CHAPTER 1

概要

この章は、次の内容で構成されています。

システム概要

Cisco Secure ACS Express（ここでは「ACS Express」と表記します）は、集中型の RADIUS および TACACS+ サーバとして動作する使いやすいアクセス コントロール サーバです。集中型のアイデンティティ ネットワーキング ソリューションで認証と認可を併用することによってアクセス セキュリティを強化し、これにより、柔軟性が高まり、ユーザ生産性が向上します。ACS Express は、有線 LAN、無線 LAN、ファイアウォール、VPN など、さまざまなアクセス接続をサポートします。

ACS Express はエントリレベルの RADIUS AAA および TACACS+ サーバで、リテール ブランチやエンタープライズ ブランチなど、中小規模の企業（SMB）を対象としています。ACS Express は、無線、有線、仮想プライベート ネットワークなどのさまざまなネットワークに対するユーザ アクセスやマシン アクセスを制御します。また、ACS Express は RADIUS と TACACS+ を使用してネットワーク デバイスへの管理アクセスの制御も行います。ACS Express は、配置や設定を簡単にする使いやすい管理インターフェイスを備えたアプライアンスとして提供されます。

ACS Express の主要な機能として、企業ネットワークにある保護されたリソースへのアクセスを要求するユーザ アクセスやクライアント マシンを制御することが挙げられます。ACS Express は AAA 対応のネットワーク デバイスと連携動作し、ユーザやデバイスの認証、エンタイトルメントが付与されたユーザやデバイスの認可を行います。

ACS Express は、RADIUS を使用した無線、有線、VPN（ネットワーク アクセス）をはじめとする各種転送方法により、エンタープライズ ネットワークに対するユーザ アクセスやクライアント アクセスを制御します。ネットワーク アクセスの場合、ACS Express と AAA 対応デバイス（ネットワーク アクセス サーバ（NAS）は、RADIUS プロトコルを使用して通信を行います。ACS Express は、Cisco IOS/PIX デバイス、Cisco VPN コンセントレータ、Cisco Airespace コントローラ、Cisco Aironet アクセス ポイント、Juniper デバイス、Microsoft デバイス、および IETF RADIUS 準拠の NAS など、さまざまな NAS をサポートします。ACS Express は、CHAP、PAP、MS-CHAPv2、EAP-TLS、PEAP、EAP-FASTv0、LEAP など、各種認証方法をサポートします。

NAS は、ユーザのクレデンシャルを ACS Express に送信した後、その内容を各種ユーザ データベースに対して確認できます。ACS Express は Active Directory、LDAP、One-Time Password（OTP; ワンタイム パスワード）のユーザ データベースと通信を行うことができます。また、ACS Express は独自のユーザ データベースの提供も行い、ローカル ユーザを管理します。クレデンシャル検証プロセス中、ユーザ データベースはエンタープライズでのユーザのプロファイルを示すデータ（ユーザ グループなど）を返すことがあります。Active Directory を使用する場合、ACS Express はマシン認証要求を処理し、ネットワークにアクセスする前にマシンとユーザの両方が正常に認証されることを強制することもできます。

クレデンシャルが確認されると、ACS Express はユーザに付与されたエンタイトルメントを判断します。ネットワーク アクセスの場合、エンタイトルメントは発信元の NAS に返された RADIUS 認証応答になります。管理者は規則を定義して、返されるエンタイトルメントを指定できます。規則における条件には、ユーザのプロファイル（ユーザ グループ）、ユーザがエンタープライズ ネットワークにアクセスする方法（無線、有線、その他）やタイミング（時間帯）を含めることができます。

ACS Express は、ネットワーク デバイス（デバイス管理アクセス）を設定するネットワーク管理者アクセスの制御も行います。デバイス管理では、ACS Express は TACACS+ または RADIUS を使用して通信する NAS をサポートします。クレデンシャルの検証とエンタイトルメントの確認は、ネットワーク アクセスでの説明と同じ方法で処理されます。デバイス管理のエンタイトルメントでは、許可される最大限の管理特権レベルを指定します。規則における条件には、ユーザのプロファイル（ユーザ グループ）、設定するデバイス、ユーザがエンタープライズ ネットワークにアクセスするタイミング（時間帯）を含めることができます。

ACS Express は最大 50 の NAS をサポートします。24 時間内に行われるユーザ認証が 350 以下である中小規模の企業に適しています。

ACS Express はアプライアンスとして提供されます。ACS Express アプライアンスのセットアップには、コマンドライン インターフェイス（CLI）を使用します。ACS Express サーバの設定には GUI を使用します。ACS Express はペアでの配置が可能で、*プライマリ* Express サーバの設定が *セカンダリ* サーバに複製されます。

ACS Express の機能

ここでは、ACS Express の機能について説明します。

プロトコル

ACS Express は、次のような主要なプロトコルをサポートします。

認証

ACS Express は、ログインが試行されると、認証を使用してユーザの ID を確認します。ACS Express は、次の認証方法を使用します。

- クレデンシャル ソース
- マシン認証

クレデンシャル ソース

ACS Express は、ローカル データベース、外部トークン サーバ、LDAP、およびネットワーク アクセス ポリシーに基づくクレデンシャル ソースとしての AD の使用をサポートします。ACS Express は、プロキシ RADIUS を使用したトークン サーバの使用をサポートします。

マシン認証

マシン認証により、ACS Express に対してコンピュータの ID とクレデンシャルを使用して、クライアント マシンは自身を認証できるようになります。ACS Express は、Active Directory に対しては Windows マシン認証のみをサポートしています。

ACS Express が各種プロトコルに対してサポートするマシン認証の設定を、表 1-1 に示します。GUI を使用して、外部および内部の EAP 方式を設定します。

表 1-1　サポートされるマシン認証プロトコル

外部方式	内部方式
PEAP	EAP-MSCHAPv2
PEAP	EAP-TLS
EAP-TLS	

証明書のセットアップの一環として、ACS Express の EAP および CA サーバ証明書をインストールし、マシン証明書を取得するクライアント マシンについて Active Directory での自動登録をイネーブルにする必要があります。

アクセス ポリシー

ACS Express は次のアクセス ポリシーをサポートします。

- Group Mapping：ユーザまたはマシンのエンタイトルメントを確認するための外部グループのマッピングをサポートします。
- Time-based：Time of Day（ToD; 時間帯）と曜日に基づいてアクセスをサポートします。
- RADIUS Response Sets：グループ マッピングおよび時間ベースの条件に基づいて認証応答での RADIUS アトリビュートまたは値を返す処理をサポートします。
- Machine Access Restrictions：ユーザ認証成功の前提条件としてマシン認証を要求するマシン アクセス制限をサポートします。
- Access Policy：アクセス サービスの定義およびアプリケーションをサポートします。

サービサビリティとアベイラビリティ

ACS Express は、プライマリ サーバの設定をセカンダリ サーバに複製します。ACS Express は、プライマリ - セカンダリ AAA サーバ配置もサポートします。この配置では、プライマリ サーバに接続できないときに、NAS がセカンダリ AAA サーバに連絡することができます。

管理

ACS Express は次の管理機能をサポートします。

- Web ベースの GUI：Web ブラウザを使用して、ACS Express のシステム管理および設定をリモートからセキュアに実行できます。
- コマンドライン インターフェイス：サーバ コンソールまたは SSH を使用して CLI にアクセスできます。CLI を使用すると、管理者は別の ACS Express サーバの設定をコピーして貼り付けることができます。CLI は、プログラム設定やバッチ設定に使用できます。
- 管理アクセス コントロール：管理者とオペレータの各種アクセス レベルを提供します。特定のページにはオペレータは読み取り専用アクセスしかできないように制限します。
- パスワード ポリシー：パスワードの失効、強制的な変更、ロックアウトをサポートします。パスワード ポリシーは、マシン上にある管理者ログに適用されます。
- ロギング：RADIUS アカウンティング ログ、デバッグ ログ、マシン ログ オフ時のバックアップをサポートします。
- レポート：使用状況レポートおよびトラブルシューティング レポートを提供します。

デジタル証明書

Cisco Secure ACS Express は、CA 証明書の追加をサポートします。管理者は、自己署名証明書のインストールや生成、設定された証明書のダウンロードを行うことができます。

システムに関する説明

Cisco Secure ACS Express は、集中型の RADIUS および TACACS+ サーバとして動作する使いやすいアクセス コントロール サーバです。集中型のアイデンティティ ネットワーキング ソリューションで認証と認可を併用することによってアクセス セキュリティを強化し、これにより、柔軟性が高まり、ユーザ生産性が向上します。ACS Express は、有線 LAN、無線 LAN、ファイアウォール、VPN など、さまざまなアクセス接続をサポートします。

Cisco Secure ACS Express は、ラック マウント可能なアプライアンスとして提供されます。ACS Express アプライアンスは Intel Celeron 3.2 GHz プロセッサ、1 GB メモリ、および 250 GB ハード ディスク ドライブを使用します。

配置シナリオ

ここでは、ACS Express が使用可能な配置シナリオについて説明します。

- エンタープライズ ブランチ
- リテール ブランチ

- 中小企業

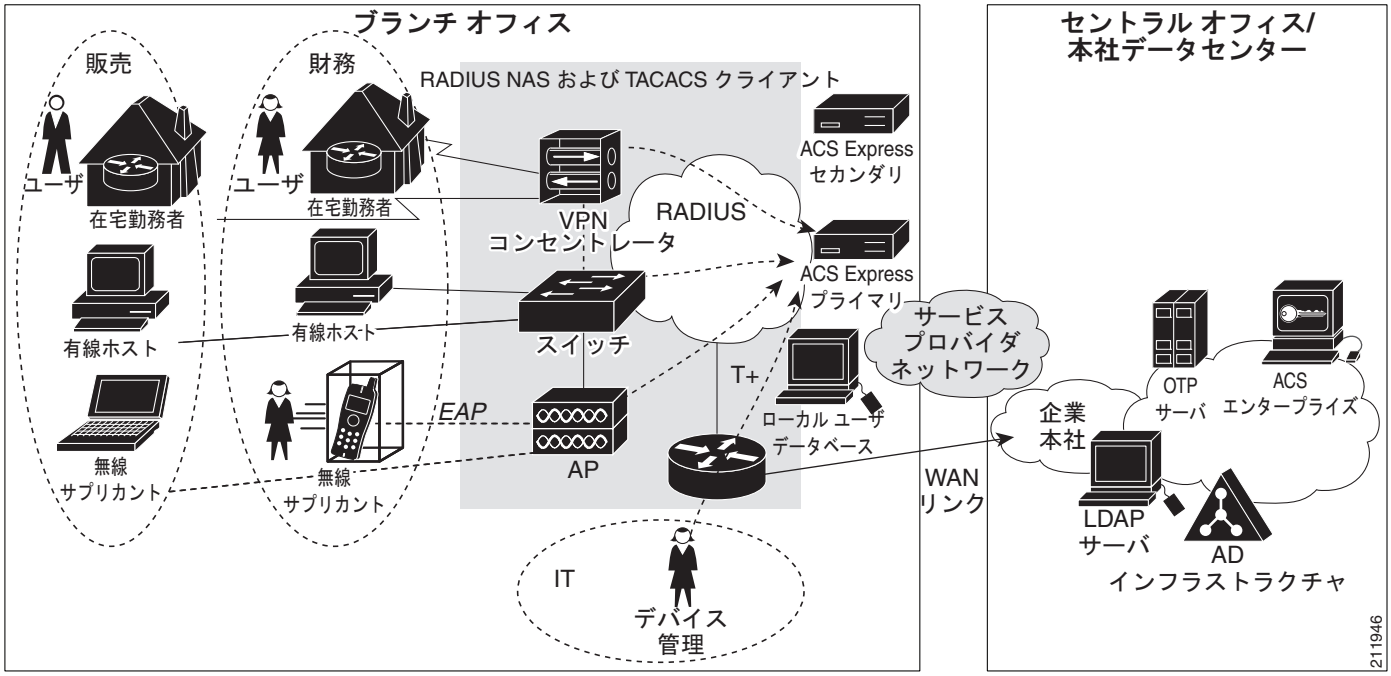
エンタープライズ ブランチ

大規模エンタープライズには、多くの場合、集中型の AAA ネットワークが装備され、企業ネットワーク内でさまざまな地域の業務を管理しています。大規模エンタープライズでは、集中型のユーザ データベース（Active Directory など）でユーザやマシンの ID の管理も行っています。

エンタープライズはブランチ サイトを展開していることがあります。この場合、WAN の停止による悪影響の軽減や、ローカル AAA サーバの使用が期待されています。ブランチ サイトには、単一またはペアにした ACS Express が配置されます。ACS Express は、集中型のユーザ データベースに対してユーザとマシンのいずれかまたは両方を認証するように設定されます。エンタープライズでは、ブランチ サイトにユーザ データベースを配置することがあります。

ブランチ サイトでは、無線および有線のネットワーク アクセスが実装されます。VPN アクセスは、セントラル オフィスで管理されるのが一般的です。図 1-1 に、エンタープライズ ブランチ配置シナリオの例を示します。

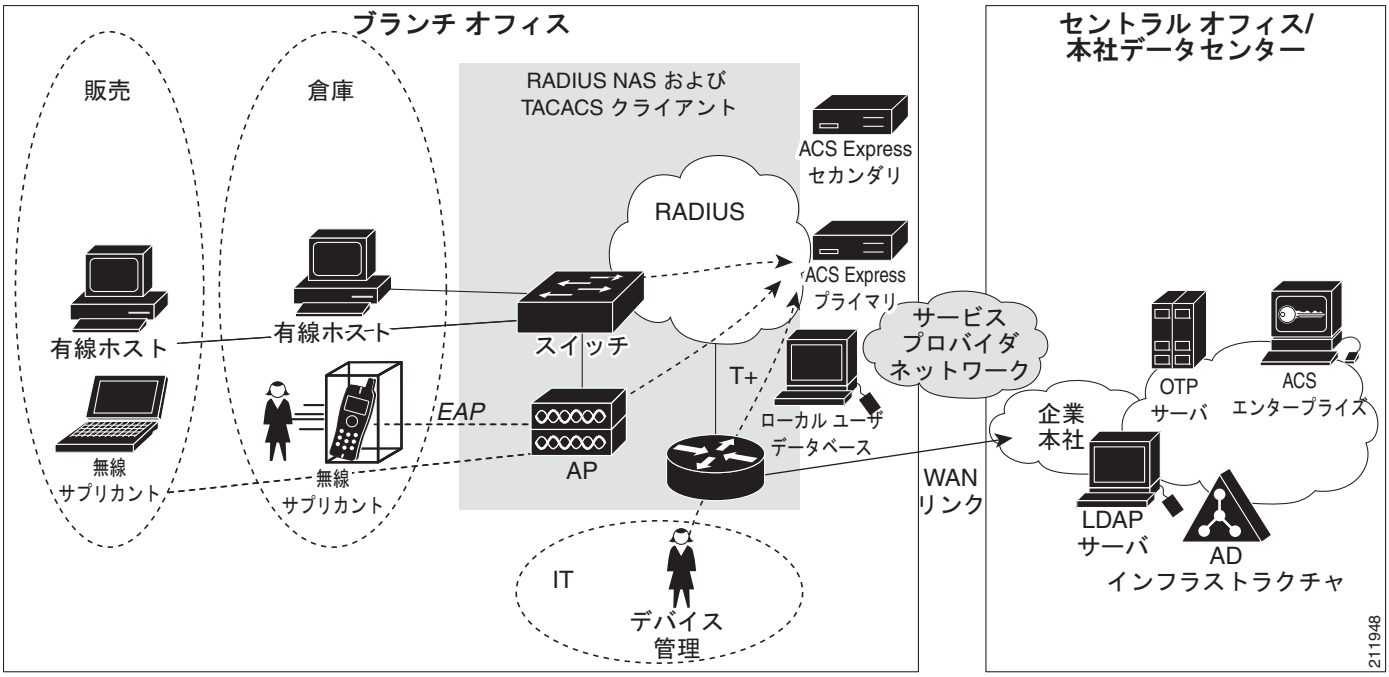
図 1-1　エンタープライズ ブランチ オフィス シナリオ



リテール ブランチ

大規模なリテール チェーンでは、各店舗または各拠点に 1 ～ 2 台の ACS Express サーバが配置されることがあります。各拠点では店舗の従業員に関する独自のデータベースが管理され、セントラル オフィスでは企業の従業員に関するデータベースが管理されます。ACS Express は、拠点と企業のデータベースに対してユーザとマシンの ID を認証するように設定されます。拠点では、無線および有線のネットワーク アクセスが実装されます。図 1-2 に、リテール ブランチ配置シナリオの例を示します。

図 1-2　リテール ブランチ オフィス シナリオ

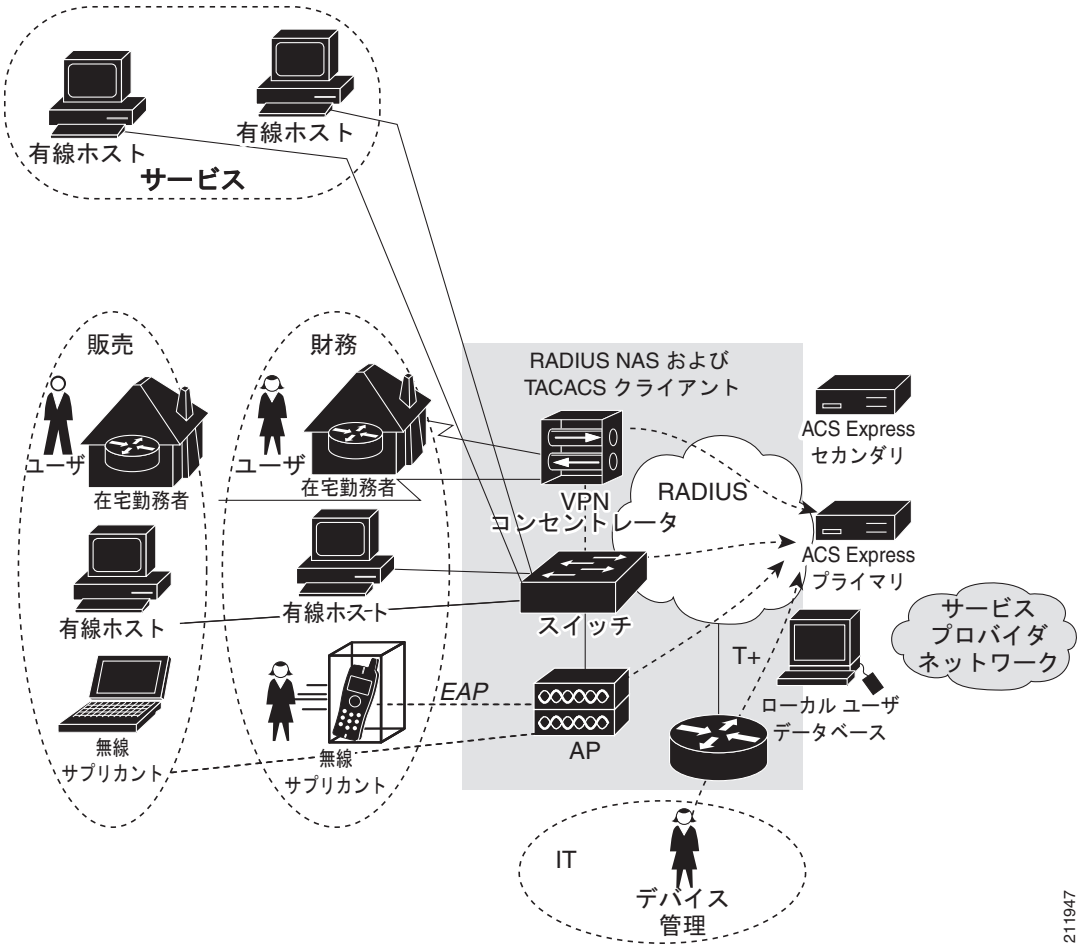


中小企業

中小企業（SMB）は、従業員が数百名の単一のサイトで構成されることがあります。ユーザとマシンの ID は、Active Directory や LDAP などの内部データベースで管理されます。SMB サイトでは、One-Time Password（OTP; ワンタイム パスワード）サーバを管理して、仮想プライベート ネットワーク（VPN）を使用したネットワークへのユーザ アクセスの認証を行うこともあります。

SMB サイトには、単一またはペアにした ACS Express サーバが配置されます。ACS Express は、アクセスの種類に基づいて適切なデータベースに対してユーザおよびマシンの ID を認証するように設定されます。SMB サイトでは、有線、無線、および VPN アクセスが提供されます。図 1-3 に、SMB 配置シナリオの例を示します。

図 1-3　中小企業シナリオ



パスワード ポリシー

ACS Express は、ローカル データベースの使用をサポートします。また、外部トークン サーバ、LDAP、およびアクセス サービスに基づくクレデンシャル ソースとしての AD の使用もサポートします。

ACS Express は、プロキシ RADIUS を使用したトークン サーバの使用をサポートします。パスワード ポリシーは管理ユーザとローカル ユーザの両方に適用されますが、パスワード ポリシーの設定にはそれぞれ異なる画面を使用します。

管理者パスワード ポリシーの設定は、ACS Express サーバに保存されます。ポリシー設定の更新には、ACS Express GUI を使用します。

ローカル ユーザ パスワード ポリシーの設定は、ローカル データベースに保存されます。ローカル ユーザのポリシー設定の更新には、ACS Express GUI を使用します。この設定は、管理者のパスワード ポリシー設定とは独立して行われます。

表 1-2 に、ACS Express パスワード ポリシー設定項目の一覧を示し、説明します。[Users & Identity Stores] > [Internal User Database] > [Users] を使用して、パスワード フィールドを変更できます。

表 1-2　パスワード ポリシー

パスワード ポリシー	説明
Minimum length	パスワードの最小の長さを指定します。
Upper-case required	ユーザ パスワードに大文字を含める必要があるかどうかを指定します。デフォルトは TRUE です。
Lower-case required	ユーザ パスワードに小文字を含める必要があるかどうかを指定します。デフォルトは TRUE です。
Number required	ユーザ パスワードに数字を含める必要があるかどうかを指定します。デフォルトは TRUE です。
Disallow user name	ユーザ パスワードにユーザ名を使用できるかどうかを指定します。デフォルトは TRUE で、ユーザ名をパスワードとして使用することはできません。
Cannot Reuse Last Password	最近のパスワードを使用できるかどうかを指定します。デフォルト は TRUE で、失効した最後のパスワードを再利用することはできません。
Enable Password Lockout after *N* Attempts	パスワード入力エラーの最大回数の有無を指定します。デフォルトは TRUE です。
Number of Failed Attempts	ユーザがシステムからロックアウトされる前にログインを試行できる回数を指定します。デフォルトは 8 です。 ログインの試行回数が上限を超えたためにユーザがロックアウトされた場合、再び使用できるようにするには、管理者がそのユーザ アカウントを再度有効にする必要があります。

パスワードの規則

パスワードは、以下の規則に従う必要があります。

- 少なくとも 1 つの小文字を含むこと
- 少なくとも 1 つの大文字を含むこと
- 少なくとも 1 つの数字を含むこと
- 少なくとも 1 つの特殊文字（下記を参照）を含むこと
  !$ % ^ & * ( ) _ + | ~ - = ` { } [ ] : " ; ' < > ?, ./
- 同じ文字列を連続して 4 回以上繰り返すことはできないこと
- 8 文字以上であること
- ユーザ名を含まないこと
- 現在のパスワードを再利用しないこと
- *cisco* または *ocsic* という語を含まないこと

内部ユーザ パスワードの変更

プロトコル パスワードの変更は、MS-CHAPv2 および TACACS+ を使用する場合にサポートされます。各ユーザは、ACS Express GUI を使用して自分のパスワードを変更できます。

内部データベースで認証するユーザは、いつでも、ACS Express プライマリ サーバでパスワードを変更できます。パスワードを変更するには、次のように、ブラウザで URL を指定します。

https://<*ホスト名*>/changeuserpassword.do

ここで、*ホスト名*は ACS Express プライマリ サーバの名前です。

AD、LDAP、OTP などの外部データベースを使用して認証するユーザの場合、この画面を使用してパスワードを変更することはできません。

（注） 複製された環境では、セカンダリ サーバでパスワードを変更することはできません。

認証、認可、アカウンティング

ACS Express は、RADIUS プロトコル、TACACS+、および EAP を使用して、認証（Authentication）、認可（Authorization）、およびアカウンティング（Accounting）（AAA または トリプル A）機能を提供します。

- 「RADIUS」（P.1-9）
- 「TACACS+」（P.1-10）
- 「EAP」（P.1-11）

RADIUS

Remote Authentication Dial In User Service（RADIUS）は、ネットワーク アクセスをサポートする Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）プロトコルです。ACS Express は、インターネット Request for Comments（RFC; コメント要求）2138 に定義されているように RADIUS プロトコルをサポートし、さらに以下の RFC もサポートしています。

（注） ACS Express は、実質的に以下の RFC に準拠しています。

- RFC 2284：PPP Extensible Authentication Protocol (EAP)
- RFC 2865：Remote Authentication Dial In User Service
- RFC 2866：RADIUS Accounting
- RFC 2867：RADIUS Accounting の拡張（トンネル プロトコルのサポート用）
- RFC 2869：RADIUS 拡張

ACS Express は、新旧の RADIUS ポートでの認証をサポートします。ACS Express は、ポート 1645 およびポート 1812 での認証要求を受け入れます。アカウンティングの場合、ACS Express はポート 1646 および ポート 1813 でのアカウンティング パケットを受け入れます。

ACS Express は、IOS/PIX、VPN コンセントレータ、Airespace、Aironet、Juniper、および Microsoft の Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）をサポートします。ACS Express を使用して、カスタム VSA を定義することもできます。

RADIUS 認証要求

ACS Express サーバは、ネットワーク デバイスから RADIUS 認証要求を受信すると、次の処理を実行します。

1. ACS Express は、一致する RADIUS アクセス サービスを見つけようとします。
2. ACS Express は、上に示した順序で RADIUS アクセス サービスを評価し、最初に一致するサービスが見つかったら検索を停止します。
3. 一致は、各サービスの選択規則を評価することによって決定されます。
4. 次に、ACS Express は、一致したサービスに指定されている認証規則を適用します。
5. 一致するサービスが見つからない場合、アクセスは拒否されます。

TACACS+

Terminal Access Controller Access-Control System（TACACS+; ターミナル アクセス コントローラ アクセス コントロール システム）プロトコルは、オリジナルの TACACS プロトコルに Cisco 独自の強化機能を加えたプロトコルです。TACACS+ は 1 台以上の中央サーバを使用してルータ、ネットワーク アクセス サーバ（NAS）、その他のネットワーク コンピューティング デバイスにアクセス コントロールを提供します。

TACACS+ は数多くのプロトコルをサポートし、TCP ポート 49 を使用して独立した認証、認可、アカウンティングの各サービスを提供します。TACACS+ は安全な通信を確立するため、TCP パケットの本体を暗号化します。

ACS Express はグループ、ローカルおよび外部の TACACS+ ユーザごとに特権レベルをサポートし、RADIUS の共有秘密情報を分離します。

TACACS+ 認証要求

ACS Express サーバは、ネットワーク デバイスから TACACS+ 認証要求を受信すると、次の処理を実行します。

- 指定されたユーザ データベースに対して、ユーザ クレデンシャルの認証を行います。クレデンシャルが有効でない場合、アクセスは拒否されます。
- 有効であると、ユーザ データベースにより、ユーザが属するユーザ グループが返されることもあります。
- アクセスしたネットワーク デバイス、ユーザ グループ、およびアクセスした時刻に基づいて、ACS Express は一致するアクセス規則を見つけようとします。
- ACS Express は、上に示した順序でアクセス サービスを評価し、最初に一致する規則が見つかったら検索を停止します。
- ACS Express は、一致する規則の結果を適用します。
- アクセスは、拒否されるか、または指定の特権レベルが付与され、アイドル タイムアウトとセッション タイムアウトが適用されて許可されます。
- 一致する規則が見つからない場合は、デフォルトの応答規則が適用されます。

EAP

RFC 3748 で定義される Extensible Authentication Protocol（EAP）は、無線ネットワークおよびポイントツーポイント接続で使用される認証フレームワークです。EAP プロトコルが最もよく使用されるのは無線 LAN ですが、有線 LAN 認証にも使用できます。

ACS Express は、以下の EAP 方式をサポートします。

- EAP-TLS：EAP-Transport Level Security は RFC 2716 に定義されています。
- PEAP v0：Protected EAP Version 0
- PEAP v1：Protected EAP Version 1
- EAP-FAST v0：Flexible Authentication via Secure Tunneling

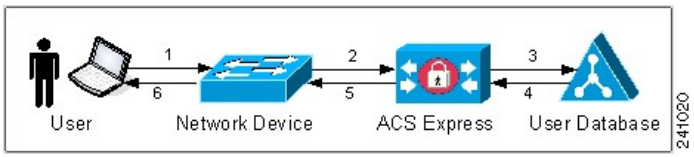
（注）　ACS Express 5.0.1 は、EAP-FASTv1 や EAP-FASTv1a などの最新の EAP-FAST RFC に対して完全準拠ではありません。

- LEAP：Lightweight Extensible Authentication Protocol

ユーザ認証の概要

ACS Express の主な役割は、ネットワークにアクセスするユーザを認証することです。ここでは、ユーザ認証の概要について説明します。図 1-4 に、ユーザ認証でのイベントの流れを示します。

図 1-4　　ユーザ認証の概要



次に、図 1-4 の番号に関連するイベントを説明します。

1. ユーザがネットワークに接続しようとします。

   ユーザのクレデンシャルが、ユーザのコンピュータからネットワーク デバイスに送信されます。たとえば、ラップトップ コンピュータの 802.1.x サプリカントが、ユーザのクレデンシャルを取得し、LEAP 経由でネットワーク デバイスに送信します。

2. ネットワーク デバイスは ACS Express サーバに認証要求を送信します。

   ネットワーク デバイスはクレデンシャルを受信すると、そのクレデンシャルの認証を受けるため ACS Express サーバに認証要求を送信します。認証要求の送信には、RADIUS または TACACS+ プロトコルが使用されます。

3. ACS Express がクレデンシャルの認証を行います。

   認証要求のプロトコル、ネットワーク デバイス、内容のいずれかまたは両方に基づいて（「選択規則」と呼ばれます）、ACS Express は適用する適切なアクセス サービスを決定します。アクセス サービスにより、クレデンシャルの認証に使用するデータベースが決まります。

   たとえば、アクセス サービスは、Active Directory に対して認証が行われる無線コントローラからの認証要求を指定することができます。

4. ユーザ データベースは、ACS Express サーバに認証応答を返します。

   ユーザ データベースは、ACS Express サーバに対して応答を返し、提供されたクレデンシャルが有効であるかどうかと、ユーザが属するユーザ グループを知らせます。ユーザ グループは、組織でのユーザの役割を示すことが一般的です。たとえば、あるユーザは Employees ユーザ グループに属し、別のユーザは Finance グループに属しています。

5. ACS Express サーバは、ネットワーク デバイスに認証応答を返します。

   ユーザのクレデンシャルが有効でない場合、ACS Express サーバは RADIUS または TACACS+ の適切な拒否応答を返します。

   クレデンシャルが有効である場合、ACS Express サーバはさらにアクセス サービスを評価し、何らかのアクセス規則が指定されているかどうかを確認します。アクセス規則は、ユーザ エンタイトルメントを指定します。一致する規則は、ユーザ グループやアクセスの時刻など、さまざまな基準に基づいて決定されます。エンタイトルメントは RADIUS または TACACS+ アトリビュートの値ペアとして指定され、これらの値はネットワーク デバイスに返されます。

   たとえば、アクセス サービスが、Employees ユーザ グループに属しているユーザに従業員用の VLAN へのアクセス権が付与されていることを示すアクセス規則を保管している場合などです。

6. ネットワーク デバイスはユーザへの認証応答を返します。

   ネットワーク デバイスが ACS Express サーバから応答を受け取ると、デバイスは指定されたエンタイトルメントを強制し、適切な応答をユーザに返します。

設定の概要

ここでは、ACS Express サーバに必要な設定の概要について説明します。図 1-5 に示すように、各セクションは ACS Express GUI にあるドロワーに関連付けられています。

図 1-5　ACS Express GUI

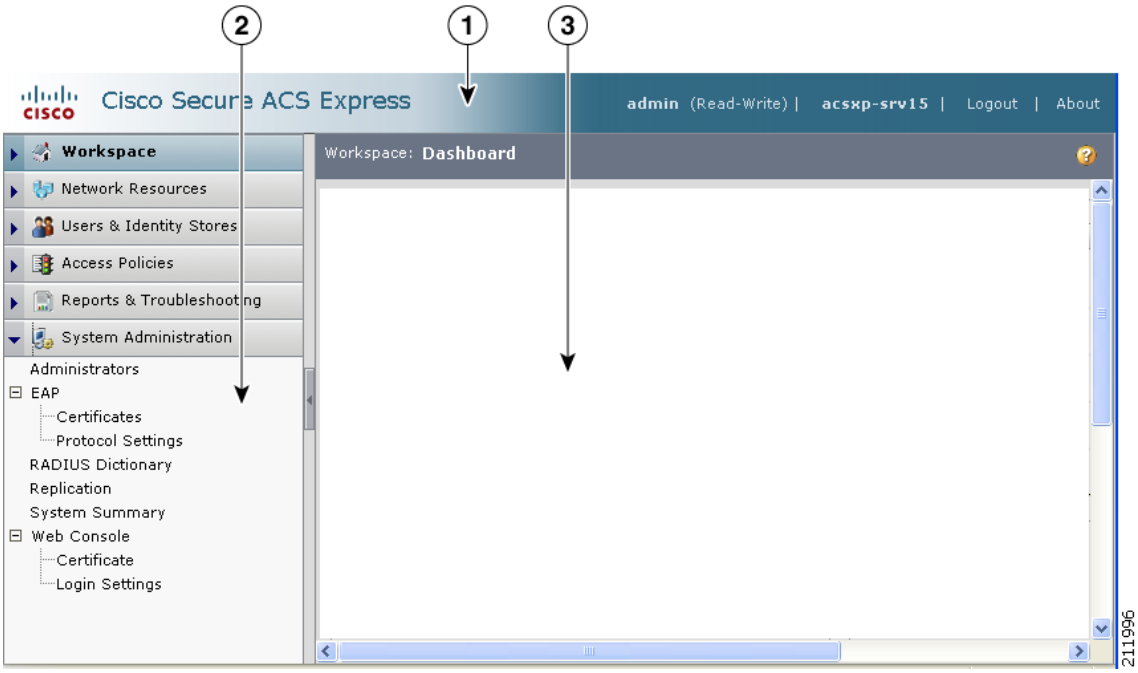


表 1-3　ACS Express GUI レイアウト

コールアウト	説明
1	[Status] ペイン
2	[Navigation] ペイン
3	[Content] ペイン

ネットワーク リソース

ネットワークを構成するデバイスとデバイス グループは、ネットワーク リソースです。GUI を使用して、設定にすべてのデバイス グループを追加してから、デバイス グループにデバイスを追加します。詳細については、「ネットワーク デバイス」（P.3-1）を参照してください。

ユーザ ストアと ID ストア

インストールする必要のあるユーザとユーザ グループを ACS Express サーバに設定します。ACS Express は、内部ユーザ データベースおよびリモートまたは外部のデータベースを使用してユーザを認証します。

- 「内部ユーザ データベース」（P.1-13）
- 「外部ユーザ データベース」（P.1-13）

内部ユーザ データベース

GUI を使用して、内部ユーザ データベースにすべてのローカル ユーザを追加します。各ローカル ユーザは、少なくとも 1 つのユーザ グループに属している必要があるため、最初にユーザ グループを作成してから、ローカル ユーザを設定します。詳細については、「内部ユーザ データベース」（P.4-1）を参照してください。

外部ユーザ データベース

ACS Express は、以下の外部ユーザ データベースをサポートします。

- 「Microsoft Active Directory」（P.4-9）
- 「LDAP データベース」（P.4-11）
- 「One-Time-Password サーバ」（P.4-15）

アクセス ポリシー

ACS Express のアクセス サービスは、次の 2 種類に分類されます。

- ネットワーク アクセス
- デバイス管理

ネットワーク アクセス ポリシーは、無線、有線、または VPN ネットワークにアクセスしようとするユーザに適用されます。ネットワーク アクセス ポリシーでも、PAP、CHAP、MSCHAPv2、PEAP、EAP-TLS、EAP-FAST、LEAP、Windows マシン認証などのさまざまな認証スキームがサポートされ

ます。ネットワーク アクセス ポリシーは、RADIUS を使用して ACS Express と通信するネットワーク デバイスに適用されます。ネットワーク アクセス ポリシーは、Active Directory、LDAP、One-Time Password（OTP; ワンタイム パスワード）データベース、または ACS Express の内部ユーザ データベースに対してユーザ認証を行うように設定できます。

デバイス管理ポリシーは、ネットワーク デバイスにアクセスして設定しようとするユーザに適用されます。ACS Express は、ユーザに対して最大限許可される特権レベルの認証および認可を行います。ネットワーク デバイスが ACS Express と通信するときには、TACACS+ または RADIUS を使用します。デバイス管理ポリシーは、Active Directory、LDAP、ワンタイム パスワード データベース、または ACS Express の内部ユーザ データベースに対してユーザ認証を行うように設定できます。

アクセス規則

アクセス規則を使用すると、ACS Express サーバを使って次のことを実行できるようになります。

- 組織でのユーザの役割に基づいてユーザ エンタイトルメントを指定します。
- 従業員と請負業者に異なる VLAN を割り当てます。
- ToD に基づいてネットワーク アクセスを制限します（たとえば、月曜日から金曜日までの午前 9:00 から午後 5:00 まで（0900 ～ 1700）、など）。

強制する規則の一覧を表示するためのワークシートを作成すると便利です。規則ごとに、アクセス条件と、結果として付与されるユーザ エンタイトルメントを指定する必要があります。アクセス条件には、ネットワーク アクセスの種類、ユーザが属するグループ、ユーザがアクセスできる ToD などが含まれます。結果には、すべての条件が満たされたときに付与されるエンタイトルメントを指定します。

表 1-4 に、ワークシートの例を示します。

表 1-4　アクセス規則ワークシートの例

ネットワーク アクセス	ユーザ グループ	アクセスの時刻	エンタイトルメント
無線アクセス	Employee	月～金、午前 8:00 ～午後 6:00（0800 ～ 1800）	VLAN *Employee* を割り当て
無線アクセス	Employee	土～日、午前 8:00 ～午後 6:00（0800 ～ 1800）	アクセスを拒否
VPN アクセス	Employee、RemoteUsers	月～日、週 7 日間/1 日 24 時間	VPN グループ *RemoteUsers* を割り当て

完成したワークシートを使用して、ユーザがネットワークにログインしたときにアクセスを許可する ToD やユーザに付与するエンタイトルメントなどのポリシー要素を設定できます。エンタイトルメントは、ネットワーク デバイスに返される RADIUS 応答として指定されます。

ポリシー要素の設定

以下のようなポリシー要素の設定の詳細については、「ポリシー要素」（P.5-12）を参照してください。

- 「RADIUS 応答」（P.5-12）
- 「時間帯」（P.5-14）

RADIUS アクセス サービス

アクセス規則を設定すると、必要な RADIUS アクセス サービスを作成できます。RADIUS アクセス サービスにより、要求を処理するネットワーク デバイス グループ、認証に使用するデータベース、プロトコル設定、エンタイトルメントを付与するアクセス規則を指定します。

ワークシートに基づいて、ネットワーク アクセスの種類ごとに RADIUS アクセス サービスを作成します。たとえば、表 1-4 に示すサンプルのワークシートから、*Wireless Access* と *VPN Access* の 2 つの RADIUS アクセス サービスを作成します。*Employee* と *RemoteUser* の 2 つのユーザ グループも設定する必要があります。

RADIUS アクセス サービスには、次の設定が必要です。

- **General Settings**：アクセス サービスの名前を指定し、説明を記述します。
- **Selection Rules**：ネットワーク アクセスの種類に対するネットワーク デバイス グループを指定します。サンプルのワークシートに基づき、*Wireless Access* アクセス サービスは、*Wireless Controllers* デバイス グループからの要求を処理します。
- **Authentication Rules**：ユーザ認証およびプロトコル設定に使用するデータベースを指定します。

ワークシートでの記述に従って、アクセス規則を設定します。詳細については、「アクセス サービス」（P.5-2）を参照してください。

デバイス管理

ネットワーク デバイスは、TACACS+ または RADIUS を使用して ACS Express と通信できます。ここでは、ネットワーク デバイスが TACACS+ を使用して通信するために必要なデバイス管理ポリシーの設定方法について説明します。

次のことは既に実行済みであることを前提に説明します。

- AAA サーバに対するログイン認証に使用するネットワーク デバイスを設定します。
  - 「ネットワーク リソース」（P.1-13）を参照してください。
- ユーザ データベースを設定します。
  - 「ユーザ ストアと ID ストア」（P.1-13）を参照してください。

アクセス規則

デバイス管理アクセス規則を定義するには、規則の一覧を表示するためのワークシートを作成すると便利です。規則ごとに、アクセス条件と、アクセスが許可される場合の特権レベルを指定する必要があります。アクセス条件には、管理対象のネットワーク デバイス グループ、ユーザが属するグループ、アクセスが許可される時間帯などが含まれます。結果には、すべての条件が満たされたときに付与される特権を指定します。デバイス アクセス規則のワークシートの例については、表 1-5 を参照してください。

表 1-5　デバイス アクセス規則ワークシートの例

ネットワーク アクセス	ユーザ グループ	アクセスの時刻	特権レベル
無線コントローラ	Read-Write Admin	月～金、午前 8:00 ～午後 6:00（0800 ～ 1800）	15
無線コントローラ	Read-Only Admins	—	アクセスを拒否
VPN コンセントレータ	Read-Only Admin	—	1

完成したワークシートを使用して、ポリシー要素を設定できます。以下のようなポリシー要素の設定の詳細については、「ポリシー要素」（P.5-12）を参照してください。

- 「RADIUS 応答」（P.5-12）
- 「時間帯」（P.5-14）

TACACS+ アクセス サービス

アクセス規則を設定すると、必要な TACACS+ アクセス サービスを作成できます。TACACS+ アクセス サービスにより、要求を処理するネットワーク デバイス グループ、ユーザ グループ、アクセスの時間帯を指定し、すべての条件が満たされたときに付与される特権レベルを指定します。TACACS+ 認証要求では、アイドル タイムアウトとセッション タイムアウトのセッション タイムアウト設定も一致することが必要です。

ワークシートに基づいて TACACS アクセス サービスを作成します。たとえば、表 1-5 に示すサンプルのワークシートから、以下のメンバーからの要求に対応する TACACS+ アクセス サービスを作成します。

- Read-Write Admin グループのメンバーである無線コントローラ
- Read-Only Admins グループのメンバーである無線コントローラ
- Read-Only Admins グループのメンバーである VPN コントローラ

ワークシートでの記述に従って、アクセス規則を設定します。詳細については、「TACACS+ アクセス サービス」（P.5-8）を参照してください。