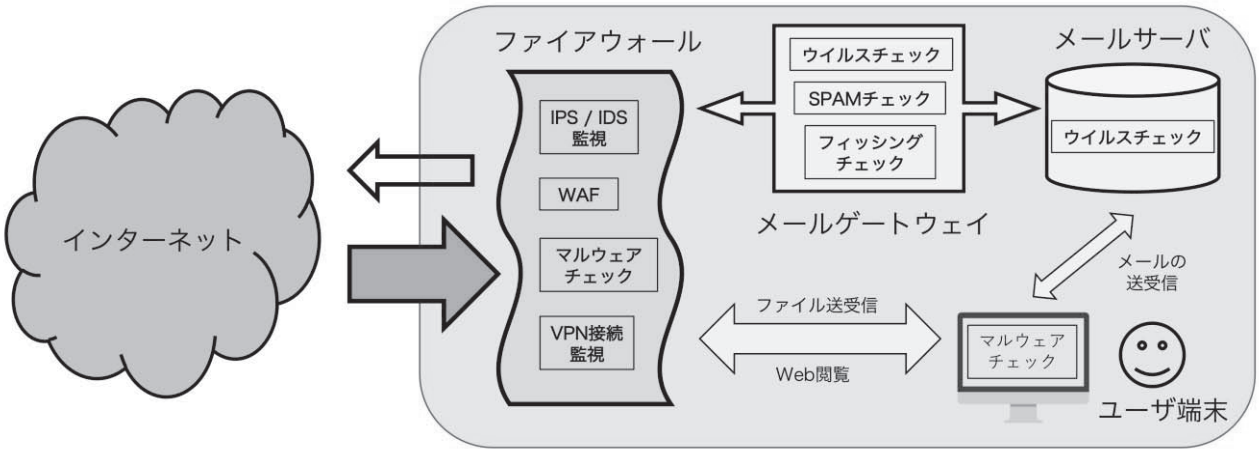
強化されたTYCOONのセキュリティと今後の課題

森河良太[1]，倉田香織[2]，宮川毅[1,2]，土橋朗[2]

1．はじめに

Windows 95の発売とWebブラウザの日本語化が行われた1995年を，日本では「インターネット元年」と呼んでいる．それから20年以上が経過する中で，日本のインターネットは学術ネットワークから享楽目的の商用インフラに変化し，携帯電話やスマートフォンの登場がそれに追い打ちをかけた．同時に個人情報が21世紀における新しい石油と呼ばれるようになり，様々な不正な手段を用いて盗まれるようになった．こうした時代の変化の中を，東京薬科大学情報ネットワークTYCOON（ToYaku COmputer Open Network）は，学術ネットワークとしての初心と目的を守りつつ，様々な障害に対処しながら変化し続けてきた．

本稿は2016年8月から2017年6月にかけて実施されたTYCOONのセキュリティを守るためのシステム更新（**図1**），特に**ファイアウオール**（Firewall，防火壁）とそれを補うための**メールゲートウェイ**の強化とその技術について述べる．



（図1）様々な不正アクセスからTYCOONを守るシステムの概要図（2018年1月現在）

2．TYCOONのファイアウォールにおける次世代への進化

2-1．IPS監視の限界と次世代ファイアウォール

ファイアウォールは，インターネットとイントラネットとの通信を監視・制御する役割を担う，組織内LANの「関所」である．本学でも2007年8月，本格的なセキュリティ監視機能であるIPS（Intrusion Prevention System：侵入防止システム）を備えたアプライアンス型ファイアウォール（ASA-5520，Cisco社）が本学ネットワークTYCOONに設置された．IPSでは，ファイアウォールを通過する通信を監視するIDS（Intrusion Detection System）を使い，不正アクセスに

[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

関係する通信であるかどうかを，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）に基づいて判定し，必要に応じて隔離または破棄する．OSI参照モデルの視点から見れば，低階層のレイヤ3（ネットワーク層）またはレイヤ4（トランスポート層）における通信パターンを，高階層（レイヤ）における通信の種別とは無関係に解析することになる．それゆえシグナチャのパターンが似ている場合，誤検知に繋がるような判定を行う可能性もある．またIPSよる検知は基本的にデータベースに依存するので，新種の不正アクセスを検知することはできない．この2つの欠点を補う新技術がそれぞれWAF（Web Application Firewall）と**サンドボックス**（sandbox：砂場）であり，これらの仕様を持つファイアウォールは**「次世代ファイアウォール」**と呼ばれる．

2-2. 次世代ファイアウォールの特徴

レイヤ3およびレイヤ4で通信制御を行う従来のファイアウォールは**パケットフィルタ型**と呼ばれ，通過するパケットがどのようなアプリケーションのものであるか，IDSなどで推測するしか方法はなかった．しかしコンピュータ機器の処理能力の向上により，レイヤ7（アプリケーション層）において通信を制御できる**アプリケーションゲートウェイ型**のファイアウォールが登場し，監視している通信がどのようなアプリケーション（HTTPやSSHなど）に結びついたものなのかを特定できるようになった．またそれに伴い，通信の内容（コンテンツ）の識別も可能となり，不正アクセスの判定をより正確に推測できるようになった．これらの能力を利用したファイアウォールがWAFであり，豊富な実績を持つIPSと併用することで，イントラネットへの不正アクセス防御効果も向上する．

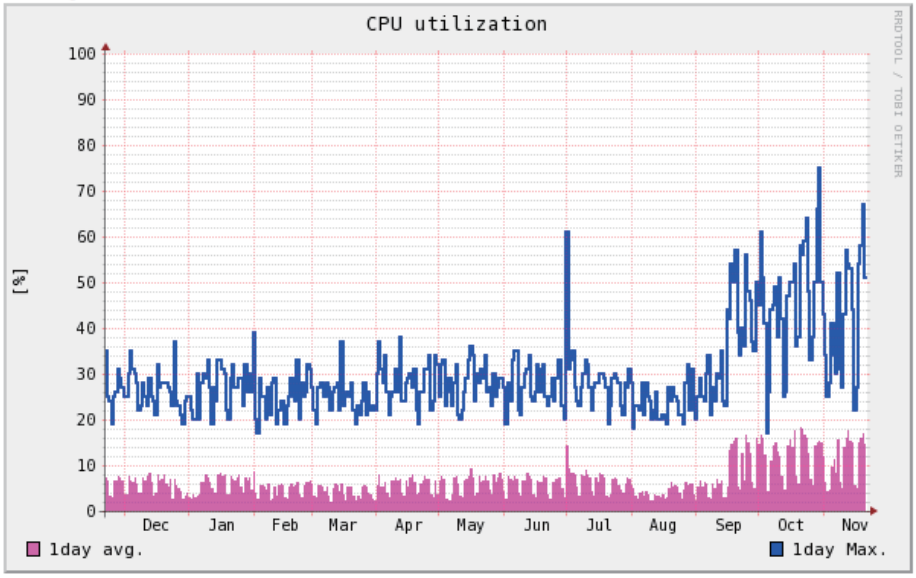
しかしWAFもIPSの場合と同様に，未知（新種）の不正アクセスに対しては全く無防備である．特に特定の組織内の情報を狙って行われる**標的型攻撃**（Targeted threat）は，その個別性から，データベースに登録されていない不正アクセスのパターンやマルウェアを使って行われる場合が多い．このような不正アクセスに対して**サンドボックス**が有効であるとされる．サンドボックスは，通信に含まれるスクリプトやプログラムなどを安全に保護された領域（**「砂場」**）で動作させることにより，システムが不正に操作されないかチェックする仕組みである．このデータベースを必要としない不正アクセス検知システムは，研究的視点からも大変魅力的な技術ではあるが，導入のためのコストが高いことがデメリットとして挙げられる．また最近は「砂場」であることを検知して，平静を装うマルウェアも出現しているので，サンドボックスを導入したからと言って，絶対に安全であるとは言えない．

2-3. TYCOONにおける次世代ファイアウォールの導入

前述のように，2007年8月にTYCOONに導入したアプライアンス型ファイアウ

ォール ASA-5520（Cisco 社）は，IPS によるセキュリティ監視は行うものの，次世代ファイアウォールとしての機能は装備していなかった．そのため近年急増する新種の不正アクセスの脅威からの防御を想定すると，技術的に十分な仕様を備えているとは言い難かった．

また 2014 年 8 月に，TYCOON から **WIDE（WIDE プロジェクト；100Mbps）** 経由したインターネット回線に加え，**SINET（学術情報ネットワーク；1Gbps）** を経由した回線も並列冗長化して開通させたことから，同年 9 月以降の TYCOON からインターネットへの通信量が増加した．それに伴い，ファイアウォールにおける CPU の最大負荷がそれまでの 40％程度から 60％程度へと増大し（**図 2**），古い技術仕様で構成される機器(ASA-5520)に大きな負荷がかかるようになった．そのためファイアウォールにおける通信データの処理が，インターネット通信速度のボトルネックとなった．



（図 2）旧ファイアウォールにおける CPU 負荷(%)の最大値(青色)と 1 日の平均値(桃色)．2013 年 11 月下旬～2014 年 11 月下旬のデータによる．

さらに機器の導入から 9 年が経過していたこともあり，ハードウェア自体の老朽化も目立つようになってきた．そこで 2016 年 8 月，冗長化された 2 台のファイアウォールを，高性能かつ高機能な次世代型ファイアウォール（**PA-3020，Palo Alto** 社）へ更新した．Palo Alto 社のファイアウォール（PA シリーズ）は，既に TYCOON 内の 2 つの独立ネットワーク(事務系ネットワークと CBT ルームネットワーク）で導入されており，十分な通信性能と耐久性が確認されていた．

PA-3020 の導入により，ファイアウォールにおける通信データの受け渡し速度（**スループット**）は，スペック値にして ASA-5520 の 450Mbps から 1Gbps に強化された．また PA-3020 はアプリケーションゲートウェイ型のファイアウォールで

あるため，WAF やサンドボックスも搭載可能である．計画当初はこれらの新機能を全て搭載することも検討されたが，次世代型は総じて導入および保守費用が大変高いため，費用対効果を考慮し，最終的には搭載するセキュリティ監視・防御機能を（**表１**）のように限定した．ただしサンドボックスや URL フィルタなど，未導入のオプションを将来において追加することはライセンス（費用）の問題だけであり，後日，必要に応じて搭載することは可能である．

オプション搭載機能	用途説明	導入
Threat prevention subscription	ウイルス，スパイウェアからの脅威防御，IPS	○
GlobalProtect Gateway	VPN 通信における不正侵入防御	○
PANDB URL filtering	不正な Web サイトに対する URL フィルタ	×
WildFire	未知のマルウェアを検証・検知（sandbox）	×

（表１）新ファイアウォール（PA-3020）の機能とオプション機能の導入状況

一方，（**表１**）の **URL フィルタ**については，学問の自由を重んじる大学では必ずしも歓迎される仕様ではなく，むしろ Web サイトへの不必要なフィルタが，教育・研究の邪魔になる可能性さえある．本当に必要とされるのは，電子メールを媒介とした**フィッシング詐欺**（メール本文に表示した URL へのリンクを使い，ユーザを不正な Web サイト誘導し，個人情報を盗む犯罪）への対策としての URL フィルタであろう．ちょうど 2015 年頃より，本学のユーザ宛に届く電子メールにはフィッシングを目的とした標的型攻撃メールが増加しており，そのための対策を講ずることも情報教育研究センターの急務であった．

３．SPAM フィルタからメールゲートウェイへ

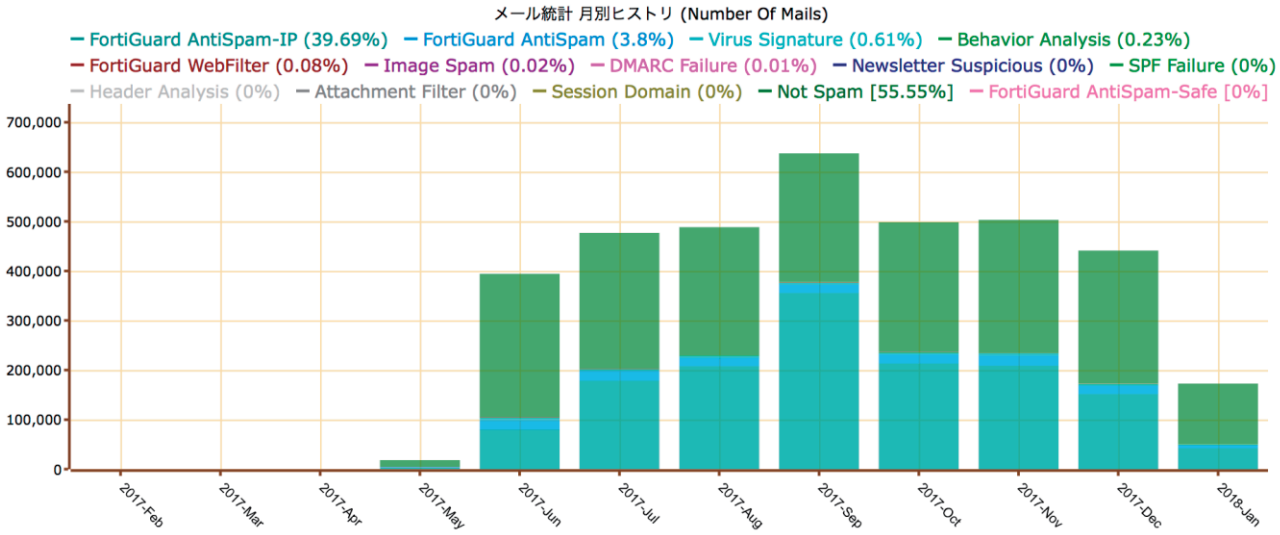
3-1. 電子メールを侵入経路とした PC クライアント攻撃

IBM は全世界 8 拠点にセキリティ・オペレーション・センター（SOC）を設置し，セキュリティ・イベント情報を収集している．その中で東京に設置された Tokyo SOC における 2017 年上半期の情報分析レポート[1]によれば，クライアント PC へのマルウェアによる攻撃の経路の 93.5%は，電子メールによるものであるという．この傾向は 2016 年上半期からほぼ変わっていないが，メールに添付されたマルウェアの種別は大きく変化している．特に組織内メールを装うために，日本語のファイル名を持つマルウェアを添付したフィッシング詐欺が増えている．前節で紹介した新ファイアウォール PA-3020 にも，こうした**フィッシングメール**を防ぐための URL フィルタがオプションとして提示されているが，それよりも SMTP（Simple Mail Transfer Protocol）によるメール送受信そのものを中継する**メールゲートウェイ**において，マルウェアやフィッシングメールをチェックした方が，より細やかな判別・対応ができると考えられる．

3-2. TYCOONにおけるメールゲートウェイの更新と強化

本学には，**SPAM（迷惑メール）**をメールゲートウェイにて除去する**SPAMフィルタ装置**が2008年4月より導入されていた．このSPAMフィルタ装置として**Ironport社**の製品（現Cisco社のESA）を選定し，8年間（最初の4年間は型式C350，2012年5月にC370へ更新）利用していた．その性能は非常に高く，SPAMの誤検知率は世界で最も低いと言われており，大変信頼のおける製品であった．しかし導入および維持コストが非常に高いことから，ウイルスやスパイウェアからの脅威防御オプションについては契約を行わず，メールサーバ（Zimbra）内でウイルスチェックを行っていた．そのため本学のユーザを狙ったフィッシングメールの増加が顕著になってきた2016年上半期から，Ironportの持つ**レピュテーション機能**（不審なメールを送信するメールサーバのリストを元に行うSPAMフィルタリング）以外にフィッシングメールを削除する手段が無くなってしまった．

そこで2017年6月に更新を予定していたSPAMフィルタ装置の後継機種として，メールに添付されたウイルスやスパイウェア，本文に記載されたフィッシングURLを個別に削除することができ，なおかつ導入と維持のコストを大幅に下げることのできる**Fortinet社**のメールゲートウェイ（**Fortimail 400E**）に更新した．この製品は，SPAMフィルタとしてはIronportに比べて1ランク精度が落ちるものの，大変安価であり，メールゲートウェイにおける最新の脅威防御に必要な機能がほぼ全て搭載されている．ただし残念ながら前述のサンドボックスについては別売りであり，ほぼ倍の導入コストが必要となるため，今回は導入を見送った．また SPAM メールである判断基準については，ユーザ側でパラメータを詳細に設定することができるが，同時にその調整に時間と手間がかかる．



（図3）新メールゲートウェイで解析された本学における受信メールの状況．SPAMの判定で最も適用された方法は，送信元のIPアドレスによる判定である．

（**図 3**）に 2017 年 6 月から 2018 年 1 月中旬までに，本学メールシステムに届いた受信メールの解析結果を示す.届いたメールの 44.45%は SPAM かウイルスメールであると判定されている．前回，SPAM フィルタ装置を更新した 2012 年 5 月では，96.5%の受信メールが SPAM であると判定されていたことを考えると，メールを介した不正アクセスが本学でも**「迷惑」な総当たり手段から「巧妙」に仕組まれた標的型に切り替わっている**様子が伺える.

４．今後の課題：プライバシーと自由な社会

インターネットの世界において，これからも更に「巧妙」な手口を使い，個人情報を盗もうとする犯罪が増加することは確実であろう．加えて AI(人工知能)の急速な進化が，その「巧妙」さを助長していくことは想像に難くない．逆に不正アクセスを防ぐ技術にも，AI が導入されていくであろう．こうした「いたちごっこ」のような人間社会の闘争は，人間が自らの個人情報を放棄しない限り，ずっと続くのかもしれない．しかしその闘争を最新の ICT 技術が補佐してくれることはあっても，それを過信して個人情報を丸々委ねてしまうことは，本来は主体的に入出力を制御すべきプライバシーの放棄に繋がるのではないかと考える．そうなると実体の定かでないクラウド(既に AI も組み込まれているかもしれない)のようなものに，「便利」,「手間要らず」という理由で個人情報を無垢に預けてしまうことは，危険極まりない行為と言える.

インターネットからプライバシーを守るためには，最終的にはユーザ自身が不正アクセスの「巧妙」さに騙されないよう，日頃から不正アクセスに関する情報に気を配り，論理的かつ冷静に ICT 機器を操作するしか方法はない．しかしそうなると，我々もそれに疲れ果てるかもしれない．実際，個人情報の漏洩事件は日常茶飯事のことであり，刺激的なニュースではなくなっている．逆にビックデータの活用が経済を活性化させると言い，個人情報が合法的に吸い上げられることを黙認させる風潮がみられるのではないか.

NSA(米国家安全保証局)による個人情報収集の手口（PRISM 計画）を告発したエドワード・スノーデン氏は,「大量監視社会」に関するインタビューで次のように述べている：「*『隠すものがないなら、恐れることはない』というのは第二次世界大戦時のナチスのプロパガンダから来ています。これは、問題点をずらした考えです。プライバシーというものは、隠すための何かではありません、守るための何かです。人々が違ったままでいられる、人々が自分自身の考えを持てる開かれた社会、自由な社会を守るためのものです。*」[2].

【参考文献】

[1] https://www.ibm.com/blogs/tokyo-soc/tokyo_soc_report2017_h1/（2018.1.18 確認）

[2] 軍司泰史,『スノーデンが語る「共謀罪」後の日本』, 岩波ブックレット（2017）