学内 PC へのセキュリティ調査の結果について

総合情報基盤センター　助教　沖野　浩二

サイバーテロという言葉がニュースに取り上げられ、社会的な問題として、認識されている。実際に、本学も多くのサイバー攻撃を受けている現状があり、これらのサイバー攻撃の被害を未然に防ぐために、学内に対して、セキュリティ調査を行った。

本稿では、サイバー攻撃の現状とセキュリティ調査の意義を述べ、今回のセキュリティ調査について説明する。最後に今回の調査結果について述べる。

1．サイバー攻撃の現状

本学は、現状として多い日では、100 万回/日以上の攻撃を受けている。この攻撃の中身を分析すると、

・攻撃の事前調査（Port scan）
・SSH へのブルートフォース攻撃
・実サービスへの攻撃

に分類できる。

実際には、SSH などを除けば、頻繁な直接攻撃を行うのではなく、事前に相手の情報を収集することが多いという結果が分かる。

これは、現在のサイバー攻撃は、効率的な攻撃を行うために、事前に収集された情報を利用することが多いからだと考えられる。具体的には、google 等の検索エンジンを利用し攻撃に利用するファイルがあるか調査を行うことや、shodanhq(図 1)などのサービス・OS 検索エンジンを利用して攻撃の成功確率が高いものに限って攻撃を行うことが知られている。

図 1　shodanhq Web Page

ここでは、shodanhq を利用して、あるメーカの Printer を調べた例を示す(図 2)。

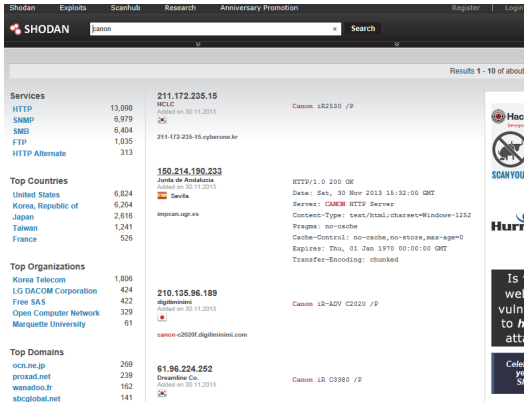

図 2　Printer の検索

ただし、現在はこれらの検索を行うためには、ユーザ登録を行う必要がある。

実際に、本学で発生したインシデントとして、この shodanhq エンジンを利用し、あるメーカの Printer を特定し、攻撃された事例がある。この攻撃では、shodanhq を利用して、Printer の種類を特定した上で、この Printer の Default Password を利用し、無意味な印刷を多量に行う攻撃が行われた。

これらの攻撃では、攻撃者が事前に情報を有しているために、OS やアプリ脆弱性、初期設定や設定ミスに対し、効率的な攻撃ができる。このような攻撃手法で情報を取得した事例として、関東地方の公立大学における NAS(Network Attached Storage)の設定ミスからの情報漏えいが挙げられる。

２．キュリティ確保の現状

２．１　FWでのセキュリティの確保の限界

このような状況な中で、セキュリティを確保するには、FW 等を利用し外部からの通信をコントロールし、セキュリティを確保することとなるが、大学においてすべての外部からの通信を遮断することは難しい。加えて、FW など外部からの通信のコントロールでは、学内に入ってしまった Virus など、内部からの攻撃に対しては無力である。実際に学内で観測された Virus が Port Scan を行っている例を示す（図 3）。

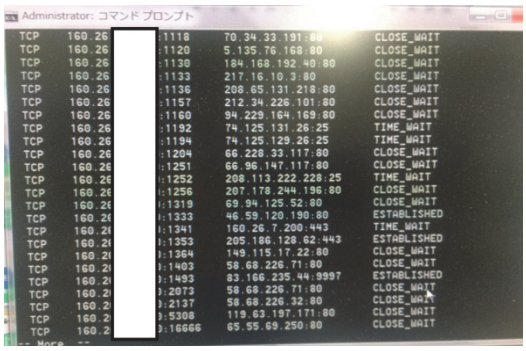

図 3 Virus 感染 PC からの Port Scan

この場合は、学内から学外に対して SMTP,HTP,HTTPS 等に対してアクセスし、情報収集を行っている。過去に本学で検出された Virus には、同様の動作を学内の IP に対して行っているものも観測されている。今後、持ち込み PC の増加により、このような内部からの攻撃が増えることは容易に想像できる。

２．２　持ち込み機器のセキュリティ

本学では持ち込み情報機器への対応として、無線ＬＡＮ環境が整備されている。2015 年 1 月現在、ピーク時には 1000 台程度の情報機器が接続されており、Windows や Mac だけでなく Android や iOS などのスマートフォンやタブレットが接続されている。これらの持ち込み情報機器のセキュリティの確保は各ユーザに任せられているが、実際にセキュリティ対策を行っているユーザは少ないと考えられる。特に Android 端末に関して、セキュリティソフトを入れる必要性を認識しているユーザは少ない。加えてスマートフォン等に導入している OS だけでなく、導入されているアプリにも UPDATE が必要だと認識しているユーザはさらに少ない。

２．３　学内設置機器のセキュリティ

学内ＬＡＮに接続される機器は、何もＰＣやスマートフォンなど個人が利用する機器だけでなく、複合機や Printer、NAS、ルータなどもある。これらの機器にも、内部に OS やアプリが動作しており、また Network 越しに利用するために、admin などの管理者 ID が設定されている場合が多い。

また、これらの機器上では、HTTP などのサービスが動作している場合がほとんどである。

しかし、機器の設置者が、管理者 ID やサービスが攻撃に利用されることを防ぐために、パスワードを変更することやファームウェアの UPDATE を行うことは少ない。実際に、これらの脆弱性を利用した Worm が存在し、Linux が組み込まれたルータに感染を広げている。

２．４　Web サーバ等のセキュリティ

一般に Web 等のサーバは、OS 上に HTTP サーバ起動されるのが基本であり、その上に目的に応じて PHP や Perl, Java Servlet 等のミドルウェアと呼ばれるアプリケーションや DB サーバを組み合わせて構築される。有名な例としては、LAMP（Linux+Apache+MySQL+PHP,Perl 等）と呼ばれるものが代表的なものである。（図４）

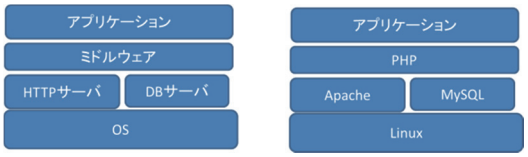

図４　Ｗｅｂサーバの構成

これらのサーバに対して行われる代表的な攻撃手法として代表的なものは、下記のように構成要素ごとに挙げられる。（図５）

図５　Ｗｅｂサーバへの攻撃 Point

実際にセキュリティを確保するためには、これらのすべてを認識し、対応していく必要がある。

２．５　EoL

2014年4月にMicrosoft社のWindowsXPはEoL(End of Life)を迎えた。EoLは、製品のセキュリティ・機能維持の終了を意味し、EoL後に、そのOSを利用するには、セキュリティを確保するための別の手段を用意しなければならない。

Microsoftでは、製品のEoLを通知しているので、利用者は危ないVersionを知ることができるが、他のOSではEoLを通知しているものは多くない。具体的には、Mac OS XやAndroidは公表していない。また、ハードウェアと一体としている複合機やＮＡＳなども公開はされていない。これらのセキュリティ状態を管理者が知ることは難しいのが現状である。

加えて、Webサーバ等のセキュリティで述べたApacheやMySQL、Java、PHPなどのOS上で動作するミドルウェアにも同様にEoLが存在し、セキュリティを守るには、これらの情報も含めて、収集する必要がある。

3. キュリティ調査の意義

ユーザは、導入時に意識的に危ない設定を行うことはなく、外部からの攻撃で利用されるセキュリティ上の問題は、ほとんどの場合、

・設定ミス
・初期Passwordの利用
・導入後発見された脆弱性
・他のシステムのID/Password

によるものである。管理者は、定期的に自分の管理しているシステムに対して設定ミスがないか、新しい脆弱性がないかを調べて、それらの問題に対応する必要があるが、実際にこれらの対応を行っている管理者は少ない。

今回、導入後経過した機器のセキュリティ対策として、総情報基盤センターにて、学内の機材に対してScan Portおよび簡単な攻撃を行った。特に、今回の調査では、すべての脆弱性をなくすこと目的とはせず、リスクの高いEoLを迎えたOSやメーカが近年セキュリティ対策を行っていないOSやミドルウェア、デフォルトIDやPasswordを利用している機器、外部から特権を取得可能な脆弱性などの調査を行った。Webアプリケーションの脆弱性診断はコストやその攻撃によりシステム停止等が発生する可能性があるため実行しなかった。

本調査では、予備調査として、センター機器に対して業者の指導の下、調査を行い、機器や評価方法を学んだうえで、センター職員が学内のアドレスに対して調査判断を行うこととした。調査に利用した機器はセキュリティ検査ソフトウェアである、商用版Nessusを利用した。商用のセキュリティソフトウェアを利用することにより、正確なEoLや脆弱性情報など付加情報も含めて判断することとなり、Portが空いているなどの簡単なセキュリティ調査ではない、より正確な情報が取得できる。加えて、調査結果の可視化や検査結果の蓄積を行うことができる。

4. セキュリティ調査の結果

セキュリティ調査を行うと下記のような情報が出力される。(図６)

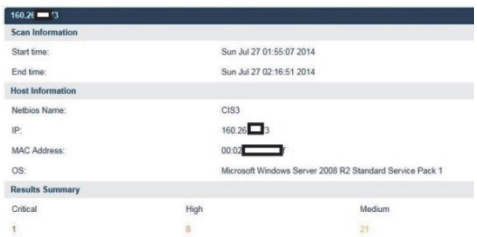

図６　　セキュリティ調査　結果

IP 毎に OS 等の情報が判断され、その PC における脆弱性数が表示される。その上で、その PC における脆弱性情報が、Port 毎に次のようにまとめて表示される。（図 7）

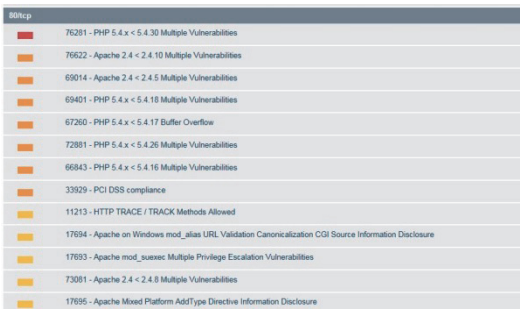

図 7　Port 毎 セキュリティ調査の結果

脆弱性は、その危険度から Critical,High,Medius 等に分類される。

今回の調査では、学内キャンパスに接続している機器に対して調査を行った。事務系のネットワークに関しては別途行うこととした。

調査の結果は、100 件程度の Critical（致命的）が判明し、High(リスクが高い)と判断されるものは、2000 件を超えた。

脆弱性に対応するためには、これらの結果をユーザに通知する必要があるが、Nessus では、これらの脆弱性に対して、

Synopsis :The remote host is running an obsolete operating system.

Description :According to its version, the remote Unix operating system is obsolete and is no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution :Upgrade to a newer version.

Risk factor :Critical / CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

などの対応情報が示される。しかし、この英語情報をそのままユーザに通知しても、ユーザが理解できない場合も多いと考えられた。そこで、今回は、

・high の数がとても多い
・一台のマシンに複数の脆弱性
・Critical のマシンに多くの脆弱性が指摘

ということがデータにより判明したため、Critical（致命的）と判断される機器を中心に対策を進めることとした。

実際の対応は、Critical と判断された機器に対しては、次のような情報を提供することとした。名称や概要などの表題、対策方法に関しては日本語化を行った。（図 8）

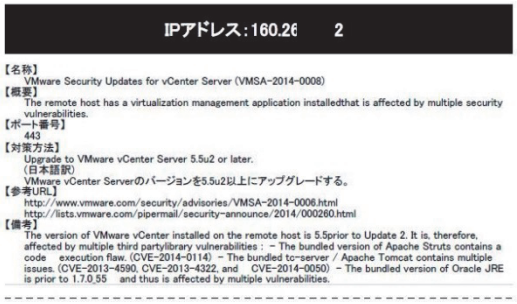

図 8　学内通知　情報の例

5．今後の課題

総合情報基盤センターでは、FW 等のセキュリティ機器を運用するだけでなく、セキュリティ情報を外部の機関や Web 等により収集し対応することを行っている。今後、さらに、これらの機能を充実することが必要だと考えられる。

加えて、外部からの攻撃を監視するシステムを構築することにより、被害を最小化するための研究を行っている。また、セキュリティ調査の研修などを行い、セキュリティ能力の強化を行う必要がある。

しかし、現実にセキュリティを維持するためには、各機器の管理者の意識が重要になる。今後、定期的にこれらの調査を継続するとともに、ユーザへの情報提供や教育の拡充をすることが必要だと考えられる。

謝辞

今回のセキュリティ調査に関して、技術指導を頂いた株式会社アズジェント様に深謝いたします。また、ユーザへの通知に関し、データ整理や日本語化を行った金森浩治技術職員に感謝します。