キーチェーン管理の設定

この章では、Cisco NX-OS デバイスでキーチェーン管理を設定する手順について説明します。

この章は、次の内容で構成されています。

キーチェーン管理について

キーチェーン管理を使用すると、キーチェーンの作成と管理を行えます。キーチェーンはキーのシーケンスを意味します（共有秘密ともいいます）。 キーチェーンは、他のデバイスとの通信をキーベース認証を使用して保護する機能と合わせて使用できます。 デバイスでは複数のキーチェーンを設定できます。

キーベース認証をサポートするルーティング プロトコルの中には、キーチェーンを使用してヒットレス キー ロールオーバーによる認証を実装できるものがあります。 詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

キーのライフタイム

安定した通信を維持するためには、キーベース認証で保護されるプロトコルを使用する各デバイスに、1 つの機能に対して同時に複数のキーを保存し使用できる必要があります。 キーチェーン管理は、キーの送信および受け入れライフタイムに基づいて、キー ロールオーバーを処理するセキュアなメカニズムを提供します。 デバイスはキーのライフタイムを使用して、キーチェーン内のアクティブなキーを判断します。

キーチェーンの各キーには次に示す 2 つのライフタイムがあります。

受け入れライフタイム

別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間。

送信ライフタイム

別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。

キーの送信ライフタイムおよび受け入れライフタイムは、次のパラメータを使用して定義します。

Start-time

ライフタイムが開始する絶対時間。

End-time

次のいずれかの方法で定義できる終了時。

- ライフタイムが終了する絶対時間
- 開始時からライフタイムが終了するまでの経過秒数
- 無限のライフタイム（終了時なし）

キーの送信ライフタイム中、デバイスはルーティング アップデート パケットをキーとともに送信します。 送信されたキーがデバイス上のキーの受け入れライフタイム期間内でない場合、そのデバイスはキーを送信したデバイスからの通信を受け入れません。

どのキーチェーンも、キーのライフタイムが重なるように設定することを推奨します。 このようにすると、アクティブなキーがないことによるネイバー認証の失敗を避けることができます。

キーチェーン管理のライセンス要件

次の表に、キーチェーン管理のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	キーチェーン管理にはライセンスは必要ありません。 ライセンス パッケージに含まれていない機能はnx-osイメージにバンドルされており、無料で提供されます。 Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

キーチェーン管理の前提条件

キーチェーン管理には前提条件はありません。

キーチェーン管理の注意事項と制約事項

キーチェーン管理に関する注意事項と制約事項は次のとおりです。

- システム クロックを変更すると、キーがアクティブになる時期に影響が生じます。

キーチェーン管理のデフォルト設定

次の表に、Cisco NX-OS キーチェーン管理パラメータのデフォルト設定を示します。

表 *1*：キーチェーン管理パラメータのデフォルト値

パラメータ	デフォルト
キーチェーン	デフォルトではキーチェーンはありません。
キー	デフォルトでは新しいキーチェーンの作成時にキーは作成されません。
受け入れライフタイム	常に有効です。
送信ライフタイム	常に有効です。
キーストリング入力の暗号化	暗号化されません。

キーチェーン管理の設定

キーチェーンの作成

デバイスにキーチェーンを作成できます。 新しいキーチェーンには、キーは含まれていません。

手順の概要

1. **configure terminal**
2. **key chain** *name*
3. （任意） **show key chain** *name*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**key chain** *name*
	
	例：
	`switch(config)# key chain bgp-keys`
	`switch(config-keychain)#`
		キーチェーンを作成し、キーチェーン コンフィギュレーション モードを開始します。

ステップ 3	**show key chain** *name* 例： `switch(config-keychain)# show key chain bgp-keys`	（任意） キーチェーンの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config-keychain)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

マスター キーの設定および AES パスワード暗号化機能のイネーブル化

キーチェーンの削除

デバイスのキーチェーンを削除できます。

（注） キーチェーンを削除すると、キーチェーン内のキーはどれも削除されます。

はじめる前に

キーチェーンを削除する場合は、そのキーチェーンを使用している機能がないことを確認してください。 削除するキーチェーンを使用するように設定されている機能がある場合、その機能は他のデバイスとの通信に失敗する可能性が高くなります。

手順の概要

1. **configure terminal**
2. **no key chain** *name*
3. （任意） **show key chain** *name*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no key chain** *name* 例： `switch(config)# no key chain bgp-keys`	キーチェーンおよびそのキーチェーンに含まれているすべてのキーを削除します。
ステップ 3	**show key chain** *name* 例： `switch(config-keychain)# show key chain bgp-keys`	（任意） そのキーチェーンが実行コンフィギュレーション内にないことを確認します。
ステップ 4	**copy running-config startup-config** 例： `switch(config-keychain)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

キーチェーンの作成, （4 ページ）

マスターキーの設定およびAESパスワード暗号化機能のイネーブル化

タイプ 6 暗号化用のマスター キーを設定し、高度暗号化規格（AES）パスワード暗号化機能をイネーブルにすることができます。

手順の概要

1. **[no] key config-key ascii**
2. **configure terminal**
3. **[no] feature password encryption aes**
4. （任意） **show encryption service stat**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**[no] key config-key ascii**
	
	例：
	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
		マスター キーを、AES パスワード暗号化機能で使用するように設定します。 マスター キーは、16 ～ 32 文字の英数字を使用できます。 マスター キーを削除するために、いつでもこのコマンドの **no** 形式を使用できます。
		
		マスター キーを設定する前に AES パスワード暗号化機能をイネーブルにすると、マスター キーが設定されていない限りパスワード暗号化が実行されないことを示すメッセージが表示されます。 マスター キーがすでに設定されている場合、新しいマスター キーを入力する前に現在のマスター キーを入力するように求められます。

ステップ 2	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	**[no] feature password encryption aes** 例： `switch(config)# feature password encryption aes`	AES パスワード暗号化機能をイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**show encryption service stat** 例： `switch(config)# show encryption service stat`	（任意） AES パスワード暗号化機能とマスター キーの設定ステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 （注） このコマンドは、実行コンフィギュレーションとスタートアップ コンフィギュレーションのマスター キーを同期するために必要です。

関連トピック

AES パスワード暗号化およびマスター暗号キーについて
AES パスワード暗号化およびマスター暗号キーについて
キーのテキストの設定，（7 ページ）
キーの受け入れライフタイムおよび送信ライフタイムの設定，（9 ページ）
キーのテキストの設定，（7 ページ）
キーの受け入れライフタイムおよび送信ライフタイムの設定，（9 ページ）

キーのテキストの設定

キーのテキストを設定できます。テキストは共有秘密です。デバイスはこのテキストをセキュアな形式で保存します。

デフォルトでは、受け入れライフタイムおよび送信ライフタイムは無限になり、キーは常に有効です。 キーにテキストを設定してから、そのキーの受け入れライフタイムと送信ライフタイムを設定します。

はじめる前に

そのキーのテキストを決めます。 テキストは、暗号化されていないテキストとして入力できます。また、**show key chain** コマンド使用時に Cisco NX-OS がキー テキストの表示に使用する暗号形式で入力することもできます。 特に、別のデバイスから **show key chain** コマンドを実行し、その出力に表示されるキーと同じキー テキストを作成する場合には、暗号化形式での入力が便利です。

手順の概要

1. **configure terminal**
2. **key chain** *name*
3. **key** *key-ID*
4. **key-string** [*encryption-type*] *text-string*
5. （任意） **show key chain** *name* [**mode decrypt**]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**key chain** *name*
	
	例：
	`switch(config)# key chain bgp-keys`
	`switch(config-keychain)#`
		指定したキーチェーンのキーチェーン コンフィギュレーション モードを開始します。

ステップ 3	**key** *key-ID*
	
	例：
	`switch(config-keychain)# key 13`
	`switch(config-keychain-key)#`
		指定したキーのキー コンフィギュレーション モードを開始します。 *key-ID* 引数は、0 ～ 65535 の整数で指定する必要があります。

ステップ 4	**key-string** [*encryption-type*] *text-string*
	
	例：
	`switch(config-keychain-key)#`
	`key-string 0 AS3cureStr1ng`
		そのキーのテキスト ストリングを設定します。 *text-string* 引数は、大文字と小文字を区別して、英数字で指定します。特殊文字も使用できます。
		
		encryption-type 引数に、次のいずれかの値を指定します。
		• 0：入力する *text-string* 引数は暗号化されていないテキストです。 これはデフォルトです。
		• 7：入力する *text-string* 引数は暗号化されています。 シスコ固有の暗号方式で暗号化されます。このオプションは、別の Cisco NX-OS デバイス上で実行した **show key chain** コマンドの暗号化出力に基づいて、テキスト文字列を入力する場合に役立ちます。

	コマンドまたはアクション	目的
ステップ 5	**show key chain** *name* [**mode decrypt**] 例： `switch(config-keychain-key)# show key chain bgp-keys`	（任意） キー テキストの設定も含めて、キーチェーンの設定を表示します。 デバイス管理者だけが使用できる mode decrypt オプションを使用すると、キーはクリアテキストで表示されます。
ステップ 6	**copy running-config startup-config** 例： `switch(config-keychain-key)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

マスター キーの設定および AES パスワード暗号化機能のイネーブル化
キーの受け入れライフタイムおよび送信ライフタイムの設定, （9 ページ）

キーの受け入れライフタイムおよび送信ライフタイムの設定

キーの受け入れライフタイムおよび送信ライフタイムを設定できます。 デフォルトでは、受け入れライフタイムおよび送信ライフタイムは無限になり、キーは常に有効です。

（注） キーチェーン内のキーのライフタイムが重複するように設定することを推奨します。 このようにすると、アクティブなキーがないために、キーによるセキュア通信の切断を避けることができます。

手順の概要

1. **configure terminal**
2. **key chain** *name*
3. **key** *key-ID*
4. **accept-lifetime** [**local**] *start-time* **duration** *duration-value* | **infinite** | *end-time*]
5. **send-lifetime** [**local**] *start-time* **duration** *duration-value* | **infinite** | *end-time*]
6. （任意） **show key chain** *name* [**mode decrypt**]
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**key chain** *name*
	
	例：
	`switch(config)# key chain bgp-keys`
	`switch(config-keychain)#`
		指定したキーチェーンのキーチェーン コンフィギュレーション モードを開始します。

ステップ 3	**key** *key-ID*
	
	例：
	`switch(config-keychain)# key 13`
	`switch(config-keychain-key)#`
		指定したキーのキー コンフィギュレーション モードを開始します。

ステップ 4	**accept-lifetime** [**local**] *start-time* **duration** *duration-value* | **infinite** | *end-time*]
	
	例：
	`switch(config-keychain-key)#`
	`accept-lifetime 00:00:00 Jun 13 2013`
	`23:59:59 Sep 12 2013`
		キーの受け入れライフタイムを設定します。 デフォルトでは、デバイスは *start-time* 引数および *end-time* 引数を UTC として扱います。 **local** キーワードを指定すると、デバイスはこれらの時間を現地時間として扱います。
		start-time 引数は、キーがアクティブになる日時です。
		ライフタイムの終了時は次のいずれかのオプションで指定できます。
		• **duration** *duration-value*：ライフタイムの長さ（秒）。 最大値は 2147483646 秒（約 68 年）です。
		• **infinite**：キーの受け入れライフタイムは期限切れになりません。
		• *end-time*：*end-time* 引数はキーがアクティブでなくなる日時です。

ステップ 5	**send-lifetime** [**local**] *start-time* **duration** *duration-value* | **infinite** | *end-time*]
	
	例：
	`switch(config-keychain-key)#`
	`send-lifetime 00:00:00 Jun 13 2013`
	`23:59:59 Aug 12 2013`
		キーの送信ライフタイムを設定します。 デフォルトでは、デバイスは *start-time* 引数および *end-time* 引数を UTC として扱います。 **local** キーワードを指定すると、デバイスはこれらの時間を現地時間として扱います。
		start-time 引数は、キーがアクティブになる日時です。
		送信ライフタイムの終了時は次のいずれかのオプションで指定できます。
		• **duration** *duration-value*：ライフタイムの長さ（秒）。 最大値は 2147483646 秒（約 68 年）です。

	コマンドまたはアクション	目的
		• **infinite**：キーの送信ライフタイムは期限切れになりません。 • *end-time*：*end-time* 引数はキーがアクティブでなくなる日時です。
ステップ 6	**show key chain** *name* [**mode decrypt**] 例： `switch(config-keychain-key)# show key chain bgp-keys`	（任意） キー テキストの設定も含めて、キーチェーンの設定を表示します。 デバイス管理者だけが使用できる mode decrypt オプションを使用すると、キーはクリアテキストで表示されます。
ステップ 7	**copy running-config startup-config** 例： `switch(config-keychain-key)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

マスター キーの設定および AES パスワード暗号化機能のイネーブル化
キーのライフタイム，（2 ページ）

アクティブなキーのライフタイムの確認

キーチェーン内のキーのうち、受け入れライフタイムまたは送信ライフタイムがアクティブなキーを確認するには、次の表のコマンドを使用します。

コマンド	目的
show key chain	デバイスに設定されているキーチェーンを表示します。

キーチェーン管理の設定の確認

キーチェーン管理の設定情報を表示するには、次の作業を行います。

コマンド	目的
show key chain	デバイスに設定されているキーチェーンを表示します。

キーチェーン管理の設定例

bgp keys という名前のキーチェーンを設定する例を示します。 各キーテキスト ストリングは暗号化されています。 各キーの受け入れライフタイムは送信ライフタイムよりも長くなっています。これは、誤ってアクティブ キーのない時間を設定してもなるべく通信が失われないようにするためです。

```
key chain bgp-keys
  key 0
    key-string 7 zqdest
    accept-lifetime 00:00:00 Jun 01 2013 23:59:59 Sep 12 2013
    send-lifetime 00:00:00 Jun 01 2013 23:59:59 Aug 12 2013
  key 1
    key-string 7 uaeqdyito
    accept-lifetime 00:00:00 Aug 12 2013 23:59:59 May 12 2013
    send-lifetime 00:00:00 Sep 12 2013 23:59:59 Aug 12 2013
  key 2
    key-string 7 eekgsdyd
    accept-lifetime 00:00:00 Nov 12 2013 23:59:59 Mar 12 2013
    send-lifetime 00:00:00 Dec 12 2013 23:59:59 Feb 12 2013
```

次の作業

キーチェーンを使用するルーティング機能については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

キーチェーン管理に関する追加情報

関連資料

関連項目	参照先
ボーダー ゲートウェイ プロトコル	『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』

標準

標準	タイトル
この機能では、新規の標準がサポートされることも、一部変更された標準がサポートされることもありません。また、既存の標準に対するサポートが変更されることもありません。	—