国内医療情報セキュリティに関する提言

――ランサムウェアリスクに直面する国内医療機関が優先すべきセキュリティ対策とは

pwc

Microsoft

目次

はじめに

昨今、医療機関（病院や診療所を指す。以下同）を標的としたサイバー攻撃が活発化しており、その被害事例がここ1、2年で多く見受けられている。最近では国内の医療機関においても医療情報システムがランサムウェアによる被害を受け、患者診療の継続性に影響を及ぼすさまざまなセキュリティインシデントが発生している。従来までは医療機関におけるセキュリティインシデントは機微性の高い患者情報の漏えい（機密性）が中心であったが、今や医療情報システムの可用性に着眼したサイバー脅威が高まっている。こうした脅威に対するセキュリティの強化は喫緊の課題になっていると言える。

国内には医療情報システムのセキュリティを考える上で不可欠なガイドラインが存在する。いわゆる「3省2ガイドライン」と呼ばれるもので、厚生労働省が医療機関向けに公表する「医療情報システムの安全管理に関するガイドライン」と、経済産業省・総務省が医療情報システム開発・運用事業者（以後、「IT事業者」と記載）向けに公表する「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」がそれに当たる。「3省2ガイドライン」は国内では医療情報システムのセキュリティを考えるうえでの、いわゆるバイブルであり、このガイドラインへの準拠をもって医療機関におけるセキュリティの信頼性が担保されると考えられる傾向が強い。しかしながら、**サイバー攻撃へのセキュリティ対策という観点から「3省2ガイドライン」を精読すれば、それは誤解であることが理解できる。**「3省2ガイドライン」への対応をもってサイバー攻撃への対策が万全であるとする誤解を解きほぐすことが、医療機関およびIT事業者が正しい目線をもって直近のサイバー脅威に対応するためにも重要であると言える。

また、国内の医療機関がセキュリティ強化の必要性に直面している一方、その多くはセキュリティに専門的に対応できるほどの経済的・人的資源を十分に保有できていないという実態がある。このような状況でガイドラインに基づきセキュリティ管理を実施しようとした結果、**医療機関の多くではセキュリティ上の共通課題が生じている**と考えられる。こうした実態を踏まえた上で、喫緊の課題となっているランサムウェアという脅威に直面する医療機関として、少なくとも対応すべき必須のセキュリティ対策とは何であるのか、について考えなければならない。

上記前提のもと、本稿では、第1章で、「3省2ガイドライン」がどのような要件により構成されているのかという観点から、医療情報システムのセキュリティにおけるバイブルが対象とするスコープを解説する。続いて第2章では、国内の医療機関における経済的・人的な資源不足が医療情報システムのセキュリティ管理にどのような影響を及ぼしているかについて解説することで、国内の医療機関固有のセキュリティ管理体制上の課題を考察する。そして第3章では、こうした課題に基づき、経済的・人的な資源不足に直面する国内の医療機関がランサムウェアという目前に迫るサイバーリスクに対して、どのような技術的対策を優先的に実施すべきかについて、PwCあらた有限責任監査法人（以下、PwCあらた）と日本マイクロソフト株式会社（以下、日本マイクロソフト）が共同で考察を行い、その結果に基づく提言を示している。

なお、各章の読者には、第1章は医療機関およびIT事業者双方、第2章は主にIT事業者、第3章は主に医療機関を想定している。

本稿が、医療の継続性を損なうランサムウェアというサイバー脅威に対してどのような対策を優先的に実施すべきなのかについて、国内の医療機関およびIT事業者が正しい相互理解のもとで、適切にコミュニケーションを行うための一助となることを願っている。

1. 3省2ガイドラインの概説

1.1 前提

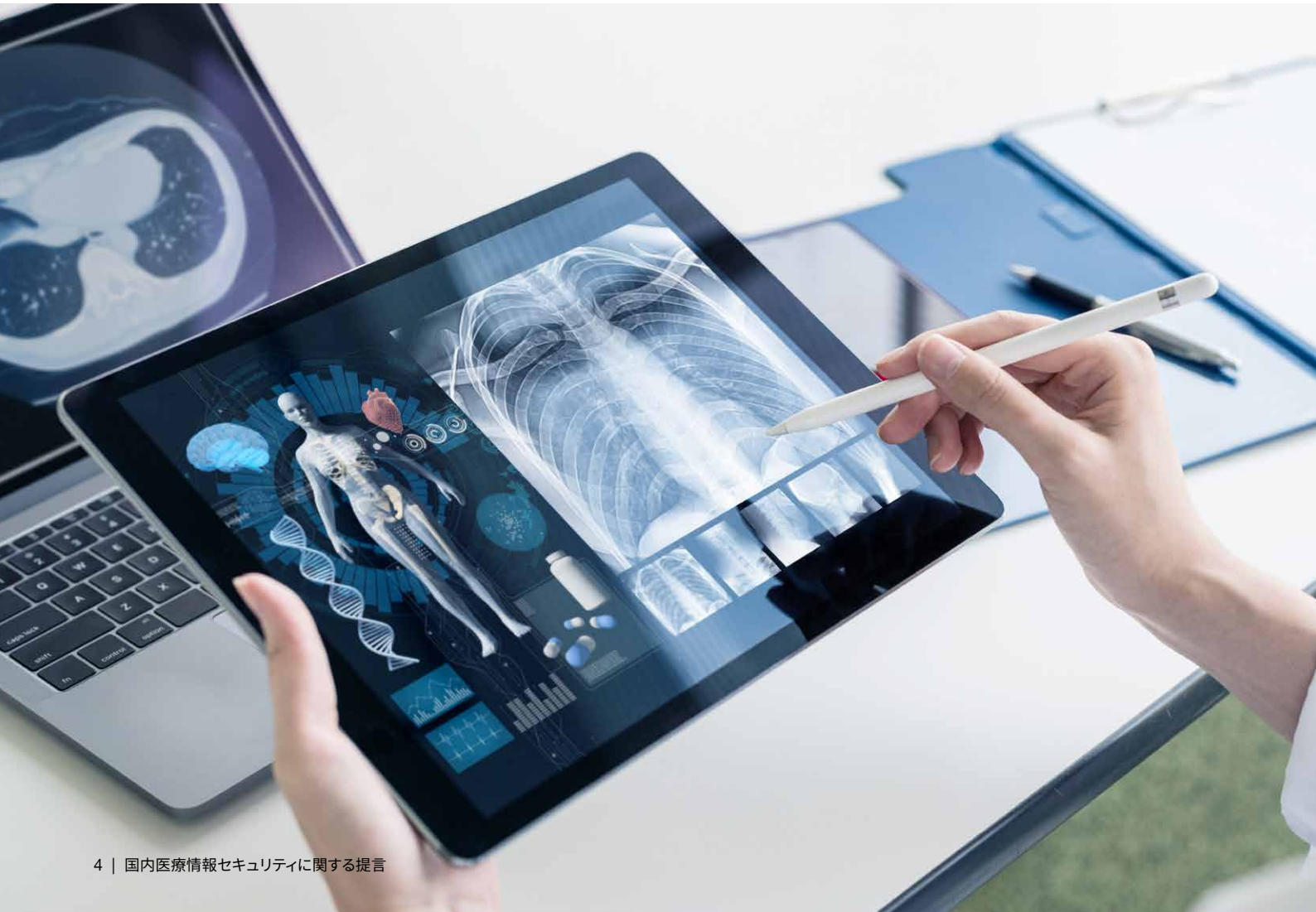
現在、「3省2ガイドライン」として通称されるものは、厚生労働省が医療機関向けに公表する「医療情報システムの安全管理に関するガイドライン[1]」（以後「厚生労働省安全管理ガイドライン」と記載）、および経済産業省・総務省がIT事業者向けに公表する「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン[2]」（以後「経済産業省・総務省安全管理ガイドライン」と記載）の2点である。

医療情報システムが抱えるセキュリティリスクは多様化しており、従来のセキュリティ管理アプローチ、つまり標準的なセキュリティ管理ルールを定義し、そのルールに基づく対策を推奨するアプローチでは、さまざまなリスクに十分に対応することが困難になってきた。そのため、2020年8月に改定された経済産業省・総務省安全管理ガイドラインでは、医療情報システムにおけるデータの流れに着眼し、IT事業者がセキュリティリスクの特定・分析・評価を行い、合理的なセキュリティ対策の設計とその継続的な運用を求めるというリスクベースの管理アプローチ（リスクマネジメント）を全面に打ち出すことになった。さらに、IT事業者はそのリスクマネジメントの内容を、医療機関がユーザーとして実施すべきリスク評価へ活用できるように説明を行った上で、医療情報システム全体のセキュリティを確保するためにお互いが何をなすべきかについて、合意形成を図ることが求められている。このように、セキュリティリスク管理体制全体を維持するための互いの役割について、従前より能動的に医療機関等とのコミュニケーションを図ること、つまりリスクコミュニケーションが重視されることになった。

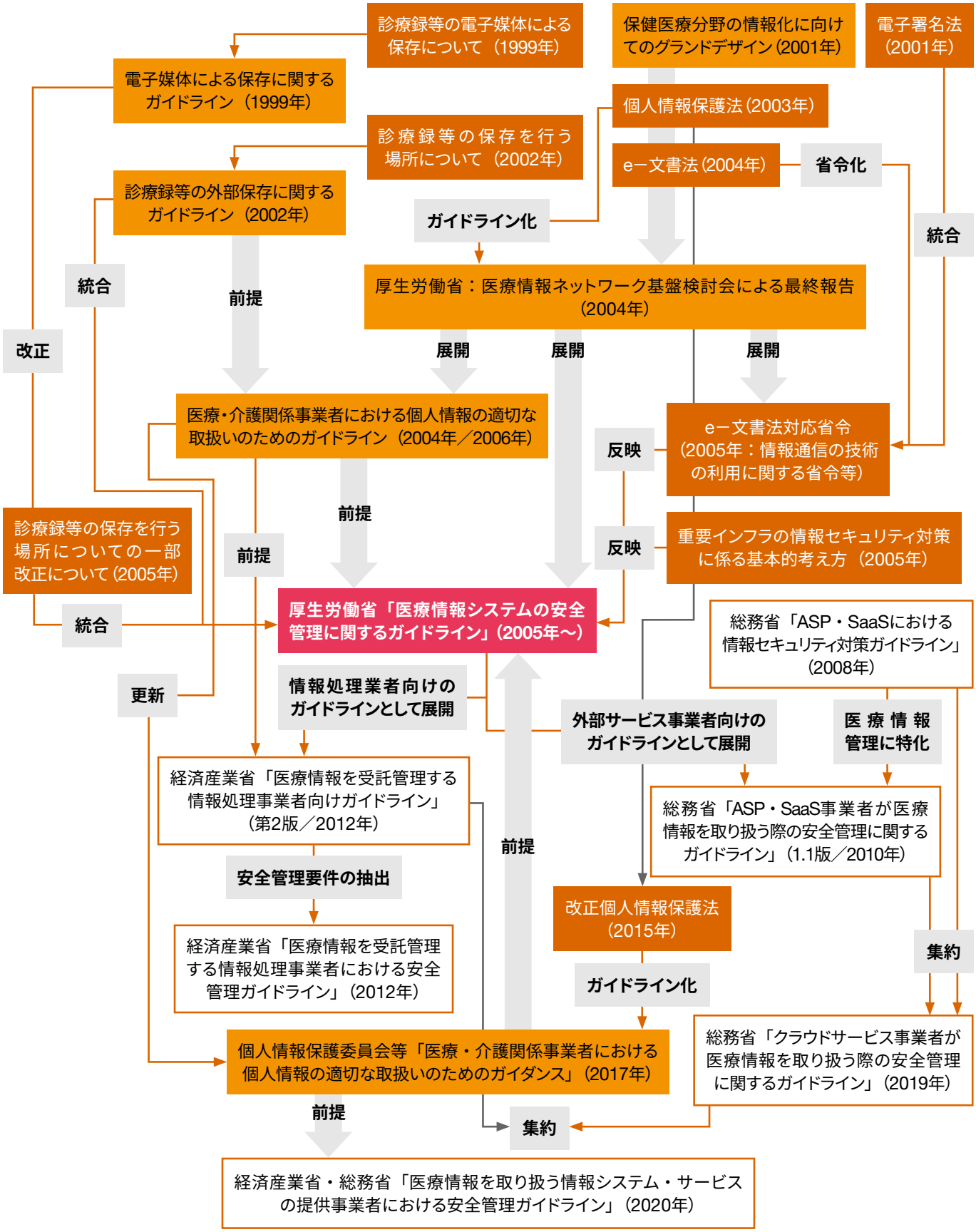
ただし、これらのガイドラインは、法令やその他ガイドライン、官公庁の通知・事務連絡等、さまざまな要件検討の変遷を経て歴史的に形成されているものである。そのため、内容も複雑であり、こうした背景への理解が十分でない場合、ガイドラインが求める要件を適切に理解することも困難になると言える。

---

1 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」（5.1版）https://www.mhlw.go.jp/content/10808000/000730541.pdf
2 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/2020/08/20200821002/20200821002-3.pdf



図表1：国内における医療情報の電子管理を取り巻く変遷



また、経済産業省・総務省安全管理ガイドラインは厚生労働省安全管理ガイドラインの内容を元に制定され、改定・更新が行われ、現在の形に至っている。そのため、マネージすべきリスク、コミュニケーションされるべきリスクの範囲も、おのずと厚生労働省安全管理ガイドラインが求める基本的な要件を前提としている。この前提についての理解が適切でない場合、日々巧妙化・高度化するサイバー攻撃に直面する医療機関において真に必要となるセキュリティ対策とは何かについて、「3省2ガイドライン」も踏まえた観点から適切に検討を行うことは難しい。そこで次節では、厚生労働省安全管理ガイドラインを構成する3つの重要な要件について解説を行う。

1.2 重要な要件

① 電子保存の要件

まず1点目の重要な要件は、医療情報を管理する媒体に関する要件である。1990年代後半の情報技術革命の中で、従来まで医療機関が紙媒体で管理していた医療情報を電子的に管理するための検討が行われ、厚生労働省（当時は厚生省）より、「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン[3]」（図表1では「電子媒体による保存に関するガイドライン」と記載）が1999年に公開された。本ガイドラインでは医療情報を電子的な媒体で保存する場合の要件が整理された。また、医療情報の一部には医師による記名押印または署名が法的に義務付けられていたが、紙媒体での文書であればインクペンによる署名が可能であった一方、電子文書では電子的な署名行為が必要となる。この署名等の行為は医師としての診断結果の信頼性を担保するものであるが、電子的に署名等の行為を行う場合の要件は2001年に制定された電子署名法により定められることになる。

加えて、医療情報は患者の診療内容等を記録する実務的な文書であると同時に、医師法・医療法等の関連法令によって保存期間が法的に義務付けられた行政上の法定保存文書としても位置付けられる。そのため、行政上の文書としても電子的な保存要件の整理が必要になるが、これらは2004年のe－文書法、および2005年の「厚生労働省の所管する法令の規定に基づく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省令[4]」（図表1では「e－文書法対応省令」と記載）により整理されることになる。なお、それまでは、紙媒体で管理していた医療文書をスキャニングして電子化しても紙媒体同等の信頼性のある文書とは判断されなかったが、同法・省令により、医療分野でもスキャニングによる電子化が認められるようになった。

このような経緯で、「3省2ガイドライン」における重要要件の1つ目である、**「電子保存」**の要件、つまり医療情報を電子的な媒体にて管理するための媒体要件は複合的に定められている。

図表2：重要要件および各要件の根拠となる関連法令等

	主だった関連法令や通知等
電子保存 （媒体要件）	✓ 電子媒体による保存に関するガイドライン ✓ 電子署名法 ✓ e－文書法
外部保存 （場所要件）	✓ 診療録等の外部保存に関するガイドライン ✓ 厚生労働省通知：「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
個人情報保護 （データそのものの管理要件）	✓ 個人情報保護法 ✓ 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

3 厚生労働省「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン等について」
https://www.mhlw.go.jp/web/t_doc?dataId=00ta6431&dataType=1&pageNo=1
4 厚生労働省「厚生労働省の所管する法令の規定に基づく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省令」の概要
https://www.mhlw.go.jp/topics/2005/03/tp0328-1a.html

② 外部保存の要件

2点目は、医療情報が管理される場所に関する要件である。紙媒体で法定保存義務のある医療情報を管理する場合、例えば、患者の紙カルテを冊子に閉じてラックで施錠管理する等、今までは病院内部で保管することが慣例的であった。しかしながら、医療情報を電子的に取り扱うシステムを開発・運用する業務を委託された外部の事業者は院外に施設を持ち、当該施設でシステム関連の業務を行うケースも多い状況であった。そのため、2002年に「診療録等の外部保存に関するガイドライン」（平成14年5月31日付け医政発第0531005号）が厚生労働省より公開され、医療機関の外部でも医療情報の一部の管理を行うことが認められた。なお、その後、厚生労働省安全管理ガイドラインが発行された2005年以降も、この外部保存の要件は、厚生労働省により複数回の見直しが図られており、調剤録等も含め、段階的に幅広い医療情報の**「外部保存」**が認められるようになっている。

③ 個人情報保護に関する要件

3点目は、医療情報の守秘性に関する要件である。医療情報は患者の病歴や治療歴等、機微性の高い情報の束であり、国内の刑法[5]でも医療従事者が患者情報を第三者に口外することは禁じられている。また、古くはヒポクラテスの誓いにまで遡るように、医師に対して守秘義務は非常に強く求められるものであった。一方、医療従事者以外の視点に立った場合、この要件の根拠は2003年に制定された個人情報保護法となる。個人情報保護法において、例えば医療情報システムの開発・運用業務を委託されるIT事業者に対しても、医療従事者同等の配慮のもとで、患者の個人情報を取り扱わなければならないこと、つまり**「個人情報保護」**が定められるようになった。医療分野固有の個人情報保護上のガイダンスも2004年に公開されたとおり、医療分野における情報の管理は業態固有の特殊性があることが分かる。

このように1990年代後半から2000年代初頭にかけて、**「電子保存」「外部保存」「個人情報保護」の3つの重要要件**が整理されていく中で、各ガイドラインや関連法の要件を統括し、1つのガイドラインとして整理したものが、2005年に公開された厚生労働省安全管理ガイドラインである。これらの重要な要件は現在の「3省2ガイドライン」においても大きく変化することはない。

1.3 ガイドラインのセキュリティスコープ

このように、あくまで**「3省2ガイドライン」は、その経緯・目的から、紙媒体で管理されていた医療情報を、IT事業者のシステムにて、医療従事者に求められる水準同等の守秘性および厳格性をもって外部保存・管理するために必要な要件をまとめたもの**、という位置付けである。よって、巧妙化・高度化されるサイバー脅威を前提にした適切なセキュリティ管理策にまで踏み込んだ管理要件を定義したものではないという点に留意しなくてはならない。当今の医療機関を脅かすランサムウェアというサイバー脅威への対策を考えるためには、もう一歩踏み込んだ検討が必要になると言える。

なお、上記の位置付けを証示するように、厚生労働省は2021年10月に厚生労働省安全管理ガイドラインの別添資料として「医療機関のサイバーセキュリティ対策チェックリスト」[6]および「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」[7]を公表している。これは上述した、ガイドラインの基本的なリスク管理要件を補足する目的のもと、医療機関が検討すべきサイバーセキュリティ対策をまとめたものである。ただし注意すべき点は、**本別添資料はあくまでさまざまなサイバー攻撃を前提とした全般的なセキュリティ管理策を整理したものであり、ランサムウェアというリスクに個別に焦点を当てたものではない**ということである。これらの施策を字義通り実施することを、医療機関を現在取り巻く具体的なサイバー脅威――つまり、ランサムウェアに対する現実的な対応策を実施することと同一だと捉えることは危険と言える。

現在国内の医療機関に求められているセキュリティは、サイバー攻撃全般を対象とした一般的なセキュリティ対策よりも、ランサムウェアという具体的な危機に対するセキュリティ対策である。こうしたセキュリティ対策を医療機関に導入するための適切な方法を検討するためには、まず医療機関におけるセキュリティ管理状況の実態を理解することが重要である。

5 刑法134条 第十三章　秘密を侵す罪 https://elaws.e-gov.go.jp/document?lawid=140AC0000000045
6 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
7 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/10808000/000844703.pdf

2. 国内医療機関における医療情報セキュリティに関する考察

2.1 セキュリティ上の課題

国内の医療機関のセキュリティ管理実態を対象とした調査としては、2021年に入って、公益財団法人医療機器センター[8]、日本医師会総合政策研究機構[9]、一般社団法人医療ISAC[10]が相次いでそれぞれ調査資料を公表している。これらのレポートからは、**病院の規模が小さくなるにしたがって、医療機関におけるセキュリティ投資費用（経済面のセキュリティリソース）やIT管理部門の充実度（人的なセキュリティリソース）が低下し、比例するようにセキュリティ管理水準も下がるという全体傾向がある**ことが把握できる。

多くの医療機関は公定価格に基づく保険診療による収入を得ているが、その収入は診療報酬によって厳しく左右され、隔年の診療報酬の改定率も縮小傾向にあり、収益差額も基本的にマイナスが多い状況[11]である。さらに、医療機関は労働集約型の組織構造である。そのため、人件費が費用の半分以上を占めることが一般的であるが、医業従事者の数の見直しは医療提供水準へ直接的な影響を及ぼすリスクが高いことから、可能な限り、周辺的な間接領域の緊縮化による収益性の向上を図る傾向がある。IT管理部門をはじめとした間接部門の縮小はその典型であり、病院規模が小さいほど経済的・人的なセキュリティリソースが低下することは、こうした病院経営を取り巻く大きな動向の中で構造的に発生しているものと言える。

最新の厚生労働省の調査結果からは、20床以上の医療機関の件数は8,000件超であるが、そのうち500床以上の大規模な病院割合は全体の5%程度にも達していない。また。20床以下の一般診療所の件数は10万件程度と報告されているが[12]、こうした一般診療所等も含めて考えた場合、専門的なIT管理組織を持ち、専任の職員が適切な役割分担のもとでシステムやセキュリティの管理を組織的に行える医療機関はほんの一握りと考えるべきである。多くの医療機関では、院内でITに相対的に詳しい職員が他の業務と兼務でシステムやセキュリティの管理を担わされているという**「名ばかりIT担当者」も決して例外ではなく、むしろそのような状況の方が多い**と言える。

このような状況にもかかわらず、医療機関としては「3省2ガイドライン」も含め、セキュリティ対応を行わなければならない。私たちの考察によれば、こうした背反した要求に対して、リソース不足の医療機関は、次にあげる主に3つの状況に直面している傾向が強いと言える。

① IT事業者への依存

院内のIT担当者のリソースが不足していることから、医療情報システムの設計・開発・導入に至る一連の作業は基本的にIT事業者に委任することになり、IT事業者主導で推進される傾向が強くなる。

院内のIT担当者としては、医療情報システムの管理においては医療機関が遵守すべき厚生労働省安全管理ガイドラインも含む各種関連ガイドラインへ準拠した開発・運用業務をIT事業者が責任をもって実施していると考える。一方、IT事業者は契約に基づく業務提供を行っているという認識を持つ。そのため、医療機関／事業者間で責任範囲に関する認識が異なり、本来求められるセキュリティ対応が十分でないという状況が多く見受けられている。このようなケースでは、院内のIT担当者に対してセキュリティ対策について確認をした場合、「IT事業者が行っているはず」との回答が多いことも特徴である。なお、院内IT担当者がこの事実を認識して、セキュリティ管理策をガイドラインに基づき自主的に実施しようにも、IT事業者が提供するシステム固有の規格・仕様の制約により、本来実施すべき対策が十分に行えない状況に陥るという別の課題も見られる。

② 非機能要件の軽視

医療情報システムの設計・開発は、限られた経済的なリソース（コスト）でIT事業者に委託せざるを得ない。そのため、予算面の制約から、医療従事者が望む業務要件（機能要件）がまずは優先されることになり、医療業務の効率性にとって副次的なものに位置する、セキュリティ等の非機能要件は相対的に劣後するという傾向が強い。設計・開発の時点で事前にセキュリティ等の要件を組み込めないまま運用が開始された医療情報システムに、事後的に同種の機能を搭載することは、ユーザーの混乱を招くなど現場の反発も強くなり、踏み込んだ対応ができないという状況に陥るケースも多い。

③ 院内システム・セキュリティの統合管理の困難

院内のIT担当者のリソースは限られているため、おのずと院内の部門システムの管理は各部門が主導となり、また個々の部門がIT事業者と直接交渉の上で導入や保守・運用の調整が図られ、事後的に院内のIT担当者へ報告が行われるケースがよく見受けら

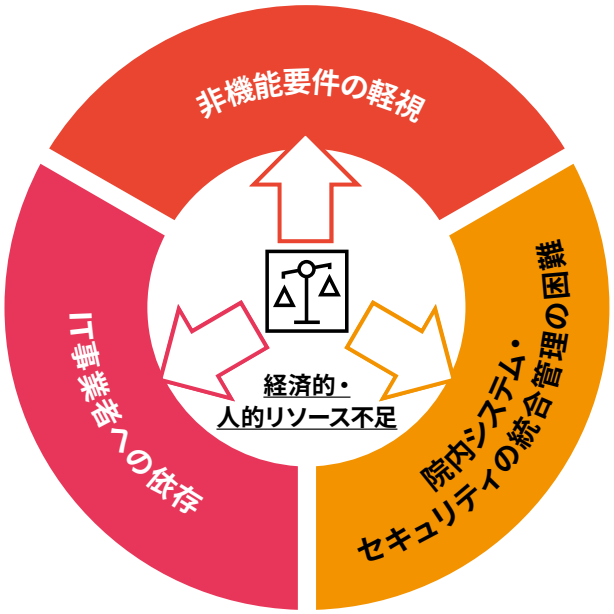
8 公益財団法人医療機器センター「医療機関の情報システムの管理体制に関する実態調査　調査結果概要」（2021年3月）
http://www.jaame.or.jp/mdsi/cs21/CS-hdos.pdf
9 日本医師会総合政策研究機構 日医総研ワーキングペーパー「病院・診療所のサイバーセキュリティ：医療機関の情報システムの管理体制に関する実態調査から」（2021年4月27日）https://www.jmari.med.or.jp/download/WP453.pdf
10 一般社団法人医療ISAC「国内病院に対するセキュリティアンケート調査の結果と考察」（2021年12月）
https://www.m-isac.jp/wp-content/uploads/2021/12/Report_20211201.pdf
11 厚生労働省「医療経済実態調査」https://www.mhlw.go.jp/bunya/iryouhoken/database/zenpan/iryoukikan.html
12 厚生労働省「令和元（2019）年医療施設（動態）調査・病院報告の概況」（2020年9月）
https://www.mhlw.go.jp/toukei/saikin/hw/iryosd/19/dl/09gaikyo01.pdf

れる。このように各部門主導で導入・運用されている部門システムに対して、事後的に医療機関としての統一的なセキュリティポリシーに基づく管理を図ることは極めて困難である。そのため、院内のIT担当者が主管する基幹系システムのセキュリティ水準とその他の部門システムのセキュリティ水準が統一されないまま、分散的に管理されることが多い。さらに部門システムと基幹系システムとの接続が医療従事者から求められ、現場の声に押し負けて、接続を許可することで、結果的に基幹系システムのセキュリティ管理水準が低下してしまうというケースも少なくない。

このようにセキュリティリソースが不足する国内の医療機関の多くでは、IT事業者主導でシステム設計・開発が行われることから、システム固有の規格による制約が強く存在することになる。これを脱して柔軟なシステム間連携やセキュリティを講じようにも追加開発が必要となるなど高コストになりやすく、容易な対応は難しいという問題がある。さらに医療情報システムはコスト面の制約により業務要件が優先され、非機能要件としてのセキュリティ要件は相対的に優先度が低下する傾向があり、前述の問題とともに、適時のセキュリティ対応の困難さがさらに深まることになる。

こうした状況に加え、院内の各部門が部門システムの導入・運用に向けた調整をIT事業者と行う中で、部門ニーズに個別最適化したシステム設計が多くなる傾向がある。IT事業者主導で、業務要件中心に導入された部門システムも含め、**事後的に全体最適の観点より院内の統括的なセキュリティの管理を行うことは実質的に難しく**、リソース不足の医療機関ではこのような課題に直面することが多い。

図表3：リソース不足が招く国内医療機関のセキュリティ上の課題



■ IT事業者への依存

IT事業者中心にシステム開発・運用が行われ、セキュリティも同様にIT事業者が実施しているという盲目的な信頼に陥りやすい。

■ 非機能要件の軽視

限られた最低限のコストで事業者にシステム開発・運用を委託するため、業務要件（機能要件）が最優先され、セキュリティ要件等の非機能要件は劣後する。

■ 院内システム・セキュリティの統合管理の困難

院内横断的な重要な基幹システムの管理にリソースを注力せざるを得ず、部門システムの導入・管理は各部門主導で行われる傾向が高い。そのため、中央集権的なセキュリティの整備を行うことが困難になる。

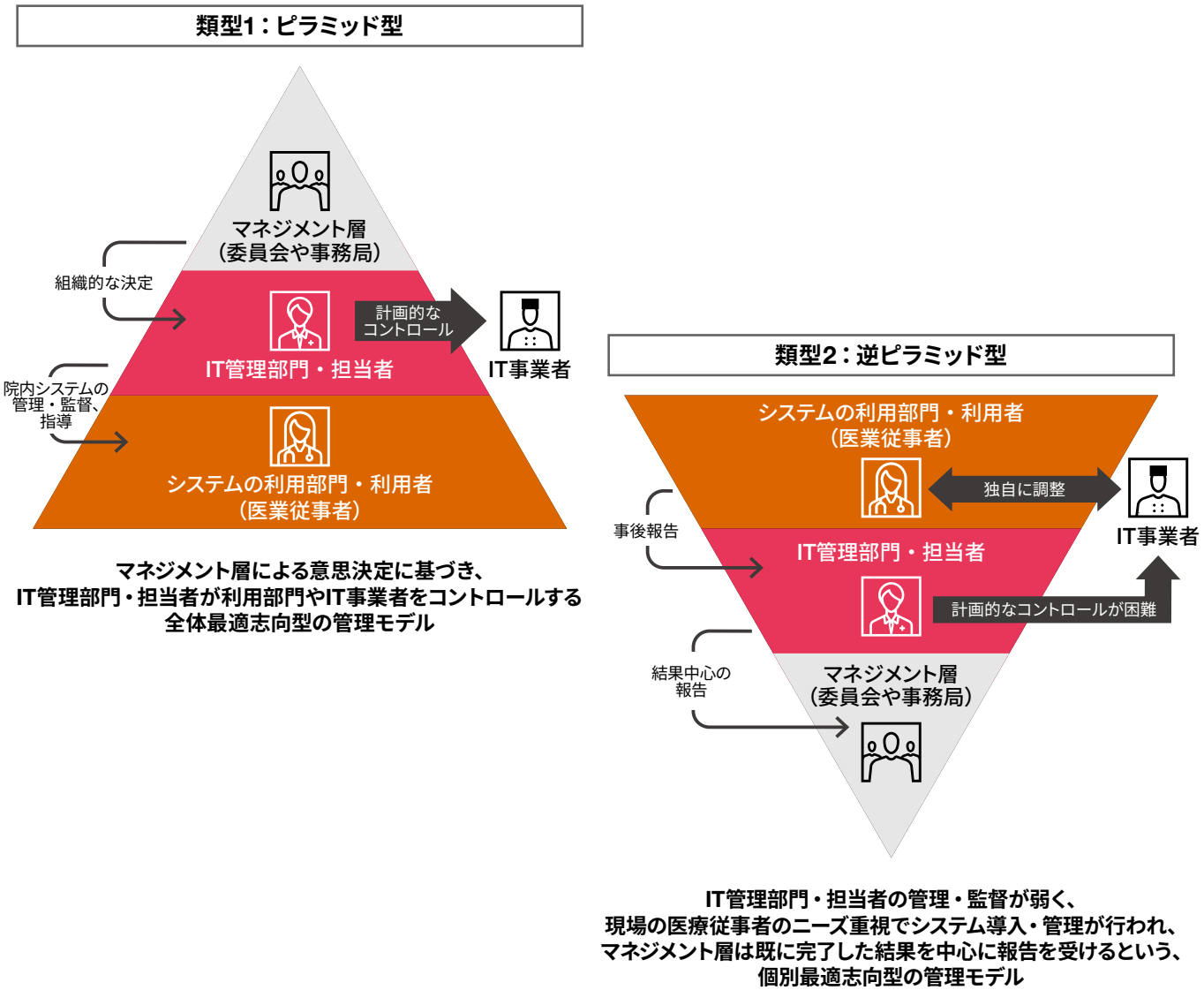
こうした課題を招きやすい、国内の医療情報システムの管理状況は、主に以下の2つに分類することができるだろう。

類型1（ピラミッド型）では理事長・院長等を含む上位組織体の管理・監督のもと、IT管理部門・担当者が計画的にIT事業者をコントロールしつつ、システム利用部門等の統括を図っていくモデルである。これは経済的・人的なリソースに恵まれた一部の病院のみに見られるものである。

一方で、経済的・人的なリソースが不足する医療機関の多くでは、類型2（逆ピラミッド型）のように、システム利用部門・利用者が医療情報システムの調達・管理業務に強い意思決定権を持ち、IT管理部門・担当者はIT事業者へのコントロールも限定的となり、その結果、部門ごとに個別最適化された医療情報システムを分散的に管理せざるを得ない状況に直面する。

類型2（逆ピラミッド型）の医療機関では院内のIT担当者は、おのずと、患者診療にとって不可欠な、「診療系」ネットワークにおける院内横断的で重要な基幹系システム（例えば電子カルテシステム）の管理に注力せざるを得なくなるだろう。つまり、「診療系」ネットワークを「非診療系」ネットワークのセキュリティ管理水準とは切り離し、「3省2ガイドライン」への対応も含め確実にセキュリティ管理を行うことで、**「診療系」ネットワークは外部と遮断した閉鎖領域として安全管理を徹底しよう**という方針である。

図表4：国内医療機関のシステム管理類型の分類



**マネジメント層による意思決定に基づき、
IT管理部門・担当者が利用部門やIT事業者をコントロールする
全体最適志向型の管理モデル**

**IT管理部門・担当者の管理・監督が弱く、
現場の医療従事者のニーズ重視でシステム導入・管理が行われ、
マネジメント層は既に完了した結果を中心に報告を受けるという、
個別最適志向型の管理モデル**

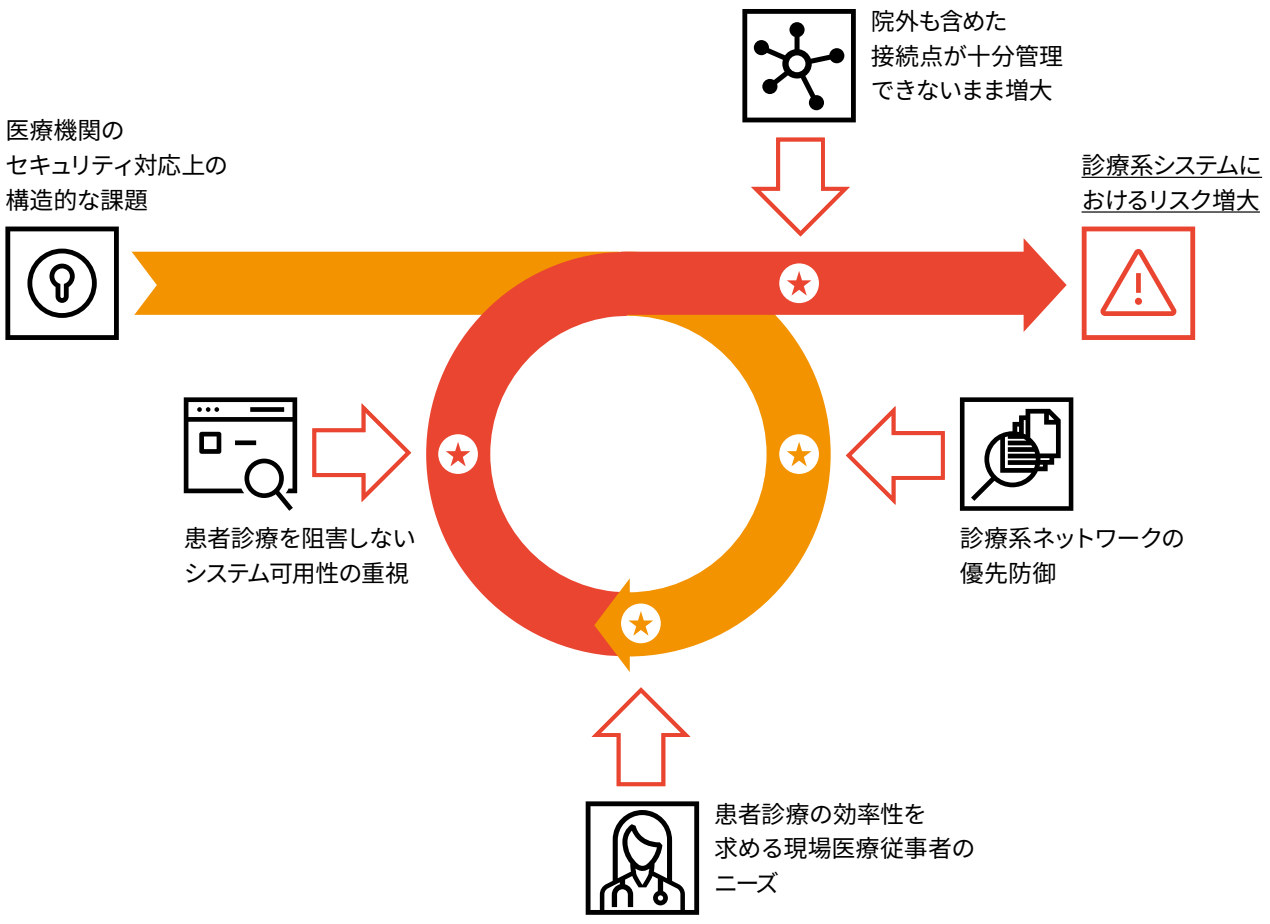
2.2 「診療系」ネットワークの「無菌性」という安全神話の危機

「診療系」ネットワークに設置される医療情報システムは医療機関では原則患者診療の継続性に係る重要な基幹系システムのみであり、これらのシステムに何らかの問題が発生することは医療機関としても許容できるものではない。医療機関では、「診療系」ネットワークに設置される基幹系システムから機微性の高い患者個人情報が漏えいしないようにするため、診療系／非診療系ネットワークの分離を実施している傾向が強い。そのため、医療機関の多くでは現在も「診療系」ネットワークは非「診療系」ネットワークから独立した、セキュアな閉鎖空間を目指す運用を行うべきという考え方が極めて根強い。またこの考え方は、病床規模が小さく、経済的・人的なセキュリティリソースが少ない医療機関においてより顕著と言える。

一方、医療機関には患者診療の実効性、つまり、患者診療に不可欠な医療情報システムを常に利用可能とする可用性も求められている。その観点で、「診療系」ネットワークに配置された医療情報システムでも障害や不具合等による利用不可を回避すべく、外部ネットワークからのリモートメンテナンス用の接続口を設定していることが通常である。さらには、遠隔読影・診断等の医師間連携（Doctor to Doctor）、オンライン診療等の医師／患者間のネットワーク接続など、外部とオンラインで接続するための仕組みが実は「診療系」ネットワークに知らずに結びついているという事例も見受けられる。また、地域医療連携ネットワークにおける医療機関間のデータ相互参照の仕組み、患者の在宅ケアに向けてIoTデバイス上のバイタルデータをクラウドを経由して確認する仕組みなど、患者診療の実効性を高めるべく、外部ネットワークとの接続を前提としたさまざまな技術的な工夫が導入・推進されはじめている。今や「診療系」ネットワークのみを閉鎖的にセキュアに堅持し続けるという選択肢は、医療機関の実態から乖離したものになりはじめており、こうした状況が今後より強まっていくことは想像に難くない。

「診療系」ネットワークは非「診療系」ネットワークと遮断しているため「無菌性」を確保できている、という安全神話は、今や危殆に瀕していると考えられる。

図表5：「診療系」ネットワークの「無菌性」を揺るがす危機の諸要素



3. 国内医療機関が優先すべきランサムウェアへの技術対策

3.1 前提

こうしたリソース不足に悩む国内の医療機関が直面するサイバー脅威の中で現在最大のリスクは、既述のとおり、診療系ネットワークに設置された医療情報システムを暗号化し利用不可とすることで、**患者診療の継続性に深刻な影響をもたらすランサムウェア**と言える。

こうした攻撃が増加した理由は、Ransomware as a Service（RaaS）という、特別なハッキング技術や攻撃準備を必要とせずとも、容易に悪意ある攻撃を大規模に実行可能とする環境が形成されたことによる。ランサムウェアのような無差別攻撃を実施するためには、手作業で逐一実施していては攻撃者も非効率であるため、スクリプトやアプリケーションを利用した自動攻撃ツールが開発された。それらのツールがダークウェブ等で取引され、攻撃に利用されている。

従来のサイバー攻撃は、明確な目的に基づき特定の組織を集中的に攻撃する、標的型攻撃という目的志向型のアプローチが一般的であった。しかし、今やRaaSという簡易ツールを用いて、不特定多数に対してランダムに攻撃を行い、その中で被害を受けた組織から金銭を奪取するアプローチが前面に出ている。そのため、「うちの病院を攻撃しても大して見返りがないのだから、攻撃されるはずがない」という根拠のない楽観は捨てなければならない。国内の医療機関であっても、攻撃者が用いるツールが対象とする脆弱性を抱えていれば、いつでもランサムウェアの被害者になり得るのである。

厚生労働省も2022年春を目途に、このようなランサムウェアリスクに対処すべく、厚生労働省安全管理ガイドラインの見直しの検討を進めている[13]。なお、今後のガイドラインでは、特に技術的な対策は各医療機関によるリスク評価の結果に基づいて行うべき対策例として整理される方針となっており、ランサムウェア対策を考える上で、医療機関は自院の医療情報ネットワーク・システム環境を踏まえ、適切なセキュリティ対策をリスクベースで選択することが求められることになる。ただし、上述のように、医療機関の多くでは、こうしたリスク評価を行い、その結果に基づく適切なランサムウェア対策を識別するためのリソースがそもそも不足している。**医療機関にとってランサムウェアへの対応を考える上で、一定の優先的な標準対策を提示することは未だ有益**であると思われる。

また、特定非営利活動法人デジタル・フォレンジック研究会では「医療機関向けランサムウェア対応検討ガイダンス[14]」を2021年11月に公表し、ランサムウェアという具体的な脅威を前にして医療機関が検討すべきポイントを整理している。ただ、バックアップデータの退避やセキュリティ専門家とのコミュニケーションパスの確保など、ランサムウェア被害からの復旧を目的とした運用上の対策に力点が大きく置かれており、ランサムウェアの被害を防止するための技術的な対策についての言及は少ないように見受けられる。

上記の外部動向も踏まえ、ランサムウェアという直近のサイバー脅威に対して被害発生を防止するために、セキュリティ投資費用が少なく、かつIT専門組織・IT専門担当者を有さない、**セキュリティリソースの限られた国内の医療機関が優先的に実施すべき、標準的な技術対策とは何か――。PwCあらたと日本マイクロソフトは共同でこの問いに対して検討を行い、その結果、以下の4つの技術対策を優先すべきものとして提言する。**

1. **脆弱性へのセキュリティパッチ適用**
2. **適切なアンチマルウェア対策**
3. **データ・ファイル単位でのアクセス制限**
4. **多要素認証の活用**

2021年10月に公開された「Microsoft Digital Defense Report[15]」でも、こうした取り組みを徹底し、既知の脆弱性が存在しない環境を維持することが、ランサムウェア、ひいては全てのサイバー攻撃への備えとして重要であることが述べられている。こうした取り組みを国内医療機関で実施するために、具体的にどのような対策に着手していくべきなのかについて、厚生労働省安全管理ガイドラインの要求事項と結びつけながら、次節で解説をおこなう。

3.2 4つの提言

① 脆弱性へのセキュリティパッチ適用

攻撃者が狙っているのは既知の脆弱性である。OSやアプリケーションのアップデートを行っていない環境を見つけ出して攻撃が行われている。特に、ランサムウェア攻撃は特定の情報を入手するといった明確な目的に基づくものでなく、身代金を要求するため無差別に攻撃が行われ、その結果、脆弱性が残存する医療情報システムで攻撃が成功している、というのが実情である。

そのため、無差別に行われるランサムウェア攻撃に対する重要な対策の1つとしては、その攻撃を無効にするため、**医療情報システム上の脆弱性に対するセキュリティパッチを適用し、常に最新状態に維持する**ことである。

13 厚生労働省「第8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資料について」（2021年12月）
https://www.mhlw.go.jp/stf/newpage_22803.html
14 特定非営利活動法人デジタル・フォレンジック協会「医療機関向けランサムウェア対応検討ガイダンス」https://digitalforensic.jp/2021/11/25/medhi-18-gl/
15 マイクロソフト「Microsoft Digital Defense Report」chapter2 The state of cybercrime（2021年10月）
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

厚生労働省安全管理ガイドラインでは、内部トラフィックにおける脅威の拡散などを防止するためのセキュリティ対策例として、OSのセキュリティパッチ適用の必要性が述べられている。この対策はランサムウェアへの技術対策を考える上で極めて重要であるが、その範囲がOSのみに限定されない点は注意すべきである。医療情報システムでは、OSやデータベース、アプリケーション等に脆弱性が発生してもセキュリティパッチを適用することで不具合の発生するリスクがあるため、こうした取り組みに対して積極的ではない可能性もある。

特にIT事業者によるリモートメンテナンスを目的としたネットワーク機器やツールは、一度、設置・導入し疎通確認が完了した後は、仮に機器・ツールに脆弱性が発生しても、パッチ適用が原因となってリモートメンテナンスの不具合が発生するリスクを回避するため、積極的なパッチ適用が行われないことも考えられる。その脆弱性を起点にしたサイバー攻撃は既に国内医療機関で発生している[16]。そのため、**医療機関に対しては、特に「診療系」ネットワーク内部の医療情報システム（リモートメンテナンス用のネットワーク機器やツールも含め）の脆弱性が放置されていないかについて定期的な確認を行い、適時のパッチ適用を行うことが推奨される。**

② 適切なアンチマルウェア対策

ランサムウェアを含むサイバー攻撃の多くはアンチマルウェア製品で対応できる。そのため、アンチマルウェア製品の導入は必須であり、厚生労働省安全管理ガイドラインでも求められているものである。医療機関の一部では、「診療系」ネットワークにはアンチマルウェア製品を導入しているものの、非「診療系」ネットワークは未導入であるなど、院内全体での導入状況にばらつきが発生しているケースも少なくない。**院内のシステム環境全体へアンチマルウェア製品を網羅的に導入するという基本的な対策**がまず重要である。

厚生労働省安全管理ガイドラインではアンチマルウェア製品のパターンファイルの更新の必要性が求められているが、これは一般的にはEndpoint Protection Platformという製品ソリューションを想定したものと言える。これは、製品メーカーが個別に対応した既知のマルウェアには有効であるが、未知のマルウェアによりセキュリティ対策が突破され、感染後の被害の拡大防止を行うという観点からは、他の医療機関、ひいては他産業への攻撃事例も含め、幅広い脅威情報（脅威インテリジェンス）に基づき、マルウェアの被害拡大を極小化するアプローチの検討が必要である。こうしたアプローチを可能にするアンチマルウェア製品は、一般的に**Endpoint Detection and Response（EDR）**と言われる。

EDRでは、既に他の医療機関や他組織で発生したランサムウェアを含めたサイバー被害をベースにした、リアルタイムなマルウェアへの対応水準を確保できる。そのため、特に「診療系」ネットワークでは、EDR型のアンチマルウェア製品の導入を検討することが推奨される。なお、EDR製品の選択においては、製品ベンダーが提供可能な情報量および情報更新の適時性に着眼した、十分な比較検討が必要である。

③ データ・ファイル単位でのアクセス制限

ランサムウェアの攻撃の多くは、なりすましによるアクセス権限の奪取によって行われている。ランサムウェアの攻撃を未遂に防いでいる組織の多くは、ファイルやデータへのアクセス権をサーバやフォルダ単位というマクロな水準でなく、単体のファイルやデータ単位というミクロな水準で設定していることが多い。例えば、技術的にフォルダにアクセス制限を行っていたとしても、フォルダ内部のファイルがコピーされた瞬間にそのアクセス権は失われる。ランサムウェア攻撃の被害に遭っている組織の多くが、アクセス制限をファイルやデータ単位の水準で十分に行っていないケースが極めて多い点には、注意が必要である。

厚生労働省安全管理ガイドラインでも、医療者が取り扱う患者個人情報を網羅的に棚卸しし、情報資産として管理することに加え、こうした情報は職務内容に応じてアクセスできる範囲を制限することが求められている。ただし、ランサムウェアへの対応におけるアクセス範囲の制限とは、多くの医療機関で既に実施されている、アプリケーションレイヤーにおける患者個人情報へのアクセス制限のみを指すものではない。これに加えて、アプリケーションを構成する医療情報システムの内部、つまりデータベースマネジメントシステム（DBMS）やOSレイヤーに配置されたシステムファイルやデータ、あるいはシステムを取り巻くネットワーク機器内部の設定ファイルなども含め、**医療情報システムの稼働に必要となる全てのデータやファイルへのアクセス権限（更新権限）の制限**という観点で考えなければならない。

ランサムウェアはファイルやデータを暗号化することで攻撃を成功させるが、暗号化にはファイルやデータの更新権限が不可欠である。更新権限が制限されていなければ、組織の中の誰の権限を奪ったとしてもデータやファイルを暗号化できることになる。逆に言えば、**医療情報システムを構成するデータやファイルの更新権限を確実に制限・管理することは、ランサムウェア被害の効果的な抑止策となる。**アプリケーションレイヤーにおける患者個人情報へのアクセス制限をいかに徹底しようとも、そのアプリケーションを搭載する医療情報システムの構成ファイル・データのアクセス制限が十分でなければ、ランサムウェアによる権限奪取には抗えないという点は、確実に理解されなければならない。

16 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）」（2021年11月26日）
https://www.hospital.or.jp/pdf/15_20211126_01.pdf?fbclid=IwAR2NmQxz8RVAOdkuHFPYsJBzs4AFtTZdIJNTBHVNbvoisbK3xcXCb1bAHu8

また、同様の観点より、医療情報システムのメンテナンスでは一般的に管理者IDに全権限が無制限に付与される傾向があるが、これもランサムウェアへの技術的対策という観点からは、メンテナンス作業に不可欠な範囲のみ操作可能な権限を付与することが推奨される。つまり、管理者IDというロールベースの権限付与ではなく、**管理者IDにより実施されるワークベースの権限付与**がランサムウェアを想定したサイバーセキュリティの観点からは検討されなければならない。ただし、国内の医療機関における医療情報システムの多くは、ロールベースの権限管理を前提としたシステム仕様になっている。作業終了後に該当する管理者（保守）IDは適時に削除すべきという厚生労働省安全管理ガイドラインの要件は、このような文脈のもとでこそ正しく理解されるべきである。これは管理者IDについてのみの話ではなく、ID・権限の付与方針とは、本質的にそのIDが求められるワークベースの権限に限定された観点から行われるべきということである。

④ 多要素認証の活用

前述のとおり、ランサムウェアの攻撃は、なりすましによるアクセス権限の奪取によって行われている。これを防ぐ方法として有効なものが、**多要素認証（Multi Factor Authentication：MFA）**である。

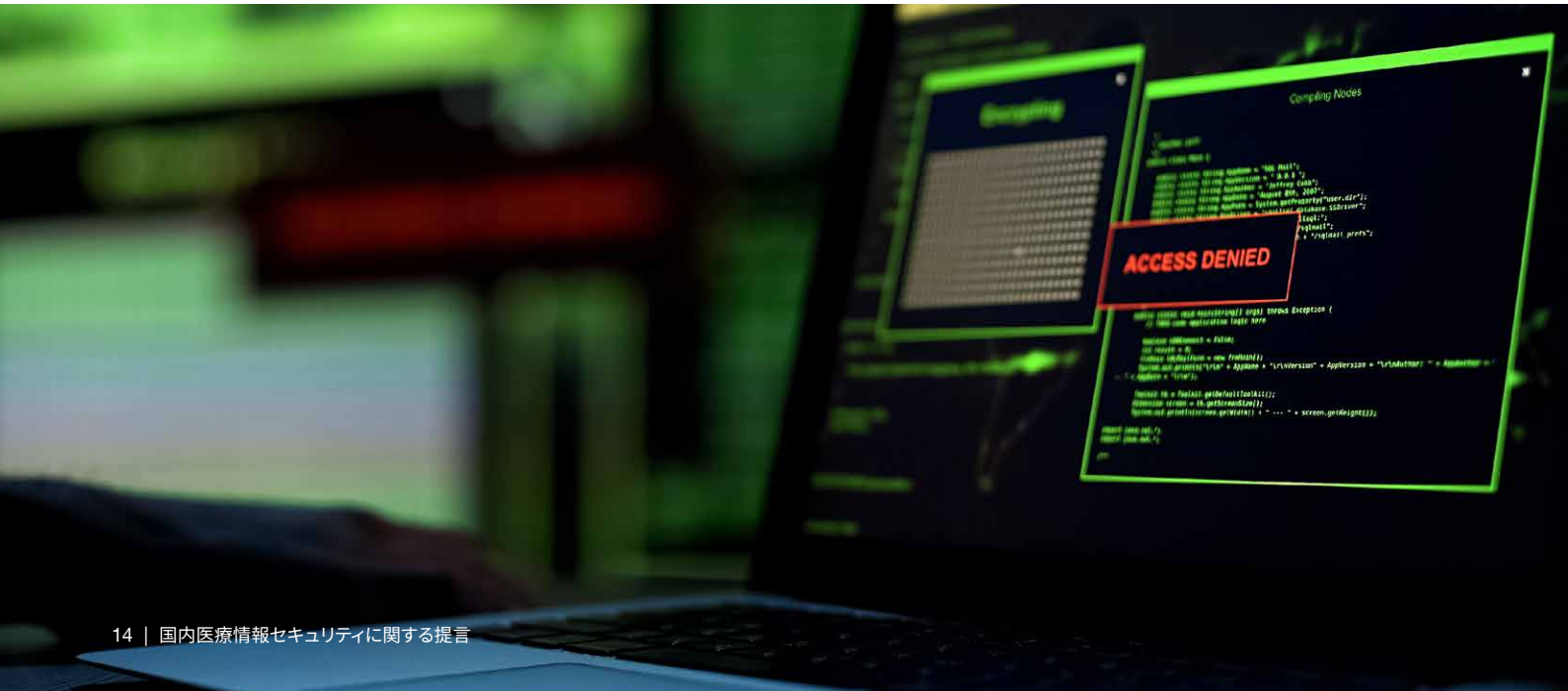
現行の厚生労働省安全管理ガイドラインでも、記憶、生体情報、物理媒体のうち2つの独立した要素を組み合わせた二要素認証（多要素認証）を、2027年度までに稼働が想定される医療情報システムへ実装することが求められている。この認証の仕組みは、一般的には認証の強化という観点のみで捉えられがちだが、もう一つの重要な効果がある。

例えば、IDとパスワードだけで認証を行っている場合、これらの情報が流出したとしても、本人が気付くことは難しい。これを防ぐために定期的にパスワードを変更する運用にしても、仮に厚生労働省安全管理ガイドラインが求めるような、2カ月に1回のパスワード変更では、最長で2カ月は悪用されるリスクがある。

一方、IDとパスワードが入力された後にスマートフォンへメッセージが送られる多要素認証を導入している場合、自らがID・パスワードを入力していないにもかかわらずスマートフォンに認証要求が届くという事実は、認証情報が流出していると本人に通知されることと同義である。この時点で悪意ある第三者によるログインをブロックし、パスワードを変更することで被害を最小限にできる。

つまり、多要素認証とはサイバーセキュリティの観点からは、認証の強化に加え、**ID・パスワードといった認証情報の流出有無にユーザー本人が気付くことのできる仕組みであり、ユーザー本人にサイバー攻撃に対する防御機能を持たせることができる**といえる。ランサムウェアにおいても、まずはアクセス権限、つまりID・パスワードといった認証情報を奪取することが起点になっている限り、被害が発生する前にユーザー自身が攻撃を予防できるようになると言える。さらに、ユーザーにとっては「自分が標的にされている」という、サイバー脅威のリアルな実感をもたらす教育的な効果も与えることが想定される。

ここまで、ランサムウェアを防止するための優先的な技術対策について解説してきた。これらの対策の多くは既に現行の厚生労働省安全管理ガイドラインでも言及されているが、本提言ではランサムウェアへの技術的な対策という観点を軸に、より具体的な対策や考え方にまで踏み込んだ。セキュリティリソースの不足する医療機関においても、現行のガイドラインに基づいて実施している諸対策を、上述の技術的な観点に基づき、より重点的・優先的に行うことで、ランサムウェアの被害を受けるリスクを低下させることが可能になると考えられる。



おわりに

国内で医療情報セキュリティのバイブルとされてきた「3省2ガイドライン」は、あくまで紙媒体で管理されていた医療情報を電子的に管理するために必要な要件を定義したものであり、日々巧妙化・高度化する当今のサイバー脅威への対応を企図したものではない。国内の医療機関においてはガイドラインへの対応に加え、サイバー脅威への対応を同時に考えなければならず、今やランサムウェアという、医療情報システムに不可欠な可用性を侵害するサイバー攻撃の猛威の前に、待ったなしの対応が求められている。

一方、国内の医療機関の大多数は、こうしたサイバー脅威への対応に注力できるだけの経済的・人的なセキュリティリソースが不足しており、その状況は病床規模が小さくなるにつれて顕著である。そのため、医療機関の大多数では、「診療系」ネットワークという基幹系システムの領域のみは安全管理すべく、限られたリソースを注力することになる。医療情報システムに求められる役割が技術変化の動向にしたがって変容し、さまざまな技術的な仕組みが患者診療の向上のために導入される中では、こうした後退戦には限界がある。それでも、患者の命・健康を扱う医療機関はそれぞれの地域医療という社会的インフラを支えるべく、「診療系」ネットワークの安全のみは確実に守らなければならない。現在の国内の医療機関の大多数は、こうした一筋縄では解決できない、非常に困難な状況に直面していると言える。

本稿では、そうした困難な状況にある国内の医療機関が、ランサムウェアという**「致死性の悪性ウイルス」**の蔓延・猛威に対して、自身の**「健康」**を守るというセルフヘルスマネジメント上、優先的に実施することが推奨される基本的な技術対策の考え方を解説した。ただし、これらの取り組みはあくまで**「応急処置」**に近いものである。今後、「診療系」ネットワークの**「無菌性」**、つまり安全神話が外部ネットワークとの接続を前提とする医療技術の進化・発展により崩壊していくことは避けられないと考えられる。また、現行のランサムウェアもさらに獰猛となり、上述してきた基本的対策の防御層を突破するものが発生する可能性は否定できない。そのような状況のもとで、経済的・人的資源が不足することを理由に、セキュリティについて現状の維持にとどまるという選択は、地域医療を支える社会インフラである医療機関として真に正しい選択と言えるのだろうか。

まずは、医療機関自身の医療情報セキュリティに関する「健康」への懸念を正直に外部のセキュリティ専門組織＝**「医療機関」**へ相談し、その上であるべき対応策を**「医療機関」**とともに考えることが、自分たち、ひいては患者個々に安全をもたらす一歩となるであろう。この一歩は、経済的・人的なセキュリティ資源の不足に直面する医療機関にとっては困難な決断かもしれないが、地域医療の継続性を念頭に、その勇気ある決断が行われることを期待したい。

お問い合わせ先

PwC Japanグループ
www.pwc.com/jp/ja/contact.html

日本マイクロソフト株式会社
www.microsoft.com/ja-jp/industry/health/microsoft-cloud-for-healthcare

---

PwCあらた有限責任監査法人
システムプロセスアシュアランス

宮村 和谷
パートナー

江原 悠介
シニアマネージャー

日本マイクロソフト株式会社

河野 省二
技術統括室 チーフセキュリティオフィサー

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約9,400人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界156カ国に及ぶグローバルネットワークに285,000人以上のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細は www.pwc.com をご覧ください。

電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/knowledge/thoughtleadership.html
発刊年月：2022年3月　管理番号：I202107-10

©2022 PwC. All rights reserved.
PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.
This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.