PKI クレデンシャル失効アラート

PKI クレデンシャル失効アラート機能を使用すると、CA 証明書が失効間近になるとアラート通知の形式で警告メカニズムが提供されます。

PKI クレデンシャル失効アラートの制約事項

アラートは、次の証明書には送信されません。

- 永続的または一時的な自己署名証明書。
- セキュアな固有デバイス識別子（SUDI）証明書。
- トラストプールに属する証明書。トラストプールには独自の失効アラートメカニズムがあります。
- トラストポイントのクローン。

PKI アラート通知の情報

アラート通知の概要

Cisco IOS 認証局（CA）サーバを使用すると、証明書が失効する前に証明書の自動登録が可能になり、認証中にアプリケーションの証明書が利用できるようになります。ただし、ネットワーク停止、クロック更新の問題、およびCA の過負荷が証明書の更新に影響を与え、認証に有効な証明書が使用できなくなることでサブシステムがオフラインになります。PKI クレデンシャル失効アラート機能は、証明書の失効が近付くと、CA クライアントが syslog サーバに通知を送信するためのメカニズムを提供します。

通知は次の間隔で送信されます。

- 最初の通知：これは証明書が失効する 60 日前に送信されます。
- 通知の繰り返し：最初の通知の後、証明書が失効する 1 週間前まで後続の通知が毎週送信されます。最後の週には、証明書の失効日まで通知が毎日送信されます。

証明書の有効期限が 1 週間以上ある場合、通知は [warning] モードで送信されます。証明書の有効期限が 1 週間未満の場合、通知は [alert] モードで送信されます。通知には次の情報が含まれます。

- 証明書が関連付けられたトラストポイント
- 証明書タイプ
- 証明書のシリアル番号
- 証明書の発行元名
- 証明書が失効するまでの残り日数
- 証明書の自動登録が有効かどうか
- 対応する証明書のシャドウ証明書が利用可能かどうか

（注） アラート通知は syslog サーバまたは Simple Network Management Protocol（SNMP）トラップを介して送信されます。トラストポイントの自動登録が設定され、対応するシャドウまたはロールオーバー証明書が有効である場合、およびシャドウまたはロールオーバー証明書の開始時刻が証明書の終了時刻と同じまたはそれ以前の場合、通知は停止します。

この機能は無効にできず、設定作業を追加する必要はありません。**show crypto pki timers** コマンドはタイマーの有効期限情報を表示できるようになりました。次に、証明書の失効間近にタイマーを表示する **show crypto pki timers detail** コマンドの出力例を示します。このタイマーが失効すると、通知が syslog サーバに送信されます。

```
Device# show crypto pki timers detail

PKI Timers
|       14:36.150  (2019-10-30T11:33:30Z)
  |       14:36.150  (2019-10-30T11:33:30Z) SESSION CLEANUP
  |2569d23:56:19.461  (2026-11-12T11:15:13Z) SHADOW test

Expiry Alert Timers
|659d 5:56:19.599  (2021-08-19T17:15:13Z)
  |659d 5:56:19.599  (2021-08-19T17:15:13Z) ID(test)
  |2875d 4:45:18.562  (2027-09-13T16:04:12Z) CA(test)

Trustpool Timers
|3464d 9:06:48.463  (2029-04-24T20:25:42Z)
  |3464d 9:06:48.463  (2029-04-24T20:25:42Z) TRUSTPOOL
```

次に、デバイスに表示される syslog メッセージを示します。

```
Device#

Dec 16 10:24:13.533: %PKI-4-CERT_EXPIRY_WARNING: ID Certificate belonging to trustpoint
 tp will expire in 60 Days 0 hours 0 mins 0 secs.
Issuer-name cn=CA
Subject-name hostname=Router
Serial-number 02
Auto-Renewal: Not Enabled
```

PKI トラップ

PKI トラップでは、ネットワーク内のデバイスの証明書情報を取得するため、PKI 展開の監視と運用が簡単になります。ルート デバイスは、デバイスに設定されたしきい値に基づいて、ネットワーク管理システム（NMS）に SNMP トラップを定期的に送信します。トラップは次のシナリオで送信されます。

- 新しい証明書がインストールされる場合。SNMP トラップ（新しい証明書通知）は、証明書のシリアル番号、証明書の発行者名、証明書の所有者名、トラストポイント名、証明書タイプ、証明書の開始日と終了日などの情報を含む SNMP サーバーに送信されます。
- 証明書が失効間近の場合。SNMP トラップ（証明書失効通知）は、証明書の終了日の 60 日から 1 週間前まで SNMP サーバに定期的に送信されます。証明書が失効する週には、トラップが毎日送信されます。トラップには、証明書のシリアル番号、証明書の発行者名、トラストポイント名、証明書タイプ、証明書の寿命などの証明書情報が含まれます。

PKI トラップを有効にするには、**snmp-server enable traps pki** コマンドを使用します。

（注） シャドウまたはロールオーバー証明書の開始時間が証明書の終了時間よりも遅い場合、シャドウ証明書が有効でないことを示すトラップが送信されます。ただし、同じトラストポイントで利用可能なシャドウ証明書とシャドウ証明書が有効な場合には、トラップは送信されません。

PKI クレデンシャル失効アラートの追加資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS 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』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

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。