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-1-01] 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
Research and study on cyber security measures for medical institutions in accordance with the promotion of informatization in the medical field

*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]（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、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）
*Hiroshi Kondoh[1], Takashi Hasegawa[2], Ryuichi Yamamoto[3], Kengo Miyo[4], Hiroyuki Hoshimoto[4]（1. Division of Medical Informatics, Tottori University Hospital, 2. Japan Telemedicine Society, 3. Medical Information System Development Center, 4. National Center for Global Health and Medicine）
キーワード：Telemedicine, Cyberattack, IMDRF, ISAC (Information Sharing and Analysis Center), Cloud Computing

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。

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

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]
*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

Research and study on cyber security measures for medical institutions in accordance with the promotion of informatization in the medical field

Hiroshi Kondoh[*1], Takashi Hasegawa[*2], Ryuichi Yamamoto[*3], Kengo Miyo[*3], Hiroyuki Hoshimoto[*3]
*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

Abstract

In the context of ICT with online medical care, telemedicine and "non-contact" in mind, Kondoh et al. interviewed cyber security experts and people involved in various medical systems about the status of cyberattacks and system structures in the field and organized the perspective of cyberattack risks in medical systems. Hasegawa and Kondoh conducted a questionnaire survey among the members of the Japanese Society of Telemedicine from this perspective and obtained survey results that suggest that awareness has not yet been fully raised. Lack of information was thought to be a major factor. Yamamoto et al. conducted a web-based questionnaire survey from the perspective of patients about online medical care, which has rapidly expanded, and found that only about 40% of the respondents understood the contents of online medical care. Miyo et al. surveyed medical institutions, and the responses from 508 medical institutions showed that while the use of IoT devices is increasing, most medical institutions are not prepared to deal with cyber security as described in the IMDRF document. In order to develop draft cyber security guidelines, it was found that an organization such as ISAC is needed to share the current cyberattack situation, case studies, countermeasures, systems, and education. From listening to the construction of ISACs in other fields, it is clear that the medical field will continue to expand its base and its difficulties, and it is important to consider structural measures against cyberattacks in the direction of the next generation of cloud computing.

Keywords: telemedicine, cyberattack, IMDRF, ISAC (Information Sharing and Analysis Center), cloud computing

1. はじめに

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」（以下、本研究）において対象範囲として考える、オンライン診療、遠隔病理診断、遠隔画像診断、地域医療連携、病院間を繋ぐオンライン研究ネットワーク、今後の生活習慣病対策から未病段階の介入、あるいは日常のモニタリングからタイムリーな介入を行うデジタルヘルス、研究も location flexible trial と拡大する mobile Health の携帯とクラウドサーバ間通信などにおいては、サイバーセキュリティ対策は必須である。しかし、従来の病院、診療所の電子カルテ等の医療情報システムに関してもインターネットから一見閉じたシステム構築をしているようであるが、システム保守や媒体接続時の感染などの危険は存在し、サイバーセキュリティ対策が無縁とは言えない。また、今後、コロナ禍で進む在宅勤務やオンライン会議、遠隔モニタリング等の接続の急速な拡大と利用者の増加もセキュリティ対策の教育活動必要性が高まってくる。このような現状と今後の医療現場の状況を把握することはサイバーセキュリティ対策を考える上で重要である。また、攻撃側のここ数年の変貌も大きく、その状況把握がサイバーセキュリティ対策を考える上で重要である。

2. 方法

近藤らはサイバーセキュリティの専門家や種々の医療システムの関係者に、その分野におけるサーバー攻撃の状況とシステム構造を聴取した。表1にまとめた。

長谷川はその観点から日本遠隔医療学会会員にアンケート調査を行った。日本遠隔医療学会会員メーリングリストを用いて、アンケートへの協力を依頼した。アンケートは、Google Formsを用いて作成して、WEB上で回答をもとめた。調査期間　2021年3月10日～20日。対象者数は、メーリングリストの有効メールアドレス506件であった。

美代賢吾、星本弘之は医療機関のサイバーセキュリティ対策について、医療機関のサイバー攻撃リスクの観点から、サイバーセキュリティ指針案の策定に資することを目的として調査検討を4000医療機関に調査票を送付し調査した.

山本隆一は医療分野におけるガイドライン作成者の視点から、各ガイドラインの作成時の状況、その後について医療情報システム開発センターの立場から国、企業系の意見を聴取を行った。また、急速に拡がったオンライン診療等について患者側の視点からWebアンケート調査をモニター会社（マクロミル）のモニター会員から１年以内に特定健診など定期健康診断や歯科のメンテナンス以外で医療機関を受診し、医師等からの病状や治療に関する説明を理解できた18歳以上の

国内在住者約1000名からWebアンケートを行なった。

3. 結果

近藤の聴取では、多数の医療システムのサイバー攻撃リスクの観点を整理し、まとめを表２に記載した。医療機関の場合はシステム全体を考える必要があるが、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。

これはこれまでの閉じた医療機関ネットワークの対策であり、外部接続は、地域医療連携、オンライン研究に限定されており、①ネットワークの入口が中心の対策になっていた。

最近では、働き方改革、COVID-19対策で在宅勤務での電子カルテ利用の要求があり、インターネット経由上のVPN経由で電子カルテを職員宅からアクセス機能も用意されている。

一方で、オンライン診療では独立したシステム運用がガイドラインで決められている。今後、画像検査や治療の説明時に電子カルテとの並行利用が必要になる。

オンライン診療でも、患者あるいは支援者が操作して得られるデジタル聴診器やデジタル耳鏡、鼻鏡、あるいは超音波検査などデータは標準フォーマットで電子カルテあるいはクラウドサーバに保存されるものが多く、これらの情報も記録参照には電子カルテ系の並行利用が必要になる。

医療DXでも進む運動量、体重、体温、脈拍等のデータを記録するモバイルヘルスではクラウド保存の独立したものが多い。

一方、サイバー攻撃に関して、NICTのインシデント分析センター（NICTER）での日本国内のインターネットの入口はサイバー攻撃の半分以上が現在IoT機器であること、2016年の米国ではIoT機器経由で医療機関への侵入がされた事例があること、医療機器工業会からは、ネットワーク接続されるIoT医療機器がシステム更新を超えて利用されるため、更新時のIoT医療機器の設定、管理に注意が必要であることが言われた。また、ウイルス対策システム会社からは、上記組織内の管理に加えて、最近のウイルスが検知ソフトに検知され難く、また、実際のメールに仕込まれたURL経由の感染、一度侵入するとネットワークで拡散する形式への変貌があり、ゼロ・トラストと呼ばれるように内部機器といえども、安心できない状況で、EDRと呼ばれるように端末での検知と対策が必要になり、変貌し、ISACと呼ばれる情報と対策の共有組織の必要性が出てきている。

他方、鳥取大学病院では2008年よりシンクライアント端末の利用を行い、2020年には仮想サーバ、仮想ストレージの導入によりセキュアで効率的な電子カルテ、画像システムを導入し、クラウド化も容易になっている。今後、大学病院のような大規模医療機関もクラウド化に進むと見られており、モバイルヘルス等ともにクラウド化に移行して広がる医療情報システム利用者のサイバーセキュリティ確保する方法が効率的と考えた。

長谷川高志の日本遠隔医療学会会員にアンケート調査では、回答件数　106件（20.9%）であった。その中で医師が最も多かった（57.4%）。遠隔医療（オンライン診療、遠隔モニタリング、画像診断等）の従事者が多く、地域医療情報連携の従事者が続いた。その中で医療情報技師やサイバーセキュリティ関連の有資格者は少なく、実事故に遭遇していない回答者が多かった。事故としてはウイルス感染と不正アクセスが多かった。ISACについては、知らないとの回答が半数以上だった。また必要性については、「何とも言えない」との回答が多かった。まだ意識が十分高まっていないと考えられる調査結果を得た。情報不足が大きな要因と考えられた。

美代 賢吾、星本 弘之の4000医療機関の調査では、508の医療機関から回答があった（回答率12.7%）。IoT機器の利用が進む中、殆どの医療機関でIMDRF文書に記載されるサイバーセキュリティへの対応ができていないことがわかった。

山本隆一のガイドライン作成者の視点からのヒアリングでは保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム （HEASNET）に参加している企業を中心に意見が聞けた。その中では事業者内部の複数事業者の関与状況や、データの国外通過・保管などが不明瞭になっており、データ種別と提供個別機能ごとのリスク対応、情報流（国内外の経由ルート・暗号化の有無、データ保存の有無、責任分担範囲等）の内容を把握の重要性等が聴取できた。一方、調査の急速に拡がったオンライン診療等について患者側の視点からWebアンケート調査では、オンライン診療の内容を理解しているものは４割ほどで、オンライン診療受けた者は殆どが満足し、回答者の殆どがオンライン診療を受けられることを望んでいた。

専門家へのインタビューでは、孫氏の言う「己を知る」こととして、現状の閉じた病院等の情報システム中の注目点の洗い出し、次に、今後、急速に進む医療DXとして広がるmobile Health、IoT分野の専門家にインタビューした。また、次に「敵を知る」意味で最近の攻撃の実態調査を行なった。インタビューを行なった先について表1に記載する。

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。

ヒアリングからは医療機関については、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と思われ、提言する。この7分野を表2に記載する。

NICTでの調査では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、これまで医療系IoT機器の事例は無いが、今後は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。

4. 考察

遠隔医療学会会員に対する調査では技術系の有資格者が少なく、事故経験も少なく、ISACに知られておらず、ヘルスケア分野のサイバーセキュリティに関する問題意識の醸成は進んでいないと考えられた。危機は目の前にあり、もしかすると実際には被害を受けているのに、気がついていないのか

もしれない。早急な意識高揚が必要と考えられた。

病院対象の調査からは、IoT機器に対するサイバー攻撃のリスク評価と対応基準の検討、IMDRF文書のセキュリティ要件に対応するための医療機関を支援する組織の必要性、日々進化するサイバー攻撃に対応し、的確な教育を行う仕組みの組織的な提供により、日本の医療機関全体のサイバー攻撃への対処能力の向上につなげる必要性が示唆された。

ガイドライン作成者の視点からのヒアリングではデータ種別と提供個別機能ごとのリスク対応、情報流(国内外の経由ルート・暗号化の有無、データ保存の有無、責任分担範囲等)の内容を把握の重要性からサービス仕様適合開示書の１(2)共通理解のための提供情報の①運用管理規程に定める必要のある事項　③全体構成図　④リスク対応一覧の作成が言われた。

また、山本隆一は、現状の「医療情報システムの安全管理に関するガイドライン　5.1版」についてサイバーセキュリティに関しても一定の記載があり、対応策も述べられている。しかし、ネットワークセキュリティに関しては、2007年にレセプトオンラインの開始に際して強化されたものの、現状のクラウド化の流れや、オンライン診療の急速な普及、あるいは保険資格のオンライン確認システムの導入やそれに伴うデータヘルス集中改革で導入が進められている様々なシステムに対応可能性について十分に検証されていないとの意見であった。

一方、オンライン診療等について患者側の視点からWebアンケート調査からは患者はオンライン診療に満足しており、制度を必要としている。現状オンライン診療システムと電子カルテ等は分離するか、同一端末で利用する場合には医療情報システムの安全管理に関するガイドラインに準拠することを求めているが、今後は対面診療とオンライン診療の有機的な結合が求められることは明白で、ITリテラシーを一律には期待できない患者端末を用いるオンライン診療システムとの接続を前提にする必要がある。この場合、リスクの大部分はサイバーセキュリティであり、十分な対策が求められる。

つまり、病院においてはネットワークのセキュリティ、IoT機器に対するサイバーセキュリティの充実のための対策が必要であり、遠隔医療関係の医療者側にも情報提供や教育、ITリテラシーを一律には期待できない患者端末を用いるオンライン診療システムとの接続を前提にする必要がある。

したがって、サイバーセキュリティ指針案の策定には現状のサイバー攻撃の状況、事例、対策、体制、教育等を共有するISACのような組織が必要であることがわかった。

また、閉じた病院のシステムでも複数の事業者の関与があるが、モバイルヘルスの広がりではIoT機器、スマホ、タブレット、クラウドサーバなど電子カルテの連携もあり、同時にオンライン診療も加わり、医療分野の裾野の広さが今後も拡大しその把握の困難さ明確である。その意味からもISACのような事業者間の情報共有は必要である。

他分野のISACの構築の聴取からは電力、金融、航空では大小、大きさの相違はあるが業務フローは類似であり、利用者の関与も一定であり、均一性を感じる。

ただ、医療機関にあるサーバ系も今後クラウド移行の方向性があり、クラウド化に移行した方が,入力系、サーバ系、参照系に単純化されるように思われる。その意味で、次世代のクラウド化のこの構造の中でサイバー攻撃対策を考えることが効率的な方法と思われた。

5. 結論

アンケート調査、ヒアリングからサイバーセキュリティへの関心、知識が少ないことがわかり、サイバーセキュリティ指針案の策定に向けて、現状のサイバー攻撃の状況、事例、対策、体制、教育等を共有するISACのような組織が必要であることがわかった。

しかし、日本の現状では働き方改革、オンライン診療、モバイルヘルスの流れからこれまで閉じていた医療システムが、急速に拡大多様化する医療システムの現状把握のためにもISACの必要性が感じられた。

他分野のISACの構築の聴取からは類似の方法で対応可能かと言えば、医療分野の裾野の広さが今後も拡大しその困難さ明確であった。

その意味で、次世代のクラウド化の方向の中で構造を単純化し、同時にサイバー攻撃対策を考えることが効率的な方法と思われた。

参考文献

1) NIST :Z ero Trust Architecture. Special Publication,800-207.2020, https://csrc.nist.gov/publications/detail/sp/800-207/final

2)鎌田敬介： 金融業界におけるサイバーセキュリティ対策の共助の仕組み. 医療梢報学連合大会論文集 2020, 40(Suppl):1 84-185

3)近藤栂史： 急速に広がるオンライン診療・遠阪医療と医旅機関のサイバーセキュリティ. 医旅情学連合大会論文集 2020, 40(Suppl) :1 65-166

4) 厚生労働省： 医療俯報システムの安全管理に関するガイドライン第5.1 版, 2021 https://www.mhlw.go.jp/content/10808000/000730541.pdf

5) 近藤博史： 世界椋準IHE を用いた医療連携システムの維持期における課題. 日本遠隔医療会誌 14: 109-11, 2018

	聴取分野	聴取した人
1	オンライン診療	MICIN坂本氏
2	医療連携 介護ネットワーク	岩美病院、おしどりネット、まめネット関係者、
3	Tele Stroke	山口大学脳神経外科 鈴木倫保教授, 聖マリアンナ医科大学 長谷川康弘教授 富士フィルムメディカル 前田氏
4	心臓血管外科 救急患者転送	旭川医科大学心臓血管外科 東信良教授
5	国立大学病院 医療情報部長会	北海道大学医学部附属病院 遠藤准教授ら
6	日本IHE協会	ITI委員会
7	NICT	サイバーセキュリティ研究室 井上大介室長
8	医療IoT	日本光電工業㈱ 技術戦略本部、松元恒一郎氏
9	鳥取大学医学部附属病院	医療情報部長、メディアセンター近藤博史
10	遠隔ICU	集中治療学会
11	SaMD(プログラム医療機器)	Siemens担当者
12	クラウドサービス	AWS 営業担当
13 14	金融系ISAC 電力系ISAC	鎌田敬介氏 谷口浩氏
15	ウイルス対策	トレンドマイクロ松山氏
16	介護系	野島病院担当者

	分類	**対策**
1	LAN の入口	FW, IPS による流入、流出の検知、VPN、GW の設置
2	裏口	検査機器等の保守
3	アクセス認証	2 要素認証、生体認証など
4	媒体	USB メモリ、CD など
5	ネットワーク	無線、有線への機器接続、通信情報の漏洩、 DNS などの管理も
6	隔壁	ネットワーク内の分離
7	重要データのバックアップ	医療では医療機関の BCP と患者の BCP の両方を 考える必要がある。