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、および例については、『*System Security Configuration Guide for Cisco NCS 5000 Series Routers*』の「Implementing Keychain Management」の章を参照してください。

（注） 現在、デフォルトの VRF のみがサポートされています。VPNv4、VPNv6、および VPN ルーティング/転送（VRF）アドレス ファミリは、今後のリリースでサポートされます。

accept-lifetime

キーチェーン上の認証キーが有効であるとして受信される時間を設定するには、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

start-time	キーが有効になる開始時間を *hh:mm:ss* 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。
duration*duration value*	（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。
infinite	（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。
end-time	（任意）キーが期限切れとなる時刻を *hh:mm:ss* 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 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
system	読み取り、書き込み

例

次に、**accept-lifetime** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# accept-lifetime 1:00:00 June 29 2006 infinite
```

accept-tolerance

ピアが使用する accept キーに許容度または制限値を秒単位で指定するには、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

value	（任意）秒で示される許容値の範囲。範囲は、1 ～ 8640000 です。
infinite	（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 6.0	このコマンドが導入されました。

使用上のガイドライン

command コマンドを設定しない場合は、許容度値はゼロに設定されます。

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	動作
system	読み取り、書き込み

例

次に、**accept-tolerance** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# accept-tolerance infinite
```

cryptographic-algorithm

キーIDに設定し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の選択を指定するには、キーチェーン 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

HMAC-MD5	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。
HMAC-SHA1-12	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。
HMAC-SHA1-20	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。
MD5	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。
SHA-1	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 6.0	このコマンドが導入されました。

使用上のガイドライン

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	動作
system	読み取り、書き込み

例

次に、**ryptographic-algorithm** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# cryptographic-algorithm HMAC-MD5
```

key（キーチェーン）

キーチェーン キーを作成または変更するには、キーチェーン 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 6.0	このコマンドが導入されました。

使用上のガイドライン

Border Gateway Protocol（BGP）のキーチェーン設定では、*key-id* 引数の範囲は 0 ~ 53 である必要があります。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す。

タスク ID

タスク ID	動作
system	読み取り、書き込み

例

次に、**key** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
```

```
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)#
```

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、**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

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

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	動作
system	読み取り、書き込み

例

次に、キーチェーンの isis キーの名前が **key chain** コマンド用である例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
```

```
RP/0/RP0/CPU0:router(config-isis-keys)#
```

key-string（キーチェーン）

キーにテキスト文字列を指定するには、キーチェーン 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

clear	キー文字列をクリアテキスト形式で指定します。
password	キーを暗号化形式で指定します。
key-string-text	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。 • プレーン テキストのキー文字列：最小 1 文字、最大 32 文字。 • 暗号化されたキー文字列：最小 4 文字、上限はなし。

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 6.0	このコマンドが導入されました。

使用上のガイドライン

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	動作
system	読み取り、書き込み

例

次に、**keystring** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router:# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# key-string password 850aefd
```

send-lifetime

有効なキーを送信し、ローカル ホストからピアへの情報を認証するには、キーチェーン 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

start-time	キーが有効になる開始時間を *hh:mm:ss* 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。
duration*duration value*	（任意）キーのライフタイムを秒で指定します。
infinite	（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。
end-time	（任意）キーが期限切れとなる時刻を *hh:mm:ss* 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 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
system	読み取り、書き込み

例

次に、**send-lifetime** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# send-lifetime 1:00:00 June 29 2006 infinite
```

show key chain

キーチェーンを表示するには、**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

パラメータを指定せずにコマンドを使用すると、すべてのキー チェーンのリストを表示します。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
system	読み取り

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。次に、**show key chain** コマンドで暗号化されたキー ラベルのみを表示する例を示します。

```
RP/0/RP0/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]
```