日医総研ワーキングペーパー

医師会共同利用施設のサイバーセキュリティ：

医師会病院と健診・検査センター・複合体の実態

No. 501

2026 年 2 月 24 日

日本医師会総合政策研究機構

坂口 一樹

（表紙裏）

医師会共同利用施設のサイバーセキュリティ：
医師会病院と健診・検査センター・複合体の実態調査

坂口一樹（主任研究員）

キーワード
◆ 医師会共同利用施設　◆ サイバーセキュリティ　◆ 医療ＤＸ
◆ 医療情報システム　◆ バックアップ

ポイント

◆全国の医師会共同利用施設（医師会病院計 65 施設と健診・検査センター・複合体 160 施設）のサイバーセキュリティ対策の現状と課題の把握を目的とし、全 225 施設を対象にウェブ・アンケート調査を実施した。

◆計 135 施設から回答、回収率は 60%であった。結果については単純集計・施設種別のクロス集計に加えて、2020 年に日本医師会が全国の医療機関を対象に実施した既往調査の結果と 2025 年に厚生労働省が病院を対象に実施した調査結果と適宜比較し、対策の進捗状況を確認した。

◆直近 3 年間にインシデント・アクシデントはあったものの、患者に被害が及ぶクリティカルな事案はなかった。ウイルス感染（端末の感染 10.9%、サーバの感染 4.3%）事案はあったが、ランサムウェア感染はなかった。

◆対策費用・財源面での問題を除けば、５年前と比べて、サイバーセキュリティに関わる体制・対策の整備は進んでいた。医療現場における対策の進展を示唆する結果である。医師会病院の体制・対策については、2025 年に厚労省が調査した同規模病院の結果と比べても、同等以上の結果だった。

◆他方で、医師会病院に比べると、総じて健診センター・検査センター・複合体の方が、体制・対策の整備がなされていない施設の割合が高かった。今後、医療 DX の進展に伴い、両者がサイバー空間上での結び付きを深めてゆく未来を想定すれば、政策的に手当てすべき課題である。

◆多くの医療施設がサイバーセキュリティ対策の費用・財源の捻出に苦慮している実態が浮かび上がる調査結果であった。施設種別に関わらず 6 割弱が「対策費用の準備なし」と回答。自由記述には費用支援に関する要望が数多く並んだ。セキュリティ対策義務化の一方で、費用の手当ては不十分である。医療現場へのサイバーセキュリティ対策費用は医療 DX の必要経費と捉え、セキュリティシステム導入のイニシャルコストは補助金で、そのランニングコストは診療報酬で賄う制度設計を展望すべきである。

目　次

１．背景と問題意識 1

２．調査概要 3
２．１　目的 3
２．２　対象と方法 3
２．３　回収状況 4

３．調査結果 5
３．１　インシデント・アクシデントの経験 5
３．２　人員と組織 9
（１）情報システムの管理体制 9
（２）業者との保守・メンテナンス契約 10
（３）サイバーセキュリティ教育 11
３．３　ＩＣＴ資産管理 12
（１）ネットワーク構成図の管理 12
（２）情報システムのアカウント管理 13
（３）脆弱性情報の入手経路 14
（４）ＶＰＮの利用と脆弱性への対応 16
３．４　万一への備え 19
（１）　データのバックアップ 19
（２）対策費用 23
（３）保険 24
（４）事業継続計画（ＢＣＰ） 25
３．５　公的な支援の活用や認知状況 26
（１）厚生労働省の施策の活用や認知状況 26
（２）日本医師会の取り組みの活用や認知状況 28
（３）公的な連絡・相談窓口の認知状況 30
（４）今後求められる政策支援 32

４．まとめと考察 33
４．１　直近３年間のインシデント・アクシデント 33
４．２　体制・対策の整備 34
４．３　費用・財源の確保 34

参考文献・資料 36
巻末資料①：調査票 37
巻末資料②：自由記述 38

１．背景と問題意識

昨今、業種・業界を問わず、企業・団体がサイバー攻撃の被害に遭う事件が相次いでいる。2025 年においても、アサヒビールやアスクルといった大企業のシステムがサイバー攻撃に遭い、供給体制が混乱して世間を騒がせた。また国立国会図書館の開発中のシステムが不正アクセスに遭い、利用者や資料等の情報が漏洩した可能性が伝えられている。国立研究開発法人情報通信研究機構（NICT）のダークネット観測によれば、昨今サイバー攻撃に関連する通信量は右肩上がりに増加中である（図表 1.1）。

図表 1.1 サイバー攻撃関連の通信量の年次推移

資料：総務省 「令和６年版　情報通信白書」

サイバー空間での脅威に関して、医療界も例外ではない。2021 年に徳島県のつるぎ町立半田病院、2022 年に大阪急性期・総合医療センターがランサムウェアによるサイバー攻撃の被害に遭った事件は大々的に報道された。2025 年には栃木県宇都宮市のクリニックのランサムウェアの被害が、本稿執筆時点（2026 年 2 月）には日本医大武蔵小杉病院がランサムウェア攻撃に遭った事

件が大きく報道されている最中である。同様の事例は、国内に限らず海外でも続発しており、2024 年 11 月には、WHO が「医療へのサイバー攻撃は無視できないグローバルな脅威である」との警告を発するに至っている[1]。

かかる状況を踏まえて、これまで官民を挙げて、医療機関のサイバーセキュリティ対策とその支援策が取られてきた。医療分野に関して言えば、所管の厚生労働省が主導し、ガイドラインや対策のチェックリスト、従業員教育のためのコンテンツ、被害時の連絡・相談窓口等が整備されてきた。また、日本医師会ではサイバーセキュリティ支援制度を開始し、トラブルや対策の相談窓口、最新の関連情報サイト、被害時の一時金支給などの仕組みを整えている。

医療現場のサイバーセキュリティ対策に関しては、2021 年に日本医師会・医療機器センターの全国調査を基に筆者らが実情と課題をレポートした[2]。また 2025 年には、厚生労働省による病院対象の実態調査結果が報告されている[3]。本稿では、足元の医師会共同利用施設（医師会病院、健診センター、検査センター、健診・検査センター複合体）を対象に直近の状況を調査し、対策の進捗状況と課題を確認した。

[1] UN News (2024)
[2] 坂口、堤（2021）。調査実施は 2020 年である。
[3] 厚生労働省 医政局 医療情報担当参事官室（2025）

２．調査概要

２．１　目的

調査目的は、医師会共同利用施設のサイバーセキュリティ対策の現状と課題の把握である。あわせて、2020 年に日本医師会が全国の医療機関を対象に実施した既往調査の結果と 2025 年に厚生労働省が病院を対象に実施した調査結果と適宜比較し、対策の進捗状況を確認した。

２．２　対象と方法

調査対象は、全国の医師会共同利用施設（医師会病院、健診センター、検査センター、健診・検査センター複合体）合計 225 施設である。詳しくは図表 2.2.1 に示した通りである。

2.2.1 調査対象

	合計	医師会病院	医師会病院以外		
			健診センター	検査センター	健診･検査複合体
対象施設数	225	65	64	49	47

調査方法は、ウェブ・アンケート調査である。ネット上に構築したアンケート調査システムへのアクセス案内と協力依頼文書を対象施設に送り、ネット経由で回答してもらった（ウェブ調査票は巻末資料を参照)。実施期間は 2025 年 8 月～10 月である。

２．３　回収状況

全体の回収率は 60.0%であった。対象施設の属性別の詳細な回収状況を図表 2.3.2 に示しておく。医師会病院の回収数は 37、医師会病院以外（健診センター、検査センター、健診・検査センター複合体）の回収数は 98 であった。

2.3.2 回収状況

	合計	医師会病院	医師会病院以外			
			合計	健診センター	検査センター	健診・検査複合体
対象施設数	225	65	160	64	49	47
合計　回答数	135	37	98	38	27	33
回収率	60.0%	56.9%	61.3%	59.4%	55.1%	70.2%

次章以降では、回答施設を「医師会病院」と「健診センター、検査センター、健診・検査センター複合体」（「健セ・検セ・複合体」と表記）の２つに区分けし施設種類別のクロス集計分析を行っている。

３．調査結果

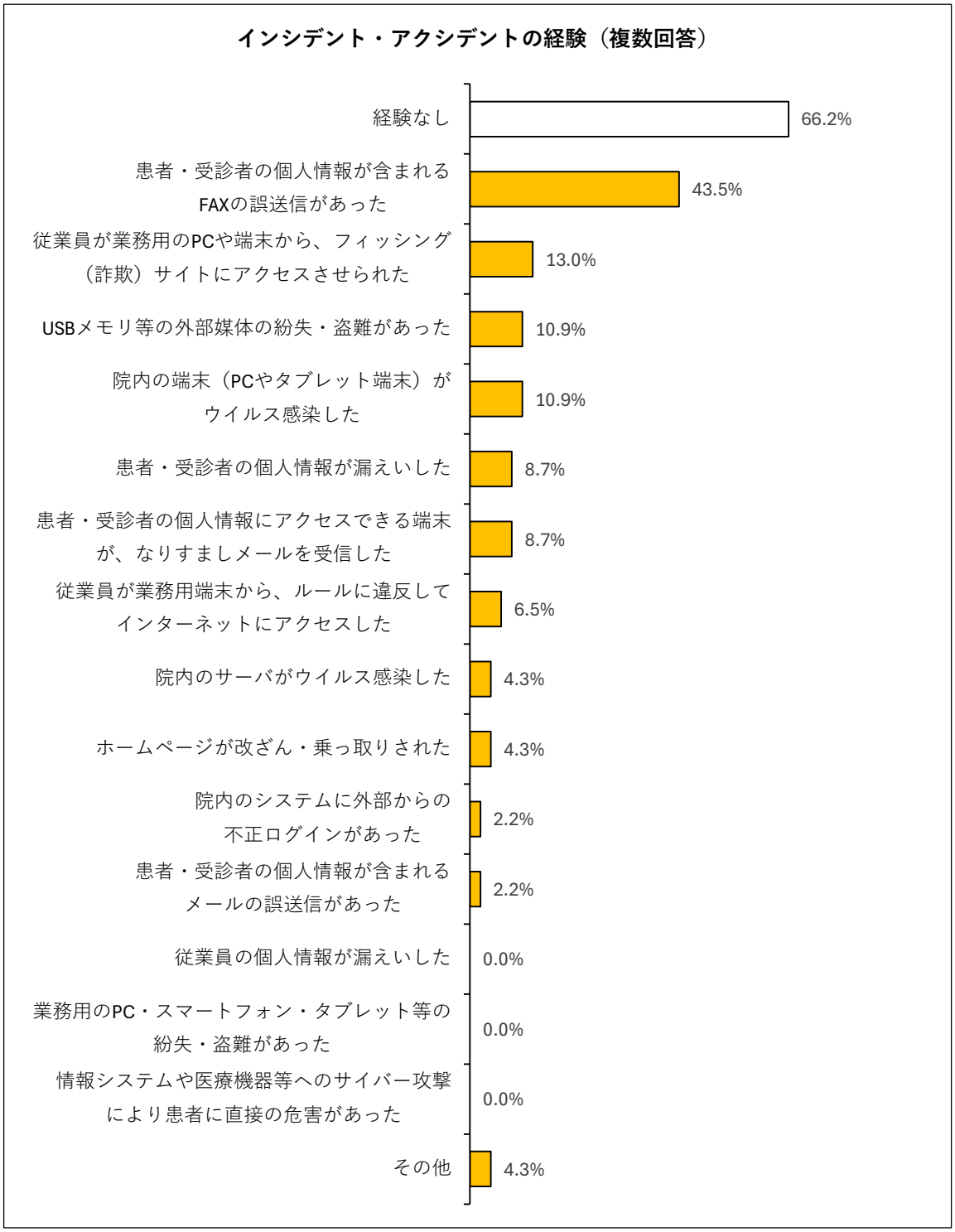
３．１　インシデント・アクシデントの経験

図表 3.1.1 は、直近 3 年間における回答施設の情報セキュリティに関わるインシデント・アクシデントの経験について示している。

回答施設全体では「経験なし」が 66.2%であった。また、最も危惧される「サイバー攻撃により患者・受診者に直接の危害があった」との事案は発生していなかった。

インシデント・アクシデントの内容では「患者・受診者の個人情報が含まれる FAX の誤送信」（43.5%）の経験割合が最も高く、次いで「フィッシング（詐欺）サイトにアクセス」（13.0%）、「外部媒体の紛失・盗難」（10.9%）、「端末のウイルス感染」（10.9%）等の事案が続いた。なお、ウイルス感染（端末の感染 10.9%、サーバの感染 4.3%）の事案はあったものの、ランサムウェアへの感染は発生していなかった。

図表 3.1.1 インシデント・アクシデントの経験

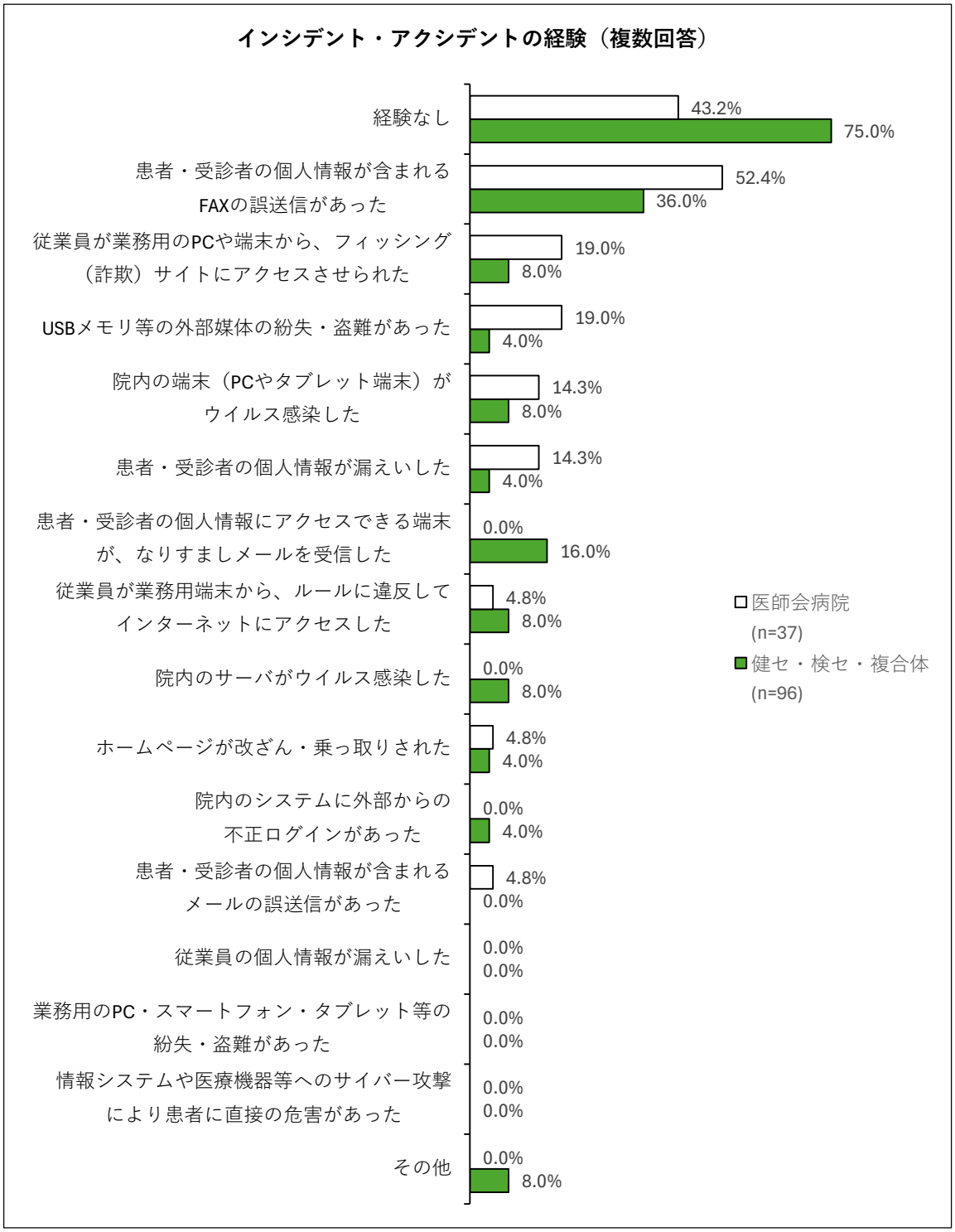


図表 3.1.2 は、同じく直近 3 年間における回答施設の情報セキュリティに関わるインシデント・アクシデントの経験について、施設種類別にクロス集計した結果を示している。

施設種類別に見ると、医師会病院では「患者・受診者の個人情報が含まれる FAX の誤送信」（52.4%）の経験割合が高く、「経験なし」（43.2%）の割合を上回る。次いで「フィッシング（詐欺）サイトにアクセス」（19.0%）、「外部媒体の紛失・盗難」（19.0%）「端末がウイルス感染」（14.3%）、「患者・受診者の個人情報が漏洩」（14.3%）の割合が高かった。

健セ・検セ・複合体では、「経験なし」（75.0%）と医師会病院に比べて高かった。インシデント・アクシデントの内容では「患者・受診者の個人情報が含まれる FAX の誤送信」（36.0%）の経験割合が最も高く、次いで「患者・受診者情報にアクセスできる端末がなりすましメールを受信」（16.0%）との結果であった。

図表 3.1.2 インシデント・アクシデントの経験（施設種類別）



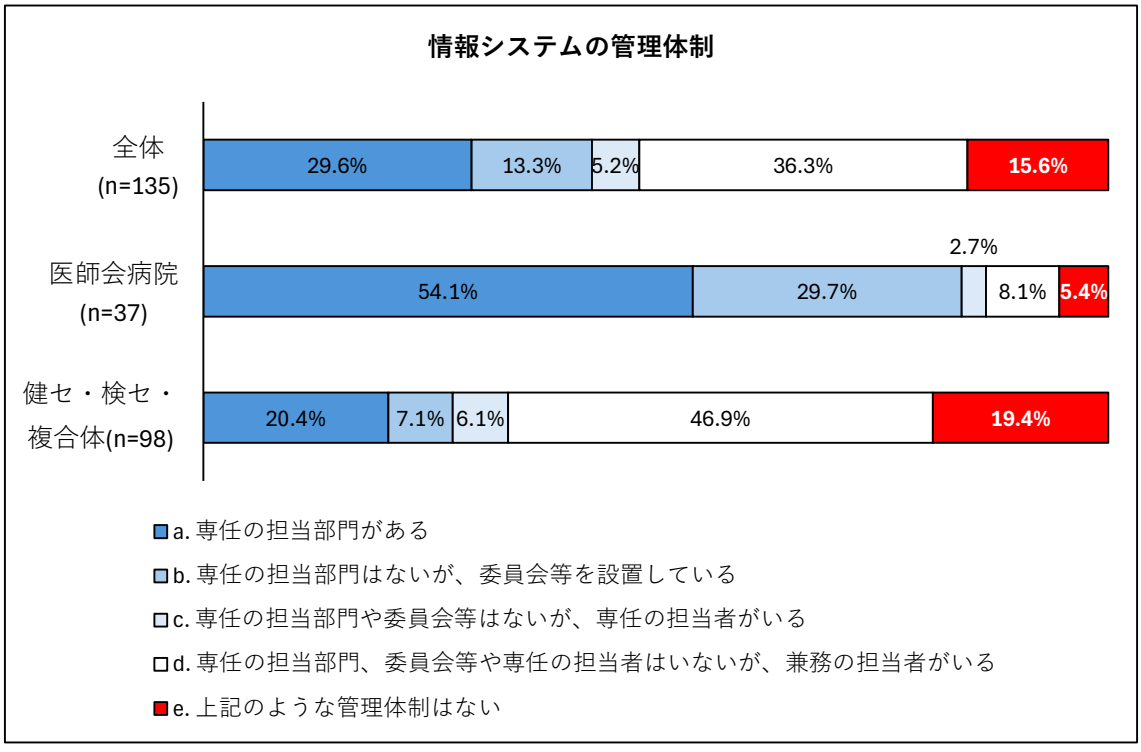
３．２　人員と組織

（１）情報システムの管理体制

図表 3.2.1 は、情報システムの管理体制について、回答者全体および対象施設別にクロス集計した結果を示している。施設種類別にみると、医師会病院の方が組織的な管理体制が整備されている割合が高い。

5 年前と比べて体制整備が進んだことが伺える。2020 年の既往調査では、全医療機関（n=2.989）の 31.6%、病院 200 床未満（n=979）の 5.4%が「管理体制なし」であった。また「専任の担当部門あり」の病院 200 床未満（n=979）は 20.5%であった。

図表 3.2.1 情報システムの管理体制

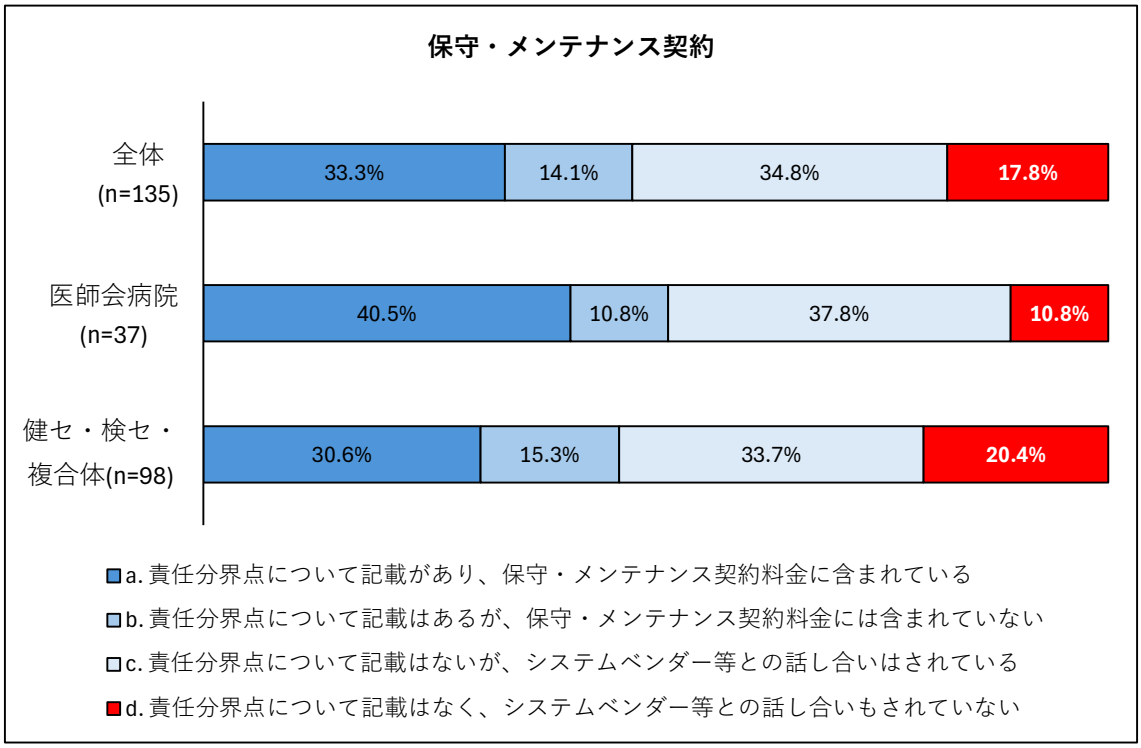


（２）業者との保守・メンテナンス契約

図表 3.2.2 は、保守・メンテナンス契約の状況について、回答者全体および対象施設別にクロス集計した結果を示している。施設種類別にみると、医師会病院の方が契約でベンダーとの責任分界点を定めている割合が高い。

医師会病院がベンダーとの責任分界点を定めている割合は、2025 年の厚労省調査の結果と同等程度である。厚労省調査では、病院 200 床未満（n=4,800）の 48～50%が、病院とベンダーとの責任分界点（役割分担）を定めていた。

図表 3.2.2 保守・メンテナンス契約

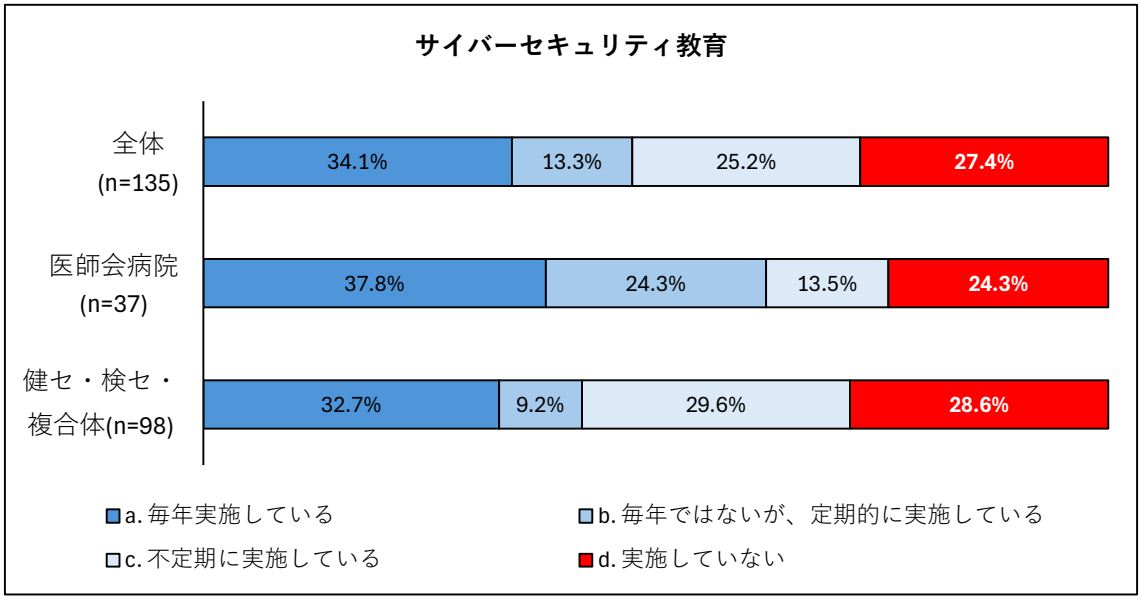


（３）サイバーセキュリティ教育

図表 3.2.3 は、従業員へのサイバーセキュリティ教育の実施状況について、回答者全体および対象施設別にクロス集計した結果を示している。施設種類別にみると、医師会病院の方が頻回に実施している割合が高い。

5 年前と比べて従業員へのサイバーセキュリティ教育の実施は大きく進んだことが伺える。2020 年の既往調査では、全医療機関の 75.1%、病院 200 床未満の 70.0%が「サイバーセキュリティ教育を実施していない」との結果だった。

図表 3.2.3 サイバーセキュリティ教育の実施状況



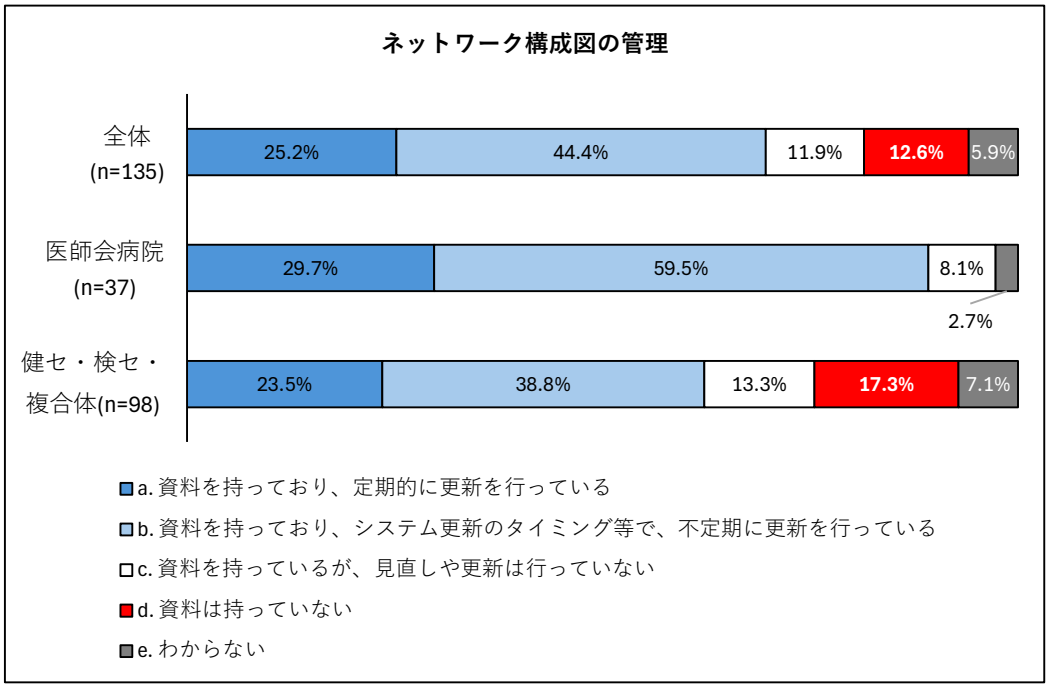
３．３　ＩＣＴ資産管理

（１）ネットワーク構成図の管理

図表 3.3.1 は、ネットワーク構成図の管理について、回答者全体および対象施設別にクロス集計した結果を示している。施設種類別にみると、医師会病院の方がより適切な管理体制がなされている割合が高い。

5 年前と比べると管理体制の整備が進んだことが伺える。2020 年の既往調査では、全医療機関の 49.2%、病院 200 床未満の 40.8%が「ネットワーク構成図を持っていない」との結果だった。また、医師会病院の管理体制は 2025 年の厚労省調査の結果と同等程度である[4]。

図表 3.3.1 ネットワーク構成図の管理

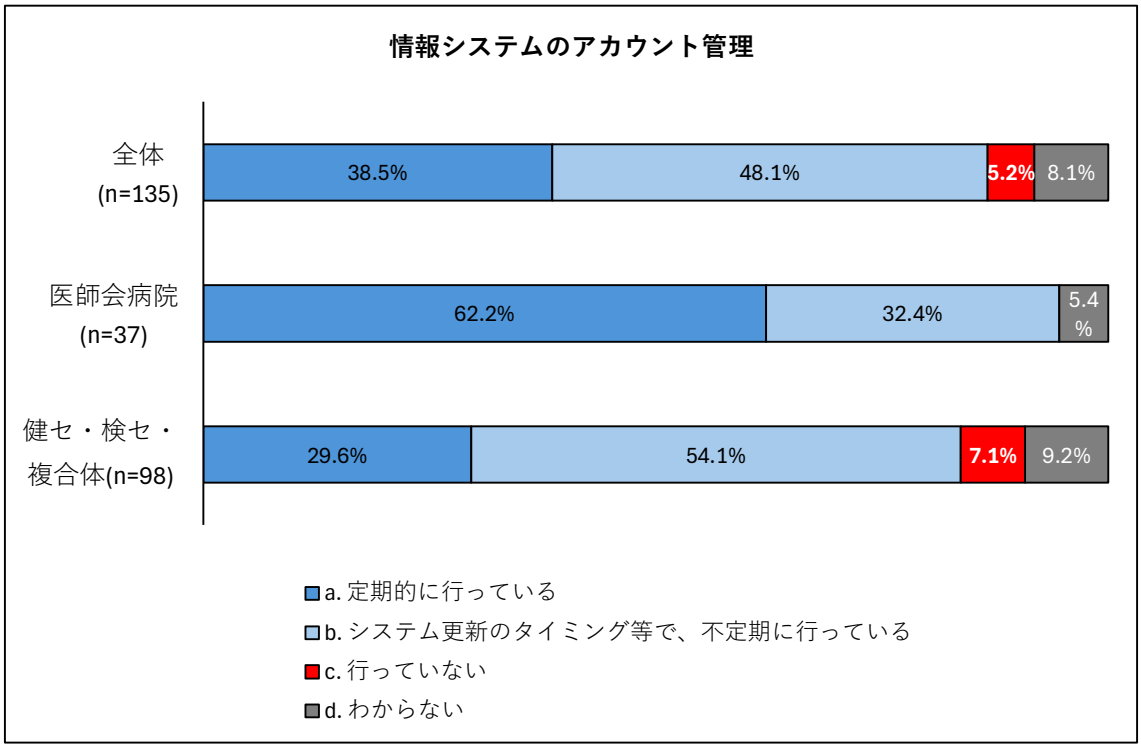


[4] 厚労省調査では、病院 200 床未満の 83～91%が「システムの台帳管理を行っている」だった。

（２）情報システムのアカウント管理

図表 3.2.2 は、情報システムのアカウント管理について、回答者全体および対象施設別にクロス集計した結果を示している。施設種類別にみると、医師会病院の方がより適切な管理がなされている割合が高い。

図表 3.2.2 情報システムのアカウント管理



（３）脆弱性情報の入手経路

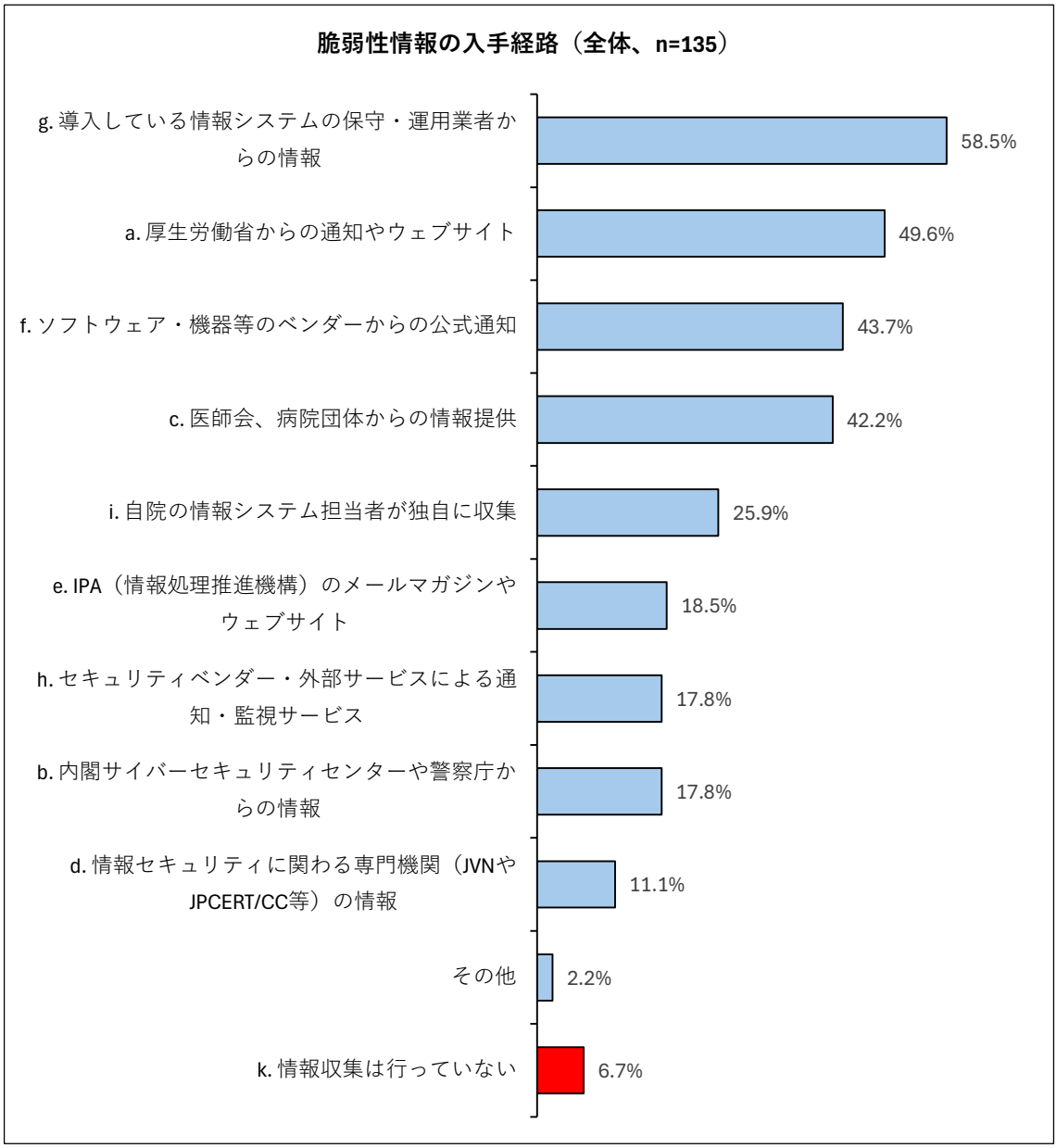
図表 3.3.3 は、情報システム・機器に関わる脆弱性情報の入手経路について、回答者全体に複数回答可で尋ねた結果を示している。

最も割合が高かった入手経路は「導入システムの保守・運用業者から」（58.5%）であり、次いで「厚生労働省の通知やウェブサイト」（49.6%）、「ベンダーからの公式通知」（43.7%）、「医師会・病院団体からの情報提供」（42.2%）等が主な入手経路であった。

他方、「情報収集は行っていない」との回答が 6.7%だった。

なお、「脆弱性情報の収集を行っていない割合」で比較すると、医師会共同利用施設の方が 2025 年の厚労省調査の結果よりも低く、病院一般よりも情報収集に努めていることが伺える。厚労省調査では、病院 200 床未満の 17～23%が脆弱性情報の収集を行っていなかった。

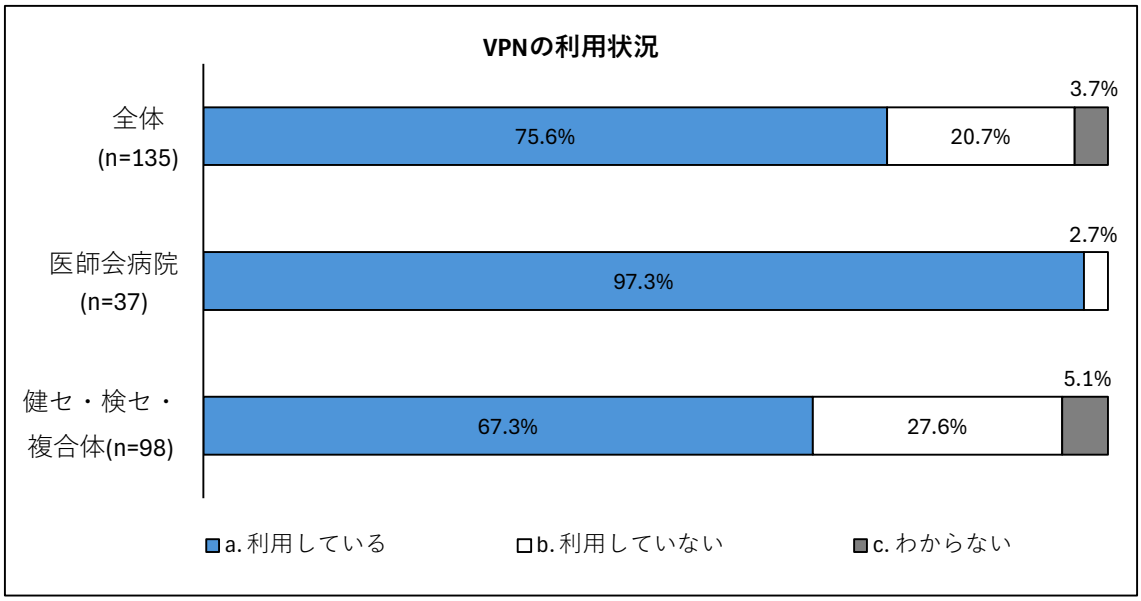
図表 3.3.3 脆弱性情報の入手経路



（４）ＶＰＮの利用と脆弱性への対応

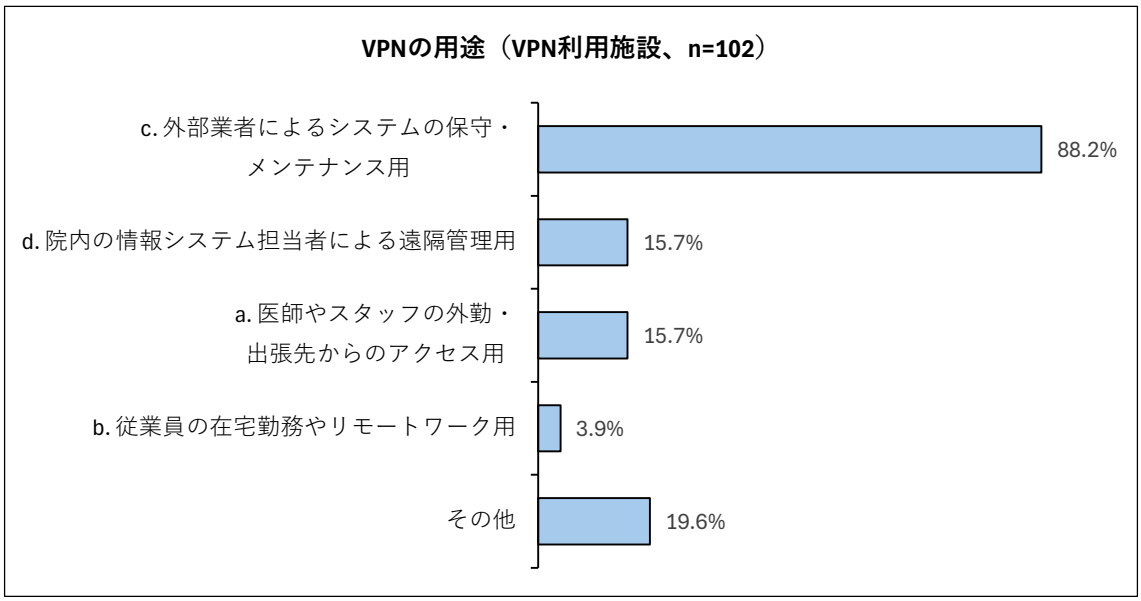
図表 3.3.4.1 は、VPN の利用状況について、回答者全体および対象施設別にクロス集計した結果を示している。施設種類別にみると、医師会病院の方がより VPN の割合が高く、ほぼ全病院（97.3%）が VPN を利用している。

図表 3.3.4.1 VPN の利用状況



図表 3.3.4.2 は、VPN 利用施設を対象とし、その用途を複数回答で尋ねた結果を示している。「外部業者によるシステムの保守・メンテナンス用」（88.2%）が主たる用途であった。

図表 3.3.4.2 VPN の用途

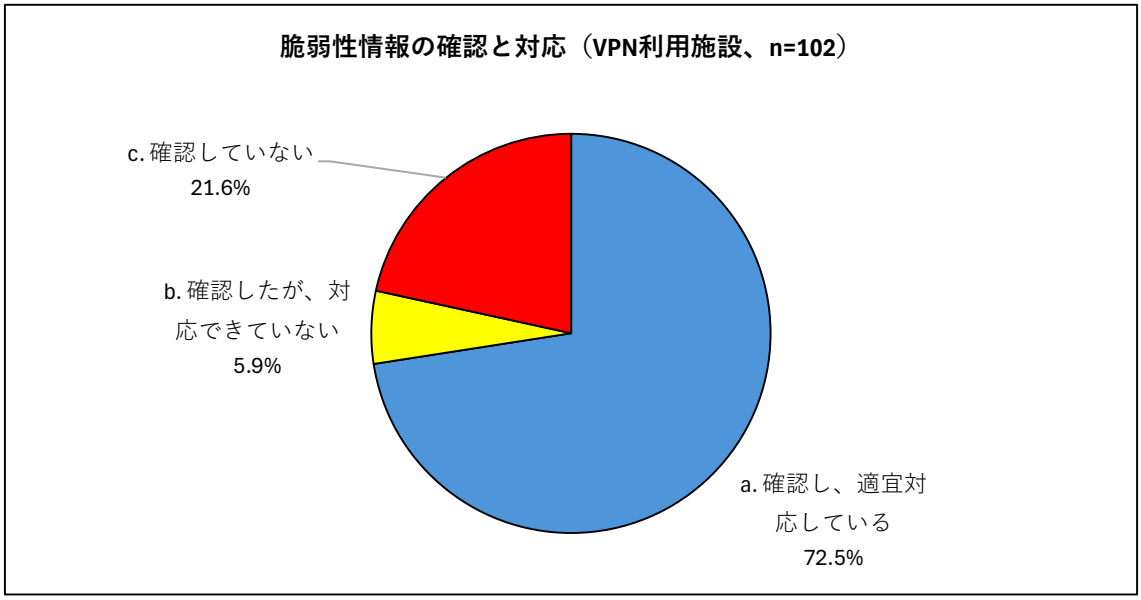


＊その他：医用画像・結果データ等の送受信、地域連携等の外部システムとの連携、拠点間 VPN 等

図表 3.3.4.3 は、VPN 利用施設を対象に、VPN 機器の脆弱性情報の確認と対応状況を示している。「確認し、適宜対応している」が 72.5%、「確認したが対応できていない」が 5.9%、「確認していない」が 21.6%であった。

VPN 機器の脆弱性情報の確認・対応の状況は、2025 年の厚労省調査の結果と同等程度である。厚労省調査では、病院 200 床未満の 74%が「ネットワーク機器へセキュリティパッチを適用している」との回答であった。

図表 3.3.4.3 VPN 機器の脆弱性情報の確認と対応



３．４　万一への備え

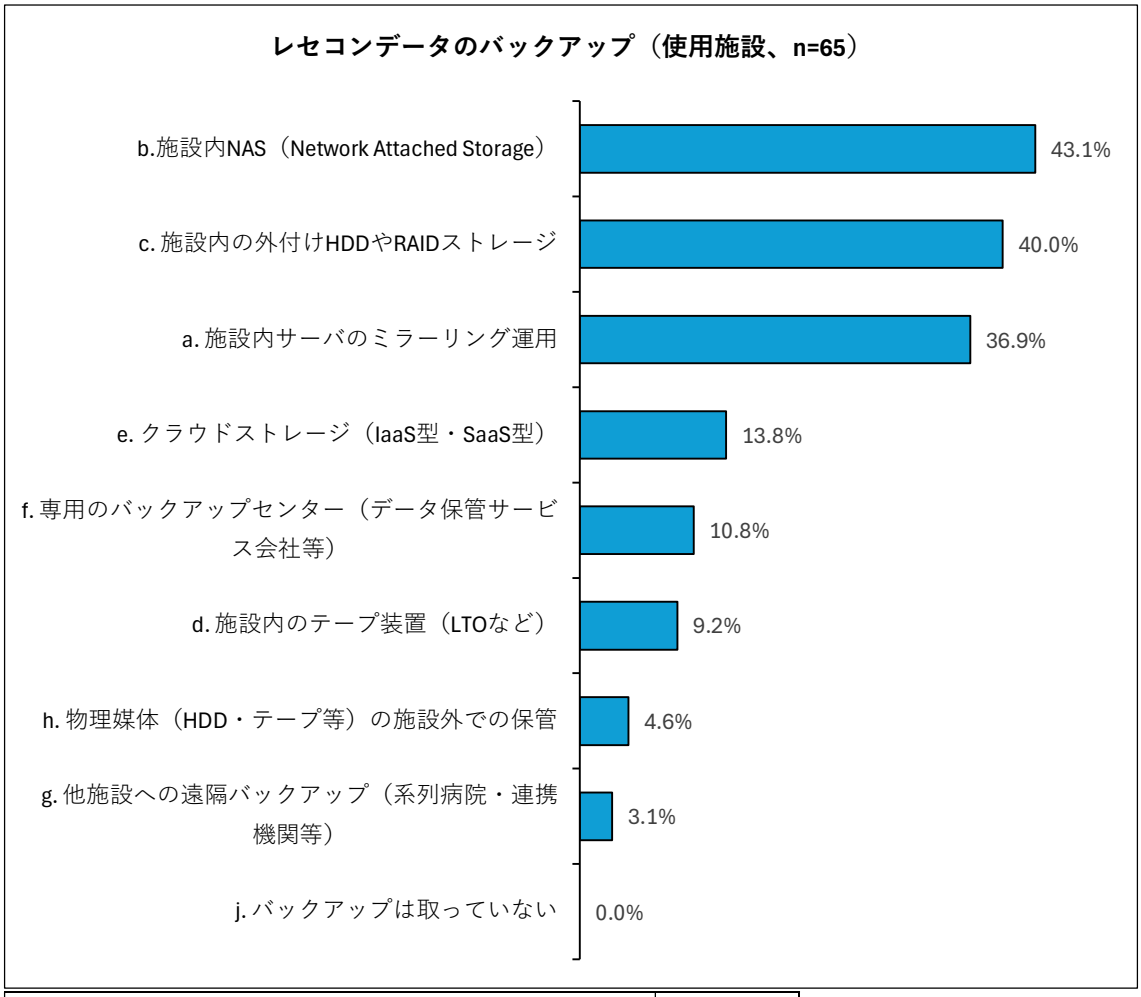
（１）データのバックアップ

図表 3.4.1.1～3.4.1.3 の 3 つは、レセコン、電子カルテ、医用画像のデータのバックアップ状況について、使用施設に複数回答で尋ねた結果について、それぞれ示している。あわせて、複数媒体のバックアップデータを取っている施設の割合とオフライン・オンラインの両方のバックアップを取っている施設の割合をグラフの下に示している。

電子カルテに関して複数のバックアップを取っている割合は、2025 年の厚労省調査における病院の結果と同程度である。厚労省調査では、病院 200 床未満の 48～57%が複数媒体のバックアップ、60～61%がオフラインバックアップを確保しているとの結果であった[5]。

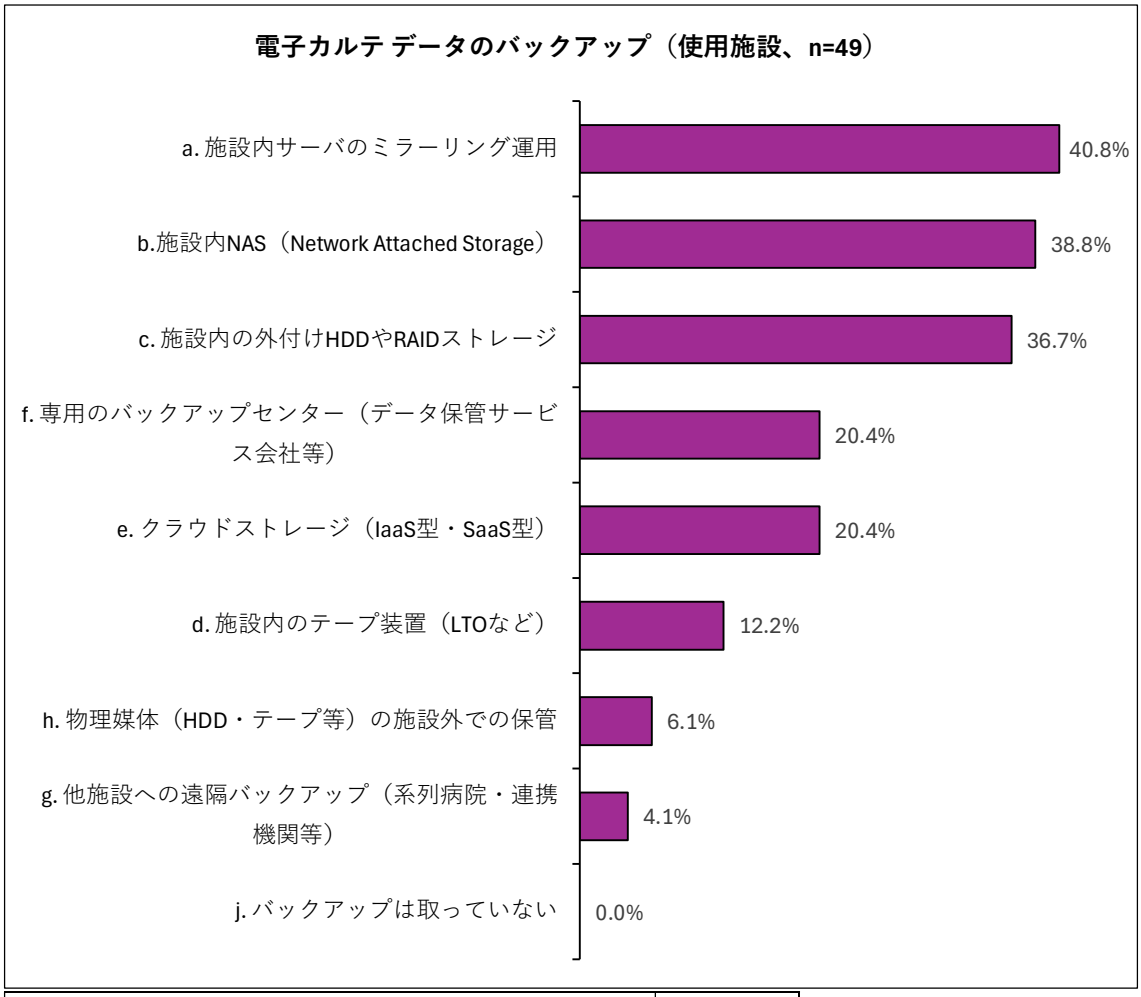
[5] 厚労省資料では、オフラインとオンラインの両方のバックアップを取っている施設の割合は明らかになっていない。

図表 3.4.1.1 レセコンデータのバックアップ



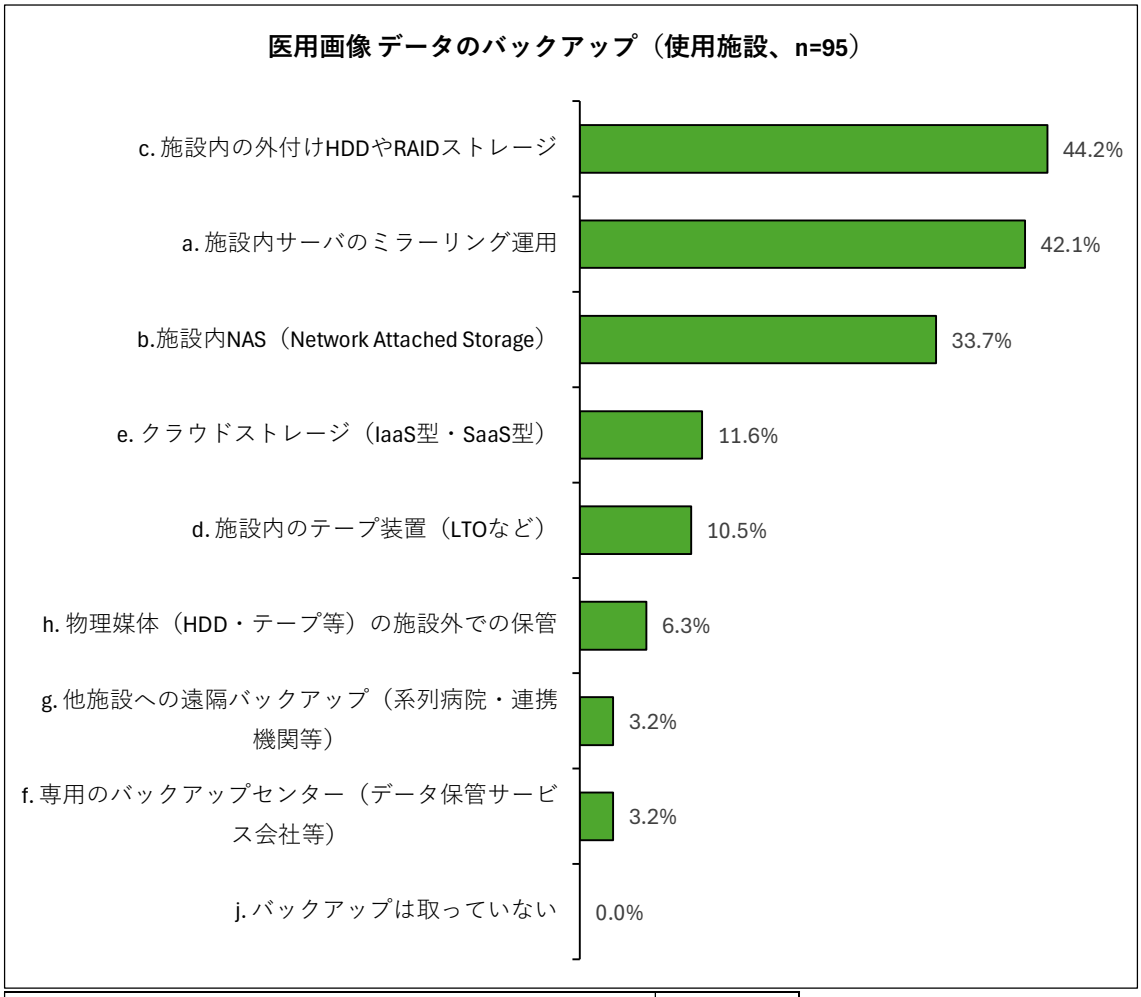
複数媒体のバックアップ	43.1%
オンライン・オフライン両方バックアップ	18.5%

図表 3.4.1.2 電子カルテ データのバックアップ



複数媒体のバックアップ	57.1%
オンライン・オフライン両方バックアップ	30.6%

図表 3.4.1.3 医用画像 データのバックアップ



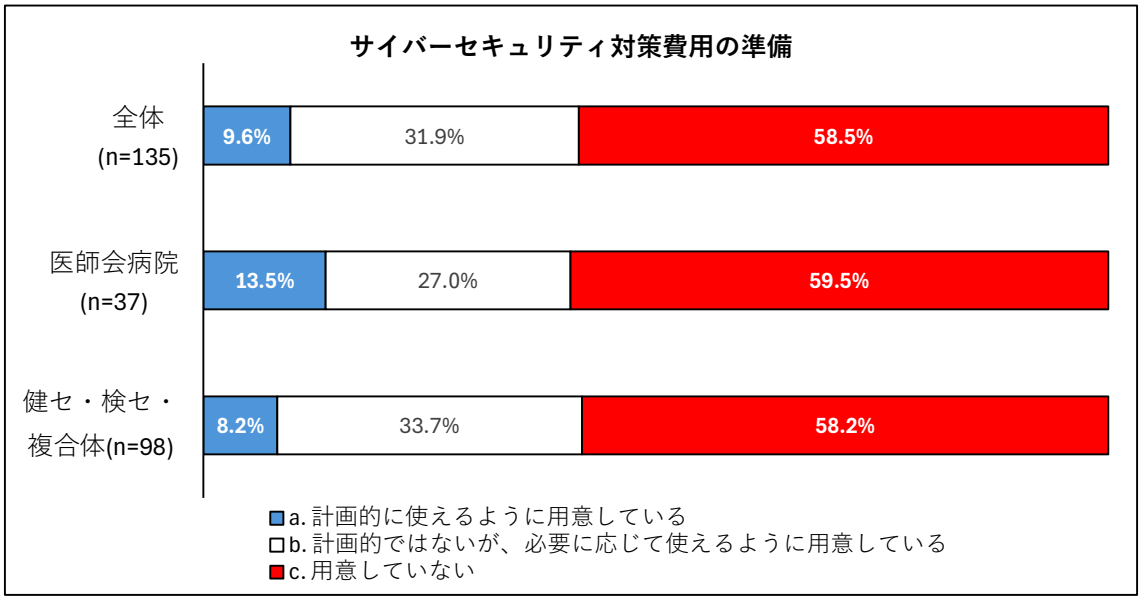
複数媒体のバックアップ	42.1%
オンライン・オフライン両方バックアップ	9.5%

（２）対策費用

図表 3.4.2 は、サイバーセキュリティ対策費用の準備状況について、回答者全体および対象施設別にクロス集計した結果を示している。施設種類別にみると、費用の準備割合自体は同程度であるが、計画的に準備している割合は医師会病院の方がやや高い。

5 年前に比べて、対策費用を準備していない施設の割合が増えており、財源の捻出に苦慮している現況が伺える。2020 年の既往調査では、全医療機関の 48.1%、病院 200 床未満の 42.5%が「対策費用の準備なし」との回答だった。

図表 3.4.2 サイバーセキュリティ対策費用の準備

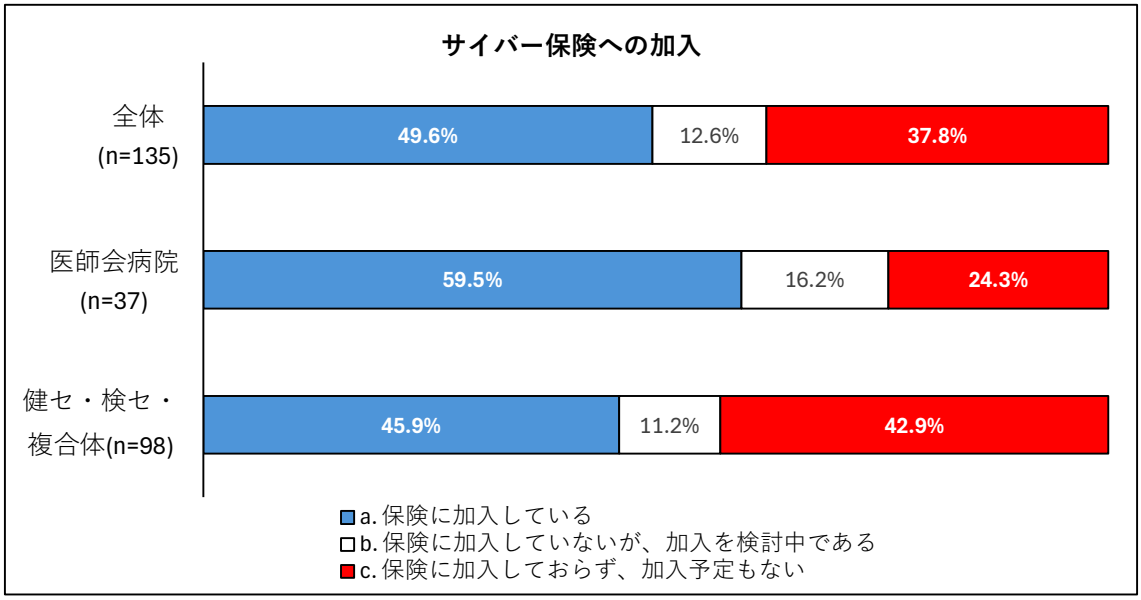


（３）保険

図表 3.4.3 は、サイバー保険への加入状況について、回答者全体および対象施設別にクロス集計した結果を示している。施設種類別にみると、医師会病院の方がサイバー保険への加入割合が高い。

5 年前に比べて、サイバー保険への加入が大きく進んでいる。2020 年の既往調査でサイバー保険に加入している施設の割合は、全医療機関の 8.9%、病院 200 床未満の 7.7%であった。

図表 3.4.3 サイバー保険への加入

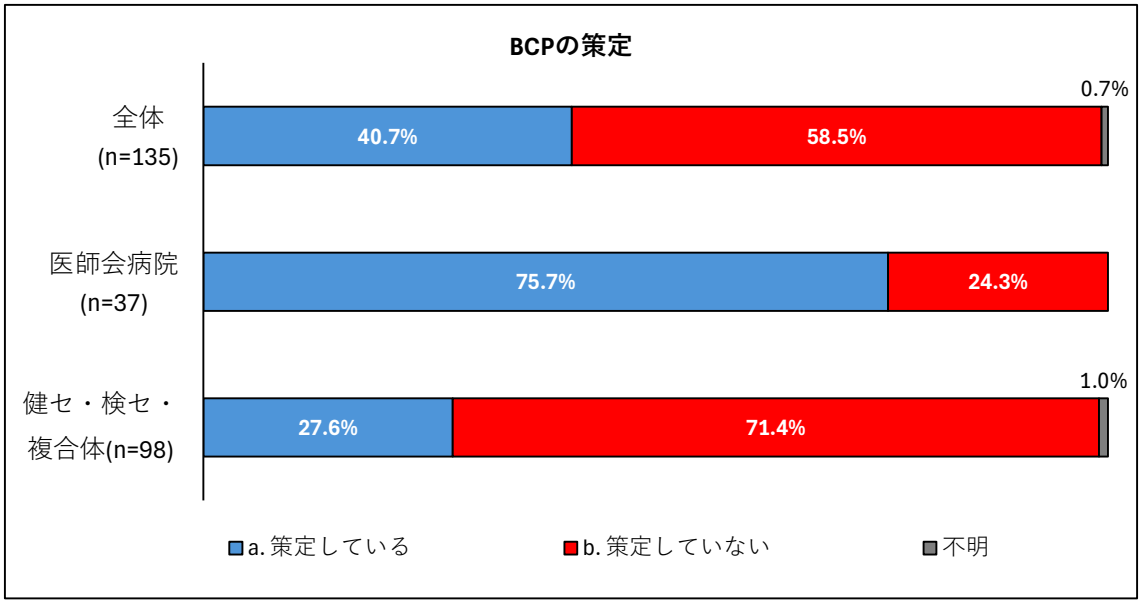


（４）事業継続計画（ＢＣＰ）

図表 3.4.4 は、BCP の策定状況について、回答者全体および対象施設別にクロス集計した結果を示している。施設種類別にみると、医師会病院の方が BCP を策定している割合が高い。

医師会病院が BCP を策定している割合は、2025 年の厚労省調査における病院の結果よりも高い。厚労省調査では、病院 200 床未満の 51～54%が BCP を策定しているとの回答結果だった。

図表 3.4.4 BCP の策定



３．５　公的な支援の活用や認知状況

（１）厚生労働省の施策の活用や認知状況

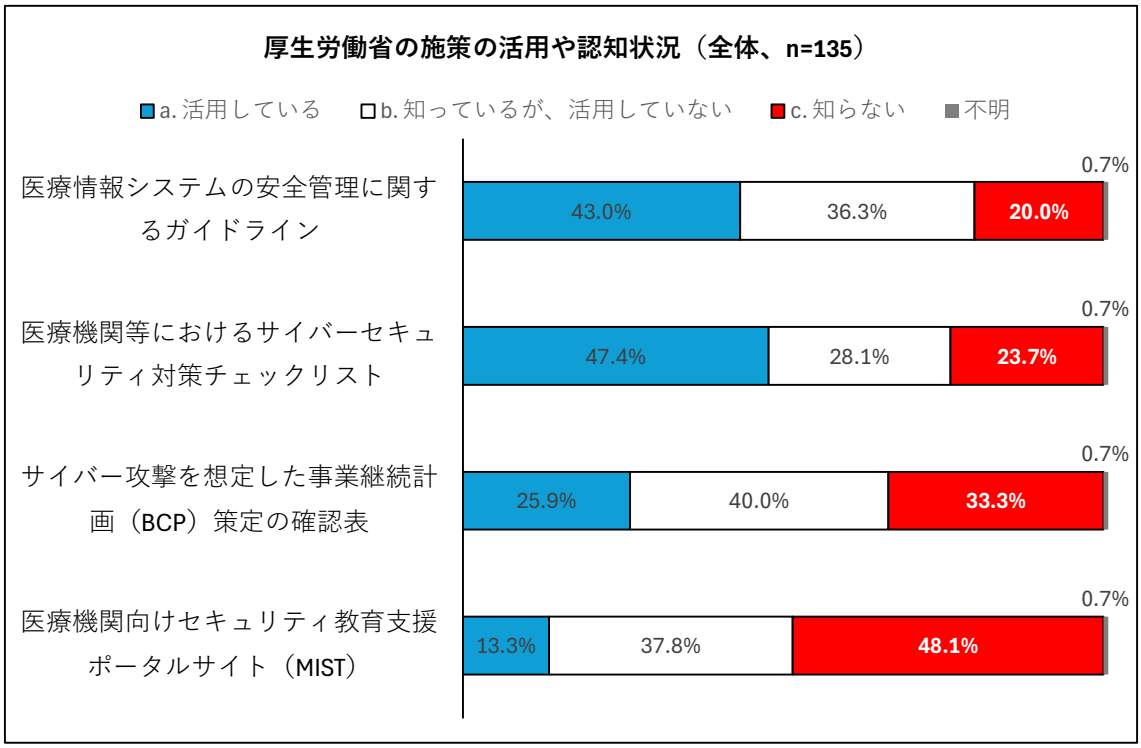
医療現場のサイバーセキュリティ対策を支援するため、厚生労働省はガイドラインに加え[6]、対策のチェックリスト[7]、そしてサイバー攻撃を想定したBCP策定の確認表を準備しており[8]、同省の委託事業として医療機関向けセキュリティ教育支援のポータルサイト（MICT）を設置している[9]。

図表 3.5.1 は、これらの厚労省の施策の活用や認知状況について、回答者全体を横棒グラフで、対象施設別にクロス集計した結果を表で、それぞれ示している。施設種類別にみると、医師会病院の方が活用・認知の割合が高く、特にガイドライン（75.7%）と対策チェックリスト（83.8%）は、多くの医師会病院で活用されている。

5 年前と比べて、ガイドラインへの認知が大きく進んだ。2020 年の既往調査では、全医療機関の 39.2%、病院 200 床未満の 21.7%が「ガイドラインを知らない」との回答結果だった。

[6] 厚生労働省（2023）
[7] 厚生労働省（2025）
[8] 厚生労働省（2024）
[9] 厚生労働省委託事業「医療機関向けセキュリティ教育支援ポータルサイト」https://mist.mhlw.go.jp/

図表 3.5.1 厚生労働省の施策の活用や認知状況



厚生労働省の施策の活用状況	医師会病院(n=37)					健セ・検セ・複合体(n=98)				
	a. 活用している	b. 知っているが、活用していない	c. 知らない	不明	計	a. 活用している	b. 知っているが、活用していない	c. 知らない	不明	計
医療情報システムの安全管理に関するガイドライン	75.7%	21.6%	2.7%	0.0%	100.0%	30.6%	41.8%	26.5%	1.0%	100.0%
医療機関等におけるサイバーセキュリティ対策チェックリスト	83.8%	13.5%	2.7%	0.0%	100.0%	33.7%	33.7%	31.6%	1.0%	100.0%
サイバー攻撃を想定した事業継続計画（BCP）策定の確認表	56.8%	32.4%	10.8%	0.0%	100.0%	14.3%	42.9%	41.8%	1.0%	100.0%
医療機関向けセキュリティ教育支援ポータルサイト（MIST）	21.6%	43.2%	35.1%	0.0%	100.0%	10.2%	35.7%	53.1%	1.0%	100.0%

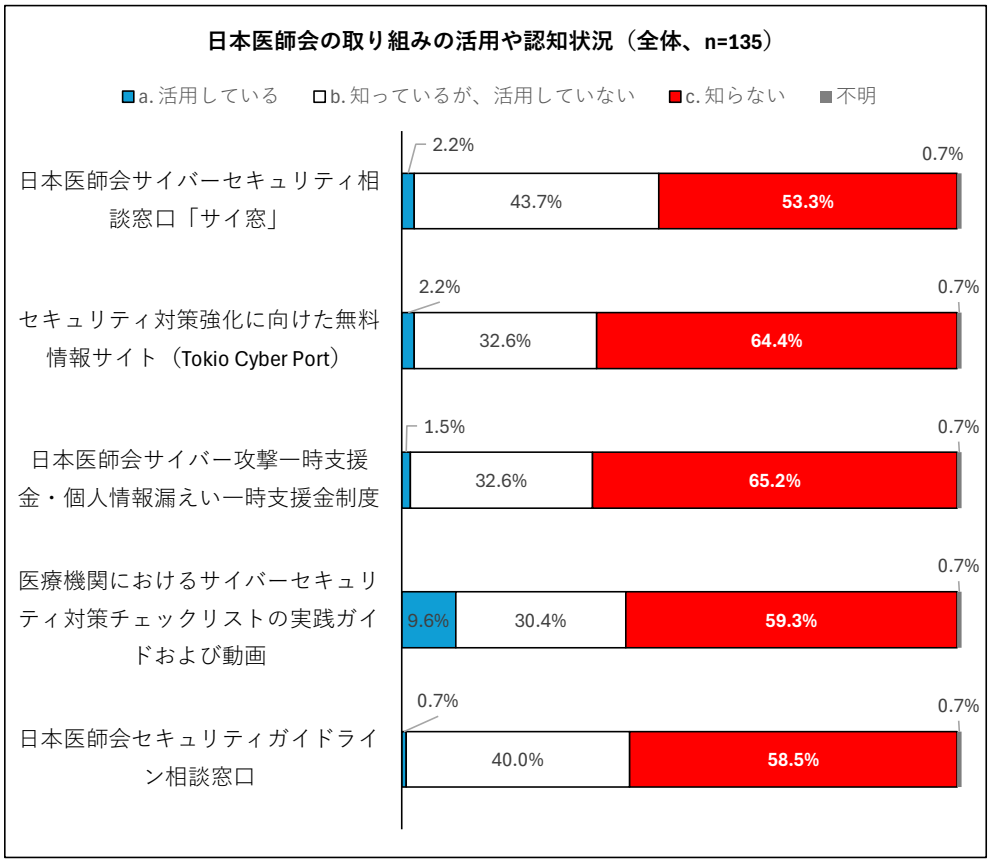
（２）日本医師会の取り組みの活用や認知状況

医療現場のサイバーセキュリティ対策を支援するため、2022 年に日本医師会は「サイバーセキュリティ支援制度」を開始、会員向けの取り組みを充実させ[10]、緊急相談窓口（サイ窓）や関連情報サイト（Tokio Cyber Port）の提供、被害時の一時金支給制度の整備、対策チェックリストの実践ガイドや動画の配信、セキュリティガイドラインに関する相談窓口の設置等を実施している。

図表 3.5.2 は、これらの日医の取り組みの活用や認知状況について、回答者全体の結果を横棒グラフで、対象施設別にクロス集計した結果を表で、それぞれ示している。施設種類別にみると、医師会病院の方が活用・認知の割合が高いものの、双方とも過半数が認知していない取り組みもあり、さらなる周知・広報活動が求められる。

[10] 日本医師会（2025）

図表 3.5.2 日本医師会の取り組みの活用や認知状況



日本医師会の取り組みの活用状況	医師会病院(n=37)					健セ・検セ・複合体(n=98)				
	a. 活用している	b. 知っているが、活用していない	c. 知らない	不明	総計	a. 活用している	b. 知っているが、活用していない	c. 知らない	不明	総計
日本医師会サイバーセキュリティ相談窓口「サイ窓」	2.7%	48.6%	48.6%	0.0%	100.0%	2.0%	41.8%	55.1%	1.0%	100.0%
セキュリティ対策強化に向けた無料情報サイト（Tokio Cyber Port）	5.4%	37.8%	56.8%	0.0%	100.0%	1.0%	30.6%	67.3%	1.0%	100.0%
日本医師会サイバー攻撃一時支援金・個人情報漏えい一時支援金制度	0.0%	37.8%	62.2%	0.0%	100.0%	2.0%	30.6%	66.3%	1.0%	100.0%
医療機関におけるサイバーセキュリティ対策チェックリストの実践ガイドおよび動画	24.3%	27.0%	48.6%	0.0%	100.0%	4.1%	31.6%	63.3%	1.0%	100.0%
日本医師会セキュリティガイドライン相談窓口	0.0%	54.1%	45.9%	0.0%	100.0%	1.0%	34.7%	63.3%	1.0%	100.0%

（３）公的な連絡・相談窓口の認知状況

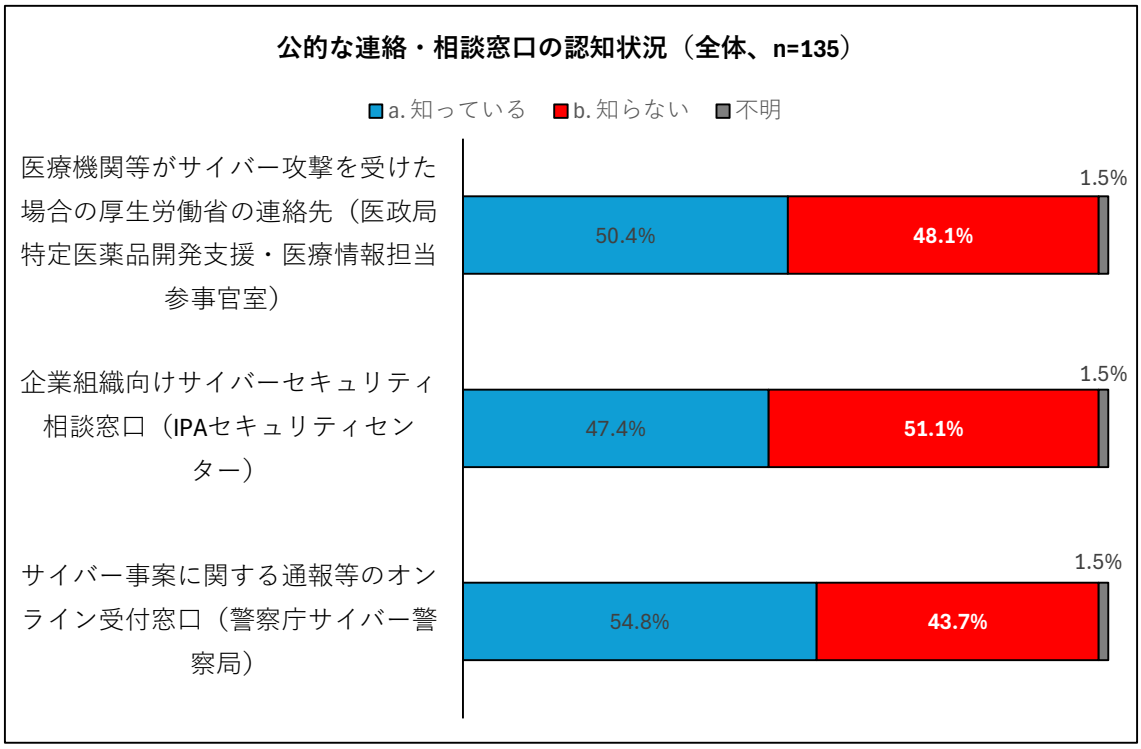
医療機関がサイバー攻撃の被害に遭った際の連絡先が厚生労働省医政局・医療情報参事官室にあり[11]、技術的な相談度口が独立行政法人情報処理推進機構（IPA）にある[12]。また、2022 年 4 月の警察庁サイバー警察局の発足に伴い、同部局には通報等のオンライン相談窓口がある[13]。

図表 3.5.3 は、これら万一の被害時の公的な連絡・相談窓口の認知状況について。回答者全体の結果を横棒グラフで、対象施設別にクロス集計した結果を表で、それぞれ示している。施設種類別にみると、医師会病院では認知している割合が高いが（7 割～8 割強が認知）、健セ・検セ・複合体ではまだまだ認知度が低い（4 割前後が認知）。

5 年前に比べると、厚労省医政局と IPA の連絡・相談窓口の認知度の進展が伺える。2020 年の既往調査では、全医療機関の 70.8%、病院 200 床未満の 64.0%が「厚労省医政局の連絡先を知らない」また、全医療機関の 76.9%、病院 200 床未満の 73.0%が「IPA 相談窓口を知らない」との結果だった。

11 厚生労働省「医療機関等がサイバー攻撃を受けた際の厚生労働省連絡先」
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html#h2_free1
12 情報処理推進機構「サイバーセキュリティ相談窓口」（企業組織向け）
https://www.ipa.go.jp/security/support/soudan.html
13 警察庁「サイバー事案に関する相談窓口」
https://www.npa.go.jp/bureau/cyber/soudan.html

図表 3.5.3 公的な連絡・相談窓口の認知状況



	医師会病院(n=37)				健セ・検セ・複合体(n=98)			
公的な連絡・相談窓口の認知状況	a. 知っている	b. 知らない	不明	総計	a. 知っている	b. 知らない	不明	総計
医療機関等がサイバー攻撃を受けた場合の厚生労働省の連絡先（医政局特定医薬品開発支援・医療情報担当参事官室）	83.8%	16.2%	0.0%	100.0%	37.8%	60.2%	2.0%	100.0%
企業組織向けサイバーセキュリティ相談窓口（IPAセキュリティセンター）	73.0%	27.0%	0.0%	100.0%	37.8%	60.2%	2.0%	100.0%
サイバー事案に関する通報等のオンライン受付窓口（警察庁サイバー警察局）	81.1%	18.9%	0.0%	100.0%	44.9%	53.1%	2.0%	100.0%

（４）今後求められる政策支援

調査では、医療分野のサイバーセキュリティに関して、（１）国政や自治体行政への要望、そして（２）日本医師会と都道府県・群市区医師会への期待を自由記述方式で収集、今後求められる政策支援の参考資料とした（巻末資料②）。

行政への要望と医師会への期待の双方において、最も目立ったのはサイバーセキュリティ対策の財源と費用支援に関する意見であった。2020 年前後に病院へのサイバー攻撃事件が相次いだ事態を受けて、医療法施行規則改正により 2023 年 4 月から医療機関へのサイバー攻撃対策が義務化された一方で、対策費用の手当てが不十分な現状を反映した内容となっている。

４．まとめと考察

本章では、本稿で実施した分析結果の要点を論じたうえで、今後の対策充実に向けた考察と提言を行う。取り上げるポイントは、(1) 直近 3 年間に発生したインシデント、(2) 現場の体制・対策の整備状況、(3) 対策費用・財源の確保の 3 点である。

４．１　直近３年間のインシデント・アクシデント

情報セキュリティ・サイバーセキュリティに関わるインシデント・アクシデントは発生していたが、患者に被害が及ぶクリティカルな事案はなかった。最も危惧される「サイバー攻撃により患者・受診者に直接の危害があった」との事案は直近３年間確認されておらず、ウイルス感染（端末の感染 10.9%、サーバの感染 4.3%）の事案はあったものの、ランサムウェアへの感染は発生していなかった。

一方、施設種別に関わらず、「患者・受診者の個人情報が含まれる FAX の誤送信」（全体 43.5%、医師会病院 52.4%、健セ・検セ・複合体 36.0%）が最多事案であった。FAX は、広義の情報通信技術（ICT）に属する、今や旧式の通信機器であるが、未だに多くの医療現場で使われている。今後の医療 DX や現場のサイバーセキュリティ確保策の検討において、医療現場における FAX の廃止や代替技術の提案もなされるべきだろう。

４．２　体制・対策の整備

対策費用・財源面での問題を除けば、５年前と比べて、サイバーセキュリティに関わる体制・対策の整備は進んでいた。これは医療現場における対策の進展を示唆する結果である。医師会病院の体制・対策について、2025 年に厚生労働省が調査した同等規模の病院の結果と比べても、同等もしくはそれ以上の体制・対策が整備されているとの結果であった。

他方で、医師会病院に比べると、総じて健診センター・検査センター・複合体の方が、体制・対策の整備がなされていない施設の割合が高かった。これは、現段階における後者側のサイバーリスクの低さを反映した結果と考えられるが[14]、今後、医療 DX の進展に伴い、両者がサイバー空間上での結び付きを深めてゆく未来を想定すれば、政策的に手当てすべき課題である。現状、主に病院・診療所を想定して形成されている厚生労働省・日本医師会の各種施策・取り組みを健診センター・検査センターにも応用・拡大する方向で、対策を進めるべきである。その際、サイバーセキュリティ対策のチェックリストの活用と行政による立入検査が、現場への対策実装のためのキーポイントとなろう。

４．３　費用・財源の確保

サイバーセキュリティ対策の費用・財源面では、多くの医療施設がその捻出に苦慮している実態が浮かび上がる調査結果であった。施設種別に関わらず回答

[14] 直近 3 年間のインシデント・アクシデント「経験なし」の割合は、医師会病院 43.2%、健セ・検セ・複合体では 75.0%であった。

施設の 6 割弱（全体 58.5%、医師会病院 59.5%、健セ・検セ・複合体 58.2%）が「対策費用の準備なし」と回答、加えて行政への要望と医師会への期待を尋ねた自由記述欄には、サイバーセキュリティ対策の財源と費用支援に関する意見が異口同音に並んだ。これらから類推するに、「対策費用を準備していない」というよりも、「準備したくてもできない」という昨今の医業経営の実情を反映した結果と解するのが自然である。

2023 年 4 月から医療機関のサイバーセキュリティ対策が法的に義務化された一方で、医療現場への対策費用の手当ては不十分である。セキュリティシステムのイニシャルコストは補助金で、恒久的にかかるランニングコストは診療報酬で賄う制度設計とするのが望ましい。今後も医療 DX を国策として推進するのであれば、避けて通れない必要経費と捉えるべきである。

参考文献・資料

United Nations (2024) “Cyberattacks on healthcare: A global threat that can’t be ignored” *UN News*
https://news.un.org/en/story/2024/11/1156751

警察庁「サイバー事案に関する相談窓口」
https://www.npa.go.jp/bureau/cyber/soudan.html

厚生労働省(2023)「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（令和 5 年 5 月)」
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html#h2_1

厚生労働省（2024）「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表等」
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html#h2_4

厚生労働省（2025）「医療機関等におけるサイバーセキュリティ対策チェックリスト（令和 7 年 5 月)」
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html#h2_3

厚生労働省「医療機関等がサイバー攻撃を受けた際の厚生労働省連絡先」
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html#h2_free1

厚生労働省 医政局 医療情報担当参事官室（2025）「病院における医療情報システムのサイバーセキュリティ対策に係る調査」の結果について
https://www.mhlw.go.jp/content/10808000/001262033.pdf

厚生労働省委託事業「医療機関向けセキュリティ教育支援ポータルサイト」
https://mist.mhlw.go.jp/

坂口一樹、堤信之（2021）「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」日医総研ワーキングペーパーNo.453　https://www.jmari.med.or.jp/result/working/post-233/

情報処理推進機構「サイバーセキュリティ相談窓口」（企業組織向け）
https://www.ipa.go.jp/security/support/soudan.html

日本医師会（2025）「日本医師会サイバーセキュリティ支援制度」(2025 年 8 月 13 日）　https://www.med.or.jp/doctor/sys/cybersecurity/001566.html

巻末資料①：調査票

※日医総研ウェブサイトで D/L 可能。

巻末資料②：自由記述

※日医総研ウェブサイトで D/L 可能。