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。

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、ユーザーにプロンプトを表示することなく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 サーバー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、Message Digest 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** コマンドと **transport output** コマンドも、これらの回線のすべてで設定されます。（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、シビラティ（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シビラティ（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、デバッグよりもシビラティ（重大度）の高いコマンドをすべてロギングサーバーに送信できます。

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有効にします。 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 is selected, then** の場合は、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、ユーザー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. **configure terminal**
3. **enable password** {*password* | [*encryption-type*] *encrypted-password* }
4. **security authentication failure rate** *threshold-rate* **log**
5. **exit** *threshold-rate* **log**
6. **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有効にします。 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	**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	**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 4	**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。
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。
ステップ 6	**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

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、このマニュアルで前述されている「管理プレーンのセキュリティ保護 （2 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 （5 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』
SNMP サポートの設定	SNMP サポートの設定
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	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 *1 : 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。**auto secure** および **show auto secure config**

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