# ロック アンド キー セキュリティの設定（ダイナミックアクセス リスト）

**機能の履歴**

| リリース | 変更内容 |
|---|---|
| Cisco IOS | Cisco IOS ソフトウェアの機能サポートに関する情報については、Cisco Feature Navigator を使用してください。 |

この章では、ルータでロックアンドキー セキュリティを設定する方法について説明します。ロック アンド キーは、IP プロトコルで使用可能なトラフィック フィルタリング セキュリティ機能です。

ロック アンド キー コマンドの詳細な説明については、『*Cisco IOS* セキュリティ コマンド リファレンス』を参照してください。この章で使用されたその他のコマンドの詳細については、コマンド リファレンス マスタ インデックスを使用するか、オンラインで検索してください。

機能に関連付けられたハードウェア プラットフォームまたはソフトウェア イメージの情報を識別するには、Cisco.com の Feature Navigator を使用して機能についての情報を検索するか、特定のリリースのソフトウェア リリースノートを参照してください。



## ロック アンド キーの設定の必須条件

ロック アンド キーは、IP 拡張アクセス リストを使用します。ロック アンド キーを設定しようとする前に、アクセス リストを使用してトラフィックをフィルタする方法について確実に理

解する必要があります。アクセス リストについては、「アクセス コントロール リスト：概要および指針」を参照してください。

ロックアンドキーは、Ciscoの認証、許可、アカウンティング（AAA）の枠組みで実装されているように、ユーザー認証と認可を使用します。ロック アンド キーを設定する前に、AAA ユーザー認証、許可、アカウンティングの設定方法について理解する必要があります。ユーザー認証および認可は、本書の「認証、認可、アカウンティング（AAA）」のセクションで説明します。

ロック アンド キーは、理解する必要のある **autocommand** コマンドを使用します。このコマンドは、『Cisco IOS Terminal *Services* コマンド リファレンス』を参照してください。

# ロック アンド キー セキュリティ（ダイナミック アクセス リスト）の設定に関する情報

## ロック アンド キーについて

ロック アンド キーは、IP プロトコル トラフィックを動的にフィルタするトラフィック フィルタリング セキュリティ機能です。ロック アンド キーは、IP ダイナミック拡張アクセス リストを使用して設定されます。ロック アンド キーは、その他の標準アクセス リストとスタティック拡張アクセス リストと共に使用できます。

ロック アンド キーが設定されると、IP トラフィックが通常ルータではブロックされる指定されたユーザーは、ルータ経由で一時的なアクセスを得ることができます。起動されると、ロック アンド キーは、指定されたユーザーに指定されたホストに到達することを許可するよう、インターフェイスの既存の IP アクセス リストを再設定します。その後、ロック アンド キーは、インターフェイスを元の状態に戻すよう、再設定します。

ユーザーがロック アンド キーが設定されたルータを介してホストへのアクセスできるようにするため、ユーザーは、最初にルータに Telnet セッションを開く必要があります。ユーザーがルータに標準 Telnet セッションを開始すると、ロック アンド キーは、自動的にユーザーを認証しようとします。ユーザーが認証されると、ルータを通じて、一時的なアクセスを取得し、宛先ホストに到達できます。

## ロック アンド キーの利点

ロックアンドキーは、標準およびスタティック拡張アクセスリストと同じ利点があります（これらの利点については、「アクセス コントロール リスト：概要および指針」で説明します）。ただし、ロック アンド キーには、標準およびスタティック拡張アクセス リストに比べ、次の利点もあります。

- ロック アンド キーは、個々のユーザーを認証するために実験機能を使用します。
- ロック アンド キーは、より大きなインターネットワークにおけるより簡素な管理を提供します。

- 多くの場合、ロック アンド キーは、アクセス リストに必要なルータ処理の量を減らします。
- ロック アンド キーは、ネットワーク ハッカーが、ネットワークへの侵入する可能性を減らします。

ロック アンド キーを使用すると、送信元および宛先がホストとなるアクセスをどのユーザーに許可するかを指定できます。これらのユーザーは、指定されたホストへのアクセスが許可される前に、ユーザー認証プロセスをパスする必要があります。ロック アンド キーは、その他の設定されたセキュリティ制約事項を損なうことなく、ファイアウォールを通じてダイナミック ユーザー アクセスを作成します。

# ロック アンド キーを使用するタイミング

ロック アンド キーを使用するタイミングの 2 つの例を以下に示します。

- 特定のリモート ユーザー（またはリモート ユーザーのグループに）が、インターネットを介して、そのリモートホストから接続して、ネットワーク内のホストへのアクセスを必要とする場合。ロック アンド キーは、ユーザーを認証し、次に、個々のホストまたはサブネットに対して、限られた時間の間、ファイアウォールを介した限られたアクセスを許可します。
- ローカル ネットワーク上のホストのサブセットがファイアウォールによって保護されたリモート ネットワーク上のホストにアクセスする必要がある場合。ロック アンド キーを使用すると、ローカル ユーザーが必要とするホストのセットに対してのみリモート ホストへのアクセスを有効にすることができます。ロック アンド キーは、ホストがリモート ホスト リモートへアクセスすることを許可する前に、ユーザーが TACACS+ サーバー、もしくはその他のサーバーを通じて、認証を行うことを必要とします。

# ロック アンド キーの機能

次のプロセスは、ロック アンド キー アクセスの動作を説明します。

1. ユーザーは、ロック アンド キー用に設定された境界（ファイアウォール）ルータへの Telnet セッションを開きます。ユーザーは、ルータ上の仮想端末ポートを介して接続します。
2. Cisco IOS ソフトウェアは、Telnet パケットを受信し、Telnet セッションを開いてパスワードを要求し、ユーザー認証プロセスを実行します。ユーザーは、ルータを介したアクセスが許可される前に、認証をパスする必要があります。認証プロセスは、ルータ、または TACACS+ または RADIUS サーバーなどの中央アクセス セキュリティ サーバーで実行することもできます。
3. ユーザーが認証をパスすると、Telnet セッションからログアウトし、ソフトウェアがダイナミック アクセス リストに一時的なエントリを作成します。（設定ごとに、この一時エントリは、ユーザーが一時的なアクセスを与えられるネットワークの範囲を制限できます。）

4. ユーザーは、ファイアウォール経由でのデータを交換します。
5. ソフトウェアは、設定されているタイムアウトに到達するか、システム管理者が手動でクリアした場合に、一時的なアクセス リスト エントリを削除します。設定されているタイムアウトは、アイドルタイムアウトまたは絶対タイムアウトのいずれかになることがあります。

（注） ユーザーがセッションを終了させた場合、一時アクセス リスト エントリは、自動的に削除されません。一時アクセスリストのエントリは、設定されているタイムアウトに到達するか、システム管理者がクリアされるまで保持されます。

# Cisco IOS リリース 11.1 以前のリリースとの互換性

**access-list** コマンドの拡張機能は、ロック アンド キーに使用されます。これらの機能拡張は、下位互換性があります。Cisco IOS リリース 11.1 以前のリリースから新しいリリースに移行する場合、アクセスリストは、機能拡張を反映するために、自動的に変換されます。ただし、次の注意の項で説明されているように、Cisco IOS リリース 11.1 以前のリリースでロック アンド キーを使用しようとすると、問題が発生する可能性があります。

注意 Cisco IOS リリース 11.1 以前のリリースは、ロック アンド キー アクセス リスト拡張機能と互換性がありません。そのため、リリース 11.1 以前のソフトウェアでアクセス リストを保存し、このソフトウェアを使用する場合、作成されたアクセスリストは、正しく解釈されません。これによって、深刻なセキュリティ上の問題が発生する可能性があります。これらのファイルと共に画像をブートする前に、Cisco IOS リリース 11.1 以降のソフトウェアを使用して、古い設定ファイルを保存する必要があります。

# ロック アンド キーによるスプーフィングのリスク

注意 ロック アンド キー アクセスを使用すると、外部イベント（Telnet セッション）がファイアウォールに穴を開けることができます。この穴がある間、ルータは、送信元アドレスのスプーフィングを受ける可能性があります。

ロック アンド キー が起動されると、ユーザー アクセスを許可するインターフェイスを一時的に再設定することで、ファイアウォール内に動的な穴が作成されます。この穴がある間は、別のホストが認証済みのユーザーのアドレスを偽装し、ファイアウォールの裏でのアクセスを獲得する可能性があります。ロック アンド キーは、アドレス スプーフィングの問題を発生させません。この問題は、ユーザーの関心事としてここに特定されるだけです。スプーフィングは、すべてのアクセス リストに伴う問題であり、ロック アンド キーは、この問題に具体的に対処していません。

スプーフィングを防ぐには、リモート ホストからのトラフィックがセキュアなリモート ルータで暗号化され、ロック アンド キーを提供するルータ インターフェイス上でローカルで復号化されるように暗号化を設定します。ルータの入力時に、ロック アンド キーを使用して、すべてのトラフィックを暗号化したい場合、ハッカーは、それらが暗号化を複製できないか、暗号化のセットアップ プロセスの必要な部分として認証できないため、送信元アドレスをスプーフィングすることはできません。

# ロック アンド キーによるルータのパフォーマンスへの影響

ロック アンド キーを設定すると、ルータのパフォーマンスは、次のように影響を受ける場合があります。

- ロック アンド キーが起動されると、ダイナミック アクセス リストは、シリコン スイッチング エンジン（SSE）上でのアクセス リストの再構成が強制されます。これによって、SSE スイッチング パスが一瞬低速になります。
- ダイナミック アクセス リストは、アイドル タイムアウト機能（タイムアウトがデフォルトになったとしても）を必要とし、SSE スイッチングにすることはできません。これらのエントリは、プロトコル ファスト スイッチング パスで処理する必要があります。
- リモート ユーザーが境界ルータでロック アンド キーを起動すると、追加のアクセス リスト エントリが境界ルータ インターフェイスで作成されます。インターフェイスのアクセス リストが動的に拡大および縮小します。エントリは、アイドル タイムアウトまたは最大タイムアウト期間が経過すると、動的に削除されます。アクセス リストが大きくなると、パケット交換のパフォーマンスが低下し、パフォーマンスの問題の劣化を通知する場合、ロック アンド キーによって生成された一時アクセス リスト エントリを削除するかどうかを確認するために、境界ルータの設定を確認する必要があります。

# ロック アンド キーの保守

ロック アンド キーを使用中の場合、ダイナミック アクセス リストは、認証エントリの追加および削除に伴って動的に増減します。エントリが存在しても、スプーフィング攻撃のリスクがあるため、タイムリーにエントリが削除されていることを確認する必要があります。また、エントリの数が増えれば、ルータのパフォーマンスへの影響も大きくなります。

アイドルまたは絶対タイムアウトを設定していない場合、エントリは、ダイナミック アクセス リスト エントリを手動で削除するまで維持されます。この場合、エントリの削除について配慮してください。

# ダイナミック アクセス リスト

ダイナミック アクセス リストを設定する場合は、次のガイドラインを参照してください。

- いずれか 1 つのアクセス リストに対して複数のダイナミック アクセス リストを作成しないで下さい。ソフトウェアは、定義された最初のダイナミック アクセス リストだけを参照します。

- 別のアクセス リストに同じ名前を割り当てないで下さい。そうすることで、既存のリストを再利用するように、ソフトウェアに指示します。すべての名前付きエントリは、設定内でグローバルに一意である必要があります。
- スタティック アクセス リストに属性を割り当てるのと同じ方法で、ダイナミック アクセス リストに属性を割り当てます。一時アクセス リスト エントリは、このリストに割り当てられているアトリビュートを継承します。
- ルータ経由でのアクセスが許可される前に、ユーザーが認証する必要があるルータに対する Telnet セッションを開く必要があるよう、プロトコルとして Telnet を設定します。
- 今度は、**autocommand** 内の **access-enable** コマンド内の **timeout** キーワードで、アイドル タイムアウトを定義するか、後で、**access-list** コマンドで絶対タイムアウト値を定義します。アイドル タイムアウトまたは絶対タイムアウトを定義する必要があります。そうしないと、一時的なアクセス リスト エントリは、管理者が手動でエントリを削除するまで（ユーザーがセッションを終了した後でも）、インターフェイスで永久に設定されたままになります。（必要に応じて、アイドル タイムアウトと絶対タイムアウトの両方を設定することもできます）。
- アイドル タイムアウトを設定する場合、アイドル タイムアウト値は、WAN アイドル タイムアウト値と等しくなる必要があります。
- アイドル タイムアウトと絶対タイムアウトの両方を設定する場合、アイドル タイムアウト値は、絶対タイムアウト値未満である必要があります。
- ジョブが ACL の絶対タイマーを超えて動作していることを認識した場合、**access-list dynamic-extend** コマンドを使用して、6 分ほどダイナミック ACL の絶対タイマーを拡張します。このコマンドにより、ロック アンド キーを使用して、自身を再認証するため、ルータに新しい Telnet セッションを開くことができます。
- 一時的なエントリで置換される唯一の値は、入力アクセス リストまたは出力アクセス リスト内にアクセス リストがあったかどうかに応じて、送信元または宛先アドレスになります。ポートなどの他の属性はすべて、メインのダイナミック アクセス リストから引き継がれます。
- ダイナミック リストへの追加はそれぞれ、ダイナミック リストの先頭に常に配置されます。一時アクセス リスト エントリの順序を指定することはできません。
- 一時アクセス リスト エントリが NVRAM には書き込まれません。
- ダイナミック アクセス リストを手動でクリアまたは表示するには、この章で後述される「ロック アンド キーの維持」を参照して下さい。

# ロック アンド キー認証

認証問い合せプロセスを設定するには、3 つの方法があります。この項では、これら 3 つの方法について説明します。

（注） Cisco は、認証問い合せプロセスには、TACACS+ サーバーを使用することを推奨します。TACACS+ は、認証、許可、アカウンティング サービスを提供します。また、プロトコル サポート、プロトコル仕様、および中央集中型セキュリティデータベースも提供します。TACACS+ サーバーの使用については、次項「方法 1 -- セキュリティ サーバーの設定」で説明します。

TACACS+ サーバーなどのネットワーク アクセス セキュリティ サーバーを使用します。この方法には、TACACS+ サーバーでの追加設定手順が必要になりますが、より厳しい認証問い合わせとより高度な追跡機能が可能になります。

```
Router(config-line)# login tacacs
```

**username** コマンドを使用します。この方法では、認証はユーザー単位で決定するため、効果的です。

```
Router(config)# username

name
 {nopassword
 |
password
 {
mutual-password
 |
encryption-type

encryption-password
}}
```

**password** および **login** コマンドを使用します。この方法は、パスワードがユーザーではなく、このポートに設定されているため、有効でありません。そのため、パスワードを知っているすべてのユーザーが正常に認証できます。

```
R
outer(config-line)# password

password
Router(config-line)# login local
```

# autocommand コマンド

**autocommand** コマンドは、ユーザーが特定の回線に接続する際に、システムが指定されている特権 EXEC コマンドを自動的に実行するように設定します。**autocommand** コマンドの設定のための次のガイドラインを使用します。

- ユーザーを認証するために TACACS+ サーバーを使用する場合、TACACS+ サーバー上で、ユーザーごとの autocommand として、**autocommand** コマンドを設定する必要があります。ローカル認証を使用する場合、回線上で **autocommand** コマンドを使用します。
- 同じ **autocommand** コマンドで、すべての仮想端末（VTY）ポートを設定します。VYT ポートで **autocommand** コマンドを省略すると、任意のホストがルータの特権 EXEC モー

ドへのアクセスを許可し、ダイナミック アクセス リスト内の一時アクセス リスト エントリを作成しません。

- **autocommand access-enable** コマンドでアイドル タイムアウトを定義しない場合、**access-list** コマンドで絶対タイムアウトを定義する必要があります。アイドル タイムアウトまたは絶対タイムアウトを定義する必要があります。そうしないと、一時的なアクセス リスト エントリは、エントリが管理者によって手動で削除されるまで（ユーザーがセッションを終了した後も）インターフェイスで永久に設定されたままになります。（必要に応じて、アイドル タイムアウトと絶対タイムアウトの両方を設定することもできます）。
- アイドル タイムアウトと絶対タイムアウトの両方を設定する場合、絶対タイムアウト値は、アイドル タイムアウト値よりも大きくする必要があります。

# ロック アンド キーセキュリティ（ダイナミック アクセス リスト）の設定方法

## ロック アンド キーの設定

ロック アンド キーを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。次の手順を実行する際、この章の「ロック アンド キー設定のガイドライン」に記載されているガイドラインに従っていることを確認します。

### 手順の概要

1. Router(config)# **access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **telnet** *source source-wildcard destination destination-wildcard*[ **precedence** *precedence*] [ **tos** *tos*] [**established**] [**log**]
2. Router(config)# **access-list dynamic-extend**
3. Router(config)# **interface** *type number*
4. Router(config-if)# **ip access-group** *access-list-number*
5. Router(config-if)# **exit**
6. Router(config)# **line vty** *line-number* [*ending-line-number*]
7. 次のいずれかを実行します。
   - Router(config-line)# **login tacacs**
   -
   - Router(config-line)# **password** *password*
8. 次のいずれかを実行します。
   - Router(config-line)# **autocommand access-enable** [**host]** [**timeout** *minutes*]
   -
   - Router# **access-enable** [**host]** [**timeout** *minutes*]

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | Router(config)# **access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** \| **permit**} **telnet** *source source-wildcard destination destination-wildcard*[ **precedence** *precedence*] [ **tos** *tos*] [**established**] [**log**] | 一時アクセス リスト エントリのテンプレートとプレースホルダとして動作するダイナミック アクセス リストを設定します。 |
| ステップ 2 | Router(config)# **access-list dynamic-extend** | （任意）ロック アンド キーを使用して、自分の再認証を実行するようにルータに別の Telnet セッションを開く際に、6 分ごとのダイナミック ACL の絶対タイマーを拡張します。ジョブが ACL の絶対タイマー前を実行する場合に、このコマンドを使用します。 |
| ステップ 3 | Router(config)# **interface** *type number* | インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | Router(config-if)# **ip access-group** *access-list-number* | アクセス リストをインターフェイスに適用します。 |
| ステップ 5 | Router(config-if)# **exit** | インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。 |
| ステップ 6 | Router(config)# **line vty** *line-number* [*ending-line-number*] | 1 つ以上の仮想端末（VTY）ポートを定義し、ライン コンフィギュレーション モードを開始します。複数の VTY ポートを指定する場合、ソフトウェアがラウンドロビン ベースで使用可能な VTY ポートをハントするため、個別に設定する必要がありません。ロック アンド キー アクセスに対して、すべての VTY ポートを設定しない場合、ロック アンド キー サポートに対してのみ、VTY ポートのグループを指定できます。 |
| ステップ 7 | 次のいずれかを実行します。<br>• Router(config-line)# **login tacacs**<br>•<br>• Router(config-line)# **password** *password*<br>**例**：<br>`Router(config-line)# login local`<br>**例**：<br>`Router(config-line)# exit`<br>**例**： | 回線またはグローバル コンフィギュレーション モードでユーザー認証を設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | then<br>例：<br>Router(config)# **username** *name* **password** *secret* | |
| ステップ 8 | 次のいずれかを実行します。<br>• Router(config-line)# **autocommand access-enable** [**host**] [**timeout** *minutes*]<br>•<br>• Router# **access-enable** [**host**] [**timeout** *minutes*] | 回線設定または特権EXECモードの一時アクセス リスト エントリを作成できます。<br>回線設定モードで **access-enable** コマンドとともに **autocommand** を使用して、回線が接続されたときに、自動的にダイナミック アクセス リスト上の一時アクセス リスト エントリを作成するようシステムを設定します。<br>任意の **host** キーワードを指定しないと、ネットワーク全体のすべてのホストが一時アクセス リスト エントリを設定できます。ダイナミック アクセス リストには、新しいネットワーク接続を許可するためのネットワーク マスクが含まれます。<br>任意の **timeout** キーワードを指定すると、一時アクセス リストに対するアイドル タイムアウトを定義します。<br>有効値の範囲は 1 ～ 9999（分）です。 |

# ロック アンド キーの設定の確認

ユーザーに接続をテストするように求めることで、ロック アンド キーがルータで正しく設定されていることを確認できます。ユーザーは、ダイナミック アクセス リストで許可されるホストである必要があり、ユーザーは、AAA 認証および許可を設定する必要があります。

接続をテストするには、ユーザーは、ルータへの Telnet 接続を行い、Telnet セッションを閉じる許可をし、ルータの反対側のホストへのアクセスを試みる必要があります。このホストは、ダイナミック アクセス リストによって許可されているものである必要があります。ユーザーは、IPプロトコルを使用するアプリケーションのあるホストにアクセスする必要があります。

次の例は、エンドユーザーが正常に認証された場合に、何が見えるかを示しています。パスワードが入力され、認証された後に、Telnet 接続は閉じられます。一時アクセス リスト エントリが作成され、Telnet セッションを開始したホストがファイアウォールの内側のホストにアクセスします。

```
Router% telnet corporate
Trying 172.21.52.1 ...
Connected to corporate.example.com.
Escape character is '^]'.
```

```
User Access Verification
Password:Connection closed by foreign host.
```

ユーザーは、ルータで **show access-lists** コマンドを使用して、ルータを介して、ユーザーのアクセスを許可する別のエントリを含む、ダイナミック アクセス リストを表示できます。

## ダイナミック アクセス リスト エントリの表示

一時アクセス リスト エントリは、使用中に表示できます。一時アクセス リスト エントリがユーザーまたは絶対またはアイドル タイムアウト パラメータによってクリアされた後は表示されなくなります。表示される一致の数は、アクセス リスト エントリがヒットした回数を示します。

現在確立されているダイナミック アクセス リスト エントリ リストおよび一時アクセス リスト エントリ リストを表示するには、特権 EXEC モードで次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| Router# **show access-lists** [*access-list-number*] | ダイナミック アクセス リストおよび一時アクセス リスト エントリを表示します。 |

## ダイナミック アクセス リスト エントリの手動削除

一時アクセス リスト エントリを手動で削除するには、特権 EXEC モードで次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| Router# **clear access-template** [*access-list-number* \| *name*] [*dynamic-name*] [*source*] [*destination*] | ダイナミック アクセス リストを削除します。 |

# ロック アンド キーの設定例

## ローカル認証を使用したロック アンド キーの例

この例は、ルータで局所的に生じた認証を使って、ロック アンド キー アクセスを設定する方法を示しています。ロック アンド キーは、Ethernet 0 インターフェイスとして設定されます。

```
interface ethernet0
 ip address 172.18.23.9 255.255.255.0
 ip access-group 101 in
access-list 101 permit tcp any host 172.18.21.2 eq telnet
access-list 101 dynamic mytestlist timeout 120 permit ip any any
line vty 0
```

```
login local
autocommand access-enable timeout 5
```

最初の access-list エントリは、ルータに Telnet だけを許可します。2 番目のアクセス リスト エントリは、ロック アンド キーがトリガーされるまで常に無視されます。

**access-list** コマンドでは、タイムアウトは絶対タイムアウトです。この例では、mytestlist ACL の有効期間は、120 分です。つまり、ユーザーがログインし、**access-enable** コマンドを有効にすると、120 分間（最大絶対時間）有効なダイナミック ACL が作成されます。セッションは使用者の有無に関係なく、120 分後に閉じられます。

**access-enable** コマンドでは、タイムアウトは、アイドル タイムアウトです。この例では、ユーザーがログインまたは認証するたびに 5 分間セッションがあります。アクティビティがないと、セッションは 5 分後に終了し、ユーザーを再認証する必要があります。ユーザーが接続を使用すると、絶対時間が作用し、セッションは 120 分後に終了します。

ユーザーがルータへの Telnet セッションを開いた後、ルータはユーザーを認証しようとします。認証に成功すると、**autocommand** が実行され、Telnet セッションが終了します。**autocommand** は、2 番目のアクセス リスト エントリ（mytestlist）に基づいて、イーサネット 0 インターフェイスで一時的な着信アクセス リスト エントリを作成します。アクティビティがない場合、タイムアウトで規定されているように、この一時エントリは 5 分後に無効となります。

# TACACS+ 認証を使用したロック アンド キーの例

Cisco は、認証に TACACS+ サーバーを使用することを推奨します。以下の例を参照して下さい。

以下の例は、TACACS+ サーバーでの認証を使用して、ロック アンド キーを設定する方法について説明しまています。ロック アンド キー アクセスは、BRI0 インターフェイスで設定されます。4 つのポートは、VTY パスワード「password1」として定義されています。

```
aaa authentication login default group tacacs+ enable
aaa accounting exec stop-only group tacacs+
aaa accounting network stop-only group tacacs+
enable password ciscotac
!
isdn switch-type basic-dms100
!
interface ethernet0
ip address 172.18.23.9 255.255.255.0
!
interface BRI0
 ip address 172.18.21.1 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 3600
 dialer wait-for-carrier-time 100
 dialer map ip 172.18.21.2 name dialermapname
 dialer-group 1
 isdn spid1 2036333715291
 isdn spid2 2036339371566
 ppp authentication chap
 ip access-group 102 in
!
access-list 102 permit tcp any host 172.18.21.2 eq telnet
```

```
access-list 102 dynamic testlist timeout 5 permit ip any any
!
!
ip route 172.18.250.0 255.255.255.0 172.18.21.2
priority-list 1 interface BRI0 high
tacacs-server host 172.18.23.21
tacacs-server host 172.18.23.14
tacacs-server key test1
tftp-server rom alias all
!
dialer-list 1 protocol ip permit
!
line con 0
 password password1
line aux 0
 line VTY 0 4
 autocommand access-enable timeout 5
 password password1
!
```

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。