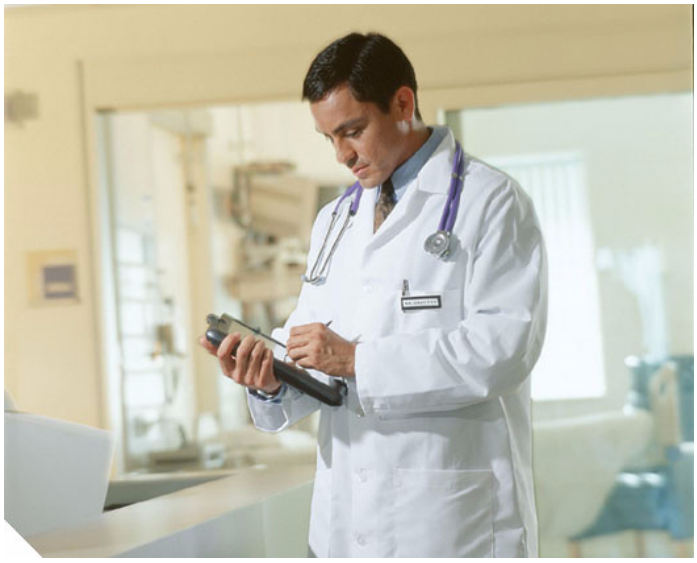
“がん”と闘う医療チームを支援するシスコの安全なネットワーク
M. D. アンダーソン基金

はじめに

テキサス大学 M. D. アンダーソン（MDA：M. D. Anderson）がんセンターは、テキサス州議会および MDA 基金によって、ヒューストンのテキサス大学の敷地内に設立されました。この MDA がんセンターは、あらゆる種類のがんの予防と根絶に力を注いでいます。1941 年の設立当初から、50 万人以上の患者が、答と希望を求めて MDA の門をくぐり、その両方をここで見つけました。そして、MDA は、世界中で働く 40,000 人以上のがんの専門家を育ててきました。MDA の研究者たちは最新のがん治療への道を開きました。MDA の使命は常に変わらず、テキサス、国内、そして世界のがんを根絶することです。

21 世紀においては、世界クラスの医療は、さまざまな要素に左右されるようになってきました。この要素には、十分な財源や適切な人材などがありますが、ますます重要性を増しているのは堅牢、柔軟かつセキュアな通信インフラストラクチャです。より多くの研究および患者情報がイントラネット、エクストラネット、そしてインターネットで伝送されるようになるにつれ、包括的なセキュリティ アーキテクチャの必要性がますます高くなっています。さらに、1966 年の Health Insurance Portability and Accountability Act（HIPAA：患者情報保護法）の施行により、医療組織は医療関係データのセキュリティとプライバシーに関する政府規制を遵守しなければならなくなりました。MDA の情報システム部門は、世界クラスのソリューションから構成されるセキュリティ アーキテクチャを独自の方法で実装して、セキュリティ問題に対処することを選択しました。



シスコのソリューションでプライバシーとセキュリティを保護

MDA は、毎年約 65,000 人の患者を診察しており、各患者の非常に個人的なデータを安全に保管および送信する必要があります。最高品質の医療を提供するため、医師は広範にわたる医療専門家のチームと、患者の履歴および診断記録を電子通信を介して共有しています。さらに、医師は在宅中または旅行中でも重要な患者データにアクセスする必要があるかもしれません。医師間で共有され、遠隔地間で送信される患者情報、個人データ、財務データを効果的に保護するため、情報システム部門のスタッフは入念に作業する必要がありました。

MDA のセキュリティ チームを率いるセキュリティ管理最高責任者 Lew Wagner 氏は、MDA へ出入りするすべての電子情報および MDA で処理または保管されるすべての電子情報の保護に責任を負っています。Wagner 氏は次のように語ります。「攻撃はさまざまな方向からやってきます。たとえば、自分の庭を攻撃から守っているとします。もし心配しなくてはならないのが前庭だけであれば、すべての時間を前庭にフェンスを建てることに費やせばいいのです。しかし、もし裏庭や側庭、または上から攻撃されたらどうしますか？攻撃がこれらすべての方向から同時に行われたらどうしますか？これらすべてを見張る方法を開発できなくてはならないのです。」Wagner 氏はさらに付け加えます。「現在の脅威は、単一ベクトルの攻撃ではありません。複数の段階またはチャネルを通過して入ってくるマルチベクトル攻撃なのです。」

Wagner 氏はこれらのことを念頭に置いて、効率的に MDA ネットワークのすべての領域を保護するために、包括的な階層化セキュリティ アーキテクチャを設計しました。このアーキテクチャは、シスコが提供する SAFE ブループリントに似ていました。つまり、ネットワークの成長や変化に合わせてセキュリティ デザイン、展開、管理を簡易化するモジュラ手法です。SAFE ネットワークは、クラス最高のセキュリティ製品とサービスから構成されています。Lew Wagner 氏と彼のチームは、シスコのセキュリティ専門家チームと連携し、侵入保護、Virtual Private Network（VPN; 仮想私設網）、ファイアウォール、無線アクセス、およびセキュリティ管理についてさまざまなシスコ ベースのソリューションを実装することにしました。

階層化セキュリティ：MDA での侵入保護

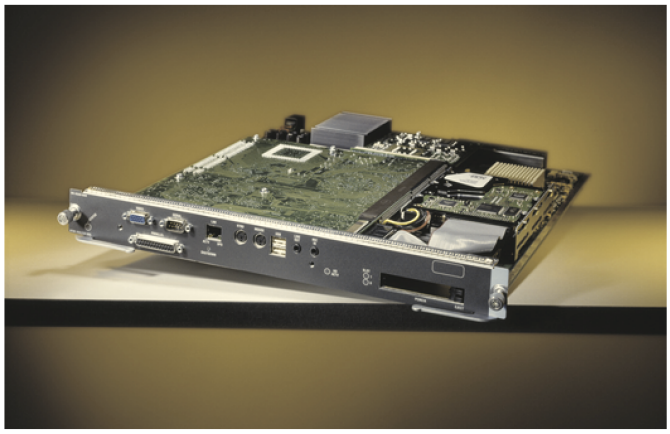
オープンで信頼される通信の新しい時代は、新たな脆弱さと問題を引き起こしています。そのため、医療組織は広範な種類のネットワーク攻撃から機密データを保護する必要があります。さらに、攻撃は外部のハッカーだけでなく、表面的には信頼できそうな内部従業員によっても行われます。

MDA は、Dynamic-Defense-In-Depth（D3）ファイアウォール マトリックス全体に Cisco PIX® セキュリティ アプライアンスを配置することにより、ネットワークの重要なノード エリアを保護しています。MDA は高いフェイルオーバーおよびアベイラビリティ機能を考慮し、Cisco PIX セキュリティ アプライアンスを選択しました。しかし、MDA セキュリティ チームは、セキュリティには階層化手法が重要であることを認識していました。彼らは、ファイアウォールだけでは処理できない危険と脆弱性に対処するためには、侵入保護テクノロジーを利用しなくてはならないと考えました。

シスコの侵入検知システム ソリューションは、たとえばインターネット ワーム、DoS 攻撃、E ビジネス アプリケーション攻撃など、費用がかかりネットワークを消耗させる攻撃から組織を保護するのに必要な、完全な侵入保護を提供します。シスコの優れた IDS は、最新の攻撃識別技術を取り入れ、既知の攻撃タイプに対抗するとともに、新しく出現した攻撃も防止します。シスコの IDS は、ダイナミックかつ変化する脅威に対処することにより、従来のテクノロジーをはるかに超えた強化セキュリティを提供し、E ビジネス システムおよびアプリケーションの耐障害性を強化します。

MDA のコアおよび部門サイトには、MDA のスイッチド インフラストラクチャの基礎である Cisco Catalyst® 6500 シリーズ スイッチが配置されています。Catalyst 6500 シリーズ スイッチは、ますます増え続ける MDA のギガビット スケーラビリティ、ハイ アベイラビリティ、広範なサービスなどへの要件に対応しています。Lew Wagner 氏のチームは、Cisco Catalyst 6500 IDS サービス モジュール（図 1）を採用し、IDS 機能をスイッチに統合しました。Cisco Catalyst 6500 IDS サービス モジュールは、IDS 機能を直接スイッチ バック プレーンに組み込むことができるので、特にスイッチド環境におけるスイッチング機能とセキュリティ機能に対応しており、1 台のシャーシで実行できます。Cisco Catalyst 6500 IDS サービス モジュールは取り付けとメンテナンスが簡単であり、リアルタイムでの攻撃防御を実施しても、スイッチ パフォーマンスが低下することはありません。

図 1
Cisco Catalyst 6500 IDS サービス モジュール — 取り付けとメンテナンスが簡単であり、リアルタイムでの攻撃防御を実施しても、スイッチ パフォーマンスが低下することはありません。



MDA は現在 8 つの Cisco Catalyst 6500 IDS サービス モジュールを配置しています。Lew Wagner 氏は、Cisco IDS モジュール（ブレード）の機能について語ります。「ブレードに決定したとき、私達はスピードを求めていました。私達は高速で透過的な製品を求めていたのです。IDS ブレードについてはきわめて良い評判を聞いていました。それまでにもシスコとは非常に密接な関係があったことも功を奏しました。今では、リアルタイムの侵入検知警報を備えています。」Wagner 氏はまた Cisco IDS の展開についても語りました。「IDS により、組織全体のネットワーク フローを把握できるようになったため、外部または内部から発生する可能性のある特定の攻撃については、今まで以上に理解して予測し、予防的に対処できるようになりました。以前は、そのようなことはできませんでした。これにより、セキュリティ上、欠けていた要素が補われたのです。」

Cisco Catalyst 6500 IDS サービス モジュールを設定して管理するため、セキュリティ チームは CiscoWorks VPN/Security Management Solution（VMS）を選択しました。Cisco VMS を利用すると、MDA のセキュリティ管理者は、ネットワークを出入りする通常のネッ

トワーク トラフィックと疑わしいネットワーク トラフィックを監視できます。VMS は、IDS モジュールから伝送された情報を関連付け、管理者がプロアクティブに行動をおこせるようにします。また、Cisco VMS を利用すると、MDA 管理者は中央からネットワーク全体のセキュリティ ポリシーを、設計、配布、実施、および監査することができます。

Cisco Catalyst 6500 IDS サービス モジュールでよい結果が得られたため、MDA IT グループは Cisco Host-based Intrusion Detection System（HIDS）ソリューションを評価することにしました。Cisco HIDS は、その HIDS がインストールされているホストで発生した攻撃を検知します。Cisco HIDS は、OS（オペレーティング システム）およびアプリケーション コールの代行受信、OS とアプリケーションの設定の保全、着信サービス要求の検証、およびローカル ログ ファイルに基づいた不審なアクティビティの事後検証を行います。NIMDA ワームが世界中の数多くの組織を攻撃したとき、MDA では Cisco IDS Host Sensor のトライアル コピーを実行していました。Cisco IDS Host Sensor はワームを識別し、MDA のデータ インフラストラクチャを深刻なダメージから保護することができました。

MDA の拡張：VPN

インフラストラクチャの拡大に伴い、MDA の多くの機能は地理的に分散するようになりました。たとえば、人事および施設部門は敷地の外にあるため、従業員と施設の管理のデータは遠隔地のこれらの部門間で安全に送信されなくてはなりません。また、敷地外の外来治療センターには、処方箋など、患者の個人的なデータが送信される薬局や診療室があります。MDA は、データをリモート サイトに送信するだけでなく、他の病院との通信も行います。さらに、MDA の高度な能力を利用した検査を受けるために、世界中の病院から患者が来院するので、MDA は検査結果を迅速かつ安全に患者の地域の医師に送る必要があります。

MDA では、シスコの VPN 対応ルータを使用して、遠隔地およびエクストラネット パートナーへのセキュアなサイト間 VPN を提供しています。MDA は、Cisco 7200 シリーズ VPN ルータをヘッドエンドで、7100 シリーズ ルータをリモート サイトで実装して、IPSec 準拠の暗号化 VPN トンネル経由でキャンパスを拡張しました。MDA はまた、Cisco 7100 および 7200 シリーズ ルータ用に VPN アクセラレーション モジュールを使用することにしました。このモジュールは、サイト間 VPN アプリケーションに適した高性能なハードウェア補助暗号化、鍵生成、および圧縮サービスを提供します。

「このルータはルータに求められる最高の働きをします。つまり、このルータは停止することなく常に稼働しています。ルータが停止したらトラフィックは止まりますが、生命にかかわる環境では、そのような事態は許されません」と Wagner 氏は語ります。

患者によっては、MDA の医師の留守中にその医師の専門技術を必要とする場合があります。MDA の医師は、緊急の診断が必要な場合に自宅で電話を受け、VPN 対応のセキュアなラップトップまたは PC で関連する履歴データとともに診断画像を見ることができます。リモート アクセス VPN 接続の実装については、Cisco VPN 3060 コンセントレータ（図 2）を使って、インターネットを含むTCP/IPネットワークでのセキュアな接続を可能にしています。Cisco VPN 3060 コンセントレータは、クライアント ソフトウェアが組み込まれたリモート アクセス VPN プラットフォームであり、アベイラビリティ、パフォーマンス、およびスケーラビリティに優れ、最新の暗号化および認証技術が採用されています。また MDA では、Cisco VPN 3060 コンセントレータを使用して、医師に患者情報や、E メールおよび会議計画プログラムなどのアプリケーションへのリモート アクセスを提供しています。

図 2
Cisco VPN 3000 シリーズ コンセントレータ — Cisco VPN 3000 シリーズ コンセントレータは、クライアント ソフトウェアが組み込まれたリモート アクセス VPN プラットフォームであり、アベイラビリティ、パフォーマンス、およびスケーラビリティに優れ、最新の暗号化および認証技術が採用されています。

最高の柔軟性：無線アクセス

効率と柔軟性を最大限にするため、MDA は医師も病院のさまざまな場所でノート型パソコンを「無線」で使用できるようにしました。シスコの無線ソリューションの導入により、医師が病院のさまざまな場所から重要な情報をリアルタイムで見直すことができるようになりました。無線クライアントの認証と許可を行うために、Cisco Aironet® アクセス ポイントが施設のさまざまな場所に配置され、Cisco Aironet クライアント アダプタがノート型パソコンに取り付けられました。

ネットワーク側では、Cisco Secure Access Control Server（ACS）がバックエンド データベースとして機能して、ユーザおよびユーザ権限についての認証情報を保持します。Cisco Secure ACS はユーザの Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を制御し、ネットワークへのアクセスを管理します。それにより、ネットワーク管理者は、MDA ネットワークに有線または無線接続でログオンできるユーザの制限と、各ユーザの権限の制御ができます。

シスコの無線アクセスを利用することで、MDA の医師は、その革命的データベース アプリケーションである ClinicStation を十分に活用できるようになりました。受賞歴のある ClinicStation は、MDA で開発されたものであり、医師と他の医療スタッフは複数の臨床データベースを統合された単一の画面で安全に利

用できます。毎月、MDA の職員は 300,000 件以上の患者照会を実行し、1,000,000 件以上の医療文書を参照します。ClinicStation は、ピーク時には 1100 人以上のユーザに同時に対応できます。

MDA では、無線でアクセスされたデータすべてを保護する方法の 1 つとして、Lightweight Extensible Authentication Protocol（LEAP）を使用しています。LEAP は、クライアントと RADIUS サーバ間の強力な相互認証をサポートするシスコ独自の無線 LAN 用 802.1X セキュア認証プロトコルです。このプロトコルは、ユーザおよびセッションごとの動的 Wired Equivalent Privacy（WEP）鍵拡張機能を提供することにより、さまざまなネットワーク攻撃を軽減します。

Wagner 氏は、Cisco LEAP ベースで情報を保護することについて説明します。「LEAP では、パスワードを動的なものにしました。パスワードは 3 分ごとに変化するので、たとえハッキングをしても何も意味がありません。3 分後に再び変化するのです。これがいわゆるワンタイム パスワード テクノロジーです。私達は、使用する無線アプリケーションのすべてについて、これを標準にしようと思っています。」

医療関係機関のセキュリティのためのパートナー

シスコのセキュリティ テクノロジーおよび製品は、高速で信頼性が高く、年中無休で MDA の情報を保護します。Wagner 氏は次のように語ります。「シスコのパフォーマンスは、帯域幅の点からも際立っていました。」MDA のセキュリティ哲学、ポリシー、およびアーキテクチャは、シスコの SAFE ブループリントの精神と共通点があります。つまり、MDA がんセンターが安全に E ビジネスに従事できるモジュラ型でスケーラブルなセキュリティ フレームワークです。

MDA は、拡張された施設およびコミュニティ全体のセキュリティを計画、実装、および展開しなくてはならない医療機関にとって、シスコは優れたパートナーであると結論づけました。シスコ製品の種類の多さ、そしてその製品が提供するスケーラビリティ、保護、管理などの点から、シスコはセキュリティ市場で、実績のある革新者、そしてリーダーとして際立っています。シスコは、販売、技術、優秀なネットワークおよびセキュリティ専門家からなるコンサルティング チームなど、優れた経験と専門知識を提供しています。

シスコの統合型ネットワーク セキュリティ ソリューションの詳細については、次の URL をご覧ください。

http://www.cisco.com/jp/powernow/security/

CISCO SYSTEMS

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/go/contactcenter/
〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
TEL: 03-6670-2992
電話でのお問合せは、 以下の時間帯で受付けております。
平日 10:00 ～ 12:00 および 13:00 ～ 17:00

お問合せ先

05.03