EAP-FAST アドミニストレータ ガイド Windows Vista 版

EAP-FAST for Windows Vista Administrator Guide

2008 年 6 月

Text Part Number: OL-16949-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CONTENTS

はじめに

ここでは、『EAP-FAST アドミニストレータ ガイド Windows Vista 版』の概要を紹介した後、その他の資料とテクニカル サポートを取得する方法について説明します。

この章では、次の項目について説明します。

対象読者

このガイドは、Windows Vista 用 EAP-FAST モジュールのインストールおよび設定を担当する管理者を対象としています。この管理者は、コンピューティング デバイスや、ネットワークの構造、用語、および概念について理解しており、Windows Vista オペレーティング システムに関する知識を有している必要があります。また、Microsoft のグループ ポリシー オブジェクト (GPO) の設定および導入方法を理解しており、加えて、Microsoft のグループ ポリシー オブジェクト エディタを使い慣れている必要があります。さらに、XML スキーマの扱い方も理解している必要があります。

目的

このガイドでは、Windows Vista 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上での EAP-FAST モジュールの設定および管理作業について説明します。

注 このガイドで説明する EAP-FAST モジュールが正常に動作するオペレーティング システムは Windows Vista のみです。

マニュアルの構成

このガイドは以下の章で構成されています。

第 1 章「EAP-FAST の概要」- EAP-FAST（Flexible Authentication via Secure Tunneling; セキュア トンネリングを介したフレキシブル認証）の概要を紹介します。

第 2 章「EAP-FAST モジュールのインストール」- EAP-FAST モジュールのインストール方法について説明します。

第 3 章「EAP-FAST の設定」- ユーザ インターフェイスで EAP-FAST モジュールを設定する方法について説明します。

第 4 章「ユーザに配布する EAP-FAST プロファイルの作成と変更」- グループ ポリシー オブジェクト エディタを使用して、または XML スキーマを変更して、EAP-FAST モジュールのプロファイルを設定する方法について説明します。また、EAP-FAST のマシン認証シングル サインオン サポートについても説明します。

第 5 章「ロギングの設定」- トラブルシューティングに役立つ、EAP-FAST モジュールのロギングの設定方法について説明します。

第 6 章「トラブルシューティング」- EAP-FAST エラーおよびプロンプト メッセージについて説明します。また、強固なパスワードを作成するためのガイドラインも示します。

付録 A「略語」- このガイドで使用されているすべての略語の完全表記を示します。

表記法

このガイドでは、次の表記法に従って手順および情報を記載します。

- コマンドは**太字**で記述します。
- 変数は*イタリック体*で記述します。
- 注および注意には、次の表記法と記号を使用します。

注　「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意　「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

資料の入手方法、サポートの利用方法、およびセキュリティに関するガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスとシスコのマニュアルに関する全般的な情報については、次の URL で、毎月更新される『What's New in Cisco Product Documentation』を参照してください。『What's New in Cisco Product Documentation』には、シスコの新規および改訂版の技術マニュアルの一覧が示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

EAP-FAST の概要

この章では、EAP-FAST（Flexible Authentication via Secure Tunneling; セキュア トンネリングを介したフレキシブル認証）の概要を紹介します。この章の内容は次のとおりです。

EAP-FAST について

注 EAP-FAST の詳細は、RFC4851 を参照してください。

EAP-FAST は、Transport Layer Security（TLS）によりクライアントと認証サーバ間でセキュリティ保護された通信を可能にし、相互認証されたトンネルを確立する EAP（拡張認証プロトコル）方式です。トンネル内では、クライアントと認証サーバ間でさらなる認証関連データを送信するために、Type-Length-Value（TLV; タイプ、長さ、値）形式のデータが使用されます。

EAP-FAST は RFC 4507 で定義されている TLS 拡張をサポートしているため、サーバ上でセッションごとの状態を保持しなくても、セキュリティ保護されたトンネルをすばやく再確立することができます。EAP-FAST ベースのメカニズムは、TLS 拡張のクレデンシャルをプロビジョニングするように定義されています。これらのクレデンシャルは Protected Access Credential（PAC）と呼ばれます。

EAP-FAST には、以下のような特徴があります。

- 相互認証

  EAP サーバ側でクライアントの ID と信頼性を検証でき、クライアント側で EAP サーバの信頼性を検証できる必要があります。

- 消極的辞書攻撃に対する耐性

  多くの認証プロトコルでは、パスワードが要求され、そのパスワードはクライアントによって EAP サーバに（クリアテキストまたはハッシュ値として）明示的に提供されます。通信において、パスワードなどの脆弱なクレデンシャルは傍受されないようにする必要があります。

- MITM（中間者）攻撃に対する耐性

  相互認証済みの保護されたトンネルを確立する際に、攻撃者がクライアントと EAP サーバ間の通信に割り込んで情報を差し替えるのをプロトコルによって回避する必要があります。

- ほとんどのパスワード認証インターフェイスに対応できる柔軟性

  クライアントを認証するためのパスワード インターフェイスには、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（MS-CHAP）、Lightweight Directory Access Protocol（LDAP）、One-Time Password（OTP）など、さまざまなものがあります。EAP-FAST では、これらの多様なパスワード タイプをサポートしています。

- コンピュータ リソースおよび電力消費の効率性

  特にワイヤレス メディアを使用している場合は、クライアントが使用できるコンピュータ リソースおよび電力は限られています。EAP-FAST により、より効率的な方法でネットワークにアクセスすることが可能になります。

- トンネル内で通信を拡張できる柔軟性

  ネットワーク インフラストラクチャの複雑化に伴って、認証、許可、アカウンティングも、ますます複雑になってきています。たとえば、相互認証を行うために複数の既存の認証プロトコルが必要な場合があります。また、クライアントの認証成功時に、適切な許可を行うために、タイプの異なる保護された通信が必要となる場合もあります。

- ユーザごとの認証における認証サーバの要件を最小限に抑える

  大規模な導入では、通常、複数のクライアントの認証サーバとして機能する複数のサーバが存在します。クライアントは、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な方法で、共有秘密キーを使用してトンネルをセキュリティ保護します。EAP-FAST により、クライアントによる単一の強固な共有秘密キーの使用が促進されると同時に、認証サーバによるユーザごとのデバイス状態のキャッシュおよび管理を最小限に抑えることが可能になります。

EAP-FAST の機能

以下の項では、EAP-FAST の機能について説明します。

- 2 つのフェーズから成るトンネルされた認証（1-2 ページ）
- Protected Access Credential（1-2 ページ）
- サーバの証明書評価（1-3 ページ）

2 つのフェーズから成るトンネルされた認証

EAP-FAST では、2 つのフェーズから成るトンネルされた認証プロセスが使用されます。

認証の第 1 フェーズでは、TLS ハンドシェイクを使用して、認証キーの交換を行い、クライアントと認証サーバ間の保護されたトンネルを確立します。トンネルでは、クライアント ID 情報がトンネル外に開示されないように保護されます。このフェーズでは、クライアントとサーバは、確実に互換性のあるバージョンのプロトコルを使用するようにするために、EAP-FAST バージョンのネゴシエーションを使用します。

トンネルが確立されると、認証の第 2 フェーズが始まります。必要な認証および許可ポリシーを確立するために、クライアントとサーバ間でさらに通信が行われます。このフェーズでは、TLV オブジェクトにカプセル化された状態で一連の要求と応答がやり取りされます。この TLV 交換では、保護されたトンネル内で EAP 方式が使用されます。TLV オブジェクトおよび TLV の形式の詳細は、RFC 4851 の 4.2 項を参照してください。

EAP-FAST モジュールには、トンネルを確立するために自動と手動のどちらの PAC プロビジョニングを使用するか、トンネルを確立するためにサーバ証明書を使用するかどうか、認証とプロビジョニングにどのタイプのユーザ クレデンシャルを使用するか、確立されたトンネルでどのタイプの認証方式を使用するか、など、さまざまな EAP-FAST 設定オプションが用意されています。

Protected Access Credential

Protected Access Credential（PAC）は、最適なネットワーク認証を実現するためにクライアントに配布されるクレデンシャルです。PAC を使用することで、クライアントと認証サーバ間で認証トンネルを確立することができます（「2 つのフェーズから成るトンネルされた認証」（1-2 ページ）で説明されている、認証の第 1 フェーズ）。PAC は、共有秘密キー、不透明要素、その他の情報という、最大 3 つのコンポーネントで構成されます。

共有秘密キー コンポーネントには、クライアントと認証サーバ間の事前共有キーが含まれます。PAC-Key と呼ばれる、この事前共有キーにより、認証の第 1 フェーズでトンネルが確立されます。

クライアントがネットワーク リソースへのアクセスを要求した場合には、不透明コンポーネントがクライアントとサーバに提供されます。PAC-Opaque と呼ばれる、このコンポーネントは可変長フィールドで、トンネル確立時に認証サーバに送信されます。EAP サーバは、PAC-Opaque を解釈して必要な情報を取得し、クライアントの ID および認証を検証します。PAC-Opaque には、PAC-Key が含まれており、PAC のクライアント ID が含まれる場合もあります。

PAC には、その他の情報も含まれる場合があります。PAC-Info と呼ばれる、このコンポーネントは可変長フィールドで、少なくとも PAC 発行元（PAC を作成したサーバ）の機関 ID を提供するために使用されます。その他の、有用であるが必須ではない情報（PAC-Key の有効期限など）も、PAC のプロビジョニングまたは更新時に、PAC 発行元サーバからクライアントに伝えることができます。

PAC は、Cisco Secure ACS などの PAC 認証機関によって作成および発行され、ID で識別されます。ユーザはサーバから自分の PAC のコピーを取得し、その ID で PAC とプロファイルがリンクされます。

マシン PAC などの永続 PAC は、EAP-FAST レジストリに保存され、暗号化されます。これらの PAC は、アクセス コントロール リスト（ACL）でも保護されているため、アクセスできるのは、指定されたユーザ（PAC の所有者）と特権ユーザ グループ（管理者など）だけです。マシン PAC は、そのマシンのすべてのユーザが使用できるように、グローバルに保存されます。

すべての PAC は、Microsoft Crypto API（CryptoProtectData）で暗号化され、ホスト マシンに関連付けられます。PAC は、他のマシンにコピーしたり、他のマシンで使用したりできません。

ユーザ認証 PAC など、すべての非永続 PAC は、揮発性メモリに保存されるため、リブート後やユーザがログオフした後に削除されます。

サーバの証明書評価

EAP-FAST 認証の第 1 フェーズの TLS ネゴシエーションでは、認証サーバがクライアントに証明書を付与します。クライアントは、EAP サーバ証明書の有効性を検証し、また、与えられた EAP サーバ名を確認して、そのサーバを信頼できるかどうかを判断する必要があります。

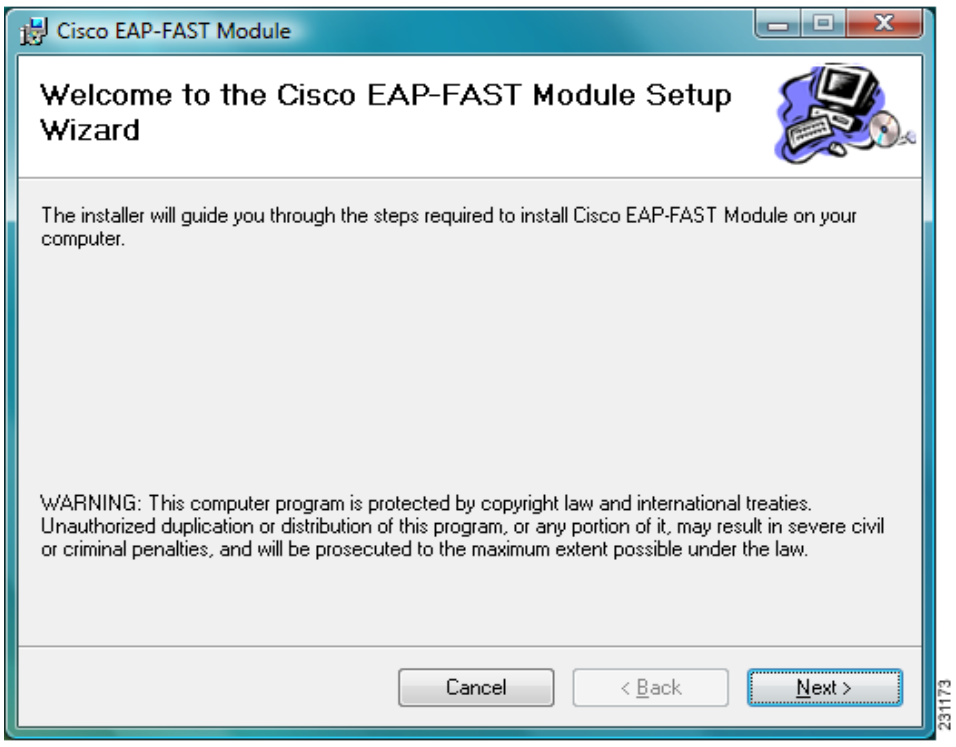
CHAPTER 2

EAP-FAST モジュールのインストール

EAP-FAST モジュールをインストールするには、次の手順を実行します。

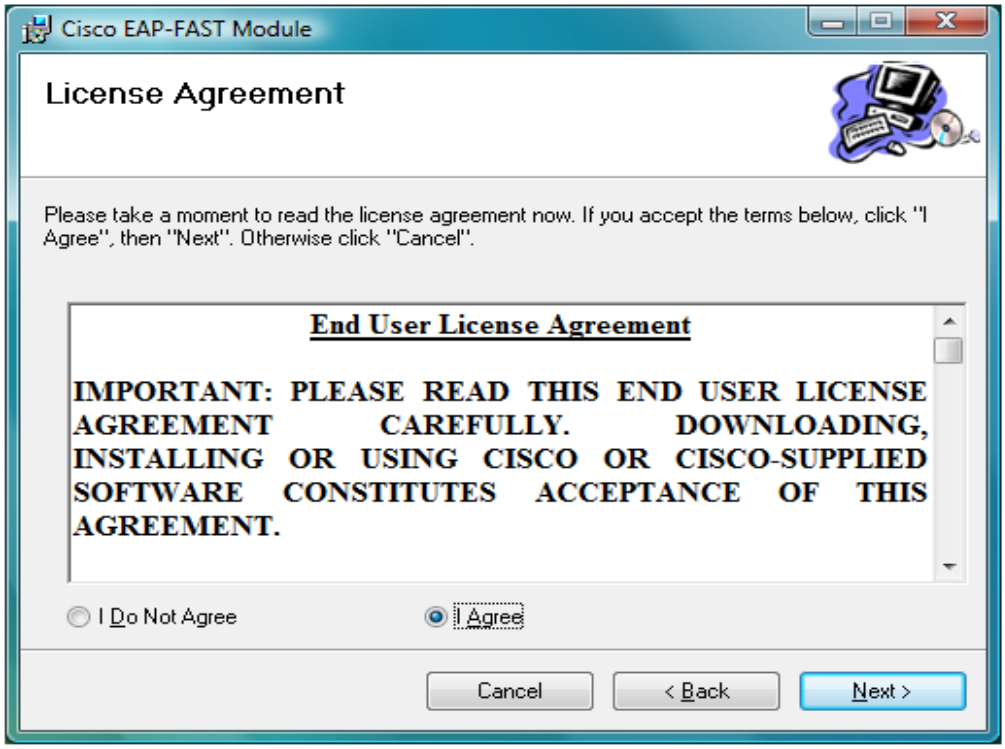
手順 1 EAP-FAST Module Setup Wizard アイコンをダブルクリックします。Welcome ウィンドウが表示されます（図 2-1 を参照）。

図 2-1 Welcome ウィンドウ



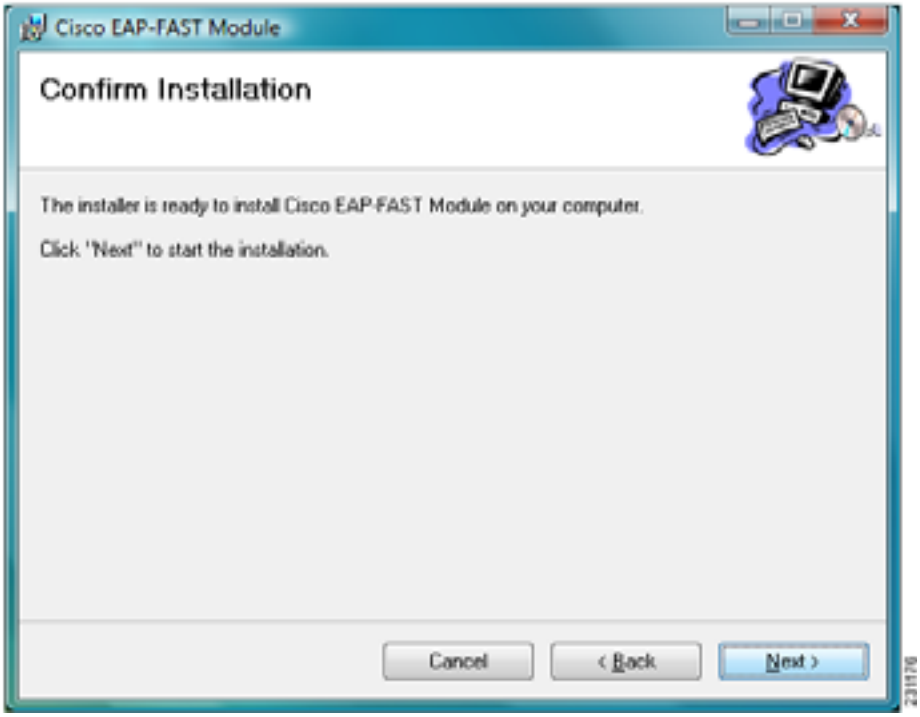
手順 2　Welcome ウィンドウで、**Next** をクリックします。License Agreement ウィンドウが表示されます（図 2-2 を参照）。

図 2-2　License Agreement ウィンドウ



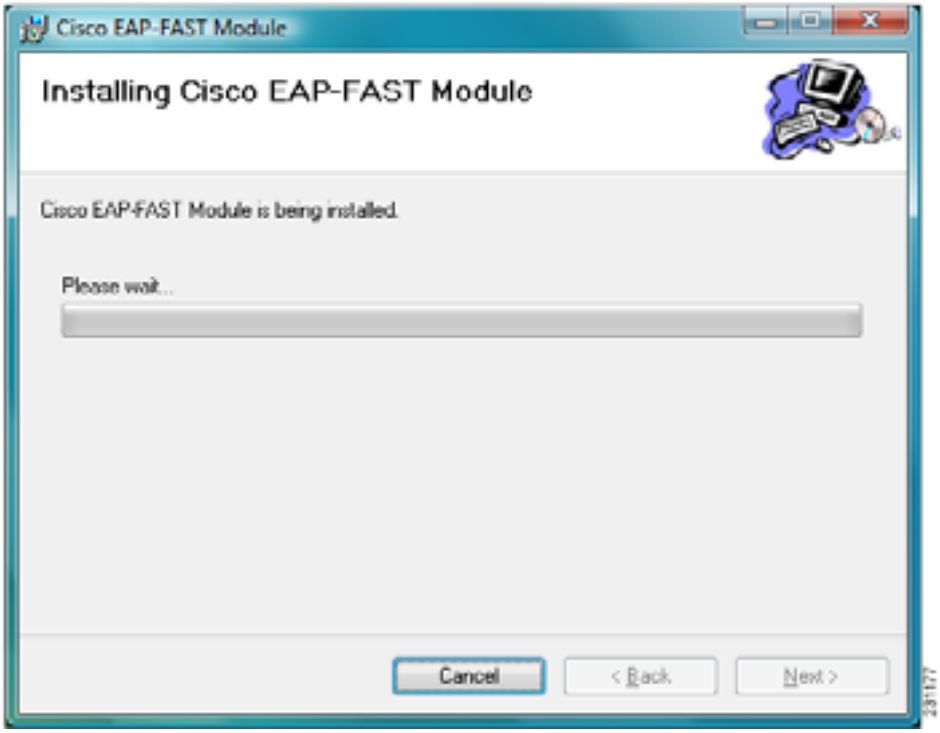
手順 3　License Agreement ウィンドウで、**I Agree** ラジオ ボタンをクリックしてライセンス契約に同意します。次に **Next** をクリックします。Confirm Installation ウィンドウが表示されます（図 2-3 を参照）。

図 2-3　Confirm Installation ウィンドウ



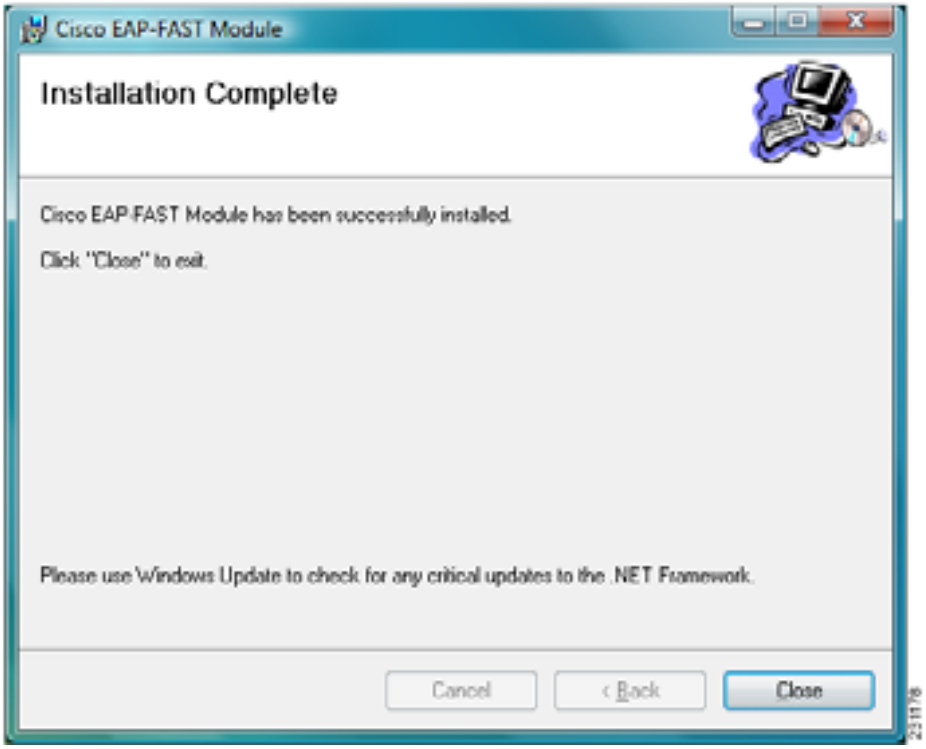
手順 4　Confirm Installation ウィンドウで、**Next** をクリックしてインストールを開始します。Installing Cisco EAP-FAST Module ウィンドウに、インストールの進行状況が表示されます（図 2-4 を参照）。

図 2-4　Installing Cisco EAP-FAST Module ウィンドウ



手順 5　EAP-FAST モジュールのインストールが完了すると、Installation Complete ウィンドウが表示されます（図 2-5 を参照）。

図 2-5　Installation Complete ウィンドウ



手順 6　**Close** ボタンをクリックします。

EAP-FAST モジュールは次の場所にインストールされます。

%Program Files¥Cisco¥Cisco EAP-FAST Module

CHAPTER 3

EAP-FAST の設定

この章では、接続設定、ユーザ クレデンシャル、認証方式など、EAP-FAST モジュールの設定を行う方法について説明します。

この章では、次の項目について説明します。

EAP-FAST のプロパティの設定

EAP-FAST Properties ウィンドウにアクセスするには、次の手順を実行します。

手順 1　デスクトップの左下にある **Start** ボタンをクリックします。

手順 2　右側のペインで **Network** を右クリックします。

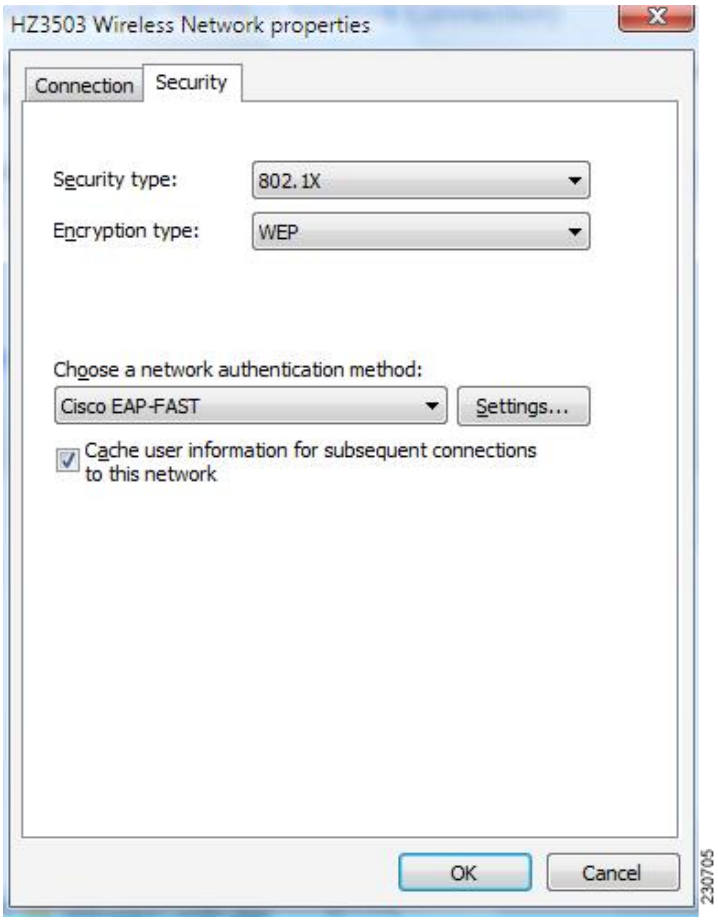
手順 3　**Properties** を選択します。

手順 4　左側のペインで **Manage wireless networks** を選択します。

手順 5　対象のワイヤレス ネットワークをダブルクリックします。

手順 6　**Wireless Network properties** ウィンドウで、**Security** を選択します（図 3-1 を参照）。

図 3-1　Wireless Network Properties ウィンドウ



手順 7　Choose a network authentication method ドロップダウン リストから **Cisco EAP-FAST** を選択します。

手順 8　**Settings** ボタンをクリックします。

手順 9　**Connection** タブ、**User Credentials** タブ、**Authentication** タブ、または **About** タブをクリックします。これらのタブの設定方法については、「Connection タブの設定」（3-3 ページ）、「ユーザ クレデンシャルの設定」（3-7 ページ）、および 「認証方式の設定」（3-10 ページ）を参照してください。デバイスでモジュールのバージョンを確認する方法については、「EAP-FAST モジュールのバージョンの確認」（3-12 ページ）を参照してください。

Connection タブの概要

EAP-FAST の Connection タブには、外部 Transport Layer Security（TLS）トンネルを確立するための設定が表示されます。設定には、ID の保護、Protected Access Credential（PAC）の使用方法、PAC のプロビジョニング、認証されたサーバ証明書をトンネルの確立に使用する方法、信頼済みルート CA（認証局）証明書のリストにある信頼済みルート CA の使用方法が含まれます。

Connection タブの設定

Connection タブで接続設定を行うことができます（図 3-2 を参照）。

図 3-2　EAP-FAST Properties ウィンドウの Connection タブ

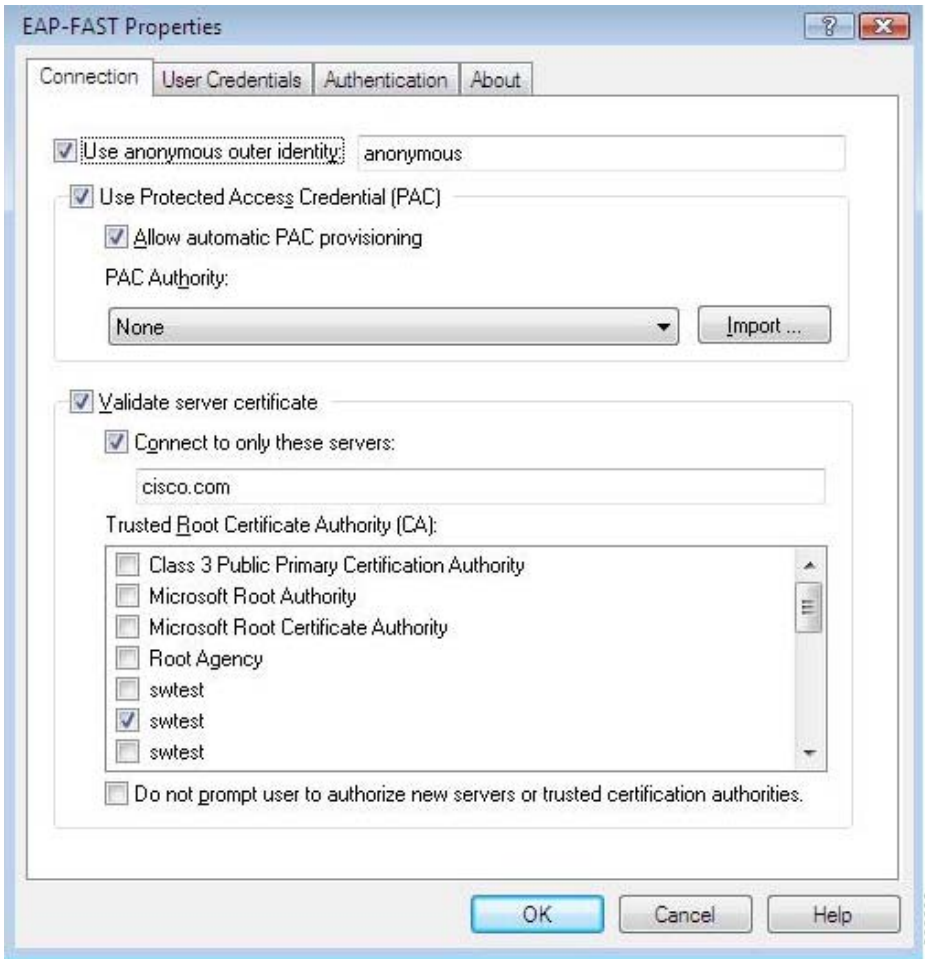


表 3-1 に、すべての接続設定とその説明を示します。

表 3-1　接続設定

接続設定	説明
Use anonymous outer identity	ID のプライバシー保護を有効にするには、このチェックボックスをオンにします。 **デフォルト**：オン
外部 ID フィールド	Use anonymous outer identity チェックボックスがオンの場合、外部 ID を入力します。外部 ID フィールドに入力する値については、管理者の指示または RFC 4282 に従ってください。 **デフォルト**：anonymous **注**　このフィールドに入力できる最大文字数は 256 文字です。
Use Protected Access Credential (PAC)	トンネルの確立で PAC の使用を有効にするには、このチェックボックスをオンにします。このチェックボックスがオンの場合、PAC のプロビジョニングが要求されます。このチェックボックスがオフの場合は、EAP-FAST が PEAP として動作し、毎回トンネルを確立する際に、認証されたサーバ証明書のみが使用されます。 PAC は、クライアントとサーバの相互認証に使用される一意の共有クレデンシャルです。特定のクライアントのユーザ名とサーバの機関 ID に関連付けられます。PAC を使用すれば、Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）とデジタル証明は必要なくなります。PAC は、自動あるいは手動で、クライアントに配布またはインポートされます。 手動 PAC プロビジョニングの場合、PAC ファイルが AAA サーバまたは EAP-FAST サーバでローカルに生成されます。手動プロビジョニングでは、ユーザ クレデンシャルがサーバに提供され、そのユーザに対する PAC ファイルが生成されます。この後、この PAC をクライアント デバイスに手動でインストールする必要があります。 **デフォルト**：オン
Allow automatic PAC provisioning	EAP-FAST 認証で PAC の自動取得を有効にするには、このチェックボックスをオンにします。 自動 PAC プロビジョニングを有効にすると、EAP-FAST 認証で PAC を自動的に取得できます。自動 PAC プロビジョニングでは、TLS と Diffie-Hellman Key Agreement プロトコルを使用して、安全なトンネルを確立します。また、MSCHAPv2 を使用して、クライアントの認証と MITM（中間者）攻撃の早期検出が行われます。 **デフォルト**：オン
PAC Authority	ドロップダウン リストから PAC 認証機関を選択します。 **デフォルト**：None **注**　ドロップダウン リストには、以前にトンネル PAC をプロビジョニングしたすべての PAC 認証機関の名前が含まれています。PAC をプロビジョニングしたことがない場合は、None のみが表示されます。None を選択して、強制的にホストに PAC のプロビジョニングを要求させることもできます。

表 3-1　接続設定 （続き）

接続設定	説明
Import	手動で PAC ファイルをインポートするには、**Import** ボタンをクリックします。このボタンをクリックすると、Import Protected Access Credentials (PAC) File ウィンドウが表示されます。選択した PAC ファイルのパスワードを入力する必要がある場合は、パスワード ウィンドウが表示されます。 有効な PAC ファイルを選択し、インポートすると、その PAC 認証機関が PAC 認証機関ドロップダウン リストに追加されます。 **デフォルト**：有効
Validate server certificate	トンネルの確立で、認証されたサーバ証明書を使用するには、このチェックボックスをオンにします。**Use Protected Access Credentials (PAC)** チェックボックスと **Validate Server Certificate** チェックボックスは両方ともオンにすることができます。両方ともオンになっている場合は、ホスト システムにインストールされている信頼済み CA 証明書のリストから、1 つまたは複数の信頼済み CA 証明書を選択できます。 両方のチェックボックスがオンになっている場合、EAP-FAST モジュールは必ず PAC を最初に使用しようとします。PAC がないか、サーバに拒否された場合、EAP-FAST モジュールはサーバ証明書を使用します。 両方のチェックボックスがオフになっている場合、EAP-FAST はサーバ証明書を検証せずに PEAP と同様に機能します。基本的な信頼性の検証が行われないため、両方のチェックボックスをオフにすることはお勧めしません。 **デフォルト**：オフ
Connect to only these servers	サーバから提供されたサーバ証明書と一致する必要があるオプションのサーバ名を入力するには、このチェックボックスをオンにします。サーバ名をセミコロンで区切り、複数のサーバ名を入力することができます。サーバ証明書のサブジェクト フィールド（CN）が、このフィールドに入力したサーバ名と一致した場合のみ、EAP-FAST モジュールは、プロンプトを表示せずに、接続の継続を許可します。 **デフォルト**：オフ **注**　サーバ名には、ワイルドカード文字としてアスタリスク（*）を使用できます。ただし、アスタリスクは name.domain.com 形式の最初のピリオド（.）より前に指定する必要があります。たとえば、「*.cisco.com」は「.cisco.com」で終わるすべてのサーバ名と一致します。サーバ名のこれ以外の場所にアスタリスクを指定すると、ワイルドカード文字として認識されません。

表 3-1　接続設定 （続き）

接続設定	説明
Trusted Root CA	システムにインストールされている証明書のリストから、1 つまたは複数の信頼済みルート CA 証明書を選択します。ホスト システムにインストールされている信頼済み CA 証明書のみが、ドロップダウン リストに表示されます。 選択した信頼済みルート CA 証明書の詳細を表示するには、証明書名をダブルクリックします。証明書名をダブルクリックすると、Windows の証明書のプロパティ画面が表示されます。この画面で、証明書の詳細を確認できます。 **デフォルト**：None
Do not prompt user to authorize new servers or trusted certificate authorities.	サーバ名が一致しない場合、またはサーバ証明書が、選択した信頼済みルート CA 証明書のいずれでも署名されていない場合に、ユーザに接続の認証を求めないようにするには、このチェックボックスをオンにします。このような場合に、このチェックボックスがオンになっていると、認証は失敗します。 **デフォルト**：オフ

User Credentials タブの概要

EAP-FAST モジュールでは、認証およびプロビジョニングで、クライアント証明書とユーザ名 / パスワードの両方をユーザ クレデンシャルとして使用できます。

クライアント証明書

クライアント証明書が使用される場合、EAP-FAST モジュールは自動的に、現在のユーザの Windows 証明書ストアからクライアント証明書を取得します。また、EAP-FAST モジュールは、ログオンしているユーザのユーザ名と一致するユーザ証明書を検出します。この証明書が期限切れになることはありません。

複数のユーザ証明書がある場合、EAP-FAST モジュールは、いずれかを選択するようユーザに求め、その選択がプロファイルに保存されます。デフォルトでは、ユーザ証明書は、保護された TLS トンネル内で EAP-TLS 内部方式または TLS 再ネゴシエーションにより、セキュリティ保護された状態で送信されます。トンネルが確立された後に、EAP-FAST サーバが、クライアント証明書を要求するための TLS 再ネゴシエーションを開始しなかった場合は、EAP-FAST モジュールが EAP-TLS 内部方式により証明書を送信します。

EAP-FAST モジュールの管理者は、これらのセキュリティ対策を講じなくても、ユーザ証明書を送信できるように、EAP-FAST モジュールの XML スキーマを設定することができます。

ユーザ名とパスワード

ユーザ名とパスワードが使用される場合、ユーザは次のいずれかのタイプのユーザ名とパスワードを指定します。

- Windows のユーザ名とパスワード — ネットワーク アクセス クレデンシャルとして Windows のユーザ名とパスワードが使用されます。パスワードが無効な場合や、パスワードの変更が必要な場合以外、ユーザにユーザ名とパスワードの入力を求められることはありません。
- 求められたユーザ クレデンシャル — ユーザは認証時にクレデンシャルを指定するよう求められます。このクレデンシャルは、Lightweight Directory Access Protocol（LDAP）クレデンシャルなど、Windows のユーザ名とパスワードとは別のクレデンシャルです。

- 保存済みユーザ クレデンシャル — EAP-FAST 設定で入力されたユーザ クレデンシャルです。保存済みクレデンシャルが失敗した場合や期限切れになった場合以外、ユーザに認証時にクレデンシャルが求められることはありません。認証成功後にユーザが入力した新しいクレデンシャルは、設定に自動的に保存されます。古い保存済みクレデンシャルを変更するために設定画面に戻る必要はありません。
- 1 回限りのパスワード（OTP）— ユーザは OTP を手動で入力する必要があります。OTP の新規 PIN モードおよびネクスト トークン モードがサポートされています。

ユーザ クレデンシャルの設定

User Credentials タブでユーザ クレデンシャルを設定できます（図 3-3 を参照）。

図 3-3　EAP-FAST Properties ウィンドウの User Credentials タブ

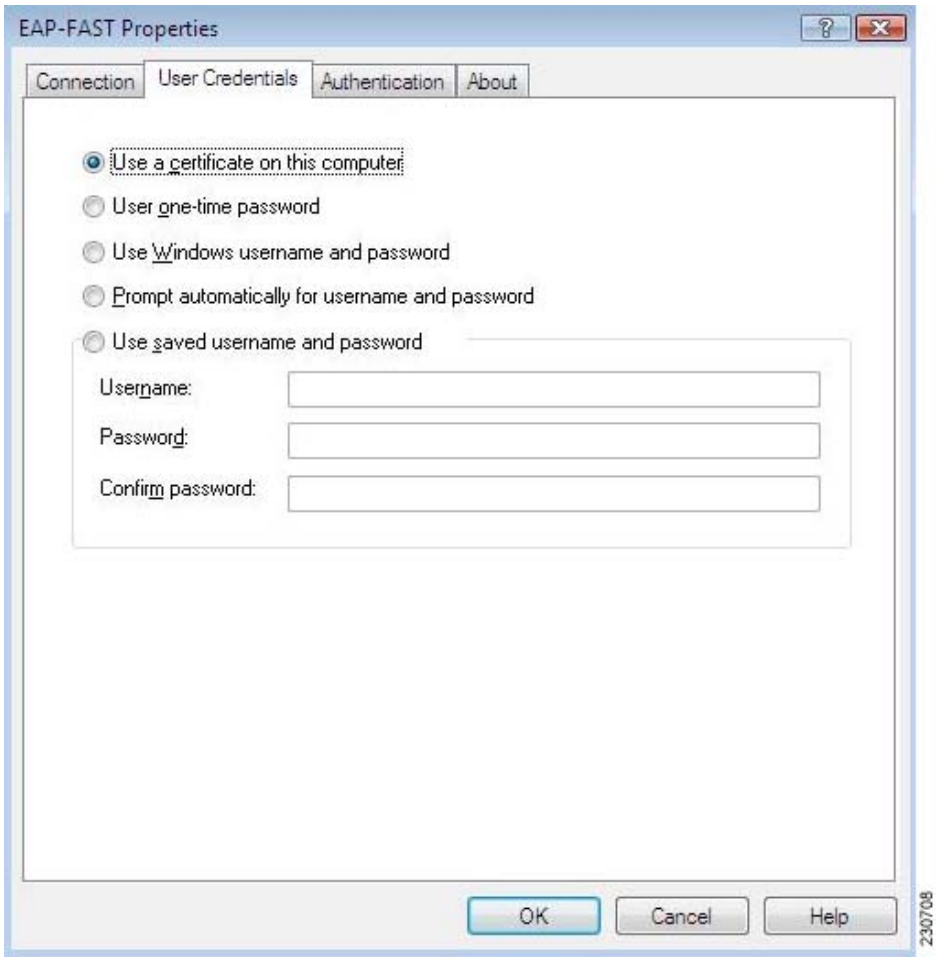


表 3-2 に、ユーザ クレデンシャルのすべてのオプションとその説明を示します。

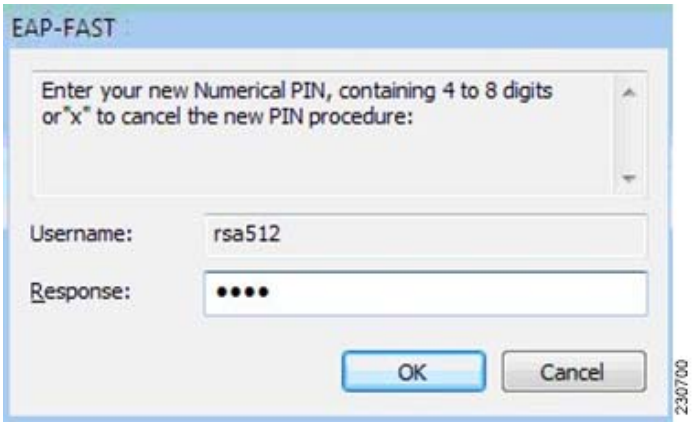
表 3-2　ユーザ クレデンシャルのオプション

ユーザ クレデンシャル	説明
Use a certificate on this computer	現在のユーザの Windows 証明書ストアからクライアント証明書を自動的に取得するには、このラジオ ボタンをクリックします。 **デフォルト**：オフ
Use one-time password	1 回限りのパスワード（OTP）を使用するには、このラジオ ボタンをクリックします。OTP の詳細は、「OTP に関する PIN モードとトークン モードの概要」（3-9 ページ）を参照してください。 **デフォルト**：オフ
Use Windows username and password	ネットワーク認証で、Windows のユーザ名とパスワードを EAP-FAST のユーザ名とパスワードとして使用するには、このラジオ ボタンをクリックします。 **デフォルト**：オン
Prompt automatically for username and password	認証を試行するたびに、Windows のユーザ名とパスワードに加えて、EAP-FAST のユーザ名とパスワードを入力するようユーザに求めるには、このラジオ ボタンをクリックします。このオプションは、LDAP など、Windows 以外のパスワードをサポートしています。 **デフォルト**：オフ
Use saved username and password	ユーザが EAP-FAST のユーザ名とパスワードを毎回入力する必要がないようにするには、このラジオ ボタンをクリックします。認証は、必要に応じて、保存されているユーザ名とパスワードを使用して自動的に行われます。ユーザ名とパスワードはバックエンド サーバに登録されています。 **デフォルト**：オフ このオプションを選択した場合、ユーザは次の情報を入力する必要があります。 • Username — 次のいずれかの形式で、ユーザ名とドメイン名を入力します。 – ドメイン修飾ユーザ名 - domain¥user – ユーザ プリンシパル名（UPN）- user@domain.com • Password — パスワードを入力します。この暗号化されたパスワードは、EAP-FAST 設定に保存されます。 • Confirm password — パスワードを正しく入力したことを確認するために、もう一度パスワードを入力します。 **注**　ユーザ名とパスワードに入力できる最大文字数は 256 文字です。

OTP に関する PIN モードとトークン モードの概要

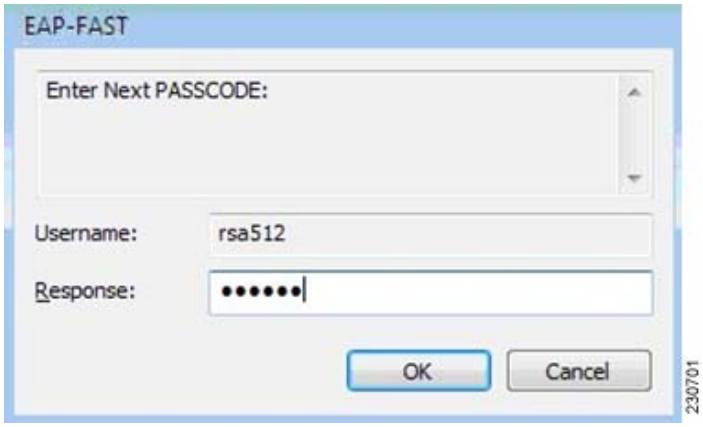
OTP の新規 PIN モードがサポートされています。新規 PIN が必要な場合、バックエンド サーバは、新規 PIN が必要であることを示すために、テキスト メッセージ（「新規 PIN を入力してください」など）を送信します。その後、EAP-FAST モジュールは、サーバからのテキスト メッセージを含むプロンプト ウィンドウを表示します（図 3-4 を参照）。バックエンド サーバは、ユーザが入力した新規 PIN を確認するために、PIN を 2 回入力するようユーザに求める場合があります。

図 3-4　　新規 PIN の入力を求めるプロンプト ウィンドウ



OTP のネクスト トークン モードもサポートされています。ネクスト トークンが必要な場合、バックエンド サーバは、ネクスト トークンが必要であることを示すために、テキスト メッセージ（「次のパスコードを入力してください」など）を送信します。その後、EAP-FAST モジュールは、サーバから送信されたテキスト メッセージを含むプロンプト ウィンドウを表示します（図 3-5 を参照）。ユーザは、OTP デバイスまたはソフトウェアからネクスト トークンを取得し、そのトークンをプロンプト フィールドに入力する必要があります。

図 3-5　　ネクスト トークンの入力を求めるプロンプト ウィンドウ



Authentication タブの概要

EAP-FAST モジュールは、EAP-GTC、EAP-MSCHAPv2、EAP-TLS の 3 つの認証方式をサポートしています。

この 3 つの認証方式では、次のタイプのクレデンシャルが使用されます。

- EAP-GTC — Active Directory のパスワード、OTP、トークン、LDAP
- EAP-MSCHAPv2 — Active Directory のパスワード
- EAP-TLS — 証明書

EAP-GTC モジュールは EAP-FAST モジュールにバンドルされています。EAP-GTC モジュールは EAPHost フレームワークに登録されておらず、他のアプリケーションでは使用できません。

EAP-MSCHAPv2 モジュールの変更バージョンも EAP-FAST モジュールにバンドルされています。この変更バージョンは、EAP-MSCHAPv2 チャレンジの変更に対応するために、匿名 TLS プロビジョニング モードで使用されます。このモジュールは、変更のない認証モードのユーザ認証もサポートしています。

EAP-FAST モジュールは、Windows Vista に付属する標準の EAP-TLS モジュールを使用します。

ユーザ インターフェイスで、この 3 つの内部認証方式のいずれか 1 つのみを選択できます。他のサードパーティの EAP 方式も、EAPHost フレームワークに登録されており、管理者インターフェイスで選択できますが、まだ正式にテストされていません。

認証方式の設定

Authentication タブで認証の設定を選択できます（図 3-6 を参照）。

図 3-6　EAP-FAST Properties ウィンドウの Authentication タブ

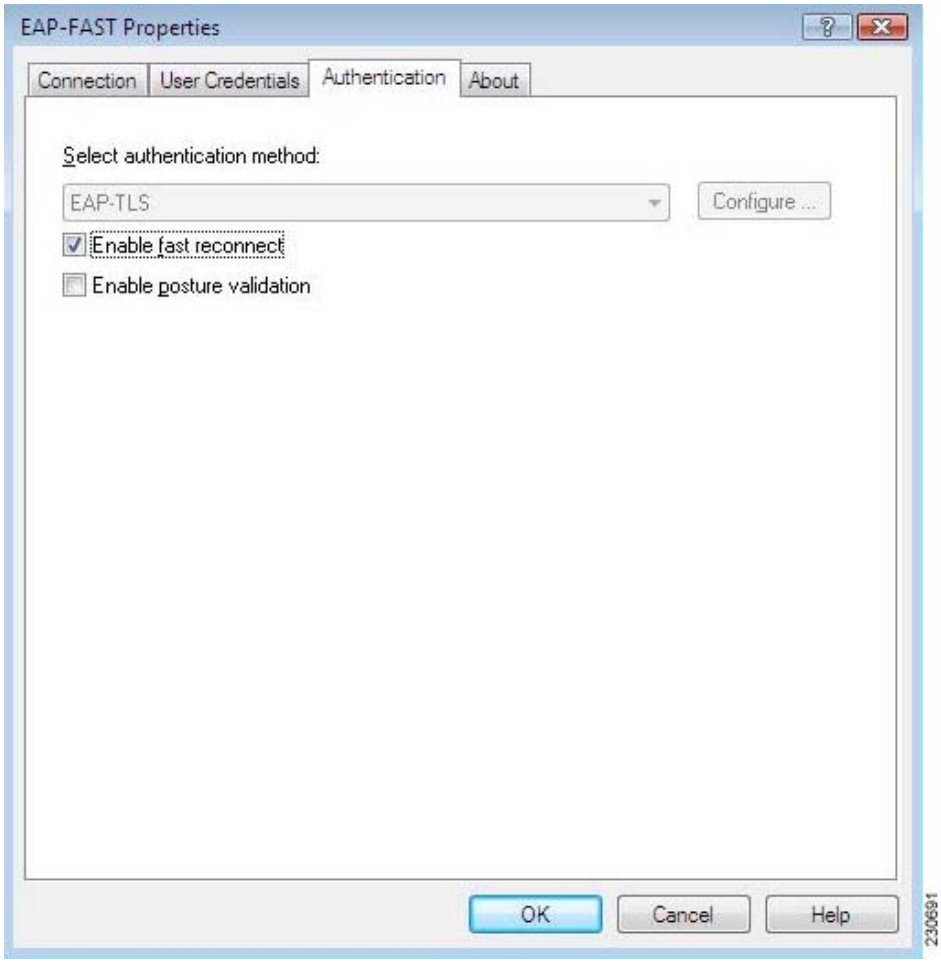


表 3-3 に、認証のオプションとその説明を示します。

表 3-3　認証設定

認証設定	説明
Select an authentication method	ドロップダウン リストから内部トンネルの EAP 方式を選択します。EAP-GTC、EAP-MSCHAPv2、EAP-TLS、Any Method の中から選択できます。 Any Method オプションを選択した場合、EAP-FAST モジュールは、EAP サーバが要求するサポート対象方式をどれでも選択できるようになります。また、この方式は、使用するユーザ クレデンシャルに適したものである必要があります。 **デフォルト**：Any Method **注**　User Credentials タブで **Use one-time password** ラジオ ボタンを選択した場合、選択可能なオプションは EAP-GTC のみになります。 **注**　User Credentials タブで **Use a certificate on this computer** ラジオ ボタンを選択した場合、選択可能なオプションは EAP-TLS のみになります。 **注**　Any Method を選択してすべての方式を許可することは、Cisco または Microsoft によってサポートされておらず、またお勧めできません。この設定は「現状のまま」使用することになります。Cisco は、サポートされていない方式が使用された場合に生じたシステムの不具合について、一切保証しません。実稼働環境では、サポートされていない方式を使用しないでください。
Configure	EAP-TLS オプションを設定するには、**Configure** ボタンをクリックします。このオプションは、認証方式として EAP-TLS を選択した場合のみ、有効になります。このボタンをクリックすると、Windows Vista 標準の EAP-TLS のプロパティ画面が表示されます。 **デフォルト**：無効
Enable fast reconnect	セッションの再開を許可するには、このチェックボックスをオンにします。 EAP-FAST モジュールでは、ユーザ認証 PAC を使用することで、再接続（セッションの再開とも呼ばれる）が迅速に行われます。Enable fast reconnect をオンにすると、クレデンシャルを再入力することなく、ローミングしたり、サスペンド モードから復帰したりすることができます。この機能は、複数のネットワーク アクセス サーバにわたって使用できます。 **デフォルト**：オン **注**　プロファイルを切り替えた場合、ログオフした場合、またはリブートした場合、再接続は迅速に試行されません。再認証が必要です。
Enable posture validation	ホスト マシンの状態の問い合わせを許可するには、このチェックボックスをオンにします。

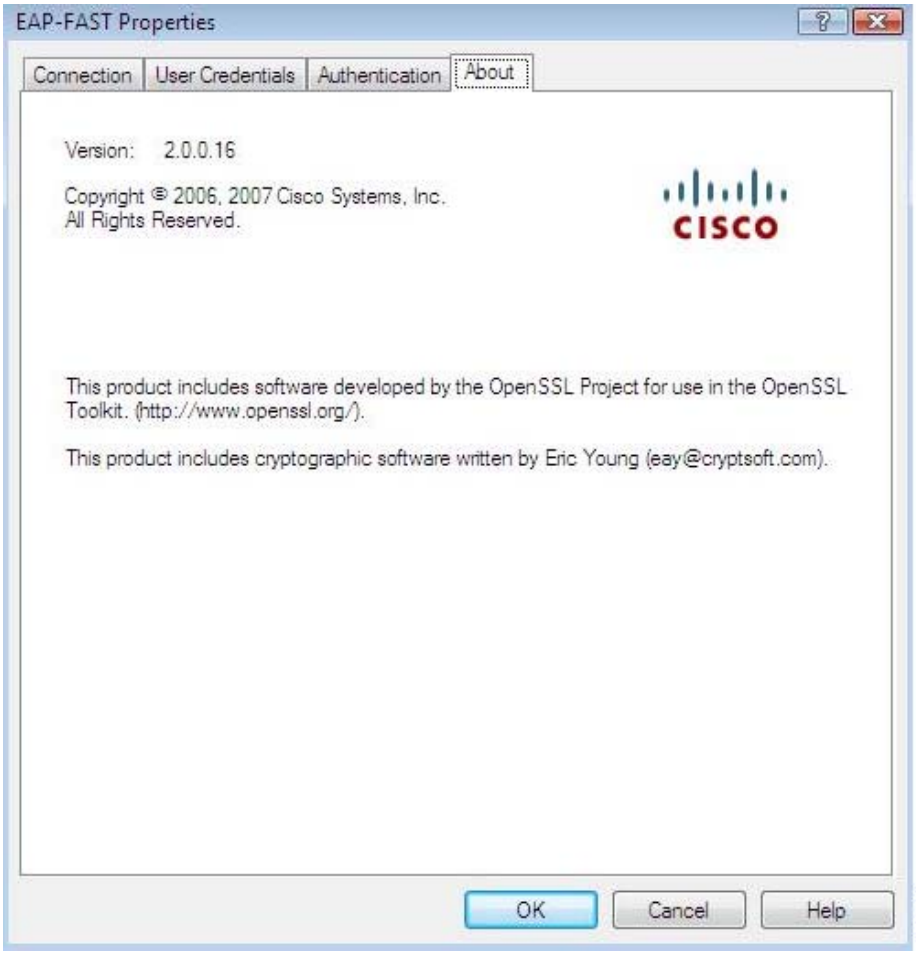
EAP-FAST モジュールのバージョンの確認

デバイスで EAP-FAST モジュールの現在のバージョンを確認するには、次の手順を実行します。

手順 1　EAP-FAST Properties ウィンドウにアクセスします。このウィンドウにアクセスする手順の詳細は、「EAP-FAST のプロパティの設定」（3-2 ページ）で説明されています。

手順 2　**About** タブをクリックします（図 3-7 を参照）。このタブで、バージョン番号、著作権情報、オープン ソース ソフトウェア情報を確認できます。

図 3-7　EAP-FAST Properties ウィンドウの About タブ



CHAPTER 4

ユーザに配布する EAP-FAST プロファイルの作成と変更

この章では、グループ ポリシー オブジェクト エディタを使用し、EAP-FAST XML スキーマを変更して、EAP-FAST モジュールのプロファイルを設定する方法について説明します。

この章では、次の項目について説明します。

グループ ポリシー オブジェクトの概要

グループ ポリシーは、Active Directory ディレクトリ サービス環境で、ユーザおよびコンピュータに対して設定を指定し管理することができるインフラストラクチャです。グループ ポリシーの設定は、グループ ポリシー オブジェクト（GPO）に含まれています。GPO はドメインに存在し、サイト、ドメイン、組織ユニット（OU）などの Active Directory コンテナに割り当てることができます。

Microsoft は、Microsoft 管理コンソール（MMC）でグループ ポリシー オブジェクト エディタを使用できるプログラム スナップインを提供しています。

MMC の詳細は、次の URL にある Microsoft 管理コンソールのヘルプを参照してください。

http://www.microsoft.com/technet/WindowsVista/library/ops/06e1cb7b-19c9-4c49-9db8-a941f6f593c3.mspx

グループ ポリシー オブジェクト エディタの追加

グループ ポリシー オブジェクトを設定する前に、グループ ポリシー オブジェクト エディタのスナップインを追加する必要があります。スナップインを追加するには、次の手順を実行します。

手順 1　MMC を開きます。

a. デスクトップの左下にある **Start** ボタンをクリックします。

b. **検索**の**ボックス**に「**mmc**」と入力し、**Enter** キーを押します。

注　既存または保存済みの MMC コンソールを開くには、Windows エクスプローラでスナップイン コンソールまたはスナップイン コンソールへのショートカットを探してダブルクリックします。

使用している別のコンソールから既存の MMC コンソールを開くこともできます。これを行うには、**File** メニューをクリックし、**Open** をクリックします。

手順 2　グループ ポリシー オブジェクト エディタのスナップインを追加します。

a. **File**、**Add/Remove Snap-in...** の順にクリックします。

Add/Remove Snap-in... ダイアログ ボックスが表示されます。

b. **Add or Remove Snap-ins** ダイアログ ボックスで、**Available snap-ins** リストの **Group Policy Object Editor** を選択し、**Add** ボタンをクリックします。

Select Group Policy Object ダイアログ ボックスが表示されます。

c. **Select Group Policy Object** ダイアログ ボックスで、**Browse** をクリックします。

Browse for a Group Policy Object ダイアログ ボックスが表示されます。

d. **Browse for a Group Policy Object** ダイアログ ボックスで、**Domains/O Us** タブを選択します。

e. **Look in** ドロップダウン リストからドメイン コントローラを選択します。

f. **OK** をクリックします。

g. **Select Group Policy Object** ダイアログ ボックスで、**Finish** をクリックします。

h. **Add or Remove Snap-ins** ダイアログ ボックスで **OK** をクリックします。

これで、グループ ポリシー オブジェクト エディタを使用することができます。

Windows Vista でのグループ ポリシー オブジェクトの作成

新しい EAP グループ ポリシー オブジェクトを作成するには、次の手順を実行します。

手順 1　**Default Domain Policy** ペインで、**Windows Settings**、**Security Settings**、**Wireless Network Policies** の順に選択します。

手順 2　**Wireless Network Policies** を右クリックし、**Create a New Policy** を選択します。

手順 3　SSID、暗号化、認証方式など、ワイヤレス ネットワークのプロパティを設定します。

手順 4　EAP 方式を選択します。

手順 5　EAP-FAST のプロパティを開き、EAP-FAST 設定を行います。

注　**Advanced Security** 画面では、マシン認証、SSO など、詳細な設定を行うことができます。マシン認証の詳細は、「マシン認証の設定」（4-14 ページ）を参照してください。SSO の詳細は、「シングル サインオンの設定」（4-15 ページ）を参照してください。

注　**Wired Network Policy** オブジェクトを選択することで、ワイヤード（有線）ネットワークの設定を行うことができます。

手順 6　完了したら、GPO を保存します。「gpupdate /force」を実行して GPO の更新を強制することにより、Vista クライアントを更新できます。新しいプロファイルが Vista マシンに追加されたのが確認できます。

GPO ネットワーク プロファイルの作成後、Vista マシンでそのプロファイルを変更することはできません。

ワイヤレス ネットワーク ポリシーの General タブでは、ポリシーの名前と説明の入力、WLAN 自動構成サービスを有効にするかどうかの指定、ワイヤレス ネットワーク ポリシーのリストと優先順位の設定を行うことができます。プロファイルを XML ファイルとしてエクスポートしたり、ワイヤレス プロファイルとして XML ファイルをインポートしたりすることもできます。

ポリシーの設定、プロファイルのエクスポート、プロファイルのインポートの詳細は、次のドキュメントを参照してください。

- Windows Vista Wireless Networking Evaluation Guide

http://technet2.microsoft.com/WindowsVista/en/library/f0b0d1fd-6dff-46a2-8e6a-bdd152d2337f1033.mspx?mfr=true

- Wireless Group Policy Settings for Windows Vista（Windows Vista 用ワイヤレス グループ ポリシーの設定）

http://www.microsoft.com/technet/technetmag/issues/2007/04/CableGuy/default.aspx

EAP-FAST XML スキーマ

EAP-FAST モジュールは、次のスキーマを使用することで、ネットワーク プロファイルのネイティブ EAP 方式セクションのすべての設定を XML として保存します。

```
<?xml version="1.0"?>

<!--
*******************************************************************************
                    Cisco EAP-FAST スキーマ          (1.0.40)
Copyright 2006-2007, Cisco Systems, Inc.            All rights reserved.
*******************************************************************************
-->

<xs:schema
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns="http://www.cisco.com/CCX"
 targetNamespace="http://www.cisco.com/CCX"
 elementFormDefault="qualified"
 attributeFormDefault="unqualified">

 <xs:element name="eapFast" type="EapFast"/>

 <xs:complexType name="EapFast">
  <xs:complexContent>
   <xs:extension base="TunnelMethods">
    <xs:sequence>
     <xs:choice>
      <xs:element name="usePac">
       <xs:complexType>
        <xs:sequence>
         <xs:element name="allowUnauthPacProvisioning" type="xs:boolean" default="true">
          <xs:annotation>
         <xs:documentation>認証されていないサーバからの PAC を受け入れます。</xs:documentation>
          </xs:annotation>
         </xs:element>
         <xs:element name="autoGrouping" type="xs:boolean" default="true">
          <xs:annotation>
           <xs:documentation>
```

aid グループは、すべて等しく信頼されている A-ID のセットです。グループ内の A-ID はどれでも使用できます。自動グループ化とは、信頼されていない A-ID がエンドユーザによって受け入れられた場合に、その A-ID が、そのプロファイルですでに信頼されている A-ID と一緒にグループ化されるこ

と、つまり、ユーザのアクションに基づいて、A-ID グループを自動的に作成および拡張することを意味します。A-ID グループの利点は、プロファイルで最初に信頼されている A-ID(1) があり、その後、そのプロファイルの使用時にエンドユーザが新しい A-ID(2) の使用を許可した場合に、再度エンドユーザに尋ねることなく、A-ID(2) が自動的に受け入れられることです。</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="userValidatesServerIdFromUnauthProv" type="xs:boolean" default="true">

<xs:annotation>

<xs:documentation>

true の場合、クライアントが認証されていないプロビジョニングを実行する前に、ユーザに、認証されていないプロビジョニングを許可するかどうかを尋ねるメッセージが表示されます。
</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="unauthProvAllowedTilPacReceived" type="xs:boolean" default="false">

<xs:annotation>

<xs:documentation>true の場合、認証されていないプロビジョニングが成功し、PAC が取得されるまで、認証されていないプロビジョニングの実行が許可され、その後、認証されているプロビジョニングのみが許可されるようになります。</xs:documentation>

</xs:annotation>

</xs:element>

<xs:choice>

<xs:element name="validateWithSpecificPacs" type="ValidateWithSpecificPacs">

<xs:annotation>

<xs:documentation>これは、この要素で参照されている PAC（およびこのプロファイルの使用時にこのプロファイルに自動的にプロビジョニングされた PAC）のみを検証で使用することを示します。</xs:documentation>

</xs:annotation>

</xs:element>

</xs:choice>

</xs:sequence>

</xs:complexType>

</xs:element>

<xs:element name="doNotUsePac" type="Empty">

<xs:annotation>

<xs:documentation>認証で PAC を使用しません。</xs:documentation>

</xs:annotation>

</xs:element>

</xs:choice>

<xs:element name="enablePosture" type="xs:boolean" default="false">

<xs:annotation>

<xs:documentation>ポスチャ情報の処理を許可します。</xs:documentation>

</xs:annotation>

```
</xs:element>
<xs:element name="authMethods">
 <xs:complexType>
  <xs:choice>
   <xs:element name="builtinMethods">
    <xs:complexType>
     <xs:choice>
      <xs:element name="authenticateWithPassword">
       <xs:complexType>
        <xs:sequence>
        <xs:element name="protectedIdentityPattern" type="IdentityPattern" minOccurs="0">
          <xs:annotation>
            <xs:documentation>形式の規則は unprotectedIdentityPattern と同じです。通常のパターンは [username]@[domain] です。パスワードのソースがこのプロファイルの場合は、ユーザ名として送信する実際の文字列になります。</xs:documentation>
          </xs:annotation>
        </xs:element>
        <xs:element name="passwordSource" type="PasswordSource"/>
        <xs:element name="methods">
         <xs:annotation>
          <xs:documentation>少なくとも 1 つの子要素が必要です。</xs:documentation>
         </xs:annotation>
         <xs:complexType>
          <xs:all>
           <xs:element name="eapMschapv2" type="Empty" minOccurs="0"/>
           <xs:element name="eapGtc" type="Empty" minOccurs="0"/>
          </xs:all>
         </xs:complexType>
        </xs:element>
       </xs:sequence>
      </xs:complexType>
     </xs:element>
     <xs:element name="authenticateWithToken">
      <xs:complexType>
       <xs:sequence>
       <xs:element name="protectedIdentityPattern" type="IdentityPattern" minOccurs="0">
         <xs:annotation>
           <xs:documentation>形式の規則は unprotectedIdentityPattern と同じです。通常のパターンは [username]@[domain] です。</xs:documentation>
         </xs:annotation>
       </xs:element>
       <xs:element name="tokenSource" type="TokenSource"/>
```

```
            <xs:element name="methods">
             <xs:complexType>
              <xs:all>
               <xs:element name="eapGtc" type="Empty"/>
              </xs:all>
             </xs:complexType>
            </xs:element>
           </xs:sequence>
          </xs:complexType>
         </xs:element>
         <xs:element name="authenticateWithCertificate">
          <xs:complexType>
           <xs:sequence>
           <xs:element name="protectedIdentityPattern" type="IdentityPattern" minOccurs="0">
             <xs:annotation>
              <xs:documentation>形式の規則は unprotectedIdentityPattern と同じです。通常のパターンは [username]@[domain] です。</xs:documentation>
             </xs:annotation>
            </xs:element>
            <xs:element name="certificateSource" type="CertificateSource"/>
            <xs:choice>
             <xs:element name="doNotUseInnerMethod">
              <xs:complexType>
               <xs:choice>
                <xs:element name="sendWheneverRequested" type="Empty"/>
                <xs:element name="sendSecurelyOnly" type="Empty"/>
               </xs:choice>
              </xs:complexType>
             </xs:element>
             <xs:element name="sendViaInnerMethod">
              <xs:complexType>
               <xs:all>
                <xs:element name="eapTls" type="Empty"/>
               </xs:all>
              </xs:complexType>
             </xs:element>
            </xs:choice>
           </xs:sequence>
          </xs:complexType>
         </xs:element>
        </xs:choice>
```

```
            </xs:complexType>
           </xs:element>
            <xs:element name="extendedInnerMethods" type="ExtendedInnerEapMethod"
maxOccurs="unbounded"/>
          </xs:choice>
         </xs:complexType>
        </xs:element>
       </xs:sequence>
     </xs:extension>
   </xs:complexContent>
 </xs:complexType>

 <xs:complexType name="IdentityPattern">
   <xs:simpleContent>
     <xs:extension base="NonEmptyString">
       <xs:attribute name="encryptContent" type="xs:boolean" use="optional" default="true">
         <xs:annotation>
           <xs:documentation>デフォルトは 'true' です。これは、この要素を暗号化する必要があること
を後処理ツールに示しています。</xs:documentation>
         </xs:annotation>
       </xs:attribute>
     </xs:extension>
   </xs:simpleContent>
 </xs:complexType>

 <xs:complexType name="PasswordFromProfile">
   <xs:simpleContent>
     <xs:extension base="xs:string">
       <xs:attribute name="encryptContent" type="xs:boolean" use="optional" default="true">
         <xs:annotation>
           <xs:documentation>デフォルトは 'true' です。これは、この要素を暗号化する必要があること
を後処理ツールに示しています。</xs:documentation>
         </xs:annotation>
       </xs:attribute>
     </xs:extension>
   </xs:simpleContent>
 </xs:complexType>

 <xs:complexType name="PasswordSource">
   <xs:choice>
     <xs:element name="passwordFromLogon" type="Empty"/>
     <xs:element name="passwordFromUser" type="Empty"/>
```

```
    <xs:element name="passwordFromProfile" type="PasswordFromProfile"/>
   </xs:choice>
  </xs:complexType>

  <xs:complexType name="TokenSource">
   <xs:choice>
    <xs:element name="passwordFromOtherToken" type="Empty">
     <xs:annotation>
      <xs:documentation> これにより、トークンから ID と OTP を取得するためのプロンプトがユーザに表示されます。</xs:documentation>
     </xs:annotation>
    </xs:element>
   </xs:choice>
  </xs:complexType>

  <xs:complexType name="CertificateSource">
   <xs:choice>
    <xs:element name="certificateFromUser" type="Empty">
     <xs:annotation>
      <xs:documentation>
認証時に使用するクライアント証明書は、表示されたリストからエンドユーザが選択したものです。
</xs:documentation>
     </xs:annotation>
    </xs:element>
    <xs:element name="certificateFromLogon" type="Empty">
     <xs:annotation>
      <xs:documentation> 認証時に使用するクライアント証明書は、Windows へのログオンでエンドユーザが使用したものです。</xs:documentation>
     </xs:annotation>
    </xs:element>
    <xs:element name="certificateFromProfile" type="ClientCertificate">
     <xs:annotation>
      <xs:documentation> 認証時に使用するクライアントのユーザ証明書が、ここに示されます。
</xs:documentation>
     </xs:annotation>
    </xs:element>
   </xs:choice>
  </xs:complexType>

  <xs:complexType name="ExtendedInnerEapMethod">
   <xs:sequence>
    <xs:element name="methodName" type="xs:string"/>
```

```
    <xs:element name="methodEapId" type="xs:unsignedInt"/>
    <xs:element name="vendorId" type="xs:integer" default="0"/>
    <xs:element name="AuthorName" type="xs:string"/>
    <xs:element name="AuthorId" type="xs:unsignedInt"/>
    <xs:any namespace="##any" processContents="lax" minOccurs="0"/>
  </xs:sequence>
 </xs:complexType>

 <xs:complexType name="TunnelMethods">
  <xs:sequence>
   <xs:choice>
    <xs:element name="validateServerCertificate" type="serverCertificateValidationParameters"/>
    <xs:element name="doNotValidateServerCertificate" type="Empty"/>
   </xs:choice>
   <xs:element name="unprotectedIdentityPattern" type="IdentityPattern" minOccurs="0">
    <xs:annotation>
     <xs:documentation>[username] および [domain]、またはそのどちらかのプレースホルダが使用
される場合：認証でクライアント証明書が使用される場合、プレースホルダの値はクライアント証明
書の CN フィールドから取得されます。クレデンシャルがエンドユーザから取得される場合、プレー
スホルダの値はユーザが入力した情報から取得されます。クレデンシャルがオペレーティング システ
ムから取得される場合、プレースホルダの値はログオン情報から取得されます。通常のパターン：
anonymous@[domain]（トンネルされた方式の場合）または [username]@[domain]（トンネルされて
いない方式の場合）。クレデンシャルのソースがこのプロファイルの場合は、ユーザ名として送信する
実際の文字列になります（プレースホルダなし）。</xs:documentation>
    </xs:annotation>
   </xs:element>
   <xs:choice>
    <xs:element name="enableFastReconnect">
     <xs:complexType>
      <xs:complexContent>
       <xs:extension base="Empty">
        <xs:choice>
         <xs:element name="alwaysAttempt" type="Empty"/>
        </xs:choice>
       </xs:extension>
      </xs:complexContent>
     </xs:complexType>
    </xs:element>
    <xs:element name="disableFastReconnect" type="Empty"/>
   </xs:choice>
  </xs:sequence>
 </xs:complexType>
```

```
 <xs:complexType name="ClientCertificate">
  <xs:choice>
   <xs:element name="certificateId" type="CertificateIdentifier">
    <xs:annotation>
     <xs:documentation> これは、OS にあらかじめ保存されている証明書への参照です。
</xs:documentation>
    </xs:annotation>
   </xs:element>
  </xs:choice>
 </xs:complexType>

 <xs:complexType name="CertificateContainer">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
   <xs:element name="certificateId" type="CertificateIdentifier">
    <xs:annotation>
     <xs:documentation> これは、OS にあらかじめ保存されている証明書への参照です。
</xs:documentation>
    </xs:annotation>
   </xs:element>
  </xs:choice>
 </xs:complexType>

 <xs:complexType name="CertificateIdentifier">
  <xs:simpleContent>
   <xs:annotation>
    <xs:documentation>X509 形式のバイナリ証明書全体にわたる SHA 1 のハッシュ値。マシンの信
頼済み CA のグローバル リストで証明書を一意に識別します（Windows の OS で管理されるストア）。
</xs:documentation>
   </xs:annotation>
   <xs:extension base="NonEmptyString">
    <xs:attribute name="reference" type="xs:boolean">
     <xs:annotation>
      <xs:documentation>true は、要素値が PEM 形式の証明書へのファイル参照であることを示しま
す。後処理ツールが、その証明書ファイルを取得し、ハッシュ値に変換し、certificateId 要素に値を投
入し、これがその証明書にわたる SHA1 のハッシュ値であることを示すために、参照を false に設定し
ます。</xs:documentation>
     </xs:annotation>
    </xs:attribute>
   </xs:extension>
  </xs:simpleContent>
 </xs:complexType>

 <xs:complexType name="Empty"/>
```

```
<xs:simpleType name="NonEmptyString">
  <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="ServerRuleFormat">
  <xs:simpleContent>
    <xs:extension base="NonEmptyString">
      <xs:attribute name="match" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="exactly"/>
            <xs:enumeration value="endsWith"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="ServerValidationRules">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:annotation>
      <xs:documentation>
ユーザがサーバを信頼できる場合のみのオプションです。サーバ検証ルールを持たないプロファイルの開始が許可されると、ユーザが信頼されていないサーバを検証するときに、検証プロセスによってそのサーバ名が検証されます。</xs:documentation>
    </xs:annotation>
    <xs:element name="matchSubjectAlternativeName" type="ServerRuleFormat">
      <xs:annotation>
        <xs:documentation>DNSName：通常は、完全修飾ドメイン名（FQDN）の形式になります。
</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="matchSubject" type="ServerRuleFormat">
      <xs:annotation>
        <xs:documentation>サブジェクト：CN（共通名）- 通常は、単純な ASCII 文字列です。または、サブジェクト：DN（ドメイン名）- 一連の DC ( ドメイン コンポーネント）属性で構成されます。
</xs:documentation>
      </xs:annotation>
```

```
    </xs:element>
   </xs:choice>
  </xs:complexType>

  <xs:complexType name="serverCertificateValidationParameters">
   <xs:sequence>
    <xs:choice>
     <xs:element name="serverNameValidationRules" type="ServerValidationRules"/>
     <xs:element name="anyServerName" type="Empty">
      <xs:annotation>
       <xs:documentation>証明書内のサーバ名はテストされません。</xs:documentation>
      </xs:annotation>
     </xs:element>
    </xs:choice>
    <xs:choice>
     <xs:element name="validateChainWithSpecificCa">
      <xs:complexType>
       <xs:complexContent>
        <xs:extension base="CertificateContainer"/>
       </xs:complexContent>
      </xs:complexType>
     </xs:element>
     <xs:element name="validateChainWithAnyCaFromOs" type="Empty">
      <xs:annotation>
       <xs:documentation>グローバル CA 証明書ストアの CA 証明書で終わっている場合、その証明
書チェーンは信頼されます。</xs:documentation>
      </xs:annotation>
     </xs:element>
    </xs:choice>
    <xs:element name="userValidatesUntrustedServerCertificate" type="xs:boolean">
     <xs:annotation>
      <xs:documentation>サーバ証明書の検証に失敗した場合、true に設定されていると、エンドユー
ザはサーバを検証するように求められます。検証すると、適切な trustedCaCerts およびサーバ名
フィールドが記憶され、次回から自動的に信頼されるようになります。</xs:documentation>
     </xs:annotation>
    </xs:element>
   </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ValidateWithSpecificPacs">
   <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:annotation>
```

<xs:documentation> これはオプションです。これにより、エンジンでサーバ PAC を検証する必要があるが、PAC が、プロファイル内のこの場所で静的に定義されるのではなく、エンドユーザのアクションまたは認証されていないプロビジョニングによって動的に追加されるということをプロファイルで示すことができます。</xs:documentation>

```
    </xs:annotation>
    <xs:element name="trustPacFromGlobalPacStoreWithThisId" type="xs:string">
     <xs:annotation>
      <xs:documentation>
PAC 用のグローバル ストア（プロファイルごとのストアではない）が存在する場合に使用されます。
</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:choice>
 </xs:complexType>

</xs:schema>
```

マシン認証の設定

グループ ポリシー オブジェクトを作成するときに、Advanced Security 画面でマシン認証を有効にすることができます。

EAPHost は、EAP-FAST モジュールに、現在の認証がマシン認証であることを通知します。

マシン認証は、次のいずれかによって実行できます。

- マシン PAC
- マシン証明書
- マシン パスワード

EAP-FAST モジュールは、最初に、マシン PAC を取得しようとします。マシン PAC を取得できない場合、EAP-FAST モジュールはマシン証明書を取得しようとします。マシン証明書を取得できない場合、EAP-FAST モジュールは Active Directory 内のマシン アカウントのマシン パスワードを取得しようとします。

マシンがマシン証明書またはマシン パスワードで認証されると、EAP-FAST モジュールは、以降の使用のために、マシン PAC のプロビジョニングを要求します。マシン証明書もマシン パスワードも取得できない場合、EAP-FAST モジュールは、ユーザがログインした後、次回のユーザ認証成功時に、マシン PAC を要求します。既存のマシン PAC が無効か、期限切れの場合、EAP-FAST モジュールはこのプロセスを使用して新しいマシン PAC を要求します。

マシン認証は Windows 802.1X サプリカントで統合およびサポートされているため、EAP-FAST モジュールが担当するのは、ネットワークへのアクセス権を取得するための認証のみとなります。マシン認証をサポートするためのその他のネットワーク管理（DHCP、マシンレベルの GPO、その他の関連するネットワーク サービスなど）は、オペレーティング システムと 802.1X サプリカントの担当になります。

シングル サインオンの設定

SSO は、以下のように、Microsoft Windows Vista でサポートされます。

- Windows ユーザ クレデンシャルは、EAPHost インターフェイスを通じて EAP-FAST モジュールに渡されます。EAP-FAST モジュールが、ネットワーク認証で Windows ユーザ クレデンシャルを使用するように設定されており、かつ、ネットワーク プロファイルが、シングル サインオンを実行するように設定されている場合、システムはユーザに追加のクレデンシャルを求めません。
- Windows 以外のネットワーク クレデンシャルは、Microsoft Windows Vista のログオン プロセスで収集されます。EAP-FAST モジュールは、ユーザにこれらのネットワーク クレデンシャルを求めるよう、ログオン モジュールに要求します。
- 必要に応じて、EAP-FAST モジュールは、ユーザが Microsoft Windows Vista にログインする前に、ユーザに追加のネットワーク クレデンシャルを求めることができます。
- ネットワーク クレデンシャルが設定に保存されている場合、EAP-FAST モジュールは、ユーザが Microsoft Windows Vista にログインする前に、これらのクレデンシャルにアクセスすることができます。

CHAPTER 5

ロギングの設定

この章では、トラブルシューティングに役立つ、EAP-FAST モジュールのロギングの設定方法について説明します。

この章では、次の項目について説明します。

ロギングの概要

トラブルシューティングに役立つログを生成するために、EAP-FAST モジュールは Windows イベント ログ サービスを使用します。ログには、イベントのタイプ、イベントの発生場所、イベントの影響を受けた機能、イベントの発生日時などの情報が記録されます。

ロギングの設定と開始

管理者のコマンド プロンプトにアクセスし、ロギングを設定および開始するには、次の手順を実行します。

手順 1　**Start**、**All Programs**、**Accessories** の順にクリックします。

手順 2　**Command Prompt** を右クリックし、**Run as administrator** を選択します。

手順 3　プロンプトで、次のコマンドを入力し、ロギングを設定および開始します。

wevtutil sl Cisco-EAP-FAST/Debug /e:true /k:*category_mask* **/l:***log_level*

構文の説明

category_mask	有効にするロギングのカテゴリのビットマスク。有効な値は次のとおりです。 • **0** — すべてのカテゴリをロギングします。 • **1** — 次の 2 つのカテゴリに該当しないすべてのメッセージをロギングします。 • **2** — 詳細ログ レベルでのみ、戻りコードとともに、機能のエントリ ポイントおよびエグジット ポイントのフローをロギングします。 • **4** — 詳細ログ レベルでのみ、パケット ダンプをロギングします。 デフォルト値は 0 です。
log_level	有効にするロギングのレベル。有効な値は次のとおりです。 • **0** — すべてのログ レベル • **1** — 重大 • **2** — エラー • **3** — 警告 • **4** — 情報 • **5** — 詳細 デフォルト値は 0 です。

注　ロギングが終了する前に、ロギングを実行しているデバイスをシャットダウンする必要がある場合、ロギングはリブート後に再開されます。ただし、ロギングが自動または手動で開始されると、ログはクリアされます。

ロギングの無効化と内部バッファのフラッシュ

必要な情報を収集した後、次のコマンドを使用すると、ロギングを停止し、すべての内部バッファをフラッシュすることができます。

wevtutil sl Cisco-EAP-FAST/Debug /e:false

注　.etl ファイルを分析するには、このコマンドを入力する必要があります。

ログ ファイルの場所

デフォルトでは、分析とデバッグに使用できる .etl ファイルは次の場所に作成されます。

C:¥Windows¥System32¥Winevt¥Logs¥Cisco-EAP-FAST%4Debug.etl

この場所を変更する場合は、管理者のコマンド プロンプトで次のコマンドを入力します。

wevtutil sl Cisco-EAP-FAST/Debug /lfn:"*path_to_etl_log_file***"**

注　ログ ファイルへのパスを変更するコマンドは、ロギングの実行中に入力しないでください。

また、ロギングを開始するときに、.etl ファイルへのパスを変更することもできます。.etl ファイルの場所を指定してロギングを開始するには、管理者のコマンド プロンプトで次のコマンドを入力します。

wevtutil sl Cisco-EAP-FAST/Debug /e:true /lfn:"*path_to_etl_log_file***"**

CHAPTER 6

トラブルシューティング

この章では、EAP-FAST のエラー メッセージについて説明します。また、強固なパスワードを作成するためのガイドラインも示します。

この章では、次の項目について説明します。

EAP-FAST のエラー メッセージ

エラー メッセージ　Automatic PAC provisioning is enabled for this profile. However, a valid PAC that matches the server to which the client adapter is connecting could not be found. Do you wish to obtain a new security credential (PAC)?

推奨処置　既存のクレデンシャルを使用して、このサーバの新しい PAC をプロビジョニングするには、**Yes** をクリックし、操作をキャンセルするには、**No** をクリックします。**No** をクリックすると、クライアント アダプタにより、認証が失敗します。

注意　不正なアクセス ポイントからの攻撃を防ぐには、必要でない限り PAC を再プロビジョニングしないでください。

エラー メッセージ　While attempting to provision your PAC during auto-provisioning, the network access device failed to authenticate itself. This condition might indicate an attack on your password by a rogue access device. Try again with your current password?

推奨処置　現在のパスワードで再認証を試行するには、**Yes** をクリックします。操作をキャンセルするには、**No** をクリックします。

注　認証の試行に再度失敗した場合は、システム管理者に連絡し、不正なアクセス デバイスであることを報告してください。パスワードが不正に使用されるリスクを軽減するには、今後は、強固なパスワードを使用するようにしてください。強固なパスワードを作成するためのヒントについては、「強固なパスワードの作成」（6-5 ページ）を参照してください。

エラー メッセージ　While attempting to provision your PAC, the network access device timed out. A timeout might indicate an attack on your password by a rogue access device. However, a timeout could be caused by a server outage or a faulty connection. Try again with your current password?

推奨処置　現在のパスワードで再認証を試行するには、**Yes** をクリックします。操作をキャンセルするには、**No** をクリックします。

注　再度タイムアウトが発生した場合は、システム管理者に連絡し、不正なアクセス デバイスである可能性があることを報告してください。パスワードが不正に使用されるリスクを軽減するには、今後は、強固なパスワードを使用するようにしてください。強固なパスワードを作成するためのヒントについては、「強固なパスワードの作成」（6-5 ページ）を参照してください。

エラー メッセージ　A valid PAC was not found for your username <username>. Click **OK**. Re-enter your username in the credential prompt or the User Credentials tab of the EAP-FAST Properties screen. If you entered your username correctly, go to the Connection tab of the EAP-FAST Properties screen either to enable automatic PAC provisioning or Validate server certificate or import a PAC file.

推奨処置　**OK** をクリックします。次のいずれかを実行します。

- ユーザ名をもう一度入力します。
- ユーザ名を正しく入力したら、EAP-FAST Properties 画面の Connection タブに移動し、PAC の自動プロビジョニングを有効にするか、PAC ファイルをインポートします。

エラー メッセージ　The EAP-FAST authentication attempt failed because you entered the wrong username and password. Please re-enter your username and password.

推奨処置　**OK** をクリックします。Enter Wireless Network Password 画面が表示されたら、EAP-FAST クレデンシャルをもう一度入力します。

エラー メッセージ　The EAP-FAST authentication attempt failed because you might have entered the wrong username and password. Please re-enter your username and password.

Warning: If you are sure that you have typed in the right username and password, you may have connected to a rogue device.This can indicate an attack on your password.Using a strong password will reduce the chance of your password being compromised.If this failure happens again, contact your system administrator to report a potential rogue access device.

推奨処置　**OK** をクリックします。次のいずれかを実行します。

- EAP-FAST クレデンシャルを正しく入力した場合は、システム管理者に連絡し、不正なアクセス ポイントである可能性があることを報告してください。パスワードが不正に使用されるリスクを軽減するには、今後は、強固なパスワードを使用するようにしてください。強固なパスワードを作成するためのヒントについては、「強固なパスワードの作成」（6-5 ページ）を参照してください。
- EAP-FAST クレデンシャルを正しく入力しなかった場合は、Enter Wireless Network Password 画面でクレデンシャルをもう一度入力します。
- ユーザ名がプロビジョニングされた PAC と一致せず、このプロファイルで自動プロビジョニングが有効になっている場合に、メッセージ「You do not appear to be registered with the authentication server.Registration requires that this device be initialized with a security credential.Do you wish to obtain a security credential?」が表示されたら **Yes** をクリックします。

– ユーザ名がプロビジョニングされた PAC と一致せず、このプロファイルで手動プロビジョニングが有効になっている場合は、EAP-FAST Properties ダイアログ ボックスの Connection タブに移動し、PAC の自動プロビジョニングを有効にするか、PAC ファイルをインポートします。

エラー メッセージ　PAC provisioning has failed. This failure is not related to an issue with the username and password. This failure is commonly caused by a server configuration issue. Contact your administrator for assistance.

推奨処置　サポートが必要な場合は、システム管理者にお問い合わせください。

エラー メッセージ　The PAC that you selected for this profile does not match the server to which the client is connecting. However, a matching PAC has been found in your PAC database. Would you like to use this matching credential authority and save it to the profile?

推奨処置　一致する PAC を使用し、この新しい PAC でプロファイルを更新するには、**Yes** をクリックします。操作をキャンセルし、プロファイルを現在の状態のままにするには、**No** をクリックします。**No** をクリックすると、クライアント アダプタでは、既存のプロファイルを使用して認証を行うことができません。

エラー メッセージ　You entered different values in the New Password field and the Confirm New Password field. The passwords must be identical. Please try again.

推奨処置　両方のフィールドに新しいパスワードをもう一度入力します。

エラー メッセージ　The password that you entered in the Old Password field does not match the password that you previously used. Please try again.

推奨処置　Old Password フィールドに古いパスワードをもう一度入力します。

エラー メッセージ　An error occurred when you attempted to change your EAP-FAST password. The new password might not conform to the server's password policy. Please try again.

推奨処置　Change Password 画面でパスワードをもう一度入力します。

エラー メッセージ　The EAP-FAST authentication process failed during initialization. Make sure that EAP-FAST and the Trusted Root Certificate Authority certificate are installed correctly.

推奨処置　EAP-FAST および信頼済みルート CA 証明書が正しくインストールされていることを確認します。

エラー メッセージ　You have connected to a server with the following server name

<server_name>

The server certificate is signed by the following Root Certification Authority (CA):

<root_ca>

This Root CA does not match the specified trusted Root CA(s).

Do you want to accept this connection?

Warning: Connecting to a server signed with untrusted CA might compromise your security.

推奨処置　セキュリティ上のリスクがあるものの、クライアント アダプタをこのサーバに接続する場合は、**Yes** をクリックします。それ以外の場合は、**No** をクリックします。

エラー メッセージ　You have connected to a server with the following server name:

<server_name>

This server name does not match the specified server name(s).

Do you want to accept this connection?

Warning: Connecting to an unsecured server might compromise your security.

推奨処置　セキュリティ上のリスクがあるものの、クライアント アダプタをこのサーバに接続する場合は、**Yes** をクリックします。それ以外の場合は、**No** をクリックします。

エラー メッセージ　Your password has expired. Please enter a new password.

推奨処置　新しいパスワードを入力し、期限切れのパスワードを変更します。

エラー メッセージ　You entered an empty username, which is not allowed.

推奨処置　ユーザ名を入力します。

エラー メッセージ　You must select a PAC when using manual PAC provisioning.

推奨処置　EAP-FAST Properties 画面で、自動プロビジョニングが無効になっており、PAC 認証機関を選択していないときに、**OK** をクリックしました。自動プロビジョニングを有効にするか、ドロップダウン リストから PAC 認証機関を選択してください。リストが空白の場合は、PAC ファイルをインポートします。

エラー メッセージ　Error opening or reading file: <filename>.

推奨処置　PAC ファイルのインポートを再度試みます。同じメッセージが表示されたら、システム管理者から新しい PAC ファイルを取得して、もう一度インポートします。

エラー メッセージ　The file is not a valid PAC file: <filename>.

推奨処置　PAC ファイルのインポートを再度試みます。同じメッセージが表示されたら、システム管理者から新しい PAC ファイルを取得して、もう一度インポートします。

エラー メッセージ　The file does not contain a valid PAC: <filename>.

推奨処置　PAC ファイルのインポートを再度試みます。同じメッセージが表示されたら、システム管理者から新しい PAC ファイルを取得して、EAP-FAST Settings 画面でインポートします。

エラー メッセージ　The file contains a PAC that will replace an existing PAC already provisioned on your system. Would you like to replace the existing PAC?

推奨処置　既存の PAC を、インポートしたファイルの新しい PAC で置き換えるには、**Yes** をクリックし、操作をキャンセルするには、**No** をクリックします。

エラー メッセージ　The password you entered to import the PAC file is incorrect. Please try again.

推奨処置　パスワードをもう一度入力してみます。

エラー メッセージ　The PAC file import operation has been aborted because of three or more attempts of incorrect passwords.

推奨処置　**OK** をクリックして続行します。

エラー メッセージ　An internal error occurred.

推奨処置　PAC のインポート中に内部エラーが発生しました。PAC をもう一度インポートしてみてください。

エラー メッセージ　Insufficient memory or other system error.

推奨処置　他のプログラムを閉じ、メモリを解放します。

エラー メッセージ　You must select “Validate server certificate” or a PAC to use user's certificate or one-time password for authentication.

推奨処置　ユーザ クレデンシャルとして、1 回限りのパスワードまたはユーザ証明書が選択されましたが、PAC が選択されていないか、Validate Server Certificate チェックボックスがオンになっていません。設定を変更してください。

エラー メッセージ　You tried to import a PAC file with the same PAC ID as a previously imported or provisioned PAC. Would you like to replace the existing PAC?

推奨処置　既存の PAC を、インポートしたファイルの新しい PAC で置き換えるには、**Yes** をクリックし、操作をキャンセルするには、**No** をクリックします。

強固なパスワードの作成

パスワードは、紙に書き留めたり、オンライン上に保存したりしないでください。代わりに、簡単に覚えることができ、かつ他人が簡単に推測できないパスワードを作成するようにします。このようなパスワードを作成する方法として、曲のタイトル、主張、その他のフレーズをベースとして使用することができます。たとえば、「This May Be One Way To Remember」というフレーズであれば、「TmB1w2R!」や「Tmb1W>r~」などのパスワードを作成できます。

注　例に示したパスワードを実際のパスワードとして使用しないでください。

強固なパスワードの特性

強固なパスワードには、次のような特性があります。

- 大文字と小文字の両方が含まれている（a ～ z と A ～ Z の両方)
- アルファベットだけでなく、数字や記号も含まれている（0 ～ 9、!@#$%^&*()_+|~ =\`{}[]:";'<>?,./ など）
- 5 文字以上の英数字である
- どの言語の単語でもない
- スラング、方言、または専門用語ではない
- 家族の名前などの個人情報に基づいていない

脆弱なパスワードの特性

脆弱なパスワードには、次のような特性があります。

- 8 文字未満である
- 辞書に載っている単語である（英語またはその他の言語）
- その他の、簡単に推測できる言葉、または一般的に使用されている言葉である。簡単に推測できる言葉の例としては、次のようなものがあります。
  - 家族、ペット、友人、同僚、または物語の登場人物の名前
  - コンピュータ関連の用語または名称（コマンド、サイト、会社、モデル、アプリケーションなど）
  - 誕生日やその他の個人情報（住所、電話番号など）
  - 予測できる英数字の組み合わせ（aaabbb、qwerty、zyxwvuts、123321 など）
  - 上記のいずれかを後ろから読んだもの
  - 上記のいずれかの前後に数字を加えたもの

パスワードのセキュリティに関する基本事項

パスワードを扱う際には、次の基本ガイドラインに従ってください。

- 家族にも、パスワードは教えない。
- 他人の前でパスワードのことを話さない。
- パスワードを知るヒントになるようなこと（「家族の名前」など）は言わない。
- 標準の ASCII 文字セット以外の文字は使用しない。ポンド（£）など、一部の記号は、システムによって、ログイン時に問題が発生する原因となる場合があります。

APPENDIX A

略語

表 A-1 は、このガイドで使用されている略語とその完全表記を示しています。

表 A-1　　略語の一覧

略語	完全表記
AAA	Authentication, Authorization, and Accounting（認証、許可、アカウンティング）
API	Application Program Interface（アプリケーション プログラミング インターフェイス）
ASCII	American Standard Code for Information Interchange（米国規格協会情報交換標準コード）
CA	Certificate Authority（認証局）
CCX	Cisco Compatible eXtensions
DHCP	Dynamic Host Configuration Protocol（ダイナミック ホスト コンフィギュレーション プロトコル）
EAP	Extensible Authentication Protocol（拡張認証プロトコル）
EAP-FAST	Extensible Authentication Protocol—Flexible Authentication via Secure Tunneling（拡張認証プロトコル - セキュア トンネリングを介したフレキシブル認証）
EAP-GTC	Extensible Authentication Protocol—Generic Token Card（拡張認証プロトコル - 汎用トークン カード）
EAP-MSCHAPv2	Extensible Authentication Protocol—Microsoft Challenge Handshake Authentication Protocol Version 2（拡張認証プロトコル - 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）
EAP-TLS	Extensible Authentication Protocol—Transport Layer Security（拡張認証プロトコル - トランスポート レイヤ セキュリティ）
ETW	Event Tracing for Windows（Vista の Windows イベント トレーシング）
GPO	Group Policy Object（グループ ポリシー オブジェクト）
LDAP	Lightweight Directory Access Protocol
MITM	Man-In-The-Middle（中間者攻撃）
MMC	Microsoft Management Console（Microsoft 管理コンソール）
MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol Version 2（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）
OTP	One-Time Password（1 回限りのパスワード）
OU	Organizational Unit（組織ユニット）
PAC	Protected Access Credential

表 A-1　略語の一覧 （続き）

略語	完全表記
PEAP	Protected Extensible Authentication Protocol（保護された拡張認証プロトコル）
PIN	Personal Identification Number（暗証番号）
PKI	Public-Key Infrastructure（公開キー インフラストラクチャ）
RADIUS	Remote Authentication Dial-In User Service（リモート認証ダイヤルイン ユーザ サービス）
RFC	Request for Comments
SDK	Software Development Kit（ソフトウェア開発キット）
SSID	Service Set Identifier（サービス セット ID）
SSO	Single Sign-On（シングル サインオン）
TKIP	Temporal Key Integrity Protocol（一時キー統合プロトコル）
TLS	Transport Layer Security（トランスレート レイヤ セキュリティ）
UPN	User Principal Name（ユーザ プリンシパル名）
XML	eXtensible Markup Language（拡張マークアップ言語）

APPENDIX B

通知とライセンス

この製品には、OpenSSL ツールキット用に OpenSSL Project（http://www.openssl.org/）で開発されたソフトウェアが含まれています。

この製品には、Eric Young 氏（eay@cryptsoft.com）が作成した暗号化ソフトウェアが含まれています。

この製品には、Tim Hudson 氏（tjh@cryptosoft.com）が作成したソフトウェアが含まれています。

```
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
```

```
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```