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。

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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「AutoSecure の機能情報」（P.15）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

- 「AutoSecure の制約事項」（P.2）
- 「AutoSecure について」（P.2）
- 「AutoSecure の設定方法」（P.6）
- 「AutoSecure の設定例」（P.9）
- 「その他の参考資料」（P.13）
- 「AutoSecure の機能情報」（P.15）

AutoSecure の制約事項

AutoSecure 機能は、実稼動ネットワークではなく、テスト環境で使用する必要があります。

AutoSecure について

AutoSecure を設定するために、次の概念を理解しておく必要があります。

- 「AutoSecure の利点」（P.2）
- 「マネジメント プレーンのセキュリティ保護」（P.3）
- 「フォワーディング プレーンのセキュリティ保護」（P.6）

AutoSecure の利点

ルータのセキュリティ設定の簡素化

AutoSecure を使用すると、すべての Cisco IOS 機能を詳しく把握していなくても、ネットワークをすばやくセキュリティ保護できるため、AutoSecure は、特別なセキュリティ操作アプリケーションを持っていない顧客にとって役に立つ機能です。

これにより、セキュリティ機能の設定を自動化したり、デフォルトで有効になり、セキュリティ ホールとして悪用されることのある特定の機能を無効化したりする CLI を作成してルータをセキュリティ保護する複雑な作業が不要になります。

強化されたパスワード セキュリティ

AutoSecure の次のメカニズムにより、ルータへのアクセスの安全性が向上しています。

- パスワードに必要な最小長を設定することができます。これにより、「lab」や「cisco」など、ほとんどの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を排除できます。

  パスワードの最小長を設定するコマンドは **security passwords min-length** です。

- 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。

  許容できるログイン失敗回数（しきい値）を設定するコマンドは、**security passwords min-length** です。

ロールバックおよびシステム ロギング メッセージのサポート

Cisco IOS Release 12.3(8)T では、AutoSecure 設定のロールバックがサポートされています。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。

（注） Cisco IOS Release 12.3(8)T よりも前のリリースでは、AutoSecure 設定をロールバックすることはできません。このため、AutoSecure を設定する前に、現行の設定を常に保存する必要があります。

システム ロギング メッセージは、現行の設定に適用されている AutoSecure 設定の変更または改ざんを捕捉します。つまり、AutoSecure を実行しているときに詳細な監査証跡情報が得られます。

マネジメント プレーンのセキュリティ保護

マネジメント プレーンのセキュリティ保護は、AutoSecure 機能の中心となる 2 つの分野の 1 つです（もう一方の中心分野は次の「フォワーディング プレーンのセキュリティ保護」で説明します）。マネジメント プレーンのセキュリティ保護は、セキュリティ攻撃のために悪用される可能性のあるいくつかのグローバル サービスとインターフェイス サービスをディセーブルにし、攻撃の脅威を軽減する効果のあるグローバル サービスをイネーブルにすることによって行われます。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 Network Management（NM; ネットワーク管理）アプリケーションで管理されている場合、マネジメント 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」（P.3）
- 「サービスのインターフェイス単位のディセーブル化」（P.4）
- 「グローバル サービスのイネーブル化」（P.4）
- 「ルータへのセキュリティ保護されたアクセス」（P.4）
- 「セキュリティを確保するためのロギング」（P.5）

グローバル サービスのディセーブル化

AutoSecure 機能を（**auto secure** コマンドで）イネーブルにすると、ルータで次のグローバル サービスが自動的にディセーブルになります。

- Finger：攻撃の前の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 Packet Assembler and Disassembler（PAD; パケット アセンブラ/ディスアセンブラ）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 User Datagram Protocol（UDP; ユーザ データグラム プロトコル）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、CPU リソースを使い果たします。
- BOOTP サーバ：BOOTP は安全ではないプロトコルで、攻撃に悪用される可能性があります。
- HTTP サーバ：Secure HTTP 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 を使用している場合は、**ip http server** コマンドを使用して HTTP サーバを手動で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; シスコ検出プロトコル）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制御が行われないと、Network Time Protocol（NTP; ネットワーク タイム プロトコル）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、Message Digest 5（MD5; メッセージ ダイジェスト 5）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、それ以外の場合はディセーブルにする必要があります。そうしないと、アクセス制御メカニズムを通過すべきパケットが、一部のアクセス制御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

AutoSecure 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。Internet Control Management Protocol（ICMP; インターネット制御マネジメント プロトコル）到達不能は、ICMP ベースの Denial of Service（DoS; サービス拒否攻撃）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。
- Maintenance Operations Protocol（MOP; メンテナンス オペレーション プロトコル）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：パスワードが設定で表示されなくなります。
- **service tcp-keepalives-in** コマンドと **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。

ルータへのセキュリティ保護されたアクセス

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** コマンドおよび **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 Secure Shell（SSH; セキュア シェル）だけが有効な転送方法です）。**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 Secure Copy（SCP; セキュア コピー）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* の各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 Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）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、SNMP を使用してデバイスをモニタおよび設定するツールが SNMP を介してデバイスと通信することができなくなります。

- Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）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。

セキュリティを確保するためのロギング

AutoSecure 機能をイネーブルにすると、セキュリティ インシデントを識別して対応することができる次のロギング オプションが使用できます。

- 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。
- ログイン関連イベントのロギング メッセージの生成。たとえば、ログイン攻撃が検出され、ルータが「待機モード」になると、「Blocking Period when Login Attack Detected」という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、SSH によるログインをすべて許可しません）。

  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 Express Forwarding（CEF; Cisco エクスプレス フォワーディング）: AutoSecure は、可能であれば CEF または distributed CEF（dCEF; 分散 CEF）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。
- 厳密な Unicast Reverse Path Forwarding（uRPF; ユニキャスト リバース パス転送）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 では、検証可能な送信元 IP アドレスがない IP パケットが破棄されます。
- 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 Context-Based Access Control（CBAC; コンテキストベース アクセス制御）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

ここでは、次の各手順について説明します。

- 「AutoSecure の設定」（P.6）（必須）
- 「その他のセキュリティ設定」（P.8）（必須）
- 「AutoSecure の確認」（P.8）（任意）

AutoSecure の設定

AutoSecure を設定するために、次の作業を行う必要があります。

auto secure コマンド

auto secure コマンドを実行すると、マネジメント プレーンとフォワーディング プレーンをセキュリティ保護するための半インタラクティブなセッション（AutoSecure ダイアログ）を行うことができます。このコマンドには、マネジメント プレーンとフォワーディング プレーンのどちらかだけをセキュリティ保護するオプションがあります。どちらのオプションも選択しない場合は、両方のプレーンを設定することを確認するメッセージがダイアログに表示されます。

また、ダイアログの非インタラクティブな部分の設定をすべて行ってから、インタラクティブな部分の設定を行うことも可能です。ダイアログの非インタラクティブな部分のイネーブル化は、オプションの **no-interact** キーワードを選択して行います。

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。

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。

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。 プロンプトが表示されたら、パスワードを入力します。

ステップ 2	`auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]`
	
	例：
	`Router# auto secure`
		ルータのマネジメント プレーンおよびフォワーディング プレーンをセキュリティ保護します。
		• **management**：マネジメント プレーンのみがセキュリティ保護されます。
		• **forwarding**：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**：インタラクティブな設定を行うためのメッセージがまったく表示されません。
		• **full**：インタラクティブな質問メッセージがすべて表示されます。これがデフォルトです。

その他のセキュリティ設定

次の作業を行って、ルータへのアクセスのセキュリティ保護を強化します。

手順の概要

1. **enable**
2. **configure terminal**
3. **security passwords min-length** *length*
4. **enable password** {*password* | [*encryption-type*] *encrypted-password*}
5. **security authentication failure rate** *threshold-rate* **log**

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。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **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	**security passwords min-length** *length* **例：** `Router(config)# security passwords min-length 6`	設定される各パスワードが、指定した長さ以上になるようにします。 • *length*：設定されるパスワードの最小長です。
ステップ 4	**enable password** {*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 5	**security authentication failure rate** *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。

AutoSecure の確認

AutoSecure の機能が正しく実行されていることを確認するには、次の手順を行います。

手順の概要

1. **enable**
2. **show auto secure 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：** `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。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show auto secure config** **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

ここでは、次の設定例について説明します。

- 「AutoSecure の設定ダイアログの例」（P.9）

AutoSecure の設定ダイアログの例

AutoSecure ダイアログの例を次に示します。**auto secure** 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「マネジメント プレーンのセキュリティ保護」および「フォワーディング プレーンのセキュリティ保護」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            10.1.1.1  YES NVRAM  up down

FastEthernet1/0            10.2.2.2  YES NVRAM  up down

FastEthernet1/1            10.0.0.1  YES NVRAM  up up

Loopback0                  unassigned YES NVRAM  up up

FastEthernet0/0            10.0.0.2  YES NVRAM  up down
```

```
Enter the interface name that is facing internet:FastEthernet0/0

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 passwords min-length 6
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
int FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int FastEthernet1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int FastEthernet1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int FastEthernet0/0
 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
 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
 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

ここでは、AutoSecure の機能の関連資料について説明します。

関連資料

内容	参照先
ログイン機能（ログイン遅延やログイン ブロッキング期間など）	「Cisco IOS Login Enhancements」フィーチャ モジュール
ルータの設定に関するその他の情報	『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4T』
その他のルータ コンフィギュレーション コマンド	『*Cisco IOS Configuration Fundamentals Command Reference Guide*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 1918	「Address Allocation for Private Internets」
RFC 2267	「*Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*」

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/public/support/tac/home.shtml

AutoSecure の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　AutoSecure の機能情報

機能名	リリース	機能情報
AutoSecure	12.3(1) 12.2(18)S 12.3(8)T 12.2(27)SBC	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。 この機能は、Cisco IOS Release 12.3(1)S で導入されました。 この機能は、Cisco IOS Release 12.2(18)S に統合されました。 Cisco IOS Release 12.3(8)T では、ロールバック機能とシステム ロギング メッセージがサポートされました。 この機能は、Cisco IOS Release 12(27)SBC に統合されました。 次のコマンドが導入または変更されました。**auto secure**、**security passwords min-length**、**show auto secure config**