APPENDIX **B**

ACS 5.2 での認証

認証とは、ユーザ情報を検証してそのユーザの 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、Challenge Authentication Handshake Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）、OTP、および高度な EAP ベース 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。ACS は、これらのさまざまな認証方式をサポートしています。

認証と認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認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。ACS 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。

認証方式の検討

ユーザ名とパスワードは、最も一般的かつ単純で、低コストな認証方式です。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による認証は確実な認証メカニズムとは言えませんが、インターネット アクセスなどのように認可レベルまたは特権レベルが低い場合は十分に対応可能です。

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。TACACS+ および RADIUS などのクライアント/サーバ アクセス制御プロトコルでは、パスワードを暗号化して、ネットワーク内でパスワードが不正に取得される事態の発生を防止します。

ただし、TACACS+ と RADIUS は AAA クライアントと ACS 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、認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 サーバで終端する Integrated Services Digital Network（ISDN; サービス総合デジタル ネットワーク）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

認証とユーザ データベース

ACS は、さまざまなユーザ データベースをサポートしています。ACS 内部データベース以外にも、次のような外部ユーザ データベースをサポートしています。

- Windows Active Directory

- LDAP
- RSA SecurID サーバ
- RADIUS ID サーバ

この付録では、次の内容について説明します。

- EAP を含まない RADIUS ベースの認証：
  - 「PAP」（P.B-2）
  - 「CHAP」（P.B-31）
  - MSCHAPv1
  - 「EAP-MSCHAPv2」（P.B-30）
- RADIUS を使用して転送される EAP プロトコル ファミリ。さらに次のように分類できます。
  - 証明書を使用しない単純な EAP プロトコル。

    EAP-MD5：詳細については、「EAP-MD5」（P.B-5）を参照してください。

    LEAP：詳細については、「LEAP」（P.B-31）を参照してください。
  - TLS ハンドシェイクを伴い、クライアントが ACS サーバ証明書を使用してサーバ認証を実行する EAP プロトコル。

    PEAP/EAP-MSCHAPv2 と PEAP/EAP-GTC のいずれかの内部方式を使用する PEAP：詳細については、「PEAPv0/1」（P.B-14）を参照してください。

    EAP-FAST/EAP-MSCHAPv2 と EAP-FAST/EAP-GTC のいずれかの内部方式を使用する EAP-FAST：詳細については、「EAP-FAST」（P.B-18）を参照してください。
  - 完全に証明書ベースの EAP プロトコル。このプロトコルでは、TLS ハンドシェイクによってサーバ認証とクライアント認証の両方に証明書が使用されます。

    EAP-TLS：詳細については、「EAP-TLS」（P.B-6）を参照してください。
- 「証明書アトリビュート」（P.B-32）
- 「マシン認証」（P.B-34）
- 「認証プロトコルと ID ストアの互換性」（P.B-35）

サプリカントに関する既知の問題のリストについては、次の URL を参照してください。
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/release/notes/acs_52_rn.html#wp123862

PAP

パスワード認証プロトコル（PAP）は、ユーザが双方向ハンドシェイクを使用してその ID を設定する単純な方式を提供します。PAP パスワードは共有秘密情報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。

ACS は、認証を確認するか接続を終了するまで、ID とパスワードのペアを外部データベースである ID ストアと比較してチェックします。

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。

（注）　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。

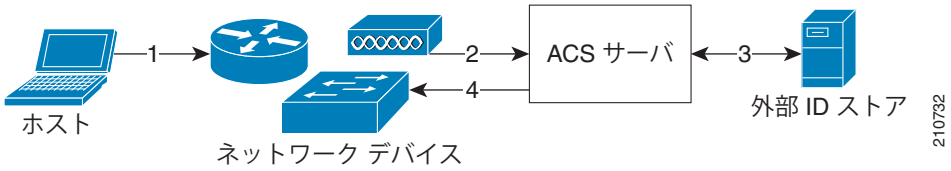
RADIUS PAP 認証

ACS 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、ACS は確認応答を返します。認証に失敗した場合、ACS 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-1 に、PAP 認証を使用した RADIUS を示します。

図 B-1　PAP 認証を使用した RADIUS の使用例



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。	**3**	ACS が外部 ID ストアを使用してユーザのクレデンシャルを確認します。
2	ネットワーク デバイスが RADIUS アクセス要求を ACS に送信します。	**4**	RADIUS 応答（Access-Accept または Access-Reject）が、決定を適用するネットワーク デバイスに送信されます。

EAP

Extensible Authentication Protocol（EAP）は、無線ネットワークとポイントツーポイント接続のための認証フレームワークです。EAP では、複数の認証方式がサポートされ、目的の認証方式のネゴシエーションに関する一般的な機能と規則が提供されます。

- サーバ認証要求
- クライアント認証応答
- サーバの成功した認証結果
- サーバの失敗した認証結果
- 整合性とセキュリティの条件を満たさない場合のクライアント パケットのサイレントな廃棄
- サーバが開始する EAP 方式ネゴシエーションの規則
- メッセージ シーケンシングと、要求に対する応答のトラッキング
- 再送信

EAP はロックステップ プロトコルです。最初の要求のあと、ACS はクライアントから有効な応答を受信するまで新しい要求を送信できません。

ACS 5.2 では、EAP は RADIUS プロトコルにカプセル化されています。着信および発信 EAP メッセージは、RADIUS EAP-Message アトリビュート（79）に格納されます。特定の EAP メッセージのサイズが最大の RADIUS アトリビュート データ サイズ（253 バイト）よりも大きい場合は、1 つの RADIUS パケットに複数の EAP-Message アトリビュートを含めることができます。

RADIUS State アトリビュート（24）は現在の EAP セッション参照情報を格納し、ACS は実際の EAP セッション データを格納します。

EAP 標準については次の資料で説明されています。

- RFC 3748：Extensible Authentication Protocol（EAP）
- RFC 3579：RADIUS Support For Extensible Authentication Protocol（EAP）

EAP プロセスでは、次の処理が行われます。

1. ホストがネットワークに接続したときに、ネットワーク デバイスが EAP 要求をホストに送信します。
2. ホストが EAP 応答をネットワーク デバイスに送信します。ネットワーク デバイスは、ホストから受信した EAP パケットを RADIUS 要求に埋め込み、EAP サーバとして動作している ACS に送信します。
3. ACS が認証について EAP 方式をネゴシエートします。クライアントは、EAP サーバが提示する EAP 方式に同意するか、Negative Acknowledgment（NAK; 否定応答）で応答して別の EAP 方式のリストを提示できます。サーバとクライアントは、認証のインスタンス化に使用する EAP 方式について合意する必要があります。

表 B-1 に、各タイプの EAP メッセージの EAP コードを示します。

表 B-1　EAP コード

EAP メッセージ タイプ	EAP コード
Accept-request	1
Response	2
Success	3
Failure	4

表 B-2 に、ACS 5.2 でサポートされる EAP 方式を示します。

表 B-2　サポートされる EAP 方式

EAP 方式	説明
EAP-MD5	Message Digest 5 プロトコル。詳細については、「EAP-MD5」（P.B-5）を参照してください。
LEAP	Lightweight Extensible Authentication Protocol。
PEAPv0v1	Protected Extensible Authentication Protocol バージョン 0 およびバージョン 1。詳細については、「PEAPv0/1」（P.B-14）を参照してください。
EAP-FAST	EAP Flexible Authentication via Secured Tunnel（EAP-FAST）プロトコル。詳細については、「EAP-FAST」（P.B-18）を参照してください。
EAP-MSCHAPv2	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。詳細については、「EAP-MSCHAPv2」（P.B-30）を参照してください。

表 B-2　サポートされる EAP 方式（続き）

EAP 方式	説明
EAP-GTC	EAP Generic Token Card。
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security。詳細については、「クレデンシャルのエクスポート」（P.B-11）を参照してください。

ACS では、EAP タイプ ネゴシエーション、メッセージ シーケンシング、メッセージ再送信など、EAP インフラストラクチャがすべてサポートされます。すべてのプロトコルで、大きなメッセージのフラグメンテーションがサポートされます。

ACS 5.2 では、アクセス サービス設定の一部として、認証の EAP 方式を設定します。アクセス サービスの詳細については、第 3 章「ACS 5.x ポリシー モデル」を参照してください。

EAP-MD5

ここでは、次の内容について説明します。

EAP-MD5 の概要

EAP 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。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。

これは、ハッカーがチャレンジと応答を見ることができるためです。サーバ認証が行われないため、偽造に対しても脆弱です。

関連トピック

- 「ホスト ルックアップ」（P.4-13）
- 「エージェントレス ネットワーク アクセスの概要」（P.4-12）

ACS 5.2 での EAP-MD 5 フロー

ACS では、ACS 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」（P.4-13）を参照してください。

関連トピック

- 「認証プロトコルと ID ストアの互換性」（P.B-35）
- 「エージェントレス ネットワーク アクセスの概要」（P.4-12）

EAP-TLS

ここでは、次の内容について説明します。

EAP-TLS の概要

EAP-TLS は、EAP 認証フレームワークの方式の 1 つであり、802.1x および EAP アーキテクチャに基づいています。802.1x および EAP 認証プロセスに関連するコンポーネントは次のとおりです。

- ホスト：エンド エンティティ。つまり、エンドユーザのマシン。
- AAA クライアント：ネットワーク アクセス ポイント。
- 認証サーバ：ACS。

EAP-TLS 標準については次の資料で説明されています。

- RFC 2716：PPP EAP-TLS Authentication Protocol
- RFC 3079：Deriving Keys for use with Microsoft Point-to-Point Encryption（MPPE）

ここでは、次の内容について説明します。

ホストでは、EAP-TLS 認証がサポートされている必要があります。アクセス ポイントでは、802.1x 環境で EAP 認証プロセスがサポートされている必要があります（アクセス ポイントは EAP 認証プロトコル タイプを認識しません）。

関連トピック

- 「CA 証明書の設定」（P.8-60）
- 「証明書ベースのネットワーク アクセス」（P.4-9）
- 「ACS および Cisco TrustSec」（P.4-23）
- 「ACS 5.2 での EAP-TLS フロー」（P.B-13）

ユーザ証明書認証

EAP-TLS は、証明書ベースの認証の相互認証方式です。クライアントとサーバが、デジタル証明書を使用して相互に認証します。認証を成功させるには、証明書がサーバとクライアント上で特定の要件を満たす必要があります。EAP と TLS は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）RFC 標準です。

EAP プロトコルは、初期認証情報、具体的には IEEE 802.1x で確立されている EAP over LAN（EAPOL）のカプセル化を伝達します。TLS は、ユーザ認証とダイナミック短期セッション キー生成に証明書を使用します。

ピアが認証され、セッションが作成されると、情報が一定期間 ACS にキャッシュされます。証明書を追加で交換しなくても、EAP-TLS セッション再開を使用することでセッションを再確立できます。

ACS 5.2 は、EAP-TLS 処理中に使用するサーバ証明書と秘密キーを ACS サーバ上のファイルに保持します。信頼できる認証局（CA）を選択してクライアント証明書に署名できます。

EAP-TLS 認証では、次の 2 つの信頼要素が必要です。

- EAP-TLS ネゴシエーションにおいて、証明書によって署名されているキーペアをユーザが所有していることを RSA 署名検証で確認することによって、エンドユーザの信頼を確立する。

  これによって、エンドユーザが特定のデジタル証明書に対する正当なキー所有者であること、およびその証明書内のユーザ ID に対応していることが確認されます。しかし、ユーザが証明書を所有していることを信頼しても、ユーザ名 / キーペアを確認するに過ぎません。

- 証明書の情報を確認する第三者署名、通常は CA の署名を使用する。第三者による確認は、パスポートのスタンプの確認にあたります。

  パスポートが信頼できるのは、特定の国 / 地域のパスポート発行機関が、そのパスポートを作成する際に行った準備と身元確認が信頼できるためです。ルート証明書の CA の署名がインストールされていることで、デジタル証明書は信頼されます。

ルート証明書の CA の署名のインストールによって提供されるこの第 2 の信頼要素は、必要ない場合もあります。証明書の正当性に対するこのような外部検証が必要ない場合は、ACS 自己署名証明書機能を使用できます。

関係するエンドユーザ クライアントによっては、エンドユーザ クライアント コンピュータ上の信頼できるルート CA 用に、ACS サーバ証明書を発行した CA の CA 証明書がローカル ストレージで必要になる場合もあります。詳細については、「認証局の追加」（P.8-61）を参照してください。

EAP-TLS に準拠した AAA クライアントの例としては、次のものが挙げられます。

- Cisco 802.1x 対応のスイッチ プラットフォーム（Catalyst 6500 シリーズなど）
- Cisco Aironet Wireless ソリューション

EAP-TLS は、セキュアな Cisco Aironet 接続を実現するために、各ユーザ、各接続に固有のダイナミックなセッション キーを生成します。

関連トピック

- 「CA 証明書の設定」（P.8-60）
- 「証明書ベースのネットワーク アクセス」（P.4-9）

PKI 認証

EAP-TLS は、公開キー インフラストラクチャ（PKI）の概念を使用します。

- ホストは、LAN ネットワークに対する認証を行うために有効な証明書を必要とする。
- AAA サーバは、クライアントに対して ID の有効性を示すためにサーバ証明書を必要とする。
- 認証局サーバ インフラストラクチャは、AAA サーバとクライアントに対して証明書を発行する。

SSL/TLS トンネル認証は、両方のピアによって実行され、クライアントによって開始されます。ACS では、トンネルは次のものによって認証できます。

- 両方のピア
- 一方のピア
- クライアントとホストのどちらも行わない

認証なしで構築されているトンネルは匿名トンネルと見なされ、通常は Diffie-Hellman キー交換プロトコルによって構築されます。ACS では、TLS に対して SSL/TLS セッション再開機能がサポートされます。ACS は、トンネル通信の確立に使用されるトンネル キーと暗号を各セッションのキャッシュに保持します。以前のセッションの取得は、クライアントごとに固有のセッション ID に基づいて行われます。

キャッシュ内の各セッションのタイムアウトをプロトコルごとに個別に設定できます。セッションのライフタイムは、カンバセーションの開始時から測定され、TLS セッションの作成時に判断されます。

ACS では、EAP-FAST プロトコルに対して、クライアントとサーバが認識している一般に共有されるキーからのトンネルの確立がサポートされます。2 つのピア間でセキュアに合意されたキーを使用して、トンネルを開くために使用される共有トンネル TLS マスターキーを取得します。このメカニズムでは TLS ネゴシエーションが短くなります。

匿名 Diffie-Hellman トンネルとは、どのピアも自身を認証しない場合にクライアントとサーバ間に完全に匿名のトンネルを確立することを意味します。ACS ランタイムでは、EAP-FAST に対して、定義済み素数と定義済み生成元（2）を使用した匿名 Diffie-Hellman トンネルがサポートされます。匿名 Diffie-Hellman トンネル暗号スイート内ではサーバ認証は行われません。

認証付き Diffie-Hellman トンネルは、匿名 Diffie-Hellman トンネルと同様です。認証付き Diffie-Hellman トンネルの追加要素は、RSA 証明書を通じてピア認証が実行されることです。ACS では、EAP-FAST に対して、サーバが自身の証明書を使用して認証される認証付き Diffie-Hellman トンネルがサポートされます。

内部 EAP 方式に EAP-MSCHAPv2 や EAP-GTC などの他のプロトコルを使用して、トンネル内で追加のクライアント認証が実行されます。

関連トピック

- 「ローカル サーバ証明書の設定」（P.18-14）
- 「CA 証明書の設定」（P.8-60）
- 「証明書認証プロファイルの設定」（P.8-64）

PKI クレデンシャル

ここでは、次の内容について説明します。

PKI の使用方法

ACS では、さまざまな PKI 使用例に対して証明書の使用がサポートされます。主な使用例は、PKI がサーバの認証だけでなくクライアントの認証にも使用される EAP-TLS プロトコルです（PEAP と EAP-FAST もサーバ認証に証明書を使用しますが、クライアント認証は実行しません）。PKI クレデンシャルを使用するその他のプロトコルは、LDAPS、HTTPS 管理プロトコル、SSH、および SFTP です。

TLS 関連 EAP プロトコルでは、単一のローカル証明書を使用して、すべての TLS 関連 EAP プロトコルのサーバを認証します。ローカル証明書ストア内に秘密キーが含まれている任意の証明書から、使用する証明書を選択できます。

HTTPS、SFTP、SSH などのその他のプロトコル、およびメッセージ バス ActiveMQ 認証の場合は、ACS を認証するための単一の証明書を設定する必要があります。ローカル証明書ストア内に秘密キーが含まれている任意の証明書から、使用する証明書を選択できます。TLS 関連 EAP プロトコルと HTTPS 管理プロトコルに対して同じローカル証明書を設定できます。

HTTPS、SFTP、SSH、および ActiveMQ では、自動生成される自己署名証明書をサーバ認証の手段として使用できます。

固定管理証明書

ACS は、自己署名証明書を生成および使用して、Web ブラウザ、HTTPS、ActiveMQ SSH、SFTP などのさまざまな管理プロトコルを識別します。

自己署名証明書は、ACS のインストール時に生成され、ACS データベースの外部にあるファイルにローカルに保持されます。これらの証明書は修正またはエクスポートできません。ただし、インポートされた証明書を管理インターフェイスに割り当てることはできます。

信頼証明書のインポート

ACS では、PEM または DER 形式の X509 証明書ファイルがサポートされています。信頼証明書を信頼証明書ストアに追加できます。ACS は、インポートした証明書が X509 形式に準拠していることを確認し、階層証明書の署名の確認は実行しません。ACS では、Microsoft 社独自の秘密キー形式もサポートされます。

TLS 関連 EAP プロトコルで直接信頼される取得済み証明書は、EAP CTL としてマークできます。信頼証明書ストアは、重複する信頼証明書を許可していません。証明書の拒否の規則は次のとおりです。

- 2 つの証明書が同じサブジェクトを持つことはできない。
- 2 つの証明書が同じ発行元と同じシリアル番号を持つことはできない。

ローカル証明書の取得

ここでは、ACS が PKI クレデンシャルを取得する方式と、ACS ドメイン内の各 ACS サーバに公開キーと秘密キーのペアを設定する方法について説明します。

X509 証明書には、公開キーを含むクレデンシャルと、一緒に送信されるパスワードで保護された秘密キーを保持する PKCS#12 [?10.1] が含まれています。

ACS ドメインには、複数の ACS サーバがある場合があります。各ドメインには、適切なインターフェイスを通じて自身の ID を証明するための PKI キーペアの固有のセットが必要です。

一部のインターフェイスは、サーバの IP に証明書をより適切にバインディングするために、Web インターフェイスに使用される HTTPS ACS サーバ証明書など、ACS を識別する証明書の Common Name（CN; 共通名）に ACS サーバの IP または FQDN が含まれていることを必要とします。

その他のインターフェイスでは、サーバ間で共有できる共通証明書を使用できる可能性がありますが、共通証明書の使用は推奨しません。各 ACS PKI クレデンシャルは、自己署名証明書から、または一般的な認証局（CA）によって署名された証明書から取得できます。

ACS の識別情報を必要とするプロトコルの場合、クライアントは、少なくとも、各 ACS の識別に使用されるすべての ACS サーバ証明書を支配する最小公倍数的な証明書で展開する必要があります。

組織で使用する PKI ポリシーを選択し、ACS ドメイン用に PKI クレデンシャルを設定できます。

設定された証明書とその秘密キーは、ACS マシンの外部では使用しないでください。

関連トピック

- 「ACS サーバ証明書のインポート」（P.B-10）
- 「自己署名証明書の初期生成」（P.B-10）
- 「証明書の生成」（P.B-10）

ACS サーバ証明書のインポート

ACS サーバ証明書を手動でインポートする場合は、証明書ファイル、秘密キーファイル、および PKCS#12 秘密キーの復号化に使用される秘密キー パスワードを指定する必要があります。証明書とその秘密キーおよび秘密キー パスワードは、ローカル証明書ストアに追加されます。暗号化されていない秘密キーの場合、ユーザが指定したパスワードは無視されることがあります。

ACS では、PEM または DER 形式の X509 証明書ファイルがサポートされています。ACS は、インポートした証明書が X509 形式に準拠していることを確認し、階層証明書の署名の確認は実行しません。

証明書のインポート時に、TLS 関連 EAP プロトコルや HTTPS 管理プロトコルなど、ACS サーバ証明書を必要とするプロトコルの証明書を設定できます。

（注）　ACS 5.2 では、証明書ベースの認証に EAP プロトコルと HTTPS 管理プロトコルだけを設定できます。

暗号上の機密情報である入力パスワードと秘密キーは、HTTPS チャネルで渡されます。HTTPS サーバ認証の自己署名証明書など、HTTPS を非認証サーバとともに使用することは、この機密情報を渡すのにセキュアな方法ではありません。

- 「信頼証明書のインポート」（P.B-9）
- 「自己署名証明書の初期生成」（P.B-10）
- 「証明書の生成」（P.B-10）

自己署名証明書の初期生成

自動生成される自己署名証明書は、各 ACS サーバのローカル証明書ストアに配置されます。この証明書は、TLS 関連 EAP プロトコルおよび HTTPS 管理プロトコルの ACS の識別に使用されます。

自己署名証明書は、HTTPS 証明書に必要なマシンのホスト名と同じ CN で生成され、ACS のインストール時に生成されます。

証明書の生成

ACS サーバ証明書は、Web インターフェイスを通じて生成できます。このプロセスの出力は、証明書または証明書要求と、対応する秘密キーおよびパスワードです。生成される秘密キーは、ランダムな 128 ビット以上に基づいて自動生成される比較的強力なパスワードを使用して、暗号化された PKCS#12 として構造化されます。

生成する秘密キーの長さは、512、1024、2048、または 4096 ビットから選択できます。ACS で使用される証明書ダイジェスト アルゴリズムは SHA1 および SHA2 256 ビットです。

（注）　SHA2 256 ビット証明書を管理証明書として使用するには、Windows XP SP3 をインストールします。

ACS サーバ証明書は、Web インターフェイスを通じて生成できます。このプロセスの出力は、証明書または証明書要求と、対応する秘密キーおよびパスワードです。生成される秘密キーは、ランダムな 128 ビット以上に基づいて自動生成される比較的強力なパスワードを使用して、暗号化された PKCS#12 として構造化されます。

生成する秘密キーの長さは、512、1024、2048、または 4096 ビットから選択できます。ACS で使用される証明書ダイジェスト アルゴリズムは SHA1 および SHA2 256 ビットです。

証明書生成には次の 2 種類があります。

- 自己署名証明書生成：ACS では、X.509 証明書と PKCS#12 秘密キーの生成がサポートされます。PKCS#12 の秘密キーの暗号化に使用されるパスフレーズは、より強力なパスワードを自動的に生成し、秘密キーはローカル証明書ストアに隠されます。

  HTTPS 管理プロトコル、TLS 関連 EAP プロトコル、またはその両方に即時に使用するために、新規に生成された証明書を選択できます。

- 証明書要求生成：ACS では、PKCS#12 秘密キーを使用した PKCS#10 証明書要求の生成がサポートされます。要求は、Web インターフェイスを通じてダウンロードされ、REQ 拡張子を持つ PEM 表現でフォーマットする必要があります。

  PKCS#12 の秘密キーの暗号化に使用されるパスフレーズは、より強力なパスワードを自動的に生成し、秘密キーは ACS データベースに隠されます。RA によってオフラインで署名するために、要求ファイルをダウンロードできます。

  RA が要求に署名したあと、返された署名付き証明書を ACS にインストールし、証明書を対応する秘密キーにバインドできます。証明書とその秘密キーのバインディングは自動的に行われます。

  署名された証明書を秘密キーにバインドしたあとで、HTTPS 管理プロトコル、TLS 関連 EAP プロトコル、またはその両方に即時に使用するようにこの証明書をマークできます。

関連トピック

- 「CA 証明書の設定」（P.8-60）
- 「証明書認証プロファイルの設定」（P.8-64）
- 「ACS 5.2 での EAP-TLS フロー」（P.B-13）

クレデンシャルのエクスポート

一般的な信頼証明書、秘密キーあり、またはなしの ACS サーバ証明書、および以前に生成された証明書要求を証明書ストアからエクスポートできます。秘密キーに対する要求はエクスポートできません。*.CER* 拡張子を持つ証明書ファイルをダウンロードできます。ファイル フォーマットは、ACS にインポートされたフォーマットから変更されません。

秘密キーも含む ACS サーバ証明書については、公開証明書を、*.CER* 拡張子を持つ通常の証明書としてダウンロードできます。ファイル フォーマットは維持されます。

証明書要求については、公開要求をエクスポートして、RA に対する証明書要求を再発行できます。要求は REQ 拡張子付きでダウンロードされ、生成時のフォーマットと同じフォーマットになります。

最高の管理者特権を持つ管理者だけが、証明書秘密キーとそのパスワードをエクスポートできます。このようなアクションのセキュリティに関連する警告は、エクスポート操作を承認するために 2 回表示されます。

この二重チェックのあとに、秘密キーファイルを *.PVK* 拡張子としてダウンロードできます。また、秘密キー パスワードを *.PWD* 拡張子としてダウンロードできます。秘密キー ファイルのフォーマットは維持されます。

クレデンシャルの配布

すべての証明書は、すべての ACS ノードに配布されてノード間で共有される ACS データベースに保持されます。ACS サーバ証明書は、特定の証明書を使用する特定のノードに関連付けられて指定されます。

公開証明書は、ACS 配布メカニズムを使用して、秘密キーおよび保護された秘密キー パスワードとともに配布されます。ACS は、保護の方式を実装して、秘密キーの指定対象であるサーバ以外のサーバによって秘密キーが使用されることを防ぎます。この保護メカニズムは、暗号化された秘密キーだけに適用されます。

秘密キーの PKI ポリシーでは、秘密キーの指定対象である ACS サーバに関連付けられていない他のエンティティはその秘密キーを使用できないことになっています。ACS では、指定対象の ACS サーバ マシンの外部で使用される可能性を防ぐために、秘密キーの暗号による保護がサポートされています。

ハードウェアの置換と証明書

ハードウェアに障害が発生した場合は、誤動作をしているノードの代わりに新しいノードが使用されます。誤動作しているノードの証明書はプライマリ サーバの配布済みデータベースから削除され、新しいノードの証明書が、新規に置換されたノードに関連付けられているプライマリに渡されます。

この証明書変更のプロセスは、新しいノードがドメインに登録されたときにハードウェア置換プロセスの一部として実行されます。証明書の配布は、サーバの IP アドレスに基づいて行われます。

暗号機密資料のセキュリティ保護

ACS データベースに格納される PKI 関連のキーにはいくつかの種類があります。これらのキーには、シスコのセキュリティ ベースラインの一部である SEC-RCV-CRED-2 に準拠する必要のあるさまざまな暗号保管要件があります。これらの要件は次のとおりです。

- 通常は証明書内にある公開キーは、クライアントにクリア テキストで渡すために使用され、公開キーだけを含んでいるため、公開されたプレーンな状態で格納できる。
- 秘密キーは、比較的強力なパスワードを使用して、PKCS#12 として暗号化して格納する必要がある。
- PKCS#12 秘密キーのパスワードは、ACS データベースに格納する必要がある。ACS データベースは暗号化されるため、セキュリティ上の重大な問題は発生しません。ACS 5.2 は、すべての ACS サーバにデータベース全体を配布します。

  ACS は、そのマシンに対してだけ存在するパスワードを使用して秘密キー パスワードを暗号化するため、秘密キーが他のマシンによって使用される可能性が阻止されます。秘密キーのパスワード キーは、ACS ファイルシステムの */opt/CSCOacs/config/prikeypwd.key* に保持されます。

tomcat キーストアなどのその他の証明書リポジトリには、ACS データベースと同じプロパティが必要です。秘密キーは、データベース内で常にセキュリティ保護されているパスワードによって暗号化されます。

秘密キーとパスワードのバックアップ

ACS データベース全体が、すべての証明書、秘密キー、および暗号化された秘密キー パスワードとともにプライマリ ACS 上に配布されてバックアップされます。プライマリ サーバの秘密キー パスワード キーも、プライマリのバックアップとともにバックアップされます。

その他のセカンダリ ACS の秘密キー パスワード キーはバックアップされません。バックアップは暗号化され、比較的セキュリティ保護された状態で ACS サーバの内部および外部に渡すこともできます。バックアップ内の秘密キーは、PKCS#12 とバックアップ ファイルの暗号化によって保護されます。PKCS#12 秘密キーを開くために使用されるパスワードは、バックアップ暗号化で保護されます。

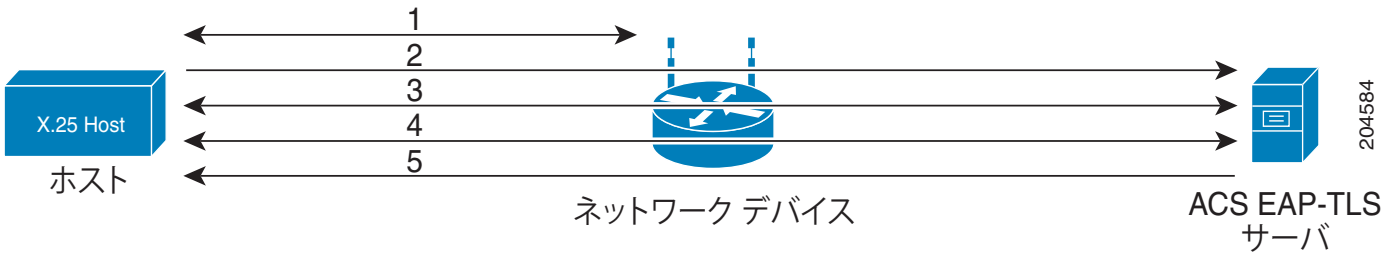
ACS 5.2 での EAP-TLS フロー

EAP-TLS サーバは、EAP 要求および応答パケットに基づくパケットを使用して、クライアントとデータを交換します。パケットは、特定の EAP-TLS データによって拡張されます。ACS は、EAP-TLS サーバとして機能し、Open Secure Sockets Layer（OpenSSL）ライブラリを使用して TLS カンバセーションを処理します。ACS EAP-TLS サーバは、クライアントとサーバ間の暗号化通信に使用される 128 ビットの MPPE 送信キーおよび受信キーを生成します。

ACS EAP-TLS サーバは、ベンダー コード Microsoft（311）、アトリビュート MS-MPPE-Send-Key（16）および MS-MPPE-Recv-Key（17）を使用して、ベンダー固有の RADIUS アトリビュート（26）でクライアントに MPPE キーを送信します。

図 B-2 に、ホスト、ネットワーク デバイス、および ACS EAP-TLS サーバ間の EAP-TLS 処理フローを示します。

図 B-2　EAP-TLS フロー



1	ホストがネットワークに接続します。ネットワーク デバイスが EAP 要求をホストに送信します。	**2**	ホストが EAP 応答をネットワーク デバイスに送信します。ネットワーク デバイスは、ホストから受信した EAP パケットを RADIUS RADIUS Access-Request に埋め込んで ACS に送信します。
3	ACS が認証について EAP 方式をネゴシエートします。サーバとクライアントは、EAP-TLS 認証をインスタンス化するための EAP 方式のネゴシエーション中に、EAP-TLS（EAP 要求方式 13）を使用するという合意に達する必要があります。	**4**	クライアント（ホスト）とサーバ（ACS）が証明書を交換します。この交換にはいくつかのメッセージが関係します。 クライアントとサーバが相互に認証されたあとで EAP-TLS 認証が成功し、各側が相手側に認証されたことを認識します。
5	ACS が、EAP Success（または EAP Failure）メッセージをホストに返し、セッション キーを含む RADIUS Access-Accept（または RADIUS Access-Reject）をネットワーク デバイスに返します。		

（注）　ホストと ACS 間のすべての通信は、ネットワーク デバイスを通じて行われます。

次の場合は EAP-TLS 認証が失敗します。

- サーバがクライアントの証明書を確認できず、EAP-TLS 認証を拒否した場合。
- クライアントがサーバの証明書を確認できず、EAP-TLS 認証を拒否した場合。

  証明書の確認は次の場合に失敗します。

  - 証明書の有効期限が切れている。
  - サーバまたはクライアントが証明書の発行元を見つけられない。
  - 署名のチェックに失敗した。
- クライアントがケースを廃棄したことにより、EAP パケットが不正な形式になった場合。

EAP-TLS では、セッション再開機能もサポートされます。ACS では、すでに完全な EAP-TLS 認証を渡したユーザを高速に再認証するために、EAP-TLS セッション再開機能がサポートされます。EAP-TLS 設定にセッション タイムアウト期間が含まれる場合、ACS はタイムアウト期間中に各 TLS セッションをキャッシュします。

設定した EAP-TLS セッション タイムアウト期間内にユーザが再接続した場合、ACS は EAP-TLS セッションを再開し、ユーザは証明書を比較せずに TLS ハンドシェイクだけを使用して再認証されます。

関連トピック

- 「PAC のタイプ」（P.B-22）
- 「ユーザ証明書認証」（P.B-6）

PEAPv0/1

ここでは、次の内容について説明します。

- 「PEAP の概要」（P.B-15）
- 「EAP-MSCHAPv2」（P.B-30）

ACS 5.2 では、次の PEAP サプリカントがサポートされます。

- Microsoft Built-In Clients 802.1x XP（PEAPv0 だけ）
- Microsoft Built-In Clients 802.1x Vista（PEAPv0 だけ）
- CSSC v.4.0
- CSSC v.5
- Funk Odyssey アクセス クライアント（最新バージョン）
- Intel Supplicant 12.4.x

PEAP の概要

PEAP は、EAP トランザクションの暗号化に使用するクライアント サーバ型のセキュリティ アーキテクチャです。これによって、EAP 認証の内容が保護されます。PEAP では、サーバ側公開キー証明書を使用してサーバが認証されます。

次に、クライアントと認証サーバ間に暗号化された SSL/TLS トンネルが作成されます。その後クライアントを認証するために行われる認証情報の交換は暗号化され、ユーザ クレデンシャルは盗聴から保護されます。

PEAP は EAP-TLS に似ていますが、別のクライアント認証方式を使用します。PEAP は、サーバ証明書を使用した認証、TLS トンネル、およびその暗号化されたトンネルを通じたクライアント認証を提供します。EAP-TLS とは異なり、PEAP ではクライアントが EAP-MSCHAPv2 などの別の EAP タイプを使用する必要があります。

PEAP 認証には常に 2 つのフェーズがあります。

- フェーズ 1 では、エンドユーザ クライアントが ACS を認証します。ここでは、サーバ証明書が要求され、ACS がエンドユーザ クライアントに対して認証されます。この結果、フェーズ 2 で送信されるユーザまたはマシンの資格情報が、信頼できる CA によって発行された証明書を持つ AAA サーバに送信されます。最初のフェーズは、TLS ハンドシェイクを使用して、エンドユーザ クライアントと AAA サーバ間に SSL トンネルを確立します。

（注）　関係するエンドユーザ クライアントによっては、エンドユーザ クライアント コンピュータ上の信頼できるルート CA 用に、ACS サーバ証明書を発行した CA の CA 証明書がローカル ストレージで必要になる場合もあります。

- 2 番めのフェーズでは、ACS が EAP 認証プロトコルを使用して、ユーザまたはマシンのクレデンシャルを認証します。フェーズ 1 で作成された SSL トンネルによって EAP 認証が保護されます。

  フェーズ 2 中にネゴシエートされる内部方式認証タイプは、EAP-MSCHAPv2 または EAP-GTC になります。外部 PEAP 方式と特定の内部 EAP 方式の組み合せは、PEAP/EAP-MSCHAPv2 や PEAP/EAP-GTC のようにスラッシュ文字を使用して示されます。

  PEAP によりセキュリティが向上していますが、その 1 つに ID 保護があります。この ID 保護により、すべての PEAP トランザクションにおいてユーザ名を保護できます。PEAP のフェーズ 1 が完了すると、通常はクリア テキストで送信されるユーザ名情報も含めて、すべてのデータが暗号化されます。

  Microsoft PEAPv0 クライアントでは ID 保護は使用できません。Microsoft PEAPv0 クライアントは、PEAP 認証のフェーズ 1 でユーザ名をクリア テキストで送信します。

ACS 5.2 では、PEAP は RADIUS プロトコルにカプセル化されています。内部方式 EAP メッセージは、EAP-TLV 方式にカプセル化されています。

サポートされる PEAP 機能

ここでは、次の内容について説明します。

サーバ認証および非認証トンネル確立モード

トンネルの確立は、攻撃者がクライアントとネットワーク アクセス サーバ（NAS）間にパケットを挿入することを防いだり、セキュリティの低い EAP 方式のネゴシエーションを可能にしたりするのに役立ちます。また、暗号化された TLS チャネルは、ACS に対する DoS 攻撃を防ぐのに役立ちます。

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。ポリシー コンポーネントが設定されていないかぎり、クライアントの PEAP メッセージは、RADIUS クライアントのメッセージが廃棄される原因になることがあります。

高速再接続

セッションを再開するときに、認証時間を短縮する方法として内部方式をスキップすることもできます。これは高速再接続とも呼ばれます。トンネルが構築されたあと、認証フローは認証情報の交換に直接進みます。認証に成功した場合には Result TLV Success（v0）/ トンネル EAP Success メッセージ、認証に失敗した場合には EAP Failure メッセージが認証情報の交換に使用されます。

高速再接続オプションをイネーブルにするように ACS を設定できます。認証に成功したあと、クライアントは一定の期間にわたって高速再接続を実行できます。PEAP 高速再接続によって、クライアントによる認証要求から ACS による応答までの遅延時間が短縮されます。

また、高速再接続では無線クライアントが認証の要求を繰り返すことなくアクセス ポイント間を移動できるため、クライアントとサーバのリソース要件が軽減されます。

高速再接続を可能にするには、ユーザ認証（内部方式）に使用されるユーザ ID とプロトコルを TLS セッションとともにキャッシュする必要があります。

セッションの再開

ACS は、PEAP 認証済みユーザ セッションに対して、セッション再開機能をサポートしています。この機能がイネーブルの場合、ACS は、ユーザが PEAP 認証のフェーズ 2 で正常に認証された場合にかぎり、PEAP のフェーズ 1 で作成された TLS セッションをキャッシュします。

ユーザが再接続しようとする場合、元の PEAP セッションがタイムアウトしていなければ、ACS はキャッシュされた TLS セッションを使用します。このため、PEAP のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。

ACS は、完全認証に成功したあと、セッションをキャッシュに格納します。クライアントは、特定の期間中は同じセッションの再開を試行できます。サーバ証明書は提示されず、トンネルは OpenSSL セッション キャッシュからのセッション情報を使用して構築されます。認証フローは内部方式に直接進みます。

クライアントがセッション再開を実行しようとしたときにタイムアウト期間が経過していた場合、ACS は完全認証フローに戻ります。

セッション再開とタイムアウトの値を設定できます。

任意のパラメータの保護された交換

TLV タプルは、セキュアなチャネル内のピアと ACS 間で任意の情報を交換する方法を提供します。

ACS 5.2 での PEAP フロー

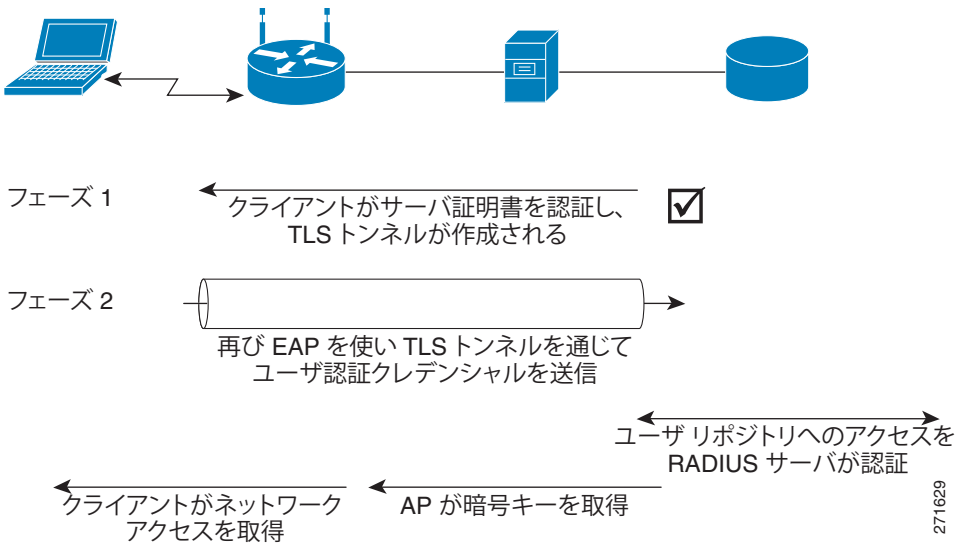
PEAP プロトコルでは、PKI ベースのセキュア トンネルの確立と、トンネル内の内部方式としての EAP-MSCHAPv2 プロトコルを使用して、ACS とピア間の認証を可能にします。ローカル証明書は、ピアによって確認されること（サーバ認証モード）と確認されないこと（サーバ非認証モード）があります。

ここでは、次の内容について説明します。

- 「TLS トンネルの作成」（P.B-17）
- 「MSCHAPv2 による認証」（P.B-18）

図 B-3 に、ホスト、アクセス ポイント、ネットワーク デバイス、および ACS EAP-TLS サーバ間の PEAP 処理フローを示します。

図 B-3　PEAP 処理フロー



TLS トンネルの作成

TLS トンネルの作成プロセスについて次に説明します。

1	論理リンクの作成後、無線 AP が EAP-Request/Identity メッセージを無線クライアントに送信します。	**2**	無線クライアントは、無線クライアントの ID（ユーザ名またはコンピュータ名）が含まれている EAP-Response/Identity メッセージで応答します。
3	無線 AP が EAP-Response/Identity メッセージを ACS に送信します。この時点から、無線 AP をパススルー デバイスとして使用して、ACS と無線クライアント間の論理通信が行われます。	**4**	ACS が EAP-Request/Start PEAP メッセージを無線クライアントに送信します。
5	無線クライアントと ACS が、TLS チャネルの暗号スイートのネゴシエーションに使用する一連の TLS メッセージを交換します。ACS 5.2 では、PEAP にクライアント証明書は使用されません。	**6**	PEAP ネゴシエーションの終了時に、ACS が無線クライアントに対する自己認証を行います。両方のノードが、（パスワードではなく公開キー暗号を使用して）TLS チャネルの相互の暗号化と署名キーを判断しています。

MSCHAPv2 による認証

TLS トンネルの作成後は、次の手順に従って、MSCHAPv2 で無線クライアントのクレデンシャルを認証します。

1	ACS が EAP-Request/Identity メッセージを送信します。	**2**	無線クライアントは、無線クライアントの ID（ユーザ名またはコンピュータ名）が含まれている EAP-Response/Identity メッセージで応答します。
3	ACS がチャレンジ文字列を含む EAP-Request/EAP-MSCHAPv2 チャレンジ メッセージを送信します。	**4**	無線クライアントは、ACS チャレンジ文字列への応答と ACS のチャレンジ文字列を含む EAP-Response/EAP-MSCHAPv2 Response メッセージで応答します。
5	ACS が EAP-Request/EAP-MSCHAPv2 成功メッセージを送信します。このメッセージは、無線クライアント応答が正しかったことを示し、無線クライアントのチャレンジ文字列への応答を含んでいます。	**6**	無線クライアントは、ACS 応答が正しかったことを示す EAP-Response/EAP-MSCHAPv2 確認応答メッセージで応答します。
7	ACS が EAP-Success メッセージを送信します。		

この相互認証の終了時に、無線クライアントは正しいパスワードを認識していることの証明（ACS チャレンジ文字列への応答）を提供し、ACS は正しいパスワードを認識していることの証明（無線クライアント チャレンジ文字列への応答）を提供しています。メッセージ交換全体が、PEAP で作成された TLS チャネルを通じて暗号化されます。

関連トピック

- 「認証プロトコルと ID ストアの互換性」（P.B-35）
- 「PEAP の設定」（P.18-3）

EAP-FAST

ここでは、次の内容について説明します。

EAP-FAST の概要

EAP Flexible Authentication via Secured Tunnel（EAP-FAST）プロトコルは、パブリックにアクセス可能な新しい IEEE 802.1x EAP タイプです。これは、強力なパスワード ポリシーを適用できないユーザがデジタル証明書を必要としない 802.1x EAP タイプを展開できるように、シスコが開発しました。

EAP-FAST は、さまざまなタイプのユーザ データベースやパスワード データベース、パスワードの変更や有効期間をサポートしています。そのため、柔軟性があり、展開や管理も容易です。EAP-FAST の詳細と、他の EAP タイプとの比較については、次の URL を参照してください。

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml

EAP-FAST は、TLS トンネルで EAP トランザクションを暗号化するクライアント サーバ型のセキュリティ アーキテクチャです。その点では PEAP に似ていますが、EAP-FAST トンネルの設定は、各ユーザに固有の強力な秘密に基づいていることが大きな相違点です。

これらの秘密は Protected Access Credentials（PAC）と呼ばれ、ACS が、ACS にしか知られていないマスターキーを使用して生成します。共有秘密情報に基づくハンドシェイクは PKI に基づくハンドシェイクよりも元々速いため、EAP-FAST は、サプリカントと ACS 間のトラフィックを暗号化するために TLS 接続を確立する高度な EAP プロトコル（EAP-TLS と PEAP を含む）の中で最も高速です。EAP-FAST の実装には証明書管理は必要ありません。

EAP-FAST は 3 つのフェーズで実行されます。

- フェーズ 0：フェーズ 0 は EAP-FAST に固有のフェーズであり、EAP-FAST エンドユーザ クライアントに、ネットワーク アクセスを要求するユーザ用の PAC を提供するトンネル セキュア機能です（「自動インバンド PAC プロビジョニング」（P.B-23）を参照）

  エンドユーザ クライアントに PAC を提供することが、フェーズ 0 の唯一の目的です。匿名インバンド プロビジョニングの場合、トンネルは匿名の Diffie-Hellman キー交換に基づいて確立されます。認証付きインバンド プロビジョニングでは、他の暗号スイートを使用します。

  EAP-MSCHAPv2 または EAP-GTC 認証が成功すると、ACS はユーザに PAC を提供します。EAP-FAST フェーズ 0 をサポートしているデータベースを確認するには、「認証プロトコルと ID ストアの互換性」（P.B-35）を参照してください。

  （注） フェーズ 0 は任意であり、PAC は手動でエンドユーザ クライアントに提供できます（「手動 PAC プロビジョニング」（P.B-24）を参照）。

  [Allow Anonymous In-Band PAC provisioning] オプションを選択すると、EAP-FAST フェーズ 0 を使用してエンドユーザ クライアントに PAC が提供されます。このチェックボックスをオンにすると、ACS は、エンドユーザ クライアントに新規 PAC を提供するために、そのクライアントとの安全な接続を確立します。

  このオプションでは、エンドユーザ クライアントと ACS の間で匿名の TLS ハンドシェイクが可能になります（EAP-MSCHAPv2 と EAP-GTC が内部方式として使用されます）。

  [Allow Authenticated In-Band PAC provisioning] オプションを選択すると、TLS サーバ側の認証とともに EAP-FAST フェーズ 0 を使用してエンドユーザ クライアントに PAC がプロビジョニングされます。このオプションを選択する場合は、サーバ証明書をインストールする必要があります。

  通常、EAP-FAST のフェーズ 0 ではネットワーク アクセスは認可されません。ただし、[Accept Client on Authenticated Provisioning] オプションを選択した場合は、ACS が PAC プロビジョニングのフェーズ 0 の正常終了時に RADIUS Access-Accept（EAP Success を含む）を送信し、クライアントは再認証を強制されません。

  このオプションは、[Allow Authenticated In-Band PAC Provisioning] オプションもイネーブルの場合にだけ、イネーブルにすることができます。

- フェーズ 1：フェーズ 1 では、ACS とエンドユーザ クライアントが、エンドユーザ クライアントによって示された PAC に基づいて TLS トンネルを確立します。このフェーズでは、ネットワーク アクセスの取得を試行するユーザ用の PAC がエンドユーザ クライアントに提供されていることと、PAC の期限が切れていないことが必要です。PAC プロビジョニングを実行する手段は関係ありません。自動プロビジョニングと手動プロビジョニングのどちらでも使用できます。

- フェーズ 2：フェーズ 2 では、ACS が EAP-MSCHAPv2 または EAP-GTC を内部 EAP 方式として使用して、フェーズ 1 で作成された保護 TLS トンネルからユーザのクレデンシャルを認証します。EAP-FAST フェーズ 2 をサポートしているデータベースを確認するには、「認証プロトコルと ID ストアの互換性」（P.B-35）を参照してください。

フェーズ 1 とフェーズ 2 は、同じ EAP-FAST カンバセーションの後続部分です。

EAP-FAST は、すべての EAP-FAST トランザクションでユーザ名を保護できます。ACS は、フェーズ 1 で示されたユーザ名に基づいてユーザ認証を実行しませんが、フェーズ 1 でユーザ名が保護されるかどうかは、エンドユーザ クライアントによって異なります。

フェーズ 1 でエンドユーザ クライアントが実際のユーザ名を送信しなければ、ユーザ名は保護されます。EAP-FAST のフェーズ 1 が完了すると、通常はクリア テキストで送信されるユーザ名情報も含めて、すべてのデータが暗号化されます。

ACS は、Windows ユーザ データベースによって認証されたユーザに対して、EAP-FAST でのパスワード エージングをサポートしています。パスワード エージングは、EAP-FAST のフェーズ 0 またはフェーズ 2 で処理できます。フェーズ 0 中にパスワード エージングでユーザがパスワードを変更する必要がある場合は、新規パスワードがフェーズ 2 で有効になります。

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。
- Man-in-the-Middle（MitM; 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。
- MSCHAPv2 や 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情報を使用してトンネルのセキュリティを確保することが推奨されます。EAP-FAST は、サーバがキャッシュおよび管理する必要のあるユーザごとおよびデバイスごとの状態を最小化できるようにする一方で、ピアによる単一の強力な共有秘密情報の使用を容易にします。

ACS 5.2 での EAP-FAST

ACS では、PKI または ADHP に基づく共有秘密クレデンシャル（PAC）を使用したピアのインバンド プロビジョニングがサポートされます（フェーズ 0）。ピアの認証と、ネットワークへのピア アクセスの許可は、フェーズ 1 とフェーズ 2 で実装されます。

ACS 5.2 では、EAP-FAST バージョン 1 および 1a がサポートされます。

ここでは、次の内容について説明します。

- 「マスターキー生成と PAC TTL」（P.B-26）
- 「TLS 再ネゴシエーション用の EAP-FAST」（P.B-26）

マスターキーについて

EAP-FAST マスターキーは、ACS が自動的に生成し、ACS だけが認識している強力な秘密です。マスターキーがエンドユーザ クライアントに送信されることはありません。EAP-FAST でマスターキーが必要な理由は 2 つあります。

- **PAC 生成**：ACS は、アクティブ マスターキーを使用して PAC を生成します。PAC の詳細については、「PAC について」（P.B-21）を参照してください。
- **EAP-FAST フェーズ 1**：ACS は、エンドユーザ クライアントによって示された PAC が、認識しているマスターキーのいずれかによって生成されたかどうかを判別します。

EAP-FAST のセキュリティを強化するために、ACS は PAC の生成に使用するマスターキーを変更します。ACS は、定義された [Master Key Generation Period] の値を使用して、新規マスターキーを生成するタイミングとすべてのマスターキーの経過時間を決定します。

アクティブ マスターキーは、ACS が PAC を生成するために使用するマスターキーです。[Master Key Generation Period] の設定によって、マスターキーがアクティブである期間が決まります。アクティブであるマスターキーは常に 1 つだけです。PAC の更新またはプロビジョニングが必要かどうかが TTL 値によってどのように決まるかについては、「マスターキー生成と PAC TTL」（P.B-26）を参照してください。

PAC について

PAC は、ACS および EAP-FAST エンドユーザ クライアントをイネーブルにし、互いを認証して EAP-FAST フェーズ 2 で使用する TLS トンネルを確立する強力な共有秘密です。ACS は、アクティブ マスターキーとユーザ名を使用して PAC を生成します。

PAC は、次のもので構成されています。

- **PAC-Key**：クライアント（およびクライアント デバイス）とサーバの ID にバインドされている共有秘密情報。
- **PAC Opaque**：クライアントがキャッシュしてサーバに渡す暗号化されたフィールド。サーバは、PAC-Key およびクライアント ID を復号化して、クライアントとの相互認証を行います。
- **PAC-Info**：クライアントがさまざまな PAC をキャッシュできるように、少なくとも認証局 ID が含まれています。PAC の有効期限などの情報が含まれていることもあります。

EAP-FAST エンドユーザ クライアントは、クライアントを使用してネットワークにアクセスする各ユーザの PAC を保存します。さらに、EAP-FAST をサポートする AAA サーバには独自の認証局 ID があります。エンドユーザ クライアントは、ユーザの PAC を、それを生成した AAA サーバの認証局 ID に関連付けます。PAC により PKI（デジタル証明書）が不要になります。

EAP-FAST フェーズ 1 で、エンドユーザ クライアントは、現在のユーザ用、および EAP-FAST トランザクションの開始時に ACS によって送信された認証局 ID 用に備えている PAC を示します。PAC プロビジョニングという、エンドユーザ クライアントに PAC を提供する手段については、「自動インバンド PAC プロビジョニング」（P.B-23）および「手動 PAC プロビジョニング」（P.B-24）を参照してください。

マスターキー生成値を修正しても、すでに作成された PAC には影響しません。マスターキー生成値に対して行う修正では、次にマスターキーが生成される期間を指定します。

プロビジョニング モード

ACS は、アウトオブバンド プロビジョニング モードとインバンド プロビジョニング モードをサポートしています。インバンド プロビジョニング モードは、キー共有に対する匿名 DH または認証付き DH、あるいは RSA アルゴリズムによって確立された TLS トンネル内で機能します。

ユーザの資格情報が危険にさらされる可能性を最小限に抑えるために、保護されたトンネルの外部ではクリア テキスト パスワードを使用しないでください。したがって、EAP-MSCHAPv2 または EAP-GTC を使用して、保護されたトンネル内でユーザのクレデンシャルを認証します。PAC に含まれている情報は、内部 EAP 方式の完了後に認証セッションでも使用できます。

EAP-FAST は、機能が拡張されて、PAC プロビジョニングが実行される認証済みトンネル（サーバ証明書を使用）をサポートするようになりました。EAP-FAST および特にサーバ証明書に対する機能拡張となる、新しい暗号スイートが使用されます。

認証済みトンネルを使用するプロビジョニング セッションの終わりに、ネットワーク アクセスを許可できます。これは、サーバとユーザが互いを認証したためです。

ACS は、プロビジョニングのためにトンネル内部で次の EAP 方式をサポートしています。

- EAP-MSCHAPv2
- EAP-GTC

デフォルトでは、EAP-MSCHAP 内部方式を使用する場合、ACS は、初期認証試行に失敗した場合に [Service] ページで設定した値まで TLS トンネルの内部での認証試行を許可します。SSL トンネル内で 4 回めの認証試行に失敗したあと、ACS は EAP カンバセーションを終了し、その結果 RADIUS Access-Reject が生成されます。

ACS では、ACS にダウンロードできる PAC を生成できるようにアウトオブバンド PAC ファイルの発行がサポートされます。

PAC のタイプ

ACS では、次に示す PAC のタイプがサポートされます。

- トンネル v1 および v1a
- CTS
- マシン
- 認可

ACS は、共有秘密を含む PAC をサプリカントにプロビジョニングします。この共有秘密は、サプリカントと ACS の間に TLS トンネルを構築する場合に使用されます。ACS がサプリカントにプロビジョニングする PAC は、状況に応じてさまざまな用途を持ちます。

サーバ ポリシーに従って、次のタイプの PAC が ACS にプロビジョニングされます。

- **トンネル/マシン PAC**：ユーザまたはマシン情報を含みますが、ポリシー情報は含みません。
- **ユーザ認可 PAC**：ポリシー要素（たとえば、ユーザ認証で使用される内部方式など）を含みます。ユーザ認可 PAC を使用すると、「セッションの再開」（P.B-16）で説明しているように、ステートレスなサーバ セッション再開ができるようになります。

エンドユーザ クライアントが PAC を受信するさまざまな手段を次に示します。

- **PAC プロビジョニング**：エンドユーザ クライアントに PAC がない場合に必要です。マスターキーと PAC の状態によって PAC プロビジョニングが必要かどうかがどのように決まるかについては、「マスターキー生成と PAC TTL」（P.B-26）を参照してください。

  PAC プロビジョニングについては次の 2 つの手段がサポートされています。

  - **自動インバンド PAC プロビジョニング**：セキュア ネットワーク接続を使用して PAC を送信します。詳細については、「自動インバンド PAC プロビジョニング」（P.B-23）を参照してください。
  - **手動プロビジョニング**：ACS を使用してユーザ用の PAC ファイルを生成し、エンドユーザ クライアントを実行しているコンピュータに PAC ファイルをコピーし、エンドユーザ クライアントに PAC ファイルをインポートする必要があります。詳細については、「手動 PAC プロビジョニング」（P.B-24）を参照してください。

- **PAC 更新**：[Proactive PAC Update When] フィールドで指定した値に基づいて行われます。マスターキーと PAC の状態によって PAC が更新されるかどうかがどのように決まるかについては、「マスターキー生成と PAC TTL」（P.B-26）を参照してください。

PAC については、PAC TTL 設定によって次の 2 つの状態が決定されます。

- **アクティブ**：PAC TTL よりも新しい PAC はアクティブと見なされ、EAP-FAST フェーズ 1 の完了に使用できます。
- **期限切れ**：PAC TTL よりも古い PAC は期限切れと見なされます。EAP-FAST フェーズ 2 の終わりに ACS がユーザ用の新規 PAC を生成し、それをエンドユーザ クライアントに提供します。

自動インバンド PAC プロビジョニング

EAP-FAST フェーズ 0 と同じ自動インバンド PAC プロビジョニングは、セキュア ネットワーク接続を介して新規 PAC をエンドユーザ クライアントに送信します。自動インバンド PAC プロビジョニングをサポートするように ACS とエンドユーザ クライアントを設定した場合、自動インバンド PAC プロビジョニングにネットワーク ユーザまたは ACS 管理者の介入は必要ありません。

（注） ACS が各ユーザを単一の ID ストアと関連付ける場合、自動インバンド PAC プロビジョニングを使用するには、EAP-FAST フェーズ 0 と互換性のある ID ストアで EAP-FAST ユーザが認証されている必要があります。ACS が EAP-FAST フェーズ 0 とフェーズ 2 をサポートできるデータベースについては、「認証プロトコルと ID ストアの互換性」（P.B-35）を参照してください。

通常、EAP-FAST のフェーズ 0 ではネットワーク アクセスは認可されません。この一般的なケースでは、クライアントがフェーズ 0 の PAC プロビジョニングを正常に実行したあとで、クライアントは新しいフェーズ 1 トンネル確立を開始するために新しい EAP-FAST 要求を送信してから、フェーズ 2 の認証を行う必要があります。

ただし、[Accept Client on Authenticated Provisioning] オプションを選択した場合は、ACS が PAC プロビジョニングのフェーズ 0 の正常終了時に RADIUS Access-Accept（EAP Success を含む）を送信し、クライアントは再認証を強制されません。このオプションは、[Allow Authenticated In-Band PAC Provisioning] オプションもイネーブルの場合にだけ、イネーブルにすることができます。

フェーズ 0 での PAC の送信は MSCHAPv2 認証によって保護されており、MSCHAPv2 はディクショナリ攻撃に弱いため、自動インバンド PAC プロビジョニングの使用は EAP-FAST の最初の展開に限定することを推奨します。

大規模な EAP-FAST 展開後は、PAC に対する高度なセキュリティを確保するために、PAC プロビジョニングを手動で実行してください。手動 PAC プロビジョニングの詳細については、「手動 PAC プロビジョニング」（P.B-24）を参照してください。

ACS が自動インバンド PAC プロビジョニングを実行するかどうかを制御するには、[System Administration] ドローアの [Global System Options] ページのオプションを使用します。詳細については、「EAP-FAST」（P.B-18）を参照してください。

手動 PAC プロビジョニング

手動 PAC プロビジョニングでは、ACS 管理者が PAC ファイルを生成し、それを該当するネットワーク ユーザに配布する必要があります。ユーザは PAC ファイルでエンドユーザ クライアントを設定する必要があります。

EAP-FAST を使用してネットワークにアクセスするユーザを制御するには、手動 PAC プロビジョニングを使用します。自動インバンド PAC プロビジョニングをディセーブルにすると、PAC でプロビジョニングされていない EAP-FAST ユーザはネットワークにアクセスできません。

ACS 展開に、各ネットワーク セグメントへのアクセスが個別の ACS によって制御されるネットワーク セグメンテーションが含まれている場合は、手動 PAC プロビジョニングによってセグメントごとに EAP-FAST アクセスを許可できます。

たとえば、会社がシカゴとボストンのオフィスでのワイヤレス アクセス用に EAP-FAST を使用していて、これら 2 つのオフィスそれぞれの Cisco Aironet Access Point が別々の ACS を使用するよう設定されている場合に、シカゴのオフィスを訪れたボストンの従業員がワイヤレス アクセスを使用できるかどうかを、従業員ごとに決定できます。

手動 PAC プロビジョニングの管理オーバーヘッドは自動インバンド PAC プロビジョニングよりもはるかに大きくなりますが、ネットワーク上で PAC を送信するリスクはなくなります。PAC を手動でプロビジョニングすると、初期展開時の多数のエンドユーザ クライアントの設定で多くの作業が必要になりますが、このタイプのプロビジョニングは PAC を展開する最も安全な方法です。

大規模な EAP-FAST 展開後は、PAC に対する高度なセキュリティを確保するために、PAC プロビジョニングを手動で実行します。

特定のユーザ名、ユーザ グループ、ユーザ名リスト、またはすべてのユーザに対して PAC ファイルを生成できます。マシンの PAC を生成し、クライアントに対して PAC を手動でプロビジョニングすることもできます。

PAC を作成するには次のパラメータが必要です。

- ユーザ PAC とマシン PAC のどちらであるかの指定
- [Internal Identity Store ID] フィールドに格納されている ID
- PAC 存続可能時間（TTL）
- PAC 暗号化のオンまたはオフ、および暗号化用のパスワード

PAC は、RC4 または AES アルゴリズムを使用して、指定したパスワードで暗号化できます。受信した PAC データを手動で復号化できるように、詳細な復号化アルゴリズムをクライアントに提供する必要があります。

ACS でサポートされる PAC の機能

ACS 5.2 では、PAC に対して次の機能がサポートされます。

マシン PAC 認証

マシン PAC ベースの認証では、ユーザ認証の前にマシンが制限付きでネットワークにアクセスできます。

予防的 PAC アップデート

ACS は、PAC TTL の設定済みパーセンテージが残っている場合に、認証の成功後に新しい PAC をクライアントに予防的に提供します。トンネル PAC アップデートは、PAC の有効期限が切れる前に実行された最初の正常な認証後に、サーバによって開始されます。

予防的 PAC アップデート時間は、[Allowed Protocols] ページで ACS サーバに対して設定されます。このメカニズムにより、クライアントは常に有効な PAC で更新されます。

（注）　マシン PAC と認可 PAC に対して予防的 PAC アップデートは行われません。

認証付きプロビジョニングでのピアの受け入れ

プロビジョニング フェーズ中にピアを認証できます。

PAC なし認証

PAC なし EAP-FAST 認証では、トンネル PAC またはマシンで生成された PAC を発行または受け入れせずに、ACS で EAP-FAST を実行できます。セキュア トンネルは、PAC 以外の証明書を使用して確立できます。一部の PAC は存続期間が長く更新されない場合があり、これが認証とセキュリティの問題の原因になることがあります。

PAC なし EAP-FAST がイネーブルになっている場合、PAC に対する要求は無視されます。認証は EAP-FAST フェーズ 0 で開始し、PAC に対する後続の要求は無視されます。フローは EAP-FAST フェーズ 2 に移動します。ACS は、Success-TLV メッセージで PAC なしで応答します。

クライアントが PAC でトンネルを確立しようとした場合、ACS は PAC Invalid メッセージで応答します。トンネルの確立は行われず、Access-Reject が送信されます。ホストまたはサプリカントは接続を再試行できます。

ADHP とも呼ばれる匿名フェーズ 0 は、プロトコルがフェーズ 2 へのロール オーバーをサポートしていないため、PAC なし認証に対してサポートされません。PAC なし EAP-Fast では設定がサポートされ、クライアント証明書は不要です。

表 B-3 に、さまざまなタイプの PAC と、それらに使用できる認証と認可の方式を示します。

表 B-3　PAC 規則の要約

PAC のタイプ	トンネル v1/v1a/CTS	マシン	認可
プロビジョニング時に要求に応じて PAC を提供	○	○	プロビジョニング時に要求に応じて PAC を提供します。
認証時に要求に応じて PAC を提供	○	○	この認証で PAC が使用されなかった場合だけ。
予防的アップデート	○	×	×
PAC の有効期限が切れたとき	拒否し、TLS フォールバックを試行し、認証の成功後にだけ新しい PAC を提供します（トンネル PAC）。	拒否し、TLS フォールバックを試行し、認証の成功後にだけ新しい PAC を提供します（マシン PAC）。	拒否し、認証の成功後にだけ新しい PAC を提供します（認可 PAC）。
ACS 3.x/4.x PAC のサポート	トンネル PAC v1/v1a だけ	○	×

関連トピック

- 「PAC について」（P.B-21）
- 「プロビジョニング モード」（P.B-22）

- 「PAC のタイプ」（P.B-22）
- 「マスターキー生成と PAC TTL」（P.B-26）

マスターキー生成と PAC TTL

マスターキー生成と PAC TTL の値によって、「マスターキーについて」（P.B-21）および「PAC のタイプ」（P.B-22）に説明するようにそれらの状態が判断されます。マスターキーと PAC の状態によって、EAP-FAST でのネットワーク アクセスの要求者に PAC プロビジョニングまたは PAC 更新が必要かどうかが判断されます。

関連トピック

- 「PAC について」（P.B-21）
- 「プロビジョニング モード」（P.B-22）
- 「PAC のタイプ」（P.B-22）
- 「ACS でサポートされる PAC の機能」（P.B-24）

TLS 再ネゴシエーション用の EAP-FAST

匿名の PAC プロビジョニング スキーマを使用する場合、パスワードの入力を 2 回求められることがあります。最初にパスワードを入力したときに、ACS は PAC をプロビジョニングして、access-reject をクライアントに送信します。次に、クライアントからプロンプトに対してパスワードを再入力すると、認証が可能になり、ネットワークへのアクセスが許可されます。

ACS は TLS クライアントのハンドシェイク レコードを確認します。TLS クライアントのハンドシェイク レコードを確認できた場合、ACS は、ユーザのアクセス要求を拒否する代わりに、EAP-FAST フェーズ 0 の最後に TLS 再ネゴシエーションを開始します。

ホストが匿名の PAC プロビジョニングを使用している場合、Vista クライアントではこのオプションを使用する必要があります。Vista クライアントではキャッシュにユーザ パスワードが保存されないので、パスワードの入力は 1 回になります。このオプションをイネーブルにしている場合、ACS は、PAC プロビジョニング後にアクセスの試行を拒否する代わりに、EAP-FAST フェーズ 0 の最後にクライアントへの TLS 再ネゴシエーション要求の送信を開始します。

ACS 5.2 での EAP-FAST フロー

（注）　EAP-FAST をサポートするようにエンドユーザ クライアントを設定する必要があります。ここでは、ACS の設定だけを取り上げます。

始める前に

この手順のステップの順番は、一例に過ぎません。ご使用のサイトで EAP-FAST をイネーブルにするときは、これらのステップを繰り返したり順番を変えたりして実行しなければならない場合があります。

たとえば、この手順では、PAC プロビジョニングをどのようにサポートするかの決定は、EAP-FAST をサポートするようユーザ データベースを設定したあとになっています。しかし、自動インバンド PAC プロビジョニングを選択すると、ユーザ データベース サポートの制限が変わります。

ACS で EAP-FAST 認証を実行できるようにするには、次の手順を実行します。

ステップ 1　EAP-FAST 認証をサポートするように ID ストアを設定します。

EAP-FAST 認証をサポートしている ID ストアを確認するには、「認証プロトコルと ID ストアの互換性」（P.B-35）を参照してください。ID ストアを設定する方法については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。

ステップ 2　マスターキー生成と PAC TTL 値を決定します。

マスターキー生成と PAC TTL 値によって PAC プロビジョニングまたは PAC 更新が必要かどうかがどのように決まるかについては、「マスターキー生成と PAC TTL」（P.B-26）を参照してください。

ステップ 3　自動 PAC プロビジョニングと手動 PAC プロビジョニングのどちらを使用するかを決めます。

PAC プロビジョニングの 2 つの手段については、「自動インバンド PAC プロビジョニング」（P.B-23）および「手動 PAC プロビジョニング」（P.B-24）を参照してください。

自動インバンド PAC プロビジョニングの使用は、少数の新規エンドユーザ クライアントをネットワークに追加するため、および期限切れのマスターキーに基づく PAC を置換するために手動 PAC プロビジョニングを使用する前の、EAP-FAST の最初の展開に限定することを推奨します。

ステップ 4　ステップ 2 およびステップ 3 での決定を使用して、[Global Systems Options] ドローアで EAP-FAST をイネーブルにします。詳細については、「EAP-FAST」（P.B-18）を参照してください。

ACS が、EAP-FAST 認証を実行できる状態になります。

（注）　内部 ID は、`the workstation not allowed` というエラーが表示されたとき、SSL ハンドシェイクに失敗したとき、EAP-PAC がプロビジョニングされているとき、および ACS が無効な PAC を受信したときにはログに記録されません。

関連トピック

- 「内部 ID ストアの管理」（P.8-4）
- 「外部 ID ストアの管理」（P.8-18）

EAP-FAST PAC 管理

ACS の EAP-FAST マスターキーは、EAP-FAST がサプリカントごとにサーバ暗号化データを格納するために使用する PAC および PAC-Opaque を暗号化または復号化、署名、および認証するために使用されます。EAP-FAST には、ACS ドメイン内の各サーバが PAC（別のサーバでパックされた PAC も含む）をセキュアにパックおよびアンパックするための配布メカニズムが必要です。

EAP-FAST マスターキーには、ACS ドメイン内のすべてのサーバが認識している共通秘密情報が必要です。マスターキーは定期的に更新され、キーはすべての ACS サーバによってセキュアに同期して置換されます。FIPS-140 などの強力な暗号標準に準拠するために、キーは高いエントロピーで生成されます。

旧バージョンの ACS では、マスターキーは ACS 配布メカニズムによって配布され、それらのキーのセキュリティを高めるためにときどき置換されました。ACS 5.2 では、マスターキー配布の簡略性、正確性、ロバストネス、およびセキュリティを提供する新しいスキームが導入されています。

ACS EAP-FAST の新しい配布スキームには、共通シードキーを配布するセキュアな方法が含まれています。各 ACS サーバは、そこから同じマスターキーのセットを決定論的に取得できます。各 PAC にはマスターキーの取得元の情報が含まれ、各サーバは、PAC を暗号化および署名したマスターキーをセキュアに再構築できます。

このスキームは、送信される暗号機密情報の量を削減することでセキュリティを向上させます。

ここでは、次の内容について説明します。

キー配布アルゴリズム

共通シードキーは、プライマリ ACS サーバによって生成される比較的大きく完全にランダムなバッファです。シードキーは、インストール時に 1 回だけ生成されるか、管理者が手動で再生成できます。シードキーを変更した場合、以前のマスターキーと PAC はすべて自動的に無効にされるため、シードキーを置換する必要はほとんどありません。

シードキーは、ランタイム暗号モジュール（CryptoLib）に存在する、FIPS で承認された RNG ジェネレータを使用して生成されます。ACS プライマリ サーバ管理は、シードキーがいつ生成されるかを判断し、新しいシードキーの生成を要求するために ACS ランタイムと通信します。

シードキーのサイズはさまざまですが、少なくとも 64 バイト（512 ビット）から構成されている必要があります。大きなシードはパフォーマンスに影響することがあります。各マスターキーの取得がそのシードに依存するためです。

任意のどの時点でも、各 ACS サーバが 1 つのシードキーを使用する必要があり、プライマリ ACS サーバが最新のシードキーをすべてのサーバに配布する必要があります。古いシードキーは廃棄する必要があります。

シードキーには、重要な暗号機密情報が含まれています。シードキー情報を開示すると、EAP-FAST PAC メカニズム全体で ID が攻撃を受けやすくなります。

このため、プライマリとセカンダリの ACS サーバ間でシードキーを送信するメカニズムは、セキュリティで十分に保護する必要があります。データベースへのシードキーの格納については、さらにセキュリティ手段を講じる必要があります。シードキーは、最も強力なセキュリティ手段で保護する必要があります。

EAP-FAST PAC-Opaque のパックとアンパック

サーバは、新しい PAC を生成するときに、使用するマスターキーを取得する必要があります。サーバが新しい PAC を受け入れるときには、マスターキー スキームに対する攻撃の可能性を防ぐために使用する検証を追加した同じアルゴリズムを、マスターキーの取得に使用する必要があります。マスターキーが過去にキャッシュにすでに配置されていた場合は、取得の計算をスキップできます。

無効化の方式

すべての PAC およびすべてのマスターキーを無効化できます。このタイプの広範な無効化で行う必要があるのは、シードキーの無効化と新しいシードキーでの置換だけです。

システムで 1 つのシードキーだけを使用すると、実装が容易になります。

ACS 4.x からの PAC の移行

設定を 4.x から移行できますが、PAC 自体はサプリカントだけに格納されているため、依然として ACS 3.x までのバージョンから発行できます。ACS 5.2 は、EAP-FAST 5.0 の予防的 PAC アップデートと同様に、バージョン 4.x 以降から移行されたマスターキーに従ってすべてのタイプの PAC を受け入れ、新しい 5.0 PAC を再発行します。

ACS 5.2 は、ACS 3.x または 4.x から PAC を受け入れると、ACS 4.x の設定から移行された 4.x マスターキーに従って PAC を復号化および認証します。このタイプの PAC の復号化と処理は、ACS 4.x の PAC が処理される方法と似ています。

移行プロセスでは、次のデータ項目の変換が行われます。

- ACS の EAP-FAST A-ID（認証局 ID）。パラメータは ACS 5.2 で展開された A-ID を置換します。
- 非アクティブな ACS 4.x マスターキーのリスト。リストは ACS 4.x の設定から取得され、ACS 5.2 の新しいテーブルに配置されます。移行された各マスターキーには、予想される有効期限が関連付けられています。テーブルは、マスターキー識別子（インデックス）、および各キーに割り当てられている PAC 暗号とともに移行されます。

RADIUS キー ラップありの EAP 認証

ACS は、RADIUS キー ラップありの PEAP、EAP-FAST、および EAP-TLS 認証を使用するように設定できます。この場合、ACS は、RADIUS メッセージを認証し、セッション キーを Network Access Server（NAS; ネットワーク アクセス サーバ）に配布できます。EAP セッション キーは、Advanced Encryption Standard（AES; 高度暗号化規格）を使用して暗号化され、RADIUS メッセージは HMAC-SHA-1 を使用して認証されます。

RADIUS は（EAP-Message アトリビュートの）EAP メッセージの転送に使用されるため、RADIUS メッセージをセキュアに認証することにより、セキュアに認証された EAP メッセージ交換が保証されます。PEAP、EAP-FAST、および EAP-TLS 認証がイネーブルの場合には、RADIUS キー ラップを外部認証方式として使用できます。キー ラップは、EAP-TLS の内部方式（たとえば、EAP-FAST または PEAP）としてはサポートされません。

ACS でサポートされる RADIUS キー ラップでは、cisco-av-pair RADIUS Vendor-Specific-Attribute（VSA; ベンダー固有アトリビュート）の次の 3 つの新しい AVP を使用します（Cisco VSA の TLV 値は [26/9/1]）。

- Random-Nonce : NAS によって生成され、キー データの暗号化および認証にランダム性を付与し、要求と応答パケットをリンクさせてリプレイ アタックを防止します。
- Key : セッション キーの配布で使用されます。
- Message-Authenticator-Code : EAP-Message アトリビュートと Key アトリビュートを含む RADIUS メッセージの認証性を保証します。

RADIUS キー ラップの使用時に、ACS はメッセージ交換とキー配布でこれら 3 つの RADIUS キー ラップ AVP を適用します。ACS は、RADIUS キー ラップ AVP と標準の RADIUS Message-Authenticator アトリビュートを含むすべての RADIUS（EAP）要求を拒否します。

PEAP、EAP-FAST、および EAP-TLS 認証で RADIUS キー ラップを使用するには、[Network Devices and AAA Clients] ページまたは [Default Network Device] ページで [EAP authentication with RADIUS Key Wrap] をイネーブルにする必要があります。

また、AAA クライアントごとに、2 つの共有秘密キーを定義する必要があります。キーはそれぞれ一意で、RADIUS 共有キーとは明確に区別される必要があります。RADIUS キー ラップはプロキシ機能をサポートしないため、プロキシ構成では使用しないでください。

EAP-MSCHAPv2

Microsoft Challenge Handshake Authentication Protocol（MSCHAP v2; 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 v2）は、相互認証とも呼ばれる双方向認証を提供します。リモート アクセス クライアントは、ダイヤルインするリモート アクセス サーバがユーザのパスワードにアクセスできることの確認を受信します。

ここでは、次の内容について説明します。

EAP-MSCHAPv2 の概要

EAP 認証プロトコル ファミリの一部のメンバー（具体的には EAP-FAST と PEAP）は、「EAP 内部方式」の概念をサポートします。したがって、別の EAP ベース プロトコルは、最初のプロトコルのコンテキスト内で追加の認証を実行します。これを「EAP 外部方式」と呼びます。

EAP-FAST および PEAP 外部方式でサポートされる内部方式の 1 つは EAP-MSCHAPv2 です。この方式は、EAP によって確立された一般フレームワークに準拠する MSCHAPv2 プロトコルの応用です。

EAP-MSCHAPv2 を内部 EAP 方式として使用すると、次のコンテキストで、無線認証用のユーザ クレデンシャルのデータベースが関連付けられた Microsoft ディレクトリ テクノロジー（Windows Active Directory など）を容易に再利用できます。

ユーザ認証用の MSCHAPv2

ACS では、EAP-FAST および PEAP の内部方式として EAP-MSCHAPv2 認証プロトコルがサポートされます。このプロトコルは、MSCHAPv2 を EAP フレームワークにカプセル化したものです。相互認証は、設定されたクレデンシャル データベースに対して行われます。

クライアントはパスワードを送信せず、パスワードの暗号化機能を送信します。EAP-MSCHAPv2 をトンネリング プロトコルの内部方式として使用すると、セキュアな通信の保護が向上します。すべてのプロトコル メッセージはトンネルとサーバの内部で暗号化され、クライアント チャレンジはランダムに生成されずに、外部方式暗号情報から取得されます。

EAP-MSCHAPv2 は、AD および ACS 内部 ID ストアに対してサポートされています。

パスワード変更のための MSCHAPv2

EAP-MSCHAPv2 を（EAP 内部方式として）使用してパスワードの有効期限が切れたユーザを認証する場合、ACS は特定の EAP-MSCHAPv2 障害通知をクライアントに送信します。クライアントは、ユーザに新しいパスワードの入力を要求するプロンプトを表示してから、同じカンバセーションで ACS にそのパスワードを提供できます。

新しいパスワードは、古いパスワードを利用して暗号化されます。ユーザ パスワードが正常に変更されると、新しいユーザ パスワードがクレデンシャル データベースに格納されます。

EAP-MSCHAPv2 パスワード変更は、AD および ACS 内部 ID ストアに対してサポートされています。

AD に対する Windows マシン認証

EAP-MSCHAPv2 は、マシン認証に使用できます。EAP-MSCHAPv2 Windows マシン認証は、ユーザ認証と同じです。違いは、マシン パスワードは時間およびその他のパラメータの関数としてマシンと AD で自動的に生成できるため、Windows ドメインの Active Directory を使用する必要があることです。生成されたパスワードは、他のタイプのクレデンシャル データベースには格納できません。

ACS 5.2 での EAP-MSCHAPv2 フロー

802.1x および MSCHAPv2 認証プロセスに関連するコンポーネントは次のとおりです。

- ホスト：エンド エンティティ。つまり、エンドユーザのマシン。
- AAA クライアント：ネットワーク アクセス ポイント。
- 認証サーバ：ACS。

MSCHAPv2 プロトコルについては、RFC 2759 で説明されています。

関連トピック

- 「認証プロトコルと ID ストアの互換性」（P.B-35）

CHAP

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、ACS 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。

ACS 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、Windows 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。

LEAP

ACS は、現時点では、Cisco Aironet ワイヤレス ネットワーキングに対してだけ LEAP を使用します。このオプションをイネーブルにしないと、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 EAP-TLS などの異なる認証プロトコルを使用する場合は、このオプションをディセーブルにすることを推奨します。

（注）　[Network Configuration] 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、またはその両方をイネーブル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。

証明書アトリビュート

ACS は、次のクライアント証明書のアトリビュートを解析します。

- 証明書シリアル番号（バイナリ形式）
- エンコード証明書（バイナリ DER 形式）
- サブジェクトの CN アトリビュート
- サブジェクトの O アトリビュート（Organization）
- サブジェクトの OU アトリビュート（Organization Unit）
- サブジェクトの L アトリビュート（Location）
- サブジェクトの C アトリビュート（Country）
- サブジェクトの ST アトリビュート（State Province）
- サブジェクトの E アトリビュート（eMail）
- サブジェクトの SN アトリビュート（Subject Serial Number）
- Subject Alternative Name（SAN）

ポリシーを定義して、受信した証明書から取得されるアトリビュートとして TLS カンバセーションで使用するプリンシプル ユーザ名を設定できます。

プリンシプル ユーザ名として使用できるアトリビュートは次のとおりです。

- Subject CN
- Subject Serial-Number（SN）
- SAN
- Subject
- SAN-email
- SAN-DNS
- SAN-otherName

設定されたアトリビュートが証明書に含まれていない場合は、認証が失敗します。

（注）　ACS 5.2 では、EAP-TLS プロトコルに対してだけ、短いハードコード化されたアトリビュートと証明書アトリビュートの確認がサポートされます。

証明書のバイナリ比較

ACS が外部 ID ストアから受信する証明書に対してバイナリ比較を実行し、比較に使用される ID ストアのパラメータを判断できます。

（注）　ACS 5.2 では、証明書を保持する外部 ID ストアは LDAP だけです。

ACS は、設定されたプリンシプル ユーザ名を使用してユーザの証明書をクエリーしてから、外部 ID ストアから受信した証明書とクライアントから受信した証明書のバイナリ比較を実行します。比較は DER 証明書形式で実行されます。

テキスト アトリビュートに関連する規則

ACS は、クライアント証明書のテキスト アトリビュートを収集し、それらを ACS コンテキスト ディクショナリに配置します。ACS は、ACS の規則アトリビュートの場合と同様に、これらのアトリビュートに規則ベースのポリシーを適用できます。

規則の確認に使用できるアトリビュートは次のとおりです。

- サブジェクトの CN アトリビュート
- サブジェクトの O アトリビュート（Organization）
- サブジェクトの OU アトリビュート（Organization Unit）
- サブジェクトの L アトリビュート（Location）
- サブジェクトの C アトリビュート（Country）
- サブジェクトの ST アトリビュート（State Province）
- サブジェクトの E アトリビュート（eMail）
- サブジェクトの SN アトリビュート（Subject Serial Number）
- Subject Alternative Name（SAN）
- Subject Serial-Number（SN）
- SAN
- Subject
- SAN-DNS
- SAN-otherName

証明書の失効

ACS が受信するすべてのクライアント証明書は、定義されているポリシーに従って、Certificate Revocation List（CRL; 証明書失効リスト）で確認されます。

CRL メカニズムは、クライアント証明書にまだ依存できるかどうかを確認します。この処理は、証明書のシリアル番号と、対応する証明書チェーンの各メンバーのシリアル番号を、失効したことがわかっている証明書のリストと比較チェックすることで行います。

証明書が失効する理由として、関連付けられている秘密キーが危険にさらされて疑いがあること、または証明書が不適切に発行されたことが判明したことが考えられます。このいずれかの条件に該当する場合は、証明書が拒否されます。

ACS では、ACS データベースに設定されている CRL ファイルの取得に使用される URL のリストを含む静的 CRL がサポートされます。

信頼されている各 CA 証明書の CRL アップデートに使用される URL のセットを設定できます。デフォルトでは、CA 証明書を追加すると、ACS が証明書 *crlDistributionPoint* に格納されているすべての URL をその CA の初期静的 CRL として自動的に設定します。ほとんどの場合、*crlDistributionPoint* は CA 証明書の無効化に使用される CRL の場所を指すために使用されますが、この CA によって発行された CRL ファイルを指すように URL を編集できます。設定できるのは、CA ごとに 1 つの HTTP ベース URL だけです。

各 CA のパラメータを設定できます。この設定は、CA に対して設定されているすべての URL に適用されます。ACS では 2 つのダウンロード モードがサポートされます。一方は定期的なダウンロード用で、もう一方は前の CRL の有効期限が切れる前に次の CRL アップデートをダウンロードするためのものです。

- 定期的なダウンロードでは、ダウンロード期間を定義できます。
- 自動ダウンロードでは、CRL ファイルの期限が切れて ACS による CRL のダウンロードが必要になるまでの時間を定義します。CRL の有効期限は [CRL nextUpdate] フィールドから取得します。

どちらのモードでも、ダウンロードでエラーが発生した場合に、ACS が CRL ファイルの再ダウンロードを試行する前に待機する時間を定義できます。

ACS は、ダウンロードした各 CRL ファイルについて、ダウンロードされた CRL ファイルが信頼ストア内のいずれかの CA によって正しく署名されていることと、それらが信頼されているかどうかを確認します。ACS は、署名の確認に成功した場合にだけ CRL ファイルを使用します。確認された CRL ファイルによって、同じ CA が発行した前の CRL ファイルが置換されます。

（注） CRL ファイルは永続化されないため、ACS の再起動時に再ダウンロードする必要があります。

URL と CA への関連付けの設定は、ACS ドメイン全体に配布されます。ダウンロードした CRL は配布されず、各 ACS サーバで並行して自動的に読み込まれます。

マシン認証

ACS では、EAP コンピュータ認証をサポートする Microsoft Windows オペレーティング システムを実行しているコンピュータの認証がサポートされます。マシン認証は、コンピュータ認証とも呼ばれ、Active Directory が認識しているコンピュータに対してだけネットワーク サービスを許可します。

この機能は、物理的な作業設備外から権限のないユーザが無線アクセス ポイントにアクセスできる無線ネットワークで特に役立ちます。

マシン認証をイネーブルにした場合、3 つの異なる種類の認証が行われます。コンピュータを起動すると、次の順序で認証が行われます。

- **マシン認証**：ACS はユーザ認証の前にコンピュータを認証します。ACS は、Windows ID ストアに対してコンピュータが与えたクレデンシャルをチェックします。

  Active Directory を使用していて AD 内の一致するコンピュータ アカウントに同じクレデンシャルがある場合、コンピュータは Windows ドメイン サービスへのアクセスを許可されます。

- **ユーザ ドメイン認証**：マシン認証が成功すると、ユーザが Windows ドメインで認証されます。マシン認証が失敗すると、コンピュータは Windows ドメイン サービスへのアクセスを許可されず、ローカル オペレーティング システムに保持されているキャッシュ クレデンシャルを使用してユーザ クレデンシャルが認証されます。

  この場合、ユーザはローカル システムにだけログインできます。ドメインの代わりにキャッシュ クレデンシャルでユーザが認証された場合、コンピュータは、ドメインによって指示されたログイン スクリプトの実行などのドメイン ポリシーを適用しません。

ヒント ユーザ パスワードが最後に変更されてから、ユーザがまだコンピュータを使用してドメインに正常にログインしていない場合は、そのコンピュータのマシン認証が失敗すると、コンピュータ上のキャッシュ クレデンシャルは新規パスワードと一致しません。ユーザがこのコンピュータからドメインへ正常にログインしたことがあれば、キャッシュ クレデンシャルはユーザの古いパスワードと一致していることになります。

- **ユーザ ネットワーク認証**：ACS はユーザを認証し、ネットワーク接続を許可します。ユーザが存在する場合は、指定された ID ストアがユーザの認証に使用されます。

  ID ストアが Windows ID ストアである必要はありませんが、ほとんどの Microsoft クライアントは、ユーザ ドメイン認証と同じクレデンシャルを使用してネットワーク認証を自動的に実行するように設定できます。この方法により、シングル サインオンが可能になります。

（注）　また、Microsoft PEAP クライアントは、ユーザがログオフするたびにマシン認証を開始できます。この機能は、次のユーザ ログインのネットワーク接続を準備するためです。Microsoft PEAP クライアントは、ユーザがログオフだけではなくコンピュータをシャットダウンまたは再起動した場合にも、マシン認証を開始する場合があります。

ACS では、マシン認証に EAP-TLS、EAP-FAST、PEAP（EAP-MSCHAPv2）、および PEAP（EAP-GTC）がサポートされます。[Active Directory: General] ページでそれぞれを個別にイネーブルにして、EAP-TLS、EAP-FAST、または PEAP（EAP-MSCHAPv2）で認証した複数のコンピュータを混合させることができます。

マシン認証を実行する Microsoft オペレーティング システムでは、ユーザ認証プロトコルが、マシン認証に使用されたのと同じプロトコルに制限される場合があります。

関連トピック

- 「Microsoft AD」（P.8-38）
- 「外部 ID ストアの管理」（P.8-18）

認証プロトコルと ID ストアの互換性

ACS では、サポートされる ID ストアで認証するさまざまな認証プロトコルがサポートされます。

表 B-4 に、EAP 以外の認証プロトコルのサポートを示します。

表 B-4　EAP 以外の認証プロトコルとユーザ データベースの互換性

ID ストア	ASCII/PAP	MSCHAPv1/MSCHAPv2	CHAP
ACS	○	○	○
Windows AD	○	○	×
LDAP	○	×	×
RSA ID ストア	○	×	×
RADIUS ID ストア	○	×	×

表 B-5 に、EAP 認証プロトコルのサポートを示します。

表 B-5　EAP 認証プロトコルとユーザ データベースの互換性

ID ストア	EAP-MD5	EAP-TLS[1]	PEAP EAP-MSCHAPv2	EAP-FAST MSCHAPv2	PEAP-GTC	EAP-FAST-GTC
ACS	○	×	○	○	○	○
Windows AD	×	○	○	○	○	○
LDAP	×	○	×	×	○	○
RSA ID ストア	×	×	×	×	○	○
RADIUS ID ストア	×	×	×	×	○	○

1. EAP-TLS 認証では、ユーザは証明書の暗号確認によって認証されます。また、ACS 5.2 では、エンドユーザ クライアントから送信されたユーザの証明書を LDAP ID ストア内のユーザのレコードにある証明書とバイナリ比較することもできます。