推奨事項

IBM Query for iSeries ライセンス・プログラムや、他の同様のプログラムの使用を計画している場合は、現行ライブラリーが特に重要になります。次のいずれかのアプローチを使用してください。

- グループ内のすべてのメンバーが共用するライブラリーを作成します。そのグループのすべての Query プログラムとファイルを、そのライブラリーに追加します。ライブラリーにグループ・プロファイルと同じ名前を付け、それをそのグループの現行ライブラリーとして指定します。
- Query の使用を計画している各ユーザーに、個人ライブラリーを与えます。ライブラリーにユーザー・プロファイルと同じ名前を指定します。グループ・プロファイルではなく、グループ・メンバーの個々のプロファイルで、そのライブラリーを現行ライブラリーとして指定します。

ユーザー記述用紙の第 2 部で、サインオンに影響する値のフィールドに、選択した値を記入してください。

サインオンに影響する値を選択したら、ユーザーが実行できる機能を制限する値を選択することができます。

ユーザーが実行できる機能を制限する値の選択

ユーザー・グループ記述用紙の第 2 部で、サインオンに影響する値の記入が完了したら、ユーザーがシステム上で実行できる機能を制限することについて考慮する必要があります。ユーザーが実行できる機能を制限することにはいくつかの理由があります。

- ユーザーが CL コマンドを使用するのを避けるため。ユーザーが何らかの実験をしてみたくなったり、不注意でシステムに損傷を与えてしまったりする恐れがあります。
- ユーザーを特定のアプリケーションや機能に制限するため。
- 不必要な選択項目によってユーザーが混乱しないよう、環境を単純化するため。

ユーザーが実行できる機能は、多くの要素によって決定されます。

- アプリケーション設計
- システム値
- 資源保護
- グループ・プロファイル
- ユーザー・プロファイル
- ジョブ記述

グループまたはユーザー・プロファイルの 2 つのフィールド、「**制限機能**」および「**ユーザー・クラス**」は、ユーザーが決定事項をどの程度一時変更できるのかを判別します。

制限機能

「**制限機能**」フィールドは、**コマンド入力行の使用制限**と呼ばれます。ユーザーがサインオン画面の値の変更、コマンドの入力、およびアテンション・キー処理プログラムの変更を行えるかどうかを制限することができます。制限は、厳重な制限 (*YES)、部分的な制限 (*PARTIAL)、または制限なし (*NO) のいずれかを選択することができます。次の表は、これらのそれぞれの値を選択した場合に実行できる機能を示しています。

表 23. 制限機能の値によって許可される機能

制限機能の値	初期プログラムの変更	初期メニューの変更	現行ライブラリーの変更	重要プログラムの変更	コマンド入力
*YES	不可	不可	不可	不可	部分的に可[1]
*PARTIAL	不可	可	不可	不可	可
*NO	可	可	可	可	可

1 許可されるコマンドは、SIGNOFF、SNDMSG、DSPMSG、DSPJOB、 DSPJOBLOG、および STRPCO です。ユーザーは F9 を使用して、「操作援助機能」メニューまたは画面からコマンド行を表示させることはできません。

ユーザー・クラス

ユーザー・クラスは、**ユーザーのタイプ**とも呼ばれ、操作援助機能メニューとシステム・メニューでユーザーに表示するオプションを決定します。また、「**特殊権限**」フィールドに権限をリストしない場合、ユーザー・クラスは、ユーザーが実行できるシステム機能も決定します。

制限機能およびユーザー・クラスに関する推奨事項

ほとんどのユーザーは、CL コマンドやシステム機能へのアクセスを必要としません。「操作援助機能」の画面では、ユーザーの作業に関連した情報、およびユーザーの作業を制御する情報が十分に提供されます。以下の推奨事項では、作業の完了に必要なシステム資源に対してのみ、ユーザーにアクセスを許可します。

- 各グループ・プロファイルで、「**制限機能**」のフィールドを *YES に設定します。「ユーザー・クラス」フィールドを *USER に設定します。
- システム機能を必要とする個々のユーザーについて、これらの指定を一時変更します。
- ユーザーがアプリケーション間を移動する必要がある場合は、メニューを使用して移動できるようにします。

ユーザー・グループ記述用紙の第 2 部で、ユーザー・クラスと制限機能に対して選択した値を記入したら、ユーザーの環境を設定する値を選択することができます。

ユーザーの環境を設定する値の選択

ユーザー・グループ記述用紙の第 2 部で、ユーザーがシステム上で実行できる機能を制限する値を選択したら、ユーザーの操作環境を決定する値を選択することができます。ユーザー・プロファイルには、ユーザーの操作環境 (使用する印刷装置、メッセージの送信先、ジョブを実行する優先順位) を決定するフィールドがたくさんあります。多くのフィールドでは、デフォルトの設定が推奨されています。続く段落では、いくつかのフィールドについて説明します。

- **ジョブ記述およびジョブ記述ライブラリー**: プロファイル内のこれらのフィールドは、ユーザーがサインオンする際に使用するジョブ記述をシステムに示します。ジョブ記述には、初期ライブラリー・リスト

が含まれています。各ユーザー・グループのジョブ記述は、グループ・プロファイルと同じ名前でなければなりません。ジョブ記述は通常、QGPL ライブラリーに置かれます。

- **印刷装置および出力待ち行列**: ユーザーが作成する印刷装置出力は、特定の印刷ジョブが他の印刷装置に送信するのでない限り、プロファイルにリストされている印刷装置に送られます。通常、ユーザー・グループのメンバーは一緒に配置され、同じ印刷装置を共用します。それで、印刷装置をグループ・プロファイルで指定し、それを各個人のユーザー・プロファイルにコピーすることができます。ユーザーの印刷装置は、**省略時の印刷装置**とも呼ばれます。

  出力待ち行列には、印刷される前の印刷装置出力が含まれます。通常、各印刷装置には、同じ名前を持つ固有の出力待ち行列があります。出力待ち行列のフィールドに *DEV を指定すると、その印刷装置の出力待ち行列を使用するようシステムに指示することができます。

  ユーザー・グループ記述用紙に、ジョブ記述とそのライブラリーの名前、および省略時の印刷装置と出力待ち行列のフィールドを入力してください。
- **「操作援助機能」インターフェースの設定**: このシステムの「操作援助機能」メニューは、システムが出荷される時点で、すべてのユーザー対応のアテンション・キー処理プログラムになっています。ユーザーがアテンション・キーを押すと、「操作援助機能 (ASSIST)」メニューが表示されます。ご使用のアプリケーション・プログラムが、すでに他のアテンション・キー処理プログラムを使用している場合は、別の方法でユーザーが「操作援助機能」メニューを表示できるようにする必要があります。
  - GO ASSIST か CALL QEZAST を使用して、メインのアプリケーションのメニューから、オプションとして「操作援助機能」メニューを追加します。
  - ユーザーに、コマンド行から GO ASSIST と入力してもらいます。

ユーザー・プロファイルの「**機能の制限**」フィールドが *YES に設定されている場合、ユーザーは GO コマンドを使用してメニューを表示することができません。操作援助機能のユーザーが ASSIST メニューにアクセスするための方法を設定する必要があります。

JKL Toy Company の Sharon Jones がユーザー・グループ記述用紙で選択した値を、例から検討することができます。

これらの計画のステップを完了するには、次のようにします。

- 社内の各ユーザー・グループについて、ユーザー・グループ記述用紙を完成します。
- 命名規則用紙で、ユーザー・グループの命名方法について記述を作成します。
- ユーザー・グループをアプリケーション図とライブラリーに追加します。

これらの作業を完了したら、個々のユーザー・プロファイルの計画を開始することができます。

例: JKL Toy Company のユーザー・グループ記述用紙 -- 第 2 部: Sharon Jones は、販売マーケティングの担当者に対してユーザー・グループ記述用紙を作成した際に、販売マーケティング部門と倉庫部門について次のようなメモを作成しました。

- 販売マーケティングの担当者は、IBM Query for iSeries を頻繁に使用する。そのため、個々のユーザーは専用ライブラリーを持つ必要がある。倉庫部門には、グループ・ライブラリーを 1 つ与える。
- 返送所で作業する倉庫部門の担当者には、初期メニューの代わりに初期プログラムが必要である。

Sharon は、これら 2 つの部門について、ユーザー・グループ記述用紙の第 2 部を作成しました。

表 24. JKL Toy Company のユーザー・グループ記述用紙: 販売マーケティング部門の例

フィールド名	推奨値	選択可能な値
グループ・プロファイル名 (ユーザー)		DSTSM
パスワード	*NONE	*NONE
ユーザー・クラス (ユーザーのタイプ)	*USER	*USER
現行ライブラリー (省略時のライブラリー)	*グループ・プロファイル名と同じ*	(グループ・プロファイルの場合はブランクにしておき、個々のユーザー・プロファイルの場合は記入する)
呼び出す初期プログラム (サインオン・プログラム)		
初期プログラム・ライブラリー		
初期メニュー (第 1 メニュー)		CPMAIN
初期メニュー・ライブラリー		CPMAINLIB
制限機能 (コマンド行の使用の制限)	*YES	*PARTIAL
テキスト (ユーザー記述)		販売マーケティング
ジョブ記述	*グループ・プロファイル名と同じ*	DPTSM
ジョブ記述ライブラリー		QGPL
グループ・プロファイル名 (ユーザー・グループ)	*NONE[1]	*NONE
印刷装置 (省略時の印刷装置)		PRT03
出力待ち行列	*DEV	*DEV

表 25. JKL Toy Company のユーザー・グループ記述用紙: 倉庫部門の例

フィールド名	推奨値	選択可能な値
グループ・プロファイル名 (ユーザー)		DPTWH
パスワード	*NONE	*NONE
ユーザー・クラス (ユーザーのタイプ)	*USER	*USER
特殊環境		
現行ライブラリー (省略時のライブラリー)	*グループ・プロファイル名と同じ*	DPTWH
呼び出す初期プログラム (サインオン・プログラム)		
初期プログラム・ライブラリー		
初期メニュー (第 1 メニュー)		ICMAIN
初期メニュー・ライブラリー		ICPGMLIB
制限機能 (コマンド行の使用の制限)	*YES	*YES
テキスト (ユーザー記述)		倉庫部門
ジョブ記述	*グループ・プロファイル名と同じ*	DPTWH
ジョブ記述ライブラリー		QGPL

表 25. JKL Toy Company のユーザー・グループ記述用紙: 倉庫部門の例 (続き)

フィールド名	推奨値	選択可能な値
グループ・プロファイル名 (ユーザー・グループ)	*NONE[1]	*NONE
印刷装置 (省略時の印刷装置)		PRT04
出力待ち行列	*DEV	*DEV

1 グループ・プロファイルの場合は、グループ・プロファイル名を必ず *NONE にしてください。グループ・プロファイルを、他のグループのメンバーにすることはできません。

続いて、個々のユーザー・プロファイルの計画を開始することができます。

個々のユーザー・プロファイルの計画

これまでの部分では、全体的なセキュリティー戦略を決定し、ユーザー・グループを計画しました。次に、個々のユーザー・プロファイルを計画することができます。

どのような用紙が必要か

個々のユーザー・プロファイルを計画するには、以下の用紙を使用します。

- 個別ユーザー・プロファイル用紙
- システム責任用紙

加えて、完成している以下の用紙の情報が必要です。

- ユーザー・グループ定義用紙
- 命名規則用紙
- アプリケーション図

ユーザー・プロファイルの命名

システムは、ユーザー・プロファイル名によってユーザーを識別します。ユーザーは、サインオン画面の「**ユーザー ID**」フィールドに、自分のユーザー・プロファイル名を入力します。ユーザーが行うすべての作業、およびユーザーが作成するすべての印刷装置出力は、ユーザーのユーザー・プロファイル名と関連付けられます。

ユーザー・プロファイルに名前を付ける際は、以下の点を考慮してください。

- ユーザー・プロファイル名は最大 10 文字までです。一部の通信方式では、ユーザー ID を 8 文字までに制限しています。
- ユーザー・プロファイル名には、文字、数字、およびいくつかの特殊文字 (ポンド (#)、ドル ($)、円 (¥)、下線 (_)、およびアットマーク (@)) を使用することができます。名前の先頭に数字や下線 (_) を使用することはできません。
- システムでは、ユーザー・プロファイル名の大文字と小文字の区別はされません。英小文字を入力すると、システムはそれらの文字を大文字に変換します。
- ユーザー・プロファイル名を管理するために使用する画面とリストでは、ユーザー・プロファイル名をアルファベット順で示します。
- IBM 提供のプロファイルにはすべて、名前の先頭に Q が付きます。ユーザーのプロファイルと IBM 提供のプロファイルを区別するため、ユーザー・プロファイル名には、Q で始まる名前を使用しないでください。

推奨事項

ユーザー・プロファイル名を割り当てる 1 つの技法として、名字の先頭から 7 文字までと名前の先頭 1 文字を使用する方法があります。 Sharon は、JKL Toy Company のユーザー・プロファイルに対して、次のような命名規則を使用しました。

表 26. JKL Toy Company の命名規則用紙: ユーザー・プロファイルの例

ユーザー名	ユーザー・プロファイル名
Anderson、George	ANDERSOG
Anderson、Roger	ANDERSOR
Jones、Sharon	JONESS

この方法を使用すれば、ユーザー・プロファイル名を覚えやすくなります。また、リストや画面にプロファイルを表示する場合にも、ユーザーの名字のアルファベット順で表示することができます。

例として、JKL Toy Company の Sharon Jones は、この技法を使用してプロファイルを命名する計画を立てました。彼女は、命名規則用紙の適当な箇所に選択した内容を追加しました。

表 27. JKL Toy Company の命名規則用紙: ユーザー・プロファイルの例

オブジェクトのタイプ	命名規則
ユーザー・プロファイル	名字の先頭から 7 文字までと名前の先頭 1 文字を使用する。ユーザー・プロファイルの説明の項には、名字、名前の順に示す。

命名規則用紙に、計画しているユーザー・プロファイルの命名規則を記述したら、システム機能の責任者の決定、および個々のユーザーの値の選択を行うことができます。

システム機能の責任者の決定

個々のユーザー・プロファイルを計画するにあたって、まず初めにシステムにおける個々の責任を決定する必要があります。システム操作の能率性を保つには、システム機能のさまざまな管理と保守を定常的に行う人が必要になります。またその場合、これらの作業を行う人々には、コマンドを発行し、そのシステム機能を実行する権限が必要になります。

『ユーザーが実行できる機能を制限する値の選択』では、「**ユーザー・クラス**」および「**制限機能**」フィールドを使用して、ユーザーがアクセスできるシステム機能を制御する方法を説明しています。通常、ほとんどのユーザーに対してはシステム機能の実行を許可しません (ユーザー・クラスには *USER を、制限機能には *PARTIAL か *YES を指定します)。しかし、一部のユーザーには、システム操作の能率性を保つために付加的な権限が必要です。

下の表は、重要なシステム管理タスクの一部をリストしたものです。また、それらの責任を持つ人々に割り当てることができる、ユーザー・クラスと特殊権限についても示しています。このリストは、システム上で特殊権限を必要とするユーザーを決定する際に利用することができます。ただしこれは、システム操作および保守のための、完全な計画のツールとして用意されているものではありません。この表に示されているユーザー・クラスと特殊権限は、ほとんどのシステムで使用することができますが、ご使用のシステムによっては、別の権限を割り当てなければならない場合もあります。

プロファイルのユーザー・クラスに *USER 以外の値を割り当てておくと、ユーザーは、システム機能を実行するための特殊権限の特定のセットを自動的に受け取ります。「ユーザー・クラス」フィールドで指定していない特殊権限をユーザーに割り当てることもできますが、これは必ずしも必要ではありません。

表 28. システム責任、ユーザー・クラス、および特殊権限

システム機能[1]	説明	必要なユーザー・クラス[2]	必要な特殊権限[3]
システム操作	印刷装置出力の管理、システム・メッセージへの応答、通常の操作の監視、初期プログラム・ロード (IPL) の実行。	*SYSOPR	*JOBCTL
システム・ハウスキーピング	自動クリーンアップのスケジュール作成や、ディスク使用率の監視などのシステム・ハウスキーピング機能の実行。	*SYSOPR	*JOBCTL
システム・バックアップ	アプリケーション・ライブラリー、システム・ライブラリー、およびセキュリティー情報の定期的な保管。これらの機能についての詳細は、Information Center の『バックアップおよび回復』のトピックを参照してください。	*SYSOPR	*SAVSYS
プロファイル管理	新規ユーザー・プロファイルの追加、既存プロファイルの保守。	*SECADM	*SECADM
資源保護管理	システム上のオブジェクトに対する権限の保守。	*SECOFR	*ALLOBJ
プログラム保守	IBM 提供のライブラリーに対する定期的なプログラムの変更 (PTF) の適用。アプリケーション・ライブラリーの変更。	*SECOFR	*ALLOBJ
セキュリティー監査	セキュリティー監査機能の設定。監査の対象となるイベント、ユーザー、およびオブジェクトの決定。		*AUDIT[4]
システム構成	システムにおける装置の追加、変更、および除去。		*IOSYSCFG[5]

1 これらの責任を割り当てるユーザーについては、「制限機能」フィールドを *NO に設定してください。

2 これは、最低限必要なユーザー・クラスを示しています。このユーザー・クラスには、機能の実行に必要なコマンドやメニュー・オプションを使用するための権限が含まれています。ご使用の資源保護によっては、さらに別の権限が必要になる場合もあります。

3 これは、ジョブの責任を果たすために必要な特定の特殊権限を示しています。指定されているユーザー・クラスには、他の付加的な特殊権限が含まれている場合もあります。

4 *AUDIT 特殊権限には、対応するユーザー・クラスがありません。 *SECOFR ユーザー・クラスには、*AUDIT 特殊権限が含まれていますが、監査を行うユーザーには、おそらく *SECOFR ユーザー・クラスに含まれている他の機能は必要ないでしょう。それで、システムでの監査を制御する必要のあるユーザーには、個別に *AUDIT 特殊権限を指定してください。

5 *IOSYSCFG 特殊権限には、対応するユーザー・クラスがありません。 *SECOFR ユーザー・クラスには、*IOSYSCFG 特殊権限が含まれていますが、システムを構成する必要のあるユーザーだけに、*IOSYSCFG 特殊権限を個別に指定するようお勧めします。この特殊権限があれば、個々のユーザーは回線の作成、制御装置および装置の作成、または TCP/IP の構成を行うことができますが、システムの構成を行うユーザーに、*SECOFR ユーザー・クラスのその他の機能は必要ないからです。

推奨事項

上の表を使用して、システム機能を実行するユーザーを計画してください。最低でも、システムのセキュリティーを管理するユーザーを 2 人、さらに操作とバックアップを管理するユーザーを 2 人割り当ててください。

システムを保守および監査するためのツールとして、システム責任用紙を使用してください。システム上で特殊権限を与えられているすべてのユーザーと、それらのユーザーに特殊権限が必要な理由を明確にしておいてください。

個々のユーザーの値を選択する前に、Sharon Jones がユーザーの責任を決定した方法の例を検討することができます。

例: JKL Toy Company のシステム責任用紙: 次の例は、Sharon Jones が完成させたシステム責任用紙を示しています。

表 29. JKL Toy Company のシステム責任用紙: 例

セキュリティーの第 1 責任者: Sharon Jones 補佐の機密保護担当者: Ken Harrison			
プロファイル名	ユーザー名	クラス	コメント
JONESS	Sharon Jones	*SECOFR	Sharon は、セキュリティーの第 1 責任者であり、システム・マネージャーである。
HARRISOK	Ken Harrison	*SECOFR	Ken は、全体のシステム・マネージャーとして、Sharon をサポートする。
JOHNSONS	Sandy Johnson	*SYSOPR	Sandy は、システム操作とバックアップの第 1 責任者である。
ROGERSK	Karen Rogers	*SYSOPR	Karen は、システムの操作とバックアップにおいて、Sandy をサポートする。
WILLISR	Rose Willis	*SYSOPR	Rose は、第 2 シフトの勤務時間にシステム操作を担当する。

システム責任用紙を完成したら、個々のユーザーの値の選択を開始することができます。

個々のユーザーの値の選択

システム上のユーザーの責任を決定したら、個々のユーザーの値を選択することができます。個々のユーザー・プロファイル用のパターンとしてグループ・プロファイルの計画を立てることにより、大部分の作業は終了しています。個別ユーザー・プロファイル用紙を使用して、個々のユーザーを正しいグループに割り当て、グループ内のユーザー同士の相違点を定義します。まず 1 つのユーザー・グループの個別ユーザー・プロファイル用紙を例として完成させ、元に戻って、それ以外のユーザー・グループについて個別ユーザー・プロファイル用紙を作成してください。

個別ユーザー・プロファイル用紙の上部に、グループ・プロファイル名と他の記述情報を記入します。

例: JKL Toy Company の個別ユーザー・プロファイル用紙の記述情報

Sharon Jones が個別ユーザー・プロファイル用紙の上部に記入した内容を以下に示します。

表 30. JKL Toy Company の個別ユーザー・プロファイル用紙: 記述情報の例

個別ユーザー・プロファイル用紙	
作成者: Sharon Jones	日付: 9/5/99
グループ・プロファイル名: DPTOP	
作成したオブジェクトの所有者:	作成されたオブジェクトに対するグループ権限:
グループ権限タイプ:	

グループ・メンバーの値の決定

個別ユーザー・プロファイル用紙に、プロファイル名とグループの各メンバーの説明 (ユーザー名) を記入します。個々のグループ・メンバーのその他の値を決定する方法について以下で説明します。

グループ・プロファイルは、個別ユーザー・プロファイルのパターンになることに注意してください。個別ユーザー・プロファイル用紙には、グループとは異なる事柄だけを指定する必要があります。

- **パスワードの割り当て**: 初期パスワードをユーザーに割り当てる最も簡単な方法は、プロファイル名と同じパスワードにすることです。次に、パスワードを満了に設定して、初めてユーザーがサインオンする際にパスワードを変更しなければならないようにすることができます。『パスワードの期限満了の設定』には、グループ・プロファイルをコピーする際にこの設定を自動的に行う方法が示されています。この方法で作業を行う場合は、個別ユーザー・プロファイル用紙にパスワードをリストする必要はありません。
- **ユーザー・クラスおよび制限機能**: システム責任用紙を見て、個々のグループについて、「**ユーザー・クラス**」フィールドと「**制限機能**」フィールドに別の値を指定する必要のあるメンバーを判別してください。グループ・プロファイルの値とは違う値を指定する必要のあるメンバーについて、個別ユーザー・プロファイル用紙に該当する情報を記入します。
- **その他の値の指定**: 特定のユーザーが、ユーザー・グループ記述用紙に指定されたグループの値とは異なる値を必要としているかどうか調べてください。グループのメンバーによっては、「**ユーザー・クラス**」フィールドと「**制限機能**」フィールドの値が異なる場合が多いため、これらのフィールドはユーザー・グループ記述用紙の上部にリストされます。それ以外のフィールドで、作業中のグループのメンバーの値が異なるものがあれば、リストしてください。

この計画ステップを終了する前に、以下のことを必ず行ってください。

- システム値選択用紙を完成させる。
- 命名規則用紙に、ユーザー・プロファイルの命名計画を記述する。
- お客様の会社のユーザー・グループごとに個別ユーザー・プロファイル用紙を作成する。

Sharon が使用している個々のユーザー情報の例を検討してから、資源保護の計画を立てることもできます。

例: JKL Toy Company の個別ユーザー・プロファイル用紙: JKL Toy Company では、発送所で働くユーザーは、プログラムを 1 つだけ実行できます。彼らが作業しているエリアでは一般の人々が簡単にワークステーションにアクセスできるため、Sharon は彼らが使用できる機能を数個に限定しています。倉庫部門のメンバーには初期プログラムはありますが、初期メニューはありません。注文処理部門では、離れた場所にある営業所にローカル印刷装置が 2 台と、印刷装置が 1 台あります。したがって、Sharon は一部のユーザーに、グループのものとは異なる印刷装置を割り当てています。

以下は、Sharon Jones が完成させた、JKL Toy Company の倉庫部門と注文処理部門の個別ユーザー・プロファイル用紙です。グループ・プロファイルで設定された値と異なるフィールドだけ記入されていることに注意してください。

表 31. JKL Toy Company の個別ユーザー・プロファイル用紙: 倉庫部門の例

グループ・プロファイル名: DPTWH					
グループのメンバーごとに項目を作成します。					
ユーザー・プロファイル	**テキスト (説明)**	**ユーザー・クラス**	**制限機能**	**初期プログラム / ライブラリー**	**初期メニュー / ライブラリー**
WILLISR	Willis, Rose	*SYSOPR	*NO		

表 31. JKL Toy Company の個別ユーザー・プロファイル用紙: 倉庫部門の例 (続き)

WAGNERR	Wagner, Ray			ICRCPT/ICPGMLIB	なし
AMESJ	Ames, Janice			ICRCPT/ICPGMLIB	なし
FOSSJ	Foss, Julie				
WOODBURC	Woodburt, Carol				

表 32. 個別ユーザー・プロファイル用紙: 注文部門の例

グループ・プロファイル名: DPTOP				
グループのメンバーごとに項目を作成します。				
ユーザー・プロファイル	**テキスト (説明)**	**ユーザー・クラス**	**制限機能**	**印刷装置**
HARRISOK	Harrison, Ken	*SECOFR	*NO	PRT05
RICHARDK	Richards, Karen			
UNGERJ	Unger, Jeff			PRT04
BELLB	Bell, Brad			PRT04

次に、資源保護の計画を始めることができます。

資源保護の計画

これで、システム上のユーザーの計画プロセスが完了したので、システム上のオブジェクトを保護するための資源保護の計画を立てることができます。『資源保護の設定』では、システム上で資源保護を設定する方法について説明されています。

システム値とユーザー・プロファイルでは、システムにアクセスするユーザーを制御し、許可のないユーザーがサインオンできないようにします。資源保護により、許可されたシステム・ユーザーが正常にサインオンした後に実行できるアクションが制御されます。資源保護では、システム上でのセキュリティーの主要な目標として、以下のものを保護するためのサポートが備えられています。

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

資源保護の計画は、お客様の会社でアプリケーションを開発したか、購入したかによって異なる場合があります。アプリケーションを開発する場合は、アプリケーションの設計時に、情報のセキュリティー要件についてプログラマーと話し合う必要があります。アプリケーションを購入する場合は、計画したいセキュリティーの必要性を判別し、それをアプリケーションの提供者が設計した方法に合わせる必要があります。以下に説明されている手法は、どちらの事例にも役立つはずです。

このトピックでは、資源保護の計画に関する基本的なアプローチについて説明します。主要な手法を紹介し、その使用方法を示します。以下に説明されている方式は、必ずしもすべての会社のすべてのアプリケーションに当てはまるとは限りません。資源保護の計画を立てる際には、プログラマーかアプリケーションの提供者と相談してください。

資源保護を計画する上で、次のトピックを検討してください。

- 資源保護の目的の決定
- 権限のタイプの理解

- アプリケーション・ライブラリーのセキュリティーの計画
- ライブラリーとオブジェクトの所有権の決定
- オブジェクトのグループ化
- 印刷装置出力の保護
- ワークステーションの保護
- 資源保護に関する推奨事項の要約
- アプリケーションの導入の計画

どのような用紙が必要か

このトピックを読みながら、以下の用紙のコピーを取って、そこに記入してください。 1 つのアプリケーションについてすべての作業を行ってから、その他のアプリケーションごとに同様の作業を繰り返してください。

表 33. 資源保護の計画に必要な計画用紙

用紙名	必要なコピーの部数
権限リスト用紙	複数
印刷装置出力およびワークステーションのセキュリティー用紙	1 部

以前に作成した以下の用紙に情報を追加してください。

表 34. 変更される計画用紙

用紙名	作成内容
ライブラリー記述用紙	ライブラリー情報の記述
ユーザー・グループ記述用紙	グループ・プロファイルの計画

以前に作成した以下の用紙を参照してください。

表 35. 資源保護を完了させるために必要な計画用紙

用紙名	作成内容
ライブラリー記述用紙	アプリケーション図の描画とユーザー・グループの識別
アプリケーション記述用紙	アプリケーション情報の記述
個別ユーザー・プロファイル用紙	個々のユーザーの値の選択
ユーザー・グループ識別用紙	ユーザー・グループの識別
システム責任用紙	システム機能の責任者の決定
物理的セキュリティー計画用紙	物理的セキュリティーの計画

資源保護の目的の決定

資源保護の計画を始めるには、まず最初に資源保護の目的について理解していなければなりません。 iSeries では柔軟な資源保護を実現しています。重要な資源を希望どおりに保護する機能が備えられています。しかし、資源保護により、ご使用のアプリケーションのオーバーヘッドも増加します。たとえば、あるオブジェクトがアプリケーションで必要になる場合、そのつどシステムはそのオブジェクトに対するユーザ

ー権限を検査する必要があります。機密性の必要を満たすこととコスト・パフォーマンスの間で平衡を取らなければなりません。資源保護について決定する際には、セキュリティーの価値とコストを比較考慮してください。

資源保護のためにご使用のアプリケーションのパフォーマンスが低下しないようにするには、以下の指針に従ってください。

- 資源保護の体系を単純にしておく。
- 保護する必要のあるオブジェクトだけを保護する。
- 情報を保護するための他のツールの代わりとしてではなく、補足するものとして、次のように資源保護を使用する。
  - ユーザーを特定のメニューとアプリケーションに制限する。
  - ユーザーがコマンドを入力できないようにする (ユーザー・プロファイルの制限機能)。

資源保護の計画は、目的を定義することから始めてください。セキュリティーの目的は、アプリケーション記述用紙かライブラリー記述用紙のどちらかで定義することができます。

使用する用紙は、ライブラリーで情報をどのように編成しているかによって決まります。

最初に、JKL Toy Company のセキュリティーの目的の例を検討してから、資源保護に使用できる権限のタイプを検討することもできます。

例: JKL Toy Company のセキュリティーの目的

JKL Toy Company の Sharon Jones は、ライブラリー記述用紙を使用して、顧客レコード・ライブラリー (CUSTLIB) のセキュリティー要件を記述しています。

表 36. JKL Toy Company のライブラリー記述用紙: セキュリティーの目的の例

ライブラリー記述用紙	1 / 2
ライブラリーに対するセキュリティーの目的の定義 (機密情報を含んでいるかどうかなど):	現在、当社の全社員が顧客情報と顧客注文を見ることができる。情報の正確度を保護するために、変更を加えることができる社員を制御する必要がある。

契約および価格アプリケーションについては、アプリケーション記述用紙を使用して、アプリケーション全体のセキュリティーの目的を記述しています。

表 37. JKL Toy Company のアプリケーション記述用紙: セキュリティーの目的の例

アプリケーション記述用紙	1 / 2
ライブラリーに対するセキュリティーの目的の定義 (機密情報を含んでいるかどうかなど):	契約と特別価格に関する情報は機密にする。この情報を見たり、変更したりできる人物は数人に限る。 • 販売マーケティング部門の担当者と管理者の全員は、契約の作成、変更、および分析を行う必要がある。彼らは、ファイルとプログラムを両方とも使用する必要がある。 • 注文処理部門の担当者は、注文の入力時と出荷時に、間接的に契約に変更を加え価格を表示する。注文の入力時か変更時以外に契約や価格を参照することは許可されていない。

ご使用のアプリケーションのセキュリティーの目的を、アプリケーション記述用紙かライブラリー記述用紙のどちらかに記入します。次に、資源保護の計画を立てる際に使用できる権限のタイプについて検討します。

権限のタイプの理解

資源保護の目的の決定を終え、決定事項をライブラリー記述用紙に記録したら、権限のタイプの計画を立てることができます。資源保護により、ユーザーがシステム上のオブジェクトにどのようにアクセスするかが定義されます。

権限とは、特定のユーザーに与えられているオブジェクトの使用許可のことです。たとえば、システム上の情報を表示したり変更したりする権限があります。システムには数種類の権限タイプがあります。 IBM では、これらの権限タイプを **システム定義の権限**というカテゴリーにグループ化しています。これは大多数の人々の必要に合ったものです。以下の表に、これらのカテゴリーのリストと、それらがどのようにファイルとプログラムの保護に適用されるかが示されています。

注: 権限の計画を立てる際には以下の表を参照してください。

表 38. システム定義の権限

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

オブジェクト権限とライブラリー権限が協働する仕方についての理解

単純な資源保護を設計するには、ライブラリー全体のセキュリティーの計画を立ててください。そのためには、システム定義の権限がライブラリーに適用される方法について理解する必要があります。以下の表に、その点が示されています。

表 39. ライブラリーに関するシステム定義の権限

権限名	許可されている操作	許可されていない操作
*USE	• ライブラリー内のオブジェクトの場合、権限によって許可されている、特定のオブジェクトに対するすべての操作。 • ライブラリーの場合、記述情報の表示。	• ライブラリーへの新規オブジェクトの追加。 • ライブラリー記述の変更。 • ライブラリーの削除。
*CHANGE	• ライブラリー内のオブジェクトの場合、権限によって許可されている、特定のオブジェクトに対するすべての操作。 • ライブラリーへの新規オブジェクトの追加。 • ライブラリー記述の変更。	• ライブラリーの削除。
*ALL	• 変更操作によって行えるすべての処理。 • ライブラリーの削除。 • 他人のライブラリーに対する権限。	• なし

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

表 40. ライブラリー権限とオブジェクト権限が協働する仕方

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

ディレクトリー権限はライブラリー権限に似ています。オブジェクトにアクセスするには、オブジェクトのパス内のすべてのディレクトリーに対する権限が必要です。

これで、アプリケーション・ライブラリーのセキュリティーの計画を立てる準備が完了しました。

アプリケーション・ライブラリーのセキュリティーの計画

資源保護の目的の決定を終えたら、アプリケーション・ライブラリーのセキュリティーの計画を立てることができます。アプリケーション・ライブラリーの 1 つを選択し、以下に説明されているプロセスに従って作業してください。ファイルとプログラムが別々のライブラリーに保管されている場合は、ファイルを含むライブラリーを選択します。このトピックを終えたら、残りのアプリケーション・ライブラリーにも同じステップを繰り返してください。

ご使用のアプリケーションとライブラリーについて収集した以下の情報を検討してください。

- アプリケーション記述用紙
- ライブラリー記述用紙
- ライブラリーが必要なグループの場合、ユーザー・グループ記述用紙
- アプリケーション、ライブラリー、およびユーザー・グループの図

ライブラリー内の情報を必要とするグループ、必要な理由、およびその情報を使用して行う事柄を考慮します。

ライブラリーの内容の決定

アプリケーション・ライブラリーには、重要なアプリケーション・ファイルが含まれています。またその他のオブジェクトも含まれていることがありますが、その大部分はアプリケーションを適切に稼働させるためのプログラミング・ツールです。次のようなものがあります。

- 作業ファイル
- データ域およびメッセージ待ち行列
- プログラム
- メッセージ・ファイル
- コマンド
- 出力待ち行列

ファイルおよび出力待ち行列以外の大部分のオブジェクトは、セキュリティー上の危険を伴うものではありません。これらのオブジェクトには通常、少量のアプリケーション・データが含まれており、多くの場合、プログラムの外側では容易に識別できない形式になっています。ライブラリー表示コマンドを使用して、ライブラリーにあるすべてのオブジェクトの名前と説明をリストできます。たとえば、CONTRACTS ライブラリーの内容をリストするには、`DSPLIB LIB(CONTRACTS) OUTPUT(*PRINT)` を発行します。

次に、アプリケーション・ライブラリーとプログラム・ライブラリーについて、必要な共通権限のタイプを決める必要があります。

アプリケーション・ライブラリーに対する共通権限の決定

資源保護の場合、**共通 (public)** とは、誰にでもシステムへのサインオンを認可することを意味します。**共通権限**があると、ユーザーは、他の特定のアクセス権がなくてもオブジェクトにアクセスできます。ライブラリーにある既存のオブジェクトへの共通権限を決定することに加えて、後でライブラリーに追加される新規オブジェクトへの共通権限も指定することができます。それには、**作成権限 (CRTAUT)** パラメーターを使用します。通常は、ライブラリー・オブジェクトに対する共通権限と、新規オブジェクトについてのライブラリー作成権限は同じにしてください。

QCRTAUT (作成権限) システム値により、新規オブジェクトのシステム・レベルの共通権限が決まります。 IBM では、出荷時に QCRTAUT システム値に *CHANGE を指定します。 QCRTAUT は多数のシステム機能で変更されるので、この値を変更しないでください。アプリケーション・ライブラリーの作成権限 (CRTAUT) に *SYSVAL を指定すると、 QCRTAUT システム値 (*CHANGE) が使用されます。

作業を単純にし、パフォーマンスを良くするために、できるだけたくさんの共通権限を使用してください。ライブラリーに対する共通権限のタイプを決めるには、以下の質問について検討してください。

- このライブラリーにある大部分の情報に対するアクセス権を、全社員に与える必要があるか。
- このライブラリーにある大部分の情報に対して、どのタイプのアクセス権を与える必要があるか。

大多数のユーザーと大部分の情報に関する決定を綿密に検討してください。後で、例外を扱う方法について説明します。資源保護の計画は、循環的なプロセスになることがよくあります。特定のオブジェクトに関する要件を考慮した後で、共通権限に変更を加えなければならないことがあります。まずオブジェクトとライブラリーの両方に対していくつかの共通権限と私用権限の組み合わせを試行し、その中からセキュリティーとパフォーマンスの必要に合ったものを選択してください。

適切な権限の確認

大部分のアプリケーション機能にとっては、オブジェクトに対する適切な権限は *CHANGE、ライブラリーに対する適切な権限は *USE です。しかし、プログラマーかアプリケーションの提供者に次のような質問をして、特定のアプリケーション機能では権限がさらに必要になるかどうか判別する必要があります。

- 処理中にライブラリーにあるファイルまたは他のオブジェクトを削除するかどうか。すべてのファイルを消去するかどうか。すべてのファイルにメンバーを追加するかどうか。オブジェクトの削除、ファイルの消去、またはファイル・メンバーの追加を行うには、オブジェクトに対する *ALL 権限が必要です。
- 処理中にライブラリーにファイルまたは他のオブジェクトを作成するかどうか。オブジェクトを作成するには、ライブラリーに対する *CHANGE 権限が必要です。

まず Sharon がオブジェクトに対する権限について行った選択の例を検討してから、プログラム・ライブラリーに対する共通権限の決定を行うことができます。

例: JKL Toy Company のライブラリー記述用紙:

Sharon Jones は、顧客レコード・ライブラリーと、顧客情報を使用するアプリケーションと部門に関する情報について、セキュリティーの目的を検討しています。その決定に関して以下のメモを作成しました。

- 倉庫部門と製造部門を除くすべての部門で、顧客情報に変更を加える必要がある。
- 倉庫部門と製造部門のすべてのユーザーには、制限機能を (Yes) に指定したユーザー・プロファイルがあり、特定のメニューまたはプログラムだけに制限されている。これらのメニューを使用して顧客情報を表示できるが、変更を加えることはできない。
- 顧客レコード・ライブラリーにあるオブジェクトの共通権限を *CHANGE に設定できる。メニュー制限により、許可のないユーザーが顧客情報に変更を加えられないようになっている。しかし、後に他の部門をシステムに追加する場合は、この設定を再評価する必要がある。

この例は、情報に対して寛容なアプローチをとっています。その場合、例外の処理は、権限の制限によるのではなく、ユーザー・プロファイルを使用して扱われます。 Sharon は、顧客レコード・ライブラリー (CUSTLIB) のライブラリー記述用紙の共通権限の部分に、次のように記入しました。

表 41. JKL Toy Company のライブラリー記述用紙 -- 第 1 部: 顧客レコードの例

ライブラリー名: CUSTLIB	記述名 (テキスト): 顧客レコード
ライブラリーへの共通権限:	*USE
ライブラリー内のオブジェクトへの共通権限:	*CHANGE
新しいオブジェクト (CRTAUT) への共通権限:	*CHANGE

Sharon Jones は、売掛管理アプリケーションの月末処理において、顧客レコード・ライブラリーにある一時ファイルの一部が消去されることに気付きました。そこで、これらのファイルに関する権限を個別に処理することにより、ライブラリー中の他のオブジェクトが不慮に削除されるリスクを避けることを選択しました。それ以外の処理活動には、*CHANGE 権限で十分です。

Sharon は、月末処理を実行する人が 2、3 人しかいないとしても、一時ファイルのセキュリティーは犯されないと判断しました。そこで、月末処理を実行する人だけに *ALL 権限を付与するのではなく、これらのファイルに対する *ALL の共通権限を付与することに決めました。以下の表は、顧客レコード・ライブラリーのライブラリー記述用紙の第 2 部を示しています。

表 42. JKL Toy Company のライブラリー記述用紙 -- 第 2 部: 顧客レコードの例

ライブラリー・オブジェクトの特定権限のリスト				
グループ・プロファイルまたはユーザー・プロファイル	オブジェクト名	オブジェクト・タイプ	必要な権限	権限リスト
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

次に、必要なプログラム・ライブラリーに対する共通権限の決定を行えます。

プログラム・ライブラリーに対する共通権限の決定

アプリケーション・プログラムが、ファイルや他のオブジェクトとは別のライブラリーに保持されることがよくあります。アプリケーション用に別のライブラリーを使用する必要はありませんが、大勢のプログラマーがアプリケーション設計時にこの手法を使用します。アプリケーション用に別のプログラム・ライブラリーを使用する場合は、これらのライブラリーに対する共通権限を決定する必要があります。ライブラリーとライブラリーにあるプログラムの両方に *USE 権限を使用すると、プログラムを十分に実行できますが、プログラム・ライブラリーには、追加権限が必要な他のオブジェクトも含まれている場合があります。プログラマーに以下の 2、3 の質問をしてください。

- プログラム間の通信のためにアプリケーションがデータ域またはメッセージ待ち行列を使用するかどうか。これらのものがプログラム・ライブラリーにあるかどうか。データ域やメッセージ待ち行列を処理するには、そのオブジェクトに対する *CHANGE 権限が必要です。
- 処理中に削除されるオブジェクト (データ域など) がプログラム・ライブラリーにあるかどうか。オブジェクトを削除するには、そのオブジェクトに対する *ALL 権限が必要です。
- 処理中に作成されるオブジェクト (データ域など) がプログラム・ライブラリーにあるかどうか。ライブラリー中に新規のオブジェクトを作成するには、そのライブラリーに対する *CHANGE 権限が必要です。

ライブラリー記述用紙の第 1 部と第 2 部の、ライブラリー所有者と権限リストの列を除くすべての箇所に、資源保護情報を記入してください。その後で、ライブラリーとオブジェクトの所有権の決定を行えます。

以下の 2 つの例は、Sharon Jones がプログラム・ライブラリーに対する権限を決定したものですが、これらの例を検討することもできます。最初の例で、Sharon は、顧客注文プログラム・ライブラリーに制限を加えない方がよいと決定しました。2 番目の例は、Sharon が売掛管理プログラム・ライブラリーには制約を加えたことを示しています。

例: JKL Toy Company のライブラリー記述用紙 -- 制限のないアプローチ: Sharon Jones は、顧客注文プログラム・ライブラリーを調べて、以下のメモを作成しました。

- プログラム間の通信には、1 つのメッセージ待ち行列 COMSGQ01 を使用する。
- このメッセージ待ち行列は消去されるが、削除されることはない。このメッセージ待ち行列に対して *CHANGE 権限が付与される。

Sharon は、プログラム・ライブラリーにあるすべてのオブジェクトに対する *USE 権限を付与し、COMSGQ01 メッセージ待ち行列を別個に定義することに決めました。以下の 2 つの表は、COPGMLIB ライブラリーのライブラリー記述用紙を示しています。

表 43. JKL Toy Company のライブラリー記述用紙: プログラム・ライブラリーの例

ライブラリー記述用紙		**1 / 2**
ライブラリー名: COPGMLIB	記述名 (テキスト): 顧客注文プログラム・ライブラリー	
ライブラリーへの共通権限: *USE ライブラリー内のオブジェクトへの共通権限: *USE 新しいオブジェクト (CRTAUT) への共通権限: *USE ライブラリー所有者:		

表 44. JKL Toy Company のライブラリー記述用紙: プログラム・ライブラリーの例

ライブラリー記述用紙				**2 / 2**
ライブラリーにある個々のオブジェクトに対する権限のリスト				
グループ・プロファイルまたはユーザー・プロファイル	オブジェクト名	オブジェクト・タイプ	必要な権限	権限リスト
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

プログラムに対する権限を使用したアクセス制御

JKL Toy Company の大多数の社員は顧客情報を変更することができますが、顧客のクレジット限度額を設定できるのは数人だけです。クレジット限度額は顧客マスター・ファイル (CUSTMAS) に保管されていますが、ARPGMLIB 中の ARPGM12 という独立したプログラムによって変更が加えられます。Sharon はこのプログラムに制限を加えて、許可のない社員がクレジット限度額に変更を加えられないようにすることができます。以下の表は、ARPGMLIB のライブラリー記述用紙を示しています。

表 45. JKL Toy Company のライブラリー記述用紙: 個別権限の例

ライブラリー記述用紙		**1 / 2**
ライブラリー名: ARPGMLIB	記述名 (テキスト): 売掛管理プログラム・ライブラリー	
ライブラリーへの共通権限: *USE ライブラリー内のオブジェクトへの共通権限: *USE 新しいオブジェクト (CRTAUT) への共通権限: *USE ライブラリー所有者:		

表 46. JKL Toy Company のライブラリー記述用紙: 個別権限の例

ライブラリー記述用紙				**2 / 2**
ライブラリーにある個々のオブジェクトに対する権限のリスト				
グループ・プロファイルまたはユーザー・プロファイル	オブジェクト名	オブジェクト・タイプ	必要な権限	権限リスト
PUBLIC	ARPGM12	*PGM	*EXCLUDE	

表 46. JKL Toy Company のライブラリー記述用紙: 個別権限の例 (続き)

JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

まず借用権限を使用する制限付きの例を検討してから、ライブラリーとオブジェクトの所有権の決定を行うことができます。

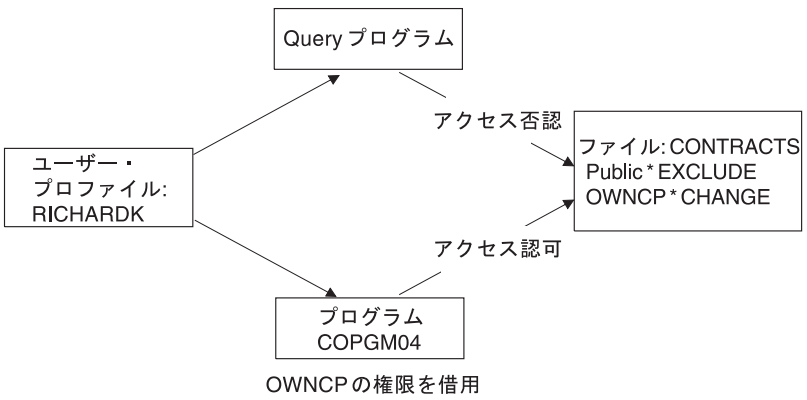
例: JKL Toy Company のライブラリー記述用紙 -- 制限付きアプローチ: これまでの例では (大多数のユーザーがライブラリー内の情報に対するアクセス権を持っているような) セキュリティーへの寛容なアプローチを示してきました。 JKL Toy Company では、契約と価格に関する情報は機密であり、厳重なアプローチをとる必要があると考えています。好都合なことに、これらの情報はすべて独立したライブラリーに保管されています。契約と価格を更新するプログラムも、特別なライブラリーに入っています。

Sharon は、契約および価格アプリケーションのセキュリティーの目的を検討しました (『資源保護の目的の決定』を参照)。また、アプリケーション記述用紙とライブラリー記述用紙も検討しました。そして、両者のアプリケーションのセキュリティーの目的を一致させるのが難しいことが分かりました。そこで、いくつかの注意事項を作成して、アプリケーションの提供者と問題について話し合いました。

- 販売マーケティング部門の担当者と管理者は、契約の作成と変更を行う必要がある。彼らは、ファイルとプログラムを両方とも使用する必要がある。
- 注文処理部門の担当者は、注文の入力時と出荷時に間接的に契約に変更を加え価格を表示するが、他の方法で契約と価格を表示することは許可されない。しかし、Query を使用して、顧客や注文に関する独自の報告書を作成する。契約および価格ファイルに対する権限を彼らに付与すると、Query プログラムを作成して、これらのファイルの表示や印刷を行える。

JKL Toy Company 社のアプリケーションの提供者は、セキュリティーの借用権限機能を使用してこの問題を解決するよう提案しました。**借用権限**を使用すると、ユーザーはプログラムの実行中にそのプログラムの所有者の権限を借用することができます。したがって、オブジェクトに対する権限は必要なくなります。

以下の図は、借用権限の適用例を示しています。注文処理部門の Karen Richards (RICHARDK) には、通常は契約ファイルの使用権限はありません。しかし、注文を入力する際には、契約の差引勘定を検査して更新する必要があります。契約の差引勘定を処理する注文入力プログラム (COPGM04) は、OWNCP プロファイルの権限を借用します。 Karen は、COPGM04 プログラムを実行している間は、契約ファイルの使用権限を付与されます。



オブジェクトの所有権の詳細については、『ライブラリーとオブジェクトの所有権の決定』を参照してください。アプリケーションの提供者かプログラマーは、プログラムの作成 (コンパイル) 時にそのプログラムが所有者の権限を借用するように指定できます。またプログラマーは、プログラムの変更 (CHGPGM) コマンドを使用してプログラムの借用権限を指定することもできます。この手法を使用する場合は、その前にプログラムのすべての機能を確実に理解しておいてください。

Sharon は、借用権限機能を使用して、販売マーケティング部門以外の社員に、契約および価格ファイルに対するアクセス権を付与することを決めました。また、契約および価格アプリケーションで使用されるすべてのオブジェクトに関する権限は、*CHANGE アクセスが妥当であると決めました。以下の表は、契約ライブラリーのライブラリー記述用紙を示しています。

表 47. JKL Toy Company のライブラリー記述用紙: 制限付き権限の例

ライブラリー記述用紙		**1 / 2**
ライブラリー名: CONTRACTS	記述名 (テキスト): 契約および価格ライブラリー	
ライブラリーへの共通権限: *EXCLUDE ライブラリー内のオブジェクトへの共通権限: *CHANGE 新しいオブジェクト (CRTAUT) への共通権限: *CHANGE ライブラリー所有者:		

表 48. JKL Toy Company のライブラリー記述用紙: 制限付き権限の例

ライブラリー記述用紙				**2 / 2**
ライブラリーにある個々のオブジェクトに対する権限のリスト				
グループ・プロファイルまたはユーザー・プロファイル	オブジェクト名	オブジェクト・タイプ	必要な権限	権限リスト
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

ライブラリーそのものに対するアクセスを制限しているため、ライブラリーにあるオブジェクトに対する権限を制限する必要はありません。また、Sharon は、管理者、販売マーケティング部門に権限を付与しています。部門の各個人に権限を付与する代わりに、グループ権限を使用しています。

注: ライブラリーに対するアクセス権を持つ熟練したプログラマーであれば、ライブラリーに対する権限が取り消された後でも、そのライブラリーにあるオブジェクトに対するアクセス権を保持できることがあります。ライブラリーにセキュリティーの必要性が大きいオブジェクトが含まれている場合、オブジェクトとライブラリーを制限して完全に保護されるようにしてください。

まず共通権限を使用した制限なしの例を検討してから、ライブラリーとオブジェクトの所有権の決定を行うことができます。

ライブラリーとオブジェクトの所有権の決定

アプリケーション・ライブラリーのセキュリティーの計画を立てた後、ライブラリーとオブジェクトの所有権を決めることができます。各オブジェクトには、作成時に所有者が割り当てられます。オブジェクトの所有者には、そのオブジェクトに対するすべての権限が自動的に付与されます。その中には、他の人にオブジェクトの使用を許可する権限、オブジェクトを変更する権限、およびオブジェクトを削除する権限が含まれます。機密保護担当者は、システム上のどのオブジェクトにもこれらの機能を実行できます。

システムでは、オブジェクト所有者のプロファイルを使用して、オブジェクトに対する権限を持つユーザーを追跡します。この機能はシステムで内部的に終了します。ユーザー・プロファイルに直接影響を与えることはありません。しかし、オブジェクト所有権の計画が適切でないと、一部のユーザー・プロファイルが大きくなり過ぎることがあります。

システムにオブジェクトが保管される場合は、所有プロファイルの名前も共に保管されます。この情報は、システムでそのオブジェクトが復元される場合に使用されます。復元されるオブジェクトの所有プロファイルがシステム上にないと、所有権がシステムから QDFTOWN という IBM 提供のプロファイルに転送されます。

推奨事項

以下の推奨事項は多くの状態に当てはまりますが、すべての状態に当てはまるというわけではありません。推奨事項を検討したら、オブジェクトの所有権についてプログラマーかアプリケーションの提供者と相談してください。アプリケーションを購入した場合は、どのプロファイルがライブラリーやオブジェクトを所有するかを制御できないことがあります。この場合、所有権を変更できないようアプリケーションが設計されていることが考えられます。

- IBM 提供のプロファイル (QSECOFR や QPGMR など) をアプリケーション所有者として使用しないでください。これらのプロファイルは、IBM 提供のライブラリーにある多数のオブジェクトを所有しており、すでにかなり大きくなっています。
- 通常は、グループ・プロファイルにアプリケーションを所有させないでください。さらに低い権限を特別に割り当てない限り、グループ中のすべてのメンバーがグループ・プロファイルと同じ権限を持つことになります。そして、結果的にはアプリケーションに対する完全な権限をグループのメンバー全員に与えていることになってしまいます。
- アプリケーション制御の責任をさまざまな部門の管理者に委任する計画を立てる場合は、それらの管理者をすべてのアプリケーション・オブジェクトの所有者にすることもできます。しかし、アプリケーションの管理者が担当を変更することがあります。このような場合は、すべてのアプリケーション・オブジェクトの所有権を新しい管理者に転送します。
- 多くの場合には、アプリケーションごとにパスワードを *NONE に設定した特別な所有者プロファイルを作成するという手法が使用されます。システムでは、その所有プロファイルを使用してアプリケーションに関する権限が管理されます。機密保護担当者 (またはこの権限を持つユーザー) は、アプリケーションの実際の管理を実行するか、または特定のアプリケーションに対する *ALL 権限を持つ管理者に委任します。

アプリケーションを所有する必要のあるプロファイルを決めてください。所有者プロファイルの情報を、個々のライブラリー記述用紙に記入してください。

まず JKL Toy Company でアプリケーション所有権を決定した様子を示す例を検討してから、ユーザー・ライブラリーの所有権とアクセス権の決定を始めることもできます。

例: JKL Toy Company のアプリケーション所有権

Sharon Jones は、アプリケーションごとに特別な所有者プロファイルを作成することに決めました。Sharon Jones と補佐の機密保護担当者の Ken Harrison が、アプリケーションのセキュリティーの管理を担当します。将来、会社のセキュリティーの要件がさらに複雑になったら、Sharon は権限の管理の担当を部門の管理者に委任することができます。

Sharon は、命名規則用紙に新しい項目を 1 つ追加しました。

表 49. JKL Toy Company の命名規則用紙: 所有者プロファイルの例

オブジェクトのタイプ	命名規則
所有者プロファイル	アプリケーションごとに所有者プロファイルを作成する。すべてのアプリケーション・ライブラリーと、その中のすべてのオブジェクトが、そのプロファイルに所有される。所有者プロファイルの名前は、OWN とアプリケーションの省略語から成る。たとえば、在庫管理所有者プロファイルは OWNIC になる。

Sharon は、所有者プロファイル名の先頭を OWN にして、表示画面やリストに所有者プロファイルがすべて一緒に表示されるようにすることに決めました。

Sharon は、すべてのアプリケーション・ライブラリーに所有者を割り当て、その情報を命名規則用紙に入力しました。ライブラリーのうち顧客レコード・ライブラリーだけは、複数のアプリケーション所有者が割り当てられている可能性があります。売掛管理アプリケーションは新規の顧客の作成やクレジット限度額の設定に使用されるので、Sharon はこのアプリケーションに顧客ファイルを所有させることに決めました。Sharon が割り当てた所有者は以下のとおりです。

ライブラリー名	所有者名
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
CONTRACTS	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

次に、 ユーザー・ライブラリーの所有権とアクセス権の決定を行えます。

ユーザー・ライブラリーの所有権とアクセス権の決定

システムに IBM Query for iSeries ライセンス・プログラム、または別の意思決定支援プログラムがある場合、ユーザーには、自分が作成した Query プログラムを保管するためのライブラリーが必要です。通常は、ユーザー・プロファイル内の**現行ライブラリー**が、このライブラリーの役割を果たします。ユーザーごとに現行ライブラリーを作成することの詳細については、『サインオンに影響する値の選択』を参照してください。 Sharon Jones は、販売マーケティング部門には現行ライブラリーを使用し、それ以外の部門にはグループ・ライブラリーを使用する計画を立てています。

- 販売マーケティング部門は、Query プログラムを頻繁に使用する。そのため、個々のユーザーは専用ライブラリーを持つ必要がある。これを行わない場合、Query プログラムに付ける名前に悩んだり、他人のプログラムを不慮に削除してしまう恐れがある。
- 開始すると、他の部門はグループ・ライブラリーを持つようになる。 Query プログラムが多数作成される場合は、個別のライブラリーについて考慮することができる。

ユーザーがあるグループに所属している場合は、ユーザー・プロファイル内のフィールドを使用して、そのユーザーが作成したオブジェクトをユーザーかグループのどちらが所有するかを指定します。ユーザーがオブジェクトを所有している場合は、そのオブジェクトを使用するためにグループ・メンバーにどの権限を付与するかを指定することができます。また、グループの権限が、1 次グループ権限か私用権限のどちらであるかを指定することもできます。 1 次グループ権限を使用する方が、パフォーマンスが向上します。
Sharon は、ユーザー・ライブラリーについて、次のような注記を加えました。

- 販売マーケティング部門が作成したオブジェクトは、グループが所有するのではなく、作成者自身が所有する必要がある。他人の Query プログラムに変更を加える必要はない。

- グループの全員が他の人の Query プログラムを実行できるようにする必要がある。つまり、グループ・メンバーが作成したオブジェクトに対して、グループは *USE 権限を持っている。
- グループの権限は 1 次グループ権限でなければならない。
- これらのライブラリーに対して、一般ユーザーはアクセス権を持つべきではない。販売マーケティング部門の担当者は、これらのライブラリーを照会して出力ファイルを生成することがある。その中には機密データが含まれている可能性がある。
- それ以外の部門の場合、グループは、グループ・ライブラリーとライブラリー内に作成されたすべてのものを所有する。したがって、グループのどのメンバーも、ライブラリー内のどれでも変更したり削除したりできる。この方法で問題が生じる場合は、別の方法を試行しなければならない可能性がある。

以下の表は、販売マーケティング部門が、ユーザーが所有しているオブジェクトを使用する場合の個別ユーザー・プロファイル用紙を示しています。

表 50. JKL Toy Company の個別ユーザー・プロファイル用紙: ユーザーが所有するオブジェクトの例

グループ・プロファイル名: DPTSM	
作成されたオブジェクトの所有者: *USRPRF	作成されたオブジェクトに対するグループ権限: *USE
グループ権限タイプ: *PGP	

以下の表は、ある部門が、グループが所有しているオブジェクトを使用する場合の個別ユーザー・プロファイル用紙を示しています。

表 51. JKL Toy Company の個別ユーザー・プロファイル用紙: グループが所有するオブジェクトの例

グループ・プロファイル名: DPTxx	
作成されたオブジェクトの所有者: *GRPPRF	作成されたオブジェクトに対するグループ権限:

作成されたオブジェクトの所有者がグループである場合は、「**作成されたオブジェクトに対するグループ権限**」フィールドは使用されません。グループ・メンバーには、作成されたすべてのオブジェクトに対する *ALL 権限が自動的に付与されます。

ユーザー・ライブラリーを所有し、それに対するアクセス権を持つユーザーを決めてください。個別ユーザー・プロファイル用紙の「**作成されたオブジェクトの所有者**」フィールドと「**作成されたオブジェクトに対するグループ権限**」フィールドに、選択内容を入力してください。これで、オブジェクトのグループ化を始める準備が完了しました。

オブジェクトのグループ化

ライブラリーとオブジェクトの所有権の決定が終わったら、システム上のオブジェクトのグループ化を始めることができます。権限の管理を単純化するには、権限リストを使用して、同じ要件を持つオブジェクトをグループ化してください。その後、リスト上の個々のオブジェクトに対する権限を付与する代わりに、権限リストに対する共通権限、グループ・プロファイル権限、およびユーザー・プロファイル権限を付与できます。システムは権限リスト別に保護されるすべてのオブジェクトを同じ仕方で処理しますが、リスト全体に対するさまざまな権限をさまざまなユーザーに付与することができます。

権限リストを使用すると、オブジェクトの復元時に権限を再確立しやすくなります。権限リストを使用してオブジェクトを保護すると、復元プロセスの際にオブジェクトは自動的にリストにリンクされます。

グループまたはユーザーに対して、権限リスト (*AUTLMGT) を管理する権限を付与することができます。権限リストを使用して管理を行うと、他のユーザーをリストに追加したりリストから除去したりでき、またそれらのユーザーに関する権限を変更できます。

推奨事項

- セキュリティーを行う必要があり、セキュリティー要件が同じであるオブジェクトの場合は、権限リストを使用してください。権限リストを使用すると、権限を個別に考慮するのではなくカテゴリーとして考慮できるようになります。また権限リストを使用すると、システム上のオブジェクトの復元や権限の監査を容易に行えます。
- 権限リスト、グループ権限、個別権限を組み合わせて、体系を込み入ったものにすることは避けてください。すべての方式を同時に使用するよりも、要件に最適の方式を選択してください。

また、権限リストの命名規則を命名規則用紙に追加する必要があります。

権限リスト用紙を作成したら、ライブラリー記述用紙に戻ってその情報を追加してください。プログラマーかアプリケーションの提供者がすでに権限リストを作成している可能性があります。それらを一緒に調べてください。

JKL Toy Company の Sharon Jones が権限リストの計画を立てた方法の例を検討すると、印刷装置および印刷装置出力のセキュリティーの計画を立てる際に役に立つはずです。

例: JKL Toy Company の権限リスト用紙

Sharon は、顧客レコード・ライブラリーのライブラリー記述を検討し、月末ごとに消去されるファイルの権限リストを作成することに決めました。消去されるファイルは 3 つだけですが、Sharon は、権限リストを使用して権限の管理を単純化することにしました。そうすれば、後で他のファイルが月末処理に追加される場合に、権限リストを使用してそれらのファイルを簡単に保護することができます。 Sharon は、ファイルから一般ユーザーを除外して、月末処理中に意図せず問題が生じるのを避けることにしました。この処理を実行するユーザーだけに *ALL 権限が付与されます。午後のシステム操作員である Rose Willis は、ファイルに関する情報を検討して月末処理を調べなければならないことがあります。したがって、*USE 権限が必要です。

以下の表は、Sharon が使用した権限リストの命名規則を示しています。

表 52. JKL Toy Company の命名規則用紙: 権限リストの例

命名規則用紙	
作成者: Sharon Jones	日付: 9/5/99
オブジェクトのタイプ	**命名規則**
権限リスト	1 つのライブラリーのオブジェクトを保護するリストの場合、ライブラリー名の一部、LST、および数値から成る。たとえば、CUSTLIB 中のオブジェクトのリストの場合、CUSTLST1 になる。複数のライブラリーのオブジェクトを保護するリストの場合、可能な限りアプリケーションの省略語を使用する (ARLST1)。リストが複数のアプリケーションに該当する場合は、分かりやすい名前を選択する。リストの説明は、主要な目的を記述したものにする。

以下の表は、CUSTLIB ライブラリーの権限リスト用紙を示しています。 Sharon は、ライブラリー記述用紙の情報を使用して、この用紙を作成しました。

表 53. JKL Toy Company の権限リストの計画: 例

権限リスト用紙
権限リスト名: CUSTLST1
説明: 月末処理時に消去されるファイル。
リストが保護するオブジェクトをリストします。

表 53. JKL Toy Company の権限リストの計画: 例 (続き)

オブジェクト名	オブジェクト・タイプ	オブジェクト・ライブラリー	オブジェクト名	オブジェクト・タイプ	オブジェクト・ライブラリー
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
リストにアクセスするグループとユーザーをリストします。					
グループまたはユーザー	許可されているアクセスのタイプ	リストの管理	グループまたはユーザー	許可されているアクセスのタイプ	リストの管理
PUBLIC	*EXCLUDE	no	ROSSG	*ALL	no
SMITHJ	*ALL	no	JONESS	*ALL	yes
WILLISR	*USE	no			

Sharon は、ライブラリー記述用紙に CUSTLIB ライブラリーの権限リスト情報を追加しました。

ライブラリー記述用紙				2 / 2
作成者: Sharon Jones			日付: 9/9/99	
ライブラリー名: CUSTLIB				
ライブラリー・オブジェクトの特定権限のリスト				
グループ・プロファイルまたはユーザー・プロファイル	オブジェクト名	オブジェクト・タイプ	必要な権限	権限リスト
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

システムが権限リストを使用して共通権限を判別するようにするため、個々のファイルの共通権限を *AUTL に変更しなければならないことに注意してください。

ライブラリー記述用紙のグループ権限と個別権限を見てください。それによって、権限リストを使用することが適切かどうか判別します。適切な場合は、権限リスト用紙を作成し、権限リスト情報を使用してライブラリー記述用紙を更新してください。次に、印刷装置および印刷装置出力のセキュリティーの計画を立てることができます。

印刷装置および印刷装置出力のセキュリティーの計画

オブジェクトのグループ化が終わったら、印刷装置出力を保護する方法の計画を立てる必要があります。システム上に保管されている情報を保護する計画はすでに開発しました。さらに、印刷時や印刷待機時に機密情報を保護する計画も必要です。お客様の会社が機密出力用に使用している印刷装置の物理的セキュリティーの計画を調べてください。

報告書を印刷するプログラムを実行すると、通常、報告書は印刷装置に直接送られません。プログラムによって、**スプール・ファイル**または**印刷装置出力**と呼ばれる、報告書のコピーが作成されます。印刷装置が使用できるようになるまで、スプール・ファイルはシステムによって**出力待ち行列**というオブジェクトに保管されます。出力待ち行列に印刷装置出力が入っている場合は、ワークステーションで報告書を表示できます。また、出力を保留にしたり、特定の印刷装置に宛先指定したりすることもできます。

スプーリングを行うと、印刷ジョブのスケジュールを立てたり、印刷装置を共用したりしやすくなります。また、機密出力を保護するのにも役立ちます。1 つまたは複数の特別な出力待ち行列を作成して機密出力を保留し、それらの出力待ち行列を表示したり管理したりできるユーザーを制限することができます。また、機密出力が待ち行列から印刷装置にいつ送信されるのか制御できます。

このトピックに沿って作業しながら、印刷装置出力およびワークステーションのセキュリティー用紙を完成させてください。

特別な出力待ち行列を作成する際には、セキュリティーに関係する以下のパラメーターを指定することができます。

- **ファイルの表示 (DSPDTA) パラメーター**: 出力待ち行列の DSPDTA パラメーターは、あるユーザーが別のユーザーの所有するスプール・ファイルの表示、送信、またはコピーを行えるかどうかを決定します。
- **検査権限 (AUTCHK) パラメーター**: 出力待ち行列の AUTCHK パラメーターは、あるユーザーが別のユーザーの所有するスプール・ファイルの変更または削除を行えるかどうかを決定します。
- **操作員制御 (OPRCTL) パラメーター**: 出力待ち行列の OPRCTL パラメーターは、*JOBCTL 特殊権限 (または *SYSOPR ユーザー・クラス) を持つユーザーが出力待ち行列を制御できるかどうかを決定します。

ユーザーが出力待ち行列にあるスプール・ファイルに対して実行できる機能を決定するには、出力待ち行列パラメーター、出力待ち行列に対するユーザー権限、およびユーザーの特殊権限を一緒に使用します。以下の表は、それらを組み合わせることにより、ユーザーがどの機能を実行できるが示されています。

印刷機能	出力待ち行列パラメーター			出力待ち行列権限	特殊権限
	DSPDTA	**AUTCHK**	**OPRCTL**		
スプール・ファイルの待ち行列への追加[1]	任意	任意	任意	*READ	なし
	任意	任意	*Yes	任意	*JOBCTL
スプール・ファイルのリストの表示 (WRKOUTQ コマンド)[2]	任意	任意	任意	*READ	なし
	任意	任意	*Yes	任意	*JOBCTL
スプール・ファイルの表示、コピー、または送信 (DSPSPLF、CPYSPFL、SNDNETSPLF、SNTCPSPLF)[2]	*YES	任意	任意	*READ	なし
	*NO	*DTAAUT	任意	*CHANGE	なし
	*NO	*OWNER	任意	所有者[3]	なし
	*YES	任意	*Yes	任意	*JOBCTL
	*NO	任意	*Yes	任意	*JOBCTL
	*OWNER[5]	任意	任意	任意	任意
スプール・ファイルの変更、削除、保留、および解放 (CHGSPLFA、DLTSPLF、HLDSPLF、RLSSPLF)[2]	任意	*DTAAUT	任意	*CHANGE	なし
	任意	*OWNER	任意	所有者[3]	なし
出力待ち行列の変更、消去、保留、および解放 (CHGOUTQ、CLROUTO、HLDOUTQ、RLSOUT)[2]	任意	*DTAAUT	任意	*CHANGE	なし
	任意	*OWNER	任意	所有者[3]	なし
	任意	任意	*YES	任意	*JOBCTL
待ち行列への書き出し機能の開始 (STRPRTWTR、 STRRMTWTR)[2]	任意	*DTAAUT	*Any	*CHANGE[4]	なし
	任意	任意	*YES	任意[4]	*JOBCTL

1	これは、ユーザーの出力を出力待ち行列に宛先指定するために必要な権限です。
2	これらのコマンドまたは画面からそれと同じ機能のオプションを使用します。
3	出力待ち行列の所有者でなければなりません。
4	印刷装置記述に対する *USE 権限も必要です。
5	スプール・ファイルの所有者であるか、または *SPLCTL 特殊権限がなければなりません。

物理的セキュリティーの計画の印刷装置の部分を検討してください。このトピックに沿って作業しながら、印刷装置出力およびワークステーションのセキュリティー用紙の出力待ち行列の部分を記入してください。

JKL Toy Company の Sharon Jones がこれらの出力待ち行列パラメーターの値を決定した方法の例を検討すると、ワークステーションの資源保護の計画を立てる際に役に立つはずです。

例: JKL Toy Company の出力待ち行列およびワークステーションのセキュリティー用紙 -- 出力待ち行列の部分

JKL Toy Company の販売マーケティング部門には、機密印刷に関する以下の 2 つの要件があります。

- 価格変更の計画を立てる際に、仮の価格リストが印刷される。販売マーケティング部門のメンバー以外は、管理者を除いてこの情報を参照できない。
- 契約は折衝中は機密である。未完成の契約ドラフトは、契約の折衝を担当している人間だけが参照でき、販売マーケティング部門の他のメンバーは参照できない。

Sharon は、以下の 2 つの特別な出力待ち行列を作成することに決めました。

PRICEQ
仮の価格リスト用に使用します。販売マーケティング部門の人間は、この出力待ち行列に対してどの機能でも実行できます。これらの部門以外の人間 (システム操作員を含む) は、この出力待ち行列を使用できません。 PRICEQ は CONTRACTS ライブラリーにあります。

NEWCP
折衝中の契約の印刷用に使用します。出力待ち行列は販売マーケティング部門のメンバーの間で共用されますが、そのファイルを制御できるのは、出力待ち行列にスプール・ファイルを作成した人だけです。 NEWCP は CONTRACTS ライブラリーにあります。

以下の表は、Sharon が作成した、出力待ち行列およびワークステーションのセキュリティー用紙の出力待ち行列の部分を示しています。

表 54. JKL Toy Company の出力待ち行列およびワークステーションのセキュリティー用紙: 印刷装置出力待ち行列の例

制限付き出力待ち行列のパラメーターのリスト:				
出力待ち行列名	出力待ち行列 ライブラリー	任意のファイルの表示 (DSPDTA)	検査権限 (AUTCHK)	操作員制御 (OPRCTL)
PRICEQ	CONTRACTS	*YES	*DTAAUT	*NO
NEWCP	CONTRACTS	*NO	*OWNER	*NO

『アプリケーション・ライブラリーに対する共通権限の決定』には、 JKL Toy Company における CONTRACTS ライブラリーの権限が示されています。管理者と、販売マーケティング部門のメンバーだけが、このライブラリーに対するアクセス権を持っています。このライブラリーのオブジェクト (前述の出力待ち行列を含む) の共通権限は *CHANGE です。

NEWCP 出力待ち行列の AUTCHK パラメーターは *OWNER なので、スプール・ファイルの所有者だけがこのファイルを処理できます (前述の『印刷機能を実行するのに要求される権限』表を参照してください)。したがって、販売マーケティング部門のメンバーは、互いに他のメンバーの新しい契約を印刷したり、出力待ち行列にある新しい契約を表示したりすることができません。

印刷装置出力待ち行列のセキュリティーの計画が完了したら、ワークステーションのセキュリティーを計画することができます。

ワークステーションのセキュリティーの計画

印刷装置および印刷装置出力のセキュリティーの計画を立てたら、ワークステーションのセキュリティーの計画を立てることができます。物理的セキュリティーの計画の際に、ロケーションが原因でセキュリティーのリスクが生じるワークステーションをリストしました。この情報を使用して、制限する必要のあるワークステーションを判別してください。

これらのワークステーションを使用するユーザーに、特にセキュリティーに注意するよう促すことができます。これらのユーザーがワークステーションから離れる際には必ずサインオフする必要があります。セキュリティー方針の中に、無防備なワークステーションのサインオフ手順に関する決定事項を記録することもできます。これらのワークステーションで実行できる機能を制限して、リスクを最小限にとどめることもできます。

ワークステーションでの機能を制限する最も簡単な方式は、限定された機能を持つユーザー・プロファイルにしか、その機能を使用できないように制限することです。JKL Toy Company の Sharon Jones は倉庫部門にこの手法を使用しました。Sharon は、発送所で働く Ray Wagner と Janice Ames が、在庫受け取りプログラムだけを実行できるようにしました。また、この 2 人だけに発送所のワークステーションにサインオンする許可を与えました。

機密保護担当者権限または保守権限を持つユーザーがサインオンできるワークステーションを制限することもできます。 QLMTSECOFR システム値を使用してこの処理を行うと、機密保護担当者権限を持つユーザーは、特別に許可されたワークステーションだけにサインオンできます。

出力待ち行列およびワークステーションのセキュリティー用紙のワークステーションの部分を作成してください。

出力待ち行列およびワークステーションのセキュリティー用紙のワークステーションの部分を作成する際に、 Sharon がワークステーションのセキュリティーの計画を立てた方法の例を検討することもできます。また、資源保護の推奨事項のリストを検討して、資源保護の計画を単純かつ完全なものにする必要もあります。例および推奨事項の検討が完了したら、アプリケーションの導入の計画を開始することができます。

例: JKL Toy Company の出力待ち行列およびワークステーションのセキュリティー用紙 -- ワークステーションの部分

Sharon Jones は、物理的セキュリティーの計画を検討して、セキュリティーのリスクがあるワークステーションを判別しました。たとえば、JKL Toy Company では、社外の人間は発送所のワークステーションおよび遠隔地の営業所のワークステーションに簡単にアクセスできます。 Sharon は、物理的セキュリティーの計画の段階で、これらのワークステーションに潜在的なセキュリティーのリスクがあるということを指摘しました。

ワークステーションでの機能を制限する最も簡単な方式は、限定された機能を持つユーザー・プロファイルにしか、その機能を使用できないように制限することです。JKL Toy Company の Sharon Jones は倉庫部

門にこの手法を使用しました。Sharon は、発送所で働く Ray Wagner と Janice Ames が、在庫受け取りプログラムだけを実行できるようにしました。また、この 2 人だけに発送所のワークステーションにサインオンする許可を与えました。

Sharon は、QLMTSECOFR システム値の選択項目を再評価しました。この値を 1(Yes) に設定して、発送所と離れた営業所にある、それぞれ無防備なワークステーションの保護を強化することに決めました。

以下の表は、Sharon が作成した、出力待ち行列およびワークステーションのセキュリティー用紙のワークステーションの部分を示しています。

表 55. JKL Toy Company の出力待ち行列およびワークステーションのセキュリティー用紙: ワークステーションの例

機密保護担当者のワークステーション: 機密保護担当者を特定のワークステーションに制限する (システム値 QLMTSECOFR を yes にする) 場合は、機密保護担当者と *ALLOBJ 権限を持つすべてのユーザーに許可されたワークステーションを以下にリストする: 以下にリストされたワークステーションを除くすべてのワークステーション	
制限されているワークステーションの権限を下にリストする:	
ワークステーション名	権限が与えられているグループまたはユーザー (*CHANGE 権限)
DSP10	AMESJ, WAGNERR
DSP11	AMESJ, WAGNERR
RMT01	UNGERJ, BELLB
RMT02	UNGERJ, BELLB

資源保護に関する推奨事項の要約を検討してから、アプリケーションの導入の計画を立てることもできます。

資源保護に関する推奨事項の要約

ワークステーションのセキュリティーの計画を立てたら、以下の資源保護に関する推奨事項を検討できます。 iSeries システムは、システム上の情報を保護するためのオプションを多数提供しています。このオプションを使用すると、資源保護の計画を設計する上で融通がきくため、お客様の会社にとって最善の設計にすることができます。しかし、この多数のオプションは複雑でもあります。

このトピックでは、例として JKL Toy Company を使用して、以下の指針を使用した基本的な資源保護の計画方法について説明します。

- 汎用権限から特定権限に移行する。
  - ライブラリーのセキュリティーを計画する。必要な場合にのみ個々のオブジェクトを扱ってください。
  - 共通権限を最初に計画し、それからグループ権限と個別権限を計画する。
- パフォーマンスを向上させ、バックアップと回復を単純にするには、共通権限ではセキュリティー要件を満たせないオブジェクトにのみ特定のセキュリティーを定義する。
- ライブラリー内の新しいオブジェクトの作成権限 (CRTAUT) は、ライブラリー内の既存オブジェクトの大多数について定義した共通権限と同じにする。
- 共通権限より低い権限をグループまたは個別に付与しない。付与すると、パフォーマンスが低下し、その後の作業で間違いを犯しやすくなったり、監査も難しくなったりします。全員がオブジェクトに対して共通権限と同等かそれ以上の権限を持っていることが分かっていれば、セキュリティーの計画や監査が行いやすくなります。

- 同じセキュリティー要件を持つグループ・オブジェクトに対して、権限リストを使用する。権限リストは個別権限よりも管理するのが簡単で、セキュリティー情報を回復するのに役立ちます。
- アプリケーション所有者として特別なユーザー・プロファイルを作成する。所有者パスワードを *NONE に設定してください。
- QSECOFR や QPGMR のような IBM 提供のプロファイルにアプリケーションを所有させることは避ける。
- 機密報告書には特別な出力待ち行列を使用する。機密情報が含まれているライブラリーに出力待ち行列も作成してください。
- 機密保護担当者権限を持つユーザーの数を制限する。
- オブジェクトまたはライブラリーに *ALL 権限を認可する際には注意する。 *ALL 権限のあるユーザーはこれらのものを意図せずに削除する可能性があります。

資源保護の設定を正しく計画したことを確認するには、以下の情報を収集する必要があります。

- すべてのアプリケーション・ライブラリーのライブラリー記述用紙の第 1 部と第 2 部を記入する。
- 個別ユーザー・プロファイル用紙の、「**作成されたオブジェクトの所有者**」フィールドと「**作成されたオブジェクトに対するグループ権限**」フィールドに記入する。
- 命名規則用紙に、権限リストの命名計画を記述する。
- 権限リスト用紙を作成する。
- ライブラリー記述用紙に権限リスト情報を追加する。
- 出力待ち行列とワークステーションのセキュリティー用紙を作成する。

これで、アプリケーションの導入の計画を立てる準備が完了しました。

アプリケーションの導入の計画

資源保護の計画を終了するには、アプリケーションを導入する準備を行う必要があります。以下のトピックは、アプリケーションを導入した後に、そのアプリケーションに対する所有権や権限を計画するのに役立ちます。しかし、ここで説明する方式が当てはまらないアプリケーションもあります。良い導入の計画を立てる際には、プログラマーかアプリケーションの提供者と相談してください。

アプリケーションの提供者からアプリケーションを入手する計画であれば、この情報を使用して、アプリケーション・ライブラリーのロード前後に行う必要のあるセキュリティーを計画してください。

プログラマーが開発したアプリケーションをご使用のシステムに導入する計画であれば、この情報を使用して、アプリケーションをテスト状況から実動状況に移行するのに必要なセキュリティー活動を計画してください。

まず、1 つのアプリケーションで、すべてのステップを実行します。次に、その他のアプリケーションに戻って、アプリケーションの導入用紙を作成します。

必要な用紙

以下の用紙をコピーして、このトピックの作業を進めながら記入してください。

表 56. アプリケーションの導入計画に必要な計画用紙

用紙名	必要なコピーの部数
アプリケーションの導入用紙	アプリケーション当たり 1 つ

以下の用紙は、アプリケーションの導入計画に必要な情報を収集するために、すでに作業したものです。これらの用紙を使用してください。

用紙名	作成内容
ライブラリー記述用紙	ライブラリー情報の記述
権限リスト用紙	オブジェクトのグループ化

『アプリケーションのロード』では、アプリケーションを導入するのに必要なステップを実行する方法が説明されています。

アプリケーションの導入を計画するには、以下のトピックを参照してください。

- 『アプリケーションのユーザー・プロファイルと導入値の決定』
- 『導入値の変更』

アプリケーションのユーザー・プロファイルと導入値の決定

アプリケーションの導入の計画を立てる際には、まずアプリケーションごとにユーザー・プロファイルと導入値を決めなければなりません。別のシステム上で作成したアプリケーションを導入する場合、その前に 1 つ以上のユーザー・プロファイルを作成しなければならないことがあります。システムにライブラリーをロードするには、アプリケーション・ライブラリーとオブジェクトを所有するユーザー・プロファイルがシステム上にすでに存在していなければなりません。ライブラリーごとに作成する必要のあるプロファイルと、それらのプロファイルに必要なパラメーターを、アプリケーションの導入用紙に記録してください。

必要な導入値を判別するには、プログラマーかアプリケーションの提供者に以下の質問をして、回答をアプリケーションの導入用紙に記録してください。

- アプリケーション・ライブラリーを所有するプロファイル。
- ライブラリーにあるオブジェクトを所有するプロファイル。
- ライブラリーに対する共通権限 (AUT)。
- 新しいオブジェクト (CRTAUT) への共通権限。
- ライブラリーにあるオブジェクトの共通権限。
- 所有者の権限を借用するプログラム (ある場合)。

プログラマーかアプリケーションの提供者が、アプリケーションの権限リストを作成しているかどうか調べてください。作成されている権限リストごとに権限リスト用紙を作成するか、権限リストに関する情報をプログラマーに尋ねてください。

これで、導入値の変更を行う必要があるかどうかを決めることができます。

アプリケーションの導入値の変更

アプリケーションの導入用紙の情報と、ライブラリー記述用紙に記録したライブラリーの資源保護計画を比較してください。両者が異なる場合は、アプリケーションの導入後にどのような変更を加えるか決める必要があります。

アプリケーション所有権の変更

プログラマーまたはアプリケーションの提供者が特別なプロファイルを作成して、アプリケーション・ライブラリーとオブジェクトを所有している場合は、命名規則が一致していなくてもそのプロファイルを使用することを考慮してください。オブジェクトの所有権を転送すると長時間かかることがあるため、避けてください。

QSECOFR や QPGMR などの IBM 提供のグループ・プロファイルの 1 つがアプリケーションを所有する場合は、そのアプリケーションの導入後に別のプロファイルに所有権を転送する必要があります。

プログラマーは、オブジェクトの所有権に関する変更を加えなくて済むように、アプリケーションを設計することがあります。制約事項の範囲内で作業しながら、セキュリティーの管理に関する独自の要件を満たしてください。しかし、QSECOFR などの IBM 提供のプロファイルがアプリケーションを所有している場合は、お客様自身とプログラマーまたはアプリケーションの提供者が相談して、所有権を変更する計画を開発する必要があります。理想的には、所有権を変更してからアプリケーションを導入してください。

共通権限の変更

オブジェクトを保管する際には、その共通権限も同時に保管することになります。システムにアプリケーション・ライブラリーを復元すると、ライブラリーとそのすべてのオブジェクトには、保管時に持っていたものと同じ共通権限があります。このことは、別のシステムにライブラリーを保管していた場合にも当てはまります。

ライブラリーの CRTAUT 値 (新しいオブジェクトの共通権限) は、復元されるオブジェクトには影響しません。ライブラリーの CRTAUT 値に関係なく、保管時の共通権限を持ったまま復元されます。

ライブラリーとオブジェクトの共通権限に変更を加え、ライブラリー記述用紙での計画と一致させる必要があります。

アプリケーションの導入を計画する際に、JKL Toy Company の Sharon Jones がアプリケーションの導入を計画した様子を示す例を検討することもできます。

アプリケーションの導入計画が終了していることを確かめるためには、以下の作業が終わっていなければなりません。

- 最初のアプリケーションの導入用紙をすべて記入し終えている。完成していたら、その他のアプリケーションに戻って、それぞれの用紙を作成してください。
- すべての用紙を検討し、完成していることを確認する。用紙をコピーし、システムとライセンス・プログラムの導入が終了するまで、安全な場所に保管してください。

これで、これらの計画作業が完了しました。ユーザー・セキュリティーの設定に進むことができます。

例: JKL Toy Company のアプリケーションの導入用紙: JKL Toy Company では、アプリケーションの提供者から顧客注文アプリケーションと売掛管理アプリケーションを購入しました。さらに、外部のプログラマーを雇って、契約および価格アプリケーションを開発し、それを顧客注文アプリケーションにリンクさせました。

Sharon Jones は、ライブラリー記述用紙の情報を使用して、アプリケーションの導入用紙を作成しました。以下の表は、Sharon が作成した、CUSTLIB のライブラリー記述用紙のコピーを示しています (『ライブラリー情報の記述』を参照してください)。

表 57. JKL Toy Company のライブラリー記述用紙: 例

ライブラリー記述用紙	**1 / 2**
作成者: Sharon Jones	日付: 9/9/99
ライブラリー名: CUSTLIB	記述名 (テキスト): 顧客レコード・ライブラリー
このライブラリーの機能についての簡単な説明: 注文と売掛管理を含む、すべての顧客ファイルを保持する。	

表 57. JKL Toy Company のライブラリー記述用紙: 例 (続き)

ライブラリーに対するセキュリティーの目的の定義 (機密情報を含んでいるかどうかなど): 現在、当社の全社員は顧客注文を見ることができる。 To protect the accuracy of information, we should limit who is allowed to change it.
ライブラリーへの共通権限: *USE ライブラリー内のオブジェクトへの共通権限: *CHANGE 新しいオブジェクト (CRTAUT) への共通権限: *CHANGE ライブラリー所有者: OWNAR

以下の表は、Sharon が作成した、顧客注文アプリケーションのアプリケーションの導入用紙を示しています。 Sharon は、アプリケーションの提供者が作成した所有者プロファイルを使用することにしたことに注意してください。プロファイル COWNER は、ファイル・ライブラリーとプログラム・ライブラリーの両方を所有しています。

Sharon は、アプリケーションを導入した後で、以下のことを行う必要があります。

- ライブラリーの共通権限に変更を加えて、ライブラリー記述用紙の資源保護計画と一致させる。
- COWNER プロファイルのユーザー・クラスを *USER に変更し、特殊権限をすべて除去する。
- COWNER プロファイルのパスワードを *NONE に変更する。

表 58. JKL Toy Company のアプリケーションの導入用紙: 例

アプリケーション名: 顧客注文 (CO)		説明: 注文の入力、追跡、出荷を行う。
アプリケーションを導入するために作成しなければならないプロファイルのリストと説明: ファイルを含むライブラリーは COWNER というプロファイルに所有される。プログラム・ライブラリーは QPGMR に所有される。		
ライブラリー名: CUSTLIB		
	導入前	**導入後**
ライブラリー所有者	COWNER	COWNER
オブジェクト所有者	COWNER	COWNER
ライブラリー共通権限	*EXCLUDE	*USE
オブジェクト共通権限	*ALL	*CHANGE
新しいオブジェクトへの共通権限	*CHANGE	*CHANGE
ライブラリー名: COPGMLIB		
	導入前	**導入後**
ライブラリー所有者	QPGMR	COWNER
オブジェクト所有者	QPGMR	COWNER
ライブラリー共通権限	*EXCLUDE	*USE
オブジェクト共通権限	*ALL	*CHANGE
新しいオブジェクトへの共通権限	*CHANGE	*CHANGE

これで、これらの計画作業が完了しました。ユーザー・セキュリティーの設定に進むことができます。

ユーザー・セキュリティーの設定

このトピックでは、コマンド行インターフェースを使用して、システム上にユーザー・セキュリティーを設定するのに必要な作業を概説します。新しいシステムを設定する場合は、これらのステップを順番に完了する必要があります。次のステップに進むたびに、各ステップの情報が使用されます。基本的なシステム・セキュリティーを設定するには、大きく分けて 2 つの作業を完了する必要があります。まず最初にユーザー・セキュリティーを定義し、次にシステム上の資源を保護しなければなりません。以下の 2 つの表は、ユーザー・セキュリティーと資源保護を設定するために、構成しなければならない個々のステップを強調しています。

注: 資源保護の設定を始めるには、その前にまずユーザー・セキュリティーを設定するためのステップをすべて完了**しなければなりません**。

表 59. ユーザー・セキュリティーの設定に関するステップ

ステップ	このステップの内容	使用する用紙
全体的な環境の設定	初期システム値とネットワーク属性の設定。機密保護担当者のユーザー・プロファイルの作成。	システム値選択用紙
セキュリティーのシステム値の設定	追加のシステム値の設定。	システム値選択用紙
アプリケーションをロードするための基本的なセキュリティー・ステップの実行	所有者プロファイルの作成。アプリケーションのロード。残りのステップを完了するためには、アプリケーション・ライブラリーとオブジェクトがシステム上にすでに存在していなければなりません。	アプリケーションの導入用紙
ユーザー・グループの設定	ジョブ記述、グループ・ライブラリー、およびグループ・プロファイルの作成。	ユーザー・グループ記述用紙
個々のユーザーの設定	個別ライブラリーとユーザー・プロファイルの作成。	個別ユーザー・プロファイル用紙

表 60. 資源保護の設定に関するステップ

ステップ	このステップの内容	使用する用紙
所有権および共通権限の設定	ライブラリーとオブジェクトの所有権と共通権限の確立。	アプリケーションの導入用紙
権限リストの作成	権限リストの作成。	権限リスト用紙
特定権限の設定	ライブラリーと個別オブジェクトに対するアクセス権の設定	ライブラリー記述用紙
印刷装置出力の保護	出力待ち行列を作成して出力を割り当てることによる、印刷装置出力の保護。	出力待ち行列およびワークステーションのセキュリティー用紙
ワークステーションの保護	ワークステーションの保護。	出力待ち行列およびワークステーションのセキュリティー用紙

上記の表にリストされているトピックに加えて、システム・セキュリティーの管理に関する以下のトピックを参照してください。

- 『セキュリティーのテスト』
- 『セキュリティー情報の変更』

- 『セキュリティー情報の保管』
- 『セキュリティーの監視』

始める前に

新しいシステムを導入する場合は、まず以下の作業を行ってからセキュリティーの設定を開始してください。

- ご使用のシステム装置と装置が導入されており、適切に作動しているか確認する。iSeries の命名規則を使用して装置の名前を指定するよう計画していない場合は、装置の命名規則を決めるシステム値 (QDEVNAMING) を変更するまで、ワークステーションと印刷装置との接続を待ってください。『新しいシステム値の適用』には、装置をいつ接続するべきか説明されています。
- 使用を計画しているすべてのライセンス・プログラムをロードします。

全体的な環境の設定

ユーザー・セキュリティーの設定を始めるには、ユーザーの全体的な環境を設定する必要があります。このトピックでは、SETUP メニューを使用してシステム値を設定し、独自のユーザー・プロファイルを作成してください。専用保守ツール (DST) プロファイルのユーザー ID とパスワードも変更します。

以下の手順では、これらのステップを示すためにコマンド行画面の例が載せられています。しかし、画面全体が示されているわけではありません。作業を完了するのに必要な情報だけが取り上げられています。

必要な用紙

『全体的なセキュリティー戦略の計画』で作成したシステム値選択用紙の情報を入力してください。

全体的な環境を設定するには、以下の作業を完了する必要があります。

1. システムへのサインオンを行います。
2. 正しい操作援助レベルを選択します。
3. 他のユーザーがサインオンできないようにします。
4. セキュリティーのシステム値を入力します。
5. 新しいシステム値を適用します。
6. 機密保護担当者プロファイルの作成

上記のステップを完了した後、保守ツールの各パスワードを変更し、これらが他人によって不正に使用されないようにする必要があります。詳細については、『保守ツール』を参照してください。

システムへのサインオン

システム環境の設定を始めるには、システムにサインオンする必要があります。

1. コンソールで、機密保護担当者 (QSECOFR) としてサインオンします。初めてサインオンする場合は、パスワード QSECOFR を使用してください。このパスワードはシステムの出荷時に期限満了に達しているため、このパスワードを変更するようプロンプト指示されます。正常にサインオンするには、このパスワードを変更しなければなりません。
2. 「サイン・オン」画面の「メニュー」フィールドに、SETUP と入力します。

注: SETUP メニューは「システム、ユーザー、および装置のカスタマイズ」メニューと呼ばれます。本書では、全体を通してこのメニューを SETUP メニューと言います。

```
                    サイン・オン
                                  システム . . . . :
                                  サブシステム . . :
                                  表示装置 . . . . :

ユーザー . . . . . .  QSECOFR
パスワード . . . . . .  _________
プログラム/プロシージャー. . . .  _________
メニュー . . . . . .  SETUP
現行ライブラリー . . . . . .  _________
```

システムへのサインオンが完了したら、正しい操作援助レベルを選択しなければなりません。

正しい操作援助レベルの選択

システムにサインオンしたら、ユーザーに適した操作援助レベルを選択できます。**操作援助レベル**により、表示される画面のバージョンが決まります。多くのシステム画面には、次の 2 種類のバージョンがあります。

- 基本援助レベルのバージョン。情報量が少なく、技術用語は使用されていません。
- 中間操作援助レベルのバージョン。情報量が基本より多くなり、技術用語が使用されています。

特定のバージョンの画面だけに表示できるフィールドや機能があります。その場合、どのバージョンを使用するか指示されます。操作援助レベルを一方から他方に変更するには、**F21** (操作援助レベルの選択) を使用してください。**F21** を使用できない画面もあります。

操作援助レベルの選択が完了したら、セキュリティーの設定時にシステムに他のユーザーがサインオンできないようにしなければなりません。

他のユーザーがサインオンできないようにする

正しい操作援助レベルを選択したら、システムに他のユーザーがサインオンできないようにしなければなりません。システムの保護が可能になる前にそのシステムを悪用する人がいないか心配な場合は、別のワークステーションでサインオンできないようにすることができます。これはオプションです。この処理は、一時セキュリティーが必要だと思う場合にのみ行ってください。

1. SETUP メニューで、**F9** を押してコマンド行を表示します。
2. コマンド行で、GO DEVICESTS と入力します。
3. 画面に「装置状況タスク」メニューが表示されます。
4. オプション **1** (表示装置の処理) を選択します。「構成状況の処理」メニューが表示される場合には、**F21** (操作援助レベルの選択) を使用して、基本援助レベルに変更します。
5. 「表示装置の処理」画面で、使用中のもの以外のワークステーションをすべて使用不可にします。この処理を行うには、それぞれのワークステーション名の前に **2** と入力して、**Enter** キーを押します。
6. **F3** (終了) を 2 回押して、SETUP メニューに戻ります。
7. **F12** (取り消し) を押して、コマンド行を除去します。

```
                              表示装置の処理

下のオプションを入力して、実行キーを押してください。
  1= 使用可能にする   2= 使用不能にする        5= 明細の表示    7=メッセージの表示
  7=Display message   8=Work with controller and line
  13=Change description

 OPT   装置       タイプ     状況
 __    DSP01      3196       QSECOFR が使用中である。
 2_    DSP02      3196       使用可能
 2_    DSP03      3196       使用可能
 2_    DSP04      3196       使用可能
```

装置を使用不可にすると、電源がオンになっていてもサインオン画面は表示されません。システムを停止して再始動するまでの間だけ、ワークステーションは使用不可のままになります。このステップを繰り返し行わなければならないこともあります。

システムに他のユーザーがサインオンできないようにしたら、セキュリティーのシステム値を入力することができます。

セキュリティーのシステム値の入力

他のユーザーがサインオンできないようにしたら、システムにシステム値を入力する必要があります。

次の手順を使用して、システム値選択用紙の第 1 部の情報を入力してください。

1. SETUP メニューで、**1** (システム・オプションの変更) を選択します。
2. システム値選択用紙の情報を、「システム・オプションの変更」画面に入力します。画面上の表示内容を変更しない場合は、タブ・キーを使用してスキップできます。
3. システムの開始時に日時を設定していなかった場合は、この画面上で正しい日時を入力します。
4. このページに情報を入力したら、次のページに移ります。画面の右下角の「続く...」は、後続のページが 1 ページ以上あることを示しています。

```
                        システム・オプションの変更
                                                          システム :
下の選択項目を入力して、実行キーを押してください。

システム名  . . . . . .  JKLTOY      名前

日付および時刻オプション :
  システム日付  . . . . . .  00/12/19    YY/MM/DD
  システム時刻  . . . . . .  13:39:26    HH:MM:SS
  日付区切り記号  . . . . . .  1          1=/
                                         2=-
                                         3=.
                                         4=,
                                         5=ブランク
  日付の形式  . . . . . .  YMD          YMD, MDY, DMY, JUL
  時刻区切り記号  . . . . . .  1          1=:
                                         2=.
                                         3=,
                                         4=ブランク


                                                          続く ...
F1= ヘルプ   F3= 終了   F5= 最新表示   F12= 取り消し
```

5. 画面の 2 ページ目に選択項目を入力し、ページ送りします。

```
                        システム・オプションの変更

下の選択項目を入力して、実行キーを押してください。

機密保護オプション :
  機密保護レベル  . . . . . .  40          10= 物理的な機密保護のみ
                                          20=パスワードによる機密保護のみ
                                          30=パスワードとオブジェクトによる
                                            機密保護
                                          40=パスワード、オブジェクト、および
                                            オペレーティング、システムの保全性
                                          50=パスワード、オブジェクト、および拡
                                            張オペレーティング・システム保全性
  :
 Allow security officers to
   sign on to any display
    置にサイン・オン可能  . . .  N                Y=YES, N=NO
```

6. 画面の 3 ページ目に選択項目を入力し、**Enter** キーを押します。

```
                        システム・オプションの変更

下の選択項目を入力して、実行キーを押してください。

装置オプション :
 Device naming format for new
 devices . . . . . .  1


  デフォルトのシステム印刷装置  . PRT01       名前、リストは F4 キー

追加オプション :
  サイン・オン時にユーザーを
    S/36 環境に入れる . . . . .  N           Y=YES, N=NO
  完了した印刷装置出力に関する
    ジョブ会計情報の保管. . . .  Y
```

7. SETUP メニューが再表示されます。画面の下部に表示される次のメッセージに注意してください。
   System options successfully changed. IPL required.

   注: システムで IPL が必要なのは、セキュリティーのレベルを変更した場合だけです。

ほとんどのシステム・タスクのトピックの最後に、考えられるエラーと回復ステップについて説明した表があります。結果が説明されているものと異なる場合に、これらの表を役立ててください。これらの表ではすべての問題を扱っているわけではありません。その目的は、問題解決の指針を示し、システムをさらに快適に使用できるようにすることです。

考えられるエラー	回復
MAIN メニューが表示される。	**F3** (終了) または **F12** (取り消し) を押しました。 GO SETUP と入力して、再試行してください。
「終結処理オプションの変更」画面など、別の画面が表示される。	SETUP メニューで間違ったオプションを選択しました。 **F3** (終了) を押してメニューに戻り、再試行してください。
Enter キーを押すと、「システム・オプションの変更」画面が再表示される。	画面の下部のエラー・メッセージを参照してください。許可されていない値を入力したと思われます。詳細情報が必要な場合は **F1** (ヘルプ) を使用してください。入力する前の状態にすべての値を復元したい場合は、**F5** (最新表示) を使用してください。その後、再試行します。

考えられるエラー	回復
画面に選択項目をすべて入力し終える前に、**Enter** キーを押した。	システム値を変更するのに必要な回数だけ、この画面を使用できます。 SETUP メニューでオプション **1** を選択して、最初に間違えた値を入力してください。**重要: システムが作動可能になったら、必ずプログラマーに相談してからセキュリティー・レベルを変更してください。また、iSeries Access の使用中、あるいは他のコンピューターとの通信中には、システム名を変更しないでください。**
ページ送りではなく **Enter** キーを押した。	SETUP メニューでオプション **1** を選択し直してからページ送りし、2 ページ目を表示します。選択項目を入力して、**Enter** キーを押します。

システム値の入力が完了したら、新しいシステム値を適用しなければなりません。

新しいシステム値の適用

システム値を入力したら、これらの値の一部を適用する必要があります。システム値に加えた変更の大部分は、直ちに有効になります。しかし、システムでのセキュリティー・レベルを変更すると、システムを停止して再始動するまで変更内容は有効になりません。「システム・オプションの変更」画面にすべての値を正しく入力したことを調べてから、新しい値を適用します。

注: ワークステーションをシステムに接続していない場合は、接続します。システムを開始すると、「システム・オプションの変更」画面で選択した命名形式を使用して、これらの装置が自動的に構成されます。

以下の手順を使用して、システムを停止してから再始動してください。システムを開始すると、「システム・オプションの変更」画面に入力した値が有効になります。

1. コンソールでサインオンしており、他のワークステーションがサインオンされていないことを確認します。
2. プロセッサー装置上のキーロック・スイッチが、通常位置にあることを確認します。
3. SETUP メニューで、「電源オンおよび電源オフ・タスク」オプションを選択します。
4. 「システムの即時電源遮断およびその後の電源投入」オプションを選択します。 **Enter** キーを押します。
5. 電源遮断要求の確認を要求する画面が表示されます。 **F16** (確認) を押します。

これで、システムは自動的に停止してから再始動します。画面は数分間、何も表示されません。続いて、サインオン画面が再表示されます。

新しいシステム値の適用が完了したら、システム上に自分で機密保護担当者プロファイルを作成しなければなりません。

機密保護担当者プロファイルの作成

システム上の**機密保護担当者**とは、*SECOFR ユーザー・クラスか、または *ALLOBJ 特殊権限および *SECADM 特殊権限を持つユーザーのことです。

「システム・オプションの変更」画面のシステム値を適用したら、自分と代理の機密保護担当者のユーザー・プロファイルを作成します。今後、機密保護担当者機能を実行する際には、QSECOFR プロファイルではなく、自分のプロファイルを使用してください。

1. QSECOFR としてシステムにサインオンし、SETUP メニューを要求します。

選択したシステム名が「サイン・オン」画面の右上に表示されることに注意してください。

```
                    サイン・オン
                                        システム . . . . :
                                        サブシステム . . :
                                        表示装置 . . . . :

  ユーザー . . . . . . . . . . . .  QSECOFR
  パスワード . . . . . . . . . . .  _________
  プログラム/プロシージャー. . . .  _________
  メニュー . . . . . . . . . . . .  SETUP
  現行ライブラリー . . . . . . . .  _________
```

2. SETUP メニューで「*ユーザー登録の処理*」オプションを選択します。「ユーザー登録の処理」画面に、システム上の現行プロファイルがリストされます。

   注: 「ユーザー・プロファイルの処理」画面が表示される場合は、 **F21** (操作援助レベルの選択) を押して、基本援助レベルに変更します。

3. 新しいプロファイルを作成するには、「*Opt*」(オプション) 列に **1** (追加) と入力し、「ユーザー」列に自分のプロファイルの名前を入力します。 **Enter** キーを押します。

```
                          ユーザー登録の処理

下のオプションを入力して、実行キーを押してください。
  1= 追加    2= 変更    3= コピー    4= 除去    5= 表示

OPT      ユーザー              記述
1        JONESS
QDOC                                内部文書ユーザー・プロファイル
QSECOFR                             機密保護担当者
```

4. 「ユーザーの追加」画面で、自分にパスワードを割り当てます。
5. サンプル画面に表示されるフィールドに、自分の該当する情報を記入します。
6. 画面の次ページにページ送りします。

```
                            ユーザーの追加

下の選択項目を入力して、実行キーを押してください。

ユーザー  . . . . . .  JONESS          名前
ユーザー記述  . . . . .  Jones, Sharon
パスワード  . . . . . .  SECRET         文字
ユーザーのタイプ  . . . .  *SECOFR      タイプ、リストは F4 キー
ユーザー・グループ  . . .  *NONE        名前、リストは F4 キー

コマンド入力行の使用制限    N           Y=YES, N=NO
省略時のライブラリー. . .               名前
省略時の印刷装置  . . . .  *WRKSTN     名前、*WRKSTN、リストは F4 キー
サイン・オン・プログラム    *NONE       名前、*NONE
  ライブラリー  . . . . .               名前

最初のメニュー  . . . . .               名前
  ライブラリー  . . . . .               名前
```

7. 画面の 2 ページ目に記入し、**Enter** キーを押します。
8. 「ユーザー登録の処理」画面の下部にある確認メッセージをチェックします。

9. **F3** (終了) を押して、 SETUP メニューに戻ります。

```
                          ユーザーの追加

下の選択項目を入力して、実行キーを押してください。

アテンション・キー・プログラム . . . .   *SYSVAL          名前、*SYSVAL、*ASSIST、*NONE
  ライブラリー  . . . . .                                  名前
```

考えられるエラー	回復
すべてのフィールドに情報を入力し終える前に、**Enter** キーを押した。	「ユーザー登録の処理」画面の「変更」オプションを使用して、作成したプロファイルを変更します。リストにプロファイルが表示されない場合は、 **F5** (最新表示) を押してページ送りし、見つけてください。

自分の機密保護担当者プロファイルの作成が完了したら、保守ツールのユーザーのユーザー ID とパスワードを変更する必要があります。詳細については、『保守ツール』のトピックを参照してください。

セキュリティーのシステム値の設定

このトピックでは、システム値の処理 (WRKSYSVAL) コマンドを使用してシステム値の変更と表示を行います。

必要な用紙

『全体的なセキュリティー戦略の計画』で作成したシステム値選択用紙の情報を入力してください。

システム値を設定するには、以下の作業を完了してください。

1. セキュリティー・システム値の変更。
2. 個別システム値の変更。

コマンド行インターフェースへのサインオン

以下の情報を使用して、システムにサインオンしてください。

プロファイル
独自のもの (*SECADM 権限と *ALLOBJ 権限が必須)

メニュー
MAIN

サインオンが完了したら、セキュリティー・システム値の変更を開始することができます。

セキュリティー・システム値の変更

システムへのサインオンが完了したら、この手順を使用して、システム値選択用紙の第 2 部に記述されているセキュリティー・システム値を入力してください。

1. コマンド行で `WRKSYSVAL *SEC` と入力し、**Enter** キーを押します。コマンド名の後の *SEC は、セキュリティーに関係のあるシステム値だけを表示するという意味です。
2. 「システム値の処理」画面で、変更したいシステム値の横にある「*OPT*」列に **2** (変更) と入力します。変更したいシステム値が画面に表示されていない場合は、表示されるまでページ送りします。

```
                              システム値の処理

 位置指定 . . . . . .                  システム値の開始文字
 タイプ別サブセット . . .  *SEC        リストは F4 キー

 オプションを入力して、実行キーを押してください。
   2= 変更   5= 表示

        System
Option  Value        Type        Description
      QINACTITV       *SEC      非活動ジョブ・タイムアウト
      QINACTMSGQ      *SEC      非活動ジョブ・メッセージ待ち行列
 2    QLMTDEVSSN      *SEC      装置セッション限界
      QLMTSECOFR      *SEC      機密保護担当者の装置アクセスの制約
      QMAXSGNACN      *SEC      サインオンの試みが失敗した場合の処置
      QMAXSIGN        *SEC      認められる最大サインオン試行回数
   ⋮
```

3. システム値として選択した項目を入力し、**Enter** キーを押します。「システム値の処理」画面が再表示されます。

```
                              システム値変更
 システム値 . . . . . :   QLMTDEVSSN
 記述 . . . . . :   装置セッション限界


 選択項目を入力して、実行キーを押してください。

   装置セッション限界 . . . . .   0          0= 制限なし
                                             1= 制限あり
```

4. 画面の下部の確認メッセージをチェックしてください。

考えられるエラー	回復
「システム値の処理」画面の例で表示されているものと違うシステム値が表示される。	*SEC を入力していません。ご使用の画面の上部にある「*タイプ別サブセット*」フィールドと、サンプル画面と比較してください。「*タイプ別サブセット*」フィールドにカーソルを移動させます。 *SEC と入力し、**Enter** キーを押してください。
指定したコマンドがシステムで処理されない。メニューが表示されたままである。	画面の下部のエラー・メッセージをチェックしてください。正しくないコマンド名を入力したと思われます。その後、再試行します。許可がないことがメッセージに示されている場合は、サインオフしてから、機密保護担当者権限を持つプロファイルを使用して再度サインオンしてください。
Enter キーを押すと、「システム値変更」画面が再表示される。	画面の下部のエラー・メッセージをチェックしてください。入力した選択項目が誤っていたか、または許可されている範囲外の値を選んだと思われます。追加情報については、**F1** (ヘルプ) を使用してください。
「システム値の処理」画面の代わりにメニューが表示される。	**Enter** キーを 2 回押したと思われます。 WRKSYSVAL *SEC と入力してください。
変更しないシステム値を選択した。	**F12** (取り消し) を押して、「システム値の処理」画面に戻ります。

* (アスタリスク) の意味

一部の値の前にアスタリスク (*) が付いていることに気付いたことでしょう。システムでは、アスタリスクを使用して、特殊値と正規の語の違いが示されます。たとえば、ユーザー・プロファイルのパスワードとして *NONE を指定すると、このプロファイルを使用しても誰もシステムにサインオンできないことを意味します。パスワードとして NONE を指定すると、ユーザーはパスワードとして文字 NONE を入力しなければなりません。

システムにセキュリティーを設定する際には、指示の中や用紙上でアスタリスクを使用するときに注意を払ってください。

セキュリティー・システム値の変更が完了したら、個別システム値を変更することができます。

個別システム値の変更

セキュリティー・システム値の変更が完了したら、個別システム値の変更することができます。

たとえば、切り離しジョブ・タイムアウト間隔 (QDSCJOBITV) システム値は、セキュリティー・システム値には含まれません。この値は、「システム値の処理」画面の *SEC サブセットには表示されません。QDSCJOBITV システム値や個別のシステム値を変更するには、以下の手順を使用してください。

1. WRKSYSVAL QDSCJOBITV と入力し、**Enter** キーを押します。
2. 「システム値の処理」画面で、 QDSCJOBITV の横にある「*OPT*」列に **2** (変更) と入力します。
3. QDSCJOBITV の選択項目を入力します。
4. 確認メッセージをチェックします。

```
                              システム値変更
システム値 . . . . . :   QDSCJOBITV
記述 . . . . . :   切り離されたジョブが終了するまでの時間間隔

選択項目を入力して、実行キーを押してください。

  時間間隔 (分数)  . . .   300           5 - 1440, *NONE
```

セキュリティー値のリスト

システム値選択用紙の情報をすべて入力したら、すべてのセキュリティー・システム値のリストを印刷できます。 WRKSYSVAL *SEC OUTPUT(*PRINT) と入力します。このリストのコピーとシステム値選択用紙を保管します。セキュリティー・システム値を変更した場合は、必ずリストを再度印刷します。

システム値選択用紙のシステム値の選択項目をすべて入力したら、アプリケーションのロードを行えます。

アプリケーションをロードするためのセキュリティー・ステップの実行

システム値を設定したら、アプリケーションをロードすることができます。このトピックには、アプリケーション・ライブラリーをシステムにロードするのに必要なセキュリティー・ステップが記述されています。プロファイルと他のセキュリティー・オブジェクトを作成したら、『所有権および共通権限の設定』と『資源保護の設定』に、アプリケーションの所有権と権限を確立する方法が説明されています。

可能な場合は、まずアプリケーション・ライブラリーをシステムにロードしてから、ユーザー・グループと個別プロファイルを設定してください。ジョブ記述とプロファイルを作成する際には、アプリケーション・オブジェクトを参照する必要があります。

グループおよび個別のプロファイルを作成する前にアプリケーションをロードできない場合は、以下のような警告メッセージが表示されることがあります。

- ジョブ記述の作成時、システムで初期ライブラリーが見つかりません。
- プロファイルの作成時、システムで初期プログラムまたはメニューが見つかりません。

アプリケーション・ライブラリーをロードするまでは、ジョブ記述やプロファイルのテストを正常に行えません。

『アプリケーションの導入の計画』で作成したアプリケーションの導入用紙を使用します。

個々のアプリケーションをロードするには、以下の作業をすべて実行してください。

1. 所有者プロファイルの作成。
2. アプリケーションのロード。

システムへのサインオン

- 所有者プロファイルを作成するには、以下のようにします。

  プロファイル
  独自のもの (*SECADM 権限が必要)

  メニュー
  MAIN

- アプリケーション・ライブラリーをロードするには、以下のようにします。

  アプリケーション・ライブラリーのロード時に機密保護担当者かアプリケーション所有者のどちらとしてサインオンすればよいか、アプリケーションの提供者に問い合わせてください。

サインオンが完了したら、アプリケーションの所有者プロファイルを作成できます。

所有者プロファイルの作成

システムにサインオンしたら、『アプリケーションの導入の計画』を調べて、アプリケーションをロードする前にプロファイルを作成する必要があるか調べてください。プロファイルを作成するには、以下のようにします。

1. CRTUSRPRF (ユーザー・プロファイル作成) と入力して、**F4** (プロンプト) を押します。
2. 「ユーザー・プロファイル作成」画面で、プログラマーかアプリケーションの提供者に指示されたとおりにフィールドに記入します。
3. **F10** (追加のパラメーター) を使用してページ送りし、追加のフィールドを表示します。

```
                ユーザー・プロファイル作成  (CRTUSRPRF)

選択項目を入力して、実行キーを押してください。

ユーザー・プロファイル  . . . .                 名前
ユーザー・パスワード  . . . . .  *USRPRF        文字値 , *USRPRF, *NONE
パスワードを満了にセット  . . .  *NO           *NO, *YES
状況  . . . . . .  *ENABLED      *ENABLED, *DISABLED
ユーザー・クラス  . . . . . .  *USER          *USER, *SYSOPR, *PGMR...
援助レベル  . . . . . .  *SYSVAL       *SYSVAL, *BASIC, *INTERMED...
現行ライブラリー  . . . . . .  *CRTDFT        名前 , *CRTDFT
呼び出す初期プログラム  . . . .  *NONE          名前 , *NONE
  ライブラリー  . . . . . .                     名前 , *LIBL, *CURLIB
初期メニュー  . . . . . .  MAIN           名前 , *SIGNOFF
  ライブラリー  . . . . . .    *LIBL        名前 , *LIBL, *CURLIB
制限機能  . . . . . .  *NO           *NO, *PARTIAL, *YES
テキスト ' 記述 ' . . . . . .  Owner of xxxxxx
```

4. 画面の下部のメッセージをチェックしてください。

注: 『グループ・プロファイルの作成』には、プロファイルの作成に関する詳細が記述されています。

アプリケーションの所有者の作成が完了したら、アプリケーションのロードを始められます。

アプリケーションのロード

アプリケーション・ライブラリーをロードする際には、アプリケーションの提供者の指示に従ってください。『所有権および共通権限の設定』では、アプリケーションに対する所有権と共通権限の設定方法が説明されています。

アプリケーションをすべてロードしたら、ユーザー・グループを設定することができます。

ユーザー・グループの設定

アプリケーションをロードするためのセキュリティー・ステップを実行したら、ユーザー・グループを設定できます。グループ・ライブラリー、ジョブ記述、およびグループ・プロファイルを作成します。 1 つのユーザー・グループに対してこのトピック全体の作業を行ったら、最初に戻り、それ以外のグループで同じステップを繰り返してください。サンプル画面では、JKL Toy Company の販売マーケティング部門のユーザー・グループ記述用紙と、倉庫部門のユーザー・グループ記述用紙の情報を示しています。

『ユーザー・グループの計画』で作成したユーザー・グループ記述用紙を使用します。

ユーザー・グループを設定するには、以下の作業をすべて実行してください。

1. ユーザー・グループのライブラリーの作成。
2. ジョブ記述の作成。
3. グループ・プロファイルの作成。

システムへのサインオン

プロファイル

独自のもの (*SECADM 権限が必要)

メニュー

MAIN

サインオンが完了したら、ユーザー・グループのライブラリーを作成することができます。

ユーザー・グループのライブラリーの作成

システムへのサインオンが完了したら、ユーザー・グループのライブラリーを作成する必要があります。オブジェクト (Query プログラムなど) のライブラリーを作成し、それをグループ内で共用するように計画している場合は、まずライブラリーを作成してからグループ・プロファイルを作成してください。

1. CRTLIB (ライブラリー作成) と入力して、**F4** (プロンプト) を押します。
2. 画面に入力します。ライブラリー名はグループ・プロファイル名にしてください。
3. **F10** (追加のパラメーター) を押します。
4. ライブラリーの共通権限と、そのライブラリーで作成される新しいオブジェクトを記入します。
5. **Enter** キーを押します。確認メッセージをチェックします。

```
                        ライブラリー作成  (CRTLIB)

選択項目を入力して、実行キーを押してください。

ライブラリー  . . . . . .   DPTWH          名前
ライブラリー・タイプ  . . . . .   *PROD        *PROD, *TEST
テキスト ' 記述 ' . . . . . .   Warehouse Library

                     追加のパラメーター

権限  . . . . . .   *USE          名前 , *LIBCRTAUT...
補助記憶域プール ID . . . . . .   1            1-32
作成権限  . . . . . .   *CHANGE       名前 , *SYSVAL, *CHANGE...
オブジェクト監査の作成  . . . .   *SYSVAL       文字値 , *SYSVAL, *NONE...
```

考えられるエラー	回復
ライブラリーの説明を入力し終える前に、**Enter** キーを押した。	**CHGLIB** と入力して、**F4** (プロンプト) を押してください。プロンプト画面にライブラリー名を入力して、**Enter** キーを押します。そして、「ライブラリー変更」画面に説明を入力します。
ライブラリーに付けた名前が間違っていた。	オブジェクト名前変更 (RNMOBJ) コマンドを使用してください。

グループのライブラリーの作成が完了したら、ジョブ記述を作成することができます。

ジョブ記述の作成

グループのライブラリーの作成が完了したら、グループごとにジョブ記述を作成することができます。

初期ライブラリー・リストに必要なライブラリーがまだシステム上にない場合は、ジョブ記述を作成する際に警告メッセージが表示されます。

1. **CRTJOBD** (ジョブ記述作成) と入力して、**F4** (プロンプト) を押します。
2. 以下のフィールドに記入します。

   ジョブ記述:
   グループ・プロファイル名と同じ。

   ライブラリー名:
   QGPL

   テキスト:
   グループの説明

3. **F10** (追加のパラメーター) を押します。
4. 「*初期ライブラリー・リスト*」フィールドにページ送りします。

```
                        ジョブ記述作成  (CRTJOBD)

選択項目を入力して、実行キーを押してください。

ジョブ記述  . . . . . .  DPTSM          名前
  ライブラリー  . . . . .  QGPL          名前 , *CURLIB
ジョブ待ち行列  . . . . .  QBATCH        名前
  ライブラリー  . . . . .    *LIBL       名前 , *LIBL, *CURLIB
ジョブ優先順位 (JOBQ での) . .  5            1-9
出力優先順位 (OUTQ での) . . .  5            1-9
印刷装置  . . . . . .  *USRPRF       名前 , *USRPRF, *SYSVAL...
出力待ち行列  . . . . . .  *USRPRF       名前 , *USRPRF, *DEV, *WRKSTN
  ライブラリー  . . . . .                名前 , *LIBL, *CURLIB
テキスト ' 記述 ' . . . . . .  Sales and Marketing
```

5. 「*初期ライブラリー・リスト*」フィールドの *SYSVAL の上に **+** (プラス符号) を入力し、値のリストを入力することを指定します。 **Enter** キーを押します。

```
                        ジョブ記述作成  (CRTJOBD)

選択項目を入力して、実行キーを押してください。

会計コード  . . . . . .  *USRPRF
経路指定データ  . . . . . .  QCMDI

要求データまたはコマンド  . . .  *NONE
  :
CL 構文検査  . . . . . .  *NOCHK       0-99, *NOCHK
初期ライブラリー・リスト  . . . > +            名前 , *SYSVAL, *NONE
              値の続きは+
```

6. 「*初期ライブラリー・リスト*」フィールドに、ユーザー・グループ記述用紙でマーク (✓) を付けたライブラリーの名前を入力します。
   - 1 行に 1 つずつライブラリー名を記入します。
   - QGPL と QTEMP を含めます。すべてのジョブは QTEMP というライブラリーを使用して一時オブジェクトを保管します。**すべての初期ライブラリー・リストに QTEMP ライブラリーがなければなりません**。ほとんどのアプリケーションの場合、初期ライブラリー・リストに QGPL ライブラリーもなければなりません。
   - ライブラリー・リストに現行 (省略時) ライブラリーを含める必要はありません。このライブラリーはサインオン時にシステムによって自動的に追加されます。
7. **Enter** キーを押します。メッセージをチェックします。 (すべてのメッセージを調べるには、ページ送りします。)

```
                    パラメーターの追加の値の指定     INLLIBL

選択項目を入力して、実行キーを押してください。

初期ライブラリー・リスト  . . . > CUSTLIB        名前 , *SYSVAL, *NONE
                                  ITEMLIB
                                  COPGMLIB
                                  ICPGMLIB
                                  QGPL
                                  QTEMP
```

考えられるエラー	回復
F10 ではなく **Enter** キーを押した。	初期ライブラリー・リストに正しいライブラリーを含めるには、**CHGJOBD** (ジョブ記述の変更) と入力してから、**F4** を押してください。
ジョブ記述を作成しようとしたら、エラー・メッセージが表示された。	エラー・メッセージが表示される最も一般的な原因は、システム上にないライブラリーを含めようとすることにあります。これは警告メッセージです。このような場合でも、ジョブ記述は初期ライブラリー・リストにあるライブラリーを使って作成されます。該当するライブラリーがシステム上にないと、このジョブ記述を指定したプロファイルを使ってサインオンできません。 該当するライブラリーがシステム上にある場合は、入力した名前が間違っていた可能性があります。ライブラリー名を調べて、再試行してください。

ジョブ記述の作成が完了したら、グループ・プロファイルを作成することができます。

グループ・プロファイルの作成

ジョブ記述の作成が完了したら、グループ・プロファイルを作成することができます。この作業を行うには、ユーザー・グループ記述用紙の第 2 部の情報を使用します。

1. ユーザー・プロファイル処理コマンドを使用します。 WRKUSRPRF *ALL と入力します。最初に、IBM 提供のプロファイルがリストされます。

   注: 「ユーザー登録の処理」画面が表示される場合は、**F21** を押して、中間操作援助レベルに変更します。

2. 新しいプロファイルを作成するには、「*OPT*」(オプション) 列に **1** と入力し、「*ユーザー・プロファイル*」列にプロファイルの名前を入力します。**Enter** キーを押します。

```
                          ユーザー・プロファイルの処理

オプションを入力して、実行キーを押してください。
  1= 作成    2= 変更    3= コピー    4= 削除    5= 表示
  12= 所有者によるオブジェクトの処理

       ユーザー・
 OPT   プロファイル     テキスト
1     DPTSM
      QDOC                      内部文書ユーザー・プロファイル
      QSECOFR                   機密保護担当者
```

3. ユーザー・グループ記述用紙の情報を、該当するフィールドに入力します。

4. **タブ・**キーを使用して、デフォルトを使用するフィールドをすべてスキップします。
5. **F10** (追加のパラメーター) を押します。
6. ページ送りします。

```
                    ユーザー・プロファイル作成  (CRTUSRPRF)

選択項目を入力して、実行キーを押してください。

ユーザー・プロファイル  . . . . > DPTSM          名前
ユーザー・パスワード  . . . . .   *NONE          名前 , *USRPRF, *NONE
パスワードを満了にセット  . . .   *NO           *NO, *YES
状況  . . . . . . . . . . . . .   *ENABLED      *ENABLED, *DISABLED
ユーザー・クラス  . . . . . . .   *USER         *USER, *SYSOPR, *PGMR...
援助レベル  . . . . . . . . . .   *SYSVAL       *SYSVAL, *BASIC, *INTERMED...
現行ライブラリー  . . . . . . .   *CRTDFT        名前 , *CRTDFT
呼び出す初期プログラム  . . . .   CPSETUP        名前 , *NONE
  ライブラリー  . . . . . . . .     CPPGMLIB     名前 , *LIBL, *CURLIB
初期メニュー  . . . . . . . . .   CPMAIN         名前 , *SIGNOFF
  ライブラリー  . . . . . . . .     CPPGMLIB     名前 , *LIBL, *CURLIB
制限機能  . . . . . . . . . . .   *YES          *NO, *PARTIAL, *YES
テキスト ' 記述 ' . . . . . . .   SALES AND MARKETING DEPARTMENT
```

7. ユーザー・グループ記述用紙の残りのフィールドを画面の追加のページに入力し、**Enter** キーを押します。

```
                    ユーザー・プロファイル作成  (CRTUSRPRF)

選択項目を入力して、実行キーを押してください。


                  追加のパラメーター

特殊権限  . . . . . . . . . . .   *USRCLS       *USRCLS, *NONE, *ALLOBJ...

 :
ジョブ記述  . . . . . . . . . .   DPTSM          名前
  ライブラリー  . . . . . . . .     QGPL         名前 , *LIBL, *CURLIB
```

```
                    ユーザー・プロファイル作成  (CRTUSRPRF)

選択項目を入力して、実行キーを押してください。

グループ権限  . . . . . . . . .   *NONE         *NONE、*ALL、*CHANGE、*USE...

 :
印刷装置  . . . . . . . . . . .   PRT03          名前、*WRKSTN、*SYSVAL
```

8. メッセージをチェックします。

留意点

グループ・プロファイルは単に特殊なタイプのユーザー・プロファイルです。多くのメッセージと画面では、グループ・プロファイルがユーザーまたはユーザー・プロファイルと見なされます。グループ・プロファイルにメンバーを追加したり、グループ識別番号 (gid) を割り当てたりした場合にのみ、システムはグループ・プロファイルが作成されたことを認識します。

考えられるエラー	回復
グループ・プロファイルに値をすべて入力し終える前に、**Enter** キーを押した。	**F5** (最新表示) を押して、作成したプロファイルを「ユーザー・プロファイル処理」画面に追加します。次に、オプション **2** (変更) を使用して、プロファイルを訂正します。
間違った名前を使用してプロファイルを作成した。	プロファイルの名前は変更できません。コピー・オプション (**3**) を使用して、正しい名前で新しいプロファイルを作成してください。そして、間違った名前のプロファイルを削除します (オプション **4**)。
ユーザー・グループ記述用紙のフィールドの一部が画面に表示されない。	中間操作援助レベルを使用しているか確認してください。基本援助レベル・バージョンの「ユーザー・プロファイル作成」画面を、「ユーザーを追加」画面といいます。操作援助レベルを変更するには、**F12** (取り消し) を押して、「ユーザー登録の処理」画面に戻ります。 **F21** を使用して、操作援助レベルを変更します。『正しい操作援助レベルの選択』を参照してください。
「ユーザー・プロファイル作成」画面から、デフォルト情報の一部を不慮に消去してしまった。	フィールドをブランクのままにしておくと、ユーザー・プロファイルの作成時にデフォルトが使用されます。デフォルトを参照したい場合は、**F5** (最新表示) を押して、画面全体を復元します。情報を再び入力してください。

結果のリスト

システム上のすべてのプロファイルの名前と記述をリストするには、権限ユーザー表示 (DSPAUTUSR) コマンドを使用します。 `DSPAUTUSR OUTPUT(*PRINT)` と入力してください。すべてのグループ・プロファイルがパスワード *NONE を持っているか調べてください。

以下の作業を完了してから、個々のユーザーを設定してください。

- ユーザー・グループごとにジョブ記述を作成する。
- グループごとにライブラリーを作成する (オプション)。
- ユーザー・グループごとにグループ・プロファイルを作成する。

個々のユーザーの設定

ユーザー・グループを設定すると、グループ・プロファイルを作成するためのステップを完了したことになります。ここで、グループのメンバーの個別プロファイルを作成します。

1 つのユーザー・グループのメンバーについてトピック全体の作業を行ったら、最初に戻り、それ以外のグループで同じステップを繰り返してください。サンプル画面では、JKL Toy Company で、Sharon Jones が

販売マーケティング部門、および倉庫部門のために作成した個別ユーザー・プロファイル用紙からユーザーを取り出して示しています。これらの用紙のコピーは、『個々のユーザー・プロファイルの計画』にあります。

『個々のユーザー・プロファイルの計画』で作成した個別ユーザー・プロファイル用紙を使用します。

グループのメンバーの個別プロファイルを作成するには、次の作業を完了させてください。

1. 個人ライブラリーの作成 (任意選択)。
2. グループ・プロファイルのコピー。
3. パスワードの期限満了の設定。
4. 追加ユーザーの作成。(任意選択)

   注: すべてのグループ・メンバー用のユーザー・プロファイルを作成するまで、個人ライブラリーの作成と追加ユーザーの作成を繰り返してください。
5. ユーザー情報の変更 (必要な場合)。
6. 結果の表示。

システムへのサインオン

プロファイル

独自のもの (*SECADM 権限が必要)

メニュー

SETUP

個人ライブラリーの作成

個々のユーザーの設定を開始するには、オブジェクトのメンバーごとに、Query プログラムなどの個人ライブラリーを作成しなければならない場合があります。個人ライブラリーは、個別のユーザー・プロファイルを作成する前に作成してください。

1. **CRTLIB** と入力して、**F4** (プロンプト) を押します。
2. ライブラリーにユーザー・プロファイルと同じ名前を指定します。
3. **F10** (追加のパラメーター) を押します。
4. ライブラリーの共通権限と、そのライブラリーで作成される新しいオブジェクトを記入します。
5. **Enter** キーを押します。確認メッセージをチェックします。

```
                          ライブラリー作成  (CRTLIB)

選択項目を入力して、実行キーを押してください。

ライブラリー  . . . . . > DPTSM          名前
ライブラリー・タイプ  . . . . .  *PROD        *PROD, *TEST
テキスト ' 記述 ' . . . . . > 'WAREHOUSE LIBRARY'

                      追加のパラメーター

権限  . . . . . .  *EXCLUDE      名前 , *LIBCRTAUT...
補助記憶域プール ID . . . . . .  1            1-32
作成権限  . . . . . .  *CHANGE       名前 , *SYSVAL, *CHANGE...
オブジェクト監査の作成  . . . .  *SYSVAL       文字値 , *SYSVAL, *NONE...
```

個人ライブラリーを作成したら、グループ・プロファイルをコピーすることにより、個別のプロファイルを作成できます。

グループ・プロファイルのコピー

グループ・プロファイルには、次の 2 つの役割があります。

1. システムはグループ・プロファイルを使用して、グループ・メンバーにオブジェクトを使用する許可があるかどうかを判別します。
2. グループ・メンバーを、個別のユーザー・プロファイルを作成するためのパターンとして使用できます。

ユーザー・グループを設定すると、グループ・プロファイルを作成したことになります。ここで、グループ・プロファイルをコピーして個別のプロファイルを作成し、さらに個別のプロファイルをコピーしてグループ内の他のプロファイルを作成することができます。

1. SETUP メニューから「ユーザー登録の処理」オプションを選択します。

   注: 「ユーザー・プロファイルの処理」画面が表示される場合は、**F21** (操作援助レベルの選択) を使用して、基本援助レベルに変更してください。

2. ユーザー・グループの前にある *OPT* 列に **3** (コピー) を入力します。「ユーザーのコピー」画面が表示されます。 (コピーしたいユーザー・グループが画面に表示されていない場合、見つかるまでページ送りを行ってください。) システムは「ユーザー名」フィールドをブランクのままにし、残りのフィールドには、コピーしたグループ・プロファイルからの情報を記入します。

```
                          ユーザー登録の処理

下のオプションを入力して、実行キーを押してください。
  1= 追加   2= 変更   3= コピー   4= 除去   5= 表示

OPT     ユーザー        記述

        DPTSM           SALES AND MARKETING DEPARTMENT
3       DPTWH           WAREHOUSE DEPARTMENT
```

3. 作成しているユーザー・プロファイルの名前と記述を入力します。
4. パスワードはブランクのままにしておきます。システムは、自動的にパスワードを新しいユーザー・プロファイル名と同じものにします。
5. グループ・プロファイル名を「ユーザー・グループ」フィールドに入れます。
6. 個々のユーザー・プロファイル用紙を調べて、ユーザーにグループとは異なる他の値があるかどうかを確認します。それらの値を入力します。
7. ページ送りをします。

```
                        ユーザーのコピー

コピー元ユーザー  . . . :   DPTWH

下の選択項目を入力して、実行キーを押してください。

ユーザー  . . . . . .   WILLISR          名前
ユーザー記述  . . . . . .   Willis,Rose
パスワード  . . . . . .                   文字
ユーザーのタイプ  . . . .   *SYSOPR         タイプ、リストは F4 キー
ユーザー・グループ  . . .   DPTWH           名前、リストは F4 キー

コマンド入力行の使用制限    N               Y=YES、N=NO

省略時のライブラリー  . .   DPTWH           名前
省略時の印刷装置  . . . .   PRT04           名前、*WRKSTN、リストは F4
サイン・オン・プログラム.   *NONE           名前、*NONE
  ライブラリー  . . . . .                   名前

最初のメニュー  . . . . .   ICPMAIN         名前
  ライブラリー  . . . . .     ICPGMLIB      名前
```

8. 画面の次のページで、必要な変更をすべて行ってから、**Enter** キーを押します。
9. 「ユーザー登録の処理」画面の下部にある確認メッセージをチェックします。

```
                        ユーザーのコピー

コピー元ユーザー  . . . :   DPTWH

下の選択項目を入力して、実行キーを押してください。

アテンション・キー・
  プログラム  . . . . . .   *SYSVAL         名前、*SYSVAL、*ASSIST、*NONE
  ライブラリー  . . . . .                   名前
```

考えられるエラー	回復
「ユーザーのコピー」画面の代わりに「ユーザー・プロファイル作成」画面が表示される。	**F12** (取り消し) を使用して、「ユーザー・プロファイル処理」画面に戻ります。 **F21** を使用して、基本援助レベルに変更します。コピー操作を再び開始します。
選択したユーザー・プロファイル名がユーザー・プロンプトに収まりきらない。	ユーザー・プロファイル名は 10 文字までですが、「ユーザーのコピー」および「ユーザーの追加」画面では 8 文字を超える名前はサポートしていません。短いユーザー名を選択するか、または中間操作援助レベルを使用して個別のユーザー・プロファイルを作成してください。

ユーザー・プロファイルのテスト

グループ内に最初の個別プロファイルを作成するときに、そのプロファイルを使用してサインオンすることにより、プロファイルをテストしなければなりません。最初のメニューが正しく表示され、サインオン・プログラムが実行されるかどうか検証します。

そのプロファイルを使用してサインオンが正常に行えない場合、システムは、そのプロファイルで指定されているものを検出できなかった可能性があります。それは、サインオン・プログラム、ジョブ記述、または

初期ライブラリー・リストのライブラリーの 1 つであるかもしれません。「印刷装置出力の処理」画面を使用して、サインオンの試行時に作成されたジョブ・ログを見つけてください。ジョブ・ログを調べれば、どのようなエラーが起こったのかがわかります。

セキュリティーを変更するときに問題をテストし、診断するための情報については、『セキュリティーのテスト』を参照してください。

ユーザー・プロファイルのテストが完了したら、パスワードの期限満了を設定することができます。

パスワードの期限満了の設定

ユーザーが初めてサインオンを行うときに、個別プロファイルで、ユーザーにパスワードの変更を求めるように設定します。「*パスワードを満了にセット*」フィールドは、基本援助レベルバージョンの「ユーザーのコピー」画面には表示されません。コピー機能を使用してユーザー・プロファイルを作成した場合は、その後でユーザー・プロファイルを個別に変更する必要があります。「*パスワードを満了にセット*」フィールドを変更するには、CHGUSRPRF *profile-name* PWDEXP(*YES) と入力します。

注: ユーザー・プロファイルを使ってサインオンすることにより、ユーザー・プロファイルをテストする場合は、パスワードの期限満了を設定する*前* にテストを行ってください。

考えられるエラー	回復
プロファイルをテストして、パスワードを変更するように強制された。	**CHGUSRPRF** *profile-name* と入力して、 **F4** (プロンプト) を押します。パスワードをユーザー・プロファイル名に戻します。 (「パスワード」フィールドにユーザー・プロファイル名を入力します。) 「*パスワードを満了にセット*」フィールドに、***YES** と入力します。これを行うには、中間操作援助レベルが必要です。

最初の個別のユーザー・プロファイルを作成したら、追加ユーザーを作成することができます。

追加ユーザーの作成

グループ・プロファイルをコピーして、最初の個別プロファイルを作成したら、追加ユーザーを作成することができます。まず最初の個別のユーザー・プロファイルをコピーして、グループ内に追加メンバーを作成します。コピー機能を使用して個別プロファイルを作成する際には、それぞれの個別プロファイルをよく見てください。個々のユーザー・プロファイル用紙を確認して、新しいユーザー・プロファイル用の固有のフィールドを必ず変更してください。

1. 「ユーザー登録の処理」画面で、コピーしたいプロファイルの前に、**3** (コピー) と入力します。
2. 「ユーザーのコピー」画面で、プロファイル名と記述を入力します。
3. 新しいユーザー用の固有のフィールドに情報を入力します。

考えられるエラー	回復
コピーしたいプロファイルが、「ユーザー登録の処理」画面に表示されない。	**F5** (最新表示) を押します。ページ戻しおよびページ送りを行います。リストにはプロファイル名がアルファベット順に表示されます。

ユーザーの情報を更新したい場合は、『ユーザー情報の変更』を参照してください。

ユーザー情報の変更

一部のユーザーにとっては、「ユーザーのコピー」画面に表示されない値を設定しなければならないことがあります。たとえば、ユーザーによっては複数のグループ・プロファイルに属していることがあります。コピー機能を使用してユーザー・プロファイルを作成したら、それを変更することができます。

1. 「ユーザー登録の処理」画面で、**F21** を押して、中間操作援助レベルに変更します。
2. 「ユーザー・プロファイルの処理」画面で、変更したいプロファイルの横にある *OPT* (オプション) 列に **2** (変更) と入力します。 **Enter** キーを押します。

```
                        ユーザー・プロファイルの処理

オプションを入力して、実行キーを押してください。
  1= 作成    2= 変更    3= コピー    4= 削除    5= 表示
  12= 所有者によるオブジェクトの処理

      ユーザー・
OPT   プロファイル     テキスト
2     AMESJ          AMES,JANICE
      DPTSM          SALES AND MARKETING DEPARTMENT
      QDOC           内部文書ユーザー・プロファイル
      QSECOFR        機密保護担当者
      WAGNERR        WAGNER,RAY
      WILLISR        Willis,Rose
```

3. 「ユーザー・プロファイル変更」画面で、**F10** (追加のパラメーター) を押します。
4. 変更したいフィールドが見つかるまでページ送りを行います。たとえば、ユーザーを追加のグループ・プロファイルのメンバーにする場合は、「*補足グループ*」フィールドが見つかるまでページ送りを行います。
5. 必要な値を入力して、**Enter** キーを押します。確認メッセージが表示されます。「ユーザー・プロファイルの処理」画面をもう一度ご覧ください。

```
                  ユーザー・プロファイル変更  (CHGUSRPRF)

選択項目を入力して、実行キーを押してください。

最大許容記憶域  . . . . . .   *NOMAX        キロバイト、*SAME、*NOMAX
最高スケジュール優先順位  . . .  3           0-9、*SAME
ジョブ記述  . . . . . .       DPTWH        名前、*SAME
ライブラリー  . . . . . .     QGPL         名前、*LIBL、*CURLIB
グループ・プロファイル  . . . .  DPTWH        名前、*SAME、*NONE
所有者  . . . . . .           *GRPPRF      *SAME、*USRPRF、*GRPPRF
グループ権限  . . . . . .     *USE         *SAME、*NONE、*ALL...
グループ権限タイプ  . . . . . .  *PGP        *PRIVATE、*PGP、*SAME
補足グループ  . . . . . .     DPTIC        名前、*SAME、*NONE
            値の続きは+
```

ユーザー情報を変更した後、結果を表示して、プロファイルを検査することができます。

ユーザー・プロファイルの表示

作成したプロファイルを表示するには、次の方法を使用することができます。

1 つのプロファイルの表示
「ユーザー登録の処理」画面または「ユーザー・プロファイルの処理」画面のいずれかで、オプション **5** (表示) を使用します。

1 つのプロファイルのリスト
ユーザー・プロファイル表示コマンド、DSPUSRPRF *profile-name* DETAIL(*BASIC) OUTPUT(*PRINT) を使用します。

グループ・メンバーの表示
DSPUSRPRF *group-profile-name* *GRPMBR と入力します。 OUTPUT(*PRINT) を使用すると、リストを印刷できます。

すべてのプロファイルのリスト
すべてのプロファイルの名前と記述をグループごとに分けてリストするには、許可ユーザーの表示コマンド、DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT) を使用します。

所有権と共通権限を設定する前に、次の作業を完了させてください。

- 個別のユーザー・プロファイルをすべて作成する。
- プロファイルごとにパスワードの期限満了を設定する。
- グループごとに分けられているすべてのプロファイルのリストを印刷し、それをユーザー・グループ記述用紙に保存する。新しいユーザーを追加したら、リストを再び印刷する。

資源保護の設定

このトピックでは、アプリケーションに対する特定権限を設定するとともに、オブジェクトの所有権および共通権限も確立します。さらに、ワークステーションと印刷装置の資源保護も設定します。 1 つのライブラリーについてトピック全体の作業を行ったら、最初に戻り、それ以外のライブラリーで同じステップを繰り返してください。 1 つのアプリケーションの資源保護の設定を完了したら、そのステップを他のアプリケーションで繰り返します。

これらの手順は、新しいアプリケーションをシステムに導入するとき、または資源保護を既存のアプリケーションに設定するときに、必ず使用するものです。

このトピックのサンプル画面では、JKL Toy Company の権限リスト用紙、ライブラリー記述用紙、さらに出力待ち行列およびワークステーションのセキュリティー用紙を示しています。これらの用紙の例は、『所有権および共通権限の設定』にあります。

必要な用紙

- 『アプリケーションの導入の計画』で作成したアプリケーションの導入用紙
- 『オブジェクトのグループ化』で作成した権限リスト用紙
- 『ライブラリーとオブジェクトの所有権の決定』で作成したライブラリー記述用紙
- 『印刷装置出力の保護』および『ワークステーションの保護』で作成した出力待ち行列およびワークステーションのセキュリティー用紙
- 『全体的なセキュリティー戦略の計画』で作成したシステム責任用紙

資源保護を設定するには、いくつかの方法があります。このトピックにある一連のステップは、アプリケーションの導入用紙、権限リスト用紙、およびライブラリー記述用紙に含まれている情報の順序と一致しています。

1. 所有権および共通権限の設定
2. 権限リストの作成
3. 権限リストによるオブジェクトの保護
4. 権限リストへのユーザーの追加
5. 特定権限の設定
6. 印刷装置出力の保護
7. ワークステーションの保護
8. システム操作員のメッセージ待ち行列へのアクセスの制限

所有権および共通権限の設定

このトピックでは、アプリケーション、ライブラリー、および個人ライブラリーの所有権および共通権限を確立します。 1 つのアプリケーションについてトピック全体の作業を行ったら、最初に戻り、それ以外のアプリケーションで同じステップを繰り返してください。サンプル画面には、Sharon Jones が『アプリケーションの導入の計画』で、顧客注文アプリケーションについて作成したアプリケーションの導入用紙が示されています。

このトピックの手順は、新しいアプリケーションをシステムに導入するとき、またはセキュリティーを既存のアプリケーションに設定するときに、必ず使用するものです。

『アプリケーションの導入の計画』で作成したアプリケーションの導入用紙を使用します。

所有権と共通権限を設定するには、次の作業を完了させてください。

1. 所有者プロファイルの作成
2. ライブラリー所有権の変更
3. アプリケーション・オブジェクトの所有権の設定
4. ライブラリーへの共通アクセスの設定
5. ライブラリーにあるすべてのオブジェクトの共通権限の設定
6. 新しいオブジェクトの共通権限の設定
7. グループおよび個人ライブラリーの処理

システムへのサインオン

プロファイル
独自のもの (*ALLOBJ 権限が必要)

メニュー
MAIN

所有者プロファイルの作成

所有者プロファイルがまだ存在しない場合は、次のことを行ってください。

- CRTUSRPRF (ユーザー・プロファイル作成) コマンドを使用して、ユーザー・プロファイルを作成します。パスワードを *NONE に設定します。

所有者プロファイルがすでに存在する場合は、次のことを行ってください。

- CHGUSRPRF (ユーザー・プロファイル変更) コマンドを使用して、パスワードを *NONE に設定します。

所有者プロファイルを作成したら、 ライブラリー所有権を変更することができます。

ライブラリー所有権の変更

このステップでは、ライブラリーにあるオブジェクトではなく、ライブラリーの所有権を変更します。

重要: アプリケーション・オブジェクトの所有権を変更する前に、必ずアプリケーションの提供者に確認してください。アプリケーションによっては、特定のオブジェクト所有権に関係している機能を使用するものがあります。

1. CHGOBJOWN (オブジェクト所有者変更) を入力して、**F4** (プロンプト) を押します。
2. ライブラリー名、オブジェクト・タイプ (*LIB)、および新規所有者を記入します。
3. 確認メッセージをチェックします。

```
                    オブジェクト所有者変更  (CHGOBJOWN)

選択項目を入力して、実行キーを押してください。

オブジェクト  . . . . . .   COPGMLIB       名前
  ライブラリー  . . . . . .   *LIBL         名前、*LIBL、*CURLIB
オブジェクト・タイプ  . . . . .   *LIB          *ALRTBL、*AUTL、*BNDDIR...
新しい所有者  . . . . . .   COWNER         名前
現行の所有者権限  . . . . . .   *REVOKE       *REVOKE、*SAME
```

考えられるエラー	回復
エラー・メッセージを受信した。	最も一般的なメッセージは、ライブラリーが見つからないか、または新規の所有者プロファイルが見つからないというものです。入力した内容にエラーがないか確認してから、再試行してください。

ライブラリー所有権の変更が完了したら、アプリケーション・オブジェクトの所有権を設定することができます。

アプリケーション・オブジェクトの所有権の設定

アプリケーション・オブジェクトの所有権を変更する場合、各オブジェクトを 1 つずつ変更しなければならないため、手間のかかる作業となります。可能であれば、プログラマーまたはアプリケーションの提供者に連絡して、所有権を確立するように依頼してください。

ライブラリーのオブジェクトのリスト

所有権を変更する前に、ライブラリー表示コマンドを使用して、ライブラリーにあるすべてのオブジェクトのリストを印刷します。これを、チェックリストとして使用できます。それには、DSPLIB *library-name* *PRINT と入力してください。

最適な方法の選択

アプリケーション・ライブラリーにあるオブジェクトの所有権を変更するには、次の 2 つの方法のどちらかを選択します。

表 61. オブジェクト所有権を変更するための方法

方法	何を行うか	いつ使用するか
所有者によるオブジェクト処理コマンド	プロファイルが所有するすべてのオブジェクトをリストする画面を表示します。画面上のオプションを使用して、オブジェクトの所有者を変更します。	この方法は簡単に使用できます。しかし、QPGMR または QSECOFR のどちらかがオブジェクトを所有する場合、 IBM では、この方法の使用をお勧めできません。これらのプロファイルは多くのオブジェクトを所有しており、リストを表示すると非常に大きなものになります。
オブジェクト所有者変更コマンド	オブジェクトごとに別々のコマンドを使用することが必要です。しかし、コマンド複写 *(Retrieve)* (**F9**) を使用して直前のコマンドを繰り返し、必要なタイプ入力の量を減らすことができます。	QPGMR または QSECOFR のどちらかがオブジェクトを所有する場合は、この方法を使用した方が速く処理されます。

所有者によるオブジェクト処理 (WRKOBJOWN) コマンドの使用: この方法は、QPGMR または QSECOFR などの IBM 提供のプロファイルがオブジェクトを所有しない 場合に、ライブラリーにあるオブジェクトの所有権を変更するために使用します。

1. WRKOBJOWN *owner-profile-name* と入力します。画面に、ユーザー・プロファイルが所有するすべてのオブジェクトのリストが表示されます。
2. 作業中のライブラリーにあるそれぞれのオブジェクトの前に、 **9** (所有者の変更) を入力します。
3. 画面の下部にあるパラメーターまたはコマンド 行に、 NEWOWN(*owner-profile-name*) を入力して、**Enter** キーを押します。
4. システムは、指示された各オブジェクトの所有者を、下部に入力された新しい所有者に変更します。画面の下部に、確認メッセージが表示されます。プロファイルはもうオブジェクトを所有していないため、画面には表示されなくなります。
5. ライブラリーにあるすべてのオブジェクトの所有権を変更するまで、 2 と 4 のステップを繰り返します。

```
                        所有者によるオブジェクトの処理

ユーザー・プロファイル . . :   OLDOWNER

オプションを入力して、実行キーを押してください。
   2= 権限の編集    4= 削除    5= 権限の表示    7= 名前の変更
   8= 記述の表示    9= 所有者の変更

OPT   オブジェクト          ライブラリー  タイプ     属性
      COPGMMSG              COPGMLIB      *MSGQ
9     CUSTMAS               CUSTLIB       *FILE
9     CUSTMSGQ              CUSTLIB       *MSGQ
      ITEMMSGQ              ITEMLIB       *MSGQ


  :

パラメーターまたはコマンド
===> NEWOWN(COWNER)
 F3= 終了       F4= プロンプト     F5= 最新表示    F9= コマンドの複写    F11= 記述の表示
 F12= 取り消し    F17= 最上部    F18= 最下部     F22= 名前全体の表示
```

考えられるエラー	回復
「オブジェクト所有者変更」画面が表示される。	この画面は、オプション **9** (所有者の変更) を指定して、「所有者によるオブジェクトの処理」画面の下部にパラメーターを何も入力しない場合に表示されます。さらにこの画面は、パラメーターを間違えて入力した場合にも表示されます。 **F12** (取り消し) を押して、「所有者によるオブジェクトの処理」画面に戻ります。その後、再試行します。例に示されているように、必ずパラメーターを入力してください。

オブジェクト所有者の変更コマンドを使用して、QPGMR または QSECOFR によって所有されているオブジェクトの所有権を変更します。

オブジェクト所有者変更コマンドの使用: この方法は、QPGMR または QSECOFR がオブジェクトを所有する 場合に、ライブラリーにあるオブジェクトの所有者を変更するために使用します。

1. CHGOBJOWN と入力して、**F4** (プロンプト) を押します。
2. 画面に、リスト内の最初のオブジェクトについての情報を入力して、**Enter** キーを押します。

```
                  オブジェクト所有者変更  (CHGOBJOWN)

選択項目を入力して、実行キーを押してください。

オブジェクト  . . . . . .  CUSTMAS       名前
ライブラリー  . . . . . .  CUSTLIB       名前、*LIBL、*CURLIB
オブジェクト・タイプ  . . . . .  *FILE        *ALRTBL、*AUTL、*BNDDIR...
新しい所有者  . . . . . .  COWNER       名前
現行の所有者権限  . . . . . .  *REVOKE      *REVOKE、*SAME
```

3. オブジェクト所有権が変更されたことを示す確認メッセージが表示されます。リストの項目のチェックを外します。
4. **F9** (検索) を押して、入力したコマンドを検索します。
5. **F4** (プロンプト) を押します。「オブジェクト所有者変更」画面で、ライブラリーにある次のオブジェクトの情報を入力し、**Enter** キーを押します。
6. ライブラリーにあるオブジェクトごとに、ステップ 4 および 5 を繰り返します。

作業の確認

ライブラリーにあるすべてのオブジェクトの所有権を変更したことを確認するには、所有者によるオブジェクト処理コマンドを使用します。 WRKOBJOWN *new-owner-profile* と入力します。その後、画面と、ライブラリーにあるオブジェクトのリストを比較します。

ライブラリーにあるオブジェクトの所有権の変更が完了したら、ライブラリーへの共通アクセスを設定することができます。

ライブラリーへの共通アクセスの設定

アプリケーション・オブジェクトの所有権を設定したら、オブジェクト権限編集 (EDTOBJAUT) コマンドを使用して、ライブラリーに対する共通権限を変更することができます。

1. EDTOBJAUT *library-name* *LIB を入力します。
2. **PUBLIC* を示している行にカーソルを移動します。

3. ライブラリーに対して持ちたい共通権限を入力して、**Enter** キーを押します。

```
                          オブジェクト権限編集

オブジェクト . . . . :   CUSTLIB         所有者 . . . . . . . :   COWNER
  ライブラリー . . . :     QSYS          1 次グループ . . . . :   *NONE
オブジェクトのタイプ :   *LIB

現行権限に対する変更を入力するには、実行キーを押してください。

  権限リストによって保護されたオブジェクト  . . . . . . . . . .   *NONE

                       オブジェクト
ユーザー     グループ    権限
COWNER                 *ALL
*PUBLIC                *CHANGE
```

4. この画面では、新しい権限を示します。

これで、ライブラリーにあるすべてのオブジェクトの共通権限を設定することができます。

ライブラリーにあるすべてのオブジェクトの共通権限の設定

オブジェクト権限取り消し (RVKOBJAUT) コマンドを使用して、ライブラリーにあるオブジェクトに対する現在の共通権限を除去します。オブジェクト権限認可 (GRTOBJAUT) コマンドを使用して、ライブラリーにあるすべてのオブジェクトに対する共通権限を設定します。

1. RVKOBJAUT と入力して、**F4** (プロンプト) を押します。
2. 表示されているようにアプリケーション・ライブラリーの名前を置き換えて、 **Enter** キーを押します。

```
                    オブジェクト権限取り消し  (RVKOBJAUT)

選択項目を入力して、実行キーを押してください。

オブジェクト  . . . . . .   *ALL          名前、総称 *、*ALL
  ライブラリー  . . . . . .    CUSTLIB     名前、*LIBL、*CURLIB...
オブジェクト・タイプ  . . . . .  *ALL      *ALL、*ALRTBL、*BNDDIR...
ユーザー  . . . . . . . . . .   *PUBLIC     名前、*ALL、*PUBLIC
            値の続きは+
権限  . . . . . . . . . . . .   *ALL       *CHANGE、*ALL、*USE...
```

注: ライブラリーにたくさんのオブジェクトがある場合、要求を処理するために数分かかることがあります。

3. GRTOBJAUT と入力して、**F4** (プロンプト) を押します。
4. 表示されているようにアプリケーション・ライブラリーの名前と必要な権限を置き換えて、 **Enter** キーを押します。

```
                    オブジェクト権限認可  (GRTOBJAUT)

選択項目を入力して、実行キーを押してください。

オブジェクト  . . . . . .  *ALL          名前、総称 , *ALL
  ライブラリー  . . . . . .    CUSTLIB     名前 , *LIBL, *CURLIB...
オブジェクト・タイプ  . . . . .  *ALL        *ALL, *ALRTBL, *BNDDIR...
ユーザー  . . . . . .  *PUBLIC       名前 , *PUBLIC
            値の続きは＋
権限  . . . . . .  *USE          *CHANGE, *ALL, *USE...
```

注: ライブラリーにたくさんのオブジェクトがある場合、要求を処理するために数分かかることがあります。

ライブラリーにあるすべてのオブジェクトの共通権限を設定したら、ジョブ・ログを使用して作業を確認することができます。

ジョブ・ログを使用した作業の確認: GRTOBJAUT コマンドを使用して、権限に対する複数の変更を行う際には、ジョブ・ログを調べてその変更が行われたことを確認します。

1. DSPJOBLOG (ジョブ・ログの表示) を入力します。
2. **F10** (詳細メッセージの表示) を押します。
3. ライブラリーにあるオブジェクトごとに、権限の変更についてのメッセージが表示されるはずです。メッセージを検討したら、リスト内のオブジェクトのチェックを外してください。

```
                        すべてのメッセージの表示
                                                    システム:   RCHASXXX
ジョブ . :   QPADEV0010    ユーザー  . :   JCHEIDEL      番号  . . . :   025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
    CUSTLIB のオブジェクト CUSTMAS タイプ *FILE の許可がユーザー *PUBLIC に認
       められた。
    CUSTLIB のオブジェクト CUSTMSGQ タイプ *MSGQ の許可がユーザー *PUBLIC に認め
       られた。
    2 オブジェクトへの権限が認められた。0 オブジェクトへの権限は認められず、
      0 オブジェクトへの権限は一部認められています。
     オブジェクト権が与えられた。
7 > DSPJOBLOG                                                          続く ...
```

考えられるエラー	回復
ジョブ・ログが、ライブラリーにあるいくつかのオブジェクトで権限が変更されなかったことを示している。	「ヘルプ」(**F1**) を使用して、メッセージの詳細を参照してください。これらのオブジェクトの権限を別々に設定するには、EDTOBJAUT を使用します。

これで、新しいオブジェクトの共通権限を設定することができます。

新しいオブジェクトの共通権限の設定

ライブラリー記述には、作成権限 (CRTAUT) と呼ばれるパラメーターがあり、これによって、ライブラリーで作成される新しいオブジェクトの共通権限が決定されます。オブジェクトを作成するコマンドは、オブジェクト・ライブラリーの CRTAUT 権限をデフォルトとして使用します。ライブラリーの CRTAUT は、ライブラリー内の既存オブジェクトの大多数に対する共通権限と同じにしてください。

1. CHGLIB *library-name* と入力して、**F4** (プロンプト) を押します。
2. **F10** (追加のパラメーター) を押します。

3. 「*作成権限*」フィールドに選択項目を入力します。

```
                        ライブラリー変更  (CHGLIB)

選択項目を入力して、実行キーを押してください。

ライブラリー  . . . . . . . . . > CUSTLIB        名前、*CURLIB
ライブラリー・タイプ  . . . . . > *PROD         *SAME、*PROD、*TEST
テキスト ' 記述 ' . . . . . . . > 'CUSTOMER RECORDS'


                        追加のパラメーター

作成権限  . . . . . . . . . . .   *CHANGE       名前、*SAME、*SYSVAL...
オブジェクト監査の作成  . . . .   *SYSVAL       *SAME、*SYSVAL、*NONE...
```

CRTAUT を *SYSVAL に設定する場合、ライブラリーに新しいオブジェクトを作成するときに、システムは QCRTAUT システム値の現行設定を使用します。ライブラリーごとに特定の CRTAUT 権限を設定すると、今後、QCRTAUT システム値が変更されないように保護します。

これで、グループおよび個人ライブラリーの処理を行うことができます。

グループおよび個人ライブラリーの処理

ご使用のプロファイルは、 ユーザー・グループおよび個々のユーザーの設定時に作成されたグループ・ライブラリーおよび個人ライブラリーを所有しています。

グループ・ライブラリーの所有権をグループ・プロファイルに変更し、個人ライブラリーの所有権を個々のユーザー・プロファイルに変更するには、すでに説明した手順を使用します。つまり、EDTOBJAUT コマンドを使用します。

グループおよび個人ライブラリーにある新しいオブジェクトの共通権限を判別するには、それらのライブラリーごとに作成権限パラメーターを設定します。この場合は、CHGLIB コマンドを使用します。

権限リストの作成を開始する前に、次の作業を完了させてください。

- アプリケーションの導入用紙とライブラリー記述用紙を使用して、すべてのアプリケーション・ライブラリーの所有権および共通権限を確立したことを確認します。
- 作成したすべてのグループと個人ライブラリーの所有権を設定して、権限を作成します。

注: システム上のすべてのライブラリーのリストを表示するには、 DSPOBJD *ALL *LIB *PRINT と入力してください。

権限リストの作成

所有権と共通権限を設定したら、権限リストを設定することができます。権限リスト用紙の情報を使用して、ライブラリーを保護するのに必要な権限リストを作成します。それには、権限リスト作成 (CRTAUTL) コマンドを使用します。

1. CRTAUTL と入力して、**F4** (プロンプト) を押します。
2. 権限リスト用紙の情報を記入します。
3. **F10** (追加のパラメーター) を押します。
4. 権限パラメーターを使用して、リストによって保護されているオブジェクトの共通権限を指定します。
5. 確認メッセージを検査します。

```
                        権限リスト作成  (CRTAUTL)

選択項目を入力して、実行キーを押してください。

権限リスト  . . . . . > CUSTLST1       名前
テキスト '記述'  . . . . . > 'FILES CLEARED AT'

                          追加のパラメーター

権限  . . . . . .  *ALL          *CHANGE、*ALL、*USE、*EXCLUDE
```

考えられるエラー	回復
リストの名前が間違って入力されている。	システムでリストの名前を一度作成したら、変更できません。リストを削除 (DLTAUTL) してから、再び行ってください。
リストに共通権限を指定していない。	権限リスト編集 (EDTAUTL) コマンドを使用します。

これで、権限リストによるオブジェクトの保護を行うことができます。

権限リストによるオブジェクトの保護

権限リストを作成したら、オブジェクト権限編集 (EDTOBJAUT) コマンドを使用して、権限リスト用紙にリストされている項目を保護します。

1. EDTOBJAUT と入力して、**F4** (プロンプト) を押します。
2. プロンプト画面に値を入力して、**Enter** キーを押します。
3. 「オブジェクト権限編集」画面で、権限リスト名を入力します。
4. オブジェクトの共通権限が権限リストから取られているものである場合は、共通権限を *AUTL に変更します。
5. これらのステップを、権限リスト用紙にあるオブジェクトごとに繰り返します。

```
                        オブジェクト権限編集

オブジェクト . . . . :   ARFILE01       所有者 . . . . . . . :   OWNAR
  ライブラリー . . . :     CUSTLIB      1 次グループ . . . . :   *NONE
オブジェクトのタイプ :   *FILE

現行権限に対する変更を入力するには、実行キーを押してください。

  権限リストによって保護されたオブジェクト  . . . . . .  CUSTLST1

                      オブジェクト
ユーザー     グループ    権限
 OWNER                  *ALL
 *PUBLIC                *AUTL
```

これで、権限リストにユーザーを追加することができます。

権限リストへのユーザーの追加

『権限リストによるオブジェクトの保護』を行ったら、権限リスト編集 (EDTAUTL) コマンドを使用して、権限リスト用紙にリストされているユーザーを追加します。

1. EDTAUTL *authorization-list-name* と入力します。
2. 「権限リスト編集」画面で、 **F6** (新ユーザーの追加) を押します。
3. ユーザーまたはグループ、そしてそのユーザーまたはグループに必要な権限をリストの項目に入力して、 **Enter** キーを押します。
4. 新しいユーザーがリストに表示されます。

```
                          新しいユーザーの追加

オブジェクト . . . . :   WSLST1          所有者 . . . . . . . :
  ライブラリー . . . :     QSYS          1 次グループ . . . . :   *NONE

新しいユーザーを入力して、実行キーを押してください。

           オブジェクト  リスト
ユーザー     権限          MGT
QSECOFR     *CHANGE
```

考えられるエラー	回復
ユーザーまたはグループに、リストに対する間違った権限を与えた。	「権限リスト編集」画面で、権限を変更できます。
リストに間違ったユーザーまたはグループを追加した。	ユーザーまたはグループを除去するには、権限リスト項目除去 (RMVAUTLE) コマンドを使用するか、または「権限リスト編集」画面でユーザーの権限にブランクを入力します。

作業の確認

権限リスト表示 (DSPAUTL) コマンドを使用して、すべてのユーザー権限を権限リストにリストします。権限リストが保護を行っているオブジェクトをすべてリストするには、画面で **F15** を使用します。

特定権限を設定する前に、次の作業を完了してください。

- CRTAUTL コマンドを使用して、アプリケーションに必要な権限リストを作成する。
- EDTOBJAUT コマンドを使用して、権限リストによるオブジェクトの保護を行う。
- EDTAUTL コマンドを使用して、ユーザーに権限リストを追加する。

特定権限の設定

『所有権および共通権限の設定』では、GRTOBJAUT コマンドを使用して、ライブラリー記述用紙の第 1 部の情報に基づいて、ライブラリーにあるすべてのオブジェクトの共通権限を設定する方法を理解しました。次に、オブジェクト権限編集 (EDTOBJAUT) コマンドを使用して、ライブラリー記述用紙の第 2 部の情報に基づいて、ライブラリーとそのライブラリーにあるオブジェクトの特定権限を指定します。

特定の権限を設定するには、次のトピックを参照してください。

- ライブラリーに対する特定権限の設定
- オブジェクトに対する特定権限の設定
- 一度に複数のオブジェクトに対する権限の設定

ライブラリーに対する特定権限の設定

ライブラリーは実際に特殊なタイプのオブジェクトです。ライブラリーの権限を設定するには、EDTOBJAUT コマンドを使用して、ライブラリー以外のオブジェクトに権限を設定するときと全く同じように行います。すべてのライブラリーは、QSYS と呼ばれる IBM 提供のライブラリーにあります。次の例にある画面では、JKL Toy Company における、CONTRACTS ライブラリーについてのライブラリー記述用紙の第 2 部を使用します。

ライブラリー・オブジェクトの特定権限のリスト				
グループ・プロファイルまたはユーザー・プロファイル	オブジェクト名	オブジェクト・タイプ	必要な権限	権限リスト
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

1. EDTOBJAUT と入力して、**F4** (プロンプト) を押します。
2. プロンプト画面に値を入力して、**Enter** キーを押します。

```
                    オブジェクト権限編集  (EDT OBJAUT)

  選択項目を入力して、実行キーを押してください。

  オブジェクト  . . . . . > CONTRACTS      名前
    ライブラリー  . . . . . >   QSYS        名前 , *LIBL, *CURLIB
  オブジェクト・タイプ  . . . . . > *LIB    *ALRTBL, *AUTL, *BNDDIR...
```

3. 「オブジェクト権限編集」画面で **F6** (新ユーザーの追加) を押して、画面にリストされていないユーザーに権限を与えます。
4. **Enter** キーを押します。

```
                          新しいユーザーの追加

  オブジェクト . . . . :   CONTRACTS      所有者 . . . . . :   OWNCP
    ライブラリー . . . :     QSYS         1 次グループ . . . . :   *NONE
  オブジェクトの
    タイプ . . . . . :   *LIB


  新しいユーザーを入力して、実行キーを押してください。

                   Object
User               Authority
   DPTSM       *USE
   DPTMG       *USE
```

5. 「オブジェクト権限編集」画面は、ライブラリー記述用紙の第 1 部と第 2 部の両方と一致しているはずです。

```
                        オブジェクト権限編集

オブジェクト . . . . :   CONTRACTS       所有者 . . . . . . . :   OWNCP
  ライブラリー . . . :     QSYS          1 次グループ . . . . :   *NONE
オブジェクト・タイプ :   *LIB

現行権限に対する変更を入力するには、実行キーを押してください。

  権限リストによって保護されたオブジェクト  . . . . . . . . . .   *NONE

                       オブジェクト
ユーザー     グループ    権限
OWNCP                   *ALL
DPTSM                   *USE
DPTMG                   *USE
*PUBLIC                 *EXCLUDE
```

新しいオブジェクトの作成権限 (CRTAUT) は、ライブラリーについては「オブジェクト権限編集」画面には表示されません。ライブラリーの CRTAUT を表示するには、ライブラリー表示 (DSPLIB) コマンドを使用します。

また、この手順を使用して、システムのオブジェクトに特定の権限を設定することもできます。

これで、オブジェクトに対して特定権限を設定することができます。

オブジェクトに対する特定権限の設定

アプリケーション・ライブラリーのオブジェクトに対して特定権限を設定するための手順は、ライブラリーに対して特定権限を設定する場合と同じです。例では、JKL Toy Company における、COPGMLIB ライブラリーについてのライブラリー記述用紙の第 2 部を使用します。

表 62. JKL Toy Company のライブラリー記述用紙

グループ・プロファイルまたはユーザー・プロファイル	オブジェクト名	オブジェクト・タイプ	必要な権限	権限リスト
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. EDTOBJAUT と入力して、**F4** (プロンプト) を押します。
2. プロンプト画面に情報を入力して、**Enter** キーを押します。
3. 「オブジェクト権限編集」画面に権限情報を入力して、**Enter** キーを押します。

```
                        オブジェクト権限編集

オブジェクト . . . . :   COMSGQ01        所有者 . . . . . . . :   OWNCO
  ライブラリー . . . :     COPGMLIB      1 次グループ . . . . :   *NONE
オブジェクト・タイプ :   *MSGQ

現行権限に対する変更を入力するには、実行キーを押してください。

  権限リストによって保護されたオブジェクト  . . . . . . . . . .   *NONE

                       オブジェクト
ユーザー     グループ    権限
OWNCO                   *ALL
*PUBLIC                 *CHANGE
```

これで、一度に複数のオブジェクトに対する権限を設定することができます。

一度に複数のオブジェクトに対する権限の設定

ここまでの例では EDTOBJAUT コマンドを使用して、1 つのオブジェクトに対する特定権限を設定しました。複数のオブジェクトに対するセキュリティーを設定するには、オブジェクト権限認可 (GRTOBJAUT) コマンドを使用します。 GRTOBJAUT と入力して、**F4** (プロンプト) を押します。次に、権限に対して複数の変更を行う場合の例を示します。

- 次の画面に含まれているフィールドでは、CUSTLIB ライブラリーにあるすべてのメッセージ待ち行列の共通権限を *CHANGE に設定します。

```
                    オブジェクト権限認可  (GRTOBJAUT)

選択項目を入力して、実行キーを押してください。

オブジェクト  . . . . . .   *ALL          名前、総称 *、*ALL
  ライブラリー  . . . . . .    CUSTLIB     名前、*LIBL、*CURLIB...
オブジェクト・タイプ  . . . . .  *MSGQ       *ALL、*ALRTBL、*BNDDIR...
ユーザー  . . . . . .   *PUBLIC       名前、*PUBLIC
            値の続きは＋
権限  . . . . . .   *CHANGE     *CHANGE、*ALL、*USE...
```

- 次の画面に入力されているフィールドでは、CUSTLIB ライブラリーにある、WRK の文字で始まる名前のファイルすべてに対する *ALL 権限をユーザー AMES に与えます。

```
                    オブジェクト権限認可  (GRTOBJAUT)

選択項目を入力して、実行キーを押してください。

オブジェクト  . . . . . .   WRK*          名前、総称 *、*ALL
  ライブラリー  . . . . . .    CUSTLIB     名前、*LIBL、*CURLIB...
オブジェクト・タイプ  . . . . .  *FILE       *ALL、*ALRTBL、*BNDDIR...
ユーザー  . . . . . .   AMES          名前、*PUBLIC
            値の続きは＋
権限  . . . . . .   *ALL          *CHANGE、*ALL、*USE...
```

この例では、**総称**名と呼ばれるパラメーターを指定する技法を使用します。大多数のコマンドでは、パラメーターに、最初の文字の後にアスタリスク (*) が続く形式を指定することができます。システムは、それらの文字で始まる名前のすべてのオブジェクトで操作を実行します。コマンドのオンライン情報では、どのパラメーターで総称名を使用できるかを示しています。

- ARLST1 という権限リストを使用して、文字 AR で開始するすべてのファイルの保護を行い、さらにファイルがリストから共通権限を得るようにするには、2 つのステップを実行する必要があります。次の画面では、必要なステップが表示されます。

```
                    オブジェクト権限認可  (GRTOBJAUT)

選択項目を入力して、実行キーを押してください。

オブジェクト  . . . . . .   AR*           名前、総称 *、*ALL
  ライブラリー  . . . . . .    CUSTLIB     名前、*LIBL、*CURLIB...
オブジェクト・タイプ  . . . . .  *FILE       *ALL、*ALRTBL、*BNDDIR...

 :
権限リスト  . . . . . .   ARLST1        名前、*NONE
```

```
                    オブジェクト権限認可  (GRTOBJAUT)

選択項目を入力して、実行キーを押してください。

オブジェクト  . . . . . .  AR*           名前、総称 *、*ALL
  ライブラリー  . . . . . .    CUSTLIB     名前、*LIBL、*CURLIB...
オブジェクト・タイプ  . . . . .  *FILE        *ALL、*ALRTBL、*BNDDIR...
ユーザー  . . . . . .  *PUBLIC      名前、*PUBLIC
            値の続きは+
権限  . . . . . .  *AUTL        *CHANGE、*ALL、*USE...
            値の続きは+
```

『ジョブ・ログを使用した作業の確認』で説明されているとおり、DSPJOBLOG コマンドを使用して、システムが要求された権限変更を行ったかどうか検証します。

『印刷装置出力の保護』に進む前に、EDTOBJAUT または GRTOBJAUT コマンドを使用して、ライブラリー記述用紙の第 2 部に特定権限を設定します。

印刷装置出力の保護

特定権限を設定したら、次のトピックにある情報を使用して、機密の印刷装置出力を保護することができます。

- 『出力待ち行列の作成』およびそれを管理できる人物の制御。
- 待ち行列に対する『特殊印刷装置出力の割り当て』。

出力待ち行列の作成

1. CRTOUTQ (出力待ち行列作成) を入力して、**F4** (プロンプト) を押します。
2. 出力待ち行列およびライブラリーの名前を記入します。
3. **F10** (追加のパラメーター) を押します。
4. 出力待ち行列のセキュリティー情報が見つかるまでページ送りを行います。

```
                      出力待ち行列作成  (CRTOUTQ)

選択項目を入力して、実行キーを押してください。

出力待ち行列  . . . . . > NEWCP          名前
  ライブラリー  . . . . . >   CONTRACTS    名前、*CURLIB
スプール・ファイル最大サイズ :
  ページ数  . . . . . .  *NONE          数値、*NONE
  開始時刻  . . . . . .                 時刻
  終了時刻  . . . . . .                 時刻
            値の続きは+
待ち行列上のファイルの順序  . .  *FIFO        *FIFO、*JOBNBR
リモート・システム  . . . . . .  *NONE

 .
 .
 .
テキスト ' 記述 ' . . . . . > 'NEW CONTRACTS QUEUE'
```

5. 出力待ち行列を使用し、管理できる人を制御するには、出力待ち行列およびワークステーションのセキュリティー用紙から情報を入力します。
6. **Enter** キーを押して、確認メッセージをチェックします。

```
                        出力待ち行列作成  (CRTOUTQ)

選択項目を入力して、実行キーを押してください。


追加のパラメーター

ファイルの表示  . . . . . .  *NO          *NO、*YES、*OWNER
ジョブ区切り  . . . . . . .  0            0-9、*MSG
操作員制御  . . . . . . . .  *NO          *YES、*NO
データ待ち行列名  . . . . .  *NONE         名前、*NONE
  ライブラリー  . . . . . .                名前、*LIBL、*CURLIB
検査権限  . . . . . . . . .  *OWNER       *OWNER、*DTAAUT
権限  . . . . . . . . . . .  *LIBCRTAUT    名前、*USE、*ALL...
```

考えられるエラー	回復
F10 ではなく **Enter** キーを押した。	出力待ち行列変更 (CHGOUTQ) コマンドを使用して、追加情報を入力します。
出力待ち行列が間違ったライブラリーに作成された。	オブジェクト移動 (MOVOBJ) コマンドを使用して、出力待ち行列を正しいライブラリーに移動します。

これで、印刷装置出力の出力待ち行列への割り当てを行うことができます。

印刷装置出力の出力待ち行列への割り当て

出力待ち行列を作成したら、出力待ち行列に印刷装置出力を割り当てることができます。通常、印刷装置ファイルは印刷装置出力の宛先を制御します。アプリケーションの提供者に連絡して、機密報告書の印刷装置ファイルの名前とライブラリーを確認してください。

この情報にアクセスしない場合は、報告書を印刷して、それを出力待ち行列に保持してください。「スプール・ファイルの処理」画面の属性オプションを使用して、印刷装置ファイルの名前を見つけます。「スプール・ファイル属性の処理」画面の「*印刷装置ファイル*」フィールドに、印刷装置ファイルが表示されます。

印刷装置ファイルの変更の宛先 (出力待ち行列) を変更するには、印刷装置ファイル変更 (CHGPRTF) コマンドを使用します。

```
CHGPRTF FILE(library-name/printer-file-name)
        OUTQ(library-name/output-queue-name)
```

だれかが再び報告書を要求するたびに、報告書は新しい宛先に送られます。出力待ち行列にすでに保持されているスプール・ファイルの宛先を変更するには、「スプール・ファイル処理」画面の変更オプションを使用します。

たとえば、JKL Toy Company の Sharon Jones が価格リスト印刷装置ファイル PRCLST1 を PRICEQ 出力待ち行列に割り当てるとします。次のように入力します。

```
CHGPRTF FILE(CONTRACTS/PRCLST1) OUTQ(CONTRACTS/PRICEQ)
```

価格リスト報告書をすべて PRICEQ 出力待ち行列に割り当てるために、 Sharon は次の総称印刷装置ファイル名を使用することもできます。

```
CHGPRTF FILE(CONTRACTS/PRCLST*) OUTQ(CONTRACTS/PRICEQ)
```

新しい契約をすべて NEWCP 出力待ち行列に送信するために、Sharon は、契約の作成に使用したサンプル・ドキュメントと関連している出力待ち行列を変更します。

作業の確認

機密印刷装置出力の保護戦略を検査する最善の方法は、それを印刷することです。そして、出力が正しい出力待ち行列に送信されるかどうかを確認します。システム操作員としてサインオンし、待ち行列にあるファイルを見たり、または操作したりできるかどうか調べます。

ワークステーションを保護する前に、必ず次のことを行ってください。

- CRTOUTQ コマンドを使用して、出力待ち行列およびワークステーションのセキュリティー用紙にリストされている出力待ち行列を作成します。
- CHGPRTF コマンドを使用して、印刷装置出力を新しい出力待ち行列に割り当てます。

ワークステーションの保護

印刷装置出力の保護を行ったら、ワークステーションの保護を行わなければなりません。ワークステーションの許可は、システム上のその他のオブジェクトを認可するときと同じように行います。 EDTOBJAUT コマンドを使用して、ワークステーションに対する権限をユーザーに与えます。

ユーザーがワークステーションでサインオンするには、*CHANGE 権限を持っていなければなりません。QLMTSECOFR システム値が「no (0)」の場合、機密保護担当者または *ALLOBJ 権限を持っている人であればだれでも任意のワークステーションでサインオンできます。

QLMTSECOFR システム値が「yes (1)」の場合、次のガイドラインを使用して、ワークステーションに権限を設定します。

ワークステーションでのサインオンを許可されているユーザー	共通権限	QSECOFR 権限	個別のユーザー権限
すべてのユーザー	*CHANGE	*CHANGE	必須ではない
選択されたユーザーのみ	*EXCLUDE	権限がない	*CHANGE
選択されたユーザーおよびすべてのオブジェクトに対する権限を持っているユーザー	*EXCLUDE	*CHANGE	*CHANGE
すべてのオブジェクトに対する権限を持っているユーザー以外のすべてのユーザー	*CHANGE	権限がない	必須ではない

システム操作員メッセージ待ち行列へのアクセスを制限する前に、出力待ち行列およびワークステーションのセキュリティー用紙に含まれている情報に基づいて、EDTOBJAUT コマンドを使用して、ワークステーションのセキュリティーを行います。

システム操作員のメッセージ待ち行列へのアクセスの制限

セキュリティーを向上させるには、印刷装置出力の保護、ワークステーションの保護、およびシステム操作員メッセージ待ち行列へのアクセスの制限を行います。

ASSIST メニューのメッセージ処理オプションを使用すると、ユーザーは機能キーを使用してシステム操作員 (QSYSOPR) メッセージ待ち行列を表示することができます。システム操作員メッセージに誤った応答をすると、システム上で問題が発生する原因となります。ユーザーがメッセージに応答したり、メッセージ待ち行列からメッセージを削除したりするには、*CHANGE 権限が必要です。この権限は、システム操作員だけが持っているべきものです。システム責任用紙を調べて、だれがシステム操作員メッセージ待ち行列に対する *CHANGE 権限を持つべきかを確認してください。

EDTOBJAUT コマンドを使用します。

1. EDTOBJAUT QSYSOPR *MSGQ と入力して、**Enter** キーを押します。
2. **F11** を押して、オブジェクト権限の詳細な情報を表示します。
3. サンプル画面で示されているように、共通 *OBJOPR 権限を与えて、**Enter** キーを押します。

```
                          オブジェクト権限編集

オブジェクト . . . . :   QSYSOPR         所有者 . . . . . . . :   QSYS
  ライブラリー . . . :     QSYS           1 次グループ . . . . :   *NONE
オブジェクト・タイプ :   *MSGQ

現行権限に対する変更を入力するには、実行キーを押してください。

  権限リストによって保護されたオブジェクト  . . . . . . . . . .   *NONE

                       オブジェクト  ----------オブジェクト----------
ユーザー     グループ      権限        OPR   MGT   存在   変更   REF
*PUBLIC                  USER DEF      X
```

4. システムは「*オブジェクト権限*」欄を USER DEF (ユーザー定義) に変更します。
5. もう一度 **F11** を押して、データ権限の詳細な情報を表示します。
6. サンプル画面で示されているように、共通 *ADD 権限を与えて、**Enter** キーを押します。

```
                          オブジェクト権限編集

オブジェクト . . . . :   QSYSOPR         所有者 . . . . . . . :   QSYS
  ライブラリー . . . :     QSYS           1 次グループ . . . . :   *NONE
オブジェクトのタイプ :   *MSGQ

現行権限に対する変更を入力するには、実行キーを押してください。

  権限リストによって保護されたオブジェクト  . . . . . . . . . .   *NONE

                      オブジェクト  ------------- データ -------------
ユーザー     グループ    権限          読取   追加   更新   削除   実行
*PUBLIC                USER DEF             X
```

7. **F6** (ユーザーの追加) を使用して、QSYSOPR メッセージに応答する必要のあるユーザーを追加します。そして、それらのユーザーに *CHANGE 権限を与えます。

重要: 共通権限 *EXCLUDE は作成しないでください。すべてのジョブ (およびユーザー) は、メッセージを QSYSOPR メッセージ待ち行列に追加できなければなりません。

資源保護の設定を終了させるには、次のことを行う必要があります。

- 権限リスト用紙とライブラリー記述用紙を使用して、すべてのアプリケーション・ライブラリーのセキュリティーを確立したことを確認します。
- 出力待ち行列およびワークステーションのセキュリティー用紙を調べて、ワークステーションが保護されており、特殊な出力待ち行列が作成されていることを確認します。
- システム操作員 (QSYSOPR) メッセージ待ち行列へのアクセスを制限します。
- アプリケーションとともに提供されている指示に従って、アプリケーション・ライブラリーを保管します。システムは、アプリケーションの所有権および共通権限に関する情報を保管します。
- セキュリティー・データの保管 (SAVSECDTA) コマンドを使用して、作成したセキュリティー情報を保管します。セキュリティー情報を保管する方法の詳細については、『セキュリティー情報の保管』を参照してください。

これで、セキュリティー・セットアップをテストすることができます。

セキュリティーのテスト

このトピックでは、システム上で設定したセキュリティーをテストするための技法について説明します。このコンテキストでのテストとは、設定したものが意図したとおりに機能するかどうかを確認することを意味します。『セキュリティーの監視』では、システムでのセキュリティーの成果を評価する方法について説明します。

システム上で大きな変更を行ったときは必ずセキュリティーをテストしてください。大きな変更には、新しいアプリケーションの追加、既存のアプリケーションの資源保護の設定、新しいユーザー・グループの追加、またはセキュリティー・レベルの変更などが含まれます。

以下のトピックから、セキュリティーに変更を加える際に生じる問題のテストおよび診断方法について学んでください。

- ユーザー・プロファイルのテスト
- 資源保護のテスト

ユーザー・プロファイルのテスト

セキュリティーのテストを開始するには、システム上に新しいグループを設定する度に必ずユーザー・プロファイルをテストする必要があります。以下の点について、グループ・プロファイルからコピーしたプロファイルを 1 つずつテストしてください。

- ユーザー・プロファイルを使用して正常にサインオンできますか。サインオンできない場合は、失敗したサインオンについて作成されたジョブ・ログを調べてください。 ASSIST メニューの「印刷装置出力の処理」オプションを使用して、ジョブ・ログを見つけ、詳細を調べます。

  起こり得る問題としては、次のものがあります。
  - 必要なオブジェクトの 1 つ、たとえば初期メニュー、現行ライブラリー、または初期プログラムが存在しない。
  - ジョブ記述に指定されているライブラリー・リストがエラーの原因となっている。ライブラリーが存在しないか、またはライブラリー・リストに QGPL と QTEMP を含めていません。
  - ユーザーに、ワークステーションに対する権限がない。
- サインオンの際に、画面に正しい初期メニューまたはプログラムが表示されていますか。
- 「サインオン」画面に初期メニューまたは現行ライブラリーが表示される場合、何が起こりますか。ユーザー・プロファイルが「制約機能 (YES)」の場合、エラー・メッセージが表示されます。
- アテンション・キーを押すと、正しい画面が表示されますか。
- 出力が正しい印刷装置に送られますか。送られない場合は、ASSIST メニューの「印刷装置出力の処理」オプションを使用して、出力の送信先を調べてください。また、ユーザー・プロファイルとジョブ記述を調べて、出力が異なる印刷装置に送信された理由を判別してください。
- コマンド行を表示できますか。
- セキュリティー・エラーを起こさずに、必須のアプリケーション機能を実行できますか。詳細については、『資源保護のテスト』を参照してください。
- 印刷装置の管理またはライブラリーの保管などの、必要なシステム・タスクを実行できますか。

プロファイルを使用してサインオンするときに、システムが新規パスワードを割り当てることを要求する場合、テストが完了したら、次のようにパスワードをユーザー・プロファイル名に戻してください。

1. 自分のプロファイル (機密保護担当者権限のあるもの) を使用してサインオンします。
2. CHGUSRPRF *profile-name* PASSWORD(*profile-name*) PWDEXP(*YES) と入力します。

これでユーザー・プロファイルのテストが完了したので、資源保護のテストを行うことができます。

資源保護のテスト

ユーザー・プロファイルのテストが終了したら、資源保護もテストしなければなりません。資源保護をテストする際には、次のものを探してください。

- ジョブを実行するのに十分な権限がないユーザー。
- 意図した以上の権限を持つユーザー。

不十分な権限のテスト

ユーザー・プロファイルに十分な権限があるかどうかを確認するには、対話式機能とバッチ機能の両方をテストします。

対話式テスト

アプリケーションの資源保護をテストするには、いくつかの異なるユーザー・プロファイルを使用してサインオンしなければならないことがあります。その目的は、割り当てた権限が十分かどうか確認することです。

- さまざまなレベルの権限 (つまり表示、変更、および削除) を必要とする機能をテストします。
- メニューだけでなく、プログラムもテストします。メニュー・オプションを選択するだけでは、権限をテストするのに十分でないことがあります。場合によっては、レコードの削除などの操作を実際に実行しようとするまで、システムがファイルにアクセスしないことがあります。権限検査は、システムがファイルを開くと行われます。アプリケーション設計によって、システムがいつファイルを開くかが左右されます。
- セキュリティー・エラーの記録を保持し、それらを解決します。権限エラーが生じると、画面にメッセージが表示され、そこには操作するには権限が不十分であること、また使用しようとしたオブジェクトは何だったかが示されます。

バッチ・テスト

- ジョブを投入するユーザーのプロファイルを使用して、アプリケーションからサンプル・バッチ・ジョブを実行します。
- さまざまなレベルの権限 (印刷情報、変更情報、月末でのファイルの消去など) を必要とするバッチ・ジョブをテストします。
- QSYSOPR メッセージ待ち行列と QHST ログでセキュリティー・エラーを調べます。 DSPLOG コマンドを使用して、QHST ログを表示します。セキュリティー・メッセージの範囲は、 CPF2200、 CPI2200、 CPC2200、 CPD2200、 CPF4A00、 CPI4A00、 CPC4A00、および CPD4A00 です。

  さらにセキュリティー監査機能を使用して、権限障害とその他のセキュリティー関連のイベントを記録することができます。

権限が多過ぎるかどうかのテスト

資源保護を設定して機密情報を保護する場合、サンプル・ユーザー・プロファイルをテストして、セキュリティーが機能するかどうかを調べます。機密ファイルにアクセスできるはずのないユーザーのプロファイルを使用してサインオンします。

- ファイルへのアクセスを許可しているメニューに進むことができますか。
- ファイルを使用するメニュー・オプションを選択すると、何が起こりますか。
- コマンド行を表示できますか。

- CPYF FROMFILE(*file-name*) TOFILE(QSYSPRT) などのコマンドを実行して、ファイルをリストすることができますか。
- Query ツールを使用してファイルを見ることができますか。

テストの結果として、セキュリティー情報の変更が必要となる場合があります。

セキュリティー情報の変更

ご使用のシステムのセキュリティーを計画し終えたので、ここでビジネスで変更の必要が生じたときに、計画が依然として有効であるか確認する必要があります。

このトピックでは、セキュリティーを設計する上での基本的な目標として、単純であることを強調しています。ユーザー・グループを個々のユーザーのパターンとして設計しました。また、特定の個別権限ではなく、共通権限、権限リスト、およびライブラリー権限を使用することにしました。セキュリティーを管理する際に、次のようにしてそのアプローチの利点を活用します。

- 新しいユーザー・グループまたは新しいアプリケーションを追加する際には、セキュリティーを計画するために使用した技法を使用します。
- セキュリティーに変更を加える必要がある場合は、特定の問題を解決するための例外を作成するのではなく、一般的なアプローチを使用するようにします。

『セキュリティー・コマンド』では、セキュリティー情報を表示、変更、および削除するために使用するコマンドについて説明します。

さまざまなタイプの変更を扱う方法については、次のトピックを参照してください。

- システムへの新しいユーザーの追加
- 新しいユーザー・グループの作成
- ユーザー・グループの変更
- 新しいアプリケーションの追加
- 新しいワークステーションの追加
- ユーザーの責任の変更
- システムからのユーザーの除去

セキュリティー・コマンド

下記の表には、システムでセキュリティー・オブジェクトを処理する際に使用するコマンドが示されています。それらのコマンドを使用して行える作業は次のとおりです。

- セキュリティー情報の表示およびリスト
- セキュリティー情報の変更
- セキュリティー情報の削除

表 63. セキュリティー・コマンド

セキュリティー・オブジェクト	表示方法	変更方法	削除方法
システム値	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	削除できません。
ジョブ記述	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD

表 63. セキュリティー・コマンド (続き)

セキュリティー・オブジェクト	表示方法	変更方法	削除方法
グループ・プロファイル	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1],[2]
ユーザー・プロファイル	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]
オブジェクト権限	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT
オブジェクト所有権	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN は、直前の所有者の権利を取り消すことを許可します。
1 次グループ	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP は、1 次グループを *NONE に設定します。
オブジェクト監査	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD (*NONE に設定) CHGAUD
権限リスト	DSPAUTL DSPAUTLOBJ	EDTAUTL (リストに対するユーザー権限) EDTOBJAUT (リストによって保護されるオブジェクト) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL (リスト全体)[3] RMVAUTLE (リストに対するユーザー権限の除去) EDTOBJAUT (リストによって保護されるオブジェクト) RVKOBJAUT

1. IBM では、「ユーザー登録の処理」画面の除去オプションを使用して、プロファイルを削除することをお勧めします。このオプションを使用すると、プロファイルが所有しているオブジェクトを削除したり、またはそれらを新規所有者に再び割り当てたりすることができます。特定の DLTUSRPRF コマンド・パラメーターを使用すると、ユーザーが所有しているすべてのオブジェクトを削除したり、またはそれらをすべて新規所有者に割り当てたりすることができます。所有されているオブジェクトを削除するか、または再び割り当てないかぎり、プロファイルを削除することはできません。さらに、プロファイルがいずれかのオブジェクトの 1 次グループである場合は、そのプロファイルを削除できません。
2. メンバーを有しているグループ・プロファイルは削除できません。 DSPUSRPRF コマンドの *GRPMBR オプションを使用して、グループのメンバーをリストしてください。グループ・プロファイルを削除する前に、それぞれの個別のグループ・プロファイルごとに「グループ・ファイル」フィールドを変更します。
3. 権限リストがオブジェクトの保護に使用されている場合、その権限リストを削除することはできません。リストが保護を行っているオブジェクトをリストするには、DSPAUTLOBJ コマンドを使用してください。リストが保護を行っているオブジェクトの権限を変更するには、EDTOBJAUT コマンドを使用してください。

セキュリティー情報の表示およびリスト

セキュリティー情報をリストするには、表示 (DSP) コマンドに印刷 (*PRINT) オプション指定して使用します。たとえば、MYLIST という権限リストを表示するには、`DSPAUTL MYLIST *PRINT` と入力します。

表示コマンドによっては、さまざまなタイプのリストのオプションを提供するものがあります。たとえば、個別のユーザー・プロファイルを作成したときに、DSPUSRPRF コマンドに *GRPMBR オプションを指定

して使用すると、グループ・プロファイルのすべてのメンバーがリストされます。プロンプト (**F4**) とオンライン情報を使用して、セキュリティー・オブジェクトに使用可能なリストを見つけてください。

表示コマンドを使用すると、画面にセキュリティー情報を表示できます。さらに、より多くの機能を提供する、... 処理 (WRK) コマンドを使用することもできます。... 処理コマンドは、リスト画面を提供します。この画面を使用して、情報の変更、削除、および表示を行うことができます。

さらに、セキュリティー・コマンドを使用すると、総称名を使用して情報をリストしたり、表示したりできます。 `WRKUSRPRF DPT*` と入力する場合、「ユーザー登録の処理」画面または「ユーザー・プロファイル処理」画面は、 *DPT* という文字で始まるプロファイルだけを表示します。コマンドのオンライン情報を使用して、総称名の使用を許可しているパラメーターを確認してください。

セキュリティー情報の変更

... 処理 (WRK) または ... 編集 (EDT) コマンドを使用して、セキュリティー情報を対話式に変更することができます。情報を表示して変更したら、その後で再び情報を表示できます。

また、... 変更 (CHG) または ... 認可 (GRT) コマンドを使用すると、セキュリティー情報を変更する前と後にその情報を表示しなくても変更することができます。この方法は、一度に複数のオブジェクトを変更する場合に特に便利です。たとえば、GRTOBJAUT コマンドを使用して、ライブラリーにあるすべてのオブジェクトの共通権限を設定しました (108 ページの『ライブラリーにあるすべてのオブジェクトの共通権限の設定』を参照)。

セキュリティー情報の削除

... 処理 (WRK) または ... 編集 (EDT) コマンドを使用して、特定のタイプのセキュリティー情報を対話式に削除または除去できます。さらに、... 削除 (DLT)、... 除去 (RMV)、および ... 取り消し (RVK) コマンドを使用して、セキュリティー情報を削除することもできます。システムがセキュリティー情報の削除を許可する前に、特定の条件を満たさなければならない場合があります。『セキュリティー・コマンド』にある注では、これらの条件のいくつかについて説明しています。

システムへの新しいユーザーの追加

システムに新しいユーザーを追加する必要があるときは、次の手順を使用します。

1. 個人をユーザー・グループに割り当てます。 ユーザー・グループ記述用紙を参考にしてください。
2. 新しいユーザーがシステム機能を実行する必要があるかどうかを決定します。その必要がある場合は、その情報をシステム責任用紙に追加します。
3. 個人を個別ユーザー・プロファイル用紙に追加します。
4. システム責任用紙とユーザー・グループ記述用紙を検討して、新しいユーザーがグループの値とは異なる値を必要とするかどうか決定します。
5. グループ・プロファイルまたはグループ・メンバーのプロファイルをコピーして、ユーザー・プロファイルを作成します。パスワードの期限満了を必ず設定してください。 (『グループ・プロファイルのコピー』を参照してください。)
6. 新しいユーザーにセキュリティーのメモのコピーを渡します。

新しいユーザー・グループを作成する方法については、『新しいユーザー・グループの作成』を参照してください。

新しいユーザー・グループの作成

次のいくつかの理由のため、新しいユーザー・グループを作成しなければならない場合があります。

- その他の部門で、そのシステムを使用する必要があるとき。
- 資源保護の必要を満たすために、ユーザー・グループをもっと特定する必要があることに気付いたとき。
- 企業が一部の部門を再編成したとき。

新しいユーザー・グループを作成するには、次のことを行ってください。

1. 『ユーザー・グループの計画』の指示に従って、ユーザー・グループ記述用紙に記入します。
2. ユーザー・グループをアプリケーション、ライブラリー、およびユーザー・グループの図に追加します。
3. グループ・メンバーがシステム機能を実行する必要があるかどうか評価します。システム責任用紙を更新します。(『システム機能の責任者の決定』を参照してください。)
4. ユーザー・グループ記述用紙およびシステム責任用紙にある情報を使用して、個々のユーザー・プロファイル用紙に記入します。
5. グループ・ライブラリーを作成します。
6. グループのジョブ記述を作成します。
7. グループ・プロファイルを作成します。

   注: ステップ 5、6、および 7 を実行するための指示については、『ユーザー・グループの設定』を参照してください。
8. グループ・メンバーに個別のユーザー・プロファイルを作成します。(『個々のユーザーの設定』を参照してください。)
9. グループが必要とするすべてのアプリケーションのライブラリー記述用紙を評価します。アプリケーション・オブジェクトに対してグループ・アクセスを行うのに必要なステップを実行する場合は、『資源保護の設定』で説明されている技法を使用してください。
10. グループのすべてのメンバーにセキュリティーのメモを渡します。

ユーザー・グループを変更する方法については、『ユーザー・グループの変更』を参照してください。

ユーザー・グループの変更

グループの特性に対して変更を加えるには、変更のタイプに応じた方法で処理する必要があります。次に、変更例とそれらを扱う方法について示します。

グループの権限の変更

グループが必要とするオブジェクトに対する権限が、計画の初期の段階では予期していなかったものであることがわかったとします。この場合、以下のことを行ってください。

1. オブジェクト権限編集 (EDTOBJAUT) コマンドを使用して、グループがオブジェクトまたは適切な権限リストに正しくアクセスできるようにします。 112 ページの『特定権限の設定』には、このことを行う方法の例が示されています。グループ権限を与えると、グループのすべてのメンバーはオブジェクトに対する権限を取得します。
2. グループ権限を機密資源に与える場合、グループの現在のメンバーを調べることができます。ユーザー・プロファイル表示コマンド (DSPUSRPRF *group-profile-name* *GRPMBR) を使用して、グループ・メンバーをリストしてください。

グループのカスタマイズの変更

グループのメンバーに合ったユーザー環境の設定を変更しなければならないことがあります。たとえば、ある部門に専用の印刷装置が設置される場合、その部門のユーザー・グループのメンバーのために、新しい印刷装置がデフォルトになるようにしたいと思うことでしょう。あるいは、システムに新しいアプリケーションが導入される際には、ユーザー・グループのメンバーは、サインオン時に別の初期メニューを表示してほしいと思うことでしょう。

グループ・プロファイルでは、グループ・メンバーに個々のプロファイルを作成するためにコピーできるパターンを提供します。しかし、グループ・プロファイルのカスタマイズ値は、個別のユーザー・プロファイルを作成した後は、それらに影響を与えることはありません。たとえば、グループ・プロファイルで「*印刷装置*」などのフィールドを変更しても、グループ・メンバーには影響を与えません。この場合には、個別のユーザー・プロファイルにある「*印刷装置*」フィールドを変更する必要があります。

「ユーザー・プロファイル処理」画面を使用して、一度に複数のユーザーのパラメーターを変更することができます。例では、グループのすべてのメンバーの出力待ち行列を変更します。

1. WRKUSRPRF *ALL と入力して、**Enter** キーを押します。
2. 「ユーザー登録の処理」画面が表示される場合は、 **F21** (操作援助レベルの選択) を使用して、「ユーザー・プロファイルの処理」画面に変更します。

```
                          ユーザー・プロファイルの処理

 オプションを入力して、実行キーを押してください。
   1= 作成    2= 変更    3= コピー    4= 削除    5= 表示
   12= 所有者によるオブジェクトの処理

           ユーザー・
 Opt       プロファイル       テキスト

                              HARRISOK              Harrison, Keith
  2                           HOGANR                Hogan, Richard
                              JONESS                Jones, Sharon
  2                           WILLISR               Willis, Rose

    :
                                                                  続く ...
 オプション 1, 2, 3, 4, 5 のパラメーターまたはコマンド
 ===> PRTDEV(PRT02)
 F3= 終了    F5= 最新表示    F12= 取消し    F16= 位置指定の繰返し    F17= 位置指定
 F21= 援助レベルの選択    F24= キーの続き
```

3. 変更したいそれぞれのプロファイルの横に **2** (変更) と入力します。
4. 画面の下部のパラメーター行に、パラメーター名と新しい値を入力します。パラメーター名がわからない場合は、**F4** (プロンプト) を押します。
5. **Enter** キーを押します。変更したプロファイルごとに確認メッセージが表示されます。

グループ・プロファイルにあるカスタマイズ・フィールドを変更してもグループ・メンバーに影響を与えることはありませんが、今後、役に立つことがあるかもしれません。後でグループにメンバーを追加したいときに、グループ・プロファイルはパターンを提供します。また、これはグループの標準フィールド値の記録ともなります。

新しいアプリケーションへのグループ・アクセスの提供

ユーザー・グループが新しいアプリケーションにアクセスする必要があるときに、グループについての情報とアプリケーションについての情報を分析する必要があります。次に推奨される方法を示します。

1. 新しいアプリケーションのアプリケーション記述用紙とアプリケーション、ライブラリー、およびユーザー・グループの図を見て、アプリケーションが使用するライブラリーを確認します。これらのライブラリーをユーザー・グループ記述用紙に追加します。
2. アプリケーション、ライブラリー、およびユーザー・グループの図を更新して、ユーザー・グループとアプリケーションの新しい関係を表示します。
3. グループの初期ライブラリー・リストにライブラリーを含める必要がある場合は、ジョブ記述変更 (CHGJOBD) コマンドを使用して、グループのジョブ記述を変更します。ジョブ記述の処理についてのヘルプが必要な場合は、 93 ページの『ジョブ記述の作成』を参照してください。

   注: ジョブ記述にあるすべてのライブラリーを初期ライブラリー・リストに追加する場合は、そのジョブ記述を使用するユーザー・プロファイルを変更する必要はありません。ユーザーが次にサインオンするときに、初期ライブラリー・リストが自動的にライブラリーを追加します。
4. 新しいアプリケーションにアクセスするために、グループの初期プログラムか初期メニューのどちらかを変更する必要があるかどうか評価します。 CHGUSRPRF コマンドを使用して、各ユーザー・プロファイルの初期メニューまたはプログラムをそれぞれ変更する必要があります。
5. アプリケーションが使用するすべてのライブラリーのライブラリー記述用紙を検討します。ライブラリーで使用可能な共通アクセスが、グループの必要を十分に満たしているかどうか判別します。十分でない場合は、グループ権限をライブラリー、特定のオブジェクト、または権限リストに与えなければならないことがあります。これを行うには、オブジェクト権限編集 (EDTOBJAUT) および権限リストの編集 (EDTAUTL) コマンドを使用します。(詳細については、『資源保護の設定』を参照してください。)

アプリケーションをシステムに追加するには、『新しいアプリケーションの追加』を参照してください。

新しいアプリケーションの追加

新しいアプリケーションのセキュリティーを計画する際には、元となるアプリケーションを計画したときと同じように注意して行う必要があります。手順も同じです。

1. アプリケーションのアプリケーション記述用紙とライブラリー記述用紙を作成します。
2. アプリケーション、ライブラリー、およびユーザー・グループの図を更新します。
3. 『資源保護の計画』の手順に従って、新しいアプリケーションのセキュリティーを行う方法を選択します。
4. 『アプリケーションの導入の計画』に説明されている方法を使用して、アプリケーションの導入用紙を作成します。
5. アプリケーションからの印刷装置出力が機密になっており、保護が必要かどうか評価します。必要に応じて、出力待ち行列およびワークステーションのセキュリティー用紙を更新してください。
6. 『所有権および共通権限の設定』、および『資源保護の設定』で説明されているステップに従って、アプリケーションの導入およびセキュリティーを行います。

ワークステーションをシステムに追加するには、『新しいワークステーションの追加』を参照してください。

新しいワークステーションの追加

新しいワークステーションをシステムに追加する際には、次のセキュリティー要件を考慮してください。

1. 新しいワークステーションの物理的な位置によって、セキュリティーのリスクが生じますか。(詳しい説明については、『物理的セキュリティーの計画』を参照してください。)

2. ワークステーションでリスクが生じる場合、出力待ち行列およびワークステーションのセキュリティー用紙を更新します。
3. 通常は、共通権限 *CHANGE を使用して新しいワークステーションを作成します。ワークステーションのセキュリティー要件を満たしていない場合は、EDTOBJAUT コマンドを使用して別の権限を指定します。

システム上でのユーザーの責任を変更するには、『ユーザーの責任の変更』を参照してください。

ユーザーの責任の変更

システム・ユーザーが社内で新しい仕事または新しい責任を担う際には、ユーザー・プロファイルに与える影響を評価する必要があります。

1. ユーザーは別のユーザー・グループに属さなければならないでしょうか。ユーザー・グループを変更するには、CHGUSRPRF コマンドを使用します。
2. プロファイル内で、印刷装置または初期メニューなどのカスタマイズ値を変更する必要がありますか。カスタマイズ値を変更する際にも、CHGUSRPRF コマンドを使用します。
3. 新しいユーザー・グループのアプリケーション権限は、その人物にとって十分でしょうか。
   - ユーザー・プロファイル表示 (DSPUSRPRF) コマンドを使用して、古いグループ・プロファイルと新しいグループ・プロファイルの権限を比較します。
   - 個別のユーザー・プロファイルの権限も調べます。
   - EDTOBJAUT コマンドを使用して、必要な変更を加えます。
4. ユーザーは何らかのオブジェクトを所有しますか。それらのオブジェクトの所有権を変更しなければなりませんか。所有者によるオブジェクト処理 (WRKOBJOWN) コマンドを使用します。
5. ユーザーはシステム機能を実行しますか。ユーザーは新しいジョブのシステム機能を実行する必要がありますか。必要に応じて、システム責任用紙を更新し、ユーザー・プロファイルを変更します。

システムからユーザーを除去する方法については、『システムからのユーザーの除去』を参照してください。

システムからのユーザーの除去

退職者がいる場合、ユーザー・プロファイルをシステムから直ちに除去しなければなりません。しかし、ユーザー・プロファイルを削除するには、その前にそのプロファイルが所有しているオブジェクトの所有権を削除するか、転送する必要があります。それには、WRKOBJOWN コマンドを使用するか、または「ユーザー登録の処理」画面でオプション **4** (除去) を使用します。

「ユーザー登録の処理」画面でオプション **4** (除去) を選択すると、付加的な画面が表示され、その画面でユーザーが所有しているオブジェクトを処理することができます。つまり、すべてのオブジェクトを新しい所有者に与えるか、またはオブジェクトを個々に処理するかを選択できます。

```
                              ユーザーの除去

ユーザー . . . . . :   HOGANR
ユーザー記述 . . . . . :   Sales and Marketing Department

このユーザーを除去するためには、下に選択項目を入力してから実行キーを押してく
  ださい。

     1. このユーザーが所有するすべてのオブジェクトを新しい所有者に渡します。
     2. このユーザーが所有する特定のオブジェクト所有者を削除または変更します。
```

オブジェクトを個々に処理することを選択する場合 (オプション **2**)、画面にはユーザーが所有するすべてのオブジェクトがリストされます。

```
                              ユーザーの除去

ユーザー . . . . . :   HOGANR
ユーザー記述 . . . . . :   Sales and Marketing Department

新しい所有者 . . . . . .                    名前、リストは F4 キー

このユーザーを除去するためには、すべてのオブジェクトの所有者を削除または変更
  してください。
下のオプションを入力して、実行キーを押してください。
  2= 新しい所有者への変更    4= 削除    5= 明細の表示

OPT  オブジェクト          ライブラリー  記述
 4   HOGANR               QUSRSYS       Hogan, Richard message queue
 4   QUERY1               DPTWH         Inventory Query
```

オブジェクトを削除することを選択する場合は、「オブジェクトの削除の確認」画面が表示されます。オブジェクトが削除されたら、ユーザー・プロファイルを除去することができます。次に「ユーザー登録の処理」画面が再び表示され、システムがユーザーを除去したことを示すメッセージが表示されます。

セキュリティー情報の保管

このトピックでは、セキュリティー情報を保管し、復元する方法の概要を示しています。システムのバックアップと回復を計画する際には、情報そのものだけでなく情報のセキュリティーについても考慮する必要があります。バックアップと回復に関する完全な計画を設計するには、 Information Center の『バックアップ、回復、およびシステムの可用性』のトピックを参照すると、役に立ちます。

次のトピックでは、セキュリティーを設定する際に作成するセキュリティー情報をバックアップして、復元する方法について説明しています。

- システム値の保管
- グループおよびユーザー・プロファイルの保管
- ジョブ記述の保管
- 資源保護情報の保管
- デフォルト所有者プロファイル (QDFTOWN) の使用
- 損傷した権限リストの回復

システム値の保管

システム値は、システム・ライブラリー QSYS に保管されます。 QSYS ライブラリーを保管するのは、次のことを行うときです。

- システム保管 (SAVSYS) コマンドを使用する。
- 「保管」メニューでオプションを使用して、システム全体を保管する。
- 「保管」メニューでオプションを使用して、システム情報を保管する。
- 「バックアップの実行 (RUNBCKUP)」メニューでオプションを使用して、システム全体のバックアップをとる。

システム全体を回復する必要がある場合は、オペレーティング・システムを復元するときに、自動的にシステム値を復元します。

次に、『グループおよびユーザー・プロファイルの保管』を参照してください。

グループおよびユーザー・プロファイルの保管

グループおよびユーザー・プロファイルは QSYS ライブラリーに保管されます。これらは、システム保管 (SAVSYS) コマンドを使用するか、メニュー・オプションを選択してシステム全体を保管するときに使用します。

さらに、グループおよびユーザー・プロファイルを保管する方法として、セキュリティー・データ保管 (SAVSECDTA) コマンドを使用することもできます。

ユーザー・プロファイルを復元するには、ユーザー・プロファイル復元 (RSTUSRPRF) コマンドを使用します。通常の手順は次のとおりです。

1. オペレーティング・システムを復元して、ライブラリー QSYS を復元します。
2. ユーザー・プロファイルを復元します。
3. 残りのライブラリーを復元します。
4. 権限復元 (RSTAUT) コマンドを使用して、オブジェクトに対する権限を復元します。

次に、『ジョブ記述の保管』を参照してください。

ジョブ記述の保管

ジョブ記述を作成する際に、それを常駐させるライブラリーを指定します。 IBM では、ジョブ記述を QGPL ライブラリーに作成するようお勧めしています。

ジョブ記述を保管するには、それが常駐するライブラリーを保管します。これを行うには、ライブラリー保管 (SAVLIB) コマンドを使用します。さらに、オブジェクト保管 (SAVOBJ) コマンドを使用して、ジョブ記述を保管することもできます。

ライブラリーの内容を復元するには、ライブラリー復元 (RSTLIB) コマンドを使用します。個々のジョブ記述を復元するには、オブジェクト復元 (RSTOBJ) コマンドを使用します。

次に、『資源保護情報の保管』を参照してください。

資源保護情報の保管

資源保護とはユーザーがオブジェクトを処理する方法を定義するものですが、これはさまざまなタイプの情報で構成され、さまざまな場所に保管されます。

表 64. 資源保護情報の保管および復元

情報のタイプ	保管場所	保管方法	復元方法
共通権限	オブジェクトの保管場所	SAVxxx コマンド[1]	RSTxxx コマンド[2]
オブジェクト監査値	オブジェクトの保管場所	SAVxxx コマンド[1]	RSTxxx コマンド[2]
オブジェクト所有権	オブジェクトの保管場所	SAVxxx コマンド[1]	RSTxxx コマンド[2]
1 次グループ	オブジェクトの保管場所	SAVxxx コマンド[1]	RSTxxx コマンド[2]
権限リスト	QSYS ライブラリー	SAVSYS または SAVSECDTA	RSTUSRPRF USRPRF(*ALL)
オブジェクトと権限リストの間のリンク	オブジェクトの保管場所	SAVxxx コマンド[1]	RSTxxx コマンド[2]
私用権限	ユーザー・プロファイルの保管場所	SAVSYS または SAVSECDTA	RSTAUT

1. SAVOBJ または SAVLIB コマンドを使用すると、ほとんどのオブジェクト・タイプを保管できます。オブジェクト・タイプ (構成など) によっては、特殊な保管コマンドを持つものがあります。
2. RSTOBJ または RSTLIB コマンドを使用すると、ほとんどのオブジェクト・タイプを復元できます。オブジェクト・タイプ (構成など) によっては、特殊な復元コマンドを持つものがあります。

アプリケーションまたはシステム全体を復元させる必要がある場合、オブジェクトに対する権限の回復を含む、回復ステップを注意深く計画する必要があります。次に、アプリケーションの資源保護情報を回復するために必要な基本ステップを示します。

1. 必要に応じて、アプリケーションを所有するプロファイルを含む、ユーザー・プロファイルを復元します。特定のプロファイルまたはすべてのプロファイルを復元するには、RSTUSRPRF コマンドを使用します。
2. アプリケーションによって使用される権限リストを復元します。 RSTUSRPRF USRPRF(*ALL) を使用すると、権限リストが復元されます。

   注: これにより、パスワードを含むすべてのユーザー・プロファイル値がバックアップ媒体から復元されます。
3. RSTLIB または RSTOBJ コマンドを使用して、アプリケーション・ライブラリーを復元します。これにより、オブジェクト所有権、共通権限、およびオブジェクトと権限リストの間のリンクが回復されます。
4. RSTAUT コマンドを使用して、オブジェクトに対する私用権限を復元します。 RSTAUT コマンドでは、権限リストに対するユーザー権限も復元します。特定のユーザーまたはすべてのユーザーの権限を復元することができます。

システム上にないオブジェクトおよび所有者プロファイルの復元方法については、『デフォルト所有者プロファイル (QDFTOWN) の使用』を参照してください。

デフォルト所有者プロファイル (QDFTOWN) の使用

オブジェクトを復元する際に所有者プロファイルがシステム上にない場合、システムはオブジェクトの所有権を QDFTOWN と呼ばれるデフォルトのプロファイルに転送します。所有者プロファイルを回復したか、または所有者プロファイルを再び作成したら、所有者によるオブジェクト処理 (WRKOBJOWN) コマンドを使用して、所有権を元に戻すことができます。

権限リストの回復については、『損傷した権限リストの回復』を参照してください。

損傷した権限リストの回復

オブジェクトが権限リストによって保護されているときに権限リストが損傷を受けた場合、そのオブジェクトへのアクセスは全オブジェクト (*ALLOBJ) 特殊権限を持っているユーザーだけに限定されます。

損傷した権限リストを回復するには、次の 2 つのステップが必要です。

1. その権限リストにあるユーザーとその権限を回復する。
2. その権限リストとオブジェクトとの関連を回復する。

*ALLOBJ 特殊権限を持つユーザーが、これらのステップを行うことができます。

ステップ 1: 権限リストの回復

権限リストに対するユーザーの権限が分かっている場合、権限リストを削除して再び権限リストを作成し、それにユーザーを追加してください。

権限リストに対するユーザー権限がすべて分かっているわけではない場合、次のステップを使用して、最新の SAVSYS または SAVSECDTA テープからユーザー権限を復元します。

1. 損傷した権限リストを削除します。

   ```
   DLTAUTL AUTL(authorization-list-name)
   ```

2. 権限リストを復元します。

   ```
   RSTUSRPRF USRPRF(*ALL)
   ```

3. 権限復元 (RSTAUT) コマンドを使用して、ユーザーをリストに追加します。

ステップ 2: オブジェクトと権限リストの関連の回復

権限リストを復元したか、または権限リストを再び作成した場合、リストと、リストによって保護されたオブジェクトの間のリンクを確立する必要があります。

1. 記憶域再利用 (RCLSTG) コマンドを使用します。 RCLSTG は、損傷を受けたか、または欠落した権限リストによって保護されているオブジェクトを、QRCLAUTL と呼ばれるデフォルト・リストに割り当てます。
2. QRCLAUTL 権限リストによって保護されているオブジェクトをリストします。

   ```
   DSPAUTLOBJ AUTL(QRCLAUTL)
   ```

3. GRTOBJAUT コマンドを使用して、正しい権限リストを持つオブジェクトを保護します。たとえば、権限リスト ARLST01 を持つ、CUSTLIB ライブラリーにある ARWRK01 ファイルを保護するには、次のように入力します。

   ```
   GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(*FILE) +
             AUTL(ARLST01)
   ```

セキュリティーの監視

このトピックでは、システム上でのセキュリティーの効果を監視するための基本的な事柄を取り上げます。

セキュリティーを定期的に監視する目的は、通常は次の 2 つです。

- 企業の資源を十分に保護する。
- システムや企業の情報に許可なくアクセスしようとすることを検出する。

どの監視タスクを定期的に実行する必要があるのかを決定する際には、セキュリティー・ポリシーに関する記述と、ユーザーに対するセキュリティーのメモを検討してください。

セキュリティーの監視の詳細については、次のトピックを参照してください。

- セキュリティーの監視のためのチェックリスト
- セキュリティー監査

セキュリティーの監視のためのチェックリスト

以下に、システムでのセキュリティーのさまざまな局面を検討するためのチェックリストを示します。これらを使用して、計画を進めてください。

物理的セキュリティーの監視

- バックアップ媒体を損傷と盗難から保護します。
- 共通エリアでのワークステーションに対するアクセスを制限します。 DSPOBJAUT コマンドを使用して、ワークステーションに対して *CHANGE 権限を持っている人を探します。

システム値の監視

- 設定がシステム値選択用紙と一致することを検査します。システム・セキュリティー属性印刷 (PRTSYSSECA) コマンドを使用します。
- 特に新しいアプリケーションを導入する際に、決定したシステム値を検討します。

グループ・プロファイルの監視

- グループ・プロファイルにパスワードがないことを検査します。すべてのグループ・プロファイルがパスワード *NONE を持っていることを検査するには、DSPAUTUSR コマンドを使用します。
- 正しい人物がグループのメンバーになっていることを検査します。グループのメンバーをリストするには、DSPUSRPRF コマンドに *GRPMBR オプションを指定して使用します。
- グループ・プロファイルごとの特殊権限を確認します。 DSPUSRPRF コマンドを使用します。セキュリティー・レベル 30、40、または 50 で実行している場合は、グループ・プロファイルに *ALLOBJ 権限を与えないでください。

ユーザー・プロファイルの監視

- システム上のユーザー・プロファイルが次のカテゴリーのいずれかに属していることを検査します。
  - 現在の従業員のユーザー・プロファイル
  - グループ・プロファイル
  - アプリケーションの所有者プロファイル
  - IBM 提供のプロファイル (Q で始まる)
- 企業がユーザーを転勤させるか、またはユーザーが退職したときに、そのユーザー・プロファイルを除去します。ユーザーの退職と同時にプロファイルを自動的に削除するか、または使用不可にするには、満了スケジュール項目変更 (CHGEXPSCDE) コマンドを使用します。
- 非活動状態のプロファイルを探して、それらを除去します。一定の時間非活動になっているプロファイルを自動的に使用不可にするには、プロファイル活動の分析 (ANZPRFACT) コマンドを使用します。
- ユーザー・プロファイル名と同じパスワードを持っているユーザーを判別します。デフォルト・パスワードの分析 (ANZDFTPWD) コマンドを使用します。このコマンドのオプションを使用して、次回ユーザーがシステムにサインオンするときに、パスワードを変更させます。

  重要: IBM 提供のプロファイルはシステムから除去しないでください。IBM 提供のプロファイルは、Q の文字で始まります。

- *USER 以外のユーザー・クラスを持つ人物とその理由を識別します。すべてのユーザーとそのユーザー・クラス、およびその特殊権限のリストを入手するには、ユーザー・プロファイルの印刷 (PRTUSRPRF) コマンドを使用します。この情報をシステム責任用紙と突き合わせます。
- 「*制限機能*」フィールドが *NO に設定されているユーザー・プロファイルを制御します。

重要なオブジェクトの監視

- 重要なオブジェクトにアクセスした人物を検討します。オブジェクトを監視するには、私用権限の印刷 (PRTPVTAUT) コマンドと共通権限オブジェクトの印刷 (PRTPUBAUT) コマンドを使用します。グループがアクセスした場合は、DSPUSRPRF コマンドの *GRPMBR オプションを使用して、グループのメンバーを検査します。
- 別のセキュリティーの方法、たとえば借用権限を使用して、オブジェクトへのアクセスを提供するアプリケーション・プログラムを使用できる人物を検査します。借用オブジェクトの印刷 (PRTADPOBJ) コマンドを使用します。

無許可アクセスの監視

- システム操作員に、QSYSOPR メッセージ待ち行列のセキュリティー・メッセージに注意するように指示します。特に、繰り返しサインオンしても成功しない場合には、機密保護担当者に通知する必要があります。セキュリティー・メッセージは、2200 から 22FF、および 4A00 から 4AFF の間にあります。接頭部は、CPF、CPI、CPC、および CPD です。
- オブジェクトに対する無許可のアクセスを記録するように、セキュリティー監査を設定します。

次に、『セキュリティー監査』を参照してください。

セキュリティー監査

セキュリティーの監視の際に、オペレーティング・システムはシステムで行われているセキュリティー・イベントを記録することができます。これらのイベントは、**ジャーナル・レシーバー**と呼ばれる特殊なシステム・オブジェクトに記録されます。ジャーナル・レシーバーを設定すると、各種のセキュリティー・イベント、たとえばシステム値またはユーザー・プロファイルの変更、またはオブジェクトへのアクセス試行の失敗などを記録することができます。次の値によって、記録されるイベントが制御されます。

- 監査制御 (QAUDCTL) システム値
- 監査レベル (QAUDLVL) システム値
- ユーザー・プロファイルの監査レベル (AUDLVL)
- ユーザー・プロファイルのオブジェクト監査 (OBJAUD)
- オブジェクトのオブジェクト監査 (OBJAUD)

監査ジャーナルの情報は、次の目的で使用されます。

- 試行されたセキュリティー違反の検出。
- より高いセキュリティー・レベルへの移行の計画。
- 機密ファイルなどの機密オブジェクトの使用の監視。

監査ジャーナルの情報をさまざまな方法で見るために、いくつかのコマンドを使用できます。

基本的なシステム・セキュリティー計画用紙

これらの用紙はブラウザーからコピーまたは印刷することができます。

基本的なセキュリティー情報全体を印刷するには、右ペインを選択して、Information Center バナーの PDF アイコンをクリックします。

1 つの計画用紙を印刷するには、印刷したい計画用紙と対応するリンクをクリックします。そして、右ペインをクリックし、ブラウザーの「印刷」アイコンをクリックします。これで、選択した用紙が印刷されます。

次に、基本システム・セキュリティーの計画および使用を成功させるのに必要なすべての計画用紙をリストします。

- 物理的セキュリティー計画用紙
- アプリケーション記述用紙
- 命名規則用紙
- ライブラリー記述用紙
- システム値選択用紙
- システム責任用紙
- ユーザー・グループ識別用紙
- ユーザー・グループ記述用紙
- 個別ユーザー・プロファイル用紙
- 権限リスト用紙
- 出力待ち行列およびワークステーションのセキュリティー用紙
- アプリケーションの導入用紙

物理的セキュリティー計画用紙

表 65. 物理的セキュリティー計画用紙

物理的セキュリティー計画用紙	
作成者:	日付:
指示 • この用紙については、『資源保護の計画』で説明されています。 • システム装置および接続装置の物理的な場所に関連したセキュリティーの問題について記述するには、この用紙を使用します。 • この用紙の情報は、システムに入力する必要はありません。	
システム装置:	
システム装置を保護するためにとったセキュリティー手段 (ロックした部屋の使用など):	
通常のキーロックの設定位置:	
キーの保管場所:	
システム装置に関連したその他の注記:	
バックアップ媒体および文書:	
バックアップ・テープのビジネスの場所での保管場所:	
バックアップ・テープの別の保管場所:	
機密保護担当者、保守、および DST パスワードの保管場所:	

表 65. 物理的セキュリティー計画用紙 (続き)

重要なシステム文書 (シリアル番号や構成など) の保管場所:	

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

アプリケーション記述用紙

表 66. アプリケーション記述用紙

アプリケーション記述用紙	
作成者:	日付:
指示 • この用紙については、『アプリケーションの記述』および『資源保護の計画』で説明されています。 • アプリケーションごとに別々の用紙を作成します。 • この用紙の情報は、システムに入力する必要はありません。	
アプリケーション名:	省略形:
アプリケーションについての簡単な説明:	
1 次メニュー名:	ライブラリー:
初期プログラム名:	ライブラリー:
アプリケーションが使用するライブラリーのリスト (ファイル用とプログラム用の両方):	
アプリケーションに対するセキュリティーの目的 (機密情報を含んでいるかどうかなど):	

命名規則用紙

表 67. 命名規則用紙

命名規則用紙	
作成者:	日付:
指示 • この用紙については、『アプリケーションの記述』で説明されています。 • 情報は、この用紙からシステムに直接入力する必要はありません。 • この用紙を使用して、システム上のオブジェクトに名前を割り当てる方法について説明します。各オブジェクトの例を示します。	
オブジェクトのタイプ	**命名規則**
グループ・プロファイル	
ユーザー・プロファイル	
権限リスト	
ライブラリー	
ファイル	
カレンダー	
装置	
テープ	

ライブラリー記述用紙

表 68. ライブラリー記述用紙

ライブラリー記述用紙	1 / 2
作成者:	日付:
指示: • この用紙については、『ユーザー・セキュリティーの計画』および『資源保護の計画』で説明されています。 • この用紙を使用して、メインのライブラリーについて説明し、それらの資源保護要件を定義します。 • システム上の主要なアプリケーション・ライブラリーごとに 1 枚ずつ用紙に記入します。 • この用紙に情報を入力する方法については、『資源保護の設定』で説明されています。	
ライブラリー名:	記述名 (テキスト):
このライブラリーの機能についての簡単な説明:	
ライブラリーに対するセキュリティーの目的の定義 (機密情報を含んでいるかどうかなど):	
ライブラリーへの共通権限:	
ライブラリー内のオブジェクトへの共通権限:	
新しいオブジェクト (CRTAUT) への共通権限:	
ライブラリー所有者:	

ライブラリー記述用紙	2 / 2
作成者:	日付:
ライブラリー名:	

第 2 部の追加指示:				
• 下記の図には、特定権限を必要とする個人またはオブジェクトがリストされています。 • 必須の権限のタイプ (*ALL、*CHANGE、*USE、または *EXCLUDE) を指定します。				
ライブラリー・オブジェクトの特定権限をリストします。				
グループ・プロファイルまたはユーザー・プロファイル	オブジェクト名	オブジェクト・タイプ	必要な権限	権限リスト

システム値選択用紙

表 69. システム値選択用紙

システム値選択用紙		1 / 2
作成者:		日付:
指示 • この用紙については、『全体的なセキュリティー戦略の計画』で説明されています。 • この用紙を使用して、セキュリティーおよびカスタマイズに影響するシステム値の選択項目を記録します。 • SETUP メニューのオプション **1** を使用して、この用紙の第 1 部を入力します。		
「システム・オプションの変更」画面からの値		
システム値 / ネットワーク属性	**推奨される選択項目**	**ユーザーの選択**
システム名		
日付区切り記号 (QDATSEP)		
日付形式 (QDATFMT)		
時刻区切り記号 (QTIMSEP)		
新しい装置の装置名形式 (QDEVNAMING)	1 (iSeries システム)	
システム印刷装置 (QPRTDEV)		
セキュリティー・レベル (QSECURITY)	40	
機密保護担当者に対するディスプレイへのサインオンの許可 (QLMTSECOFR)	N	
完了した印刷装置出力に関するジョブ会計情報の保管 (QACGLVL)	N (*NONE)	

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

システム責任用紙

表 70. システム責任用紙

システム責任用紙			
作成者:			日付:
指示: • この用紙については、『個々のユーザー・プロファイルの計画』で説明されています。 • この用紙を使用して、*USER 以外のユーザー・クラスを持つ人物をリストします。 • 情報をこの用紙から個別ユーザー・プロファイル用紙の「ユーザー・クラス」列に転送します。			
セキュリティーの第 1 責任者: 補佐の機密保護担当者:			
プロファイル名	ユーザー名	クラス	コメント

ユーザー・グループ識別用紙

表 71. ユーザー・グループ識別用紙

ユーザー・グループ識別用紙								
作成者:		日付:						
指示: • この用紙については、『ユーザー・グループの計画』で説明されています。 • この用紙は、同様のアプリケーションを必要としているユーザーのグループを識別するのに役立ちます。 1. 主要なアプリケーションを用紙の上部にリストします。 2. ユーザーを左側の列にリストします。 3. ユーザーごとに必要なアプリケーションをマークします。 • この用紙の情報は、システムに入力する必要はありません。								
		アプリケーションに対して必要なアクセス						
ユーザー名	部門	APP:	APP:	APP:	APP:	APP:	APP:	APP:
注: • *寛容な* セキュリティー環境の場合は、ユーザーが必要とするアプリケーションに **X** を付けます。 • *厳重な* セキュリティー環境の場合は、アプリケーションの使用方法 を指定するために、 **C** (変更) および **V** (表示) のマークを付けます。								

ユーザー・グループ記述用紙

表 72. ユーザー・グループ記述用紙

ユーザー・グループ記述用紙	1 / 2
作成者:	日付:
第 1 部の指示 • この用紙を作成する方法については、『ユーザー・グループの計画』で説明されています。 • この用紙に入力する方法については、『ユーザー・セキュリティーの設定』で説明されています。 • システムを使用するグループごとに別々の用紙を作成します。 • ジョブ記述作成 (CRTJOBD) コマンドを使用して、グループのジョブ記述を作成します。ジョブ記述には、グループの初期ライブラリー・リストがあります。	
グループ・プロファイル名: グループの記述:	

表 72. ユーザー・グループ記述用紙 (続き)

グループの 1 次アプリケーション: グループが必要とする他のアプリケーションのリスト:
グループに必要な各ライブラリーをリストします。グループの初期ライブラリー・リストに含める必要のある各ライブラリーにはマーク (✓) を付けます。
注: 前の部分にリストされているアプリケーションごとに、アプリケーション記述用紙を調べて、アプリケーションが使用するライブラリーを見つけてください。

ユーザー・グループ記述用紙		2 / 2
第 2 部の追加指示 • 下の表では、「ユーザー・プロファイルの作成」画面に表示されるフィールドをすべてリストしています。フィールドは、自分で選択しなければならないものと、IBM でデフォルト値を使用するようお勧めしているものの 2 つのグループに分けられています。 • 「ユーザー・プロファイルの処理」画面またはユーザー・プロファイル作成 (CRTUSRPRF) コマンドを使用して、用紙の第 2 部からシステムに情報を入力します。		
グループ・プロファイル内の各フィールドの値を選択する:		
フィールド名	**推奨される選択項目**	**ユーザーの選択**
グループ・プロファイル名 (ユーザー)		
パスワード	*NONE	
ユーザー・クラス (ユーザーのタイプ)	*USER	
現行ライブラリー (省略時のライブラリー)	*グループ・プロファイル名と同じ*	
呼び出す初期プログラム (サインオン・プログラム)		
初期プログラム・ライブラリー		
初期メニュー (第 1 メニュー)		
初期メニュー・ライブラリー		
制限機能 (コマンド行の使用の制限)	*YES	
テキスト (ユーザー記述)		
ジョブ記述	*グループ・プロファイル名と同じ*	
ジョブ記述ライブラリー		
グループ・プロファイル名 (ユーザー・グループ)	*NONE	
印刷装置 (省略時の印刷装置)		
出力待ち行列	*DEV	
注: フィールドの順番は、「ユーザー・プロファイルの作成」画面 (F4 を使用) で表示される順序と同じです。		
次のフィールドには、システム提供の値 (デフォルト) を使用する:		
会計コード	キーボード・バッファリング	共通権限
操作援助レベル	言語 ID	パスワードの期限満了の設定
アテンション・プログラム	装置セッション限界	分類順序
コード化文字セット識別コード	最大記憶域	特殊権限

国または地域 ID	メッセージ待ち行列	特殊環境
サインオン情報の表示	パスワードの満了間隔	状況
文書パスワード	優先順位限界	ユーザー・オプション
注: このリストのフィールドは、アルファベット順に配列されています。		

個別ユーザー・プロファイル用紙

表 73. 個別ユーザー・プロファイル用紙

個別ユーザー・プロファイル用紙						
作成者:				日付:		
指示: • この用紙を作成する方法については、『個々のユーザー・プロファイルの計画』で説明されています。 • この用紙を使用して、個々のシステム・ユーザーの情報を記録します。システム上のユーザー・グループ (グループ・プロファイル) ごとに 1 枚ずつ用紙に記入します。 • 個々のユーザーに指定したい追加フィールドについては、右側のブランクの欄を使用します。 • この用紙に入力する方法については、『個々のユーザーの設定』で説明されています。						
グループ・プロファイル名:						
作成したオブジェクトの所有者:			作成されたオブジェクトに対するグループ権限:			
グループ権限タイプ:						
グループのメンバーごとに項目を作成します。						
ユーザー・ プロファイル	テキスト (説明)	ユーザー・ クラス	制限機能			

権限リスト用紙

表 74. 権限リスト用紙

権限リスト用紙					
作成者:			日付:		
指示 • この用紙については、『資源保護の計画』で説明されています。 • 権限リストごとに、この用紙を 1 枚ずつ作成します。 • この用紙を使用して、リスト、およびリストにアクセスするグループと個人が保護するオブジェクトをリストします。 • この用紙に入力する方法については、『資源保護の設定』で説明されています。					
権限リスト名:					
記述:					
リストが保護するオブジェクトをリストします。					
オブジェクト名	オブジェクト・タイプ	オブジェクト・ライブラリー	オブジェクト名	オブジェクト・タイプ	オブジェクト・ライブラリー
リストにアクセスするグループとユーザーをリストします。					
グループまたはユーザー	許可されているアクセスのタイプ	リストの管理	グループまたはユーザー	許可されているアクセスのタイプ	リストの管理

印刷装置出力待ち行列およびワークステーションのセキュリティー用紙

表 75. 印刷装置出力待ち行列およびワークステーションのセキュリティー用紙

印刷装置出力待ち行列およびワークステーションのセキュリティー用紙				
作成者:		日付:		
指示 • この用紙については、『印刷装置出力の保護』で説明されています。 • 特殊な保護が必要なワークステーションまたは出力待ち行列があれば、この用紙に項目を作成します。 • この用紙に入力する方法については、『ワークステーションの保護』で説明されています。				
制限付き出力待ち行列のパラメーターのリスト:				
出力待ち行列名	出力待ち行列ライブラリー	ファイルの表示 (DSPDTA)	検査する権限 (AUTCHK)	操作員制御 (OPRCTL)
機密保護担当者のワークステーション: 機密保護担当者のワークステーションを特定のものに制限する場合 (システム値 QLMTSECOFR は、はい)、機密保護担当者および *ALLOBJ 権限を持つすべての人に許可されているワークステーションを下にリストします。				
制限されているワークステーションの権限を下にリストする:				
ワークステーション名	権限が与えられているグループまたはユーザー (*CHANGE 権限)			
注: 制限されたワークステーションの共通権限は、*EXCLUDE に設定されていなければなりません。				

アプリケーションの導入用紙

表 76. アプリケーションの導入用紙

アプリケーションの導入用紙		1 / 2
作成者:		日付:
指示 • この用紙については、『アプリケーションの導入の計画』で説明されています。 • 導入するアプリケーションごとに、この用紙を 1 枚ずつ作成します。 • この用紙を使用して、所有権および共通権限をロードした後でそれらをアプリケーションに設定する方法を計画します。 • この用紙に入力する方法については、『資源保護の設定』で説明されています。		
アプリケーション名:		
記述:		
アプリケーションを導入するために作成しなければならないプロファイルをリストし、その説明を加えます。		
ライブラリー名:		
	導入前	導入後
ライブラリー所有者		
オブジェクト所有者		

表 76. アプリケーションの導入用紙 (続き)

ライブラリー共通権限		
オブジェクト共通権限		
新しいオブジェクトへの共通権限		
ライブラリー名:		
	導入前	導入後
ライブラリー所有者		
オブジェクト所有者		
ライブラリー共通権限		
オブジェクト共通権限		
新しいオブジェクトへの共通権限		

アプリケーションの導入用紙		2 / 2
ライブラリー名:		
	導入前	導入後
ライブラリー所有者		
オブジェクト所有者		
ライブラリー共通権限		
オブジェクト共通権限		
新しいオブジェクトへの共通権限		
ライブラリー名:		
	導入前	導入後
ライブラリー所有者		
オブジェクト所有者		
ライブラリー共通権限		
オブジェクト共通権限		
新しいオブジェクトへの共通権限		
ライブラリー名:		
	導入前	導入後
ライブラリー所有者		
オブジェクト所有者		
ライブラリー共通権限		
オブジェクト共通権限		
新しいオブジェクトへの共通権限		

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

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

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

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

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

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

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

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。

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

本書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。

商標

以下は、IBM Corporation の商標です。

Application System/400
AS/400
e (ロゴ)
IBM
iSeries
Operating System/400
OS/400
400
Lotus
Freelance
WordPro

MMX™ および Pentium® 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 の米国およびその他の国における商標です。

UNIX® は、The Open Group の米国およびその他の国における登録商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

資料に関するご使用条件

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

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

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

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

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

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

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

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

Printed in Japan

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