



## キーチェーン管理コマンド

---

ここでは、キーチェーン管理を設定するために使用されるコマンドについて説明します。

キーチェーン管理の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』の「*Implementing Keychain Management on Cisco ASR 9000 Series Router*」設定モジュールを参照してください。

- [accept-lifetime, 2 ページ](#)
- [accept-tolerance, 4 ページ](#)
- [cryptographic-algorithm, 6 ページ](#)
- [key \(キーチェーン\), 8 ページ](#)
- [key chain \(キーチェーン\), 10 ページ](#)
- [key-string \(キーチェーン\), 12 ページ](#)
- [send-lifetime, 14 ページ](#)
- [show key chain, 16 ページ](#)

## accept-lifetime

キーチェーンの認証キーが有効なキーとして受信される期間を設定するには、キー コンフィギュレーション モードで **accept-lifetime** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**accept-lifetime** *start-time* [**duration** *duration value*|**infinite**|*end-time*]

**no accept-lifetime** *start-time* [**duration** *duration value*|**infinite**|*end-time*]

### 構文の説明

<i>start-time</i>	キーが有効になる開始時間を <i>hh:mm:ss</i> 日月年の形式で指定します。範囲は 0:0:0 ~ 23:59:59 です。 日付の範囲は 1 ~ 31 です。 年の範囲は 1993 ~ 2035 です。
<b>duration</b> <i>duration value</i>	(任意) キーのライフタイムを秒で指定します。範囲は、1 ~ 2147483646 です。
<b>infinite</b>	(任意) 有効になった後、そのキーが期限切れにならないことを示します。
<i>end-time</i>	(任意) キーが期限切れとなる時刻を <i>hh:mm:ss</i> 日月年の形式で指定します。範囲は 0:0:0 ~ 23:59:59 です。

コマンド デフォルト なし

コマンド モード キー 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
リリース 3.7.2	このコマンドが追加されました。

**使用上のガイドライン** このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
system	read, write

## 例

次に、**accept-lifetime** コマンドの使用例を示します。

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# accept-lifetime 1:00:00 June 29 2006 infinite
```

## 関連コマンド

コマンド	説明
<a href="#">key (キーチェーン)</a> , (8 ページ)	キーチェーンのキーを作成または変更します。
<a href="#">key chain (キーチェーン)</a> , (10 ページ)	キーチェーンを作成または変更します。
<a href="#">key-string (キーチェーン)</a> , (12 ページ)	キー文字列のテキストを指定します。
<a href="#">send-lifetime</a> , (14 ページ)	有効なキーを送信します。
<a href="#">show key chain</a> , (16 ページ)	キーチェーンを表示します。

# accept-tolerance

ピアが使用する受け入れキーの許容値、つまり受け入れ可能な限度を秒で指定するには、キーチェーン コンフィギュレーション モードで **accept-tolerance** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**accept-tolerance** [*value*] **infinite**]

**no accept-tolerance** [*value*] **infinite**]

## 構文の説明

<i>value</i>	(任意) 秒で示される許容値の範囲。範囲は、1 ~ 8640000 です。
<b>infinite</b>	(任意) 指定された許容値が無限であることを示します。この受け入れキーは期限切れになりません。無限の許容限度は、受け入れキーが常に受け入れ可能であり、ピアが使用する際に検証されることを意味します。

## コマンド デフォルト

デフォルト値は、許容しないことを意味する 0 です。

## コマンド モード

キーチェーン 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
リリース 3.7.2	このコマンドが追加されました。

## 使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**accept-tolerance** コマンドを設定しない場合、許容値は 0 に設定されます。

キーが有効なライフタイムの範囲外にある場合でも、許容限度内にあればそのキーは受け入れ可能と判断されます (たとえば、ライフタイムの開始前やライフタイムの終了後など)。

## タスク ID

タスク ID	操作
system	read, write

## 例

次に、**accept-tolerance** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# configure  
RP/0/RSP0/CPU0:router(config)# key chain isis-keys  
RP/0/RSP0/CPU0:router(config-isis-keys)# accept-tolerance infinite
```

## 関連コマンド

コマンド	説明
<a href="#">accept-lifetime</a> , (2 ページ)	有効なキーを受け入れます。
<a href="#">key chain</a> (キーチェーン), (10 ページ)	キーチェーンを作成または変更します。
<a href="#">show key chain</a> , (16 ページ)	キーチェーンを表示します。

# cryptographic-algorithm

キーIDに設定されたキー文字列を使用して、パケットに適用する暗号化アルゴリズムを選択するには、キーチェーンおよびキーコンフィギュレーションモードで **cryptographic-algorithm** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**cryptographic-algorithm** [HMAC-MD5| HMAC-SHA1-12| HMAC-SHA1-20| MD5| SHA-1]

**no cryptographic-algorithm** [HMAC-MD5| HMAC-SHA1-12| HMAC-SHA1-20| MD5| SHA-1]

## 構文の説明

<b>HMAC-MD5</b>	HMAC-MD5 をダイジェストサイズ 16 バイトの暗号化アルゴリズムとして設定します。
<b>HMAC-SHA1-12</b>	HMAC-SHA1-12 をダイジェストサイズ 12 バイトの暗号化アルゴリズムとして設定します。
<b>HMAC-SHA1-20</b>	HMAC-SHA1-20 をダイジェストサイズ 20 バイトの暗号化アルゴリズムとして設定します。
<b>MD5</b>	MD5 をダイジェストサイズ 16 バイトの暗号化アルゴリズムとして設定します。
<b>SHA-1</b>	SHA-1-20 をダイジェストサイズ 20 バイトの暗号化アルゴリズムとして設定します。

## コマンド デフォルト

デフォルトの動作または値はありません。

## コマンド モード

キーチェーンのキー 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
リリース 3.7.2	このコマンドが追加されました。

## 使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

暗号化アルゴリズムを設定しない場合、MAC 計算と API 検証は無効になります。

各プロトコルがサポートする暗号化アルゴリズムは次のとおりです。

- ボーダー ゲートウェイ プロトコル (BGP) は HMAC-MD5 と HMAC-SHA1-12 だけをサポート
- Intermediate System-to-Intermediate System (IS-IS) は HMAC-MD5 だけをサポート
- Open Shortest Path First (OSPF) は MD5 だけをサポート

## タスク ID

タスク ID	操作
system	read, write

## 例

次に、**cryptographic-algorithm** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# cryptographic-algorithm HMAC-MD5
```

## 関連コマンド

コマンド	説明
<a href="#">accept-lifetime</a> , (2 ページ)	有効なキーを受け入れます。
<a href="#">key chain</a> (キーチェーン), (10 ページ)	キーチェーンを作成または変更します。
<a href="#">show key chain</a> , (16 ページ)	キーチェーンを表示します。

## key (キーチェーン)

キーチェーンのキーを作成または変更するには、キーチェーンのキー コンフィギュレーション モードで **key** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**key** *key-id*

**no key** *key-id*

### 構文の説明

*key-id* 48 ビット整数型のキー ID。範囲は 0 ～ 281474976710655 です。

### コマンド デフォルト

デフォルトの動作または値はありません。

### コマンド モード

キーチェーンのキー 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
リリース 3.7.2	このコマンドが追加されました。

### 使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ボーダー ゲートウェイ プロトコル (BGP) のキーチェーン設定では、*key-id* 引数の範囲は 0 ～ 63 でなければなりません。この範囲が 63 の値を超えると、BGP キーチェーンの操作は拒否されません。

### タスク ID

タスク ID	操作
system	read, write

## 例

次に、**key** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)#
```

## 関連コマンド

コマンド	説明
<a href="#">accept-lifetime</a> , (2 ページ)	有効なキーを受け入れます。
<a href="#">key chain</a> (キーチェーン), (10 ページ)	キーチェーンを作成または変更します。
<a href="#">key-string</a> (キーチェーン), (12 ページ)	キー文字列のテキストを指定します。
<a href="#">send-lifetime</a> , (14 ページ)	有効なキーを送信します。
<a href="#">show key chain</a> , (16 ページ)	キーチェーンを表示します。

## key chain (キーチェーン)

キーチェーンを作成または変更するには、グローバルコンフィギュレーションモードで **key chain** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**key chain** *key-chain-name*

**no key chain** *key-chain-name*

### 構文の説明

*key-chain-name* キーチェーンの名前を指定します。最大文字数は 48 です。

### コマンド デフォルト

デフォルトの動作または値はありません。

### 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
リリース 3.7.2	このコマンドが追加されました。

### 使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ボーダーゲートウェイプロトコル (BGP) のキーチェーンは、ネイバー、セッショングループ、またはネイバーグループとして設定できます。BGPはこのキーチェーンを使用して、ヒットしないキー更新を認証にインプリメントできます。

### タスク ID

タスク ID	操作
system	read, write

## 例

次の例は、キーチェーン名 isis-keys が **key chain** コマンド用であることを示しています。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)#
```

## 関連コマンド

コマンド	説明
<a href="#">accept-lifetime</a> , (2 ページ)	有効なキーを受け入れます。
<a href="#">accept-tolerance</a> , (4 ページ)	キーチェーンのキーを受け入れる際の許容値を設定します。
<a href="#">key</a> (キーチェーン), (8 ページ)	キーチェーンのキーを作成または変更します。
<a href="#">key-string</a> (キーチェーン), (12 ページ)	キー文字列のテキストを指定します。
<a href="#">send-lifetime</a> , (14 ページ)	有効なキーを送信します。
<a href="#">show key chain</a> , (16 ページ)	キーチェーンを表示します。

## key-string (キーチェーン)

キーのテキスト文字列を指定するには、キーチェーンのキー コンフィギュレーション モードで **key-string** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**key-string** [**clear**| **password**] *key-string-text*

**no key-string** [**clear**| **password**] *key-string-text*

### 構文の説明

<b>clear</b>	キー文字列をクリアテキスト形式で指定します。
<b>password</b>	キーを暗号化形式で指定します。
<i>key-string-text</i>	キーのテキスト文字列。パーサー プロセスによって暗号化されてから、設定に保存されます。テキスト文字列には、次の文字制限があります。 <ul style="list-style-type: none"> <li>プレーン テキストのキー文字列：最小 1 文字、最大 32 文字。</li> <li>暗号化されたキー文字列：最小 4 文字、上限はなし。</li> </ul>

### コマンド デフォルト

デフォルト値は **clear** です。

### コマンド モード

キーチェーンのキー 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
リリース 3.7.2	このコマンドが追加されました。

### コマンド履歴

リリース	変更内容
リリース 3.3.0	このコマンドが追加されました。

**使用上のガイドライン**

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

暗号化パスワードが有効であるためには、次の条件を満たしている必要があります。

- 文字列に 4 文字以上の偶数個の文字が含まれている。
- パスワード文字列の最初の 2 文字は 10 進数、残りの文字は 16 進数である。
- 最初の 2 桁は 53 以下である。

次の例は、どちらも有効な暗号化パスワードです。

**1234abcd**

または

**50aefd**

**タスク ID**

タスク ID	操作
system	read, write

**例**

次に、**keystring** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router:# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# key-string password 850aefd
```

**関連コマンド**

コマンド	説明
<a href="#">accept-lifetime</a> , (2 ページ)	有効なキーを受け入れます。
<a href="#">key</a> (キーチェーン), (8 ページ)	キーチェーンのキーを作成または変更します。
<a href="#">key chain</a> (キーチェーン), (10 ページ)	キーチェーンを作成または変更します。
<a href="#">send-lifetime</a> , (14 ページ)	有効なキーを送信します。
<a href="#">show key chain</a> , (16 ページ)	キーチェーンを表示します。

## send-lifetime

有効なキーを送信し、ピアのローカル ホストからの情報を認証するには、キーチェーンおよびキー コンフィギュレーションモードで **send-lifetime** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**send-lifetime** *start-time* [**duration** *duration value*| **infinite**| *end-time*]

**no send-lifetime** *start-time* [**duration** *duration value*| **infinite**| *end-time*]

### 構文の説明

<i>start-time</i>	キーが有効になる開始時間を <i>hh:mm:ss</i> 日月年の形式で指定します。範囲は 0:0:0 ~ 23:59:59 です。 日付の範囲は 1 ~ 31 です。 年の範囲は 1993 ~ 2035 です。
<b>duration</b> <i>duration value</i>	(任意) キーのライフタイムを秒で指定します。
<b>infinite</b>	(任意) 一旦有効になると、そのキーは期限切れにならないことを示します。
<i>end-time</i>	(任意) キーが期限切れとなる時刻を <i>hh:mm:ss</i> 日月年の形式で指定します。範囲は 0:0:0 ~ 23:59:59 です。

### コマンド デフォルト

デフォルトの動作または値はありません。

### コマンド モード

キーチェーンのキー 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
リリース 3.7.2	このコマンドが追加されました。

### 使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
system	read, write

## 例

次に、**send-lifetime** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# send-lifetime 1:00:00 June 29 2006 infinite
```

## 関連コマンド

コマンド	説明
<a href="#">accept-lifetime</a> , (2 ページ)	有効なキーを受け入れます。
<a href="#">key</a> (キーチェーン), (8 ページ)	キーチェーンのキーを作成または変更します。
<a href="#">key chain</a> (キーチェーン), (10 ページ)	キーチェーンを作成または変更します。
<a href="#">key-string</a> (キーチェーン), (12 ページ)	キー文字列のテキストを指定します。

# show key chain

キーチェーンを表示するには、EXEC モードで **show key chain** コマンドを使用します。

**show key chain** *key-chain-name*

## 構文の説明

*key-chain-name* 指定したキーチェーンのキーの名前です。最大文字数は32です。

## コマンド デフォルト

デフォルトの動作または値はありません。

## コマンド モード

EXEC

## コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

## 使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
system	read

## 例

セキュアなキーストレージが使用可能になった場合は、ユーザにマスターパスワードの入力を要求し、暗号化してからキー ラベルを表示するのが、キーチェーン管理にとっては望ましい方法です。次の例では、**show key chain** コマンドに対して暗号化キー ラベルだけが表示されます。

```
RP/0/RSP0/CPU0:router# show key chain isis-keys
Key-chain: isis-keys/ -
accept-tolerance -- infinite
Key 8 -- text "8"
```

```
cryptographic-algorithm -- MD5
Send lifetime: 01:00:00, 29 Jun 2006 - Always valid [Valid now]
Accept lifetime: 01:00:00, 29 Jun 2006 - Always valid [Valid now]
```

## 関連コマンド

コマンド	説明
<a href="#">accept-lifetime</a> , (2 ページ)	有効なキーを受け入れます。
<a href="#">accept-tolerance</a> , (4 ページ)	キーチェーンのキーを受け入れる際の許容値を設定します。
<a href="#">key</a> (キーチェーン), (8 ページ)	キーチェーンのキーを作成または変更します。
<a href="#">key chain</a> (キーチェーン), (10 ページ)	キーチェーンを作成または変更します。
<a href="#">key-string</a> (キーチェーン), (12 ページ)	キー文字列のテキストを指定します。
<a href="#">send-lifetime</a> , (14 ページ)	有効なキーを送信します。

■ **show key chain**