公益社団法人日本人間ドック学会
セキュリティアンケート調査結果

公益社団法人日本人間ドック学会
/一般社団法人医療ISAC

2023年3月

＜目次＞

1．調査概要

調査目的

健診施設のサイバーセキュリティに関する緊急アンケート調査

昨今、病院やクリニックを標的としたランサムウェア攻撃が猛威を振るっている状況で、直近でも大阪急性期総合医療センターの基幹系システムがランサムウェアに感染し、外来診療や予定手術の一時停止、急患受入れの制限等、医療業務の継続性に深刻な影響を及ぼす事態が発生しています。

まだ、表立った報道には上がっていませんが、介護サービスの提供事業者や健診施設、調剤薬局におけるランサムウェアの被害も見受けられています。

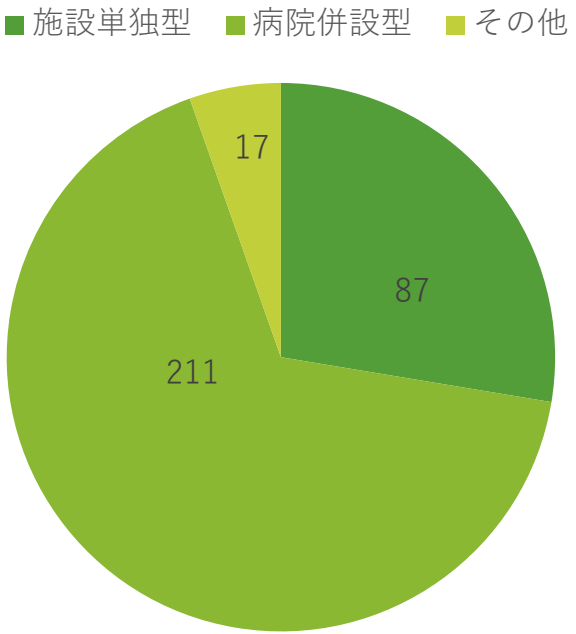
このような状況下、ITシステムを導入済みの健診施設を主な対象として、現状のサイバーセキュリティ上の課題を調査することで、課題解消の方向性を検討するとともに、今後、IT化を導入する事業者が留意すべきポイントを洗い出す必要があると考えます。
そのため、健診システム、及び当該システムと連携する電子カルテシステムの利用状況および、そのセキュリティに関する調査にご協力をお願い申し上げます。

本調査は日本人間ドック学会と医療ISACの共同事業となります。

調査対象

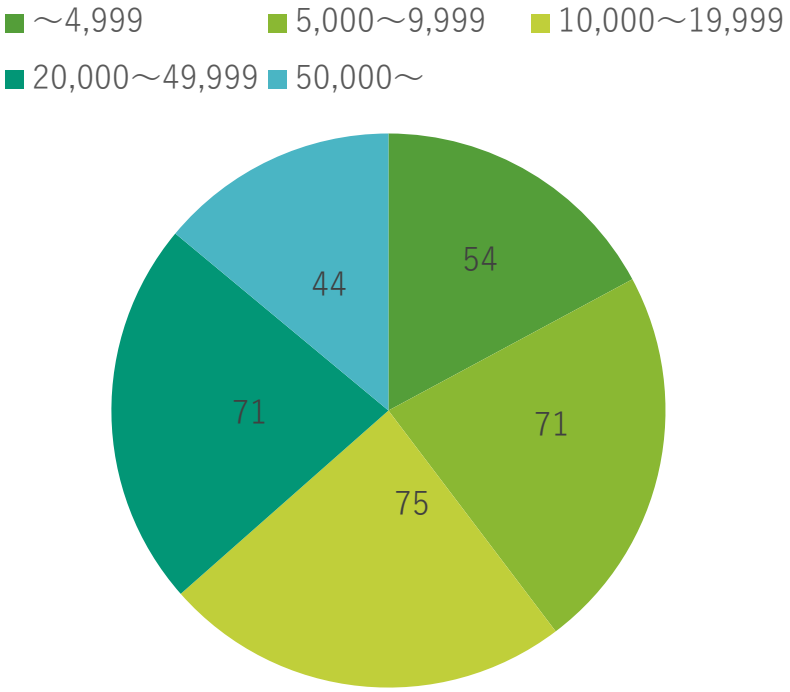
- 実施期間：2023年1月23日～2月18日
- 回答合計数：318件 / 1788件
- 回答率：17.8%
- うち調査対象数：315件（ITシステム未利用の施設/3件は調査対象外）
- 調査組織：（公社）日本人間ドック学会/（一社） 医療ISAC

＜施設類型別内訳＞

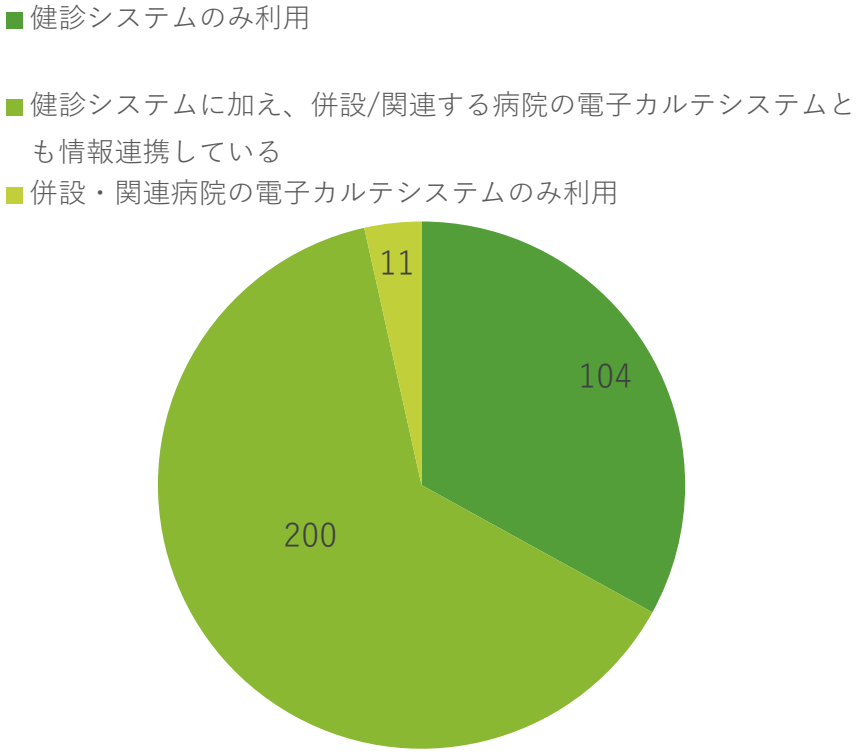


＜年間健診実施数別内訳＞

※：令和4年1月1日から令和4年12月31日までの健診実施件数



＜IT利用環境別内訳＞



調査項目(1/3)

調査項目は以下の16項目となる。

カテゴリ	調査項目	回答項目
ITの利用状況	①：IT利用の形態は？	□ 健診システムのみを利用している □ 健診システムに加え、併設/関連する病院の電子カルテシステムとも情報連携している □ 併設・関連病院の電子カルテシステムのみ使用している □ 紙情報で管理している ※「紙情報で管理」と回答した施設は、続く回答は未実施
サイバー攻撃への脅威	②最近のサイバー関連報道や関係省庁からの注意喚起を見聞して、サイバー攻撃への脅威を感じるか？	□感じる　□感じない　□わからない
脆弱性対策	③：NISC、厚生労働省から脆弱性が指摘され、対策するように求められているVPN機器やソリューションを使用しているか？	□使用している　□使用していない　□わからない
	④：③が「利用している」の場合、脆弱性に対するパッチを適用しているか？	□している　□していない　□わからない
	⑤：④が「していない」の場合、その理由は？（複数選択可）	□脆弱性が指摘されていることを知らなかった □脆弱性が指摘されているのは把握していたが、予算的に対応できなかった □その他
バックアップ対策	⑥：介護系システムのデータバックアップはどのように取得・管理しているか？（複数選択可）	□バックアップは保管していない □オンラインのバックアップを保管している □オフラインのバックアップを保管している □オフサイト（クラウド）のバックアップを保管している

調査項目(2/3)

カテゴリ	調査項目	回答項目
IT人材	⑦-1)施設内のシステム担当者は何人いるか ⑦-2)うち常勤の担当者は何人いるか	（人数を記入）
監査	⑧：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」を知っているか？	□知っている　□知らない
	⑨：セキュリティ監査（外部監査または内部監査）を実施しているか？	□ 計画を立てて、定期的に実施している □ 1年前に実施したが、その後は未実施 □ 2年前、またはそれ以前に実施したが、その後は未実施 □ 実施したことがない
セキュリティ予算	⑩：セキュリティに関する概算年間予算（人件費・委託費を含む）はどの程度か	□500万円未満 □500万円以上～1,000万円未満 □1,000万円以上～2,000万円未満 □2,000万円以上～5,000万円未満 □5,000万円以上 □わからない
	⑪：セキュリティ予算は十分か？	□感じている　□感じていない　□どちらでもない
サイバー保険	⑫：サイバー保険に加入しているか？	□日本ドック学会の団体保険「情報漏えい損害補償制度（サイバーリスク保険）」に加入している □日本ドック学会以外のサイバーリスク保険に加入している □サイバーリスク保険には加入していない □わからない
クローズドネットワークの安全性	⑬：診療系ネットワークに設置された医療・介護情報システムのセキュリティは安全であるという考え方に共感できるか	□ 共感できる □ 部分的に（条件付きであれば）共感できる □ 共感できない □その他

調査項目(3/3)

カテゴリ	調査項目	回答項目
システム提供事業者とのコミュニケーション状況	⑭：IT事業者は、施設に設置している基幹系システム（健診システム/電子カルテシステム）について、経済産業省・総務省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」に基づき、検討・実施すべきセキュリティ対策の指示を行っているか？	□実施している　□実施していない　□わからない
	⑮：システム導入に関する契約をIT事業者と取り交わす際に、経済産業省・総務省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」に基づく事業者による対応、及び自施設の支援を行うことを条項として明示的に定め、取り交わしを行っていますか？	□している　□していない　□わからない
	⑯：健診システムのセキュリティ対応について、IT事業者が十分に対応していると思いますか？	□思う　□思わない　□わからない

２．全体結果

＜アンケート調査結果_全体総評＞

- 今回の調査対象健診施設のうち、**8割以上はサイバーリスクへの脅威**を感じている。

- 脆弱性の指摘のあったForitnet社製VPN製品の利用率は3割強だが、そのうち脆弱性対応は８割以上は完了しているものの、**おおよそ１割程度の施設ではベンダによる非対応判断・指示、あるいはクローズドネットワークの安全神話等の理由により未対応**であった。なお、**全体の３割程度はVPN製品の種別を把握していないため、潜在的な脆弱性リスクを抱えている状況**でもある。

- バックアップの取得率は７割弱だが、そのうち**半数以上はランサムウェア被害に備えたオフライン/オフサイト保管方式を実施している。**

- IT人材配置数は全体平均で３人弱/常勤率は9割だが、**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」を把握している割合は９割近くに及び、５割以上がセキュリティ監査を計画的に実施**している。IT人材におけるセキュリティリテラシーも全体的に高く、＜外部の目線＞を介したセキュリティ監査の実施率の高さも相まって、**セキュリティリテラシー向上が循環的に実現されている**構図が見受けられる。

- 年間セキュリティ予算は５００万未満が４割弱を占める一方、**５００万以上を確保する施設は２割を占め、うち５０００万以上の施設も数パーセント存在する**状況である。ただし、セキュリティ予算が十分と回答する割合は１割強程度であり、**施設のIT規模が求めるセキュリティ予算が十分確保できていない事態**が浮き彫りになっている。

- サイバー保険の加入割合は**2割以上であり、かつ、「加入していない」割合もその他の医療・介護分野と比較した際に低い**点が特徴と言える。ただし、外部との接点を持たない無菌室でシステムセキュリティを考える思考傾向（＝診療系ＮＷはクローズド環境であるため安全と考える傾向）は**他分野同様、高止まりしている**。

- IT事業者によるセキュリティ対策の指示等を受けている組織は半数近く（49%)に達しているものの、IT事業者によるセキュリティ対応を信頼している割合はそれ以下（44%)であることが示されており、**一部の施設ではIT事業者をしっかり管理しなければならないというリスク認識が浸透**していることがうかがえる。一方で、**セキュリティ面も含めた契約締結を行っている施設は3割強にとどまっており、確実なセキュリティ面を含めた契約を通したIT事業者のハンドリングの必要性**が浮き彫りになっている。

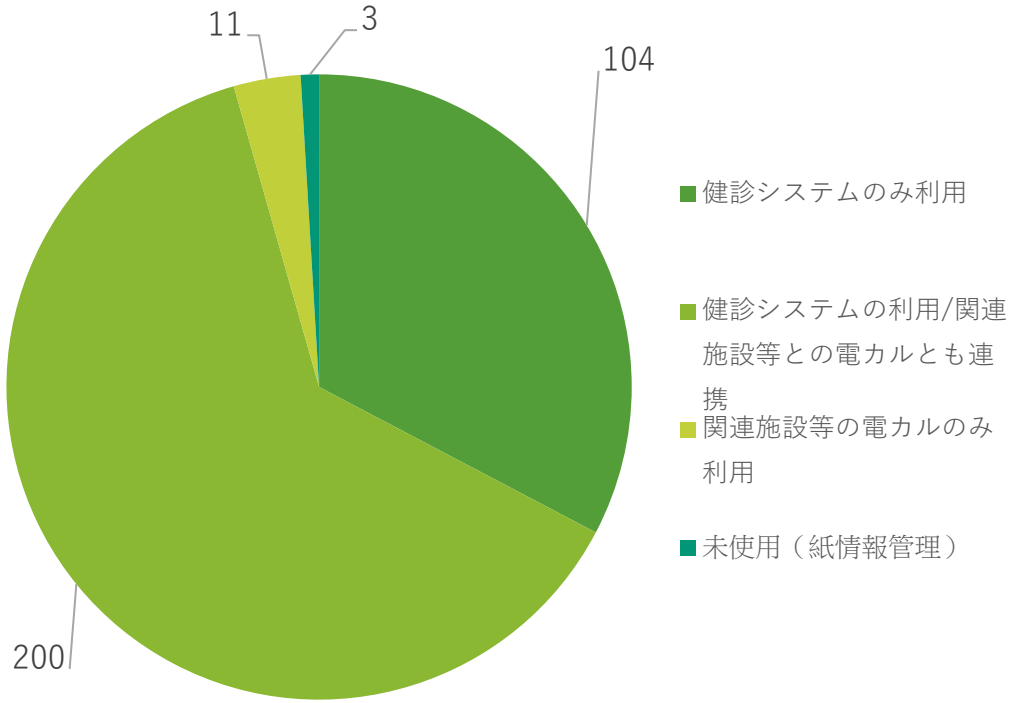
- 総合すると、健診分野では、セキュリティ予算を相応に確保し、厚労省GLを踏まえた観点より、IT事業者という外部委託先をマネージしながら、セキュリティ監査等を通したセキュリティPDCAに取り組めている施設が一部存在する一方、まだ**多くの施設がITの規模に一致したセキュリティ予算を確保できず、かつ、IT事業者とのセキュリティ面を含めた契約管理を通したリスクコミュニケーションの恩恵等を十分に受けられていない**状況が推察される。そのため、**こうしたセキュリティPDCAに通じた施設の成功事例等を参考にしながら、業界全体として、セキュリティ管理水準の底上げを図っていくことが重要**といえる。

＜アンケート調査結果_全体結果(1/8)＞

【IT利用の形態】

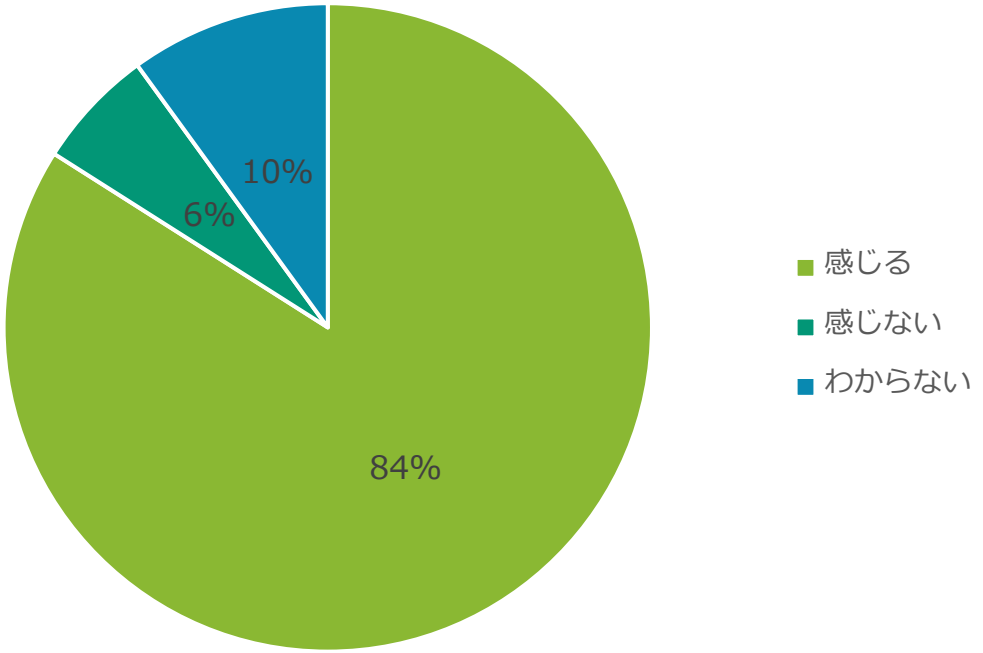
＜①：ITの利用形態は？＞　※N＝318

※：以降の調査は紙管理施設は対象外



【サイバー攻撃への脅威】

＜②：サイバー攻撃への脅威を感じるか？＞　※N＝315



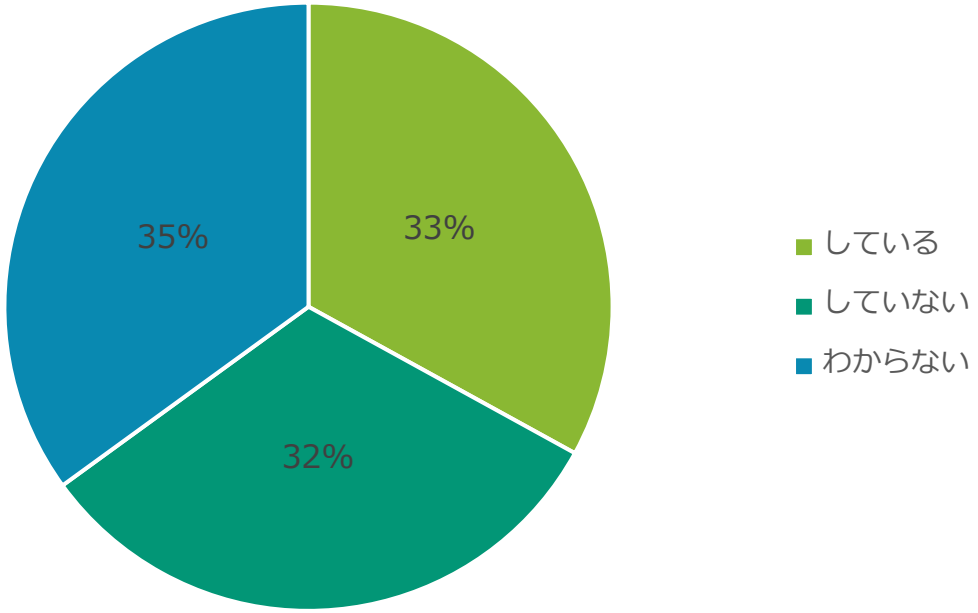
ITシステムを利用している健診施設の**8割以上がサイバー攻撃への脅威を感じている**

＜アンケート調査結果_全体結果(2/8)＞

【脆弱性対策】

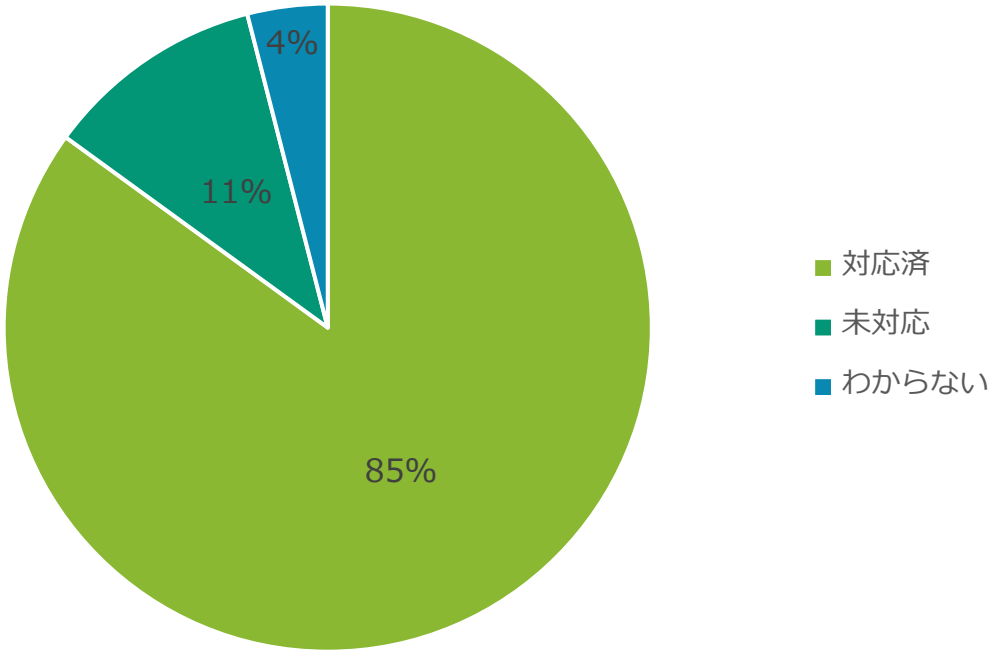
＜③：厚労省等から脆弱性が指摘されたForitnet社製VPN機器を使用しているか？＞

※N＝315



＜④：③が「使用している」の場合、脆弱性対応は完了しているか？＞

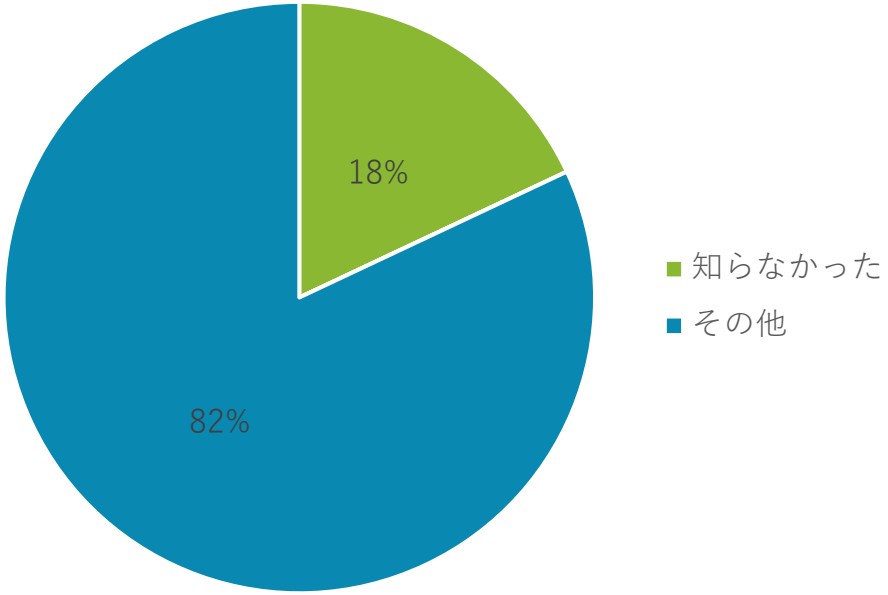
※N＝103



厚労省から脆弱性が周知されたVPN機器を利用している健診施設の割合は3割強であるが、**9割近くはこれらの脆弱性対応は完了している状況である。**

＜アンケート調査結果_全体結果(3/8)＞

＜⑤：④が「未対応」の場合、その理由は？＞　※N＝11



【その他】の概要

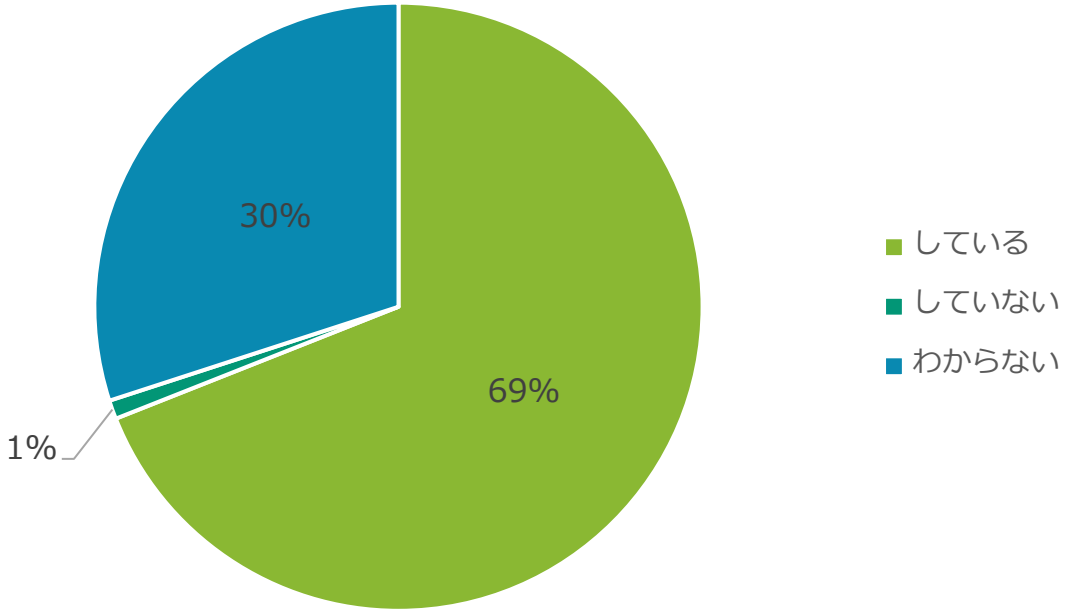
■バージョンが古いためベンダから対応不要と言われた
■ベンダからセキュリティパッチ適用を禁止されているため
■外部との接続点のないオフライン運用環境のため
■パッチ適用に伴う不具合が不安なため
等・・・

脆弱性のあるVPN機器への対応が未了の健診施設については、**ベンダからの対応禁止指示やオフライン運用環境（クローズドネットワーク）による安全神話等が特に多い状況**であった。

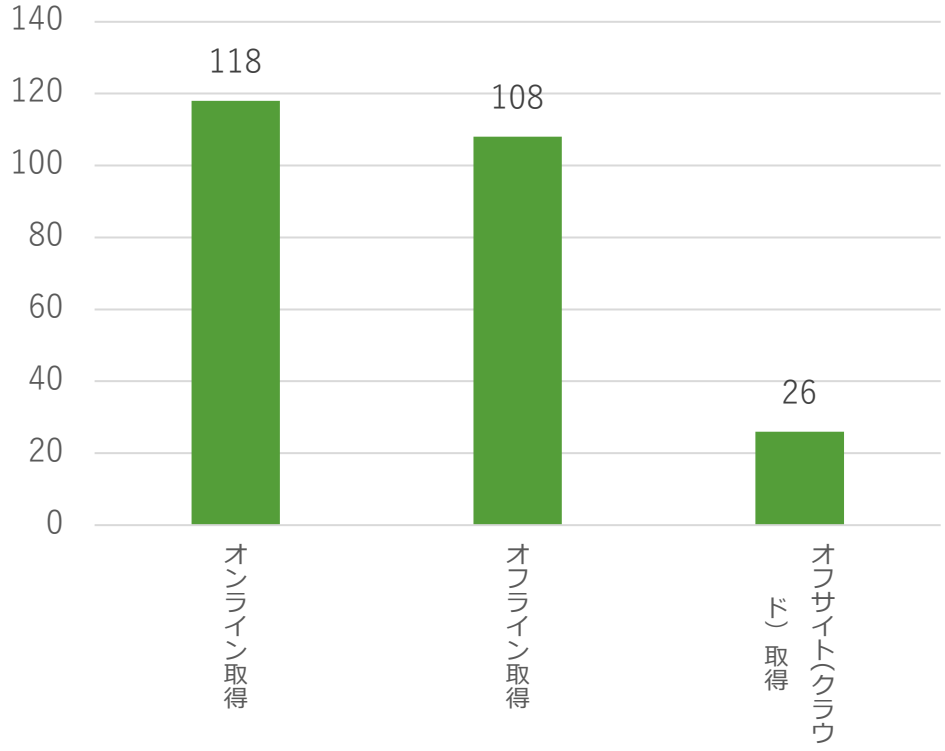
＜アンケート調査結果_全体結果(4/8)＞

【バックアップ対策】

＜⑥-1：バックアップの取得率＞　※N＝315



＜⑥-2：バックアップの取得方式(複数選択式）＞　※N＝252



バックアップの取得率は7割程度であるが、**ランサムリスクを低減するオフライン/オフサイトも含めた保管を行っている組織は全体の半数以上に及ぶ**ことが示されている。

＜アンケート調査結果_全体結果(5/8)＞

【IT人材】

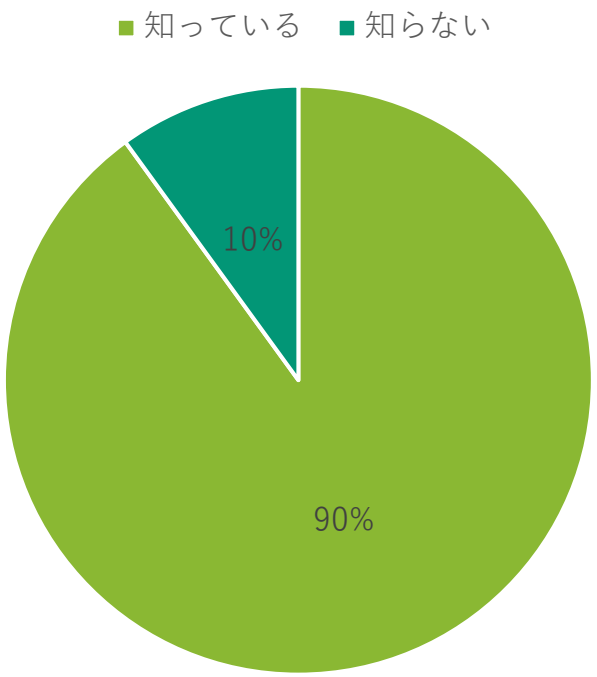
＜⑦：IT人材数＞　※N＝315

種別	平均人数
施設内システム担当者	**2.9人**
うち、常勤数	**2.6人**
常勤率：90%	

【監査】

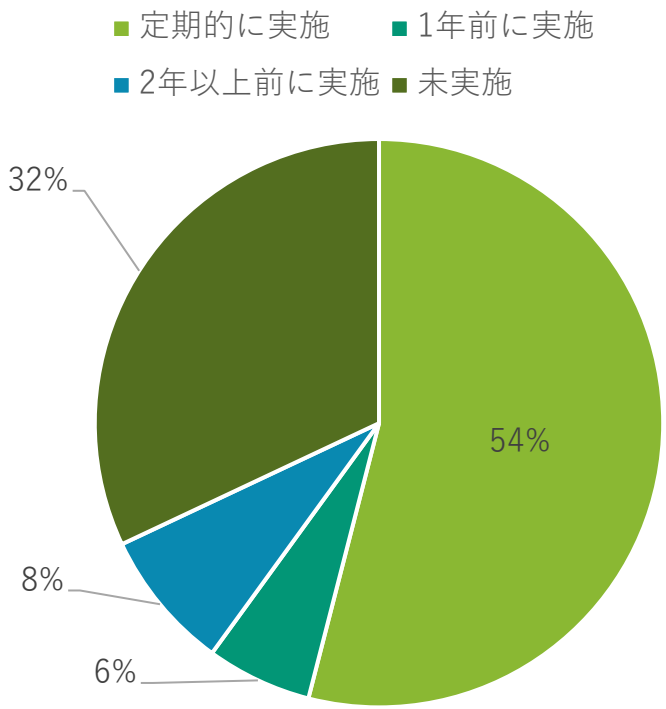
＜⑧：厚労省安全管理GLの認識状況＞

※N＝315



＜⑨：セキュリティ監査の実施状況＞

※N＝315

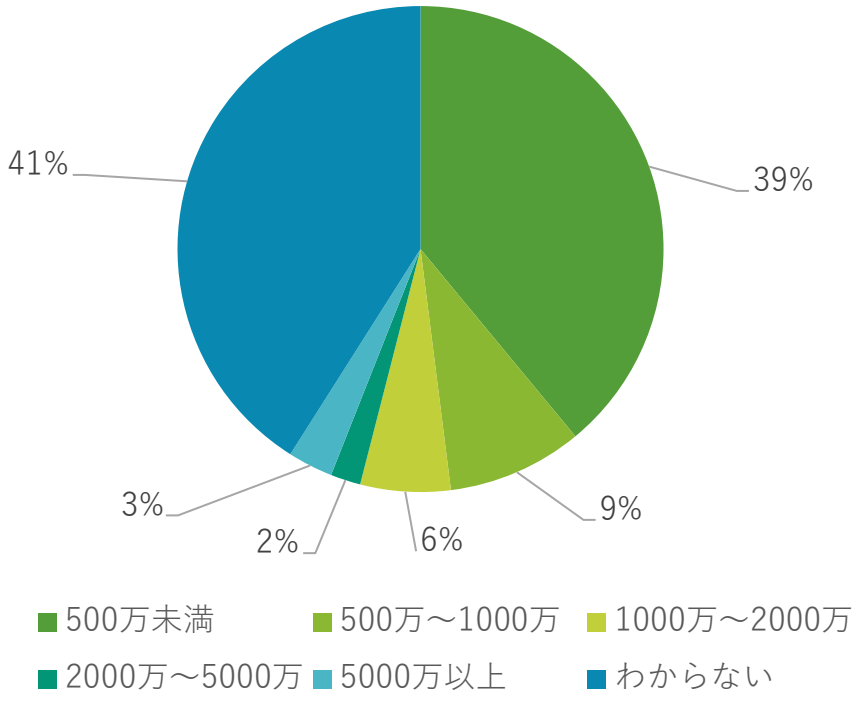


IT人材数は3名弱と比較的に多く、また**厚労省安全管理GLの把握率は9割**に及び、
セキュリティ監査の定期実施率も5割以上に達しており、非常に高い取組率といえる。

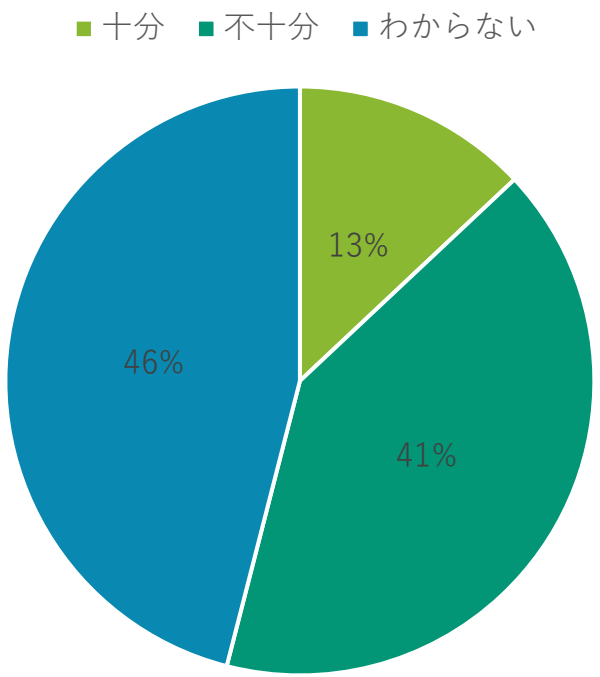
＜アンケート調査結果_全体結果(6/8)＞

【セキュリティ予算】

＜⑩：年間のセキュリティ予算＞　※N＝315



＜⑪：セキュリティ予算の十分性＞　※N＝315

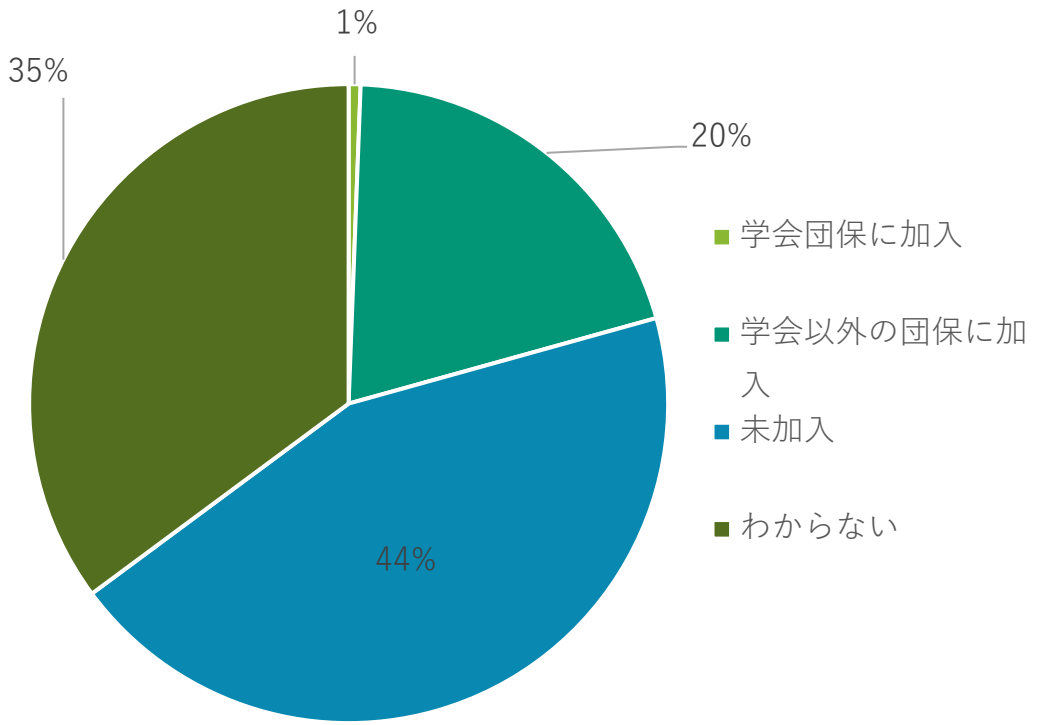


年間セキュリティ予算は500万未満（「分からない」含む）が最も多いが、**1000万以上の予算を確保できている施設も一定数存在**している。ただし、セキュリティ予算が十分と回答した施設割合は1割強あり、**施設のIT規模に求められるセキュリティ対応が十分に行えていない状況が観られる。**

＜アンケート調査結果_全体結果(7/8)＞

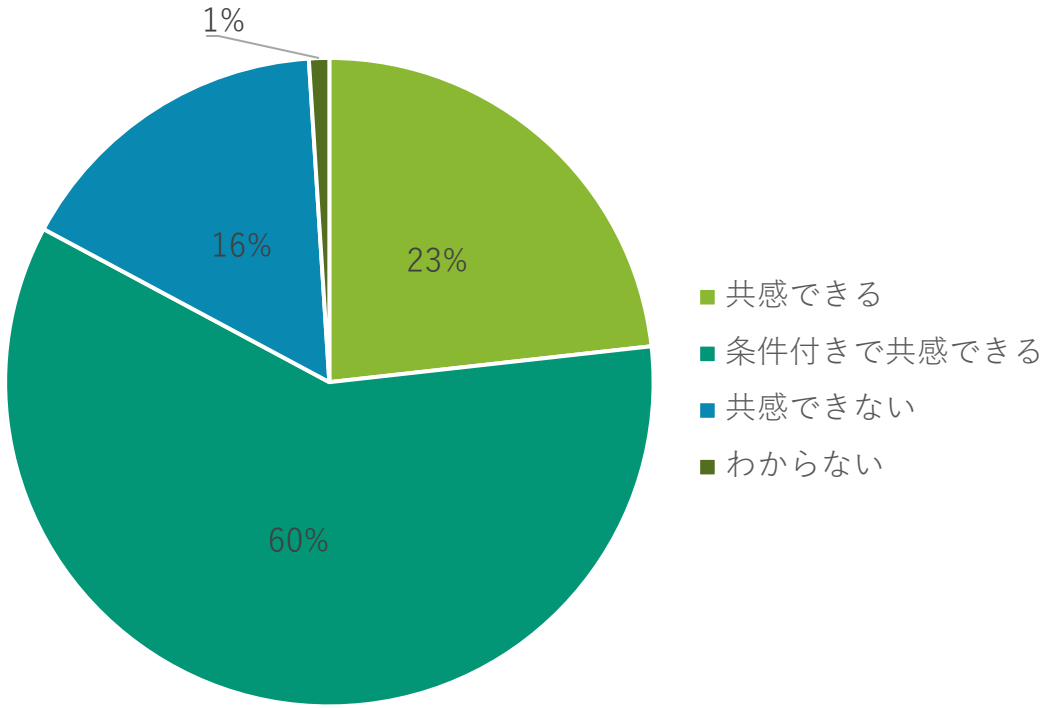
【サイバー保険】

＜⑫：サイバー保険の加入状況＞　※N＝315



【クローズドNWの安全性】

＜⑬：診療系NWは安全という考え方への共感状況＞　※N＝315

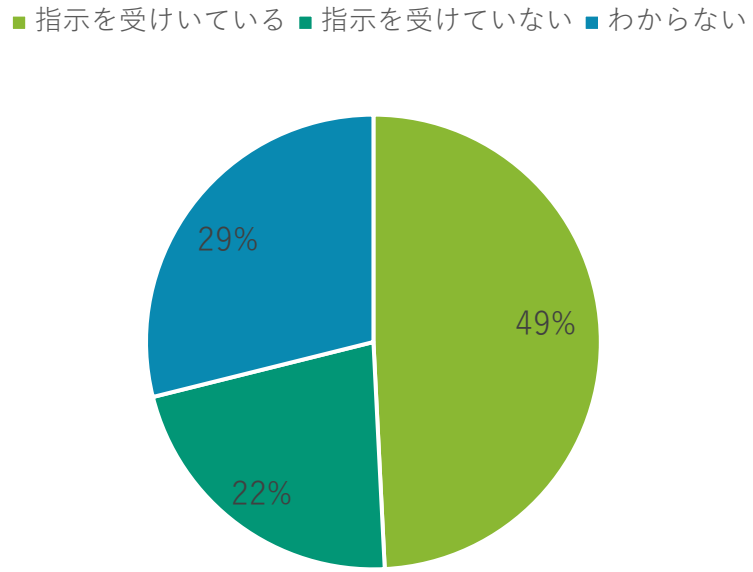


サイバー保険の加入割合は**2割以上に及んでおり、医療・介護分野と比較した際に相対的に高い**点が特徴と言える。ただし、外部との接点を持たない無菌室でシステムセキュリティを考える思考傾向（＝診療系ＮＷはクローズド環境であるため安全と考える傾向）は**他分野同様、高止まりしている**状況である。

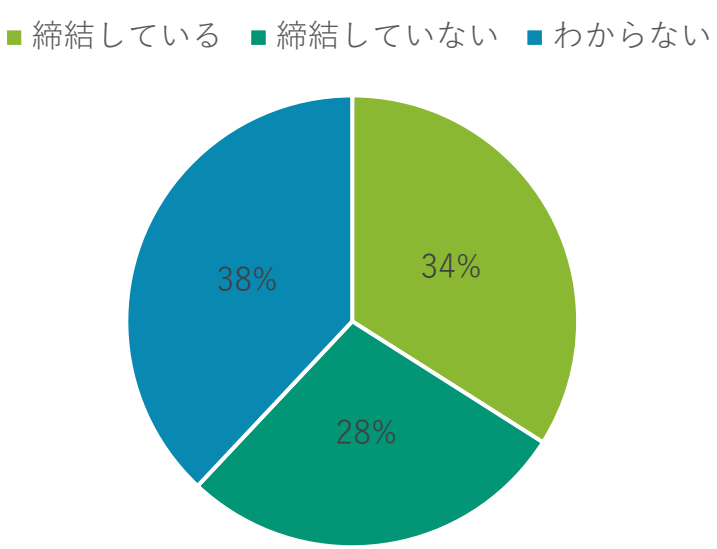
＜アンケート調査結果_全体結果(8/8)＞

【システム提供事業者とのコミュニケーション状況】 ※N＝315

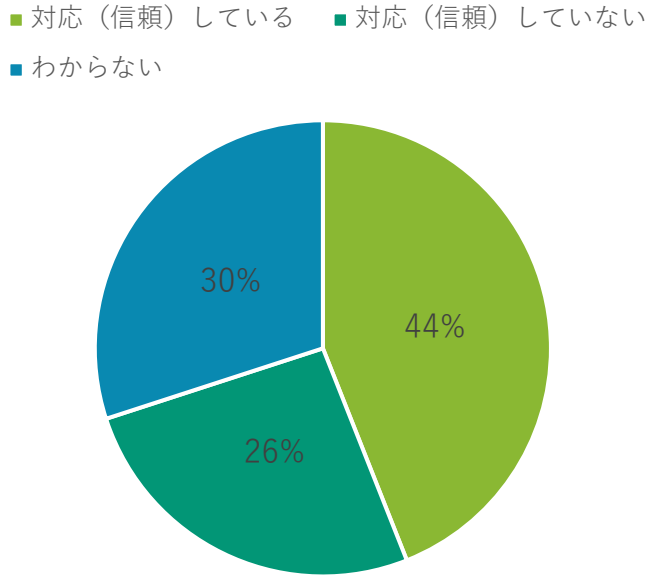
＜⑭：IT事業者によるセキュリティ対策指示状況＞



＜⑮：IT事業者とのセキュリティ契約締結状況＞



＜⑯：IT事業者はセキュリティ対応をしてくれていると思うか（信頼状況）＞



今回の調査結果からは、 IT事業者によるセキュリティ対策の指示等を受けている組織は半数近く（49%)に達しているものの、IT事業者によるセキュリティ対応を信頼している割合はそれ以下（44%)であることが示されており、**一部の施設ではIT事業者をしっかり管理することの重要性が浸透**していることがうかがえる。一方で、セキュリティ面も含めた契約締結を行っている施設は3割強にとどまっており、**確実なセキュリティ面を含めた契約を通したIT事業者の管理の必要性が浮き彫り**になっている。

３．年間健診数（規模）別結果

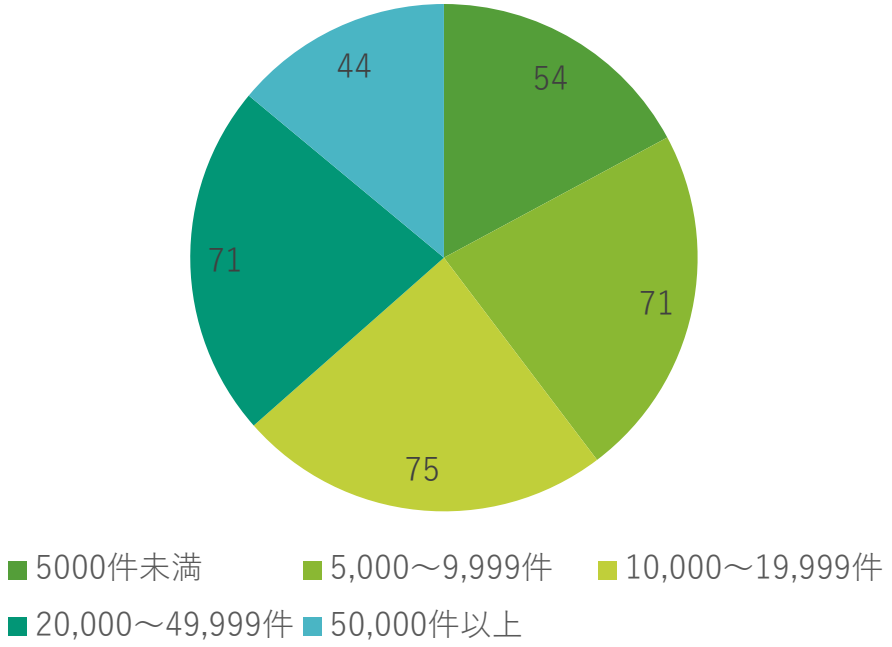
＜アンケート調査結果総評_年間健診数別＞

- 年間健診実施数という観点（「規模」の区分）でみると、健診実施数が多い施設ほど**サイバー攻撃リスクへの感受率も高い傾向**がある。
- また、同じく、**年間健診実施数の多さに応じて、施設内で利用されるVPN機器の把握率が高く**（「わからない」率が低い）、かつ、**脆弱性への対応の完了率も高い**傾向が示されている。
- バックアップの取得率の高低も年間健診実施数の多寡と比例する関係にあるが、**オフラインでのバックアップ取得率は平均的に全ての区分において高い**状況であり、健診施設におけるランサム被害に備えた復旧策は一定の充実度にあると想定される。
- 年間健診実施数が多いほどIT人材配置数が多いが、**厚生労働省安全管理GLの把握率は平均的に全ての区分で高い状況**である。また、**セキュリティ監査の非実施率も健診実施件数が多いほど比例的に低く**なり、５万件以上の区分の施設（大規模施設）が最も監査未実施率が低い。
- **年間健診実施数とセキュリティ予算額もほぼ比例する関係**にある。特に健診数5千件以上の各区分施設における１割以上は500万以上の予算、さらに5万件以上の施設の4分の1は2000万以上の予算が確保されている状況である。**しかしながら、セキュリティ予算が十分と回答した施設は全体平均で1割程度であり、施設のIT規模とセキュリティ予算がかみ合っていない状況**が見受けられる。
- **年間健診実施数が多いほどサイバー保険未加入率も低くなる**傾向がある。一方で、クローズドNWの安全神話への共感率は健診数の多さによって高まる傾向があり、**サイバー保険に加入していない、健診数の少ない施設ほど、隠れた外部との接続リスクに対する感度が高い**といえる。
- **年間健診実施数の各区分において、IT事業者に対するユーザセキュリティの実施内容の確認率、セキュリティ面も含めた契約締結率、IT事業者への信頼率はほぼ同率の状況**と言える。健診数の多寡自体が、IT事業者とのコミュニケーション率に大きな影響を及ぼしていることはないと言える。
- 総合すると、**年間健診実施数が多いほど、セキュリティ予算の確保率も高く、VPN機器の脆弱性対応やセキュリティ監査の実施等のセキュリティPDCAを回すことが出来ている**状況と言える。なお、**これらの健診実施数の多寡は、IT事業者との契約に基づくセキュリティ面を含めたリスクコミュニケーション率を左右するような影響は見られない**。

＜アンケート調査結果_年間健診数別(1/7)＞

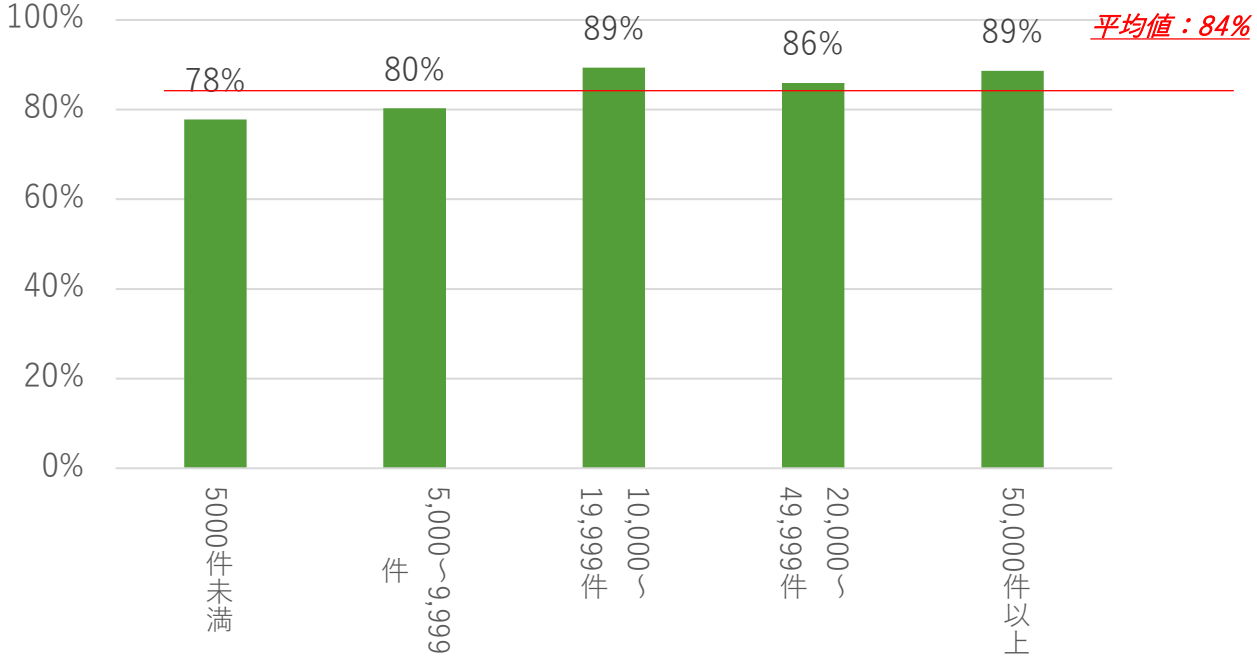
【ITの利用形態】

＜①：ITの利用形態（件数）＞　※N＝315



【サイバー攻撃への脅威】

＜②：サイバー攻撃への脅威を感じている施設割合＞　※N＝315

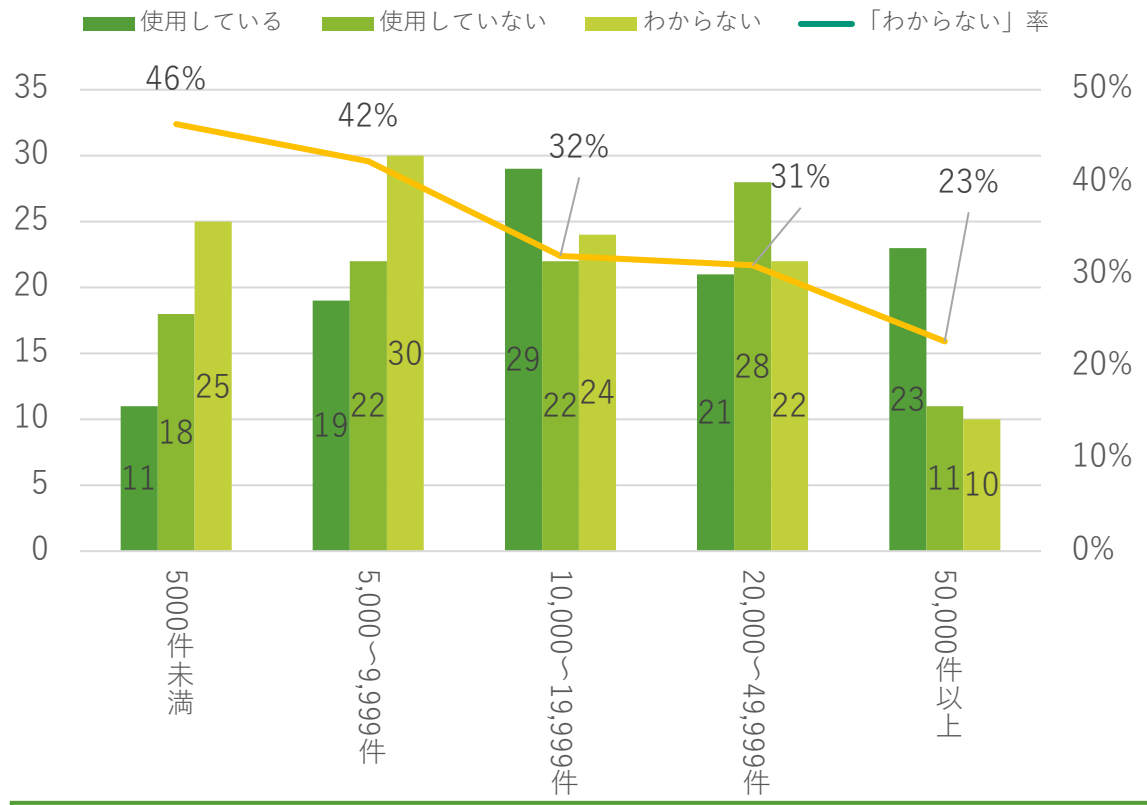


年間健診実施数の多さに応じて、サイバー攻撃リスクへの感受率も高い傾向がある

＜アンケート調査結果_年間健診数別(2/7)＞

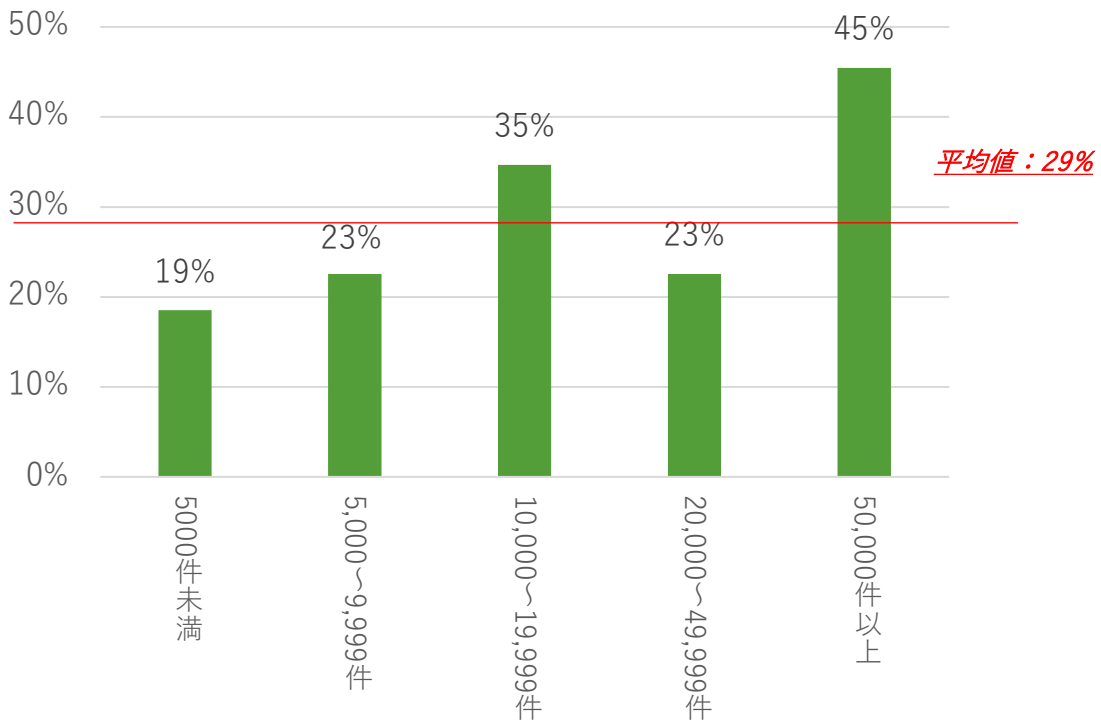
【脆弱性対策】

<③：厚労省等から脆弱性が指摘されたForitnet社製VPN機器を使用している施設割合＞ ※N＝315



<④：③が「使用している」の場合、脆弱性対応済みの施設割合＞

※N＝103

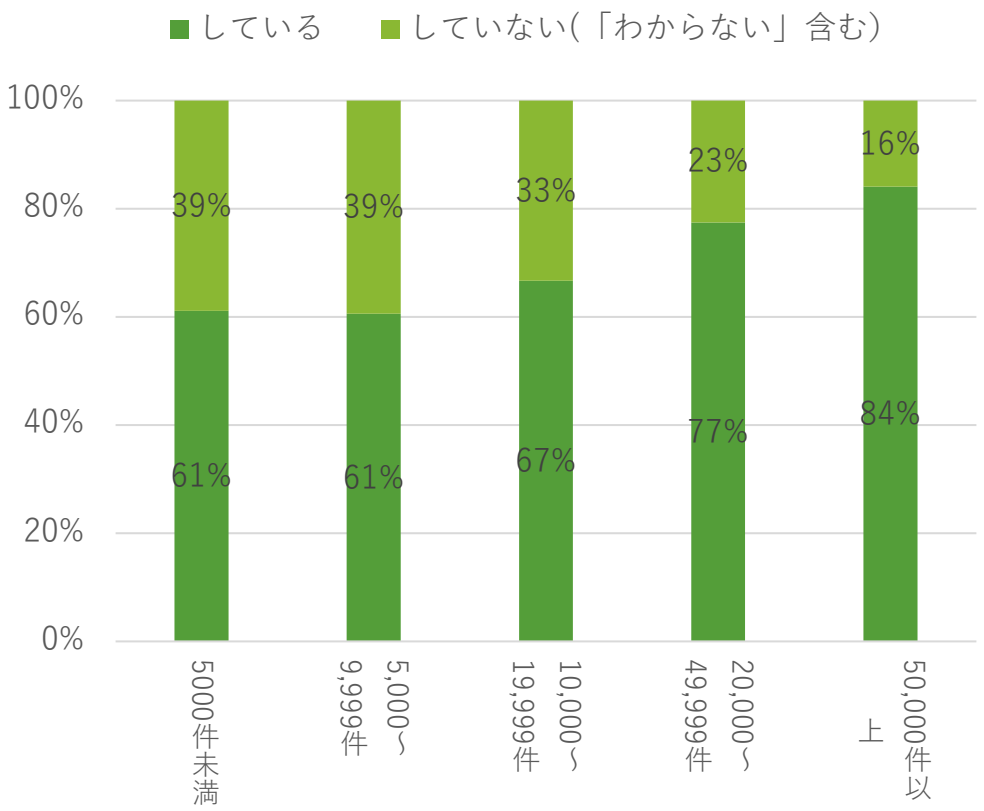


年間健診実施数の多さに応じて、施設内で利用されるVPN機器の把握率が高く（「わからない」率が低い）、かつ、脆弱性への対応も完了している傾向が示されている。

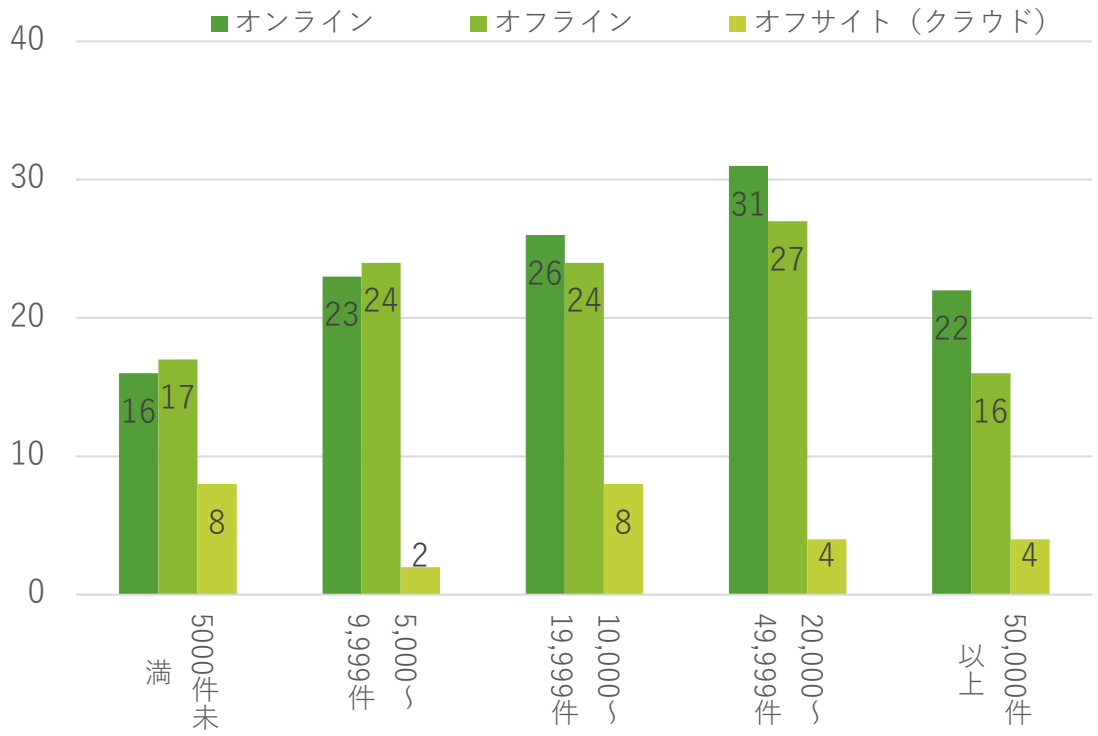
＜アンケート調査結果_年間健診数別(3/7)＞

【バックアップ対策】

＜⑥-1：バックアップの取得率＞ ※N＝315



＜⑥-2：バックアップの取得方式（件数：複数選択式）＞ ※N＝252



<u>バックアップの取得率の高低も年間健診実施数の多寡と比例する</u>関係にあるが、
<u>オフラインでのバックアップ取得率は平均的に全てにおいて高い</u>状況である。

＜アンケート調査結果_年間健診数別(4/7)＞

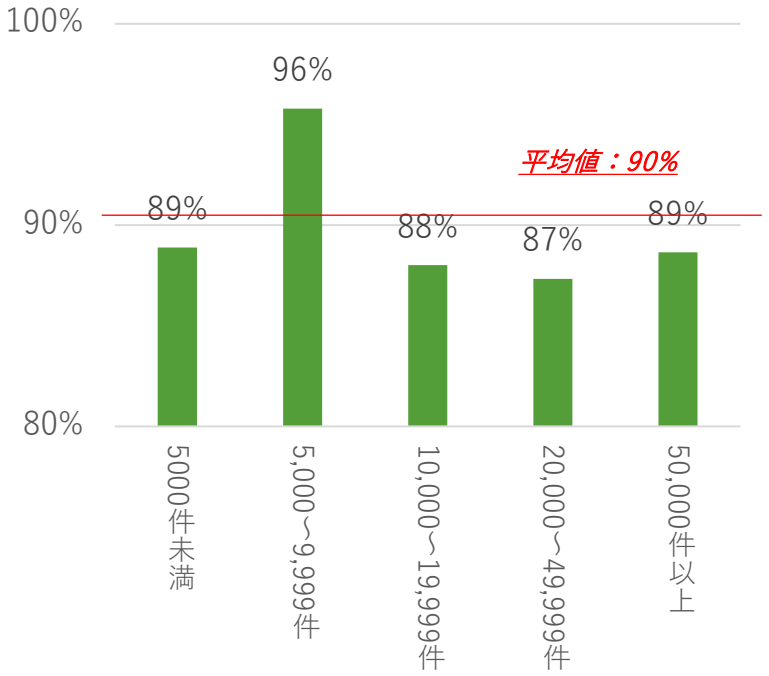
【IT人材】 ※N＝315

＜⑦：IT人材数＞

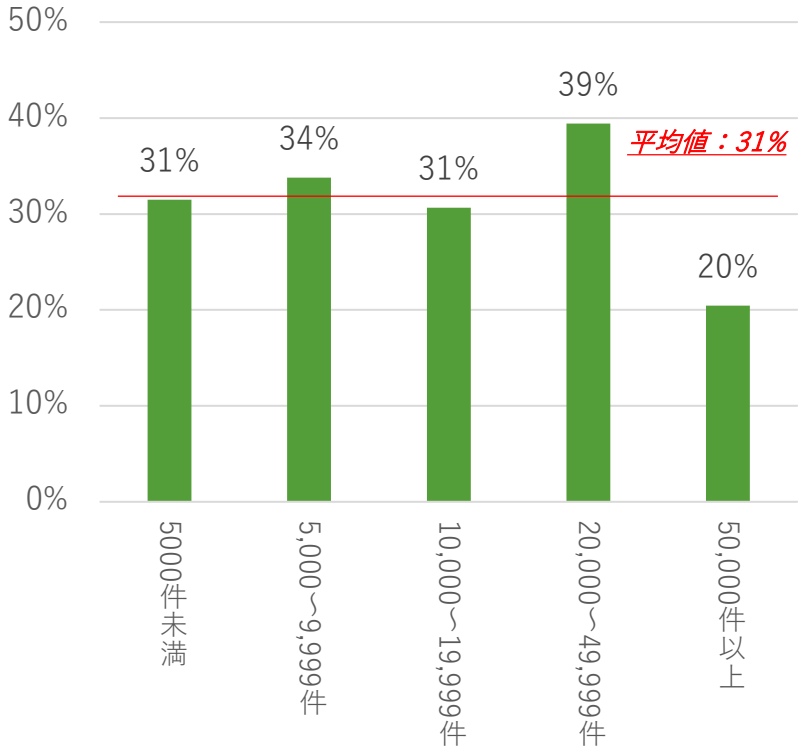
年間健診数	施設内システム担当者	うち、常勤数	常勤率
5000件未満	2.5人	2.2人	91%
5,000～9,999件	2.6人	2.5人	93%
10,000～19,999件	2.5人	2.2人	91%
20,000～49,999件	3.1人	2.8人	90%
50,000件以上	3.8人	3.6人	96%

【監査】 ※N＝315

＜⑧：厚労省安全管理GLを知っている施設割合＞



＜⑨：セキュリティ監査を一切実施していない施設割合＞

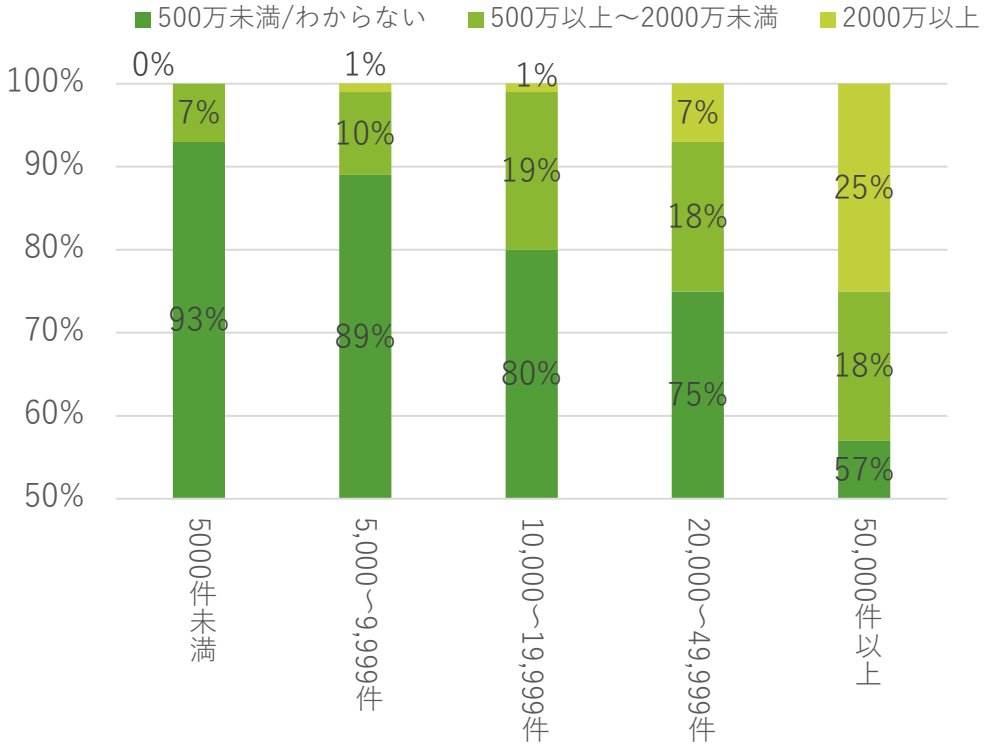


年間健診実施数が多いほどIT人材配置数が多いが、**厚生労働省安全管理GLの把握率は平均的に全ての区分で高い状況**である。
また、セキュリティ監査の非実施率も概ね健診実施数に比例しているが、**特に５万件以上の区分の大規模施設ではセキュリティ監査実施率が他区分と比較しても高い（未実施率が低い）**。

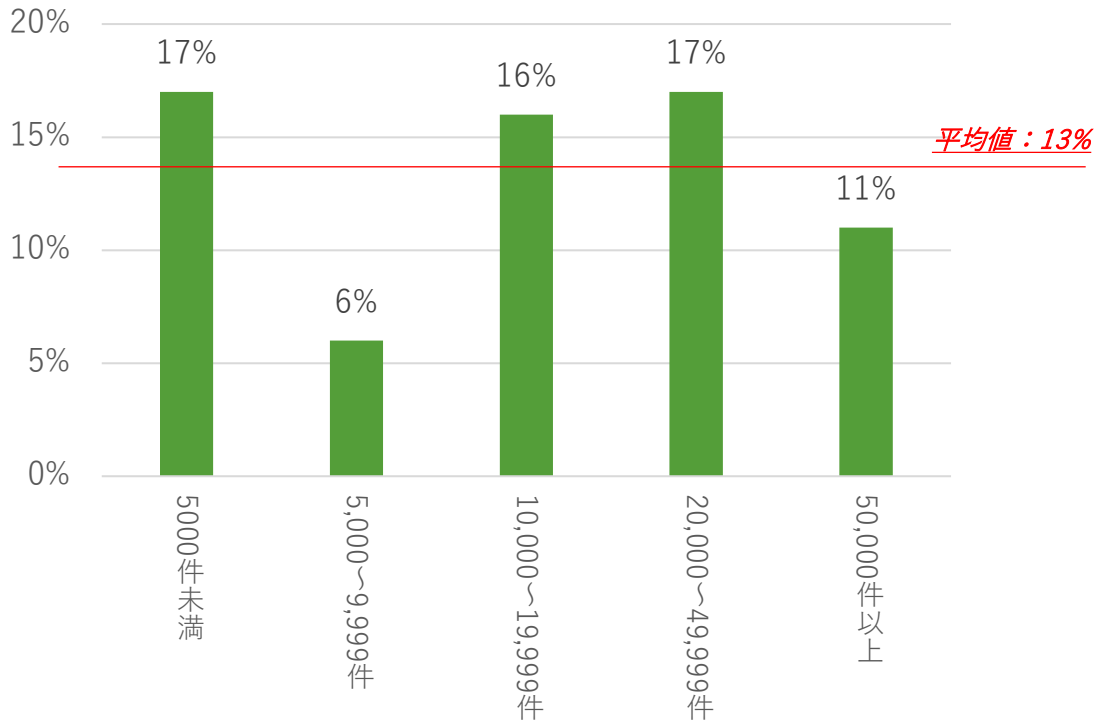
＜アンケート調査結果_年間健診数別(5/7)＞

【セキュリティ予算】 ※N＝315

＜⑩：年間のセキュリティ予算幅における施設別割合＞



＜⑪：セキュリティ予算が十分と回答した施設の割合＞

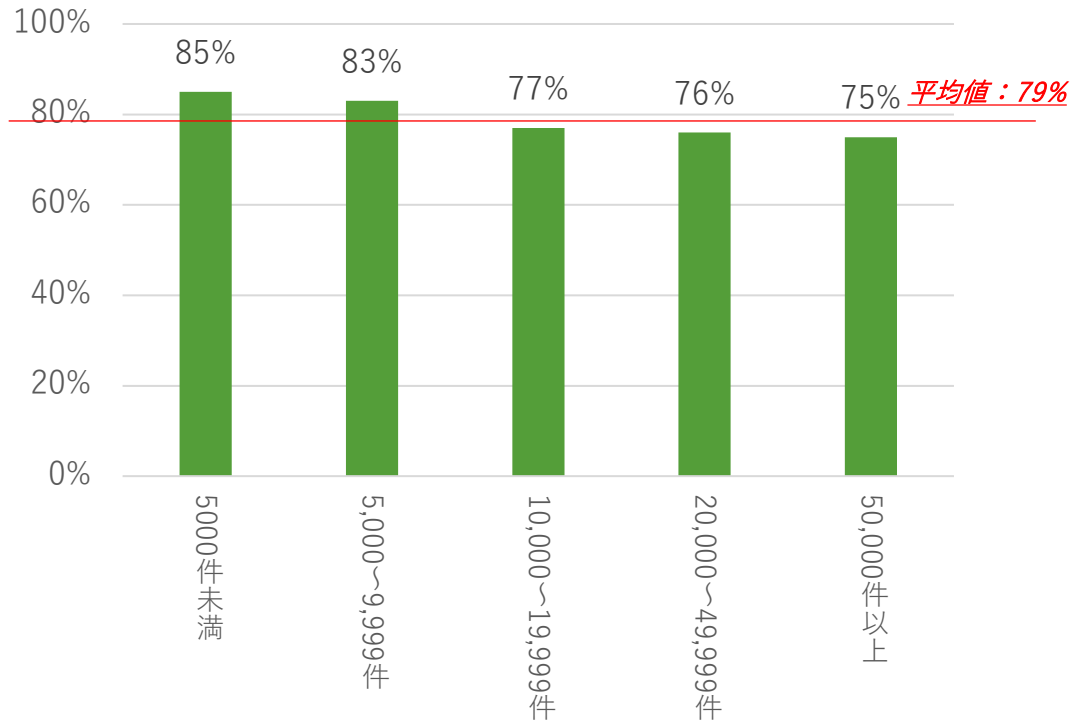


年間健診実施数とセキュリティ予算額もほぼ比例する関係にある。特に**健診数5千件以上の各区分施設における１割以上は500万以上の予算、さらに5万件以上の施設の4分の1は2000万以上の予算が確保されている**状況である。しかしながら、**セキュリティ予算が十分と回答した施設は全体平均で1割程度**であり、施設のIT規模とセキュリティ予算がかみ合っていない状況が見受けられる。

＜アンケート調査結果_年間健診数別(6/7)＞

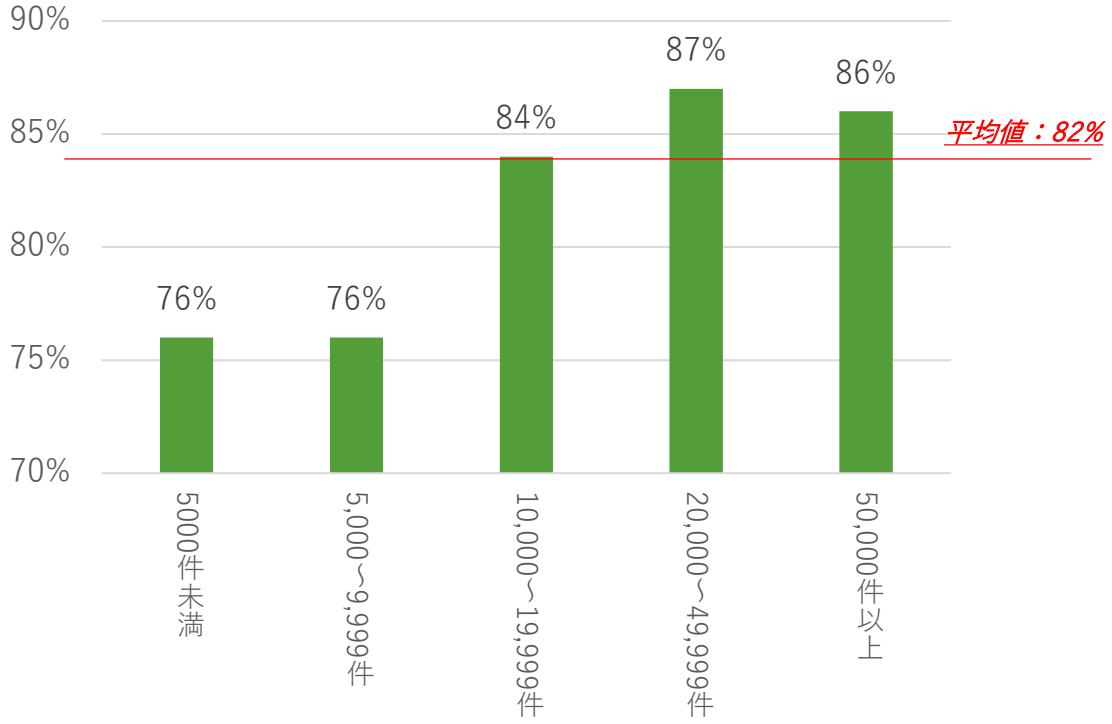
【サイバー保険】 ※N＝315

＜⑫：サイバー保険を「加入」以外で回答（「わからない」含む）した施設割合＞



【クローズドNWの安全性】 ※N＝315

＜⑬：診療系NWは安全という考え方に何らかのかたちで「共感」すると回答した施設割合＞

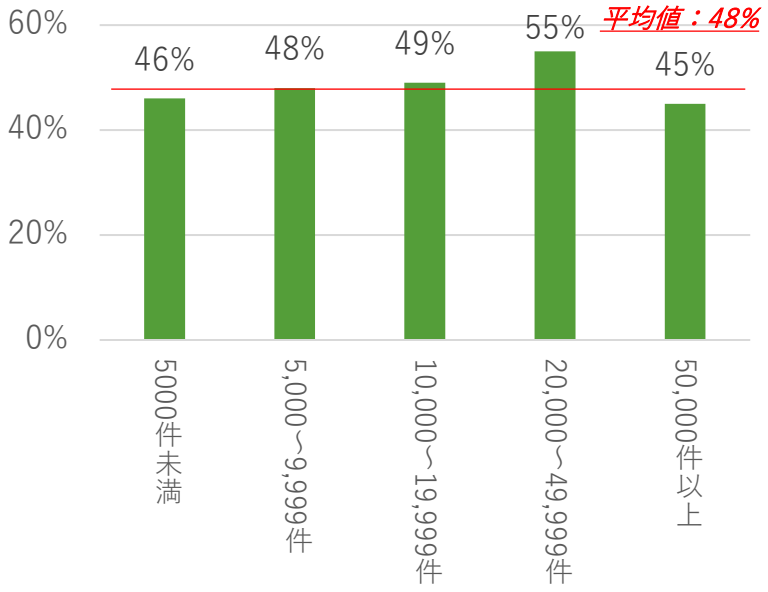


年間健診実施数が多いほどサイバー保険未加入率も低くなる傾向がある。
一方で、クローズドNWの安全神話への共感率は健診数の多さによって高まる傾向があり、**サイバー保険に加入していない、健診数の少ない施設ほど、隠れた外部との接続リスクに対する感度が高い**といえる。

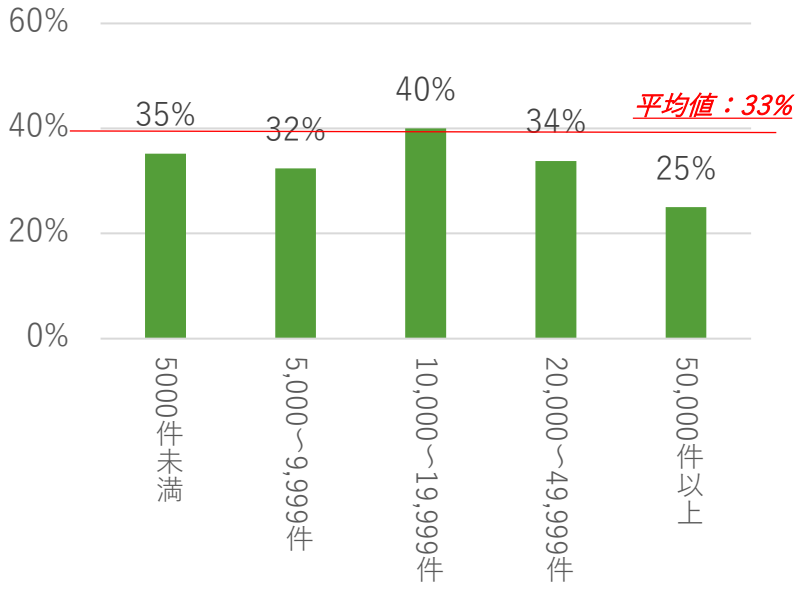
＜アンケート調査結果_年間健診数別(7/7)＞

【システム提供事業者とのコミュニケーション状況】 ※N＝315

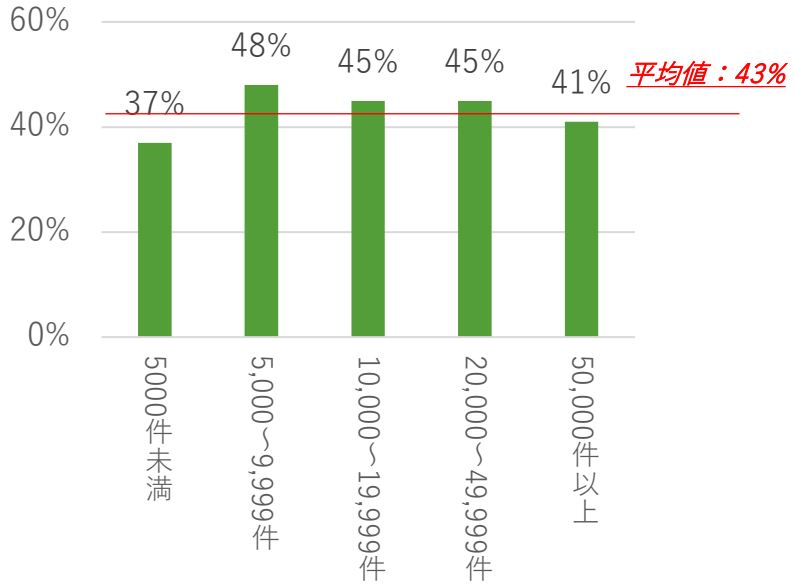
＜⑭：IT事業者によるセキュリティ対策の「指示を受けている」と回答した施設割合＞



＜⑮：IT事業者とのセキュリティ契約を「締結している」と回答した施設割合＞



＜⑯：IT事業者のセキュリティ対応を「信頼」していると回答した施設割合＞



年間健診実施数の各区分において、IT事業者に対するユーザセキュリティの実施内容の確認率、セキュリティ面も含めた契約締結率、IT事業者への信頼率はほぼ同率の状況と言える。5万件以上区分でIT業者との契約締結率の低さ、5千件未満区分でIT事業者への信頼率の低さが一部見受けられるが、大きな偏りはなく、健診数の多寡自体が、IT事業者とのコミュニケーション率に大きな影響を及ぼしていることはないと言える。

４．施設類型別結果

＜アンケート調査結果総評_施設類型別＞

- 施設類型別（施設単独/病院併設/その他）でみると、**どの類型においてもほぼ同等の高い水準でサイバー攻撃への脅威を感じている**状況である。

- 一方、**病院併設型**において、相対的に、脆弱性の指摘されたVPN機器の「わからない」率が高く、また脆弱性対応完了率も低く、さらにはバックアップ取得率も低い傾向が示されている。ただし、バックアップ取得方式では、病院併設型も含め全ての類型において、オフラインでのバックアップ率が半数以上と高い割合で実施されている。

- 「その他」型は、IT人材配置数が多い一方で、セキュリティ監査の未実施率が高い状況であった。ただし、「その他」型も含め、**厚労省安全管理GLの把握率はどの施設類型においても共通的に高い**。

- **施設単独型が500万以上のセキュリティ予算確保の割合が高く（3割弱）、また施設単独型・「その他」ともに、2000万以上のセキュリティ予算率が1割強**に及んでいる。そのため、「施設単独型」がセキュリティ予算が十分と回答した割合がもっとも高いと考えられる一方、特に500万以上の予算確保率がもっとも低い病院併設型が予算が不十分と回答するに至っていると考えられる。

- **「その他」類型がもっともサイバー保険加入率が高く、病院併設型が最も低い傾向**が示されている。そのため、**病院併設型がもっとも外部接続リスクへの感度が高く、「その他」類型が最も感度が低い**結果になっているといえる。

- IT事業者によるユーザセキュリティ指示率は「その他」類型がもっとも高く、そのため事業者への信頼度も高い傾向である。一方で、施設単独/病院併設型ではユーザセキュリティ指示率/IT事業者への信頼率はほぼ同水準（4割前後）で、セキュリティ面も含めた契約率も相対的に高い状況（3割前後）ではあるが、**おおよそ1割程度は契約がない中で、ユーザセキュリティを教授されているのみであるため、その信用度（情報アップデートも含め）には不安が残る**というべきであろう。

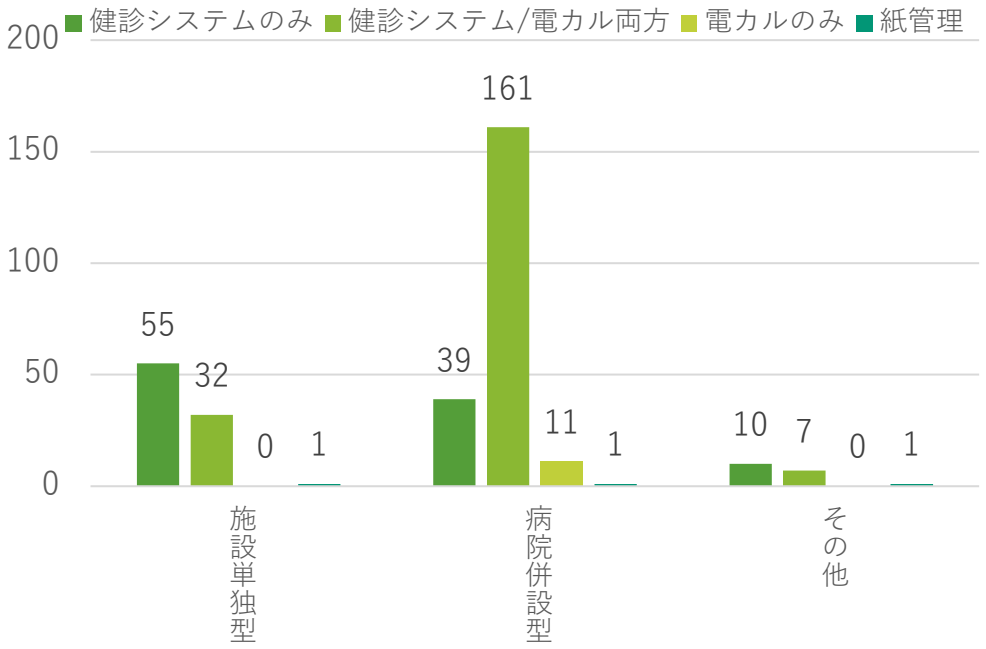
- 総合すると、健診分野では、**施設単独型が最も平準的な取組**、VPN機器の脆弱性対応を行い、オフライン保管も含めたバックアップ取得が行えており、厚労省安全管理GLを把握する相応のIT人材配置数のもとで、セキュリティ監査を実施する等の取組が行えていると言える。ただし、**当該施設類型も含め、セキュリティ予算の不十分さ**は訴えられている。また、IT事業者とのリスクコミュニケーションにおいても、**一部はTI事業者との契約もないなかで、業者を信用している施設も見受けられており、こうした「甘え」は見直される必要がある**といえる。

＜アンケート調査結果_施設類型別(1/7)＞

【ITの利用形態】

＜①：ITの利用形態(件数) ＞　※N＝318

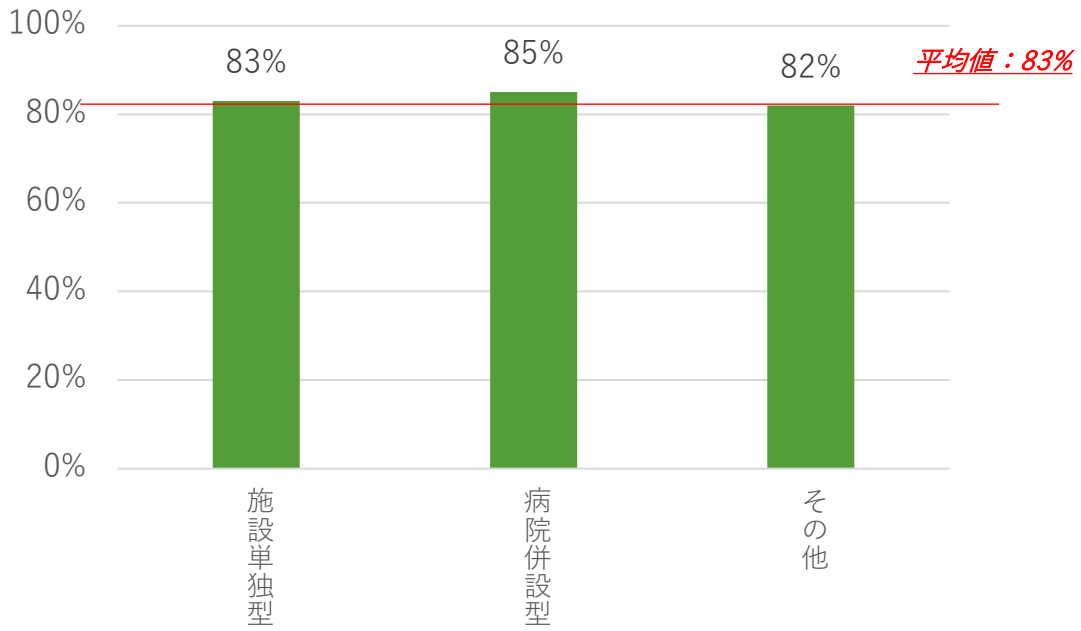
※：以降の調査は紙管理施設は対象外



※「その他」の内訳：
診療所併設型、施設健診/巡回健診型、巡回専門型、無床診療所

【サイバー攻撃への脅威】

＜②：サイバー攻撃への脅威を感じている施設割合＞　※N＝315



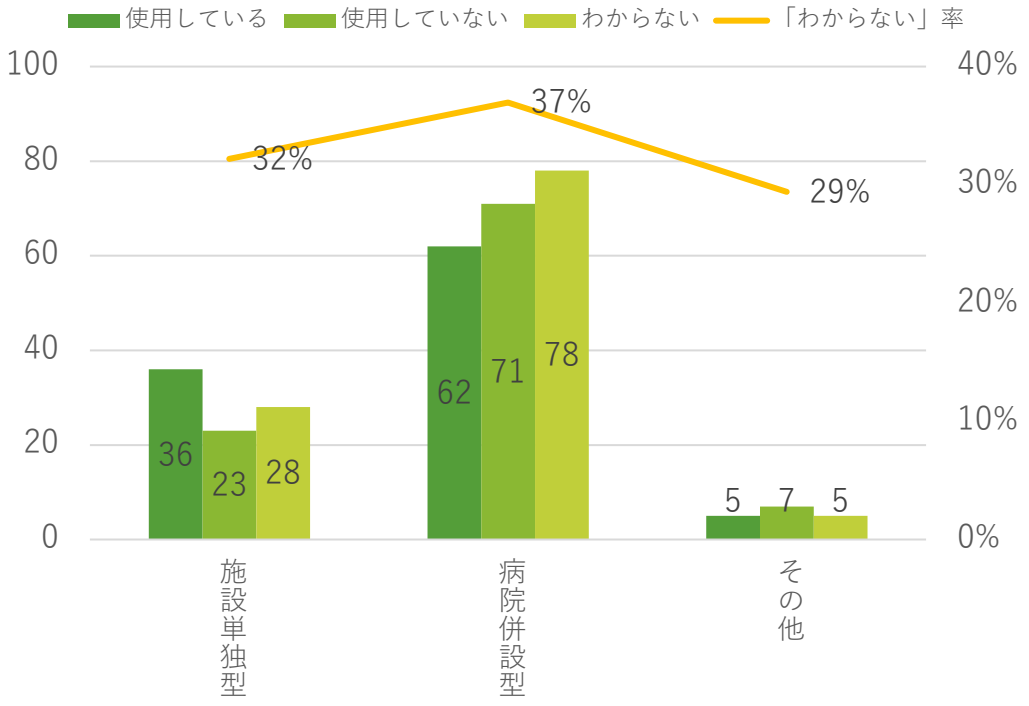
施設類型別でみると、**どの類型においてもほぼ同等の高い水準でサイバー攻撃への脅威を感じている**状況である。

＜アンケート調査結果_施設類型別(2/7)＞

【脆弱性対策】

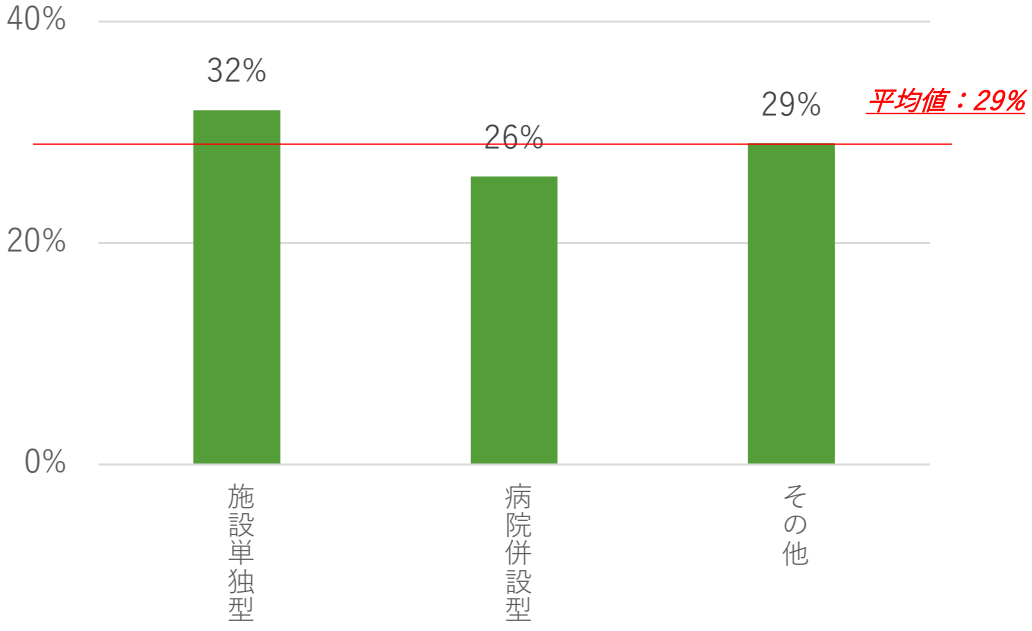
<③：厚労省等から脆弱性が指摘されたForitnet社製VPN機器を使用している施設件数>

※N＝315



<④：③が「使用している」の場合、脆弱性対応済みの施設割合>

※N＝103

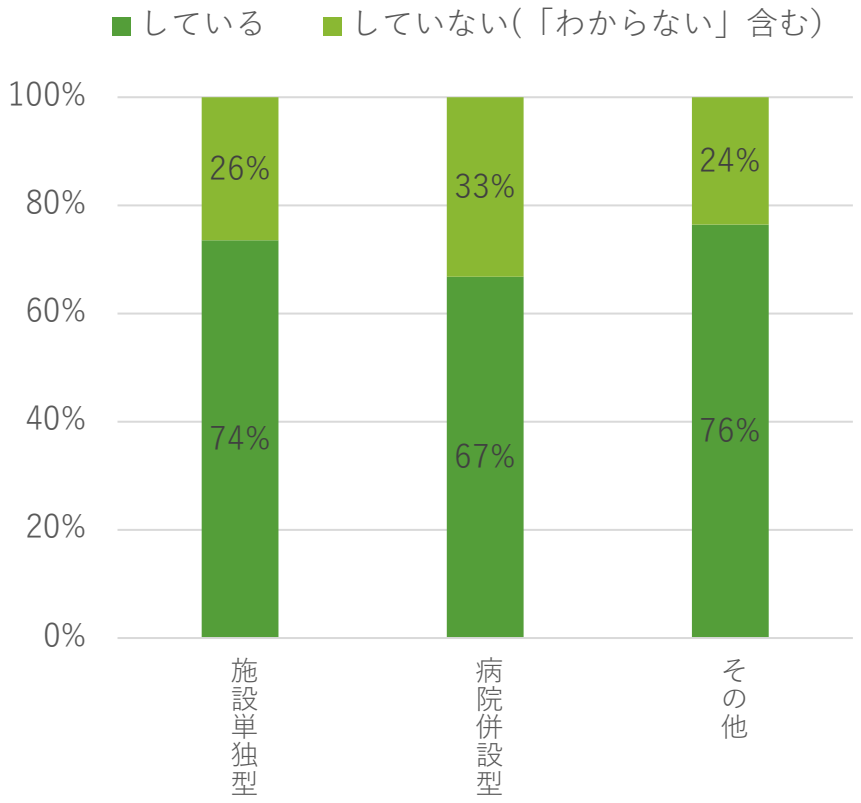


病院併設型において、相対的に、脆弱性の指摘されたVPN機器の「わからない」率が高く、
また脆弱性対応完了率も低い状況といえる。

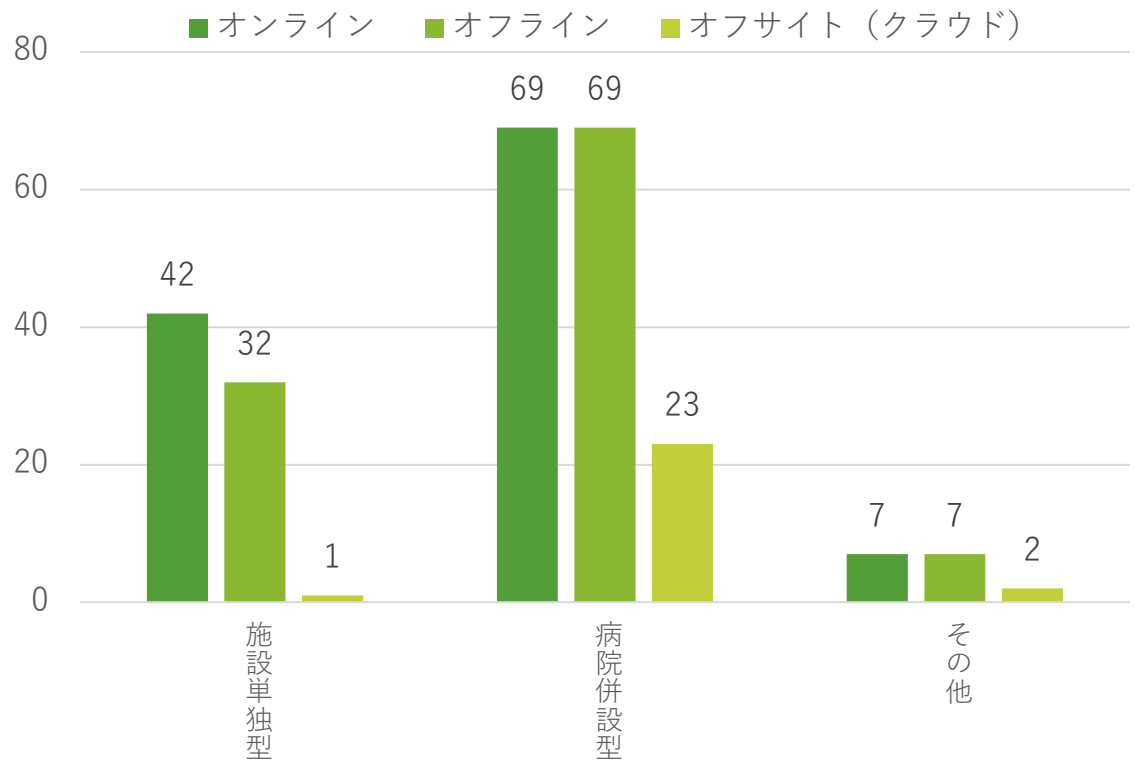
＜アンケート調査結果_施設類型別(3/7)＞

【バックアップ対策】

<⑥-1：バックアップの取得率＞ ※N＝315



<⑥-2：バックアップの取得方式(複数選択式）＞ ※N＝252



病院併設型においてバックアップ取得率が相対的に低いが、**オフラインでのバックアップ取得はどの施設類型においても半数程度が実施している**状況である。

＜アンケート調査結果_施設類型別(4/7)＞

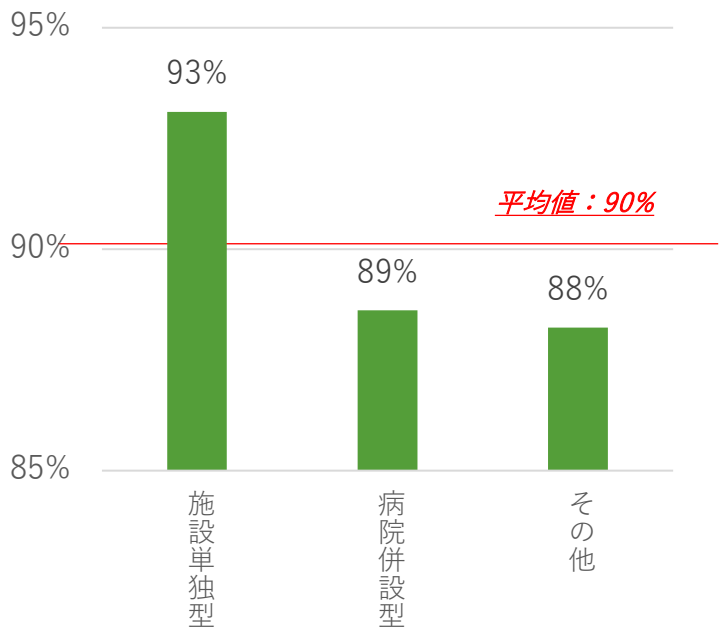
【IT人材】 ※N＝315

＜⑦：IT人材数＞

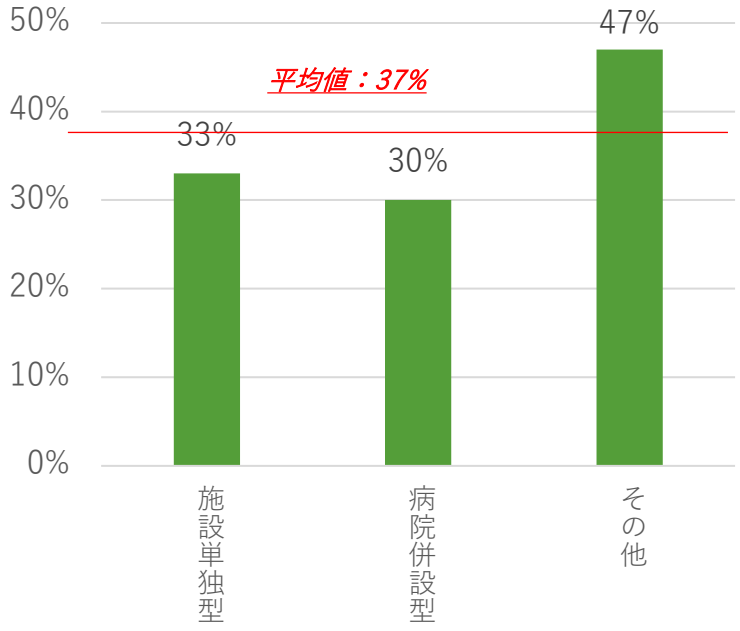
施設別類型	施設内システム担当者	うち、常勤数	常勤率
施設単独型	2.7人	2.5人	92%
病院併設型	2.9人	2.6人	92%
その他	3.1人	2.7人	89%

【監査】 ※N＝315

＜⑧：厚労省安全管理GLを知っている施設割合＞



＜⑨：セキュリティ監査を一度も実施していない施設割合＞

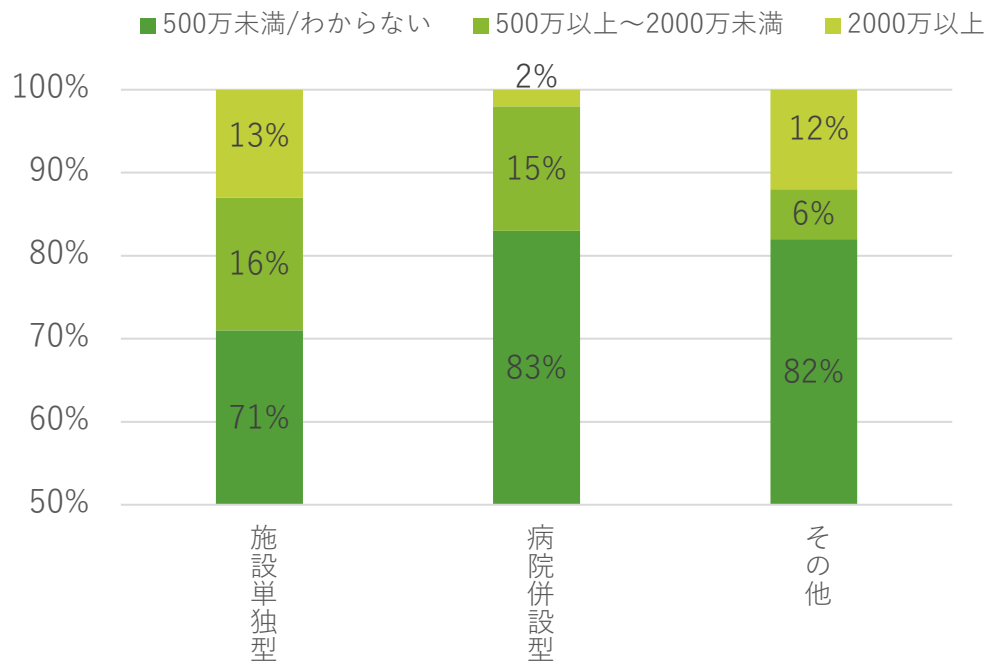


「その他」型は、IT人材配置数が多い一方で、セキュリティ監査の未実施率が高い。
なお、**厚労省安全管理GLの把握率はどの施設類型においても共通的に高い。**

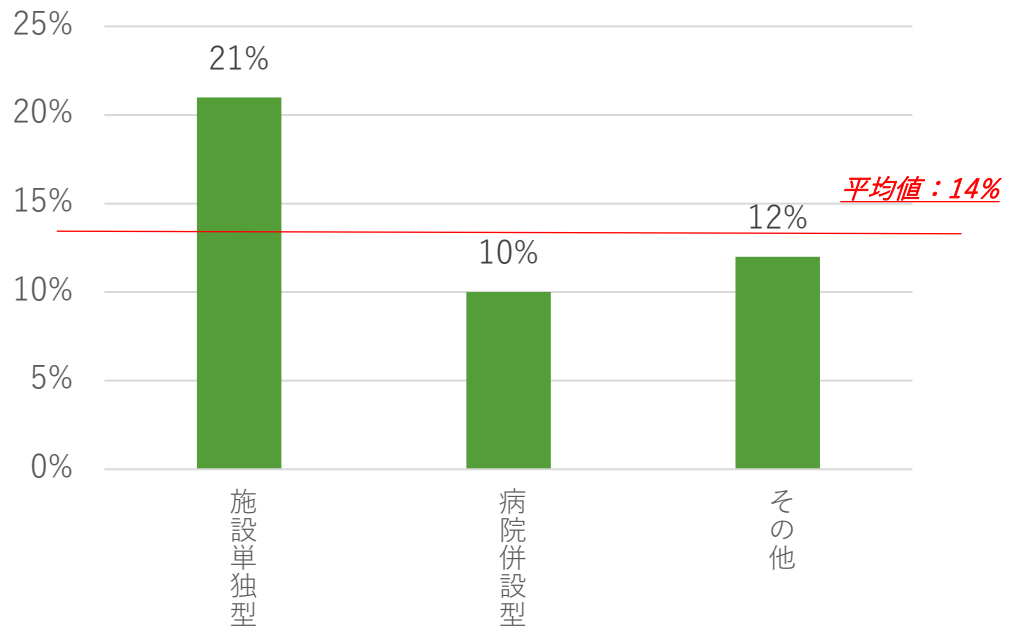
＜アンケート調査結果_施設類型別(5/7)＞

【セキュリティ予算】 ※N＝315

＜⑩：年間のセキュリティ予算幅の施設類型別割合＞



＜⑪：セキュリティ予算が十分と回答した施設の割合＞

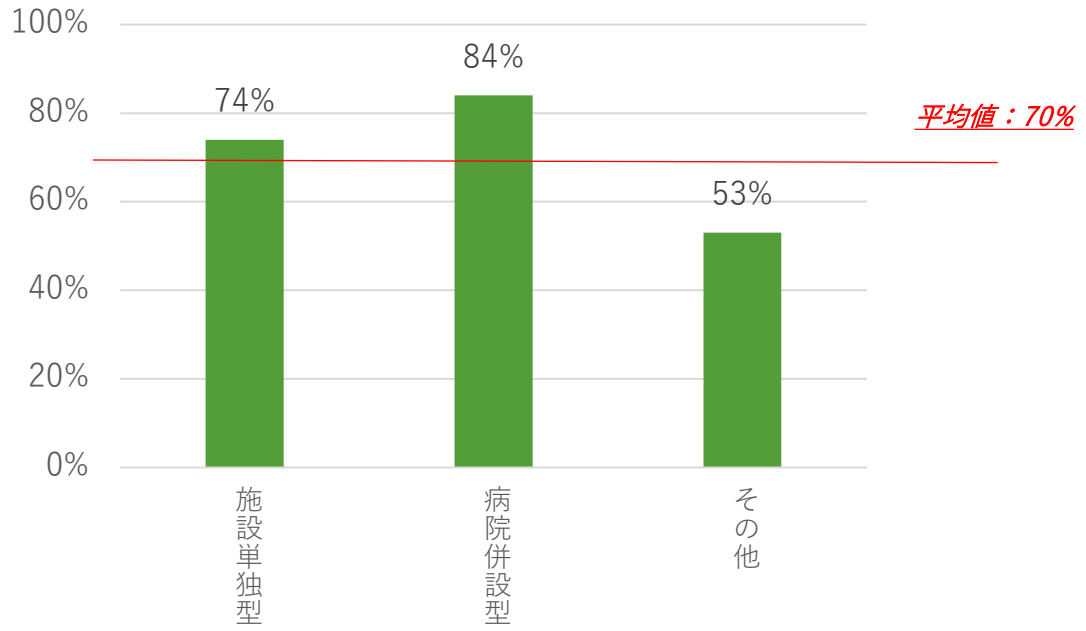


施設単独型が500万以上のセキュリティ予算確保の割合が高く（3割弱）、また「施設単独型」「その他」ともに、2000万以上のセキュリティ予算率が1割強に及んでいる。そのため、**「施設単独型」がセキュリティ予算が十分と回答した割合がもっとも高いと考えられる一方、特に500万以上の予算確保率がもっとも低い病院併設型が予算が不十分と回答する**に至っているといえる。

＜アンケート調査結果_施設類型別(6/7)＞

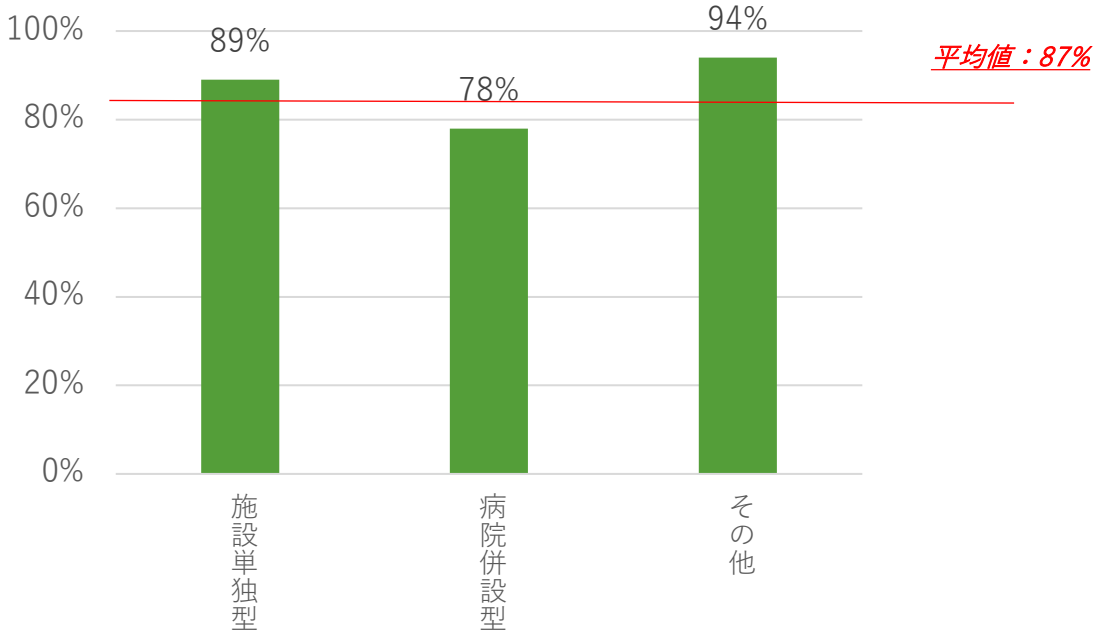
【サイバー保険】 ※N＝315

＜⑫：サイバー保険を「加入」以外（「わからない」含む）で回答した施設割合＞



【クローズドNWの安全性】 ※N＝315

＜⑬：診療系NWは安全という考え方に何らかのかたちで「共感」すると回答した施設割合＞

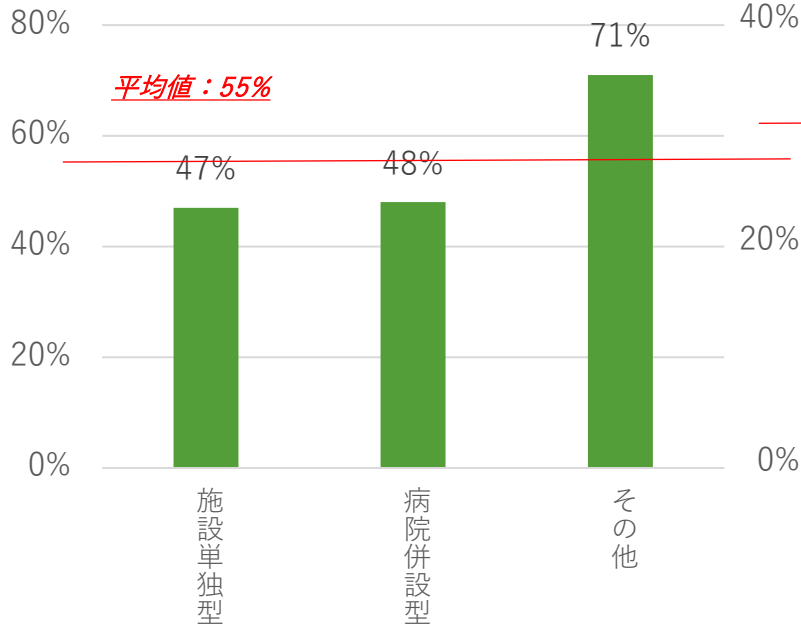


「その他」類型がもっともサイバー保険加入率が高く、病院併設型が最も低い傾向が示されている。こうした背景もあり、**病院併設型がもっとも外部接続リスクへの感度が高く、「その他」類型が最も感度が低い**結果になっているといえる。

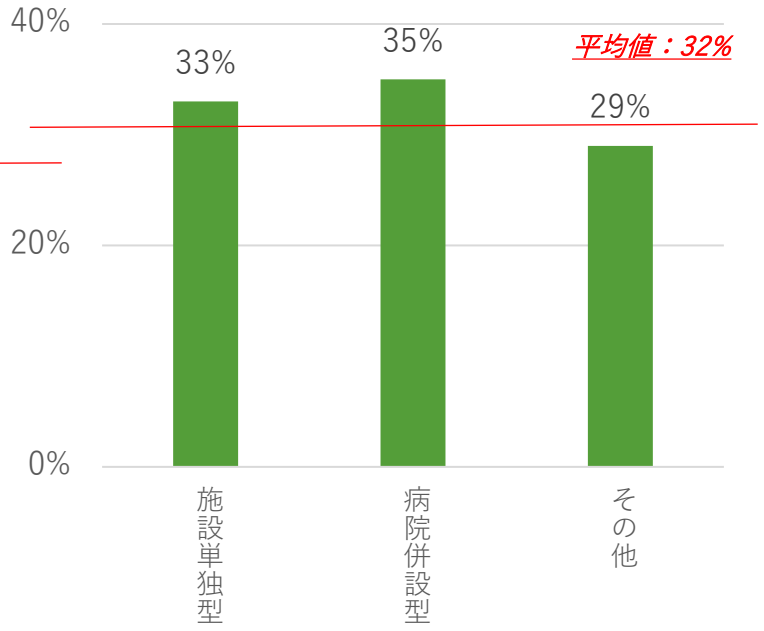
＜アンケート調査結果_施設類型別(7/7)＞

【システム提供事業者とのコミュニケーション状況】 ※N＝315

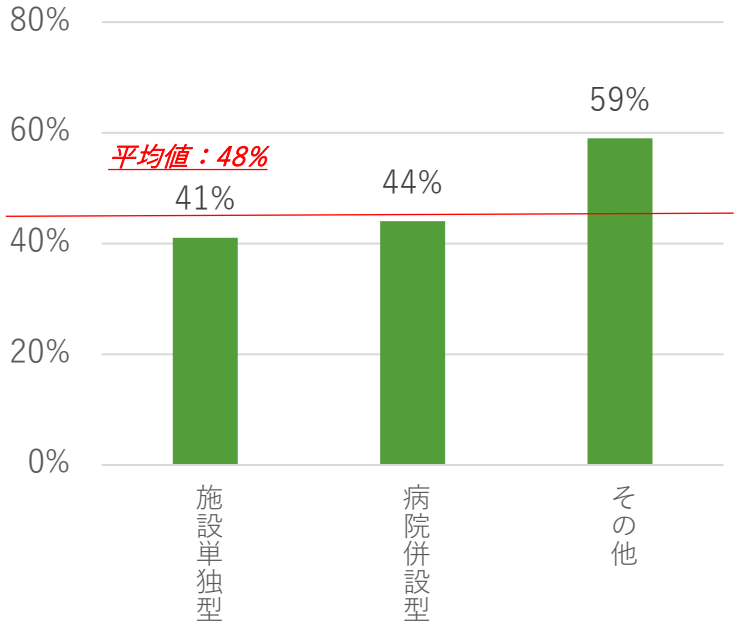
＜⑭：IT事業者によるセキュリティ対策の「指示を受けている」と回答した施設割合＞



＜⑮：IT事業者とのセキュリティ契約を「締結している」と回答した施設割合＞



＜⑯：IT事業者のセキュリティ対応を「信頼」していると回答した施設割合＞



IT事業者によるユーザセキュリティ指示率は「その他」類型がもっとも高く、そのため事業者への信頼度も高い傾向である。
一方で、施設単独/病院併設型ではユーザセキュリティ指示率/IT事業者への信頼率はほぼ同水準（4割前後）で、セキュリティ面も含めた契約率も相対的に高い状況（3割前後）ではあるが、**おおよそ1割程度は契約がない中で、ユーザセキュリティを教授されているのみであるため、その信用度（情報アップデートも含め）には不安が残る**といえる。

５．IT利用環境(IT活用度）別結果

＜アンケート調査結果総評_IT利用環境別＞

- 調査対象組織におけるIT利用環境（「健診システムのみ利用」「健診システム+電カル連携」「電カルのみ利用」）、つまりIT活用度に係る３つの観点よりアンケート結果を整理したところ、**サイバー攻撃リスクへの感度は全体的に高水準である。**

- **電カルのみの利用施設では、VPN機器の利用状況の非把握率（「わからない」率）が高く、かつ、脆弱性対応完了率が低い**状況である。なお、**バックアップ取得率については、電カルとの連携/利用が含まれると全体的に低下する**傾向があるが、**オフラインバックアップ取得率はどの環境においても同水準で高い**状況である。

- **電カル利用のみ施設におけるIT担当者配置数が多いが、厚労省安全管理GLの把握率がも低く、セキュリティ監査も実施率が低い**ことが示されている。ただし、**いずれの利用環境においてもGL把握率は8割以上を占め、セキュリティ監査実施率も5割以上を占めている。**

- **健診システムのみ利用施設は2000万以上のセキュリティ予算の確保率が1割以上に及ぶ**一方、**電カルを利用する環境条件が高まると、それに応じて予算が少なくなる状況である**。また、健診システムの利用組織はセキュリティ予算は十分と回答する割合が相対的に多い一方、**電カル利用型の組織ではその割合が低下**していく傾向がある。

- **サイバー保険の未加入率は、健診システムのみ利用組織が高く、電カルのみ利用組織が低い**状況である。これに反比例するように、**診療系NWの安全神話＝外部接続リスクへの鈍感度は健診システムのみ利用組織がもっとも高いが、電カルのみ利用組織は相対的に低い**状況である。

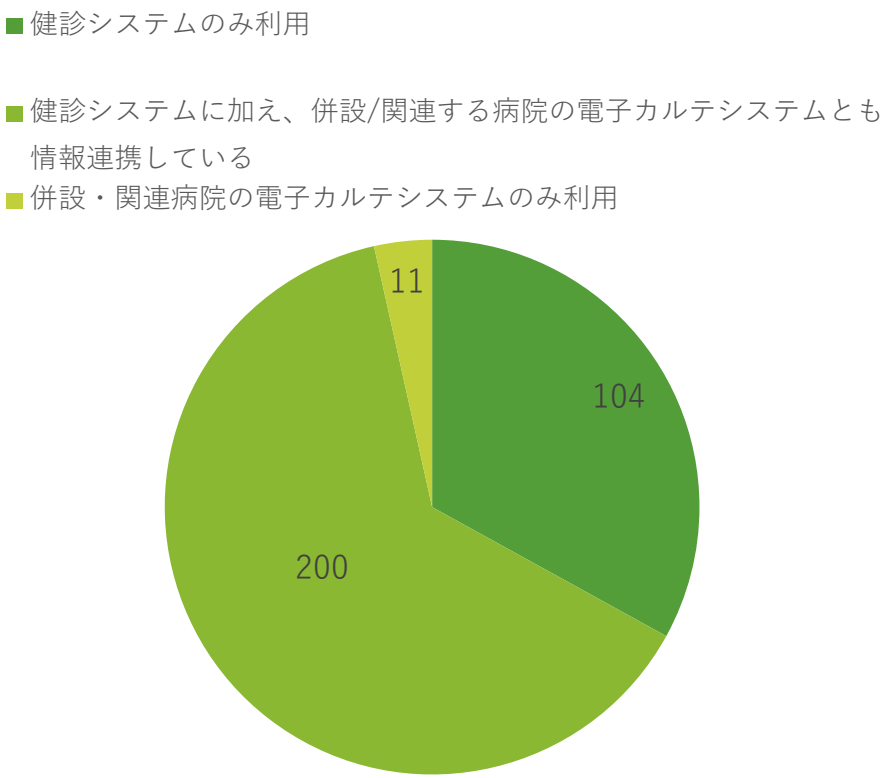
- **健診システム＋電カル連携施設がIT事業者によるユーザセキュリティ指示率/IT事業者との契約締結率が最も高く、かつ、IT事業者への信頼率も高い**状況である。一方、**電カルのみ利用施設はそれらの割合が最も低く、IT事業者との契約締結率とともに、信頼率も低い傾向**が示されている。

- 総合すると、IT活用度の観点では、**健診システムのみ利用施設のほうがVPN機器の脆弱性対応やバックアップ取得率も高まる**傾向がある。**これはセキュリティ予算の規模、あるいは十分性への考え方とも連動**している一方で、IT事業者との付き合い方 --- リスクコミュニケーション --- を考えた場合、健診システム＋電カル連携施設がその取組率が最も高いものの、電カルのみ利用施設は特にIT事業者への信頼率が低い等、**電カル利用有無がIT事業者とのリスクコミュニケーション水準の程度に影響を与えていることが把握できる。**

＜アンケート調査結果_ IT利用環境別(1/7)＞

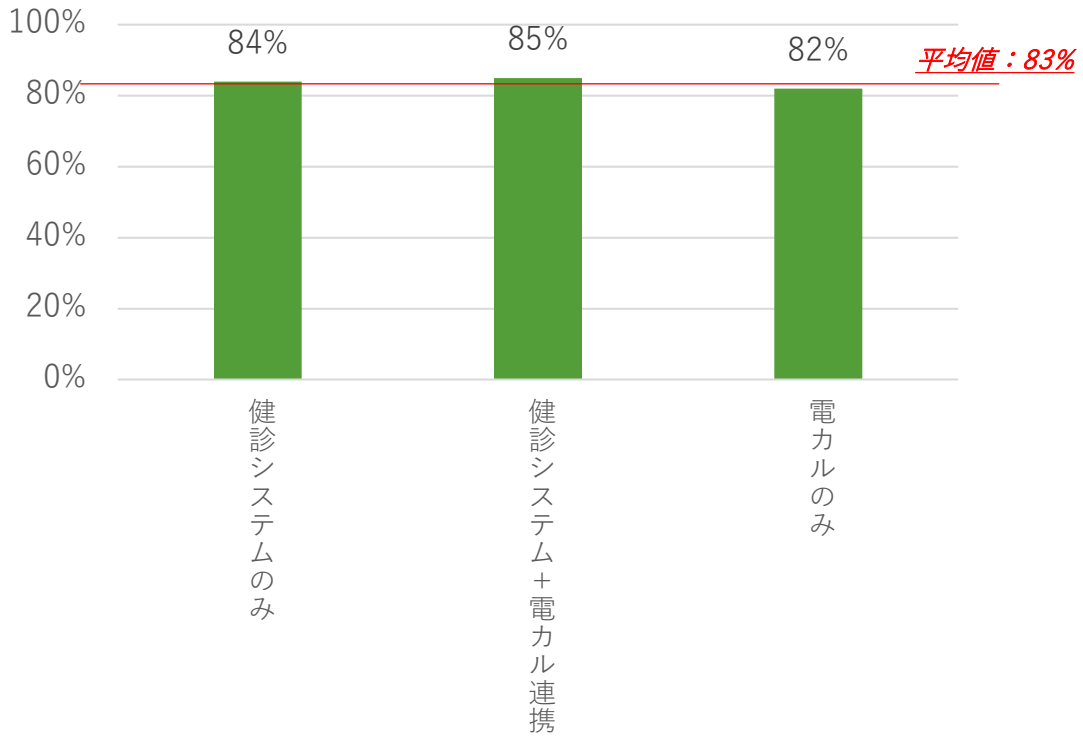
【ITの利用形態】

＜①：ITの利用形態(件数）＞　※N=315



【サイバー攻撃への脅威】

＜②：サイバー攻撃への脅威を感じている施設割合＞　※N＝315



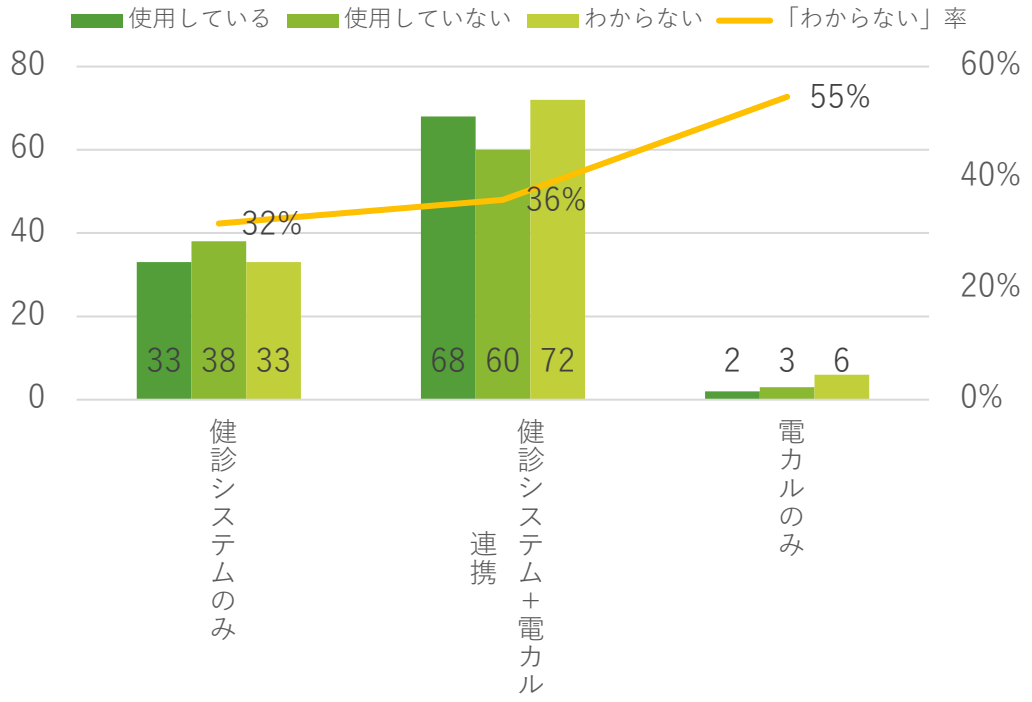
サイバー攻撃リスクへの感度は、IT利用環境によって大きな差はなく、**平均的に高水準である。**

＜アンケート調査結果_ IT利用環境別(2/7)＞

【脆弱性対策】

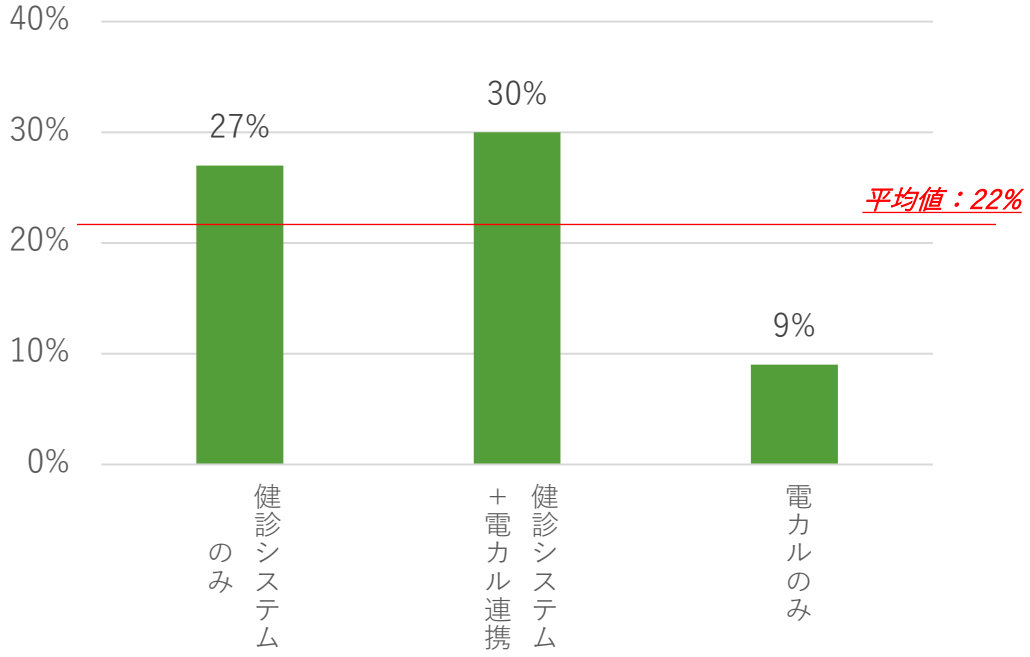
＜③：厚労省等から脆弱性が指摘されたForitnet社製VPN機器を使用している施設件数＞

※N＝315



＜④：③が「使用している」の場合、脆弱性対応済みの施設割合＞

※N＝103

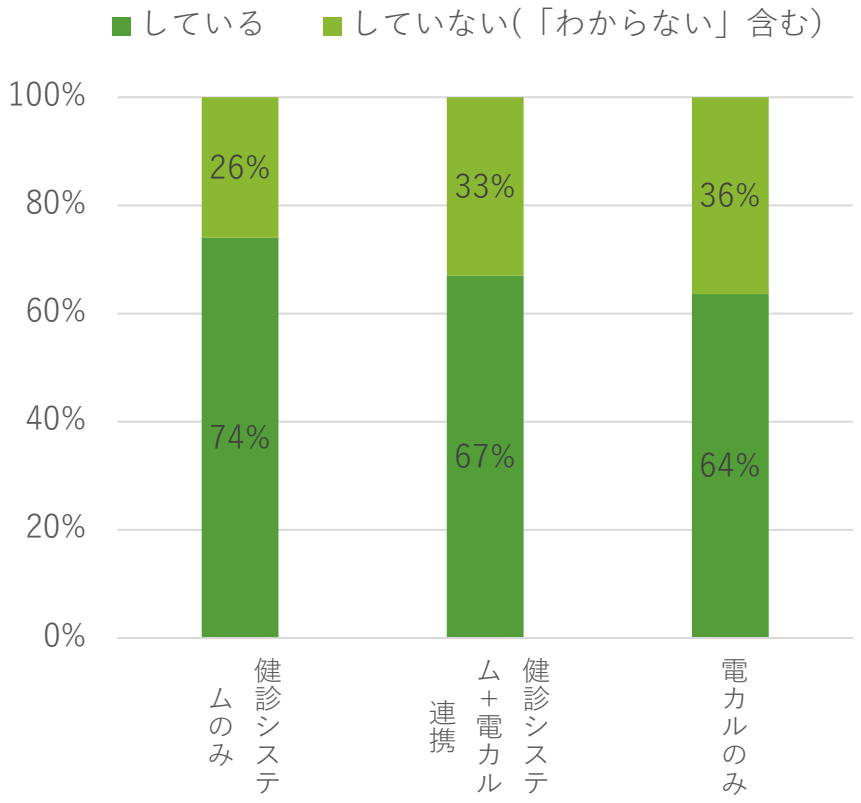


電カルのみ利用施設が最もVPN機器の利用状況の非把握率（「わからない」率）が高く、脆弱性対応完了率も低い状況である。

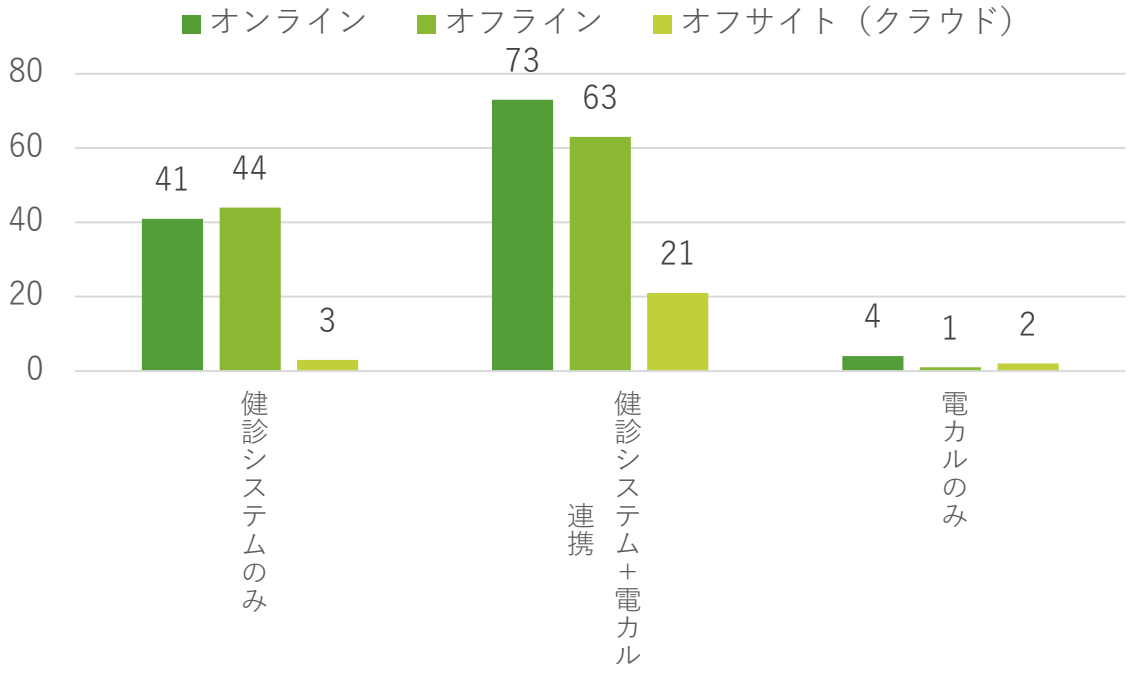
＜アンケート調査結果_ IT利用環境別（3/7）＞

【バックアップ対策】

＜⑥-1：バックアップの取得率＞ ※N＝315



＜⑥-2：バックアップの取得方式(件数/複数選択式）＞ ※N＝252



関連/併設施設の電カルがIT利用環境に含まるとバックアップ取得率が低下する傾向があるが、
オフラインバックアップ取得率はどの利用環境においても同じく高い状況である。

＜アンケート調査結果_ IT利用環境別(4/7)＞

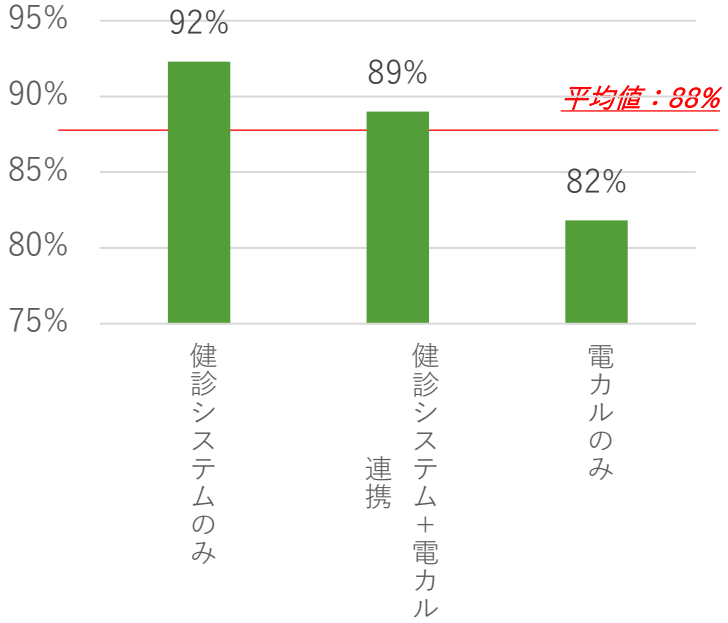
【IT人材】 ※N＝315

＜⑦：IT人材数＞

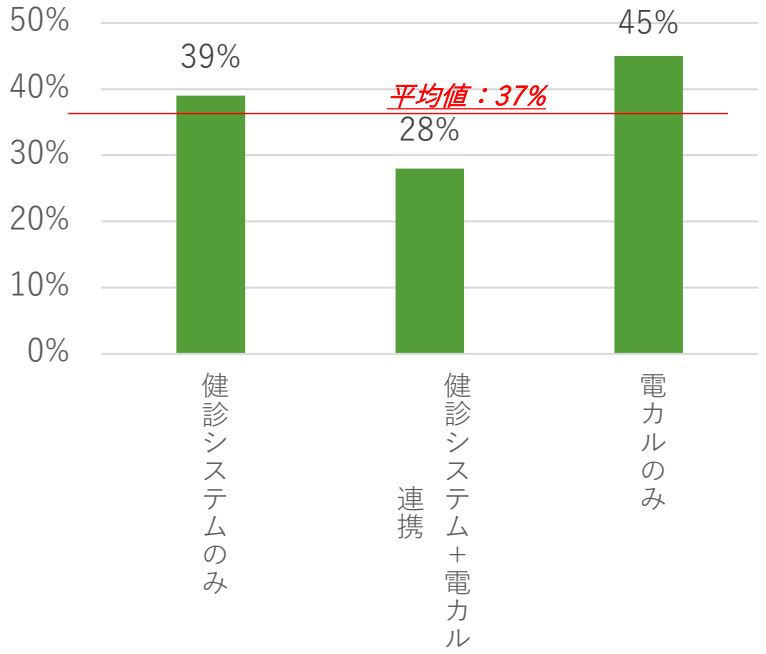
IT利用環境別	施設内システム担当者	うち、常勤数	常勤率
健診システムのみ利用	2.8人	2.6人	92%
健診システム＋電カル連携	2.8人	2.6人	92%
電カルのみ利用	3.4人	3.4人	100%

【監査】 ※N＝315

＜⑧：厚労省安全管理GLを知っている施設割合＞



＜⑨：セキュリティ監査を一度も実施していない施設割合＞

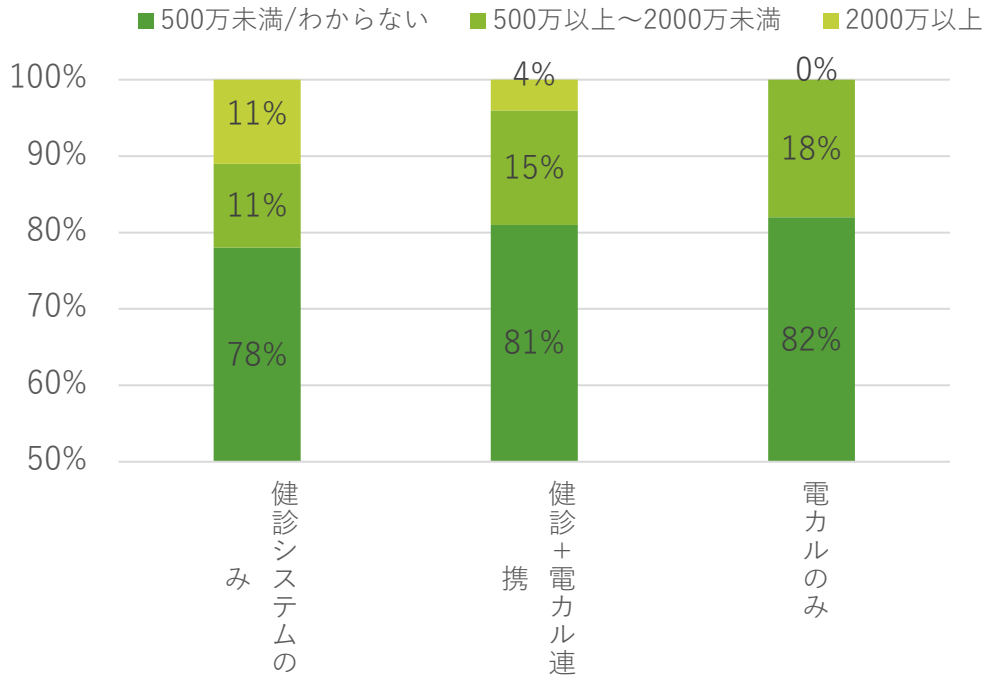


<u>電カル利用のみ施設</u>におけるIT担当者配置数が最も多い状況だが、
<u>厚労省安全管理GLの把握率は最も低く、セキュリティ監査の未実施率も高い</u>ことが示されている。

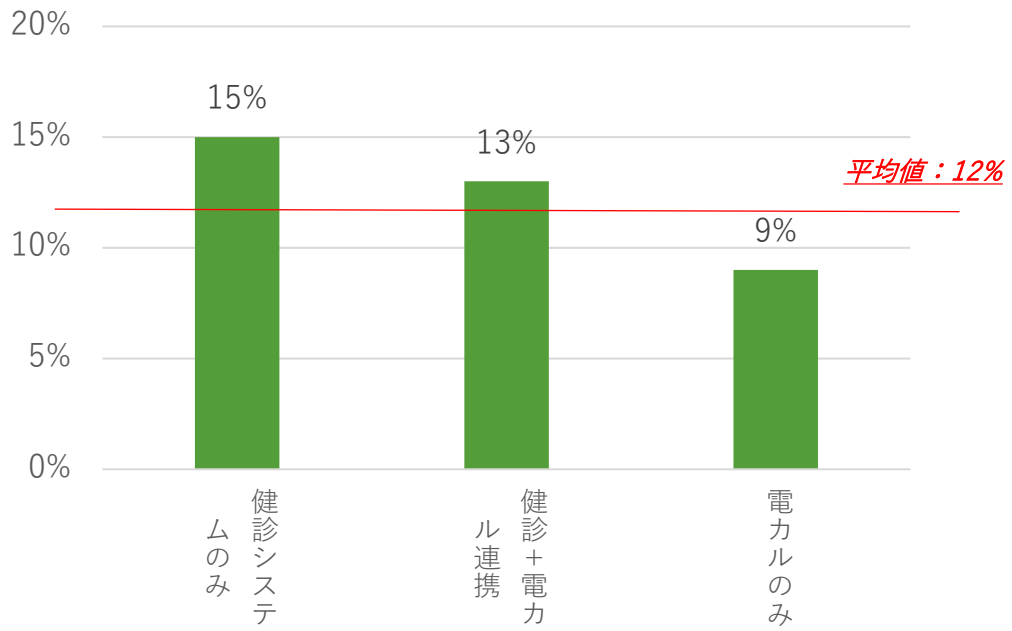
＜アンケート調査結果_ IT利用環境別(5/7)＞

【セキュリティ予算】 ※N＝315

＜⑩：年間のセキュリティ予算幅の環境別割合＞



＜⑪：セキュリティ予算が十分と回答した施設の割合＞

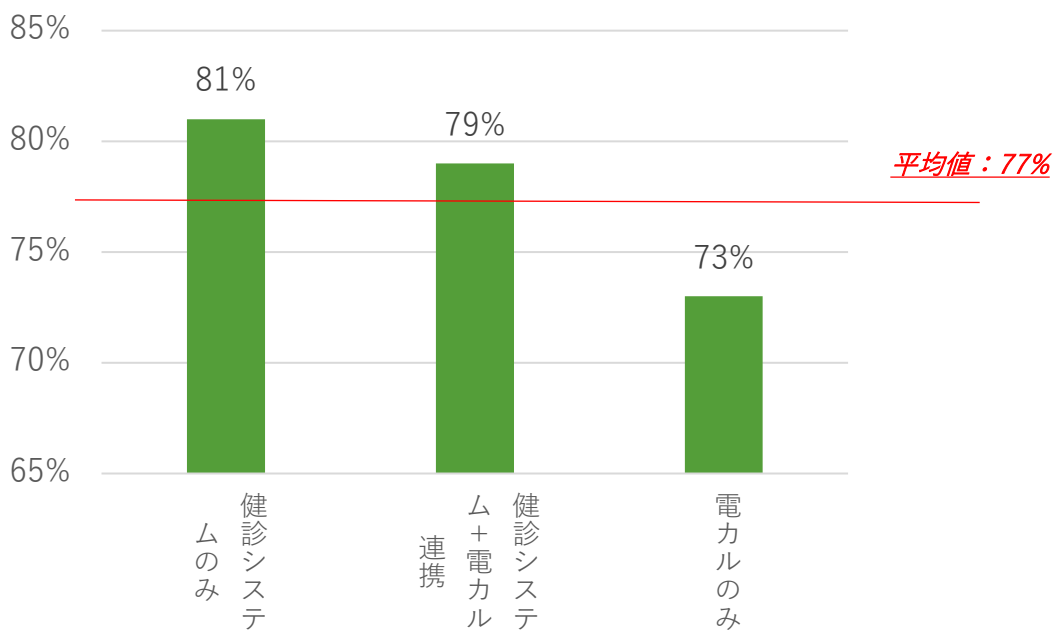


健診システムのみ利用組織は2000万以上のセキュリティ予算の確保率が1割以上に及ぶ一方、**関連施設等の電カルを利用する施設になると予算が少なくなる状況である**。また、健診システムの利用組織はセキュリティ予算は十分と回答する割合が相対的に多い一方、**電カル利用型の組織ではその割合が低下**していく傾向がある。

＜アンケート調査結果_ IT利用環境別(6/7)＞

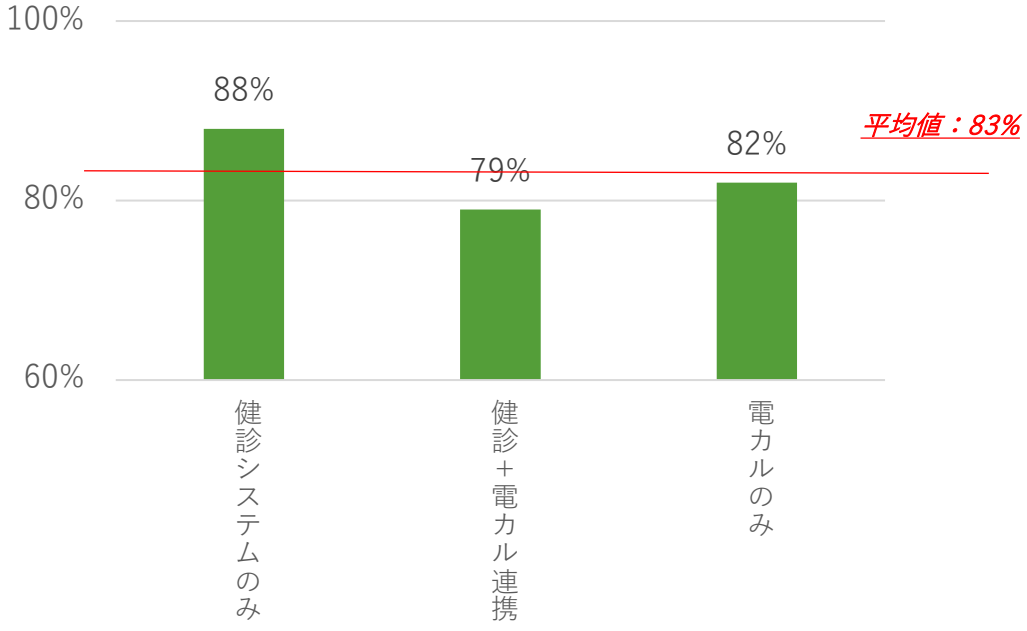
【サイバー保険】 ※N＝315

＜⑫：サイバー保険を「加入」以外(「わからない」含む）で回答した施設割合＞



【クローズドNWの安全性】 ※N＝315

＜⑬：診療系NWは安全という考え方に何らかのかたちで「共感」すると回答した施設割合＞

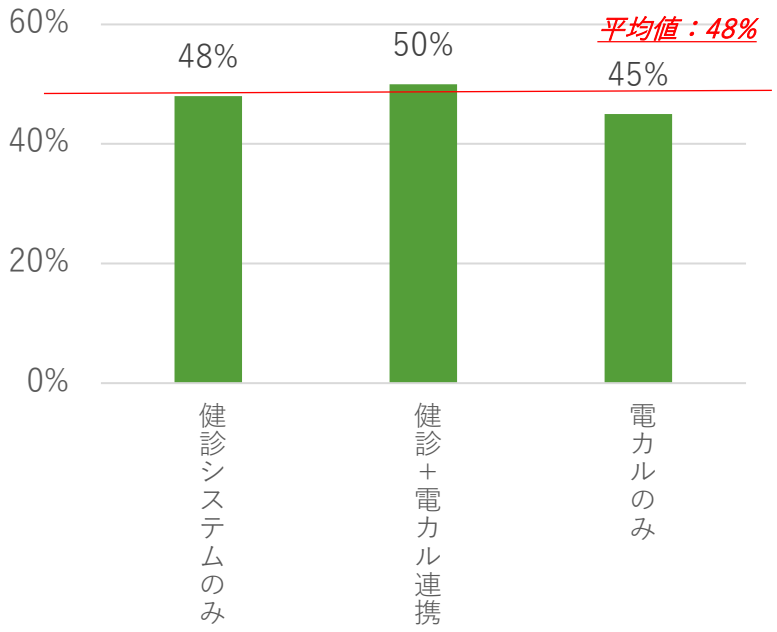


<u>サイバー保険の未加入率は、健診システムのみ利用組織が高く、電カルのみ利用組織が低い</u>状況である。
これに反比例するように、**<u>診療系NWの安全神話＝外部接続リスクへの鈍感度は健診システムのみ利用組織は高いが、電カルのみ利用組織は相対的に低い</u>**状況である。

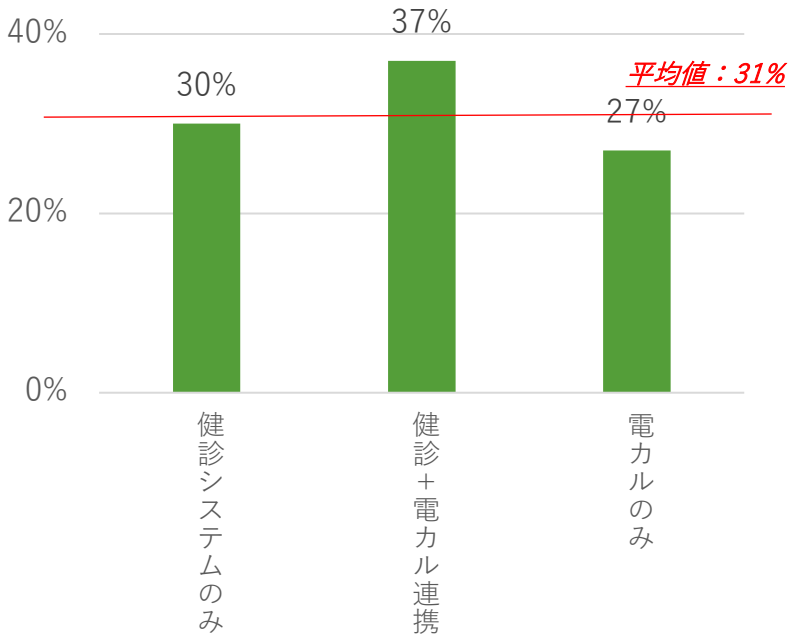
＜アンケート調査結果_ IT利用環境別(7/7)＞

【システム提供事業者とのコミュニケーション状況】 ※N＝315

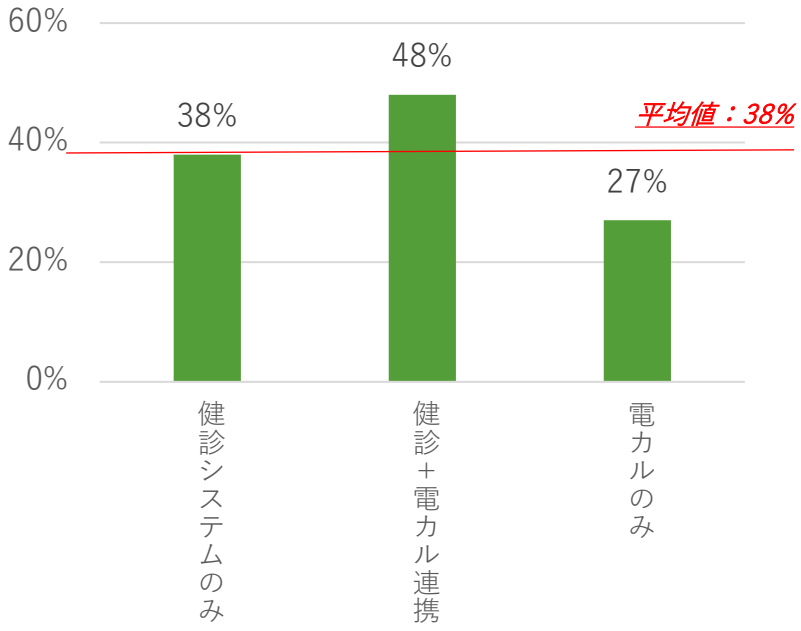
＜⑭：IT事業者によるセキュリティ対策の「指示を受けている」と回答した施設割合＞



＜⑮：IT事業者とのセキュリティ契約を「締結している」と回答した施設割合＞



＜⑯：IT事業者のセキュリティ対応を「信頼」していると回答した施設割合＞



健診システム＋電カル連携施設がIT事業者によるユーザセキュリティ指示率/IT事業者との契約締結率が最も高く、かつ、IT事業者への信頼率も高い状況である。一方、**電カルのみ利用施設はそれらの割合が最も低く、IT事業者との契約締結率とともに、信頼率も低い傾向**が示されている。


Medical Information Sharing and Analysis Center