# Cisco Secure Network Analytics

## x2xx シリーズ ハードウェア アプライアンス設置ガイド 7.5.0

# 目次

# はじめに

## 概要

このガイドでは、Cisco Secure Network Analytics（旧 Stealthwatch）x2xx シリーズのハードウェアアプライアンスの設置方法について説明します。このガイドでは、Secure Network Analytics ハードウェアのマウントと設置についても説明します。

> ⚠ Secure Network Analytics x2xx シリーズのアプライアンスを設置する前に、『法規制の遵守および安全性情報』のドキュメントをお読みください。

x2xx シリーズのハードウェアには、次のものが含まれます。

| アプライアンス | 部品番号 |
|---|---|
| Manager 2210<br>（旧 Stealthwatch Management Console） | ST-SMC2210-K9 |
| Data Store 6200（3 つの Data Node） | ST-DS6200-K9（3 つの ST-DNODE-G1） |
| Flow Collector 4210 | ST-FC4210-K9 |
| Flow Collector 5210 エンジン | ST-FC5210-E |
| Flow Collector 5210 データベース | ST-FC5210-D |
| UDP Director 2210 | ST-UDP2210-K9 |
| Flow Sensor 1210 | ST-FS1210-K9 |
| Flow Sensor 3210 | ST-FS3210-K9 |
| フローセンサー 4240 | ST-FS4240-K9 |

## 対象読者

このガイドは、Secure Network Analytics ハードウェア設置の担当者を対象にしています。ネットワーク機器の設置について、ある程度の理解がすでにあることを前提としています。

専門家によるインストールを希望する場合は、最寄りのシスコパートナーまたはシスコサポートに連絡してください。

## アプライアンスの設置とシステムの設定

Secure Network Analytics のインストールと設定の全体的なワークフローに注意してください。

1. **アプライアンスの設置**：この設置ガイドを使用して、Secure Network Analytics x2xx シリーズハードウェア（物理）アプライアンスを設置します。Virtual Edition アプライアンスをインストールするには、Virtual Edition アプライアンス インストール ガイドの指示に従ってください。
2. **Secure Network Analytics の設定**：ハードウェアと仮想アプライアンスをインストールしたら、管理対象システムに Secure Network Analytics を構成できます。『Secure Network Analytics System Configuration Guide v7.5.0』[英語] の手順に従います。

## 関連情報

Secure Network Analytics の詳細については、次のオンラインリソースを参照してください。

- **法規制の遵守および安全性情報**：Secure Network Analytics x2xx シリーズのアプライアンスを設置する前に、『法規制の遵守および安全性情報』をお読みください。
- **概要**：https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html [英語]
- **Data Store 設計ガイド**：https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf [英語]
- **ハードウェアおよびソフトウェアバージョンのサポートマトリックス**：https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html
- **アプライアンスの仕様**：https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html

## 用語

このガイドでは、すべての Secure Network Analytics 製品に対して「**アプライアンス**」という用語を使用します。

「**クラスタ**」は、Manager が管理する Secure Network Analytics アプライアンスのグループです。

## 略語

このガイドでは、次の略語が使用されます。

| 省略形 | 説明 |
|---|---|
| DMZ | 非武装地帯（境界ネットワーク） |
| HTTPS | Hypertext Transfer Protocol（Secure） |
| ISE | Identity Services Engine |
| NIC | ネットワーク インターフェイス カード |

| 省略形 | 説明 |
| --- | --- |
| NTP | ネットワーク タイム プロトコル |
| PCIe | Peripheral Component Interconnect Express; ペリフェラル コンポーネント インターコネクト エクスプレス |
| SNMP | Simple Network Management Protocol（簡易ネットワーク管理プロトコル） |
| SPAN | スイッチ ポート アナライザ |
| TAP | テスト アクセス ポート |
| UPS | 無停電電源 |
| VLAN | 仮想ローカル エリア ネットワーク |

# Secure Network Analytics アプライアンスについて

Secure Network Analytics ネットワークのパフォーマンスとセキュリティを改善するために、ネットワークに関する情報の収集、分析、および提示を行う、いくつかのハードウェアアプライアンスで構成されています。このセクションでは、Secure Network Analytics x2xx シリーズの各アプライアンスについて説明します。

## Manager 2210

Manager は、システムのさまざまなコンポーネントすべてを管理、調整、設定、および編成します。Secure Network Analytics ソフトウェアを使用すると、Web ブラウザにアクセス可能な任意のコンピュータからコンソールの Web UI にアクセスできます。企業全体の重要なセグメントのセキュリティとネットワークに関するリアルタイムの情報に簡単にアクセスできます。Manager は Java ベースの独立したプラットフォームを採用しており、次のことが可能です。

- 最大 25 の Secure Network Analytics Flow Collector に対する集中型の管理、設定およびレポート
- トラフィックの視覚化のためのグラフィカル チャート
- トラブルシューティングのためのドリルダウンの分析
- 統合型のカスタマイズ可能なレポート
- トレンド分析
- パフォーマンス モニタリング
- セキュリティ違反の即時通知

Data Store を展開するユーザーは、スループットを向上させるため、10 Gbps SFP+ DAC インターフェイスを備えた Manager 2210 を eth0 として設定できます。Data Store を展開していない場合は、1 Gbps/10 Gbps インターフェイスのみを eth0 として設定できます。

## データストア 6200

Data Store は、Flow Collector によって収集されたネットワークのテレメトリを保存する中央リポジトリを提供します。Data Store は、Data Store のクラスタで構成されます。各クラスタには、データの一部と個別 Data Node のデータのバックアップが含まれます。すべてのデータが 1 つの集中型データベースに存在し、複数の Flow Collector に分散されていないため、Manager はすべての Flow Collector に個別にクエリする場合よりも Data Store から迅速にクエリ結果を取得できます。Data Store クラスタは、耐障害性の向上、クエリ応答の改善、グラフとチャート生成の迅速化を実現します。

詳細については、「Secure Network Analytics（Data Store あり）」を参照してください。

## フローコレクタ 4210 および 5210

Flow Collector は、NetFlow、cFlow、J-Flow、Packeteer 2、NetStream、IPFIX のデータを収集することで、動作に基づくネットワーク保護を提供します。

Flow Collector は高速ネットワークの動作データをさまざまなネットワークやネットワーク セグメントから集約することで、エンドツーエンドの保護を提供し、地理的に分散したネットワークのパフォーマンスを改善します。

Data Store を展開するユーザーは、スループットを向上させるため、10 Gbps SFP+ DAC インターフェイス を備えた Flow Collector 4210 を eth0 として設定できます。Data Store を展開していない場合は、100 Mbps/1 Gbps/10 Gbps 銅線インターフェイスのみを eth0 として設定できます。

> Flow Collector は、データを受信すると、パケット暗号化やフラグメンテーションとは無関係に、既知または未知の攻撃、内部での不正使用、ネットワークデバイスの誤設定を特定します。Secure Network Analytics が動作を特定すると、システムは、特定された種類の動作に対して設定済みのアクション（存在する場合）を実行できます。

## UDP Director 2210

UDP Director は、高速かつ高パフォーマンスの UDP パケット レプリケータです。UDP Director は、NetFlow、sFlow、syslog、または Simple Network Management Protocol（SNMP）のトラップをさまざまなコレクタに再配分するうえで非常に役立ちます。コネクションレス型 UDP アプリケーションからデータを受信し、それを複数の宛先に再伝送し、必要に応じてデータを複製できます。

UDP Director の高可用性（HA）構成を使用する場合は、クロスケーブルで 2 台の UDP Director アプライアンスを接続する必要があります。手順については、「2. ネットワークへのアプライアンスの接続」を参照してください。

## フローセンサー 1210 、3210、および 4240

Flow Sensor は、スイッチポートアナライザ（SPAN）、ミラーポート、イーサネット テスト アクセス ポート（TAP）にプラグインできる、従来のパケット キャプチャ アプライアンスや IDS と似た機能を持つネットワークアプライアンスです。フロー センサーは、次のネットワーク領域の可視性を強化します。

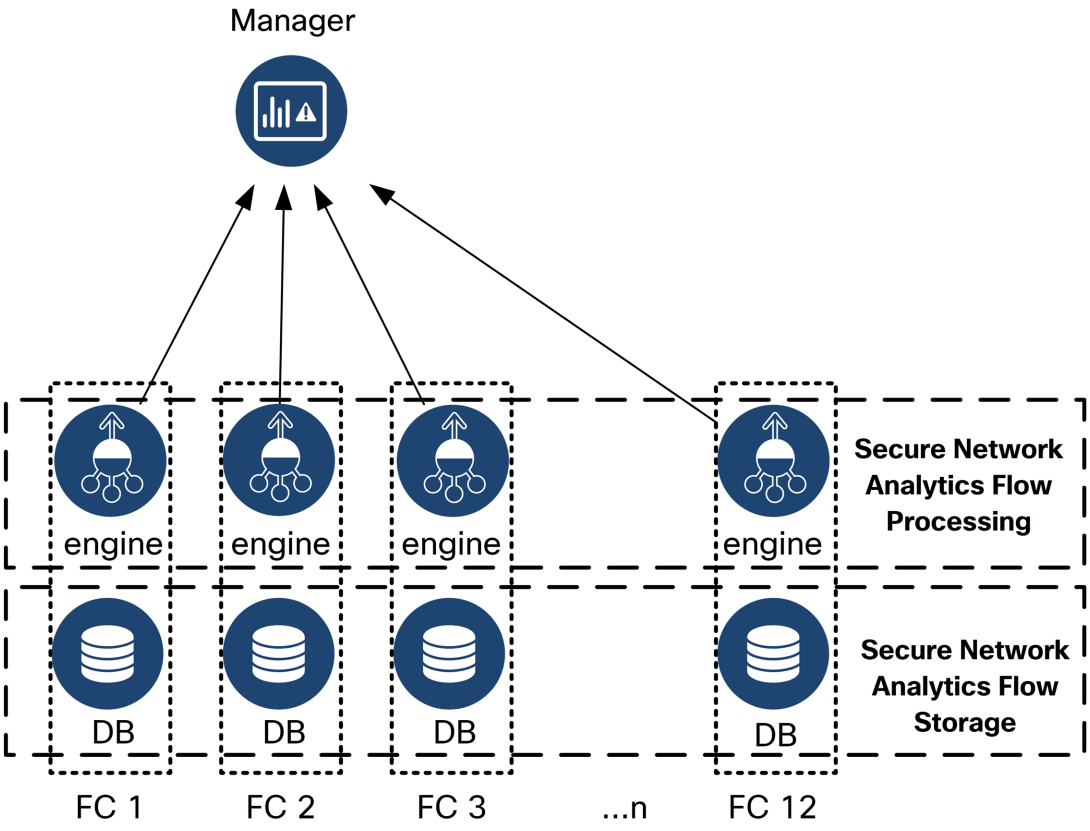
- NetFlow を使用できない領域。
- NetFlow は使用可能であるものの、パフォーマンス メトリックとパケット データに対する優れた可視性が必要な領域。

Flow Sensor を NetFlow v9 対応の Flow Collector に誘導することで、価値のある詳細なトラフィック統計情報を NetFlow から得ることができます。また、Flow Sensor を Secure Network Analytics Flow Collector と組み合わせると、評価指標や動作指標に関する深い洞察を得ることができます。これらのフロー パフォーマンス指標から、ネットワークまたはサーバー側アプリケーションに由来するラウンドトリップ遅延についての洞察が得られます。

フロー センサーはパケット レベルの可視性を備えているので、TCP セッションのラウンドトリップ時間（RTT）、サーバー応答時間（SRT）、パケット損失を計算できます。これらの付加的フィールドすべては、Flow Collector に送られる NetFlow レコードに含まれています。

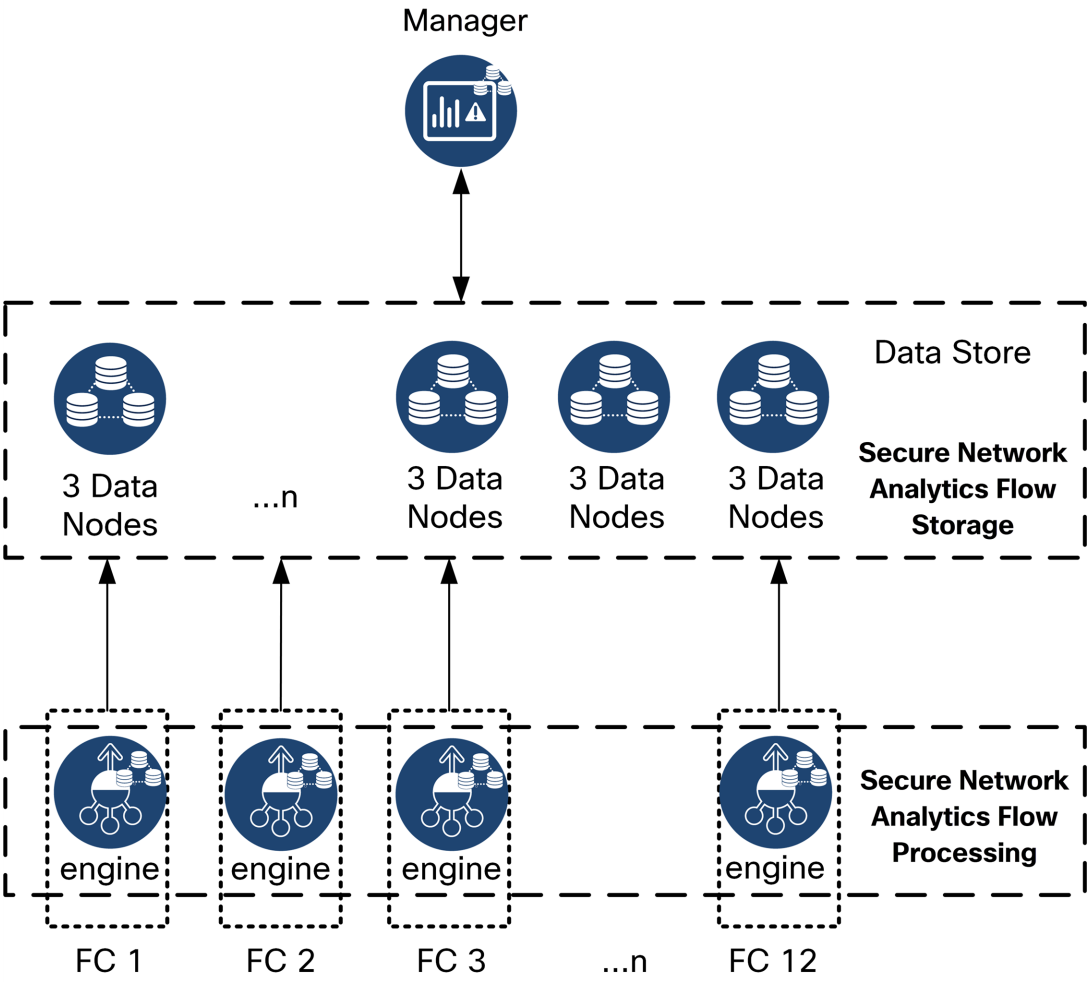
# Secure Network Analytics（Data Store なし）

Data Store なしの Secure Network Analytics の展開では、1 つ以上の Flow Collector がデータを取り込んで複製し、分析を実行してデータと結果を Manager に直接レポートします。グラフやチャートを含むユーザーが送信したクエリを解決するために、Manager は管理対象のすべての Flow Collector に照会します。各 Flow Collector は、一致する結果を Manager に返します。Manager はさまざまな結果セットからの情報を照合し、結果を表示するグラフまたはチャートを生成します。この展開では、各 Flow Collector はローカルデータベースにデータを格納します。例として次の図を参照してください。



# Secure Network Analytics（Data Store あり）

Data Store Secure Network Analytics を使用した Cisco Secure Network Analytics の展開では、Data Store クラスタは Manager と Flow Collector の間に配置されます。1 つ以上の Data Store がフローを取り込み、重複排除し、分析を実行して、データと結果を Data Store に直接報告し、すべての Data Node にほぼ均一に分散させます。Data Store は、データの保管を容易にし、すべてのトラフィックを複数の Flow Collector に分散させずに一元化された場所に保持して複数の Flow Collector よりも大きなストレージ容量を提供します。例として次の図を参照してください。




Data Store は、Flow Collector によって収集されたネットワークのテレメトリを保存する中央リポジトリを提供します。Data Store は、Data Store のクラスタで構成されます。各クラスタには、データの一部と個別 Data Node のデータのバックアップが含まれます。すべてのデータが 1 つの集中型データベースに存在し、複数の Flow Collector に分散されていないため、Manager はすべての Flow Collector に個別にクエリする場合よりも Data Store から迅速にクエリ結果を取得できます。Data Store クラスタは、耐障害性の向上、クエリ応答の改善、グラフとチャート生成の迅速化を実現します。

## クエリ

グラフやチャートを含むユーザーが送信したクエリを解決するために、Manager は Data Store に照会します。Data Store は、クエリに関連する列で一致する結果を検索し、一致する行を取得してクエリ結果を Manager に返します。Manager は、複数の Flow Collector からの複数の結果セットの照合を必要とせずに、グラフまたはチャートを生成します。したがって、複数の Flow Collector にクエリする場合と比較して、クエリのコストが軽減され、クエリのパフォーマンスが向上します。

## Data Store のストレージと耐障害性

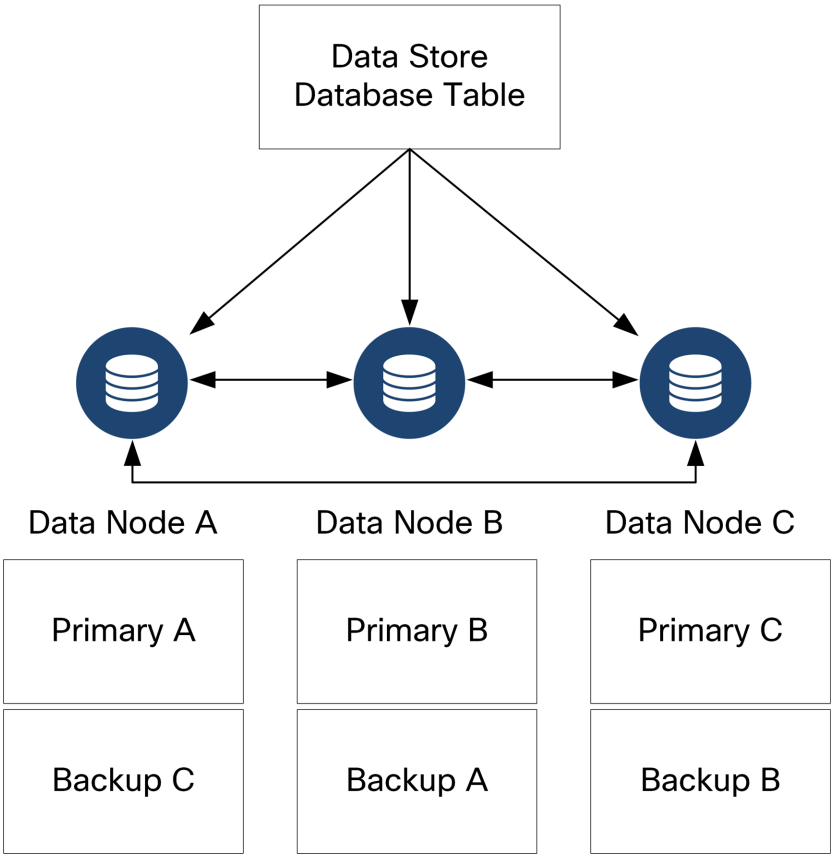
Data Store では、Flow Collector からデータを収集し、クラスタ内の Data Node に均等に分散させます。それぞれの Data Node に、全体のテレメトリの一部が格納され、さらに別の Data Node のテレメトリについてのバックアップも格納されます。この方法でデータを格納することで、次のような利点があります。

- ロードバランシングに役立ちます。
- 各ノードに処理が分散されます。
- Data Store に取り込まれたすべてのデータのバックアップが保持され、耐障害性が確保されます
- Data Node の数を増やすことで、全体的なストレージとクエリのパフォーマンスを向上させることができます

Data Store に 3 つ以上の Data Node がある状況で、いずれかの Data Node が停止した場合、そのバックアップを格納している Data Node がまだ使用可能であり、Data Node の総数の少なくとも半分が稼働していれば、Data Store は全体として稼働状態を維持します。その結果、停止した接続または障害のあるハードウェアを修復する時間的余裕が得られます。問題がある Data Node を交換すると、Data Store により、交換されたノードのデータが隣接する Data Node に格納されている既存のバックアップから復元され、その Data Node にデータのバックアップが作成されます。

## テレメトリストレージの例

3 つの Data Node におけるテレメトリの格納方法の例については、次の図を参照してください。



# 一般的な展開要件

開始する前に、このガイドを参照して、プロセス、およびインストールを計画するために必要な準備、時間、リソースについて確認してください。

## インストール方法

仮想アプライアンスのインストールには、VMware 環境または KVM（カーネルベース仮想マシン）を使用できます。

> ⚠ インストールを開始する前に、次のセクションに記載されている「**互換**」の情報と「**リソース要件**」を確認します。

| 方法 | 設置手順（参照用） | インストールファイル | 詳細 |
|---|---|---|---|
| VMware vCenter | **3a. VMware vCenter を使用した仮想アプライアンスのインストール（ISO）** | ISO | VMware vCenter を使用して仮想アプライアンスをインストールします。 |
| VMware ESXi スタンドアロンサーバー | **3b. ESXi スタンドアロンサーバーへの仮想アプライアンスのインストール（ISO）** | ISO | ESXi スタンドアロンホストサーバーに仮想アプライアンスをインストールします。 |
| KVM および Virtual Machine Manager | **3c. KVM ホストへの仮想アプライアンスのインストール（ISO）** | ISO | KVM と Virtual Machine Manager を使用して仮想アプライアンスをインストールします。 |

## 互換

VMware 環境または KVM（カーネルベースの仮想マシン）に仮想アプライアンスをインストールする場合は、次の互換性情報を確認してください。

### すべてのアプライアンスの一般的な要件

| 要件 | 説明 |
|---|---|
| 専用リソース | すべてのアプライアンスには専用リソースの割り当てが必要であり、他のアプライアンスまたはホストと共有することはできません。 |
| ライブマイグレーションなし | アプライアンスは、破損の可能性があるため、vMotion をサポートしていません。 |

| 要件 | 説明 |
| --- | --- |
| ネットワークアダプタ | すべてのアプライアンスには、少なくとも 1 つのネットワークアダプタが必要です。<br>Flow Sensor を、追加のアダプタを使用して設定し、追加のスループットをサポートできます。<br>Data Node には、Data Store の一部として他の Data Node と通信するための 2 番目のネットワークアダプタが必要です。 |
| ストレージ コントローラ | VMware で ISO を設定する場合は、SCSI コントローラのタイプとして [LSI論理 SAS（LSI Logic SAS）] を選択します。 |
| ストレージのプロビジョニング | 仮想アプライアンスを展開する際、シックプロビジョニング（Lazy Zeroed）のストレージプロビジョニングを割り当てます。 |
| CPU 命令セットの要件 | CPU が AVX/AVX2 命令セットに対応していることを確認します。ESXi の場合は、VM ハードウェアバージョン 11 以上を選択します。KVM の場合は、ホストパススルーを使用することを推奨します。 |

## VMware

- **互換性**：VMware 7.0 または 8.0
- **オペレーティングシステム**：Debian 11 64 ビット
- **ネットワーク アダプタ**：最高のパフォーマンスを得られるよう、VMXNET3 アダプタタイプの使用をお勧めします。
- **ISO 展開**：Cisco Secure Network Analytics v7.5.0 には VMware 7.0 および 8.0 との互換性があります。VMware 6.0、6.5、または 6.7 と Cisco Secure Network Analytics v7.5.x はサポートしていません。詳細については、『vSphere 6.0, 6.5, and 6.7 End of General Support』の VMware のマニュアルを参照してください。
- **ライブマイグレーション**：ホストからホストへのライブマイグレーション（vMotion の使用など）はサポートされていません。
- **スナップショット**：仮想マシンのスナップショットはサポートされていません。

> ⚠ すでにインストールされているカスタムバージョンが上書きされるため、Secure Network Analytics 仮想アプライアンスに VMware ツールをインストールしないでください。インストールすると、仮想アプライアンスが動作不能になり、再インストールが必要になります。

## KVM

- **互換性**：任意の互換 Linux ディストリビューションを使用できます。
- **KVM ホスト バージョン**：KVM ホスト上での仮想マシンのインストールに使用される方法は複数あります。次のコンポーネントを使用して KVM をテストし、適切なパフォーマンスが確認されました。

  - libvirt 2.10 ～ 7.1.0
  - qemu-KVM 2.6.1 ～ 5.2.0
  - Open vSwitch 2.6.x ～ 2.15.x****
  - Linux カーネル 4.4.x、および一部の 5.10.x
- **オペレーティングシステム**：Debian 11 64 ビット。
- **仮想化ホスト**：最小要件と最適なパフォーマンスについては、「**リソース要件**」セクションを確認するとともに、Cisco.com にあるアプライアンスのハードウェア仕様シートを参照してください。

> システム パフォーマンスはホスト環境に左右されます。パフォーマンスは変動する場合があります。

## ソフトウェアのダウンロード

Cisco Software Central を使用して、仮想アプライアンス（VE）のインストールファイル、パッチ、およびソフトウェア更新ファイルをダウンロードします。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。手順については、「**2. Virtual Edition インストールファイルのダウンロード**」を参照してください。

## TLS

アプライアンスの TLS バージョン構成を次のように選択できます。

- TLS 1.2 および 1.3（デフォルト）
- TLS 1.3 のみ（Data Store ではサポートされていません）

## サード パーティ製アプリケーション

Secure Network Analytics は、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をサポートしていません。

## ブラウザ

- **互換性のあるブラウザ**：Secure Network Analytics は Chrome、Firefox、および Microsoft Edge の最新バージョンをサポートしています。
- **Microsoft Edge**：Microsoft Edge には、ファイル サイズの制限がある可能性があります。Microsoft Edge を使用して Virtual Edition ISO ファイルをインストールすることは推奨されません。

## ホスト名

アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。

## ドメイン名

各アプライアンスには完全修飾ドメイン名が必要です。ドメインが空のアプライアンスはインストールできません。

## NTP サーバー

- **設定**：各アプライアンスに少なくとも 1 台の NTP サーバーが必要です。
- **問題のある NTP**：130.126.24.53 NTP サーバーがサーバーのリストに含まれている場合は削除します。このサーバーには問題があることが判明しており、シスコのデフォルトの NTP サーバー リストからはすでに除外されています。

## タイム ゾーン

すべての Secure Network Analytics アプライアンスは協定世界時（UTC）を使用します。

- **仮想ホスト サーバー**：仮想ホスト サーバーが正しい時刻に設定されていることを確認します。

> ⚠ 仮想アプライアンスをインストールする仮想ホスト サーバーに設定された時刻が正しい時刻に設定されていることを確認します。正しくない場合、アプライアンスを起動できないことがあります。

## 標準アプライアンスの要件（Data Store なし）

Data Store なしで Secure Network Analytics をインストールする場合は、次のアプライアンスをインストールします。

| アプライアンス | 要件 |
|---|---|
| マネージャ | • 1 つ以上の Manager |
| フローコレクタ | • 1 つ以上の Flow Collector |
| UDP Director | オプション |
| フローセンサー | オプション |

Data Store ありの Secure Network Analytics に関するアプライアンスのインストール要件については、「**Data Store の展開要件**」を参照してください。

## Manager と Flow Collector の展開要件

展開する Manager と Flow Collector のそれぞれについて、ルーティング可能な IP アドレスを `eth0` 管理ポートに割り当てます。

# Data Store の展開要件

Data Store ありの Secure Network Analytics を展開するには、展開に関する次の要件と推奨事項を確認してください。

## アプライアンスの要件（Data Store あり）

次の表に、Data Store を使用した Secure Network Analytics の展開に必要なアプライアンスの概要を示します。

| アプライアンス | 要件 |
|---|---|
| マネージャ | • 1 つ以上の Manager |
| データストア | • 少なくとも 1 つまたは 3 つの Data Node<br>• Data Store を拡張するための付加的な 3 つの Data Node のセット（Data Node の最大数は 36 個）<br>• 1 つのクラスタに 2 つの Data Node のみを展開することはできません。 |
| フローコレクタ | • 1 つ以上の Flow Collector |
| フローセンサー | オプション |

⚠ アプライアンスの機能に問題が発生する可能性があるため、アプライアンスの BIOS を更新しないでください。

## Manager と Flow Collector の展開要件

展開する Manager と Flow Collector のそれぞれについて、ルーティング可能な IP アドレスを `eth0` 管理ポートに割り当てます。

- **eth0 ポート設定**：Manager および Flow Collector `eth0` 管理ポートには、**BASE-T** 銅線 1G/10G ポートまたは SFP+ Twinax ケーブル 10G ポートを使用するように設定できます。
- **スループット**：Data Store で使用する BASE-T 銅線ポートには 10G のスループットが必要です。Data Store を展開していない場合は、100Mbps/1Gbps/10 Gbps 銅線インターフェイスのみを `eth0` として設定できます。

## Data Node の展開要件

各 Data Store は、複数の Data Node で構成されます。

- **ハードウェア**：各ハードウェア Data Node は独自のシャーシです。（3 つのセットに）1 つ、3 つ、またはそれ以上の Data Nodes を展開できます。
- **Virtual Edition**：仮想 Data Store をダウンロードすると、1 つ、3 つ、またはそれ以上の Data Node Virtual Edition を導入できます（3 つで 1 セット）。

Data Node がすべてハードウェアであるか、すべて Virtual Edition であることを確認してください。ハードウェア Data Node と仮想 Data Node の混在はサポートされておらず、ハードウェアは同じハードウェア世代（すべて DS 6200 またはすべて DN 6300）である必要があります。

## 複数 Data Node 展開

複数 Data Node 展開により、パフォーマンスの面で最大の成果を得られます。たとえば、3 つの Data Node 6300 Data Store 展開では、約 90 日間にわたり 1 秒あたり約 150 万フローを保持できます。

次の点に注意してください。

- **3 つで 1 セット**：Data Node は、Data Store の一部として、最小 3 つから最大 36 まで 3 の倍数でクラスタ化できます。1 つのクラスタに 2 つの Data Node のみを展開することはできません。
- **すべてハードウェアまたはすべて仮想**：Data Node がすべて（同じ世代の）ハードウェアである、またはすべて Virtual Edition であることを確認します。ハードウェア Data Node と仮想 Data Node の混在、または Data Store 6200 と Data Node 6300 の混在はサポートされていません。

## サポートされるハードウェアメトリック（Analytics が有効な場合）

| ノード数 | 1 秒あたりのフロー | 固有内部ホスト |
|---|---|---|
| 1 | 600,000 | 1.3 万 |
| 3 以上 | 600,000 | 1.3 万 |
| 3 以上 | 850,000 | 700,000 |

これらの推奨事項では、テレメトリのみを考慮しています。パフォーマンスは、ホスト数、Flow Sensor の使用、トラフィックプロファイル、その他のネットワーク特性など、追加の要因によって異なる場合があります。サイジングについては、シスコ サポート までお問い合わせください。

## サポートされるハードウェアメトリック（Analytics が有効になっていない場合）

| ノード数 | 1 秒あたりのフロー | 固有内部ホスト |
|---|---|---|
| 1 | 最大 100 万 | 最大 3,300 万 |
| 3 以上 | 最大 300 万 | 最大 3,300 万 |

これらの数値は、130 万の固有ホストにより平均顧客データを使用してシスコのテスト環境で算出したものです。それぞれ環境でのパフォーマンスは、ホスト数や平均フローサイズなど、いくつかの要因によって影響を受ける可能性があります。サイジングについては、シスコ サポート までお問い合わせください。

### 単一 Data Node 展開

単一（1 つ）の Data Node を展開することを選択した場合：

- **Flow Collector**：最大 4 つの Flow Collector がサポートされます。
- **Data Node の追加**：Data Node を 1 つだけ展開した場合、将来展開に Data Node を追加できます。詳細については、「**複数 Data Node 展開**」を参照してください。

> これらの推奨事項では、テレメトリのみを考慮しています。パフォーマンスは、ホスト数、Flow Sensor の使用、トラフィックプロファイル、その他のネットワーク特性など、追加の要因によって異なる場合があります。サイジングについては、シスコサポートにお問い合わせください。

> 現在、Data Store では、プライマリ Data Node が停止した場合のスペア Data Node との自動交換はサポートされていません。ガイダンスについては、シスコサポートにお問い合わせください。

## Data Node の設定要件

Data Store を展開するには、各 Data Node に以下を割り当てます。お客様が準備する情報は、『システム コンフィギュレーション ガイド』を使用して初回セットアップで設定されます。

- **ルーティング可能な IP アドレス（eth0）**：Secure Network Analytics アプライアンスに対する管理、取り込み、クエリ通信に使用します。
- **eth0 ポート設定**：`eth0` 管理ポートには、サポート対象のトランシーバで、BASE-T 銅線 1G/10G ポートまたは SFP+ Twinax ケーブル 10G ポートを使用するように設定できます。
- **スループット**：Data Store で使用する BASE-T 銅線ポートには 10G のスループットが必要です。
- **Data Node 間通信**：Data Node 間通信に使用されるプライベート LAN または VLAN 内の `169.254.42.0/24` CIDR ブロックからルーティング不可能な IP アドレスを設定します。

  スループットパフォーマンス向上のため、Data Node の `eth2` ポート（または `eth2` と `eth3` を含むポートチャネル）を Data Node 間通信用のスイッチに接続します。Data Store の一部として、Data Node は相互に通信します。
- **ネットワーク接続**：管理、取り込み、クエリ通信用と Data Node 間通信用の 2 つの 10G ネットワーク接続が必要です。
- **追加の接続 とスイッチ**：（オプション）ハードウェア Data Node のみを対象とする、ネットワークの冗長性および Data Node 間通信の重要性に応じた、追加の 10G 接続、および Data Node のポートチャネルを確立する追加のスイッチ。

> 隣接する番号の Data Node に個別の冗長電源から電力を供給するように Data Node を構成します。この構成により、データの冗長性と Data Node の全体的な稼働時間が向上します。

## ネットワーキングとスイッチングに関する考慮事項

次の表に、Data Store ありの Secure Network Analytics を展開する場合のネットワーキングとスイッチングに関する考慮事項の概要を示します。

| ネットワークに関する考慮事項 | 説明 |
| --- | --- |
| Data Node 間通信 | • Data Node 間での推奨されるラウンドトリップ時間（RTT）の遅延を 200 マイクロ秒未満 に設定します。<br>• Data Node 間のクロックスキューを 1 秒以下に保ちます。<br>• Data Node 間での推奨スループットを 6.4 Gbps 以上（10 Gbps 全二重スイッチ接続）に設定します。<br>• ハードウェア Data Node の場合、通常の Data Node 間の通信には、`eth2` ポートで 10G のスループットを設定すれば十分です。最大 20G のスループットを実現するボンディングされた LACP `eth2/eth3` ポートチャネルを作成すると、Data Node 間の高速な通信が可能になり、新しい各 Data Node が隣接する Data Node からトラフィックを受信してデータを取り込むため、Data Store への Data Node の追加や交換が迅速になります。LACP ポートボンディングは、ハードウェア Data Node で使用できる唯一のボンディングオプションであることに注意してください。 |
| Data Node ハードウェアの電源 | • ハードウェア Data Node の電源が予期せず失われると、データが破損する可能性があります。無停電電源装置と、別回路の電源装置の両方を使用します。<br>• Data Store クラスタの初期化時に、各 Data Node が使用する電源に基づいて Data Node の設定を切り替えます。この操作により、電源が失われた場合にダウンする Data Node の数を最小限に抑えることで、耐障害性を最適化できます。 |
| Data Node のスイッチング | • Data Node は、Data Node 間通信を可能にするために独自のレイヤ 2 VLANを必要とします。ハードウェア Data Node は、共有または専用の 10G スイッチに接続できます。<br>• ハードウェア Data Node を 2 台のスイッチに接続して、スイッチの停止時およびアップグレード時にも接続が保たれるようにすることを推奨します。Data Node 間通信には低遅延が必要なため、シスコでは、2 台のスイッチが相互接続され両方のスイッチでレイヤ 2 VLAN が伝送される、スイッチの冗長ペアを推奨しています。 |
| Secure Network Analytics アプライアンス通信 | • Manager および Flow Collector は、すべての Data Node に到達できる必要があります<br>• Data Node は、Manager、すべての Flow Collector、および各 Data Node に到達できる必要があります |

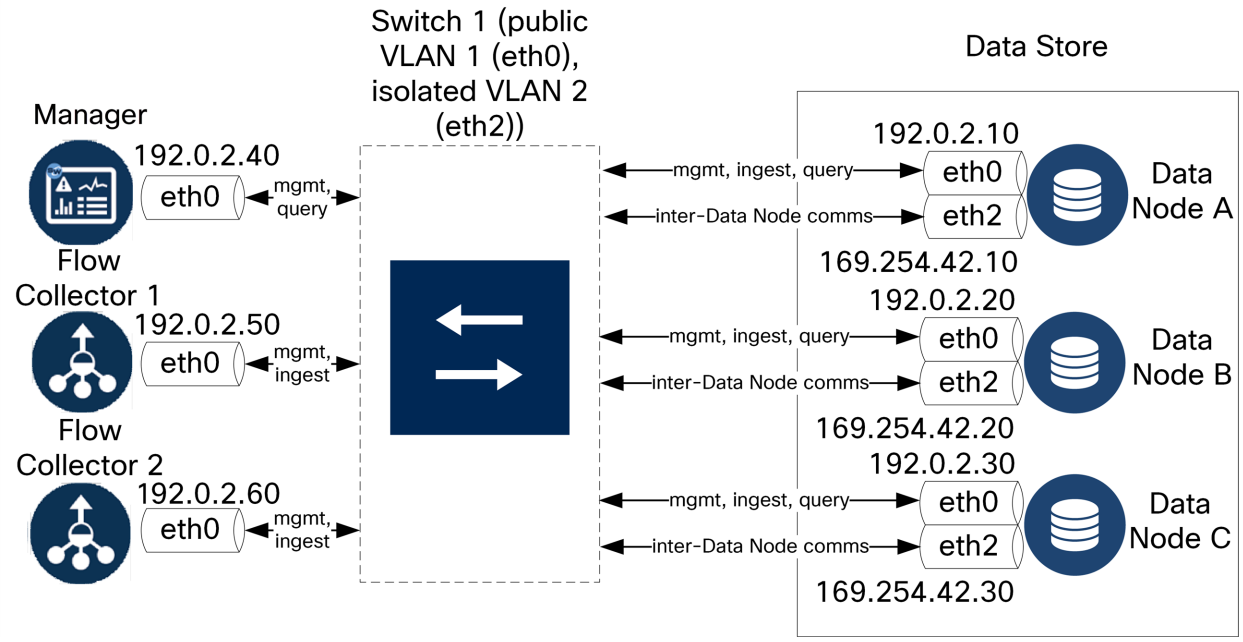
現在、Data Store では、プライマリ Data Node が停止した場合のスペア Data Node との自動交換はサポートされていません。ガイダンスについては、シスコサポートにお問い合わせください。

## ハードウェアスイッチの例

`eth2` または `eth2/eth3` ポートチャネルを介した Data Node 間の通信を有効にするには、10G の速度をサポートするスイッチを 1 台導入します。

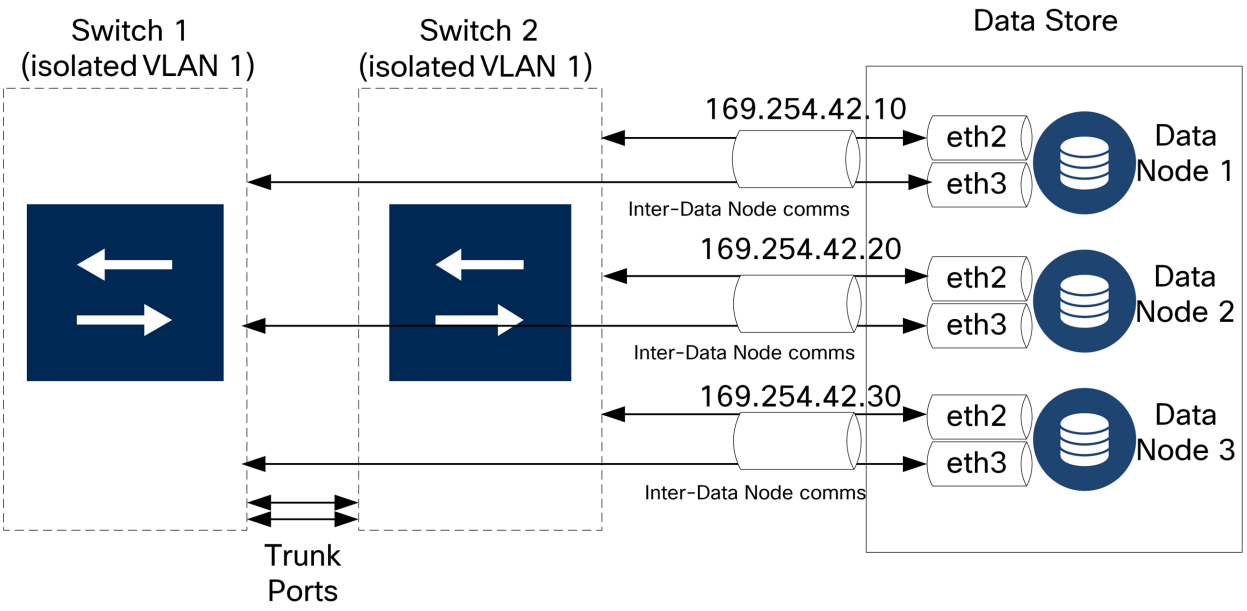
Data Node の Manager および Flow Collector との `eth0` 通信用に LAN または VLAN を設定し、Data Node 間の通信用に独立した LAN または VLAN を設定します。

これらのスイッチは他のアプライアンスと共有できますが、追加のアプライアンストラフィック用に別の LAN または VLAN を作成してください。例として次の図を参照してください。




Data Store クラスタでは、独立 VLAN 内のノード間で継続的なハートビートが必要です。このハートビートがないと、Data Node がオフラインになる可能性があり、Data Store が停止するリスクが高まります。

スイッチの更新や計画的停止に備えてネットワークの冗長性をさらに高める場合は、Data Node で Data Node 間の通信専用のポートチャネルを設定してください。それぞれの Data Node について、各物理ポートを異なるスイッチに接続して 2 つのスイッチに接続します。例として次の図を参照してください。




導入の計画については、Cisco プロフェッショナルサービスにお問い合わせください。

## Data Store の配置に関する考慮事項

Data Node は、それぞれがすべての Flow Collector、Manager、および他の Data Node と通信できるように配置します。最適なパフォーマンスを得るには、Data Node と Flow Collector を同じ場所に配置して通信の遅延を最小限に抑え、Data Node と Manager を同じ場所に配置してクエリのパフォーマンスを最適化します。

- **ファイアウォール**：シスコでは、Data Node をファイアウォール内（NOC 内など）に配置することを強く推奨しています。
- **電力**：電力の喪失やハードウェアの障害が原因で Data Store が停止すると、データ破損やデータ損失のリスクが高くなります。Data Node の設置においては、常に稼働時間が維持されるように考慮します。

Data Node の電源が予期せずに失われ、アプライアンスをリブートした場合、その Data Node のデータベースインスタンスが自動的に再起動しないことがあります。データベースのトラブルシューティングと手動での再起動については、『システム コンフィギュレーション ガイド』を参照してください。

- **ポリシー**：ハードウェア Data Node の電源復元ポリシーが［最後の状態の復元（Restore Last State）］に設定されていることを確認します。この設定の場合、電源喪失後に Data Node が自動的に再起動し、実行中のプロセスの復元が試行されます。CIMC での電源復元ポリシーの設定の詳細については、『UCS C-Series GUI Configuration Guide』を参照してください。

## Analytics の展開の要件

Secure Network Analytics は、ダイナミック エンティティ モデリングを使用してネットワークの状態を追跡します。Secure Network Analytics のコンテキストにおけるエンティティとは、ネットワーク上のホストやエンドポイントといった、何らかの経時的に追跡できるものです。ダイナミック エンティティ モデリングは、ネットワークで送信されるトラフィックと実行されるアクティビティに基づいて、エンティティに関する情報を収集します。詳細については、『 Analytics: Detections, Alerts, and Observations Guide』を参照してください。

Analytics を有効にするには、以下の条件で展開を設定する必要があります。

- 任意の数の Flow Collector を備えた仮想またはハードウェア Data Store 展開で設定する。
- Secure Network Analytics Data Store ドメインは 1 つのみ使用する。

# 1. 通信用ファイアウォールの設定

アプライアンスが適切に通信できるようにするには、ファイアウォールまたはアクセス コントロール リストによって必要な接続がブロックされないようにネットワークを設定する必要があります。この項に示される情報を使用して、アプライアンスがネットワークを介して通信できるようにネットワークを設定します。

## オープンポート（すべてのアプライアンス）

次のポートが開いた状態になってアプライアンス（Manager、Flow Collector、Data Node、Flow Sensor、UDP Director）で無制限のアクセスが可能になるように、ネットワーク管理者と話し合ってください。

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 8910
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

## Data Node 用のその他のオープンポート

また、Data Node をネットワークに展開する場合は、次のポートが開いた状態で、無制限のアクセスを提供できることを確認してください。

- TCP 5433
- TCP 5444
- TCP 9450

## 通信ポートおよびプロトコル

Secure Network Analytics でポートがどのように使用されるかを次の表に示します。

| 送信元（クライアント） | 宛先（サーバ） | ポート | プロトコル |
|---|---|---|---|
| 管理者ユーザーの PC | すべてのアプライアンス | TCP/443 | HTTPS |
| すべてのアプライアンス | ネットワークの時刻源 | UDP/123 | NTP |
| Active Directory | Manager | TCP/389、UDP/389 | LDAP |
| Cisco ISE | Manager | TCP/443 | HTTPS |
| Cisco ISE | Manager | TCP/8910 | XMPP |
| 外部ログ ソース | Manager | UDP/514 | SYSLOG |
| Flow Collector | Manager | TCP/443 | HTTPS |
| UDP Director | Manager | TCP/443 | HTTPS |
| UDP Director | Flow Collector（sFlow） | UDP/6343* | sFlow |
| UDP Director | Flow Collector（NetFlow） | UDP/2055* | NetFlow |
| UDP Director | サードパーティのイベント管理システム | UDP/514 | SYSLOG |
| Flow Sensor | Manager | TCP/443 | HTTPS |
| Flow Sensor | Flow Collector（NetFlow） | UDP/2055 | NetFlow |
| NetFlow エクスポータ | Flow Collector（NetFlow） | UDP/2055* | NetFlow |
| sFlow エクスポータ | Flow Collector（sFlow） | UDP/6343* | sFlow |
| Manager | UDP Director | TCP/443 | HTTPS |
| Manager | Cisco ISE | TCP/443 | HTTPS |
| マネージャ | Cisco ISE | TCP/8910 | XMPP |
| Manager | DNS | UDP/53 | DNS |

| 送信元（クライアント） | 宛先（サーバ） | ポート | プロトコル |
|---|---|---|---|
| Manager | Flow Collector | TCP/443 | HTTPS |
| Manager | Flow Sensor | TCP/443 | HTTPS |
| Manager | Flow エクスポータ | UDP/161 | SNMP |
| マネージャ | LDAP | TCP/636 | TLS |
| マネージャ | CRL 分散ポイント | TCP/80 | HTTP |
| マネージャ | OCSP レスポンダ | TCP/80 | OCSP |
| ユーザー PC | Manager | TCP/443 | HTTPS |

＊これはデフォルト ポートですが、任意の UDP ポートをエクスポータで設定できます。

## Data Store 用のその他のオープンポート

Data Store を展開するためにファイアウォールで開く通信ポートを次に示します。

| # | 送信元（クライアント） | 宛先（サーバー） | ポート | プロトコルまたは目的 |
|---|---|---|---|---|
| 1 | マネージャ | Flow Collector と Data Node | 22/TCP | SSH（Data Store データベースの初期化に必要） |
| 1 | Data Node | 他のすべての Data Node | 22/TCP | SSH（Data Store データベースの初期化およびデータベース管理タスクに必要） |
| 2 | Manager、Flow Collector、および Data Node | NTP サーバー | 123/UDP | NTP（時刻同期に必要） |
| 2 | NTP サーバー | Manager、Flow Collector、および Data Node | 123/UDP | NTP（時刻同期に必要） |
| 3 | マネージャ | Flow Collector と Data Node | 443/TCP | HTTPS（アプライアンス間のセキュア通信に必要） |
| 3 | Flow Collector | マネージャ | 443/TCP | HTTPS（アプライアンス間のセキュア通信に必要） |

| | | | | |
|---|---|---|---|---|
| 3 | Data Node | マネージャ | 443/TCP | HTTPS（アプライアンス間のセキュア通信に必要） |
| 4 | NetFlow エクスポータ | Flow Collector：NetFlow | 2055/UDP | NetFlow の取り込み |
| 5 | Data Node | 他のすべての Data Node | 4803/TCP | Data Node 間メッセージングサービス |
| 6 | データノード | 他のすべての Data Node | 4803/UDP | Data Node 間メッセージングサービス |
| 7 | Data Node | 他のすべての Data Node | 4804/UDP | Data Node 間メッセージングサービス |
| 8 | Manager、Flow Collector、および Data Node | Data Node | 5433/TCP | Vertica クライアント接続 |
| 9 | データノード | 他のすべての Data Node | 5433/UDP | Vertica メッセージングサービスのモニターリング |
| 10 | sFlow エクスポータ | Flow Collector（sFlow） | 6343/UDP | sFlow の取り込み |
| 11 | Data Node | 他のすべての Data Node | 6543/UDP | Data Node 間メッセージングサービス |

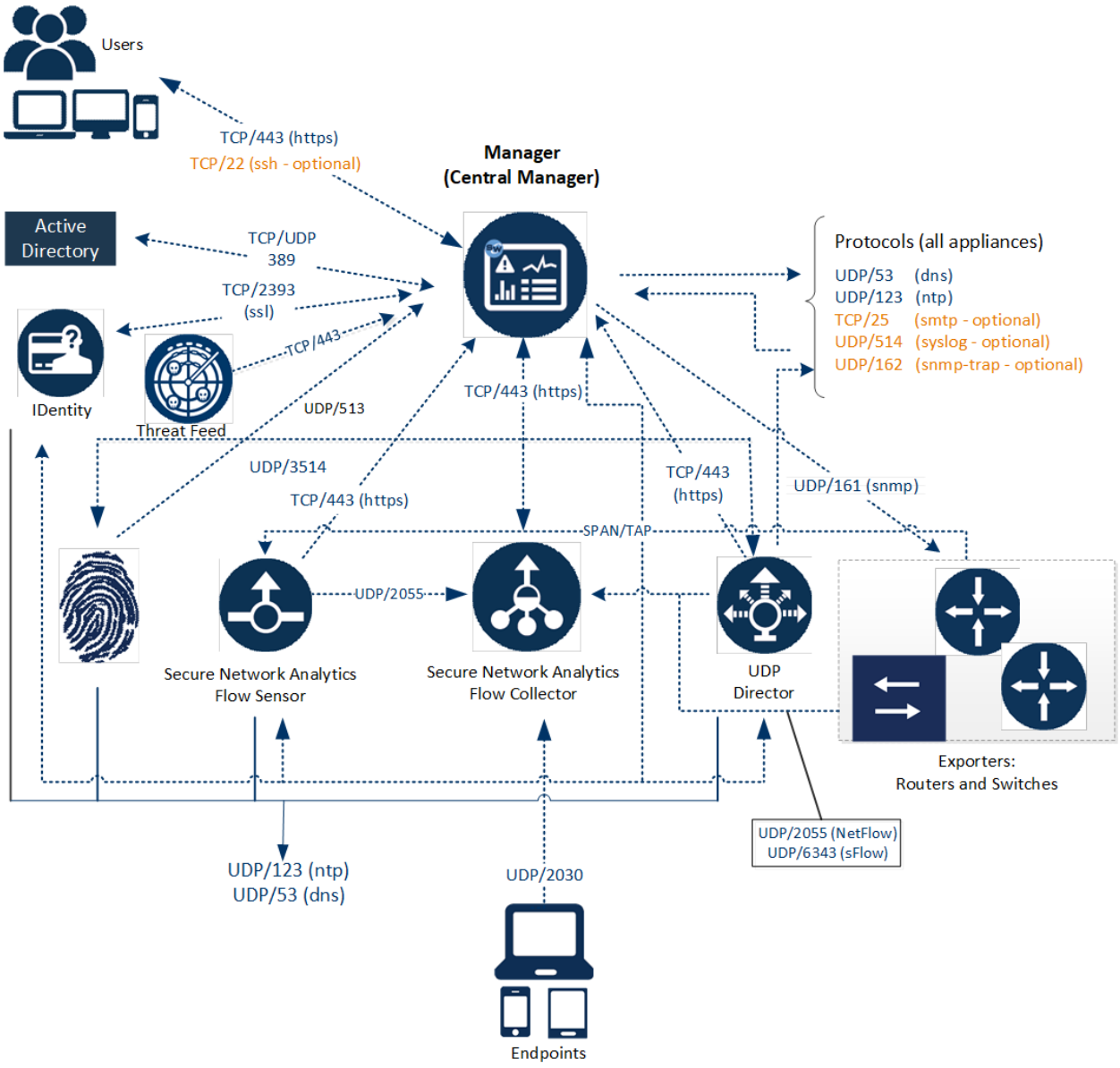
## オプションの通信ポート

次の表に、ネットワーク要件によって決まる任意の設定を示します。

| 送信元（クライアント） | 宛先（サーバ） | ポート | プロトコル |
|---|---|---|---|
| すべてのアプライアンス | ユーザー PC | TCP/22 | SSH |
| Manager | サードパーティのイベント管理システム | UDP/162 | SNMP – トラップ |
| Manager | サードパーティのイベント管理システム | UDP/514 | SYSLOG |
| Manager | 電子メール ゲートウェイ | TCP/25 | SMTP |
| Manager | 脅威フィード | TCP/443 | SSL |
| ユーザー PC | すべてのアプライアンス | TCP/22 | SSH |

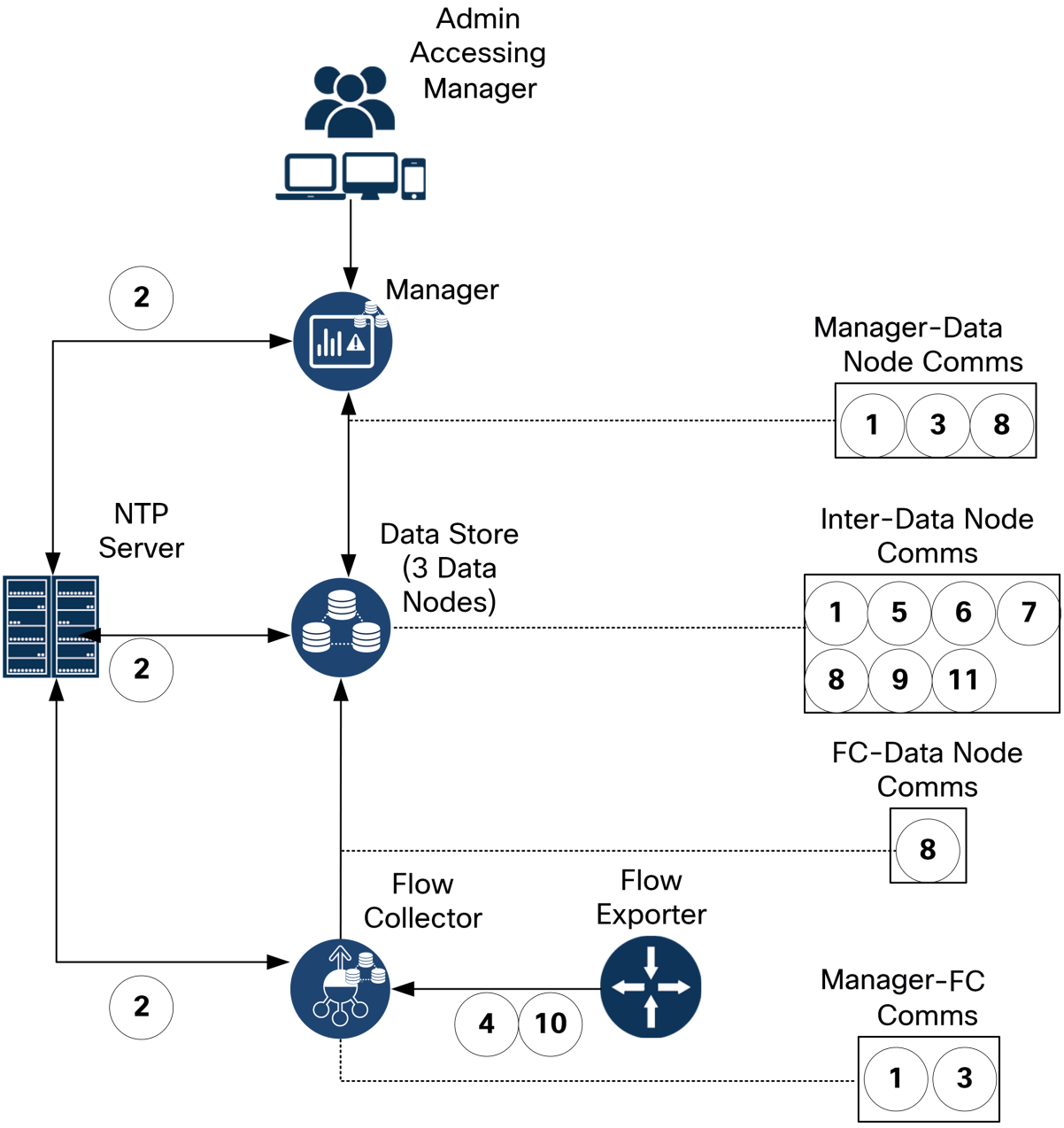
## Secure Network Analytics 展開例

次の図は、Secure Network Analytics システムによって使用されるさまざまな接続を示しています。これらのポートの一部はオプションです。



## Secure Network Analytics Data Store を使用した展開の例

以下の図に示すように、Secure Network Analytics アプライアンスは、内部ネットワーク、ネットワーク周辺、または DMZ 内のいずれであっても、ネットワーク全体で重要なネットワークセグメントの最適なカバレッジが提供されるように戦略的に展開することができます。



# 2. 設置に関する警告およびガイドライン

## 設置に関する警告

Secure Network Analytics x2xx シリーズのアプライアンスを設置する前に、『 Regulatory Compliance and Safety Information』のドキュメントをお読みください。

次の警告に注意してください。

ステートメント 1071：警告の定義

安全上の重要な注意事項

⚠ 「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。警告の各国版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

⚠ ステートメント 1004：設置方法

設置手順を読んでから、システムを使用、取り付け、または電源に接続してください。

⚠ ステートメント 1005：回路ブレーカー

この製品は、設置する建物にショート（過電流）保護機構が備わっていることを前提に設計されています。

⚠ ステートメント 1006：ラックへの設置と保守に関するシャーシ警告

ラックへのユニットの設置や、ラック内のユニットの保守作業を行う場合は、負傷事故を防ぐため、システムが安定した状態で置かれていることを十分に確認してください。安全を確保するために、次の注意事項を守ってください。
・ラック内の装置が 1 台だけの場合は、ラックの一番下に取り付けます。
・ラックにすでに他の装置が搭載されている場合は、最も重いコンポーネントをラックの一番下にして、重い順に下から上へと搭載するようにしてください。
・ラックにすでに他の装置が搭載されている場合は、最も重いコンポーネントをラックの一番下にして、重い順に下から上へと搭載するようにしてください。

ステートメント 1015：バッテリの取り扱い

火災、爆発、または可燃性液体やガス漏れのリスクを軽減するには：
・交換用バッテリは元のバッテリと同じものか、製造元が推奨する同等のタイプのものを使用してください。
・分解、粉砕、破壊、鋭利な道具を使った取り外し、外部接点のショート、バッテリーの火中への廃棄は行わないでください。
・バッテリーがゆがんだり、膨らんだりしているときは使用しないでください。
・60° C（140° F）を超える温度でバッテリーを保管または使用しないでください。
・69.7 kPa よりも低い低気圧環境でバッテリーを保管または使用しないでください。

ステートメント 1017：立ち入り制限区域

この装置は、出入りが制限された場所に設置されることを想定しています。熟練者、教育を受けた担当者、または資格保持者のみが立ち入り制限区域に入ることができます。

ステートメント 191：日本向け VCCI クラス A に関する警告

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き 起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求される ことがあります。

ステートメント 164：持ち上げに関する要件

製品の重い部分を持ち上げるには 2 人の人員が必要です。けがをしないように、背中はまっすぐにして、腰ではなく足に力を入れて持ち上げます。

ステートメント 256：クラス A の警告（ハンガリー）

この装置はクラス A 製品であり、ハンガリーの MC クラス A 要件（MSZEN55022）に準拠して使用、設置される必要があります。クラス A 装置は、一般の民間組織用に設計され、特別な設置条件と保護距離条件が適用されます。

ステートメント 294：クラス A の警告（韓国）

これは、クラス A 準拠装置であり、工業用の電磁適合性（EMC）要件のために登録されます。営業担当者または購入者はこれを認識する必要があります。このタイプを誤って販売または購入した場合、住宅用途タイプと交換する必要があります。

ステートメント 340：CISPR22/EN55022/CISPR32/EN55032 に関するクラス A の警告

本製品はクラス A 製品です。国内環境で本製品を使用すると、電波障害を引き起こす可能性があります。その場合には、ユーザーが十分な対策を講じるように求められることがあります。

ステートメント 1021：SELV 回路

感電を防ぐため、安全超低電圧（SELV）回路を電話網電圧（TNV）回路に接続しないでください。LAN ポートには SELV 回路が、WAN ポートには TNV 回路が組み込まれています。一部の LAN ポートおよび WAN ポートでは、共に RJ-45 コネクタが使用されています。ケーブルを接続する際は、注意してください。

ステートメント 1024：アース導体

この装置は、接地させる必要があります。絶対にアース導体を破損させたり、アース線が正しく取り付けられていない装置を稼働させたりしないでください。アースが適切かどうかはっきりしない場合には、電気検査機関または電気技術者に確認してください。

ステートメント 1028：複数の電源

この装置には複数の電源装置接続が存在する場合があります。感電の危険を減らすために、すべての接続を取り外してユニットの電源を切ります。

ステートメント 1029：ブランクの前面プレートおよびカバー パネル

ブランクの前面プレートおよびカバーパネルには、3 つの重要な機能があります。感電および火災のリスクを軽減すること、他の装置への電磁波干渉（EMI）の影響を防ぐこと、およびシャーシ内の冷気の流れを適切な状態に保つことです。システムは、必ずすべてのカード、前面プレート、前面カバー、および背面カバーを正しく取り付けた状態で運用してください。

ステートメント 1030：機器の設置

この装置の設置、交換、または保守は、訓練を受けた相応の資格のある人が行ってください。

ステートメント 1032：シャーシの持ち上げ

怪我またはシャーシの破損を防ぐために、モジュール（電源装置、ファン、カードなど）のハンドルを持ってシャーシを持ち上げたり、傾けたりすることは絶対に避けてください。これらのハンドルには、ユニットの重量を支える強度はありません。

ステートメント 9001：製品の廃棄

本製品の最終処分は、各国のすべての法律および規制に従って行ってください。

ステートメント 1051：レーザー放射

接続されていない光ファイバ ケーブルやコネクタからは目に見えないレーザー光が放射されている可能性があります。レーザー光を直視したり、光学機器を使用して直接見たりしないでください。

ステートメント 1055：クラス I およびクラス 1M レーザーまたはその一方

目に見えないレーザー放射があります。望遠鏡を使用しているユーザーに光を当てないでください。これは、クラス 1/1M のレーザー製品に適用されます。

ステートメント 1008：クラス 1 レーザー製品

この製品はクラス 1 レーザー製品です。

ステートメント 1056：未終端の光ファイバ ケーブル

未終端の光ファイバの末端またはコネクタから、目に見えないレーザー光が放射されている可能性があります。光学機器で直接見ないでください。ある種の光学機器（ルーペ、拡大鏡、顕微鏡など）を使用し、100 mm 以内の距離でレーザー出力を見ると、目を傷めるおそれがあります。

| ファイバの種類とコア径（μm） | 波長（nm） | 最大電力（mW） | ビーム発散（rad） |
|---|---|---|---|
| SM 11 | 1200 ～ 1400 | 39 ～ 50 | 0.1 ～ 0.11 |
| MM 62.5 | 1200 ～ 1400 | 150 | 0.18 NA |
| MM 50 | 1200 ～ 1400 | 135 | 0.17 NA |
| SM 11 | 1400 ～ 1600 | 112 ～ 145 | 0.11 ～ 0.13 |

ステートメント 1089：教育を受けた担当者および熟練者の定義

教育を受けた担当者とは、熟練者から教育やトレーニングを受け、機器を操作する際に必要な予防措置を講じられる人です。

熟練者または資格保持者とは、機器の技術に関するトレーニングを受けているか経験があり、機器を操作する際に潜む危険を理解している人です。

ステートメント 1090：熟練者による設置

この機器の設置、交換、または修理は、熟練者のみが実施できます。熟練者の定義については、「ステートメント 1089」を参照してください。

ステートメント 1091：教育を受けた担当者による設置

この機器の設置、交換、または修理は、教育を受けた担当者または熟練者のみが実施できます。教育を受けた担当者または熟練者の定義については、「ステートメント 1089」を参照してください。

ステートメント 1074：地域および国の電気規則への適合

機器の取り付けは各地域および各国の電気規格に適合する必要があります。

ステートメント 2017：FCC に関するクラス A の注意

シスコの許可なしに装置を改造した場合、装置がクラス A のデジタル装置に対する FCC 要件に準拠しなくなることがあります。その場合、装置を使用するユーザの権利が FCC 規制により制限されることがあり、ラジオまたはテレビの通信に対するいかなる干渉もユーザ側の負担で矯正するように求められることがあります。
この機器は、FCC 規定の Part 15 に基づくクラス A デジタル デバイスの制限に準拠していることがテストによって確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザー側の負担で干渉防止措置を講じる必要があります。

ステートメント 2021：クラス A の注意（カナダ）

このクラス A デジタル装置は、カナダの ICES-003/NMB-003 に準拠しています。

ステートメント 7001：静電気の軽減

この装置は、静電気に弱い可能性があります。装置を取り扱う前に、常に静電気防止用アンクルまたはリスト ストラップを使用してください。静電気防止用ストラップの装置側を塗装されていない装置のシャーシの面、または提供されている場合は装置の ESD ジャックに接続します。

ステートメント 7003：建物内雷サージに対するシールドケーブルの要件

装置またはサブアセンブリの屋内ポートでは、シールドされた建物内配線または、両端がアースに接続された配線を使用する必要があります。
次のポートは、この機器の建物内ポートと見なされます。

ステートメント 7005：建物内落雷サージおよび AC 電源障害

装置またはサブアセンブリのイントラビルディング ポートは、建物内配線や非露出配線、またはケーブル配線だけの接続に適しています。機器またはサブアセンブリの屋内ポートは、OSP またはその配線につながるインターフェイスに 6 m（約 20 フィート）以上にわたって金属的に接続しないでください。これらのインターフェイスは屋内インターフェイス専用（GR-1089 に記載されたタイプ 2、タイプ 4、またはタイプ 4a ポート）に設計されており、屋外用の OSP ケーブルと区別する必要があります。一次保護装置を追加しても、これらのインターフェイスを OSP 配線系統に金属的に接続するには保護が不十分です。次のポートは、この機器の建物内ポートと見なされます。

## 設置に関するガイドライン

次の警告を記録しておいてください。

ステートメント 1047：過熱の防止

システムの過熱を防ぐため、周囲温度が推奨範囲の最大値である 5 ～ 35° C（41 ～ 95° F）度を超える場所ではシステムを使用しないでください。

ステートメント 1019：主要な切断装置

いつでも装置の電源を切断できるように、プラグおよびソケットにすぐ手が届く状態にしておいてください。

ステートメント 1075：電源コードおよび AC アダプタ

製品を設置する際は、同梱または指定のケーブル、電源ケーブル、および AC アダプタ/バッテリを使用してください。他のケーブルやアダプタを使用すると、誤動作や発火が生じることがあります。電気用品安全法により、シスコによって指定された製品以外の電気製品で、UL 認定のケーブル（コードに「UL」または「CSA」と記載）を使用することは禁じられています。同法で規制されていないものはコードに「PSE」と表示されます。

ステートメント 1073：ユーザーが保守可能な部品なし

スイッチ内部にはユーザーが保守できる部品はありません。筐体を開けないでください。

シャーシを設置するときは、次のガイドラインに従ってください。

- シャーシの作業に支障がないように、また適切なエアーフローが確保されるように、アプライアンス周辺に十分なスペースを確保できることを確認してください。シャーシのエアーフローは、前面から背面に向かいます。

シャーシを取り付ける際は、適切なエアーフローを確保するために、レール キットを使用する必要があります。レール キットを使用せずに、ユニットを別のユニットの上に物理的に置く、つまり積み重ねると、シャーシの上部にある通気口がふさがれ、過熱したり、ファンの回転が速くなったり、電力消費が高くなったりする原因となる可能性があります。シャーシをラックに取り付けるときは、これらのレールによりシャーシ間で必要な最小の間隔が提供されるので、レール キットにシャーシをマウントすることを推奨します。レール キットを使用してマウントする場合は、シャーシ間の間隔を余分にとる必要はありません。

- 空調が 5 ～ 35° C（41 ～ 95° F）の温度でシャーシを維持できることを確認します。
- キャビネットまたはラックが、ラック要件に適合していることを確認します。
- 設置場所の電源が、「仕様シート」に記載された電源要件に適合していることを確認します。使用可能な場合は、電源障害に備えて UPS を使用してください。

鉄共振テクノロジーを使用する UPS タイプは使用しないでください。このタイプの UPS は、システムに使用すると、データトラフィック パターンの変化によって入力電流が大きく変動し、動作が不安定になるおそれがあります。

## 安全に関する推奨事項

次の情報により、安全を確保し、シャーシを保護することができます。この情報には、作業環境で生じる可能性のある危険な状況がすべて網羅されているわけではありません。絶えず注意して、的確な判断を心がけてください。

これらの安全に関する注意事項を遵守してください。

- 設置作業中および作業後は、設置場所を整理し、埃のない状態に保ってください。
- 工具は、通行の邪魔にならない場所に置いてください。
- ゆったりとした衣服やイヤリング、ブレスレット、ネックレスなどの装飾品は身につけず、シャーシに引っかかることがないようにしてください。
- 目が危険にさらされる状況で作業する場合は、保護眼鏡を着用してください。
- 人身事故や装置障害を引き起こす可能性のある作業は行わないでください。
- 重量が 1 人で扱える範囲を超えているものを、単独で持ち上げないでください。

## 電気製品を扱う場合の注意

シャーシの作業を行う前に、必ず電源コードを抜いてください。

電気機器を取り扱う際には、次の注意事項に従ってください。

- 危険を伴う作業は、一人では行わないでください。
- 電源が切断されていると思い込まずに、必ず確認してください。
- 床が濡れていないか、アースされていない電源延長コード、すり減った電源コード、保護アースの不備などがないかどうか、作業場所の安全を十分に確認してください。
- 電気事故が発生した場合は、次のように対処してください。
    - 負傷しないように注意してください。
    - システムの電源を切断してください。

    - 可能であれば、だれかに頼んで救護を呼んでもらいます。それができない場合は、負傷者の状況を見極めてから救援を要請してください。
    - 負傷者に人工呼吸または心臓マッサージが必要かどうかを判断し、適切な処置を施してください。
- シャーシは、指定された定格電力の範囲内で、製品の使用説明書に従って使用してください。

## 静電破壊の防止

電子部品の取り扱いが不適切な場合、ESD が発生し、機器の損傷や電気回路の破損を引き起こす可能性があります。その結果、機器の断続的障害または完全な故障を引き起こします。

部品の取り外しまたは交換を行うときは、必ず静電気防止手順に従ってください。シャーシが電気的にアースに接続されていることを確認してください。静電気防止用リスト ストラップを肌に密着させて着用してください。アースクリップをシャーシフレームの塗装されていない表面に止めて、静電気が安全にアースに流れるようにします。静電放電による損傷とショックを防止するには、リストストラップとコードを効果的に作用させる必要があります。リストストラップがない場合は、シャーシの金属部分に触れて、身体を接地してください。

安全を確保するために、静電気防止用ストラップの抵抗値を定期的にチェックしてください。抵抗値は 1 ～ 10 MΩ である必要があります。

## 設置場所の環境

機器故障を予防し、環境に起因するシャットダウンを防ぐため、注意して設置場所のレイアウトや機器の配置を検討してください。既存の装置で停止やエラーが頻繁に起きている場合にも、この考慮事項を参考にすることにより、障害の原因を突き止め、今後問題が起きないように予防できます。

## 電源モジュールに関する考慮事項

シャーシを設置する際には、以下のことを考慮してください。

- シャーシを設置する前に、設置場所の電源を調べ、スパイクやノイズがないかどうかを確認してください。必要に応じて電源調整器を設置し、アプライアンス入力電圧にて適切な電圧および電力レベルを確保してください。
- 設置場所で適切にアースし、雷や電力サージによる損傷を防止してください。
- シャーシでは、ユーザが動作範囲を選択できません。シャーシの正確なアプライアンス入力所要電力については、そのラベルを参照してください。
- 複数の種類の AC 入力電源コードをアプライアンスに使用できます。設置場所に適したタイプを使用してください。
- デュアル冗長（1 + 1）電源を使用している場合は、各電源に独立した電気回路を使用することを推奨します。
- できるだけ、無停電電源装置を使用してください。

## ラックの構成に関する考慮事項

ラックの構成を決めるときは、次のことを考慮してください。

- 開放型ラックにシャーシをマウントする場合、ラックのフレームで吸気口や排気口をふさがないように注意してください。
- 閉鎖型ラックに十分な通気があることを確認してください。各シャーシで熱が発生するため、ラック内に装置を詰め込みすぎないように注意してください。冷気が回るように、閉鎖型ラックにはルーバーが付いた側面とファンが必要です。
- 閉鎖型ラックの上部に換気用ファンが付いている場合には、ラックの下段に設置した装置の熱が上昇し、上段の装置の吸気口から入り込む可能性があります。ラック下段の装置に対して、十分な換気が行われるようにしてください。
- バッフルは吸気から排気を分離するときに役立ちます。また、シャーシ内に冷気を取り込むためにも役立ちます。隔壁は、シャーシ内に冷気を行き渡らせるためにも有効です。隔壁の最適な取り付け位置は、ラック内の空気がどのように流れるかによって異なります。

# 3. アプライアンスのマウント

Secure Network Analytics アプライアンスは、標準の 19 インチラックまたはキャビネット、その他の適切なキャビネット、または平らな面に直接マウントすることができます。ラックまたはキャビネット内にアプライアンスをマウントする場合は、レール マウント キットに含まれている手順に従ってください。アプライアンスの配置場所を決める場合は、前面および背面パネルまでのスペースが以下の要件を満たしていることを確認します。

- 前面パネルのインジケータが見やすいこと。
- 背面パネルのポートに無理なくケーブルを接続できること。
- 背面パネルの電源コネクタが調整済み AC 電源の近くにあること。
- アプライアンスの周囲および通気口を通過するエアーフローが妨げられないこと。

## アプライアンスに付属するハードウェア

Secure Network Analytics アプライアンスには、次のハードウェアが含まれます。

- AC 電源コード
- アクセス キー（前面プレート）
- ラック マウント用のレール キットまたは小型アプライアンス用のマウント用取り付け金具
- Flow Collector 5210 シリーズ アプライアンスの場合は、10 GB SFP ケーブル

## 追加で必要なハードウェア

以下のハードウェアを追加で用意する必要があります。

- 標準の 19 インチ ラック用取り付けネジ。
- 設置している 各 Stealthwatch システム製品の無停電電源装置（UPS）。
- （オプション）ローカルに設定するには、次のいずれかの方法を使用します。
    - ラップトップとビデオ ケーブルおよび USB ケーブル（キーボード用）
    - ビデオ モニターとビデオ ケーブルおよびキーボードと USB ケーブル

# 4. ネットワークへのアプライアンスの接続

各アプライアンスを同じ方法でネットワークに接続します。接続に関する唯一の相違点は、使用するアプライアンスのタイプです。

## 1. 仕様の確認

各アプライアンスを同じ方法でネットワークに接続します。接続に関する唯一の相違点は、使用するアプライアンスのタイプです。

- **仕様シート**：各アプライアンスの仕様の詳細については、Secure Network Analytics 仕様シートを参照してください。
- **UCS プラットフォーム**：すべての Cisco x2xx ハードウェアは、UCSC-C240- M5SX を使用する Flow Collector 5210 DB を除いて、同じ UCS プラットフォーム（ UCSC-C220-M5SX）を使用します。アプライアンスの違いは、NIC カード、プロセッサ、メモリ、ストレージおよび RAID にあります。
- **Manager 2210**：Data Store を展開する場合は、スループットを向上させるため、10Gbps SFP+ DAC インターフェイスを備えた Manager 2210 を eth0 として設定できます。Data Store を展開していない場合は、100 Mbps/1 Gbps/10 Gbps 銅線インターフェイスのみを eth0 として設定できます。
- **Flow Collector 4210**：Data Store を展開する場合は、スループットを向上させるため、10Gbps SFP+ DAC インターフェイスを備えた Flow Collector 4210 を eth0 として設定できます。Data Store を展開していない場合は、100 Mbps/1 Gbps/10 Gbps 銅線インターフェイスのみを eth0 として設定できます。
- **Flow Collector 5210**：Flow Collector 5210 は、接続された 2 台のサーバー（データベースとエンジン）で構成されており、これらのサーバーは単一のアプライアンスとして機能します。このため、他のアプライアンスとは設置方法が若干異なります。まず、両サーバーを 10G SFP+ DA クロス接続ケーブルで相互に直接接続します。次に、ネットワークに接続します。
- システムを設定するときは、システム構成ガイドで指定されている順序でデータベースとエンジンを設定してください。

> ⚠ アプライアンスの機能に問題が発生する可能性があるため、アプライアンスの BIOS を更新しないでください。

## 2. ネットワークへのアプライアンスの接続

アプライアンスをネットワークに接続するには、次の手順に従います。

1. イーサネットケーブルをアプライアンスの背面にある管理ポートに接続します。
2. Flow Sensor と UDP Director の少なくとも 1 つのモニター ポートを接続します。

    - **UDP Director 高可用性**：クロスケーブルで 2 つの UDP Director を接続します。1 つの UDP Director の eth2 ポートを 2 つ目の UDP Director の eth2 ポートに接続します。同様に、2 本目のクロス ケーブルで各 UDP Director の eth3 ポートを接続します。ケーブルには、光ファイバまたは銅線を使用できます。

- **イーサネットラベル**：各ポートのイーサネットラベル（eth2、eth3 など）を書き留めます。これらのラベルは、システム設定で使用されるネットワーク インターフェイス（eth2、eth3 など）に対応します。

3. イーサネット ケーブルのもう一方の端をネットワークのスイッチに接続します。
4. 電源コードを電源に接続します。一部のアプライアンスには、電源 1 と電源 2 の 2 つの電源接続があります。

# 5. アプライアンスへの接続

このセクションでは、システム設定のためにアプライアンスに接続する方法について説明します。

接続手順を選択します。

- **キーボードとモニターを使用した接続**
- **シリアルケーブルまたはシリアルコンソールによる接続**
- **CIMC との接続（リモートアクセスに必要）**リモートアクセスのためにアプライアンスに接続するには、この手順に従います。

## キーボードとモニターを使用した接続

IP アドレスをローカルに設定するには、次の手順を実行します。

1. 電源ケーブルをアプライアンスに差し込みます。
2. 電源ボタンを押してアプライアンスをオンにします。起動が完全に終了するまで待機します。起動プロセスを中断しないでください。

> 場合によっては、電源を適用するために前面パネルを取り外す必要があります。
>
> 一部のモデルでは、システムの電源が入っていないときに電源ファンがオンになります。前面パネルの LED がオンになっているか確認します。
>
> アプライアンスを必ず無停電電源装置（UPS）に接続してください。電源には電力が必要です。電力がない場合、エラーが表示されます。

3. 次の手順でキーボードを接続します。
    - 標準キーボードの場合は、標準のキーボード コネクタに接続します。
    - USB キーボードの場合は、USB コネクタに接続します。
4. ビデオ コネクタにビデオ ケーブルを接続します。ログイン プロンプトが表示されます。
5. 「**6. Secure Network Analytics システムの設定**」に進みます。

## シリアルケーブルまたはシリアルコンソールによる接続

シリアルケーブルまたはシリアルコンソール（ターミナルエミュレータを搭載したラップトップなど）を使用して、アプライアンスに接続することもできます。手順の例としてラップトップを使用します。

1. 次のいずれかの方法を使用してラップトップをアプライアンスに接続します。
    - ラップトップのシリアル ポート コネクタ（DB9）からアプライアンスのコンソール ポートに RS232 ケーブルを接続します。
    - ラップトップのイーサネット ポートからアプライアンスの管理ポートにクロス ケーブルを接続します。

2. 電源ケーブルをアプライアンスに差し込みます。
3. 電源ボタンを押してアプライアンスをオンにします。起動が完全に終了するまで待機します。起動プロセスを中断しないでください。

> 場合によっては、電源を適用するために前面パネルを取り外す必要があります。
>
> 一部のモデルでは、システムの電源が入っていないときに電源ファンがオンになります。前面パネルの LED がオンになっているか確認します。アプライアンスを必ず無停電電源装置(UPS)に接続してください。電源には電力が必要です。電力がない場合、エラーが表示されます。

4. ラップトップで、アプライアンスへの接続を確立します。

   任意のターミナル エミュレータを使用して、アプライアンスと通信できます。

5. 次の設定を適用します。

   - BPS:115200
   - データ ビット:8
   - ストップ ビット:1
   - パリティ:なし
   - フロー制御:なし

   ログイン画面とログイン プロンプトが表示されます。

6. 「**6. Secure Network Analytics システムの設定**」に進みます。

## CIMC との接続(リモートアクセスに必要)

Cisco Integrated Management Controller(CIMC)を使用すると、サーバーの構成と仮想サーバー コンソールにアクセスし、ハードウェアの健全性をモニターすることができます。Secure Network Analytics のシステム設定でも CIMC を使用します。

1. 『Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide』の手順に従います。
2. 管理者として CIMC にログインし、[パスワード(Password)] フィールドに **password** と入力します。
3. ネットワークのセキュリティを確保するためにデフォルトのパスワードを変更します。
4. 「**6. Secure Network Analytics システムの設定**」に進みます。

# 6. Secure Network Analytics システムの設定

Virtual Edition アプライアンスやハードウェアアプライアンスのインストールが完了したら、管理対象システムに Secure Network Analytics を構成できます。

> ⚠ Secure Network Analytics を設定するには、『Secure Network Analytics System Configuration Guide v7.5.0』の手順に従ってください。この手順は、システムの設定と通信を正常に完了させるために重要です。
>
> 必ず、システム構成ガイドで指定されている順序でアプライアンスを設定してください。

## システム設定要件

CIMC を介してアプライアンスコンソールにアクセスできることを確認します。

次の表を使用して、各アプライアンスに必要な情報を準備します。

| 設定要件 | 詳細 | アプライアンス |
|---|---|---|
| IPアドレス | ルーティング可能な IP アドレスを以下に割り当てます。`eth0` 管理ポートを選択します。 | |
| ネットマスク | | |
| ゲートウェイ | | |
| ホスト名 | アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。 | |
| ドメイン名 | 各アプライアンスには完全修飾ドメイン名が必要です。ドメインが空のアプライアンスはインストールできません。 | |
| DNS サーバ | 名前解決のための内部 DNS サーバー | |
| NTP サーバ | サーバー間同期のための内部タイムサーバー。各アプライアンスに少なくとも 1 台の NTP サーバーが必要です。<br>130.126.24.53 NTP サーバーがサーバーのリストに含まれている場合は削除します。このサーバーには問題があることが判明しており、シスコのデフォルトの NTP サーバー リストからはすでに除外されています。 | |
| メールリレーサーバー | アラートと通知を送信する SMTP メールサーバー | |

| | | |
|---|---|---|
| Flow Collector エクスポートポート | Flow Collector のみに必要です。<br>NetFlow のデフォルト：2055 | |
| プライベート LAN または VLAN 内のルーティング不可能な IP アドレス（Data Node 間通信用） | Data Node のみに必要です。<br>• ハードウェア eth2、または eth2 と eth3 のボンディング。LACP `eth2/eth3` ボンディングポートチャネル（最大 20G のスループット）を作成すると、Data Node 間の高速な通信が可能になり、Data Store への Data Node の追加や交換が迅速になります。LACP ポートボンディングは、ハードウェア Data Node で使用できる唯一のボンディングオプションであることに注意してください。<br>• 仮想 eth1<br>**IP アドレス：（IP Address:）**提供された IP アドレスを使用するか、Data Node 間通信の次の要件を満たす値を入力できます。<br>• **ルーティング不可能な IP アドレス 、169.254.42.0/24 CIDR ブロック由来、**169.254.42.2 ～ 169.254.42.254。<br>• **最初の 3 オクテット：**169.254.42<br>• **サブネット：**/24<br>• **逐次：**メンテナンスを容易にするために、連続した IP アドレス（169.254.42.10、169.254.42.11、169.254.42.12 など）を選択します。<br>**ネットマスク：**<br>ネットマスクは 255.255.255.0 にハードコードされており、変更できません。 | |
| eth0 ハードウェア接続ポート | Data Store での Secure Network Analytics Data Store ハードウェアアプライアンスを使用する Cisco Secure Network Analytics にのみ必要です。<br>• マネージャ<br>• Flow Collector<br>• Data Node<br>eth0 ハードウェア接続ポートオプション：<br>• **SFP+**： | |

# 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：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

# 変更履歴

| マニュアルのバージョン | 公開日 | 説明 |
| --- | --- | --- |
| 1_0 | 2023 年 12 月 15 日 | 初版 |

# 著作権情報