PKI

概要・基本設定

IPsec VPN の構築をサポートする PKI（Public Key Infrastructure）モジュールについて解説します。PKI モジュールを使うと、IPsec（ISAKMP）の相手認証に RSA デジタル署名（RSA Signature）を利用できるようになります。

✎ PKI モジュールを使用するにはフィーチャーライセンス AT-FL-06 が必要です。

✎ PKI は AR320 では使用できません。

PKI とは

PKI（Public Key Infrastructure）は、公開鍵暗号を安心して利用するための基盤技術です。公開鍵暗号の信頼性は、使用する公開鍵が本当に対象者のものであるかに依存しています。PKI システムでは、認証局（CA）が発行する公開鍵証明書により、公開鍵とその所有者の関係を証明する仕組みが提供されています。本製品では、オプションのフィーチャーライセンス AT-FL-06 をご購入いただくことにより、ITU-T X.509 勧告の定める公開鍵証明書を利用した PKI システムを使用することができます。PKI モジュールを使うことにより、IPsec VPN の相手ルーター認証に RSA デジタル署名を利用できるようになります。

IPsec と PKI

IPsec VPN では、通信開始に先立ち ISAKMP フェーズ 1 で相手機器（ルーターや VPN クライアント）の認証を行います。本製品がサポートしている相手認証方式は次の 2 つです。

- 事前共有鍵（pre-shared key）方式
  あらかじめ各ルーターに入力しておいたパスフレーズ（共有鍵）を使って相手を認証する方式。接続先の数だけ共有鍵を設定しておく必要がある。もっとも基本的な認証方式であり、オプションなしで使用できる。
- RSA デジタル署名（RSA Signature）方式
  相手から受け取ったデジタル署名を検証することによって相手を認証する方式。検証に必要な X.509 公開鍵証明書は署名と一緒に入手できるため、接続先ごとに情報を登録しておく必要がない。正当な相手かどうかは、認証局が証明書を発行しているかどうかによって判断される。PKI フィーチャーライセンスが必要。

VPN 機器の台数が多くなるにしたがい、事前共有鍵方式よりも RSA デジタル署名方式のほうが登録すべき鍵の数が少なくなるため、手間が軽減される傾向がありますが、どちらの方法を用いた場合でも IPsec VPN の機能自体に差異はありません。
RSA デジタル署名を用いる場合には、VPN 機器の他に X.509 証明書の発行や保管を行うコンピューターが必要となるため、事前共有鍵を用いた場合に比べて VPN システムの規模が大きくなり、証明書の維持や管理のコストが発生します。
しかし、PKI は本製品がサポートする IPsec VPN だけでなく、SSL / TLS や S / MIME などのセキュリティーアプリケーションでも利用できることから、すでに PKI をベースとしたセキュリティーポリシーのもとでこうしたアプリケーションが利用されている場合は、本製品による IPsec VPN をそのポリシーに統合できる

メリットがあります。

PKI の運用に必要なもの

本製品の IPsec VPN で PKI を使用するためには、以下のものが必要になります。

認証局

各ルーターに対して、認証局自身のデジタル署名を施した公開鍵証明書を発行します。また、期限切れ前に無効となった証明書の一覧（証明書失効リスト）を管理する役割もあります。通常、認証局は UNIX や Windows などの OS 上で動作するアプリケーションソフトウェアです。「CA（Certification Authority）」や「認証機関」などと呼ばれることもあります。

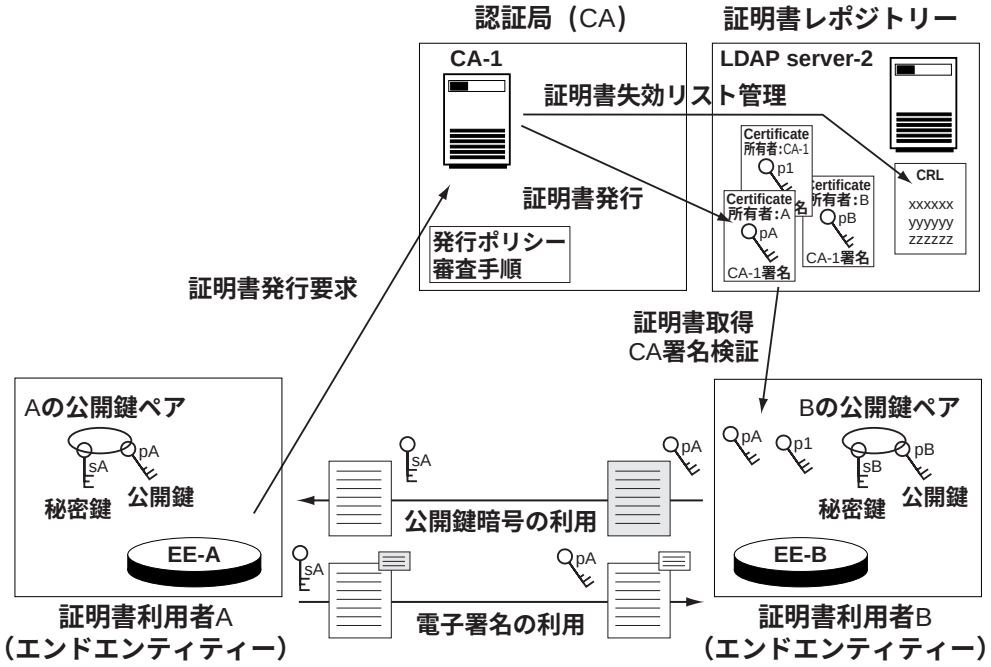
証明書レポジトリー

認証局が発行した公開鍵証明書や証明書失効リストを保管しているサーバーです。通常、LDAP などのディレクトリーサーバーが使用されます。認証局と同じく、コンピューター上で動作する 1 アプリケーションです。認証局と同じコンピューター上で動作させる場合と、別のコンピューターで動作させる場合があります。また認証局によっては、レポジトリーを持たず、発行した証明書をファイルに書き出すだけのものもあります。

IPsec ルーター

IPsec プロトコル群をサポートする VPN 構築用のルーターです。本製品は、暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着することにより、IPsec ルーターとして機能します。VPN ルーター、セキュリティーゲートウェイなどと呼ばれることもあります。また、PKI の用語では、PKI を利用するものという意味でエンドエンティティー（EE = End Entity）と呼びます。通常、PKI は認証局（CA）、証明書レポジトリー、エンドエンティティー（EE）の 3 要素で構成されます。

✎ 暗号・圧縮ボード（AR011）は AR700 シリーズでのみ使用できます。



CA 証明書

認証局自身の公開鍵証明書です。添付の公開鍵が間違いなく認証局のものであることを示しています。CA 証明書は、認証局が発行した他のルーターの証明書が正しいものであるかどうかを検証するために用いられます。公開鍵証明書には、識別名（DN = Distinguished Name）と呼ばれる名前が付けられています。CA 証明書の場合、識別名は CA の名前になります。また、CA 証明書には有効期限が設定されています。認証局が 1 つしかない場合、CA 証明書は認証局自身が自署して発行することになります。複数認証局がある場合は、認証局をツリー上の階層構造にして、上位の認証局が下位の認証局の証明書を発行します。ツリーの最上位に位置する認証局は、自分自身で証明書を発行します。最上位の認証局をルート認証局と呼び、その認証局の証明書はルート CA 証明書と呼びます。認証局が 1 つしかない場合、その証明書はルート CA 証明書となります。

エンドエンティティー証明書

エンドエンティティーである IPsec ルーターの公開鍵証明書です。各ルーターからの要求を受けて、認証局が発行します。ルーター A の公開鍵証明書は、添付の公開鍵がルーター A のものであることを証明する文書です。証明書には認証局のデジタル署名が施されているため、各ルーターでは、CA 証明書に添付されている認証局の公開鍵を用いて、第三者による改変がされていないか確認することができます。エンドエンティティー証明書には、各ルーターを区別するための識別名（DN = Distinguished Name）と呼ばれる名前が付けられています。また、エンドエンティティー証明書には有効期限が設定されています。

証明書失効リスト

何らかの理由により有効期限前に無効となったエンドエンティティー証明書の一覧です。失効の理由として

は、証明書記載内容（アドレス等）の変更や該当エンドエンティティーの運用停止などが挙げられます。証明書失効リストは、認証局が管理するもので、失効した証明書のシリアル番号が列挙されています。通常は、証明書レポジトリー上に置かれており、各エンドエンティティーが随時ダウンロードして利用できます。CRL（Certificate Revocation List）とも呼ばれます。

識別名

公開鍵証明書には、証明書に添付された公開鍵の所有者を示す名前が付けられています。たとえば、ルーター A の公開鍵証明書には、ルーター A を一意に識別できる名前が付けられています。この名前を識別名（DN = Distinguished Name）と呼びます。識別名は、c（国）、o（組織）、名前（cn）のようなさまざまな属性を組み合わせたもので、郵便で使われる住所やインターネットで使われるドメイン名と似ています。たとえば、ルーター A の識別名として、次のような名前を付けることができます。

```
cn=RouterA,o=allied,c=jp
```

識別名は次のような構文で表します。

```
DISTNAME=“[cn=common-name, ]
  [list of [dc=domain-name-component, ]]
  [ou=organisation-unit-name, ] [o=organisation-name, ]
  [street=street-address, ] [st=state-or-province-name, ]
  [l=locality-name, ] [c=country-name, ]”
```

属性名	名称	説明
cn	Common Name（一般名）	名前を示す文字列
dc	Domain Component（ドメイン構成要素）	インターネットドメイン名の構成要素をカンマ区切りで列挙したもの。たとえば、foo.bar.com というドメイン名に対応する dc 属性は、”dc=foo, dc=bar, dc=com”のようになる
ou	Organisation Unit	
o	Organisation（組織名）	組織を示す文字列
street	Street Address（街区住所）	所在地（住所）を示す文字列
st	State（州/県など）	所在地（住所）を示す文字列
l	Locality Name	
c	Country Name（国名）	国コード（ISO3166）

表 1: X.500 識別名の属性

識別名では、属性の順序が重要な意味を持ちます。通常は、詳細なもの（cn など）から大まかなもの（c など）の順に記述します。

本製品の IPsec VPN では、個々のルーターの識別名は管理者が決定しますが、利用する認証局のポリシーによって使用できる属性に制限があるため、認証局の管理者と相談して決めてください。

LDAP URL

LDAP（Lightweight Directory Access Protocol）ディレクトリー上のファイルは、LDAP 用の URL（Universal Resource Locator）で表すことができます。LDAP URL は次のような形式になります。

```
ldap://address[:port]/[base-object]
```

address	LDAP サーバーの IP アドレスかホスト名
port	LDAP サーバーのポート番号（1〜65535）
base-object	ファイルの識別名（DN）

表 2: LDAP URL の要素

IPsec VPN 構築のための PKI 設定手順

デジタル署名を使用して VPN を構築する場合の設定手順について説明します。

1. 認証局に証明書の発行を要求する。
   証明書発行要求は、RSA Laboratories の定める PKCS#10 形式ファイルによるオフライン要求と、RFC2510 などで定められている PKIX-CMP プロトコルによるオンライン要求があります。どちらの方式を使用するかは、認証局の管理者にご相談ください。なお、証明書を要求するにあたっては、証明対象となる自分自身の RSA 公開鍵ペアを作成し、また、自分の識別名を設定しておく必要があります。

   ■ 証明書の発行対象となる RSA 公開鍵ペアを作成するには CREATE ENCO KEY コマンド（「暗号・圧縮」の 18 ページ）を使います。

   ```
   CREATE ENCO KEY=0 TYPE=RSA LENGTH=1024 ↵
   ```

   ■ 公開鍵証明書の発行を要求するには、ルーター自身の X.500 識別名（DN = Distinguished Name）を設定しておく必要があります。これは、SET SYSTEM DISTINGUISHEDNAME コマンド（「運用・管理」の 277 ページ）で行います。DN の属性（c、o、cn など）は小文字で記述する必要がありますのでご注意ください。

   ```
   SET SYSTEM DISTINGUISHEDNAME="cn=RouterA,o=birds,c=jp" ↵
   ```

   ■ PKI で使用される時刻は UTC（協定世界時）なので、ルーターを使用している地域の現地時間と UTC との時差を設定しておきます。

   ```
   SET NTP UTCOFFSET=JST ↵
   ```

   ■ 証明書発行要求（CSR）を作成するには、CREATE PKI ENROLLMENTREQUEST コマンド（18 ページ）を使います。手動方式（PROTOCOL=MANUAL）では、発行要求がファイルに書き出されますので、そのファイルを認証局（CA）に渡して証明書の発行を依頼してください。ファイル名は ENROLLMENTREQUEST パラメーターに指定した名前に拡張子「.csr」が付いたものになります。また、ファイルの形式は PKCS#10 形式とします。

```
CREATE PKI ENROLLMENTREQUEST=mycer PROTO=MANUAL KEYPAIR=0 TYPE=PKCS10
  FORMAT=PEM ↵
```

■ 手動方式の場合、作成した証明書発行要求（CSR）ファイルを別のコンピューターにアップロードします。アップロードしたファイルを CA アプリケーションに渡し、証明書の発行を依頼してください。

```
UPLOAD FILE=mycer.cer SERVER=192.168.1.5 ↵
```

■ 証明書発行要求を直接 CA に送信するには、CA が CMP（Certificate Management Protocol）をサポートしている必要があります。その場合、証明書の形式は PKIX（デフォルト）とします。REFERENCE（参照番号）と SECRET（承認コード）については、CA の管理者に確認した上で入力してください。

```
CREATE PKI ENROLLMENTREQUEST=mycer PROTO=CMP KEYPAIR=0 REF=98765432
  SECRET=fugafuga LOCATION=192.168.1.5 ↵
```

✎ ご利用の認証局によっては、承認コードのフォーマットが本製品の期待しているものと異なる場合があります。たとえば、Entrust 社の認証局は「SLS7-6PNC-TWPR」のようなフォーマットですが、この場合ハイフンと最終桁のチェックストリングは入力不要です。

2. 発行された証明書をルーターの証明書データベースに登録する。
認証局によって発行された証明書は、証明書レポジトリー（LDAP サーバーなど）に置かれる場合と、ファイルで提供される場合があります。レポジトリー上に置かれている場合は、LDAP によってルーターの証明書データベースに直接ロードできます。一方、ファイルで提供された場合は、TFTP 等でいったんルーターのファイルシステム上に転送した上で、証明書データベースに登録します。
いずれの場合も、ロードした証明書が正しいかどうかを検証するため、CA 証明書が必要になります。最初に CA 証明書を登録してください。

■ 証明書が LDAP レポジトリーに置かれている場合は、ADD PKI CERTIFICATE コマンド（13 ページ）を使って、レポジトリーから直接データベースに取り込むことができます。最初に CA 証明書を登録します。LOCATION パラメーターに、CA 証明書を示す LDAP URL を指定してください。CERTIFICATE パラメーターに指定する文字列は、証明書データベース内で各証明書を識別するための名前で任意です。TYPE パラメーターには CA 証明書であることを示す「CA」を指定します。

```
ADD PKI CERTIFICATE=cacert LOCATION="ldap://172.16.10.1/o=test,c=jp"
  TYPE=CA ↵
```

■ 証明書がファイルで提供されている場合は、TFTP サーバーなどを利用して、CA 証明書ファイルをいったんルーターのファイルシステム上にダウンロードします。証明書ファイルの拡張子は.cer とします。

```
LOAD FILE=ca.cer SERVER=192.168.1.5 ↵
```

次に、ダウンロードした認証局の証明書ファイルをシステムの証明書データベースに登録します。TYPE パラメーターには CA 証明書であることを示す「CA」を指定します。

```
ADD PKI CERTIFICATE=cacer LOCATION=ca.cer TYPE=CA ↵
```

■ CA 証明書を登録したら、SHOW PKI CERTIFICATE コマンド（43 ページ）を実行して CA 証明書の内容を表示し、別途入手したプリントアウト等と見比べ、間違いなく CA の証明書であるかどうかを検証してください。

```
SHOW PKI CERTIFICATE=cacer ↵
```

✎ 証明書内容の検証方法については、認証局の管理者にご確認ください。

■ 確認ができたら、CA 証明書を信頼できるものとして受け入れるため、次のコマンドを実行します。これは、CA 証明書「cacer」を信頼するという意思表示です。これを実行しないと、CA 証明書を使用できません。

```
SET PKI CERTIFICATE=cacer TRUSTED=TRUE ↵
```

✎ CA 証明書を登録する際、直接認証局から証明書を入手したりして CA 証明書の信頼性が極めて高いと考えられるときは、ADD PKI CERTIFICATE コマンド（13 ページ）を実行するときに TRUSTED=TRUE を付けることで、証明書の確認を省略することができます。ただし、証明書すり替え等のリスクを十分認識した上で行ってください。

■ CA 証明書を登録したら、次に発行された自分の証明書を登録します。証明書がレポジトリーに置かれている場合は、ADD PKI CERTIFICATE コマンド（13 ページ）を使って、レポジトリーから直接データベースに取り込むことができます。LOCATION パラメーターに、自分の証明書を示す LDAP URL を指定してください。TYPE パラメーターには自分自身の証明書であることを示す「SELF」を指定します。

```
ADD PKI CERTIFICATE=mycert
  LOCATION="ldap://172.16.10.1/cn=RouterA,o=birds,c=jp" TYPE=SELF ↵
```

■ 証明書がファイルで提供されている場合は、TFTP サーバーなどを利用して、自分の証明書ファイルをいったんルーターのファイルシステム上にダウンロードします。証明書ファイルの拡張子は.cer とします。

```
LOAD FILE=mine.cer SERVER=192.168.1.5 ↵
```

次に自分自身の証明書をデータベースに登録します。

```
ADD PKI CERTIFICATE=mycer LOCATION=mine.cer TYPE=SELF ↵
```

3. 証明書失効リスト（CRL）をルーターの CRL データベースに登録する。
認証局が証明書失効リスト（CRL）をサポートしている場合、リストを CRL データベースにロードすることにより、他者の証明書が失効していないかどうかを確認できるようになります。証明書失効リストも、レポジトリーに置かれる場合とファイルで提供される場合があります。証明書のロードと同様の操作でリストを登録してください。LDAP レポジトリーに置かれている場合は、指定した間隔でリストを自動更新することも可能です。

■ 証明書失効リストがLDAPレポジトリーに置かれている場合は、ADD PKI CRLコマンド（15ページ）で直接データベースに登録できます。CRLのLDAP URLについては、認証局の管理者にご確認ください。LDAPサーバーからCRLを登録した場合は、一定の間隔でCRLの自動取得・更新が行われます。更新間隔のデフォルトは24時間ですが、SET PKIコマンド（32ページ）のCRLUPDATEPERIODパラメーターで変更も可能です。

```
ADD PKI CRL=ourcrl
  LOCATION="ldap://172.16.10.1/cn=crl1,o=test,c=jp" ↵
```

■ CRLがファイルで提供されている場合は、TFTPサーバーなどを利用して、CRLファイルをいったんルーターのファイルシステム上にダウンロードします。CRLファイルの拡張子は.crlとします。

```
LOAD FILE=ca.crl SERVER=192.168.1.5 ↵
```

次にCRLファイルを指定して、CRLをデータベースに登録します。

```
ADD PKI CRL=ca_crl LOCATION=ca.crl ↵
```

✎ CRLをファイルから登録した場合は、認証局がCRLを更新するたびにルーターの管理者が手動で上記の手順を再実行し、ルーターのデータベース上のCRLを更新する必要があります。

4. IPsecの設定を行う

ISAKMPポリシーの作成時に、認証方式としてRSAデジタル署名（RSASIG）を指定し、自分のRSA公開鍵ペアを指定することにより、デジタル署名を利用したIPsecが利用できるようになります。実際のIPsec通信時には、ISAKMP/IKEプロトコルにより、接続相手の証明書を自動的に確認します。これ以降は、ロードされた証明書や証明書失効リストを用いて接続相手の認証を自動的に行います。

■ IPsecルーターのグローバルIPアドレスが固定されている場合、次のようにしてISAKMPポリシーを作成します。PEERには相手ルーターのアドレスを、AUTHTYPEにはRSAデジタル署名を示すRSASIGを、LOCALRSAKEYには自分のRSA公開鍵ペアの番号を指定します。

```
CREATE ISAKMP POLICY=i PEER=12.34.56.78 AUTHTYPE=RSASIG LOCALRSAKEY=1
  SENDN=TRUE ↵
```

■ 片一方のIPsecルーターのグローバルIPアドレスが固定されていない場合（ダイヤルアップ環境など）は、アドレス固定側と不定側で設定が異なります。
アドレスが一定のセンター側では、次のようにしてISAKMPポリシーを作成します。PEERには相手ルーターのアドレスが不定なためANYを指定し、さらにREMOTEIDパラメーターで相手の識別名を指定します。AUTHTYPEにはRSAデジタル署名を示すRSASIGを、LOCALRSAKEYには自分のRSA公開鍵ペアの番号を指定します。

```
CREATE ISAKMP POLICY=i PEER=ANY AUTHTYPE=RSASIG LOCALRSAKEY=1
  SENDN=TRUE REMOTEID="cn=RouterB,o=birds,c=jp" ↵
```

一方、アドレスが不定のリモート側では、次のようにしてISAKMPポリシーを作成します。PEERにはセンター側ルーターのIPアドレスを指定します。AUTHTYPEにはRSAデジタル署名を示すRSASIGを、LOCALRSAKEYには自分のRSA公開鍵ペアの番号を指定します。

```
CREATE ISAKMP POLICY=i PEER=12.34.43.21 AUTHTYPE=RSASIG LOCALRSAKEY=1
  SENDN=TRUE ↵
```

なお、認証方式に RSA デジタル署名を使うときは、片側のアドレスが不定でも Aggressive モードを使う必要はありません。デフォルトの Main モードを使用します。

5. 証明書を更新する
   証明書には有効期限があるため、継続して使用する場合は有効期限が満了する前に手順 1 からの手順を再度行う必要があります。

コマンドリファレンス編

機能別コマンド索引

ADD PKI CERTIFICATE

カテゴリー：PKI / 証明書データベース
対象機種：AR300 V2、AR300L V2、AR720、AR740

ADD PKI CERTIFICATE=*cert-name* LOCATION={***url*|***filename***}
[PASSWORD=*password*] [PROXYADDRESS={*hostname*|*ipadd*}] [PROXYPORT=*port*]
[TRUSTED={TRUE|FALSE|YES|NO|ON|OFF}] [TYPE={CA|SELF|ENDENTITY|EE}]
[USERNAME=*username*]

cert-name: 証明書名（1〜24 文字。空白を含む場合はダブルクォートで囲む）
url: URL（LDAP または HTTP）
filename: ファイル名（拡張子は.cer）
password: パスワード（1〜64 文字）
hostname: ホスト名
ipadd: IP アドレス
port: TCP ポート番号（1〜65535）
username: ユーザー名（1〜64 文字）

解説

証明書データベースに公開鍵証明書を登録する。
証明書は、ファイルシステム上のファイル（.cer）から取り込むことも、リモートのレポジトリーから LDAP または HTTP 経由で直接取り込むこともできる。

パラメーター

CERTIFICATE　証明書の名前。システム上で証明書を識別するためのもので、任意の名前を付けることができる。

LOCATION　証明書のある場所。ファイルシステム上のローカルファイルから取り込むときは、証明書ファイル（.cer）の名前を指定する。レポジトリーからダウンロードするときは、LDAP サーバーか HTTP サーバーの URL を指定する。

PASSWORD　レポジトリーにアクセスするためのパスワード

PROXYADDRESS　（HTTP）プロキシーサーバーの IP アドレスまたはホスト名

PROXYPORT　（HTTP）プロキシーサーバーのポート番号

TRUSTED　登録する証明書を自動的に信頼するかどうか。TRUE（YES、ON も同じ）を指定した場合は、証明書の形式が不正であったり効力を失っていたりした場合でも、無条件で信頼できるものとして扱う。FALSE（NO、OFF も同じ）を指定した場合は、信頼できる他の証明書に付属の公開鍵ペアによる署名があってはじめて、この証明書を信頼できるものと見なす。デフォルトは FALSE。なんらかの方法により証明書の指紋（fingerprint）を確認できるときは、本コマンド実行時に TRUSTED=FALSE を指定し（TRUSTED パラメーターを省略しても同じ）、SHOW PKI CERTIFICATE コマンドで証明書の内容を確認してから、SET PKI CERTIFICATE コマンドで TRUSTED=TRUE を指定して証明書を信頼できるものとして設定することが望ましい。

TYPE　証明書の種類。CA（CA 証明書）、SELF（ルーター自身の証明書）、EE または ENDENTITY（他のエンドエンティティーの証明書）から選択する。デフォルトは ENDENTITY

USERNAME　レポジトリーにアクセスするためのユーザー名

例

■LDAP サーバー 192.168.10.5 から、DN（識別名）「cn=routera,o=myorg,c=jp」を持つ自分自身の証明書をダウンロードして登録する。

```
ADD PKI CERTIFICATE=routera
  LOCATION="ldap://192.168.10.5/cn=routera,o=myorg,c=jp" TYPE=SELF
```

関連コマンド

DELETE PKI CERTIFICATE（22 ページ）
SET PKI CERTIFICATE（33 ページ）
SHOW PKI CERTIFICATE（43 ページ）

ADD PKI CRL

カテゴリー：PKI / CRL データベース
対象機種：AR300 V2、AR300L V2、AR720、AR740

ADD PKI CRL=*crl-name* LOCATION={***url***|***filename***} [PASSWORD=*password*]
[PROXYADDRESS={*hostname*|*ipadd*}] [PROXYPORT=*port*] [USERNAME=*username*]

crl-name: CRL 名（1〜24 文字。空白を含む場合はダブルクォートで囲む）
url: URL（LDAP または HTTP）
filename: ファイル名（拡張子は.crl）
password: パスワード（1〜64 文字）
hostname: ホスト名
ipadd: IP アドレス
port: TCP ポート番号（1〜65535）
username: ユーザー名（1〜64 文字）

解説

CRL データベースに証明書失効リスト（CRL = Certificate Revocation List）を登録する。
CRL は、ファイルシステム上のファイル（.crl）から取り込むことも、リモートのレポジトリーから LDAP または HTTP 経由で直接取り込むこともできる。
ルーターは指定された場所から CRL を定期的に取り込み、CRL データベースを更新する。更新間隔は SET PKI コマンドの CRLUPDATEPERIOD パラメーターで変更できる。

パラメーター

CRL　CRL の名前。システム上で CRL を識別するためのもので、任意の名前を付けることができる。
LOCATION　CRL のある場所。ファイルシステム上のローカルファイルから取り込むときは、証明書ファイル（.crl）の名前を指定する。レポジトリーからダウンロードするときは、LDAP サーバーか HTTP サーバーの URL を指定する。
PASSWORD　レポジトリーにアクセスするためのパスワード
PROXYADDRESS　（HTTP）プロキシーサーバーの IP アドレスまたはホスト名
PROXYPORT　（HTTP）プロキシーサーバーのポート番号
USERNAME　レポジトリーにアクセスするためのユーザー名

例

■LDAP サーバー 192.168.10.5 から、DN（識別名）「cn=potecrl,o=myorg,c=jp」を持つ証明書失効リスト（CRL）をダウンロードして登録する。

```
ADD PKI CRL=potecrl
  LOCATION="ldap://192.168.10.5/cn=potecrl,o=myorg,c=jp"
```

関連コマンド

DELETE PKI CRL（23 ページ）
SET PKI（32 ページ）
SHOW PKI CRL（46 ページ）

ADD PKI LDAPREPOSITORY

カテゴリー：PKI / 証明書レポジトリー
対象機種：AR300 V2、AR300L V2、AR720、AR740

ADD PKI LDAPREPOSITORY=*repos-name* LOCATION=*url* [PASSWORD=*password*]
[USERNAME=*username*]

repos-name: レポジトリー名（1〜24 文字。空白を含む場合はダブルクォートで囲む）
url: URL（LDAP）
password: パスワード（1〜64 文字）
username: ユーザー名（1〜64 文字）

解説

リモートレポジトリーの情報（URL、ユーザー名、パスワード）を登録する。
本コマンドでレポジトリーを登録している場合、システムは必要な証明書をレポジトリーから自動的に取得する。

パラメーター

LDAPREPOSITORY　リモートレポジトリーの名前。システム上でレポジトリーを識別するためのもので、任意の名前を付けることができる。
LOCATION　レポジトリー（LDAP サーバー）の URL
PASSWORD　レポジトリーにアクセスするためのパスワード
USERNAME　レポジトリーにアクセスするためのユーザー名

例

■LDAP レポジトリーを登録する。

```
ADD PKI LDAPREPOSITORY=myorg_repository LOCATION="ldap://192.168.10.5"
```

関連コマンド

DELETE PKI LDAPREPOSITORY（24 ページ）
SET PKI LDAPREPOSITORY（35 ページ）
SHOW PKI LDAPREPOSITORY（51 ページ）

CREATE PKI ENROLLMENTREQUEST

カテゴリー：PKI / 証明書発行要求
対象機種：AR300 V2、AR300L V2、AR720、AR740

CREATE PKI ENROLLMENTREQUEST=*csr-name* KEYPAIR=*key-id* [FORMAT={DER|PEM|BASE64}] [LOCATION={*hostname*|*ipadd*}] [PROTOCOL={CMP|MANUAL}] [REFERENCENUMBER=*refnum*] [SECRETVALUE=*password*] [TYPE={PKCS10|PKIX}]

csr-name: 証明書発行要求名（1〜24 文字。ただし、PROTOCOL=MANUAL のときは 1〜8 文字）
key-id: 鍵番号（0〜65535）
hostname: ホスト名
ipadd: IP アドレス
refnum: 参照番号（1〜24 文字）
password: パスワード（1〜24 文字）

解説

公開鍵証明書の発行要求を作成する。
発行要求は、自分の公開鍵ペアに対する公開鍵証明書の作成を認証局（CA）に依頼するためのもので、CMP プロトコルにより直接 CA に送信する方法と、発行要求をファイルに書き出し手動で CA に渡す方法がある。
発行要求を作成するには、あらかじめ SET SYSTEM DISTINGUISHEDNAME コマンドで自分の識別名（DN）を設定しておく必要がある。

パラメーター

ENROLLMENTREQUEST　個々の証明書発行要求を識別するための名前。手動方式では、この名前が発行要求ファイルのベースファイル名にもなる（名前が name なら、ファイル名は name.csr となる）。

KEYPAIR　証明書の発行対象となる RSA 鍵ペアの番号（CREATE ENCO KEY コマンドで指定した鍵番号）

FORMAT　手動方式における、証明書発行要求ファイルのエンコード形式。DER はバイナリーの DER（Distinguished Encoding Rules）形式、PEM は BASE64 エンコードし前後にマークを付けた PEM（Privacy Enhanced Mail）形式、BASE64 は純粋な BASE64 形式。本パラメーターは、PROTOCOL に MANUAL を指定したときのみ有効。デフォルトは DER

LOCATION　CA のホスト名または IP アドレス。PROTOCOL に CMP を指定したときのみ有効

PROTOCOL　証明書発行要求を CA に提出する方法。CMP を指定した場合は、PKI Certificate Management Protocol（CMP）を使って直接 CA に要求を送信する。MANUAL を指定した場合は、発行要求をルーターのファイルシステム上にファイルとして書き出す。ファイル名は、ENROLLMENTREQUEST パラメーターで指定した名前を name として、「name.csr」の形式となる。手動の場合は、このファイルをなんらかの手段によって CA に送ることで証明書の発行を依頼する。デフォルトは CMP。

REFERENCENUMBER　CMP による自動方式で必要な参照番号。CA の管理者によって指定されたものを入力する。手動方式の場合は不要。

SECRETVALUE　CMP による自動方式で必要な承認コード（パスワード）。CA の管理者によって指定されたものを入力する。

TYPE　証明書発行要求の形式。ファイルによる手動方式で使われる PKCS10（PKCS#10 形式）と、CMP プロトコルで使用される PKIX（RFC2511）形式がある。CMP を使うときは PKIX でなくてはならない。デフォルトは PKIX。

入力・出力・画面例

PROTOCOL=MANUAL **時に書き出される証明書発行要求ファイルの形式**

■ DER（Distinguished Encoding Rules）**形式（バイナリーダンプ）**

```
00000000  30 81 f9 30 81 84 02 01  00 30 00 30 7d 30 0d 06  |0..0.....0.0}0..|
00000010  09 2a 86 48 86 f7 0d 01  01 01 05 00 03 6c 00 30  |.*.H.........l.0|
00000020  69 02 61 00 bf 65 95 3e  4f 79 9c c9 02 40 74 9f  |i.a..e.>Oy...@t.|
00000030  83 e9 47 bc de b2 06 6e  93 7f 96 16 f5 27 0a 0f  |..G....n.....'..|
00000040  cc 54 6b 92 f7 09 b9 b3  c3 6a 62 f2 c5 19 61 79  |.Tk......jb...ay|
00000050  c6 3b 35 e2 11 a1 32 60  6e f4 24 9b aa 78 61 a9  |.;5...2`n.$..xa.|
00000060  24 f4 24 05 92 39 ba a4  2d e0 d5 55 fc fc b7 10  |$.$..9..-..U....|
00000070  c5 92 d8 df 52 c4 c9 8e  cf 27 5e dd 43 8c f0 7f  |....R....'^.C...|
00000080  e2 de 6a 7d 02 04 00 01  00 01 30 0d 06 09 2a 86  |..j}......0...*.|
00000090  48 86 f7 0d 01 01 05 05  00 03 61 00 0c c5 94 b3  |H.........a.....|
000000a0  d6 0f b7 cb 71 de 0e cf  db d9 78 6c cf 09 3b 2a  |....q.....xl..;*|
000000b0  10 34 b2 c9 f3 0b 8e 62  6b 3f 7b 5c 94 a8 a5 eb  |.4.....bk?{\....|
000000c0  40 48 5a dd 57 34 06 a5  e4 3e 7c b8 56 ab 1f 00  |@HZ.W4...>|.V...|
000000d0  6e a5 90 34 d5 92 33 af  74 22 54 02 63 86 a7 90  |n..4..3.t"T.c...|
000000e0  74 f8 ae 89 bf 4b bb 7a  a2 49 29 bc e4 92 64 6e  |t....K.z.I)...dn|
000000f0  b4 90 40 a9 bc ff 18 68  ec 85 32 02              |..@....h..2.|
000000fc
```

■ PEM（Privacy Enhanced Mail）**形式**

```
-----BEGIN CERTIFICATE REQUEST-----
MIH5MIGEAgEAMAAwfTANBgkqhkiG9w0BAQEFAANsADBpAm
EAv2WVPk95nMkCQHSfg+lHvN6yBm6Tf5YW9ScKD8xUa5L3
Cbmzw2pi8sUZYXnGOzXiEaEyYG70JJuqeGGpJPQkBZI5uq
Qt4NVV/Py3EMWS2N9SxMmOzyde3UOM8H/i3mp9AgQAAQAB
MA0GCSqGSIb3DQEBBQUAA2EADMWUs9YPt8tx3g7P29l4bM
8JOyoQNLLJ8wuOYms/e1yUqKXrQEha3Vc0BqXkPny4Vqsf
AG6lkDTVkjOvdCJUAmOGp5B0+K6Jv0u7eqJJKbzkkmRutJ
BAqbz/GGjshTIC
-----END CERTIFICATE REQUEST-----
```

■ Base64 **形式**

```
MIH5MIGEAgEAMAAwfTANBgkqhkiG9w0BAQEFAANsADBpAm
EAv2WVPk95nMkCQHSfg+lHvN6yBm6Tf5YW9ScKD8xUa5L3
Cbmzw2pi8sUZYXnGOzXiEaEyYG70JJuqeGGpJPQkBZI5uq
Qt4NVV/Py3EMWS2N9SxMmOzyde3UOM8H/i3mp9AgQAAQAB
MA0GCSqGSIb3DQEBBQUAA2EADMWUs9YPt8tx3g7P29l4bM
8JOyoQNLLJ8wuOYms/e1yUqKXrQEha3Vc0BqXkPny4Vqsf
AG6lkDTVkjOvdCJUAmOGp5B0+K6Jv0u7eqJJKbzkkmRutJ
```

```
BAqbz/GGjshTIC
```

例

■RSA 鍵ペア「0」に対する公開鍵証明書の発行を CA「192.168.10.5」に要求する。要求は、PKIX-CMP プロトコルを使って直接 CA に送信する。

```
CREATE PKI ENROLL=mycert PROT=CMP KEYPAIR=0 REF=98765432 SEC=ABCDEFGH
  LOC=192.168.10.5
```

■RSA 鍵ペア「0」に対する公開鍵証明書の発行要求ファイルを作成する。ファイル形式は PKCS#10 で、メール添付用の PEM エンコーディングを指定する。ファイルは「mycerreq.csr」の名前で作成される。このファイルを CA に送ることで鍵ペア「0」の証明書発行を依頼できる。

```
CREATE PKI ENROLL=mycerreq PROT=MANUAL KEYPAIR=0 FORMAT=PEM TYPE=PKCS10
```

備考・注意事項

本コマンドは設定ファイルに記述しても無効なので注意。
Entrust 社の CA では、承認コードが「XXXX-XXXX-XXXX」のような形式だが、SECRETVALUE パラメーターで指定するときはハイフンと最終桁のチェックコードは入力しなくてよい。

関連コマンド

DESTROY PKI ENROLLMENTREQUEST（25 ページ）
SET SYSTEM DISTINGUISHEDNAME（「運用・管理」の 277 ページ）
SHOW PKI ENROLLMENTREQUEST（48 ページ）

CREATE PKI KEYUPDATEREQUEST

カテゴリー：PKI / 公開鍵更新要求
対象機種：AR300 V2、AR300L V2、AR720、AR740

CREATE PKI KEYUPDATEREQUEST=*req-name* CERTIFICATE=*cert-name*
KEYPAIR=*key-id* [LOCATION={*hostname*|*ipadd*}]

req-name: 鍵更新要求名（1〜24 文字。空白を含む場合はダブルクォートで囲む）
cert-name: 証明書名（1〜24 文字。空白を含む場合はダブルクォートで囲む）
key-id: 鍵番号（0〜65535）
hostname: ホスト名
ipadd: IP アドレス

解説

CMP をサポートしている認証局（CA）に対して、発行済みの公開鍵証明書に添付されている RSA 公開鍵の更新を要求する。
本コマンドを実行するには、自分の鍵ペアに対する公開鍵証明書が発行されており、それがルーターの証明書データベースに登録されている必要がある。また、公開鍵証明書が有効期限内でなくてはならない。

パラメーター

KEYUPDATEREQUEST　更新要求を識別するための名前
CERTIFICATE　対象となる公開鍵証明書の名前。証明書データベースの登録名を指定する。
KEYPAIR　新しい RSA 鍵ペアの番号
LOCATION　CA のホスト名または IP アドレス

関連コマンド

DESTROY PKI KEYUPDATEREQUEST（26 ページ）
SHOW PKI KEYUPDATEREQUEST（50 ページ）

DELETE PKI CERTIFICATE

カテゴリー：PKI / 証明書データベース
対象機種：AR300 V2、AR300L V2、AR720、AR740

DELETE PKI CERTIFICATE={***cert-name***|**ALL**}

cert-name: 証明書名（1〜24 文字。空白を含む場合はダブルクォートで囲む）

解説

証明書データベースに登録されている公開鍵証明書を削除する。

パラメーター

CERTIFICATE　証明書の名前。ADD PKI CERTIFICATE コマンドで指定したもの。

関連コマンド

ADD PKI CERTIFICATE（13 ページ）
SET PKI CERTIFICATE（33 ページ）
SHOW PKI CERTIFICATE（43 ページ）

DELETE PKI CRL

カテゴリー：PKI / CRL データベース
対象機種：AR300 V2、AR300L V2、AR720、AR740

DELETE PKI CRL={***crl-name***|**ALL**}

crl-name: CRL 名（1〜24 文字。空白を含む場合はダブルクォートで囲む）

解説

CRL（証明書失効リスト）データベースから CRL を削除する。

パラメーター

CRL　CRL の名前。ADD PKI CRL コマンドで指定したもの。

関連コマンド

ADD PKI CRL（15 ページ）
SET PKI CRL（34 ページ）
SHOW PKI CRL（46 ページ）

DELETE PKI LDAPREPOSITORY

カテゴリー：PKI / 証明書レポジトリー
対象機種：AR300 V2、AR300L V2、AR720、AR740

DELETE PKI LDAPREPOSITORY={***repos-name***|**ALL**}

repos-name: レポジトリー名（1〜24 文字。空白を含む場合はダブルクォートで囲む）

解説

リモートレポジトリーの情報（URL、ユーザー名、パスワード）を削除する。

パラメーター

LDAPREPOSITORY　リモートレポジトリーの名前。ADD PKI LDAPREPOSITORY コマンドで指定したもの。

関連コマンド

ADD PKI LDAPREPOSITORY（17 ページ）
SET PKI LDAPREPOSITORY（35 ページ）
SHOW PKI LDAPREPOSITORY（51 ページ）

DESTROY PKI ENROLLMENTREQUEST

カテゴリー：PKI / 証明書発行要求
対象機種：AR300 V2、AR300L V2、AR720、AR740

DESTROY PKI ENROLLMENTREQUEST={***csr-name***|**ALL**}

csr-name: 証明書発行要求名（1〜24 文字。ただし、PROTOCOL=MANUAL のときは 1〜8 文字）

解説

公開鍵証明書発行要求を取り消す。

パラメーター

ENROLLMENTREQUEST　証明書発行要求名。CREATE PKI ENROLLMENTREQUEST コマンドで指定した名前のこと。ALL を指定した場合は、まだ処理されていない発行要求をすべて取り消す。

例

■証明書発行要求「gimmecer」を取り消す。

```
DESTROY PKI ENROLLMENTREQUEST=gimmecer
```

関連コマンド

CREATE PKI ENROLLMENTREQUEST（18 ページ）
SHOW PKI ENROLLMENTREQUEST（48 ページ）

DESTROY PKI KEYUPDATEREQUEST

カテゴリー：PKI / 公開鍵更新要求
対象機種：AR300 V2、AR300L V2、AR720、AR740

DESTROY PKI KEYUPDATEREQUEST={***req-name***|**ALL**}

req-name: 鍵更新要求名（1〜24 文字。空白を含む場合はダブルクォートで囲む）

解説

RSA 公開鍵更新要求を取り消す。

パラメーター

KEYUPDATEREQUEST　鍵更新要求名。CREATE PKI KEYUPDATEREQUEST コマンドで指定した名前のこと。ALL を指定した場合は、まだ処理されていない更新要求をすべて取り消す。

関連コマンド

CREATE PKI KEYUPDATEREQUEST（21 ページ）
SHOW PKI KEYUPDATEREQUEST（50 ページ）

DISABLE PKI DEBUG

カテゴリー：PKI / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR720、AR740

```
DISABLE PKI DEBUG={ALL|CERTTRACE|CMDTRACE|CRTDBTRACE|CRTRUTRACE|
    CRTVGSTATE|CRTVGTRACE|CRTVUSTATE|CRTVUTRACE|MPPACKET|MPPKT|MPSTATE|
    MPTRACE|OPHTTPTRACE|OPLDAPTRACE|OPPACKET|OPPKT|PACKET|PKT|STATE|
    TRACE}[,...]
```

解説

PKI モジュールのデバッグオプションを無効にする。

パラメーター

DEBUG　デバッグオプション。カンマ区切りで複数指定が可能。ALL を指定した場合は、すべてのデバッグオプションが無効になる。

CERTTRACE	証明書ユニットのトレース
CMDTRACE	コマンドハンドラーのトレース
CRTDBTRACE	証明書データベースのトレース
CRTRUTRACE	証明書取得ユニットのトレース
CRTVGSTATE	証明書検証プロセスの状態表示
CRTVGTRACE	証明書検証プロセスのトレース
CRTVUSTATE	証明書検証ユニットの状態表示
CRTVUTRACE	証明書検証ユニットのトレース
MPPACKET	PKI 管理プロトコルパケットの表示
MPPKT	MPPACKET と同じ
MPSTATE	PKI 管理プロトコルの状態表示
MPTRACE	PKI 管理プロトコルのトレース
OPHTTPTRACE	HTTP トレース
OPLDAPTRACE	LDAP トレース
OPPACKET	オペレーションプロトコルパケットの表示
OPPKT	OPPACKET と同じ
PACKET	すべての PKI プロトコルパケットの表示
PKT	PACKET と同じ
STATE	すべての状態表示
TRACE	すべてのトレース

表 3: デバッグオプション一覧

関連コマンド

ENABLE PKI DEBUG（29 ページ）

ENABLE PKI DEBUG

カテゴリー：PKI / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR720、AR740

ENABLE PKI DEBUG={**ALL**|**CERTTRACE**|**CMDTRACE**|**CRTDBTRACE**|**CRTRUTRACE**|
CRTVGSTATE|**CRTVGTRACE**|**CRTVUSTATE**|**CRTVUTRACE**|**MPPACKET**|**MPPKT**|**MPSTATE**|
MPTRACE|**OPHTTPTRACE**|**OPLDAPTRACE**|**OPPACKET**|**OPPKT**|**PACKET**|**PKT**|**STATE**|
TRACE}[,...]

解説

PKI モジュールのデバッグオプションを有効にする。

パラメーター

DEBUG　デバッグオプション。カンマ区切りで複数指定が可能。ALL を指定した場合は、すべてのデバッグオプションが有効になる。

CERTTRACE	証明書ユニットのトレース
CMDTRACE	コマンドハンドラーのトレース
CRTDBTRACE	証明書データベースのトレース
CRTRUTRACE	証明書取得ユニットのトレース
CRTVGSTATE	証明書検証プロセスの状態表示
CRTVGTRACE	証明書検証プロセスのトレース
CRTVUSTATE	証明書検証ユニットの状態表示
CRTVUTRACE	証明書検証ユニットのトレース
MPPACKET	PKI 管理プロトコルパケットの表示
MPPKT	MPPACKET と同じ
MPSTATE	PKI 管理プロトコルの状態表示
MPTRACE	PKI 管理プロトコルのトレース
OPHTTPTRACE	HTTP トレース
OPLDAPTRACE	LDAP トレース
OPPACKET	オペレーションプロトコルパケットの表示
OPPKT	OPPACKET と同じ
PACKET	すべての PKI プロトコルパケットの表示
PKT	PACKET と同じ
STATE	すべての状態表示
TRACE	すべてのトレース

表 4: デバッグオプション一覧

関連コマンド

DISABLE PKI DEBUG（27 ページ）

PURGE PKI

カテゴリー：PKI / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR720、AR740

PURGE PKI

解説

PKI の設定情報をすべて削除する。
証明書情報、LDAP レポジトリーの情報、証明書失効リスト（CRL）、証明書発行要求、鍵更新要求などの情報はすべて失われる。また、デバッグオプションはすべて無効になり、SET PKI コマンドで変更したパラメーターもすべてデフォルト値に戻る。

備考・注意事項

ランタイムメモリー上にある PKI 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

関連コマンド

SHOW PKI（36 ページ）
SHOW PKI CERTIFICATE（43 ページ）
SHOW PKI CRL（46 ページ）
SHOW PKI ENROLLMENTREQUEST（48 ページ）
SHOW PKI KEYUPDATEREQUEST（50 ページ）

SET PKI

カテゴリー：PKI / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR720、AR740

```
SET PKI [CERTSTORELIMIT=12..256] [CMPRETRYMAX=0..10]
   [CMPRETRYPERIOD=10..600] [CRLUPDATEPERIOD=1..168] [SUBJECTALTNAME={ipadd|
   altname}]
```

ipadd: IP アドレス
altname: 名前（1〜64 文字。空白を含む場合はダブルクォートで囲む）

解説

PKI モジュールのグローバル設定パラメーターを変更する。

パラメーター

CERTSTORELIMIT　証明書データベースに保存する証明書の最大数を指定する。証明書の数が最大値を超えたときは、自動的に取得した証明書のうちで最も古いものが削除される。デフォルトは 24
CMPRETRYMAX　CMP メッセージの再送リトライ回数。デフォルトは 1
CMPRETRYPERIOD　CMP メッセージの再送間隔（秒）。デフォルトは 30 秒
CRLUPDATEPERIOD　CRL データベース内の証明書失効リスト（CRL）を再読み込みする間隔（時間）。デフォルトは 24 時間。
SUBJECTALTNAME　証明書の発行を要求するときに、Subject の Alternative Name（所有者の別名）として指定する名前。IP アドレスか名前で指定する。

関連コマンド

SHOW PKI（36 ページ）

SET PKI CERTIFICATE

カテゴリー：PKI / 証明書データベース
対象機種：AR300 V2、AR300L V2、AR720、AR740

SET PKI CERTIFICATE=*cert-name* [TRUSTED={TRUE|FALSE|YES|NO|ON|OFF}]
[TYPE={CA|SELF|ENDENTITY|EE}]

cert-name: 証明書名（1〜24 文字。空白を含む場合はダブルクォートで囲む）

解説

証明書データベースに登録されている公開鍵証明書の信頼レベルを変更する。

パラメーター

CERTIFICATE　証明書の名前。ADD PKI CERTIFICATE コマンドで指定したもの

TRUSTED　証明書の信頼レベル。TRUE（YES、ON も同じ）は信頼する、FALSE（NO、OFF も同じ）は信頼しない。ADD PKI CERTIFICATE コマンドで証明書をデータベースに登録するときに、TRUSTED=TRUE を指定しなかった場合、SHOW PKI CERTIFICATE コマンドで指紋（fingerprint）をはじめとする証明書の内容を確認してから、本コマンドで TRUSTED=TRUE を指定して証明書を信頼できるものとして設定する。

TYPE　証明書の種類。CA（CA 証明書）、SELF（ルーター自身の証明書）、EE または ENDENTITY（他のエンドエンティティーの証明書）から選択する。デフォルトは ENDENTITY

関連コマンド

ADD PKI CERTIFICATE（13 ページ）
DELETE PKI CERTIFICATE（22 ページ）
SHOW PKI CERTIFICATE（43 ページ）

SET PKI CRL

カテゴリー：PKI / CRL データベース
対象機種：AR300 V2、AR300L V2、AR720、AR740

SET PKI CRL=*crl-name* [LOCATION={*url*|*filename*}] [PASSWORD=*password*]
[USERNAME=*username*]

crl-name: CRL 名（1〜24 文字。空白を含む場合はダブルクォートで囲む）
url: URL（LDAP または HTTP）
filename: ファイル名（拡張子は.crl）
password: パスワード（1〜64 文字）
username: ユーザー名（1〜64 文字）

解説

CRL データベースに登録されている証明書失効リスト（CRL）の情報を変更する。

パラメーター

CRL　CRL の名前。ADD PKI CRL コマンドで指定したもの
LOCATION　CRL のある場所。ファイルシステム上のローカルファイルから取り込むときは、証明書ファイル（.crl）の名前を指定する。レポジトリーからダウンロードするときは、LDAP サーバーか HTTP サーバーの URL を指定する。
PASSWORD　レポジトリーにアクセスするためのパスワード
USERNAME　レポジトリーにアクセスするためのユーザー名

関連コマンド

ADD PKI CRL（15 ページ）
DELETE PKI CRL（23 ページ）
SHOW PKI CRL（46 ページ）

SET PKI LDAPREPOSITORY

カテゴリー：PKI / 証明書レポジトリー
対象機種：AR300 V2、AR300L V2、AR720、AR740

SET PKI LDAPREPOSITORY=*repos-name* [LOCATION=*url*] [PASSWORD=*password*]
[USERNAME=*username*]

repos-name: レポジトリー名（1〜24 文字。空白を含む場合はダブルクォートで囲む）
url: URL（LDAP）
password: パスワード（1〜64 文字）
username: ユーザー名（1〜64 文字）

解説

リモートレポジトリーの情報（URL、ユーザー名、パスワード）を変更する。
レポジトリーが登録されている場合、システムは必要な証明書をレポジトリーから自動的に取得する。

パラメーター

LDAPREPOSITORY　リモートレポジトリーの名前。ADD PKI LDAPREPOSITORY コマンドで指定したもの
LOCATION　レポジトリー（LDAP サーバー）の URL
PASSWORD　レポジトリーにアクセスするためのパスワード
USERNAME　レポジトリーにアクセスするためのユーザー名

関連コマンド

ADD PKI LDAPREPOSITORY（17 ページ）
DELETE PKI LDAPREPOSITORY（24 ページ）
SHOW PKI LDAPREPOSITORY（51 ページ）

SHOW PKI

カテゴリー：PKI / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW PKI [COUNTERS]

解説

PKI モジュールに関する情報を表示する。

パラメーター

COUNTERS　PKI モジュールの統計カウンターを表示させるときに指定する。

入力・出力・画面例

```
SecOff bulbul> show pki

PKI Module parameters:
  subjectAltName ..........
  CRL update period ....... 24 seconds
  CMP retry period ........ 30 seconds
  CMP maximum retries ..... 1
  Max. # of certificates .. 24
  Debug device ............ 16
  Debug types enabled:  none

SecOff bulbul> show pki counters
PKI CERTIFICATE UNIT COUNTERS:
 GENERAL COUNTERS:
  checkExtractParseFail            0  checkExtractFieldGetFail         0
  createFingerprintFail            0

 VALIDATION UNIT COUNTERS:
  eventRequestNotFound             0
  startRequest                     4  startRequestEquivReqFnd          0
  stopRequestFail                  0  stopRequestGood                  0
  gncicResultNoCIC                 0
  actionIllegal                    0
  startInitChecksTooDeep           0  startInitChecksBadTime           0
  startInitChecksIssNotCA          0  startInitChcksBadKeyUsge         0
  startInitChcksSSignNotCA         0  startInitChcksSSgnUntrst         1
  startInitChecksRevoked           0
  startValCICCertNotFound          0  startValCICAlreadyTrustd         2
  startValCICAlrdyVldating         0  startValCICStartVURqFail         0
```

```
  startVerifyCertNotFound           0  startVerifyCertParseFail          0
  startVerifyCrtFldGetFail          0
  startVerifyCICParseFail           0  startVerifyCICFldGetFail          0
  startVerifyFailImm                0  startVerifyStarted                3
  verifyCbackReqNotFound            0  verifyCallbackVerifyGood          3
  verifyCallbackVerifyFail          0
  createRequest                     4  destroyRequest                    4
  dbAdd                             4  dbRemoveFail                      0
  dbFindFail                        0  dbFindByRequestorFail             4
  dbFindByCertFail                  1

 VALIDATION UNIT GET NEXT CANDIDATE ISSUER CERTIFICATE COUNTERS:
  eventRequestNotFound              0  getNextCICNotFound                0
  remoteRetrievdReqNotFnd           0  actionIllegal                     0
  startGetRemoteFail                0

 RETRIEVAL UNIT COUNTERS:
  startOPStartFail                  0  retrievedRequestNotExist          0
  getFileNotExist                   0  getFileOpenFail                   0
  getFileReadFail                   0  getFileCloseFail                  0

PKI CRL UNIT COUNTERS:
 GENERAL COUNTERS:
  retrievedNotFound                 0  retrievedParseFail                0
  retrievedGetFieldsFail            0  retrievedRUStartFail              0
  timeoutRUStartFail                0
  addAlreadyExists                  0  addRUStartFail                    0
  addGood                           0
  setNotFound                       0  setRUStartFail                    0
  setGood                           0  setNothingSet                     0
  deleteNotFound                    0  deleteGood                        0
  purgeGood                         0  showNotFound                      0
  showListParseFail                 0

 RETRIEVAL UNIT COUNTERS:
  startOPStartFail                  0  retrievedRequestNotExist          0
  getFileNotExist                   0  getFileOpenFail                   0
  getFileReadFail                   0  getFileCloseFail                  0

PKI MANAGEMENT UNIT COUNTERS:
 CMP COUNTERS:
  startedEnrollment                 0  startedKeyUpdate                  0
  receivedPKIMessage                0  receivedPKIFIN                    0
  receivedTCPError                  0  receivedMsgVerifyOK               0
  receivedMsgVerifyFail             0  illegalEvent                      0
  requestFailed                     0  requestCompleted                  0
  receivedMessageDiscarded          0  retryEvent                        0
  timeoutEvent                      0  requestQueueError                 0

 MANUAL ENROLLMENT COUNTERS:
  started                           1  fileOpenFailed                    0
```

```
failed                          0  completed                       1
fileOpenOK                      1  fileClosed                      1
fileWriteFailed                 0  CSRCreationError                0
```

subjectAltName	ルーター自身の公開鍵証明書に付加される SubjectAltName（別名）
CRL update period	証明書失効リスト（CRL）の再読み込み間隔
CMP retry period	CMP メッセージの再送間隔
CMP maximum retries	CMP メッセージの再送リトライ回数
Max. # of certificates	証明書データベースに格納する証明書の最大数
Debug device	PKI モジュールのデバッグ情報を出力するデバイスの番号
Debug types enabled	有効なデバッグオプション

表 5:

PKI CERTIFICATE UNIT COUNTERS セクション	PKI 証明書ユニットのイベントカウンターが表示される
GENERAL COUNTERS	PKI 証明書ユニットの一般イベントカウンター
checkExtractParseFail	フォーマットエラーのため証明書の解析に失敗した回数
checkExtractFieldGetFail	フォーマットエラーのため証明書のフィールド読み込みに失敗した回数
createFingerprintFail	証明書のフィンガープリント生成に失敗した回数
VALIDATION UNIT COUNTERS	PKI 証明書検証ユニットのイベントカウンター
eventRequestNotFound	取り消された証明書検証要求に対してイベントが発生した回数
startRequest	証明書検証要求の開始に成功した回数
startRequestEquivReqFnd	同じ証明書に対する検証要求がすでに存在していたため新たな要求を出さなかった回数
stopRequestFail	証明書検証要求がすでに削除されていたため、取り消し要求がエラーとなった回数
stopRequestGood	証明書検証要求の停止に成功した回数
gncicResultNoCIC	「no candidate issuer certificate found」イベント受信回数
actionIllegal	証明書検証状態機械が不正なアクションを発生させた回数
startInitChecksTooDeep	検証チェーンが長くなりすぎたため証明書検証要求が失敗した回数
startInitChecksBadTime	証明書が有効でなかったために証明書検証要求が失敗した回数
startInitChecksIssNotCA	証明書が別の証明書の署名に使われていたが CA の証明書ではなかったために証明書検証要求が失敗した回数
startInitChcksBadKeyUsge	証明書が別の証明書の署名に使われていたが署名が禁じられていたために証明書検証要求が失敗した回数
startInitChcksSSignNotCA	CA 証明書でないにもかかわらず自署されていたため、証明書検証要求が失敗した回数

startInitChcksSSgnUntrst	自署されていたが信頼されていないために証明書検証要求が失敗した回数
startInitChecksRevoked	証明書が失効していたために証明書検証要求が失敗した回数
startValCICCertNotFound	証明書発行者の証明書が見つからないため証明書検証要求が失敗した回数
startValCICAlreadyTrustd	証明書検証要求に対し、発行者の信頼できる証明書が見つかった回数
startValCICAlrdyVldating	発行者の証明書がまだ検証中の段階にあるため、証明書検証要求が失敗した回数
startValCICStartVURqFail	発行者の証明書の検証に失敗したため、証明書検証要求が失敗した回数
startVerifyCertNotFound	証明書が削除されていたため、証明書の署名を検証できなかった回数
startVerifyCertParseFail	フォーマットエラーのため証明書を解析できず、証明書の署名を検証できずに証明書検証要求が失敗した回数
startVerifyCrtFldGetFail	フォーマットエラーのため証明書のフィールドを読み込めず、証明書の署名を検証できずに証明書検証要求が失敗した回数
startVerifyCICParseFail	フォーマットエラーのため発行者の証明書を解析できず、証明書の署名を検証できずに証明書検証要求が失敗した回数
startVerifyCICFldGetFail	フォーマットエラーのため発行者の証明書のフィールドを読み込めず、証明書の署名を検証できずに証明書検証要求が失敗した回数
startVerifyFailImm	署名検証が即時に失敗したため、証明書検証要求が失敗した回数
startVerifyStarted	証明書検証要求における署名の検証が正常に開始された回数
verifyCbackReqNotFound	証明書の署名検証は完了したが、その時点で証明書検証要求が取り消されていた回数
verifyCallbackVerifyGood	証明書検証要求における署名の検証に成功した回数
verifyCallbackVerifyFail	証明書検証要求における署名の検証に失敗した回数
createRequest	証明書検証要求が作成された回数
destroyRequest	証明書検証要求が削除された回数
dbAdd	証明書検証要求データベースに検証要求が追加された回数
dbRemoveFail	指定された証明書検証要求が見つからないため、検証要求データベースから削除された回数
dbFindFail	指定された証明書検証要求が検証要求データベース内に見つからなかった回数
dbFindByRequestorFail	指定された要求者の証明書検証要求が検証要求データベース内に見つからなかった回数
dbFindByCertFail	指定された証明書に対する検証要求がデータベース内に見つからなかった回数
VALIDATION UNIT GET NEXT CANDIDATE ISSUER CERTIFICATE COUNTERS	PKI の「get next candidate issuer certificate」ユニットのイベントカウンター

eventRequestNotFound	「get next candidate issuer certificate request」に関するイベントを受信したが、同要求がすでに取り消されていた回数
getNextCICNotFound	「get next candidate issuer certificate」ユニットが他の発行者証明書を見つけられなかった回数
remoteRetrievdReqNotFnd	「get next candidate issuer certificate request」に応じて証明書を取得したが、そのときには要求が取り消されていた回数
actionIllegal	「get next candidate issuer certificate」状態機械が不正なアクションを発生させた回数
startGetRemoteFail	「get next candidate issuer certificate request」によるリモート証明書の取得に失敗した回数
RETRIEVAL UNIT COUNTERS	PKI 証明書取得ユニットのイベントカウンター
startOPStartFail	PKI オペレーショナルプロトコルによる証明書取得要求の失敗回数
retrievedRequestNotExist	証明書の取得が完了したときに要求がすでに取り消されていた回数
getFileNotExist	ファイルが存在していなかったためファイルからの証明書取り込みに失敗した回数
getFileOpenFail	ファイルをオープンできなかったためファイルからの証明書取り込みに失敗した回数
getFileReadFail	ファイルを読めなかったためファイルからの証明書取り込みに失敗した回数
getFileCloseFail	ファイルをクローズできなかったためファイルからの証明書取り込みに失敗した回数
PKI CRL UNIT COUNTERS	PKI CRL ユニットのイベントカウンター
GENERAL COUNTERS	PKI CRL ユニットの一般イベントカウンター
retrievedNotFound	CRL を取得したが CRL 要求が取り消されていた回数
retrievedParseFail	フォーマットエラーのため取得した CRL を解析できなかった回数
retrievedGetFieldsFail	フォーマットエラーのため取得した CRL のフィールドを読み込めなかった回数
retrievedRUStartFail	CRL 要求が変更されたため CRL の取得に失敗した回数
timeoutRUStartFail	定期更新時に CRL 要求に失敗した回数
addAlreadyExists	CRL データベース内に同一の CRL が登録されていたため、CRL の追加に失敗した回数
addRUStartFail	データベースへの追加時に CRL 取得に失敗した回数
addGood	CRL データベースへの CRL 追加成功回数
setNotFound	CRL データベース内に指示された CRL が存在しなかったため、CRL の属性変更に失敗した回数
setRUStartFail	CRL 情報の変更後に CRL の取得に失敗した回数
setGood	CRL データベース内の CRL の情報変更に成功した回数
setNothingSet	CRL 情報の変更要求があったが、指定された情報が以前と同じであったため変更が行われなかった回数

deleteNotFound	CRL データベース内に指示された CRL が存在しなかったため、CRL の削除に失敗した回数
deleteGood	CRL データベースから CRL の削除に成功した回数
purgeGood	CRL データベースから全エントリーの削除に成功した回数
showNotFound	CRL データベース内に指示された CRL が存在しなかったため、CRL の情報表示に失敗した回数
showListParseFail	CRL のフォーマットエラーのため、CRL の情報表示に失敗した回数
RETRIEVAL UNIT COUNTERS	PKI CRL 取得ユニットのイベントカウンター
startOPStartFail	PKI オペレーショナルプロトコルによる証明書失効リスト（CRL）取得処理の失敗回数
retrievedRequestNotExist	CRL の取得が完了したときに取得要求が取り消されていた回数
getFileNotExist	ファイルが存在していなかったためファイルからの CRL 取り込みに失敗した回数
getFileOpenFail	ファイルをオープンできなかったためファイルからの CRL 取り込みに失敗した回数
getFileReadFail	ファイルを読めなかったためファイルからの CRL 取り込みに失敗した回数
getFileCloseFail	ファイルをクローズできなかったためファイルからの CRL 取り込みに失敗した回数
PKI MANAGEMENT UNIT COUNTERS	PKI 管理ユニットのイベントカウンター
CMP COUNTERS	CMP による自動発行要求ユニットのイベントカウンター
startedEnrollment	証明書発行要求数
startedKeyUpdate	鍵更新要求数
receivedPKIMessage	PKI CMP メッセージ受信数
receivedPKIFIN	CMP Transport から受信した PKI FIN メッセージの数
receivedTCPError	CMP Transport によって示された TCP エラーの数
receivedMsgVerifyOK	受信メッセージのうち内容が有効であったものの数
receivedMsgVerifyFail	受信メッセージのうち内容が無効であったものの数
illegalEvent	内部で発生した不正なイベント数
requestFailed	正常に処理されなかった証明書発行要求と鍵更新要求の数
requestCompleted	正常に処理された証明書発行要求と鍵更新要求の数
receivedMessageDiscarded	受信メッセージ破棄回数
retryEvent	リトライイベント発生回数
timeoutEvent	タイムアウトイベント発生回数
requestQueueError	CMP リクエストキューエラーの発生回数
MANUAL ENROLLMENT COUNTERS	PKI 手動発行要求作成ユニットのイベントカウンター

started	手動方式の証明書発行要求の処理開始回数
fileOpenFailed	ファイルのオープンに失敗した回数
failed	手動方式の証明書発行要求の処理に失敗した回数
completed	手動方式の証明書発行要求の処理が完了した回数
fileOpenOK	ファイルのオープンに成功した回数
fileClosed	ファイルのクローズに成功した回数
fileWriteFailed	ファイルへの書き込みに失敗した回数
CSRCreationError	証明書発行要求（CSR）の作成中にエラーが発生した回数

表 6: COUNTERS オプション指定時

関連コマンド

SET PKI（32 ページ）

SHOW PKI CERTIFICATE

カテゴリー：PKI / 証明書データベース
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW PKI CERTIFICATE[=*cert-name*]

cert-name: 証明書名（1〜24 文字。空白を含む場合はダブルクォートで囲む）

解説

証明書データベース内の証明書に関する情報を表示する。

パラメーター

CERTIFICATE　証明書の名前。ADD PKI CERTIFICATE コマンドで指定したもの。

入力・出力・画面例

```
SecOff bulbul> show pki certificate

Certificate Database: [ref.#: 12332-1396]

  Name                                    State       MTrust Type   Source
-------------------------------------------------------------------------------
  u0 (cn=RouterB, o=birds, c=jp)          TRUSTED     FALSE  EE     UM_ISAKMP
  mycer                                   TRUSTED     FALSE  SELF   COMMAND
  cacer                                   TRUSTED     TRUE   CA     COMMAND
-------------------------------------------------------------------------------

SecOff bulbul> show pki certificate=cacer

Certificate:
  name ................ cacer
  state ............... TRUSTED
  manually trusted .... TRUE
  type ................ CA
  source .............. COMMAND

  version ............. V3
  serial number .......
  signature alg ....... MD5 with RSA
  public key alg ...... RSA
  not valid before .... 10:06:10 - 04-Oct-2001  (GMT)
  not valid after ..... 10:06:10 - 04-Oct-2002  (GMT)
  subject ............. cn=mycert, o=birds, c=jp
```

```
issuer ............... cn=mycert, o=birds, c=jp

cert. fingerprint ... 1478 f278 ea6d a068 2adc
(sha1)                eff2 89f7 fde7 f729 415e

key fingerprint ..... ab73 6a4e e8f0 5d4b 9b95
(sha1)                5a1b ef75 440b 6633 b095

key usage ............ {C}Digital Signature
                          Non Repudiation
                          Certificate Signing
                          CRL Signing
basic constraints {C}
  subject type ...... CA
  path length ....... No constraint
subject key ID ...... 7fa5b7c05b62b7064c1582a2794aec9306065837
authority key ID .... 7fa5b7c05b62b7064c1582a2794aec9306065837

validation path ..... [ manually trusted, self-signed ]

Source Location:
  file ............... ca.cer
```

Name	証明書の名前。ユーザーがつけたもの、あるいは、ルーターが自動的に取得した証明書の場合は証明書の Subject
State	証明書の信頼レベル。TRUSTED（信頼できる）、UNTRUSTED（まだ信頼できない）、VALIDATING（検証中）のいずれか
MTrust	ユーザーのコマンド入力によって手動で「信頼できる」ものとして設定されたかどうか。TRUE か FALSE
Type	証明書の種類。SELF（ルーター自身の証明書）、CA（認証局の証明書）、EE（その他エンドエンティティーの証明書）がある
Source	証明書がどのようにしてデータベースに登録されたか。COMMAND（ユーザーのコマンド入力）、VLD_UNIT（証明書検証ユニットによる自動取得）、UM_ISAKMP（ISAKMP モジュール）、MGMT_PROT（CMP プロトコル）のいずれか

表 7:

Certificate セクション	証明書に関する情報が表示される
name	証明書の名前。ユーザーがつけたもの、あるいは、ルーターが自動的に取得した証明書の場合は証明書の Subject
state	証明書の信頼レベル。TRUSTED（信頼できる）、UNTRUSTED（まだ信頼できない）、VALIDATING（検証中）のいずれか
manually trusted	ユーザーのコマンド入力によって手動で「信頼できる」ものとして設定されたかどうか。TRUE か FALSE

type	証明書の種類。SELF（ルーター自身の証明書）、CA（認証局の証明書）、EE（その他エンドエンティティーの証明書）がある
source	証明書がどのようにしてデータベースに登録されたか。COMMAND（ユーザーのコマンド入力）、VLD_UNIT（証明書検証ユニットによる自動取得）、UM_ISAKMP（ISAKMP モジュール）、MGMT_PROT（CMP プロトコル）のいずれか
version	証明書が準拠している X.509 のバージョン
serial number	証明書のシリアル番号
sha1 fingerprint	ハッシュ関数 SHA1 による証明書のフィンガープリント
signature alg	証明書に対する電子署名に用いられたアルゴリズム
public key alg	証明書の発行対象である公開鍵のアルゴリズム
not valid before	証明書の有効期間開始日（発効日）
not valid after	証明書の有効期間終了日（失効日）
subject	証明書の所有者（サブジェクト）の識別名
issuer	証明書の発行者の識別名
key usage	公開鍵の正当な用途
subject alt name	証明書所有者（サブジェクト）の代替名
validation path	証明書の検証パスを構成する証明書一覧
Source Location セクション	証明書の取得元に関する情報が表示される
file	ファイルシステム上のファイル名
type	アドレスの種類。LDAP か HTTP のいずれか
IP address	IP アドレス
domain name	ホスト名
distinguished name	証明書の場所を示す識別名
port	ポート番号
HTTP file name	HTTP ファイル名
username	レポジトリーにアクセスするためのユーザー名
password	レポジトリーにアクセスするためのパスワード

表 8: 名前指定時

関連コマンド

ADD PKI CERTIFICATE（13 ページ）
DELETE PKI CERTIFICATE（22 ページ）
SET PKI CERTIFICATE（33 ページ）

SHOW PKI CRL

カテゴリー：PKI / CRL データベース
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW PKI CRL[=*crl-name*]

crl-name: CRL 名（1〜24 文字。空白を含む場合はダブルクォートで囲む）

解説

証明書失効リスト（CRL）データベース内の CRL の情報を表示する。

パラメーター

CRL　CRL の名前。ADD PKI CRL コマンドで指定したもの。

Name	CRL 名
State	CRL の状態。GETTINGFIRST（初回のロード中）、GETTING（2 回目以降の更新のためのロード中）、NOTFOUNDFIRST（初回のロードに失敗）、NOTFOUND（2 回目以降の更新のためのロードに失敗）、UPTODATE（CRL は最新の状態にあり、現在使用中）、NOTVALIDATED（最新の CRL は検証できていない）、OUTOFDATE（最新の CRL は現時点では有効でない）、UNRECFORMAT（最新の CRL はフォーマットにエラーがある）がある
Minutes-to-next-update	次回更新までの時間（分）

表 9:

PKI CRL	CRL 名
State	CRL の状態。GETTINGFIRST（初回のロード中）、GETTING（2 回目以降の更新のためのロード中）、NOTFOUNDFIRST（初回のロードに失敗）、NOTFOUND（2 回目以降の更新のためのロードに失敗）、UPTODATE（CRL は最新の状態にあり、現在使用中）、NOTVALIDATED（最新の CRL は検証できていない）、OUTOFDATE（最新の CRL は現時点では有効でない）、UNRECFORMAT（最新の CRL はフォーマットにエラーがある）がある

Minutes to next update	次回更新までの時間（分）
Number of updates	これまでの更新回数
Type	CRL の種類。現時点では CRL のみ
Version	X.509 CRL のバージョン
Issuer	CRL を発行した認証局（CA）の識別名
Signature algorithm	発行元 CA が CRL に署名するときに使用したアルゴリズム
Number of entries	CRL に記載されている失効した証明書の数
This update	現在の CRL の発行日時
Next update	次に CRL が発行される日時
Source Location	CRL の取得元
Certificate List セクション	CRL に記載されている失効した証明書のリスト
Certificate Serial Number	失効した証明書のシリアル番号
Revocation Date	失効日時
Revocation Reason	失効理由

表 10: 名前指定時

関連コマンド

ADD PKI CRL（15 ページ）
DELETE PKI CRL（23 ページ）
SET PKI CRL（34 ページ）

SHOW PKI ENROLLMENTREQUEST

カテゴリー：PKI / 証明書発行要求
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW PKI ENROLLMENTREQUEST[=*csr-name*]

csr-name: 証明書発行要求名（1〜24 文字。ただし、PROTOCOL=MANUAL のときは 1〜8 文字）

解説

処理が完了していない公開鍵証明書発行要求の情報を表示する。

パラメーター

ENROLLMENTREQUEST　証明書発行要求名。CREATE PKI ENROLLMENTREQUEST コマンドで指定した名前のこと。名前を指定した場合は、該当する発行要求の詳細を表示する。名前を指定しなかった場合は、まだ処理されていないすべての発行要求を一覧表示する。

入力・出力・画面例

```
Manager > show pki enrollmentrequest

Enrollment Requests
  Name                                    KeyId   Protocol      State
-------------------------------------------------------------------------------
  gimmecer                                    1   CMP           WAIT_FOR_IP
-------------------------------------------------------------------------------

Manager > show pki enrollmentrequest=gimmecer

Enrollment Request:

  Name ................ gimmecer
  KeyID ............... 1
  Protocol ............ CMP
  State ............... WAIT_FOR_IP
  Secret Value ........ abcdefgh
  Reference Number .... 12345678
  Location:
    IP address ........ 192.168.1.100
```

Name	公開鍵証明書発行要求を識別するための名前
KeyID	証明書の発行対象となる RSA 鍵ペアの番号

Protocol	発行要求を認証局（CA）に渡すための方式。CMP（PKI Certificate Management Protocol による自動方式）か MANUAL（手動方式）のどちらか
State	発行要求の処理状況。WAIT_FOR_IP（CA からの Initialisation Response Message を待っている状態）、WAIT_FOR_CERT_CHECK（新しい証明書を検証している状態）、WAIT_FOR_CONFOK （CA からの Confirmation OK Indication を待っている状態）がある

表 11:

Name	公開鍵証明書発行要求を識別するための名前
KeyID	証明書の発行対象となる RSA 鍵ペアの番号
Protocol	発行要求を認証局（CA）に渡すための方式。CMP（PKI Certificate Management Protocol による自動方式）か MANUAL（手動方式）のどちらか
State	発行要求の処理状況。WAIT_FOR_IP（CA からの Initialisation Response Message を待っている状態）、WAIT_FOR_CERT_CHECK（新しい証明書を検証している状態）、WAIT_FOR_CONFOK （CA からの Confirmation OK Indication を待っている状態）がある
Secret Value	秘密鍵を所有していることを証明するための承認コード
Reference Number	発行要求の参照番号
Location	CA の IP アドレス（IP address）またはホスト名（domain name）

表 12: 名前指定時

関連コマンド

CREATE PKI ENROLLMENTREQUEST（18 ページ）
DESTROY PKI ENROLLMENTREQUEST（25 ページ）

SHOW PKI KEYUPDATEREQUEST

カテゴリー：PKI / 公開鍵更新要求
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW PKI KEYUPDATEREQUEST[=*req-name*]

req-name: 鍵更新要求名（1〜24 文字。空白を含む場合はダブルクォートで囲む）

解説

処理が完了していない RSA 公開鍵更新要求の情報を表示する。

パラメーター

KEYUPDATEREQUEST　鍵更新要求名。CREATE PKI KEYUPDATEREQUEST コマンドで指定した名前のこと。名前を指定した場合は、該当する更新要求の詳細を表示する。名前を指定しなかった場合は、まだ処理されていないすべての更新要求を一覧表示する。

Name	鍵更新要求を識別するための名前
KeyID	新しい RSA 鍵ペアの番号
Certificate	鍵を更新する公開鍵証明書の名前
State	鍵更新要求の処理状況。WAIT_FOR_IP（CA からの Initialisation Response Message を待っている状態）、WAIT_FOR_KUP（CA からの Key Update Response Message を待っている状態）、WAIT_FOR_CERT_CHECK（新しい証明書を検証している状態）、WAIT_FOR_CONFOK（CA からの Confirmation OK Indication を待っている状態）がある

表 13:

Name	鍵更新要求を識別するための名前
KeyID	新しい RSA 鍵ペアの番号
Certificate Name	鍵を更新する公開鍵証明書の名前
Location	CA の IP アドレス（IP address）またはホスト名（domain name）

表 14: 名前指定時

関連コマンド

CREATE PKI KEYUPDATEREQUEST（21 ページ）
DESTROY PKI KEYUPDATEREQUEST（26 ページ）

SHOW PKI LDAPREPOSITORY

カテゴリー：PKI / 証明書レポジトリー
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW PKI LDAPREPOSITORY

解説

登録されているリモートレポジトリーの情報（URL、ユーザー名、パスワード）を表示する。

Index	LDAP レポジトリーのインデックス番号
Name	LDAP レポジトリーの名前（ユーザーがつけたもの）
Address	LDAP レポジトリーの IP アドレスかホスト名

表 15:

関連コマンド

ADD PKI LDAPREPOSITORY（17 ページ）
DELETE PKI LDAPREPOSITORY（24 ページ）
SET PKI LDAPREPOSITORY（35 ページ）