

セントラルフロリダ大学

安全なキャンパスを実現するためのシスコとの取り組み

セントラルフロリダ大学 (UCF) は、フロリダ州オーランドに位置し、約 42,000 人の学生が、メインキャンパスおよび周辺の 21 のキャンパスで学んでいます。UCF は大都市圏の研究大学であり、教育、研究、サービスの包括的なプログラムを提供することを目的としています。コンピュータサイエンス、工学、光学、およびシミュレーションの優秀さで知られる UCF では、人種、民族、社会的経済力を問わず、さまざまな年齢の学生が、学士、修士、博士課程で質の高い教育を受けています。また、この大学には、発展中の新興ビジネスを支援するためのビジネス インキュベータ プログラムもあります。UCF は、インキュベータ プログラムを含むさまざまな方法で公共団体および民間企業と創造的なパートナーシップを築き、フロリダ州の経済的發展に貢献しています。



ネットワーク セキュリティの強化に対する UCF のニーズ

UCF のキャンパス データ ネットワーク は、ほぼすべての高等教育機関と同様に、教育、研究、管理サービス、およびキャンパスでの通信をサポートする重要なリソースとなっています。したがって、ネットワークの信頼性を最大限に向上させることが必須の条件になっています。インターネットに接続されたすべての組織が直面しているウィルス、サービス拒絶 (DoS) 攻撃などの脅威は着実に増加しており、ネットワークのセキュリティと監視を強化する必要があることは明白でした。



2000年初頭、Chris Vakhordjian氏は、ポリシー、テクノロジー、管理を含む、包括的なセキュリティプランの開発と実装を行うためのネットワークセキュリティ管理者としてUCFに招かれました。Vakhordjian氏の最初の仕事は、ネットワークのデバイス、プロトコル、セキュリティゾーンの総合的なマップを作成して、ネットワークの利用状況と脆弱性を徹底的に調査することでした。

第一の保護層：Cisco PIX セキュリティ アプライアンス

Vakhordjian氏は、UCF Network Operations Center DirectorであるRobert Scott氏とCisco® SystemsのエンジニアであるTim Ryanの協力を得て、エッジ用ファイアウォールを導入することからUCFのネットワークセキュリティ強化に着手することを決定しました。Vakhordjian氏と彼のチームは、コンピュータセキュリティ市場を調査して、製品評価を詳細に比較し、最終的にCisco PIX® セキュリティ アプライアンスを選択しました。Vakhordjian氏はこの決定について、「私たちがシスコを選んだ理由は、充実したサポートと、Cisco PIX セキュリティ アプライアンスの性能と、高度な機能です」と述べています。また、Vakhordjian氏はこう付け加えています。「Cisco PIX セキュリティ アプライアンスのトラフィック処理量とインターフェイス数の豊富さには強い印象を受けました。特に、フェールオーバー機能が魅力的でした。他社の製品ではUCFが必要としているすべての機能が満たされておらず、UCFのレベルのネットワークトラフィックを処理できる製品はほとんどありませんでした。」

Vakhordjian氏と彼のチームは、UCFのネットワークエッジに2台のCisco PIX 535 セキュリティ アプライアンスを実装しました。Cisco PIX 535 セキュリティ アプライアンスは、ギガビットイーサネットのスループットを備え、ステートフルファイアウォール機能とIP Security (IPsec) Virtual Private Network (VPN; バーチャルプライベートネットワーク)機能を統合した専用アプライアンスです。UCFが実装したPIX 535 セキュリティ アプライアンスのうち1台は、冗長化ホットスタンバイユニットとして機能しています。このフェールオーバー構成では、自動ステートフル同期機能によって同時接続が維持され、システム障害が発生した場合でもセッションが保持されるため、スタンバイファイアウォールへの切り替えはネットワークユーザに対して完全に透過的です。

また、UCFでは、イントラネットおよびインターネットの機密性の高い用途、およびユーザ数を保護するために、Cisco PIX セキュリティ アプライアンスをさらに導入しました。たとえば、Graduate Studies 事務局やBusiness Incubator 事務局などにCisco PIX 501 セキュリティ アプライアンスが追加されました。Cisco PIX 501 セキュリティ アプライアンスは、比較的小規模な環境用に設計されており、Cisco PIX 535と同様の堅牢なセキュリティ機能を備えています。また、College of Health and Public Affairsでは、Cisco Catalyst® 6500 シリーズスイッチにCisco Firewall Services Module (FWSM)が組み込まれました。FWSMは、Cisco PIX セキュリティ アプライアンステクノロジーをベースとした、Cisco Catalyst 6500 シリーズスイッチ用の高速な統合型ファイアウォールモジュールであり、5 Gbpsのスループットと、1,000,000の同時接続をサポートします。FWSMは、優れたセキュリティ、信頼性、パフォーマンスを企業に提供します。Vakhordjian氏はCisco PIX セキュリティ アプライアンスを導入したことについて「UCFでの経験から、PIX アプライアンスが正しい選択であったことが立証されました」と述べています。

第二の保護層：Cisco Intrusion Protection

Chris Vakhordjian氏は、Cisco PIX セキュリティ アプライアンスの導入には満足しましたが、アプライアンスだけでは常に変化するさまざまなセキュリティ上の脅威に対して、最高水準の保護を実現できないということを認識していました。Code Red ワームによる世界的な被害を熟知していたVakhordjian氏は、Code Redのような悪質な攻撃を防ぐために、侵入保護ソリューションを導入してファイアウォール機能を補完する必要があると考えていました。彼は再びシスコのセキュリティ専門技術に注目しました。



Cisco Intrusion Detection System (IDS) は、ワーム、DoS 攻撃、およびアプリケーション攻撃など、既知および未知の攻撃を正確に特定して分類するように設計されています。そのため、Cisco IDS では、ステートフルパターン認識、プロトコル分析、トラフィックアノマリー（異常）検知、プロトコルアノマリー（異常）検知などの複数の検出方式が採用されています。Cisco IDS は攻撃を正確に特定して分類した後、被害が発生する前に攻撃を阻止することができます。IDS では、パケットの破棄、セッションの終了、ルータおよびスイッチの Access Control List (ACL; アクセスコントロールリスト) の再設定、ファイアウォールポリシーの動的変更といった方法で、侵入者を「排除」することができます。

UCF では、2 台の Cisco IDS 4210 センサーをネットワーク エッジに実装しました。Cisco IDS 4210 センサー アプライアンスは、UCF ネットワークを通過するトラフィックのコピーを受信し、キャプチャしたパケットを分析し、それらを一般的な侵入行動（シグニチャ）と比較します。キャプチャしたパケットがルールセットで定義されている侵入パターンと一致した場合、センサーは管理コンソールにアラームを送信し、管理者の定義に従って自動的に対処します。エッジに展開した Cisco PIX セキュリティ アプライアンスと連携させるために、Vakhordjian 氏は、Cisco IDS の排除機能を利用するように Cisco 4210 センサーを設定しました。エッジに導入された 2 台の IDS アプライアンスは、Secure Shell (SSH) 接続によって PIX アプライアンスとリンクされ、Vakhordjian 氏が指定した信号に基づいて攻撃を排除します。その後、Vakhordjian 氏が排除レポートを調査して、ブロックされたトラフィックを確認します。Vakhordjian 氏はこの排除機能について、「これは、Cisco PIX セキュリティ アプライアンスと Cisco Intrusion Detection System のすばらしい機能の 1 つです」と述べています。彼はまた次のようにも述べています。「私は、これらのアプライアンスを高く評価しています。どちらの製品もスループットに優れているので、将来的なトラフィックの増大にも十分に対処できるでしょう。」

また、UCF のセキュリティ チームは、コアの Cisco Catalyst 6500 シリーズ スイッチに Catalyst 6500 IDS Services モジュールを統合しました。これにより、スイッチのバックプレーンからトラフィックを直接分析できるようになりました。Catalyst 6500 IDS Services モジュールは、スタンドアロン型の IDS センサーと同様に、ネットワークを通過する不正なアクティビティを検出し、検出したイベントの詳細とともにアラームを管理コンソールに送信します。このモジュールは、各 Cisco Catalyst 6500 シリーズ スイッチのスロットを 1 つしか占領せず、スイッチのパフォーマンスには影響を与えません。UCF での帯域幅需要が増加し、監視が必要なトラフィックが増大したときは、スイッチ シャーシにモジュールを追加するだけでそれらに対処することができます。

「Cisco IDS の初期設定作業は比較的簡単でした。私にとっては "ごく単純な" 作業でした」と Vakhordjian 氏は述べています。侵入検知システムの管理と日常のメンテナンスも彼にとっては簡単な作業です。Vakhordjian 氏は、CiscoWorks VPN/Security Management Solution (VMS) を使用して、アラートを参照し管理しています。CiscoWorks VMS では、IDS モジュールから送信される情報が相互に関連付けられるため、管理者は事前に対策を講じることができます。Vakhordjian 氏は、IDS によって生成されたアラームを調査するための体系的なプロセスを確立しました。彼は、アラームをさまざまな攻撃タイプのカテゴリに分類し、「優先度の高い」アラームとして分類されるものに重点を置いています。また、それらのアラートについてのレポートを毎日作成しています。

Vakhordjian 氏は、将来的に Cisco Threat Response テクノロジーを導入して、IDS の日常管理業務をさらに簡素化しようと考えています。これにより、誤ったアラームがほぼ一掃され、迅速な注意が必要な脅威を自動的に特定することが可能になります。Vakhordjian 氏は、侵入保護システムの導入について次のように述べています。「IDS は非常に重要で、ネットワーク上の監視カメラのようなものです。IDS がなければ、厳しい状況になるでしょう。私は IDS を高く評価していて、可能な限り多くの IDS をインストールしたいと考えています。」



安全なアクセス：VPN とワイヤレス

効率のよい研究環境の実現に取り組んだ結果、UCFの学生は、キャンパス内のほぼすべての場所からオンラインで作業ができるようになりました。UCFのITチームは、ワイヤレスインフラストラクチャを構築し、100台以上のCisco Aironet® 1200シリーズおよび350シリーズアクセスポイントを設置して、図書館、教室、屋外の中庭など、ほぼすべての場所からインターネットにアクセスして、研究、学習、電子メールの送受信などを行える環境を実現しました。

UCFでは、ワイヤレス接続のセキュリティを確保するために、VPNによるネットワーク接続の暗号化を学生に対して奨励しています。また、同大学では、教職員に対しても、自宅や乗り物の中から作業を行えるVPNテクノロジーを提供しています。UCFは、VPN接続でのリモートアクセスを可能にするために、インターネットなどのTCP/IPネットワークを介して安全な接続を確立するCisco VPN 3030 Concentratorを導入しました。Cisco VPN 3030 Concentratorは、クライアントソフトウェア付属のリモートアクセスVPNプラットフォームで、 Availability、パフォーマンス、スケーラビリティに優れ、最新の暗号化技術と認証技術をサポートしています。この製品は、現場交換およびお客様ご自身でのアップグレードが可能なコンポーネントで構成されるスケーラブルなプラットフォームなので、UCFでは、学生や教員によるリモートアクセスおよびワイヤレスアクセスの需要が高まるにしたがって、サポート可能なユーザ数を簡単に増やすことができます。

UCFにおける新しいセキュリティ感覚

Chris Vakhordjian氏は、セキュリティポリシーを作成し、保守、監視、および学生や教員への普及活動を継続的に行うことで、これらのテクノロジーを補完しています。UCFのセキュリティポリシーは、Vakhordjian氏が実装したすべてのソリューションを統合し、継続的に適用される安全対策は、UCFの教員、スタッフ、寄宿生によって固く守られています。

広範囲に渡るネットワークのセキュリティ強化を実施し、3年以上が経過した現在、UCFの経営陣は、大学のデータと信用性が内部および外部のリスクから十分に保護されているという安心感を得ています。Chris Vakhordjian氏は、日常のセキュリティ管理業務に従事すると同時に、最も効率のよい最新のシスコセキュリティソリューションをUCFで展開できるようにシスコとの協力関係を継続しています。彼は、シスコによる継続的なサポートを高く評価して、次のように述べています。「私は、シスコから多大なサポートを受けていて、彼らとの協力関係にはたいへん満足しています。彼らはクライアントをほんとうによくサポートしてくれます。」

©2004 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。
この資料に記載された仕様は予告なく変更する場合があります。



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.03-6670-2992

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

お問い合わせ先