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、次の項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。
- キーチェーンの設定タイプは、クライアントプロトコル内でリンクされているタイプと一致している必要があります。これらのタイプの不一致がある状態で試行されると、ユーザーに通知するための syslog メッセージが生成されます。

  たとえば、 **keychain_abc** という名前のキーチェーンが Macsec キーチェーンとして設定されていても、OSPF でクラシック キーチェーンとして関連付けられている場合はサポートされません。同様に、キーチェーンが最初にクライアントに関連付けられ（前方参照と呼

ばれるプロセス）、別のキーチェーン タイプとして設定される場合もサポートされません。

- ネイバー/テンプレートのパスワードをプログラム的に（restconf/Netconfなどで）設定する場合は、ユーザーのパスワードのタイプとパスワードを指定することを強くお勧めします。プログラムの呼び出しでどちらかのプロパティが欠落している場合、BGPは欠落しているプロパティについて、すでに使用可能な（またはデフォルトの）値を使用して、ネイバー/テンプレートのパスワードを構成します。

  ユーザーがプロパティを指定せずに構成する必要がある場合、ユーザーは両方のピア ルータで同じ手順を実行する必要があります。

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。

Table 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。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:**	グローバル構成モードを開始します。

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**key chain** *name*
	Example:
	`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	(Optional) **show key chain** *name* **Example:** `switch(config-keychain)# show key chain bgp-keys`	キーチェーンの設定を表示します。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-keychain)# 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。

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。

Note 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。

Before you begin

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**no key chain** *name* **Example:** `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。

	Command or Action	Purpose
ステップ 3	(Optional) **show key chain** *name* **Example:** `switch(config-keychain)# show key chain bgp-keys`	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	(Optional) **copy running-config startup-config** **Example:** `switch(config-keychain)# 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。

プライマリ キーの設定および AES パスワード暗号化機能の有効化

タイプ6暗号化用のプライマリ キーを構成し、高度暗号化規格（AES）パスワード暗号化機能を有効にすることができます。

Cisco NX-OS リリース 10.3(3)F 以降では、RPM レガシー キーチェーンでタイプ 6 暗号化がサポートされています。

Procedure

	Command or Action	Purpose

ステップ 1	[**no**] **key config-key ascii**[<new_key> old <old_master_key>]
	Example:
	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
		プライマリ キー（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。プライマリ キーは、16 ～ 32 文字の英数字を使用できます。このコマンドの **no** 形式を使用すると、いつでもプライマリ キーを削除できます。
		プライマリ キーを設定する前に AES パスワード暗号化機能を有効にすると、プライマリ 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。プライマリ キーがすでに設定されている場合は、新しいプライマリ キーを入力する前に現在のプライマリ キーを入力するように求められます。
		Note
		Cisco NX-OS リリース 10.3(2)F 以降、DME ペイロードおよび非インタラクティブ モードを使用して、プライマリ キーを構成できます。

	Command or Action	Purpose

ステップ 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 3	[**no**] **feature password encryption aes tam** **Example:** `switch(config)# feature password encryption aes tam`	AES パスワード暗号化機能を有効化または無効化します。
ステップ 4	**encryption re-encrypt obfuscated** **Example:** `switch(config)# encryption re-encrypt obfuscated`	既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換します。
ステップ 5	(Optional) **show encryption service stat** **Example:** `switch(config)# show encryption service stat`	AES パスワード暗号化機能とプライマリ キーの設定ステータスを表示します。
ステップ 6	**copy running-config startup-config** **Example:** `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。 **Note** 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プライマリ キーを同期するために必要です。

Related Topics

AES パスワード暗号化およびプライマリ暗号キーについて
AES パスワード暗号化およびプライマリ暗号キーについて
キーのテキストの設定 （6 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。

MACsec および RPM レガシー キーチェーンの場合、AES パスワード暗号化機能が有効になっており、プライマリ キーが構成されている場合、テキストはタイプ 6 形式で暗号化されて保存されます。それ以外の場合は、タイプ 7 暗号化形式で保存されます。

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。

Before you begin

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**key chain** *name*
	Example:
	`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*
	Example:
	`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* **Example:** `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。*key-ID* 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：入力した *text-string* 引数は、暗号化されていないテキスト文字列です。これがデフォルトです。 • 6：Cisco NX-OS リリース 10.3(3)F 以降、Cisco Nexus 9000 シリーズ プラットフォーム スイッチでシスコ独自の（タイプ 6 暗号化）方式がサポートされています。

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td></td><td></td><td>
7：入力した 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。
key-string コマンドには、text-string での次の特殊文字の使用に関する制限があります。
<table>
<tr><th>特殊文字</th><th>説明</th></tr>
<tr><td>|</td><td>縦棒</td></tr>
<tr><td>></td><td>右辺</td></tr>
<tr><td>\</td><td>バッ</td></tr>
<tr><td>(</td><td>左丸</td></tr>
<tr><td>'</td><td>アポ</td></tr>
<tr><td>"</td><td>引用</td></tr>
<tr><td>?</td><td>疑問</td></tr>
</table>
コマンドでの特殊文字の使用方法の詳細については、「コマンドラインインターフェイスについて」セクションを参照してください。
</td></tr>
<tr><td>ステップ 5</td><td>(Optional) show key chain name [mode decrypt]
Example:
<pre>switch(config-keychain-key)# show key chain bgp-keys</pre></td><td>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。</td></tr>
</table>

	Command or Action	Purpose
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-keychain-key)# 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。

Related Topics

プライマリ キーの設定および AES パスワード暗号化機能の有効化

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

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。

Note 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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**key chain** *name*
	Example:
	`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*
	Example:
	`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*] **Example:** `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* 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。

	Command or Action	Purpose
		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*：The *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*] **Example:** `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* 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。 • **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*：The *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	(Optional) **show key chain** *name* [**mode decrypt**] **Example:** `switch(config-keychain-key)# show key chain bgp-keys`	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。

	Command or Action	Purpose
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-keychain-key)# 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。

Related Topics

プライマリ キーの設定および AES パスワード暗号化機能の有効化

OSPFv2 暗号化認証用のキーの設定

OSPFv2のメッセージダイジェスト5（MD5）またはハッシュベースのメッセージ認証コードセキュアハッシュアルゴリズム（HMAC-SHA）認証を設定できます。

手順

	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)#`
		グローバル構成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。
		（注）
		OSPFv2 の場合、key key-id コマンドのキー ID の値は 0 ～ 255 です。

ステップ 4	[**no**] **cryptographic-algorithm** {**HMAC-SHA-1** | **HMAC-SHA-256** | **HMAC-SHA-384** | **HMAC-SHA-512** | **MD5**} 例： `switch(config-keychain-key)# cryptographic-algorithm HMAC-SHA-1`	指定キーに使用される OSPFv2 暗号アルゴリズムを設定します。1 つのキーに設定できる暗号化アルゴリズムは 1 つだけです。

	コマンドまたはアクション	目的
ステップ 5	（任意） **show key chain** *name* 例： `switch(config-keychain-key)# show key chain bgp-keys`	キーチェーンの設定を表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config-keychain-key)# 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。

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	デバイスで設定された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 *name*	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

「ospf-keys」 という名前のキーチェーンを構成する例を示します。各キー テキスト ストリングは暗号化されています。キーは、暗号化アルゴリズムとして MD5 を使用するように構成されます。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いため、キーのペア間で重複が発生します。この例では、キー 1 とキー 2、およびキー 2 とキー 3 の間にオーバーラップが設定されています。これにより、アクティブなキーがない期間が回避され、基盤となるプロトコルの通信の中断を回避できます。

```
key chain ospf-keys
  key 1
    key-string 7 070c285f4d0658544541
    accept-lifetime local 00:00:00 May 13 2024  12:00:00 Sep 14 2024
    send-lifetime local 00:00:00 May 13 2024  00:00:00 Sep 14 2024
```

```
    cryptographic-algorithm MD5
  key 2
    key-string 7 070c285f4d0658574446
    accept-lifetime local 00:00:00 Sep 13 2024  12:00:00 Jan 15 2025
    send-lifetime local 10:00:00 Sep 13 2024  12:00:00 Jan 15 2025
    cryptographic-algorithm MD5
  key 3
    key-string 7 070c285fad0622474941
    accept-lifetime local 00:00:00 Jan 15 2025  12:00:00 Jun 15 2025
    send-lifetime local 10:00:00 Jan 15 2025  12:00:00 Jun 15 2025
    cryptographic-algorithm MD5
```

次に、タイプ 6 暗号を使用する「bgp-keys」という名前のキーチェーンを構成する例を示します。この暗号化モードは、feature password encryption aes が有効になっている場合に使用できます。

```
key chain bgp-keys
  key 1
    key-string 6
JDYkbN6ZTz3Hqrv5ZWliyxqlYiQXYc0wWpOnK7epMGoHK6qVJPeJtSYAGhQ9V+QKG4ZrcWeuunTtAA==
    accept-lifetime local 00:00:00 May 13 2024  12:00:00 Sep 14 2024
    send-lifetime local 00:00:00 May 13 2024  00:00:00 Sep 14 2024
  key 2
    key-string 6
JDYkO6Di45Bu1ikPja/r8VJNoSTa4I4QMxtzzG3DQzal9G9LJA6F1WNGX8GRgn95SPuf4naoTZCtAA==
    accept-lifetime local 00:00:00 Sep 13 2024  12:00:00 Jan 15 2025
    send-lifetime local 10:00:00 Sep 13 2024  12:00:00 Jan 15 2025
  key 3
    key-string 6
JDYk8DJ15ZdOQ/O7vnj2M92lRiR2x8VrL0Muj/30TNlIK5f+JMFEHoWy0Rfuy827G/H10w2it7eVAA==
    accept-lifetime local 00:00:00 Jan 15 2025  12:00:00 Jun 15 2025
    send-lifetime local 10:00:00 Jan 15 2025  12:00:00 Jun 15 2025
```

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	マニュアル タイトル
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*』
OSPFv2	『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。