Cisco Live Protect による NX- OS のセキュア化

この章では、NXSecure 構成が有効な場合に NX- OSをセキュアにする Cisco Live Protect 機能について説明します。この章は、次の項で構成されています。

Cisco Live Protect

Cisco Live Protect は：

- シスコ ネットワーク デバイスのコントロールプレーンを保護するセキュリティ機能です。
- NX- OS デバイスで NXSecure 設定を有効にする必要があります。
- リアルタイムのセキュリティ イベントの検出と分析により、包括的なセキュリティのオブザーバビリティを提供します。

Cisco NX-OSリリース 10.6(1)F では、NX- OS を保護する Cisco Live Protect 機能が導入されており、NX- OS デバイス コントロール プレーンのセキュリティとソフトウェア完全性のアシュアランスが強化されています。このリリースではモニタリング モードのみがサポートされています。

NXSecure： NXSecure は、 Nexusスイッチ向けのセキュリティ設定ツールです。コントロールプレーンをセキュリティの脆弱性から保護します。NXSecure は、拡張バークレイ パケット フィルタ（eBPF）と呼ばれるテクノロジーを内部的に使用して、セキュリティ イベントをリアルタイムに追跡、検出、レポートします。NXSecure は、ファイルの監視、プロセスの追跡、システム コールの追跡も行います。

トレース ポリシー： Cisco Live Protect 機能では、トレース ポリシーを使用してセキュリティのオブザーバビリティを提供します。これらのポリシーは、NX- OS イメージにパッケージ化されています。

モニタリング モード： 設定されたポリシーに基づいて、モニタリング モードはシステムが各異常イベントのログ ファイルを検出して生成できるようにします。

イベントログ：イベント ログはモニタリング モードで生成されます。NXSecure の正しいセンサー パスが構成されている場合は、テレメトリを使用してイベント ログをエクスポートできます。

Cisco Live Protect の注意事項と制約事項

Cisco Live Protect を使用する場合は、ご使用のソフトウェアリリースでプラットフォームと機能がサポートされていることを必ず確認してください。次の注意事項と制約事項に従って、互換性を確保し、サポートされていない展開を回避してください。

- **プラットフォーム サポート**： Cisco NX-OS リリース 10.6(1)F 以降で、この機能には以下の特徴があります：
  - 24G 以上の RAM を搭載した Cisco Nexus 9300-FX、-FX2、-FX3、-GX、-GX2、-H1、および -H2R スイッチでサポートされます。
  - Nexus 9800 および N9324C-SE1U を含む SiliconOne スイッチではサポートされていません。
- **他の機能との互換性**：アプリケーション ホスティングまたは AuditD 機能ではサポートされていません。

Cisco Live Protect の NXSecure 機能の有効化

NXSecure 機能を有効にするには、次の手順を実行します。

手順

NXSecure 機能を有効にするには、**feature nxsecure** コマンドを使用します。

例：

```
switch(config)# feature nxsecure
```

NXSecure 機能を無効にするには、このコマンドの **no** 形式を使用します。

NXSecure 機能が有効になっていること。Docker および NXSecure コンテナが開始されます。

Cisco Live Protect の NXSecure 設定の確認

Cisco Live Protect 機能の NXSecure 設定のステータスを確認するには、次の show コマンドを使用します。

コマンド	目的
show nxsecure status	NXSecure のステータスを表示します。
show nxsecure logfiles	生成されたログ ファイルの現在のセットを表示します。
show tech-support nxsecure	NXSecure のデバッグ ログを表示します。
show telemetry transport sessions	テレメトリ トランスポート セッションをループし、そのようなセッションに関する情報を表示します

検証コマンドの出力例

参考のために、リストされている show コマンドの出力例をここに示します。

- **show nxsecure status**

```
switch# show nxsecure status
Tetragon Agent Status: Running
```

- **show nxsecure logfiles**

```
switch# show nxsecure logfiles
tetragon-2025-03-17T22-17-32.948.log
tetragon-2025-03-17T22-21-59.194.log
tetragon-2025-03-17T22-25-58.694.log
tetragon.log
```

- **show telemetry transport sessions**

```
switch# show telemetry transport sessions
Session Id: 0
Dst Grp Id: 1000
IP Address:Port <ip address>
Transport: EVTLOG
Status: Connected
Last Connected: Tue Jun 24 14:33:32.577 IST
Last Disconnected: Tue Jun 24 14:33:32.570 IST
Tx Error Count: 0
Last Tx Error: None
```

イベント ログ

イベント ログは、以下のようなログ ファイルです：

- セキュリティ異常ごとに NXSecure モニタリング モードで生成されます。

- JSON 形式で出力されます。
- テレメトリを使用してエクスポートされます。

JSON ログ ファイル： NXSecure は、カーネル プログラムから受信した JSON イベントとアラートを含むログ ファイルを、プレーン JSON データとして生成します。システムは、最大 5 つの JSON イベントファイルを生成するように設定されています。各ファイルには、サイズ制限（3 MB）または時間制限（120 秒）があり、どちらか早い方が適用されます。

テレメトリを使用したログ ファイルのエクスポート：テレメトリ トランスポートは、NXSecure ログ ファイルをリモート HTTPS サーバにエクスポートするために使用されます。これは、**path event-nxsecure** センサータイプが設定されている場合にのみ可能です。

テレメトリ パス センサー タイプを構成します

テレメトリを構成するときに、パス センサー タイプが構成されます。event-history や event-monitor などの既存のパス センサー タイプに加えて、NX- OSリリース 10.6(1)F では、新しいテレメトリ パス センサー タイプである event-nxsecure が導入されています。このセンサー タイプは、ログ ファイルを外部の受信者にエクスポートするために使用されます。新しい**path event-nxsecure** センサー タイプを設定するには、設定例を参考にしてください。

パス センサー タイプの設定の詳細については、該当するバージョンの『Cisco Nexus 9000 シリーズ NX- OSプログラマビリティ ガイド』の「テレメトリ」の章を参照してください。

設定例

```
switch(config)# telemetry
switch(config-telemetry)# certificate /bootflash/server.pem <ip address>
switch(config-telemetry)# destination-group 1
switch(conf-tm-dest)# ip address <ip address> port 8083 protocol HTTP encoding Form-data
switch(conf-tm-dest)# sensor-group 1
switch(conf-tm-sensor)# path event-nxsecure
switch(conf-tm-sensor)# data-source native
switch(conf-tm-sensor)# subscription 1
switch(conf-tm-sub)# dst-grp 1
switch(conf-tm-sub)# snsr-grp 1 sample-interval 0
```

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。