一般口演
# 一般口演4
# 情報セキュリティとプライバシー・ネットワーク
2018年11月23日(金) 10:15 ～ 11:45 H会場 (福岡サンパレスHパレスホール)

[2-H-1-1] 医療機関の情報ネットワークに対する外部からの不正アクセスに関する解析

○松永 敏明[1], 矢野 弘章[1], 山下 龍士[1], 難波 孝宏[1], 森 龍太郎[2], 紀ノ定 保臣[2] （1.岐阜大学医学部附属病院　経営企画課医療情報係, 2.岐阜大学医学部附属病院　医療情報部）

【背景・目的】　これまでの医療情報システムは外部と隔離した状態で稼働していたが，現在では地域医療連携，遠隔医療，研究推進等のため，インターネットを通じて外部機関と院内のシステムを接続することが増えてきた。それに伴い，病院が保有する情報の窃取等を試みる外部からの不正アクセスが増加している。このため医療情報システムの高い安全性を今後も確保するためには，外部から不正アクセスを試みている通信を把握し，状況に応じた対処を行うことが重要である。本稿では院内ネットワークと院外ネットワークの境界線に設置したUTMで，遮断した外部からの不正アクセス通信ログを解析し，医療機関に対する不正アクセスの傾向について解析した。　【解析方法】　UTMから取得した，2017年4月から2018年3月の間のログ情報（約70万件）より，月別，発信元IPの国別，通信ポートごとに不正アクセスを試みた数の推移やその傾向等について解析した。　【結果・考察】月別：不正アクセス数は1年間同じように推移していた。しかし，2月には他の月の1.6倍の不正アクセス数があった。その要因は，2月14日にブルガリアからポートスキャンと思われる不正アクセスであった。発信元IPの国別：中国，アメリカ，オランダ，ブルガリア，ブラジルが発信元の上位国であった。オランダは11月から月を重ねるごとに増加していた。通信ポート：他を圧倒する件数で23番ポートへの不正アクセスを試みがあった。次いで22番，1433番，53413番，80番が多かった。不正アクセスの定番と言われる通信ポートに加え，ルータの脆弱性やWannaCry等のマルウェアに関する通信ポートが多く見受けられた。対策：脆弱性を狙った不正アクセスは継続的に行われていた。安定稼働が重要視される医療情報システムの中でセキュリティパッチを適用することはリスクを伴うが，不正アクセスによる被害のリスクが大きいため積極的に適用したい。

医療機関の情報ネットワークに対する外部からの不正アクセスに関する解析

松永　敏明[*1]、矢野　弘章[*1]、山下　龍士[*1]、難波　孝宏[*1]、
森　龍太郎[*2]、紀ノ定　保臣[*2]
*1 岐阜大学医学部附属病院　経営企画課、*2 岐阜大学医学部附属病院　医療情報部

An analysis of the unauthorized outside access of an information network at a medical institution

Toshiaki Matsunaga[*1], Hiroaki Yano[*1], Ryushi Yamashita[*1], Takahiro Nanba[*1],
Ryutaro Mori[*2], Yasutoshi Kinosada[*2]
*1 Management Planning Division, Gifu University Hospital,
*2 Division of Medical Information, Gifu University Hospital

Abstract.
Historically, medical information systems have operated in isolation from external networks, such as the Internet, however, in recent years, such systems have become increasingly connected via external networks for the purpose of regional medical cooperation and research. Accordingly, instances of illegal external access for the purpose of obtaining highly confidential information held by hospitals, such as patient information, are increasing.
In order to prevent unauthorized external access, it is important to understand the attack methods and trends. For this reason, in this paper, we analyzed the methods and trends in attempts made to illegally access an external publishing server operated by Gifu University Hospital.

Keywords: Computer Security, Data Interpretation, Access to Information.

1. 緒論・目的

これまでの医療情報システムはインターネット等の外部ネットワークとは隔離した状態で稼働していたが、近年では地域医療連携や研究等の目的で、外部ネットワークと繋がることが増えてきた。それに伴い、患者情報等の病院が保持する機密性の高い情報を狙う等の外部ネットワークからの不正アクセスが増加している。

外部ネットワークからの不正アクセスを防止するには、攻撃方法や傾向を把握することが重要である。このため、本稿では、外部ネットワークから岐阜大学医学部附属病院（以下、本院と言う。）で運用している外部公開用サーバに対して行われた不正アクセスの試みについて、その攻撃方法や傾向について解析を行った。

2. 方法

本院では、インターネットと院内ネットワークとの境界にUTM（統合脅威管理）装置を設置している。このUTM装置で自動取得している通信ログ情報（2017 年 1 月から 2018 年 8 月までの間）を用い、外部公開用サーバに対する不正アクセスの傾向について時間、不正アクセス発信元 IP アドレスの国、通信ポートについて解析を行った。

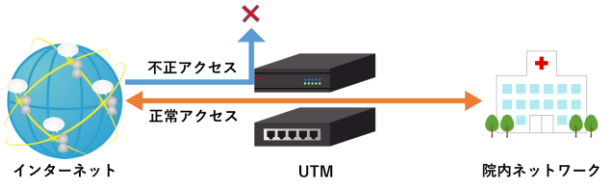

図1　UTM 装置のイメージ

3. 結果・考察

3. 1 時間別傾向解析

月別不正アクセスの傾向を図2に示す。月により増減のばらつきはあるが、近似曲線が示すように、不正アクセスは全体的に増加の傾向があると言える。

また、2018 年 2 月には前月の約 1.7 倍の不正アクセスの件数が確認された。詳細を確認したところ、2 月 14 日にブルガリアから 34556 個のポートに対する不正アクセスがあった。多くのポートに各 1 回ずつの不正アクセスを試みていることから、外部公開用サーバの脆弱性を探索するためにポートスキャンが行われたと考えられる。

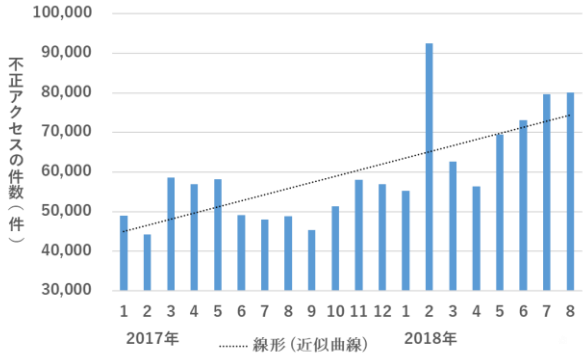

図2　月別不正アクセスの傾向

次に、曜日別不正アクセスの傾向を図3に示す。1 日で他日の数十倍の不正アクセスのあった 2018 年 2 月 14 日は除いている。木曜日と日曜日が若干増加しているが、特定の曜日に不正アクセスが増加するような傾向はみられなかった。これは、近年の不正アクセスは、自動化されたプログラムによって行われることが多いため、不正アクセスの件数が平滑化されたものであると考えられる。

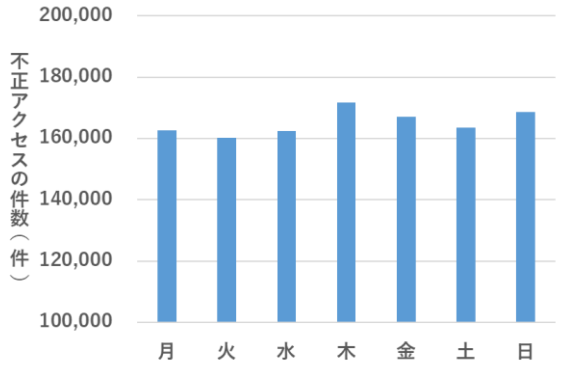

図3 曜日別不正アクセスの傾向

時間帯別不正アクセスの傾向については図4に示すとおり、日中帯の方が夜間帯より不正アクセスの件数が多い傾向がある。これは通常のアクセスに紛れるため、システムや機器を利用している時間帯を狙ったものではないかと推測される。

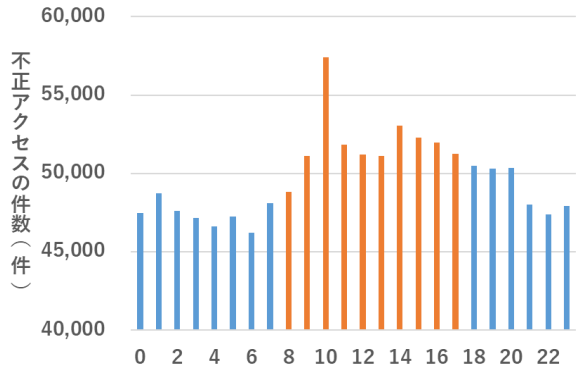

図4 時間帯別不正アクセスの傾向

3.2 発信元 IP アドレスの国別傾向

不正アクセスを試みた発信元の IP アドレスを国別に分けたものを図5に示す。不正アクセスの発信元は、中国とアメリカとオランダが大半を占めていた。

JPCERT/CC のインターネット定点観測レポート[1]でも、不正な通信の送信元地域トップ 5 がアメリカ、中国、ロシア、チリ、オランダとなっており、医療機関においても社会一般と同様に不正アクセスの脅威が存在していると言える。

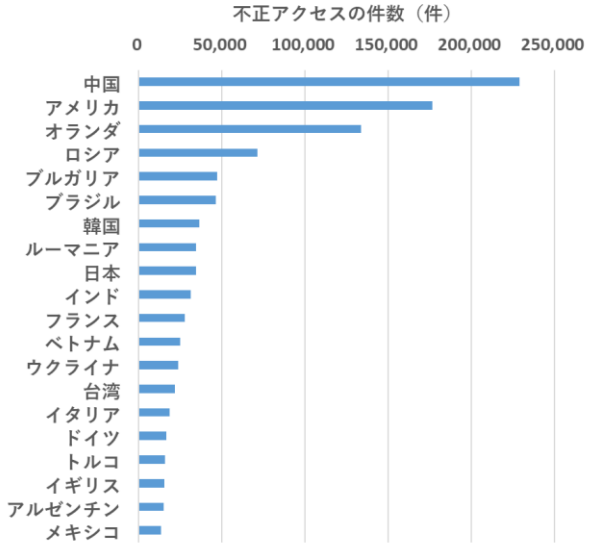

図5 国別の不正アクセスの傾向

また、不正アクセスの件数が多い上位 5 ヶ国の月別不正アクセスの傾向を図6に示す。中国、アメリカは月により増減はあるが、一定件数の不正アクセスを試みていた。一方で、オランダでは 2017 年 11 月より、ロシアでは 2018 年 5 月より不正アクセスの試みが急増していた。

先述のとおり、ブルガリアについては、2018 年 2 月 14 日に大量の不正アクセスの試みが行われた結果がグラフに現れている。

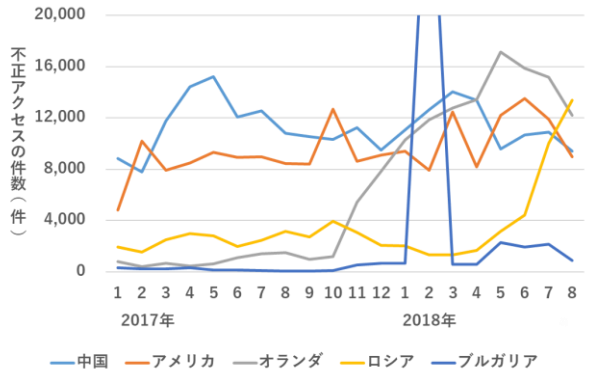

図6 上位 5 ヶ国の月別不正アクセスの傾向

3.3 通信ポート別傾向

通信ポートは、サーバ上で稼働する複数のサービスを区別するために割り当てられた識別子で、主要なサービスの通信ポート番号は予め決まっている。(例:HTTPS なら 443 番ポート、SSH なら 22 番ポート等)このため、不正アクセスが行われた通信ポートを解析することで、サーバ上のどのサービスが狙われた、または、狙われる傾向を知ることができる。

今回、ログ情報を解析した結果、攻撃対象となったポート別不正アクセスの傾向を図7に示すとおり、不正アクセスの件数は他を圧倒する数で 23 番ポートへのアクセスが確認できた。23 番ポートはサーバやネットワーク機器をコマンドラインにより遠隔制御できる Telnet で用いられるポートであり、ブルートフォースアタック(パスワードの総当たりによる攻撃)などにより攻撃者に乗っ取られ、さらなる攻撃の踏み台として悪用さ

れる可能性がある。このため、@police の IoT 機器を標的とした攻撃の観測について[2]やJPCERT/CC のインターネットに接続された機器の管理に関する注意喚起[3]でも広く注意を呼びかけられている。

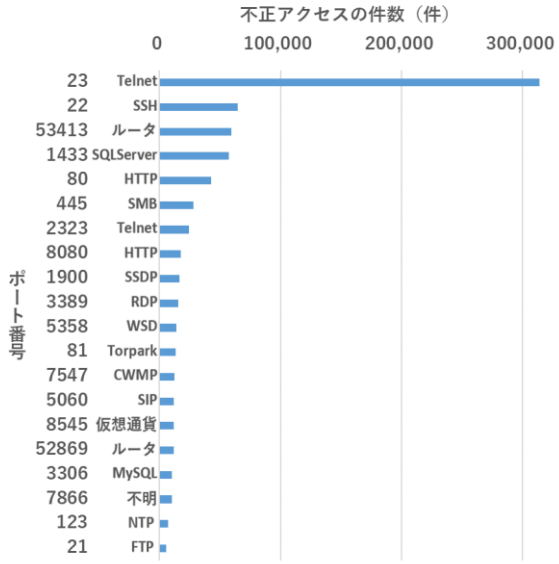

図7　ポート別不正アクセスの傾向

また、53413 番ポートでも多くの不正アクセスが確認できた。53413 番ポートは中国の Netcore（中国国内）/Netis（中国国外）社製ルータで利用され、このルータの脆弱性を利用すると、ルータをほぼ完全に制御される可能性がある。こちらについても、JPCERT/CC のインターネット定点観測レポート(2015 年 4～6 月)[4]やトレンドマイクロセキュリティブログの UDP ポートを開放した状態にする Netis 製ルータに存在する不具合を確認[5]でも広く注意を呼びかけられている。

その他 JPCERT/CC のインターネット定点観測レポート[1]でも、宛先ポート番号トップ 5 が 23 番、445 番、80 番、22 番、1433 番となっており、発信元 IP アドレスの国別と同様に医療機関においても社会一般と同様に不正アクセスの脅威が存在していると言える。

3.4 特定国の不正アクセスの多い上位 5 ポートの月別傾向

オランダを発信元とした不正な通信に関し、不正アクセスの多い上位 5 つの通信ポートについて解析を行った月別傾向を図8に示す。2017 年 11 月より 8545 番ポートでの不正アクセスが急増している。これは仮想通貨の Ethereum（イーサリアム）のクライアントソフトのデフォルトポートである。ユーザ IP とウォレットのアドレスがわかれば、自由にウォレットへアクセス可能となることから、脆弱性を持つウォレットを探索していた痕跡であると考えられる。

また、月により不正アクセス数の増減はあるが、53413 番ポート（上述のルータの脆弱性）についても不正アクセスが繰り返されていた。

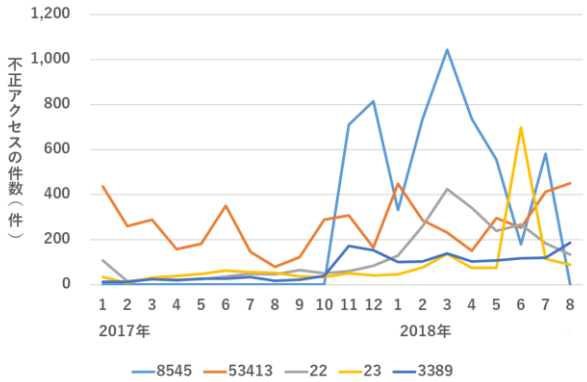

図8　オランダの上位 5 ポートの月別不正アクセスの傾向

同様にロシアを発信元とした不正な通信に関し、解析を行った月別傾向を図9に示す。不正アクセスの大半が 23 番ポートであった。こちらについては、IoT 機器の脆弱性探査が行われた痕跡であると考えられる。

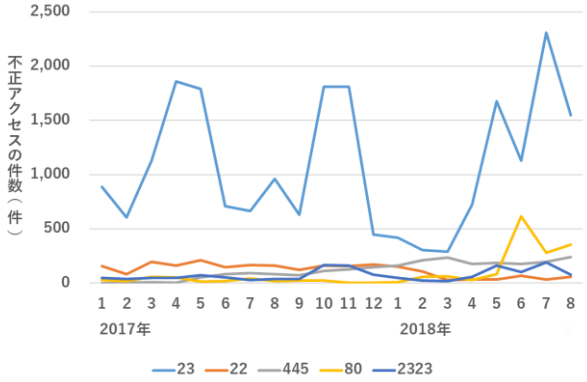

図9　ロシアの上位 5 ポートの月別不正アクセスの傾向

また、全ての月別ポート毎の不正アクセスをイメージ化したものを図10に示す。横軸はポート番号を対数表示、縦軸は上から 2017 年 1 月と月表示、円の大きさが不正アクセスの件数を表示する。特定のポート番号への不正アクセスが集中しているのがわかる。一方で、小さいながら円が全体にあることからほぼ全てのポート番号へ不正アクセスが行われていた。

4. 結論

本稿では医療機関に向けられた不正アクセスについて解析を行った。外部からの不正アクセスの試みは、社会一般と同様に昼夜を問わず医療機関に対しても行われていることが明確となった。特に IoT 機器（23 番ポート）やルータ（53413 番ポート）やデータベースサーバ（1433 番ポート）を狙った大量の不正アクセスの試みが日々行われており、不正アクセスは、医療機関においても大きな脅威であることを明示的に確認することができた。

これまでの医療機関では、「病院のネットワークは外部ネットワークとは繋がっていないから安全だ」という認識が長く続き、インターネットからの不正アクセスについてあまり意識が向けられていなかった。しかし、今後は、地域医療連携や研究等を起点に、院内ネットワークと外部ネットワークとの接続が各医療機関において急速に広がっていくことが予測される。

院内ネットワーク内に保管してある大切な患者情報や診療情報を安全に保持し続けるためには、全ての医療機関で「病院のネットワークは外部ネットワークとは繋がっていないから

安心だ」という意識を捨て、真剣に不正アクセス対策を検討する時期にあると考える。特に地域医療連携では連携機関の患者情報を相互利用することも想定され、ひとつの医療機関だけでなく、全ての医療機関において不正アクセスや情報セキュリティを強く意識した対策の徹底を進める必要があると考えられる。

参考文献

1) JPCERT/CC. インターネット定点観測レポート(2018 年 4～6 月). JPCERT/CC, 2018. [https://www.jpcert.or.jp/tsubame/report/report201804-06.html (cited 2018-Aug-31)].
2) @police. IoT 機器を標的とした攻撃の観測について. 警察庁, 2015. [https://www.npa.go.jp/cyberpolice/detect/pdf/20151215_1.pdf (cited 2018-Aug-31)].
3) JPCERT/CC. インターネットに接続された機器の管理に関する注意喚起. JPCERT/CC, 2016. [https://www.jpcert.or.jp/at/2016/at160050.html (cited 2018-Aug-31)].
4) JPCERT/CC. インターネット定点観測レポート(2015 年 4～6 月). JPCERT/CC, 2015. [https://www.jpcert.or.jp/tsubame/report/report201504-06.html (cited 2018-Aug-31)].
5) Threat Researcher - Tim Yeh. UDP ポートを開放した状態にする Netis 製ルータに存在する不具合を確認. トレンドマイクロセキュリティブログ, 2014. [https://blog.trendmicro.co.jp/archives/9725 (cited 2018-Aug-31)].

巻末

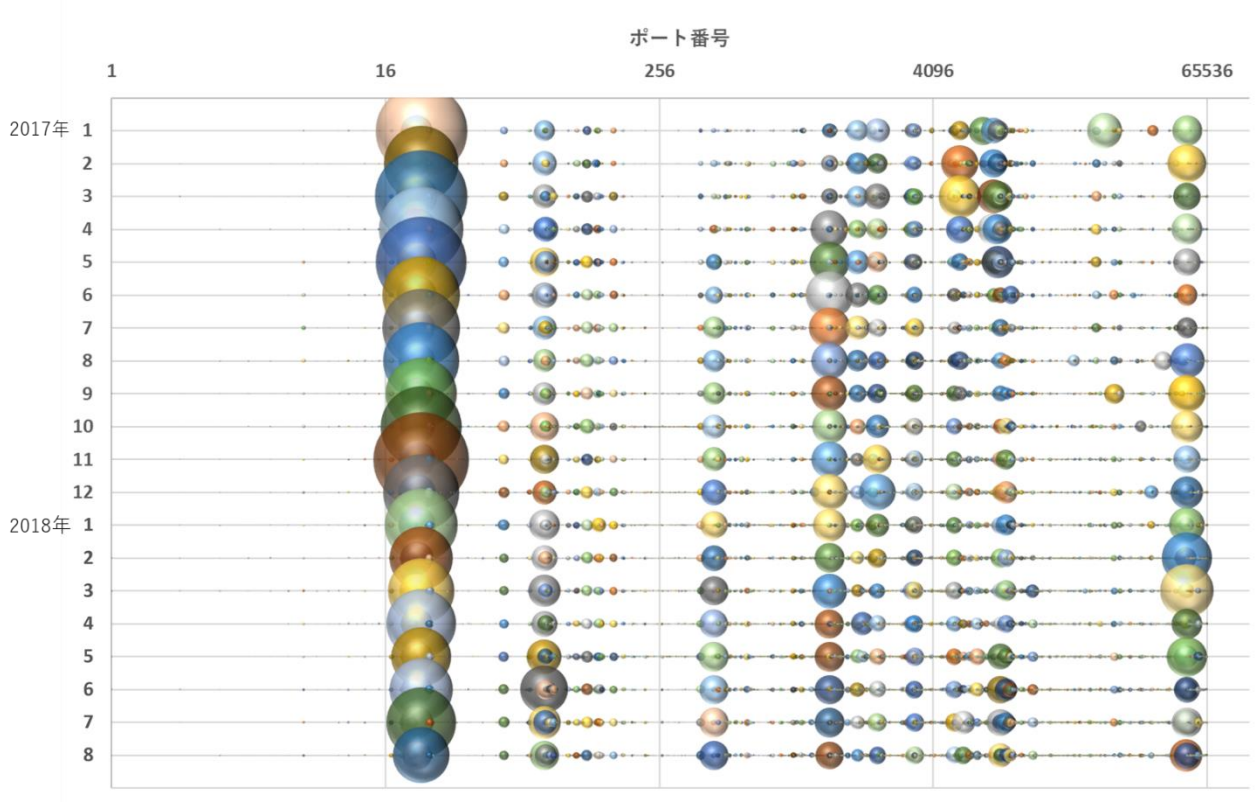

図10 月別ポート毎の不正アクセスをイメージ化