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

No.453

2021年4月27日

日本医師会総合政策研究機構
坂口一樹、堤　信之

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

坂口一樹（主任研究員）、堤　信之（主任研究員）

キーワード

◇ 医療情報システム　◇ サイバー攻撃　◇ サイバーセキュリティ
◇ 情報セキュリティ　◇ リスクマネジメント

要　旨

◆ 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、全国調査を実施した（病院 約 5,000 施設と診療所 約 5,000 施設を対象とし調査、回収数 2,989、回収率 30.4%）。主な結果は、以下の通り。

◆ 医療現場の組織体制は問題含みである。院内システムのネットワーク構成図を保有し、計画的に見直しをしているのは 5.7%に過ぎず、約半数は構成図を持っていなかった。専任の担当部門があるのは２割強で、３分の２弱は兼務の担当者あるいは院長自ら管理という体制である。計画的に対策費用を準備しているのは１割強であり、半数近くは費用を準備していなかった。

◆ 行政の取り組みの認知度・活用度にも課題がある。情報システムの安全管理に関する厚労省ガイドラインを認知・活用している割合は 27.9%、サイバー攻撃を受けた際の届出先の認知割合は 29.2%、不正アクセス等に関する相談窓口の認知割合は 23.1%と、いずれも３割に満たなかった。

◆ サイバーセキュリティに関するリスクマネジメント体制にも、次の通り課題がある。【事前対策の状況】患者・受診者情報が保管されている情報端末の管理ルールや USB メモリ等の外部媒体の管理ルールについて、３割前後～４割強が「ルールなし」であった。４分の３超の施設は、サイバーセキュリティに関する従業員教育を実施していなかった。【発生時対策の状況】３分の２弱から８割強が、インシデント発生時の明文化された手順やルールがないとの回答であった。【事後対策の状況】サイバーセキュリティ保険への加入割合は１割に満たなかった。また、過去３年間にインシデントを経験した回答者のうち、４割超は再発防止に向けた対応にまで至っていなかった。

◆ 以上の組織体制、行政の取り組みの認知度、リスクマネジメント体制については、総じて病床規模の大きさに応じて状況が良くなる傾向にあった。別の言い方をすれば、診療所や中小規模の病院ほど、情報セキュリティやサイバーセキュリティに関わる対策全般に問題を抱えているということである。

◆ 直近３年間における実際のインシデント・アクシデントの経験に関しては、最も危惧される「サイバー攻撃により患者に直接の危害があった」との事象は確認されなかった。一方で、ウイルス感染や外部からの不正アクセス等のサイバーセキュリティに関わるインシデントの発生が確認できた。

◆ 現場からの要望では、「サイバーセキュリティ対策の費用面での公的支援」と「自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み」の２つが、ともに５割を超える施設が挙げた２大要望であった。

◆ 以上の結果を踏まえて考察を加え、組織体制の充実、リスクマネジメント体制の強化、現場の要望への対応に向けた具体的な提言を行った。

目　次

１．背景と問題意識

現在、インターネットをはじめとする情報通信技術（ICT）は、私たちの生活にとって欠かせない存在となっている。電気、ガス、水道から公共交通、政府機関に至る公共インフラの多くでもICTが活用されており、情報機器・ネットワークは、今や経済・社会のあらゆる局面に浸透している。政府は、サイバー空間と現実空間が融合した「Society 5.0」を提唱しており、情報機器・ネットワークと経済・社会の関係は、今後ますます強まると考えられる。

一方で、今日のサイバースペースにおいては、日々進歩するデジタルテクノロジーを悪用して、コンピュータウイルスの送信や情報システムへの不正侵入等といった脅威が世界規模で生じている。その結果、個人や企業等に対する情報の悪用や改ざん、詐欺行為、プライバシーの侵害の他、企業等に対する標的型攻撃による身代金要求といった悪質な犯罪としてリスクが顕在化し、インターネットを利用する私たちに襲いかかっている[1]。

そのような流れに、新型コロナウイルス感染拡大による急激な働き方の変化が拍車をかけている。テレワークの増加や、業務基盤のクラウドへのシフトの進展により、セキュリティの問題はさらに複雑化している。アンチウイルスやネットワークでの不正アクセス防止、暗号化など多岐にわたるセキュリティ対策の基本となる端末管理において、急速なテレワークの普及によって端末の数が一気に増加し、しかもインターネットにむき出しでつながる状態では、従来の対策では十分と言えない。しかも、持ち出された端末がマルウェアに感染すれば、組織内ネットワークに再接続したときに、感染が組織全体に広がる危険性も大きい。

医療界も例外ではなく、さまざまな攻撃や不正な活動に晒されている[2]。インターネットに接続できる医療機器は業務効率を向上させ、特にIoT（モノのインターネット）の技術は、患者のケアと医療施設の機能向上に貢献し、結果として患者や医療従事者の生活改善につながる。しかし医療機関と患者が病院内のネットワークに持ち込むデバイスの多様化、IoT技術の成長は、サイバー攻撃を受ける可能性も拡大させる。発生する不正行為として主に考えられるのは、個人データ（医療記録や健康に関わる各種データ）そのものの価値に着目し、ネットワーク等を通じその窃取を目的とする犯罪、医療機関内のネットワーク等に支障を生じさせて医療行為を妨害する犯罪、さらには、医療用IoTデバイスに対する攻撃により患者データを直接改ざんする犯罪などであるが、いずれも深刻度の高い犯罪である。

---

[1] この段落で説明しているリスクを、本稿では「サイバーリスク」として取り上げる。
[2] 深津（2020）。

個人データ窃取犯罪では、医療機関から得たPII[3]やPHI[4]を「闇市場」で売買することで、犯罪者は利益を得る。個人情報の窃取、金銭目的の詐欺、カスタマイズしたフィッシング・メールの作成と、とりわけ医療に関わる個人データは幅広い不正行為に活用できることから、高い需要があると言われている[5]。

医療行為妨害犯罪のうちで、医療機関を脅迫し、妨害行為をやめる代わりに金銭をせしめるものが「ランサムウェア[6]攻撃」と呼ばれている。ランサムウェアによって電子カルテのデータが読めなくなれば、たちまちに患者の生命に関わる事態となる。医療機関を狙うランサムウェア攻撃は今に始まったことではなく、海外のみならず国内でも事件発生が相次ぎ報告されている（図表 1-1）。

図表 1-1. 医療機関をターゲットとした最近のサイバー攻撃事件

主な事件名	事件概要（筆者らまとめ）
ハリウッド・プレスビテリアン医療センター事件[7]	2016 年 2 月、同病院はランサムウェアによる攻撃で、患者情報等のファイルを暗号化され、人質に取られ、約 10 日間に亘って業務に深刻な影響が出た。ウイルス解除のため、1 万 7000 ドル相当の身代金が支払われたとされる。
ハンコックヘルス病院事件[8]	2018 年 1 月、同病院はランサムウェアによる攻撃で、電子カルテシステムが使えなくなったが、4 ビットコイン（当時約 700 万円相当）の身代金を支払うことにより 4 日間で復旧したとされる。
奈良県宇陀市立病院事件[9]	2018 年 10 月、奈良県の宇陀市立病院において導入したばかりの電子カルテシステムがランサムウェアに感染し、同システムの利用ができない状況になり、復旧作業を経てシステムの利用を再開したが、一部のデータファイルが暗号化されたことで、患者カルテの参照ができない状況になった。
福島県立医科大学附属病院事件[10]	2017 年 8 月以降、院内システムがウイルスに感染して被害が出ていたことが、2020 年 12 月に公表された。院内ネットワークがランサムウェアに感染し、放射線撮影装置の不具合で再撮影を余儀なくされた事案が 2 件、患者には影響ないが医療機器の再起動などの不具合が発生した事案が 9 件発生した。

[3] Personally Identifiable Information（個人を特定できる情報）の略称。
[4] Personally Health Information（個人健康情報）の略称。
[5]「医療データは闇市場でクレカ情報より約 20 倍の値がつく」（ITmedia News、2019 年 3 月 14 日）、「個人の医療データは売買されており数千億円規模のお金が動いている」（Gigazine 、2017 年 1 月 12 日）など。
[6] ランサムウェアとは、パソコンやサーバに保存されたデータを暗号化するなどして利用不能にして、元に戻したければ金銭（身代金）を支払うよう求める目的で使用されるウイルス（マルウェア）をいう。
[7]「新型コロナ禍の医療機関にランサムウェア、極悪非道のサイバー攻撃者を許すな」（日経クロステック、2020 年 5 月 20 日）
[8]「ランサムウェア感染から 4 日で復旧　素早い判断で被害を最小限に」（日経クロステック、2018 年 5 月 10 日）
[9]「ランサムウェアで電子カルテが利用不能に、復旧が長引いた理由とは」（日経クロステック、2020 年 5 月 8 日）
[10]「福島の病院、サイバー被害　17 年発生　県立医大付属、公表せず　身代金ウイルス、医療機器停止　病院に攻撃海外で相次ぐ　手術延期のケースも」（日本経済新聞、2020 年 12 月 3 日朝刊）

しかも 2020 年 4 月初めには、インターポール（国際刑事警察機構）から、新型コロナウイルスの対応に協力している医療機関等がランサムウェアの標的となっているとして、警告文書が公開され、併せてインターポールに加盟する 194 の国・地域の警察に通知された。インターポールによると、攻撃者はランサムウェアを使って病院の電子カルテ等を人質に身代金を要求するという[11]。さらに海外では、病院がランサムウェア（身代金要求型マルウェア）攻撃を受け、その影響で患者が死亡した可能性がある事例まで発生している[12]。

また、医療用 IoT デバイスに対する攻撃犯罪では、攻撃が原因でこれらの機器が正常に機能しなくなれば、患者の命がたちまちに危険にさらされる恐れがあるという点で、一般消費者向けデバイスの脆弱性がもたらす脅威よりもはるかに深刻度が高い。

上記の状況に鑑み、サイバーセキュリティ対策として、2014 年にわが国では「サイバーセキュリティ基本法」が制定された[13]。また新たな体制として内閣に「サイバーセキュリティ戦略本部」が設置され、その事務局である「内閣サイバーセキュリティセンター」が組織化された。さらに、2017 年には「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」が定められるなど、「医療」他の重要インフラサービスの安全かつ持続的提供のため、サイバー攻撃に備える行政の取り組みが稼働している[14]。

他方、日本の医療機関のサイバーセキュリティに関する実態はあまりよく分かっておらず、関連する既往調査も限られている。筆者らが 2020 年に実施したパイロット調査[15]によれば、医療界における ICT 部門や専門家の不在、人材の不足、ベンダー任せの体制、トラブル発生時の対応体制の不備やセキュリティ対策を含めた事前対策の欠如という実態が強く示唆される結果であった。医事会計システム（レセコン等）、診療支援システム（電子カルテ、オーダリング等）に加え、地域医療構想に基づく医療機関（または医療関係組織）相互の情報共有や遠隔医療の進展、オンライン資格確認の開始、さらには PHR（Personal Health Record）の新たな構築という社会的要請[16]等を背景に、医療界における ICT 化

11「新型コロナ禍の医療機関にランサムウェア、極悪非道のサイバー攻撃者を許すな」（日経クロステック、2020 年 5 月 20 日）

12 デュッセルドルフ大学病院事件の概要は以下の通り。AP 通信がドイツ当局の話として 2020 年 9 月 17 日に報道したところによると、78 歳の女性患者が同病院へ搬送されていた時、デュッセルドルフ大学病院は他の組織を狙ったとみられるランサムウェア攻撃を受けて、同病院の IT システムがダウンした。この攻撃が原因で、女性患者はやむを得ず近隣都市のブッパータールに搬送され、後に死亡した。救急治療が遅れたために死亡した可能性があると説明されている。「史上初の身代金ウイルス攻撃による死者、ドイツの病院で発生」（Forbes Japan、2020 年 9 月 19 日）

13 サイバーセキュリティ基本法第二条によれば、「サイバーセキュリティ」とは、電磁的方式に係る情報の安全管理や、情報システム及び情報通信ネットワークの安全性、信頼性確保のための必要措置が講じられ維持管理されることと定義されている（筆者らによる要約）。法について詳しくは、三角（2020）。

14 神足（2020）。

15 坂口・堤（2020）。

16 山本（2017）。

は、まったなしの環境に置かれているにもかかわらず、サイバーセキュリティ対策の遅れと情報システムの脆弱性が懸念される。医療機関におけるサイバーインシデントの発生状況、情報システムの接続環境や管理体制等のサイバーセキュリティ対策のみならず、広く情報セキュリティ[17]対策等について、その実態を早期に把握し、潜在的なリスクを把握した上で、医療機関や行政で適切な対応策を講じる必要がある。

以上のような背景と問題意識を基に今般、日本医師会は、医療機器センターと合同で医療情報システムの管理体制に関わる全国調査を実施した。本稿では、その調査結果の概要と今後に向けての提言をまとめた。

[17] 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」を包含する概念と位置づけられている。

２．調査概要と本稿の位置付け

２．１　調査の目的

全国の医療機関（病院・診療所）における情報システムの管理体制に関わる実態把握を目的とした。

調査設計にあたっては、特に（１）情報セキュリティ・サイバーセキュリティに関する組織体制、（２）行政の取り組みの認知度、（３）インシデントへの対応と実際の経験、の３点に焦点を当てた。

２．２　対象と方法

調査対象は、全国の医療機関名簿から無作為抽出した病院 5,000 施設、診療所 5,000 施設の合計 10,000 施設である[18]。

対象施設には、調査画面へのアクセス方法を記載した案内状を郵送し、ウェブ調査画面を通じて回答してもらった。なお、本調査は、公益社団法人日本医師会と公益財団法人医療機器センターの合同調査である。上記の案内状とあわせて、両団体の会長名による調査協力の依頼文書を同送した。

上述の通り、本調査の実施主体は日本医師会と医療機器センターである。調査設計にあたっては、前者のシンクタンクである日本医師会総合政策研究機構と後者のシンクタンクである医療機器産業研究所とが協働した[19]。

実施にあたっては、医療機器産業研究所を調査事務局とし、日本医療研究開発機構の委託研究費を活用した。実施期間は 2021 年 1 月 7 日～2 月 3 日であった。一部、紙媒体の返送による回答も受け付けることとした。

２．３　本稿の位置付け

調査項目には、実施時期および医療機器センターとの合同調査とした関係から、（１）オンライン資格確認システムの導入予定と（２）医療機器のサイバーセキュリティに関わる設問も含まれる。これら２つについては別稿で触れることとし、本稿では、日本の病院・診療所におけるサイバーセキュリティをはじめ、医療情報システムの管理体制に関わる調査結果の分析に焦点を絞った。

---

[18] 医療経済研究機構の「全国保険医療機関（病院・診療所）一覧（平成 30 年度版）」を活用した。
[19] 後者の正式名称は「公益財団法人医療機器センター附属医療機器産業研究所」である。
https://jaame.or.jp/mdsi/mdsi.html

２．４　回収状況および回答者属性

回収した有効回答数は、n=2,989（回収率 30.4%、未達 175 件）であった。図表 2-4-1～図表 2-4-3 に、主な回答者属性を示した。

図表 2-4-1. 回答者属性（全体、n=2,989）

		n	%
開設主体	個人	616	20.6%
	医療法人	1661	55.6%
	国公立・公的	443	14.8%
	その他の法人	269	9.0%
病床規模	無床診療所	1289	43.1%
	有床診療所	111	3.7%
	病院　20～99床	468	15.7%
	病院　100～199床	511	17.1%
	病院　200～499床	463	15.5%
	病院　500床以上	147	4.9%

		n	%
院長の年齢	３０歳代以下	25	0.8%
	４０歳代	285	9.5%
	５０歳代	790	26.4%
	６０歳代	1355	45.3%
	７０歳代	457	15.3%
	８０歳代以上	77	2.6%
回答者職位	理事長	297	9.9%
	院長	709	23.7%
	システム担当	986	33.0%
	事務長	515	17.2%
	その他	482	16.1%

図表 2-4-2. 回答者の主な診療科（診療所のみ。n=1,400）

	単一回答	n	%
	全体	1,400	
1	内科	638	45.6
2	外科	35	2.5
3	整形外科	119	8.5
4	眼科	113	8.1
5	耳鼻咽喉科	91	6.5
6	小児科	93	6.6
7	皮膚科	60	4.3
8	泌尿器科	29	2.1
9	精神科	64	4.6
10	産科・産婦人科	56	4.0
11	婦人科	19	1.4
12	脳神経外科	19	1.4
13	その他	64	4.6

図表 2-4-3. 回答者の病院種別（病院のみ。n=1,589）

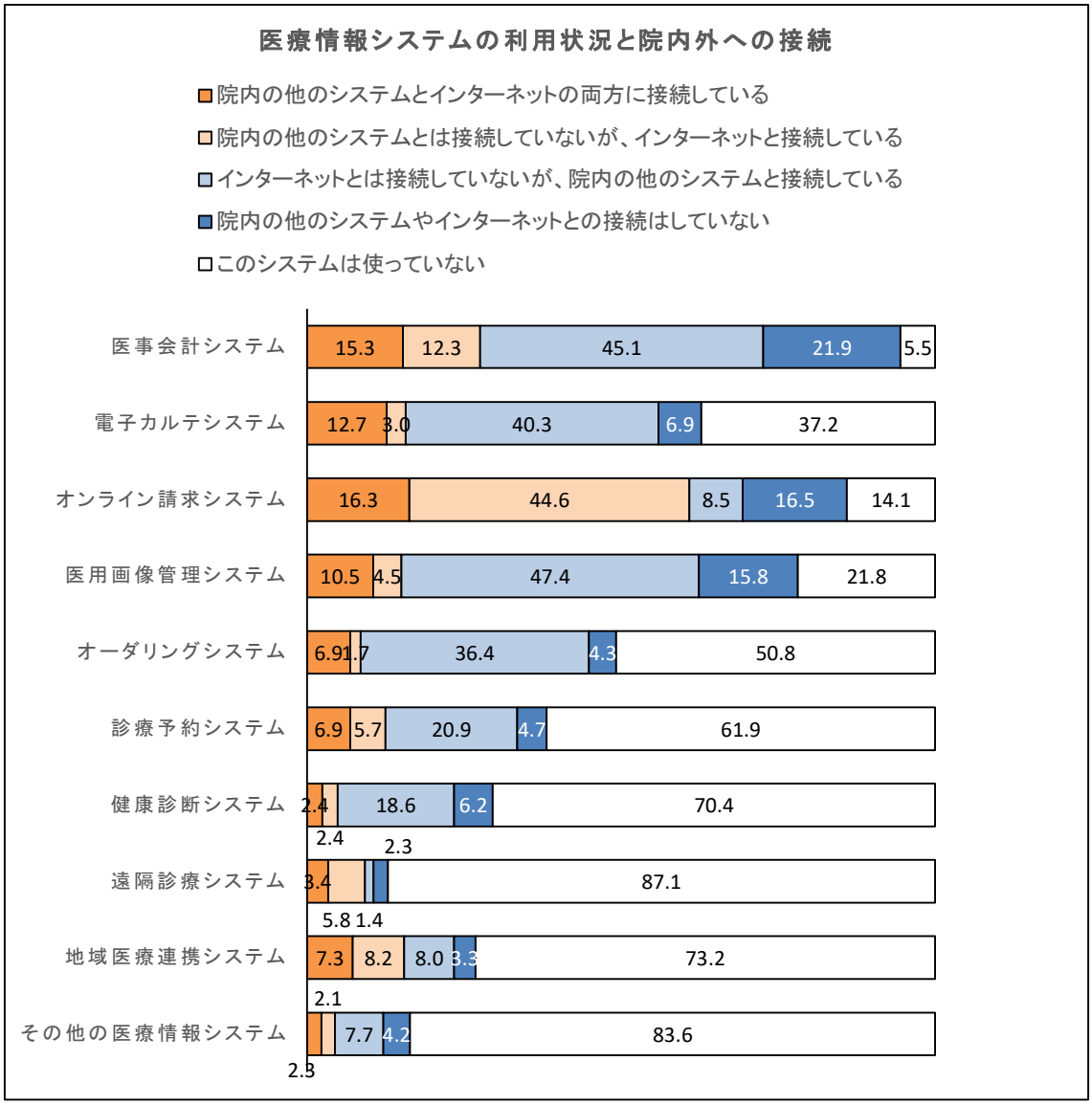
	単一回答	n	%
	全体	1,589	
1	一般病院	1,383	87.0
2	精神科病院	206	13.0

３．分析結果

３．１　医療情報システムの利用状況と院内外への接続

図表 3-1-1 は、医療情報システムの利用状況と院内外への接続の状況を示している。濃いオレンジ色で示したのが「院内の他のシステムとインターネットの両方に接続している」割合、淡いオレンジ色で示したのが「院内の他のシステムには接続していないが、インターネットに接続している」割合である[20]。

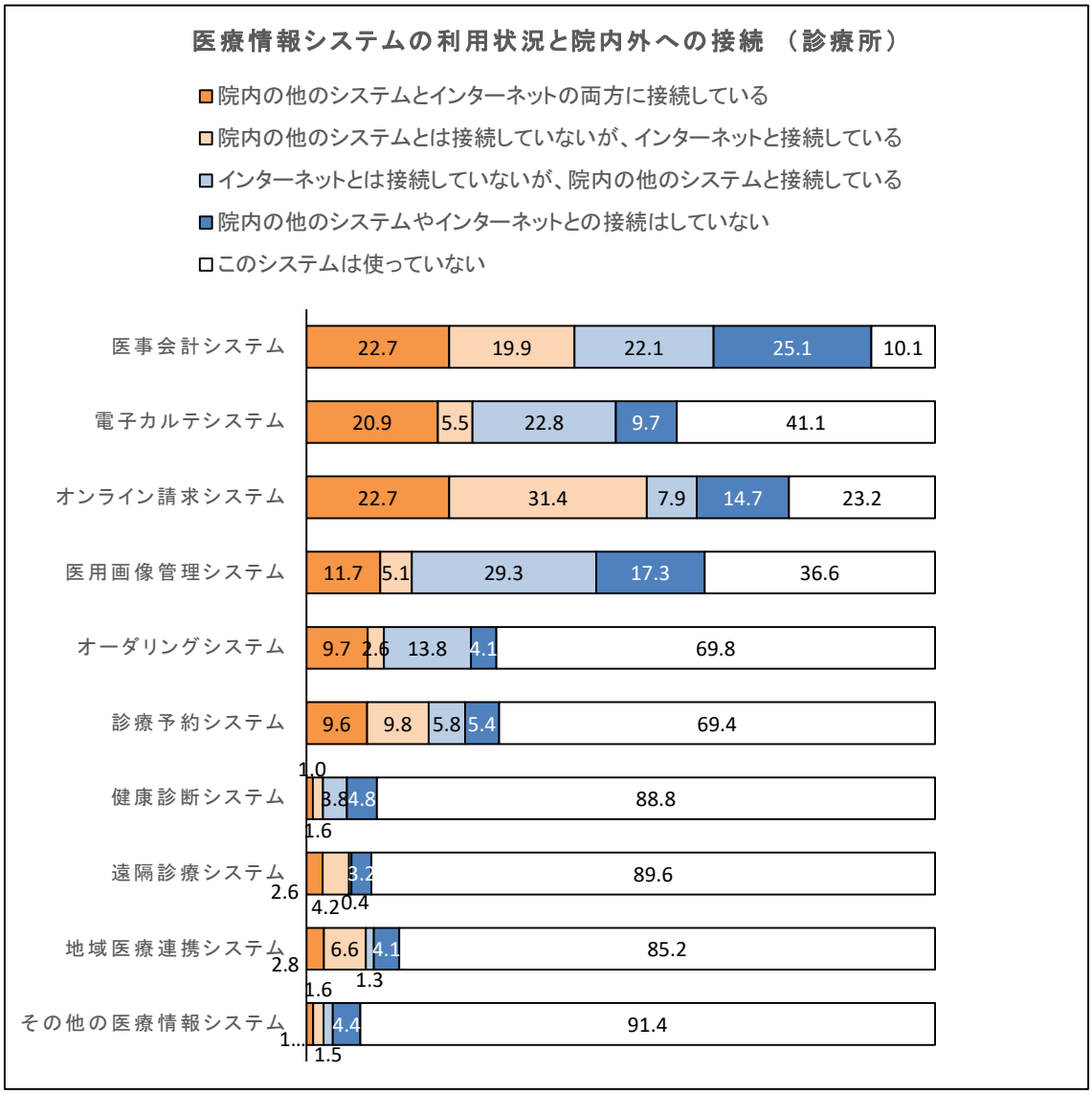
図表 3-1-1.　医療情報システムの利用状況と院内外への接続（全体、n=2,989、百分比）



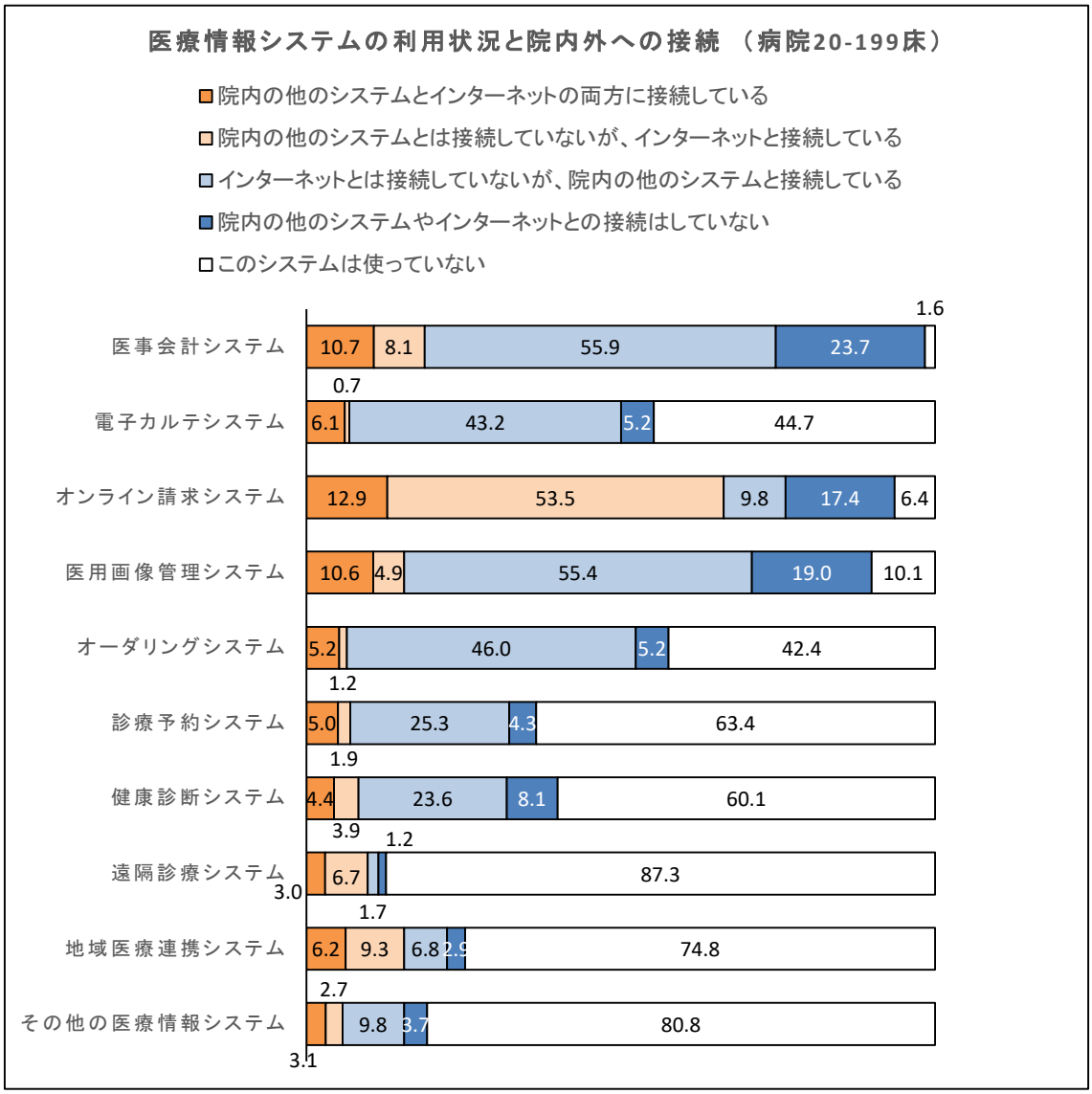
[20] 調査では「インターネット」と「院内の他のシステム」との接続状況をシンプルに尋ねたのみで、それらのシステムのセキュリティレベルについては確認していない。現在、ネット接続下でも相応のセキュリティの確保をうたっているシステムが販売されているが、その性能や使用については確認していない。

図表 3-1-2～図表 3-1-5 は、医療情報システムの利用状況と院内外への接続の状況について、診療所の状況、20-199 床の病院の状況、200-499 床の病院の状況、500 床以上の病院の状況という順に、病床規模別に示している。濃いオレンジ色で示したのが「院内の他のシステムとインターネットの両方に接続している」割合、淡いオレンジ色で示したのが「院内の他のシステムには接続していないが、インターネットに接続している」割合である。

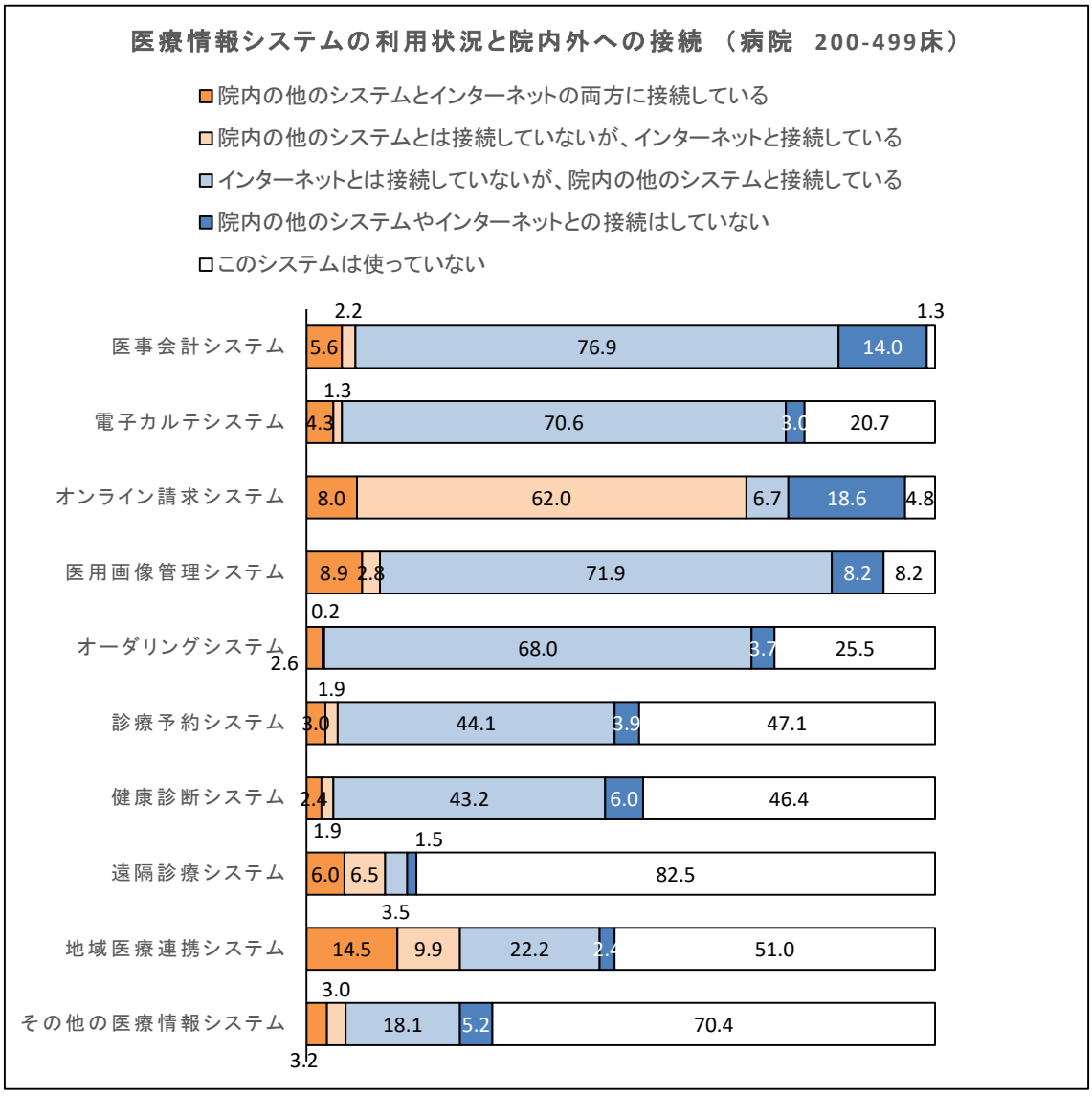
図表 3-1-2. 医療情報システムの利用状況と院内外への接続（診療所、n=1,400、百分比）



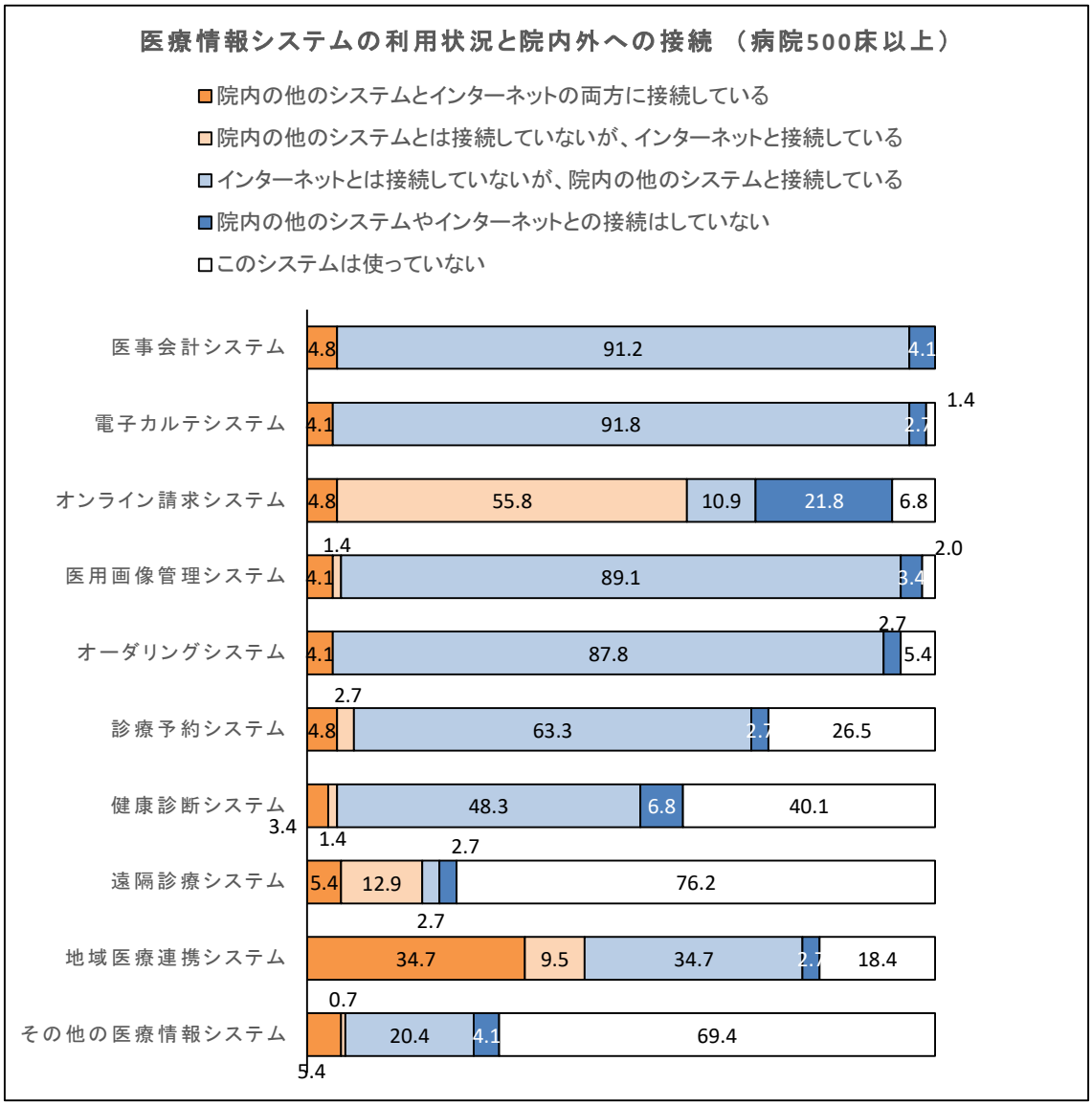
図表 3-1-3.　医療情報システムの利用状況と院内外への接続（病院 20-199 床、n=979、百分比）



図表 3-1-4. 医療情報システムの利用状況と院内外への接続（病院 200-499 床、n=463、百分比）



図表 3-1-5. 医療情報システムの利用状況と院内外への接続（病院 500 床以上、n=147、百分比）



３．２　サイバーセキュリティ対策の組織体制

（１）ネットワーク構成図の保有状況

図表 3-2-1 は、ネットワーク構成図の保有状況について、全体および病床規模別の状況を示している。

院内システムのネットワーク構成図を保有し計画的に見直しているのは 5.7%で、49.2%は構成図を持っていない。

病床規模別にみると、規模が大きくなるほど構成図を保有し、見直しをしている割合が高くなっている。

図表 3-2-1. ネットワーク構成図の保有状況

		全体	資料を持っており、計画的に見直しや更新を行っている	資料を持っており、ネットワークの追加・修正のあるタイミングで見直しや更新を行っている	資料を持っているが、見直しや更新は行っていない	資料は持っていない
全体		2,989	169 5.7	938 31.4	411 13.8	1471 49.2
病床規模	診療所	1,400	43 3.1	229 16.4	141 10.1	987 70.5
	病院　20～199床	979	59 6.0	344 35.1	177 18.1	399 40.8
	病院　200～499床	463	42 9.1	269 58.1	77 16.6	75 16.2
	病院　500床以上	147	25 17.0	96 65.3	16 10.9	10 6.8

（２）情報システムの管理体制

図表 3-2-2 は、情報システムの管理体制について、全体および病床規模別の状況を示している。

専任の担当部門があるのは 20.6%であり、兼務の担当者（33.2%）または院長自ら管理（31.6%）している割合が 64.8%と３分の２近くに及ぶ。

病床規模別にみると、規模が大きくなるほど専任の担当部門がある割合が高くなっていた。一方で、診療所では 64.4%が「院長自らが管理」という体制であり、規模によって大きく管理体制が異なることがわかる。

図表 3-2-2. 情報システムの管理体制

		全体	専任の担当部門がある	専任の担当部門はないが、委員会等を設置している	専任の担当部門や委員会等はないが、専任の担当者がいる	専任の担当部門、委員会等や専任の担当者はいないが、兼務の担当者がいる	上記のような管理体制はなく、院長が自ら管理している
全体		2,989	617 20.6	244 8.2	191 6.4	993 33.2	944 31.6
病床規模	診療所	1,400	42 3.0	19 1.4	73 5.2	365 26.1	901 64.4
	病院　20～199床	979	201 20.5	161 16.4	82 8.4	495 50.6	40 4.1
	病院　200～499床	463	245 52.9	55 11.9	35 7.6	125 27.0	3 0.6
	病院　500床以上	147	129 87.8	9 6.1	1 0.7	8 5.4	0 0.0

（３）対策費用の準備状況

図表 3-2-3 は、サイバーセキュリティ対策費用の準備状況について、全体および病床規模別の状況を示している。

費用を計画的に使えるように用意しているのは 10.4%であり、計画的ではないが必要に応じて使えるように用意しているのは 41.5%であった。一方で、費用を用意していない割合は 48.1%と半数近くに及んでいた。

病床規模別にみると、規模が大きくなるほど費用を計画的に使えるように用意している割合が高くなっていた。ただし、500 床以上の病院でも、その割合は 27.9%と３割に満たない。他方で、費用を用意していない割合については、規模が大きくなるほど低くなっていたが、500 床以上の病院でも、３割近く（28.6%）の病院において、対策費用の準備がなかった。

図表 3-2-3. 対策費用の準備状況

		全体	計画的に使えるように用意している	計画的ではないが、必要に応じて使えるように用意している	用意していない
全体		2,989	312 10.4	1240 41.5	1437 48.1
病床規模	診療所	1,400	105 7.5	494 35.3	801 57.2
	病院　20～199床	979	96 9.8	467 47.7	416 42.5
	病院　200～499床	463	70 15.1	215 46.4	178 38.4
	病院　500床以上	147	41 27.9	64 43.5	42 28.6

（４）システムのメンテナンス体制

図表 3-2-4 は、システムのメンテナンス体制について、全体および病床規模別の状況を示している。

内部スタッフと外部の業者のサービスにより実施しているとの回答割合が最も多く 47.0%、次いで外部の業者のサービスを利用して実施（28.2%）、内部スタッフにより実施（14.8%）であった。メンテナンスを実施していないとの回答も 7.9%あった。

病床規模別にみると、内部スタッフと外部の業者のサービスにより実施しているとの回答割合が、規模が大きくなるほど高くなっていた。メンテナンスを実施していないとの回答割合は、規模が小さいほど高く、診療所では 12.6%であった。

図表 3-2-4. システムのメンテナンス体制

		全体	内部スタッフ(院長含む)により実施している	外部の業者のサービスを利用して実施している	内部スタッフ(院長含む)および外部の業者のサービスにより実施している	実施していない	わからない
全体		2,989	441 14.8	844 28.2	1405 47.0	237 7.9	62 2.1
病床規模	診療所	1,400	210 15.0	536 38.3	427 30.5	176 12.6	51 3.6
	病院　20～199床	979	159 16.2	214 21.9	544 55.6	54 5.5	8 0.8
	病院　200～499床	463	62 13.4	79 17.1	312 67.4	7 1.5	3 0.6
	病院　500床以上	147	10 6.8	15 10.2	122 83.0	0 0.0	0 0.0

３．３　行政の取り組みの認知度・活用度

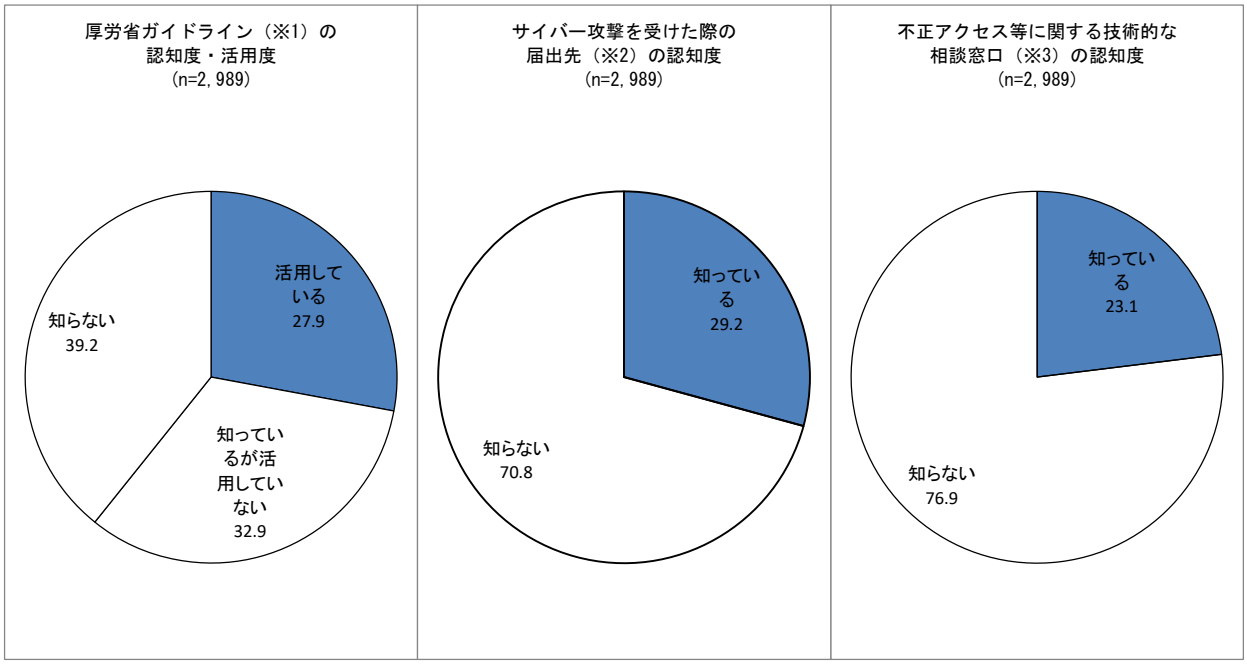
（１）認知度・活用度の全体像

図表 3-3-1 は、政府の取り組みの認知度・活用度の全体像を示している。

情報システムの安全管理に関する厚労省ガイドラインを認知・活用している割合は 27.9%、サイバー攻撃を受けた際の届出先（厚生労働省 医政局 研究開発推進課 医療情報技術推進室）を認知している割合は 29.2%、マルウェアや不正アクセス等に関する技術的な相談窓口（独立行政法人情報処理推進機構 情報セキュリティ安心相談窓口）を認知している割合は 23.1%と、いずれも 3 割に満たない結果であった。

病院・診療所の情報セキュリティ・サイバーセキュリティ確保に関して、行政は決して手をこまねいているわけではなく、既に安全管理のガイドラインが整備され、事案発生時の届出先や相談窓口も存在している。しかし、それらの取り組みを医療現場が認識し、活用しているかという点では、まだまだ課題がある。

図表 3-3-1. 行政の取り組みの認知度・活用度



※1.「医療情報システムの安全管理に関するガイドライン」
※2. 厚生労働省 医政局 研究開発推進課 医療情報技術推進室
※3. 独立行政法人情報処理推進機構 情報セキュリティ安心相談窓口

（２）厚労省ガイドラインの認知度・活用度

図表 3-3-2 は、情報システムの安全管理に関する厚労省ガイドラインの認知度・活用度について、病床規模別の状況を示している。

活用しているとの割合は、規模が大きくなるほど高くなっていた。

図表 3-3-2. 厚労省ガイドラインの認知度・活用度

		全体	活用している	知っているが活用していない	知らない
全体		2,989	27.9	32.9	39.2
病床規模	診療所	1,400	7.7	28.7	63.6
	病院　20～199床	979	34.1	44.2	21.7
	病院　200～499床	463	57.5	27.4	15.1
	病院　500床以上	147	85.7	13.6	0.7

（３）サイバー攻撃を受けた際の届け出先の認知度

図表 3-3-3 は、サイバー攻撃を受けた際の届出先の認知度について、病床規模別の状況を示している。

知っているとの割合は、規模が大きくなるほど高くなっていた。

図表 3-3-3. サイバー攻撃を受けた際の届け出先の認知度

		全体	知っている	知らない
全体		2,989	29.2	70.8
病床規模	診療所	1,400	12.6	87.4
	病院　20～199床	979	36.0	64.0
	病院　200～499床	463	50.5	49.5
	病院　500床以上	147	75.5	24.5

（４）不正アクセス等に関する技術的な相談窓口の認知度

図表 3-3-4 は、マルウェアや不正アクセス等に関する技術的な相談窓口の認知度について、病床規模別の状況を示している。

知っているとの割合は、規模が大きくなるほど高くなっていた。

図表 3-3-4. 不正アクセス等に関する技術的な相談窓口の認知度

		全体	知っている	知らない
全体		2,989	23.1	76.9
病床規模	診療所	1,400	8.8	91.2
	病院　20～199床	979	27.0	73.0
	病院　200～499床	463	44.9	55.1
	病院　500床以上	147	63.9	36.1

３．４　リスクマネジメントの体制

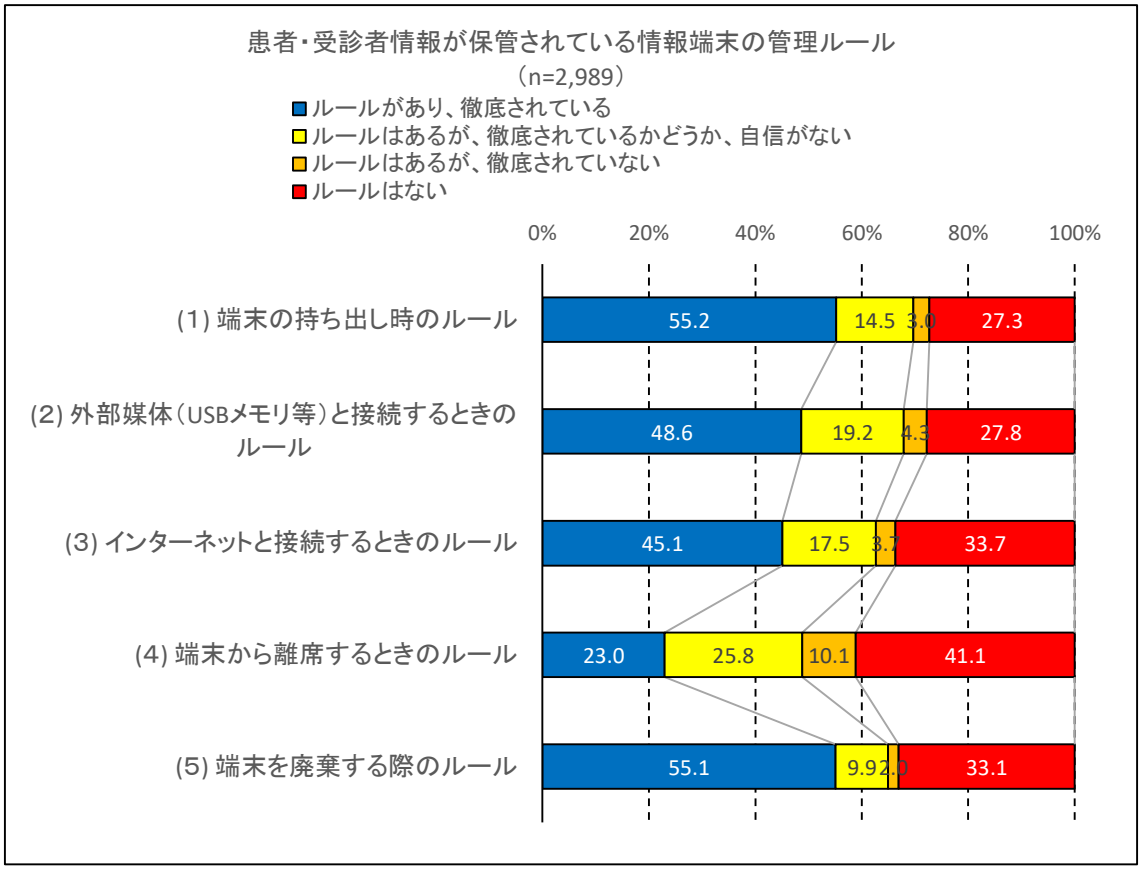
（１）事前対策

患者・受診者情報が保管されている情報端末の管理ルール

図表 3-4-1-1 は、患者・受診者情報が保管されている情報端末の管理ルールの状況を示している。

「（１）端末の持ち出し」「（２）外部媒体（USB メモリ等）との接続」「（３）インターネットと接続」「（４）端末から離席」「（５）端末を廃棄」という、５つのタイミングにおけるルールの状況を尋ねたが、３割前後～４割強の割合でルールがないとの回答結果であり、ルールの徹底度合いについても、「自信がない」「徹底されていない」との回答が少なくなかった。

図表 3-4-1-1. 患者・受診者情報が保管されている情報端末の管理ルール



図表 3-4-1-2 は、患者・受診者情報が保管されている情報端末の管理ルール５つそれぞれについて、「ルールはない」と回答した割合を病床規模別に示している。

５つのルールすべてにおいて、病床規模が大きくなるほど「ルールはない」という割合は低くなっていた。

図表 3-4-1-2. 患者・受診者情報が保管されている情報端末の管理ルール
病床規模別にみたルールなしの割合【%】

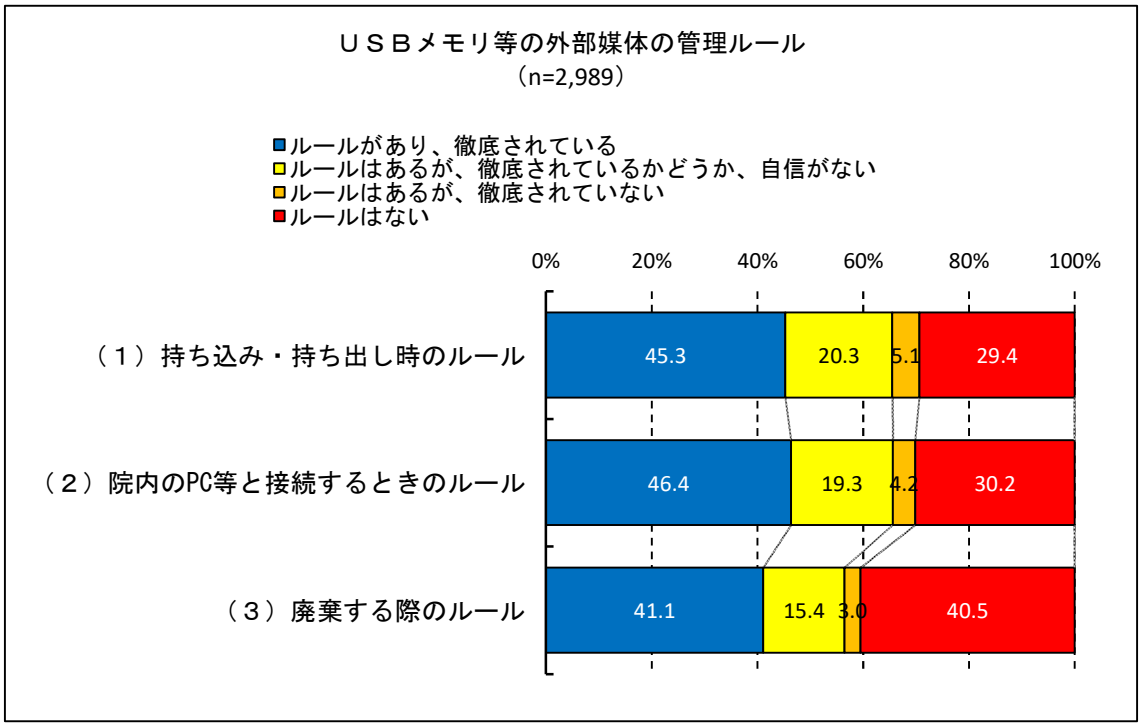
	（１）端末の持ち出し時のルール	（２）外部媒体（USBメモリ等）と接続するときのルール	（３）インターネットと接続するときのルール	（４）端末から離席するときのルール	（５）端末を廃棄する際のルール
全体（n=2,989）	27.3	27.8	33.7	41.1	33.1
診療所（n=1,400）	43.9	46.9	48.0	59.3	50.1
病院　20～199床（n=979）	17.1	15.8	27.9	32.8	23.0
病院　200～499床（n=463）	6.9	3.9	13.0	15.8	11.4
病院　500床以上（n=147）	1.4	0.0	1.4	3.4	6.1

ＵＳＢメモリ等の外部媒体の管理ルール

図表 3-4-1-3 は、ＵＳＢメモリ等の外部媒体の管理ルールの状況を示している。

「（１）持ち込み・持ち出し時」「（２）院内の PC 等と接続」「（３）廃棄する際」という、３つのタイミングにおけるルールの状況を尋ねたが、３割前後～４割強の割合でルールがないとの回答結果であり、ルールの徹底度合いについても、「自信がない」「徹底されていない」との回答が少なくなかった。

図表 3-4-1-3. ＵＳＢメモリ等の外部媒体の管理ルール



図表 3-4-1-4 は、ＵＳＢメモリ等の外部媒体の管理ルール３つそれぞれについて、「ルールはない」と回答した割合を病床規模別に示している。

３つのルールすべてにおいて、病床規模が大きくなるほど「ルールはない」という割合は低くなっていた。

図表 3-4-1-4. ＵＳＢメモリ等の外部媒体の管理ルール
病床規模別にみたルールなしの割合【%】

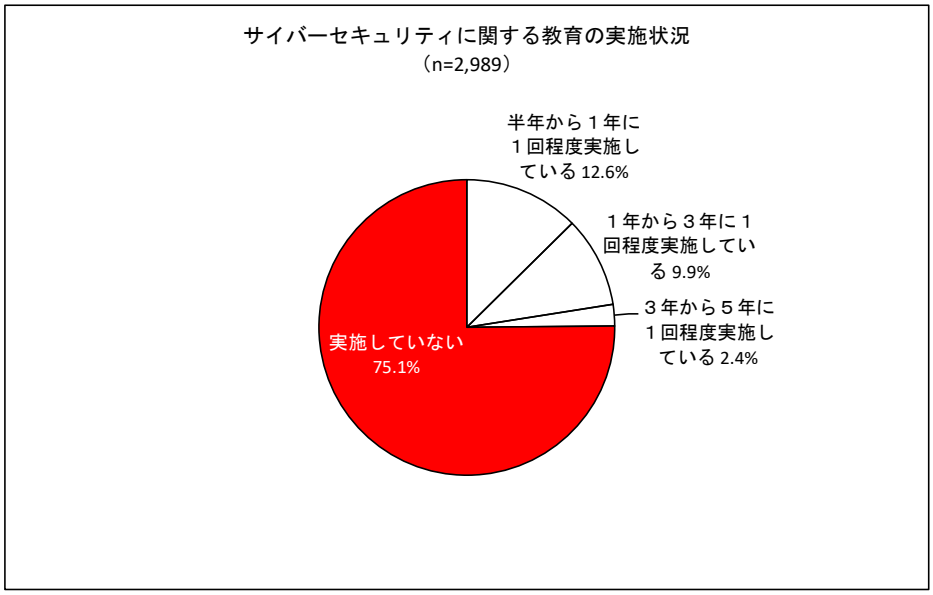
	（１）持ち込み・持ち出し時のルール	（２）院内のPC等と接続するときのルール	（３）廃棄する際のルール
全体（n=2,989）	29.4	30.2	40.5
診療所（n=1,400）	47.2	48.4	51.6
病院　20～199床（n=979）	18.8	19.7	35.1
病院　200～499床（n=463）	6.7	6.5	25.5
病院　500床以上（n=147）	2.0	0.7	17.7

教育の実施状況

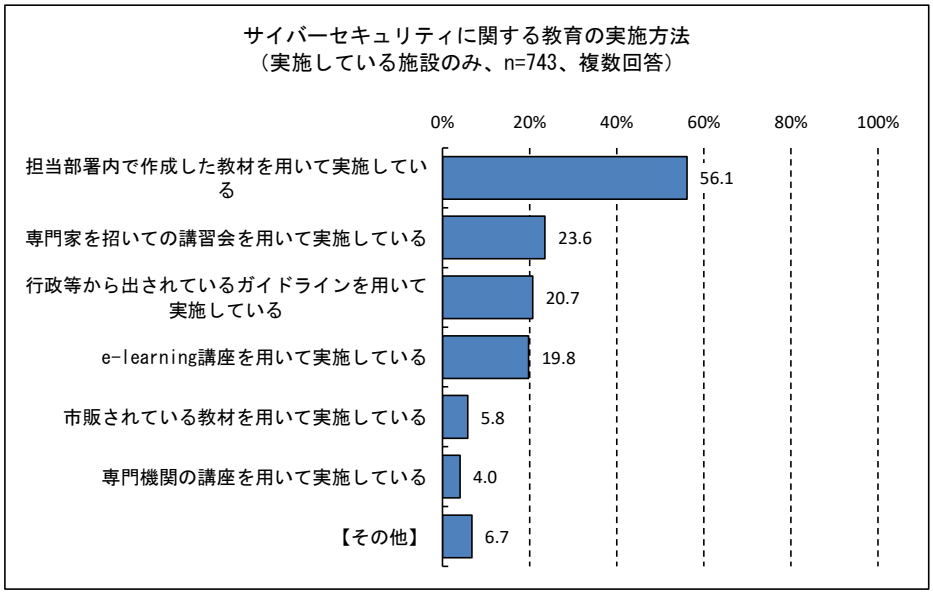
図表 3-4-1-5 は、サイバーセキュリティに関する教育の実施状況を示している。「半年から１年に１回程度実施」が 12.6%、「１年から３年に１回程度実施」が 9.9%、「３年から５年に１回程度実施」が 2.4%であり、約４分の１が教育を実施していたが、残りの約４分の３は教育を実施していなかった。

図表 3-4-1-6 は、教育を実施していると回答した施設の実施方法について示している。

図表 3-4-5-1. サイバーセキュリティに関する教育の実施状況



図表 3-4-1-6. 教育の実施方法



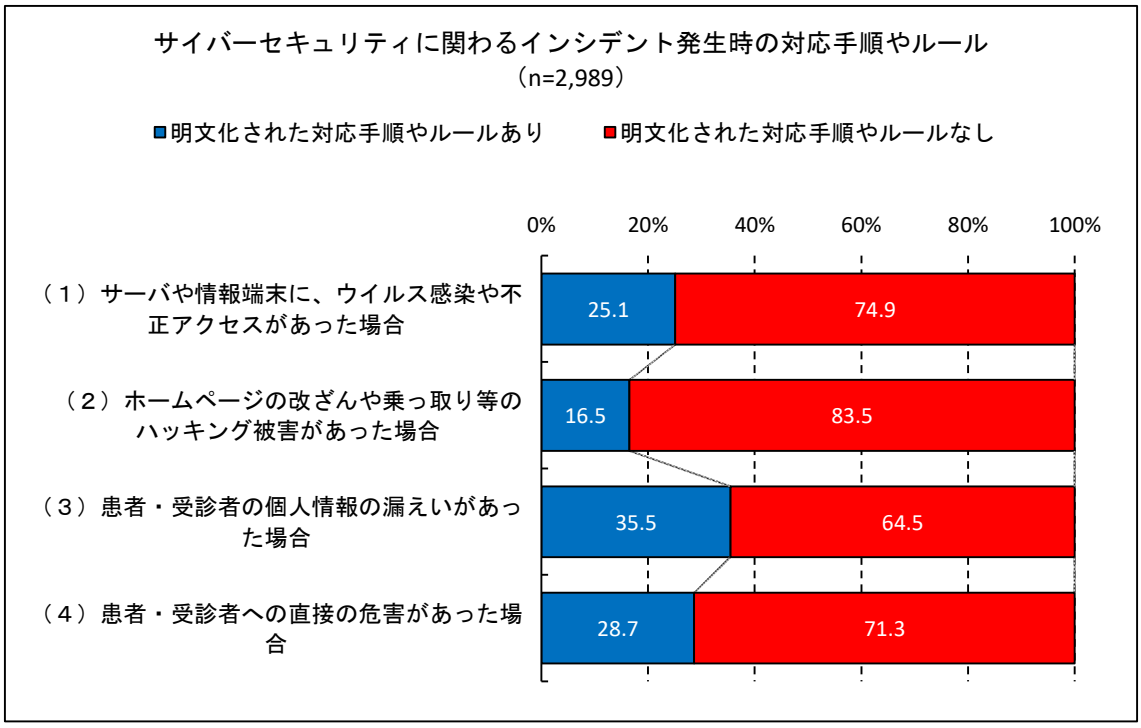
（２）発生時対策

インシデント発生時の対応手順やルール

図表 3-4-2-1 は、サイバーセキュリティに関わるインシデント発生時の明文化された対応手順やルールの有無の状況を示している。

「（１）サーバや情報端末に、ウイルス感染や不正アクセスがあった場合」「（２）ホームページの改ざんや乗っ取り等のハッキング被害があった場合」「（３）患者・受診者の個人情報の漏えいがあった場合」「（４）患者・受診者への直接の危害があった場合」という、４つのケースにおける対応手順やルールの有無について尋ねたが、３分の２弱から８割強の割合で、明文化された手順やルールがないとの回答結果であった。

図表 3-4-2-1. インシデント発生時の対応手順やルール



図表 3-4-2-2 は、インシデント発生時の明文化された対応手順やルール４つそれぞれについて、「対応手順やルールはない」と回答した割合を病床規模別に示している。

４つのルールすべてにおいて、病床規模が大きくなるほど「対応手順やルールはない」という割合は低くなっていた。

図表 3-4-2-2. インシデント発生時の対応手順やルール

病床規模別にみた明文化された対応手順やルールなしの割合【%】

	（１）サーバや情報端末に、ウイルス感染や不正アクセスがあった場合	（２）ホームページの改ざんや乗っ取り等のハッキング被害があった場合	（３）患者・受診者の個人情報の漏えいがあった場合	（４）患者・受診者への直接の危害があった場合
全体（n=2,989）	74.9	83.5	64.5	71.3
診療所（n=1,400）	89.7	91.3	86.4	87.6
病院　20～199床（n=979）	71.9	83.9	53.2	63.0
病院　200～499床（n=463）	51.2	70.6	36.5	50.1
病院　500床以上（n=147）	27.9	48.3	20.4	38.8

（３）事後対策

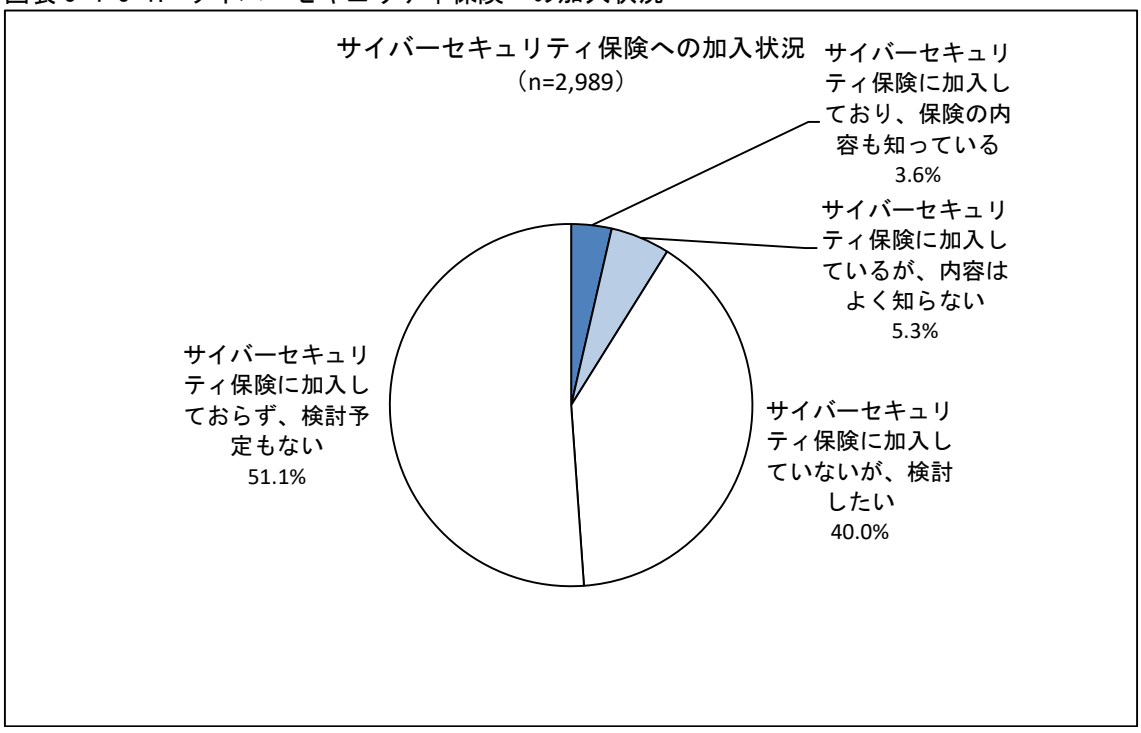
サイバーセキュリティ保険への加入状況

図表 3-4-3-1 は、サイバーセキュリティ保険への加入状況を示している。

「サイバーセキュリティ保険に加入しており、保険の内容も知っている」との回答割合は 3.6%であり、「サイバーセキュリティ保険に加入しているが、内容はよく知らない」との回答割合は 5.3%であった。また、同保険への加入割合は 8.9%であり、１割に満たない。

一方で、「サイバーセキュリティ保険に加入していないが、検討したい」との回答割合が 40.0%、「サイバーセキュリティ保険に加入しておらず、検討の予定もない」との回答割合が 51.1%であった。

図表 3-4-3-1. サイバーセキュリティ保険への加入状況



再発防止策（発生したインシデントへの対応状況）

図表 3-4-3-2 は、発生したインシデントへの対応状況を示している。

「インシデントの原因分析と今後の対応まで整理できている」との回答割合は 58.3%であり、「インシデントの原因分析と今後の対応まで整理できている」は 15.2%、「インシデントが発生したという事実まで整理できている」は 23.8%であった。

病床規模別にみると、「インシデントの原因分析と今後の対応まで整理できている」との割合、すなわち原因を分析して、再発防止策を講じるに至っている割合は、規模に応じて高くなる傾向にあった。

図表 3-4-3-2. 発生したインシデントへの対応状況

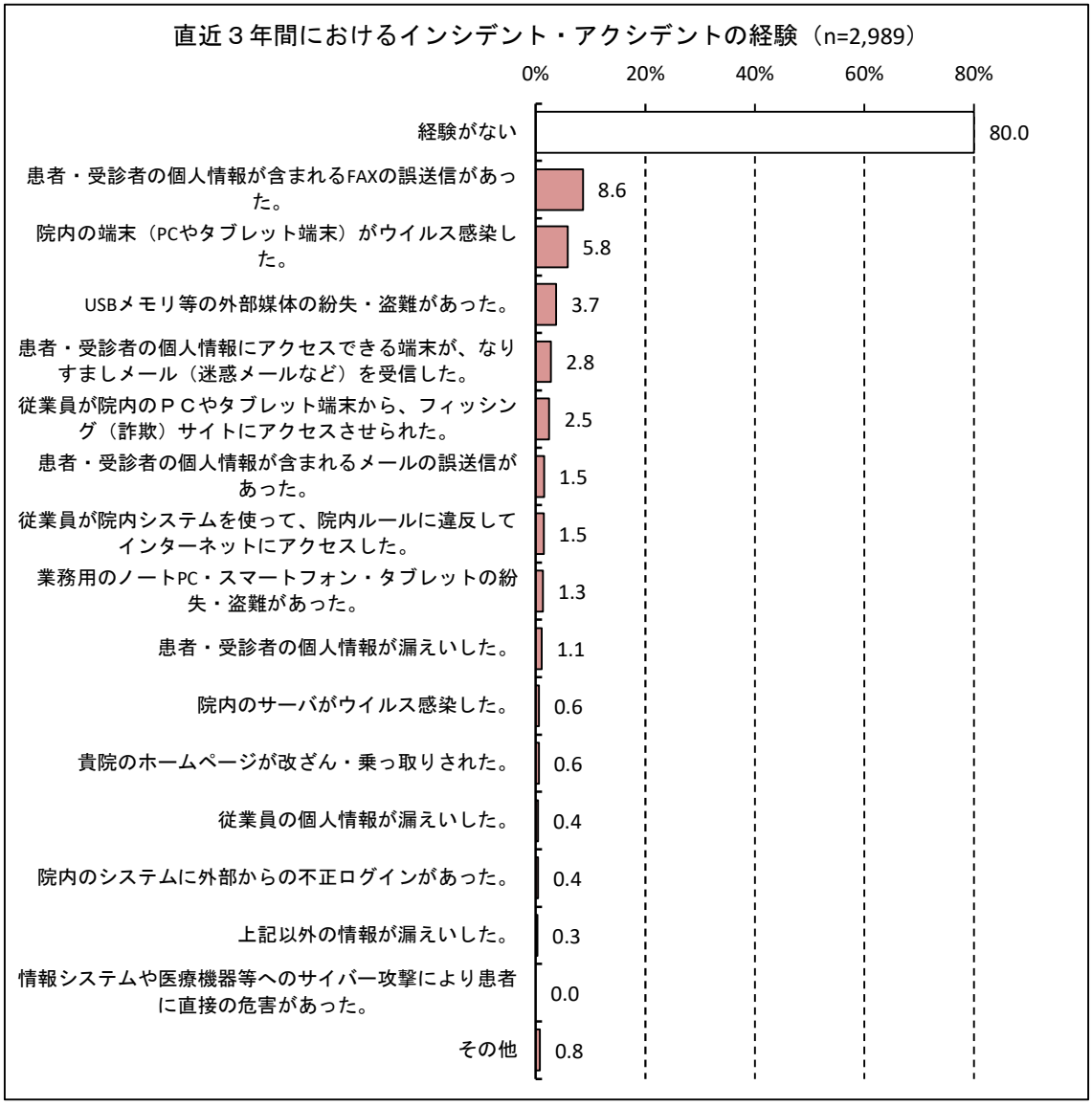
		全体	インシデントの原因分析と今後の対応まで整理できている	インシデントの原因分析まで整理できている	インシデントが発生したという事実まで整理できている	その他
全体		597	58.3	15.2	23.8	2.7
病床規模	診療所	69	40.6	15.9	36.2	7.2
	病院　20～199床	238	48.7	20.6	28.2	2.5
	病院　200～499床	187	64.2	12.3	20.9	2.7
	病院　500床以上	103	81.6	7.8	10.7	0.0

３．５　実際の経験

図表 3-5-1 は、直近３年間におけるインシデント・アクシデントの経験を示している。

「経験なし」が 80%であった。また、最も危惧される「サイバー攻撃により患者に直接の危害があった」との事象は確認されなかった。一方で、情報の誤送信やウイルス感染、端末の盗難・紛失等といったインシデント・アクシデントの発生が確認できた。

図表 3-5-1. 直近３年間におけるインシデント・アクシデントの経験（複数回答あり）

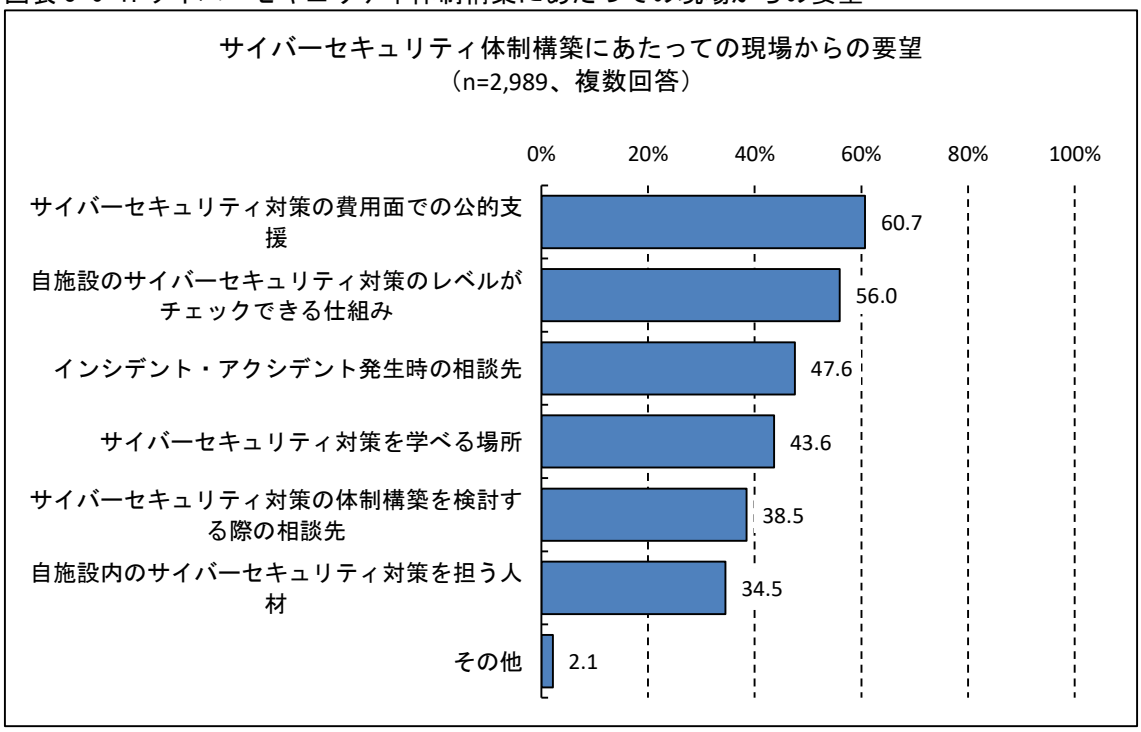


３．６　医療現場からの要望

図表 3-6-1 は、サイバーセキュリティ体制構築にあたっての医療現場からの要望について示している。

「サイバーセキュリティ対策の費用面での公的支援」を挙げた割合が最も高く 60.7%であり、次いで「自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み」を挙げたのが 56.0%と、これら２つの要望を挙げた割合が５割を超えていた。

図表 3-6-1. サイバーセキュリティ体制構築にあたっての現場からの要望



図表 3-6-2 は、サイバーセキュリティ体制構築にあたって最も優先度が高いひとつを選んでもらった回答結果について、全体および病床規模別の状況を示している。

自院のセキュリティのレベルをチェックできる仕組みが欲しいとの要望が、病床規模に関わらず優先度が高かった。また、セキュリティ対策の費用面での公的支援の要望は、病床規模が大きくなるほど優先度が高かった。

図表 3-6-2. サイバーセキュリティ体制構築にあたって最も優先度が高い要望

		全体	自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み	インシデント・アクシデント発生時の相談先	サイバーセキュリティ対策の体制構築を検討する際の相談先	サイバーセキュリティ対策を学べる場所	自施設内のサイバーセキュリティ対策を担う人材	サイバーセキュリティ対策の費用面での公的支援	その他
全体		2,989	27.4	14.2	9.9	9.4	15.2	22.3	1.7
病床規模	診療所	1,400	28.9	21.0	12.5	10.6	7.7	16.6	2.6
	病院　20～199床	979	25.7	9.8	8.1	9.7	21.3	24.6	0.7
	病院　200～499床	463	26.6	6.0	6.5	6.9	21.6	30.9	1.5
	病院　500床以上	147	25.9	4.1	7.5	2.7	25.9	33.3	0.7

４．考察と提言

本稿では、医療情報システムの管理体制の実態把握を目的とし、全国の病院・診療所を対象に実施した調査結果（n=2,989）を基に議論を進めてきた。

まず、主な医療情報システムの利用状況と院内外との接続状況を概観したうえで、対策の組織体制、行政の取り組みの認知度・活用度、リスクマネジメントの体制、実際の経験、医療現場からの要望、という順に整理し、日本の医療機関における情報セキュリティとサイバーセキュリティについて、病床規模別の状況も含めて、その実情を個別に確認した。

４．１　まとめと考察

まず調査結果について、上記の流れに沿って、以下に概略まとめておく。

（１）サイバーセキュリティ対策の組織体制

- 現状、現場の組織体制は問題含みである。院内の医療情報システムのネットワーク構成図を保有し、計画的に見直しをしているのは 5.7%に過ぎず、約半数（49.2%）はネットワーク構成図を持っていない。情報システムの管理体制においては、専任の担当部門があるのは２割強（20.6%）であり、３分の２弱（64.4%）は兼務の担当者あるいは院長自らが管理、という体制である。対策費用の準備状況を見ると、計画的に対策費用を準備しているのは１割強（10.4%）であり、半数近くの医療機関は費用を準備していない。

- これらの組織体制は、総じて病床規模の大きさに応じて状況が良くなる傾向にあったが、換言すれば、診療所や中小規模の病院ほど組織体制に問題を抱えているということである。病床規模に応じて、組織の ICT リテラシーに格差がある現状が推察される。

（２）行政の取り組みの認知度・活用度

- 医療機関のサイバーセキュリティ確保にあたり、すでに行政のガイドラインが整備されており、事案発生時の届出先や相談窓口も存在している。しかし、それらの取り組みを医療現場が然るべく認識し、活用しているかという点では、まだまだ課題がある。情報システムの安全管理に関する厚労省ガイドライン（医療情報システムの安全管理に関するガイドライン）を認知・活用している割合は 27.9%、サイバー攻撃を受けた際の届出先（厚生労働省 医政局 研究開発推進課 医療情報技術推進室）を認知している割合は 29.2%、マルウェアや不正アクセス等に関する技術的な相談窓口（独立行政法人情報処理推進機構 情報セキュリ

ティ安心相談窓口）を認知している割合は 23.1%と、いずれも３割に満たない結果であった。

- これらの認知度・活用度についても、総じて病床規模の大きさに応じて状況が良くなる傾向にあった。

（３）リスクマネジメントの体制

- サイバーセキュリティに関するリスクマネジメント体制には、課題がある。本稿では事前対策、発生時対策、事後対策に分けて結果をまとめたが、その概略は、以下の通りである。
  【事前対策の状況】患者・受診者情報が保管されている情報端末の管理ルールについては３割前後～４割強が、USB メモリ等の外部媒体の管理ルールについても３割前後～４割強が「ルールなし」との回答であった。また、４分の３超（75.1%）の施設は、サイバーセキュリティに関する従業員教育を実施していなかった。
  【発生時対策の状況】インシデント発生時の手順やルールの整備状況については、３分の２弱から８割強の割合で、明文化された手順やルールがないとの結果であった。
  【事後対策の状況】サイバーセキュリティ保険に加入している施設は１割に満たなかった（8.9%）。また、過去３年間にインシデントを経験した回答者のうち、原因分析と今後の対応まで整理できているとの回答割合は６割弱（58.3%）であり、４割超は再発防止に向けた対応にまで至っていなかった。

- これらリスクマネジメント体制についても、総じて病床規模の大きさに応じて状況が良くなる傾向にあった。

（４）実際の経験

- 直近３年間における実際のインシデント・アクシデントの経験に関しては、８割が「経験なし」との回答であり、最も危惧される「サイバー攻撃により患者に直接の危害があった」との事象は確認されなかった。一方で、発生割合が多い順に並べると、情報の誤送信（8.6%）やウイルス感染（5.8%）、端末の盗難・紛失（3.7%）等といった事象の発生が確認できた。

- 情報の誤送信や端末や媒体の紛失・盗難といった情報セキュリティに関わるインシデントだけではなく、「院内の端末がウイルス感染」（5.8%）、「なりすましメールを受信」（2.8%）、「フィッシングサイトにアクセス」（2.5%）、「院内のサーバがウイルス感染」（0.6%）、「ホームページが改ざん・乗っ取り」（0.6%）、「外部からの不正ログイン」（0.4%）といったサイバーセキュリティに関わるインシデントの発生が確認できたことは、特筆すべきである。

（５）医療現場からの要望

- 「サイバーセキュリティ対策の費用面での公的支援」と「自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み」の２つが、ともに５割を超える施設が挙げた２大要望であった。

- 優先順位と病床規模を勘案すると、自院のセキュリティのレベルをチェックできる仕組みが欲しいとの要望が、病床規模に関わらず優先度が高かった。また、セキュリティ対策の費用面での公的支援の要望は、病床規模が大きくなるほど優先度が高かった。

４．２　提言

最後に、今後に向けた提言を列挙し、結論に代えたい。

（１）組織体制を充実させる

組織体制の課題は、ヒト（人材の確保）とカネ（費用の確保）の２つに集約できる。前者について言えば、一部の大病院・大規模法人を除けば組織内部で情報システムやそのセキュリティに詳しい専門人材を雇用し育成することは難しいと考えられる。今回データとして明らかになった現状は、かかる実情の裏返しと推察される。

- 医療現場には、医療安全すなわち、医療事故対応や患者安全の確保で培ったPDCA モデルが根付いている。まずは、現場の医療安全の担当者をはじめ、すべての医療従事者に対して、サイバーセキュリティに関する安全確保について、身近な問題としてあらためて意識づけをすることが重要である。医療安全の教育プログラムに、サイバーセキュリティに関する内容を組み込むことも有効かもしれない。医療安全担当者にはサイバーセキュリティを含むICT リテラシーの涵養が求められ、一方で、サイバーセキュリティ対策に従事する情報システム担当者には、医療安全のノウハウや知識を身に付けることが求められる。
- 自前の専門人材を採用・育成することが難しい診療所や中小規模の病院に対しては、例えば地域医師会等が主体となって人材を計画に配備し、各地域の複数医療機関でシェアするという手法が有効ではないだろうか。また、このような人材を育成し地域ごとに確保していくうえでも、医療現場への費用面での公的支援を政策として実現することが必須である。
- 人材育成に関しては、「ICT リテラシー底上げのための人材育成」と「自前での専門家育成」（特に、大病院・大規模法人向け）の少なくとも２通りのプログラムが必要である。組織の ICT リテラシーの格差に応じた教育支援

が求められる[21]。

（２）リスクマネジメント体制を強化する

医療現場のサイバーリスクの実態がデータとして明らかになって初めて、それらのリスクに合理的に対処することも可能になる。そういった意味でも、すでにある行政のガイドラインや届出先、相談窓口について、より一層の現場の認知度向上が必要である。また、医療機関のリスクマネジメント強化のために、周辺業界が有する知見やノウハウを積極的に活用することも有効ではなかろうか。

- サイバーセキュリティ対策に医療安全に関わる現場のノウハウが応用可能ではないだろうか。具体的には、行政が全国で発生したインシデントやアクシデントの事案を収集、リスクマネジメントの専門家の協力を得て収集されたデータを分析し、そこから得られた知見を現場にフィードバックすることで、医療の質や安全を高めるという手法である。
- 同様に、医療情報システムと医療機器を開発・販売している業界・業者からのサイバーセキュリティに関するより積極的な情報提供が望まれる。現状のように、各社の自主性に任されている状況では不十分である。個別のシステムやデバイスのセキュリティ・インシデント情報について、業界を挙げてより体系的に収集・分析し、再発防止に役立てるような仕組みが求められる。
- 民間保険会社では「サイバーセキュリティ保険」によるセキュリティ・インシデント発生後の金銭的補償という本来の保険機能に加え、発生時、さらには発生前のサイバーリスク軽減に資する付帯サービス[22]を順次開発・提供している。これらの医療分野に役立つサービスの開発に医療界／保険業界共同で取り組むことも考えられる。

（３）現場の要望に応える

今回の調査では、「サイバーセキュリティ対策の費用面での公的支援」、「自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み」、「インシデント・アクシデント発生時の相談先」、「サイバーセキュリティ対策を学べる場所」、「サイバーセキュリティ体制構築を検討する際の相談先」、「自施設内のサイバーセキュリティ対策を担う人材」について尋ねたが、「その他」を挙げた回答は非常に少なく[23]、現場の要望としては、ほぼこれらの５つに集約されると考えてよいだろう。

---

[21] 関連する行政の取り組み事例としては、厚生労働省の「医療分野のサイバーセキュリティ対策について」のページに研修用動画と研修教材がある。
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html
医療界の取り組み事例としては、「メディカル ICT リーダー養成講座【初級】」（日本医師会 ORCA 管理機構　オルカモ・ウェブ・ラーニング）等が挙げられる。https://owl.orcamo.co.jp/medict/

[22] サイバーリスク情報提供サービス、リスク診断サービス、緊急時対応サービス等。

[23] 「その他」を挙げた割合は、複数回答可で 2.1%、もっとも優先度が高い択一回答で 1.7%であった。

- 関連政策に割くことのできる予算や人員も限られていることから、優先順位をつけて対処していくのが現実的と思われる。今回、「サイバーセキュリティ対策の費用面での公的支援」と「自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み」の２つが、医療現場からの要望として、特にプライオリティが高いことが明らかになった。前者については診療報酬や補助金として、医療政策に反映させるべきである。後者については、行政が責任を持ち、医師会や関連学会がそれに協力する形で、チェックリストやフローチャート、安全マニュアル等の整備を具体的に進めるべきである。

参考文献

医療経済研究機構（2019）「全国保険医療機関（病院・診療所）一覧（平成 30 年度版）」
https://www.ihep.jp/publications/other/?y=2019

神足祐太郎（2020）「サイバーセキュリティ政策の現状」調査と情報—ISSUE BRIEF—, 第 1078 号, 国立国会図書館.
https://dl.ndl.go.jp/view/download/digidepo_11423782_po_1078.pdf?contentNo=1

坂口一樹・堤信之（2020）「医療機関におけるサイバーセキュリティ実態調査：パイロット調査」日医総研リサーチエッセイ, No.84
https://www.jmari.med.or.jp/research/research/wr_702.html

深津博（2020）「医療機関におけるサイバーセキュリティの現状と課題」The Journal of JAHMC, 2020, Vol.31, No.5, p.12-17.

三角育生（2020）「サイバーセキュリティ基本法制定・改正の経緯」日本セキュリティ・マネジメント学会誌, Vol.34, No.1, p.28-34.

山本隆一（2017）「医療の IT 化をめぐる問題」JRI レビュー. Vol.9. No.48
https://www.jri.co.jp/MediaLibrary/file/report/jrireview/pdf/9996.pdf