一般社団法人医療ISAC

全国保険医団体連合会
セキュリティアンケート調査結果

国民医療の向上をめざす
全国保険医団体連合会

調査の背景・目的

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Fortinet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**。

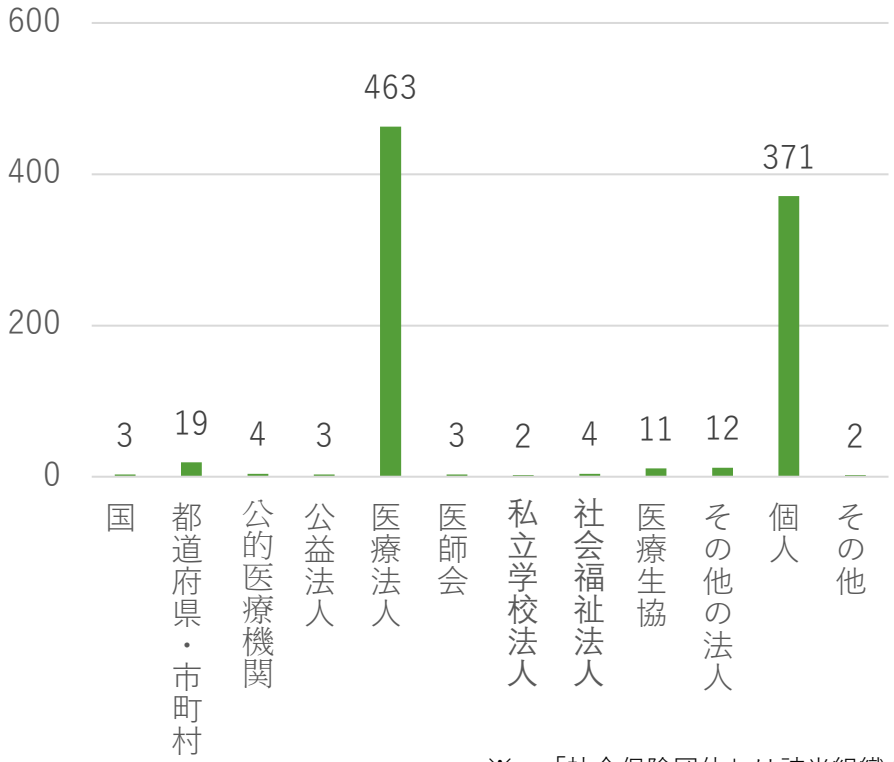
一方、2022年1月～2月にかけての四病院団体協議会加盟組織のアンケート結果からも把握できる通り、**国内の医療機関の多くは経済的・人的リソース不足により、こうした製品の脆弱性管理も含めて、医療情報システムのセキュリティ管理業務は外部ITベンダに依存せざるを得ない状況**である。
医療機関の基幹系システム＝電子カルテシステムには高い可用性が求められることから、リモートメンテナンス接続経路が外部ITベンダにより設置されることはほぼ一般的である。こうしたリモートメンテナンスの保守業務も医療情報システムを提供する外部ITベンダに医療機関では委託しているが、**その役割関係を明確に契約上で定義すること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と共同で、本会に所属する病院・診療所に対して**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、その結果を分析する。

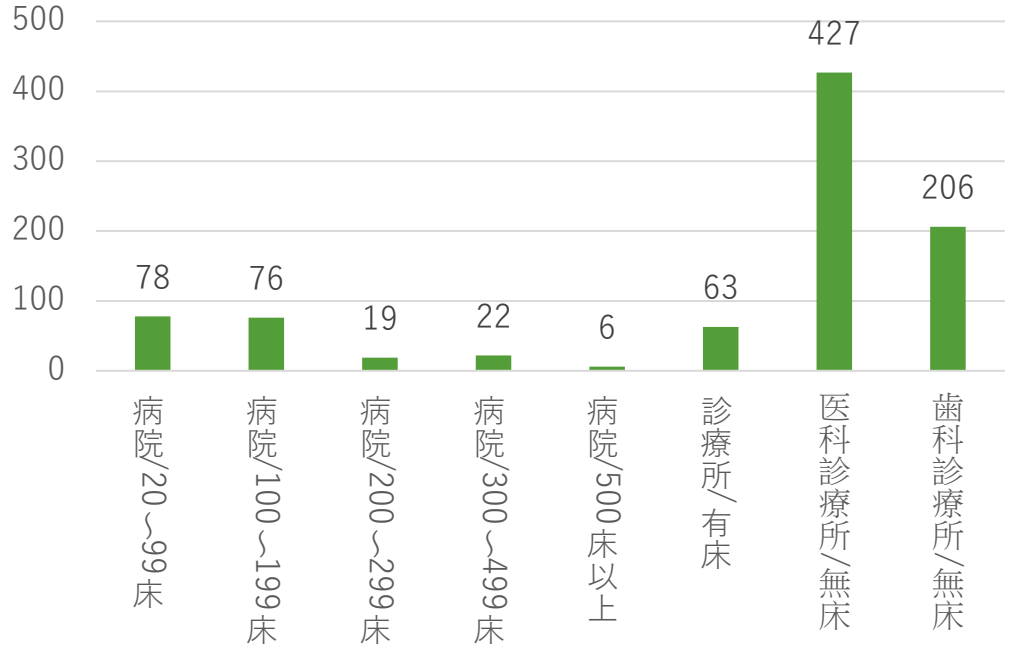
調査対象

- 実施期間：2022年11月15日～12月26日
- 調査対象組織数：107,409人（全国保険医団体連合会加盟組織）
- 回答組織数：897組織

＜開設者別内訳＞



＜病床別内訳＞



※：「社会保険団体」は該当組織なし

調査項目

調査項目は以下の4つのカテゴリに基づき実施し、回答はすべて「はい」「いいえ（わからない）」のいずれかを選択するものとした。

【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Fortinet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、Fortinet社以外のリモートメンテナンス用の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)

1. 全体結果

＜全体結果総評＞

- アンケート回答した組織全897件のうち、院内システムにリモートメンテナンス環境を導入している組織は全体の7割に達しているが、**院内でどのようなリモートメンテナンス機器が利用されているかについて正確に把握している組織はそのうち3割程度**であった。

- 2022年10月に深刻な脆弱性の報告のあったFortinet社製品を利用している組織のうち9割近くが脆弱性対応を行っている一方で、**それ以外の製品を利用している組織の5割強は脆弱性への対応を特に行っていない状況**であった。
- Fortinet社製品の脆弱性の警告・報道が多く行われるなか、該当製品の脆弱性リスクへの意識は高まっているものの、**それ以外の製品についてのリスク認識はまだ十分でない。**
- Fortinet社製品か否かを問わず、リモートメンテナンス用機器には外部からの悪意あるアクセスを可能にしかねない脆弱性が継続的に発生し、適時の対応が求められるものである。そうしたリスク認識をしっかり持つことが医療機関にも求められる。

- ベンダとセキュリティ対応を含めた契約上の役割・責任を定めた契約を取り交わしている医療機関は全体の1割強であり、**9割弱はそうした取り交わしを行っていない状況**である。
- 契約を取り交わしている医療機関の割合が、ベンダからの定期報告を受け、内容を確認している医療機関の割合とほぼ同率であることを考慮した場合、ベンダとしては、**医療機関との間でセキュリティの役割・責任を含めた契約・SLAを明示的に取り交わさない限り、医療機関とのリスクコミュニケーションが難しい**という一面がうかがえる。これは商慣習上の当然事であり、医療機関はベンダとの間で明確なセキュリティも含めた契約関係を合意し、ベンダの協力を仰げる態勢を整備することこそが重要といえる。

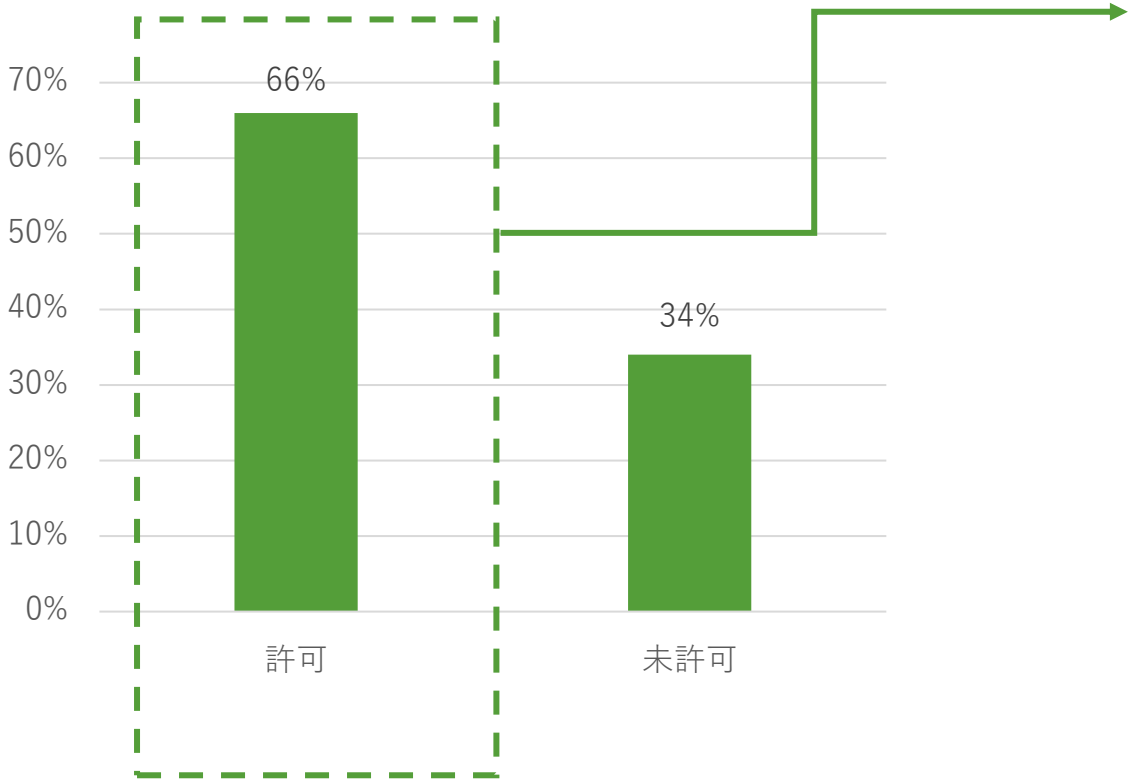
- 一方、ベンダからの報告内容については、**医療機関として理解しづらく、セキュリティ向上に役に立たないとの回答した組織が4割強存在**した。
- 経済産業省・総務省安全管理GLが求める、医療機関が安全管理措置を講じるためのサポート役として、**医療機関と同じ目線に立ち、ベンダが医療セキュリティの改善に向けたリスクコミュニケーションの工夫を凝らす**とともに、医療機関側のセキュリティリテラシーの向上も重要課題の一つといえる。

＜アンケート調査結果_全体(1/5)＞

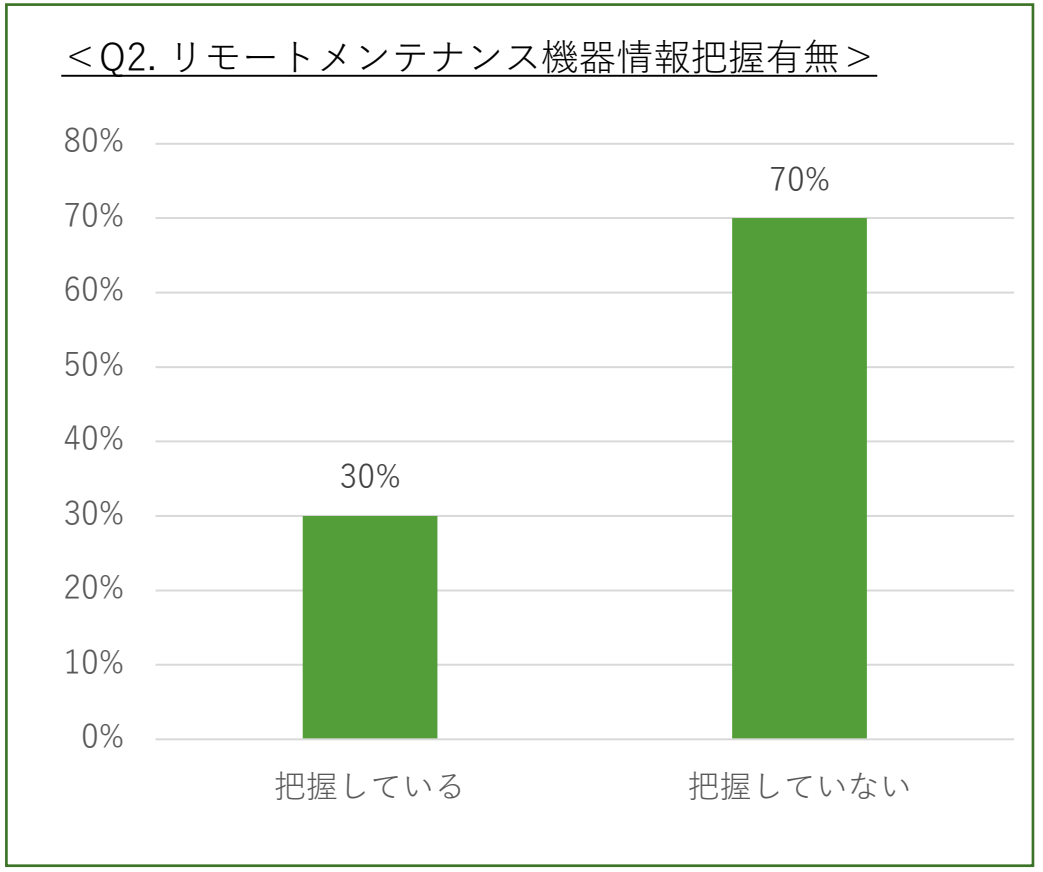
【①：リモートメンテナンス用製品の利用・把握状況】

- 院内システムへのリモートメンテナンスを許可している組織は全体の7割弱であり、そのうちどのようなリモートメンテナンス機器が利用されているかについての情報を把握している割合は3割程度。
- **<u>7割の組織は院内のリモートメンテナンス機器の情報が把握できていない</u>**状況である。

＜Q1：リモートメンテナンス許可有無＞



＜Q2. リモートメンテナンス機器情報把握有無＞

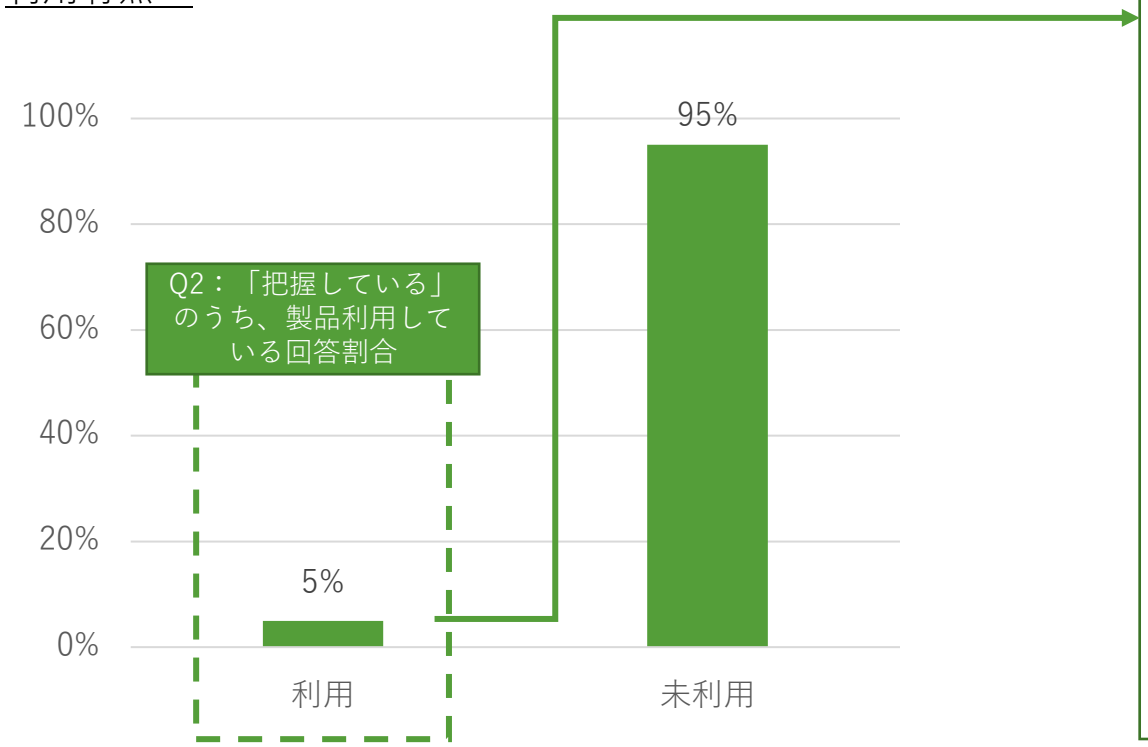


＜アンケート調査結果_全体(2/5)＞

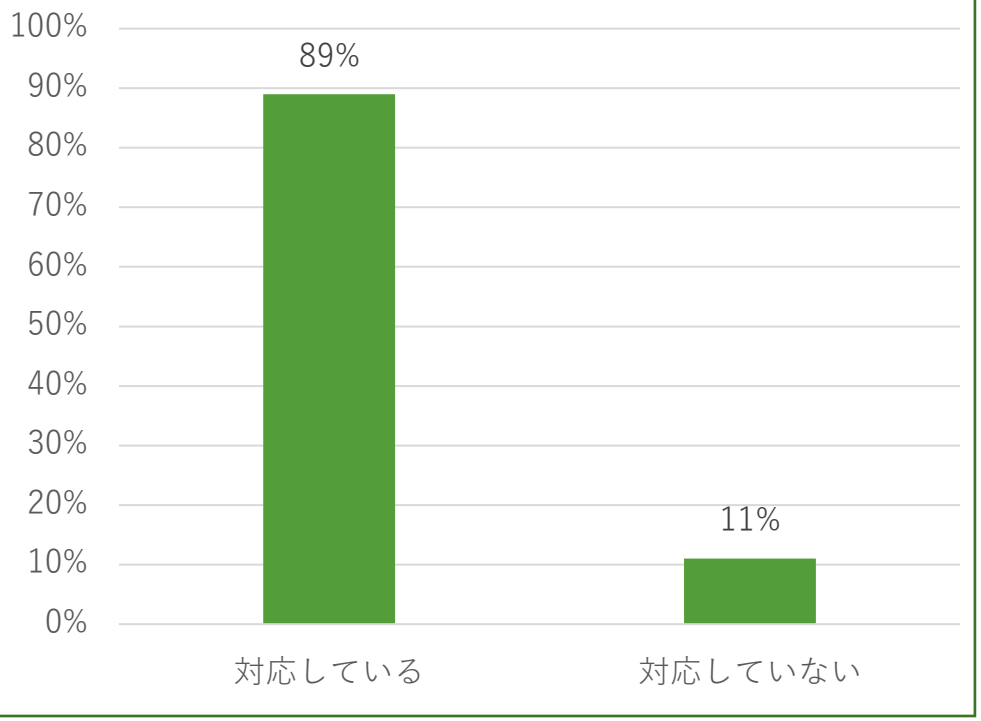
【②-A：Fortinet社リモートメンテナンス用製品の利用・脆弱性対応状況】

- 22年10月に脆弱性報告されたFortinet製品を利用していた割合は、**リモートメンテナンス機器情報を把握している組織全体の5%程度であり、そのうち9割近くは脆弱性対応が図られている**。

＜Q3：22年10月に脆弱性報告されたFortinet製品の利用有無＞



＜Q4：脆弱性へのベンダ対応の有無＞

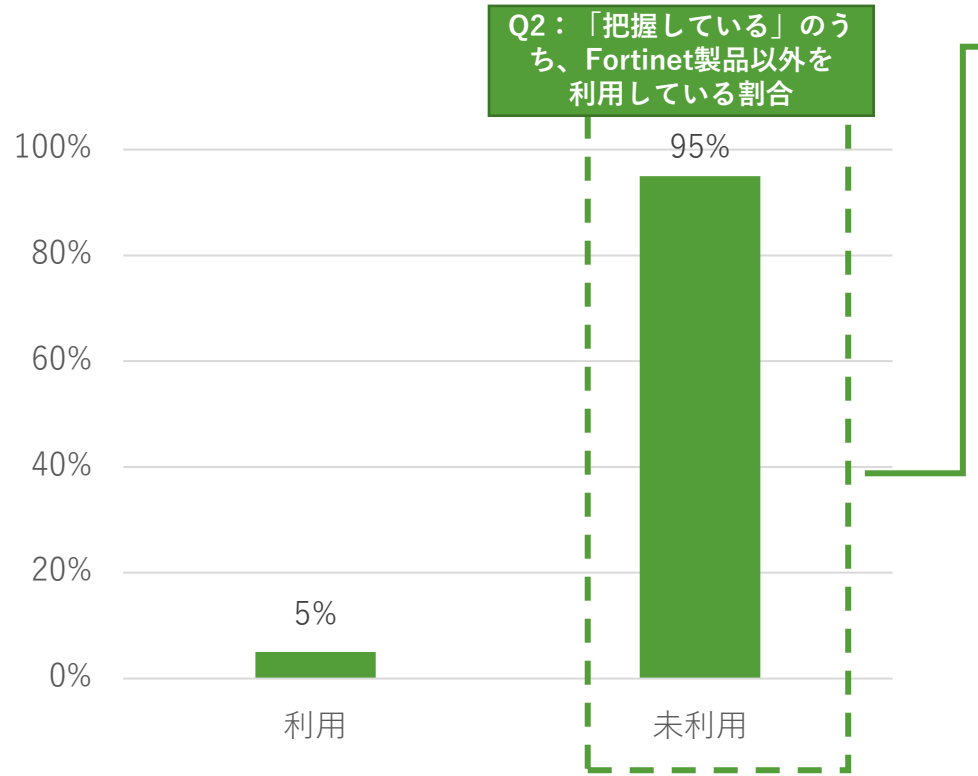


＜アンケート調査結果_全体(3/5)＞

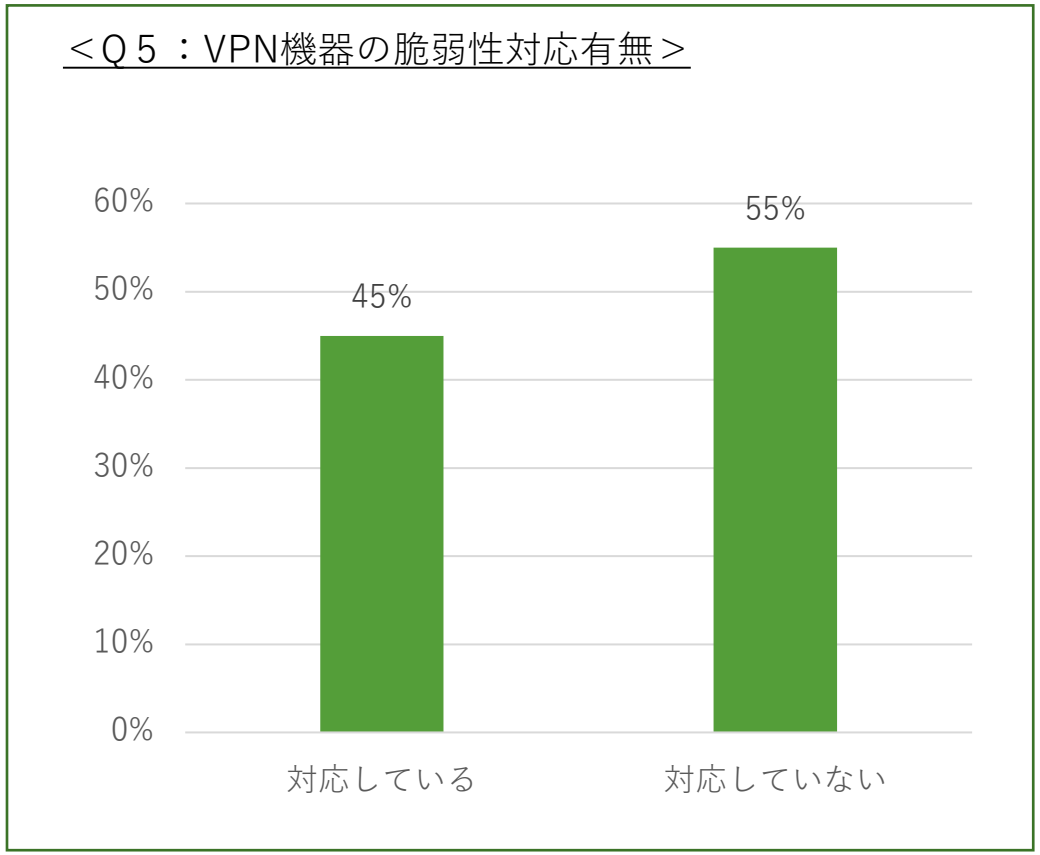
【②-B：それ以外のリモートメンテナンス用製品の利用・脆弱性対応状況】

- 一方、22年10月に脆弱性報告されたFortinet社製品以外のリモートメンテナンス機器を利用している組織のうち、**該当機器の脆弱性対応を行っているとの回答割合は5割以下**であった。

＜Q3：22年10月に脆弱性報告されたFortinet製品の利用有無＞



＜Q５：VPN機器の脆弱性対応有無＞

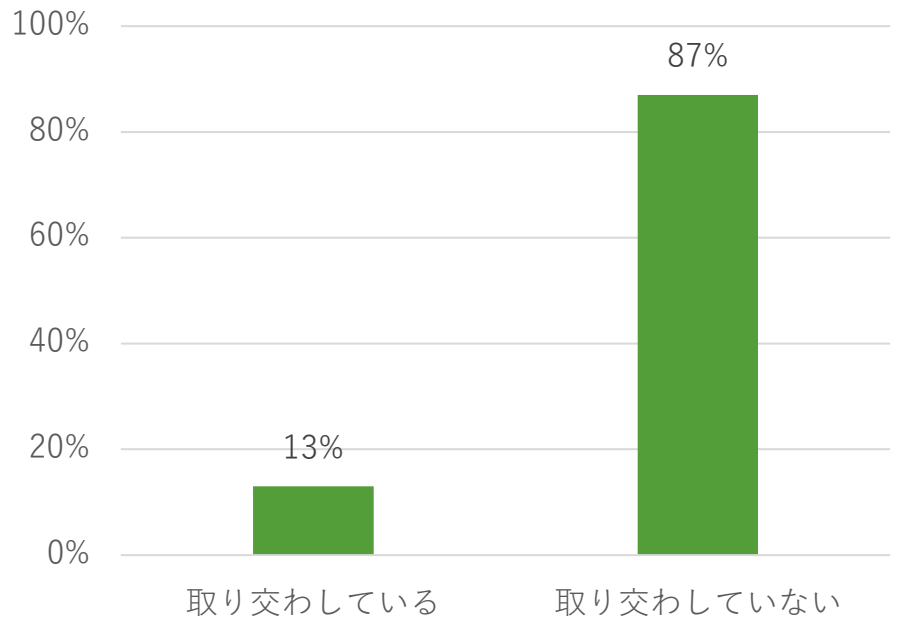


＜アンケート調査結果_全体(4/5)＞

【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)

- 院内システムにおける保守等の契約・SLA等においてセキュリティ上の役割・責任を外部ITベンダと取り交わしている組織は、全体の1割強程度であり、**9割弱はそのような契約上の取り決めを行っていない状況**である。

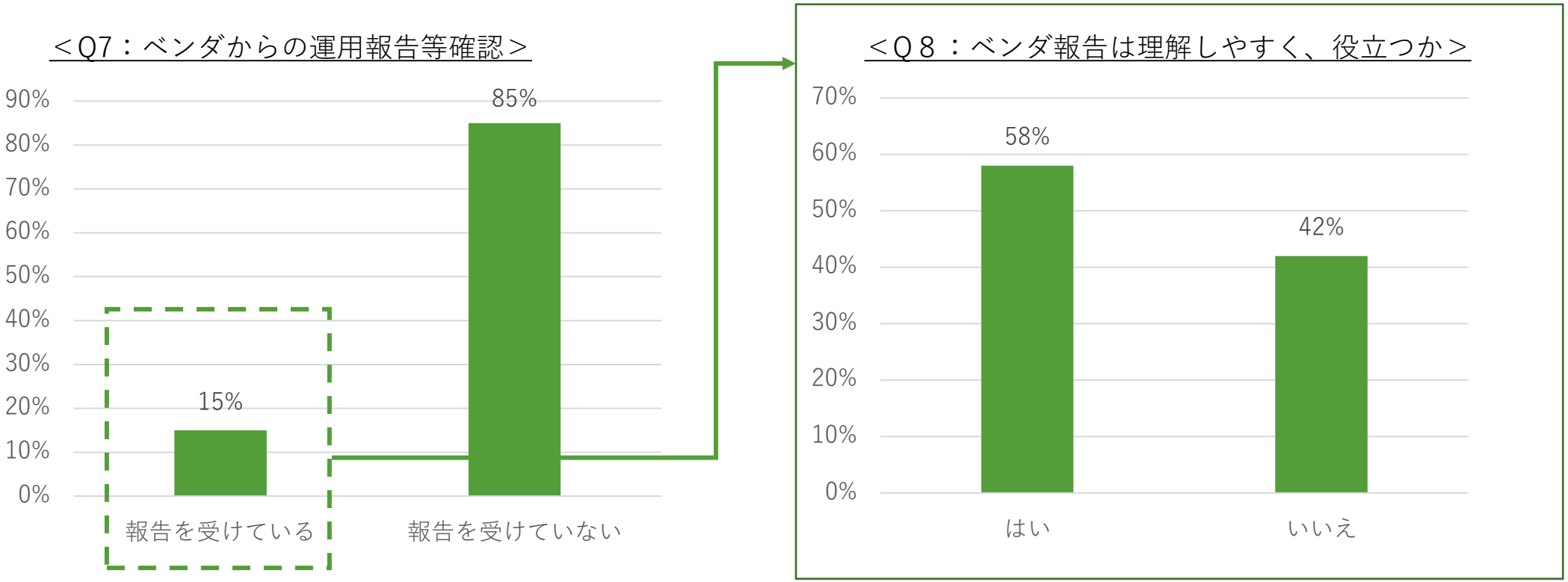
＜Q6：契約書におけるセキュリティ責任分界の定義＞



＜アンケート調査結果_全体(5/5)＞

【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】(2/2)

- 厚労省安全管理GLに基づき、ベンダからのシステム運用状況等について、機器の脆弱性情報等も含めて、**定期的な報告を受けている組織の割合は1割強程度**である。
- これらの組織においてベンダからの報告内容に満足している組織は全体の6割弱に及ぶが、**4割強はその報告内容は理解しづらく、リスクコミュニケーションに求められる分かりやすさを満たしていないとの回答**であった。



2. 病床規模別調査結果

＜病床規模別総評＞

- 病床規模別にみると、全体的に、リモートメンテナンス用機器の情報把握、機器の脆弱性対応、セキュリティ上の役割・責任を契約等でベンダとの合意形成等、**セキュリティの取組率は病床数が小さいほど低く、特に診療所（無床/有床、医科・歯科問わず）にその傾向は強いと**言える。これは経済的・人的セキュリティリソースに構造的に乏しい国内の医療機関固有の現象と言える。

- 2022年10月に深刻な脆弱性が報告されたFortinet社製品の脆弱性対応は無床/有床診療所も含めてほぼ対応が図られている。
- しかしながら、**Fortinet社製品以外のリモートメンテナンス用機器への脆弱性対応率は、診療所のみでなく、20床以上の病院も含めて低い**状況であった。
- 特に今回アンケートに回答した組織のうち、200床以上の病院群はFortinet社以外のリモートメンテナンス用機器をすべて(100%)導入しているにもかかわらず、その脆弱性対応は半数（50%)、あるいはそれ以下となっており、**大規模病院においても未だリモートセキュリティ上の懸念が残る状況**と言える。
- 医療機関は、製品メーカにとらわれず、外部との接続に用いる機器等にセキュリティ上の脆弱性が発生するリスクを適切に認識する必要がある。

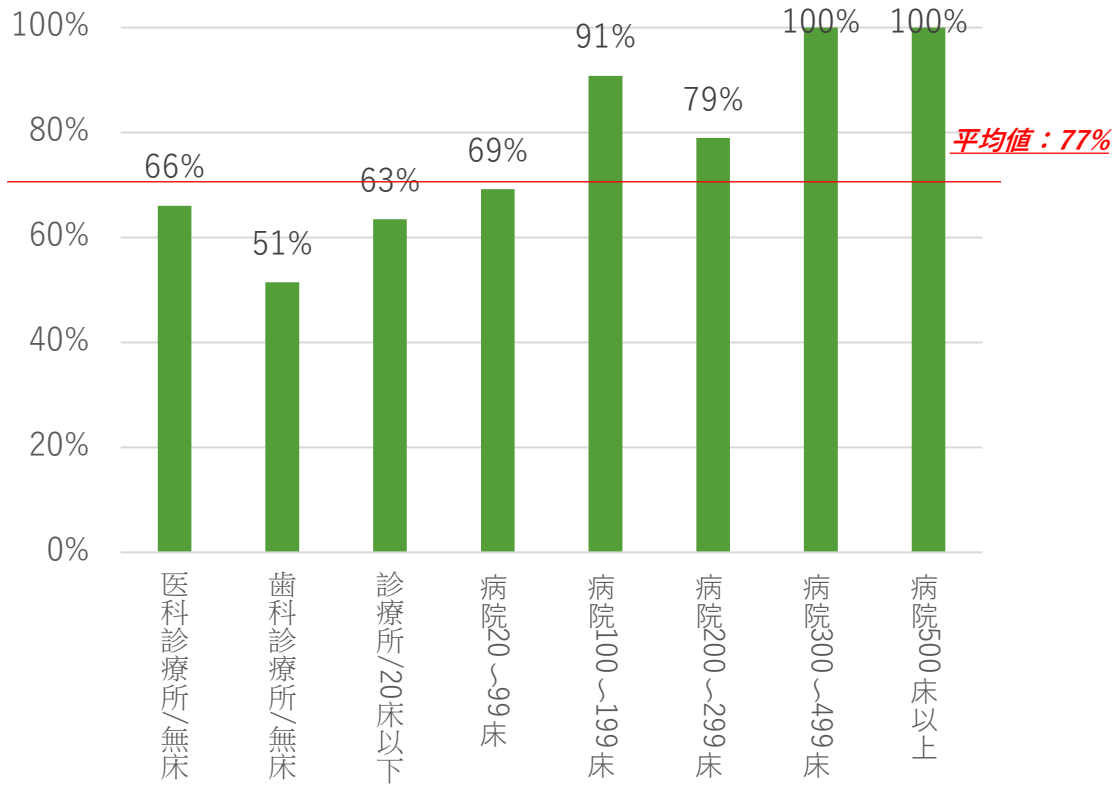
- 医療機関におけるベンダとのセキュリティ責任分界も含めた契約締結率は**医科・歯科の無床診療所、及び200床～299床病院群という層において全体平均より低い**状況である。
- これらの層は、ベンダからのセキュリティ含めた運用状況の報告内容の確認率、その報告内容への満足度も**相対的に低い状況**である。
- 医療機関が求めるベンダ報告が十分でないことがセキュリティ面の契約締結率の低さをもたらすのか、あるいはその逆であるのか、「鶏が先か卵が先か」は不明だが、少なくとも、**これらの層において、セキュリティ責任分界を含めた契約率の低さ/運用報告内容の確認率/その内容への満足度率が循環的に影響を及ぼしていることは確実**だと思われる。

＜アンケート調査結果_病床規模別(1/5)＞

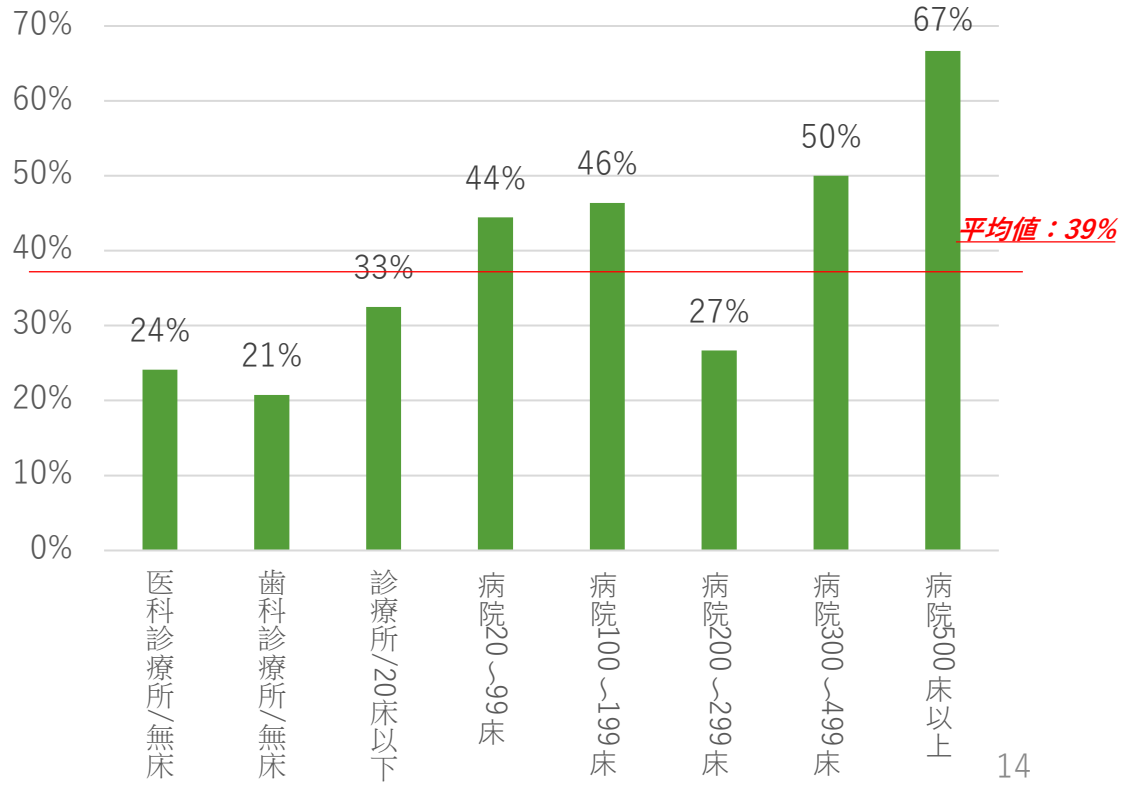
【①：リモートメンテナンス用製品の利用・把握状況】

- 一般的に、病床数の増大に応じて院内システムも増加し、それに伴いリモートメンテナンス導入率も高まる傾向がうかがえる。
- リモートメンテナンス用機器の情報の把握率も**基本的には病床規模の増加にしたがって高まる傾向**がある。
- 全体平均を下回るものは、**無床、有床（20床以下）、200床～299床病院群**であった。

＜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＞

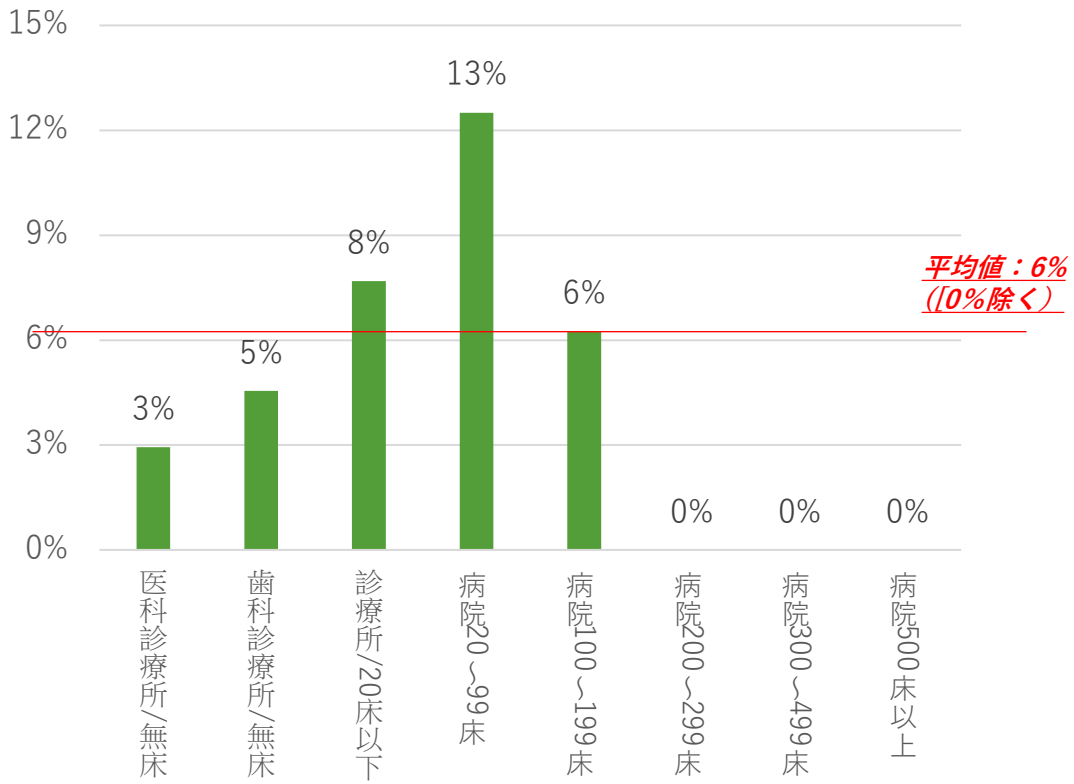


＜アンケート調査結果_病床規模別(2/5)＞

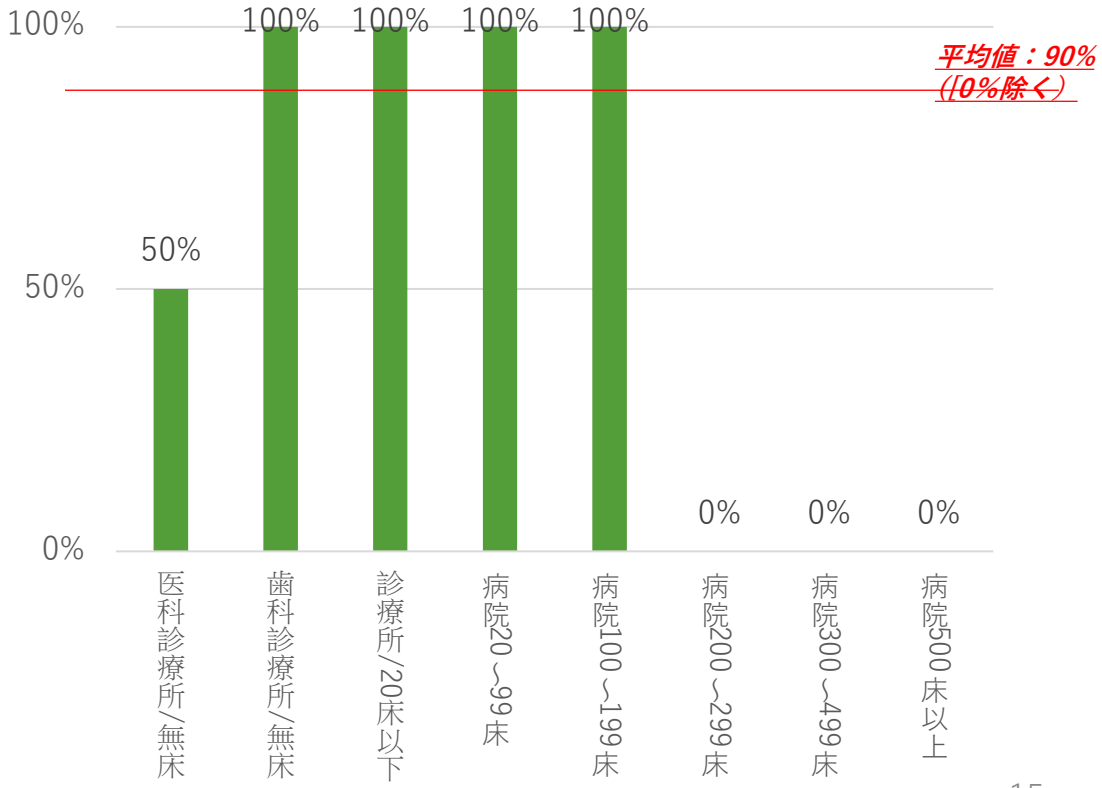
【②-A：Fortinet社リモートメンテナンス用製品の利用・脆弱性対応状況】

- 全体結果でも言及した通り、22年10月に深刻な脆弱性が報告されたFortinet社製品を利用する医療機関は今回のアンケート結果からは非常に少ない状況である。また脆弱性対応もすでに実施済みとの回答が平均9割となっている。

＜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＞

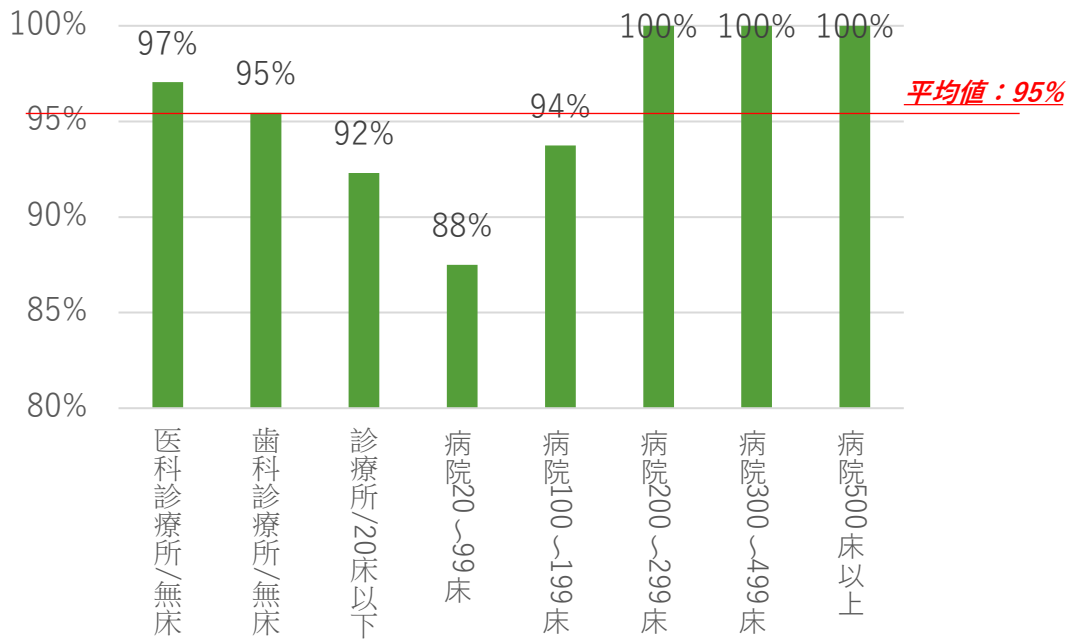


＜アンケート調査結果_病床規模別(3/5)＞

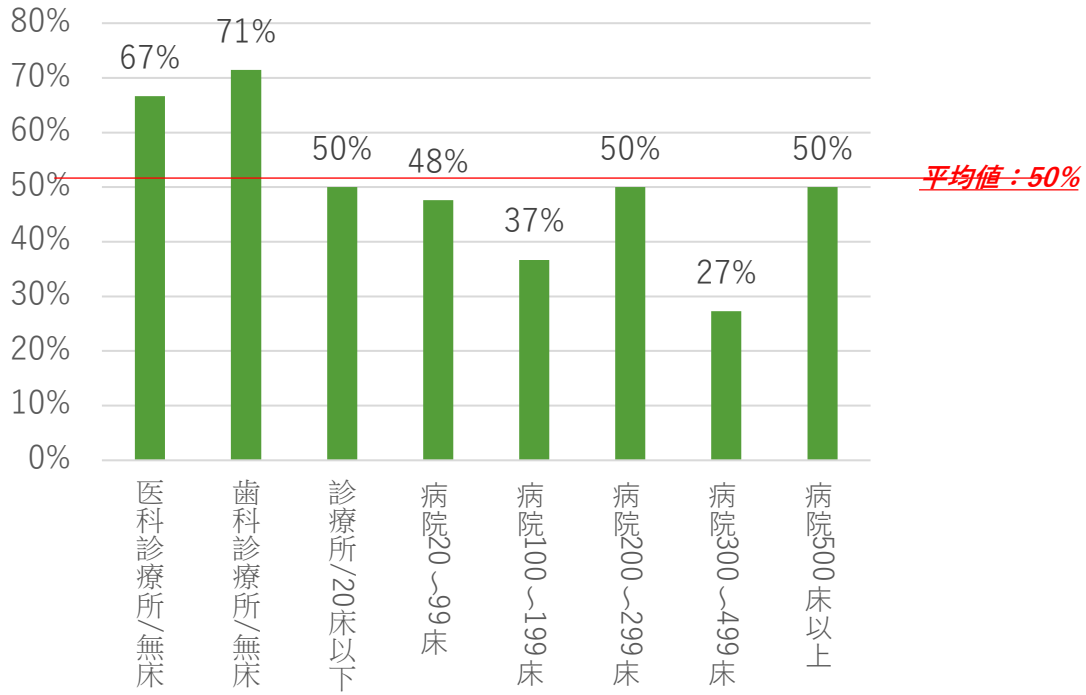
【②-B：それ以外のリモートメンテナンス用製品の利用・脆弱性対応状況】

- **全体平均で半数（50%)ほどがFortinet社以外のリモートメンテナンス用機器について、脆弱性パッチの適用対応等を行っていない**状況であった。特に病床規模が小さいほどその傾向は顕著であり、**医科・歯科の無床クリニックでは6割～7割が未対応であるが、その他の20床以上の病院群でも高い割合が示されている**。
- なお、病床数200床以上の病院はFortinet社以外の機器をすべての組織（100%)で利用している一方、**脆弱性対応を行っている割合は半分あるいはそれ以下であり、相対的に低い状況である。**

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



＜Q５：Q3以外のリモートメンテ機器の**脆弱性対応を行っていない**と回答した組織の割合＞

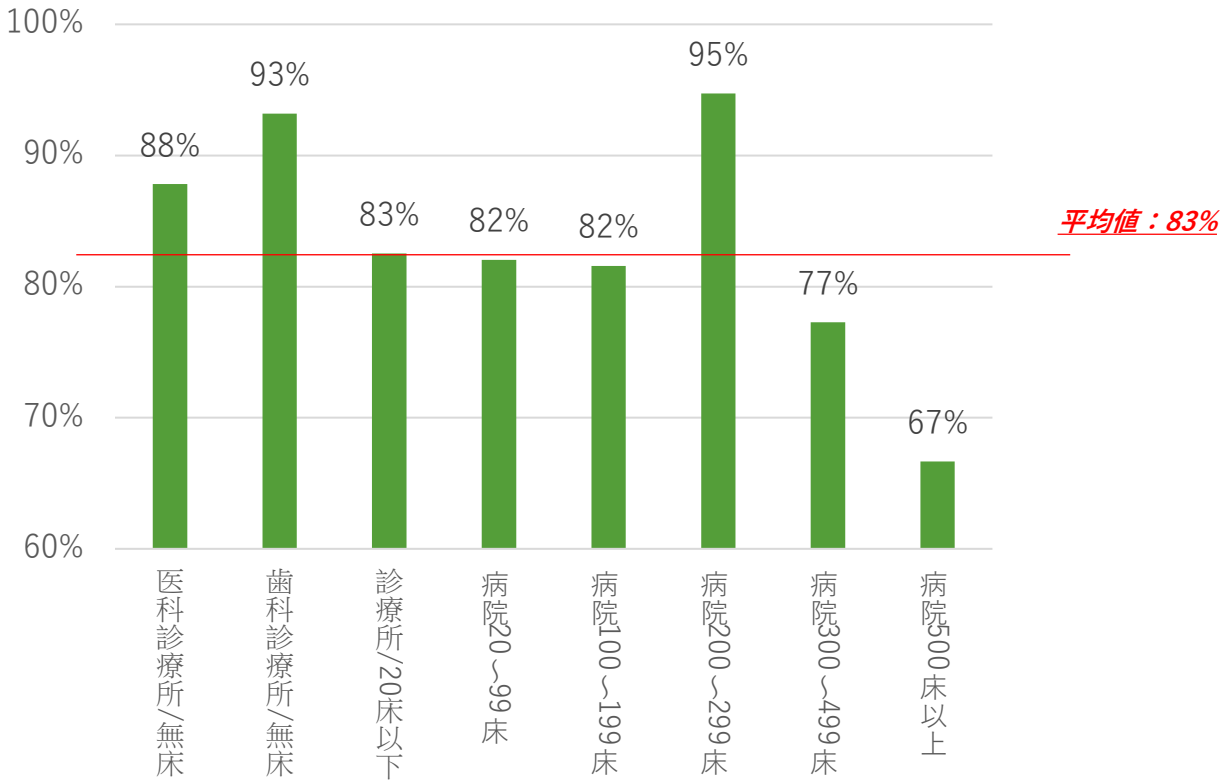


＜アンケート調査結果_病床規模別(4/5)＞

【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)

- 院内システムにおける保守等の契約・SLA等においてセキュリティ上の役割・責任を外部ITベンダと特に取り交わしていない組織についても、病床規模が小さいほどその傾向は全体的に強い。
- **特に医科・歯科の無床クリニック、及び200床～299床の病院群が全体平均と比較しても、相対的にセキュリティ面での契約管理の取組水準が低い状況**といえる。

＜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＞

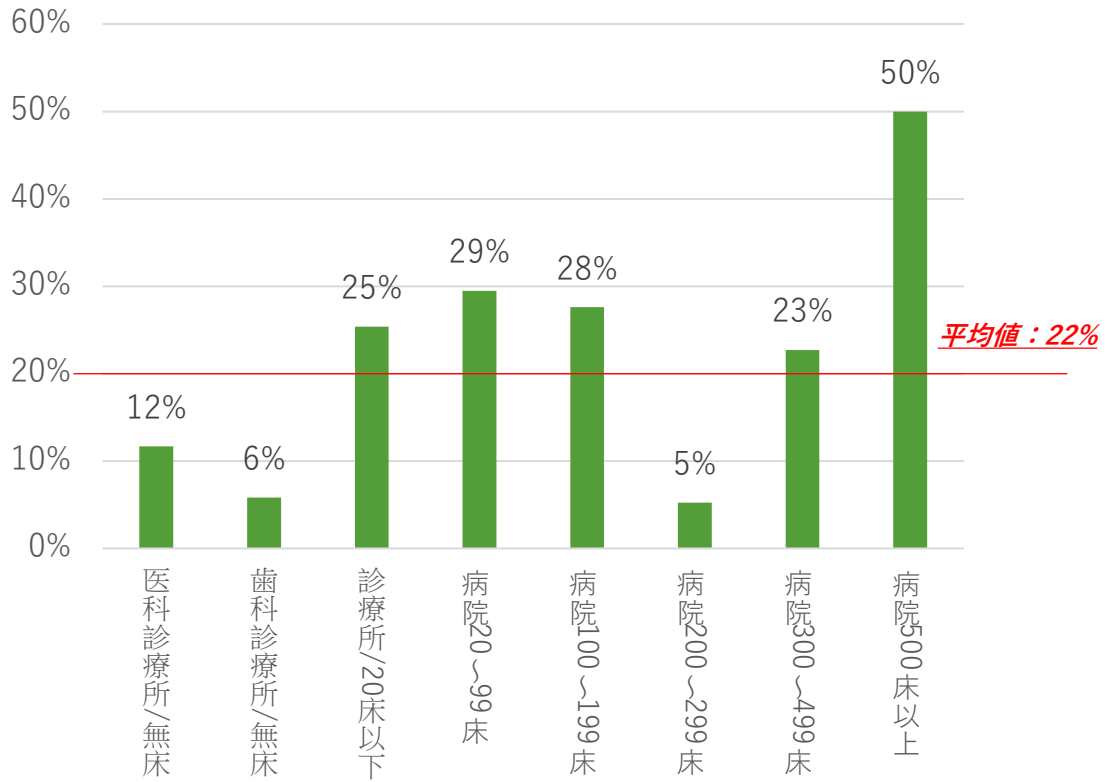


＜アンケート調査結果_病床規模別(5/5)＞

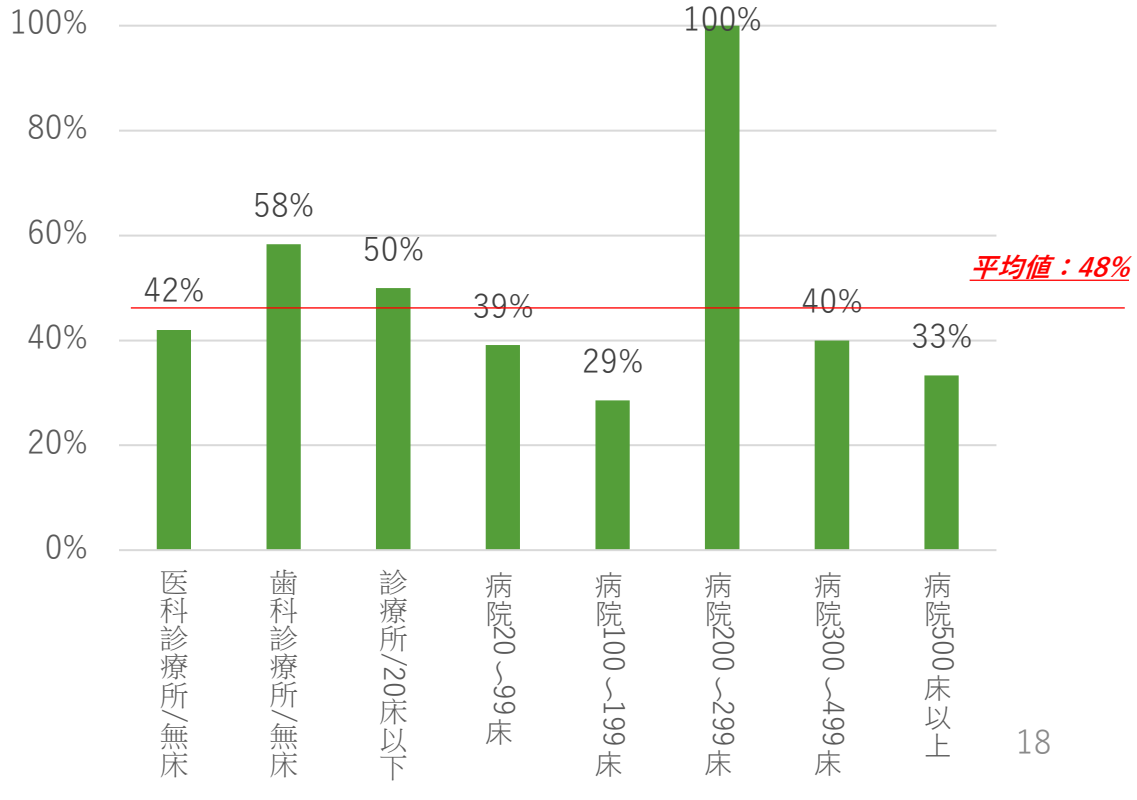
【③：医療機関/ベンダーとのリスクコミュニケーション状況】(2/2)

- ベンダからのセキュリティ脆弱性の情報等も含めた運用報告の確認率、及びその内容の理解・利活用度についても、病床規模が小さいほど低くなる傾向がうかがえる。
- **無床の医科・歯科クリニック、200床～299床病院群はベンダからの運用報告の確認実施率が全体平均より著しく低いことに加え、ベンダからの報告内容・情報についても満足していない割合が相対的に高い。**

＜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＞



3. 開設者別調査結果

＜開設者別総評＞

- リモートメンテナンスを導入しながらも、該当機器の情報を把握できていない割合が特に大きい開設者区分で見ると、「**公的医療機関」(100%導入/25%把握）、「医療法人」（72%導入/31%把握）、「個人」（57%導入/22%把握）**が該当する。一方で、リモートメンテナンス機器情報を把握しているという**回答率が100%に該当する開設者は、「私立大学法人」、「公益法人」、「医師会」**となる。

- Fortinet製品以外のリモートメンテナンス機器を利用しながら、その脆弱性の対応を行っていない割合が高い開設者区分は、**「国」「医師会」「社会福祉法人」「医療生協」「個人」**が挙げられる。一方で、十分な対応が行われている開設者としては、**「都道府県・市町村」「公的医療機関」**が続く。

- 契約・SLA等においてセキュリティ上の役割・責任を外部ITベンダと取り交わしていない組織として、開設者区分で見ると、**「公益法人」「私大法人」「その他」は全回答組織（100%)が該当、その次に 「個人」、「都道府県・市長村」が続いている**。「社会福祉法人」「その他法人」は相対的に契約・SLA等におけるセキュリティ上の諸事項の取り交わしを行っている割合が相対的に高い。

- ベンダからの運用報告の確認率/医療機関におけるベンダ報告内容への不満足率自体は**全体平均で3割程度である**。特にベンダ報告内容への不満足率としては、「社会福祉法人」(100%」、「医療生協」(67%)、「国」(50%）が高い状況である。

- 特に今回のアンケート回答数の高い開設者区分の「医療法人」「個人」を中心に見ると、**両者の対応/非対応割合はほぼ同率と言える。ただし、22年10月の脆弱性報告のあったFortinet社製品以外を用いたリモートメンテ機器の脆弱性対応状況は医療法人のほうが高い**状況である。

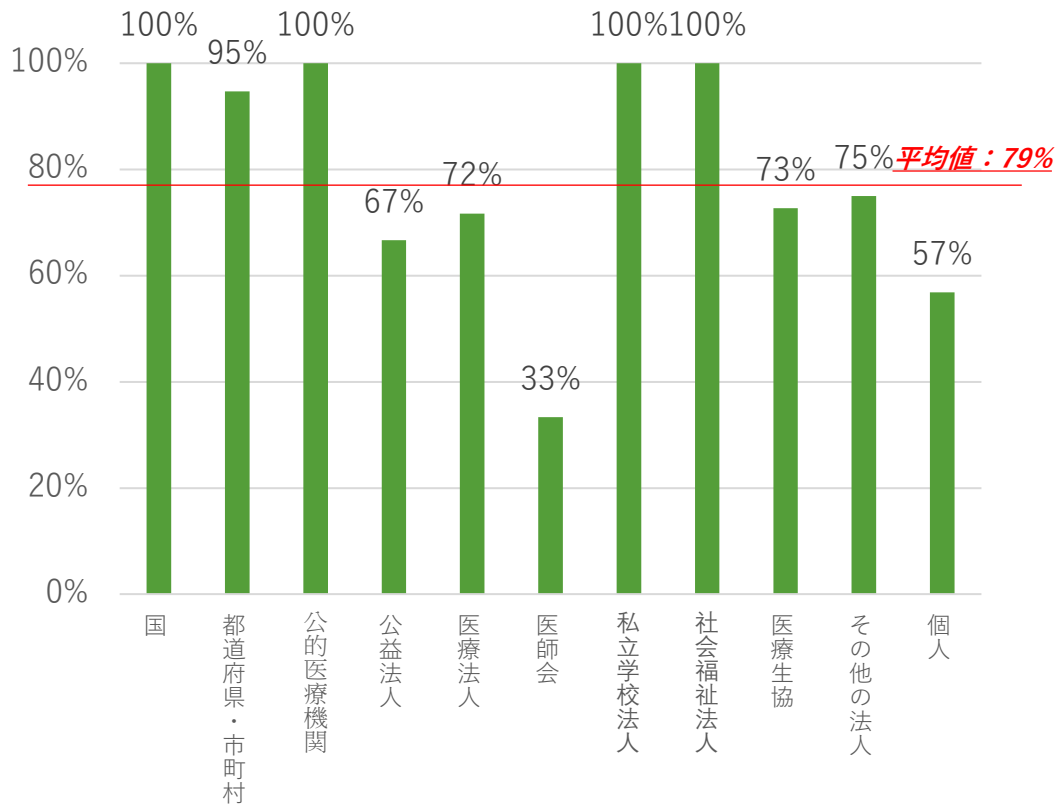
＜アンケート調査内容_開設者別(1/5)＞

※：「その他」はリモートメンテナンス未許可との回答のため、対象外としている

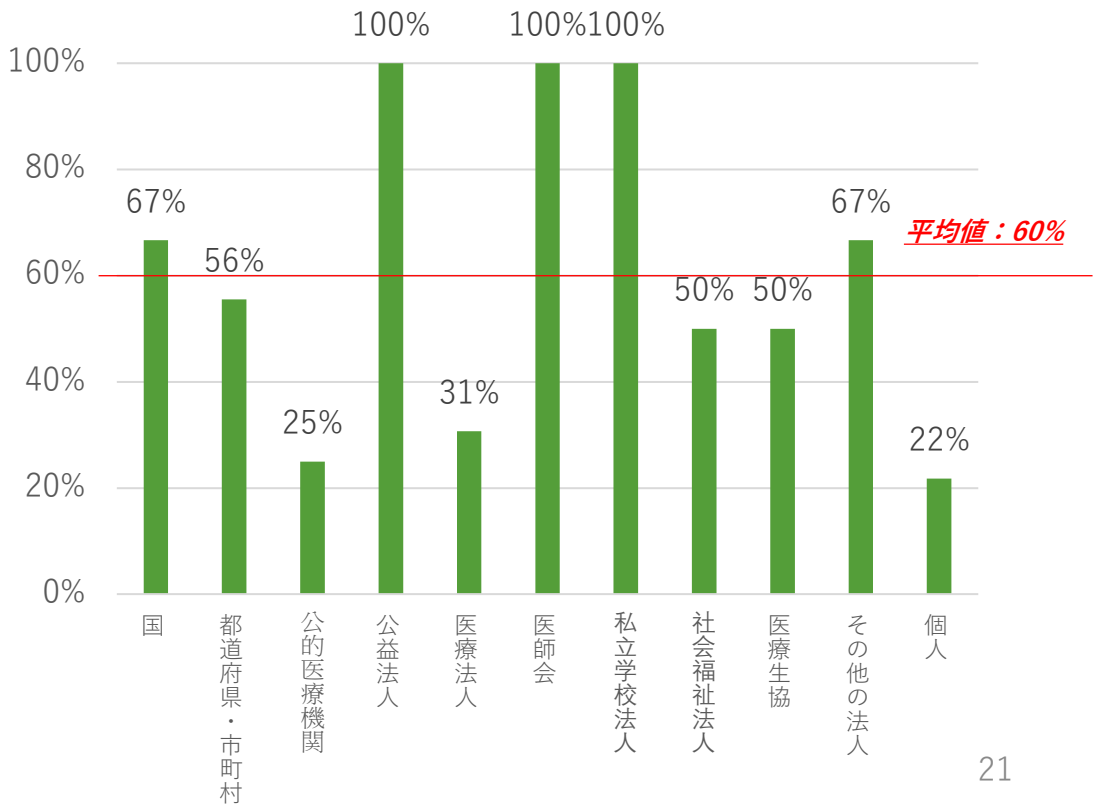
【①：リモートメンテナンス用製品の利用・把握状況】

- リモートメンテナンスを導入しながらも、該当機器の情報を把握できていない割合が特に大きい開設者区分で見ると、「**公的医療機関」(100%導入/25%把握）、「医療法人」（72%導入/31%把握）、「個人」（57%導入/22%把握）**が挙げられる。
- リモートメンテナンス機器情報を把握しているという回答率が100%に該当する開設者は、「私立大学法人」、「公益法人」、「医師会」となる。

＜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＞



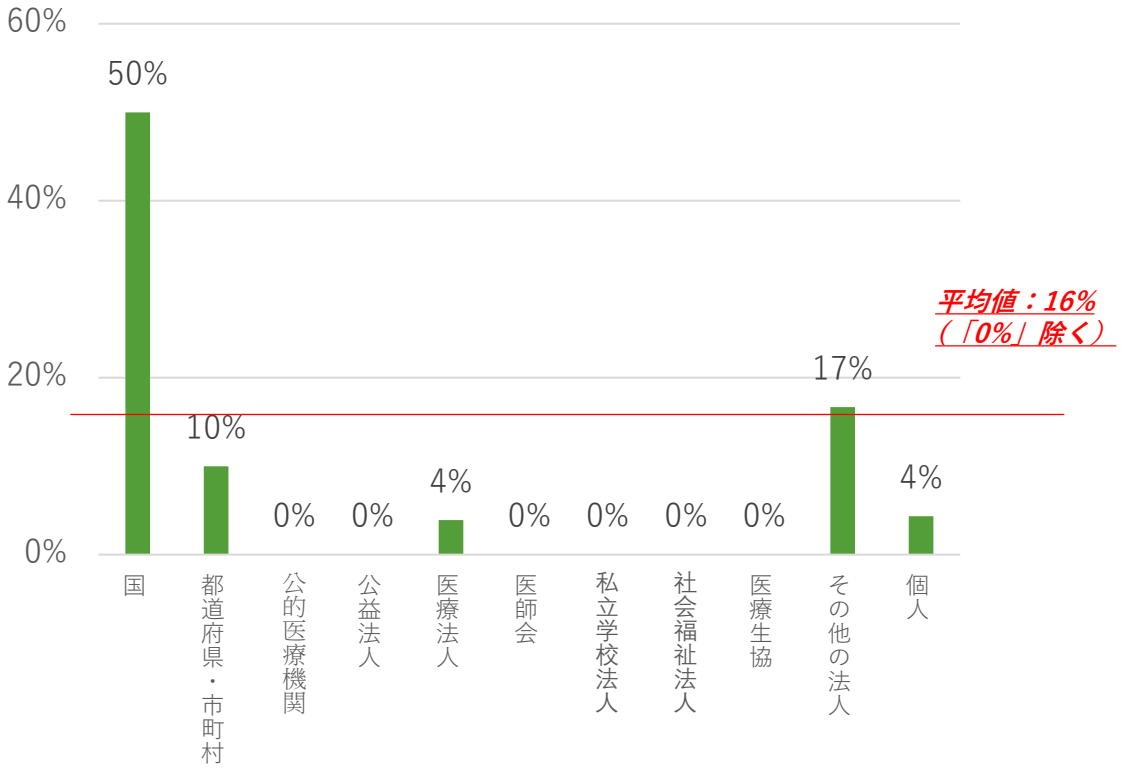
＜アンケート調査内容_開設者別(2/5)＞

※：「その他」はリモートメンテナンス未許可との回答のため、対象外としている

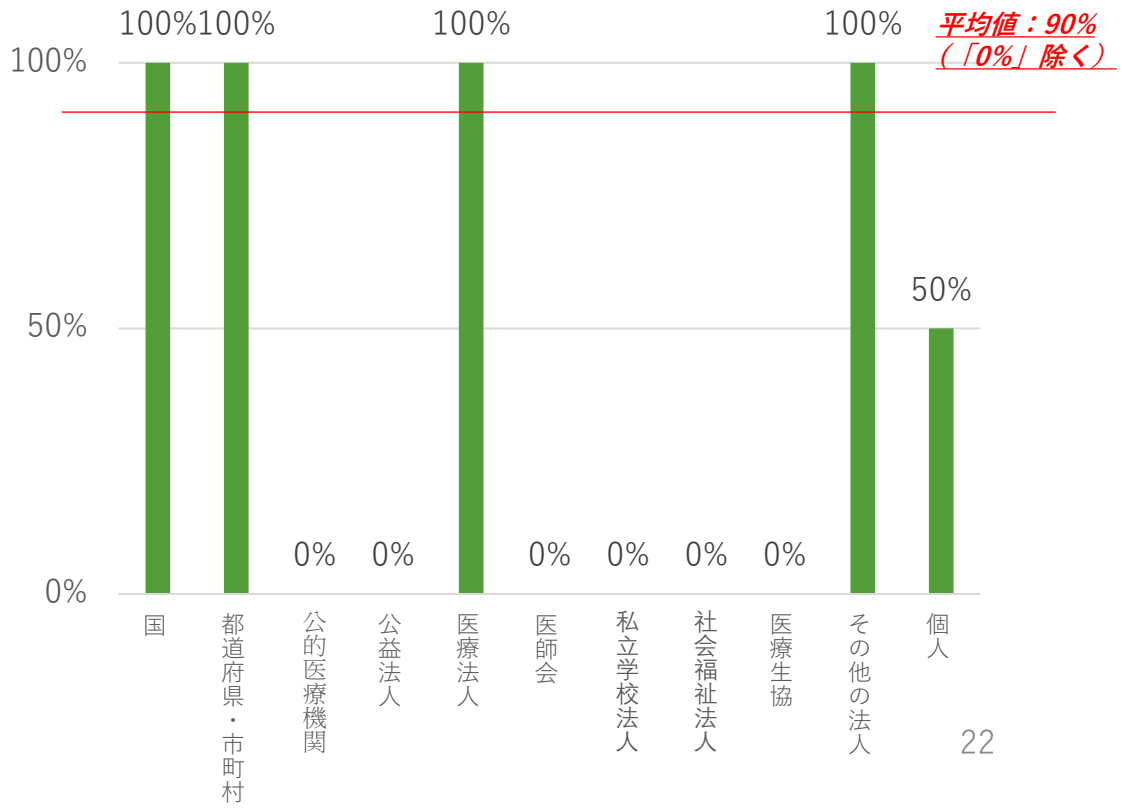
【②-A：Fortinet社リモートメンテナンス用製品の利用・脆弱性対応状況】

- 22年10月に深刻な脆弱性報告がされたFortinet社製品の利用率は「国」（国立大）以外は低く、かつ、「国」も含めてほぼ脆弱性対応が行われている状況である。

＜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＞



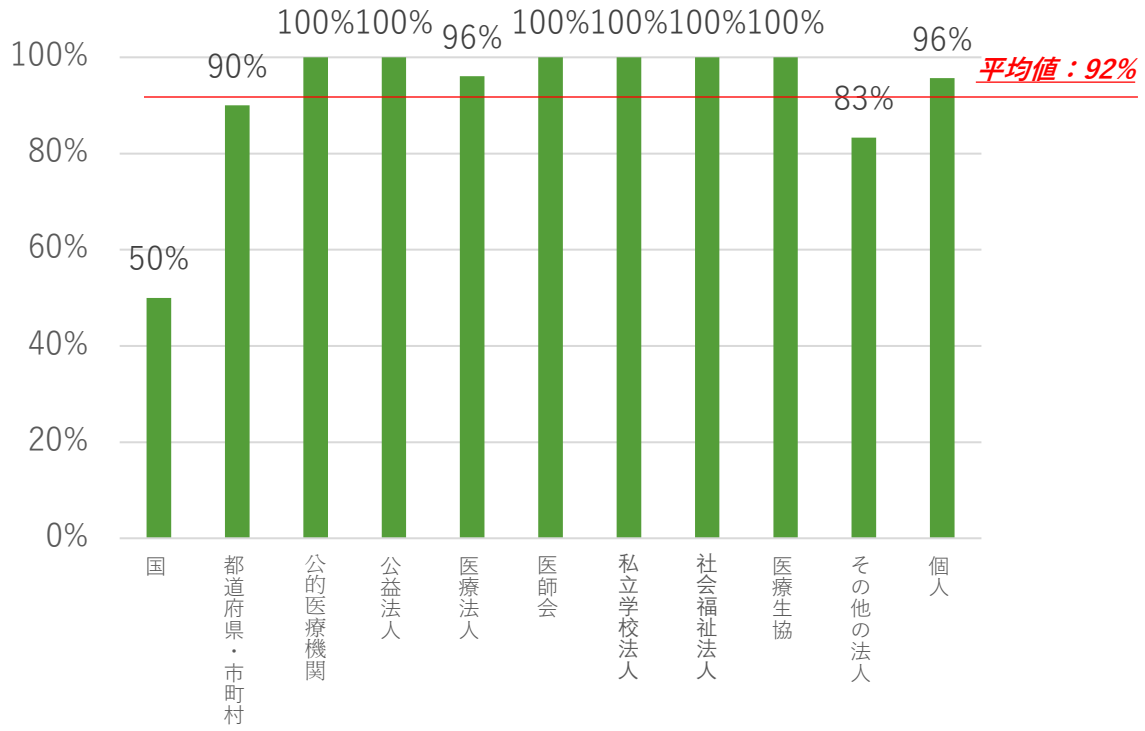
＜アンケート調査内容_開設者別(3/5)＞

※：「その他」はリモートメンテナンス未許可との回答のため、対象外としている

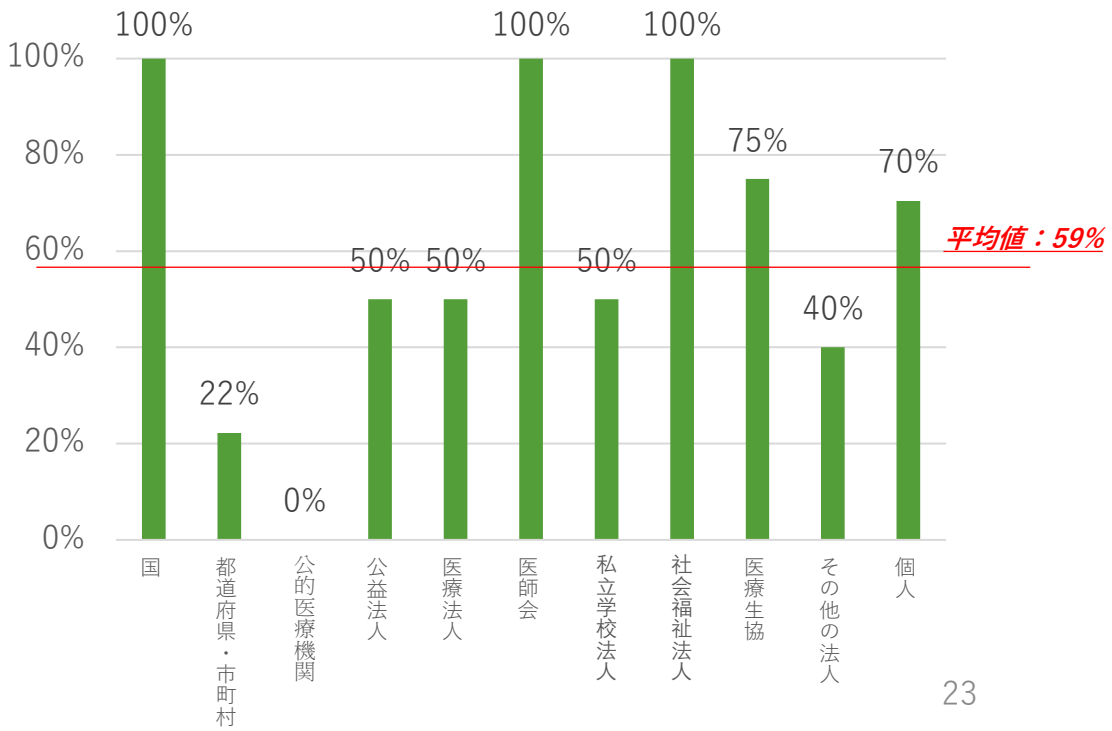
【②-B：それ以外のリモートメンテナンス用製品の利用・脆弱性対応状況】

- 「国」(50%利用/100%未対応)、「医師会」（100%利用/100%未対応）、「社会福祉法人」（100%利用/100%未対応）、「医療生協」（100%利用/75%未対応）、「個人」（96%利用/70%未対応）等、**一部の開設者区分において特に、Fortinet製品以外のリモートメンテナンス機器を利用しながら、その脆弱性の対応を行っていない割合が高い状況である。**
- 「都道府県・市町村」（90%利用/22%未対応）、「公的医療機関」(100%利用/0%未対応）等、開設者によっては十分な対応が行われているものも見受けられる。

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



＜Q５：Q3以外のリモートメンテ機器の**脆弱性対応を行っていない**と回答した組織の割合＞

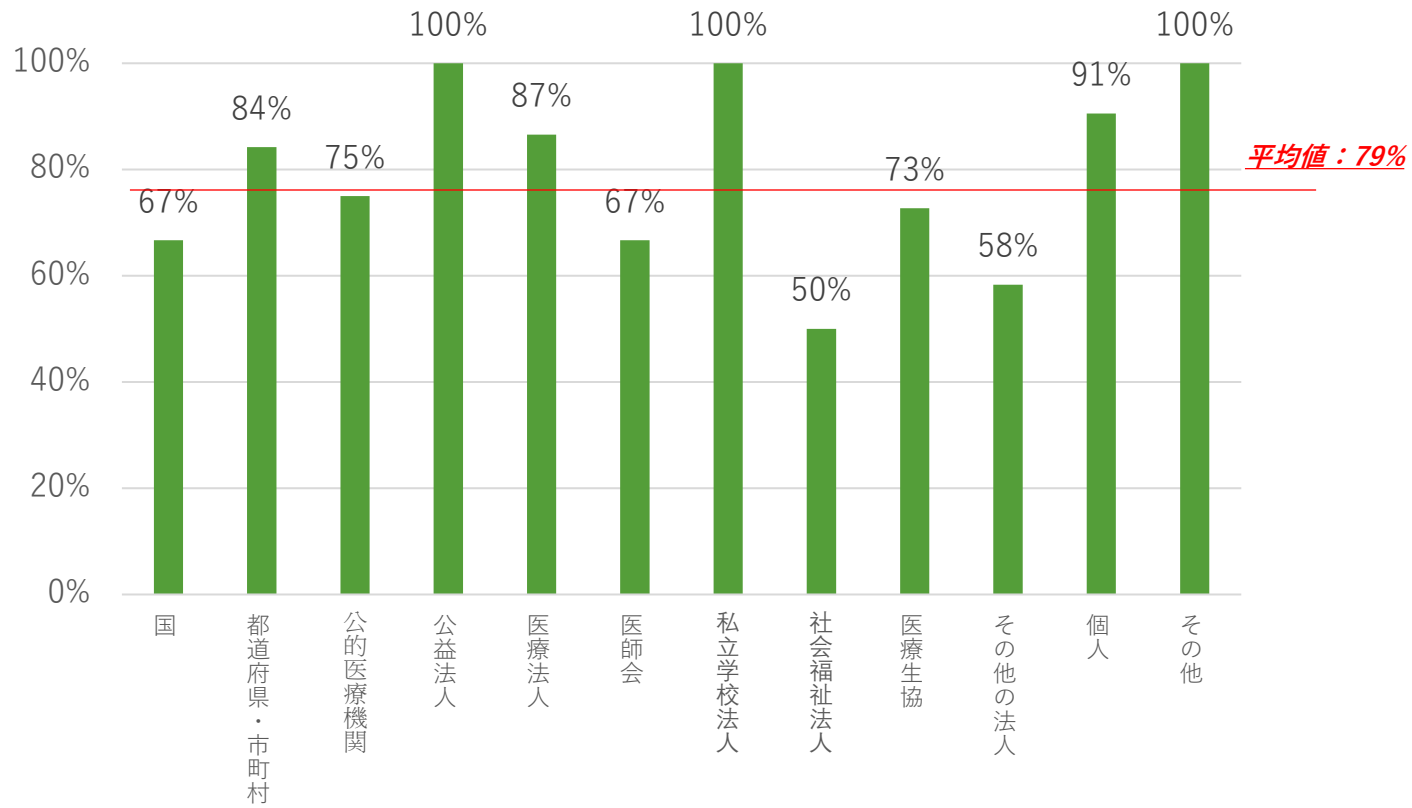


＜アンケート調査内容_開設者別(4/5)＞

【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)

- 契約・SLA等においてセキュリティ上の役割・責任を外部ITベンダと取り交わしていない組織として、全体平均割合（79%)を超える開設者区分は、**「公益法人」「私大法人」「その他」は全回答組織（100%)が該当、「個人」は91%、「都道府県・市長村」は84%が該当**する。
- そのような契約上の取り決めを相対的に高く行っている組織体としては、「社会福祉法人」「その他法人」が該当する。

＜Q6：契約書・SLAにおいてセキュリティ責任分界等を**定めていない**と回答した組織の割合＞

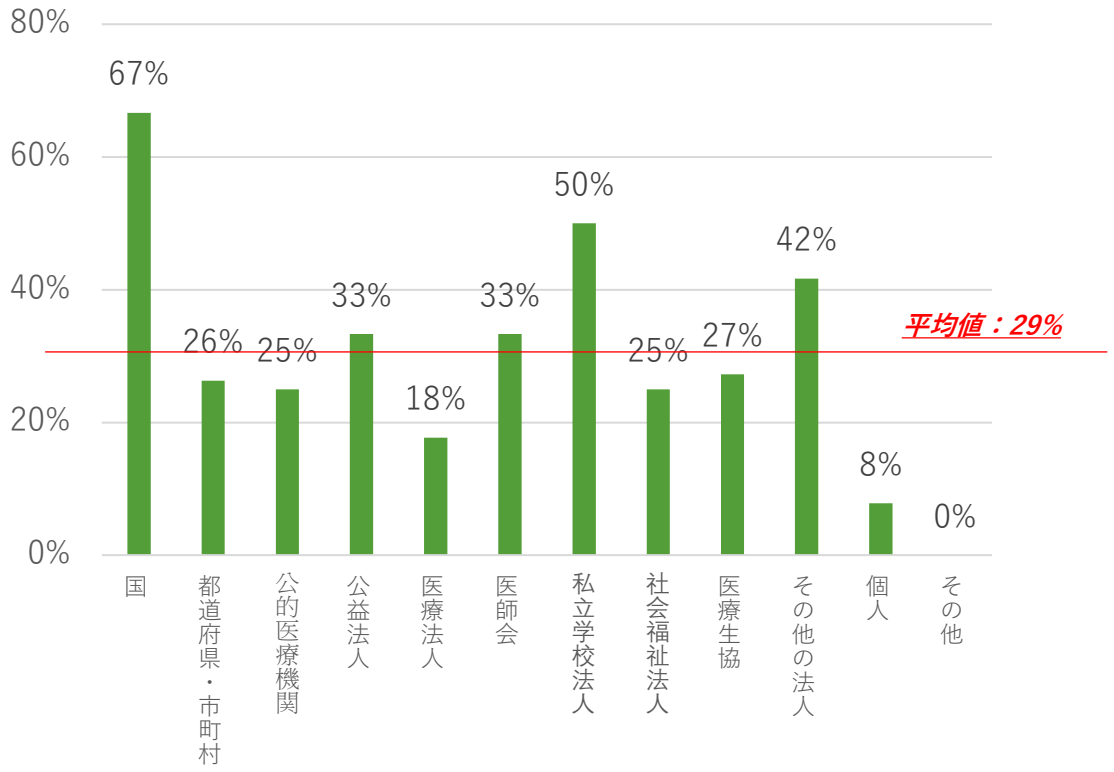


＜アンケート調査内容_開設者別(5/5)＞

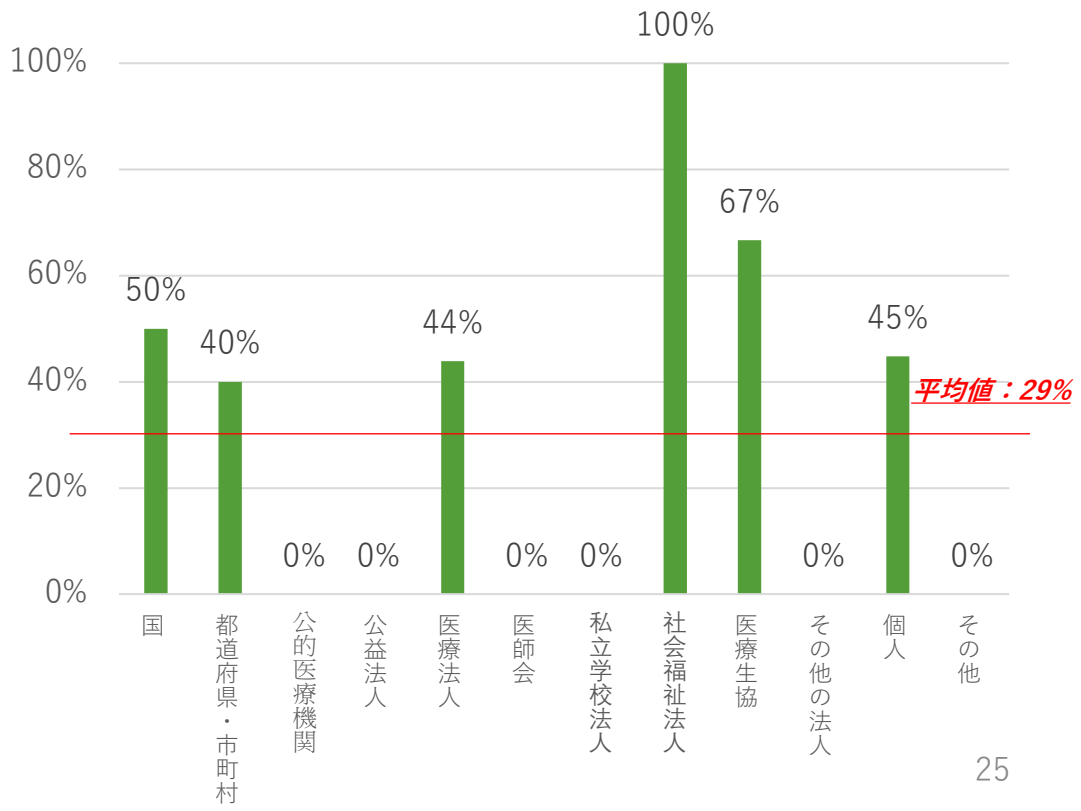
【③：医療機関/ベンダーとのリスクコミュニケーション状況】(2/2)

- ベンダからの運用報告の確認割合は「国」（67%)、「私大法人」(50%)、「その他法人」(42%)が特に高く、**全体平均は3割弱である。**
- 医療機関におけるベンダ報告内容への不満足率は、「社会福祉法人」(100%」、「医療生協」(67%)、「国」(50%）と続き、**全体平均は同じく3割弱**である。

＜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＞



国民医療の向上をめざす

全国保険医団体連合会