



# Cisco EPN Manager セキュリティ

この章は次のトピックで構成されています。

- [セキュリティの概要 \(1 ページ\)](#)
- [セキュアなアーキテクチャ \(2 ページ\)](#)
- [セキュアなデフォルト設定 \(8 ページ\)](#)
- [インストールの強化 \(8 ページ\)](#)
- [CSDL プロセス \(18 ページ\)](#)

## セキュリティの概要

Cisco EPN Manager には、ネットワークとそのデータが侵害されないようにする高レベルのセキュリティが必要です。これは、ネットワークを完全に管理し、デバイスのクレデンシャルを保存するのに特に重要です。この目的のために、Cisco EPN Manager は次のセキュリティアプローチを利用します。

- **セキュアなアーキテクチャ**：Cisco EPN Manager アーキテクチャは、存在する可能性のある未知のソフトウェアの欠陥へのアクセスを制限し、悪意のある目的に使用できないように設計されています。
- **セキュアなデフォルトの設定**：Cisco EPN Manager は製品のセキュリティを強化するデフォルトの設定が標準装備されています。たとえば、セキュアでない FTP サービスや TFTP サービスがサポートされていても、デフォルト設定ではアクティブ化されません。
- **インストールの強化**：シスコのアドバンスド サービス チームは、Cisco EPN Manager のインストールの具体的な内容を評価し、必要と思われる追加のセキュリティ強化タスクを実行できます。
- **シスコ セキュア開発ライフサイクル (CSDL) プロセス**：開発からリリースまで、CSDL プロセスに従って Cisco EPN Manager のセキュリティを向上させます。

以降の項では、これらのアプローチについてさらに詳しく説明します。

## セキュアなアーキテクチャ

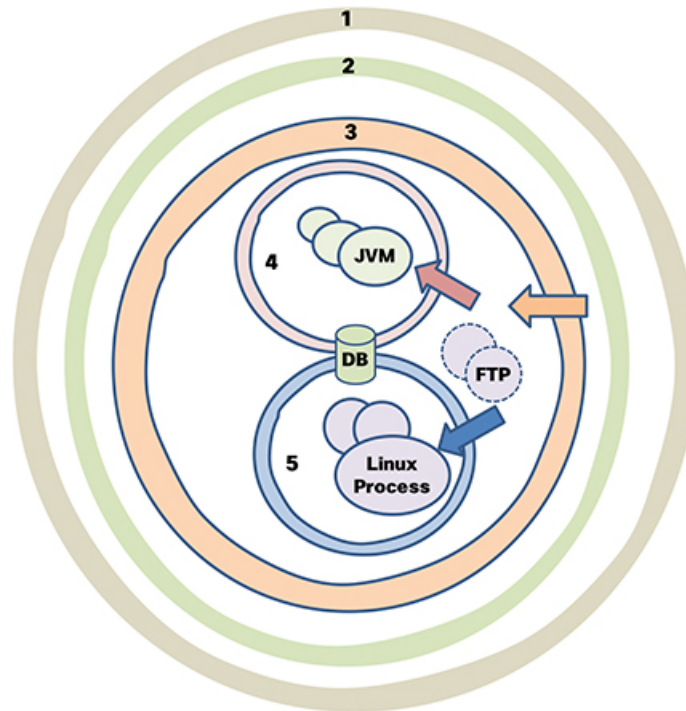
Cisco EPN Manager のアーキテクチャ設計では、攻撃者がシステムに侵入するには次の3つの条件が同時に存在する必要があるという前提に基づいています。

- システムに欠陥がある。
- 攻撃者がその欠陥にアクセスできる。
- 悪意のある目的でこの欠陥を悪用する能力が攻撃者にある (Hughes, J., & Cybenko, G. 2013 年。Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity. *Technology Innovation Management Review*, 3(8): 15-24)。

欠陥はそのままであれば無害です。攻撃者が欠陥にアクセスでき、悪用する方法知っている場合にのみ、その欠陥は脆弱性となります。この欠陥と脆弱性の区別を理解しておくことが重要です。欠陥が公になっただけで、それが自動的に脆弱性となるわけではありません。特定の状況下でのみ、欠陥は脆弱性になり得ます。

セキュリティリスクを管理するために Cisco EPN Manager で用いられているアプローチの鍵は、システムの欠陥へのアクセスを制限することです。見つかる可能性があるどの欠陥にも攻撃者が容易にアクセスすることができないように Cisco EPN Manager アーキテクチャは設計されています。ユーザが常に欠陥を排除したり、攻撃者による悪用を防ぐことができるとは限らないため、これは実用的で合理的なアプローチです。複数のセキュリティレイヤを配置することで、存在する特定の欠陥へのアクセスを制限できます。Cisco EPN Manager は、図 1 に示すように、境界セキュリティの3つのレイヤを使用します。

図 1: 複数レイヤで保護された境界アーキテクチャ：強化された外部シェルを備えた仮想アプライアンスシステム

**1: Network Firewall Layer**

Allows only valid traffic. See Tables 1 and 2 and the firewall configuration tips provided in the Cisco EPN Manager installation guide.

**2: Encrypted Link Layer**

SSH, SSL/TLS, TLS-EAP, and SNMPv3 encryption scheme protects from snooping and man-in-the-middle attacks.

**3: Embedded Application Firewall Layer**

Only allows certain incoming TCP and UDP port traffic. Details are provide in Table 1.

**4: Webserver**

Configuration restricts resource access based on security and access policies.

**5: CARS Shell**

Proprietary shell allows whitelisted command set.

これら3つのレイヤのうち、1つはCisco EPN Managerの内部に存在し、2つは外部に存在します。内部レイヤはCisco EPN Managerで事前に設定され、インストールが完了すると動作できるようになります。2つの外部レイヤは事前に設定されていないため、外部ネットワークファイアウォールと暗号化された通信リンクレイヤを作成して実装する必要があります。会社のテクニカルチームとシスコアドバンスドサービスとが連携し、これらのアイテムを作成することをお勧めします。



(注) ネットワークに使用するのに適切なタイプの暗号化プロトコルを選択するには、Cisco EPN Manager内の一部の設定を変更する必要があります。

内部レイヤはCisco EPN Managerに組み込まれており、次のコンポーネントで構成されています。

- 組み込みファイアウォール：内部コンポーネントに関する最初の保護レイヤーを提供します。これにより、着信トラフィックに対して開かれるポートはごくわずかになります。そのため、Linux OSおよびOracleデータベースの複数の欠陥（既知と不明の両方）へのアクセスを制限することで、攻撃の領域が減少します。
- CARS シェル：Linuxでの実行を許可されているコマンドのホワイトリストを適用し、OSとのやり取りを制限することで、Linuxに関する保護レイヤを提供します。

- Web サーバ : Linux、Java 仮想マシン、およびデータベースに関する保護レイヤを提供します。このレイヤには、Java およびデータベースリソースとメソッドへのアクセスを制限するためのセキュリティ フィルタが設定されています。

この内部レイヤは、次の例で説明するような多くのリスクからシステムを保護します。これらの欠陥は、保護されていないシステムの脆弱性と見なされますが、Cisco EPN Manager には存在しません。次の例では (National Vulnerability Database ID によって識別)、外部ファイアウォールと暗号化されたリンクのレイヤは攻撃者によって侵害されたか、または実在していないかのいずれかです。

- CVE-2013-5211 : Linux NTPD コンポーネントの NTP の実装での欠陥。着信 NTP トラフィックにポート 23 からアクセスされた後に DoS 攻撃が発生します。組み込みファイアウォールはこのトラフィックを許可していないため、攻撃者はこの欠陥にアクセスできません。そのため、Cisco EPN Manager でのリスクではありません。
- CVE-2016-0634 : Linux bash シェルの欠陥 : この攻撃は、ポート 22 を介して bash シェルを標的にした認証済みユーザによって行われる可能性があります。Cisco EPN Manager は、ポート 22 を介した bash シェルへの直接アクセスを提供していません。代わりに、CARS シェルには通常の認証済みユーザからアクセスできます。そのため、この欠陥は Cisco EPN Manager のリスクではありません。
- CVE-2017-12617 : Apache Tomcat の欠陥 : PUT 要求が行われたときにこの攻撃が発生する可能性があります。Cisco EPN Manager の Web サーバの設定ではこのタイプのアクセスは許可されないため、この欠陥は危険ではありません。
- CVE-2015-4863 : Oracle データベースの欠陥 : この攻撃は Oracle Net プロトコルを介してネットワーク上で発生する可能性があります。Oracle データベースは組み込みファイアウォールと Web サーバの背後にあるため、この問題は Cisco EPN Manager のリスクではありません。そのため、ネットワークを通じてデータベースにアクセスできません。

## セキュリティアーキテクチャの影響

このアーキテクチャのため、Cisco EPN Manager は非常に密接に統合されたシステムであり、組み込まれている OS やデータベースは、どのような管理目的や操作目的であってもユーザーアクセスに対してオープンではありません。ユーザは、Cisco EPN Manager の GUI と Cisco EPN Manager の管理 CLI を使用してのみ、システムにアクセスして管理することができます。この管理 CLI は Linux CLI ではありません (ユーザインターフェイスとユーザタイプを参照)。また、Cisco EPN Manager は仮想マシンとしてデプロイおよび管理されます。つまり、Cisco EPN Manager はスタンドアロンの仮想マシン (VM) としてデプロイする OVA ファイルとして使用できます。したがって、Cisco EPN Manager の管理は、Linux OS 上で実行されデータベースに接続する Web アプリケーションの管理とは大きく異なります。この結果、ユーザには次のような制限が生じます。

- サードパーティ製またはシスコ以外のパッチによって個々のコンポーネントに対するパッチ適用やアップグレードを行うことはできません。シスコは、組み込みの Linux や Oracle を含むすべての内部コンポーネントについてパッチをリリースします。

- シスコはテクニカルサポートを提供できないため、組み込みの Red Hat Linux OS にサードパーティ製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。
- 組み込みのコンポーネント (Linux、Oracle、Java) を通常のサーバのように簡単に管理することはできません。
- このガイドでユーザが変更可能として記載されていない内部設定を変更しないようにしてください。そのような変更を加えた場合、全体のセキュリティが低下したり、システムの機能やパフォーマンスが無効になったり低下したりする可能性があるためです。



(注) Cisco EPN Manager は、Linux と Oracle が組み込まれてはいますが、Linux OS 上で実行され Oracle データベースに接続する通常の Web アプリケーションではありません。言い換えれば、全体としての総和と各部分の総和とが同じではありません。

Cisco EPN Manager は、強化された外部シェルと密接に統合された仮想アプライアンスです。そのため、Linux、Oracle、および通常の Web アプリケーションのセキュリティを評価するために使用する基準を、Cisco EPN Manager の評価に使用することは「できません」。Oracle の評価に Linux OS の基準を使用することはできません。これらは別々の製品であるためです。同様に、Linux を対象とする基準や方法を使用して Cisco EPN Manager を評価したり、Cisco EPN Manager を評価する目的で Oracle 用の基準や方法を使用することもできません。Cisco EPN Manager のセキュリティを評価するには、Cisco EPN Manager のアーキテクチャに適した別の一連の基準やテスト方法が必要になります。

## Cisco EPN Manager で使用するポート

Cisco EPN Manager は、正当なトラフィックのみがサーバに対して許可されるように、組み込みアプリケーションのファイアウォール設定で出荷されています。表1に、デバイスからの接続要求をリッスンし、着信トラフィックを承認するポートを示します。ファイアウォール内のこれらのポートの開閉は、特定の機能を有効または無効にすると Cisco EPN Manager によって自動的に行われます。ファイアウォール内のポートを有効または無効にする必要はありません。Cisco EPN Manager を回避するファイアウォール設定を指定しようとする、そのセキュリティと整合性が損なわれることがあります。



(注) 次の表には、インストール後のセキュリティ強化を実行するために必要な情報も示されています (詳細については、「[セキュアなデフォルト設定](#)」を参照してください)。

表 1: 組み込みのファイアウォールを介した開いているポートのリスニング

ポート	プロトコル	使用方法	無効にしても安全か?	注記
21	TCP	FTP を使用してデバイスとの間でファイルを転送する。	可	Web GUI の [管理 (Administration) ] > [設定 (Settings) ] > [システム設定 (System Settings) ] から [全般 (General) ] > [サーバ (Server) ] を選択して FTP を無効にします。FTP を無効にした後に CLI 管理者ユーザとしてサーバを停止し、再起動します。
22	TCP	Cisco EPN Manager サーバとの SSH 接続を開始し、SCP または SFTP を使用してファイルを Cisco EPN Manager サーバにコピーする。	場合による	これは、TFTP のみをサポートし、SFTP または SCP をサポートしていない古い管理対象デバイスでも必要になる場合があります。
69	UDP	TFTP を使用してデバイスにイメージを配布する。	場合による	SCP、SFTP、HTTPS などの代替プロトコルがイメージ配布に使用され、管理対象デバイスでサポートされている場合にのみ。
162	UDP	ネットワーク デバイスから SNMP トラップを受信する。	なし	—
443	TCP	HTTPS を介した Cisco EPN Manager サーバへのブラウザアクセスの場合。	なし	—
514	UDP	ネットワーク デバイスから syslog メッセージを受信する。	なし	—
1522	TCP	アクティブとスタンバイの Cisco EPN Manager サーバ間での高可用性 (HA) 通信の場合。  Oracle データベース同期用の Oracle JDBC トラフィックを許可するために使用されます。	可	少なくとも 1 台の Cisco EPN Manager サーバが HA 用に設定されていないとこのポートは自動的に無効になります。
2021	TCP	FTP を使用してデバイスにイメージを配布する。	なし	—

ポート	プロトコル	使用方法	無効にしても安全か?	注記
8082	TCP	HA ヘルス モニタの Web インターフェイスの場合 (HTTP 経由)。 プライマリ サーバとセカンダリサーバが HTTP を介してヘルスステータスを監視するために使用します。	いいえ (HA が設定されている場合)	—
8087	TCP	HA セカンダリ バックアップサーバ上のソフトウェアを更新する (トランスポートとして HTTPS を使用)。	なし	—
9991	UDP	Netflow データ パケットを受信する。	可	Cisco EPN Manager は Netflow をサポートしていません。ネットワークファイアウォールでこのトラフィックを無効にする必要があります。
9992	TCP	HTTP または HTTPS を使用して M-Lync を管理する。	可	Cisco EPN Manager は M-Lync をサポートしていません。ネットワークファイアウォールでこのトラフィックを無効にする必要があります。
11011 ～ 11014	TCP	独自の Cisco Networking Services (CNS) プロトコルトラフィックの PnP 操作の場合。	可	Cisco EPN Manager は PnP をサポートしていません。ネットワークファイアウォールでこのトラフィックを無効にする必要があります。
61617	TCP	Java メッセージング サービス (JMS) 接続上での MTOSINBI 通知の場合。 PnP 操作にも使用されます。	可	Cisco EPN Manager は JMS または PnP 上で MTOSI をサポートしていません。ネットワークファイアウォールでこのトラフィックを無効にする必要があります。

## セキュアなデフォルト設定

Cisco EPN Manager 可能な限りセキュアなデフォルトのアプリケーション設定が搭載されています。それらの設定は、脅威モデルを分析し、特定の状況のリスクを評価した後にのみ、変更できます。デフォルト設定では、Cisco EPN Manager は次を行うよう、最善を尽くします。

- デフォルトのパスワードを使用しない。
- 不要な OS や Oracle パッケージ/サービスにアクセスできないようにする。
- Cisco EPN Manager のリリース時に、組み込み OS および Oracle に最新のセキュリティパッチが適用されます。
- 人間のユーザによる Oracle アクセス パスワードの使用を許可しない。これらのパスワードはマシンで生成され、内部コンポーネントによって使用されます。

## インストールの強化

Cisco EPN Manager のインストールを強化するには、次のタスクを実行する必要があります。

1. 正当なトラフィックのみを許可するように、組み込みの内部および外部のネットワークファイアウォールを設定します。
2. すべての着信トラフィックと発信トラフィックに暗号化を使用します。
3. 正当なトランザクションのみを送信できるように、Cisco EPN Manager とそのピア システムを設定します。

先に進む前に、まず Cisco EPN Manager がピア システムとやり取りする方法を理解する必要があります。一般的な HA 展開用の管理トラフィックフローと外部ネットワークファイアウォールとともに、これを次の図に示します。

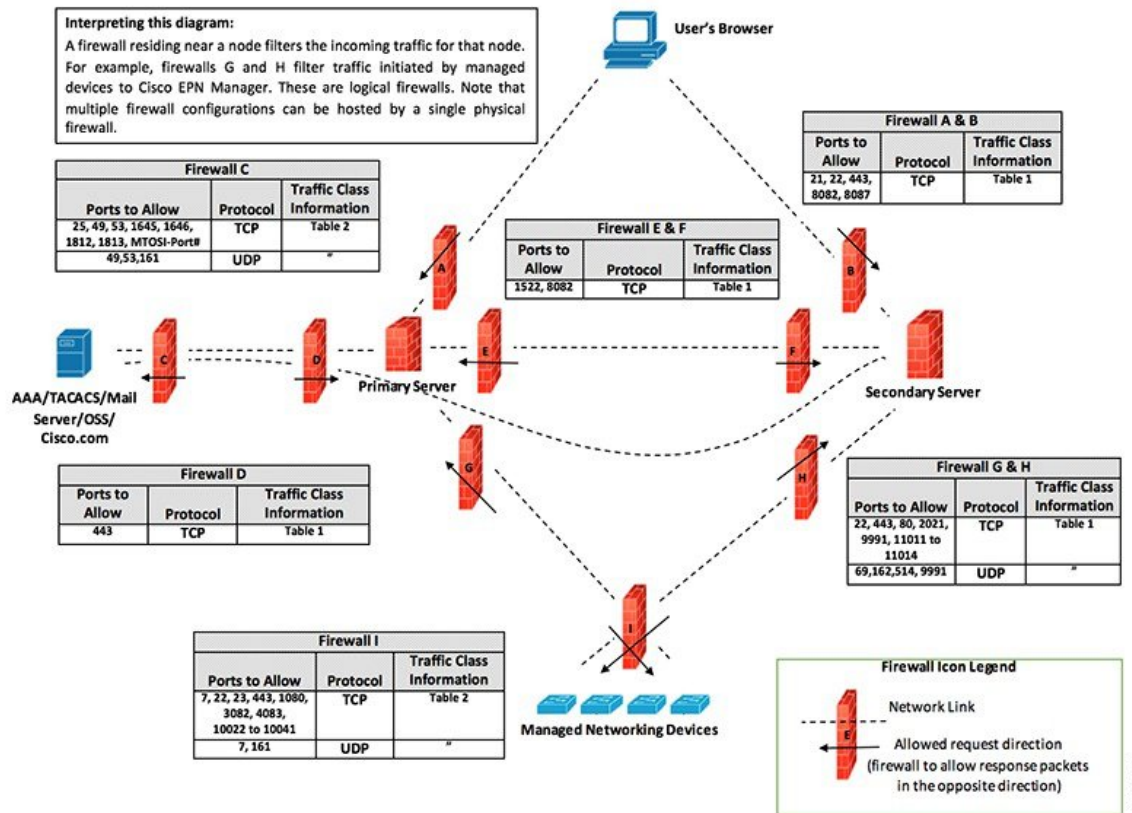


---

(注) これらのファイアウォールを実装することをお勧めしますが、必須ではありません。

---





411494

インストール環境によっては、ファイアウォールの設定をカスタマイズしてセキュリティをさらに向上させることが必要になります。一般的なポリシーとして、不要なポートやセキュでないポート（暗号化されたトラフィックを送信しないなど）をすべて無効にする必要があります。

## 組み込み型アプリケーションファイアウォールの設定

アプリケーションファイアウォールを設定するには、インストール環境で実行する必要のない Cisco EPN Manager の機能を無効にする必要があります。これにより、ファイアウォール内の対応するリスニングポートが自動的にシャットダウンされます。

**ステップ 1** 現在有効になっているポートを識別します。

- 外部に公開される展開で使用するポートのリストを表示するには、Cisco EPN Manager CLI 管理者ユーザとしてログインし、**show security-status** コマンドを実行します。
- 組み込みファイアウォールによってブロックされているものも含め、OS レベルで開いているすべてのリスニングポートのリストを表示するには、Linux CLI 管理者ユーザとしてログインし、**netstat -aln** コマンドを実行します。

**ステップ 2** ガイダンスについては表 1: 組み込みのファイアウォールを介した開いているポートのリスニング (6 ページ) を使用して、これらのポートの中で Cisco EPN Manager の通常の機能を中断させることなく安全に無効にできるものを特定します。

次の点に注意してください。

- Cisco EPN Manager は、内部操作に一部のリスニング ポートを使用します。これらのポートは、組み込みファイアウォールの背後に隠されたままになります。
- 表 1: 組み込みのファイアウォールを介した開いているポートのリスニング (6 ページ) に示す手順のみを使用してポートを有効または無効にする必要があります。

## 外部ネットワーク ファイアウォールの設定

組み込みファイアウォールに加えて、Cisco EPN Manager とそのピア システムが使用するリスニング ポートを対象とするトラフィックのみを許可するようにネットワーク ファイアウォールを展開することもできます。「インストールの強化」のトピックで示した図では、表 1: 組み込みのファイアウォールを介した開いているポートのリスニング (6 ページ) および表 2: 宛先ポートの使用元 Cisco EPN Manager (10 ページ) に示すポート情報を使用してファイアウォールルールをセットアップする方法を説明しています。この図を使用して、管理ネットワークに適したファイアウォール設定を決定します。

- トラフィッククラスを識別するには、表 1: 組み込みのファイアウォールを介した開いているポートのリスニング (6 ページ) の「使用方法」の列を参照してください。Cisco EPN Manager のインストール環境で使用されていないサービスが使用するポートを無効にすることをお勧めします。
- また、ネットワーク ファイアウォールで (ネットワーク デバイスまたはピア システムに接続するために) Cisco EPN Manager が発信トラフィックに使用する宛先ポートも有効にする必要があります。これらの宛先ポートとそれらの目的のリストについては、表 2: 宛先ポートの使用元 Cisco EPN Manager (10 ページ) を参照してください。

表 2: 宛先ポートの使用元 Cisco EPN Manager

ポート	プロトコル	使用する場合
7	TCP/UDP	ICMP を使用したエンドポイントの検出。
22	TCP	管理対象デバイスとの SSH 接続の開始。
23	TCP	Telnet を使用した管理対象デバイスとの通信。
25	TCP	SMTP サーバを使用した電子メールの送信。
49	TCP/UDP	TACACS を使用した Cisco EPN Manager ユーザの認証。

ポート	プロトコル	使用する場合
53	TCP/UDP	DNS サービスへの接続。
161	UDP	SNMP を使用したポーリング。
443	TCP	HTTPS を使用した Cisco NCS 2000 デバイスのイメージのアップロードおよびダウンロードと設定バックアップ/復元の実行。
1522	TCP	プライマリとセカンダリの HA サーバ間での通信（プライマリとセカンダリのサーバ間での Oracle データベースの同期に Oracle JDBC トラフィックを許可する）。
1080	TCP	Socket Secure (SOCKS) プロトコルを使用した Cisco オプティカル ネットワーキング システム (ONS) および Cisco NCS 2000 シリーズのデバイスとの通信。
1645、1646、および 1812、1813	UDP	RADIUS を使用した Cisco EPN Manager ユーザの認証。
3082	TCP	TL1 プロトコルを使用した Cisco ONS および Cisco NCS 2000 のデバイスとの通信。
4083	TCP	TL1 プロトコルを使用した Cisco ONS および Cisco NCS 2000 シリーズのデバイスとの通信。
8082	TCP	HTTPS を使用したプライマリとセカンダリの HA サーバ間の通信による相互の正常性の監視。
10022 ~ 10041	TCP	パッシブ FTP ファイル転送（デバイスの設定やレポートの取得など）。
MTOSI/RESTCONF TCP ポート番号	TCP	Cisco EPN Manager サーバに接続された NBI クライアントでリッスンする（このポートが NBI クライアントシステムによって設定された後、ポート番号を含む登録通知メッセージが Cisco EPN Manager サーバに送信される）。詳細については、 <a href="#">MTOSI または RESTCONF API のガイド</a> を参照してください。

## トラフィック暗号化のセットアップ

次のトラフィック グループを暗号化する必要があります。

- ノースバウンドトラフィック：このグループは、人間のユーザのブラウザからのクライアント/サーバトラフィックか、またはビジネス サポート システム/運用サポート システム (BSS/OSS) からの NBI トラフィックで構成されます。このトラフィックは HTTP 経由で

送信されるため、HTTPS (TLS で暗号化された HTTP) を実装する必要があります。HTTPS をセットアップする方法については、「[Web サーバを保護する HTTPS のセットアップ](#)」を参照してください。

- サウスバウンドトラフィック：このグループは、SNMP や HTTP などの幅広いプロトコルを使用して管理対象デバイスを照会または設定する管理トラフィックで構成されます。SSH や SNMPv3 などのプロトコルを使用して、このトラフィックを保護できます。このトラフィックを暗号化するために実行する必要がある設定手順の説明については、「[SNMPv3 を使用した Cisco EPN Manager とデバイス間の通信の強化](#)」を参照してください。
- ピア システム間の水平方向のトラフィック：このグループは、Cisco EPN Manager と、外部認証サーバ (TLS-EAP によって保護) や SMTP メールサーバ (TLS によって保護) などの他のさまざまなサポートシステム間のトラフィックで構成されます。保護する必要があるアプリケーションプロトコルに応じて、異なる暗号化プロトコルが使用されます。一部のアプリケーションプロトコルには、暗号化が組み込まれている場合もあります。
- HA 展開のプライマリ サーバとセカンダリ サーバ間の水平方向のトラフィック：このグループは、プライマリ モードとセカンダリ モードで実行している 2 台の Cisco EPN Manager サーバ間のトラフィックで構成されます。各サーバは、もう一方のサーバの正常性を監視し、HTTPS で保護されている接続を介してデータベースとその他のファイルのコンテンツの同期を保ちます。

## SNMPv3 を使用した Cisco EPN Manager とデバイス間の通信の強化

SNMPv3 は、SNMPv2 よりもセキュリティ機能が高いプロトコルです。デバイスが SNMPv3 をサポートしている場合は、SNMPv3 を使用して Cisco EPN Manager サーバと通信するようにデバイスを設定します。次の手順は、新しいデバイスを追加するときに SNMPv3 を指定する方法について説明しています。

デバイスの追加方法	SNMPv3 を指定する方法	詳細については、以下を参照してください。
1 つのデバイスの追加	[デバイスの追加 (Add Device)] ダイアログボックスで、[SNMP プロパティ (SNMP Properties)] ページに移動し、[バージョン (Versions)] ドロップダウンリストから [v3] を選択します。	<a href="#">手動によるデバイスの追加 (新規デバイスタイプまたはデバイスシリーズ)</a>
複数のデバイスの追加 (一括インポート)	CSV ファイルを編集するときは、次のように入力します。 <ul style="list-style-type: none"> <li>• [SNMP バージョン (SNMP Version)] 列で <b>3</b> を入力します。</li> <li>• [snmpv3_user_name]、[snmpv3_auth_type]、[snmpv3_auth_password]、[snmpv3_privacy_type]、および [snmpv3_privacy_password] の各列に適切な値を入力します。</li> </ul>	<a href="#">CSV ファイルを使用したデバイスのインポート</a>

デバイスの追加方法	SNMPv3 を指定する方法	詳細については、以下を参照してください。
ディスカバリを使用した複数のデバイスの追加	[ディスカバリ設定 (Discovery Settings) ]ダイアログボックスで、[クレデンシャルの設定 (Credential Settings) ]エリアに移動し、[SNMPv3 クレデンシャル (SNMPv3 Credentials) ]をクリックします。[+] 記号をクリックして、デバイス クレデンシャルを追加します。	カスタマイズされたディスカバリ設定でのディスカバリの実行

### 始める前に

SNMPv3 をサポートするネットワーク デバイスで、(HMAC-SHA-96 などの適切なセキュリティ アルゴリズムを使用して) SNMPv3 が有効になっていることを確認します。

## CLI を使用した外部認証の設定

ユーザアカウントとパスワードを管理するには、RADIUS や TACACS+ などのセキュアな認証プロトコルで稼働する専用のリモート認証サーバを使用することを推奨します。以下の手順に従って認証を設定することに加えて、外部認証ベンダーに連絡して、その他のセキュリティ強化案を問い合わせてください。



- (注) ローカル ユーザ認証を使用することにした場合は、デフォルトのパスワードポリシーを確認し、強化する必要があるかどうかを判断してください。ローカル認証のためのグローバルパスワードポリシーの設定を参照してください。

外部 AAA サーバを使用してユーザを認証するように Cisco EPN Manager を設定します。サーバを設定は、Web GUI を使用しても、コマンドラインインターフェイス (CLI) を使用しても行えます。リモート ユーザ認証を GUI で設定する場合は、外部認証の設定を参照してください。

CLI を使用して外部認証を設定するには、次の手順に従います。EPNM は CLI を介した TACACS+ の設定のみをサポート

**ステップ 1** Cisco EPN Manager サーバとの SSH セッションの確立の説明に従って、コマンドラインを使用して、Cisco EPN Manager にログインします。

**ステップ 2** コンフィギュレーション モードを開始します。

**ステップ 3** 次のコマンドを入力して外部認証 TACACS+ サーバをセットアップします。

```
aaa authentication tacacs+ server tacacsIP key plain shared-secret
```

ここで、

- *tacacsIP* はアクティブな TACACS+ サーバの IP アドレスです。
- *shared-secret* はアクティブな TACACS+ サーバのプレーンテキストの共有秘密です。

**ステップ 4** 次のコマンドを入力して、管理者権限を持つユーザを作成します。このユーザは、前のステップで指定したサーバによって認証されます。

```
username username password remote role admin [email emailID]
```

ここで、

- *username* はユーザ ID の名前です。
- *password* はユーザのプレーンテキストのパスワードです。
- *emailID* はユーザのメールアドレスです（オプション）。

## ブルートフォース パスワード攻撃に対する SSH の強化

パスワードベースの SSH 認証はブルートフォース攻撃に対して脆弱であるため、Cisco EPN Manager のインストール後に、承認されている公開キーのタイプ（PubkeyAcceptedKeyTypes）のいずれかに切り替えることをお勧めします。Cisco EPN Manager 3.1 で承認されている公開キーのタイプ（PubkeyAcceptedKeyTypes）のリストは次のとおりです。

- `ecdsa-sha2-nistp256-cert-v01@openssh.com`
- `ecdsa-sha2-nistp384-cert-v01@openssh.com`
- `ecdsa-sha2-nistp521-cert-v01@openssh.com`
- `ssh-ed25519-cert-v01@openssh.com`
- `ssh-rsa-cert-v01@openssh.com`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`
- `ssh-ed25519`

切り替えるには、次の手順を実行します。

**ステップ 1** Linux CLI 管理者ユーザとしてログインします。

- a) Cisco EPN Manager サーバで SSH セッションを開始して、Cisco EPN Manager CLI 管理者ユーザとしてログインします。
- b) `shell` コマンドを実行します。
- c) シェルアクセス パスワードを入力します。

**ステップ 2** 現在のユーザを確認します。

```
# whoami
```

結果の出力は、Linux ルートユーザではなく、Linux 管理者ユーザであることを示す必要があります。

**ステップ 3** Cisco EPN Manager 管理者ユーザの場合は、承認されている公開キータイプ (PubkeyAcceptedKeyTypes) のいずれかを使用し、2048 ビット以上の強度を持つツール (puTTYgen など) を使用してキーペアと SSH 文字列を作成します。

たとえば、次のように ed25519 を使用してキーを生成します。

```
$ ssh-keygen -t ed25519 -N ""
```

SSH 文字列は次のようになります。

```
ssh-ed25519 AAAAC3Nza... .....root@localhost.localdomain
```

**ヒント** 秘密キーをファイルに保存します。できれば、パスフレーズを使用して暗号化された形式で保存してください。また、パスフレーズを手元に置いてください。

**ステップ 4** authorized\_keys ファイルを作成し、適切なアクセス権限を Cisco EPN Manager 管理者ユーザに割り当てます。

- a) 管理者ユーザのホームディレクトリで、.ssh ディレクトリを作成し、このディレクトリの読み取り、書き込み、および実行の権限を管理者ユーザのみに割り当てます。

```
# cd ~
# mkdir .ssh
# chmod 700 ~/.ssh
```

- b) 承認されたキーファイルを作成します。

```
# cd .ssh
# vi authorized_keys
```

- c) ステップ 3 で作成した SSH 文字列を authorized\_keys ファイルにコピーして貼り付け、ファイルを保存します。

- d) authorized\_keys ファイルの読み取り、書き込み、および実行の権限を管理者ユーザのみに割り当てます。

```
# chmod go= ~/.ssh/authorized_keys
# chmod u=rwx ~/.ssh/authorized_keys
```

- e) authorized\_keys ファイルに適切なアクセス権を割り当てたことを確認します。

```
# ls -al
```

結果の出力は次のようになります。

```
total 6
drwx-----. 2 admin gadmin 1024 May 10 00:25 .
drwx-----. 6 admin gadmin 1024 May 10 00:24 .
-rwx-----. 1 admin gadmin 398 May 10 00:25 authorized_keys
```

この例では、Linux 管理者ユーザは admin という名前です

**ステップ 5** bash シェルのルートユーザに切り替えます。

```
# sudo -i
```

**ステップ 6** sshd\_config ファイルを更新します。

- a) /etc/ssh ディレクトリにある sshd\_config ファイルの現在のバージョンと元のバージョンをコピーします。

```
# cp /etc/ssh/sshd_config /etc/ssh/sshd_config.orig
```

- b) vi エディタに `sshd_config` ファイルを開きます。

```
# vi /etc/ssh/sshd_config
```

- c) 次のキーと値のペアを入力します。

```
Protocol 2
MaxAuthTries 3
PasswordAuthentication no
PermitRootLogin no
AuthenticationMethods publickey
PubkeyAuthentication yes
```

**重要** デフォルトの `sshd_config` ファイルでは、これらのキーと値のペアの一部が既に指定されていることがあります。この場合は、次のいずれかを行います。

- 上記の値と一致しない値を変更します。
- 既存のキーと値のペアをコメントアウトし、新しい行に必要なエントリを指定します。

こうすることで、キーと値のペアの競合や重複を防ぐことができます。

- d) ファイルを保存します。

**ステップ 7** `sshd` をリロードします。

```
# systemctl reload sshd.service
```

**注意** `sshd` は再起動しないでください。前述の設定手順のいずれかが適切に完了せず、`sshd` を再起動した場合は、SSH にアクセスできなくなります。現在の SSH セッションは維持されるため、`sshd` をリロードする方がはるかに安全です（必要な修正を行えるようにします）。

SSH 認証の構成が完了しました。設定が成功したことを確認するには、既存の SSH セッションを開いたままにして（何かを修正する必要がある場合に備えて）、この手順のステップ 3 で作成した秘密キーとパスワードを使用して新しい SSH セッションを開きます。

## NTP の強化

Network Time Protocol (NTP) は、サーバの日付と時刻の更新を認証します。NTP での時刻同期を実行するために、Cisco EPN Manager サーバを設定することをお勧めします。ネットワーク全体の NTP 同期の管理で障害が発生した場合、異常な結果が発生する可能性があります。ネットワーク時刻精度の管理は組織のネットワークアーキテクチャを含む広範囲の問題であり、このガイドの範囲外です。このトピックの詳細については、シスコホワイトペーパー『[Network Time Protocol: Best Practices](#)』などを参照してください。

次の点に注意してください。

- NTP を使用すると、セキュリティ侵害に関連する障害が発生する可能性があるため、NTP バージョン 4 (NTPv4) を使用して Cisco EPN Manager サーバの NTP 機能を強化する必要があります。また、Cisco EPN Manager は NTPv4 には NTPv3 との後方互換性があるため、NTPv3 もサポートしています。



- Cisco EPN Manager には最大 5 台の NTP サーバを設定できます。

## Cisco EPN Manager サーバでの NTP のセットアップ

Network Time Protocol (NTP) を使用して、NTP サーバを使用するサーバとネットワーク デバイス上のクロックを同期するには、まず Cisco EPN Manager 上に NTP をセットアップする必要があります。その実行方法については、[サーバでの NTP の設定](#) を参照してください。

### 認証された NTP の更新の有効化

次の手順を実行し、認証された NTP の更新をセットアップします。

**ステップ 1** [Cisco EPN Manager サーバとの SSH セッションの確立](#)の説明に従って、コマンドラインを使用して、Cisco EPN Manager にログインします。

**ステップ 2** コンフィギュレーション モードを開始します。

**ステップ 3** 次のコマンドを入力して外部 NTPv4 サーバをセットアップします。

```
ntp server serverIP userID plain password
```

ここで、

- *serverIP* は、使用する認証 NTPv4 サーバの IP アドレスです。
- *userID* は、NTPv4 サーバの MD5 キー ID です。
- *password* は NTPv4 サーバに対応する md5 プレーン テキスト パスワードです。

次に例を示します。

```
ntp server 209.165.202.128 20 plain myPass123
```

**ステップ 4** 次のテストを実行して、NTP 認証が正しく動作していることを確認します。

a) NTP 更新の詳細を確認します。

```
show run
```

b) NTP 同期の詳細を確認します。

```
show ntp
```

## NFS ベースの外部ストレージ サーバの設定

NFS サーバは、特にデータ バックアップの場合、Cisco EPN Manager のインストールで外部ストレージとして使用できます。NFS には組み込みのセキュリティがないので、NFS サーバをセキュアにするために次のセキュリティ対策をできる限り多く実装する必要があります。

- NFS サーバの前にファイアウォールを設定します。実質的にはこれを行うには、NFS がさまざまな設定ファイルで使用するポートを固定し、ファイアウォールの設定でこれらのポートを指定します。
- ポート マッパーを使用します。NFS サーバで、特定の IP アドレスを含む NFS トランザクションのみ許可します。
- 感染した DNS 経由の攻撃を防ぐには、NFS を構成するときに（ドメイン名ではなく）IP アドレスのみ指定します。
- フォルダのエクスポートを設定する際に、`/etc/exports` ファイルで `[root_squash]` オプションを使用します。
- `/etc/exports` ファイルを設定する際に、`[セキュア (secure)]` オプションを使用します。
- バックアップ ステージングとストレージフォルダを設定する際に、`nosuid` オプションと `noexec mount` オプションを使用します。



(注) ステージング フォルダを設定することは必須ではありません。

- ストレージフォルダ（およびオプションのステージング フォルダ）に対して、ファイルアクセス許可値 `[755]`（すべてのユーザに読み取りおよび書き込み特権を付与）を設定し、`userid[65534]`（システム権限を持っていないユーザ `[nobody]`）を所有者として設定します。
- SSH または SSL/TLS のいずれかを介して NFS トラフィックをトンネリングします。SSH の場合、ユーザ認証ではなく RSA キーベースの認証を使用します。

NFS ベースのストレージの安全性のためには、これらの対策の 1 つのみに頼らないください。最善策は、状況に合わせて最適な対策の組み合わせを実装することです。また、このリストは網羅的なものではないことに注意してください。ストレージを強化するときは、高レベルの信頼を達成するために、事前に Linux システム管理者およびセキュリティ専門家と状況について相談することをお勧めします。

## CSDL プロセス

Cisco EPN Manager の開発は、シスコセキュア開発ライフサイクル（CSDL）プロセスに準拠しています。これは、製品とインストールのセキュリティを向上させるために、開発から展開までの期間全体を対象としています。Cisco EPN Manager の製品設計は、特定の基準に対するセキュリティの観点からレビューされ、製品はセキュリティツールとテスト方法を使用してテストされます。さらに、Cisco EPN Manager は外部のセキュリティ専門家や侵入テストの担当

者によってレビューされます。（Cisco EPN Manager の更新のライフサイクルの一般としての）セキュリティ修正の展開方法の説明については、「[シスコのセキュリティ問題解決プロセス](#)」

## シスコのセキュリティ問題解決プロセス

欠陥と脆弱性には、顧客が見つけたものとシスコが発見したものの2つのタイプがあります。Cisco EPN Manager についてシスコがそれらにどのように対処しているかについて説明します。

### 顧客が見つけた欠陥と脆弱性

1. Cisco Technical Assistance Center (TAC) を使用して顧客がサービス要求を行った後、Cisco TAC は Cisco Defect and Enhancement Tracking System (CDETS) 障害レポートを開くことができるサポートチーム（問題に応じて異なる）と共にケースを開きます。
2. シスコは欠陥を評価し、その欠陥が Cisco EPN Manager にセキュリティ上のリスクをもたらすかどうかを判断します。この欠陥がセキュリティにリスクをもたらす場合、シスコは脆弱性として分類します。それ以外の場合、シスコは欠陥をソフトウェアの通常の欠陥として扱います。
3. シスコでは、次のいずれかを実行します。
  - セキュリティの脆弱性については、シスコは Cisco Product Security Incident Response Team (PSIRT) に報告し、Cisco PSIRT ガイドラインに準拠した修正プログラムを開発して Cisco PSIRT がクライアントへの脆弱性の開示とパッチの配信の両方を処理できるようにします。
  - 欠陥の場合、シスコはその重大度を判断し、修正プログラムのリリースをスケジュールします。

### シスコが発見した欠陥と脆弱性

Cisco EPN Manager のバージョンの販売終了日から1年間、シスコは TACS または Cisco.com Web サイトを通じて報告された重大なバグとセキュリティ上の脆弱性に対するバグ修正、メンテナンス リリース、対応策、またはパッチを提供します。

