crypto key generate rsa

crypto key generate rsa

Rivest, Shamir, and Adelman（RSA）キー ペアを生成するには、グローバル コンフィギュレーション モードで **crypto key generate rsa** コマンドを使用します。

crypto key generate rsa [**general-keys**| **usage-keys**| **signature**| **encryption**] [**label** *key-label*] **[exportable]** [**modulus** *modulus-size*] [**storage** *devicename* **:**] **[redundancy]** [**on** *devicename* **:**]

構文の説明

general-keys	（任意）デフォルトで汎用キー ペアが生成されるように指定します。
usage-keys	（任意）2 つの RSA 特殊用途キー ペア（1 つの暗号化ペアと 1 つのシグニチャ ペア）が生成されるように指定します。
signature	（任意）生成される RSA 公開キーが署名用の特殊用途キーになるように指定します。
encryption	（任意）生成される RSA 公開キーが暗号化用の特殊用途キーになるように指定します。
label *key-label*	（任意）RSA キー ペアのエクスポート時に使用される名前を指定します。 キー ラベルが指定されていない場合は、ルータの完全修飾ドメイン名（FQDN）が使用されます。
exportable	（任意）RSA キー ペアをルータなどの別のシスコ デバイスにエクスポートできるように指定します。

modulus *modulus-size*	（任意）キー モジュラスの IP サイズを指定します。 デフォルトでは、認証局（CA）キーのモジュラス サイズは 1024 ビットです。 推奨される CA キーのモジュラスは 2048 ビットです。 CA キーのモジュラスの範囲は 350 ～ 4096 ビットです。 （注） Cisco IOS XE Release 2.4 および Cisco IOS Release 15.1(1)T から、秘密キー操作の最大キー サイズは 4096 ビットに拡張されました。 これより前のリリースの秘密キー操作の最大値は 2048 ビットです。
storage *devicename* **:**	（任意）キー ストレージの場所を指定します。ストレージデバイスの名前の後にはコロン（:）を付けます。
redundancy	（任意）キーがスタンバイ CA に同期するように指定します。
on *devicename* **:**	（任意）Universal Serial Bus（USB）トークン、ローカル ディスク、または NVRAM など、指定されたデバイスに RSA キー ペアが作成されるように指定します。 装置の名前の後にはコロン（:）を付けます。 USB トークン上で作成されるキーは、2048 ビット以下である必要があります。

コマンド デフォルト

RSA キー ペアは存在しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.3	このコマンドが導入されました。
12.2(8)T	*key-label* 引数が追加されました。
12.2(15)T	**exportable** キーワードが追加されました。

リリース	変更内容
12.2(18)SXD	このコマンドが、Cisco IOS Release 12.2(18)SXD に統合されました。
12.4(4)T	**storage** キーワードおよび *devicename* **:** 引数が追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.4(11)T	**storage** キーワードおよび *devicename* **:** 引数が、Cisco 7200VXR NPE-G2 プラットフォームに実装されました。 **signature**、**encryption** および **on** キーワードと *devicename* **:** 引数が追加されました。
12.4(24)T	IPv6 セキュア ネイバー探索（SeND）のサポートが追加されました。
XE 2.4	秘密キー操作の最大 RSA キー サイズが 2048 ビットから 4096 ビットに拡張されました。
15.0(1)M	このコマンドが変更されました。 **redundancy** キーワードが追加されました。
15.1(1)T	このコマンドが変更されました。 **modulus** キーワードの値の範囲が 360 ～ 2048 ビットから 360 ～ 4096 ビットに拡張されました。

使用上のガイドライン

（注） セキュリティ上の脅威と、これに対抗するための暗号テクノロジーは、絶えず変化しています。 最新のシスコの暗号化に関する推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

このコマンドは、シスコデバイス（ルータなど）の RSA キーペアを生成するために使用します。

RSA キーはペアで生成されます。1 つは公開 RSA キーで、もう 1 つは秘密 RSA キーです。

このコマンドの発行時に、ルータに RSA キーがすでに設定されている場合は、警告が表示され、既存のキーを新しいキーと置き換えるよう求めるプロンプトが表示されます。

（注） このコマンドを発行する前に、ルータにホスト名および IP ドメイン名が設定されていることを確認します（**hostname** および **ip domain-name** コマンドを使用）。 ホスト名および IP ドメイン名なしで **crypto key generate rsa** コマンドを完了することはできません （名前付きのキーペアのみを生成する場合を除きます）。

crypto key generate rsa

（注） RSA キーなしでルータのキー ペアを生成すると、セキュア シェル（SSH）によって RSA キー ペアが生成される場合があります。 追加のキー ペアは、SSH のみが使用し、{*router_FQDN* }.server などの名前が付けられます。 たとえば、ルータの名前が「router1.cisco.com」の場合は、キーの名前が「router1.cisco.com.server」になります。

このコマンドはルータ コンフィギュレーションに保存されません。ただし、このコマンドによって生成された RSA キーは、次回に NVRAM にコンフィギュレーションが書き込まれる際に NVRAM のプライベート コンフィギュレーションに保存されます（ユーザには表示されません。また、別のデバイスにバックアップもされません）。

（注） コンフィギュレーションが NVRAM に保存されない場合、生成されたキーは次回のルータのリロード時に失われます。

RSA キー ペアには特殊用途キーと汎用目的キーの 2 つのタイプがあり、これらは相互に排他的です。 RSA キーペアを生成する場合、特殊用途キーまたは汎用目的キーのいずれかを選択するように求められます。

特殊用途キー

特殊用途キーを生成すると、RSA キーが 2 ペア生成されます。 一方のペアは、認証方式として RSA シグニチャを指定するインターネット キー交換（IKE）ポリシーで使用され、もう一方のペアは、認証方式として RSA 暗号キーを指定する IKE ポリシーで使用されます。

CA は、RSA シグニチャを指定する IKE ポリシーでのみ使用され、RSA 暗号化ナンスを指定する IKE ポリシーでは使用されません （ただし、複数の IKE ポリシーを指定し、一方のポリシーに RSA シグニチャを指定し、もう一方のポリシーに RSA 暗号化ナンスを指定することはできます）。

IKE ポリシーに両方のタイプの RSA 認証方式を使用する場合は、特殊用途キーを生成します。 特殊用途キーを使用すると、各キーは不必要に暴露されなくなります （特殊用途キーを使用しない場合、1 つのキーが両方の認証方式に使用されるため、そのキーが暴露される危険性が高くなります）。

汎用目的キー

汎用目的キーを生成すると、RSA キーが 1 ペアだけ生成されます。 このペアは、RSA シグニチャまたは RSA 暗号化キーのいずれかを指定する IKE ポリシーで使用されます。 したがって、汎用目的キー ペアは、特殊用途キー ペアよりも頻繁に使用される可能性があります。

名前付きのキー ペア

key-label 引数を使用して名前付きのキー ペアを生成する場合は、**usage-keys** キーワードまたは **general-keys** キーワードを指定する必要があります。 名前付きのキー ペアを使用すると、複数の RSA キー ペアを持つことが可能になり、Cisco IOS ソフトウェアがアイデンティティ証明書ごとに異なるキー ペアを維持できます。

モジュラス長

RSA キーを生成すると、モジュラス長を入力するように求められます。 モジュラス長が長いほど、セキュリティが強力になります。 ただし、モジュラス長が長いほど生成に時間がかかり（次の表の生成時間の例を参照）、使用するのに時間がかかります。

表 *1*：モジュラス長による *RSA* キーの生成時間の例

ルータ	360 ビット	512 ビット	1024 ビット	2048 ビット（最大）
Cisco 2500	11 秒	20 seconds	4 分 38 秒	1 時間以上
Cisco 4700	1 秒未満	1 秒	4 秒	50 秒

Cisco IOS ソフトウェアは、4096 ビットより大きいモジュラスはサポートしません。 512 ビット未満の長さは、通常は推奨されません。 モジュラスが短いと IKE で適切に機能しない場合があるため、少なくとも 2048 ビット以上のモジュラスを使用することを推奨します。

（注） Cisco IOS Release 12.4(11)T の時点では、最大 4096 ビットまでのピアの公開 RSA キーのモジュラス値が自動的にサポートされます。 秘密 RSA キーの最大モジュラス値は 4096 ビットです。したがって、ルータが生成またはインポートできる RSA 秘密キーの最大サイズは、4096 ビットです。 ただし、RFC 2409 では、RSA 暗号化の秘密キーのサイズを 2048 ビット以下に制限しています。 CA に対して推奨されるモジュラスは 2048 ビット、クライアントに対して推奨されるモジュラスは 2048 ビットです。

RSA キーが暗号化ハードウェアによって生成されるときは、追加の制限が適用される場合があります。 たとえば、RSA キーが Cisco VPN Services Port Adapter（VSPA）によって生成される場合は、RSA キーのモジュラスの最小値は 384 ビットで、64 の倍数である必要があります。

RSA キーの保管場所の指定

crypto key generate rsa コマンドを **storage** *devicename* **:** キーワードおよび引数で発行すると、RSA キーは指定されたデバイスに保存されます。 この場所は、**crypto key storage** コマンドの設定に優先します。

RSA キーを生成するデバイスの指定

Cisco IOS Release 12.4(11)T 以降のリリースでは、RSA キーを生成するデバイスを指定できます。サポートされているデバイスには、NVRAM、ローカルディスク、および USB トークンがあります。 ルータに設定済みで利用可能な USB トークンがある場合、USB トークンは、ストレージデバイスだけでなく暗号化デバイスとして使用することもできます。 USB トークンを暗号化デバイスとして使用すると、トークンでクレデンシャルのキー生成、署名、認証などの RSA 操作を実行できます。 秘密キーは決して USB トークンから出ないようになっており、エクスポートできません。 公開キーはエクスポート可能です。

on *devicename* **:** キーワードおよび引数を使用すると、設定済みの利用可能な USB トークンで RSA キーが生成される場合があります。 USB トークン上に常駐するキーは、生成された段階でトークンの永続的な保管場所に保存されます。 USB トークンで生成されるキーの数は、使用可能な空き

領域によって制限されます。USB トークンでキーを生成するときに使用可能な空き領域がない場合は、次のメッセージが表示されます。

```
% Error in generating keys:no available resources
```

キーの削除操作を行うと、トークンに保存されているキーは、永続的な保管場所からただちに削除されます（トークン上に常駐していないキーは、**copy** またはそれに類するコマンドが発行されると、トークン以外の保管場所で保存や削除が行われます）。

USB トークンの設定の詳細については、『Cisco IOS Security Configuration Guide, Release 12.4T』の「Storing PKI Credentials」の章を参照してください。 トークン上の RSA クレデンシャルの使用の詳細については、『Cisco IOS Security Configuration Guide, Release 12.4T』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章を参照してください。

デバイスでの RSA キーの冗長性の生成の指定

エクスポート可能な場合にだけ、既存のキーの冗長性を指定できます。

例

次に、「ms2」というラベルの USB トークンでの汎用 1024 ビット RSA キー ペアの生成と、それとともに表示される暗号エンジンのデバッギング メッセージの例を示します。

```
Router(config)# crypto key generate rsa label ms2 modulus 2048 on usbtoken0:
The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw)(ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw)(ipsec)
```

これで、「ms2」というラベルが付けられた、トークン上のキーを登録に使用できます。

次に、特殊用途 RSA キーを生成する例を示します。

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

次に、汎用目的 RSA キーを生成する例を示します。

（注） 特殊用途キーと汎用目的キーの両方は生成できません。いずれか一方だけを生成できます。

```
Router(config)# crypto key generate rsa general-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

次に、汎用目的 RSA キー ペア「exampleCAkeys」を生成する例を示します。

```
crypto key generate rsa general-keys label exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url
http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

次に、「usbtoken0:」の RSA キーの保管場所を「tokenkey1」に指定する例を示します。

crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:

次に、**redundancy** キーワードを指定する例を示します。

```
Router(config)# crypto key generate rsa label MYKEYS redundancy
```

キーの名前は MYKEYS になります。

汎用目的キーのキー モジュラスのサイズを 360 ～ 2048 の

範囲で選択します。 512 より大きいサイズのキー モジュラスを選択した場合は生成に

数分かかる場合があります。

How many bits in the modulus [512]:

% Generating 512 bit RSA keys, keys will be non-exportable with redundancy...[OK]

関連コマンド

コマンド	説明
copy	特権 EXEC モードで copy コマンドを使用して、送信元から宛先にファイルをコピーします。
crypto key storage	RSA キー ペアのデフォルトの保管場所を設定します。
debug crypto engine	暗号エンジンに関するデバッグ メッセージを表示します。
hostname	ネットワーク サーバのホスト名を指定または修正します。
ip domain-name	デフォルトのドメイン名を定義して、未修飾のホスト名（ドット付き 10 進表記で記載されていない名前）を完成します。
show crypto key mypubkey rsa	ルータの RSA 公開キーを表示します。
show crypto pki certificates	PKI 証明書、認証局、および登録局証明書に関する情報を表示します。