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。

（注） AAA の「待機モード」機能を使用する場合は、**aaa new-model** コマンドを使用して aaa new-model を設定する必要があります。

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 コマンドの **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

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、デフォルトのログイン機能を有効にする **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. **aaa new-model**

4. **login block-for** *seconds* **attempts** *tries* **within** *seconds*
5. **login quiet-mode access-class** {*acl-name* | *acl-number*}
6. **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	**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	**aaa new-model** 例： `Router(config)# aaa new-model`	認証、許可、およびアカウンティング（AAA）アクセス コントロール モデルをイネーブルにします。
ステップ 4	**login block-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 5	**login quiet-mode access-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かぎり、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。 次に例を示します。 `Router#show access-lists sl_def_acl`

	コマンドまたはアクション	目的
		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 6	**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。

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 （5 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. **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	**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)# aaa new-model
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。 この機能により、次のコマンドが変更されました。**login block-for**、**login delay**、 **login quiet-mode access-class**、**show login**。

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。