3. 平成 23 年度　情報基盤にかかる業務報告

情報メディア基盤センター　柳生　大輔

０．はじめに

平成 23 年度に実施した情報基盤に関する事業等について、簡単に紹介させて頂きます。

１．新ファイアウォール（情報セキュリティ装置）について

本学のキャンパス情報ネットワークとインターネットの境界に位置し、通過する通信内容を監視・制限することにより、インターネットからの攻撃を防御するとともに、内部からの情報漏洩を防ぐための情報セキュリティ装置（ファイアウォール及び SINET 接続用ルータ）について、平成 23 年 3 月に更新を行い、4 月より運用を開始しました。これらの装置については、本来その性質上詳細は明らかにできませんが、平成 23 年 4 月に実施した第 3 回情報メディア基盤エンター講習会でお話しした内容から、その機能について説明させていただきます。

１．１　インターネットにおけるコンピュータ間の通信

ファイアウォールの機能を理解する上で、コンピュータ間の通信がどのように行われるのか、という知識が必要となります。そこで、

そもそも、インターネット上において、コンピュータ間の通信はどのように行われるのでしょうか。ので、例として、国立情報学研究所の Web サーバ（www.nii.ac.jp）にアクセスすることを例に考えてみます。ユーザが自端末の Web ブラウザに URI(http://www.nii.ac.jp)を入力すると、以下のような手順でコンピュータ同士が通信を行います。

1) 端末は、本学の DNS キャッシュサーバに対してホスト名 www.nii.ac.jp に対応する IP アドレスを尋ねる

※コンピュータは端末やサーバを IP アドレスで特定・通信します

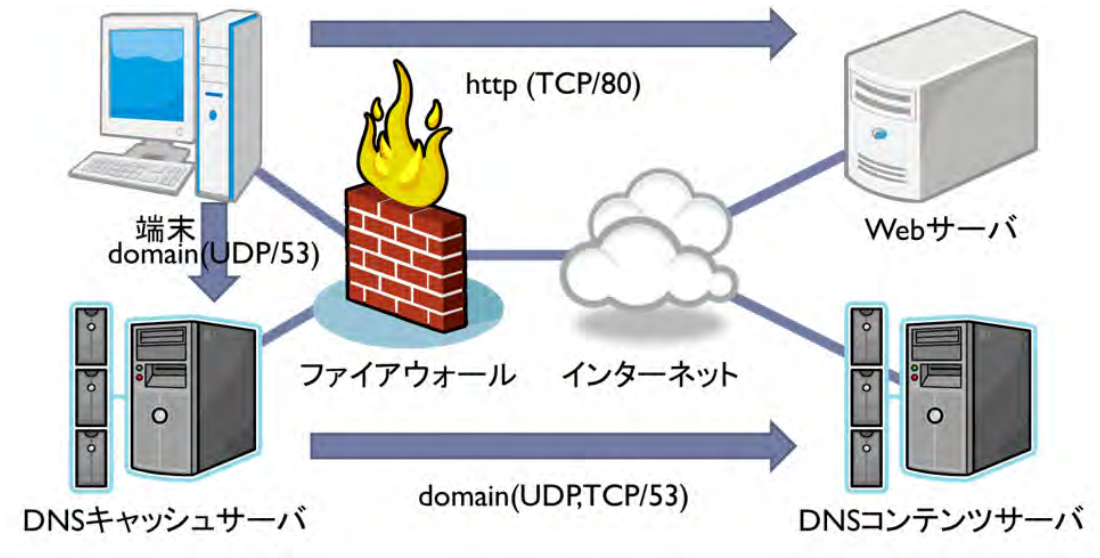
・本学の DNS キャッシュサーバは、インターネット上の DNS コンテンツサーバから www.nii.ac.jp に対応する IP アドレスを調べて端末に回答します。この例では、IP アドレスは 136.187.7.10 となります。

2) IP アドレス 136.187.7.10 が付されたサーバの 80 番ポート（Web であるため。SSL で暗号化されたページの場合は 443 番ポート）に対して、TCP でセッションを張り、ページのコンテンツをリクエストします。

※1 台のサーバで、複数のサービスを提供することができます。ポート番号は、言うならば、

提供を受けるサービスを指定するための番号です。
※この際、端末に振られた IP アドレスがプライベートアドレスであるならば、ファイアウォールやブロードバンドルータなどの装置によって、アドレス変換等が行われます。

・Web サーバから端末に対してコンテンツが送信されます。コンテンツのリクエスト・転送のプロトコルとして http が用いられます。
3) ブラウザがコンテンツを解釈し、画面を構成して表示します。
・ページ内に画像等のファイルや他の Web サーバに掲載されたコンテンツがあるようなら上記の手順を繰り返します。



１．２　ファイアウォールとは

前節でわかることは、インターネット上コンピュータ同士の通信は、インターネット上では IP アドレスで通信相手のコンピュータを識別し、ポート番号でサービスを識別する、ということです。また、プロトコルでデータのやり取りの方法が規定され、そのプロトコルに基づいて通信を行い、様々なサービスが提供されます。例えば Web についても、単に情報発信されている Web ページを見るだけではなく、現在ではブラウザさえあれば、Webmail やファイルアーカイブシステム、skype や facebook などの Web アプリケーションが利用できるようになっています。

さて、学生や教職員が用いる業務用システムについて、学内専用や学部専用といったシステムがあるのは御存じだと思います。つまり、利用できるユーザが制限されたシステムです。これらについては、利用する正当な権限を持たない人の利用を制限する、すなわち、アクセス制御を行う必要があります。アクセス制御の方法には ID やパスワードを用いた方式もありますが、そもそも利用を想定するコンピュータからの接続のみ許可し、利用を想

定しないコンピュータからの接続を遮断する、という方法も考えられます。サーバの OS 等でもそうですが、実は普通の PC の OS でも、ユーザが知らないまま、通信を受け付けているポート番号があったりするのです。以前の PC 用 OS では、デフォルトでインストールし、セキュリティ対策ソフト等を何もインストールしないで、インターネットに直接接続すると、2 時間程度で乗っ取られた、というレポートもあります。

そこで、通信を制御し不必要な遮断等を行うために用いられる機器や機能の概念のことを、「ファイアウォール」と呼びます（実装の形態を問いません）。

ファイアウォールにはいくつか種類があり、その種類によって、制御・防御できる対象が異なります。※説明を簡単にするため省略した型もあります。

・（単純な）パケットフィルタ型

通信を許す IP アドレスやポート番号を識別して、通信を制御・遮断するものです。動的制御を行えるものでは、ある通信が外部に対して行われたら、そこから帰ってくるパケットを受信することを一定時間許可し、それ以外は遮断する、という動きをします。

家庭でインターネットに接続する際に、ブロードバンドルータと呼ばれる装置が用いられますが、この装置ではアドレス変換が行われるため、その仕組み上、内部のコンピュータと外部のコンピュータ間では、パケットフィルタ機能が働きます。一応、外部からの不必要な接続を遮断することができます。

・ステートフルインスペクション型

実際のコンピュータの通信では、通信を開始するための信号を送り、受け手がその通信を了解する信号を返し、それから実際の通信が行われる、というような通信状態の制御が行われます。ステートフルインスペクション型では、パケットフィルタ型の機能に加え、このような通信状態が正当なものかを判断し、正当でないものは遮断します。高級なブロードバンドルータ等にも実装されているものもあります。Unix 系 OS のソフトウェアファイアウォールにも実装されています。

・アプリケーションゲートウェイ型

上記のファイアウォールでは、通信相手や通信状態等により通信制御を行うため、実際の通信の内容に触れることはありません。このことから、防御できる対象には限界があります。たとえば、コンピュータウィルスに感染したメールなどです。メールの送信手続として適正に行われた場合、上記のファイアウォールでは通過してしまいます。他には、許可されたプロトコル（にあたるポート番号）を用いて他のプロトコルで通信を行おうとした、組織の情報漏洩防止として特定の種類のファイルの学外への送信が禁止されているのに送信を行おうとした、また、業務上必要ない特定のサイトにはアクセスさせない、などがありますが、これらはこの型のファイアウォールでないと防御できません。各 OS やアプリケーションで時々発見される脆弱性についても同様です。更新前のファイアウォールはこのタイプでした。

１．３　更新したファイアウォールの機能：アプリケーション識別

更新したファイアウォールは、メーカに言わせると「アプリケーション識別型」ファイアウォールです。アプリケーション識別とは、これまでのファイアウォールの機能（アプリケーション脆弱性・ウィルス・スパイウェア・ワームのリアルタイム検知・ブロック）に加えて、どのサービス・アプリケーション（PC にインストールされたアプリケーションと Web アプリケーションの両方を含みます）が利用されているか、さらには、そのサービス・アプリケーションのどの機能が利用されているか、ということを識別できる、ということです。識別した結果に基づき、個別に通信を制御することができます。たとえば、skype というアプリケーションの利用についても、ビデオチャットするという機能・行為と、ファイルを転送するという機能・行為を個別に識別することができます。

１．４　P2P ソフトウェアにかかる通信の遮断開始

更新したファイアウォールの機能を用いて、平成 24 年 1 月よりファイル共有ソフトウェア（P2P ソフトウェア）にかかる通信の遮断を開始しました。

P2P ネットワーク内で交換されているファイルの多くが著作権等を侵害したものであること、また、意図的にコンピュータウィルスに感染させたファイルが流通していることが報告されています。P2P ソフトウェアの利用は著作権侵害を助長し、また端末のウィルス感染等を通じて本学の情報ネットワークの脅威となります。本学の事例ではありませんが、ウィルスに感染させた端末を遠隔操作した（脅迫・威力業務妨害となる内容を送信した）事例も報道されているとおりです。

なお、その性質上、対象となるアプリケーションの公表はしませんので、教育研究上必要な場合は、個別に御相談をお願いいたします。

１．５　研究室や家庭でも

本センター（情報企画課）では本学のキャンパス情報ネットワークの管理を行っておりますが、学部や研究室、家庭といった狭い範囲のネットワーク内での事象については、防御できないこともあります。学部や研究室、家庭の PC 端末等についても、必ず OS やアプリケーションのアップデート、ウィルス対策ソフト等を導入し定期的にスキャンをかけるなどの対策を実施していただきますよう、お願いいたします。

なお､本センターでは Android 端末用ウィルス対策ソフトの提供も平成 28 年 2 月末までの期間限定で行っておりますので、ご利用ください。

２．電子メールサービスにかかる update

２．１　Outbound Port 25 Blocking の開始

「電子メール」においては、
・メールソフトからメールサーバへの送信・メールサーバからメールサーバへの配信で同じ smtp を用いる（Webmail の利用を除きます）
・From（発信者名）は自由に設定できる。よって、メールの From だけでは本人かどうか確認できない
・25 番ポートによる送信の場合（組織・プロバイダ内では）送信時認証を行わない場合がある
などの特徴があります。

Outbound Port 25 Blocking(OP25B)とは、プロバイダ・組織が設置するメールサーバを用いずにプロバイダ・組織外のメールサーバ（の 25 番ポート）に対して直接メールを送信しようとする通信をプロバイダ・組織側（送信者が所属する側）のファイアウォール等で遮断すること、をいいます。本来は、家庭やモバイル端末など発信元 IP アドレスがプロバイダ等によって動的に割り当てられる IP アドレスである場合に適用されることが多く、自らサーバを立てるような固定 IP を取得している場合には適用されないこともあります。

大学等の機関においては、教員の異動（採用・退職）が多く、複数の組織に地位を有する方もおられ、利用者の中には、大学等の組織が発行したメールアドレスではなく、プロバイダや gmail 等のメールアドレスを公表・利用している方も少なくありません。

このため、これまではこれらの学外メールサービスを利用いただけるよう、特に通信制限は課していませんでしたが、
・SPAM の発信源や情報漏洩の原因となる可能性がある
・学外メールサービスにおいて、ほぼ全てで Webmail サービスや Submission ポート（587 番ポート）による送信サービスが提供されるようになった

・ホテル等のインターネット接続サービスやモバイル接続サービスでも 25 番ポートを用いた直接送信が遮断されるようになった

という状況から、本学においても、平成 24 年 5 月より 25 番ポートを用いたメール送信については、許可制（原則として遮断し、業務上の必要がある場合には通過するよう申請を受け付ける）といたしました。

本措置は、本学の電子メールシステムのみを利用している一般ユーザに影響を与えるものではありませんが、サーバ等や監視装置等を運用されている場合には申請が必要となります。詳細については、本センターの Web をご覧ください。

２．２　SPF 認証設定情報の投入

昨今、電子メールの SPAM 等迷惑メールの存在が大きな問題となっています。電子メールについてはその仕組み上、送信者のメールアドレス（From フィールド）は自由に設定できるため、メールアドレスの所有者の意思とは無関係にそのメールアドレスを騙られたメールが第三者から発信されたり、また、何らかの理由により受け取りを拒否された結果としてのエラーメールが本来のメールアドレスの所有者に戻ってきたりするなどの問題が生じることがあります。迷惑メールについても、送信者のメールアドレスを騙って送信されることが少なくありません。

この問題の対策の一つとして、SPF(Sender Policy Framework)認証があります。SPF は、受信側メールサーバが、そのメールが送信者のメールドメインの所有者が指定した送信側メールサーバ（IP アドレス範囲）から送信されていることを確認することにより、なりすましメールであるかどうかを判断する技術です。各メールドメインの所有者は、そのメールドメインのメールがどのメールサーバから送信する、ということを宣言することができますが、その情報をどう取り扱うかは、それぞれの受信メールサーバのポリシーにより異なります。

本学においても、本センターが管理するメールアドレスで送信されるメールは、本学が指定したメールサーバからのみ送信する、ということを宣言する SPF 認証情報の登録を平成 23 年 9 月に行いました。

本学のメールサーバ（Webmail サービスを含む）を用いて一般的にメールを送受信される方には、設定変更を行っていただくなどの影響はありません。詳細については、本センターの Web をご覧ください。

２．３　net/net2 ドメインメールサービスの廃止について（予告）

本センターでは、平成 6 年から@net.nagasaki-u.ac.jp（主に教員、医師に交付）、@net2.nagasaki-u.ac.jp（事務系その他の職員に交付）のメールサービスを提供してきまし

たが、平成 18 年 3 月に@nagasaki-u.ac.jp（以下、大学ドメインといいます。）の新メールサービスの提供を開始し、すでに教職員の大多数が@nagasaki-u.ac.jp へ移行されております。

現在は、新旧両ドメインを運用しておりますが、運用ドメインを削減することにより、システム構成を単純化できコストの削減が可能であること、また、迷惑メールの削減等も図れることから、平成 25 年 9 月 2 日（月）をもって net・net2 ドメインのメールサービスを廃止することになりました。

まだ、移行がお済みでないユーザにつきましては、廃止日までに計画的に移行をお願いいたします。詳細は、本センターの Web をご覧ください。

３．その他

平成 23 年度に実施したその他の事業等について簡単に紹介させていただきます。

・東京事務所の学内 LAN 化について

VPN 技術を用いて東京事務所と本学データセンターを接続し、東京事務所内のネットワークについて、学内 LAN の一部となるよう構成変更を行いました。東京事務所内からも、本学キャンパス内で利用できるネットワークサービスがすべて利用できるようになりました。また、遠隔会議システム（polycom）を設置いたしましたので、本学キャンパス内と東京事務所での遠隔会議が可能です。遠隔会議システムの利用につきましては、東京事務所・広報戦略本部にお尋ねください。

・データセンター非常信号メール発報システムの構築

データセンターについては、建屋・ラックの温度や消費電力、ドア開閉について常時監視（異常時のメール発報等を含む）を行っております。今年度、これらの監視に加え、自家用発動発電機や無停電電源装置の運転状態、また、万が一の火災に備えた窒素自動消火装置の運転状態について、ネットワークを通じた監視、異常時のメール発報等を行うシステムを構築しました。

※当然ですが、消防法上自動火災報知設備（感知器）は設置してあり、移報は守衛室で受信されます。

・サーバ仮想化のための電源切替実施

本センター・情報企画課では、業務システムの信頼性向上、省エネ化のため、業務シス

テムのサーバの仮想化を順次実施しております。仮想化する場合、その目的上処理能力を集中させることになりますので、仮想化プラットフォームは相当な電力を消費します。そこで、仮想化プラットフォームを安定して運用し、増設が容易にできるよう、分電盤・分電装置の追加設置を行いました。

なお、平成 24 年度より、学部や研究室のサーバ等をデータセンターにてお預かりするサービス（有料）を開始しております。詳細につきましては、本センター事務室にお尋ねください。