コンプライアンスを使用した設定の監査の実行

この章は次のトピックで構成されています。

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 Prime Infrastructure Quick Start 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） Prime Infrastructure バージョン 3.0 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 データ収集が停止されます。コンプライアンス設定を機能させるには、ユーザが Prime Infrastructure サーバ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（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 Prime Infrastructure 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、Prime Infrastructure サーバ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、[i] アイコンをクリックし、[ポリシーの複製（Duplicate Policy）] を選択します。

次のタスク

コンプライアンス ポリシーにルールを追加します。コンプライアンス ポリシー ルールの作成（3 ページ） を参照してください。

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）。

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） [新しいルール（New Rule）] ウィンドウに表示されるフィールドの説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください（そのドキュメントの情報も Prime Infrastructure に適用されます）。

（注） Prime Infrastructure 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 （5 ページ）の例を参考にしてください。

[ブロックオプション（Block Options）] セクションの [ブロックとして解析（Parse as Blocks）] チェック ボックスをオンにして、実行コンフィギュレーション全体をブロックに分割し、各ブロック内の条件一致基準値を検索します。

[ブロック開始式（Block Start Expression）] および [ブロック終了式（Block End Expression）] テキスト ボックスで指定した開始式と終了式に基づいて、ブロックが分割されます。ブロックが形成されると、各ブロックは [条件一致基準（Condition Match Criteria）] セクションの [値（Value）] フィールドで指定された条件と照合され、対応するアクションが実行されます。2 番目の条件では、[以前に一致したブロック（Previously Matched Blocks）] として [条件の範囲（Condition Scope）] を選択して解析する必要があります。

（注） [ブロックとして解析（Parse as Blocks）] チェック ボックスをオンにせずに一致条件値を検索すると、実行コンフィギュレーション全体が解析され、一致するすべてのインスタンスに対して 1 つの違反が発生します。

[一致アクションの選択（Select Match Action）] セクションで [続行（Continue）] オプションを選択し、[不一致アクションの選択（Select Does not Match Action）] セクションで [違反を発生させない（Does Not Raise a Violation）] オプションを選択することは避けてください（逆も同様）。新しいルールの作成ではこれらの組み合わせは無効です。

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

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。

（注） コンプライアンス ポリシーを設定すると、1 つの入力変数で複数の入力値を使用できます。ルール入力領域で [複数の値の使用（Accept Multiple Values）] チェックボックスを選択します。

次に、[条件一致基準（Condition Match Criteria）] 領域の [値（Value）] フィールドで指定された変数の例を示します。

[snmp-server community <_community> RO]：最後のルールが入力されるまで、すべてのルール入力値に基づいて違反を確認します。 この場合、違反メッセージには、すべての入力値がカンマ区切り値として含まれます。たとえば、SNMP コミュニティ [デモ、チェック] が見つかりません。

[snmp-server community <_community.4> RO]：4 番目のルール入力値のみに基づいて違反を確認します。

指定するルール入力値の数が、演算子「.」の後に記載された数字以外にならないようにします。

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）	ユーザ定義の違反メッセージ
		違反テキスト（Violation Text）	NTP サーバを 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、管理者ユーザ、またはスーパー ユーザ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（Users）]** > **[ユーザ、ロール、およびAAA（Users, Roles & AAA）]** > **[ユーザグループ（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。ユーザ定義のポリシーが、[ユーザ定義（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、Prime Infrastructure 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

  このオプションを選択すると、Prime Infrastructure 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、Prime Infrastructure 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。

（注） コンプライアンス ルールの指定時に [デバイス コマンドの出力（Device Commands Outputs）] に [条件付き範囲（Conditional Scope）] を選択した場合、show コマンドの出力は最新または現在のアーカイブ済み設定からではなく、デバイスから直接取得されます。

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 8 ジョブの完了後に電子メールが届きます。電子メールの件名には、ホスト名：ジョブ タイプ：プロファイル名：監査ジョブのジョブ ステータス、およびホスト名：ジョブ タイプ：修正ジョブのジョブ ステータスが含まれています。[メールサーバ設定（Mail Server Configuration）] 画面または [ジョブ通知メール（Job Notification Mail）] 画面でユーザが件名を指定している場合は、これも含まれます。

ステップ 9 監査ジョブに対してトリガーされた電子メールでは、ジョブ名、ジョブ タイプ、ステータス、前回の実行ステータス、PI ホスト名、PI ホスト IP、ポリシープロファイル名、総デバイス数、監査対象デバイス数、非監査対象デバイス数、およびプロファイルとジョブの詳細を確認するためのリンクが提供されます。

ステップ 10 修正ジョブに対してトリガーされた電子メールでは、ジョブ名、ジョブ タイプ、ステータス、前回の実行ステータス、PI ホスト名、PI ホスト IP、およびジョブの詳細を確認するためのリンクが提供されます。

ステップ 11 ジョブの詳細は、CSV 形式の添付ファイルとして届きます。CSV ファイルはパスワードで保護されていません。

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 Prime Infrastructure 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。

- 失敗のサマリーについては、[ジョブの詳細と違反（Job Details and Violations）] を確認します。フィールドの説明については、『Cisco Prime Infrastructure Field Reference』の *[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザジョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）]* のセクションを参照してください。
- デバイスごとの詳細については、[デバイス別の違反（Violations by Device）] 領域を確認します。

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 （14 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

Prime Infrastructure では、デバイスで発生するコンプライアンス違反を修正できます。

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 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 コンプライアンス違反が検出されたいずれかのジョブの [最後の実行結果（Last Run Result）] 列で [失敗（Failure）] をクリックします。Prime Infrastructure に、コンプライアンス監査の一部として実行されたすべてのポリシーの違反ステータスが表示されます。

ステップ 3 [違反の詳細（Violation Details）] ページで単一または複数の修正可能な違反を選択し、[次へ（Next）] をクリックします。

修正可能なすべての違反を選択した場合や、修正可能な違反の数が 15,000 件を超える場合は、最初の 15,000 行のみが選択されます。

ステップ 4 [起動設定の保存（Save Startup Config）] をクリックし、[実行中の設定を起動設定にコピー（Copy Running Config to Startup）] オプションを選択して、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーできます。

ステップ 5 展開矢印をクリックし、[修正の入力（Enter Fix Input）] オプションが有効になっているデバイスを表示します。

ステップ 6 修正を適用するデバイスを選択して [修正の入力（Enter Fix Input）] をクリックし、詳細を入力します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定変更をデバイスに適用するスケジュールを選択して、[修正ジョブのスケジュール（Schedule Fix Job）] をクリックします。

重要 コンプライアンス ポリシーは、すでに追加されている管理対象デバイスに対するデバイス OS、ファミリ、および製品の変更要求を無視します。デバイスの移行中にデバイスを削除して再追加することをお勧めします。

関連トピック

新しいコンプライアンス ポリシーの作成 （3 ページ）
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）
コンプライアンス監査の結果の表示 （13 ページ）
違反サマリーの詳細の表示 （15 ページ）
違反ジョブの詳細の表示 （16 ページ）

違反サマリーの詳細の表示

レポートを実行して、失敗したすべての監査ジョブの違反を要約した詳細を表示できます。レポートを生成するには、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）] > [違反サマリー（Violation Summary）] を選択します。

レポートには、ジョブ失敗の要約情報が表示されます。

ステップ 2 PDF および CSV 形式でレポートをダウンロードできます。

サーバ メモリが設定されたメモリよりも少ない場合、次のコンプライアンス レポートをエクスポートすることはできません。また、1 つのコンプライアンス エクスポート ジョブが実行中の場合、別のコンプライアンス レポートをエクスポートすることはできません。

- 違反サマリ レポート
- PSIRT および EOX レポート（デバイス PSIRT、デバイス ハードウェア EOX、デバイス ソフトウェア EOX、フィールド通知）
- コンプライアンス ジョブ
  - 監査ジョブの障害 > 違反の詳細レポート
  - 監査ジョブの成功レポート
  - 修正ジョブの成功レポート
  - 修正ジョブの失敗レポート

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。

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。

e) インポートに失敗したポリシーのログを確認するには、[ポリシーのインポート（Import Policies）] の横にある警告アイコンをクリックします。

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。Prime Infrastructure 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。

PSIRT レポートには、セキュリティ影響評価（SIR）が「重要」または「高」であるデータのみが含まれます。現在 Prime Infrastructure では、PSIRT 脆弱性評価に CLI 出力を使用することはサポートされていません。

（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。

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 [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。

[モジュールPID（Module PID）] 列に PID データが表示されます。これは、1 つの PID または PID のグループです。PID のグループの場合、特定のモジュール ハードウェアにマッピングされた PID に基づいてサポート終了の詳細が表示されます。同様に、別のサポート終了の詳細と PID をマッピングすることはできません。特定の EOL の詳細と PID をマッピングするには、レポートを手動で確認する必要があります。ハードウェアがコンテナで使用できない場合、[モジュールPID（Module PID）] 列にデータは表示されません。モジュール シャーシ PID とサブモジュール PID が同じ場合、PAS の詳細は表示されません。固定モジュールには PID がありません。したがって、EOL の詳細は表示されません。

ステップ 4 （任意）モジュール ハードウェア 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。

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。FieldNotice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。