PortScan 調査からのセキュリティ状況

総合情報基盤センター　沖野　浩二

サイバー攻撃が現実的な問題として認識されています。実際に、本学でもサイバー攻撃を受け、被害が発生しています。サイバー攻撃の被害を未然に防ぐまたは軽減するために、本学では学内向けセキュリティ調査を定期的に行っています。

本稿では、サイバー攻撃の背景の述べたうえで、調査の概要と結果について説明します。最後に、サイバー攻撃に対策するために必要なことを述べたいと思います。

1.　攻撃の現状

2017 年から WannaCry とその派生型などのネットワークで拡散する Ransomware（感染したコンピュータの利用やデータへのアクセスを制限し、この制限を解除するためには、身代金(Ransom)を支払せようとするマルウェア）が猛威を振っています。WannaCry は、セキュリティにコストをかけているはずの大企業やインフラ企業などにも感染し、サイバー攻撃の危険性に対し、身を持って感じる機会となりました。

さらに、近年の攻撃は、PC やサーバだけを対象にしたものだけではなく、ネットワークに接続された IoT（Internet of Things）と呼ばれるセンサーや建物管理システムなどにもその対象が広がっていいます。

これらの攻撃の中には、国家またはテロ集団などが行っているサイバー攻撃も含まれていると言われおり、これらの攻撃に対処することが世界的に求められています。

IoT 機器への攻撃が増加している理由は、

- ネットワークに接続されている機器の絶対数が多くなっていること
- PC やサーバに比べて、セキュリティ対策が行われていない場合が多いこと
- 長期間稼働しており、いつでも利用可能であること

などが挙げられます。さらに、攻撃が成功し、乗っ取られた IoT 機器は、他の機器への感染を広げようと次の攻撃を始めます。

広げる攻撃は、同種の攻撃の場合もあれば、他の機種（例えば、Mirai など）への攻撃の場合もあります。

現在の攻撃が増えている背景は、これら乗っ取られている IoT 機器からの攻撃が増えていることも一つの要因となっています。

2.　本学への攻撃の実例

サイバー攻撃は本学に対しても発生しており、実際の IoT 機器への攻撃例として、2013 年に、外部からのプリンタを不正に利用される事例が発生しました。この事例は、学外からプリンタに不正に操作され、ANONYMOUS のロゴ（図 1 ）が大量に出力されたものです。

この攻撃を受け、早急に Firewall の設定見直しを行いましたが、今後の攻撃レベルが向上することを考えると、学内設置機器全体に対する継続的な更なる対策を行う必要があることは明白でした。

図 1　出力された画像

3.　PortScan 調査

　更なる対策として検討されたものの一つが、学内の機器に対するセキュリティに対する実態調査を行うものでした。実態を調査する方法として、学内機器に対して PortScan と呼ばれる手法を適用しました。PortScan は実態に機器と通信を行い、機器の情報や脆弱性等を検出する手法です。この手法は、実際のサイバー攻撃でも利用されているものであり、攻撃者側と同様のこの調査を通じ、

- 学内の脆弱性がある機器の実態把握

を目的とし、その調査結果を受け、

- 脆弱な状態であることを機器管理者への通知

を行うことで学内のセキュリティレベルの向上を求めました。

　実際に行った PortScan 手法は、以下の通りです。

利用 Scanner

Tenable 社製　Nessus Professional 版

適応ルール

基本 PCIDSS を利用し、一部部分カスタム

適応ポート　All　Port

4.　調査結果

　本 PortScan は、2014 年から継続して実施されており、Nessus により検出された脆弱性の数は図 2 の通りです。

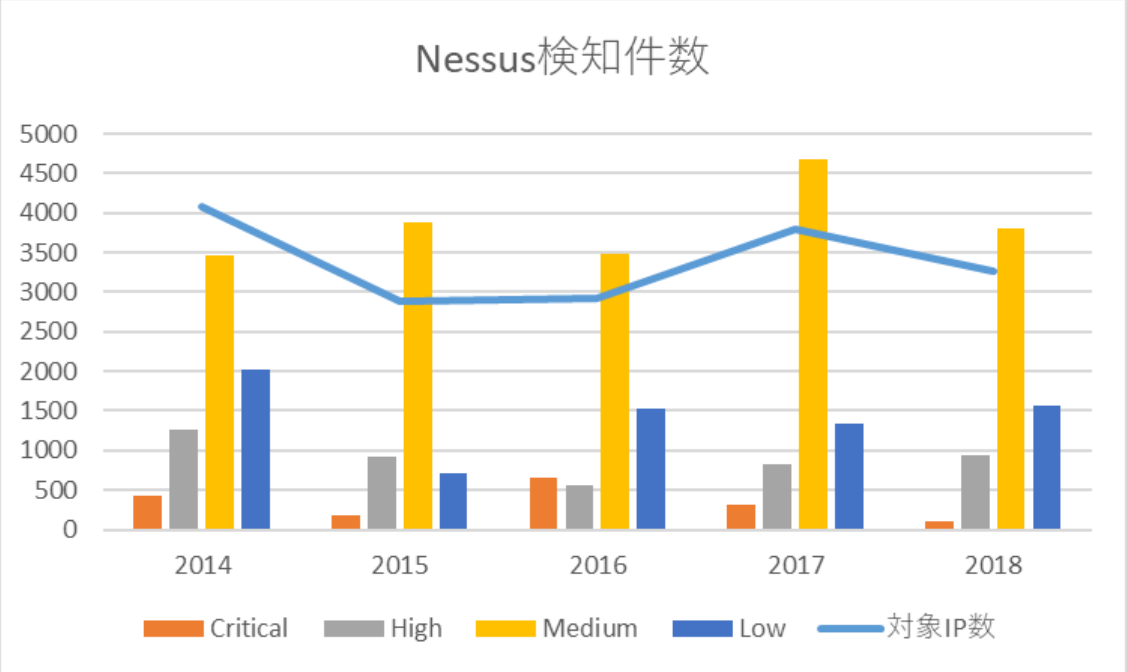


図 2　Nessus 検知件数

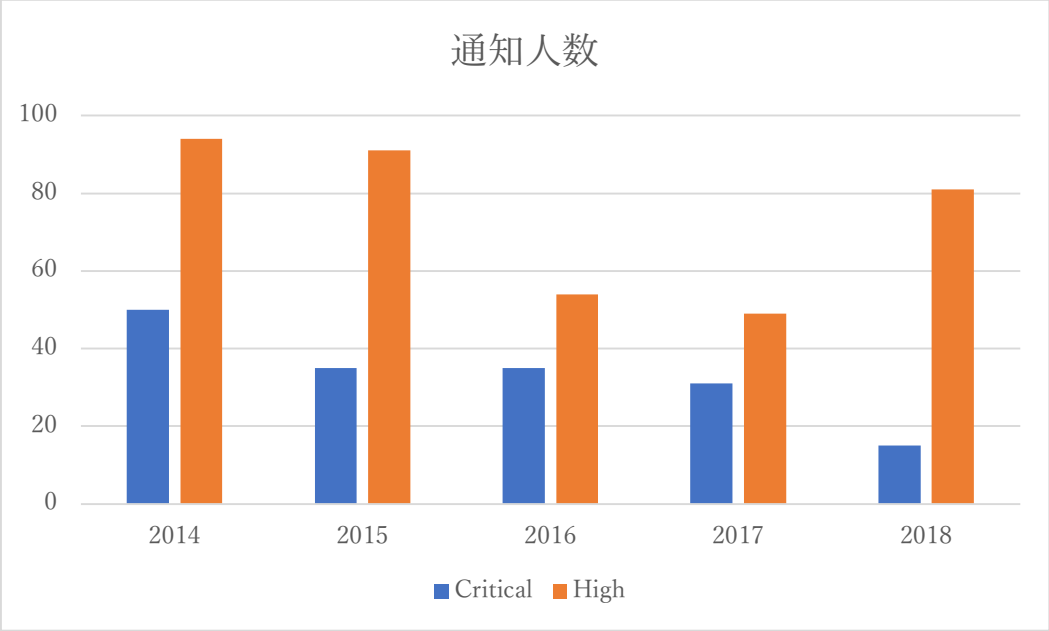


図 3　通知人数

PortScan を行うと、IP 毎に OS 等の情報が判断され、その IP を利用している機器の脆弱性（攻撃に利用できるセキュリティ上問題個所）を調べることができます。脆弱性は、その危険度から Critical,High,Medius, Low に分類されます。特に Critical と判断されるものは、攻撃が容易であり、早急な対策が必要と判断されるものです。

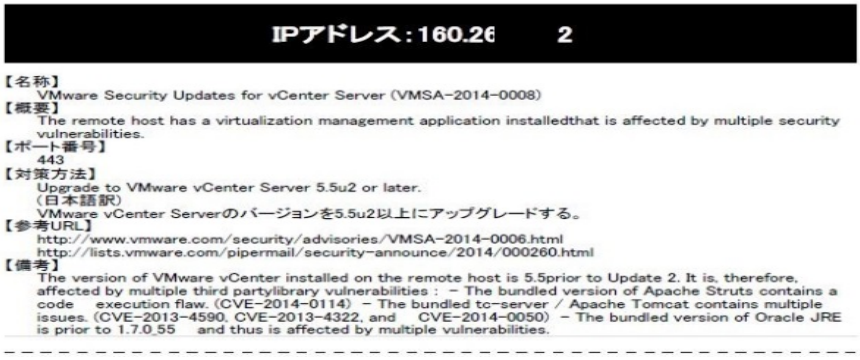
PortScan により検知される対象 IP 数は、3500 台前後となっています。調査年により、その検出台数が大きく変化しているのは、PortScan が行われる時間帯によりその稼働している機器の台数が大きく変化しているからです。また、当初 2014 年の台数が 4000 台を超えているのは、調査対象に無線 LAN の空間を加えていました。2015 年調査からは、機器の入れ替わりが多いため対象から除外しています。

調査結果から、学内には脆弱性を有している機器が一定数存在していることが判明しています。調査結果からは、脆弱性の内、特に危険度が高い Critical の数は減少しており、また、他の危険度も大きな変化は発生していないことがわかります。

脆弱性は、毎日新しく発見されており、学内で検出される数が変化していないのは、ある程度適切にセキュリティ対策が行われている状態であると考えられます。

また、2018 年の調査では、一部の IP アドレスに対して、デフォルトの ID/Password でのアクセス検査も行いました。この調査の結果、学内からのアクセスではありますが、建物管理システムや複合機に保管されている出勤表などのデータを取得できることが確認できました。

PortScan の結果を受けて、Critical のすべてと High の一部の脆弱性が検出されたものに加えて、上記のデータ閲覧に関しては、CIO から、脆弱性に対する通知(図 4)を行いました。


IPアドレス：160.26　　2

【名称】
VMware Security Updates for vCenter Server (VMSA-2014-0008)
【概要】
The remote host has a virtualization management application installedthat is affected by multiple security vulnerabilities.
【ポート番号】
443
【対策方法】
Upgrade to VMware vCenter Server 5.5u2 or later.
（日本語訳）
VMware vCenter Serverのバージョンを5.5u2以上にアップグレードする。
【参考URL】
http://www.vmware.com/security/advisories/VMSA-2014-0006.html
http://lists.vmware.com/pipermail/security-announce/2014/000260.html
【備考】
The version of VMware vCenter installed on the remote host is 5.5prior to Update 2. It is, therefore, affected by multiple third partylibrary vulnerabilities : - The bundled version of Apache Struts contains a code execution flaw. (CVE-2014-0114) - The bundled to-server / Apache Tomcat contains multiple issues. (CVE-2013-4590, CVE-2013-4322, and CVE-2014-0050) - The bundled version of Oracle JRE is prior to 1.7.0_55 and thus is affected by multiple vulnerabilities.

図４　学内通知　情報の例

脆弱性の検知は一台の機器から複数検出されることがあるため、また、一人の機器管理者が複数の機器を管理しているため、実際にこの通知を受け取る方の人数を図３に示しています。この結果から毎年１００名程度の方がこの通知を受け取っておられます。ただ、この結果からも分かるように特に注意が必要な Critical の通知人数は、毎年減少しており、学内での通知が有効に効いているとも判断できます。

5.　サイバー攻撃への対策

学内の方には、脆弱性の学内通知を受けたられた方がおられると思います。学内通知には、対策方法が書かれていますので、必ず対応をお願いいたします。また、中には、昨年と同様な通知が届いている方もおられます。通知を受け取り、機器のファームウェアが長期に渡り更新されていない場合は、その機器の EoL（End of Life:機器のメンテナンス上の寿命）を迎えている可能性が高いものです。これらの機器は計画的な更新をお願いいたします。

一般的に、セキュリティに対する対策としては、

- OS やファームウェアは最新に UPDATE を行う
- アプリケーションも最新版を利用する
- Password はデフォルトを必ず変更したうえで利用する

を必ず行うようにしてください。

そのほかにも、OS 関係としては、2020 年に迎える Windows7 の EoL の対策とともに、Mac を利用するユーザに関しては必ず最新（10.14 Mojave）または一つ前の Version（10.13 High Sierra）を利用するようにしてください。

また、無線機器に関してですが、ここ数年で効率的な攻撃方法が多数発表されています。無線の設定に関しては、WPA2 以降の規格を利用するとともに、古い機器は利用しないことをお願いします。

さらに、古い NAS に関し、セキュリティ対策として最新の Windows10 からアクセスできないものがあります。最新の Windows10 からアクセスできないような NAS は、セキュリティの問題を含んだ製品であるため、新しい機器への更新をお願いいたします。