コンプライアンスを使用した設定の監査の実行

コンプライアンス監査の実行方法

次の表に、コンプライアンス機能を使用するための基本的な手順を示します。

	説明	参照先：
1	名前と他の説明テキストを含むコンプライアンス ポリシーを作成します。	新しいコンプライアンス ポリシーの作成 （3 ページ）
2	コンプライアンス ポリシーにルールを追加します。ルールは違反を構成するものを指定します。	コンプライアンス ポリシー ルールの作成 （3 ページ）

3	（ネットワーク デバイスで監査を実行するために使用する）コンプライアンス プロファイルを作成し、次の手順を実行します。 • コンプライアンス ポリシーをそのプロファイルに追加します。 • 監査に含めるポリシー ルールを選択します。 同じプロファイルに複数のカスタム ポリシーや定義済みのシステム ポリシーを追加できます。	ポリシーとルールが含まれているコンプライアンス プロファイルの作成 （10 ページ）
4	プロファイルを選択し、監査ジョブをスケジューリングして、コンプライアンス監査を実行します。	コンプライアンス監査の実行 （12 ページ）
5	コンプライアンス監査の結果を表示し、必要に応じて違反を修正します。	コンプライアンス監査の結果の表示 （13 ページ）

コンプライアンス監査の有効化および無効化

コンプライアンス機能は、デバイス設定ベースラインと監査ポリシーを使用して、ネットワーク デバイスの設定の逸脱を検出して訂正します。一部のコンプライアンス レポートはシステムパフォーマンスに影響する可能性があるため、デフォルトではこれは無効になっています。コンプライアンス機能を有効にするには、次の手順を実行します。

（注） コンプライアンス機能を使用するには、システムが『Cisco Evolved Programmable Network Manager Installation Guide』で指定されているプロフェッショナル サイジング要件を満たす必要があります。

（注） Cisco EPN Manager で、コンプライアンス監査を無効にすると、GUI からのコンプライアンスが無効になり、バックグラウンドでのコンプライアンスデータの収集が停止します。コンプライアンス設定を機能させるには、ユーザーが Cisco EPN Manager サーバーを再起動してデバイスを再同期する必要があります。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択し、**[一般（General）]** > **[サーバー（Server）]** を選択します。

ステップ 2 [コンプライアンス サービス（Compliance Services）] の横の [有効化（Enable）] をクリックし、次に [保存（Save）] をクリックします。

ステップ 3 アプリケーションを再起動します。

ステップ 4 デバイス インベントリを再同期します。手順としては、[インベントリ（Inventory）] > [ネットワークデバイス（Network Devices）] の順に選択し、すべてのデバイスを選択した後、[同期（Sync）] をクリックします。

（注） バージョン 3.0 にアップグレードする前に Cisco EPN Manager でコンプライアンスが有効になっていた場合、アップグレード後は [システム設定（System Settings）] でコンプライアンスが無効になります。ユーザーは、この項で説明する手順に従って手動でコンプライアンスを有効にする必要があります。この場合は、Cisco EPN Manager サーバーの再起動とデバイスの再同期は必要ありません。

新しいコンプライアンス ポリシーの作成

空のポリシー テンプレートから新しいコンプライアンス ポリシーを作成できます。

ステップ 1 **[設定（Configuration）]** > **[コンプライアンス（Compliance）]** > **[ポリシー（Policies）]** を選択します。

ステップ 2 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域にある [コンプライアンス ポリシーの作成（Create Compliance Policy）]（+）アイコンをクリックします。

ステップ 3 ダイアログボックスに名前と任意の説明を入力し、[作成（Create）] をクリックします。ポリシーが左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域に追加されます。

ポリシーを複製するには、ポリシーオプションボタンを選択し、[複製（Duplicate）] をクリックします。

コンプライアンス ポリシー ルールの作成

コンプライアンス ポリシー ルールはプラットフォーム固有であり、デバイスの違反と見なされるものを定義します。また、違反を修正する CLI コマンドをルールに含めることもできます。コンプライアンス監査ジョブを設定する際に監査に含めるルールを選択できます（コンプライアンス監査の実行 （12 ページ）を参照）。

Cisco EPN Manger は、AireOS ワイヤレス LAN コントローラ プラットフォームの監査をサポートします。

ステップ 1 **[設定（Configuration）]** > **[コンプライアンス（Compliance）]** > **[ポリシー（Policies）]** を選択して、左側のナビゲーション領域からポリシーを選択します。

ステップ 2 作業領域ペインから [新規（New）] をクリックし、新しいルールを追加します。

類似するルールがある場合は、[複製（Duplicate）] をクリックし、ルールを編集して新しい名前で保存することができます。

ステップ 3 ルールの基準を入力して新しいルールを設定します。

（注） Cisco EPN Manager は、すべての Java ベースの正規表現をサポートしています。http://www.rexegg.com/regex-quickstart.htmlを参照してください。

a) タイトル、説明、およびその他の情報を [ルール情報（Rule Information）] テキスト フィールドに入力します。この情報は、フリー テキストであり、ルールの設定には影響しません。

b) このルールの対象デバイスを [プラットフォームの選択（Platform Selection）] 領域に指定します。

c) （任意）[ルールの入力（Rule Inputs）] 領域で、[新規（New）] をクリックし、このルールを含んでいるポリシーの実行時にユーザーに表示する入力フィールドを指定します。たとえば、IP アドレスの入力を求めるプロンプトを表示できます。

（注） [複数の値の承認（Accept Multiple Values）] チェックボックスをオンにした場合は、すべてのルール入力が条件に一致している場合にのみ監査に合格します。

d) [条件とアクション（Conditions and Actions）] 領域で、[新規（New）] をクリックし、確認する基準を指定します。これにより、ルールの合否の条件が決定します。例：ルールの条件とアクション （4 ページ）の例を参考にしてください。

ステップ 4 [作成（Create）] をクリックします。ルールがコンプライアンス ポリシーに追加されます。

必要な数だけルールを作成できます。監査ジョブを実行する場合は、検証するルールを選択できることを覚えておいてください。

（注） 新しいコンプライアンス ポリシー ルールを作成したとき、正規表現を使用してルールまたはコマンドを検証するには、Java 正規表現を使用して式をテストすることをお勧めします。

次のタスク

コンプライアンス ポリシーとそのルールを含むプロファイルを作成し、そのプロファイルを使用して監査を実行します。ポリシーとルールが含まれているコンプライアンス プロファイルの作成 （10 ページ） を参照してください。

例：ルールの条件とアクション

条件およびアクションの例：デバイスに設定された DNS サーバー

このコンプライアンス ポリシーは、**IP name-server 1.2.3.4** または **IP name-server2.3.4.5** がデバイスに設定されているかどうかを確認します。設定されている場合、ポリシーは「DNSサー

バーを1.2.3.4または2.3.4.5として設定する必要があります（DNS server must be configured as either 1.2.3.4 or 2.3.4.5）」というメッセージで違反を発生させます。

タブ	タブ領域	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	条件一致基準（Condition Match Criteria）	演算子	式と一致させます。
		値	ip name-server {1.2.3.4|2.3.4.5}
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	違反は発生しません
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させる
		違反メッセージタイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	DNS サーバーを 1.2.3.4 または 2.3.4.5 として設定する必要があります

例：ブロック オプション

このコンプライアンス ポリシーでは、ある特定のブロック内に定義されている不正または未承認の SNMP コミュニティ文字列があるかどうかを確認します。ブロック内で検出された場合、ポリシーは「承認されていないコミュニティ文字列<1.1>を検出しました（Detected unauthorized community string <1.1>）」というメッセージで違反を報告し、すべての非準拠 SNMP 文字列をブロックから削除します。

タブ	タブ領域	フィールド	値
ルール情報（Rule Information）		ルール タイトル（Rule Title）	snmp-server community having non-standard entries
プラットフォームの選択（Platform Selection）			Cisco IOS デバイス、Cisco IOS-XE デバイス
Condition 1			

[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	ブロック オプション（Block Options）	ブロック開始表現（Block Start Expression） （このフィールドは、[ブロックとして解析（Parse as Blocks）] チェックボックスがオンになっている場合にのみ有効になります）	^snmp-server community .*
	条件一致基準（Condition Match Criteria）	演算子	式と一致させます。
		値	snmp-server community (.*)
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させません（Does Not Raise a Violation）
Condition 2			

[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	以前に一致したブロック（Previously Matched Blocks）
	ブロック オプション（Block Options）	ブロック開始表現（Block Start Expression） （このフィールドは、[ブロックとして解析（Parse as Blocks）] チェックボックスがオンになっている場合にのみ有効になります）	^snmp-server community .*
	条件一致基準（Condition Match Criteria）	演算子	式と一致させます。
		値	snmp-server community ((public RO)|(private RW))
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させます。
		違反メッセージ タイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	承認されていないコミュニティ文字列 <1.1> を検出しました。（Detected unauthorized community string <1.1>.）

（注） 上記の例では、最初の条件での一致基準は 1.1、1.2 などと呼びます。2 番目の条件での一致基準は 2.1、2.2 などと呼びます。

条件およびアクションの例：コミュニティ文字列

このコンプライアンス ポリシーは、**snmp-server community public** または **snmp-server community private** が（望ましくない）デバイスに設定されているかを確認します。設定されている場合、ポリシーは「コミュニティストリングxxxxxが設定されています（Community string *xxxxx* configured）」というメッセージで違反を発生させます。ここで、*xxx* は最初に見つかった違反です。

タブ	タブ領域	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	条件一致基準（Condition Match Criteria）	演算子	式と一致させます。
		値	snmp-server community {public|private}
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	違反を発生させる
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	続行（Continue）
		違反メッセージ タイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	コミュニティ ストリング *xxxxx* が設定されています。

条件およびアクションの例：IOS ソフトウェア バージョン

このコンプライアンス ポリシーは、Cisco IOS ソフトウェアのバージョン **15.0(2)SE7** がデバイスにインストールされているかどうかを確認します。インストールされていない場合、ポリシーは「show versionの出力に文字列xxxxxが含まれています（Output of show version contains the string *xxxxx*）」というメッセージで違反を発生させます。ここで *xxxx* は 15.0(2)SE7 と一致しない Cisco IOS ソフトウェア バージョンです。

タブ	タブ領域	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	デバイス コマンド出力
		show コマンド（Show Commands）	show version
	条件一致基準（Condition Match Criteria）	演算子	文字列を含む
		値	15.0(2)SE7

アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させます。
		違反メッセージ タイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	show version の出力に文字列 *xxxxx* が含まれています。

条件およびアクションの例：NTP サーバーの冗長性

このコンプライアンス ポリシーは、デバイスでコマンド **ntp server** が少なくとも 2 回表示されるかどうかを確認します。表示されない場合、ポリシーは、「少なくとも2つのNTPサーバーを構成する必要があります（At least two NTP servers must be configured）」というメッセージで違反を発生させます。

タブ	タブ領域	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	条件一致基準（Condition Match Criteria）	演算子	式と一致させます。
		値	(ntp server.*\n){2,}
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させる
		違反メッセージ タイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	NTP サーバーを 2 つ以上設定する必要があります。

ポリシーとルールが含まれているコンプライアンスプロファイルの作成

コンプライアンス プロファイルには、1 つ以上のコンプライアンス ポリシーが含まれています。コンプライアンス ポリシーをプロファイルに追加すると、すべてのポリシー ルールがプロファイルに適用されます。含めるポリシー ルールを選択すること（および、その他を無視すること）で、プロファイルをカスタマイズできます。複数のポリシーをプロファイルにグループ化すると、ルールをポリシーごとに選択したり、選択を解除することができます。

ルート ユーザー、管理者ユーザー、またはスーパー ユーザーとしてログインする場合は、次の操作を行えます。

- プロファイルの作成、編集、削除。
- [ポリシー（Policies）] ページで作成したルールの選択。

（注） 「その他」のユーザーが関連アクションを実行するには、次のタスク権限を有効にする必要があります。

- [コンプライアンス監査プロファイルアクセス（Compliance Audit Profile Access）] : プロファイルを実行および更新し、プロファイル内のポリシーを参照する。
- [コンプライアンス監査プロファイル編集アクセス（Compliance Audit Profile Edit Access）] : コンプライアンス監査プロファイルを作成および編集する。

タスク権限は、**[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** > **[ユーザーグループ（User Groups）]** ページで確認できます。

[コンプライアンス監査プロファイルへのアクセス（Compliance Audit Profile Access）] タスク権限を選択していないと、[コンプライアンス監査プロファイルの編集アクセス（Compliance Audit Profile Edit Access）] タスク権限を選択していても、[プロファイル（Profile）] ページを表示できません。

ステップ 1 **[設定（Configuration）]** > **[コンプライアンス（Compliance）]** > **[プロファイル（Profiles）]** を選択します。

ステップ 2 [コンプライアンス プロファイル（Compliance Profiles）] ナビゲーション領域にある [ポリシー プロファイルの作成（Create Policy Profile）]（+）アイコンをクリックします。この操作によって [コンプライアンス ポリシーの追加（Add Compliance Policies）] ダイアログボックスが開きます。

ステップ 3 プロファイルに含めるポリシーを選択します。ユーザー定義のポリシーが、[ユーザー定義（User Defined）] カテゴリで使用できるようになります。

a) [コンプライアンス ポリシーの追加（Add Compliance Policies）] ダイアログ ボックスで、追加するポリシーを選択します。

b) [OK] をクリックします。ポリシーが [コンプライアンス ポリシー セレクタ（Compliance Policy Selector）] 領域に追加されます。

ステップ 4 ポリシーに含めるルールを選択します。

a) [コンプライアンス ポリシー セレクタ（Compliance Policy Selector）] 領域でポリシーを選択します。ポリシーのルールは、右側の領域に表示されます。

b) 特定のルールを選択するか、または選択を解除して、[保存（Save）] をクリックします。

（注） ここで選択したルールのみが、このプロファイルのポリシー インスタンスに適用されます。この選択によって、コンプライアンス ポリシーの元のバージョンが変更されることはありません。

次のタスク

コンプライアンス監査の実行 （12 ページ）の説明に従って、コンプライアンス監査ジョブをスケジュールします。

コンプライアンス監査プロファイルのインポートおよびエクスポート

コンプライアンス プロファイルは XML ファイルとして保存されます。個々のコンプライアンス プロファイルをインポートおよびエクスポートできます。ファイルは、XML 形式でのみインポートできます。

コンプライアンス監査プロファイルのインポート

コンプライアンス監査プロファイルをインポートする前に、プロファイルに関連付けられているすべてのユーザー定義ポリシーが Cisco EPN Manager で使用可能であることを確認します。コンプライアンス プロファイルをインポートするには、次の手順を実行します。

1. **[設定（Configuration）]** > **[コンプライアンス（Compliance）]** > **[プロファイル（Profiles）]** に移動します。
2. 左側の **[コンプライアンス プロファイル（Compliance Profiles）]** 領域にある [プロファイルのインポート（Import Profiles）] アイコンをクリックします。
3. **[プロファイルのインポート（Import Profiles）]** ダイアログボックスで、**[プロファイルの選択（Choose Profiles）]** をクリックします。
4. プロファイル XML ファイルを参照して選択します。
5. （オプション）複数のプロファイルをインポートするには、**[追加ファイルの選択（Choose more files）]** をクリックし、プロファイル XML ファイルをアップロードします。
6. [Import] をクリックします。

Cisco EPN Managerは、無効なプロファイルXMLファイルがアップロードされた場合にエラーメッセージを表示します。インポートに失敗したプロファイルのログを確認するには、**[プロファイルのインポート（Import Profiles）]**ダイアログの警告アイコンをクリックします。

コンプライアンス監査プロファイルのエクスポート

コンプライアンス プロファイルをエクスポートするには、次の手順を実行します。

1. 左側の**[コンプライアンスプロファイル（Compliance Profiles）]**ナビゲーション領域のプロファイルの横にある [i] アイコンの上にマウスを合わせます。
2. **[ポリシープロファイル（Policy Profile）]**ポップアップウィンドウで、**[XMLとしてプロファイルをエクスポート（Export Profile as XML）]**ハイパーリンクをクリックし、ファイルを保存します。

コンプライアンス監査の実行

コンプライアンス監査を実行するには、プロファイルを選択し、監査するデバイスを選択し（プロファイル内のポリシーとルールを使用）、監査ジョブのスケジュールを設定します。

ステップ 1 **[設定（Configuration）]**>**[コンプライアンス（Compliance）]**>**[プロファイル（Profiles）]**を選択します。

ステップ 2 左側の[コンプライアンスプロファイル（Compliance Profiles）]ナビゲーション領域でプロファイルを選択します。

ステップ 3 [コンプライアンス プロファイル（Compliance Profiles）] ナビゲーション領域で [コンプライアンス監査の実行（Run Compliance Audit）] アイコンをクリックします。

ステップ 4 [デバイスおよび設定（Devices and Configuration）] 領域で、目的のデバイスと監査するコンフィギュレーション ファイルを選択します。

a) デバイス（またはデバイス グループ）を選択します。

b) 監査するコンフィギュレーション ファイルを指定します。

- [最新のアーカイブ済みの設定を使用（Use Latest Archived Configuration）]：アーカイブから最新のバックアップ ファイルを監査します。使用可能なバックアップ ファイルがない場合、Cisco EPN Managerはデバイスの監査を実行しません。
- [現在のデバイス設定を使用（Use Current Device Configuration）]：デバイスの実行コンフィギュレーションをポーリングし、監査します（たとえば、showコマンド出力はデバイスの実行コンフィギュレーションから生成されます）。

  このオプションを選択すると、Cisco EPN Managerは最初にデバイスからコンフィギュレーションのバックアップを取得してから監査を実行します。これは、定期的またはイベントがトリガーしたコンフィギュレーションバックアップが有効になっていない場合に役に立ち、また、Cisco EPN Managerにアーカイブ済みのコンフィギュレーションがデバイスとの同期が取れていないことが頻繁にあるため、便利です。

c) [次へ（Next）] をクリックします。

ステップ 5 [アイドル時間制限の設定（分）（Configure Idle Time Limit (min)）] フィールドに値を入力します。デフォルトでは、制限時間は 5 分に設定されます。ユーザーが制限時間を変更する場合は、5 ～ 30 の数字を入力できます。設定された制限時間の間アイドル状態が続くと、監査ジョブは中止されます。

ステップ 6 すぐに監査ジョブをスケジュール設定する場合は [今すぐ（Now）] を選択し、後でスケジュール設定する場合は [日付（Date）] を選択して日時を入力します。

監査ジョブを定期的に繰り返すには、[定期（Recurrence）] オプションを使用します。

ステップ 7 [終了（Finish）] をクリックします。監査ジョブがスケジュール設定されます。監査ジョブがスケジュールされると、通知ポップアップが表示されます。監査ジョブのステータスを表示するには、[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザージョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）] を選択します。

次のタスク

コンプライアンス監査の結果の表示 （13 ページ）の説明に従って、監査結果を確認します。

コンプライアンス監査の結果の表示

この手順を使用して、監査ジョブの結果を確認します。結果から、監査したデバイス、スキップしたデバイス、違反があったデバイスなどがわかります。単一のデバイスでさまざまなコンプライアンス ポリシーが実行されている場合があります。

ジョブを作成したら、そのジョブに関して次の設定を行えます。

- [シリーズを一時停止（Pause Series）]：後日に実行するようにスケジュール設定されているジョブのみに適用できます。実行中のジョブを一時停止することはできません。
- [シリーズを再開（Resume Series）]：一時停止されているジョブのみに適用できます。
- [スケジュールを編集（Edit Schedule）]：スケジュール済みのジョブを別の時間に再度スケジュール設定します。

ステップ 1 [管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザージョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）] を選択します。

ステップ 2 [監査ジョブ（Audit Jobs）] タブをクリックしてジョブを見つけ、[前回の実行（Last Run）] 列の情報を確認します。

最後の実行結果の値	説明
[失敗（Failure）]	監査した 1 つ以上のデバイスが、プロファイルで指定されたポリシーに違反しています。
[一部成功（Partial Success）]	コンプライアンス ジョブに、監査済みおよび監査なしのデバイスが両方含まれ、監査済みデバイスのコンプライアンス ステータスは成功です。

[成功 (Success)]	監査したすべてのデバイスは、プロファイルで指定されたポリシーに準拠しています。

コンプライアンス監査ジョブの場合、サポートされる違反の数は Cisco EPN Manager の標準設定で 20,000 件、Pro 以上の設定では 80,000 件です。

ステップ 3 監査の確認が失敗した場合は、次の手順を実行します。

- 失敗したデバイスを確認するには、[失敗（Failure）] ハイパーリンクの横にある [i] アイコンにカーソルを合わせて詳細のポップアップを表示します。
- ジョブを選択し、[ジョブの詳細を表示（View Job Details）] をクリックし、ポップアップのデバイスの横にある [i] アイコンをクリックして [デバイス 360（Device 360）] ビューを起動します。

ステップ 4 最も詳細な情報を確認するには、[失敗（Failure）] ハイパーリンクをクリックして [コンプライアンス監査違反の詳細（Compliance Audit Violation Details）] ウィンドウを開きます。

（注） [コンプライアンス監査違反の詳細（Compliance Audit Violation Details）] ウィンドウを行き来するには、[次へ（Next）] および [前へ（Previous）] ボタンを使用します。

次のタスク

違反を修正するには、デバイスのコンプライアンス違反の修正 （16 ページ）を参照してください。

違反ジョブの詳細の表示

次の表に、[違反の詳細（Violation Details）] ページから表示できる詳細を示します。

表示内容	選択方法
スケジュール済み修正可能違反ジョブのステータス。	**1.** [違反の詳細（Violation Details）] ページに移動します。 **2.** [修正可能（Fixable）] 列のフィルタ ボックスをクリックして、[実行中（Running）] を選択します。
修正済み違反ジョブの詳細。	**1.** [違反の詳細（Violation Details）] ページに移動します。 **2.** [修正可能（Fixable）] 列のフィルタ ボックスをクリックして、[修正済み（Fixed）] を選択します。 **3.** [修正済み（Fixed）] リンクをクリックします。

修正失敗違反ジョブの詳細。	**1.** [違反の詳細（Violation Details）] ページに移動します。 **2.** [修正可能（Fixable）] 列のフィルタ ボックスをクリックして、[修正失敗（Fix Failed）] を選択します。 **3.** [修正失敗（Fix Failed）] リンクをクリックします。

監査の失敗および違反のサマリー詳細の表示

詳細な違反情報を表示し、このデータをエクスポートし、コンプライアンス ジョブの詳細を表示できます。特定のジョブの詳細データをエクスポートしたり、複数のジョブのサマリーデータをエクスポートすることができます。

ステップ 1 [管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザージョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）] を選択します。

ステップ 2 特定の監査ジョブの詳細を表示するには、次の手順を実行します。

a) [監査ジョブ（Audit Jobs）] タブをクリックして、ジョブを見つけます。

b) [失敗（Failure）] ハイパーリンクをクリックし、[コンプライアンス監査の詳細（Compliance Audit Details）] ウィンドウを表示します。

ポリシー名、設定したルール、そのコンプライアンス状態、合計違反数、ジョブのインスタンス カウント、その中で最も重大度の高い値、および無視したカウント値に関する情報を表示できます。

c) これらの詳細をエクスポートするには、次のいずれかのオプションを使用します。

- 違反の詳細は Microsoft Excel スプレッドシートに XLS でエクスポートするには、[XLS としてエクスポート（Export as XLS）] をクリックします。
- 違反の詳細を Microsoft Excel スプレッドシートにカンマ区切りのテキストでエクスポートするには、[CSV としてエクスポート（Export as CSV）] をクリックします。
- 違反の詳細を HTML ファイルにエクスポートするには、[HTML としてエクスポート（Export as HTML）] をクリックします。

d) [ファイルの保存（Save File）] をクリックします。

ステップ 3 すべての監査ジョブの総合的なサマリーを表示するには、次の手順を実行します。

a) [違反サマリー（Violation Summary）] タブをクリックします。

違反が発生したすべてのデバイス、その関連のポリシーとプロファイル名、監査ジョブ ID、関連ルールとルールの重大度値、違反の修正が可能かどうかの詳細、またはすでに修正されているかどうか、違反に関連付けられたメッセージについて総合的なレポートを表示できます。

b) この詳細なサマリー レポートをエクスポートするには、ドロップダウン メニューから次のいずれかのオプションを選択します。

- サマリーを Microsoft Excel spreadsheet にカンマ区切りのテキストでエクスポートするには、[違反レポート CSV（Violation Report CSV）] をクリックします。
- サマリーを PDF ファイルをエクスポートするには、[違反レポート PDF（Violation Report PDF）] をクリックします。

c) [ファイルの保存（Save File）] をクリックします。

次のタスク

違反を修正するには、デバイスのコンプライアンス違反の修正 （16 ページ）を参照してください。

デバイスのコンプライアンス違反の修正

この手順を使用して、失敗したコンプライアンス監査のコンプライアンス違反を修正します。

ステップ 1 [管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザージョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）] を選択します。

ステップ 2 [監査ジョブ（Audit Jobs）] をクリックしてジョブを見つけ、[前回の実行結果（Last Run Result）] 列の情報を確認します。

ステップ 3 [失敗（Failure）] ハイパーリンクをクリックし、[コンプライアンス監査違反の詳細（Compliance Audit Violation Details）] ウィンドウを開きます。

（注） [コンプライアンス監査違反の詳細（Compliance Audit Violation Details）] ウィンドウを行き来するには、[次へ（Next）] および [前へ（Previous）] ボタンを使用します。

ステップ 4 [ジョブの詳細と違反（Job Details and Violations）] 領域で [次へ（Next）] をクリックします。

ステップ 5 [デバイス別の違反（Violations by Device）] 領域でデバイスと違反を選択し、[次へ（Next）] をクリックします。

ステップ 6 [修正ルールの入力（Fix Rule Inputs）] 領域で、以前にポリシーで定義した修正コマンドをプレビューし、[次へ（Next）] をクリックします。

条件に対するアクションとして修正 CLI の ^<Rule input ID>^ を使用してカスタム ポリシーを作成した場合は、[修正ルールの入力（Fix Rule Inputs）] タブが表示されます。必須の修正ルールの値を入力して [次へ（Next）] をクリックします。

ステップ 7 [修正コマンドのプレビュー（Preview Fix Commands）] ポップアップに表示された設定を確認します。

ステップ 8 生成された設定がデバイスに展開できるように修正ジョブのスケジュールを設定し、[修正ジョブのスケジュール設定（Schedule the Fix Job）] をクリックします。

（注） ユーザーは、デバイスのスタートアップ コンフィギュレーションにコンプライアンス修正 CLI を追加できます。これにより、デバイスの再起動時にも修正 CLI が保持されます。

次のタスク

違反ジョブの詳細を表示するには、監査の失敗および違反のサマリー詳細の表示 （15 ページ）を参照してください。

監査の失敗および違反のサマリー詳細の表示

詳細な違反情報を表示し、このデータをエクスポートし、コンプライアンス ジョブの詳細を表示できます。特定のジョブの詳細データをエクスポートしたり、複数のジョブのサマリーデータをエクスポートすることができます。

ステップ 1 [管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザージョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）] を選択します。

ステップ 2 特定の監査ジョブの詳細を表示するには、次の手順を実行します。

a) [監査ジョブ（Audit Jobs）] タブをクリックして、ジョブを見つけます。

b) [失敗（Failure）] ハイパーリンクをクリックし、[コンプライアンス監査の詳細（Compliance Audit Details）] ウィンドウを表示します。

ポリシー名、設定したルール、そのコンプライアンス状態、合計違反数、ジョブのインスタンス カウント、その中で最も重大度の高い値、および無視したカウント値に関する情報を表示できます。

c) これらの詳細をエクスポートするには、次のいずれかのオプションを使用します。

- 違反の詳細は Microsoft Excel スプレッドシートに XLS でエクスポートするには、[XLS としてエクスポート（Export as XLS）] をクリックします。
- 違反の詳細を Microsoft Excel スプレッドシートにカンマ区切りのテキストでエクスポートするには、[CSV としてエクスポート（Export as CSV）] をクリックします。
- 違反の詳細を HTML ファイルにエクスポートするには、[HTML としてエクスポート（Export as HTML）] をクリックします。

d) [ファイルの保存（Save File）] をクリックします。

ステップ 3 すべての監査ジョブの総合的なサマリーを表示するには、次の手順を実行します。

a) [違反サマリー（Violation Summary）] タブをクリックします。

違反が発生したすべてのデバイス、その関連のポリシーとプロファイル名、監査ジョブ ID、関連ルールとルールの重大度値、違反の修正が可能かどうかの詳細、またはすでに修正されているかどうか、違反に関連付けられたメッセージについて総合的なレポートを表示できます。

b) この詳細なサマリー レポートをエクスポートするには、ドロップダウン メニューから次のいずれかのオプションを選択します。

- サマリーを Microsoft Excel spreadsheet にカンマ区切りのテキストでエクスポートするには、[違反レポート CSV（Violation Report CSV）] をクリックします。
- サマリーを PDF ファイルをエクスポートするには、[違反レポート PDF（Violation Report PDF）] をクリックします。

c) [ファイルの保存（Save File）] をクリックします。

次のタスク

違反を修正するには、デバイスのコンプライアンス違反の修正 （16 ページ）を参照してください。

コンプライアンス ポリシーのインポートおよびエクスポート

コンプライアンス ポリシーは XML ファイルとして保存されます。個別のコンプライアンス ポリシーをエクスポートし、必要に応じて、それらのポリシーを別のサーバーにインポートすることができます。ファイルは、XML 形式でのみインポートできます。

ステップ 1 **[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）]** を選択します。

ステップ 2 コンプライアンス ポリシーをエクスポートするには、次の手順を実行します。

a) 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域のポリシーの横にある [i] アイコンの上にマウスを合わせます。

b) ポップアップ ウィンドウで、[XML としてポリシーをエクスポート（Export Policy as XML）] ハイパーリンクをクリックし、ファイルを保存します。

ステップ 3 コンプライアンス ポリシーをインポートするには、次の手順を実行します。

a) 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域の上にある [ポリシーのインポート（Import Policies）] アイコンをクリックします。

b) [ポリシーのインポート（Import Policies）] ダイアログボックスで、[ポリシーの選択（Choose Policies）] をクリックします。

c) XML ファイルを参照して選択します。

d) [インポート（Import）] をクリックします。

コンプライアンスポリシーXMLファイルのコンテンツの表示

コンプライアンス ポリシーは XML ファイルとして保存されます。ポリシーの XML ファイルの内容を表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）]** を選択します。

ステップ 2 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域でポリシーを見つけ、そのポリシーの横にある [i] アイコンの上にマウスを合わせます。

ステップ 3 ポップアップ ウィンドウで、[XMLとしてポリシーを表示（View Policy as XML）] ハイパーリンクをクリックします。Cisco EPN Manager によって内容が XML 形式で表示されます。

PSIRT および EOX 情報の表示

（注） [PSIRTとEOX（PSIRT and EOX）] ページには、PAS および RBML バンドルの生成日が表示されます。PAS レポートには、バンドルの生成日以前に公開された PSIRT および EoX レコードが保持されます。バンドルの生成後に公開された PSIRT レコードは表示されません。

デバイスのセキュリティ脆弱性の表示

レポートを実行して、Cisco Product Security Incident Response Team（PSIRT）によって定義されているセキュリティの脆弱性が、ネットワーク内のデバイスにあるかどうかを判断できます。レポートには、[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報が含まれます。また、特定の脆弱性に関するマニュアルを参照できます。このマニュアルでは、脆弱性の影響と環境を保護するために必要と考えられる手順が説明されています。

（注） PSIRT および EOX レポートを特定のデバイスに対して実行することはできません。PSIRT および EOX ジョブのスケジュールを設定すると、管理対象で完了状態にあるすべてのデバイスに対してレポートが生成されます（[インベントリ（Inventory）]>[設定（Configuration）]>[ネットワークデバイス（Network Devices）] ページ）。

始める前に

ジョブのスケジュールを設定する前にデバイスを同期します。**[設定（Configuration）]**>**[ネットワーク デバイス（Network Devices）]** を選択し、デバイスを選択して [同期（Sync）] をクリックします。

ステップ 1 **[レポート（Reports）]** > **[PSIRT と EOX（PSIRT and EoX）]** を選択します。

ステップ 2 ジョブのスケジュールを設定して実行します。[スケジュール（Schedule）] ダイアログボックスが表示されます。[開始時刻（Start Time）] オプションと [繰り返し（Recurrence）] オプションを設定してから、[送信（Submit）] ボタンをクリックしてジョブをスケジュールすることができます。表示されるポップアップで [OK] ボタンをクリックして、すでにスケジュールされているジョブを削除し、新しいジョブを作成します。

[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。作成する必要のないジョブはそれぞれのタブで区別します。

ステップ 3 PSIRT レポートの現在のステータスを表示するには、[ジョブの詳細を表示（View Job Details）] をクリックします。

ステップ 4 レポートが完了したら、[デバイス PSIRT（Device PSIRT）] タブをクリックして PSIRT 情報を表示します。

ステップ 5 [PSIRT タイトル（PSIRT Title）] 列のハイパーリンクをクリックすると、セキュリティの脆弱性の詳しい説明が表示されます。

ステップ 6 （任意）デバイスの PSIRT の詳細はデバイスごと、またはすべてのデバイスをまとめて PDF 形式および CSV 形式でエクスポートできます。

デバイスのハードウェアとソフトウェアのサポート終了レポートの表示

レポートを実行して、ネットワーク内のシスコ デバイス ハードウェアまたはソフトウェアがサポート終了（EOX）に到達しているかどうかを判断できます。これは、製品のアップグレードや代替オプションを決定する際に役立ちます。

ステップ 1 [レポート（Reports）] > [PSIRTとEOX（PSIRT and EOX）] を選択します。

ステップ 2 [ジョブのスケジュール（Schedule Job）] をクリックします。[スケジュール（Schedule）] ダイアログボックスが表示されます。[開始時刻（Start Time）] オプションと [繰り返し（Recurrence）] オプションを設定してから、[送信（Submit）] ボタンをクリックしてジョブをスケジュールすることができます。表示されるポップアップで [OK] ボタンをクリックして、すでにスケジュールされているジョブを削除し、新しいジョブを作成します。

[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。タブごとに個別のジョブは作成しません。

ステップ 3 ジョブの完了後に、次のEOXタブのいずれかをクリックすると、そのタブ固有のレポート情報が表示されます。

- **デバイス ハードウェア EOX（Device Hardware EOX）**
- **デバイス ソフトウェア EOX（Device Software EOX）**

ステップ 4 （任意）これらのデバイス EOX の詳細は、デバイスごとまたはすべてのデバイスをまとめて PDF 形式および CSV 形式でエクスポートできます。

モジュール ハードウェアのサポート終了レポートの表示

レポートを実行して、ネットワーク内のシスコモジュールハードウェアがサポート終了（EOX）に到達しているかどうかを判断できます。これは、製品のアップグレードや代替オプションを決定する際に役立ちます。

ステップ 1 [レポート（Reports）] > [PSIRTとEOX（PSIRT and EOX）] を選択します。

ステップ 2 [ジョブのスケジュール（Schedule Job）] をクリックします。[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。タブごとに個別のジョブは作成しません。

ステップ 3 [モジュールハードウェアEOX（Module Hardware EOX）] タブをクリックして、モジュール ハードウェアの情報を表示します。

ステップ 4 （任意）これらの EOX の詳細は、モジュールごとに PDF 形式および CSV 形式でエクスポートできます。

デバイスのフィールド通知の表示

レポートを実行して、完全なインベントリ収集が完了している管理対象シスコデバイスにField Noticeがあるかどうかを判断できます。Field Noticeとは、セキュリティ脆弱性の問題以外でシスコ製品に直接関係する重要な問題に関する通知です。通常、アップグレード、回避策、またはその他の対策が必要となります。

ステップ 1 [レポート（Reports）] > [PSIRTとEOX（PSIRT and EOX）] を選択します。

ステップ 2 [ジョブのスケジュール（Schedule Job）] をクリックします。[スケジュール（Schedule）] ダイアログボックスが表示されます。[開始時刻（Start Time）] オプションと [繰り返し（Recurrence）] オプションを設定してから、[送信（Submit）] ボタンをクリックしてジョブをスケジュールすることができます。表示されるポップアップで [OK] ボタンをクリックして、すでにスケジュールされているジョブを削除し、新しいジョブを作成します。

[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。タブごとに個別のジョブは作成しません。

ステップ 3 [フィールド通知（Field Notice）] タブをクリックすると、フィールド通知の情報が表示されます。

ステップ 4 [脆弱（Vulnerable）] 列の [i] アイコンをクリックして、[フィールド通知URL（Field Notice URL）] および [警告の詳細（Caveat Details）] ダイアログボックスを開きます。cisco.com で詳細を確認するには、[フィールド通知URL（Field Notice URL）] をクリックします。

ステップ 5 （任意）デバイスのフィールド通知の詳細はデバイスごと、またはすべてのデバイスをまとめてPDF形式およびCSV形式でエクスポートできます。