APPENDIX **B**

ネットワーク アクセス フロー

この付録では、RADIUS ベースの拡張認証プロトコル（EAP）と EAP 以外のプロトコルを使用した Cisco Identity Services Engine（ISE）の認証フローについて説明します。

認証とは、ユーザ情報を検証してユーザ ID を確認することです。従来の認証方式では、名前とある決まったパスワードが使用されていました。さらに安全な方式では、チャレンジ ハンドシェイク認証プロトコル（CHAP）、ワンタイム パスワード（OTP）、および高度な EAP ベースのプロトコルの内部で使用されるような暗号化技術を使用します。Cisco ISE は、これらのさまざまな認証方式をサポートしています。

認証と許可には基本的な暗黙の関係があります。ユーザに与えられる許可特権が多くなればなるほど、それに応じて認証を強化する必要があります。Cisco ISE では、さまざまな認証方式を提供することにより、この関係がサポートされています。

最もよく使用され、単純で、コストのかからない認証方式は、ユーザ名とパスワードを使用することです。この方式の欠点は、ユーザ名やパスワードの情報が簡単に第三者に伝えられたり、推測または不正に取得されたりする可能性がある点です。単純な暗号化されていないユーザ名とパスワードを使用する方法は、強力な認証方式とは考えられていませんが、インターネット アクセスなど、許可または特権レベルが低い場合は十分に要件を満たす可能性があります。

ネットワーク上でパスワードが不正に取得される危険性を低減するには、暗号化を使用する必要があります。RADIUS などのクライアント/サーバ アクセス コントロール プロトコルでは、パスワードを暗号化することにより、ネットワーク内でパスワードが不正に取得される事態を防止します。ただし、RADIUS は認証、許可、アカウンティング（AAA）クライアントと Cisco ISE との間でだけ動作します。認証プロセスでは、このポイントの前で、許可されていないユーザが次のようなセットアップで暗号化されていないパスワードを入手する可能性があります。

- 電話回線を介してダイヤルアップ接続を行うエンドユーザ クライアントとの間の通信
- ネットワーク アクセス サーバで終了する ISDN 回線
- エンドユーザ クライアントとホスティング デバイスの間の Telnet セッションを介して行われる通信

RADIUS は、クライアント/サーバ プロトコルです。リモート アクセス サーバは、このプロトコルを使用して中央サーバと通信してダイヤルイン ユーザを認証し、要求されたシステムまたはサービスへのアクセスを許可します。RADIUS を使用すると、すべてのリモート サーバが共有できる中央データベースでユーザ プロファイルを管理できます。このプロトコルはセキュリティを向上させます。また、このプロトコルを使用して、単一の管理ネットワーク ポイントで適用されるポリシーを設定できます。

RADIUS は、Cisco ISE の RADIUS クライアントとしても機能し、リモート RADIUS サーバへの要求をプロキシ処理します。また、アクティブ セッション中に許可変更（CoA）アクティビティを提供します。

Cisco ISE では、RFC 2865 と、その仕様および拡張仕様に記載されている一般的な RADIUS 属性の包括的なサポートに従って、RADIUS プロトコルのフローがサポートされます。Cisco ISE では、Cisco ISE ディクショナリで定義されているベンダーだけを対象に、ベンダー固有属性の解析がサポートされます。ディクショナリの詳細については、「ディクショナリおよびディクショナリ属性」（P.7-1）を参照してください。

RADIUS インターフェイスでは、RFC 2865 で定義されている次の属性データ型がサポートされます。

- テキスト（Unicode Transformation Format（UTF））
- 文字列（バイナリ）
- アドレス（IP）
- 整数
- 時刻

ネットワーク アクセスの使用例

ネットワーク アクセスでは、ホストはネットワーク デバイスに接続し、ネットワーク リソースの使用を要求します。ネットワーク デバイスは、新しく接続されたホストを識別し、転送方式として RADIUS プロトコルを使用して、ユーザの認証および許可を Cisco ISE に要求します。

Cisco ISE では、RADIUS プロトコルを使用して転送されるプロトコルに応じて、次のカテゴリのネットワーク アクセス フローがサポートされます。

- 「EAP を使用しない RADIUS ベースのプロトコル」（P.B-2）
- 「RADIUS ベースの EAP プロトコル」（P.B-5）

EAP を使用しない RADIUS ベースのプロトコル

EAP を含まない RADIUS ベースのプロトコルは、次のとおりです。

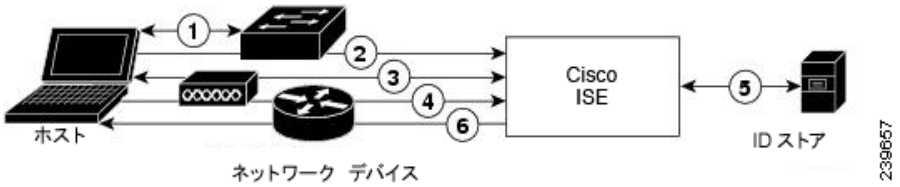
- パスワード認証プロトコル（PAP）
- CHAP
- Microsoft Challenge Handshake Authentication Protocol version 1（MS-CHAPv1）
- MS-CHAP バージョン 2（MS-CHAPv2）

ここでは、EAP 認証を使用しない RADIUS ベースのフローについて説明します。PAP 認証を使用する RADIUS ベースのフローは、次のプロセスで発生します。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスが RADIUS Access-Request を Cisco ISE に送信します。この要求には、使用する特定のプロトコル（PAP、CHAP、MS-CHAPv1、または MS-CHAPv2）に適した RADIUS 属性が含まれます。
3. Cisco ISE では、ID ストアを使用してユーザ クレデンシャルを検証します。
4. RADIUS 応答（Access-Accept または Access-Reject）がネットワーク デバイスに送信されて、決定が適用されます。

図 B-1 に、EAP を使用しない RADIUS ベースの認証を示します。

図 B-1　EAP を使用しない RADIUS ベースの認証



ここでは、Cisco ISE でサポートされる、EAP 以外のプロトコルについて説明します。次のトピックを扱います。

- 「パスワード認証プロトコル」（P.B-3）
- 「チャレンジ ハンドシェイク認証プロトコル」（P.B-4）
- 「Microsoft Challenge Handshake Authentication Protocol Version 1」（P.B-4）
- 「Microsoft Challenge Handshake Authentication Protocol Version 2」（P.B-4）

パスワード認証プロトコル

PAP では、ユーザが双方向ハンドシェイクを使用して ID を確立できる単純な方法が提供されます。PAP パスワードは共有秘密を使用して暗号化されるため、最もセキュリティ レベルの低い認証プロトコルです。

Cisco ISE では、ID ストアに対してユーザ名とパスワードのペアをチェックし、最終的にその認証を確認するか、接続を終了します。

PAP は、反復的な試行錯誤攻撃に対する保護がほとんどないため、確実な認証方式ではありません。

PAP 認証フローを使用する RADIUS には、試行の成功と失敗のロギングが含まれます。

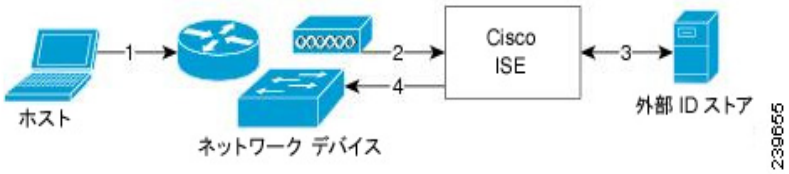
RADIUS PAP 認証

Cisco ISE では、異なるセキュリティ レベルを同時に使用して、さまざまな要件に対応できます。PAP は双方向ハンドシェイク手順を適用します。認証に成功した場合、Cisco ISE は確認応答を返します。認証に失敗した場合、Cisco ISE は接続を終了するか、認証の要求元にもう一度チャンスを与えます。

認証の要求元が、試行の頻度とタイミングを総合的に制御します。したがって、より強力な認証方式を使用できるサーバは、PAP よりも前にその方式のネゴシエーションを提案します。PAP は RFC 1334 で定義されています。

図 B-2 に、PAP 認証を使用した RADIUS を示します。

図 B-2　PAP 認証を使用する RADIUS



1. ホストがネットワークに接続します。ホストに応じて任意の通信プロトコルを使用できます。
2. ネットワーク デバイスが RADIUS Access-Request を Cisco ISE に送信します。
3. Cisco ISE では、外部 ID ストアを使用してユーザ クレデンシャルを検証します。
4. RADIUS 応答（Access-Accept または Access-Reject）がネットワーク デバイスに送信されて、決定が適用されます。

Cisco ISE では、RADIUS UserPassword 属性に基づく標準の RADIUS PAP 認証がサポートされます。RADIUS PAP 認証は、すべての ID ストアと互換性があります。

チャレンジ ハンドシェイク認証プロトコル

CHAP は、応答時に一方向の暗号化を使用するチャレンジ/レスポンス方式です。CHAP を使用することで、Cisco ISE は、セキュリティ レベルの高い順からセキュリティ暗号化方式をネゴシエートし、プロセス中に伝送されるパスワードを保護します。CHAP パスワードは再利用が可能です。Cisco ISE 内部データベースを認証に使用している場合は、PAP または CHAP のどちらかを使用できます。CHAP は、Microsoft ユーザ データベースでは使用できません。RADIUS PAP と比較した場合、エンドユーザ クライアントから AAA クライアントに通信するときに CHAP を使用すると、パスワードが暗号化されるため、高いセキュリティ レベルを確保できます。

Cisco ISE では、RADIUS ChapPassword 属性に基づく標準の RADIUS CHAP 認証がサポートされます。Cisco ISE では、外部 ID ストアを使用した RADIUS CHAP 認証だけがサポートされます。

Microsoft Challenge Handshake Authentication Protocol Version 1

Cisco ISE では、RADIUS MS-CHAPv1 認証およびパスワード変更機能がサポートされます。RADIUS MS-CHAPv1 には、Change-Password-V1 と Change-Password-V2 という 2 つのバージョンのパスワード変更機能が含まれます。

（注） Cisco ISE では、RADIUS MS-CHAP-CPW-1 属性に基づく Change-Password-V1 はサポートされず、MS-CHAP-CPW-2 属性に基づく Change-Password-V2 だけがサポートされます。

RADIUS MS-CHAPv1 認証およびパスワード変更機能は、次の ID ソースでサポートされます。

- 内部 ID ストア
- Microsoft Active Directory ID ストア

Microsoft Challenge Handshake Authentication Protocol Version 2

RADIUS MS-CHAPv2 認証およびパスワード変更機能は、次の ID ソースでサポートされます。

- 内部 ID ストア
- Active Directory ID ストア

RADIUS ベースの EAP プロトコル

EAP では、さまざまな認証タイプをサポートする拡張可能なフレームワークが提供されます。ここでは、Cisco ISE でサポートされる EAP 方式について説明します。次のトピックを扱います。

- Extensible Authentication Protocol-Message Digest 5
- Lightweight Extensible Authentication Protocol

（注） 上記にリストした方式は、証明書を使用しない単純な EAP 方式です。

- 保護拡張認証プロトコル/EAP-MS-CHAPv2
- 保護拡張認証プロトコル/EAP-GTC
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling/EAP-MS-CHAPv2
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling/EAP-GTC

（注） 上記にリストした方式は、クライアントが Cisco ISE サーバ証明書を使用してサーバ認証を実行する EAP 方式です。

上記にリストした方式とは別に、サーバ認証とクライアント認証の両方に証明書を使用する EAP 方式があります。

認証プロセスで EAP が使用される場合は常に、そのプロセスよりも、具体的にどの EAP 方式（および該当する場合は内部方式）を使用する必要があるかを決定するネゴシエーション フェーズが先行します。EAP ベースの認証は、次のプロセスで発生します。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスが EAP 要求をホストに送信します。
3. ホストは、EAP 応答によって、ネットワーク デバイスに応答します。
4. ネットワーク デバイスは、ホストから受信した EAP 応答を RADIUS Access-Request 内に（EAP-Message RADIUS 属性を使用して）カプセル化し、RADIUS Access-Request を Cisco ISE に送信します。
5. Cisco ISE は、RADIUS パケットから EAP 応答を抽出して新しい EAP 要求を作成し、この EAP 要求を RADIUS Access-Challenge 内に（この場合も EAP-Message RADIUS 属性を使用して）カプセル化し、ネットワーク デバイスに送信します。
6. ネットワーク デバイスは、EAP 要求を抽出し、ホストへ送信します。

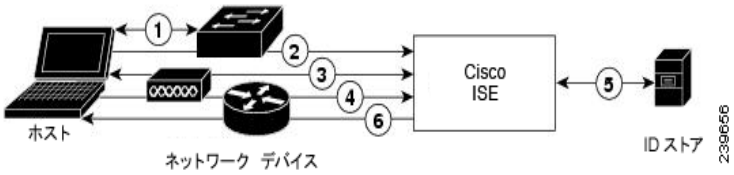
この方法で、ホストと Cisco ISE は間接的に EAP メッセージを交換します（EAP メッセージは、RADIUS を使用して転送され、ネットワーク デバイスを介して渡されます）。この方法で交換される EAP メッセージの最初のセットによって、特定の EAP 方式がネゴシエートされます。その後、認証を実行する場合に、この EAP 方式が使用されます。

その後交換される EAP メッセージは、実際の認証の実行に必要なデータを伝送するために使用されます。ネゴシエートされた特定の EAP 認証方式で必要な場合、Cisco ISE では ID ストアを使用してユーザ クレデンシャルを確認します。

Cisco ISE では、認証が成功か失敗かを決定した後、EAP-Success または EAP-Failure メッセージを、RADIUS Access-Accept または Access-Reject メッセージ内にカプセル化された状態で、ネットワーク デバイスに（最終的にはホストにも）送信します。

図 B-3 に、EAP を使用する RADIUS ベースの認証を示します。

図 B-3　EAP を使用する RADIUS ベースの認証



この項では、次のトピックを扱います。

- 「Extensible Authentication Protocol-Message Digest 5」（P.B-6）
- 「Lightweight Extensible Authentication Protocol」（P.B-6）
- 「保護拡張認証プロトコル」（P.B-6）
- 「Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling」（P.B-8）

Extensible Authentication Protocol-Message Digest 5

Extensible Authentication Protocol-Message Digest 5（EAP-MD5）では、一方向のクライアント認証が提供されます。サーバは、クライアントにランダム チャレンジを送信します。クライアントは、チャレンジとそのパスワードを MD5 でハッシュすることにより、その ID を証明します。中間者がチャレンジと応答を見ることができるため、EAP-MD5 は、公開メディアで使用される場合にはディクショナリ攻撃に対して脆弱です。サーバ認証が行われないため、スプーフィングに対しても脆弱です。Cisco ISE では、ISE 内部 ID ストアに対する EAP-MD5 認証がサポートされます。EAP-MD5 プロトコルを使用している場合は、ホスト ルックアップもサポートされます。ホスト ルックアップの詳細については、「表 16-3 許可されるプロトコル サービス」（P.16-15）を参照してください。

Lightweight Extensible Authentication Protocol

Cisco ISE では現在、Lightweight Extensible Authentication Protocol（LEAP）を Cisco Aironet ワイヤレス ネットワーキングに対してだけ使用します。このオプションを有効にしないと、LEAP 認証を実行するように設定された Cisco Aironet エンドユーザ クライアントは、ネットワークにアクセスできなくなります。Cisco Aironet エンドユーザ クライアントすべてが Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）などの異なる認証プロトコルを使用する場合は、このオプションを無効にすることを推奨します。

（注）　[ネットワーク デバイス（Network Devices）] セクションで RADIUS（Cisco Aironet）デバイスとして定義された AAA クライアントを使用してユーザがネットワークにアクセスする場合は、LEAP、EAP-TLS、またはその両方を有効にする必要があります。これ以外の場合、Cisco Aironet ユーザは認証を受けることができません。

保護拡張認証プロトコル

保護拡張認証プロトコル（PEAP）では、相互認証が提供され、脆弱なユーザ クレデンシャルの機密性と整合性が保証されます。またこのプロトコルでは、自身をパッシブ（盗聴）およびアクティブ（中間者）攻撃から保護し、セキュアに暗号キー関連情報を生成します。PEAP は、IEEE 802.1X 標準および RADIUS プロトコルと互換性があります。Cisco ISE では、Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol（EAP-MS-CHAP）、Extensible Authentication Protocol-Generic Token Card（EAP-GTC）、および EAP-TLS 内部方式で PEAP バー

ジョン 0（PEAPv0）と PEAP バージョン 1（PEAPv1）がサポートされます。Cisco Secure Services Client（SSC）サプリカントでは、Cisco ISE でサポートされるすべての PEAPv1 内部方式がサポートされます。

PEAP の使用の利点

PEAP を使用すると、次のような利点があります。

- PEAP は、広く実装されセキュリティが細部にわたって確認された TLS に基づいています。
- キーを生成しない方式に対しては、キーを確立します。
- トンネル内で ID を送信します。
- 内部方式の交換と結果メッセージを保護します。
- フラグメンテーションがサポートされます。

サポートされるサプリカント

PEAP では、次のサプリカントがサポートされます。

- Microsoft Built-In Clients 802.1X XP
- Microsoft Built-In Clients 802.1X Vista
- Cisco Secure Services Client（SSC）Release 4.0
- Cisco SSC Release 5.1
- Funk Odyssey Access Client 4.72
- Intel 12.4.0.0

PEAP プロトコルのフロー

PEAP カンバセーションは、次の 3 つの部分に分かれます。

1. Cisco ISE とピアが TLS トンネルを構築します。Cisco ISE は自身の証明書を提示しますが、ピアは提示しません。ピアと Cisco ISE はキーを作成して、トンネル内のデータを暗号化します。
2. 内部方式によって、次のようにトンネル内のフローが決定されます。
   - EAP-MS-CHAPv2 内部方式 : EAP-MS-CHAPv2 パケットは、ヘッダーなしでトンネル内を移動します。ヘッダーの先頭のバイトにタイプ フィールドが含まれます。EAP-MS-CHAPv2 内部方式では、パスワード変更機能がサポートされます。ユーザがパスワード変更を試行できる回数を Cisco ISE ユーザ インターフェイスで設定できます。ユーザ認証試行は、この数値によって制限されます。
   - EAP-GTC 内部方式 : PEAPv0 と PEAPv1 の両方で、EAP-GTC 内部方式がサポートされます。サポートされるサプリカントでは、EAP-GTC 内部方式を使用する PEAPv0 はサポートされません。EAP-GTC では、パスワード変更機能がサポートされます。ユーザがパスワード変更を試行できる回数を Cisco ISE ユーザ インターフェイスで設定できます。ユーザ認証試行は、この数値によって制限されます。
   - EAP-TLS 内部方式 : Windows 組み込みサプリカントでは、トンネルが確立された後のメッセージのフラグメンテーションはサポートされず、このことは EAP-TLS 内部方式に影響を与えます。Cisco ISE では、トンネルが確立された後の外部 PEAP メッセージのフラグメンテーションはサポートされません。トンネルの確立中、フラグメンテーションは PEAP のマニュアルで指定されているとおりに動作します。PEAPv0 では EAP-TLS パケットのヘッダーが削除され、PEAPv1 では EAP-TLS パケットがそのまま送信されます。
   - Extensible Authentication Protocol-type, length, value（EAP-TLV）拡張 : EAP-TLV パケットはそのまま送信されます。EAP-TLV パケットは、トンネル内をヘッダー付きで移動します。
3. カンバセーションが内部方式に到達した場合、保護された成功と失敗の確認応答があります。

（注） クライアント EAP メッセージは常に RADIUS Access-Request メッセージで送信され、サーバ EAP メッセージは常に RADIUS Access-Challenge メッセージで送信されます。EAP-Success メッセージは、常に RADIUS Access-Accept メッセージで送信されます。EAP-Failure メッセージは、常に RADIUS Access-Reject メッセージで送信されます。クライアント PEAP メッセージをドロップすると、RADIUS クライアント メッセージがドロップされます。

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）は、相互認証を提供する認証プロトコルであり、共有秘密を使用してトンネルを確立します。このトンネルは、パスワードに基づく弱い認証方式を保護するために使用されます。Protected Access Credentials（PAC）キーと呼ばれる共有秘密は、トンネルのセキュリティを確保するときにクライアントとサーバを相互認証するために使用されます。

EAP-FAST の利点

EAP-FAST は、他の認証プロトコルに比べて次の利点があります。

- 相互認証：EAP サーバはピアの ID と信頼性を確認できる必要があり、ピアは EAP サーバの信頼性を確認できる必要があります。
- パッシブ ディクショナリ攻撃に対する耐性：多くの認証プロトコルでは、ピアから EAP サーバにパスワードがクリア テキストまたはハッシュとして明示的に提供される必要があります。
- 中間者攻撃に対する耐性：相互認証された保護トンネルの確立時に、プロトコルは、ピアと EAP サーバとの間のカンバセーションに攻撃者が情報を挿入することを防ぐ必要があります。
- MS-CHAPv2 や汎用トークン カード（GTC）などの多くの異なるパスワード認証インターフェイスをサポートできる柔軟性：EAP-FAST は、同じサーバで複数の内部プロトコルをサポートできる拡張可能なフレームワークです。
- 効率性：無線メディアを使用する場合、ピアは計算資源と電源リソースを制限されます。EAP-FAST では、ネットワーク アクセス通信の計算を軽量化できます。
- 認証サーバのユーザごとの認証状態要件の最小化：大規模な展開では、通常、多くのサーバが多くのピアに対する認証サーバとして機能する必要があります。ユーザ名とパスワードを使用してネットワークにアクセスするのと同じように、ピアが同じ共有秘密を使用してトンネルのセキュリティを確保することも強く推奨されます。EAP-FAST により、サーバでキャッシュおよび管理する必要があるユーザごとおよびデバイスごとの状態を最小にすることができ、ピアによる強力な単一共有秘密の使用が容易になります。

EAP-FAST フロー

EAP-FAST プロトコルのフローは常に、次のフェーズを組み合わせたものになります。

- プロビジョニング フェーズ：これは EAP-FAST のフェーズ 0 です。このフェーズでは、Cisco ISE とピアとの間で共有される、PAC と呼ばれる一意の強力な秘密を使用して、ピアがプロビジョニングされます。
- トンネル確立フェーズ：PAC を使用して新しいトンネル キーを確立することによって、クライアントとサーバを相互認証します。トンネル キーはその後、残りのカンバセーションを保護するために使用され、メッセージの機密性と信頼性を提供します。
- 認証フェーズ：認証がトンネル内で処理され、セッション キーの生成と保護された終了が行われます。

Cisco ISE では、EAP-FAST バージョン 1 および 1a がサポートされます。