Q&A

Cisco Identity-Based Networking Services

シスコでは、Cisco Identity-Based Networking Services（ IBNS）ソリューションによって有線・無線 LAN アクセスのセキュリティを拡張しています。Cisco IBNS は、アクセス制御とユーザ プロファイルを組み合せて、階層化されたユーザの柔軟性と機動性を高めています。この組み合せによってネット ワーク接続、サービス、アプリケーションの安全性が拡張され、ユーザの生産性向上と運用コスト の削減が可能になります。

Q. Cisco IBNS とは何ですか。

A. Cisco Identity-Based Networking Services（IBNS）とは、IEEE 802.1X 標準に基づいて構築されている企業ネットワークへの物理アクセスと論理アクセスの安全性を高めるソリューションです。

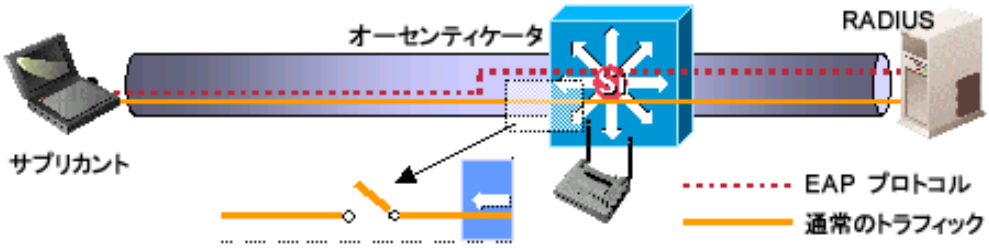
Cisco IBNS により、ユーザ レベルとポート レベルでの本格的な ID ベースのネットワーク アクセス制御の実装とポリシーの適用が可能になります。安全で信頼性の高い強力な認証テクノロジーを使用して、ユーザとデバイスの識別を行います。このソリューションは、識別したエンティティをポリシーに関連付けます。このポリシーは、管理者によって作成および管理が行われ、より詳細なアクセス制御を実現します。

Q. 802.1X とは何ですか。

A. IEEE 802.1X とは、ユーザ ID 単位またはデバイス単位でネットワーク クライアント（またはポート）の認証を行うための標準です。このプロセスは「ポートレベル認証」と呼ばれます。Remote Authentication Dial-In User Service（RADIUS）の方法論を利用し、それをサプリカント、オーセンティケータ、認証サーバという 3 つの個別のグループに分けています。

802.1X 標準は、ポートや Cisco CatalystR® スイッチ、Cisco AironetR® シリーズ アクセス ポイントなどのデバイス（オーセンティケータ）への接続を試みる終端装置とユーザ（サプリカント）に適用されます。Cisco Secure ACS などの認証サーバへのバックエンド通信により、認証と許可が行われます。IEEE 802.1X により、ユーザ識別の自動化、認証の一元化、キー管理、LAN 接続のプロビジョニングが実現されます。802.1X. の図については、図 1 を参照してください。

図 1：
802.1X



Q. 802.1X の利点は何ですか。

A. 従来、アクセス制御はネットワークのエッジで管理されていました。シスコでは、有線および無線の LAN スイッチと Cisco Secure ACS に 802.1X のサポートを追加して、LAN 内部に RADIUS ベースの Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）機能を提供しています。特に、802.1X と Cisco Secure ACS の組み合せには、以下の利点があります。

- Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）、トークン、スマートカード（また、将来的には指紋、声紋など）を使用した、強力な認証。これは、相互認証方式を使用しない限り不正なセキュリティ攻撃に対して脆弱な、無線 LAN 環境において特に効果的です。
- ユーザ クォータ単位、Virtual LAN（VLAN）単位などでの柔軟なポリシー割り当て。
- ユーザのアカウンティングおよび監査と、LAN 内部のユーザの行動を追跡しモニタする機能。

Q. Cisco IBNS は収益にどのような効果を与えますか。

A. Cisco IBNS は、ポートレベル セキュリティの集中管理によって、ネットワーク管理運用に必要な人員数を低減します。また、ユーザの機動性を高め、有線ネットワークおよび無線ネットワークにアクセスしやすくすることで、ユーザの生産性を高める効果があります。コストの節減と生産性の向上は、収益の増大につながります。

Q. Cisco IBNS はオープンな実装ですか。シスコの機器だけを使用して動作させる必要がありますか。

A. シスコの実装は、IEEE 802.1X 標準に準拠しており、互換性のあるすべての RADIUS サーバとクライアント（サプリカント）をサポートしています。ただし、シスコの拡張機能は、この Q & A に記載されているシスコ製品のみでサポートされます。

Q. Cisco IBNS には、今後も機能が追加されますか。

A. Cisco IBNS ソリューションは、標準またはお客様の要件の変化に適応し、その要件を満たします。現在は、数段階に及ぶ実装の初期の段階に相当します。

Q. 互換性のある認証サーバには、どのようなものがありますか。

A. Cisco IBNS ソリューションは、RADIUS および 802.1X の標準的な実装に準拠しています。この 2 つの標準に準拠したすべての IETF 認証サーバとの相互運用性があります。シスコでは Cisco Secure ACS を特に強化してきております。

Q. このサポートを利用するには、どのような変更が必要ですか。

A. ハードウェア インフラストラクチャの変更は必要ありません。ほとんどの場合、LAN アクセス デバイス（有線と無線）、スイッチ、クライアント ワークステーション、RADIUS サーバ上の各オペレーティング システム ソフトウェアをアップグレードする必要があるだけです。

Q. 802.1X ではどのようなタイプのセキュリティ ポリシーを適用できますか。

A. Cisco IBNS ソリューションには、ID に基づいてネットワーク アクセスの安全性を確保するポートベースの動的な認証のほかに、VLAN と ACL をユーザごとに動的に割り当てる機能があります。Cisco Secure ACS サーバには、以下の追加ポリシーがあります。

- 日時および曜日による制限
- NAS IP アドレスに基づいてユーザとスイッチを制限する、Network Access Server（NAS; ネットワーク アクセス サーバ）IP フィルタ
- デバイスの認証をデバイスの MAC アドレスに基づいて制限する、MAC アドレス フィルタリング
- ユーザごとの VLAN
- ユーザごとの ACL

Q. ユーザ アクセス プロファイルの管理には、どのような管理ツールがありますか。

A. Cisco Secure ACS は、ユーザと管理者のネットワーク アクセスの拡張に伴なう管理作業を大幅に軽減します。Cisco Secure ACS を利用すると、Web ベースのグラフィカル ユーザ インタフェースによって、すべてのユーザの AAA プロファイルを集中管理し、これらのプロファイルをネットワーク内の数千箇所のアクセス ポイントに配布することができます。また、アカウンティング サービスとして、ネットワーク内のユーザの行動の追跡と報告、すべてのリモート アクセス接続またはデバイスの設定変更の記録が可能になります。

Q. 複数のサイトがある場合、RADIUS サーバをどこに配置すればよいですか。

A. Cisco Secure ACS では、複数の RADIUS サーバを設定して、分散された環境に展開できます。これには、以下のような利点があります。

- リモート ACS サーバに対するプロキシ認証（ダイアルインによるリモートのモバイル アクセスの場合）
- NAS 間のクラスタ設定と ACS 上のデータベース複製機能を利用した、フェールオーバーと冗長性
- 集中型のリモート ロギング機能

Cisco Secure ACS をネットワーク内に配置する際のガイドラインは、次のサイトにある White Paper に要約されています。

http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/secre_wp.htm

Q. Cisco IBNS を実装した場合、Cisco ACS にはどのような負荷が加わりますか。

A. 主にバックエンドでの負荷が増加します。シスコでは、Windows 2000 および NT 向けの Cisco Secure ACS を Oracle や Sybase などの高性能のバックエンド データベースと連携させ、クラスタ方式で展開しています。このスケーラビリティは、ユーザ レコード数が数千件に及ぶお客様に適しております。

Cisco Secure ACS の詳細については、以下のサイトを参照してください。

http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/acs/index.shtml

Q. Cisco IBNS ソリューションに含まれている特定の製品についての詳細は、どこにありますか。

A. IBNS Solution の詳細については、Cisco Contact Center（シスココンタクトセンター）までお問い合せください。http://www.cisco.com/japanese/warp/public/3/jp/service/contactcenter/

各製品の詳細については、以下のサイトを参照してください。

Cisco Secure Access Control Server （ACS）

http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/acs/index.shtml

Cisco Aironet® シリーズ製品

http://www.cisco.com/japanese/warp/public/3/jp/product/hs/wireless/

Cisco Catalyst シリーズ スイッチ

http://www.cisco.com/japanese/warp/public/3/jp/product/hs/switches/

お問い合わせ先

シスコシステムズ株式会社

URL:http://www.cisco.com/jp/
問合せ URL: http://www.cisco.com/jp/service/contactcenter/
〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
TEL 03-6655-4433
電話でのお問合せは、以下の時間帯で受け付けております。
平日 10:00 ～ 12:00 および 13:00 ～ 17:00

02.06