CHAPTER 1

ACS サーバの展開について

この章では、ACS サーバの考えられる展開方法とそのコンポーネントの概要について説明します。

この章の内容は、次のとおりです。

- 「展開シナリオ」（P.1-1）
- 「ACS サーバの設定について」（P.1-5）

展開シナリオ

ここでは、ACS を使用する次の 3 つの展開シナリオについて説明します。

- 「小規模 ACS 展開」（P.1-1）
- 「中規模 ACS 展開」（P.1-3）
- 「大規模 ACS 展開」（P.1-3）

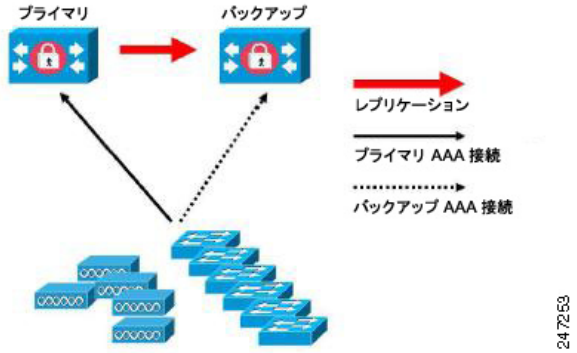
小規模 ACS 展開

最も基本的な ACS の展開は、図 1-1 に示すように、2 台のサーバで構成されます。第 1 のサーバは、ネットワークのすべての設定、認証、ポリシー要件を満たすプライマリ サーバです。

第 2 のサーバは、AAA クライアントとプライマリ サーバ間の接続が失われた場合にバックアップ サーバとして使用されます。プライマリ ACS サーバからセカンダリ サーバへのレプリケーションを使用して、セカンダリ サーバがプライマリ サーバと同期している状態を保ちます。

小規模なネットワークでは、この構成により、プライマリとセカンダリの RADIUS サーバを、すべての AAA クライアントで同じように設定できます。

図 1-1　小規模 ACS 展開



組織内のユーザと AAA クライアントの数の増加に応じて、ACS の展開方法を基本的な設計から変更し、図 1-2 に示す分割 ACS 展開設計を使用することを推奨します。

分割 ACS 展開

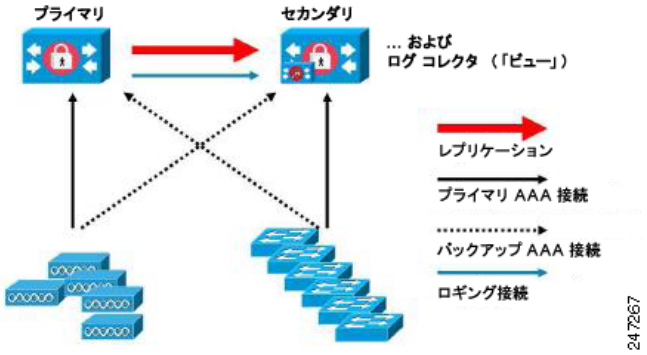
分割 ACS 展開では、小規模 ACS 展開と同様にプライマリ サーバとセカンダリ サーバを使用しますが、AAA の負荷を 2 台のサーバに分散し、AAA フローを最適化します。AAA 接続に問題が発生した場合は、各サーバが両方のサーバのすべての負荷を処理しますが、通常運用時には、どちらのサーバも認証要求のすべての負荷を処理しません。

サーバのこの特性により、各 ACS システムへの負荷が最適化され、正常動作を通じてセカンダリ サーバの動作状態を知ることができます。

この配置のもう 1 つの利点は、各サーバを、デバイスの管理やネットワークの許可など特定の運用のために使用しながら、障害時にすべての AAA 機能を実行できることです。

2 台の ACS システムが、AAA クライアントからの認証要求の処理とアカウンティング データの収集を行うため、一方のシステムをログ コレクタとして使用することを推奨します。図 1-2 では、セカンダリ ACS サーバをログ コレクタとして使用しています。

図 1-2　分割 ACS 展開

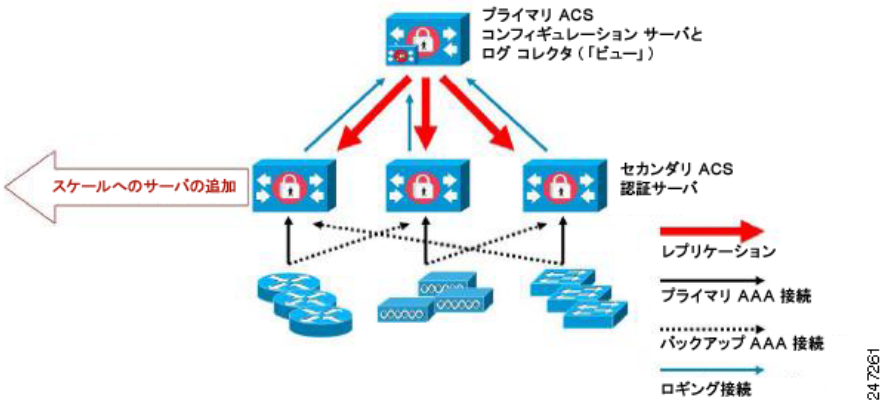


この設計のもう 1 つの利点は、図 1-3 に示すように拡張が可能なことです。

中規模 ACS 展開

ローカル ネットワークの成長に応じて、さらに ACS サーバをシステムに追加する必要があります。このシナリオでは、プライマリ サーバを昇格させて構成サービスを実行し、セカンダリ サーバを AAA 機能で使用することを検討します。ログ トラフィックの量が増えた場合、プライマリ サーバを集中化されたログ コレクタとして使用するか、1 台の専用の ACS サーバをログ コレクタとして使用します。中規模 ACS 展開は、3 ～ 6 台のサーバから構成されます。

図 1-3　　中規模 ACS 展開



大規模 ACS 展開

図 1-4 に示すような大規模 ACS 展開では、集中化されたロギングを使用することを強く推奨します。大規模 ACS 展開は、7 ～ 10 台のサーバから構成されます。使用率の高いネットワークでは、大量の syslog トラフィックが生成される可能性があるため、専用のロギング サーバ（モニタリングおよびレポート サーバ）を使用することが推奨されます。ACS は発信ログ トラフィックに対して syslog メッセージを生成するため、RFC-3164 に準拠した任意の syslog サーバを使用して発信ロギング トラフィックを収集できます。

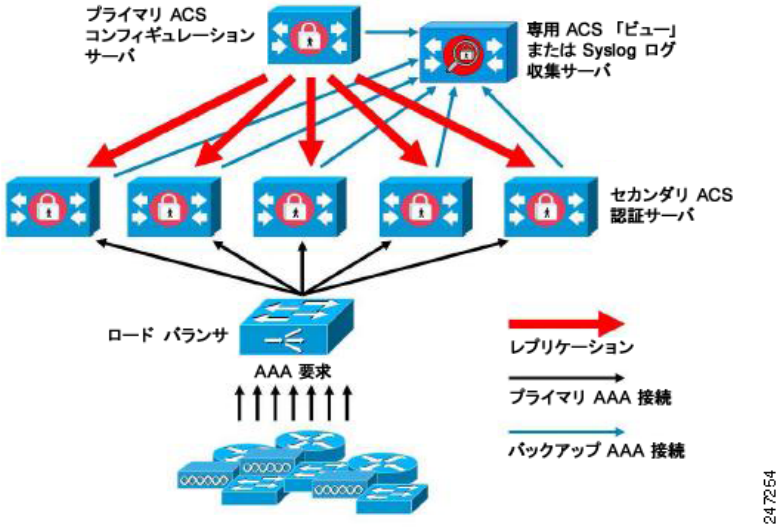
このタイプのサーバでは、すべての ACS サーバに対して、ACS が備えているレポート機能とアラート機能を使用できます。これには特別なライセンスが必要です（『User Guide for the Cisco Secure Access Control System 5.3』を参照してください）。ACS サーバのインストールの詳細については、「ACS サーバのインストール」（P.5-2）を参照してください。

モニタリングおよびレポートサーバと汎用 syslog サーバの両方にログを送信するようにサーバを設定することも検討してください。汎用 syslog サーバを追加することにより、モニタリングおよびレポート サーバが失われた場合に、バックアップが提供されます。

大規模で集中化されたネットワークでは、ロード バランサを使用する必要があります。図 1-4 を参照してください。これにより、AAA クライアントの展開が単純化され、AAA サーバに対するエントリが 1 つで済みます。ロード バランサは、使用可能なサーバへの AAA 要求のルーティングを最適化します。

ロード バランサが 1 台しかないと、シングル ポイント障害となります。したがって、冗長性を持たせるために 2 台のロード バランサを展開する必要があります。そのためには、各 AAA クライアントで 2 つの AAA サーバ エントリを設定する必要があり、この設定はネットワーク全体で同じになります。

図 1-4　大規模 ACS 展開



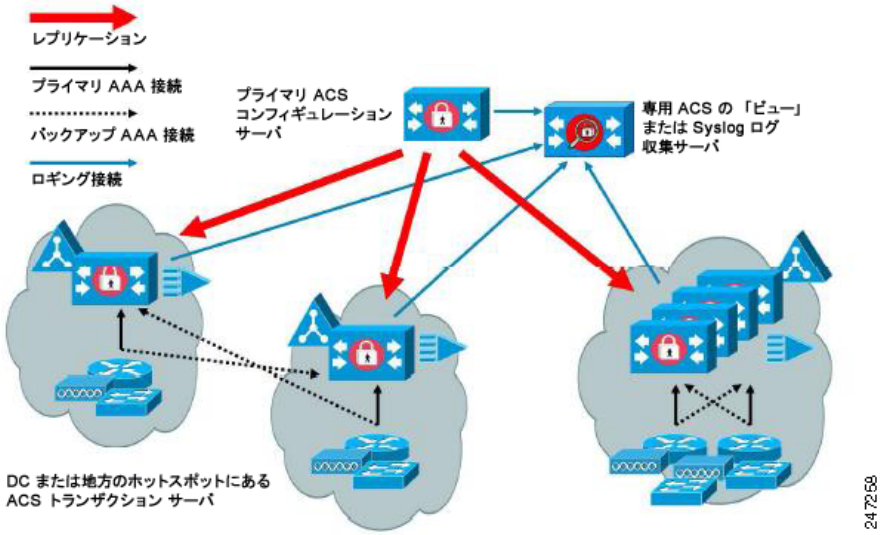
分散 ACS 展開

分散 ACS 展開は、世界中にキャンパスがある組織で有効です。ホーム キャンパスにプライマリ ネットワークがある場合もありますが、さまざまな地域のキャンパスに、小規模から大規模の LAN が存在することもあります。

AAA パフォーマンスを最適化するために、これらの各リモート キャンパスには独自の AAA インフラストラクチャを配置します。図 1-5 を参照してください。一貫性のある同期された AAA ポリシーを維持するためには、集中化された管理モデルを使用する必要があります。

集中化された構成でも、プライマリ ACS サーバと個別のモニタリングおよびレポート サーバを使用する必要があります。しかし、各リモート キャンパスには固有の要件があります。

図 1-5　分散 ACS 展開



リモート サイトがあるネットワークを計画する際に検討すべき要素としては、次のものがあります。

- 中央または外部データベース（AD または LDAP）を使用しているかどうかを確認します。最適化のために、ACS がアクセス可能な、外部データベースの同期されたインスタンスを各リモート サイトに配置する必要があります。
- AAA クライアントの場所も重要な留意事項です。ネットワークの遅延による影響や、WAN 障害によってアクセスできなくなる可能性を減らすために、ACS サーバは、できるだけ AAA クライアントの近くに配置する必要があります。
- ACS では、バックアップなどの一部の機能にコンソールからアクセスできます。各サイトで端末を使用することを検討します。これにより、ネットワークの外部から各サーバに対するセキュアなコンソール アクセスが可能になります。
- 小規模なリモート サイトが近くにあり、他のサイトへの信頼できる WAN 接続がある場合は、近くのサイトにある ACS サーバをローカル サイトのバックアップ サーバとして使用し、冗長性のある構成とすることもできます。
- 外部データベースにアクセスできるようにするには、すべての ACS ノードで DNS を適切に設定する必要があります。

ACS サーバの設定について

ここでは、各種 ACS サーバの役割と、その設定方法についての概要を説明します。ロールのサーバへの割り当てと設定の詳細については、『*User Guide for the Cisco Secure Access Control System 5.3*』を参照してください。

ここでは、次の内容について説明します。

- 「プライマリ サーバ」（P.1-5）
- 「セカンダリ サーバ」（P.1-6）
- 「ログ収集サーバ」（P.1-6）

インストール手順は、どの ACS サーバでも同様です。

CSACS-1121 アプライアンスを使用した ACS のインストールについては第 5 章「CSACS-1121 を使用した Cisco Secure Access Control System のインストールと設定」を参照してください。VMware ESX を使用した ACS のインストールについては第 6 章「VMware 仮想マシンへの ACS のインストール」を参照してください。ACS 展開では、最初に必ずプライマリ サーバをインストールしてください。

プライマリ サーバ

ACS 展開では、1 つのインスタンスだけが ACS プライマリとなり、構成機能を提供するとともに、レプリケーションのソースとなります。

ACS プライマリ サーバでは、ACS の展開に必要なすべてのシステム設定を行うことができます。ただし、ライセンスとローカル証明書は、各 ACS セカンダリ サーバで個別に設定する必要があります。

セカンダリ サーバ

プライマリ サーバを除く他のすべてのインスタンスはセカンダリ サーバとして機能します。

セカンダリ ACS サーバは、プライマリ サーバからすべてのシステム設定を受け取ります。ただし、次のものは各セカンダリ サーバで設定する必要があります。

- ライセンス：展開内の各 ACS セカンダリ サーバに対し、固有の基本ライセンスをインストールします。
- 新しいローカル証明書：セカンダリ サーバでローカル証明書を設定するか、プライマリ サーバからローカル証明書をインポートします。
- ログ収集サーバ：プライマリ サーバとセカンダリ サーバのいずれかを、ACS のログ収集サーバとして設定できます。セカンダリ ACS サーバをログ収集サーバとして設定することを推奨します。

セカンダリ サーバを ACS 環境の一部とするためには、アクティベーションを行う必要があります。管理者は、セカンダリ サーバのアクティベーションを行うか、自動アクティベーションを設定する必要があります。デフォルトでは、アクティベーションは自動に設定されます。

セカンダリ サーバは、アクティベーションが行われると、設定の完全な同期とレプリケーションの更新をプライマリ サーバから受信し始めます。

ログ収集サーバ

プライマリ サーバまたはいずれかのセカンダリ サーバがログ収集サーバとして機能できます。

ログ収集サーバは、展開内のプライマリ サーバとすべての ACS セカンダリ サーバからログを受信します。ACS セカンダリ サーバのうちの 1 台をモニタリングおよびレポート サーバとして割り当て、このセカンダリ サーバを AAA アクティビティから除外することを推奨します。

3 つの主なロギング カテゴリは、監査、アカウンティング、および診断です。

ロギング カテゴリと設定の詳細については、『*User Guide for the Cisco Secure Access Control System 5.3*』を参照してください。