公募シンポジウム
シンポジウム10
IoTにおけるサイバーセキュリティの現状と対策、および対策としてのISAC

2021年11月21日(日) 09:10 〜 11:10 F会場 (2号館2階224)

[4-F-1] コロナ禍における IoTを含たサイバーセキュリティの現状と対策、および対策としての ISAC
Current status and measures of cyber security including IoT in Corona disaster and ISAC as a countermeasure

*近藤 博史[1]、長谷川 高志[2] （1. 鳥取大学医学部附属病院医療情報部、2. NPO法人日本遠隔医療協会）
*Hiroshi Kondoh[1], Takashi Hasegawa[2] （1. Division of Medical Informatics, Tottori University Hospital, 2. Japan Telemedicine Society）

キーワード：Cyber Security, IoT, ISAC (Information Sharing and Analysis Center)

我々は厚労省の補助金を得て「医療分野の情報化の推進に伴う医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究」を行っている。コロナ禍で感染を避けるために遠隔医療の仕組みの利用が有効性から導入が進むと考えられたが、時限的に認められた初診からのオンライン診療は進んでいない。また、昨年の本シンポジウムでは、 NICT田中氏の報告で日本のサイバー攻撃の半分が IoTを対象にしていた。日本の医療分野ではまだ攻撃事例はないが、米国では既に医療用 IoTからの侵入が報告されていた。そこで、今回はコロナ禍における IoTを含めたに医療機関等におけるサイバーセキュリティの現状と対策、および対策としての ISAC(Information Sharing and Analysis Center)について議論する。今回は研究代表の鳥取大学の近藤より昨年からの本調査研究のこれまでの成果を報告する。次にパロアルトの林薫氏からサーバー攻撃の現状を報告する。次に日本医療機器連合会担当の日本光電の松元恒一郎氏から日本医療機器工業会の対策の報告を行う。最後に厚労省の前田彰久氏から厚労省の現状把握と対策をご報告願う。最後に講演者と会場の皆様と医療機関等における IoT含めた管理の現状とサイバーセキュリティ対策を議論し、 ISACの組織化の方向について議論する。

コロナ禍における IoT を含めたサイバーセキュリティの現状と対策、および対策としての ISAC

近藤博史[*1]、長谷川高志[*2]、
山本隆一[*3]、美代賢吾[*4]、星本弘之[*4]、松元 恒一郎[*5]、林 薫[*6]、前田 彰久[*7]、井髙 貴之[*7]
*1 鳥取大学医学部附属病院医療情報部、*2 日本遠隔医療協会、
*3 医療情報システム開発センター、*4 国立国際医療研究センター、*5 日本光電工業株式会社　技術戦略本部、*6 パロアルトネットワークス株式会社、*7 厚生労働省

Current status and measures of cyber security including IoTs in Corona disaster and ISAC as a countermeasured

Hiroshi Kondoh[*1], Takashi Hasegawa[*2], Ryuichi Yamamoto[*3], Kengo Miyo[*4], Hiroyuki Hoshimoto[*4], Haruo Kuroki [*5], Koichiro Matsumoto [*6], Akihisa Maeda, Takayuki Idaka [*8]
*1 Division of Medical Informatics Tottori University Hospital , *2 Japan Telemedicine society,
*3 Medical Information System Development Center (MEDIS) , *4 National Center for Global Health and Medicine,
*6 Nihon Kohden Corp. *7 Palo Alto Networks K.K., *8 Ministry of Health, Labor and Welfare

Abstract

We have the Research and Study on Cyber Security Measures in Medical Institutions for the Promotion of Informatization in the Medical Field with a subsidy from the Ministry of Health, Labor and Welfare (MHLW). It was thought that the use of telemedicine system would be introduced due to its effectiveness to avoid infection by coronaviruses, but online medical treatment from the first visit, which was allowed for a limited time, has not progressed. In addition, half of the cyber-attacks in Japan targeted the IoT, as reported by Mr. Tanaka, NICT, in this symposium last year. Although there have been no attack cases in the medical field in Japan yet, intrusions from medical IoT had already been reported in the US. Therefore, we will discuss the current status and countermeasures of cyber security in medical institutions, including IoT, and ISAC (Information Sharing and Analysis Center) as a countermeasure. In this session, Dr. Kondoh will report on the results of this research since last year. Next, Mr. Hayashi of Palo Alto will report on the current status of server attacks. Next, Mr. Matsumoto of Nihon Kohden, who is in charge of the Japan Medical Devices Federation, will report on the measures taken by the Japan Medical Devices Association. Finally, Dr. Maeda of the MHLW will report on the MHLW's understanding of the current situation and countermeasures. Finally, the speakers and the audience will discuss the current status of management and cyber security measures.

Keywords: Cyber Security, IoT, ISAC (Information Sharing and Analysis Center)

1. 初めに

日本の医療 ＤＸ はコロナ禍でオンライン診療中心に TV 会議システムの普及が中心に医療 DX が言われているが、海外では mobile Health, Interoperability がキーワードで使われることが多い。DX は出版や音楽業界でコンテンツがデジタル化された後、その市場、社会構造が大きく変化したことを呼ぶところから、医療 DX を考えると、医療のコンテンツがデジタル化され、電子カルテが普及した後、市場、社会構造が大きく変化することになり、日本の医療も大きく変わりつつあることには変わらない。これまでセキュリティ上閉じていた診療情報は遠隔医療の進展によりインターネットの世界に大きく広がりつつある。医療機関の外で電子カルテや ＴＶ 会議を診療に扱うのみならず、Telemonitoring, digital therapeutics, Location Flexible Trialなど患者が直接扱う領域にも広がり、サイバーセキュリティ関係者が大きく広がる時代になってきた。また、サイバー攻撃もゼロトラストと呼ばれるような大きな時代になってきており、世界的にも ISAC と呼ばれる情報共有、解析、共有する組織が社会分野別に組織が始まっている。

2. 方法

近藤らは２０２０年度の厚生労働省の調査研究「オンライン診療・遠隔医療や「非接触」を念頭に置いた ICT 化の中で医療機関が具備すべきサイバーセキュリティ対策や技術を踏まえたサイバーセキュリティ指針の策定」の結果の要点を研究代表として報告する。

黒木はコロナ禍で広がるオンライン診療の現場からそのセキュリティに関して報告する。

松元は今後サイバーセキュリティー対策の重要な IoT 機器のサイバーセキュリティの現状を報告する。

林は、ウイルス対策の専門会社の立場からコロナ禍のサイバー攻撃の現状を報告する。

最後に前田は厚生労働省の立場からインターネットの世界に広がる医療情報システムの現状と世界的に広が理、日本でも電力、金融、航空などの分野で組織化された ISAC の医療分野における方向を説明する。

3. 結果

近藤博史、長谷川高志、山本隆一、美代賢吾、星本弘之は厚労省の補助金を得て「医療分野の情報化の推進に伴う医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究」を行った。孫氏の言う「己を知る」ことから、現状の閉じた病院情報システム中の注目点の洗い出し、急速に進む医療 DX として広がる mobile Health、IoT 分野、次に「敵を知る」意味で最近の攻撃の変化、ウイルス検知され難い亜型の増加、WannaCry, Emotet に見る既存メールの中の偽造 URL 経由の攻撃、攻撃後の内部ネットワーク経由のサーバ操作、また、これらの対策としての EDR(Endpoint Detection and Response)、産業毎の対策組織 ISAC(Information Sharing and Analysis Center), ゼロトラストの時代の対応についてヒアリングのより調査した。また、医療関係者に対するアンケート調査、遠隔医療学会会員に対するアンケート調査、オンライン診療利用の患者視点からのアンケート調査を行った。ヒアリングからは①ネットワークの入口, ②ネットワークの裏口, ③利用者のアクセス認証, ④端末上のデータの入力・出力部分, ⑤管轄するネットワーク, 無線 LAN などからの漏えい・侵入, ⑥重要部分までの隔壁構造の設置, ⑦データバックアップに分類して対策を考えることが必要であった。海外から日本への攻撃の半分以上が IoT を対象としており、医療系 IoT 機器の事例は無いが、今後注意が必要であった。遠隔医療学会会員のアンケート調査では被害者は少なく、IoT 機器の利用が進む医療機関の調査では IMDRF 文書にある対策は十分行われていなかった。患者視点からの調査ではオンライン診療未利用者は情報漏洩の危惧があるが、利用者は利用に満足していた。

黒木は COVID-19 対策には遠隔医療が不可欠であり、基本である。delta 株が蔓延した場合には、医療における地域連携が重要である。専門病院、二次病院、一次医療機関が連携して対策を講じる必要があります。このようなシステムを構築するための基盤となるのが遠隔医療です。遠隔医療ではまず、画面上の患者さんに話しかけ、通常の問診を行います。その際、患者さんの意識レベルや全身状態を確認します。患者さんにはカメラの前で口を開けてもらって咽頭所見を確認し、上半身を見せてもらって呼吸や咳を確認します。医師はその場で患者の酸素飽和度モニターによる酸素飽和度と脈拍数を確認することができる。今、日本では COVID-19 の患者さんの多くが、医療を受けられずに自宅で待機しています。遠隔医療はそのような患者さんをつなぐことができます。医師は、遠隔医療により感染症のリスクなく診療を行うことができます。患者さんも負担なく医療を続けられるようになります。COVID-19 対策としての遠隔医療の行政支援も可能になりつつあります。SARS-Cov-2、特に delta 系統の感染が拡大した場合には、遠隔医療が必要となります。

www.DeepL.com/Translator（無料版）で翻訳しました。

松元は近年、医療機器は、有線／無線のネットワークを介しての他の機器やソフトウェアと連携等システム化や USB メモリ等の携帯型メディアを使って医療情報を入出力する機会も増えて来ており、ネットワーク等には医療機器以外の電気機器も接続されており、医療機器の使用環境が常にセキュアであるとは限らない。このため、医療機器の有効性及び安全性を確保するためにサイバーセキュリティの重要性がより増している。本稿では、医療機器を経由して侵入されるセキュリティリスクの事例を説明し、院外を中心としたモバイルヘルスの活用がより推進されること鑑み、平成 28 年に総務省・経産省から発出された「IoT セキュリティガイドラン Ver1.0」をベースとして医療機器との特性について論じる。さらに厚生労働省からは、平成 27 年、「医療機器におけるサイバーセキュリティの確保について」、平成 30 年「医療機器のサイバーセキュリティの確保に関するガイダンスについて」が主として医療機器製造業者に対して発出されている。サイバーセキィリティとしては、他の機器・ネットワーク等と接続して使用する又は他からの不正なアクセス等が想定される医療機器については、サイバーリスクを含む危険性を評価・除去し、リスクマネジメントを行い、使用者に対する必要な情報提供や注意喚起を含めて適切な対策を行うこととしている。2020 年 4 月には、国際医療機器規制当局フォーラム（IMDRF）から医療機器サイバーセキュリティの原則及び実践に関するガイダンスが公表された。これは、一般原則及びベストプラクティスについて、全ての責任関係者に対して推奨事項を提供するもので、製造業者、医療提供者、使用者、規制当局及び脆弱性報告者を含むすべての利害関係者の共同責任であり、2023 年を目途に国内でも導入の検討が進んでいる。さらにモバイルヘルの観点も踏まえて安全管理ガイドラインとサイバーセキュリティガイダンスについて論じる。

林は進化する手術ロボットやネットワークに接続される医療機器、クラウドを使ったサービスの普及、収集された大量のデータを機械学習で解析するなど、他業種と同じく医療業界においてもデジタルトランスフォーメーションの波が押し寄せている。人間や機械、その他の資源が互いに通信することで情報を共有し、既存プロセスの効率化や新たな価値の発見につながる大きな変革の機会だけでなく、つながることによるリスクの高まりに対しても備える必要がある。本稿では IoT やクラウド利用など DX が進んだ他業種におけるサイバー脅威の被害の実例を紹介し、さらなるデジタル化が進むと予想される医療業界において検討すべきポイントについて論じる。特にここ数年、最も深刻な被害をもたらしているサイバー攻撃の一つが身代金を要求するランサムウェアである。ランサムウェアの被害は広範にわたっており、医療を含む多くの業界に被害をもたらしている。弊社の調査では 2020 年の平均支払額は 3000 万円以上であり、最も高額な要求額は 10 億円であった。金銭的な側面だけでなく被害組織が数週間にわたって事業を停止せざるを得ないような事業継続性に影響を与えるケースも多発している。さらに米国ではランサムウェアによるサイバー攻撃の被害により重要インフラである石油パイプラインが5日間停止してしまい、一時的に燃料不足が発生するなど社会生活に大きな影響を与える事例も発生してしまった。攻撃手法のマニュアル化、ダークウェブなどの匿名化技術の発達そして仮想通貨の流通により、ランサムウェアをはじめとするサイバー犯罪は逮捕されるリスクが低く、高額なリターンが得られるとあって新規参入する攻撃者が増えている。本稿ではランサムウェアによる侵害の実態の解説と、今後のセキュリティ対策の根幹となるゼロトラストについて論じ

る。

前田らは医療機関では、医療情報システムを取り巻く環境の変化や医療情報システム・機器の高度化等により、サイバーセキュリティ対策を講じることが喫緊の課題となっている。

厚生労働省では、医療機関等における電子的な医療情報の取扱いに関して「医療情報システムの安全管理に関するガイドライン」を定めており、令和 3 年 1 月には第 5.1 版への改定を行った。サイバー攻撃を受けた（疑い含む）場合等には厚生労働省への報告を求め、内閣サイバーセキュリティセンター等と連携し、必要に応じて当該医療機関に対するサイバーセキュリティに係る技術的事項等の助言や、マルウェアや不正アクセスに関する技術的な相談窓口の紹介等を行っている。データヘルス改革では、令和 3 年 6 月に 2025 年度に向けた工程表を策定しており、こうした動きも踏まえ、医療機関等を中心とした医療分野のサイバーセキュリティ対策の強化はより一層重要となっている。

厚生労働省では、令和 2 年度に医療機関等が自院のサイバーセキュリティ対策の現状を把握することを目的としたサイバーセキュリティ対策チェックリストや、医療情報システム等の障害発生時の対応フローチャート等を整備し、さらに医療機関等向けの研修・E-learning も実施した。加えて、実際に医療現場の利用者を募り、情報共有・掲示板ツールを用いた情報共有・相談体制等を試行することで、その意義や効果、課題等についても検討を行った。

今後の医療分野におけるサイバーセキュリティ対策に当たって、医療機関同士の共助の精神の下、医療機関同士が安心して相談や意見交換をし合える場を整備することには一定の有用性がある。厚生労働省としても引き続き医療機関等のサイバーセキュリティ対策の支援、研修・E-learning の実施、情報共有・相談体制の試行を予定しており、医療分野のサイバーセキュリティに関する共助の取組が進んでいくことに期待したい。