MSCHAP バージョン 2

Cisco IOS リリース 12.2(2)XB5 で導入された MSCHAP バージョン 2 機能を使用すると、Cisco ルータは、Microsoft Windows オペレーティング システムを使用するコンピュータとネットワーク アクセス サーバ（NAS）間の PPP 接続にマイクロソフト チャレンジ ハンドシェイク認証プロトコル バージョン 2（MSCHAP V2）の認証を使用できます。

Cisco IOS リリース 12.4(6)T では、MSCHAP V2 が新機能をサポートするようになりました。これを MSCHAPv2 のパスワード エージングの AAA でのサポートと呼びます。Cisco IOS リリース 12.4(6)T よりも前のバージョンでは、パスワード認証プロトコル（PAP）ベースのクライアントが認証、許可、アカウンティング（AAA）サブシステムにユーザ名とパスワードの値を送信すると、AAA が RADIUS サーバへの認証要求を生成していました。パスワードが失効している場合は、RADIUS サーバにより認証失敗のメッセージが返信されますが、認証が失敗した理由は AAA サブシステムには渡されていませんでした。そのため、認証が失敗したためにユーザはアクセスを拒否されますが、アクセスが拒否された理由は通知されませんでした。

Cisco IOS リリース 12.4(6)T で使用可能になったパスワード エージング機能は、パスワードが失効したことをクリプトベースのクライアントに通知し、ユーザがパスワードを変更するための一般的な方法を提供します。パスワードエージング機能では、クリプトベースのクライアントのみをサポートします。

MSCHAP バージョン 2 の前提条件

- **interface** コマンドを使用してインターフェイス タイプを設定し、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。

- **encapsulation** コマンドを使用して、PPP をカプセル化するためのインターフェイスを設定します。
- クライアントのオペレーティング システムが MSCHAP V2 のすべての機能をサポートしていることを確認してください。
- Cisco IOS リリース 12.4(6)T のパスワード エージング機能は、クリプトベースのクライアントの RADIUS 認証のみをサポートします。
- RADIUS サーバーが送信する認証失敗属性を MSCHAP バージョン 2 機能が正しく解釈していることを確認するには、**ppp max-bad-auth** コマンドを設定し、認証のリトライ回数を 2 回以上に設定する必要があります。

また、 **radius server vsa send authentication** コマンドを設定し、RADIUS クライアントがベンダー固有属性を RADIUS サーバーに送信できるようにする必要があります。パスワード変更機能は、RADIUS 認証のみでサポートされています。

- Microsoft Windows 2000、Microsoft Windows XP、および Microsoft Windows NT のオペレーティング システムには、パスワード変更機能の動作を妨げる既知の注意事項があります。次の URL で Microsoft のパッチをダウンロードする必要があります。

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q326770

これらのタスクの実行の詳細については、『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』の「PPP Configuration」を参照してください。RADIUS サーバで認証を設定する必要があります。RADIUS サーバでの RADIUS 認証の設定の詳細については、ベンダー固有のマニュアルを参照してください。

MSCHAP バージョン 2 の制約事項

- MSCHAP V2 の認証は、MSCHAP V1 の認証と互換性がありません。
- パスワード変更オプションは RADIUS 認証のみでサポートされており、ローカル認証では使用できません。

MSCHAP バージョン 2 の概要

MSCHAP V2 の認証は、Microsoft Windows 2000 オペレーティング システムが使用するデフォルトの認証方式です。この認証方式をサポートする Cisco ルータを使用すると、Microsoft Windows 2000 オペレーティング システムのユーザは、クライアントで認証方式を設定せずにリモートの PPP セッションを確立できます。

MSCHAP V2 の認証では、MSCHAP V1 または標準の CHAP 認証では使用できない追加機能が導入されました。それは、パスワードの変更機能です。パスワード変更機能を使用すると、パスワードが失効したことを RADIUS サーバがレポートした場合に、クライアントがアカウントのパスワードを変更できます。

（注） MSCHAP V2 の認証は更新バージョンの MSCHAP です。これは、MSCHAP バージョン 1（V1）と似ていますが、互換性はありません。MSCHAP V2 では、ピアとパスワード変更機能の間の相互認証が導入されました。

MSCHAP バージョン 2 の設定方法

MSCHAP V2 の認証の設定

ローカル認証または RADIUS 認証で MSCHAP V2 認証を受け入れるように NAS を設定し、RADIUS 認証の認証失敗属性およびベンダー固有の RADIUS 属性を適切に解釈できるようにするには、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。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server vsa send authentication**
4. **interface** *type number*
5. **ppp max-bad-auth** *number*
6. **ppp authentication ms-chap-v2**
7. **end**

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	**radius-server vsa send authentication** 例： `Device(config)# radius-server vsa send authentication`	ベンダー固有属性を認識して使用するように NAS を設定します。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 1/0/1`	インターフェイス タイプを設定し、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 5	**ppp max-bad-auth** *number* 例： `Device(config-if)# ppp max-bad-auth 2`	認証が失敗した直後、または指定された認証のリトライ回数の範囲内である場合にはリセットするように、ポイントツーポイント インターフェイスを設定します。 • *number* 引数のデフォルト値は 0 秒（即座に実行）です。 • 範囲は 0 ～ 255 です。 （注） NAS が認証失敗属性を解釈できるように、*number* 引数の値には最低でも 2 を設定する必要があります。
ステップ 6	**ppp authentication ms-chap-v2** 例： `Device(config-if)# ppp authentication ms-chap-v2`	NAS で MSCHAP V2 認証をイネーブルにします。

ステップ 7	**end**
	例：
	`Device(config-if)#`
	`end`
		特権 EXEC モードに戻ります。

MSCHAP V2 設定の確認

MSCHAP バージョン 2 機能が正しく設定されているかどうかを確認するには、次の手順を実行します。

手順の概要

1. **show running-config interface** *type number*
2. **debug ppp negotiation**
3. **debug ppp authentication**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show running-config interface** *type number* 例： `Device# show running-config interface Asynch65`	MSCHAP V2 の設定が、指定されたインターフェイスの認証方式であることを確認します。
ステップ 2	**debug ppp negotiation** 例： `Device# debug ppp negotiation`	MSCHAP V2 のネゴシエーションが成功していることを確認します。
ステップ 3	**debug ppp authentication** 例： `Device# debug ppp authentication`	MSCHAP V2 認証が成功していることを確認します。

クリプトベースのクライアントのパスワード エージングの設定

AAA セキュリティ サービスにより、さまざまなログイン認証方式を容易に実行できるようになります。**aaa authentication login** コマンドを使用すると、サポートされているログイン認証方式のいずれを使用するかに関係なく、AAA 認証が有効になります。 **aaa authentication login** コマンドを使用すると、ログイン時に試行する認証方式リストを 1 つまたは複数作成できます。これらのリストは、**login authentication** ライン コンフィギュレーション コマンドによって適用されます。

RADIUS サーバが新しいパスワードを要求すると、AAA はクリプト クライアントにクエリーを実行し、今度はユーザに新しいパスワードを入力するように求めます。

クリプトベースのクライアントにログイン認証とパスワード エージングを設定するには、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。

（注） AAA のパスワード失効インフラストラクチャは、パスワードが失効したことを Easy VPN に通知し、ユーザがパスワードを変更するための一般的な方法を提供します。RADIUS サーバのドメイン削除機能と AAA のパスワード失効のサポートをうまく組み合わせて使用してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*]
5. **crypto map** *map-name* **client authentication list** *list-name*

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	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルに有効にします。
ステップ 4	**aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*] 例： `Device(config)# aaa authentication login userauthen passwd-expiry group radius`	ローカルの認証リストでクリプトベースのクライアントのパスワード エージングをイネーブルにします。
ステップ 5	**crypto map** *map-name* **client authentication list** *list-name* 例： 例： `Device(config)# crypto map clientmap client authentication list userauthen`	既存のクリプトマップで、ユーザ認証（認証方式のリスト）を設定します。

設定例

ローカル認証の設定の例

次の例では、非同期インターフェイスに PPP を設定し、ローカルで MSCHAP V2 認証をイネーブルにします。

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
```

```
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  username client password secret
```

RADIUS 認証の設定の例

次の例では、非同期インターフェイスに PPP を設定し、RADIUS を使用して MSCHAP V2 認証をイネーブルにします。

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  exit
aaa authentication ppp default group radius
 radius-server host 10.0.0.2 255.0.0.0
 radius-server key secret
 radius-server vsa send authentication
```

クリプト認証を使用したパスワード エージングの設定の例

次の例では、クリプトベースのクライアントを持つ AAA を使用して、パスワード エージングを設定します。

```
aaa authentication login userauthen passwd-expiry group radius
!
aaa session-id common
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group 3000client
 key cisco123
 dns 10.1.1.10
 wins 10.1.1.20
 domain cisco.com
 pool ippool
 acl 153
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
 set transform-set myset
!
crypto map clientmap client authentication list userauthen
!
radius-server host 10.140.15.203 auth-port 1645 acct-port 1646
radius-server domain-stripping prefix-delimiter $
radius-server key cisco123
radius-server vsa send authentication
radius-server vsa send authentication 3gpp2
```

```
!
end
```

その他の参考資料

ここでは、MSCHAP バージョン 2 の機能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
PPP インターフェイスの設定	『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』の「PPP Configuration」
シスコのネットワーキング装置の設定および管理に必要なタスクとコマンドの説明	『*Cisco IOS Dial Technologies Command Reference*』
IOS セキュリティ コマンドの一覧	『*Cisco IOS Security Command Reference*』
AAA を使用した PPP 認証の設定	『*Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T』の「Configuring Authentication」モジュールの「Configuring PPP Authentication Using AAA」
RADIUS 認証の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T』の「Configuring RADIUS」モジュール

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	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
RFC 1661	ポイントツーポイント プロトコル（*PPP*）
RFC 2548	『*Microsoft Vendor-specific RADIUS Attributes*』
RFC 2759	「*Microsoft PPP CHAP Extensions, Version 2*」

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

MSCHAP バージョン 2 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 : MSCHAP* バージョン *2* の機能情報

機能名	リリース	機能情報
MSCHAP バージョン 2	Cisco IOS XE Release 3.9S	MSCHAP バージョン 2 機能を使用すると、Cisco ルータは、Microsoft Windows オペレーティング システムを使用するコンピュータとネットワーク アクセス サーバ（NAS）間の PPP 接続にマイクロソフト チャレンジ ハンドシェイク認証プロトコル バージョン 2（MSCHAP V2）の認証を使用できます。 次のコマンドが導入または変更されました。**aaa authentication login** および **ppp authentication ms-chap-v2.**

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。