



## CHAPTER 4

# Cisco Unified オペレーティング システムのセキュリティ

- 「セキュリティを最適化するブラウザの設定」 (P.1)
- 「IPSEC ポリシーの管理方法」 (P.1)

## セキュリティを最適化するブラウザの設定

サーバから証明書をダウンロードするには、Internet Explorer のセキュリティ設定が正しく設定されている必要があります。

### 手順

- ステップ 1** Internet Explorer を起動します。
- ステップ 2** [ツール (Tools) ] > [インターネット オプション (Internet Options) ] を選択します。
- ステップ 3** [詳細設定 (Advanced) ] タブを選択します。
- ステップ 4** [詳細設定 (Advanced) ] タブの [セキュリティ (Security) ] セクションまでスクロールします。
- ステップ 5** 必要に応じて、[暗号化されたページをディスクに保存しない (Do not save encrypted pages to disk) ] をオフにします。
- ステップ 6** [OK] を選択します。

## IPSEC ポリシーの管理方法

- 「IPSec ポリシーの作成」 (P.2)
- 「既存の IPSec ポリシーの有効化または無効化」 (P.4)
- 「IPSec ポリシーの削除」 (P.4)



(注) IPsec は、Cisco Unified Presence のインストール中、クラスタのノード間で自動的に確立されません。

## IPSec ポリシーの作成

新しい IPSec ポリシーを設定できます。ただし、Cisco Unified Presence サーバのアップグレード中は IPSec ポリシーを作成しないでください。



**注意**

---

IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

---

### はじめる前に

[セキュリティ (Security)] メニューの項目にアクセスするには、管理者パスワードを使用して [Cisco Unified オペレーティング システムの管理 (Cisco Unified Operating System Administration)] に再サインインする必要があります。

### 手順

- 
- ステップ 1** [Cisco Unified オペレーティング システムの管理 (Cisco Unified Operating System Administration)] にサインインします。
  - ステップ 2** [セキュリティ (Security)] > [IPSEC 設定 (IPSEC Configuration)] を選択します。
  - ステップ 3** [新規追加 (Add New)] を選択します。

## ステップ 4 適切なフィールドに新しい値を入力します。

フィールド	説明
ポリシー グループ名 (Policy Group Name)	IPSec ポリシーが属するグループ名を指定します。
ポリシー名 (Policy Name)	IPSec ポリシーの名前を指定します。
認証方式 (Authentication Method)	[ 証明書 (Certificate) ] など、認証方法を指定します。
共有キー (Preshared Key)	[ 認証方式 (Authentication Method) ] フィールドで [ 事前共有キー (Pre-shared Key) ] を選択した場合は、事前共有キーを指定します。
ピア タイプ (Peer Type)	ピアのタイプが同じか異なるかを指定します。
証明書の名前 (Certificate Name)	認証に使用する証明書の名前を指定します。
接続先アドレス (Destination Address)	接続先の IP アドレスまたは FQDN を指定します。
接続先ポート (Destination Port)	接続先のポート番号を指定します。
ソース アドレス (Source Address)	ソースの IP アドレスまたは FQDN を指定します。
ソース ポート (Source Port)	ソースのポート番号を指定します。
モード (Mode)	[ トンネル (Tunnel) ] または [ 転送 (Transport) ] モードを指定します。
リモート ポート (Remote Port)	接続先で使用されるポート番号を指定します。
プロトコル (Protocol)	特定のプロトコルまたは [ すべて (Any) ] を指定します。 <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• すべて (Any)</li> </ul>
暗号化アルゴリズム (Encryption Algorithm)	リスト ボックスから暗号化アルゴリズムを選択します。選択肢は次のとおりです。 <ul style="list-style-type: none"> <li>• DES</li> <li>• 3DES</li> </ul>
ハッシュ アルゴリズム (Hash Algorithm)	ハッシュ アルゴリズムを指定します。 <ul style="list-style-type: none"> <li>• SHA1 : フェーズ 1 IKE ネゴシエーションで使用されるハッシュ アルゴリズム</li> <li>• MD5 : フェーズ 1 IKE ネゴシエーションで使用されるハッシュ アルゴリズム</li> </ul>
ESP アルゴリズム (ESP Algorithm)	リスト ボックスから、ESP アルゴリズムを選択します。選択肢は次のとおりです。 <ul style="list-style-type: none"> <li>• NULL_ENC</li> <li>• DES</li> <li>• 3DES</li> <li>• BLOWFISH</li> <li>• RIJNDAEL</li> </ul>

フィールド	説明
フェーズ 1 のライフタイム (Phase One Life Time)	フェーズ 1 の IKE ネゴシエーションのライフタイムを秒単位で指定します。
フェーズ 1 の DH (Phase One DH)	リスト ボックスからフェーズ 1 の DH 値を選択します。選択肢には、2、1、5、14、16、17、および 18 があります。
フェーズ 2 のライフタイム (Phase Two Life Time)	フェーズ 2 の IKE ネゴシエーションのライフタイムを秒単位で指定します。
フェーズ 2 の DH (Phase Two DH)	リスト ボックスからフェーズ 2 の DH 値を選択します。選択肢には、2、1、5、14、16、17、および 18 があります。
ポリシーの有効化 (Enable Policy)	IPSec ポリシーを有効にするにはオンにします。

### 次の作業

「既存の IPSec ポリシーの有効化または無効化」(P.4)

## 既存の IPSec ポリシーの有効化または無効化

既存の IPSec ポリシーを有効または無効にすることができます。ただし、Cisco Unified Presence サーバのアップグレード中は IPSec ポリシーの作成、有効化または無効化を行わないでください。



**注意**

IPSec はシステムのパフォーマンスに影響します (特に暗号化した場合)。

### はじめる前に

「IPSec ポリシーの作成」(P.2) の手順を実行します。

### 手順

- ステップ 1** [Cisco Unified オペレーティング システムの管理 (Cisco Unified Operating System Administration) ] にサインインします。
- ステップ 2** [IPSEC 設定 (IPSEC Configuration) ] ウィンドウで、次のいずれかの操作を実行します。
  - a.** ポリシーを有効にする場合は、[ポリシーの有効化 (Enable Policy) ] をオンにします。
  - b.** ポリシーを無効にする場合は、[ポリシーの有効化 (Enable Policy) ] をオフにします。

## IPSec ポリシーの削除

1 つ以上の IPSec ポリシーを削除できます。ただし、Cisco Unified Presence サーバのアップグレード中は IPSec ポリシーを削除しないでください。



**注意**

IPSec はシステムのパフォーマンスに影響します (特に暗号化した場合)。

### はじめる前に

[セキュリティ (Security) ] メニューの項目にアクセスするには、管理者パスワードを使用して [Cisco Unified オペレーティング システムの管理 (Cisco Unified Operating System Administration) ] に再サインインする必要があります。

### 手順

- 
- ステップ 1** [Cisco Unified オペレーティング システムの管理 (Cisco Unified Operating System Administration) ] にサインインします。
- ステップ 2** [セキュリティ (Security) ] > [IPSEC 設定 (IPSEC Configuration) ] を選択します。
- ステップ 3** 削除するポリシーを選択します。
- ステップ 4** [削除 (Delete) ] を選択します。
-

