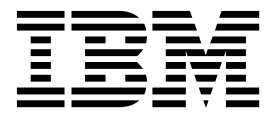


**IBM PowerSC
Standard Edition**

バージョン 1.1.6

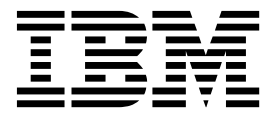
PowerSC Standard Edition



**IBM PowerSC
Standard Edition**

バージョン 1.1.6

PowerSC Standard Edition



注記

本書および本書で紹介する製品をご使用になる前に、 205 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 1.1.6、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 1.1.6
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

© Copyright IBM Corporation 2017.

目次

本書について	vii
--------	-----

PowerSC Standard Edition の新機能	1
-------------------------------	---

PowerSC Standard Edition PDF ファイル	3
-----------------------------------	---

PowerSC Standard Edition の概念	5
------------------------------	---

PowerSC Standard Edition のインストール	7
----------------------------------	---

セキュリティおよびコンプライアンス自動化	9
----------------------	---

セキュリティおよびコンプライアンス自動化の概念	9
-------------------------	---

米国防総省の STIG への準拠	10
------------------	----

Payment Card Industry - Data Security	
---------------------------------------	--

Standard への準拠	77
---------------	----

Sarbanes-Oxley 法令および COBIT への準拠	95
---------------------------------	----

医療保険の積算と責任に関する法律 (HIPAA)	
--------------------------	--

(Health Insurance Portability and	
-----------------------------------	--

Accountability Act (HIPAA))	96
-----------------------------	----

北米電力信頼度協議会 (North American	
----------------------------	--

Electric Reliability Corporation) への準拠	102
--	-----

セキュリティおよびコンプライアンス自動化の管	
------------------------	--

理	105
---	-----

失敗したルールの調査	106
------------	-----

失敗したルールの更新	106
------------	-----

カスタム・セキュリティ構成プロファイルの作	
-----------------------	--

成	107
---	-----

AIX Profile Manager を使用したアプリケーション	
-----------------------------------	--

のテスト	107
------	-----

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	108
--------------------------------	-----

PowerSC のセキュリティおよびコンプライア	
--------------------------	--

ス自動化の構成	108
---------	-----

PowerSC のコンプライアンス・オプション設定	
---------------------------	--

の構成	108
-----	-----

コマンド・ラインからの PowerSC のコンプラ	
---------------------------	--

イアンスの構成	109
---------	-----

AIX Profile Manager を使用した PowerSC の	
-------------------------------------	--

コンプライアンスの構成	109
-------------	-----

PowerSC リアルタイム・コンプライア	
-----------------------	--

ンス	111
----	-----

PowerSC リアルタイム・コンプライアンス のイン	
-----------------------------	--

ストール	111
------	-----

PowerSC リアルタイム・コンプライアンス の構成	111
-----------------------------	-----

PowerSC リアルタイム・コンプライアンス フ	
---------------------------	--

ィーチャーによってモニターされるファイルの識	
------------------------	--

別	112
---	-----

PowerSC リアルタイム・コンプライアンス に	
---------------------------	--

対するアラートの設定	112
------------	-----

トラステッド・ブート	113
------------	-----

トラステッド・ブートの概念	113
---------------	-----

トラステッド・ブートの計画	114
---------------	-----

トラステッド・ブートの前提条件	114
-----------------	-----

修復の準備	114
-------	-----

マイグレーションに関する考慮事項	115
------------------	-----

トラステッド・ブートのインストール	115
-------------------	-----

コレクターのインストール	115
--------------	-----

ベリファイヤーのインストール	116
----------------	-----

トラステッド・ブートの構成	116
---------------	-----

システムの登録	116
---------	-----

システムの認証	117
---------	-----

トラステッド・ブートの管理	117
---------------	-----

認証結果の解釈	117
---------	-----

システムの削除	118
---------	-----

トラステッド・ブートのトラブルシューティング	118
------------------------	-----

トラステッド・ファイアウォール	121
-----------------	-----

トラステッド・ファイアウォールの概念	121
--------------------	-----

トラステッド・ファイアウォールのインストール	123
------------------------	-----

トラステッド・ファイアウォールの構成	124
--------------------	-----

トラステッド・ファイアウォール・アドバイザー	124
------------------------	-----

トラステッド・ファイアウォール・ロギング	125
----------------------	-----

複数の共用イーサネット・アダプター	125
-------------------	-----

共用イーサネット・アダプターの除去	127
-------------------	-----

ルールの作成	127
--------	-----

ルールの非アクティブ化	128
-------------	-----

トラステッド・ロギング	131
-------------	-----

仮想ログ	131
------	-----

仮想ログ・デバイスの検出	132
--------------	-----

トラステッド・ロギングのインストール	132
--------------------	-----

トラステッド・ロギングの構成	133
----------------	-----

AIX 監査サブシステムの構成	133
-----------------	-----

syslog の構成	133
------------	-----

仮想ログ・デバイスへのデータの書き込み	134
---------------------	-----

トラステッド・ネットワーク接続 (TNC)	135
-----------------------	-----

トラステッド・ネットワーク接続の概念	135
--------------------	-----

トラステッド・ネットワーク接続のコンポーネン	
------------------------	--

ト	135
---	-----

トラステッド・ネットワーク接続のセキュア通信	137
------------------------	-----

トラステッド・ネットワーク接続プロトコル	137
----------------------	-----

IMC および IMV モジュール	138
-------------------	-----

TNC の要件	138
---------	-----

TNC コンポーネントのセットアップ	138
TNC コンポーネントのオプションの構成	140
トラステッド・ネットワーク接続 (TNC) サーバ	
ーのオプションの構成	140
トラステッド・ネットワーク接続 (TNC) クライ	
アントの追加オプションの構成	140
TNC パッチ管理サーバーのオプションの構成	141
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	142
VIOS での IP リファラーの構成	143
トラステッド・ネットワーク接続 (TNC) コンポー	
ネットの管理	144
トラステッド・ネットワーク接続サーバーのログ	
の表示	144
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	144
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	145
トラステッド・ネットワーク接続の検証結果の表	
示	146
トラステッド・ネットワーク接続クライアントの	
更新	146
パッチ管理ポリシーの管理	146
トラステッド・ネットワーク接続の証明書のイン	
ポート	147
TNC サーバーのレポート作成	147
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	148

PowerSC グラフィカル・ユーザー・インターフェース (GUI) 151

PowerSC GUI の概念	151
PowerSC GUI セキュリティー	151
エンドポイントの内容をコンプライアンス・ペー	
ジに取り込む	152
PowerSC GUI のインストール	153
PowerSC GUI エージェント	153
PowerSC GUI サーバー	153
PowerSC GUI 要件	153
エンドポイントへのトラストストア・セキュリテ	
ー証明書の配布	154
エンドポイントへのトラストストア・ファイルの	
手動でのコピー	154
仮想化マネージャーを使用したエンドポイントへ	
のトラストストア・ファイルのコピー	155
ユーザー・アカウントのセットアップ	155
グループ・セットアップ・コマンドおよびスクリ	
プトの実行	156
PowerSC GUI の使用	156
PowerSC GUI 言語の指定	158
PowerSC GUI のナビゲート	158
エンドポイントとサーバーとの通信を管理	158
エンドポイントとサーバーとの通信を検査	159
エンドポイント PowerSC GUI モニタリング	
から除外	159
鍵ストア要求の検査および生成	159

エンドポイントの編成およびグループ化	161
カスタム・グループの作成	161
既存グループに割り当てられたシステムの追加ま	
たは削除	161
グループの削除	162
グループの名前変更	162
グループの複製	162
コンプライアンス・プロファイルの操作	162
コンプライアンス・プロファイルの表示	163
カスタム・プロファイルの作成	163
プロファイルをグループ・メンバーにコピー	164
カスタム・プロファイルの削除	164
コンプライアンス・レベルおよびプロファイルの管	
理	164
コンプライアンス・レベルおよびプロファイルの	
適用	165
コンプライアンス・レベルを元に戻す	166
最後に適用されたコンプライアンス・レベルおよ	
びプロファイルの検査	166
適用されていないコンプライアンス・レベルまた	
はプロファイルの検査	167
コンプライアンス・イベント発生時の E メール	
通知の送信	167
エンドポイント・セキュリティーのモニター	168
リアルタイム・コンプライアンス (RTC) の構成	168
以前の日時へのリアルタイム・コンプライアンス	
(RTC) 構成オプションの復元	168
他のグループへのリアルタイム・コンプライアン	
ス (RTC) 構成オプションのコピー	169
リアルタイム・コンプライアンス (RTC) ファイ	
ル・リストの編集	169
以前の構成へのリアルタイム・コンプライアンス	
(RTC) ファイル・モニター・オプションの復元	169
他のグループへのリアルタイム・コンプライアン	
ス (RTC) ファイル・リスト・モニター・オプシ	
ョンのコピー	170
リアルタイム・コンプライアンス (RTC) 検査の	
実行	170
トラステッド実行 (TE) の構成	170
他のグループへのトラステッド実行 (TE) オプシ	
ョンのコピー	171
トラステッド実行 (TE) ファイル・リストの編集	171
他のグループへのトラステッド実行 (TE) ファイ	
ル・リスト・モニター・オプションのコピー	171
他の PowerSC フィーチャーの状況の表示	172
トラステッド実行モニターの切り替え	173
セキュリティー・イベント発生時の E メール通	
知の送信	173
レポートの操作	174
レポート・グループの選択	174
E メールを介したレポートの配布	175

PowerSC Standard Edition コマンド 177

chvfilt コマンド	177
genvfilt コマンド	178
lsvfilt コマンド	180

mkvfilt コマンド	180
pmconf コマンド	181
psconf コマンド	186
I pscuiserverctl コマンド	194
pscxpert コマンド	196
rmvfilt コマンド	201
vlantfw コマンド	202

特記事項	205
プライバシー・ポリシーに関する考慮事項	207
商標	207
索引	209

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

この製品の開発と製造には、ISO 9000 登録済み高品質システムが使用されました。

PowerSC Standard Edition の新機能

PowerSC™ Standard Edition バージョン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 (1) が付いている場合があります。

2017 年 9 月

以下のフィーチャーが PowerSC GUI に追加されました。

- すべてのコンプライアンス状況情報およびリアルタイムのファイル保全性状況情報の要約一覧が表示される、最上位のセキュリティおよびコンプライアンス・ダッシュボードが追加されました。
- Open Stack 統合を介した PowerVC などの仮想化マネージャーとの統合が追加されました。これにより、エンドポイントの自動化されたセキュアなディスカバリーが提供されます。また、統合では、VM 作成直後からのセキュリティ可視性を備えたクラウド環境がサポートされます。
- 監査をサポートするレポート作成機能が追加されました。フォーマット設定された HTML と CSV ファイルの両方で、コンプライアンスおよびファイル保全性に関する概要レポートと詳細レポートが使用可能になりました。これらのレポートは、即時に配布または毎日配布するようにスケジュールできます。
- プロファイル・エディターが拡張され、コンプライアンス・ルールおよびプロファイルのカスタマイズ機能が改善されました。ルールは、複数のソースから組み合わせ、GUI を介して編集できるようになりました。
- QRadar などのセキュリティ・イベント情報マネージャーとの統合が追加されました。意味のあるコンプライアンス・イベントおよびファイル保全性イベントのために Syslog 項目を提供することで、簡単に統合できます。
- 「元に戻す」機能が改善され、適用されたプロファイルを元に戻す複雑なタスクを簡素化できます。PowerSC 1.1.6 は、PCI プロファイルでのシームレスな「元に戻す」機能を目指して大きなステップを進めています。
- コンプライアンスのために GUI スケーラビリティが改善されました。GUI サーバーは水平にスケラブルであり、各インスタンスは最大で 1,000 以上のエンドポイントをサポートできます。

トラステッド・ネットワーク接続パッチ管理 (TNCPM) 用の以下のフィーチャーが追加されました。

- TNCPM をインターネットから隔離できるようにすることで追加のセキュリティ・レイヤーを提供するプロキシ・サーバーが導入されました。
- TNCPM への暫定修正 (iFix) の統合が完全に自動化されました。TNCPM は、ユーザー介入なしで、オペレーティング・システムに該当する脆弱性をモニターしてパッチを適用できます。
- オープン・ソース・パッケージのダウンロードが TNCPM に統合され、オープン・ソース・ワークフローが簡素化されました。

コンプライアンス機能を強化するために以下のフィーチャーが追加されました。

- 適用時にプロファイルに組み込まれるルールに関する詳細を提供するレポート・オプションが追加されました。

PowerSC Standard Edition PDF ファイル

PowerSC Standard Edition 資料は PDF ファイルとしてご覧いただけます。

- PowerSC Standard Edititon
- PowerSC Standard Edition リリース・ノート

PowerSC Standard Edition 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・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・ベース・ハードウェアに関する詳細を示します。

表 1. 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 • AIX 7.2	• 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 • AIX 7.2 • 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 1. 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 • AIX 7.2	• 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・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 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
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・ネットワーク接続クライアントには、オペレーティング・システムとともにリストされているコンポーネントのいずれかが必要です。	• 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 • パッチ管理のために、SUMA 環境に AIX バージョン 7.2.1 サービス更新管理アシスタント (SUMA) コンソール・システム	

PowerSC Standard Edition 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 および PowerSC グラフィカル・ユーザー・インターフェース (GUI) 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。コンプライアンス・プログラムでは、「/」ファイル・システム内に少なくとも 5 MB の使用可能なディスク・スペースが必要です。
- | • powerscStd.vtspm: 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。AIX ベース・メディアまたは https://www-01.ibm.com/marketing/iwm/iwm/web/preLogin.do?source=aixbp&S_PKG=vtspm から powerscStd.vtspm ファイル・セットを手に入れます。
- | • 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: パッチ管理用のサービス更新管理アシスタント (SUMA) 7.2.1.0 の環境内に SUMA コンソール・システムとともに、AIX バージョン 7.1 TL4 以降でインストールされます。IBM セキュリティ・サイトからの ifix のセキュアな伝送のために、TNC パッチ・マネージャー上に Curl 7.52.1-1 がインストールされている必要があります。
- | • 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。
- | • powerscStd.uiAgent.rte: PowerSC グラフィカル・ユーザー・インターフェース (GUI) を使用して管理される AIX システムにインストールされます。powerscStd.uiAgent.rte 116 をインストールするために、ファイル・セット powerscStd.ice 115 以上が必要です。
- | • powerscStd.uiServer.rte: 特に PowerSC グラフィカル・ユーザー・インターフェース (GUI) サーバーを実行するように構成されている 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 および PowerSC グラフィカル・ユーザー・インターフェース (GUI) 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します。

```
% 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。

PowerSC グラフィカル・ユーザー・インターフェース (GUI) のインストールについて詳しくは、153 ページの『PowerSC GUI のインストール』を参照してください。

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 を使用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 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。

115 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。

関連タスク:

123 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。

132 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。

138 ページの『TNC コンポーネントのセットアップ』

各トラステッド・ネットワーク接続 (TNC) コンポーネントでは、お客様固有の環境で実行するために、セットアップが必要です。

セキュリティおよびコンプライアンス自動化

AIX Profile Manager は、セキュリティ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 リアルタイム・コンプライアンス 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設定の適用、セキュリティ設定のモニター、およびセキュリティ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・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・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 (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/pscxpert/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 2. 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	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 <code>/etc/security/pscxpert/dodv2/trust</code> 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	<code>securetcip</code> コマンドを使用する必要があります。	位置 <code>/etc/security/pscxpert/dodv2/dodsecuretcip</code> 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。
AIX00060	2	無許可の <code>setuid</code> ファイル、および許可された <code>setuid</code> 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 <code>/etc/security/pscxpert/dodv2/trust</code> 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 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
AIX00080	1	SYSTEM 属性が、任意 のアカウントで <i>none</i> に設定されてはな りません。	位置 /etc/security/pscxpert/dodv2/SYSattr 準拠アクション 確実に、指定された属性が <i>none</i> 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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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。
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/pscxpert/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.c1 ファイルが存在してい る必要があります。	位置 /etc/security/pscxpert/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/pscxpert/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。

表 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
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/psccexpert/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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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	位置 /etc/security/psccexpert/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。

表 2. 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
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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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/psccexpert/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/psccexpert/dodv2/dodv2loginherald 準拠アクション このログイン・バナーは、米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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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。

表 2. 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	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
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/pwscexpert/dodv2/chusrattdod 準拠アクション 必要なパスワード設定値を設定します。
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/pwscexpert/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/pwscexpert/dodv2/chusrattdod 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/pwscexpert/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/pwscexpert/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/pwscexpert/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/pwscexpert/dodv2/chusrattdod 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/pwscexpert/dodv2/chusrattdod 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 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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/psccexpert/dodv2/chusrattdod 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/psccexpert/dodv2/loginout /etc/security/psccexpert/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/psccexpert/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/psccexpert/dodv2/chusrattdod 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/psccexpert/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/psccexpert/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/psccexpert/dodv2/chusrattdod 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 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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/psccexpert/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・ディレクトリが ルート・ディレクトリ (/) であってはなり ません。	位置 /etc/security/psccexpert/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/psccexpert/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/psccexpert/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。
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/psccexpert/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 2. 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	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
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/pscxpert/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/pscxpert/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/pscxpert/dodv2/remotconsole 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/pscxpert/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/pscxpert/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。
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/pscxpert/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/pscxpert/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/pscxpert/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。

表 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
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/pscxpert/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/pscxpert/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。
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 みが含まれる必要あり ます。	位置 /etc/security/pscxpert/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 まれる必要ありま す。	位置 /etc/security/pscxpert/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/pscxpert/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 2. 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	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/pscxpert/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/pscxpert/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/pscxpert/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。
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/pscxpert/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/pscxpert/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/pscxpert/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。

表 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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。
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/psccexpert/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。

表 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert 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。
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/psccexpert/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/psccexpert/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。

表 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
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/psccexpert/dodv2/wwdevfiles /etc/security/psccexpert/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/psccexpert/dodv2/lockacc_rlogin /etc/security/psccexpert/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。
GEN002660	2	監査が使用可能でなければなりません。	位置 /etc/security/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
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/psccexpert/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。
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/psccexpert/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、監査システ ムを構成する必要があります。	位置 /etc/security/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 2. 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	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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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/psecexpert/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 ィレクトリ内のプロ グラム、または全ユー ー書き込み可能ディ レクトリに從属する プログラムを実行して はなりません。	位置 /etc/security/psecexpert/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/psecexpert/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/psecexpert/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/psecexpert/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。
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/psecexpert/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/psecexpert/dodv2/ntwkoptsdod 準拠アクション bcstping 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/psecexpert/dodv2/ntwkoptsdod 準拠アクション bcstping ネットワーク・オプションの値を 0 に設定 します。

表 2. 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	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
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/psccexpert/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/psccexpert/dodv2/ntwkoptsdod 準拠アクション ipsrccroutesend 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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
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/psccexpert/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/psccexpert/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。
GEN003820-3860	1,2,3	rsh、rexexec、および telnet デモン、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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/dodv2/sendmailhelp /etc/security/psccexpert/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。
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/psccexpert/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。

表 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
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/pscxpert/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/pscxpert/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/pscxpert/dodv2/SMTpuudecode 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/pscxpert/dodv2/sendmaildod 準拠アクション メール・リレーを制限します。
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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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 に機能シェルがあつて はなりません。	位置 /etc/security/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 以降のパ ージョンのみを使用す る必要があります。	位置 /etc/security/psccexpert/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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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 2. 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	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
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/pwscexpert/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/pwscexpert/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/pwscexpert/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/pwscexpert/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/pwscexpert/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/pwscexpert/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。
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/pwscexpert/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/pwscexpert/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 2. 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	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
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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。
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 後により圧縮を許可す る必要があります。	位置 /etc/security/psccexpert/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/psccexpert/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 2. 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	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
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/psecexpert/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/psecexpert/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。
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/psecexpert/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/psecexpert/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/psecexpert/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/psecexpert/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/psecexpert/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。

表 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
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 転送を使用可能にはなりません。	位置 /etc/security/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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。
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/psccexpert/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。

表 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
GEN006460	2	いずれかの NIS+ サー バーが、セキュリティ ・レベル 2 で動作 しなければなりません。	位置 /etc/security/psccexpert/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 ・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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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。

表 2. 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	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
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/psccexpert/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/psccexpert/ipv6.conf ファイルの <i>ipv6_enabled</i> 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、 <i>ipv6_enabled</i> 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/psccexpert/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。
GEN007820	2	システムで IP トンネルが構成されてはなりません。	位置 /etc/security/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/dodv2/ntwkoptsdod 準拠アクション <i>ipignoreredirects</i> 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/psccexpert/dodv2/ntwkoptsdod 準拠アクション <i>ipsendredirects</i> ネットワーク・オプションの値を 0 に設定します。

表 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
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/psccexpert/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。
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/psccexpert/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/psccexpert/dodv2/ntwkoptsdod 準拠アクション ipsrccrouterecv 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/psccexpert/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/psccexpert/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/psccexpert/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。

表 2. 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	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
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 が入っていないはなりま せん。	位置 /etc/security/psccexpert/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/psccexpert/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。
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 ドするために弱い弱ポ ートを 5 分間回避す る必要があります。	位置 /etc/security/psccexpert/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、 <i>deny-all</i> 、 <i>allow-by-exception</i> ポリ シーを実装する必要が あります。	位置 /etc/security/psccexpert/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。 <i>port_number:ip_address:</i> <i>action</i> ここで、 <i>action</i> 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/psccexpert/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/psccexpert/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。

表 2. 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	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
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/psccexpert/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。
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/psccexpert/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 (ttldbserver) サービスがアクティブであってはなりません。	位置 /etc/security/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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。
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/psccexpert/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 2. DoD の一般的な要件 (続き)

米国防総省の STIG のチェック ポイント ID	STIG ルールのカ テゴリ	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
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一 りません。	位置 /etc/security/pscxpert/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一 りません。	位置 /etc/security/pscxpert/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/pscxpert/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 であっては一りませ ん。	位置 /etc/security/pscxpert/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 であっては一りませ ん。	位置 /etc/security/pscxpert/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。
GEN009290	2	システムでは systat サービスがアクティブ であっては一りませ ん。	位置 /etc/security/pscxpert/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 ブであっては一りませ ん。	位置 /etc/security/pscxpert/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 であっては一りませ ん。	位置 /etc/security/pscxpert/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 2. 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
GEN009320	2	システムでは <code>sprayd</code> サービスがアクティブであってはなりません。	位置 <code>/etc/security/psccexpert/dodv2/inetdservices</code> 準拠アクション <code>/etc/inetd.conf</code> 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 <code>rstatd</code> サービスがアクティブであってはなりません。	位置 <code>/etc/security/psccexpert/dodv2/inetdservices</code> 準拠アクション <code>/etc/inetd.conf</code> 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 <code>/etc/security/psccexpert/dodv2/dodv2cmntrows</code> 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 3. 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	<code>/etc/netshvc.conf</code> ファイルは <code>root</code> が所有している必要があります。	位置 <code>/etc/security/psccexpert/dodv2/chowndodfiles</code> 準拠アクション 確実に、指定されたファイルを <code>root</code> が所有するようにします。
AIX00090	<code>/etc/netshvc.conf</code> ファイルは、 <code>bin</code> 、 <code>sys</code> 、または <code>system</code> によってグループ所有されなければなりません。	位置 <code>/etc/security/psccexpert/dodv2/chowndodfiles</code> 準拠アクション 確実に、指定されたファイルが <code>bin</code> 、 <code>sys</code> 、または <code>system</code> によってグループ所有されるようにします。
AIX00320	<code>/etc/ftpaccess.ctl</code> ファイルは <code>root</code> が所有している必要があります。	位置 <code>/etc/security/psccexpert/dodv2/chowndodfiles</code> 準拠アクション 確実に、指定されたファイルを <code>root</code> が所有するようにします。
AIX00330	<code>/etc/ftpaccess.ctl</code> ファイルは、 <code>bin</code> 、 <code>sys</code> 、または <code>system</code> によってグループ所有されなければなりません。	位置 <code>/etc/security/psccexpert/dodv2/chowndodfiles</code> 準拠アクション 確実に、指定されたファイルが <code>bin</code> 、 <code>sys</code> 、または <code>system</code> によってグループ所有されるようにします。

表 3. 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
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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。

表 3. 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
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/pscxpert/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/pscxpert/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/pscxpert/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。
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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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。

表 3. 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
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/pscxpert/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/pscxpert/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/pscxpert/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。
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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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。

表 3. 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
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/pscxpert/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/pscxpert/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/pscxpert/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。
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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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。

表 3. 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
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/psccexpert/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/psccexpert/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/psccexpert/dodv2/ chowndodfiles /etc/security/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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。

表 3. DoD の所有権の要件 (続き)

米国防総省の 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
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/pscxpert/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/pscxpert/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/pscxpert/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。
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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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。

表 3. DoD の所有権の要件 (続き)

米国防総省の 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
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つて はなりません。	位置 /etc/security/pscxpert/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/pscxpert/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/pscxpert/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。
GEN003160	Cron ロギングが実装されなければなりませ ん。	位置 /etc/security/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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。

表 3. DoD の所有権の要件 (続き)

米国防総省の 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
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/pscxpert/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/pscxpert/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/pscxpert/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。
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/pscxpert/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/pscxpert/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/pscxpert/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ませ ん。	位置 /etc/security/pscxpert/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。

表 3. DoD の所有権の要件 (続き)

米国防総省の 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
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/pscxpert/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/pscxpert/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/pscxpert/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。
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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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。

表 3. 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
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/psccexpert/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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 3. 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
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/pscxpert/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/pscxpert/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/pscxpert/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。
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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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・ディレクトリはすべて、root が所 有している必要があります。	位置 /etc/security/pscxpert/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 3. 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
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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/dodv2/ chowndodfiles 準拠アクション 確実に、指定されたディレクトリが 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/psccexpert/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。

表 3. 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
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/pscxpert/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/pscxpert/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/pscxpert/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。
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/pscxpert/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. 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/netsh.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/pscxpert/dodv2/ fpmddodfiles 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.txt 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/pscxpert/dodv2/ fpmddodfiles 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/pscxpert/dodv2/ fpmddodfiles 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 4. 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
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/pscxpert/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/pscxpert/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。
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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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 4. 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
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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 4. 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
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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 4. 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
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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 4. 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
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/psccexpert/dodv2/ fpmddodfiles 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/psccexpert/dodv2/ fpmddodfiles 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。
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/psccexpert/dodv2/ fpmddodfiles 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/psccexpert/dodv2/ fpmddodfiles 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/psccexpert/dodv2/ fpmddodfiles 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/psccexpert/dodv2/ fpmddodfiles 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/psccexpert/dodv2/ fpmddodfiles 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。

表 4. 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
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/psccexpert/dodv2/ fpmddfiles 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/psccexpert/dodv2/ fpmddfiles 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。
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/psccexpert/dodv2/ fpmddfiles 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/psccexpert/dodv2/ fpmddfiles 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/psccexpert/dodv2/ fpmddfiles 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/psccexpert/dodv2/ fpmddfiles 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/psccexpert/dodv2/ fpmddfiles 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 4. ファイル許可に関する DoD 標準 (続き)

米国防総省の 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
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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 4. 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
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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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 4. 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
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/psccexpert/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/psccexpert/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。
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/psccexpert/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/psccexpert/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 5. 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/netshvc.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/psccexpert/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 5. 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
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/psccexpert/dodv2/ acltodfiles 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。
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/psccexpert/dodv2/ acltodfiles 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/psccexpert/dodv2/ acltodfiles 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/psccexpert/dodv2/ acltodfiles 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 5. DoD アクセス制御リスト (ACL) の要件 (続き)

米国防総省の 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
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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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 5. 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
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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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 5. DoD アクセス制御リスト (ACL) の要件 (続き)

米国防総省の 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
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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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 5. 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
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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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 5. DoD アクセス制御リスト (ACL) の要件 (続き)

米国防総省の 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
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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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 5. 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
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/psccexpert/dodv2/ acltodfiles 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。
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/psccexpert/dodv2/ acltodfiles 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/psccexpert/dodv2/ acltodfiles 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/psccexpert/dodv2/ acltodfiles 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 5. DoD アクセス制御リスト (ACL) の要件 (続き)

米国防総省の 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
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/psccexpert/dodv2/ aclododfiles 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。
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/psccexpert/dodv2/ aclododfiles 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/psccexpert/dodv2/ aclododfiles 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/psccexpert/dodv2/ aclododfiles 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 5. 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
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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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 5. DoD アクセス制御リスト (ACL) の要件 (続き)

米国防総省の 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
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/psccexpert/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。
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/psccexpert/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/psccexpert/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/psccexpert/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 5. 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
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/psccexpert/dodv2/ aclododfiles 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。
GEN005395	/etc/syslog.conf ファイルには、拡張 ACL があ ってではありません。	位置 /etc/security/psccexpert/dodv2/ aclododfiles 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 ってではありません。	位置 /etc/security/psccexpert/dodv2/ aclododfiles 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 がなくてではありません。	位置 /etc/security/psccexpert/dodv2/ aclododfiles 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 5. DoD アクセス制御リスト (ACL) の要件 (続き)

米国防総省の 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
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/psccexpert/dodv2/ aclododfiles 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。
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/psccexpert/dodv2/ aclododfiles 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/psccexpert/dodv2/ aclododfiles 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/psccexpert/dodv2/ aclododfiles 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 5. 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
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/psccexpert/dodv2/ acltodfiles 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。
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/psccexpert/dodv2/ acltodfiles 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・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、`pscxpert` 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が必要にする。

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・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/psccexpert/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 6. 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/psccexpert/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/psccexpert/bin/chusrattr

表 6. 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/pscxpert/bin/chusrattr
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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/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/pscxpert/bin/chusrattr

表 6. 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 8.5.13 PCI バージョン 3 8.1.6	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/pscxpert/bin/chusrattr
PCI バージョン 2 8.5.13 PCI バージョン 3 8.1.6	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/pscxpert/bin/chdefstanza • /etc/security/login.cfg
PCI バージョン 2 8.5.14 PCI バージョン 3 8.1.7	ロックアウトの期間を少なくとも 30 分、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/pscxpert/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・テクノロジーを活性化すること。	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性化でき、作業が完了したら非活動化できます。	• /etc/security/pscxpert/bin/chuserstanza • /etc/security/user
8.1.1	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/pscxpert/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/pscxpert/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	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/pscxpert/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/pscxpert/bin/rctcpip

表 6. 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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/bin/rctcpip

表 6. 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	rshtd 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。	rshtd 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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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。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/psccexpert/bin/cominetdconf

表 6. 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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/bin/cominetdconf

表 6. 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/psccexpert/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/psccexpert/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。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/psccexpert/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/psccexpert/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/psccexpert/bin/cominetdconf

表 6. 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 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/psccexpert/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 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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/bin/cominetdconf

表 6. 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	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/pscxpert/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/pscxpert/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 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/pscxpert/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/pscxpert/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/pscxpert/bin/cominetdconf

表 6. 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	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/psccexpert/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	tttdbserver 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。	tttdbserver 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/psccexpert/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/psccexpert/bin/cominetdconf
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・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/psccexpert/bin/rmsuidfrmcmds
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・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・レベルを使用可能にします。	/etc/security/psccexpert/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・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/psccexpert/bin/nfsconfig

表 6. 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 2.2.2 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/psccexpert/bin/dismtdmns
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/psccexpert/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/psccexpert/bin/rmetchostsequiv
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/psccexpert/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/psccexpert/bin/ntwkopts

表 6. 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
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/psccexpert/bin/ ipsecshunhostls 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、ipsecshunhostls.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/psccexpert/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、ipsecshunhostls.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。
7.1.1	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/psccexpert/bin/chusrattr
7.1.1	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/psccexpert/bin/limitsysacc
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/psccexpert/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/psccexpert/bin/ rmdotfrmpathnroot

表 6. 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
2.2.3	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/psccexpert/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/psccexpert/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/psccexpert/bin/sedconfig
8.2	ルートのパスワードが弱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/psccexpert/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/psccexpert/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/psccexpert/bin/tcptr_psccexpert
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 (IPSec) トンネル作成の自動化を使用可能にします。	/etc/security/psccexpert/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/psccexpert/bin/ipsecpermithostorport
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、および保護を行うことにより、システム保全性を維持します。	/etc/security/psccexpert/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/psccexpert/bin/EnableRbac

表 6. 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	安全でないといみなされ 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/psccexpert/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/psccexpert/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/psccexpert/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/psccexpert/bin/sshPCIconfig

表 6. 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/psccexpert/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 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/psccexpert/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/psccexpert/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、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/psccexpert/bin/sshPCIconfig

表 6. 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、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/psccexpert/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/psccexpert/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/psccexpert/bin/rctcpip
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/psccexpert/bin/disableacctpci
PCI バージョン 3 2.2.3	アプリケーション内で Secure Sockets Layer (SSL) v3 および Transport Layer Security (TLS) v1.0 を無効にします。	Courier POP3 サーバー (Pop3d) 構成内で SSLv3 および TLS v1.0 を無効にします。	/etc/security/psccexpert/bin/disableSSL
PCI バージョン 3 2.2.3	アプリケーション内で SSL v3 および TLS v1.0 を無効にします。	Courier IMAP サーバー (imapd) 内で SSLV3 および TLS v1.0 を無効にします。	/etc/security/psccexpert/bin/disableSSL

表 6. 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 3 8.2.1	アプリケーション内で SSL v3 および TLS v1.0 を無効にします。	Network Time Protocol (NTP) 構成ファイルで、TLS 1.1 以降のセキュリティ適 用を検査します。	/etc/security/psccexpert/bin/checkNTP
PCI バージョン 3 2.2.3	アプリケーション内で SSL v3 および TLS v1.0 を無効にします。	ファイル転送プロトコル・デ ーモン (FTPD) 構成ファイル で、TLS 1.1 以降のセキュリ ティー適用を検査します。	/etc/security/psccexpert/bin/secureFTP
PCI バージョン 3 2.2.3	アプリケーション内で SSL v3 および TLS v1.0 を無効にします。	ファイル転送プロトコル (FTP) 構成ファイルで、TLS 1.1 以降のセキュリティ適 用を検査します。	/etc/security/psccexpert/bin/secureFTP
PCI バージョン 3 2.2.3	アプリケーション内で SSL v3 および TLS v1.0 を無効にします。	sendmail 構成内で SSLv3 お よび TLS v1.0 を無効にしま す。	/etc/security/psccexpert/bin/ sendmailPCIConfig
PCI バージョン 3 2.2.3	アプリケーション内で SSL v3 および TLS v1.0 を無効にします。	AIX 上の SSL バージョンが 1.0.2 よりも新しいかどうかを 検査します。	/etc/security/psccexpert/bin/sslversion
PCI バージョン 3 8.2.1	2 要素認証を強制しま す。	2 要素認証 (SHA-256 や SHA-512 など) を強制しま す。	/etc/security/psccexpert/bin/pwdalgchk

関連情報:

 Payment Card Industry - Data Security Standard への準拠

Sarbanes-Oxley 法令および COBIT への準拠

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

SOX のセクション 404 では、内部統制に対する管理評価を義務付けています。大半の組織では、内部統制の範囲は、会社の財務データを処理および報告する情報技術システムにまで及びます。SOX 法は、IT および IT セキュリティーに関する具体的な詳細を規定します。多くの SOX 監査員は、適切な IT ガバナンスおよび統制を測定および監査する方法として、COBIT などの規格を使用します。PowerSC 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に設計されています。

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に設計されており、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・プロファイルです。

HIPAA セキュリティ・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・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・ルールに従わなければなりません。

HIPAA セキュリティ・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・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・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/psccexpert/bin` ディレクトリにあります。

表 7. 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・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・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。

表 7. 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、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。
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。

表 7. 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。	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。
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。

表 7. 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。	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。
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。

表 7. 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。	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: <pre>grep TMOUT= /etc/security /profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}</pre> 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。
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。CHKEEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL, TE=ON 例えば、次のとおりです。trustchk -p TE=ON CHKEEXEC = 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: <pre># lsipp -l grep openssh > /dev/null 2>&1</pre> 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 8. 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: <pre>errpt -d H</pre> 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。

表 8. HIPAA 機能および実装の詳細 (続き)

HIPAA 機能	実装仕様	aixpert の実装	コマンドおよび戻り値
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/psccexpert/bin/RbacEnablement.

関連情報:

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

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 9. 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 <code>set-user identification (SUID)</code> 属性と <code>set-group identification (SGID)</code> 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。	<code>/etc/security/psccexpert/bin/filepermgr</code> <code>/etc/security/psccexpert/bin/rmsuidfrmrmscmds</code>

表 9. 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-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/pscxpert/bin/EnableRbac
CIP-005-3a R2.1-R2.4	セキュリティ・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/pscxpert/bin/sshstart
CIP-005-3a R2.5 CIP-007-5 R1.1	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/pscxpert/bin/comntrows
CIP-005-3a R2.5 CIP-007-5 R1.1	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/pscxpert/bin/rctcpip

表 9. 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 CIP-007-5 R1.1	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 • tttdbserver 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 CIP-007-5 R1.1	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 CIP-007-5 R4.4	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-007-3a R3 CIP-007-5 R2.1	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 CIP-007-5 R3.3	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 9. 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/pscxpert/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/pscxpert/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/pscxpert/bin/chusrattr
CIP-007-5 R5.5.1	各パスワードを 8 文字以上に設定します。	/etc/security/pscxpert/bin/chusrattr
CIP-007-3a R5.3.2 CIP-007-5 R5.5.2	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/pscxpert/bin/chusrattr
CIP-007-3a R5.3.3 CIP-007-5 R5.6	各パスワードを年 1 回変更します。	/etc/security/pscxpert/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/pscxpert/bin/GeneralMsg
CIP-007-5 R5.7	認証の試みの失敗回数を制限します。	/etc/security/pscxpert/bin/chusrattr
CIP-010-1 CIP-010-2 R2.1	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/pscxpert/bin/GeneralMsg

関連情報:

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

セキュリティ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・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・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>Implements portions of PCI Section 8.2,
Check group definitions: Verifies the correctness of group definitions
and fixes the errors
</AIXPertDescription
<AIXPertPrereqList>>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・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・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・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 10. 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	米国防総省の <i>UNIX Security Technical Implementation Guide</i>
% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml	<i>Health Insurance Portability and Accountability Act</i>
% pscxpert -f /etc/security/aixpert/custom/PCI.xml	<i>Payment Card Industry-Data Security Standard</i>
% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml	<i>Sarbanes-Oxley Act of 2002</i> (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・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. 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	米国防総省の <i>UNIX Security Technical Implementation Guide</i>
% viosecure -file /etc/security/aixpert/custom/Hipaa.xml	<i>Health Insurance Portability and Accountability Act</i>
% viosecure -file /etc/security/aixpert/custom/PCI.xml	<i>Payment Card Industry-Data Security Standard</i>
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	<i>Sarbanes-Oxley Act of 2002</i> (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・プロファイルデータをデータ・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:

105 ページの『セキュリティ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 リアルタイム・コンプライアンス

PowerSC リアルタイム・コンプライアンス 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 リアルタイム・コンプライアンス 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構成ポリシーの違反が発生した場合、PowerSC リアルタイム・コンプライアンス 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 リアルタイム・コンプライアンス フィーチャーは、受動的なセキュリティ・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 リアルタイム・コンプライアンス のインストール

PowerSC リアルタイム・コンプライアンス 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 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. PowerSC Standard Edition 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 Standard Edition 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 リアルタイム・コンプライアンス の構成

PowerSC リアルタイム・コンプライアンス 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 リアルタイム・コンプライアンス 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 リアルタイム・コンプライアンス 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 リアルタイム・コンプライアンス フィーチャーは、ハイレベル・セキュリティ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、システムを再起動せずに変更がモニターされます。

PowerSC リアルタイム・コンプライアンス に対するアラートの設定

PowerSC リアルタイム・コンプライアンス 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 リアルタイム・コンプライアンス 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 Profile Manager 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・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:

118 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:

118 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 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.vtvm** 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:

117 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」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 12. 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。 <pre>ssh ptsc@hostname</pre> 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。 <pre>ptsc -i</pre>
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 12. 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。
対話式的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:

114 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。

113 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・システムの間で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。

122 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。

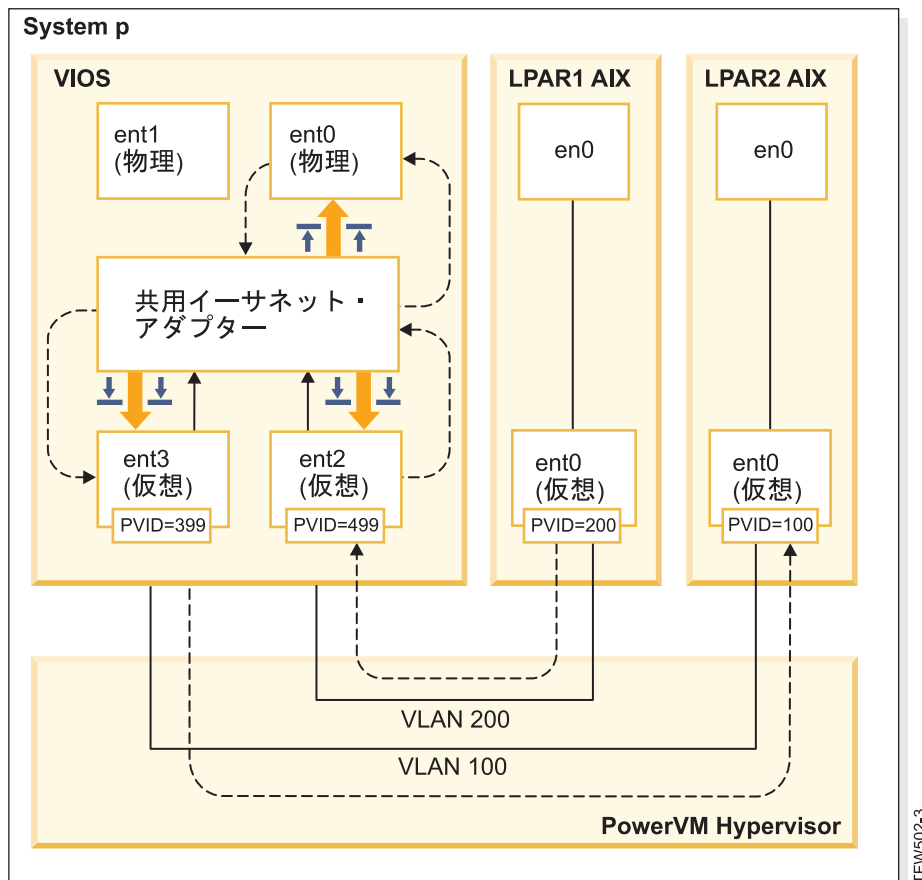


図 1. トラステッド・ファイアウォールを使用しない、VLAN 間の情報転送の例

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、123 ページの図 2 に示されています。

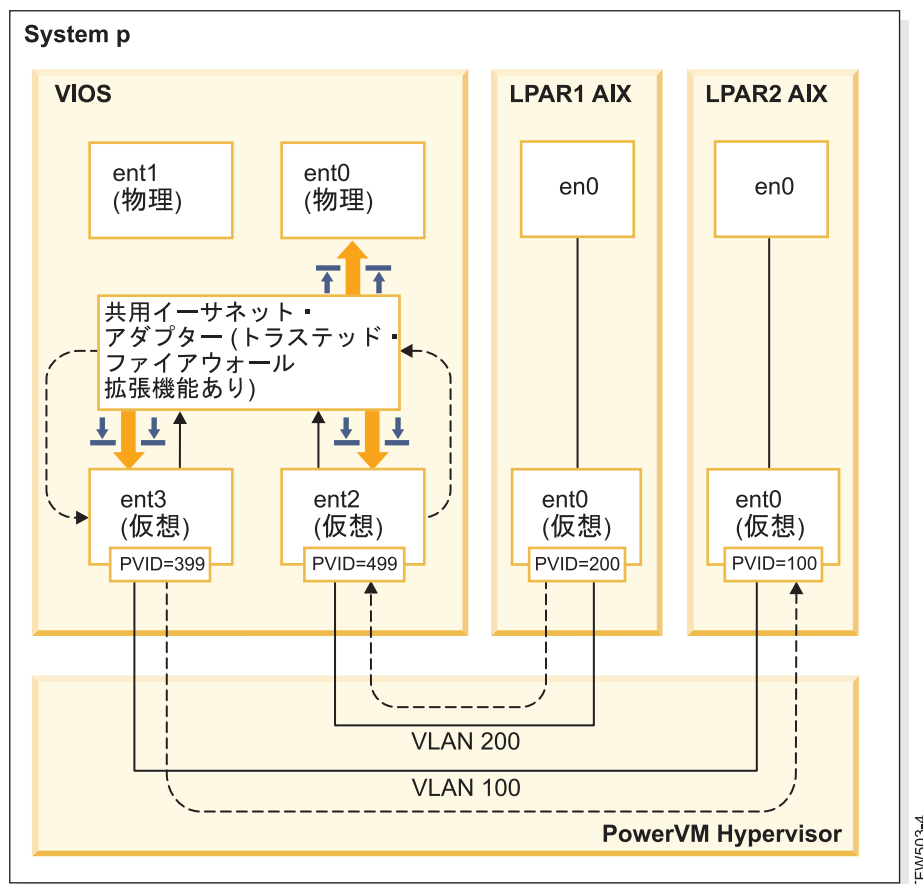


図 2. トラステッド・ファイアウォールを使用した、VLAN 間の情報転送の例

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、以下のようになります。

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 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・アドバイザが、トラフィックを内部的にルーティングすることによって効率性が改善されると判断した場合、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。

126 ページの図 3 では、複数の SEA を使用した環境を示します。

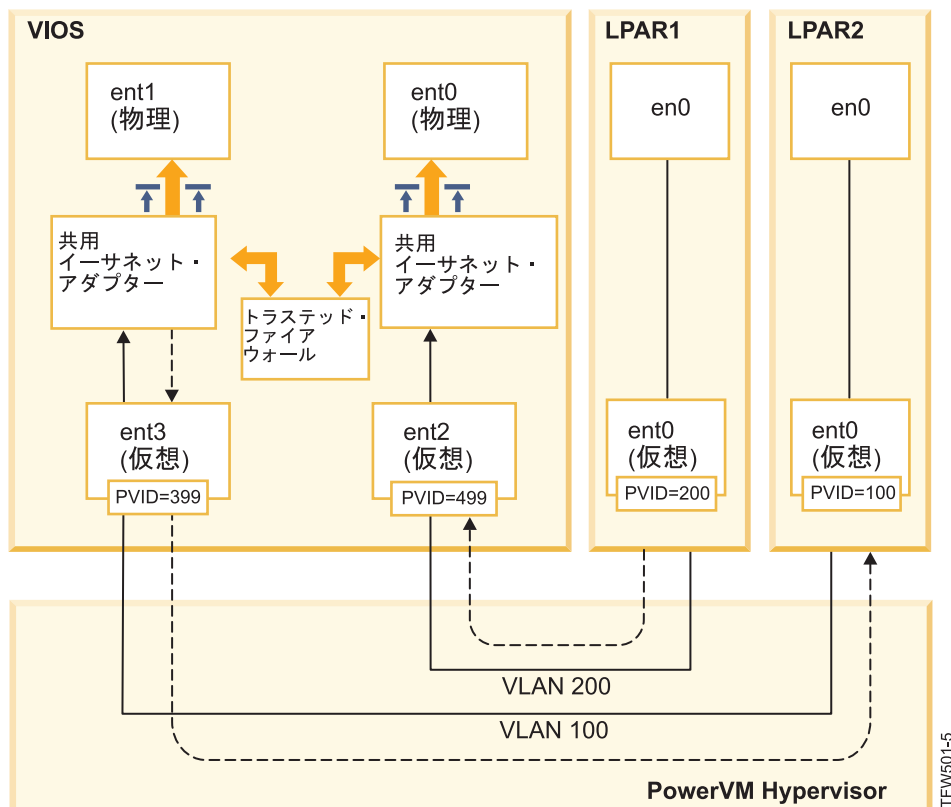


図 3. 単一の VIOS 上で複数の共用イーサネット・アダプターを使用する構成

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 ドライバーを初期化します。

```
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 (1 行で) 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 -0 gt -P 23
```

注: 1 つのフィルター・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 -0 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 -0 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 -0 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を使用できます。

- 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:

178 ページの『genvfilt コマンド』

180 ページの『mkvfilt コマンド』

202 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 トピックス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:

127 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:

180 ページの『lsvfilt コマンド』

201 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と同じです (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、v1 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 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、132 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、132 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 デーモンを再始動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:

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 (TNC)

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 (TNC) には以下の 4 つのコンポーネントがあります。

- TNC サーバー
- TNC パッチ管理
- TNC クライアント
- TNC の IP リファラー

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 (TNC) 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。

TNC 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、サービス更新管理アシスタント (SUMA) および cURL と統合して、パッチ管理ソリューションを提供します。

パッチ・マネージャーは、IBM ECC および Fix Central Web サイトで入手可能な最新のサービス・パッチ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 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。

↓ 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するために、このデーモンは、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。

↓ パッチ管理は、以下のいずれかの方法で提供されます。

- ↓ コマンド・ライン・インターフェース (**pmconf**) を使用する
- ↓ デーモン (**tncpmd2**) を使用する

↓ コマンド・ライン・インターフェース (**pmconf**) を使用したパッチ管理の提供:

↓ **pmconf add** コマンドを使用してサービス・パック・レベル (SP レベル) をダウンロードすると、SUMA および cURL が呼び出されます。

↓ **pmconf add** コマンドを使用してサービス・パック・レベル (SP レベル) をダウンロードすると、SUMA が呼び出され、SP レベルがダウンロードされて TNC に登録されます。また、cURL が呼び出され、新規セキュリティや欠落しているセキュリティ・フィックスがすべてダウンロードされます。

↓ 以下の **pmconf get** コマンド引数により、セキュリティ・フィックスの管理をさらに制御できます。

- ↓ **display-only** により、ユーザーは、SP レベルで適用可能なセキュリティ・フィックスによって解決される脆弱性の説明を調べることができます。このコマンドを使用しても、セキュリティ・フィックスはダウンロードされません。
- ↓ **download-only** により、ユーザーは、セキュリティ・フィックスを、適用することなく、ユーザー指定のダウンロード・ディレクトリにダウンロードできます。フィックスは適用されません。

↓ デーモン (**tncpmd2**) を使用したパッチ管理の提供:

↓ デーモンのスケジューラー・コンポーネントは、TNC クライアントのセキュリティに影響する更新について自動的に検査するように構成できます。

↓ ダウンロード間隔により、スケジューラーが新規サービス・パック・レベルがないかを検査する頻度が制御されます。TNC に現在登録されているテクノロジー・レベル (TL) の新規サービス・パック・レベルが検出された場合、新規サービス・パック・レベルと、欠落しているセキュリティ・フィックスや新規セキュリティ・フィックスがすべてダウンロードされ、リポジトリに追加されます。ダウンロード間隔は、**pmconf init** コマンドを使用して設定します。推奨値は、1 カ月に 1 回以上 (43,200 分) です。

↓ 「ifix_download_interval」により、公開された新規セキュリティ暫定修正がないかをスケジューラーが検査する頻度が制御されます。新規セキュリティ・フィックスがあった場合、ダウンロードされてリポジトリに追加されます。推奨される ifix ダウンロード間隔は、1 日に 1 回 (1440 分) です。

↓ トラストッド・ネットワーク接続クライアント

↓ トラストッド・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 (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、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® ファミリー 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: クライアントに OS レベルおよびファイルセット情報を要求して、それをベースライン情報と比較します。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:

186 ページの『psconf コマンド』

TNC の要件

各 TNC コンポーネントのすべてのフィーチャーを完全に使用するには、ご使用の環境で最小要件が使用可能であることを確認する必要があります。

TNC パッチ管理

AIX	SUMA	OpenSSL	注記
7.2 TL1	7.2.1.0	1.0.2	OS に付属
7.2 TL0	7.2.1.0	1.0.2	SUMA/Java を別途インストールする必要があることがあります。
7.1 TL4	7.2.1.0	1.0.2	SUMA/Java を別途インストールする必要があることがあります。
7.1 TL1, TL2, TL3			AIX 7.2 サービス・パック・レベルのダウンロードのサポートなし
7.1 TL0			TNCPM でサポートされる最小リリース・レベル

TNC コンポーネントのセットアップ

各トラステッド・ネットワーク接続 (TNC) コンポーネントでは、お客様固有の環境で実行するために、セットアップが必要です。

TCN コンポーネントをセットアップするために、以下の手順の各ステップが必要です。

1. TNC サーバー、TNC 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システムの IP アドレスを確認します。

| 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。TNCPM サーバーとして構成されるシステムは NIM マスターです。sets:bos.sysmgmt.nim.master ファイル・セットがこのシステムにインストールされている必要があります。

| 3. 新規サービス・バックおよびセキュリティ・フィックスを TNC サーバーに自動的に通知するために、Autonomic Health Advisor (AHA) を有効にする必要があります。AHA が有効になっていない場合、TNC スケジューラーが、スケジュールされた間隔で TNC サーバーを更新します。自動通知のために AHA を有効にするには、以下のようになります。

```
| mkdir /aha  
| /usr/sbin/mount -v ahafs /aha /aha
```

| 4. TNC パッチ管理用のフィックス・リポジトリを初期化するには、次のコマンドを (1 行で) 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・リポジトリは、/var/tnc/tncpm/fix_repository ファイル内です。別のディレクトリを指定するには、**-P** フラグを使用します。

| 5. TNCPM サーバーをセットアップします。TNCPM サーバーは、NIM システムでセットアップできます。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。TNCPM サーバーは、cURL を使用して IBM セキュリティ・サイトから ifix 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:

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

| 6. 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、144 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。

| 7. 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:

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

| 8. 各コンポーネントのオプション・ステップを実行して、TNC コンポーネントのセットアップを実行します。

| 関連資料:

| 186 ページの『psconf コマンド』

| 関連情報:

| 7 ページの『PowerSC Standard Edition 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

| **TNC コンポーネントのオプションの構成**

| 各 TNC コンポーネントの 1 つ以上のオプションを構成できます。

| **トラステッド・ネットワーク接続 (TNC) サーバーのオプションの構成**

| 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/tncs.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:

| 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 で、pmserver ポートに使用されるデフォルト
| 値は 38240 です。

| 関連資料:

| 186 ページの『psconf コマンド』

| **トラステッド・ネットワーク接続 (TNC) クライアントの追加オプションの | 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/tncs.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:

| 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:
- | 186 ページの『psconf コマンド』

| TNC パッチ管理サーバーのオプションの構成

- | トラステッド・ネットワーク接続マネージャー (TNCMP) サーバーは、SUMA および cURL 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。
- | TNC クライアントを更新できるように、TNCMP 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。
- | 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・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

| TNCPM オープン・パッケージ・リポジトリを管理するには、以下のコマンドの 1 つ以上を入力します。

```
| pmconf add -o <package name> -V <version> -T [installp|rpm] -D <User defined path>
| pmconf delete -o <package name> -V <version>
| pmconf list -o <package name> -V <version>
| pmconf list -O [-c] [-q]
```

| オープン・パッケージが、次のデフォルト・ディレクトリーに追加されます。

| `/var/tnc/tncpm/fix_repository/packages`

| ユーザー定義のパス = システム上のパッケージ・ロケーション

| 特定のサービス・パック・レベルのセキュリティー・フィックスによって対応される記述情報を表示するが、フィックスをリポジトリに適用しない場合は、以下のコマンドを入力します。

| `pmconf get -L -p <SP>`

| 例:

| `pmconf get -L -p 7200-01-01`

| 特定のサービス・パック・レベルのセキュリティー・フィックスをダウンロードするが、フィックスをリポジトリに適用しない場合は、以下のコマンドを入力します。

| `pmconf get -p <SP> -D <download directory>`

| 注: このコマンドを実行する前に、`download directory` が存在している必要があります。

| 例:

| `pmconf get -p 7200-01-01 -D /tmp/ifixes_7200-01-01`

| 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** コマンドをサポートします。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、すべてのクライアント更新が含まれたログも保持します。

| 関連資料:

| 186 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:

| `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:

| `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:

| 186 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/tncs.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:

| `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。

| 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:

| `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。

| 関連資料:

| 186 ページの『psconf コマンド』

| トラステッド・ネットワーク接続 (TNC) コンポーネントの管理

| 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する方法について説明します。

| 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、次の **psconf** コマンドを実行します。

| `psconf list -H -i <ip |ALL>`

| 関連資料:

| 186 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ます、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:

| `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> <rel100-TL-SP>`

```
| 例:
| 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:
| 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:
| psconf add -P mypol fspolicy=myfspol,myfspol1

| OpenPackage ポリシーを追加するには、次のコマンドを入力します。
| pconf add -O <openpkggrp> <openpkgname:version>

| OpenPackage ポリシーを追加するときの例:
| psconf add -O opengrp2 openssl:1.0.1.516

| OpenPackage ポリシーを Fspolicy に割り当てるには、次のコマンドを入力します。
| psconf add -O opengrp2 fspolicy=fspolicy1

| 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:
| 186 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。

```
| pconf 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:

┆ 186 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:

┆ 186 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:

┆ `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。

┆ クライアントをオープン・パッケージで更新するには、次のコマンドを入力します。

┆ `psconf update -i <ip> -O.opengrp2`

┆ 関連資料:

┆ 186 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:

| `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:

| 181 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 (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:

| 186 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・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・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・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}`

登録済みオープン・ソース・パッケージのリストを表示するには、次の `report` コマンドを入力します。

`psconf report -O ALL -o TEXT`

関連資料:

186 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 13. 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。 - 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。 <code>ps -eaf grep tnccsd</code> - 実行されていない場合は、<code>/var/tnc/.tncsock</code> ファイルを削除します。 - 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 <code>/etc/tnccs.conf</code> 構成ファイルで <code>component = SERVER</code> エントリーがあるか確認します。

表 13. 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 (続き)

問題	解決方法
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。 <code>ps -eaf grep tncpmd</code> - TNC パッチ管理サーバーの <code>/etc/tncss.conf</code> 構成ファイルで <code>component = TNCPM</code> 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。 <code>ps -eaf grep tnccsd</code> <code>/etc/tncss.conf</code> 構成ファイルで TNC クライアントに関する <code>component = CLIENT</code> 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。 <code>ps -eaf grep tnccsd</code> - VIOS の <code>/etc/tncss.conf</code> 構成ファイルで <code>component = IPREF</code> 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。 <code>/etc/tncss.conf</code> ファイルで <code>level=info</code> 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 グラフィカル・ユーザー・インターフェース (GUI)

このセクションでは、IBM PowerSC グラフィカル・ユーザー・インターフェース (GUI) について説明します。このインターフェースをインストール、保守、および使用方法に関する情報があります。

IBM PowerSC GUI は、コマンド・ラインとログ・ファイルとの対話に代わる手段を提供することによって、PowerSC Standard Edition 製品のユーザビリティを向上させます。PowerSC GUI には、エンドポイントとそれらの状況の視覚化、コンプライアンス・レベルの適用、元に戻す操作、または検査、コンプライアンス・レベル・アクションのアプリケーションのシステムのグループ化、およびコンプライアンス構成プロファイルの表示およびカスタマイズのための中央管理コンソールが用意されています。

PowerSC GUI には、ファイル保全性モニタリング (FIM) も含まれています。FIM には、リアルタイム・コンプライアンス (RTC) とトラステッド実行 (TE) があります。PowerSC GUI を使用して、RTC および TE を構成し、リアルタイムのイベントを表示できます。PowerSC GUI には、豊富なプロファイル編集およびレポート作成機能も用意されています。

PowerSC GUI の概念

PowerSC GUI を使用する前に、セキュリティおよびエンドポイント・ディスカバリーに関する一般的な概念を理解しておく必要があります。

PowerSC GUI セキュリティー

PowerSC GUI には、それぞれが AIX エンドポイント上にある PowerSC GUI サーバーと PowerSC GUI エージェントとの間の双方向 HTTPS 通信を使用したセキュリティが用意されています。

TLS ハンドシェイク・プロセスでは、PowerSC GUI サーバーと PowerSC GUI エージェントの両方で有効な証明書が使用されます。PowerSC GUI エージェントまたは PowerSC GUI サーバーのどちらかが通信を開始しているため、TLS ハンドシェイク・プロセスは、どちらの方向でも単一認証をサポートします。エージェントは、最初の接続の間に PowerSC GUI サーバーに送信される nonce (乱数) を作成します。その後、PowerSC GUI サーバーはこの nonce を、そのエージェントに送信されるコマンドすべてに組み込みます。この nonce は、信頼できる PowerSC GUI サーバーから送信されたコマンドが実行されているというもう 1 つの確認のレイヤーをエンドポイント・エージェントに提供します。エンドポイントは、Web サービス呼び出しのソースが信頼できるものであることを確認する必要があります。最初のハンドシェイクと nonce で、この信頼が保証されます。

PowerSC GUI エージェントと PowerSC GUI サーバーとの間の通信はすべて、保護対象システムのセキュリティ要件との整合性を持つプロトコルおよび暗号スイートによって暗号化されます。現在、プロトコル・レベルは TLS 1.2 です。PowerSC GUI サーバーは、すべての PowerSC GUI エージェントと、またすべての PowerSC GUI ユーザーと対話を行います。そのため、PowerSC GUI サーバーには、ユーザーの Web ブラウザーによる接続のすべてによって信頼される証明書が必要です。例えば、ウェルノウン認証局 (Verisign など) から取得した証明書や、内部的に信頼できる認証局から取得した証明書です。

インストールの間に、PowerSC GUI サーバーは、それ自体が使用するための自己署名証明書を作成します。この証明書は無期限で使用できますが、一時的に使用されることを目的にしているため、ユーザー指定の広く認識される証明書で置き換えてください。PowerSC GUI サーバー・インストールでは、すべてのエンドポイント証明書に署名するために使用される署名証明書も作成されます。

各エンドポイントのトラストストア・ファイルは、インストール・プロセスによって自動的に作成されます。このトラストストア・ファイルはどのエンドポイントでも同じものであるため、PowerSC GUI サーバーからそれぞれのエンドポイントにコピーする必要があります。PowerSC GUI サーバーとエンドポイントの両方における、この証明書の組み合わせによって、ハイレベルの通信セキュリティが実現します。

- | UNIX グループを使用すると、これ以上のセキュリティ管理が可能です。PowerSC GUI にログインするためには、LDAP ユーザーやオペレーティング・システムによって定義されているローカル・ユーザーなどのいずれのユーザーも、指定された UNIX グループのメンバーでなければなりません。管理者は、
- | **pscuiserectl** コマンドを使用して、グループ・メンバーシップを設定または変更できます。

ログインした後、表示専用モードに制限されている場合があります。ユーザー権限機能を使用すると、UNIX グループ・メンバーシップによって制御されているエンドポイントに対してアクションを実行できます。アクションを実行するためには、エンドポイントの管理を許可されている UNIX グループのメンバーでなければなりません。詳しくは、トピック『ユーザー・アカウントのセットアップ』を参照してください。

デフォルトでは、セキュリティ・グループのメンバーであるユーザーはすべて、PowerSC GUI に表示されるエンドポイントすべてを管理できます。PowerSC 管理者は、個別のエンドポイント・レベルへのユーザー・アクセスを **setGroups.sh** コマンドで制限できます。

- | 管理ユーザーのみが実行できるさまざまな構成コマンドがあります。例としては、グローバル E メール設定の変更機能や新規プロファイルの作成機能があります。管理ユーザー権限は、UNIX グループを使用して設定され、**pscuiserectl** コマンドを使用して構成できます。

エンドポイントの内容をコンプライアンス・ページに取り込む

PowerSC GUI サーバーと PowerSC GUI エージェントはエンドポイントとの通信を行って、コンプライアンス・レベルを検出します。

始動時に、また成功するまで断続的に、エージェントは PowerSC GUI サーバーとの接続を開始しようと試みます。接続が確立されると、一回限りのエージェント/サーバー・セキュリティ・ハンドシェークが実行されます。エージェント/サーバー・セキュリティ・ハンドシェークが初めて正常に折衝された後、サーバーは、エンドポイントの内部表記として固有 ID (UID) を持つドメイン・エレメントを作成し、その UID をエンドポイントに戻します。その後、この UID は、エージェントからサーバーへのすべての通信に組み込まれます。このアクションで、ディスカバリー・プロセスが完了します。PowerSC GUI サーバーとエンドポイントは、どちらの方向においてもセキュア通信を行うことができます。

最初のディスカバリー・ハンドシェークが完了した後、または PowerSC GUI エージェントが再始動した後、PowerSC GUI エージェントは、そのエンドポイントの現在のコンプライアンス状況情報を判別しようと試み、PowerSC GUI サーバーを更新します。エンドポイントおよび現在のコンプライアンス情報があれば、その情報が PowerSC GUI のコンプライアンス状況ページに取り込まれます。コンプライアンス状況情報を判別できないと、このエントリはコンプライアンス状況ページで使用不可になります。

PowerSC GUI サーバーには、認識されているエンドポイント (最初のエージェント/サーバー接続および通信の結果として自動的に作成されるエンドポイント) すべての表記が入っています。エンドポイント・エージェントはエンドポイントのコンプライアンス状況の変更をトラッキングするため、それらの変更はサーバーに渡され、保存されます。PowerSC GUI からのすべてのユーザーのエンドポイントとの対話は、PowerSC GUI サーバーを介して行われます。ユーザー・インターフェースが直接、エンドポイントやエンドポイント・エージェントと対話することはありません。

PowerSC GUI のインストール

PowerSC GUI エージェントおよび PowerSC GUI サーバー・コンポーネントは、PowerSC Standard Edition のインストール時にインストールされます。installp ファイル・セットからそれぞれがインストールされます。

PowerSC GUI エージェント

PowerSC GUI エージェントは、AIX エンドポイントごとにインストールされます。PowerSC GUI エージェントはエンドポイント上のアクティビティーをトラッキングして、その情報を PowerSC GUI サーバーに提供します。

また、PowerSC GUI エージェントは、PowerSC GUI から起動されたコマンドを実行します。PowerSC GUI エージェントと PowerSC GUI サーバーとの間の通信はすべて暗号化されています。

installp コマンドは、コア PowerSC Standard Edition 製品および PowerSC GUI エージェントをインストールします。powerscStd.uiAgent.rteinstallp ファイルセットが、PowerSC GUI エージェント・インストールに使用されます。次の例は、エンドポイントそれぞれで実行される installp コマンドを示しています。

注: この例では、インストーラー・イメージは /tmp/inst.images/ ディレクトリーに展開されます。

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiAgent.rte
```

PowerSC GUI サーバー

PowerSC GUI サーバーはどのような AIX システムでも稼働しますが、PowerSC GUI サーバーをインストールして実行する、専用の AIX LPAR サーバーを作成することをお勧めします。

installp コマンドは、コア PowerSC Standard Edition 製品および PowerSC GUI サーバーをインストールします。powerscStd.uiServer.rte installp ファイルセットが、PowerSC GUI サーバー・インストールに使用されます。次の例は、エンドポイントで実行される installp コマンドを示しています。

注: この例では、インストーラー・イメージは /tmp/inst.images/ ディレクトリーに展開されます。

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiServer.rte
```

PowerSC GUI 要件

PowerSC GUI のハードウェア要件とソフトウェア要件について説明します。

ハードウェア

- PowerSC GUI サーバー・コンポーネントは独立した LPAR に、または AIX 7.1 以降で稼働する VM にインストールする必要があります。
- PowerSC GUI エージェント・コンポーネントは、AIX エンドポイントごとにインストールする必要があります。

ソフトウェア

- PowerSC GUI サーバーには、AIX 7.1 以降が必要です。
- PowerSC GUI サーバーでは、sendmail デーモンが実行されている必要があります。
- PowerSC GUI において英語以外の言語でプロファイル・ルールの説明を正しく表示するには、ファイル・セット bos.loc.utf.<LANG> がインストールされている必要があります。

エンドポイントへのトラストストア・セキュリティ証明書の配布

システム管理者は、すべてのエンドポイントにトラストストアのセキュリティ証明書をデプロイする必要があります。

インストール時に、トラストストア・ファイルが作成されます。これは、すべてのエンドポイントで使用できます。ファイルの名前は、`endpointTruststore.jks` です。このファイルは、`/etc/security/powersc/uiServer/` ディレクトリー内にあります。

インストール後、`endpointtruststore.jks` ファイルを各エンドポイントに配置する必要があります。これにより、各エンドポイント上の PowerSC GUI エージェントが、PowerSC GUI サーバーと通信し、エンドポイントで鍵ストアを作成することになるプロセスを開始できます。

以下のいずれかの方法でトラストストア・ファイルを配布できます。

- `endpointTruststore.jks` ファイルを各エンドポイントに手動でコピーする。
- ご使用の環境で PowerVC (または別の仮想化マネージャー) を使用している場合、`endpointTruststore.jks` ファイルを PowerVC イメージに配置できます。PowerVC イメージがエンドポイントにデプロイされると、PowerSC GUI エージェントとトラストストア・ファイルの両方が組み込まれます。

いずれかの方法を使用して `endpointTruststore.jks` をデプロイした後、エンドポイントの実行が開始すると、PowerSC GUI エージェントはトラストストア・ファイルを使用して、PowerSC GUI サーバーが実行されている場所を判別します。次に、PowerSC GUI エージェントは、使用可能なモニター対象エンドポイントのリストの結合要求とともにメッセージを PowerSC GUI サーバーに送信します。

1 エンドポイントへのトラストストア・ファイルの手動でのコピー

システム管理者は、環境内の既存の各エンドポイントにトラストストア・ファイルを手動でコピーする必要があります。

トラストストア・ファイルは、追加された各新規エンドポイントにもコピーする必要があります。

注: PowerVC などのデータ仮想化マネージャーがある場合、PowerSC GUI エージェントとトラストストア・ファイルの両方が含まれたイメージを作成することで、トラストストア・ファイルを新規エンドポイントにコピーできます。155 ページの『仮想化マネージャーを使用したエンドポイントへのトラストストア・ファイルのコピー』を参照してください。

1. エンドポイント・トラストストア `/etc/security/powersc/uiServer/endpointTruststore.jks` ファイルを各エンドポイント上の `/etc/security/powersc/uiAgent/endpointTruststore.jks` ファイルにコピーするには、以下の `scp` コマンドを実行します。

```
# scp endpointTruststore.jks user@endpoint-host-name:  
/etc/security/powersc/uiAgent
```

2. セキュリティ証明書をインストールした後にエンドポイント・エージェントを再始動するには、エンドポイントで以下のコマンドを実行します。

```
stopsrc -s pscuiagent  
startsrc -s pscuiagent
```

3. 既存のエンドポイントごとに、および (データ仮想化マネージャーがない場合は) 新規エンドポイントを追加するごとに、ステップ 1 と 2 を繰り返します。

仮想化マネージャーを使用したエンドポイントへのトラストストア・ファイルのコピー

- システム管理者は、PowerVC などの仮想化マネージャーを使用して、PowerSC エージェントとトラストストア・ファイルが含まれたイメージによって、トラストストア・ファイルを各新規エンドポイントにコピーできます。
- 1. エンドポイントのトラストストア `/etc/security/powersc/uiServer/endpointTruststore.jks` ファイルを PowerVC イメージにコピーします。
- 2. システムに追加した各新規エンドポイントに PowerVC イメージをデプロイします。

ユーザー・アカウントのセットアップ

デフォルトでは、PowerSC GUI にログインするためには、どのユーザーも (LDAP ユーザーであっても、オペレーティング・システムによって定義されているローカル・ユーザーであっても) セキュリティー・グループのメンバーでなければなりません。

管理者は、この必須グループ・メンバーシップを `pscuiserverctl` コマンドで変更できます。PowerSC GUI にログインした後、ユーザーは、自身のユーザー・アカウントがエンドポイントの管理を許可されている UNIX グループのメンバーである場合にのみ、エンドポイントの状況を表示できます。管理者は、個別のエンドポイント・レベルのユーザー・アカウント設定を `setGroups.sh` コマンドで変更できます。

以下の点を考慮してください。

- エンドポイントと AIX グループとの間には、次の多対多の関係があります。
 - 1 つの AIX グループをいくつものエンドポイントに関連付けることができます。
 - 1 つのエンドポイントをいくつもの AIX グループに関連付けることができます。
- ユーザーが PowerSC GUI にログインした後、そのユーザーが特定のエンドポイントに対するコマンドの実行を許可されるか、またはエンドポイント状況の表示のみ許可されるかは、グループ関連付けによって決定されます。
 - PowerSC GUI を使用して特定のエンドポイントに対するコマンドを実行するには、ユーザーは、そのエンドポイントに関連付けられているグループのいずれかに関連付けられている必要があります。
 - ユーザーのグループ・メンバーシップは、各エンドポイントに関連付けられているグループのセットと比較されます。ユーザーのグループ・メンバーシップと、各エンドポイントに関連付けられているグループが一致している場合、そのユーザーは、そのグループに対するコマンド (「プロファイルの適用」、「元に戻す」、「検査」など) の実行を許可されます。ユーザーのグループ・メンバーシップと、各エンドポイントに関連付けられているグループが一致しない場合は、そのユーザーは、そのエンドポイントの状況の表示のみ許可されます。

PowerSC GUI サーバーでは、以下のシェル・スクリプトが `/opt/powersc/uiServer/bin/` ディレクトリーに用意されています。

表 14. グループ・シェル・スクリプト

シェル・スクリプト	説明
<code>pscuiserverctl</code>	PowerSC GUI にログインするためにユーザーがメンバーとして属している必要がある AIX ログイン (UNIX) グループを指定します。ユーザーは、いずれか 1 つのグループのみのメンバーになる必要があります。
<code>setGroups.sh</code>	特定のエンドポイントに対するコマンド実行するためにユーザーがメンバーとして属している必要がある 1 つ以上の AIX グループを指定します。

グループ・セットアップ・コマンドおよびスクリプトの実行

システム管理者は、**pscuiserverctl** コマンドおよび **setGroups** スクリプトを実行して、どのオペレーティング・システム・グループが PowerSC GUI へのログイン、管理者機能の実行、および特定のエンドポイントでのコマンドの実行を許可されているかを指定する必要があります。

1. PowerSC GUI サーバーで、`/opt/powersc/uiServer/bin/` ディレクトリーに移動します。
2. 次のコマンドを実行して、PowerSC GUI にログインするためにユーザーがメンバーでなければならない AIX グループを指定します。指定したグループは、`/etc/security/powersc/uiServer/uiServer.conf` ファイルに書き込まれます。

```
pscuiserverctl set logonGroupList abp,security
```

ヒント: このコマンドを実行する前に、**groups username** コマンドを使用して、ユーザーがメンバーになっているグループを調べることができます。

3. 以下のコマンドを実行して、PowerSC GUI を使用した管理者機能の実行が許可される UNIX グループを指定します。

```
pscuiserverctl set administratorGroupList unixgrpadmin1,unixgrpadmin2
```

4. 次のスクリプトを実行して、特定のエンドポイントでコマンドを実行するためにユーザーがメンバーでなければならない AIX グループを指定します。エンドポイントの完全修飾ホスト名を指定する必要があります。指定したグループは、`/etc/security/powersc/uiServer/groups.txt` ファイルに書き込まれます。

```
./setGroups.sh groupname "comma separated list of endpoint host names"
```

注: エンドポイントの検索にあたって、制限付きワイルドカード文字がサポートされています。例えば、「Boston_」で始まる名前または「.rs.com」で終わる名前を持つすべてのエンドポイントを指定するには、以下の指定が有効です。

- `./setGroups.sh groupname "Boston_*`
- `./setGroups.sh groupname "*.rs.com"`

ヒント: このコマンドでサポートされるワイルドカード文字はアスタリスク (*) のみです。使用可能な位置は、ストリングの先頭または末尾のみです。

PowerSC GUI の使用

PowerSC GUI を使用すると、ご使用のシステムで検出されたエンドポイントの表示、カスタマイズされたグループの作成、カスタマイズされたプロファイルの作成、カスタム・プロファイルのエンドポイントへのコピー、およびプロファイルの適用を行うことができます。さらに、エンドポイントと PowerSC GUI サーバーとの間の通信を検査し、エンドポイントと PowerSC GUI サーバーとの間の通信を終了することもできます。

PowerSC GUI のメインページには、以下のセクションがあります。

- 「グループ」トレイ：ご使用の環境に定義されているグループがリストされます。グループとは、共通性に基づいてグループ化されたエンドポイントの集合です。ご使用の環境でエンドポイントが検出されると、「すべてのシステム」グループが自動的に作成されます。カスタマイズされたグループを作成できます。例えば、共通性が HIPPA であるエンドポイントのグループを作成することができます。
- 「コンプライアンス」ページには、以下の 3 つのセクションがあります。
 - 上部ペインには、「グループ」トレイで選択したグループの統計情報が表示されます。この統計情報は、選択したグループ内のエンドポイントに適用された最終コンプライアンス・レベルの結果を示します。選択したグループについて、システム合格/不合格のパーセンテージ、検査されたルール の総数、および失敗した特定のルールを表示できます。
 - 中央ペインには、1 つ以上のエンドポイントに対してアクションを実行するためのタスクバーがあります。コンプライアンス・レベルを適用し、元に戻し、また検査することができます。
 - 下部ペインには、ご使用の環境で使用可能な、すべてのエンドポイントまたはエンドポイントのグループが入ったテーブルが表示されます。このテーブルには、エンドポイントごとに以下の情報があります。
 - システム名
 - コンプライアンス・ルール・タイプ
 - コンプライアンス・レベルがエンドポイントに適用された日時
 - コンプライアンス・レベルがエンドポイントで検査された日時
 - コンプライアンス・レベル状況
 - エンドポイント上の失敗したルールの数
 - コンプライアンス・レベル検査において正常に合格した、エンドポイント上のルールの数
- 「セキュリティ」ページには、以下の 2 つのセクションが含まれています。
 - 上部ペインには、「グループ」トレイで選択したエンドポイントのグループに関するリアルタイムのセキュリティ情報が表示されます。選択したグループについて、リアルタイム・コンプライアンス (RTC) イベントの総数、トラステッド実行 (TE) イベントの総数、TNC パッチが最新のエンドポイントのパーセンテージ、トラステッド・ブートがインストールされているエンドポイントのパーセンテージ、トラステッド・ファイアウォールがインストールされているエンドポイントの数、およびトラステッド・ロギングがインストールされているエンドポイントのパーセンテージを表示できます。
 - 下部ペインには、グループ内のシステム・エンドポイントが含まれている表が表示されます。このテーブルには、エンドポイントごとに以下の情報があります。
 - システム・エンドポイントの名前
 - ファイル保全性イベント・インジケータ
 - RTC 活動化状況
 - TE 活動化状況
 - 最新の TNC パッチ状況
- 「レポート」ページには、コンプライアンスに関するレポートおよびファイル保全性レポートが含まれます。概要レポートと詳細レポートの両方が含まれています。
- 「プロファイル・エディター」ページには、以下の 3 つのセクションが含まれています。
 - 上部ペインには、使用可能な組み込みおよびカスタム・プロファイルをリストしたドロップダウン・メニューがあります。
 - 中央ペインには、プロファイルの削除、新規プロファイルの作成、およびグループの一部であるエンドポイントへのプロファイルのコピーを行うために使用できるタスクバーがあります。

- 下部ペインには、選択したプロファイルに含まれているすべてのルールが入っている表が表示されます。ルールごとに、以下の情報が表示されます。
 - コンプライアンス・ルール名
 - コンプライアンス・ルール・タイプ
 - ルールの説明

PowerSC GUI 言語の指定

PowerSC GUI は、さまざまな言語に対応しています。

- | PowerSC GUI の言語を選択するには、メインページのメニュー・バーにある「言語および設定 (Languages and Settings)」アイコンをクリックします。インターフェースのレンダリングに使用されている現行言語がメニューで表示されます。言語を変更するには、関連アイコンをクリックします。使用可能な言語のリストから、ご使用のセッション用の言語を選択します。

PowerSC GUI のナビゲート

PowerSC GUI から、エンドポイントとサーバーの通信のセットアップと管理、エンドポイントの編成とグループ化、組み込みおよびカスタムのコンプライアンス・レベルとプロファイルのモニターと適用、エンドポイント・セキュリティのモニターと構成、スケジュールに基づいたレポートの生成と配布を行うことができます。

- | 1. PowerSC GUI を開きます。PowerSC GUI でホーム・ページが表示されます。
- | 2. エンドポイントとサーバーの通信を管理するには、メインページのメニュー・バーにある「言語および設定 (Languages and Settings)」アイコンをクリックします。「エンドポイント管理」アイコンをクリックして、エンドポイントと PowerSC GUI サーバー間の通信を確認または停止します。詳しくは、『エンドポイントとサーバーとの通信を管理』を参照してください。
- | 3. 「コンプライアンス」ページまたは「セキュリティ」ページのナビゲーション・ペインにある水平線の楕円をクリックして、グループ・エディターを開きます。グループ・エディターを使用して、エンドポイントのカスタム・グループを作成できます。詳しくは、161 ページの『カスタム・グループの作成』を参照してください。
- | 4. カスタム・コンプライアンス・プロファイルを作成する場合、およびプロファイルを終端ポイントにコピーする場合は、「プロファイル・エディター」タブをクリックします。詳しくは、162 ページの『コンプライアンス・プロファイルの操作』を参照してください。
- | 5. 組み込みおよびカスタムのコンプライアンス・レベルとプロファイルをモニターおよび適用する場合は、「コンプライアンス」タブをクリックします。詳しくは、『コンプライアンス・レベルおよびプロファイルの適用』を参照してください。
- | 6. エンドポイント・セキュリティをモニターおよび構成する場合は、「セキュリティ」タブをクリックします。詳しくは、『エンドポイント・セキュリティのモニター』を参照してください。
- | 7. オンデマンドまたはスケジュールに基づいてレポートを生成および配布する場合は、「レポート」タブをクリックします。詳しくは、『レポートの操作』を参照してください。

エンドポイントとサーバーとの通信を管理

- | 「エンドポイント管理」ページで、エンドポイントと PowerSC GUI サーバーとの間の通信を確認または停止することができます。鍵ストア要求を確認および生成することもできます。

エンドポイントとサーバーとの通信を検査

検出されたエンドポイントと PowerSC GUI サーバーとの間の通信を検査することができます。

1. メインページのメニュー・バーにある「言語および設定 (**Languages and Settings**)」アイコンをクリックします。「エンドポイント管理」をクリックします。エンドポイント管理ページが開きます。
2. 「グループ」トレイから、検査するエンドポイントが入っているグループを選択します。そのグループのエンドポイントが、エンドポイント・テーブルにリストされます。
3. 選択したグループのシステム・エンドポイントすべてが、コンプライアンス・テーブルに表示されます。「テキストによるフィルター」フィールドを使用して、表示されるエンドポイントをフィルターに掛けることができます。フィルター基準にするテキストをフィールドに入力し、Enter を押してください。選択したグループにあるエンドポイントのリストが動的にフィルターに掛けられ、そのテキストを含んでいる行だけが表示されます。
4. 状況情報を最新表示するには、「テーブルの最新表示」をクリックしてください。
5. 検査するエンドポイントごとに、関連付けられているチェック・ボックスを選択します。
6. 「検査」アイコンをクリックします。
7. 有効な接続に関する確認メッセージが、「検査済み (**Verified**)」列と「接続性診断」列に表示されます。

エンドポイントを PowerSC GUI モニタリングから除外

エンドポイントは、検出されると継続的にモニターされます。エンドポイントが環境から除去された場合、そのエンドポイントを PowerSC GUI サーバーからも除去する必要があります。

PowerSC GUI のモニター対象からエンドポイントを除去するには、以下の手順を実行します。

1. メインページのメニュー・バーにある「言語および設定 (**Languages and Settings**)」アイコンをクリックします。「エンドポイント管理」をクリックします。エンドポイント管理ページが開きます。
2. 「グループ」トレイから、除去するエンドポイントが入っているグループを選択します。そのグループのエンドポイントが、エンドポイント・テーブルにリストされます。
3. 選択したグループのシステム・エンドポイントすべてが、コンプライアンス・テーブルに表示されます。「テキストによるフィルター」フィールドを使用して、表示されるエンドポイントをフィルターに掛けることができます。フィルター基準にするテキストをフィールドに入力し、Enter を押してください。選択したグループにあるエンドポイントのリストが動的にフィルターに掛けられ、そのテキストを含んでいる行だけが表示されます。
4. 状況情報を最新表示するには、「テーブルの最新表示」をクリックしてください。
5. モニターを停止するエンドポイントごとに、関連付けられているチェック・ボックスを選択します。
6. 「削除」アイコンをクリックします。
7. エンドポイントの削除に関する確認メッセージが、「検査済みタイム・スタンプ」列と「接続性診断」列に表示されます。

鍵ストア要求の検査および生成

1. エンドポイントごとに、鍵ストア要求が有効であることを検査する必要があります。有効である場合、当該
1. エンドポイントの鍵ストアを生成できます。

1 エンドポイントの初回実行開始時、PowerSC GUI エージェントはトラストストア・ファイルを使用して、PowerSC GUI サーバーが実行されている場所を判別します。次に、PowerSC GUI エージェントは、使用可能なモニター対象エンドポイントのリストの結合要求とともにメッセージを PowerSC GUI サーバーに送信します。

2 「エンドポイント管理者 (Endpoint Administrator)」の「鍵ストア要求」ページで、鍵ストア要求が有効かを検査できます。有効な場合、当該エンドポイントの鍵ストアを生成できます。

1. メインページのメニュー・バーにある「言語および設定 (Languages and Settings)」アイコンをクリックします。「エンドポイント管理」をクリックします。「エンドポイント - すべてのシステム (Endpoint - All Systems)」管理ページが開きます。
2. 既知の各エンドポイントは、「システム名」列にリストされます。「鍵ストア要求」をクリックして、保留中の鍵ストア要求がないかを検査します。「エンドポイント管理」の「鍵ストア要求」ページが開きます。
3. すべての新規サーバーまたは追加されたサーバーの鍵ストア要求が、「ホスト名」列にリストされます。鍵ストアをエンドポイントに拡張することを確認した後に、エンドポイントのチェック・ボックスを選択し、「検査」をクリックします。
4. 検査は、PowerVC によって実行されます。「PowerVC 資格情報が必要です」ウィンドウにユーザー ID とパスワードを指定します。「OK」をクリックします。PowerVC がない場合は、このステップと次のステップをスキップします。

注: 検査は、Openstack API を使用して、PowerVC が新規に宣言されたエンドポイントを認識しているかどうかを確認するプロセスです。PowerVC がユーザー環境にない場合、または `powervcKeystoneUrl` が (`pscuiscserverctl` を使用して) 適切に構成されていない場合、PowerSC はエンドポイントを検査できません。

5. 検査後に、「ホスト名」列に吹き出しテキストとしてメッセージが表示されます。メッセージにより、PowerVC が新規エンドポイントを認識しているかどうかを確認されます。メッセージ内の情報に基づいて、鍵ストアの生成を選択できます。
6. 鍵ストアを生成するには、「鍵ストアの生成」をクリックします。鍵ストアの生成中は、表内のエンドポイント行が点滅します。完了すると、「生成済み鍵ストア」列の値が「いいえ」から「はい」に変化します。

注: PowerVC を使用してエンドポイントを検査していない場合、検査に進むかどうかを尋ねるメッセージが表示されます。エンドポイントを認識していて、鍵ストアを生成する場合は、「続行」をクリックします。

鍵ストアが生成済みであることを PowerSC エージェントがディスカバーするまでに数分かかることがあります。エージェントによって鍵ストアがインストールされると、PowerSC GUI の「エンドポイント管理 - すべてのシステム (Endpoint Admin - all systems)」、「コンプライアンス」、「セキュリティー」、および「レポート」の各ページで、新規エンドポイントが完全管理対象エンドポイントとしてリストされます。

7. エンドポイントの鍵ストアを生成しない場合は、要求を削除できます。削除するエンドポイントのチェック・ボックスを選択し、「削除」アイコンをクリックします。
8. 鍵ストアの検査を待機しているすべてのエンドポイントが、エンドポイントの表に表示されます。「テキストによるフィルター」フィールドを使用して、表示されるエンドポイントをフィルターに掛けることができます。フィルター基準にするテキストをフィールドに入力し、**Enter** を押してください。エンドポイントのリストが動的にフィルターに掛けられ、そのテキストを含んでいる行だけが表示されます。

9. エンドポイント・テーブル情報を最新表示するには、「テーブルの最新表示」をクリックしてください。

エンドポイントの編成およびグループ化

システム管理者は、いくつかの一般的なプロパティに基づいて、エンドポイントを編成およびグループ化することができます。カスタム・グループを定義でき、それらのグループに、PowerSC GUI で管理されている、明示的に選択したエンドポイントのセットを組み込むことができます。

例えば、3 つまたは 4 つの環境がある場合、実動エンドポイント、テスト・エンドポイント、および品質保証エンドポイントを入れるグループを作成することができます。

インストール中に、「すべてのシステム」という名前のデフォルト・グループが作成されます。このグループには、ご使用の環境で検出されたエンドポイントがすべて入っています。

カスタム・グループの作成

明示的に選択した、エンドポイントの列挙型リストでカスタム・グループを作成できます。

1. 「グループ」トレイから、「新規グループの作成」を選択します。「新規グループの作成」トレイが開きます。「グループ」トレイが展開されていない場合は、インターフェースのメイン・ページの左ペインにある水平線の楕円をクリックします。
2. 新規グループの固有の名前を入力し、Enter キーを押します。新しいグループは、「グループ」トレイに追加されます。
3. そのグループに組み込むシステムを追加します。使用可能なエンドポイント・システムの「すべてのシステム」リストで、グループに組み込むシステムを選択します。右矢印をクリックして、選択したすべてのシステムを新規グループに移動します。グループからエンドポイント・システムを削除するには、新規グループ・リスト内のエンドポイントを強調表示してから、左矢印をクリックします。
4. グループ・メンバーを追加または削除した後に、コンテンツ・ペインのメニュー・バーにある「保存」アイコンをクリックして変更を保存します。
5. 水平の楕円をクリックして、「グループ」トレイに戻ります。新規グループがリストされます。

既存グループに割り当てられたシステムの追加または削除

既存のグループに割り当てられているエンドポイントを追加または削除できます。

1. 「グループ」トレイで、エンドポイント・システムを追加または削除するグループの右にある楕円をクリックします。「グループ」トレイが展開されていない場合は、インターフェースのメイン・ページの左ペインにある水平線の楕円をクリックします。
2. 「グループの編集」をクリックします。
3. エンドポイント・システムをグループに追加するには、「すべてのシステム」リストからシステムを選択し、右矢印をクリックします。そのシステムが「**GroupName**」リストに追加されます。
4. エンドポイントをグループから削除するには、「グループ・システム (Group Systems)」リストからシステムを選択し、左矢印をクリックします。そのシステムが「**GroupName**」リストから削除されます。
5. 「グループ変更の保存」アイコンをクリックして、変更を保存します。
6. システムをグループから削除するには、システムを選択し、左矢印をクリックします。
7. グループに対する変更をキャンセルするには、「グループ変更のキャンセル」をクリックします。
8. 「グループ」の楕円をクリックして、「グループ」トレイに戻ります。

グループの削除

適用可能ではなくなったグループを削除することができます。

1. 「グループ」トレイから、削除するグループの右にある楕円をクリックします。「グループ」トレイが展開されていない場合は、インターフェースのメイン・ページのナビゲーション・ペインにある水平線の楕円をクリックします。
2. 「グループの削除」をクリックします。グループが削除され、「グループ」トレイ内のグループのリストから削除されます。

グループの名前変更

グループを名前変更できます。

1. 「グループ」トレイから、名前変更するグループの右にある楕円をクリックします。「グループ」トレイが展開されていない場合は、インターフェースのメイン・ページのナビゲーション・ペインにある水平線の楕円をクリックします。
2. 「グループの名前変更」をクリックします。「グループ名」フィールドにグループの新規名を指定します。

グループの複製

グループを複製して、同じエンドポイントが含まれている複製を新規名前で作成できます。

1. 「グループ」トレイから、削除するグループの右にある楕円をクリックします。「グループ」トレイが展開されていない場合は、インターフェースのメイン・ページのナビゲーション・ペインにある水平線の楕円をクリックします。
2. 「グループの複製」をクリックします。グループがコピーされ、新規名が割り当てられます。

コンプライアンス・プロファイルの操作

PowerSC GUI プロファイル・エディターを使用すると、組み込みコンプライアンス・プロファイルを表示し、カスタム・プロファイルを作成し、またプロファイルシステム・エンドポイントにコピーすることができます。

PowerSC Standard Edition 製品には、システム・エンドポイントのそれぞれが以下のセキュリティー標準を満たすように、そのエンドポイントの構成に使用できる、組み込みプロファイルのセットが付属しています。

- Payment Card Industry (PCI) - Data Security Standard への準拠
- Sarbanes-Oxley 法令および COBIT への準拠 (SOX-COBIT)
- 米国国防総省 (DoD) STIG 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))
- 北米電力信頼度協議会 (NERC) への準拠

組み込みプロファイルについて詳しくは、トピック: 9 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概念』を参照してください。

それぞれの組み込みプロファイルには、セキュリティー要件を満たすために、エンドポイントに適用される必要があるルールが入っています。これらのルールの一部のみまたは別の組み合わせを適用するか、またはコンプライアンス・レベルをカスタマイズする必要がある場合、カスタム・プロファイルを作成できます。

ほとんどの環境で、問題となっているルールを除去するために、管理者はコンプライアンス・ファイルを頻繁に編集します。互換性チェックが完了した後、コンプライアンス・ルール・ファイルは安定したものと見なされ、実動サーバーにデプロイされます。

PowerSC GUI を使用して、組み込みプロファイル (または他のカスタム・プロファイル) のルールを組み合わせることによってカスタム・プロファイルを作成できます。

コンプライアンス・プロファイルの表示

組み込みプロファイルおよびカスタム・プロファイルのそれぞれに組み込まれているルールを表示できます。

1. メインページから、「プロファイル・エディター」タブを選択します。「プロファイル・エディター」ページが開きます。
2. 下向き矢印をクリックして、プロファイルのリストを開きます。ドロップダウン・メニューで、使用可能な組み込みプロファイルおよびカスタム・プロファイルがリストされます。
3. 表示するプロファイルを選択します。そのプロファイルに組み込まれているルールがそれぞれ、その名前、タイプ、および説明と一緒に表示されます。ルールの詳細については、9 ページの『セキュリティおよびコンプライアンス自動化の概念』のトピックを参照してください。
4. 選択したプロファイルのルールすべてが、プロファイル・テーブルに表示されます。「テキストによるフィルター」ボックスを使用して、表示されるプロファイルをフィルターに掛けることができます。フィルター基準にするテキストをテキスト・ボックスに入力してください。選択したプロファイル内のルールのリストが最新表示されます。

カスタム・プロファイルの作成

既存のプロファイルに基づいた新規プロファイルを作成してから、その新規プロファイルをカスタマイズして特定のルール・セットのみを組み込むようにすることができます。

1. メインページから、「プロファイル・エディター」タブを選択します。「プロファイル・エディター」ページが開きます。
2. 下向き矢印をクリックして、プロファイルのリストを開きます。ドロップダウン・メニューで、使用可能な組み込みプロファイルおよびカスタム・プロファイルがリストされます。
3. 新規プロファイルのベースにするプロファイルを選択します。
4. 「新規プロファイルの作成」アイコンをクリックします。「新規プロファイル名およびプロファイル・タイプ」ウィンドウが開きます。
5. 「プロファイル名」フィールドに新規プロファイルの名前を入力します。
6. 「プロファイル・タイプ」フィールドにタイプを入力します。入力するタイプでは通常、新規プロファイルのベースである組み込みポリシーのタイプに固有の ID を加えたものを指定します。例: PCIxx、SOX-COBITxy、DoDxyz、HIPAAwxyz、NERCabc
7. 「確認」をクリックします。
8. ルールをカスタム・プロファイルに追加するには、カスタム・プロファイルのベースとしている元のプロファイルからルールを選択し、右矢印をクリックします。ルールが新規カスタム・プロファイルに追加されます。組み込むルールごとに繰り返します。
9. カスタム・プロファイルからルールを削除するには、カスタム・プロファイルからルールを選択し、左矢印をクリックします。ルールが新規カスタム・プロファイルから削除されます。削除するルールごとに繰り返します。
10. ルールの追加が終わったら、「保存」をクリックします。

プロファイルをグループ・メンバーにコピー

カスタム・プロファイルをエンドポイントのグループにコピーできます。カスタム・プロファイルは、エンドポイントにコピーされた後、そのエンドポイントに対するアプリケーションに有効になります。また、エラーなしでエンドポイントに適用できるかどうかを検査することもできます。

1. メインページから、「プロファイル・エディター」タブを選択します。「プロファイル・エディター」ページが開きます。
2. 下向き矢印をクリックして、プロファイルのリストを開きます。ドロップダウン・メニューで、使用可能な組み込みプロファイルおよびカスタム・プロファイルがリストされます。
3. グループのメンバーにコピーするプロファイルを選択します。
4. 「プロファイルをグループ・メンバーにコピー」アイコンをクリックします。「*profilename* を次のメンバーにコピー (Copy *profilename* to)」ウィンドウが開きます。
5. 組織用に作成したグループそれぞれが、関連付けられているチェック・ボックスと一緒にリストされます。選択したプロファイルをコピーする先のグループごとに、チェック・ボックスを選択します。
6. 「コピー (Copy)」をクリックします。
7. プロファイルを適用または検査するには、「コンプライアンス」タブを選択して、「コンプライアンス」ページに戻ります。

カスタム・プロファイルの削除

カスタム・プロファイルを削除することができます。

1. メインページから、「プロファイル・エディター」タブを選択します。「プロファイル・エディター」ページが開きます。
2. 下向き矢印をクリックして、プロファイルのリストを開きます。ドロップダウン・メニューで、使用可能な組み込みプロファイルおよびカスタム・プロファイルがリストされます。
3. 「カスタム・プロファイル」リストを展開します。
4. 削除するプロファイルを選択します。
5. 「プロファイルの削除」アイコンをクリックします。選択したカスタム・プロファイルが削除されます。

コンプライアンス・レベルおよびプロファイルの管理

システム管理者は、複数のエンドポイント上の組み込みおよびカスタムのコンプライアンス・レベルおよびプロファイルを適用したり、検査したり、元に戻したりすることができます。

下の表には、PowerSC Standard Edition によってサポートされている定義済みプロファイルおよびコンプライアンス・レベルがリストされています。

表 15. PowerSC Standard Edition によってサポートされている定義済みプロファイルおよびコンプライアンス・レベル

プロファイル	レベル
Database	低
DoD	中
DoD_to_AIXDefault	高
DoDv2	デフォルト
DoDv2_to_AIXDefault	
HIPAA	

表 15. PowerSC Standard Edition によってサポートされている定義済みプロファイルおよびコンプライアンス・レベル (続き)

プロファイル	レベル
NERC	
NERC_to_AIXDefault	
NERCv5	
NERCv5_to_AIXDefault	
PCI	
PCI_to_AIXDefault	
PCIv3	
PCIv3_to_AIXDefault	
SOX-COBIT	

PowerSC GUI の「コンプライアンス」ページでは、以下のタスクを実行できます。

- 定義済みプロファイルまたはレベルを選択して、1 つ以上のエンドポイントに適用します。
- 1 つ以上のエンドポイントに対して「元に戻す」操作を起動します。
- 定義済みプロファイルまたはレベルと、1 つ以上のエンドポイントの現在の状況を照合します。この検査操作によってエンドポイントに変更が加えられることはありませんが、いつ最終チェックが行われたかを示すために、「チェック済みタイム・スタンプ」値が設定されます。

コンプライアンス・レベルおよびプロファイルの適用

コンプライアンス・レベルまたはプロファイルを、選択したグループにおける 1 つ以上のエンドポイントに適用することができます。

1. メインページから、「コンプライアンス」タブを選択します。「コンプライアンス」ページが開きます。
2. 「グループ」トレイから、コンプライアンス・レベルおよびプロファイルを適用する対象のエンドポイントが入っているグループを選択します。
3. 選択したグループのシステム・エンドポイントすべてが、コンプライアンス・テーブルに表示されます。「テキストによるフィルター」テキスト・ボックスを使用して、表示されるエンドポイントをフィルターに掛けることができます。フィルター基準にするテキストをテキスト・ボックスに入力し、**Enter** を押してください。選択したグループにあるエンドポイントのリストが動的にフィルターに掛けられ、そのテキストを含んでいる行だけが表示されます。
4. 状況情報を最新表示するには、「テーブルの最新表示」をクリックしてください。最新表示が自動的に行われる頻度を設定するには、「最新表示間隔」をクリックします。
5. 「コンプライアンス・ルール・タイプ」列で、関連付けられているエンドポイントにコピーされたレベルおよびプロファイルを調べることができます。エンドポイントに適用するレベルおよびプロファイルを選択します。関連付けられているチェック・ボックスにチェック・マークを付けてください。
6. コンプライアンス・レベルおよびプロファイルを適用する対象の、グループ内のエンドポイントごとに、ステップ 5 を繰り返します。
7. 「プロファイルの適用」アイコンをクリックします。
8. 選択したコンプライアンス・レベルおよびプロファイルが、選択したエンドポイントそれぞれに適用されます。1 つ以上のルールを適用できない場合、それらは不合格になったと考えられます。1 つ以上のルールが不合格であれば、そのエンドポイントには、赤いバーでフラグが立てられます。また、テキスト「不合格」が「不合格ルール数」列に表示されます。

9. フラグが立てられたエンドポイントごとの「不合格ルール数」列で、ルールが不合格であった理由を調べることができます。カスタム・プロファイルを作成または編集することによって、適用されているルールを調整できます。

コンプライアンス・レベルを元に戻す

選択したグループにおける 1 つ以上のエンドポイントに適用されている、最終コンプライアンス・レベルまたはプロファイルを元に戻すことができます。

コンプライアンス・レベルを元に戻すには、以下の手順を実行します。

1. メインページから、「コンプライアンス」タブを選択します。「コンプライアンス」ページが開きます。
2. 「グループ」トレイから、コンプライアンス・レベルおよびプロファイルを元に戻す対象のエンドポイントが入っているグループを選択します。
3. 選択したグループのエンドポイントすべてが、コンプライアンス・テーブルに表示されます。「テキストによるフィルター」テキスト・ボックスを使用して、表示されるエンドポイントをフィルターに掛けることができます。フィルター基準にするテキストをテキスト・ボックスに入力し、**Enter** を押してください。選択したグループにあるエンドポイントのリストが動的にフィルターに掛けられ、そのテキストを含んでいる行だけが表示されます。
4. 状況情報を最新表示するには、「テーブルの最新表示」をクリックしてください。最新表示が自動的に行われる頻度を設定するには、「最新表示間隔」をクリックします。
5. エンドポイントに適用されたレベルまたはプロファイルを元に戻すには、以下のようになります。
 - a. そのエンドポイントに関連付けられているチェック・ボックスにチェック・マークを付けます。
 - b. 「元に戻す」アイコンをクリックします。

最後に適用されたコンプライアンス・レベルおよびプロファイルの検査

選択したグループにおける 1 つ以上のエンドポイントに適用された最終コンプライアンス・レベルまたはプロファイルを検査できます。

1. メインページから、「コンプライアンス」タブを選択します。「コンプライアンス」ページが開きます。
2. 「グループ」トレイから、コンプライアンス・レベルおよびプロファイルを検査する対象のエンドポイントが入っているグループを選択します。
3. 選択したグループのエンドポイントすべてが、コンプライアンス・テーブルに表示されます。「テキストによるフィルター」テキスト・ボックスを使用して、表示されるエンドポイントをフィルターに掛けることができます。フィルター基準にするテキストをテキスト・ボックスに入力し、**Enter** を押してください。選択したグループにあるエンドポイントのリストが動的にフィルターに掛けられ、そのテキストを含んでいる行だけが表示されます。
4. 状況情報を最新表示するには、「テーブルの最新表示」をクリックしてください。最新表示が自動的に行われる頻度を設定するには、「最新表示間隔」をクリックします。
5. 適用された最終レベルまたはプロファイルを検査する対象のエンドポイント・システム名について、関連付けられているチェック・ボックスを選択します。
6. コンプライアンス・レベルおよびプロファイルを検査する対象の、グループ内のエンドポイントごとに、ステップ 5 (165 ページ) を繰り返します。
7. 「検査」アイコンをクリックします。

8. エンドポイントが検査され、コンプライアンス・レベルまたはプロファイルにあるルールが適用可能であるかどうか分かります。エンドポイントが更新されることはありません。どのルールも適用できない場合、それらは適用時に失敗したものと考えられます。1 つ以上のルールが不合格であれば、そのエンドポイントには、赤いバーでフラグが立てられます。また、テキスト「不合格」が「不合格ルール数」列に表示されます。
9. フラグが立てられたエンドポイントごとの「不合格ルール数」リストで、ルールが不合格であった理由を示すメッセージを調べることができます。カスタム・プロファイルを作成することによって、適用されているルールを調整できます。

適用されていないコンプライアンス・レベルまたはプロファイルの検査

選択したグループにおける 1 つ以上のエンドポイントに適用されていないコンプライアンス・レベルまたはプロファイルを検査できます。

1. メインページから、「コンプライアンス」タブを選択します。「コンプライアンス」ページが開きます。
2. 「グループ」トレイから、コンプライアンス・レベルまたはプロファイルの効果を検査する対象のエンドポイントが入っているグループを選択します。
3. 選択したグループのエンドポイントすべてが、コンプライアンス・テーブルに表示されます。「テキストによるフィルター」テキスト・ボックスを使用して、表示されるエンドポイントをフィルターに掛けることができます。フィルター基準にするテキストをテキスト・ボックスに入力し、Enter を押してください。選択したグループにあるエンドポイントのリストが動的にフィルターに掛けられ、そのテキストを含んでいる行だけが表示されます。
4. 状況情報を最新表示するには、「テーブルの最新表示」をクリックしてください。最新表示が自動的に行われる頻度を設定するには、「最新表示間隔」をクリックします。
5. 適用された最終レベルまたはプロファイルを検査する対象のエンドポイント・システム名について、関連付けられているチェック・ボックスを選択します。複数のエンドポイントを選択できます。
6. 「最終検査済みタイプ」ドロップダウン・リストを開きます。以下のいずれかを選択します。
 - すべての使用可能レベル: エンドポイントに対して検査できるすべての使用可能なレベルのリストが表示されます。
 - すべての使用可能プロファイル: エンドポイントに対して検査できるすべての使用可能なプロファイルのリストが表示されます。
7. エンドポイントに対して検査するレベルまたはプロファイルを選択します。
8. 「検査」アイコンをクリックします。検査の結果が返され、エンドポイントの下にリストされます。

コンプライアンス・イベント発生時の E メール通知の送信

「コンプライアンス」ページで、コンプライアンス・イベントの発生時に 1 人以上の受信者に E メール通知を送信できます。

1. メインページから、「コンプライアンス」タブを選択します。「コンプライアンス」ページが開きます。
2. メニュー・バーの右上にある「E メール設定」アイコンをクリックします。「E メール設定」ウィンドウが開きます。
3. 「E メール送信可能」チェック・ボックスを選択します。
4. 「アドレス (コンマ区切り)」フィールドに、各受信者の E メール・アドレスをコンマ区切りで入力します。

| エンドポイント・セキュリティのモニター

| 「セキュリティ」ページで、エンドポイント・セキュリティをリアルタイムでモニターできます。

| 「セキュリティ」ページでは、リアルタイム・コンプライアンス (RTC) とトラステッド実行 (TE) でモニターされているエンドポイントの状況が表示されます。

| RTC (PowerSC のサブコンポーネント) と TE (AIX のコンポーネント) はともに、ファイル保全性モニターリング (FIM) 機能です。FIM は、重要なファイルに対する変更をモニターして、ファイルに影響するイベントが許可されるかを確認します。セキュリティに影響する可能性があるイベントには、ファイルに対する許可が予期せず変更された場合、ファイルの内容が更新された場合、スケジュールされていないアプリケーションがインストールされた場合などがあります。これらのイベントを認識して、重要なファイルおよびアプリケーションを保護する必要があります。

| 「セキュリティ」ページは、PowerSC GUI のリアルタイム・モニター・ページです。RTC または TE によってモニターされているファイルが変更された場合に生成されるイベントが表示されます。イベントには、ファイルの内容がいつ変更されたのか、エンドポイントがいつアクセスされたのか、構成がいつ変更されたのかに関する詳細が含まれます。

| 「セキュリティ」ページを使用して、以下のタスクを実行できます。

- | • RTC および TE のリアルタイム・モニターの情報を表示する
- | • すべてのエンドポイントに対して RTC および TE を構成する
- | • エンドポイント上の他の PowerSC 製品の状況を表示する
- | • TE のオンとオフを切り替える

| リアルタイム・コンプライアンス (RTC) の構成

| 「セキュリティ」ページから、特定のエンドポイントまたはエンドポイント・グループのリアルタイム・コンプライアンス (RTC) 製品を構成できます。

- | 1. RTC 構成を編集するエンドポイントの右にある楕円をクリックします。
- | 2. 「**RTC** の構成」をクリックします。「RTC ポリシー構成」ウィンドウが開きます。
- | 3. すべての使用可能な RTC 構成オプションが説明とともにリストされます。1 つ以上の RTC 構成オプションを変更するには、オプションの左にあるチェック・ボックスを選択するかクリアします。一部のケースでは、オプションに対する変更は、サーバーが再始動されるまで実装されません。
- | 4. 「保存」をクリックします。

| 以前の日時へのリアルタイム・コンプライアンス (RTC) 構成オプションの復元

| 以前の日時に RTC 構成を復元できます。

- | 1. RTC 構成オプションを以前のバージョンにロールバックするエンドポイントの右にある楕円をクリックします。
- | 2. 「**RTC** のロールバック」をクリックします。RTC の各構成バージョンのタイム・スタンプがリストされます。
- | 3. 戻す先の構成バージョンのタイム・スタンプをクリックします。その日時に設定されていた RTC 構成オプションが復元されます。

他のグループへのリアルタイム・コンプライアンス (RTC) 構成オプションのコピー

別のエンドポイント・グループまたは特定のエンドポイント・セットに RTC 構成オプションをコピーできます。

1. 別のエンドポイント・グループまたは特定のエンドポイント・セットに構成オプションをコピーするエンドポイントの右にある楕円をクリックします。
2. 「**RTC** 構成のコピー」をクリックします。「すべてのシステム」グループなどの各エンドポイント・グループがリストされます。
3. 以下のいずれかの方法でグループまたは特定のエンドポイントを選択します。
 - 使用可能なグループのリストからエンドポイント・グループのチェック・ボックスを選択します。そのグループ内の各エンドポイントに構成オプションがコピーされます。
 - 右矢印を使用してグループを展開し、グループ内のすべてのエンドポイントのリストを表示します。構成オプションをコピーする先のグループの各エンドポイントのチェック・ボックスを選択します。
 - 「すべてのシステム」グループ内のエンドポイントのリストを展開します。エンドポイントをコピーする先のグループの各エンドポイントのチェック・ボックスを選択します。
4. 「**OK**」をクリックします。構成オプションが、選択したグループまたは選択したエンドポイントにコピーされます。

リアルタイム・コンプライアンス (RTC) ファイル・リストの編集

エンドポイント上の各ファイルの RTC モニター・オプションを表示および編集できます。

1. RTC モニター・オプションを表示または編集するファイルをホストしているエンドポイントの右にある楕円をクリックします。
2. 「**RTC** ファイル・リストの編集」をクリックします。「**RTC** ファイル・リスト構成」ページが開き、エンドポイント上にあるすべてのディレクトリおよびファイルがリストされます。ディレクトリ・フォルダー・アイコン上のチェック・マークは、そのディレクトリ内の 1 つ以上のファイルがモニターされていることを示します。
3. オプションを編集するファイルがディレクトリ内にある場合、そのディレクトリをダブルクリックしてファイルをリストします。ディレクトリ内の各ファイルがリストされます。
4. エンドポイント上の各ファイルのモニター・オプションが、「内容」列および「属性」列にリストされます。ファイルの内容の変更がモニターされている場合、「内容」列のチェック・ボックスが選択されます。ファイルの属性変更がモニターされている場合、「属性」列のチェック・ボックスが選択されます。モニター・オプションを編集するには、エンドポイント上の 1 つ以上のファイルのチェック・ボックスを選択またはクリアします。
5. 「保存」をクリックします。

以前の構成へのリアルタイム・コンプライアンス (RTC) ファイル・モニター・オプションの復元

RTC によってモニターされているファイルの以前のバージョンにロールバックできます。

1. RTC ファイル・モニター・オプションを以前のバージョンにロールバックするエンドポイントの右にある楕円をクリックします。
2. 「**RTC** ファイル・リストのロールバック」をクリックします。モニター対象ファイルの各構成バージョンのタイム・スタンプがリストされます。

- 3. 戻す先のモニター・オプション構成バージョンのタイム・スタンプをクリックします。その日時に設定されていた構成オプションが復元されます。

他のグループへのリアルタイム・コンプライアンス (RTC) ファイル・リスト・モニター・オプションのコピー

別のエンドポイント・グループまたは特定のエンドポイント・セットに RTC ファイル・モニター・オプションをコピーできます。

1. 別のエンドポイント・グループまたは特定のエンドポイント・セットにファイル・モニター・オプションをコピーするエンドポイントの右にある楕円をクリックします。
2. 「**RTC** ファイル・リストのコピー」をクリックします。「すべてのシステム」グループなどの各エンドポイント・グループがリストされます。
3. 以下のいずれかの方法でグループまたは特定のエンドポイントを選択します。
 - 使用可能なグループのリストからエンドポイント・グループのチェック・ボックスを選択します。そのグループ内の各エンドポイントにファイル・リスト・モニター・オプションがコピーされます。
 - 右矢印を使用してグループを展開し、グループ内のすべてのエンドポイントのリストを表示します。ファイル・モニター・オプションをコピーする先のグループの各エンドポイントのチェック・ボックスを選択します。
 - 「すべてのシステム」グループ内のエンドポイントのリストを展開します。エンドポイントをコピーする先のグループの各エンドポイントのチェック・ボックスを選択します。
4. 「**OK**」をクリックします。ファイル・モニター・オプションが、選択したグループまたは選択したエンドポイントにコピーされます。

リアルタイム・コンプライアンス (RTC) 検査の実行

「セキュリティ」ページで、リアルタイム・コンプライアンス検査を実行して、エンドポイントがまだ準備しているかどうかを確認できます。

1. リアルタイム・コンプライアンス (RTC) 検査を実行するエンドポイントの右にある楕円をクリックします。
2. 「コンプライアンス検査の実行」をクリックします。「コンプライアンス」ページが開き、エンドポイント行が点滅し、検査が実行中であることが示されます。
3. いずれかのルール適用に失敗すると、失敗を示すメッセージが「不合格ルール数」列に表示されます。エンドポイントの左にある下矢印を使用して、失敗したルールを表示します。

トラステッド実行 (TE) の構成

「セキュリティ」ページから、特定のエンドポイントまたはエンドポイント・グループのトラステッド実行 (TE) 製品を構成できます。

1. TE 構成オプションを編集するエンドポイントの右にある楕円をクリックします。
2. 「**TE** の構成」をクリックします。「TE ポリシー構成」ウィンドウが開きます。
3. すべての TE 構成オプションが説明とともにリストされます。1 つ以上の TE 構成オプションを変更するには、関連するチェック・ボックスを選択するかクリアします。一部のケースでは、オプションに対する変更は、サーバーが再始動されるまで実装されません。
4. 「保存」をクリックします。

他のグループへのトラステッド実行 (TE) オプションのコピー

- 別のエンドポイント・グループまたは特定のエンドポイント・セットに TE 構成オプションをコピーできます。
- 1. 別のエンドポイント・グループまたは特定のエンドポイント・セットに構成オプションをコピーするエンドポイントの右にある楕円をクリックします。
- 2. 「TE 構成のコピー」をクリックします。「すべてのシステム」グループなどの各エンドポイント・グループがリストされます。
- 3. 以下のいずれかの方法でグループまたは特定のエンドポイントを選択します。
 - 使用可能なグループのリストからエンドポイント・グループのチェック・ボックスを選択します。そのグループ内の各エンドポイントに構成オプションがコピーされます。
 - グループを展開し、グループ内のすべてのエンドポイントのリストを表示します。構成オプションをコピーする先のグループの各エンドポイントのチェック・ボックスを選択します。
 - 「すべてのシステム」グループ内のエンドポイントのリストを展開します。エンドポイントをコピーする先のグループの各エンドポイントのチェック・ボックスを選択します。
- 4. 「OK」をクリックします。構成オプションが、選択したグループまたは選択したエンドポイントにコピーされます。

トラステッド実行 (TE) ファイル・リストの編集

- エンドポイント上の各ファイルの TE モニター・オプションを表示および編集できます。
- 1. TE モニター・オプションを表示または編集するファイルをホストしているエンドポイントの右にある楕円をクリックします。
- 2. 「TE ファイル・リストの編集」をクリックします。「TE ファイル・リスト構成」ページが開き、エンドポイント上にあるすべてのディレクトリーおよびファイルがリストされます。ディレクトリー・フォルダー・アイコン上のチェック・マークは、そのディレクトリー内の 1 つ以上のファイルがモニターされていることを示します。
- 3. オプションを表示または編集するファイルがディレクトリー内にある場合、そのディレクトリーをダブルクリックしてファイルをリストします。ディレクトリー内の各ファイルがリストされます。
- 4. エンドポイント上の各ファイルのモニター・オプションが、「TE」列および「揮発性」列にリストされます。ファイルの内容の変更がモニターされている場合、「TE」列のチェック・ボックスが選択されています。ファイルの許可の変更のみがモニターされている場合、「揮発性」列のチェック・ボックスが選択されています。モニター・オプションを変更するには、エンドポイント上の 1 つ以上のファイルのチェック・ボックスを選択またはクリアします。
- 5. 「保存」をクリックします。

他のグループへのトラステッド実行 (TE) ファイル・リスト・モニター・オプションのコピー

- 別のエンドポイント・グループまたは特定のエンドポイント・セットに TE ファイル・モニター・オプションをコピーできます。
- 1. 別のエンドポイント・グループまたは特定のエンドポイント・セットにファイル・モニター・オプションをコピーするエンドポイントの右にある楕円をクリックします。
- 2. 「TE ファイル・リストのコピー」をクリックします。「すべてのシステム」グループなどの各エンドポイント・グループがリストされます。
- 3. 以下のいずれかの方法でグループまたは特定のエンドポイントを選択します。

- ・ 使用可能なグループのリストからエンドポイント・グループのチェック・ボックスを選択します。そのグループ内の各エンドポイントにファイル・リスト・モニター・オプションがコピーされます。
 - ・ グループを展開し、グループ内のすべてのエンドポイントのリストを表示します。ファイル・モニター・オプションをコピーする先のグループの各エンドポイントのチェック・ボックスを選択します。
 - ・ 「すべてのシステム」グループ内のエンドポイントのリストを展開します。エンドポイントをコピーする先のグループの各エンドポイントのチェック・ボックスを選択します。
4. 「OK」をクリックします。ファイル・モニター・オプションが、選択したグループまたは選択したエンドポイントにコピーされます。

他の PowerSC フィーチャーの状況の表示

「セキュリティ」ページで、各 PowerSC フィーチャー (トラステッド・ブート、トラステッド・ファイアウォール、およびトラステッド・ロギング) の状況を表示できます。エンドポイント上のトラステッド・ネットワーク接続 (TNC) 更新の状況も表示できます。

1. メインページから、「セキュリティ」タブを選択します。「セキュリティ」ページが開きます。
2. PowerSC の TNC コンポーネントは、各エンドポイントでのセキュリティ・パッチの検査および更新に使用されます。エンドポイントの表の「TNC によって最新に保つ」列は、TNC サーバーの観点からエンドポイントが最新かどうかを示します。ダッシュボード・バナーの「TNC によって最新に保つ」セクションには、グループ内の最新のエンドポイントのパーセンテージが表示されます。「セキュリティ」ページで TNC 更新情報が表示されないようにするには、以下のステップを実行します。
 - a. メインページのメニュー・バーにある「言語および設定 (Languages and Settings)」アイコンをクリックします。
 - b. 「サブ製品の使用」をクリックします。
 - c. 「TNC によって最新に保つ」をオフに設定します。
 - d. 表示を復元するには、「TNC によって最新に保つ」をオンにスライドします。
3. エンドポイントの表の「TB」列は、PowerSC トラステッド・ブートがエンドポイントで使用可能かどうかを示します。ダッシュボード・バナーの「信頼できるブート」セクションには、現在選択されているグループで PowerSC トラステッド・ブートが活動化されているエンドポイントのパーセンテージが表示されます。「セキュリティ」ページで PowerSC トラステッド・ブート情報が表示されないようにするには、以下のステップを実行します。
 - a. メインページのメニュー・バーにある「言語および設定 (Languages and Settings)」アイコンをクリックします。
 - b. 「サブ製品の使用」をクリックします。
 - c. 「信頼できるブート」に関連付けられたトグル・スイッチをオフにスライドします。
 - d. 表示を復元するには、トグル・スイッチをオンにスライドします。
4. エンドポイントの表の「TF」列は、PowerSC トラステッド・ファイアウォールがエンドポイントで使用可能かどうかを示します。ダッシュボード・バナーの「信頼できるファイアウォール」セクションには、現在選択されているグループで PowerSC トラステッド・ファイアウォールがアクティブなエンドポイントのパーセンテージが表示されます。「セキュリティ」ページでトラステッド・ファイアウォール情報が表示されないようにするには、以下のステップを実行します。
 - a. メインページのメニュー・バーにある「言語および設定 (Languages and Settings)」アイコンをクリックします。
 - b. 「サブ製品の使用」をクリックします。

- | c. 「信頼できるファイアウォール」に関連付けられたトグル・スイッチをオフにスライドします。
- | d. 表示を復元するには、トグル・スイッチをオンにスライドします。
- | 5. エンドポイントの表の「TL」列は、PowerSC トラストッド・ロギングがエンドポイントで使用可能かどうかを示します。ダッシュボード・バナーの「信頼できるロギング」セクションには、現在選択されているグループで PowerSC トラストッド・ロギングがアクティブなエンドポイントのパーセンテージが表示されます。「セキュリティ」ページでトラストッド・ロギング情報が表示されないようにするには、以下のステップを実行します。
- | a. メインページのメニュー・バーにある「言語および設定 (Languages and Settings)」アイコンをクリックします。
- | b. 「サブ製品の使用」をクリックします。
- | c. 「信頼できるロギング」に関連づけられたトグル・スイッチをオフにスライドします。
- | d. 表示を復元するには、トグル・スイッチをオンにスライドします。

| トラストッド実行モニターの切り替え

- | トラストッド実行 (TE) モニターをオン/オフにすることができます。TE モニターをオフにし、指定時間間隔に基づいてオンになるようにスケジュールすることもできます。
- | 1. 「トラストッド実行の切り替え」アイコンをクリックします。
- | 2. ドロップダウン・トレイから、以下のオプションのいずれかを選択します。
 - | • すべてのエンドポイントについてオンにする: 各エンドポイントの TE モニターをオンにします。
 - | • すべてのエンドポイントについてオフにする: 各エンドポイントの TE モニターをオフにします。
- | 3. TE モニターがオフになっている場合、TE モニターの再始動時間を設定するオプションが使用可能になります。以下のいずれかの再始動時間を選択できます。
 - | • 1 時間
 - | • 5 時間
 - | • 1 日
 - | • 1 週間
 - | • なし
- | 4. 「保存」をクリックします。

| セキュリティー・イベント発生時の E メール通知の送信

- | 「セキュリティ」ページで、セキュリティ・イベントの発生時に 1 人以上の受信者に E メール通知を送信できます。
- | 1. メインページから、「セキュリティ」タブを選択します。「セキュリティ」ページが開きます。
- | 2. メニュー・バーの右隅にある「E メール設定」アイコンをクリックします。「E メール設定」ウィンドウが開きます。
- | 3. 「E メールで通知」チェック・ボックスにチェック・マークを付けてください。
- | 4. 「アドレス (コンマ区切り)」フィールドに、各受信者の E メール・アドレスをコンマ区切りで入力します。

レポートの操作

PowerSC GUI の「レポート」ページから複数のレポートにアクセスできます。

以下のレポートが使用可能です。

- **コンプライアンスの概要:** このレポートは、インターフェースの「コンプライアンス」ページに表示される概要情報のスナップショットです。
- **コンプライアンスの詳細:** このレポートは、「コンプライアンス」ページに表示される概要および詳細情報のスナップショットです。
- **ファイル保全性の概要:** このレポートは、インターフェースの「セキュリティ」ページに表示される概要情報のスナップショットです。
- **ファイル保全性の詳細:** このレポートは、「セキュリティ」ページに表示される概要および詳細情報のスナップショットです。
- **コンプライアンスと FIM との結合**

デフォルトでは、「レポート」ページには、「すべてのシステム」グループの「コンプライアンスの概要」レポートおよび「ファイル保全性の概要」レポートが表示されます。「コンプライアンスの詳細」レポート、「ファイル保全性の詳細」、および「コンプライアンスと FIM との結合」レポートに指定されているデフォルト・グループはありません。

「すべてのシステム」グループおよび定義した各グループに対してそれぞれのタイプのレポートを生成できます。グループ内のすべてのエンドポイントに対して、またはグループ内のエンドポイントのサブセットに対して、レポートを生成できます。レポートの生成後、オンデマンドで、または毎日、1 人以上の E メール受信者に、HTML フォーマットの E メールおよび CSV ファイルとしてレポートを配布するようにスケジュールできます。

「レポート」ページに表示されるレポートのリストは、ユーザー・ログイン ID によって異なります。ログイン ID に基づいて自分が管理しているエンドポイントに対してのみレポートを生成できます。特定のセッションで生成した各レポートは、次のセッションを開いたときにリストされます。

レポート・グループの選択

「すべてのシステム」グループおよび定義したすべてのグループに関する各レポートを実行できます。グループに組み込まれているすべてのエンドポイントについて、あるいはグループ内のエンドポイントのサブセットについて、レポートを実行するように選択できます。

1. メインページから、「レポート」タブをクリックします。「レポート」ページが開きます。
2. 実行するレポートのタイプの右にある楕円をクリックします。
3. 「グループの変更」をクリックします。
4. 使用可能なすべてのグループがリストされた選択ボックスが開きます。レポートを実行する対象のグループの横にあるラジオ・ボタンを選択します。「確認」をクリックします。レポートが実行され、メイン・ペインの内容が最新表示されて、選択したグループの情報が示されます。
5. エンドポイントのサブセットに対するレポートを実行するには、「すべてのシステム」グループを展開します。使用可能なすべてのエンドポイントのリストが表示されます。レポートに組み込む各エンドポイントの横にあるチェック・ボックスを選択します。「確認」をクリックして、レポートを実行します。

- 注: 特定のエンドポイント・グループに関するレポートを実行する場合、該当するエンドポイントが含まれたグループを作成できます。グループを作成すると時間が節約されます。また、グループはグローバルである (インターフェースのすべてのユーザーが表示できる) ため、そのグループをすべてのユーザーが使用できます。
6. 検索テキスト・ボックスに特定のエンドポイントの名前を入力することで、そのエンドポイントを検索できます。「確認」をクリックして、そのエンドポイントに関するレポートを実行します。

E メールを介したレポートの配布

レポートのグループを設定した後に、HTML フォーマットの E メールの形式および CSV ファイル形式で配布するようにスケジュールできます。1 人以上の E メール受信者に即時に、または毎日送信するように E メールをスケジュールできます。

CSV バージョンのレポートを含めると、受信者は、レポート・データをスプレッドシートにロードしたり、CSV ファイルを利用する他のソフトウェア・アプリケーションにインポートしたりすることができます。CSV ファイルには、グラフィックスやダッシュボードの概念はありません。概要レポートから生成された CSV ファイルには、各列見出しがコンマで区切られて最初の行に含まれています。後続の行には、エンドポイント、および各列の値がリストされます。

詳細レポートからは、複数の CSV ファイルが生成されます。最初の CSV ファイルは、概要レポートとよく似たフォーマットです。レポートの詳細レベルごとに別個の CSV ファイルが生成されます。例えば、ファイル保全性の詳細レポートでは、以下の詳細レベルで別個の CSV ファイルが生成されます。

- **TE** 構成
- **RTC** 構成
- サブ製品状況

1. メインページから、「レポート」タブをクリックします。「レポート」ページが開きます。
2. 使用可能なレポートのリストから、配布するレポートを選択します。レポートが実行され、メインページの内容が最新表示されます。
3. 配布するレポートの右にある楕円をクリックします。
4. 「E メール・オプション」をクリックします。「レポートを E メールで送信」ウィンドウが開きます。
5. 「アドレス」フィールドに各受信者の E メール・アドレスを指定します。複数の受信者アドレスは、セミコロン (;) で区切ります。
6. 「件名」フィールドに Eメールの説明を指定します。
7. 次のオプションのいずれかを選択してください。
 - 「毎日送信する時刻:」チェック・ボックスを選択して、レポートを受信者に毎日送信します。時分で時刻を選択して、レポートを送信する現地時間を指定します。「保存」および「閉じる」をクリックします。レポートは、毎日指定時刻に送信されます。
 - 「すぐに送信」をクリックしてレポートを送信します。レポートが送信され、ウィンドウが閉じます。

PowerSC Standard Edition コマンド

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 変更する必要が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
- 0** 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

- 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 -0 lt -P 345 -c tcp
```

- 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 -0 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、以下の終了値を返します。

- 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』

202 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、以下の終了値を返します。

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:

128 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

- 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:

178 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 7.2 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 -o <package name> -V <version> -T [installp|rqm] -D <User defined path>
```

```
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
pmconf chtncpm attribute = value
pmconf delete -l <TL list>
pmconf delete -o <package name> -V <version>
pmconf delete -p <SP List>
pmconf delete -p <SP>-e ifix file
pmconf export -f filename
| pmconf get -o <package> -V <version> -T <installp | rpm> -D <download directory>
| pmconf get -L -o <package> -V <version | all> -T <installp | rpm>
| pmconf get -L -p <SP>
| pmconf get -p <SP> -D <download directory>
pmconf hist -d
pmconf hist -u
pmconf import -f cert_filename -k key_filename
pmconf list -s [-c] [-q]
pmconf list -a SP
pmconf list -C
pmconf list -l SP
pmconf list -o <package name> -V <version>
pmconf list -o [-c] [-q]
pmconf log loglevel = info | error | none
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 proxy display

```

| **pmconf proxy** [enable=yes | no] [host=<hostname>] [port=<portnum>]

pmconf restart

pmconf status

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・フィックス情報を含むフィックス・リポジトリを作成します。

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 chtncpm	TNCPM を使用して新しいテクノロジー・レベルを登録します。 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。
get	使用可能なセキュリティ・フィックスおよびオープン・ソース・パッケージに関する情報を表示またはダウンロードします。 更新およびダウンロードの履歴を表示します。
history	TNCPM に関する情報を表示します。
list	TNC コンポーネントのログ・レベルを設定します。
log	TNCPM サーバーを作成します。
mktncpm	tncpm.conf 属性を変更します。
modify	プロキシ・サーバー・パラメーターの構成を管理します。
proxy	TNCPM サーバーを除去します。
rmtncpm	TNCPM サーバーを始動します。
start	TNCPM サーバーを停止します。
stop	

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。
-a SP	サービス・パックのセキュリティ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。 <i>SP</i> 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)。
-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。 <i>download_interval</i> 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。
-L	リストまたは検索専用モードを指定します。
-o package name	検索またはダウンロードするオープン・ソース・パッケージの名前。

項目	説明
-P <i>fix_repository_path</i>	TNCPM によってダウンロードされるフィックス・リポジトリ用のダウンロード・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。
-p <i>SP_list</i>	ダウンロードするサービス・バ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・バック 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 <i>APAR_type_list</i>	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 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。
T <i>package type</i>	検索またはダウンロードするオープン・ソース・パッケージのタイプを指定します。
-U <i>user_defined_fix_repository</i>	ユーザー定義のフィックス・リポジトリ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・バックを指定します。
-s	登録済みサービス・バックのレポートを生成します。
-l <i>SP</i>	サービス・バックに関する lspp 情報のレポートを生成します。 <i>SP</i> 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・バック 04 を表しています)。
-u	クライアント更新履歴のレポートを生成します。
V <i>version</i>	検索またはダウンロードするオープン・ソース・パッケージのバージョン。検索モード (-L) では、値「all」を指定して、指定したパッケージの使用可能なすべてのバージョンを検索できます。
-d	サービス・バックのダウンロード・履歴のレポートを生成します。
-C	サーバー証明書レポートを生成します。
-f <i>filename</i>	証明書ファイル名を指定します。
-k	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 lspp 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. 更新履歴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・履歴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
| 18. 使用可能なすべての rpm 形式バージョンの「emacs」オープン・ソース・パッケージを表示するに
| は、以下のコマンドを入力します。
| pmconf get -L -o emacs -V all -T rpm
| 19. バージョン 4.5.1 の「lsof」オープン・ソース・パッケージ (rpm 形式) を /tmp/new_lsof ディレク
| トリーにダウンロードするには、以下のコマンドを入力します。
| mkdir /tmp/new_lsof
| pmconf get -o lsof -V 4.5.1 -T rpm -D /tmp/new_lsof
| 20. 使用可能なすべてのバージョンの OpenSSH (installp 形式) を表示するには、以下のコマンドを入力
| します。
| pmconf get -o openssh -T installp -L -V all
| 21. オープン・ソース・パッケージまたはセキュリティー・フィックスをダウンロードする際に cURL で
| 使用する現行プロキシ構成設定を表示するには、以下のコマンドを入力します。
| pmconf proxy display
| 22. プロキシ構成を無効にするように設定するには、以下のコマンドを入力します。
| pmconf proxy enable=no

```

- | 23. プロキシを有効にしてホストを「myProxyServer」(ポート 9876) に設定するには、以下のコマンド
| を入力します。
| pmconf proxy enable=yes host=myProxyServer port=9876
- | 24. 使用するプロキシ・サーバー・ポートを変更するには、以下のコマンドを入力します。
| pmconf proxy port=1234
- | 25. サービス・パック・レベル 7100-03-02 のセキュリティー・フィックスによって解決された既知の脆弱
| 性を表示するには、以下のコマンドを入力します。
| pmconf get -L -p 7100-03-02
- | 26. サービス・パック・レベル 7200-00-01 のセキュリティー・フィックスを /tmp/ifixes_for_7.2.0.1 デ
| ィレクトリーにダウンロードするが、適用しない場合は、以下のコマンドを入力します。
| mkdir /tmp/ifixes_for_7.2.0.1
| pmconf get -p 7200-00-01 -D /tmp/ifixes_for_7.2.0.1

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> [tserver=<host>] [
recheck_interval=<time_in_minutes> | d (日) : h (時間) : m (分) ] [dbpath = <user-defined directory> ]
[default_policy=<yes | no > ] [clientData_interval=<time_in_minutes> | d (日) : h (時間) : m (分) ] [
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,...> | -O <openpkggrp1, openpkggrp2,...>}

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> |
-O <openpkggrp|ALL>} [-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>

psconf clientData {-l | -g} -i <ip|host>

psconf add -O <openpkggrp> <openpkgname:version>

psconf delete -O <openpkggrp> <openpkgname:version>

psconf delete -O <openpkggrp>

psconf delete -O ALL

psconf add -O <openpkggrp> fspolicy=<fspolicy name>

psconf report -O ALL -o TEXT

| psconf add -V <ifixgrp> autoupdate=<yes|no>

| psconf reboot -i <host> last one

```

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・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・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・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
add	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。
	<i>clientDataPath</i> 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。 <i>clientDataPath</i> 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。
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。

項目	説明
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。
Openpkggrp	クライアントの検査に使用されるファイルセット・ポリシーの一部として、 openpkg グループ名を指定します。
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。
reboot	変数 <i><host></i> の IP アドレスによって指定された TNC クライアントをリブートします。
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 16. *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。
-f filename	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。 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。
-Gipgroupname 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。
-O <openpkggrp>	ポリシーの openpkg グループ名を指定します。
-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。

項目	説明
-r <i>buildinfo</i>	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・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。
-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 <CVEid ALL>	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脆弱性を表示します。 CVEid All 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脆弱性をすべて表示します。
-v <ifix1, ifix2,...>	コンマで区切られた暫定修正リストを指定します。
-V <ifixgrp>	暫定修正グループ名を指定します。
-V <ifixgrp>	指定した ifix グループ名の下の ifix が自動的に更新されるかどうかを指定します。
autoupdate =<yes no>	Yes TNC サーバーで新規 ifix を受け取った場合に fspolicy に定義されるポリシーを自動的に更新します。 No TNC サーバーで新規 ifix を受信した後に、その ifix を手動でポリシーに割り当てることを指定します。「No」がデフォルト値です。

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. 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. **COMPLIANT** 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 COMPLIANT -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履歴を表示するには、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をログ・履歴から削除するには、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 クライアントの履歴を表示するには、次のコマンドを入力します。
`psconf list -H -i [ip|ALL]`

セキュリティ

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」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。

| **pscuiserverctl** コマンド

| 目的

| PowerSC GUI サーバー・オプションをセットアップするために使用します。

| 構文

| **pscuiserverctl -r set [arg1 [arg2 [arg3]]]**

| **pscuiserverctl set [httpPort]**

| **pscuiserverctl set [httpsPort]**

| **pscuiserverctl set [administratorGroupList]**

| **pscuiserverctl set [logonGroupList]**

| **pscuiserverctl set [powervcKeystoneUrl]**

| **pscuiserverctl set [QRadarSyslogResponseEnabled]**

| **pscuiserverctl set [tncServer]**

| フラグ

| **-r** パラメーター値の適用後に PowerSC GUI サーバーを再始動します。

| **set**

| PowerSC GUI サーバー・オプションを設定または取得します。

| パラメーター

| **httpPort** *httpPortno*

| PowerSC GUI で使用するデフォルト・ポートを表示または指定します。

| **httpsPort** *httpsPortno*

| PowerSC GUI で使用するデフォルト・セキュア・ポートを表示または指定します。

| **administratorGroupList** *unixgrp1,unixgrp2,...*

| PowerSC GUI を使用した管理者機能の実行が許可される UNIX グループを表示または指定します。

| **logonGroupList** *unixgrp1,unixgrp2,...*

| PowerSC GUI へのログインが許可される UNIX グループを表示または指定します。

| **powervcKeystoneUrl** *powervcKeystoneurl*

| PowerVC 鍵ストア・サーバーの URL を表示または指定します。

| **QRadarSyslogResponseEnabled on | off**

| PowerSC GUI からの Syslog ロギングの現行設定を表示するか、Syslog ロギングをオン/オフに設定
| します。

| **tncServer tncserver.abc.com**

| TNC サーバーのホスト名を表示または指定します。TNC サーバーのホスト名を変更した場合、
| PowerSC GUI サーバーを再始動する必要があります。

| 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. PowerSC GUI によって使用されるデフォルト・ポートとして現在指定されているものを表示する場
| 合:

| pscuiserverctl set httpPort

| 2. PowerSC GUI によって使用されるデフォルト・ポートを設定する場合:

| pscuiserverctl set httpPort 80

| 3. PowerSC GUI によって使用されるデフォルト・セキュリティー・ポートとして現在指定されている
| ものを表示する場合:

| pscuiserverctl set httpsPort

| 4. PowerSC GUI によって使用されるデフォルト・セキュリティー・ポートを設定する場合:

| pscuiserverctl set httpsPort 483

| 5. PowerSC GUI を使用した管理者機能の実行が許可される UNIX グループを表示する場合:

| pscuiserverctl set administratorGroupList

| 6. PowerSC GUI を使用した管理者機能の実行が許可される UNIX グループを設定する場合:

| pscuiserverctl set administratorGroupList securitygroup1,admingrp1

| 7. PowerSC GUI へのログインが許可される UNIX グループを表示する場合:

| pscuiserverctl set logonGroupList

| 8. PowerSC GUI へのログインが許可される UNIX グループを設定する場合:

| pscuiserverctl set logonGroupList unixgroup1,unixgrp2

| 9. PowerVC 鍵ストア・サーバーの URL を表示する場合:

| pscuiserverctl set powervcKeystoneUrl

| 10. PowerVC 鍵ストア・サーバーの URL を設定する場合:

| pscuiserverctl set powervcKeystoneUrl https://powervc/server/example/

| 11. PowerSC GUI からの Syslog ロギングがオンなのかオフなのかを表示する場合:

| pscuiserverctl set QRadarSyslogResponseEnabled

| 12. PowerSC GUI からの Syslog ロギングをオンまたはオフに設定する場合:

| pscuiserverctl set QRadarSyslogResponseEnabled on
| pscuiserverctl set QRadarSyslogResponseEnabled off

| 13. TNC サーバーのホスト名を表示する場合:

| pscuiserverctl set tncServer

- | 14. TNC サーバーのホスト名を設定する場合:
- | pscuiserverctl set tncServer tncserver.abc.com
- | 15. TNC サーバーのホスト名を設定した場合、PowerSC GUI サーバーを再始動する必要があります。
- | PowerSC GUI サーバーを再始動するには、以下のようにします。
- | pscuiserverctl -r set tncServer tncsl.rs.com

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 ] [-r|-R]
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・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・レベルに関連したすべてのセキュリティ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
-f

説明

指定された *Profile* ファイルに設定されたセキュリティ設定を適用します。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・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・オプションを指定します。 l low 低水準のセキュリティ・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・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・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 <code>/etc/security/aixpert/core/appliedaixpert.xml</code> 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 <code>/etc/security/aixpert/core/undo.xml</code> 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・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・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	-p フラグにより、端末と <code>aixpert.log</code> ファイルの両方への詳細出力が有効になります。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 <code>/etc/security/aixpert/check_report.txt</code> ファイルに書き込みます。出力をセキュリティ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。 注: -r フラグでは、プロファイルの適用操作のみがサポートされます。レベルの適用操作はサポートされません。
-R	-r オプションを指定した場合、ルールのメッセージ全体 (1 行以上) が表示されます。 -r フラグと同じ出力を生成します。また、このフラグは、構成設定の実装に使用されるルール・スクリプトまたはプログラムの説明の追加も行います。 注: -R フラグでは、プロファイルの適用操作のみがサポートされます。レベルの適用操作はサポートされません。
-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。

項目	説明
-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 <code>_AIXDefault.xml</code> になっているプロファイルを適用します。例えば、<code>NERC.xml</code> プロファイルを除去するには、<code>NERC_to_AIXDefault.xml</code> プロファイルを適用する必要があります。 • 適用操作後のシステムに対する変更は、元に戻す操作で失われます。設定は、適用操作前に存在していた値に戻ります。

パラメーター

項目	説明
<i>File</i>	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、 <code>root</code> アクセス権が必要です。
<i>Level</i>	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。
<i>Profile</i>	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、 <code>root</code> 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/pscxpert/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
<code>/usr/sbin/pscexpert</code>	pscexpert コマンドが入っています。

ファイル

項目	説明
<code>/etc/security/aixpert/log/aixpert.log</code>	適用済みセキュリティ設定のトレース・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。 pscexpert 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。
<code>/etc/security/aixpert/log/firstboot.log</code>	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、セキュリティ設定のトレース・ログが入っています。
<code>/etc/security/aixpert/core/undo.xml</code>	元に戻すことのできるセキュリティ設定の 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

- 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:

128 ページの『ルール of 非アクティブ化』
 トラストッド・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** | **-I** | **-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。
- I** 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. トラストッド・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. トラストッド・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. トラストッド・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:

178 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

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を提供し、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 Director of Licensing

IBM Corporation

North Castle Drive, MD-NC119

Armonk, NY 10504-1785

US

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。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

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ます、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を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は、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年).

このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。

© Copyright IBM Corp. _年を入れる_.

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ご確認ください。

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](http://www.ibm.com) は、世界の多くの国で登録された International Business Machines Corporation 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> 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]

アプリケーションのテスト 107
インストール 7, 138

[カ行]

概念 135
概要 5, 135
仮想ログ 131
仮想ログ・デバイスの表示 132
仮想ログ・デバイスへのデータの書き込み 134
クライアントの検証 145
クライアントの構成 140
クライアント・ポリシー 144
計画 114
継続的なコンプライアンスのためのシステムのモニター 108
検証結果の表示 146
コマンド
 chvfilt 177
 genvfilt 178
 lsvfilt 180
 mkvfilt 180
 pscuiserverctl 194
 rmvfilt 201
 vlantfw 202
コレクターのインストール 116
コンポーネント 135

[サ行]

サーバーの構成 140
システムの削除 118
システムの登録 116
システムの認証 117
失敗したルールの更新 107
失敗したルールの調査 106
修復の準備 114
証明書のインポート 137, 147
セキュア通信 137
セキュリティ
 PowerSC
 リアルタイム・コンプライアンス 111
セキュリティおよびコンプライアンス自動化の管理 105, 106,
 107, 108
前提条件 114

[タ行]

電子メール通知 143
トラステッド・ネットワーク接続 135, 136, 137, 138, 140, 141,
 143, 144, 145, 146, 147
トラステッド・ネットワーク接続およびバッチ管理 135
トラステッド・ネットワーク接続サーバー 143, 144
トラステッド・ブート 113, 114, 115, 116, 117, 118
トラステッド・ブートのインストール 115
トラステッド・ブートの概念 113
トラステッド・ブートの管理 117
トラステッド・ブートの構成 116
トラステッド・ファイアウォール 121
 インストール 123
 構成 124
 複数の SEA 125
 除去
 SEA 127
 ルールの作成 127
 ルールの非アクティブ化 128
トラステッド・ファイアウォールの概念 121
トラステッド・ロギング 131, 132, 134
 インストール 132
トラステッド・ロギングの概要 131
トラステッド・ロギングの構成 133
トラブルシューティング 118

[ナ行]

認証結果の解釈 117
の構成 140

[ハ行]

ハードウェア要件とソフトウェア要件 5
バッチ管理 135, 136, 138
バッチ管理サーバーの構成 141
フィーチャー
 PowerSC リアルタイム・コンプライアンス 111
プロトコル 137
米国国防総省の STIG への準拠 10
ベリファイヤーのインストール 116
ポリシーの管理 147

[マ行]

マイグレーションに関する考慮事項 115

[ラ行]

リアルタイム・コンプライアンス 111
レポート
 操作 174
 配布 175
 レポート・グループの選択 174
ログの表示 144

A

AIX syslog 133
AIX 監査サブシステム 133

C

chvfilt コマンド 177
cURL 135, 138

G

genvfilt コマンド 178
GUI インターフェース
 以前のタイム・スタンプへの RTC のロールバック 168
 以前のモニター構成への RTC ファイルのロールバック 169
 インストール 153
 エージェント 153
 エンドポイント 152
 エンドポイントとサーバーとの通信 159
 エンドポイントとサーバーとの通信を検査 159
 エンドポイントのグループ化 161
 エンドポイントの除去 159
 エンドポイントをグループに追加 161
 エンドポイント・グループの削除 162
 エンドポイント・グループの指定 155
 エンドポイント・グループの名前変更 162
 エンドポイント・グループの複製 162
 エンドポイント・セキュリティのモニター 168
概要 151
鍵ストア要求の検査 160
鍵ストア要求の生成 160
カスタム・エンドポイント・グループ 161
カスタム・プロファイルの削除 164
グループへの RTC 構成オプションのコピー 169, 171
グループ・スクリプトの実行 156
言語 158
コンプライアンス・イベント通知 167
コンプライアンス・プロファイル 162
コンプライアンス・プロファイルの検査 166, 167
コンプライアンス・プロファイルの作成 163
コンプライアンス・プロファイルの適用 164, 165
コンプライアンス・プロファイルの表示 163
コンプライアンス・プロファイルを元に戻す 166
サーバー 153
使用 157

GUI インターフェース (続き)

 セキュリティ 151
 セキュリティ証明書の作成 154
 セキュリティ・イベント通知 173
 他のグループへの RTC ファイル・リスト・モニター・オプションのコピー 170
 他のグループへの TE ファイル・リスト・モニター・オプションのコピー 171
 ナビゲート 158
 プロファイルをエンドポイントにコピー 164
 要件 153
PowerSC 製品の状況の表示 172
RTC 検査の実行 170
RTC の構成 168
RTC ファイル・リストの編集 169
TE の構成 170
TE ファイル・リストの編集 171
TE モニターの切り替え 173

I

IMC および IMV モジュール 138
IP リファラー 137

L

lsvfilt コマンド 180

M

mkvfilt コマンド 180

P

pmconf 136
pmconf コマンド 181
PowerSC 10, 95, 105, 108
 トラステッド・ファイアウォール
 インストール 123
 構成 124
 複数の SEA を使用した構成 125
 ルールの作成 127
 ルールの非アクティブ化 128
 SEA の除去 127
 トラステッド・ロギング
 インストール 132
 リアルタイム・コンプライアンス 111
PowerSC Standard Edition 5, 7
PowerSC Standard Edition のインストール 7
PowerSC のセキュリティおよびコンプライアンス自動化の構成 108
psconf コマンド 186
pscuiserverctl コマンド 194
pscxpert コマンド 196

R

rmvfilt コマンド 201

S

Server 135

SOX および COBIT 95

SUMA 135, 136, 138

T

TNC 148

TNC およびパッチ管理のトラブルシューティング 148

TNC クライアント 136

TNC クライアントの更新 146

TNC コンポーネントの管理 144

TNCPM 用のレポートおよび管理ツール

 pmconf コマンドを使用する 181

TNC、SUMA 用のレポートおよび管理ツール

 psconf コマンドを使用する 186

V

VIOS の IP リファラー 143

vlanfw コマンド 202



Printed in Japan