ベスト プラクティス：Cisco EPN Manager のセキュリティ強化

セキュリティを強化するには、次のコンポーネントがセキュリティ メカニズムを最適化できるように調整する必要があります。

- Cisco EPN Manager Web サーバ
- Cisco EPN Manager サーバ
- Cisco EPN Manager ストレージ システム（ローカルまたは外部）
- Cisco EPN Manager とデバイス間の通信
- ユーザ認証システム（ローカルまたは外部）
- Network Time Protocol（NTP）を使用する時刻同期システム

この付録ではまず、管理者が知っておくべきいくつかの主要なセキュリティの概念を紹介します。次に、Cisco EPN Manager のセキュリティを最適化するために実行する必要がある特定のタスクについて説明します。

主要なセキュリティ概念

Cisco EPN Manager 製品のセキュリティの最適化を目指す管理者は、次のセキュリティ概念をよく理解しておく必要があります。

HTTPS

Hypertext Transfer Protocol Secure（HTTPS）では、チャネルを介して送信されるデータの暗号化に、セキュア ソケット レイヤ（SSL） またはその後続の標準規格である Transport Layer Security（TLS）が使用されます。SSL で複数の脆弱性が見つかったため、Cisco EPN Manager では現在 TLS のみがサポートされています。

（注） TLS は大まかに SSL と呼ばれることが多いため、本ガイドでもこの表記に従います。

SSL は、プライバシー、認証、およびデータ整合性を組み合わせることで、クライアントとサーバの間のデータ転送を保護します。これらのセキュリティ メカニズムを有効にするために、SSL は証明書、秘密キー/公開キー交換ペア、および Diffie-Hellman 鍵共有パラメータを使用します。

SSL 証明書

SSL 証明書と秘密キー/公開キー ペアは、ユーザ認証および通信パートナーの ID 検証に使われるデジタル ID の一種です。VeriSign や Thawte などの認証局（CA）は、エンティティ（サーバまたはクライアント）を識別するための証明書を発行します。クライアントまたはサーバ証明書には、発行認証局の名前とデジタル署名、シリアル番号、証明書が発行されたクライアントまたはサーバの名前、公開キー、および証明書の有効期限が含まれます。CA は、1 つ以上の署名証明書を使用して SSL 証明書を作成します。各署名証明書には、CA 署名の作成に使用される照合秘密キーがあります。CA は署名付き証明書（公開キーが埋め込まている）を簡単に入手できるようにしているため、誰でもその証明書を使用して、SSL 証明書が実際に特定の CA によって署名されたことを確認できます。

一般に、ハイ アベイラビリティ（HA）と非 HA の両方の環境で証明書を設定するには、次の手順が必要です。

1. サーバの ID 証明書を生成する。
2. サーバに ID 証明書をインストールする。
3. 対応するルート証明書をクライアントまたはブラウザにインストールする。

実行する必要がある具体的なタスクは、ご利用の環境によって異なります。

次の点に注意してください。

- サーバの開始/停止シーケンシングは、HA 環境で慎重に行う必要があります。
- 仮想 IP アドレスが設定されている非 HA 環境では、より複雑な証明書要求プロセスを完了する必要があります。

1 方向 SSL 認証

これは、クライアントが適切なサーバ（中間サーバではなく）に接続していることを保証する必要がある場合に使用される認証方法で、オンラインバンキングの Web サイトなどのパブリック リソースに適しています。認証は、クライアントがサーバ上のリソースへのアクセスを要求したときに開始されます。リソースが存在するサーバは、その ID を証明するために、サーバ証明書（別名 SSL 証明書）をクライアントに送信します。クライアントは受信したサーバ証明書を、クライアントまたはブラウザにインストールする必要がある別の信頼できるオブジェクト（サーバルート証明書）と照合して検証します。サーバの検証後、暗号化された（つまりセキュアな）通信チャネルが確立されます。ここで、Cisco EPN Manager サーバは HTML フォームへの有効なユーザ名とパスワードの入力を求めます。SSL 接続が確立された後にユーザ クレデンシャルを入力すると、未認証の第三者による傍受を防ぐことができます。最終的に、ユーザ名とパスワードが受け入れられた後、サーバ上に存在するリソースへのアクセスが許可されます。

（注） クライアントは複数のサーバとやり取りするために、複数のサーバ証明書を格納する必要がある場合があります。

クライアントにルート証明書をインストールする必要があるかどうかを判断するには、ブラウザの URL フィールドでロック アイコンを探します。通常このアイコンが表示される場合は、必要なルート証明書がすでにインストール済みであることを示します。多くの場合、これはより大きいいずれかの認証局（CA）によって署名されたサーバ証明書に該当します。一般的なブラウザではこれらの CA からのルート証明書が含まれているからです。

クライアントがサーバ証明書に署名した CA を認識しない場合は、接続がセキュリティで保護されていないことを意味します。これは必ずしも大きな問題ではなく、接続するサーバの ID が検証されていないことを示しているだけです。1 つは必要なルート証明書をクライアントまたはブラウザにインストールできます。ブラウザの URL フィールドにロック アイコンが表示された場合は、証明書が正常にインストールされたことを意味します。

Cisco EPN Manager セキュリティ強化の概要

Cisco EPN Manager のセキュリティを強化するには、次のタスクを完了する必要があります。

（インストール時）

- HTTPS の設定、スタンドアロン サーバおよび HA 環境の 1 方向 SSL 認証のセットアップ
- 非セキュア ポートと未使用ポートのシャットダウン
- ネットワーク ファイアウォールの設定
- 外部認証の設定

（インストール後）

- 変更（新しいホスト名または IP アドレスの設定など）に応じた証明書の更新
- 必要に応じた Cisco EPN Manager サーバの強化

主な情報源として、シスコの担当者が各導入環境に固有のサーバ強化ガイダンスをご提供しますが、以下の手順に従って Cisco EPN Manager を保護することもできます。

強化手順	強化手順の対象：
HTTPS を使用した Web サーバ接続の保護 （5 ページ）	Cisco EPN Manager Web サーバ
Web クライアントの証明書ベースの認証の設定 （5 ページ）	
サーバでの OCSP の設定と管理 （7 ページ）	
非セキュアなポートおよびサービスの無効化 （9 ページ）	Cisco EPN Manager サーバ
SNMPv3 を使用した Cisco EPN Manager とデバイス間の通信の強化	
CLI を使用した外部認証の設定	
日常業務に不要なアカウントの無効化 （10 ページ）	
NTP の強化	
Cisco EPN Manager ストレージの強化 （10 ページ）	Cisco EPN Manager ストレージ システム（ローカルまたは外部）

Cisco EPN Manager Web サーバの強化

Cisco EPN Manager Web サーバを強化するには、以下を実行します。

HTTPS を使用した Web サーバ接続の保護

Cisco EPN Manager Web サーバは、HTTP の代わりに HTTPS を使用するように設定されている必要があります。これにより、Cisco EPN Manager Web サーバに接続するシステムが保護され、いずれかのクライアントが Web サーバやその他の参加システムに間接的に侵入する可能性が回避されます。HTTPS では、Web サーバ内の認証局（CA）証明書と、適切な SSL メカニズムを使用することが必要です。セットアップ方法の詳細は。

Web クライアントの証明書ベースの認証の設定

セキュリティを強化するには、Cisco EPN Manager サーバでクライアント認証に証明書ベースの認証を使用する必要があります。この認証方式では、Cisco EPN Manager は最初にクライアントに関連付けられている証明書を検証してクライアントが正当であることを確認し、次にユーザ名とパスワードを検証します。このメカニズムにより、未承認のマシン（証明書が存在しないマシン）は Web サーバに接続できません。Cisco EPN Manager はオンライン証明書ステータス プロトコル（OCSP）を使用してこの機能を実行します。

（注） このトピックで説明する証明書は、クライアントを一意に識別します。これは、HTTPS 操作の設定に使用された *Web* サーバの証明書とは異なります。この手順は、Web サーバ証明書の CER ファイルの生成手順に似ていますが、完全に同一というわけではありません。場合によっては、その他のツール（OpenSSL など）を使用する必要があります。また、CA 証明書ファイルの生成方法は複数あります。サポートが必要な場合は、シスコ担当者にお問い合わせください。

証明書ベースの認証を設定するには、次の手順を実行します。

ステップ 1 CA を使用してクライアント証明書ファイルを生成します。これには、通常次の手順が含まれます。

a) 公開キーを生成します。
b) 公開キーを含む CSR ファイルを生成します。
c) 証明書ファイルを取得するため、CSR ファイルを CA に送信します。
d) 複数のファイルを受信する場合は、ファイルを連結して 1 つの CER/PEM ファイルを作成しないでください。代わりに次のようにします。

- クライアント マシンで保持するためにクライアント証明書ファイルをアプリケーション ユーザに配布します。
- ルート CA 証明書とすべての中間 CA 証明書を維持します。これらの証明書は、ステップ 4 でサーバにインポートします。

ベスト プラクティス：Cisco EPN Manager のセキュリティ強化

（注） ルート CA サーバと中間 CA サーバからこれらの証明書を取得する必要があります。信頼できないソースから受信したファイルは使用しないでください。

（注） クライアント CA 証明書を Web サーバにインポートしないでください。このファイルは、クライアント マシン（挿入可能なカード、ハードウェアまたはソフトウェア トークン デバイスなど）で維持します。クライアント ブラウザが Cisco EPN Manager Web サーバへの接続を試行すると、Web サーバはクライアント ブラウザに対し、クライアント証明書を要求するよう指示します。ユーザはクライアント証明書を提供し、ユーザ名とパスワードを入力する必要があります。

ステップ 2 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 サーバにログインします。コンフィギュレーション モードを開始しないでください。

ステップ 3 ルート CA 証明書ファイルと中間 CA 証明書ファイルを、1 つずつ Cisco EPN Manager Web サーバにインポートします。

a) このコマンドでルート CA 証明書ファイルをインポートします。

```
ncs key importcacert aliasName rootCACertFile repository repoName
```

ここで、

- *aliasName* は CA 証明書に対して指定されている短い名前です。
- *rootCACertFile* はルート CA 証明書ファイル名です。
- *repoName* は証明書ファイルが格納されている Cisco EPN Manager リポジトリの場所です。

（注） このコマンドは、サーバ証明書を適用するコマンドとは大きく異なることに注意してください。

b) このコマンドで中間 CA 証明書ファイルをインポートします。

```
ncs key importcacert aliasName intermediateCACertFile repository repoName
```

ここで、

- *intermediateCACertFile* は中間 CA 証明書ファイル名です。

ステップ 4 サーバを再起動します。展開環境がハイ アベイラビリティに対応して設定されているかどうかに応じて、実行する手順は異なります。

ハイ アベイラビリティを使用しない展開環境では、変更を適用するため Cisco EPN Manager サーバを再起動します。

```
ncs stop
ncs start
```

ハイ アベイラビリティを使用する展開環境では、次の手順に従い、サーバを正しい順序で再起動します。

a) セカンダリ サーバで Cisco EPN Manager CLI admin ユーザとしてログインし、サーバを停止します。

```
ncs stop
```

（注） ステップ 5（e）まではセカンダリ サーバを再起動しないでください。

b) セカンダリ サーバが停止していることを確認します。
c) プライマリ サーバで Cisco EPN Manager CLI admin ユーザとしてログインし、サーバを停止します。

```
ncs stop
```

（注） ステップ 5（f）まではプライマリ サーバを再起動しないでください。

d) プライマリ サーバが停止していることを確認します。
e) セカンダリ サーバで、次のコマンドを実行します。

1. **ncs start** コマンドを実行してサーバを再起動します。
2. セカンダリ サーバが再起動したことを確認します。
3. **ncs status** コマンドを実行して、ヘルス モニタ プロセスが実行中であることを確認します。
4. **ncs ha status** コマンドを実行し、セカンダリ サーバの HA ステータスが [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] であることを確認します。

f) プライマリ サーバで、次のコマンドを実行します。

1. **ncs start** コマンドを実行してサーバを再起動します。
2. プライマリ サーバが再起動したことを確認します。
3. **ncs status** コマンドを実行して、ヘルス モニタ プロセスとその他のプロセスが再開していることを確認します。

プライマリ サーバですべてのプロセスが稼働したら、セカンダリ サーバとプライマリ サーバの間で HA 登録が自動的にトリガーされます（また、登録されている電子メール アドレスに電子メールが送信されます）。自動 HA 登録は通常、数分で完了します。

g) プライマリ サーバとセカンダリ サーバで **ncs ha status** コマンドを実行し、両方のサーバの HA ステータスを確認します。次が表示されます。

- プライマリ サーバの状態は [プライマリ アクティブ（Primary Active）] です。
- セカンダリ サーバの状態は [セカンダリ同期（Secondary Syncing）] です。

サーバでの OCSP の設定と管理

Online Certificate Status Protocol（OCSP）は、OCSP レスポンダを使用して Web クライアントの証明書ベース認証を可能にします。通常、OCSP レスポンダの URL は証明書の Authority Information Access（AIA）から読み取られます。フェールオーバー メカニズムとして、Cisco EPN Manager サーバで OCSP レスポンダの URL を設定します。

サーバでのカスタム OCSP レスポンダの設定

Cisco EPN Manager サーバでカスタム OCSP レスポンダの URL を設定する手順は次のとおりです。

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 サーバにログインします。コンフィギュレーション モードを開始しないでください。

ステップ 2 次のコマンドを入力して、クライアント証明書認証を有効化します。

```
ocsp responder custom enable
```

ステップ 3 次のコマンドを入力して、カスタム OCSP レスポンダの URL を設定します。

```
ocsp responder set url responderNumber responderURL
```

ここで、

- *responderNumber* は、定義する OCSP レスポンダの番号です（1、2 など）。
- *responderURL* は、クライアントの CA 証明書から取得される OCSP レスポンダ の URL です。

サーバからのカスタム OCSP レスポンダの削除

Cisco EPN Manager サーバで定義されている既存のカスタム OCSP レスポンダを削除する手順は次のとおりです。

ステップ 1 **show security-status** コマンドを実行して、サーバに現在設定されているカスタム OCSP レスポンダを表示し、削除するレスポンダの番号を特定します。

ステップ 2 次のコマンドで OCSP レスポンダをサーバから削除します。

```
ocsp responder clear url responderNumber
```

Cisco EPN Manager サーバの強化

Cisco EPN Manager サーバを強化するには、次の手順に従ってください。

1. 非セキュアなポートおよびサービスの無効化 （9 ページ）
2. SNMPv3 を使用した Cisco EPN Manager とデバイス間の通信の強化
3. CLI を使用した外部認証の設定
4. 日常業務に不要なアカウントの無効化 （10 ページ）
5. NTP の強化

非セキュアなポートおよびサービスの無効化

一般的なポリシーとして、不要なポートや非セキュアなポートをすべて削除する必要があります。まず、どのポートが有効になっているかを確認した後、ご使用の導入環境で Cisco EPN Manager の通常の機能を妨げることなく安全に無効化できるポートを判別する必要があります。これを行うには、開いているポートを一覧表示して、安全に無効化できるポートの一覧と比較します。

安全に無効化できるポートの一覧は、『Cisco Evolved Programmable Network Manager Installation Guide』、（Cisco EPN Manager で使用されるポートとサービスを示す）から取得できます。

有効になっているポートを確認するには、次の手順に従います。

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い、コマンドラインを使用して Cisco EPN Manager にログインします。コンフィギュレーション モードを開始しないでください。

ステップ 2 show security-status コマンドは、現在開いている（有効化されている）サーバの TCP/UDP ポート、システムで使用している他のサービスのステータス、およびその他のセキュリティ関連の設定情報を表示します。次のような出力が表示されます。

```
show security-status
Open TCP Ports        22 443 1522 8082
Open UDP Ports        162 514 9991
FIPS Mode             enabled
TFTP Service          disabled
FTP Service           disabled
JMS port (61617)      disabled
Root Access           disabled
Client Auth           enabled
OCSP Responder1       http://209.165.200.224/ocsp
OCSP Responder2       http://209.165.202.128/ocsp
```

ステップ 3 『Cisco Evolved Programmable Network Manager Installation Guide』にある、Cisco EPN Manager で使用されるポートの一覧表を調べて、その表にご使用のポートが示されているかどうかを確認します。この表を参考にすると、どのサービスがポートを使用しているか、およびどのサービスが不要で、安全に無効化できるかを判別できます。この場合の「安全」とは、製品に悪影響を及ぼさずにポートを安全に無効化できることを意味します。

（注） ポートまたはサービスを無効化する必要があるかどうかが不明の場合は、Cisco の担当者にお問い合わせください。

ステップ 4 Cisco EPN Manager GUI を使用して、非セキュア ポートを無効化します。

この例では、非セキュアなプロトコルとして無効化すべき FTP と TFTP を無効化します（代わりに SFTP または SCP を使用します）。TFTP および FTP は通常、ネットワーク デバイスと Cisco EPN Manager の間でファームウェアやソフトウェアのイメージを転送するために使用されます。

a) 管理者権限を持つユーザ ID を使用して Cisco EPN Manager にログインします。
b) **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [サーバ（Server）]** を選択します。
c) [FTP] および [TFTP] の下で、[無効化（Disable）] を選択して [保存（Save）] をクリックします。
d) Cisco EPN Manager を再起動します。「Cisco EPN Manager の停止と再起動」を参照してください。

（注） ハイアベイラビリティ設定では、ハイアベイラビリティを設定する前に、セカンダリサーバでFTPサービスおよびTFTPサービスが無効になっていることを確認します。詳細については、サーバでの FTP/TFTP/SFTP サービスの有効化を参照してください。

ステップ 5 ネットワークにファイアウォールがある場合は、Cisco EPN Managerの動作に必要なトラフィックのみを許可するようにファイアウォールを設定してください。詳細については、『Cisco Evolved Programmable Network Manager Installation Guide』を参照してください（特に、Cisco EPN Managerで使用されるポートに関する情報と、推奨されるファイアウォール設定）。さらに支援が必要な場合は、Ciscoの担当者にお問い合わせください。

日常業務に不要なアカウントの無効化

Cisco EPN Manager Web GUI のルート ユーザは、ルート権限を持つ他の Web GUI ユーザを 1 人以上作成した後に無効化する必要があります。Web GUI ルート ユーザの無効化および有効化 を参照してください。

Cisco EPN Manager ストレージの強化

データベース、バックアップ サーバなど、Cisco EPN Manager のインストールに含めるすべてのストレージ要素を保護することをお勧めします。

内部ストレージまたは外部ストレージの強化の詳細については、シスコの担当者にお問い合わせください。外部ストレージの場合は、ストレージ ベンダーにもご連絡ください。

Cisco EPN Manager をアンインストールまたは削除する場合は、センシティブ データを含む可能性があるすべてのVM関連ファイルがデジタルで破棄（単に削除されるのではなく）されていることを確認してください。

NFS ベース ストレージの強化

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。

ベスト プラクティス：Cisco EPN Manager のセキュリティ強化

- /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] と [noexec] マウント 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 つのみに頼らないでください。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。

ベスト プラクティス：**Cisco EPN Manager** のセキュリティ強化