

Cisco and IBM: Integrated Security Solutions Overview
 エンタープライズセキュリティの新しいモデル

Overview



- 米国の大手専門サービス会社 Deloitte & Touche LLP 社が 2004 年に実施したセキュリティに関するアンケート調査では、次のことが明らかになりました。
 - 外部からのセキュリティ攻撃が 1 年前と比べて 2 倍以上に増加している
 - 回答者の 83% が稼働中のシステムに脆弱性があると認識している (2003 年度の調査では 39%)
 - 回答者の 40% が金銭的な損害を被ったことがある
- IT 業界の世界的な調査および分析サービスを提供する大手リサーチ会社である Gartner 社が 2004 年に行った調査によると、互いに顔の見えない売り手と買い手の信頼関係に基づく e-ビジネスのマーケットは、1 兆 6 千億ドル規模になるだろうと予測されています。

セキュリティに関する今日の課題

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の活用とネットワーク、システム、およびアプリケーションの強化に取り組んでいます。顧客、サプライヤ、およびパートナーとの接続を効率化するための IT 投資は、年ごとに増大しています。

ところが、今日のコンピューティング環境への接続にはリスクが伴います。最近のウイルス、ワーム、およびインターネット攻撃の大量発生によって、企業は甚大な損害を被り、これらのセキュリティ侵犯は生産性の著しい低下を引き起こしています。これらの拡大する脅威に対処するために従来以上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十分に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、多くの企業では情報の取り扱いに関係する業界および政府のさまざまな規制事項を順守することも要求されています。これらの問題に対処するため、多くの企業では複数のポイント製品ベンダーのセキュリティソリューションを組み合わせ導入してきました。しかし、複数ベンダーのソリューションを統合して運用するのはコストが高くつくだけでなく、企業のセキュリティ要件を完全に満たすことも不可能でした。TCO (総所有コスト) の高騰も大きな問題となっています。

このような従来のモデルでは、お客様のニーズを満たせないのは明らかです。セキュリティが経済的な影響も与えるようになった今、パートナーシップによる効果的で効率的なセキュリティの提供、全社的な整合性、脅威への適応能力と回復力に優れた IT インフラストラクチャが求められています。

エンタープライズセキュリティの新モデル：IBM とシスコ

IBM は企業向けコンピューティングシステム、セキュリティ管理、アプリケーション、ミドルウェア、およびサービスの分野で世界的に高く評価されている会社であり、エンタープライズセキュリティ管理でも主導的な役割を果たしています。シスコは企業およびインターネット環境でのネットワークシステムの世界的なリーディングカンパニーであり、ファイアウォール、侵入検知と防御、および Virtual Private

強く競争力のある企業に必要なビジネスの拡大、必要に応じた進化、および継続性を実現するためのインテリジェントなネットワーク インフラストラクチャの活用と自己管理型システムの展開を IBM とシスコが提供いたします。

Networking (VPN; 仮想私設網) システムの第一人者でもあります。

e-ビジネスにとっての懸念事項であるエンドツーエンドでのセキュリティという問題を解決するために、IBM とシスコはそれぞれの製品とアーキテクチャの連携によって戦略的アライアンスを強化し、標準化に向けて共同開発を進めています。強く競争力のある企業に必要なビジネスの拡大、必要に応じた進化、および継続性を実現するためのインテリジェントなネットワーク インフラストラクチャの活用と自己管理型システムの展開を IBM とシスコが提供いたします。企業が直面しているセキュリティ上の問題への取り組みを、最も信頼する 2 社に任せられるのです。シスコと IBM の強力な提携によって、リスクの軽減、生産性の向上、およびコストの削減をもたらす統合型セキュリティ ソリューションが実現されます。

IBM とシスコ — 統合化された効率的なセキュリティ

IBM とシスコは、お客様のセキュリティ実装をより効果的および効率的にするために、それぞれの製品の統合化と新たな技術開発を進めています。IBM では総合的な IT セキュリティ ソリューション サービスも提供する予定です。2 社の提携関係は、リソースの効率的利用、生産性の向上、および技術革新による差別化と新たな価値の創出を目指し、あらゆる顧客のニーズ、商機、または外部からの脅威に対して柔軟かつ迅速に対応することを目的とする、IBM の「オンデマンド」構想に即したものです。同様に、セキュリティ上の脅威に対する識別、防止、および適応能力の大幅な強化を目的とするシスコの自己防衛型ネットワーク構想もサポートしています。

IBM とシスコのセキュリティ コラボレーション

- **IBM Tivoli Identity Manager** とシスコのセキュリティおよび管理製品との統合化による、アイデンティティベースのアクセスの提供およびユーザのライフサイクル管理コストの削減。IBM とシスコは、ユーザおよびアイデンティティ管理に関する両社の製品間のインターオペラビリティを実現し、ユーザ アカウントの管理を大幅に簡素化します。たとえば、Tivoli Identity Manager (TIM) によって管理されるユーザ管理ライフサイクル プロセスには、Cisco Secure Access Control Server (Cisco Secure ACS) が組み込み可能です。その結果、あらゆる IT リソース間でセキュリティ アクセス ポリシーの自動化、監査、および実施機能を備えた中央集中型のアイデンティティ管理が実現されます。また、Cisco Catalyst® スイッチ上の Cisco Identity-Based Networking Services (IBNS) と TIM を統合化することで、スイッチ ポート レベルで厳密にプロビジョニングされるアイデンティティベース アクセスを提供します。これによって、ネットワーク リソースにアクセスするユーザを動的に識別して制御することができます。
- **IBM Tivoli** ソリューションと **Cisco Network Admission Control (NAC)** 機能の統合化による、エンドポイントからシステムおよびアプリケーションへのセキュアかつインテリジェントな接続。Cisco NAC を使用すると、エンドポイントのセキュリティ ステータスを検証し、セキュリティ ポリシーに適合するエンドポイントだけにネッ

トワークおよびシステム リソースの使用許可を与えることができます。IBM とシスコは、Tivoli Security Compliance Manager と Cisco NAC 対応インフラストラクチャの統合化を進めています。これが実現すれば、エンドポイント システムのさまざまなパラメータを解析し、セキュリティ ポリシーに適合しているかどうかに基づいて、ネットワークが適切なアドミッション制御を実行できます。さらに、Cisco NAC アーキテクチャへの Tivoli Provisioning Manager の統合化によって、インテリジェントな自己管理型システムの活用が可能になり、ポリシー違反で隔離されたエンドポイントに対する修復サービスも実行できます。この統合化は、効果的かつ効率的なユーザアドミッションを実現するとともに、ヘルプ デスクの負担を減らして全体的な運用コストを削減します。

- **Cisco Security Agent (CSA) と IBM のプラットフォーム組み込みセキュリティ機能の統合化による、IBM ハードウェア プラットフォームのセキュリティ強化。** IBM とシスコは、IBM のラップトップおよびデスクトップ プラットフォームのセキュリティを強化する複数のソリューションを共同開発しています。一部の ThinkPad® システムおよび ThinkCentre™ システムで使用可能な IBM のエンベデッド セキュリティ サブシステムである ThinkVantage™ テクノロジーは、サードパーティ製の認証証明書および暗号鍵をサポートするハードウェアベースの保護機能を提供します。IBM とシスコはすでにこの組み込み機能を Cisco VPN Client と統合しており、高度なセキュリティとユーザの透過性を備えた VPN 接続を実現しています。また、IBM Tivoli Compliance Manager を Cisco Trust Agent と統合化する計画もあり、それによってもう 1 つの ThinkVantage テクノロジーである Rescue and Recovery 製品が、エンドポイントのポリシー適合性を調べ、Cisco NAC 環境で迅速に問題を解決できるようになります。IBM とシスコは、IBM プラットフォームへの攻撃に対する保護対策も共同開発しています。侵入防止のためのパーソナル ファイアウォール テクノロジーである CSA が、新種のウィルスやワームによる「Day-Zero」攻撃からの保護機能およびパッチ管理機能を IBM システム ユーザに提供します。CSA は「動作 (behavior)」に基づくアプローチを採用しているため、従来のウィルス対策ソリューションで必要とされた、エンドポイント攻撃データベースの頻繁な更新が不要になります。IBM は IBM.com® を通じてサーバ、デスクトップ、ラップトップ版の CSA を提供します。
- **IBM とシスコのセキュリティ ソリューションの価値を提供する IBM グローバル サービス。** IBM グローバル サービスは、ネットワークとセキュリティの統合を適切に設計し、ネットワーク環境の継続的な管理を支援するための各種サービスを提供します。ユーザ プロビジョニング、アイデンティティベースのネットワーキング サービス、Cisco NAC の実装における Tivoli 管理製品とシスコ ネットワークの統合化など、あらゆるサービスが完備されています。また、プラットフォーム侵入防止や CSA 用のイベント統合化サービスなど、さらに充実した内容となっています。IBM グローバル サービスは、豊富な業界の専門知識に基づき、ビジネス ニーズに応じた高度なセキュリティのエンドツーエンドのネットワーキング ソリューションを提供します。

詳細情報

エンタープライズ セキュリティに関する 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/ibm

www.ibm.com/services/cisco



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



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, and the Cisco Systems logo 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.

IBM, IBM.com, the IBM logo, the e-business logo, ThinkCentre, ThinkPad, ThinkVantage, and Tivoli 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.