TYCOONにおける情報セキュリティの現状と対策

森河良太[1]，小杉義幸[2]，宮川毅[1,2]，倉田香織[2]，
松﨑日出海[3]，土橋朗[2]

1．はじめに

研究機関や大学，一部の企業を中心に発達してきたインターネットには，特定の集中した責任主体は存在しない．また管理についても，インターネットに接続している組織の総意として，国際的に中立とされるICANN（The Internet Corporation for Assigned Names and Numbers）やIETF(Internet Engineering Task Force)にその主体を委ねている．1995年に誕生した東京薬科大学情報ネットワークTYCOON（ToYaku COmputer Open Network）も，このようなインターネットの一部として運営を開始した[1]．しかしインターネットの普及と商用化が進むにつれ，日本国内でもインターネットの規制，特にセキュリティ問題に対処するための動きが現れてきた．2000年2月13日に施行された「不正アクセス行為の禁止等に関する法律」を始めとして，2005年4月1日より施行された「個人情報の保護に関する法律（個人情報保護法）」，またそれに続く様々な法令等は，その対処の一部を具現化したものである．しかしそれに対し，1984年以来日本に徐々に浸透してきたインターネットとその文化は，それらの法令が登場するまでの15年の間，学術の世界において練られ，熟成されてきたものであると言える．

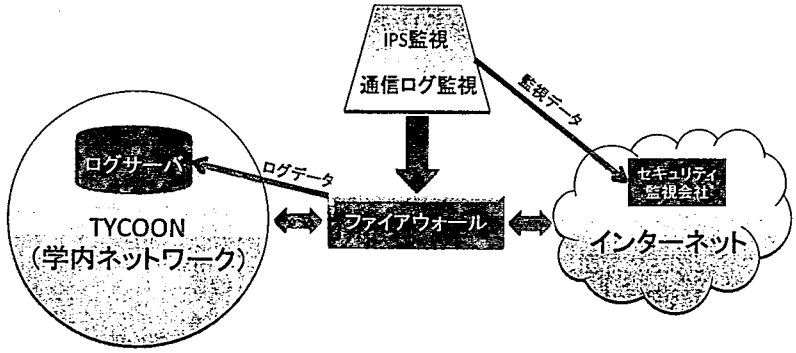
インターネットを規制するために国家によって定められた法令と，学術機関が育ててきたインターネット文化の間に，基本的精神や方針の相違が出てくることは必然の理である．本稿では，このせめぎ合いの中に置かれた大学という組織の中で，情報のセキュリティがどのように取り扱われるべきかを，「TYCOONにおける不正アクセスの監視状況」を題材にしながら具体的に考えてみたい．

2．ファイアウォールにおける通信制御とIPS監視制御

2-1．TYCOONにおけるファイアウォールの設置

1995年にTYCOONが構築された当初は，WIDEインターネットと学内LANの間の通信を規制する仕組みは何もなかった．JPNICより割り振られた7つのクラスCのIPアドレス空間をそのままネットワーク端末に割り振り，電子メールやWeb閲覧のために用いていた．当時はインターネットを利用するほとんどのユーザが，大学や研究機関の関係者に限られており，またそれらを彼ら自身で管理していたため，互いを害するような行為はほとんど行われることはなかった．

[1] 生命科学部コンピュータ委員会
[2] 情報教育研究センター
[3] 総務部検収センター



（図 1）侵入防止システムを備えた TYCOON ファイアウォールの構成（現在）

しかし TYCOON 内の IP アドレスをクラス A のプライベート IP アドレス（約 1,600 万個）に変更し，学内における IP アドレス枯渇問題に対処するため，1998 年 10 月，TYCOON の入口に初めてファイアウォールを設置した．その後 TYCOON とインターネット間の通信量が日々増加し，また SPAM（迷惑メール）やウイルスメールも日常的に送受信されるようになると，ハードウェアへの過負荷によるファイアウォール機器の故障頻度も多くなってきた．そこで 2007 年 8 月，本学のファイアウォールを（図 1）のように，大容量通信に対応しつつ，なおかつ侵入防止システム（IPS）を備えた専用アプライアンス機器に更新した[2]．

2-2. IPS(Intrusion Prevention System) ：侵入防止システム

IPS はネットワークやコンピュータへの不正な侵入を監視し，阻止するためのシステムである．IPS では IDS（Intrusion Detection System）と呼ばれる侵入検知システム（不正アクセス監視システム）を用いて不正アクセスに関係すると思われる通信パケットを検出し，その不正のレベルに応じて通信の遮断を実施する．IDS では，監視対象となるトラフィックが不正アクセスに関係する通信であるかどうかを，データベース化された過去の不正アクセスの通信パターン（シグナチャデータベース）に基づいて判定を行う．この判定を行うためには，多くの経験とワールドワイドな状況の把握，そして最新のアルゴリズム群を駆使することが要求される．また IDS の運用では，シグナチャデータベースを常に更新し，チューニングを行う必要がある．よって TYCOON では，24 時間体制で IPS の運用を委託している．しかし IPS による検知は，基本的にデータベースに依存するので，未知の手法による不正アクセスを検知することはできないし，また対象のシグナチャが似ている場合には，誤検知が生じる可能性も十分にある．これらの基本的な注意事項を十分に理解した上で IPS の外部委託を行うことは，クラウド時代のインターネットセキュリティに必要な心構えであると言える．

3．TYCOONファイアウォールにおけるIPS監視（2012年4～12月）

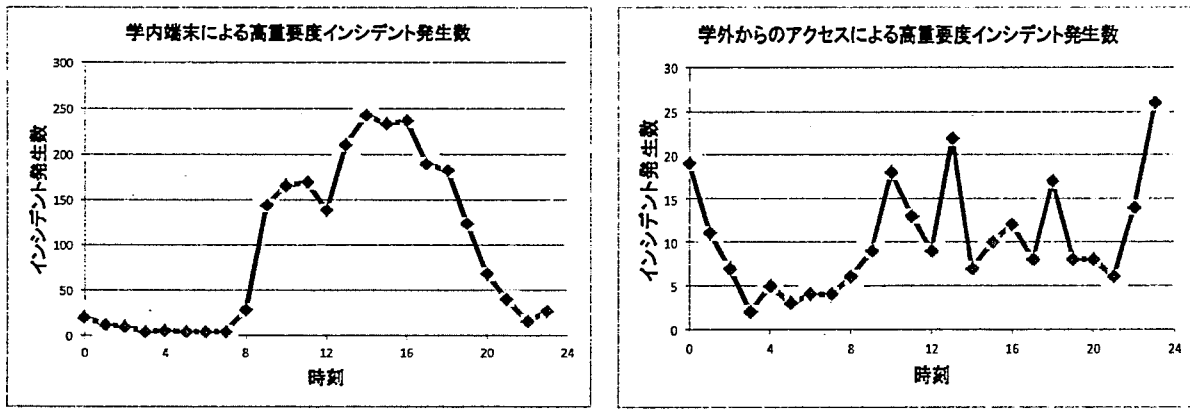
3-1．不正アクセスに関わるインシデントの概要

前述したTYCOONのファイアウォールとして，IPS機能を搭載したCisco社のASA5500シリーズ(ASA5520)が設置されている．このASA5520は日本屈指のセキュリティ会社によって24時間監視されており，ファイアウォールのログから，明らかに不正アクセスであると判別できるインシデントとIPSによるインシデントを，それぞれ「低重要度」「中重要度」「高重要度」の3つのレベルに分けてファイアウォール管理者に提示している．ここでは明らかにマルウェアの感染による不正アクセスが行われているとみなされる「高重要度」のインシデントについて，2012年4月から12月におけるデータをまとめてみる．まずファイアウォールにおいて観測されたインシデントの概要と件数を（表1）に示す．

インシデント概要	件数
不審な通信の遮断	1986
外部のホストからのSQLインジェクション	248
内部ホストのボット感染の疑い	29
NetBIOSサービスへの感染活動の疑い	8
内部ホストのウイルス感染の疑い（Gumblar）	4
DNSサービスへの調査活動の疑い	1
合計	2276

（表1）2012年4月から12月におけるインシデントの概要と件数

「**不審な通信の遮断**」とは，TYCOON内に接続された端末（パソコンだけでなく，スマートフォンなどの携帯端末を含む）から学外の端末に向けて，不正アクセスと思われる通信が行われ，これを遮断したインシデントを表す．後で具体的なシグナチャを示す際に明らかになるように，これらの不正アクセスのほとんどは，マルウェアに感染したファイル共有ソフトによるものである．「外部のホストからのSQLインジェクション」は，インターネットからTYCOON内のSQL系データベース（DB）サーバに対する不正アクセスを示す．具体的にはSQL系DBをサーバシステム内に内包するZimbraのような多機能メールシステムやLMS（オンライン学習システム）[3][4]，CMS（ホームページのコンテンツマネージメントシステム）[5]に対する不正アクセスが行われようとした痕跡を表している．これらの不正アクセスは全部で248件を数えるが，そのほとんどが日曜祭日もしくは平日の深夜に行われていることが分かっている．すなわちマルウェアに感染した学生や職員の自宅のパソコン，もしくは自宅に持ち帰ったマルウェアに感染したノート型パソコンから，学内ICTサービスを提供する既知のサーバに不正にアクセスしていることが推測される（図2）．



（a）　（b）

（図 2）時刻毎に集計した高重要度インシデント発生数．学内端末によるインシデント（a）は朝 9 時頃から夜 8 時頃までの間に集中している．一方，学外からのアクセスによるインシデント（b）は，休日の昼間もしくは平日の夜間に発生している（グラフは合計値を示す）．

「内部ホストのボット感染の疑い」が検知された端末では，パソコンを遠隔操作するウイルスやワーム（ボット）に感染した可能性があり，感染した端末（ゾンビコンピュータ）は互いに連携し合い，特定のサイトを攻撃したり，大量の SPAM を送信したりする危険性があるので注意しなければならない．「NetBIOS サービスへの感染活動の疑い」は，Nimda 等のワームに感染した Windows 端末が，セキュリティ保護されていない Windows ファイル共有を通じて他の Windows 端末に感染拡大する活動を検知したものである．「内部ホストのウイルス感染の疑い（Gumblar）」が検知された場合，TYCOON 内にはガンブラー（Gumblar）に感染した端末が存在し，特定の Web サイトを改ざんしようと活動している可能性がある．また「DNS サービスへの調査活動の疑い」では，学内外の DNS サーバに対して無作為にアクセスを繰り返し，DNS に関する情報を収集する活動を検知している．この活動自体は特に障害を引き起こすことはないが，この収集情報を利用して、次の段階の不正アクセスを起す可能性は否めない．

以上のインシデント概要から，本学における不正アクセスの源は，TYCOON 内で教員や事務員が利用している端末や学生個人が所有しているノート型パソコンの一部がマルウェアに感染して生じている可能性が大きい．

3-2. IPS シグナチャ名による不正アクセスの原因の特定

それでは TYCOON に接続されたパソコン端末におけるどのような利用方法に問題があるのであろうか．マルウェアがパソコン端末に感染する経路には，1）電子メールのメッセージを経由，2）Web ブラウザを経由，3）ファイル交換（共有）ソフトを経由，4）ネットワーク（LAN）に接続するだけで侵入，5）USB

メモリやフロッピーディスクを経由，などのケースが想定される．これらのほとんどの経路については，パソコンの OS を最新の状態保ち（Microsoft update やソフトウェアアップデートのこまめな実施），ウイルス対策ソフトを導入して最新のウイルスのパターンファイルを用いた検疫を実施することで，その多くを遮断することができるはずである．しかし実際には IPS による多くの「不審な通信の遮断」が実施されている．この「不審な通信の遮断」の対象となった不正アクセスの具体的なトラフィックパターン（IPS シグナチャ名）を（表 2）に示す．

IPS シグナチャ名	件数	IPS シグナチャ名	件数
KuGoo P2P Activity	646	Rustock Botnet	58
Gnutella Client Request	612	uTorrent Activity	23
BitTorrent Client Activity	390	Limewire File Request	12
SQL Query in HTTP Request	193	JSIG-WEB:GUMBLAR-CTRL	8
Bittorrent Tracker Query	110	eDonkey Activity	7
UTorrent Client Activity	97	ET Trojan	1
Generic SQL Injection	89	合計	2246

（表 2）2012 年 4 月から 12 月の間に検出された IPS シグナチャ名と件数

この表から分かるように，全体の約 84.5%のシグナチャが KuGoo や Gnutella，Bittorrent などのファイル共有ソフトと関係がある．すなわち IPS による「不審な通信の遮断」の多くは，ファイル共有ソフトに対するものであると考えられる．TYCOON では，音楽や映像の違法な交換を促すファイル共有ソフト（P2P ソフト）については，著作権を侵害するおそれのあることから，その使用を禁止している（ただしインターネット電話サービスである Skype 等，元々別の目的で作成された P2P アプリケーションについては，使用を禁止していない）．そして『情報リテラシー』や『情報科学』といった学部授業の中で，これら違法行為を促すファイル共有ソフトを使用しないよう，担当教員は呼びかけを行ってきた．

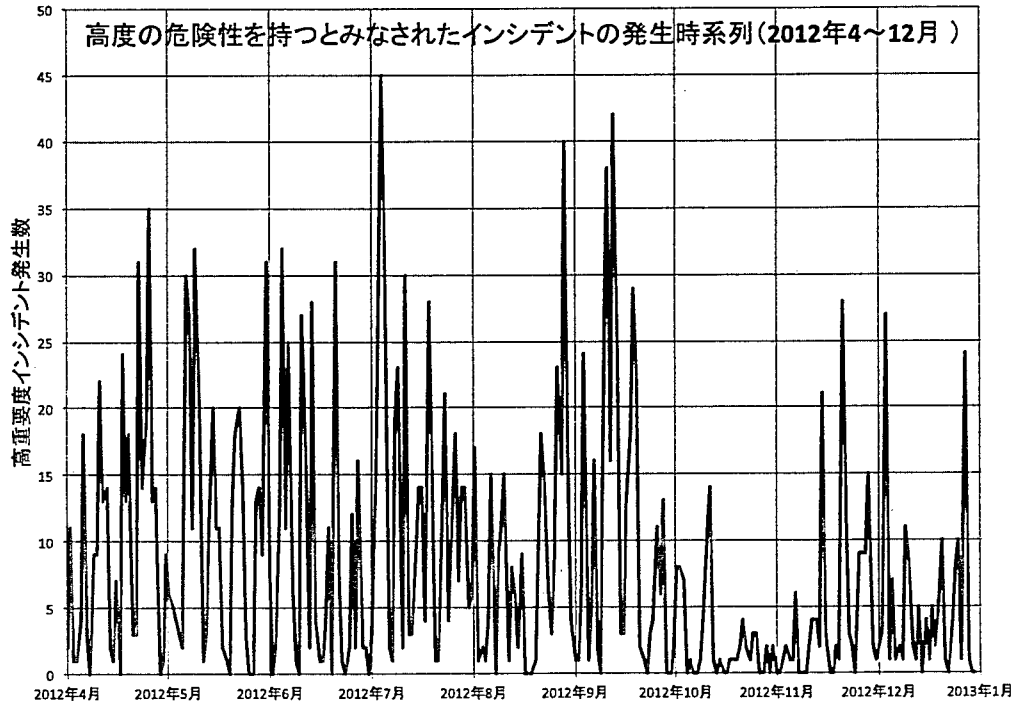
場所	件数
教育棟（教育 1～5 号館）	982
研究棟（研究 1～4 号館，医療薬学研究棟，DR 研究棟）	717
無線 LAN（学生会館，研究 4 号館，他）	259
学生会館 PIT	71
合計	2029

（表 3）TYCOON 接続端末から検知された不正アクセスのインシデント件数

しかし（表 3）が示すように，「不審な通信の遮断」は，学生が自由にノート型パソコンを接続できる教育棟を筆頭に，研究棟や無線 LAN 施設など，場所に関係なく行われているようにみえる．

3-3. ネットワークリテラシー向上キャンペーンの実施

前節のデータから，TYCOON 内における不正アクセスの諸要因は学内ユーザのネットワークの利用形態にあると言える．これに対処するための方策として，不正アクセスに関係すると思われる通信をポートのレベルで全て遮断してしまうことがすぐに思いつく．しかしその方法を強く押し進めると，有益である通信ツール，例えば P2P 技術を取り入れている Skype についても制限の対象になってしまう．またユーザに対するネットワークリテラシー教育の観点からすれば，ユーザの見えないところ（ブラックボックス）で安全かつ快適な環境をお膳立てすることは，ユーザの主体的なインターネットの利用を促進する上で，決して良い影響を与えるものでないと考えられる．



（図 3）高重要度のインシデント発生数の推移（2012 年 4～12 月）

こうした方針を踏まえ，情報教育研究センターでは個々のユーザに対する教育的配慮を第一に考え，1）**著作権法遵守**，2）**アンチウイルスソフトの利用**，3）**フィシングに関する注意喚起**，4）**ファイル共有に関する注意喚起**の 4 項目について，「ネットワークリテラシー向上キャンペーン」を 2012 年度に実施した．具体的には学内の講義室前の掲示板に，数種類のよく目立つカラーポスターを，

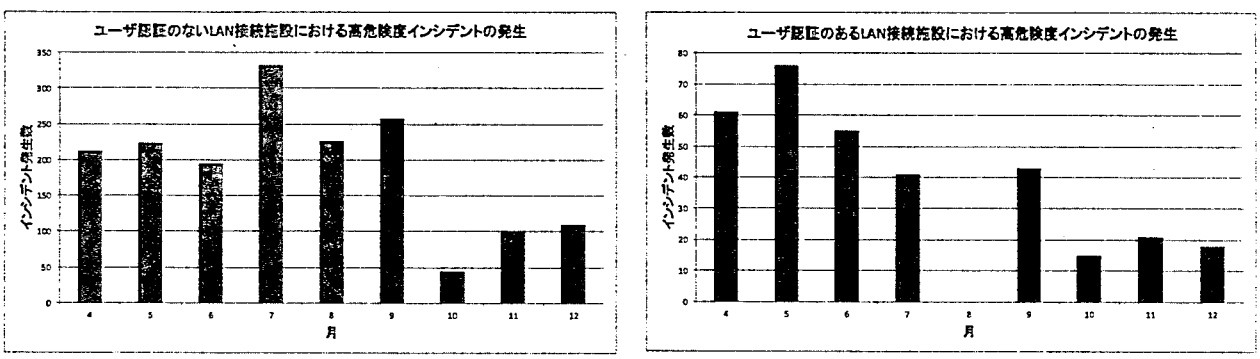
3つの時期（5/15～，11/15～，1/17～）に分けて掲示することから始めた．またマルウェアに感染したと思われる端末の管理者に対し，個別に注意喚起を行った．

（図3）に2012年4月から12月における高重要度のインシデント発生数の推移グラフを示す．まず5月中旬に不正アクセス数が一時的に減少している様子が見える．これは前述の第1回キャンペーンによるものではないかと期待している．次に8月を中心とした夏休みの時期は，予想通り不正アクセス数が減少していることが分かる．また9月後半から11月前半にかけて不正アクセスが大きく減少しているのは，2012年10月1日より「著作権法の一部を改正する法律」が施行され，いわゆる「違法ダウンロードの刑事罰化」が実施されるようになり，学生がファイル共有ソフトの利用を自粛し始めたことが原因ではないかと考えられる．但し11月中旬から再び不正アクセスの件数が増加しているが，前述の第2回キャンペーンが功を奏して，12月には再び減少しているようである．

このように2012年は，「著作権法の一部を改正する法律」の施行と情報教育研究センターによる「ネットワークリテラシー向上キャンペーン」により，総じて不正アクセスは減少の傾向を辿っていると言えるであろう．

3-4. 認証付きLAN接続施設の効用

近年多くの大学において，学内LANに接続するノート型パソコンやスマートフォン対して，ユーザ認証や機器認証を要求するケースが増えている．これは大学関係者以外が学内LANにアクセスすることがないようにするための，セキュリティ上の方策であるが，同時に学内ネットワークにアクセスしたユーザの履歴（ログ）を収集することもできる．本学では1995年より，学生のノート型パソコンをLAN接続できる講義室を設置しているが，このような認証システムを全学的に導入したのは，増改築された学生会館（旧厚生棟）にLANを敷設した2010年12月以降である．学生会館は学内の他の施設と異なり，学内関係者以外の出入りが非常に多い場所であるということから，有線および無線によるLAN接続についてユーザ認証を行うことにした．



（a）　（b）

（図4）ユーザ認証の(a)ない場合，(b)ある場合における高重度インシデントの発生

ユーザ認証を通じて LAN 接続を行うということは，アクセスの主体がユーザ個人であることを明確にすることでもある．また管理者側は，そのような不正アクセスを起こったユーザに対して注意喚起を行うことができる．その結果（**図4(b)**）に示す通り，ユーザ認証を必要とする端末からの不正アクセスは，5月の「ネットワークリテラシー向上キャンペーン」の実施後，減少に向かっている様子が見られる．これはユーザ認証と学生への注意喚起が組合わさった場合に見られる副次的な効果であり，リテラシーとしても効果的であると思われる．

4．今後の計画とインターネットの「玄関」

2012 年度における IPS による不正アクセスの解析と学生への注意喚起を含む「ネットワークリテラシー向上キャンペーン」は，TYCOON における不正アクセス，特にファイル共有ソフトの利用による意図しない不正アクセスの防止および学生への情報リテラシーに有効であることが分かった．今後は教育 4 号館を中心とする教育棟における LAN 接続ユーザ認証化を推進し，同時に教育の中で情報リテラシーの向上に努めていきたいと考えている．しかしセキュリティの根本的問題解決は，このような単純な対応だけでは到底十分とは言えないことを心に留めておくべきである．

「玄関」とは，建物の出入口に設けられている空間であるが，禅における「玄妙の道に入る關門」という意味に語源を持つ．「玄妙」とは，大辞林第三版によれば「道理や技芸が，奥深く微妙なさま」とある．またさらに時代を遡れば，禅の成立に強い影響を与えた『老子』の中に「玄牝の門」という言葉を見いだすことができる[6]．TYCOON には，ファイアウォールや LAN 接続口を始めとする様々なインターフェイスが存在するが，これを禅や老子で謂うところの「玄関」とみなした時，我々は情報教育におけるより深い哲学と論理の必要性，そして広い意味での情報学への希求を思いめぐらすのである．

【参考文献】

[1] 森河良太，林昌樹，宮川毅，土橋朗，東京薬科大学研究紀要，第 1 号（1998）77-84.

[2] 松崎日出海，濱田真向，宮川毅，森河良太，小杉義幸，加藤哲太，平成 19 年度情報処理教育研究集会（2007）

[3] 倉田香織，土橋朗，東京薬科大学研究紀要，第 10 号（2007）57-64.

[4] 森河良太，萩原明子，松崎日出海，宮川毅，東浦康友，東京薬科大学研究紀要，第 14 号（2010）53-59.

[5] 森河良太，宮川毅，林昌樹，東京薬科大学研究紀要，第 10 号（2007）77-82.

[6]「谷神不死 是謂玄牝 玄牝之門 是謂天地之根 緜緜若存 用之不勤」（『老子』第 6 章）