



ネットワーク セキュリティ アドバイザリ の識別

- [セキュリティアドバイザリの概要](#) (1 ページ)
- [前提条件](#) (1 ページ)
- [セキュリティアドバイザリの表示](#) (2 ページ)
- [セキュリティ アドバイザリ スキャンのスケジュール設定](#) (3 ページ)
- [アドバイザリに対するデバイスの表示/非表示](#) (5 ページ)
- [デバイスに対するアドバイザリの表示/非表示](#) (5 ページ)
- [一致パターンの追加](#) (6 ページ)
- [一致パターンの AND/OR の定義](#) (6 ページ)
- [一致パターンの編集](#) (7 ページ)
- [一致パターンの削除](#) (7 ページ)

セキュリティアドバイザリの概要

Cisco Product Security Incident Response Team (PSIRTT; プロダクトセキュリティ インシデントレスポンスチーム) は、シスコ製品セキュリティインシデントに対応し、セキュリティ脆弱性ポリシーを規制し、[シスコのセキュリティアドバイザリとアラート](#)を推奨します。

セキュリティアドバイザリ ツールは、これらの推奨されるアドバイザリを使用して、Cisco DNA Center 内のインベントリをスキャンし、既知の脆弱性を持つデバイスを検出します。

前提条件

セキュリティアドバイザリ ツールを使用するには、機械推論パッケージをインストールする必要があります。『[Cisco DNA Center Administrator Guide](#)』の「[Download and Install Packages and Updates](#)」を参照してください。

オブザーバとして Cisco DNA Center にログインすると、ホームページで [Security Advisories] ツールを表示できません。

セキュリティアドバイザリの表示

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Tools] > [Security Advisories] の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

Cisco DNA Center では、セキュリティの問題を特定して自動分析を改善するためにナレッジベースを使用します。最新のセキュリティアドバイザリを表示するには、定期的にナレッジベースを更新することをお勧めします。

- Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[System] > [Settings] > [Machine Reasoning Knowledge Base] の順に選択します。
- [Import] をクリックするか、[Download] をクリックして最新の使用可能なナレッジベースをダウンロードしてから [Import] をクリックします。
- 自動更新に登録するには、[AUTO UPDATE] トグルボタンをクリックします。

- (注)
- セキュリティアドバイザリ ダッシュボードにはシスコが公開しているセキュリティアドバイザリが表示されます。アドバイザリは現行のソフトウェアイメージに基づいており、ネットワーク上のデバイスに影響する場合があります。脆弱性が実際に存在するかどうかを判断するには、設定、プラットフォームの詳細、またはその他の基準をさらに詳しく分析する必要があります。
 - [Overview] タブのセキュリティアドバイザリのグラフィックには、[Critical]、[High]、[Medium]、[Low]、[Informational] など、ネットワークに対するそれぞれの影響の割合が表示されます。
 - セキュリティアドバイザリ スキャンは、サポートされている最小ソフトウェアバージョン以上を実行しているルータおよびスイッチでのみ使用できます。詳細については、「[Cisco DNA Center Supported Devices](#)」を参照してください。
 - 表示されるセキュリティアドバイザリは、「[シスコのセキュリティ脆弱性ポリシー](#)」に基づいています。

次の表に、使用できる情報を記載します。

カラム	説明
アドバイザリ ID	ネットワークで検出されたセキュリティアドバイザリの ID。ID をクリックして、それぞれのアドバイザリ Web ページに移動します。
アドバイザリタイトル	ネットワークデバイスに適用可能なセキュリティ脆弱性アドバイザリの名前。
CVSS スコア	共通脆弱性評価システム (CVSS) モデルに基づいて評価されたスコア。
Impact	脆弱性がネットワークに及ぼす影響。

カラム	説明
CVE	脆弱性の Common Vulnerabilities and Exposures (CVE) 識別子。
デバイス	脆弱性の影響を受けるデバイスの数。この特定のアドバイザーに基づいて脆弱性が存在する可能性のあるデバイスを表示するには、番号をクリックし、必要に応じてデバイスをアップグレードします。
Match Type	検出された脆弱性が [Image Version] の一致と [Configuration] の一致のどちらに基づくかを示します。
検出以降の期間 (日数)	脆弱性が検出されてからの経過日数。
Last updated	アドバイザーが最後に更新された日付。

ステップ 3 各デバイスに適用可能なアドバイザーの数を表示するには、[Devices] タブをクリックします。

- a) デバイスに一致するものをすべて表示するには、アドバイザーの数をクリックします。
- b) デバイストポロジを表示するには、右上隅にあるトポロジアイコンをクリックします。トポロジ内のデバイスをクリックすると、デバイスに一致するすべてのアドバイザーが表示されます。

デバイスの横にあるロックアイコンは、デバイスに適用可能な 1 つ以上のアドバイザーがあることを示します。

ステップ 4 いつでも [Scan Network] をクリックすれば、表示された結果を更新できます。

セキュリティ アドバイザリ スキャンのスケジュール設定

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Tools] > [Security Advisories] の順に選択します。

ステップ 2 [Scan Network] をクリックします。

[Scan Network] ウィンドウが表示されます。

ステップ 3 セキュリティアドバイザーをすぐにスキャンするには、[Now] オプションボタンをクリックし、[Start] をクリックします。

ステップ 4 スキャンを後で実行するようにスケジュールするには、[Later] オプションボタンをクリックし、日付と時刻を指定します。

ステップ 5 [Time Zone] ドロップダウンリストを使用して、スキャンのスケジュール設定に使用するタイムゾーンを選択します。

ステップ 6 繰り返しオプションとして [None] (デフォルト)、[Daily]、[Weekly] のいずれかを選択します。

ステップ 7 [Run at Interval] フィールドに、スキャンの繰り返しの間隔 (日または週の数) を入力します。

- ステップ 8** (オプション) スケジュールの終了日や終了までの回数を指定する場合は、[Set Schedule End] チェックボックスをオンにします。
- スキャン終了日をスケジュールするには、[End Date] オプションボタンをクリックし、日付と時刻を定義します。
 - スキャンの繰り返し回数を定義するには、[End After] オプションボタンをクリックします。
- ステップ 9** [Schedule] をクリックします。
- ステップ 10** Cisco DNA Center GUI で [Menu] アイコン (≡) をクリックして選択します[Activities] > [Tasks] の順に選択して、スキャンのスケジュールと繰り返しを確認します。



- (注) Cisco DNA Center リリース 2.1.1.x 以降では、シスコによるテレメトリの収集を許可するかどうかを選択できます。収集を許可すると、cisco.com ID、システムテレメトリ、機能使用状況テレメトリ、ネットワーク デバイス インベントリ、およびソフトウェア利用資格の情報が収集されます。テレメトリは、アプリケーションごとや機能ごとではなく、Cisco DNA Center 全体について開示されます。Cisco DNA Center 2.1.1.x 以降では、テレメトリの収集は必須です。収集されたテレメトリは、ユーザーが使用している機能の開発に役立てられます。収集されるデータの詳しいリストについては、「[Cisco DNA Center のデータシート](#)」を参照してください。
- セキュリティ アドバイザリ スキャンの実行時に収集されるテレメトリデータは次のとおりです。
- ナレッジパッケージの自動更新が設定されているかどうか。
 - 繰り返しのスキャンおよび繰り返しのレポートが設定されているかどうか。
 - 実行されたレポートの数。
 - ソフトウェアのバージョンと設定に基づいて一致するセキュリティ アドバイザリがあるデバイスの数。
 - 各スキャンの受理と拒否の数。
 - 検索で入力された手動設定とそれに関連するアドバイザリ。
 - ソフトウェアのバージョンと設定 (製品ファミリーを含む) が一致するアドバイザリの数。
 - 他のカテゴリ (アドバイザリなし、不明、サポート対象外) に基づくデバイスの数。
 - スキャンの成功、失敗、終了の数。
 - 平均スキャン時間。

アドバイザリに対するデバイスの表示/非表示

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Tools] > [Security Advisories] の順に選択します。
- ステップ 2** [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。
- ステップ 3** [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。
- ステップ 4** デバイスのアドバイザリを非表示にするには、次の手順を実行します。
- [Focus] ドロップダウンリストから、[Advisories] を選択します。
 - [Devices] 列で、デバイスを非表示にするアドバイザリに対応するデバイス数をクリックします。
[Active] タブには、これらのアドバイザリが発行されたデバイスの数が表示されます。
 - 非表示にするデバイスを選択し、[Suppress Device] をクリックします。
非表示にしたデバイスは、[Suppressed] タブで確認できます。
 - アドバイザリウィンドウを閉じ、このアドバイザリのデバイス数の変化を確認します。
- ステップ 5** デバイスをアドバイザリに復元するには、次の手順を実行します。
- [Focus] ドロップダウンリストから、[Advisories] を選択します。
 - [Devices] 列で、デバイスを再表示するアドバイザリに対応するデバイス数をクリックします。
 - [Suppressed] タブをクリックして、非表示のデバイスを表示します。
 - 再表示するデバイスを選択し、[Mark as Active] をクリックします。
復元されたデバイスは、[Active] タブで確認できます。
 - アドバイザリウィンドウを閉じ、このアドバイザリのデバイス数の変化を確認します。

デバイスに対するアドバイザリの表示/非表示

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Tools] > [Security Advisories] の順に選択します。
- ステップ 2** [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。
- ステップ 3** [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。
- ステップ 4** デバイスのアドバイザリを非表示にするには、次の手順を実行します。
- [Focus] ドロップダウンリストから、[Devices] を選択します。
 - [Advisories] 列で、アドバイザリを非表示にするデバイスに対応するアドバイザリカウントをクリックします。
[Active] タブには、このデバイスに対して発行されたアドバイザリの数が表示されます。

- c) 非表示にするアドバイザリを選択し、[Suppress Advisory] をクリックします。
非表示のアドバイザリは、[Suppressed] タブで確認できます。
- d) デバイスウィンドウを閉じ、このデバイスのアドバイザリカウントの変化を確認します。

ステップ 5 デバイスのアドバイザリを復元するには、次の手順を実行します。

- a) [Focus] ドロップダウンリストから、[Devices] を選択します。
- b) [Advisories] 列で、アドバイザリを再表示するデバイスに対応するアドバイザリカウントをクリックします。
- c) [Suppressed] タブをクリックして、非表示のアドバイザリを表示します。
- d) 再表示するアドバイザリを選択し、[Mark as Active] をクリックします。
復元されたアドバイザリは、[Active] タブで確認できます。
- e) デバイスウィンドウを閉じ、このデバイスのアドバイザリカウントの変化を確認します。

一致パターンの追加

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Tools] > [Security Advisories] の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 アドバイザリを選択し、[Match Type] 列で [Add match pattern] をクリックします。

ステップ 5 [Add Configuration Match Pattern] ウィンドウで、[CONDITIONS] テキストボックスにデバイスと一致する条件を入力します。

ステップ 6 [保存 (Save)] をクリックします。

一致パターンがアドバイザリに追加されます。

ステップ 7 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの AND/OR の定義

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Tools] > [Security Advisories] の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

- ステップ4 アドバイザリを選択し、[Match Type] 列で [Add match pattern] をクリックします。
- ステップ5 [Add Configuration Match Pattern] ウィンドウで、次の手順を実行します。
- [CONDITIONS] テキストボックスに条件を入力し、[Add] アイコンをクリックします。
 - ドロップダウンリストから、[AND] または [OR] を選択し、次の条件を入力します。
 - 条件を削除する場合は、[Remove] アイコンをクリックします。
 - [保存 (Save)] をクリックします。
一致パターンがアドバイザリに追加されます。
- ステップ6 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。
-

一致パターンの編集

- ステップ1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Tools] > [Security Advisories] の順に選択します。
- ステップ2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。
- ステップ3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。
- ステップ4 すでに一致パターンがあるアドバイザリを選択し、[Match Type] 列で [Edit match pattern] をクリックします。
- ステップ5 [Edit Configuration Match Pattern] ウィンドウで、[CONDITIONS] テキストボックスにデバイスと一致する条件を入力します。
- ステップ6 [保存 (Save)] をクリックします。
一致パターンが変更されます。
- ステップ7 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。
-

一致パターンの削除

- ステップ1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Tools] > [Security Advisories] の順に選択します。
- ステップ2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。
- ステップ3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。
- ステップ4 すでに一致パターンがあるアドバイザリを選択し、[Match Type] 列で [Edit match pattern] をクリックします。
- ステップ5 [Edit Configuration Match Pattern] ウィンドウで、[Delete] をクリックします。

一致パターンが削除されます。

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。