



展開前

セキュリティ分析とロギング（オンプレミス）を展開する前に、『[Getting Started with Security Analytics and Logging Guide](#)』および『[Security Analytics and Logging On Premises: Firewall Event Integration Guide](#)』を確認してください。



重要 スタンドアロンのアプライアンス（マネージャのみ）としてのマネージャでのアプリケーションのインストール、または Cisco Secure Network Analytics フローコレクタ NetFlow と Cisco Secure Network Analytics データノード（データストア）を管理する マネージャ のインストールがサポートされています。データノードを管理せずに 1 つ以上のフローコレクタを管理する場合は、マネージャ にアプリケーションをインストールすることはできません。

- [バージョンの互換性](#) (1 ページ)
- [ソフトウェアのダウンロード](#) (6 ページ)
- [サードパーティ製アプリケーション](#) (7 ページ)
- [ブラウザ](#) (7 ページ)

バージョンの互換性

次の表に、セキュリティ分析とロギング（オンプレミス）の展開でファイアウォールのイベントデータの保存に Secure Network Analytics の使用が必要なソリューションのコンポーネントの概要を示します。

ファイアウォール アプライアンス

次のファイアウォール アプライアンスを展開する必要があります。

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス）のライセンス	注記
Secure Firewall Management Center (ハードウェアまたは仮想)	v7.2+ 以前のバージョンを実行している Management Center の場合は、 「 https://cisco.com/go/sal-on-prem-docs 」を参照してください。	なし	<ul style="list-style-type: none"> • Management Center ごとに 1 つの マネージャ。また、必要に応じて複数のフローコレクタとデータストアを展開できます。
Secure Firewall 管理対象のデバイス	v7.0+（ウィザードを使用） Threat Defense v6.4 以降（syslog を使用） NGIPS v6.4（syslog を使用）	なし	<ul style="list-style-type: none"> • Threat Defense v6.4 以降で syslog を使用する方法については、「以前のバージョンの Threat Defense デバイスからのイベントの送信」を参照してください。
ASA デバイス	v9.12+	なし	

Secure Network Analytics アプライアンス

Secure Network Analytics の展開には次のオプションがあります。

- **マネージャのみ**：マネージャのみを展開してイベントを取り込んで保存したり、イベントを確認および照会します。
- **データストア**：フローコレクタを展開してイベントを取り込み、データストアを展開してイベントを保存し、マネージャを展開してイベントを確認および照会します。

表 1: マネージャのみ

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス）のライセンス	注記
マネージャ	Secure Network Analytics v7.4.0+	なし	<ul style="list-style-type: none"> • 複数台の Threat Defense デバイスからイベントを受信できます。これらはすべて1つの Management Center によって管理されます。 • イベントを取り込んで マネージャの Web アプリケーションでファイアウォールイベントを表示するにはセキュリティ分析とロギング（オンプレミス）アプリケーションをインストールする必要があります。
セキュリティ分析とロギング（オンプレミス）アプリケーション	セキュリティ分析とロギング（オンプレミス）アプリ v3.1+	GB/日に基づくスマートライセンスのロギングおよびトラブルシューティング	<ul style="list-style-type: none"> • マネージャにこのアプリケーションをインストールし、syslog の取り込みを有効にするように設定します。

表 2: データストア

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス）のライセンス	注記
マネージャ	Secure Network Analytics v7.4.0+	なし	<ul style="list-style-type: none">• イベントを取り込んでマネージャの Web アプリケーションでファイアウォールイベントを表示するにはセキュリティ分析とロギング（オンプレミス）アプリケーションをインストールする必要があります。• Secure Network Analytics v7.4.1 はシングルノードデータストアとマルチテレメトリが必要です。

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス）のライセンス	注記
Flow Collector	Secure Network Analytics v7.4.0+	なし	<ul style="list-style-type: none"> • データストア用に設定された最大5つのフローコレクタを展開できます。 • 複数台の Threat Defense デバイスからイベントを受信できます。これらはすべて1つの Management Center によって管理されます。 • 複数の ASA デバイスから ASA イベントを受信できます。 • Secure Network Analytics v7.4.1 はシングルノードデータストアとマルチテレメトリが必要です。
データストア	Secure Network Analytics v7.4.0+	なし	<ul style="list-style-type: none"> • 3つのデータノードのセットに1つ、3つ、またはそれ以上を展開できます。 • フローコレクタで受信したファイアウォールイベントを保存できます。 • Secure Network Analytics v7.4.1 はシングルノードデータストアとマルチテレメトリが必要です。

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス）のライセンス	注記
セキュリティ分析とロギング（オンプレミス）アプリケーション	セキュリティ分析とロギング（オンプレミス）アプリ v3.1+	GB/日に基づくスマートライセンスのロギングおよびトラブルシューティング	<ul style="list-style-type: none"> マネージャにこのアプリケーションをインストールし、syslog の取り込みを有効にするように設定します。

これらのコンポーネントに加えて、すべてのアプライアンスが NTP を使用して時刻を同期できることを確認する必要があります。

Secure Firewall または Secure Network Analytics アプライアンスのコンソールにリモートでアクセスする場合は、SSH 経由のアクセスを有効にできます。

ソフトウェアのダウンロード

次の点に注意してください。

- **パッチ**：アップグレードする前に、アプライアンスに最新のロールアップパッチをインストールしていることを確認してください。Cisco Software Central (<https://software.cisco.com>) の Cisco スマートアカウントからファイルをダウンロードできます。
- **ファイルのダウンロード**：
 1. <https://software.cisco.com> で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。
 2. [ダウンロードとアップグレード (Download and Upgrade)] セクションで、[ソフトウェアのダウンロード (Software Download)] を選択します。
 3. [セキュリティ (Security)] > [Network Visibility and Segmentation (ネットワークの可視性とセグメンテーション)] > [Secure Analytics (Stealthwatch)] > [Secure Network Analytics 仮想マネージャ (Secure Network Analytics Virtual Manager)] > [アプリケーション - Security Analytics and Logging オンプレミス (App - Security Analytics and Logging On Prem)] を選択します。
 4. Security Analytics and Logging オンプレミス アプリケーション ファイル app-smc-sal-3.1.0-v2.swu をダウンロードします。

サードパーティ製アプリケーション

アプライアンスへのサードパーティ製アプリケーションのインストールはサポートしていません。

ブラウザ

Secure Firewall および Secure Network Analytics は、Google Chrome および Mozilla Firefox の最新バージョンをサポートしています。

