大会企画

2019年11月23日(土) 9:00 ~ 11:00 D会場 (国際会議場 2階中会議室201)

大会企画2
医療機関を取り巻く情報セキュリティの現状：何が脅威で、何を守るために、できることは何か

オーガナイザー：美代 賢吾（国立国際医療研究センター 医療情報基盤センター）
座長：黒田 知宏（京都大学医学部附属病院 医療情報企画部）

[3-D-1] 医療機関を取り巻く情報セキュリティの現状：何が脅威で、何を守るために、できることは何か

美代 賢吾[1]、松山 征嗣[2,3]、林 薫[4]、青木 眞夫[5] (1. 国立研究開発法人 国立国際医療研究センター、2. トレンドマイクロ株式会社、3. 内閣府日本医療研究開発機構・医療情報基盤担当室、4. パロアルトネットワークス株式会社、5. 独立行政法人 情報処理推進機構)

キーワード：Information Security、Information Network、Hospital Information System、Internet of Things、Hospital Administration

医療機関の電子化は進み、情報システムは今の医療に必要不可欠なものとなっている。多くの場合、電子カルテシステムなど個人情報を扱うシステムは、インターネットとは切り離された環境で運用されているが、現実には、地域連携やリモートメインテナンス、ソフトウェアやマスタアップデートのためのサーバ接続、オンライン請求など、何らかの形で部分的に接続されていることも多い。従前は、マルウェアの増殖にともなうネットワークやサーバ負荷の増加によるシステムダウンなどがインシデント事例として見られたが、近年では、個人レベルの愉快犯的なサイバー攻撃ではなく、国家規模のレベルで実行される、金銭や情報の窃取を目的としたサイバー攻撃が増加している。これに伴い、我々は、既知のマルウェアの駆除を目的とした対応から、未知の攻撃に対する対応へとシフトしていく必要がある。
このシンポジウムでは、実際に起こった、医療機関へのサイバー攻撃の事例を紹介するとともに、世界的な状況と日本に対するサイバー攻撃の現状、そして近年特に注目されているIoT機器のセキュリティについて、専門機関およびセキュリティベンダーから、現状の報告と、対策と効果について説明し、我々がとりうる方策について議論をおこなう。

医療機関を取り巻く情報セキュリティの現状
－ 何が脅威で、何を守るために、できることは何か－

美代 賢吾[*1]、松山 征嗣[*2*3]、
林 薫[*4]、青木 眞夫[*5]
*1 国立研究開発法人 国立国際医療研究センター、*2 トレンドマイクロ株式会社、
*3 内閣府日本医療研究開発機構・医療情報基盤担当室、*4 パロアルトネットワークス株式会社、
*5 独立行政法人 情報処理推進機構

Current Status of Information Security in Medical Institutions:
- What Are the Threats and What Can We Do to Protect Against These Threats? -

Kengo Miyo[*1], Seiji Matsuyama[*2*3], Kaoru Hayashi[*4], Masao Aoki[*5]
*1 National Center for Global Health and Medicine, *2 Trend Micro Inc.,
*3 The Office for Japan Agency for Medical Research and Development, *4 Palo Alto Networks K.K.,
*5 Information-technology Promotion Agency

Abstract

Information systems are widely used in medical institutions and are indispensable within the modern medical field. In most cases, systems that process personal data, such as electronic health record systems, are not connected to the internet. However, in some cases, these systems may be partially connected to an outside network to facilitate regional healthcare networks, remote maintenance, software and master updates, healthcare bill information exchanges, etc. Therefore, such systems must be prepared for cyber threats.
In the past, typical security incidents involved a system going down due to an increase in network and server load caused by the proliferation of malware created by individuals seeking pleasure. However, in recent years, there has been an increase in large-scale cyber-attacks aimed at stealing money and valuable information. Therefore, the defense strategy must be shifted from known malware extermination to defense against unknown attacks.
In this paper, four experts from a healthcare institution, information security vendors, and a specialized information security agency discuss current healthcare information security topics. First, we introduce some real-life examples of cyber-attacks on medical institutions. Then, we explain the current state of cyber-attacks in Japan and the rest of the world, and the security of the Internet of Things (IoT). Finally, we discuss what can be done to protect against such cyber-attacks.

Keywords: Information Security, Information Network, Hospital Information System, Internet of Things, Hospital Administration

1. 医療機関を取り巻く状況

医療機関の電子化は進み、情報システムは今の医療に必要不可欠なものとなっている。多くの場合、電子カルテシステムなど個人情報を扱うシステムは、インターネットとは切り離された環境で運用されているが、現実には、地域連携やリモートメインテナンス、ソフトウェアやマスタアップデートのためのサーバ接続、オンライン請求など、何らかの形で部分的に接続されていることも多い。従前は、マルウェアの増殖にともなうネットワークやサーバ負荷の増加によるシステムダウンなどがインシデント事例として見られたが、近年では、個人レベルの愉快犯的なサイバー攻撃ではなく、国家規模のレベルで実行される、金銭や情報の窃取を目的としたサイバー攻撃が増加している。これに伴い、我々は、既知のマルウェアの駆除を目的とした対応から、未知の攻撃に対する対応へとシフトしていく必要がある。

本稿では、実際に起こった、医療機関へのサイバー攻撃の事例を紹介するとともに、世界的な状況と日本に対するサイバー攻撃の現状、そして近年特に注目されているIoT機器のセキュリティについて、専門機関およびセキュリティベンダーから、現状の報告と、対策と効果について説明し、我々がとりうる方策について述べる。

2. 医療機関への攻撃の実例とその対応：今ここで何が起こっているのか

2007年9月に、ある大学病院で、病院情報システムがマルウェアに感染し、院内の端末やサーバなどに被害がおよび、処方箋の発行や会計ができなくなるなどの影響が出た。2009年2月にも、別の大学病院でUSB経由でマルウェアに感染し、やはり病院情報システムに大きな影響が出たとされている。これらの事案ではいずれも、攻撃者が意図して引き起こしたものでは無く、偶然職員が持ち込んだマルウェアによって、業務の遂行が困難になった事例である。

しかし、その後の10年で、情報セキュリティに関わる状況は大きく変わってきた。日本年金機構の例を出すまでもなく、攻撃者が情報窃取や金銭の要求などの明確な目的をもって攻撃する事例が増えている。国立国際医療研究センター（NCGM）にも、様々な標的型メールやばらまき型メール、ま

た公開サーバーへの攻撃などが観測されており、従来の対策と異なるアプローチでの取り組みの必要性に迫られている。本講演では、医療機関への攻撃の一例として、当センターへのサイバー攻撃の最近の状況について説明する。これらの攻撃に対して、システム、組織体制、教育の面でどのような対処を行っているか、具体的事例とそれに対する我々の取り組みを紹介することで、職員への教育も含めた医療機関における情報セキュリティ対策の議論のきっかけとしたい。（美代賢吾）

3. IoT 機器のセキュリティリスクと対策

ハードウェアの小型化、高機能化、通信インフラの充実も伴い、従来、ネットワークに繋がっていなかった機器がインターネットプロトコルを介してネットワークに参加するようになっている。ネットワークカメラやセンサーなど多種多様な機器が、店舗や工場、農業、自然災害監視などあらゆる環境、目的で活用が進んでおり、医療介護分野においてもその活用が大いに期待されている。一方で、セキュリティリスクへの考慮が不足しているためにセキュリティの実装や対策が十分になされていないものがサイバー脅威にさらされ、攻撃者に悪用されるケースも目立ち始めている。

一般的なインターネット接続する情報システムにおいても同様に必要とされる対策が、IoT 機器のセキュリティを考える際に、ハードウェアの制限や機器の構成上あるいは運用上困難となる問題など少なくない。製品製造元での開発段階において、そのセキュリティを考慮した実装や、運用保守段階における脆弱性の修正プログラムなどセキュリティの有効性を維持するアップデート、サポートの仕組みが重要となっている。

また、IoT 機器を遠隔で管理し、活用する際に機器とサーバ間の通信も秘匿性確保や改ざん防止を考慮する場合、暗号通信やコンテンツの暗号化、デジタル署名などにより対策を行う必要がある。

さらに、認められた機器のみが接続されることを確実にするためには認証の仕組みも重要となる。単純な ID 登録や使いまわしが発生しやすい脆弱なパスワード認証では不正接続のリスクを生じるため、運用ではなく技術的に認証を強化する方法の一つとしてクライアント証明書の活用も有効となる。

次世代携帯電話網である 5G では IoT 機器の接続、活用を後押しすることが期待されているが、その 5G ネットワークを通じて接続される IoT 機器のセキュリティ対策を通信事業者のネットワーク内で解決するアプローチも提唱されている。（松山征嗣）

4. 2019 年サイバー攻撃のトレンドとその対策

サイバー攻撃は年々増大しており、質的にも変化し続けている。現在では様々な攻撃ツールやノウハウなどの情報が広くインターネット上で共有されており、サイバー攻撃には必ずしも高度な技術力は必要ではなくなった。一方で洗練された攻撃者も多数活動しており、ターゲットやキャンペーンごとにツールや戦術を変えている場合もある。防御側は攻撃者や攻撃手法、ツールなどに関する脅威インテリジェンスを活用し、適切な対策と対応を行うことが不可欠となっている。

我々が収集したデータによると、2019 年上半期の国別攻撃検出数で日本は米国に次いで多く、その大半はメールに不正なファイルやリンクを添付して送りつけるものであった。メールは過去20年にわたりサイバー攻撃の主要な攻撃ベクターとして使われているが、攻撃者は開封率を高めるためのテクニックや感染に気づかれないための技術開発を現在でも継続している。

メール等で侵入した攻撃者は、最初の感染端末を足がかりに組織内部奥深くに侵入していき、重要データやシステムを見極めてから破壊やデータ窃取などを行う。こうした手法は以前から標的型攻撃で行われていたが、ツールと手口の一般化が進んだ結果、現在では多くのサイバー犯罪者も使うようになり被害の拡大につながっている。特に今年前半はランサムウェアを使った攻撃で多数の組織で業務の停止や、多額のシステム復旧費用がかかる等の被害が発生している。

医療業界は他の産業に比べ、個人に関する機微な情報を多く取り扱うこと、そしてシステムの停止などによって重大インシデント化する可能性があることから、攻撃者にとっては格好のターゲットになりやすく、事実そうした事故・事件が数多く報告されている。

本セッションではパロアルトネットワークスで収集した脅威データの分析から判明した2019年におけるサイバー攻撃のトレンドとその対策について紹介する。（林薫）

5. サイバー状況把握から見る、最近の攻撃傾向

近年、標的型サイバー攻撃という単語が一般化しているが、実際にどのような攻撃者像が、どのような活動をしているかを把握することは難しくなっていると考えられる。特に、ステートスポンサードと呼ばれる、他国が支援する攻撃については、センセーショナルな論調が多く、結果を一元的に見てしまう傾向も多いのではないかと思われる。

IPA/J-CRAT（サイバーレスキュー隊：以降当隊）では、主にステートスポンサードによるサイバー諜報活動に対する対策の支援を実施している。レスキュー活動に加え、皆様からの情報提供や公開情報等の調査を通じて、一連の攻撃を、攻撃対象となった組織に加え具体的に攻撃対象となった人物像まで見て行くことで、攻撃対象を組織群ではなく、対象人物の共通項で見ることの重要性がわかってきた。

また攻撃による被害を分解し、「気づかれずに侵入される」という点にフォーカスすることで、結果的に大量の情報が窃取されたという事案を、破壊や改ざん、妨害など複数の活動が可能であった事案として扱い、注意を払う必要があることがわかった。

ところで、当隊活動を医療関係への対応として見直してみると、いくつか関係者に対してお知らせすべきことも多いことがわかった。特に、スタンドアローン、孤立・独立システムであるとされながら、遠隔保守用途や、セキュリティアップデートのためにインターネット接続がされているケースが散見され、意図せず攻撃者の侵入を許してしまったケースである。これらのケースでは、組織の大小に変わらず「気づかずに侵入」され、攻撃ツールを仕掛けられていたが、情報系システムではないため、侵入対策や侵入後の対策の準備ができず、また情報系システム部門が対処できないシステムであるため、対策に時間を要するものであった。関係者は、組織の情報資源を攻撃者同様に全体俯瞰し把握することの重要性を知っていただきたい。（青木眞夫）