Login Password Retry Lockout

Login Password Retry Lockout 機能により、システム管理者はユーザによるログイン試行が設定した回数失敗すると、ローカルの認証、許可、アカウンティング（AAA）ユーザ アカウントをロックアウトできます。

Login Password Retry Lockout の前提条件

- AAA コンポーネントを含む Cisco IOS イメージを実行する必要があります。

Login Password Retry Lockout の制約事項

- パスワードを推測している攻撃者とパスワードを誤って複数回入力している認証されたユーザとの区別はされないため、認証されたユーザもロックアウトされます。
- サービス拒絶（DoS）攻撃もあり得ます。つまり、認証されたユーザのユーザ名が攻撃者に知られた場合、認証されたユーザがロックアウトされる可能性もあります。

Login Password Retry Lockout に関する情報

ローカル AAA ユーザ アカウントのロックアウト

Login Password Retry Lockout 機能により、システム管理者は、AAA ユーザ アカウントに一致するユーザ名を使用したユーザによるログインが指定した回数失敗すると、ローカル AAA ユーザ アカウントをロックアウトできます。ロックアウトされたユーザは、ユーザ アカウントが管理者によってロック解除されるまで、再度正常にログインすることはできなくなります。

ユーザがシステムによってロックされるか、システム管理者によってロック解除されると、システム メッセージが生成されます。次に示すのは、このようなシステム メッセージの例です。

```
%AAA-5-USER_LOCKED: User user1 locked out on authentication failure.
```

システム管理者はロックアウトできません。

（注） システム管理者は特殊なユーザで、最大の特権レベル（ルート権限 - レベル 15）を使用して設定されています。これより低い特権レベルを使用して設定されたユーザーは、**enable** コマンドを使用して特権レベルを変更できます。ルート権限（レベル 15）に変更可能なユーザは、システム管理者として機能できます。

この機能は、ASCII、チャレンジ ハンドシェイク認証プロトコル（CHAP）およびパスワード認証プロトコル（PAP）など、任意のログイン認証方式に適用できます。

（注） ロックされたステータスによる認証エラー後、ユーザにメッセージは表示されません（つまり、通常の認証エラーとユーザのロックされたステータスによる認証エラーは区別されません）。

Login Password Retry Lockout の設定方法

Login Password Retry Lockout の設定

Login Password Retry Lockout 機能を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **username** *name* [**privilege** *level*] **password** *encryption-type password*

4. **aaa new-model**
5. **aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts*
6. **aaa authentication login default method**

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： `Device> 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： `Device# 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	**username** *name* [**privilege** *level*] **password** *encryption-type password* 例： `Device(config)# username user1 privilege 15 password 0 cisco`	ユーザ名をベースとした認証システムを構築します。
ステップ 4	**aaa new-model** 例： `Device(config)# aaa new-model`	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 5	**aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts* 例： `Device(config)# aaa local authentication attempts max-fail 3`	ユーザがロックアウトされるまでの試行の失敗回数の上限を指定します。
ステップ 6	**aaa authentication login default method** 例： `Device(config)# aaa authentication login default local`	ログイン時の認証、許可、アカウンティング（AAA）認証方式を設定します。たとえば、**aaa authentication login default** *local* はローカル AAA ユーザーデータベースを指定します。

ログインがロックアウトされたユーザのロック解除

ログインがロックアウトされたユーザをロック解除するには、次の手順を実行します。

（注） この作業を実行できるのは、ルート権限（レベル 15）を持つユーザだけです。

手順の概要

1. **enable**
2. **clear aaa local user lockout** {**username** *username* | **all**}

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： `Device> 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	**clear aaa local user lockout** {**username** *username*	**all**} 例： `Device# clear aaa local user lockout username user1`	ロックアウトされたユーザをロック解除します。

ユーザの失敗したログイン試行のクリア

この作業は、ユーザ設定が変更され、すでに記録されている、失敗したユーザのログイン試行をクリアする必要がある場合に役立ちます。

すでに記録されている、失敗したユーザのログイン試行をクリアするには、次の手順を実行します。

手順の概要

1. **enable**
2. **clear aaa local user fail-attempts** {**username** *username* | **all**}

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： `Device> 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	**clear aaa local user fail-attempts** {**username** *username*	**all**}	失敗したユーザの試行をクリアします。

	コマンドまたはアクション	目的
	例： `Device# clear aaa local user fail-attempts username user1`	• このコマンドは、ユーザ設定が変更され、すでに記録されている失敗した試行をクリアする必要がある場合に役立ちます。

Login Password Retry Lockout のステータスのモニタおよびメンテナンス

Login Password Retry Lockout 設定ステータスのモニタとメンテナンスを行うには、次の手順を実行します。

手順の概要

1. **enable**
2. **show aaa local user lockout**

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： `Device> 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 aaa local user lockout** 例： `Device# show aaa local user lockout`	現在の Login Password Retry Lockout 設定でロックアウトされているユーザのリストを表示します。

例

次の出力は、user1 がロックアウトされていることを示しています。

```
Device# show aaa local user lockout
          Local-user          Lock time
          user1               04:28:49 UTC Sat Jun 19 2004
```

Login Password Retry Lockout の設定例

Login Password Retry Lockout 設定の表示の例

次の **show running-config** コマンド出力は、Login Password Retry Lockout 設定で、ユーザーの試行の失敗回数の上限が 2 に設定されていることを示します。

```
Device # show running-config
Building configuration...
Current configuration : 1214 bytes
!
version 12.3
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname LAC-2
!
boot-start-marker
boot-end-marker
!
!
username sysadmin
username sysad privilege 15 password 0 cisco
username user1 password 0 cisco
aaa new-model
aaa local authentication attempts max-fail 2
!
!
aaa authentication login default local
aaa dnis map enable
aaa session-id common
```

その他の参考資料

ここでは、Login Password Retry Lockout に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

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 IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、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
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/en/US/support/index.html

Login Password Retry Lockout の機能情報

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 : Login Password Retry Lockout* の機能情報

機能名	リリース	機能情報
Login Password Retry Lockout	Cisco IOS XE Release 3.9S	Login Password Retry Lockout 機能により、システム管理者はユーザによるログイン試行が設定した回数失敗すると、ローカル AAA ユーザ アカウントをロックアウトできます。 次のコマンドが導入または変更されました。**aaa local authentication attempts max-fail**、**clear aaa local user fail-attempts**、**clear aaa local user lockout**。

用語集

- **local AAA method**：ルータ上にローカル ユーザー データベースを設定し、そのデータベースから、AAA にユーザーの認証または認可を提供させる方式。
- **local AAA user**：ローカル AAA 方式を使用して認証されたユーザー。

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。