全国保険医団体連合会/
日本病院会
セキュリティアンケート結果調査

一般社団法人医療ISAC

2023年1月

1. 調査概要
2. 全体結果
3. 病床規模別結果
4. その他

１．調査概要

調査の目的・背景

2022年においても国内の医療機関においてランサムウェア被害が多発している状況である。

2022年10月には国内の医療機関でリモートメンテナンス用装置として多用されているForitnet社製品を対象とした深刻な脆弱性が新たに存在することが公開され 、当該脆弱性が放置された場合、外部の第三者が製品の管理画面に容易にアクセスし、ネットワーク内部へ侵入を行えるリスクが指摘されている。

こうした脆弱性に対して、JPCERT/CCやIPA等もパッチ適用の必要性の注意喚起を行っている状況下において、大阪急性期総合医療センターが、外部の給食管理サービスを提供している外部事業者が利用していたFortinet社の製品の脆弱性が悪用され、ランサムウェア被害を受け、診療業務の継続性に深刻な被害が発生したことは記憶に新しい。

厚生労働省が2022年11月に本件を受けて、医療機関が有する外部との接続経路を棚卸したうえで、適切なセキュリティ対策を講じることを緊急周知しているように、いまや医療機関の診療系ネットワークを外部と遮断した無菌室であるため、セキュリティ面で問題がないと考える「安全神話」は完全に崩壊したと言える。

一方、2022年１月～２月にかけて医療ISAC/四病院団体協議会によるセキュリティアンケート調査結果からも把握できる通り、国内の医療機関の多くは経済的・人的リソース不足により、こうした製品の脆弱性管理も含めて、医療情報システムのセキュリティ管理業務は外部ITベンダに依存せざるを得ない状況である。

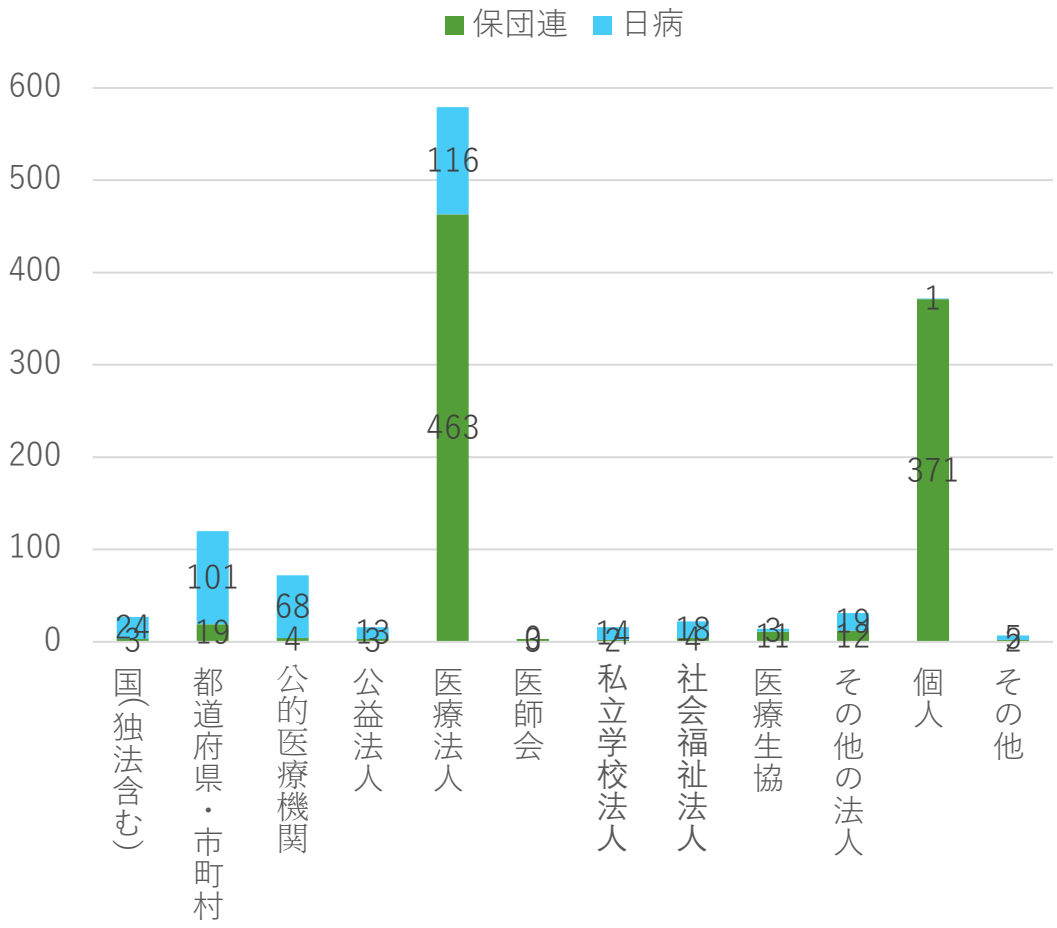
医療機関の基幹系システム＝電子カルテシステムには高い可用性が求められることから、リモートメンテナンス接続経路が外部ITベンダにより設置されることはほぼ一般的である。こうしたリモートメンテナンスの保守業務も医療情報システムを提供する外部ITベンダに医療機関では委託しているが、その役割関係を明確に契約上で定義することはあまり実施されていないことも実情である。

上記の国内医療機関を取り巻く現状を踏まえ、今回、医療ISACは全国保険医団体連合会（保団連）/日本病院会（日病）とそれぞれ、リモートメンテナンスセキュリティ、外部ITベンダとの契約管理・コミュニケーション状況についてアンケートを行い、その結果を分析した。

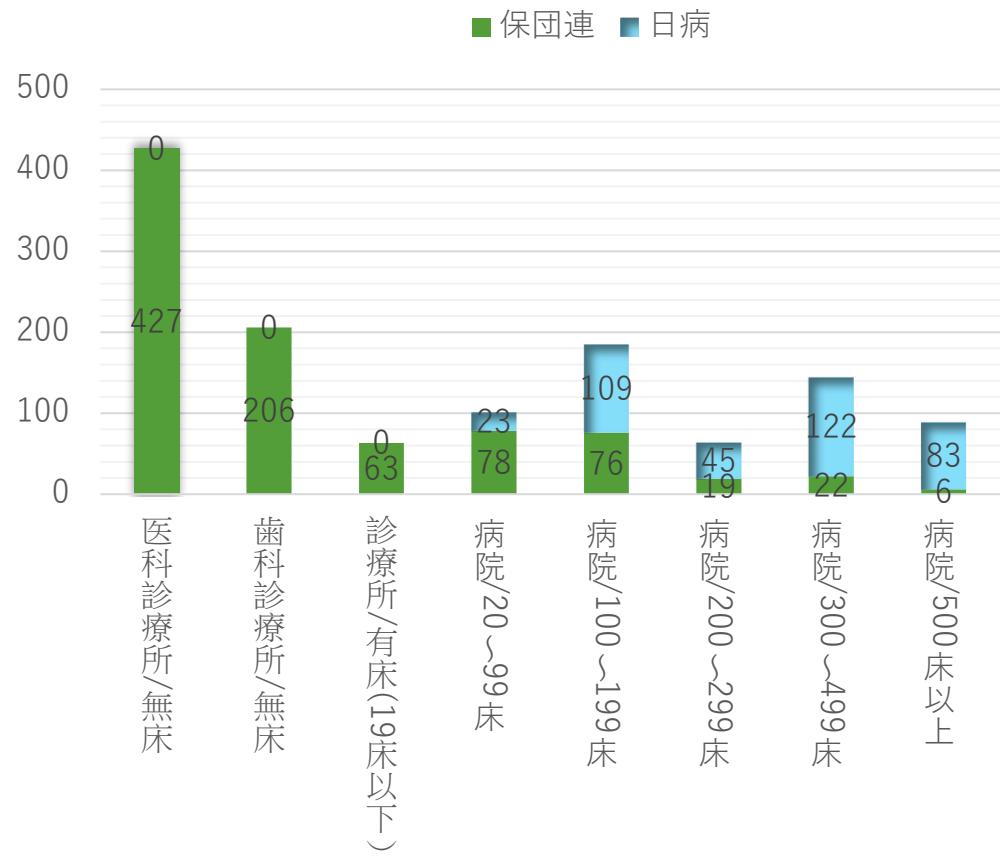
調査対象

- 実施期間：2022年11月～12月
- 対象組織合計数：1279件（保団連897件、日病382件）

＜開設者別内訳＞



＜病床規模別内訳＞



調査項目

調査項目は以下の通り。
回答はすべて「はい」「いいえ（わからない）」のいずれかを選択。

【①：リモートメンテナンス用製品の利用・把握状況】
Q1：院内の医療情報システムのうち、１つでも、外部ITベンダによるリモートメンテナンスを許可していますか
Q2：Q1が「許可している」の場合、医療機関としてリモートメンテナンスで用いられるネットワーク機器（VPN機器）の製品情報、バージョン情報は把握できていますか。

【②-A：Fortinet社リモートメンテナンス用製品の利用・脆弱性対応状況】
Q3：Q2が＜把握している＞の場合、その製品は2022年10月に脆弱性報告がされたForitnet社製品を利用していますか。
Q4：Q3が＜利用している＞の場合、2022年10月に告知された脆弱性について、自院として外部ITベンダに対応指示を行う、あるいは外部ITベンダから報告があり対応を行っていますか？

【②-B：それ以外のリモートメンテナンス用製品の利用・脆弱性対応状況】
Q5：Q3が＜利用していない＞の場合、それ以外のVPN機器の脆弱性パッチ適用を最新情報に基づき、定期的に自院として外部ITベンダに対応指示を行う、あるいは外部ITベンダから報告があり対応を行っていますか？

【③：医療機関/ベンダーとのリスクコミュニケーション状況】
Q6：医療機関として、電子カルテシステムや医事会計システム等、患者診療/医療経営の継続性に影響を及ぼす医療情報システムの保守管理について、外部ITベンダとの契約書・SLAの中で明示的にシステムセキュリティに関する責任分界（リモートメンテナンス機器のセキュリティパッチ適用は外部ITベンダの責任である旨の明記等）を取り交わしていますか
Q7：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」に基づき、医療情報システムを提供する外部ITベンダから、システムの開発・保守、運用状況等について、システム・機器の脆弱性対応も含めて、一定の頻度（定期的）に基づき、医療機関として報告を受け、内容の確認を行っていますか？
Q8：Q7で＜報告を受け、確認をしている＞場合、外部ITベンダからの情報は、院内の医療情報システムのセキュリティを向上・改善するに資する、分かりやすく役に立つ報告内容の水準となっていますか。(運用状況をテクニカルに報告した内容のみで、医療機関のIT担当者やマネジメント層にとっては理解に悩む、一方通行的で、読解が困難な内容ではないですか)

2．全体結果

＜アンケート調査結果_全体総評＞

- 今回のアンケート回答組織のうち、８割は院内システムへのベンダによるリモートメンテナンスを行わせているものの、**そのうち５割弱はメンテナンス用の機器・製品の種別・バージョン情報を把握していない状況**である。

- 22年10月に深刻な脆弱性が報告されたFortinet社のリモートメンテナンス製品・機器の利用率は1割弱と少なく、かつ、該当組織において脆弱性対応が既に完了していると回答した組織は全体の9割程度に及んでおり、**Fortinet社製品の脆弱性へのリスク認識が高く、それゆえ適切な対応が図られている状況**が見受けられる。

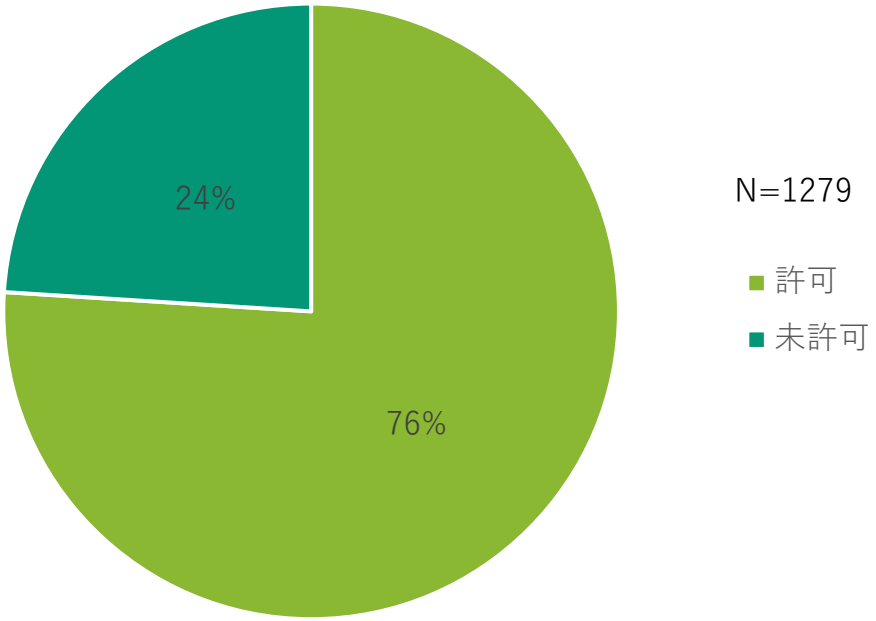
- 一方で、**Fortinet社製品以外のリモートメンテナンス機器・製品**については、種別・バージョン情報等を把握しているものの、**4割強の組織が特段脆弱性対応を実施していない**状況である。そのため、**Fortinet社以外の機器の脆弱性を悪用したサイバー攻撃が発生するリスクはまだ根強く残存している**ことが把握できる。

- ベンダとの間で医療機関としてセキュリティ上の役割・責任分担を定め、**契約等で合意形成している組織は全体の1割強**にしか満たず、さらにセキュリティ等の情報提供も含めた**報告を定期的に行わせている組織は2割強程度**にしか満たない。
- さらにベンダの報告内容が医療機関の職員にとって理解しやすい水準で整理され、提供されていると回答した組織は6割弱だが、**4割程度はその内容は理解しづらく、満足していない状況**であった。
- 経済産業省・総務省安全管理ガイドラインではベンダは医療機関がセキュリティ上の安全管理措置を講じるうえで、適切な情報提供を行うことが求められている。**ベンダは医療機関におけるITリテラシー水準を考慮したうえで、コミュニケーションの工夫を行い、医療機関はベンダと共同でITリテラシーを高める取組等を促進することが不可欠**であるといえる。

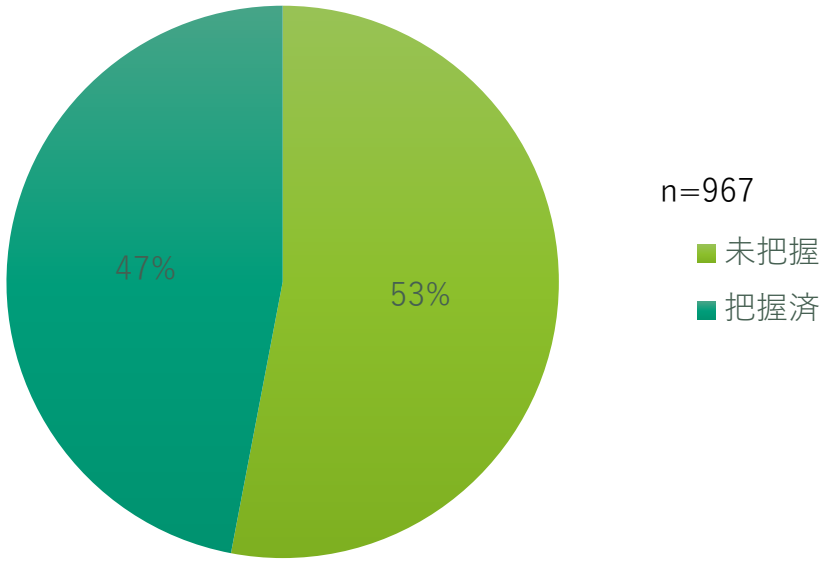
＜アンケート調査結果_全体結果(1/4)＞

【①：リモートメンテナンス用製品の利用・把握状況】

＜Q1：リモートメンテナンスを許可していると回答した組織割合＞



＜Q2. リモートメンテナンス機器情報を把握していると回答した組織割合＞

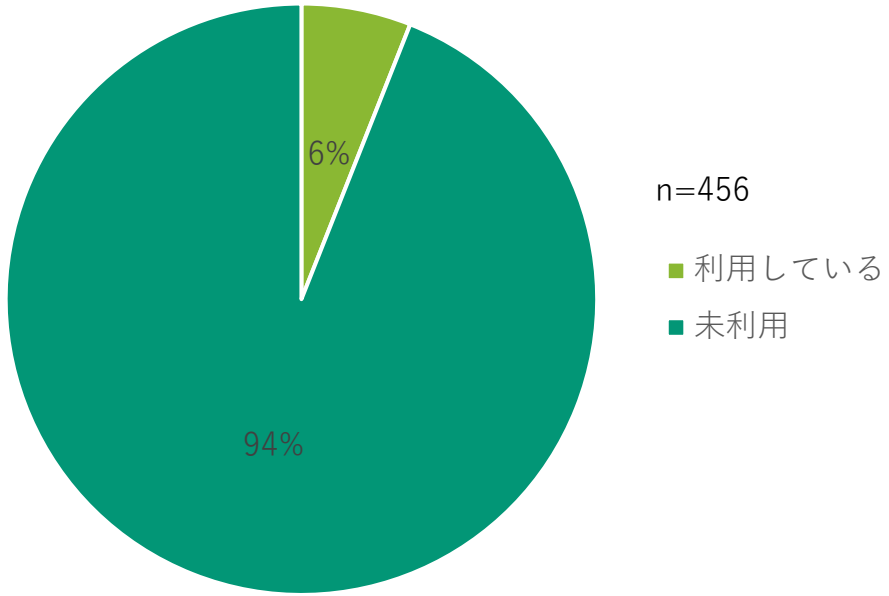


リモートメンテナンスを許可していると回答した組織は全体の７６%、そのうち**リモートメンテナンスに利用している機器・製品のバージョン情報等を把握している組織は４７%であった**。

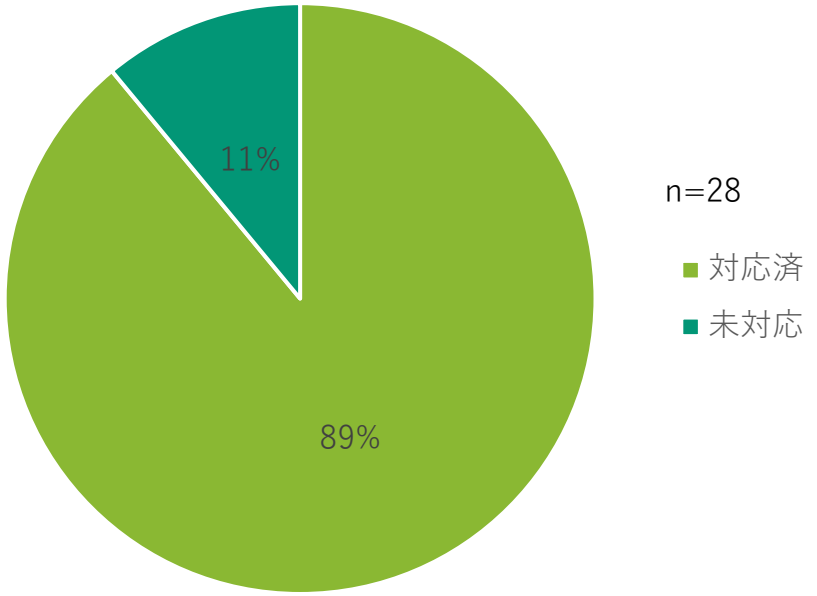
＜アンケート調査結果_全体結果(2/4)＞

【②-A：Fortinet社リモートメンテナンス用製品の利用・脆弱性対応状況】

＜Q3：22年10月に脆弱性報告されたFortinet製品を利用していると回答した組織の割合



＜Q4：脆弱性へのベンダ対応が完了していると回答した組織の割合＞

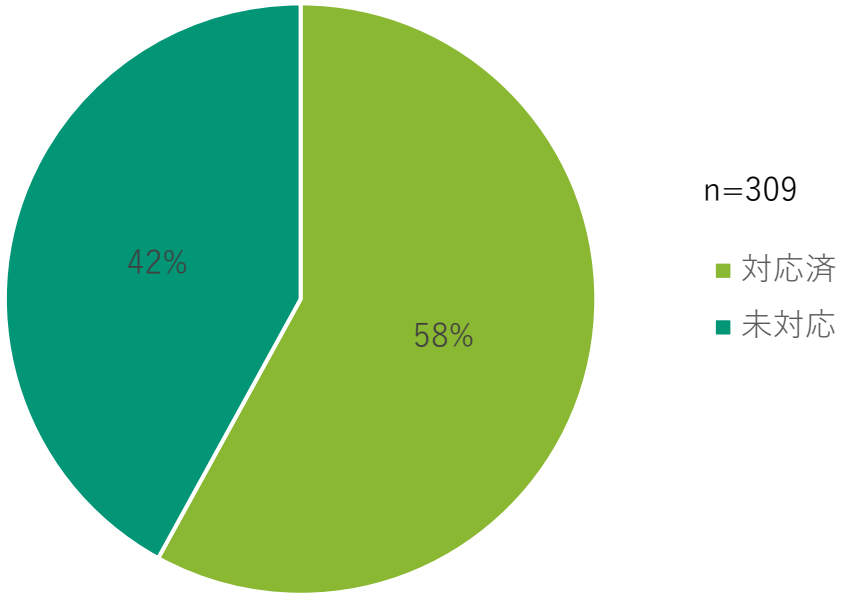


リモートメンテナンス機器・製品のバージョン情報を把握している組織の中で、２２年１０月に深刻な脆弱性が発生したForitnet社製品を利用している組織は6%、そのうち**脆弱性対応が未了の組織は1割程度**であり、ほとんどの組織で対応が完了している。

＜アンケート調査結果_全体結果(3/4)＞

【②-B：それ以外のリモートメンテナンス用製品の利用・脆弱性対応状況】

＜Q５：Q3以外のリモートメンテ機器を把握しているが、特に脆弱性対応を行っていないと回答した組織の割合＞

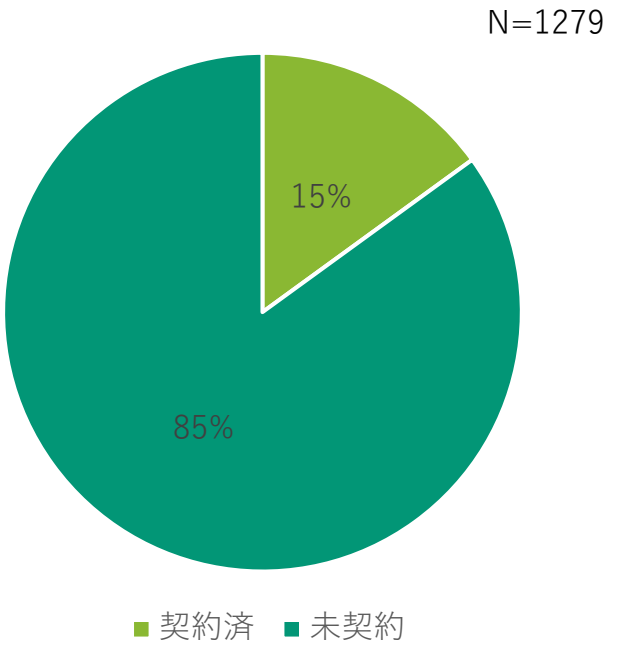


２２年１０月に深刻な脆弱性が発生したForitnet社製品以外のリモートメンテナンス機器・製品を利用している組織のうち、該当機器・製品へのセキュリティ上の脆弱性対応を行っている組織の割合は58%であり、**４割強は特段対応を実施していない**。

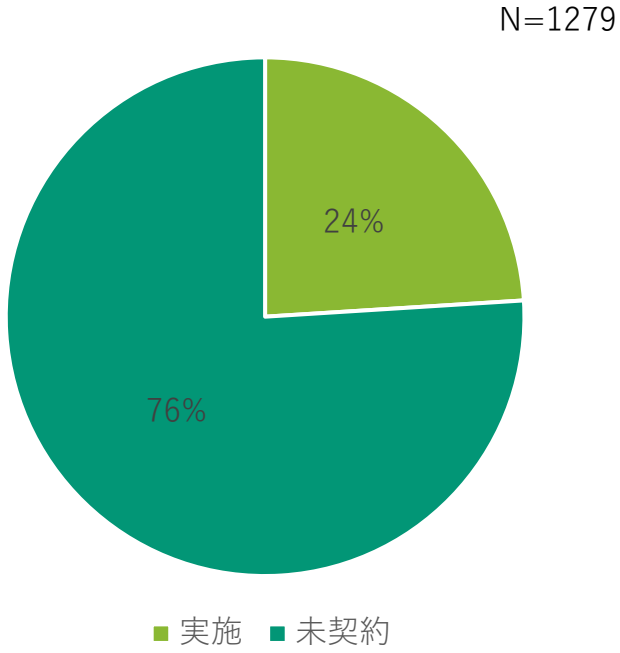
＜アンケート調査結果_全体結果(4/4)＞

【③：医療機関/ベンダーとのリスクコミュニケーション状況】

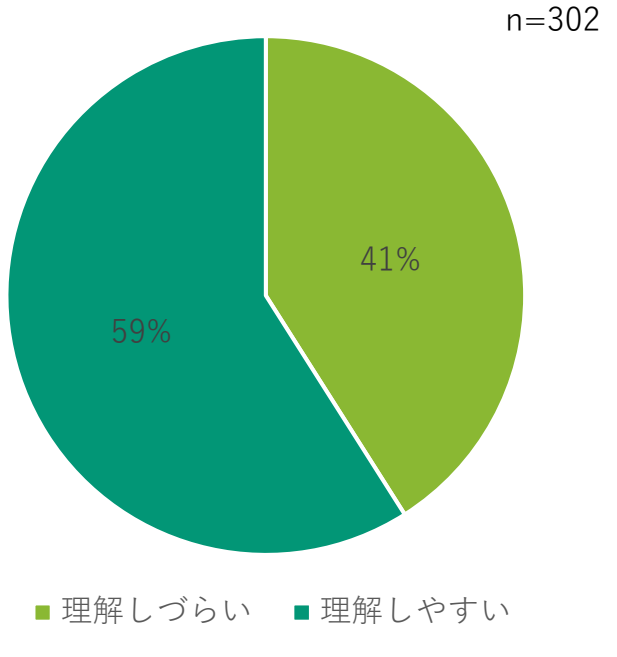
＜Q6：契約書・SLAにおけるセキュリティ責任分界を定めていないと回答した組織の割合＞



＜Q7：ベンダからの運用報告等の内容確認を行っていると回答した組織の割合＞



＜Q８：ベンダ報告は理解しづらく、院内セキュリティ向上にプラスになっていないと回答した組織の割合＞



ベンダと契約等でセキュリティの役割・責任を定めている組織の割合は**15%**、さらにベンダからセキュリティ等も含めた報告を行わせている組織は**24%にしか満たない**。
報告を受けている組織においてもその内容は理解しづらく、セキュリティ向上に資さないと回答した割合は**41%**に及んだ。

３．病床規模別結果

＜アンケート調査結果_病床規模別＞

- 病床規模別で見ると、基本的に、リモートメンテナンス導入率、及びリモートメンテナンス製品情報の把握率ともに、**病床規模が大きいほど高くなる**傾向がある。

- Fortinet社製品の利用率は今回のアンケート結果からは**いずれの病床規模区分においても利用率は低く**、さらに利用している組織においてほぼ22年10月の深刻な脆弱性対応は完了している状況である。

- 一方、Fortinet社以外のリモートメンテナンス機器の種別・バージョン情報等を把握しているにもかかわらず、脆弱性の対応を最新情報に基づき実施していないと回答した組織は**病床規模が小さいほど多く見られる**傾向があった。病床の小さい医療機関では**Fortinet社以外の製品を用いたリモートメンテナンス機器の脆弱性が悪用されるリスク**が高いといえる。

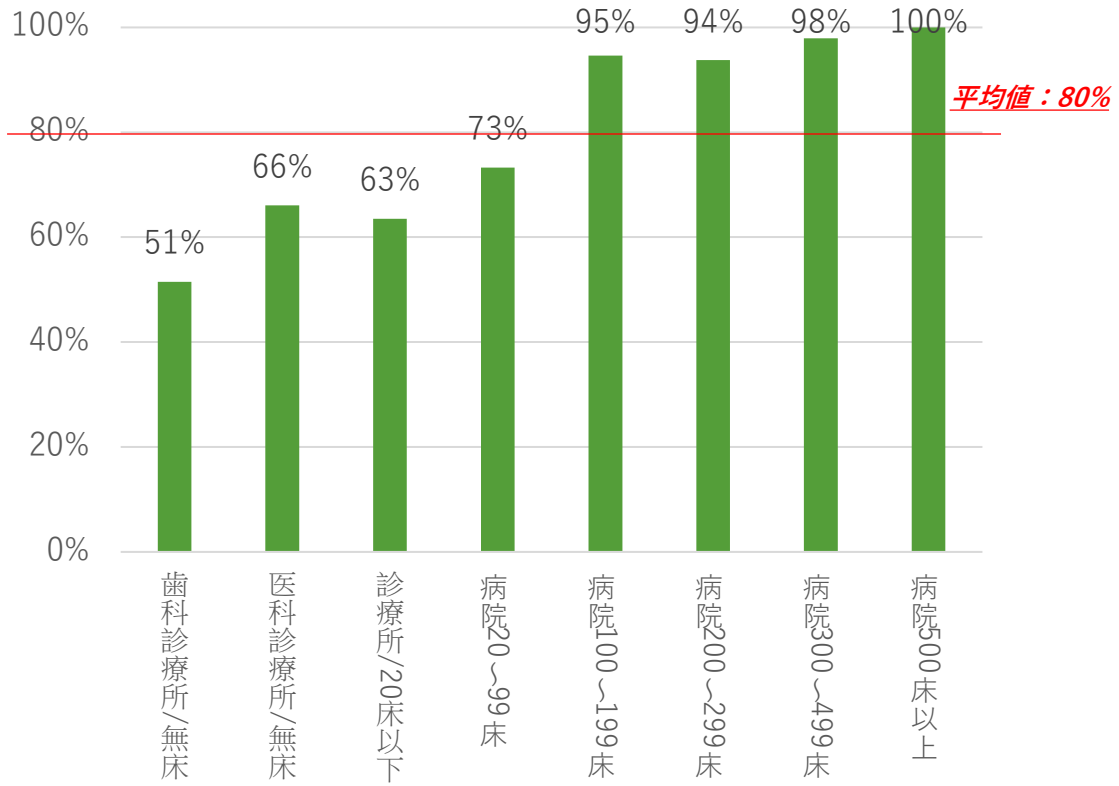
- セキュリティ上の役割・責任をベンダと契約等で締結・合意形成している組織、及び厚生労働省安全管理GLが求める、ベンダからセキュリティ等も含めた情報提供・報告を定期的に受け、確認している組織は、**病床規模が小さいほど割合が少ない**状況である。

- なお、ベンダからの報告内容が医療機関の職員にとって理解しづらく、院内セキュリティ向上に役立ないと回答する組織は、全ての病床規模区分で共通的に存在している状況である。**ベンダと医療機関におけるセキュリティ情報の非対称性という問題は特定の病床に限定されない、構造的な課題であることが浮き彫りになっている**。

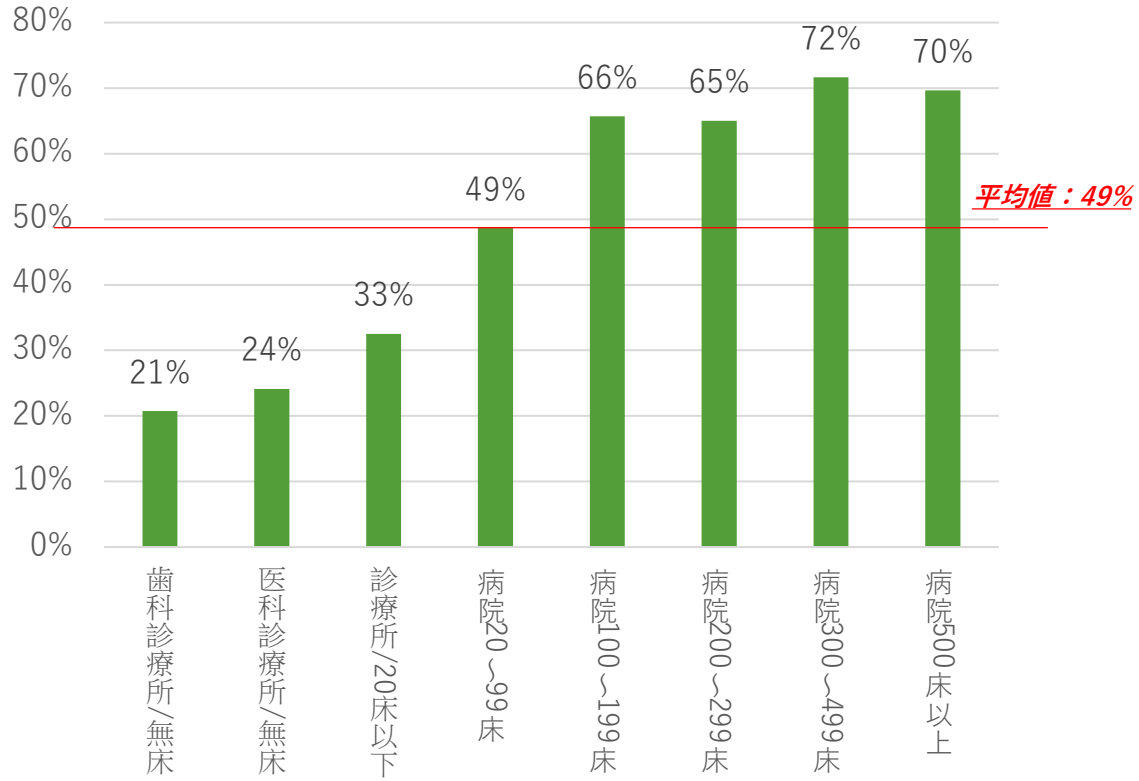
＜アンケート調査結果_病床規模別(1/4)＞

【①：リモートメンテナンス用製品の利用・把握状況】

＜Q1：リモートメンテナンスを許可していると回答した組織割合＞



＜Q2. リモートメンテナンス機器情報を把握していると回答した組織割合＞

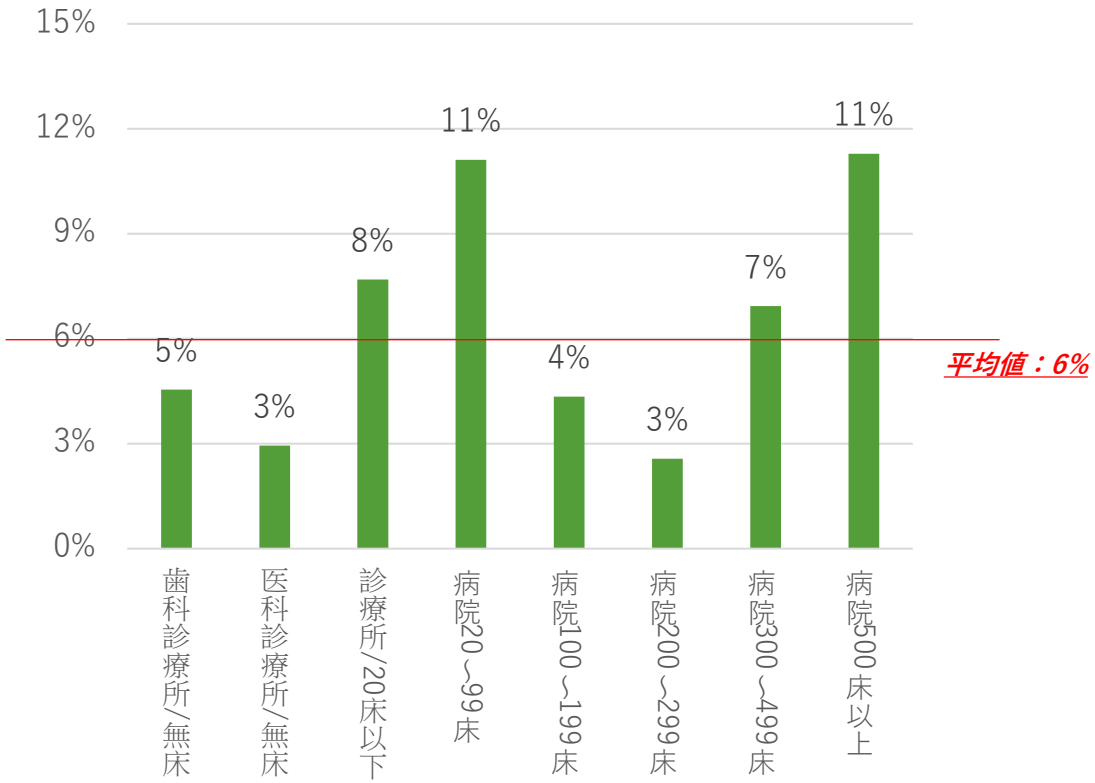


リモートメンテナンス導入率、及び該当機器の種別・バージョン情報の把握率は、**病床規模が大きいほど高まる**傾向がある。

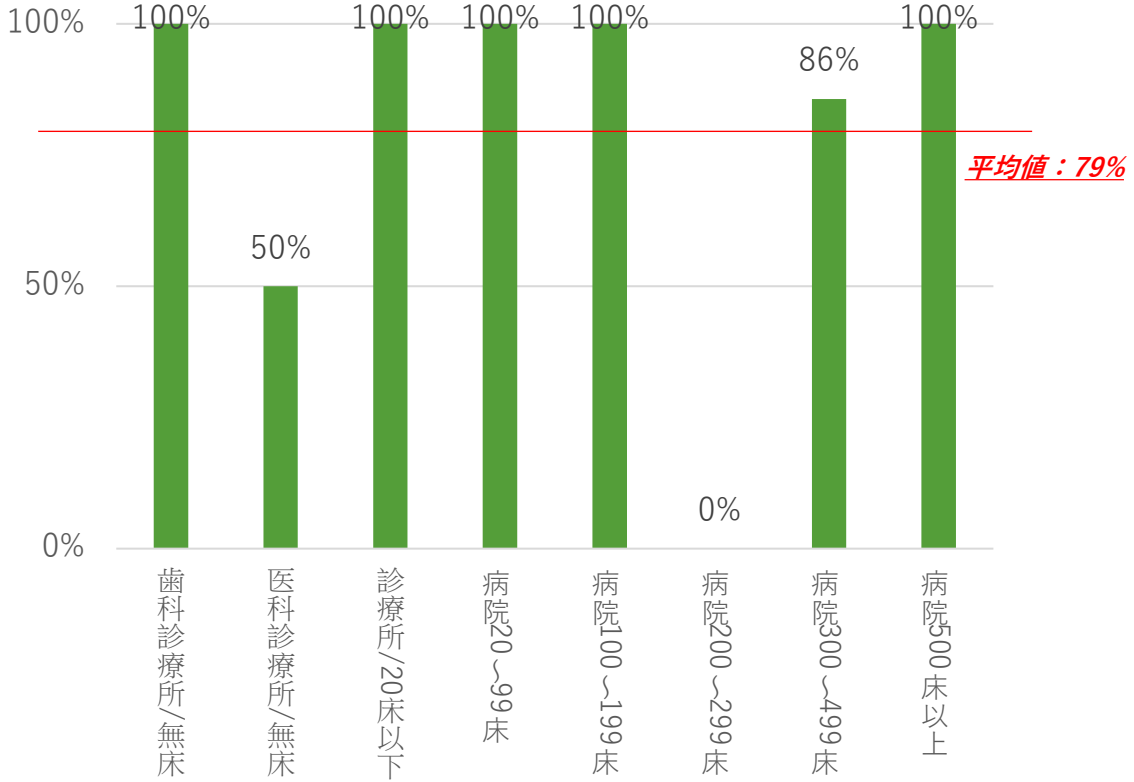
＜アンケート調査結果_病床規模別(2/4)＞

【②-A：Fortinet社リモートメンテナンス用製品の利用・脆弱性対応状況】

＜Q3：22年10月に脆弱性報告されたFortinet製品を利用していると回答した組織の割合＞



＜Q4：脆弱性へのベンダ対応が完了していると回答した組織の割合＞

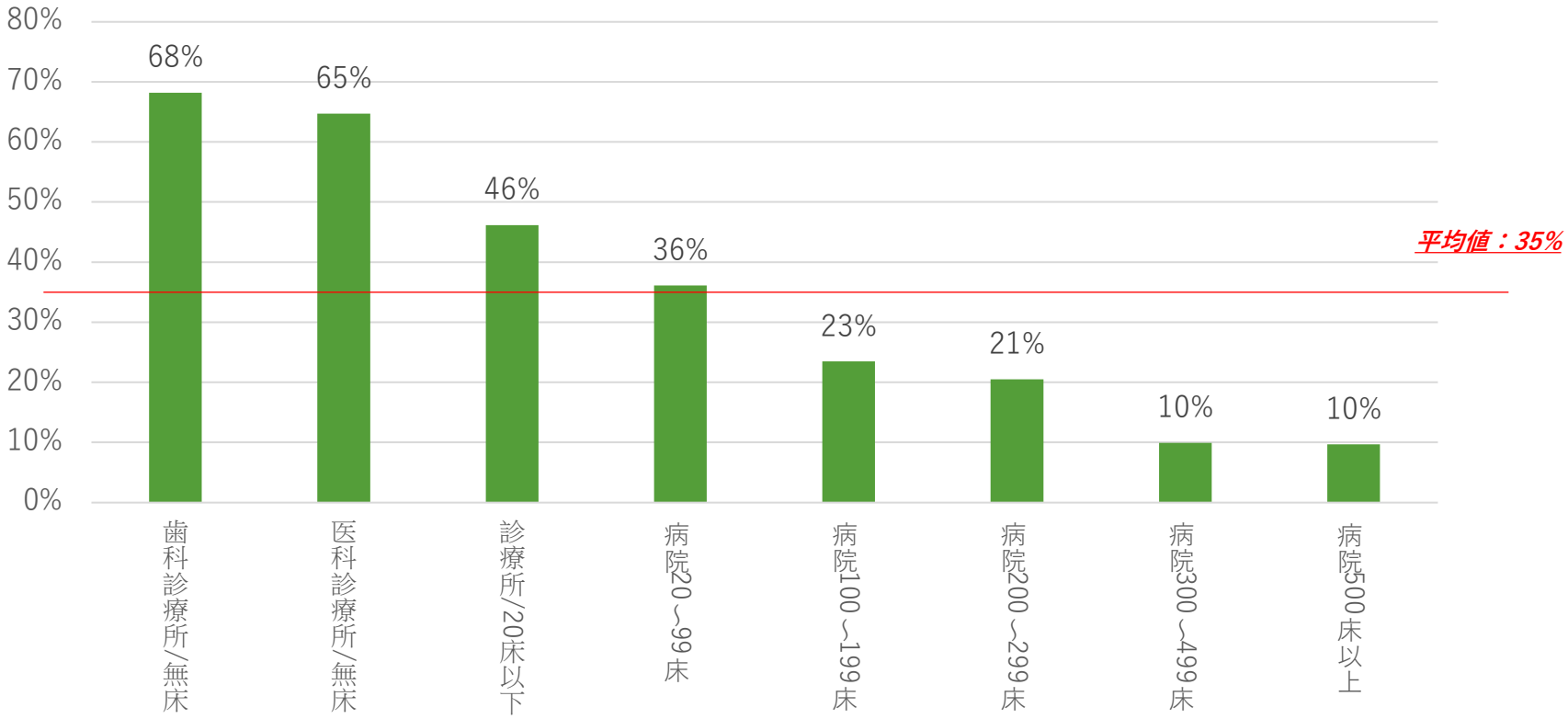


22年10月に脆弱性報告されたFortinet社製品の利用率は**いずれの病床規模においても低く、いずれの区分の組織においても対応がほぼ完了**している。

＜アンケート調査結果_病床規模別(3/4)＞

【②-B：それ以外のリモートメンテナンス用製品の利用・脆弱性対応状況】

＜Q５：Q3以外のリモートメンテ機器を把握しているが、特に脆弱性対応を行っていないと回答した組織の割合＞

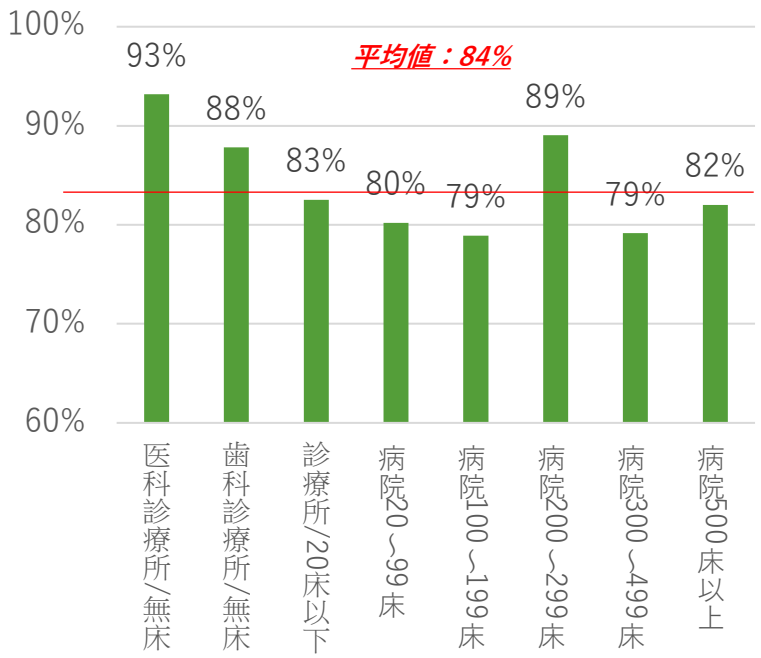


Fortinet社製品以外のリモートメンテナンス機器の種別・情報等を把握しながら、脆弱性対応を行っていない組織の割合は、**病床規模が小さいほど高くなる**傾向が見受けられる。

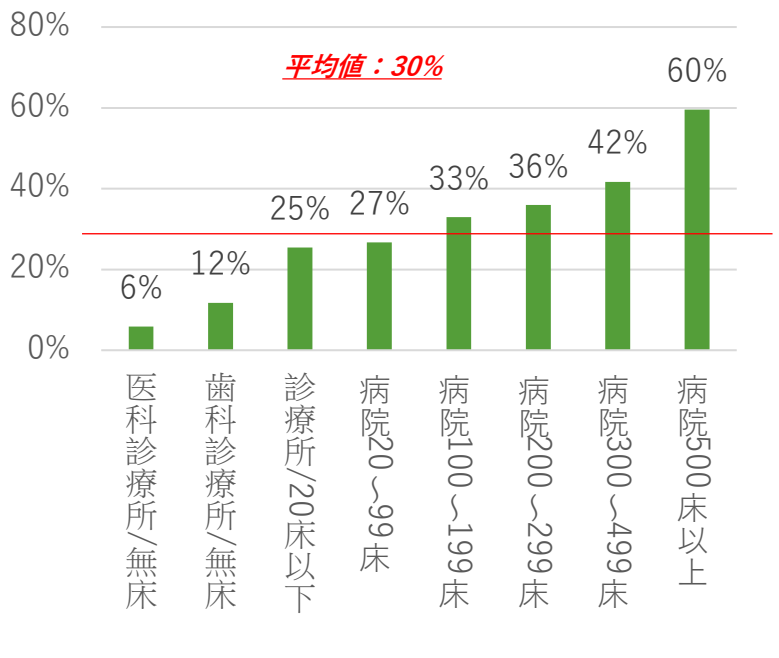
＜アンケート調査結果_病床規模別(4/4)＞

【③：医療機関/ベンダーとのリスクコミュニケーション状況】(1/2)

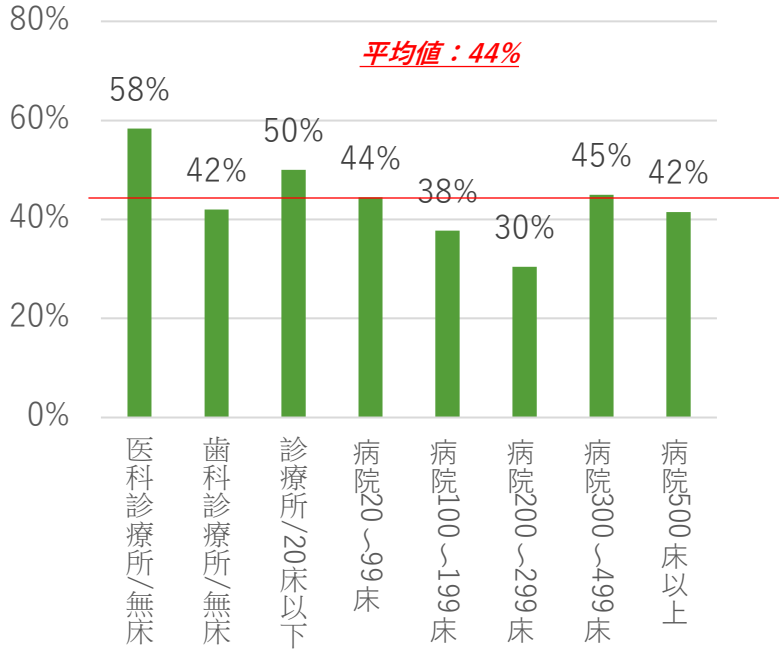
＜Q6：契約書・SLAにおけるセキュリティ責任分界を定めていないと回答した組織の割合＞



＜Q7：ベンダからの運用報告等の内容確認を行っていると回答した組織の割合＞



＜Q８：ベンダ報告は理解しづらく、院内セキュリティ向上にプラスになっていないと回答した組織の割合＞



セキュリティ責任分界の契約書での合意形成、ベンダからの運用報告確認も**病床規模が大きいほど実施率が高い**傾向がある。
ただし、ベンダの報告・情報提供が医療機関のセキュリティ向上に役立っていないという回答率は、**いずれの病床においても平均値からの大幅な落差はなく、医療機関/ベンダ間のセキュリティ情報の非対称性は全体的な課題としてある**ことが想定される。

４．その他

その他分析

日本病院会のアンケート回答結果（382施設）のうち、**利用率の高い上位4社の電カルベンダを対象に、以下３つの調査項目で検討**を行うことで、電カルベンダとのセキュリティ面を含む契約率、ベンダ報告確認状況、ベンダ報告内容の分かりやすさについて分析を行った。

■対象ベンダ

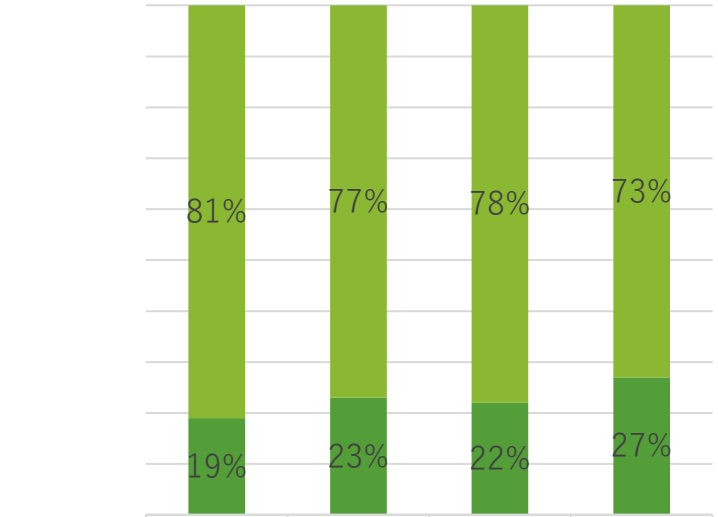
電カルベンダ	導入数	（参考）医事会計システム導入ベンダ該当数
A社	１４１件	146件
B社	６４件	64件
C社	６０件	74件
D社	２２件	2件

■検討項目

① 契約書・SLAにおけるセキュリティ責任分界の定義・締結を電カルベンダベンダと行っているか
② 電カルベンダからの運用報告等の内容確認を行っているか（医療機関が確認すべき水準の内容について、ベンダが報告を行っているか）
③ ②が「はい」の場合、電カルベンダからの報告・情報提供内容は、理解しづらく、院内セキュリティ向上に役立たないものか？

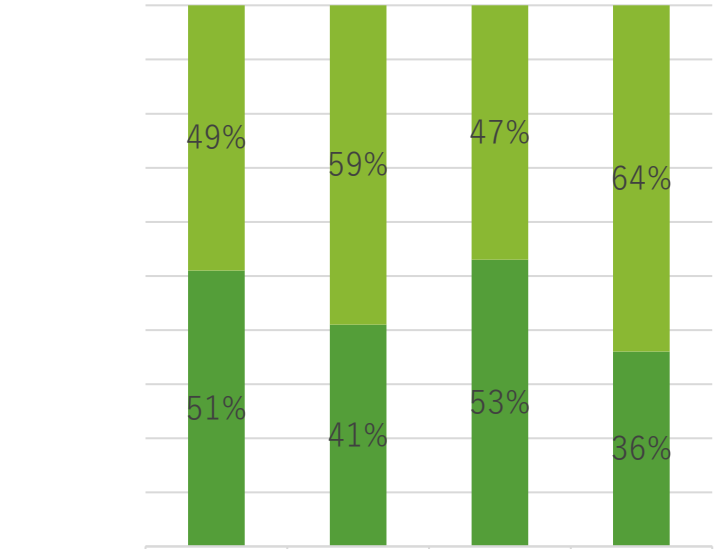
分析結果

①：契約書・SLAにおけるセキュリティ責任分界の定義・締結を電カルベンダと行っているか



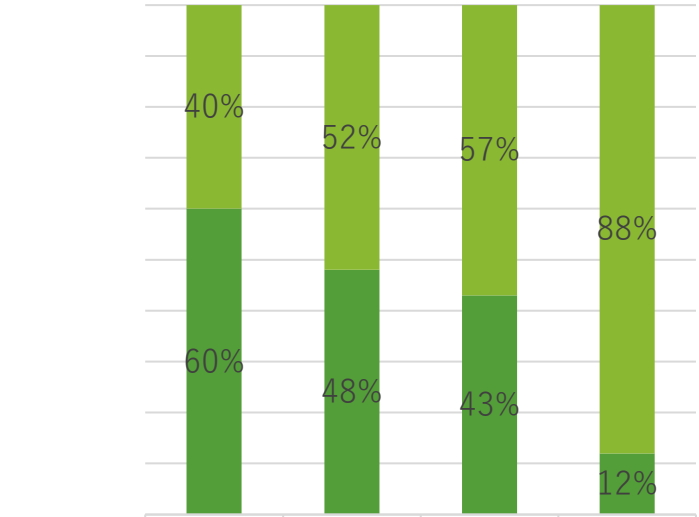
	A社	B社	C社	D社
いいえ	81%	77%	78%	73%
はい	19%	23%	22%	27%

②：電カルベンダからの運用報告等の内容確認を行っているか



	A社	B社	C社	D社
いいえ	49%	59%	47%	64%
はい	51%	41%	53%	36%

③：②が「はいの場合」、電カルベンダからの報告・情報提供内容は、理解しづらく、院内セキュリティ向上に役立たないものか？



	A社	B社	C社	D社
いいえ	40%	52%	57%	88%
はい	60%	48%	43%	12%

※すべての質問ともに、「いいえ」は「わからない」も含む

電カルベンダとの間で**セキュリティに係る契約締結は全体の2割程度**しか行われていない。
電カルベンダからの運用報告の確認は**医療機関の半数程度が行っているが、その内容の分かりやすさ・セキュリティ上の有用性にはベンダごとに差がある**ことがわかる。


Medical Information
Sharing and Analysis Center