CHAPTER 64

AutoSecure

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

AutoSecure の前提条件

これらの質問に答える準備ができている必要があります。

- 装置はインターネットに接続する予定かどうか。
- いくつのインターフェイスをインターネットに接続するか。
- インターネットに接続するインターフェイスの名前は何か。
- どのようなローカル ユーザ名およびパスワードを使用するか。
- スイッチのホスト名およびドメイン名は何か。

AutoSecure の制約事項

- AutoSecure によって行われた設定変更を元に戻すコマンドがないため、AutoSecure の設定を行う前に実行コンフィギュレーションを必ず保存してください。
- 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 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。
- 使用している装置を NM アプリケーションによって管理している場合は、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になり、NM アプリケーションのサポートが中断されます。
- SDM 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。
- 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。

AutoSecure について

注意　AutoSecure はスイッチのセキュリティ保護に役立ちますが、スイッチの完全なセキュリティを保証するものではありません。

AutoSecure の概要

AutoSecure の利点

AutoSecure 機能を使用すると、すべてのセキュリティ機能を理解することなく、スイッチが保護されます。AutoSecure は簡単なセキュリティ設定プロセスです。不必要なシステム サービスをディセーブルにし、基本的な推奨セキュリティ ポリシーをイネーブルにすることで、セキュアなネットワーキング サービスを保証します。

簡素化されたスイッチのセキュリティ設定

AutoSecure は、スイッチのセキュリティ機能の設定を完全に自動化します。AutoSecure はセキュリティ ホールとして悪用されるおそれがある、デフォルトでイネーブルになっているある種の機能をディセーブルにします。AutoSecure は、個々のニーズに応じて次の 2 つのモードで実行できます。

- インタラクティブ モード：サービスおよびその他のセキュリティ機能を指示に従ってイネーブルまたはディセーブルにするオプションです。各オプションのデフォルト設定が示されます。
- 非インタラクティブ モード：シスコの推奨するデフォルト設定を自動的に実行します。

AutoSecure によってイネーブルになる拡張パスワードのセキュリティ

- 最低限必要なパスワード長を指定できます。これにより、ネットワーク上で広く使用されている「lab」や「cisco」などの脆弱なパスワードの使用を制限できます。

  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。
- ログイン試行の失敗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るようにすることができます。

  ログイン試行の失敗許容回数（しきい値率）を設定するには、**security authentication failure rate** コマンドを使用します。

システム ロギング メッセージのサポート

システム ロギング メッセージは、実行コンフィギュレーションに適用されている AutoSecure 設定に対してあとから変更が行われた場合にその変更をキャプチャします。その結果、AutoSecure を実行するときにさらに詳細な監査証跡が可能になります。

AutoSecure によってイネーブルになるマネジメント プレーンのセキュリティ

注意　使用している装置をネットワーク管理（NM）アプリケーションによって管理している場合は、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になり、NM アプリケーションのサポートが中断されます。

マネジメント プレーンのセキュリティの概要

AutoSecure により、スイッチ管理インターフェイス（マネジメント プレーン）およびデータ ルーティングとスイッチングの機能（フォワーディング プレーン。「AutoSecure にってイネーブルになるフォワーディング プレーンのセキュリティ」（P.64-6）を参照）を保護できます。マネジメント プレーンの

セキュリティ保護は、セキュリティ攻撃で悪用される可能性のある特定のグローバル サービスおよびインターフェイス サービスをディセーブルにし、攻撃の脅威を最小限に抑える役に立つグローバル サービスをイネーブルにすることで実施されます。また、セキュア アクセスおよびセキュア ロギングをスイッチに設定します。

AutoSecure によってディセーブルになるグローバル サービス

- Finger：攻撃の前のシステムの情報を収集（探査）します。
- PAD：すべてのパケット アセンブラ/ディスアセンブラ（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。
- 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）診断ポート攻撃を引き起こします。送信者は、スイッチの UDP 診断サービスに偽の要求を大量に送信して、すべての CPU リソースを消費させます。
- 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 サーバを使用するか、関連する ACL を持つ HTTP サーバに組み込まれた認証を使用しなければ、HTTP サーバはセキュアではなく、攻撃で悪用されます（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） SDM 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：セキュアではないプロトコル（RFC 1413 で定義）です。外部ホストから TCP ポートに識別情報を照会できます。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）パケットがスイッチに送信されると、スイッチの利用可能なメモリが消費され、スイッチがクラッシュします。

（注） 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 コントロールを行っていない場合は、ネットワーク タイム プロトコル（NTP）はセキュアではありません。攻撃者は、このプロトコルを使用して NTP パケットを送信してスイッチをクラッシュまたは過負荷状態にさせます。

  NTP が必要な場合は、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 がグローバルでイネーブルになっている場合は、NTP を必要としないインターフェイスすべてでディセーブルにします。
- 送信元ルーティング：送信元ルーティングはデバッグ目的でだけ提供されており、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、パケットがスイッチのアクセス コントロール メカニズムのいくつかを回避する可能性があります。

AutoSecure によってディセーブルになるインターフェイス単位のサービス

- 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。機能が正しく設定されているネットワークにとっては特に有用というわけではなく、攻撃者はセキュリティ ホールを悪用するためにこの機能を使用することがあります。

- 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）到達不能は、ICMP ベースの DoS 攻撃（サービス拒絶攻撃）を可能にする方法の 1 つ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上でディセーブルにします。プロキシ ARP 要求は、DoS 攻撃を可能にする方法の 1 つとして知られています。これは、攻撃者が繰り返し送信した要求に応答しようとすることで、スイッチの利用可能な帯域幅およびリソースを消費するためです。
- 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上でディセーブルにします。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。

AutoSecure によってイネーブルになるグローバル サービス

- **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。

AutoSecure によってセキュリティが確保されるスイッチ 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、スイッチ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。

- テキスト バナーがない場合は、バナーを追加するよう要求されます。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@example.com +1 408 5551212 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 およびセキュア シェル（SSH）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。
- 装置上のイメージが暗号化イメージである場合、AutoSecure はスイッチにアクセスし、ファイル転送を行うために SSH およびセキュア コピー プロトコル（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* 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）。
- スイッチで簡易ネットワーク管理プロトコル（SNMP）を使用しないとユーザが指定する場合は、次の機能のいずれかが発生します。
  - インタラクティブ モードでは、ユーザはコミュニティ ストリングの値にかかわらず SNMP をディセーブルにするかどうか尋ねられます。コミュニティ ストリングはパスワードと同様に機能し、スイッチ上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 は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、AutoSecure はローカル AAA を設定します。AutoSecure はユーザにスイッチ上でローカル ユーザ名およびパスワードを設定するよう要求します。

AutoSecure によってイネーブルになるロギング オプション

- 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に対するロギング メッセージ。たとえば、ログイン攻撃が検出され、スイッチが待機モードに入ると、メッセージ「Blocking Period when Login Attack Detected」が表示されます。（待機モードでは、スイッチは Telnet、HTTP、または SSH を使用したログイン試行を許可しません）。
- **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。

AutoSecure にってイネーブルになるフォワーディング プレーンのセキュリティ

- ストリクト ユニキャスト リバース パス転送（uRPF）を設定して、偽装された（スプーフィングされた）送信元 IP アドレスが入ってくることで引き起こされる問題を軽減できます。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。
- ハードウェアのレート制限：AutoSecure では、ユーザにプロンプトを表示することなく、次のトラフィック タイプのハードウェアのレート制限をイネーブルにします。
  - IP エラー
  - RPF 失敗
  - ICMP のルートなしメッセージ
  - ICMP の ACL ドロップ メッセージ
  - IPv4 マルチキャスト FIB 欠落メッセージ
  - 部分的にスイッチングされている IPv4 マルチキャスト フローのメッセージ

  AutoSecure では、次のトラフィック タイプについて、ハードウェアのレート制限のオプションが利用できます。
  - ICMP リダイレクト
  - TTL 失敗

- MTU 失敗
- IP ユニキャスト オプション
- IP マルチキャスト オプション
- 入力と出力の ACL ブリッジド パケット

（注）　入力および出力 ACL ブリッジド パケットのレート制限は、ACL ロギングの障害となることがあり、TCP 代行受信、NAT、レイヤ 3 WCCP などのハードウェア加速機能のセッション セットアップ レートを増大させることがあります。

AutoSecure の設定方法

AutoSecure パラメータの設定

auto secure コマンドを使用すると、マネジメント プレーンおよびフォワーディング プレーンのセキュリティを保護するための半インタラクティブなセッション（別名 AutoSecure セッション）を実行できます。このコマンドは、マネジメント プレーンまたはフォワーディング プレーンのセキュリティを保護するだけです。コマンド ラインでどちらのオプションも選択されていない場合は、セッション中にどちらかのプレーンまたは両方のプレーンを選択して設定できます。

またこのコマンドでは、セッション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います。セッションの非インタラクティブな部分は、任意で **no-interact** キーワードを選択することでイネーブルにできます。

プロンプトが表示されているときに疑問符（**?**）を入力するとヘルプが表示され、Ctrl+C を押すとセッションが中断されます。

インタラクティブ モードでは、セッション終了時に、生成された設定をスイッチの実行コンフィギュレーションにコミットするかどうか尋ねられます。非インタラクティブ モードでは、変更は実行コンフィギュレーションに自動的に適用されます。

（注）　AutoSecure により行われた設定変更を元に戻すコマンドはありません。**auto secure** コマンドを実行する前に実行コンフィギュレーションを必ず保存する必要があります。

AutoSecure 設定プロセスを実行するには、特権 EXEC モードを開始して、次の作業を行います。

コマンド	目的
`Router# auto secure [management | forwarding] [no-interact | full]`	スイッチのどちらかのプレーンか両方のプレーンを設定するために AutoSecure セッションを実行します。 • **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。これはデフォルトです。

AutoSecure セッションの例については、「AutoSecure の設定例」（P.64-9）を参照してください。

その他のセキュリティ設定

AutoSecure 設定が終わってから、次の作業を行うことでスイッチへの管理アクセスのセキュリティをさらに強化できます。

	コマンドまたはアクション	目的
ステップ 1	`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 2	`Router(config)# security passwords min-length length`	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。範囲は 0 ～ 16 文字です。
ステップ 3	`Router(config)# enable password {password | [encryption-type] password}`	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。 • *encryption-type*：値が 0 である場合は、暗号化されないパスワードを指定することを示します。値が 7 である場合は、隠しパスワードを指定することを示します。 （注）　シスコのルータまたはスイッチにより暗号化されているパスワードを入力する場合を除いて、暗号化タイプを入力することは通常ありません。
ステップ 4	`Router(config)# security authentication failure rate threshold-rate 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。有効範囲は 1 ～ 1024 です。 • **log**：1 分間に失敗回数がしきい値を超える場合の Syslog 認証失敗

次に、スイッチで最短パスワード長を 10 文字に、パスワードの失敗の許容しきい値を 1 分間に 3 回に設定する例を示します。また、非表示ローカル パスワードを設定する例も示します。

```
Router# configure terminal
Router(config)# security passwords min-length 10
Router(config)# security authentication failure rate 3
Router(config)# enable password 7 elephant123
```

AutoSecure の確認

AutoSecure 機能の実行に成功していることを確認するには、次の作業を行います。

コマンド	目的
`Router# show auto secure config`	AutoSecure 設定の一部として追加されているすべてのコンフィギュレーション コマンドを表示します。出力はコンフィギュレーションにより生成される出力と同じです。

AutoSecure の設定例

次に、AutoSecure セッションの例を示します。**auto secure** コマンドを実行すると、AutoSecure は **no-interact** キーワードをイネーブルにしている場合を除いて、これと同様の応答が自動的に表示されます （ディセーブルにする機能とイネーブルにする機能の詳細については、「AutoSecure によってイネーブルになるマネジメント プレーンのセキュリティ」（P.64-3）および「AutoSecure にってイネーブルになるフォワーディング プレーンのセキュリティ」（P.64-6）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 it absolutely resistant
to all security attacks ***

 AutoSecure will modify the configuration of your device.

All the configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
AutoSecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

If this device is being managed by a network management station,
AutoSecure configuration may block network management traffic.
Continue with AutoSecure? [no]: y

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: y
Enter the number of interfaces facing the internet [1]: 1
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan77                 77.1.1.4        YES NVRAM  down                  down
GigabitEthernet6/1     unassigned      YES NVRAM  administratively down down
GigabitEthernet6/2     21.30.30.1      YES NVRAM  up                    up
Loopback0              3.3.3.3         YES NVRAM  up                    up
Tunnel1                unassigned      YES NVRAM  up                    up
```

```
Enter the interface name that is facing the internet: Vlan77

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

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of <Name of Enterprise>.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:
k
banner
k
Enter the new enable secret:
Confirm the enable secret :
Enable password is not configured or its length
is less than minimum no. of charactersconfigured
Enter the new enable password:
Confirm the enable password:

Configuration of local user database
Enter the username: cisco
Enter the password:
Confirm the password:
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected (in seconds): 5

Maximum Login failures with the device: 3

Maximum time period for crossing the failed login attempts (in seconds): ?
% A decimal number between 1 and 32767.

Maximum time period for crossing the failed login attempts (in seconds): 5

Configure SSH server? [yes]: no

Configuring interface specific AutoSecure services
```

```
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling unicast rpf on all interfaces connected
to internet

The following rate-limiters are enabled by default:
  ...

Would you like to enable the following rate-limiters also?
...

Enable the above rate-limiters also? [yes/no]: yes

Would you like to enable the rate-limiters for Ingress/EgressACL bridged packets also?
NOTE: Enabling the ACL in/out rate-limiters can affect ACL logging
      and session setup rate for hardware accelerated features such
      as NAT, Layer 3 WCCP and TCP Intercept
...

Enable the ACL in/out rate-limiters also? [yes/no]: no

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
banner k
banner
k
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$30kP$f.KDndYPz/Hv/.yTlJStN/
enable password 7 08204E4D0D48574446
username cisco password 7 08204E4D0D48574446
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line vty 0 15
 login authentication local_auth
 transport input telnet
login block-for 5 attempts 3 within 5
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
```

```
int Vlan1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int Vlan77
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int GigabitEthernet6/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int GigabitEthernet6/2
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Vlan77
 ip verify unicast source reachable-via rx
...
!
end


Apply this configuration to running-config? [yes]: yes

Applying the config generated to running-config

Router#
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する