# IOS PKI の自動登録、自動ロールオーバー、およびタイマー

## 内容



## 概要

このドキュメントでは、自動登録と自動ロールオーバーのCisco IOS®公開キーインフラストラクチャ(PKI)操作がどのように動作し、これらの操作に対してそれぞれのPKIタイマーがどのように計算されるかについて説明します。

証明書のライフタイムが固定され、ある時点で期限切れになります。証明書がVPNソリューションの認証の目的で使用されている場合（たとえば）、これらの証明書が期限切れになると、認証失敗の可能性があり、その結果、エンドポイント間のVPN接続が失われます。この問題を回避するには、証明書の自動更新に次の2つのメカニズムを使用できます。

- クライアント/スポークルータの自動登録
- 認証局(CA)サーバルータの自動ロールオーバー

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- PKIと信頼の概念
- ルータでのCAの基本設定

## 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

# 用語

### 自動登録

エンドデバイス上の証明書が期限切れになる直前に、自動登録は中断することなく新しい証明書を取得します。自動登録が設定されている場合、クライアント/スポークルータは、自身の証明書（IDまたはID証明書）が期限切れになる前に、新しい証明書を要求できます。

### 自動ロールオーバー

このパラメータは、証明書サーバ(CS)がロールオーバー（シャドウ）証明書を生成するタイミングを決定します。このコマンドが引数なしでCS設定に入力された場合、デフォルトの時間は30日です。

> **注**：このドキュメントの例では、このパラメータの値は10分です。

CAサーバ上の証明書が期限切れになる直前に、自動ロールオーバーにより、CAは中断することなく新しい証明書を取得できます。自動ロールオーバーが設定されている場合、CAルータは自身の証明書が期限切れになる前に、新しい証明書を生成できます。シャドウ証明書またはロールオーバー証明書と呼ばれる新しい証明書は、現在のCA証明書が期限切れになる正確な時点でアクティブになります。

このドキュメントの「概要」セクションで説明されている2つの機能を使用すると、PKIの導入が自動化され、スポークまたはクライアントデバイスは現在のCA証明書が期限切れになる前にシャドウ/ロールオーバーID証明書とシャドウ/ロールオーバーCA証明書を取得できます。これにより、現在のIDおよびCA証明書の期限が切れたときに、新しいIDおよびCA証明書に中断することなく移行できます。

### lifetime ca-certificate

このパラメータは、CA証明書の有効期間を指定します。このパラメータの値は、日/時間/分で指定できます。

> **注**：このドキュメントの例では、このパラメータの値は30分です。

### 生涯証明書

このパラメータは、CAルータによって発行されるID証明書の有効期間を指定します。このパラメータの値は、日/時間/分で指定できます。

**注**:このドキュメントの例では、このパラメータの値は20分 です

# 設定

注:**このドキュメントでは、キーの自動登録と自動ロールオーバーの概念を説明するために**、*lifetime*、*auto-rollover*、**および***auto-enroll***のPKIタイマー値を小さくしたものを使用しています。**ライブネットワーク環境では、これらのパラメータにデフォルトのライフタイムを使用することをお勧めします。

**ヒント**：正規の時刻源がない場合は、ロールオーバーや*再登録*など、PKIタイマーベースのすべてのイベントが影響を受ける可能性があります。このため、PKIを実行するすべてのルータでネットワークタイムプロトコル(NTP)を設定することを推奨します。

## Cisco IOS CAサーバの設定

このセクションでは、Cisco IOS CAサーバの設定例を示します。

```
RootCA#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 10.1.1.1 YES manual up up

crypto pki server ios-ca
issuer-name CN=Root-CA,OU=TAC,C=IN
grant auto
hash sha512
lifetime certificate 0 0 20
lifetime ca-certificate 0 0 30
cdp-url http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
auto-rollover 0 0 10
database url flash:
```

**注**:auto-rolloverコマンドで指定する値は、現在のCA証明書の終了日*前に*、*ロールオーバー証明書が生成される日数/時/分*数です。したがって、CA証明書が12:00 ~ 12:30の範囲で有効な場合、**auto-rollover 0 0 10は、ロールオーバーCA証明書が12:20前後に生成されることを意味します。**

**show crypto pki certificate**コマンドを入力して、Cisco IOS CAサーバの設定を確認します。

```
RootCA#show crypto pki certificate
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
```

```
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
```

この出力に基づいて、ルータには9:16 ~ 9:46 IST Nov 25, 2012のCA証明書が含まれています。自動ロールオーバーが10分間設定されているため、シャドウ/ロールオーバー証明書は2012年11月25日に*9.36 ISTによって生成される*予定です。

確認するには、**show crypto pki timer**コマンドを入力します。

```
RootCA#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:19:22.283 IST Sun Nov 25 2012
PKI Timers
| 12:50.930
| 12:50.930 SESSION CLEANUP
CS Timers
| 16:43.558
| 16:43.558  CS SHADOW CERT GENERATION
| 26:43.532 CS CERT EXPIRE
| 26:43.558 CS CRL UPDATE
```

次の出力に基づいて、**show crypto pki timer**コマンドが9.19 ISTで発行され、シャドウ/ロールオーバー証明書は16.43分以内に生成される予定です。

[09:19:22 + 00:16:43] = **09:36:05**。これは[end-date_of_current_CA_cert - auto_rollover_timer];つまり、[09:46:05 - 00:10:00] = **09:36:05となります**。

## クライアント/スポークルータの設定

このセクションでは、クライアント/スポークルータの設定例を示します。

```
Client-1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 172.16.1.1 YES manual up up

crypto pki trustpoint client1
enrollment url http://10.1.1.1:80
subject-name CN=Client-1,OU=TAC,c=IN
revocation-check crl
auto-enroll 70 regenerate
```

> **注**:**auto-enrollコマンド**は、ルータの自動登録機能を有効にします。コマンド構文は**auto-enroll** [*val%*] [*regenerate*]です。

上記の出力では、自動登録機能は70 %として指定されています。つまり、[**lifetime of current_ID**_cert]の70%で、**ルータは自動的にCAに登録**し直されます。

> **ヒント**:PKIタイマーが正しく動作するように、auto-enrollの値を60 %以上に設定することを推奨します。

*regenerate*オプションは、証明書の再登録/更新を目的とした新しいRivest-Shamir-

Addleman(RSA)キーの作成に使用されます。このオプションを指定しない場合は、現在のRSAキーが使用されます。

# 自動登録の実行

自動登録機能を確認するには、次の手順を実行します。

1. クライアントルータのトラストポイントを手動で認証するには、**crypto pki authenticate**コマンドを入力します。

```
Client-1(config)#crypto pki authenticate client1
```

**注**：このコマンドの詳細については、『Cisco IOS Securityコマンドリファレンス』を参照してください。
コマンドを入力すると、次のような出力が表示されます。

```
Certificate has the following attributes:
Fingerprint MD5: 006B2E44 37FBC3F1 AA14F32B CDC4462E
Fingerprint SHA1: 2999CC53 8BF65247 C0D704E9 FDC73002 A33910D4

% Do you accept this certificate? [yes/no]:
```

2. クライアントルータでCA証明書を受け入れるために**yes**と入力します。次に、ルータで**RENEW**タイマーが開始されます。

```
Client-1#show crypto pki timer
PKI Timers
| 0.086
| 0.086 RENEW cvo-pki
| 9:51.366 SESSION CLEANUP
```

3. **RENEW**タイマーが**ゼロに**達すると、クライアントルータはID証明書を取得するために自動的にCAに登録します。証明書が受信されたら、**show crypto pki certificate**コマンドを入力して証明書を表示します。

```
Client-1#show crypto pki certificate
Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:16:57 IST Nov 25 2012
```

```
end date: 09:36:57 IST Nov 25 2012
renew date: 09:30:08 IST Nov 25 2012
Associated Trustpoints: client1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

更新日は09:30:08で、次のように計算されます。

開始時刻+ (%renewal of ID_cert_lifetime)

または

09:16:57 +（70% * 20分）= 09:30:08

PKIタイマーは同じことを反映します。

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:19:01.714 IST Sun Nov 25 2012
PKI Timers
| 1:21.790
| 1:21.790 SESSION CLEANUP
| 11:06.894  RENEW client1
```

4. RENEWタイマーが満了すると、ルータは新しいID証明書を取得するためにCAを使用して登録を変更します。証明書の更新が発生した後、show crypto pki certコマンドを入力して、新しいID証明書を表示します。

```
Client-1#show crypto pki cert
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:55.063 IST Sun Nov 25 2012
Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
```

```
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

更新日がなくなることに注意してください。代わりに、SHADOWタイマーが開始されます。

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922IST Sun Nov 25 2012
PKI Timers
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618 SHADOW client1
```

プロセスロジックは次のとおりです。

- IDCA証明書の終了日がCA証明書の終了日と等しくない場合は、自動登録の割合に基づいて更新日を計算し、RENEWタイマーを開始します。
- ID証明書の終了日がCA証明書の終了日と等しい場合は、現在のID証明書が有効である限り、現在のID証明書が有効であるため、更新プロセスは不要です。代わりに、SHADOWタイマーが開始されます。

このタイマーは、auto-enrollコマンドで指定したパーセンテージに基づいて計算されます。たとえば、前の例に示されている更新されたID証明書の有効期間の日付を検討します。

```
Validity Date of current ID cert:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
```

この証明書の有効期間は16分です。したがって、ロールオーバータイマー（つまりSHADOWタイマー）は16分の70 %で、約11分に相当します。この計算は、ルータが[09:30:09 + 00:11:00] = 09:41:09でシャドウ/ロールオーバー証明書の要求を開始することを意味します。これは、このドキュメントで前述したPKI SHADOWタイマーに対応しています。

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922 IST Sun Nov 25 2012
PKI Timers
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618  SHADOW client1
```

# 自動ロールオーバーの動作

この項では、動作する自動ロールオーバー機能について説明します。

## Cisco IOS CAサーバ

SHADOWタイマーが期限切れになると、ロールオーバー証明書がCAルータに表示されます。

```
RootCA#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:36:28.184 IST Sun Nov 25 2012
CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
 start date: 09:46:05 IST Nov 25 2012
end   date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
```

## クライアントルータ

このドキュメントで前述したように、自動登録機能はクライアントルータでSHADOWタイマーを開始しました。SHADOWタイマーの期限が切れると、自動登録機能により、ルータはロールオーバー/シャドウCA証明書をCAサーバに要求することができます。受信されると、ロールオーバー

/シャドウID証明書も照会します。その結果、ルータには2つの証明書ペアがあります。現在のペアと、ロールオーバー/シャドウ証明書を含むもう1つのペア：

```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: client1

Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
```

```
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

ロールオーバーID証明書の有効性に注意してください。

```
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
```

証明書の有効期間はわずか4分です（Cisco IOS CAサーバで設定されているように、予想される20分の代わりに）。 Cisco IOS CAサーバごとに、絶対ID証明書のライフタイム*は20分である必要があります(つまり、特定のクライアントルータでは、それに対して発行されるID証明書（現在の+シャドウ）のライフタイムの合計は20分以下である必要があります)。*

このプロセスの詳細は、次のとおりです。

- ルータの現在のID証明書の有効性を次に示します。

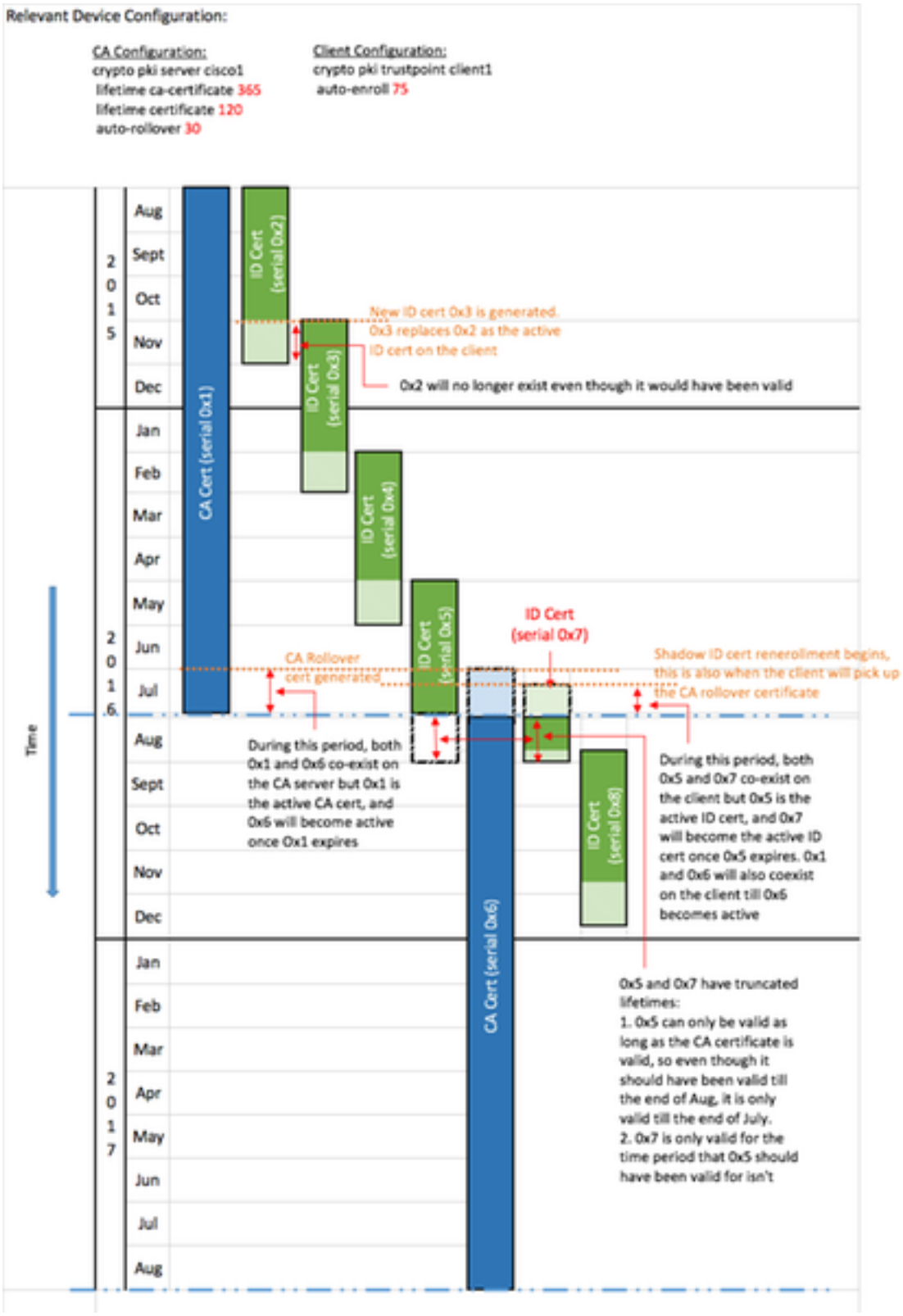
  ```
  start date: 09:30:09 IST Nov 25 2012
  end date: 09:46:05 IST Nov 25 2012
  ```

  したがって、*current_id_cert_lifetimeは16*分です。
- ロールオーバーID証明書の有効性を次に示します。

  ```
  start date: 09:46:05 IST Nov 25 2012
  end date: 09:50:09 IST Nov 25 2012
  ```

  したがって、*rollover_id_cert_lifetime*は4分です。
- Cisco IOSでは、[current_id_cert_lifetime]が[rollover_id_cert_lifetime]に追加される場合、[total_id_cert_lifetime]と等しくなければなりません。この場合もそうである。

# ロールオーバーと登録を使用したPKIタイムラインの例




# 重要な考慮事項

- PKIタイマーが正しく機能するには、正規のクロックが必要です。クライアントルータとCisco IOS CAルータの間でクロックを同期するために、NTPを使用することを推奨します。NTPがない場合は、ルータのシステム/ハードウェアクロックを使用できます。ハードウェアクロックを設定して正規のものにする方法については、『Basic System Management Configuration Guide, Cisco IOS Release 12.4T』を参照してください。

- ルータのリロード時に、NTPの同期に数分かかることがあります。ただし、PKIタイマーはほ

ぼ即時に確立されます。バージョン15.2(3.8)Tおよび15.2(4)Sでは、PKIタイマーはNTPの同期後に自動的に再評価されます。

- PKIタイマーは絶対ではありません。これらは残りの時間に基づいて、リブート後に再計算されます。たとえば、クライアントルータに100日間有効なID証明書があり、自動登録機能が80 %に設定されているとします。その後、再登録は80日後に行われる予定です。ルータが60日目にリロードされると、次に示すように、ルータは起動し、PKIタイマーを再計算します。 (*残時間*) * (*%auto-enroll*) = (100-60) * 80% = 32日

  したがって、[60 + 32] = 92日目に再登録が行われます。

- 自動登録タイマーと自動登録タイマーを設定する場合、PKIクライアントが自動登録タイマーを要求するときに、PKIサーバでSHADOW CA証明書を使用可能にする値を設定することが重要です。これにより、大規模な環境で発生する可能性のあるPKIサービスの障害を軽減できます。

# 関連情報

- Deploying Cisco IOS Security with a Public-Key Infrastructureホワイトペーパー
- 公開キーインフラストラクチャ：導入の利点と機能に関するホワイトペーパー
- 公開キー インフラストラクチャ構成ガイド
- テクニカル サポートとドキュメント – Cisco Systems