2023 年 4 月 11 日

日医総研リサーチレポート　No.136

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

坂口一樹（主任研究員）、堤　信之（客員研究員）、原　祐一（副所長）

要　旨

◆ 本稿は、最近（2021 年下半期～2022 年上半期）、サイバー攻撃の被害に遭った医療機関を対象とした事例研究である。民間の病院・診療所の 3 事例を精査し、現状の問題点と将来に向けた課題解決のヒントを抽出した。

◆ 問題点としては、次の 5 点が挙げられる。(1) サイバー攻撃からの復旧には多大なコストと労力がかかる（数千万円規模）。(2) 医療機関で情報システム管理にあたる人員体制が手薄である。(3) 行政から事前に注意喚起がなされていた既知の脆弱性が侵入経路となっている。(4) 情報システムやネットワーク機器の販売業者・保守業者との間にサイバー攻撃時の復旧作業や費用負担に関する取り決めがなされていない。(5) サイバー攻撃の被害に遭った医療現場への支援という点で、行政の対応や連携は問題含みである。

◆ 将来に向けたヒントとしては、(1) サイバー攻撃を想定した非常時行動計画（BCP）の策定が有事に役立ちうること。(2) 地域医療連携システムにアップロードした診療データが、有事のバックアップとして活用可能であること。(3) 誰もが標的になりうるリスクとして、サイバーリスクに対する経営陣と医療従事者の意識改革が必要なこと、の 3 点が挙げられる。それらに加えて、聴取した情報を基に、官公庁や公的機関、団体からあるべき支援と情報提供について、具体的にまとめた。

◆ 以上をベースに考察を加え、(1) 行政間の連携を強化し、専門機関と連携して被害現場を支援すべきこと、(2) 行政が発信するシステム等の脆弱性情報が医療現場に周知されるまでの流れを再確認すべきこと、(3) BCP 策定や机上訓練、対策チェックリストの充実等の現場の対策支援を充実させるべきこと、(4) 医療機関のセキュリティ対策に関する人材と費用を手当てすべきこと、の 4 点を提言した。

目　次

１．背景と目的

１．１　背景と問題意識

昨今、サイバー攻撃の脅威は世界中で増大し、過激化の傾向にある[1]。日本も同様の状況にあり、2022 年 9 月～11 月末のサイバー攻撃の標的数は世界 2 位であったと報告されている[2]。警察庁によれば[3]、昨今、国内ではサイバー攻撃の中でもランサムウェアによる感染被害が増加傾向にあり、事業活動の停止・遅延等、社会経済活動に多大な影響を及ぼしている。

医療界も例外ではない。警察庁によれば、2022 年の医療・福祉分野におけるランサムウェア被害の届出件数は 20 件（全産業で 230 件）であった。昨年は、大阪急性期・総合医療センターのランサムウェア被害事件（2022 年 10 月）が大きく報道された[4]。また、病院だけではなく、診療所が攻撃のターゲットとなった事例も報じられている[5]。

これらの事件や徳島県のつるぎ町半田病院事件（2021 年 11 月）を通じて[6]、医療機関がサイバー攻撃を受けることにより直接的な損害（業務継続費用、被害復旧費用等）にとどまらず、患者が医療を受けられないことによる健康被害や患

---

[1] WIRED「ランサムウェア集団による“オンライン恐喝”が、さらに凶悪化する新局面に突入した」（2023 年 3 月 16 日）https://wired.jp/article/ransomware-tactics-cancer-photos-student-records/
[2] BlackBerry（2022）
[3] 警察庁（2023）
[4] 給食委託事業者の VPN 装置がランサムウェアの侵入口となり、当病院の電子カルテなどが暗号化され、外来診療や各種検査の停止を余儀なくされ、復旧には 2 カ月を要した。
日経クロステック「ランサムウェア被害の大阪の病院、初動から全面復旧まで 2 カ月間の全貌」（2023 年 1 月 27 日）https://xtech.nikkei.com/atcl/nxt/column/18/01157/012600079/
[5] NHK「沼津市内の医療機関にサイバー攻撃　電子カルテシステムに障害」（2022 年 11 月 8 日）https://www3.nhk.or.jp/lnews/shizuoka/20221108/3030018212.html
[6] つるぎ町立半田病院「コンピュータウイルス感染事案有識者会議調査報告書について」（2022 年 6 月 7 日）https://www.handa-hospital.jp/topics/2022/0616/index.html

者等の個人情報漏洩、関連する風評被害等も懸念されることが意識されるようになった。加えて、当該医療機関が地域で担う公的な役割を遂行できないことにより、地域医療全体に重大な影響を及ぼす怖れがある。

このような医療界における懸念を払拭することは、オンライン資格確認やマイナンバーカードの健康保険証活用の本格稼働等を端緒とする医療 DX を進展させるための大前提と言えよう。そのためには、医療界に内在するサイバーセキュリティ対策上の課題を明らかにすることが重要である。

医療機関のサイバーセキュリティについて、これまで日医総研では実態調査を基に、組織体制およびリスクマネジメント上の課題を確認してきた[7]。本稿ではさらに踏み込み、実際にサイバー攻撃の被害に遭った医療機関から生の情報を直接聴取した。サイバー攻撃による被害の詳細が公表されている資料は現状限られていることから、筆者ら独自に情報収集することとした。

１．２　本稿の目的と構成

本稿の目的は、医療機関がサイバー攻撃の被害に遭った事例を収集、それらの背景事情を精査、問題点を抽出し、将来に向けた提言を行うことである。

本稿の構成は以下の通りである。第 2 章では、調査対象とインタビュー調査の実施方法について述べる。第 3 章では、今回対象とした３つの被害事例について、各事例の概要を表に整理し、被害の発覚から復旧に至る経過やサイバー攻撃の侵入経路、その他事例の特徴について解説を加える。第 4 章では、事例から

[7] 坂口・堤（2021）、坂口ら（2021）

抽出した現状の医療現場の問題点と将来の向けたヒントについて、主要な論点ごとに整理し、記述する。第 5 章では、それまでの議論をベースに、行政向けの提言を行う。

２．対象と方法

２．１　調査対象

調査対象は、サイバー攻撃の被害に遭った国内の病院２施設、診療所１施設の計３医療機関である。インタビューに先立ち実施した文献調査および日医総研のネットワークを通じて選定し、依頼した。調査内容の機微性と秘匿性を考慮し、インタビューに際して聴取内容は政策提言や調査研究等の公益・学術目的のみに使用することとし、報告書等の作成・公表にあたっては個人や組織が特定できない形で執筆することを条件とした。

２．２　調査方法

調査方法は、半構造化面接法を採用した。対象者には、あらかじめ調査趣旨とインタビュー・ガイド（巻末資料として添付）を送付した。項目のみの箇条書きと口語の質問調の２種類のガイドを準備し、場面によって適宜使い分けた。

主な調査項目は、下記の通りである。

1. **サイバー攻撃を受けてから復旧に至るまでの経緯**
2. **攻撃への対応、システムの復旧に当たった人員体制**
3. **外部の業者や公的機関、専門家等からの助言や支援**
4. **医療情報システムその他の物的な被害状況**
5. **サイバー攻撃のシステムへの侵入経路とその特定**
6. **システムの復旧に要した費用と時間**
7. **攻撃を想定した事前の備えの状況（管理体制、保険、教育訓練、BCP）**
8. **官公庁や公的機関、団体からのあるべき支援や情報提供**

調査期間は 2022 年 9 月から 2022 年 12 月である。新型コロナウイルス感染症の感染状況と聴取内容の機微性・秘匿性の双方を考慮し、インタビューの実施場所は、すべて対象者の要望に応じた。結果、１件がオンライン、２件が現地での実施となった。

聴取内容の正確性と客観性の担保のため、すべて複数のインタビュアー体制（2 名または 3 名）で実施し、聴取内容については毎回記録メモに起こした後、当該インタビューに参加した複数の眼でチェックした。なお、先方から要望があった場合、確認のため事後的に記録メモを対象者に送付した。

３．事例の概要

３．１　事例Ａ（病院）

図表 3-1 は、一つ目の被害事例（事例Aと呼ぶ）の概要である。事例は 2022 年上半期に発生した。攻撃を受けたのは、地方中核都市にある医療法人立の中小規模の病院（99 床未満）である。攻撃の種類はランサムウェア（Cring）であり、電子カルテシステムのサーバにあるデータが、同一サーバ内にあったバックアップごと暗号化された。フォレンジック調査の結果、VPN 機器の脆弱性を突かれて侵入されたとの推測だった。この侵入経路は、すでに行政からの注意喚起がなされていた既知の脆弱性であった。

事例 A で直接の対応に当たったのはシステム責任者 1 名である。そこに内部ではシステムに詳しい放射線技師 1 名、外部からは電子カルテやネットワーク機器ベンダーから複数のメンバーが支援に駆け付けた。その他、個人情報漏洩対策で弁護士を新たに雇用し、保険会社から紹介された業者にフォレンジック調査を外注した。また、厚労省医政局に連絡し、IPA（情報処理推進機構）に相談、都道府県警のサイバー犯罪窓口に通報を行った。

本件では、攻撃の 2 週間前に別システムの更新作業があり、業者が外部に保存していたバックアップデータが偶然残っており、そこから復旧できた。また、薬や検査のオーダーについて、一部紙カルテ運用を残していたことも復旧作業に役立った。しかし、これらの偶然に恵まれたにもかかわらず、復旧には保険では賄いきれない程の多大なコストと労力を要した。

図表 3-1. 事例Ａ（病院）の概要

<table>
<tr><td>被害の時期</td><td>2022 年上半期</td><td>時間帯</td><td>早朝</td></tr>
<tr><td>所在地</td><td>地方中核都市</td><td rowspan="6">病床規模</td><td rowspan="6">☐病院　500 床以上
☐病院　200～499 床
☐病院　100～199 床
☑病院　99 床未満
☐有床診療所
☐無床診療所</td></tr>
<tr><td rowspan="5">開設主体</td><td rowspan="5">☐国公立・公的
☐社会保険関係団体
☑医療法人
☐その他の法人
☐個人</td></tr>
</table>

攻撃の種類	ランサムウェア（Cring）
侵入経路	VPN 機器（Fortinet 社製 FortiGate）
被害を受けたシステム	電子カルテシステム（サーバ） データのバックアップはとっていたが、同一サーバ内にミラーリングする運用にしたため、バックアップデータも暗号化された。
間接的に被害を受けたシステム	上記とつながるすべての端末および医療情報システム 同一サーバ内にあった共有ストレージ（各部署の業務ファイルの保管場所）も同時に暗号化された。
復旧時間	診療可能となるまでに１日 システム再構築とデータ復旧までに２週間
復旧費用	約 5,000 万円 内訳は、①データ復旧と新システム購入費用に 2500 万円、②外注業者の費用および院内の人件費に 400～500 万円、③個人情報漏洩対策費（詫び状郵送やコールセンター設置、弁護士費用）2,000 万円
対応人員（内部）	システム責任者１名（システムに詳しい放射線技師１名が支援）
対応人員（外部）	電子カルテベンダー：３名 VPN 機器ベンダー：１名
その他外部の支援者	顧問弁護士から紹介された弁護士：個人情報漏洩対策を支援。 フォレンジック業者：保険会社からの紹介があり、調査を外注。 民間保険会社：個人情報漏えい保険、フォレンジック業者を紹介。
行政機関への連絡相談	厚労省医政局に連絡し、IPA に相談。 都道府県警のサイバー犯罪窓口に通報および相談。
サイバー保険への加入	加入あり。　ただし、個人情報漏洩被害のみを補償する保険だった。したがって被害額のうち、個人情報漏洩対策費用の 2,000 万円はカバーされたものの、残りの 3,000 万円は持ち出しとなった。
役職員向け教育訓練	なし。　震災等を想定し、ICT 機器が使えなくなった場合の教育訓練が必要だと議論していたが、実現には至っていなかった。
非常時行動計画（BCP）	あり。　ただし、サイバー攻撃ではなく自然災害を想定した BCP だった。今後はサイバー攻撃時の対応を盛り込む予定。
その他特記事項	偶然、サイバー攻撃を受けた２週間前に院内の別システムの更新作業があり、電子カルテ会社が外部にバックアップを取っており、そこからデータ復旧できた。また、一部紙カルテを併用（薬や検査のオーダー内容を紙カルテに貼付）していたことも、復旧作業に役立った。

３．２　事例Ｂ（病院）

図表 3-2 は、二つ目の被害事例（事例Ｂと呼ぶ）の概要である。事例は 2022 年上半期に発生。攻撃を受けたのは、大都市圏近郊にある医療法人立の中小規模の病院（100-199 床）である。攻撃の種類はランサムウェア（LockBit2.0）であり、電子カルテシステムのサーバにあるデータが暗号化された。システムとつながるオーダリングや医事会計のシステムも使えなくなり、復旧までの約 2 か月間は紙カルテと代替機のレセコンで凌いだ。都道府県警（以下、警察）の調査では、侵入経路は VPN 機器の脆弱性である可能性大との結果だった。事例Ａと同様、行政から注意喚起がなされていた既知の脆弱性であった。

事例Ｂの被害病院にはシステム専任の担当者はおらず、対応に当たったのは事務長を中心として立ち上げた対策本部のメンバーだった。外部からは電子カルテベンダーからサポート要員が派遣され、復旧を支援した。警察への被害届や個人情報漏洩対応で弁護士にも相談した。警察からは全面的な協力を得られたが、厚労省や IPA からは具体的な助言や支援は得られなかった。

本件で注目すべきは、システム専任者はいなかったものの、システム障害を想定した机上訓練をしており、災害医療の原則に沿って対策本部を立ち上げ、粛々と復旧作業を進行した点にある。時間とコストの観点からフォレンジック調査を実施しない意思決定をした一方で、警察の協力を得て侵入経路を特定、ダークウェブ調査で個人情報漏洩がないことを確認、地域医療連携のクラウドデータを活用しつつ、手書きと代替機レセコンで、データ復旧までの 2 カ月を凌いだ。ただし、それでもデータ復旧費用だけで 5 千万円、その他の費用も含めると 7 千万円強のコストと労力を要した。時間の制約があったため、十分精査できなかった事情はあるが、データ復旧費用の額と内訳はやや不透明である。

図表 3-2. 事例Ｂ（病院）の概要

被害の時期	2022 年上半期	時間帯	深夜～早朝
所在地	大都市圏近郊	病床規模	□病院　500 床以上 □病院　200～499 床 ☑病院　100～199 床 □病院　99 床未満 □有床診療所 □無床診療所
開設主体	□国公立・公的 □社会保険関係団体 ☑医療法人 □その他の法人 □個人		
攻撃の種類	ランサムウェア（LockBit2.0）		
侵入経路	VPN 機器（Fortinet 社製 FortiGate）		
被害を受けたシステム	電子カルテシステム（サーバ） サーバの管理画面に LockBit2.0 の表示が出ており、一見してサイバー攻撃を受けたと分かった。		
間接的に被害を受けたシステム	上記とつながるすべての端末および医療情報システム オーダリングシステム（検査や処方）と医事会計システム（レセコン）も使えず、紙カルテ運用とレセコン代替機で凌いだ。		
復旧時間	当日早朝に診療可能と判断し、診療は休止しなかった。 システム再構築とデータ復旧までに２か月間。復旧までは紙カルテでの運用とした。		
復旧費用	約 7,000 万円強 内訳は、①ダークウェブ調査費用に数百万円、②サーバのデータ復旧費用に約 5,000 万円（基本料金 3,800 万円＋成功報酬 1,000 万円）、③残業代の増加その他の費用に約 2,000 万円		
対応人員（内部）	事務長および対策本部メンバー（理事長・院長・各部署の長）		
対応人員（外部）	電子カルテベンダーからサポート要員が派遣		
その他外部の支援者	警察からの全面的な協力・支援があった。一方、厚労省は報告を求めるのみで助言や支援はなく、IPA からも特に具体的なアドバイスはなかった。個人情報漏洩や被害届提出にあたって弁護士にも相談した。		
行政機関への連絡相談	厚労省医政局に連絡し、IPA に相談 都道府県警のサイバー犯罪窓口に被害届を提出し相談		
サイバー保険への加入	加入あり。　ただし、補償上限が 1,000 万円までのプランであったため、残りは持ち出しとなった。		
役職員向け教育訓練	あり。　システム障害を想定し、対応マニュアルを整備し、日頃から机上訓練をしていた。ちょうど２か月前に訓練をしたばかりだった。		
非常時行動計画（BCP）	あり。　災害医療の基本原則 CSCATTT（スキャット）に沿った対応マニュアルがあり、対策本部のメンバーも予め決まっていた。		
その他特記事項	地域医療連携のため、各種診療データをクラウド上にアップロードしており、データの復旧まではそのテータが役立った。フォレンジック調査は時間と費用が掛かるため実施せず、原則すべての端末を感染しているものとして取り扱い、データ復旧に専念した。 システム担当の専任者はおらず、事務長を中心とする対策本部のメンバーが、業者と警察の支援を活用し、対応に当たった事例。		

３．３　事例Ｃ（診療所）

図表 3-3 は、三つ目の被害事例（事例Ｃと呼ぶ）の概要である。事例は 2021 年下半期に発生。攻撃を受けたのは、大都市圏にある個人立の無床診療所である。攻撃の種類はランサムウェア（Cring）であり、電子カルテシステムのサーバ内にある診療データが暗号化された。電子カルテと接続された各種医療情報システムが使えなくなったほか、同一サーバにあった人事・経理の基幹業務システムのデータも参照できなくなった。侵入経路は、フォレンジック調査の結果、VPN 機器の脆弱性との推定だった。事例ＡとＢと同様、行政から注意喚起がなされていた既知の脆弱性だったため、セキュリティを含むシステムの保守管理業者との間で、復旧の費用負担について問題となった。

事例Ｃで直接対応したのは、総務システム担当者 1 名だった。外部から、院内システムの保守管理委託業者がサポートした。厚労省医政局に連絡し、警察にも通報したが、特に助言や支援は得られなかった。1 人体制の復旧作業で多忙な中、厚労省からは頻回に報告のみを求められ、ストレスフルな状況があったという。暗号化データは、保守委託業者の技術者によって 9 割程度復元できた。しかし、完全な復旧とは言えず、攻撃から 1 年半経っても過去データ参照のためだけに別システムを稼働し、2 重の手間とコストがかかっている状況である。

本件では、注意喚起があった VPN 機器の脆弱性について保守委託業者は知りつつも対応しなかったばかりか、顧客にも伝えておらず、事後的に問題となった。加えて、厚労省の対応も問題含みである。行政への報告を求めて情報を得るだけで、現場には大きな負荷がかかった。被害現場に寄り添って助言や支援を行ったり、復旧をサポートする専門機関を案内したりという対応はなかった。

図表 3-3. 事例Ｃ（診療所）の概要

被害の時期	2021 年下半期	時間帯	深夜
所在地	大都市圏	病床規模	□病院　500 床以上 □病院　200～499 床 □病院　100～199 床 □病院　99 床未満 □有床診療所 ☑無床診療所
開設主体	□国公立・公的 □社会保険関係団体 □医療法人 □その他の法人 ☑個人		
攻撃の種類	ランサムウェア（Cring）		
侵入経路	VPN 機器（Fortinet 社製 FortiGate）		
被害を受けたシステム	電子カルテシステム（サーバ） システムの保守管理を委託している業者から、電子カルテが使えなくなった旨の連絡があり発覚。		
間接的に被害を受けたシステム	上記とつながるすべての端末および医療情報システム 医事会計システム、オーダリングシステム、オンラインシステム、医用画像管理システム、診療予約システム。同一サーバにあった人事・経理の基幹業務システムも使えなくなった。		
復旧時間	診療は休止せず。前日迄のデータが参照できず、手探りで診療継続。データ復旧は未だ途中（過去データを参照するためだけに別システムを運用しており、２重の手間とコストが掛かっている）。		
復旧費用	数千万円規模（※具体的金額は聞けず） 内訳は、①フォレンジック調査費用、②システムの再構築費用（サーバと端末、ネットワーク機器とソフトウェアの再設定）、③暗号化データの復元費用（保守委託業者の技術者が復元）、　④電子カルテシステムと接続されている全システムのフルスキャンと再設定費用。 その他従業員の残業代や心理的負担は計り知れない。		
対応人員（内部）	総務システム担当１名		
対応人員（外部）	院内システムの保守管理委託業者（従前より、電子カルテシステムを含む院内システムの保守管理を同社に委託していた）		
その他外部の支援者	顧問弁護士：保守委託業者との復旧費用負担について相談 （厚労省からは具体的な助言や支援はなく、報告を求めるのみ。警察は犯人が分からないと対応しようがないとの回答であった）		
行政機関への連絡相談	厚労省医政局に連絡 警察のサイバー犯罪窓口に通報		
サイバー保険への加入	加入なし。　今後も加入予定はない。		
役職員向け教育訓練	なし。　現在は、保守委託業者と協力して標的型メール訓練やＥラーニングを行っている。		
非常時行動計画（BCP）	あり。　ただし、震災に備えた BCP であり、役に立たなかった。		
その他特記事項	保守委託業者が VPN の脆弱性を知りつつ対応しておらず、その後、攻撃を受けた。ゆえに業者との間で復旧費用の負担が問題となった。 また厚労省と警察からは具体的支援はなく、しかも厚労省からは頻回に報告のみを求められ、被害の現場には多大な負荷がかかった。		

４．現状の問題点と将来に向けたヒント

本章では、分析対象とした３つの被害事例から、現状の医療現場のサイバーセキュリティに関する問題点と共に、将来に向けた対策のヒントを抽出・整理した。

４．１　現状　５つの問題点

（１）復旧にかかる多額のコストと労力

第一の問題点は、医療機関のサイバー攻撃による被害からの復旧には数千万円規模の多額の費用と労力がかかるという点である。今回の調査対象は、中小規模の病院と診療所であるが、事例Ａ（病院）では約 5 千万円、事例Ｂ（病院）では約 7 千万円、事例Ｃ（診療所）では具体的な金額は聞けなかったが、数千万円規模の復旧費用がかかったという。しかも、事例Ａは攻撃の 2 週間前にタイミング良く業者が外部に取っていたバックアップから復元できたという偶然があった事例であり、事例Ｂはシステム障害を想定した机上訓練をしており、直ぐに対策本部を組織し、所轄の警察の応援も得て復旧に当たった事例である。これらを考慮すると、医療機関においてサイバー攻撃による被害があった場合、少なくとも 5 千万円～1 億円程度の復旧費用が掛かると想定しておくべきと考える。

復旧の費用に加えて、院内の人員に相応の負荷と労力がかかる点も、強調しておきたい。インタビューでは、次のような声があった。

- **「夜を徹したシステム周りの作業となり、他部署に人員の応援を求めるわけにもいかなかった」**[8]
- **「システム対応も大変だったが、個人情報漏洩の対応にも非常におカネと労力を要した。**（コールセンターを設置したが）**捌ききれない案件が数十件単位であり、来院してクレームされる方もいた」**
- **「実際に被害を経験してみて言えるのは、中小病院で情報システムのことを把握している人員が少ないと事態を収拾するにあたって非常に厳しい。それを痛感した」**
- **「大変だったのは、電子カルテシステムが復旧してからだった。紙カルテとレセコン代替機で仮運用していた２か月分の患者データを復旧した電子カルテに転記する作業が大変だった」**
- **「**（対応するシステム担当と同部署にいる事務長は）**同じ管理部門にいても、システムのことはよくわからないので手を貸したくても貸せず、見ているだけでもつらかった」**
- **「残業代や従業員の心理的コストは、測り知れない。それに加えて、患者に及ぼした影響や風評被害のコストも甚大である」**

（２）手薄なシステム管理の人員体制

第二の問題点は、医療現場における医療情報システムを管理する人員体制の手薄さである。今回のケースでは、事例Ａ（病院）と事例Ｃ（診療所）では１人体制、事例Ｂ（病院）では担当者なし（日頃は管理部門の職員がシステム業者との連絡窓口を兼務）という体制だった。となると、必然的に**「最小限の人員体制**

[8] 本章における**「ゴシック体」**は、インタビュー調査から直接得た情報を意味する。聴取内容の臨場感とそれに伴う説得力を重視し、できる限り口語体で記載した。

で運営しているところに、予期せぬサイバー攻撃があったという状況」という事態を招きかねない。

インタビューでは、人員体制の現状について、次のような意見があった。

- **「自院の規模だと、自分を含めて 2 名体制だと、ずいぶん状況は変わってくるのではないかと感じている。実際、自身の業務も情報システムの管理運営に特化できている訳ではなく、他の業務と兼務している状況である。情報システムの管理に手が回っていないところがある」**
- **「400 床以上の病院だと、システム安全管理責任者を置くと診療報酬上の加算があるが、当院の場合は該当しない。システムエンジニアの経験者を雇用しようにもコスト的に見合わない」**
- **「院内で直接対応に当たったのは、総務システム担当の１人だけだった。事務長から見ても、当院の規模でシステム担当を一人だけでやるのは厳しいと思う。システムに詳しいとはいえ**（前職でシステム保守業務を担当）**、自分で構築したシステムではないし、ストレスフルな状況だったと想像する」**

（３）狙われた既知の脆弱性

第三の問題点は、今回の 3 つの事例はいずれも VPN 機器の脆弱性が攻撃の侵入経路となっており、それは行政が事前に文書にて注意喚起していた既知の脆弱性だったことである。2021 年 4 月 30 日、内閣サイバーセキュリティセンター（NISC）は、ランサムウェアを用いた攻撃に悪用されている具体的な機器名やソフトウェア名を列挙し、文書での注意喚起を行っている（図表 4-1）。奇しくも今回の 3 事例はすべて同文書発出の事後に発生し、そこで注意喚起されていた VPN 機器の脆弱性が狙われたものだった。

図表 4-1. 内閣サイバーセキュリティセンター（NISC）による注意喚起【抜粋】

チェックポイント

- インターネット等外部ネットワークからアクセス可能な機器については、外部ネットワーク公開の必要性を十分検討したうえで、セキュリティパッチを迅速に適用する、外部からの管理機能、不要なポート（137（TCP/UDP）、138（UDP）、139（TCP）、445（TCP/UDP）、3389（TCP/UDP）など）やプロトコルを外部に開放しない等の対応策等、IT 資産管理を改めて確認する。特に、通信プロトコル「SMB」や「RDP」については、これまでも必要最小限のポートの開放や SMBv1 の無効化等を呼びかけているところ、ファイアウォールを含む各機器の設定を改めて確認する。
- ソフトウエアや機器等の脆弱性については、ランサムウエアを用いる攻撃者グループによる悪用が報告されているものを含む以下の脆弱性に十分留意する。
  - Fortinet 製 Virtual Private Network（VPN）装置の脆弱性（CVE-2018-13379）[2]
  - Ivanti 製 VPN 装置「Pulse Connect Secure」の脆弱性（CVE-2021-22893、CVE-2020-8260、CVE-2020-8243、CVE-2019-11510）[3]
  - Citrix 製「Citrix Application Delivery Controller」「Citrix Gateway」「Citrix SD-WAN WANOP」の脆弱性（CVE-2019-19781）[4]
  - Microsoft Exchange Server の脆弱性（CVE-2021-26855 等）[5]
  - SonicWall Secure Mobile Access（SMA）100 シリーズの脆弱性（CVE-2021-20016）[6]
  - QNAP Systems 製 NAS（Network Attached Storage）製品「QNAP」に関する脆弱性（CVE-2021-28799、CVE-2020-36195、CVE-2020-2509 等）[7]
  - Windows のドメインコントローラーの脆弱性（CVE-2020-1472 等）[8]
- テレワーク等に関連し、職場から持ち出した PC について、休暇中に長期間、十分な管理下になかった PC を職場で再び利用する際は、パッチの適用やウイルススキャンの実施など必要に応じて実施する。
- 最近では、マルウエア「Emotet」に代わり、マルウエア「IcedID」に感染させる不正なメール等も確認されていることから、ウイルス対策ソフトの導入及び最新化、定期スキャンの実施、メール環境に対するセキュリティ対策等、通常のマルウエア対策も実施する。

資料：内閣官房　内閣サイバーセキュリティセンター（2021）

（４）販売業者・保守管理業者との契約の不備

第四の問題点は、情報システムあるいはネットワーク機器の販売業者や保守管理業者との間に、サイバー攻撃による被害が生じた際の復旧作業や費用負担について、取り決めがなされていなかった点である。今回の 3 事例では、いずれも明確な取り決めはなされていなかった。

事例Ｃでは、3.3 節で述べた通り、セキュリティ対応を含む院内システムの保守管理を全面的に業者に委託していたため、既知の脆弱性が経路となったことがシステム保守管理の委託業者との間で問題となった。**「業者側には認識があったが、当院の側は使っている VPN 機器の脆弱性について知らなかった。業者の言い分はセキュリティの更新には費用が掛かるから伝えなかったというものだった。当院からすれば、委託料を払ってセキュリティを任せているのになぜ伝えなかったのだとなった」**という。本ケースでは、最終的に双方のトップ同士での話し合いとなり、保守管理の委託業者も相応の費用負担をすることで決着がついた。

被害が発生した際の深刻度合いを考慮すると、保守やメンテナンス契約に、サイバー攻撃を想定した条項を盛り込むことは必須と言える。ただ一方で、**「費用が掛かるから伝えなかった」**との業者の言い分にも、一分の理があるかもしれない。サイバー攻撃を想定した保守メンテナンスにかかる費用までは、現行の診療報酬体系では賄えていないからである。現況について、今回のインタビューでは、次のような現場の見解と要望を得た。

- **「医療のＤＸやＩＣＴ化を政府は推進しており、診療報酬上の加算や補助金がついているものもあるが、現場からすれば費用対効果が見合わない。システム周りでは、特に保守やメンテナンスの費用が嵩むので、１回限りの補助**

金でなく、診療報酬上の加算でそれらの費用を賄うことができるような制度設計を望む」

（５）行政の対応と連携体制の問題

第五の問題点は、サイバー攻撃の被害に遭った医療現場に対する行政の対応とその連携体制の問題である。今回調査した 3 事例では、厚生労働省医政局にある連絡先に連絡したが、いずれの事例でも具体的な助言や支援を得ることはできなかった。事例Ｃにおいては、被害現場で独り対応に当たるシステム担当者が、次のような状況に追い込まれた。

- **「厚生労働省医政局の窓口には連絡したが、助言やサポートはなく報告を求められるのみだった。そればかりか、『報告がないのなら立ち入り検査をします』との連絡がきた。被害者なのに傷口に塩を塗るような対応だと感じた。当院としてもできる限りの対応をしていたが、復旧対応で手いっぱいなうえ、院内システムをネットから遮断して、最低限のシステムで運用をしていたので、メールを送るのも難しいような状況があった。厚労省からは『早く報告をせよ』の一点張りで、とても対応に苦慮した」**

厚労行政にとってサイバー攻撃の被害データの収集は重要な職務だが、まずは被害現場の状況に寄り添い、警察や IPA 等と適宜連携して、必要な助言と支援を行うことのできる体制を望みたい。他方で事例Ｂは、同じく厚労省からは特に助言や支援はなかったものの、都道府県警からは全面的なサポートを得ることができた好事例である。ただ、他の事例では、都道府県警に通報はしたものの特に支援はなく、都道府県警の対応に地域によって差があるという点で同様にサイバー攻撃の被害者への行政の対応の問題点として、指摘できる。

４．２　将来に向けた対策のヒント

（１）非常時行動計画（BCP）と日頃からの訓練

将来に向けた一つ目のヒントは、サイバー攻撃を想定した非常時行動計画（BCP）と日頃からの訓練の有用性である。事例Ｂでは、院内に情報システムの専任者はいなかったが、システム障害を想定した非常時行動計画（BCP）が存在し、それを基にスタッフは日頃から机上訓練をしていた。現に、サイバー攻撃の発覚後、直ぐに対策本部を組織し、災害医療の基本原則に則って復旧対応に当たった。被害発覚直後の状況を振り返り、事務長は次のように語った。

- **「深夜に、事務当直者から自分にランサムウェア感染疑いの旨の連絡があったが、直ちに、電子カルテベンダーのサポートセンターへの連絡と紙カルテの準備の指示を出した。連絡は深夜だったが、あまり慌てたりはせず、とりあえず寝ようと１時間くらい寝て、目が覚めてから災害医療の基本原則CSCATTTのことを思い出し、やるべきことが整理できた。それから災害モードに切り替えて、予め決まっていた対策本部のメンバーに連絡をした。復旧作業は実際とても大変だったが、災害等に備えて日頃から訓練はしており、ちょうどシステム障害を想定した訓練を２か月前にしたばかりだったので、何とかなるだろうと考えており、さほど慌てなかったのだと思う」**

ただし、システム障害やサイバー攻撃を想定した行動計画を作成しておくべきことは強調しておきたい。事例Ａと事例Ｂでは震災等の自然災害を想定した非常時行動計画（BCP）はあったが、いずれもサイバー攻撃への対応に当たっては大して役に立たなかったという。

（２）バックアップデータとしての地域医療連携システムの活用

将来に向けた二つ目のヒントは、サイバー攻撃を受けた際のバックアップデータとして、地域医療連携システムにアップロードした自院の診療データが活用できるということである。実際に、事例Ｂ（病院）では、**「関連施設や、地域の医療機関、介護施設との地域連携のために使っていた情報共有システムのクラウド上に診療データをアップロードしていた。再診患者については、そのクラウド上の患者データが参照できた。そのデータが参照できなかったら、おそらく再診患者の診療を止めるか、制限していたと思う」**といった状況があった。

現状では、震災等の自然災害時に、地域医療連携システムにアップロードした自院の診療データを電子カルテのバックアップデータとして活用可能であることを同システムの利用者拡大に向けてアピールしている事例がある。今後は、サイバー攻撃被害時のバックアップデータとしても活用可能であることを喧伝することで、さらなる利用者へのアピールが期待できる。ただ現状では、地域医療連携システムにアップロードした診療データは他施設からの閲覧用に簡略化されており、データの仕様もシステムごとに異なるため、同データから電子カルテ等のデータを容易に復元できるわけではない。一方で今般、政府が掲げる医療ＤＸの具体策のひとつとして「電子カルテ情報の標準化」が進められており、これらの問題が解決の方向に進むことも期待される。

（３）経営陣と医療従事者の意識改革

将来に向けた三つ目のヒントは、病院・診療所の経営陣と医療従事者の意識改革に関するものである。医療情報システムの利活用にはサイバーリスクが伴う。かかるリスクへの対処は、被害額や社会的影響の大きさから考えても、医療機関マネジメントの一環として経営陣がコミットすべき経営上の課題である。また、

医療情報システムを使うすべての医療従事者が認識しておくべき課題でもある。

今回のインタビュー対象者は、管理部門やシステム部門の責任者であったが、本件に関連して、以下のようなストレートな見解があった。

- **「医療業界の人々は、他の業界と比較して、システム周りに疎い人が多い。サイバーセキュリティに関する意識向上のためには、まず経営陣の意識を変えることが必要だが、然るべくサイバーセキュリティ対策をすると診療報酬上のメリットがあるような制度を展望すべきである」**

特に、情報システムの脆弱性に関して、経営陣の意識改革が求められる。今回の３事例は共に同じ機器の脆弱性が狙われており、攻撃者は、立地や組織規模の大小にかかわらず、脆弱性を有するシステムをランダムに狙っていると推測される。すなわち、情報システムを使っている以上、どの医療機関にもサイバー攻撃のリスクがあるということである。そうなれば、使っているシステムやネットワーク機器等の脆弱性情報に日頃からアンテナを伸ばしておくことは、医療機関経営者の責務のひとつである。むろんシステムの脆弱性には即時対応すべきであるが、何かの事情で対策を取るまでに時間がかかる場合でも、次善策としてのリスク低減策を講じるべきである。

（４）その他　あるべき公的支援と情報提供

官公庁や公的機関、団体からどのような支援や情報提供があるべきか。前述したように診療報酬に情報システムのセキュリティに関わる保守・メンテ費用を盛り込むことは最低限必要である。その他にも、今回聴取した被害経験者の貴重な意見について、以下に列挙しておく。

- 「被害について相談できる公の窓口があるとよい。（中略）厚労省に被害を連絡したが、警察や他の行政機関、専門機関と連携してサイバー攻撃の被害者をサポートしようという姿勢が一切なかった」
- 「安全管理ガイドラインやシステム障害時のフローチャートは、見たけれども、あまり役に立たない。というのも、大病院やクリニックを沢山抱えているような大規模法人を前提としているもので、専任の情報システム管理者もいないような小規模施設には、応用が難しい。せめて、組織の規模別にどのような管理体制であるべきか、汎用例を示して欲しい」
- 「サイバー攻撃の被害に遭った場合、しばらく診療報酬の請求ができなくなるケースが出てくる。そういったケースに対応する補償の仕組みなどがあるとよい」
- 「脆弱性情報等のセキュリティ関係の情報は医療現場の人員では分かりようがないので、システムの団体を通じて個々のシステムベンダーから、該当するシステムを使っている医療現場に届くような仕組みがあるべき」
- 「（医師会や病院団体からは）医療現場向けのサイバー保険についての情報提供があると良い」
- 「医師会や病院団体に対しては、医療現場での事案発生時の対応マニュアルの整備等を支援して頂けたらありがたい」

５．考察と提言

本稿では、最近（2021 年下半期～2022 年上半期）、サイバー攻撃の被害に遭った医療機関の３事例を精査し、現状の問題点と将来に向けた課題解決のヒントを抽出、主要な論点ごとに整理し、検討した。

最後に、これまでの議論をベースに考察を加え、主として行政機関に向けて、いくつかの提言を行って結論に代えたい（図表 5.1 に提言要旨）。

提言１．行政間の連携強化、専門機関と連携した被害現場の支援

サイバー攻撃に遭遇した医療機関は、犯罪行為の被害者である。被害に遭った医療現場の復旧と事業継続の支援という観点から、関係省庁および専門機関が適宜連携したサポート体制の構築が、第一に求められる。具体的には、被害時の連絡先や通報先である厚生労働省医政局と都道府県警のサイバー犯罪の担当部署に加えて、技術的な相談窓口である IPA（情報処理推進機構）の担当部門といった行政・専門機関のタテ・ヨコの連携が、最低限求められる。今回の被害事例を見る限りでは、関係省庁間の連携体制や被害現場の支援体制には課題があり、対応は業者任せで、技術的な公的相談窓口はあまり活用されていないという現状がある。まずは被害現場の支援という視点から、全体的に連携体制の見直しが必要ではないか[9]。また、原因究明や侵入経路の特定のためのフォレンジック調査は犯罪捜査に類するものであり、公的機関が実施すべきである。公的機関が認定した民間の機関が実施する等の方法も考えられる。

[9] 2023 年 4 月 6 日、警察庁はサイバー事案の被害の潜在化防止に向けた検討会の報告書を公表し（警察庁サイバー警察局 2023）、関係省庁との連携強化とサイバー事案の被害に関する報告相談窓口の一元化を今後の方策として掲げた。このような取り組みが推進されることを期待したい。

提言２．脆弱性情報の医療現場への周知

第二に、行政が発信するシステムやネットワーク機器等の脆弱性情報が医療現場に周知されるまでの流れについて、再度確認しておくべきである。今回調査した３つの被害事例では、奇しくもすべて同じネットワーク機器の既知の脆弱性が侵入経路となっていた。この脆弱性については、内閣サイバーセキュリティセンター（NISC）が具体的な機器名やソフトウェア名を列挙し、文書での注意喚起を行っていた。しかし医療現場には情報が届いておらず（2 事例）、あるいは届いていたものの差し迫ったリスクとは捉えられておらず（1 事例）、サイバー攻撃の被害につながった。医療現場の経営陣は多くの場合、医師である。診療の合間を縫って自院のシステムの脆弱性を調べるとは考えにくく、医師に定期的に脆弱性情報をチェックさせるのも現実的ではない。行政から発信される情報がシステムの業者や業界団体を通じて医療現場に届き、対策がなされるように、情報伝達のフローを再確認するべきである。

提言３．非常時行動計画（BCP）作成や机上訓練、チェックリストの充実等の支援

第三に、医療現場向けサイバーセキュリティの支援策としては、サイバー攻撃やシステム障害等を想定した BCP 作成や机上訓練、セキュリティ対策のチェックリストの充実、院内研修の実施支援が有用と考えられる。現状では、厚生労働省のウェブサイトに医療分野のサイバーセキュリティ対策に関する情報が整理され[10]、安全管理ガイドラインに加えて[11]、セキュリティ対策のチェックリストとシステム障害発生時の対応フローチャートが準備され[12]、同省の委託事業とし

---

[10] 厚生労働省「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
[11] 厚生労働省（2022）
[12] 厚生労働省「医療機関の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/10808000/000845417.pdf
厚生労働省「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」
https://www.mhlw.go.jp/content/10808000/000936170.xlsx

て医療機関向けセキュリティ教育支援のポータルサイトが運営されている[13]。これらの追加コンテンツとして、サイバー攻撃やシステム障害を想定した机上訓練と BCP の作成支援、より現実的な対策に向けた病床規模別のチェックリストとフローチャートの整備、その他役職員向けの研修資材等の提供を提言したい。なお、日本医師会は会員向けに「サイバーセキュリティ支援制度」を運営しており、相談窓口や情報提供、被害発生時の一時金支給と併せて、標的型メール訓練や各種マニュアル・テキスト提供等のサービスを提供している。コンテンツの充実にあたって、行政と同制度が連携することも、選択肢のひとつであろう。

提言４．医療現場のセキュリティ対策に対する人材と費用の手当て

最後に、医療現場のセキュリティ対策に対する人材と費用の手当てについて、具体的なあり方を提言したい。まず人材については、今回の３事例のような中小病院・診療所の場合、自前での専門人材確保は難しい。坂口・堤（2021）でも述べた様に、「地域医師会等が主体となって人材を計画に配備し、各地域の複数の医療機関でシェアする」という手法をあらためて提案したい。次に費用面については、医療情報システムのセキュリティに関わる保守やメンテナンス等の費用については診療報酬で賄い、前述した地域の医療機関でシェアする専門人材の確保やサイバー攻撃時のバックアップデータとしての地域医療連携システムの活用といった施策に関しては、地域医療再生基金のような補助金を活用するといった方向性が望ましい。

医療分野のサイバーセキュリティ確保は、政府が推進する医療 DX の大前提であり、平時の国家安全保障である医療をサイバー攻撃から守るにあたって必

[13] 厚生労働省「医療機関向けセキュリティ教育支援のポータルサイト」
https://mhlw-training.saj.or.jp/

要不可欠な施策である。政策的にも財政的にも、高い優先順位で取り組むことが望まれる。

図表 5.1　本稿の提言

項　目	ポイント
行政間の連携強化、専門機関と連携した被害現場の支援	被害に遭った医療現場の復旧と事業継続の支援という観点から、関係省庁および専門機関が適宜連携したサポート体制を構築する。
脆弱性情報の医療現場への周知	行政から発信される情報がシステムの業者や業界団体を通じて医療現場に届き、対策がなされるように、情報伝達のフローを再確認する。
非常時行動計画(BCP)作成や机上訓練、対策チェックリストの充実等の支援	現状整備されているガイドライン等の追加コンテンツとして、サイバー攻撃を想定した BCP の作成や机上訓練の支援、より現実的な対策に向けた病床規模別のチェックリストとフローチャートの整備、その他役職員向けの研修資材等を提供する。
医療現場のセキュリティ対策に対する人材と費用の手当て	セキュリティに関わる保守やメンテナンス等の費用については診療報酬で賄い、地域の医療機関でシェアする専門人材の確保やサイバー攻撃時のバックアップデータとしての地域医療連携システムの活用といった施策に関しては、地域医療再生基金のような補助金を活用する。

参考文献・資料

警察庁（2023）「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」（2023 年 3 月 16 日）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

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.npa.go.jp/bureau/cyber/pdf/20230406_2.pdf

厚生労働省（2022）「医療情報システムの安全管理に関するガイドライン　第 5.2 版」（令和 4 年 3 月）https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html

坂口一樹、堤信之（2021）「病院・診療所のサイバーセキュリティ： 医療機関の情報システムの管理体制に関する実態調査から」 日医総研ワーキングペーパーNo.453
https://www.jmari.med.or.jp/result/working/post-233/

坂口一樹、堤信之、松橋祐輝、本田大輔、中野壮陛（2021）日医総研ワーキングペーパー No.465「医療機器に関わるサイバーセキュリティの動向」
https://www.jmari.med.or.jp/result/working/post-3389/

内閣官房　内閣サイバーセキュリティセンター（2021）「ランサムウエアによるサイバー攻撃に関する注意喚起について」p.2
https://www.nisc.go.jp/pdf/policy/infra/ransomware20210430.pdf

BlackBerry（2022）「グローバル脅威インテリジェンスレポート」
https://www.blackberry.com/ja/jp/solutions/threat-intelligence/2023/threat-intelligence-report-jan-jp

謝辞

お忙しい中、大変なご経験に関するインタビューにご協力いただき、貴重な情報提供を賜りました医療現場の皆さまに、この場をお借りして深く感謝申し上げます。また、本文中のすべての誤りは筆者らの責に帰するものです。

巻末資料：インタビューガイド

インタビューガイド【項目のみ】

1. サイバー攻撃を受けてから復旧に至るまでの経緯について

2. サイバー攻撃への対応、システムの復旧にあたった人員体制について

3. 外部の業者や公的機関、専門家等からの助言や支援について

4. 医療情報システム及びその他の物的な被害状況について

5. サイバー攻撃のシステムへの侵入経路とその特定について

6. 院内の情報システムや端末、USB メモリ等の管理ルールの整備状況について

7. システムの復旧に要した直接的・間接的費用と時間について

8. サイバー攻撃による被害を補償する保険への加入状況について

9. サイバー攻撃を想定した役職員向けの教育・訓練の実施状況について

10. サイバー攻撃を想定した対応手順や非常時行動計画等の策定状況について

11. 官公庁、公的機関・団体からのあるべき支援や情報提供について

※聴取内容は、報告書作成や政策提言等の研究・公益目的のみに使用し、その他の目的には使用いたしません。また、調査結果を対外的に公表する場合には、個別の医療機関が特定できないよう、十分配慮のうえ、公表いたします。

以　上

インタビューガイド【口語での質問調】

1. サイバー攻撃を受けてから復旧に至るまでの経緯について、なるべく詳しく教えてください。

2. サイバー攻撃への対応、システムの復旧にあたった人員体制について、教えてください。実際の対応や復旧にあたり、どのような点に苦労しましたか？　その後、経験を踏まえて、院内の人員や組織体制を改変しましたか？　どう変えましたか？

3. サイバー攻撃への対応、システムの復旧にあたり、どのような外部の業者や公的機関、専門家等に相談しましたか？　彼らからは、それぞれどのような助言や支援がありましたか？　それらの助言や支援は、実際どのように役立ちましたか？

4. サイバー攻撃の被害に遭った貴院の情報システムについて教えてください。被害に遭ったシステムはひとつだけですか？　それとも連鎖的に複数のシステムが被害に遭いましたか？　その他、物的な被害の状況全般について、教えてください。

5. サイバー攻撃のシステムへの侵入経路について、教えてください。侵入経路の特定に至った経緯について、教えてください。その侵入経路については、その後、どのような対策を施しましたか？

6. 院内の情報システムや端末、USB メモリ等の外部媒体の管理ルールの整備状況について、教えてください。その後、経験を踏まえて、それらの管理ルールに改変を加えましたか？　どのように変えましたか？

7. システムの復旧に要した直接的・間接的費用と時間について、具体的に教えてください。その他サイバー攻撃を受けたことによる直接的・間接的被害について、教えてください。それらの被害をお金に換算するといくらくらいになりそうですか？

8. サイバー攻撃による被害を補償する保険には加入していましたか？
（加入していた場合）保険によって、実際の被害・損失のどの程度を賄うことができましたか？　保険の補償内容や付帯サービスに関して、サイバー攻撃の経験者として何か気づいた点があれば、教えてください。

9. サイバー攻撃を想定した役職員向けの教育・訓練の実施状況について、教えてください。それらの教育・訓練は、実際の場面でどのように役立ちましたか？　その後、経験を踏まえて、教育・訓練のやり方に改変を加えましたか？　どのように変えましたか？

10. サイバー攻撃を想定した対応手順や非常時の行動計画等の策定状況について、教えてください。それらの対応手順や行動計画は、実際の場面でどのように役立ちましたか？　その後、経験を踏まえて、対応手順や行動計画に改変を加えましたか？どのように変えましたか？

11. 医療機関のサイバーセキュリティ確保にあたり、次に挙げるような官公庁、公的機関・団体から医療現場に対して、どのような支援やサポート、情報提供があるべきだと考えますか？　サイバー攻撃の経験者として、お気づきの点を教えてください。
    （１）厚生労働省
    （２）警察
    （３）総務省、経済産業省、デジタル庁等、ICT やデジタル技術に関わる省庁
    （４）医療情報システムや医療機器の業界団体
    （５）医師会や病院団体
    （６）その他