日医総研ワーキングペーパー

医療現場のサイバーセキュリティ確保に向けて：
専門家インタビュー調査から

No. 488

2024 年 12 月 10 日

日本医師会総合政策研究機構

坂口 一樹、堤 信之

医療現場のサイバーセキュリティ確保に向けて：
専門家インタビュー調査から

坂口 一樹（主任研究員）、堤 信之（客員研究員）

キーワード

◆医療 DX　◆サイバーセキュリティ　◆ICT 資産管理　◆脆弱性対応

◆ネットワーク構成図　◆セキュリティオペレーションセンター（SOC）

ポイント

◆本稿の目的は、医療 DX が進展する将来を念頭に、医業経営の実情を踏まえた現実的なサイバーセキュリティ確保策の提言である。情報通信技術（ICT）やデジタル技術、情報セキュリティの専門家・実務家・学識経験者を対象に実施したインタビュー調査で得た知見を基に具体策を検討し、医療現場を取り巻く各ステークホルダー向けに、提言を取りまとめた。

◆医療機関には、システム管理の徹底、すなわち ICT 資産管理、院内システムのネットワーク構成図の作成と更新、ネットワークの出入口対策、情報端末・通信機器のセキュリティ対策と脆弱性対応、ネットワーク内部の監視、有事の被害最小化策といった具体策が求められる。また。経営者と従業員の意識改革とあわせて、ベンダー（情報システムの販売業者）の活用や希少な ICT 専門人材を地域毎にシェアする仕組みの構築を提言したい。

◆（1）医療界には、DX やサイバーリスクに関する情報の現場への伝達、集団交渉による対策費用の低減、経営者向けの啓発活動に加え、支援人材の受け皿や有事の現場支援を担う役割が期待される。また、(2)情報システム業界には一部ベンダーの質の改善を、(3)保険業界には、適正なリスク計算のための事例蓄積とサイバーリスク低減につながる付帯サービスの充実を、それぞれ期待したい。

◆国には、① 司令塔組織（NISC）の見直しと強化、② 脆弱性情報の確実な伝達と現場の対策実装支援、③ システム仕様書を点検する第三者機関の創設、④ サイバー空間のセキュリティ監視組織（SOC）の制度化と医療機関向け地域別 SOC の構築、⑤ 有事の相談窓口の一本化に加え、⑥ 財源の確保と DX 進展に伴うリスクに関する国民・患者向けの説明責任遂行を提言した。また、⑦社会全体の DX が進む将来に向けて、健康・医療に関するデータの廃棄ルールや真正性の担保手続、フェイク情報拡散への対処法についての政策議論を始めておくべきである。

目　次

1. はじめに

昨今、わが国における企業・団体等へのサイバー攻撃事件はますます増加傾向にあり[1]、業界を問わず、甚大な被害を被った事案は枚挙にいとまない[2]。「情報セキュリティ 10 大脅威 2024」によれば[3]、「ランサムウェア」と「標的型攻撃」が上位を占めた他、攻撃手法として「サプライチェーンの弱点の悪用」「修正プログラム公開前の攻撃」「脆弱性対策情報の公開に伴う悪用」等が挙げられており、併せて「犯罪のビジネス化」がその要因と懸念されている。とりわけ“ランサムウェア”を使用した攻撃事案では、システム侵入後にデータを暗号化し利用不能にした上でその解除を条件に身代金を要求するにとどまらず、窃取したデータをさらに悪用するという悪質さが際立っている。警察庁サイバー警察局の報告書ではサイバー犯罪の組織化と手法の洗練化が指摘されており、当局は防犯に加え、被害の潜在化防止に努めている[4]。

かかる現状を踏まえて医療現場を見れば、取り扱う個人情報の秘匿性の高さから、犯罪者のビジネスの観点からは目をつけられる可能性が高い一方で、その人員や組織の規模、財政的制約からサイバーセキュリティ対策は必ずしも万全とは言えず、犯罪者のターゲットにされるリスクは低くないと考えられる。他方、昨今の日本政府は医療 DX を国策として推進し、経済界もこれに賛同している。医療 DX とは医療現場への情報通信技術（ICT）やデジタル技術のさらなる導入に他ならず、それに伴うリスクへの対処、すなわち医療現場のサイバーセキュリティ確保は、官民を挙げて取り組むべき最優先課題のひとつである。

---

[1] 警察庁サイバー警察局（2024）
[2] 國谷武史（2024）
[3] 情報処理推進機構（2024）
[4] 警察庁サイバー警察局（2023）

わが国の政府は決して手をこまねいているわけではない。2014 年には基本法が成立[5]、内閣府に政策の司令塔が設置され[6]、国内外の政府・専門機関とも連携してセキュリティに関わる情報を共有し、医療を含む重要インフラ毎に産業をグルーピングして連携し、各現場に必要なセキュリティ対策が実装される体制を取ってきた[7]。有事に対しては、かねてより医療機関等のサイバー攻撃被害時の連絡先が厚生労働省医政局内にあり、技術的な事柄に関する相談窓口が情報処理推進機構（IPA）に設置されている。また、サイバー犯罪の通報・相談先が各都道府県警にあり、警察庁にはオンラインの相談窓口がある。

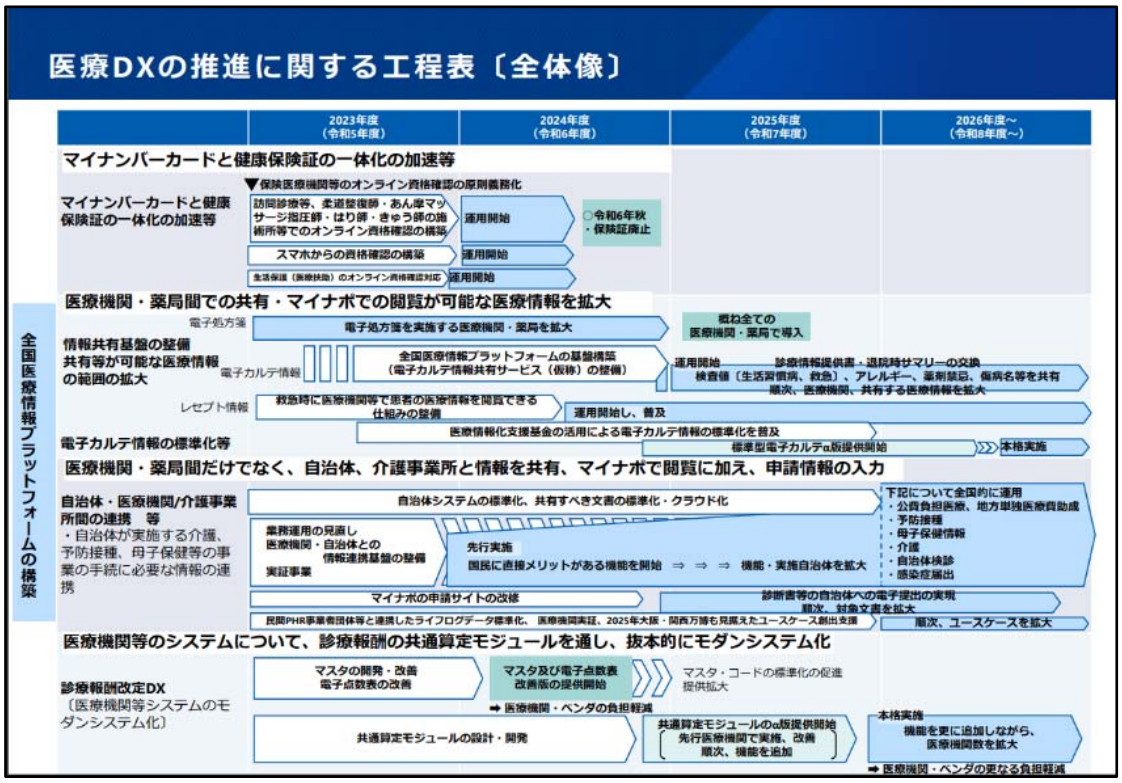
また昨今、病院・診療所のサイバー攻撃による被害事例が続発している情勢を踏まえて、厚生労働省は医療現場のサイバーセキュリティ確保に向けた取り組みを加速させてきた[8]。これまでガイドライン文書の更新[9]、医療機関・事業者向けの対策チェックリストの作成[10]、事業継続計画（BCP）の策定支援、情報機器・ソフトウェアの脆弱性に関わる注意喚起やリーフレット作成といった施策に加え、委託事業による教育・研修体制の整備もなされてきている[11]。他省庁においても、経済産業省と IPA によるサイバーセキュリティお助け隊サービスの始動（2021 年 4 月）、警察庁でのサイバー警察局の発足（2022 年 4 月）、内閣官房の有識者会議での能動的サイバー防御の検討（2024 年 8 月）等、サイバーセキュリティ確保に向けた行政による施策が次々と打ち出されている。

---

[5] サイバーセキュリティ基本法
[6] 内閣サイバーセキュリティセンター（NISC）　https://www.nisc.go.jp/
[7] サイバーセキュリティ戦略本部（2024）
[8] 最新情報は「医療分野のサイバーセキュリティ対策について」
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html
[9] 厚生労働省（2023a）
[10] 医療機関と業者が共同で作業するためのチェックリスト本体に加えて、マニュアルも用意されている。
厚生労働省（2024a）　厚生労働省（2024b）
[11] 医療機関向けセキュリティ教育支援ポータルサイト　https://mhlw-training.saj.or.jp/

しかし現状は、事態の鎮静化に至ったとはとても言えまい。2024 年以降も、複数の医療機関がサイバー攻撃被害に遭ったとの報道や分析がなされており[12]、海外に目を移せば、サイバー攻撃によってさらに深刻な事態の発生が報じられている[13]。そのような中、政策工程表に沿う形で、政府が掲げる“医療 DX”が着々と進められているというのが、今の日本の医療の姿の一面である。

図表 1-1. 政府が掲げる医療 DX の政策工程表



「医療 DX の推進に関する工程表（全体像）」（令和 5 年 6 月 2 日医療 DX 推進本部決定）
https://www.mhlw.go.jp/content/12600000/001163650.pdf

---

[12] 2024 年以降も、鹿児島や岡山の病院がランサムウェア攻撃の被害に遭った事件が大きく報道された。また、三井物産セキュアディレクション（2024）によれば、2024 年 6 月～7 月の医療・福祉分野への攻撃は 12 件増加、全業種で 3 番目の多さである。

[13] たとえば、日本経済新聞「米病院、サイバー攻撃の的　身代金目的にデータ奪う、被害多発で政府対策へ」（2024 年 4 月 9 日朝刊）、CNN「大手医療法人にサイバー攻撃、救急車迂回　米で相次ぐ病院の被害」（2024 年 5 月 10 日）、CNN「主要病院で医療サービス中止、請負業者へのランサムウェア攻撃　英ロンドン」（2024 年 6 月 5 日）等。

以上のような情勢を踏まえて、医療現場のサイバーセキュリティを取り巻く現況と医療現場への ICT とデジタル技術が進む今後に向けてのあるべき施策を論点として、関係分野の専門家、実務家、学識経験者の見解・意見を聴取した。日本のサイバーセキュリティ政策の課題と対応策を整理し、筆者らの考察を加えて、関係各所への提言と将来に向けた事態の改善に繋げたい。

2. 調査概要

2.1 本稿の目的

本稿の目的は、医療 DX の進展、すなわち医療現場への情報通信技術（ICT）とデジタル技術のさらなる導入が見込まれる将来を念頭に、昨今の医業経営の実情を踏まえた現実的なサイバーセキュリティ確保策の提言である。

医療現場に実装するべき具体策の検討にあたっては、ICT やデジタル技術、情報セキュリティの専門家・実務家・有識者を対象にインタビュー調査がベースとなっている。主に以下の 3 点に焦点を当てて聴取内容を精査し、医療を取り巻くステークホルダーに向けて、今後のあるべき施策・取り組みの提言を目的とした。

1. **現在および医療 DX が進行した将来のサイバーリスク**
2. **あるべき日本政府のサイバーセキュリティ政策・取り組み**
3. **医療現場の人員・組織体制の実状を踏まえた具体的な対策**

2.2 調査対象

インタビュー調査の対象者は、ICT・デジタル技術・情報セキュリティの専門家・実務家・学識経験者である[14]。官・民・学をまたがる形で可能な限り広範に論点をカバーすることを意識し、選定した。対象とした組織・団体とその属性は、図表 2-2-1 の通りである。計 8 団体、18 人＋α（ウェブ参加）を対象とした。

図表 2-2-1. インタビュー調査の対象（五十音順）

組織・団体	属　性
医療サイバーセキュリティ協議会	情報セキュリティに関する専門家
NTT東日本	ICT・情報セキュリティに関する実務家
NTT Risk Manager	ICT・DX・情報セキュリティに関する実務家
大阪大学 D3センター	ICT・DX・情報セキュリティに関する学識経験者
情報処理推進機構（IPA）	情報セキュリティに関する専門家
ソフトウェア協会	ICT・DX・情報セキュリティに関する専門家
デロイトトーマツ	ICT・DX・情報セキュリティに関する実務家
トレンドマイクロ	情報セキュリティに関する実務家

また上記に加えて、2022 年 4 月発足の警察庁サイバー警察局を訪問し、現下の情勢とセキュリティ確保のための施策・対策に関する意見交換を行った。

[14] 情報セキュリティマネジメントシステム管理基準「JIS Q 27002ISO/IEC27002)」、「ISO/IEC27032」によれば、「情報セキュリティ」とは「情報の機密性・完全性・可用性を維持すること」と定義され、「情報セキュリティ」は「サイバーセキュリティ」を包含する上位概念との位置付けである。

2.3 調査方法

インタビュー調査方法としては、非構造化面接法を採用した。あらかじめ当方から主な論点やインタビュー・ガイドを提示したが、原則は実施当日の話の流れに沿って、自由に回答してもらった。インタビューはすべて対面で実施したが、一部先方からのウェブ参加となったケースもある。実施時期は、2024 年 5 月～10 月である。

なお、率直で闊達な意見や見解等の聴取のため、論文化・報告書化にあたっては個別の発言の出所は明示しない前提とした。したがって、本稿の記述は同前提に従っている。また、聴取した内容の客観性・正確性の担保のため、インタビュー実施にあたっては、すべて複数名体制で臨んだ。

インタビュー調査の主要論点は、下記の通りである。使用したインタビュー・ガイドは、巻末資料として添付した。

（１）昨今のサイバー攻撃の類型と特徴

（２）医療ＤＸの進展に伴うサイバーリスクについての見解

（３）現状の行政のサイバーセキュリティ対策に対する意見

（４）医療機関のリスクマネジメント体制についての意見

（５）民間のサイバー保険とその付帯サービスについての意見

（６）関係する業界団体に対する期待

（７）その他の重要論点

3. 調査結果

本章では、インタビュー調査で聴取した情報を極力そのままの表現を活かし、論点ごとに整理して、掲載した。

3.1 医療現場に求められる管理体制とセキュリティ対策

（1）【総　論】システム管理の重要性

- いま医療機関で起きているインシデントのほとんどが、VPN 機器やルーター等のネットワーク機器の設定不備といった初歩的なセキュリティ設定の不備に起因している。ただ、全面的にベンダー側に責任があるかというと、原則、情報機器の管理責任は、所有者である医療機関側にある。

- 情報システムの導入・調達にあたって、医療機関側には仕様書を書ける人材がいないため、多くのケースでコンサルやベンダーに丸投げになっている。結果として、ベンダー側の利益優先で仕様書が作成されて、医療機関側には要らない・使わない機能が盛り沢山のシステムになっており、システムの全体像はおろか、IT 資産管理もなされていないケースがよくある。

- IT 資産管理をしっかり実施し、AS（アタックサーフェイス）[15]をもれなく

[15] インターネットと接続しているところを「アタックサーフェイス」と呼び、ここがサイバーセキュリティ対策上の優先度が最も高い。

把握することが重要であるが、大きな病院だとシステムや契約が複雑でリスクの全体像を把握するには一手間必要である、中小だとベンダーに依存せざるを得ない一方で契約上ベンダーにサイバーセキュリティ対応まで規定されておらず担い手がいない、という課題をそれぞれ抱えている。

（２）【各　論】技術・組織体制

① ネットワークの出入口対策

- 院内システム・ネットワークの出入口をいかに集約していくかが、管理体制を構築するうえでのカギのひとつである。ネットワーク環境でなければ保守しないというベンダーも多い一方で、侵入経路となり得るネットワークの出入口をなるべく少なくするというのがセキュリティ対策の常套手段である。先ずは、出入口をどう束ねていくかである。

- UTM をルーター下に設置し[16]、ネットワークの出入口の監視、不正通信の検知・遮断を行うことが有効である。

② 機器・端末のセキュリティ対策・脆弱性対応

- 一般的に使われるインターネット VPN において、当該接続点がよく狙われている。ベンダーの保守サービス（リモートアクセス）に使われるのはほぼ

[16] UTM（Unified Threat Management）とは、日本語で統合脅威管理と呼び、不正アクセスや疑わしい通信を検知・遮断する機能（IDS/IPS）やファイアウォール、アンチウイルス等、他の機能も備えた製品パッケージのことである。

こちらだろう。訪問診療も同様である。この方式だとコストは安いが入口まではたどり着けてしまう。それだけに中に入らせないため、以下のような対策が重要になる。

〇電子メール等への警戒

〇認証情報の適切な管理

〇アクセス権等の権限の最小化

〇ネットワーク機器のアップデート（脆弱性情報のキャッチ）等

- 医療機器の保守を遠隔で行うことが一つの売りになっている以上、完全な閉域網ではなく、サイバーリスクと無縁ではない。システムのアップデートに関わるリスク、すなわち、しないことにより被るサイバーリスクと、することにより当システムおよび繋がる先のシステムに悪影響を及ぼすリスクをどう評価し差配するかが大きな問題である。医療機関自らができないなら、適切にリードしてくれるベンダーと付き合うか、上記に適合する能力ある人材シェアの仕組みを真剣に考えるしかない。

- ネットワークの出入口を突破された後の備えとして、ウイルス対策ソフトの導入が有効である。

③ 閉域網 VPN（IP-VPN）の利用

- インターネットと直接つながず、キャリア閉域網を経由して VPN をつなぐサービスを利用することが考えられる。ただし安心度は高まるが、コストは格段に高くなる。

④ 回線・アカウントの運用見直し

- 外部との常時接続が不要な回線について、不要時は電源を落としておく運用も有効である。大阪急性期・総合医療センター（以下「大阪急性期」）のサイバー攻撃事件は、原因となった外部取引先と常時接続していなければ防ぐことができた可能性がある。また、回線を日常用と保守用に物理的に分けておき、保守用は使用時以外、電源を落としておくことも有効である。

- 端末・回線について、私的利用が可能なものと院内ネットワークとを物理的に分けておくことは、すぐに実施可能なセキュリティ確保策である。

- 院内ネットワークを管理して定期的に棚卸しを行い、不要になったアカウントを消去するだけでも、相応のリスクを回避することができる。

⑤ リスクシミュレーションとアセスメントサービスの定期的実施

- まずはリスクシミュレーションが重要である。何ができていて何ができていないかが、そもそも把握されていないことが多い。リスクの所在、レベルが分からないと、適切な対応がとれないことに加え、余計なコストがかかることにもなりかねない。

- リスクに応じてシステムをセグメント分けし優先順位付けしておくことが重要である。基本的にはインターネットと接続しているところをアタックサーフェイス（AS）と呼び、この優先度が高い。接続点があってもルーターが設定されているなら通常は安全性高いとセグメントされる。一方で、ルー

ターの脆弱性が判明した場合には緊急性が高くなることを理解し、状況に応じたリスク判断をすることも重要である。ASM（アタックサーフェイスマネジメント）[17]を活用する手もある。

- セキュリティリスクへの対応をベンダーに委託するにしても、複数システムが導入されていると保守運用まで何とかカバーできたとしても有事の対応はネットワーク構成図がないと不可能である。例えばソフトのアップデートにより他のシステムや既存ソフトに影響が出る可能性について、一般的にはベンダーがサービスでアドバイスしていると思われるが、院内ネットワーク情報がなければ、対応に限界がある。総合的な相談先（プライムベンダー）を決めるにも状況確認、現状把握を医療機関がすることが肝心である。

- 厚生労働省の「医療機関におけるサイバーセキュリティ確保事業」[18]では、補助金を活用し、病院のネットワークシステムについて外部ネットワークとの接続の安全性の検証・検査を行った上でバックアップ体制の整備まで行うという内容で 2024～25 年度にかけて順次実施されている。予防策として有効であるが、電子カルテシステム導入の病院が対象で、クリニックは対象外である。

- 民間のコンサルティング会社のアセスメントサービスは大規模病院が対象であり、中小病院やクリニックは顧客として想定していない。

---

[17] アタックサーフェスマネジメント（ASM）とは、攻撃者の視点からサイバー攻撃が行われる可能性のある組織のアタックサーフェス（攻撃対象領域）を把握し、セキュリティを強化する取り組みや技術のことである。

[18] 厚生労働省医政局　事務連絡「医療機関におけるサイバーセキュリティ確保事業」の実施に係る支援対象病院の選定について（依頼）」（令和 6 年 2 月 16 日）
https://www.ajha.or.jp/topics/admininfo/pdf/2024/240219_2.pdf

- クリニック・中小病院向けのリスクアセスメントサービス（ネットワーク環境の状況確認）を用意している民間企業もある[19]。同サービスの一例では、現地を訪問調査し 1～2 週間でレポートする。ネットワーク構成図を作成したうえで、本来繋げてはいけないところが繋がったりしていないか、例えば患者用 Wi-Fi に院内システムが繋がっていないか等をについて確認することができる。なお同サービス料金は、院内設置端末台数 20 台とした場合で、60,500 円／回との見積である。

- ネットワーク環境は各種要因により随時変化する可能性があるため、初回実施後、少なくとも年 1 回の確認作業を継続するべきである。

⑥ ネットワーク内部の監視

- ネットワーク外部からの攻撃だけでなく、内部を監視するべきである。例えば、とある業者が設定を簡便に行うために好意で持ち込んだポケット Wi-Fi ルーターが病院のシステム管理者が知らないうちに院内端末のインターネット接続に使われていて、これが「シャドーIT」[20]となり、そこから侵入されたというケースがある。このようなケースは、内部の通信を監視していれば、事前に検知できる。

---

[19] A 社「おまかせ ICT 診断サービス」。なお上記料金は PC 台数に応じて増えるが、1 台あたりの料金は漸減する。ただし MAX60 台を前提とした料金体系である。

[20] 企業が使用許可をしていない、あるいは従業員が利用していることを企業側が把握できていないデバイスや外部サービスのこと。つまり、管理対象外のデバイスやサービスのこと。

⑦ 保守契約の見直し

- 通信機器の所有者、すなわち医療機関が全てのリスクに主体的に対応するのが原則であり、総合的な対策をサステナブルに実施していくには医療機関が費用負担する前提で取り組むのが筋である。保守契約上、曖昧な部分が多いと、責任の所在が不明瞭になり、最終的には患者に迷惑がかかることになる。

- 現実的には医療機関がサイバーセキュリティ対策を適切に実施することは難しいこと、ベンダーにも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としての責任があることから、専門家であるベンダーに頼るケースが多い。一方で、サイバーセキュリティ対策を誰がどこまで対応するのか、ベンダーが行うとした場合、その費用をどう負担するのか、等についての決めは、当初導入時の契約や保守契約では必ずしも明確にされていない。

- 医療機関としてはサイバーセキュリティ対策について、積極的に何を決めておくべきかを明確にする必要がある。たとえばファームウェアのアップデートを誰がするのか、VPN は誰の所有物かといったことになるが、現状ではこの作業に適したチェックリストがないという問題がある。

- 保守契約書のひな形は各ベンダーが用意しているが、契約上どういう点を考慮すべきかを箇条書きにするだけでも医療機関に有用だろう。現状のチェックリストに対策上必要な要素は盛り込まれているので、自分でできない要素についてどうするかを保守契約に盛り込んでいるかがポイントになる。

- 医療機関としては積極的に、何を決めておくべきかを明確にする必要がある。

例えばファームウェアのアップデートを誰がするのか、VPN は誰の持ち物かといったことになるが、現状ではこの作業に適したチェックリストがないという問題がある。

- ソフトウェアのアップデートは、システムが不具合を起こさないかの動作確認をしてからでないと実施すべきではない。誰がどこまで作業対応するのか、ベンダーが行う場合、アップデート費用をどう負担するのか、導入時の契約や保守契約で明確にされていることが望ましい。

⑧ 被害最小化対策

- システム・ネットワークのセグメンテーションも重要である（ネットワーク・セグメンテーション）。大阪急性期のケースでは、あらゆるシステムが同じアドレスに配置されていた。それだと、一か所が侵入され被害を受けると、すべてのシステムが被害を受けてしまう。そうならないように、すなわち万一の場合も被害を局所化できるように、できる限り院内ネットワークを小分けして運用しておくことが、セキュリティ上、重要である。

⑨ データのバックアップ

- バックアップに関して、レガシー機器の活用というのも手である。最近のバックアップは、高性能でスピードも速い。一方、大阪急性期の事例では、バックアップ・システムもランサムウェア攻撃を受けたが、調達時期の関係で、一部旧式のテープ・デバイスを使っていた。テープ・デバイスは動作が遅いゆえに暗号化を免れ、そこから（10 日前のデータになったが）データ

復旧できた。最新のシステムは高性能で動作も速いがゆえに暗号化されるのも速い。テープ・デバイスは動作は遅いが安定しており、銀行も未だに使っている。医療機関でも活用を考えた方が良いかもしれない。

- 厚労省施策のオフラインバックアップは対処策として有効だが、継続運用の必要性を医療機関側にどれだけ意識付けできるか、ベンダー側がどれだけ対応できるかという課題があるように思う。

⑩ BCP、非常時行動計画の策定

- サイバー攻撃を受けた場合は、全てのマシンの復旧作業が必要になる。復旧作業の間の診療継続のためには、代替機（スタンドアロンで動作する通常のWindows PC でよい）が必要である。なお、これまでの経験上、被害を受けたからと言ってベンダーが代替機の無償提供をすることはない。

⑪ サイバー保険の手配

- 被害時の一時金支払いやフォレンジック等の費用が賄われるので、リスクの移転という意味でも、サイバー保険に加入しておくことは望ましいと思う。一方で海外では、身代金支払いまで保険金支払いの対象になっている商品もあり、保険料が高騰しているケースもあると聞く。今後は、ガイドラインに準拠していると保険料が安くなる等の工夫が必要だろう。

- サイバー保険について、まだ事故事例の蓄積が少なく、保険料を決めるリスク評価基準が定まっていない状況なので、確立のための努力を続けるべき。

また、保険の付帯サービスとしての医療現場のサイバーリスクの見守りサービスのようなアイデアはあり得るかもしれない。

- BCP 策定しようとすると院内に CSIRT（シーサート）[21]の設置が求められるが、サイバー保険に加入しその窓口に委託することで代替可能になる。人的問題等で設置が難しい医療機関には一つのメリットになる。

⑫ 被害を受けた医療機関職員のメンタルヘルスケア

- サイバー攻撃を受けた医療機関で働く職員のメンタルヘルスケアも重要である。診療休止を知らずに来院した患者からの厳しい苦情等、プレッシャーでメンタルをやられた方は少なくない。

（3）【各　論】人材

① 望ましい人材像

- ネットワーク全体像を把握している人が必要である。技術的なことより管理のレベルが問題である。何があるかを把握しており、それぞれについて誰に聞けばよいかが分かるだけでもよい。

- 人材レベルとしては、機器の脆弱性が悪用されるとどうなるのかの危機感を持ち、どこに何があるかを把握した上で、起こった事象についてどうすれば

[21] CSIRT とは、Computer Security Incident Response Team のアクロニムであり、コンピュータ関連のセキュリティに関わる事故対応チームのことである。

よいかを自ら判断できずとも、事象毎に誰に聞くかが分かるくらいでよい。リスク対応の優先順位がつけられれば、なおよい。

② 職員教育

- 厚労省の教育研修ポータルサイトは[22]、人材育成が重要といわれているにもかかわらず、余り活用されていない印象である。認知が十分でないことが原因ではないか。「情報管理責任者」は、診療報酬制度上で評価されたため、ポスト設置は進んだが形だけの印象である。

- 職員のリテラシーレベルに起因する問題として、オンライン資格確認システムにインターネットにつながっている端末が不用意につながれている実態が挙げられる。これはサイバーセキュリティ対策上好ましくないが技術的には可能であり、現状禁止もされていないので、ベンダーとしては、医療機関から要望されたら応えるしかない。

③ 人材シェア

- 医療機関にサイバーセキュリティ対策に関する課題を受け止められる人材が必要であるが、診療報酬を念頭に常駐で雇う事を考えるより、支援できる人材を用意し、そのコストを行政が補助するという考えもあるだろう。

- ベンダーが想定する保守費用は、小さい医療機関にはとても受け入れられな

[22] 医療機関向けセキュリティ教育支援ポータルサイト　https://mhlw-training.saj.or.jp/

い額になる可能性が高く、実現性に問題がある。また地場のベンダーには技術がないという問題もある。となると、上記に適合する人材を地域でシェアする仕組みを新たに構築しないと対応できなくなる恐れがある。

- 少し前線で、サイバーセキュリティ対策に当たる部隊も必要なのではないか。たとえば、医療計画に盛り込んで都道府県単位で対応する、人口規模の大きな都道府県は（二次医療圏単位とか、人口 100 万人単位とか）さらに小さい単位のレイヤーで対応する、といった重層的な対策の主体のあり方が求められるのではないか。

- すべての医療機関にセキュリティ対策ができる人材を配備するのはどう考えても現実的ではない。そのような人材は 10 年以上の長期にわたって全産業的にも枯渇しており、もしいたとしても医療機関の給与体系には見合わない。したがって、そういった希少な人材を全国の医療現場のセキュリティ対策のポイント毎に、計画的に配置するといった戦略が必要になるだろう。

- 医療現場のセキュリティ人材の育成や活用方法について、医師と同じように他の医療機関をサポートできるよう、積極的に副業・兼業を認めていってはどうだろうか。そのような人材は希少だが、待遇や活躍の場に恵まれていないように見受けられる。医師に限らず、医療系の人材は勉強熱心で、思いがあって医療業界にいるケースが多い。その意欲を地域の医療機関のセキュリティ対策に活かしたい。

- 現在のセキュリティ人材の年収相場は 1000 万円超、外資系だと 1500 万円超のケースもあり、医療界の相場とは見合わない。そうなると、地域単位や

複数の病院・診療所単位でコストを負担しあって、人材をシェアリングしていくことを考えていくべきである。医師の先生が複数の医療機関で勤務しているように、医療現場のセキュリティ人材もそのような形で勤務できる環境を整えていくべきである。

④ ベンダー活用

- 必要とされる人材（医療機関の）は、内部の人間でなくともベンダーにお願いすることでもよい。

- サイバーセキュリティ対策上の注意喚起が発せられた場合の自主対応をクリニック規模の医療機関にまで求めることには無理がある。ベンダーに任せることを保守契約上明確にし、費用は政策で賄うのが解決策ではないか。

- ベンダーが複数の導入システム毎に分かれている場合、プライムベンダーを設置しておくことも有効である。

- これまであまりソフトのアップデート時におけるシステム安全性の担保が議論されてこなかったというのが課題である。システムベンダーとの契約そのものから見直しが必要ともいえる。対処法の王道としては、代表となるシステムベンダー（プライムベンダー）が取りまとめて、他のシステムへの影響の検証も含め、対応するという契約にしておくことである。そうでなければ、医療機関が自前でやるということになる。さすがに契約にないことをベンダー側にやってもらうというわけにはいかない。

- サイバーセキュリティ対策においてベンダー活用を想定する場合、その費用負担の問題がある。

⑤ 経営者の意識改革

- サイバーセキュリティ対策は、経営者が現場にヒトやカネといった経営資源を割かないと始まらない。情報セキュリティに対するトップマネジメントのリーダーシップは、ISMS（情報セキュリティマネジメントシステム）でのISO 認証（ISO/IEC 27001）の取得要件のひとつでもある。

- 医療機関の情報セキュリティ・ポリシーにトップマネジメントが責任を持つ体制が第一に重要である。トップが医師で多忙なのは理解できるが、「私はよくわからないので、君たちよろしく」という姿勢ではいけない。

- 気になるのは、サイバーセキュリティ対策を何故やるのかという啓蒙の部分がまだまだ足りないことである。そこで、実際の事故に際してどういったことが起きているのか、逆に言えば管理していないとどういったことが起きるのか、をもっとアピールする目的で作成されたツール（被害額を想定する計算シート）を活用し、具体的な被害額を示してそのリスクを回避することが重要な経営アジェンダということをトップに認識してもらう活動を実施している。

- 医療機関経営者が、セキュリティリスク対応費用を経営コストとして認識することが重要であろう。

（4）【各　論】予算・財源

①　対策費用の予算化、経営コスト化

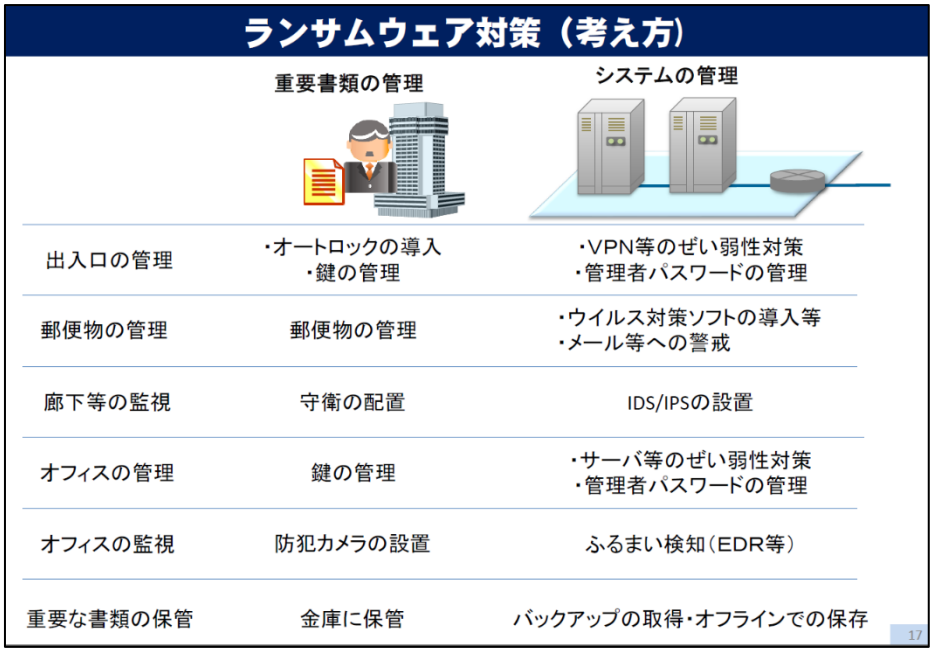
- システムのアップデートは、ベンダーが不具合を起こさないかの動作確認をする必要があるが、アップデート料金には、ベンダーが前記評価をする作業料が上乗せされる。一方、アップデート作業の頻度は例えばフォーティネットだと 10 回／年アップデートがある等、個別性が高いため、料金を予め見積もることが難しい。

- 1 回あたり数百万円になることもある。また、どこまでが当初導入時の契約や保守契約に含まれるのか個別性が高い。さらに言えば、全部対応したとしてもリスクをセロにできるわけでない。現実的には、対策にかける費用限度と優先順位を決めて、取り組むしかない。

- 民間のコンサルティング会社が大規模病院レベルを対象に実施するリスクアセスメントサービスだけでも、1 回当たり 500 万円程度の費用感である。前記アセスメント調査結果を基にどこまで費用をかけるかを検討するのが現実的である。たとえば。300 床規模の病院のシステム構築だと、一般的には 5,000 万円程度の費用を想定し、その中にどれくらいのセキュリティ対策を含めるかを検討してネットワークを構築する。なお、保守契約費用は導入コストの 5～7%くらいが目安と言われており、本ケースだと年間 300 万円程度となる。

- 以下、A～C 社に対策費用の見積もりを取るにあたっては、下記の通り警察庁が示す、ランサムウェア対策の考え方を基に、依頼した。

図表 3.1.1.　警察庁が提示するランサムウェア対策の考え方



資料：警察庁サイバー警察局

- クリニック、中小病院向けに A 社が用意するランサムウェア対策総合サービスでは以下の通りコストが見積もられている。

＊以下、院内設置端末台数 20 台とした場合の導入コスト

①UTM の設置：12,100 円／月

② ウイルス対策ソフト+EDR の導入：24,200 円／月

③リモートアクセス対策サービス（インターネット VPN の場合）の導入：7,700 円／月

④ ランサムウェア対策バックアップサービスの導入：14,300 円／月

⑤ リスクアセスメントサービスの実施：60,500 円　／回

従って、院内設置端末台数 20 台規模のクリニックが①～⑤を導入・実施する場合の年間コストは、760,100 円となる。

- Ｂ社からの聴取（クリニックレベルのセキュリティ対策の年間の費用感）

□ VPN 等の脆弱性対策、PW 管理：保守契約に含みゼロとする

□ ウイルス対策ソフトの導入：20 万円前後

□ IDS／IPS の設置：10～50 万円

□ サーバの脆弱性対策：まずはウインドウズパッチ、それに加えて 20～50 万円

□ ふるまい検知（EDR）：10～50 万円

□ パックアップ・オフライン保存：10 万円～（但し頻度、サイズ、方法次第）

上記合計は年間 70 万円～180 万円となる（リスクアセスメントサービス含まず)。

- Ｃ社（同上）

□ VPN 等の脆弱性対策、PW 管理：保守契約に含みゼロとする

□ ウイルス対策ソフトの導入：15 万円～（PC30 台レベル）

□ メール等への警戒：10 万円～

□ IDS／IPS の設置：20 万円～（～100 台)、40 万円（～300 台）

□ サーバの脆弱性対策：10～100 万円（脆弱性診断ツール／サービス）

□ ふるまい検知（EDR）：450 円／台／月額

□ パックアップ・オフライン保存：3～5 万円（外付け HD･1TB）

上記合計は年間 68 万円～160 万円となる（PC20 台)。

② 医療 DX 推進のための診療報酬等による財源確保

- 厚労省の安全管理ガイドラインは Ver.6.0 になって、サイバーセキュリティ対策をはじめ、様々な項目が盛り込まれたが、実に現場泣かせである。なぜならカネがつかないとできないことばかりだからである。半田病院と大阪急性期の事件があって、厚労省の意識は大きく変わった。それがガイドライン Ver.5.2 から 6.0 の変化である。ただ、ガイドラインを作るのが目的ではないので、診療所のレベルまで対策ができるような財源を確保するべきである。

- セキュリティ対策コストの原資をどうするかの問題は、たとえば、地震被害を受けた医療現場への支援や建物耐震化対策の医療機関への補助金の制度を参考にして制度設計するのも一案ではないか。

3.2 現行の政策に対する評価と改善提案

① 有事の行政窓口の一本化

- 行政の体制については、まずはインシデント・アクシデント発生時の窓口を一本化するべきである。厚労省に連絡し、警察に届け、IPA に相談し、個人情報漏洩がある場合には、個人情報保護委員会への速報・確報の報告をしなければならない。そのうえ事案によっては内閣サイバーセキュリティセンター（NISC）から報告を求められることもある。これは、医療に限ったことではない。

- 本来であれば、司令塔である NISC に報告をすれば、そこから関係する行政官庁やセプター事務局に必要な情報が伝わるべきだし、そのような体制にしておかないとインシデント発生時に現場が大変である。

- 何かあった時の連絡先は非常に重要である。厚労省医政局に病院向けの連絡先もあるが、われわれの業界からすると、先ずは警察である。110 番でもよい。サイバーの窓口につないでくれるし、今はサイバー事案に力を入れている。また、警察は地域の様々な関係者とつながっているので、それが助けになることもある。たとえば、ランサムウェア攻撃を受けると患者向けに連絡する手段もなくなるので、警察から地元メディアを通じて診療休止をお知らせすることもできる。

- サイバー攻撃を受けた時の連絡先が厚労省医政局である必要性はない。警察

でも良いし、政府共通のコールセンターでもよいので、有事に 24 時間 365 日連絡が繋がって、そこから関連省庁に連携がなされるネットワークがあることが重要で、複数省庁にまたがる連絡先があったり、日や時間帯によってつながらなかったり等の理由で初動が遅れるのは大変よろしくない。

② 行政における情報・ノウハウの集約

- 医政局の担当部署はサイバー事故被害事例を収集しているが、それらの情報がどのように対策に活かされているのか、今ひとつ明確でない。そういった情報を活用しつつ、より現場に対して具体的にわかりやすく、セキュリティ対策の必要性を理解してもらえるような工夫が欲しい。現状は、NISC が出した PDF ファイルに各自のカバーレターが加えられて、転送されているだけという状態で、せっかくの仕組みがもったいないと感じている。

- 行政の人員体制が弱い結果、ベンダー頼りになり、統一的な対応が出来ていない。たとえば、医療機関のサイバーセキュリティに関わる英国の行政官は約 4,000 人いるのに対し、日本の厚労省では約 40 人である。

- 政府の体制でいうと、デジタル庁の立ち位置もよくわからない。マイナンバーのことだけやっているわけではなく、デジタル庁にもサイバーセキュリティの部隊はいる。

- 医療 DX だけでなく、電子政府も含め、目標設定が明確でない。日本では、そこはアンタッチャブルになっているように見える。政策関係者には、医療

DX やマイナンバーの活用について、大方針を設定することを期待したい。

③ 政策の司令塔組織の再編・強化

- 内閣サイバーセキュリティセンター（NISC）は、かつては内閣官房の専門部隊として、セキュリティに詳しいエキスパートや技術者のいる司令塔的組織だったのが、政府の一機関としてお役所化し、あまり情報が集まらなくなってしまった。

- NISC のような政府の司令塔に集まった脆弱性情報が医療現場に伝わり、対策が実装されない限り、医療現場のサイバーセキュリティは進まない。ただ最近の NISC は最新の情報も持っていないし、人材もおらず、近いうちに解体されるのではないかと見ている。NICS 内部のリーダーシップのある行政官も、また不在である。

④ 行政ガイドライン、チェックリストの改善

- 医療情報システム事業者向けガイドラインについては、あまりにも事業者側の落ち度が低い場合にも行政指導が入るというような内容になっており、何か工夫が必要である。

- 対策チェックリストについては、医療機関とシステム事業者の双方でチェックする仕組みになっており、それは望ましいことだが、事業者からの提出がなされないケースが散見される。そのようなケースに対しては、医療機関が強く申し入れできるよう規制当局がバックアップするような仕掛けが必要

である。現状のガイドラインでは、「民法に基づき双方で合意形成をせよ」ということになっている。システムベンダー側について言えば、医療機関側の脆弱性への対応について、他人事感が強い。

- 厚労省のガイドライン、チェックリスト現場では意識されているが、経営層は自分のところは大丈夫だろうと考え、費用かけてまでセキュリティ対策をやられていないのが実態である。一方、チェックリストができたことにより、従来はベンダーに丸投げされていたシステム管理が、ベンダーと一緒にチェックするケースが増えて、一定の進化には寄与していると思う。

- 医療機関向けに出している厚労省のガイドラインは、医療現場がやるべき対策の記述が抽象的である。たとえば、ネットワーク機器のファームウェアの更新のやり方や院内ネットワークの中で重点的にセキュリティ対策をすべき場所等、セキュリティ対策にあたって医療現場の具体的な作業の案内になるような内容がもっとあってもよい。現場で対策の具体的な作業さえ進めば、今のサイバー攻撃のほとんどは防ぐことができると思われる。

- 現行のガイドラインは記述が抽象的であり、具体的な作業につながる案内が欲しい。また、診療所から大病院まで、ひとつのガイドラインでカバーしようというのは無理がある。組織や事業の規模別、あるいはシステム環境の規模別に、ガイドラインを分けて作るべきではないか。

- ガイドライン、チェックリストが医療機関の規模レベル別になっていないので、理解しにくい。チェックリストの位置づけとガイドラインとの関係が、クリニック、病院それぞれの立場で書き分けられておらず、理解しにくいの

でないか。

- チェックリストについては、保健所が理解していない（認識していない）。チェックリストをせっかく作っておいたけれども、立ち入り検査の際に保健所がチェックしなかったという話をよく聞く。チェックリストが機能しているのか、いったい誰がチェックしているのか、チェック後に具体的な対策につながっているのか、再確認が必要である。

- チェックリスト（点検表）の形骸化には気を付けるべきである。チェックリストに〇を付けることが目的化してしまうと現場を疲弊させるだけになる。チェックは×でもよい。現状で自組織のどこが弱いのかを認識するための気づきのツールであることを認識して活用すべきである。

- 現状のチェックリストに対策上必要な要素は盛り込まれている。したがって、自院で対応できない要素についての対応が保守契約に盛り込まれているかを確認するという活用方法がある。

- チェックリストに達成段階別にレベル分けをしてはどうか。例えば、自動車工業会のチェックリストは 3 段階に分かれており、縦軸に実施すべき事項があり、横軸に必須レベルの 1 から 3 段階がある。いきなり全て達成するというのでなく、レベル 3 に向けて段階的にレベルを上げていくイメージで、取り組みの計画を立てやすいというメリットがある。

⑤ 地域毎のセキュリティ監視体制の構築

- 厚労行政にお願いしたいのは、医療機関向けの SOC（Security Operation Center）の設置である。セキュリティ監視のための機器を設置したとしても問題はそこから吐き出されたデータを解読できる人材が医療現場にいないことである。くわえて、SOC は原則 24 時間 365 日体制で運営する必要があり、運用にコストがかかる。厚労行政には、地域毎に 20～30 施設くらいの複数の医療機関を束ねるような SOC を設置する制度設計を具体的に検討していただきたい。安全管理ガイドライン Ver.6.0 では、ある程度の病床数を有している病院に対して SOC を設置するように求めているが、現実には無理難題である。

- 上記の地域毎の SOC を提言する背景には、大阪商工会議所が主体となり実施している「サイバーセキュリティお助け隊」（経産省の事業）サービスの好事例がある。大阪にはいわゆる町工場が多いが、昨今は入札参加にあたってセキュリティ要件を満たしていることが求められるケースが珍しくない。一方で、セキュリティベンダーに SOC を依頼すると非常に高額になる（1,000 万円単位が相場であり、セキュリティベンダーは同サービスで儲けているとも言える）。これらを背景に、簡便で安価なサービスを実現している。見守りサービスだけでなく、相談もできる。こういった事例を参考に、医療機関向けの地域単位での SOC 構築を検討すべきである。

- 現在、経産省・IPA の「サイバーセキュリティお助け隊サービス」については厚労省の「医療機関におけるサイバーセキュリティ対策の更なる強化策」において、200 床以下の医療機関に対し、インシデント発生時の駆けつけ対

応としての活用が推奨されている[23]。相談窓口、監視、緊急時のかけつけ支援とその費用を補償する簡易サイバー保険がセットになっている。ただし怪しい動きを検知して遮断した場合に遠隔医療等に影響が及ぶリスクに鑑み、大阪での事例では医療機関について同サービスへの参加は見送られている。監視サービスを入れる前に現状をよく把握した上で同サービスを活用することは有効と思われるが、医療機関での採用はまだ聞かない。今後の活用に期待したい。

[23] 2023 厚生労働省第 19 回 健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ「サイバーセキュリティお助け隊サービスとの連携について」（2023 年 11 月 6 日）

3.3 医療現場の DX 進展に伴う課題

（1）政府が推進する“医療 DX”に伴うリスク

① 医療現場が優先的に狙われるリスク

- ランサムウェアの事案は、シンプルにおカネ目当てである。攻撃者は逮捕されるリスクもあるため、確実にセキュリティ対策が弱いところから、身代金を支払ってくれそうなところから、優先的に狙っている。そういった意味では、医療機関は格好のターゲットである。

- オンライン資格確認システムは、構成上は支払基金のデータセンターを中心として各施設が専用線もしくは拠点間 VPN で繋ぐことになっているので、その経路上から侵入されて被害を受けるという事態は起こりにくいシステムになっている。また、支払基金側もセキュリティ監視には大変厳しく注力しており、支払基金側が被害を受けるリスクは、リスク評価する際の順序・順番という文脈では、低いと考えられる。一方、医療機関側のセキュリティは、相対的に見ると、どうしても弱い。

- オンライン資格確認システムや全国医療情報プラットフォームは、いわゆる閉域網であり、それ自体にはリスクはないと思う。ただし怖いのは、現場の都合や利便性のために、その閉域網のネットワークとインターネットとつながっているネットワークとを安易につないでしまうという事態が起きてしまうことである。

- 全国医療情報ネットワークといっても、そこで特殊な通信プロトコルを使っているわけではなく、インターネットと同じ通信プロトコルを使っている。ただ、ネットワークを切り離しているから安全だという建付けになっている。しかし、ハブを使ってインターネットと繋がっているネットワークと接続することは可能である。利便性のために現場が安易に繋いでしまって、そこがセキュリティ・ホールになるということはあり得る。

② セキュリティ有事の際のネットワークからの切断リスク

- 医療現場にサイバー攻撃等のインシデントが発生した際、支払基金とのネットワークから切り離されることによって、業務が停止する、あるいは遅延するというリスクがある。そして、現在はオンライン資格確認にのみ使っているネットワークが、今後、電子処方箋や各種医療情報の参照などに使われるほど、医療機関の運営にとってのリスクは増大することになる。オンライン資格確認にのみ使っている現状でも受付業務等は混乱するだろうし、今後そのネットワークがさまざまな医療システムにつながるほど、業務停止や遅延のリスクが高まる。

- 支払基金とのネットワークから切り離されることが、医療機関経営における、いわゆる SPOF（シングルポイントオブフェイラー、単一障害点）になりつつあると言える。医療 DX 推進の議論において、良い話ばかりが強調されており、このリスクについての議論が不足しているのではないか。

- サイバー攻撃やシステム障害によって支払基金とのネットワークから切り離されたという事例はいくつか聞いている。くわえて、再接続する際の要件

がかなり厳格だという話も聞く。切断された場合の再接続の要件の詳細については開示されていないので詳細わからないが、「再接続しても安全であることの証明」の要件はかなり厳しいものだと考えられる。

- サイバー攻撃を受けてクラウドやデータセンターから切断された後に再接続しても安全であることを証明する確立された手順や手続のようなものは存在せず、セキュリティ専門業者の支援を受けつつ、個別に証明・検証しているというのが復旧現場の実情である。セキュリティ専門業者でない電子カルテ業者等が再接続の対応をできるとは考えづらい。なお、セキュリティ専門業者に支払う費用は、医療情報システムの規模に応じて、数百万円から数千万円といったところだろう。

- 対策としては、医療現場にサイバー攻撃等のインシデントで支払基金とのネットワークから切り離された場合の代替ネットワーク、あるいは代替システム等の次善策が必要である。

③ ソフトウェアアップデート時のシステム停止リスク

- 「診療報酬改定 DX」については、共通算定のための新たなモジュール（※ソフトウェア・モジュール）を組み込んだことでシステム全体に障害が発生するような事態を招くリスクが考えられる。先般発生したクラウドストライクの事案のように、世界的にシステム障害が発生して航空会社のシステムが止まってしまうような事態を想像してもらうとよい。

- ソフトウェアをアップデートすることにより他のシステムや既存ソフトに

影響が出る可能性については、ネットワーク機器のレベルではほぼ大丈夫だが、PC レベルでは旧バージョンが多く混在しているため、リスクはある。

- システム障害の予防には、事前の十分な検証が必要である。診療報酬改定は2年に一度の定期的なものなので十分に事前検証が可能と思う。支払基金が医療 DX に関するシステムの開発・運用主体の母体であるため、支払基金が配布されるモジュールの事前の検証を実施する体制が望ましい。

（２）医療 DX 全般に関わる中長期的な課題

① データの真正性の問題

- 医療 DX を進めるにあたって、医療機関がデジタルで取得し保存している医療データの真正性の議論は避けて通れないと思う。たとえば、ある医療機関の検査機器が２年の間、ウイルスに感染していたことが発覚したケースがあった。そのような場合、感染期間に取得・保存した医療データは適正と言えるのか、その真正性は誰が担保するのか、といった根本的な疑念・懸念が存在する。

- 感染したシステム内の医療データの真正性を確かめる技術については、追求すればきりがないが、データ同士のハッシュ値を突合したり、ウイルススキャンをして感染がないことなどを確かめたり等の方法がある。技術的にはさほど難しいことではない。

② 貯蔵される健康・医療データの廃棄ルール

- データ化された医療情報（医療データ）の廃棄についてはルール化しておかないと、各現場で体系だった廃棄はなされないと思われる。廃棄せずに無尽蔵にデータを貯蔵すると、サイバー攻撃を受けたり、情報漏洩が発生したりした際の被害が甚大に（あるいは不明に）なるリスクがある。

- データの場合、端末上で消去したからと言って完全に消えるわけでもない。医療データの廃棄については、紙媒体のカルテ情報の廃棄ルールのように、行政がルール化しておく必要がある。

③ 健康・医療に関わるフェイク情報の拡散

- 生成 AI 技術について言うと、ディープフェイク[24]や SNS による拡散と組み合わさって、フェイク医療情報のまん延につながるようなリスクがある。

- 生成 AI については、情報の信頼性の観点からの懸念が主ではないかと捉えている。

- 生成 AI を技術的に言えば、すでにある情報をかき集めて統計学を駆使して、より確からしい回答を質問に沿った形で提示するという技術である。したがって、悪意ある人が事前に偽情報を大量に流し込んでいたりすると、巷間ハルシネーションと言われるような、もっともらしいウソの情報に基づく回

[24] ディープフェイクとは、人物の動画や音声などを人工的に合成する最新の AI 処理技術である。そのリアルさから犯罪に悪用されるケースも増えている。

答が返ってくる。

- 個々の技術というよりは、それが組み合わさったソフトウェアや ICT サービスとなった時のリスクに目を向けるべきである。

3.4 その他の重要論点

① 医師会・病院団体の役割

- 政府が言う医療 DX 自体は進めるべきだが、進めるにあたってのリスクについての説明が不足しているのではないか。また、政府の説明不足はあるが、医療現場も理解への努力をすべきだし、医療の業界団体は政府の説明を咀嚼して医療現場に伝え、現場の要望を政府にモノ申すべきだと思う。

- 他に「重要インフラ」とされている業界と比べて、医療セプターの事業者はひとつひとつの事業規模が小さい。行政のガイドライン文書や注意喚起文書などの内容をそのまま渡されても理解し対策できるような人材が現場に少ない。したがって、その内容を咀嚼し、現場にわかりやすい形で伝える主体（医師会、病院団体、その他業界団体等）の存在が重要と言える。

- セキュリティ対策には、人的コストに加えて、物的コスト（システムのコスト）もかかる。個々に対策をすれば相応の費用がかかるが、たとえば地域の医師会単位でまとめて契約すれば、セキュリティ・システムのベンダーとしてもやり易いだろうし、交渉やボリューム・ディスカウントも容易になる。

- 診療所の規模からするとサイバーセキュリティ対策の個別対応は現実的には難しく、医師会や病院団体がシェアードサービスを担うことが望まれる。

- サイバーセキュリティ案件に関しては、業界の利益や団体の垣根を越えて、

協調・連携していくような体制が望ましい。たとえば、医療分野で一本化された緊急時の相談窓口の設置等が考えられる。

- 経営者から「高い」といわれるセキュリティコストをどれだけ社会通念上妥当と捉えてもらえるようにできるかが大きなポイントではないか。医師会には、医療機関経営者への啓発を期待する。

② ベンダー側の問題

- いま医療機関で起きているインシデントのほとんどが、VPN やルーター等のネットワーク機器の設定不備といった初歩的なセキュリティ設定の不備に起因している。ベンダー側の設定不備と言っても過言ではないとみている。

- 医療 DX を推進するということは、デジタル技術とネットワークを使っていくということなので、考え方の切り替えが必要である。たとえば、USB を一律使わないという考え方からセキュアな使い方をするという様に、考えを切り替えていかなければならない。その考え方の切り替えが、医療機関の方々はもちろん、システムベンダー側もできていない現状がある。

- 未だに「閉域網だから大丈夫です」と言うようなベンダーが存在する。医療機関にシステムを納入しているのはベンダーなので、ベンダー側の意識改革も進めていかないと医療 DX は進まないと思われるし、進んでもリスクが高いものになるだろう。

- 対策チェックリストについては、医療機関とシステム事業者の双方でチェッ

クする仕組みになっており、それは望ましいことだが、事業者からの提出がなされないケースが散見される。そのようなケースに対しては、医療機関が強く申し入れできるよう規制当局がバックアップするような仕掛けが必要である。現状のガイドラインでは、「民法に基づき双方で合意形成をせよ」ということになっている。システムベンダー側について言えば、医療機関側の脆弱性への対応について他人事感が強い。この件については、業界団体に期待したい。

- 情報システムの導入・調達において仕様書を書くにあたり、多くの場合、医療機関側には仕様書を書ける人材がいないため、コンサルやベンダー丸投げになっている。結果としてベンダー側の利益優先で仕様書が作成され、医療機関側には要らない・使わない機能が盛り沢山のシステムになっているようなケースがある。このようにして作成された仕様書を第三者的立場で、精査する仕掛けがあるとよい。医療機関側に負担をかけるのは現実的でないので、第三者的なチェック機関があると望ましい。

- ベンダーは、必ずしもセキュリティの専門家ではなく、他システムのことは対応しないケースが多い。

- 医療機関自らリスク評価ができないなら、適切にリードしてくれるベンダーを選んで付き合うしかないが、地場のベンダーにはサイバーセキュリティ対策を遂行する技術がないという問題もある。

- ベンダーもシステム毎にバラバラで、ベンダー内にも医療情報システム全体をみる人材がいないというケースがよくある。医療機関側に補助金を出すの

でなく、ベンダー側に責任を持たせる代わりにそちらに補助金を出すという発想もあってもよい。

③ 保険業界に期待される役割

- サイバー保険について、まだ事故事例の蓄積が少なく、保険料を決めるリスク評価基準が定まっていない状況なので、確立のための努力を続けるべき。また、保険の付帯サービスとしての医療現場のサイバーリスクの見守りサービスのようなアイデアもあり得る。

- サイバー保険に関しては、補償金額と保険料とが見合っていないという話を経営者から聞くことがある（補償金額が上限 2 億円・保険金は年間 100 万円位が相場）。このことは保険会社も認識しているようで、最近では付帯サービスで相談ができる保険商品の評判が良いようだ。被害時に代替機の手配ができるような付帯サービスもある。

- 海外ではランサムウェア被害による身代金支払いまで保険金支払いの対象になっている商品もあり、保険料が高騰しているケースもあると聞く。今後はガイドラインに準拠していると保険料が安くなる等の工夫が必要だろう。

4. 考察と提言

本章では、前章に整理したインタビュー調査に基づく専門家の意見・見解を踏まえて考察を加え、医療現場を取り巻く各ステークホルダーが具体的に何をなすべきか、各主体への提言の形でまとめた。以下に、医療機関による自助、業界団体による共助、政治と行政による公助の順に論ずる。

4.1 医療機関（自助）

院内情報システムの管理を「技術・組織体制」「人材」「予算・財源」の観点から強化する必要がある。

- **ICT 資産管理とサイバーセキュリティ対策の実装**

ICT 資産管理が確実になされておらず、院内ネットワークと外部との接続点の把握やセキュリティ対策の優先順位付けができていない医療機関が未だに存在する。結果として初歩的なセキュリティ設定の不備等による被害が発生しており、この改善が喫緊の課題である。

  - **ネットワーク構成図の作成と更新**

    リスク評価がシステム管理の入口となる。評価の基礎データであるネットワーク構成図が作成されていない、あるいは更新されていない医療機関については、まずはこの徹底を早急に図るべきである。

➢ ネットワーク出入口対策

ネットワーク構成が把握できたら、次に取り組むべきは院内ネットワークの出入口対策である。以下のシステム運営上の見直し対策によって、院内ネットワーク出入口の集約化を図るだけでも、サイバーセキュリティ上の効果が期待できる。その際、取引先との接続点にも留意する必要がある（サプライチェーン攻撃対策）。

◆ **外部との常時接続を要しない回線/機器の不要時の接続/電源 OFF**

◆ **私的利用可能な機器・端末と院内ネットワークとの物理的な分岐**

◆ **情報機器・ソフトウェアの定期的な棚卸し、不要アカウントの消去**

上記に加えて、UTM[25]の導入といった技術的予防策もある。

➢ 端末のセキュリティ対策

ネットワークの出入口を突破された場合の次なる備えとして、ウイルス対策ソフト（EDR[26]含む）の導入は必須の予防策である。

また PC 等の OS、ソフトウェアアップデートの徹底も重要である。

➢ VPN 機器等の脆弱性対策

一般的に使用されるインターネット VPN では[27]、外部との接続点から院内ネットワーク内への侵入に対する予防策が重要である。具体的には、電子メール等への警戒、認証情報（ID・PW 等）の適切な管理、アクセス権限の最小化、ネットワーク機器のファームウェア[28]のアップデート

[25] UTM（Unified Threat Management）とは、日本語で統合脅威管理と呼び、不正アクセスや疑わしい通信を検知・遮断する機能（IDS/IPS）やファイアウォール、アンチウイルス等、他の機能も備えた製品パッケージのことである。

[26] Endpoint Detection & Response の略で、PC 等の不審な振る舞いを検知し､対処するためのツールやサービス。未知のウイルス対策に有効であり、通常、ウイルス対策ソフトとセットで提供される。

[27] VPN（Virtual Private Network）とは、日本語で仮想専用線と呼び、インターネット接続の際に仮想的な専用回線を利用する技術またはそのネットワークのことである。

[28] ファームウェアとは、電子機器の内部に組み込まれ、機器の制御や動作を管理するための基本ソフト

（脆弱性情報への対応等）である[29]。

- **ネットワーク内部の監視**

  ネットワーク外部からの攻撃だけでなく、内部も監視するべきである。たとえば、医療機関のシステム管理者が知らないうちに職員等の不注意から携帯型 Wi-Fi ルーターが院内端末のインターネット接続に使われるような状況があると、そこから侵入されるリスクが生じる。このようなケースでも内部の通信状態（通信データの量や時間帯等）を監視していれば、早期に検知しやすくなる。

- **被害最小化対策**

  被害最小化対策、迅速な復旧策として以下のような対策が重要である。

  ◆ **データのバックアップ**

  厚生労働省施策でもあるオフラインバックアップ体制の整備は[30]、対策として有効である。継続運用の必要性を医療機関に引き続き意識付けしていく必要がある。

  ◆ **院内ネットワーク・セグメンテーション**

  院内ネットワークのセグメンテーションを行い、万一の場合も被害を局所化できるように、できる限り院内ネットワークを小分けして運用しておくことも予防策として検討に値する。

ウェアのことである。

[29] インターネットと直接つながず通信キャリアのネットワークを経由して VPN をつなぐサービスを利用する、さらには物理的に専用線を設けるといった手法も考えられるが、セキュリティが高まる一方で、コストは格段に高くなる。

[30] 厚生労働省医政局　事務連絡「医療機関におけるサイバーセキュリティ確保事業」の実施に係る支援対象病院の選定について（依頼）」（令和 6 年 2 月 16 日）
https://www.ajha.or.jp/topics/admininfo/pdf/2024/240219_2.pdf

◆ 有事の備え：BCP の策定とサイバー保険の検討

サイバーリスクを完全に回避することは難しい。万一の場合に備えた事業継続計画（BCP）を策定し、職員等に浸透させることが必要である[31]。なお、民間サイバー保険の活用も検討すべきポイントの一つである。

● 職員教育と経営者の意識改革

医療機関の職員のセキュリティ意識の向上を図り、システムベンダー[32]任せの実態から脱却しなければならないが、そのためにも経営者がまずは課題意識を持つことが重要である。

➢ 職員教育

厚生労働省の教育研修ポータルサイト[33]等の活用により、人材レベルの底上げを図ることが求められる。少なくとも責任者には、院内ネットワークの概要を把握し、サイバーリスクに対する危機意識を持っていることが望まれる。

➢ 経営者の意識改革

経営者の意識が変わらない限り、職員そして組織を変えることは難しい。サイバーセキュリティ対策は、まず経営者が現場にヒトやカネといった経営資源を割かないと始まらないが、現状は意識レベルの啓発は不十分と言わざるを得ない。

---

[31] 厚生労働省（2024）「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」（令和６年６月）https://www.mhlw.go.jp/content/10808000/001261299.pdf

[32] 組織の情報システムの構築・運用などの業務を一括して請け負う事業者のこと（以下「ベンダー」）。

[33] 医療機関向けセキュリティ教育支援ポータルサイト　https://mhlw-training.saj.or.jp/

実際の事故に際して、システム管理ができていないケースではどのような事態が起き、どれくらいの被害が発生するのかといったことに経営者自身が関心を持ち、セキュリティリスクへの対応費用を経営コストとして認識することが重要であろう[34]。

- **ベンダーの活用**

システムの所有者、すなわち医療機関が全てのリスクに主体的に対応するのが原則である。しかし、医療機関がサイバーセキュリティ対策を適切に実施することは人材面で難しいこと、ベンダーにも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としての責任があることから、専門家であるベンダーに委託するのが現実的である。ベンダーへの委託内容を保守契約上明確にし、医療機関側が費用も負担するというのが解決策ではないだろうか。

- **保守契約への明記**

保守契約上の双方の責務を明らかにする具体的手法としては次の通りである。（1）現状のチェックリストに挙げられた項目のうち[35]、自院での対応が難しい項目を保守契約上の委託事項に明記する。（2）自院の実情に合わせて考慮すべき点を箇条書きにし、それらへの対応を保守契約に明記する。

- **プライムベンダーの設置**

複数の導入システム毎にベンダーが分かれているような場合には、総合

[34] 坂口ら（2023）
[35] 厚生労働省「医療機関におけるサイバーセキュリティ対策チェックリスト」
https://www.mhlw.go.jp/content/10808000/001253950.pdf

的な相談先となるベンダー（プライムベンダー）を設置し、保守契約上明記することが有効である。たとえば、ソフトのアップデート時におけるシステムの安全性担保[36]についても、プライムベンダーが取りまとめて、他のシステムへの影響の検証も含め、対応するという契約が望ましい。

- **サイバーセキュリティ対策をベンダーに委託する場合の費用の目安**

◆ 大規模病院

システムの規模ごとに費用は大きく異なり、一概にいうことは難しい。なお一般的には、保守契約費用は導入コストの 5～7%くらいが目安とされている。また、大規模病院を対象にサイバーリスクを評価するだけでも、１回当たり 500 万円～といった費用感だという。

◆ クリニック、中小病院 （費用詳細は 27-29 ページ参照）

■A 社のランサムウェア対策総合サービス

（院内設置端末台数 20 台とした場合の導入コスト）

699,600 円*／年＋60,500 円（リスクアセスメントサービス１回）

＊UTM の設置、ウイルス対策ソフト（含む EDR）の導入、リモートアクセス対策サービス（インターネット VPN の場合）の導入、ランサムウェア対策バックアップサービスの導入

■B 社（診療所レベルのセキュリティ対策の年間の費用感）

70 万円～180 万円*／年

＊ウイルス対策ソフトの導入、IDS／IPS の設置、サーバの脆弱性対策、

[36] ソフトウェアのアップデートは本来、当該システムだけでなく接続する他のシステムや既存ソフトウェアが不具合を起こさないかの動作確認をしてから実施すべきである。

ふるまい検知（EDR)、パックアップ・オフライン保存

■C 社（院内設置端末台数 20 台レベルのセキュリティ対策の年間の費用感）

68 万円～160 万円*／年

＊ウイルス対策ソフトの導入、メール等への警戒、IDS／IPS の設置、サーバの脆弱性対策、ふるまい検知（EDR)、パックアップ・オフライン保存（外付け HD･1TB）

- **その他の取り組み**

  - **セキュリティに詳しい人材のシェア**

    医療情報システムに詳しい人材が地域の他の医療機関をサポートできるよう、積極的に副業・兼業を認めることで、その処遇向上に繋げる仕組み作りが考えられるのではないだろうか。

  - **サイバー攻撃を受けた職員のメンタルヘルスケア**

    被害を受けた医療機関の職員は、想定外の激務に追われるばかりか、患者からの苦情にも対応を要する等、プレッシャーに晒されるため、メンタルヘルスへの心配りが必要である。

4.2 業界（共助）

（１）医療界（医師会・病院団体）

医療機関のサイバーリスクや想定される被害軽減、事業継続のための支援に一層注力することが期待される。

- **医療 DX とサイバーリスクに関する情報の伝達**

医師会や病院団体がその内容を咀嚼し、現場にわかりやすい形で伝える役割を引き続き担うべきである。たとえば、日本医師会で作成した「サイバーセキュリティ支援制度概要および利用マニュアル」[37]、「セキュリティガイドライン相談窓口」[38]、「令和 6 年度版 医療機関におけるサイバーセキュリティ対策チェックリスト」及び「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル ～医療機関・事業者向け～」[39]等の周知活動が該当する。

- **集団価格交渉による対策費用低減**

サイバーセキュリティ対策を個々にするのでなく、地域の医師会・病院団体等でまとめて契約する仕組みを作ることで、システムベンダー等との価格交渉による費用低減の効果が期待できる。

- **医療機関経営者向けの啓発活動**

医師会・病院団体は医療機関経営者に対し、セキュリティリスクへの対応費用を必要な経営コストと捉えるよう、啓発する役割を積極的に果たしていくべき

[37] 日医発 第 1414 号（情シ）2023 年 11 月 8 日
[38] 日医発 第 1414 号（情シ）2023 年 11 月 8 日
[39] 日医発 第 361 号（情シ）2024 年 5 月 17 日

である。

- **支援人材の受け皿**

地域の経済団体や行政（含、都道府県警）との連携・基金の活用等による人材シェアを検討する場合に、医師会や病院団体が当該人材の受け皿を担うことも検討に値する。

- **有事の直接的支援**

サイバー攻撃を受けた医療機関の相談窓口の設置や資金援助等、有形無形の支援制度を業界で構築することが考えられる。例えば、すでに実施している日本医師会のサイバーセキュリティ支援制度（サイバーセキュリティ対応相談窓口【緊急相談窓口】、サイバー攻撃一時支援金・個人情報漏えい一時支援金制度等）[40]が該当する。

（２）情報システム業界

- **一部ベンダーの質の改善**

医療現場のセキュリティに詳しい人材不足を補う役割を業界には望みたいが、ベンダーの現状に対しては、むろん一部の事案とはいえ、以下に列挙するような能力面、意識面での問題点を強く指摘する意見が目立った。業界として、改善に向けた取り組みに期待したい。

- ◆ ベンダー側の設定不備に起因するサイバーインシデントの発生
- ◆ サイバーセキュリティ対策を遂行する技術がないベンダーの存在

[40] 日医発 第 470 号（情シ）2023 年 6 月 5 日

◆ ベンダー側の利益優先で作成されるシステム仕様書の存在

◆ 自社が納入していないシステムのサイバーセキュリティ対策への不関与

◆ 顧客のサイバーセキュリティ対策に対する他人事の意識

（３）保険業界

- **適正なリスク計算のためのデータ・事例の蓄積**

保険業界を挙げて、適正な料率体系の確立のための努力を続けることが望まれる。サイバーリスクを完全に回避することは難しく、リスクの移転という意味でも、保険加入が望ましいと考えるが、まだまだ事故事例の蓄積が少なく、保険料を決めるリスク評価基準が定まっていない状況である。

- **リスク低減につながる付帯サービスの充実**

サイバー保険に関して、単に事後の金銭的な補填という保険機能だけでなく、リスク低減に繋がる付帯サービスの充実を期待したい。現在提供される同保険にも一定の現物サービスが付帯されているが[41]、さらに拡充されていけば、サイバーリスクに対する事前・事後の備えを総合的に提供する商品に、位置づけが進化する可能性がある。

[41] 平常時から利用可能な電話相談窓口サービス、コンピュータセキュリティに対応するための専門組織（CSIRT：Computer Security Incident Response Team）の設置代替機能の提供等が該当する。

4.3 政治・行政（公助）

省庁間を超えて、また中央と地方が一体となり、医療機関のサイバーリスクや想定される被害軽減、事業継続のための仕組み作りに取り組むことを求めたい。

- **司令塔組織（NISC）の見直しと強化**

政策の司令塔組織である内閣サイバーセキュリティセンター（NISC）の体制を見直し、再編・強化することで関係省庁間の連携をより円滑にすべきである。政府の司令塔には、世界中の専門組織（CSIRTs）[42]と連携してサイバーリスクに関する情報と対処法を集約し、所管省庁と業界団体のネットワークを通じて重要インフラを担う各産業の現場まで伝え、対策の実装まで見守る役割が期待される。今回の調査では、NISC の人員や組織、情報収集能力に関するネガティブな意見が目立った[43]。平時からの情報・ノウハウの集約は、セキュリティ確保策の要である。政府の司令塔に必要な人材と組織体制のあり方から、見直しが求められる。

- **脆弱性情報の確実な伝達と現場の対策実装サポート**

情報通信機器やソフトウェアの脆弱性に関わる情報は、医療現場がサイバーリスクに対処するにあたっての最重要情報のひとつである。医療現場に必要な情報が確実に伝わり、対策が実装されるまでの流れの再確認が求められる。行政発の注意喚起文書が医師会・病院団体等を通じて各医療現場に回付されているのが現状だが、(1) 伝達経路の多様化、(2) 対応の緊急性等の情報付加、(3) 現

[42] CSIRT とは、Computer Security Incident Response Team の略。コンピュータのセキュリティ・インシデントに関わる活動を行っている組織のことであり、世界各国に存在し、ネットワーク化されている。
[43] NISC の機能不全については、次のような記事もある。日本経済新聞「政府サイバー組織、被害収集ままならず　霞が関で影薄く」(2023 年 4 月 13 日電子版)

場の対策実装支援といった視点でのさらなる工夫を求めたい。たとえば、(3)の具体策として、すでに厚生労働省が電子カルテ導入病院を対象に実施している「①外部ネットワークとの接続の安全性の検証・検査および②オフライン・バック アップ体制整備の支援」[44]について中小病院や診療所への対象拡大が考えられる。

- **情報システムの仕様書をチェックする第三者機関の創設**

医療機関に導入される情報システム仕様書の妥当性を判断する第三者機関の創設を検討してはどうか。医療現場に専門性を有する人材が少ないため、仕様書の作成は販売業者やコンサルタント任せになっているケースが多い。それゆえ、自院のシステムの構成を把握しておらず、管理体制もセキュリティ対策もおざなりな医療機関が少なくない。自院のシステム構成に関する認識の欠如は有事の対応の遅れにもつながる。また、業者の利益優先で組まれたシステムは、不要な機能も盛り込まれ、サイバーリスクを増大させがちである。政府主導で、中立な第三者による仕様書チェックの仕組みの構築と導入を展望すべきである。

- **SOC の制度化と医療機関向け地域別 SOC の構築支援**

サイバー空間におけるセキュリティ上の不審な動きを監視する SOC（Security Operation Center）を制度化し、地域毎に複数の医療機関をまとめて監視する SOC を設置する仕組みを構築すべきである。個別の医療機関にセキュリティ・システムが導入されても、その 24・365 体制での監視や有事の対応には、また別に専門人材が必要である。かかる人材の確保を個々の組織に任せ

[44] 厚生労働省医政局　事務連絡「医療機関におけるサイバーセキュリティ確保事業」の実施に係る支援対象病院の選定について（依頼）」（令和 6 年 2 月 16 日）
https://www.ajha.or.jp/topics/admininfo/pdf/2024/240219_2.pdf

るのは、求められる人材の専門性やコスト面を考慮しても現実的ではない。医療は地域住民の生活インフラである。そのインフラを支える医療機関を取り巻くサイバー空間のセキュリティ監視の体制構築は、公的な財源で整備されることが望ましい[45]。たとえば、経産省・IPA のサイバーセキュリティお助け隊サービスの活用等の具体策が考えられる[46]。

- **有事の相談窓口の一本化**

サイバーセキュリティに関わる有事の相談窓口の一本化が必要である。24 時間 365 日対応可能な行政の相談窓口を設置し、被害現場に負荷をかけずとも、適時・適切な情報が省庁間を超えてワンストップで連携される体制が望ましい[47]。現状、セキュリティ有事に医療現場が報告・連絡・相談を求められる行政の窓口は複数省庁に跨って多岐に渡り、限られた人員と時間で対応に追われる現場の負担となっている。時間帯によっては直ぐに連絡がつかないこともあり、初動の遅れが事態の深刻化を招くケースもある。

- **財源の確保と国民・患者向けの説明**

リスクのあるすべての医療現場にセキュリティ・システムが導入されるための財源確保が必要である。2023 年 4 月からサイバーセキュリティの確保は医療機関管理者の法的義務となっている。一方で、今回の調査では警察庁が指摘する水準のセキュリティ・システムには、導入費用に加えて診療所規模で年間 100 万円規模の運用コストがかかるとの見解を得た。医療 DX の推進を継続するのであれば、医療現場への ICT とデジタル技術の導入に伴うリスクについても国民

[45] ここで提案する SOC の仕組みは、物理空間における警察のパトロールに近い“公共財”である。
[46] 厚生労働省（2023b）
[47] 必要に応じて、被害現場への専門家チームの派遣や代替機の提供につながる体制構築が望ましい。

に丁寧に説明し、必要な財源確保を行うのが、政治と行政の責務であろう。なお、システムの導入コストについては補助金を活用し、運用コストについては診療報酬上のプラス評価で賄うのが望ましい。

- **DX が進展する未来に向けた健康・医療情報の政策議論**

社会全体の DX が進展する未来を見据えて、健康・医療に関わるデータの（1）廃棄のルール、（2）真正性の担保、（3）フェイク情報拡散への対処についての政策議論を開始するべきである。（1）についてはデジタル化されて無尽蔵に貯蔵される健康・医療情報の定期廃棄のルール化、（2）についてはハッキングされた健康・医療情報の真正性担保の手順や基準の策定、（3）についてはディープフェイク等の AI 技術と SNS 等での拡散を組み合わせた巧妙な偽情報拡散に対する法整備等が、喫緊の論点となろう。

4.4 結語

以上、医療を取り巻く「自助」「共助」「公助」の順に、それぞれを担う主体に向けて、考察と提言をまとめた。

今後、いかに ICT 化とデジタル化が進もうとも、医療が平時の国家安全保障であることには変わりがない。安心・安全なデジタル・プラットフォームの構築は国、すなわち政治と行政の責務であり（公助)、プラットフォームにつなぐまでの現場でのリスク管理は、情報システム業界や医療界の業界団体や個別のベンダーとの協力体制のもと（共助)、原則として、各医療機関の責務である（自助)。今後、政府が推進する医療 DX を現場が安全に実装するためにも、国に対しては各医療機関がサイバーリスクに適切に対処し得るだけの財源の確保をあらためて望みたい。

謝　辞

誠にご多忙な中、インタビュー調査への貴重なご協力を賜りました以下の皆様方に、この場をお借りして深謝申し上げます。なお、言うまでもなく、本文中のすべての誤りは筆者らの責に帰するものです。

松山征嗣 様（一般社団法人医療サイバーセキュリティ協議会 常任理事、元・トレンドマイクロ株式会社 シニアマネジャー[当時]）
竹下洸 様（東日本電信電話株式会社 ビジネス開発本部 CX ビジネス部 セキュリティサービス担当 担当課長）
桑名潤 様（東日本電信電話株式会社 ビジネス開発本部 CX ビジネス部 セキュリティサービス担当 チーフ）
岩崎敏彦 様（株式会社 NTT Risk Manager コンサルティング事業部 担当部長）
北山隆 様（株式会社 NTT Risk Manager コンサルティング事業部 担当部長）
猪俣敦夫 様（大阪大学 D3 センター　教授，CISO）
高柳大輔 様（独立行政法人情報処理推進機構 セキュリティセンター センター長）
菅野和弥 様（独立行政法人情報処理推進機構 セキュリティセンター リスクマネジメント部 部長）
高橋将 様（独立行政法人情報処理推進機構 セキュリティセンター 企画部 副部長）
加賀屋伸一郎 様（独立行政法人情報処理推進機構 セキュリティセンター 普及啓発・振興部 副部長）
萩原健太 様（一般社団法人ソフトウェア協会 副会長）
香野剛 様（デロイト トーマツ リスクアドバイザリー合同会社　ガバメント&パブリックサービシーズ　パートナー）
渡辺典之 様（デロイト トーマツ リスクアドバイザリー合同会社　ヘルスケア　パートナー）
竹内友之 様（デロイト トーマツ リスクアドバイザリー合同会社　ヘルスケア　パートナー）
根本大介 様（デロイト トーマツ リスクアドバイザリー合同会社　ヘルスケア　マネージングディレクター）
鈴木紀秀 様（デロイト トーマツ リスクアドバイザリー合同会社　ヘルスケア　シニアマネジャー）
鈴木邦彦 様（デロイト トーマツ リスクアドバイザリー合同会社　ヘルスケア　マネジャー）

（順不同）

【参考資料・文献リスト】

國谷武史（2024）「サイバー攻撃で暗躍するイニシャルアクセスブローカー、犯罪凶悪化の温床にも」ZDNET（2024-10-18）
https://japan.zdnet.com/article/35225056/

警察庁サイバー警察局（2023）「サイバー事案の被害の潜在化防止に向けた検討会報告書 2023」（令和５年３月）
https://www.wic-net.com/material/static/00008873/00008873.pdf

警察庁サイバー警察局（2024）「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」（令和６年９月）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

厚生労働省（2023a）「医療情報システムの安全管理に関するガイドライン　第6.0版（令和５年５月）」
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

厚生労働省（2023b）「厚生労働省における医療機関のサイバーセキュリティ対策にかかる取組について」
https://mhlw-training.saj.or.jp/wp/wp-content/uploads/2023/02/01-mhlw.pdf

厚生労働省（2024a）「医療機関におけるサイバーセキュリティ対策チェックリスト（令和６年５月）」
https://www.mhlw.go.jp/content/10808000/001253953.pdf

厚生労働省（2024b）「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～（令和６年５月）」
https://www.mhlw.go.jp/content/10808000/001253953.pdf

厚生労働省（2024c）「【医療機関用】サイバー攻撃を想定したBCP策定の確認表（PDF）（令和６年６月）」
https://www.mhlw.go.jp/content/10808000/001261299.pdf

厚生労働省（2024d）「【医療機関用】サイバー攻撃を想定したBCP策定の確認表のための手引き（令和６年６月）」
https://www.mhlw.go.jp/content/10808000/001261301.pdf

厚生労働省（2024e）「医療情報システム部門等におけるBCPのひな形（PDF）（令和６年６月）」
https://www.mhlw.go.jp/content/10808000/001261302.pdf

サイバーセキュリティ戦略本部（2024）「重要インフラのサイバーセキュリティに係る行動計画」（2024 年 3 月 28 日改定）
https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf

坂口一樹、堤信之、原祐一（2023）「医療機関へのサイバー攻撃の事例研究：民間病院診療所の被害事例に学ぶ」日医総研リサーチレポート No.316
https://www.jmari.med.or.jp/wp-content/uploads/2023/04/RR136.pdf

情報処理推進機構（2024）「情報セキュリティ 10 大脅威 2024」
https://www.ipa.go.jp/security/10threats/10threats2024.html

三井物産セキュアディレクション（2024）「暴露型ランサムウェア攻撃統計 CIG マンスリーレポート 2024 年 8 月号」
https://www.mbsd.jp/report/files/MBSD_Ransomware_Statistics_CIG_MonthlyReport_2024_08_JPN_Rev.1.00.pdf

巻末資料：インタビュー・ガイド

1. 昨今のサイバー攻撃の類型と特徴

2. 医療ＤＸの進展に伴うサイバーリスクについてのご見解
（1） 現在の政府（厚労省）の医療ＤＸ及び関連施策に伴うリスク
（ア） 全国医療情報プラットフォーム
（イ） 電子カルテ情報の標準化
（ウ） 診療報酬改定ＤＸ
（エ） オンライン資格確認（＊）
（オ） その他
（2） その他の先進的デジタル技術、ＩＣＴの利活用に伴うリスク
（ア） 生成ＡＩ等のＡＩ技術
（イ） ＩｏＴ機器
（ウ） 遠隔診療（オンライン診療）
（エ） ロボティクス技術
（オ） その他

3. 現状の行政・公的機関のセキュリティ対策・体制に関するご意見
（1） 内閣府　内閣サイバーセキュリティセンター（NISC）の体制
（2） 情報セキュリティに関わる注意喚起文書の伝達
（3） 重要インフラ事業者グループ（セプター）
（4） 厚労省　医療機関向け安全管理ガイドライン
（5） 総務省・経産省　医療情報システム事業者向けガイドライン
（6） 厚労省　教育・研修ポータルサイト
（7） 厚労省　サイバーセキュリティ対策チェックリスト
（8） 厚労省　医療情報システム部門　事業継続計画（BCP）のひな型
（9） 厚労省　医政局　サイバー攻撃を受けた際の連絡先
（10） 情報処理推進機構（IPA）　技術相談窓口
（11） 警察庁　サイバー警察局
（12） 経産省　サイバーお助け隊
（13） 内閣官房「能動的サイバー防御」の導入
（14） その他（デジタル庁、防衛省、公安調査庁、文部科学省　等）

4. 医療機関のリスクマネジメント体制についてのご意見
（1） 人員、組織体制

（2）　情報システム・関連機器の管理体制
（3）　情報通信ネットワークの管理体制
（4）　医療情報の管理体制
（5）　外注業者の管理体制
（6）　その他、病院・診療所の組織的な特性に関連して

5.　民間のサイバー保険とその付帯サービスについてのご意見

6.　業界団体に期待されること、実施すべきこと
（1）　医師会や病院団体
（2）　医療機器や医療情報システムの業界団体
（3）　その他の業界団体（損保業界？　テック業界？　経済界？）

7.　その他の重要論点

以上