



統合データセンターのネットワーク基盤を刷新し、 ネットワークの柔軟性向上と 強固なセキュリティを実現

学校法人東京電機大学

●導入の背景/課題

- 従来のネットワーク機器は、コアのスイッチと末端のスイッチが別々のベンダーで管理しずらく、これを統一したかった。
- コアスイッチの機能が限られ、柔軟なネットワーク構成への対応に限界があった。
- 機能を付加しようとする別のベンダーの製品をコアスイッチに接続するしかなく、運用管理が煩雑になるのでそれを避けたかった。
- インターネット接続の際、必ず神田キャンパスを経由する構造になっていたため、神田キャンパスのトラブルが他キャンパスのインターネット接続に影響していた。
- 学生の私物のPCがネットワークにアクセスするため、万一ウイルスやワームに感染したPCがアクセスしても学校のネットワークに影響が出ず、自動的に回避できるしくみが必要だった。

●導入ソリューション

- IPネットワーク
 - Cisco Catalyst 6506
 - Cisco Catalyst 6500 スイッチ Anomaly Guard モジュール
 - Cisco Catalyst 6500 スイッチ Traffic Anomaly Detector サービス モジュール
 - Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール
 - Cisco Catalyst 6500 シリーズ コンテンツマネージメントモジュール
 - Cisco Catalyst 3750
 - Cisco Catalyst 2960
- セキュリティソリューション
 - Cisco VPN 3005 コンセントレータ
 - Cisco PIX セキュリティ アプライアンス

●導入効果 (期待される導入効果)

- ネットワークの仮想化が実現し、論理設計と物理設計を分けることができたので、ネットワークの柔軟性が向上し、新たな要求に迅速に対応できるようになった。
- ネットワークの仮想化によりソフトウェアだけで構成変更ができるので、現地に行かなくてもさまざまな設定変更などが可能になった。
- シスコのネットワーク機器は、コアからエッジまですべて基本ソフトが同一なので、ひとつのインタフェースですべてのスイッチを設定でき、管理が容易になった。
- DDoS攻撃やボット攻撃を自動的に検出し、通信を迂回させることが可能になり、手間をかけずにセキュリティの強化を図ることができた。
- 各機能を分離することにより、問題が起きても他の機能に影響しないようになり、ネットワーク全体の可用性が向上した。

東京電機大学は、1907年に創立され、今年100周年を迎える理工系の総合大学である。キャンパスが東京千代田区神田、埼玉県鳩山町、千葉県千葉ニュータウンと3つに分かれ、学生が約10,000人、大学院生約1,000人が学んでいる。同大学では1992年という早い時期から全学にネットワークを構築し、以降約5年ごとに見直しを行っている。今回の見直しでは、主にネットワークの柔軟性向上とセキュリティの強化を目指し、「Cisco Catalyst 6506」を導入。「コンテンツスイッチングモジュール」により仮想化されたサーバへの最適なアクセス環境を実現し、より柔軟なネットワークの構成変更を可能にすると共に、「Anomaly Guardモジュール」と「Traffic Anomaly Detectorモジュール」により、DDoS攻撃やボット攻撃を自動的に検出し、問題のトラフィックだけを迂回させるという強固なセキュリティを実現した。

従来のコアスイッチの限界とセキュリティの強化が課題

東京電機大学は、1989年から実験的にインターネットの利用を始め、92年に全学でネットワークを構築するなど、先進的なネットワーク利用を行ってきた。今や財務や人事など法人としての基幹業務はもとより、教育研究にもITは不可欠で、学生の履修届けや図書館の書籍予約などもPCから行うため、万一止まるとその影響は非常に大きい。

同校が2001年に導入したネットワーク機器は、コアと末端のスイッチが別々のベンダーで使いく、コアスイッチの機能が限られていたために、柔軟なネットワーク構成への対応に限界があった。また、ファイアウォールなど他の機能を付加しようすると、他ベンダーの製品を接続するしかなく、障害の切り分けと運用管理が煩雑になるという問題があった。

また、インターネットに接続する際は、どのキャンパスからアクセスしても、すべて神田キャンパスのローカルエリアネットワークを経由する構造になっていたため、同キャンパスのネットワークにトラブルがあると、他キャンパスのインターネット接続にも影響が出ていた。

加えて、学内にある情報コンセントに同大学の学生が自由に自分のPCを接続できるというセキュリティポリシーのため、セキュリティ上の課題があった。情報コンセントに接続する際に接続認証は行っているものの、学生のPCが確実にセキュリティ対策が施されている保証はない。従来も、万一ウイルスやワームに感染したPCがアクセスするとアラートがあがる仕組みにはなっていたが、その度に担当者が対応する必要があり、運用上の大きな負荷となっていた。東京電機大学 総合メディアセンター 技師 橋本明人氏は、「かといって、1万人を越えるユーザに対してエージェントを配布して、アクセスできるPCを制限することは不可能です。企業のように会社の資産であれば可能でしょうが、学生のPCは私物ですから、そこまでの面倒は見られません。また、端末のOSも統一できません。そうはいつても、感染がネットワークに広がると困るので、万一感染したPCがアクセスしても、学内ネットワークに影響が出ず、自動的に回避できるしくみが必要でした」と語っている。

「Cisco Catalyst 6506」に多彩なサービスモジュールを付加することで、ネットワークの柔軟性向上と強固なセキュリティを実現

学校法人東京電機大学



「以前は事務用と研究用の線が別で、レイアウト変更の度に引き直していました。今は線さえあれば、ソフトウェアの設定変更だけで対応できるので、今後いろいろな要求に柔軟に対応できます」

学校法人東京電機大学
総合メディアセンター（企画・推進担当）
課長
佐藤 龍 氏

「Cisco Catalyst 6506」の高度な機能と、さらに機能を付加できる多彩なサービスモジュールを評価

そこで同校は、2005年4月から検討を開始し、データセンターの集約とネットワークの刷新を図ることとした。2006年1月にはネットワーク機器をシスコにすることを決定し、同年6月に末端の機器から徐々に入れ替えを始め、2006年8月に構築を終えた。

同校がシスコのネットワーク機器を選じたのは、コアスイッチ「Cisco Catalyst 6506」そのものの高度な機能と、さまざまなサービスモジュールが用意され、この一台で高度なネットワーク環境を実現できる点を評価したからだ。橋本氏は、「機能ごとに機器をつないでいくとマルチベンダーになってしまいますし、物理結線ができるため構成の変更がソフトウェアでは行えません。その点、Cisco Catalyst 6506は、多くのサービスモジュールが揃っており、それらを追加するだけでさまざまな機能を付加できるので、そこを評価しました」と語っている。

また、運用の手間を軽減するため、ブロック内のネットワーク機器は単一ベンダーにしたいという考えがあり、コアからエッジまで製品ラインナップが揃っている点も評価した。さらに橋本氏は、「シスコはホワイトペーパーなどのドキュメントが充実しており、ネットワークの構成を考えるうえで非常に参考になりました。特にデータセンターに関するホワイトペーパーから、今回の構成の発想を得ることができました」と語っている。

ネットワークの仮想化と、DDoS攻撃やボット攻撃を自動回避する機能をサービスモジュールで実現

今回構築したネットワークは、各キャンパスのネットワーク、データセンター、インターネット接続の各機能のコアスイッチにそれぞれ「Cisco Catalyst 6506」を、キャンパス間接続には「Cisco Catalyst 3560」を利用している。

データセンターの「Cisco Catalyst 6506」には「コンテンツスイッチングモジュール」を搭載。これにより仮想化されたサーバへの最適なアクセス環境を実現し、より柔軟なネットワークの構成変更を可能にした。また、インターネット接続の「Cisco Catalyst 6506」には、「ファイアウォールサービスモジュール」と「Anomaly Guardモジュール」、「Traffic Anomaly Detectorモジュール」を搭載し、高速なインターネット接続と高度なセキュリティを両立している。

特に、「Anomaly Guardモジュール」、「Traffic Anomaly Detectorモジュール」は、インターネットからのDDoS攻撃（分散型サービス拒否）とイントラネットからのボット攻撃（キャンパスのネットワークに接続されたウイルスに感染しているPCの外部への攻撃）への防御に高い効果を発揮する。まず、DDoS攻撃やボット攻撃などの異常なトラフィックがネットワークに侵入すると、「Traffic Anomaly Detectorモジュール」がこれらを自動検出し、「Anomaly Guardモジュール」の自動起動を行う。そして、「Anomaly Guardモジュール」が、攻撃と判断されたトラフィックだけを迂回させ、正常なトラフィックと分離することでサービスの継続性を実現している。さらに、この検出において



学内に設置された「情報コンセント」を利用し、パソコンを使用する学生たち。

「Cisco Catalyst 6506」に多彩なサービスモジュールを付加することで、
ネットワークの柔軟性向上と強固なセキュリティを実現

学校法人東京電機大学



「Cisco Catalyst 6506 は、多くのモジュールが揃っており、それらを追加するだけでさまざまな機能を付加できるので、そこを評価しました」

学校法人東京電機大学
総合メディアセンター（企画・推進担当/鳩山キャンパス担当）
技師
橋本 明人 氏

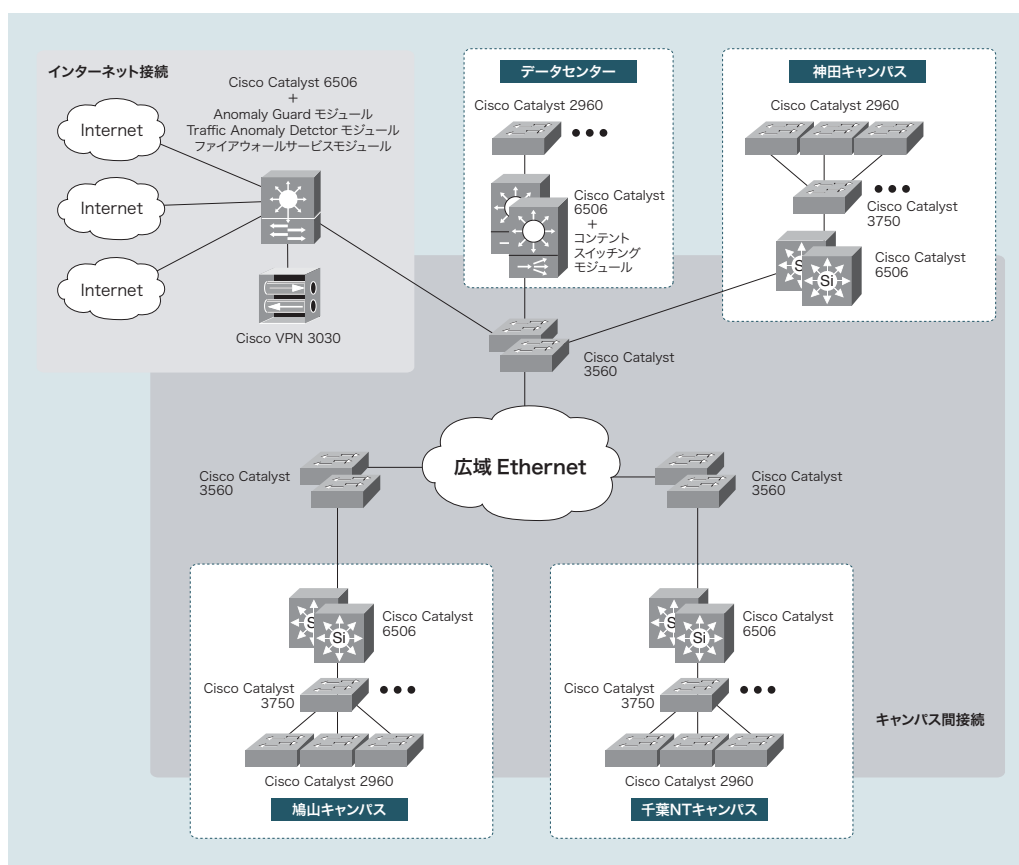
ウイルスに感染しているPCを特定する。

橋本氏は、「よくDDoS攻撃への対処に利用されるIDS（不正侵入検知）は、既知の攻撃は検知しますが、トラフィックの傾向が異常でも未知の攻撃は検知できません。しかし、多くのネットワークトラブルは、異常なトラフィックが流れたときに起きるので、未知でも異常なトラフィックなら、それを検知して隔離することが重要です。その点、Traffic Anomaly DetectorモジュールとAnomaly Guardモジュールは、トラフィックの異常を素早く検出して対処するので、安心して任せられます。初期設定が容易だったのも、よかったですね」と語っている。

同大学では、ウイルスに感染したPCを学内ネットワークにつないだ学生に対し、教育的な観点からネットワークの利用権を止め、クリーンになったことを担当者が確認できるまで再びアクセスさせないように指導し、高いネットワーク・リテラシーを保っている。東京電機大学 総合メディアセンター 課長 佐藤龍氏は、「もし本学が少人数の文系の大学なら、個人のPCも守るべきなのかもしれません。しかし、理工系の大学であり、多くの学生が卒業後はエンジニアとして社会に出て行きます。それを考えると、温室で守るのではなく、自分で自分の持ち物を守る術を、多少痛い目をみなが



学内の待合室で無線LANを使用する学生たち。



「Cisco Catalyst 6506」に多彩なサービスモジュールを付加することで、ネットワークの柔軟性向上と強固なセキュリティを実現

学校法人東京電機大学

らでも学んでもらう方が、教育的にも有効だろうと考えました」と語っている。

ネットワークの柔軟性と保守性、セキュリティの強化を実現

東京電機大学が今回のネットワークによって得たメリットは、4つある。

まずひとつは、柔軟性の向上である。ネットワークの仮想化により論理設計と物理設計を分けることができ、たとえば急にある部屋でテレビ会議を行いたいと言われても、物理的な設計を変更することなく、簡単に対応できるようになった。ネットワークは、学内全体で200以上のVLANで分かれており、異常箇所の検出も容易になった。

2つめが、保守性の向上である。仮想化によりソフトウェアだけで構成変更ができるので、現地に行かなくても設定や変更が可能になった。特にキャンパスが3カ所に分かれているので、この効果は大きい。さらに、「Cisco VPN 3005」を利用して、インターネット経由での設定変更も可能にしている。また、シスコのネットワーク機器は、コアからエッジまですべて基本ソフトが同一なので、同じインタフェースですべてのスイッチを管理できる。個々に機器の操作を覚える必要がなく、管理が容易になった。

そして3つめが、セキュリティの強化である。ウイルスやDDoS攻撃などのネットワークの脅威を検出し、自動的に通信を迂回させることが可能になり、手間をかけずにセキュリティの強化を図ることができた。また、検出から異常なトラフィックの隔離までを自動的に行うため、担当者が居なくても対応可能で、DDoS攻撃を原因とするパフォーマンスの劣化が起こらなくなった。

最後は、機能分離による可用性の向上だ。各キャンパスのネットワーク、キャンパス間接続、データセンター、インターネット接続をそれぞれ機能分離しパッケージ化することで、問題が起きても他の機能に影響しなくなり、ネットワーク全体の可用性が向上した。

柔軟で拡張性のあるインフラにより 要求にあわせたサービス提供が可能に

東京電機大学は、今回のネットワーク再構築により、柔軟で拡張性のあるインフラを手にすることができた。橋本氏は、「当面はどんな要求にも応えられるインフラができたと考えています」と胸を張る。佐藤氏も、「事務所の移動などを行う場合、以前は事務用と研究用の線が別々だったので、レイアウトを変えるとそれに合わせて線を引き直すなど物理的な構成変更を行う必要がありました。しかし、今は線さえあれば、あとはソフトウェアの設定変更だけで対応できます。そういうインフラができたことで、今後いろいろな要求に柔軟に対応できます」と語っている。

同校は、今後この情報基盤を活用し、学内の約12,000名のユーザに対し、より優れたサービスを提供していくことだろう。

Profile

学校法人東京電機大学

所在地: 東京都千代田区神田錦町2-2

創立: 1907年

東京電機大学は、1907年東京・神田に創立された電機学校を母体とし、戦後1949年に開設された。初代学長はFAXの開発者として名高い丹羽保次郎博士で、丹羽博士の言葉である「技術は人なり」を教育・研究理念に理工系総合大学として発展を遂げてきた。創立以来の「実学尊重」教育と「技術は人なり」の理念で、技術で社会に貢献する人材を数多く世に送り出している。2007年には創立100周年を迎え、新たに「未来科学部」を新設するなど、ますます成長を続けている。

<http://atom.dendai.ac.jp/>

©2007 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料の記載内容は2007年6月現在のものです。

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

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先 (シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間: 平日 10:00~12:00、13:00~17:00

お問い合わせ先