ネットワークデバイスのコンプライアンス監査

コンプライアンスの概要

コンプライアンスは、元のコンテンツに影響を与えることなく注入または再設定される可能性があるネットワークのインテント逸脱やアウトオブバンドの変更を特定するのに役立ちます。

ネットワーク管理者は、Cisco DNA Center でソフトウェアイメージ、PSIRT、ネットワークプロファイルなどコンプライアンスのさまざまな側面のコンプライアンス要件を満たさないデバイスを簡単に特定できます。

コンプライアンスチェックは、自動化することも、オンデマンドで実行することもできます。

- 自動コンプライアンスチェック：Cisco DNA Center でデバイスから収集された最新のデータを使用します。このコンプライアンスチェックは、インベントリやSWIMなどさまざまなサービスからのトラップと通知をリッスンして、データを評価します。
- 手動コンプライアンスチェック：Cisco DNA Center でユーザーが手動でコンプライアンスをトリガーできます。
- スケジュールされたコンプライアンスチェック：スケジュールされたコンプライアンスジョブは、毎週実行されるコンプライアンスチェック（毎週土曜日の午後 11 時に実行）です。

手動コンプライアンスの実行

Cisco DNA Center では、コンプライアンスチェックを手動でトリガーできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 一括してコンプライアンスチェックを行う場合は、次の手順を実行します。

a) 該当するすべてのデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

ステップ 3 デバイスごとにコンプライアンスチェックを行う場合は、次の手順を実行します。

a) コンプライアンスチェックを実行するデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

c) あるいは、[Compliance] 列（使用可能な場合）をクリックし、[Run Compliance] をクリックします。

ステップ 4 デバイスの最新のコンプライアンスステータスを表示するには、次の手順を実行します。

a) デバイスとインベントリを選択します。デバイス情報の再同期を参照してください。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

（注）
- 到達不能のデバイスやサポートされていないデバイスに対してコンプライアンスの実行をトリガーすることはできません。
- デバイスに対してコンプライアンスを手動で実行しない場合、コンプライアンスチェックはコンプライアンスのタイプに応じて一定期間後に実行されるように自動的にスケジュールされます。
- CLIテンプレートコンプライアンスは、実現されたテンプレートをデバイスの実行コンフィギュレーションと比較します。実行コンフィギュレーションは、デバイスで使用可能な最新のアーカイブから取得されます。

  イベントベースのアーカイブは、トラップを受信してから更新されるまでに少なくとも 5 分かかります。したがって、正確な結果を得るには、構成の変更後にコンプライアンスを手動で実行する前に、少なくとも 5 分間待つことをお勧めします。

コンプライアンスサマリーの表示

インベントリページには、デバイスごとにコンプライアンスの集約ステータスが表示されます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

コンプライアンス列には、デバイスごとに集約コンプライアンスステータスが表示されます。

ステップ 2 コンプライアンスステータスをクリックすると、コンプライアンス サマリー ウィンドウが開きます。このウィンドウには、選択したデバイスに適用可能な次のコンプライアンスチェックが表示されます。

- スタートアップ設定と実行中の設定
- ソフトウェア イメージ
- 重大なセキュリティの脆弱性
- ネットワークプロファイル
- ファブリック
- アプリケーションの可視性

（注） [Network Profile]、[Fabric]、および [Application Visibility] はオプションであり、デバイスが必要なデータでプロビジョニングされている場合にのみ表示されます。

デバイスのスタートアップ設定と実行中の設定の同期

デバイスのスタートアップ コンフィギュレーションと実行コンフィギュレーションに不一致がある場合、修復同期を実行して設定を一致させることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 一括修復の場合は、次の手順を実行します。

a) 該当するすべてのデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Sync Start vs Run Configuration]** の順に選択します。

デバイスごとの修復の場合は、次の手順を実行します。

a) 修復同期を実行するデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Sync Start vs Run Configuration]** の順に選択します。または、コンプライアンスの列をクリックし、**[Compliance Summary]** > **[Startup vs Running Configuration]** > **[Sync Device Config]** の順に選択します。

ステップ 3 デバイスの修復ステータスを表示するには、次の手順を実行します。

a) メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Compliance Remedial Status]** の順に選択します。

コンプライアンスのタイプ

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
スタートアップ設定と実行中の設定	このコンプライアンスチェックは、デバイスのスタートアップ設定と実行中の設定が同期しているかどうかを識別するために役立ちます。デバイスのスタートアップ設定と実行中の設定が同期していない場合は、コンプライアンスがトリガーされ、アウトオブバンド変更の詳細レポートが表示されます。スタートアップ設定と実行中の設定の比較に関するコンプライアンスは、アウトオブバンド変更の 5 分以内にトリガーされます。	• [Noncompliant]：スタートアップ設定と実行中の設定は同じではありません。詳細ビューには、スタートアップと実行中との違いか、または実行中と以前の実行中との違いが表示されます。 • [Compliant]：スタートアップ設定と実行中の設定は同じです。 • [NA (Not Applicable)]：このコンプライアンスタイプのデバイス（AireOS など）はサポートされていません。
ソフトウェアイメージ	このコンプライアンスチェックは、Cisco DNA Center のタグ付きのゴールデンイメージがデバイスで実行されているかどうかをネットワーク管理者が確認するために役立ちます。これにより、デバイスのゴールデンイメージと実行中のイメージとの違いがわかります。ソフトウェアイメージに変更があると、遅延なくすぐにコンプライアンスチェックがトリガーされます。	• [Noncompliant]：デバイスは、デバイスファミリのタグ付きのゴールデンイメージを実行していません。 • [Compliant]：デバイスは、デバイスファミリのタグ付きのゴールデンイメージを実行しています。 • [NA (Not Applicable)]：選択したデバイスファミリではゴールデンイメージを使用できません。
重大なセキュリティ（PSIRT）	このコンプライアンスチェックでは、ネットワークデバイスが重大なセキュリティの脆弱性なしで実行されているかどうかを確認できます。	• [Noncompliant]：デバイスに重要なアドバイザリがあります。詳細レポートには、その他のさまざまな情報が表示されます。 • [Compliant]：デバイスに重大な脆弱性はありません。 • [NA (Not Applicable)]：Cisco DNA Center でネットワーク管理者がセキュリティ アドバイザリ スキャンを実行していないか、デバイスがサポートされていません。

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
ネットワークプロファイル	Cisco DNA Centerでは、ネットワークプロファイルでインテント設定を定義して、そのインテントをデバイスにプッシュできます。アウトオブバンド変更またはその他の変更のために任意の時点で違反が検出された場合、このチェックにより、それが識別されて、評価され、フラグが立てられます。違反は、コンプライアンス サマリー ウィンドウの [Network Profiles] でユーザーに対して表示されます。 （注） ネットワークプロファイルコンプライアンスは、ルータおよびワイヤレスコントローラに適用されます。	• [Noncompliant]：デバイスでプロファイルのインテント設定が実行されていません。 • [Compliant]：ネットワークプロファイルがデバイスに適用されており、同時に、Cisco DNA Center からプッシュされたデバイス設定がデバイスでアクティブに実行されています。 • [Error]：根本的なエラーのため、コンプライアンスがステータスを計算できませんでした。詳細については、エラーログを参照してください。
ファブリック（SDA） この機能はベータ版です。	ファブリックコンプライアンスは、ファブリックインテント違反（ファブリック関連の設定のアウトオブバンド変更など）の識別に役立ちます。	• [Noncompliant]：デバイスでインテント設定が実行されていません。 • [Compliant]：デバイスでインテント設定が実行されています。
アプリケーションの可視性	Cisco DNA Centerでは、アプリケーション可視性インテントを作成して、CBARおよびNBARを介してデバイスにプロビジョニングできます。デバイスにインテント違反がある場合、このチェックにより、違反が識別されて、評価され、[Application Visibility] ウィンドウに準拠または非準拠として表示されます。 自動コンプライアンスチェックは、トラップの受信の 5 時間後に実行されるようにスケジュールされます。	• [Noncompliant]：デバイスで CBAR/NBAR 設定が実行されていません。 • [Compliant]：デバイスで CBAR/NBAR のインテント設定が実行されています。
モデル設定	このコンプライアンスチェックにより、ネットワーク管理者は、モデル設定の設計意図との不一致をチェックできます。違反は、[Compliance Summary] ウィンドウの [Network Profiles] に表示されます。	• [Noncompliant]：モデル設定の属性の実際の値と意図された値が一致しません。 • [Compliant]：モデル設計の属性が意図した値に一致します。

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
CLIテンプレート	Cisco DNA Center ではネットワーク管理者は、CLI テンプレートをデバイスの実行コンフィギュレーションと比較できます。コンフィギュレーションの不一致にはフラグが立てられます。違反は、[Compliance Summary] ウィンドウの [Network Profiles] に表示されます。 CLI テンプレート コンプライアンス用の実行コンフィギュレーションは、デバイスで使用可能な最新のアーカイブから取得されます。イベントベースのアーカイブは、トラップを受信してから更新されるまでに少なくとも 5 分かかります。したがって、正確な結果を得るには、構成の変更後にコンプライアンスを手動で実行する前に、少なくとも 5 分間待つことをお勧めします。 （注） CLI テンプレート コンプライアンスにはいくつかの制限があります。「CLI テンプレート コンプライアンスの制限事項 （7 ページ）」を参照してください。	• [Noncompliant]：CLI テンプレートとデバイスの実行コンフィギュレーションが一致しません。 • [Compliant]：CLI テンプレートとデバイスの実行コンフィギュレーションの間に不一致はありません。

ネットワークデバイスのコンプライアンス監査レポートの生成

Cisco DNA Center では、個々のネットワークデバイスのコンプライアンスステータスを示す統合されたコンプライアンス監査レポートを取得できます。このレポートを使用すると、ネットワークを完全に可視化できます。

詳細については、『Cisco DNA Center Platform User Guide』の「Run a Compliance Report」を参照してください。

デバイスのアップグレード後のコンプライアンス動作

- デバイスのアップグレードが正常に完了すると、該当するすべてのデバイス（システムでコンプライアンスが実行されたことがないデバイス）のコンプライアンスチェックがトリガーされます。

- コンプライアンスは、[Startup vs Running] タイプを除き、インベントリに含まれるデバイスのステータスを計算して表示します。
- アップグレード後、[Startup vs Running] タイルに [NA] が「Configuration data is not available」というテキストとともに表示されます。
- アップグレードが正常に完了してから 1 日後に、1 回限りのスケジューラが実行され、デバイスで構成データを使用できるようになります。[Startup vs Running] タイルに、正しいステータス（[Compliant]/[Non-Compliant]）と詳細データが表示され始めます。
- トラップを受信すると、設定アーカイブサービスが構成データを収集し、コンプライアンスチェックが再度実行されます。

（注） アップグレードセットアップでは、[Flex Profile] インターフェイスのコンプライアンスの不一致は無視してください。インターフェイス名の場合、[1] が [management] にマッピングされます。

CLI テンプレート コンプライアンスの制限事項

Cisco DNA Center では、CLI テンプレートをデバイスの実行コンフィギュレーションと比較して、意図との不一致を識別することができます。次のコンパレータエンジンの制限事項に注意してください。

- CLI テンプレートコンパレータは、変数と値の大文字の使用をサポートしています。
- コマンドキーワードに大文字を使用しないでください。
- CLI テンプレートコンパレータは、エイリアスの使用をサポートしています。
- 非準拠としてフラグが設定されている省略または短縮コマンドの使用は避けてください。
- コマンドが欠落していて、それがセクションレベルにある場合、欠落しているコマンドに続くセクションレベルのコマンドにもフラグが付けられます。インデントを付けることで、この問題を回避できます。

  次に例を示します。

  インデントのないコマンドの CLI テンプレートコンパレータ出力：

実現されたテンプレート	実行コンフィギュレーション	出力
#interface Vlan111 #description SVI interface kan-111 #ip address 111.2.3.4 255.255.255.0 #ip helper-address 7.7.7.8 #no mop enabled #no mop sysid #!	#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!	以下のコマンドが欠落としてマークされています。 # ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid

インデントを含むコマンドの CLI テンプレートコンパレータ出力：

実現されたテンプレート	実行コンフィギュレーション	出力
#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!	#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!	欠落しているコマンドのみに、コンパレータによってフラグが付けられます。 #ip helper-address 7.7.7.7

- 対話型およびイネーブルモードのコマンドは、コンプライアンスのために比較されません。コマンドですべてのオプションと値を指定することにより、対話型コマンドの代替形式を使用できます。

  たとえば、テンプレートコードが以下のように **#ENABLE** と **#INTERACTIVE** モードのコマンドを一緒に指定した場合、コマンドの比較は行われません。

```
#MODE_ENABLE
 #INTERACTIVE
    mkdir <IQ>Create directory<R>xyz
 #ENDS_INTERACTIVE
 #MODE_END_ENABLE
#end
```

- コンパレータによってフラグが設定されているコマンドでは範囲を使用しないでください。範囲は拡張形式で使用する必要があります。
- 同じテンプレート内のオーバーライドしているコマンドにフラグが付けられます。以下に示すように、コマンドを ignore - Compliance 構文で囲むことで、不一致を回避できます。

  次に例を示します。

実現されたテンプレート	実行コンフィギュレーション	出力

`#no banner motd #Welcome to Cisco .:|:.#`
`#banner motd #Welcome to Cisco .:|:.#`
	`#banner motd ^CWelcome to Cisco .:|:.^C`	• 以下のコマンドは、欠落としてフラグが付けられています。
		`no banner motd #Welcome to Cisco .:|:.#`
		• 実行中のコマンドはすでに上記のコマンドと比較されているため、以下のコマンドも欠落としてマークされています。
		`banner motd #Welcome to Cisco .:|:.#`

不一致を回避するには、次の操作を行います。

実現されたテンプレート	実行コンフィギュレーション	出力

`#! @start-ignore-compliance`
`#no banner motd #Welcome to Cisco .:|:#`
`#! @end-ignore-compliance`
`#banner motd #Welcome to Cisco .:|:.#`
	`#banner motd ^CWelcome to Cisco .:|:.^C`	構文で囲まれたコマンドは比較されないため、不一致はありません。

- Cisco IOS XE の以降のリリースでは、一部のデフォルトコマンドは、**show run** コマンドではなく、**show run all** コマンドが発行された場合にのみ表示されます。したがって、これらのコマンドは実行コンフィギュレーションに表示されず、非準拠としてフラグが設定されます。
- パスワードを含むコマンドは、デバイスに暗号化された形式で保存されるため、コンパレータによってフラグが設定されます。

（注） 次の構文でコマンドを囲むことで、パスワードを含むコマンドと一部のデフォルトコマンドの不一致を回避できます。

```
! @start-ignore-compliance
! @end-ignore-compliance
```

次に、変更が表示されるようにテンプレートを再プロビジョニングします。

CLIテンプレートとデバイスの実行コンフィギュレーションとの不一致を避けるために、実行コンフィギュレーションと同様のコマンドを使用することをお勧めします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。