



# S/MIME セキュリティ サービス

この章は、次の項で構成されています。

- [S/MIME セキュリティ サービスの概要 \(1 ページ\)](#)
- [E メール セキュリティ アプライアンスでの S/MIME セキュリティサービス \(2 ページ\)](#)
- [S/MIME を使用した発信メッセージの署名、暗号化、または署名と暗号化 \(5 ページ\)](#)
- [S/MIME を使用した着信メッセージの検証、復号、または復号と検証 \(18 ページ\)](#)
- [S/MIME 証明書の要件 \(24 ページ\)](#)
- [公開キーの管理 \(26 ページ\)](#)

## S/MIME セキュリティ サービスの概要

Secure/Multipurpose Internet Mail Extensions (S/MIME) は、安全な検証済みの電子メールメッセージを送受信するための標準ベースの方式です。S/MIME では、公開/秘密キーのペアを使用してメッセージを暗号化または署名します。この方法により、

- メッセージが暗号化されている場合、メッセージ受信者のみが暗号化されたメッセージを開くことができます。
- メッセージが署名されている場合、メッセージ受信者は送信者のドメインのアイデンティティを検証して、転送中にメッセージが変更されていないことを確信できます。

S/MIME の詳細については、次の RFC を確認してください。

- RFC 5750 : Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Certificate Handling
- RFC 5751 : Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Message Specification
- RFC 3369 : Cryptographic Message Syntax

# Eメールセキュリティ アプライアンスでの S/MIME セキュリティサービス

組織では、すべてのエンドユーザが独自の証明書を所有していなくても、S/MIME を使用して安全に通信したいと考えています。このような組織に対してアプライアンスは、個々のユーザではなく組織を識別する証明書を使用して、ゲートウェイレベルで S/MIME セキュリティサービス（署名、暗号化、検証および復号）をサポートします。

アプライアンスは、Business-to-Business (B2B) および Business-to-Consumer (B2C) シナリオに次の S/MIME セキュリティサービスを提供します。

- S/MIME を使用したメッセージの署名、暗号化、または署名と暗号化 [S/MIME を使用した発信メッセージの署名、暗号化、または署名と暗号化 \(5 ページ\)](#) を参照してください。
- S/MIME を使用したメッセージの検証、復号、または復号と検証 [S/MIME を使用した着信メッセージの検証、復号、または復号と検証 \(18 ページ\)](#) を参照してください。

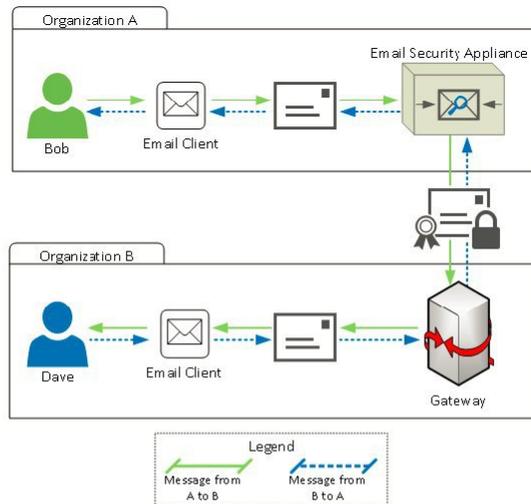
## 関連項目

- [S/MIME セキュリティ サービスのしくみについて \(2 ページ\)](#)

## S/MIME セキュリティ サービスのしくみについて

- シナリオ : [Business-to-Business \(B2B\) \(3 ページ\)](#)
- シナリオ : [Business-to-Consumer \(4 ページ\)](#)

## シナリオ : Business-to-Business (B2B)



企業 A と B は、両社の中でやり取りするすべてのメッセージを、S/MIME を使用して署名および暗号化したいと考えています。企業 A は、ゲートウェイレベルで S/MIME セキュリティ サービスを実行するように E メールセキュリティ アプライアンスを設定しています。企業 B は、ゲートウェイ レベルで S/MIME セキュリティ サービスを実行するようにサードパーティ アプリケーションを設定しています。



(注) 現在の例では、企業 B はサードパーティ アプリケーションを使用して S/MIME セキュリティ サービスを実行していると仮定します。実際には、これはゲートウェイレベルで S/MIME セキュリティ サービスを実行できる任意のアプリケーションまたはアプライアンス (E メールセキュリティ アプライアンスを含む) になります。

#### 企業 A が企業 B にメッセージを送信 :

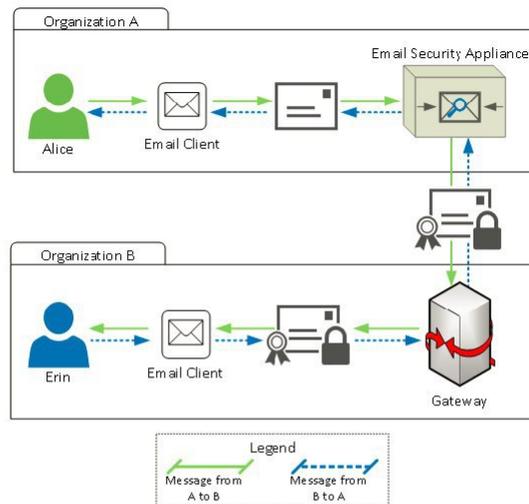
1. Bob (企業 A) は電子メール クライアントを使用して、未署名の暗号化されていないメッセージを Dave (企業 B) に送信します。
2. 企業 A の E メールセキュリティ アプライアンスは、メッセージを署名および暗号化して企業 B に送信します。

3. 企業Bのゲートウェイで、サードパーティアプリケーションはメッセージを復号および検証します。
4. Dave は暗号化されていない署名付きメッセージを受信します。

#### 企業 B が企業 A にメッセージを送信 :

1. Dave (企業B) は電子メールクライアントを使用して、未署名の暗号化されていないメッセージを Bob (企業 A) に送信します。
2. 企業Bのゲートウェイで、サードパーティアプリケーションはメッセージを署名および暗号化して企業 A に送信します。
3. 企業AのEメールセキュリティアプライアンスは、メッセージを復号および検証します。
4. Bob は暗号化されていない署名付きメッセージを受信します。

## シナリオ : Business-to-Consumer



企業 A と B は、両社の間でやり取りするすべてのメッセージを、S/MIME を使用して署名および暗号化したいと考えています。企業 A は、ゲートウェイレベルで S/MIME セキュリティサービスを実行するように E メールセキュリティアプライアンスを設定しています。企業 B は、すべてのユーザの電子メールクライアントを、S/MIME セキュリティサービスを実行するように設定しています。

**企業 A が企業 B にメッセージを送信：**

1. Alice（企業 A）は電子メールクライアントを使用して、未署名の暗号化されていないメッセージを Erin（企業 B）に送信します。
2. 企業 A の E メールセキュリティ アプライアンスは、メッセージを署名および暗号化して企業 B に送信します。
3. 企業 B の電子メールクライアントは、メッセージを復号および検証して Erin に表示します。

**企業 B が企業 A にメッセージを送信：**

1. Erin（企業 B）は電子メールクライアントを使用し、メッセージを署名および暗号化して Alice（企業 A）に送信します。
2. 企業 A の E メールセキュリティ アプライアンスは、メッセージを復号および検証します。
3. Alice は暗号化されていない未署名のメッセージを受信します。

## S/MIME を使用した発信メッセージの署名、暗号化、または署名と暗号化

- [E メールセキュリティ アプライアンスでの S/MIME 署名および暗号化ワークフロー](#)（5 ページ）
- [S/MIME を使用して発信メッセージの署名、暗号化、または署名と暗号化を行う方法](#)（6 ページ）
- [S/MIME 署名用の証明書の設定](#)（8 ページ）
- [S/MIME 暗号化用の公開キーの設定](#)（10 ページ）
- [S/MIME 送信プロファイルの管理](#)（13 ページ）
- [署名、暗号化、または署名と暗号化を行うメッセージの決定](#)（16 ページ）
- [コンテンツフィルタを使用したメッセージの署名、暗号化、または署名と暗号化および即時配信](#)（16 ページ）
- [コンテンツフィルタを使用した配信時のメッセージの署名、暗号化、または署名と暗号化](#)（17 ページ）



---

(注) アプライアンスを使用して、発信および着信メッセージの署名、暗号化、および署名と暗号化を行うことができます。

---

## E メールセキュリティ アプライアンスでの S/MIME 署名および暗号化ワークフロー

- [S/MIME 署名ワークフロー](#)（6 ページ）
- [S/MIME 暗号化ワークフロー](#)（6 ページ）

## S/MIME 署名ワークフロー

次のプロセスでは、アプライアンスで S/MIME 署名を実行する方法について説明します。

1. メッセージにハッシュアルゴリズムを適用して、メッセージダイジェストを作成します。
2. アプライアンスの S/MIME 証明書の秘密キーを使用して、メッセージダイジェストを暗号化します。
3. 暗号化されたメッセージダイジェストおよびアプライアンスの S/MIME 証明書の公開キーを使用して、PKCS7 署名を作成します。
4. メッセージに PKCS7 署名を添付して、メッセージに署名します。
5. 署名されたメッセージを受信者に送信します。

## S/MIME 暗号化ワークフロー

次のプロセスでは、アプライアンスで S/MIME 暗号化を実行する方法について説明します。

1. 疑似乱数セッション キーを作成します。
2. セッション キーを使用してメッセージ本文を暗号化します。
3. 受信者（ゲートウェイまたはコンシューマ）の S/MIME 証明書の公開キーを使用して、セッション キーを暗号化します。
4. 暗号化されたセッション キーをメッセージに添付します。
5. 暗号化されたメッセージを受信者に送信します。



(注) アプライアンスで PXE 暗号化と S/MIME 暗号化が有効になっている場合、まず S/MIME を使用して、次に PXE を使用してメッセージが暗号化されます。

## S/MIME を使用して発信メッセージの署名、暗号化、または署名と暗号化を行う方法

手順	操作手順	詳細
ステップ 1	S/MIME 証明書の要件を把握します。	<a href="#">S/MIME 証明書の要件 (24 ページ)</a> を参照してください。

手順	操作手順	詳細
ステップ 2	要件に応じて、次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• S/MIME 署名の場合、S/MIME 署名証明書を設定します。</li> <li>• S/MIME 暗号化の場合、受信者の S/MIME 証明書の公開キーを設定します。</li> <li>• S/MIME 署名および暗号化の場合、S/MIME 署名証明書と受信者の S/MIME 証明書の公開キーをそれぞれ設定します。</li> </ul>	参照先： <ul style="list-style-type: none"> <li>• <a href="#">S/MIME 署名用の証明書の設定 (8 ページ)</a></li> <li>• <a href="#">S/MIME 暗号化用の公開キーの設定 (10 ページ)</a></li> </ul>
ステップ 3	メッセージの署名、暗号化、または署名と暗号化を行うためのプロファイルを作成します。	<a href="#">メッセージの署名、暗号化、または署名および暗号化用の S/MIME 送信プロファイルの作成 (13 ページ)</a> を参照してください。
ステップ 4	アプライアンスでメッセージの署名、暗号化、または署名と暗号化を行うために、メッセージが満たすべき条件を定義します。	<a href="#">署名、暗号化、または署名と暗号化を行うメッセージの決定 (16 ページ)</a> を参照してください。
ステップ 5	電子メールのワークフローでいつメッセージの署名、暗号化、または署名と暗号化を行うかを決定します。	参照先： <ul style="list-style-type: none"> <li>• <a href="#">コンテンツフィルタを使用したメッセージの署名、暗号化、または署名と暗号化および即時配信 (16 ページ)</a></li> <li>• <a href="#">コンテンツフィルタを使用した配信時のメッセージの署名、暗号化、または署名と暗号化 (17 ページ)</a></li> </ul>
ステップ 6	メッセージを署名または暗号化するユーザグループを定義します。	メールポリシーを作成します。 <a href="#">メールポリシー</a> を参照してください
ステップ 7	定義した署名または暗号化アクションを、定義したユーザグループに関連付けます。	メールポリシーにコンテンツフィルタを関連付けます。 <a href="#">メールポリシー</a> を参照してください



- (注) CLIを使用してS/MIME署名、暗号化、または署名と暗号化を実行する場合は、**smimeconfig** コマンドを使用します。『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

## S/MIME 署名用の証明書の設定

メッセージに署名するための S/MIME 証明書を設定する必要があります。アプライアンスでは、次のいずれかの方法を使用して S/MIME 署名証明書を設定できます。

- アプライアンスを使用して自己署名 S/MIME 証明書を作成します。[自己署名 S/MIME 証明書の作成 \(8 ページ\)](#) を参照してください。
- 既存の S/MIME 証明書をアプライアンスにインポートします。[S/MIME 署名証明書のインポート \(10 ページ\)](#) を参照してください。



- (注) 署名されたメッセージを企業内のユーザに送信、またはテスト環境で送信するには、自己署名 S/MIME 証明書を使用することが推奨されます。署名されたメッセージを外部ユーザに送信、または実稼働環境で送信するには、信頼できる CA から取得した有効な S/MIME 証明書を使用します。

S/MIME の証明書要件については、[S/MIME 証明書の要件 \(24 ページ\)](#) を参照してください。

## 自己署名 S/MIME 証明書の作成

Web インターフェイスまたは CLI を使用して、RFC 5750 (Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Certificate Handling) に準拠する自己署名 S/MIME 証明書を生成できます。



- (注) 署名されたメッセージを企業内のユーザに送信、またはテスト環境で送信するには、自己署名 S/MIME 証明書を使用することが推奨されます。

### 手順

- ステップ 1 [ネットワーク (Network) ] > [証明書 (Certificates) ] をクリックします。
- ステップ 2 [証明書の追加 (Add Certificate) ] をクリックします。
- ステップ 3 [自己署名 S/MIME 証明書の作成 (Create Self-Signed S/MIME Certificate) ] を選択します。
- ステップ 4 自己署名証明書に、次の情報を入力します。

共通名	完全修飾ドメイン名
組織	組織の正確な正式名称。
組織単位	組織の部署名。
市（地名）	組織の本拠地がある都市。
州/県	組織の本拠地がある州、郡、または地方。
国	組織の本拠地がある 2 文字の ISO 国名コード。
失効までの期間	証明書が期限切れになるまでの日数。
サブジェクトの別名（ドメイン）	このフィールドを設定した場合、指定したドメインのユーザは署名されたメッセージを送信できます。  署名されたメッセージの送信元のドメイン名。たとえば、 <b>domain.com</b> や <b>*.domain.net</b> などです。複数エントリの場合、カンマ区切りリストを使用します。
サブジェクトの別名（E メール）	このフィールドを設定した場合、指定したユーザのみが署名されたメッセージを送信できます。  署名されたメッセージを送信するユーザの電子メールアドレス（例： <b>user@somedomain.com</b> ）。複数エントリの場合、カンマ区切りリストを使用します。
秘密キーサイズ	証明書署名要求（CSR）を生成する秘密キーのサイズ。

(注) S/MIME 署名証明書には、サブジェクトの別名（ドメイン）とサブジェクトの別名（E メール）の両方を含めることができます。

**ステップ 5** [次へ (Next)] をクリックして、証明書および署名情報を確認します。

**ステップ 6** 要件に応じて、次を実行します。

- 証明書の名前を入力します。
- 自己署名証明書の CSR を認証局に送信する場合、[証明書署名要求をダウンロード (Download Certificate Signing Request)] をクリックしてローカルまたはネットワークマシンに PEM 形式で CSR を保存します。

**ステップ 7** 変更を送信し、保存します。

### 次のタスク



(注) CLI を使用して自己署名 S/MIME 証明書を生成するには、**certconfig** コマンドを使用します。

## S/MIME 署名証明書のインポート

メッセージに署名するための S/MIME 証明書がすでにある場合、インポートしてアプライアンスに追加できます。

### はじめる前に

インポートする S/MIME 証明書が、[S/MIME 証明書の要件 \(24 ページ\)](#) に記載されている要件を満たしていることを確認します。

### 手順

- ステップ 1 [ネットワーク (Network) ]>[証明書 (Certificates) ] をクリックします。
- ステップ 2 [証明書の追加 (Add Certificate) ] をクリックします。
- ステップ 3 [証明書のインポート (Import Certificate) ] を選択します。
- ステップ 4 ネットワーク上またはローカル マシンの証明書ファイルへのパスを入力します。
- ステップ 5 ファイルのパスフレーズを入力します。
- ステップ 6 [次へ (Next) ] をクリックして証明書の情報を表示します。
- ステップ 7 証明書の名前を入力します。
- ステップ 8 変更を送信し、保存します。

### 次のタスク



(注) CLI を使用して S/MIME 証明書をインポートするには、**certconfig** コマンドを使用します。

## S/MIME 暗号化用の公開キーの設定

メッセージを暗号化するには、受信者の S/MIME 証明書の公開キーをアプライアンスに追加する必要があります。組織のポリシーおよびプロセスに応じて、次のいずれかの方法を使用して公開キーをアプライアンスに追加できます。

- 受信者に、電子メールなどの電子チャネルを使用して公開キーを送信するよう要求します。その後、Web インターフェイスまたは CLI を使用して公開キーを追加できます。

公開キーを追加する手順については、[S/MIME 暗号化用の公開キーの追加 \(11 ページ\)](#)を参照してください。

- Web インターフェイスまたは CLI を使用して公開キーの収集をイネーブルにし、受信者に署名されたメッセージを送信するよう要求します。E メールセキュリティ アプライアンスは、署名されたメッセージから公開キーを収集できます。

署名された着信メッセージから公開キーを収集する方法については、[公開キーの収集 \(12 ページ\)](#)を参照してください。

## S/MIME 暗号化用の公開キーの追加

### はじめる前に

- 公開キーが[S/MIME 証明書の要件 \(24 ページ\)](#)に説明されている要件を満たしていることを確認します。
- 公開キーが PEM 形式であることを確認します。

### 手順

---

**ステップ 1** [メール ポリシー (Mail Policies) ]>[公開キー (Public Keys) ]をクリックします。

**ステップ 2** [公開キーを追加 (Add Public Key) ]をクリックします。

**ステップ 3** 公開キーの名前を入力します。

**ステップ 4** 公開キーを入力します。

**ステップ 5** 変更を送信し、保存します。

---

### 次のタスク



---

(注) CLI を使用して公開キーを追加するには、**smimeconfig** コマンドを使用します。

---

## S/MIME 収集済み公開キー

公開キーを着信 S/MIME 署名済みメッセージから取得 (収集) し、収集したキーを使用して暗号化済みメッセージを収集したキーの所有者 (ビジネスまたはコンシューマ) に送信するように、アプライアンスを設定できます。

公開キーの収集は、メール フロー ポリシーでイネーブルにできます。収集したすべての公開キーは、[S/MIME 収集済み公開キー (S/MIME Harvested Public Key) ]ページに表示されます。

### 関連項目

- [公開キーの収集 \(12 ページ\)](#)

## 公開キーの収集

公開キーを着信 S/MIME 署名済みメッセージから取得（収集）し、これを使用して暗号化済みメッセージを収集したキーの所有者（ビジネスまたはコンシューマ）に送信するように、アプライアンスを設定できます。



(注) デフォルトでは、期限切れまたは自己署名 S/MIME 証明書の公開キーは収集されません。

### はじめる前に

送信者の S/MIME 証明書の公開キーが、[S/MIME 証明書の要件 \(24 ページ\)](#) に説明されている要件を満たしていることを確認します。

### 手順

**ステップ 1** [メール ポリシー (Mail Policies)] > [メール フロー ポリシー (Mail Flow Policies)] をクリックします。

**ステップ 2** 新しいメール フロー ポリシーを作成するか、既存のポリシーを変更します。

**ステップ 3** [セキュリティサービス (Security Features)] セクションまでスクロールします。

**ステップ 4** [S/MIME 公開キーの収集 (S/MIME Public Key Harvesting)] で以下を実行します。

- S/MIME 公開キーの収集をイネーブルにします。
- (任意) 署名された着信メッセージの検証に失敗した場合、公開キーを収集するかどうかを選択します。
- (任意) 更新された公開キーを収集するかどうかを選択します。

(注) 48 時間以内に同じドメインまたはメッセージから複数の更新された公開キーを受信すると、アプライアンスは警告アラートを送信します。

**ステップ 5** 変更を送信し、保存します。

### 次のタスク



(注) アプライアンス上の、収集された公開キーのリポジトリのサイズは 512 MB です。リポジトリが一杯になると、アプライアンスにより未使用の公開キーが自動的に削除されます。

CLI を使用してキーの収集をイネーブルにするには、**listenerconfig** コマンドを使用します。

### 次のステップ

署名されたメッセージをアプライアンスの管理者に送信するよう、受信者に要求します。アプライアンスは、署名されたメッセージから公開キーを収集し、[メールポリシー (Mail Policies)] > [収集済み公開キー (Harvested Public Keys)] ページに表示します。

#### 関連項目

- [S/MIME 収集済み公開キー \(11 ページ\)](#)

## S/MIME 送信プロファイルの管理

S/MIME 送信プロファイルでは、次のようなパラメータを定義できます。

- 署名、暗号化など、使用する S/MIME モード。
- 署名を行うための S/MIME 証明書
- 不透明、分離など、使用する S/MIME 署名モード。
- 受信者の S/MIME 証明書の公開キーをアプライアンス で利用できない場合に実行するアクション。

たとえば、ある組織に送信するメッセージはすべて署名済みである必要があり、別の組織に送信するメッセージはすべて署名済みかつ暗号化済みである必要があるとします。このシナリオでは、署名のみ、および署名および暗号化の2つの送信プロファイルを作成する必要があります。

Web インターフェイスまたは CLI を使用して、S/MIME 送信プロファイルを作成、編集、削除、インポート、エクスポート、および検索できます。

#### 関連項目

- [メッセージの署名、暗号化、または署名および暗号化用の S/MIME 送信プロファイルの作成 \(13 ページ\)](#)
- [S/MIME 送信プロファイルの編集 \(15 ページ\)](#)

## メッセージの署名、暗号化、または署名および暗号化用の S/MIME 送信プロファイルの作成

#### 手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [送信プロファイル (Sending Profiles)] をクリックします。
- ステップ 2** [プロファイルを追加 (Add Profile)] をクリックします。
- ステップ 3** 次のフィールドを設定します。

S/MIME プロファイル名	送信プロファイルの名前を入力します。
S/MIME モード (S/MIME Mode)	<p>S/MIME モードを選択します。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 署名</li> <li>• 暗号化</li> <li>• 署名/暗号化 (<b>Sign/Encrypt</b>)。署名してから暗号化します</li> <li>• 3 倍 (<b>Triple</b>)。署名、暗号化してから再度署名します</li> </ul> <p>(注) [署名 (Sign) ]、[署名/暗号化 (Sign/Encrypt) ]または[3 倍 (Triple) ]のいずれかの S/MIME モードを使用している場合、署名に失敗するとメッセージはバウンスされます。</p>
署名付き証明書 (Signing Certificate)	<p>使用する署名付き証明書を選択します。</p> <p>(注) このフィールドを設定する必要があるのは、[署名 (Sign) ]、[署名/暗号化 (Sign/Encrypt) ]または[3 倍 (Triple) ]のいずれかの S/MIME モードを選択した場合のみです。</p>
S/MIME 署名モード (S/MIME Sign Mode)	<p>S/MIME 署名モードを選択します。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 不透明 (<b>Opaque</b>)。不透明署名メッセージでは、メッセージと署名が1番目の部分に結合されて含められ、署名を検証することのみ読み取ることができます。</li> <li>• 分離 (<b>Detached</b>)。署名情報は、署名されるテキストと分離されます。この MIME タイプは2番目の部分に application/(x-)pkcs7-mime の MIME サブタイプを持つ multipart/signed です。</li> </ul> <p>(注) このフィールドを設定する必要があるのは、[署名 (Sign) ]、[署名/暗号化 (Sign/Encrypt) ]または[3 倍 (Triple) ]のいずれかの S/MIME モードを選択した場合のみです。</p>

S/MIME プロファイル名	送信プロファイルの名前を入力します。
S/MIME アクション (S/MIME Action)	<p>受信者の公開キーを利用できない場合にアプライアンスが実行する必要があるアクションを選択します。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>バウンス (Bounce)</b>。いずれかの受信者の公開キーを利用できない場合、メッセージは送信者にバウンスされます。</li> <li>• <b>ドロップ (Drop)</b>。いずれかの受信者の公開キーを利用できない場合、メッセージはドロップされます。</li> <li>• <b>分割 (Split)</b>。メッセージが分割されます。公開キーを利用できない受信者へのメッセージは暗号化されずに配信され、公開キーを利用できる受信者へのメッセージは暗号化されて配信されます。</li> </ul> <p>例：bob@example1.com と dave@example2.com にメッセージを送信し、dave@example2.com の公開キーを利用できないとします。このシナリオで [分割 (Split)] を選択した場合、アプライアンスは次の処理を行います。</p> <ul style="list-style-type: none"> <li>• メッセージを暗号化してから bob@example1.com に配信します。</li> <li>• メッセージを暗号化せずに dave@example2.com に配信します。</li> </ul> <p>(注) このフィールドを設定する必要があるのは、[暗号化 (Encrypt)]、[署名/暗号化 (Sign/Encrypt)] または [3 倍 (Triple)] のいずれかの S/MIME モードを選択した場合のみです。</p>

ステップ 4 変更を送信し、保存します。

次のタスク



(注) CLI を使用して送信プロファイルを作成するには、**smimeconfig** コマンドを使用します。

## S/MIME 送信プロファイルの編集

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [送信プロファイル (Sending Profiles)] をクリックします。
- ステップ 2 変更する送信プロファイルをクリックします。
- ステップ 3 [メッセージの署名、暗号化、または署名および暗号化用の S/MIME 送信プロファイルの作成 \(13 ページ\)](#) に説明されているように、フィールドを編集します。

ステップ4 変更を送信し、保存します。

## 署名、暗号化、または署名と暗号化を行うメッセージの決定

送信プロファイルを作成したら、署名、暗号化、または署名と暗号化を行うメッセージを決定する発信コンテンツフィルタを作成する必要があります。コンテンツフィルタは、発信電子メールをスキャンしてメッセージが指定された条件に一致するか判断します。コンテンツフィルタによってメッセージが条件に一致すると判断されたら、アプライアンスはメッセージの署名、暗号化、または署名と暗号化を行います。

### 関連項目

- [コンテンツに基づくメッセージのフィルタリング方法](#)

## コンテンツフィルタを使用したメッセージの署名、暗号化、または署名と暗号化および即時配信

### はじめる前に

コンテンツフィルタの条件を作成する概念を理解します。[コンテンツフィルタの仕組み](#)を参照してください。

### 手順

- ステップ1 [メールポリシー (Mail Policies) ]>[発信コンテンツフィルタ (Outgoing Content Filters) ]に移動します。
- ステップ2 [フィルタ (Filters) ]セクションで、[フィルタを追加 (Add Filter) ]をクリックします。
- ステップ3 [条件 (Conditions) ]セクションで、[条件を追加 (Add Condition) ]をクリックします。
- ステップ4 署名、暗号化、または署名と暗号化を行うメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ（「Confidential」など）を含むメッセージを識別する条件を追加できます。
- ステップ5 [OK] をクリックします。
- ステップ6 [アクション (Actions) ]セクションで、[アクションを追加 (Add Action) ]をクリックします。
- ステップ7 [アクションを追加 (Add Action) ]リストから[S/MIME 署名/暗号化 (最終アクション) (S/MIME Sign/Encrypt (Final Action) ) ]を選択します。
- ステップ8 コンテンツフィルタに関連付ける送信プロファイルを選択します。
- ステップ9 [OK] をクリックします。
- ステップ10 変更を送信し、保存します。

### 次のタスク

コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルトポリシーでコンテンツフィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、[メール ポリシーの概要](#)を参照してください。

## コンテンツフィルタを使用した配信時のメッセージの署名、暗号化、または署名と暗号化

配信時にメッセージを署名、暗号化、または署名および暗号化するコンテンツフィルタを作成します。すなわち、メッセージは次の処理段階に進み、すべての処理が完了したら、メッセージは署名、暗号化、または署名および暗号化されて配信されます。

### はじめる前に

- コンテンツ フィルタの条件を作成する概念を理解します。[コンテンツ フィルタの概要](#)を参照してください。

### 手順

- 
- ステップ 1** [メールポリシー (Mail Policies) ]>[発信コンテンツフィルタ (Outgoing Content Filters) ] に移動します。
  - ステップ 2** [フィルタ (Filters) ] セクションで、[フィルタを追加 (Add Filter) ] をクリックします。
  - ステップ 3** [条件 (Conditions) ] セクションで、[条件を追加 (Add Condition) ] をクリックします。
  - ステップ 4** 署名、暗号化、または署名と暗号化を行うメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ（「Confidential」など）を含むメッセージを識別する条件を追加できます。
  - ステップ 5** [OK] をクリックします。
  - ステップ 6** [アクション (Actions) ] セクションで、[アクションを追加 (Add Action) ] をクリックします。
  - ステップ 7** [アクションを追加 (Add Action) ] リストから [S/MIME 署名/配信時に暗号化 (S/MIME Sign/Encrypt on Delivery) ] を選択します。
  - ステップ 8** コンテンツ フィルタに関連付ける送信プロファイルを選択します。
  - ステップ 9** [OK] をクリックします。
  - ステップ 10** 変更を送信し、保存します。
- 

### 次のタスク

コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルトポリシーでコンテンツフィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、[メール ポリシーの概要](#)を参照してください。

# S/MIME を使用した着信メッセージの検証、復号、または復号と検証

- [E メールセキュリティ アプライアンスでの S/MIME 検証および復号ワークフロー](#) (18 ページ)
- [S/MIME を使用して着信メッセージの検証、復号、または復号と検証を行う方法](#) (19 ページ)
- [メッセージを復号するための証明書の設定](#) (20 ページ)
- [署名されたメッセージを検証するための公開キーの設定](#) (21 ページ)
- [S/MIME 復号および検証のイネーブル化](#) (23 ページ)
- [S/MIME 暗号化済みまたは検証済みメッセージ用のアクションの設定](#) (24 ページ)



(注) アプライアンスの S/MIME セキュリティ サービスを使用して、発信および着信メッセージの検証、復号、または復号と検証を行うことができます。

## E メールセキュリティ アプライアンスでの S/MIME 検証および復号ワークフロー

- [S/MIME 検証ワークフロー](#) (18 ページ)
- [S/MIME 復号ワークフロー](#) (18 ページ)

### S/MIME 検証ワークフロー

次のプロセスでは、アプライアンスで S/MIME 検証を実行する方法について説明します。

1. 署名されたメッセージにハッシュ アルゴリズムを適用して、メッセージ ダイジェストを作成します。
2. 送信者の S/MIME 証明書の公開キーを使用し、署名されたメッセージに添付された PKCS7 署名を復号してメッセージ ダイジェストを取得します。
3. 生成されたメッセージ ダイジェストを、署名されたメッセージから取得したメッセージ ダイジェストと比較します。メッセージ ダイジェストが一致した場合、メッセージは検証されます。
4. 認証局で送信者ドメインの S/MIME 証明書を検証します。

### S/MIME 復号ワークフロー

次のプロセスでは、アプライアンスで S/MIME 復号を実行する方法について説明します。

1. アプライアンスの S/MIME 証明書の秘密キーを使用して、セッションキーを復号します
2. セッション キーを使用してメッセージ本文を復号します。

## S/MIME を使用して着信メッセージの検証、復号、または復号と検証を行う方法

手順	操作手順	詳細
ステップ 1	S/MIME 証明書の要件を把握します。	<a href="#">S/MIME 証明書の要件 (24 ページ)</a> を参照してください。
ステップ 2	要件に応じて、次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• S/MIME 復号の場合、組織の S/MIME 証明書（復号の実行に必要な秘密キーを含む）をアプライアンスに追加します。</li> <li>• S/MIME 検証の場合、検証の実行に必要な送信者の S/MIME 証明書の公開キーをアプライアンスに追加します。</li> <li>• S/MIME 復号および検証の場合、以下をアプライアンスに追加します。 <ul style="list-style-type: none"> <li>• 組織の S/MIME 証明書（復号の実行に必要な秘密キーを含む）をアプライアンスに追加します。</li> <li>• 送信者ドメインの認証局。</li> <li>• 検証の実行に必要な送信者 S/MIME 証明書の公開キー。</li> </ul> </li> </ul>	参照先 <ul style="list-style-type: none"> <li>• <a href="#">メッセージを復号するための証明書の設定 (20 ページ)</a></li> <li>• <a href="#">署名されたメッセージを検証するための公開キーの設定 (21 ページ)</a></li> <li>• <a href="#">カスタム認証局リストのインポート</a></li> </ul>
ステップ 3	S/MIME を使用して着信メッセージの検証、復号、または復号と検証を行うメールフローポリシーを設定します。	<a href="#">S/MIME 復号および検証のイネーブル化 (23 ページ)</a> を参照してください。
ステップ 4	（任意）アプライアンスが復号済みまたは検証済みのメッセージに対して実行するアクションを定義します。	<a href="#">S/MIME 暗号化済みまたは検証済みメッセージ用のアクションの設定 (24 ページ)</a> を参照してください。



(注) CLI を使用して S/MIME 検証、復号、または復号と検証を実行する場合は、**listenerconfig > hostaccess** コマンドを使用します。詳細については、CLI インライン ヘルプを参照してください。

## メッセージを復号するための証明書の設定

組織の S/MIME 証明書（復号の実行に必要な秘密キーを含む）をアプライアンスに追加する必要があります。

### はじめる前に

- 次のいずれかの方法で、アプライアンスの S/MIME 証明書の公開キーを送信者（ビジネスまたはコンシューマ）と共有します。
  - 電子メールなどの電子チャネルを使用して、公開キーを送信します。
  - キー収集を使用して公開キーを取得するように、送信者に要求します。

送信者はこの公開キーを使用して、暗号化されたメッセージをアプライアンスに送信できます。



(注) B2C のシナリオでは、組織の S/MIME 証明書がドメイン証明書の場合、一部の電子メールクライアント（Microsoft Outlook など）は組織の S/MIME 証明書の公開キーを使用して暗号化済みメッセージを送信できないことがあります。これは、これらの電子メールクライアントがドメイン証明書の公開キーを使用した暗号化をサポートしていないためです。

- インポートする S/MIME 証明書が、[S/MIME 証明書の要件（24 ページ）](#)に記載されている要件を満たしていることを確認します。

### 手順

- ステップ 1 [ネットワーク (Network)] > [証明書 (Certificates)] をクリックします。
- ステップ 2 [証明書の追加 (Add Certificate)] をクリックします。
- ステップ 3 [証明書のインポート (Import Certificate)] を選択します。
- ステップ 4 ネットワーク上またはローカルマシンの証明書ファイルへのパスを入力します。
- ステップ 5 ファイルのパスフレーズを入力します。
- ステップ 6 [次へ (Next)] をクリックして証明書の情報を表示します。
- ステップ 7 証明書の名前を入力します。
- ステップ 8 変更を送信し、保存します。

### 次のタスク



(注) CLI を使用して S/MIME 証明書を追加するには、`certconfig` コマンドを使用します。

## 署名されたメッセージを検証するための公開キーの設定

署名されたメッセージを検証するには、送信者の S/MIME 証明書の公開キーをアプライアンスに追加する必要があります。組織のポリシーおよびプロセスに応じて、次のいずれかの方法を使用して公開キーをアプライアンスに追加できます。

- 送信者に、電子メールなどの電子チャネルを使用して公開キーを送信するよう要求します。その後、Web インターフェイスまたは CLI を使用して公開キーを追加できます。

公開キーを追加する手順については、[S/MIME 暗号化用の公開キーの追加 \(11 ページ\)](#) を参照してください。

- キー収集を使用して公開キーを取得します。[公開キーの収集 \(12 ページ\)](#) を参照してください。

### S/MIME 検証用の公開キーの追加

#### はじめる前に

- 公開キーが [S/MIME 証明書の要件 \(24 ページ\)](#) に説明されている要件を満たしていることを確認します。
- 公開キーが PEM 形式であることを確認します。

#### 手順

---

**ステップ 1** [メール ポリシー (Mail Policies)] > [公開キー (Public Keys)] をクリックします。

**ステップ 2** [公開キーを追加 (Add Public Key)] をクリックします。

**ステップ 3** 公開キーの名前を入力します。

**ステップ 4** 公開キーを入力します。

**ステップ 5** 変更を送信し、保存します。

---

#### 次のタスク



---

(注) CLI を使用して公開キーを追加するには、`smimeconfig` コマンドを使用します。

---

### S/MIME 検証用の公開キーの収集

公開キーを着信 S/MIME 署名済みメッセージから取得 (収集) し、これを使用して収集したキーの所有者 (ビジネスまたはコンシューマ) からの署名済みメッセージを検証するように、アプライアンスを設定できます。



- (注) デフォルトでは、期限切れまたは自己署名 S/MIME 証明書の公開キーは収集されません。
1. Web インターフェイスまたは CLI を使用して、公開キーの収集をイネーブルにします。[公開キーの収集のイネーブル化 \(22 ページ\)](#) を参照してください。
  2. 送信者に、署名されたメッセージを送信するよう要求します。
  3. 収集が完了したら、収集した公開キーをアプライアンスに追加します。[S/MIME 検証用の収集された公開キーの追加 \(23 ページ\)](#) を参照してください。

この手順により、メッセージは確実にゲートウェイ レベルで検証されます。

## 公開キーの収集のイネーブル化

### 手順

- ステップ 1 [メール ポリシー (Mail Policies) ] > [メール フロー ポリシー (Mail Flow Policies) ] をクリックします。
- ステップ 2 新しいメール フロー ポリシーを作成するか、既存のポリシーを変更します。
- ステップ 3 [セキュリティサービス (Security Features) ] セクションまでスクロールします。
- ステップ 4 [S/MIME 公開キーの収集 (S/MIME Public Key Harvesting) ] で以下を実行します。
  - S/MIME 公開キーの収集をイネーブルにします。
  - (任意) 署名された着信メッセージの検証に失敗した場合、公開キーを収集するかどうかを選択します。
  - (任意) 更新された公開キーを収集するかどうかを選択します。

(注) 48時間以内に同じドメインまたはメッセージから複数の更新された公開キーを受信すると、アプライアンスは警告アラートを送信します。
- ステップ 5 変更を送信し、保存します。

### 次のタスク



- (注) アプライアンス上の、収集された公開キーのリポジトリのサイズは 512 MB です。リポジトリが一杯になると、アプライアンスにより未使用の公開キーが自動的に削除されます。
- CLI を使用してキーの収集をイネーブルにするには、`listenerconfig` コマンドを使用します。

## S/MIME 検証用の収集された公開キーの追加

### 手順

- ステップ 1** [メール ポリシー (Mail Policies) ]>[収集済み公開キー (Harvested Public Keys) ]をクリックします。
- ステップ 2** 目的の収集された公開キーをクリックして、公開キーをコピーします。
- ステップ 3** 公開キーをアプライアンスに追加します。 [S/MIME 検証用の公開キーの追加 \(21 ページ\)](#) を参照してください。
- ステップ 4** 変更を送信し、保存します。

## S/MIME 復号および検証のイネーブル化

### 手順

- ステップ 1** [メール ポリシー (Mail Policies) ]>[メールフローポリシー (Mail Flow Policies) ]をクリックします。
- ステップ 2** 新しいメールフローポリシーを作成するか、既存のポリシーを変更します。
- ステップ 3** [セキュリティサービス (Security Features) ]セクションまでスクロールします。
- ステップ 4** [S/MIME の復号/検証 (S/MIME Decryption/Verification) ]で以下を行います。
  - S/MIME 復号および検証をイネーブル化します。
  - S/MIME の検証後、デジタル署名を維持するかメッセージから削除するかを選択します。エンドユーザに S/MIME ゲートウェイ検証について知られたくない場合は、[削除 (Remove) ]を選択します。トリプルラップされたメッセージの場合、内部署名のみが維持または削除されます。
- ステップ 5** 変更を送信し、保存します。

### 次のタスク



- ヒント** S/MIME 復号および検証がメールフローポリシーでイネーブルになっている場合、すべての S/MIME メッセージは、復号および検証ステータスに関係なく配信されます。S/MIME 暗号化済みまたは検証済みメッセージを処理するアクションを設定する場合は、メッセージフィルター ルール smime-gateway-verified および smime-gateway を使用できます。詳細については、[S/MIME 暗号化済みまたは検証済みメッセージ用のアクションの設定 \(24 ページ\)](#) を参照してください。

## S/MIME 暗号化済みまたは検証済みメッセージ用のアクションの設定

アプライアンスでS/MIME復号、検証、またはその両方を実行した後、結果に応じて異なるアクションを行うことができます。メッセージフィルタルール `smime-gateway-verified` および `smime-gateway` を使用して、復号、検証、またはその両方の結果に基づいてメッセージに対してアクションを実行できます。詳細については、[メッセージフィルタを使用した電子メールポリシーの適用](#)を参照してください。



- (注) また、復号または検証、あるいはその両方の結果に基づいたアクションをメッセージで実行するには、コンテンツフィルタ条件の [S/MIME ゲートウェイ メッセージ (S/MIME Gateway Message) ] および [S/MIME ゲートウェイ 検証済み (S/MIME Gateway Verified) ] も使用できます。詳細については、[コンテンツフィルタ](#)を参照してください。

例：検証、検証、復号、またはその両方に失敗した S/MIME メッセージの隔離

次のメッセージフィルタでは、メッセージが S/MIME メッセージであるかどうかを確認し、S/MIME を使用した検証または復号に失敗した場合は隔離します。

```
quarantine_smime_messages:if (smime-gateway-message and not smime-gateway-verified)
{ quarantine("Policy"); }
```

## S/MIME 証明書の要件

- [署名のための証明書の要件 \(24 ページ\)](#)
- [暗号化のための証明書の要件 \(25 ページ\)](#)

### 署名のための証明書の要件

署名を行うための S/MIME 証明書には、次の情報を含める必要があります。

共通名	完全修飾ドメイン名
組織	組織の正確な正式名称。
組織単位	組織の部署名。
市 (地名)	組織の本拠地がある都市。
州/県	組織の本拠地がある州、郡、または地方。
国	組織の本拠地がある 2 文字の ISO 国名コード。
失効までの期間	証明書が期限切れになるまでの日数。

共通名	完全修飾ドメイン名
サブジェクトの別名（ドメイン）	署名されたメッセージの送信元のドメイン名。たとえば、 <b>domain.com</b> や <b>*.domain.net</b> などです。複数エントリの場合、カンマ区切りリストを使用します。
サブジェクトの別名（Eメール）	署名されたメッセージを送信するユーザの電子メールアドレス（例： <b>user@somedomain.com</b> ）。複数エントリの場合、カンマ区切りリストを使用します。
秘密キーサイズ	CSR 用に生成する秘密キーのサイズ。
キーの使途（Key Usage）	<p>キーの使用状況は、証明書を何に使用できるかを決定する制約方式です。キーの使用状況の拡張が指定されている場合は、<b>digitalSignature</b> および <b>nonRepudiation</b> ビットが設定されている必要があります。</p> <p>キーの使用状況の拡張が指定されていない場合、受信側クライアントは、<b>digitalSignature</b> および <b>nonRepudiation</b> ビットが設定されていると推定する必要があります。</p>

S/MIME 証明書の詳細については、RFC 5750 : Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Certificate Handling を参照してください。

## 暗号化のための証明書の要件

暗号化を行うための S/MIME 証明書には、次の情報を含める必要があります。

共通名	完全修飾ドメイン名
組織	組織の正確な正式名称。
組織単位	組織の部署名。
市（地名）	組織の本拠地がある都市。
州/県	組織の本拠地がある州、郡、または地方。
国	組織の本拠地がある 2 文字の ISO 国名コード。
失効までの期間	証明書が期限切れになるまでの日数。
サブジェクトの別名（ドメイン）	<p>暗号化されたメッセージの送信先のドメイン名。たとえば、<b>domain.com</b> や <b>*.domain.net</b> などです。複数エントリの場合、カンマ区切りリストを使用します。</p> <p>暗号化されたメッセージをドメイン内のすべてのユーザに送信する場合は、公開キーに SAN ドメインを含める必要があります。</p>

共通名	完全修飾ドメイン名
サブジェクトの別名 (E メール)	暗号化されたメッセージを送信するユーザの電子メールアドレス (例: user@somedomain.com)。複数エントリの場合、カンマ区切りリストを使用します。
秘密キーサイズ	CSR 用に生成する秘密キーのサイズ。
キーの使途 (Key Usage)	キーの使用状況は、証明書を何に使用できるかを決定する制約方式です。キーの使用状況の拡張が指定され、keyEncipherment ビットが設定されている必要があります。

S/MIME 証明書の詳細については、RFC 5750 : Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Certificate Handling を参照してください。

## 公開キーの管理

アプライアンスでは次が必要です。

- 発信メッセージを暗号化するための、受信者の S/MIME 暗号化証明書の公開キー。
- 署名済み着信メッセージを検証するための、送信者の S/MIME 署名証明書の公開キー。

次のいずれかの方法で、公開キーをアプライアンスに追加できます。

- 目的の PEM 形式の公開キーがある場合は、Web インターフェイスまたは CLI を使用して追加できます。[公開キーの追加 \(26 ページ\)](#) を参照してください。
- 目的の公開キーが含まれたエクスポートファイルがある場合は、そのエクスポートファイルを /configuration ディレクトリにコピーし、Web インターフェイスまたは CLI を使用してインポートできます。[既存のエクスポートファイルからの公開キーのインポート \(27 ページ\)](#) を参照してください。

アプライアンスでは、キーの収集もサポートしています (署名済み着信メッセージから自動的に公開キーを取得)。詳細については、[S/MIME 収集済み公開キー \(11 ページ\)](#) を参照してください。

## 公開キーの追加

はじめる前に

- 公開キーが [S/MIME 証明書の要件 \(24 ページ\)](#) に説明されている要件を満たしていることを確認します。
- 公開キーが PEM 形式であることを確認します。

### 手順

- ステップ1 [メール ポリシー (Mail Policies) ]>[公開キー (Public Keys) ]をクリックします。
- ステップ2 [公開キーを追加 (Add Public Key) ]をクリックします。
- ステップ3 公開キーの名前を入力します。
- ステップ4 公開キーを入力します。
- ステップ5 変更を送信し、保存します。

### 次のタスク



- (注) CLI を使用して公開キーを追加するには、**smimeconfig** コマンドを使用します。

## 既存のエクスポート ファイルからの公開キーのインポート

### はじめる前に

エクスポートファイルをアプライアンスの /configuration ディレクトリにコピーします。エクスポート ファイルを作成する手順については、[公開キーのエクスポート \(27 ページ\)](#) を参照してください。

### 手順

- ステップ1 [メール ポリシー (Mail Policies) ]>[公開キー (Public Keys) ]をクリックします。
- ステップ2 [公開キーをインポート (Import Public Keys) ]をクリックします。
- ステップ3 エクスポート ファイルを選択して [送信 (Submit) ]をクリックします。

- (注) 多数の公開キーを持つファイルをインポートする場合、インポートプロセスに時間がかかることがあります。Web インターフェイスまたは CLI 無活動タイムアウトを適宜調整してください。

- ステップ4 変更を保存します。

## 公開キーのエクスポート

アプライアンスのすべての公開キーは、1 つのテキストファイルにまとめてエクスポートされ、/configuration ディレクトリに保存されます。

## 手順

---

- ステップ1 [メール ポリシー (Mail Policies)] > [公開キー (Public Keys)] を選択します。
  - ステップ2 [公開キーをエクスポート (Export Public Keys)] をクリックします。
  - ステップ3 ファイルの名前を入力し、[送信 (Submit)] をクリックします。
-

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。