IBM PowerSC
Standard Edition
バージョン 1.1.4

PowerSC Standard Edition

IBM PowerSC
Standard Edition
バージョン 1.1.4

PowerSC Standard 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、 179 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 Standard Edition のバージョン 1.1.4、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
Standard Edition
Version 1.1.4
PowerSC Standard 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

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。

PowerSC Standard Edition 1.1.4 の新機能

PowerSC™ Standard Edition バージョン 1.1.4 のトピック集の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。

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。

2015 年 12 月

- 以下のトピックに、コンプライアンス・プロファイルに関する情報が追加されました。
  - 110 ページの『北米電力信頼度協議会 (North American Electric Reliability Corporation) への準拠』
  - 86 ページの『Payment Card Industry - Data Security Standard への準拠』
  - 10 ページの『米国国防総省の STIG への準拠』
  - 103 ページの『Sarbanes-Oxley 法令および COBIT への準拠』
  - 104 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))』
- 121 ページの『PowerSC Real Time Compliance』のトピックに、リアルタイム・コンプライアンス機能に関する情報が追加されました。
- **psconf** コマンドに、**clientData** 操作と **default_policy** 操作、および **-l** フラグと **-g** フラグが追加されました。
- **pscxpert** コマンドのフラグ **-a**、**-c**、**-l**、および **-n** が更新されました。
- **pmconf** コマンドの **-i** フラグと **-x** フラグが更新されました。

PowerSC Standard Edition リリース・ノート・バージョン 1.1.4

このリリース・ノートには、資料が完成した後に確認された PowerSC Standard Edition バージョン 1.1.4 に対する変更についての情報が記載されています。

PowerSC Standard Edition ファイルセットの変更

PowerSC Express Edition は IBM® から購入できなくなりました。PowerSC Standard Edition 1.1.4 以降には、以前 PowerSC Express Edition で使用可能だった以下の機能とフィーチャーが含まれています。

- 米国国防総省の STIG への準拠
- Sarbanes-Oxley 法令および COBIT 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)) への準拠
- リアルタイム・コンプライアンス

次の表に、PowerSC Standard Edition バージョン 1.1.4 以降のファイルセットにマージされた PowerSC Express Edition ファイルセットの名前を示します。

表 1. PowerSC Standard Edition 1.1.4 以降のファイル・セット

PowerSC Express Edition ファイルセット	PowerSC Standard Edition ファイルセット
powerscExp.rtc	powerscStd.rtc
powerscExp.msg.<LANG>	powerscStd.msg.<LANG>
powerscExp.license	powerscStd.license
powerscExp.ice	powerscStd.ice

PowerSC Standard Edition のインストール前に読む情報

最新版のリリース・ノートを表示するには、IBM Knowledge Center に掲載されているオンライン・リリース・ノート (http://www.ibm.com/support/knowledgecenter/SSTQK9_1.1.4/com.ibm.powersc114.se/powersc_se_rn.htm) を参照してください。

PowerSC Standard Edition はライセンス・プログラムであり、AIX オペレーティング・システムには含まれていません。

注: このソフトウェアには、ビジネスに重大な影響を及ぼす可能性があるエラーが含まれている場合があります。このソフトウェア製品を使用する前に、使用可能な最新のフィックスをインストールしてください。

インストール、移行、アップグレード、および構成の情報

PowerSC Standard Edition のインストールについては、PowerSC Standard Edition 1.1.4 のインストールを参照してください。

PowerSC Standard Edition 用にサポートされているハードウェアおよび AIX オペレーティング・システムのバージョンについては、PowerSC Standard Edition 1.1.4 の概念を参照してください。

Trusted Network Connect を実行するための追加のファイルセット要件

Trusted Network Connect を実行するには、IBM PowerSC Standard Edition DVD に含まれる `powerscStd.tnc_commands` ファイルセットをインストールする必要があります。**installp** コマンドを使用して、AIX システムにこのファイルセットをインストールしてください。このファイルセットでは、**psconf** コマンドおよび **pmconf** コマンドの機能が提供されます。

注: Trusted Network Connect の IP リファラー機能を使用する場合は、ご使用の VIOS システムに `powerscStd.tnc_commands` ファイルセットもインストールする必要があります。

コマンドの変更

以下のコマンドが変更されました。

- IBM AIX 6 (テクノロジー・レベル 8 適用) 以降では、**tncconsole** コマンドを使用して、Trusted Network Connect (TNC) サーバー、TNC クライアント、TNC IP Referrer (IPRef)、および Service Update Management Assistant (SUMA) のレポート作成と管理を行えます。ただし、**tncconsole** コマンドの機能は限定されています。**tncconsole** コマンドのすべての機能を使用するには、PowerSC Standard Edition をインストールする必要があります。PowerSC Standard Edition では、**tncconsole** コマンドの名前が変更され、**psconf** コマンドになりました。
- **pscxpert** コマンドから **-o** フラグが除去されました。

PowerSC Standard Edition 1.1.4 の概念

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

PowerSC Standard Edition 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強力な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 Standard Edition は、セキュリティーおよびコンプライアンス自動化、トラステッド・ブート、トラステッド・ファイアウォール、トラステッド・ロギング、トラステッド・ネットワーク接続およびパッチ管理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 2. PowerSC Standard Edition のコンポーネント、説明、オペレーティング・システム・サポート、およびハードウェア・サポート

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® • POWER8
トラステッド・ブート	ブート・イメージ、オペレーティング・システム、およびアプリケーションを計測し、仮想トラステッド・プラットフォーム・モジュール (TPM) テクノロジーを使用してそれらの信頼性を認証します。	• AIX 6 (6100-07 適用) 以降 • AIX 7 (7100-01 適用) 以降	POWER7 ファームウェア eFW7.4 以降
トラステッド・ファイアウォール	同じ 仮想 I/O サーバー が制御する指定された仮想 LAN (VLAN) の間で直接ルーティングを使用可能にすることで、時間とリソースを節約します。	• AIX 6.1 • AIX 7.1 • VIOS バージョン 2.2.1.4 以降	• POWER6 • POWER7 • POWER8 • 仮想 I/O サーバー バージョン 6.1S 以降

表 2. PowerSC Standard Edition のコンポーネント、説明、オペレーティング・システム・サポート、およびハードウェア・サポート (続き)

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
トラステッド・ロギング	AIX のログは、リアルタイムで仮想入出力サーバー (VIOS) に集中的に配置されます。このフィーチャーは、改ざん防止機能を備えたロギングと、便利なログ・バックアップおよび管理を提供します。	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7 • POWER8
トラステッド・ネットワーク接続およびパッチ管理	仮想環境のすべての AIX システムが指定のソフトウェアおよびパッチ・レベルであることを検査して、すべての AIX システムが指定のソフトウェア・レベルであることを確認するための管理ツールを提供します。ダウン・レベルの仮想システムがネットワークに追加された場合や、システムに影響を与えるセキュリティー・パッチが発行された場合にアラートを提供します。	• AIX 5.3 • AIX 6.1 • AIX 7.1 トラステッド・ネットワーク接続クライアントには、次のいずれかのコンポーネントが必要です。 • AIX 6.1 (6100-06 適用) 以降 • パッチ管理のために、SUMA 環境に AIX バージョン 7.1 サービス更新管理アシスタント (SUMA) コンソール・システム	• POWER5 • POWER6 • POWER7 • POWER8

PowerSC Standard Edition 1.1.4 のインストール

PowerSC Standard Edition の特定の機能ごとに、ファイルセットを 1 つインストールする必要があります。

PowerSC Standard Edition では以下のファイルセットを使用できます。

- `powerscStd.ice`: PowerSC Standard Edition のセキュリティーおよびコンプライアンスの自動化フィーチャーを必要とする AIX システムにインストールされます。
- `powerscStd.vtpm`: PowerSC Standard Edition のトラステッド・ブート・フィーチャーを必要とする AIX システムにインストールされます。
- `powerscStd.vlog`: PowerSC Standard Edition のトラステッド・ロギング・フィーチャーを必要とする AIX システムにインストールされます。
- `powerscStd.tnc_pm`: AIX バージョン 6.1 (6100-06 テクノロジー・レベル適用) 以降、またはサービス更新管理アシスタント (SUMA) 環境内の AIX バージョン 7.1 以降の SUMA コンソール・システムにパッチ管理のためにインストールされます。
- `powerscStd.svm`: PowerSC Standard Edition のルーティング・フィーチャーから利益を得る可能性がある AIX システムにインストールされます。
- `powerscStd.rtc`: PowerSC Standard Edition のリアルタイム・コンプライアンス・フィーチャーを必要とする AIX システムにインストールされます。

以下のいずれかのインターフェースを使用して、PowerSC Standard Edition をインストールすることができます。

- コマンド・ライン・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 Standard 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/powerscStd.vtpm` 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。

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 Standard 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/powerscStd.vtpm
```

関連概念:

5 ページの『PowerSC Standard Edition 1.1.4 の概念』
この PowerSC Standard Edition の概要では、フィーチャー、コンポーネント、および PowerSC Standard Edition フィーチャーに関連するハードウェア・サポートについて説明します。

125 ページの『トラステッド・ブートのインストール』
トラステッド・ブートをインストールするには、ハードウェアおよびソフトウェアの構成がいくつか必要です。

147 ページの『トラステッド・ネットワーク接続のインストール』
トラステッド・ネットワーク接続 (TNC) のコンポーネントをインストールするには、特定のステップを実行する必要があります。

関連タスク:

133 ページの『トラステッド・ファイアウォールのインストール』
PowerSC トラステッド・ファイアウォールのインストールは、他の PowerSC フィーチャーのインストールと同様です。

142 ページの『トラステッド・ロギングのインストール』
コマンド・ライン・インターフェースまたは SMIT ツールを使用して、PowerSC トラステッド・ロギング・フィーチャーをインストールすることができます。

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 Standard Edition に組み込まれています。

PowerSC Standard Edition インストール・パッケージ 5765-PSE 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 **pscxpert** コマンドを使用してシステム上に実装できる `powerscStd.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。

注: セキュリティー・プロファイルを適用する前に、システムにすべてのアプリケーションをインストールしてください。

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)、Payment Card Industry (PCI) Data Security Standard (DSS)、Sarbanes-Oxley 法令、COBIT コンプライアンス (SOX/COBIT)、および医療保険の積算と責任に関する法律 (Health Insurance Portability and Accountability Act (HIPAA)) に従って 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、2.0、または 3.0 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 Standard Edition の XML プロファイルは、ICEE と同様に **pscxpert** コマンドで使用できます。

PowerSC Standard 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 Standard 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 Security Technical Implementation Guide (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 Standard 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/dodv2` ディレクトリーにあります。

PowerSC Standard Edition は、AIX DoD STIG のバージョン 1 リリース 2 の要件に対応しています。これらの要件およびその準拠を確保する方法の要約が、以下のテーブルに記載されています。

表 3. DoD の一般的な要件

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
AIX00020	2	AIX トラステッド・コンピューティング・ベース・ソフトウェアを実装する必要があります。	**位置** `/etc/security/pscexpert/dodv2/trust` **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
AIX00040	2	**securetcpip** コマンドを使用する必要があります。	**位置** `/etc/security/pscexpert/dodv2/dodsecuretcpip` **準拠アクション** 確実に、システムが指定の要件を満たすようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
AIX00060	2	無許可の setuid ファイル、および許可された setuid ファイルに対する無許可の変更がないか、システムを週 1 回調べる必要があります。	**位置** /etc/security/pscexpert/dodv2/trust **準拠アクション** 指定されたファイルの変更を特定するために週 1 回確認します。
AIX00080	1	SYSTEM 属性が、任意のアカウントで *none* に設定されていてはなりません。	**位置** /etc/security/pscexpert/dodv2/SYSattr **準拠アクション** 確実に、指定された属性が *none* 以外の値に設定されるようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
AIX00200	2	システムは、ダイレクテッド・ブロードキャストがゲートウェイを介して移動することを許可してはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** direct_broadcast ネットワーク・オプションの値を *0* に設定します。
AIX00210	2	システムは、TCP 接続上の Internet Control Message Protocol (ICMP) アタックからの保護を提供する必要があります。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** tcp_icmpsecure ネットワーク・オプションの値を *1* に設定します。
AIX00220	2	システムは、接続リセット、同期 (SYN)、およびデータ注入の各アタックから、TCP スタックを保護する必要があります。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** 確実に、tcp_tcpsecure ネットワーク・オプションの値が *7* に設定されるようにします。
AIX00230	2	システムは、IP フラグメント化アタックからの保護を提供する必要があります。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** ip_nfrag ネットワーク・オプションの値を *200* に設定します。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
AIX00300	1,2,3	システムでは bootp サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** 指定されたサービスを使用不可にします。
AIX00310	2	/etc/ftpaccess.ctl ファイルが存在している必要があります。	**位置** /etc/security/pscexpert/dodv2/dodv2loginherald **準拠アクション** 確実に、そのファイルが存在するようにします。
GEN000020	2	システムは、シングルユーザー・モードで開始するときに認証を要求する必要があります。	**位置** /etc/security/pscexpert/dodv2/rootpasswd_home **準拠アクション** 確実に、ブート可能なパーティションの root アカウントのパスワードが /etc/security/passwd ファイルにあるようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN000100	1	オペレーティング・システムは、サポートされているリリースでなければなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2cat1 **準拠アクション** 指定されたルール・テストの結果を表示します。
GEN000120	2	最新のシステム・セキュリティー・パッチおよび更新がインストールされなければなりません。	**位置** /usr/sbin/instfix -i /etc/security/pscexpert/dodv2/dodv2cat1 **準拠アクション** トラステッド・ネットワーク接続機能を使用してこれを構成します。
GEN000140	2	無許可の setuid ファイル、および許可された setuid ファイルに対する無許可の変更がないか、システムを週 1 回調べる必要があります。	**位置** /etc/security/pscexpert/dodv2/trust **準拠アクション** 指定されたファイルの変更を特定するために週 1 回確認します。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN000220	2	無許可の setuid ファイル、および許可された setuid ファイルに対する無許可の変更がないか、システムを週 1 回調べる必要があります。	**位置** /etc/security/pscexpert/dodv2/trust **準拠アクション** 指定されたファイルの変更を特定するために週 1 回確認します。
GEN000240	2	システム・クロックは、信頼できる米国国防総省 (DoD) の時刻ソースに同期されなければなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2cmntrows **準拠アクション** 確実に、システム・クロックが対応するようにします。
GEN000241	2	システム・クロックは、連続して、または少なくとも毎日同期されなければなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2cmntrows **準拠アクション** 確実に、システム・クロックが対応するようにします。
GEN000242	2	システムは、クロック同期のために少なくとも 2 つの時刻ソースを使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodv2netrules **準拠アクション** 確実に、複数の時刻ソースがクロックの同期に使用されるようにします。
GEN000280	2	以下のタイプのアカウントへの直接ログインを許可してはなりません。 • アプリケーション • デフォルト • 共有 • ユーティリティー	**位置** /etc/security/pscexpert/dodv2/lockacc_rlogin **準拠アクション** 指定されたアカウントへの直接ログインを防止します。
GEN000290	2	システムに不要なアカウントがあってはなりません。	**位置** /etc/security/pscexpert/dodv2/lockacc_rlogin **準拠アクション** 確実に、未使用のアカウントがないようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN000300 (GEN000320、GEN000380、GEN000880 に関連)	2	システム上のすべてのアカウントに、固有のユーザー名またはアカウント名、および固有のユーザー・パスワードまたはアカウント・パスワードが必要です。	**位置** /etc/security/pscexpert/dodv2/grpusrpass_chk **準拠アクション** 確実に、すべてのアカウントが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN000320 (GEN000300、GEN000380、GEN000880 に関連)	2	システム上のすべてのアカウントに、固有のユーザー名またはアカウント名、および固有のユーザー・パスワードまたはアカウント・パスワードが必要です。	**位置** /etc/security/pscexpert/dodv2/grpusrpass_chk **準拠アクション** 確実に、すべてのアカウントが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN000340	2	システム・アカウント用に予約されているユーザー ID (UID) およびグループ ID (GID) は、システム以外のアカウントまたはシステム以外のグループに割り当ててはなりません。	**位置** /etc/security/pscexpert/dodv2/account **準拠アクション** このルールを適用するために、この設定は自動的に使用可能になります。
GEN000360	2	システム・アカウント用に予約されている UID および GID は、システム以外のアカウントまたはシステム以外のグループに割り当ててはなりません。	**位置** /etc/security/pscexpert/dodv2/account **準拠アクション** このルールを適用するために、この設定は自動的に使用可能になります。
GEN000380 (GEN000300、GEN000320、GEN000880 に関連)	2	システム上のすべてのアカウントに、固有のユーザー名またはアカウント名、および固有のユーザー・パスワードまたはアカウント・パスワードが必要です。	**位置** /etc/security/pscexpert/dodv2/grpusrpass_chk **準拠アクション** 確実に、すべてのアカウントが指定の要件を満たすようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN000400	2	コンソール・ログイン・プロンプトの直前に、またはコンソール・ログイン・プロンプトの一部として、米国国防総省 (DoD) のログイン・バナーが表示されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/dodv2loginherald` **準拠アクション** 必要なバナーを表示します
GEN000402	2	グラフィカル・デスクトップ環境ログイン・プロンプトの直前に、またはグラフィカル・デスクトップ環境ログイン・プロンプトの一部として、DoD のログイン・バナーが表示されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/dodv2loginherald` **準拠アクション** このログイン・バナーは、米国国防総省のバナーに設定されます。
GEN000410	2	システム上の File Transfer Protocol over SSL (FTPS) サービスまたはファイル転送プロトコル (FTP) サービスは、DoD のログイン・バナーを使用して構成されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/dodv2loginherald` **準拠アクション** FTP を使用する場合はバナーを表示します。
GEN000440	2	ログイン試行およびログアウト試行の成功と失敗が記録されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/loginout` **準拠アクション** 必要なロギングを使用可能にします。
GEN000452	2	システムは、各ログイン時に前回成功したアカウント・ログインの日時を表示しなければなりません。	**位置** `/etc/security/pscexpert/dodv2/sshDoDconfig` **準拠アクション** 必要な情報を表示します
GEN000460	2	このルールは、3 回連続してログオン試行に失敗した後、アカウントを使用不可にします。	**位置** `/etc/security/pscexpert/dodv2/chusrattrdod` **準拠アクション** ログイン試行回数の制限を指定の値に設定します。
GEN000480	2	このルールは、ログイン遅延時間を 4 秒に設定します。	**位置** `/etc/security/pscexpert/dodv2/chdefstanzadod` **準拠アクション** ログイン遅延時間を必要な値に設定します。
GEN000540	2	このルールは、確実に、システム・グローバル・パスワード構成ファイルが、パスワード要件にしたがって構成されるようにします。	**位置** `/etc/security/pscexpert/dodv2/chusrattrdod` **準拠アクション** 必要なパスワード設定値を設定します。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN000560	1	システム上のすべてのアカウントに、有効なパスワードが必要です。	**位置** /etc/security/pscexpert/dodv2/grpusrpass_chk **準拠アクション** 確実に、アカウントがパスワードを持つようにします。
GEN000580	2	このルールは、確実に、すべてのパスワードに、最小でも 14 文字が含まれるようにします。	**位置** /etc/security/pscexpert/dodv2/chusrattrdod **準拠アクション** パスワードの最小の長さを 14 文字に設定します。
GEN000585	2	システムは、アカウント・パスワード・ハッシュの生成に連邦情報処理標準 (FIPS) 140-2 承認の暗号ハッシュ・アルゴリズムを使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/fipspasswd **準拠アクション** 確実に、パスワード・ハッシュで、承認されたハッシュ・アルゴリズムを使用するようにします。
GEN000590	2	システムは、アカウント・パスワード・ハッシュの生成に FIPS 140-2 承認の暗号ハッシュ・アルゴリズムを使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/fipspasswd **準拠アクション** 確実に、パスワード・ハッシュで、承認されたハッシュ・アルゴリズムを使用するようにします。
GEN000595	2	システムに保管されるパスワード・ハッシュの生成時に、FIPS 140-2 承認の暗号ハッシュ・アルゴリズムを使用してください。	**位置** /etc/security/pscexpert/dodv2/fipspasswd **準拠アクション** 確実に、パスワード・ハッシュで、承認されたハッシュ・アルゴリズムを使用するようにします。
GEN000640	2	このルールには、パスワードに 1 文字以上の非英字が必要です。	**位置** /etc/security/pscexpert/dodv2/chusrattrdod **準拠アクション** パスワードに含める非英字の最小文字数を 1 に設定します。
GEN000680	2	このルールは、確実に、パスワードに含まれる連続した反復文字が 3 文字以下であるようにします。	**位置** /etc/security/pscexpert/dodv2/chusrattrdod **準拠アクション** パスワードに含める反復文字の最大数を 3 に設定します。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN000700	2	このルールは、確実に、システム・グローバル・パスワード構成ファイルが、パスワード要件にしたがって構成されるようにします。	**位置** /etc/security/pscexpert/dodv2/chusrattrdod **準拠アクション** 確実に、パスワード構成ファイルが要件を満たすようにします。
GEN000740	2	非対話式の自動化処理アカウント・パスワードはすべて、ロックされなければなりません (GEN000280)。共有、デフォルト、アプリケーション、ユーティリティーの各アカウントへの直接ログインを許可してはなりません。 (GEN002640) デフォルトのシステム・アカウントは使用不可にするか、削除されなければなりません。	**位置** /etc/security/pscexpert/dodv2/loginout /etc/security/pscexpert/dodv2/lockacc_rlogin **準拠アクション** この設定は、自動的に使用可能になります。
GEN000740	2	非対話式の自動化処理アカウント・パスワードはすべて、少なくとも年 1 回変更するか、またはロックされなければなりません。	**位置** /etc/security/pscexpert/dodv2/lockacc_rlogin **準拠アクション** 確実に、指定されたパスワードが年 1 回変更されるか、ロックされるようにします。
GEN000750	2	このルールでは、新規パスワードに、旧パスワードに含まれていなかった文字が 4 文字以上含まれることが必要です。	**位置** /etc/security/pscexpert/dodv2/chusrattrdod **準拠アクション** 新規パスワードに必要な新規文字の最小数を 4 に設定します。
GEN000760	2	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なければなりません。	**位置** /etc/security/pscexpert/dodv2/disableacctdod **準拠アクション** 35 日間アクティビティーがない場合、アカウントをロックします。
GEN000790	2	システムは、辞書に記載されているワードをパスワードに使用させないようにする必要があります。	**位置** /etc/security/pscexpert/dodv2/chuserstanzadod **準拠アクション** 確実に、設定中のデフォルトのパスワードがぜい弱でないようにします。
GEN000800	2	このルールは、確実に、直前の 5 つのパスワードが再使用されないようにします。	**位置** /etc/security/pscexpert/dodv2/chusrattrdod **準拠アクション** 確実に、新規パスワードが、直前の 5 つのパスワードと同じものにならないようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN000880 (GEN000300、GEN000320、GEN000380 に関連)	2	システム上のすべてのアカウントに、固有のユーザー名またはアカウント名、および固有のユーザー・パスワードまたはアカウント・パスワードが必要です。	**位置** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **準拠アクション** 確実に、すべてのアカウントが指定の要件を満たすようにします。
GEN000900	3	root ユーザーのホーム・ディレクトリーがルート・ディレクトリー (*/*) であってはなりません。	**位置** `/etc/security/pscexpert/dodv2/rootpasswd_home` **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN000940	2	root アカウントの実行可能検索パスは、ベンダーのデフォルトでなければならず、絶対パスのみを含む必要があります。	**位置** `/etc/security/pscexpert/dodv2/fixpathvars` **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN000945	2	root アカウントのライブラリー検索パスは、システム・デフォルトでなければならず、絶対パスのみを含む必要があります。	**位置** `/etc/security/pscexpert/dodv2/fixpathvars` **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN000950	2	root アカウントにおけるプリロード済みライブラリーのリストは空でなければなりません。	**位置** /etc/security/pscexpert/dodv2/fixpathvars **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN000960 (GEN003000、GEN003020、GEN003160、GEN003360、GEN003380 に関連)	2	root アカウントには、その実行可能検索パスに全ユーザー書き込み可能ディレクトリーがあってはなりません。	**位置** /etc/security/pscexpert/dodv2/rmwwpaths **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN000980	2	システムは、システム・コンソールからの場合を除いて、root アカウントに直接ログインするのを防止する必要があります。	**位置** /etc/security/pscexpert/dodv2/chuserstanzadod **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN001000	2	リモート・コンソールを使用不可にするか、無許可アクセスから保護しなければなりません。	**位置** /etc/security/pscexpert/dodv2/remoteconsole **準拠アクション** 確実に、指定のコンソールが使用不可であるようにします。
GEN001020	2	root アカウントを直接ログインに使用してはなりません。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** root アカウントに直接ログインするのを使用不可にします。
GEN001060	2	システムは、root アカウントへのアクセス試行の成功と失敗をログに記録する必要があります。	**位置** /etc/security/pscexpert/dodv2/loginout **準拠アクション** 確実に、システムが指定の要件を満たすようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001100	1	テキスト形式の root パスワードは、ネットワークを介して受け渡してはなりません。	**位置** /etc/security/pscexpert/dodv2/chuserstanzadod **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN001120	2	システムは、SSH プロトコルを使用した root ログインを許可してはなりません。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** SSH の root ログインを使用不可にします。
GEN001440	3	すべての対話式ユーザーは、/etc/passwd ファイルでホーム・ディレクトリーが割り当てられなければなりません。	**位置** /etc/security/pscexpert/dodv2/grpusrpass_chk **準拠アクション** 確実に、すべての対話式ユーザーに指定のディレクトリーがあるようにします。
GEN001475	2	/etc/group ファイルにグループ・パスワード・ハッシュが含まれてはなりません。	**位置** /etc/security/pscexpert/dodv2/passwdhash **準拠アクション** 確実に、指定されたファイルにグループ・パスワード・ハッシュがないようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001600	2	Run Control スクリプトの実行可能検索パスには、絶対パスのみが含まれる必要があります。	**位置** /etc/security/pscexpert/dodv2/fixpathvars **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001605	2	Run Control スクリプトのライブラリー検索パスには、絶対パスのみが含まれる必要があります。	**位置** /etc/security/pscexpert/dodv2/fixpathvars **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001610	2	Run Control スクリプトのプリロード済みライブラリーのリストには、絶対パスのみが含まれる必要があります。	**位置** /etc/security/pscexpert/dodv2/fixpathvars **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001840	2	すべてのグローバル初期化ファイルの実行可能検索パスには、絶対パスのみが含まれる必要があります。	**位置** /etc/security/pscexpert/dodv2/fixpathvars **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001845	2	すべてのグローバル初期化ファイルのライブラリー検索パスには、絶対パスのみが含まれる必要があります。	**位置** /etc/security/pscexpert/dodv2/fixpathvars **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001850	2	すべてのグローバル初期化ファイルのプリロード済みライブラリーのリストには、絶対パスのみが含まれる必要があります。	**位置** /etc/security/pscexpert/dodv2/fixpathvars **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001900	2	すべてのローカル初期化ファイルの実行可能検索パスには、絶対パスのみが含まれる必要があります。	**位置** /etc/security/pscexpert/dodv2/fixpathvars **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001901	2	すべてのローカル初期化ファイルのライブラリー検索パスには、絶対パスのみが含まれる必要があります。	**位置** /etc/security/pscexpert/dodv2/fixpathvars **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001902	2	すべてのローカル初期化ファイルのプリロード済みライブラリーのリストには、絶対パスのみが含まれる必要があります。	**位置** /etc/security/pscexpert/dodv2/fixpathvars **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001940	2	ユーザー初期化ファイルは、全ユーザーが書き込み可能なプログラムを実行してはなりません。	**位置** /etc/security/pscexpert/dodv2/rmwwpaths **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN001980	2	.rhosts、.shosts、hosts.equiv、shosts.equiv、/etc/passwd、/etc/shadow、または /etc/group の各ファイルには、NIS+ ネットグループのエントリーを定義しない場合、正符号 (+) を含んではなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2netrules **準拠アクション** 確実に、指定されたファイルが、指定された要件を満たすようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN002000	2	システムに .netrc ファイルがあってはなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2netrules **準拠アクション** 確実に、システム上に指定のファイルがないようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN002020	2	すべての .rhosts、.shosts、または hosts.equiv ファイルには、信頼できるホストとユーザーのペアのみを含む必要があります。	**位置** /etc/security/pscexpert/dodv2/dodv2netrules **準拠アクション** 確実に、指定されたファイルがこの要件に準拠するようにします。
GEN002040	1	このルールは、.rhosts、.shosts、および hosts.equiv ファイルまたは shosts.equiv ファイルを使用不可にします。	**位置** /etc/security/pscexpert/dodv2/mvhostsfilesdod **準拠アクション** 指定されたファイルを使用不可にします。
GEN002120	1,2	このルールは、ユーザー・シェルを検査して構成します。	**位置** /etc/security/pscexpert/dodv2/usershells **準拠アクション** 必要なシェルを作成します。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN002140	1,2	ログインを防止するために指定されるシェルを除いて、/etc/passwd リストで参照されるシェルはすべて、/etc/shells ファイルにリストされなければなりません。	**位置** /etc/security/pscexpert/dodv2/usershells **準拠アクション** 確実に、これらのシェルが正しいファイルにリストされるようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN002280	2	デバイス・ファイルおよびディレクトリーは、システム・アカウントを使用するユーザーによってのみ、またはシステムがベンダーによって構成される際に書き込み可能でなければなりません。	**位置** /etc/security/pscexpert/dodv2/wwdevfiles **準拠アクション** システム上で非公開ディレクトリーにある全ユーザー書き込み可能デバイス・ファイル、ディレクトリー、およびその他のすべてのファイルを表示します。
GEN002300	2	バックアップに使用されるデバイス・ファイルは、root ユーザーまたはバックアップ・ユーザーによってのみ読み取り可能または書き込み可能、もしくはその両方が可能でなければなりません。	**位置** /etc/security/pscexpert/dodv2/wwdevfiles **準拠アクション** システム上で非公開ディレクトリーにある全ユーザー書き込み可能デバイス・ファイル、ディレクトリー、およびその他のすべてのファイルを表示します。
GEN002400	2	無許可の setuid ファイル、および許可された setuid ファイルに対する無許可の変更がないか、システムを週 1 回調べる必要があります。	**位置** /etc/security/pscexpert/dodv2/trust **準拠アクション** 指定されたファイルの変更を特定するために週 1 回確認します。 **注:** 無許可のアクティビティーがなかったことを確認するために、/var/security/pscexpert ディレクトリーで作成される最新の 2 回の週次ログを比較します。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN002420	2	承認された setuid ファイルを含まない取り外し可能メディア、リモート・ファイルシステム、および任意のファイルシステムは、*nosuid* オプションを使用してマウントする必要があります。	**位置** /etc/security/pscexpert/dodv2/fsmntoptions **準拠アクション** 確実に、リモート側でマウントされたファイルシステムに、指定のオプションがあるようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN002430	2	承認されたデバイス・ファイルを含まない取り外し可能メディア、リモート・ファイルシステム、および任意のファイルシステムは、*nodev* オプションを使用してマウントする必要があります。	**位置** /etc/security/pscexpert/dodv2/fsmntoptions **準拠アクション** 確実に、リモート側でマウントされたファイルシステムに、指定のオプションがあるようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN002480	2	公開ディレクトリーのみが全ユーザー書き込み可能ディレクトリーでなければなりません。また、全ユーザー書き込み可能ファイルは公開ディレクトリーのみに置かれなければなりません。	**位置** /etc/security/pscexpert/dodv2/wwdevfiles /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 全ユーザー書き込み可能ファイルが公開ディレクトリーにない場合は報告します。
GEN002640	2	デフォルトのシステム・アカウントは使用不可にするか、削除されなければなりません。	**位置** /etc/security/pscexpert/dodv2/lockacc_rlogin /etc/security/pscexpert/dodv2/loginout **準拠アクション** デフォルト・システム・アカウントを使用不可にします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN002660	2	監査が使用可能でなければなりません。	**位置** /etc/security/pscexpert/dodv2/dodaudit **準拠アクション** 監査を使用可能にする dodaudit コマンドを使用可能にします。
GEN002720	2	ファイルおよびプログラムへのアクセス試行の失敗を監査するように、監査システムを構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodaudit **準拠アクション** 指定された監査を自動的に使用可能にします。
GEN002740	2	ファイルの削除を監査するように、監査システムを構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodaudit **準拠アクション** 指定された監査を自動的に使用可能にします。
GEN002750	3	アカウントの作成を監査するように、監査システムを構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodaudit **準拠アクション** 指定された監査を自動的に使用可能にします。
GEN002751	3	アカウントの変更を監査するように、監査システムを構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodaudit **準拠アクション** 指定された監査を自動的に使用可能にします。
GEN002752	3	使用不可になったアカウントを監査するように、監査システムを構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodaudit **準拠アクション** 指定された監査を自動的に使用可能にします。
GEN002753	3	アカウントの終了を監査するように、監査システムを構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodaudit **準拠アクション** 指定された監査を自動的に使用可能にします。
GEN002760	2	管理、特権、セキュリティーの各アクションをすべて監査するように、監査システムを構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodaudit **準拠アクション** 指定された監査を自動的に使用可能にします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN002800	2	ログイン、ログアウト、およびセッション開始を監査するように、監査システムを構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodaudit **準拠アクション** 指定された監査を自動的に使用可能にします。
GEN002820	2	任意アクセス制御の許可変更をすべて監査するように、監査システムを構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodaudit **準拠アクション** 指定された監査を自動的に使用可能にします。
GEN002825	2	動的カーネル・モジュールのロードとアンロードを監査するように、監査システムを構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodaudit **準拠アクション** 指定された監査を自動的に使用可能にします。
GEN002860	2	監査ログを毎日置き換える必要があります。	**位置** /etc/security/pscexpert/dodv2/rotateauditdod **準拠アクション** 確実に、監査ログが置き換えられるようにします。
GEN002960	2	cron ユーティリティーへのアクセスは、cron.allow ファイルまたは cron.deny ファイル、もしくはその両方を使用して制御されなければなりません。	**位置** /etc/security/pscexpert/dodv2/limitsysacc **準拠アクション** 確実に、準拠の制限が使用可能であるようにします。
GEN003000 (GEN000960、GEN003020、GEN003160、GEN003360、GEN003380 に関連)	2	Cron は、グループ書き込み可能プログラムまたは全ユーザー書き込み可能プログラムを実行してはなりません。	**位置** /etc/security/pscexpert/dodv2/rmwwpaths **準拠アクション** 確実に、準拠の制限が使用可能であるようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003020 (GEN000960、GEN003000、GEN003160、GEN003360、GEN003380 に関連)	2	Cron は、全ユーザー書き込み可能ディレクトリー内のプログラム、または全ユーザー書き込み可能ディレクトリーに従属するプログラムを実行してはなりません。	**位置** /etc/security/pscexpert/dodv2/rmwwpaths **準拠アクション** 全ユーザー書き込み可能許可を cron プログラム・ディレクトリーから除去します。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN003060	2	デフォルトのシステム・アカウント (root を除く) が、cron.allow ファイルにリストされてはならないか、または cron.allow ファイルが存在しない場合は、cron.deny ファイルに含まれなければなりません。	**位置** cron.allow または cron.deny **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN003160 (GEN000960、GEN003000、GEN003020、GEN003360、GEN003380 に関連)	2	Cron ロギングが実行中でなければなりません。	**位置** /etc/security/pscexpert/dodv2/rmwwpaths **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN003280	2	at ユーティリティーへのアクセスは、at.allow ファイルおよび at.deny ファイルを使用して制御されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chcronfilesdod **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN003300	2	at.deny ファイルが存在する場合、このファイルは空であってはなりません。	**位置** /etc/security/pscexpert/dodv2/chcronfilesdod **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN003320	2	root でないデフォルトのシステム・アカウントが、at.allow ファイルにリストされてはならないか、または at.allow ファイルが存在しない場合は、at.deny ファイルに含まれなければなりません。	**位置** /etc/security/pscexpert/dodv2/chcronfilesdod **準拠アクション** 確実に、システムが指定の要件を満たすようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003360 (GEN000960、GEN003000、GEN003020、GEN003160、GEN003380 に関連)	2	at デーモンは、グループ書き込み可能プログラムまたは全ユーザー書き込み可能プログラムを実行してはなりません。	**位置** /etc/security/pscexpert/dodv2/rmwwpaths **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN003380 (GEN000960、GEN003000、GEN003020、GEN003160、GEN003360 に関連)	2	at デーモンは、全ユーザー書き込み可能ディレクトリー内のプログラム、または全ユーザー書き込み可能ディレクトリーに従属するプログラムを実行してはなりません。	**位置** /etc/security/pscexpert/dodv2/rmwwpaths **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN003510	2	カーネルのコア・ダンプが必要な場合を除いて、これを使用不可にする必要があります。	**位置** /etc/security/pscexpert/dodv2/coredumpdev **準拠アクション** カーネルのコア・ダンプを使用不可にします。
GEN003540	2	システムは、実行不能プログラム・スタックを使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/sedconfigdod **準拠アクション** 実行不能プログラム・スタックの使用を実施します。
GEN003600	2	システムは、送信元で経路指定された IPv4 パケットを転送してはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** ipsrcforward ネットワーク・オプションの値を *0* に設定します。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003601	2	TCP バックログ・キュー・サイズが適切に設定されなければなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** clean_partial_conns ネットワーク・オプションの値を *1* に設定します。
GEN003603	2	システムは、ブロードキャスト・アドレスに送信される Internet Control Message Protocol バージョン 4 (ICMPv4) エコーに応答してはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** bcastping ネットワーク・オプションの値を *0* に設定します。
GEN003604	2	システムは、ブロードキャスト・アドレスに送信される ICMP タイム・スタンプ要求に応答してはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** bcastping ネットワーク・オプションの値を *0* に設定します。
GEN003605	2	システムは、TCP 応答に逆方向の発信元経路指定を適用してはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** nonlocsrcroute ネットワーク・オプションの値を *0* に設定します。
GEN003606	2	システムは、ローカル・アプリケーションが送信元で経路指定されたパケットを生成しないようにする必要があります。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** ipsrcroutesend ネットワーク・オプションの値を *0* に設定します。
GEN003607	2	システムは、送信元で経路指定された IPv4 パケットを受け入れてはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** 送信元で経路指定された IPv4 パケットを受け入れる機能を使用不可にします。
GEN003609	2	システムは、IPv4 ICMP リダイレクト・メッセージを無視する必要があります。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** ipignoreredirects ネットワーク・オプションの値を *1* に設定します。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003610	2	システムは、IPv4 ICMP リダイレクト・メッセージを送信してはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** ipsendredirects ネットワーク・オプションの値を *0* に設定します。
GEN003612	2	システムは、TCP SYN フラッディングが発生するときに TCP syncookies を使用するように構成されなければなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** clean_partial_conns ネットワーク・オプションの値を *1* に設定します。
GEN003640	2	ルート・ファイルシステムは、ジャーナリング、またはファイルシステムの一貫性を確保する別の方法を使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/chkjournal **準拠アクション** ルート・ファイルシステムでジャーナリングを使用可能にします。
GEN003660	2	システムは、認証情報データをログに記録する必要があります。	**位置** /etc/security/pscexpert/dodv2/chsyslogdod **準拠アクション** auth および info データのロギングを使用可能にします。
GEN003700	2	inetd および xinetd は、ネットワーク・サービスで使用されていない場合、使用不可にするか、除去する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodv2services **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN003810	2	この portmap または rpcbind サービスは、必要でない限り、実行中であってはなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2services **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN003815	2	この portmap または rpcbind サービスは、使用されない限り、インストールしてはなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2services **準拠アクション** 確実に、システムが指定の要件を満たすようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003820-3860	1,2,3	rsh、rexexec、および telnet デーモン、ならびに rlogind サービスは実行中であってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN003865	2	ネットワーク分析ツールをインストールしてはなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2services **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN003900	2	hosts.lpd ファイル (または同等なもの) に、加算記号 (+) が含まれてはなりません。	**位置** /etc/security/pscexpert/dodv2/printers **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN004220	1	ローカル・サービス管理に必要な場合を除いて、管理アカウントで Web ブラウザーを実行してはなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2cat1 **準拠アクション** 指定されたルール・テストの結果を表示します。
GEN004460	2	このルールは、auth データと info データをログに記録します。	**位置** /etc/security/pscexpert/dodv2/chsyslogdod **準拠アクション** auth および info データのロギングを使用可能にします。
GEN004540	2	このルールは、sendmail help コマンドを使用不可にします。	**位置** /etc/security/pscexpert/dodv2/sendmailhelp /etc/security/pscexpert/dodv2/dodv2cmntrows **準拠アクション** 指定されたコマンドを使用不可にします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN004580	2	システムは、.forward ファイルを使用してはなりません。	**位置** /etc/security/pscexpert/dodv2/forward **準拠アクション** 指定されたファイルを使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN004600	1	SMTP サービスは最新バージョンでなければなりません。	**位置** /etc/security/pscexpert/dodv2/SMTP_ver **準拠アクション** 確実に、指定されたサービスの最新バージョンが実行されるようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN004620	2	sendmail サーバーでは、デバッグ機能が使用不可になっている必要があります。	**位置** /etc/security/pscexpert/dodv2/SMTP_ver **準拠アクション** sendmail デバッグ機能を使用不可にします。
GEN004640	1	SMTP サービスには、アクティブな uudecode 別名があってはなりません。	**位置** /etc/security/pscexpert/dodv2/SMTPuucode **準拠アクション** uudecode 別名を使用不可にします。
GEN004710	2	メール・リレーを制限する必要があります。	**位置** /etc/security/pscexpert/dodv2/sendmaildod **準拠アクション** メール・リレーを制限します。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN004800	1,2,3	暗号化されていない FTP をシステムで使用してはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN004820	2	匿名 FTP が許可されていない限り、匿名 FTP がシステムでアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/anonuser **準拠アクション** システムで匿名 FTP を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN004840	2	システムが匿名 FTP サーバーである場合、非武装地帯 (DMZ) ネットワークに分離する必要があります。	**位置** /etc/security/pscexpert/dodv2/anonuser **準拠アクション** 確実に、システム上の匿名 FTP が DMZ ネットワークにあるようにします。
GEN004880	2	ftpusers ファイルが存在している必要があります。	**位置** /etc/security/pscexpert/dodv2/chdodftpusers **準拠アクション** 確実に、指定されたファイルがシステムにあるようにします。
GEN004900	2	ftpusers ファイルには、FTP プロトコルの使用を許可されていないアカウント名が含まれていなければなりません。	**位置** /etc/security/pscexpert/dodv2/chdodftpusers **準拠アクション** 確実に、ファイルに必要なアカウント名が含まれているようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN005000	1	匿名 FTP アカウントに機能シェルがあってはなりません。	**位置** /etc/security/pscexpert/dodv2/usershells **準拠アクション** 匿名 FTP アカウントからシェルを除去します。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN005080	1	TFTP デーモンは、ホスト・ファイルシステム上の単一ディレクトリーのみにアクセスできるようにするセキュア・モードで動作しなければなりません。	**位置** /etc/security/pscexpert/dodv2/tftpdod **準拠アクション** 確実に、デーモンが指定の要件を満たすようにします。
GEN005120	2	TFTP デーモンは、専用の TFTP ユーザー・アカウント、非ログイン・シェル (/bin/false など)、TFTP ユーザーが所有するホーム・ディレクトリーを含めて、ベンダーの仕様に合わせて構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/tftpdod **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005140	1,2,3	アクティブな TFTP デーモンはすべて、システム認定パッケージで許可され、承認されなければなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** 確実に、デーモンが許可されるようにします。
GEN005160	1,2	どの X Window システム・ホストも .Xauthority ファイルを作成する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodv2disableX **準拠アクション** 確実に、ホストが指定のファイルを作成するにします。
GEN005200	1,2	どの X Window システム表示も公開でエクスポートすることはできません。	**位置** /etc/security/pscexpert/dodv2/dodv2disableX **準拠アクション** 指定されたプログラムの配布を使用不可にします。
GEN005220	1,2	X Window システム・サーバーへのアクセスを制限するには、.Xauthority ファイルまたは X*.hosts (または同等の) ファイルを使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/dodv2disableX **準拠アクション** 確実に、指定されたファイルが、サーバーへのアクセスの制限に使用できるようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN005240	1,2	.Xauthority ユーティリティーは、許可されたホストのみへのアクセスを可能にする必要があります。	**位置** /etc/security/pscexpert/dodv2/dodv2disableX **準拠アクション** 確実に、アクセスが、許可されたホストに制限されるようにします。
GEN005260	2	このルールは、X Window システム接続と XServer ログイン・マネージャーを使用不可にします。	**位置** /etc/security/pscexpert/dodv2/dodv2cmntrows **準拠アクション** 必要な接続とログイン・マネージャーを使用不可にします。
GEN005280	1,2,3	システムでは UUCP サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN005300	2	SNMP コミュニティーをデフォルト設定から変更する必要があります。	**位置** /etc/security/pscexpert/dodv2/chsnmp **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005305	2	SNMP サービスは、SNMPv3 以降のバージョンのみを使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/chsnmp **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005306	2	SNMP サービスでは、FIPS 140-2 の使用を要求する必要があります。	**位置** /etc/security/pscexpert/dodv2/chsnmp **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005440	2	システムは、リモート syslog サーバー (ログ・ホスト) を使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/EnableTrustedLogging **準拠アクション** 確実に、システムがリモート syslog サーバーを使用するようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN005450	2	システムは、リモート syslog サーバー (ログ・ホスト) を使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/EnableTrustedLogging **準拠アクション** 確実に、システムがリモート syslog サーバーを使用するようにします。
GEN005460	2	システムは、リモート syslog サーバー (ログ・ホスト) を使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/EnableTrustedLogging **準拠アクション** 確実に、システムがリモート syslog サーバーを使用するようにします。
GEN005480	2	システムは、リモート syslog サーバー (ログ・ホスト) を使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/EnableTrustedLogging **準拠アクション** 確実に、システムがリモート syslog サーバーを使用するようにします。
GEN005500	2	SSH デーモンは、セキュア・シェル・バージョン 2 (SSHv2) プロトコルのみを使用するように構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005501	2	SSH クライアントは、SSHv2 プロトコルのみを使用するように構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005504	2	SSH デーモンは、管理以外の用途が許可されている場合を除いて、管理ネットワーク・アドレスでのみ listen することが必要です。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005505	2	SSH デーモンは、連邦情報処理標準 (FIPS) 140-2 規格に準拠する暗号のみを使用するように構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005506	2	SSH デーモンは、FIPS 140-2 規格に準拠する暗号のみを使用するように構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN005507	2	SSH デーモンは、FIPS 140-2 規格に準拠する暗号ハッシュ・アルゴリズムを持つメッセージ認証コード (MAC) のみを使用するように構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005510	2	SSH クライアントは、FIPS 140-2 規格に準拠する暗号を使用する MAC のみを使用するように構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005511	2	SSH クライアントは、FIPS 140-2 規格に準拠する暗号を使用する MAC のみを使用するように構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005512	2	SSH デーモンは、FIPS 140-2 規格に準拠する暗号ハッシュ・アルゴリズムを使用する MAC のみを使用するように構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005521	2	SSH デーモンは、ログインを特定のユーザーまたはグループ、もしくはその両方に制限する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005536	2	SSH デーモンは、ホーム・ディレクトリー構成ファイルの厳密モードの検査を実行する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005537	2	SSH デーモンは、特権分離を使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005538	2	SSH デーモンは、Rivest-Shamir-Adleman (RSA) 暗号方式を使用して rhosts が認証されることを許可してはなりません。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN005539	2	SSH デーモンは、圧縮を許可してはなりません。または正常な認証後にのみ圧縮を許可する必要があります。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005550	2	SSH デーモンは、DoD のログオン・バナーを使用して構成されなければなりません。	**位置** /etc/security/pscexpert/dodv2/sshDoDconfig **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005560	2	IPv4 用に構成されているデフォルト・ゲートウェイがあるかどうかを確認してください。	**位置** /etc/security/pscexpert/dodv2/chkgtway **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。 **注:** システムが IPv6 プロトコルを実行している場合は、/etc/security/pscexpert/ipv6.conf ファイルの *ipv6_enabled* 設定が、yes の値に設定されていることを確実にしてください。システムが IPv6 を使用していない場合は、*ipv6_enabled* 値が no に設定されていることを確実にしてください。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN005570	2	IPv6 用に構成されているデフォルト・ゲートウェイがあるかどうかを確認してください。	**位置** /etc/security/pscexpert/dodv2/chkgtway **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。 **注:** システムが IPv6 プロトコルを実行している場合は、/etc/security/pscexpert/ipv6.conf ファイルの *ipv6_enabled* 設定が、yes の値に設定されていることを確実にしてください。システムが IPv6 を使用していない場合は、*ipv6_enabled* 値が no に設定されていることを確実にしてください。
GEN005590	2	システムがルーターである場合を除いて、システムはルーティング・プロトコル・デーモンを実行中であってはなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2cmntrows **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005590	2	システムがルーターである場合を除いて、システムはルーティング・プロトコル・デーモンを実行中であってはなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2cmntrows **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN005600	2	システムがルーターである場合を除いて、IPv4 用の IP 転送を使用可能にしてはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** ipforwarding ネットワーク・オプションの値を *0* に設定します。
GEN005610	2	システムが IPv6 ルーターである場合を除いて、システムは、IPv6 用の IP 転送を使用可能にしてはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** ip6forwarding ネットワーク・オプションの値を *1* に設定します。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN005820	2	NFS 匿名 UID および GID は、許可がない値に構成されなければなりません。	**位置** /etc/security/pscexpert/dodv2/nfsoptions **準拠アクション** 確実に、指定の ID が許可を持たないようにします。
GEN005840	2	NFS サーバーは、ファイルシステム・アクセスをローカル・ホストに制限するように構成されなければなりません。	**位置** /etc/security/pscexpert/dodv2/nfsoptions **準拠アクション** アクセスをローカル・ホストに制限するように NFS サーバーを構成します。
GEN005880	2	NFS サーバーは、リモート root アクセスを許可してはなりません。	**位置** /etc/security/pscexpert/dodv2/nfsoptions **準拠アクション** NFS サーバーでリモート root アクセスを使用不可にします。
GEN005900	2	*nosuid* オプションは、すべての NFS クライアント・マウントで使用可能でなければなりません。	**位置** /etc/security/pscexpert/dodv2/nosuid **準拠アクション** すべての NFS クライアント・マウントで *nosuid* オプションを使用可能にします。
GEN006060	2	必要な場合を除いて、システムは Samba を実行してはなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2services **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN006380	1	システムは NIS または NIS+ に UDP を使用してはなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2cat1 **準拠アクション** 指定されたルール・テストの結果を表示します。
GEN006400	2	Network Information System (NIS) プロトコルを使用してはなりません。	**位置** /etc/security/pscexpert/dodv2/nisplus **準拠アクション** 指定されたプロトコルを使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN006420	2	NIS マップは、推測しにくいドメイン・ネームを使用して保護されなければなりません。	**位置** /etc/security/pscexpert/dodv2/nisplus **準拠アクション** 確実に、ドメイン・ネームが判別しにくい名前であるようにします。
GEN006460	2	いずれかの NIS+ サーバーが、セキュリティー・レベル 2 で動作しなければなりません。	**位置** /etc/security/pscexpert/dodv2/nisplus **準拠アクション** 確実に、サーバーが、指定された最小セキュリティー・レベルであるようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN006480	2	無許可の setuid ファイル、および許可された setuid ファイルに対する無許可の変更がないか、システムを週 1 回調べる必要があります。	**位置** /etc/security/pscexpert/dodv2/trust **準拠アクション** 指定されたファイルの変更を特定するために週 1 回確認します。
GEN006560	2	無許可の setuid ファイル、および許可された setuid ファイルに対する無許可の変更がないか、システムを週 1 回調べる必要があります。	**位置** /etc/security/pscexpert/dodv2/trust **準拠アクション** 指定されたファイルの変更を特定するために週 1 回確認します。
GEN006580	2	システムは、アクセス制御プログラムを使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/checktcpd **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN006600	2	システムのアクセス制御プログラムは、各システム・アクセス試行をログに記録する必要があります。	**位置** /etc/security/pscexpert/dodv2/chsyslogdod **準拠アクション** 確実に、アクセス試行がログに記録されるようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN006620	2	システムのアクセス制御プログラムは、特定のホストへのシステム・アクセスを認可または拒否するように構成する必要があります。	**位置** /etc/security/pscexpert/dodv2/chetchostsdod **準拠アクション** hosts.deny ファイルと hosts.allow ファイルを必要な設定値に構成します。
GEN007020	2	Stream Control Transmission Protocol (SCTP) を使用不可にする必要があります。	**位置** /etc/security/pscexpert/dodv2/dodv2netrules **準拠アクション** 指定されたプロトコルを使用不可にします。
GEN007700	2	必要な場合を除いて、IPv6 プロトコル・ハンドラーをネットワーク・スタックにバインドしてはなりません。	**位置** /etc/security/pscexpert/dodv2/rminet6 **準拠アクション** IPv6 プロトコル・ハンドラーが /etc/ipv6.conf ファイルで指定されている場合を除いて、ネットワーク・スタックからこのプロトコル・ハンドラーを使用不可にします。 **注:** システムが IPv6 プロトコルを実行している場合は、/etc/security/pscexpert/ipv6.conf ファイルの *ipv6_enabled* 設定が、yes の値に設定されていることを確実にしてください。システムが IPv6 を使用していない場合は、*ipv6_enabled* 値が no に設定されていることを確実にしてください。
GEN007780	2	システムでは 6to4 トンネルが使用可能であってはなりません。	**位置** /etc/security/pscexpert/dodv2/rmiface **準拠アクション** 指定されたトンネルを使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN007820	2	システムで IP トンネルが構成されていてはなりません。	**位置** /etc/security/pscexpert/dodv2/rmtunnel **準拠アクション** IP トンネルを使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN007840	2	使用されていない場合、DHCP クライアントを使用不可にする必要があります。	**位置** /etc/security/pscexpert/dodv2/dodv2services **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN007850	2	DHCP クライアントは、動的 DNS 更新を送信してはなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2services **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN007860	2	システムは、IPv6 ICMP リダイレクト・メッセージを無視する必要があります。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** ipignoreredirects ネットワーク・オプションの値を *1* に設定します。
GEN007880	2	システムは、IPv6 ICMP リダイレクトを送信してはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** ipsendredirects ネットワーク・オプションの値を *0* に設定します。
GEN007900	2	システムが IPv6 を使用する場合、システムは、IPv6 ネットワーク・トラフィックに適切な逆パス・フィルターを使用する必要があります。	**位置** /etc/security/pscexpert/dodv2/chuserstanzadod **準拠アクション** 確実に、システムが指定の要件を満たすようにします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN007920	2	システムは、送信元で経路指定された IPv6 パケットを転送してはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** ip6srcrouteforward ネットワーク・オプションの値を *0* に設定します。
GEN007940: GEN003607	2	システムは、送信元で経路指定された IPv4 または IPv6 パケットを受け入れてはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** ipsrcrouterecv ネットワーク・オプションの値を *0* に設定します。
GEN007950	2	システムは、ブロードキャスト・アドレスに送信される ICMPv6 エコー要求に応答してはなりません。	**位置** /etc/security/pscexpert/dodv2/ntwkoptsdod **準拠アクション** bcastping ネットワーク・オプションの値を *0* に設定します。
GEN008000	2	システムが認証またはアカウント情報に Lightweight Directory Access Protocol (LDAP) を使用している場合、LDAP サーバーに対する認証に使用される証明書は、DoD PKI または DoD によって承認される方式から提供されなければなりません。	**位置** /etc/security/pscexpert/dodv2/ldap_config **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN008020	2	システムが認証またはアカウント情報に LDAP を使用している場合、LDAP トランスポート層セキュリティー (TLS) 接続では、サーバーが有効なトラスト・パスを使用して証明書を提供することを要求する必要があります。	**位置** /etc/security/pscexpert/dodv2/ldap_config **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN008050	2	システムが認証またはアカウント情報に LDAP を使用している場合、/etc/ldap.conf ファイル (または同等のもの) にパスワードが入っていてはなりません。	**位置** /etc/security/pscexpert/dodv2/ldap_config **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN008380	2	無許可の setuid ファイル、および許可された setuid ファイルに対する無許可の変更がないか、システムを週 1 回調べる必要があります。	**位置** /etc/security/pscexpert/dodv2/trust **準拠アクション** 指定されたファイルの変更を特定するために週 1 回確認します。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN008520	2	システムは、ポート・スキャンからホストをガードするローカル・ファイアウォールを使用する必要があります。このファイアウォールは、ポート・スキャンからホストをガードするためにぜい弱ポートを 5 分間回避する必要があります。	**位置** `/etc/security/pscexpert/dodv2/ipsecshunports` **準拠アクション** 確実に、システムが指定の要件を満たすようにします。
GEN008540	2	システムのローカル・ファイアウォールは、*deny-all*、*allow-by-exception* ポリシーを実装する必要があります。	**位置** `/etc/security/pscexpert/dodv2/ipsecshunhosthls` **準拠アクション** 確実に、システムが指定の要件を満たすようにします。 **注:** `/etc/security/aixpert/bin/filter.txt` ファイルに追加のフィルター・ルールを入力することができます。これらのルールは、プロファイルを適用するときに、`ipsecshunhosthls.sh` スクリプトによって組み込まれます。エントリーは次の形式でなければなりません。 *port_number*:*ip_address*:*action* ここで、*action* に使用可能な値は、`Allow` または `Deny` です。
GEN008600	1	システムは、システム・ブート構成からのみ開始するように構成されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/dodv2cat1` **準拠アクション** 確実に、システムの開始には、システム・ブート構成のみを使用するようにします。
GEN008640	1	システムは、取り外し可能メディアをブート・ローダーとして使用してはなりません。	**位置** `/etc/security/pscexpert/dodv2/dodv2cat1` **準拠アクション** 確実に、システムが取り外し可能ドライブからブートしないようにします。
GEN009140	1,2,3	システムでは `chargen` サービスがアクティブであってはなりません。	**位置** `/etc/security/pscexpert/dodv2/inetdservices` **準拠アクション** `/etc/inetd.conf` ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN009160	1,2,3	システムでは Calendar Management Service Daemon (CMSD) サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009180	1,2,3	システムでは tool-talk database server (ttdbserver) サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009190	1,2,3	システムでは comsat サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009200-9330	1,2,3	システムでは、他のサービスやデーモンをアクティブにすることはできません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009210	2	システムでは discard サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009220	2	システムでは dtspc サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN009230	2	システムでは echo サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009240	2	システムでは Internet Message Access Protocol (IMAP) サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009250	2	システムでは PostOffice Protocol (POP3) サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009260	2	システムでは talk または ntalk サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009270	2	システムでは、InetD プロセスで netstat サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009280	2	システムでは PCNFS サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。

表 3. DoD の一般的な要件 (続き)

米国国防総省の STIG のチェックポイント ID	STIG ルールのカテゴリー	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN009290	2	システムでは systat サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009300	2	inetd デーモンでは、inetd time サービスがシステムでアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009310	2	システムでは rusersd サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009320	2	システムでは sprayd サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009330	2	システムでは rstatd サービスがアクティブであってはなりません。	**位置** /etc/security/pscexpert/dodv2/inetdservices **準拠アクション** /etc/inetd.conf ファイルでエントリーをコメント化することによって、必要なデーモンとサービスを使用不可にします。
GEN009340	2	X サーバー・ログイン・マネージャーが X11 セッション管理に必要な場合を除いて、このログイン・マネージャーが実行中であってはなりません。	**位置** /etc/security/pscexpert/dodv2/dodv2cmntrows **準拠アクション** このルールは、X Window システム接続と XServer ログイン・マネージャーを使用不可にします。

表 4. DoD の所有権の要件

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
AIX00085	/etc/netsvc.conf ファイルは root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
AIX00090	/etc/netsvc.conf ファイルは、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。
AIX00320	/etc/ftpaccess.ctl ファイルは root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
AIX00330	/etc/ftpaccess.ctl ファイルは、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。
GEN000250	時刻同期構成ファイル (/etc/ntp.conf など) は、root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN000251	時刻同期構成ファイル (/etc/ntp.conf など) は、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。
GEN001160	すべてのファイルとディレクトリーには、有効な所有者が必要です。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、すべてのファイルとディレクトリーに有効な所有者があるようにします。
GEN001170	すべてのファイルとディレクトリーには、有効なグループ所有者が必要です。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、すべてのファイルとディレクトリーに有効な所有者があるようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001220	すべてのシステム・ファイル、プログラム、およびディレクトリーは、システム・アカウントによって所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、システム・ファイル、プログラム、およびディレクトリーが、システム・アカウントによって所有されるようにします。
GEN001240	システム・ファイル、プログラム、およびディレクトリーは、システム・グループによってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** すべてのシステム・ファイル、プログラム、およびディレクトリーは、システム・グループによってグループ所有されます。
GEN001320	ネットワーク情報システム (NIS)/NIS+/yp ファイルは、root、sys、または bin によって所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルが root、sys、または bin によって所有されるようにします。
GEN001340	NIS/NIS+/yp ファイルは、sys、bin、other、または system によってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルが sys、bin、other、または system によって所有されるようにします。
GEN001362	`/etc/resolv.conf` ファイルは root が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN001363	`/etc/resolv.conf` ファイルは、bin、sys、または system によってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。
GEN001366	`/etc/hosts` ファイルは root が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001367	/etc/hosts ファイルは、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。
GEN001371	/etc/nsswitch.conf ファイルは root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN001372	/etc/nsswitch.conf ファイルは、root、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが root、bin、sys、または system によってグループ所有されるようにします。
GEN001378	/etc/passwd ファイルは root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN001379	/etc/passwd ファイルは、bin、security、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、security、sys、または system によってグループ所有されるようにします。
GEN001391	/etc/group ファイルは root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN001392	/etc/group ファイルは、bin、security、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、security、sys、または system によってグループ所有されるようにします。
GEN001400	/etc/security/passwd ファイルは root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001410	/etc/security/passwd ファイルは、bin、security、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、security、sys、または system によってグループ所有されるようにします。
GEN001500	対話式ユーザーのすべてのホーム・ディレクトリーは、それぞれのユーザーによって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、対話式ユーザーのすべてのホーム・ディレクトリーが、それぞれのユーザーによって所有されなければならないようにします。
GEN001520	対話式ユーザーのすべてのホーム・ディレクトリーは、ホーム・ディレクトリー所有者の 1 次グループによってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、対話式ユーザーのすべてのホーム・ディレクトリーが、ホーム・ディレクトリー所有者の 1 次グループによってグループ所有されるようにします。
GEN001540	対話式ユーザーのホーム・ディレクトリー内に含まれているすべてのファイルおよびディレクトリーは、ホーム・ディレクトリーの所有者によって所有される必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、対話式ユーザーのホーム・ディレクトリー内に含まれているすべてのファイルおよびディレクトリーが、ホーム・ディレクトリーの所有者によって所有されるようにします。
GEN001550	ユーザーのホーム・ディレクトリー内に含まれているすべてのファイルおよびディレクトリーは、ホーム・ディレクトリーの所有者がメンバーであるグループによってグループ所有される必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、ユーザーのホーム・ディレクトリー内に含まれているすべてのファイルおよびディレクトリーが、ホーム・ディレクトリーの所有者がメンバーであるグループによってグループ所有される必要があるようにします。
GEN001660	すべてのシステム始動ファイルは、root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN001680	すべてのシステム始動ファイルは、sys、bin、other、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが sys、bin、other、または system によってグループ所有されるようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001740	すべてのグローバル初期化ファイルは、root が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN001760	すべてのグローバル初期化ファイルは、sys、bin、system、または security によってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルが sys、bin、system、または security によってグループ所有されるようにします。
GEN001820	すべてのスケルトン・ファイルおよびディレクトリー (通常は `/etc/skel` 内にある) は、root または bin によって所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルおよびディレクトリーが root または bin によって所有されるようにします。
GEN001830	すべてのスケルトン・ファイル (通常は `/etc/skel` 内にある) は、security によってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルを security がグループ所有するようにします。
GEN001860	すべてのローカル初期化ファイルは、ユーザーまたは root が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルをユーザーまたは root が所有するようにします。
GEN001870	ローカル初期化ファイルは、ユーザーの 1 次グループまたは root によってグループ所有される必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、ローカル初期化ファイルが、ユーザーの 1 次グループまたは root によってグループ所有される必要があるようにします。
GEN002060	`.rhosts`、`.shosts`、`.netrc`、または `hosts.equiv` ファイルはすべて、root または所有者によってのみアクセス可能でなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、root または所有者のみが指定のファイルにアクセスできるようにします。
GEN002100	`.rhosts` ファイルは、Pluggable Authentication Module (PAM) によってサポートされてはなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定のファイルが、PAM を使用して使用可能にならないようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN002200	すべてのシェル・ファイルは、root または bin が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルを root または bin が所有するようにします。
GEN002210	すべてのシェル・ファイルは、root、bin、sys、または system によってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルが root、bin、sys、または system によってグループ所有されるようにします。
GEN002340	オーディオ・デバイスは、root が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、すべてのオーディオ・デバイスを root が所有するようにします。
GEN002360	オーディオ・デバイスは、root、sys、bin、または system によってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、すべてのオーディオ・デバイスが、root、sys、bin、または system によってグループ所有されるようにします。
GEN002520	すべての公開ディレクトリーは、root またはアプリケーション・アカウントによって所有される必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、すべての公開ディレクトリーが、root またはアプリケーション・アカウントによって所有されるようにします。
GEN002540	すべての公開ディレクトリーは、システムまたはアプリケーション・グループによってグループ所有されている必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、すべての公開ディレクトリーが、システムまたはアプリケーション・グループによってグループ所有されるようにします。
GEN002680	システム監査ログは、root が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN002690	システム監査ログは、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが、bin、sys、または system によってグループ所有されるようにします。
GEN003020	Cron は、全ユーザー書き込み可能ディレクトリー内のプログラム、または全ユーザー書き込み可能ディレクトリーに従属するプログラムを実行してはなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** cron が、全ユーザー書き込み可能ディレクトリー内のプログラム、または全ユーザー書き込み可能ディレクトリーに従属するプログラムを実行しないようにします。
GEN003040	Crontabs は、root または crontab 作成者によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、Crontabs が、root または crontab 作成者によって所有されるようにします。
GEN003050	Crontab ファイルは、system、cron、または crontab 作成者の 1 次グループによってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、Crontab ファイルが、system、cron、または crontab 作成者の 1 次グループによってグループ所有されるようにします。
GEN003110	Cron ディレクトリーおよび crontab ディレクトリーには、拡張アクセス制御リストがあってはなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたディレクトリーに拡張アクセス制御リストがないようにします。
GEN003120	Cron ディレクトリーと crontab ディレクトリーは root または bin によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、Cron ディレクトリーと crontab ディレクトリーが root または bin によって所有されるようにします。
GEN003140	Cron ディレクトリーと crontab ディレクトリーは system、sys、bin、または cron によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたディレクトリーが system、sys、bin、または cron によってグループ所有されるようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003160	Cron ロギングが実装されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、Cron ロギングが実装されるようにします。
GEN003240	cron.allow ファイルは、root、bin、または sys によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが root、bin、または sys によって所有されるようにします。
GEN003250	cron.allow ファイルは、system、bin、sys、または cron によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが system、bin、sys、または cron によってグループ所有されるようにします。
GEN003260	cron.deny ファイルは、root、bin、または sys によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが root、bin、または sys によって所有されるようにします。
GEN003270	cron.deny ファイルは、system、bin、sys、または cron によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが system、bin、sys、または cron によってグループ所有されるようにします。
GEN003420	at ディレクトリーは、root、bin、sys、daemon、または cron によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたディレクトリーが root、sys、daemon、または cron によって所有されるようにします。
GEN003430	at ディレクトリーは、system、bin、sys、または cron によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたディレクトリーが system、bin、sys、または cron によってグループ所有されるようにします。
GEN003460	at.allow ファイルは、root、bin、または sys によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが root、bin、または sys によって所有されるようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003470	at.allow ファイルは、system、bin、sys、または cron によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが system、bin、sys、または cron によってグループ所有されるようにします。
GEN003480	at.deny ファイルは、root、bin、または sys によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが root、bin、または sys によって所有されるようにします。
GEN003490	at.deny ファイルは、system、bin、sys、または cron によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが system、bin、sys、または cron によってグループ所有されるようにします。
GEN003720	inetd.conf ファイル、xinetd.conf ファイル、および xinetd.d ディレクトリーは、root または bin によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルおよびディレクトリーが root または bin によって所有されるようにします。
GEN003730	inetd.conf ファイル、xinetd.conf ファイル、および xinetd.d ディレクトリーは、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルおよびディレクトリーが、bin、sys、または system によってグループ所有されるようにします。
GEN003760	services ファイルは root または bin によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが root または bin によって所有されるようにします。
GEN003770	services ファイルは、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003920	`hosts.lpd` (または同等の) ファイルは、root、bin、sys、または lp によって所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルが root、bin、sys、または lp によって所有されるようにします。
GEN003930	`hosts.lpd` (または同等の) ファイルは、bin、sys、または system によってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。
GEN003960	**traceroute** コマンドの所有者は root でなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、このコマンドの所有者が root であるようにします。
GEN003980	**traceroute** コマンドは、sys、bin、または system によってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、このコマンドが sys、bin、または system によってグループ所有されるようにします。
GEN004360	`alias` ファイルは root が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN004370	`aliases` ファイルは、sys、bin、または system によってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルが sys、bin、または system によってグループ所有されるようにします。
GEN004400	メール `aliases` ファイルを使用して実行されるファイルは、root によって所有される必要があり、root によってのみ所有されて書き込み可能であるディレクトリー内に置かれなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、メール `aliases` ファイルを使用して実行されるファイルが、root によって所有され、root によってのみ所有されて書き込み可能であるディレクトリー内に置かれるようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN004410	メール `aliases` ファイルを使用して実行されるファイルは、root、bin、sys、または other によってグループ所有されなければなりません。また、root、bin、sys、または other によってグループ所有されるディレクトリー内に置かれなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、メール `aliases` ファイルを使用して実行されるファイルが、root、bin、sys、または other によってグループ所有され、root、bin、sys、または other によってグループ所有されるディレクトリー内にあるようにします。
GEN004480	SMTP サービス・ログ・ファイルは root が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN004920	`ftpusers` ファイルは root が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN004930	`ftpusers` ファイルは、bin、sys、または system によってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。
GEN005360	`snmpd.conf` ファイルは root が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN005365	`snmpd.conf` ファイルは、bin、sys、または system によってグループ所有されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。
GEN005400	`/etc/syslog.conf` ファイルは root が所有している必要があります。	**位置** `/etc/security/pscexpert/dodv2/chowndodfiles` **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN005420	/etc/syslog.conf ファイルは、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。
GEN005610	システムが IPv6 ルーターである場合を除いて、システムで、IPv6 の IP 転送が使用可能であってはなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、システムが IPv6 ルーターとして使用されている場合を除いて、IPv6 の IP 転送が使用可能にならないようにします。
GEN005740	NFS エクスポート構成ファイルは root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN005750	NFS エクスポート構成ファイルは、root、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが root、bin、sys、または system によってグループ所有されるようにします。
GEN005800	NFS エクスポートされたシステム・ファイルとシステム・ディレクトリーはすべて、root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN005810	NFS エクスポートされたシステム・ファイルとシステム・ディレクトリーはすべて、root、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルとディレクトリーが root、bin、sys、または system によってグループ所有されるようにします。
GEN006100	/usr/lib/smb.conf ファイルは root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN006120	/usr/lib/smb.conf ファイルは、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。
GEN006160	/var/private/smbpasswd ファイルは root が所有している必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN006180	/var/private/smbpasswd ファイルは、sys または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが sys または system によってグループ所有されるようにします。
GEN006340	/etc/news ディレクトリー内のファイルは、root または news によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたディレクトリーが root または news によって所有されるようにします。
GEN006360	/etc/news 内のファイルは system または news によってグループ所有されている必要があります。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが system または news によってグループ所有されるようにします。
GEN008080	システムが認証またはアカウント情報に LDAP を使用している場合、/etc/ldap.conf (または同等の) ファイルは root によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。
GEN008100	システムが認証またはアカウント情報に LDAP を使用している場合、/etc/ldap.conf (または同等の) ファイルは security、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。
GEN008140	システムが認証またはアカウント情報に LDAP を使用している場合、TLS 認証局ファイルまたはディレクトリーは root によって所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルを root が所有するようにします。

表 4. DoD の所有権の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN008160	システムが認証またはアカウント情報に LDAP を使用している場合、TLS 認証局ファイルまたはディレクトリーは root、bin、sys、または system によってグループ所有されなければなりません。	**位置** /etc/security/pscexpert/dodv2/chowndodfiles **準拠アクション** 確実に、指定されたファイルが bin、sys、または system によってグループ所有されるようにします。

表 5. ファイル許可に関する DoD 標準

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
AIX00100	/etc/netsvc.conf ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
AIX00340	/etc/ftpaccess.ctl ファイルには、モード 0640、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN000252	時刻同期構成ファイル (/etc/ntp.conf など) には、モード 0640、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN000920	root アカウントのホーム・ディレクトリー (/ 以外) には、モード 0700 が必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ディレクトリーが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001140	システム・ファイルとディレクトリーのアクセス許可は等しくなければなりません。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、アクセス許可が一致するようにします。

表 5. ファイル許可に関する DoD 標準 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001180	すべてのネットワーク・サービス・デーモン・ファイルには、モード 0755、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001200	すべてのシステム・コマンド・ファイルには、モード 0755、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001260	システム・ログ・ファイルには、モード 0640、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001280	マニュアル・ページ・ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001300	ライブラリー・ファイルには、モード 0755、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001360	NIS/NIS+/yp ファイルには、モード 0755、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001364	`/etc/resolv.conf` ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。

表 5. ファイル許可に関する DoD 標準 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001368	/etc/hosts ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001373	/etc/nsswitch.conf ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001380	/etc/passwd ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001393	/etc/group ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001420	/etc/security/passwd ファイルには、モード 0400 が必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001480	ユーザーのすべてのホーム・ディレクトリーには、0750 またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001560	ユーザーのホーム・ディレクトリー内に含まれているすべてのファイルおよびディレクトリーには、モード 0750、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。

表 5. ファイル許可に関する DoD 標準 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001580	すべての Run Control スクリプトには、モード 0755、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001640	Run Control スクリプトは、全ユーザー書き込み可能プログラムまたはスクリプトを実行してはなりません。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** cron などのプログラムで、全ユーザー書き込み可能プログラムまたはスクリプトがないか確認します。
GEN001720	すべてのグローバル初期化ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001800	すべてのスケルトン・ファイル (例えば、/etc/skel 内のファイル) には、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN001880	すべてのローカル初期化ファイルには、モード 0740、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN002220	すべてのシェル・ファイルには、モード 0755、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN002320	オーディオ・デバイスには、モード 0660、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、オーディオ・デバイスが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。

表 5. ファイル許可に関する DoD 標準 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN002560	システムおよびユーザーのデフォルト **umask** は 077 でなければなりません。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、指定された設定値が *077* であるようにします。
GEN002700	システム監査ログには、モード 0640、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN002717	システム監査ツール実行可能ファイルには、モード 0750、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN002980	`cron.allow` ファイルには、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN003080	Crontab ファイルには、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN003090	`Crontab` ファイルは、拡張アクセス制御リスト (ACL) があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、指定されたファイルに拡張 ACL がないようにします。
GEN003100	Cron および crontab ディレクトリーには、モード 0755、またはそれより許容度の低いモードが必要です。	**位置** `/etc/security/pscexpert/dodv2/fpmdodfiles` **準拠アクション** 確実に、指定されたディレクトリーが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。

表 5. ファイル許可に関する DoD 標準 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003180	cronlog ファイルには、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN003200	cron.deny ファイルには、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN003252	at.deny ファイルには、モード 0640、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN003340	at.allow ファイルには、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN003400	at ディレクトリーには、モード 0755、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ディレクトリーが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN003440	At ジョブでは、**umask** パラメーターを 077 より制限の少ない値に設定してはなりません。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、このパラメーターが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN003740	inetd.conf ファイルおよび xinetd.conf ファイルには、モード 0440、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。

表 5. ファイル許可に関する DoD 標準 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003780	services ファイルには、モード 0444、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN003940	hosts.lpd ファイル (または同等のもの) には、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN004000	traceroute ファイルには、モード 0700、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN004380	alias ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN004420	メール aliases ファイルを使用して実行されるファイルには、モード 0755、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN004500	SMTP サービス・ログ・ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN004940	ftpusers ファイルには、モード 0640、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。

表 5. ファイル許可に関する DoD 標準 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN005040	すべての FTP ユーザーには、デフォルトの **umask** 設定値 077 が必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、設定値が正しいものであるようにします。
GEN005100	TFTP デーモンには、モード 0755、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、このデーモンが指定のモード、またはそれより許容度の低いモードに設定されるようにします。
GEN005180	すべての .Xauthority ファイルには、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN005320	snmpd.conf ファイルには、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN005340	管理情報ベース (MIB) ファイルには、モード 0640、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN005390	/etc/syslog.conf ファイルには、モード 0640、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN005522	SSH 公開ホスト鍵ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。

表 5. ファイル許可に関する DoD 標準 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN005523	SSH 秘密ホスト鍵ファイルには、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN006140	/usr/lib/smb.conf ファイルには、モード 0644、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN006200	/var/private/smbpasswd ファイルには、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN006260	/etc/news/hosts.nntp ファイル (または同等のもの) には、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN006280	/etc/news/hosts.nntp.nolimit ファイル (または同等のもの) には、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN006300	/etc/news/nnrp.access ファイル (または同等のもの) には、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN006320	/etc/news/passwd.nntp ファイル (または同等のもの) には、モード 0600、またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。

表 5. ファイル許可に関する DoD 標準 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN008060	システムが認証またはアカウント情報に LDAP を使用している場合、/etc/ldap.conf (または同等の) ファイルには、0644 またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、ファイルが指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。
GEN008180	システムが認証またはアカウント情報に LDAP を使用している場合、TLS 認証局ファイルまたはディレクトリー、もしくはその両方には、0644 (ディレクトリーの場合は 0755) またはそれより許容度の低いモードが必要です。	**位置** /etc/security/pscexpert/dodv2/fpmdodfiles **準拠アクション** 確実に、指定されたファイルまたはディレクトリー、もしくはその両方が指定の許可モード、またはそれより許容度の低いモードに設定されるようにします。

表 6. DoD アクセス制御リスト (ACL) の要件

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
AIX00110	/etc/netsvc.conf ファイルには、拡張アクセス制御リスト (ACL) があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
AIX00350	/etc/ftpaccess.ctl ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN000253	時刻同期構成ファイル (/etc/ntp.conf など) には、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN000930	root アカウントのホーム・ディレクトリーには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001190	すべてのネットワーク・サービス・デーモン・ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001210	すべてのシステム・コマンド・ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001270	許可ソフトウェアのサポートに必要な場合を除いて、システム・ログ・ファイルには拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001310	すべてのライブラリー・ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001361	NIS/NIS+/yp コマンド・ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001365	`/etc/resolv.conf` ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001369	/etc/hosts ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001374	/etc/nsswitch.conf ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001390	/etc/passwd ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001394	/etc/group ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001430	/etc/security/passwd ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001570	ユーザーのホーム・ディレクトリー内に含まれているすべてのファイルおよびディレクトリーには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001590	すべての Run Control スクリプトには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001730	すべてのグローバル初期化ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN001810	スケルトン・ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN001890	ローカル初期化ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN002230	すべてのシェル・ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN002330	オーディオ・デバイスには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN002710	すべてのシステム監査ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN002990	`cron.allow` ファイルおよび `cron.deny` ファイルの拡張 ACL は使用不可に設定されなければなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN003090	Crontab ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN003110	Cron ディレクトリーおよび crontab ディレクトリーには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003190	cron ログ・ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN003210	`cron.deny` ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN003245	`at.allow` ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN003255	`at.deny` ファイルには、拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN003410	at ディレクトリーには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN003745	inetd.conf および xinetd.conf ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN003790	サービス・ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN003950	hosts.lpd ファイル (または同等のもの) には、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN004010	traceroute ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN004390	alias ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN004430	メール aliases ファイルを使用して実行されるファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN004510	SMTP サービス・ログ・ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN004950	ftpusers ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN005190	.Xauthority ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN005350	管理情報ベース (MIB) ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN005375	snmpd.conf ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN005395	/etc/syslog.conf ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN006150	/usr/lib/smb.conf ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN006210	/var/private/smbpasswd ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN006270	/etc/news/hosts.nntp ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN006290	/etc/news/hosts.nntp.nolimit ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN006310	/etc/news/nnrp.access ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN006330	/etc/news/passwd.nntp ファイルには、拡張 ACL があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 指定された拡張 ACL を使用不可にします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。
GEN008120	システムが認証またはアカウント情報に LDAP を使用している場合、/etc/ldap.conf (または同等の) ファイルには、拡張アクセス制御リスト (ACL) があってはなりません。	**位置** /etc/security/pscexpert/dodv2/acldodfiles **準拠アクション** 確実に、指定されたファイルに拡張 ACL がないようにします。 **注:** DoDv2_to_AIXDefault.xml ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

表 6. DoD アクセス制御リスト (ACL) の要件 (続き)

米国国防総省の STIG のチェックポイント ID	説明	アクションが定義されているスクリプトの場所、および準拠を可能にするアクションの結果
GEN008200	システムが認証またはアカウント情報に LDAP を使用している場合、LDAP TLS 認証局ファイルまたはディレクトリー (該当する場合) には拡張 ACL があってはなりません。	**位置** `/etc/security/pscexpert/dodv2/acldodfiles` **準拠アクション** 確実に、指定されたディレクトリーまたはファイルに拡張 ACL がないようにします。 **注:** `DoDv2_to_AIXDefault.xml` ファイルを使用してポリシーが AIX のデフォルト・ポリシーにリセットされるときに、この設定が自動的に変更されることはありません。この設定を手動で変更する必要があります。

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。
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。

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。
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 (`pscxpert -c` コマンドなど) を実行していると終了するため、pscexpert 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。

- 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。
- パスワードの長さは 7 文字以上を必要とする。
- 数字と英字の両方が入ったパスワードを使用する。
- 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。
- 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。
- 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。
- 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。
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。
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 Standard Edition を使用すると、PCI DSS バージョン 2.0 および PCI DSS バージョン 3.0 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 Standard 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。

PCI プロファイルがデータベース環境に適用される場合、ソフトウェア・スタックによって使用される複数の TCP ポートと UDP ポートが制限によって使用不可になります。アプリケーションとワークロードを実行するために、これらのポートを使用可能にし、トラステッド実行機能を使用不可にする必要があります。ポートの制限を除去し、トラステッド実行機能を使用不可にするには、以下のコマンドを実行してください。

```
trustchk -p TE=OFF
tcptr -delete 9091 65535
tcptr -delete 9090 9090
tcptr -delete 112 9089
tcptr -add 9091 65535 1024 1
```

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 Standard 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 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
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。	**minage** パラメーターの値を 0 に設定することによって、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。	/etc/security/pscexpert/bin/chusrattr
PCI バージョン 2 8.5.9 **PCI バージョン 3** 8.2.4	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。	**maxage** パラメーターの値を 13 に設定することによって、パスワードが有効な最大週数を 13 週に設定します。	/etc/security/pscexpert/bin/chusrattr
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。	**maxexpired** パラメーターの値を 8 に設定することによって、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。	/etc/security/pscexpert/bin/chusrattr

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 8.5.10 **PCI バージョン 3** 8.2.3	パスワードの長さは 7 文字以上を必要とする。	**minlen** パラメーターの値を 7 に設定することによって、パスワードの最小長を 7 文字に設定します。	/etc/security/pscexpert/bin/chusrattr
PCI バージョン 2 8.5.11 **PCI バージョン 3** 8.2.3	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。この設定では、**minalpha** パラメーターの値を 1 に設定することによって、パスワードに英字が確実に含まれるようにします。	/etc/security/pscexpert/bin/chusrattr
PCI バージョン 2 8.5.11 **PCI バージョン 3** 8.2.3	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。この設定では、**minother** パラメーターの値を 1 に設定することによって、パスワードに英字以外の文字が確実に含まれるようにします。	/etc/security/pscexpert/bin/chusrattr
PCI バージョン 2 2.1 **PCI バージョン 3** 8.2.2	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。	**maxrepeats** パラメーターの値を 8 に設定することによって、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。	/etc/security/pscexpert/bin/chusrattr
PCI バージョン 2 8.5.12 **PCI バージョン 3** 8.2.5	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。	**histexpire** パラメーターの値を 52 に設定することによって、パスワードの再利用が可能になるまでの週数を 52 に設定します。	/etc/security/pscexpert/bin/chusrattr
PCI バージョン 2 8.5.12 **PCI バージョン 3** 8.2.5	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。	**histsize** パラメーターの値を 4 に設定することによって、ユーザーが再使用できないそれ以前の (直近の) パスワードの数を 4 に設定します。	/etc/security/pscexpert/bin/chusrattr
PCI バージョン 2 8.5.13 **PCI バージョン 3** 10.2.4	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。	**loginentries** パラメーターの値を 6 に設定することによって、アカウントを使用不可にする連続ログイン試行失敗の回数を、非 root アカウントごとに 6 回に設定します。	/etc/security/pscexpert/bin/chusrattr
PCI バージョン 2 8.5.13 **PCI バージョン 3** 10.2.4	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。	**logindisable** パラメーターの値を 6 に設定することによって、ポートを使用不可にする連続ログイン試行失敗の回数を 6 回に設定します。	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 8.5.14 **PCI バージョン 3** 10.2.4	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。	**loginreenable** パラメーターの値を 30 に設定することによって、*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。	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
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。	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
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。	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
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。	/etc/security/pscexpert/bin/pciaudit
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/comntrows
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/comntrows
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/rctcpip
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/rctcpip

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/rctcpip
PCI バージョン 2 2.1 **PCI バージョン 3** 2.1.1	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。	/etc/security/pscexpert/bin/rctcpip
PCI バージョン 2 2.1 **PCI バージョン 3** 2.1.1	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することによって、このデーモンを使用不可にします。	/etc/security/pscexpert/bin/rctcpip
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することによって、このデーモンを使用不可にします。	/etc/security/pscexpert/bin/rctcpip
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することによって、このデーモンを使用不可にします。	/etc/security/pscexpert/bin/rctcpip
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/rctcpip
PCI バージョン 2 2.1 **PCI バージョン 3** 2.2.2	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。	/etc/security/pscexpert/bin/rctcpip
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/rctcpip

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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 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、それら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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
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)。	/etc/inetd.conf ファイル内の対応するエントリーをコメント化することによって、netstat コマンドを使用不可にします。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 2.2.3	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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 2.2.3	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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 2.2.3	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。また、AIX Security Expert ユーティリティーは、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のコメント化も行います。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 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。	/etc/security/pscexpert/bin/cominetdconf

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 2.2.3 **PCI バージョン 3** 2.2.4	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) コマンドを自動的に使用可能にする /etc/inetd.conf ファイル内の対応するエントリーをコメント化することによって、このコマンドを除去します。	/etc/security/pscexpert/bin/rmsuidfrmrcmds
PCI バージョン 2 2.2.3 **PCI バージョン 3** 2.2.4	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。	/etc/security/pscexpert/bin/filepermgr
PCI バージョン 2 2.2.3 **PCI バージョン 3** 2.2.4	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。	PCI セキュリティー要件に準拠する制限付きの設定を使用して、ネットワーク・ファイルシステム・プロトコルを変更します。これらの制限付きの設定には、リモート root アクセスおよび匿名 UID と GID アクセスの使用不可化があります。	/etc/security/pscexpert/bin/nfsconfig
PCI バージョン 2 2.2.2 **PCI バージョン 3** 2.2.3	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。	/etc/security/pscexpert/bin/disrmtdmns
PCI バージョン 2 2.2.2 **PCI バージョン 3** 2.2.3	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。	/etc/security/pscexpert/bin/rmrhostsnetrc
PCI バージョン 2 2.2.2 **PCI バージョン 3** 2.2.3	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。	/etc/security/pscexpert/bin/rmetchostsequiv

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 1.3.6 **PCI バージョン 3** 2.2.3	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。	/etc/security/pscexpert/bin/ntwkopts
PCI バージョン 2 2.2.2 **PCI バージョン 3** 2.2.3	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。	/etc/security/pscexpert/bin/ntwkopts
1.2	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構成します。	/etc/security/pscexpert/bin/ipsecshunhosthls **注:** /etc/security/aixpert/bin/filter.txt ファイルに追加のフィルター・ルールを入力することができます。これらのルールは、プロファイルを適用するときに、ipsecshunhosthls.sh スクリプトによって組み込まれます。エントリーは次の形式でなければなりません。 *port_number*:*ip_address*:*action* ここで、*action* に使用可能な値は、Allow または Deny です。
1.2	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構成します。こうすることで、ポート・スキャンできないようにします。	/etc/security/pscexpert/bin/ipsecshunports **注:** /etc/security/aixpert/bin/filter.txt ファイルに追加のフィルター・ルールを入力することができます。これらのルールは、プロファイルを適用するときに、ipsecshunhosthls.sh スクリプトによって組み込まれます。エントリーは次の形式でなければなりません。 *port_number*:*ip_address*:*action* ここで、*action* に使用可能な値は、Allow または Deny です。
1.2	オブジェクト作成権限を制限すること。	**umask** パラメーターの値を 22 に設定することによって、デフォルトのオブジェクト作成許可数を 22 に設定します。	/etc/security/pscexpert/bin/chusrattr
1.2	システム・アクセスを制限すること。	ルート ID が cron.allow ファイルにリストされる唯一のルート ID になるようにし、さらに、cron.deny ファイルをシステムから削除します。	/etc/security/pscexpert/bin/limitsysacc

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
6.5.8	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	/etc/security/pscexpert/bin/rmdotfrmpathroot
6.5.8	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	/etc/security/pscexpert/bin/rmdotfrmpathnroot
2.2.3	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。	/etc/security/pscexpert/bin/chetcftpusers
2.1	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。	/etc/security/pscexpert/bin/execmds
6.5.2	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。	/etc/security/pscexpert/bin/sedconfig
8.2	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。	/etc/security/pscexpert/bin/chuserstanza
PCI バージョン 2 8.5.15 **PCI バージョン 3** 8.1.8	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。	/etc/security/pscexpert/bin/autologoff
1.3.5	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。	/etc/security/pscexpert/bin/tcptr_pscexpert
1.3.5	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。	/etc/security/pscexpert/bin/cfgsecmig
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。	/etc/security/pscexpert/bin/ipsecpermithostorport

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
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。	/etc/security/pscexpert/bin/manageITsecurity
PCI バージョン 2 セクション 7 **PCI バージョン 3** セクション 7	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。	/etc/security/pscexpert/bin/EnableRbac
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 2.3	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より多くのセキュリティー・フィーチャーを実装すること。	セキュア・シェル (SSH)、SSH ファイル転送プロトコル (S-FTP)、Secure Sockets Layer (SSL)、Internet Protocol Security Virtual Private Network (IPsec VPN) などのセキュア・テクノロジーを使用して、NetBIOS、ファイル共有、Telnet、FTP などの非セキュアなサービスを保護します。また、SSHv2 プロトコルのみを使用するように SSH デーモンを構成します。	/etc/security/pscexpert/bin/sshPCIconfig
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 2.3	SSH クライアントは、SSHv2 プロトコルのみを使用するように構成する必要があります。	SSHv2 プロトコルを使用するように SSH クライアントを構成します。	/etc/security/pscexpert/bin/sshPCIconfig
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 2.3	SSH デーモンは、管理以外の用途が許可されている場合を除いて、管理ネットワーク・アドレスのみを listen する必要があります。	SSH デーモンが listen のみを目的としてセットアップされるようにします。	/etc/security/pscexpert/bin/sshPCIconfig

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 2.3	SSH デーモンは FIPS 140-2 承認済み暗号のみを使用するように構成する必要があります。	SSH デーモンが FIPS 140-2 暗号のみを使用するようにします。	/etc/security/pscexpert/bin/sshPCIconfig
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 2.3	SSH デーモンは、FIPS 140-2 承認済み暗号ハッシュ・アルゴリズムを採用するメッセージ認証コード (MAC) のみを使用するように構成する必要があります。	MAC で上記の承認済みアルゴリズムが実行されるようにします。	/etc/security/pscexpert/bin/sshPCIconfig
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 2.3	SSH デーモンは、ログイン機能を特定のユーザーまたはグループに制限する必要があります。	システムへのログインを特定のユーザーとグループに制限します。	/etc/security/pscexpert/bin/sshPCIconfig
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 2.3	システムは、ログイン時に前回成功したアカウント・ログインの日時を表示する必要があります。	前回成功したログインの情報を維持しておき、次回ログインが成功した後にその情報を表示します。	/etc/security/pscexpert/bin/sshPCIconfig

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 2.3	SSH デーモンは、ホーム・ディレクトリー構成ファイルの厳密モードの検査を実行する必要があります。	ホーム・ディレクトリー構成ファイルが正しいモードに設定されていることを確認します。	/etc/security/pscexpert/bin/sshPCIconfig
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 2.3	SSH デーモンは、特権分離を使用する必要があります。	SSH デーモンが、その特権の分離分を、適正な量だけ保有していることを確認します。	/etc/security/pscexpert/bin/sshPCIconfig
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 2.3	SSH デーモンでは、rhosts に対する RSA 認証が許可されてはなりません。	SSH デーモンを使用する場合に、rhosts に対する RSA 認証を使用不可にします。	/etc/security/pscexpert/bin/sshPCIconfig
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 2.3	ログイン・セッションの最大数をユーザー当たり 2 に制限すること。	ログイン・セッションの最大数をユーザー当たり 2 に設定します。	/etc/security/pscexpert/bin/sshPCIconfig
PCI バージョン 2 1.1.5 2.2.2 **PCI バージョン 3** 10.4	構成の標準およびプロセスを調べ、PCI DSS 要件 6.1 および 6.2 に従って時刻同期テクノロジーが実装され、最新に保たれていることを確認します。	ntp デーモンを使用可能にします。	/etc/security/pscexpert/bin/rctcpip

表 7. PCI DSS コンプライアンスのバージョン 2.0 およびバージョン 3.0 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	値を変更するスクリプトの場所
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 8.1.5	使用されていないユーザー・アカウントを使用不可にします。	35 日間アクティビティーがなかったユーザー・アカウントを使用不可にします。	`/etc/security/pscexpert/bin/disableacctpci`
PCI バージョン 2 バージョン 2 のプロファイルには含まれておらず、バージョン 3 に追加されました。 **PCI バージョン 3** 8.2	ログイン・セッションの最大数をユーザー当たり 2 に制限すること。	**maxulogs** パラメーターの値を 2 に設定することによって、ユーザーのアクティブ・セッションの最大数を 2 に設定します。	`/etc/security/pscexpert/bin/chusrattr`

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 Standard 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、以下のバージョンの AIX オペレーティング・システムで稼働します。

- AIX 6.1
- AIX 7.1
- AIX 7.2

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

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 8. 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。	確実に、すべてのパスワードに、最小でも 14 文字が含まれるようにします。	**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 8. 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。	確実に、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ようにします。	**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 8. 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 8. 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 8. 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 9. 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**、および **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**、および **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/pscexpert/bin/RbacEnablement**.

北米電力信頼度協議会 (North American Electric Reliability Corporation) への準拠

北米電力信頼度協議会 (North American Electric Reliability Corporation (NERC)) は、電力システム業界の標準を策定する非営利企業です。 PowerSC Standard Edition には事前に構成された NERC プロファイルが含まれています。このプロファイルは、重要な電力システムの保護に使用できるセキュリティー標準を提供します。

NERC プロファイルは重要インフラ保護 (Critical Infrastructure Protection (CIP)) 標準に従っています。

NERC プロファイルは `/etc/security/aixpert/custom/NERC.xml` に入っています。NERC プロファイルに適用されている CIP 要件は、`/etc/security/aixpert/custom` ディレクトリーにある NERC_to_AIXDefault.xml プロファイルを適用してデフォルトの状態にリセットできます。このプロセスは、NERC プロファイルの取り消し操作と同じではありません。

次の表に、AIX オペレーティング・システムに適用される CIP 標準に関する情報と、PowerSC Standard Edition による CIP 標準の扱いに関する情報を示します。

表 10. PowerSC Standard Edition での CIP 標準

CIP 標準	AIX Security Expert の実装	値を変更するスクリプトの場所
CIP-003-3 R5.1	バイナリー・ファイルから set-user identification (SUID) 属性と set-group identification (SGID) 属性を除去することにより、問題を防ぐようにシステム・セキュリティー・パラメーターを構成します。	• `/etc/security/pscexpert/bin/filepermgr` • `/etc/security/pscexpert/bin/rmsuidfrmrcmds`
CIP-003-3 R5.1.1	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。	`/etc/security/pscexpert/bin/EnableRbac`
CIP-005-3a R2.1-R2.4	セキュリティー・アクセス用のセキュア・シェル (SSH) を使用可能にします。	`/etc/security/pscexpert/bin/sshstart`
CIP-005-3a R2.5	以下の不要かつ非セキュアなサービスを使用不可にします。 • **lpd** デーモン • 共通デスクトップ環境 (CDE)	`/etc/security/pscexpert/bin/comntrows`
CIP-005-3a R2.5	以下の不要かつ非セキュアなサービスを使用不可にします。 • **timed** デーモン • **NTP** デーモン • **rwhod** デーモン • **DPID2** デーモン • DHCP エージェント	`/etc/security/pscexpert/bin/rctcpip`

表 10. PowerSC Standard Edition での CIP 標準 (続き)

CIP 標準	AIX Security Expert の実装	値を変更するスクリプトの場所
CIP-005-3a R2.5	以下の不要かつ非セキュアなサービスを使用不可にします。 • **comsat** デーモン • **dtspcd** デーモン • **fingerd** デーモン • **ftpd** デーモン • **rshd** デーモン • **rlogind** デーモン • **rexecd** デーモン • **systat** デーモン • **tfptd** デーモン • **talkd** デーモン • **rquotad** デーモン • **rstatd** デーモン • **rusersd** デーモン • **rwalld** デーモン • **sprayd** デーモン • **pcnfsd** デーモン • **telnet** デーモン • cmsd サービス • ttdbserver サービス • TCP echo サービス • TCP discard サービス • TCP chargen サービス • TCP daytime サービス • TCP time サービス • UDP echo サービス • UDP discard サービス • UDP chargen サービス • UDP daytime サービス • UDP time サービス	/etc/security/pscexpert/bin/cominetdconf
CIP-005-3a R2.5	ポートに対するサービス妨害の緩和要求を実施します。	/etc/security/pscexpert/bin/tcptr_aixpert
CIP-005-3a R3 CIP-007-3a R5、R6.5	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。	/etc/security/pscexpert/bin/pciaudit
CIP-005-3a R3	新規に作成されたユーザー、ロール、およびイベントによって監査構成ファイルを更新します。	/etc/security/pscexpert/bin/auditconfig
CIP-007-3a R3	トラステッド・ネットワーク接続 (TNC) を使用可能にするためのメッセージを表示します。	/etc/security/pscexpert/bin/GeneralMsg
CIP-007-3a R4	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。	/etc/security/pscexpert/bin/manageITsecurity

表 10. PowerSC Standard Edition での CIP 標準 (続き)

CIP 標準	AIX Security Expert の実装	値を変更するスクリプトの場所
CIP-007-3a R5.2.1	ロックされていないすべてのデフォルト・ユーザー・アカウントについて、最初のログイン時にパスワードを変更できるようにします。	/etc/security/pscexpert/bin/pwdchg
CIP-007-3a R5.2.2-R5.2.3	すべてのデフォルト・ユーザー・アカウントをロックします。	/etc/security/pscexpert/dodv2/lockacc_rlogin
CIP-007-3a R5.3.1	各パスワードを 6 文字以上に設定します。	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.2	各パスワードを英字、数字、および特殊文字の組み合わせに設定します。	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.3	各パスワードを年 1 回変更します。	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R7	暗号化ファイルシステム (EFS) を使用可能にするためのメッセージを表示します。	/etc/security/pscexpert/bin/GeneralMsg
CIP-010-1	リアルタイム・コンプライアンス (RTC) を使用可能にするためのメッセージを表示します。	/etc/security/pscexpert/bin/GeneralMsg

次のリストに、AIX オペレーティング・システムに適用される CIP 標準に関する情報を示します。

標準 CIP–003–3 — サイバー・セキュリティー — セキュリティー管理制御

R5. アクセス制御

責任者は、保護された重要サイバー資産 (CCA) 情報へのアクセスを管理するためのプログラムを文書化および実装します。

- **R5.1:** 責任者は、保護情報への論理的アクセスまたは物理的アクセスを許可する、指定担当者のリストを維持します。
- **R5.1.1:** 担当者は、名前、役職、およびそれらの担当者がアクセスを許可する情報によって識別されます。

標準 CIP–005–3a — サイバー・セキュリティー — 電子的セキュリティー・ペリメーター

R2. 電子的アクセス制御

責任者は、電子的セキュリティー・ペリメーターへのすべての電子的アクセス・ポイントで電子的アクセスを制御するための、組織的プロセスと技術的および手続き的な仕組みを実装および文書化します。

- **R2.1:** これらのプロセスと仕組みにおいては、デフォルトでアクセスが拒否されるためアクセス許可を明示的に指定することが求められる、アクセス制御モデルが使用されます。
- **R2.2:** 電子的セキュリティー・ペリメーターへのすべてのアクセス・ポイントで、責任者は、操作用、および電子的セキュリティー・ペリメーター内のサイバー資産のモニター用に必要なポートとサービスのみを使用可能にし、それらのポートとサービスの構成を個別に、または指定されたグループごとに文書化します。
- **R2.3:** 責任者は、電子的セキュリティー・ペリメーターへのダイヤルアップ・アクセスを保護するための手順を実装および維持します。
- **R2.4:** 電子的セキュリティー・ペリメーター内への外部の対話式アクセスが有効な場合、責任者は、アクセス・ポイントで強固な手続き的または技術的な制御を実施して、そのアクセス元の確実性を確認します (技術的に可能な場合)。
- **R2.5:** 要求される文書では、以下を (少なくとも) 識別し、説明します。

– **R2.5.1:** アクセス要求および許可に関するプロセス。
– **R2.5.2:** 認証方式。
– **R2.5.3:** 標準 CIP-004-3 の要件 R4 に従った、許可権限のレビュー・プロセス。
– **R2.5.4:** ダイヤルアップでアクセス可能な接続を保護するために使用される制御。

R3. 電子的アクセスのモニター

責任者は、電子的セキュリティー・ペリメーターへのアクセス・ポイントにおいてアクセスを 1 日 24 時間、週 7 日モニターおよび記録する、電子的または手動によるプロセスを実装および文書化します。

- **R3.1:** ルーティング可能でないプロトコルを使用する、ダイヤルアップによってアクセス可能な重要サイバー資産の場合、責任者は、ダイヤルアップ・デバイスへの各アクセス・ポイントでのモニター・プロセスを実装および文書化します (技術的に可能な場合)。
- **R3.2:** 技術的に可能な場合、セキュリティー・モニター・プロセスが、無許可アクセスの試みまたは実際に行われた無許可アクセスを検出し、アラートを発行します。これらのアラートでは、指定された応答担当者に適切な通知が送られます。アラートの発行が技術的に可能でない場合、責任者は、少なくとも 90 日ごとに、無許可アクセスの試みまたは実際に行われた無許可アクセスに関するアクセス・ログを確認または取得します。

標準 CIP-007-3a - サイバー・セキュリティー - システム・セキュリティー管理

R2. ポートおよびサービス

責任者は、通常の操作および緊急時の操作に必要なポートとサービスのみを使用可能にするプロセスを確立、文書化、および実装します。

- **R2.1:** 責任者は、通常の操作および緊急時の操作に必要なポートとサービスのみを使用可能にします。
- **R2.2:** 責任者は、電子的セキュリティー・ペリメーター内のすべてのサイバー資産を実動に使用する前に、テスト用に使用されるポートを含め、他の用途のポートとサービスを使用不可にします。
- **R2.3:** 技術的な制約により未使用のポートとサービスを使用不可にできない場合、責任者は、リスク・エクスポージャーを緩和するために適用する補償的対策を文書化します。

R3. セキュリティー・パッチ管理

責任者は、電子的セキュリティー・ペリメーター内のすべてのサイバー資産に適用可能なサイバー・セキュリティー・ソフトウェア・パッチをトラッキング、評価、テスト、およびインストールするためのセキュリティー・パッチ管理プログラムを、別個に、または CIP-003-3 の要件 R6 に指定の文書化された構成管理プロセスのコンポーネントとして、確立、文書化、および実装します。

- **R3.1:** 責任者は、セキュリティー・パッチまたはセキュリティー・アップグレードが入手可能になってから 30 日以内に、それらのパッチとアップグレードの適用可能性の評価を文書化します。
- **R3.2:** 責任者は、セキュリティー・パッチの実装を文書化します。パッチがインストールされていない場合、責任者は、リスク・エクスポージャーを緩和するために適用する補償的対策を文書化します。

R4. 悪意のあるソフトウェアの阻止

責任者は、アンチウィルス・ソフトウェアやその他の悪意のあるソフトウェア (マルウェ

ア) 防止ツールを使用して (技術的に可能な場合)、電子的セキュリティー・ペリメーター内のすべてのサイバー資産に対するマルウェアの導入、エクスポージャー、および伝搬を検出、防止、阻止、および緩和します。

- **R4.1:** 責任者は、アンチウィルス・ツールおよびマルウェア防止ツールを文書化および実装します。アンチウィルス・ソフトウェアおよびマルウェア防止ツールがインストールされていない場合、責任者は、リスク・エクスポージャーを緩和するために適用する補償的対策を文書化します。
- **R4.2:** 責任者は、アンチウィルス・シグニチャーおよびマルウェア防止シグニチャーの更新のプロセスを文書化および実装します。このプロセスでは、これらのシグニチャーのテストおよびインストールを処理する必要があります。

R5. アカウント管理

責任者は、すべてのユーザー・アクティビティーのアクセス認証の実施およびそれらのアクティビティーの責任担当の適用を行うとともに、無許可のシステム・アクセスのリスクを緩和する、技術的および手続き的な制御を確立、実装、および文書化します。

- **R5.1:** 責任者は、個別および共有のシステム・アカウントと認可されたアクセス許可が、実行される作業上の職務に関する**知る必要性**の概念と整合するか検証します。
  - **R5.1.1:** 責任者は、少なくとも年 1 回ユーザー・アカウントを調べて、アクセス特権が標準 CIP-003-3 に従っているか検証します。
  - **R5.1.2:** 責任者は、最低でも 90 日間にわたる、個別のユーザー・アカウントのアクセス・アクティビティーのヒストリカル監査証跡を作成するために十分な詳細を含むログを生成する、方法、プロセス、および手順を確立します。
  - **R5.1.3:** 責任者は、少なくとも年 1 回ユーザー・アカウントを調べて、アクセス特権が標準 CIP-003-3 に従っているか検証します。
- **R5.2:** 責任者は、出荷時のデフォルト・アカウントを含む、管理者アカウント、共有アカウント、およびその他の汎用アカウントの特権の適用範囲と許容用途を最小限に抑え、管理するポリシーを実装します。
  - **R5.2.1:** このポリシーには、それらのアカウントの除去、無効化、または名前変更が含まれます (可能な場合)。有効なまま維持する必要があるアカウントの場合、システムを稼働させる前にパスワードを変更します。
  - **R5.2.2:** 責任者は、共有アカウントへのアクセス権限を持つ個人を識別します。
  - **R5.2.3:** これらのアカウントを共有する必要がある場合、責任者は、許可を持つユーザーのみにアクセスを制限するアカウント使用管理ポリシー、アカウント使用 (自動または手動) の監査証跡、担当者変更時 (割り当て変更や解雇などの場合) のアカウント保護手順を用意しています。
- **R5.3:** 少なくとも、責任者は以下の条件に従ったパスワードを使用する必要があります (技術的に可能な場合)。
  - **R5.3.1:** 各パスワードは 6 文字以上でなければなりません。
  - **R5.3.2:** 各パスワードは、英字、数字、および特殊文字の組み合わせで構成されている必要があります。
  - **R5.3.3:** 各パスワードは、リスクに基づき、年 1 回以上の頻度で変更する必要があります。

R6. セキュリティー状況モニター

責任者は、電子的セキュリティー・ペリメーター内のすべてのサイバー資産に、(技術的に

可能な場合) サイバー・セキュリティーに関連するシステム・イベントをモニターするための自動化ツールや組織的プロセス制御が実装されているか確認します。

- **R6.1:** 責任者は、電子的セキュリティー・ペリメーター内のすべてのサイバー資産に関するセキュリティー・イベントをモニターするための、組織的プロセスと技術的および手続き的な仕組みを実装および文書化します。
- **R6.2:** セキュリティー・モニター制御では、検出されたサイバー・セキュリティー・インシデントに関する自動および手動のアラートが発行されます。
- **R6.3:** 責任者は、サイバー・セキュリティーに関連するシステム・イベントのログを維持し (技術的に可能な場合)、標準 CIP-008-3 で求められているインシデントへの対応をサポートします。
- **R6.4:** 責任者は、要件 R6 で指定されているすべてのログを 90 日間保存します。
- **R6.5:** 責任者は、サイバー・セキュリティーに関連するシステム・イベントのログを調べ、それらのログのレビューを文書化したレコードを維持します。

R7. 破棄または再デプロイメント

責任者は、標準 CIP-005-3 内に示され、記載されている内容に従い、電子的セキュリティー・ペリメーター内のサイバー資産の破棄または再デプロイメントに関する正式な方法、プロセス、および手順を確立および実装します。

- **R7.1:** これらの資産を破棄する前に、責任者はデータ保管メディアを破壊または消去して、機密のサイバー・セキュリティー・データや信頼性データが無許可で取得されないようにします。
- **R7.2:** これらの資産の再デプロイメント前に、責任者は少なくともデータ保管メディアを消去して、機密のサイバー・セキュリティー・データや信頼性データが無許可で取得されないようにします。

CIP–010–1 — サイバー・セキュリティー — 構成変更管理および脆弱性評価

R1: 責任者は、該当する各要件部分を集合的に含む 1 つ以上の文書化されたプロセスを (欠陥を特定、評価、および訂正する方法で) 実装します。

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。

```
pscxpert –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・ラインから 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・ラインからの PowerSC のコンプライアンスの構成

AIX システムでは **pscxpert** 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 11. AIX の PowerSC コマンド

コマンド	コンプライアンス規格
% pscxpert -f /etc/security/aixpert/custom/DoD.xml	*米国国防総省の UNIX Security Technical Implementation Guide*
% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml	*Health Insurance Portability and Accountability Act*
% pscxpert -f /etc/security/aixpert/custom/PCI.xml	*Payment Card Industry-Data Security Standard*
% pscxpert -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 12. 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/Hipaa.xml	*Health Insurance Portability and Accountability Act*
% 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 **pscxpert** 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:

115 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 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 Standard Edition バージョン 1.1.4 以降とともにインストールされ、ベースの AIX オペレーティング・システムには含まれていません。

PowerSC Real Time Compliance 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)
   - AIX バージョン 7.2 以降 (AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 7.2.0.0) 以降付き)
2. PowerSC Real Time Compliance フィーチャーのファイルセットを更新またはインストールするには、PowerSC Standard Edition バージョン 1.1.4 以降のインストール・パッケージから `powerscStd.rtc` ファイルセットをインストールします。

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 **pscxpert** 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。

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

トラステッド・ブート

トラステッド・ブート・フィーチャーは、Trusted Computing Group の TPM の仮想インスタンスである仮想トラステッド・プラットフォーム・モジュール (VTPM) を使用します。 VTPM は、システム・ブートの計測値を将来の検証のために安全に保管する目的で使用されます。

トラステッド・ブートの概念

ブート・プロセスの保全性、およびブートをトラステッド・ブートまたは非トラステッド・ブートとして分類する方法を理解することは、重要です。

ハードウェア管理コンソール (HMC) を使用して、物理システムごとに最大 60 の VTPM 対応ロジカル・パーティション (LPAR) を構成できます。構成された VTPM は、LPAR ごとに固有のものになります。VTPM は、AIX トラステッド実行テクノロジーと一緒に使用されると、以下のパーティションに対してセキュリティーと保証を提供します。

- ディスク上のブート・イメージ
- オペレーティング・システム全体
- アプリケーション層

管理者は、AIX 拡張パックで入手可能な **openpts** ベリファイヤーと一緒にインストールされる中央コンソールから、トラステッド・システムと非トラステッド・システムを表示できます。**openpts** コンソールは、1 台以上の Power Systems サーバーを管理して、データ・センター内の AIX システムのトラステッド状態をモニターまたは認証します。認証は、コレクターがトラステッド・ブートを実行したかどうかをベリファイヤーが判別 (または認証) するプロセスです。

トラステッド・ブート状況

コレクターの保全性をベリファイヤーが正常に認証した場合、パーティションはトラステッドであると言えます。ベリファイヤーは、コレクターがトラステッド・ブートを実行したかどうかを判別するリモート・パーティションです。コレクターは、仮想トラステッド・プラットフォーム・モジュール (VTPM) が接続され、Trusted Software Stack (TSS) がインストールされた AIX のパーティションです。これは、VTPM 内で記録された計測値がベリファイヤーによって保持されている参照セットと一致することを示しています。トラステッド・ブート状態は、パーティションが信頼できる方法でブートされたかどうかを示します。この記述は、システムのブート・プロセスの保全性に関するものであり、システムの現在または持続的なセキュリティー・レベルを示すものではありません。

非トラステッド・ブート状況

ベリファイヤーがブート・プロセスの保全性を正常に認証できない場合、パーティションは非トラステッド状態になります。非トラステッド状態は、ブート・プロセスの何らかの側面がベリファイヤーによって保持されている参照情報と矛盾していることを示します。認証の失敗の考えられる原因として、別のブート・デバイスからのブート、別のカーネル・イメージのブート、および既存のブート・イメージの変更が挙げられます。

関連概念:

128 ページの『トラステッド・ブートのトラブルシューティング』
トラステッド・ブートの使用時における認証失敗の理由を特定するには、一般的なシナリオと修復手順がい

くつか必要です。

トラステッド・ブートの計画

トラステッド・ブートをインストールするために必要なハードウェアおよびソフトウェアの構成について説明します。

トラステッド・ブートの前提条件

トラステッド・ブートをインストールするには、コレクターとベリファイヤーを構成する必要があります。

トラステッド・ブートをインストール済みのシステムに AIX オペレーティング・システムを再インストールする際は、事前に `/var/tss/lib/tpm/system.data` ファイルをコピーし、再インストールの完了後にそのファイルで同じ場所にあるファイルを上書きする必要があります。このファイルをコピーしない場合は、管理コンソールから仮想トラステッド・プラットフォーム・モジュールを取り外して、パーティションに再インストールする必要があります。

コレクター

コレクターをインストールするための構成要件には、以下の前提条件が含まれます。

- POWER7 ハードウェアが 740 ファームウェア・リリースで稼働している。
- IBM AIX 6 (テクノロジー・レベル 7 適用) または IBM AIX 7 (テクノロジー・レベル 1 適用) をインストールする。
- ハードウェア管理コンソール (HMC) バージョン 7.4 以降をインストールする。
- VTPM と最小 1 GB のメモリーを使用してパーティションを構成する。
- セキュア・シェル (SSH)、特に OpenSSH またはこれと同等のものをインストールする。

ベリファイヤー

openpts ベリファイヤーには、コマンド・ライン・インターフェース、および幅広いプラットフォームで実行されるように設計されたグラフィカル・ユーザー・インターフェースからアクセスできます。OpenPTS ベリファイヤーの AIX バージョンは、AIX 拡張パックで入手できます。Linux およびその他のプラットフォーム向けの OpenPTS ベリファイヤーのバージョンは、Web ダウンロードで入手できます。構成要件には、以下の前提条件が含まれます。

- SSH、特に OpenSSH またはこれと同等のものをインストールする。
- コレクターへのネットワーク接続を (SSH を介して) 確立する。
- グラフィカル・インターフェースから **openpts** コンソールにアクセスするために Java™ 1.6 以降をインストールする。

修復の準備

ここで説明するトラステッド・ブートに関する情報は、修正が必要な場合があるシチュエーションを識別するためのガイドとして役立ちます。ブート・プロセスに影響はありません。

認証の失敗を引き起こす状況は数多くあり、発生する可能性がある状況を予測するのは困難です。状況に応じて適切なアクションを決定する必要があります。ただし、いくつかの重大なシナリオに備えて準備し、そのような問題に対処する上で役立つポリシーまたはワークフローを用意しておくことをお勧めします。修復とは、認証により、1 つ以上のコレクターがトラステッドでないことが報告される場合に実行する必要がある修正処置です。

例えば、ブート・イメージがベリファイヤーの参照と異なることが原因で、認証の失敗が起こった場合、以下の質問に対する回答を検討してください。

- 脅威が確かであることをどのようにして検証できますか?
- 計画的保守または AIX のアップグレードが行われたか、新しいハードウェアが最近取り付けられましたか?
- この情報にアクセスできる管理者に連絡できますか?
- システムが最後にトラステッド状態でブートされたのはいつですか?
- セキュリティー脅威が確かであると思われる場合、どのようなアクションを実行する必要がありますか? (監査ログの収集、ネットワークからのシステムの切断、システムの電源オフ、およびユーザーへのアラートなどが推奨されます。)
- チェックする必要のある、信用性に欠けるシステムが他にありますか?

関連概念:

128 ページの『トラステッド・ブートのトラブルシューティング』
トラステッド・ブートの使用時における認証失敗の理由を特定するには、一般的なシナリオと修復手順がいくつか必要です。

マイグレーションに関する考慮事項

仮想トラステッド・プラットフォーム・モジュール (VTPM) に対して使用可能にされたパーティションのマイグレーションを行う前に、以下の前提条件について考慮してください。

物理 TPM よりも VTPM の方が優れている点は、VTPM を保持しながらシステム間でパーティションを移動できることです。ロジカル・パーティションを安全にマイグレーションするために、ファームウェアは VTPM データを送信前に暗号化します。確実に安全なマイグレーションを行うには、マイグレーションの前に、以下のセキュリティー対策を実装する必要があります。

- マイグレーションを実行する 仮想 I/O サーバー (VIOS) 間で IPSEC を使用可能にします。
- マイグレーション後に VTPM データを暗号化解除できる管理対象システムを制御するために、ハードウェア管理コンソール (HMC) を使用してトラステッド・システムの鍵を設定します。データを正常にマイグレーションするには、マイグレーションの宛先システムにソース・システムと同じ鍵が必要です。

関連情報:

HMC の使用

VIOS のマイグレーション

トラステッド・ブートのインストール

トラステッド・ブートをインストールするには、ハードウェアおよびソフトウェアの構成がいくつか必要です。

関連情報:

7 ページの『PowerSC Standard Edition 1.1.4 のインストール』
PowerSC Standard Edition の特定の機能ごとに、ファイルセットを 1 つインストールする必要があります。

コレクターのインストール

AIX の基本 CD からファイルセットを使用してコレクターをインストールする必要があります。

コレクターをインストールするには、**smit** または **installp** コマンドを使用して、基本 CD にある powerscStd.vtpm および openpts.collector パッケージをインストールします。

ベリファイヤーのインストール

OpenPTS ベリファイヤー・コンポーネントは、AIX オペレーティング・システムおよびその他のプラットフォーム上で稼働します。

ベリファイヤーの AIX バージョンは、AIX 拡張パックを使用してファイルセットからインストールできます。AIX オペレーティング・システムにベリファイヤーをインストールするには、**smit** または **installp** コマンドを使用して、AIX 拡張パックから openpts.verifier パッケージをインストールします。このインストールにより、ベリファイヤーのコマンド・ラインとグラフィカル・インターフェースの両方のバージョンがインストールされます。

その他のオペレーティング・システム用の OpenPTS ベリファイヤーは、Download Linux OpenPTS Verifier For Use With AIX Trusted Boot からダウンロードできます。

関連情報:

Download Linux OpenPTS Verifier For Use With AIX Trusted Boot

---

トラステッド・ブートの構成

システムを登録して、トラステッド・ブートでシステムを認証する手順について説明します。

システムの登録

システムをベリファイヤーに登録する手順について説明します。

システムの登録は、ベリファイヤーに一連の初期計測値を提供するプロセスであり、後続の認証要求の基礎となります。コマンド・ラインからシステムを登録するには、ベリファイヤーから以下のコマンドを使用します。

```
openpts -i <hostname>
```

登録されたパーティションに関する情報は、$HOME/.openpts ディレクトリーに置かれます。新しい各パーティションは、登録プロセス中に固有 ID を割り当てられ、登録されたパーティションに関する情報は固有 ID に対応するディレクトリーに保管されます。

グラフィカル・インターフェースからシステムを登録するには、以下のステップを実行します。

1. **/opt/ibm/openpts_gui/openpts_GUI.sh** コマンドを使用してグラフィカル・インターフェースを起動します。
2. ナビゲーション・メニューから「**登録 (Enroll)**」を選択します。
3. システムのホスト名および SSH 資格情報を入力します。
4. 「**登録 (Enroll)**」をクリックします。

関連概念:

127 ページの『システムの認証』
コマンド・ラインおよびグラフィカル・インターフェースを使用してシステムを認証する手順について説明します。

システムの認証

コマンド・ラインおよびグラフィカル・インターフェースを使用してシステムを認証する手順について説明します。

システム・ブートの保全性を照会するには、ベリファイヤーから次のコマンドを使用します。

```
openpts <hostname>
```

グラフィカル・インターフェースからシステムを認証するには、以下のステップを実行します。

1. ナビゲーション・メニューからカテゴリーを選択します。
2. 認証する 1 つ以上のシステムを選択します。
3. 「**認証 (Attest)**」をクリックします。

パスワードを使用しないシステムの登録と認証

認証要求は セキュア・シェル (SSH) を介して送信されます。パスワードを使用せずに SSH 接続を許可するには、ベリファイヤーの証明書をコレクターにインストールします。

ベリファイヤーの証明書をコレクターのシステムでセットアップするには、以下のステップを実行します。

- ベリファイヤーで、次のコマンドを実行します。

  ```
  ssh-keygen    # No passphrase
  scp ~/.ssh/id_rsa.pub <collector>:/tmp
  ```

- コレクターで、次のコマンドを実行します。

  ```
  cat /tmp/id_rsa.pub >> ~/.ssh/authorized_keys
  ```

トラステッド・ブートの管理

トラステッド・ブートの認証結果を管理する手順について説明します。

認証結果の解釈

認証結果を表示して理解する手順について説明します。

認証の結果は、次のいずれかの状態になります。

1. 認証要求の失敗: 認証要求は正常に完了しませんでした。失敗の考えられる原因を理解するには、トラブルシューティングのセクションを参照してください。
2. システム保全性が有効: 認証が正常に完了して、システム・ブートがベリファイヤーによって保持されている参照情報と一致しています。これは、正常なトラステッド・ブートを示しています。
3. システム保全性が無効: 認証要求は完了しましたが、システム・ブート時に収集された情報とベリファイヤーによって保持されている参照情報との間に不一致が検出されました。これは、非トラステッド・ブートを示しています。

認証では、以下のメッセージが使用されて、コレクターに更新が適用されたかどうかも報告されます。

システム更新が使用可能: このメッセージは、更新がコレクターに適用され、次回のブートから有効になる一連の更新済み参照情報が使用可能であることを示しています。ベリファイヤーで更新を受け入れるか、拒否するかのプロンプトがユーザーに対して出されます。例えば、ユーザーは、コレクターで保守が行われていることを認識している場合に、これらの更新を受け入れることを選択できます。

グラフィカル・インターフェースを使用して認証の失敗を調査するには、以下のステップを実行します。

1. ナビゲーション・メニューからカテゴリーを選択します。
2. 調査するシステムを選択します。
3. システムに対応するエントリーをダブルクリックします。「プロパティー」ウィンドウが表示されます。このウィンドウには、失敗した認証に関するログ情報が含まれています。

システムの削除

ベリファイヤーのデータベースからシステムを削除する手順について説明します。

ベリファイヤーのデータベースからシステムを削除するには、次のコマンドを実行します。

```
openpts -r <hostname>
```

トラステッド・ブートのトラブルシューティング

トラステッド・ブートの使用時における認証失敗の理由を特定するには、一般的なシナリオと修復手順がいくつか必要です。

システムの現行のブート状態がベリファイヤーで保持されている参照情報と一致しない場合、**openpts** コマンドはシステムを無効として宣言します。**openpts** コマンドは、保全性が無効になった理由として考えられるものを判別します。完全な AIX のブートにはいくつかの変数があり、認証が失敗した場合は、失敗の原因を判別するために分析する必要があります。

次の表に、失敗の理由を特定するための一般的なシナリオと修復手順をリストします。

表 13. 一般的な失敗のシナリオのトラブルシューティング

失敗の理由	失敗の考えられる原因	推奨される修復手順

認証が完了しなかった。	• ホスト名が誤っています。
	• ソースと宛先の間にネットワーク経路がありません。
	• セキュリティー資格情報が誤っています。
		次のコマンドを使用して、セキュア・シェル (SSH) 接続を検査します。
		`ssh ptsc@hostname`
		
		SSH 接続が正常である場合は、認証失敗の以下の理由について確認します。
		• 認証対象のシステムが **tcsd** デーモンを実行していません。
		• 認証対象のシステムが、**ptsc** コマンドによって初期化されていません。このプロセスは、システム始動時に自動的に行われるはずですが、コレクター上に `/var/ptsc/` ディレクトリーが存在していることを確認してください。`/var/ptsc/` ディレクトリーが存在しない場合、コレクターで次のコマンドを実行します。
		`ptsc -i`

CEC ファームウェアが変更された。	• ファームウェア・アップグレードが適用されました。 • LPAR は、別のバージョンのファームウェアを実行していたシステムからマイグレーションされました。	LPAR をホスティングしているシステムのファームウェア・レベルを確認します。
LPAR に割り当てられているリソースが変更された。	LPAR に割り当てられている CPU またはメモリーが変更されました。	HMC のパーティション・プロファイルを確認します。

表 13. 一般的な失敗のシナリオのトラブルシューティング (続き)

失敗の理由	失敗の考えられる原因	推奨される修復手順
LPAR で使用可能なアダプターのファームウェアが変更された。	LPAR でハードウェア・デバイスの追加または取り外しが行われました。	HMC のパーティション・プロファイルを確認します。
LPAR に接続されているデバイスのリストが変更された。	LPAR でハードウェア・デバイスの追加または取り外しが行われました。	HMC のパーティション・プロファイルを確認します。
オペレーティング・システム・カーネルを含むブート・イメージが変更された。	• AIX の更新が適用されましたが、ベリファイヤーが更新を認識しませんでした。 • **bosboot** コマンドが実行されました。	• コレクターの管理者に、最後のリブート操作の前に保守作業が行われたかどうかを確認します。 • コレクターのログで、保守アクティビティーが行われたかどうかを確認します。
LPAR が別のデバイスからブートされた。	• ネットワーク・インストールの直後に登録が行われました。 • システムが保守デバイスからブートされました。	ブート・デバイスおよびフラグは、**bootinfo** コマンドを使用して検査できます。ネットワーク・インストール管理 (NIM) のインストールの直後、リブート操作が行われるまでの間に登録が実行された場合、登録された詳細はネットワーク・インストールに関連しており、次回のディスク・ブートには関連していません。登録を削除してロジカル・パーティションを再登録することにより、この登録を修復できます。
対話式のシステム管理サービス (SMS) ブート・メニューが呼び出された。		システムがトラステッドとなるためには、ユーザー対話なしに中断されることなくブート・プロセスが実行される必要があります。SMS ブート・メニューに入ると、ブートは無効になります。
トラステッド実行 (TE) データベースが変更された。	• TE データベースでバイナリー・ファイルが追加されたか、削除されました。 • データベース内のバイナリー・ファイルが更新されました。	**trustchk** コマンドを実行して、データベースを検査します。

関連概念:

124 ページの『修復の準備』
ここで説明するトラステッド・ブートに関する情報は、修正が必要な場合があるシチュエーションを識別するためのガイドとして役立ちます。ブート・プロセスに影響はありません。

123 ページの『トラステッド・ブートの概念』
ブート・プロセスの保全性、およびブートをトラステッド・ブートまたは非トラステッド・ブートとして分類する方法を理解することは、重要です。

関連情報:

HMC の使用

トラステッド・ファイアウォール

トラステッド・ファイアウォール・フィーチャーは、同一の Power Systems サーバー上の異なる仮想 LAN (VLAN) セキュリティー・ゾーン間で通信する際のパフォーマンスとリソース効率を向上する、仮想化層のセキュリティーを提供します。指定されたルールに合致するファイアウォール・パケットのフィルタリング機能を仮想化層に移動することにより、トラステッド・ファイアウォールによって外部ネットワークでの負荷が減少します。このフィルタリング機能は容易に定義できるネットワーク・フィルター・ルールによって処理されます。これにより、仮想環境のままで、トラステッド・ネットワーク・トラフィックが VLAN セキュリティー・ゾーン間を移動することが許可されます。トラステッド・ファイアウォールは、AIX、IBM i、および Linux オペレーティング・システムの間の内部ネットワーク・トラフィックを保護し、ルーティングします。

トラステッド・ファイアウォールの概念

トラステッド・ファイアウォールを使用する際には、基本的な概念をいくつか理解する必要があります。

Power Systems ハードウェアは、複数の仮想 LAN (VLAN) セキュリティー・ゾーンを使用して構成することができます。トラステッド・ファイアウォールのフィルター・ルールとして作成されたユーザー構成ポリシーによって、いくつかのトラステッド・ネットワーク・トラフィックが、複数の VLAN セキュリティー・ゾーン間を移動し、仮想化層の内部にとどまることが許可されます。これは、ネットワーク接続された物理的ファイアウォールを仮想化環境に導入するのと類似しており、ファイアウォール機能を実装するためのパフォーマンス効率が高い方式を、仮想化データ・センターに提供します。

トラステッド・ファイアウォールを使用すると、他のタイプのトラフィックを制限して高水準のセキュリティーを維持したまま、仮想 I/O サーバー (VIOS) 上のある VLAN から、同じ VIOS 上にある別の VLAN に直接転送するための特定のタイプのトラフィックを許可するルールを構成することができます。これは、Power Systems サーバーの仮想化層内の構成可能なファイアウォールです。

132 ページの図 1 の例では、情報をセキュアかつ効率的に VLAN 200 上の LPAR1 および VLAN 100 上の LPAR2 から転送できるようになることが目標です。トラステッド・ファイアウォールがない場合、LPAR1 から LPAR2 を宛先とした情報は内部ネットワークの外部のルーターに送信され、このルーターが情報を LPAR2 に経路指定します。

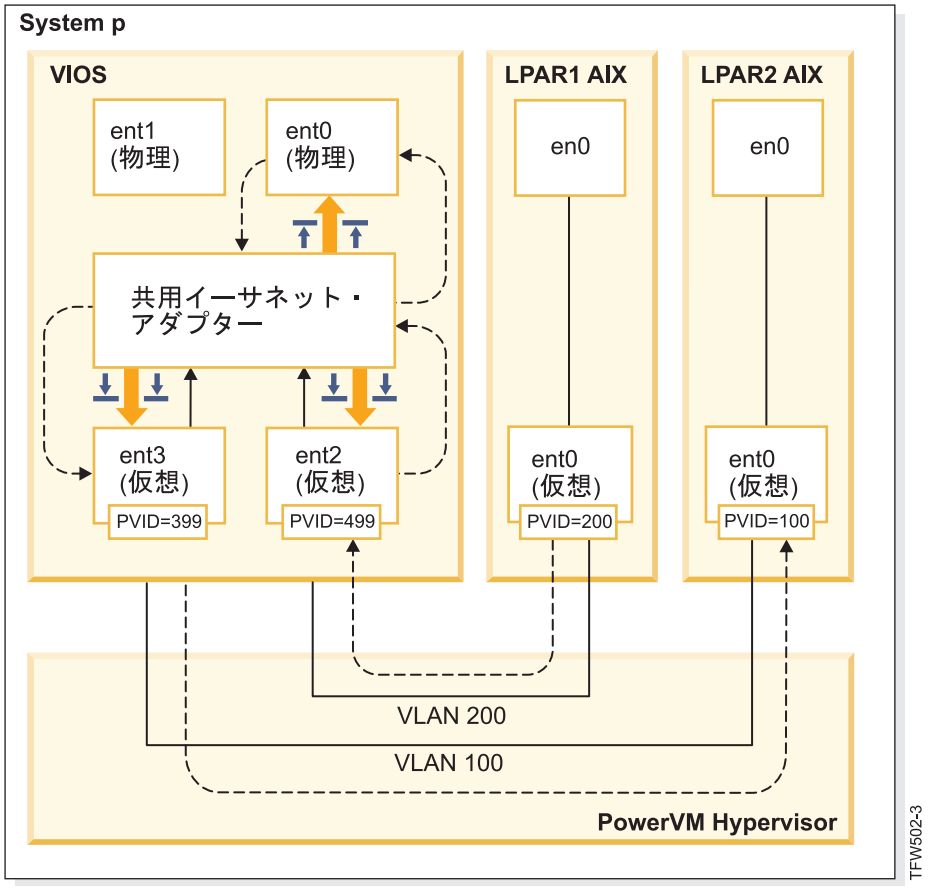

図 1. トラステッド・ファイアウォールを使用しない、VLAN 間の情報転送の例

トラステッド・ファイアウォールを使用して、情報が内部ネットワークの外部に出ずに LPAR1 から LPAR2 にパスされるのを許可するルールを構成することができます。このパスは、 133 ページの図 2 に示されています。

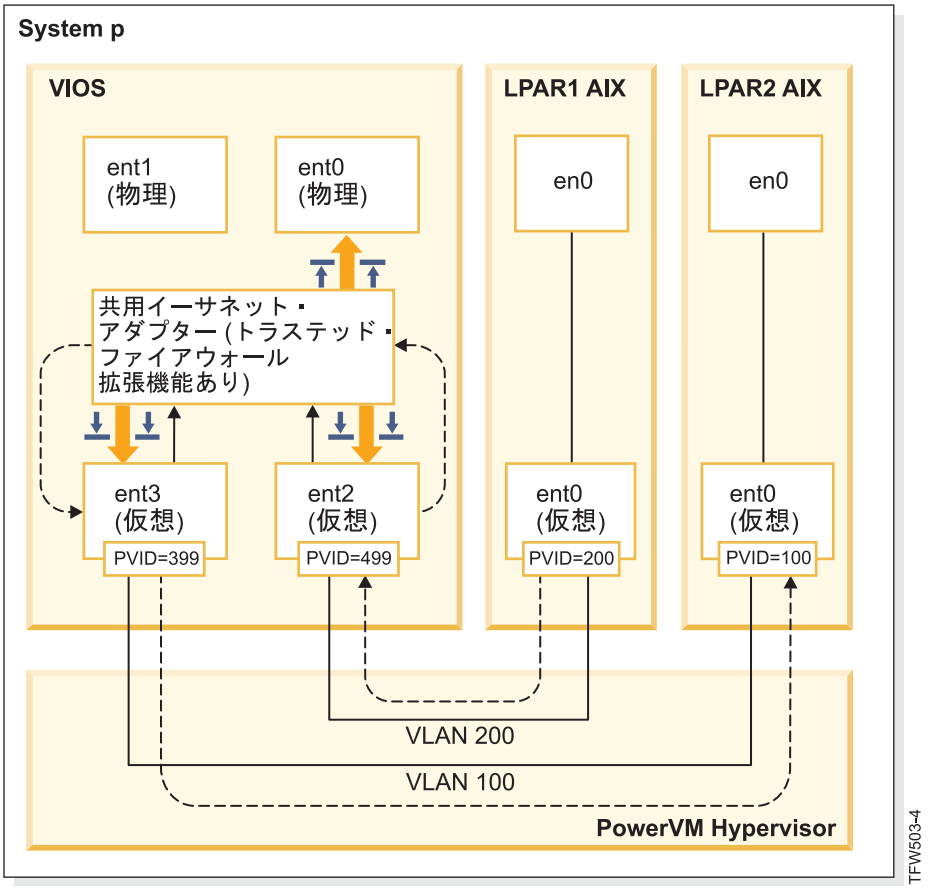

図 2. トラステッド・ファイアウォールを使用した、VLAN 間の情報転送の例

特定の情報が VLAN 間をセキュアにパスすることを許可する構成ルールによって、宛先へのパスが短くなります。トラステッド・ファイアウォールでは、共用イーサネット・アダプター (SEA) および Security Virtual Machine (SVM) カーネル・エクステンションを使用して、通信が可能になります。

共用イーサネット・アダプター

SEA は、経路指定の開始点および終着点です。SVM が登録されると、SEA はパケットを受け取り、それを SVM に転送します。パケットの宛先が同一の Power Systems サーバー上の LPAR であると SVM が判断した場合、SVM はパケットの層 2 のヘッダーを更新します。パケットは、システム内部または外部ネットワーク上の最終の宛先に転送するために、SEA に戻されます。

Security Virtual Machine

SVM は、フィルター・ルールの適用地点です。フィルター・ルールは、内部ネットワークのセキュリティーを維持するために必要です。 SVM を SEA に登録すると、パケットは外部ネットワークに送信される前に SVM に転送されます。パケットが内部ネットワークにとどまるか、または外部ネットワークに移動するかを、SVM がアクティブなフィルター・ルールに基づいて判別します。

トラステッド・ファイアウォールのインストール

PowerSC トラステッド・ファイアウォールのインストールは、他の PowerSC フィーチャーのインストールと同様です。

前提条件:

- 1.1.1.0 より前の PowerSC バージョンには、トラステッド・ファイアウォールをインストールするために必要なファイルセットがありませんでした。バージョン 1.1.1.0 以降の PowerSC インストール CD を必ず準備してください。
- トラステッド・ファイアウォールを利用するには、仮想 LAN (VLAN) を構成するためにハードウェア管理コンソール (HMC) または 仮想 I/O サーバー (VIOS) を既に使用したことがなければなりません。

トラステッド・ファイアウォールは、PowerSC Standard Edition のインストール CD で、追加のファイルセットとして提供されています。ファイル名は `powerscStd.svm.rte` です。トラステッド・ファイアウォールは、PowerSC バージョン 1.1.0.0 以降の既存のインスタンスに追加することも、PowerSC バージョン 1.1.1.0 以降の新規インストールの一環としてインストールすることも可能です。

トラステッド・ファイアウォール機能を既存の PowerSC インスタンスに追加するには、以下のようにします。

1. VIOS バージョン 2.2.1.4 以降を実行していることを確認します。
2. バージョン 1.1.1.0 の PowerSC インストール CD を挿入するか、インストール CD のイメージをダウンロードします。
3. ルート・アクセスに **oem_setup_env** コマンドを使用します。
4. **installp** コマンドまたは SMIT ツールを使用して、`PowerscStd.svm.rte` ファイルセットをインストールします。

関連情報:

7 ページの『PowerSC Standard Edition 1.1.4 のインストール』
PowerSC Standard Edition の特定の機能ごとに、ファイルセットを 1 つインストールする必要があります。

トラステッド・ファイアウォールの構成

トラステッド・ファイアウォール・フィーチャーをインストールしたら、追加の構成設定が必要です。

トラステッド・ファイアウォール・アドバイザー

トラステッド・ファイアウォール・アドバイザーは、さまざまなロジカル・パーティション (LPAR) からのシステム・トラフィックを分析し、トラステッド・ファイアウォールの実行により、システム・パフォーマンスが向上するかどうか判断するのに情報を提供します。

トラステッド・ファイアウォール・アドバイザー機能が、同一の中央電子処理装置上のさまざまな仮想 LAN (VLAN) からの大量のトラフィックを記録する場合は、トラステッド・ファイアウォールを使用可能化することがシステムにメリットをもたらします。

トラステッド・ファイアウォール・アドバイザーを使用可能にするには、次のコマンドを入力します。

```
vlantfw -m
```

トラステッド・ファイアウォール・アドバイザーの結果を表示するには、次のコマンドを入力します。

```
vlantfw -D
```

トラステッド・ファイアウォール・アドバイザーを使用不可にするには、次のコマンドを入力します。

```
vlantfw -M
```

トラステッド・ファイアウォール・ロギング

トラステッド・ファイアウォール・ロギングは、中央電子処理装置内のネットワーク・トラフィック・パスのリストをコンパイルします。このリストは、トラステッド・ファイアウォールがトラフィックのルーティングに使用するフィルターを示します。

トラステッド・ファイアウォール・アドバイザーが、トラフィックのルーティングにより内部的に効率性が改善されたと判断した場合、トラステッド・ファイアウォール・ロギングは svm.log ファイル内にパスのリストを保持します。svm.log ファイルのサイズは 16 MB に制限されています。エントリーが 16 MB の制限を超えると、最も古いエントリーがログ・ファイルから削除されます。

トラステッド・ファイアウォール・ロギングを開始するには、以下のコマンドを入力します。

```
vlantfw -l
```

トラステッド・ファイアウォール・ロギングを停止するには、以下のコマンドを入力します。

```
vlantfw -L
```

このログ・ファイルの場所は、/home/padmin/svm/svm.log です。

注: これらのコマンドを使用してトラステッド・ファイアウォール・ロギングを開始および停止できるのは、root ユーザーとして認証されている場合のみです。

複数の共用イーサネット・アダプター

複数の共用イーサネット・アダプターを使用するシステム上で、トラステッド・ファイアウォールを構成することができます。

一部の構成では、同一の 仮想 I/O サーバー (VIOS) 上で複数の共用イーサネット・アダプターが使用されます。複数の SEA によって、フェイルオーバー保護およびリソース平準化という利点が実現します。トラステッド・ファイアウォールは複数の SEA が同一の VIOS 上にある場合、複数の SEA 全体のルーティングをサポートします。

136 ページの図 3 では、複数の SEA を使用した環境を示します。

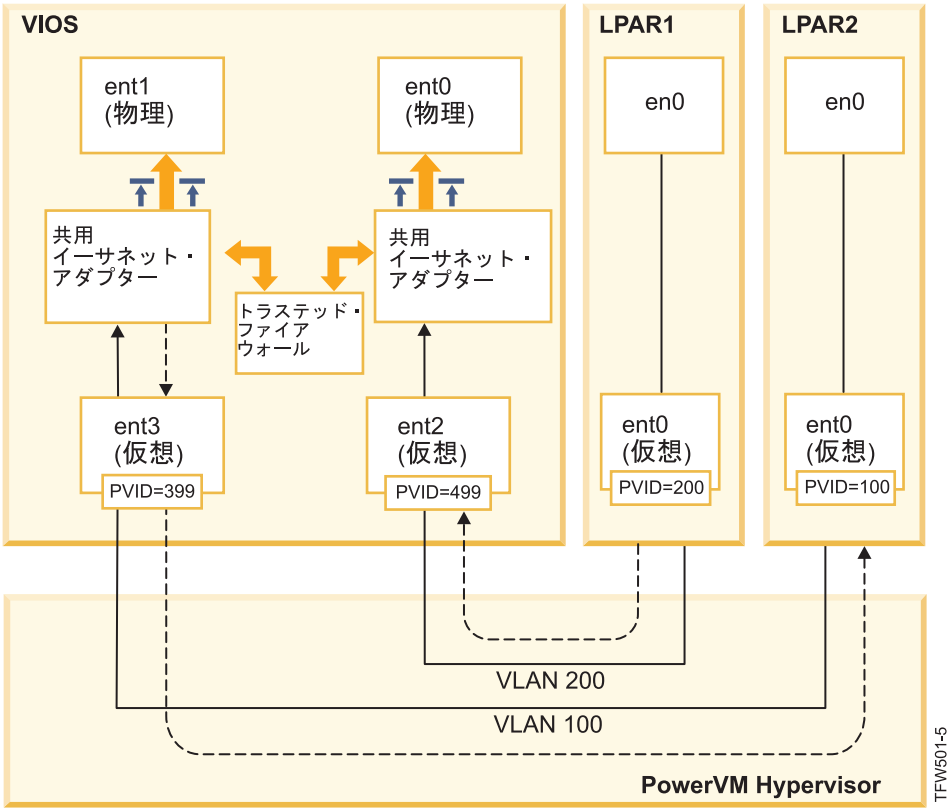

図 3. 単一の VIOS 上で複数の共用イーサネット・アダプターを使用する構成

トラステッド・ファイアウォールによってサポートされる複数の SEA 構成の例は、以下のとおりです。

- 同一の Power® ハイパーバイザー仮想スイッチ上で、トランク・アダプターを使用して SEA が構成される。この構成がサポートされるのは、各 SEA が異なる VLAN ID を使用してネットワーク・トラフィックを受信するためです。
- 複数の異なる Power ハイパーバイザー仮想スイッチ上で、トランク・アダプターを使用して SEA が構成され、各トランク・アダプターは異なる VLAN ID 上にある。この構成でも、各 SEA は異なる VLAN ID を使用してネットワーク・トラフィックを受信します。
- 複数の異なる Power ハイパーバイザー仮想スイッチ上で、トランク・アダプターを使用して SEA が構成され、この仮想スイッチ上では同一の VLAN ID が再利用される。この場合、両方の SEA に対するトラフィックでは同じ VLAN ID が使用されます。

  この構成の例としては、仮想スイッチ 10 の VLAN200 で LPAR2 が使用され、仮想スイッチ 20 の VLAN200 で LPAR3 が使用されます。両方の LPAR およびそれに対応する SEA では、同一の VLAN ID (VLAN200) が使用され、両方の SEA はその VLAN ID のパケットにアクセスすることができます。

複数の VIOS でブリッジングを使用可能にすることはできません。これが理由で、以下の複数の SEA の構成はトラステッド・ファイアウォールによってサポートされません。

- 複数の VIOS および複数の SEA ドライバー。
- 冗長 SEA ロード共有。VLAN 間のルーティング用に構成されたトランク・アダプターは、VIOS サーバーの間で分割することができません。

共用イーサネット・アダプターの除去

共用イーサネット・アダプター装置をシステムから除去する手順は、特定の順序で実行する必要があります。

ご使用のシステムから共用イーサネット・アダプターを除去するには、以下のステップを実行します。

1. 以下のコマンドを入力して、SEA に関連付けられている Security Virtual Machine を除去します。

   ```
   rmdev -dev svm
   ```

2. 以下のコマンドを入力して、SEA を除去します。

   ```
   rmdev -dev shared ethernet adapter ID
   ```

注: SVM を除去する前に SEA を除去すると、システム障害が発生する可能性があります。

ルールの作成

トラステッド・ファイアウォールの VLAN 間ルーティングを使用可能にするためのルールを作成することができます。

トラステッド・ファイアウォールのルーティング機能を使用可能にするために、許可される通信を指定するルールを作成する必要があります。セキュリティーを強化するために、システム上にあるすべての VLAN 間での通信を許可するという単一のルールはありません。アクティブ化された各ルールは、指定されたエンドポイントに対して双方向の通信を許可しますが、許可された接続にはそれぞれ独自のルールが必要です。

ルールの作成は 仮想 I/O サーバー (VIOS) インターフェースで行われるため、コマンドに関する追加情報は、Power Systems ハードウェア・インフォメーション・センターの VIOS トピックの集合で入手可能です。

ルールを作成するには、以下のステップを実行します。

1. VIOS コマンド・ライン・インターフェースを開きます。
2. 以下のコマンドを入力して、SVM ドライバーを開始します。

   ```
   mksvm
   ```

3. 以下の開始コマンドを入力して、トラステッド・ファイアウォールを開始します。

   ```
   vlantfw -s
   ```

4. 既知のすべての LPAR IP および MAC アドレスを表示するには、以下のコマンドを入力します。

   ```
   vlantfw -d
   ```

   作成するルールの対象となるロジカル・パーティション (LPAR) の IP アドレスと MAC アドレスが必要になります。

5. 以下のいずれかのコマンドを入力して、2 つの LPAR (LPAR1 および LPAR2) の間で通信を許可するフィルター・ルールを作成します。
   - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]`
   - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]-o any -p 0 -O gt -P 23`

   注: 一方のフィルター・ルールでは、ポートおよびプロトコルの入力に応じて、デフォルトで双方向の通信が許可されます。例えば、以下のコマンドを実行して、LPAR1 から LPAR2 の Telnet を使用可能にすることができます。

   ```
   genvfilt -v4 -a-P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress] -o
   any -p 0 -O eq -P 23
   ```

6. 以下のコマンドを入力して、カーネル内のすべてのフィルター・ルールをアクティブにします。

```
mkvfilt -u
```

注: この手順では、このルールおよびシステム内に存在する他のすべてのフィルター・ルールがアクティブにされます。

追加の例

以下の例では、トラステッド・ファイアウォールを使用して作成することができる他のフィルター・ルールを示しています。

- VLAN 100 上の LPAR から VLAN 200 上の LPAR へのセキュア・シェル通信を許可するには、以下のコマンドを入力します。

  ```
  genvfilt -v4 -a P -z 100 -Z 200 -o any -p 0 -O eq -P 22 -c tcp
  ```

- 0 から 499 のすべてのポート間でのトラフィックを許可するには、以下のコマンドを入力します。

  ```
  genvfilt -v4 -a P -z 100 -z 200 -o lt -p 500 -O lt -P 500 -c tcp
  ```

- LPAR 間でのすべての TCP トラフィックを許可するには、以下のコマンドを入力します。

  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c tcp
  ```

  ポート、またはポート操作を指定しない場合、トラフィックではすべてのポートが使用されます。

- LPAR 間での Internet Control Message Protocol メッセージングを許可するには、以下のコマンドを入力します。

  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c icmp
  ```

関連概念:

『ルールの非アクティブ化』
トラステッド・ファイアウォール・フィーチャーで、VLAN 間ルーティングを使用可能にするルールを非アクティブにすることができます。

関連資料:

158 ページの『genvfilt コマンド』
160 ページの『mkvfilt コマンド』
176 ページの『vlantfw コマンド』

関連情報:

仮想入出力サーバー (VIOS)

ルールの非アクティブ化

トラステッド・ファイアウォール・フィーチャーで、VLAN 間ルーティングを使用可能にするルールを非アクティブにすることができます。

ルールの非アクティブ化は 仮想 I/O サーバー (VIOS) インターフェースで行われるため、コマンドおよび処理に関する追加情報は、Power Systems ハードウェア・インフォメーション・センターの VIOS トピックの集合で入手可能です。

ルールを非アクティブにするには、以下のステップを実行します。

1. VIOS コマンド・ライン・インターフェースを開きます。
2. アクティブなすべてのフィルター・ルールを表示するには、以下のコマンドを入力します。

   ```
   lsvfilt -a
   ```

オブジェクト・データ・マネージャーに保管されているすべてのフィルター・ルールを表示する場合、**-a** フラグを省略することができます。

3. 非アクティブにするフィルター・ルールの識別番号をメモしてください。この例では、フィルター・ルールの識別番号は 23 です。
4. 以下のコマンドを入力して、フィルター・ルール 23 がカーネル内でアクティブである場合に、このルールを非アクティブにします。

   ```
   rmvfilt -n 23
   ```

   カーネル内のすべてのフィルター・ルールを非アクティブにするには、以下のコマンドを入力します。

   ```
   rmvfilt -n all
   ```

関連概念:

137 ページの『ルールの作成』
トラステッド・ファイアウォールの VLAN 間ルーティングを使用可能にするためのルールを作成することができます。

関連資料:

160 ページの『lsvfilt コマンド』

175 ページの『rmvfilt コマンド』

トラステッド・ロギング

PowerVM® のトラステッド・ロギングにより、AIX 論理区画 (LPAR) では、接続された 仮想 I/O サーバー (VIOS) に保管されているログ・ファイルへの書き込みを行うことができます。データはハイパーバイザーを使用して VIOS に直接送信され、クライアント LPAR と VIOS の間にネットワーク接続は必要ありません。

仮想ログ

仮想 I/O サーバー (VIOS) の管理者はログ・ファイルを作成して管理します。これらのファイルは、仮想ディスクまたは仮想光メディアと同様に /dev ディレクトリー内の仮想ログ・デバイスとして AIX オペレーティング・システムに提示されます。

ログ・ファイルを仮想ログとして保管すると、それらが生成されたクライアント LPAR で root 権限を持つユーザーがそれらのファイルを変更できないため、記録の信頼性のレベルが向上します。複数の仮想ログ・デバイスを同じクライアント LPAR に接続することができます。各ログは、/dev ディレクトリー内の別個のファイルになります。

トラステッド・ロギングにより、複数のクライアント LPAR のログ・データを VIOS からアクセス可能な単一のファイルシステムに統合できます。そのため、VIOS は、ログの分析およびアーカイブのためのシステム上の単一の場所を提供します。クライアント LPAR の管理者は、データを仮想ログ・デバイスに書き込むようにアプリケーションおよび AIX オペレーティング・システムを構成できます。これは、ローカル・ファイルにデータを書き込むのと似ています。監査記録を仮想ログに送信するように AIX 監査サブシステムを構成できます。syslog などのその他の AIX サービスは既存の構成と連動して、データを仮想ログに送信します。

仮想ログを構成するために、VIOS の管理者は、次の個別のコンポーネントで構成される、仮想ログの名前を指定する必要があります。

- クライアント名
- ログ名

これらの 2 つのコンポーネントの名前は、VIOS 管理者が任意の値に設定できます。ただし、クライアント名は、通常は特定の LPAR に接続されたすべての仮想ログで同じです (例えば、LPAR のホスト名)。ログ名は、ログの目的 (監査または syslog など) を識別するために使用されます。

AIX LPAR では、それぞれの仮想ログ・デバイスは /dev ファイルシステム内の 2 つの機能的に同等なファイルとして存在します。最初のファイルの名前にはデバイスの名前が使用され (例えば、/dev/vlog0)、2 番目のファイルには、vl プレフィックスをログ名およびデバイス番号と連結した名前が付けられます。例えば、仮想ログ・デバイス vlog0 のログ名が audit である場合、その仮想ログ・デバイスは、/dev ファイルシステム内で vlog0 および vlaudit0 の両方として存在します。

関連情報:

仮想ログの作成

仮想ログ・デバイスの検出

VIOS の管理者が仮想ログ・デバイスを作成してクライアント LPAR に接続した後、そのデバイスが認識されるには、クライアント LPAR のデバイス構成をリフレッシュする必要があります。

クライアント LPAR の管理者は、以下のいずれかの方法を使用して設定をリフレッシュします。

- クライアント LPAR のリブート
- **cfgmgr** コマンドの実行

lsdev コマンドを実行して、仮想ログ・デバイスを表示します。デバイスには、デフォルトで vlog のプレフィックスが付けられています。次に、2 つの仮想ログ・デバイスが存在する AIX LPAR での **lsdev** コマンド出力の例を示します。

```
lsdev
vlog0  Virtual Log Device
vlog1  Virtual Log Device
```

lsattr –El *<device name>* コマンドを使用して、個々の仮想ログ・デバイスのプロパティーを検査します。このコマンドにより、次のような出力が生成されます。

```
lsattr -El vlog0
PCM                     Path Control Module            False
client_name    dev-lpar-05 Client Name                   False
device_name    vlsyslog0   Device Name                   False
log_name       syslog      Log Name                      False
max_log_size   4194304     Maximum Size of Log Data File  False
max_state_size 2097152     Maximum Size of Log State File False
pvid           none        Physical Volume Identifier     False
```

この出力には、クライアント名、デバイス名、および VIOS が保管できるログ・データの量が表示されます。

仮想ログは、次の 2 つのタイプのログ・データを保管します。

- ログ・データ: AIX LPAR のアプリケーションによって生成された生のログ・データ。
- 状態データ: デバイスの構成、オープン、クローズ、およびログ・アクティビティーの分析に使用されるその他の操作の実行時に関する情報。

VIOS の管理者は、各仮想ログに保管できる**ログ・データ**および**状態データ**の量を指定します。これらの量は、max_log_size 属性および max_state_size 属性によって示されます。保管されているデータの量が指定の制限を超える場合、最も古いログ・データが上書きされます。VIOS の管理者は、ログを保存するためにログ・データの収集とアーカイブが頻繁に行われるようにする必要があります。

トラステッド・ロギングのインストール

コマンド・ライン・インターフェースまたは SMIT ツールを使用して、PowerSC トラステッド・ロギング・フィーチャーをインストールすることができます。

トラステッド・ロギングをインストールするための前提条件は、VIOS 2.2.1.0 以降、および IBM AIX 6 (テクノロジー・レベル 7 適用) または IBM AIX 7 (テクノロジー・レベル 1 適用) です。

トラステッド・ロギング・フィーチャーをインストールするためのファイル名は powerscStd.vlog で、これは PowerSC Standard Edition のインストール CD に含まれています。

トラステッド・ロギングの機能をインストールするには、次のようにします。

1. VIOS バージョン 2.2.1.0 以降を実行していることを確認します。
2. PowerSC インストール CD を挿入するか、インストール CD のイメージをダウンロードします。
3. **installp** コマンドまたは SMIT ツールを使用して、powerscStd.vlog ファイルセットをインストールします。

関連情報:

7 ページの『PowerSC Standard Edition 1.1.4 のインストール』
PowerSC Standard Edition の特定の機能ごとに、ファイルセットを 1 つインストールする必要があります。

トラステッド・ロギングの構成

AIX 監査サブシステムのトラステッド・ロギングおよび syslog を構成する手順について説明します。

AIX 監査サブシステムの構成

ローカル・ファイルシステムにログを書き込むほか、仮想ログ・デバイスにバイナリー・データを書き込むために、AIX 監査サブシステムを構成することができます。

注: AIX 監査サブシステムを構成する前に、142 ページの『仮想ログ・デバイスの検出』の手順を完了しておく必要があります。

AIX 監査サブシステムを構成するには、以下のステップを実行します。

1. バイナリー (auditbin) モードでデータをログに記録するように AIX 監査サブシステムを構成します。
2. /etc/security/audit/config 構成ファイルを編集して、AIX の監査のためにトラステッド・ロギングを活動化します。
3. bin: スタンザに virtual_log = /dev/vlog0 パラメーターを追加します。

   注: LPAR の管理者が auditbin データを /dev/vlog0 に書き込みたい場合、この指示は有効です。
4. 次の順序で AIX 監査サブシステムを再始動します。

```
audit shutdown
audit start
```

ローカル・ファイルシステムへのログの書き込みに加えて、監査レコードが、指定された仮想ログ・デバイスを介して 仮想 I/O サーバー (VIOS) に書き込まれます。ログは、/etc/security/audit/config 構成ファイルの bin: スタンザの既存の bin1 および bin2 パラメーターの制御下で保管されます。

関連情報:

監査サブシステム

syslog の構成

/etc/syslog.conf ファイルにルールを追加することによって、メッセージを仮想ログに書き込むように syslog を構成できます。

注: /etc/syslog.conf ファイルを構成する前に、142 ページの『仮想ログ・デバイスの検出』の手順を完了しておく必要があります。

/etc/syslog.conf ファイルを編集し、以下の基準に基づいてログ・メッセージを突き合わせることができます。

- 機能

- 優先順位レベル

syslog メッセージのために仮想ログを使用するには、目的のメッセージを /dev ディレクトリーの適切な仮想ログに書き込むルールを指定して /etc/syslog.conf ファイルを構成する必要があります。

例えば、何らかの機能によって生成されたデバッグ・レベル・メッセージを vlog0 仮想ログに送信するには、以下の行を /etc/syslog.conf ファイルに追加します。

```
*.debug /dev/vlog0
```

注: データを仮想ログに書き込むコマンドに対して、syslogd デーモンで使用可能なログのローテーション機能を使用しないでください。/dev ファイルシステム内のファイルは正規ファイルではなく、名前変更したり、移動したりすることはできません。 VIOS 管理者は、VIOS 内の仮想ログのローテーションを構成する必要があります。

構成の後、次のコマンドを使用して syslogd デーモンを再開する必要があります。

```
refresh -s syslogd
```

関連情報:

syslogd デーモン

仮想ログ・デバイスへのデータの書き込み

/dev ディレクトリーの適切なファイルを開き、そのファイルにデータを書き込むことによって、任意のデータが仮想ログ・デバイスに書き込まれます。仮想ログを開くことができるプロセスは一度に 1 つのみです。

例えば、次のように入力します。

echo コマンドを使用して仮想ログ・デバイスにメッセージを書き込むには、次のコマンドを入力します。

```
 echo "Log Message" > /dev/vlog0
```

cat コマンドを使用して仮想ログ・デバイスにファイルを保管するには、次のコマンドを入力します。

```
cat /etc/passwd > /dev/vlog0
```

個別の最大書き込みサイズは 32 KB に制限されており、さらに多くのデータを 1 回の書き込み操作で書き込もうとするプログラムは入出力 (EIO) エラーを受け取ります。**cat** コマンドなどのコマンド・ライン・インターフェース (CLI) ユーティリティーは自動的に転送を 32 KB の書き込み操作に分割します。

トラステッド・ネットワーク接続およびパッチ管理

トラステッド・ネットワーク接続 (TNC) は、エンドポイントの保全性を検証するための規格を規定する Trusted Computing Group (TCG) の一部を成しています。 TNC は、管理者がポリシーを適用してネットワーク・インフラストラクチャーへのアクセスを効果的に制御する上で役立つオープン・ソリューション・アーキテクチャーを定義しています。

トラステッド・ネットワーク接続の概念

トラステッド・ネットワーク接続 (TNC) のコンポーネント、セキュア通信の構成、およびパッチ管理システムについて説明します。

トラステッド・ネットワーク接続のコンポーネント

トラステッド・ネットワーク接続 (TNC) フレームワークのコンポーネントについて説明します。

TNC モデルは、以下のコンポーネントで構成されます。

トラステッド・ネットワーク接続サーバー

トラステッド・ネットワーク接続 (TNC) サーバーは、ネットワークに追加されたクライアントを識別して、それらに対する検証を開始します。

TNC クライアントは、検証のために必要なファイルセット・レベルの情報をサーバーに提供します。サーバーは、クライアントが管理者によって構成されたレベルであるかどうかを判別します。クライアントが準拠していない場合、TNC サーバーは、管理者に必要な修復処置について通知します。

TNC サーバーは、ネットワークへのアクセスを試行しているクライアントに対する検証を開始します。TNC サーバーは、クライアントから保全性計測値を要求して検証することができる一連の保全性計測ベリファイヤー (IMV) をロードします。AIX には、システムのファイルセットおよびセキュリティー・パッチ・レベルを検証するデフォルトの IMV があります。TNC サーバーは、複数の IMV モジュールをロードして管理するフレームワークです。クライアントを検証する際、クライアントからの情報を要求するために IMV を使用して、クライアントを検証します。

パッチ管理

トラステッド・ネットワーク接続 (TNC) サーバーは、SUMA と統合して、パッチ管理ソリューションを提供します。

AIX SUMA は、IBM ECC および Fix Central で入手可能な最新の Service Pack およびセキュリティー・フィックスをダウンロードします。TNC およびパッチ管理デーモンは、最新の更新済み情報を TNC サーバーにプッシュします。この情報は、クライアントを検証するための基本的なファイルセットとして機能します。

サービス更新管理アシスタント (SUMA) のダウンロードを管理して、ファイルセット情報を TNC サーバーにプッシュするには、**tncpmd** デーモンを構成する必要があります。更新を自動的にダウンロードできるようにするには、このデーモンが、インターネットに接続されたシステムでホストされている必要があります。TNC パッチ管理サーバーをインターネットに接続せずに使用する場合、ユーザー定義のフィックス・リポジトリーを TNC パッチ管理サーバーに登録することができます。

注: TNC サーバーおよび **tncpmd** デーモンを同じシステムでホストすることができます。

トラステッド・ネットワーク接続クライアント

トラステッド・ネットワーク接続 (TNC) クライアントは、検証のために TNC サーバーで必要となる情報を提供します。

サーバーは、クライアントが管理者によって構成されたレベルであるかどうかを判別します。クライアントが準拠していない場合、TNC サーバーは、管理者に必要な更新について通知します。

TNC クライアントは、始動時に IMC をロードし、IMC を使用して必要な情報を収集します。

トラステッド・ネットワーク接続の IP リファラー

トラステッド・ネットワーク接続 (TNC) サーバーは、ネットワークの一部であるクライアントに対する検証を自動的に開始できます。仮想 I/O サーバー (VIOS) パーティションで実行される IP リファラーは、VIOS によってサービス提供されている新規クライアントを検出して、それらの IP アドレスを TNC サーバーに送信します。TNC サーバーは、定義されているポリシーに関してクライアントを検証します。

トラステッド・ネットワーク接続のセキュア通信

トラステッド・ネットワーク接続 (TNC) デーモンは、トランスポート層セキュリティー (TLS) または Secure Sockets Layer (SSL) によって使用可能になる暗号化チャネルを介して通信します。

セキュア通信とは、ネットワークを行き来するデータとコマンドが確実に認証され、安全であるようにすることです。各システムには独自の鍵と証明書が必要です。これらは、コンポーネントに対する初期化コマンドが実行されるときに生成されます。このプロセスは管理者に対して完全に透過的であるため、管理者が介入する必要性が減ります。

新規クライアントを検証するには、そのクライアントの証明書をサーバーのデータベースにインポートする必要があります。最初に証明書には非トラステッドのマークが付けられます。管理者は **psconf** コマンドを使用して証明書を表示し、次のコマンドを入力してその証明書にトラステッドのマークを付けます。

```
psconf certadd –i<ip> -t<TRUSTED|UNTRUSTED>
```

別の鍵と証明書を使用するために、**psconf** コマンドは、証明書をインポートするオプションを提供します。

サーバーから証明書をインポートするには、次のコマンドを入力します。

```
psconf import  -S -k<key filename> -f<key filename>
```

クライアントから証明書をインポートするには、次のコマンドを入力します。

```
psconf import -C -k<key filename> -f<key filename>
```

トラステッド・ネットワーク接続プロトコル

トラステッド・ネットワーク接続 (TNC) プロトコルは、ネットワーク保全性を維持するために、TNC フレームワークと共に使用します。

TNC は、エンドポイントの保全性を検証するための規格を提供します。アクセスを要求するエンドポイントは、稼働環境に影響を与える可能性がある重要なコンポーネントの保全性計測に基づいて評価されます。TNC フレームワークにより、管理者はネットワーク内のシステムの保全性をモニターすることができます。TNC は AIX パッチ配布インフラストラクチャーと統合され、完全なパッチ管理ソリューションを構築します。

TNC の規格は、AIX および POWER® family システム体系の要件を満たす必要があります。 TNC のコンポーネントは、AIX オペレーティング・システムで完全なパッチ管理ソリューションを提供するように設計されています。この構成により、管理者は AIX デプロイメントのソフトウェア構成を効率的に管理することができます。システムのパッチ・レベルを検査して、準拠していないクライアントに関するレポートを生成するツールが用意されています。さらに、パッチ管理は、パッチをダウンロードしてインストールするプロセスを簡素化します。

IMC および IMV モジュール

トラステッド・ネットワーク接続 (TNC) サーバーまたはクライアントは、サーバーの検証のために保全性計測コレクター (IMC) モジュールおよび保全性計測ベリファイヤー (IMV) モジュールを内部的に使用します。

このフレームワークでは、複数の IMC および IMV モジュールをサーバーとクライアントにロードすることができます。オペレーティング・システム (OS) レベルおよびファイルセット・レベルの検証を実行するモジュールは、デフォルトで AIX オペレーティング・システムに付属しています。AIX オペレーティング・システムに付属のモジュールにアクセスするには、以下のいずれかのパスを使用します。

- `/usr/lib/security/tnc/libfileset_imc.a`: クライアント・システムからインストールされた OS レベルおよびファイルセットに関する情報を収集して、検証のために IMV (TNC サーバー) に送信します。
- `/usr/lib/security/tnc/libfileset_imv.a`: クライアントから OS レベルおよびファイルセット情報を要求して、それを基本的な情報と比較します。また、TNC サーバーのデータベースでクライアントの状況を更新します。状況を表示するには、以下のコマンドを入力します。

  ```
  psconf list -s<COMPLIANT|IGNORE|FAILED|ALL>-i<ip|ALL> [-c] [-q]
  ```

関連資料:

165 ページの『psconf コマンド』

トラステッド・ネットワーク接続のインストール

トラステッド・ネットワーク接続 (TNC) のコンポーネントをインストールするには、特定のステップを実行する必要があります。

TNC のコンポーネントを使用するためのセットアップを構成するには、以下のステップを実行します。

1. TNC サーバー、トラステッド・ネットワーク接続およびパッチ管理 (TNCPM) サーバー、および 仮想 I/O サーバー (VIOS) の TNC IP リファラーをセットアップするための、システムの IP アドレスを確認します。

   注: TNC サーバーを TNC クライアントとして構成することはできません。
2. ネットワーク・インストール管理 (NIM) サーバーをセットアップします。サーバーとして構成されるシステムは NIM マスターであり、`sets:bos.sysmgt.nim.master` ファイルセットがクライアント・システムにインストールされている必要があります。
3. TNCPM サーバーを構成します。この構成は、NIM システムでセットアップすることができます。TNCPM サーバーは、SUMA を使用して、IBM Fix Central および ECC Web サイトからパッチをダウンロードします。更新をダウンロードするには、システムはインターネットに接続されている必要があります。次のコマンドを入力して、TNCPM サーバーを構成します。

   ```
   pmconf mktncpm [pmport=<port>]tncserver=<host:port>
   ```

   例えば、次のように入力します。

   ```
   pmconf mktncpm pmport=20000 tncserver=1.1.1.1:10000
   ```

4. TNC サーバーでポリシーを構成します。クライアントを検証するためのポリシーを作成するには、 152 ページの『トラステッド・ネットワーク接続クライアントに関するポリシーの作成』を参照してください。
5. VIOS で TNC IP リファラーを構成します。VIOS 上のこの構成は、ネットワークに接続するクライアントに対する検証をトリガーします。次のコマンドを入力して、リファラーを構成します。

   ```
   psconf mkipref tncport=<port> tncserver=<ip:port>
   ```

   例えば、次のように入力します。

   ```
   psconf mkipref tncport=10000 tncserver=1.1.1.1:10000
   ```

   注: サーバー・ポートとクライアント・ポートの TNC ポートの値は同じでなければなりません。
6. 次のコマンドを使用して、クライアントを構成します。

   ```
   psconf mkclient tncport=<port> tncserver=<serverip>:<port>
   ```

   例えば、次のように入力します。

   ```
   psconf mkclient tncport=10000 tncserver=10.1.1.1:10000
   ```

関連資料:

165 ページの『psconf コマンド』

関連情報:

7 ページの『PowerSC Standard Edition 1.1.4 のインストール』
PowerSC Standard Edition の特定の機能ごとに、ファイルセットを 1 つインストールする必要があります。

NIM でのインストール

IBM Fix Central

パスポート・アドバンテージ・オンライン・ヘルプ・センター

トラステッド・ネットワーク接続およびパッチ管理の構成

トラステッド・ネットワーク接続 (TNC) を、パッチ管理デーモンとして構成する必要があります。 TNC サーバーは、SUMA と統合して包括的なパッチ管理ソリューションを提供します。

トラステッド・ネットワーク接続サーバーの構成

TNC サーバーを構成する手順について説明します。

TNC サーバーを構成するには、`/etc/tnccs.conf` ファイルに次のような値が入っている必要があります。

```
component = SERVER
```

システムをサーバーとして構成するには、次のコマンドを入力します。

```
psconf mkserver tncport=<port> pmserver=<ip|hostname[,ip2|hostname2..]:port>
[recheck_interval=<time in mins>]
```

例えば、次のように入力します。

```
psconf mkserver tncport=10000 pmserver=2.2.2.2:20000 recheck_interval=20
```

注: `tncport` ポートと `pmserver` ポートは、異なる値に設定する必要があります。`recheck_interval` パラメーターの値が指定されない場合、デフォルト値の 1440 分が使用されます。

tncport ポートに使用されるデフォルトのポート値は 42830 分で、pmserver ポートに使用されるデフォルト値は 38240 分です。

関連資料:

165 ページの『psconf コマンド』

トラステッド・ネットワーク接続クライアントの構成

トラステッド・ネットワーク接続 (TNC) クライアントを構成する手順と、セットアップに必要な構成設定について説明します。

TNC クライアントを構成するには、/etc/tnccs.conf ファイルに次のような値が入っている必要があります。

```
component = CLIENT
```

システムをクライアントとして構成するには、次のコマンドを入力します。

```
psconf mkclient tncport=<port> tncserver=<ip:port>
```

例えば、次のように入力します。

```
psconf mkclient tncport=10000 tncserver=1.1.1.1:10000
```

注: サーバー・ポートとクライアント・ポートの tncport の値は同じでなければなりません。

関連資料:

165 ページの『psconf コマンド』

パッチ管理サーバーの構成

システムをパッチ管理サーバーとして構成する手順について説明します。

TNC クライアントを更新できるように、トラステッド・ネットワーク接続 (TNC) パッチ管理サーバーをネットワーク・インストール管理 (NIM) サーバー上で構成する必要があります。

TNC パッチ管理のフィックス・リポジトリーを初期化するには、以下のコマンドを入力します。

```
pmconf init -i <download interval> -l <TL list> [-A] [-P <download path>][-x <ifix interval>]
[-K <ifix key>]
```

pmconf コマンドの例は、以下のとおりです。

```
pmconf init -i 1440 -l 6100-07,7100-01
```

init コマンドでは、各テクノロジー・レベルに対して最新の Service Pack がダウンロードされ、TNC サーバー用に使用可能にされます。更新済みの Service Pack によって、TNC サーバーが基本的な TNC クライアントの検証を実行できるようになり、TNC パッチ管理サーバーで TNC クライアントの更新をインストールできるようになります。クライアントの更新を実行する際に、すべてのご使用条件に同意するには、**-A** フラグを指定します。デフォルトでは、TNC パッチ管理サーバーがダウンロードするフィックス・リポジトリーは、/var/tnc/tncpm/fix_repository ファイル内です。別のディレクトリーを指定するには、**-P** フラグを使用します。

IBM セキュリティー・アドバイザリーおよび暫定修正の自動ダウンロードを可能にするには、暫定修正の間隔を指定します。この機能により、新規に公開されるセキュリティー暫定修正および関連する Common Vulnerabilities and Exposures (CVE) 識別子が自動的に通知されます。セキュリティー・アドバイザリーおよび暫定修正はすべて、TNC に登録される前に検査されます。暫定修正を自動的にダウンロードするため

に必須の IBM AIX ぜい弱性公開鍵は、IBM AIX セキュリティーの Web サイトで入手できます。Service Pack および暫定修正の自動ダウンロードは、ダウンロードの間隔と暫定修正の間隔の両方を 0 に設定することによって無効になります。

Service Pack および暫定修正の登録を手動で更新することもできます。IBM セキュリティー・アドバイザリーを対応する暫定修正とともに手動で登録するには、以下のコマンドを入力します。

```
pmconf add -y <advisory file> -v <signature file>  -e <ifix tar file>
```

スタンドアロン暫定修正を手動で登録するには、以下のコマンドを入力します。

```
pmconf add -p <SP> -e <ifix file>
```

新規のテクノロジー・レベルを登録し、その最新の Service Pack をダウンロードするには、以下のコマンドを入力します。

```
pmconf add -l <TL list>
```

最新ではないバージョンの Service Pack をダウンロードする場合、または検証およびクライアントの更新に使用するテクノロジー・レベルをダウンロードする場合は、以下のコマンドを入力します。

```
pmconf add -l <TL list> -d
pmconf add -s <SP List>
```

システム上に存在する Service Pack またはテクノロジー・レベルのフィックス・リポジトリーを登録するには、以下のコマンドを入力します。

```
pmconf add -s <SP> -p <user_defined_fix_repository>
pmconf add -l <TL> -p <user_defined_fix_repository>
```

システムがパッチ管理サーバーとして機能するように構成するには、次のコマンドを入力します。

```
pmconf mktncpm [pmport=<port>] tncserver=ip_list[:port]
```

このコマンドの例は、以下のとおりです。

```
pmconf mktncpm pmport=20000 tncserver=1.1.1.1:100000
```

TNC パッチ管理サーバーは、セキュリティーの Authorized Problem Analysis Reports (APAR) の管理を常にサポートします。その他のタイプの APAR を管理するように TNC パッチ管理を構成するには、以下のコマンドを入力します。

```
pmconf add -t <APAR_type_list>
```

直前の例の <APAR_type_list> は、以下のタイプの APAR を含むコンマ区切りリストです。

- HIPER
- PE
- 拡張

TNC パッチ管理サーバーは、Service Pack、テクノロジー・レベル、およびクライアント更新のダウンロードにおける **syslog** をサポートします。機能は `user` で、優先順位は `info` です。この例は `user.info` です。

また、TNC パッチ管理サーバーは、`/var/tnc/tncpm/log/update/<ip>/<timestamp>` ディレクトリーにあるすべてのクライアント更新と共にログも維持します。

関連資料:

165 ページの『psconf コマンド』

関連情報:

IBM AIX Security

トラステッド・ネットワーク接続サーバーの電子メール通知の構成

トラステッド・ネットワーク接続 (TNC) サーバーの電子メール通知を構成する手順について説明します。

TNC サーバーはクライアントのパッチ・レベルを表示します。TNC サーバーは、クライアントが準拠していないことを検出すると、結果と必要な修復処置を示す電子メールを管理者に送信します。

管理者の電子メール・アドレスを構成するには、次のコマンドを入力します。

```
psconf add –e <email_id>[ipgroup=[±]G1, G2 ..]
```

例えば、次のように入力します。

```
psconf add –e abc@ibm.com ipgroup=vayugrp1,vayugrp2
```

上記の例では、IP グループ *vayugrp1* および *vayugrp2* に関する電子メールが abc@ibm.com という電子メール・アドレスに送信されます。

電子メール・アドレスが割り当てられていない IP グループに関するメールをグローバル電子メール・アドレスに送信するには、次のコマンドを入力します。

```
psconf add –e <mailaddress>
```

例えば、次のように入力します。

```
psconf add –e abc@ibm.com
```

上記の例では、IP グループに電子メール・アドレスが割り当てられていない場合に、abc@ibm.com という電子メール・アドレスにメールが送信されます。これは、グローバル電子メール・アドレスとして機能します。

関連資料:

165 ページの『psconf コマンド』

VIOS での IP リファラーの構成

仮想 I/O サーバー (VIOS) で IP リファラーを構成して、検証を自動的に開始する方法を説明します。

注: IP リファラーを構成する前に、仮想入出力サーバー (VIOS) で SVM カーネル・エクステンションを構成する必要があります。

TNC IP リファラーを構成するには、`/etc/tnccs.conf` 構成ファイルに `component = IPREF` のような設定値がなければなりません。

次のコマンドを入力して、システムをクライアントとして構成することができます。

```
psconf mkipref tncport=<port> tncserver=<ip:port>
```

例えば、次のように入力します。

```
psconf mkipref tncport=10000 tncserver=1.1.1.1:10000
```

`tncserver` ポートと、クライアント・ポートの `tncport` の値は同じでなければなりません。

関連資料:

165 ページの『psconf コマンド』

トラステッド・ネットワーク接続およびパッチ管理の管理

トラステッド・ネットワーク接続 (TNC) を管理して、クライアント、ポリシー、ログ、検証結果の追加、クライアントおよび TNC に関連した証明書の更新といったタスクを実装します。

トラステッド・ネットワーク接続サーバーのログの表示

トラステッド・ネットワーク接続 (TNC) サーバーのログを表示する方法を説明します。

TNC サーバーは、すべてのクライアントの検証結果をログに記録します。ログを表示するには、**psconf** コマンドを実行します。

```
psconf list –H –i <ip |ALL>
```

関連資料:

165 ページの『psconf コマンド』

トラステッド・ネットワーク接続クライアントに関するポリシーの作成

トラステッド・ネットワーク接続 (TNC) クライアントに関連するポリシーをセットアップする方法を説明します。

psconf コンソールは、TNC ポリシーを管理するために必要なインターフェースを備えています。各クライアントまたはクライアント・グループをポリシーに関連付けることができます。

以下のポリシーを作成できます。

- インターネット・プロトコル (IP) グループには複数のクライアント IP アドレスが含まれます。
- 各クライアント IP は、1 つのグループのみに所属できます。
- IP グループはポリシー・グループに関連付けられます。
- ポリシー・グループには、さまざまな種類のポリシーが含まれます。例えば、クライアントに必要なオペレーティング・システム・レベル (リリース、テクノロジー・レベル、および Service Pack) を指定するファイルセット・ポリシーがあります。ポリシー・グループには複数のファイルセット・ポリシーが含まれる場合があり、このポリシーを参照するクライアントは、いずれかのファイルセット・ポリシーで指定されているレベルでなければなりません。

以下のコマンドは、IP グループ、ポリシー・グループ、およびファイルセット・ポリシーの作成方法を示しています。

IP グループを作成するには、次のコマンドを入力します。

```
psconf add –G <ipgrpname> ip=[±]<ip1,ip2,ip3 ...>
```

例えば、次のように入力します。

```
psconf add –G myipgrp ip=1.1.1.1,2.2.2.2
```

注: グループの場合、少なくとも 1 つの IP を指定する必要があります。複数の IP はコンマで区切る必要があります。

ファイルセット・ポリシーを作成するには、次のコマンドを入力します。

```
psconf add –F <fspolicyname> <rel00-TL-SP>
```

例えば、次のように入力します。

```
psconf add –F myfspol  6100-02-03 aparlist=IY0001,IY0002
```

注: ビルド情報は、<rel00-TL-sp> の形式でなければなりません。

ポリシーを作成して IP グループを割り当てるには、次のコマンドを入力します。

```
psconf add –P <policyname> ipgroup=[±] <ipgrp1, ipgrp2 ...]
```

例えば、次のように入力します。

```
psconf add –P mypol ipgroup=myipgrp,myipgrp1
```

ファイルセット・ポリシーをポリシーに割り当てるには、次のコマンドを入力します。

```
psconf add –P <policyname> fspolicy=[±]<fspol1, fspol2 ...>
```

例えば、次のように入力します。

```
psconf add –P mypol fspolicy=myfspol,myfspol1
```

注: 複数のファイルセット・ポリシーが指定される場合、システムは、クライアントに一致する最適なポリシーを適用します。例えば、クライアントが 6100-02-01 にあり、ファイルセット・ポリシー 7100-03-04 および 6100-02-03 を指定する場合、このクライアントには 6100-02-03 が適用されます。

関連資料:

165 ページの『psconf コマンド』

トラステッド・ネットワーク接続クライアントの検証の開始

トラステッド・ネットワーク接続 (TNC) クライアントを検証する方法を説明します。

クライアント検証のために以下のいずれかの方法を使用します。

- 仮想 I/O サーバー (VIOS) の IP リファラー・デーモンが、クライアント IP を TNC サーバーに転送します。クライアント LPAR は、IP を取得してネットワークへのアクセスを試行します。VIOS の IP リファラー・デーモンは、新しい IP アドレスを検出して、それを TNC サーバーに転送します。TNC サーバーは新しい IP アドレスを受信するとすぐに、検証を開始します。
- TNC サーバーが、定期的にクライアントを検証します。管理者は、検証されるクライアント IP を TNC ポリシー・データベースに追加することができます。 TNC サーバーは、データベース内のクライアントを検証します。再検証は、/etc/tnccs.conf 構成ファイルで指定されている recheck_interval 属性値を参照して定期的な間隔で自動的に行われます。
- 管理者が、クライアント検証を手動で開始します。管理者は、次のコマンドを実行することにより、検証を手動で開始して、クライアントがネットワークに追加されたかどうかを検証できます。

  ```
  tncconsole verify -i <ip>
  ```

注: VIOS に接続されないリソースの場合、クライアントが手動で TNC サーバーに追加されると、検証および更新することができます。

関連資料:

165 ページの『psconf コマンド』

トラステッド・ネットワーク接続の検証結果の表示

トラステッド・ネットワーク接続 (TNC) クライアントの検証結果を表示する手順について説明します。

ネットワーク内のクライアントの検証結果を表示するには、次のコマンドを入力します。

```
psconf list -s ALL -i ALL
```

このコマンドにより、**IGNORED**、**COMPLIANT**、または **FAILED** 状況のすべてのクライアントが表示されます。

- **IGNORED**: クライアント IP は IP リストで無視されます (つまり、クライアントの検証を免除できます)。
- **COMPLIANT**: クライアントは検証に合格しました (つまり、クライアントはポリシーに準拠しています)。
- **FAILED**: クライアントの検証は失敗しました (つまり、クライアントはポリシーに準拠しておらず、管理アクションが必要です)。

失敗の理由を判別するには、次のように、失敗したクライアント IP を指定して **psconf** コマンドを実行します。

```
psconf list -s ALL -i <ip>
```

関連資料:

165 ページの『psconf コマンド』

トラステッド・ネットワーク接続クライアントの更新

トラステッド・ネットワーク接続 (TNC) サーバーは、クライアントを検証し、クライアントの状況と検証結果を使用してデータベースを更新します。管理者は、結果を表示し、クライアントを更新するためのアクションを実行できます。

旧レベルのクライアントを更新するには、次のコマンドを入力します。

```
psconf update -i <ip> -r <buildinfo> [-a apar1,apar2...]
```

例えば、次のように入力します。

```
psconf update –i 4.4.4.4 –r 6100-02-03 –a IY0004
```

psconf コマンドは、未インストールのビルドおよび APAR をインストールしてクライアントを更新します。

関連資料:

165 ページの『psconf コマンド』

パッチ管理ポリシーの管理

パッチ管理ポリシーを構成するために、**pmconf** コマンドが使用されます。

パッチ管理ポリシーは、TNC サーバーの IP アドレスや SUMA 更新を開始する時間間隔などの情報を提供します。

パッチ管理ポリシーを管理するには、次のコマンドを入力します。

```
pmconf mktncpm [pmport=<port>] tncserver=<host:port>
```

例えば、次のように入力します。

```
pmconf mktncpm pmport=2000 tncserver=10.1.1.1:1000
```

注: `pmport` と `tncserver` は、異なるポートでなければなりません。

関連資料:

161 ページの『pmconf コマンド』

トラステッド・ネットワーク接続の証明書のインポート

証明書をインポートして、ネットワークでデータを安全に送信する手順について説明します。

トラステッド・ネットワーク接続 (TNC) デーモンは、トランスポート層セキュリティー (TLS) または Secure Sockets Layer (SSL) プロトコルによって使用可能になる暗号化チャネルを介して通信します。このデーモンは、ネットワーク上を移送されるデータとコマンドが確実に認証され、安全であるようにします。各システムには独自の鍵と証明書があります。これらは、コンポーネントに対する初期化コマンドが実行されるときに生成されます。このプロセスは管理者に対して透過的であるため、管理者が介入する必要性が減ります。クライアントが初めて検証されるとき、その証明書がサーバーのデータベースにインポートされます。最初に証明書には非トラステッドのマークが付けられます。管理者は **psconf** コマンドを使用して証明書を表示し、次のコマンドを入力してその証明書にトラステッドのマークを付けます。

```
psconf certadd –i <ip> -t <TRUSTED|UNTRUSTED>
```

管理者が別の鍵と証明書を使用する必要がある場合、**psconf** コマンドは、その鍵と証明書をインポートするための機能を提供します。

サーバーから証明書をインポートするには、次のコマンドを入力します。

```
psconf import  -S -k <key filename> -f <filename>
```

クライアントから証明書をインポートするには、次のコマンドを入力します。

```
psconf import -C -k <key filename> -f <filename>
```

関連資料:

165 ページの『psconf コマンド』

TNC サーバーのレポート作成

トラステッド・ネットワーク接続 (TNC) サーバーは、その Common Vulnerabilities and Exposures (CVE)、IBM セキュリティー・アドバイザリー、TNC サーバー・ポリシー、TNC クライアント・セキュリティー・フィックス、登録済みサービス・パックおよび暫定修正のレポート作成に、コンマ区切り値 (CSV) 形式とテキスト出力形式の両方をサポートします。

CVE レポートには、登録済みサービス・パックに共通する機密漏れの危険性およびぜい弱性がすべて表示されます。このレポートの結果を表示するには、以下のコマンドを入力します。

```
psconf report -v {CVEid|ALL} -o {TEXT|CSV}
```

IBM セキュリティー・アドバイザリー・レポートには、インストールされた IBM ソフトウェアの、セキュリティーに関する既知のぜい弱性が表示されます。このレポートの結果を表示するには、以下のコマンドを入力します。

```
psconf report -A <advisoryname>
```

TNC サーバー・ポリシー・レポートには、TNC サーバー上で実行されるセキュリティー・ポリシーが表示されます。このレポートの結果を表示するには、以下のコマンドを入力します。

```
psconf report -P {policyname|ALL} -o {TEXT|CSV}
```

TNC クライアント・フィックス・レポートには、TNC クライアントのインストール済みまたは欠落した暫定修正が表示されます。このレポートの結果を表示するには、以下のコマンドを入力します。

```
psconf report -i {ip|ALL} -o {TEXT|CSV}
```

また、登録済みサービス・パックと、関連するプログラム診断依頼書 (APAR) および暫定修正のリストを生成するレポートを実行することもできます。このレポートの結果を表示するには、以下のコマンドを入力します。

```
psconf report -B {buildinfo|ALL} -o {TEXT|CSV}
```

関連資料:

165 ページの『psconf コマンド』

トラステッド・ネットワーク接続およびパッチ管理のトラブルシューティング

障害の考えられる原因と、TNC およびパッチ管理システムのトラブルシューティングを行う手順について説明します。

TNC およびパッチ管理システムのトラブルシューティングを行うには、次の表にリストされている構成設定を検査します。

表 14. TNC およびパッチ管理システムの構成設定のトラブルシューティング

問題	解決方法
TNC サーバーが始動しないか、応答しない	以下の手順を実行します。 1. 次のコマンドを入力して、TNC サーバー・デーモンが実行されているかどうかを判別します。 `ps -eaf | grep tnccsd` 2. 実行されていない場合は、`/var/tnc/.tncsock` ファイルを削除します。 3. サーバーを再始動します。 問題が解決されない場合には、TNC サーバーの `/etc/tnccs.conf` 構成ファイルで `component = SERVER` エントリーがあるか確認します。
TNC パッチ管理サーバーが始動しないか、応答しない	• 次のコマンドを入力して、TNC パッチ管理サーバー・デーモンが実行されているかどうかを判別します。 `ps –eaf | grep tncpmd` • TNC パッチ管理サーバーの `/etc/tnccs.conf` 構成ファイルで `component = TNCPM` エントリーがあるか確認します。
TNC クライアントが始動しないか、応答しない	• 次のコマンドを入力して、TNC クライアント・デーモンが実行されているかどうかを判別します。 `ps -eaf | grep tnccsd` • TNC クライアントの `/etc/tnccs.conf` 構成ファイルで `component = CLIENT` エントリーがあるか確認します。
TNC IP リファラーが 仮想 I/O サーバー (VIOS) で実行されていない	• 次のコマンドを入力して、TNC IP リファラー・デーモンが実行されているかどうかを判別します。 `ps -eaf | grep tnccsd` • VIOS の `/etc/tnccs.conf` 構成ファイルで `component = IPREF` エントリーがあるか確認します。
システムを TNC サーバーとクライアントの両方として構成できない	TNC サーバーとクライアントは同じシステム上で同時に稼働することはできません。
デーモンは実行されているが、検証が行われない	デーモンに対してログ・メッセージを有効にします。`/etc/tnccs.conf` ファイルで `level=info` ログを設定します。ログ・メッセージを分析することができます。

PowerSC Standard Edition コマンド入力

PowerSC Standard Edition は、コマンド・ラインを使用して、トラステッド・ファイアウォールのコンポーネントおよびトラステッド・ネットワーク接続のコンポーネントとの通信を可能にするコマンドを提供します。

chvfilt コマンド

目的

既存の仮想 LAN 間のフィルター規則の値を変更します。

構文

chvfilt [**-v <4|6>**] **-n fid** [**-a <D|P>**] [**-z <svlan>**] [**-Z <dvlan>**] [**-s <s_addr>**] [**-d <d_addr>**] [**-o <src_port_op>**] [**-p <src_port>**] [**-O <dst_port_op>**] [**-P <dst_port>**] [**-c <protocol>**]

説明

chvfilt コマンドは、仮想 LAN 間のフィルター規則 (フィルター規則テーブルにある) の定義を変更するのに使用します。

フラグ

-a アクションを指定します。有効な値は次のとおりです。
- D (拒否): トラフィックをブロックします。
- P (許可): トラフィックを許可します。

-c フィルター規則を適用できるさまざまなプロトコルを指定します。有効な値は次のとおりです。
- udp
- icmp
- icmpv6
- tcp
- any

-d 宛先アドレスを、IPv4 または IPv6 形式で指定します。

-m 送信元のアドレス・マスクを指定します。

-M 宛先のアドレス・マスクを指定します。

-n 変更する必要のあるフィルター規則のフィルター ID を指定します。

-o 送信元ポートまたは Internet Control Message Protocol (ICMP) タイプの操作を指定します。有効な値は次のとおりです。
- lt
- gt
- eq
- any

-O 宛先ポートまたは ICMP コード操作を指定します。有効な値は次のとおりです。

- lt
- gt
- eq
- any

-p 送信元ポートまたは ICMP タイプを指定します。

-P 宛先ポートまたは ICMP コードを指定します。

-s 送信元アドレスを、v4 または v6 形式で指定します。

-v フィルター規則テーブルの IP バージョンを指定します。有効な値は 4 と 6 です。

-z 送信元のロジカル・パーティションの仮想 LAN ID を指定します。

-Z 宛先のロジカル・パーティションの仮想 LAN ID を指定します。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. カーネルに存在する有効なフィルター規則を変更する場合は、次のコマンドを入力します。

   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

2. フィルター規則 (n=2) がカーネルに存在しない場合、出力は以下のようになります。

   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   システムは次の出力を表示します。

   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   Cannot Change the filter rule.
   ```

---

genvfilt コマンド

目的

同一の IBM Power Systems サーバー上のロジカル・パーティションの間にある仮想 LAN (VLAN) のフィルター規則を追加します。

構文

genvfilt -v <4|6> -a <D|P> -z <svlan> -Z <dvlan> [**-s <s_addr>**] [**-d <d_addr>**] [**-o <src_port_op>**] [**-p <src_port>**] [**-O <dst_port_op>**] [**-P <dst_port>**] [**-c <protocol>**]

説明

genvfiltコマンドは、同一の IBM Power Systems サーバー上のロジカル・パーティションの間にある仮想 LAN (VLAN) のフィルター規則を追加するのに使用します。

フラグ

-a アクションを指定します。有効な値は次のとおりです。

- D (拒否): トラフィックをブロックします。
- P (許可): トラフィックを許可します。

-c フィルター規則を適用できるさまざまなプロトコルを指定します。有効な値は次のとおりです。

- udp
- icmp
- icmpv6
- tcp
- any

-d 宛先アドレスを、v4 または v6 形式で指定します。

-m 送信元のアドレス・マスクを指定します。

-M 宛先のアドレス・マスクを指定します。

-o 送信元ポートまたは Internet Control Message Protocol (ICMP) タイプの操作を指定します。有効な値は次のとおりです。

- lt
- gt
- eq
- any

-O 宛先ポートまたは ICMP コード操作を指定します。有効な値は次のとおりです。

- lt
- gt
- eq
- any

-p 送信元ポートまたは ICMP タイプを指定します。

-P 宛先ポートまたは ICMP コードを指定します。

-s 送信元アドレスを、IPv4 または IPv6 形式で指定します。

-v フィルター規則テーブルの IP バージョンを指定します。有効な値は 4 と 6 です。

-z 送信元の LPAR の仮想 LAN ID を指定します。仮想 LAN ID は、1 から 4096 の範囲の値でなければなりません。

-Z 宛先の LPAR の仮想 LAN ID を指定します。仮想 LAN ID は、1 から 4096 の範囲の値でなければなりません。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. 送信元 VLAN ID 100 から、特定のポート上の宛先 VLAN ID 200 への TCP データを許可するフィルター規則を追加する場合は、次のコマンドを入力します。

```
genvfilt -v4 -a P -z 100 -Z 200  -o lt -p 345 -O lt -P 345 -c tcp
```

関連資料:

『mkvfilt コマンド』

176 ページの『vlantfw コマンド』

---

lsvfilt コマンド

目的

仮想 LAN 間のフィルター規則を、フィルター・テーブルからリストします。

構文

lsvfilt [**-a**]

説明

lsvfilt コマンドは、仮想 LAN 間のフィルター規則およびその状況をリストするのに使用されます。

フラグ

-a アクティブなフィルター規則のみをリストします。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. カーネル内のアクティブなフィルター規則をすべてリストするには、次のコマンドを入力します。

```
lsvfilt -a
```

関連概念:

138 ページの『ルールの非アクティブ化』

トラステッド・ファイアウォール・フィーチャーで、VLAN 間ルーティングを使用可能にするルールを非アクティブにすることができます。

---

mkvfilt コマンド

目的

genvfilt コマンドで定義した、仮想 LAN 間のフィルター規則をアクティブにします。

構文

mkvfilt -u

説明

mkvfilt コマンドは、**genvfilt** コマンドで定義した、仮想 LAN 間のフィルター規則をアクティブにします。

フラグ

-u フィルター・ルール・テーブル内のフィルター・ルールを活動化します。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. カーネル内のフィルター規則をアクティブにするには、次のコマンドを入力します。

```
mkvfilt -u
```

関連資料:

158 ページの『genvfilt コマンド』

---

pmconf コマンド

目的

最新フィックスを適用するためのテクノロジー・レベルと TNC サーバーを登録し、TNCPM 状況に関するレポートを生成することにより、トラステッド・ネットワーク接続パッチ管理 (TNCPM) サーバーのレポート作成と管理を行います。

注: サービス・パック・メタデータのダウンロードを可能にするために、TNCPM サーバーは 7100-02 テクノロジー・レベルの AIX バージョン 7.1 上でのみ実行する必要があります。

構文

pmconf mktncpm [**pmport=**<*port*>] **tncserver=***ip* | hostname **:** *port*

pmconf rmtncpm

pmconf start

pmconf stop

pmconf init -i <*download interval*> **-l** <*TL List*> **-A** [**-P** <*download path*>] [**-x** <*ifix interval*>] [**-K** <*ifix key*>]

pmconf add -l *TL_list*

pmconf add -p <*SP List*> [**-U** <*user-defined SP path*>]

pmconf add -p <*SP*> **-e** <*ifix file*>

pmconf add -y <*advisory file*> **-v** <*signature file*> **-e** <*ifix tar file*>

pmconf delete -l *TL_list*

pmconf delete -p <*SP List*>

pmconf delete -p <*SP*>**-e** *ifix file*

pmconf list -s [**-c**] [**-q**]

pmconf list -l *SP*

pmconf list -C

pmconf list -a *SP*

pmconf hist -u

pmconf hist -d

pmconf import -f *cert_filename* **-k** *key_filename*

pmconf export -f *filename*

pmconf modify -i < *download interval*>

pmconf modify -P <*download path*>

pmconf modify -g <*yes or no to accept all licenses*>

pmconf modify -t <*APAR type list*>

pmconf modify -x <*ifix interval*>

pmconf modify -K <*ifix key*>

pmconf delete -l <*TL list*>

pmconf restart

pmconf status

pmconf log loglevel = info | error | none

pmconf chtncpm attribute = *value*

説明

pmconf コマンドの機能は次のとおりです。

フィックス・リポジトリー管理
テクノロジー・レベルの登録または登録抹消、TNC サーバーの登録抹消を行います。 TNCPM は、テクノロジー・レベルごとに、そのテクノロジー・レベルの最新フィックス、**lslpp** 情報 (例えば、インストールされているファイルセットや、ファイルセットの更新に関する情報)、およびセキュリティー・フィックス情報を含むフィックス・リポジトリーを作成します。

レポート作成
TNCPM の状況に関するレポートを生成します。

pmconf コマンドを使用して、次の操作を実行できます。

項目	説明
追加	TNCPM を使用して新しいテクノロジー・レベルを登録します。
chtncpm	tnccs.conf ファイルの属性を変更します。 TNCPM サーバーで変更を有効にするには、明示的 **start** コマンドが必要です。
delete	TNCPM を使用してテクノロジー・レベルを登録抹消します。
history	更新およびダウンロードのヒストリーを表示します。
list	TNCPM に関する情報を表示します。
log	TNC コンポーネントのログ・レベルを設定します。
mktncpm	TNCPM サーバーを作成します。
modify	tncpm.conf 属性を変更します。
rmtncpm	TNCPM サーバーを除去します。
start	TNCPM サーバーを始動します。
stop	TNCPM サーバーを停止します。

フラグ

項目	説明
-A	クライアントの更新を実行するときにすべてのご使用条件を受け入れます。
-a <advisory file>	**ifix** パラメーターに対応する勧告ファイルを指定します。勧告ファイルが提供されていない場合、**ifix** パラメーターは暫定修正の Common Vulnerabilities and Exposures (CVE) アドレスとして表示されません。
-e <ifix file>	TNCPM に追加された暫定修正を指定します。
-i *download_interval*	登録済みテクノロジー・レベル用の新しいサービス・パックがあるかどうか TNCPM が検査する間隔を指定します。この間隔は、分数を表す整数値、または「**d** (日数): **h** (時間数): **m** (分数)」の形式を表します。*download_interval* のサポートされる範囲は 30 分から 525600 分までです。
-K <ifix key>	ダウンロードされた勧告および暫定修正の認証に使用する IBM AIX Product Security Incident Response Tool (PSIRT) の公開鍵を指定します。この公開鍵は、**0x28BFAA12** ID を使用して PGP 公開鍵サーバーからダウンロードすることができます。
-p *SP_list*	ダウンロードするサービス・パックのリストを指定します。このリストは、REL00-TL-SP の形式のコンマ区切りリストです (例えば、`6100-01-04` はテクノロジー・レベル 01 およびバージョン 6.1 のサービス・パック 04 を表しています)。 -U フラグを使用する場合は、SP を 1 つだけ指定します。
-t *APAR_type_list*	TNCPM がクライアント更新および TNC サーバー・リスト作成のためにサポートする、APAR タイプを指定します。セキュリティー APAR は常にサポートされます。APAR_type_list は、HIPER、FileNet® Process Engine、Enhancement の各タイプのコンマで区切られたリストです。
-P *fix_repository_path*	TNCPM によってダウンロードされるフィックス・リポジトリー用のダウンロード・ディレクトリーを指定します。デフォルトのディレクトリーは **/var/tnc/tncpm/fix_repository** です。
-U *user_defined_fix_repository*	ユーザー定義のフィックス・リポジトリーへのパスを指定します。クライアントの検証および更新に使用されるフィックス・リポジトリーに関連付けられているリリース、テクノロジー・レベル、およびサービス・パックを指定します。
-s	登録済みサービス・パックのレポートを生成します。
-l *SP*	サービス・パックに関する **lslpp** 情報のレポートを生成します。 *SP* の形式は REL00-TL-SP です (例えば、`6100-01-04` はテクノロジー・レベル 01 およびバージョン 6.1 のサービス・パック 04 を表しています)。
-u	クライアント更新ヒストリーのレポートを生成します。
-d	サービス・パックのダウンロード・ヒストリーのレポートを生成します。
-C	サーバー証明書のレポートを生成します。
-a *SP*	サービス・パックのセキュリティーに関するプログラム診断依頼書 (APAR) 情報のレポートを生成します。*SP* の形式は REL00-TL-SP です (例えば、`6100-01-04` はテクノロジー・レベル 01 およびバージョン 6.1 のサービス・パック 04 を表しています)。
-f *filename*	証明書ファイル名を指定します。
-k *key_filename*	インポート操作の場合は、証明書鍵を読み取る元のファイルを指定します。

-c	以下のように、コロン区切りレコードでユーザー属性を表示します。
	`# name: attribute1: attribute2: ...`
	`policy: value1: value2: ...`

-v <*signature file*>	IBM AIX ぜい弱性勧告の署名ファイルを指定します。
-y <*advisory file*>	IBM AIX ぜい弱性勧告ファイルを指定します。
-q	ヘッダー情報を抑止します。
-x <*ifix interval*>	新しい暫定修正がないか検査してダウンロードする間隔を分単位で指定します。この値が 0 に設定されている場合、暫定修正の自動ダウンロードおよび通知は使用不可になっています。デフォルトの間隔は、24 時間ごとです。<*ifix interval*> のサポートされる範囲は 30 分から 525600 分までです。

終了状況

このコマンドは、以下の終了値を戻します。

項目	説明
0	コマンドが正常に実行され、要求された変更がすべて行われました。
>0	エラーが発生しました。出力されるエラー・メッセージに、障害のタイプに関する詳細情報が示されます。

例

1. TNCPM を初期化するには、以下のコマンドを入力します。

   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```

2. TNCPM デーモンを作成するには、以下のコマンドを入力します。

   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```

3. サーバーを始動するには、以下のコマンドを入力します。

   ```
   pmconf start
   ```

4. サーバーを停止するには、以下のコマンドを入力します。

   ```
   pmconf stop
   ```

5. TNCPM を使用して新しいテクノロジー・レベルを登録するには、以下のコマンドを入力します。

   ```
   pmconf add -l 6100-01
   ```

6. TNCPM からテクノロジー・レベルを登録抹消するには、以下のコマンドを入力します。

   ```
   pmconf delete -l 6100-01
   ```

7. IP アドレス 11.11.11.11 を持つ TNC サーバーを TNCPM から登録抹消するには、以下のコマンドを入力します。

   ```
   pmconf delete -t 11.11.11.11
   ```

8. 以前のサービス・パックの新バージョンを TNCPM に登録するには、以下のコマンドを入力します。

   ```
   pmconf add -s 6100-01-04
   ```

9. TNCPM から以前のサービス・パックを登録抹消するには、以下のコマンドを入力します。

   ```
   pmconf delete -s 6100-01-04
   ```

10. 登録済みテクノロジー・レベルごとのフィックス・リポジトリーのレポートを生成するには、以下のコマンドを入力します。

    ```
    pmconf list -s
    ```

11. 登録済みテクノロジー・レベルの **lslpp** 情報のレポートを生成するには、以下のコマンドを入力します。

    ```
    pmconf list -l 6100-01-02
    ```

12. 更新ヒストリーからレポートを生成するには、以下のコマンドを入力します。

    ```
    pmconf hist -u
    ```

13. ダウンロード・ヒストリーからレポートを生成するには、以下のコマンドを入力します。

    ```
    pmconf hist -d
    ```

14. サーバー証明書のレポートを生成するには、以下のコマンドを入力します。

    ```
    pmconf list -C
    ```

15. サービス・パック・セキュリティー APAR 情報のレポートを生成するには、以下のコマンドを入力します。

```
pmconf list -a 6100-01-02
```

16. サーバー証明書をインポートするには、以下のコマンドを入力します。

```
pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
```

17. サーバー証明書をエクスポートするには、以下のコマンドを入力します。

```
pmconf export -f /tmp/server.txt
```

---

psconf コマンド

目的

トラステッド・ネットワーク接続 (TNC) サーバー、TNC クライアント、TNC IP Referrer (IPRef)、および Service Update Management Assistant (SUMA) のレポート作成と管理を行います。このコマンドは、ネットワークを脅威やアタックから保護するために、ネットワークの接続時または接続後のエンドポイント (サーバーおよびクライアント) の保全性に関するファイルセット管理ポリシーおよびパッチ管理ポリシーを管理します。

構文

TNC サーバーの操作:

| **psconf mkserver** [**tncport=**<*port*>] **pmserver=**<*host*:*port*> [tsserver=<host>] [
| **recheck_interval=**<*time_in_minutes*> | **d** (days) : **h** (hours) : **m** (minutes)] [**dbpath** = <*user-defined
| *directory*>] [**default_policy=**<*yes* | *no* >] [**clientData_interval=**<*time in mins* > | **d** (days) : **h** (hours) : **m**
| (minutes)] [**clientDataPath=**<*Full_path* >]

psconf { **rmserver** | **status** }

psconf { **start** | **stop** | **restart** } **server**

psconf chserver attribute = *value*

| **psconf clientData -i** *host* **[-l | -g]**

psconf add -F <*FSPolicyname*> -r <*buildinfo*> [**apargrp=** [±]<*apargrp1, apargrp2..* >] [*ifixgrp*=[+|-]<*ifixgrp1*,*ifixgrp2...*>]

psconf add { **-G** <*ipgroupname*> **ip=**[±]<*host1, host2...*> | {**-A**<*apargrp*> [**aparlist=**[±]*apar1, apar2...* | {**-V** <*ifixgrp*> [*ifixlist*=[+|-]*ifix1*,*ifix2...*]}

psconf add -P <*policyname*> { **fspolicy=**[±]<*f1,f2...*> | **ipgroup=**[±]<*g1,g2...*> }

psconf add -e *emailid* [-E FAIL | COMPLIANT | ALL] [**ipgroup=** [±]<*g1,g2...*>]

psconf add -I ip= [±]<*host1, host2...*>

psconf delete { **-F** <*FSPolicyname*> | **-G** <*ipgroupname*> | **-P** <*policyname*> | **-A** <*apargrp*> | **-V** <*ifixgrp*>}

psconf delete -H -i <*host* | **ALL**> **-D** <*yyyy-mm-dd*>

psconf certadd -i <*host*> **-t** <**TRUSTED** | **UNTRUSTED**>

psconf certdel -i <*host*>

psconf verify -i <*host*> | **-G** <*ipgroup*>

psconf update [-p] {-i< *host* >| **-G** <*ipgroup*> [**-r** <*buildinfo*> | **-a** <*apar1, apar2...*> | [**-u**] **-v** <*ifix1, ifix2,...*>}

psconf log loglevel=<info | error | none>

psconf import -C -i <*host*> **-f** <*filename*> | **–d** <*import database filename*>

psconf { **import -k** <*key_filename*> | **export**} **-S -f** <*filename*>

psconf list { **-S** | **-G** < *ipgroupname* | **ALL** > | **-F** < *FSPolicyname* | **ALL** > | **-P** < *policyname* | **ALL** > | **-r** < *buildinfo* | **ALL** > | **-I -i** < *ip* | **ALL** > | **-A** < *apargrp* | **ALL** > | **-V** <*ifixgrp*>} [**-c**] [**-q**]

psconf list { **-H** | **-s** <**COMPLIANT** | **IGNORE** | **FAILED** | **ALL**> } **-i** <*host* | **ALL**> [**-c**] [**-q**]

psconf export -d <*path to export directory*>

psconf report -v <CVEid|ALL> -o <TEXT|CSV>

psconf report -A <advisoryname>

psconf report -P <policyname|ALL> -o <TEXT|CSV>

psconf report -i <ip|ALL> -o <TEXT|CSV>

psconf report -B <buildinfo|ALL> -o <TEXT|CSV>

TNC クライアントの操作:

psconf mkclient [**tncport=**<*port*>] **tncserver=**<*host:port*>

psconf mkclient tncport=<*port*> -T

psconf { **rmclient** | **status** }

psconf {**start** | **stop** | **restart** } **client**

psconf chclient attribute = *value*

psconf list { **-C** | **-S** }

psconf export { **-C** | **-S** } **-f** <*filename*>

psconf import { **-S** | **-C -k** <*key_filename*> } **-f** <*filename*>

TNC IPRef の操作:

psconf mkipref [**tncport=**<*port*>] **tncserver=**<host:port>

psconf { **rmipref** | **status**}

psconf { **start** | **stop** | **restart**} ipref

psconf chipref attribute = *value*

psconf { **import -k** <*key_filename*> | **export** } **-R -f** <*filename*>

psconf list -R

説明

TNC テクノロジーは、エンドポイントの認証、プラットフォームの保全性の計測、およびセキュリティー・システムの統合に関する、オープンな標準に基づいたアーキテクチャーです。TNC アーキテクチャーは、保護されたネットワーク上でエンドポイント (ネットワーク・クライアントおよびサーバー) を受け入れる前に、セキュリティー・ポリシーに準拠しているかどうかエンドポイントを検査します。仮想 I/O サーバー (VIOS) 上で新しい IP が検出されると、TNC IPRef は TNC サーバーにそのことを通知します。

SUMA を使用すると、システム管理者が Web からメンテナンス更新を手動で取得する作業が不要になります。システム管理者がフィックスをフィックス配布 Web サイトから各システムにダウンロードするための自動化インターフェースをセットアップできるようにする柔軟なオプションが提供されます。

psconf コマンドは、セキュリティー・ポリシーの追加または削除、トラステッドまたは非トラステッドとしてのクライアントの検証、レポートの生成、およびサーバーとクライアントの更新によって、ネットワーク・サーバーおよびクライアントを管理します。

psconf コマンドを使用して、次の操作を実行できます。

項目	説明
追加	ポリシー、クライアント、または E メール情報を TNC サーバーに追加します。
apargrp	TNC クライアントの検証に使用されるファイルセット・ポリシーの一部として APAR グループ名を指定します。
aparlist	APAR グループの一部である APAR のリストを指定します。
certadd	証明書にトラステッドまたは非トラステッドのマークを付けます。
certdel	クライアント情報を削除します。
chclient	`tnccs.conf` ファイルの属性を変更します。 TNC クライアントで変更を有効にするには、明示的 **start** コマンドが必要です。attribute=value の構文は、**mkclient** の構文と同じです。
chipref	`tnccs.conf` ファイルの属性を変更します。 IPRef で変更を有効にするには、明示的 **start** コマンドが必要です。attribute=value の構文は、**mkipref** の構文と同じです。
chserver	`tnccs.conf` ファイルの属性を変更します。 TNC サーバーで変更を有効にするには、明示的 **start** コマンドが必要です。attribute=value の構文は、**mkserver** の構文と同じです。 **注: dbpath** 属性は、**chserver** コマンドを使用して変更することはできません。この属性は、**mkserver** の実行中にのみ設定できます。
clientData	TNC クライアントに関する情報 (インストールされているオペレーティング・システム・レベルやファイルセット) のスナップショットを作成します。 *clientDataPath* パスは、スナップショット収集情報が保管されている場所を識別します。デフォルトの場所は、TNC サーバー上の `/var/tnc/clientData/` ディレクトリーの中です。*clientDataPath* パスの変更または設定を行うには、**chserver** サブコマンドまたは **mkserver** サブコマンドを使用します。 TNC クライアントのスナップショット収集は、TNC サーバーからコマンド・ラインで **clientData** サブコマンドを実行して開始できます。コマンド・ラインから実行される **clientData** サブコマンドは、**clientData_interval** 間隔とは関係なく動作します。
clientData_interval	**chserver** サブコマンドまたは **mkserver** サブコマンドを使用すると、**clientData_interval** 間隔に値を指定することによって、一定の間隔で実行されるようスナップショット収集を構成できます。 **clientData_interval** 間隔の値を 0 (ゼロ) 以外に指定すると、スナップショット収集が自動的に開始されます。 デフォルトでは、スナップショット収集はスケジューラーによって使用不可になります。スケジューラーを使用可能にするには、**clientData_interval** の値を 30 以上に指定します。スケジューラーを使用不可にするには、**clientData_interval** の値を 0 (ゼロ) に指定します。サポートされている **clientData_interval** 間隔の範囲は、30 分から 525600 分までです。
dbpath	TNC データベースの位置を指定します。デフォルト値は `/var/tnc` です。

項目	説明
default_policy	TNC クライアントと同じレベルの暫定修正 (ifix) と APAR があるか確認するための TNC クライアントの自動検証を有効または無効にします。自動検証を有効にする場合は *yes* を指定します。自動検証を無効にする場合は *no* を指定します。 **default_policy** サブコマンドについて詳しくは、default_policy の表を参照してください。
delete	ポリシーまたはクライアント情報を削除します。
export	クライアントまたはサーバーの証明書、あるいは TNC サーバー上のデータベースをエクスポートします。
fspolicy	TNC クライアントの検証に使用される、リリース、テクノロジー・レベル、およびサービス・パックのファイルセット・ポリシーを指定します。
import	クライアントまたはサーバー上の証明書、あるいは TNC サーバー上のデータベースをインポートします。
ipgroup	複数の IP アドレスまたはホスト名を含むインターネット・プロトコル (IP) グループを指定します。
list	TNC サーバー、TNC クライアント、または SUMA に関する情報を表示します。
log	TNC コンポーネントのログ・レベルを設定します。
mkclient	TNC クライアントを構成します。
mkipref	TNC IPRef を構成します。
mkserver	TNC サーバーを構成します。
pmport	**pmserver** が listen するポート番号を指定します。デフォルト値は 38240 です。
pmserver	IBM® ECC Web サイトおよび IBM Fix Central Web サイトから入手可能な最新のサービス・パックとセキュリティー・フィックスをダウンロードする **suma** コマンドのホスト名または IP アドレスを指定します。
recheck_interval	TNC クライアントを検証する TNC サーバーの間隔を分単位または「d (日) : h (時間) : m (分)」のフォーマットで指定します。サポートされている **recheck_interval** 間隔の範囲は、30 分から 525600 分までです。 **注記:** 値が **recheck_interval=0** の場合、クライアントの検証がスケジューラーによって一定の間隔で開始されるのではなく、登録されたクライアントがその起動時に自動的に検証されることを意味します。そのような場合、クライアントは手動で検証できます。
report	.txt または .csv ファイル拡張子を持つレポートを生成します。
restart	TNC クライアント、TNC サーバー、または TNC IPRef を再始動します。
rmclient	TNC クライアントを構成解除します。
rmipref	TNC IPRef を構成解除します。
rmserver	TNC サーバーを構成解除します。
start	TNC クライアント、TNC サーバー、または TNC IPRef を開始します。
status	TNC 構成の状況を表示します。
stop	TNC クライアント、TNC サーバー、または TNC IPRef を停止します。
tncport	TNC サーバーが listen するポート番号を指定します。デフォルト値は 42830 です。
tncserver	TNC クライアントを検証または更新する TNC サーバーを指定します。
tssserver	Trusted Surveyor サーバーの IP またはホスト名を指定します。
update	クライアントにパッチをインストールします。
verify	クライアントの手動検証を開始します。

次の表に、**default_policy** サブコマンドの値を *yes* または *no* に構成した結果を示します。

表 15. default_policy サブコマンドの結果

FSpolicy (ファイルセット・ポリシー)	**default policy=***yes*	**default policy=***no*
TNC クライアントが、暫定修正 (iFix) と APAR グループが定義されたファイルセット・ポリシーに属している	デフォルト・ポリシーは、ファイルセット・ポリシーで提供される iFix と APAR によってオーバーライドされます。	デフォルト・ポリシーは使用されません。ファイルセット・ポリシーで提供される iFix と APAR は、TNC クライアントの検証プロセス時に考慮されます。
TNC クライアントが、iFix と APAR グループが定義されていないファイルセット・ポリシーに属している	デフォルト・ポリシーは、TNC クライアントの検証プロセス中に iFix および APAR とともに使用されます。検証プロセスでは、TNC クライアントのレベルと一致する iFix と APAR のみが使用されます。	デフォルト・ポリシーは使用されません。

フラグ

項目	説明
-A <advisoryName>	レポートの勧告的な名前を指定します。
-B <buildinfo>	パッチ・レポートを作成するための構築情報を指定します。

-c	以下のように、コロン区切りレコードでユーザー属性を表示します。
	`# name: attribute1: attribute2: ...`
	`policy: value1: value2: ...`

-C	操作の対象がクライアント・コンポーネントであることを指定します。
-d *database file location/dir path of database*	データベースのインポート用のファイル・パス・ロケーションを指定するか、またはデータベースのエクスポート用のディレクトリー・パス・ロケーションを指定します。
-D *yyyy-mm-dd*	ログ・ヒストリー内の特定のクライアント・エントリーに対して日付を指定します。ここで、*yyyy* は年、*mm* は月、*dd* は日です。
-e *emailid* **ipgroup=[±]***g1, g2...*	E メール ID とコンマ区切りの IP グループ名リストを続けて指定します。
-E | FAIL | COMPLIANT | ALL |	E メールを構成済み E メール ID に送信する必要がある場合のイベントを指定します。 FAIL - クライアントの検証状況が FAILED の場合にメールが送信されます。 COMPLIANT - クライアントの検証状況が COMPLIANT の場合にメールが送信されます。 ALL - メールはクライアント検証のすべての状況に対して送信されます。
-f *filename*	インポート操作の場合は証明書を読み取る元のファイルを指定し、エクスポート操作の場合は証明書を書き込む先の場所を指定します。
-F *fspolicy buildinfo*	ファイルシステム・ポリシー名とビルド情報を続けて指定します。ビルド情報は、次の形式で指定できます。 `6100-04-01` (ここで、`6100` はバージョン 6.1 を表し、`04` はメンテナンス・レベル、`01` はサービス・パックです)
-g	指定された TNC クライアントで **clientData** サブコマンドを実行します。このフラグは、**clientData** サブコマンドと一緒にしか使用できません。
-G *ipgroupname* **ip=[±]***ip1, ip2...*	IP グループ名と、コンマ区切りの IP リストを続けて指定します。
-H	ヒストリー・ログをリストします。
-i *host*	IP アドレスまたはホスト名を指定します。
-I ip=[±]*ip1, ip2...* **|** [±]host1,host2...	検証時に無視する必要がある IP/ホスト名を指定します。
-k *filename*	インポート操作の場合は、証明書鍵を読み取る元のファイルを指定します。
-l	TNC サーバー上にある、指定された TNC クライアントのスナップショットの詳細をリストします。このフラグは、**clientData** サブコマンドと一緒にしか使用できません。
-p	TNC クライアントの更新をプレビューします。
-P <policyName>	クライアント・ポリシー・レポートを作成するためのポリシー名を指定します。
-q	ヘッダー情報を抑止します。
-r *buildinfo*	ビルド情報に基づいてレポートを生成します。ビルド情報は、次の形式で指定できます。 `6100-04-01` (ここで、`6100` はバージョン 6.1 を表し、`04` はメンテナンス・レベル、`01` はサービス・パックです)
-R	操作の対象が IPRef コンポーネントであることを指定します。
-s COMPLIANT | IGNORE | FAILED | ALL	次のように、クライアントを状況別に表示します。 **COMPLIANT** アクティブ・クライアントを表示します。 **IGNORE** いずれかの検証対象から除外されたクライアントを表示します。 **FAILED** 構成ポリシーに基づく検証に失敗したクライアントを表示します。 **ALL** 状況に関係なく、すべてのクライアントを表示します。
-S <host>	クライアント・セキュリティー・フィックス・レポートを作成するためのホスト名を指定します。

項目	説明
-t TRUSTED | UNTRUSTED	指定したクライアントにトラステッドまたは非トラステッドのマークを付けます。 **注:** サーバーまたはクライアントがトラステッドまたは非トラステッドであることの確認は、システム管理者のみが行うことができます。
-T	有効な証明書を持っている TS サーバーからの要求をクライアントが受け入れることができることを指定します。
-u	TNC クライアントにインストールした暫定修正をアンインストールします。
-v	コンマで区切られた暫定修正リストを指定します。
-V	暫定修正グループ名を指定します。

終了状況

このコマンドは、以下の終了値を戻します。

項目	説明
0	コマンドが正常に実行され、要求された変更がすべて行われました。
>0	エラーが発生しました。出力されるエラー・メッセージに、障害のタイプに関する詳細情報が示されます。

例

1. TNC サーバーを開始するには、以下のコマンドを入力します。

   ```
   psconf start server
   ```

2. ビルド 7100-04-02 に対してファイルシステム・ポリシー 71D_latest を追加するには、以下のコマンドを入力します。

   ```
   psconf add -F 71D_latest 7100-04-02
   ```

3. ファイルシステム・ポリシー 71D_old を削除するには、以下のコマンドを入力します。

   ```
   psconf delete -F 71D_old
   ```

4. IP アドレス 11.11.11.11 を持つクライアントが**トラステッド**であることを確認するには、以下のコマンドを入力します。

   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```

5. IP アドレス 11.11.11.11 を持つクライアントをサーバーから削除するには、以下のコマンドを入力します。

   ```
   psconf certdel -i 11.11.11.11
   ```

6. IP アドレス 11.11.11.11 を持つクライアントの情報を検証するには、以下のコマンドを入力します。

   ```
   psconf verify -i 11.11.11.11
   ```

7. IP アドレス 11.11.11.11 を持つクライアントの情報を表示するには、以下のコマンドを入力します。

   ```
   psconf list -i 11.11.11.11
   ```

8. **COMPLAINT** 状況にあるクライアントに関するレポートを生成するには、以下のコマンドを入力します。

   ```
   psconf list -s CPMPLIANT -i ALL
   ```

9. ビルド 7100-04-02 に関するレポートを生成するには、以下のコマンドを入力します。

   ```
   psconf list -r 7100-04-02
   ```

10. IP アドレス 11.11.11.11 を持つクライアントの接続ヒストリーを表示するには、以下のコマンドを入力します。

    ```
    psconf list -H -i 11.11.11.11
    ```

11. 2009 年 2 月 1 日またはそれより古い、IP アドレス 11.11.11.11 を持つクライアントのエントリーをログ・ヒストリーから削除するには、以下のコマンドを入力します。

```
psconf delete -H -i 11.11.11.11 -D 2009-02-01
```

12. IP アドレス 11.11.11.11 を持つクライアントのクライアント証明書をサーバーからインポートするには、以下のコマンドを入力します。

    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```

13. クライアントからサーバー証明書をエクスポートするには、以下のコマンドを入力します。

    ```
    psconf export -S -f /tmp/server.txt
    ```

14. IP アドレス 11.11.11.11 を持つクライアントをサーバーからの適切なレベルに更新するには、以下のコマンドを入力します。

    ```
    psconf update -i 11.11.11.11
    ```

15. クライアントの状況を表示するには、以下のコマンドを入力します。

    ```
    psconf status
    ```

16. クライアント証明書を表示するには、以下のコマンドを入力します。

    ```
    psconf list -C
    ```

17. クライアントを開始するには、以下のコマンドを入力します。

    ```
    psconf start client
    ```

18. **clientData** サブコマンドを使用して収集されたスナップショット情報を表示するには、次のコマンドを入力します。

    ```
    psconf clientData -l [ip|host]
    ```

19. TNC クライアントのヒストリーを表示するには、次のコマンドを入力します。

    ```
    psconf list –H –i [ip|ALL]
    ```

セキュリティー

RBAC ユーザーと Trusted AIX ユーザーへの注意:

このコマンドは特権命令を実行できます。特権命令を実行できるのは特権ユーザーのみです。許可と特権の詳細については、「セキュリティー」の『特権コマンド・データベース』を参照してください。このコマンドに関連する特権と許可のリストについては、**lssecattr** コマンドまたは **getcmdattr** サブコマンドを参照してください。

---

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 -l {high|medium|low|default|sox-cobit} [**-p**]

pscxpert -l {h|m|l|d|s} [**-p**]

pscxpert -f Profile [**-p**]

pscxpert -u [**-p**]

pscxpert -c [**-p**] [**-r**|**-R**] [**-P** Profile] [**-l** Level]

pscxpert -t

pscxpert -l <Level> [**-p**] **<-a** *File1* | **-n** *File2* | **-a** *File3* **-n** *File4***>**

pscxpert -f Profile **-a** File [**-p**]

pscxpert -d

説明

pscxpert コマンドは、さまざまなシステム構成を設定して、指定されたセキュリティー・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、**-n** フラグおよび **-a** フラグを指定して **pscxpert -l** コマンドを実行すると、セキュリティー設定は *File* パラメーターで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。

ターゲットの仮想 I/O サーバーの root ユーザーとして **pscxpert** コマンドを実行します。ターゲットの仮想 I/O サーバーの root ユーザーとしてログインしていない場合は、コマンドを実行する前に **oem_setup_env** コマンドを実行してください。

pscxpert コマンドの別のインスタンスが既に実行されているときに **pscxpert** コマンドを新たに実行すると、エラー・メッセージが出され、その **pscxpert** コマンドは終了します。

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	関連するセキュリティー・レベル・オプションを含む設定が、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。
-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。この検査は、任意のデフォルト・プロファイルまたはカスタム・プロファイルに対して実行できます。
-d	文書型定義 (DTD) を表示します。

項目	説明
-f	指定された *Profile* 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。 **DoDv2.xml** このファイルには、バージョン 2 の米国国防総省の Security Technical Implementation Guide (STIG) 設定の要件が入っています。 **DoDv2_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。 **NERC.xml** このファイルには、北米電力信頼度協議会 (North American Electric Reliability Corporation (NERC)) 設定の要件が入っています。 **NERC_to_AIXDefault.xml** このファイルは、デフォルトの AIX 設定に対する NERC 設定の変更を行います。 **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。 **PCIv3.xml** このファイルには、Payment Card Industry Data Security Standard バージョン 3 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。 **PCIv3_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。 **SOX-COBIT.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** フラグを指定すると、**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。 **s|sox-cobit** Sarbanes-Oxley 法令および COBIT セキュリティー・オプションを指定します。 **-l** と **-n** の両方のフラグを指定すると、セキュリティー設定はシステムに実装されず、指定され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** フラグを使用すると、**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	関連するセキュリティー・レベル・オプションを含む設定を指定されたファイルに書き込みます。
-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** フラグを使用すると、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** のいずれのフラグ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** フラグと一緒に使用されます。**-c** フラグと **-P** フラグを使用すると、システムと渡されたプロファイルとの互換性が検査されます。
-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。 **注: -u** フラグを使用して、DoD、DoDv2、NERC、PCI、または PCIv3 のプロファイルの適用を取り消すことはできません。これらのプロファイルを追加後に除去するには、末尾が `_AIXDefault.xml` になっているプロファイルを適用します。例えば、NERC.xml プロファイルを除去するには、NERC_to_AIXDefault.xml プロファイルを適用する必要があります。

パラメーター

項目	説明
File	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。
Level	前に適用された設定に対する検査を行うカスタム・レベル。
Profile	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 /etc/security/pscexpert/plugin/myPreferredSettings.xml
   ```

   このコマンドの実行後は、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 コメント文字列で囲む (<-- でコメントを開始し、-¥> でコメントを閉じる) 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. システム上の NERC プロファイルのセキュリティー設定のカスタム・レベルを確認したり、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 -l NERC
   ```
6. 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。このファイルは 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。

rmvfilt コマンド

目的

仮想 LAN 間のフィルター規則を、フィルター・テーブルから削除します。

構文

rmvfilt -n [**fid|all>**]

説明

rmvfilt コマンドは、仮想 LAN 間のフィルター規則を、フィルター・テーブルから削除するのに使用されます。

フラグ

-n 削除するフィルター規則の ID を指定します。**all** オプションは、すべてのフィルター規則を削除する場合に使用します。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. すべてのフィルター規則を削除する場合、またはカーネル内のすべてのフィルター規則を非アクティブにする場合は、次のコマンドを入力します。

   ```
   rmvfilt -n all
   ```

関連概念:

138 ページの『ルールの非アクティブ化』
トラステッド・ファイアウォール・フィーチャーで、VLAN 間ルーティングを使用可能にするルールを非アクティブにすることができます。

---

vlantfw コマンド

目的

IP およびメディア・アクセス制御 (MAC) マッピング情報を表示または消去し、ロギング機能を制御します。

構文

vlantfw -h | **-s** | **-t** | **-d** | **-f** | **-G** | **-q** | **-D** | **-E** | **-F** | **-i** | **-l** | **-L** | **-m** | **-M** | **-N** *integer*

説明

vlantfw コマンドは、IP および MAC マッピング・エントリーを表示または消去します。また、このコマンドにより、トラステッド・ファイアウォールのロギング機能を開始または停止することもできます。

フラグ

-d IP マッピング情報をすべて表示します。

-D 収集した接続データを表示します。

-E さまざまな中央処理装置上のロジカル・パーティション (LPAR) 間の接続データを表示します。

-f IP マッピング情報をすべて削除します。

-F 接続データのキャッシュをクリアします。

-G トラステッド・ファイアウォールを使用して、トラフィックを内部的にルーティングするために構成できるフィルター規則を表示します。

-I 異なる VLAN ID に関連付けられているが、同一の中央処理装置を共有する LPAR 間の接続データを表示します。

-l トラステッド・ファイアウォールのロギング機能を開始します。

-L トラステッド・ファイアウォールのロギング機能を停止し、トレース・ファイルの内容を `/home/padmin/svm/svm.log` ファイルにリダイレクトします。

-m トラステッド・ファイアウォール・モニターを使用可能にします。

-M トラステッド・ファイアウォール・モニターを使用不可にします。

-q セキュアな仮想マシンの状況を照会します。

-s トラステッド・ファイアウォールを開始します。

-t トラステッド・ファイアウォールを停止します。

パラメーター

-N *integer*
指定された整数に対応するフィルター規則を表示します。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. すべての IP マッピングを表示するには、次のコマンドを入力します。
   ```
   vlantfw -d
   ```
2. すべての IP マッピングを除去するには、次のコマンドを入力します。
   ```
   vlantfw -f
   ```
3. トラステッド・ファイアウォールのロギング機能を開始するには、次のコマンドを入力します。
   ```
   vlantfw -l
   ```
4. セキュアな仮想マシンの状況を検査するには、次のコマンドを入力します。
   ```
   vlantfw -q
   ```
5. トラステッド・ファイアウォールを開始するには、次のコマンドを入力します。
   ```
   vlantfw -s
   ```
6. トラステッド・ファイアウォールを停止するには、次のコマンドを入力します。
   ```
   vlantfw -t
   ```
7. 中央処理装置内のトラフィックをルーティングするフィルターの生成に使用可能な、対応する規則を表示するには、次のコマンドを入力します。
   ```
   vlantfw -G
   ```

関連資料:

158 ページの『genvfilt コマンド』

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
USA

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。これらのサンプル・プログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。 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。

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。

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。

Linux は、Linus Torvalds 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、Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

索引

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

[ア行]

[カ行]

[サ行]

[タ行]

[ナ行]

[ハ行]

[マ行]

［ラ行］

A

C

G

I

L

M

P

R

S

T

V

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