アプリケーションの変化における課題とセキュリティ対策

斉藤 晃一
株式会社日立ソリューションズ　ネットワークプロダクト部
koichi.saito.uf@hitachi-solutions.com

概要：大学キャンパスのネットワークでは、様々なアプリケーションが利用されています。近年、利用されるアプリケーションが変化しており、その利用状況を把握することが困難になっています。アプリケーションの識別、制御を実現し、安全かつ利便性が高いネットワークを構築することが必要です。

キーワード：セキュリティ、ファイアウォール、情報漏えい対策、P2P 対策

1. はじめに

今、アプリケーションの利用が大きく変化しています。

米国企業 Palo Alto Networks 社が、2010 年 3 月から 9 月の間に世界 720 の組織において実施したアプリケーションの使用に関する調査結果をまとめました。この報告書では、特に以下の 3 つにフォーカスしています。

①Web メールやインスタントメッセージングなどのアプリケーションによる「発言」
②ソーシャルネットワークアプリケーションによる「交友」
③P2P や Web ベースのファイル共有アプリケーションによる「ファイル交換」

この調査で大多数が利用しているアプリケーションは、グローバルな視点でみても同じような利用がされています。Facebook は全世界的にみても Web メールやインスタントメッセージングを超えて利用が進んでいます。代表的な Web メールである Gmail や Yahoo! IM は Facebook のメールとチャットにその場を追われようとしています。

224 種類の「発言」を行うアプリケーション（Web メール、IM)、「交友」のためのアプリケーション（SNS)、「ファイル交換」のためのアプリケーションが、96%の組織で確認されました。さらに、これらのアプリケーションによって消費されている帯域は全体の 1/4 に上ります。さらにこれらのアプリケーションは監視や制御がされることもなく、その結果、発信側においては情報の漏洩や損失やコンプライアンスの問題を引き起こしかねません。同様に受信側においては、これらのアプリケーションはマルウェアの転送および脆弱性の露見を起こす可能性があります。

クラウドベースのアプリケーションの利用が進んでいることも示されています。ユビキタスなネットワーク接続によって誰が開発し、どこにホスティングされているかに関わらず、多くの人が利用しているアプリケーションがさらにその利用者を増やしています。調査対象全体、およびある組織におけるアプリケーションが利用される頻度、利用場所、そして消費する帯域の総量は、いかにそのアプリケーションの利用が拡がっているかを示す例となります。

これらの調査結果より、教育・研究などの目的で利用されるアプリケーション以外に、監視、制御すべきアプリケーションが数多く利用されていることが分かります。

（※出典元：アプリケーション利用とリスクに関する報告書 第 6 版 2010 年 10 月 Palo Alto Networks）
http://www.paloaltonetworks.jp/literature/forms/aur-report.html

これらの「発言」「交友」「ファイル交換」アプリケーションは、学内でどれくらい使用されているのでしょうか。さらには Twitter、2 ちゃんねる、ブログの閲覧、更新はどれくらいされているか、YouTube、ニコニコ動画はどれくらい視聴されているか、そして、これらのアプリケーションが使用しているネットワークの帯域はどれくらいでしょうか。

2. キャンパスネットワークに求められる課題と対策

我が国では IT 化が進む中で、多くの大学

が PC を利用した授業を取り入れ、学生それぞれに PC を用意し、キャンパス内から有線・無線で自由にインターネットへアクセスできる環境を提供している学校が数多く見られます。

そのような環境の中で大学のネットワークでは、「安全かつ利便性の高いネットワーク」の構築が求められています。安全なネットワークの構築には、大学のセキュリティポリシーで定められた内容をきちんと運用できることが重要です。

例えば、大学のセキュリティポリシーの中に、P2P アプリケーションの利用を禁止するポリシーがあるとします。P2P アプリケーションの利用については、分散ストレージ、CDN（Contents Delivery Network）など正当な目的で利用されている場合もあります。しかしながら、「Winny」「Share」をはじめとする P2P アプリケーションの多くは、著作権の侵害や、操作ミス、ウイルス感染などによる個人情報の漏えいを引き起こす可能性が高いため、使用を禁止する大学が増えています。その場合、そのセキュリティポリシーをきちんと運用できているのかが重要です。

安全かつ利便性が高いネットワークの構築には、
①不正に利用されるアプリケーションの制御
②外部及び内部ネットワークを経由するマルウェア等の脅威検知
③アプリケーションやユーザによるポリシー設定や管理が柔軟に行えること
が必要です。

2.1　アプリケーションの利用抑止

課題：
アクセス制御が必要なアプリケーションは「Winny」「Share」等の P2P アプリケーションだけではありません。動画や音声などの帯域を大幅に消費するアプリケーションの利用はネットワークに負荷をかけ、他のユーザに遅延やネットワークの切断の影響を与えます。また、オンラインゲームや動画観賞など学業に関係の無いもの、フィッシング詐欺などのサイバー犯罪など、Web アクセスを中心としたセキュリティも向上させる必要があります。

さらに検出を回避するアプリケーションが多数存在しています。その中には、自身を正当なトラフィックのように偽装していたり、ポート番号を動的に変更したり、SSL 暗号化されたトンネルを介してファイアウォールをすり抜けたりするものもあります。こういったアプリケーションの例には、インスタントメッセンジャー、RSS、Web メール等があります。これらの多くのアプリケーションはデータ損失、プライバシー侵害などを引き起こす可能性が十分にあります。

Web メールやインスタントメッセージング、2 ちゃんねるなどの掲示板、Facebook/mixi（ミクシィ）などの SNS は、ファイルだけではなく、テキストの書き込みで情報漏えいが発生するケースがあります。

また、「Winny」「Share」など、特定のアプリケーションのみを検知するための対策の一例として、不正侵入防御システム（IPS）の導入があります。しかし、一般的な IPS は、アプリケーションのカテゴリー分類が粗く、検出精度に問題がある場合もあり、P2P を含むアプリケーションを制御するには不十分と言えます。

対策：
ネットワーク上の流れるアプリケーションを正しく把握する必要があります。「ファイル交換」の P2P アプリケーションだけではなく、「発言」「交友」に使用されるアプリケーションを識別し、アクセスを制御する必要があります。
大学のセキュリティポリシーに従ったルールを適用し、これらのアプリケーションの使用を制限する必要があります。

2.2　マルウェアへの対策

多くの大学が、ネットワークを経由するマルウェア等を検知・ブロックするためのセキュリティ機器を導入しています。このセキュリティ機器の一例として、統合脅威管理（UTM）があります。マルウェアなどの巧妙化した攻撃に対するセキュリティを、簡単かつコストをかけずに実現するために、ファイアウォール / アンチウイルス /IPS/URL フィルタリング機能などがオールインワンで搭載された UTM が考案されました。

しかし、学内全てのトラフィックに対してこれら複数の脅威を検知しようとした場合、セキュリティ機器のパフォーマンスが大幅に劣化することが予想されます。これはこれまでの UTM 製品が、従来の FW/VPN 製品の機能上に、アンチウイルス、アンチスパイウェア、不正侵入防御（IPS）、URL フィルタリング機能を個別に実装したため、それぞれのエンジンで順に処理されるオーバーヘッドがパフォーマンス低下につながるためです。そのため、学内 LAN のゲートウェイに UTM を設置し、全ての機能を利用している大学は少ないと言えます。

また、フィッシングサイトへの Web ブラウジングのセキュリティ対策として URL フィルタリングの導入がありますが、この URL フィルタリングを回避する手法も数多く存在します。その一つが、インターネットで公開されているプロキシサイトを踏み台にし、URL フィルタリングで禁止されている Web サイトにアクセスする手法です。この方法では URL フィルタリングで検知することができません。この手法はインターネット上で一般に公開されており、誰でも簡単に利用することができます。よって、URL フィルタリングの導入だけで安全なネットワークということはできません。

対策：
アクセス制御だけではなく、ウイルス、スパイウェア、不正侵入、URL フィルタリングへの対策が必要です。ゲートウェイ（ファイアウォール）だけではなく、クライアント PC での対策も必要になります。
これらの複数のセキュリティ機能を使用してもパフォーマンスの低下が小さければ、複数のセキュリティ機器を 1 台に集約することができ、導入、運用のコスト削減を図ることができます。

2.3　柔軟なポリシー設定

課題：
P2P アプリケーションの利用を禁止するといったアクセスコントロールリストによるポリシー制御が運用されている場合、学生の著作権侵害や、情報漏えいの防止、ネットワーク帯域幅の確保に繋がり、安全なネットワークの構築が可能になります。

しかしその一方で、正当な目的で P2P アプリケーションを利用したいというニーズもあります。例えば、遠方の研究室同士を繋ぎビデオ通話を行うために利用する P2P 技術を使ったアプリケーション「Skype」があります。

「Skype」は無料の音声通話、ビデオ通話、インスタントメッセージをインターネット経由で利用することができるアプリケーションです。「Skype」を利用すれば、料金、時間、距離を気にせず、研究室同士でテレビ会議をすることが可能です。ただし既知の脆弱性や帯域の浪費など、全てのユーザに許可するにはリスクも伴います。

このように、セキュリティは強化しつつ、個々のユーザビリティを向上したいというニーズがあった場合、ネットワーク機器のポリシー設定は煩雑になりやすいと言えます。

対策：
アプリケーションの識別だけではなく、ユーザの識別が必要です。またアプリケーションとユーザを組み合わせたアクセス制御を柔軟に設定することで、大学のセキュリティポリシーを実現し、ユーザの要望にも柔軟に対応することができます。

リアルタイムでそのアプリケーションを利用しているユーザを特定する必要があります。また、ユーザをただ表示するだけでなく、そのユーザが関連している脅威、帯域消費やセッション数、トラフィックの送受信場所も閲覧できると便利です。さらに、そのユーザがアクセスしているその他のすべてのアプリケーションを簡単に調査することができると、管理者はそのユーザが使用中のすべてのアプリケーション、帯域消費、セッション数などを一覧で確認することが可能になります。

3.　まとめ

様々なアプリケーションが利用される大学のネットワーク環境においては、まずネットワークで「利用されているアプリケーションを把握」することが肝要です。

安全なネットワークの構築には、利用されるアプリケーションの制御に加えて、外部及び内部ネットワークを経由する「ウイルス、

マルウェア等の脅威検知、不正侵入防御」が必要です。

利便性が高いネットワークの構築には、ユーザを識別できることで、ユーザの要望にこたえる柔軟なポリシー設定（アクセス制御）が必要です。

① ネットワークを流れるトラフィックをアプリケーションで識別、制御する必要があります。
例えば不正な目的で利用される P2P アプリケーションを制御することで、著作権侵害や情報漏えいを防止することができます。
またネットワーク帯域を大幅に消費する動画 / 音声などのアプリケーションを制御することで、帯域を確保することができます。

② 複数のセキュリティ機能（アンチウイルス / アンチスパイウェア /IPS/URL フィルタリング）を使用する必要があります。
これらの機能を同時に利用してもパフォーマンス低下を最小限にすることができれば、セキュリティ機器を 1 台に集約でき、導入と運用のコスト削減が可能です。

③ ユーザ / 研究室毎の柔軟なポリシー設定やアクセス管理ができると、ユーザビリティを向上させることが可能です。
例えば研究者は「Skype」を利用することができるが、学生は利用できないといった制御ができると便利です。