寄稿

サイバー攻撃から診療記録を守るために何をすべきか？

鳥飼　幸太　群馬大学医学部附属病院システム統合センター 副センター長／准教授

「サイバー攻撃」とは

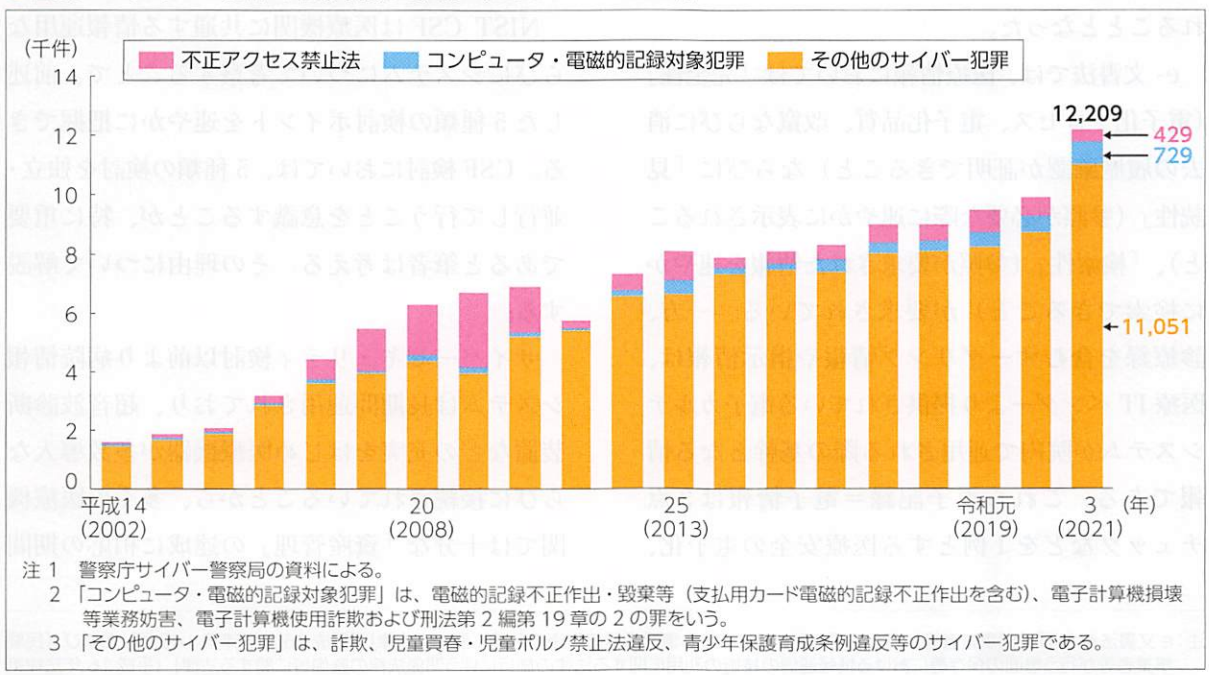
本稿は、医療機関において「サイバー攻撃から診療記録を守る」ために必要な知識背景と行動につき、解説ならびに提案することを目的とする。

まず、「サイバー攻撃」というキーワードの背景について考察する。

サイバー攻撃は犯罪行為の1つであり（図表1）、「情報処理の高度化等に対処するための刑法等の一部を改正する法律案」（サイバー刑法）により、コンピュータ・ウイルス作成罪などの罰則ならびに情報技術（Information Technology：IT）の発展に対応できる操作手続きの整備が定められている[1]。サイバー空間はいわゆる「インターネット空間」であり、自身のパソコンやスマートフォンを通じ、今ではサイバー空間に常時接続された状態に置かれている。サイバー攻撃は「貧者の兵器」と呼ばれ、医療機関において法律ならびに施行規則によって保存が規定されている診療上の記録は、「「診療録等の保存を行う場所について」の一部改正について」（平成25年3月25日付医政発0325第15号・薬食発0325第9号・保発0325第5号厚生労働省医政局長・医薬食品局長・保険局長連名通知）に記載されている[2]。

サイバー攻撃のうち、特定の個人、あるいは組織を狙って行われる攻撃、標的に対して持続的に行われる攻撃（APT〈Advanced Persistent Threat〉攻撃）の実施者は国際的サイバー犯罪

●図表1　サイバー犯罪の検挙件数の推移（2002～2021年）



注1　警察庁サイバー警察局の資料による。
2　「コンピュータ・電磁的記録対象犯罪」は、電磁的記録不正作出・毀棄等（支払用カード電磁的記録不正作出を含む）、電子計算機損壊等業務妨害、電子計算機使用詐欺および刑法第2編第19章の2の罪をいう。
3　「その他のサイバー犯罪」は、詐欺、児童買春・児童ポルノ禁止法違反、青少年保護育成条例違反等のサイバー犯罪である。

出所：法務省『令和4年版犯罪白書』、p.194

組織を含む。このためサイバー攻撃により医療機関が被害を受けた際、重要インフラとしての被害が大きい[3]半面、犯罪者の特定、検挙ならびに賠償請求を行える確率が低いと想定されることがサイバー犯罪対処の困難さとして挙げられる。サイバー攻撃者の特定には、サイバー攻撃被害が発生した際、診療の復旧と相まって、犯罪立証のための電磁的記録の解析技術およびその手続き（サイバーフォレンジック〈Forensics〉）作業を並行することが求められる。

診療情報の電子化・保全は不可欠

次に、「診療記録を守る」というキーワードの背景について考察する。

診療録を中心とする診療記録については、サイバー攻撃対策の是非にかかわらず、すべての医療機関において定められた年限の保管が義務付けられている。診療情報の電子化過渡期においては、処方箋などを原紙で保管するなどで対処されてきたが、2005年4月に施行されたe-文書法[注]によって、各種法令で書面（紙媒体）での保存が義務付けられている文書について、電磁的記録（電子データ）による保存が容認されることとなった。

e-文書法では、医療情報においては「完全性」（電子化プロセス、電子化品質、改竄ならびに消去の履歴確認が証明できること）ならびに「見読性」（参照が必要な際に速やかに表示されること）、「検索性」（参照が要求された情報を速やかに検索できること）が要求されている。一方、診療録を含むオーダリング情報や指示情報は、医療ITベンダーより提供されている電子カルテシステムが院内で運用される際の基幹となる情報である。これら電子記録＝電子情報は3点チェックなどを1例とする医療安全の電子化、ならびに診療記録の共有、適切な診療報酬の算定支援などに不可欠であり、医療機関は法的要請の有無にかかわらず、診療情報の電子化ならびにその保全が不可欠である。

セキュリティ強化に有用なNIST CSF

医療機関がサイバー攻撃から診療記録を守るための調査ならびに検討事項として、サイバー攻撃の侵攻手順、ならびにこの侵攻手順が病院情報システムならびに診療プロセスのどのポイントに該当するかを把握する必要がある。この課題に関しては米国国立標準技術研究所（National Institute of Standards and Technology：NIST）が公開しているサイバーセキュリティフレームワーク（Cybersecurity Framework：以下CSF）に基づく検討が広く知られている[4,5]。CSFは、①識別（Identification：ID）、②防御（Protection：PR）、③検知（Detection：DE）、④対応（Response：RS）、⑤復旧（Recovery：RC）の項目に沿って自施設のサイバーセキュリティ整備・運用状況を整理し、不足箇所の認識ならびにサイバーセキュリティ強化の着手箇所を検討するために有用である（図表2）。

NIST CSFは医療機関に共通する情報運用ならびにシステムについて考察することで、前述した5種類の検討ポイントを速やかに把握できる。CSF検討においては、5種類の検討を独立・並行して行うことを意識することが、特に重要であると筆者は考える。その理由について解説する。

サイバーセキュリティ検討以前より病院情報システムは長期間運用されており、超音波診断装置などの充実をはじめ医療機器が多数導入ならびに接続されていることから、多くの医療機関では十分な「資産管理」の達成に相応の期間

注：e文書法とは、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成16年法律第149号）および「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」（平成16年法律第150号）の総称。

●図表 2　NIST サイバーセキュリティフレームワークにおける機能の 5 分類

出所：米国国立標準技術研究所：重要インフラのサイバーセキュリティを改善するためのフレームワーク，独立行政法人情報処理推進機構翻訳監修，p.6，2018 年 4 月

●図表 3　医療機関における NIST CSF に基づく検討と対策の一例

フレームワーク機能	検討箇所の例	対策ツールの例	対策運用の例
識別 Identification (ID)	病院情報システム全体の接続機器･IP アドレス、セグメンテーション、接続経路、脆弱性等の把握	ネットワーク可視化ツール、脆弱性把握ツール	資産管理手順に沿った調査（リストアップ）、脆弱性情報の迅速把握
防御 Protection (PR)	外部保守接続箇所（放射線診断･治療装置、PACS/ 電子カルテ等）、DMZ 端末、診療録サーバ	VPN、ランサム対策ストレージ	情報漏洩を起こさない院内情報運用研修、診療情報アクセス制御設定、ファイヤウォール設定、セキュリティ保守契約の充実、バックアップ手段と階層、運用の策定と実装
検知 Detection (DE)	電子カルテ端末挙動、ネットワークトラフィック監視、ストレージ / CPU 負荷変動	IDS、EDR（D）、NDR（D）	日常のシステムパフォーマンスモニタにおけるトレンド把握と差異の知覚、対策ツールが提供するダッシュボード機能による監視
対応 Response (RS)	不特定多数や多数のスタッフがアクセスできる機器、電子カルテにアクセスできる端末またはサーバとポート、攻撃検知時のカルテデータバックアップ経路	IPS、EPP、EDR（R）、NDR（R）	インシデント時連絡先の把握と役割分担の検討、医療安全と情報保全、診療継続を両立する対策方法やツール挙動設定の検討、インシデント対応訓練への参加
復旧 Recovery (RC)	電子カルテサーバを中心とする保存義務を有する情報サーバ、診療継続に不可欠な情報端末の運用	バックアップ復元ツール、情報サーバ仮想化インフラ	復元手順の BCP への記載、復元テスト、環境設定を伴った包括的サーババックアップの実施、バックアップ周期の短縮化

略語：PACS（Picture Archive and Communication System）、VPN（Virtual Private Network）、DMZ（Demilitarized Zone）、IDS（Intrusion Detection System）、IPS（Intrusion Prevention System）、EDR（Endpoint Detection and Response）、NDR（Network Detection and Response）、EPP（Endpoint Protection）

とマンパワーを必要とする。一方、近年の急激な国際情勢の変化に伴うサイバー攻撃に対しては、迅速に整備対策を進める必要があり、資産管理を待たずに着手可能な手段を、逐次実施することが必要だからである。

図表 3 に、医療機関における NIST CSF に基づく検討と対策の一例を示し、着手すべき順等を考察する。まず、診療記録を守る上で不可欠な対策は電子化診療録の実運用サーバがサイバー攻撃に対し、情報ならびに機能を失わない

ことである。これに該当するサーバは電子カルテサーバである。実施対策としては②PRならびに⑤RCの機能について調査し、不足であれば該当箇所を強化する手法の検討ならびに実施を速やかに行う。次に、病院経営の継続が病院収入を維持する必要条件であり、診療継続に不可欠な情報サーバならびに端末がサイバー攻撃を受けたとしても、情報ならびに機能を失わないことを考える。これに該当するサーバは、オーダリングサーバのほか、患者受付機能を提供するサーバ、会計算定機能を提供するサーバ等が該当する。診療ワークフロー上では、検体検査、画像検査が停滞することで外来ならびに入院患者の診療継続に多大な支障が生じることから、これらの機能を提供するために不可欠なサーバならびに端末を特定し、サイバー攻撃耐性を高める手当てを実施することが肝要である。また一例として、当該機能を提供しているサーバは、物理サーバと仮想サーバの別により、データ保全や機能保全の具体的手法が異なるなど、サイバーセキュリティ対策においてはシステム構成情報に基づき実施することが必要である。

多要素の認証プロセスを導入し パスワードの定期的変更を確実に

サイバーセキュリティ対策においては、過去に一度有効性が疑われて主運用から外された技術が、セキュリティ環境全体の変化に伴い、再び必要な対策として見直されるケースが存在する。一例として、ユーザー名とパスワードの運用について取り上げる。

The Hacker Newsは「It's a Zero-day? It's Malware? No! It's Username and Password」において、攻撃者の武器で最も強力な武器は盗んだユーザー名とパスワードだとして、その深刻さと課題、Active Directory環境の保護の重要性について報じている。これは、サイバー攻撃の検出が電子情報処理プロセスやネットワークトラフィック、ユーザーの行動など様々なアクティビティの異常を特定することに依存しているため、攻撃者が正常に認証されてしまうと、その後の攻撃を検出することが難しくなることに起因している。

このような状況で診療記録を守るための活動として、認証プロセスにおいて複数の独立したデバイス（パソコンとスマートフォンなど）を操作するよう求められる多要素認証の適用箇所を増加させるとともに、ユーザー名やパスワードの漏洩が起きている可能性があることを前提とし、パスワードを定期的に変更する運用の確実な実施が効果的であると考えられる。サイバーセキュリティの最適解は情勢によって変化することから、その対策の有効性や効果についても適宜見直しができることが望ましい。

責を負うのは経営者 検討では「数値として」決定する

医療機関の経営者視点でサイバーセキュリティを見た場合、その向上対策を「診療報酬に結びつかない固定費」と捉えがちである。しかしながら、経営において誤ったリスク評価に基づく損害の責を負うのは経営者であることが、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版に明記された[6]。

本検討における「リスク」とは、サイバー被害について「被害発生確率×被害額」によって計算される量である。一般にリスク評価においては、リスクについて年間被害額の計算を行い、これを低減する対策実施に必要な適正支出額を算出する、と説明されている。しかしながらこの計算方法にのみ依存すると、長期的に効果の高いリスク低減手法である「ITネットワークインフラの再構成」が提案された場合に、一過性の支出が大きいことのみを理由として申請が否定される傾向にあることが複数医療機関との議論から把握されている。特に、中規模以上の総合病院においてはITインフラを構成する機器ならびにネットワーク要素が多いため、再構

成の見通しを得るために必要な労力を割り当てられないこともその素因を構成していると考えられる。

経営者視点でサイバーセキュリティ対策を考える上では、最も厳しい検討条件として「当該事業所は、サイバー攻撃を含む諸般の外乱により診療停止を行わざるを得ない場合、破綻に至らない停止期間は何日間までだろうか」という問いを設定し、「数値として」決定することが肝要である。その上で、この数値を下回るように情報システムの稼働信頼性を確保するよう検討する。診療において運用している病院情報システムについては、医療 IT ベンダーの担当者と担保すべきシステム稼働信頼性について協議し、Service Level Assurance（SLA）として保守契約を定めることが有効である。SLA では、サイバー攻撃を含むシステム停止が生じた場合の駆けつけまたは対応開始までの時間、手段や条件、障害内容の切り分けならびにフォレンジック作業の受け入れ、診療継続状態維持のための 1 次手当ての方針策定と実施、正常診療状態への復旧等について項目を設け、医療機関側で実施担保する内容と医療 IT ベンダー側で実施担保する内容を分界する（責任分界点の設定）を明確化することで、リスク低減対策に対する支出を決定する。

医療サイバーセキュリティ人材は医療人と同様の登用と配置を

長期的なリスク低減を行う上では、経費の上でも対応の迅速さ確保の上でも、外注と比較してセキュリティ部門の組織化とセキュリティ運用の内製化を段階的に行い、CSF の全体レベルを向上させるための長期戦略を策定して、計画的に実施する能力を涵養することが望ましい。この点においては、社会全体におけるスキルを有する IT 人材が慢性的に不足している実情があり、採用公募のみで適切な人材を確保することが難しいと考えられる。（一社）医療情報学会ならびに医療情報技師育成部会では、医療情報技師能力検定等を定め、高度な医療 IT スキルを有する人材の輩出に努めている。また、（一社）医療サイバーセキュリティ協議会では、医療機関、医療 IT ベンダー、政府機関など立場の異なる役職により、医療サプライチェーンのセキュリティを俯瞰できる教育の提供ならびにユーザー間での ISAC 機能を提供している[7]。

医療 IT 運用は、医療人の育成と同じく「現場から学ぶ」On the Job Training（OJT）の要素が強いと筆者は考えており、読者諸賢においては、素質のある人材を定着させ、育成の視点を踏まえた医療サイバーセキュリティ人材の登用と配置についてご検討、ご配慮いただけたらと願う[8]。

[参考文献]
1) 法務省：いわゆるサイバー刑法に関する Q&A，https://www.moj.go.jp/content/001267488.pdf［2023.9.19 確認］
2) セコム医療システムウェブサイト：電子カルテの保存期間と医療機関における文書保管について、https://medical.secom.co.jp/it/karte/column/post-5.html［2023.9.19 確認］
3) サイバー攻撃で「核の大惨事」の恐れも、米露の元軍指揮官ら警告，AFP 通信 2015 年 5 月 2 日号，https://www.afpbb.com/articles/-/3047155［2023.9.19 確認］
4) 米国国立標準技術研究所：連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項　Minimum Security Requirements for Federal Information and Information Systems，独立行政法人情報処理推進機構翻訳監修，2006 年 3 月，https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025322.pdf［2023.9.19 確認］
5) 米国国立標準技術研究所：重要インフラのサイバーセキュリティを改善するためのフレームワーク，独立行政法人情報処理推進機構翻訳監修，2018 年 4 月，https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000071204.pdf［2023.9.19 確認］
6) 厚生労働省：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，2023 年 5 月
7) 松山征嗣：医療機関におけるサイバーセキュリティ対策，病院，82 (9)，2023.
8) 鳥飼幸太：医療現場の BCP としてのサイバーセキュリティ対策，病院，82 (9)，2023.

PROFILE

とりかい　こうた：1979 年福岡県生まれ。2006 年九州大学大学院工学府エネルギー量子工学専攻博士課程修了（工学博士）。医学物理士。2002 年高エネルギー加速器研究機構特別共同利用研究員、2006 年量子科学技術研究開発機構博士研究員、2008 年群馬大学重粒子線医学研究センターを経て現在に至る。2011～2016 年特命病院長補佐（通信・エネルギー）。日本 M テクノロジー学会理事、（一社）医療サイバーセキュリティ協議会常任理事、日本医療情報学会会員、日本加速器学会会員。

令和5年10月1日発行（毎月1回発行） 通巻第407号 第34巻第10号

The Journal of JAHMC

［機関誌 JAHMC（ジャーマック）］
2023 October /vol.34 No.10

2023 10

Japan Association of Healthcare Management Consultants

INTERVIEW **新たな社会基盤としての医療DXを** 小笠原 克彦 氏

REPORT **デジタルヘルスの社会実装**
CASE1 リアルワールドエビデンス（RWE）の創出
CASE2 短縮・迅速化を実現した救急搬送システム
CASE3 モバイルクリニック&ドローンを積極活用

寄稿 **サイバー攻撃から診療記録を守るために何をすべきか？** 鳥飼 幸太

誌上研修 医療DXの新しい潮流 第4回
地域完結型医療をDXで推進
蔭山 裕之

公益社団法人
日本医業経営コンサルタント協会
Japan Association of Healthcare Management Consultants