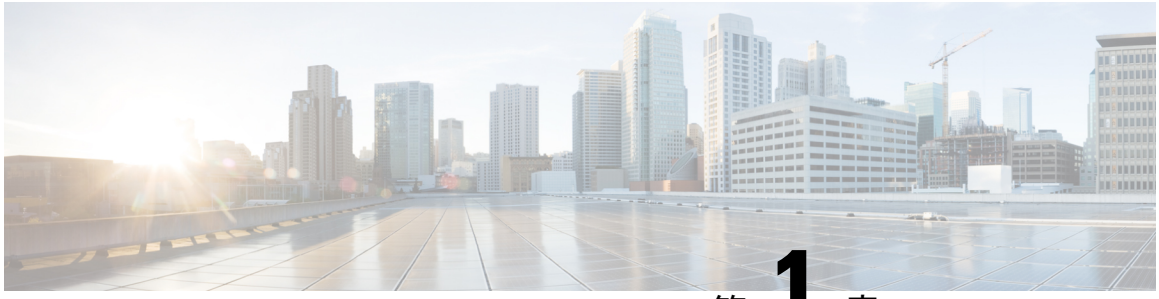
Cisco Security Analytics and Logging（オンプレミス）v3.1.0 リリースノート

初版：2022 年 4 月 18 日

最終更新：2022 年 4 月 18 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

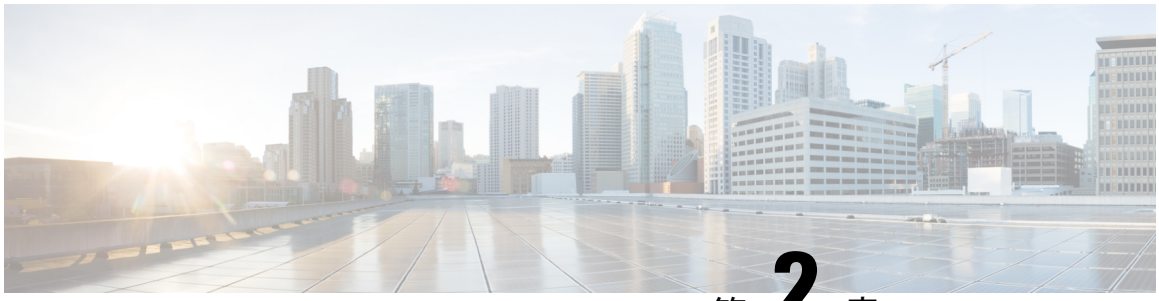
はじめに

概要

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）v3.1.0 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 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（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

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	• 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	• 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	• 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	• 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	• 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で必要です。

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	• 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で必要です。
データストア	Secure Network Analytics v7.4.0+	なし	• 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で必要です。

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	• 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**：

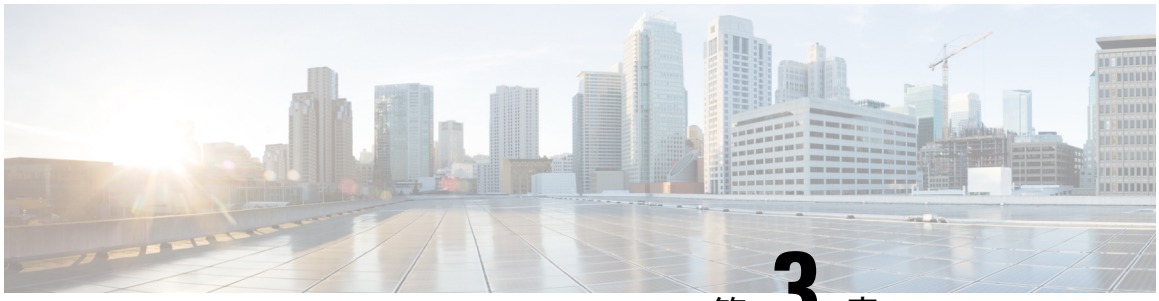
1. https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。
2. [ダウンロードとアップグレード（Download and Upgrade）] セクションで、[ソフトウェアのダウンロード（Software Download）] を選択します。
3. [セキュリティ（Security）] > [Network Visibility and Segmentation（ネットワークの可視性とセグメンテーション）] > [Secure Analytics（Stealthwatch）] > [Secure Network 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。



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（マネージャのみ）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（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。

- Secure Network Analytics とアプリケーションの互換性 （11 ページ）
- リソース使用状況 （13 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。

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
  - フローコレクタとデータノードを管理
- 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。

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。

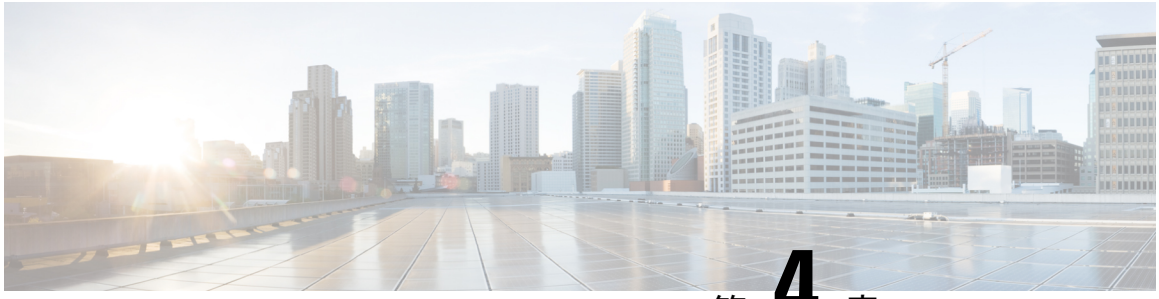
ステップ 1 [グローバル設定（Global Settings）]アイコンをクリックし、ドロップダウンメニューから [集中管理（Central Management）] を選択します。

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 v3.1.0 の新機能と改善点は次のとおりです。

新機能

ブランディングの更新

展開オプションのブランドを、シングルノードおよびマルチノードから Manager のみおよびデータストアに変更しました。この更新は、Secure Network Analytics の同様の用語による混乱を避けるためのものです。

データストア展開のための複数フローコレクタのサポート

Secure Firewall Management Center v7.2 では、セキュリティ分析とロギング（オンプレミス）ウィザードを使用して、データストア用に設定する最大 5 つのフローコレクタへのファイアウォールイベントを送信できます。複数のフローコレクタを設定する方法の詳細については、『Security Analytics and Logging (On Premises) v3.1: Firewall Event Integration Guide』の「イベントデータをデータストア展開に送信できるように *Secure Firewall Management Center* を設定する」セクションを参照してください。

Secure Network Analytics マルチテレメトリのサポート

以前は、テレメトリ取り込みの制限により、セキュリティ分析とロギング（オンプレミス）は Secure Network Analytics の個別の展開を必要としていました。Secure Network Analytics v7.4.1 では、データストアの展開は、次のテレメトリタイプの取り込みを同時にサポートします。

- ファイアウォールイベント
- NetFlow
- Network Visibility Module（NVM）

詳細については、「Secure Network Analyics リリースノート v7.4.1」を参照してください。

Secure Network Analytics 単一ノードのデータストア

データストアの展開では、以前のリリースでは3つ以上のデータノードが必要とされていましたが、1 つのデータノードでもサポートされるようになりました。詳細については、「Secure Network Analyics リリースノート v7.4.1」を参照してください。

EMBLEM ロギング形式のサポート

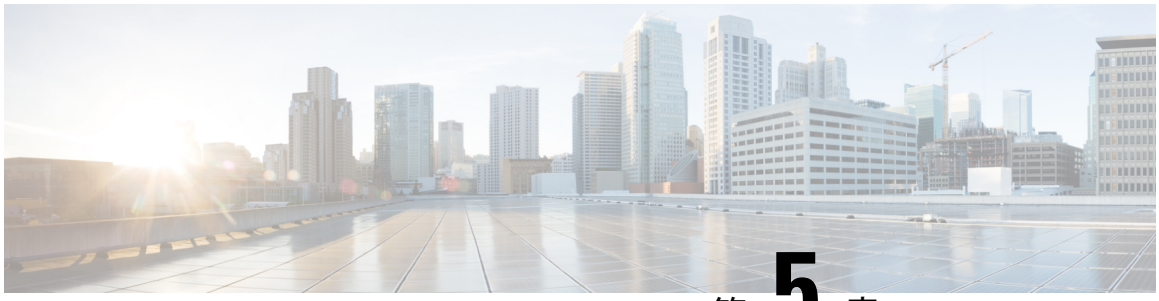
EMBLEM ロギング形式は、Secure Network Analytics v7.4.0 および v7.4.1 でサポートされるようになりました。設定するには、『ファイアウォールイベント統合ガイド』の「*ASA* デバイスから *Syslog* イベントを送信するための *ASDM* 設定」または「*ASA* デバイスから *Syslog* イベントを送信するための *CSM* 設定」セクションを参照してください。

（注） v7.4.0 の場合、Flow Collector NetFlow Patch Rollup007 以降をダウンロードしてインストールする必要があります。詳細については、「パッチの readme」を参照してください。

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

v3.1.0

なし

既知の問題

v3.1.0

なし