『ユーザ セキュリティ コンフィギュレーション ガイド』

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

Cisco IOS Login Enhancements（Login Block） 3

機能情報の確認 3

Cisco IOS Login Enhancements について 4

サービス拒絶攻撃および辞書ログイン攻撃からの保護 4

Login Enhancements 機能の概要 4

連続するログイン試行間の遅延 4

DoS 攻撃が疑われる場合のログイン シャットダウン 5

Cisco IOS Login Enhancement の設定方法 5

ログイン パラメータの設定 5

次の作業 7

ログイン パラメータの確認 7

ログイン パラメータの設定例 9

ログイン パラメータの設定例 9

その他の参考資料 9

Cisco IOS Login Enhancements（Login Block）に関する機能情報 11

パスワード、特権、およびログインによるセキュリティ設定 13

機能情報の確認 14

パスワード、特権、およびログインによるセキュリティ設定の制約事項 14

パスワード、特権、およびログインによるセキュリティ設定について 14

セキュリティ スキームを作成する利点 14

Cisco IOS XE CLI モード 15

ユーザ EXEC モード 16

特権 EXEC モード 18

グローバル コンフィギュレーション モード 20

インターフェイス コンフィギュレーション モード 21

サブインターフェイス コンフィギュレーション モード 22

Cisco IOS XE CLI セッション 23
ローカル CLI セッション 23
リモート CLI セッション 23
端末回線はローカルおよびリモート CLI セッションに使用される 24
Cisco IOS XE EXEC モードへのアクセスの保護 24
ユーザ EXEC モードへのアクセスの保護 25
特権 EXEC モードへのアクセスの保護 25
Cisco IOS XE のパスワード暗号化レベル 25
Cisco IOS XE CLI セッションのユーザ名 27
Cisco IOS XE の特権レベル 27
Cisco IOS XE のパスワード設定 28
パスワード、特権、およびログインによるセキュリティの設定方法 29
ユーザ EXEC モードへのアクセスの保護 29
リモート CLI セッションのパスワードの設定と確認 29
トラブルシューティングのヒント 31
次の作業 31
ローカル CLI セッションのパスワードの設定と確認 32
トラブルシューティングのヒント 33
次の作業 34
特権 EXEC モードへのアクセスの保護 34
イネーブル パスワードの設定と確認 34
トラブルシューティングのヒント 36
次の作業 36
クリア テキスト パスワードのパスワード暗号化の設定 36
イネーブル シークレット パスワードの設定と確認 37
トラブルシューティングのヒント 39
次の作業 39
ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定 39
CLI セッションとコマンドへのアクセスを管理するセキュリティ オプションの設定 41
窓口のテクニカル サポート スタッフ用のネットワーク デバイスの設定 42
窓口のテクニカル サポート スタッフ用の設定の確認 44

トラブルシューティングのヒント 47
次の作業 47
窓口のテクニカル サポート スタッフのユーザ名を必須にするデバイスの設定 47
ローカル セッションの忘失パスワードおよび誤設定パスワードの復元 51
ネットワーク デバイスがリモート CLI セッションを許可するように設定されている 51
ネットワーク デバイスがリモート CLI セッションを許可するように設定されていない 51
リモート セッションの忘失パスワードおよび誤設定パスワードの復元 51
ネットワーク デバイスがローカル CLI セッションを許可するように設定されている 51
ネットワーク デバイスがローカル CLI セッションを許可するように設定されていない 52
特権 EXEC モードの忘失パスワードまたは誤設定パスワードの復元 52
誤設定された特権 EXEC モードのパスワードが保存されていない 52
パスワード、特権、およびログインによるセキュリティ設定の設定例 53
例：ユーザがリモート セッションをクリア可能にするデバイスの設定 53
例：ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定 54
例：ユーザがインターフェイスをシャットダウンおよびイネーブル化することを可能にするデバイスの設定 55
次の作業 56
その他の参考資料 56
パスワード、特権、およびログインによるセキュリティ設定に関する機能情報 58
ロールベースの CLI アクセス 61
機能情報の確認 61
ロールベースの CLI アクセスの前提条件 62
ロールベースの CLI アクセスの制約事項 62
ロールベースの CLI アクセスに関する情報 62
CLI ビューを使用するメリット 62
ルート ビュー 62
合法的傍受ビュー 63
スーパービュー 63

ビュー認証と新しい AAA 属性 63
ロールベースの CLI アクセスの使用方法 64
CLI ビューの設定 64
トラブルシューティングのヒント 66
合法的傍受ビューの設定 66
トラブルシューティングのヒント 68
スーパービューの設定 68
ビューとビュー ユーザのモニタリング 70
ロールベースの CLI アクセスの設定例 70
例：CLI ビューの設定 70
例：CLI ビューの確認 70
例：合法的傍受ビューの設定 71
例：スーパービューの設定 72
ロールベースの CLI アクセスに関する追加情報 72
ロールベースの CLI アクセスに関する機能情報 73
AutoSecure 75
機能情報の確認 75
AutoSecure の制約事項 76
AutoSecure について 76
管理プレーンのセキュリティ保護 76
グローバル サービスのディセーブル化 76
サービスのインターフェイス単位のディセーブル化 77
グローバル サービスのイネーブル化 78
ルータへのアクセスの保護 78
セキュリティ ロギング 79
フォワーディング プレーンのセキュリティ保護 80
AutoSecure の設定方法 81
AutoSecure の設定 81
強化されたルータへのセキュリティ アクセスの設定 82
AutoSecure の設定例 83
その他の参考資料 85
AutoSecure に関する機能情報 86

Kerberos の設定 89

機能情報の確認 89

Kerberos に関する情報 89

Kerberos クライアントのサポート操作 92

境界ルータに対する認証 92

KDC からの TGT の取得 93

ネットワーク サービスに対する認証の取得 93

Kerberos を設定する方法 94

Kerberos コマンドによる KDC の設定 95

KDC データベースへのユーザの追加 95

KDC での SRVTAB の作成 96

SRVTAB の抽出 97

Kerberos プロトコルを使用するルータの設定 97

Kerberos レルムの定義 97

SRVTAB ファイルのコピー 99

Kerberos 認証の指定 100

認定証転送のイネーブル化 100

ルータに対する Telnet セッションの開始 100

暗号化された Kerberos 対応 Telnet セッションの確立 101

必須の Kerberos 認証のイネーブル化 102

Kerberos インスタンス マッピングのイネーブル化 102

Kerberos の監視とメンテナンス 103

Kerberos 設定の例 103

Kerberos レルムの定義例 103

SRVTAB ファイルのコピー例 104

暗号化された Telnet セッションの例 104

その他の参考資料 104

Kerberos の設定に関する機能情報 106

合法的傍受アーキテクチャ 109

機能情報の確認 110

合法的傍受の前提条件 110

合法的傍受の制約事項 111

合法的傍受に関する情報 111
合法的傍受の概要 111
Cisco Service Independent Intercept アーキテクチャ 111
PacketCable 合法的傍受アーキテクチャ 112
CISCO ASR 1000 シリーズ ルータ 112
VRF 対応 LI 113
合法的傍受 MIB 114
合法的傍受 MIB へのアクセスの制限 114
RADIUS ベースの合法的傍受 115
傍受の動作 115
Service Independent Intercept（SII） 116
信頼できるホストへのアクセス制限（暗号化なし） 117
合法的傍受をするトラフィックの暗号化および信頼できるホストへのアクセス制限 117
ルータの暗号化の設定 117
信頼できるホストへのアクセス制限（暗号化あり） 118
VPN クライアントの設定 118
合法的傍受の設定方法 119
合法的傍受 MIB の制限付き SNMP ビューの作成 119
次の作業 121
合法的傍受のための SNMP 通知のイネーブル化 121
SNMP 通知のディセーブル 123
RADIUS セッション傍受のイネーブル化 124
回線 ID ベースのタッピングの設定 127
合法的傍受の設定例 130
例：メディエーション デバイス アクセスの合法的傍受 MIB の有効化 130
例：RADIUS セッションの合法的傍受のイネーブル化 130
その他の参考資料 131
合法的傍受に関する機能情報 132
IPoE セッションの LI サポート 137
機能情報の確認 137
IPoE セッションの LI サポートの制約事項 137

IPoE セッションの LI サポートに関する追加情報 138
IPoE セッションの LI サポートに関する機能情報 139
イメージ検証 141
機能情報の確認 141
イメージ検証の制約事項 142
イメージ検証について 142
イメージ検証の利点 142
イメージ検証の動作 142
イメージ検証の使用方法 143
イメージの完全性のグローバルな検証 143
次の作業 144
コピーしようとしているイメージの完全性の検証 144
リロードしようとしているイメージの完全性の検証 145
イメージ検証の設定例 146
グローバル イメージ検証の例 146
copy コマンドを使用したイメージ検証の例 147
reload コマンドを使用したイメージ検証の例 147
verify コマンドの出力例 147
その他の参考資料 147
イメージ検証に関する機能情報 149

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

Cisco IOS XE リリース 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、コンバージドリリースの 1 つのバージョン - Cisco IOS XE 16 - に統合されました。この 1 つのリリースでスイッチングおよびルーティング ポートフォリオのアクセスおよびエッジ製品を幅広くカバーしています。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が、使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術構成ガイドが製品のランディング ページに表示されると、その機能が該当のプラットフォームでサポートされているかどうかが示されます。

第 2 章

Cisco IOS Login Enhancements（Login Block）

Cisco IOS Login Enhancements（Login Block）機能により、ユーザはサービス拒絶（DoS）攻撃と思われる攻撃が検出された場合、ログイン試行を自動的にブロックするオプションを設定して、ルータのセキュリティを強化できます。

この機能により導入された Login Block オプションおよび Login Delay オプションで、Telnet または SSH 仮想接続を設定できます。この機能をイネーブルにすると、接続試行の失敗が複数回検出された場合に、「待機時間」を強制して「辞書攻撃」をスローダウンし、ルーティング デバイスをサービス拒絶（DoS）攻撃攻撃から保護できます。

- 機能情報の確認，3 ページ
- Cisco IOS Login Enhancements について，4 ページ
- Cisco IOS Login Enhancement の設定方法，5 ページ
- ログイン パラメータの設定例，9 ページ
- その他の参考資料，9 ページ
- Cisco IOS Login Enhancements（Login Block）に関する機能情報，11 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Cisco IOS Login Enhancements について

サービス拒絶攻撃および辞書ログイン攻撃からの保護

ユーザまたは経営幹部レベルで、デバイスを管理する目的によるルーティング デバイスへの接続は、リモート コンソール（PC など）から Telnet または SSH（セキュア シェル）を使用して最も頻繁に実行されます。ユーザのデバイスと管理デバイスとの間の通信トラフィックが暗号化されるため、SSH では、よりセキュアな接続オプションが提供されます。Login Block 機能をイネーブルにすると、Telnet 接続と SSH 接続の両方に適用されます。

この機能によって導入される自動有効化、および Login Block 機能および Quiet Period 機能のロギングは、個人が使用するとネットワーク デバイスを阻害したり、損なう可能性のある 2 つの既知の方法に特に対処したりすることで、デバイスのセキュリティをさらに強化するように設計されています。

デバイスの接続アドレスが検出され、到達可能である場合、悪意あるユーザが接続要求のフラッディングによってデバイスの通常の動作を妨げようとする可能性があります。通常のルーティング サービスを適切に処理しようとして、繰り返し行われるログイン接続試行を処理しようとしたり、デバイスがビジーになったり、正規のシステム管理者に通常のログイン サービスを提供できなくなる可能性があるため、この種の攻撃は、サービス拒絶（DoS）攻撃の試行と呼ばれます。

辞書攻撃の主な意図は、一般的な DoS 攻撃とは異なり、デバイスへの管理アクセスを実際に取得することです。辞書攻撃とは、数千、時には数百万ものユーザ名/パスワードの組み合わせでログインを試行する自動プロセスです（このタイプの攻撃は、まず最初に、有効なパスワードとして一般的な辞書で見られるあらゆる言葉が使用されるため、「辞書攻撃」と呼ばれています）。このアクセスを試行するためにスクリプトやプログラムが使用されていて、このような試みのプロファイルは通常、DoS 試行のものと同じです。短期間で複数のログインを試行します。

検出プロファイルをイネーブルにすることにより、ログイン試行の失敗が反復する場合は、以降の接続要求を拒否して対応するように、ルーティングデバイスを設定できます（ログインブロッキング）。このブロックには「待機時間」と呼ばれる、一定の時間を設定できます。システム管理者との関連付けが把握されているアドレスを使用してアクセス リスト（ACL）を設定し、待機時間中でも正規の接続試行を許可できます。

Login Enhancements 機能の概要

連続するログイン試行間の遅延

シスコのデバイスは、仮想接続をできる限り高速で処理して受け入れることができます。ログイン試行間に遅延を導入すると、シスコのデバイスを辞書攻撃や DoS 攻撃などの悪意あるログイン接続から保護することができます。遅延は次のいずれかの方法でイネーブルにできます。

- **auto secure** コマンドを介します。AutoSecure 機能をイネーブルにすると、デフォルトで 1 秒のログイン遅延時間が自動的に強制されます。

- **login block-for** コマンドを介します。**login delay** コマンドを発行する前に、このコマンドを入力する必要があります。**login block-for** コマンドのみを入力すると、デフォルトで 1 秒のログイン遅延時間が自動的に強制されます。
- ログイン遅延時間の強制を秒単位で指定できる、新しいグローバル コンフィギュレーション モード コマンド、**login delay** を介します。

DoS 攻撃が疑われる場合のログイン シャットダウン

設定された回数の接続試行が指定期間内で失敗しても、シスコのデバイスは「待機時間」のどのような追加接続も受け付けません。（事前定義されたアクセス コントロール リスト（ACL）によって許可されたホストは待機時間から除外されます）。

待機時間をトリガーする失敗した接続試行の回数は、新しいグローバル コンフィギュレーション モード コマンド **login block-for** で指定できます。待機時間から除外される定義済みの ACL は、新しいグローバル コンフィギュレーション モード コマンド **login quiet-mode access-class** で指定できます。

この機能は、デフォルトではディセーブルです。AutoSecure がイネーブルの場合はイネーブルになりません。

Cisco IOS Login Enhancement の設定方法

ログイン パラメータの設定

シスコのデバイスへの DoS 攻撃の疑いを検出し、辞書攻撃による影響の緩和に役立つログイン パラメータを設定するには、ここに示す手順を実行します。

すべてのログインパラメータは、デフォルトではディセーブルです。他のログイン コマンドを使用する前に **login block-for** コマンドを発行して、デフォルトのログイン機能をイネーブルにする必要があります。**login block-for** コマンドをイネーブルにすると、次のデフォルトが強制されます。

- デフォルトの 1 秒のログイン遅延
- Telnet または SSH を通じて行われるすべてのログイン試行は、待機時間中拒否されます。つまり、**login quiet-mode access-class** コマンドが発行されるまで、ACL はログイン時間から除外されません。

手順の概要

1. **enable**
2. **configureterminal**
3. **loginblock-for***seconds***attempts***tries***within***seconds*
4. **loginquiet-modeaccess-class** {*acl-name* | *acl-number*}
5. **logindelay***seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**loginblock-for***seconds***attempts***tries***within***seconds* 例： `Router(config)# login block-for 100 attempts 2 within 100`	Cisco IOS XE デバイスで DoS 検出の提供に役立つログイン パラメータを設定します。 （注） このコマンドは、その他のログイン コマンドを使用する前に発行する必要があります。
ステップ 4	**loginquiet-modeaccess-class** {*acl-name* | *acl-number*} 例： `Router(config)# login quiet-mode access-class myacl`	（任意）このコマンドはオプションですが、ルータが待機モードに切り替わるときにルータに適用される ACL を指定するように設定することを推奨します。ルータが待機モードになっている間は、すべてのログイン要求が拒否され、使用できる接続はコンソール経由の接続のみになります。 このコマンドを設定しない限り、デフォルトの ACL **sl_def_acl** はルータ上に作成されます。この ACL は実行コンフィギュレーションでは非表示です。デフォルトの ACL のパラメータを表示するには、**show access-list sl_def_acl** を使用します。

	コマンドまたはアクション	目的

		次に例を示します。
		`Router#show access-lists sl_def_acl`
		
		`Extended IP access list sl_def_acl`
		`10 deny tcp any any eq telnet`
		`20 deny tcp any any eq www`
		`30 deny tcp any any eq 22`
		`40 permit ip any any`

ステップ 5	**logindelay***seconds* 例： `Router(config)# login delay 10`	（任意）連続するログイン試行間の遅延を設定します。

次の作業

ルータでログイン パラメータを設定した後、設定を確認する必要がある場合があります。この作業を完了するには、「ログイン パラメータの確認, （7 ページ）」を参照してください。

ログイン パラメータの確認

ルータに適用されたログイン設定と現在のログイン ステータスを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **showloginfailures**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showloginfailures** 例： `Router# show login`	ログイン パラメータを表示します。 • **failures**：失敗したログイン試行に関連する情報のみを表示します。

例

showlogin コマンドからの次のサンプル出力は、ログイン パラメータが指定されていないことを確認します。

```
Router# show login
No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps
Router NOT enabled to watch for login Attacks
```

showlogin コマンドからの次のサンプル出力は、**loginblock-for** コマンドが発行されたことを確認します。この例で、コマンドは 100 秒以内に 16 回以上のログイン要求が失敗した場合、ログイン ホストを 100 秒ブロックするように設定されています。すでに 5 回のログイン要求が失敗しています。

```
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

showlogin コマンドからの次のサンプル出力は、ルータが待機モードになっていることを確認します。この例で、**loginblock-for** コマンドは、100 秒以内に 3 回以上のログイン要求が失敗した場合、ログイン ホストを 100 秒ブロックするように設定されています。

```
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for 100
 seconds.
```

```
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
Denying logins from all sources.
```

showloginfailures コマンドからの次のサンプル出力は、ルータ上で失敗したすべてのログイン試行を表示します。

```
Router# show login failures
Information about login failure's with the device
Username      Source IPAddr  lPort Count  TimeStamp
try1          10.1.1.1        23    1     21:52:49 UTC Sun Mar 9 2003
try2          10.1.1.2        23    1     21:52:52 UTC Sun Mar 9 2003
```

showloginfailures コマンドからの次のサンプル出力は、現在記録されている情報がないことを確認します。

```
Router# show login failures
*** No logged failed login attempts with the device.***
```

ログイン パラメータの設定例

ログイン パラメータの設定例

次に、100 秒以内に 15 回ログイン試行が失敗した場合に 100 秒の待機時間に入るようにルータを設定する例を示します。待機時間中、ACL “myacl” からのホスト以外、すべてのログイン要求が拒否されます。

```
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# login quiet-mode access-class myacl
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
AutoSecure の設定	AutoSecure の機能モジュール。
セキュリティ 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 IOS Security Command Reference*』
セキュアな管理/管理アクセス	「Role-Based CLI Access」機能モジュール

標準

標準	タイトル
なし。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco IOS Login Enhancements（Login Block）に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1*：*Cisco IOS Login Enhancements*（*Login Block*）に関する機能情報

機能名	リリース	機能の設定情報
Cisco IOS Login Enhancements	Cisco IOS XE Release 2.1	Cisco IOS Login Enhancements（Login Block）機能により、ユーザはサービス拒絶（DoS）攻撃と思われる攻撃が検出された場合、ログイン試行を自動的にブロックするオプションを設定して、ルータのセキュリティを強化できます。 この機能は、Cisco IOS XE リリース 2.1 では、Cisco ASR 1000 シリーズ サービス アグリゲーション ルータに導入されていました。 次のコマンドは、次の機能によって変更されました。**loginblock-for**、**logindelay**、**loginquiet-modeaccess-class**、**showlogin**。

第 3 章

パスワード、特権、およびログインによるセキュリティ設定

Cisco IOS ベースのネットワーキング デバイスには、デバイスで実行されているオペレーティング システムだけを使用して、基本的なセキュリティを実装できる機能が複数あります。たとえば、次のような機能があります。

- ネットワーキング デバイスのステータスを変更できるコマンドと、デバイスの監視に使用されるコマンドに対するアクセスを制御する CLI セッションの複数の認可レベル
- CLI セッションにパスワードを割り当てる機能
- ユーザがユーザ名を使用してネットワーキング デバイスにログインする操作を必須にする機能
- CLI セッション用に新しい認可レベルを作成するコマンドの特権レベルを変更する機能

このモジュールは、使用しているネットワーキング デバイスについて、基本レベルのセキュリティを実装する手順です。基本レベルのセキュリティを実装するために使用できる、最もシンプルなオプションを中心に説明します。セキュリティ オプションを設定せずにネットワークにネットワーキング デバイスをインストールした場合、またはこれからネットワーキング デバイスをインストールする予定で、基本的なセキュリティを実装する方法を理解する必要がある場合、このドキュメントが役立ちます。

- 機能情報の確認，14 ページ
- パスワード、特権、およびログインによるセキュリティ設定の制約事項，14 ページ
- パスワード、特権、およびログインによるセキュリティ設定について，14 ページ
- パスワード、特権、およびログインによるセキュリティの設定方法，29 ページ
- パスワード、特権、およびログインによるセキュリティ設定の設定例，53 ページ
- 次の作業，56 ページ
- その他の参考資料，56 ページ

- パスワード、特権、およびログインによるセキュリティ設定に関する機能情報，58 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

パスワード、特権、およびログインによるセキュリティ設定の制約事項

任意のローカルまたはリモートの認証、許可、アカウンティング（AAA）セキュリティ機能を使用するようにネットワーキング デバイスを設定しないでください。このドキュメントでは、ネットワーク デバイスでローカルで設定できる非 AAA セキュリティ機能のみを説明します。

ネットワーク デバイスでローカルで実行できる AAA セキュリティ機能の設定方法、または TACACS+ や RADIUS サーバを使用したリモート AAA セキュリティの設定方法については、『*Securing User Services Configuration Guide Library*』を参照してください。

パスワード、特権、およびログインによるセキュリティ設定について

セキュリティ スキームを作成する利点

ネットワークの優れたセキュリティ スキームの基礎は、ネットワーキング デバイスのユーザ インターフェイスを不正アクセスから保護することです。ネットワーキングデバイス上のユーザインターフェイスに対するアクセスを保護することで、ネットワークの安定を妨げ、ネットワークセキュリティを危険にさらすような設定の変更を不正ユーザが行うことを回避できます。

このドキュメントで説明する Cisco IOS XE の機能をさまざまな方法で組み合わせて、実際の各ネットワークデバイスに固有のセキュリティ スキームを作成できます。次に、いくつかの設定例を示します。

- コマンドを実行可能なレベルを非管理特権レベルまで下げることで、非管理ユーザに対して、ネットワーキングデバイスで使用できる管理コマンドの一部の実行を許可できます。この処理は、次のシナリオに役立ちます。
  - ISP で、窓口のテクニカルサポートスタッフが、新規顧客の新規インターフェイスをイネーブルにするタスク、または接続がトラフィックのパスを停止した顧客の接続をリセットするタスクなどを実行できるようにする場合。その実行方法の例については、「例：ユーザがインターフェイスをシャットダウンおよびイネーブル化することを可能にするデバイスの設定，（55 ページ）」を参照してください。
  - 窓口のテクニカル サポート スタッフが、ターミナル サーバから不正に接続解除されたコンソール ポート セッションをクリアする機能を実行できるようにする場合。その実行方法の例については、「例：ユーザがリモート セッションをクリア可能にするデバイスの設定，（53 ページ）」を参照してください。
  - 窓口のテクニカル サポート スタッフが、ネットワーク デバイスの設定を変更ではなく表示し、ネットワークの問題を解決する機能を実行できるようにする場合。その実行方法の例については、「例：ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定，（54 ページ）」を参照してください。

Cisco IOS XE CLI モード

シスコ デバイスの設定を支援するために、Cisco IOS XE コマンドライン インターフェイスは、さまざまなコマンドモードに分かれています。各コマンドモードには、ルータとネットワークの動作を設定、メンテナンス、モニタリングするための独自のコマンドセットがあります。常に使用可能なコマンドは、モードによって異なります。システムプロンプト（デバイスプロンプト）で疑問符（**?**）を入力すると、各コマンド モードで使用できるコマンドのリストを取得できます。

特定のコマンドを使用すると、コマンド モードを変更できます。ユーザがモードにアクセスする標準の順序は、ユーザ EXEC モード、特権 EXEC モード、グローバル コンフィギュレーション モード、特定のコンフィギュレーションモード、コンフィギュレーションサブモード、およびコンフィギュレーション サブモードです。

（注） Cisco IOS XE ソフトウェア ベースのネットワーク デバイスのデフォルト設定で使用できるのは、ユーザ EXEC モード（ローカルおよびリモート CLI セッションの場合）と特権 EXEC モードへのアクセスを保護するパスワードを設定する操作だけです。ここでは、ユーザ名、パスワード、および **privilege** コマンドを組み合わせて他のモードへのアクセスおよびコマンドを保護することで、追加レベルのセキュリティを提供する方法について説明します。

ほとんどの EXEC モード コマンドは、現在の設定ステータスを表示する **show** コマンドまたは **more** コマンドや、カウンタやインターフェイスをクリアする **clear** コマンドのように、1 回限りのコマンドです。EXEC モードのコマンドは、ルータをリブートすると保持されません。

特権 EXEC モードから、グローバル コンフィギュレーション モードに入ることができます。このモードでは、一般的なシステム特性を設定するためのコマンドを実行できます。また、グローバ

ル コンフィギュレーション モードを使用して特定のコンフィギュレーション モードを開始することもできます。グローバルコンフィギュレーションモードを含むコンフィギュレーションモードでは、実行コンフィギュレーションを変更できます。後で設定を保存すると、ルータをリブートしてもこれらのコマンドが保持されます。

グローバルコンフィギュレーションモードから、さまざまなプロトコル固有または機能固有のコンフィギュレーション モードを開始できます。CLI 階層では、グローバル コンフィギュレーション モードからしかこれらのコンフィギュレーション モードを開始できません。たとえば、インターフェイス コンフィギュレーション モードは、共通して使用されるコンフィギュレーション モードです。

コンフィギュレーションモードから、コンフィギュレーションサブモードを開始できます。コンフィギュレーションサブモードは、特定のコンフィギュレーションモードの範囲内で特定の機能を設定するために使用します。たとえば、この章では、インターフェイス コンフィギュレーション モードのサブモードであるサブインターフェイス コンフィギュレーション モードについて説明します。

ROM モニタ モードは、ルータが適切にブートできない場合に使用される別のモードです。システム（ルータ、スイッチ、またはアクセス サーバ）のブート時に適切なシステムイメージが見つからない場合、システムは ROM モニタ モードを開始します。ROM モニタ（ROMMON）モードには、起動時にブート シーケンスに割り込むことでもアクセスできます。ROMMON には使用できるセキュリティ機能がないため、このドキュメントでは説明していません。

ユーザ EXEC モード

ルータでセッションを開始するときは、通常、EXEC モードの 2 つあるアクセス レベルの 1 つであるユーザ *EXEC* モードから始めます。セキュリティのために、ユーザ EXEC モードで使用できる EXEC コマンドは制限されています。このアクセス レベルは、ルータのステータスを確認するなど、ルータの設定を変更しない作業のために予約されています。

デバイスの設定で、ユーザのログインが必須の場合、そのログイン プロセスはユーザ名とパスワードが必須になります。接続が拒否されるまでにパスワードを 3 回入力できます。

ユーザ EXEC モードは、デフォルトで特権レベル 1 に設定されています。特権 EXEC モードは、デフォルトで特権レベル 15 に設定されています。詳細については、「特権 EXEC モード，（18 ページ）」を参照してください。ユーザ EXEC モードでネットワーキング デバイスにログインしている場合、システムは特権レベル 1 で実行されます。デフォルトで、特権レベル 1 の EXEC コマンドは、特権レベル 15 で使用できるコマンドのサブセットです。特権 EXEC モードでネットワーキングデバイスにログインしている場合、システムは特権レベル 15 で実行されます。**privilege** コマンドを使用すると、1 ～ 15 の任意の特権レベルにコマンドを移動できます。特権レベルおよび **privilege** コマンドの詳細については、「Cisco IOS XE の特権レベル，（27 ページ）」を参照してください。

一般に、ユーザ EXEC コマンドでは、リモート デバイスへの接続、端末回線の一時的な設定変更、基本的なテストの実行、システム情報の表示を行うことができます。

使用可能なユーザ EXEC コマンドの一覧を表示するには、次のコマンドを使用します。

コマンド	目的
`Device(config)#` **?**	ユーザ EXEC モード コマンド リストを表示します

ユーザ EXEC モード プロンプトは、デバイスのホスト名と、それに続く山カッコ（>）で構成されます。次に例を示します。

```
Device>
```

setup EXEC コマンドで初期設定時に変更していなければ、通常はデフォルトのホスト名は Router です。また、ホスト名の変更には、**hostname** グローバル コンフィギュレーション コマンドを使用します。

（注） Cisco IOS XE のドキュメントの例では、「デバイス」のデフォルト名を使用することを想定しています。さまざまなデバイス（アクセス サーバ）が異なるデフォルト名を使用できます。デバイス（ルータ、アクセス サーバ、またはスイッチ）に、**hostname** コマンドで名前が設定されている場合、デフォルトの名前の代わりにその名前がプロンプトに表示されます。

ユーザ EXEC モードで使用できるコマンドの一覧を表示するには、次の例に示すように疑問符（**?**）を入力します。

```
Device> ?

Exec commands:
 <1-99>           Session number to resume
 connect          Open a terminal connection
 disconnect       Disconnect an existing telnet session
 enable           Turn on privileged commands
 exit             Exit from Exec mode
 help             Description of the interactive help system
 lat              Open a lat connection
 lock             Lock the terminal
 login            Log in as a particular user
 logout           Exit from Exec mode and log out
 menu             Start a menu-based user interface
 mbranch          Trace multicast route for branch of tree
 mrbranch         Trace reverse multicast route to branch of tree
 mtrace           Trace multicast route to group
 name-connection  Name an existing telnet connection
 pad              Open a X.29 PAD connection
 ping             Send echo messages
 resume           Resume an active telnet connection
 show             Show running system information
 systat           Display information about terminal lines
 telnet           Open a telnet connection
 terminal         Set terminal line parameters
 tn3270           Open a tn3270 connection
 trace            Trace route to destination
 where            List active telnet connections
 x3               Set X.3 parameters on PAD
```

コマンドの一覧は、使用しているソフトウェア機能セットおよびプラットフォームによって異なります。

（注） コマンドは、大文字、小文字、または大文字と小文字を混在させて入力できます。大文字と小文字の区別があるのはパスワードだけです。ただし、Cisco IOS XE のマニュアルの表記法では、コマンドは常に小文字になっています。

特権 EXEC モード

すべてのコマンドにアクセスするには、EXEC モードの第 2 レベルのアクセスである特権 *EXEC* モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードが必要です。特権 EXEC モードでは、任意の EXEC コマンドを入力できます。これは、特権 EXEC モードが、ユーザ EXEC モード コマンドのスーパーセットであるためです。

多くの特権 EXEC モード コマンドは操作パラメータを設定するため、不正使用を防ぐために、特権 EXEC レベル アクセスをパスワードで保護する必要があります。特権 EXEC コマンド セットには、ユーザ EXEC モードに含まれているこれらのコマンドが含まれます。また、特権 EXEC モードでは、**configure** コマンドを使用することで各種コンフィギュレーション モードにアクセスでき、**debug** などの高度なテスト コマンドも含まれています。

特権 EXEC モードは、デフォルトで特権レベル 15 に設定されています。ユーザ EXEC モードは、デフォルトで特権レベル 1 に設定されています。詳細については、「ユーザ EXEC モード，（16 ページ）」を参照してください。特権 EXEC モードでネットワーキング デバイスにログインしている場合、システムは特権レベル 15 で実行されます。ユーザ EXEC モードでネットワーキング デバイスにログインしている場合、システムは特権レベル 1 で実行されます。デフォルトで、特権レベル 15 の EXEC コマンドは、特権レベル 1 で使用できるコマンドのスーパーセットです。**privilege** コマンドを使用すると、1 ～ 15 の任意の特権レベルにコマンドを移動できます。特権レベルおよび **privilege** コマンドの詳細については、「Cisco IOS XE の特権レベル，（27 ページ）」を参照してください。

特権 EXEC モード プロンプトは、デバイスのホスト名と、それに続くポンド記号（#）で構成されます。次に例を示します。

```
Device#
```

特権 EXEC モードにアクセスするには、次のコマンドを使用します。

コマンド	目的

`Device>` **enable**
`Password`
`Device#` **exit**
`Device>`
	特権 EXEC モードをイネーブルにします。
	• 特権 EXEC モードのパスワードを選択すると、enable コマンドの発行後にパスワードの入力が求められます。
	• 特権 EXEC モードを終了するには、exit コマンドを使用します。

（注） 特権 EXEC モードは、モードの開始に、**enable** コマンドを使用するため、「イネーブル モード」とも呼ばれます。

システムでパスワードが設定されている場合、特権 EXEC モードへのアクセスが許可される前にパスワードを入力するよう求められます。パスワードは画面には表示されません。また、大文字と小文字が区別されます。イネーブル パスワードが設定されていない場合、特権 EXEC モードには、ローカル CLI セッション（コンソール ポートに接続された端末）からしかアクセスできません。

Telnet 接続など、リモート接続上のルータで特権 EXEC モードへのアクセスを試行しても、特権 EXEC モードのパスワードを設定していない場合は、**%Nopasswordset** エラー メッセージが表示されます。リモート接続の詳細については、「リモート CLI セッション，（23 ページ）」を参照してください。システム管理者は、**enablesecret** または **enablepassword** グローバル コンフィギュレーション コマンドを使用して、特権 EXEC モードへのアクセスを制限するパスワードを設定します。特権 EXEC モードのパスワード設定の詳細については、「特権 EXEC モードへのアクセスの保護，（34 ページ）」を参照してください。

ユーザ EXEC モードに戻るには、次のコマンドを使用します。

コマンド	目的
`Device#` **disable**	特権 EXEC モードを終了し、ユーザ EXEC モードに戻ります。

次に、特権 EXEC モードにアクセスするプロセスの例を示します。

```
Device> enable
Password:<letmein>
Device#
```

入力してもパスワードが表示されませんが、ここでは説明のために表示しています。特権 EXEC モードで使用できるコマンドの一覧を表示するには、プロンプトで **?** コマンドを発行します。次の項で説明するように、特権 EXEC モードからグローバル コンフィギュレーション モードにアクセスできます。

（注） 特権 EXEC コマンド セットには、ユーザ EXEC モードで使用できるすべてのコマンドが含まれているため、一部のコマンドはどちらのモードでも実行できます。Cisco IOS XE のドキュメントでは、ユーザ EXEC モードまたは特権 EXEC モードで入力できるコマンドは、EXEC モード コマンドと呼ばれます。ユーザまたは特権とドキュメントに特記されていない場合、どちらのモードでもそのコマンドを入力できることを示します。

グローバル コンフィギュレーション モード

「グローバル」という言葉は、システム全体に影響する特性や機能を示すために使用されています。グローバル コンフィギュレーション モードは、システムをグローバルに設定したり、インターフェイスやプロトコルなどの特定の要素を設定したりする目的で、特定のコンフィギュレーション モードを開始するために使用します。**configureterminal** 特権 EXEC コマンドを使用して、グローバル コンフィギュレーション モードに入ります。

グローバル コンフィギュレーション モードにアクセスするには、特権 EXEC モードで次のコマンドを入力します。

コマンド	目的
Device# **configure terminal**	特権 EXEC モードで、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。

次に、特権 EXEC モードからグローバル コンフィギュレーション モードを開始するプロセスの例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#
```

システム プロンプトが変わり、グローバル コンフィギュレーション モードに入ったことが示されることに注意してください。グローバル コンフィギュレーション モードのプロンプトは、デバイスのホスト名と、それに続く（config）およびポンド記号（#）で構成されます。特権 EXEC モードで使用できるコマンドの一覧を表示するには、プロンプトで **?** コマンドを発行します。

グローバル コンフィギュレーション モードでコマンドを入力すると、すぐに実行コンフィギュレーション ファイルが更新されます。つまり、設定に対する変更は、有効なコマンドの後で Enter キーまたは Return キーを押すたびに有効になります。ただし、これらの変更は、**copyrunning-configstartup-config** EXEC モード コマンドを発行するまで、スタートアップ コンフィギュレーション ファイルに保存されません。この動作は、このマニュアルの後の項で詳しく説明します。

上記の例のように、コントロール（Ctrl）キーと「z」キーを同時に押すと、システム ダイアログでコンフィギュレーション セッションを終了するプロンプトが表示されます。これらのキー操作で、**^Z** が画面に出力されます。実際にコンフィギュレーション セッションを終了するには、Ctrl+Z キーの組み合わせ、**end** コマンド、または Ctrl+C キーの組み合わせを使用できます。現在のコンフィギュレーション セッションを終了することをシステムに示すための方法としては、**end** コマンドが推奨されます。

注意 有効なコマンドを入力してから、コマンド ラインの最後で Ctrl+Z キーを使用すると、そのコマンドが実行コンフィギュレーション ファイルに追加されます。つまり、Ctrl+Z キーを使用することは、終了前に Enter（復帰）キーを押すことと同じです。このような理由から、**end** コマンドを使用してコンフィギュレーション セッションを終了するほうが安全です。また、改行信号を送信せずにコンフィギュレーション セッションを終了するには、Ctrl+C キーの組み合わせを使用できます。

また、**exit** コマンドを使用して、グローバル コンフィギュレーション モードから EXEC モードに戻ることもできますが、使用できるのはグローバル コンフィギュレーション モードだけです。Ctrl+Z キーを押すか **end** コマンドを入力することにより、どのコンフィギュレーション モードまたはコンフィギュレーション サブモードにいるかにかかわらず、常に EXEC モードに戻ることができます。

グローバル コンフィギュレーション コマンド モードを終了して特権 EXEC モードに戻るには、次のいずれかのコマンドを使用します。

コマンド	目的
`Device(config)#` **end** または `Device(config)#` **^Z**	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
`Device(config)#` **exit**	現在のコマンドモードを終了して、前のモードに戻ります。たとえば、グローバル コンフィギュレーションモードから特権EXECモードに戻ります。

グローバルコンフィギュレーションモードから、いくつかのプロトコル固有、プラットフォーム固有、機能固有のコンフィギュレーション モードを開始できます。

次のセクションで説明されているインターフェイスコンフィギュレーションモードは、グローバル コンフィギュレーション モードから入ることができるコンフィギュレーション モードの例です。

インターフェイス コンフィギュレーション モード

グローバル コンフィギュレーション モードから開始する特定のコンフィギュレーション モードの一例が、インターフェイス コンフィギュレーション モードです。

多くの機能は、インターフェイスごとにイネーブルになります。インターフェイス コンフィギュレーション コマンドは、イーサネット、FDDI、シリアル ポートなど、インターフェイスの動作を変更します。インターフェイス コンフィギュレーション コマンドは常に、インターフェイス タイプを定義する **interface** グローバル コンフィギュレーション コマンドの後に指定します。

帯域幅やクロック レートなど、一般的なインターフェイスパラメータに影響があるインターフェイス コンフィギュレーション コマンドの詳細については、Release 12.2 の『*Cisco IOS Interface Configuration Guide*』を参照してください。プロトコル固有のコマンドについては、該当する Cisco IOS XE ソフトウェア コマンド リファレンスを参照してください。

インターフェイスコンフィギュレーションコマンドにアクセスし、その一覧を表示するには、次のコマンドを使用します。

コマンド	目的
`Device(config)#` **interface** *type number*	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。

次に、シリアル インターフェイス 0 についてユーザがインターフェイス コンフィギュレーション モードを開始する例を示します。新しいプロンプト、*hostname*（config-if）# は、インターフェイス コンフィギュレーション モードを示しています。

```
Device(config)# interface serial 0
Device(config-if)#
```

インターフェイス コンフィギュレーション モードを終了しグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。

コンフィギュレーション サブモードは、他のコンフィギュレーション モード（グローバル コンフィギュレーションモード以外）から開始されるコンフィギュレーションモードです。コンフィギュレーションサブモードは、コンフィギュレーションモード内の特定の要素を設定するためにあります。コンフィギュレーション サブモードの 1 つの例は、次の項で説明するサブインターフェイス コンフィギュレーション モードです。

サブインターフェイス コンフィギュレーション モード

インターフェイスコンフィギュレーションモードから、サブインターフェイスコンフィギュレーションモードに入ることができます。サブインターフェイスコンフィギュレーションモードは、インターフェイス コンフィギュレーション モードのサブモードの 1 つです。サブインターフェイス コンフィギュレーション モードでは、1 つの物理インターフェイスに複数の仮想インターフェイス（別名サブインターフェイス）を設定できます。サブインターフェイスは、さまざまなプロトコルにとって個別の物理インターフェイスのように見えます。

サブインターフェイスの設定方法の詳細については、Cisco IOS XE ソフトウェア マニュアル セットの特定のプロトコルの該当するドキュメンテーション モジュールを参照してください。

サブインターフェイス コンフィギュレーション モードにアクセスするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Device(config-if)#` **interface** *type number*	設定する仮想インターフェイスを指定し、サブインターフェイスコンフィギュレーションモードを開始します。

次の例では、シリアル ライン 2 のサブインターフェイスで、フレーム リレー カプセル化を設定します。シリアル インターフェイス 2 のサブインターフェイス 1 であることを示すため、サブインターフェイスは「2.1」として識別されます。新しいプロンプトの *hostname*（config-subif）#は、サブインターフェイス コンフィギュレーション モードを示します。サブインターフェイスは、1 つ以上のフレーム リレー PVC をサポートするように設定できます。

```
Device(config)# interface serial 2
Device(config-if)# encapsulation frame-relay
Device(config-if)# interface serial 2.1
Device(config-subif)#
```

サブインターフェイス コンフィギュレーション モードを終了しインターフェイス コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。コンフィギュレーション セッションを終了し特権 EXEC モードに戻るには、Ctrl+Z キーを押すか、**end** コマンドを入力します。

Cisco IOS XE CLI セッション

ローカル CLI セッション

ローカル CLI セッションでは、ネットワーク デバイスのコンソール ポートへの直接アクセスが要求されます。ローカル CLI セッションは、ユーザ EXEC モードで開始されます。使用しているネットワーク デバイスでサポートされるさまざまなモードの詳細については、「Cisco IOS XE CLI モード，（15 ページ）」を参照してください。ネットワーキング デバイスの設定とおよび管理に必要なすべてのタスクは、ローカル CLI セッションを使用して実行できます。ローカル CLI セッションを確立する最も一般的な方式は、PC 上のシリアル ポートを、ネットワーキング デバイスのコンソール ポートに接続し、PC で端末エミュレーション アプリケーションを起動する方法です。必要とされるケーブルとコネクタの種類および PC 上の端末エミュレーション アプリケーションの設定は、設定しているネットワーク デバイスの種類によって異なります。ローカル CLI セッションでネットワーキング デバイスを設定する方法の詳細については、そのデバイスのマニュアルを参照してください。

リモート CLI セッション

リモート CLI セッションは、PC などのホストとネットワーク上のルータなどのネットワーク デバイス間で、Telnet やセキュア シェル（SSH）などのリモート端末アクセス アプリケーションを

使用して作成されます。ローカル CLI セッションは、ユーザ EXEC モードで開始されます。使用しているネットワーク デバイスでサポートされるさまざまなモードの詳細については、「Cisco IOS XE CLI モード, （15 ページ）」を参照してください。ネットワーク デバイスの設定とおよび管理に必要なほとんどのタスクは、リモート CLI セッションを使用して実行できます。例外は、ROM モニタ モードのときのネットワーク デバイスとの通信や、（コンソール ポートで新しい OS イメージをアップロードすることによる、破壊されたオペレーティング システム（OS）の復元など）、コンソール ポートと直接的に通信するタスクです。

このドキュメントでは、リモート Telnet セッションのセキュリティを設定する方法について説明します。Telnet は、ネットワーキング デバイスでリモート CLI セッションにアクセスする際に最も一般的な方式です。

（注） ただし、SSH の方が Telnet よりも安全な方式です。SSH には、PC などのローカル管理デバイスと、管理しているネットワーキング デバイスとの間のセッション トラフィックを暗号化する機能があります。SSH を使用してセッション トラフィックを暗号化すると、ハッカーがトラフィックを傍受しても、トラフィックをデコードできなくなります。SSH を使用する詳細については、「Secure Shell Version 2 Support」フィーチャ モジュールを参照してください。

端末回線はローカルおよびリモート CLI セッションに使用される

シスコ ネットワーク デバイスでは、ローカルおよびリモート CLI セッションを管理するソフトウェア コンポーネントを参照するため語線を使用します。**lineconsole0** グローバル コンフィギュレーション コマンドを使用してライン コンフィギュレーション モードを開始し、パスワードなど、コンソール ポートのオプションを設定します。

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# password password-string
```

リモート CLI セッションでは、仮想テレタイプ（VTY）の行である回線を使用しています。**linevty***line-number* [*ending-line-number*] グローバル コンフィギュレーション コマンドを使用してライン コンフィギュレーション モードに入り、パスワードなど、リモート CLI セッションのオプションを設定します。

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config-line)# password password-string
```

Cisco IOS XE EXEC モードへのアクセスの保護

Cisco IOS XE では、次へのアクセスを保護するパスワードを設定できます。

ユーザ EXEC モードへのアクセスの保護

ネットワーク デバイスの安全な環境の構築に向けた第一歩は、ローカルおよびリモート CLI セッションのパスワードを設定することで、ユーザ EXEC モードへのアクセスを保護することです。

ローカル CLI セッションでユーザ EXEC モードに対するアクセスを保護するには、コンソール ポートでパスワードを設定します。ローカル CLI セッションのパスワードの設定と確認, （32 ページ）を参照してください。

リモート CLI セッションでユーザ EXEC モードに対するアクセスを保護するには、仮想端末回線（VTY）でパスワードを設定します。リモート CLI セッションのパスワード設定方法の手順については、「リモート CLI セッションのパスワードの設定と確認, （29 ページ）」を参照してください。

特権 EXEC モードへのアクセスの保護

ネットワーキング デバイスのセキュア環境を作成するための第 2 段階は、特権 EXEC モードに対するアクセスをパスワードで保護することです。特権 EXEC モードに対するアクセスを保護する方式は、ローカルおよびリモートの CLI セッションと同じです。

特権 EXEC モードに対するアクセスを保護するには、そのモード用のパスワードを設定します。特権 EXEC モードを開始するコマンドが **enable** なので、このパスワードもイネーブル パスワードと呼ばれることがあります。

コマンド	目的

enable
`Device>` **`enable`**
`Password`
 	
`Device#`
	特権 EXEC モードをイネーブルにします。
	• パスワードを入力します（要求された場合）。パスワードはターミナル ウィンドウに表示されません。
	• プロンプト文字列の末尾の「>」は、特権 EXEC モードにいることを示す「#」に変更されました。

Cisco IOS XE のパスワード暗号化レベル

ネットワークデバイスで設定するパスワードの中には、プレーンテキストで設定に保存されるものもあります。これは、ディスクにコンフィギュレーション ファイルのコピーを保存すると、コンフィギュレーション ファイルを読み取ることで、ディスクへのアクセス権を持つ誰もが、パスワードがわかることを意味します。次の種類のパスワードは、デフォルトでプレーン テキストで設定に保存されます。

- ローカル CLI セッションのコンソール パスワード

- リモート CLI セッションの仮想端末回線のパスワード
- パスワードを設定するため、デフォルトの方法を使用したユーザ名のパスワード
- **enable password** *password* コマンドで設定されるときの特権 EXEC モードのパスワード
- RIPv2 と EIGRP で使用されている認証キー チェーン パスワード
- BGP ネイバーを認証するための BGP パスワード
- OSPF ネイバーの認証に使用する OSPF 認証キー
- ISIS ネイバーを認証するための ISIS パスワード

ルータの設定ファイルからのこの引用文は、クリア テキストとして保存されたパスワードと認証キーの例を示しています。

```
!
enable password O9Jb6D
!
username username1 password 0 kV9sIj3
!
key chain trees
 key 1
  key-string willow
!
interface Ethernet1/0.1
 ip address 172.16.6.1 255.255.255.0
 ip router isis
 ip rip authentication key-chain trees
 ip authentication key-chain eigrp 1 trees
 ip ospf authentication-key j7876
 no snmp trap link-status
 isis password u7865k
!
line vty 0 4
 password V9jA5M
!
```

service password-encryption コマンドを使用することで、これらのクリア テキストのパスワードをコンフィギュレーション ファイルで暗号化できます。パスワードを暗号化するのに **service password-encryption** コマンドによって使用された暗号化アルゴリズムは、公で使用可能なツールを使用して暗号化されるテキスト ストリングを作成するため、これは最小レベルのセキュリティにすぎないと見なされる必要があります。また、**service password-encryption** コマンドを使用後、コンフィギュレーション ファイルのどのような電子または文書でのコピーに対するアクセスも保護する必要があります。

パスワードがリモート デバイスに送信されるとき、**service password-encryption** コマンドではパスワードを暗号化しません。ネットワークに対するアクセス権があるネットワーク トラフィック アナライザを使用するユーザは、デバイス間でパケットを送信するときに、パケットからこのようなパスワードをキャプチャできます。コンフィギュレーション ファイルでのクリア テキスト パスワードの暗号化の詳細については、「クリア テキスト パスワードのパスワード暗号化の設定, （36 ページ）」を参照してください。

クリア テキスト パスワードを使用する Cisco IOS XE 機能の多くは、より安全な MD5 アルゴリズムを使用するように設定することもできます。MD5 アルゴリズムによって、暗号化がはるかに難しいコンフィギュレーション ファイル内でテキスト ストリングが作成されます。MD5 アルゴリズムは、リモートデバイスにパスワードを送信しません。これによって、トラフィック アナライ

ザのユーザが、内部ネットワークのトラフィックをキャプチャしてパスワードを検出することを防ぎます。

ネットワーキングデバイスのコンフィギュレーションファイルにパスワード文字列とともに保存されている数字によって、使用されているパスワード暗号化の種類を判断できます。下記のコンフィギュレーションの引用文での数字 5 は、イネーブル シークレット パスワードは MD5 アルゴリズムを使用して暗号化されていること示しています。

enable secret 5 1fGCS$rkYbR6.Z8xo4qCl3vghWQ0

下記の引用文での数字 7 は、**service password-encryption** コマンドによって使用された、より安全でないアルゴリズムを使用してイネーブル パスワードが暗号化されたことを示しています。

!

enable password 7 00081204

Cisco IOS XE CLI セッションのユーザ名

これらのパスワードを設定して、ユーザ EXEC モードおよび特権 EXEC モードへのアクセスを保護した後に、個々のユーザにネットワーク デバイスの CLI セッションへのアクセスを制限するためのユーザ名を設定することで、ネットワークデバイスのセキュリティ レベルをさらに強化できます。

ネットワーキング デバイスの管理に使用するユーザ名は、次のような追加オプションを使用して変更できます。

『*Cisco IOS Security Command Reference*』を参照してください。**username** コマンドの設定方法の詳細については、（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS XE の特権レベル

Cisco IOS XE ベースのネットワーク デバイスのデフォルト設定では、ユーザ EXEC モードに特権レベル 1 を、特権 EXEC に特権レベル 15 を使用します。特権レベル 1 のユーザ EXEC モードで実行できるコマンドは、特権レベル 15 の特権 EXEC モードで実行できるコマンドのサブセットです。

privilege コマンドは、1 つの特権レベルから別の特権レベルへコマンドを移動するのに使用されます。たとえば、一部の ISP では、窓口のテクニカル サポート スタッフに対して、新しい顧客の接続をアクティブ化するインターフェイスをイネーブルまたはディセーブルにする機能、およびトラフィックの送信を終了した接続を再起動する機能を許可しています。このオプションの設定方法の例については、「例：ユーザがインターフェイスをシャットダウンおよびイネーブル化することを可能にするデバイスの設定，（55 ページ）」を参照してください。

privilege コマンドは、ユーザ名に特権レベルを割り当てるために使用できるため、ユーザがこのユーザ名でログインすると、セッションは、**privilege** コマンドで指定された特権レベルで実行されます。たとえば、テクニカル サポート スタッフに対して、ネットワーク デバイス設定の表示を許可することで、設定を変更することなくネットワークの問題を解決できるようにする場合、

ユーザ名を作成し、特権レベル 15 を使用してユーザ名を設定し、**show running-config** コマンドを自動的に実行するように設定できます。ユーザがそのユーザ名でログインすると、実行コンフィギュレーションが自動的に表示されます。ユーザがコンフィギュレーションの最後の行を表示すると、ユーザのセッションは自動的にログアウトされます。このオプションの設定方法の例については、「例：ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定, （54 ページ）」を参照してください。

このようなコマンドの特権は、TACACS+ および RADIUS による AAA を使用するときにも実装できます。たとえば、TACACS+ には、ユーザ別またはグループ別にルータ コマンドの認可を制御する方法が 2 つあります。1 つ目の方法では、コマンドに特権レベルを割り当て、指定した特権レベルでユーザが認可されているかどうかについて、TACACS+ サーバを使用するルータで確認します。2つ目の方法では、ユーザ別またはグループ別に、明示的に許可するコマンドを TACACS+ サーバに指定します。TACACS+ および RADIUS による AAA の実装の詳細については、『How to Assign Privilege Levels with TACACS+ and RADIUS』のテクニカル ノートを参照してください。

Cisco IOS XE のパスワード設定

Cisco IOS XE ソフトウェアでは、パスワードが意図したとおりに正確に入力されたことを確認するため、設定するパスワードの再入力を求めるプロンプトを採用していません。新しいパスワードおよび既存のパスワードへの変更は、パスワードコンフィギュレーションコマンド文字列の末尾に、Enter キーを入力すると、ただちに有効になります。新しいパスワードを入力し、ネットワーク デバイスのスタートアップ コンフィギュレーション ファイルに設定を保存し、特権 EXEC モードを出たときに間違えた場合、間違えたことを認識する前に、デバイスを管理できなくなっていることがわかる場合があります。

発生する可能性のある一般的な状況は次のとおりです。

- コンソール ポートでローカル CLI セッションのパスワード設定時に間違えます。
  - リモート CLI セッションでネットワーク デバイスに対するアクセスを適切に設定した場合、コンソール ポートで Telnet をして、パスワードを再設定できます。
- リモート Telnet または SSH セッションのパスワード設定時に間違えます。
  - ローカル CLI セッションでネットワーキング デバイスに対するアクセスを適切に設定した場合、端末に接続して、リモート CLI セッションのパスワードをリセットできます。
- 特権 EXEC モードでパスワード（イネーブル パスワードまたはイネーブル シークレット パスワード）を設定するときに誤入力しました。
  - 失われたパスワードの復元手順を実行する必要があります。
- ユーザ名パスワード設定するときに誤入力し、ネットワーキングデバイスからそのユーザ名を使用してログインするように求められました。
  - 別のアカウント名へのアクセス権を持っていない場合、失われたパスワード復元手順を実行する必要があります。

忘失パスワードの復元手順を実行する必要がないようにするには、ネットワーキング デバイスに対して 2 つの CLI セッションを開き、特権 EXEC モードでその一方を開いたままで、他のセッションを使用してパスワードをリセットします。2 つの CLI セッションまたは 2 種類のデバイスを実行するときに、同じデバイス（PC または端末）を使用できます。この手順には、ローカルの CLI セッションとリモート CLI セッションを使用するか、2 つのリモート CLI セッションを使用できます。パスワードの設定に使用する CLI セッションを、パスワードが適切に変更されたことを確認するために利用することもできます。最初の設定で誤入力した場合、特権 EXEC モードで開いておいたもう一方の CLI セッションはパスワードを変更するときにも利用できます。

実行コンフィギュレーションで行ったパスワードの変更は、そのパスワードが適切に変更されたことを確認できるまで、スタートアップ コンフィギュレーションに保存しないでください。パスワードの設定時に誤入力したことに気づき、上記のような第 2 の CLI セッションの手法を使用して問題を解決できなかった場合、スタートアップ コンフィギュレーションに保存されている以前のパスワードに戻すように、ネットワーキング デバイスの電源を再投入します。

パスワード、特権、およびログインによるセキュリティの設定方法

ユーザ EXEC モードへのアクセスの保護

リモート CLI セッションのパスワードの設定と確認

このタスクを実行すると、リモート CLI セッションのパスワードが割り当てられます。このタスクを完了すると、この次にリモート CLI セッションを起動するときに、ネットワーク デバイスからパスワードの入力が求められます。

Cisco IOS XE ベースのネットワーク デバイスでは、リモート CLI セッション用に設定されたパスワードが必要になります。リモート CLI セッション用に設定されたパスワードがないデバイスでリモート CLI セッションを開始しようとすると、パスワードが必要で、設定されていないことを示すメッセージが表示されます。リモート CLI セッションは、リモート ホストによって終了されます。

はじめる前に

以前にリモート CLI セッションのパスワードを設定していない場合、コンソール ポートに接続している端末、または端末エミュレーション アプリケーションを実行する PC を使用して、ローカル CLI セッションでこのタスクを実行する必要があります。

ネットワーキングデバイス上のコンソールポートに使用される設定によって、端末、または端末エミュレーション アプリケーションを設定する必要があります。ほとんどのシスコのネットワーク デバイスのコンソール ポートには、次の設定が必要です。9600 ボー、8 データ ビット、1 ストップ ビット、パリティなし、およびフロー制御は "none" に設定します。これらの設定が端末で機能しない場合は、ネットワーク デバイスのマニュアルを参照してください。

このタスクの確認手順（手順 6）を実行するには、ネットワーキング デバイスに、動作状態のインターフェイスが必要です。インターフェイスは有効な IP アドレスを持っている必要があります。

（注） 以前にリモート CLI セッションのパスワードを設定していない場合、コンソール ポートに接続している端末を使用して、ローカル CLI セッションでこのタスクを実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **linevty***line-number* [*ending-line-number*]
4. **password***password*
5. **end**
6. **telnet***ip-address*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**linevty***line-number* [*ending-line-number*] 例： `Device(config)# line vty 0 4`	ライン コンフィギュレーション モードを開始します。
ステップ 4	**password***password* 例： `Device(config-line)# password H7x3U8`	引数 *password* は、ライン パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。 • 最初の文字を数値にはできません。

	コマンドまたはアクション	目的
		• ストリングには、80 文字以下の任意の英数字（スペースを含む）を指定できます。数字-スペース-任意の文字の形式ではパスワードを指定できません。 • パスワードは大文字と小文字が区別されます。
ステップ 5	**end** 例： `Device(config-line)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**telnet***ip-address* 例： `Device# telnet 172.16.1.1`	動作状態（インターフェイスがアップ、ライン プロトコルがアップ）のネットワーキング デバイスで、インターフェイスの IP アドレスを使用して、現在の CLI セッションからネットワーキング デバイスとのリモート CLI セッションを開始します。 • プロンプトが表示されたら、手順 4 で設定したパスワードを入力します。 （注） この手順は、ネットワーキング デバイス自体からネットワーキング デバイスへのリモート Telnet セッションを開始するため、再帰的 Telnet セッションの開始とも呼ばれます。
ステップ 7	**exit** 例： `Device# exit`	ネットワーキング デバイスとのリモート CLI セッション（再帰的 Telnet セッション）を終了します。

トラブルシューティングのヒント

合法的傍受ビューにアクセス可能なすべてのユーザに関する情報を表示するには、**show users lawful-intercept** コマンドを発行します。（このコマンドは、認可された合法的傍受ビュー ユーザしか使用できません）。

次の作業

「ローカル CLI セッションのパスワードの設定と確認, （32 ページ）」に進みます。

ローカル CLI セッションのパスワードの設定と確認

このタスクを実行すると、コンソール ポートでのローカル CLI セッション用のパスワードが割り当てられます。このタスクを完了した後に、コンソール ポートでローカル CLI セッションを起動すると、ネットワーキング デバイスからパスワードの入力が求められます。

このタスクは、コンソール ポートを使用するローカル CLI セッションまたはリモート CLI セッションで実行できます。パスワードを適切に設定したことを確認するオプションの手順を実行する場合、コンソール ポートでローカル CLI セッションを使用して、このタスクを実行する必要があります。

はじめる前に

ローカル CLI セッション パスワードを確認するオプションの手順を実行する場合、ローカル CLI セッションを使用してこのタスクを実行する必要があります。ネットワーク デバイスのコンソール ポートに、端末または端末エミュレーション プログラムが稼働している PC を接続する必要があります。ネットワーキングデバイス上のコンソールポートに使用される設定によって、端末を設定する必要があります。ほとんどのシスコのネットワークデバイスのコンソールポートには、次の設定が必要です。9600 ボー、8 データ ビット、1 ストップ ビット、パリティなし、およびフロー制御は "none" に設定します。これらの設定が端末で機能しない場合は、ネットワーク デバイスのマニュアルを参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **lineconsole0**
4. **password***password*
5. **end**
6. **exit**
7. Enter キーを押します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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 3	**lineconsole0** 例： `Device(config)# line console 0`	ライン コンフィギュレーション モードを開始し、設定しているラインとしてコンソール ポートを選択します。
ステップ 4	**password***password* 例： `Device(config-line)# password Ji8F5Z`	引数 *password* は、ライン パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。 • 最初の文字を数値にはできません。 • ストリングには、80 文字以下の任意の英数字（スペースを含む）を指定できます。数字-スペース-任意の文字の形式ではパスワードを指定できません。 • パスワードは大文字と小文字が区別されます。
ステップ 5	**end** 例： `Device(config-line)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**exit** 例： `Device# exit`	特権 EXEC モードを終了します。
ステップ 7	Enter キーを押します。	（任意）コンソール ポートでローカル CLI セッションを開始します。 • プロンプトが表示されたら、ステップ 4 で設定したパスワードを入力して、適切に設定されたことを確認します。 （注） この手順を実行できるのは、このタスクの実行にローカル CLI セッションを使用している場合だけです。

トラブルシューティングのヒント

新しいパスワードを受け入れられなかったら次に何をするのかについては、パスワード、特権、およびログインによるセキュリティ設定の設定例に進みます。

次の作業

「特権 EXEC モードへのアクセスの保護, （34 ページ）」に進みます。

特権 EXEC モードへのアクセスの保護

イネーブル パスワードの設定と確認

シスコは特権 EXEC モードのパスワード設定に **enablepassword** コマンドを使用することを推奨しなくなりました。**enablepassword** コマンドを使用して入力したパスワードは、ネットワーク デバイスのコンフィギュレーションファイルにプレーンテキストとして保存されます。ネットワーク デバイスのコンフィギュレーションファイルに含まれる **enablepassword** コマンドのパスワードを暗号化するには、**servicepassword-encryption** コマンドを使用します。ただし、**servicepassword-encryption** コマンドで使用される暗号化レベルは、インターネットで入手できるツールを使用して復号化できます。

シスコでは、**enablepassword** コマンドを使用する代わりに、**enablesecret** command コマンドを使用することを推奨します。設定したパスワードが、強力な暗号化方式で暗号化されるためです。パスワード暗号化問題の詳細については、「Cisco IOS XE のパスワード暗号化レベル, （25 ページ）」を参照してください。**enablesecret** コマンドの設定の詳細については、「イネーブル シークレット パスワードの設定と確認, （37 ページ）」を参照してください。

（注） このタスクを正常に実行するため、ネットワーク デバイスでは、**enablesecret** コマンドを使用してパスワードを設定しないでください。**enablesecret** コマンドを使用して特権 EXEC モードのパスワードを既に設定している場合、設定されたパスワードは、このタスクで **enablepassword** コマンドを使用して設定するパスワードより優先されます。

enablesecret コマンドおよび **enable***password* コマンドに同じパスワードは使用できません。

手順の概要

1. **enable**
2. **configureterminal**
3. **enablepassword***password*
4. **end**
5. **exit**
6. **enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**enablepassword***password*
	
	例：
	
	`Device(config)# enable password t6D77CdKq`
		引数 *password* は、イネーブル パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。
		
		• 1 ～ 25 文字の大文字と小文字の英数字を含める必要があります。
		• 先頭の文字に数字は指定できません。
		• 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。
		• パスワードを作成するときに、Ctrl+v キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、abc?123 というパスワードを作成するには、次の手順を実行します。
		  • abc と入力します。
		  • Crtl-v キーを押します。
		  • ?123 と入力します。

ステップ 4	**end** 例： `Device(config)# end`	現在のコンフィギュレーションモードを終了し、特権EXECモードに戻ります。
ステップ 5	**exit** 例： `Device# exit`	特権 EXEC モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 手順 3 で設定したパスワードを入力します。

トラブルシューティングのヒント

新しいパスワードを受け入れられなかったら、次に何をするのかについては、特権 EXEC モードの忘失パスワードまたは誤設定パスワードの復元セクションに進みます。

次の作業

「クリア テキスト パスワードのパスワード暗号化の設定, （36 ページ）」で説明した手順を使用して、ネットワーク デバイスのコンフィギュレーション ファイルにクリア テキストで保存されているイネーブル パスワードを暗号化します。

クリア テキスト パスワードのパスワード暗号化の設定

Cisco IOS XE は、一部の機能について、ネットワーク デバイスのコンフィギュレーション ファイルにクリア テキストでパスワードを保存します。たとえば、ローカルおよびリモートの CLI セッションのパスワード、およびルーティング プロトコルのネイバー認証のパスワードなどです。コンフィギュレーション ファイルのアーカイブ コピーにアクセスできれば、誰でもクリア テキストで保存されているパスワードを発見できるため、クリア テキスト パスワードはセキュリティ リスクです。**servicepassword-encryption** コマンドを使用して、ネットワーク デバイスのコンフィギュレーション ファイルに含まれるクリア テキスト コマンドを暗号化できます。詳細については、「Cisco IOS XE のパスワード暗号化レベル, （25 ページ）」を参照してください。

ネットワーキング デバイスのコンフィギュレーション ファイルにクリア テキストとして保存されているパスワードについて、パスワード暗号化を設定するには、次の手順を実行します。

はじめる前に

このコマンドの結果を即時に確認するために、クリア テキスト パスワードを使用する機能が 1 つ以上、ネットワーキング デバイスに設定されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **servicepassword-encryption**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**servicepassword-encryption** 例： `Device(config)# service password-encryption`	すべてのクリア テキスト パスワード（ユーザ名パスワード、認証キー パスワード、特権コマンド パスワード、コンソールおよび仮想端末ライン アクセス パスワード、および Border Gateway Protocol ネイバー パスワード）について、パスワード暗号化をイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

イネーブル シークレット パスワードの設定と確認

シスコは、**enable***password* コマンドの代わりに **enablesecret** コマンドを使用して特権 EXEC モードを設定することを推奨しています。**enablesecret** コマンドで作成されたパスワードは、より安全な MD5 アルゴリズムで暗号化されます。

（注） **enablesecret** コマンドおよび **enable***password* コマンドに同じパスワードは使用できません。

手順の概要

1. **enable**
2. **configureterminal**
3. 次のいずれかの手順を実行します。
   - **enablesecret***password*
   - **enablesecret5***previously-encrypted-password*
4. **end**
5. **exit**
6. **enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	次のいずれかの手順を実行します。
	
	• **enablesecret***password*
	• **enablesecret5***previously-encrypted-password*
	
	例：
	
	`Device(config)# enable secret t6D77CdKq`
	
	例：
	
	`Device(config)# enable secret 5 $1$/x6H$RhnDI3yLC4GA01aJnHLQ4/`
		引数 *password* は、**enablesecret** パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。
		
		• 1 ～ 25 文字の大文字と小文字の英数字を含める必要があります。
		• 先頭の文字に数字は指定できません。
		• 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。
		• パスワードを作成するときに、Ctrl+v キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、abc?123 というパスワードを作成するには、次の手順を実行します。
		  • abc と入力します。
		  • Crtl-v キーを押します。
		  • ?123 と入力します。

	コマンドまたはアクション	目的
		または 前に暗号化した文字列の前に数字 5 を入力することで、以前に暗号化した特権 EXEC モードのパスワードを設定します。この方式を使用するには、**enablesecret** コマンドによって以前に暗号化されたコンフィギュレーション ファイルから、パスワードの正確なコピーを入力する必要があります。
ステップ 4	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**exit** 例： `Device# exit`	特権 EXEC モードを終了します。
ステップ 6	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 手順 3 で設定したパスワードを入力します。

トラブルシューティングのヒント

新しいパスワードを受け入れられなかったら次に何をするのかについては、パスワード、特権、およびログインによるセキュリティ設定の設定例に進みます。

次の作業

ローカルおよびリモートの CLI セッションのパスワードを設定し終わり、ユーザ名や特権レベルなど、追加のセキュリティ機能を設定する場合、「CLI セッションとコマンドへのアクセスを管理するセキュリティ オプションの設定, （41 ページ）」に進みます。

ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定

レベル 15 より低い特権レベルで **showrunning-config** コマンドを使用してデバイスの実行コンフィギュレーションにアクセスするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **privilege exec all level***levelcommand-string*
4. **file privilege***level*
5. **privilege configure all level***levelcommand-string*
6. **end**
7. **show privilege**
8. **show running-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	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**privilege exec all level***levelcommand-string* 例： `Device(config)# privilege exec all level 5 show running-config`	指定されたコマンドの特権レベルを、1 つの権限レベルから別の特権レベルに変更します。
ステップ 4	**file privilege***level* 例： `Device(config)# file privilege 5`	特権レベルのユーザが、ファイル システムを含むコマンドをデバイスで実行できるようにします。
ステップ 5	**privilege configure all level***levelcommand-string* 例： `Device(config)# privilege configure all level 5 logging`	特権レベルのユーザが、特定のコンフィギュレーションコマンドを表示できるようにします。たとえば、特権レベル 5 のユーザが、実行コンフィギュレーションでロギング コンフィギュレーション コマンドを表示できるようにします。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show privilege** 例： `Device# show privilege`	現在の特権レベルを表示します。
ステップ 8	**show running-config** 例： `Device# show running-config`	指定された特権レベルの現在の実行コンフィギュレーションを表示します。

show running-config コマンドの次の出力は、実行コンフィギュレーションのロギング コンフィギュレーション コマンドを表示します。15 未満の特権レベルを持つユーザは、**privilege configure all level***levelcommand-string* コマンドを設定した後、実行コンフィギュレーションを表示できます。

```
Device# show running-config

Building configuration...

Current configuration : 128 bytes
!
boot-start-marker
boot-end-marker
!
no logging queue-limit
logging buffered 10000000
no logging rate-limit
!
!
!
end
```

CLI セッションとコマンドへのアクセスを管理するセキュリティ オプションの設定

ここでは、特権EXECモードで使用できる全コマンドに対してはアクセス権が持たないユーザが、特権EXECモード コマンドのサブセットを使用できるように、ネットワーキング デバイスを設定するタスクについて説明します。

このようなタスクは、複数レベルのネットワーク サポート スタッフがいて、各レベルのスタッフに、異なるサブセットの特権 EXEC モード コマンドに対するアクセス権を付与したい会社に役立ちます。

このタスクでは、特権EXECモードで使用できる全コマンドに対してはアクセス権を持たないユーザは、窓口のテクニカル サポート スタッフと呼びます。

ここでは、次の手順について説明します。

窓口のテクニカル サポート スタッフ用のネットワーク デバイスの設定

このタスクでは、窓口のテクニカル サポート スタッフ ユーザ用にネットワーキング デバイスを設定する方法について説明します。通常、窓口のテクニカルサポートスタッフは、ネットワーキング デバイスの特権EXECモードで（特権レベル15）使用できる全コマンドの実行は許可されていません。また、特権 EXEC モードに割り当てられているパスワード、またはネットワーキング デバイスに設定されている他の役割に対してアクセス権が付与されていないため、権限がないコマンドを実行できません。

privilege コマンドは、ある特権レベルのコマンドを別の特権レベルに移動するために使用されます。この操作で、ネットワーク デバイスに追加レベルの管理が作成されます。このような操作は、さまざまなスキル レベルを持つ、さまざまなレベルのネットワーク サポート スタッフがいる会社の場合に必要です。

Cisco IOS XE デバイスのデフォルトの設定では、2 種類のユーザが CLI にアクセスできます。1 つ目のユーザは、ユーザ EXEC モードだけにアクセスできるユーザです。2 つ目のユーザは、特権 EXEC モードにアクセスできるユーザです。ユーザ EXEC モードへのアクセスが許可されているだけのユーザは、ネットワークデバイスの設定を表示または変更したり、ネットワークデバイスの稼働状態を変更することはできません。一方、特権 EXEC モードにアクセスできるユーザは、CLI に許可されているネットワーキング デバイスを変更できます。

この作業では、通常特権レベル 15 で動作する 2 つのコマンドは、特権コマンドを使用して特権レベル 7 にリセットされます。窓口のテクニカル サポート スタッフ ユーザが 2 つのコマンドを実行できるようにするためです。特権レベルをリセットする 2 つのコマンドは、**clearcounters** コマンドと **reload** コマンドです。

- **clearcounters** コマンドは、受信されたパケット、送信されたパケット、およびエラーなどの統計情報のために、インターフェイスのカウンタ フィールドをリセットするために使用されます。窓口のテクニカル サポート スタッフ ユーザがネットワーク デバイス間で、またはネットワークに接続しているリモートユーザとの間で、インターフェイスに関する接続の問題を解決しているときに、インターフェイスの統計情報をゼロにリセットしたり、インターフェイスの統計情報カウンタの値が変化するかを見るため、一定の時間インターフェイスを監視するのに役立ちます。
- **reload** コマンドは、ネットワーク デバイスのリブート シーケンスを開始するのに使用します。窓口のテクニカル サポート スタッフによる一般的な reload コマンドの使用方法の 1 つは、メンテナンス ウィンドウでネットワーク デバイスをリブートすることです。この操作によって、高い権限レベルのユーザが以前にネットワーク デバイスのファイル システムにコピーした新しいオペレーティング システムがロードされます。

窓口のテクニカル サポート ユーザ ロールの特権レベルに割り当てられている **enablesecret** パスワードを知る権限を持つユーザは、窓口のテクニカル サポート ユーザとしてそのネットワーク デバイスにアクセスできます。ネットワーク デバイスのユーザ名を設定し、ユーザによるユーザ名とパスワードの把握を必須にして、新たなセキュリティ レベルを追加できます。追加レベルのセキュリティとしてユーザ名を設定する方法については、「窓口のテクニカルサポートスタッフのユーザ名を必須にするデバイスの設定，（47 ページ）」を参照してください。

（注） ネットワーク デバイスでは、**aaanew-model** コマンドをイネーブルにしないでください。コンソール ポートでのローカル CLI セッションの場合、またはリモート CLI セッションの場合、**loginlocal** コマンドを設定しないでください。

（注） このタスクの手順では、わかりやすくするために、各手順に関係する引数とキーワード構文に使用しています。これらのコマンドと併用できるその他の引数とキーワードの詳いては、お使いの Cisco IOS リリースの Cisco IOS コマンド リファレンス マニュアルをてください。

注意 コマンドの特権レベルをデフォルトにリセットする場合、**privilege** コマンドの no 形式しないでください。コンフィギュレーションが適切なデフォルト状態に戻らない可能性ます。コマンドをデフォルトの特権レベルに戻すには、**privilege** コマンドに **reset** キーを使用します。たとえば、コンフィギュレーション コマンドから **privilegeexeclevel***reloa*ンドを削除し、**reload** コマンドをデフォルトの特権レベル 15 に戻すには、**privilegeexecres**コマンドを使用します。

手順の概要

1. **enable**
2. **configureterminal**
3. **enablesecretlevel***levelpassword*
4. **privilegeexeclevel***levelcommand-string*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**enablesecretlevel***levelpassword* 例： `Device(config)# enable secret level 7 Zy72sKj`	特権レベル 7 の新しいイネーブル シークレット パスワードを設定します。
ステップ 4	**privilegeexeclevel***levelcommand-string* 例： `Device(config)# privilege exec level 7 clear counters`	**clearcounters** コマンドの特権レベルを、特権レベル 15 から特権レベル 7 に変更します。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。

窓口のテクニカル サポート スタッフ用の設定の確認

ここでは、ネットワーキング デバイスが窓口のテクニカル サポート スタッフ用に適切に設定されていることを確認するタスクについて説明します。

はじめる前に

次のコマンドは、このタスクのために特権レベル 7 で実行するように変更済みです。

- **clearcounters**
- **reload**

手順の概要

1. **enable***levelpassword*
2. **showprivilege**
3. **clearcounters**
4. **clearipr oute***
5. **reloadintime**
6. **reloadcancel**
7. **disable**
8. **showprivilege**

手順の詳細

ステップ 1 **enable***levelpassword*

level 引数に指定した特権レベルで、ネットワーキング デバイスにログインします。

例：

```
Device> enable 7 Zy72sKj
```

ステップ 2 **showprivilege**

現在の CLI セッションの特権レベルを表示します。

例：

```
Device# show privilege

Current privilege level is 7
```

ステップ 3 **clearcounters**

clear counters コマンドは、インターフェイスのカウンタをクリアします。このコマンドは、特権レベル 15 から特権レベル 7 に変更されました。

例：

```
Device# clear counters

Clear "show interface" counters on all interfaces [confirm]
Device#
02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
```

ステップ 4 **clearipr oute***

clear コマンドの *iproute* 引数文字列は、特権レベル 15 から特権レベル 7 に変更されていないため、使用できません。

例：

```
Device# clear ip route *
                                                                    ^
% Invalid input detected at '^' marker.
```

ステップ 5 **reloadintime**

reload コマンドによって、ネットワーキング デバイスはリブートされます。

例：

```
Device# reload in

10
Reload scheduled in 10 minutes by console
Proceed with reload? [confirm]

Device#

***
*** --- SHUTDOWN in 0:10:00 ---
***
02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20
```

ステップ 6 **reloadcancel**

reloadcancel コマンドによって、以前に **reloadin***time* コマンドで設定したリロードが終了します。

例：

```
Device# reload cancel

***
*** --- SHUTDOWN ABORTED ---
***
04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED:  Scheduled reload cancelled at 15:38:46 PST Sun Mar
27 2005
```

ステップ 7 **disable**

現在の特権レベルを終了し、特権レベル 1 に戻します。

例：

```
Device# disable
```

ステップ 8 **showprivilege**

現在の CLI セッションの特権レベルを表示します。

例：

```
Device> show privilege
```

```
Current privilege level is 1
```

トラブルシューティングのヒント

設定が希望どおりに機能しないため、設定から privilege コマンドを削除する場合、コマンドをデフォルトの特権レベルに戻すには、**privilege** コマンドに **reset** キーワードを使用します。たとえば、コンフィギュレーションから **privilege exec level** *reload* コマンドを削除し、**reload** コマンドをデフォルトの特権レベル 15 に戻すには、**privilege exec reset** *reload* コマンドを使用します。

次の作業

窓口のテクニカル サポート スタッフがログイン名を使用することを必須にして、セキュリティレベルを追加する場合、「窓口のテクニカルサポートスタッフのユーザ名を必須にするデバイスの設定, （47 ページ）」に進みます。

窓口のテクニカル サポート スタッフのユーザ名を必須にするデバイスの設定

このタスクでは、窓口のテクニカル サポート スタッフが、admin のログイン名を使用してネットワーキングデバイスにログインすることを必須にするように、ネットワーキングデバイスを設定します。このタスクで設定された admin ユーザ名には、特権レベル 7 が割り当てられています。この名前を使用してログインするユーザは、前のタスクで特権レベル 7 に再割り当てされたコマンドを実行できます。ユーザがユーザ名 admin で正常にログインすると、CLI セッションは自動的に特権レベル 7 に入ります。

Cisco IOS XE リリース 2.3 よりも前のリリースでは、2 種類のパスワードがユーザ名に関連付けられていました。タイプ 0 は、ルータの特権モードにアクセスできるすべてのユーザから確認できるクリア テキスト パスワードです。また、タイプ 7 は、**servicepasswordencryption** コマンドで暗号化されたパスワードです。

Cisco IOS XE リリース 2.3 以降のリリースでは、**username** コマンドに新しい **secret** キーワードを使用することで、ユーザ名のパスワードに Message Digest 5（MD5）暗号化を設定できます。

はじめる前に

次のコマンドは、このタスクのために特権レベル 7 で実行するように変更済みです。

- **clearcounters**
- **reload**

コマンドの特権レベルを変更する手順については、「窓口のテクニカル サポート スタッフ用のネットワーク デバイスの設定, （42 ページ）」を参照してください。

（注） **username** コマンドの MD5 暗号化は、Cisco IOS XE リリース 2.3 よりも前の Cisco IOS ソフトウェアバージョンではサポートされません。

ネットワーキング デバイスでは、aaa-new model コマンドをイネーブルにしないでください。コンソール ポートでのローカル CLI セッションの場合、またはリモート CLI セッションの場合、**loginlocal** コマンドを設定しないでください。

（注） このタスクの手順では、わかりやすくするために、各手順に関係する引数とキーワードだけ構文に使用しています。これらのコマンドと併用できるその他の引数とキーワードの詳細については、お使いの Cisco IOS XE リリースの Cisco IOS コマンド リファレンス マニュアルを照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **username***username***privilege***level***secret***password*
4. **end**
5. **disable**
6. **login***username*
7. **showprivilege**
8. **clearcounters**
9. **clear***iproute**
10. **reloadin***time*
11. **reloadcancel**
12. **disable**
13. **showprivilege**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**username***username***privilege***level***secret***password* 例： `Device(config)# username admin privilege 7 secret Kd65xZa`	ユーザ名を作成し、*password* テキスト ストリングに MD5 暗号化を適用します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**disable** 例： `Device# disable`	現在の特権レベルを終了し、ユーザ EXEC モードに戻します。
ステップ 6	**login***username* 例： `Device> login admin`	ユーザにログインします。プロンプトが表示されたら、手順3で設定したユーザ名とパスワードを入力します。

ステップ 7	**showprivilege**
	
	例：
	
	`Device# show privilege`
	
	`Current privilege level is 7`
		showprivilege コマンドで、CLI セッションの特権レベルが表示されます。

ステップ 8	**clearcounters**
	
	例：
	
	`Device# clear counters`
	
	`Clear "show interface" counters on all interfaces [confirm]`
	`Device#`
	`02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console`
		clearcounters コマンドでインターフェイス カウンタがクリアされます。このコマンドは、特権レベル 15 から特権レベル 7 に変更されました。

	コマンドまたはアクション	目的

ステップ 9	**clear***iproute**
	
	例：
	
	`Device# clear ip route *`
	
	`^`
	`% Invalid input detected at '^' marker.`
		clear コマンドの *iproute* 引数文字列は、特権レベル 15 から特権レベル 7 に変更されていないため使用できません。

ステップ 10	**reloadin***time*
	
	例：
	
	`Device# reload in`
	
	`10`
	`Reload scheduled in 10 minutes by console`
	`Proceed with reload? [confirm]`
	`Device#`
	`***`
	`*** --- SHUTDOWN in 0:10:00 ---`
	`***`
	`02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20`
		reload コマンドによって、ネットワーキングデバイスはリブートされます。

ステップ 11	**reloadcancel**
	
	例：
	
	`Device# reload cancel`
	
	`***`
	`*** --- SHUTDOWN ABORTED ---`
	`***`
	`04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED: Scheduled reload cancelled at 15:38:46 PST Sun Mar 27 2005`
		reloadcancel コマンドによって、以前に **reloadin***time* コマンドで設定したリロードが終了します。

ステップ 12	**disable** 例： `Device# disable`	現在の特権レベルを終了し、ユーザ EXEC モードに戻します。

ステップ 13	**showprivilege**
	
	例：
	
	`Device> show privilege`
	
	`Current privilege level is 1`
		現在の CLI セッションの特権レベルを表示します。

ローカルセッションの忘失パスワードおよび誤設定パスワードの復元

コンソール ポートでローカル CLI セッションの忘失パスワードおよび誤設定パスワードを復元するために使用できる方式は 3 つあります。使用する方式は、ネットワーキング デバイスの現在の設定によって変わります。

ネットワーク デバイスがリモート CLI セッションを許可するように設定されている

ローカル CLI セッションの忘失パスワードまたは誤設定パスワードを復元するのに最も速い方法は、ネットワーク デバイスでリモート CLI セッションを確立し、「ローカル CLI セッションのパスワードの設定と確認, （32 ページ）」を繰り返すことです。この手順を実行するには、リモート CLI セッションを許可するようにネットワーキング デバイスを設定し、さらにリモート CLI セッションのパスワードを知っている必要があります。

ネットワーク デバイスがリモート CLI セッションを許可するように設定されていない

- ネットワーキング デバイスに対するリモート セッションを確立できず、誤設定したローカル CLI セッション パスワードをスタートアップ コンフィギュレーションに保存していない場合、ネットワーキング デバイスを再起動できます。ネットワーキング デバイスを再起動すると、スタートアップ コンフィギュレーション ファイルが読み込まれます。以前のローカル CLI セッション パスワードが復元されます。

注意 ネットワーキング デバイスの再起動によって、トラフィックの転送が停止されます。また、DHCP サーバ サービスなど、ネットワーキング デバイスで実行されているすべてのサービスが中断されます。必要な操作は、ネットワークのメンテナンスに割り当てられた期間中に、ネットワーキング デバイスを再起動することだけです。

リモートセッションの忘失パスワードおよび誤設定パスワードの復元

忘失または誤設定したリモート CLI セッション パスワードから復元するために使用できる方式は 3 つあります。使用する方式は、ネットワーキング デバイスの現在の設定によって変わります。

ネットワーク デバイスがローカル CLI セッションを許可するように設定されている

リモート CLI セッションの忘失パスワードまたは誤設定パスワードを復元する最速の方法は、ネットワーク デバイスでローカル CLI セッションを確立し、「リモート CLI セッションのパスワードの設定と確認, （29 ページ）」を繰り返すことです。この手順を実行するには、ローカル CLI セッションを許可するようにネットワーキング デバイスを設定し、さらにローカル CLI セッションのパスワードを知っている必要があります。

ネットワーク デバイスがローカル CLI セッションを許可するように設定されていない

- ネットワーキング デバイスに対するローカル CLI セッションを確立できず、誤設定したリモート CLI セッション パスワードをスタートアップ コンフィギュレーションに保存していない場合、ネットワーキング デバイスを再起動できます。ネットワーキング デバイスを再起動すると、スタートアップ コンフィギュレーション ファイルが読み込まれます。以前のリモート CLI セッション パスワードが復元されます。

注意 ネットワーキング デバイスの再起動によって、トラフィックの転送が停止されます。また、DHCP サーバ サービスなど、ネットワーキング デバイスで実行されているすべてのサービスが中断されます。必要な操作は、ネットワークのメンテナンスに割り当てられた期間中に、ネットワーキング デバイスを再起動することだけです。

特権 EXEC モードの忘失パスワードまたは誤設定パスワードの復元

忘失または誤設定した特権 EXEC モード パスワードから復元するために使用できる方式は 2 つあります。使用する方式は、ネットワーキング デバイスの現在の設定によって変わります。

誤設定された特権 EXEC モードのパスワードが保存されていない

- 誤設定した特権 EXEC モード パスワードをスタートアップ コンフィギュレーションに保存していない場合、ネットワーキング デバイスを再起動できます。ネットワーキング デバイスを再起動すると、スタートアップ コンフィギュレーション ファイルが読み込まれます。以前の特権 EXEC モード パスワードが復元されます。

注意 ネットワーキング デバイスの再起動によって、トラフィックの転送が停止されます。また、DHCP サーバ サービスなど、ネットワーキング デバイスで実行されているすべてのサービスが中断されます。必要な操作は、ネットワークのメンテナンスに割り当てられた期間中に、ネットワーキング デバイスを再起動することだけです。

パスワード、特権、およびログインによるセキュリティ設定の設定例

例：ユーザがリモートセッションをクリア可能にするデバイスの設定

次に、管理者以外のユーザがリモート CLI セッションの仮想端末（VTY）回線をクリアできるように、ネットワーキング デバイスを設定する例を示します。

最初の項は、この例の実行コンフィギュレーションの抜粋です。ここでは、この例を使用する方法を示します。

次の項は、実行コンフィギュレーションの抜粋です。

```
!
privilege exec level 7 clear line
!
no aaa new-model
!
!
username admin privilege 7 secret 5 $1$tmIw$1aM7sadKhWMpkVTzxNw1J.
!
privilege exec level 7 clear line
!
! the privilege exec level 7 clear command below is entered automatically
! when you enter the privilege exec level 7 clear line command above, do
! not enter it again
!
privilege exec level 7 clear
!
```

次の項では、**login** コマンドを使用して、ユーザが admin のユーザ名を使用してネットワーク デバイスにログインする場合を示します。

```
R1> login
Username: admin
Password:
```

次の項では、**showprivilege** コマンドを使用して、現在の特権レベルが 7 であることを示します。

```
R1# show privilege

Current privilege level is 7
R1#
```

次の項では、**showuser** コマンドを使用して、現在、2 ユーザ（admin と root）がネットワーク デバイスにログインしていることを示します。

```
R1# show user

    Line       User       Host(s)              Idle       Location
*  0 con 0     admin      idle                 00:00:00
   2 vty 0     root       idle                 00:00:17 172.16.6.2
  Interface    User               Mode         Idle     Peer Address
```

次の項では、**clearline***2* コマンドを使用して、ユーザ名 root に使用されているリモート CLI セッションを終了します。

```
R1# clear line  2
```

```
[confirm]
 [OK]
```

次の項では、**showuser** コマンドを使用して、ネットワーク デバイスに現在ログインしているユーザは admin だけであることを示します。

```
R1# show user
    Line       User       Host(s)              Idle       Location
*  0 con 0     admin      idle                 00:00:00
  Interface    User               Mode         Idle     Peer Address
```

例：ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定

特権レベル 15 を持つユーザ

次に、管理者以外のユーザ（特権EXECモードへのアクセスなし）が、実行コンフィギュレーションを自動的に表示できるようにネットワーキング デバイスを設定する例を示します。この例では、ユーザ名を特権レベル 15 に設定する必要があります。コンフィギュレーション ファイルの多くのコマンドは、特権レベル 15 へのアクセス権を持つユーザだけが表示できるためです。

この点を解決するには、**showrunning-config** コマンドの実行中、一時的に特権レベル 15 へのユーザ アクセスを許可し、コンフィギュレーション ファイルの表示後に、CLI セッションを終了します。この例では、設定ファイルの表示後に、ネットワーキング デバイスが CLI セッションを自動的に終了します。その他の設定手順は必要ありません。

注意 **username** コマンドに **noescape** キーワードを含める必要があります。これは、コンフィギュレーション ファイルの表示を終了し、特権レベル 15 で実行するセッションを終了するエスケープ文字をユーザが入力しないようにするためです。

```
!
!
username viewconf privilege 15 noescape secret 5 $1$zA9C$TDWD/Q0zwp/5xRwRqdgc/.
username viewconf autocommand show running-config
!
```

レベル 15 より低い特権レベルを持つユーザ

次の例は、レベル15より低い特権レベルを持つユーザが、実行コンフィギュレーションを表示可能にするネットワーク デバイスの設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# privilege exec all level 5 show running-config
Device(config)# file privilege 5
Device(config)# privilege configure all level 5 logging
Device(config)# end
Device# show privilege

Current privilege level is 5
```

```
Device# show running-config

Building configuration...

Current configuration : 128 bytes
!
boot-start-marker
boot-end-marker
!
no logging queue-limit
logging buffered 10000000
no logging rate-limit
!
!
!
end
```

例：ユーザがインターフェイスをシャットダウンおよびイネーブル化することを可能にするデバイスの設定

次に、管理者以外のユーザが、インターフェイスをシャットダウンおよびイネーブルにできるように、ネットワーキング デバイスを設定する例を示します。

最初の項は、この例の実行コンフィギュレーションの抜粋です。ここでは、この例を使用する方法を示します。

次の項は、実行コンフィギュレーションの抜粋です。

```
!
no aaa new-model
!
username admin privilege 7 secret 5 $1$tmIw$1aM7sadKhWMpkVTzxNw1J.
!
privilege interface all level 7 shutdown
privilege interface all level 7 no shutdown
privilege configure level 7 interface
privilege exec level 7 configure terminal
!
! the privilege exec level 7 configure command below is entered automatically
! when you enter the privilege exec level 7 configure terminal command above, do
! not enter it again
!
privilege exec level 7 configure
!
```

次の項では、**login** コマンドを使用して、ユーザが admin のユーザ名を使用してネットワーク デバイスにログインする場合を示します。

```
R1> login
Username: admin
Password:
```

次の項では、**showprivilege** コマンドを使用して、現在の特権レベルが 7 であることを示します。

```
R1# show privilege
Current privilege level is 7
```

次の項では、**showuser** コマンドを使用して、ネットワーク デバイスに現在ログインしているユーザは admin だけであることを示します。

```
R1# show user
    Line       User       Host(s)              Idle       Location
```

```
*  0 con 0     admin      idle                 00:00:00
  Interface    User               Mode         Idle     Peer Address
```

次の項は、admin ユーザがインターフェイスをシャットダウンおよびイネーブルにできる権限を持つことを示します。

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface ethernet 1/0
R1(config-if)# shutdown
R1(config-if)# no shutdown
R1(config-if)# exit
R1#
```

次の作業

ネットワーキング デバイスのセキュリティの基本を設定したら、次のように高度なオプションを考慮できます。

- ロールベースの CLI アクセス：ネットワーク マネージャが、さまざまなレベルのテクニカル サポート スタッフに、異なるレベルの CLI コマンドのアクセスを付与する場合、ロールベースの CLI アクセス機能には、（このドキュメントで説明する）**privilege** コマンドよりも包括的なオプション セットが用意されています。
- AAA セキュリティ：多くのシスコ ネットワーク デバイスは、認証、許可、およびアカウンティング（AAA）機能を使用して、高度なレベルのセキュリティを提供しています。ネットワーキング デバイスで AAA を使用し、リモート TACACS+ または RADIUS サーバを併用することで、このドキュメントで説明しているすべてのタスクと、他のより高度なセキュリティ機能を実装できます。ネットワーク デバイスのローカルで実行できる AAA セキュリティ機能を設定する方法、または TACACS+ や RADIUS サーバを使用してリモート AAA セキュリティを設定する方法については、『*Cisco IOS XE Security Configuration Guide:Securing User Services* リリース 2』を参照してください。

その他の参考資料

ここでは、パスワードによるセキュリティの設定、およびネットワーキング デバイスでの CLI セッションのログイン ユーザ名に関連する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
CLI コマンドおよび設定情報に対するユーザ アクセスの管理	『*Cisco IOS XE Security Configuration Guide: Securing User Services*』Release 2 の「Role-Based CLI Access」
AAA セキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*』Release 2

関連項目	マニュアル タイトル
TACACS+ および RADIUS での特権レベルの割り当て	『How to Assign Privilege Levels with TACACS+ and RADIUS』

標準

規格	タイトル
この機能によってサポートされる新しい RFC または変更された RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC または変更された RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

パスワード、特権、およびログインによるセキュリティ設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2*：ネットワーク デバイス上の *CLI* セッションでのパスワード、特権レベル、およびログイン ユーザ名によるセキュリティ設定に関する機能情報

機能名	リリース	機能の設定情報
強化されたパスワード セキュリティ		Enhanced Password Security 機能を使用すると、ユーザ名のパスワードに MD5 暗号化を設定できます。MD5 暗号化は、暗号化されたパスワードの逆送信を不可能にする一方向ハッシュ関数であり、強力な暗号化保護を可能にします。MD5 暗号化を使用すると、クリア テキスト パスワードを取得できません。MD5 で暗号化されたパスワードは、クリア テキスト パスワードを取得可能にすることを必須にするプロトコルでは使用できません。たとえば、チャレンジ ハンドシェーク認証プロトコル（CHAP）などのプロトコルです。

第 4 章

ロールベースの CLI アクセス

ロールベースのCLIアクセス機能を使用すれば、ネットワーク管理者はビューを定義できます。ビューは、Cisco IOS EXEC コマンドおよびコンフィギュレーション（config）モード コマンドへのアクセスを精選したり部分的に制限する、操作コマンドと設定機能のセットです。ビューで、ユーザの Cisco IOS コマンドライン インターフェイス（CLI）や設定情報へのアクセスを制限します。つまり、ビューで、使用するコマンドや表示する設定情報を定義できます。したがって、ネットワーク管理者はシスコ ネットワーキング デバイスへのアクセスを柔軟に管理できます。

- 機能情報の確認，61 ページ
- ロールベースの CLI アクセスの前提条件，62 ページ
- ロールベースの CLI アクセスの制約事項，62 ページ
- ロールベースの CLI アクセスに関する情報，62 ページ
- ロールベースの CLI アクセスの使用方法，64 ページ
- ロールベースの CLI アクセスの設定例，70 ページ
- ロールベースの CLI アクセスに関する追加情報，72 ページ
- ロールベースの CLI アクセスに関する機能情報，73 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ロールベースの CLI アクセスの前提条件

イメージで CLI ビューをサポートする必要があります。

ロールベースの CLI アクセスの制約事項

合法的傍受イメージの制限

CLI ビューは Cisco IOS パーサーの一部であるため、すべてのプラットフォームおよび Cisco IOS イメージの一部です。ただし、合法的傍受ビューは、合法的傍受サブシステムが組み込まれたイメージ内でしか使用できません。

許可されたビューの最大数

1 つの合法的傍受ビューを含む CLI ビューとスーパービューの設定可能な最大数は 15 です（これには、ルート ビューは含まれません）。

ロールベースの CLI アクセスに関する情報

CLI ビューを使用するメリット

ユーザは特権レベルとイネーブルモードパスワードの両方を介して CLI アクセスを制御できますが、これらの機能では、ネットワーク管理者に Cisco IOS デバイスを操作するのに必要な詳細レベルが提供されません。CLI ビューは、より詳細なアクセス コントロール機能をネットワーク管理者に提供するため、Cisco IOS ソフトウェア全体のセキュリティとアカウンタビリティが向上します。

Cisco IOS Release 12.3(11)T 以降では、ネットワーク管理者が、ビューへのインターフェイスまたはインターフェイス グループを指定することもできます。そのため、指定されたインターフェイスに基づくアクセスが可能になります。

ルート ビュー

システムがルート ビューになっている場合は、レベル 15 の権限を持つユーザとして、すべてのアクセス権限が付与されます。管理者がシステムのビュー（CLI ビュー、スーパービュー、合法的傍受ビューなど）を設定する場合は、システムをルート ビューにする必要があります。

レベル 15 権限を持つユーザとルート ビュー ユーザの違いは、ルート ビュー ユーザは、新しいビューを設定したり、ビューに対してコマンドを追加または削除したりできることです。また、CLI ビューでは、ルート ビュー ユーザがそのビューに追加したコマンドにしかアクセスできません。

合法的傍受ビュー

CLI ビューと同様に、合法的傍受ビューは、特定のコマンドと設定情報へのアクセスを制限します。具体的には、合法的傍受ビューを使用すれば、ユーザは、コールとユーザに関する情報を保存する簡易ネットワーク管理プロトコル（SNMP）コマンドの特別なセットである TAP-MIB 内に保持された合法的傍受コマンドへのアクセスを保護できます。

合法的傍受ビュー内で使用可能なコマンドは、次のカテゴリのいずれかに属します。

- 他のビューまたは権限レベルでは使用不可にすべき合法的傍受コマンド
- 合法的傍受ユーザにとっては有効であるが、他のビューまたは権限レベルから除外する必要のない CLI ビュー

スーパービュー

スーパービューは、1 つ以上の CLI ビューで構成されています。このビューでは、受け入れるコマンドと表示する設定情報を定義できます。スーパービューを使用すれば、ネットワーク管理者は、複数の CLI ビューをユーザ グループに割り当てなくても、設定された CLI ビュー内のすべてのユーザをスーパービューに割り当てることができます。

スーパービューには次の特性があります。

- CLI ビューを複数のスーパービュー間で共有できます。
- スーパービューにはコマンドを設定できません。つまり、CLI ビューにコマンドを追加してから、その CLI ビューをスーパービューに追加する必要があります。
- スーパービューにログインしたユーザは、そのスーパービューに属している CLI ビューに設定されたすべてのコマンドにアクセスできます。
- スーパービューごとにパスワードが設定されます。このパスワードは、スーパービューを切り替えたり、CLI ビューからスーパービューに切り替えたりするために使用されます。
- スーパービューが削除されても、関連する CLI ビューは削除されません。

ビュー認証と新しい AAA 属性

ビュー認証は、新しい属性の **cli-view-name** を介して、外部の認証、許可、およびアカウンティング（AAA）サーバで実行されます。

AAA 認証は特定のユーザに 1 つのビュー名のみを関連付けます。つまり、認証サーバ内の 1 人のユーザに対して 1 つのビュー名しか設定できません。

ロールベースの CLI アクセスの使用方法

CLI ビューの設定

このタスクを実行して、CLI ビューを作成し、必要に応じて、コマンドまたはインターフェイスをビューに追加します。

はじめる前に

ビューを作成する前に、次のタスクを実行する必要があります。

- **aaanew-model** コマンドを使用して AAA をイネーブルにします。
- システムが特権レベル 15 ではなく、ルート ビューになっていることを確認します。

手順の概要

1. **enableview**
2. **configureterminal**
3. **parserview***view-name* [**inclusive**]
4. **secret** [**0** | **5**]*encrypted-password*
5. **commands***parser-mode* {**exclude** | **include-exclusive** | **include**} [**all**] [**interface***interface-name* | *command*]
6. **end**
7. **enable** [*privilege-level* | **view***view-name*]
8. **showparserviewall**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enableview** 例： `Device> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルート パスワードなど）を入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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 3	**parserview***view-name* [**inclusive**]
	
	例：
	
	`Device(config)# parser view first inclusive`
	`Device(config-view)#`
		すべてのコマンドを含むビューがデフォルトで作成されます。**inclusive** キーワードオプションを選択しないと、すべてのコマンドを除くビューがデフォルトで作成されます。ビューの設定モードになります。

ステップ 4	**secret** [**0** | **5**]*encrypted-password* 例： `Device(config-view)# secret 5 secret`	CLI ビューまたはスーパービューとパスワードを関連付けます。 （注） このコマンドを発行しなければ、ビューのその他の属性が設定できません。 （注） CSCts50236 を使用すると、パスワードは削除または上書きできます。設定されたパスワードを削除するには、**no secret** コマンドを使用します。
ステップ 5	**commands***parser-mode* {**exclude** | **include-exclusive** | **include**} [**all**] [**interface***interface-name* | *command*] 例： `Device(config-view)# commands exec include show version`	コマンドまたはインターフェイスをビューに追加し、指定されたコマンドがあるモードを指定します。 （注） parser view プロファイルを設定するときは、次の **no** または **default** コマンドはスタートアップ コンフィギュレーションには保存されません。これらのコマンドは、デバイスがリロードされるまで使用中です。デバイスをリロードしたら、必要な結果が得られるように、これらのコマンドを再適用します。 • **commands configure include all no** • **commands interface include all no** • **commands configure include all default**
ステップ 6	**end** 例： `Device(config-view)# end`	ビューのコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**enable** [*privilege-level* | **view***view-name*] 例： `Device# enable view first`	設定済みの CLI ビューにアクセスするためのパスワードを求めるプロンプトが表示され、1 つのビューから別のビューへ切り替えられます。 パスワードを入力して CLI ビューにアクセスします。
ステップ 8	**showparserviewall** 例： `Device# show parser view all`	（任意）デバイス上で設定されるすべてのビューに関する情報を表示します。

	コマンドまたはアクション	目的
		（注） このコマンドはルート ユーザと合法的傍受ユーザの両方に使用できますが、**all** キーワードはルート ユーザしか使用できません。ただし、**all** キーワードは、ルート ビュー内のユーザが、合法的傍受ビューや CLI ビュー内のユーザに使用を許可するように設定できます。

トラブルシューティングのヒント

パスワードとビューを関連付ける必要があります。パスワードを関連付けずに、**commands** コマンド経由でビューにコマンドを追加しようとすると、次のようなシステム メッセージが表示されます。

```
%Password not set for view <viewname>.
```

合法的傍受ビューの設定

このタスクを実行して、ビューを初期化し、合法的傍受固有のコマンドと設定情報用に設定します

はじめる前に

合法的傍受ビューを初期化する前に、**privilege** コマンド経由で特権レベルが 15 に設定されていることを確認します。

（注） レベル 15 権限を持っている管理者またはユーザだけが合法的傍受ビューを初期化できます。

手順の概要

1. **enableview**
2. **configureterminal**
3. **li-view***li-password* **user***username* **password***password*
4. **usernamelawful-intercept** [*name*] [**privilege***privilege-level*| **view***view-name*] **password***password*
5. **parserview***view-name*
6. **secret5***encrypted-password*
7. **name***new-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	**enableview** 例： `Device> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルートパスワードなど）を入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**li-view***li-password***user***username***password***password* 例： `Device(config)# li-view lipass user li_admin password li_adminpass`	合法的傍受ビューを初期化します。 li-view が初期化されたら、**user***username***password***password* オプション経由で少なくとも 1 人のユーザを指定する必要があります。
ステップ 4	**usernamelawful-intercept** [*name*] [**privilege***privilege-level*| **view***view-name*] **password***password* 例： `Device(config)# username lawful-intercept li-user1 password li-user1pass`	シスコ デバイス上で合法的傍受ユーザを設定します。
ステップ 5	**parserview***view-name* 例： `Device(config)# parser view li view name`	（任意）ビュー コンフィギュレーション モードに入ります。このモードでは、合法的傍受ビューのパスワードや名前を変更できます。
ステップ 6	**secret5***encrypted-password* 例： `Device(config-view)# secret 5 secret`	（任意）合法的傍受ビューの既存のパスワードを変更します。
ステップ 7	**name***new-name* 例： `Device(config-view)# name second`	（任意）合法的傍受ビューの名前を変更します。 このコマンドが発行されなかった場合、合法的傍受ビューのデフォルト名は "li-view" になります。

トラブルシューティングのヒント

合法的傍受ビューにアクセス可能なすべてのユーザに関する情報を表示するには、**show users lawful-intercept** コマンドを発行します。（このコマンドは、認可された合法的傍受ビュー ユーザしか使用できません）。

スーパービューの設定

このタスクを実行して、スーパービューを設定し、スーパービューに少なくとも 1 つの CLI ビューを追加します。

はじめる前に

CLI ビューをスーパービューに追加する前に、スーパービューに追加する CLI ビューがシステム内で有効なビューであることを確認します。つまり、ビューが、**parserview** コマンド経由で正常に作成されたことを確認します。

（注） スーパービューにビューを追加するには、スーパービューに対してパスワードを設定する必要があります（**secret5** コマンド経由）。その後で、ビュー コンフィギュレーション モードで **view** コマンドを発行して、少なくとも 1 つの CLI ビューをスーパービューに追加します。

手順の概要

1. **enableview**
2. **configureterminal**
3. **parserview***superview-name***superview**
4. **secret5***encrypted-password*
5. **view***view-name*
6. **end**
7. **showparserviewall**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enableview** 例： `Device> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルート パスワードなど）を入力します。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**parserview***superview-name***superview** 例： `Device(config)# parser view su_view1 superview`	スーパービューを作成して、ビュー コンフィギュレーション モードに入ります。
ステップ 4	**secret5***encrypted-password* 例： `Device(config-view)# secret 5 secret`	CLI ビューまたはスーパービューとパスワードを関連付けます。 （注） このコマンドを発行しなければ、ビューのその他の属性が設定できません。
ステップ 5	**view***view-name* 例： `Device(config-view)# view view_three`	正常な CLI ビューをスーパービューに追加します。 特定のスーパービューに追加する各CLIビューに対して、このコマンドを発行します。
ステップ 6	**end** 例： `Device(config-view)# end Device#`	ビューのコンフィギュレーションモードを終了し、特権EXECモードに戻ります。
ステップ 7	**showparserviewall** 例： `Device# show parser view`	（任意）デバイス上で設定されるすべてのビューに関する情報を表示します。 （注） このコマンドはルート ユーザと合法的傍受ユーザの両方に使用できますが、**all** キーワードはルート ユーザしか使用できません。ただし、**all** キーワードは、ルート ビュー内のユーザが、合法的傍受ビューやCLIビュー内のユーザに使用を許可するように設定できます。

ビューとビュー ユーザのモニタリング

すべてのビュー ルート、CLI、合法的傍受、およびスーパービューに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debugparserview** コマンドを使用します。

ロールベースの CLI アクセスの設定例

例：CLI ビューの設定

次の例は、2 つの CLI ビュー "first" と "second" の設定方法を示しています。その後、実行コンフィギュレーションの CLI ビューを確認できます。

```
Device(config)# parser view first inclusive
Device(config-view)# secret 5 firstpass
Device(config-view)# command exec exclude show version
Device(config-view)# command exec exclude configure terminal
Device(config-view)# command exec exclude all show ip
Device(config-view)# exit
Device(config)# parser view second
Device(config-view)# secret 5 secondpass
Device(config-view)# command exec include-exclusive show ip interface
Device(config-view)# command exec include logout
Device(config-view)# exit
!
!
Device(config-view)# do show running-config | beg view

parser view first inclusive
 secret 5 $1$MCmh$QuZaU8PIMPlff9sFCZvgW/
 commands exec exclude configure terminal
 commands exec exclude configure
 commands exec exclude all show ip
 commands exec exclude show version
 commands exec exclude show
!
parser view second
 secret 5 $1$iP2M$R16BXKecMEiQesxLyqygW.
 commands exec include-exclusive show ip interface
 commands exec include show ip
 commands exec include show
 commands exec include logout
!
```

例：CLI ビューの確認

CLI ビューの "first" と "second" を設定したら、**enableview** コマンドを発行して、各ビュー内で使用可能なコマンドを確認できます。次の例は、ユーザが CLI ビューの "first" にログイン後に、どのコマンドがこのビュー内で使用可能かを示しています。（**showip** コマンドは all オプションと一緒に設定されているため、second ビュー内で **include-exclusive** キーワードを使用している **showipinterface** コマンドを除く、すべてのサブオプションのセットが表示されます）。

```
Device# enable view first
Password:
```

```
Device# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information
Device# show ?
  ip       IP information
  parser   Display parser information
  version  System hardware and software status
Device# show ip ?

  access-lists            List IP access lists
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
  drp                     Director response protocol
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Device Discovery Protocol
.
.
.
```

例：合法的傍受ビューの設定

次の例は、合法的傍受ビューの設定方法、ビューへのユーザの追加方法、および追加されたユーザの確認方法を示しています。

```
!Initialize the LI-View.
Device(config)# li-view lipass user li_admin password li_adminpass
Device(config)# end
! Enter the LI-View; that is, check to see what commands are available within the view.
Device# enable view li-view
Password:
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parser view li-view

Device(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views
Device(config-view)#
! NOTE:LI View configurations are never shown as part of 'running-configuration'.
! Configure LI Users.
Device(config)# username lawful-intercept li-user1 password li-user1pass

Device(config)# username lawful-intercept li-user2 password li-user2pass
! Displaying LI User information.
```

```
Device# show users lawful-intercept
li_admin
li-user1
li-user2
Device#
```

（注） 合法的傍受ビューは特定のイメージに対してのみ使用でき、表示名オプションは合法的傍受ビューでのみ使用できます。

例：スーパービューの設定

次の **showrunning-config** コマンドのサンプル出力は、"view_one" と "view_two" がスーパービューの "su_view1" に追加され、"view_three" と "view_four" がスーパービューの "su_view2" に追加されていることを示しています。

```
Device# show running-config
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

ロールベースの CLI アクセスに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

関連項目	マニュアル タイトル
SNMP、MIB、CLI 設定	『*Cisco IOS Network Management Configuration Guide , Release 15.0.*』
権限レベル	「パスワード、特権、およびログインによるセキュリティ設定」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ロールベースの CLI アクセスに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3*：ロールベースの *CLI* アクセスに関する機能情報

機能名	リリース	機能情報
ロールベースの CLI アクセス		ロールベースのCLIアクセス機能は、ネットワーク管理者が、CLIと設定情報に対するユーザアクセスを制限できるようにします。 CLI ビュー機能は、インターフェイス単位レベルでユーザアクセスを制限するように拡張されました。新しいCLIビューは、拡張されたビュー機能をサポートするために導入されました。また、設定された CLI ビューをスーパービューにグループ分けするためのサポートが導入されました。 次のコマンドが導入または変更されました。**commands**（**view**）、**enable**、**li-view**、**name**（**view**）、**parserview**、**parserviewsuperview**、**secret**、**showparserview**、**showusers**、**username**、および **view**。
ロールベースのCLI包含ビュー		ロールベースのCLI包含ビュー機能によって、すべてのコマンドを含む標準 CLI ビューがデフォルトで有効になっています。 次のコマンドが変更されました。**parserviewinclusive**。

第 5 章

AutoSecure

AutoSecure 機能では、1 つの CLI コマンドによって、ネットワーク攻撃に悪用されるおそれのある一般的な IP サービスを無効にしたり、攻撃を受けたときにネットワークを防御するのに役立つ IP サービスや機能を有効にしたりできます。また、ルータのセキュリティ設定を簡素化しつつ機能を堅牢にすることができます。

AutoSecure では、「lab」や「cisco」など、ネットワークで広く使用されているありふれたパスワードが排除され、最小限必要なパスワード長が設定されることで、ルータへのセキュアなアクセスが強化されています。正常に実行できなかった回数が、設定したしきい値を超えると、syslog メッセージが生成されます。

また、ロールバックを有効にすると、AutoSecure 設定に失敗しても、ルータを前の設定状態に戻すことができます。

AutoSecure を有効にすると、システム ロギング メッセージの詳細な監査証跡によって、実行コンフィギュレーションに適用される可能性のある AutoSecure の設定変更または改ざんがキャプチャされます。

- 機能情報の確認，75 ページ
- AutoSecure の制約事項，76 ページ
- AutoSecure について，76 ページ
- AutoSecure の設定方法，81 ページ
- AutoSecure の設定例，83 ページ
- その他の参考資料，85 ページ
- AutoSecure に関する機能情報，86 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモ

ジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

AutoSecure の制約事項

AutoSecure の設定は、実行時またはセットアップ時に行います。AutoSecure をイネーブルにした後に、関連する設定を変更した場合は、AutoSecure の設定が完全に有効にならないことがあります。

AutoSecure について

管理プレーンのセキュリティ保護

管理プレーンのセキュリティ保護は、潜在的にセキュリティ攻撃に利用される可能性がある特定のグローバルおよびインターフェイス サービスをオフにし、攻撃の脅威を軽減できるグローバル サービスをオンにすることで行います。また、セキュリティ保護されたアクセスとロギングもルータに設定できます。

注意 デバイスがネットワーク管理（NM）アプリケーションで管理されている場合、管理プレーンのセキュリティ保護によって、HTTP サーバなどのいくつかのサービスがディセーブル化され、NM アプリケーションのサポートが妨げられることがあります。

ここでは、AutoSecure がマネジメント プレーンのセキュリティ保護にどのように役立つかを説明します。

グローバル サービスのディセーブル化

この機能をイネーブルにすると（**auto secure** コマンドを介して）、次のグローバル サービスはルータで自動的にディセーブルになります。

- Finger：攻撃の前にシステムの情報を収集（探査）します。イネーブルになっている場合、この情報により、デバイスが攻撃に対して脆弱なままになることがあります。
- PAD：すべてのパケット アセンブラ/逆アセンブラ（PAD）コマンドと、PAD デバイスとアクセス サーバとの接続をイネーブルにします。イネーブルになっている場合、このサービスにより、デバイスが攻撃に対して脆弱なままになることがあります。

- スモール サーバ：TCP およびユーザ データグラム プロトコル（UDP）の診断ポート攻撃の原因となります。この攻撃では、送信者がルータの UDP 診断サービスに偽の要求を大量に送信し、すべての CPU リソースを使い果たします。
- BOOTP サーバ：BOOTP はセキュアではないプロトコルです。攻撃で悪用されます。
- HTTP サーバ：Secure HTTP サーバが使用されていないか、ACL を関連付けて HTTP サーバに組み込まれる認証が使用されていない場合、HTTP サーバは安全ではなく、攻撃に悪用されることがあります。（HTTP サーバをイネーブルにする必要がある場合は、適切な認証またはアクセス リストの指定を求めるメッセージが表示されます）。

（注） Cisco Configuration Professional（CCP）を使用している場合は、**ip http server** コマンドを介して手動で HTTP サーバをイネーブルにする必要があります。

- 識別サービス：RFC 1413 で定義されている安全ではないプロトコルです。TCP ポートで ID を照会することが可能です。攻撃者は、ID サーバでユーザに関する個人的な情報にアクセスできます。
- CDP：大量の Cisco Discovery Protocol（CDP）パケットがルータに送信されると、ルータの使用可能なメモリが消費され、ルータがクラッシュすることがあります。

注意 CDP を使用してネットワーク トポロジを検出する NM アプリケーションは、検出を実行できなくなります。

- NTP：認証またはアクセス コントロールが行われないと、ネットワーク タイム プロトコル（NTP）は安全ではありません。攻撃者はこのプロトコルを使用して NTP パケットを送信し、ルータをクラッシュさせたり、過負荷状態にしたりすることが可能です。（NTP を有効にする場合は、メッセージ ダイジェスト 5（MD5）および **ntp access-group** コマンドを使用して NTP 認証を設定する必要があります。NTP がグローバルにイネーブルになっている場合は、NTP が不要なすべてのインターフェイスでディセーブルにしてください）。
- 送信元ルーティング：デバッグ作業でのみ使用するため、それ以外のすべての場合でルーティングをディセーブルにする必要があります。そうしないと、アクセス コントロール メカニズムを通過すべきパケットが、一部のアクセス コントロール メカニズムを回避する可能性があります。

サービスのインターフェイス単位のディセーブル化

この機能をイネーブルにすると、次のインターフェイス単位のサービスが自動的にルータでディセーブルになります。

- ICMP リダイレクト：すべてのインターフェイスでディセーブルになります。このサービスは、正しく設定されたネットワークにとっては有益な機能ではなく、セキュリティホールを悪用するために攻撃者によって使用される可能性があります。
- ICMP 到達不能：すべてのインターフェイスでディセーブルになります。インターネット制御マネジメントプロトコル（ICMP）到達不能は、ICMP ベースのサービス拒否攻撃（DoS）の原因として知られています。
- ICMP マスク応答メッセージ：すべてのインターフェイスでディセーブルになります。ICMP マスク応答メッセージにより、攻撃者はインターネットワークの特定のサブネットワークのサブネットマスクを入手できます。
- プロキシ Arp：すべてのインターフェイスでディセーブルになります。プロキシ Arp 要求は、DoS 攻撃の原因として知られています。これは、攻撃者が何度も送信した要求に応答しようとしてルータの使用可能な帯域幅とリソースが消費されることがあるためです。
- ダイレクトブロードキャスト：すべてのインターフェイスでディセーブルになります。DoS を生じさせるための SMURF 攻撃の原因となる可能性があります。
- メンテナンス オペレーション プロトコル（MOP）サービス：すべてのインターフェイスでディセーブルになります。

グローバル サービスのイネーブル化

AutoSecure 機能をイネーブルにすると、次のグローバル サービスが自動的にルータでイネーブルになります。

- **service password-encryption** コマンド：設定でパスワードが表示されなくなります。
- **service tcp-keepalives-in** および **service tcp-keepalives-out** コマンド：異常終了した TCP セッションが確実に削除されます。

ルータへのアクセスの保護

注意 デバイスが NM アプリケーションによって管理されている場合に、ルータへのアクセスをセキュリティ保護すると、重要なサービスが無効化されたり、NM アプリケーションのサポートが妨げられたりすることがあります。

AutoSecure 機能をイネーブルにすると、ルータへのアクセスをセキュリティ保護する次のオプションをユーザが使用できるようになります。

- テキストバナーがない場合は、バナーの追加を求めるメッセージが表示されます。AutoSecure 機能には次のサンプル バナーが用意されています。

```
Authorized access only
This system is the property of ABC Enterprise
```

```
Disconnect IMMEDIATELY if you are not an authorized user!
Contact abc@xyz.com +99 876 543210 for help.
```

- ログインおよびパスワード（サポートされている場合はシークレット パスワードを推奨）は、コンソール、AUX、TTY の各回線で設定されます。**transport input** および **transport output** コマンドも、これらのすべての回線で設定されます。（Telnet およびセキュア シェル（SSH）のみが有効な転送方式です。）**exec-timeout** コマンドは、コンソールと AUX の各回線で 10 に設定されます。
- デバイスのイメージが暗号化イメージである場合、AutoSecure はルータに対するアクセスとファイル転送に SSH とセキュア コピー（SCP）をイネーブルにします。**ip ssh** コマンドの **timeout** *seconds* および **authentication-retries** *integer* オプションは最小数に設定されます。（Telnet および FTP は、この操作の影響を受けず、引き続き動作します）。
- AutoSecure ユーザが、デバイスで簡易ネットワーク管理プロトコル（SNMP）を使用しないと指定した場合は、次のいずれかの状態になります。
  - インタラクティブ モードでは、コミュニティ ストリングの値に関係なく SNMP をディセーブルにするかどうかを尋ねるメッセージがユーザに表示されます。コミュニティ ストリングは、パスワードと同じように機能し、ルータのエージェントへのアクセスを規制します。
  - 非インタラクティブ モードでは、コミュニティ ストリングが "public" または "private" である場合に SNMP がディセーブルになります。

（注） AutoSecure がイネーブルになると、装置のモニタおよび設定のために SNMP を使用するツールは、SNMP を使用する装置との通信を行うことができなくなります。

- 認証、許可、アカウンティング（AAA）が設定されていない場合は、ローカル AAA を設定します。ユーザは、ローカルのユーザ名とそのパスワードをルータで設定するように AutoSecure から要求されます。

セキュリティ ロギング

次のロギング オプションは、AutoSecure をイネーブルにした後で使用できます。これらのオプションは、セキュリティ インシデントを特定し、顧客に対応する方法を提供します。

- すべてのデバッグ メッセージおよびログ メッセージのシーケンス番号とタイム スタンプ。このオプションは、ロギング メッセージを監査するときに役立ちます。
- ロギング メッセージはログ関連のイベントに対して生成されます。たとえば、ログイン攻撃が検出されルータが「待機モード」に入ると、「Blocking Period when Login Attack Detected」のメッセージが表示されます。（待機モードでは、ルータは Telnet、HTTP、または SSH を使用したログイン試行を許可しません）。

ログイン関連のシステム メッセージの詳細については、『Cisco IOS Release 12.3(4)T feature module Cisco IOS Login Enhancements』を参照してください。

- **logging console critical** コマンド。これにより、システム ロギング（syslog）メッセージがすべての使用可能な TTY 回線に送信され、重大度に応じてメッセージが制限されます。
- **logging buffered** コマンド。これにより、ロギング メッセージが内部バッファにコピーされ、バッファに記録されるメッセージが重大度に応じて制限されます。
- **logging trap debugging** コマンド。これにより、デバッグよりも重大度の高いコマンドをすべてロギング サーバに送信できます。

フォワーディング プレーンのセキュリティ保護

ルータのフォワード プレーンでの攻撃の危険を最小限にするために、AutoSecure には次の機能が用意されています。

- Cisco エクスプレス フォワーディング（CEF）：AutoSecure は、可能であれば CEF または分散 CEF（dCEF）をルータでイネーブルにします。トラフィックが新たな宛先に到着し始めたときにキャッシュ エントリを作成する必要がないため、大量のトラフィックが多数の宛先に送信される場合でも、CEF は他のモードよりも予測しやすい方法で動作します。このため、CEF 用に設定されているルータは、SYN 攻撃下において、従来のキャッシュ方法を採用しているルータと比較して高い性能を発揮します。

（注） CEF は従来のキャッシュよりもメモリを多く消費します。

- TCP インターセプト機能が使用可能な場合、この機能をルータで接続タイムアウト用に設定することができます。
- ストリクト ユニキャスト リバース パス転送（uRPF）が使用可能である場合、偽造（詐称）された送信元 IP アドレスが入ってくることによって発生する問題を軽減できるようにするために、この uRPF をルータで設定できます。uRPF は検証可能な送信元 IP アドレスが不足している IP パケットを廃棄します。
- ルータは、ファイアウォールとして使用されている場合、インターネットに繋がっているパブリック インターフェイスでコンテキストベース アクセス コントロール（CBAC）用に設定することができます。

（注） AutoSecure ダイアログの冒頭では、パブリック インターフェイスのリストの指定を求めるメッセージが表示されます。

AutoSecure の設定方法

AutoSecure の設定

注意 **auto secure** コマンドでルータのセキュリティ保護を行うことはできますが、ルータが完全にセキュリティ保護されるという保証はありません。

手順の概要

1. **enable**
2. auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 パスワードを入力します（要求された場合）。

ステップ 2	auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]
	
	例：
	
	`Router#`
	`auto secure`
		セミインタラクティブ ダイアログ セッションは、**management** または **forwarding** キーワードが選択されているときに、ルータの管理またはフォワーディング プレーンのセキュリティ保護を開始します。いずれのオプションも選択しないと、ダイアログによってどちらのプレーンにも設定するよう尋ねられます。**management** キーワードが選択されると、管理プレーンだけがセキュリティ保護されます。**forwarding keyword が選択されると**、フォワーディング プレーンのみがセキュリティ保護されます。
		
		no-interact キーワードが選択されると、どのようなインタラクティブな設定も求められません。
		
		full キーワードが選択されると、デフォルトで、ユーザはすべてのインタラクティブな質問を入力するように求められます。

強化されたルータへのセキュリティ アクセスの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **enablepassword** {*password* | [*encryption-type*] *encrypted-password* }
4. **securityauthenticationfailurerate***threshold-rate***log**
5. **exit***threshold-rate***log**
6. **showautosecureconfig**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**enablepassword** {*password* | [*encryption-type*] *encrypted-password* } 例： `Router(config)# enable password elephant`	さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。
ステップ 4	**securityauthenticationfailurerate***threshold-rate***log** 例： `Router(config)# security authentication failure rate 10 log`	許容されるログイン失敗回数を設定します。 • *threshold-rate*：許容されるログイン失敗回数。 • **log**：回数がしきい値を超えた場合、syslog 認証は失敗します。
ステップ 5	**exit***threshold-rate***log** 例： `Router(config)# exit`	コンフィギュレーション モードを終了して、特権 EXEC 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 6	**showautosecureconfig** 例： `Router# show auto secure config`	（任意）AutoSecure の設定の過程で追加されたコンフィギュレーション コマンドをすべて表示します。

AutoSecure の設定例

AutoSecure ダイアログの例を次に示します。**autosecure** コマンドを実行すると、下記のようなダイアログが自動的に表示されます。ただし、**no-interact** キーワードを指定した場合を除きます。（ディセーブルになっているサービスと、イネーブルになっている機能については、このマニュアルの「管理プレーンのセキュリティ保護, （76 ページ）」および「フォワーディング プレーンのセキュリティ保護, （80 ページ）」を参照してください）。

```
Router# auto secure
                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of the router but it will not make router
 absolutely secure from all security attacks ***
All the configuration done as part of AutoSecure will be shown here. For more details of
why and how this configuration is useful, and any possible side effects, please refer to
Cisco documentation of AutoSecure.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
Gathering information about the router for AutoSecure
Is this router connected to internet? [no]:y
Enter the number of interfaces facing internet [1]:
Interface                  IP-Address OK? Method Status
Protocol
FastEthernet0/1/0          10.1.1.1  YES NVRAM  up down
FastEthernet1/0/0            10.2.2.2  YES NVRAM  up down
FastEthernet1/1/0            10.0.0.1  YES NVRAM  up up
Loopback0                  unassigned YES NVRAM  up up
FastEthernet0/0/0            10.0.0.2  YES NVRAM  up down
Enter the interface name that is facing internet:FastEthernet0/0/0
Securing Management plane services..
Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Enable secret is either not configured or is same as enable password
Enter the new enable secret:abc123
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport
Configure SSH server? [yes]:
Enter the domain-name:example.com
Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:
```

```
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces
Securing Forwarding plane services..
Enabling CEF (it might have more memory requirements on some low end
platforms)
Enabling unicast rpf on all interfaces connected to internet
Configure CBAC Firewall feature? [yes/no]:yes
This is the configuration generated:
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
ip domain-name example.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet1/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet1/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
```

```
 no ip mask-reply
 no mop enabled
interface FastEthernet0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
ip cef
interface FastEthernet0/0/0
 ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0/0
 ip inspect autosec_inspect out
 ip access-group 100 in
!
end
Apply this configuration to running-config? [yes]:yes
Applying the config generated to running-config
The name for the keys will be:ios210.example.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys ...[OK]
Router#
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
『Configuring SNMP Support』	『Configuring SNMP Support』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

規格	タイトル
PacketCable™ コントロール ポイント検出インターフェイス仕様	『*PacketCable™ Control Point Discovery Interface Specification*』（PKT-SP-CPD-I02-061013）

MIB

MIB	MIB のリンク
• CISCO-802-TAP-MIB • CISCO-IP-TAP-MIB • CISCO-MOBILITY-TAP-MIB • CISCO-TAP2-MIB • CISCO-USER-CONNECTION-TAP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC-2865	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC-3576	「*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*」
RFC-3924	『*Cisco Architecture for Lawful Intercept in IP Networks*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

AutoSecure に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 4：*AutoSecure* に関する機能情報

機能名	リリース	機能情報
AutoSecure の管理性	Cisco IOS XE Release 2.3	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 単一のコマンドラインインターフェイス（CLI）を使用することで、AutoSecure 機能ではユーザは次の機能を実行することができます。 • ネットワーク攻撃のために不正利用される可能性のある、一般的な IP サービスをディセーブルする。 • 攻撃を受けたときにネットワークの防御を支援できる IP サービスと機能をイネーブルにする。 この機能は、ルータのセキュリティ設定を簡素化し、ルータの設定も強化します。 次のコマンドが導入または変更されました。**autosecure** および **showautosecureconfig**。

第 6 章

Kerberos の設定

- 機能情報の確認，89 ページ
- Kerberos に関する情報，89 ページ
- Kerberos を設定する方法，94 ページ
- Kerberos 設定の例，103 ページ
- その他の参考資料，104 ページ
- Kerberos の設定に関する機能情報，106 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Kerberos に関する情報

Kerberos は、マサチューセッツ工科大学（MIT）が開発した秘密キーネットワーク認証プロトコルであり、暗号化と認証にデータ暗号規格（DES）暗号アルゴリズムを使用します。Kerberos は、ネットワーク リソースの要求を認証するために設計されました。Kerberos は他の秘密キー システムと同様に、ユーザとサービスのセキュアな検証を実行する、信頼できるサード パーティの概念に基づいています。Kerberos プロトコルでは、この信頼できるサード パーティは、キー発行局（KDC）と呼ばれます。

Kerberos の主な用途は、ユーザと、そのユーザが使用するネットワーク サービスの身元が主張どおりであることを検証することです。この検証のために、信頼できる Kerberos サーバがユーザにチケットを発行します。有効期限のあるこれらのチケットは、ユーザの認定証キャッシュに保存されており、標準のユーザ名とパスワードの認証メカニズムの代わりに使用できます。

Kerberos の認定証スキームは、「シングル ログイン」という概念を表しています。この手順では、ユーザを 1 回認証することが必要で、ユーザ クレデンシャルが有効な間は（他のパスワードの暗号化を行わずに）セキュア認証が可能になります。

Cisco IOS XE ソフトウェアは Kerberos 5 をサポートするようになりました。そのため、Kerberos 5 をすでに配置している組織の場合、ルータ上で、他のネットワーク ホスト（UNIX サーバや PC など）ですでに使用している同じ Kerberos 認証データベースを使用できます。

次のネットワーク サービスは、Cisco IOS XE ソフトウェアの Kerberos 認証機能によってサポートされています。

- Telnet
- rlogin
- rsh
- rcp

（注） Kerberos クライアント サポートのシスコの実装は、MIT のコードから派生した CyberSafe が開発したコードに基づいています。そのため、シスコの Kerberos 実装は、CyberSafe Challenger 製の市販 Kerberos サーバおよび無料配布されている MIT のサーバ コードとの完全互換性テストに成功しています。

一般的な Kerberos 関連の用語と定義を下表に示します。

表 5 : *Kerberos* の用語

用語	定義
認証	ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントがルータに対して認証したり、ルータが他のルータに対して認証したりすることができます。
許可	ネットワークまたはルータでユーザが持っている特権、および実行できるアクションをルータが判断する手段です。

用語	定義
クレデンシャル	認証チケット（チケット認可チケット（TGT）、サービスクレデンシャルなど）を表す総称。Kerberos クレデンシャルで、ユーザまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することを決定すると、ユーザとパスワードを再入力する代わりにそのチケットを使用できます。クレデンシャルの有効期限は、8 時間がデフォルトの設定です。
インスタンス	Kerberos プリンシパルの承認レベル ラベル。ほとんどの Kerberos プリンシパルは、user@REALM という形式です（たとえば、smith@EXAMPLE.COM）。Kerberos インスタンスを指定した Kerberos プリンシパルは、user/instance@REALM という形式です（たとえば、smith/admin@EXAMPLE.COM）。Kerberos インスタンスは、認証が成功した場合のユーザの承認レベルを指定するために使用できます。Kerberos インスタンスの認可マッピングを実装および実施するのは、各ネットワーク サービスのサーバ次第です。Kerberos レルム名は、大文字で指定する必要があります。
Kerberos 対応	Kerberos 証明書の基盤をサポートするように変更されたアプリケーションおよびサービス。
Kerberos レルム	Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバを信頼して、ユーザまたはネットワーク サービスに対する別のユーザまたはネットワーク サービスの ID を検証します。Kerberos レルムは、常に大文字にする必要があります。
Kerberos サーバ	ネットワーク ホスト上で稼働しているデーモン。ユーザおよびネットワーク サービスはそれぞれ Kerberos サーバに ID を登録します。ネットワーク サービスは Kerberos サーバにクエリーを送信して、他のネットワーク サービスの認証を得ます。

用語	定義
キー発行局（KDC）	ネットワーク ホストで実行される Kerberos サーバとデータベース プログラム。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。
サービス認定証	ネットワーク サービスのクレデンシャル。この認定証は、KDC から発行されるとき、ネットワーク サービスと KDC で共有されるパスワード、およびユーザの TGT で暗号化されます。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。ネットワーク サービスは、SRVTAB（別名 KEYTAB）を使用することにより、暗号化されたサービス証明書を認証して解読します。
チケット認可チケット（TGT）	キー発行局（KDC）が認証済みユーザに発行する認定証。TGT を受け取ったユーザは、KDC が示した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。

Kerberos クライアントのサポート操作

ここでは、Kerberos セキュリティ システムが、セキュリティ サーバとして機能する Cisco ルータと連携する方法について説明します。（便宜上または技術的な理由から）Kerberos は多様な方法でカスタマイズできますが、ネットワーク サービスにアクセスを試みるリモート ユーザは、3 レイヤのセキュリティを通過してからネットワーク サービスにアクセスする必要があります。

境界ルータに対する認証

ここでは、リモート ユーザがネットワークにアクセスを試みるときに通過する必要があるセキュリティの第 1 レイヤについて説明します。Kerberos 認証プロセスの第 1 段階は、ユーザが境界ルータに対して自身を認証することです。次のプロセスでは、ユーザが境界ルータに対して認証する方法について説明します。

1. リモート ユーザは、会社サイトのルータに対して PPP 接続を開きます。
2. ルータは、ユーザに対してユーザ名とパスワードの入力を求めます。
3. ルータは、そのユーザに関する KDC の TGT を要求します。

4 KDC は、（他の情報も含まれますが）ユーザの ID を含む暗号化済み TGT をルータに送信します。

5 ルータは、ユーザが入力したパスワードを使用して、TGT の復号化を試行します。復号化に成功すると、リモート ユーザはルータに対して認証されます。

PPP セッションの開始、および境界ルータに対する認証に成功するリモート ユーザは、ファイアウォール内にいますが、ネットワーク サービスにアクセスするには KDC に対して直接認証する必要があります。これは、KDC から発行された TGT はルータに保存され、ユーザが物理的にルータにログインしない限り、追加の認証には役立ちません。

KDC からの TGT の取得

ここでは、境界ルータに対して認証されたリモートユーザが、KDC に対して自身を認証する方法について説明します。

リモート ユーザが境界ルータに対して認証すると、そのユーザは技術的にはネットワークの一部になります。つまり、ネットワークは、そのリモート ユーザとユーザのマシンまたはネットワークを含むように拡張されます。ただし、リモートユーザがネットワーク サービスに対するアクセス権を得るには、KDC から TGT を取得する必要があります。次のプロセスでは、リモート ユーザが KDC に対して認証する方法について説明します。

1 リモート サイトにあるワークステーションを使用するリモート ユーザは、KINIT プログラム（Kerberos プロトコルに付属するクライアント ソフトウェアの一部）を起動します。

2 KINIT プログラムは、ユーザの ID を検索し、KDC から TGT を要求します。

3 KDC は TGT を作成します。TGT には、ユーザの ID、KDC の ID、および TGT の有効期限が含まれます。

4 KDC は、ユーザのパスワードをキーとして使用して、TGT を暗号化し、その TGT をワークステーションに送信します。

5 KINIT プログラムは暗号化された TGT を受信すると、ユーザにパスワード（KDC でそのユーザ用に定義されているパスワード）の入力を求めます。

6 ユーザが入力したパスワードを使用して KINIT プログラムが TGT を復号化できる場合、ユーザは KDC に対して認証され、KINIT プログラムはユーザの認定証キャッシュに TGT を保存します。

この時点で、ユーザは TGT を持っており、KDC と安全に通信できます。次に、TGT によってユーザは他のネットワーク サービスに対して認証することができます。

ネットワーク サービスに対する認証の取得

次のプロセスでは、TGT を持つリモートユーザが、特定の Kerberos レルム内でネットワーク サービスに対して認証する方法について説明します。ここでは、ユーザはリモート ワークステーション（Host A）上にあり、Host B にログインしようとしているとします。

1. Host A 上のユーザは、Host B に対して Kerberos 化アプリケーション（Telnet など）を開始します。
2. Kerberos 化アプリケーションはサービス認定証要求を構築し、KDC に送信します。サービス認定証要求には、（他の情報も含まれますが）ユーザの ID と目的のネットワーク サービスの ID が含まれます。TGT は、サービス認定証要求を暗号化するために使用されます。
3. KDC は、Host A 上のユーザに対して発行された TGT を使用して、サービス認定証要求を復号化しようとします。KDC がパケットを復号化できる場合、要求の発行元が Host A 上の認証済みユーザであると確認されます。
4. KDC は、サービス認定証要求に含まれるネットワーク サービス ID を記録します。
5. KDC は、Host A 上のユーザの代理で、適切なネットワーク サービスのサービス認定証を Host B に構築します。サービス認定証には、クライアントの ID および必要なネットワーク サービスの ID が含まれます。
6. 次に、KDC はサービス認定証の暗号化を 2 回実行します。まず、認定証に指定されたネットワーク サービスと共有する SRVTAB を使用して認定証を暗号化します。次に、ユーザ（この場合は Host A 上のユーザ）の TGT を使用して結果のパケットを暗号化します。
7. KDC は、2 回暗号化された認定証を Host A に送信します。
8. Host A は、ユーザの TGT を使用してサービス認定証の復号化を試行します。Host A がサービス認定証を復号化できる場合、その認定証の発行元が KDC であると確認されます。
9. Host A はサービス認定証を目的のネットワーク サービスに送信します。認定証は、まだ KDC とネットワーク サービスに共有されている SRVTAB で暗号化されています。
10. ネットワーク サービスは、SRVTAB を使用してサービス認定証の復号化を試行します。
11. ネットワーク サービスが認定証を復号化できる場合、その認定証の発行元が KDC であると確認されます。ネットワーク サービスは、ユーザから間接的に送信されたデータでも、KDC から送信された復号化できるデータであれば、常に信頼します。これは、ユーザがまず KDC で認証されているためです。

この時点で、ユーザは Host B のネットワーク サービスに認証されます。このプロセスは、ユーザが Kerberos レルムのネットワーク サービスにアクセスするときは毎回繰り返されます。

Kerberos を設定する方法

通信と相互認証を行う Kerberos レルムのホストと KDC について、相互に識別する必要があります。そのために、KDC 上の Kerberos データベースにホストのエントリを追加し、KDC が生成する SRVTAB ファイルを Kerberos レルムのすべてのホストに追加します。また、KDC データベースにユーザのエントリも作成します。

ここでは、Kerberos 認証済みのサーバ クライアント システムを設定する方法について説明します。内容は次のとおりです。

このセクションは、KDC 認識された UNIX ホストで Kerberos 管理プログラムをインストールし、データベースを初期化して、Kerberos レルム名とパスワードを選択していることを前提とします。

これらのタスクの実行に関する手順については、Kerberos ソフトウェアに付属のマニュアルを参照してください。

（注） KDC のホスト名または IP アドレス、KDC で照会のために監視するポート番号、およびサービスを提供する Kerberos レルムの名前を書き留めます。この情報は、ルータの設定で必要になります。

Kerberos コマンドによる KDC の設定

Kerberos レルムで KDC として動作するようにホストを設定した後は、レルムのすべてのプリンシパルの KDC データベースに対してエントリを作成する必要があります。プリンシパルは、Cisco ルータおよびホスト上のネットワーク サービスの場合、またはユーザの場合があります。

Kerberos コマンドで KDC データベースにサービスを追加するには（また、既存のデータベース情報を変更するには）、以下の項のタスクを実行します。

（注） すべての Kerberos コマンド例は、オリジナルの MIT 実装の Kerberos 5 Beta 5 に基づいています。それよりも新しいバージョンでは、やや異なるインターフェイスを使用しています。

KDC データベースへのユーザの追加

KDC にユーザを追加し、そのユーザの特権インスタンスを作成するには、KDC を実行するホストのルートになるために **su** コマンドを実行します。また、kdb5_edit プログラムを使用して、特権 EXEC モードで次のコマンドを使用します。

手順の概要

1. Router# **ank***username@REALM*
2. Router# **ank***username/instance@REALM*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router# **ank***username@REALM*	**ank**（新しいキーを追加）コマンドを使用して、ユーザを KDC に追加します。このコマンドを実行するとパスワードの入力が求められ、ユーザはルータに対して認証するために入力する必要があります。

	コマンドまたはアクション	目的
ステップ 2	Router# **ank***username/instance@REALM*	**ank** コマンドを使用して、ユーザの特権インスタンスを追加します。

次の作業

たとえば、Kerberos レルム CISCO.COM のユーザ *loki* を追加するには、次の Kerberos コマンドを入力します。

```
ank loki@CISCO.COM
```

（注） Kerberos レルム名は、大文字で指定する必要があります。

ネットワーク管理がイネーブル レベルでルータに接続できるように、特権インスタンスを作成できます。たとえば、イネーブル モードを開始するためにクリア テキスト パスワードを入力する（またセキュリティを脅かす）必要がないようにできます。

新しい特権（この場合 enable ですが、任意に指定できます）を使用して *loki* のインスタンスを追加するには、次の Kerberos コマンドを入力します。

```
ank loki/enable@CISCO.COM
```

以下の各例では、パスワードの入力が求められます。このパスワードは、ユーザ *loki* がログイン時に使用できるように、ユーザに付与する必要があります。

「Kerberos インスタンス マッピングのイネーブル化, （102 ページ）」では、Kerberos インスタンスを多様な Cisco IOS XE 特権レベルにマッピングする方法について説明します。

KDC での SRVTAB の作成

Kerberos プロトコルを使用するために認証するすべてのルータは、SRVTAB を持っている必要があります。この項および「SRVTAB の抽出, （97 ページ）」では、*router1* というルータの SRVTAB を作成し抽出する方法について説明します。「SRVTAB ファイルのコピー, （99 ページ）」では、SRVTAB ファイルをルータにコピーする方法について説明します。

KDC に SRVTAB エントリを作成するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **ark** *SERVICE/HOSTNAME@REALM*	**ark**（add random key）コマンドを使用して、ホストまたはルータがサポートするネットワーク サービスを KDC に追加します。

たとえば、*router1* という Cisco ルータ用の Kerberos 化認証サービスを Kerberos レルム CISCO.COM に追加するには、次の Kerberos コマンドを入力します。

```
ark host/router1.cisco.com@CISCO.COM
```

すべての Kerberos 化ホスト上に、認証にこの KDC を使用するすべてのネットワーク サービスに関するエントリを作成します。

SRVTAB の抽出

SRVTAB には、（他の情報も含まれますが）KDC データベースに入力したサービス プリンシパルのパスワードまたはランダムに生成されたキーが含まれます。サービスプリンシパルキーは、そのサービスを実行するホストと共有する必要があります。そのためには、SRVTAB をファイルに保存し、Kerberos レルムにあるルータおよびすべてのホストにそのファイルをコピーします。SRVTAB エントリをファイルに保存することを、SRVTAB の抽出といいます。SRVTAB を抽出するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# xst router-name host`	Kdb5_edit コマンド **xst** を使用して、SRVTAB エントリをファイルに書き込みます。

たとえば、host/router1.cisco.com@CISCO.COM SRVTAB をファイルに書き込むには、次の Kerberos コマンドを入力します。

```
xst router1.cisco.com@CISCO.COM host
```

quit コマンドを使用して、kdb5_edit プログラムを終了します。

Kerberos プロトコルを使用するルータの設定

Kerberos レルムの定義

ルータが、Kerberos データベースに定義されているユーザを認証するには、KDC を実行するホストのホスト名または IP アドレスと Kerberos レルムの名前を知っている必要があります。また、オプションで、ホスト名またはドメイン ネーム システム（DNS）ドメインを Kerberos レルムにマッピングする機能がルータに必要です。

特定の Kerberos レルムで、指定した KDC に対して認証するようにルータを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。DNS ドメイン名の先頭にはドット（.）を付ける必要があります。

手順の概要

1. Router(config)# **kerberoslocal-realm***kerberos-realm*
2. Router(config)# **kerberosserver***kerberos-realm* {*hostname* | *ip-address* } [*port-number*]
3. Router(config)# **kerberosrealm** {*dns-domain* | *host* } *kerberos-realm*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **kerberoslocal-realm***kerberos-realm*	ルータのデフォルト レルムを定義します。
ステップ 2	Router(config)# **kerberosserver***kerberos-realm* {*hostname* | *ip-address* } [*port-number*]	特定の Kerberos レルムで使用する KDC、およびオプションで KDC が監視するポート番号をルータに指定します（デフォルト値は 88 です）。
ステップ 3	Router(config)# **kerberosrealm** {*dns-domain* | *host* } *kerberos-realm*	（任意）ホスト名または DNS ドメインを Kerberos レルムにマッピングします。

次の作業

（注） KDC を実行するマシンおよびすべての Kerberos 化ホストは 5 分の期限内で通信する必要があり、通信できない場合、認証は失敗します。そのため、すべての Kerberos 化マシン（特に KDC）は、ネットワーク タイム プロトコル（NTP）を実行する必要があります。

kerberoslocal-realm、**kerberosrealm**、および **kerberosserver** の各コマンドは、UNIX の krb.conf ファイルと同等です。下記の表は、Cisco IOS XE コンフィギュレーション コマンドから Kerberos 5 コンフィギュレーション ファイル（krb5.conf）への対応一覧です。

表 *6* : ***Kerberos 5*** のコンフィギュレーション ファイルおよびコマンド

krb5.conf ファイル	**Cisco IOS XE** のコンフィギュレーション コマンド
[libdefaults] `default_realm = DOMAIN.COM`	（コンフィギュレーション モードで） **`kerberos local-realm`** *`DOMAIN.COM`*

krb5.conf ファイル	Cisco IOS XE のコンフィギュレーション コマンド

[domain_realm]
 	
`.domain.com = DOMAIN.COM`
 	
`domain.com = DOMAIN.COM`
	（コンフィギュレーション モードで）
	
	kerberos realm *.domain.com DOMAIN.COM*
	kerberos realm *domain.com DOMAIN.COM*

[realms]
 	
`kdc = DOMAIN.PIL.COM:750`
 	
`admin_server = DOMAIN.PIL.COM`
 	
`default_domain = DOMAIN.COM`
	（コンフィギュレーション モードで）
	
	kerberos server *DOMAIN.COM 172.65.44.2*
	(*172.65.44.2* is the example IP address for *DOMAIN.PIL.COM*)

Kerberos レルムの定義例については、Kerberos レルムの定義例のモジュールを参照してください。

SRVTAB ファイルのコピー

リモート ユーザが Kerberos 認定証を使用してルータに対して認証できるようにするには、ルータが KDC 秘密キーを共有する必要があります。そのためには、KDC で抽出した SRVTAB をルータにコピーする必要があります。

SRVTAB ファイルを Kerberos レルムのホストにコピーする最もセキュアな方式は、ファイルを物理メディアにコピーし、各ホストの場所に行き、そのシステムに手動でファイルをコピーすることです。ルータに物理メディア ドライバがない場合、SRVTAB ファイルをルータにコピーするには、TFTP を使用してネットワークを介して転送する必要があります。

KDC からルータに対して SRVTAB ファイルをリモート コピーするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)#` **kerberos srvtab remote** {*hostname* | *ip-address*} {*filename*}	KDC から SRVTAB ファイルを取得します。

SRVTAB ファイルをルータから KDC にコピーする場合、**kerberos srvtab remote** コマンドでこのファイルの情報を分析し、**kerberos srvtab entry** 形式でルータの実行コンフィギュレーションに保存します。ルータをリブートしたときに SRVTAB が使用できるようにするには（KDC から取得する必要はありません）、**write memory** コンフィギュレーション コマンドを使用し、実行コンフィギュレーション（分析した SRVTAB ファイルを含みます）を NVRAM に書き込みます。

SRVTAB ファイルのコピー例については、「SRVTAB ファイルのコピー例, （104 ページ）」を参照してください。

Kerberos 認証の指定

これまでの操作でルータの Kerberos の設定が完了しました。そのため、ルータは Kerberos を使用して認証できます。次の手順は、認証するようにルータに指示することです。AAA によって Kerberos 認証が容易になるため、**aaa authentication** コマンドを入力し、認証方式として Kerberos を指定する必要があります。詳細については、「認証の設定」の章を参照してください。

認定証転送のイネーブル化

これまでの手順で Kerberos を設定すると、Kerberos 化ルータに対して認証されているユーザは TGT を持ち、その TGT を使用してネットワーク上のホストに対して認証できます。ただし、ユーザがホストの認証後に認定証のリストを表示しようとすると、出力には Kerberos 認定証が表示されません。

Kerberos 化された Telnet、rcp、rsh、および rlogin（適切なフラグ付き）を使用するときに、ルータからネットワーク上の Kerberos 化リモート ホストに対して認証する場合、オプションで、ユーザの TGT を転送するようにルータを設定できます。

Kerberos レルムで他のホストに接続するときにユーザの認定証を転送するように、すべてのクライアントに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)#` **kerberos credentials forward**	Kerberos 認証に成功したときに、すべてのクライアントがユーザの認定証を転送するように強制します。

認定証の転送をイネーブルにすると、ユーザの TGT は、認証を受ける次のホストへ自動的に転送されます。この方法で、ユーザは Kerberos レルム内の複数のホストに接続できます。新しい TGT を取得するたびに KINIT プログラムを実行する必要はありません。

ルータに対する Telnet セッションの開始

ネットワーク内からルータに対して Telnet セッションを開始するユーザを認証するために、Kerberos を使用するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)#` **aaa authentication login** {**default** | *list-name*} **krb5_telnet**	Telnet を使用してルータに接続する場合、ログイン認証を設定して Kerberos 5 Telnet 認証プロトコルを使用します。

ルータに対する Telnet セッションは認証されますが、イネーブル モードを開始するには、ユーザがクリア テキスト パスワードを入力する必要があります。後述する **kerberos instance map** コマンドを使用すると、事前に定義した特権レベルでルータに対して認証できます。

暗号化された Kerberos 対応 Telnet セッションの確立

ユーザがセキュア Telnet セッションを開始するもう 1 つの方法は、Encrypted Kerberized Telnet を使用することです。Encrypted Kerberized Telnet を使用すると、Telnet セッションを確立する前に、ユーザは Kerberos 認定証によって認証されます。Telnet セッションは、64-bit Cipher Feedback（CFB）による 56-bit データ暗号規格（DES）暗号を使用して暗号化されます。送受信データは暗号化され、クリアテキストではないため、着信したルータまたはアクセス サーバの整合性は制御しやすくなります。

（注） この機能を使用できるのは、56-bit 暗号化イメージを持っている場合だけです。56 ビット DES 暗号化は、米国政府の輸出管理規制の対象となります。

ルータからリモート ホストに対して、Encrypted Kerberized Telnet セッションを確立するには、EXEC コンフィギュレーション モードで次のコマンドのいずれかを使用します。

コマンド	目的
`Router(config)#` **connect** *host* [*port*] **/encrypt kerberos** または `Router(config)#` **telnet** *host* [*port*] **/encrypt kerberos**	暗号化された Telnet セッションを確立します。

ユーザが Cisco ルータからリモート ホストに対する Telnet セッションを開始すると、ルータとリモート ホストは、Kerberos 認定証を使用してユーザを認証するためにネゴシエートします。この認証に成功すると、ルータとリモート ホストは、暗号化を使用するかどうかをネゴシエートします。このネゴシエーションに成功すると、着信および発信トラフィックは、64-bit CFB による 56-bit DES を使用して暗号化されます。

ユーザが、リモート ホストから Kerberos 認証用に設定された Cisco ルータに対してダイヤルインすると、Telnet セッションに暗号化を使用するかどうかについて、ホストとルータでネゴシエーションが試行されます。このネゴシエーションに成功すると、ルータは Telnet セッション中のすべての発信データを暗号化します。

暗号化のネゴシエーションに成功しなかった場合、セッションは終了し、ユーザは、暗号化された Telnet セッションの確立に失敗したというメッセージを受信します。

リモート ホストから双方向暗号化をイネーブル化する方法については、リモート ホスト デバイスのマニュアルを参照してください。

暗号化された Kerberos 対応 Telnet を使用してセキュアな Telnet セッションを開始する例については、この章で後述する「暗号化された Telnet セッションの例, （104 ページ）」を参照してください。

必須の Kerberos 認証のイネーブル化

セキュリティの追加レイヤとして、リモート ユーザがルータに対して認証した後に、ユーザは Kerberos 化 Telnet、rlogin、rsh、および rcp だけを使用してネットワーク上の他のサービスに対して認証できます。Kerberos 認証を必須にしていない状態で Kerberos 認証に失敗すると、アプリケーションは、そのネットワーク サービスのデフォルト認証方式を使用して、ユーザの認証を試行します。たとえば、Telnet および rlogin はパスワードの入力を求め、rsh はローカル rhost ファイルを使用して認証を試行します。

Kerberos 認証を必須にするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)#` **kerberos clients mandatory**	リモート ホストとの間で Kerberos プロトコルをネゴシエートできない場合、Telnet、rlogin、rsh、および rcp を失敗に設定します。

Kerberos インスタンス マッピングのイネーブル化

「KDC での SRVTAB の作成, （96 ページ）」で説明したように、KDC データベースにユーザの管理インスタンスを作成することができます。**kerberos instance map** コマンドを使用すると、その管理インスタンスを Cisco IOS XE 特権レベルにマッピングできます。それによって、事前定義した特権レベルで、ユーザはルータに対するセキュア Telnet セッションを開くことができます。イネーブルモードを開始するためにクリアテキストのパスワードを入力する必要はありません。

Kerberos インスタンスを Cisco IOS XE 特権レベルにマッピングするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)#` **kerberos instance map** *instance privilege-level*	Kerberos インスタンスを Cisco IOS XE 特権レベルにマッピングします。

KDC データベースにユーザ *loki*（たとえば、*loki/admin*）の Kerberos インスタンスがある場合、ユーザ *loki* は、loki/admin としてルータに対して Telnet セッションを開始し、特権レベル 15 で自動的に認証します。インスタンス「admin」は特権レベル 15 にマッピングされるという前提です。（「ルータに対する Telnet セッションの開始, （100 ページ）」を参照してください）。

Cisco IOS XE コマンドを多様な特権レベルに設定するには、**privilege level** コマンドを使用します。

Cisco IOS XE の特権レベルに Kerberos インスタンスをマッピングした後は、ユーザがログインするたびに Kerberos インスタンスをチェックするようにルータを設定する必要があります。ユーザがマッピングされた Kerberos インスタンスに基づいた EXEC シェルの実行を許可されているかどうかを判断する認可を実行するには、**krb5-instance** キーワードを使用して **aaa authorization** コマンドを使用します。詳細については、「認可の設定」の章を参照してください。

Kerberos の監視とメンテナンス

現在のユーザの認定証を表示または削除するには、EXEC モードで次のコマンドを使用します。

手順の概要

1. Router# **show kerberos creds**
2. Router# **clear kerberos creds**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router# **show kerberos creds**	現在のユーザの認定証キャッシュに含まれる認定証を一覧表示します。
ステップ 2	Router# **clear kerberos creds**	転送済みの認定証を含め、現在のユーザの認定証キャッシュに含まれるすべての認定証を破棄します。

Kerberos 設定の例

Kerberos レルムの定義例

デフォルトの Kerberos レルムとして CISCO.COM を定義するには、次のコマンドを使用します。

```
kerberos local-realm CISCO.COM
```

CISCO.COM KDC が、ホスト 10.2.3.4 でポート番号 170 を使用して実行されていることをルータに示すには、次の Kerberos コマンドを使用します。

```
kerberos server CISCO.COM 10.2.3.4 170
```

DNS ドメイン cisco.com を Kerberos レルム CISCO.COM にマッピングするには、次のコマンドを使用します。

```
kerberos realm.cisco.com CISCO.COM
```

SRVTAB ファイルのコピー例

host123.cisco.com というホスト上の SRVTAB ファイルを、router1.cisco.com というルータにコピーするには、次のようなコマンドを使用します。

```
kerberos srvtab remote host123.cisco.com router1.cisco.com-new-srvtab
Valid Starting          Expires                 Service Principal
13-May-1996 14:59:44    13-May-1996 23:00:45    krbtgt/CISCO.COM@CISCO.COM
chet-2500# show privilege
Current privilege level is 15
chet-2500# q
Connection closed by foreign host.
chet-ss20% telnet chet-2500
Trying 172.16.0.0 ...
Connected to chet-2500.cisco.com.
Escape character is '^]'.
User Access Verification
Username: chet/restricted
Password:
chet-2500# show kerberos creds
Default Principal:  chet/restricted@CISCO.COM
Valid Starting          Expires                 Service Principal
13-May-1996 15:00:32    13-May-1996 23:01:33    krbtgt/CISCO.COM@CISCO.COM
chet-2500# show privilege
Current privilege level is 3
chet-2500# q
Connection closed by foreign host.
chet-ss20%
```

暗号化された Telnet セッションの例

ルータから「host1」というリモート ホストに対して、暗号化された Telnet セッションを確立する例を示します。

Router> **telnet host1 /encrypt kerberos**

その他の参考資料

次の項では、No Service Password-Recovery 機能の関連資料を示します。

関連資料

関連項目	マニュアル タイトル
パスワードの設定、変更および忘失パスワードの回復	「Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices」機能モジュール
システム イメージのロードと再起動	「Using the Cisco IOS Integrated File System」機能モジュール

関連項目	マニュアル タイトル
セキュリティ 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、使用上の注意事項、および例	『*Cisco IOS Security Command Reference*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Kerberos の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *7*：***Kerberos*** の設定に関する機能情報

機能名	リリース	機能情報
暗号化された Kerberos 対応 Telnet	Cisco IOS XE Release 2.1	Encrypted Kerberized Telnet を使用すると、Telnet セッションを確立する前に、ユーザは Kerberos 認定証によって認証されます。Telnet セッションは、64-bit Cipher Feedback（CFB）による 56-bit データ暗号規格（DES）暗号を使用して暗号化されます。送受信データは暗号化され、クリア テキストではないため、着信したルータまたはアクセス サーバの整合性は制御しやすくなります。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**connect** および **telnet**。
Kerberos V クライアントのサポート	Cisco IOS XE Release 2.1	Kerberos 5 のサポートでは、Kerberos 5 をすでに配置している組織は、ルータ上で、他のネットワーク ホスト（UNIX サーバや PC など）ですでに使用している同じ Kerberos 認証データベースを使用できます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

第 7 章

合法的傍受アーキテクチャ

合法的傍受（LI）機能は、法執行機関（LEA）の要件を満たす際にサービス プロバイダーをサポートし、管轄または行政命令によって承認されている電子サーベイランスを提供します。サーベイランスは、エッジ ルータを通過する Voice over Internet Protocol（VoIP）またはデータ トラフィックを傍受するため、盗聴を利用して実行されます。LEA は、ターゲットのサービス プロバイダーに盗聴を要求します。サービス プロバイダーには、IP セッションを使用してその個人が送受信するデータ通信を傍受する責任があります。

このマニュアルでは、Cisco Service Independent Intercept アーキテクチャと PacketCable Lawful Intercept アーキテクチャを含む、LI アーキテクチャについて説明します。また、LI 機能の構成要素と、システムで LI 機能を設定するための手順についても説明します。

Cisco IOS XE リリース 2.5 以前は、PPP セッションはアカウンティング セッションに基づいてタップされました。回線 ID ベースのタッピングは、Cisco IOS XE リリース 2.5 で導入されました。

Cisco IOS XE リリース 2.6 では、ユーザ セッションはイーサネット（PPPoE）回線 ID タグを介する独自の PPP に基づいてタップされます。この回線 ID タグは、デバイスの PPPoE ユーザ セッションの固有のパラメータとして機能します。タップされたユーザ セッションは SNMP を使ってプロビジョニングされ、ユーザ セッションのデータ パケットおよび RADIUS 認証のデータ パケットはタップされます。

- 機能情報の確認，110 ページ
- 合法的傍受の前提条件，110 ページ
- 合法的傍受の制約事項，111 ページ
- 合法的傍受に関する情報，111 ページ
- 合法的傍受の設定方法，119 ページ
- 合法的傍受の設定例，130 ページ
- その他の参考資料，131 ページ
- 合法的傍受に関する機能情報，132 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

合法的傍受の前提条件

Cisco LI MIB ビューへのアクセスは、メディエーション デバイスと、ルータ上の合法的傍受について知っておく必要があるシステム管理者に制限されます。MIB にアクセスするには、ルータ上でレベル 15 のアクセス権がユーザに必要です。

メディエーション デバイスとの通信

ルータがメディエーション デバイスと通信して合法的傍受を実行するには、次の構成要件が満たされている必要があります。

- ルータとメディエーションデバイスの両方のドメイン名が、ドメインネームシステム（DNS）に登録されている必要があります。

DNS で、ルータの IP アドレスは、通常はルータ上の FastEthernet0/0/0 インターフェイスのアドレスです。

- メディエーション デバイスに Access Function（AF）および Access Function Provisioning Interface（AFPI）が必要です。
- メディエーション デバイスを、CISCO-TAP2-MIB ビューにアクセスできるシンプル ネットワーク管理プロトコル（SNMP）ユーザ グループに追加する必要があります。グループに追加するユーザとして、メディエーション デバイスのユーザ名を指定します。

メディエーション デバイスを CISCO-TAP2-MIB ユーザとして追加するときに、必要に応じてメディエーション デバイスの認可パスワードを指定できます。パスワードの長さは、最低 8 文字である必要があります。

合法的傍受の制約事項

一般的な制約事項

ルータで LI を設定するためのコマンドライン インターフェイス（CLI）はありません。すべてのエラー メッセージは、メディエーション デバイスに SNMP 通知として送信されます。すべての傍受は、SNMPv3 だけを使用してプロビジョニングされます。

合法的傍受 MIB

合法的傍受について知る必要があるメディエーション デバイスとユーザだけに LI MIB へのアクセスが許可されます。

Cisco LI MIB は、その機密性から、LI 機能をサポートしているソフトウェア イメージだけで使用できます。これらの MIB には、Network Management Software MIBs Support ページ（http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からはアクセスできません。

SNMP 通知

LI の SNMP 通知は、メディエーションデバイス上のユーザデータグラム プロトコル（UDP）ポート 161 に送信する必要があります。ポート 162（SNMP のデフォルト）ではありません。詳細については、合法的傍受のための SNMP 通知のイネーブル化,（121 ページ）を参照してください。

合法的傍受に関する情報

合法的傍受の概要

LI は、司法当局（LEA）が、司法命令または行政命令の許可に従って、電子的監視を行うためのプロセスです。ますます多くの法律が採択され、規制が施行されるのに伴い、サービス プロバイダー（SP）やインターネット サービス プロバイダー（ISP）は、許可された電子監視を明示的にサポートするネットワークを実装する必要性に迫られています。LI の指令に従う必要がある SP または ISP の種類は、国によって大きく異なります。米国での LI への準拠は、Commission on Accreditation for Law Enforcement Agencies（CALEA）で規定されています。

シスコでは、LI に対し、PacketCable と Service Independent Intercept の 2 つのアーキテクチャをサポートしています。LI コンポーネントだけでは、該当する規制に準拠できません。LI コンポーネントは、SP および ISP が、LI 準拠のネットワークを構築するために使用可能なツールを提供します。

Cisco Service Independent Intercept アーキテクチャ

『Cisco Service Independent Intercept Architecture Version 3.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 5.0 を非 PacketCable ネットワークで使用した、VoIP ネットワーク向

けの LI の実装について説明しています。Packet Cable Event Message 仕様バージョン 1.5-I01 は、コール識別情報と、コールの内容に対する Cisco Tap MIB バージョン 2.0 を提供するために使用されます。

『Cisco Service Independent Intercept Architecture Version 2.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 4.4 および 4.5 を非 PacketCable ネットワークで使用した、VoIP ネットワーク向けの LI の実装について説明しています。PacketCable ネットワークではありませんが、PacketCable Event Messages Specification バージョン I08 は、コール識別情報と、コール内容に対する Cisco Tap MIB のバージョン 1.0 またはバージョン 2.0 を提供するために引き続き使用されています。『*Cisco Service Independent Intercept Architecture Version 2.0*』では、IP アドレスとセッション ID の両方でデータを傍受するための追加機能について説明しています。これは、どちらも Cisco Tap MIB（CISCO-TAP2-MIB）のバージョン 2.0 でサポートされています。

『Cisco Service Independent Intercept Architecture Version 1.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 3.5 および 4.1 を非 PacketCable ネットワークで使用した、VoIP ネットワーク向けの LI の実装について説明しています。PacketCable ネットワークではありませんが、PacketCable Event Message Specification バージョン I03 は、コール識別情報と、コール内容に対する Cisco Tap MIB（CISCO-TAP-MIB）のバージョン 1.0 を提供するために引き続き使用されています。IP アドレスによる単純なデータの傍受についても説明されています。

PacketCable 合法的傍受アーキテクチャ

『*PacketCable Lawful Intercept Architecture for BTS Version 5.0*』では、PacketCable Event Messages Specification バージョン 1.5-I01 に準拠した PacketCable ネットワークで、Cisco BTS 10200 Softswitch コール エージェント バージョン 5.0 を使用した、VoIP 向けの LI の実装について説明しています。

『*PacketCable Lawful Intercept Architecture for BTS Versions 4.4 and 4.5*』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 4.4 および 4.5 を、PacketCable Event Messages Specification バージョン I08 に準拠した PacketCable ネットワークで使用した、VoIP 向けの LI の実装について説明しています。

『PacketCable Lawful Intercept Architecture for BTS Versions 3.5 and 4.1』では、Cisco Broadband Telephony Softswitch (BTS) 10200 Softswitch コール エージェント バージョン 3.5 および 4.1 を、PacketCable Event Message Specification バージョン I03 に準拠した PacketCable ネットワークで使用した、Voice over IP（VoIP）向けの LI の実装について説明しています。

『*PacketCable Control Point Discovery Interface Specification*』では、指定された IP アドレスのコントロール ポイントを発見するために使用可能な IP ベースのプロトコルが定義されています。コントロール ポイントとは、Quality of Service（QoS）操作、LI コンテンツ タッピング操作、その他の操作を実行可能な場所です。

CISCO ASR 1000 シリーズ ルータ

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、通常および広帯域（加入者ごと）の 2 種類の LI をサポートしています。広帯域の盗聴は、アクセス サブインターフェイスおよびトンネル インターフェイス上で実行します。通常の盗聴は、アクセス サブインターフェイス、トンネル インターフェイス、および物理インターフェイス上で実行します。内部インターフェイス上

では盗聴は不要であり、実行されません。ルータは、ターゲット トラフィックが使用しているインターフェイスに基づいて、実行する盗聴の種類を決定します。

Cisco ASR 1000 シリーズ ルータ上の LI は、次の 1 つ以上のフィールドの組み合わせに基づいてトラフィックを傍受できます。

- 宛先 IP アドレスとマスク（IPv4 または IPv6 アドレス）
- 宛先ポートまたは宛先ポートの範囲
- 送信元 IP アドレスとマスク（IPv4 または IPv6 アドレス）
- 送信元ポートまたは送信元ポート範囲
- プロトコル ID
- Type of Service（TOS）
- ルータ内で *vrf-tableid* 値に変換される Virtual Routing and Forwarding（VRF）名
- 加入者（ユーザ）接続 ID

Cisco ASR 1000 シリーズ ルータ上の LI の実装は、SNMP3 を使用してプロビジョニングされ、次の機能がサポートされています。

- RADIUS セッションは傍受し、次のいずれかの方法で実行できます。
  - アクセス許可パケットを介した傍受では、セッションの開始時に傍受が開始されるようにできます。
  - CoA 要求パケットによる傍受では、ルータがセッション中に傍受を開始または停止することができます。
- 通信内容の傍受。ルータは、傍受した各パケットを複製し、パケットのコピーを UDP ヘッダーでカプセル化されたパケットに（設定された CCCid とともに）格納します。ルータは、カプセル化したパケットを LI メディエーション デバイスに送信します。複数の合法的傍受が同じデータ フローに対して設定されている場合でも、パケットの 1 つのコピーだけメディエーション デバイスに送信されます。必要に応じて、メディエーション デバイスは各 LEA に対しパケットを複製できます。
- IPv4、IPv4 マルチキャスト、IPv6、および IPv6 マルチキャストフローの傍受。

VRF 対応 LI

VRF 対応 LI は、特定のバーチャル プライベート ネットワーク（VPN）での IPv4 データの LI 盗聴をプロビジョニングする機能です。この機能により、LEA は、その VPN 内のターゲット データを合法的に傍受できます。VRF ベースの LI タップを受けるのは、その VPN 内の IPv4 データのみです。

VRF 対応の LI は、次の種類のトラフィックに対して使用できます。

- ip2ip

- ip2tag（IP から MPLS）
- tag2ip（MPLS から IP）

VPN ベースの IPv4 タップをプロビジョニングするために、LI 管理機能（メディエーション デバイスで動作します）は、CISCO-IP-TAP-MIB を使用して、ターゲットの VPN が使用している VRF テーブルの名前を特定します。VRF 名は、タップを実行するために LI をイネーブルにする VPN インターフェイスを選択するのに使用します。

ルータは、傍受するトラフィックと、傍受したパケットを送信するメディエーション デバイスを、VRF 名（および送信元および宛先アドレス、送信元および宛先ポート、およびプロトコル）に基づいて決定します。

（注） Cisco-IP-TAP-MIB を使用する場合、VRF 名がストリーム エントリで指定されていない場合、デフォルトでグローバル IP ルーティング テーブルが使用されます。

合法的傍受 MIB

Cisco LI MIB は、その機密性から、LI 機能をサポートしているソフトウェア イメージだけで使用できます。これらの MIB には、Network Management Software MIBs Support ページ（http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からはアクセスできません。

合法的傍受 MIB へのアクセスの制限

合法的傍受について知る必要があるメディエーション デバイスとユーザだけに LI MIB へのアクセスを許可する必要があります。これらの MIB へのアクセスを制限するには、次の作業を実行する必要があります。

1. Cisco LI MIB を含むビューを作成します。
2. このビューへの読み取りおよび書き込みアクセス権を持つ SNMP ユーザ グループを作成します。このユーザ グループに割り当てられたユーザだけが、MIB の情報にアクセスできます。
3. ユーザをシスコ LI ユーザ グループに追加し、合法的傍受に関連する MIB および情報にアクセスできるユーザを定義します。このグループのユーザとして、メディエーションデバイスを追加してください。追加しないと、ルータで合法的傍受を実行できません。

詳細は、「合法的傍受 MIB の制限付き SNMP ビューの作成」を参照してください。

（注） Cisco LI MIB ビューへのアクセスは、メディエーション デバイスと、ルータ上の合法的傍受について知っておく必要があるシステム管理者に制限されます。MIB にアクセスするには、ルータ上でレベル 15 のアクセス権がユーザに必要です。

RADIUS ベースの合法的傍受

RADIUS ベースの合法的傍受ソリューションを使用すると、傍受要求は RADIUS サーバからネットワーク アクセス サーバ（NAS ）またはレイヤ 2 トンネル プロトコル アクセス コンセントレータ（LAC）に（アクセス許可パケットまたは認可変更（CoA）要求パケットを介して）送信されるようになります。PPP または L2TP セッションとやり取りされるすべてのトラフィック データは、仲介デバイスに渡されます。RADIUS ベースの合法的傍受のもう 1 つの利点は、ソリューションの同期です。すべてのターゲット トラフィックを傍受するように、タップはアクセス許可パケットで設定されます。

傍受要求は、SNMPv3 メッセージによって仲介デバイスで開始されるため、特定の IP アドレスから送受信されるすべてのトラフィック データは仲介デバイスに渡されます。IP アドレスに基づいた傍受は、IP アドレスがセッションに割り当てられるまでセッションがタップされるのを防ぎます。

RADIUS ベースの合法的傍受機能は、次のモードの合法的傍受にハイ アベイラビリティ（HA）サポートを提供します。

- 新しいセッションのアクセス許可ベースの LI
- 既存のセッションの CoA ベースの LI

RADIUS ベースの LI HA は、RADIUS ベースのプロビジョニングのみをサポートします。SNMP ベースのプロビジョニングはサポートされません。

傍受の動作

傍受要求がアクセス許可パケット内で動作するしくみ

傍受ターゲットが接続の確立を開始するとき、アクセス要求パケットは RADIUS サーバに送信されます。RADIUS サーバは、4 つの RADIUS 属性を含むアクセス許可パケットで応答します。

NAS または LAC は値 1 の LI-Action 属性を受け取り、新しいセッションの開始時に NAS または LAC でトラフィック データを複製できるようにします。また、属性、MD IP アドレス、および MD ポート番号を通して指定された仲介デバイスに複製されたデータを転送できるようにします。

（注） NAS または LAC が新しいセッションのトラフィック データの傍受を開始することができなければ、セッションは確立されません。

アカウンティングが（**aaaaccountingnetwork** コマンドおよび **aaaaccountingsendstop-recordauthenticationfailure** コマンドを介して）イネーブル化されると、アカウンティング停止パケットは、Acct-Termination-Cause 属性（49）が 15 に設定されて送信される必要があります。つまり、サービスは利用できないということです。

傍受要求が CoA 要求パケット内で動作するしくみ

セッションが傍受ターゲットに対して確立された後、次のタスクに CoA 要求パケットを使用できます。

- 既存のセッションの傍受の開始。LI-Action の属性は 1 に設定されます。
- 既存のセッションの傍受の停止。LI-Action の属性は 0 に設定されます。
- ダミーの傍受要求の発行。LI-Action の属性は 2 に設定されます。NAS または LAC は、どのセッションの傍受も実行することはできません。代わりに、CoA 要求パケットで指定されている Acct-Session-Id 属性値に基づいてセッションを検索します。セッションが存在すると、NAS または LAC は RADIUS サーバへ CoA の確認応答（ACK）を送信します。セッションがなければ、NAS または LAC は「セッションが見つかりません」のエラー メッセージを発行します。

各ケースで RADIUS サーバは、特定の属性と Acct-Session-Id 属性の CoA 要求パケットを送信する必要があります。これらの属性はそれぞれ、パケットである必要があります。

Acct-Session-Id 属性は傍受されるセッションを識別します。Acct-Session-Id 属性は、アクセス要求パケットまたはアカウンティング停止パケットから取得できます。

セッションがタップされセッションが終了すると、タップが停止します。アクセス許可が開始タップを示すか、CoA 要求がセッションを開始するように送信されることを示さない限り、加入者のログが戻るときにセッションは開始されません。

（注） CoA 要求パケットの頻度は、10 分ごとに 1 つの要求のレートを超えることはありません。

Service Independent Intercept（SII）

シスコでは、サービス プロバイダー カスタマーの合法的傍受のサポート要件に対応するため、Service Independent Intercept（SII）アーキテクチャを開発しました。SII アーキテクチャは、コンテンツの傍受アクセス ポイント（IAP）として機能するシスコ機器とメディエーション デバイス間に、明確に定義されたオープン インターフェイスを提供します。SII アーキテクチャのモジュラ特性により、サービス プロバイダーは、特定のネットワーク要件と警察当局の収集機能へのインターフェイスに対する地域的な標準ベースの要件とを満たす最適なメディエーション デバイスを選択できます。

メディエーション デバイスは SNMPv3 を使用してコール接続（CC）IAP を指示し、CC を複製してメディエーション デバイスにコンテンツを送信します。CC IAP は、エッジ ルータまたは音声のトランキング ゲートウェイのいずれか、およびエッジ ルータまたはデータのアクセス サーバのいずれかにできます。

セキュリティを強化し、SNMPv3 脆弱性を緩和するには、次のタスクが必要です。

信頼できるホストへのアクセス制限（暗号化なし）

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方をサポートします。セキュリティ モデルは、ユーザおよびユーザに属するグループに合わせて設定される認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMP パケットを処理するときに適用されるセキュリティ メカニズムが決定されます。

さらに、名前付きアクセス リストの SNMP サポート機能により、いくつかの SNMP コマンドに、標準の名前付きアクセス コントロール リスト（ACL）へのサポートが追加されます。

新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを設定するには、グローバル コンフィギュレーション モードで **snmp-servergroup** コマンドを使用します。

```
access-list my-list permit ip host 10.10.10.1
snmp-server group my-group v3 auth access my-list
```

この例では、**my-list** という名前のアクセス リストは 10.10.10.1 以降の SNMP トラフィックのみ許可します。次にこのアクセス リストは、**my-group** という名前の SNMP グループに適用されます。

合法的傍受をするトラフィックの暗号化および信頼できるホストへのアクセス制限

ルータ（コンテンツ インターセプト アクセス ポイント（IAP））と仲介デバイス（MD ）間で傍受されたトラフィックを暗号化することを強く推奨します。

次のように設定する必要があります。

- ルータの暗号化および MD の暗号化クライアント、またはトラフィックを複合化するため MD に関連付けられたルータを設定します。
- 信頼できるホストへのアクセスを制限します。
- VPN クライアントを設定します。

ルータの暗号化の設定

最初に、認証、許可、およびアカウンティング（AAA）パラメータを設定します。次に、パラメータを設定する例を示します。

```
aaa authentication login userauthen local
username <username> password 0 <password>
```

次の例は、内部データベースを使用しています。ただし、認証を実行するように、外部認証サーバを指定できます。

AAA パラメータを設定した後、Internet Security Association and Key Management Protocol（ISAKMP）ポリシーとクリプトマップを設定します。次の例では、フェーズ 1（Internet Key Exchange（IKE））の暗号化プロトコルとして事前共有キー、Diffie-Hellman（DH）グループ 2 および AES 256 を使用します。クリプト マップはダイナミック マップと呼ばれ、VPN グループは LI グループと呼ば

れます。アクセス リスト 108 によって、ルータに許可されるトラフィックが定義されます（この状況で ip プールは 10.1.1.254 を介した 10.1.1.1 です）。

```
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
!
crypto isakmp client configuration group LI-group
key <password>
dns 10.10.10.10
wins 10.10.10.20
domain cisco.com
pool ippool
acl 108
!
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
set transform-set myset
!
!
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
interface GigabitEthernet0/3
ip address <IP address of LI-enabled router> 255.255.255.0
crypto map clientmap
!
!
ip local pool ippool 10.1.1.1 10.1.1.254
!
!
access-list 108 permit ip  10.1.1.0 0.0.0.255 host 10.0.24.4 <IP address of LI-enabled
router>
```

信頼できるホストへのアクセス制限（暗号化あり）

次の例は、VPN クライアントの IP プール（10.1.1.0/24）のみを許可する ACL の作成方法と、SNMPv3 グループへのその ACL の割り当て方法を示しています。

```
access-list my-list permit ip 10.1.1.0 0.0.0.255
snmp-server group my-group v3 auth access my-list
```

VPN クライアントの設定

See the
Installing the VPN Client
document to download and configure the Cisco VPN Client for Solaris. See the
Cisco VPN Client installation instructions
document to download and configure the Cisco VPN Client for other operating systems.

合法的傍受の設定方法

ルータで合法的傍受をプロビジョニングするための直接のユーザ コマンドはありませんが、LI MIB へのアクセスの有効化、SNMP 通知の設定、LI RADIUS セッション機能のイネーブル化など、いくつかの設定作業を実行する必要があります。ここでは、必要なタスクの実行方法について説明します。

合法的傍受 MIB の制限付き SNMP ビューの作成

ユーザを作成して、シスコの合法的傍受 MIB を含む SNMP ビューに割り当てるには、ここに示す手順を実行します。

はじめる前に

- コマンドは、レベル 15 のアクセス権で、グローバル コンフィギュレーション モードで実行する必要があります。
- デバイスで SNMPv3 が設定されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaaintercept**
4. **snmp-serverview***view-nameMIB-name***included**
5. **snmp-serverview***view-nameMIB-name***included**
6. **snmp-serverview***view-nameMIB-name***included**
7. **snmp-servergroup***group-name***v3noauthread***view-name***write***view-name*
8. **snmp-serveruser***user-namegroup-name***v3authmd5***auth-password*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**aaaintercept** 例： `Device(config)# aaa intercept`	デバイスで合法的傍受をイネーブルにします。 • このコマンドが削除されたときに許可のないユーザが傍受を停止できないように、このコマンドを高い管理セキュリティに関連付けます。 （注） **aaaintercept** コマンドは、IP セッションを使用した盗聴の設定に必要です。
ステップ 4	**snmp-serverview***view-nameMIB-name***included** 例： `Device(config)# snmp-server view exampleView ciscoTap2MIB included`	CISCO-TAP2-MIB を含む SNMP ビューを作成します（ここで、*exampleView* は、MIB に対して作成するビューの名前です）。 • この MIB は、通常とブロードバンドの両方の合法的傍受に必要です。
ステップ 5	**snmp-serverview***view-nameMIB-name***included** 例： `Device(config)# snmp-server view exampleView ciscoIpTapMIB included`	CISCO-IP-TAP-MIB を SNMP ビューに追加します。
ステップ 6	**snmp-serverview***view-nameMIB-name***included** 例： `Device(config)# snmp-server view exampleView cisco802TapMIB included`	CISCO-802-TAP-MIB を SNMP ビューに追加します。
ステップ 7	**snmp-servergroup***group-name***v3noauthread***view-name***write***view-name* 例： `Device(config)# snmp-server group exampleGroup v3 noauth read exampleView write exampleView`	LI MIB ビューにアクセス可能な SNMP ユーザ グループを作成し、グループのビューに対するアクセス権を定義します。

	コマンドまたはアクション	目的
ステップ 8	**snmp-serveruser***user-namegroup-name***v3authmd5***auth-password* 例： `Device(config)# snmp-server user exampleUser exampleGroup v3 auth md5 examplePassword`	指定したユーザ グループにユーザを追加します。
ステップ 9	**end** 例： `Device(config)# end`	現在のコンフィギュレーションモードを終了し、特権EXECモードに戻ります。

次の作業

これで仲介デバイスは合法的傍受 MIB にアクセスし、SNMP の **set** および **get** 要求を発行して、ルータ上で合法的傍受を設定および実行できるようになります。ルータがメディエーション デバイスに SNMP 通知を送信するよう設定する方法については、「合法的傍受のための SNMP 通知のイネーブル化」を参照してください。

合法的傍受のための SNMP 通知のイネーブル化

SNMP は、合法的傍受イベントについての通知を自動的に生成します。合法的傍受通知をメディエーション デバイスに送信するようにルータを設定するには、ここに示す手順を実行します。

はじめる前に

- コマンドは、レベル 15 のアクセス権で、グローバル コンフィギュレーション モードで実行する必要があります。
- ルータで SNMPv3 が設定されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-serverhost***ip-address***community-stringudp-port***portnotification-type*
4. **snmp-serverenabletrapssnmpauthenticationlinkuplinkdowncoldstartwarmstart**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**snmp-serverhost***ip-address***community-stringudp-port***portnotification-type* 例： `Device(config)# snmp-server 10.2.2.1 community-string udp-port 161 udp`	メディエーション デバイスの IP アドレスと、通知要求とともに送信されるパスワードに似たコミュニティ ストリングを指定します。 • 合法的傍受では、**udp-port** は 162（SNMP のデフォルト）ではなく 161 とする必要があります。
ステップ 4	**snmp-serverenabletrapssnmpauthenticationlinkuplinkdowncoldstartwarmstart** 例： `Device(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`	RFC 1157 通知をメディエーション デバイスに送信するようにルータを設定します。 • これらの通知は、認証の失敗、リンク ステータス（アップまたはダウン）、およびルータ再起動を示します。
ステップ 5	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SNMP 通知のディセーブル

ルータ上で SNMP 通知をディセーブルにするには、ここに示す手順を実行します。

（注） 合法的傍受通知をディセーブルにするには、SNMPv3 を使用して CISCO-TAP2-MIB オブジェクト cTap2MediationNotificationEnable を false(2) に設定します。SNMPv3 を通じて合法的傍受の通知を再度イネーブルにするには、オブジェクトに true（1）を再設定します。

手順の概要

1. **enable**
2. **configureterminal**
3. **nosnmp-serverenabletraps**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**nosnmp-serverenabletraps** 例： `Device(config)# no snmp-server enable traps`	システムで使用可能なすべての SNMP 通知タイプをディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RADIUS セッション傍受のイネーブル化

メディエーション デバイスまたはタップをプロビジョニングするために使用可能なユーザ CLI コマンドはありません。しかし、CISCO-TAP-MIB を通じて傍受をイネーブルにするには、account-session-id 値をメディエーション デバイスが使用できるようにシステムを設定する必要があります。ルータで RADIUS セッション傍受をイネーブルにするには、ここに示す手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaaintercept**
4. **aaaauthenticationpppdefaultgroupradius**
5. **aaaaccountingdelay-startall**
6. **aaaaccountingsendstop-recordauthenticationfailure**
7. **aaaaccountingnetworkdefaultstart-stopgroupradius**
8. **radius-serverattribute44include-in-access-req**
9. **radius-serverhost***host-name*
10. **aaaserverradiusdynamic-author**
11. **client***ip-address*
12. **domain** {**delimiter***character*| **stripping[right-to-left]**}
13. **server-key***word*
14. **port***port-number*
15. **exit**
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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 3	**aaaintercept** 例： `Device(config)# aaa intercept`	ルータで合法的傍受をイネーブルにします。 • このコマンドが削除されたときに許可のないユーザが傍受を停止できないように、このコマンドを高い管理セキュリティに関連付けます。
ステップ 4	**aaaauthenticationpppdefaultgroupradius** 例： `Device(config)# aaa authentication ppp default group radius`	ポイントツーポイント プロトコル（PPP）を実行中のシリアルインターフェイス上で使用する認証方式を指定します。 （注） このコマンドが必要なのは、タップ情報がRADIUSサーバにしかないためです。ローカルに設定した情報で認証できますが、ローカルに設定した情報ではタップを指定できません。
ステップ 5	**aaaaccountingdelay-startall** 例： `Device(config)# aaa accounting delay-start all`	アカウンティング開始レコードの生成を、ユーザのIPアドレスが確立されるまで遅らせます。**all**キーワードを指定することにより、遅延がすべての VRF ユーザおよび非 VRF ユーザに適用されます。 （注） このコマンドは、メディエーション デバイスがターゲットに割り当てられた IP アドレスを参照できるようにするために必要です。
ステップ 6	**aaaaccountingsendstop-recordauthenticationfailure** 例： `Device(config)# aaa accounting send stop-record authentication failure`	（任意）ログイン時またはセッションのネゴシエーション中に認証に失敗したユーザに対するアカウンティング停止レコードを生成します。 （注） 合法的傍受の動作 1 でタップが開始されない場合、停止レコードのAcct-Termination-Cause（属性49）に 15（サービス使用不能）が設定されます。
ステップ 7	**aaaaccountingnetworkdefaultstart-stopgroupradius** 例： `Device(config)# aaa accounting network default start-stop group radius`	（任意）すべてのネットワーク関連のサービス要求に対するアカウンティングをイネーブルにします。 （注） このコマンドは、タップが開始されなかった理由を特定するためだけに必要です。
ステップ 8	**radius-serverattribute44include-in-access-req** 例： `Device(config)# radius-server attribute 44 include-in-access-req`	（任意）ユーザ認証前のアクセス要求パケット（事前認証の要求を含む）中で、RADIUS 属性 44（アカウンティング セッション ID）を送信します。

	コマンドまたはアクション	目的
		（注） このコマンドは、Access-Request パケットから属性 44 を取得するために入力します。そうしない場合、属性 44 の値を特定するには、アカウンティング パケットが受信されるのを待つ必要があります。
ステップ 9	**radius-serverhost***host-name* 例： `Device(config)# radius-server host host1`	（任意）RADIUS サーバ ホストを指定します。
ステップ 10	**aaaserverradiusdynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	デバイスを認証、許可、アカウンティング（AAA）サーバとして設定して外部ポリシーサーバとの通信を容易にし、ダイナミック認可ローカルサーバコンフィギュレーション モードを開始します。 （注） セッションの開始時に常にタップが開始される場合、このコマンドはオプションです。CoA-Requests を使用して既存のセッションでタップを開始および停止する場合は、このコマンドは必須です。
ステップ 11	**client***ip-address* 例： `Device(config-locsvr-da-radius)# client 10.0.0.2`	（任意）デバイスが CoA-Request パケットを受け付ける RADIUS クライアントを指定します。

ステップ 12	**domain** {**delimiter***character*| **stripping[right-to-left]**}
	
	例：
	
	`Device(config-locsvr-da-radius)# domain stripping right-to-left`
	
	例：
	
	`Device(config-locsvr-da-radius)# domain delimiter @`
		（任意）RADIUS アプリケーションについてユーザ名のドメイン オプションを設定します。
		
		• **delimiter** キーワードで、ドメイン デリミタを指定します。次のいずれかのオプションを *character* 引数に指定できます。**@**、/、**$**、**%**、\、**#** または **-**。
		
		• **stripping** キーワードは、着信のユーザ名と、**@** ドメイン デリミタの左側にある名前を比較します。
		
		• **right-to-left** キーワードは、右から左方向に見て最初のデリミタで文字列を終了します。

	コマンドまたはアクション	目的
ステップ 13	**server-key***word* 例： `Device(config-locsvr-da-radius)# server-key samplekey`	（任意）デバイスと RADIUS クライアントの間で共有する RADIUS キーを設定します。
ステップ 14	**port***port-number* 例： `Device(config-locsvr-da-radius)# port 1600`	（任意）デバイスが CoA-Request パケットを受け付ける RADIUS クライアントを指定します。
ステップ 15	**exit** 例： `Device(config-locsvr-da-radius)# exit`	ダイナミック認可ローカル サーバ コンフィギュレーションモードを終了し、グローバルコンフィギュレーション モードに戻ります。
ステップ 16	**end** 例： `Device(config)# end`	現在のコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

回線 ID ベースのタッピングの設定

ルータのユーザ セッションのデータ パケットと RADIUS 認証のデータ パケットの回線 ID ベースのタッピングを設定するには、このセクションの手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **subscriberaccessspppoeunique-keycircuit-id**
4. **end**
5. **showpppoesessionall**
6. **showidmgrsessionkeycircuit-id***circuit-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**subscriberaccesspppoeunique-keycircuit-id** 例： `Device(config)#subscriber access pppoe unique-key circuit-id`	PPPoE のユーザ セッションの一意の回線 ID タグがルータでタップされるように指定します。
ステップ 4	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**showpppoesessionall** 例： `Device# show pppoe session all`	次の手順でユーザセッションの検証に使用される、PPPoE セッションの回線 ID タグを表示します。

ステップ 6	**showidmgrsessionkeycircuit-id***circuit-id*
	
	例：
	
	`Device# show idmgr session key circuit-id Ethernet4/0.100:PPPoE-Tag-1`
	
	例：
	
	例：
	
	`session-handle = AA000007`
	
	例：
	
	`aaa-unique-id = 0000000E`
		一意の回線 ID タグを指定して、ID Manager（IDMGR）データベースのユーザ セッション情報を確認します。

	コマンドまたはアクション	目的

	例：
	`circuit-id-tag = Ethernet4/0.100:PPPoE-Tag-1`
	
	例：
	`interface = nas-port:0.0.0.0:0/1/1/100`
	
	例：
	`authen-status = authen`
	
	例：
	`username = user1@cisco.com`
	
	例：
	`addr = 106.1.1.3`
	
	例：
	`session-guid = 650101020000000E`
	
	例：
	`The session hdl AA000007 in the record is valid`
	
	例：
	`The session hdl AA000007 in the record is valid`
	
	例：
	`No service record found`	

合法的傍受の設定例

例：メディエーション デバイス アクセスの合法的傍受 MIB の有効化

次に、メディエーションデバイスが合法的傍受MIBにアクセスできるようにする例を示します。この例では、4 つの LI MIB（CISCO-TAP2-MIB、CISCO-IP-TAP-MIB、CISCO-802-TAP-MIB、CISCO-USER-CONNECTION-TAP-MIB）を含む SNMP ビュー（tapV）を作成します。また、tapV ビュー内の MIB に読み込み、書き込み、通知アクセス可能なユーザ グループも作成します。

```
aaa intercept
snmp-server view tapV ciscoTap2MIB included
snmp-server view tapV ciscoIpTapMIB included
snmp-server view tapV cisco802TapMIB included
snmp-server view tapV ciscoUserConnectionTapMIB included
snmp-server group tapGrp v3 noauth read tapV write tapV notify tapV
snmp-server user MDuser tapGrp v3 auth md5 MDpasswd
snmp-server engineID local 1234
```

例：RADIUS セッションの合法的傍受のイネーブル化

次に、イーサネットの PPP connection over Ethernet（PPPoE）リンクを使用したネットワーク アクセス サーバ（NAS）デバイスとして機能するルータ上で、RADIUS ベースの合法的傍受ソリューションを設定する例を示します。

```
aaa new-model
!
aaa intercept
!
aaa group server radius SG
server 10.0.56.17 auth-port 1645 acct-port 1646
!
aaa authentication login LOGIN group SG
aaa authentication ppp default group SG
aaa authorization network default group SG
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group SG
!
aaa server radius dynamic-author
client 10.0.56.17 server-key cisco
!
vpdn enable
!
bba-group pppoe PPPoE-TERMINATE
virtual-template 1
!
interface Loopback0
ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet4/1/0
description To RADIUS server
ip address 10.0.56.20 255.255.255.0
duplex auto
!
interface GigabitEthernet4/1/2
description To network
ip address 10.1.1.1 255.255.255.0
```

```
duplex auto
!
interface GigabitEthernet5/0/0
description To subscriber
no ip address
!
interface GigabitEthernet5/0/0.10
encapsulation dot1q 10
protocol pppoe group PPPoE-TERMINATE
!
interface Virtual-Template1
ip unnumbered Loopback0
ppp authentication chap
!
radius-server attribute 44 include-in-access-req
radius-server attribute nas-port format d
radius-server host 10.0.56.17 auth-port 1645 acct-port 1646
radius-server key cisco
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
『Configuring SNMP Support』	『*Configuring SNMP Support*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

規格	タイトル
PacketCable™ コントロール ポイント検出インターフェイス仕様	『*PacketCable™ Control Point Discovery Interface Specification*』（PKT-SP-CPD-I02-061013）

MIB

MIB	MIB のリンク
• CISCO-TAP2-MIB • CISCO-IP-TAP-MIB • CISCO-802-TAP-MIB • CISCO-USER-CONNECTION-TAP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC-2865	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC-3576	「*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*」
RFC-3924	『*Cisco Architecture for Lawful Intercept in IP Networks*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

合法的傍受に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *8*：合法的傍受に関する機能情報

機能名	リリース	機能情報
合法的傍受	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.15S	合法的傍受（LI）機能を利用すると、サービス プロバイダーは、エッジ ルータを通過する Voice-over-Internet（VoIP）トラフィックまたはデータ トラフィックを傍受できる機能を提供するという、司法当局による要求を満たすことができます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 Cisco IOS XE リリース 3.15S で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータのトンネルインターフェイスに合法的傍受機能が導入されました。
VRF 対応の LI（合法的傍受）	Cisco IOS XE Release 2.4	VRF 対応 LI は、特定のバーチャル プライベート ネットワーク（VPN）での IPv4 データの LI 盗聴をプロビジョニングする機能です。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

機能名	リリース	機能情報
RADIUS ベースの合法的傍受	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.5S	合法的傍受の実装は SNMP3 を使用してプロビジョニングされ、RADIUS セッションの傍受をサポートします。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 Cisco IOS XE リリース 3.5 では、ハイ アベイラビリティのサポートが RADIUS ベースの合法的傍受用に追加されました。
合法的傍受の PPP セッションの回線 ID ベースのタッピング	Cisco IOS XE Release 2.5	Cisco IOS XE リリース 2.5 では、PPP セッションの回線 ID ベースのタッピングが導入されました。回線 ID ベースのタッピングは、ユーザ セッションがアクティブになった後、タップがプロビジョニングされる場合にのみ動作します。このインスタンスでは、ユーザセッションは回線 ID タグで一意に識別されることを前提としています。

機能名	リリース	機能情報
合法的傍受の回線 ID ベースのタッピング	Cisco IOS XE Release 2.6	Cisco IOS XE リリース 2.6 では、PPP セッションの回線 ID ベースのタッピングの事前プロビジョニングが導入されました。ユーザ セッションがアクティブになる前にタップがプロビジョニングされる場合、タップはユーザ セッションがアクティブになればいつでも有効になります。また、対応する RADIUS 認証とアカウンティングパケットもタップされます。このインスタンスでは、ユーザセッションは回線 ID タグで一意に識別されることを前提としています。
非合法的傍受（Non-LI）のイメージ	Cisco IOS XE Release 3.10S	Cisco IOS XE リリース 3.10S では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 非合法的傍受のイメージは、Cisco IOS XE リリース 3.10S 以降で使用可能で、合法的傍受サブシステムは含まれません。

第 8 章

IPoE セッションの LI サポート

IPoE セッションの LI サポート機能は、RFC 2866 に準拠した IP over Ethernet（IPoE）セッションへのプロビジョニングされた合法的傍受（LI）のサポートを拡張しています。このドキュメントでは、IPoE 用の RADIUS ベースの合法的傍受を説明します。合法的傍受アーキテクチャとコンポーネントの情報およびコンフィギュレーション タスクと例については、「合法的傍受アーキテクチャ」モジュールを参照してください。

- 機能情報の確認，137 ページ
- IPoE セッションの LI サポートの制約事項，137 ページ
- IPoE セッションの LI サポートに関する追加情報，138 ページ
- IPoE セッションの LI サポートに関する機能情報，139 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IPoE セッションの LI サポートの制約事項

次の制約事項は IPoE セッションの RADIUS ベースの合法的傍受に適用されます。

- アクセス許可パケットは、LIパラメータが暗号化されるとき、RADIUSプロキシセッションに対してタップを開始するために使用することはできません。

- **aaaintercept** コマンドは、RADIUS ベースの LI に関連付けられた属性値ペア（AVP）を受け付けるように設定する必要があります。開始、停止、または非動作の認可変更（CoA）要求の頻度は、10 分あたり 1 のレートを超えることはありません。
- 異なるユーザから傍受されたトラフィックは、同じ仲介デバイス（MD ）に送信されます。各 MD ごとに固有のストリーム ID（8 桁の傍受 ID の最初の 4 桁で構成される）を使用する必要があります。
- RADIUS ベースの LI を使用してキャプチャされた傍受パケットの形式には、L2 ヘッダーが含まれます。これは SNMP ベースの LI の形式とは異なります。
- フロー単位のタップは、RADIUS ベースの LI を介してはサポートされていません。SNMP ベースの LI でサポートされます。

IPoE セッションの LI サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
『Configuring SNMP Support』	『*Configuring SNMP Support*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

規格	タイトル
PacketCable™ コントロール ポイント検出インターフェイス仕様	『*PacketCable™ Control Point Discovery Interface Specification*』（PKT-SP-CPD-I02-061013）

MIB

MIB	MIB のリンク
• CISCO-IP-TAP-MIB • CISCO-TAP2-MIB • CISCO-802-TAP-MIB • CISCO-USER-CONNECTION-TAP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2866	『*RADIUS Accounting*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPoE セッションの LI サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *9*：*IPoE* セッションの *LI* サポートに関する機能情報

機能名	リリース	機能情報
IPoE セッションの LI サポート	Cisco IOS XE Release 3.10S	RFC 2866 に従って、IPoE セッションへのプロビジョニング LI サポートを拡張します。

第 9 章

イメージ検証

イメージ検証機能を使用すると、Cisco IOS XE イメージとプロビジョニング ファイルの完全性を自動的に検証できます。そのため、ユーザは、イメージまたはプロビジョニング ファイルが偶発的な破壊から保護されていることを確認できます。破壊は、シスコによってファイルが作成される瞬間からユーザに届くまで、輸送中にいつでも起きる可能性があります。

- 機能情報の確認，141 ページ
- イメージ検証の制約事項，142 ページ
- イメージ検証について，142 ページ
- イメージ検証の使用方法，143 ページ
- イメージ検証の設定例，146 ページ
- その他の参考資料，147 ページ
- イメージ検証に関する機能情報，149 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

イメージ検証の制約事項

イメージ検証は、任意のファイルに適用され実行されますが、ファイルがイメージ ファイルまたはプロビジョニング ファイルでない場合、イメージ検証は実行されず、「SIGNATURE-4-NOT_PRESENT」というエラーが表示されます。

（注） イメージ検証機能は、Cisco IOS XE デバイスに格納されている Cisco IOS XE ソフトウェア イメージまたはプロビジョニング ファイルの完全性を確認するためにだけに使用できます。リモート ファイル システム上のイメージや、メモリ内で実行されているイメージの完全性を確認するためは使用できません。

イメージ検証について

（注） このドキュメントでは、Cisco IOS XE イメージに関する記述は、プロビジョニング ファイルにも適用されます。

イメージ検証の利点

転送エラーやディスク破壊の結果、偶発的にイメージやプロビジョニング ファイルの完全性が破壊される場合に、ルータが自動的に検出できるようになったため、Cisco IOS XE ルータの効率は向上しています。

イメージ検証の動作

実稼働イメージは、一連の転送を経てルータのメモリにコピーされるため、イメージの完全性が転送のたびに偶発的に破壊される危険があります。Cisco.com からイメージをダウンロードするとき、ユーザはダウンロードしたイメージに対してメッセージ ダイジェスト 5（MD5）ハッシュを実行し、Cisco.com で公開されている MD5 ダイジェストが、ユーザのサーバで計算した MD5 ダイジェストと同じであることを確認できます。しかし、MD5 ダイジェストが 128 ビット長であり、検証が手動であることから、多くのユーザはMD5ダイジェストを実行しません。イメージ検証により、ユーザは、ダウンロードしたすべてのイメージの完全性を自動的に検証できるため、ユーザの操作が大幅に削減されます。

イメージ検証の使用方法

イメージの完全性のグローバルな検証

fileverifyauto コマンドを使用すると、イメージの検証がグローバルにイネーブルになります。つまり、コピー（**copy** コマンドを使用）またはリロード（**reload** コマンドを使用）されるすべてのイメージが自動的に検証されます。**copy** コマンドと **reload** コマンドには、イメージの検証をイネーブルにする **/verify** キーワードがありますが、イメージをコピーまたはリロードするたびにキーワードを指定する必要があります。**fileverifyauto** コマンドを使用すると、デフォルトでイメージの検証がイネーブルになるため、イメージ検証を何度も指定する必要がなくなります。

デフォルトでイメージ検証をイネーブルにし、特定のイメージのコピーまたはリロードで検証をディセーブルにする場合は、**/noverify** キーワードは、**copy** コマンドまたは **reload** コマンドを指定することで、**fileverifyauto** コマンドを上書きします。

自動的なイメージ検証をイネーブルにするには、ここに示す手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **fileverifyauto**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	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	**fileverifyauto** 例： `Device(config)# file verify auto`	自動的なイメージ検証をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	グローバルコンフィギュレーションモードを終了します。 イメージをコピーまたはリロードする場合は、グローバルコンフィギュレーション モードを終了する必要があります。

次の作業

file verify auto コマンドを実行した後は、**/verify** キーワードを **copy** または **reload** コマンドで発行する必要はなくなります。これは、コピーまたはリロードされる各イメージが自動的に検証されるためです。

コピーしようとしているイメージの完全性の検証

copy コマンドを実行するとき、**/verify** キーワードを指定することで、コピーされるファイルの完全性を検証できます。完全性の確認に失敗した場合、コピーされたファイルは削除されます。コピーしようとしているファイルにハッシュが埋め込まれていない場合（古いイメージの場合）、コピー処理を続行するかどうかを質問されます。続行を選択すると、ファイルは正常にコピーされ、続行しないことを選択すると、コピーされたファイルが削除されます。

/verify キーワードを指定しないと、**copy** コマンドにより有効でないファイルがコピーされる可能性があります。そのため、**copy** コマンドを正常に実行した後、いつでも **verify** コマンドを実行して、ルータのストレージに格納されているファイルの完全性を確認できます。

ルータにコピーする前にイメージの完全性を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **copy** [**/erase**] [**/verify**| **/noverify**] *source-urldestination-url*
3. **verify** [**/md5** [*md5-value*]] *filesystem:file-url*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**copy** [**/erase**] [**/verify**| **/noverify**] *source-urldestination-url* 例： `Device# copy /verify tftp://10.1.1.1/cat3k_caa-universalk9.SSA.16.1.0.EFT3-1.bin flash:`	コピー元からコピー先に任意のファイルをコピーします。 • **/verify**：コピー先のファイルのシグニチャを検証します。検証に失敗すると、ファイルは削除されます。 • **/noverify**：イメージをコピーする前にコピー先ファイルのシグニチャを検証しません。 （注） **/noverify** は、多くの場合、**fileverifyauto** コマンドがイネーブルになっており、コピーするすべてのイメージのシグニチャが自動的に検証される場合に使用されます。
ステップ 3	**verify** [**/md5** [*md5-value*]] *filesystem:file-url*] 例： `Device# flash: tftp://10.1.1.1/cat3k_caa-universalk9.SSA.16.1.0.EFT3-1.bin flash:`	（任意）デバイスのストレージに格納されているイメージの完全性を検証します。

リロードしようとしているイメージの完全性の検証

reload コマンドを/**verify** キーワード付きで実行することにより、システムにロードしようとしているイメージの完全性が確認されます。/**verify** キーワードを指定した場合、システムがリブートを開始する前にイメージの検証が実行されます。そのため、検証に失敗すると、イメージはロードされません。

（注） プラットフォームが異なれば、ロードするファイルの取得方法も異なるため、BOOTVAR で指定されたファイルが検証されます。ファイルが指定されていない場合、各サブシステム上の最初のファイルが検証されます。プラットフォームによっては、設定レジスタなどの変数があるため、検証されるファイルがロードされるファイルになるとは限りません。

ルータにリロードする前にイメージの完全性を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **reload** [[**warm**] [**/verify**| **/noverify**] *text* | [**warm**] [**/verify**| **/noverify**] **in** [*hh*:*mm* [*text*] | [**warm**] [**/verify**| **/noverify**] **at***hh*:*mm* [*monthday* | *daymonth*] [*text*] | [**warm**] [**/verify**| **/noverify**] **cancel**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**reload** [[**warm**] [**/verify**| **/noverify**] *text* | [**warm**] [**/verify**| **/noverify**] **in** [*hh*:*mm* [*text*] | [**warm**] [**/verify**| **/noverify**] **at***hh*:*mm* [*monthday* | *daymonth*] [*text*] | [**warm**] [**/verify**| **/noverify**] **cancel**] 例： `Device# reload /verify`	オペレーティング システムをリロードします。 • **/verify**：コピー先のファイルのシグニチャを検証します。検証に失敗すると、ファイルは削除されます。 • **/noverify**：イメージをリロードする前にコピー先ファイルのシグニチャを検証しません。 （注） **/noverify** は、多くの場合、**fileverifyauto** コマンドがイネーブルになっており、コピーするすべてのイメージのシグニチャが自動的に検証される場合に使用されます。

イメージ検証の設定例

グローバル イメージ検証の例

次に、自動的なイメージ検証をイネーブルにする例を示します。このコマンドをイネーブルにした後、コピー（**copy** コマンドを使用）またはリロード（**reload** コマンドを使用）されるすべてのイメージに対し、イメージ検証が自動的に実行されます。

```
Device(config)# file verify auto
```

copy コマンドを使用したイメージ検証の例

次に、イメージをコピーする前にイメージ検証を指定する例を示します。

```
Device# copy /verify tftp://10.1.1.1/jdoe/c7200-js-mz disk0:
Destination filename [c7200-js-mz]?
Accessing tftp://10.1.1.1/jdoe/c7200-js-mz...
Loading jdoe/c7200-js-mz from 10.1.1.1 (via FastEthernet0/0):!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 19879944 bytes]
19879944 bytes copied in 108.632 secs (183003 bytes/sec)
Verifying file integrity of disk0:/c7200-js-mz
.................................................................................
.................................................................................
.................................................................................
.........................Done!
Embedded Hash   MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash       MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash               MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
```

reload コマンドを使用したイメージ検証の例

次に、デバイスにイメージをリロードする前にイメージ検証を指定する例を示します。

```
Device# reload /verify
Verifying file integrity of bootflash:c7200-kboot-mz.121-8a.E
%ERROR:Signature not found in file bootflash:c7200-kboot-mz.121-8a.E.
Signature not present. Proceed with verify? [confirm]
Verifying file disk0:c7200-js-mz
.......................................................................
.......................................................Done!
Embedded Hash     MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash      MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash          MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
Proceed with reload? [confirm]n
```

verify コマンドの出力例

次に、**verify** コマンドでイメージ検証を指定する例を示します。

```
Device# verify disk0:c7200-js-mz
%Filesystem does not support verify operations
Verifying file integrity of disk0:c7200-js-mz.......................................
.........................................................................Done!
Embedded Hash     MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash      MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash          MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
```

その他の参考資料

ここでは、イメージ検証機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
システムイメージのロード、メンテナンス、リブートに関する設定作業と情報	『Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide』
システムイメージをロード、メンテナンス、リブートするためのその他のコマンド	『Cisco IOS Master Command List, All Releases』

標準

規格	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。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

イメージ検証に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *10*：イメージ検証に関する機能情報

機能名	リリース	機能情報
イメージ検証		イメージ検証機能を使用すると、ユーザは Cisco IOS XE イメージの完全性を自動的に検証できます。 次のコマンドが導入または変更されました。**copy**、**fileverifyauto**、**reload**、**verify**。