



Cisco Security Analytics and Logging (オンプレミス) v3.0.0 リリースノート

初版：2021年10月8日

最終更新：2021年10月28日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



第 1 章

はじめに

- [概要](#) (1 ページ)
- [用語](#) (1 ページ)

概要

このドキュメントでは、シスコのセキュリティ分析とロギング（オンプレミス）v3.0.0の新機能と改善点、バグ修正、および既知の問題について説明します。詳細については、[cisco.com](https://www.cisco.com) をご覧ください。

用語

このガイドでは、Cisco Secure Network Analytics Manager（旧 Stealthwatch 管理コンソール）Virtual Edition などの仮想製品を含むすべてのファイアウォールまたは Cisco Secure Network Analytics（旧 Stealthwatch）製品に対し「アプライアンス」という用語を使用しています。



第 2 章

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（単一ノード）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 3 つのデータノード（マルチノード）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。3 つの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](#)（3 ページ）
- [ソフトウェアのダウンロード](#)（8 ページ）
- [サードパーティ製アプリケーション](#)（8 ページ）
- [ブラウザ](#)（8 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できます。

| 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 |
|--|---|-----------------------------|---|
| Firepower Management Center（ハードウェアまたは仮想） | v7.0+ 以前のバージョンを実行している FMC 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"> • Firepower Management Center ごとに 1 つのマネージャ。また、必要に応じて 1 つのフローコレクタと 1 つの Cisco Secure Network Analytics データストア（データノード X 3）を展開できます。 |
| Firepower 管理対象のデバイス | v7.0+（ウィザードを使用） FTD v6.4+（syslog を使用） NGIPS v6.4 | なし | |
| ASA デバイス | v9.12+ | なし | <ul style="list-style-type: none"> • 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 v3.0.0+ および Secure Network Analytics v7.4.0+ マルチノード展開でサポートされています。 |

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。

- 単一ノード：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。
- マルチノード：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。



注 Secure Network Analytics ハードウェアと Secure Network Analytics VE アプライアンスを混在させて展開することはできません。

表 1: 単一ノード

| 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"> • マネージャ 2210 ハードウェアアプライアンスまたはマネージャの仮想エディション（VE）のいずれかを展開できます。 • 複数台の Firepower 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 Firepower 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。 |

| 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 | 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 v3.0+、 app-smc-sal-3.0.0-v2.swu | 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 | 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: マルチノード

| 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"> • マネージャ 2210 ハードウェアアプリケーションまたはマネージャの仮想エディション（VE）のいずれかを展開できます。 • イベントを取り込んで Secure Network Analytics 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。 |

| 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"> Flow Collector 4210 ハードウェアアプライアンスまたはフローコレクタ VE アプライアンスのいずれかを展開できます。 複数台の Firepower 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 Firepower 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。 |
| データストア（データノード X 3） | Secure Network Analytics v7.4.0+ | なし | <ul style="list-style-type: none"> Data Store 6200（データノード X 3）ハードウェアまたはデータストア VE（データノード VE X 3）のいずれかを展開できます。 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。 |
| セキュリティ分析とロギング（オンプレミス） アプリ | 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 v3.0+、 app-smc-sal-3.0.0-v2.swu | 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 | 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。

Firepower 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-3.0.0-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

Firepower と 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。



第 3 章

セキュリティ分析とロギング（オンプレミス）アプリケーションのインストール

Central Management のアプリケーションマネージャを使用してセキュリティ分析とロギング（オンプレミス）をインストールします。ブラウザは Chrome または Firefox を使用することをお勧めします。

1. マネージャにログインします。
2. [グローバル設定 (Global Settings)] アイコンをクリックします。
3. [集中管理 (Central Management)] を選択します。
4. [アプリケーションマネージャ (App Manager)] タブをクリックします。
5. [参照 (Browse)] をクリックします。
6. 画面に表示される指示に従って、アプリケーションファイルをアップロードします。



重要

スタンドアロンのアプライアンス（単一ノード）としてのマネージャのインストール、またはフローコレクタと3つのデータノード（マルチノード）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。3つの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。

- [Secure Network Analytics とアプリケーションの互換性](#)（9 ページ）
- [リソース使用状況](#)（11 ページ）

Secure Network Analytics とアプリケーションの互換性

Secure Network Analytics の更新の際、現在インストールされているアプリケーションは保持されます。ただし、アプリケーションと新しい Secure Network Analytics バージョンとの間に互換性がない場合があります。Secure Network Analytics の特定のバージョンでサポートされるアプ

リケーションのバージョンを確認するには、『[Secure Network Analytics Apps Version Compatibility Matrix](#)』を参照してください。

マネージャにインストールできるアプリケーションのバージョンは1つのみです。インストール済みのアプリケーションを管理するには、[アプリケーションマネージャ (App Manager)] ページを使用します。このページから、アプリケーションのインストール、更新、アンインストール、またはステータスの確認を実行できます。確認可能なアプリケーションのステータスについては、以下の表を参照してください。

より新しいバージョンのアプリケーションがあっても [アプリケーションマネージャ (App Manager)] に表示されないことがあるため、必ず [Cisco Software Central](#) で新しいバージョンがないかどうかを確認してください。



重要 アプリケーションを新しいバージョンに更新するには、新しいバージョンを既存のバージョンにそのままインストールします。既存のアプリケーションをアンインストールする必要はありません。セキュリティ分析とログギング（オンプレミス）をアンインストールすると、一時ファイルやファイアウォールイベント データなど、関連付けられているすべてのファイルが削除されます。

表 3:

| ステータス | 定義 | 対処 |
|-----------------|--|---|
| UpToDate | インストール済みのアプリケーションは最新バージョンです。 | 特に対処の必要はありません。 |
| UpdateAvailable | 新しいバージョンの Secure Network Analytics にアップグレードしています。既存のアプリケーションは、このバージョンの Secure Network Analytics でサポートされていますが、このアプリケーションの新しいバージョンがあります。 | 必要な場合は、Cisco Software Central にアクセスして最新バージョンのダウンロードとインストールを行ってください（これにより既存のバージョンが置き換えられます）。 |
| UpgradeRequired | 新しいバージョンの Secure Network Analytics にアップグレードしましたが、既存のアプリケーションは、現在使用している Secure Network Analytics バージョンでサポートされていません。 | このアプリケーションを引き続き使用するには、Cisco Software Central にアクセスして最新バージョンのダウンロードとインストールを行ってください（既存のバージョンが置き換えられます）。 |

| ステータス | 定義 | 対処 |
|-----------------|--|--|
| AppNotSupported | 新しいバージョンの Secure Network Analytics にアップグレードしています。このアプリケーションは、現在使用しているバージョンの Secure Network Analytics でサポートされなくなる可能性があります。このアプリケーションが廃止されたか、このアプリケーションの新しいバージョンがまだリリースされていない可能性があります。 | 新しいバージョンがリリースされたかどうかを確認するには、Cisco Software Central に移動します。 |
| NewApp | これは新しいアプリケーションです。 | 必要な場合は、Central Manager を使用してこの新しいアプリケーションをインストールしてください。 |
| Error | 関連付けられているアプリケーションのインストール、アップグレード、または削除プロセスが正常に完了しませんでした。 | Secure Network Analytics サポートに連絡してください（サポートの連絡先情報については、本書の最後のセクションを参照）。このアプリケーションが、部分的にインストール、アップグレード、または削除された可能性があります。その場合は修正が必要です。 |

Secure Network Analytics アプリケーションのバージョンに関する詳細については、『[Secure Network Analytics Apps Version Compatibility Matrix](#)』を参照してください。

リソース使用状況

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

- マネージャが次の場合にのみ展開できます。
 - フローコレクタを管理しない、または
 - フローコレクタと3つのデータノードを管理している
- インストールには次のディスク容量が必要です。
 - /lancope : 50 MB

- /lancope/var : 10 MB（このディスク容量は開始点であり、システムにデータが蓄積されるにつれて消費量が増加することに注意）
- イベントを保持するために推奨されるディスク容量の詳細については、『[Security Analytics and Logging \(On Premises\): Firewall Event Integration Guide](#)』を参照してください。1 TB、2 TB、および4 TBのディスクストレージを持つマネージャに対し、イベント保持のテストを実行済みです。

ディスク使用状況の統計を確認する

アプライアンスのディスク使用状況の統計情報を取得するには、次の手順を実行します。

始める前に

- Secure Network Analytics Web アプリケーションに管理者としてログインします。

-
- ステップ 1** [グローバル設定 (Global Settings)] アイコンをクリックし、ドロップダウンメニューから [集中管理 (Central Management)] を選択します。
 - ステップ 2** [アプライアンスマネージャ (Appliance Manager)] タブをクリックします。
 - ステップ 3** アプライアンスの [アクション (Actions)] メニューをクリックし、コンテキストメニューから [アプライアンス統計情報の表示 (View Appliance Statistics)] を選択します。
 - ステップ 4** プロンプトが表示されたら、アプライアンス管理インターフェイスにログインします。
 - ステップ 5** [ディスク使用量 (Disk Usage)] セクションまでスクロールします。
-



第 4 章

新機能

セキュリティ分析とロギング（オンプレミス）リリース v3.0.0 の新機能と改善点は次のとおりです。

- [新機能](#)（13 ページ）
- [サポートへの問い合わせ](#)（14 ページ）

新機能

マルチノード展開でサポートされる ASA デバイス

ASA デバイスは、CLI、ASDM、または CSM を使用して、syslog 経由でファイアウォールイベントを Secure Network Analytics マルチノード展開に送信するように設定できます。詳細については、『[Security Analytics and Logging \(On Premises\): Firewall Event Integration Guide](#)』の「ASA の設定」セクションを参照してください。

Firepower Management Center 設定ウィザードに追加された FTD データプレーンイベント

FTD データプレーンイベントは、Firepower Management Center の設定ウィザードを使用して Secure Network Analytics に送信できます。これらのイベントを送信するには、追加の要件があります。詳細については、『[Security Analytics and Logging \(On Premises\): Firewall Event Integration Guide](#)』の「Firepower の設定」セクションを参照してください。

イベントビューアの機能拡張

イベントビューアを使用して、次のことができるようになりました。

- エクスポートするデバイスタイプ（FTD、ASA、または NGIPS）に基づいて ASA イベントをフィルタ処理する
- [イベントタイプ（Event Type）] 列で ASA イベントをフィルタ処理する
- ASA イベントに固有の列を使用して ASA イベントを検索する

サポートへの問い合わせ

テクニカルサポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
 - Web でケースを開く場合：<http://www.cisco.com/c/en/us/support/index.html>
 - 電子メールでケースを開く場合：tac@cisco.com
 - 電話でサポートを受ける場合：1-800-553-2447（米国）
 - ワールドワイドサポート番号：
https://www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html



第 5 章

解決済みの問題と既知の問題

- [解決済みの問題](#) (15 ページ)
- [既知の問題](#) (15 ページ)

解決済みの問題

表 4: v3.0.0

| 障害 | 説明 |
|-------------|---|
| SWONE-15345 | マルチノード展開で Firepower Threat Defense v6.4-6.7 を使用すると、タイムスタンプが正しくありませんでした。 |

既知の問題

v3.0.0

なし

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。

