

## Cisco Secure ACS ( Access Control Server ) V2.4 for Windows NT

Cisco Secure ACS ( Access Control Server ) for Windows NTは、AAA ( Authentication, Authorization and Accounting ) 機能を提供する、シスコのセキュリティ専用ソフトウェア・ソリューションの1つです。Cisco Secure ACS for Windows NTは、中小規模のアクセス環境に対して使いやすいアクセス制御サービスを提供します。これは、VPN ( Virtual Private Network )、時間に基づいたアクセス制御、および定義可能なセキュア通信レベルといった差別化サービスの展開と運用を簡素化する、密接に統合されたWindows NTサービスです。

Cisco Secureは、セキュリティ管理の初期実装時に導入して、その後でより複雑な環境およびポリシーに発展にした場合にも速やかに対応できます。Cisco Secureのアーキテクチャは、TACACS+およびRADIUSを使って数千ポートにサービスを提供する一方で、分散環境のニーズに対応して拡張できます。AAAの中央管理によって、あらゆるアクセスインフラストラクチャの展開が補完されます。

Cisco Secure ACS for Windows NTによって、ダイヤルアップアクセスサーバ、ファイアウォール、ルータに対するユーザーの許可を集中管理することが可能になります。データの中央レポジトリからアクセスを制御することで、各デバイスでネットワーク許可/権利を継続的に同期化するという面倒な作業が不要になり、ネットワークインフラストラクチャの拡張が簡素化されます。

ネットワークルータは、ダイヤルインフラストラクチャに不可欠の要素です。Cisco SecureはCisco IOSソフトウェアと密接に連携するため、ルータで使用されるCisco IOSコマンドに対して、権限認証や課金機能を提供できます。

さらに、Cisco SecureはCisco IOSソフトウェアと連携して、Bチャネルに対する異なるNAS ( Network Access Server ) 上でのマルチシャーシ・マルチリンクPPPのサポートといったシスコ独自のパワフルな機能を、サードパーティ製デバイスとの通信を妨げることなく利用可能にします。

### Cisco Secure ACS for Windows NT のアプリケーション

Cisco Secureは、ダイヤルアップ環境で次のようなアクセス制御サービスに利用できます。

#### Windows NT ユーザーデータベースとシングルログインの活用

相当のリソースを投資してWindows NT ユーザーデータベースに基づくユーザーアクセスの設定を行った組織は、Cisco Secure ACS 2.4を使用すれば、システム管理者が何もなくても、そのデータベースを構築するために投入した投資や労力を活用できます。これによって同じ情報を持つ2つの異なるデータベースを構築する必要がなくなります。Cisco Secure ACS 2.4 for Windows NTは、Windows NT ユーザーデータベースですでに設定されているユーザー名とパスワードに対して、ユーザー名とパスワードを認証するように構成できます。

Cisco Secure ACS 2.4とWindows NT データベースを組み合わせることで、ネットワークセキュリティの管理が簡便化されます。Windows NTのユーザーマネージャ内からユーザーアクセスをさらに制御したい場合は、Cisco Secureが「ダイヤルインの許可を与える」のWindows NT 設定もチェックするように構成できます。このように構成すると、このパラメータが無効のユーザーに対しては、アクセスが許可されなくなります。

Windows NTユーザーデータベースを使用することには、認証に使用されるユーザー名とパスワードをネットワークログインに使用できる、という利点もあります。したがってユーザーは、ユーザー名とパスワードを一度入力するだけで済みます。

#### ルータ管理

ルータなどのネットワークデバイスにアクセスするユーザーを制御することは、管理上の懸念となってきています。多くのネットワークにはルータなどのデバイスが数百台から数千台も含まれており、ネットワーク管理者は1つ1つにアクセスする必要があります。これらに対する適切なアクセスを持つユーザーを制御することは、膨大な作業になります。Cisco Secureを利用すれば、これらすべてのデバイスに対するアクセスを集中制御できます。

Cisco SecureのCisco IOSソフトウェアへのリンクにより、Ciscoルータのアクセスポリシーを定義することが可能になります。ネットワーク管理者がログインやCisco IOSコマンドの使用を試みた際は、Cisco SecureにしたがってCiscoルータのAAAサービスを設定するようにできます。ルータ管理へのアクセスやCisco IOSコマンドに対しては、中央のサーバによって許可が行われるため、各ルータにパスワードを格納するよりも安全で管理しやすくスケーラブルなソリューションが実現します。

## VPN サービス

Cisco Secure ACS V.2.4 for Windows NTは、サービスプロバイダーと企業ユーザーのどちらでも、VPN (Virtual Private Network) サービスのトンネル情報や実際のユーザー検証機能を提供するコントロールサーバとして利用できます。

VPN ソリューションを使用するサービスプロバイダーは、企業が自身のACSを維持することでセキュリティの最終的制御を失わないで済む、優れたアウトソーシングソリューションを企業に提供することが可能になります。ACS管理は既存のWindows NTサポート構造のもとに置くことができるため、面倒な作業をする必要はありません。

Cisco Secureは、VPN トンネルの起点側終端 (VPN ユーザーがダイヤルインするサイトで、VPN トンネルの「NAS」終端とも呼ばれる) またはトンネルのエンドポイント (VPN トンネルを終端するプライベートネットワークで、「ホームゲートウェイ」とも呼ばれる) のどちらでも利用できます (図1参照)。

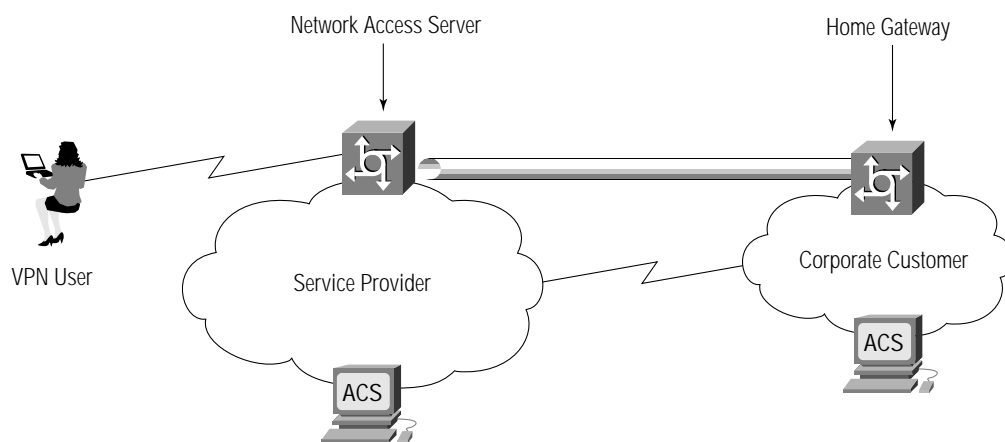
## Cisco IOS マルチシャシー・マルチリンク PPP 機能の拡張

大量のダイヤルアップアクセスサーバが導入されているアプリケーションに対して、シスコではスケーラブルなネットワークを構築するための機能をいくつか提供しており、Cisco Secure ACSがこれらの機能を最適化します。

複数のCiscoアクセスサーバが導入されているISDN環境では、一人のユーザーが2台の異なるアクセスサーバからBチャンネルを使用するという事態が起こる可能性があります。Cisco IOSソフトウェアはマルチシャシー・マルチリンクPPPという機能を使って、Bチャンネルをグループ化することができます。Cisco Secureでは、同じ場所から2つの接続に対して認証、権限認証、課金を行うことができます。このように、Cisco IOSソフトウェアとCisco Secureアプリケーションのパワフルな連携によって、優れた利点がもたらされます。

認証リクエストは、2台の異なるアクセスサーバから受信します。ただし、認証リクエストは中央ロケーション、つまりCisco Secure ACSに送信されて検証されるため、1つのリンクでは許可されてもう1つのリンクでは拒否された、というような事態は起こりません。さらに、Security Dynamicsのトークンカードを使用すると、Bチャンネルの到達するのが同じアクセスサーバであっても異なるアクセスサーバであっても、それに関係なくトークンキャッシング機能が提供されます。いずれの場合も、ACSによって、複数シャシーへの拡張を簡単に展開し管理することが可能になります。

図1：VPNのコンポーネント



## Cisco Secure ACS V.2.4 for Windows NT の機能と利点

機能	利点
Cisco IOSソフトウェアと密接に結合	Bチャネルに対するマルチシャシー・マルチリンクPPPでの認証と権限認証を提供 Cisco IOSコマンドの権限認証とロギングによるデバイス管理
HTML/Java Webインタフェース	使用が簡単 ネットワークのどこからでも管理可能
Windows NTと密接に統合	Windows NTに既存のユーザー名を認証に使用 Windows NTへのシングルログインを提供 パフォーマンスモニターなどのWindows NTツールを使ってリアルタイムで統計データを表示
VPNサポート	Cisco SecureはISPアクセスサーバにトンネル情報を提供することが可能 VPNトンネルの確立後、ユーザーの認証と権限認証をサポート
各種認証レベル	PAPによりWindows NTネットワークにシングルログインでダイヤルアップ接続可能 MS-CHAPによりMicrosoftダイヤルアップのセキュリティを提供 CHAPにより認証セキュリティを強化 AppleクライアントのためのARA
TACACS+およびRADIUSのサポート	多様なアクセス制御プロトコル(TACACS+, IETF RADIUS, Cisco RADIUS, およびRADIUS属性)をサポートする柔軟なソリューション
トークンカードのクライアントサポート	SDI, Safe Word, CryptoCard, およびAxent Technologiesトークンカードのクライアントとしてトークンサーバをサポート
時間によるアクセス制御	1日の特定の時間にユーザーがアクセス可能になるサービスを定義 ネットワークアクセスが許可される日時を制限することで、ネットワークのセキュリティを保護
サーバあたりのライセンス	無制限のユーザー数 無制限のポート数 無制限のデバイス数

## Cisco Secure ACS V.2.4 for Windows NT システム要件

最小ハードウェア要件	ソフトウェア要件
Intel Pentium 200-MHz PC または互換機	Microsoft Windows NTサーバ V.4.0
64 MB RAM(128を推奨)	Microsoft Internet Explorer V.3.02またはNetscape Navigator V.3.0
150 MBのハードドライブ空き容量	
CD-ROMドライブ	
800 x 600以上の画面解像度	

## Cisco IOS の要件

ネットワークデバイスではIOSリリース11.1以降が必要。ダウンロード可能なアクセス制御リストにはIOSリリース11.3以降が必要。

©2000 Cisco Systems, Inc. All rights reserved.

Cisco と Cisco Systems は商標です。Cisco のロゴは Cisco Systems, Inc. の登録商標です。

この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。

本仕様は予告なしに変更される場合があります。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

E-mail: [cnac@cisco.com](mailto:cnac@cisco.com)

〒100-0005 東京都千代田区丸の内3-2-3 富士ビルディング

TEL.03-5645-8856 FAX.03-5641-3523

お問い合わせ先