香川大学ネットワークシステムの今昔

今井 慈郎[1]　山下 俊昭[2]　川口 政秀[2]　土居 敬典[3]　高橋 岳水[4]
Y.Imai[1]　T.Yamashita[2]　M.Kawaguchi[2]　Y.Doi[3]　T.Takahashi[4]
（総合情報センター[1]，情報グループ[2]，農学部会計係[3]，医学部情報ネットワーク管理室[4]）

１．まえがき

現行「香川大学ネットワークシステム」（以下NS）は平成最後（その次の世代への架け橋）でもあり、ここで少し回想することも許されると考え現在から過去を振り返りつつ、「今昔」を述べる。すなわち、二世代前から現行NSへの流れをまとめておきたい（ページ数が２倍となった）。

この十有余年はセキュリティ対策と防災対策の世相を反映した時代であったことを再認識している。MS Blasterの出現から否応なしでセキュリティ対策を、兵庫県南部地震から東日本大震災大津波へと厳しい時代から防災対策を、意識したネットワーク構築の急務となった。高速性や高機能性が「計算環境」とほぼ同様に追及されていた要求仕様が、徐々に、いやむしろ急激に上記の２つの必須項目重視へと舵をきることになった。

もちろん、分散キャンパスという特徴を持つ本学においては、ネットワーク環境は「ネットワークシステム」と「キャンパス間高速通信」との両輪が相補的に機能することが不可欠であり、今や遠隔会議や遠隔教育が常態化（必要インフラ）とみなされる状況となり、NSの要求仕様の中核であることも事実である。従って、本稿で扱う項目としては、「セキュリティ対策」「防災対策」「キャンパス間高速通信」の流れが現行NSへとどのように受け継がれてきたか、という今昔物語とも言えるかもしれない。以下ではこれら３つの項目についてこれまでの変遷を俯瞰する。

２．セキュリティ対策とファイアウォール

三世代前になるがコンピュータウイルスという言葉が社会に衝撃を持って認識されたのは、その爆発的に拡大する影響力（悪影響）と他人事ではないという心理状態からであったかもしれない。事実、夏季休業を地元で過ごした学生が新学期でキャンパスに集うと授業より先にウイルス対策を強いられるような事態はまさに前代未聞の珍事となっていた。キャンパス間にもセキュリティ対策が必要との認識をもたらした（それまで大学の内と外を開閉する番兵的な「ファイアウォール（以下F/W)」はお飾りではないにしても「一応設置しておくもの」程度の認識であったと記憶している。しかし、コンピュータウイルスの衝撃は、それでは役に立たないことも明確になった。同時に"UTM(Unified Threat Management)"という聞き慣れないキーワードを耳にし始め、1台数百万円以上もする機器を各キャンパスの入り口に配置することでウイルスの不正侵入感知や抑制ができるとの触れ込みで、二世代前のNS構築の１つの目玉になっていった。

少し話が前後するが20世紀最後の工学部と銘を打って創設された香川大学工学部では学生個人所有ノートPCを１つの特徴としていたので，IP接続してネットワーク環境を利用するためDHCPサービスが不可避であった。しかし、残念ながらウイルス対策が完全表裏一体とはなっておらず、ある意味、平和な時代だったとも言えた。従って、本格的セキュリティ対策はやはり二世代前のNSから始まったとする認識を持っている。

しかし、今からすれば不思議なことながら、当時は「一度導入すればレンタル期間中は大丈夫」との安心感がセキュリティ対策機器に対しても例外なく適応されていたように思われる。もちろん実情がそれを徐々に許さなくなっていったのは周知の事実である。メールサービスは別、Webサービスは別・・と次々に追加増資でセキュリティ機器の導入更新を迫られることで、導入時の検討事項をはるかに超える運用時の膨大なケアに忙殺されていったことで、「これがグローバル化の実態か」との感慨を新たにした。

運用規則を如何に効率的に設定し、適切に進捗させるか、は「セキュリティポリシー」が重要であるとの認識が学内外に起こり、しかも時代に即応して動的に変化できること（より正確には単なる「機能増減」ではなく、新規機能を渋滞なくリ

アルタイムに運用中のシステムへ導入できる体制作りを可能とすること）が再認識され、固定的な機能のF/Wの時代から戦略的なF/Wの時代に大きく進化したのが先代（一世代前）からである。
その意味では現行NSのF/Wと同一メーカーの製品(Palo Alto Networks)であり、現在世界最高水準のF/W専用メーカーの製品を導入し、運用してきた。これは決して「最高水準なのだから仮に支障があっても我慢して欲しい」等と訴えようとしている訳ではないが、１台数千万円もする機器をDual System構成として採用するとコスト高を招来する象徴とも言える。しかし、NSにはこのような機能が不可欠となっている状況をご理解いただきたいと、心の底で祈念していることも事実である。NSに関する紹介を中心に行っているのでセキュリティ機能の詳細までには言及しないが、現行コンピュータシステムの一部として導入されている「spamメール対策機器」と相補って本学のセキュリティ対策の根幹をなしている事実と実績は大きい。先に述べた二世代前の状況を考えると安易に「未来永劫も」という訳にはいかないような「歴史的教訓」も頭をよぎる。現行NSではどうにか持ち応えることを祈念するばかりだが、次世代となると・・やはり不安も隠し切れない。今後も学内外の衆知を結集しセキュリティ対策を講じる必要性・重大性を強く感じている。後にも述べるが、人材育成と適材適所化が今後も本学の課題であり続ける点も強調しておきたい。

３．防災対策とデータセンター利用

日本が悲惨な震災（含む大津波）に襲われた記憶は色褪せない。多くの犠牲者と共に情報システムおよびそこに蓄積されていた情報そのものの喪失も大きな社会問題となった（なっていると現在形で述べるべきか)。本学における防災対策も前世代から本格的にスタートした。役員会のご理解・了承を取り付け、分散キャンパスの状況をむしろ奇貨居くべしとする対策を講じたのが一世代前である。結果としてキャンパス間通信（高速性）の必要性が増した。

クラウドサービスの普及も追い風となっている。世はまさに総クラウド化でGoogle、AMAZON等が幕開け役を演じたクラウド化の波は情報処理・情報通信という限られたドメインに収まりきらず今や社会現象化している状況である。遠隔会議やe-Learningと言ったキーワードもその推進役となっている。これに防災対策も相乗りを決めていることは周知に事実である。すなわち、特定キャンパスが被災しても大学全体としては機能してキャンパスが他のキャンパスにおけるサービスを可能な限り代行できる構成とする。そのためには、基幹ネットワークの高速化が不可欠となる。大学が共同利用しているSINETインターネットバックボーンが10ギガ接続サービスを提供しており、本学の現行NSもこれを受けての環境整備という側面を持つ。

一方、二世代前よりも以前から幸町キャンパスは本学における「扇の要」を演じてきたが、高潮被害が懸念されることもあって、低いながら山頂にある医学部キャンパスをもう一方のインターネット窓口とする防災対策を講じてきた。そのような経験を踏まえ、現行NSでは（正確には現行NS導入後に）「扇の要」を近隣のデータセンターに移設することで、より適切な防災対策を実現できるネットワークを構成することとした。しかし、「扇の要」にはF/Wを含む各種サーバを含む本学の言わば「NS的中枢」となる機器を移設（システム構築の動的修正）することになり、本学としても一大プロジェクトを組んで対応する必要があった。それでなくても、「ネットワークは正常に稼働して当然」という認識が一般的であり、一夜のうちに墨俣城を構築した木下藤吉郎の如き采配が強く望まれるものとなった。

ここでデータセンター利用のメリットをおさらい（要約）すると、

① データセンターの利用法：ハウジングVSホスティング
② 堅牢な構造：地震や災害に強い建物構造
③ 情報セキュリティは当然で、物理的セキュリティも重要
④ 意外に重要な立地条件：あまり遠いとアクセスが不便！？
⑤ 電源設備に加えて回線・通信サービスの充実も必要条件
⑥ 決め手は管理体制とマネジメントの信頼性

⑦　（忘れてならない）コストメリット

等が挙げられる。本学の場合、「NS 的中枢」機器の移設でも明らかなように①「ハウジング」型であり、②～⑤が最重要判断基準であったことも明確である。コストメリットは総てにかかる事案であるが、光熱水費低減でも実は導入効果があった様子だ。⑤ではインターネットバックボーン接続とキャンパス間接続の両方を兼ねている点でもデータセンター移行の効果（利用効果）があったと言える。

５．現行 NS の特徴

ここまで複数世代を俯瞰し NS の今昔を述べてきたので、改めて現行 NS の特徴について紹介しておきたい。

（１）**高機能 F/W の継続的導入**：これまでも述べてきたように Palo Alto F/W の特徴は高いセキュリティ性能であるが、キャッチフレーズ等を要約すると、(a)低機能パケットフィルタ型 F/W ではなく高機能ゲートウェイ型 F/W の代表であり、(b)通過するアプリケーションの可視化（識別と個別制御、併せて本学ではサンドボックス機能を利用した高度セキュリティ対策も実施中）を高速実行する専用ハードウェアとして実装され、(c)ユーザ ID（Active Directory 等）と連携可能でセキュリティポリシーの柔軟な実現を可能とし、(d)トータルコストに優れた運用支援を「謳い文句」としている。実際、運用経験からも機器の導入が返って運用コストまで高騰させる事実を苦々しく感じてきたので、現行 NS ではセキュリティレポートを導入業者にも分担してもらい機動性を高めている。

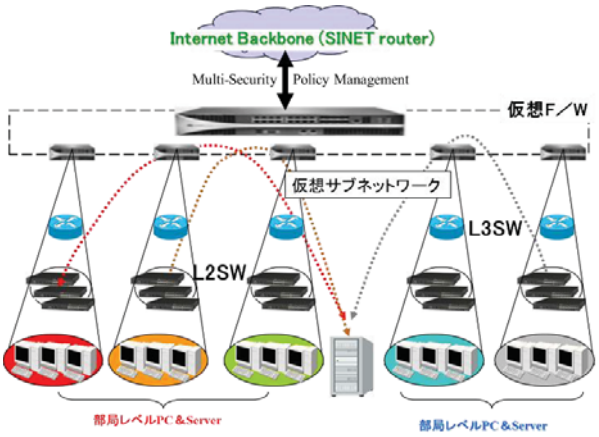

図１　仮想的サブネットワークの構築

図１のように、仮想的サブネットワークを構成することで、柔軟なセキュリティポリシーを容易に実現でき、かつ全体を統合できる。これは以降で述べるデータセンター移行時にも効果を発揮することになる。

（２）**ネットワークの高性能化とデータセンターの活用**：キャンパス間を 10G 高速回線で、インターネットバックボーンとは 10G×2 の余裕かつ柔軟性のある回線で接続しており、ネットワーク性能は過去最高レベルとなっている。また、データセンター利用のメリットは前述の通りである。従来 NS が幸町キャンパスを中心とするスター型（前述の「扇の要」）のトポロジーを採用していたため、幸町キャンパス被災時の影響が大きいという問題点を、新 NS では中心拠点をデータセンターへ変更し、耐災害性能とコストメリットに優れるデータセンターへ Computing & Network 機能をシフトし、被災リスク、管理・省エネコストの低減と機能性の向上を図っている点が大きな進化と言える。

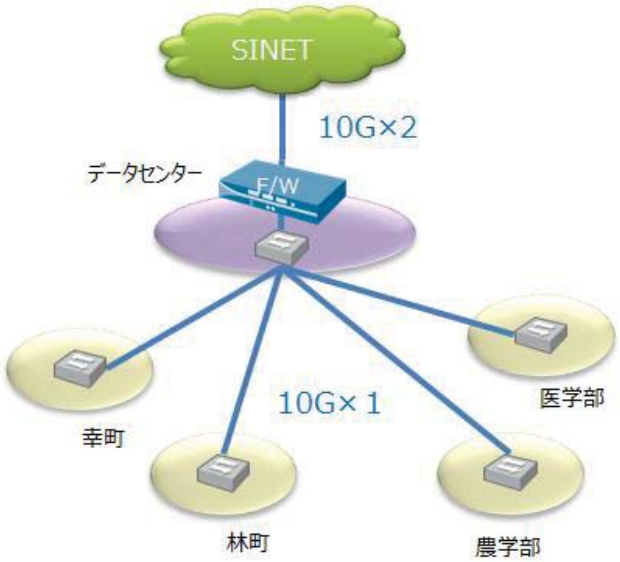

図２　データセンター移設後の現行 NS

図２の構成からも見通しの良いネットワーク環境が実現できていることが明確である。

（３）**スマートフォンや PC に代表される持込機器への対応**：従来方式の DHCP ではセキュリティ対策の面でも、ユーザ利便性の面でも限界となりつつあった。そこで、より柔軟なユーザ認証と

持込機器認証とを融合した認証システムの導入を図ってきた。情報化の影響から持込みノート PC 数の増加、スマートフォン利用者数の急増、無線 LAN 経由の機器認証作業の煩雑化に対応することが現行 NS のもう１つの特徴である。旧システムでは採用された ONG は導入コストと運用コストの問題で採用を見送り、同時に従来はスイッチ認証方式でなかったため、未登録端末でも手動で IP アドレスを設定すると通信可能となっていた。そこで、MAC 認証機能を有するスイッチを採用すること未登録端末の接続を排除し、認証機能強化の方針が採用された。

採用されたスイッチ認証方式は図３の赤色機器 Account Adapter と呼ばれるスイッチにより、「認証前アクセスリスト」と呼ばれる未認証の端末（図３の不正利用者の PC 等）に対して認証前の端末の通信に適用されるアクセスリスト機能が使用できる。認証済みの端末（図３の左の利用者が使用する PC 等）は許可する一方で「認証前アクセスリスト」の利用により MAC アドレス登録前の端末が学内ネットワークに接続することをブロックでき、また不正な利用者が未認証のネットワークを利用した不正な通信も抑制可能となっている。

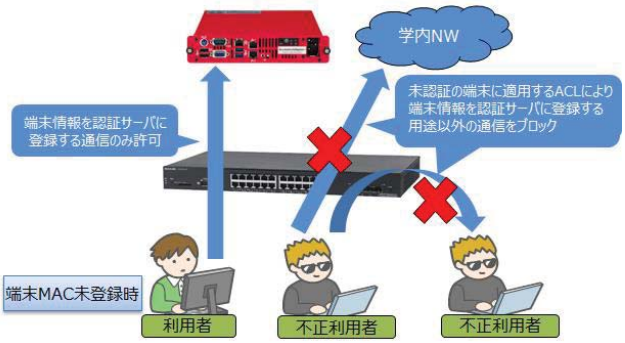

図３　スイッチ認証の有無（済み、未認証）によるネットワーク環境の動的な端末対応

６．ネットワーク利用の可視化

現行 NS に切り替わる以前からネットワーク利用状況の可視化を図４のような形式で実施してきた。対象となるのは、①SINET ルータ、幸町キャンパス、医学部キャンパス、工学部（林町）キャンパス）および農学部キャンパスに関する所定の１週間の幹線ネットワークの利用状況、と②各キャンパスにおける無線 LAN の利用状況である。ちなみに、図４の上２つは幹線ネットワークの利用状況（２番目はピーク時１，２時間の詳細利用状況）となっている。一方、図４の下２つは無線 LAN の状況であり、医学部（４番目）のみ測定形式が他と異なっている。

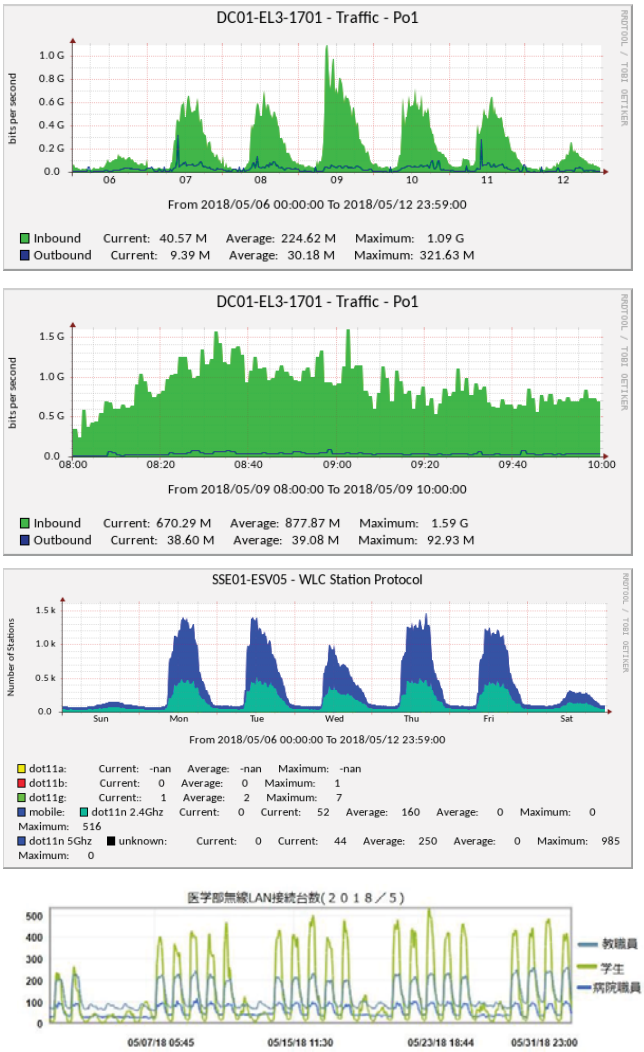

図４　ネットワーク利用の可視化の実例

５．あとがき

現行 NS は分散キャンパス（含む附属施設）という本学の現状に即しつつ、可能な限り効率良く管理・運用されている。しかし、課題も少なくない。平成 30 年度当初、創造工学部１年生の PC 認証時に生じた障害によって、機能設計は適正でも運用時の想定外の現象を予測することの難しさを突き付けられた。人材育成という課題もある。引く続き、大学全体の理解と学内外の支援を祈念しつつ筆を置くことにする。