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

一般社団法人医療 ISAC

2021 年 12 月

謝辞

本アンケートの実施に当たり、多大なるご協力をいただいた

一般社団法人日本病院会に感謝致します。

目次

1. 目的 4

2. 調査方法 5

3. 回答病院の属性 8

4　調査結果について 11

4-1. 病床規模別の調査結果 11

4-2. 開設者別の調査結果 20

5　考察 29

5-1. 調査結果全体に基づく考察 29

5-2. 個々のセキュリティ対策の実施状況に基づく考察 29

6　結論 32

1. 目的

ランサムウェアを中心とするサイバー攻撃は増加傾向[1]であり、さらに攻撃手法の巧妙化[2]も相まって世界的に大きな社会問題となっている。医療分野は情報の機微性に伴う金銭的な価値の高さからも、サイバー攻撃の標的となりやすい傾向にあり、その対策は未だ効果的とは言えない現状がある[3]。

わが国においては、厚生労働省の方針により病院等の電子カルテを含む基幹システムはインターネットに直接接続しない形で普及が進んだため、海外事例にみられるような、インターネットからの直接的な攻撃事例は従来ほとんど報告されてこなかったが、2021 年 5 月に発生した、東大阪市の総合病院のランサムウェア感染事例は、遠隔読影サービスからのネットワークを介しており、今後の被害の多発も懸念される重要なケースである。また 2021 年 10 月には徳島県の総合病院におけるランサムウェア感染が発生し、診療の継続性に大きな影響を及ぼす事案になる等、医療分野のセキュリティ水準の向上は喫緊の課題になっているといえる。

医療 ISAC ではこのような状況において、実際の医療機関がどのようなセキュリティ対策を講じているかの実態を把握するために、一般社団法人日本病院会の協力を得て、セキュリティに関するアンケート調査を行い、586 病院から回答を得た。
本資料ではこの調査から把握できる実態と課題、考えられる対策等について考察し、今後の対策につながる情報を読者と共有することを目的とする。

ランサムウェアをはじめとするサイバー攻撃の激化や、国際標準規格や国内法、ガイドラインの変更等に伴い様々な対応が必要となるなど、セキュリティ対策を取り巻く状況は急速に変化している。このような結果をアンケート非回答医療機関も含めて共有し、現在存在するリスクや課題等を共有することは、多くの医療機関の利益になると考えている。

---

[1] 警察庁広報資料 令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について 令和３年９月９日
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf
[2] 「国内標的型分析レポート 2021 年版」トレンドマイクロ社レポート
https://www.trendmicro.com/ja_jp/about/press-release/2021/pr-20210916-01.html?_ga=2.44397984.505691587.1635061387-846609737.1635061387
[3] 米澤祥子 損保ジャパン RM レポート２０２ 医療分野におけるサイバー攻撃の動向と医療機関でのサイバーセキュリティ対策
https://image.sompo-rc.co.jp/reports/r220.pdf

2. 調査方法

本調査では、一般社団法人日本病院会の会員である 2479 病院を対象として、2021 年 7 月 26 日から 8 月 31 日の期間で、Web 上でアンケート調査を行った。

調査項目は ISO27002(2018)をベースに、その医療分野の規格である ISO27799(2016)で定義された医療分野固有の要件を含めた観点より精査し、複数の調査要件カテゴリのもとで、合計 22 件の項目を設定した。(図 2-1)
具体的な調査要件カテゴリ・踏査項目は以下の通り。

(図 2-1)調査要件カテゴリ/調査項目の内容

No	調査項目
セキュリティガバナンス	
Q1	組織全体における情報セキュリティを実現するための全体ルールを整備し、定期的且つ重大な変化が発生した場合に見直しを行っている
セキュリティ管理組織	
Q2	組織全体のルールに基づいて、情報セキュリティ管理を確実に実施するための役割と責任の範囲を定義している。また、厚生労働省や関連団体と情報連携・共有するための仕組みを確立している
テレワークセキュリティ	
Q3	モバイル機器の利用及びテレワーキングに関するセキュリティを確実にする手続を実施している
人的セキュリティ	
Q4	雇用前の段階で、組織として、従業員が、求められている役割と責任に応じたセキュリティ水準に到達しているかを確認している。
Q5	雇用期間中、組織として従業員に求めるセキュリティ意識を一定水準で維持するための教育・研修を継続的に実施している。
Q6	雇用終了後の従業員に、組織が求めるセキュリティ水準を遵守し続けさせるための手続を実施している。
情報資産管理	
Q7	組織の情報資産を特定し，適切な保護に向けたルール、役割・責任を定めている。
Q8	情報資産の重要度・機微性に応じて、適切なセキュリティ管理ルールを整備している。

No	調査項目
Q9	外部記憶媒体（USB、HD、CD/DVD、MO 等）が取り扱う情報の重要度に応じて適切なセキュリティ管理ルールを整備している。
アクセスコントロール	
Q10	医療情報へのアクセス方針を定め、方針に基づく不適切なアクセスを制限している。
Q11	医療情報システムへのアクセスは許可された利用者にのみ付与されており，未許可のアクセスを防止している。
暗号化	
Q12	情報の機密性，真正性及び／又は完全性を保護するために，暗号の適切かつ有効な利用を実施している。
物理的セキュリティ	
Q13	医療情報システム、及び当該システムへアクセス可能な端末へのアクセスに関する物理的なセキュリティ対策を実施している。
システム運用・利用時のセキュリティ	
Q14	医療情報システムを正確かつ安全に利用・運用するためのセキュリティ対策を実施している。
Q15	医療情報システムの重要度に応じて、必要なデータ・プログラムを定期的にバックアップするルールを定めている。
Q16	医療情報システムへのアクセスログを取得し、一定の頻度に基づき点検し、問題があれば是正活動を行っている。
Q17	医療情報システムに未許可のソフトウェアがインストールされないように管理手続を定めている。また、既にインストールされたソフトウェア、及びオペレーティングシステムの技術的な脆弱性への対応を一定の頻度で実施している。
ネットワークセキュリティ	
Q18	ネットワークを介して利用される医療情報システムを確実に保護し、組織内外との情報授受において、一定のルールに基づくセキュリティ対策を実施している。
新規システムの開発・導入におけるセキュリティ対応	
Q19	情報セキュリティが医療情報システムに欠くことのできないという前提のもと、医療情報システムの新規開発・導入に関する自組織としてのポリシーを整備し、ベンダーへの指示・監督も含めて、セキュリティに配慮したシステムの開発・導入を主導している。
外部サービス利用時のリスク管理	
Q20	外部委託先や外部サービス提供がアクセス可能できる、あるいは自動的にデータ連携している院内の医療情報システムについて、自組織が合意可能な適切なセキュリティ水準に基づいて、データの連携等が行われるように、サービス利用前またはサービス利用中の期間においてモニタリングし、是正指示等を行っている。

No	調査項目
情報セキュリティインシデントへの対応	
Q21	情報セキュリティインシデントが発生した場合、事前に役割・責任を定めた担当者・責任者が連携しながら、業務への影響、または患者への被害を最小限化するために対応を実施し、同様の事象が再発しないための対策を講じている。
事業継続/BCP	
Q22	自組織において自然災害やシステム障害等が発生した場合を想定した業務継続計画を策定し、一定の頻度で訓練を実施して、その実効性を高める取組を組織全体として実施している。また、自組織が被災し、システムが利用不可となった場合に備え、自組織の外部に災対系のバックアップ施設を準備している。

回答は原則として、「○」=「対応できている」、「△」=「一部対応できている」、「×」=「対応できていない」、という三つの選択肢から選択させている。また、回答者が補足等のためにコメントを記載する欄を全ての項目で設けた。

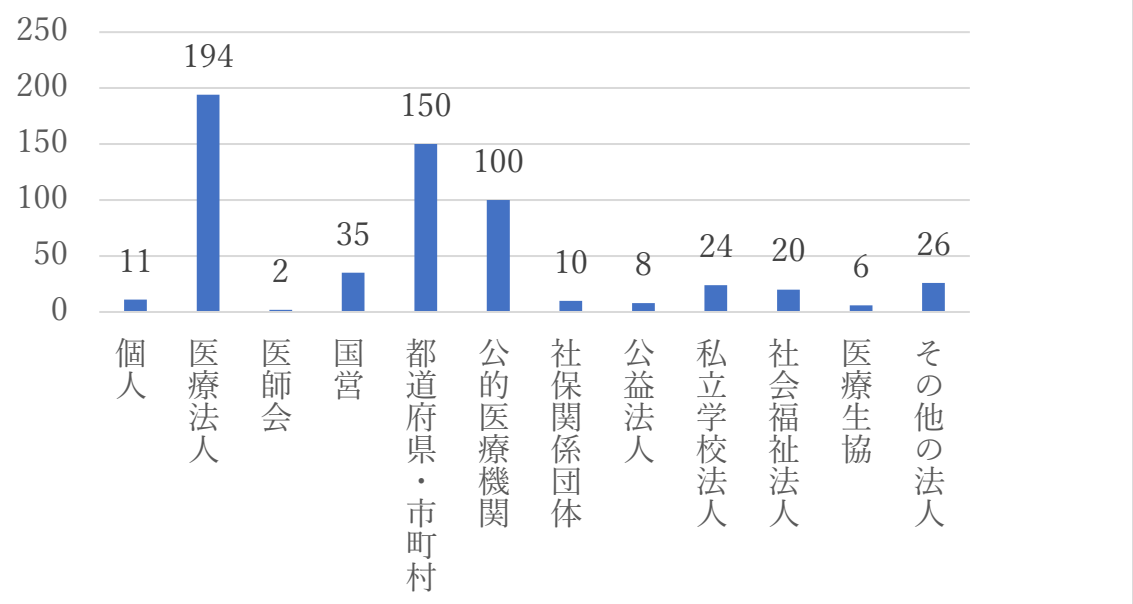
なお、回答者には、病院の属性として、開設者、病床規模、情報システム管理態勢、情報システム保守態勢の 4 点についても併せて回答を求めている。

3. 回答病院の属性

2479 病院に対してアンケート調査を依頼し、586 病院から回答を得た。回答率は 23.6%であった。

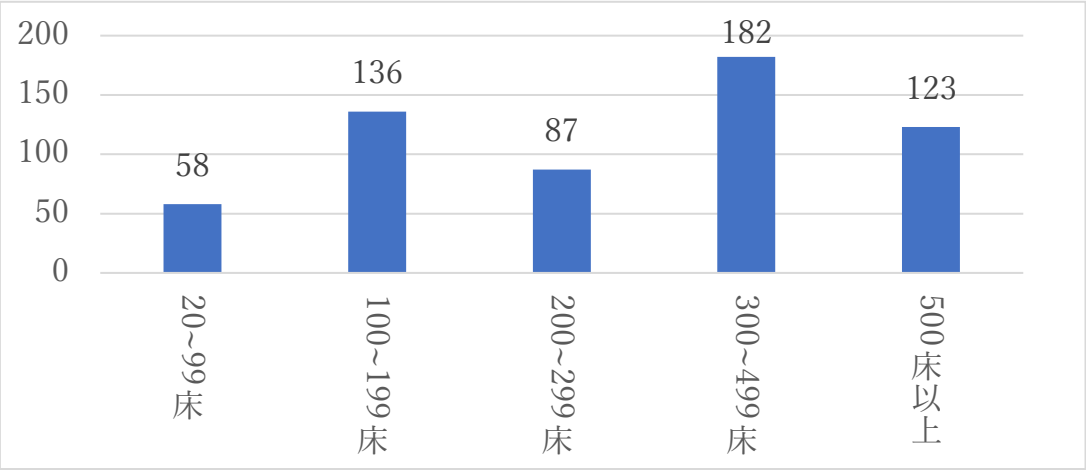
開設者別の回答病院の内訳(図 3-1)としては、医療法人が 194 施設と最も多く、次いで都道府県・市町村の 150 施設、公的医療機関の 100 施設と続いた。

(図 3-1)開設者別回答病院数



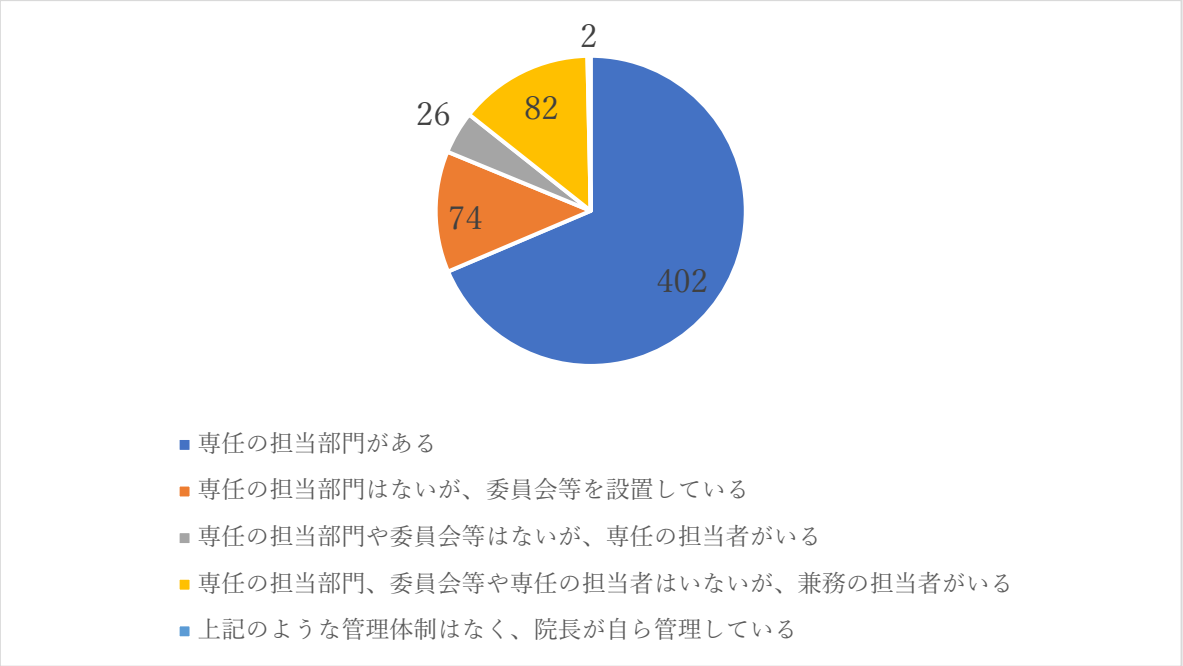
病床規模別の回答病院の内訳(図 3-2)としては、300-499 床が 182 施設と最多で、次いで 100-199 床の 136 施設、500 床以上の 123 施設と続いた。

(図 3-2) 病床規模別回答病院数

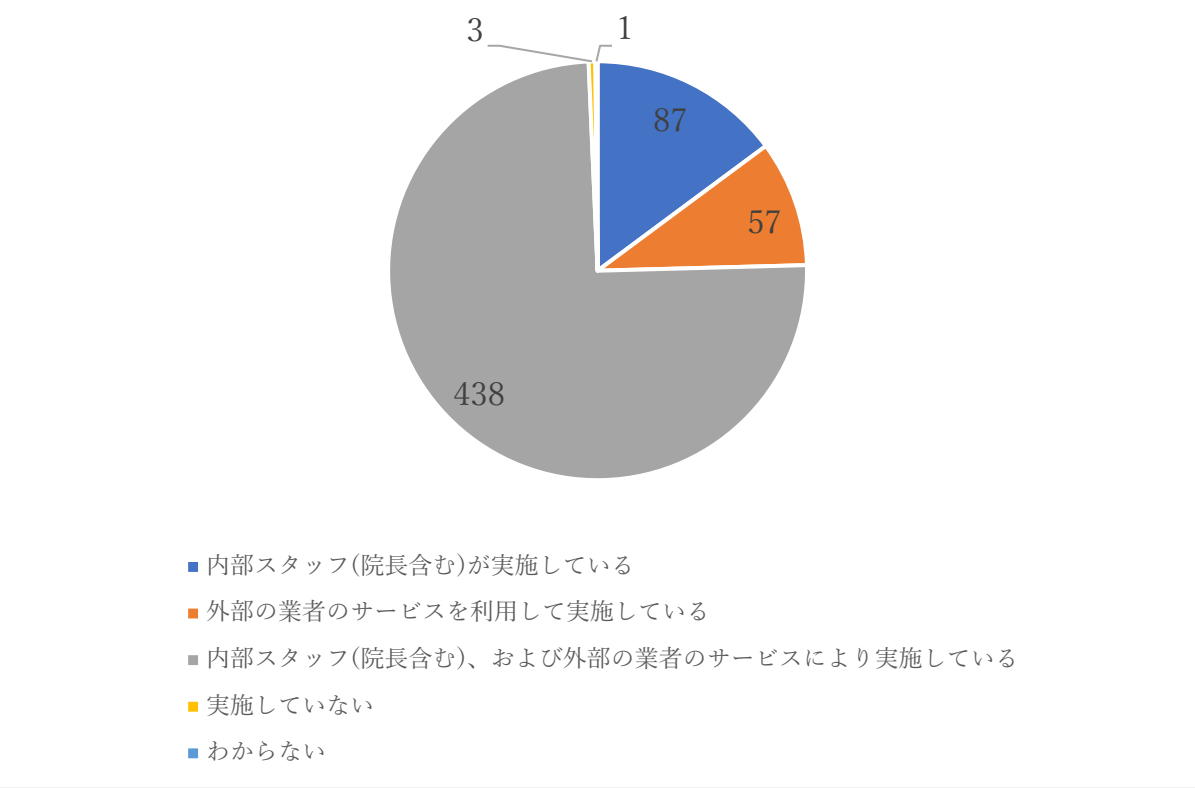


また、情報システムの管理態勢(図 3-3)では、全体の 7 割程度が「専任の担当部門がある」との回答であり、情報システムの保守状況(図 3-4)でも全体の 7 割近くが「内部スタッフ(院長含む)及び外部の業者のサービスにより実施している」との回答であった。このため、今回の回答病院の多くは、専任の担当部門を持ち、外部事業者のみでなくシステム管理部門の職員も含めてセキュリティ対応を行っていることが想定される。

(図 3－3)情報システムの管理態勢



(図 3-4)情報システムの保守状況



4　調査結果について

本章では、アンケート調査結果のうち、医療機関のセキュリティ管理を考える上で重要な示唆を得ることが出来た調査項目等を中心に、病床規模、及び開設者別に調査結果を示す。

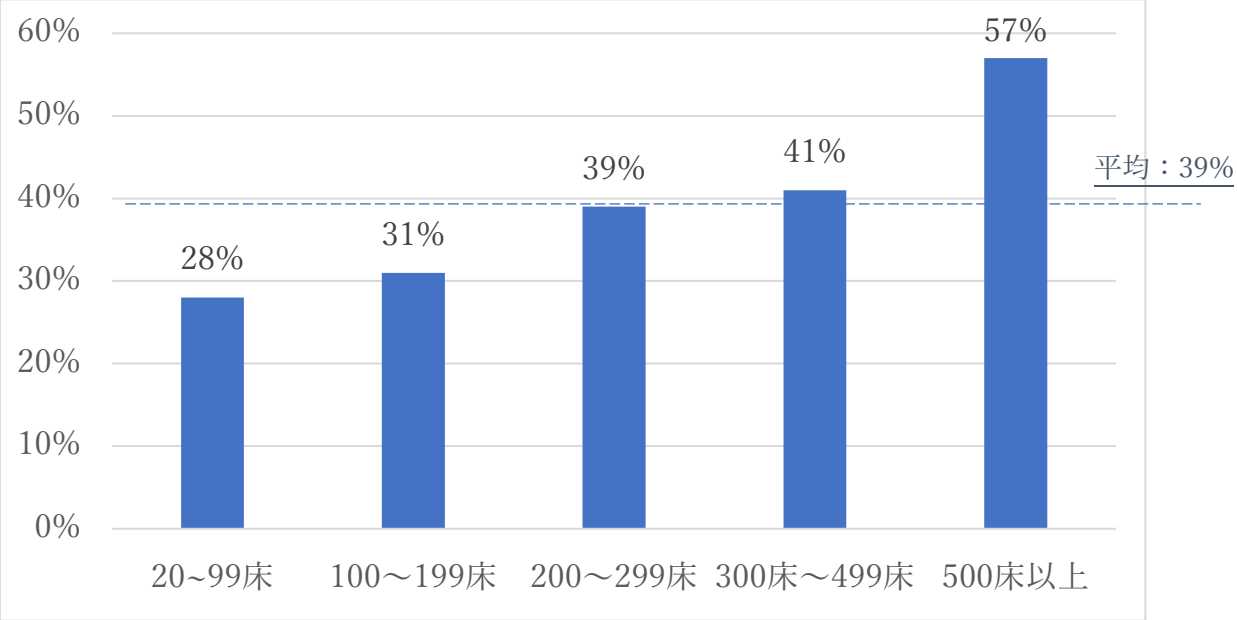
4-1. 病床規模別の調査結果

病床規模別の調査件数の母集団は 586 病院となる。なお、各数値は小数点以下を切り捨てた表記となる。

4-1-1. 全体傾向

全設問に対する「対応できている（「○」）」との回答率を比較すると、500 床以上の病院は 57%と非常に高く、**病床規模が小さいほど段階的に「○」の回答率が低下し、「△」（部分的に対応できている）、「×」（対応できていない）の割合が多くなる傾向**がみられた（図 4-1）

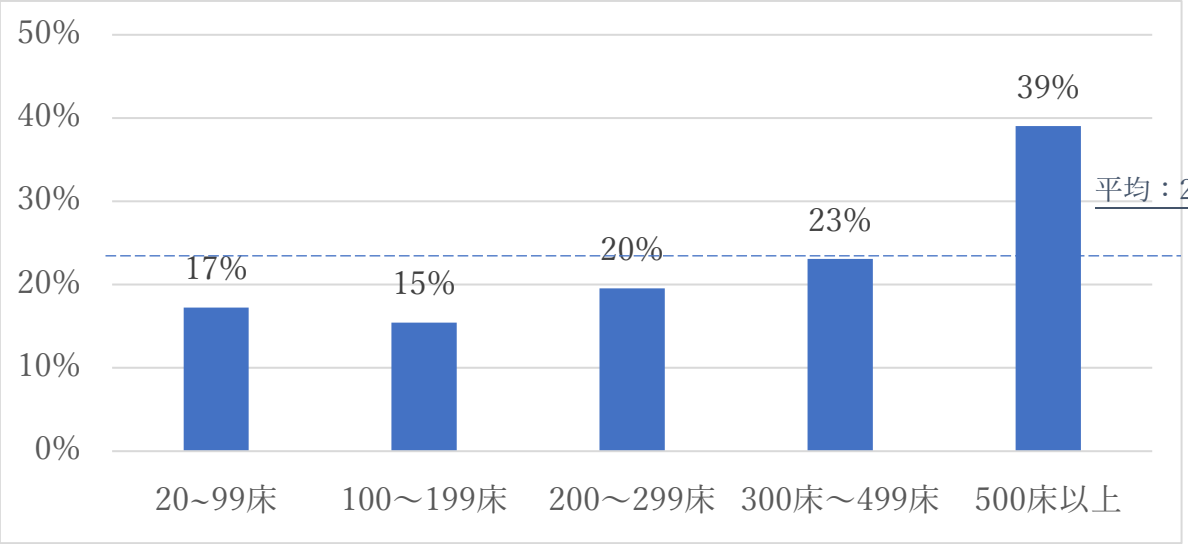
（図 4-1）病床規模別の全体傾向



4-1-2. テレワークセキュリティ

テレワークセキュリティに関して、「モバイル機器の利用及びテレワーキングに関するセキュリティを確実にする手続を実施しているか？」との調査項目に対して、「対応できている」との回答率は、500 床以上の病院とそれ以下の病床数の病院とで大きな隔たりがあることが示されている。(図 4-2)

(図 4-2)病床規模別テレワークセキュリティ実施率



4-1-3. 人的セキュリティ

人的セキュリティに関しては、雇用前/雇用期間中/雇用終了後に関わる観点より、以下の 3 つの調査項目を設定したが、全て「対応できている」と回答した病院は、500 床以上で 51%と最も高く、病床数が減少するにつれて低下する傾向がみられた。(図 4-3)

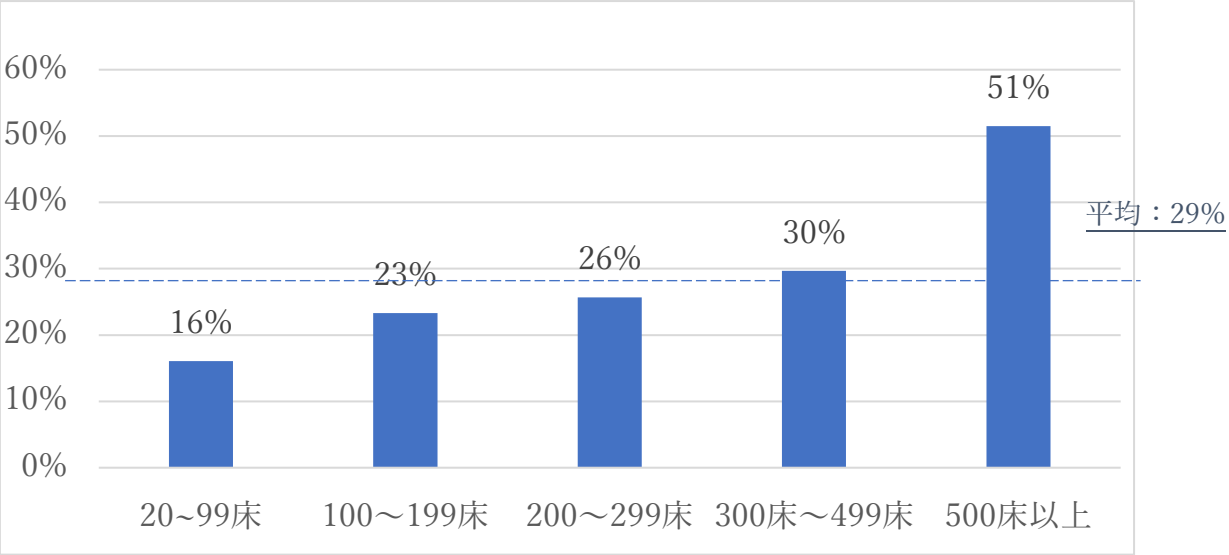
(調査項目)

① 雇用前の段階で、組織として、従業員が、求められている役割と責任に応じたセキュリティ水準に到達しているかを確認しているか？

② 雇用期間中、組織として従業員に求めるセキュリティ意識を一定水準で維持するための教育・研修を継続的に実施しているか？

③ 雇用終了後の従業員に、組織が求めるセキュリティ水準を遵守し続けさせるための手続を実施しているか？

(図 4-3) 人的セキュリティの設問全てに「対応できている」と回答した病床規模別病院割合

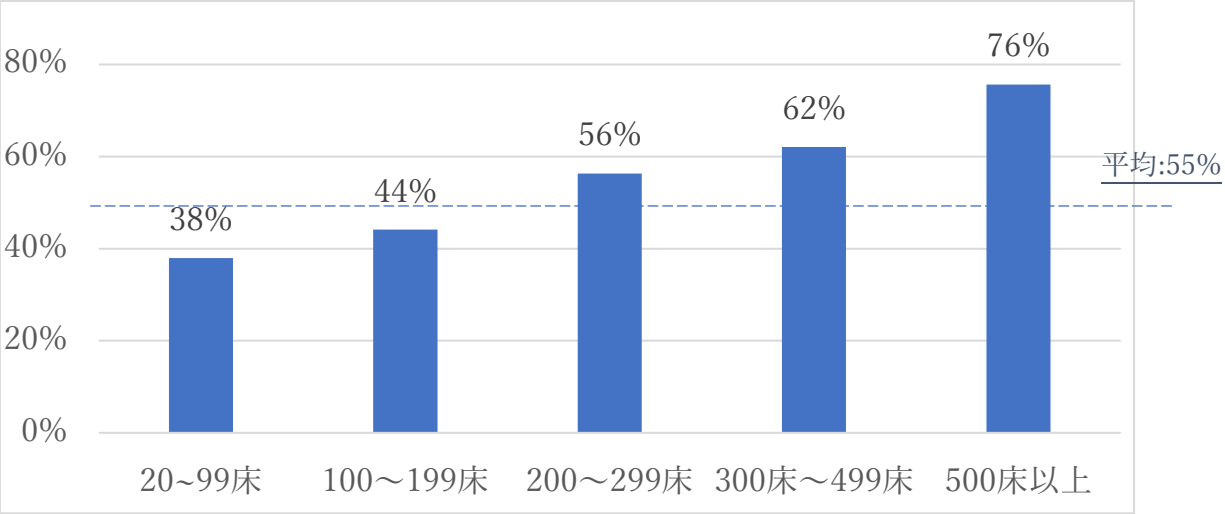


4-1-4. アクセスコントロール

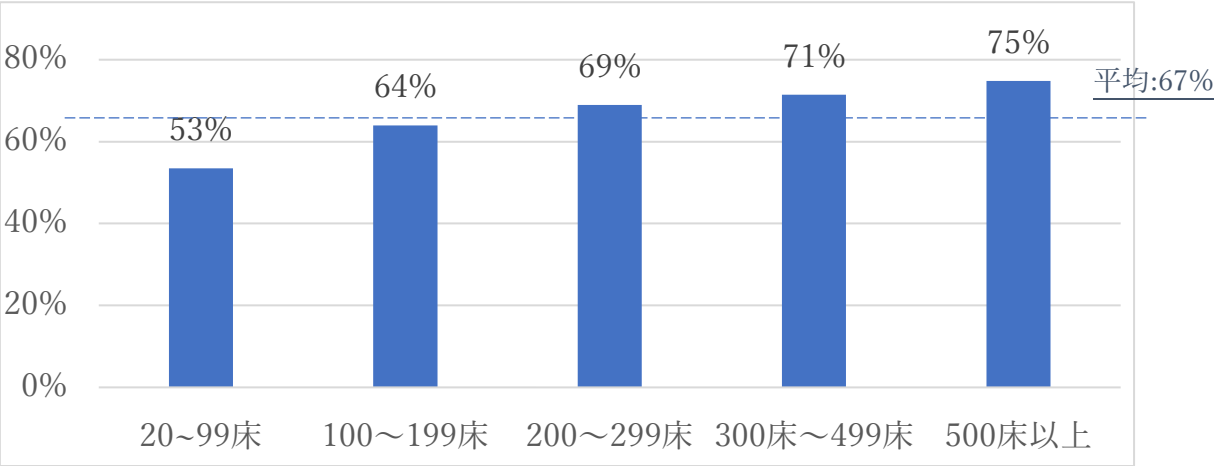
アクセスコントロールについては、アクセス方針を定めた上でのアクセス制限を実施していることについて対応済みの病院の割合は特に 200 床以下の病院では対応率が低い(図 4-4)

一方で許可された利用者へのアクセス権限の付与管理への対応済みとの回答率はいずれの病院においても高い実態(図 4-5)が示されている。

(図 4-4)『医療情報へのアクセス方針を定め、方針に基づき不適切なアクセスを制限しているか？』に「対応できている」と回答した病床規模別病院の割合



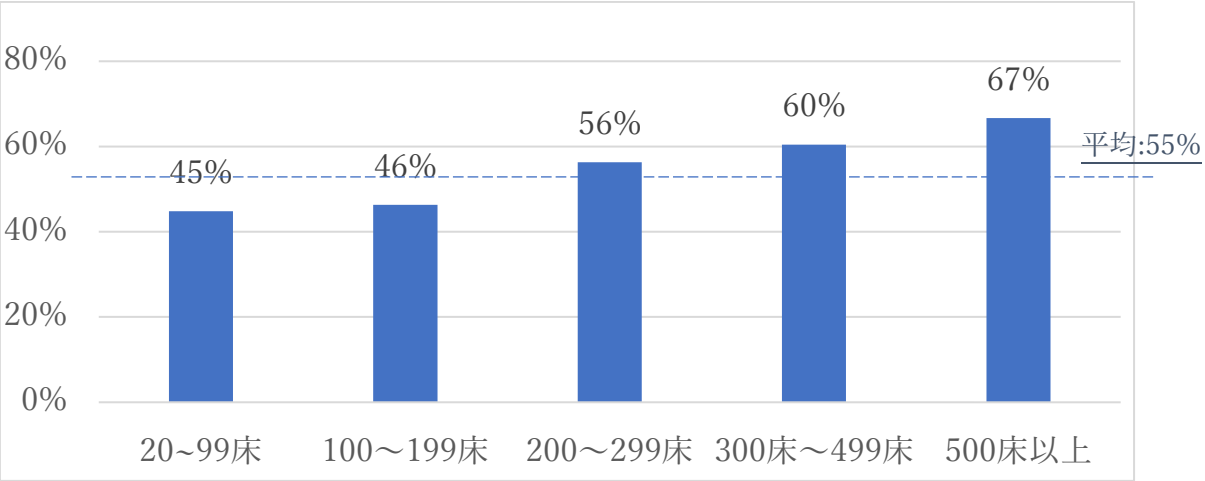
(図 4-5)『医療情報システムへのアクセスは許可された利用者にのみ付与されており，未許可のアクセスを防止しているか？』に「対応できている」と回答した病床規模別病院の割合



4-1-5.. バックアップ

「医療情報システムの重要度に応じて、必要なデータ・プログラムを定期的にバックアップしているか」という調査項目に対して「対応できている」との回答率は全体として 55%程度と比較的高い。(図 4-6)

(図 4-6)病床規模別バックアップ実施率

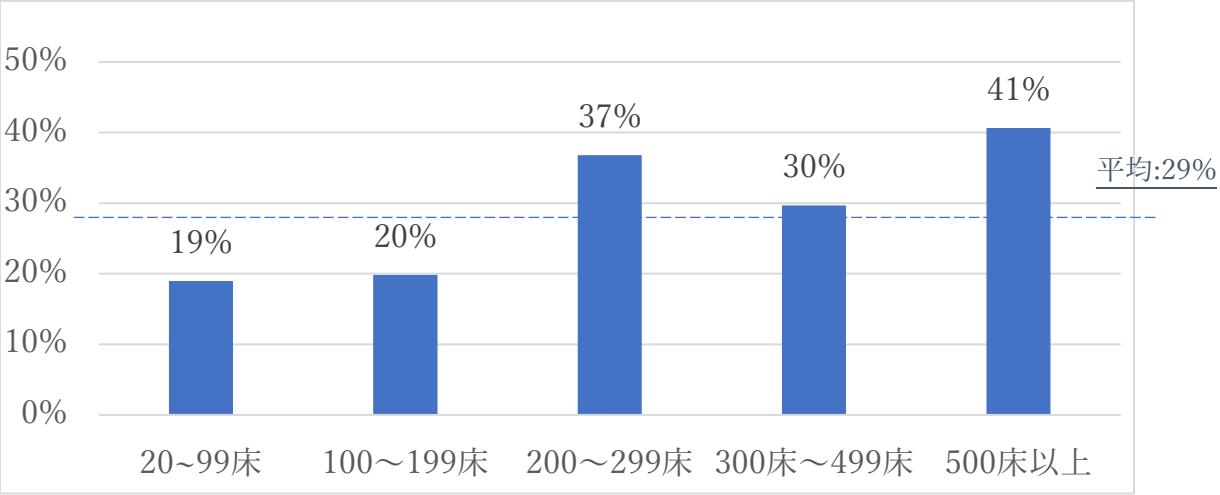


なお、特に 200 床未満の病院では、自由コメントのなかで、「オンラインストレージにバックアップを取得している」「DAT でバックアップを取得し、複数世代管理を行っている」等のコメントが多く、オフライン環境へのバックアップ退避までには取り組めていない現状が見受けられた点を補足しておく。

4-1-6. ログ保管・モニタリング

「医療情報システムへのアクセスログを取得し、一定の頻度に基づき点検し、問題があれば是正活動を行っているか」という調査項目に対して、「対応できている」との回答率は平均 29%と他の調査項目と比較しても全体的に低い。
一番高い 500 床以上でも 4 割程度と全体として低い傾向がみられた。(図 4-7)

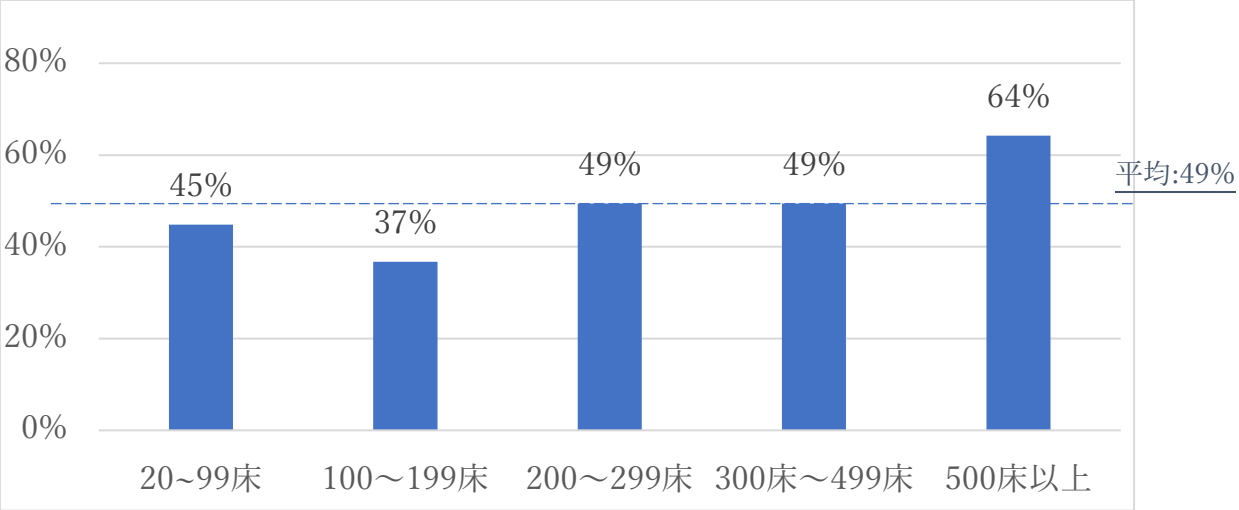
(図 4-7)病床規模別ログ保管・モニタリング実施率



4-1-7. 運用上のセキュリティ管理

「医療情報システムに未許可のソフトウェアがインストールされないように管理手続を定めているか。また、既にインストールされたソフトウェア、及びオペレーティングシステムの技術的な脆弱性への対応を一定の頻度で実施しているか」という調査項目に対して「対応できている」との回答率(図 4-8)は、500 床以上の病院では 64%と対応率が高かったが、500 床未満の病院では、50%未満の対応率であった。

(図 4-8)病床規模別運用セキュリティ管理実施率



但し、技術的な脆弱性への対応については、診療系ネットワークは外部ネットワークと接続していないため、特に実施していないとのコメントが特に 200 床以下の病院を中心に見受けられていた点を補足しておく。

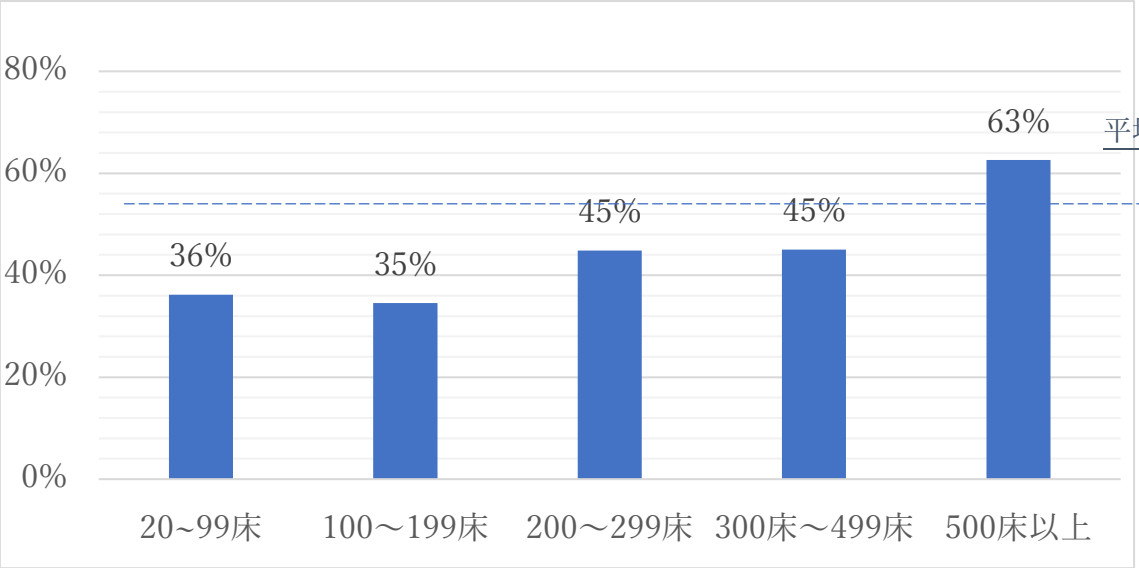
4-1-8. インシデントレスポンス/BCP

以下の調査項目について、①に「対応できている」との回答率は平均 45%程度の対応率(図 4-9)であったのに対して、②に「対応できている」との回答率は、平均 21%であり、①の半分以下の低い結果(図 4-10)となった。

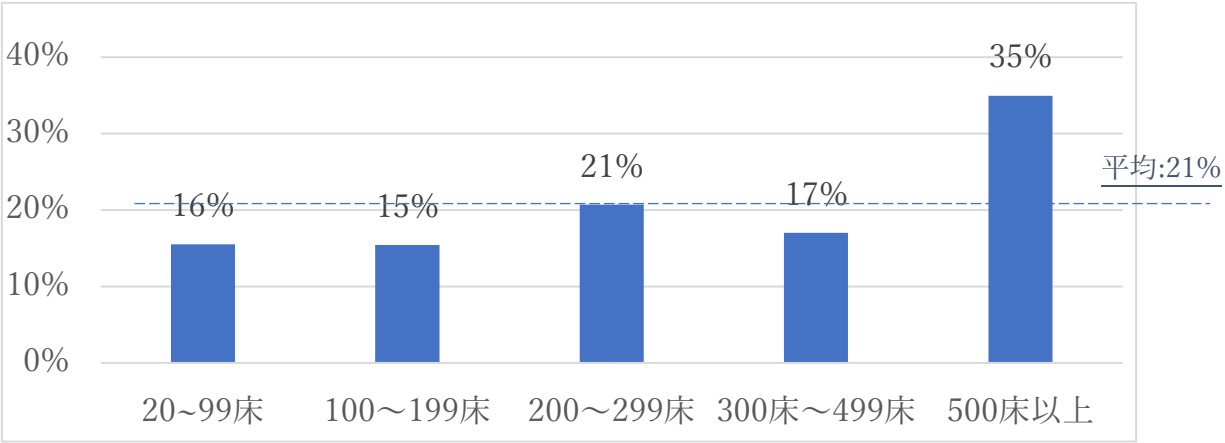
① 情報セキュリティインシデントが発生した場合、事前に役割・責任を定めた担当者・責任者が連携しながら、業務への影響、または患者への被害を最小限化するために対応を実施し、同様の事象が再発しないための対策を講じているか。

② 自組織において自然災害やシステム障害等が発生した場合を想定した業務継続計画を策定し、一定の頻度で訓練を実施して、その実効性を高める取組を組織全体として実施しているか。また、自組織が被災し、システムが利用不可となった場合に備え、自組織の外部にバックアップ施設を準備しているか。

(図 4-9) ①が「○」と回答した病床規模別病院割合



(図 4-10) ②が「○」と回答した病床規模別病院割合



4-2. 開設者別の調査結果

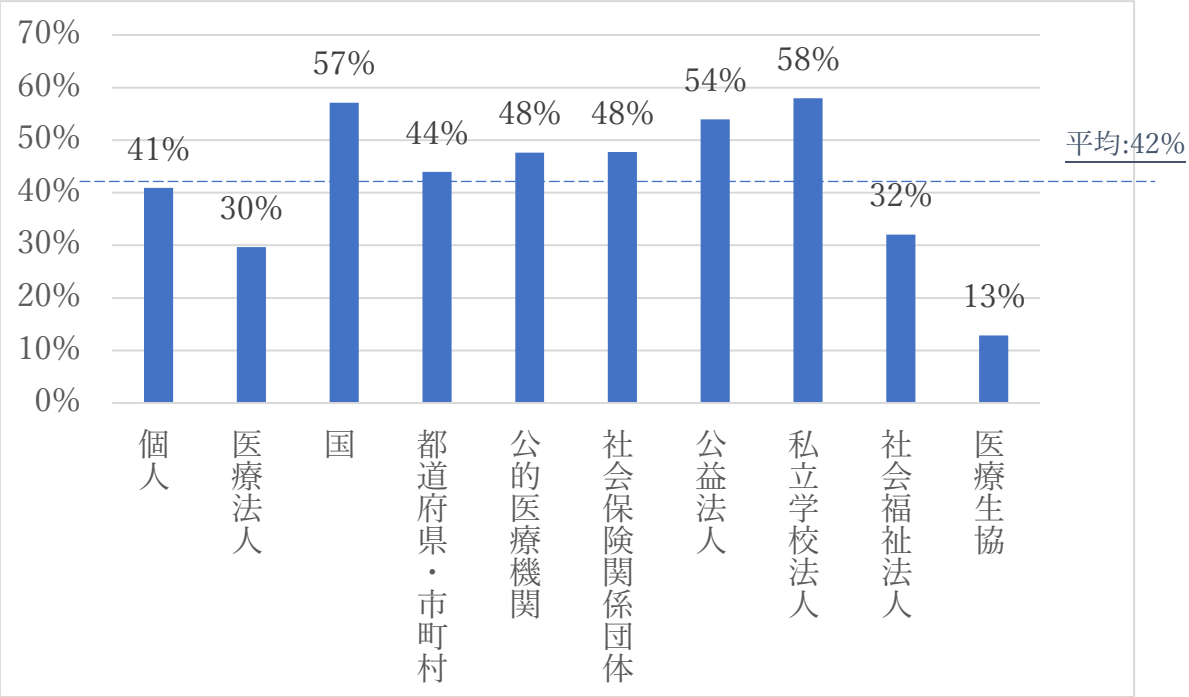
本調査に回答した病院全体件数（586 件） のうち、「その他法人」(26 件）は開設者に着眼した精査が困難、及び「医師会」（2 件）は「対応できている」（「○」の回答がなかったため、以下の調査結果からは除外している。そのため、開設者別の調査結果の母集団は 558 件となる。
なお、各数値は小数点以下を切り捨てた表記となる。

4-2-1. 全体傾向

全設問に対する「対応できている」（「○」）」との回答率は、全体平均では 42%であったが、**国（国立/独法含む）、公益法人、私大は「対応済」回答平均率が 5 割を超えており、対応水準も高い**と考えられる。

一方で、**医療法人、社会福祉法人による全項目へ「対応できている」との回答率は 3 割前後であり、さらに医療生協では 1 割程度にとどまっている等、開設者別病院の区分のなかでは比較的に低い状況**であった。（図 4-11）

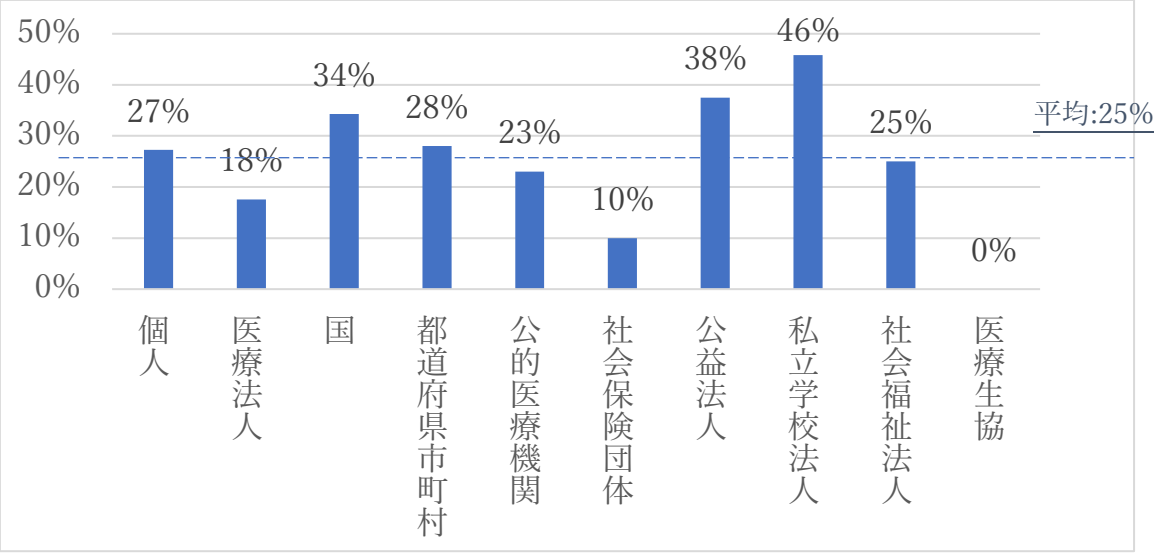
（図 4-11）開設者別の全体傾向



4-2-2. テレワークセキュリティ

テレワークセキュリティについては、私大病院による「対応できている」との回答率が最も高い状況であった。（図 4-12）

（図 4-12）開設者別テレワークセキュリティ実施率



4-2-3. 人的セキュリティ

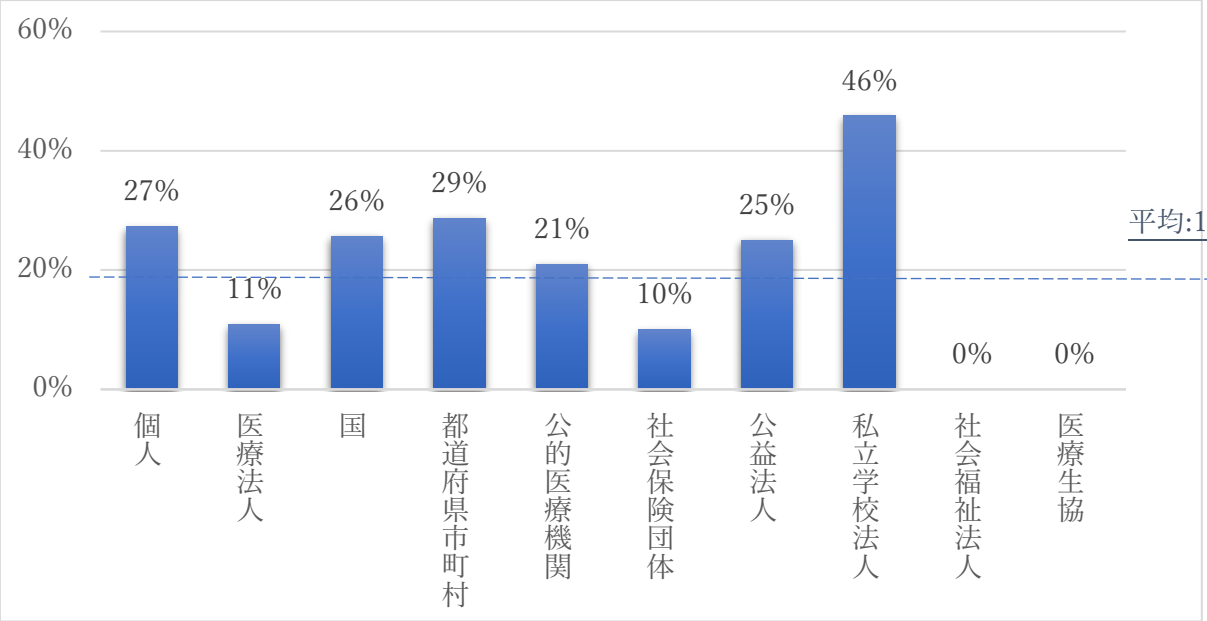
人的セキュリティに係る調査項目は以下の 3 点となる。

① 雇用前の段階で、組織として、従業員が、求められている役割と責任に応じたセキュリティ水準に到達しているかを確認しているか？
② 雇用期間中、組織として従業員に求めるセキュリティ意識を一定水準で維持するための教育・研修を継続的に実施しているか？
③ 雇用終了後の従業員に、組織が求めるセキュリティ水準を遵守し続けさせるための手続を実施しているか？

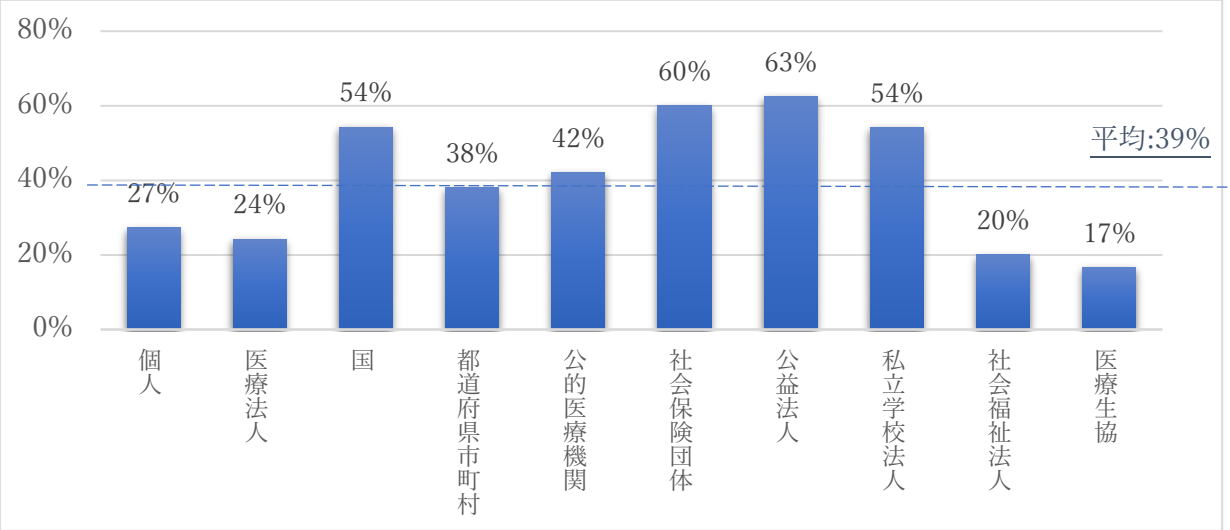
雇用前チェック(①)を「対応できている」との回答率は全開設者ともに平均 19.5%と低い。(図 4-13)

一方、②の雇用期間中の教育・研修へ「対応できている」とした回答率(図 4-14)は私立大学病院が最も高く、さらに③の雇用後の NDA について「対応できている」とした回答率(図 4-15)を見ると、公益法人、社会保険団体、国営、私立大学の区分が平均を大きく上回る結果となっている。

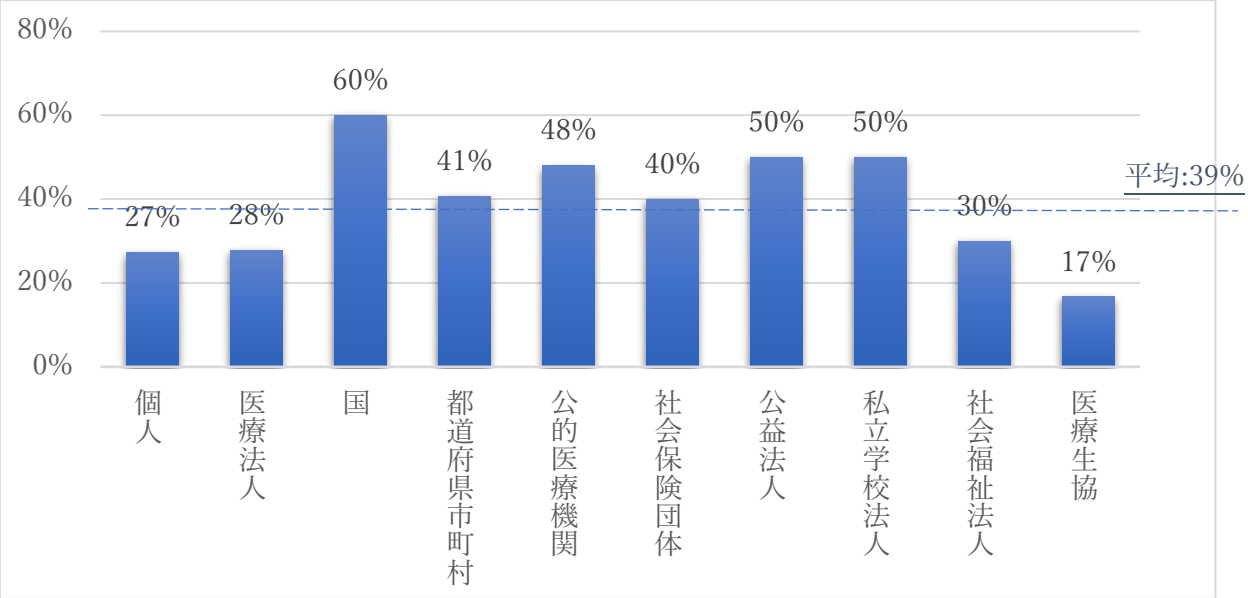
(図 4-13)開設者別雇用前セキュリティチェック実施率



（図 4-14）開設者別雇用期間中セキュリティチェック実施率



（図 4-15）開設者別雇用後セキュリティチェック実施率



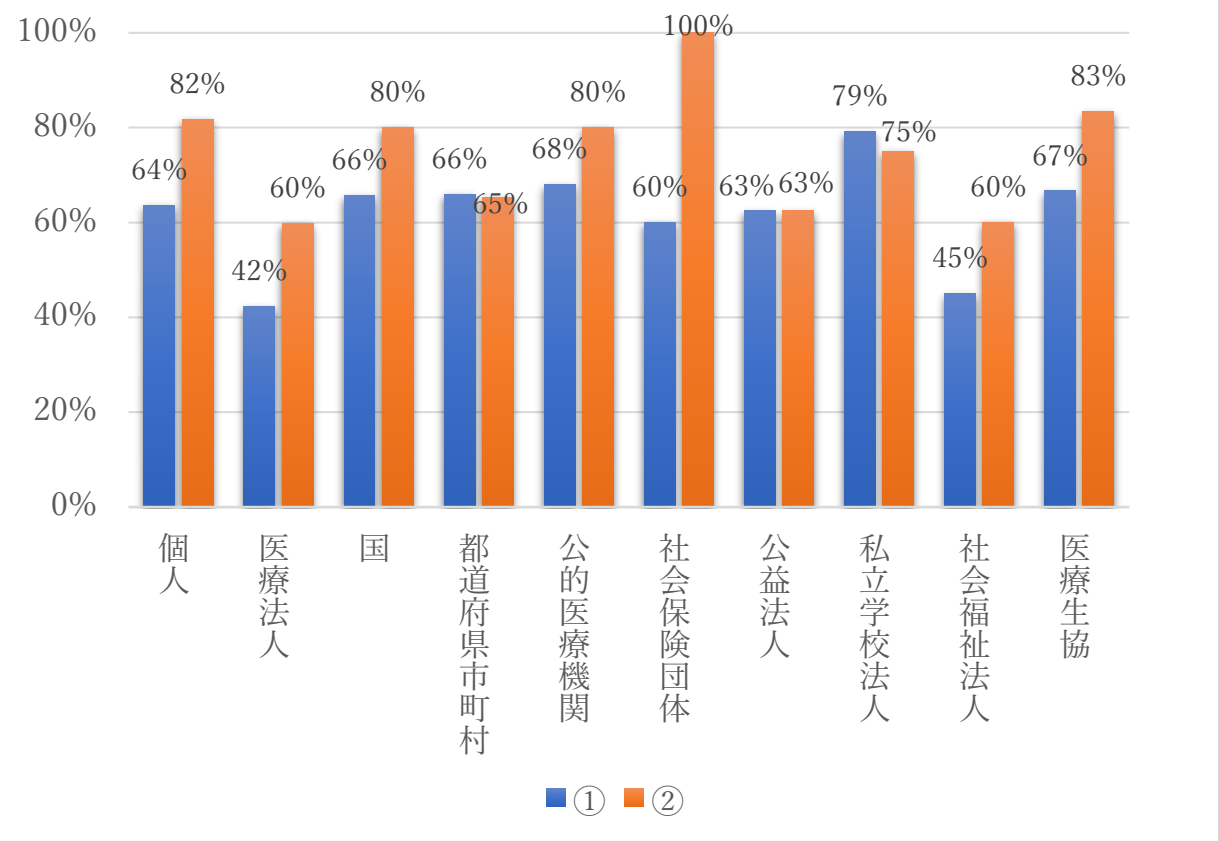
4-2-4. アクセスコントロール

以下 2 つの調査項目への「対応できている」とした回答率としては、アクセス管理の実施という観点では全開設者ともに 6 割以上を示しているのに対して、アクセス管理ルール整備の取組は医療法人と社会福祉法人で低い結果となった。(図 4-16)

① 医療情報へのアクセス方針を定め、不適切なアクセスを制限しているか？

② 医療情報システムへのアクセスは許可された利用者にのみ付与されており，未許可のアクセスを防止しているか？

(図 4-16)：①・②を「対応できている」と回答した病院の開設者別割合

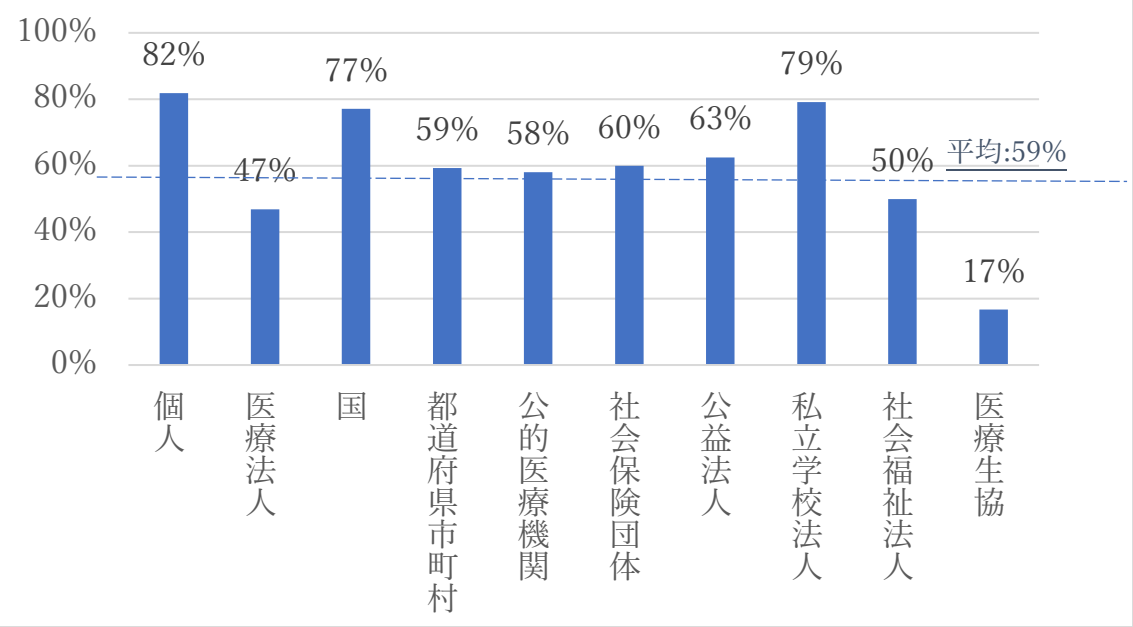


4-2-5. バックアップ

「医療情報システムの重要度に応じて、必要なデータ・プログラムを定期的にバックアップしているか」という調査項目に対する回答率としては、個人/国営/私大病院が高い一方、社会福祉法人や医療法人が低い状況であった。

特に回答率の低い社会福祉法人や医療法人からは、オフライン環境へのバックアップ退避の取組にまで踏み込めていないコメントが特に見受けられている。(図 4-17)

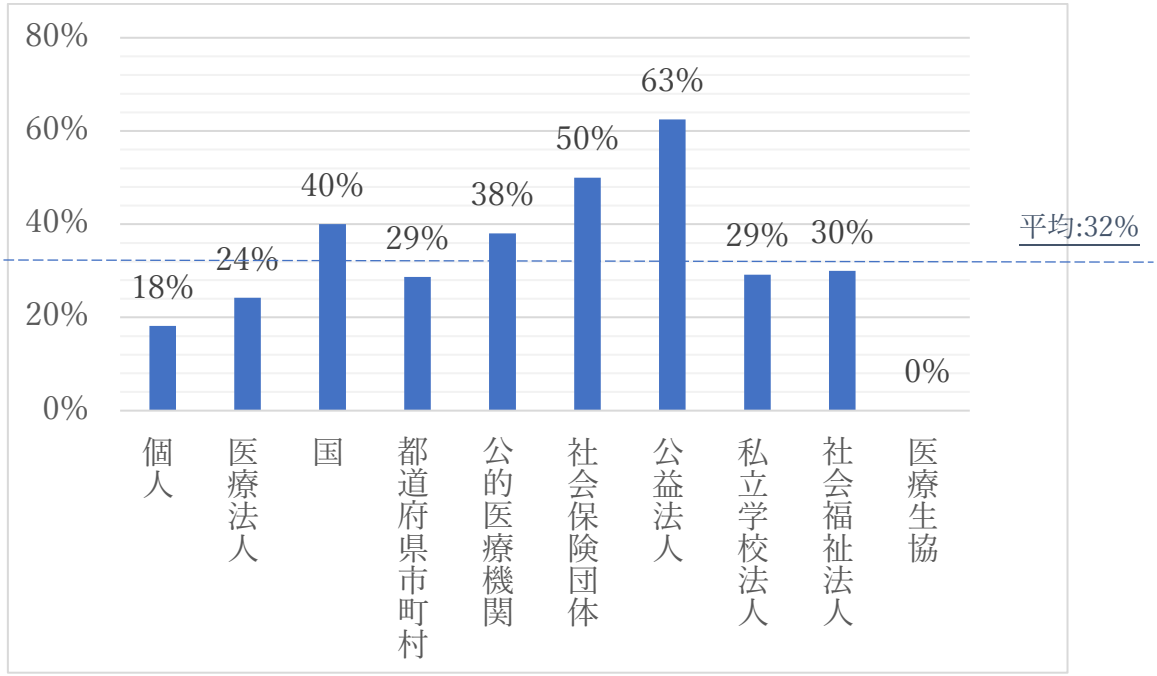
(図 4-17))開設者別バックアップ実施率



4-2-6. ログ保管・モニタリング

「医療情報システムへのアクセスログを取得し、一定の頻度に基づき点検し、問題があれば是正活動を行っているか？」との設問に対して、全体的に「対応できている」との回答率は 32%と低いものの、公益法人と社保では相対的に対応率が高いことが判明している(図 4-18)

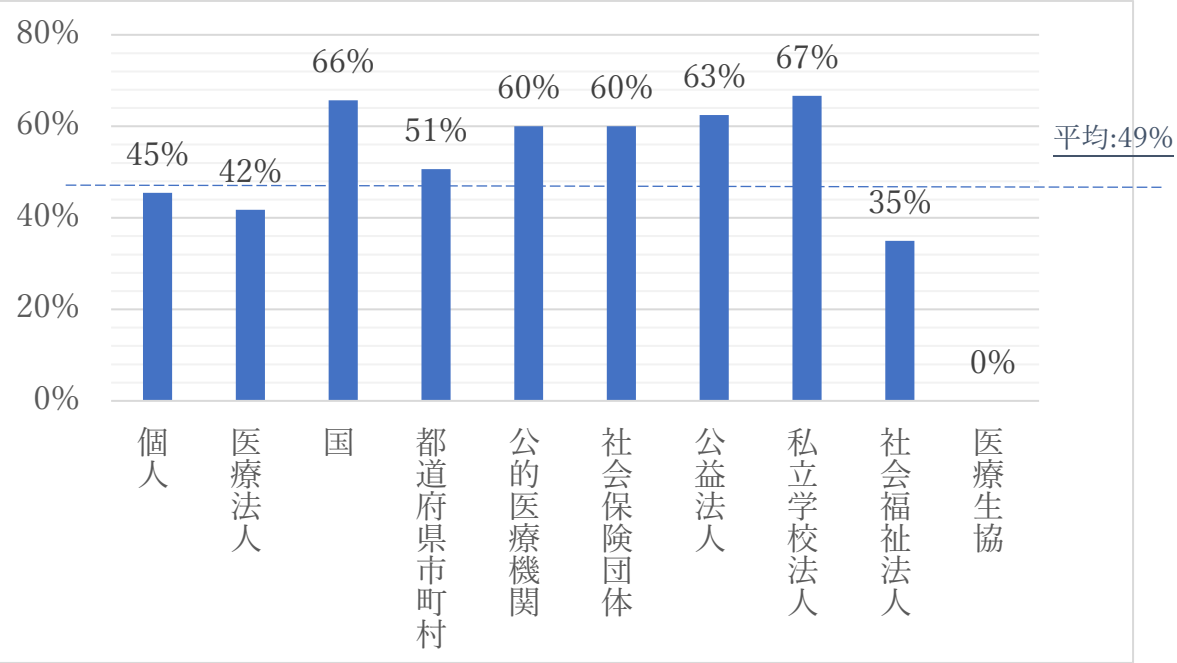
(図 4-18)開設者別ログ保管・モニタリング実施率



4-2-7. 運用上のセキュリティ管理

「医療情報システムに未許可のソフトウェアがインストールされないように管理手続を定めているか。また、既にインストールされたソフトウェア、及びオペレーティングシステムの技術的な脆弱性への対応を一定の頻度で実施しているか」という調査項目に対する「対応できている」との回答率（図 4-19）は、医療法人・社会福祉法人・個人・医療生協が平均より低いことがわかる。

（図 4-19）開設者運用セキュリティ管理実施率



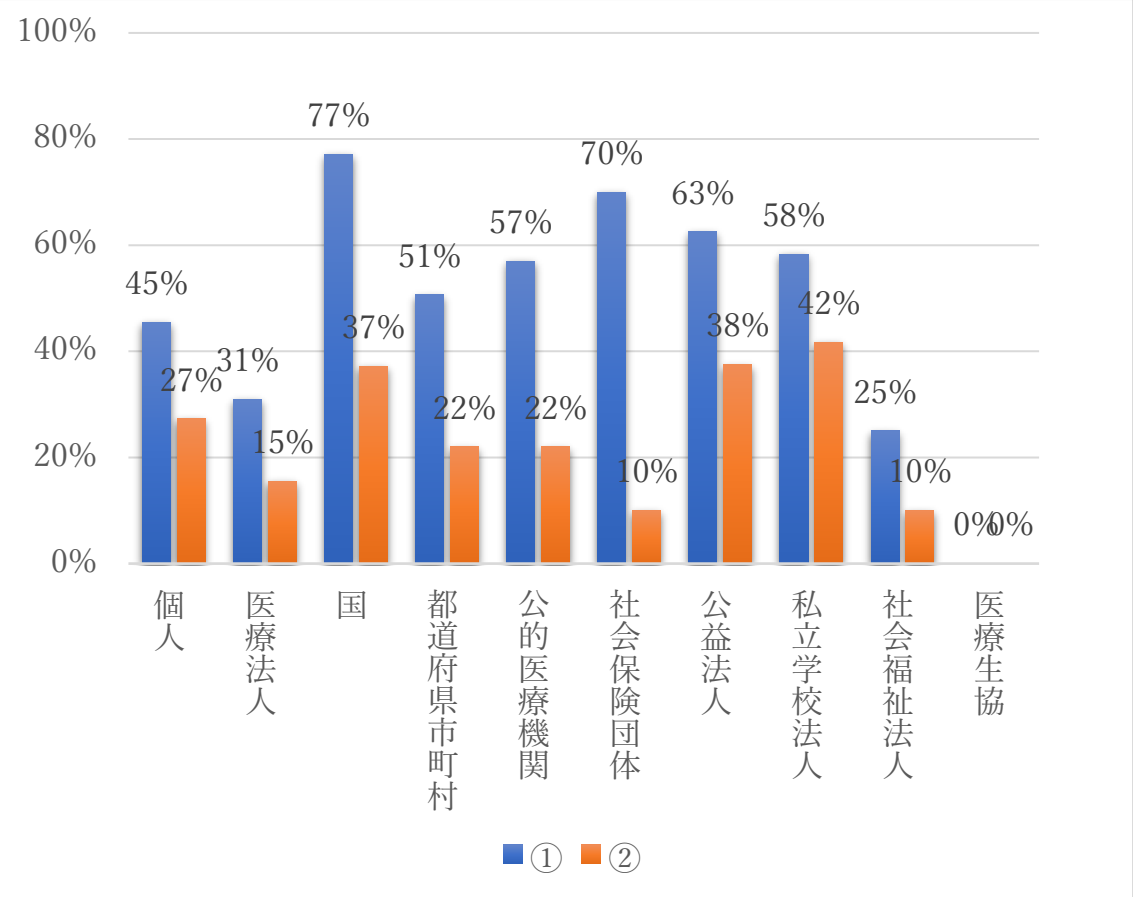
4-2-8. インシデントレスポンス/BCP

以下 2 つの調査項目に対して「対応できている」との回答率を見ると、全体的にインシデントレスポンス（①）の対応率は高いが、業務継続計画（②）は低いという傾向がみられた。ただ、業務継続計画への対応率は私大病院が相対的に高い状況であることも示された。（図 4-20）

① 情報セキュリティインシデントが発生した場合、事前に役割・責任を定めた担当者・責任者が連携しながら、業務への影響、または患者への被害を最小限化するために対応を実施し、同様の事象が再発しないための対策を講じているか。

② 自組織において自然災害やシステム障害等が発生した場合を想定した業務継続計画を策定し、一定の頻度で訓練を実施して、その実効性を高める取組を組織全体として実施しているか。また、自組織が被災し、システムが利用不可となった場合に備え、自組織の外部にバックアップ施設 を準備しているか。

（図 4-20） ①・②を「対応できている」と回答した開設者別病院割合



5　考察

5-1. 調査結果全体に基づく考察

病床規模別でみると、500 床以上のセキュリティ対応策の実施率（対応済み回答率）は高い一方、500 床以下となると、病床規模の縮小化に伴い、段階的に実施率が低下する全体傾向がある。

また開設者別でみると、国営（国立/独法含む）、公益法人、私大は「対応済」回答平均率が 5 割を超えており、対応水準も高いと考えられる。一方、医療法人、社会福祉法人による対応率は 3 割前後、医療生協では 1 割程度にとどまっており、他病院と比較して低い状況である。

これらを総合すると、本調査結果を考察する限りでは、500 床以上の国営・公益法人・私大病院群はセキュリティ対応水準が高い一方で、それ以下の病床数の、医療法人・社会福祉法人、医療生協運営の病院群にはセキュリティ対応上の課題が多く存在する可能性が示唆される。

5-2. 個々のセキュリティ対策の実施状況に基づく考察

以下では、個々の調査結果の内容から導出しうる、病院固有のセキュリティ管理状況の傾向、またはそこから得られる洞察について記す。

5-2-1. テレワークセキュリティについて

病床規模別で見ると、テレワークセキュリティへの取組は全体として着手が遅れている。
クローズドのオンプレ環境を長らく前提にしてきた医療情報システムの利用環境の弊害が表れていると言える。
なお、開設者別でみると、私大病院での推進率が最も高い状況。私大の管轄でもある文部科学書による IT 化や BCP 策定指示の恩恵を私大病院も受けていることも一因と想定される。

5-2-2. 人的セキュリティについて

病床規模別でみると、雇用前/雇用期間中/雇用終了後の三点に基づく人的セキュリテイの実施率は 500 床以上の病院については高いものの、それ以下は大きく対応率が低下するという、一般的な病床規模別傾向を踏襲している。

ただし、開設者別でみると、雇用前/雇用期間中/雇用終了後の各取組への対応率の高いものは私立大学病院であることが把握でき、この取組については私立大学病院が高い対応水準にある

ことがうかがえる。
また、開設者別で見た場合、雇用前チェック率は全開設者ともに平均が 20%以下と著しく引く一方で、雇用期間中の教育・研修率、雇用終了後（離職後）の機密保持の締結については、全体平均が 40%近くに達している。

この事実からは、雇用前の機密保持チェックについては、医療従事者固有の秘密保持のルールが存在するため明示的にその取り決めを行うことは少ないものの、雇用後の教育・研修、あるいは離職後の機密保持については相対的にリソースを注入する病院が多いことを示していると言える。

5-2-3. アクセスコントロールについて

病床規模で見た場合、アクセス方針の整備は 200 床以下の病院では対応率が低いが、許可された利用者へのアクセス権限の付与管理を実務的に行う取組に関する対応率はいずれの病院規模の病院においても 50%を超えている状況であった。
なお開設者別にみると、アクセス方針の整備は医療法人と社福での実施率が低いが、アクセス管理の実務的な対応という観点では全開設者ともに 6 割以上の実施率を示している。

これらの事実からは、事前にアクセス管理方針を職務別に厳格に定義するアクセスコントロールの運営ではなく、常勤・非常勤等の労働形態、あるいは医師、看護師、薬剤師、コメディカル、ひいては医療事務等を担う非医療従事者も含め、人材が多様且つ流用動的な病院の現場実態にあわせて、実務的なアクセス管理を行う運用が優先されていることが推測される。

5-2-4. バックアップについて

病床規模別でみると、バックアップについて対応できているとの回答率は全体的に高い状況である。
一方、開設者別でみると、個人/国営/私大病院のバックアップ取得率が高いものの、社会福祉法人や医療法人でのバックアップ取得率が低い結果が示されている。

なお、自由コメントからは、バックアップの取得スキームの多くがサーバに据え付けられた DAT 等の記録媒体へのバックアップ取得、あるいはネットワーク接続しているファイルサーバへのバックアップ取得等を行っている状況が多いことが把握できている。

仮にランサムウェアに感染した場合、オンラインでバックアップを取得していたとしても、そのバックアップにも感染被害が拡大する可能性が著しく高く、従来のバックアップの管理方式の見直しも必要である。

5-2-5. ログ保管・モニタリングについて

ログ保管・モニタリングの実施率は全ての病床規模の区分を問わず、全体的に実施率が低い状況である。

不規則に多職種が連携して患者ケアを行う病院職員の活動モデルを考えた場合、不適切なアクセスの実績有無を規則に照らして定期的に点検するログモニタリングという発見的な対策は効果が低くなりがちと言える。

このような現場の活動モデルを考えた場合、ログモニタリングの実施率は低い一方で、【5-2-2】に記載する通り、現場のニーズに照らした柔軟なアクセスコントロールを実務的に行うことで、不適切なアクセスの未然防止に注力することが優先される傾向が病院には強いと考えられる。

5-2-6. 運用上のセキュリティ管理について

不要ソフトインストール制限や外部記憶媒体の利用制限は病床規模・開設者の区分を問わず、対応率が高く、昨今の病院での内部関係者による不正や誤謬による情報漏洩対策が進んでいることがうかがえる。

一方、システムの脆弱性管理については、コメントからはベンダへの依存度が高いことがうかがえる。(「ベンダがやっているはず」とのコメント)
また、同様にコメントからは、診療系ネットワークは外部と接続していないため、特に対策を講じていないという病院が社会福祉法人や医療法人を中心に多くみられている。(「診療系ネットワークは外部と接続していない」とのコメント)
このコメントの傾向は特に 200 床以下の規模の病院になるとさらに強く見受けられるものであった。

そのため、仮に診療系ネットワークへ侵入されてしまったというリスクシナリオに立った場合、技術的な脆弱性を悪用された外部者による悪意ある攻撃への防御層はまだ薄いことが想定される。

5-2-7. インシデントレスポンス/BCP

インシデントレスポンスへの対応率は比較的に高い一方で、病床規模・開設者別の区分を問わず、自然災害やシステム障害等によりシステムダウンが発生した場合の業務継続計画(BCP)の対応率はおおよそ半分程度にまで低下している。

これはシステムの可用性へ影響を及ぼさないインシデント(情報漏洩等)への対応率は高くなっている一方、外部の悪意ある攻撃者(ランサムウェア)によってシステム停止等が発生した場合の病院のレジリエンス(復旧力)は未だ低いことがうかがえる。

6　結論

医療機関におけるサイバーセキュリティ対策は、他業種と比較してかなり遅れていると言われて来た[4]。その理由としては、大病院であっても上場企業等の大企業と比較すると事業規模が小さくセキュリティ人材等を確保しにくい状況であること、専門性の高い職種が多くリテラシーレベルが不揃いであること、国内病院の収支構造上、セキュリティ投資に積極的に取組にくい状況等が考えられるだろう。

一方で世界的にサイバー攻撃の手法はより大規模かつ巧妙化しており、医療系企業や医療機関は主な標的となっている。特にランサムウェアによる攻撃は刻一刻と進化しており、昨今では暗号化を行なわれた被害者が身代金を支払わなかった場合に、あらかじめ窃取しておいた情報を公開すると脅してさらに身代金を要求する二重脅迫の手口も加速度的に猛威をふるっている。[5]

日本における医療機関のサイバーセキュリティ対策の実態を調査した最近の調査報告としては、2021 年 3 月に公表された公益財団法人医療機器センターによるもの[6]や 2021 年 4 月に日本医師会総合政策研究機構が公表したものが先行してある。[7]
これらの調査は設問内容が我々の調査項目と異なるため、その結果を一概には比較できない。
しかしながら、これらの調査のうち、多くの病院がインシデントレスポンスやサイバー攻撃を想定した BCP に関して十分な備えができていない状況であること、小規模の病院ほどサイバーセキュリティに関しての対策が不十分であること、という指摘は我々の調査結果による考察と合致すると言えるだろう。

今回の調査では、500 床以上の国営・公益法人・私大病院群はセキュリティ対応水準が高い一方で、それ以下の病床数の、医療法人・社会福祉法人、医療生協運営の病院群にはセキュリティ対応上の課題が多く存在する可能性が浮き彫りになった。このように病床規模の大小のみでなく、開設者によってもサイバーセキュリティ対策の成熟度が異なることが把握できた。今後は病床規模に加え、開設者の区分も軸とした観点に立った更なる実態調査が必要と思われる。

以上

---

[4] Anshul Gupte & Shriram Ramanathan, Ph.D. Lux Research
THE LAGGING CYBERSECURITY FRONT OF DIGITAL HEALTH https://www.luxresearchinc.com/blog/the-lagging-cybersecurity-front-of-digital-health
[5] Michael Sentonas. Forbes Technology Council COUNCIL POST Ransomware: Double The Trouble In 2021
https://www.forbes.com/sites/forbestechcouncil/2021/09/24/ransomware-double-the-trouble-in-2021/?sh=d01190f1275b
[6] 公益財団法人医療機器センター 専務理事 中野壮陛 / 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
[7] 坂口一樹（主任研究員）、堤 信之（主任研究員）日医総研ワーキングペーパー No.453 2021/4 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