キーチェーン管理の実装

このモジュールでは、キーチェーン管理の実装方法について説明します。キーチェーン管理は、相互に信頼を確立する前に、キーなどの秘密を交換するすべてのエンティティに共有秘密を設定する、認証の一般的な方法です。 Cisco IOS XR ソフトウェアのルーティング プロトコルおよびネットワーク管理アプリケーションでは、ピアとの通信中におけるセキュリティ向上のために、認証が頻繁に使用されます。

キーチェーン管理の実装の機能履歴

リリース	変更点
リリース 3.7.2	この機能を追加しました。

キーチェーン管理の設定に関する前提条件

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。 このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

キーチェーン管理の実装に関する制約事項

システム クロックを変更すると、既存の設定におけるキーの有効性に影響を与えることに注意してください。

キーチェーン管理の実装について

キーチェーン自体は関連性を持っていません。このため、キー（認証用）を使用してピアと通信する必要があるアプリケーションで使用される必要があります。キーチェーンは、ライフタイムに基づいてキーとロールオーバーを処理する、セキュリティの高いメカニズムを提供します。ボーダー ゲートウェイ プロトコル（BGP）、Open Shortest Path First（OSPF）、および Intermediate System-to-Intermediate System（IS-IS）では、キーチェーンを使用して認証用のヒットレス キー ロールオーバーを実装します。BGP は TCP 認証を使用します。この認証では、認証オプションを有効にし、キーチェーン用に設定された暗号化アルゴリズムに基づいたメッセージ認証コード（MAC）を送信します。BGP、OSPF、および IS-IS のキーチェーン設定の詳細については、を参照してください。

- リソース予約プロトコル（RSVP）は、認証にキーチェーンを使用します。 RSVP の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide*』を参照してください。
- IP サービス レベル契約（IP SLA）は、IP SLA 制御メッセージの MD5 認証にキーチェーンを使用します。 IP SLA の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Configuration Guide*』を参照してください。また、**key-chain** コマンドの詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Comand Reference*』を参照してください。

キーチェーン管理を実装するには、次の項で説明されているキーのライフタイムの概念を理解しておく必要があります。

キーのライフタイム

セキュリティ方式としてキーを使用する場合は、キーのライフタイムを指定して、期限が切れた際には定期的にキーを変更する必要があります。 安定性を維持するには、各パーティがアプリケーションのキーを複数保存して同時に使用できるようにする必要があります。 キーチェーンは、同じピア、ピアのグループ、またはその両方を認証するために一括管理されている一連のキーです。

キーチェーン管理では、一連のキーをキーチェーンの下にまとめてグループ化し、キーチェーン内の各キーをライフタイムに関連付けます。

（注） ライフタイムが設定されていないキーはすべて無効と見なされるため、キーは設定中に拒否されます。

キーのライフタイムは、次のオプションによって定義されます。

- Start-time：絶対時間を指定します。
- End-time：開始時間に対応する絶対時間を指定するか、無期限を指定します。

キーチェーン内のそれぞれのキーの定義では、キーが有効な期間（ライフタイムなど）を指定する必要があります。 指定したキーのライフタイム期間中は、この有効なキーとともにルーティング更新パケットが送信されます。 キーが有効ではない期間はキーを使用できません。 このため、指定したキーチェーンでは、キーの有効期間を重複させて、有効なキーの不在期間をなくすことを推奨します。 有効なキーの不在期間が発生した場合、ネイバー認証は行われず、ルーティング更新は失敗します。

複数のキーチェーンを指定できます。

キーチェーン管理の実装方法

この項では、次の手順について説明します。

キーチェーンの設定

この作業では、キーチェーンの名前を設定します。

キーチェーンの名前を作成または変更できます。

手順の概要

1. **configure**
2. **key chain** *key-chain-name*
3. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
4. **show key chain** *key-chain-name*

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** 例： `RP/0/RSP0/CPU0:router# configure`	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** *key-chain-name*
	
	例：
	`RP/0/RSP0/CPU0:router(config)# key chain isis-keys`
	`RP/0/RSP0/CPU0:router(config-isis-keys)#`
		キーチェーンの名前を作成します。
		
		（注） キーの ID を設定せずにキーチェーン名のみを設定しても、操作は無効と見なされます。 設定を終了しても、キーの ID と 1 つ以上のグローバル コンフィギュレーション モードの属性または keychain-key コンフィギュレーション モードの属性（ライフタイムやキー文字列など）を設定するまでは、変更のコミットは要求されません。

ステップ 3	次のいずれかのコマンドを使用します。
	
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	**show key chain** *key-chain-name* 例： `RP/0/RSP0/CPU0:router# show key chain isis-keys`	（任意）キーチェーン名を表示します。 （注） *key-chain-name* 引数はオプションです。 *key-chain-name* 引数の名前を指定しない場合、すべてのキーチェーンが表示されます。

次の作業

キーチェーン設定が完了したら、キーを受け付ける許容値の設定，（5 ページ）の項を参照してください。

キーを受け付ける許容値の設定

この作業では、キーを受け付ける許容値を設定し、キーチェーンによるアプリケーション（ルーティングプロトコルや管理プロトコルなど）のヒットレスキーロールオーバーを容易にします。

手順の概要

1. **configure**
2. **key chain** *key-chain-name*
3. **accept-tolerance** *value* [**infinite**]
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

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** 例： `RP/0/RSP0/CPU0:router# configure`	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** *key-chain-name* 例： `RP/0/RSP0/CPU0:router(config)# key chain isis-keys`	キーチェーンの名前を作成します。

	コマンドまたはアクション	目的
ステップ 3	**accept-tolerance** *value* [**infinite**] 例： `RP/0/RSP0/CPU0:router(config-isis-keys)# accept-tolerance infinite`	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。 • *value* 引数を使用して、許容値の範囲を秒数で設定します。 範囲は、1 ～ 8640000 です。 • **infinite** キーワードを使用して、許容値が無期限であることを指定します。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

キーチェーンのキー ID の設定

この作業では、キーチェーンのキー ID を設定します。

キーチェーンのキーを作成または変更できます。

手順の概要

1. **configure**
2. **key chain** *key-chain-name*
3. **key** *key-id*
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

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** 例： `RP/0/RSP0/CPU0:router# configure`	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** *key-chain-name* 例： `RP/0/RSP0/CPU0:router(config)# key chain isis-keys`	キーチェーンの名前を作成します。
ステップ 3	**key** *key-id* 例： `RP/0/RSP0/CPU0:router(config-isis-keys)# key 8`	キーチェーンのキーを作成します。 キー ID 番号は 10 進数から 16 進数に変換され、コマンド モード サブプロンプトが作成されます。 • *key-id* 引数は 48 ビット整数型として使用します。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。

	コマンドまたはアクション	目的
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

次の作業

キーチェーンのキー ID を設定したら、キー文字列のテキストの設定, （8 ページ）の項を参照してください。

キー文字列のテキストの設定

この作業では、キー文字列のテキストを設定します。

手順の概要

1. **configure**
2. **key chain** *key-chain-name*
3. **key** *key-id*
4. **key-string** [**clear** | **password**] *key-string-text*
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

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** 例： `RP/0/RSP0/CPU0:router# configure`	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。

	コマンドまたはアクション	目的
ステップ 2	**key chain** *key-chain-name* 例： `RP/0/RSP0/CPU0:router(config)# key chain isis-keys`	キーチェーンの名前を作成します。

ステップ 3	**key** *key-id*
	
	例：
	`RP/0/RSP0/CPU0:router(config-isis-keys)# key 8`
	`RP/0/RSP0/CPU0:router(config-isis-keys-0x8)#`
		キーチェーンのキーを作成します。

ステップ 4	**key-string** [**clear** | **password**] *key-string-text* 例： `RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# key-string password 8`	キーのテキスト文字列を指定します。 • クリア テキスト形式でキー文字列を指定するには **clear** キーワードを使用します。暗号化形式でキーを指定するには **password** キーワードを使用します。 • 文字列を有効なパスワードにするには、次の規則に従う必要があります。 ◦ 偶数個の文字が含まれている。 ◦ 最小文字数は 4 文字である。 ◦ 最初の 2 桁は 10 進数、残りの桁は 16 進数である。 ◦ 最初の 2 桁は 53 以下である。 有効なパスワードの例は、次のとおりです。 ◦ 12abcd ◦ 32986510 •
ステップ 5	次のいずれかのコマンドを使用します。 • **end** • **commit** 例： `RP/0/RSP0/CPU0:router(config)# end`	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 `Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:` ◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレー

	コマンドまたはアクション	目的
	または `RP/0/RSP0/CPU0:router(config)# commit`	ション セッションが終了して、ルータが EXEC モードに戻ります。 ◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 ◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

次の作業

キー文字列のテキストを設定したら、アウトバウンド アプリケーションのトラフィックの認証ダイジェストを生成するキーの設定, （12 ページ）の項を参照してください。

有効なキーの確認

この作業では、ローカル アプリケーションがリモート ピアを認証するための有効なキーを決定します。

手順の概要

1. **configure**
2. **key chain** *key-chain-name*
3. **key** *key-id*
4. **accept-lifetime** *start-time* [**duration** *duration-value* | **infinite** | *end-time*]
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

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** 例： `RP/0/RSP0/CPU0:router# configure`	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** *key-chain-name* 例： `RP/0/RSP0/CPU0:router(config)# key chain isis-keys`	キーチェーンの名前を作成します。

ステップ 3	**key** *key-id*
	
	例：
	`RP/0/RSP0/CPU0:router(config-isis-keys)# key 8`
	`RP/0/RSP0/CPU0:router(config-isis-keys-0x8)#`
		キーチェーンのキーを作成します。

ステップ 4	**accept-lifetime** *start-time* [**duration** *duration-value* | **infinite** | *end-time*] 例： `RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# accept-lifetime 1:00:00 october 24 2005 infinite`	（任意）クロック タイムの観点から、キーのライフタイムの有効性を指定します。

ステップ 5	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュ

	コマンドまたはアクション	目的
		レーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

アウトバウンドアプリケーションのトラフィックの認証ダイジェストを生成するキーの設定

この作業では、アウトバウンド アプリケーションのトラフィックの認証ダイジェストを生成するキーを設定します。

手順の概要

1. **configure**
2. **key chain** *key-chain-name*
3. **key** *key-id*
4. **send-lifetime** *start-time* [**duration** *duration-value* | **infinite** | *end-time*]
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

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** 例： `RP/0/RSP0/CPU0:router# configure`	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** *key-chain-name* 例： `RP/0/RSP0/CPU0:router(config)# key chain isis-keys`	キーチェーンの名前を作成します。

	コマンドまたはアクション	目的

ステップ 3	**key** *key-id*
	
	例：
	`RP/0/RSP0/CPU0:router(config-isis-keys)# key 8`
	`RP/0/RSP0/CPU0:router(config-isis-keys-0x8)#`
		キーチェーンのキーを作成します。

ステップ 4	**send-lifetime** *start-time* [**duration** *duration-value* | **infinite** | *end-time*] 例： `RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# send-lifetime 1:00:00 october 24 2005 infinite`	（任意）キーチェーンの認証キーが有効に送信される設定期間を指定します。 クロック タイムの観点から、キーのライフタイムの有効性を指定できます。 さらに、start-time 値と次のいずれかの値を指定できます。 • **duration** キーワード（秒） • **infinite** キーワード • *end-time* 引数 キーのライフタイムを設定する場合は、ネットワーク タイム プロトコル（NTP）または他の時刻同期方式を推奨します。

ステップ 5	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

	コマンドまたはアクション	目的

暗号化アルゴリズムの設定

この作業では、暗号化アルゴリズムを選択してキーチェーン設定に反映できます。

手順の概要

1. **configure**
2. **key chain** *key-chain-name*
3. **key** *key-id*
4. **cryptographic-algorithm** [**HMAC-MD5** | **HMAC-SHA1-12** | **HMAC-SHA1-20** | **MD5** | **SHA-1**]
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

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** 例： `RP/0/RSP0/CPU0:router# configure`	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** *key-chain-name*
	
	例：
	`RP/0/RSP0/CPU0:router(config)# key chain isis-keys`
	`RP/0/RSP0/CPU0:router(config-isis-keys)#`
		キーチェーンの名前を作成します。

ステップ 3	**key** *key-id*
	
	例：
	`RP/0/RSP0/CPU0:router(config-isis-keys)# key 8`
	`RP/0/RSP0/CPU0:router(config-isis-keys-0x8)#`
		キーチェーンのキーを作成します。

	コマンドまたはアクション	目的
ステップ 4	**cryptographic-algorithm** [**HMAC-MD5** | **HMAC-SHA1-12** | **HMAC-SHA1-20** | **MD5** | **SHA-1**] 例： `RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# cryptographic-algorithm MD5`	暗号化アルゴリズムを選択します。 次のアルゴリズムのリストから選択できます。 • HMAC-MD5 • HMAC-SHA1-12 • HMAC-SHA1-20 • MD5 • SHA-1 ルーティング プロトコルは、それぞれ異なる暗号化アルゴリズムのセットをサポートしています。 • 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 と HMAC-MD5 だけをサポート

ステップ 5	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。

	コマンドまたはアクション	目的
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

キーチェーン管理の実装の設定例

この項では、次の設定例について説明します。

キーチェーン管理の設定：例

次に、キーチェーン管理を設定する例を示します。

```
configure
key chain isis-keys
accept-tolerance infinite
key 8
key-string mykey91abcd
cryptographic-algorithm MD5
send-lifetime 1:00:00 june 29 2006 infinite
accept-lifetime 1:00:00 june 29 2006 infinite
end

Uncommitted changes found, commit them? [yes]: yes

show key chain isis-keys

Key-chain: isis-keys/ -

accept-tolerance -- infinite
Key 8 -- text "1104000E120B520005282820"
  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]
```

参考資料

ここでは、キーチェーン管理の実装に関連する参考資料について説明します。

関連資料

関連項目	ドキュメント名
キーチェーン管理のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference*』のキーチェーン管理コマンド

標準

標準	タイトル
この機能でサポートが追加または変更された標準はありません。また、この機能で変更された既存の標準のサポートはありません。	—

MIB

MIB	MIB リンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検出およびダウンロードするには、URL（http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）にある Cisco MIB Locator を使用して、[Cisco Access Products] メニューでプラットフォームを選択します。

RFC

RFC	タイトル
この機能でサポートが追加または変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html