医療機関を狙った セキュリティインシデント事例と 求められるセキュリティ対応

内橋七海

CONTENTS

要　約

1　2021年10月に徳島県つるぎ町立半田病院で起きたランサムウェアへの感染は、その被害規模から国内の象徴的なセキュリティインシデント事例となった。国内外でセキュリティインシデントが相次ぐ背景として、医療情報のデータ化、院内ネットワークの外部接続、サイバー攻撃の高度化、などが挙げられる。

2　公開されたレポートにより医療機関におけるセキュリティ対策がまだ十分に浸透していないことが明らかになっているが、その要因として、医療機関が「医療の質」を重視するあまりセキュリティ対策が後回しになっていることが推察される。医療機関では医療の質を保ちつつ、セキュリティ対策レベルを高める工夫が求められる。

3　医療機関が実行すべきセキュリティ対策として、大・中規模の医療機関では厚生労働省の「医療情報システムの安全管理に関するガイドライン（厚労省ガイドライン）」、小規模の医療機関では医療機関のサイバーセキュリティ対策チェックリスト（医療機関向けチェックリスト）を使用したアセスメントによる現状把握、が挙げられる。

4　近年はヘルステックサービスの増加や高度な医療機器の誕生といった技術革新が進み、医療機関に求められるセキュリティ対策も高度化・複雑化している。患者が安心して医療機関を利用できる状況を維持するためにも、重要インフラとして医療機関におけるセキュリティ対策が今まで以上に求められている。

Ⅰ 医療分野を取り巻く環境

1 医療機関のセキュリティインシデントは年々増加

近年、医療機関、特に病院のセキュリティインシデントが相次いでいる（表1）。

海外の事例では、2018年7月にポルトガルのデータ保護機関が、同国のバレイロ・モンティージョ中央病院に対してセキュリティ管理の不備による不適切なアカウント管理を指

表1　医療機関におけるセキュリティインシデント事例

国内／海外	病院名	発生年	インシデント概要
国内	宇陀市立病院（奈良県）	2018年10月	電子カルテシステムのサーバーと一部のクライアントPCがランサムウェアに感染し、**患者1,133人のカルテ情報が暗号化**された。電子カルテシステムを使用した**診療を数日間に渡って停止**した[注1]
国内	多摩北部医療センター（東京都）	2019年6月	所属する医師の端末・メールアカウントに不正アクセスがあり、同端末内の情報を利用して都庁メールサーバーや同公社メールサーバー、その他当該医師とメールの送受信があったユーザーにスパム攻撃が確認された。**患者や医療関係者など計約3,700人分の個人情報が流出**した疑いがあると発表された[注2]
国内	横浜市立大学付属病院（神奈川県）	2019年8月	所属する医師が、研究目的で神奈川県内の複数の病院から収集した**膀胱がん患者3,275人の個人情報を、使用者不明の二つのメールアドレスに誤送信**したことが確認された。医師は、学内から正常に送信できないアドレスが多かったため、個人用の端末から再度送信していた[注3]
国内	新潟大学医歯学総合病院（新潟県）	2020年1月	2019年11月に殺人事件で亡くなった女性（当時20歳）の**電子カルテに院内の緊急治療や司法解剖といった業務とは直接の関係がない部署からアクセス**があったことが確認された[注4]
国内	福島県立医科大学付属病院（福島県）	2020年12月	2017年夏に**パソコンや医療機器がランサムウェアに感染してロックされ、使用不能**になっていたことを明らかにした。病院関係者がウイルスに感染した私用のパソコンをネットワークに接続したことで感染した可能性がある。病院は身代金の要求には応じず、データの復元を断念した[注5]
国内	つるぎ町立半田病院（徳島県）	2021年10月	電子カルテシステムのメインサーバーがランサムウェアによる攻撃により暗号化され、約**85,000人の患者データにアクセスが不能**となった。電子カルテが使用できなくなったため、復旧するまでの約2カ月間、紙のカルテを新規作成して対応することを余儀なくされた[注6]
国内	日本歯科大学病院（東京都）	2022年1月	病院内の歯科と医科それぞれの電子カルテと会計システムが作動する計三つのサーバーがコンピューターウイルスに感染し、**4日間にわたって新規患者の受け入れや診療の一部を停止**する事態となった。患者の情報が閲覧できなくなった影響で、予約患者のみ受け入れるなど一部の診療を中止した[注7]
ポルトガル	バレイロ・モンティージョ中央病院	2018年7月	同国のデータ保護機関が、同院に対し、**セキュリティ管理の不備により不適切なアカウント管理があるとしてEUデータ保護規則（GDPR）違反**とし40万ユーロ（約5,000万円）の制裁金を課した[注8]
チェコ	ブルノ大学病院	2020年3月	コンピュータシステムがサイバー攻撃され、**ITシステム全体がシャットダウン**した。この事態により、患者情報が入ったコンピュータの機能が停止し、**急遽手術が中止**となったり、**急患を受け入れられなくなったりする事態**となった[注9]
ドイツ	デュッセルドルフ大学病院	2020年9月	病院内のネットワークがランサムウェア攻撃を受け、院内のサーバー30台以上が感染した。この対応に追われていたことで、**同院に搬送中であったものの、受け入れができず別の病院に移送された救急患者**もいた[注10]

摘し、EUデータ保護規則（GDPR）違反として40万ユーロ（約5000万円）の制裁金を課した。本病院には医師が296人しか存在していないにもかかわらず、病院のシステムには985人のユーザーが医師としてアカウント登録されていたこと、すべての医師が全患者データにアクセスできるようになっていたこと、さらには医師以外のスタッフも患者データにアクセスできていたことなどが、ポルトガルのデータ保護機関（CNPD）による調査の結果明らかとなった[注8]。

また20年９月には、ドイツのデュッセルドルフ大学病院のネットワークがランサムウェア攻撃を受け、院内のサーバー30台以上が感染した。この対応に追われていたことで、同院に搬送中であったものの、受け入れができず別の病院に移送された救急患者もいた[注10]。

こうした事例はもはや対岸の火事ではなく、日本でもさまざまなセキュリティインシデントが発生している。最近では、21年10月に徳島県つるぎ町立半田病院で起きたランサムウェア（「身代金」と「ソフトウエア」を組み合わせた造語）への感染が大きな話題となった。本事件では、電子カルテシステムのメインサーバーがランサムウェアによる攻撃で暗号化され、電子カルテシステムと同サーバーデータを参照する会計システムが使用できなくなった。これにより、一時救急や新規患者の受け入れを中止せざるをえなくなり、手術も可能な限り延期となったほか、外部委託先のセキュリティ会社がサーバー復旧に成功するまでの約２カ月間、手書きでのカルテ記録対応や診療報酬の算定、請求の業務停止など、業務を大幅に制限せざるを得ない事態となった[注6]。

つるぎ町立半田病院の事例はその被害規模から、18年10月に奈良県の宇陀市立病院で起きたランサムウェアの感染事例を上回るものとして認知され、セキュリティインシデントの発生によって、重要インフラとしての医療機関の可用性（「保有する情報が正確であり、完全である状態を保持することで、情報が不正に改ざんされたり、破壊されたりしないこと[注11]」）が損なわれ得ることを示す日本の象徴的な事例となった。この事件の状況は頻繁に報道され、厚生労働省も「医療機関を標的としたランサムウェアによるサイバー攻撃について」という注意喚起を医療関係団体などに向け再通知した[注12]。

つるぎ町立半田病院の事例が発生する前の調査ではあるが、日本医師会総合政策研究機構（日医総研）が、医療機関における情報システムの管理体制の実態把握を目的として全国の病院・診療所を対象に実施した調査レポート「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[注13]」では、医療機関におけるサイバーセキュリティ対策の組織体制や行政の取り組みの認知度・活用度、医療機関におけるリスクマネジメントの体制について問題提起している。また、一般社団法人医療ISACの「国内病院に対するセキュリティアンケート調査の結果と考察[注14]」でも、病床規模や、国営・医療法人などの運営方法の違いによる対応率の差や、病院におけるインシデントレスポンス、サイバー攻撃を想定したBCP（Business Continuity Plan：事業継続計画）の不十分さなどが指摘されており、医療機関におけるセキュリティ対策推進が大きな課題となっていることが読み取れる。

2 セキュリティインシデントの危険性は高まっている

つるぎ町立半田病院の事例を含め、近年発生したセキュリティインシデントの背景としては、主に次の三点を挙げることができる。

(1) 医療情報のデータ化

一点目は、これまで紙媒体で記録・保管されていた医療情報のデータ化が進んでいるという点である。

たとえば電子カルテである。厚労省の調査で、電子カルテの普及率は一般病院（精神科病床のみ、および結核病床のみを有する病院を除いたもの）全体では2008～20年にかけて14.2％から57.2％に、400床以上の一般病院では38.8％から91.2％に増加していることが判明しており、電子カルテシステムの利用は今後もさらに拡大することが予想される[注15]。

このように、医療情報のデータ化が進み利便性や効率性が高まる一方で、第三者によるアクセスの恐れも大きくなっている。医療機関が情報セキュリティやサイバーセキュリティの脅威の対象となっているのである。

(2) 外部サービスの利用やメンテナンスによる院内ネットワークの外部接続

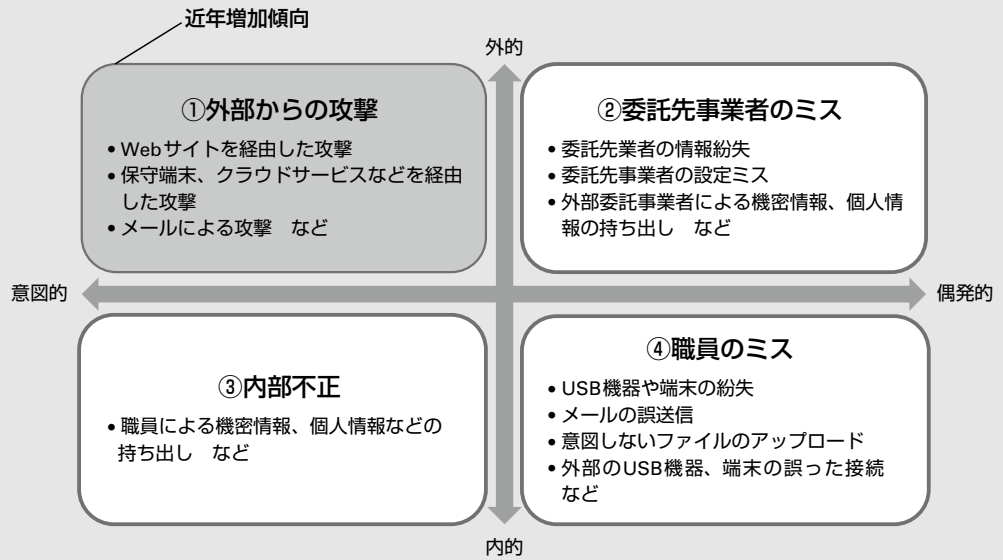
二点目は、医療機関のネットワークと外部のネットワークの接続機会が増えているという点である。

たとえば、電子カルテなどのシステムのリモートによるメンテナンス時や外部サービスの利用時には、外部ネットワークから医療機関のネットワーク、もしくは医療機関のネットワークからインターネットを含む外部ネットワークに接続される。これにより、ネットワーク上の盗聴・なりすましやサイバー攻撃など、セキュリティインシデントの脅威となり得るものが増えているのが現状である。

(3) サイバー攻撃の高度化

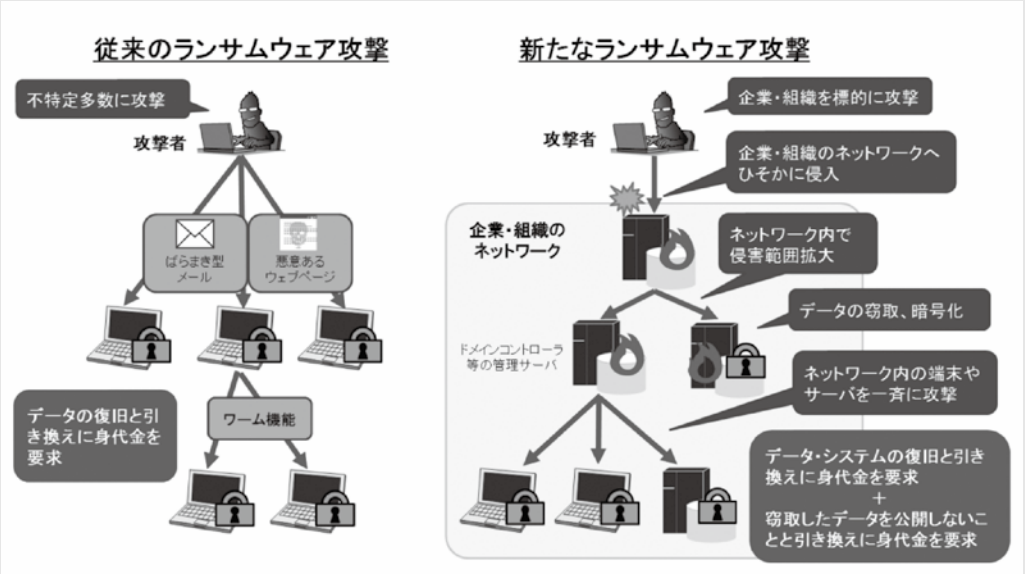
三点目は、サイバー攻撃の手口が高度化しているという点である。

図1　セキュリティインシデントの要因



出所）厚生労働省「医療機関を取り巻く情報セキュリティ対策の現状」[注16]資料より作成

図2　従来の／新たなランサムウェア攻撃の差異



出所）情報処理推進機構（IPA）「事業継続を脅かす新たなランサムウェア攻撃について[注18]」より引用

セキュリティインシデントの要因は、図1のように「意図的（故意）」「偶発的（過失）」「外的」「内的」の四象限に分けることができるが、この中で「意図的（故意）」かつ「外的」に当てはまる部分、いわゆる外部からの攻撃、中でもサイバー攻撃が近年高度化している。

たとえば警察庁の調査「令和3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」[注17]では、ランサムウェアに関して、不特定多数の利用者を狙って、ウイルスの仕込まれた添付ファイルや不正なリンク付きの電子メールを送信するといった従前の「ばらまき型」の手口から、最近ではテレワークや、リモートによる保守業務で使用されているVPN機器をはじめとする企業のネットワークにおけるインフラの脆弱性を狙って侵入するなど、特定の個人や企業・団体を標的とした手口に変化している、と報告している（図2）。

加えて最近の事例では、データの暗号化のみならずデータを窃取した上で「対価を支払わなければ当該データを公開する」と企業に金銭を要求する二重恐喝（ダブルエクストーション）という手口が多くを占めている。これら以外にも、攻撃者が攻撃後にログ（侵入の痕跡）を削除するなど、サイバー攻撃の手法や技術、手口が巧妙化、高度化している実態がある。

Ⅱ　医療機関で対応が求められるセキュリティガイドライン・指針や法規制

それでは、医療機関で実施が求められるセキュリティ対策はどのように定義されているのか。ここでは海外・国内における、医療機関が対応すべきセキュリティ関連ガイドライ

ンや法規制について説明する。

1 先進する海外のガイドラインや法規制

まずは海外における事例として、米国、英国の法規制を紹介する。

(1) 米国の事例

米国では、医療機関に向けられた法規制として米国保健福祉省（HHS）によって規制され、公民権局（OCR）によって施行されているHIPAA（Health Insurance Portability and Accountability Act：医療保険の相互運用性と説明責任に関する法律）およびHITECH（Health Information Technology for Economic and Clinical Health Act：経済的及び臨床的健全性のための医療情報技術に関する法律）が存在する。HIPAA／HITECH法は、電子化された医療情報（PHI）に関するプライバシー保護・セキュリティ確保について定めた米国の法律であり、医療機関はHIPAA法で定められているプライバシーとセキュリティのルール違反があった場合に公民権局（OCR）から罰金が科される可能性がある。

加えて、HIPAA／HITECH法の対象には医療機関やその外部委託先だけでなく、医療情報（PHI）の生成、収集、維持、交換を行うクラウドサービス事業者やその下請け事業者も含まれており、医療機関以外のさまざまな事業者が対象となっていることがポイントである。

(2) 英国の事例

英国では、公的医療制度を担う国民保健サービス（NHS：National Health Service）の医療システムの情報や、ITシステムなどを提供する国営機関であるNHSデジタルから、サイバーセキュリティやデータセキュリティに関する複数のガイダンスが公表されている。たとえば医療情報のクラウド保存に関するものや、サイバー攻撃やフィッシングメールへの対策など、さまざまなカテゴリーのものが存在する。

また、欧州のEU加盟国で適用されているGDPR（一般データ保護規則）はEU離脱後に適用対象外となったものの、GDPRと同水準の要件が規定された国内法であるData Protection Act 2018（2018年データ保護法）が存在し、医療分野を含むデータの保護に関して厳しい規定がなされている。

2 国内では主に個人情報保護法と厚労省ガイドラインの二本柱

一方、わが国でも医療機関が守るべきガイドラインや法規制が存在する。

(1) 個人情報保護法

医療機関も一事業者として個人情報保護法を遵守する必要がある。個人情報保護委員会と厚労省が公表している「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス[注19]」には、医療・介護の関係事業者が個人情報を取り扱う上での具体的な留意点や事例などについて記載されている。医療機関におけるクラウドサービスの利用や学会での医療情報の使用などへの対応をはじめとした、医療機関での実態に沿った個人情報保護法の考え方が記されているため、医療機関関係者は必ず理解・対応することが求め

られる。

(2) 厚労省ガイドライン

加えて、医療機関が確認すべきセキュリティガイドラインとして「医療情報システムの安全管理に関するガイドライン（以下、厚労省ガイドライン[注20]）」があり、2022年３月には第5.2版が公表された。もともとは医療機関に対し、個人情報保護法への適切な対応策を示すものとして作成されたが、改定を重ねるごとに情報セキュリティの規定なども盛り込まれ、現在は個人情報保護や情報セキュリティの観点から医療機関などが遵守すべき事項が「A. 制度上の要求事項」「B. 考え方」「C. 最低限のガイドライン」「D. 推奨されるガイドライン」に整理されている。

(3) その他のガイドライン

医療機関が確認すべきその他のガイドラインや指針として、たとえば遠隔読影を行う医療機関では「遠隔画像診断に関するガイドライン 2018」[注21]を確認する必要がある。このガイドラインは、セキュリティ対策を主眼としたガイドラインではないものの、遠隔画像診断を行う端末には「個人の所有する、あるいは個人の管理下にある端末の業務利用（BYOD：Bring Your Own Device）は原則として行わない」と明記されているなど、画像情報の管理体制の一環でセキュリティについて触れられている。

その他、たとえばオンライン診療を行う場合では「オンライン診療の適切な実施に関する指針[注22]」、電子処方箋を利用する場合では「電子処方箋の運用ガイドライン[注23]」、オンライン資格確認を導入している場合では「オンライン資格確認等、レセプトのオンライン請求及び健康保険組合に対する社会保険手続きに係る電子申請システムに係るセキュリティに関するガイドライン[注24]」などが存在する。医療機関は厚労省ガイドラインや個人情報保護法に加え、各医療機関で保持する機能に応じてガイドラインを参照し、ガイドライン内で言及されているセキュリティ対策を確認することが求められる。

Ⅲ 医療機関における セキュリティ対策の実態

このように医療機関が対応すべきガイドラインが整備されている一方で、実態として医療機関におけるセキュリティ対策はどの程度浸透しているだろうか。以下、公開されているレポートから判明している実態と、その要因を医療機関の特性から述べる。

1 外部調査から判明している 医療機関の実態

前述した日医総研のレポート「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」では、主に組織体制、行政の取り組みの認知度、リスクマネジメント体制の三つに分けて結果を整理している。その中で、情報システムの専任の担当部門があるのは全体の20.6％であり、64.4％は兼務の担当者あるいは院長自らが管理していることや、病院における厚労省ガイドラインの認知度は27.9％であることが示されている。

また、インシデント発生時の手順やルールについては、患者・受診者の個人情報漏洩が

あった場合の対応については六割程度が、ウイルス感染や不正アクセスの場合の対応については七割程度が明文化していないこと、さらには病床規模が小さいほど組織体制、行政の取り組みの認知度、リスクマネジメント体制の三つの状況が悪くなる傾向にあることも明らかにしている。

2　医療機関の特性から読み解く要因

こうした実態が起きている背景・要因について、医療機関固有の特性の観点から推察する。

第一に、自明ではあるが医療の主な目的は、患者の治療や人々の健康の維持・増進であり、場合によっては生命にかかわる対応を行っている点である。医療機関、特に病院はこの人命救助の第一線である。

第二に、医療機関、特に病院がこの人命救助の第一線にあるが故に「医療の質」を保つことが重要視される点である。

前提として、組織においてセキュリティ対策を高めていくに当たり、なかなか現場の理解を得られないことが多い。これは、セキュリティ対策の実施によりユーザーである職員が不便を強いられることがあるためで、セキュリティ対策の実施においては「利便性」がセキュリティと対立するもの（利便性を取るか、セキュリティを取るか）として捉えられがちである。一方で医療機関、特に病院では、先の理由から「医療の質」が何よりも枢要なものであり、医療従事者においては「利便性」に加えて「医療の質」が重要視される。「不便であること」が「医療の質の追求を妨げる制約」と捉えられ、「医療の質」とセキュリティとが対立するものとして、結果セキュリティ対応が後回しになってしまうケースが考えられる。たとえば、業務において私物PC端末の利用はセキュリティ上望ましくないが、「医療の質の追求」という観点で利便性を優先し、私物PC端末が利用されている、といったことが起こり得る。

しかし、つるぎ町立半田病院の事例にもあるとおり、実際にセキュリティリスクが顕在化すると医療行為を含む業務の根幹であるシステムに影響が及び、医療の質そのものが損なわれる結果となってしまう可能性がある。医療の質を求めることは非常に重要なことだが、セキュリティ対策を疎かにすることで発生し得るセキュリティインシデントが、医療の質にも影響を及ぼすことを忘れてはならない。医療機関のセキュリティ推進においては、医療の質の観点とセキュリティ対策の観点を両立させること、つまり医療の質を保ちつつ、セキュリティ対策レベルを高める工夫が求められる。

Ⅳ 医療機関が実行すべきこと

では、医療機関は「医療の質」を保ちつつセキュリティを推進するに当たって、何に注意しどう実行すればよいのか。以下に対策のポイントと、実行すべき内容を整理する。

1　厚労省ガイドラインに基づきセキュリティ対策を行う上でのポイント

（1）ルールと体制があってこそ技術対策が活かされる

医療機関は、まず厚労省ガイドラインに基づく対応が必要である。ここで肝心なのは、セキュリティ対策はただ「技術」対策として

セキュリティ製品を導入すればよいものではなく、セキュリティ対策を「ルール」化すること、そしてルールを運用できる「体制」の構築を偏りなく進めることである。医療機関およびその他事業者において、技術の導入を優先的に進め、ルール化や体制の構築は後回しにしてしまうケースが見られるが、導入した技術的対策の効果を継続的に維持・向上するためにも、「ルール」「体制」「技術」はセットで検討すべきである。

たとえばランサムウェアの対策を検討する際には、技術的対策の一つとしてバックアップの取得が考えられる。しかし、この対策に効力を持たせるには、バックアップのための機器を購入・設置しただけでは不十分であり、導入後に必要なタイミングで適切な「担当者（体制）」が適切な「手順（ルール）」に基づき、バックアップの取得対応を実施する必要がある。

(2) 医療機関における役割ごとに考慮するセキュリティ対策は異なる

セキュリティ対策を推進する上では、システム管理者のみが全量を考慮しなければならないのではなく、経営層や医療従事者、事務スタッフ、システム管理者といった役割ごとに考慮しなければならない対策は異なる。

現在の厚労省ガイドラインでは、医療機関における役割ごとに考慮すべき要件が明記されているわけではないが、厚労省が公表している「医療機関のサイバーセキュリティ対策チェックリスト（以下、医療機関向けチェックリスト）[注25]」では明記されているため、適宜用いるとよい。「医療機関向けチェックリスト」は、経営層向け、システム管理者向け、医療従事者・一般のシステム利用者向けの三種類計130問ほどの項目から成り立っており、各役割で考慮すべき対策が整理されている。

(3) インシデント事例などから最新の脅威動向を取り込む

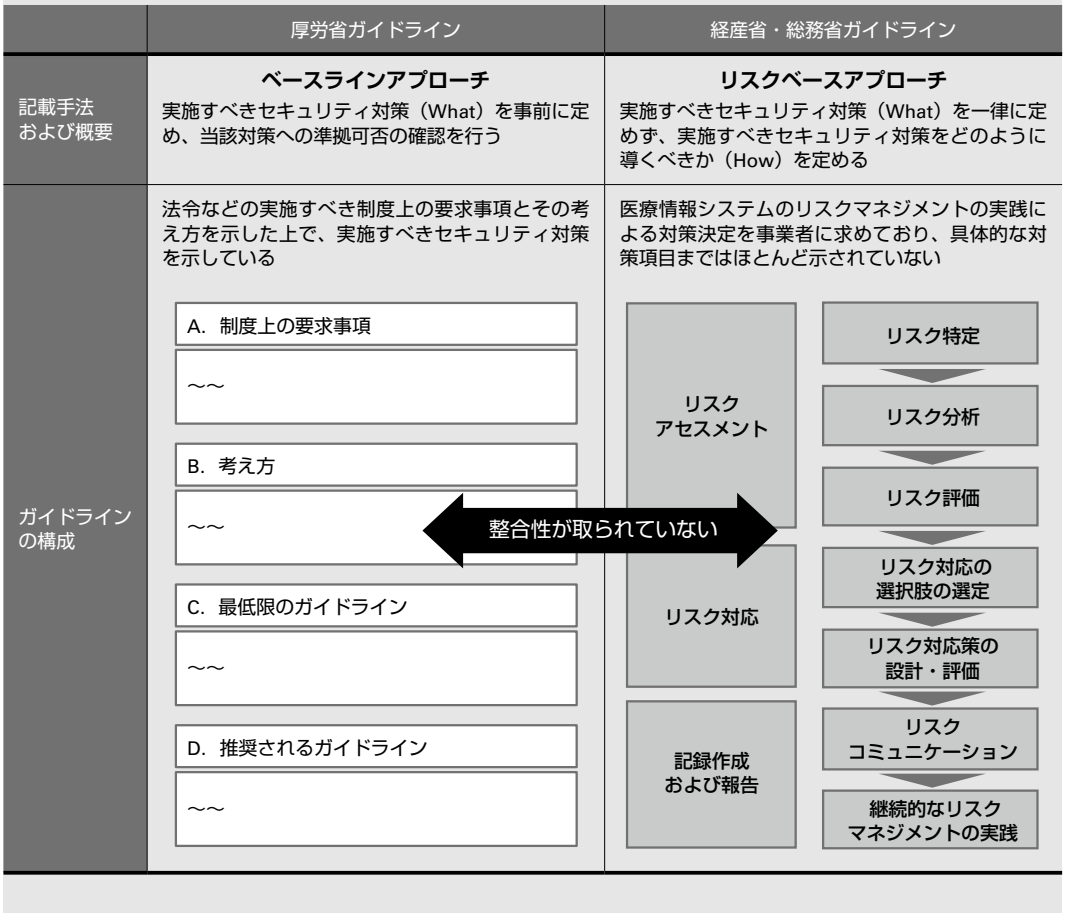
現状の厚労省ガイドラインは数年に一度改定されているが、日々変化する脅威動向にリアルタイムに追いついているわけではない。医療機関側は、報道される医療機関や他事業者のセキュリティインシデントの事例から最新の脅威動向を理解し、事例から学べる教訓を実装するなど、その都度対策をアップデートすることが重要だ。

(4) 経産省・総務省ガイドラインを理解する

前提として、医療機関におけるセキュリティ対策は、医療機関だけなく医療機関が使用する医療機器やサービス、システムの提供側（医療機器メーカーや医療情報を取り扱うシステム・サービス提供事業者）双方で必要だということを忘れてはならない。医療機関のセキュリティ対策実施においては、双方が互いのセキュリティ対策や責任分界点について共通理解を持つことが重要である。

厚労省ガイドラインと併せて扱われることが多いガイドラインとして、経済産業省・総務省が公表している「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、経産省・総務省ガイドライン）[注26]」がある。このガイドラインは、医療機関と契約などを結び、医療情報を取り扱うシステムやサービスを提供す

表2　厚労省ガイドラインと経産省・総務省ガイドライン



る事業者（以下、提供事業者）向けのガイドラインであり、厚労省ガイドラインと併せて三省二ガイドラインと呼ばれ、セットで取り扱われることが多い。

この経産省・総務省ガイドラインでは、提供事業者に実施を求めるセキュリティ対策を列挙するのではなく、提供事業者が自社のシステム・サービスの情報の流れ（情報流）を洗い出し、それを基にリスクを網羅的に導出後、対応策を検討する「リスクベースアプローチ」の手法を取っている。それに対して、厚労省ガイドラインは「ベースラインアプローチ」の手法を取っており、実施すべきセキュリティ対策を列挙しているため、両者間の整合性が取られていない（表2）。

そのため、医療機関は委託先の提供事業者に厚労省ガイドラインで求められるセキュリティ対策を依頼するのみでなく、経産省・総務省ガイドラインに即したリスクマネジメントの実践によるセキュリティ対応を依頼し、委託元医療機関として経産省・総務省ガイドラインの内容も理解することが求められる。

（5）厚労省ガイドラインの改定をウォッチする

たとえば近年は地域医療ネットワークな

ど、医療機関の間で情報連携を行うことが増えているが、現在の厚労省ガイドラインでは基本的に個々の医療機関を対象とした記載となっており、複数の医療機関がまとまったシステムが想定されていないという課題がある。

厚労省ガイドラインの内容は、こうした課題に対し数年に一度の改定で改善が図られるため、医療機関は厚労省ガイドラインが改定されたタイミングでその都度改定事項を確認し、医療機関の対策も併せてアップデートすることを忘れてはならない。なお、2022年6月7日に閣議決定された「新しい資本主義のグランドデザイン及び実行計画・フォローアップ[注27]」のフォローアップ資料では、医療のDX投資の記載の中で厚労省ガイドラインについて、「最新の技術的な動向、多様化・巧妙化する医療機関へのサイバー攻撃状況などを踏まえて、2022年度中に見直す」と言及している。

2 大規模な医療機関はセキュリティアセスメントによる現状把握から

大規模な医療機関（大・中規模の病院や大手薬局など）ほど、多様な業務やシステムを有しており、さまざまなセキュリティリスクが存在し得る。影響度の大きなリスクへの対策から優先的に対応するなど、セキュリティ対策を効率的に推進するため、まずはセキュリティアセスメントによってリスクの全容を明らかにすることが望ましい。

具体的には、現在のセキュリティ対策レベルを可視化するために、厚労省ガイドラインで実施を求められている事項と医療機関の現状の対策を整理することで、実施できていない対策事項を抽出する。ここで、医療情報システムを提供する事業者には経産省・総務省ガイドラインへの準拠対応を依頼し、「サービス仕様適合開示書」などの文書で委託先の対策状況を収集する。

現状で対策ができていないリスクを洗い出した後は、影響度の大きいリスクから実施すべきである。このとき、実施する対策は医療機関のルール（運用管理規程）として文書化するとともに、対策を実行するための体制の整備が求められる。

3 小規模の医療機関はチェックリストの確認から

小規模の医療機関（クリニックや個人経営の薬局など、もしくは大規模な医療機関であるものの前節の内容を実施できる予算や人員がいない場合）においても、大規模な医療機関と同じく、まずは現状を把握することが重要である。前述した厚労省公表の医療機関向けチェックリストの項目に回答し、未実施の項目に対して順に対策を実施していくことが望ましい。

加えて、厚労省から公表される通知を定期的に確認し、新しい規制をウォッチしていくことも重要である。一般的なお知らせのほかに、厚労省が実施している検討会の資料なども確認しておきたい。たとえば「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[注28]」では、数カ月に一度のペースで医療情報の利活用に関する推進とセキュリティ対策について議論されている。資料からは医療機関におけるサイバーセキュリティ対策の厚労省の取り組み方針を確

認することができるため、今後より重要視されるセキュリティ対策の動向などを読み取ることも可能だ。

V 最後に

医療分野は、内閣サイバーセキュリティセンター（NISC）が2017年に発行した「重要インフラの情報セキュリティ対策に係る 第4次行動計画」において「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤[注29]」として、重要インフラに指定されている。重要インフラの一つとして、医療機関としての機能を継続的に患者に提供するためにもセキュリティ対策の実施は必要な対応である。

そのような中、健康（Health）と技術（Technology）を掛け合わせたヘルステック（HealthTech）と呼ばれる造語が生まれるなど、健康・医療・介護分野における課題をICTやAI技術で解決するソリューションやサービスを生み出すベンチャー企業やスタートアップ、新たにこの分野に挑む既存企業が増加している。加えて、「IoMT（Internet of Medical Things）」と呼ばれるIoTと医療を組み合わせた言葉があるように、遠隔で手術可能なロボットや患者が身に着けることで血糖値が測定できるウエアラブルデバイスなど、高度な医療機器は誕生し続けている。

このような技術革新によって患者に提供される医療の質が進化する中で、医療システムに接続される機器や取り扱われるデータ量は今後増え続け、同時にセキュリティ面で管理すべき対象やアタックサーフェス（攻撃対象領域）も増え続けることになる。

状況が目まぐるしく変化する中でも、患者が安心して医療機関を利用できる状況を維持するために、医療機関におけるセキュリティ対策は今まで以上に重要になる。医療機関は国や提供事業者などのステークホルダーと協力しながら、適切なセキュリティ対策を実施することが求められる。

注

1 日経メディカル「奈良の宇陀市立病院がランサムウエアの被害に」
https://medical.nikkeibp.co.jp/leaf/mem/pub/hotnews/int/201810/558453.html

2 産経新聞「患者情報など3700人流出疑い 多摩北部医療センター 医師に不正アクセス」（2019/5/20）
https://www.sankei.com/article/20190520-QVGFQEGWVNKFXMDVTS3LW72AFY/

3 横浜市立大学附属病院「公立大学法人横浜市立大学記者発表資料」（2019/8/5）
https://www.yokohama-cu.ac.jp/news/2019/dr3e64000000pb77-att/20190805_info.pdf

4 朝日新聞「殺人被害者のカルテ、業務外で閲覧か　新潟大病院が調査」（2020/1/29）
https://www.asahi.com/articles/ASN1Y4DQWN1YUOHB001.html

5 日本経済新聞「福島医大病院でランサム被害 17年夏、公表せず」（2020/12/2）
https://www.nikkei.com/article/DGXMZO66895900S0A201C2CC1000/

6 日本経済新聞「サーバー復旧、通常診療へ 徳島のサイバー攻撃被害病院」（2022/1/3）
https://www.nikkei.com/article/DGXZQOUF0316J0T00C22A1000000
朝日新聞「サイバー攻撃受けた徳島・半田病院 約2カ月ぶりに通常診療全面再開」（2022/1/4）
https://www.asahi.com/articles/ASQ145J9MQ13PTLC00P.html
徳島県つるぎ町立半田病院「徳島県つるぎ町立

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」
https://www.handa-hospital.jp/topics/2022/0616/index.html
日経クロステック「ランサムウエア攻撃に遭った徳島・半田病院、被害後に分かった課題とは」
https://xtech.nikkei.com/atcl/nxt/column/18/01157/041900059/
7 朝日新聞「日本歯科大病院のサーバーがウイルス感染　電子カルテ使えず診療停止」(2022/1/18)
https://digital.asahi.com/articles/ASQ1L4TX0Q1LULZU007.html
8 “First GDPR fine in Portugal issued against hospital for three violations”（iapp）
https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/
9 東洋経済オンライン「コロナ対応のチェコ病院でサイバー攻撃の衝撃　世界で増加『コロナ便乗の攻撃』の怖い実態」(2020/3/22)
https://toyokeizai.net/articles/-/338041?page＝4
10 AP通信“German hospital hacked, patient taken to another city dies”
https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94
11 総務省「情報セキュリティの概念」
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/02.html
12 厚生労働省「医療機関を標的としたランサムウェアによるサイバー攻撃について（再注意喚起）」
https://anshin.pref.tokushima.jp/med/experts/docs/2021112800010/files/001.pdf
13 日本医師会総合政策研究機構「日医総研ワーキングペーパー　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」
https://www.jmari.med.or.jp/download/WP453.pdf
14 一般社団法人医療 ISAC「国内病院に対するセキュリティアンケート調査の結果と考察」
https://www.m-isac.jp/wp-content/uploads/2021/12/Report_20211201.pdf
15 厚生労働省「医療分野の情報化の推進について 医療分野の情報化の現状『電子カルテシステム等の普及状況の推移』」
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html
16 厚生労働省「医療機関を取り巻く情報セキュリティ対策の現状」
https://www.mhlw.go.jp/content/10808000/000644753.pdf
17 警察庁「令和3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」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf
18 情報処理推進機構「事業継続を脅かす新たなランサムウェア攻撃について『人手によるランサムウェア攻撃』と『二重の脅迫』」
https://www.ipa.go.jp/files/000084974.pdf
19 厚生労働省 個人情報保護委員会「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」
https://www.mhlw.go.jp/content/000909511.pdf
20 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5.2版（令和4年3月）」
https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html
21 日本医学放射線学会「遠隔画像診断に関するガイドライン 2018」
http://www.radiology.jp/member_info/guideline/20190218_01.html
22 厚生労働省「オンライン診療の適切な実施に関する指針」
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/rinsyo/index_00010.html
23 厚生労働省「電子処方箋の運用ガイドラインの一部改正について」
https://www.mhlw.go.jp/stf/denshishohousengl_00005.html
24 厚生労働省「オンライン資格確認等、レセプトのオンライン請求及び健康保険組合に対する社

会保険手続きに係る電子申請システムに係るセキュリティに関するガイドライン」
https://www.mhlw.go.jp/content/10200000/000679712.pdf
25 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/stf/shingi/0000516275_00002.html
26 経済産業省・総務省「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」
https://www.meti.go.jp/press/2020/08/20200821002/20200821002.html
27 内閣官房「新しい資本主義のグランドデザイン及び実行計画・フォローアップ（2022年）」
https://www.cas.go.jp/jp/seisaku/atarashii_sihonsyugi/index.html
28 厚生労働省「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」
https://www.mhlw.go.jp/stf/shingi/other-isei_210261.html
29 内閣サイバーセキュリティセンター「重要インフラグループ」
https://www.nisc.go.jp/policy/group/infra/index.html

著者

内橋七海（うちはしななみ）
NRIセキュアテクノロジーズ リスクマネジメントコンサルティング部グローバル＆リサーチグループコンサルタント
専門は医療機関、医療機器メーカーをはじめとした医療分野のセキュリティ全般、およびセキュリティアセスメント、規程・プロセス策定など