

Case Study



[導入事例]

京都大学が導入した セキュリティ性に優れた KUINS-III と 日本初の 10Gbit ネットワーク

京都大学

京都大学は、1987年から3年間をかけて国立大学としては初となった本格的な情報通信ネットワークシステム(KUINS-I: Kyoto University Integrated information Network System-I)を構築。96年には、ATMによる超高速ネットワークシステム(KUINS-II)を本格運用するなど、ネットワーク先進大学として学術情報基盤の整備を行ってきた。そして今年4月には、日本初の超高速10Gigabit イーサネットの導入と同時に、セキュリティ面でも堅牢で安定性の高い新世代ネットワークシステム KUINS-III の運用を始めた。

コンセプトはセキュリティを 徹底的に高めること

京都大学のキャンパスコンピュータネットワークは87年から3年をかけて構築された。東北大学と並び国立大学としては初めての本格的な学内ネットワークである。専任の担当官を置かず、さま

ざまなセクションの教官や事務系の職員などがいわばボランティア的にネットワークの管理運用を行ってきた。そんな状況の中でも、基幹ループLANなどは確実に進化を遂げていく。KUINS-Iと名付けられたネットワークはその後KUINS-IIとなり、ATMの導入でさらに高速化される。これらのネットワークは国内外との情報通信を支えることで、多くの研究に貢献してきた。しかし注目度が高い分、スーパーコンピュータや学内にある1万台をはるかに超える多数のコンピュータは、常に外部からの不法侵入などの危険にさらされることとなる。実際に京都大学ではかなりの数の攻撃に合い、奇しくもシスコのネットレンジャーが大活躍したということも多数あったのである。

そこで京都大学ではKUINS-IIのほかに、セキュリティ面を強化した新しい高速ネットワークシステムKUINS-IIIを構築することとなった。2001年に情報ネットワーク危機管理委員会を立ち上げ、そこでセキュリティ強化の計画が進められた。とはいえ、すべてのネットワークを一から作り替えるのではなく、これまでのネットワークは従来通り運用しつつ、セキュリティのより強固な新しいネットワークを追加する形となっている。

「京都大学ではネットワーク改革が進んできました。そのひとつの表れが危機管理委員会であり、組織としては学術情報メディアセンターなのです。学術情報メディアセンターは大型計算機センター、総合情報メディアセンター、KUINS機構の統合によって生まれた組織です。結果的に組織の構築とKUINS-IIIの導入は同期が取れました。学術情報メディアセンターを作ること、その時



学術情報メディア
センター長
松山 隆司 教授



のネットワーク基盤がしっかりしたものであること、セキュリティのモニタリングも十分に行い旧常的なネットワークとしても安全であること。この3本セットがかみ合っただけの形ができてあがりつづきます」と学術情報メディアセンター長・松山隆司教授は語ってくれた。

KUINS-IIIは外からの通信を直接行わせないことにより、堅牢なセキュリティを確保している。KUINS-IIIから既存のKUINS-IIへアクセスすることはできるが、KUINS-IIからKUINS-IIIへのアクセスは禁止されている。外部からKUINS-IIIに直接アクセスできなくすることで、KUINS-IIIはあくまでも独立したネットワークとして存在することになる。自由度より先セキュリティを重視した学内ネットワーク、これがKUINS-IIIのコンセプトである。

ただし、学外ネットワークであるWebやFTPへは、外部のサーバセグメントに置いたプロキシサーバを中継して接続できるようになっている。ま

た既存のKUINS-IIとの並行運用により、研究に必要な自由度は従前通り確保されている。もちろん、外部との接続を行うKUINS-IIやサーバセグメントのセキュリティ対策も十二分に行っている。京都大学直轄の研究所や観測所などの遠隔地に関しては、事務データなどのデータを外部へ流すことがないように、遠隔地接続ルータによってIPsecで暗号通信を行っている。

Catalystが多数のVLANを支える

システムそのものは5000ものVLAN(Virtual LAN)を作り、外部との接続を考えていないため、DHCPによるプライベートIPアドレスを使用し運用が行われる。キャンパス全体で5000にもなるVLANを一元で管理するのは困難なため、基幹スイッチのCatalyst6509とCatalyst6513の計9台を割り当て、基幹スイッチ1台で600個から800個のVLANを運用する形をとる。館内スイッチにCatalyst3508を201台、末端スイッチには

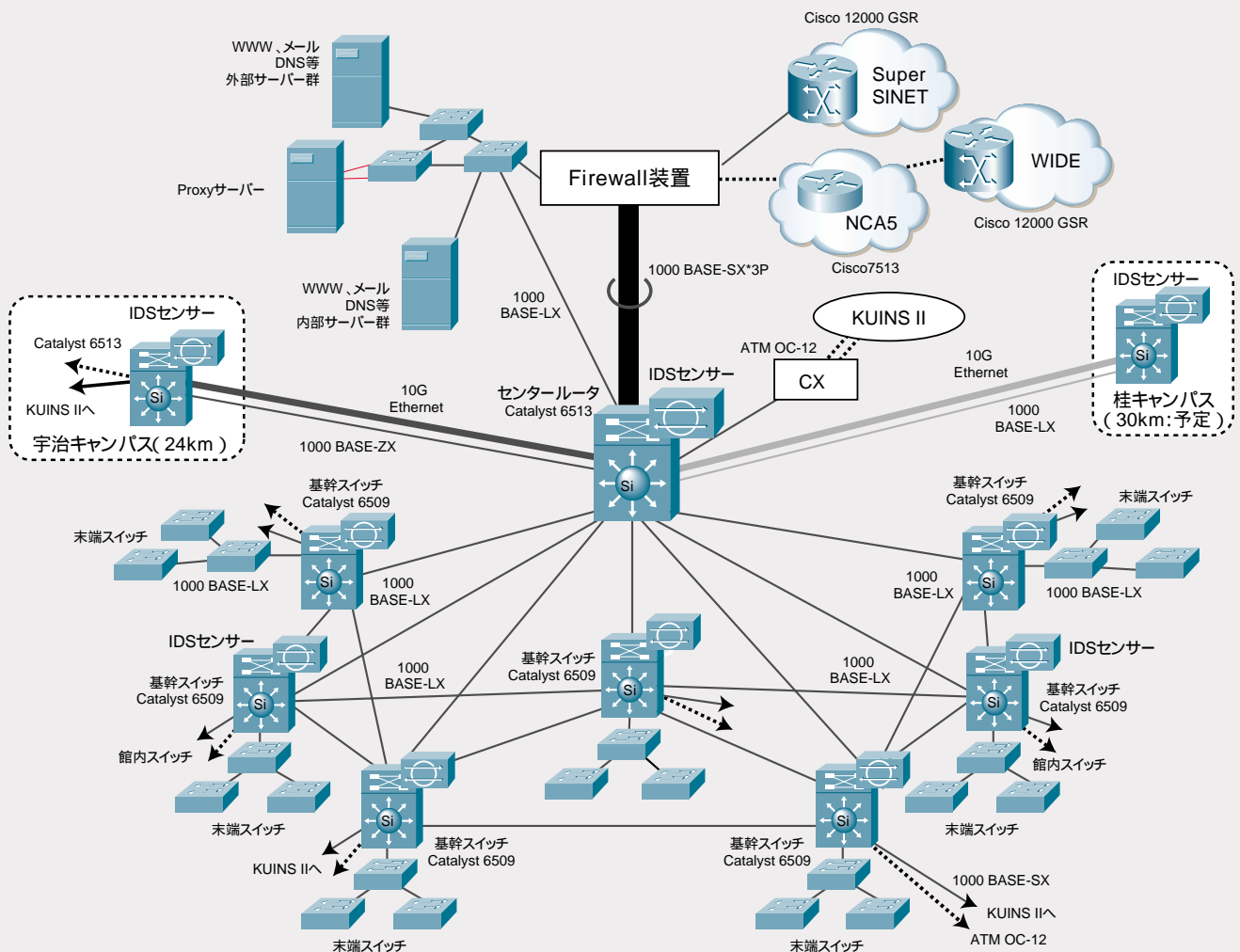
Catalyst3512、3524、3548を合計679台導入している。学内の各部屋や廊下などには情報コンセント16000個が設置されている。情報コンセントは、フタの色が黄色と緑の2種類に分けられている。緑はKUINS-III専用で外部への直接の通信は行えない。黄色の方はKUINS-IIIでも、KUINS-IIのセグメントでも使用が可能だ。

既存の学内ネットワークは建物にひとつのサブネットで、ネットワーク内部は共通のポリシーで運用されていた。今回のKUINS-IIIは小さなVLANを多数使うことで、同じ建物内であっても廊下や部屋ごとに細かく区切る形態となっている。それは、部局や教官によってネットワークやセキュリティの考え方に相違があるため、各セクションできめ細かな制限をかけられるシステムが必要だったためだ。

館内は1Gbitのイーサネット、末端は100Mbpsのイーサネットで接続される。館内のネットワークについてはVLAN間の通信は原則と

京都大学システム構成図

日本初の10Gbitの超高速ネットワークは、現在吉田キャンパスと宇治キャンパス間を結んでいる。近い将来には吉田キャンパスと桂キャンパス間でも10Gbitのネットワークが構築される



して行えず、担当教官などから運用者に対してプリンタやファイル共有などの申請があった場合に関しては、VLAN間でのルーティングが許可されるようになっている。つまり、使える場所や使える機能を運用者である学術情報メディアセンターがきめ細かく管理することができるのだ。たとえば、一方的に教官が学生の部屋へアクセスでき、学生が教官の部屋にはアクセスできないようにするといった設定も可能となっているのである。ただし、メールのやりとりなどに支障が出ないように、学内のグローバル系のネットワークサーバに対してアクセスすることは可能だ。

また、KUINS-IIIは外部への通信を行わない前提でシステムを構築しているため、完全なプライベートIPアドレスを利用している。接続されるPCのほとんどがノートパソコンであることを前提に、固定IPアドレスは基本的に使用していない。とはいえ、ファイルサーバやプリンタのIPアドレスが頻繁に変わるのはいきにくい。そこで学術情報メディアセンターでは、各セクションから申請が出た必要台数分の固定IPアドレスをVLANごとに変えて発行するといった対応も行っている。

「自由なネットワークを得るためには、それなりに責任が生じることになるというのが基本的な考え方です。そのため、VLANのひとつひとつに責任者を立ててもらおうと各部署に要請を行っています。責任者は教職員とし、VLANの中で起こったことに関しては法的な責任を負ってもらうことを説明しています」と学術情報メディアセンターネットワーク研究部門の岡部寿男教授は語っている。

KUINS-IIでは各建物までのネットワークに対して学術情報メディアセンターが責任を持っていた

が、KUINS-IIIでは各部屋や廊下などに設置されている約16000のコンセントまでの責任を持つことになる。そこから先はVLANの責任者の管理下に置かれるというわけだ。VLANシステムを細分化し、責任の所在を明確にしている点も新しい学内ネットワークの運用システムといえるだろう。「その結果、学内でのセキュリティに関する意識が非常に高まっており、これまでのネットワークから新しいネットワークシステムに積極的に切り替えて使用する人も増え、我々としてもさらに責任を感じています」と学術情報メディアセンターネットワーク研究部門の高倉弘喜助教授は言う。

シスコ製品の信頼性の高さが

KUINS-IIIを支える

今回のネットワーク構築に際しては、京都大学が機器の選定を直接指示したわけではなく、必要なシステムやスペックの仕様書に基づき入札を行った。その結果、学内ネットワークはシスコのユニットによって構築されることとなった。

「安全にネットワークを運営したい、技術的な冒険をするのではなく実績のあるユニットを導入してほしいという要望は出していました。実験でのデータがいかによっても実運用時に半分くらいのスペックになってしまうのでは困るということもご担当の方にお伝えしました。とにかく安全であること、安定していること、これがKUINS-IIIの根幹なのです」と学術情報メディアセンターデジタルコンテンツ研究部門の沢田篤史助教授は語る。京都大学側としては信頼性と安定性、そして性能の高いユニットを求めており、シスコの製品はその要望にマッチしたといえる。「シスコには日頃から



学術情報メディアセンター
ネットワーク研究部門
岡部 寿男 教授



学術情報メディアセンター
ネットワーク研究部門
高倉 弘喜 助教授

堅牢なセキュリティを確保するKUINS-IIIはシスコの製品が支えている





学術情報メディアセンター
デジタルコンテンツ研究部門
沢田 篤史 助教授

ソフトやハード面に関してさまざまな情報提供をいただいており、非常に助かりました」と岡部教授は言う。

「ユニットに対する機能的な要望なども伝えやすいし、それにシスコ製品は製品の世代が変わってもコマンドやインターフェースの継続性がある。そういう点を高く評価しています。また将来、ネットワークの管理を外部に委託するというケースがあったとしても、KUINS-IIIのメインユニットはすべてシスコ製なので外注管理がしやすいともいえます」と沢田助教授はシスコに対しての印象を語っている。

京都大学の学内ネットワークの特徴でもある日本初の10Gbitの超高速ネットワークは、現在吉田キャンパスと宇治キャンパス間を結んでおり、近い将来には吉田キャンパスと桂キャンパス間でも10Gbitのネットワークが構築される。この10Gbitのネットワークに関しては将来のさまざまな情報サービスを念頭に置いて、現段階で最善のネットワークを構築するという観点から導入に踏み切った。

このネットワークの管理運営を行う学術情報メディアセンターはネットワーク研究部門、コンピューティング研究部門、教育支援システム研究部門、

デジタルコンテンツ研究部門の4つを大きな柱として構成されている。学術情報メディアセンターはe-Universityの実現に向けて、強力なIT研究開発体制と確固たる情報基盤を確立し、学術の研究教育の現場とネットワーク社会をシームレスに繋いでいこうとしている。

研究・教育現場でのネットワークの未来について松山教授はつぎのように語っている。

「ビデオなどを活用したメディア系の遠隔講義も臨場感のあるものにし、オンライン上での講義とデジタル化された教科書をどうやってリアルタイムにリンクさせるかなど今後の課題はたくさんあります。それらのメディア系のコンテンツをリアルタイムで流すためには、超高速のネットワークが必要です。今後は学内ネットワークもリアルタイムで流す必要性がさらに高まっていくはず。それが現実のものとなったとき、ネットワークは研究・教育の基盤になったといえるのではないのでしょうか」

安全性と信頼性が高く、なおかつグローバル性も両立させた新しいスタイルの学内ネットワークは最新のシスコ製品が支えている。この学内ネットワークシステムは今後、他の大学ネットワークや地域ネットワークのモデルケースとなるであろう。

Profile

京都大学

新しい学問を創造することを目的として明治30年に設立される。ネットワーク先進大学として学術情報基盤の整備を率先して行う。2002年4月、日本初の超高速10Gigabit イーサネットの導入と同時に、セキュリティ面でも非常に堅牢で安全性と安定性の高い新世代ネットワークシステム KUINS-IIIの運用を開始した。

〒606-8501 京都市左京区吉田本町
<http://www.kyoto-u.ac.jp/>

©2002 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。

その他、記載されている会社名、製品名は各社の商標、登録商標または登録サービスマークです。

この資料の記載内容は2003年5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

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: 03-6655-4433

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

お問い合わせ先