Cisco Systems | Corporate Alliance

IBM

ソリューション

IBM とシスコが提供する Identity-Based Networking Service

IBM とシスコ：次世代の e-ビジネス ソリューション

概要：

- **ポート レベルのユーザ認証を行う場合の顧客アイデンティティ管理を簡易にする、Tivoli Identity Manager と Cisco Identity-Based Networking Service（IBNS）の統合**
- **すべての IT リソースにわたるセキュリティ アクセス ポリシーの自動化、監査、実施が可能な中央集中型のアイデンティティ管理を実現**
- **厳密にプロビジョニングされたアイデンティティベースのアクセスをスイッチ ポート レベルで提供**
- **ネットワーク リソースにアクセスしているユーザを動的に識別し、制御することが可能**

企業に対する脅威

競争の激しい現在の e-ビジネスで勝ち抜くために、各企業は自社の IT インフラストラクチャを活用し、IT 投資をネットワーク、システム、およびアプリケーションに拡張して、顧客、サプライヤ、およびビジネス パートナーとの接続を効率化しています。しかし、接続先が増えることには、非常に大きなメリットがあるだけでなく、相当のリスクが伴います。最近相次いでいるウィルス、ワーム、およびインターネット攻撃は、IT インフラストラクチャに多大な被害をもたらし、多くの企業の生産性を大幅に低下させています。これらの拡大する脅威に対処するために多くの予算を投入しているにもかかわらず、現行のセキュリティ機能はその課題を克服できるだけの発達を遂げていないのが実情です。

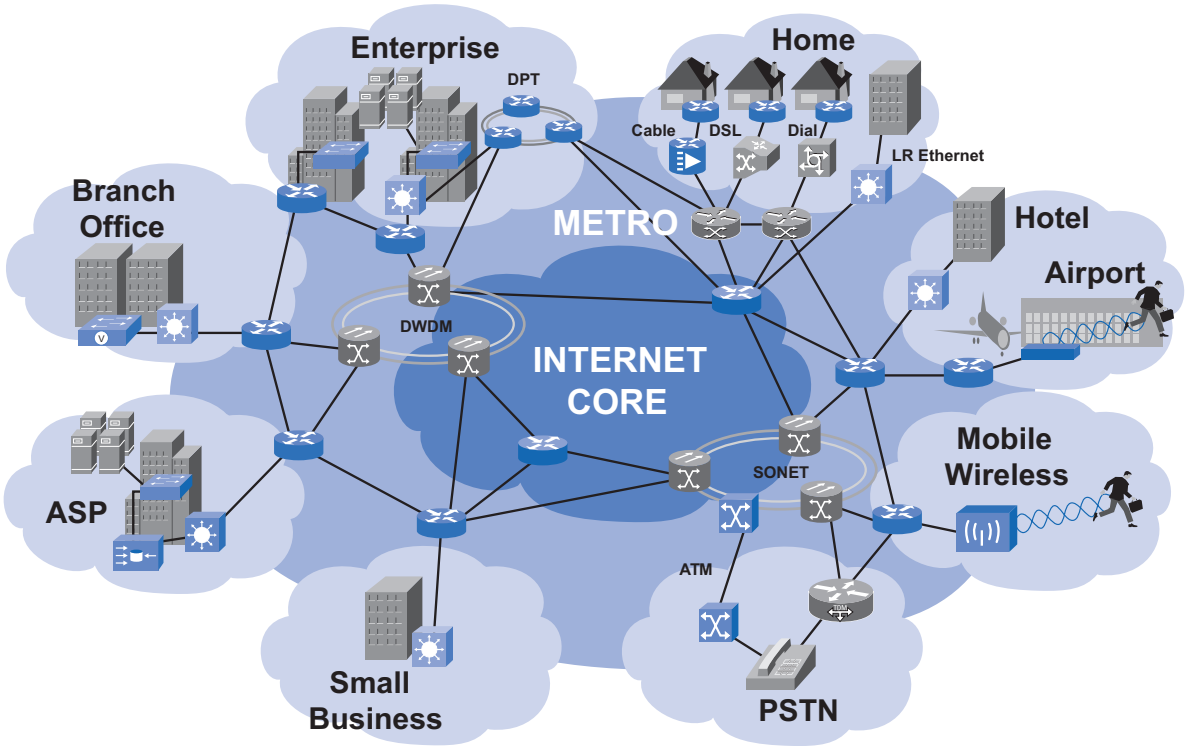
IBM とシスコシステムズは、2 つの重要な分野で、企業がこうしたセキュリティへの脅威に対処できるように支援しています。第 1 は、企業ネットワークに接続するユーザのアイデンティティを管理することであり、第 2 は、ネットワークに接続するデバイスの「健全性」を管理することです。企業ネットワークに接続する個人のアイデンティティを把握することによって、企業はそのユーザのアクセスをより効果的に管理できます。このソリューション概要では、ネットワーク経由で許可されていないユーザがリソースにアクセスできないようにするための技術を紹介します。

ユーザのアイデンティティ

現在のほとんどの企業では、企業ネットワークに接続する個人のアイデンティティを確認していません。ユーザが（有線または無線で）接続しようとすると、その際に TCP/IP アドレスが付与されます。そのため、このユーザのアクセスが許可されているか否かにかかわらず、企業内の保護されていない任意の情報にアクセスできるようになります。現在の最先端

機密情報へのアクセスは、それが**ビジネス パートナーや競合企業**の関与したものであれ、**単に職務上の必要性を超えたもの**であれ、**多くの企業**にとっての**脅威**となります。

図 1：ネットワークの拡大はセキュリティに影響を与える



の技術でも、証明書、最終的にはリソースへのアクセス管理は、重要性の高いアプリケーションに限定されています。これらのアプリケーションに関連するユーザ管理の多くは、IT スタッフにとって時間のかかる面倒な作業であるため、中央集中型のユーザ権限管理は行われてきませんでした。これでは、企業ネットワークに接続してしまえば、誰でも広範囲にわたる不正アクセスを実行できることになります（図 1 を参照）。

このように企業ネットワークへのアクセスを開放状態にしておくと、悪意があろうとなかろうと、企業のセキュリティにとって脅威となるユーザが出現する可能性があります。この問題は、オンデマンドのような新しいコンピューティングおよびビジネス モデルの需要によって大幅に増加しています。これらのモデルは、企業にアクセスするユーザ数の増加につながり、その中にはビジネス パートナーや臨時社員、さらには競合企業が含まれる場合もあるからです。企業のなかには、基本的なアイデンティティ インフラストラクチャを構築し、一部のアプリケーションへのアクセスを制限しているところもあります。しかし、多くの企業のコンピューティング インフラストラクチャ上にあるデータは、誰でも入手できる状態になっている可能性があります。

多様なネットワーク ユーザが多くの情報にアクセスできることには、さまざまな問題があります。機密情報へのアクセスは、それがビジネス パートナーや競合企業の関与したものであれ、単に職務上の必要性を超えたものであれ、多くの企業にとっての脅威となります。また、多くの人に企業ネットワークへのアクセスを許可することによって、無許可のユーザや悪意を持つユーザが、コンピューティング インフラストラクチャにアクセスできるようになる可能性が高くなります。無許可のユーザが大混乱を引き起こしたとしたら、それを企業では検出できないかもしれません。

ネットワーク アクセスのアイデンティティの確認

アイデンティティベースのネットワーキング

モバイル環境のおかげで、ユーザはさまざまな場所からネットワークに接続できるようになりました。しかし、現在のネットワークでは、リソースを要求しているユーザが誰であるかを確認できません。こうした脅威には、シスコのネットワー

ク アクセス デバイスとCisco Secure Access Control Server（ACS）を組み合わせることで対処できます。アクセス要求が行われると、ネットワークは、ネットワーク リソースを利用するための有効な証明書を提供するように要求します。

シスコでは、業界標準の 802.1X プロトコルを利用してこの機能を提供しています。このプロトコルでは、ネットワーク アクセスのためにアイデンティティを要求することができます。また、現在、一般的なエンド ポイント システムのほとんどでサポートされています。これは、無線アクセスのユーザ認証で一般的に使用されているものと同じプロトコルです。ネットワークに対して要求が発行されると、有効なユーザ アイデンティティが確立されるまで、その要求は完了されません。

エンド ポイントがネットワーク要求を発行すると、ユーザを確認してから、ネットワーク アクセス デバイスがその要求を承認します。ネットワーク アクセス デバイスは、エンド システムに対してアイデンティティを要求します。エンドシステムがアイデンティティを提供すると、この情報をネットワーク アクセス デバイスは Cisco Secure ACS に送信します。Cisco Secure ACS によってアイデンティティが確認され、有効なユーザであることが保証されると、Cisco Secure ACS からアクセス ポイントに対して、その要求を承認するように指示します。有効なユーザでなければ、その要求は拒否されます。

Cisco Secure ACS は、ネットワーク アクセスのポリシー定義ポイントです。そのため、Cisco Secure ACS には、ネットワークにアクセスする際にデバイスが提供する、有効なユーザと証明書についての情報がすべて格納されています。ネットワーク アクセス デバイスがユーザ認証要求を生成すると、Cisco Secure ACS は、このユーザが有効かどうかを確認して、必要な応答をアクセス デバイスに返します。

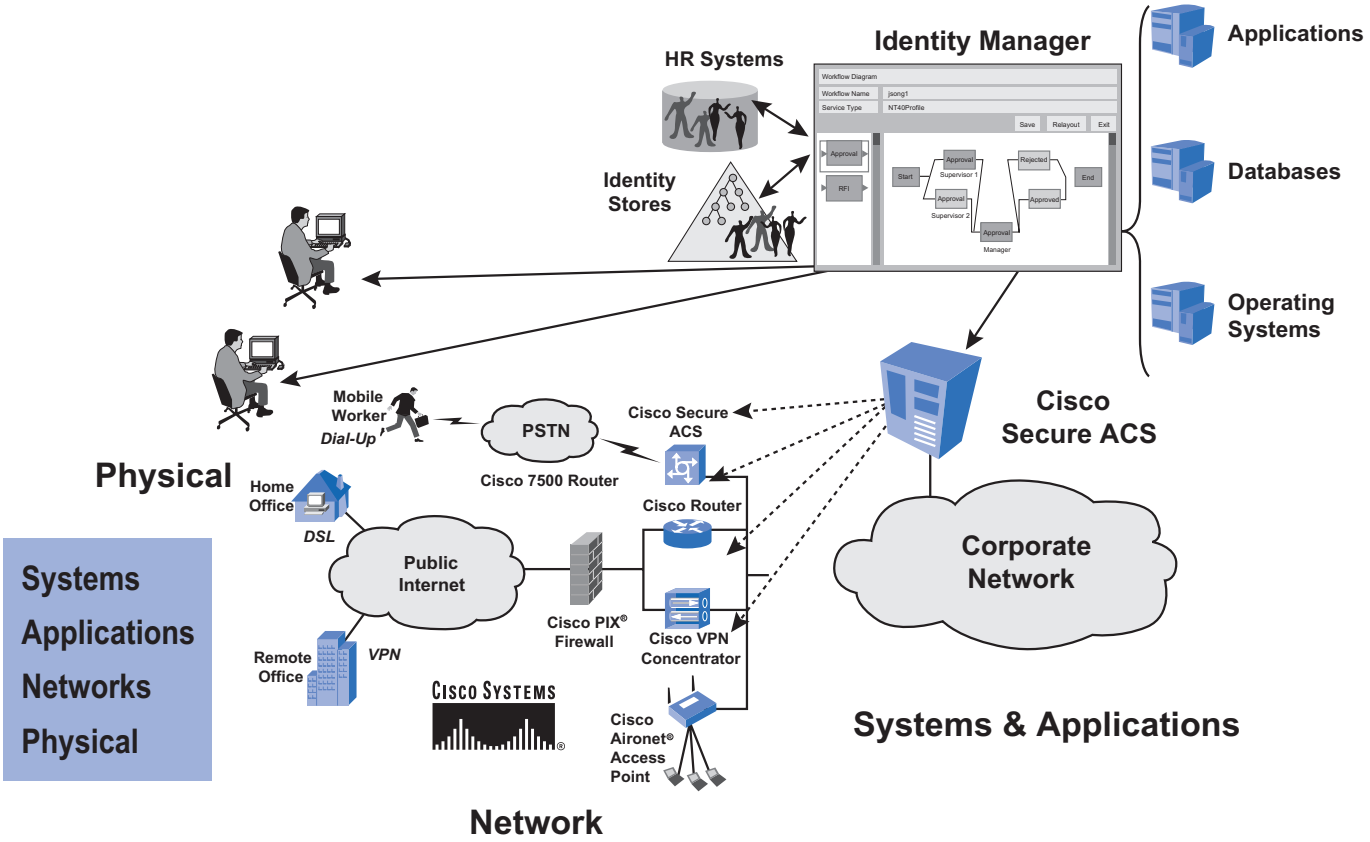
ユーザ アクセスを規制するための階層型のアプローチは、企業で利用される最良の方式の 1 つです。リソースに対するアクセスを効果的に管理しようとしている企業のアーキテクチャを考えた場合、アクセスの規制は多層化する必要があります。IBM とシスコでは、強固な階層型の規制機能を提供しています。Cisco Secure ACS とネットワークの階層は、未知のユーザをネットワークから排除する第 1 の防御ラインです。アクセス制御のための次の階層は、Web アプリケーションへのアクセスを管理する Tivoli Access Manager、Cisco Security Agent などのエンド ポイント侵入防御システム、Resource Access Control Facility（RACF）が稼働している z/OS のようなオペレーティング システムによるアクセス制御、アプリケーション特有のアクセス機能などによって提供されます。こうしたアクセス制御では、さらに精密にデータ テーブル内の特定の行へのアクセスを規制したり、プライバシー条件に応じてデータと要求者とを関連付けたりすることもできます。

ユーザ集団の管理

ネットワーク レベルのアイデンティティ モデルに必要とされるユーザ数を実装し、保守するために、企業には強固な管理ソリューションが必要です。企業へのアクセスを許可されているユーザとそれらのユーザが企業内で持つ権限との関係を保守し、インフラストラクチャの「規制」部門としての機能を維持することは、管理上、非常に大きな問題となります。Tivoli Identity Manager に加えて、シスコのアイデンティティベースのネットワーキングを使って実現される統合化を活用することで、この環境の管理が容易になります。また、物理的セキュリティ製品（バッジ リーダー、スマート カード、デジタル ビデオ監視）との統合によって、この「論理的アクセス管理」を物理環境にまで拡張できます。

このプロセスは、従業員データベースのような、企業が保持している信頼性のあるユーザ情報源から始まります。このデータベースには、企業内での権限を持っている個人が登録されています。そのほか、パートナーや顧客などを登録したリレーションシップ マネジメント システムのような「信頼性のある」情報源が存在する場合もあります。これらのシステムには、所属部門、職責、役職など、ユーザに関する有用な情報が格納されています。Tivoli Identity Manager には、これらのアプリケーションに対応した XML インターフェイスが用意されており、変更をインポートすることで企業の規制エンジンをアップデートできます。これらの信頼性のある情報源から提供される情報は、個人のアクセス権限を特定するために使用されます。各ユーザに与えるアクセス権限は、リソースへのアクセスを定義された企業のポリシーに適合している必要があります。これらのポリシーによって、アクセス確立、ネットワーク アクセス（通過を許可されるサブネットを含む）、およびアクセス可能なアプリケーションとデータに関する権限が決定されます。これらのアクセス領域は、信頼性のある情報源の属性設定に基づいて変化します（図 2 を参照）。

図 2：ユーザ プロビジョニング システム、アプリケーション、ネットワーク、および物理的アクセスの統合



このプロセスを機能させるためのカギは、アイデンティティ ソリューションの自動化にあります。ユーザ アイデンティティの変更に伴うビジネス プロセスの自動化は、ライフサイクル管理と呼ばれています。企業のセキュリティを確保するうえで特に重要なのは、必要のなくなったユーザ権限を削除することです。これは、企業のセキュリティおよびリスク管理のための主要な属性となります。アイデンティティ ソリューションには、サービス開始までの経過時間の短縮、定型管理作業の自動化、エラーの解消といった効果があります。ユーザが自分のアクセスを部分的に管理できるインターフェイスが用意されていることも、システム全体を向上させます。さらに、企業ネットワークを管理する立場であれば、企業を組織的に捉え、自分に与えられた変更にすばやく対応できます。IBNS の場合、ネットワーク トポロジーに対するアクセスの権限レベルを管理することが重要です。また、ダイナミックなビジネス状況では、アクセス ベースでの権限が常に変更されます。この変更は、企業全体で効率的かつ効果的に伝達される必要があります。

個人の権限を決定する場合、Tivoli Identity Manager によって、ユーザが適切な規制ポイントにプロビジョニングされます。これらの規制ポイントには、バッジ リーダー、ネットワーク（Cisco Secure ACS 経由）、Web アプリケーション（Tivoli Access Manager 経由）、オペレーティング システム、またはアプリケーション（従来のメカニズム）などがあります。

Tivoli Identity Manager には、これらのアクセス権限を管理する機能が用意されています。企業は迅速な対応を必要としますが、資産を保護するには、適切な管理機能を備えることも必要です。これらの管理機能には、終了させる必要のあるアクセスを回収するプロセスの自動化などがあります。企業が重要性の高いリソースへのアクセスを適切に提供するには、(1) 安全なリソースの所有者に対する承認要求に関連するワークフロー、および (2) 制御レベルを提供するメカニズムが必要です。また、ポリシーに含まれなくなったアカウントを削除または停止することにより、ネットワークやアプリケーションへの不正アクセスが発生しないようにすることも重要です。Tivoli Identity Manager は、ユーザ アクセスのポリシーと実際

のアクセスとの間の不一致を常に判定できる調整機能を提供します。ほとんどのお客様は、この機能を週 1 回といった定期的なスケジュールで実行しています。

IBNS 構成の管理をネットワーク チームに委譲する機能は、ネットワーク チームが独立してネットワーク トポロジーを管理している多くの企業では主要なコンポーネントとなります。この委譲機能により、中央集中型の管理とローカルでの自律的管理が維持されるので、機密システムに関するセキュリティと一貫性のあるポリシーを保証できます。さらにネットワーク チームは、引き続きネットワークの重要なトポロジーと特性を十分に把握できます。

リモート アクセスが定常的に発生するわけではない大規模環境では、自己メンテナンス機能の提供はきわめて重要です。パスワードを忘れたユーザがアクセスを取り戻すために使うツールも、わかりやすくなっている必要があります。ユーザの母親の旧姓などのデータをユーザ ID とともに提供するか、場合によっては第 3 の認証方法を用意します。この機能によって、ヘルプデスクの負荷が減少し、リソースをより重要性の高い作業に利用できます。

ネットワークへの汎用化されたアクセスを提供すると、多くの場合、政府による個人情報保護のための規則や規制に違反することになります。こうした規則や規制の多くは、プロセスに関係したものであり、アクセスの承認に使用される方式を対象としています。監査は、適合性を検証したり、企業が必要としている制御機能を保証したりするために実行されます。導入されるインフラストラクチャは、正確なレポート機能を提供し、内部および外部監査に対応する必要があります。Tivoli Identity Manager では、幅広い監査機能とレポート ツールを利用できます。これを使用すれば、ネットワークとアプリケーションについて、ユーザのアクセス権限に関連するレポートを生成できます。

つまり管理インフラストラクチャでは、高レベルのセキュリティの提供に伴うコストを抑える必要があり、それは IBNS アプローチによって実現できるのです。これらのセキュリティ措置によって、企業は不正アクセスから保護されます。これらのツールは、変化するビジネス ニーズに対応できると同時に、規制およびビジネス プロセスの管理に必要とされる監査機能を備えている必要があります。

ソリューションのコンポーネント

シスコ製品

Cisco Catalyst® スイッチ（Catalyst 6500、4500、3550、2950 スイッチなど）
Cisco Secure Access Control Server
Cisco Aironet® アクセス ポイント

IBM 製品

IBM Tivoli Identity Manager
ソリューションには、以下が含まれる場合もあります。
IBM Tivoli Access Manager for e-business
IBM Tivoli Directory Integrator
IBM Tivoli Directory Server
IBM WebSphere® Portal
IBM WebSphere
IBM @server

世界最高級のサービスを保証

円滑な実装を保証するため、IBM グローバル サービスは、お客様と共同でセキュリティ ポリシーとアクセス制御要件を定義し、定義済みの適合性および改善ポリシーに基づいてソリューションを設計および計画し、統合されたアイデンティティ ソリューションの導入とテストを行います。これには、ビジネスおよびシステム コンサルティング、設計、プロジェクト管理、調達、およびケーブル配線などが含まれます。

世界有数のサービス プロバイダーである IBM グローバル サービスは、ユーザ管理プロセス プロジェクトの実装を成功させるため、IT、ネットワーキング、セキュリティ、およびアイデンティティ管理技術を提供します。このような技術を提供できるのは、あらゆる規模のユーザへのソリューション導入という、長年にわたるコンサルティングおよび展開の実績があるからです。IBM グローバル サービスは、ユーザ ライフサイクル管理に関連したテクノロジーを備えた技術的およびプロセス上の手法を発展させてきました。この経験をユーザ管理プロジェクトに適用すれば、実施を迅速化し、プロジェクトのリスクを管理できます。

コンサルティング、プランニング、設計から、統合およびテストに至るまで、IBM グローバル サービスは、アイデンティティベースのネットワーキング管理に対応したエンドツーエンドのサービス ソリューションを提供できます。IBM グローバル サービスのビジネスおよび技術コンサルタントは、業界での幅広い経験と確かな実績を持っており、ユーザが業務で果たす重要な役割を理解しています。

アイデンティティベースのネットワーキング管理に関する IBM とシスコの共同作業についての詳細は、次の URL をご覧ください。

www.cisco.com/go/ibm
www.cisco.com/en/US/products/sw/conntsw/index.html
www.ibm.com/security/cisco
www.ibm.com/websphere
www.ibm.com/tivoli
www.ibm.com/security
www.ibm.com/software

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
www.cisco.com/go/ibm

IBM Global Services
Route 100
Somers, NY 10589
www.ibm.com/security/cisco

Copyright © 2005 IBM Corporation. All rights reserved.

IBM, the IBM logo, the e-business logo, the eServer logo, Tivoli and WebSphere are trademarks or registered trademarks of International Business Machines Corporation or Tivoli Systems, Inc. in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates or for an unlimited period of time. IBM reserves the right to alter product offerings, prices and specifications at any time, without notice.

Aironet, Catalyst, Cisco, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

MD/09/04
Inv. #956464