IBM PowerSC Express Edition

バージョン 1.1.3

PowerSC Express Edition

IBM PowerSC Express Edition

バージョン 1.1.3

PowerSC Express Edition

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、 37 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 PowerSC Express のバージョン 1.1.3、および新しい版で明記されていない限り、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。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM PowerSC
Express Edition
Version 1.1.3
PowerSC Express Edition

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

第1刷 2013.10

目次

本書について

本書は、ファイル、システム、およびネットワーク・セキュリティーに関する詳細な情報をシステム管理者に提供します。

強調表示

本書では、以下の強調表示規則を使用します。

太字	コマンド、サブルーチン、キーワード、ファイル、構造体、ディレクトリー、およびシステムによって名前が事前に定義されているその他の項目を示します。また、ユーザーが選択するボタン、ラベル、およびアイコンなどのグラフィカル・オブジェクトも示します。
イタリック	実際の名前または値をユーザーが指定する必要があるパラメーターを示します。
モノスペース	特定のデータ値の例、画面に表示されるものと同様のテキスト例、プログラマーが作成するものと同様のプログラム・コード部分の例、システムからのメッセージ、実際に入力する必要がある情報などを示します。

AIX® でのケース・センシティブ

AIX オペレーティング・システムでは、すべてケース・センシティブとなっています。これは、英大文字と小文字を区別するということです。例えば、**ls** コマンドを使用するとファイルをリスト表示できます。`LS` と入力すると、システムはそのコマンドが「`not found` (見つからない)」と応答します。同様に、`FILEA`、`FiLea`、および `filea` は、同じディレクトリーにある場合でも、3 つの異なるファイル名です。予期しない処理が実行されないように、常に正しい大/小文字を使用するようにしてください。

ISO 9000

当製品の開発および製造には、ISO 9000 登録品質システムが使用されました。

IBM PowerSC Express Edition 1.1.3

IBM® PowerSC™ Express Edition には、セキュリティーおよびコンプライアンスの事前定義プロファイルを管理するセキュリティーおよびコンプライアンス自動化フィーチャーが組み込まれています。PowerSC Express Edition には PowerSC Real Time Compliance フィーチャーも組み込まれており、このフィーチャーを、違反行為が発生した場合や特定の重要なファイルが変更された場合にリアルタイム・アラートを提供するように構成することができます。

PowerSC Express Edition 1.1.3 の新機能

PowerSC Express Edition 1.1.3 の新機能のトピック集に関する新規情報または大幅に変更された情報について説明します。

新規情報または変更情報の参照方法

この PDF ファイルでは、新規情報および変更情報の左端にリビジョン・バー (|) が付いている場合があります。

2013 年 12 月

以下の情報では、 PowerSC Express Edition 1.1.3 の新しい内容、および更新された内容について要約しています。

- README.ICEexpress ファイルについての情報が、 2 ページの『PowerSC Express Edition バージョン 1.1.3 のインストール』に追加されました。
- Payment Card Industry - Data Security Standard 標準のバージョン 2.0 への準拠のサポートについての情報が 5 ページの『Payment Card Industry - Data Security Standard への準拠』 で更新されました。
- 32 ページの『pscxpert コマンド』が追加されました。

2013 年 5 月

AIX Security Expert フィーチャーが Payment Card Industry - Data Security Standard にどのように準拠するかを説明する表が 5 ページの『Payment Card Industry - Data Security Standard への準拠』に追加されました。

2012 年 11 月

以下の情報では、 PowerSC Express Edition 1.1.2 の新しい内容、および更新された内容について要約しています。

- リアルタイム・コンプライアンス・フィーチャーについて説明する資料を 30 ページの『PowerSC Real Time Compliance』に追加しました。
- 19 ページの『医療保険の積算と責任に関する法律 (HIPAA) (Health Insurance Portability and Accountability Act (HIPAA))』 によって定義された規格のサポートに関する資料を追加。

PowerSC Express Edition 1.1.3 の概念

この PowerSC の概要では、フィーチャー、コンポーネント、および PowerSC Express Edition フィーチャーに関連するハードウェアのサポートについて説明します。

PowerSC Express Edition 1.1.3 は、クラウドまたは仮想化データ・センターで稼働するシステムのセキュリティーと制御を実現し、エンタープライズ・ビューと管理機能を提供します。PowerSC Express Edition は、セキュリティーおよびコンプライアンス自動化、およびリアルタイム・コンプライアンスを含むフィーチャー・スイートです。仮想化層に採用されているセキュリティー・テクノロジーは、スタンドアロン・システムのセキュリティーを強化します。

次の表に、エディション、エディションに含まれるフィーチャー、コンポーネント、および各コンポーネントを使用できるプロセッサー・ベース・ハードウェアに関する詳細を示します。

表 1. PowerSC Express Edition コンポーネント、説明、サポートされるオペレーティング・システム、サポートされるハードウェア

コンポーネント	説明	サポートされるオペレーティング・システム	サポートされるハードウェア
セキュリティーおよびコンプライアンス自動化	以下の規格について、セキュリティーおよびコンプライアンス構成の設定、モニター、および監査を自動化します。 • Payment Card Industry Data Security Standard (PCI DSS) • Sarbanes-Oxley 法令および COBIT への準拠 (SOX/COBIT) • U.S. 米国国防総省 (DoD) STIG • 医療保険の積算と責任に関する法律 (HIPAA) (Health Insurance Portability and Accountability Act (HIPAA))	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6® • POWER7®
リアルタイム・コンプライアンス	使用可能にされた AIX システムをセキュリティー維持のためにモニターし、システムへの変更を行うことで構成ポリシー内で識別されるルールに違反した場合にアラートを出します。	• IBM AIX 6 (テクノロジー・レベル 7 適用) 以降 (AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 6.1.7.0) 以降付き) • IBM AIX 7 (テクノロジー・レベル 1 適用) 以降 (AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 7.1.1.0 以降付き)	固有のハードウェア要件はありません。

PowerSC Express Edition バージョン 1.1.3 のインストール

PowerSC Express Edition には `powerscExp.ice` パッケージが含まれています。`powerscExp.ice` パッケージは、AIX 5.3、AIX 6.1 および AIX バージョン 7.1 をサポートします。

`powerscExp.ice` パッケージは、PowerSC Express Edition のセキュリティーおよびコンプライアンスのフィーチャーを必要とするすべての AIX システムにインストールする必要があります。

以下のいずれかのインターフェースを使用して、PowerSC Express Edition をインストールします。

- コマンド行インターフェース (CLI) の **installp** コマンド
- SMIT インターフェース

SMIT インターフェースを使用して PowerSC Express Edition をインストールするには、以下のステップを実行します。

1. 次のコマンドを実行する。

   ```
   % smitty installp
   ```

2. 「**ソフトウェアのインストール**」オプションを選択します。
3. ソフトウェアの入力デバイスまたはディレクトリーを選択して、IBM Compliance Expert インストール・イメージの場所とインストール・ファイルを指定します。例えば、インストール・イメージのディレクトリー・パスとファイル名が `/usr/sys/inst.images/powerscExp.ice` である場合は、「**入力**」フィールドにファイル・パスを指定する必要があります。
4. ご使用条件を表示し、受け入れます。下矢印を使用して「**新規ご使用条件に同意する**」を選択し、Tab キーを押して値を「**はい**」に変更し、ご使用条件を受け入れます。
5. **Enter** キーを押して、インストールを開始します。
6. インストールの完了後、コマンド状況が「**OK**」であることを確認します。

`README.ICEexpress` という名の README ファイルが `/etc/security/aixpert` ディレクトリーにインストールされます。このファイルには、PowerSC Express Edition に含まれているコンプライアンス・プロファイルに関する実装の詳細が入っています。

ソフトウェア・ライセンスの表示

ソフトウェア・ライセンスは、CLI で次のコマンドを使用して表示できます。

```
% installp -lE -d path/filename
```

ここで、*path/filename* は、PowerSC Standard Edition インストール・イメージを指定します。

例えば、PowerSC Express Edition に関連するライセンス情報を指定するために、CLI をして以下のコマンドを入力することができます。

```
% installp -lE -d  /usr/sys/inst.images/powerscExp.ice
```

セキュリティーおよびコンプライアンス自動化

AIX Profile Manager は、セキュリティーおよびコンプライアンスの事前定義プロファイルを管理します。PowerSC Real Time Compliance は、使用可能にされた AIX システムを継続的にモニターし、これらのシステムの構成の一貫性と安全性を確認します。

XML プロファイルは、Payment Card Data Security Standard、Sarbanes-Oxley 法令、または米国国防総省の UNIX Security Technical Implementation Guide および医療保険の相互運用性と説明責任に関する法律 (Health Insurance Portability and Accountability Act (HIPAA)) と一致するように、IBM の AIX 推奨システム構成を自動化します。セキュリティー規格に準拠する組織は、事前定義されたシステム・セキュリティー設定を使用する必要があります。

AIX Profile Manager は、 AIX オペレーティング・システムと 仮想 I/O サーバー (VIOS) の両方のシステムでセキュリティー設定の適用、セキュリティー設定のモニター、およびセキュリティー設定の監査を簡素化する IBM Systems Director プラグインとして稼働します。セキュリティー・コンプライアンス・フィーチャーを使用するには、PowerSC アプリケーションが、コンプライアンス規格に適合する AIX 管理対象システムにインストールされている必要があります。セキュリティーおよびコンプライアンス自動化フィーチャーは、PowerSC Express Edition および PowerSC Standard Edition に組み込まれています。

PowerSC Express Edition インストール・パッケージ 5765-G82 を AIX 管理対象システムにインストールする必要があります。インストール・パッケージは、AIX Profile Manager または **aixpert** コマンドを使用してシステム上に実装できる `powerscExp.ice` ファイルセットをインストールします。IBM Compliance Expert Express (ICEE) のコンプライアンスが組み込まれた PowerSC が XML プロファイルを管理および改善するために使用可能に設定されます。XML プロファイルは、AIX Profile Manager によって管理されます。

セキュリティーおよびコンプライアンス自動化の概念

PowerSC のセキュリティーおよびコンプライアンス・フィーチャーは、米国国防総省 (DoD) の Security Technical Implementation Guide (STIG) に従った AIX システムの構成および監査を自動化する方法です。

PowerSC は、Payment Card Industry (PCI) Data Security Standard (DSS) バージョン 1.2 に準拠する必要があるシステムの構成およびモニターを自動化する上で役立ちます。したがって、PowerSC のセキュリティーおよびコンプライアンス・フィーチャーは、DoD UNIX STIG、PCI DSS、Sarbanes-Oxley 法令、COBIT への準拠 (SOX/COBIT)、および医療保険の相互運用性と説明責任に関する法律 (Health Insurance Portability and Accountability Act (HIPAA)) の IT コンプライアンス要件に対応するために使用されるセキュリティー構成を自動化する正確かつ完全な方法です。

注: PowerSC のセキュリティーおよびコンプライアンスは、IBM Compliance Expert Express (ICEE) エディションによって使用される既存の XML プロファイルを更新します。PowerSC Express Edition の XML プロファイルは、ICEE と同様に **aixpert** コマンドで使用できます。

PowerSC Express Edition と共に提供される事前構成済みコンプライアンス・プロファイルにより、コンプライアンスの文書を解釈して、規格を特定のシステム構成パラメーターとして実装する管理ワークロードが減ります。このテクノロジーは、プロセスを自動化することによってコンプライアンスの構成および監査のコストを削減します。IBM PowerSC Express Edition は、外部規格への準拠に関連するシステム要件を効果的に管理する上で役立つように設計されています。これにより、コストを削減してコンプライアンスを改善できる可能性があります。

米国国防総省の STIG への準拠

米国国防総省 (DoD) は、高度な機密保護機能を備えたコンピューター・システムを義務付けています。DoD によって定義されているこのレベルのセキュリティーおよび品質は、AIX on Power Systems™ サーバーの品質と顧客基盤に対応しています。

規定されているセキュリティーの目標を達成するには、AIX などのセキュア・オペレーティング・システムを正確に構成する必要があります。DoD は、指令 8500.1 ですべてのオペレーティング・システムのセキュリティー構成の必要性を認めています。この指令では、方針を定め、セキュリティー構成のガイダンスを提供する責任を米国国防情報システム局 (DISA) に任命しています。

DISA は、機密情報を含むミッション保証カテゴリー (MAC) II の機密レベルで稼働する DoD システムのセキュリティー要件を満たしているか、それ以上の環境を規定する UNIX STIG の原則およびガイドラインを作成しました。米国 DoD は、厳格な IT セキュリティー要件を設定して、システムの安全な稼働を確保するために必要な構成設定の詳細を列挙しています。必要となる専門家のガイダンスを活用できます。PowerSC Express Edition は、DoD によって定義されている設定の構成プロセスを自動化する上で役立ちます。

注: DoD への準拠を維持するために提供されるすべてのカスタム・スクリプト・ファイルは、`/etc/security/pscexpert/bin` ディレクトリーにあります。

関連情報:

米国国防総省の STIG への準拠

Payment Card Industry - Data Security Standard への準拠

Payment Card Industry - Data Security Standard (PCI - DSS) は、IT セキュリティーを 12 要件およびセキュリティー評価手順と呼ばれる 12 のセクションに分類しています。

PCI - DSS によって定義されている IT セキュリティーの 12 要件およびセキュリティー評価手順には、以下の項目が含まれます。

要件 1: カード所有者のデータを保護するためにファイアウォール構成を導入し、維持すること。

セクション 1.1.5 およびセクション 2.2.2: ビジネスに必要なサービスとポートを文書化したリスト。この要件を、不要かつ安全でないサービスを使用不可にすることにより実装します。

セクション 1.3.6: ルーター構成ファイルの保護と同期。この要件を、ネットワーク・オプション *clean_partial_conns* の値を 1 に設定することにより実装します。

要件 2: システム・パスワードおよびその他のセキュリティー・パラメーターに、ベンダー提供のデフォルトを使用しないこと。

セクション 2.1: ネットワークにシステムをインストールする前に、ベンダー提供のデフォルトを必ず変更すること。この要件を、 Simple Network Management Protocol (SNMP) デーモンを使用不可にすることにより実装します。

要件 3: カード所有者の保管データを保護すること。

この要件を、AIX オペレーティング・システムに備わっている暗号化ファイル・システム (EFS) フィーチャーを使用可能にすることにより実装します。

要件 4: オープン・パブリック・ネットワーク全体にカード所有者のデータを送信するときに、データを暗号化すること。

この要件を、AIX オペレーティング・システムに備わっている IP セキュリティー (IPSEC) フィーチャーを使用可能にすることにより実装します。

要件 5: アンチウィルス・ソフトウェア・プログラムを使用し、定期的に更新すること。

この要件を、Trusted Execution ポリシー・プログラムを使用することにより実装します。Trusted Execution は推奨されるアンチウィルス・ソフトウェアであり、 AIX オペレーティング・システムに組み込まれています。PCI では、アラートをモニターする「セキュリティー情報とイベント管理 (SIEM)」を使用可能にすることにより Trusted Execution プログラムからのログを取得することを要求しています。Trusted Execution プログラムをログ専用モードで稼働することにより、ハッシュの不一致が原因でエラーが発生しても、このプログラムは検査を停止しません。

要件 6: セキュアなシステムおよびアプリケーションを開発し、保守すること。

この要件を実装するには、必要なパッチをシステムに手動でインストールする必要があります。PowerSC Standard Edition を購入していれば、トラステッド・ネットワーク接続 (TNC) フィーチャーを使用できます。

要件 7: カード所有者データへの業務上のアクセスを必要範囲に制限すること。

ルールと役割を使用可能にする RBAC フィーチャーを使用することにより、強力なアクセス制御手段を実装できます。RBAC を使用可能にするには管理者の入力が必要なため、RBAC を自動化することはできません。

RbacEnablement は、役割用のプロパティーである isso、so、および sa が存在するかどうか判断するためにシステムを検査します。これらのプロパティーが存在しなければ、スクリプトにより作成されます。このスクリプトは、コマンド (aixpert -c コマンドなど) を実行していると終了するため、AIXPert 検査の一部としても実行されます。

要件 8: コンピューターへのアクセス権限を持つ個人に固有 ID を割り当てること。

PCI プロファイルを使用可能にすることにより、この要件を実装できます。以下のルールが PCI プロファイルに適用されます。

- セクション 8.5.9: ユーザー・パスワードを少なくとも 90 日おきに変更する。
- セクション 8.5.10: パスワードの長さは 7 文字以上を必要とする。
- セクション 8.5.11: 数字と英字の両方が入ったパスワードを使用する。
- セクション 8.5.12: 最後の 4 回に使用されたパスワードと同じ新規パスワードを個人が登録できないようにする。
- セクション 8.5.13: アクセスの試行が 6 回失敗したらユーザー ID をロックアウトすることにより、試行の繰り返しを制限する。
- セクション 8.5.14: ロックアウトの期間を 30 分か、管理者がユーザー ID を再度使用可能にするまでに設定する。
- セクション 8.5.15: 端末が 15 分以上使用されていない後で端末を再度アクティブにするには、ユーザーによるパスワード再入力を必要にする。

要件 9: カード所有者のデータへの物理的なアクセスを制限すること。

カード所有者の重要データの入ったリポジトリーをアクセスが制限された部屋に保管します。

要件 10: ネットワーク・リソースおよびカード所有者データへのすべてのアクセスを追跡し、モニターすること。

セクション 10.2: この要件を、システム・コンポーネントについて、自動ログを使用可能にしてアクセスをログに記録することにより実装します。

要件 11: セキュリティー・システムおよびセキュリティー・プロセスを定期的にテストすること。

この要件を、リアルタイム・コンプライアンス・フィーチャーを使用することにより実装します。

要件 12: 従業員および請負業者の機密保護に対応するセキュリティー・ポリシーを維持すること。

セクション 12.3.9: 使用後にすぐに使用不能化するという条件でベンダーから要求された場合のみ、ベンダーのモデムを活動化する。この要件を、リモート・ルート・ログインを使用不可にすること、必要な場合にシステム管理者が活動化すること、およびリモート・ルート・ログインが不要になったら使用不能化することにより実装します。

PowerSC Express Edition を使用すると、 PCI DSS で定義されているガイドラインに対応するために必要な構成管理が減ります。ただし、プロセス全体を自動化することはできません。

例えば、ビジネス要件に基づきカード所有者のデータへのアクセスを制限することは、自動化できません。AIX オペレーティング・システムは、ロール・ベースのアクセス制御 (RBAC) などの強力なセキュリティー・テクノロジーを提供しますが、 PowerSC Express Edition は、アクセスを必要とする個人と必要としていない個人を判別できないため、この構成を自動化することはできません。IBM Compliance Expert は、PCI 要件と一致したその他のセキュリティー設定の構成を自動化することができます。

注: PCI - DSS への準拠を維持するために提供されるすべてのカスタム・スクリプト・ファイルは、/etc/security/pscexpert/bin ディレクトリーにあります。

以下の表は、PowerSC Express Edition が AIX Security Expert ユーティリティーの機能を使用することにより、 PCI DSS 標準の要件をどのように対処するかを示しています。

表 2. PCI DSS コンプライアンス 2.0 標準に関連する設定

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
2.1	ネットワークにシステムをインストールする前に、ベンダー提供のデフォルトを必ず変更すること。例えば、パスワード、 Simple Network Management Protocol コミュニティー・ストリングを含めてから、不要なアカウントを除去します。	パスワードを変更するために経過しなければならない最小の週数を 0 週に設定します。	**位置** /etc/security/pscexpert/bin/chusrattr **準拠値** minage=0
8.5.9	ユーザー・パスワードを少なくとも 90 日おきに変更すること。	パスワードが有効な最大の週数を 13 週に設定します。	**位置** /etc/security/pscexpert/bin/chusrattr **準拠値** maxage=13
2.1	ネットワークにシステムをインストールする前に、ベンダー提供のデフォルトを必ず変更すること。例えば、パスワード、 Simple Network Management Protocol コミュニティー・ストリングを含めてから、不要なアカウントを除去します。	期限切れのパスワードを持つアカウントがシステム内に残る週数を 8 週に設定します。	**位置** /etc/security/pscexpert/bin/chusrattr **準拠値** maxexpired=8
8.5.10	パスワードの長さは 7 文字以上を必要とする。	パスワードの最小の長さを 7 文字に設定します。	**位置** /etc/security/pscexpert/bin/chusrattr **準拠値** minlen=7
8.5.11	数字と英字の両方が入ったパスワードを使用すること。	パスワード内に必要な英字の最小数を 1 に設定します。このように設定すると、パスワードに英字が確実に含まれます。	**位置** /etc/security/pscexpert/bin/chusrattr **準拠値** minalpha=1
8.5.11	数字と英字の両方が入ったパスワードを使用すること。	パスワード内に必要な英字以外の文字の最小数を 1 に設定します。このように設定すると、パスワードに英字以外の文字が確実に含まれます。	**位置** /etc/security/pscexpert/bin/chusrattr **準拠値** minother=1
2.1	ネットワークにシステムをインストールする前に、ベンダー提供のデフォルトを必ず変更すること。例えば、パスワード、 Simple Network Management Protocol コミュニティー・ストリングを含めてから、不要なアカウントを除去します。	パスワード内で文字を繰り返すことができる最大回数を 8 に設定します。この設定は、パスワード内の文字は、その他のパスワードの制限に従う限り何回でも繰り返せることを示します。	**位置** /etc/security/pscexpert/bin/chusrattr **準拠値** maxrepeats=8
8.5.12	個人が、最後の 4 回に使用したパスワードのいずれかと同じ新規パスワードを登録できないようにすること。	パスワードを再使用できるようになるまでの週数を 52 に設定します。	**位置** /etc/security/pscexpert/bin/chusrattr **準拠値** histexpire=52

表 2. *PCI DSS コンプライアンス 2.0 標準に関連する設定 (続き)*

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
8.5.12	個人が、最後の 4 回に使用したパスワードのいずれかと同じ新規パスワードを登録できないようにすること。	ユーザーが再使用できない以前のパスワードの数を 4 に設定します。	**位置** /etc/security/pscexpert/bin/chusrattr **準拠値** histsize=4
8.5.13	多くとも 6 回の試行後にユーザー ID をロックアウトすることにより、アクセス試行の繰り返しを制限すること。	アカウントを使用不可にする連続ログイン試行失敗の数を、非ルート・アカウントごとに 6 回に設定します。	**位置** /etc/security/pscexpert/bin/chusrattr **準拠値** loginretries=6
8.5.13	多くとも 6 回の試行後にユーザー ID をロックアウトすることにより、アクセス試行の繰り返しを制限すること。	ポートを使用不可にする連続ログイン試行失敗の数を 6 回に設定します。	**位置** /etc/security/pscexpert/bin/chdefstanza /etc/security/login.cfg **準拠値** logindisable=6
8.5.14	ロックアウトの期間を少なくとも 30 分か、管理者がユーザー ID を使用可能にするまでに設定すること。	*logindisable* 属性によりポートが使用不可にされた後にポートがロックされる期間を 30 分に設定します。	**位置** /etc/security/pscexpert/bin/chdefstanza /etc/security/login.cfg **準拠値** loginreenable=30
12.3.9	使用後にすぐに使用不能化するという条件で、ベンダーおよびビジネス・パートナーから要求された場合のみ、ベンダーおよびビジネス・パートナーのリモート・アクセス・テクノロジーを活動化すること。	リモート・ルート・ログイン機能を、その機能の値を false に設定することにより使用不可にします。システム管理者は、リモート・ログイン機能を必要に応じて活動化でき、作業が完了したら非活動化できます。	**位置** /etc/security/pscexpert/bin/chuserstanza /etc/security/user **準拠値** rlogin=false root
8.1	すべてのユーザーがシステム・コンポーネントまたはカード所有者のデータにアクセスできるようにする前に、すべてのユーザーに固有 ID を割り当てること。	すべてのユーザーが、システム・コンポーネントまたはカード所有者のデータにアクセスできるようになる前に固有のユーザー名を持つようにする機能を、その機能の値を true に設定することにより使用可能にします。	**位置** /etc/security/pscexpert/bin/chuserstanza /etc/security/user **準拠値** login=true root
10.2	システムで監査を使用可能にすること。	システムでバイナリー・ファイルの監査を使用可能にします。	**位置** /etc/security/pscexpert/bin/pciaudit **準拠値** h
1.1.5 2.2.2	lpd デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	lpd デーモンを停止して、そのデーモンを自動的に開始する、 /etc/inittab ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/comntrows **準拠値** lpd: /etc/inittab : d
1.1.5 2.2.2	共通デスクトップ環境 (CDE) を含む、不要かつ安全でないサービスを使用不可にすること。	Layer Four Traceroute (LFT) が構成されていない場合は、CDE 機能を使用不可にします。	**位置** /etc/security/pscexpert/bin/comntrows **準拠値** "dt" "/etc/inittab" ":" d

表 2. *PCI DSS コンプライアンス 2.0 標準に関連する設定 (続き)*

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
1.1.5 2.2.2	timed デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	timed デーモンを停止して、そのデーモンを自動的に開始する、 /etc/rc.tcpip ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/rctcpip **準拠値** timed d
1.1.5 2.2.2	NTP デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	NTP デーモンを停止して、そのデーモンを自動的に開始する、 /etc/rc.tcpip ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/rctcpip **準拠値** xntpd d
1.1.5 2.2.2	rwhod デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	rwhod デーモンを停止して、そのデーモンを自動的に開始する、 /etc/rc.tcpip ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/rctcpip **準拠値** rwhod d
2.1	ネットワークにシステムをインストールする前に、ベンダー提供のデフォルトを変更すること (SNMP デーモンの使用不可化を含む)。	SNMP デーモンを停止して、そのデーモンを自動的に開始する、 /etc/rc.tcpip ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/rctcpip **準拠値** snmpd d
2.1	ネットワークにシステムをインストールする前に、ベンダー提供のデフォルトを変更すること (SNMPMIBD デーモンの使用不可化を含む)。	SNMPMIBD デーモンを使用不可にします。	**位置** /etc/security/pscexpert/bin/rctcpip **準拠値** snmpmibd d
2.1	ネットワークにシステムをインストールする前に、ベンダー提供のデフォルトを変更すること (AIXMIBD デーモンの使用不可化を含む)。	AIXMIBD デーモンを使用不可にします。	**位置** /etc/security/pscexpert/bin/rctcpip **準拠値** aixmibd d
2.1	ネットワークにシステムをインストールする前に、ベンダー提供のデフォルトを変更すること (HOSTMIBD デーモンの使用不可化を含む)。	HOSTMIBD デーモンを使用不可にします。	**位置** /etc/security/pscexpert/bin/rctcpip **準拠値** hostmibd d
1.1.5 2.2.2	DPID2 デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	DPID2 デーモンを停止して、そのデーモンを自動的に開始する、 /etc/rc.tcpip ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/rctcpip **準拠値** dpid2 d
2.1	ネットワークにシステムをインストールする前に、ベンダー提供のデフォルトを変更すること (DHCP サーバーの停止を含む)。	DHCP サーバーを使用不可にします。	**位置** /etc/security/pscexpert/bin/rctcpip **準拠値** dhcpsd d

表 2. PCI DSS コンプライアンス 2.0 標準に関連する設定 (続き)

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
1.1.5 2.2.2	DHCP エージェントを含む、不要かつ安全でないサービスを使用不可にすること。	DHCP リレー・エージェントを停止して使用不可にしてから、そのエージェントを 自動的に開始する、/etc/rc.tcpip ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/rctcpip **準拠値** dhcprd d
1.1.5 2.2.2	rshd デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	rshd デーモンおよび rshdpci_shell サービスのすべてのインスタンスを停止して使用不可にしてから、そのインスタンスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** shell tcp d
1.1.5 2.2.2	rlogind デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	rlogind デーモンおよび rlogindpci.rlogin サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのインスタンスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** login tcp d
1.1.5 2.2.2	rexecd デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	rexecd デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、 /etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** exec tcp d
1.1.5 2.2.2	comsat デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	comsat デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** comsat udp d
1.1.5 2.2.2	fingerd デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	fingerd デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** finger tcp d

表 2. PCI DSS コンプライアンス 2.0 標準に関連する設定 (続き)

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
1.1.5 2.2.2	systat デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	systat デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** systat tcp d
2.1	ネットワークにシステムをインストールする前に、ベンダー提供のデフォルトを変更すること (netstat コマンドの使用不可化を含む)。	netstat コマンドを使用不可にします。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** netstat tcp d
1.1.5 2.2.2	tftp デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	tftp デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、 /etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** tftp udp d
1.1.5 2.2.2	talkd デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	talkd デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** talk udp d
1.1.5 2.2.2	rquotad デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	rquotad デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** rquotad udp d
1.1.5 2.2.2	rstatd デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	rstatd デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** rstatd udp d

表 2. *PCI DSS コンプライアンス 2.0 標準に関連する設定 (続き)*

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
1.1.5 2.2.2	rusersd デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	rusersd デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** rusersd udp d
1.1.5 2.2.2	rwalld デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	rwalld デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** rwalld udp d
1.1.5 2.2.2	sprayd デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	sprayd デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** sprayd udp d
1.1.5 2.2.2	pcnfsd デーモンを含む、不要かつ安全でないサービスを使用不可にすること。	pcnfsd デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** pcnfsd udp d
1.1.5 2.2.2	TCP echo サービスを含む、不要かつ安全でないサービスを使用不可にすること。	echo(tcp) サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** echo tcp d
1.1.5 2.2.2	TCP discard サービスを含む、不要かつ安全でないサービスを使用不可にすること。	discard(tcp) サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** discard tcp d

表 2. PCI DSS コンプライアンス 2.0 標準に関連する設定 (続き)

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
1.1.5 2.2.2	TCP chargen サービスを含む、不要かつ安全でないサービスを使用不可にすること。	chargen(tcp) サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** chargen tcp d
1.1.5 2.2.2	TCP daytime サービスを含む、不要かつ安全でないサービスを使用不可にすること。	daytime(tcp) サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** daytime tcp d
1.1.5 2.2.2	TCP time サービスを含む、不要かつ安全でないサービスを使用不可にすること。	timed(tcp) サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** time tcp d
1.1.5 2.2.2	UDP echo サービスを含む、不要かつ安全でないサービスを使用不可にすること。	echo(udp) サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** echo udp d
1.1.5 2.2.2	UDP discard サービスを含む、不要かつ安全でないサービスを使用不可にすること。	discard(udp) サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** discard udp d

表 2. *PCI DSS コンプライアンス 2.0 標準に関連する設定 (続き)*

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
1.1.5 2.2.2	chargen サービスを含む、不要かつ安全でないサービスを使用不可にすること。	chargen(udp) サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** chargen udp d
1.1.5 2.2.2	UDP daytime サービスを含む、不要かつ安全でないサービスを使用不可にすること。	daytime(udp) サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** daytime udp d
1.1.5 2.2.2	UDP time サービスを含む、不要かつ安全でないサービスを使用不可にすること。	timed(udp) サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** time udp d
1.1.5 2.2.2	FTP サービスを含む、不要かつ安全でないサービスを使用不可にすること。	ftpd デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** ftp tcp d
1.1.5 2.2.2	telnet サービスを含む、不要かつ安全でないサービスを使用不可にすること。	telnetd デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのデーモンを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** telnet tcp d

表 2. *PCI DSS コンプライアンス 2.0 標準に関連する設定 (続き)*

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
1.1.5 2.2.2	dtspc を含む、不要かつ安全でないサービスを使用不可にすること。	dtspc デーモンのすべてのインスタンスを停止して使用不可にします。AIX Security Expert も、 /etc/inittab ファイル内で LFT が構成されておらず CDE が使用不可の場合にそのデーモンを自動的に開始する、/etc/inittab ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** dtspc tcp d
1.1.5 2.2.2	ttdbserver サービスを含む、不要かつ安全でないサービスを使用不可にすること。	ttdbserver サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** ttdbserver tcp d
1.1.5 2.2.2	cmsd サービスを含む、不要かつ安全でないサービスを使用不可にすること。	cmsd サービスのすべてのインスタンスを停止して使用不可にします。AIX Security Expert ユーティリティーも、そのサービスを自動的に開始する、/etc/inetd.conf ファイル内の対応するエントリーをコメント化します。	**位置** /etc/security/pscexpert/bin/cominetdconf **準拠値** cmsd udp d
2.2.3	誤用を防止するためにシステム・セキュリティー・パラメーターを構成すること。	Set User ID (SUID) コマンドを除去します。	**位置** /etc/security/pscexpert/bin/rmsuidfrmrcmds **準拠値** r
2.2.3	誤用を防止するためにシステム・セキュリティー・パラメーターを構成すること。	ファイル・アクセス権マネージャーの最小セキュリティー・レベルを使用可能にします。	**位置** /etc/security/pscexpert/bin/filepermgr **準拠値** l
2.2.3	誤用を防止するためにシステム・セキュリティー・パラメーターを構成すること。	ネットワーク・ファイル・システム・プロトコルにより提供されるセキュリティー・パラメーターを使用可能にします。	**位置** /etc/security/pscexpert/bin/nfsconfig **準拠値** e
2.2.2	システムの正しい機能に必要な、必要かつ安全なサービス、プロトコル、デーモンなどのみを使用可能にすること。安全でないとみなされる、必要なサービス、プロトコルまたはデーモンに対してセキュリティー・フィーチャーを実装すること。	安全ではない、rlogind、rshd、および tftpd デーモンを使用不可にします。	**位置** /etc/security/pscexpert/bin/disrmtdmns **準拠値** d

表 2. PCI DSS コンプライアンス 2.0 標準に関連する設定 (続き)

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
2.2.2	システムの正しい機能に必要な、必要かつ安全なサービス、プロトコル、デーモンなどのみを使用可能にすること。安全でないとみなされる、必要なサービス、プロトコルまたはデーモンに対してセキュリティー・フィーチャーを実装すること。	安全ではない、rlogind、rshd、および tftpd デーモンを使用不可にします。	**位置** /etc/security/pscexpert/bin/rmrhostsnetrc **準拠値** h
2.2.2	システムの正しい機能に必要な、必要かつ安全なサービス、プロトコル、デーモンなどのみを使用可能にすること。安全でないとみなされる、必要なサービス、プロトコルまたはデーモンに対してセキュリティー・フィーチャーを実装すること。	安全ではない、logind、rshd、および tftpdpci_rmetchostsequiv デーモンを使用不可にします。	**位置** /etc/security/pscexpert/bin/rmetchostsequiv **準拠値** 準拠値は不要です。
1.3.6	確立された接続のみがネットワーク上で許可されるステートフル・インスペクション、すなわちパケット・フィルタリングを実装すること。	ネットワーク **clean_partial_conns** オプションを、その値を 1 に設定することにより使用可能にします。	**位置** /etc/security/pscexpert/bin/ntwkopts **準拠値** clean_partial_conns=1 s
1.3.6	確立された接続のみがネットワーク上で許可されるステートフル・インスペクション、すなわちパケット・フィルタリングを実装すること。	TCP セキュリティーを、ネットワーク **tcp_tcpsecure** オプションの値を 7 に設定することにより使用可能にします。このように設定することで、データ、リセット (RST)、および TCP 接続要求 (SYN) の攻撃から保護します。	**位置** /etc/security/pscexpert/bin/ntwkopts **準拠値** tcp_tcpsecure=7 s
	未使用ポートへの無許可アクセスから保護すること。	その他のシステムが未使用ポートにアクセスできないように、システムがホストを 5 分間回避するようにセットアップします。	**位置** /etc/security/pscexpert/bin/ipsecshunhosthls **準拠値** 準拠値は不要です。
	ホストをポート・スキャンから保護すること。	システムがぜい弱なポートを 5 分間回避するようにセットアップします。こうすることで、ポート・スキャンできないようにします。	**位置** /etc/security/pscexpert/bin/ipsecshunports **準拠値** 準拠値は不要です。
	オブジェクト作成権限を制限すること。	デフォルトのオブジェクト作成権限を 22 に設定します。	**位置** /etc/security/pscexpert/bin/chusrattr **準拠値** umask=22

表 2. *PCI DSS コンプライアンス 2.0 標準に関連する設定 (続き)*

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
	システム・アクセスを制限すること。	ルート ID を、cron.allow ファイルにリストされる唯一のルート ID にするとともに、cron.deny ファイルをシステムから削除します。	**位置** /etc/security/pscexpert/bin/limitsysacc **準拠値** h
	ドットをパス root から除去すること。	root ホーム・ディレクトリーにある以下のファイル内の PATH 環境変数からドットを除去します。 • .cshrc • .kshrc • .login • .profile	**位置** /etc/security/pscexpert/bin/rmdotfrmpathroot **準拠値** 準拠値は不要です。
	ドットを非 root パスから除去すること。	ユーザー・ホーム・ディレクトリーにある以下のファイル内の *PATH* 環境変数からドットを除去します。 • .cshrc • .kshrc • .login • .profile	**位置** /etc/security/pscexpert/bin/rmdotfrmpathnroot **準拠値** 準拠値は不要です。
	システム・アクセスを制限すること。	root ユーザー機能およびユーザー名を /etc/ftpusers ファイルに追加します。	**位置** /etc/security/pscexpert/bin/chetcftpusers **準拠値** a
	ゲスト・アカウントを削除すること。	ゲスト・アカウントおよびそのファイルを削除します。	**位置** /etc/security/pscexpert/bin/execmds **準拠値** rmuser guest; rm -rf /home/guest; ODMDIR=/etc/objrepos odmdelete -qloc0=/home/guest -o inventory
	コンテンツ・スペースでプログラムを起動しないようにすること。	スタック実行不可 (SED) フィーチャーを使用可能にします。	**位置** /etc/security/pscexpert/bin/sedconfig **準拠値** 準拠値は不要です。
	ルートのパスワードがぜい弱でないことを確認すること。	ルート・パスワード完全性チェックをルート・パスワードに対して開始します。こうすることで、強力なルート・パスワードになります。	**位置** /etc/security/pscexpert/bin/chuserstanza **準拠値** /etc/security/user dictionlist=/etc/security/aixpert/dictionary/English rootpci_rootpwdintchk
8.5.15	セッション・アイドル時間を設定することにより、システムへのアクセスを制限すること。	アイドル時間制限を 15 分に設定します。セッションが 15 分より長く使用されていなければ、ユーザーはパスワードを再入力する必要があります。	**位置** /etc/security/pscexpert/bin/autologoff **準拠値** 900

表 2. PCI DSS コンプライアンス 2.0 標準に関連する設定 (続き)

以下の PCI DSS 標準の実装	実装仕様	AIX Security Expert の実装	コンプライアンスに必要な値と設定の位置 (利用可能な場合)
	カード所有者の情報へのトラフィック・アクセスを制限すること。	TCP トラフィック規定を、その最も高い設定にします。こうすることで、ポートに対するサービス妨害が強制的に緩和されます。	**位置** /etc/security/pscexpert/bin/tcptr_aixpert **準拠値** pci
	データ・マイグレーション時にセキュア接続を維持すること。	ライブ・パーティション・マイグレーション時に Virtual I/O Server 間の IP セキュリティー (IPSec) トンネル作成の自動化を使用可能にします。	**位置** /etc/security/pscexpert/bin/cfgsecmig **準拠値** on
1.3.5	ソースが不明なパケットを制限すること。	ハードウェア管理コンソールからパケットを許可します。	**位置** /etc/security/pscexpert/bin/ipsecpermithostorport **準拠値** 準拠値は不要です。
5.1.1	アンチウィルス・ソフトウェアを維持すること。	既知の種類の悪意あるソフトウェアに対して検出、除去、および保護を行なうことにより、システム保全性を維持します。	**位置** /etc/security/pscexpert/bin/manageITsecurity **準拠値** 準拠値は不要です。
	必要に応じてアクセスすること。	必要な権限を持ったシステム・オペレーター、システム管理者、および情報システム・セキュリティー担当者の役割を作成することにより、ロール・ベースのアクセス制御 (RBAC) を使用可能にします。	**位置** /etc/security/pscexpert/bin/EnableRbac **準拠値** 準拠値は不要です。

関連情報:

Payment Card Industry DSS への準拠

Sarbanes-Oxley 法令および COBIT への準拠

アメリカ合衆国の第 107 回連邦議会に基づく Sarbanes-Oxley (SOX) Act of 2002 (2002 年の Sarbanes-Oxley (SOX) 法令) は、投資家の利益を保護するために、証券取引法の対象となる株式公開企業の監査および関連する問題を取り締まるものです。

SOX のセクション 404 では、内部統制に対する管理評価を義務付けています。大半の組織では、内部統制の範囲は、会社の財務データを処理および報告する情報技術システムにまで及びます。SOX 法は、IT および IT セキュリティーに関する具体的な詳細を規定します。多くの SOX 監査員は、適切な IT ガバナンスおよび統制を測定および監査する方法として、COBIT などの規格を使用します。PowerSC Express Edition の SOX/COBIT XML 構成オプションは、COBIT コンプライアンス・ガイドラインに対応するために必要な AIX および 仮想 I/O サーバー (VIOS) システムのセキュリティー構成を提供します。

IBM Compliance Expert Express Edition は、AIX 7.1、AIX 6.1、および AIX 5.3 で稼働します。

外部規格への準拠は、AIX システム管理者が責任を負うワークロードです。IBM Compliance Expert Express Edition は、規格準拠に必要なオペレーティング・システムの設定と報告の管理を簡素化するよう設計されています。

IBM Compliance Expert Express Edition と共に提供される事前構成済みコンプライアンス・プロファイルにより、コンプライアンスの文書を解釈して、これらの規格を特定のシステム構成パラメーターとして実装する管理ワークロードが減ります。

IBM Compliance Expert Express Edition の機能は、お客様が、外部規格への準拠に関連するシステム要件を効果的に管理する上で役立つように設計されています。これにより、コンプライアンスを改善しながらコストを削減できる可能性があります。すべての外部のセキュリティー規格には、システム構成設定以外の側面もあります。IBM Compliance Expert Express Edition の使用によって、規格準拠が保証されるわけではありません。 Compliance Expert は、システム構成設定の管理を簡素化するよう設計されており、管理者が規格準拠の他の側面に集中する上で役立ちます。

関連情報:

COBIT への準拠

Sarbanes-Oxley (SOX) への準拠

医療保険の積算と責任に関する法律 (HIPAA) (Health Insurance Portability and Accountability Act (HIPAA))

医療保険の積算と責任に関する法律 (Health Insurance Portability and Accountability Act (HIPAA)) は、保護されるべき電子医療情報（Electronic Protected Health Information (EPHI)）に焦点を絞ったセキュリティー・プロファイルです。

HIPAA セキュリティー・ルールでは EPHI の保護が明確な焦点となっており、ほんの一部の機関が、その機能と EPHI の使用法に基づいて HIPAA セキュリティー・ルールに従っています。

一部の連邦政府機関と同様に、HIPAA の対象となるすべての団体が、HIPAA セキュリティー・ルールに従わなければなりません。

HIPAA セキュリティー・ルールは、その中で明確に示されているように、EPHI の機密性、保全性、および可用性の保護に重点を置いています。

対象となる団体が作成、受信、維持、または送信する EPHI は、当然予期される脅威や災害、および未許可の使用法や暴露から保護する必要があります。

HIPAA セキュリティー・ルールの要件、規格、および実装仕様は、対象となる以下の団体に適用されます。

- 医療サービス提供者
- 医療保険会社
- 医療事務処理会社
- 医療保険制度の処方薬カードの資金提供者

次の表では、HIPAA セキュリティー・ルールの複数のセクションの詳細を示しています。各セクションには、いくつかの規格および実装仕様が含まれています。

注: HIPAA への準拠を維持するために提供されるすべてのカスタム・スクリプト・ファイルは、`/etc/security/pscexpert/bin` ディレクトリーにあります。

表 3. HIPAA ルールおよび実装の詳細

HIPAA セキュリティー・ルールのセクション	実装仕様	aixpert の実装	コマンドおよび戻り値
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	情報システムのアクティビティーの記録 (監査ログ、アクセス・レポート、セキュリティー・インシデント・レポートなど) を定期的に検討するための手順を実装します。	システム内で監査が有効になっているかどうかを判別します。	**コマンド**: **#audit query** **戻り値**: 正常に実行されると、このコマンドは 0 の値を返して終了します。実行が失敗すると、コマンドは 1 の値を返して終了します。
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	情報システムのアクティビティーの記録 (監査ログ、アクセス・レポート、セキュリティー・インシデント・レポートなど) を定期的に検討するための手順を実装します。	システム内で監査を有効にします。また、キャプチャーするイベントの構成も行います。	**コマンド**: **# audit start >/dev/null 2>&1** **戻り値**: 正常に実行されると、このコマンドは 0 の値を返して終了します。実行が失敗すると、コマンドは 1 の値を返して終了します。 監査対象のイベントは次のとおりです。 **FILE_Mknod, FILE_Open, FS_Mkdir, PROC_Execute, DEV_Create, FILE_Acl, FILE_Chpriv, FILE_Fchpriv, FILE_Mode, INIT_Start, PASSWORD_Change, PASSWORD_Check, PROC_Adjtime, PROC_Kill, PROC_Privilege, PROC_Setpgid, USER_SU, USER_Change, USER_Create, USER_Login, USER_Logout, USER_Reboot, USER_Remove, USER_SetEnv, USER_SU, FILE_Acl,FILE_Fchmod,FILE_Fchown**
164.312 (a) (2) (iV)	暗号化および暗号化解除 (A):EPHI を暗号化および暗号化解除するためのメカニズムを実装します。	暗号化されたファイル・システム (EFS) がシステム上で使用可能にされているかどうかを判別します。	**コマンド**: **# efskeymgr -V >/dev/null 2>&1** **戻り値**: EFS が既に使用可能にされている場合、このコマンドは 0 の値を返して終了します。EFS が使用可能ではない場合、このコマンドは 1 の値を返して終了します。
164.312 (a) (2) (iii)	自動ログオフ (A): 事前に定義された期間アクティビティーがなかった場合に、電子セッションを終了する電子的な手順を実装します。	15 分間アクティビティーがなかった場合に、対話式処理からログアウトするようにシステムを構成します。	**コマンド**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT** **戻り値**: コマンドで値 **TMOUT=15** を検出できなかった場合、スクリプトは 1 の値を返して終了します。それ以外の場合、コマンドは 0 の値を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	すべてのパスワードに、最小でも 14 文字が含まれていることを確認します。	**コマンド**: **chsec -f /etc/security/user -s user -a minlen=8** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、スクリプトはエラー・コード 1 を返して終了します。

表 3. HIPAA ルールおよび実装の詳細 (続き)

HIPAA セキュリティー・ルールのセクション	実装仕様	aixpert の実装	コマンドおよび戻り値
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	すべてのパスワードに少なくとも 2 文字の英字が含まれ、そのうち 1 文字は大文字であることを確認します。	**コマンド**: **chsec -f /etc/security/user -s user –a minalpha=4** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	パスワードに含める非英字の最小文字数を 2 に指定します。	**コマンド**: **#chsec –f /etc/security/user –s user –a minother=2** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	すべてのパスワードに、反復文字が含まれていないことを確認します。	**コマンド**: **#chsec –f /etc/security/user –s user –a maxrepeats=1** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	最近行われた 5 回の変更の中で、同一のパスワードが再利用されていないことを確認します。	**コマンド**: **#chsec –f /etc/security/user –s user –a histsize=5** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	パスワードの有効期間である週の最大数を 13 週間に指定します。	**コマンド**: **#chsec –f /etc/security/user –s user –a maxage=8** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	パスワードの変更が可能になるまでの最小週数要件を除去します。	**コマンド**: **#chsec –f /etc/security/user –s user –a minage=2** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。

表 3. HIPAA ルールおよび実装の詳細 (続き)

HIPAA セキュリティー・ルールのセクション	実装仕様	aixpert の実装	コマンドおよび戻り値
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	ユーザーが設定した **maxage** パラメーターの値の期限が切れた後に、期限切れのパスワードを変更するための最大週数を 4 週間に指定します。	**コマンド**: **#chsec –f /etc/security/user –s user –a maxexpired=4** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	旧パスワードから繰り返し使用できない最小文字数を、4 文字に指定します。	**コマンド**: **#chsec –f /etc/security/user –s user –a mindiff=4** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	パスワード変更が必要であるという警告をシステムが出すまでの日数を 5 に指定します。	**コマンド**: **#chsec –f /etc/security/user –s user –a pwdwarntime = 5** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	ユーザー定義が正しいことを確認して、エラーを修正します。	**コマンド**: **/usr/bin/usrck -y ALL** **/usr/bin/usrck –n ALL** **戻り値**: このコマンドは値を返しません。このコマンドは、エラーがある場合はその検査および修正を行います。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	3 回連続でログイン試行が失敗した場合、そのアカウントをロックします。	**コマンド**: **#chsec –f /etc/security/user –s user –a loginretries=3** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	1 回のログイン失敗と、もう 1 回のログイン失敗の間の遅延を 5 秒に指定します。	**コマンド**: **chsec -f /etc/security/login.cfg -s default -a logindelay=5** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。

表 3. HIPAA ルールおよび実装の詳細 (続き)

HIPAA セキュリティー・ルールのセクション	実装仕様	aixpert の実装	コマンドおよび戻り値
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	ポートがロックされるまでの、ポートでのログイン試行失敗の回数を 10 に指定します。	**コマンド**: **chsec -f /etc/security/lastlog -s username -a ¥ unsuccessful_login_count=10** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	ポートが使用不可にされるまでの、ログイン試行失敗の時間間隔を 60 秒に指定します。	**コマンド**: **#chsec -f /etc/security/lastlog -s user –a time_last_unsuccessful_login=60** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	ポートのロックが解除されるまで、およびポートが使用不可にされるまでの時間間隔を 30 分に設定します。	**コマンド**: **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	パスワードを入力する時間間隔を、30 秒に指定します。	**コマンド**: **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30** **戻り値**: 正常に実行されると、このスクリプトは 0 の値を返して終了します。実行が失敗すると、コマンドはエラー・コード 1 を返して終了します。
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	パスワード管理 (A):パスワードを作成、変更、および保護するための手順を実装します。	35 日間アクティビティーがない場合、アカウントがロックされるようにします。	**コマンド**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}** **戻り値**: コマンドで **account_locked** の値を **true** にできなかった場合、スクリプトは 1 の値を返して終了します。それ以外の場合、コマンドは 0 の値を返して終了します。

表 3. HIPAA ルールおよび実装の詳細 (続き)

HIPAA セキュリティー・ルールのセクション	実装仕様	aixpert の実装	コマンドおよび戻り値
164.312 (c) (1)	EPHI を不正な改ざんまたは破壊行為から保護するためのポリシーおよび手順を実装します。	トラステッド実行 (TE) ポリシーをオンに設定します。	**コマンド**: 以下のコマンドをオンにします。**CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON 例えば、次のとおりです。trustchk –p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON** **戻り値**: 失敗した場合、スクリプトは 1 の値を返して終了します。
164.312 (e) (1)	電子通信ネットワークを介して送信される EPHI への無許可アクセスを防止するための、技術的なセキュリティー対策を実装します。	**ssh** ファイルセットがインストールされているかどうかを判別します。インストールされていない場合は、エラー・メッセージが表示されます。	**コマンド**: **# lslpp –l | grep openssh > /dev/null 2>&1** **戻り値**: このコマンドの戻りコードが 0 の場合、スクリプトは 0 の値を返して終了します。ssh ファイルセットがインストールされていない場合、スクリプトは 1 の値を返して終了し、エラー・メッセージ「`Install ssh filesets for secure transmission`」が表示されます。

次の表では、HIPAA セキュリティー・ルールの複数の機能の詳細を示しています。各機能には、いくつかの規格および実装仕様が含まれています。

表 4. HIPAA 機能および実装の詳細

HIPAA 機能	実装仕様	aixpert の実装	コマンドおよび戻り値
エラー・ロギング	異なる複数のログからエラーを集約して、電子メールを管理者に送信します。	ハードウェア・エラーが存在するかどうかを判別します。 ロケーション `/var/adm/ras/trcfile` にある **trcfile** ファイルに、リカバリー不能エラーがあるかどうかを判別します。 エラーを **root@<hostname>** に送信します。	**コマンド**: **errpt -d H** **戻り値**: 正常に実行されると、このコマンドは 0 の値を返して終了します。実行が失敗すると、コマンドは 1 の値を返して終了します。
FPM 使用可能化	ファイル・アクセス権を変更します。	**fpm** コマンドを使用して、アクセス権およびファイルのリストから、ファイルのアクセス権を変更します。	**コマンド**: **# fpm -1 <level> -f <commands file>** **戻り値**: 正常に実行されると、このコマンドは 0 の値を返して終了します。実行が失敗すると、コマンドは 1 の値を返して終了します。
RBAC 使用可能化	**isso**、**so**、**sa** の各ユーザーを作成し、そのユーザーに該当する役割を割り当てます。	**isso**、**so**、**sa** のユーザーを作成するように勧めます。 それらのユーザーに、該当する役割を割り当てます。	**コマンド**: **/etc/security/aixpert/bin/RbacEnablement**

セキュリティーおよびコンプライアンス自動化の管理

承認された IT ガバナンスおよびコンプライアンスの手順に従って、システムのグループで PowerSC のセキュリティーおよびコンプライアンス自動化プロファイルの計画を立ててデプロイする手順について説明します。

コンプライアンスと IT ガバナンスの一環として、類似したワークロードとデータのセキュリティー・クラスを実行する複数システムを一貫した方法で管理および構成する必要があります。システム上のコンプライアンスを計画してデプロイするには、以下のタスクを実行します。

システムのワークグループの識別

コンプライアンスおよび IT ガバナンスのガイドラインには、類似したワークロードとデータのセキュリティー・クラスを実行する複数システムを一貫した方法で管理および構成する必要があることが記述されています。したがって、類似したワークグループ内のシステムをすべて識別する必要があります。

初期セットアップ用の非実動テスト・システムの使用

適切な PowerSC のコンプライアンス・プロファイルをテスト・システムに適用します。

AIX オペレーティング・システムへのコンプライアンス・プロファイルの適用について、以下の例を検討してください。

例 1: DoD.xml の適用

```
% aixpert -f /etc/security/aixpert/custom/DoD.xml
Processedrules=38       Passedrules=38  Failedrules=0   Level=AllRules

Input file=/etc/security/aixpert/custom/DoD.xml
```

この例では失敗したルールはありません。つまり、Failedrules=0 となっています。これは、すべてのルールが正常に適用され、テスト・フェーズを開始できることを意味します。失敗が起こった場合、詳細な出力が生成されます。

例 2: 失敗が起こった PCI.xml の適用

```
# aixpert -f /etc/security/aixpert/custom/PCI.xml
do_action(): rule(pci_grpck) : failed.
Processedrules=85       Passedrules=84  Failedrules=1   Level=AllRules

Input file=/etc/security/aixpert/custom/PCI.xml
```

pci_grpck ルールの失敗を解決する必要があります。失敗の考えられる原因には、以下の理由があります。

- ルールが環境に適用されないため、削除する必要があります。
- システム上に修正が必要な問題があります。

失敗したルールの調査

大半の場合、PowerSC セキュリティーおよびコンプライアンス・プロファイルを適用するときに失敗は起こりません。ただし、システムで、インストールに関連する前提条件の欠落や、管理者の注意を必要とするその他の問題が発生することがあります。

以下の例を使用して、失敗の原因を調査できます。

/etc/security/aixpert/custom/PCI.xml ファイルを表示して、失敗したルールを見つけます。この例では、ルールは pci_grpck です。 **fgrep** コマンドを実行して、失敗したルール pci_grpck を検索し、関連付けられている XML ルールを表示します。

```
fgrep -p pci_grpck /etc/security/aixpert/custom/PCI.xml
<AIXPertEntry name="pci_grpck" function="grpck"
<AIXPertRuleType type="DLS"/
<AIXPertDescription&gt;Implements portions of PCI Section 8.2,
Check group definitions: Verifies the correctness of group definitions and fixes the errors
</AIXPertDescription
<AIXPertPrereqList&gt;bos.rte.security,bos.rte.date,bos.rte.ILS</AIXPertPrereqList
<AIXPertCommand
/etc/security/aixpert/bin/execmds</AIXPertCommand
<AIXPertArgs
"/usr/sbin/grpck -y ALL; /usr/sbin/grpck -n ALL"</AIXPertArgs
<AIXPertGroup
User Group System and Password Definitions</AIXPertGroup
</AIXPertEntry
```

pci_grpck ルールから、/usr/sbin/grpck コマンドを表示できます。

失敗したルールの更新

PowerSC のセキュリティーおよびコンプライアンス・プロファイルを適用する際、エラーが検出される場合があります。

システムでは、インストール前提条件の欠落や、管理者の注意を必要とするその他の問題が発生することがあります。失敗したルールの基礎となるコマンドを判別した後で、システムを検査して、失敗した構成コマンドを理解します。システムにセキュリティー問題が発生している可能性があります。また、特定のルールがシステムの環境に適用されない場合もあります。その場合は、カスタム・セキュリティー・プロファイルを作成する必要があります。

カスタム・セキュリティー構成プロファイルの作成

ルールがシステムの特定の環境に適用されない場合、大半のコンプライアンス組織は文書化された例外を許可します。

ルールを削除してカスタム・セキュリティー・ポリシーおよび構成ファイルを作成するには、以下のステップを実行します。

1. 以下のファイルの内容を、/etc/security/aixpert/custom/<*my_security_policy*>.xml という名前の単一のファイルにコピーします。

   ```
   /etc/security/aixpert/custom/[PCI.xml|DoD.xml|SOX-COBIT.xml]
   ```

2. 適用されないルールを、最初の XML タグ <AIXPertEntry name... と最後の XML タグ </AIXPertEntry の間から削除することにより、<*my_security_policy*>.xml ファイルを編集します。

セキュリティーに関する追加の構成ルールを挿入できます。追加のルールは、XML AIXPertSecurityHardening スキーマに挿入します。PowerSC のプロファイルを直接的に変更することはできませんが、プロファイルをカスタマイズすることはできます。

大半の環境では、カスタム XML ポリシーを作成する必要があります。カスタマー・プロファイルを他のシステムに配布するには、カスタマイズした XML ポリシーを、同じ構成を必要とするシステムに安全な方法でコピーする必要があります。カスタム XML ポリシーを他のシステムに配布するために Secure File Transfer Protocol (SFTP) などのセキュア・プロトコルが使用され、プロファイルは安全な場所 /etc/security/aixpert/custom/<*my_security_policy.xml*>/etc/security/aixpert/custom/ に保管されます。

カスタム・プロファイルを作成する必要があるシステムにログオンして、次のコマンドを実行します。

```
aixpert -f :  /etc/security/aixpert/custom/<my_security_policy>.xml
```

AIX Profile Manager を使用したアプリケーションのテスト

セキュリティー構成は、アプリケーションおよびシステムへのアクセス方法とシステムの管理方法に影響を与える可能性があります。システムを実稼働環境にデプロイする前に、アプリケーションおよび予期されるシステム管理方法をテストすることが重要です。

規制コンプライアンス規格では、出来合いの構成よりも厳しいセキュリティー構成が義務付けられます。システムをテストするには、以下のステップを実行します。

1. AIX Profile Manager のウェルカム・ページの右側のペインから「**プロファイルの表示および管理**」を選択します。
2. モニター対象のシステムにデプロイするためのテンプレートによって使用されているプロファイルを選択します。
3. 「**比較**」をクリックします。
4. 管理対象グループを選択するか、グループ内の個々のシステムを選択して、「**追加**」をクリックし、それらを選択済みボックスに追加します。
5. 「**OK**」をクリックします。

比較操作が開始されます。

継続的なコンプライアンスのための、AIX Profile Manager を使用したシステムのモニター

セキュリティー構成は、アプリケーションおよびシステムへのアクセス方法とシステムの管理方法に影響を与える可能性があります。システムを実稼働環境にデプロイする際に、アプリケーションおよび予期されるシステム管理方法をモニターすることが重要です。

AIX Profile Manager を使用して AIX システムをモニターするには、以下のステップを実行します。

1. AIX Profile Manager のウェルカム・ページの右側のペインから「**プロファイルの表示および管理**」を選択します。
2. モニター対象のシステムにデプロイするためのテンプレートによって使用されているプロファイルを選択します。
3. 「**比較**」をクリックします。
4. 管理対象グループを選択するか、グループ内の個々のシステムを選択して、それらを選択済みボックスに追加します。
5. 「**OK**」をクリックします。

比較操作が開始されます。

PowerSC のセキュリティーおよびコンプライアンス自動化の構成

コマンド行から AIX Profile Manager を使用して、セキュリティーおよびコンプライアンス自動化のために PowerSC を構成する手順について説明します。

PowerSC のコンプライアンス・オプション設定の構成

PowerSC のセキュリティーおよびコンプライアンス自動化フィーチャーの基礎、非実動テスト・システムでの構成のテスト、設定の計画およびデプロイメントについて説明します。コンプライアンス構成を適用する際、設定により、オペレーティング・システムの多くの構成設定が変更されます。

注: Telnet は平文パスワードを使用するため、一部のコンプライアンス規格およびプロファイルによって Telnet が使用不可に設定されます。そのため、Open SSH がインストールされ、構成され、作動している必要があります。構成されているシステムとの間で、他の安全な通信手段を使用することができます。これらのコンプライアンス規格では、root ログインを使用不可にする必要があります。構成変更の適用を続行する前に、1 人以上の非 root ユーザーを構成します。この構成では root は使用不可にならず、非 root ユーザーとしてログインして、root に対して **su** コマンドを実行することができます。システムへの SSH 接続を確立して、非 root ユーザーとしてログインし、root に対してコマンドを実行することができるかどうかテストしてください。

DoD、PCI、SOX、または COBIT 構成プロファイルにアクセスするには、次のディレクトリーを使用します。

- AIX オペレーティング・システムのプロファイルは、/etc/security/aixpert/custom ディレクトリーにあります。
- 仮想 I/O サーバー (VIOS) のプロファイルは、/etc/security/aixpert/core ディレクトリーにあります。

コマンド行からの PowerSC のコンプライアンスの構成

AIX システムでは **aixpert** コマンド、仮想 I/O サーバー (VIOS) では **viosecure** コマンドを使用して、コンプライアンス・プロファイルを実装または検査します。

AIX システムで PowerSC のコンプライアンス・プロファイルを適用するには、適用するセキュリティー・コンプライアンスのレベルに応じて以下のいずれかのコマンドを入力します。

表 5. AIX の PowerSC コマンド

コマンド	コンプライアンス規格
% aixpert -f /etc/security/aixpert/custom/DoD.xml	*米国国防総省の UNIX Security Technical Implementation Guide*
% aixpert -f /etc/security/aixpert/custom/PCI.xml	*Payment Card Industry-Data Security Standard*
% aixpert -f /etc/security/aixpert/custom/SOX-COBIT.xml	*Sarbanes-Oxley Act of 2002 (2002 年サーベンス・オクスリー法) - COBIT IT ガバナンス*

VIOS システムで PowerSC のコンプライアンス・プロファイルを適用するには、適用するセキュリティー・コンプライアンスのレベルに応じて以下のいずれかのコマンドを入力します。

表 6. 仮想 I/O サーバー の PowerSC コマンド

コマンド	コンプライアンス規格
% viosecure -file /etc/security/aixpert/custom/DoD.xml	*米国国防総省の UNIX Security Technical Implementation Guide*
% viosecure -file /etc/security/aixpert/custom/PCI.xml	*Payment Card Industry-Data Security Standard*
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	*Sarbanes-Oxley Act of 2002 (2002 年サーベンス・オクスリー法) - COBIT IT ガバナンス*

AIX システムの **aixpert** コマンド、および VIOS の **viosecure** コマンドは、システム全体を検査または設定してセキュリティー関連の構成変更を行うため、実行に時間がかかることがあります。出力は、次の例のようになります。

```
Processedrules=38       Passedrules=38  Failedrules=0   Level=AllRules
```

ただし、AIX 環境、インストール・セット、および以前の構成によっては、一部のルールが失敗します。

例えば、システムに必要なインストール・ファイルセットがないことが原因で、前提条件ルールが失敗することがあります。コンプライアンス・プロファイルをデータ・センター全体にデプロイする前に、それぞれの失敗を理解して解決する必要があります。

関連概念:

25 ページの『セキュリティーおよびコンプライアンス自動化の管理』
承認された IT ガバナンスおよびコンプライアンスの手順に従って、システムのグループで PowerSC のセキュリティーおよびコンプライアンス自動化プロファイルの計画を立ててデプロイする手順について説明します。

AIX Profile Manager を使用した PowerSC のコンプライアンスの構成

AIX Profile Manager を使用して PowerSC のセキュリティーおよびコンプライアンス・プロファイルを構成し、構成を AIX 管理対象システムにデプロイする手順について説明します。

AIX Profile Manager を使用して PowerSC のセキュリティーおよびコンプライアンス・プロファイルを構成するには、以下のステップを実行します。

1. IBM Systems Director にログインして、AIX Profile Manager を選択します。
2. 以下のステップを実行して、いずれかの PowerSC のセキュリティーおよびコンプライアンス・プロファイルに基づくテンプレートを作成します。
   a. AIX Profile Manager のウェルカム・ページの右側のペインで「**テンプレートの表示および管理**」をクリックします。
   b. 「**作成**」をクリックします。
   c. 「**テンプレート・タイプ (Template type)**」リストで「**オペレーティング・システム (Operating System)**」をクリックします。
   d. 「**構成テンプレート名 (Configuration template name)**」フィールドにテンプレートの名前を指定します。
   e. 「**続行**」 > 「**保存**」をクリックします。
3. 「**このテンプレートに使用するプロファイルの選択**」オプションで「**ブラウズ**」を選択して、テンプレートに使用するプロファイルを選択します。プロファイルでは、以下の項目が表示されます。
   - `ice_DLS.xml` は、AIX オペレーティング・システムのデフォルトのセキュリティー・レベルです。
   - `ice_DoD.xml` は、米国国防総省の Security and Implementation Guide (UNIX 用) の設定です。
   - `ice_HLS.xml` は、AIX 設定に関する汎用の高水準のセキュリティーです。
   - `ice_LLS.xml` は、AIX 設定に関する低水準のセキュリティーです。
   - `ice_MLS.xml` は、AIX 設定に関する中間レベルのセキュリティーです。
   - `ice_PCI.xml` は、AIX オペレーティング・システムに関する Payment Card Industry の設定です。
   - `ice_SOX.xml` は、AIX オペレーティング・システムに関する SOX または COBIT の設定です。
4. 選択済みボックスからプロファイルを削除します。
5. 必要なプロファイルを選択済みボックスに移動するには、「**追加**」を選択します。
6. 「**保存**」をクリックします。

構成を AIX 管理対象システムにデプロイするには、以下のステップを実行します。

1. AIX Profile Manager のウェルカム・ページの右側のペインで「**テンプレートの表示および管理**」を選択します。
2. デプロイ対象として必要なテンプレートを選択します。
3. 「**デプロイ**」をクリックします。

4. プロファイルのデプロイ先となるシステムを選択して、「**追加**」をクリックし、必要なプロファイルを選択済みボックスに移動します。
5. 「**OK**」をクリックして、構成テンプレートをデプロイします。プロファイルの選択済みテンプレートに従ってシステムが構成されます。

DoD、PCI、または SOX に関するデプロイメントが正常に行われるために、PowerSC Express Edition または PowerSC Standard Edition が AIX システムのエンドポイントにインストールされている必要があります。デプロイされるシステムに PowerSC がインストールされていない場合、デプロイメントは失敗します。IBM Systems Director は、選択された AIX システムのエンドポイントに構成テンプレートをデプロイして、コンプライアンス要件に従ってそれらを構成します。

関連情報:

AIX Profile Manager

IBM Systems Director

PowerSC Real Time Compliance

PowerSC Real Time Compliance フィーチャーは、使用可能にされた AIX システムを継続的にモニターし、これらのシステムの構成の一貫性と安全性を確認します。

PowerSC Real Time Compliance フィーチャーは、PowerSC コンプライアンス自動化および AIX Security Expert のポリシーと連動し、コンプライアンスの違反が発生した場合、またはモニター対象のファイルが変更された場合に通知します。システムのセキュリティー構成ポリシーの違反が発生した場合、PowerSC Real Time Compliance フィーチャーは 電子メールまたはテキスト・メッセージを送信して、システム管理者にアラートを出します。

PowerSC Real Time Compliance フィーチャーは、受動的なセキュリティー・フィーチャーであり、米国国防総省の Security Technical Implementation Guide、Payment Card Industry Data Security Standard、Sarbanes-Oxley 法令、および COBIT のコンプライアンスを含む、事前定義または変更されたコンプライアンス・プロファイルをサポートします。このフィーチャーは、変更をモニターするファイルのデフォルト・リストを提供しますが、このリストにはファイルを追加することができます。

PowerSC Real Time Compliance のインストール

PowerSC Real Time Compliance フィーチャーは、PowerSC Express Edition と共にインストールされます。また、このフィーチャーは、ベースの AIX オペレーティング・システムの一部ではありません。

PowerSC Real Time Compliance を含む PowerSC Express Edition をインストールするには、以下のステップを実行します。

1. PowerSC Real Time Compliance フィーチャーをインストールする予定のシステムで、以下のいずれかの AIX オペレーティング・システムが稼働していることを確認します。
   - IBM AIX 6 (テクノロジー・レベル 7 適用) 以降 (AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 6.1.7.0) 以降付き)
   - IBM AIX 7 (テクノロジー・レベル 1 適用) 以降 (AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 7.1.1.0 以降付き)
2. PowerSC Express Edition バージョン 1.1.2.0 以降を既にインストールしている場合は、PowerSC Express Edition を再インストールするか、インストール済みの PowerSC Real Time Compliance フィーチャーを最新バージョンに更新することによって、PowerSC Real Time Compliance フィーチャーに必要なファイルを追加することができます。

3. PowerSC Real Time Compliance フィーチャーのファイルセットを更新するには、PowerSC Express Edition バージョン 1.1.2.0 以降のインストール・パッケージから `powerscExp.rtc` ファイルセットをインストールします。
4. PowerSC Express Edition バージョン 1.1.2.0 以前を新しくインストールする場合は、PowerSC Express Edition バージョン 1.1.2 以前のインストール (Installing PowerSC Express Edition Version 1.1.2, or earlier) の説明に従ってください。

PowerSC Real Time Compliance の構成

PowerSC Real Time Compliance を構成して、コンプライアンス・プロファイルの違反またはモニター対象のファイルの変更が発生した場合に、アラートを送信するようにします。プロファイルの例としては、米国国防総省の Security Technical Implementation Guide、Payment Card Industry Data Security Standard、Sarbanes-Oxley 法令、および COBIT があります。

以下のいずれかの方式を使用して、PowerSC Real Time Compliance を構成することができます。

- **mkrtc** コマンドを入力します。
- 以下のコマンドを入力して、SMIT ツールを実行します。

  ```
  smit RTC
  ```

PowerSC Real Time Compliance フィーチャーによってモニターされるファイルの識別

PowerSC Real Time Compliance フィーチャーは、ハイレベル・セキュリティー設定からのファイルのデフォルト・リストに変更がないかどうかをモニターします。この設定は、`/etc/security/rtc/rtcd_policy.conf` ファイルにあるファイル・リストでファイルを追加または削除することによって、カスタマイズすることができます。

システムに適用されるコンプライアンス・テンプレートを識別するには、2 つの方式があります。 1 つは **aixpert** コマンドを使用し、もう 1 つの方式では IBM Systems Director で AIX プロファイル・マネージャーを使用します。

コンプライアンス・プロファイルが識別されたら、モニター対象のファイル・リストにファイルを追加することができます。これを行うには、`/etc/security/rtc/rtcd_policy.conf` ファイルに追加のファイルを組み込みます。ファイルを保存したら、新しいリストがすぐにベースラインとして使用され、システムを再始動せずに変更がモニターされます。

PowerSC Real Time Compliance に対するアラートの設定

PowerSC Real Time Compliance フィーチャーの通知を、アラートのタイプとアラートの受信者を指示することによって構成する必要があります。

PowerSC Real Time Compliance フィーチャーのメイン・コンポーネントである rtcd デーモンは、アラートのタイプと受信者に関する情報を `/etc/security/rtc/rtcd.conf` 構成ファイルから取得します。テキスト・エディターを使用してこのファイルを編集し、情報を更新することができます。

オプション、およびこのファイルの変更方法については、rtcd.conf ファイルに関する情報を参照してください。

関連情報:
リアルタイム・コンプライアンスの /etc/security/rtc/rtcd.conf ファイル・フォーマット

PowerSC Express Edition コマンド

PowerSC Express Edition で使用可能なコマンドでは、コマンド行を使用することによりコンプライアンス設定を変更する方法を提供します。

pscxpert コマンド

目的

システム管理者を補助して、セキュリティー構成を設定します。

構文

pscxpert

pscxpert -l h|high | m|medium | l|low | d|default [-p] [-n -o *filename*] [**-a -o** *filename*]

pscxpert -c [-P *filename*] [**-r**] [**-R**] [**-l h|high | m|medium | l|low | d|default**] [**-p**]

pscxpert -u [-p]

pscxpert -d

pscxpert [**-f** *profile_name*]

pscxpert [**-f** *profile_name*] [**-a -o** *filename*] [**-p**]

pscxpert -t

説明

pscxpert コマンドは、いろいろなシステム構成を設定して、望ましいセキュリティー・レベルを使用可能にします。

pscxpert コマンドを **-l** フラグ設定のみで実行すると、ユーザーが設定を構成できるようにすることなく、セキュリティー設定が迅速に実装されます。例えば、 **pscxpert -l high** コマンドを実行すると、すべての高水準のセキュリティー設定がシステムに自動的に適用されます。ただし、 **pscxpert -l** コマンドを **-n** および **-o** の *filename* オプションで実行すると、セキュリティー設定は *filename* パラメーターによって指定されたファイルに保管されます。その次に **-f** フラグが新規構成を適用します。

最初に選択した後で、その選択済みセキュリティー・レベルに関連したすべてのセキュリティー構成オプションを示すメニューが表示されます。これらのオプションは、全体または個別に (オフまたはオンを切り替えて) 受け入れることができます。第 2 の変更の後で、**pscxpert** コマンドはこのセキュリティー設定をコンピューター・システムに適用し続けます。

注: ソフトウェアのインストールまたは更新などの大きなシステム変更の後に、 **pscxpert** コマンドを再実行します。**pscxpert** コマンドが再実行されるときに、特別なセキュリティー構成の項目を選択解除すると、その構成項目はスキップされます。

フラグ

項目	説明
-a	関連したレベルのセキュリティー・オプションを持つ設定は、 **-o** フラグによって指定されたファイルに省略フォーマットで書き込まれます。**-a** オプションを指定する場合は、**-o** オプションも指定する必要があります。
-c	前に適用された規則のセットに照らし合わせてセキュリティー設定を検査します。規則についての検査が失敗した場合は、その規則の前のバージョンも検査されます。このプロセスは検査がパスするまで、または **/etc/security/aixpert/core/appliedaixpert.xml** ファイル内にある失敗した規則のすべてのインスタンスが検査されるまで継続されます。
-d	文書型定義 (DTD) を表示します。
-f	指定された *profile_name* ファイルに設定されたセキュリティー設定を適用します。このプロファイルは、`/etc/security/aixpert/custom` ディレクトリーにあります。使用可能なプロファイルには、以下の標準プロファイルが含まれています。 **DataBase.xml** このファイルには、デフォルトのデータベース設定の要件が入っています。 **DoD.xml** このファイルには、米国国防総省の Security Technical Implementation Guide (STIG) 設定の要件が入っています。 **DoD_to_AIXDefault.xml** これは、デフォルトの AIX 設定に対する設定変更を行います。 **Hipaa.xml** このファイルには、医療保険の積算と責任に関する法律 (Health Insurance Portability and Accountability Act (HIPAA)) 設定の要件が入っています。 **PCI.xml** このファイルには、Payment Card Industry Data Security Standard 設定の要件が入っています。 **PCI_to_AIXDefault.xml** このファイルは、デフォルトの AIX 設定に対する設定変更を行います。 **SCBPS.xml** このファイルには、Sarbanes-Oxley 法令および COBIT の設定の要件が入っています。 既存の XML ファイルの名前変更および変更を行なうことにより、同じディレクトリーにカスタム・プロファイルを作成して、それを設定に適用することもできます。 例えば、以下のコマンドでは HIPAA プロファイルをシステムに適用します。 `pscxpert -f /etc/security/aixpert/custom/Hipaa.xml` **-f** オプションを指定すると、 **appliedaixpert.xml** ファイルをシステムからシステムへ安全に転送し適用することによって、セキュリティー設定を整合性のとれた状態でシステムからシステムへ適用できるようになります。 正常に適用されたルールはすべて **/etc/security/aixpert/core/appliedaixpert.xml** ファイルに書き込まれ、対応する「元に戻す」アクションのルールは、 **/etc/security/aixpert/core/undo.xml** ファイルに書き込まれます。

項目	説明
-l	システム・セキュリティー設定を、指定されたレベルに設定します。このフラグには次のオプションがあります。 **h|high** 高水準のセキュリティー・オプションを指定します。 **m|medium** 中間レベルのセキュリティー・オプションを指定します。 **l|low** 低水準のセキュリティー・オプションを指定します。 **d|default** AIX 標準レベルのセキュリティー・オプションを指定します。 **-l** フラグと **-n** フラグの両方を指定すると、セキュリティー設定はシステムに実装されず、**-o** フラグで指定したファイルに書き込まれるのみとなります。 正常に適用されたルールはすべて **/etc/security/aixpert/core/appliedaixpert.xml** ファイルに書き込まれ、対応する「元に戻す」アクションのルールは **/etc/security/aixpert/core/undo.xml** ファイルに書き込まれます。 **重要: d|default** オプションを使用すると、 **pscxpert** コマンド (またはそれ以外の方法) で以前に設定したセキュリティー設定を上書きして、システムを従来のオープン構成に戻すことができます。
-n	関連したレベルのセキュリティー・オプションを持つ設定を、 **-o** フラグによって指定されたファイルに書き込みます。**-n** オプションを使用する場合は、**-o** オプションも指定する必要があります。
-o	セキュリティー出力を *filename* 変数によって指定されたファイルに保管します。出力ファイルの読み取りおよび書き込みの権限は、セキュリティー予防措置として root に設定されます。このファイルは、望ましくないアクセスに対して保護されていなければなりません。
-p	詳細出力を使用して、セキュリティー・ルールの出力結果が表示されるように指定します。**監査の設定**オプションがオンの場合に **-p** オプションを使用すると、処理済みのルールが、監査サブシステムのログに記録されます。このオプションは、 **-l**、**-u**、**-c**、および **-f** のいずれのオプションとも一緒に使用できます。
-P	プロファイル名を入力として受け入れます。このオプションは、**-c** オプションと一緒に使用されます。**-c** オプションを **-P** オプションと一緒に使用すると、パス済みのプロファイルとシステムの互換性を検査することができます。
-r	システムの既存設定を `/etc/security/aixpert/check_report.txt` ファイルに書き込みます。出力をセキュリティーまたはコンプライアンスの監査レポートで使用できます。レポートは、各設定、設定が規制のコンプライアンス要件とどのように関係しているか、およびチェックが合格したか失敗したかを記述します。
-R	**-r** フラグと同じ出力を生成しますが、このフラグでは構成設定を実装するために使用された各スクリプトまたは各プログラムに関する記述も付加します。
-t	システムで適用されるプロファイルのタイプを表示します。
-u	適用されるセキュリティー設定を元に戻します。

パラメーター

項目	説明
filename	セキュリティー設定を保管する出力ファイル。このファイルをアクセスするには、root アクセス権が必要です。
profile_name	システムのコンプライアンス・ルールを提供するプロファイルのファイル名。このファイルをアクセスするには、root アクセス権が必要です。

セキュリティー

pscxpert コマンドを実行できるのは、root のみです。

例

1. 高水準のセキュリティー・オプションをすべて出力ファイルに書き込むには、次のコマンドを入力します。

   ```
   pscxpert -l high -n -o /etc/security/pscexpert/plugin/myPreferredSettings.xml
   ```

   このコマンドの完了後は、出力ファイルを編集でき、特定のセキュリティー・ロールを標準 XML コメント文字列 (<-- でコメントを開始し、 -\> でコメントを閉じる) で囲むことによってコメント化できます。
2. 米国国防総省 STIG 構成ファイルからセキュリティー設定を適用するには、次のコマンドを入力します。

   ```
   pscxpert -f /etc/security/aixpert/custom/Dod.xml
   ```
3. HIPAA 構成ファイルからセキュリティー設定を適用するには、次のコマンドを入力します。

   ```
   pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
   ```
4. システムのセキュリティー設定を確認したり、失敗したルールを監査サブシステムのログに記録したりするには、次のコマンドを入力します。

   ```
   pscxpert –c -p
   ```
5. レポートを生成して /etc/security/aixpert/check_report.txt ファイルに書き込むには、次のコマンドを入力します。

   ```
   pscxpert -c -r
   ```

位置

項目	説明
/usr/sbin/pscxpert	**pscxpert** コマンドが入っています。

ファイル

項目	説明
/etc/security/aixpert/log/aixpert.log	適用済みセキュリティー設定のトレース・ログが入っています。これは syslog 標準を使用しません。**pscxpert** コマンドは、ファイルに対する直接書き込みを行い、読み取り/書き込みの権限を持ち、さらに root セキュリティーを必要とします。
/etc/security/aixpert/log/firstboot.log	デフォルトの保護機能 (SbD) をインストールして最初にブートする際に適用された、セキュリティー設定のトレース・ログが入っています。
/etc/security/aixpert/core/undo.xml	元に戻すことのできるセキュリティー設定の XML リストが入っています。

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。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

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

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

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

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

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Dept. LRAS/Bldg. 903
11501 Burnet Road

Austin, TX 78758-3400
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

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

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

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

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

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

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

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。 このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。 従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。サンプル・プログラムは、いかなる種類の保証なしに、現存するままの状態で提供されます。 IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。 IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらのCookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

この「ソフトウェア・オファリング」は、Cookie もしくはその他のテクノロジーを使用して個人情報を収集することはありません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie などの各種テクノロジーの使用について詳しくは、『IBM オンラインでのプライバシー・ステートメントのハイライト』(http://www.ibm.com/privacy/jp/ja/)、『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』というタイトルのセクション、および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corp. の商標です。 他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。 現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml の「Copyright and trademark information」をご覧ください。

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。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[ハ行]

[ラ行]

P

S

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21