日医総研 委託研究報告書

医療機器高度化に伴う医療情報の
サイバーセキュリティマネジメントに関する研究

2021 年 3 月

日本医師会総合政策研究機構
秋冨慎司

医療機器高度化に伴う医療情報のサイバーセキュリティマネジメントに関する研究

日本医師会総合政策研究機構	秋冨慎司

研究協力者（五十音順）

日本医師会総合政策研究機構	澤倫太郎
株式会社川口設計	川口洋
ヘルスケアクラウド研究会	笹原英司
株式会社 BLUE	篠田佳奈
国立研究開発法人　情報通信研究機構（NICT）	園田道夫
産業技術総合研究所	鎮西清行
株式会社 Eyes, JAPAN	山寺純
SOMPO リスクマネジメント株式会社	Assaf Marco

キーワード

◆サイバーセキュリティ　◆IoT　◆サイバーセキュリティマネジメント
◆サイバーテロ　◆マルウェア

目次

１．はじめに

背景：

中央官庁やグローバル企業のみならず、中小企業においてもサイバー攻撃が多発し、多くの情報漏えいや業務停止、身代金支払いが発生し多大な損害が発生している。すでに世界各国でサイバーセキュリティに対して多額の費用を投じて対応をしている。東京オリンピック･パラリンピックを迎えるにあたり、大規模イベント時のサイバーセキュリティ対策のための投資が行われているが、問題が発生した場合に人命に関わる病院のサイバーセキュリティに対しては議論が始まったばかりで、準備はまだ不完全の状態である。仮に病院を一斉に攻撃された場合に混乱が 1 週間以上続き、重症患者の受け入れが困難になるだけでなく、通常の外来受診機や定期手術などの病院機能が消失する可能性があり、オリンピック・パラリンピック関係なくその対策は急務を要する状況である。

また、1999 年に厚生省（現厚生労働省）より「診療録等の電子媒体による保存について」が、医政局から出され、電子カルテの使用が認められた。それ以降、様々な電子カルテが２０年以上使用され、使用自体が一般的となっているが、医療関係者のサイバーセキュリティの脅威への認識が極めて低く、また多くの脅威は形を様々に変えて攻撃を繰り返すため、医療機関が取るべき医療情報のセキュリティ対策も常にアップデートが必要な状況である。

目的：

病院は複雑なシステムで成り立ている。例えば、電子カルテのシステムだけでなく、検査などのオーダーリングシステム、画像や血液データなどの参照システム、文章管理システムなど複雑なシステムで構成されている。また各部門のシステムも存在している。例えば、血液検査システム、生理検査システム、放射線検査システムなども別々のシステムで構成されている例がある。どのシステムを攻撃しても、病院機能は確実に低下する。しかも別々の会社がシステムを構築し、他の会社のサイバーリスクまで理解せずに、病院内を構築しているシステムだけが巨大化しており、全体像が見えなくなっている。

また電子カルテに対するサイバー攻撃のみならず、インターネットに接続された医療機器（IoT 機器）へのハッキングは比較的容易であり、今後は身代金目的やその他の犯罪に絡み、医療施設がハッカーからの標的になることは十分に考えられる。そのため現在、医療現場で発生している実際の事案について情報を収集し、対策のための分析を行う。

２．医療分野におけるインターネット活用とサイバーセキュリティへの危機意識

レセプトオンラインの義務化からはじまった環境の変化：

2006 年に「レセプトオンライン請求」が始まり、それまでレセプト コンピューター や電子カルテは、ネット環境に接続することはなく、印刷して紙で提出していた環境が一変した。レセプトには、患者の個人情報、保険情報、診療行為、薬剤など重要な個人情報が記載され、 その情報のセキュリティレベルは高度な環境を必要としていたため、政府はレセプトをオンラインで請求するために VPN（Virtual Private Network）を使用した暗号化技術による回線の使用を義務づけた。2019 年の社会保険診療報酬基金の「レセプト請求形態別の請求状況（平成 30 年度）」では、医療機関全体でオンラインでの請求は 60.0％、電子媒体での請求は 34.0％、紙での請求はわずか 6.0％となった。

また、2010 年に厚生労働省が「診療録等の外部保存について」という通知を一部改正し、医療機関か医療機関に準ずる施設でしか認めていなかった診療録等の医療情報の管理を、企業が運営するサーバで管理する、クラウドサービス（クラウドコンピューティング）を利用することを解禁した。2011 年、東日本大震災では、津波により多くのカルテや患者の個人情報が消失し、バックアップの重要性を認識されるに至ったが、さらなるサイバーセキュリティーレベルの高度化が必要とされ

ているが、その必要性や重要性については、未だに医療従事者には浸透しておらず、電子カルテ PC に自前の USB フラッシュメモリを利用して情報を抜き取ったり、電子カルテの PC で自分のメールを開封し、危険性を認識せずに添付資料を利用することによるコンピュータウイルス感染による被害が後を絶たない。さらに次々と IoT 化した医療機器に対して、対策を講じる必要性についてはあまり認識されていないまま、医療現場におけるクラウド化や IoT 化が進んでいるのが現状である。

クラウド化に関するガイドラインの問題：

医療分野においてクラウドサービスの活用が進みつつある中、ガイドラインは厚生労働省、総務省、経済産業省の 3 省が出していた。この「3 省 4 ガイドライン」は、厚生労働省が「医療情報システムの安全管理に関するガイドライン（2005 年策定、2017 年第 5 版)」、総務省が「ASP/SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン（2009 年策定、2010 年第 1.1 版)」と「ASP/SaaS における情報セキュリティ対策ガイドライン（2008 年策定」、経済産業省が「医療情報を受託管理する情報処理事業者における安全管理ガイドライン（2008 年策定、2012 年第 2 版)」と言われていたが、その内容の違いを明確に分けることは難しく、現場の医療従事者が理解するには非常に困難であった・

そのため、2018 年に総務省の二つのガイドラインを一つに整理し「クラウドサ

ービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」としてまとめ、電子カルテや PHR（Personal Health Record)、オンライン診療等のクラウド活用の位置づけを明確化し、2019 年にさらに経済産業省のガイドラインと統合が試みられ整理を行うことで、「経済産業省・総務省による事業者向けガイドライン」が発行され、医療分野におけるクラウド活用が促進される環境が整備されてきた。

しかし、4 つあったガイドラインをまとめる上で、医療機関や事業者側の負担が軽減されることの検討課題が明確になっておらず、結果的に負担が残存する形となった。さらに厚生労働省のガイドラインが医療機関向け、経済産業省・総務省のガイドラインは事業者向けであるのにも関わらず、両方を参照しなければガイドラインを遵守することができず、管理者側が負うべき義務と、受託事業者側が負うべき義務が対応関係を明らかにする必要があり、2 つのガイドラインの統合が求められていた。

2020 年 8 月に国内で医療情報を電子的に取り扱う際に遵守が求められる 3 省 3 ガイドラインのうち、医療情報システム・サービスを提供する事業者向けの 2 つのガイドライン（経済産業省：「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」、及び総務省：「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」）が、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（以下、『統合ガイドライ

ン』）という一つのガイドラインに改定され、そのドラフト版（「案」）が現在公開されている。

　今後は、さらに統合されたガイドライン作成を進めなければならないが、内容に対して長文ではなく箇条書きにしたり、何をすべきか明確にするなどの改善も必要である。さらにサイバー攻撃時の対応について、所管省庁への連絡などが記載されているが、具体的な例や相談などできる環境は乏しく、事前の必要なサイバーセキュリティ環境の構築とアップデート、そして攻撃発生時のネットワークの切断など具体的対応の情報処理の観点からの記載が乏しいため、これらの改善も必要とされている。

3．医療環境における2つのサイバーセキュリティの型とその関係

クラウド型とオンプレ型のそれぞれのセキュリティ：

今まで多くの医療機関において活用されていたのは、オンプレ型と言われる医療機関自らがサーバを保有し、管理する形が主流であった。理由は当初にクラウド型電子カルテが存在しなかったことと、個人情報がインターネットを通じて外部で保存するという事に対して、情報の外部流出するのではという考えが大きく、またネットにつなぐことに対するサイバー攻撃によるリスクが高くなるという危機感があった。しかし、レセプトオンラインの義務化によりインターネット接続環境が当たり前になると、医療機関で情報をサイバー攻撃から守るためには、大きな負担が発生することが分かっており、また情報漏えいや改ざんなどについてのリスクも、インターネットにつながないオンプレ型は、サーバテロなどのネットワーク上の脅威にさらされることは少ないが、IoT 化により知らない間につながっているリスクが高くなってきていることや、関係者や外部の侵入者による持ち出し、故意の書き換えなどのリスクがより高くなってきており、物理的な対策も講じる必要が生じてきた。

一方、インターネットにつなぐクラウド型のサーバは、ユーザーの ID／アクセス権限管理、通信や保存データの暗号化などサーバテロへの脅威に対する対策を企業側が厳格に行う必要があるが、企業がサーバを管理するクラウド型の方が厳格な

運用を求められているため、より安全であるという認識が高まってきている。以下に、医療情報システムの安全管理に関するガイドライン（第５版）「8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準　C. 最低限のガイドライン」を添付する（表１）。

	医療機関のサーバで管理する場合	企業のサーバで管理する場合
（ア）	病院や診療所の内部で診療録等を保存すること。	医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保 存した情報の取扱いに対して監督を行えること。
（イ）	保存を受託した診療録等を委託した病院、診療所や患者の許可なく分析等を目的として取り扱わないこと。	医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「 6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること。
（ウ）	病院、診療所等であっても、保存を受託した診療録等について分析等を行う場合は、委託した病院、診療所及び患者の同意を得た上で、不当な営利、利益を目的としない場合に限ること。	受託事業者が民間事業者等に課せられた経済産業省のガイドラインや総務省のガイドライン等を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。
（エ）	匿名化された情報を取り扱う場合においても、匿名化の妥当性の検証を検証組織で検討することや、取扱いをしている事実を患者等に掲示等を使って知らせる等、個人情報の保護に配慮した上で実施すること。	保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。
（オ）	情報を保存している機関に患者がアクセスし、自らの記録を閲覧するような仕組みを提供する場合は、情報の保存を受託した病院、診療所は適切なアクセス権を規定し、情報漏えいや、誤った閲覧が起こらないように配慮すること。	外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること。
（カ）	情報の提供は、原則、患者が受診している医療機関等と患者間の同意で実施されること。	保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、誤った閲覧が起こらないようにさせること。
（キ）		医療機関等において（ア）から（カ）を満たした上で、外部保存を受託する事業者の選定基準を定めること。少なくとも以下の 4 点に つい

		て確認すること。 （a） 医療情報等の安全管理に係る基本方針・取扱規程等の整備 （b） 医療情報等の安全管理に係る実施体制の整備 （c） 実績等に基づく個人データ安全管理に関する信用度 （d）財務諸表等に基づく経営の健全性

表１：医療情報システムの安全管理に関するガイドライン（第５版）「8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準　C. 最低限のガイドライン」

４．医療機器の IoT 化によるサイバー攻撃のリスク

医療機器の IoT 化

近年、病院などの医療機関に対するサイバー攻撃が増加している。一般的にウイルス対策ソフトなどで守られているパソコンと異なり、IoT 医療機器には十分なセキュリティ対策が施されていないのが現状でアップデートもままならず、また IoT 医療機器の多くが共通のプロトコルや OS を利用していない。スマートフォンの OS(Android や iOS など)を活用した小型医療機器やセンサが数多く開発されているが、これらの特徴は小型医療機器として機能するだけでなく、インターネット接続し、より便利な活用が盛んに行われてきている。例えば、体に付けたセンサなどから生体データや環境データを取得し、ビックデータとして活用する医療・ヘルスケアサービスも提供されている。特に Bluetooth などが代表される、体に付けたセンサなどの体表や体内から 10 メートル程度の通信範囲で携帯端末との間で構成される短距離無線ネットワーク（Body Area Network, BAN）は、生活習慣病予防のためのモニタリングや在宅ケアに向けた見守りシステムとして導入が進んでいる。

そのため、IoT のセキュリティを高めるために、PC ハードウェア耐タンパ性[注 1]を持つトラステッド・ プラットフォーム・モジュール（Trusted Platform Module, TPM）セキュリティチップが、コンピューター環境の信頼性を高めるモジュールとして開発された（注 1：機器や装置、ソフトウェアなどが、外部から内

部構造や記録されたデータなどを解析、読み取り、改竄されにくいようになっている状態のこと)。

RSA 暗号演算・鍵生成・鍵格納，SHA-1 ハッシュ計算とそのハッシュ値保存，乱数生成，単純増加カウンタ，オーナ権委任，不揮発性ストレージ保存の機能から成っている。組込み機器のセキュリティ機能を詰めていくにあたってはディペンダビリティ[注2]の視点が必要で、TPM を策定した Trusted Computing Group（TCG）の出したガイダンス TCG Guidance for Securing IoT があり、IoT 機器そのものが持たなければならないセキュリティ要件として以下をリストアップしている（注2：一般的な信頼性にとどまらず、たとえ一部が壊れても残りの部分でうまく働くといった自立的自己修復的な動作をさす概念である。大規模集積回路、コンピューターシステムなどで使われる言葉)。

（１）デバイスアイデンティティの確保と保護（Establishing and Protecting Device Identity）

（２）マルウェア感染からの防御（Protection Against Malware Infection）

（３）ハードウェア改ざんからの保護（Protecting Against Hardware Tampering）

（４）平常時での機密性，整合性，可用性（Confidentiality, Integrity, and Availability of Data at Rest）

（５）デバイスの転売あるいは廃棄（Reselling or Decommissioning a

Device）

（ 6 ）暗号プロトコルの採用（Meeting Cryptographic Protocol Requirements）

（ 7 ）プロビジョニング[注 3]の複数モデルサポート （Supporting Multiple Models of Provisioning）

（ 8 ）監査ログの維持（Maintaining Audit Logs），リモートメンテナンス（Remote Manageability）

（ 9 ）レガシーハードウェアのセキュリティ保護 （Securing Legacy Hardware）

（注 3：事前の準備のことだが、IT 業界では顧客に対する技術やサービスの提供）

そのため、サービスを受ける際のなりすまし不正や、不正 IoT 機器からの IoT サービスアクセスを防ぐ必要があり、IoT 機器と IoT サービス間において相互認証を実現する事が重要である（MBAN 搭載医療機器では，時々刻々変化する暗号キー生成方式を採用しており相互認証方式となる）。

また大きな課題として、IoT 機器自体へのマルウェア感染があげられる。IoT 機器の数は非常に多く，事前にマルウェアに感染しないようにするためのシステムを最初から考慮する必要があり、更に定期的で最新のセキュアなバージョンをアップデートする必要がある。

しかしながら、サイバー攻撃を受ける可能性がある OS で機動するシステムが患者情報を扱いつつネットワーク環境に対して接続された場合、サイバー攻撃などにより予期しない事が発生する可能性が高く、実際に IoT 化した小型医療機器のデータを改ざんが可能なことが証明されている。また、膨大な数によって構成される医療現場の医療機器がすべて IoT 化されれば、さらにネットワークに接続された IoT 医療機器の全体構成を把握するのが困難である。

実際、2013 年に米国食品医薬品局（FDA）が、医療機器や病院内ネットワークに関連する脆弱性からサイバー攻撃の標的になる可能性のある事例を挙げ、医療機器メーカーに対して、機器セキュリティを強化の通達を出した。日本でも医療機器は他の組込み機器と同様、小型化、携帯化が進んでおり一部の医療機器にも Bluetooth を中心とした短距離無線通信機能が搭載されているため、他の ICT 化された組込み機器で発生したセキュリティの脅威が医療機器上で顕在化する可能性がある。情報処理推進機構（IPA）は「医療機器における情報セキュリティに関する調査（2013 年度)」報告書 3）を出した。病院内で利用される医療機器については、今までの閉じたネットワークから汎用技術を用いた高機能化がさらに進む事から、リモートメンテナンス用ネットワークに接続され、さらには医療データの共有のために携帯端末の利用が加速していき、そのリスクはさらに顕著化することが予想されている。

IoT 医療機器のサイバーセキュリティ対策

近年、病院などの医療機関に対するサイバー攻撃が増加している。一般的にウイルス対策ソフトなどで守られているパソコンへの脅威も大きいが、特に今後増加するであろう IoT 医療機器には十分なセキュリティ対策が施されていないのが現状である。異なるメーカーの IoT 医療機器、違う型番、OS の違いや OS は同じだがバージョンが違うと機能も動作環境も異なることが多く、大きな課題となっている。さらに数が多い場合や、意外なところで使用されているなどして、病院の情報システム管理者ですら把握出来なくなるという問題があり、ネットワークに接続された IoT 医療機器の全体構成を把握するのが困難を極める。

5．　医療サイバーインシデントの現状

原因別から考察する、実際の医療機関のセキュリティインシデント事例

［事例 1：内部要因／PC の盗難・紛失に起因するインシデント］

2015 年 11 月 24 日、保健福祉省（HHS)の公民権室（OCR：Office of Civil Rights）は、マサチューセッツ州のレイヒ病院・医療センター（タフツ大学付属病院の 1 つ）で発覚した暗号化されていないラップトップ PC の盗難による患者情報漏えいに関連して、85 万米ドル（約 9 千万円相当）の制裁金を支払うことで和解したと発表した。

レイヒ病院・医療センターでは、ポータブル CT スキャナーから医用画像を取り込み、医用画像保存通信システム（PACS）に保存するためにラップトップ PC を利用していた。2011 年 8 月 11 日深夜、暗号化されていないラップトップ PC が盗難に遭い、患者の電子保護対象保健情報（ePHI）599 件を紛失したことが発覚した。

その後の OCR の調査により、以下のような点について不備があったことが判明している。

・すべての ePHI について、リスク分析を実施していなかった

・ePHI にアクセスしたワークステーションを物理的に保護していなかった

・診断／検査機器に接続して利用していたワークステーション上で維持していた ePHI の保護に関連するポリシーおよび手順を導入・維持していなかった

・このインシデントで問題となったワークステーションに関連して、ユーザー識別子を特定・追跡するための固有ユーザー名が欠如していた

・このインシデントで問題となったワークステーションにおける活動を記録・検証した手順を導入していなかった

・個人 599 件分の ePHI の許容できない開示

レイヒ病院・医療センターは、85 万米ドルの制裁金を支払うと同時に、包括的な組織全体のリスク分析を OCR に提供してリスクマネジメント計画に対応し、また特定のイベントを報告して法令遵守に関する証拠を提供することによって、医療保険の携帯性と責任に関する法律（HIPAA）の規則を遵守していなかった履歴を提出することを受け入れている。

なお、HIPAA の侵害通知規則では、500 人以上に影響を与える保護対象保健情報（PHI）侵害の場合、適用主体は原則として発見後 60 日内に保健福祉省（HHS）まで報告する義務がある。

出典：U.S. Department of Health & Human Services: HIPAA Settlement Reinforces Lessons for Users of Medical Devices, November 24, 2015(https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/lahey.html)

[事例 2：内部要因／PC とハードディスクドライブの盗難・紛失に起因するインシデン

ト］

2019 年 11 月 5 日、米国保健福祉省（HHS)の公民権室（OCR)は、ニューヨーク州のロチェスター大学医療センター（URMC)で発覚した暗号化されていないハードウェアの紛失・盗難による患者情報漏えいに関連して、300 万米ドル（約 3 億 2 千万円相当）の制裁金を支払うことで和解したと発表した。

URMC は、2013 年および 2017 年、暗号化されていないフラッシュドライブの紛失および暗号化されていないラップトップ PC の盗難により、保護対象保健情報（PHI)が許容範囲を越えたレベルの状態で公開されていたというインシデントを OCR に報告していた。

その後 OCR は URMC に対する調査を実施し、HIPAA のプライバシー・セキュリティ規則の要求事項のうち、以下の点について不備があることを指摘した。

・組織全体のリスク分析の実施

・相当の適切なレベルまでリスクおよび脆弱性を低減するのに十分なセキュリティ対策の導入

・デバイスおよび媒体に対するコントロールの有効活用

・相当の適切な措置が必要な場合における、保護対象電子保健情報（ePHI）を暗号化・復号するメカニズムの導入

上記のインシデントとは別に、OCR は、2010 年、暗号化されていないフラッシュドライブの紛失に起因するインシデントに関連して URMC を調査し、技術的対策の

支援を行っていた。それにも関わらず、暗号化の不備が患者情報に対する高いリスクとなり、暗号化されていないモバイルデバイスの継続的な使用を認めていたことが発覚したことから、今回、URMC に対して、高額の制裁金が課される結果となった。なお URMC は、OCR が HIPAA 遵守状況を 2 年間モニタリングすることを含む是正計画を受け入れている。

出典：U.S. Department of Health & Human Services: Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement, November 5, 2019 (https://www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html)

[事例 3：外部要因／マルウェアを介した不正アクセスに起因するインシデント]

2018 年 2 月 5 日、マサチューセッツ州でブリガム・アンド・ウィメンズ病院、マサチューセッツ総合病院などを運営する非営利法人組織のパートナーズ・ヘルスケアは、マルウェアを介した権限のない第三者による不正アクセスにより、患者の個人情報約 2,600 件分が影響を受けた可能性があることを公表した。

2017 年 5 月 8 日、パートナーズ・ヘルスケアのモニタリングシステムが、疑いのある振る舞いを発見し、直ちにマルウェアを遮断して第三者のフォレンジックコンサルタントに調査を依頼した。パートナーズの調査によると、2017 年 5 月 8 日～17 日の間、影響を受けたコンピューター上でのユーザーの振る舞いにより、マルウェアが

特定のデータへの不正アクセスを引き起こす可能性があったとしている。パートナーズは、影響を受けたコンピューターを特定して、影響拡大を抑制するコンピューターを導入した。

2017 年 7 月 11 日、インシデント発覚後の継続的なレビューにより、データに個人の医療情報が含まれている可能性があることが判明した。その後、2017 年 12 月、手作業によるデータ分析が完了し、名前、サービス日および／または特定の臨床情報（例．手順のタイプ、診断および／または薬物治療）が含まれている可能性があることが判明した。一部の患者については、社会保障番号と金融口座データが含まれていた可能性があることも判明した。

今回のマルウェアは、特にパートナーズ・ヘルスケアの情報を標的として仕掛けられたものではなく、電子カルテシステムへのアクセスは確認されなかったとしている。

出典：Partners HealthCare: Partners HealthCare notifies 2,600 patients of potential privacy issue, February 5, 2018 (https://www.massgeneral.org/news/press-release/partners-healthcare-notifies-2600-patients-of-potential-privacy-issue)

[事例 4：外部要因／フィッシング攻撃メールに起因するインシデント]

2019 年 5 月 13 日、オレゴン保健医療局は、オレゴン州立病院で発覚したデータ侵害に関する通知を行ったことを公表した。オレゴン保健医療局とエンタープライ

ズ・セキュリティオフィス・インシデント対応チームによると、同月 6 日、規制対象情報の侵害が発生したことを確認したとしている。

オレゴン州立病院の職員宛に発信されたフィッシング攻撃メールを当該職員が開封して、資格情報が外部に露出したことが、インシデントの発端となったという。危険に晒された電子メールには、患者の保護対象保健情報（PHI）が含まれており、氏名、生年月日、電子カルテ番号、診断、治療計画およびその他の患者治療用に提供された情報が含まれていた可能性があるとしている。

電子メールシステムから患者の個人情報が複製されたり、不適切に利用されたりしたという事実は確認されていなかったものの、外部の第三者が保護対象保健情報にアクセス可能な状態にあったことから、保健医療局側は外部通知に踏み切ったとしている。

出典：Oregon Health Authority: Oregon Health Authority notifies public of data breach at Oregon State Hospital, May 13, 2020 (https://www.oregon.gov/oha/ERD/Pages/OHA-Notify-Public-State-Hospital-Data-Breach.aspx)

以下に、海外におけるサイバーインシデント事例一覧（表２）と、国内におけるサイバーインシデント事例一覧を添付する（表３）。

表２：海外におけるサイバーインシデント事例一覧

タイトル	概要	内容
2020 年 7 月 PHI Compromised in CVS Pharmacy and Walgreens Break-ins	CVS 薬局は、2020 年 5 月 27 日から 6 月 8 日 にかけ複数の事件が発生。個人情報と PHI の一部が失われたことを特定の患者に警告。Walgreens 薬局も同期間に同様のインシデントを報告。	何者かがいくつかの店舗へのアクセスを獲得し、薬局の大量の処方箋をダウンロードした。ワクチン同意書と紙の処方箋も紛失し、事件で盗まれた可能性がある。侵害される情報の種類には、氏名、住所、生年月日、薬剤名、処方者情報、およびプライマリケアプロバイダー情報が含まれる。CVS 薬局は、インシデントを HHS の公民権局に合計で 21,289 人の個人に影響を与えていると報告している。 参照元： https://www.hipaajournal.com/phi-compromised-in-cvs-pharmacy-and-walgreens-break-ins/
2020 年 7 月 Highpoint Foot and Ankle Center Ransomware Attack Impacts 25,554 Patients	ペンシルベニア州ニューブリテンタウンシップの Highpoint Foot and Ankle Center は、2020 年 5 月にランサムウェア攻撃で患者情報が暗号化、流出された可能性。	調査が開始され、外部の何者かがランサムウェアをコンピューターシステムにリモートでインストールしたことが判明した。コンピューター科学捜査会社が調査を実施、25,554 人の患者の保護された健康情報を含むファイルが侵害された可能性があることが判明。氏名、住所、生年月日、社会保障番号、診断、治療情報、およびリリース状態がファイルに含まれていた。影響を受けたすべての患者にはメールで通知される。 参照元： https://www.hipaajournal.com/university-of-utah-reports-phishing-attack-involving-the-phi-of-up-to-10000-patients/
2020 年 7 月 National Cardiovascular Partners Email Hack Impacts 78K Patients	National Cardiovascular Partners（NCP）は、従業員の電子メールアカウントへのアクセス権を奪われ 78,070 人の患者データが侵害された可能性があることを通知した。	NCP は最初に 5 月 19 日にアカウントの不正を確認した。 外部のサイバーセキュリティ会社によって行われた調査の結果、侵害されたデータには、氏名、連絡先情報、および患者ごとに異なる多数の機密データを含む患者情報が含まれていることが判明。NCP は、インシデント再発を防止するために従業員に電子メールでのセキュリティ訓練を実施している。 参照元： https://healthitsecurity.com/news/national-cardiovascular-partners-email-hack-impacts-78k-patients

2020 年 5 月 Snake Ransomware hits Europe's largest private hospital operator Fresenius during COVID-19 outbreak	ヨーロッパ最大の民間病院事業者 Fresenius が Snake Ransamware による攻撃を受ける。 下記が脅迫文。 “ As noted by MalwareHunterTeam, the ransom note named 'Decrypt-Your-Files.txt' from this week's attacks, the Snake operators have added text stating that they will publish stolen databases and document if not paid within 48 hours. “	ヨーロッパ最大の民間病院事業者であり、COVID-19 の流行により需要が非常に高い透析製品およびサービスの主要プロバイダーであるフレゼニウスは、そのテクノロジーシステムに対するランサムウェアサイバー攻撃の被害を受けた。 これはフレゼニウスが被った最初のランサムウェア攻撃ではなく、同社はすでに 150 万ドルを支払って、以前のランサムウェア感染後に業務を再開した。 スネークランサムウェアのオペレーターも、他のオペレーターと同様に、感染したシステムを暗号化する前に暗号化されていないファイルを盗み、被害者が身代金を支払わないとデータを解放すると脅迫された 参照元： https://securityaffairs.co/wordpress/102878/cyber-crime/snake-ransomware-healthcare.html
2020 年 7 月 National Cardiovascular Partners Email Hack Impacts 78K Patients	メリーランド州エリコットシティに本拠を置くロリアンヘルスサービスは 9 つの生活支援施設を運営しており、2020 年 6 月 6 日にランサムウェア攻撃の犠牲になったと発表した。	6 月 10 日、調査担当者は、攻撃者が居住者の氏名、住所、生年月日、診断、治療情報、社会保障番号、および一部の従業員情報を含むファイルにアクセスし、一部のデータが盗まれたことを確認した。 Netwalker ランサムウェアによる攻撃で、Lorien Health Services が身代金の支払いを拒否すると、盗まれたデータのサンプルがオンラインで公開された。 Lorien Health はインシデントを FBI に報告し、調査中。 保健福祉省に提出された違反レポートは、侵害されたシステムに 47,754 人の保護された健康情報が含まれていたことを示している。 これらの個人には、無料の信用監視および個人情報盗難防止サービスが提供されている。 通知レターは、攻撃の 10 日後、2020 年 6 月 16 日には、影響を受けたすべての個人に送信された。 参照元： https://healthitsecurity.com/news/national-cardiovascular-partners-email-hack-impacts-78k-patients

2020 年 5 月 Quantum Imaging and Therapeutic Associates Investigating Possible Facebook HIPAA Breach	患者の同意なしにソーシャルメディアネットワークで医療画像を共有、患者のプライバシーと HIPAA 違反の疑いがある。	Quantum は Facebook に声明を発表し、プライバシー侵害についての報告を受け取ったことを確認し、「Quantum は患者のプライバシーを尊重することを約束し、これらの報告に深く落胆している」と伝えた。この問題はフェアビュータウンシップの警察に報告され、調査が開始されましたが、現時点で当事者は逮捕されていない。 何千人もの人々が画像を閲覧できると、複数のコメントが Facebook に認めた。 参照元： https://www.hipaajournal.com/quantum-imaging-and-therapeutic-associates-investigating-possible-facebook-hipaa-breach/
2020 年 5 月 Mille Lacs Health System Phishing Attack Impacts 10,600 Patients	Mille Lacs Health System は、フィッシング攻撃を受け 10,000 人を超える患者情報の漏えいの可能性。一部の従業員には、不正な Web サイトに誘導するフィッシングメールが送信された。	2019 年 11 月、フィッシング攻撃を確認、調査を開始。2019 年 8 月 26 日から 2020 年 1 月 7 日の間に、盗まれた電子メール認証情報による不正アクセスが確認された。 攻撃者がアクセスした情報は、姓名、住所、生年月日、提供者名、勤務日、臨床情報、治療情報、手順の種類、特定の個人の場合は社会保障番号など。全電子メールアカウントに対してパスワードの初期化が実行され、セキュリティ強化のための追加対策が実装された。 参照元：https://www.hipaajournal.com/mille-lacs-health-system-phishing-attack-impacts-10600-pati
2020 年 5 月 Geisinger Wyoming Valley Medical Center and District Medical Group Disclose Data Breaches	アリゾナ州で統合医療サービスを提供するアリゾナメディカルグループは、保護されている健康情報の一部が侵害されている可能性があることを 10,190 人の患者に報告した。	違反したアカウントの電子メールと添付ファイルの分析により、名前、医療記録番号、医療情報、健康保険情報などの患者情報が含まれていることが判明。また、限られた数の社会保障番号も侵害された可能性がある。不正アクセスを防止するためにすぐにパスワードの初期化が行わた。調査の結果、2020 年 2 月 4 日から 2 月 10 日までの間で複数の電子メールアカウントが侵害されたことが判明。アリゾナメディカルグループは従業員教育と追加のセキュリティ対策を講じた。 参照元： https://www.hipaajournal.com/geisinger-wyoming-valley-medical-center-and-district-medical-group-disclose-data-breaches/

表３：国内におけるサイバーインシデント事例一覧

（医療機関等におけるマルウェア感染、情報漏えい）

事案	概要
宛先設定ミスで誤送信、医療機関のメールアドレス41件が流出｜大阪府	大阪府は 2020 年 6 月 18 日、府の感染症対策課が府内にある各医療機関に宛てた電子メールにて誤送信が発生し、府内の医療機関のメールアドレス 41 件（個人が識別できるアドレス 28 件）が流出したと明らかになった。
新型コロナ感染者 2 名の電子カルテを職員が不正閲覧｜鳥取県立中央病院	鳥取市に位置する鳥取県立中央病院は 2020 年 6 月 9 日、新型コロナウイルスに感染し入院していた患者ら 2 名の電子カルテデータについて、内部関係者による不正な閲覧が確認されたと明らかになった。
メール誤送信で個人情報含む名簿を別の企業に流出｜岩手県予防医学協会	健康診断などを手掛ける公益財団法人・岩手県予防医学協会は 2020 年 5 月 25 日、協会内でメール誤送信が発生し、本来受診予定であった企業受診者 29 名の個人情報データを別の企業宛てに送信したと明らかにした。
職員が入院患者 101 名の個人情報記録した USB メモリを紛失 - 広島市立病院機構	地方独立行政法人・広島市立病院機構は 2020 年 5 月 1 日、機構が保有する入院患者の個人情報 101 名の氏名や年齢、処方箋等の診療情報を記録した USB を外部に持ち出した上に紛失し、流出の可能性が発生している現状と明らかにした。
2017 年 3 月、岡山大学病院医療用端末のウイルス感染	医療用端末 2 台がウイルスに感染し、外部と不正な通信を行っていたことが判明した。
2018 年 10 月、宇陀市立病院が GrandCrab に感染	医療情報システムの中核である、電子 カルテシステムがウイルスに感染、電子カルテシステムの利用が不可能となる。 システムデータが暗号化されたこともあり、電子カルテシステム他影響のあったシステムの再構築を実施。電子カルテシステムは丸二日間全面停止となった。
2019 年 5 月、多摩北部医療センターへの不正アクセス、医師の端末がマルウェア「Emotet」の亜種に感染	職務用パソコン端末へ送信されたメールの添付ファイルを当該職員が開封した結果、ウイルスに感染したことが判明した。
2019 年 5 月、佐世保共済病院がマルウェアに感染	放射線検査機器を接続した PC でウイルスを検知。電子カルテシステムのパソコンへも感染が確認された。 被害の拡大を防ぐため、ネットワークを遮断対応した。
某年、某病院にてマルウェアに感染	院内 PC がランサムウェアに感染し、MRI などの放射線関連医療機器などが停止したが、侵襲性のある医療機器事故であったが、法令に基づいたフォレンジック（証拠保全）や NDA（秘密保持契約；Non-disclosure agreement）の観点から、届け出や情報提供がなかった。

６．　今後の対策

医療機関に対するサイバー攻撃の状況とサイバーセキュリティの問題点；最近の状況からの考察

VERINT が発表したデータでは（Changes in the Threat Landscape under the Global Influence of COVID 19 ；　https://cis.verint.com/resources/changes-in-the-threat-landscape-under-the-global-influence-of-covid-19/)、今年に入り新型コロナウイルス感染症拡大による混乱に乗じてサイバー攻撃は悪化の一途を辿っており（図１）、COVID-19 で被害が大きければ大きいほど、サイバー攻撃をされている（図２）。

特に注目すべきは医療機関の混乱に乗じ、医療機関へのサイバー・インシデントの状況は更に悪化し（図３）、特に海外ではメールを使ったフィッシングや標的型攻撃といったランサムウェアなどによるファイルやシステムの機能不全で、診療業務の一部が停止するような状況が発生している。日本では、この混乱に乗じた内部不正、不注意・ミスによる情報紛失・メール誤送信などが多くみられ、いずれにしても攻撃者は COVID-19 パンデミック を活用し、普段以上の攻撃を仕掛けているのが現状である。

このように、常に世界情勢と混乱にあわせて、変化しつつ攻撃内容と攻撃対象を拡大していくため、対応する側も柔軟かつ迅速な対応が求められている。

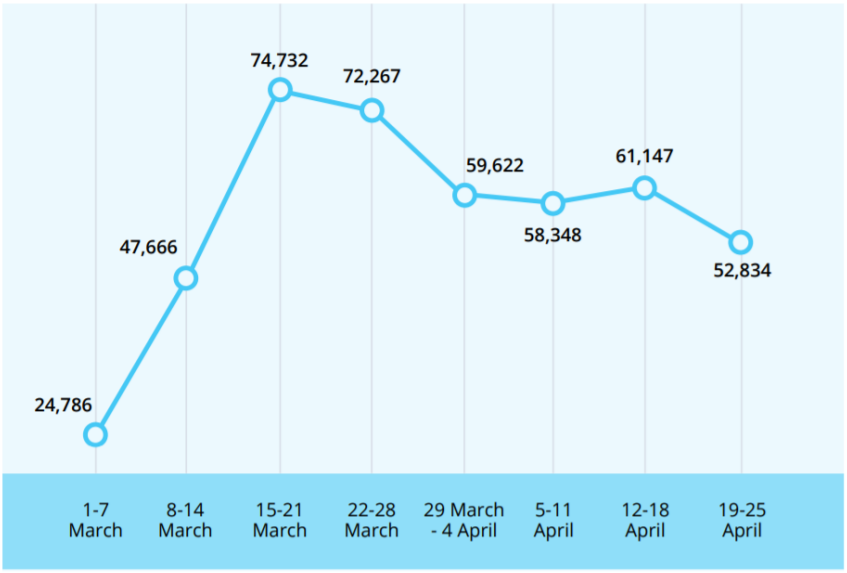

図１：新型コロナウイルス関連のダークウェーブ活動推移

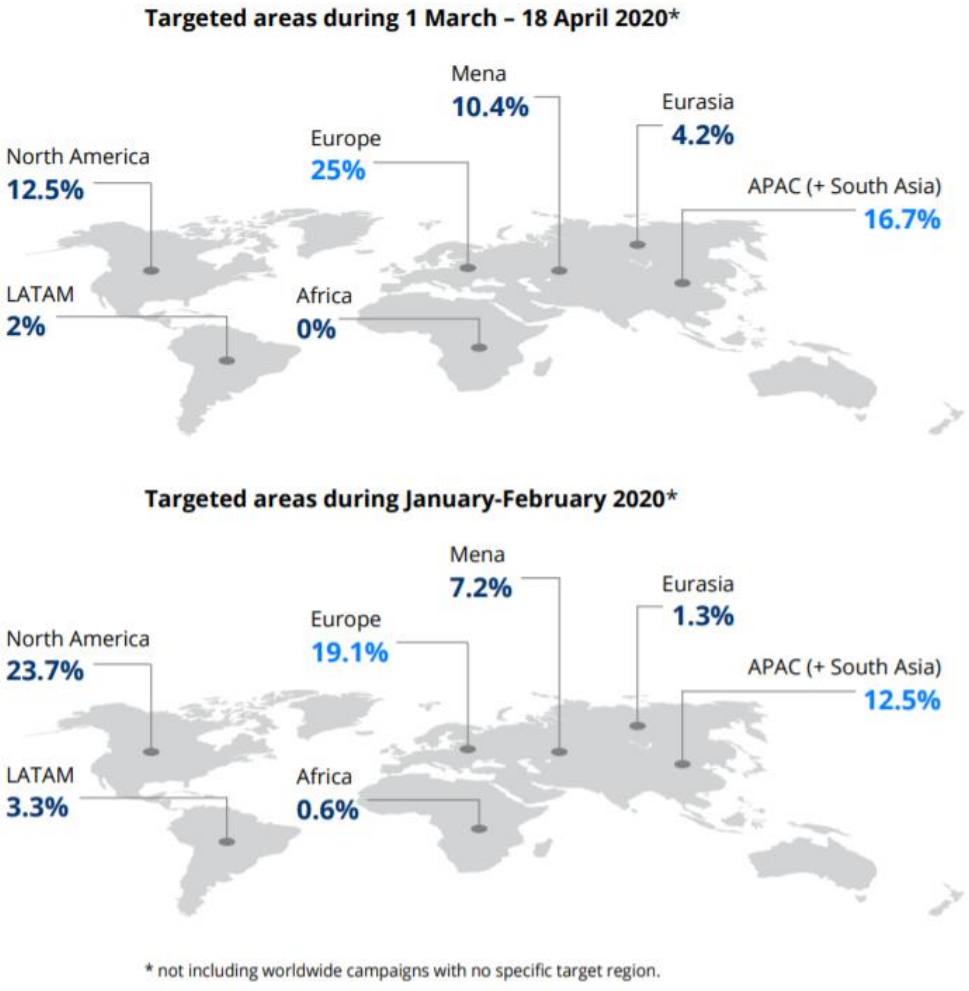

図２：新型コロナウイルス被害が大きければ大きいほど、サイバー攻撃をされる

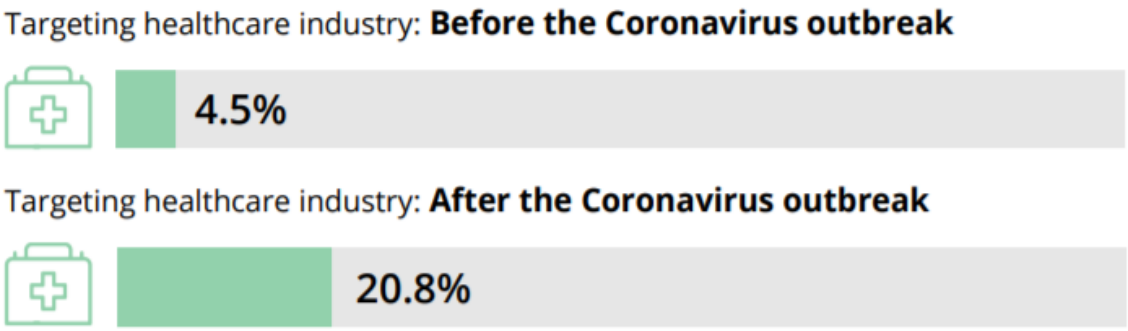

図３：医療業界へのサイバー攻撃　コロナアウトブレーク後に急激に増加

医療機関に対するサイバー攻撃の状況とサイバーセキュリティの問題点；最近の状況からの考察

医療サイバーセキュリティに関する情報を大別すると、脅威情報（例．COVID-19 を契機とする世界レベルでの大規模サイバー攻撃)、脆弱性情報（例．保存データの暗号化に関わるソフトウェア機能の不具合)、インシデント情報（例．データ漏えい発見時の規制当局や患者への通知）がある。今後は、脅威、脆弱性、インシデントに関する情報を継続的に収集・分析して、臨床現場の具体的なアクションを支援する組織／職域横断的な情報管理の仕組みづくりと役割分担が求められる。その上で、サイバーセキュリティ対策は、現状把握、リスク分析、対策方針・優先順位付け、対策実施のステップで行うが、災害訓練と同様にサイバーセキュリティ対策の訓練も企画しつつ、病院全体でそのリスクに対して危機意識を芽生えさせる必要があり、その必要性は急務となっている。

実際問題として、サイバーセキュリティ対策の基本である「現状把握」が医療現場においては十分に実施されておらず、攻撃側からすると非常に攻撃しやすい状況が続いており、本来ならば COVID-19 対応の前に対策すべき課題であったことは否めない。

医療従事者自身の IT リテラシーの欠如により、電子カルテなど院内ネットワークがインターネットに接続されていないから安心している事が多いが、サイバー攻撃はネットワーク経由だけでなく、USB メモリ、医療機器メーカーのメンテナンス用ネットワークおよび作業用 PC など様々存在し、その先には資産管理などのセキュリティ対策ですら、手が回らない状況が続いている。

理由としてはその問題の 1 つには、病院のネットワークシステム全体が把握できていない状況があり、医療機器に関するサイバーセキュリティは医療機器メーカーが対応しているのではという認識があり、病院側が率先してセキュリティ対策をする必要がないという認識である。

IMDRF（国際医療機器規制当局フォーラム；International Medical Device Regulators Forum）でのガイダンスのリリースと 3 年後の国内導入に向け、厚生労働省は医療機器メーカーの医療機器サイバーセキュリティに対する意識向上をより強く意識しているが、現場との乖離は否定できない。

現在、厚生労働省と経済産業省では、医療現場におけるインターネットやクラウドのさらなる利活用をめざし、その先には「医療の質向上」と「効率化」をめざしているが、現在ある病院で決められた規則では、医療関連データをクラウドに上げられない、イン

ターネットに接続できないなどの弊害も起きてきている。

　さらに多くの医療施設において、診療ネットワークはクローズドでサイバー攻撃を受けないことが前提となっているような、インターネットにつないでいなければ安心という誤った認識のため、Firewall や IDS など不正や異常の防御・検知システムはほとんど導入されていないのも原因である。

医療機関に対するサイバー攻撃の状況とサイバーセキュリティの問題点；歴史と新たな試み

サイバーセキュリティ業界における医療機器セキュリティの歴史は、医療機器にネットワーク技術が組み込まれ始めた頃から、医療機器セキュリティは業界でも長く注目を浴びてきたが、医療従事者がそのことに興味を持っていないことが多い事や、対策の必要性を認識できなかったところから始める必要がある。その理由の１つとして日本では医師が経営者の場合が多く、そこまで認識する時間的な余裕がないことも原因があると思われる。

歴史的には、心臓ペースメーカーの最初の脆弱性の発表が 2008 年のＩＥＥＥシンポジウムでのミシガン大学の研究者グループによる発表がある。心臓ペースメーカーは患者に個別にカスタマイズが必要なデバイスだが、近接な距離ではあるが、ワイヤレスでペースメーカーの再プログラミングを可能にする仕様が脆弱性に繋がってしまった（Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, https://ieeexplore.ieee.org/document/4531149?arnumber=4531149)。

日本においても、非政府機関における医療セキュリティの企画も進んでいる。例えば 2012 年から 2017 年にかけて日本でもハッカソンと呼ばれる、ソフトウェア開発分野のプログラマやグラフィックデザイナー、ユーザインタフェース設計者、プロジェクトマネージャらが集中的に作業をするソフトウェア関連プロジェクトのイベント

で、すでに医療版のハッカソンを開催して実績を作っている（https://www.fukushimahackathon.jp/event.html；株式会社 Eyes, JAPAN）。そこで優勝した日本のチームは、2012 年にシリコンバレーHealth2.0 医療ハッカソンで 7 位、2013 年には優勝をしている。その 5 年の間に、日医標準レセプトソフトウェア ORCA や、アメリカの退役軍人病院で使われているソフト群、ヨーロッパで使われている院内システム、またソフトウェアだけではなく PCR や分注ロボットなど IoT デバイス、医療機器、そして今後医療サービスに広く使われていくであろうブロックチェーン（分散化台帳システム）や AI の脆弱性を発見している。しかしながら、まだ医療機器メーカーは自社の製品の脆弱性の公開に対して、その方法とタイミングなどの経験が不十分であり、その支援とシステムの構築は急務と思われる。

また、2013 年の Black Hat USA というハッカーカンファレンス（Black Hat USA 2012, IMPLANTABLE MEDICAL DEVICES: HACKING HUMANS　https://www.blackhat.com/us-13/briefings.html#Jack）の Barnaby Jack 氏の発表では、約 15m 離れた距離からでも心臓ペースメーカーへの攻撃を可能にする脆弱性の報告であった。これ以前にも彼は組み込みデバイスセキュリティの研究の中で、インスリンポンプの脆弱性にも言及し、その脆弱性によって患者を命の危険に晒しているため、医療機器メーカーやＦＤＡにもっとセキュリティ対策に目を向けるよう訴えている。実際にメーカーは講演後に次のバージョンで修正している。（2012 年, McAfee's Barnaby Sees Hacking Risk for Medical Devices, https://www.youtube.com/watch?v=

YJ8PZeRwweA, Hacker shows off vulnerabilities of wireless insulin pumps, https://medcitynews.com/2012/03/hacker-shows-off-vulnerabilities-of-wireless-insulin-pumps/)。

その後も、医療機器に関するセキュリティの報告は続いており、セキュリティ業界、医療業界の有志で、医療機器セキュリティの向上に向けた対策を検討し続けている。その流れで米国の Def Con という数万人規模のセキュリティ関係者が集まるカンファレンスで、Medical Device Village というコミュニティが生まれている。

2016 年には米国政府が、デジタルミレニアム著作権法（ＤＭＣＡ）において医療機器を含む IoT デバイスを適用外にすると発表した事で、セキュリティ研究者は一定の条件下での合法的な研究が認められることとなり、医療機器セキュリティは大きな動きとなった。

結果として、前述した Medical Device Village の主催者は、ＦＤＡ や、医療機器メーカーやセキュリティ専門家達の協力を得て、2019 年カリフォルニア州立工科大学の協力の下、Def Con 会場の約 242 平方メートルの部屋に病院を再現した（https://wired.jp/2019/09/09/defcon-medical-device-village/)。

消極的だったＦＤＡがサイバーセキュリティを強く打ち出すようになり、今では市場にある医療機器の監視の一環として自らサイバーセキュリティ問題の報告を奨励している（https://www.fda.gov/medical-devices/digital-health/cybersecurity)。

日本では、2013 年からＣＯＤＥ　ＢＬＵＥのカンファレンスという最先端のサイバー

セキュリティ動向を伝える企画があり、実際に国内外のセキュリティ専門家約 1000 人が集まっている。特に 2015 年、ドイツのセキュリティアナリストの Florian Grunow 氏による医療機器のセキュリティの講演では、医療セキュリティの問題として、様々な医療機器への攻撃が可能であることを証明する動画で示し、医療機器メーカーの脆弱性対策の不備を示しつつ、ドイツでは病院と連携して研究を進めていることを発表した。日本でもドイツのような、病院の医療機器のセキュリティテストを無料で提供する代わりに、病院は彼に研究結果を医療機器メーカーに相談するか、あるいは公開するような企画を進める必要があると考える（https://codeblue.jp/2015/result/#speaker-florian https://codeblue.jp/2015/en/result/#speaker-florian）。

また、2019 年には SOMPO リスクマネジメント株式会社が協賛企業としてイスラエルの企業 MEDIGATE CORPORATION と協力し、医療機器セキュリティのワークショップが開催された。ここでは実際に、血糖値の測定とモニタリングを行う医療機器へのリモートからの攻撃デモを含むワークショップを提供した（ https://codeblue.jp/2019/contests/workshop_01/ ）（ https://www.tv-tokyo.co.jp/news/original/2019/10/30/007065.html）。

企業も対策が必要であるが、セキュリティコミュニティと協調してセキュリティを向上させる取り組みは各メーカーにも広がっており、外部からの脆弱性報告を受け付ける窓口を設け、どのような報告にも対応できるように脆弱性ハンドリングの体制を構築しつつある。下記の Bugcrowd が運営するバグバウンティのリストには、企業の脆弱勢報

告窓口がリストされており、中にはトヨタやパナソニック等も含まれており、日本企業も脆弱性の報告受付を積極的に打ち出していることがわかる（https://www.bugcrowd.com/bug-bounty-list/）。

しかしながら、医療機器は動作不良により患者の安全に影響し健康被害を生じさせるため、「可用性」や「完全性」が「機密性」よりも優先され、一般業務系のシステムと比較して、医療機器はセキュリティ対策が容易ではないといわれている。

しかし、2020 年 3 月 IMDRF による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、我が国においても 2020 年 5 月 厚生労働省が IMDRF を 3 年後に国内導入を発表された。医療機器製造業者、ヘルスケアプロバイダ、規制当局、脆弱性発見者の共同責任が明記されているが、医療機関によっては数千台規模の医療機器、IoT 機器があるため、その状況把握は困難を極める。そのため、診療ネットワークや稼働中の医療機器に影響を与えず、自動的に医療機器の情報を収集し現状把握を行う必要がある。

また、総務省からも 2020 年 8 月に、医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（案）に対する意見募集の結果及び当該ガイドラインの公表も行われ、ますますその動向に注目しつつ、実装のための方策を講じて現場レベルでの対応が必要となると思われる。

日本医師会の IT 化推進；現場の取り組みと今後の可能性について

日本医師会として、その歴史は 2001 年に日医標準レセプトソフト（ORCA：Online Receipt Computer Advantage）をスタートさせ「日医 IT 化宣言」により、医療現場のＩＴ（情報技術）化を進めるため、土台となるネットワークづくりを行うことを宣言した。先進的な取り組みであった。各医療現場に標準化されたオンライン診療レセプトシステムを導入し、互換性のある医療情報をやりとりできるようにするＯＲＣＡ計画を推進し、日医が開発したプログラムやデータベースはすべて無償で公開された。このように先進的な取り組みを行い、医療現場の事務作業の効率化を図り、コストを軽減させると同時に、誰もが自由に利用できる開放的なネットワークを形成し、国民に高度で良質な医療を提供することをめざし、IT 化医療先進国として機能してきた。

今後は個人情報保護等の課題や診療の質などの問題をクリアーしつつ、厚生労働省が中心となり 2021 年 3 月より、オンライン診療確認等システムが開始され、顔認証付きカードリーダーにより、健康保険証と一体化したマイナンバーの顔写真と本人を認証し、スムーズな診療開始が可能となる。健康保険証と一体化したマイナンバーとオンライン診療確認等システムにより、今までのレセプト情報からどのような治療や処方をしたかという情報や、健康診断の情報も含めて閲覧できるようになる。今までの診療情報を活用できることにより、違う地域や他院の医師であっても、効率的な処方や副作用などの情報にアクセスしやすくなる。また今までの処方が分かるため、災害時にも活用できるようになるなどのメリットがある。

今後はこのように通常の効率的な診療や処方のためにも、新型コロナウイルス感染症の流行や大規模災害に対しても対応可能になるために、日本の医療環境に適した現場優先の IT 化を進める必要がある。

表在化してきたサイバーセキュリティの課題について

2020 年に入りさらに医療におけるサイバーセキュリティ対策の課題が表在化してきた。奈良県宇陀市立病院で、病院のシステムで起こったウイルス感染への事後対応を担当した職員が、その膨大な作業に忙殺され 2 月に自殺し、内部調査は「期限内に対応するよう上司などから指示され多大な神経を使っていた」などの指摘があったが、結果的にサイバー攻撃対応による心身の負担が原因の可能性は否定できず、事前の準備を徹底し現場を守ることが重要と思われた。

また 5 月には新型コロナウイルスの混乱に乗じて、日本医師会ホームページの偽サイトが出現した。そのような中、8 月に富山県警察と公的病院長協議会が、新型コロナウイルスの感染拡大後、医療機関を狙ったサイバー攻撃が海外で多発している状況のため、サイバー犯罪防止に関する協定を締結した。協定によって病院側はセキュリティ対策を強化し攻撃を受けた際の通報体制をつくり、富山県警察は病院と連携した捜査を推進し被害防止に向けた最新情報を病院側に提供することとなった。

今後は医療従事者への積極的なアナウンスや多機関多職種との連携を強化しつつ、目

に見える危機感を向上させるためにも、実攻撃シミュレーションなどを実施し医療従事者や医療関係学生の中からサイバーセキュリティ関連に詳しい有志を全国から募り、医療従事者主体でサイバーセキュリティの必要性を認識できる組織設立などを計画するなど、医療従事者自身が課題提案、課題解決ができる環境整備も急務であると思われる。

現在、必要とされる医療サイバーセキュリティの方向性について、すでに大病院ではありとあらゆるシステムや医療機器や検査機器に網の目のように接続され、巨大なネットワークを形成しており、通常のサイバーセキュリティ対策を行うことは困難である。巨大なネットワークに対して対応できる、医療システムに特化したサイバーセキュリティ対策が必要であり、例えば医療ネットワークで使用される通信プロトコル（ＤＩＣＯＭ[注4]やHL 7[注5]など他多数)、医療現場での業務フロー、医療機器でのデータフローなど医療に特化したところに対しても対応する必要がある。サイバー攻撃は、このような医療に特化した部分を利用して攻撃をしかけてくる可能性があり、今後は医療機関にサイバーセキュリティを提供するベンダー、利用するユーザーおよび医療機器メーカーは、サイバーセキュリティに関して密に情報連携を行う必要がある。

（注4、注5：1987年に米国で規定された、施設間・システム間での臨床情報や管理情報を交換するための標準規約。主にDICOMが医用画像情報の規格であるのに対して、HL7は文字情報を取り扱う。特にHealth Level 7の情報の範囲は広く、患者管理（診療受付、入退転院、紹介、予約等々）、オーダー管理、会計情報、検査結果などがある）

海外では、ヨーロッパでは、欧州連合サイバーセキュリティ庁（ENISA：The European Union Agency for Cybersecurity）や、米国ではアメリカ合衆国保健福祉省（HHS：Department of Health and Human Services）の国家医療 IT 調整室（ONC：The Office of National Coordinator for health Information Technology）などで、医療 IT の監視、監督および教育などを提供している。日本では、厚生労働省、総務省、経済産業省に担当部署が存在しており、現在、その 3 省にまたがっていた 4 つのガイドラインは統一されてきており、さらに対応する部署も統一されてくるものと思われるが、分かりづらい状況が続いている。医療 IT のセキュリティー対策は待ったなしであり、政府機関でも迅速にその対応が可能となる新たなセクターの創設は急務で有り、また民間でも統一した報告フォームと義務を認識しつつ、日本医師会としては政府と民間を調整しつつ、現場の意見を吸い上げて提供、提案していく必要がある。

今後はさらに地域医療連携、ヘルスケアサプライチェーン、医療 IoT 導入の充実がはかられ、より一層の IT・IoT 化の進展により、さらにリスクは広範囲かつ深化していきつつあり、医療を安全で安心した形で、患者に寄り添うデジタル化を推進するためには、医療現場の状況を把握しつつ、日本医師会が責任ある形で政府や民間に提供、提案していく必要があると思われる。

7．情報共有：実際の情報セキュリティ事故について

国立研究開発法人産業技術総合研究所における情報システムへの不正アクセスに関する報告（2018 年 7 月 20 日）

情報セキュリティ事故を体験して

筆者（鎮西清行氏）は国立研究開発法人に所属する研究者である。筆者の所属研究所は、2018 年に不正アクセスを受けていたことが発覚した。執筆時点でも犯人の背景等は明らかになっていない。ここでは、情報セキュリティ事故が起こると、そこで勤務する者がどのような対応を迫られるかの体験記である。医療機関とは異なる事情の元での事案であるが、一旦ことが起こると、どう業務に影響し、どう尾を引くかについて、他山の石としていただければ幸いである。なお、この記事における筆者の体験と個人意見にわたる部分は、所属組織の公式見解ではない。

1. 事案について

事案に関しては研究所の公式の報告書[i]にて詳しく記載されている。それによると、研究所の主たる情報システムであるクラウドサービスを利用するメールシステムと独自に構築した内部システムの双方に順次不正なアクセスが行われ、職員のログイン ID の窃取、パスワード試行攻撃によるパスワード探知、これらを用いた内部システムへの不正侵入、内部システムのサーバの踏み台化、メールシステム及び内部システムの複数の

サーバに保管したファイルの窃取又は閲覧と言った一連の不正行為が行われた。

内部システムへの侵入を防ぐためのファイヤウォールは設置されていたが、侵入者は外側に置かれていた研究用の Web サイトを通じて内部のコンピューターの OS を遠隔操作した。ここを踏み台として管理用ネットワークのサーバを外部から遠隔操作して、他のサーバから職員のアカウント情報等を窃取した。

被害としては、未公表の研究情報、共同研究契約等の情報、個人情報、全職員の氏名所属、一部のメールアカウントのメール、添付文書が外部漏洩又は閲覧された可能性があった。

被害を発生・拡大させた要因として、システム・機器の問題（ログイン方法（多要素認証でなかった)、内部サーバと連携した外部サイト、広域でフラットな内部ネットワーク、内部ネットワークの不十分な監視等)、外部委託の運用、マネジメントの課題が挙げられている。

攻撃は前年の 10 月末から始まっていたが、事案が発覚したのは 2018 年 2 月 6 日、年度末の様々な締め切りの時期であった。

2. 初動対応

2 月 9 日前後に全員の内部システムログイン用のパスワードが強制変更され、また内部の業務システム、メールシステムの大半が停止となった。2 月 13 日に研究所は事案を外部公表し、研究所からのインターネット接続を完全に遮断した。研究所は情報セキュリティ対策本部を設置して、調査等を開始した。

研究現場の筆者が指示を受けたのは、2 月 8 日ごろと記憶する。最初は、「SSH の稼働しているサーバの不審挙動の有無を調べて報告せよ。発見した場合は現状保全のまま至急連絡。」だった。後段は通常は出ない指示であり、普通でない事態が起きたことが予感された。

3. 拡大

すぐに、調査対象にはサーバの姿形をしたものだけでなく、ネットワークにつながるプリンタ、カメラ、無線 LAN、実験機器も含まれることがわかった。対象が一挙に増えた。筆者らは通常業務を止めて調べねばならなかった。全員が IT 技術の専門家ではないので、IT 技術に詳しい者がお助けすることとなった。

その過程で筆者の身の回りからも、ログが残らない機器、ファームウェアが何年も前から更新されていない機器なども次々に見つかった。量販店で入手可能な大手ブランドの機器も少なくなかった。また、DHCP で接続されている機器が多かったことも調査を

難しくした。

調査の結果、3 月上旬までに踏み台となった可能性のあるサーバ、不正なログイン等が発見された。また 2 月下旬には安全が確認できた優先度の高いシステムから再開された。アクセス時間やアクセスを許可する部署の制限が取られていたと記憶する。

4. 収束

3 月下旬には主な内部業務システムが再稼動して、その後は調査結果の解析と再発防止のための調査委員会が設置されて、報告書を 7 月に公表した。この事案では、情報漏洩の実害は確認されていない。しかし、研究所では漏洩の可能性が否定できない企業等の外部機関に経緯説明、謝罪等の対応をとった。

現場の筆者らも様々な作業を行った。禁止事項、定期的に実行すべき事項が追加された。例えば、

- ログを残さないファイルサーバ、アップデータの提供されていないプリンタ等のネットワークからの撤去
- これらの機器のアップデータの定期的な確認と記録
- 私物の所内ネットワークへの一切の接続禁止
- 仕様書等に記載すべき、情報セキュリティに関する要求事項と関係部署における審査

- 所外の Web サーバ等への定期的な頑健性試験

全パソコンへのアンチウイルスソフトの配布、パソコン OS バージョンの制限、USB メモリ等の管理はこの事案以前から行われてきたが、これらについても強化が図られた。

5. 最後に

2 年後のいま振り返ると、発覚当初は被害の全容把握そのものが難しい作業だったと思う。不正アクセスで何をされたのか全貌がわからないと対策が終わらず、対応指示も終わらない。当初はこの先どうなるのか大変不安だった。2018 年 2 月の発覚直後は現場の筆者らもその作業に相応の時間を割いた。一度調べたものを再調査ということもあった。インターネットアクセスができないので、それぞれの機器のログの調べ方、アップデートの入手はモバイルルータなどで行わねばならなかった。ネットワークに接続できないことで生じた業務上の不利益もあったと思う。

3 月以降は、業務の再開と再発防止策の実行に多大なエネルギーを費やした。数字は公表されていないが、情報セキュリティに関連する経費は事案発生前と比較して相当増加したはずである。研究所では、今日に至るまで情報ネットワークシステムの抜本的な再設計、規則類の整備、暗号化ファイルを添付したメール送信を止めるための代替手段の導入、定期的な監査、全構成員に対する教育等の努力を継続している。

8.【参考資料】

- 医療情報システムの安全管理に関するガイドライン（第５版）p.117

  「8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準　C. 最低限のガイドライン」

  https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/00 00166260.pdf

- ３省３ガイドライン・３省２ガイドラインの課題と改善点, 弁護士水町雅子

  http://www.miyauchi-law.com/f/190731iryou3guidelinesissue.pdf#search='%E3%80%8C3%E7%9C%812%E3%82%AC+%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3%E3%80%8D'

- 総務省　医療情報安全管理関連ガイドライン検討ロードマップ

  https://www.soumu.go.jp/main_content/000567201.pdf#search='%E3%80%8C3%E7%9C%812%E3%82%AC+%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3%E3%80%8D'

- CODE BLUE　２０１９（TOKYO）

  https://codeblue.jp/2019/contests/workshop_01/

- 【注意喚起】　当院からのメールを受け取った方へ, 市立福知山市民病院

  https://www.city.fukuchiyama.lg.jp/site/hosp/19530.html

- 「患者のデータが人質に…」病院がランサムウェアに狙われている…「今年のセキュリティ課題」を IIJ が総括， 高橋正和
  https://internet.watch.impress.co.jp/docs/event/1220499.html
- 産総研の情報システムに対する 不正なアクセスに関する報告， 国立研究開発法人 産業技術総合研究所
  https://www.aist.go.jp/pdf/aist_j/topics/to2018/to20180720/20180720aist.pdf
- グローバルサイバーセキュリティキャンプ　ホワイトハッカー， 篠田佳奈
  https://r.nikkei.com/article/DGKKZO53251510S9A211C1EAC000?s=4
- 患者情報を記録したノート PC と外付けハードディスクを病院外で紛失、持ち出し時に匿名化を実施せず， 昭和大学病院
  https://s.netsecurity.ne.jp/article/2020/01/14/43519.html
- 医療機器セキュリティと IoT 化への道 黒田正博
  https://www.jstage.jst.go.jp/article/safety/54/6/54_430/_pdf/-char/ja
- Cybersecurity is something that impacts everyone, especially in the field of health care. Cybersecurity protects patients personal and health data. Learn more about cybersecurity measures at the AMA， American Medical Association
  https://www.ama-assn.org/topics/cybersecurity
- Dicom Systems, Google Cloud Team on Secure Medical Imaging Storage， Karen D. Schwartz

https://www.itprotoday.com/cloud-security/dicom-systems-google-cloud-team-secure-medical-imaging-storage

- 国際標準化が加速する医療機器サイバーセキュリティ、AI 活用の前提条件, 笹原英司
  https://monoist.atmarkit.co.jp/mn/articles/1912/13/news021.html
- Blue Button 2.0 API Update, Centers for Medicare & Medicaid Services(CMS)
  https://bluebutton.cms.gov/blog/bbapi-update.html
- CMS Advances Interoperability & Patient Access to Health Data though New Proposals, Centers for Medicare & Medicaid Services(CMS)
  https://www.cms.gov/newsroom/fact-sheets/cms-advances-interoperability-patient-access-health-data-through-new-proposals
- From cyber attack to heart attack: the hidden human impact of hospital hacks, Anjuli RK Shere（researcher at the University of Oxford）, New Statesman
  https://www.newstatesman.com/politics/health/2019/12/cyber-attack-heart-attack-hidden-human-impact-hospital-hacks?amp=&utm_medium=social&utm_source=linkedin&utm_campaign=postfity&utm_content=postfityccefa
- A Hacker's Guide to Healthcare: How to Improve Lives with Data, Chaos-West Stage
  https://fahrplan.chaos-west.de/36c3/talk/AQSTLX/
- １０億件を超える患者の画像が米国の医療機関からオンラインに流出, Zack Wittaker

https://jp.techcrunch.com/2020/01/13/2020-01-10-medical-images-exposed-pacs/

- Nation-State Attacks: Why Healthcare Must Prepare,　Errol Weiss of H-ISAC

  https://h-isac.org/nation-state-attacks-why-healthcare-must-prepare/