OCSP 応答ステープリング

OCSP 応答ステープリング機能では、Online Certificate Status Protocol（OCSP）を使用してデジタル証明書に含まれるピアのユーザまたはデバイス クレデンシャルの有効期間を確認できます。

OCSP 応答ステープリングの情報

OCSP 応答ステープリングの概要

ピアが失効情報を取得し、この情報を検証して証明書失効のステータスを確認する場合、Online Certificate Status Protocol（OCSP）は証明書失効を確認するための方式になります。この方式では、証明書失効のステータスは、クラウドを介してOCSP応答者に到達するピアの能力、または証明書失効情報を検索する際の証明書送信者の能力によって制限されます。

OCSP 応答ステープリングは、デバイスの独自の証明書で OCSP 応答を取得する新しい方式をサポートします。この機能を使用すると、OCSP サーバに接続し、この結果とその証明書をピアに直接送信して、その独自の証明書失効情報を入手できます。その結果、ピアがOCSP応答者に接続する必要はありません。

OCSP 応答ステープリングの設定方法

EKU 属性を要求するための PKI クライアントの設定

次の作業を実行し、OCSP（Online Certificate Status Protocol）応答ステープリングを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **ocsp url** *url*
5. **eku request** *attribute*
6. **match eku** *attribute*
7. **revocation-check** *method1* ［*method2* ［*method3*］］
8. **exit**
9. **exit**
10. **show cry pki counters**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 1. パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル 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	**crypto pki trustpoint** *name* 例： `Device(config)# crypto pki trustpoint msca`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。

ステップ 4	**ocsp url** *url*
	例：
	`Device(ca-trustpoint)# ocsp url http://ocsp-server`
	例：
	`Device(ca-trustpoint)# ocsp url http://10.10.10.1:80`
	例：
	`Device(ca-trustpoint)# ocsp url http://[2001DB8:1:1::2]:80`
		url 引数は、トラストポイントが証明書ステータスをチェックできるように OCSP サーバーの URL を指定します。この URL は、証明書の AIA 拡張部に指定されている OCSP サーバーの URL（存在する場合）を上書きします。設定したトラストポイントに関連するすべての証明書は、OCSP サーバーによって確認されます。使用可能な URL は、ホスト名、IPv4 アドレス、または IPv6 アドレスです。
		（注） OCSP 要求 URL が HTTP プロキシサーバーではなく **ocsp url** *url* コマンドで設定されていることを確認してください。

	コマンドまたはアクション	目的
ステップ 5	**eku request** *attribute* 例： `Device(ca-trustpoint)# eku request ssh-client`	証明書に指定した eku *attribute* を含めるように要求します。この要求は、PKI クライアントで設定した場合、登録時に CA サーバに送信されます。 *attribute* 引数には次のいずれかを指定できます。 • client-auth • code-signing • email-protection • ipsec-end-system • ipsec-tunnel • ipsec-user • ocsp-signing • server-auth • time-stamping • ssh-server • ssh-client
ステップ 6	**match eku** *attribute* 例： `Device(ca-trustpoint)# match eku client-auth`	指定した属性が証明書内に存在し、他の検証が失敗した場合のみ、PKI はピア証明書を検証できます。 *attribute* 引数には次のいずれかを指定できます。 • client-auth • code-signing • email-protection • ipsec-end-system • ipsec-tunnel • ipsec-user • ocsp-signing • server-auth • time-stamping • ssh-server • ssh-client

	コマンドまたはアクション	目的
ステップ 7	**revocation-check** *method1* ［*method2* ［*method3*］］ 例： `Device(ca-trustpoint)# revocation-check ocsp none`	（任意）証明書の失効ステータスをチェックします。 • crl：CRL によって証明書をチェックします。これがデフォルトのオプションです。 • none：証明書のチェックを無視します。 • ocsp：OCSP サーバによって証明書をチェックします。 2 番目と 3 番目の方法を指定した場合、各方法はその直前の方法でエラーが返された場合（サーバがダウンしている場合など）にだけ使用されます。
ステップ 8	**exit** 例： `Device(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 10	**show cry pki counters** 例： `Device# show cry pki counters`	（任意）デバイスの PKI カウンタを表示します。

EKU 属性を追加するための PKI サーバの設定

次の作業を実行し、OCSP（Online Certificate Status Protocol）応答ステープリングを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *cs-label*
5. **eku request** *attribute*
6. **exit**
7. **exit**
8. **show crypto pki counters**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 1. パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル 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	**ip http server** 例： `Device(config)# ip http server`	ご使用のシステムの HTTP サーバをイネーブルにします。
ステップ 4	**crypto pki server** *cs-label* 例： `Device(config)# crypto pki server server-pki`	証明書サーバのラベルを定義し、証明書サーバ コンフィギュレーション モードを開始します。 （注） 手動で RSA キー ペアを生成した場合、*cs-label* 引数はキー ペアの名前と一致する必要があります。
ステップ 5	**eku request** *attribute* 例： `Device(cs-server)# eku request ssh-server`	証明書に指定した eku *attribute* を含めるように要求します。 *attribute* 引数には次のいずれかを指定できます。 • client-auth • code-signing • email-protection • ipsec-end-system • ipsec-tunnel • ipsec-user • ocsp-signing • server-auth • time-stamping • ssh-server • ssh-client

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(cs-server)# exit`	cs-server コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 8	**show crypto pki counters** 例： `Device# show crypto pki counters`	（任意）デバイスの PKI カウンタを表示します。

例

次に、**show crypto pki counters** の出力例を示します。

```
Device# show crypto pki counters

PKI Sessions Started: 0
PKI Sessions Ended: 0
PKI Sessions Active: 0
Successful Validations: 0
Failed Validations: 0
Bypassed Validations: 0
Pending Validations: 0
CRLs checked: 0
CRL - fetch attempts: 0
CRL - failed attempts: 0
CRL - rejected busy fetching: 0
OCSP - fetch requests: 0
OCSP - received responses: 0
OCSP - failed attempts: 0
OCSP - staple requests: 0
AAA authorizations: 0
```

OCSP 応答ステープリングの追加資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 2560	『*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*』
RFC 4806	『*Online Certificate Status Protocol (OCSP) Extensions to IKEv2*』
RFC 5280	『*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*』
RFC 6187	『*X.509v3 Certificates for Secure Shell Authentication*』
RFC 6066	『*Transport Layer Security (TLS) Extensions: Extension Definitions*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

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。