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 DoS 攻撃から保護できます。

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、「Cisco IOS Login Enhancements（Login Block）の機能情報」（P.9）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 Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

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。12.3(33)SRB2、12.2(33)SXH2、および 12.4(15)T1 以降のリリース バージョンでは、Login Block 機能は HTTP 接続にも適用されます。

この機能によって導入される自動アクティベーション、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（この種の攻撃は、通常、まず、使用可能なパスワードの標準的な辞書のすべての単語を使用するため、「辞書攻撃」と呼ばれます）。このアクセスの試行には、スクリプトまたはプログラムが使用されるため、このような試行のプロファイルは、通常、DoS 攻撃と同じで、短時間に複数のログイン試行が行われます。

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

Cisco IOS 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、Cisco IOS ソフトウェアベース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。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。このコマンドは、**login delay** コマンドを発行する前に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**。

DoS 攻撃が疑われる場合のログインのシャットダウン

指定した時間内に設定した回数の接続試行が失敗した場合、Cisco IOS デバイスは「待機時間」に追加の接続を受け入れません（定義済みの Access Control List（ACL; アクセス コントロール リスト）により許可されるホストは待機時間から除外されます）。

待機時間を発生させる接続試行の失敗回数は、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」（P.3）（必須）
- 「ログイン パラメータの確認」（P.4）（任意）

ログイン パラメータの設定

Cisco IOS デバイスへの DoS 攻撃と思われる攻撃の検出と辞書攻撃の低減に役立つログイン パラメータを設定するには、次の作業を実行します。

ログイン パラメータのデフォルト

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、デフォルトのログイン機能をイネーブルにする **login block-for** コマンドを発行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. **configure terminal**
3. **login block-for** *seconds* **attempts** *tries* **within** *seconds*
4. **login quiet-mode access-class** {*acl-name* | *acl-number*}

5. **login delay** *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。 • 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	**login block-for** *seconds* **attempts** *tries* **within** *seconds* **例：** `Router(config)# login block-for 100 attempts 2 within 100`	Cisco IOS 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	**login quiet-mode access-class** {*acl-name* | *acl-number*} **例：** `Router(config)# login quiet-mode access-class myacl`	（任意）待機モードに切り替わるときに、ルータに適用される ACL を指定します。 このコマンドをイネーブルにしない場合、待機モード中、すべてのログイン要求が拒否されます。
ステップ 5	**login delay** *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。

この次の手順

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」（P.4）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. **show login** [**failures**]

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。 • 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 login** [**failures**] **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

show login 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
```

show login コマンドからの次のサンプル出力は、**login block-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.
```

show login 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、**login block-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.
```

show login failures 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
```

show login failures 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 回ログイン要求が失敗した場合に 100 秒の待機モード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

内容	参照先
AutoSecure	「AutoSecure」フィーチャ モジュール
セキュアな管理/管理アクセス	「Role-Based CLI Access」フィーチャ モジュール

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
なし	—

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/cisco/web/support/index.html

Cisco IOS Login Enhancements（Login Block）の機能情報

表 1 に、この機能のリリース履歴を示します。

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、ソフトウェア イメージがサポートする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確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。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ソフトウェア リリースだけが記載されています。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。

表 1　Cisco IOS Login Enhancements（Login Block）の機能情報

機能名	リリース	機能情報
Cisco IOS Login Enhancements（Login Block）	12.3(4)T 12.2(25)S 12.2(33)SRA 12.2(33)SRB 12.2(33)SXH 12.4(15)T1	Cisco IOS Login Enhancements（Login Block）により、ユーザは 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 Release 12.3(4)T で導入されました。 この機能は、Cisco IOS Release 12.2(25)S に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRA に統合されました。 HTTP ログイン ブロッキングのサポートは、Cisco IOS Release 12.2(33)SRB、12.2(33)SXH、12.4(15)T1 に統合されました。