Cisco Systems | Corporate Alliance

IBM

企業に接続するユーザとデバイスを管理し、
セキュリティを最大限に強化

WHITE PAPER

セキュリティ確保には信頼できるプロバイダーの統合型リソースが不可欠

リビジョン 1
2004 年 10 月

目次

概要

競争の激しい現在のオンデマンド ビジネスで勝ち抜くために、各企業はネットワーク、システム、およびアプリケーションへの IT 投資を活用して、顧客、サプライヤ、およびパートナーとの接続を効率化しています。IT インフラストラクチャの多くの部分に接続できるユーザや企業が増加することは、非常に大きな利益をもたらす一方で、それに対応するリスクをも生み出す可能性があります。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、企業の生産性を大幅に低下させています。企業は、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する必要がありますが、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。

電子的な脅威に対処することに加えて、企業は現在、2005 年 4 月に施行される「個人情報保護法」など、業界および政府のさまざまな規制に準拠する必要があります。さらに企業によっては、コンプライアンス イニシアチブを利用して、主要なプロセスを自動化することで既存の IT 運用における品質の合理化と最適化を行っています。

この資料では、セキュリティおよび規制上の脅威に取り組む企業のために、IBM とシスコシステムズが支援できる以下の 2 つの主要分野について説明します。

- 企業に接続するユーザのアイデンティティの管理 — 企業は、アイデンティティ管理を実装することによって、有効な ID を持たないユーザが企業ネットワークに接続することを防止できます。さらに企業は、企業の内部および外部での役割に基づいて、個人別にさまざまなレベルのアクセス制御を実施できます。

- ネットワークに接続するデバイスの、セキュリティに関する脆弱性とポリシー違反の監視― ネットワークに接続するデバイスへのセキュリティ適合性要件を定義することによって、企業は不正な、または感染したデバイスからの脅威を抑制しやすくなります。たとえば、OS（オペレーティング システム）のパッチ レベル、ウィルス対策、または Cisco Security Agent を備えていないデバイスを隔離することが可能です。さらに企業は、デバイスがセキュアなネットワークにアクセスするための要件を満たせるようにする修正手順を確立できます。

アイデンティティ管理とセキュリティ適合性の両方でポリシーベースのシステムを確立すれば、企業は多数のシステムおよびユーザにわたって一貫した方法でセキュリティを管理できます。さらに、ポリシーベースのセキュリティ ソリューションを確立すれば、企業はポリシーの実施を自動化し、それらのポリシーを迅速に変更できます。既存の IT システムは、企業のビジネス プライオリティをより高速かつ安全にサポートでき、監査要件への適合にも役立ちます。

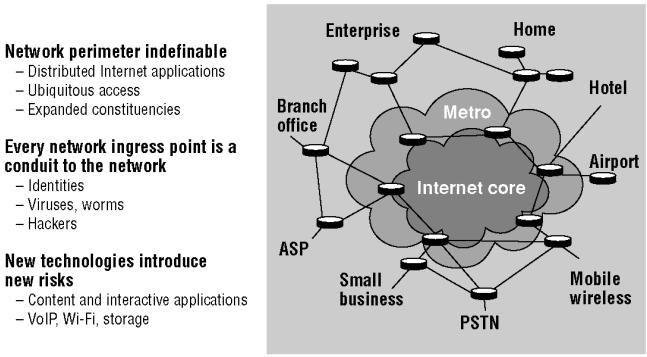
ユーザ アイデンティティ情報の不足がセキュリティへの脅威となる可能性

現在、多くの企業では、自社のネットワークに接続する各人のアイデンティティを確認していません。個人は、有線または無線接続を確立する際、TCP/IP アドレスを付与されます。これによって、誰もが（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ます。このように広くアクセスを開放すると、内外のユーザに対して企業資産のセキュリティ上の脆弱性が露出することになります。悪意の有無に関係なく、これらのユーザが情報の機密性を脅かし、そのうえそれを検出できない場合があります。

この問題は、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。たとえば、IBM のオンデマンド ビジネス イニシアチブでは、企業は効率を高め、収益を生み出す新事業を推進するため、（パートナー、契約社員、ときには競合企業との接続を含めて）きわめて幅広い接続を可能にしています。企業は、機密情報をパートナーや競合企業とやりとりする場合、その情報（およびその他の内部情報）をネットワークにアクセスできる他のユーザから保護する責任があります。

従来のアイデンティティ インフラストラクチャでは、企業は特定のアプリケーションへのアクセスをユーザごとに制限できるものの、データの多くは誰でも入手できる状態にあります。証明書およびリソースへの最終的なアクセスの管理は、個々のアプリケーションによって処理されるため、ユーザ権限の管理は、ほとんどの IT スタッフにとって時間のかかる面倒な作業であり、重要性の高いアプリケーションだけに限定されて実施されていました。多くの企業では、自社のネットワークに接続しているユーザのアクセスを適切に制限できる、自動化された中央集中型のユーザ権限管理は行われていません。

図 1 戦略的ソリューション ― Identity-Based Networking Services



デバイスのセキュリティ適合性はもう 1 つの課題

デバイスのセキュリティ適合性はもう 1 つの課題

ネットワーク アクセスに使用されるデバイス（携帯電話、PDA、ラップトップ、デスクトップ、サーバなど）は、すべて異なるソフトウェアが実行されており、企業のセキュリティ確保を複雑化させる要因となっています。企業では、不正デバイス（企業の管理外にあるデバイス）から十分に把握されているサーバまで、多様なデバイスを管理する必要があります。デバイスがセキュリティ モデルの弱点となるシナリオには、以下のような例があります。

- 未知の属性を持つ不正デバイスは、ネットワークにアクセスする際、制限を受けない他のユーザに偽装する可能性がある。
- 既知のデバイスに最新のセキュリティ アップデートが適用されていない場合、ネットワーク上で信頼のおけるデバイスとして機能しない場合がある。

各デバイスのアイデンティティと状態を確認することによって、企業はネットワークに対するデバイスの関係を管理でき、デバイスのセキュリティ上の脆弱性とポリシー違反に基づいてアクセスを制限できます。

不正デバイス（企業の管理外にあるデバイス）は、大きなセキュリティ リスクとなる可能性があります。プリンタのように一定の機能しか持たないデバイスは、企業に損害を与える可能性がないため、ネットワークに参加できます。しかし、他の「より利口な」デバイスは、ネットワークに接続するためには最新の状態を提示する必要があり、定義済みのセキュリティ ポリシーに適合しない場合はアクセス制限を受けることになります。これらのデバイスの多くは、ベンダーや訪問者のデバイスのように、実際には適正である場合もありますが、ネットワーク アクセスは制限する必要があります。

急速に変化する今日のビジネス環境で新しい脅威に対処するには、製品とシグニチャの両方に対して、セキュリティ アップデートを常に利用できるようにしておく必要があります。企業から分断されているデバイス（出張中に使用されるデバイスなど）や、企業のアップデート要件に注意を払わない個人は、悪意のある攻撃の格好の標的となります。したがって企業は、事前にこれらの脅威に対処し、特定されたセキュリティ上の脆弱性とポリシー違反に対応できるまで、これらのデバイスをセキュアなネットワークから隔離する必要があります。

デバイスがますます複雑になり、企業の安全な境界の外にまで移動するようになるにつれて、デバイスのアイデンティティを確認することはますます困難になります。より高レベルのセキュリティを達成するため、企業はハードウェアベースのテクノロジーを採用し、デバイスのアイデンティティをより正確に確認できるようにしています。

ポリシーベースのアプローチを実装したユーザ アイデンティティとデバイスの管理

ユーザ アイデンティティの管理とデバイス設定の管理では、企業で管理する必要のあるデータおよびリソースの種類と量が増加しているので、手動によるソリューションは現実的ではありません。管理者には、一貫性のあるコスト効率の高い方法で、ユーザおよびデバイスの権限のあらゆる組み合わせを適用したり、保守したりする時間はありません。

企業ネットワークには、一貫性をもって実施される一連のアクセス権限ポリシーを定義する機能が必要です。個々のユーザまたはデバイスに変更が発生した場合、ポリシーをすばやく適用し、該当するアクセス権限を付与したり、剥奪したりしなければなりません。また、ポリシーに変更が発生した場合は、影響を受けるすべてのユーザおよびデバイスに変更したポリシーを適用する必要があります。

ネットワーク アクセスを要求するアイデンティティの確認

そうしたポリシーベースのセキュリティ インフラストラクチャを構築する場合、企業には、管理者が非常に効率よくビジネス ポリシーを作成および変更できるようなツールが必要です。さらに、ポリシーへの変更を自動的に実行および適用することによって管理者の負荷を減らし、正確さを高められるようなソリューションが必要です。

この資料の残りの各セクションでは、企業において IBM とシスコのソリューションを組み合わせ、ポリシーベースのセキュリティ ソリューションを実装する方法を説明します。

- まず、IBM とシスコのソリューションによって企業がアイデンティティベースのネットワーキングを実装し、ユーザ アイデンティティとアクセス ポリシーの両方を管理する方法を説明します。
- 次に、企業が IBM とシスコのソリューションを展開してデバイスのセキュリティ適合性をチェックし、デバイスのセキュリティ適合性ポリシーを管理し、安全ではないデバイスを修正する方法を検討します。
- 最後に、企業で効果的なセキュリティ ソリューションを確立するために現在使用できる、主要なハードウェアおよびソフトウェア コンポーネントを簡単に説明します。

ネットワーク アクセスを要求するアイデンティティの確認

階層型または多層型のアプローチは、リソースへのユーザ アクセスを効果的に管理しようとする企業にとって、ベスト プラクティスとなる場合があります。IBM とシスコは、一連の安定した階層型の実施機能を提供します。第 1 の防御ラインは、Cisco Secure Access Control Server（Cisco Secure ACS）とネットワーク層によって構成されます。これらは、企業が未知のユーザを自社ネットワークから排除するのに役立ちます。

現在のモバイル環境では、ネットワークに接続する個人は、さまざまな場所から接続してきます。シスコのネットワーク アクセス デバイスを Cisco Secure ACS と組み合わせて使用することによって、企業は、この問題に対処する手段を実装できます。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 リソースの利用を許可する前に、そのユーザに対して有効な証明書を提供するように要求します。

シスコのソリューションを使用すれば、企業は、業界標準の 802.1X プロトコルを利用できます。これは、ネットワーク アクセス要求に対応してアイデンティティの確認を行うように設計されています。現在、ほとんどの一般的なエンド ポイント システムでこの機能がサポートされています。たとえば、802.1X は無線アクセスの場合のユーザ認証で最も一般的に使用されるプロトコルです。

エンド ポイントによってネットワーク要求が発行された場合、その要求を承認する前に、ネットワーク アクセス デバイスはそのエンド システムに対して確認のために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、ネットワーク アクセス デバイスはそのアイデンティティ情報を確認のために Cisco Secure ACS へと送信します。そのユーザが有効であれば、Cisco Secure ACS はネットワーク アクセス デバイスに対して要求を承認するように指示します。有効でなければ、ネットワーク アクセス デバイスはその要求を拒否します。

Cisco Secure ACS には、デバイスがネットワークにアクセスする際に提供する必要のある有効なユーザと証明書がすべて格納されており、ネットワーク アクセス ポリシーを定義するポイントとして機能します。次の 2 つのセクション、「ユーザ集団の管理」と「自動化を利用してアクセス権限に影響を与える急速な変化を管理」では、企業が強固なネットワーク アクセス ポリシーを定義して実施することにより、ユーザ管理の課題に対処するうえで、IBM とシスコのソリューションがいかに役立つかを詳細に説明します。

ネットワーク層のあとは、その他のアクセス制御レイヤによって、企業は以下のようにアプリケーション、OS、およびデータへのアクセスをより精密に制御できます。

- IBM Tivoli® Access Manager を使用して Web アプリケーションへのアクセスを管理する。
- Remote Access Control Facility（RACF®）によって提供される IBM z/OS® の安定した機能を利用して、OS 固有のアクセス制御を確立する。
- 主要な OS 上で実行される重要性の高いアプリケーションに固有のアクセス制御を実施する。たとえば、企業がプライバシー要件に対応できるように、IBM ソリューションでは、企業はデータ テーブル内の特定の行にのみアクセスを許可したり、データと要求者の間に関連性がある場合にのみデータを公表したりできる。

ユーザ集団の管理

ネットワーク ユーザ数の増加には、さまざまなアクセス権限の増加と実施インフラストラクチャの規模の拡大が伴うため、ネットワークレベルのアイデンティティ モデルを実装し、保守するには、企業は安定した管理ソリューションを実装する必要があります。主要なアイデンティティ管理ソリューションの 1 つである IBM Tivoli Identity Manager を使用すれば、企業は、Cisco Identity-Based Networking Service（IBNS）との統合を利用して、ネットワークレベルのアイデンティティ環境の展開を自動化できます。

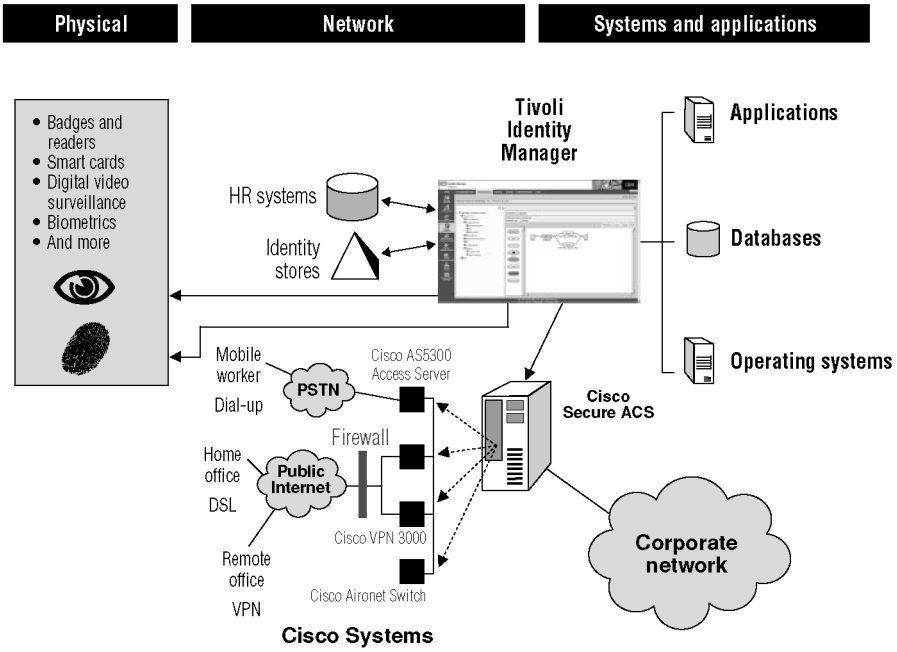
IBM のソリューションは、企業が物理的セキュリティ製品（バッジ リーダー、スマート カード、デジタル ビデオ監視など）を導入しやすい設計となっています。管理は、アプリケーションや OS のような論理的エンティティのアクセス管理から、物理環境のアクセス管理へと拡張できるので、エンドツーエンドのセキュリティを実現できます。

アイデンティティ管理は、企業内で権限を持っている社員を定義する人材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。パートナー、顧客、その他のグループに関する信頼性のある情報は、リレーションシップ管理システムのような、ほかの情報源に格納されている場合もあります。これらすべてのシステムには、所属部門、職責、役職など、ユーザに関する情報が格納されています。Tivoli Identity Manager には、ユーザ情報源に対応した XML インターフェイスが用意されており、変更をインポートして企業のポリシー実施エンジンをアップデートするために使用できます。

Tivoli Identity Manager を導入している企業では、これらの情報源から提供される情報を使用し、企業がリソース アクセス用に定義したポリシーに基づいて、各個人のアクセス権限を決定します。ポリシーによって、物理的な建物、ネットワークとサブネット（特に IBNS の場合に重要）、アプリケーション、およびデータへのアクセス権限を決定できます。個人の権限が決定されると、Tivoli Identity Manager によって、ユーザは以下のような適切な実施ポイントにプロビジョニングされます。

- バッジ リーダー
- ネットワーク（Cisco Secure ACS を使用）
- Web アプリケーション（IBM Tivoli Access Manager for e-Business を使用）
- OS
- アプリケーション（従来のメカニズムを使用）

図 2 セキュリティ ソリューションの全体構造



自動化を利用してアクセス権限に影響を与える急速な変化を管理

自動化を利用してアクセス権限に影響を与える急速な変化を管理

ビジネス条件が急速に変化する場合は、アクセスベースで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。個人の属性が情報源で変更される場合（またはアクセス ポリシーが変更される場合）は、その個人がアクセスできる範囲を動的に変更する必要があります。たとえば、必要がなくなった場合にユーザ権限を剥奪または停止することは、ネットワークやアプリケーションへの不正アクセスを抑制するうえで特に重要です。

ユーザ アイデンティティが変更される場合に適切なビジネス プロセスを正確に実行することは、ライフサイクル管理と呼ばれています。効果的なライフサイクル管理のカギは自動化です。Tivoli Identity Manager は、自動化されたアイデンティティ管理ソリューションであり、企業が以下を最小限に抑えるのに役立ちます。

- 権限の有効化 / 無効化にかかる経過時間
- 管理者が定型作業に使う時間
- アクセス権限のプロビジョニングにおけるエラー

Tivoli Identity Manager の自動化機能によって、企業は、資産保護に必要な管理能力を損なうことなく変更に対応できます。たとえば、企業は、アクセスに必要な承認を手動で取得するプロセスを自動化できます。Tivoli Identity Manager によって、企業は、承認要求をセキュアなリソースの「所有者」に送信するためのワークフローを確立しやすくなり、さらにそれらのワークフローを企業のポリシーに基づいて自動的に実行できます。

そのうえ、Tivoli Identity Manager は、ユーザ アクセス ポリシーと承認される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。この機能をスケジューリングして（たとえば週 1 回）実行することによって、企業は、アクセス権限の変更への対応を、設定するビジネス ポリシーと整合させることができます。

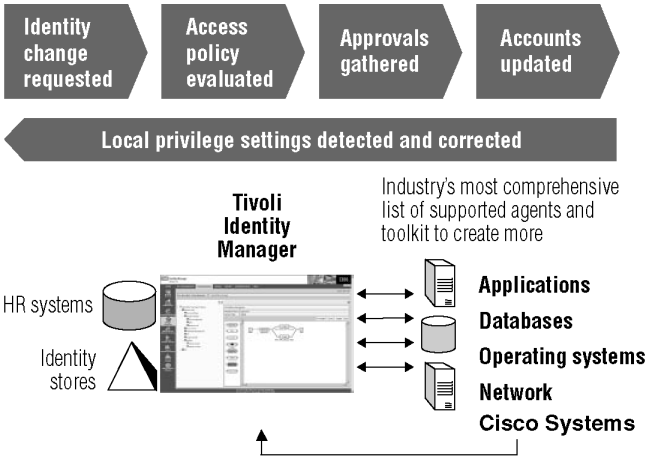
管理、自己修復、および法規制への準拠の委譲

Tivoli Identity Manager によって、ユーザ アイデンティティ情報とビジネス ポリシーの変更への対応が自動化されるので、これらの定型管理作業による管理者への負荷は軽減されます。IBM のソリューションによって、管理者は以下の作業負荷も最小限に抑えられます。

- 企業全体で他者が管理する必要のあるセキュリティ データおよびポリシーの管理
- パスワード要求への対応
- 監査および規制上の要件への準拠

多くの企業では、ネットワーク チームが独立しており、ネットワーク トポロジーの管理を行っています。そうした企業では、Tivoli Identity Manager によって、IBNS 構成の細部の管理作業をネットワーク チームに委譲することが可能です。このソリューションによって、企業は中央集中型の管理を維持しながら、ローカルでの自律的な運用が可能です。これにより、機密システムにおいてセキュリティと一貫性のあるポリシーを推進できます。さらに、ネットワーク チームは、Tivoli Identity Manager によってネットワークのトポロジーと特性を完全に把握できるので、ネットワーク アクセス ポリシーを細かく調整できます。

図 3 アイデンティティ管理ソリューションの構造



自己修復機能の提供は、自分のパスワードを頻繁に使用しないユーザがいる大規模環境では、きわめて重要です。Tivoli Identity Manager によって、ユーザは、パスワードを忘れた場合でも個人データの一部、ユーザ ID、および（場合によっては）第 3 の認証手段を提供することでアクセスを回復できます。この機能によって、企業はヘルプデスクの負荷を最小限に抑えて、リソースをより重要性の高い作業に振り分けることができます。さらに、自己修復機能を使用するユーザは、自分のアクセス権限に影響を与える変更にすばやく対処できます。

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。企業は、これを使用してネットワークおよびアプリケーション ユーザのアクセス権限に関連するレポートを作成できます。正確なレポートを作成することによって、企業は内部および外部の監査への準拠を示すことができます。要約すると、IBM とシスコのソリューションを利用したポリシーベースの自動アイデンティティ管理インフラストラクチャを導入した場合、企業では以下のことが可能になります。

- IBNS アプローチによって高レベルのセキュリティを提供することに伴うコストを最小限に抑える。
- 内部および外部の脅威に対するネットワーク、OS、およびアプリケーションのセキュリティを最大限に高める。
- ビジネスの変化するニーズに対応する。
- 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を提供する。

デバイス接続のセキュリティ適合性ポリシーの定義

この資料の冒頭で説明したように、セキュリティ管理の他の主要なカテゴリは、デバイスに関係するものです。不正デバイス、またはセキュリティ上の脆弱性やポリシー違反に対応できていないデバイスからネットワークを保護するためには、デバイスの特性を把握する手段が必要です。エンド ポイント（任意のデバイス）が企業に接続する場合、その企業では、以下のようなセキュリティ適合性基準を評価できる必要があります。

- OS のレベル
- パッチ レベル
- ウィルス対策ソフトウェアのレベル
- 動作ベースの侵入防止機能
- デバイスおよび企業を保護する構成設定値

デバイス接続のセキュリティ適合性ポリシーの定義

アクセス要求を発行するデバイスを評価するため、企業では、まず各クラスのデバイスについてポリシーを定義します。このポリシーは、企業が受け入れるリスクに対応したものです。次に企業は、そのポリシーを企業内のデバイスに伝達し、各デバイスでセキュリティ適合性をチェックできるようにします。

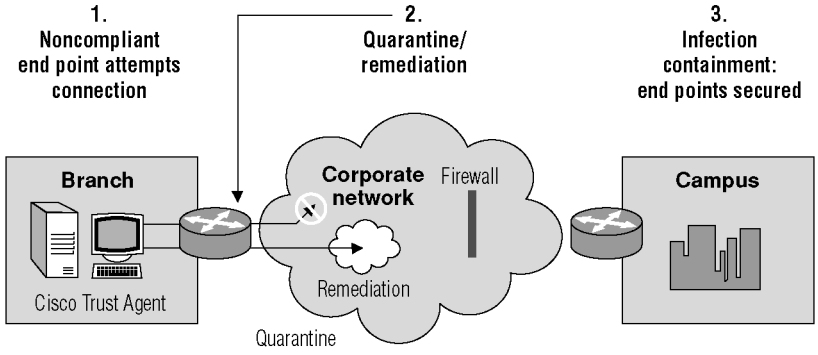
最後に、ネットワークでセキュリティ ポリシーを実施する必要があります。デバイスをネットワークから除去するだけでは十分ではありません。企業はクローズドループ プロセスを実行して、デバイスがセキュアなネットワークから隔離された原因を評価し、さらに必要な修正措置を適用する必要があります。この包括的プロセスによってのみ、隔離されたデバイスはセキュアな環境に復帰でき、それによってユーザの生産性を回復できます。

シスコは、ネットワークに接続するデバイスから企業を保護するセキュリティ基準を定義し、実施することを支援するため、Network Admission Control（NAC）ソリューションを開発しました。シスコが開発したメカニズムでは、デバイスの特性を伝達し、そのデバイスのネットワーク アクセス許可の是非を判定できるように、ネットワーク層の EAP プロトコルがレイヤ 2（EAP over 802.1X）およびレイヤ 3（EAP over UDP）に拡張されています。次に、ネットワーク アクセス デバイスは、デバイスに対して現在の状態の問い合わせを行い、個々のデバイスのネットワーク アクセスを許可するかどうかを決定します。さらに、このプロセスでは、Cisco Secure ACS を利用してアクセス権限が定義されます（アクセス権限の定義および管理を最適化する方法の詳細については、次のセクション「デバイスの適合性ポリシーの効果的な管理」で説明します）。

ネットワーク アクセスのほとんどを安全なデバイスだけに制限する企業では、各エンド ポイント デバイスで Cisco Trust Agent（CTA）ソフトウェアをインストールし、応答のないデバイスには限定的なアクセスのみを提供することもできます。CTA は無料で入手可能なソフトウェアで、顧客とパートナーに対するネットワーク アクセス デバイスへのインターフェイスを提供します。Cisco Security Agent（およびウィルス対策ベンダー）は、CTA を組み込んで利用し、ネットワークに対してエンド ポイント デバイスの特性に関する情報を提供します。デバイスがネットワーク アクセス デバイスに接続する場合、またはネットワーク アクセス デバイスがエンド ポイント デバイスをポーリングする場合、CTA はエンド ポイントの適合性プラグインおよびネットワーク アクセス デバイスの両方と通信を行います。

ネットワーク アクセス デバイスは、エンド ポイント デバイスの情報を要求し、その情報を Cisco Secure ACS に送信します。次に、Cisco Secure ACS は、その情報を定義済みのセキュリティ ポリシーと照合し、必要に応じて、エンド ポイント デバイスを正しい VLAN（仮想 LAN）に接続します。

図 4 隔離 / 修正プロセスの手順



デバイスの適合性ポリシーの効果的な管理

エンド ポイント デバイスがセキュリティ ポリシーに適合しない場合、ネットワーク アクセス デバイスは、そのデバイスをプライベートな「隔離」ネットワーク内に隔離し、次に隔離の理由と修正方法を CTA に返信します。さらにネットワーク アクセス デバイスは、プライベート ネットワーク上のエンド ポイント デバイスが修正されるまで、そのデバイスをポーリングします。最後に、ネットワーク アクセス デバイスによって、修正済みのエンド ポイント デバイスは企業ネットワークへのアクセスを許可されます。

シスコは、こうした隔離 / 修正機能を備えた複数のネットワーク アクセス デバイスを出荷しており、これらの機能をシスコのネットワーク アクセス デバイス全体に幅広く装備する計画です。「セキュリティ ポリシーに適合しないデバイスの隔離と修正」のセクションでは、IBM のソリューションとシスコのこれらの機能を組み合わせることによって、企業がセキュリティ措置を実施し、生産性を回復する方法を説明します。

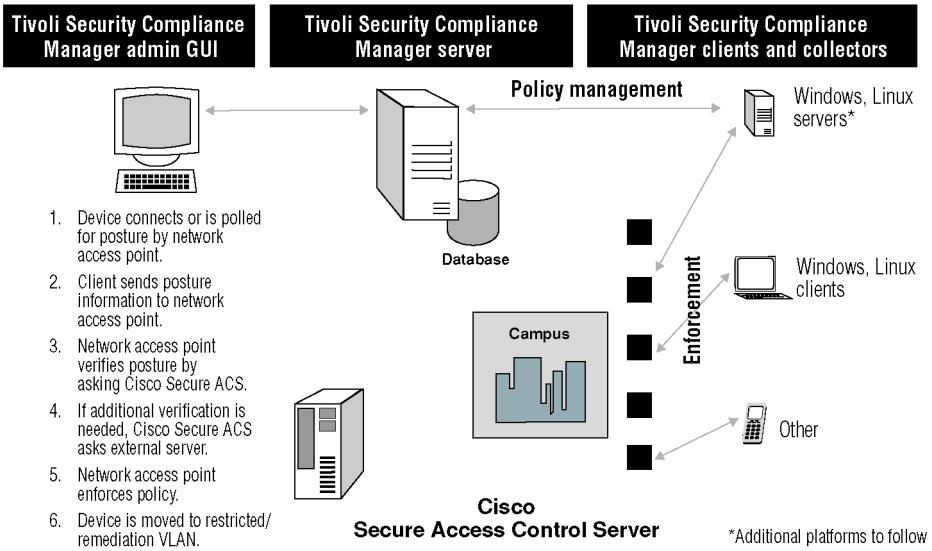
デバイスの適合性ポリシーの効果的な管理

企業のネットワークに接続するデバイスのセキュリティ アクセス ポリシーを設定し、保守することは、コンピューティング インフラストラクチャを悪意のある攻撃や不慮の損害から効果的に保護するうえで重要です。Cisco Secure ACS には、企業が実施する必要のあるポリシーを定義するためのユーザ インターフェイスが用意されています。ただし、Cisco Secure ACS は、ネットワーク インフラストラクチャの中でも重要な、パフォーマンスに影響されやすいコンポーネントなので、企業は高度なポリシー マッチングによって Cisco Secure ACS に過剰な負荷をかけないようにする必要があります。

そのため企業では、IBM Tivoli Security Compliance Manager を、Cisco NAC 用のポリシー定義および管理コンポーネントとして使用できます。Tivoli Security Compliance Manager を利用すれば、Cisco Secure ACS のリソース制約を緩和でき、高度なポリシー定義およびチェックが可能です。Tivoli Security Compliance Manager によって、企業は以下のことを実行できます。

- 柔軟性の高い GUI を使用して、各種デバイスのポリシーを定義する。
- ポリシーのコレクタ コンポーネントを管理する。コレクタは、エンド ポイント システム上で実行される Java™ ルーチンであり、固有の定義された適合性基準の存在および不在を判定するために使用する。各適合性基準には、対応するエンド ポイントの動作環境で特定の脅威をチェックする方法を認識するルーチンが必要である。Tivoli Security Compliance Manager によって、企業は、使用可能なコレクタを特定のポリシーと関連付けることができる。
- ポリシー（およびそのポリシーに関連付けられたコレクタ）を必要なエンド ポイントに提供する。
- ネットワークによって要求された場合、適合性チェックを実行する。
- 企業内のエンド ポイントの適合性ステータスをレポートする。Tivoli Security Compliance Manager には、監査に対応できる豊富なレポート機能が用意されています。

図 5 Tivoli Security Compliance Manager のアーキテクチャと処理手順



セキュリティ ポリシーに適合しないデバイスの隔離と修正

Cisco Secure ACS では、各デバイスが従うべきポリシーを記録する必要があります。Tivoli Security Compliance Manager は、企業がこの要件を簡略化する（および Cisco Secure ACS の作業負荷を最小化する）のに役立ちます。これは、Cisco Secure ACS において、デバイスの各クラスが従うべきポリシーを項目ごとに細かくチェックするのではなく、そのポリシーの数のみを認識されるようにすることで実現します。Tivoli Security Compliance Managerでは、Cisco Secure ACS のために詳細なチェック情報が要約されます。適合性基準に変更があれば、企業はローカルな適合性ポリシーを更新してデバイスの保護を維持します。

デバイスが企業に接続する際（およびデバイスが常時接続している場合は定期的に）、シスコのネットワーク アクセス デバイスは、適合した現行のポリシーを提供するようにデバイスに要求できます。Tivoli Security Compliance Manager クライアントが実行されているデバイスは、そのエンド ポイントの現行のポリシー ステータスによってネットワークに応答できます（CTA を使用する場合と同様に、企業では、各デバイスで Tivoli Security Compliance Manager クライアントを実行し、Tivoli Security Compliance Manager の要求に応答しないデバイスへのアクセスを制限することができます）。

Tivoli Security Compliance Manager サーバは、エンド ポイントの適合性を記録し、管理するための高度な機能を提供できるように設計されています。必ずしもすべてのエンド ポイントの特性を、ネットワーク アドミッション プロセスに含める必要はありません。企業は、追加のセキュリティ措置をアクセス制御に使用しなくても、それらの措置の適合性を監視し、記録することが可能です。この監視機能は、レポートや監査の際、および実施レイヤへの適合性基準の追加を準備する際に使用できます。

要約すると、企業は Tivoli Security Compliance Manager を使用して、自社で定義するポリシーへのエンド ポイントの適合性を集中管理し、デバイスによるネットワーク接続の前または最中にポリシーを実施し、最新の状態に関する監査とレポートを実行します。

セキュリティ ポリシーに適合しないデバイスの隔離と修正

エンド ポイントが企業のポリシーに適合しないか、その要求に応答しない場合、シスコのネットワーク アクセス デバイスは（Cisco Secure ACS と連携して）、そのエンド ポイントをネットワークの隔離部分に移動させます。隔離されたエンド ポイントは、設定に誤りがあるか、必要なソフトウェア アップデートまたはセキュリティ製品が欠けている可能性があります。また、企業は、パスワード強度やパワーオン パスワードのような追加的な要件をユーザに課すことで一定のセキュリティ レベルを維持することもできます。

隔離の理由が何であろうと、そして隔離がすべてのアクセスを制限するものであるかネットワークの一部へのアクセスを制限するものであるかにかかわらず、隔離はユーザの生産性に影響を与える可能性があります。エンド ポイントを適切にセキュアなネットワークに戻し、それによってユーザの生産性を回復するには、これらの問題を是正できるソリューションの導入が必要です。IBM のソリューションは、シスコのソリューションと密接に連携して隔離されたデバイスを修正します。

セキュリティ ポリシーに適合しないデバイスの隔離と修正

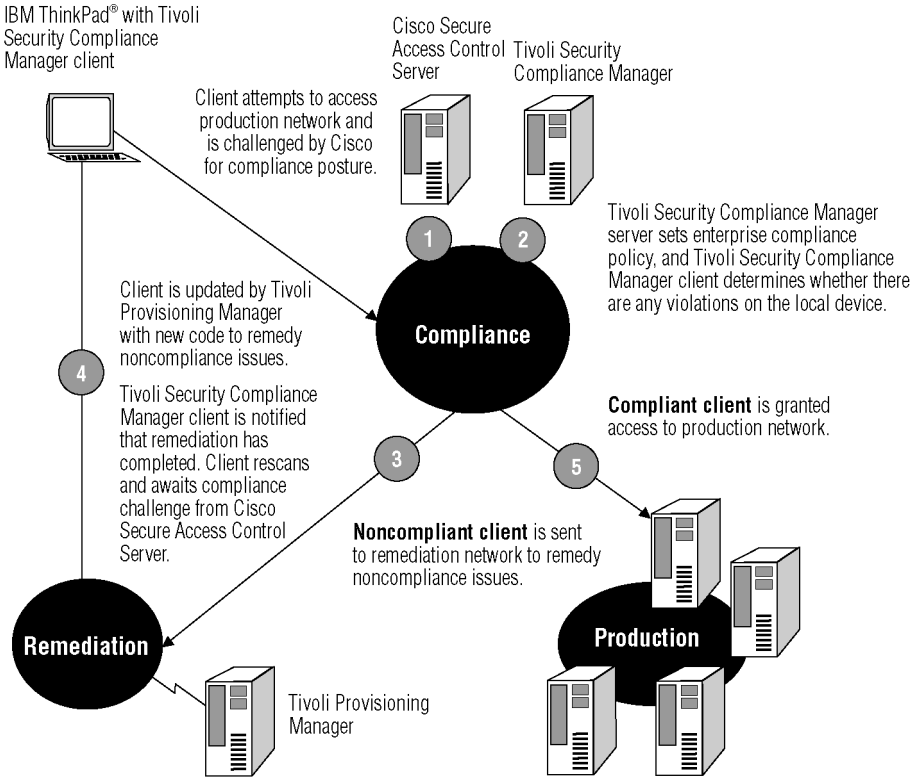
デバイスを隔離した場合、ネットワークは、そのエンド ポイントによる本稼働ネットワークへのアクセスを拒否した理由を示すトークンを、Tivoli Security Compliance Manager クライアントに返します。これには、エンド ポイントが不適切なポリシー レベルにあるか、どの適合性チェックに不合格となったかのいずれかの情報が含まれます。それに加えて、トークンには、そのエンド ポイントの修正箇所を示す文字列が含まれます。次に、Tivoli Security Compliance Manager クライアントによって、エラーが存在する箇所を修正するサブシステムが起動されます。

IBM Tivoli Provisioning Manager は、企業がエンド ポイントを修正するために使用できるソリューションを提供します。このソリューションの機能豊富なワークフロー環境とさまざまなエンド ポイントを利用して、企業はエンド ポイントのソフトウェアと設定を集中管理できます。

Tivoli Provisioning Manager は、Tivoli Security Compliance Manager からトークンを受け取ると、修正措置を起動する一連のプロセスを実行します。これらのプロセスでは、トークンを検査して、エンド ポイントに必要な変更点を確認し、自動または対話式のプロセスを起動して必要な修正を施します。Tivoli Provisioning Manager には、以下の修正シナリオが含まれます。

- ソフトウェア レベル（通常、OS のレベルと修正パック）
- パッチ レベル
- ウィルス対策およびファイアウォールのアップデート
- 最新のウィルス スキャン
- パスワードの強度と履歴
- ポリシー レベル

図 6 適合性 / 修正プロセスの手順



含まれている修正機能を使用するため、企業では、ネットワーク内のエンド ポイントに必要な特定のアップデートを適用して Tivoli Provisioning Manager を準備します。エンド ポイントが隔離された場合、Tivoli Provisioning Manager は、特定の修正サービスを利用してトークン内で指定されているエラーを修正します。修正では、ソフトウェア アップデートのインストレーションか、設定上の問題の修正が行われます。

必要な変更を行うために Tivoli Provisioning Manager で使用される最も基本的な方式は、Secure Shell（SSH; セキュア シェル）セッションを経由するものです。将来的には、より高度なデバイス管理機能がターゲット システムのアップデート用に提供される予定です。

エラーが修正されると、ネットワークは再度エンド ポイントに問い合わせを行います。この時点で適合性チェックが成功すると、デバイスはセキュアなネットワークへの参加を許可されます。

Tivoli Provisioning Manager は、修正プロセスとソフトウェア管理プロセスの拡張と自動化のために企業で利用できる、エンド ポイント用の包括的なソフトウェア管理機能とそのフレームワークを提供します。この製品では、企業はニーズに応じて修正プロセスを追加できます。

Microsoft® Windows® 環境では、IBM Rescue and Recovery with Antidote Delivery Manager によって、エンド ポイントがアップデートを取得してポリシーに適合するための類似の機能が提供されます。Tivoli Security Compliance Manager が適合性のないWindowsエンド ポイントを隔離ネットワークに移動させた場合、IBM Rescue and Recovery クライアントが必要なアップデートのリポジトリをチェックするように設定できます。

Tivoli ソフトウェアが存在しない環境では、Antidote Delivery Manager によって、最新の Antidote Delivery Manager ログ エントリが企業の要件に適合しないような状況に対応できます。Antidote Delivery Manager は、エンド ポイントをネットワークから除去するために Cisco NAC を利用できるように設計される予定です。

IBM およびシスコ製品による高度に安全な企業コンピューティング インフラストラクチャの実現

企業のコンピューティング インフラストラクチャを保護するうえで重要なことは、企業のリソースにアクセスできるユーザ、および接続に使用される各デバイスのセキュリティ状態を確認することです。ネットワークやその他のリソースへのアクセス制限は、幅広い自動化されたアイデンティティ管理機能、および実施への階層化アプローチを採用することで達成できます。企業に接続するエンド ポイントの適合性を高度に管理するには、エンド ポイントが企業のセキュリティ ポリシーに適合しない場合にそれらを修正する機能が必要です。

以下の IBM とシスコの統合型製品は、企業がアイデンティティおよびデバイス管理機能を実装して、自社の内部管理における弱点を緩和し、政府の法規制と監査の要件への適合性を最適化するのに役立ちます。

ユーザ アクセスおよびアイデンティティ管理コンポーネント

- Cisco Secure ACS — すべてのシスコ製デバイスとセキュリティ管理アプリケーションをカバーする、中央集中型のアイデンティティ ネットワーキング ソリューションとユーザ管理環境を提供します。Cisco Secure ACS を使用することで、ネットワークにログインできるユーザと各ユーザの権限をネットワーク管理者が管理し、指定されたポリシーを実施できます。また、セキュリティ監査またはアカウント課金情報を記録します。中央集中型のアイデンティティ ネットワーキング フレームワークから認証、ユーザおよび管理者アクセス、ポリシー管理を組み合わせることができ、アクセス セキュリティが拡張されます。これは、柔軟性とモビリティ、セキュリティ、およびユーザの生産性を最大限に引き上げるうえで効果的です。

- Tivoli Access Manager for e-business ― オンデマンド ビジネスおよび企業アプリケーション向けにポリシーベースのアクセス制御ソリューションを実装します。この製品は、Gartner 社の Magic Quadrant で Leader Quadrant に選ばれています。幅広い Web およびアプリケーション リソースにわたって拡張と複雑性を管理し、増大する管理コストを抑制し、セキュリティ ポリシーの実装に伴う問題に対処するのに役立ちます。また、すぐに使用できるオンデマンド ビジネス アプリケーションと統合し、安全な、カスタマイズされた統合環境を提供します。認証および許可 API を利用し、J2EE™ のようなアプリケーション プラットフォームと統合しているので、企業グループ全体に広がった業務上重要なアプリケーションとデータに対するアクセスのセキュリティを確保できます。
- Tivoli Identity Manager と IBM Directory Server ― Tivoli Identity Manager は、安全な自動化されたポリシーベースのユーザ管理ソリューションを、従来の環境とオンデマンド ビジネス環境の両方で提供します。わかりやすい Web ベースの管理およびセルフサービス インターフェイスと既存のビジネス プロセスを統合することにより、ユーザ管理とリソース権限のプロビジョニングを簡略化し、自動化します。Tivoli Identity Manager では、ユーザのライフサイクル管理を自動化し、アイデンティティ データを監査、レポートなどのために使用できます。また、IBM Directory Server の安定したスケーラビリティと信頼性を活用することもできます。

デバイスの適合性および修正コンポーネント

- Tivoli Security Compliance Manager ― セキュリティ ポリシー適合性製品を、あらゆる規模の企業に展開します。セキュリティ上の脆弱性とセキュリティ ポリシー違反を特定する早期警戒システムを実装します。一貫性のあるセキュリティ ポリシーを定義し、これらの定義済みセキュリティ ポリシーの適合性を監視します。セキュリティ ポリシーを、内部のセキュリティ要件と業界標準のセキュリティ ポリシーの両方に準拠させます。
- Cisco Trust Agent ― ネットワークによるアクセス許可の前に、ポリシー状態の有効性を確認する必要があるホストに、クライアント ソフトウェアをインストールします。Cisco NAC モデルを利用して、適合性のあるシステムにのみネットワーク リソースへのアクセスを許可し、それによって不正システムまたは未更新システムによる潜在的なセキュリティ リスクを抑制します。Cisco Security Agent とウィルス対策ソフトウェアがインストールされて最新であるかどうか、および現行の OS のレベルとパッチ レベルを、Cisco NAC で判定します。Cisco Trust Agent は、シスコから単独のアプリケーション、または Cisco Security Agent にバンドルされた形のいずれかで、あるいは Cisco NAC の協業企業（Trend Micro の OfficeScan など）から、無料で入手できます。
- IBM ThinkVantage™ テクノロジー ― より高度なユーザおよびデバイス認証を提供し、IBM のラップトップおよびデスクトップに対する不正変更の脅威を抑制します。これによって、ハードウェアベースの信頼性機能を備えた「利口な」デバイスを提供し、業界をリードしています。
- Tivoli Provisioning Manager ― ベスト プラクティスのワークフローを使用して、手動のプロビジョニングおよび展開プロセスを自動化します。構築済みのワークフローを利用して、主要なベンダーの製品の管理と設定を行います。カスタマイズされたワークフローを作成すれば、データ センターのベスト プラクティスと最良の手順を、一貫したエラーのない方法で自動的に実行できます。たとえば、自動化ワークフローを使用すれば、サーバのプロビジョニングと展開を（初期状態 [bare metal] からフル稼働まで）ボタン 1 つで実行できます。
- IBM Rescue and Recovery with Antidote Delivery Manager ― プライマリ OS がウィルス、ワーム、または他のソフトウェアの問題によって使用不能になった場合でもクライアントを修正できる、独自の機能を使用します。ペイロードを配信する機能を常に提供することにより、Windows イベントに対してすばやく効率的に、安定して対応します。Windows の接続機能を無効化して有害なソフトウェアの拡大を防止します。アップデート用の安全なリポジトリが作成されます。IBM Rescue and Recovery のバックアップ機能を利用すれば、重大なワームおよびウィルス攻撃からの復旧が容易になります。

デバイスの適合性および修正コンポーネント

その他の情報

IBM が提供するセキュリティ ソリューションと統合型ソリューションについての詳細は、IBM の営業担当者にご連絡いただくか、次の URL をご覧ください。
http://www-6.ibm.com/jp/services/strategy/issue/safety_security.shtml

Tivoliセキュリティ管理ソリューションについての詳細は、次の URL をご覧ください。
http://www-6.ibm.com/jp/software/tivoli/products/

IBM とシスコのセキュリティ ソリューションについての詳細は、次の URL をご覧ください。
http://www-6.ibm.com/jp/domino05/ewm/NewsDB.nsf/2004/09241

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

International Business Machines Corporation
New Orchard Rode
Armonk, NY 10504
ibm.com/security/cisco