次期キャンパス情報ネットワークシステムについて

ICT 基盤センター　情報基盤デザイン部門
柳生　大輔

1　はじめに

本センターでは，令和 2 年 10 月稼働開始予定の次期キャンパス情報ネットワークシステム（以下，「次期NWシステム」とします．）の設計・調達を行っています．本稿では，次期NWシステムの導入の背景やこれまでのネットワークとの変更点，特徴について説明いたします．

2　導入の背景

2.1　キャンパス情報ネットワークの歴史

キャンパス情報ネットワークシステム(NUNET)は，本学の教育，研究，事務等のあらゆる業務を支える基盤です．さまざまな業務が電子化・システム化された現在，その重要性はますます高まっています．

本学の情報通信・コンピュータネットワークについては，遡れば汎用電子計算機の端末回線等に源流を見ることになりますが，現在のような構成員全員が使用する業務・学習基盤としてのキャンパス情報ネットワークについては，平成5年度補正予算で導入された，FDDI による IP ネットワークから始まっているともいえます．

「internet」という単語を辞書で引けば，もちろん，幅広く使われている「インターネット」（The Internet）も記載されていますが，他にも「ネットワーク(間)のネットワーク《ネットワークどうしをさらにネットワークで結んだもの》」（出典：研究社　英和コンピューター用語辞典）のような記載もあります．

どのレイヤで見るかによって見方は変わりますが，ネットワークは一つのフラットなものではありません．本学のキャンパス情報ネットワークについても，規則の定義上は「部局 LAN」「基幹 LAN」という言葉があり，部局 LAN はその表記のとおり（基幹 LAN に接続する）部局内のネットワークを指しており，基幹 LAN はすべての部局 LAN や学外への上位ネットワークを接続するための中継機器，通信ケーブルや監視装置等を指しています．部局 LAN については各部局，基幹 LAN については ICT 基盤センターが維持・管理を行うことになっています．

前述の「維持・管理」には，大きく分けて 2 つの役割（業務）があります．一つは「維持」で，教育，研究や事務等の業務が滞りなく行えるよう，機器や配線等からなるネットワークの稼働を維持しなければなりません．障害が発生した場合には，機器を交換したりするなどの必要があります．世の中壊れない機器はありませんから，重要な機器については多重化するなどして，仮に一の機器に障害が発生した場合でも，継続して利用できるようにするなどの対応を行う場合もあります．

もう一つは「管理」です．コンピュータネットワークにおいては，それぞれの機器が独立して通信ができるよう，その機器を特定する番号が必要になります．いわゆるインターネットやキャンパス情報ネットワークの場合は Internet Protocol を用いて通信を行いますが，その（特定する）ために必要な番号が IP アドレスです．また組織や家庭のネットワークでも，誰でも彼でも接続してよいわけではありません．本学においては，部局 LAN 管理者（部局長）が，接続の可否を判断し，許可した場合には利用者（機器）に IP アドレスを割り当てる，という運用になっています．いわゆるマルウェア感染等情報インシデントが発生した場合，この割り当ての情報により利用者（感染した機器）を特定することになります．

このような形で，キャンパス情報ネットワークは運用されているわけですが，法人化や時代の変化により，より一層の業務効率の向上を求められるようになりました．前述の（特に部局 LAN の）維持・管理を実務的に担っていただく方として，部局 LAN 管理者から部局 LAN 管理運用担当者（多くは教育職員）が指名されていますが，部局 LAN 管理運用担当者としての業務は多くはボランティアとして位置づけられている現状である，また，教育・研究にかかる業務の発生源入力など多忙になり，障害やトラブルが発生しても，十分な対応が行えないということもお聞きしておりました．

そこで，平成 22 年 4 月運用開始のキャンパス情報ネットワークシステム「情報通信基盤システム」において，主に「維持」の範疇の，機器の維持（障害対応）や通信トラブルの調査・対応については，全学的に ICT 基盤センターが対応するようにしました[1]．また，前年の平成 21 年 12 月には通信設備やシステム稼働の拠点となるデータセンターを設置し，可用性の向上をはかっています．

今回導入を予定している次期 NW システムは，後述する情報セキュリティ強化を図るため，ネットワーク構造を大幅に変更するとともに，残る「管理」の部分のほとんどを ICT 基盤センターが全学的に担当しようと考えています．

2.2　情報ネットワークにおけるセキュリティ

いわゆる「インターネット」の普及により，我々の生活は本当に便利になりました．わざわざ店舗や空港・駅に出向かなくても，買い物をしたり，チケットを予約・購入することができ，世界中の情報を調べることができます．しかしながら別の見方をすれば，悪意をもつ人とも繋がることにもなります．

各コンピュータ・通信機器は，通信制御や同一ネットワーク内のファイル共有等を目的として， 常時通信を待ち受けている場合（ポート等が開いている，応答するなど）があります．これは，コンピュータが他の機器と連携する場合に必要なものです．本来は必要な通信相手とだけ通信できるようになっていればよいのですが，悪意をもつ人がこれを使って通信・運用妨害を試みたり，脆弱性を用いて侵入しようとしたりする場合があります（この脆弱性を塞ぐために，コンピュータやスマートフォンのパッチ適用が必要なのです）．

大学のように，1 台 1 台のコンピュータや機器の管理がそれぞれの構成員に任されている場合，全員がそれを守るコストをまとめると，大きなものになります．

そこで，一般的には，ネットワークの境界（学外と学内の境界）に「ファイアウォール」と呼ばれる機器を設置し，包括的に通信制御（通信の可否を制御）を行います．

図 1(a)は，現在の本学のキャンパス情報ネットワークの構成を示しています．本学のキャンパス情報ネットワークと上位ネットワークである SINET との境界にファイアウォールを設置しています．この機器により，学外に公開するものとして事前に本センターに申請され開かれているポート以外に接続しようとする学外からの通信を遮断しています．また，通信の内容を解析し，開かれているポートの場合でも，攻撃，妨害や侵入を目的とする通信については排除するようにしています．

本センターでは，次期 NW システムの一部として，平成 31 年 3 月に，このファイアウォールを最新の機器に更新しました．単に処理性能の向上だけではなく，サンドボックス機能や URL フィルタリング機能の稼働等，ネットワークを介した情報セキュリティの向上を図っています．

2.3　現在の情報インシデントの状況

ここで，IPA（独立行政法人情報処理推進機構）が発表している「情報セキュリティ 10 大脅威 2019」を見てみます．対組織では，「標的型攻撃による被害」が第 1 位，「ランサムウェアによる被害」が第 3 位，「内部不正による情報漏えい」が第 5 位になっています[2]．これらはその多くが電子メールを経由してマルウェアに感染し，（遠隔コマンド投入により）マルウェアが活動することによって引き起こされるものです．

昨今では，マルウェア対策ソフト（や同様の機能をもつファイアウォール）により新種のマルウェアを検出できる率は 10%～30%と言われています．また（ランサムウェアのような活動がわかりやすいものは除き）情報漏洩を目的とするもの等は，潜伏してから検出されるまで 60 日以上かかっているとの報告もあります．これは，標的型攻撃用にカスタマイズしたマルウェアが容易に生成できるようになってしまっており，マルウェア対策ソフトのベンダーが検体を持たないマルウェアについては，検出しにくいことに起因しています．したがって，これらの脅威に対しては，マルウェア対策ソフトやファイアウォールなどのシステム的対策だけでは十分でなく，人的対策等を含めた多層的な防御が必要になります．

次に，第 3 位「ランサムウェアによる被害」，第 5 位「内部不正による情報漏えい」，第 6 位「サービス妨害攻撃によるサービスの停止」について考えてみます．これらは，その攻撃や被害がネットワークを経由して発生しています．本学の場合，パソコン必携化が施行されていることや，タブレット・スマートフォンの普及もあり，私物のデバイスがキャンパス情報ネットワークに接続される機会も多くあります．また大学においては，学会出張等で大学の経費で購入したノートパソコンを持ち出すこともあります．

改めて，図 1(a)を見ていただくと，現時点では，学内にはネットワークの障壁が少ないことがご理解いただけると思います．学部をまたいだ複合領域研究等の形もあることなどから，これまでは，学内での障壁を積極的に設けてはいませんでした． また，研究にはさまざまな領域があることから，学内から学外への通信についても，ある程度の自由度を持たせていました．一度学内にマルウェアが入ってしまうと，この構造のため，影響が広がる範囲が広くなってしまいます．また，歴史的な経緯から，学外から利用される研究用サーバ等は各部局のネットワ

ークに接続されています．研究用のサーバ等に侵入されてしまうと，学内への攻撃への踏み台となってしまいます．また，他の研究室の学生が（別の）研究室のプリンタに印刷した，などのトラブルも生じています．

また，現在の接続許可は，機器に対して行われています．実際にだれが使用しているか，共用の機器の場合その時点でだれが使用しているかは，追跡が困難な場合も少なくありません．

情報ネットワークの運用やセキュリティを考える際，大切なのは，どの範囲（機器・人）を信用してどの範囲を信用しないのかということが大きなポイントとなります．極端なことを言えば，自分のみもしくは研究室内は信じるがそれ以外は信じない，という考え方もあり得ます．

学部によっては各教員に IP アドレスが 1 つしか配られておらず複数の機器で共用する必要がある，ノートパソコン等は学外で利用することもありアドレス設定を自動で行うため DHCP を利用したい，研究室で無線 LAN が使いたいなどの理由から，研究室において，無線ブロードバンドルータが設置されている場合も少なくありません．ブロードバンドルータにおいては，IP アドレスを共有するため NAT（アドレス変換）が行われるため，結果として，その外側から内側への接続を通さないようになり，ネットワークを分離するのと同じような効果が得られます．しかしながら弊害もあり，本学のインシデント検出装置や学外機関による通報などにより，情報インシデントを認識した際，そのブロードバンドルータの配下に対象機器があることはわかっても，アドレス変換記録が残っていなければ，どの機器であるかは特定できません．一般的なブロードバンドルータでは，その記録は長期間残りません．最近のマルウェアの状況を考えれば，現実的には特定が困難になってしまいます．

次は第 8 位「IoT 機器の脆弱性の顕在化」，第 6 位「サービス妨害攻撃によるサービスの停止」の観点です．ネットワークに接続される機器は，パソコンやサーバだけではありません．昨今の IoT(Internet of Things)の流れの中で，カメラやセンサなどの機器もネットワークに接続されるようになっています．これらの IoT 機器もコンピュータですから，内部では汎用の OS が稼働している場合もあります．パソコン等のユーザが直接使用する機器の OS については，いわゆる賞味期限がありますし，脆弱性を塞ぐアップデートを行わなければならないという意識も浸透していることから問題は少ないのですが，IoT 機器についてはトラブルが起こらなければ（メンテナンスを行わずに）物理的に故障するまで使用し続けられることも少なくありません．物理的な故障といっても，パソコンのような（故障率の高い）回転部品がないものも多く，10 年以上稼働し続けるものもあるでしょう．これらの IoT 機器もファームウェアのアップデートを行わなければ，発見された脆弱性が積み上がっていく，ということになります．前述のブロードバンドルータも IoT 機器の一つです．現在，これらの IoT 機器の脆弱性を利用し，侵入の踏み台としたり，サービス妨害攻撃のリフレクタ・アンプとて使用したりされている事象が確認・報告されています．

本センターが行っている「情報セキュリティ基礎講習会」でも解説されていますが，いわゆる「情報」に関わらず，「セキュリティ」は，さまざまな要因がある中で，一番低いレベル（弱い箇所）が，全体のレベルを決めてしまうという側面があります．ですから一人一人の意識はもちろん大切なのですが，そのコストを全構成員に負担させてしまうと，組織全体としてのコストは膨大なものになってしまいます．

3 新 NW システムの機能と変更点

そこで本センターでは，これまでのネットワーク利用の実態，ネットワーク管理運用で培った経験のみならず，これからの向こう 10 年を見据え，情報セキュリティ対策の強化，新たな学習の仕方・働き方，IT サービスのクラウド化への移行等の社会状況の変化にも対応し，本学の構成員がこれらの基盤を用いて，有効・有意義な成果を出し続けられることができるよう，新たな情報通信の基盤となる新 NW システムの導入を計画し，予算要求や調達事務を行っています（一部の機能については，予算の都合上，現在行っている調達では実施せず，後年度の実施となるものもあります）．

新 NW システムでは，図 1(b)に示すとおり，主に情報セキュリティの強化を目的として新たな機能や運用の変更を行うことを計画しています．以下，キーワードに沿って説明いたします．

3.1　ネットワークの機能・目的ごとのパーティショニング

新 NW システムでは，これまで，学外・学内・講義用無線 LAN の区分けしかなかったネットワークのゾーニングを細分化し，ファイアウォール等で分離することにより，万が一，機器への侵入やマルウェア感染等の事象が発生した場合でも，影響する範囲を局所化できるようにします．また，不適切な情報の取得ができない構造とします．表 1 に示すようなゾーニングを計画しています．

いわゆる，一般的なパソコンや研究室のプリンタ等は「個別 NAT ゾーン」に移行することになります．また，これまで学部のネットワーク内に接続されていた，外部からの接続を受け付けるサーバ等は「学外公開サーバゾーン」に移行することになります．移行完了後，学部等の単位でファイアウォールを稼働させ，被害極限や情報流出等の防止を図ります．

移行については，新 NW システム稼働（令和 2 年 10 月予定）後，順次行っていきます．

3.2　マイクロセグメンテーション（個別 NAT の提供）

前述のように，現在は，部局内のネットワークはサブネット程度の分割しか行っていないため， 隣の研究室の学生が自研究室のプリンタに印刷した，などのトラブルが起こります．

また，これまでブロードバンドルータが設置されている場合も，前述の変換記録の保存の問題や，メンテナンスがなされていないルータの脆弱性の問題があります．

そこで，新 NW システムでは，研究室等の単位でプライベートアドレス空間を提供する，マイクロセグメンテーションを実施します．

具体的には，研究室等ごとに閉じたプライベートネットワーク環境を提供し，アドレス変換を行い学内に接続するものです．これにより，研究室等のネットワークの前段に簡易的なファイアウォールを設置した形になることから，他研究室等からも，研究室等のネットワークおよび接続された機器を秘匿・防御できます．

また，このプライベートアドレス空間では，DHCP サービスを提供します（IP アドレスを固定して利用いただけるアドレス空間も提供します）．これまで，パソコン等をネットワークに

接続する際には IP アドレス等の手動での設定が必要でしたが，LAN ケーブルを挿すだけで自動的に IP アドレス設定等が完了します．DHCP のリース記録やアドレス変換記録については，本センターが保管します．二重にアドレス変換を行うとトラブルが起こることもあり得ることから，現在無線 LAN 接続用として，ブロードバンドルータを利用されている場合は，いわゆる「ルータモード」から「ブリッジモード」に変更して，利用いただくことになります．
※研究室等とは，講座，教室，研究室，事務の課・室等を想定しております．研究や組織運営にはさまざまな形態があることから，前述の個別 NAT 環境の提供単位については，部局 LAN 管理運用担当者を通じて，今後協議を進めてまいります．

個別 NAT 環境への移行についても，新 NW システム稼働後，順次行っていきます．

ゾーン名称	ゾーンの概要
学外公開サーバゾーン	学外からのコネクションを受け入れるホストを設置する．このゾーンから他ゾーンのコネクションは許可しない．
学内グローバルアドレスゾーン	グローバルアドレスを使用するホストを設置する．（部局ごとに）学外からのコネクションを受け入れるホストの「学外公開サーバゾーン」への移行後，学外からのコネクションを遮断する．大まかな部局ごとに一方向のファイアウォールを設置する．一般的なクライアント等は，「個別 NAT ゾーン」に移行させる。部局の共同プリンタ等のデバイスに使用する．
学内公開サーバゾーン	学内にのみ ICT サービスを提供することを意図するホストを設置する．情報漏洩の阻止のため，このゾーンから学外への通信はアップデート等の通信を除き原則許可しない．
個別 NAT ゾーン	研究室，講座，部課係等の単位を基本として提供するプライベートアドレス空間である．異なる個別 NAT の内側間では通信を許可しない．
ハイセキュアゾーン	特に高度な情報管理が必要な端末を設置する．エンドポイントセキュリティソフトウェアの導入を必須とするなど，高度なセキュリティを提供する．
教育系ネットワークゾーン	教室，会議室等不特定多数が入室しうる場所で使用する．本学は PC 必携化を実施しているので，特に教室等においては，収容人員が同時に無線 LAN を快適に使用できることが必要である．各教室に設置された情報コンセントもこのゾーンに収容する．
ゲストゾーン	「教育系ネットワークゾーン」と同様であるが，本学構成員以外のゲストが使用するため，学内のリソース等へはアクセスできない．Eduroam 等を含む，

表 1：ゾーニング構成案

3.3　個人認証・機器認証

現在の管理スキームでは，（教育用のネットワークを除き）機器をネットワークに接続する際には，部局 LAN 管理者の許可が必要です．しかしながら，許可を得なくてもネットワーク的に接続できてしまうため，勝手に IP アドレスを割り振って利用していた，管理台帳が適切に管理されていない等の理由で，インシデント検出の際に，機器の特定や対処に時間がかかった例も見受けられます（※本センターが管理するネットワーク機器の制御データから，部屋程度は特定できます）．

そこで，新 NW システムでは，ゾーンによっては NW システム側に機器の登録等を必要とし，不正な接続等を阻止します．機器の登録は有効期限を設け，廃棄した機器が不正に接続されることを防止し， 盗難された機器が接続された場合は，即座に検出できるようにします．

ネットワーク利用時の個人認証も開始します．共用機器等が本学構成員外に利用されることを阻止するとともに，本学構成員しか知ってはならない情報を防護します．また，インシデント検出時に直接利用者とコンタクトすることにより，事態の早急な収束を図ります．将来的には，利用者の属性（学生・教職員や所属部局等）により，認められた範囲のリソースのみが利用できるように制御することを検討しています．

3.4　無線 LAN の性能・利便性向上

現在運用している無線 LAN システムは，もともとカジュアルな利用を前提として導入したものに，パソコン必携化に対応するため数量的にはアクセスポイントを増設しましたが，機能・性能は必ずしも十分ではありませんでした．

新 NW システムでは，定着してきた必携パソコンの授業時間内・時間外での利用をさらに推進するため，性能を向上した（新たな無線通信規格に対応した）機器に入れ替えます．

また，これまで無線 LAN を利用いただく際には，PSK(Pre Shared Key)を事前に知っておいていただく必要がありましたが，新たに IEEE 802.1X による認証をサービス開始し，長大 ID とパスワードがあれば，無線 LAN を利用できるようになります．

災害発生時の本学の地域貢献として，災害用統一 SSID の提供も検討しています．

3.5　eduroam の提供範囲拡大

これまで本学では，前述の経緯のとおり無線 LAN システムの性能の観点から，IEEE 802.11ac 規格に対応した無線 LAN アクセスポイントでのみ eduroam の提供を行っています．新 NW システムではすべてのアクセスポイントが少なくとも IEEE 802.11ac 規格となることから，技術的には全アクセスポイントで eduroam を提供できるようになります．ただし，eduroam を提供するアクセスポイントについては公表する必要があることと，それにより学外者が使える場所であるとして，実は部外者立入禁止である場所に（無許可で）進入する可能性も考えられることから，提供にあたっては，本センターから各部局に対し，アクセスポイントごとに eduroam の提供を行ってよいかを確認させていただいた上で，提供することといたします．

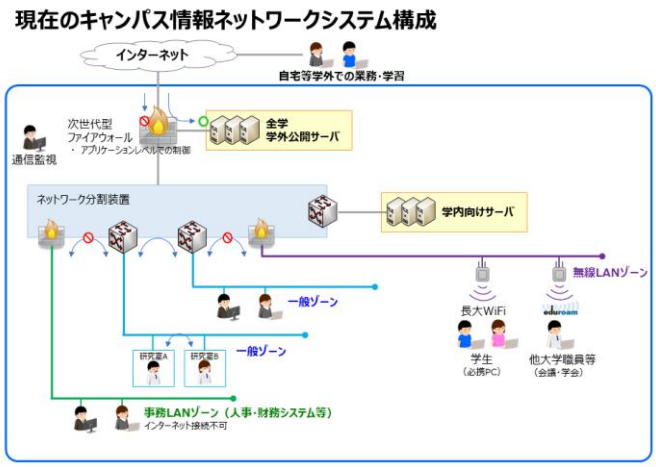

図 1(a)：現在のキャンパス情報ネットワークシステム構成

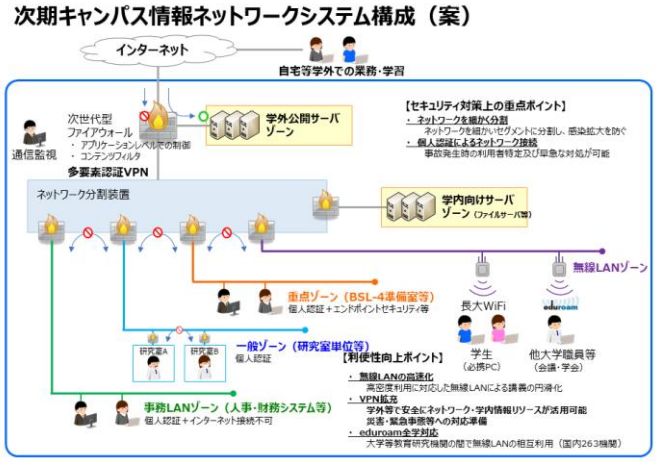

図 1(b)：次期キャンパス情報ネットワークシステム構成

4 おわりに

新 NW システムは，情報セキュリティ強化や利便性向上を主な目的としていますが，本学のキャンパス情報ネットワークの歴史において，大規模な構造・考え方の変更を伴うものです．構成員のみなさまへは，令和 2 年度に説明会等で丁寧な説明に務めるとともに，切替え等について個別にヒアリング・サポートを行いますので，移行へのご理解・ご協力をお願いいたします．

参考文献

[1] 「平成 22 年度　情報通信基盤にかかる事業報告」，柳生　大輔，長崎大学情報メディア基盤センターレポート 2010，pp.29-35
http://hdl.handle.net/10069/28562

[2] 「情報セキュリティ 10 大脅威 2019」，独立行政法人情報通信推進機構，2019 年 7 月
https://www.ipa.go.jp/security/vuln/10threats2019.html