Vol.2015-IOT-31 No.7
Vol.2015-SPT-15 No.7
2015/9/25

nmapを利用した学外からの学内ネットワーク監視と対策

杉谷 賢一[1,a)]　中野 裕司[1,b)]　武藏 泰雄[1,c)]　辻 一隆[1,d)]　島本 勝[1,e)]　木田 健[1,f)]

概要：熊本大学では，学内の承認を受けた上で，学内ネットワークの一部のポートに関して外部ネットワークから nmap による日々の監査を行っている．監査結果のデータベースへの保存とメールによるアラートを行い，その結果に基づき，外部から見えるプリンター等への対策を行ってきた．
本稿では，本学で行った外部ネットワークから見えるプリターへの対応の方法等について報告する．

キーワード：nmap，ネットワークプリンター，インターネット，情報漏えい

The campus network monitoring from off-campus using nmap

Abstract: In Kumamoto University, we have been performing the campus-approved daily network monitoring of specific service ports in the campus network from the Internet, employing the nmap scanner tool. Based on the monitoring results stored in a database and e-mailed as alerts, we have been taking measures against the campus networked printers which are accessible from the Internet. In this paper, we report the corresponding methods for the Internet-globally-accessible networked printers in the campus.

Keywords: nmap, networked printer, Internet, Information leakage

1. はじめに

近年，Web サーバーの機能をはじめとするネットワークサーバー機能を搭載したオフィス機器が増えている．そのため，それらの機器をネットワークへ接続する際には，インターネットと当該機器との不要な通信を遮断するなど，セキュリティを考慮した安全な接続が求められている．

そのような状況の中，研究室や事務室等に設置されているネットワークに接続されたプリンターや複合機（以下では「複合機等」と呼ぶ）が，学外から不正にアクセスされ，当該機器に残っていたデータが盗み出されるというセキュリティ事故が多発している [1], [2], [3].

これらの事故の多くは，機器の管理者が当該機器にそのような脅威が及ぶ可能性があるという意識がなく，単にネットワークに接続して利用できれば良い，ということから発生しているものと考えられる．

一方，ネットワークに接続して使用する機器は，一般的に，利用者の利便性を考えて，できるだけ簡単にネットワークに接続できるよう，設定項目を最低限にしてあるものが多い．また，一旦ネットワークに接続したら，その後の運用・管理は手持ちの PC からできるように，Web サーバー機能を有していることが多く，その機能がデフォルトで有効になっているのがほとんどである．機器メーカーが利用者のためにと考えて整備したこれらのことが，ネットワークに関する知識の少ないユーザに，セキュリティ事故を起こさせやすい原因となってしまっている．

これらの問題を解決するには，ネットワークに接続する機器は，組織の管理部門で一括管理するか，それができないときは，各機器の管理者（大学の場合，当該機器を購入した教員等）の意識改革に頼るか，問題のある機器の管理者に直接連絡して設定変更をしてもらうことになる．

本稿では，本学で行なっている上記の対策ならびに現状について報告する．

[1] 熊本大学
Kumamoto University, Kurokami, chuou-ku, Kumamoto 860–8555, Japan
[a)] sugitani@cc.kumamoto-u.ac.jp
[b)] nakano@cc.kumamoto-u.ac.jp
[c)] musashi@cc.kumamoto-u.ac.jp
[d)] kazu@kumamoto-u.ac.jp
[e)] masaru@kumamoto-u.ac.jp
[f)] tkida@kumamoto-u.ac.jp

2. 本学のネットワーク運用に関する諸問題

2.1 グローバル IP によるネットワーク運用による問題

本学は，歴史的な経緯によりクラス B の IP アドレスを運用しており，SINET[4] との間に FierWall を設けている現在も，学内のネットワーク機器の多くはグローバル IP を設定している．

そのため，インターネットからの攻撃が，各ネットワーク機器に及ぶという問題が常にあり，本稿で主な対象となるネットワーク・プリンターや複合機がその標的となってしまうことになる．

ただ，近年，IP アドレスの不足の対策として，また外部からの攻撃防御のために，研究室内のネットワークは，ブロードバンドルーターによって構成することを推奨している．これにより，複合機等も攻撃対象と成ることが少なくなってきている．

ところが，研究室以外のネットワークから印刷したいとか，全学無線 LAN に接続した機器から印刷したいという理由から，安易にグローバル IP を振ることが多いようで，このような機器の設定はアクセス制限などは考慮されていないのがほとんどである．

2.2 ネットワーク機器管理の部局委譲による問題

本学では教育研究用情報ネットワークの運用方針として，幹線ネットワークは総合情報統括センターが管理し，支線ネットーワークは IP アドレスの管理も含めて各部局で行うということにしている．そのため，各教員が購入しネットワークに接続する機器の情報は，部局で把握・管理することになっている．これにより，総合情報統括センターの管理業務は大幅に少くなっているが，一方では管理を部局の担当者にお願いしているため，その担当者に大きな負担をかけてしまうことになり，場合によっては各機器の管理者へのサポートが適切にできないこともある．このような状況のため，機器毎に設定方法が異るネットワーク機器の細かな設定について，全学的な統一を図ることは，なかなか難しい状態にある．

2.3 複合機等のネットワーク設定に関する問題

複合機等は，PC と異なり機能が限定されている．そのため購入して設置する際に設定する項目としては，IP アドレス，ネットマスク，デフォルトゲートウェイ程度であり，それで利用する PC から印刷できれば，その時点で設定完了となることが多い．特に，当該機器の LCD パネルを見ながらの設定となると，操作性が悪いため，早く設定作業から逃れたいと思うのが当然であるので，最小限の設定しかされないというのが普通になってしまう．

一方，最近の複合機等は，印刷機能が豊富にあるだけでなく，Web サーバー機能をはじめとするインターネットサーバー機能をたくさん持つものが多い．機能が多いのは利便性が上がり良いかもしれないが，意図して設定変更しないと，すべてのサーバー機能が有効になっていることは問題であると思われる．ネットワーク的な知識のない一般ユーザにとって，これらの機能は不要であることが多いにもかかわらず動作しているということは，単にセキュリティレベルを下げるための機能と言えなくもない．

以上のような状況にあるので，本学のようにグローバル IP でネットワークを運用している組織では，複合機等に不正にアクセスするというのは，簡単なことであることが多い．その被害にあわないようにするためには，複合機等を設置する際に，接続するネットワークの選択や複合機等のネットワーク周りの設定に，十分な注意を払う必要がある．

3. 対策の方法

本学が行った対策の概略は，次のような方法である．

(1) 学外ネットワークに接続した監査サーバーにより定期的に学内の複合機等がアクセスできるか調査し，その結果をデータベースに登録
(2) 登録された情報から新規に発見した複合機等の IP アドレスの一覧を総合情報統括センターの管理者にメールする
(3) 学外から見えている複合機等の IP アドレスの管理部局の担当者に連絡して対応を依頼
(4) 対応済みの報告により当該 IP を再度チェック
(5) 解決できていればその IP については終了．解決できていないときは再度対応を依頼．

上記の手順の詳細について以下に述べます．

3.1 監査サーバー

意図せず学外に公開されている複合機等を調査する監査サーバーは，**図 1** のように，学内に設置しているものの，SINET ではなく商用の ISP のネットワークに接続して利用している．

このサーバは，2007 年ごろ本学の公式 Web ページの動作チェックのために設けたものであり，当初は本学のトップページが学外から見えているか，（不正な）書き換えが行われていないかのチェックをさせていた．

その後，Web サーバの安定運用が確認できてきたので，意図しないサービスが学外に公開されていないかをチェックすることを考え，当センターの限られたネットワークセグメントに対して，いくつかのポートへの接続具合を調べることにした．

その時，利用したのがセキュリティスキャナーの一つである nmap[5] である．nmap は，ポートスキャンだけでなく，OS やサービスまで検出する機能もついている高機能なものである．

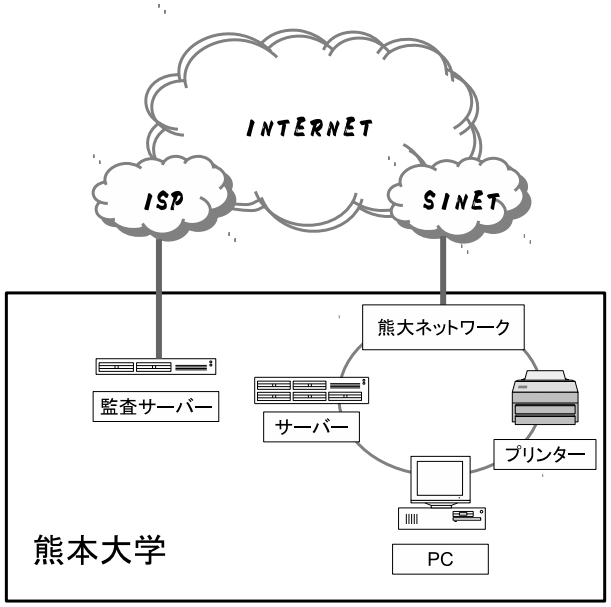

図 1　監査サーバーのネットワーク
Fig. 1　Network of scanning server

cron で，毎日一回，当センターの職員の PC が接続されいる IP アドレスのレンジを指定すると同時に，辞書攻撃が盛んに行われる 22 番ポートに対して，チェック（スキャン）を行った．行った結果は，整形して DB に登録するようなプログラムを作成し，cron での処理の中に組み込んだ．

そのデータは，時々調べて，ポートが開いている IP アドレスがあれば，意図した設定なのかを，当該 IP の管理者である当センターの教職員に問い合わせるというチェックを行った．

その後，監査の対象範囲を全学に広げることを検討し，2013 年に全学の委員会で承認を受け，毎日全学の IP に対して監査を行うことにした．その際，22 番ポートだけでなく，よく利用されかつ攻撃対象になりそうなポートについてもアクセスの可否を調べることにした．ターゲットとしたのは，23，25，80，443，1720，8080，8443，10000 と 22 番を併せた 9 つのポートである．

3.2　学外から見えている複合機等の判別とその対応

監査データは日々蓄えられていく中，複合機等が外部からの攻撃で一時保存されていたデータが盗まれるという事象が，ニュース等で報じられるようなった．そのため，監査データを蓄えた DB から，外部からアクセスできる機器の中で複合機等と推測される機器を抜き出す処理を追加した．そして，複合機等と推測される機器が新たに見つかった場合，その IP を当センターの管理者にメールで通知するようにした．

通知を受けた管理者は，当該 IP の利用者に設定変更をしてもらうよう，通知を受けた IP を確認して，当該サブネットの管理者にメールで連絡するようにした．設定変更の依頼内容としては，当該機器へアクセスを許可するネットワークをできる限り狭い範囲に限定するようにすることである．いろいろなところから利用する場合，最低でも学内限定にすることを依頼している．

4.　監査状況

これまで蓄えた監査データについて，いくつかの切り口から整理したのでその結果を以下に示す．

まず，全学に対して監査をかけた期間で，学外から見えているホスト数の経時変化を図 **2** に示す．

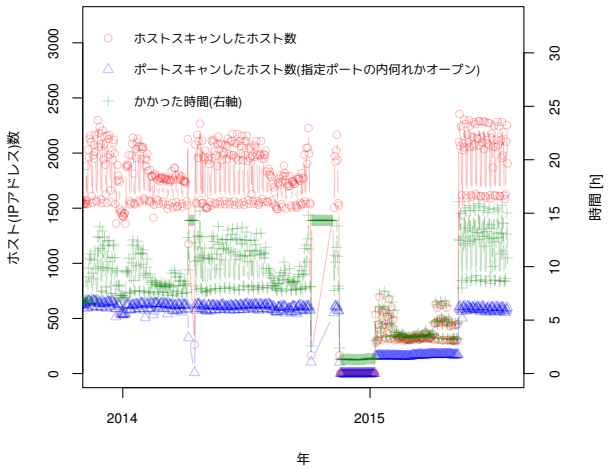

図 2　学外から見えているホスト数
Fig. 2　Number of scanned hosts

2014 年の 11 月頃から 2015 年の 3 月くらいまでの期間は，全く違う傾向になっているが，これはシステムトラブルのためにデータがうまく取得されていないことに起因するもであるので，この部分は無視してほしい．

ホスト数が時期により減少しているのは，春・夏・冬の各休みの影響によるものと考えられる．監査に要した時間もこの影響を受けて，同様の傾向にある．ただ，監査対象とした 9 つのポートのどれかが開いている機器の数は，季節に関係なくほぼ一定である．これは，学外からアクセスできるサーバー機や複合機等の総数を表しているものと考えられる．

次に，監査対象としたポート別に，開いているホストの数の経時変化を図 **3** に示す．予想されるとおり開いているポートとして 80 番ポートが一番多いことがわかるが，もちろん，これには学外に公開している Web サーバが含まている．ただ，少しずつではあるが，80 番ポートが開いているホスト数が減少していることがわかる．また，この影響で，学外からアクセスできるホスト数の総数も減少していることがわかる．

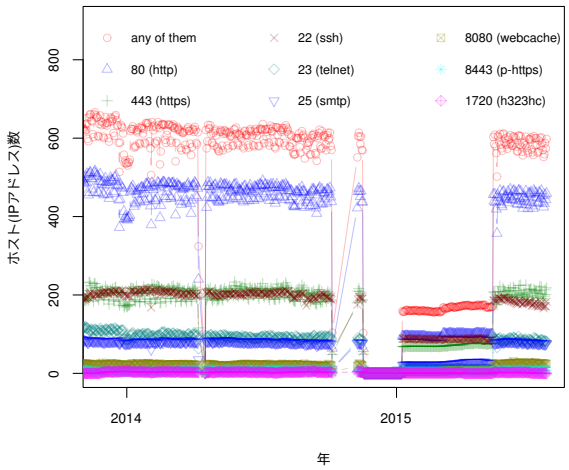

図 3　開いているポート別のホスト数
Fig. 3　Number of hosts by type of opened port

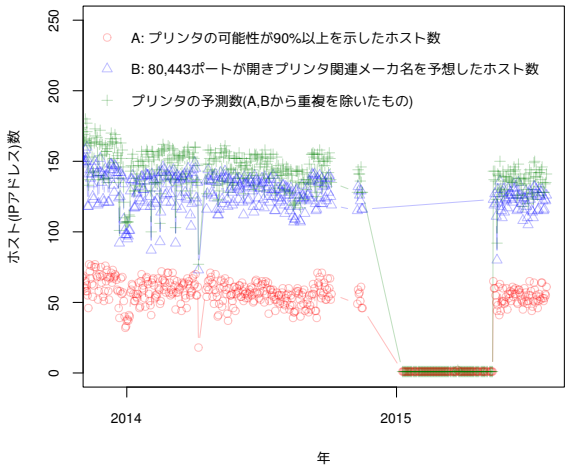

図 4　複合機等と推測されるホスト数
Fig. 4　Number of hosts that are supposed to be printers

続いて，複合機等と推測されるホスト数の経時変化を図 4 に示す．これまでの図と同様に，2014 年の最後から 2015 年の 3 月までのデータは無視していただきたい．nmap がプリンターと判断した台数が，わずかながら減少していることがわかる．また，nmap がプリンターとは判断していないが，nmap が出力したデータ中に，プリンター関連メーカー名が含まれたものも同図で表示させているが，nmap がプリンターと判断したものの倍程度あることから，それなりに多くの複合機等が学外からアクセスできる状態にあることが推測される．

最後に，複合機等と推測されるホスト数の今年の 5 月から 7 月までの様子を図 5 に示す．日々の数が上下するのは，複合機等の電源を必要があるときだけ ON にするような運用をされている機器があるのが原因だと思われる．この 3 月間は，ほぼ一定のホスト数のようにも見えるが，7 月にはわずかに増加しているようにも思われる．

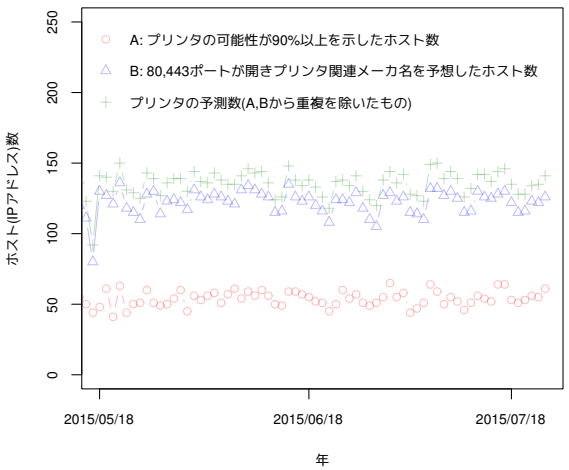

図 5　複合機と推測されるホスト数の近況
Fig. 5　Recent number of hosts that are supposed to be printers

5. おわりに

本稿では，本学で実施した学外から見えている複合機等を検出し，当該機器の管理者に連絡して見えなくなるよう対応してもらうプロセスと現状の報告を行った．

1990 年代の前半からインターネットに接続している大学としては，できる限り自由にネットワーク環境を利用できるよう，今後もグローバル IP での運用を続けていきたいと考えている．だが，ネットワークに接続した機器の振る舞いには興味はなく，単にネットワークを利用出来れば良い，というユーザが増えていく現状を考えると，中長期的にはプライベート IP 化も，一つの選択肢として考えながら，新しい学内ネットワーク運用方法を考え直す時期に来ているのかもしれない．

参考文献

[1] 日本経済新聞: 狙われるオフィスの複合機　対策放置が招く情報漏えい，入手先 ⟨http://www.nikkei.com/article/DGXNASFK1302W_T11C13A1000000/⟩ (2015,08,13).
[2] IPA: 複合機やウェブカメラ，情報家電なども適切なアクセス制限を，入手先 ⟨http://www.ipa.go.jp/security/announce/20150317-netdevice.html⟩ (2015,03,17).
[3] IPA: IPA テクニカルウォッチ　「増加するインターネット接続機器の不適切な情報公開とその対策」の公開，入手先 ⟨http://www.ipa.go.jp/about/technicalwatch/20140227.html⟩ (2014,02,27).
[4] SINET: 学術情報ネットワーク, http://www.sinet.ad.jp/.
[5] nmap: Nmap Security Scanner, https://nmap.org/.