2020 年 6 月 15 日

日医総研リサーチエッセイ　No.84

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

坂口一樹（主任研究員）、堤　信之（主任研究員）

要　旨

- 日本の医療機関（病院・診療所）におけるサイバーセキュリティに関わる状況の実態把握を目的とし、日本医師会ＯＲＣＡ管理機構が実施する通信講座・セミナーの受講者を対象にアンケート調査を行った。

- 最も危惧される「患者・受診者の情報が漏えいした」という事象は、直近 3 年間の経験を問うた今回の調査では確認されなかった。

- 他方で、「なりすましメールを受信」や「FAX・メールの誤送信」、「従業員が不正なウェブサイトにアクセス」、「院内の端末がウイルス感染」等のインシデント・アクシデントがあったことが確認された。医療機関においても、然るべきサイバーセキュリティ対策が必須なことは言うまでもない。

- サイバーセキュリティ対策にあたっての基本的なルールの整備状況、組織体制の実態、予算確保の状況を見ると、いずれも問題含みである。ルールや組織体制、予算が整備されていないケースが決して少なくない。

- 対策にあたっての課題や不安を問うた結果からは、医療現場のサイバーセキュリティを担える人材の育成と確保が主たる課題である、という認識が浮かび上がった。

- 調査を総括して言えることは、医療現場におけるサイバーセキュリティはまだまだ発展途上である、ということだろう。ただし、今回はパイロット調査であり、サンプル数も少ない（n=128）。対象を全国の医療機関に拡大した本格的な調査実施を検討するべきと考える。

目　次

1. はじめに

今日のサイバースペース、特にインターネットを利用するのは善意の人たちばかりではない。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コンピュータへの不正侵入等といった脅威が世界規模で生じている[1]。情報の悪用や改ざん、詐欺行為、プライバシーの侵害などが発生しており、インターネットを利用する私たちには様々なリスクが降りかかっている。

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。私たちの健康・医療に関する情報は、最も機微性が高い情報のひとつであり、これらの悪用や改ざんによって人々が受ける被害は計り知れない。実際、サイバースペースに存在する闇市場では人々の医療データが高額で取引されている実情が報告されており[2]、現実の世界でも、医療機関がランサムウェア[3]の被害にあった事例が国内外で見受けられる[4]。

こうした状況に鑑み、わが国は 2014 年の段階で「サイバーセキュリティ基本法」を制定している。新体制として内閣に「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」が定められた。医療その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すでに稼働している。

他方で、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いない。関連する既往調査も限られている。ただしこれは、サイバーセキュリティに関わるインシデント・アクシデントについては医療現場が素直に答えたがらないという、ごく当たり前の実態の裏返しかもしれず、大規模調査の実施には慎重にならざるを得ない。そこで筆者らは、まずは比較的身近な対象（関連会社が提供する e ラーニング等の受講者）に向けて、パイロット調査を行った。

---

1 例えば、次の記事。「つながる工場　攻撃 7 倍　サイバーリスク　IoT 普及で高まる」『日本経済新聞』（2020 年 6 月 11 日　朝刊 1 面）

2 「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」
https://www.itmedia.co.jp/news/articles/1903/14/news017.html
"Your private medical data is for sale – and it's driving a business worth billions"
https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns

3 ランサムウェアとは、パソコンやサーバー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。

4 国内では奈良県の宇陀市立病院の事件、海外では米国の Hollywood Presbyterian Medical Center や Hancock Regional Hospital、カナダの The Ottawa Hospital の事件が挙げられる。

2. 調査の概要

2.1. 調査の目的

調査の目的は、日本の医療機関（病院・診療所）におけるサイバーセキュリティに関わる状況の実態把握である。単にインシデント・アクシデントの発生の有無だけではなく、サイバーセキュリティに関わるリスクマネジメント体制全般（事前の備えと事案発生時の対応手順等）について尋ねた。調査にあたって、着目したポイントは以下の 5 点である。

1. **インシデント・アクシデントの経験**
2. **情報端末（PC 等）や外部媒体（USB メモリ等）の管理ルール**
3. **インシデント・アクシデント発生時の対応手順**
4. **サイバーセキュリティ対策の組織体制**
5. **サイバーセキュリティ対策にあたっての課題と不安**

また、本調査の位置づけはパイロット調査である。全国の医療機関を対象とした大規模調査の実施を展望し、実現可能性の検証やより精緻な調査設計のための仮説構築を企図して、まずは身近な調査対象に向けて実施した。

2.2. 対象と方法

今回、調査対象としたのは、日本医師会ＯＲＣＡ管理機構が主に医療関係者を対象に実施している e-ラーニング講座[5]の受講者、そして同機構が 2019 年 6 月に実施したサイバーセキュリティに関わるシンポジウム[6]の受講者の合計 1,559 名である。

調査方法は、ウェブを活用したアンケート調査である。筆者らが設計した調査票【別添資料１】を基にしたアンケート・フォームを日本医師会ＯＲＣＡ管理機構がウェブ上に設置。そのうえで対象者らにメールで回答を依頼し、インターネットを通じて回答してもらった。過去のインシデント・アクシデントについて尋ねるという調査の性質上、匿名調査とした。調査実施期間は、2020 年 2 月 17 日から 3 月 16 日である。同期間において 128 件の有効回答を得た。回答率は 8.2%（128 / 1,559）であった。

---

[5] e-ラーニング講座「OWL（オウル）」日本医師会 ORCA 管理機構。https://owl.orcamo.co.jp/
[6] 社会人プログラミング教育研究実行委員会シンポジウム「今そこにあるサイバー危機」
https://www.med.or.jp/nichiionline/article/008602.html

2.3. 回答者の属性

本節では、回答者の主な属性（主たる勤務先、職位と職種、患者・受診者情報を扱うシステム環境）について示す。

（１）主たる勤務先

図表 2-1. 主たる勤務先（n=128）※

病院 200床以上	18	14.1%
病院 100-199床	16	12.5%
病院 20-99床	9	7.0%
診療所	67	52.3%
その他	18	14.1%
総計	**128**	**100.0%**

※「その他」としては、医師会等の医療関係団体が主であった。

（２）職位と職種

図表 2-2. 職位と職種（n=128）

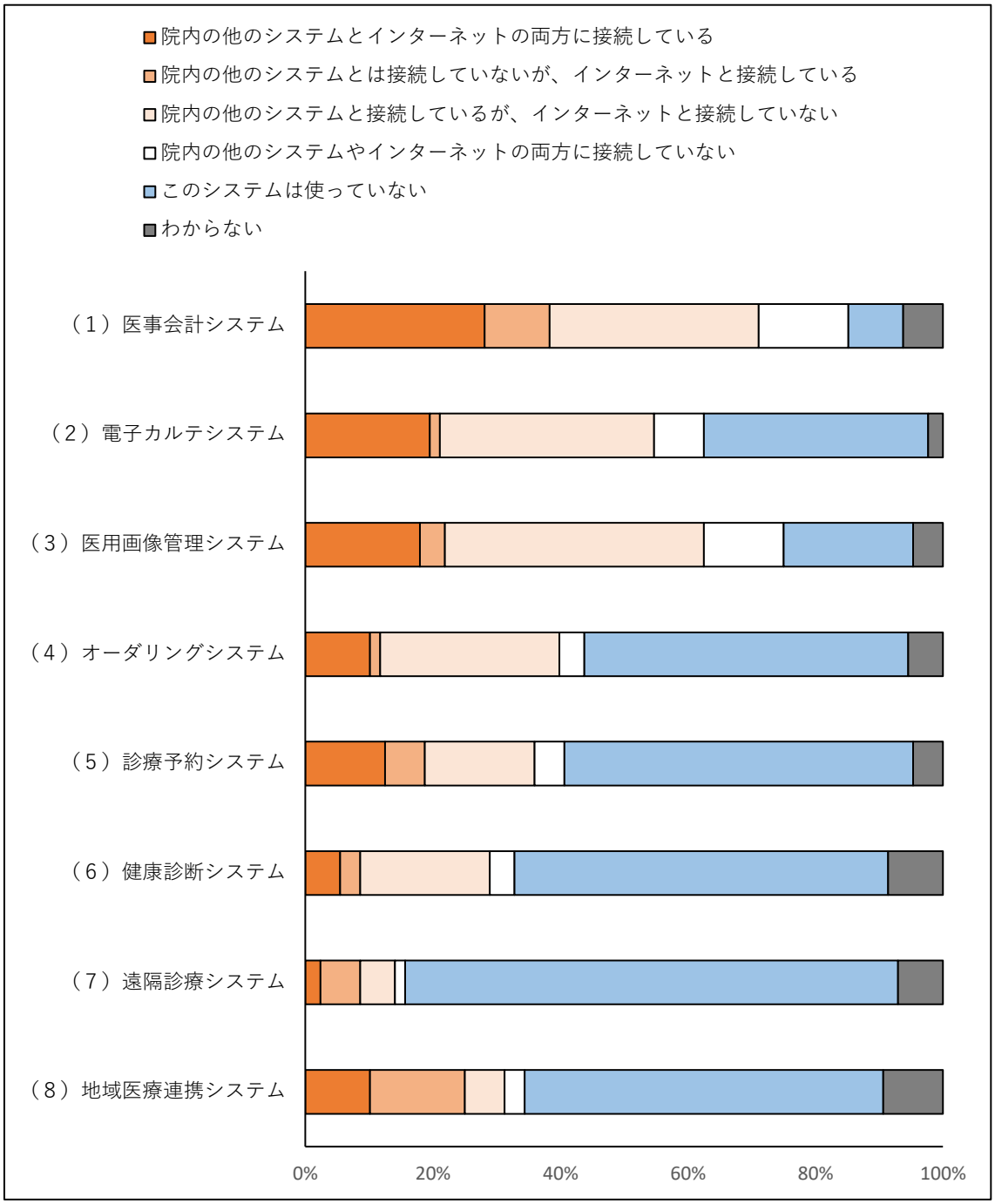
経営者・役員	37	28.9%
管理職 システム担当	33	25.8%
管理職 システム担当ではない	26	20.3%
非管理職 システム担当	18	14.1%
非管理職 システム担当ではない	14	10.9%
総計	**128**	**100.0%**

（３）患者・受診者情報を扱うシステム環境

図表 2-3-1. 患者・受診者情報を扱うシステム環境（n=128）

	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	院内の他のシステムとは接続していないが、インターネットと接続している	院内の他のシステムと接続しているが、インターネットと接続していない	院内の他のシステムやインターネットの両方に接続していない	このシステムは使っていない	わからない
（1）医事会計システム（レセコン）	28.1%	10.2%	32.8%	14.1%	8.6%	6.3%
（2）電子カルテシステム	19.5%	1.6%	33.6%	7.8%	35.2%	2.3%
（3）医用画像管理システム	18.0%	3.9%	40.6%	12.5%	20.3%	4.7%
（4）オーダリングシステム	10.2%	1.6%	28.1%	3.9%	50.8%	5.5%
（5）診療予約システム	12.5%	6.3%	17.2%	4.7%	54.7%	4.7%
（6）健康診断システム（健診・人間ドック等の受診者管理システム）	5.5%	3.1%	20.3%	3.9%	58.6%	8.6%
（7）遠隔診療システム	2.3%	6.3%	5.5%	1.6%	77.3%	7.0%
（8）地域医療連携システム（医療連携、医療・介護連携のシステム）	10.2%	14.8%	6.3%	3.1%	56.3%	9.4%

図表 2-3-2. 患者・受診者情報を扱うシステム環境【再掲[注]】(n=128)



注：オレンジ色が濃いシステムほど、サイバーセキュリティのリスクが高いと考えられる。

3. 調査結果

本章では、調査結果の単純集計分析とクロス集計分析の結果を示す。クロス集計にあたっては、勤務先別（病院 200 床以上、病院 200 床未満、診療所、その他）、職位別（経営者・役員、経営者・役員以外）でクロス集計を行った。

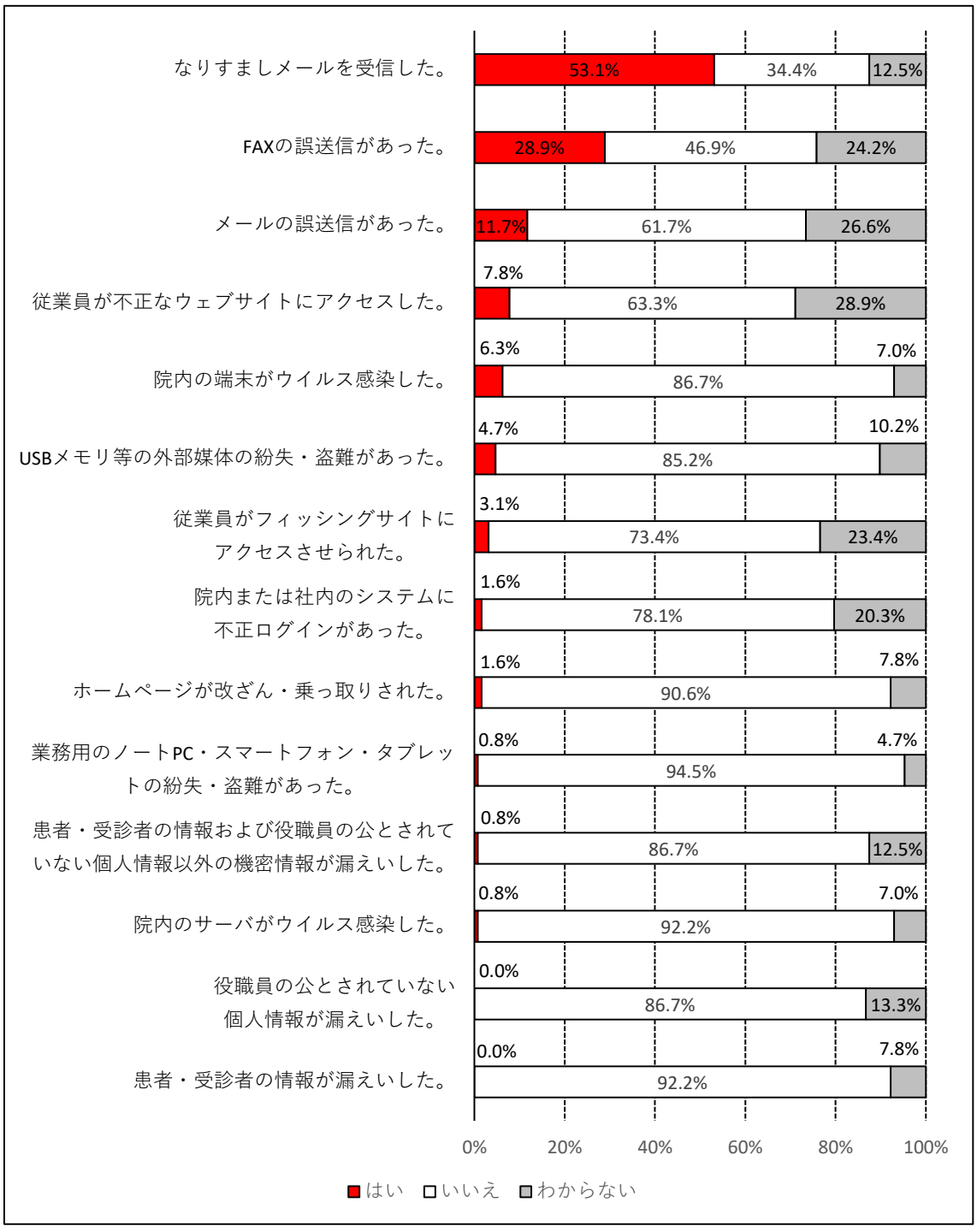
3.1. 過去 3 年間におけるインシデント・アクシデントの経験

図表 3-1-1 は、過去 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。「なりすましメールを受信」（53.1%）、「FAX の誤送信」（28.9%）、「メールの誤送信」（11.7%）、「従業員が不正なウェブサイトにアクセス」（7.8%）、「院内の端末がウイルス感染」（6.3%）の順に多かった。一方で、「役職員の公とされていない情報が漏えい」（0.0%）や「患者・受診者の情報が漏えい」（0.0%）との回答は、ともに無かった。

勤務先別クロス集計（図表 3-1-2）を見ると、「なりすましメールを受信」が、すべての勤務先において最も経験した割合が高かった。ただ、病院・診療所の同割合が 40.0～50.7%だったのに対し、その他の同割合は 88.9%であり、その差が際立った。病院・診療所の場合、他業界に比べてなりすましメール受信の経験が比較的少ないのかもしれない。

職位別クロス集計（図表 3-1-3）を見ると、「院内または社内のシステムに不正ログイン」（18.9%）、「従業員が不正なウェブサイトにアクセス」（13.5%）、「従業員がフィッシングサイトにアクセス」（10.8%）については、1 割超の経営者・役員が「わからない」と回答、すなわち実態を把握していなかった。

図表 3-1-1. 過去 3 年間におけるインシデント・アクシデントの経験（n=128）



図表 3-1-2. 過去 3 年間におけるインシデント・アクシデントの経験【勤務先別】

（1）院内のサーバがウイルス感染した。
（2）院内の端末（PCやタブレット端末）がウイルス感染した。
（3）従業員が不正なウェブサイトにアクセスした。
（4）従業員がフィッシング（詐欺）サイトにアクセスさせられた。
（5）ホームページが改ざん・乗っ取りされた。
（6）なりすましメール（迷惑メールなど）を受信した。
（7）患者・受診者の情報が漏えいした。
（8）役職員の公とされていない個人情報が漏えいした。
（9）（7）および（8）以外の機密情報が漏えいした。
（10）院内または社内のシステムに不正ログインがあった。
（11）業務用のノートPC・スマートフォン・タブレットの紛失・盗難があった。
（12）USBメモリ等の外部媒体の紛失・盗難があった。
（13）メールの誤送信があった。
（14）FAXの誤送信があった。

選択肢	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
病院 200床以上 (n=18)														
はい	5.6%	11.1%	22.2%	5.6%	11.1%	44.4%	0.0%	0.0%	0.0%	0.0%	0.0%	16.7%	16.7%	33.3%
いいえ	83.3%	77.8%	44.4%	55.6%	72.2%	33.3%	83.3%	77.8%	77.8%	66.7%	83.3%	61.1%	61.1%	33.3%
わからない	11.1%	11.1%	33.3%	38.9%	16.7%	22.2%	16.7%	22.2%	22.2%	33.3%	16.7%	22.2%	22.2%	33.3%
病院200床未満 (n=25)														
はい	0.0%	4.0%	4.0%	0.0%	0.0%	40.0%	0.0%	0.0%	0.0%	4.0%	0.0%	4.0%	8.0%	36.0%
いいえ	96.0%	88.0%	52.0%	64.0%	92.0%	40.0%	96.0%	88.0%	88.0%	72.0%	96.0%	80.0%	52.0%	24.0%
わからない	4.0%	8.0%	44.0%	36.0%	8.0%	20.0%	4.0%	12.0%	12.0%	24.0%	4.0%	16.0%	40.0%	40.0%
診療所 (n=67)														
はい	0.0%	6.0%	3.0%	1.5%	0.0%	50.7%	0.0%	0.0%	0.0%	1.5%	0.0%	1.5%	13.4%	25.4%
いいえ	95.5%	89.6%	73.1%	83.6%	97.0%	38.8%	94.0%	89.6%	89.6%	83.6%	98.5%	95.5%	68.7%	61.2%
わからない	4.5%	4.5%	23.9%	14.9%	3.0%	10.4%	6.0%	10.4%	10.4%	14.9%	1.5%	3.0%	17.9%	13.4%
その他 (n=18)														
はい	0.0%	5.6%	16.7%	11.1%	0.0%	88.9%	0.0%	0.0%	5.6%	0.0%	5.6%	5.6%	5.6%	27.8%
いいえ	83.3%	83.3%	61.1%	66.7%	83.3%	11.1%	88.9%	83.3%	83.3%	77.8%	88.9%	77.8%	50.0%	38.9%
わからない	16.7%	11.1%	22.2%	22.2%	16.7%	0.0%	11.1%	16.7%	11.1%	22.2%	5.6%	16.7%	44.4%	33.3%

図表 3-1-3. 過去 3 年間におけるインシデント・アクシデントの経験【職位別】

（1）院内のサーバがウイルス感染した。
（2）院内の端末（PCやタブレット端末）がウイルス感染した。
（3）従業員が不正なウェブサイトにアクセスした。
（4）従業員がフィッシング（詐欺）サイトにアクセスさせられた。
（5）ホームページが改ざん・乗っ取りされた。
（6）なりすましメール（迷惑メールなど）を受信した。
（7）患者・受診者の情報が漏えいした。
（8）役職員の公とされていない個人情報が漏えいした。
（9）（7）および（8）以外の機密情報が漏えいした。
（10）院内または社内のシステムに不正ログインがあった。
（11）業務用のノートPC・スマートフォン・タブレットの紛失・盗難があった。
（12）USBメモリ等の外部媒体の紛失・盗難があった。
（13）メールの誤送信があった。
（14）FAXの誤送信があった。

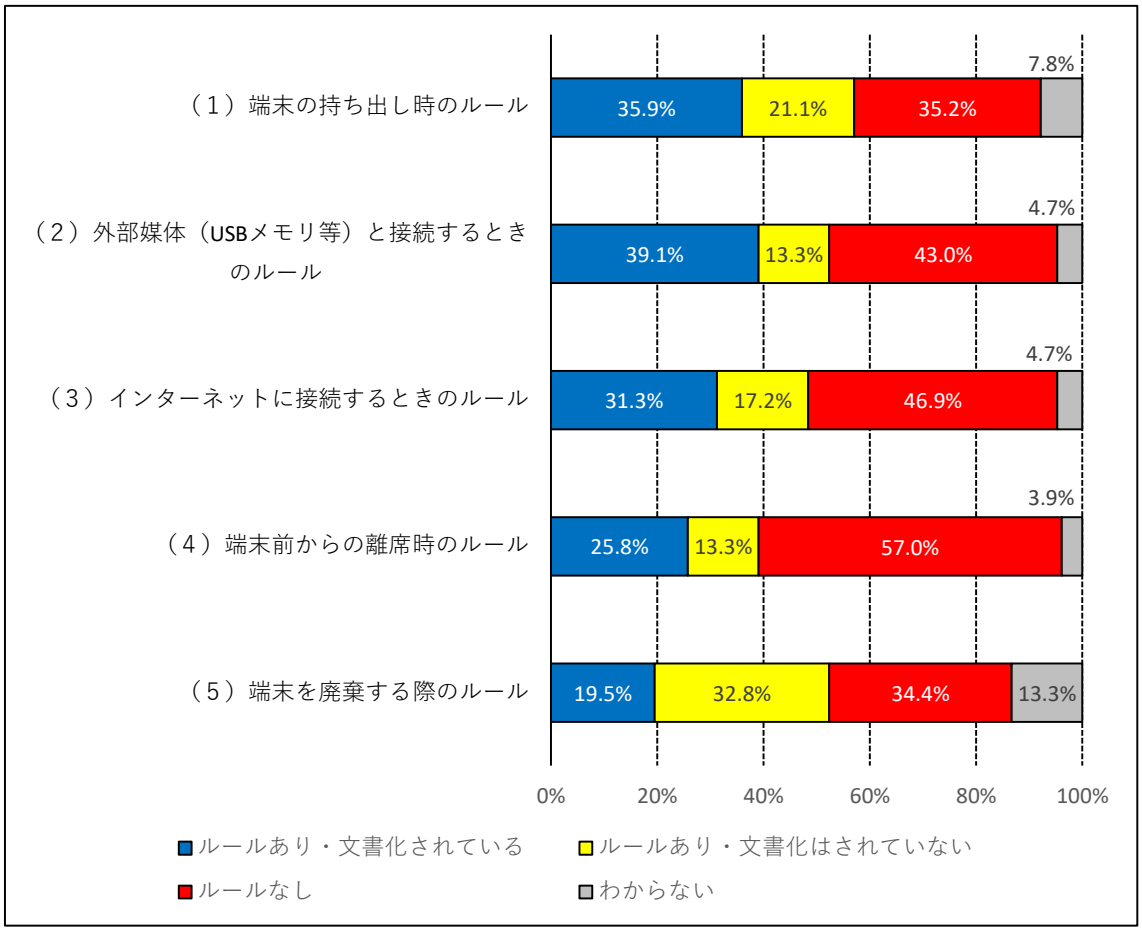
選択肢	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
経営者･役員（n=37）														
はい	0.0%	0.0%	2.7%	0.0%	0.0%	62.2%	0.0%	0.0%	0.0%	2.7%	0.0%	0.0%	10.8%	18.9%
いいえ	97.3%	94.6%	83.8%	89.2%	100.0%	37.8%	97.3%	91.9%	91.9%	78.4%	100.0%	97.3%	81.1%	75.7%
わからない	2.7%	5.4%	13.5%	10.8%	0.0%	0.0%	2.7%	8.1%	8.1%	18.9%	0.0%	2.7%	8.1%	5.4%
経営者･役員以外（n=91）														
はい	1.1%	8.8%	9.9%	4.4%	2.2%	49.5%	0.0%	0.0%	1.1%	1.1%	1.1%	6.6%	12.1%	33.0%
いいえ	90.1%	83.5%	54.9%	67.0%	86.8%	33.0%	90.1%	84.6%	84.6%	78.0%	92.3%	80.2%	53.8%	35.2%
わからない	8.8%	7.7%	35.2%	28.6%	11.0%	17.6%	9.9%	15.4%	14.3%	20.9%	6.6%	13.2%	34.1%	31.9%

3.2. PC 等の情報端末の管理ルール

図表 3-2-1 は、PC 等の情報端末の管理ルールの整備状況を示している。ケースにもよるが、3 割 5 分～5 割強でルールが整備されていない。また、文書化されたルールが整備されているのは、2 割～4 割弱である。

勤務先別クロス集計（図表 3-2-2）を見ると、概ね、病床規模が大きいほどルールが整備されている割合が高いことが分かる。職位別クロス集計（図表 3-2-3）を見ると、経営者・役員以外では 5%強～15%強がルールの整備状況について把握していない。

図表 3-2-1. PC 等の情報端末の管理ルール（n=128）



図表 3-2-2. PC 等の情報端末の管理ルール【勤務先別】

（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）インターネットに接続するときのルール
（4）端末前からの離席時のルール
（5）端末を廃棄する際のルール

選択肢	(1)	(2)	(3)	(4)	(5)
病院 200床以上（n=18）					
ルールあり・文書化されている	66.7%	77.8%	55.6%	55.6%	61.1%
ルールあり・文書化はされていない	16.7%	5.6%	16.7%	16.7%	11.1%
ルールなし	5.6%	5.6%	11.1%	11.1%	5.6%
わからない	11.1%	11.1%	16.7%	16.7%	22.2%
病院200床未満（n=25）					
ルールあり・文書化されている	48.0%	56.0%	40.0%	36.0%	16.0%
ルールあり・文書化はされていない	20.0%	12.0%	20.0%	12.0%	32.0%
ルールなし	24.0%	28.0%	36.0%	48.0%	32.0%
わからない	8.0%	4.0%	4.0%	4.0%	20.0%
診療所（n=67）					
ルールあり・文書化されている	17.9%	17.9%	16.4%	7.5%	3.0%
ルールあり・文書化はされていない	20.9%	16.4%	17.9%	13.4%	37.3%
ルールなし	52.2%	61.2%	62.7%	77.6%	49.3%
わからない	9.0%	4.5%	3.0%	1.5%	10.4%
その他（n=18）					
ルールあり・文書化されている	55.6%	55.6%	50.0%	50.0%	44.4%
ルールあり・文書化はされていない	27.8%	11.1%	11.1%	11.1%	38.9%
ルールなし	16.7%	33.3%	38.9%	38.9%	11.1%
わからない	0.0%	0.0%	0.0%	0.0%	5.6%

図表 3-2-3. PC 等の情報端末の管理ルール【職位別】

（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）インターネットに接続するときのルール
（4）端末前からの離席時のルール
（5）端末を廃棄する際のルール

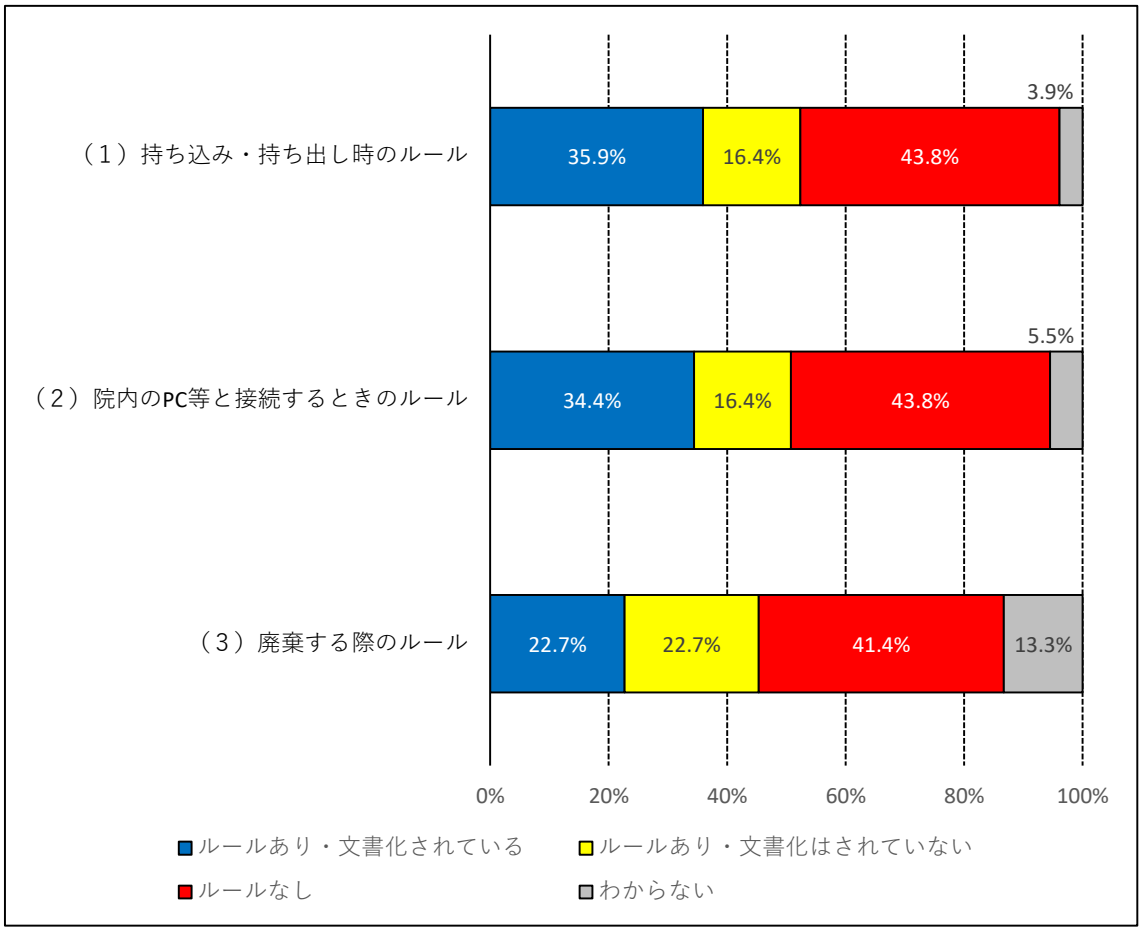
	(1)	(2)	(3)	(4)	(5)
経営者･役員（n=37）					
ルールあり・文書化されている	21.6%	21.6%	16.2%	13.5%	8.1%
ルールあり・文書化はされていない	16.2%	5.4%	16.2%	16.2%	32.4%
ルールなし	59.5%	73.0%	67.6%	70.3%	54.1%
わからない	2.7%	0.0%	0.0%	0.0%	5.4%
経営者･役員以外（n=91）					
ルールあり・文書化されている	41.8%	46.2%	37.4%	30.8%	24.2%
ルールあり・文書化はされていない	23.1%	16.5%	17.6%	12.1%	33.0%
ルールなし	25.3%	30.8%	38.5%	51.6%	26.4%
わからない	9.9%	6.6%	6.6%	5.5%	16.5%

3.3. USB メモリ等の外部媒体の管理ルール

図表 3-3-1 は、USB メモリ等の情報端末の管理ルールの整備状況を示している。ケースにもよるが、4 割強でルールが整備されていない。また、文書化されたルールが整備されているのは、2 割強～35%強である。

勤務先別クロス集計（図表 3-3-2）を見ると、概ね、病床規模が大きいほどルールが整備されている割合が高いことが分かる。職位別クロス集計（図表 3-3-3）を見ると、経営者・役員でも 5%強～1 割弱、経営者・役員以外では 5%強～15%強がルールの整備状況について把握していない。

図表 3-3-1. USB メモリ等の外部媒体の管理ルール（n=128）



図表 3-3-2. USB メモリ等の外部媒体の管理ルール【勤務先別】

	（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
病院 200床以上（n=18）			
ルールあり・文書化されている	72.2%	72.2%	44.4%
ルールあり・文書化はされていない	16.7%	5.6%	16.7%
ルールなし	5.6%	11.1%	16.7%
わからない	5.6%	11.1%	22.2%
病院200床未満（n=25）			
ルールあり・文書化されている	48.0%	48.0%	24.0%
ルールあり・文書化はされていない	12.0%	12.0%	16.0%
ルールなし	28.0%	28.0%	40.0%
わからない	12.0%	12.0%	20.0%
診療所（n=67）			
ルールあり・文書化されている	14.9%	11.9%	9.0%
ルールあり・文書化はされていない	19.4%	22.4%	26.9%
ルールなし	64.2%	64.2%	52.2%
わからない	1.5%	1.5%	11.9%
その他（n=18）			
ルールあり・文書化されている	61.1%	61.1%	50.0%
ルールあり・文書化はされていない	11.1%	11.1%	22.2%
ルールなし	27.8%	22.2%	27.8%
わからない	0.0%	5.6%	0.0%

図表 3-3-3. USB メモリ等の外部媒体の管理ルール【職位別】

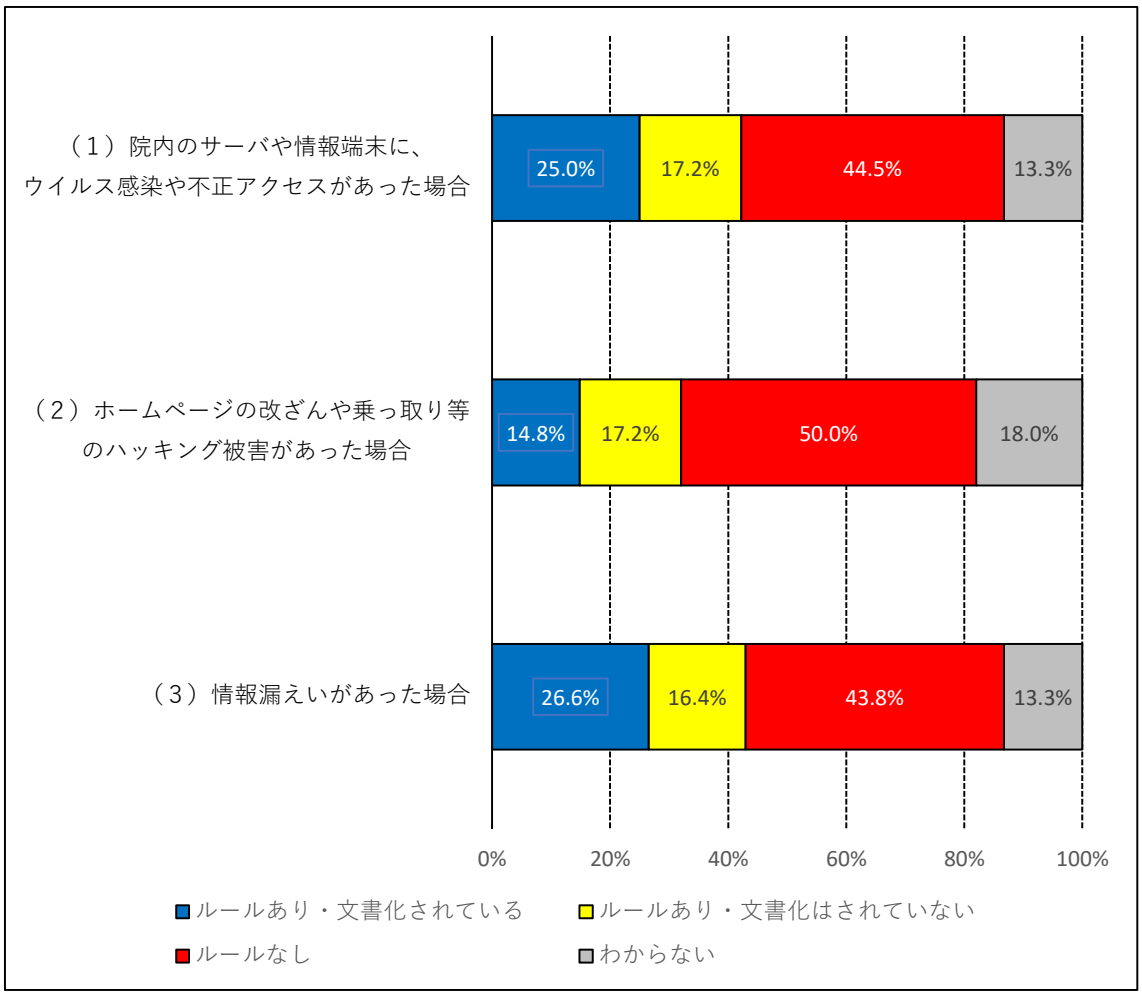
	（1）持ち込み・持ち出し時のルール	（2）院内のPC等と接続するときのルール	（3）廃棄する際のルール
経営者･役員（n=37）			
ルールあり・文書化されている	18.9%	16.2%	10.8%
ルールあり・文書化はされていない	13.5%	10.8%	29.7%
ルールなし	67.6%	73.0%	54.1%
わからない	0.0%	0.0%	5.4%
経営者･役員以外（n=91）			
ルールあり・文書化されている	42.9%	41.8%	27.5%
ルールあり・文書化はされていない	17.6%	18.7%	19.8%
ルールなし	34.1%	31.9%	36.3%
わからない	5.5%	7.7%	16.5%

3.4. サイバーセキュリティ事案発生時の対応手順

図表 3-4-1 は、サイバーセキュリティ事案[7]発生時の対応手順の整備状況を示している。ケースにもよるが、4 割強～5 割でルールが整備されていない。また、文書化されたルールが整備されているのは、15%弱～25%強である。「あり・文書化されている」の場合、ルールを文書化したきっかけを尋ねたが（自由記載）、そこでは、「個人情報保護法法制化」や「Ｐマークや ＩＳＯ等の外部審査の認定」等を契機に文書化ルールを整備したとの回答が多かった。

勤務先別クロス集計（図表 3-4-2）を見ると、概ね、病床規模が大きいほどルールが整備されている割合が高いことが分かる。職位別クロス集計（図表 3-4-3）からは、経営者・役員以外では 15%強～2 割強がルールの整備状況について把握していない。

図表 3-4-1. サイバーセキュリティ事案発生時の対応手順（n=128）



[7] サイバーセキュリティに関わるインシデント・アクシデント等の事案のこと。

図表 3-4-2. サイバーセキュリティ事案発生時の対応手順【勤務先別】

	（1）院内の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）情報漏えいがあった場合
病院 200床以上（n=18）			
ルールあり・文書化されている	55.6%	38.9%	55.6%
ルールあり・文書化はされていない	5.6%	5.6%	5.6%
ルールなし	5.6%	22.2%	11.1%
わからない	33.3%	33.3%	27.8%
病院200床未満（n=25）			
ルールあり・文書化されている	32.0%	8.0%	24.0%
ルールあり・文書化はされていない	12.0%	24.0%	24.0%
ルールなし	40.0%	44.0%	32.0%
わからない	16.0%	24.0%	20.0%
診療所（n=67）			
ルールあり・文書化されている	9.0%	4.5%	13.4%
ルールあり・文書化はされていない	19.4%	17.9%	16.4%
ルールなし	62.7%	67.2%	62.7%
わからない	9.0%	10.4%	7.5%
その他（n=18）			
ルールあり・文書化されている	44.4%	38.9%	50.0%
ルールあり・文書化はされていない	27.8%	16.7%	16.7%
ルールなし	22.2%	22.2%	22.2%
わからない	5.6%	22.2%	11.1%

図表 3-4-3. サイバーセキュリティ事案発生時の対応手順【職位別】

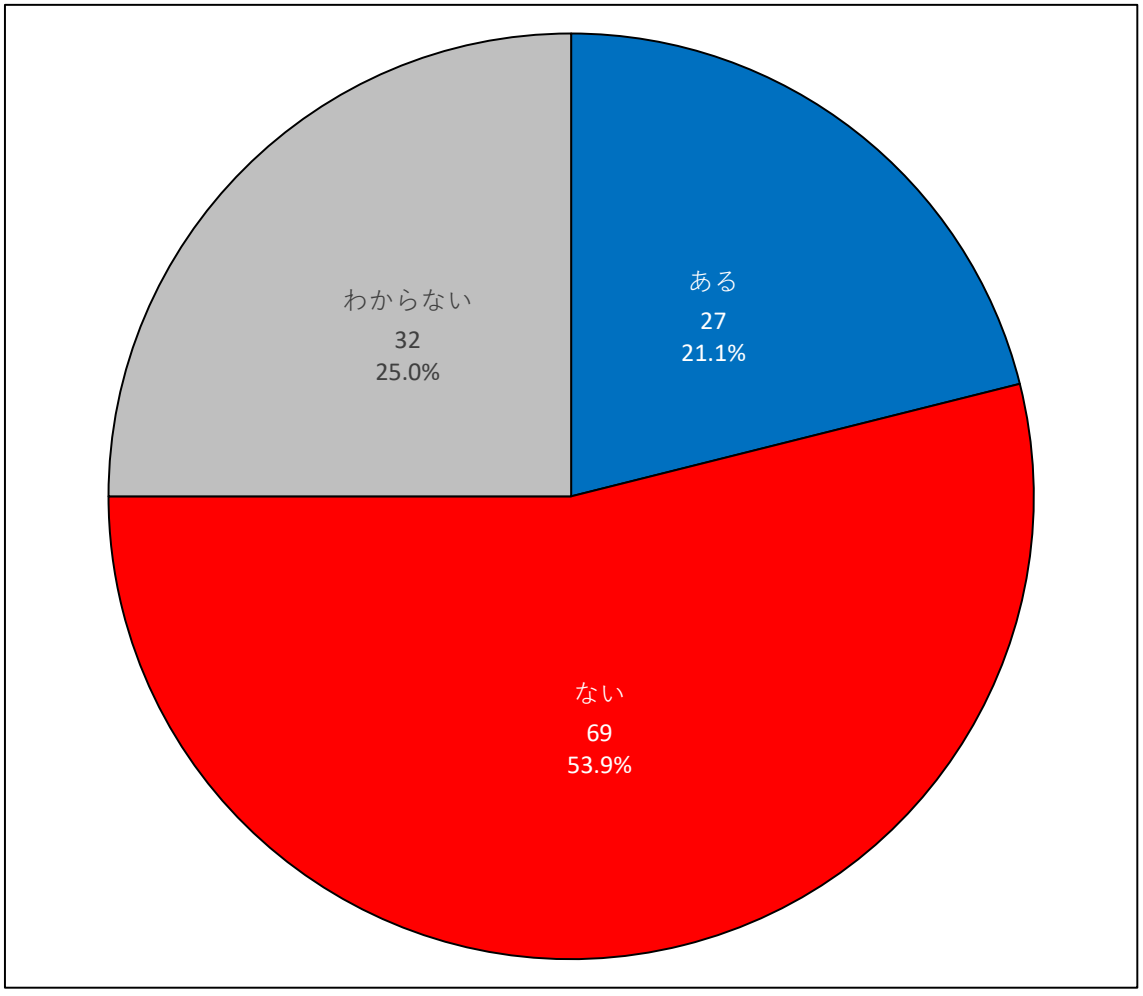
	（1）院内のサーバや情報端末に、ウイルス感染や不正アクセスがあった場合	（2）ホームページの改ざんや乗っ取り等のハッキング被害があった場合	（3）情報漏えいがあった場合
経営者･役員（n=37）			
ルールあり・文書化されている	8.1%	5.4%	10.8%
ルールあり・文書化はされていない	10.8%	8.1%	8.1%
ルールなし	75.7%	78.4%	75.7%
わからない	5.4%	8.1%	5.4%
経営者･役員以外（n=91）			
ルールあり・文書化されている	31.9%	18.7%	33.0%
ルールあり・文書化はされていない	19.8%	20.9%	19.8%
ルールなし	31.9%	38.5%	30.8%
わからない	16.5%	22.0%	16.5%

3.5. サイバーセキュリティ事案への対策予算

図表 3-5-1 は、サイバーセキュリティ事案への対策予算の状況を示している。「ある」が 21.1%、「ない」が 53.9%、「わからない」が 25.0%であった。半数超には対策予算が存在しない。

勤務先別クロス集計（図表 3-5-2）を見ると、病床規模が大きいほど予算がある割合が高いというわけではないと分かる。職位別クロス集計（図表 3-2-3）を見ると、経営者・役員では 1 割強、経営者・役員以外では 3 割強が対策予算について把握していない。

図表 3-5-1. サイバーセキュリティ事案への対策予算（n=128）



図表 3-5-2. サイバーセキュリティ事案への対策予算【勤務先別】

病院 200床以上（n=18）	
ある	16.7%
ない	44.4%
わからない	38.9%
病院200床未満（n=25）	
ある	24.0%
ない	32.0%
わからない	44.0%
診療所（n=67）	
ある	16.4%
ない	68.7%
わからない	14.9%
その他（n=18）	
ある	38.9%
ない	38.9%
わからない	22.2%

図表 3-5-3. サイバーセキュリティ事案への対策予算【職位別】

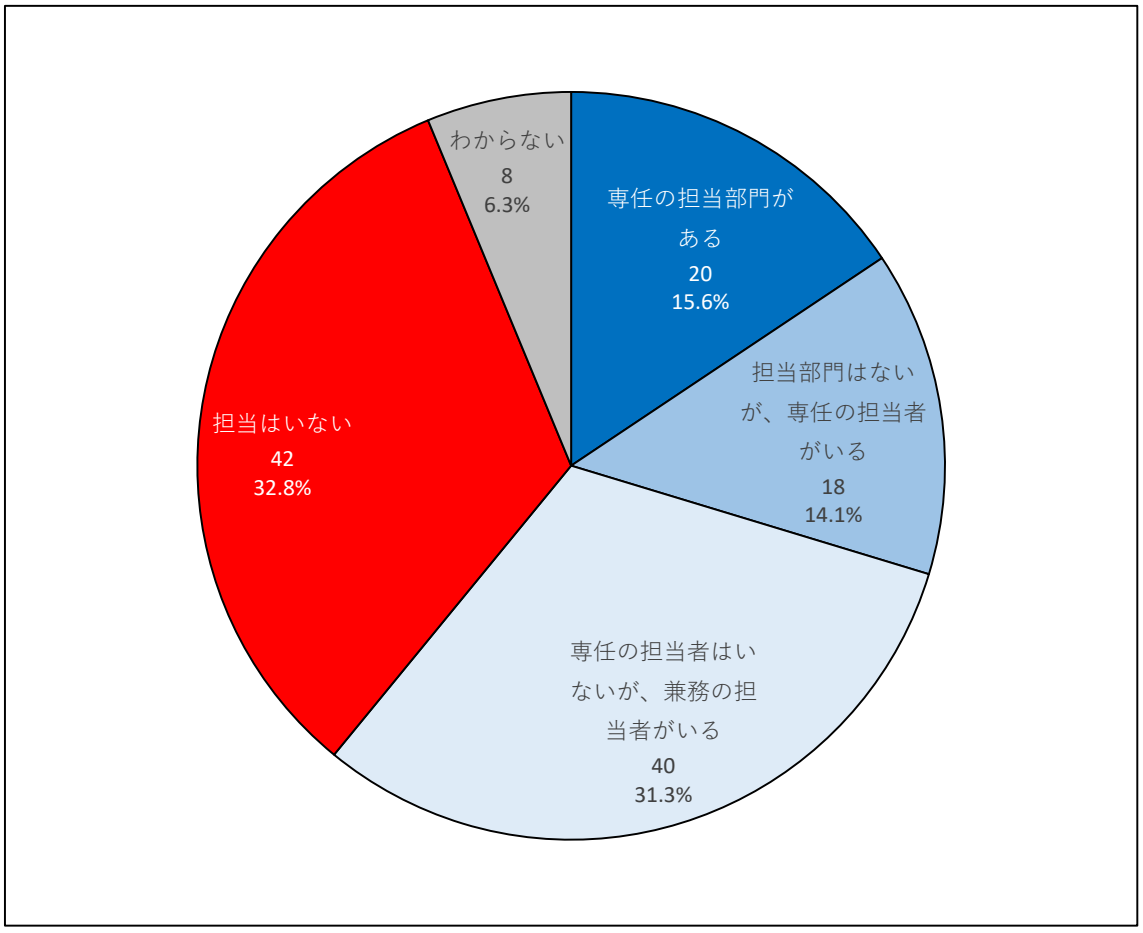
経営者･役員（n=37）	
ある	13.5%
ない	75.7%
わからない	10.8%
経営者･役員以外（n=91）	
ある	24.2%
ない	45.1%
わからない	30.8%

3.6. サイバーセキュリティ対策の組織体制

図表 3-6-1 は、サイバーセキュリティ対策の組織体制の状況を示している。「専任の担当部門がある」が 15.6%、「担当部門はないが、専任の担当者がいる」が 14.1%、「専任の担当者はいないが、兼務の担当者がいる」が 31.3%、「担当はいない」が 32.8%、「わからない」が 6.3%であった。

概ね、病床規模が大きいほど組織体制が整備されている割合が高いことが分かる。職位別クロス集計（図表 3-4-3）を見ると、経営者・役員の 2.7%、経営者・役員以外では 7.7%が組織体制について把握していない。

図表 3-6-1. サイバーセキュリティ対策の組織体制（n=128）



図表 3-4-2. サイバーセキュリティ対策の組織体制【勤務先別】

病院 200床以上（n=18）	
専任の担当部門がある	38.9%
担当部門はないが、専任の担当者がいる	5.6%
専任の担当者はいないが、兼務の担当者がいる	38.9%
担当はいない	11.1%
わからない	5.6%
病院200床未満（n=25）	
専任の担当部門がある	8.0%
担当部門はないが、専任の担当者がいる	28.0%
専任の担当者はいないが、兼務の担当者がいる	36.0%
担当はいない	20.0%
わからない	8.0%
診療所（n=67）	
専任の担当部門がある	7.5%
担当部門はないが、専任の担当者がいる	9.0%
専任の担当者はいないが、兼務の担当者がいる	26.9%
担当はいない	50.7%
わからない	6.0%
その他（n=18）	
専任の担当部門がある	33.3%
担当部門はないが、専任の担当者がいる	22.2%
専任の担当者はいないが、兼務の担当者がいる	33.3%
担当はいない	5.6%
わからない	5.6%

図表 3-4-3. サイバーセキュリティ対策の組織体制【職位別】

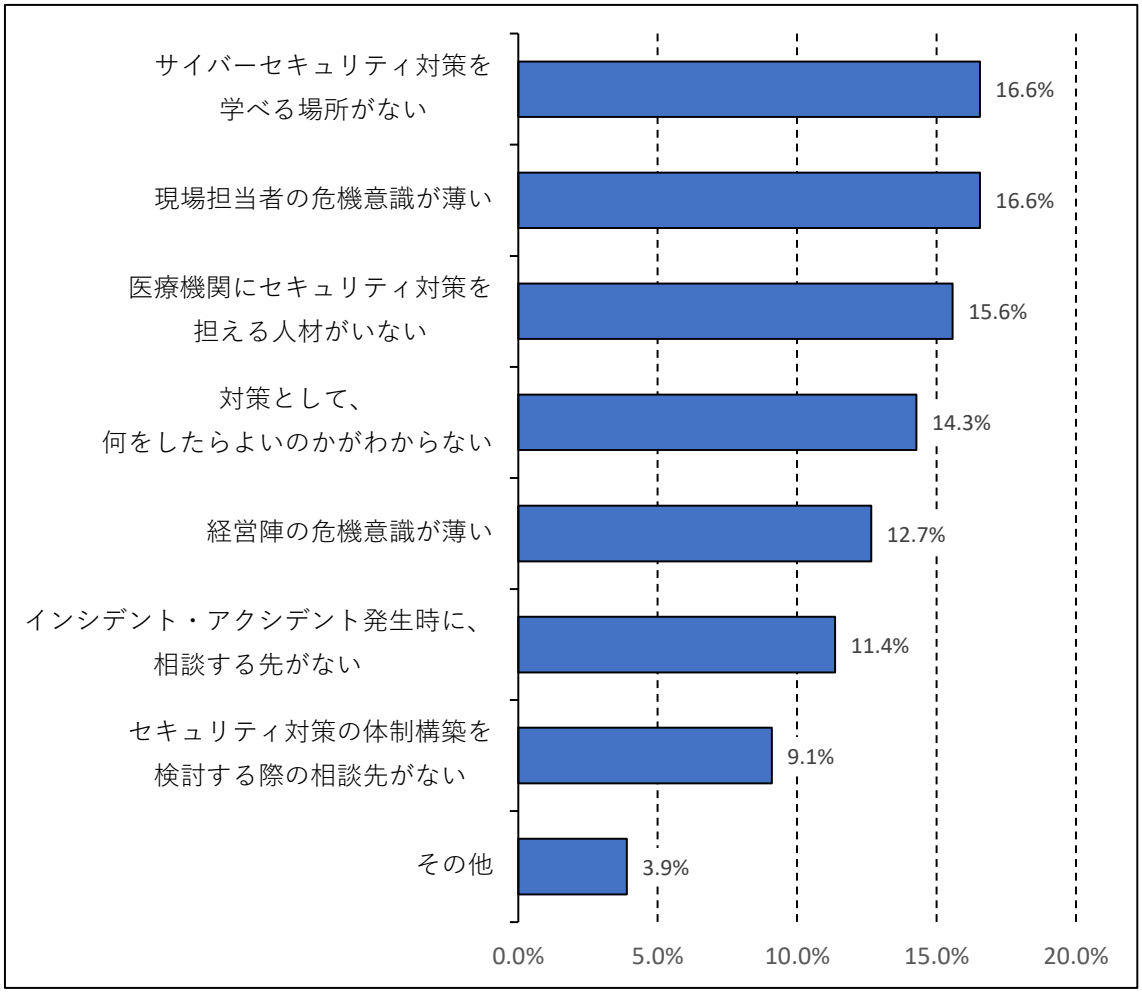
経営者･役員（n=37）	
専任の担当部門がある	2.7%
担当部門はないが、専任の担当者がいる	10.8%
専任の担当者はいないが、兼務の担当者がいる	24.3%
担当はいない	59.5%
わからない	2.7%
経営者･役員以外（n=91）	
専任の担当部門がある	20.9%
担当部門はないが、専任の担当者がいる	15.4%
専任の担当者はいないが、兼務の担当者がいる	34.1%
担当はいない	22.0%
わからない	7.7%

3.7. 対策にあたっての課題と不安

図表 3-7-1 は、サイバーセキュリティ対策にあたっての課題と不安について示している。「対策を学べる場所がない」（16.6%）、「現場担当者の危機意識が薄い」（16.6%）、「医療機関にセキュリティ対策を担える人材がいない」（15.6%）、「対策として、なにをしたらよいのかがわからない」（14.3%）、「経営陣の危機意識が薄い」（12.7%）の順に多かった。セキュリティ対策を担える人材の育成と確保が主たる課題ということである。クロス集計の結果も、概ね同様であった。

その他の回答としては「対策予算や費用面での課題と不安」、「サイバー攻撃の進化への対応など技術面での課題と不安」が挙げられていた。

図表 3-7-1. 対策にあたっての課題と不安（n=128）



図表 3-7-2. 対策にあたっての課題と不安【勤務先別】

病院 200床以上（n=18）	
インシデント・アクシデント発生時に、相談する先がない	8.7%
経営陣の危機意識が薄い	17.4%
現場担当者の危機意識が薄い	17.4%
セキュリティ対策の体制構築を検討する際の相談先がない	8.7%
医療機関にセキュリティ対策を担える人材がいない	13.0%
サイバーセキュリティ対策を学べる場所がない	19.6%
対策として、何をしたらよいのかがわからない	6.5%
その他	8.7%
病院200床未満（n=25）	
インシデント・アクシデント発生時に、相談する先がない	13.6%
経営陣の危機意識が薄い	12.1%
現場担当者の危機意識が薄い	16.7%
セキュリティ対策の体制構築を検討する際の相談先がない	9.1%
医療機関にセキュリティ対策を担える人材がいない	16.7%
サイバーセキュリティ対策を学べる場所がない	19.7%
対策として、何をしたらよいのかがわからない	10.6%
その他	1.5%
診療所（n=67）	
インシデント・アクシデント発生時に、相談する先がない	11.9%
経営陣の危機意識が薄い	10.7%
現場担当者の危機意識が薄い	15.1%
セキュリティ対策の体制構築を検討する際の相談先がない	8.2%
医療機関にセキュリティ対策を担える人材がいない	17.6%
サイバーセキュリティ対策を学べる場所がない	14.5%
対策として、何をしたらよいのかがわからない	18.9%
その他	3.1%
その他（n=18）	
インシデント・アクシデント発生時に、相談する先がない	8.1%
経営陣の危機意識が薄い	16.2%
現場担当者の危機意識が薄い	21.6%
セキュリティ対策の体制構築を検討する際の相談先がない	13.5%
医療機関にセキュリティ対策を担える人材がいない	8.1%
サイバーセキュリティ対策を学べる場所がない	16.2%
対策として、何をしたらよいのかがわからない	10.8%
その他	5.4%

図表 3-7-3. 対策にあたっての課題と不安【職位別】

経営者・役員（n=37）	
インシデント・アクシデント発生時に、相談する先がない	15.9%
経営陣の危機意識が薄い	5.7%
現場担当者の危機意識が薄い	12.5%
セキュリティ対策の体制構築を検討する際の相談先がない	12.5%
医療機関にセキュリティ対策を担える人材がいない	18.2%
サイバーセキュリティ対策を学べる場所がない	12.5%
対策として、何をしたらよいのかがわからない	18.2%
その他	4.5%
経営者・役員以外（n=91）	
インシデント・アクシデント発生時に、相談する先がない	9.5%
経営陣の危機意識が薄い	15.5%
現場担当者の危機意識が薄い	18.2%
セキュリティ対策の体制構築を検討する際の相談先がない	7.7%
医療機関にセキュリティ対策を担える人材がいない	14.5%
サイバーセキュリティ対策を学べる場所がない	18.2%
対策として、何をしたらよいのかがわからない	12.7%
その他	3.6%

4. まとめと考察

第 3 章で示した調査結果について、まず簡潔にまとめておこう。結果の要点は次の通りである。

- 医療分野において最も危惧される「患者・受診者の情報が漏えいした」という事象は、直近 3 年間の経験を問うた今回の調査では確認されなかった。

- 他方で、「なりすましメールを受信」や「FAX・メールの誤送信」、「従業員が不正なウェブサイトにアクセス」、「院内の端末がウイルス感染」等のインシデント・アクシデントがあったことが確認された。医療機関においても、しかるべきサイバーセキュリティ対策が必須なことは言うまでもない。

- サイバーセキュリティ対策にあたっての基本的なルールの整備状況、組織体制の実態、予算確保の状況を見ると、いずれも問題含みである。ルールや組織体制、予算が整備されていないケースが決して少なくない。

- 対策にあたっての課題や不安を問うた結果からは、医療現場のサイバーセキュリティを担える人材の育成と確保が主たる課題であるという認識が浮かび上がった。

昨今の社会的要請や産業界からの期待をみれば[8]、医療分野のさらなる ICT 化は、まったなしの状況にある。今後 ICT 化が進行すれば、サイバーリスクも増大する。医療機関の内外で、医療機器をはじめとする様々な機器を制御するシステム同士が相互に繋がるようになり、事故発生時の影響も増大しやすくなる。すなわち、医療分野の ICT 化の進行にあわせて、医療現場のサイバーセキュリティの強化も必要ということである。

今回の調査を総括して言えることは、医療現場におけるサイバーセキュリティはまだまだ発展途上にある、ということだろう。2018 年に筆者らが実施した

[8] 医療界から見た議論としては、例えば、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
他の産業界から見た議論としては、安宅和人（2017）「“シン・ニホン”AI×データ時代における日本の再生と人材育成」イノベーションを通じた生産性向上に関する研究会, 財務総合政策研究所.
https://www.mof.go.jp/pri/research/conference/fy2017/inv2017_04_02.pdf

医療機関の ICT システム部門が抱える課題についてのアンケート調査があるが[9]、そこで明らかになったのは、ICT 専門部署のある医療機関は少数派、多くは専任者すらおらず、ベンダー任せの姿勢、トラブル発生時の対応体制の不備を含めた事前対策の欠如という実態と人材の確保・育成という課題であった。今回の調査が示唆する医療機関におけるサイバーセキュリティの現状と課題も、おおむね似たようなものと言えるだろう。実際、病院・診療所の ICT 化への対応が他の業界に比べて立ち遅れているとの声が巷間少なくない[10]。今回の調査結果が示唆するのは、同様に、病院・診療所のサイバーセキュリティも、他の業界に比べて立ち遅れているということではないか。

とはいえ、今回の調査はパイロット調査であり、サンプル数も少ない（n=128）。対象を全国の医療機関に拡大した本格的な調査実施を検討するべきと考える。今回の調査結果から導き出される、特に着目すべき仮説は、「医療現場には大きなサイバーリスクが内在するにもかかわらず、医療機関経営にはリスクマネジメントの意識が欠落しているのではないか。あるいは、かかるリスクを認識していながら、医療現場には対策に割ける予算や人員が不足しているのではないか」ということであろう。実際にはサイバーインシデント・アクシデントが既に発生しているにもかかわらず、当医療機関において発見されていないケースがある可能性すら、排除しきれないのが実情ではないだろうか。

図らずも、今回の調査実施と時期を同じくした COVID-19 パンデミックが明らかにしたのは、ナショナルセキュリティ（国家安全保障）におけるインフラとしての医療の重要性であった。国家を支える医療のサイバーセキュリティ確保にあたり、将来の政策立案に資する調査実施を展望したい。

---

[9] 坂口一樹（2018）「医療機関の ICT システム部門が抱える課題：メディカル ICT リーダー養成講座 受講者アンケートから」第 20 回 医療マネジメント学会学術総会（2018 年 6 月 9 日）。発表内容は日医総研ホームページからダウンロード可能にしている【別添資料２】。

[10] しかし、「これまで医療になかなか ＩＴが活用されてこなかったのは機微性が高い医療情報を"守る"ことに力点を置いてきたからである」との見解もある。　日本医師会 IT 委員会（2020）「そもそも医療の IT 化とは何か　―原点から考え、そして未来へつなぐ―」2018・2019 年度 医療 IT 委員会 答申．日本医師会．http://dl.med.or.jp/dl-med/teireikaiken/20200610_2.pdf