全国老人保健施設協会
セキュリティアンケート調査結果

公益社団法人全国老人保健施設協会/
一般社団法人医療ISAC

2023年3月

＜目次＞

１．調査概要

調査目的

介護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、医療/介護併設型施設の提供事業者、施設型介護サービスの提供事業者においてランサムウェアの被害も見受けられています。

国内の介護領域は未だIT化が十分に浸透していない面もありますが、すでにITを導入している介護事業者を主な対象として、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。

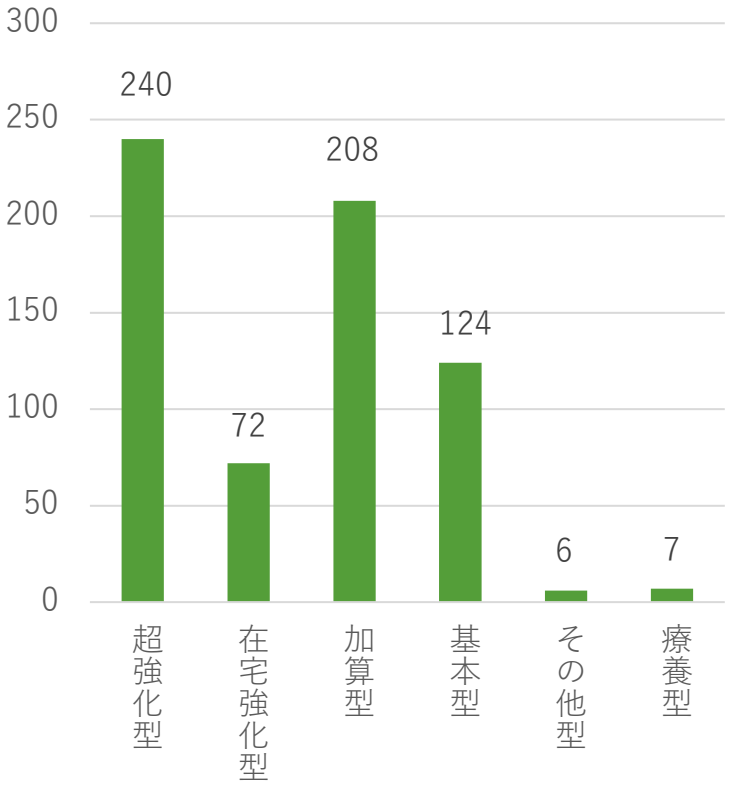
そのため、電子的な介護情報管理システム（ケアプランシステム）、及び当該システムと連携する電子カルテシステムを利用状況および、そのセキュリティに関する調査にご協力をお願い申し上げます。

本調査は全国老人保健施設協会と医療ISACの共同事業となります。

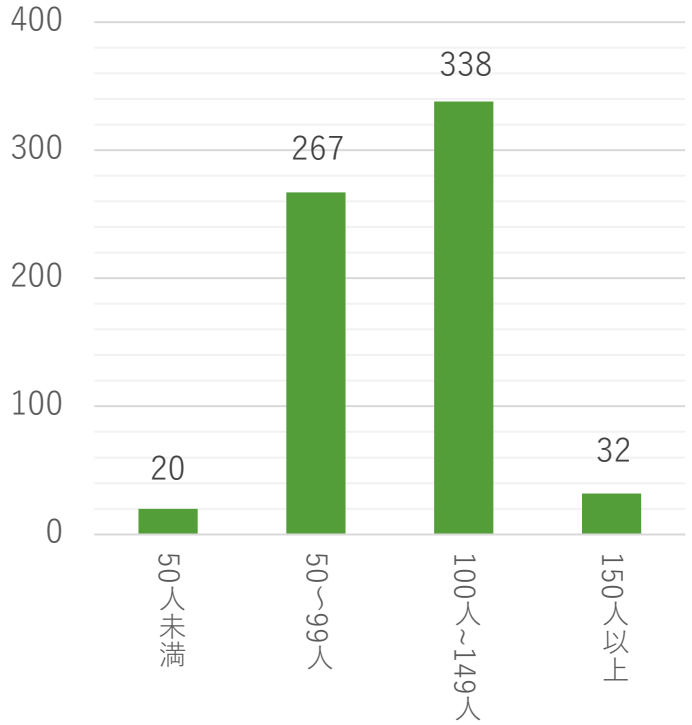
調査対象

- 実施期間：2023年1月12日～2月2日
- 全体組織数：3570件(23年1月時点)
- 回答組織合計数：788件（回答率：22%)
- 調査対象数：657件（ITシステム未利用の施設/131件は調査対象外）
- 調査組織：全国老人保健施設協会/ 医療ISAC

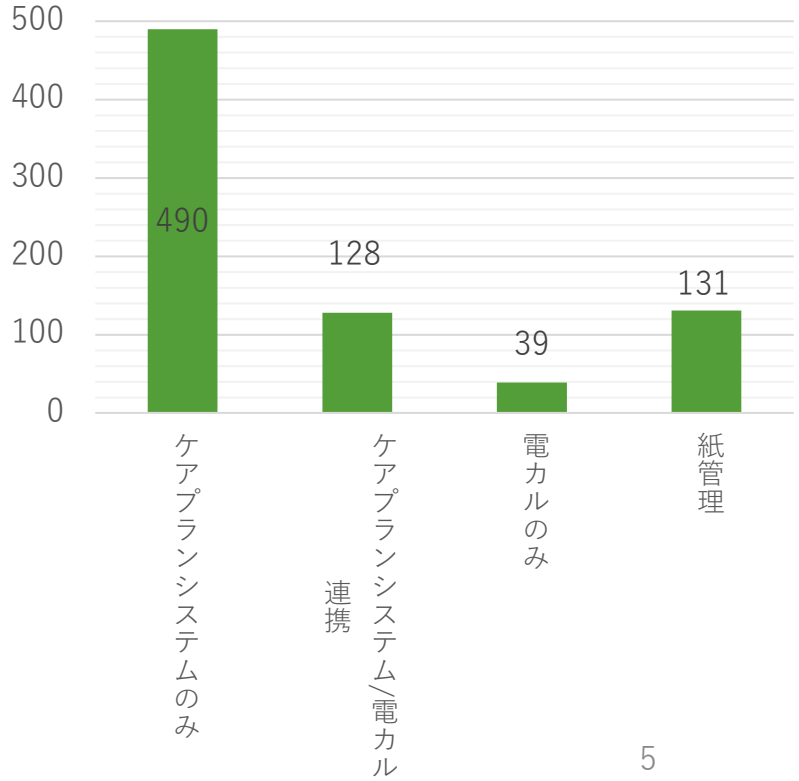
＜施設類型別内訳＞ ※令和４年11月末に算定した施設類型



＜入居定員規模別内訳＞



＜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？	□ ケアプランシステムのみを利用している □ ケアプランシステムに加え、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？	□全老健の団体保険「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 □全老健の団体保険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、介護基幹系システム（ケアプランシステム/電子カルテシステム等）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：IT事業者との契約のなかに、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（介護施設支援）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るか？	□している　□していない　□わからない
	⑯：介護基幹系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うか？	□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＞

- 今回の調査対象施設のうち、6割以上はサイバーリスクへの脅威を感じている一方で、**半数以上は年間セキュリティ予算は500万未満であり、セキュリティ予算が十分と回答した割合は1割弱**である。介護系システムを利用している施設においてもサイバー脅威の高まりを把握しているものの、**介護報酬という公定価格のもとでセキュリティ予算が計画的かつ十分に確保できない現状が医療分野における同種のアンケート結果同様、示されている**。

- 厚労省等から脆弱性を通知されたForitGate社VPN機器を利用している施設において該当機器への脆弱性対応は概ね行われているものの、IT人材は全施設平均で1名弱であり、ほぼ常勤者となっている。そうした人材のうち、介護系システムにおけるセキュリティの基本を定めた厚労省安全管理GLの認識率は半数以下であり、セキュリティ監査は8割以上の施設で一度も実施されていない状況である。**＜外部の目線＞の介入、または公知のセキュリティガイドラインへの理解度も低い状況下では、自発的なセキュリティPDCAサイクルを運用することは事実上、困難な状況であることも医療分野と同様**と言える。

- バックアップについては、オンラインのみでなく、ランサムウェア被害への対策としてのオフライン、あるいはクラウド上での保管が多くの施設で行われている点が医療分野との大きな違いである。**医療機関と比較した場合、ケアプランシステムを中心とする基幹系システムの少なさ（非分散性）がこうした取組率の高さに寄与している**と考えられる。

- サイバー保険の加入率は全体で2割程度であり、かつ、外部との接点を持たないクローズドネットワークの「安全神話」への共感率は7割強と高い。**保険加入率の低さはセキュリティ予算の確保困難さ**（ひいては介護報酬の構造的な安価さ）も原因と考えられるが、逆にいえば**「安全神話」への共感率の高さも、サイバー攻撃を想定した保険加入率の低さにつながっている**ともいえる。

- IT事業者とのセキュリティ契約を明示的に行っている施設は1割弱である一方、経産省・総務省安全管理GLに基づくユーザセキュリティの指示を受けている施設は2割強存在し、**医療分野と比較すると、介護IT事業者が介護施設に寄り添う姿勢の高さを相対的に示している**。そのため、介護IT事業者のセキュリティ対応を信頼する施設も3割程度存在するが、契約がない状況下で行われるセキュリティコミュニケーションはあくまで「善意による施し」でしかない。**契約の中で確実にセキュリティ上の役割・責任を求めなければ、いつ「手のひら返し」が発生するかは分からないため、確実なセキュリティ面の契約により、介護IT事業者と同等の立場でセキュリティについての協議・対応を行う必要がある。**

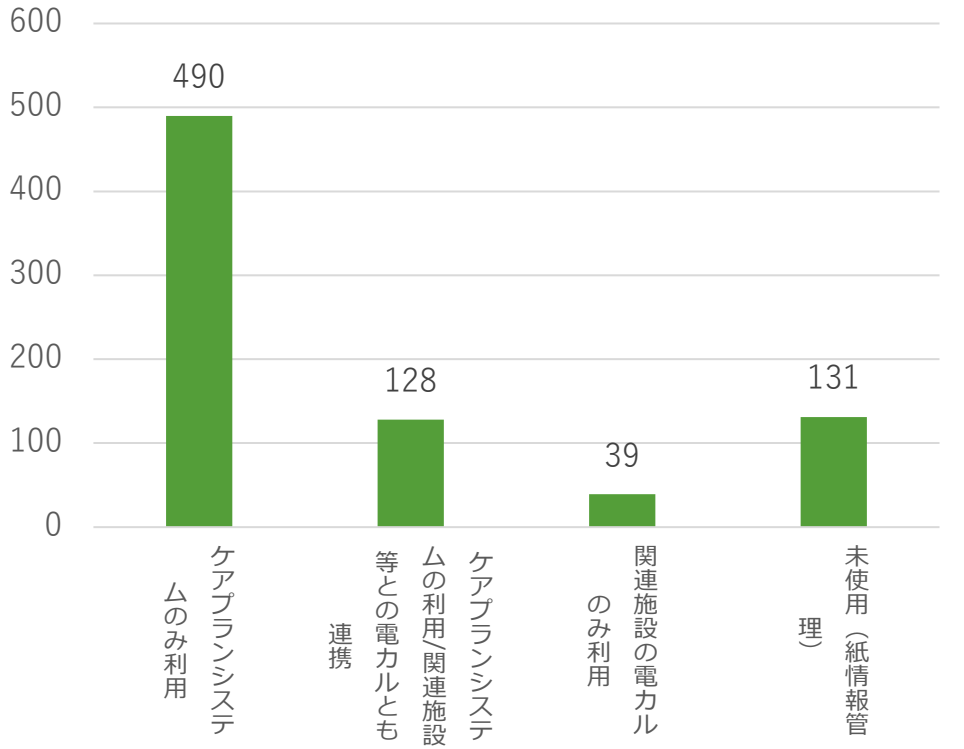
- なお、IT事業者とのコミュニケーション状況に係る調査項目のうち、**「わからない」の回答率が全体的に高い**傾向にあった。これは**介護系システムを利用する施設としてどのようなセキュリティ対策を事業者に求め、かつ、自らも行うべきかについて十分理解できていない状況に起因する**とも考えられる。介護系システムのセキュリティは厚労省安全管理GLに基づき担保されることが求められていることからも、システム担当者も含め、介護施設におけるユーザセキュリティ意識の向上（教育）にまずは着手することが必要である。

＜アンケート調査結果_全体結果(1/8)＞

【IT利用の形態】

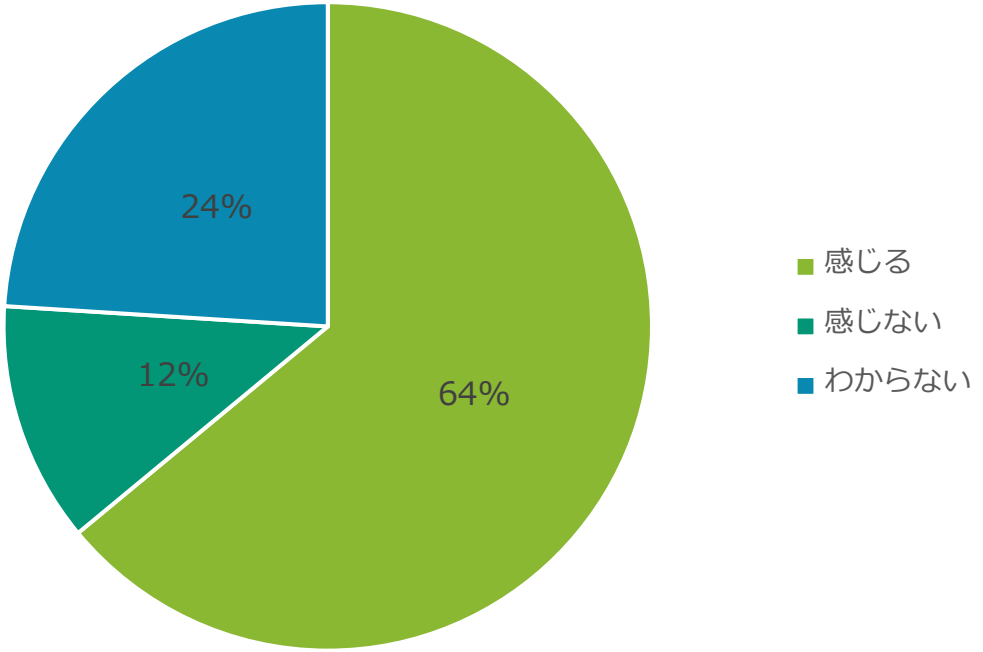
＜①：ITの利用形態は？＞　※N＝788

※：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＝657

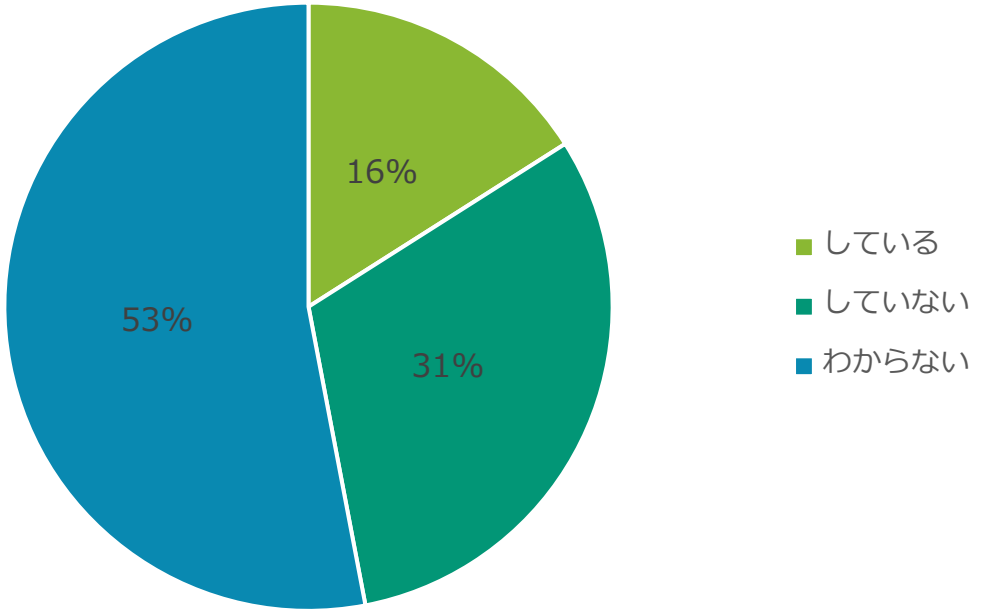


ITシステムを利用している介護施設の**6割以上がサイバー攻撃への脅威を感じている**

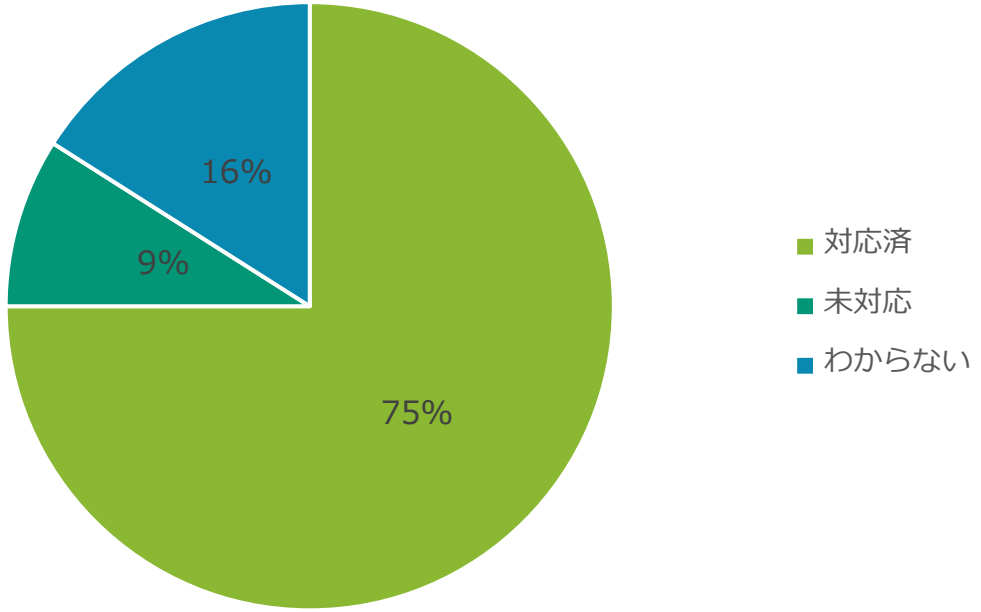
＜アンケート調査結果_全体結果(2/8)＞

【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＝657



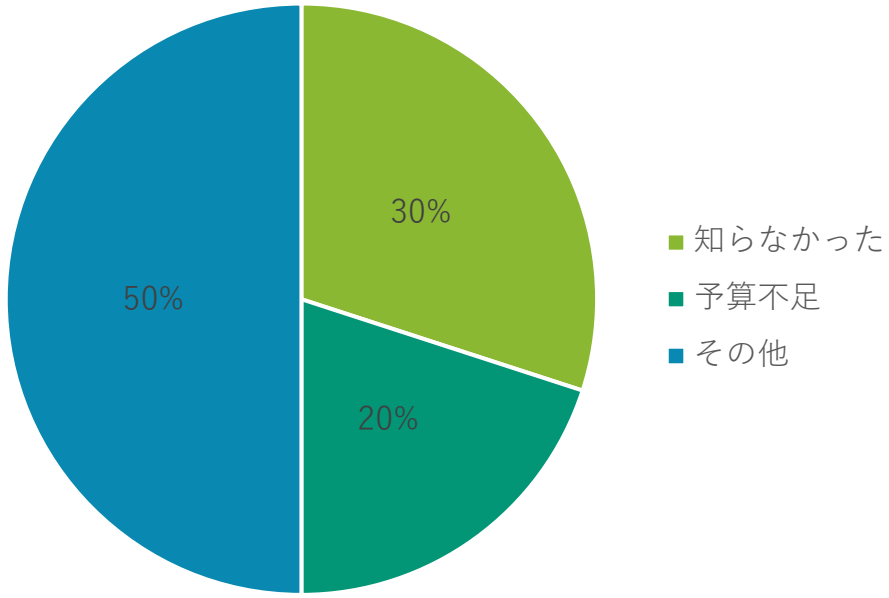
＜④：③が「使用している」の場合、脆弱性対応は完了しているか？＞　※N＝108



厚労省等から脆弱性が通知されたForitnet社製VPN機器の利用組織は全体の2割以下であり、
そのうち4分の３は脆弱性対応が完了している一方で、**4分の１は未対応あるいは状況把握ができておらず、**
セキュリティリスクが放置されている。

＜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＝10



【その他】の概要

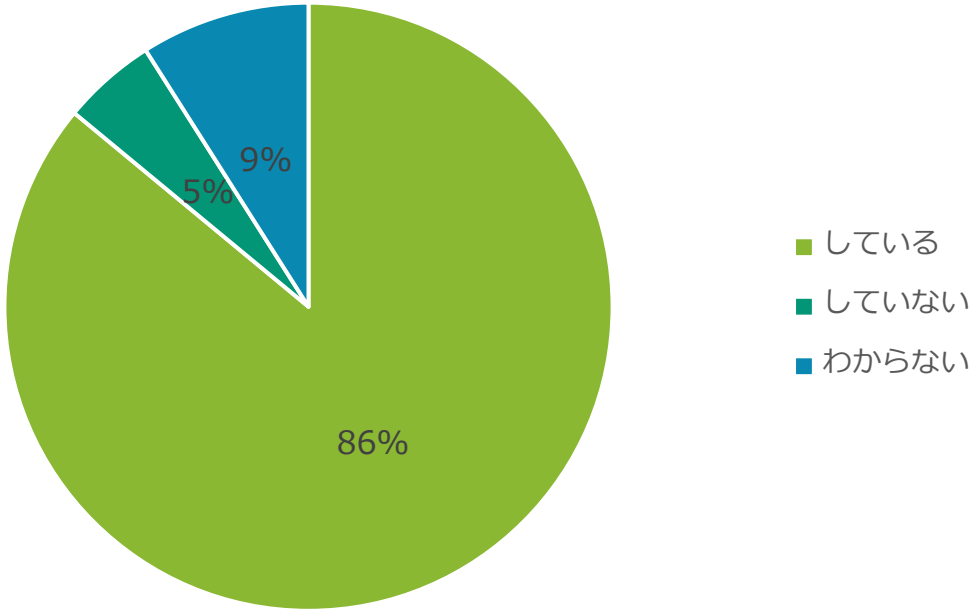
■院外と接続せず、院内ネットワークでしか利用していない機器のため、対策不要と判断
■外部ベンダが設置しており、設定不明
■外部連携先が設置・利用しており、自施設では把握してない
等・・・

情報を把握していない/予算不足が半数程度を占め、
さらには**院内ネットワークで利用しているため対策不要と判断する施設が一定数存在**している

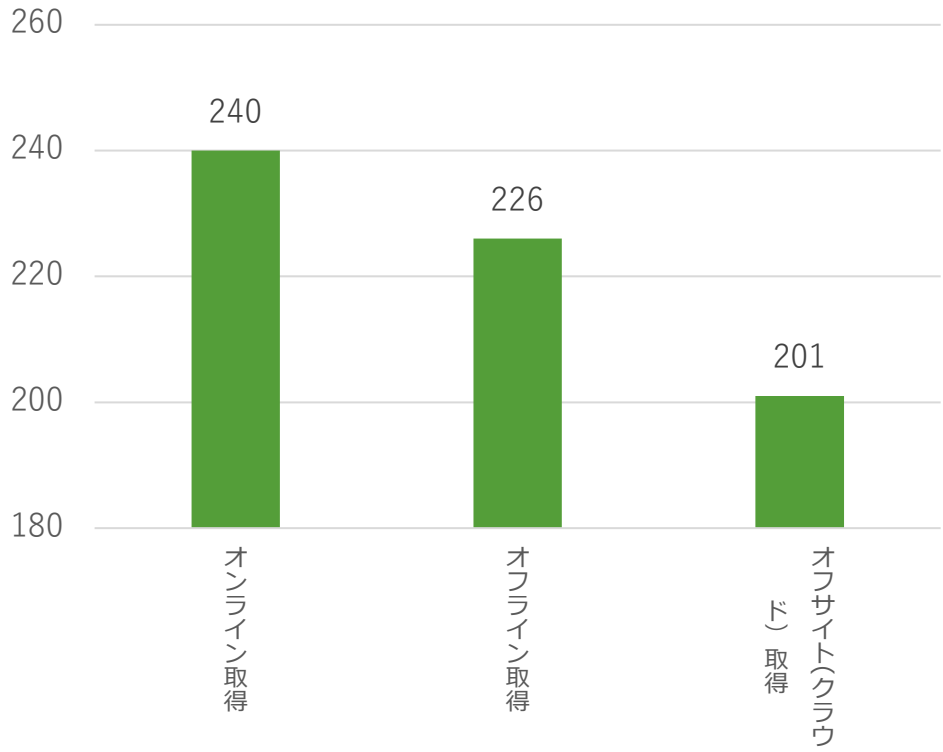
＜アンケート調査結果_全体結果(4/8)＞

【バックアップ対策】

＜⑥-1：バックアップの取得率＞　※N＝657



＜⑥-2：バックアップの取得方式(複数選択式）＞　※N＝563



ケアプランシステム等、介護系システムのバックアップの取得率は9割弱であり、オンライン取得のみでなく、
オフライン取得/オフサイト（クラウド）取得方式の採用率も高い

＜アンケート調査結果_全体結果(5/8)＞

【IT人材】

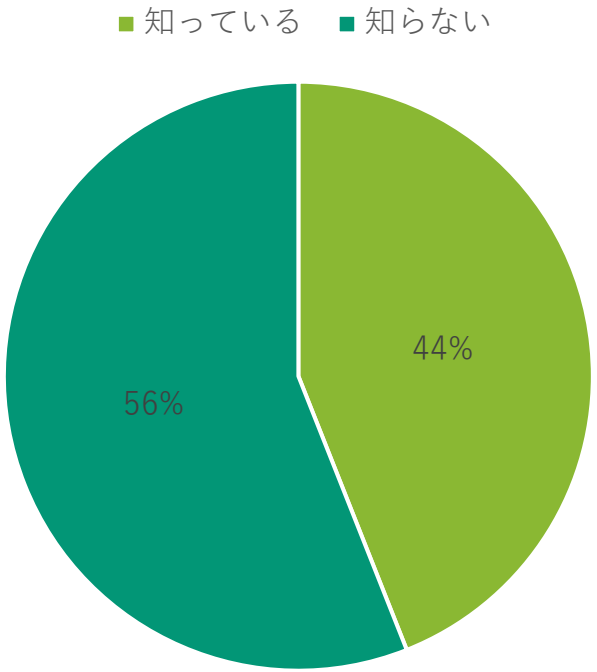
＜⑦：IT人材数＞　※N＝657

種別	平均人数
施設内システム担当者	1.6人
うち、常勤数	1.5人

【監査】

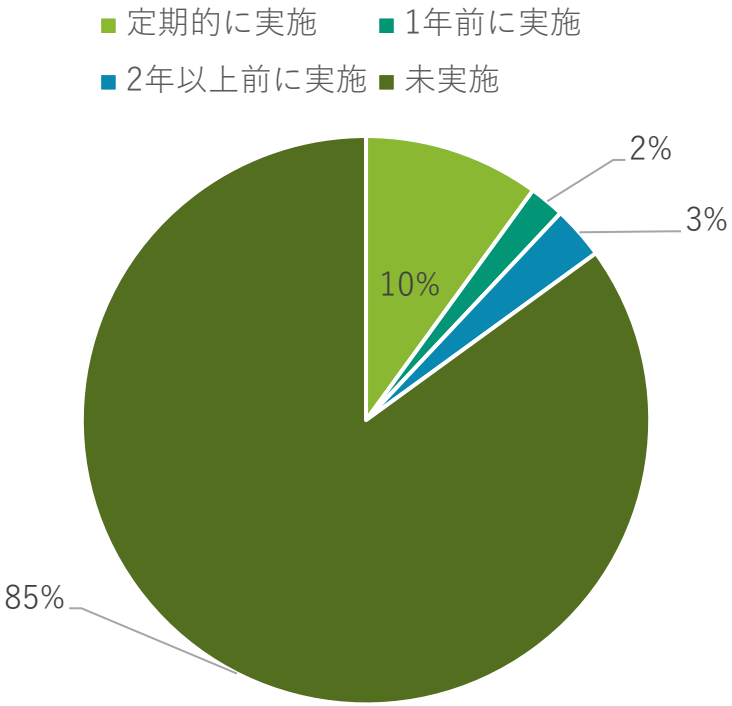
＜⑧：厚労省安全管理GLの認識状況＞

※N＝657



＜⑨：セキュリティ監査の実施状況＞

※N＝657

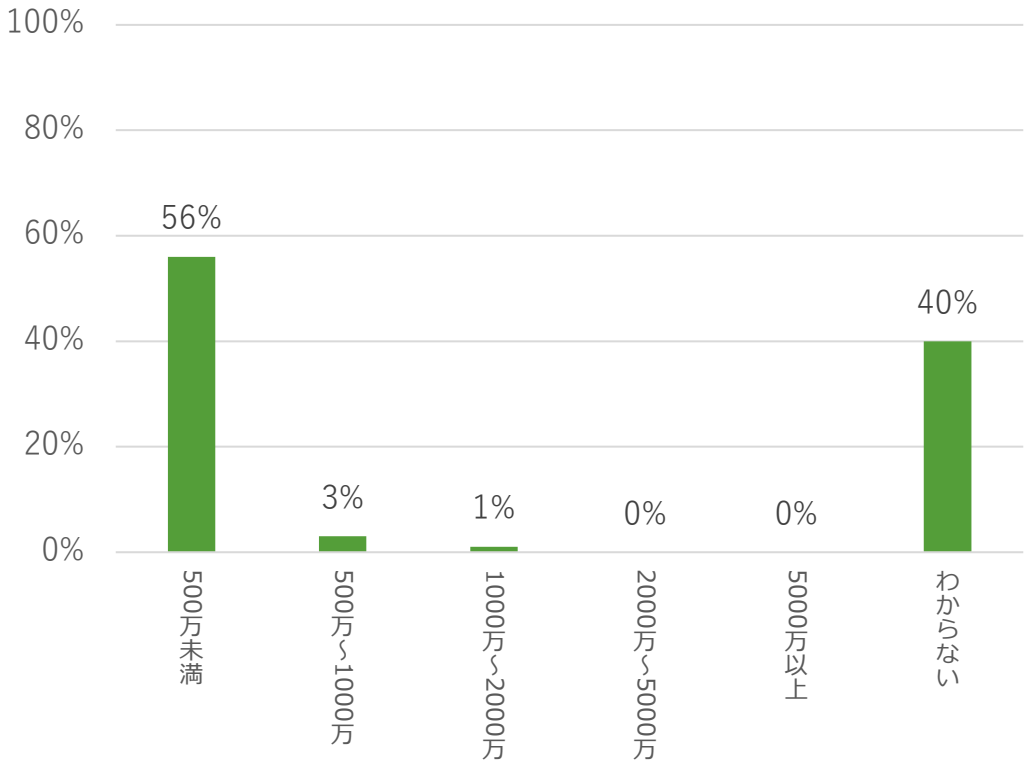


介護施設のシステム担当者はほぼ常勤である。
ただし、**厚労省安全管理GLの内容を半数以上が知らず**、**セキュリティ監査も8割以上が今まで実施したことがない**状況である。

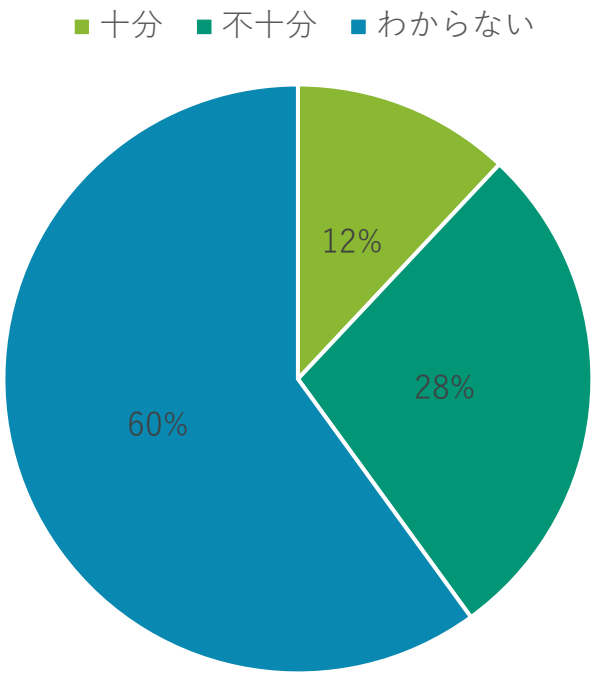
＜アンケート調査結果_全体結果(6/8)＞

【セキュリティ予算】

＜⑩：年間のセキュリティ予算＞　※N＝657



＜⑪：セキュリティ予算の十分性＞　※N＝657

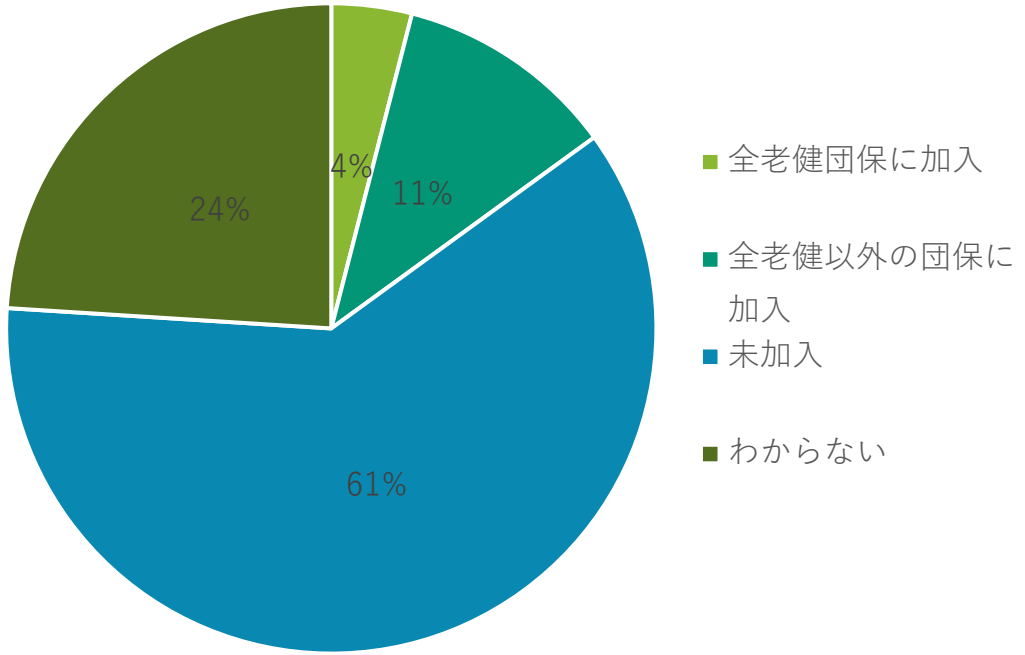


介護施設の年間セキュリティ予算は500万未満が半数以上を占め、**500万以上は全体の数パーセント**にとどまる。
セキュリティ予算が十分との回答は1割程度で、セキュリティ予算不足が業界的に特に深刻と言える。

＜アンケート調査結果_全体結果(7/8)＞

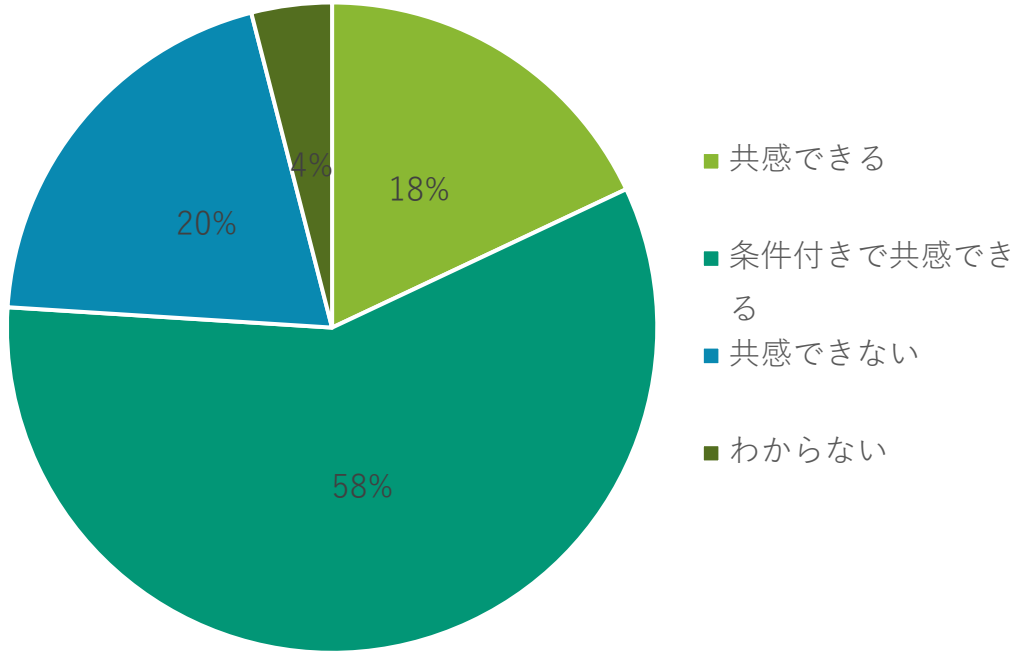
【サイバー保険】

＜⑫：サイバー保険の加入状況＞　※N＝657



【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＝657

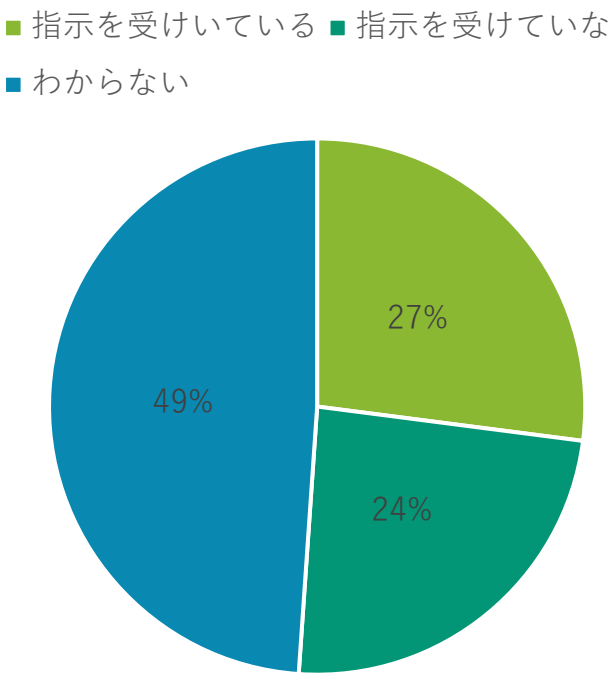


サイバー保険の加入率は**全体で2割以下**であり、
また、診療系NWは安全という考え方には**7割以上が何らかの形で共感できる**との回答である。

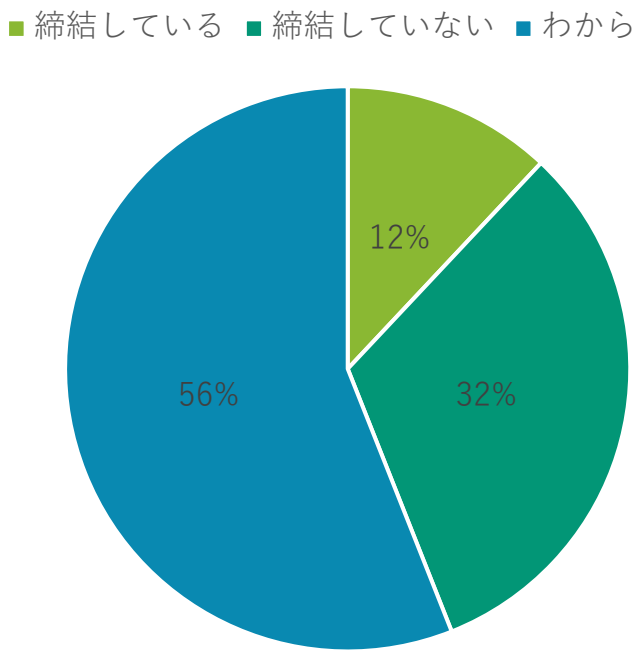
＜アンケート調査結果_全体結果(8/8)＞

【システム提供事業者とのコミュニケーション状況】 ※N＝657

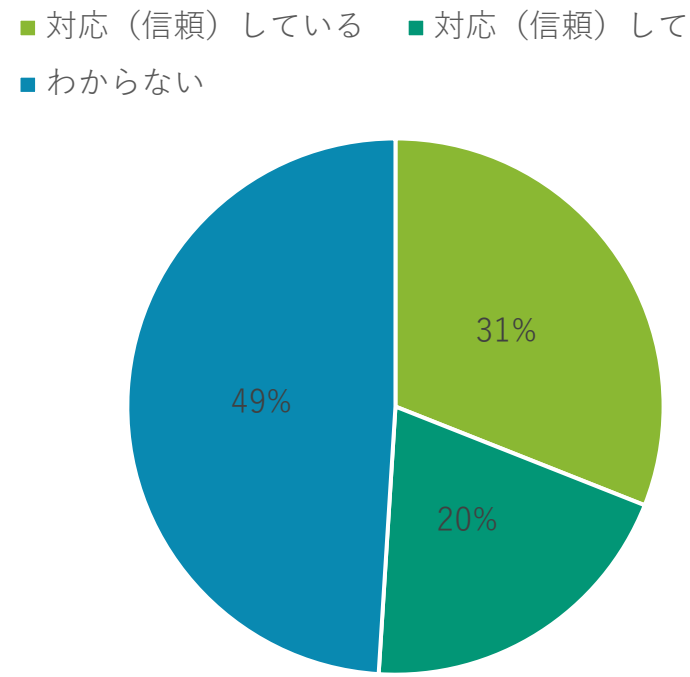
＜⑭：IT事業者によるセキュリティ対策指示状況＞



＜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）＞



IT事業者からユーザセキュリティ対策の指示を受けている施設は3割弱だが、**セキュリティ締結を明示的に行っている施設は1割弱**である。一方でIT事業者はセキュリティ対応を行ってくれていると信頼している施設数は3割を超えており、**IT事業者への盲目的な依存度が高い**と言える。なお、全体的に「分からない」の回答率が高く、**施設としてどのようなセキュリティをIT事業者に求めるべきかが把握できていない状況**も浮き彫りになっている。

３．入居者定員別結果

＜アンケート調査結果総評_入居者定員別＞

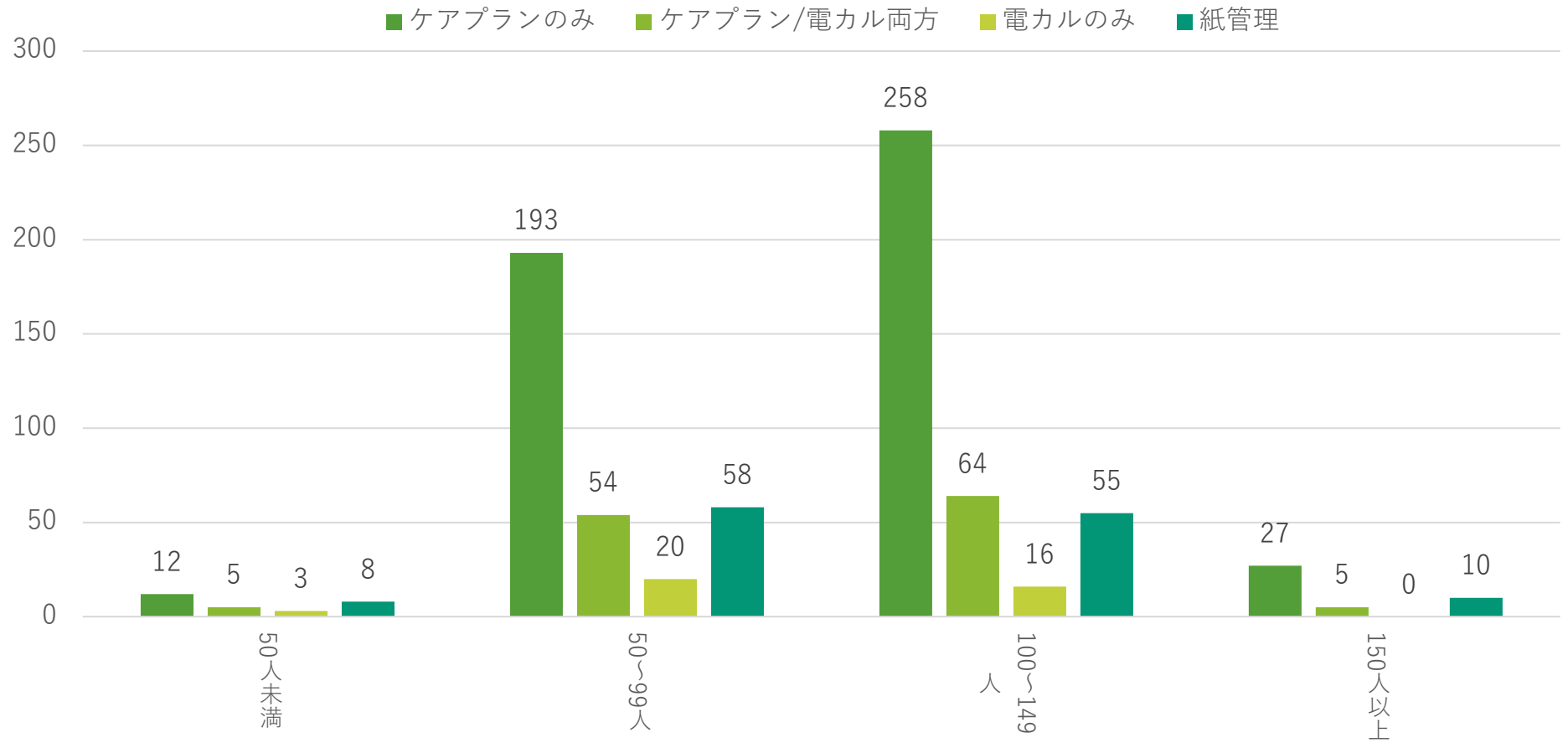
- 入居者定員（規模）別で見ると、**定員規模が高い施設ほどサイバー脅威への感度が高い**傾向が示されているが、。
- Fortinet社製品の利用率は今回の調査結果では50～99人/100～149人区分の施設での使用率が相対的に高く、**施設平均で7割弱は脆弱性対応を実施している**状況であった。しかしながら、全体としてはどの規模の施設においても、**利用機器の種別が分からないという回答率が最も高く**、仮に脆弱性に該当する機器が利用されていた場合、その潜在的なセキュリティリスクは大きいと考えられる。
- バックアップの取得率は規模が大きいほど高く、**どの規模の施設においてもオフライン/オフサイトの取組率が高い**ことが特徴的である。
- IT人材数は（一部変則的な結果も含まれるが）基本的には規模の大きさに比して増大する傾向にあると考えられる。ただし、**厚労省安全管理GLの認識率、セキュリティ監査の実施率は共通的に低く**、強いていえば150人以上の施設でGLの認識率が5割に至っているが、あくまで多少の偏差でしかない。
- 今回の調査結果では、年間セキュリティ予算が500万未満あるいは「わからない」と回答し、かつ、セキュリティ予算が十分でないと回答した規模区分は50～99人/100～149人層が該当している。ただし、これも相対的な差でしかなく、**いずれの規模の施設においても全体平均としてはセキュリティ予算は少なく、かつ、十分でないと認識**していると言える
- 何らかのサイバー保険に加入しているとの回答率が最も高かった規模区分は150人以上である。ただし、いずれの規模区分の施設においても**8割弱は診療系ネットワークは外部との接点を持たないため安全と考える境界防御的なセキュリティ思想から脱し切れていない**状況が示されている。
- 規模が大きいほどＩＴ事業者からのセキュリティ指示受領率が高くなる傾向があるが、**明示的にセキュリティ面の契約を取り交わしている施設割合は全体平均で1割弱程度にしか満たない**。特に、セキュリティコミュニケーション/契約率の低い、**50人未満の小規模施設ではＩＴ事業者への信頼度が高く、盲目的な依存率が相対的に強い傾向**があると言える。

＜アンケート調査結果_入居者定員別(1/8)＞

【ITの利用形態】

＜①：ITの利用形態＞　※N＝788

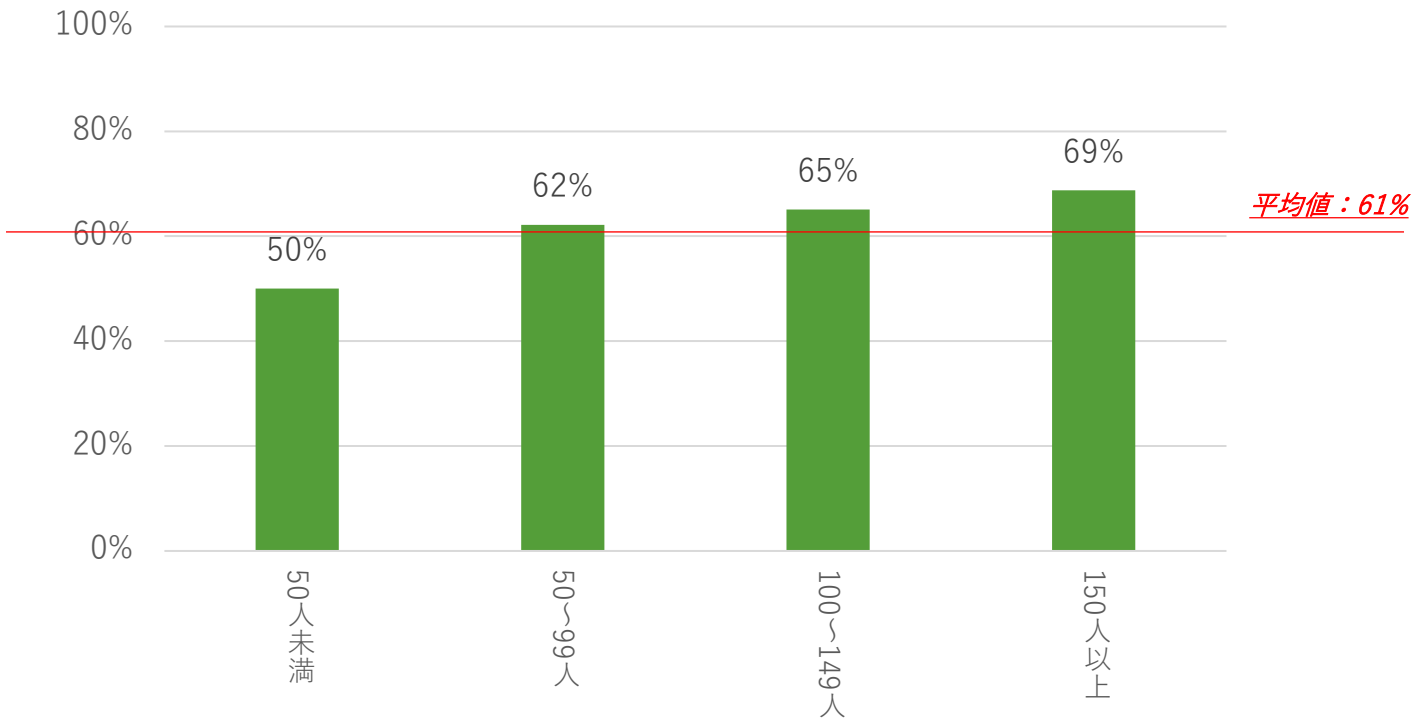
※：以降の調査は紙管理施設は対象外



＜アンケート調査結果_入居者定員別(2/8)＞

【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＝657



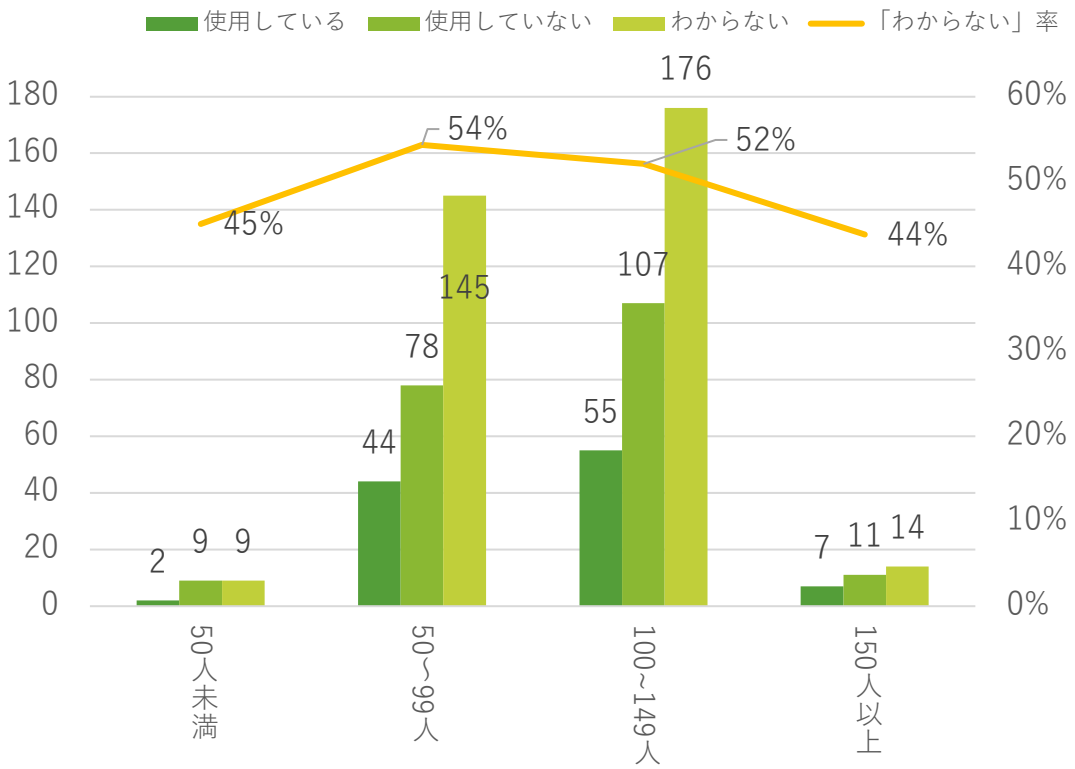
施設規模が大きいほど、サイバー攻撃への脅威を感じる傾向が示されている。

＜アンケート調査結果_入居者定員別(3/8)＞

【脆弱性対策】

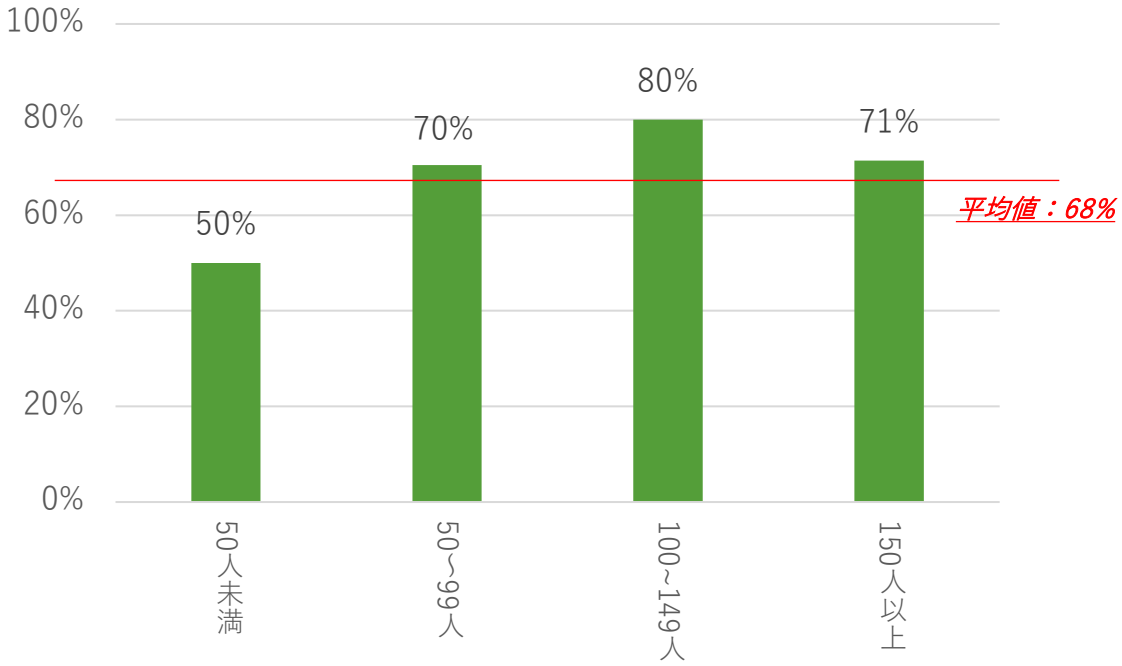
<③：厚労省等から脆弱性が指摘されたForitnet社製VPN機器を使用している施設割合>

※N＝657



<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＝108

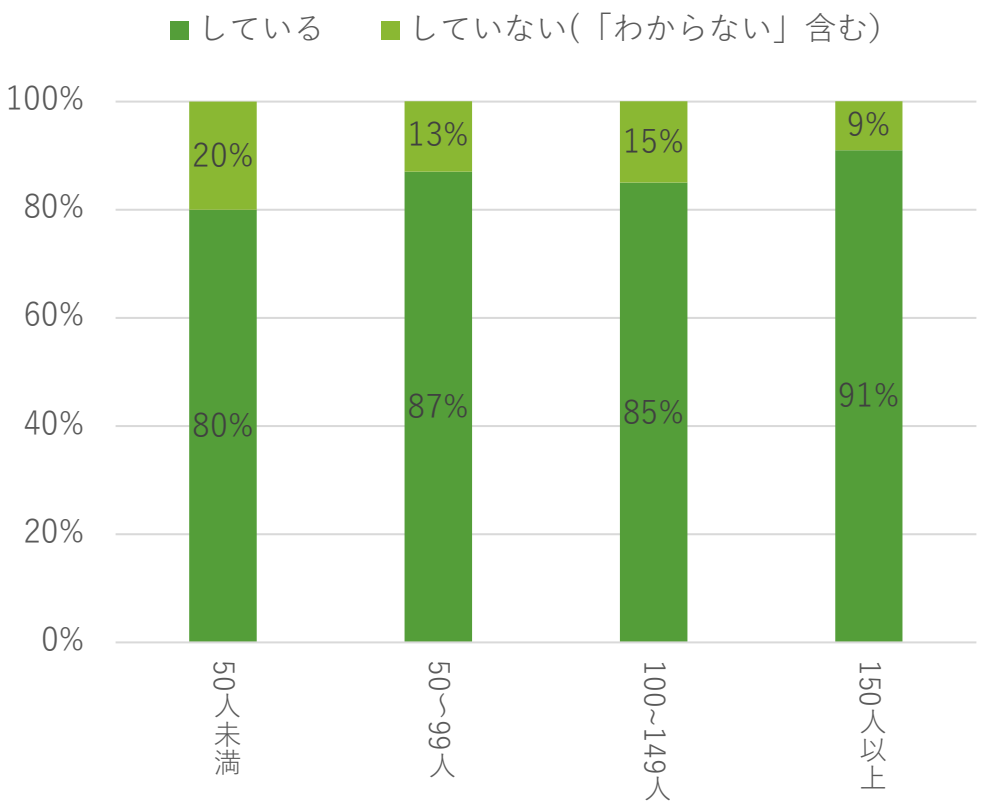


入居者定員規模が大きい施設ほどVPN機器の脆弱性対応率が高い。特に50～99人/100～149人の層は
VPN機器の利用状況自体を把握していない施設件数も増大している。

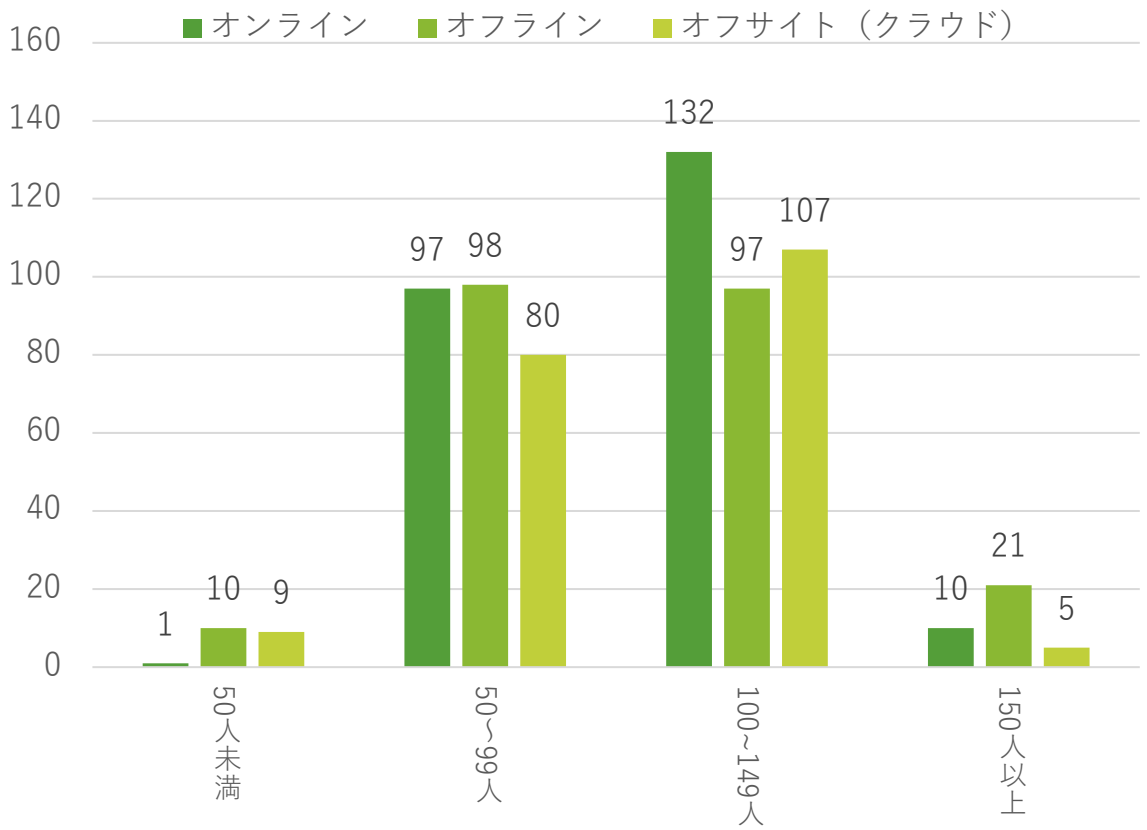
＜アンケート調査結果_入居者定員別(4/8)＞

【バックアップ対策】

＜⑥-1：バックアップの取得率＞ ※N＝657



＜⑥-2：バックアップの取得方式(複数選択式）＞ ※N＝563



バックアップ取得率も定員規模が大きいほど高い。
なお、**全施設共通で、オンライン以外のバックアップ取得方式の採用率が高い**。

＜アンケート調査結果_入居者定員別(5/8)＞

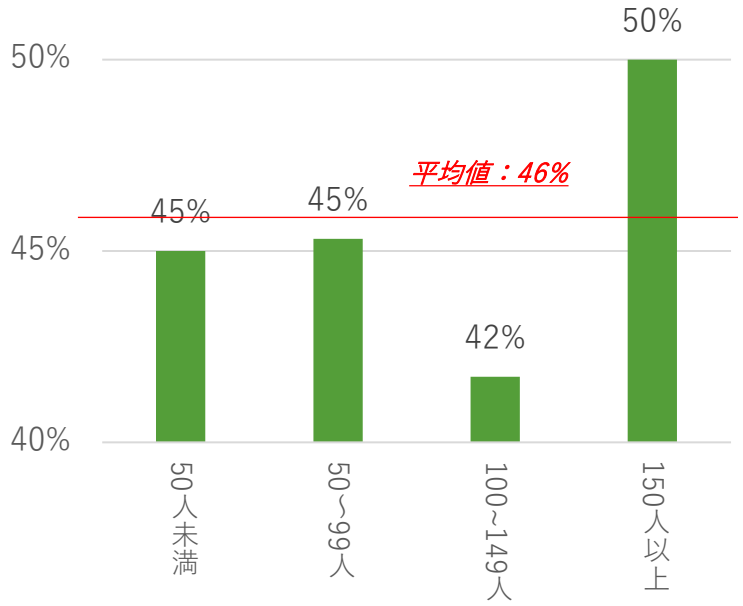
【IT人材】 ※N＝657

＜⑦：IT人材数＞

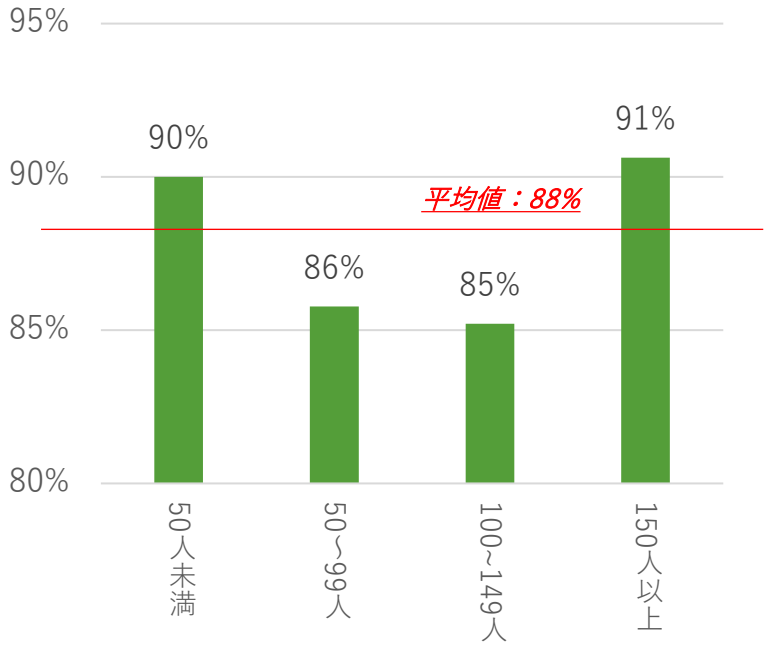
入居者定員区分	施設内システム担当者	うち、常勤数
50人未満	1.1人	1.0人
50～99人	2.1人	1.9人
100~149人	2.1人	2.1人
150人以上	1.1人	1.0人

【監査】 ※N＝657

＜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＞

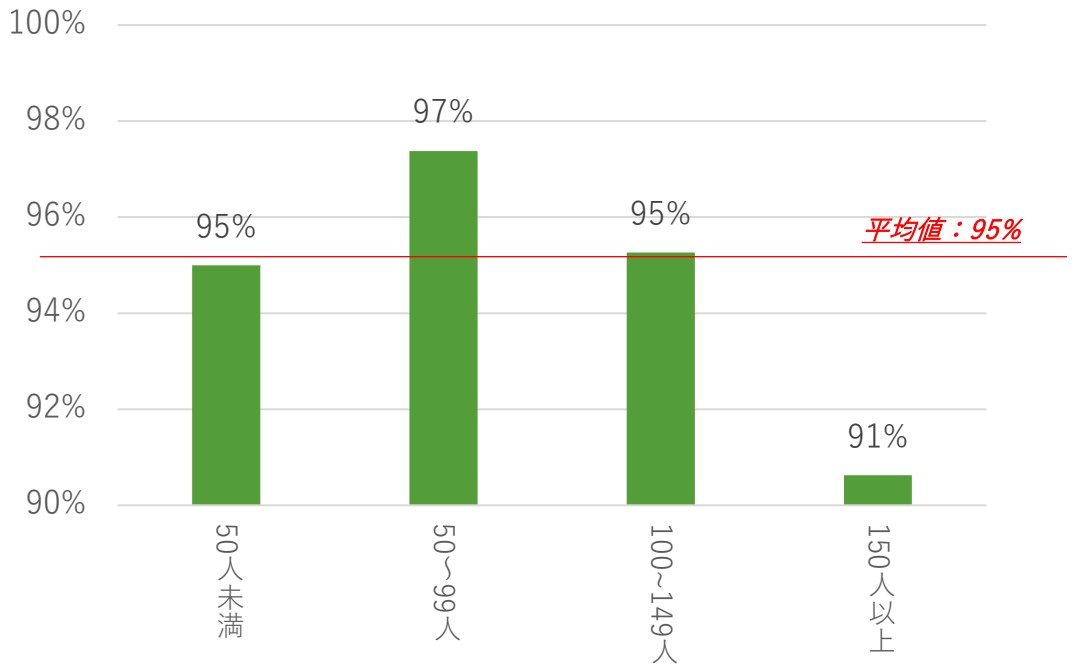


IT人材は多くても2名程度で、介護系システムが準拠すべき厚労省安全管理GLを知らない割合も平均5割弱に及ぶ。
セキュリティ監査も今まで一度も実施されていない施設は平均9割弱の範囲に収まっており、
監査面では、定員規模による大きなセキュリティ水準の差異はない。

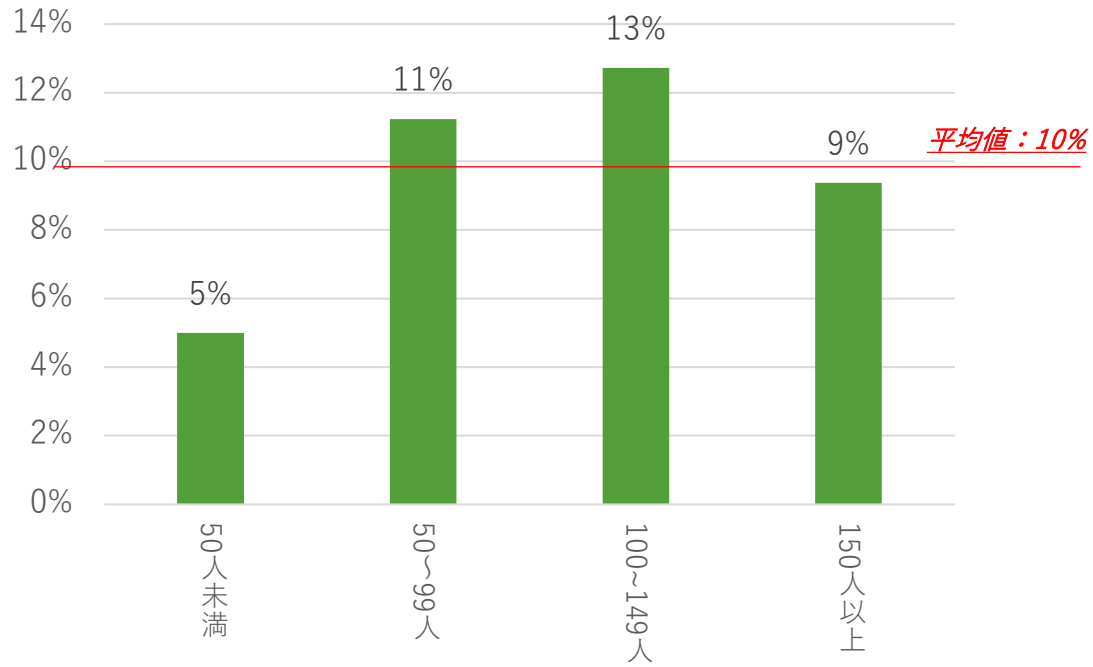
＜アンケート調査結果_入居者定員別(6/8)＞

【セキュリティ予算】 ※N＝657

＜⑩：年間のセキュリティ予算のうち、「500万未満」及び「分からない」と回答した（「500万以上」以外で回答した）施設割合＞



＜⑪：セキュリティ予算が十分と回答した施設の割合＞

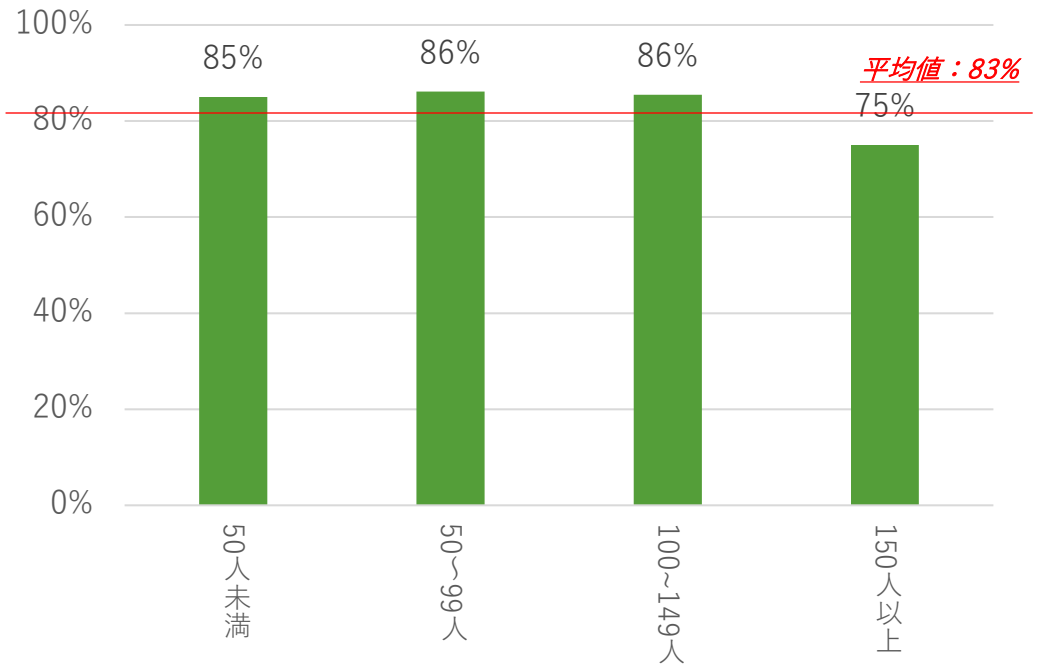


年間セキュリティ予算が500万未満（「分からない」を含む）は9割強と非常に高く、
セキュリティ予算が十分と回答した施設は定員規模別の全体平均で1割にしか満たない。

＜アンケート調査結果_入居者定員別(7/8)＞

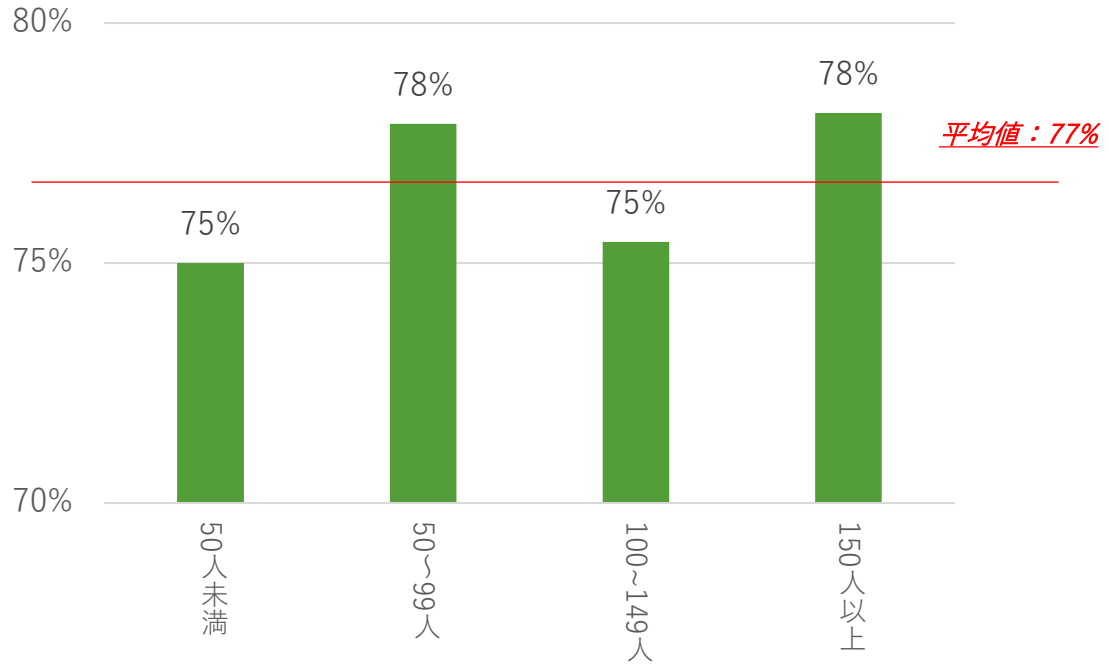
【サイバー保険】 ※N＝657

＜⑫：サイバー保険を「加入」以外で回答した（「未加入」/「わからない」と回答した）施設割合＞



【クローズドNWの安全性】 ※N＝657

＜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＞

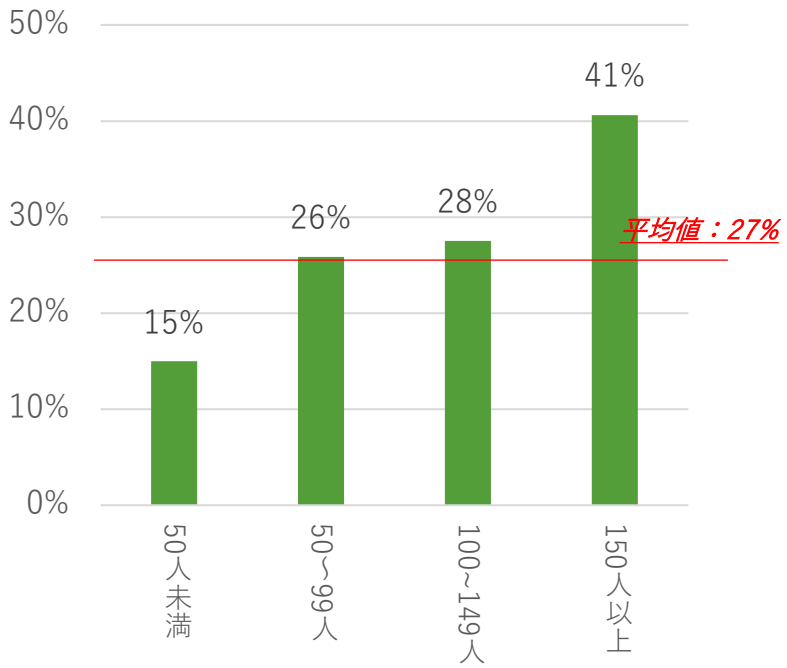


<u>150人以上の施設規模ではサイバー保険の加入率が相対的に高く</u>、
全体として診療ネットワークの安全神話への信頼率は8割弱と高い傾向にある。

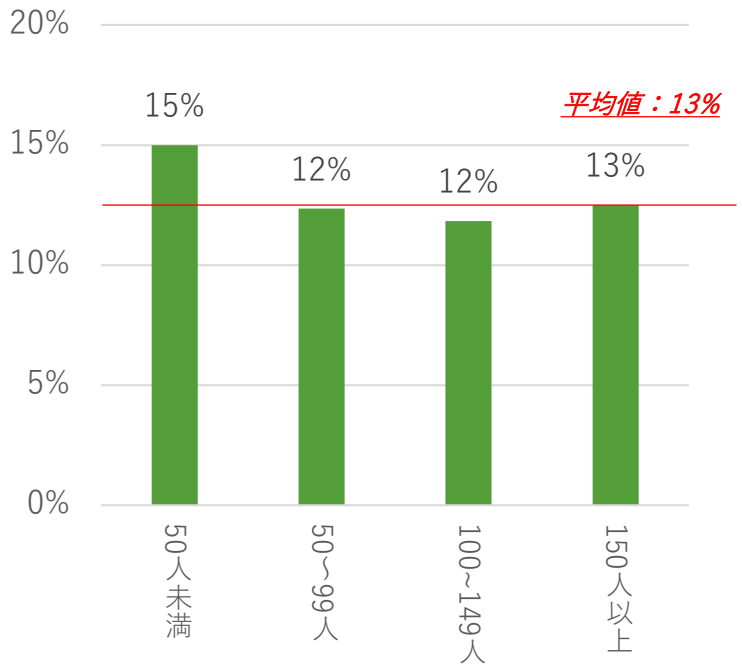
＜アンケート調査結果_入居者定員別(8/8)＞

【システム提供事業者とのコミュニケーション状況】 ※N＝657

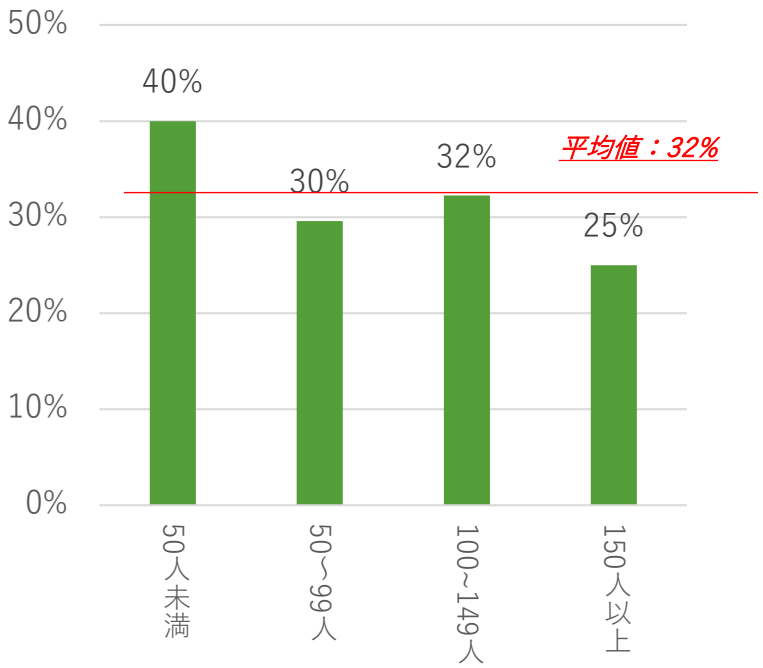
＜⑭：IT事業者によるセキュリティ対策の「指示を受けている」と回答した施設割合＞



＜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＞



施設規模が大きいほどＩＴ事業者からのセキュリティ指示受領率が高いが、**明示的にセキュリティ面の契約を取り交わしている施設割合は全体平均で1割弱程度にしか満たない。**特に、セキュリティコミュニケーション/契約率の低い、**50人未満の小規模施設ではＩＴ事業者への信頼度が高く、盲目的な依存率が相対的に強い傾向**があると言える。

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（令和４年11月末に算定した施設類型）別でみると、「超強化型」、「在宅強化型」等、**介護機能の充実度の高い施設（介護報酬率の高い施設）が相対的にサイバー攻撃への脅威を感じる割合が高い**傾向が示されている。

- 「超強化型」の施設でのVPN機器の使用率が高く、一部施設を除いて脆弱性対応はほぼ完了している。しかしながら、**どの施設類型でも平均的にVPN機器の使用状況が不明という回答率がもっとも高く、潜在的なセキュリティリスクが高い**状況と言える。

- どの施設類型でも**バックアップ取得率は8割以上**に達している。複数のバックアップ方式を採用している施設は少なく、オンライン/**オフライン/オフサイトでのバックアップ方式の採用率は概ね三等分**されている。

- どの施設類型でもIT人材は1～2名、ほぼ常勤であり、超強化型/加算型/基本型の施設類型では相対的に人員数が多い。厚労省安全管理GLの認識率は介護機能の充実度の高い施設（超強化型・在宅強化型等）が相対的に高いが、セキュリティ監査の実施率は全施設共通で低い状況である。

- **どの施設類型においても年間セキュリティ予算が500万未満（「分からない」を含む）が非常に高く**、**セキュリティ予算が十分と回答した施設は平均で1割以下**である。なお、「その他類型」「療養型」においては年間セキュリティ予算が500万以上、かつ、セキュリティ予算が十分と回答した施設は1件も存在しない状況であった。

- サイバー保険の加入率、及びクローズドNWの安全神話への非共感率は、「超強化型」・「在宅強化型」等、介護機能の充実性の高い施設類型群が相対的に上回っている状況であるが、全体平均でみればサイバー保険未加入率は9割弱、安全神話へ共感する割合も8割弱と、セキュリティ懸念は高い。

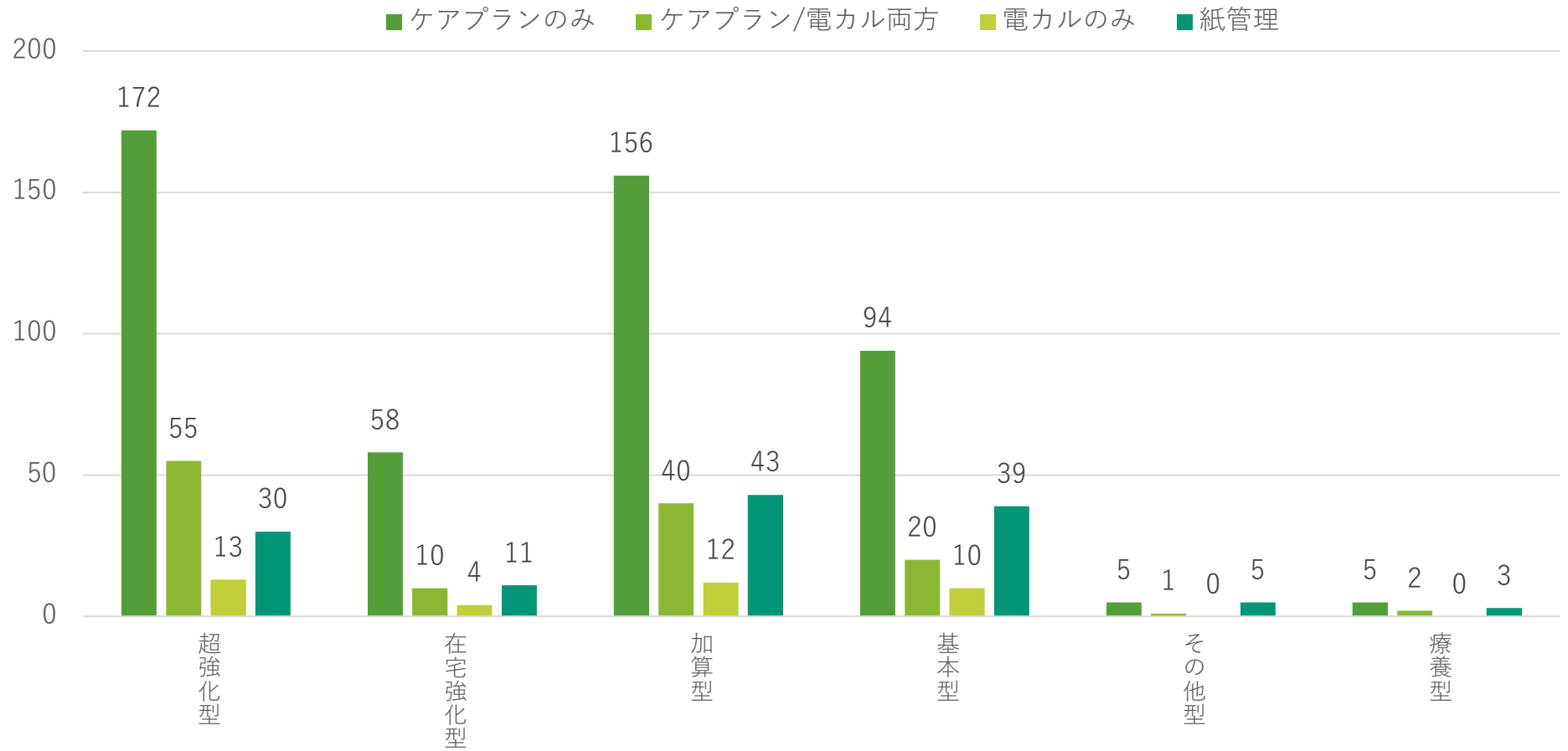
- 「超強化型」・「加算型」・「基本型」は介護IT事業者によるユーザセキュリティ指示率は相対的に高く、セキュリティ契約締結率も平均以上である一方、**事業者への信頼度は低く、セキュリティの自助意識が相対的に高い**と言える。一方、「その他型」はセキュリティ指示も受けず、契約締結していないものの、IT事業者への信頼度が高く、**事業者への盲目的な依存度が高い**。また、「療養型」は契約率/信頼率は同数だが、セキュリティ指示受領率は低く、**有効にIT事業者をセキュリティ面で活用できていない**と言える。

＜アンケート調査結果_施設類型別(1/8)＞

【ITの利用形態】

＜①：ITの利用形態＞　※N＝788

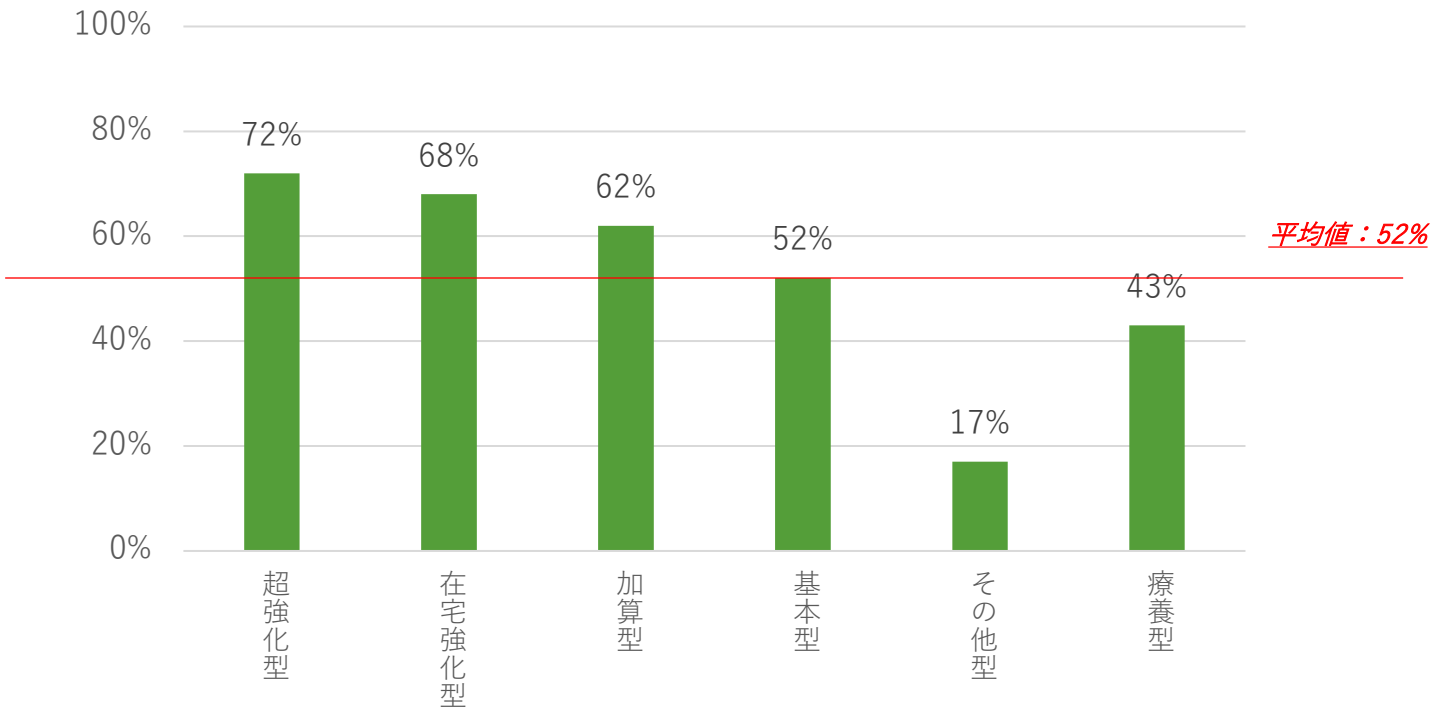
※：以降の調査は紙管理施設は対象外



＜アンケート調査結果_施設類型別(2/8)＞

【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＝657



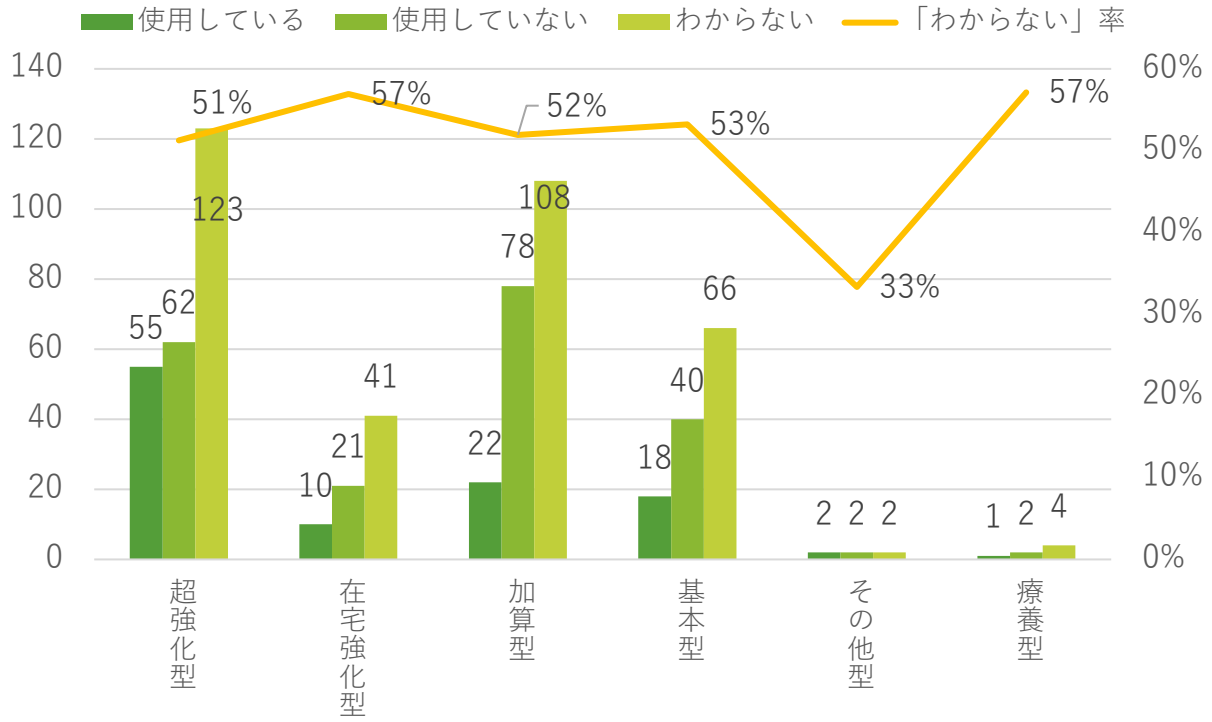
「療養型」「その他類型」は平均値より低いが、「超強化型」/「在宅強化型」等、**介護機能の充実度の高い施設が相対的にサイバー攻撃への脅威を感じる割合が高い**傾向が示されている。

＜アンケート調査結果_施設類型別(3/8)＞

【脆弱性対策】

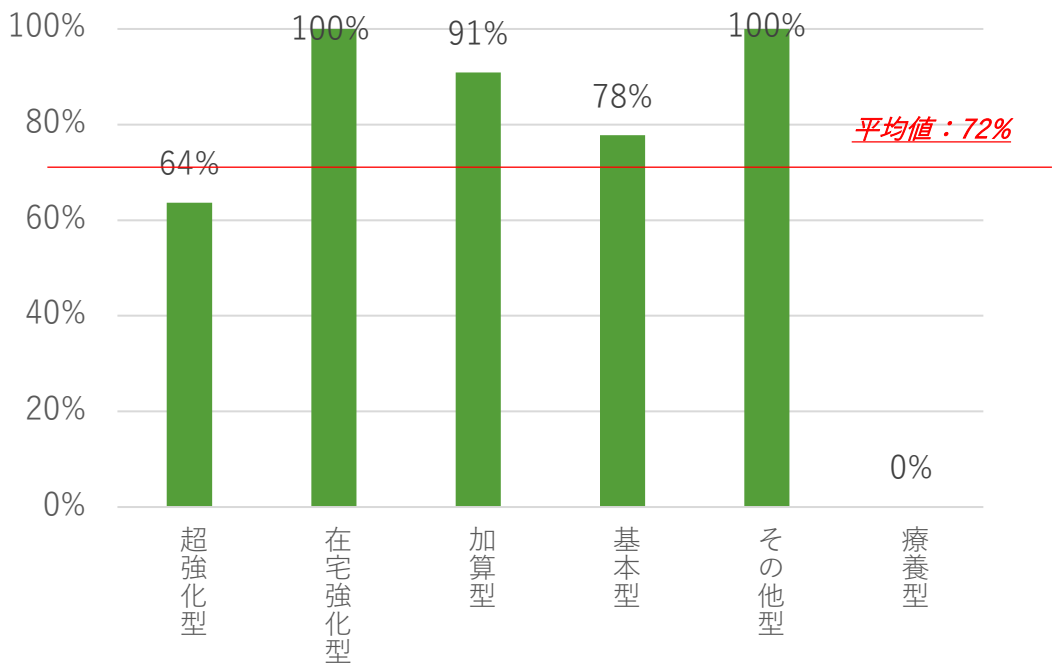
<③：厚労省等から脆弱性が指摘されたForitnet社製VPN機器を使用している施設割合>

※N＝657



<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＝108

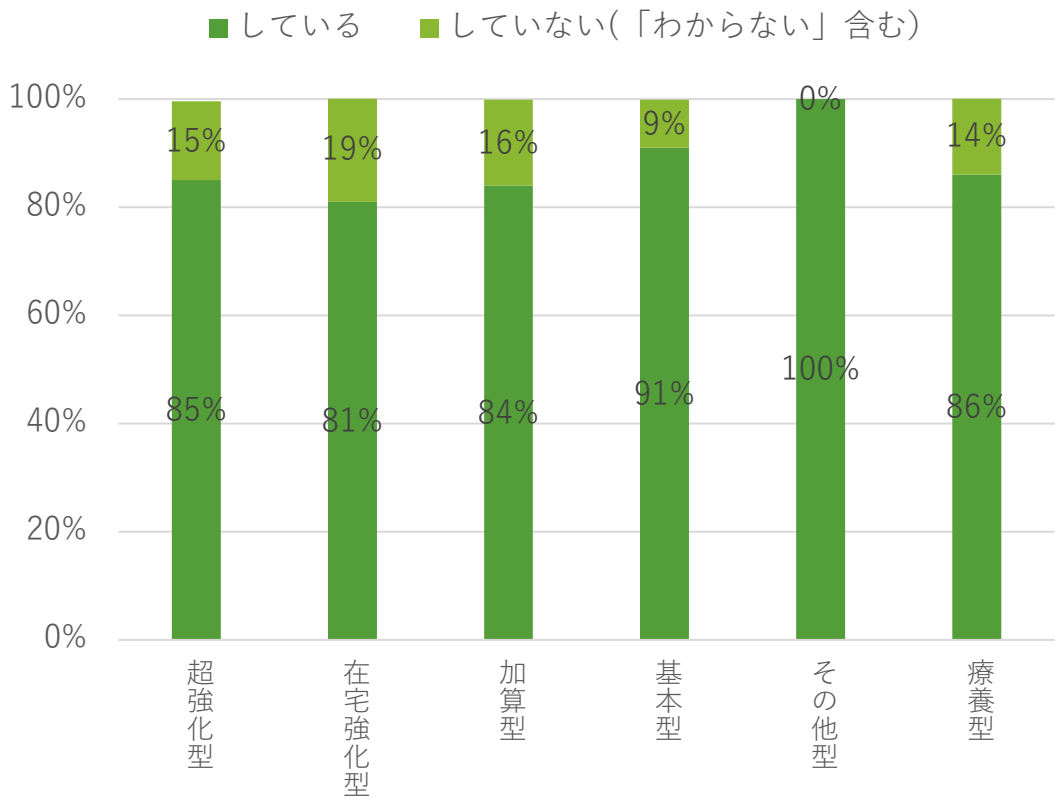


「超強化型」の施設でのVPN機器の使用率が高く、一部施設を除いて脆弱性対応はほぼ完了しているものの、
どの施設類型でも平均的にVPN機器の使用状況が不明という回答率がもっとも高く、
セキュリティリスクが潜在している施設が多い状況である。

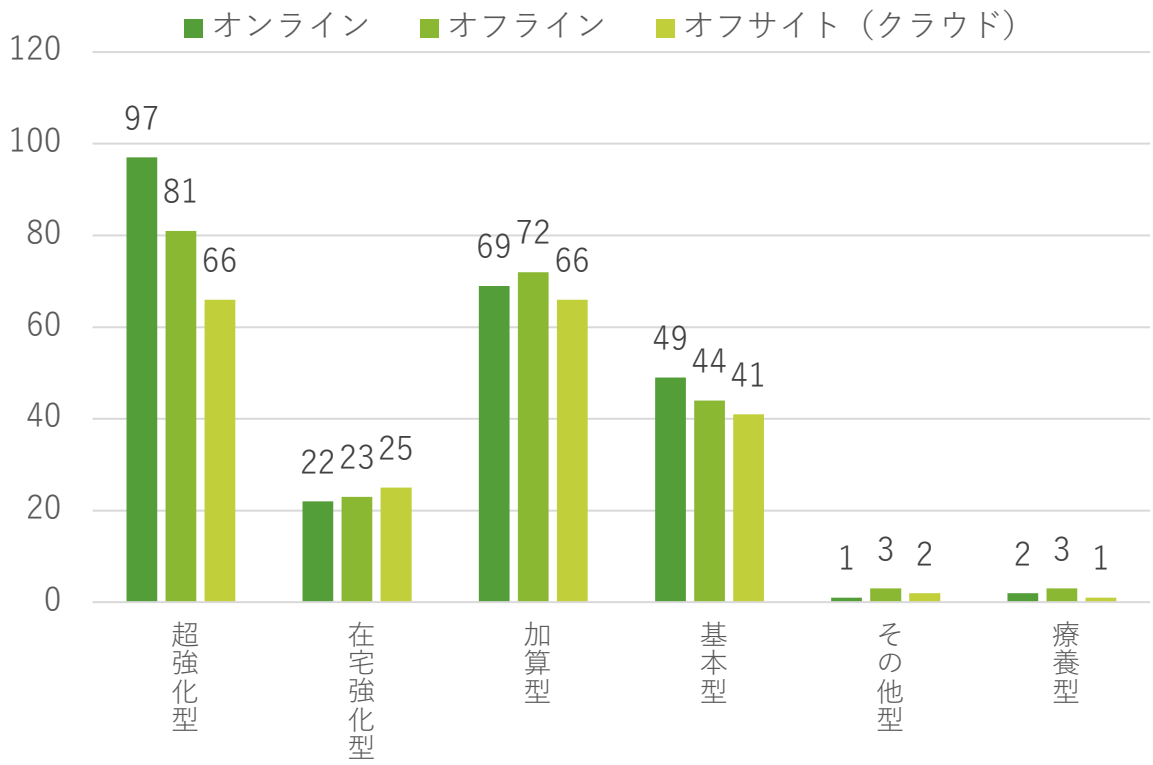
＜アンケート調査結果_施設類型別(4/8)＞

【バックアップ対策】

＜⑥-1：バックアップの取得率＞ ※N＝657



＜⑥-2：バックアップの取得方式(複数選択式）＞ ※N＝563



どの施設類型でも**バックアップ取得率は8割以上**に達している。複数のバックアップ方式を採用している施設は少なく、
3分の2程度がオフライン/オフサイトでのバックアップ方式を採用している。

＜アンケート調査結果_施設類型別(5/8)＞

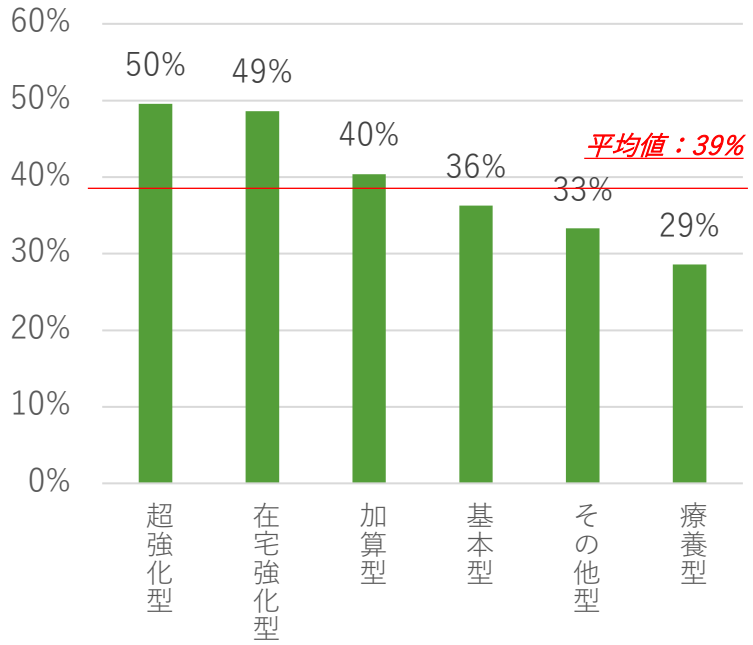
【IT人材】 ※N＝657

＜⑦：IT人材数＞

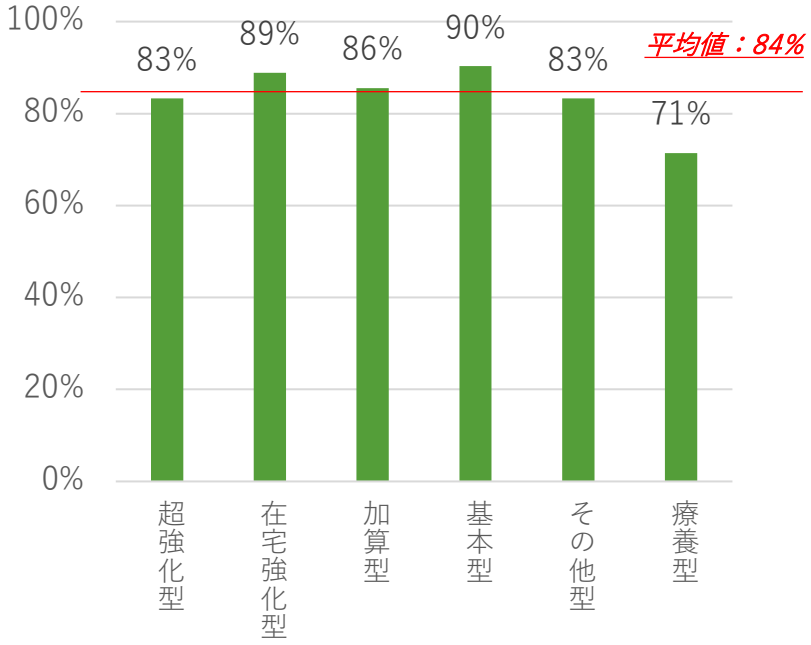
施設類型	施設内システム担当者	うち、常勤数
超強化型	2.4人	2.1人
在宅強化型	0.9人	0.8人
加算型	2.0人	2.0人
基本型	2.0人	1.8人
その他型	1.3人	1.2人
療養型	1.6人	1.6人

【監査】 ※N＝657

＜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＞

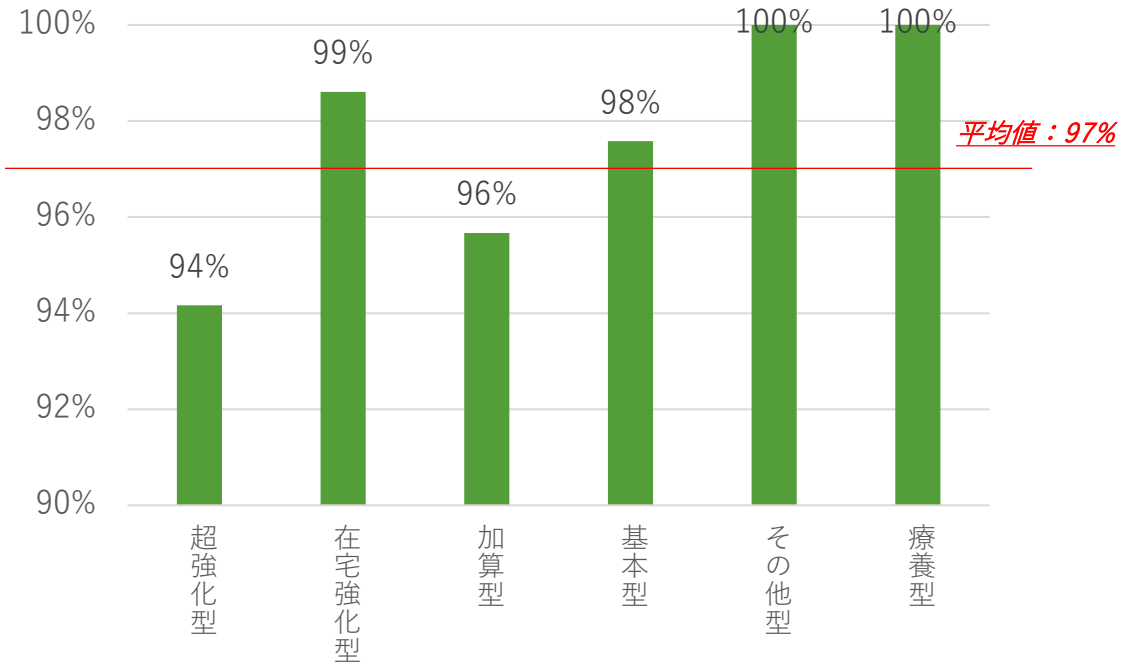


どの施設類型でもIT人材は1～2名、ほぼ常勤であり、**超強化型/加算型/基本型の施設類型では相対的に人員数が多い**。
厚労省安全管理GLの認識率は介護機能の充実度の高い施設（超強化型・在宅強化型等）が相対的に高いが、
セキュリティ監査の実施率は全施設共通で低い状況である。

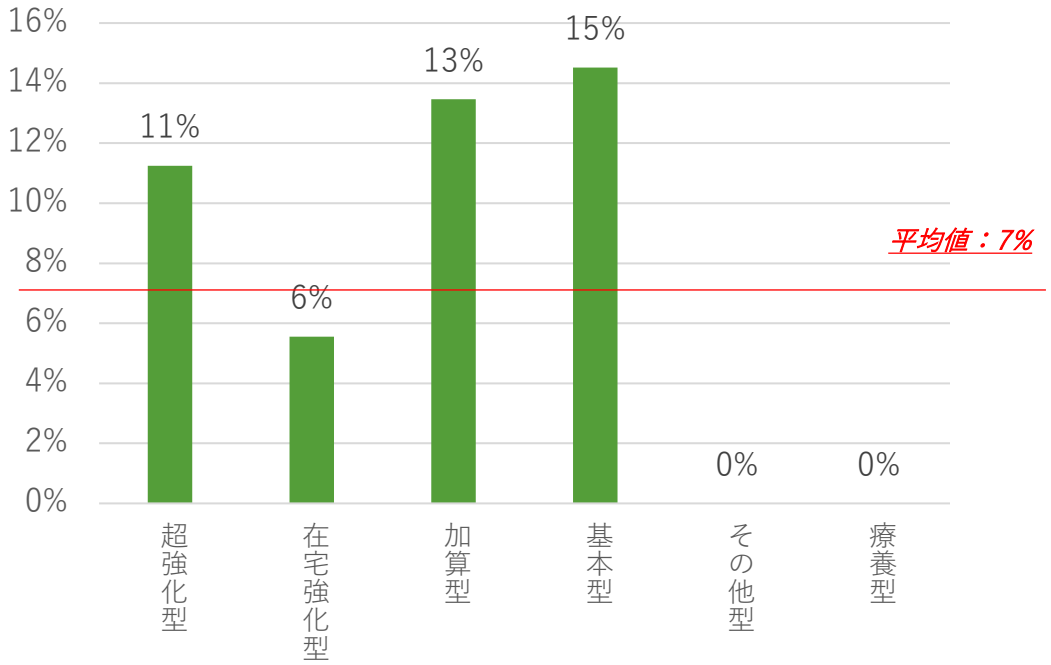
＜アンケート調査結果_施設類型別(6/8)＞

【セキュリティ予算】 ※N＝657

＜⑩：年間のセキュリティ予算のうち、「500万未満」及び「分からない」と回答した（「500万以上」以外で回答した）施設割合＞



＜⑪：セキュリティ予算が十分と回答した施設の割合＞

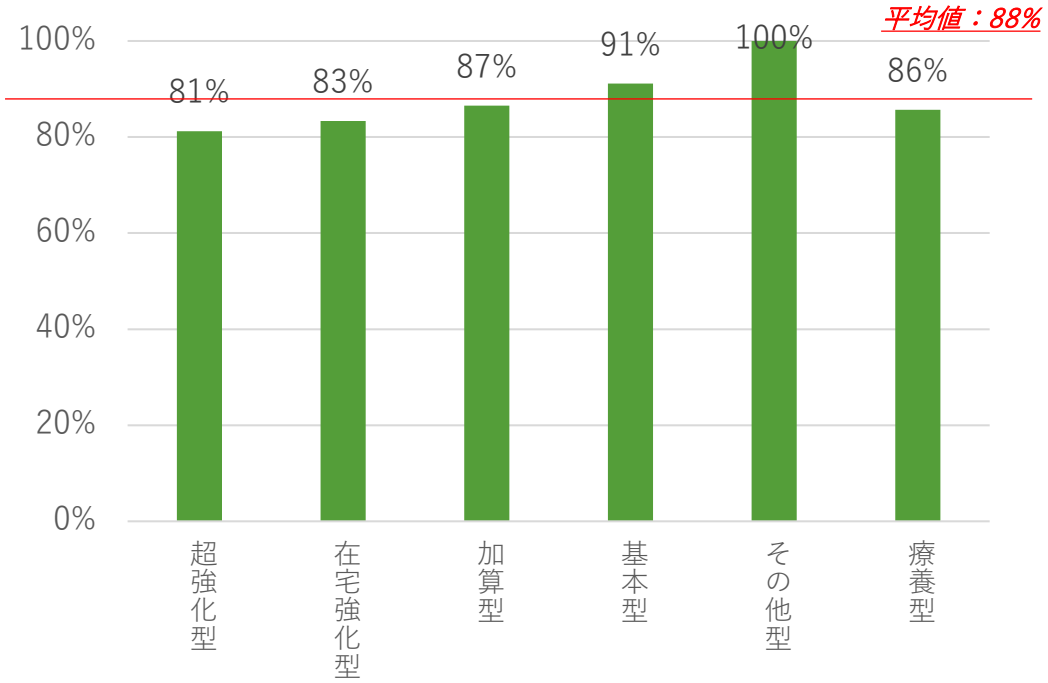


どの施設類型においても年間セキュリティ予算が500万未満（「分からない」を含む）が非常に高く、
セキュリティ予算が十分と回答した施設は平均で1割以下である。なお、「その他類型」「療養型」においては年間セキュリティ予算が500万以上、かつ、セキュリティ予算が十分と回答した施設は1件も存在しない状況であった。

＜アンケート調査結果_施設類型別(7/8)＞

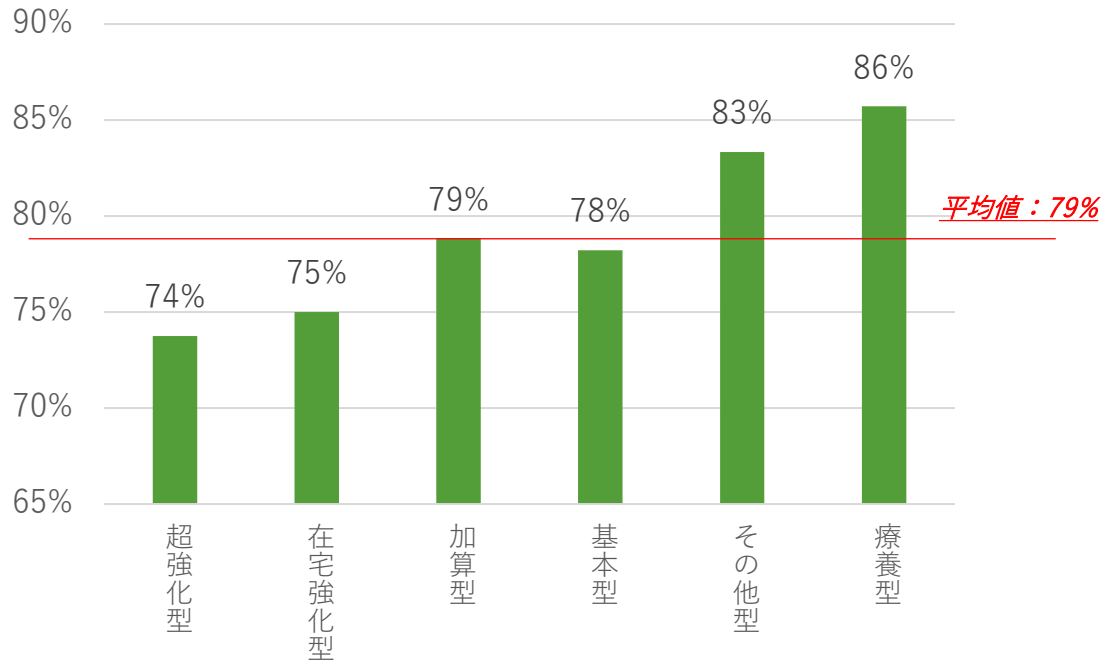
【サイバー保険】 ※N＝657

＜⑫：サイバー保険を「加入」以外で回答した（「未加入」/「分からない」と回答した）施設割合＞



【クローズドNWの安全性】 ※N＝657

＜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＞

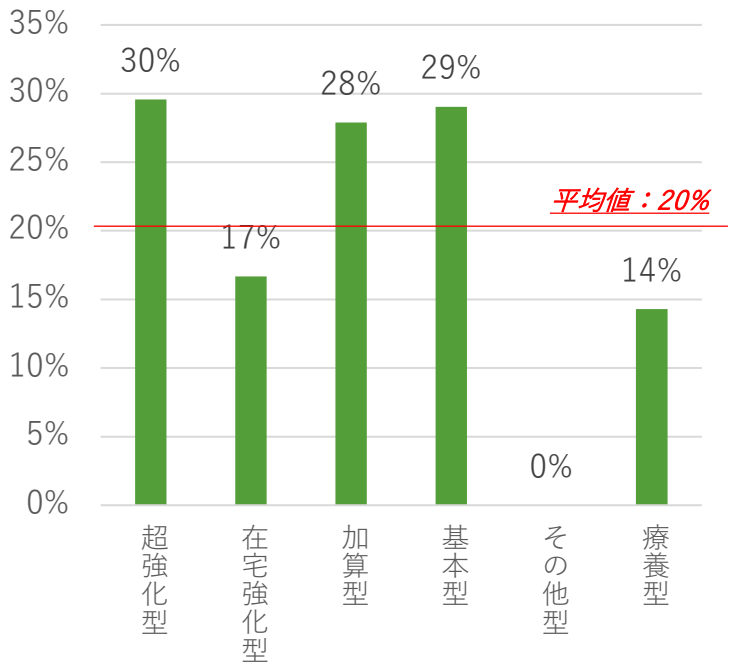


サイバー保険の加入率、及びクローズドNWの安全神話への非共感率は、**介護機能の充実性の高い施設が相対的に上回っている状況であるが、そもそも全体平均としても高い割合を示している**。

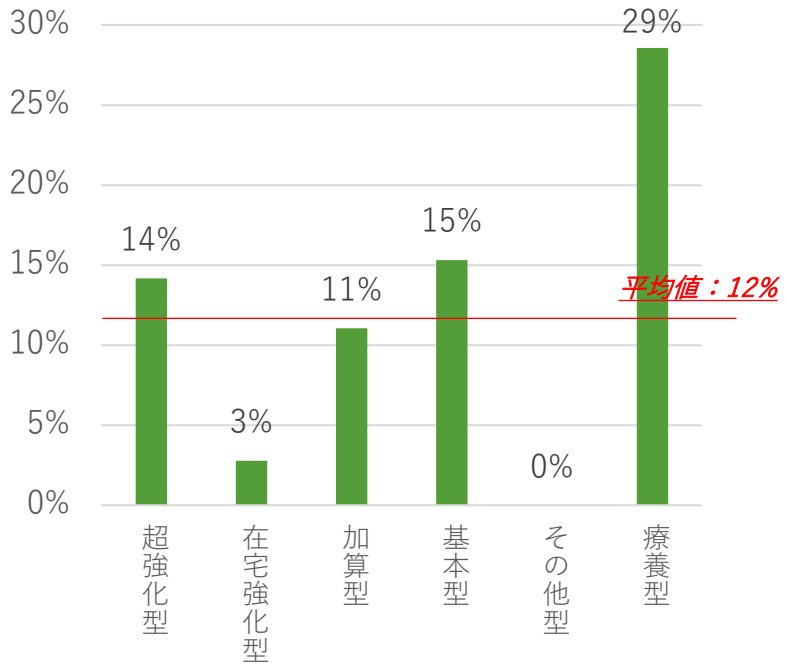
＜アンケート調査結果_施設類型別(8/8)＞

【システム提供事業者とのコミュニケーション状況】 ※N＝657

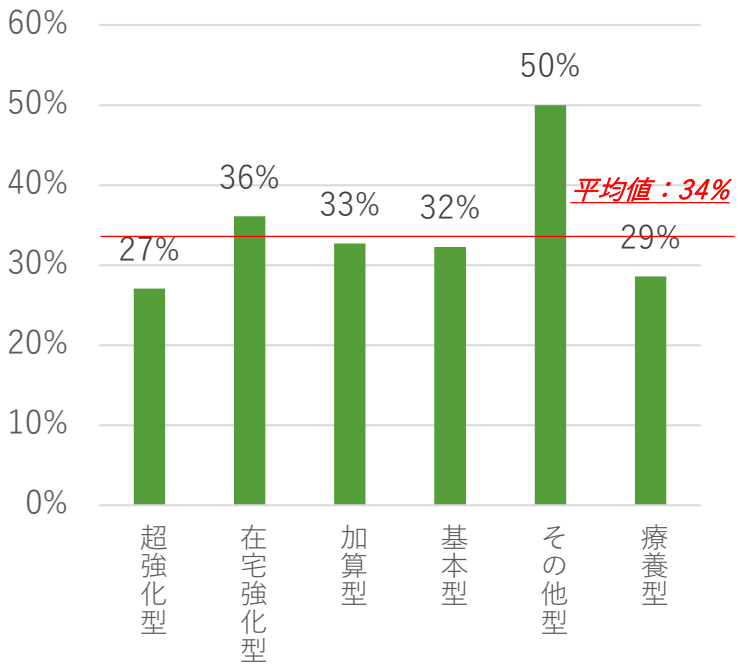
＜⑭：IT事業者によるセキュリティ対策の「指示を受けている」と回答した施設割合＞



＜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＞



「超強化型」・「加算型」・「基本型」は介護IT事業者によるユーザセキュリティ指示率は相対的に高く、セキュリティ契約締結率も平均以上である一方、**事業者への信頼度は低い**。一方で、「その他型」はセキュリティ指示も受けず、契約締結していないものの、IT事業者への信頼度が高く、**事業者への盲目的な依存度が高い**。
また、「療養型」は契約率/信頼率は同数だが、セキュリティ指示受領率は低く、**有効にIT事業者をセキュリティ面で活用できていない**と言える。

５．IT利用環境別結果

＜アンケート調査結果総評_IT利用環境別結果＞

- IT利用環境を「ケアプランシステムのみ」/「ケアプランシステム及び関連施設等の電子カルテ連携あり」/「関連施設等の電子カルテのみ利用」という３つの観点から整理し、サイバー攻撃脅威への感受率を見たところ、ケアプランシステムのみの利用組織が最も割合が低い状況である。直近の医療機関におけるランサム被害の報道等のインパクトにより、**電カルという医療性資源の高いシステムの利用有無が、介護分野においても相応にサイバーリスクへの感受性に影響を及ぼしている**と言える。

- 一方、どのIT利用環境においても、**そもそもどういったVPN機器が利用されているかについて把握していない層が最も高く**、電カルのみ利用組織がこのなかで最も脆弱性対応率が低い。これは電カルのみ利用組織が相対的に機器のインベントリー情報を把握している割合が低いことによる。

- バックアップの取得率は環境によらず概ね９割前後であり、ランサム感染に備えたオフライン/オフサイト型の保管方式もいずれも高い傾向が示されている。

- ケアシステムのみの利用施設が最もIT人材数が高い一方で、厚労省GLの把握率/セキュリティ監査実施率は他のIT利用環境組織と比較すると低い状況である。**これらの層では、人はいても、知識/ノウハウが不足しており、セキュリティ面でのリソース活用が十分でない点が示されている**。

- 年間セキュリティ予算はどのIT利用環境でも共通的に低く、その満足率は一律低い。

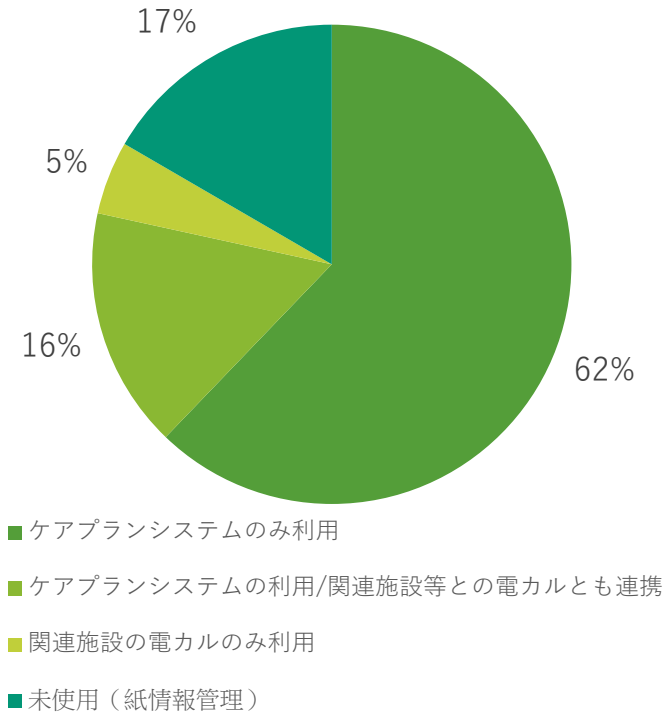
- **電カルを利用する組織では、サイバー保険の加入率が高まる傾向**にある。一方で、クローズドNWの安全神話への共感度自体はどのIT利用環境組織においても大きな差異はない。

- 電カルシステムを利用している組織は、ケアシステムのみ利用の組織と比較して、IT事業者によるセキュリティ指示率が高い。相対的に、IT事業者とのセキュリティ契約率はケアシステム/電カルの双方を利用する組織が高く、そうした組織におけるセキュリティ対応報告への信頼率は他と比較しても低い。**IT化の成熟度が高いほど、セキュリティ面の契約を結び、かつ、一定の不満をIT事業者に抱いていることがわかる。**

＜アンケート調査結果_IT利用環境別結果(1/7)＞

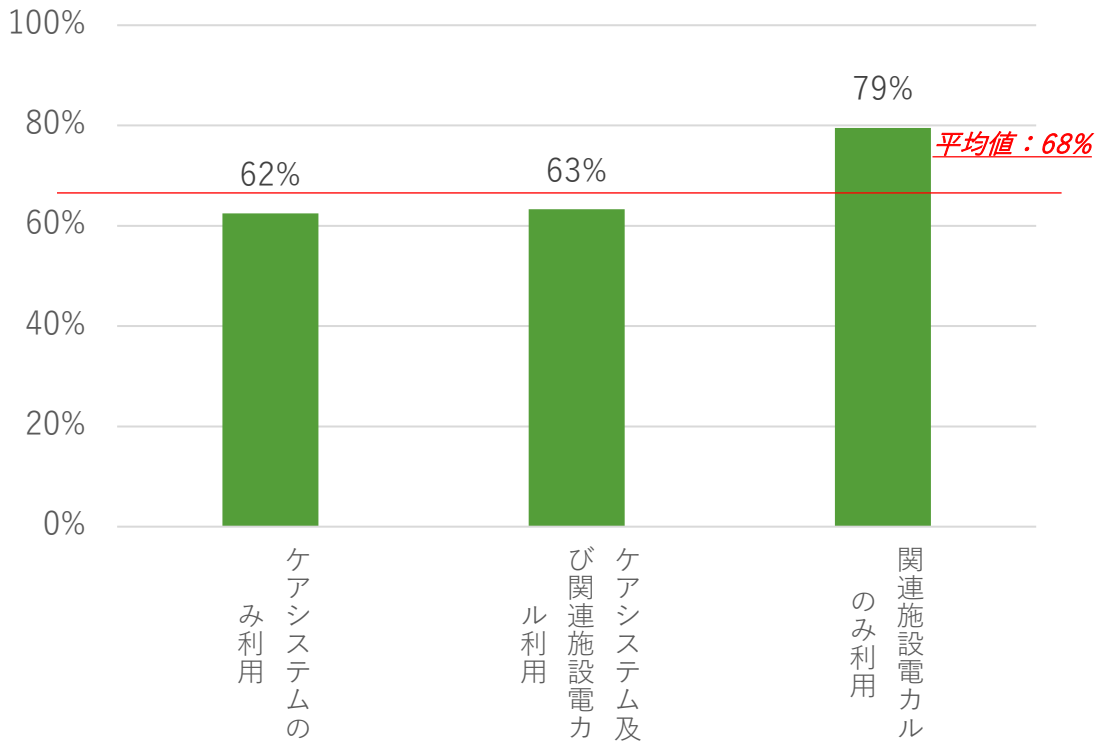
【ITの利用形態】

＜①：ITの利用形態＞　※N＝788



【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＝657



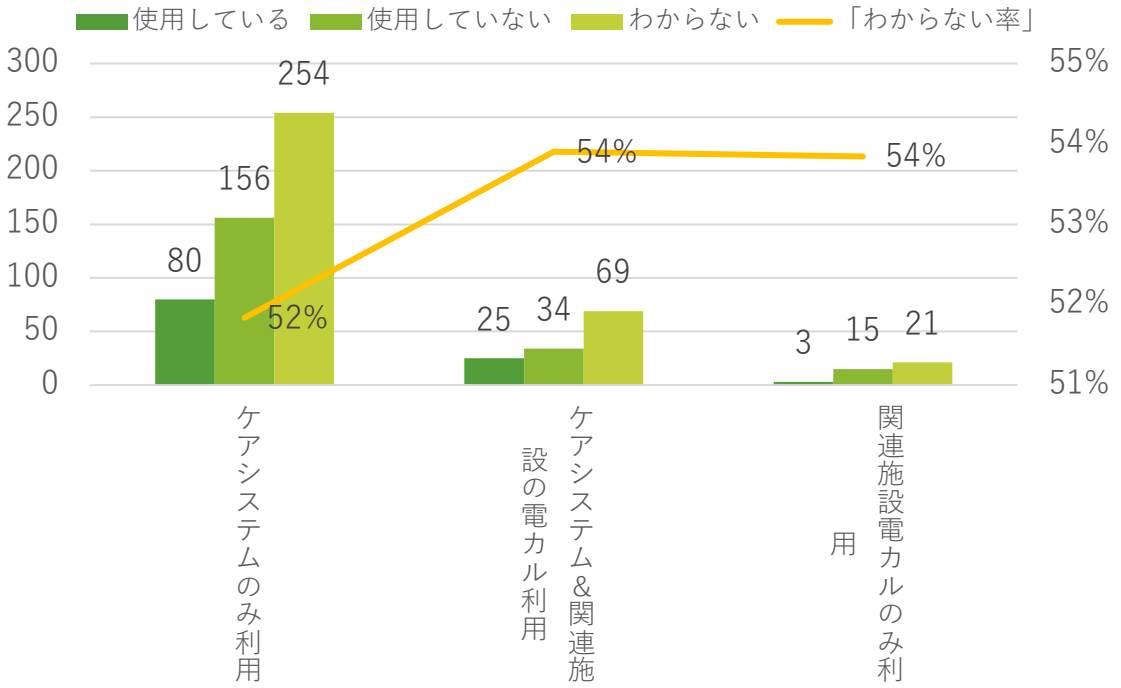
IT利用形態別でみると、サイバーリスクへの感受性については、**関連施設の電カルのみを利用している組織が高い**一方で、**ケアシステムのみを利用している組織が低い**状況が示されている。

＜アンケート調査結果_ IT利用環境別結果(2/7)＞

【脆弱性対策】

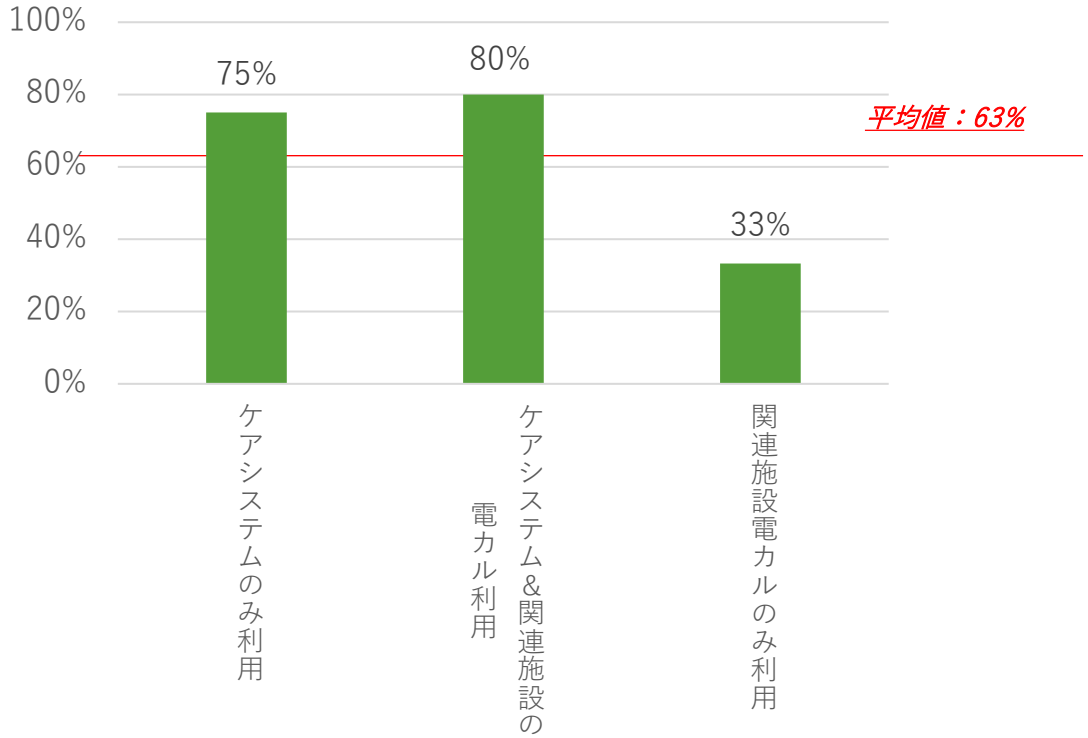
<③：厚労省等から脆弱性が指摘されたForitnet社製VPN機器を使用している施設割合>

※N＝657



<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＝108

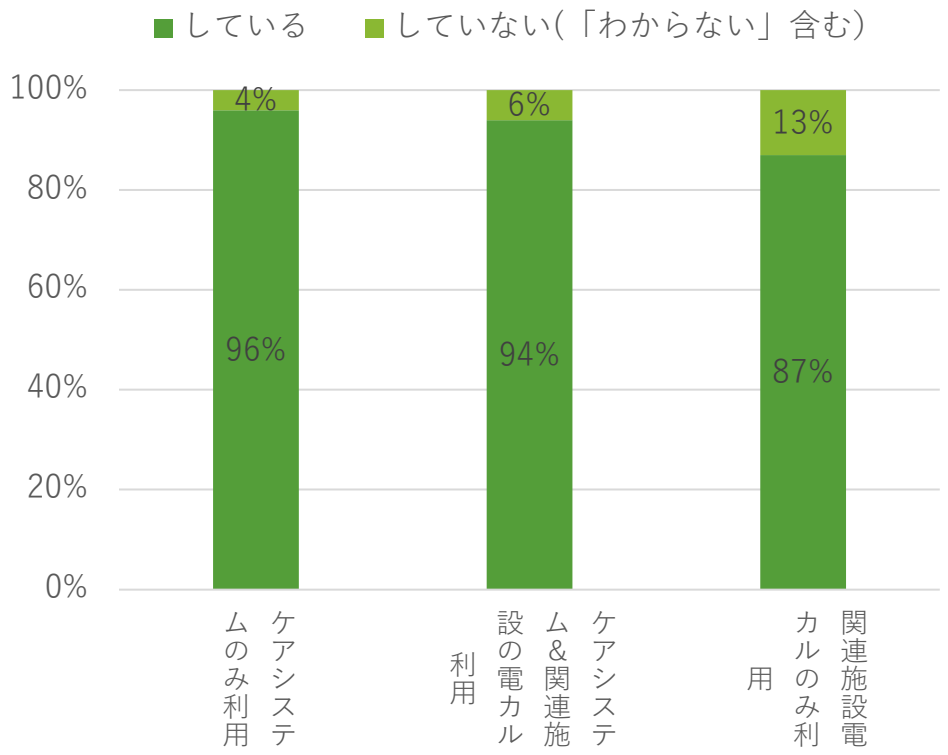


どのIT利用形態においても、**脆弱性報告が行われているVPN機器の利用有無をそもそも把握してない割合が最も高い**。
また、脆弱性対応が未了との回答割合は、関連施設の電カルのみ利用している施設が多い。

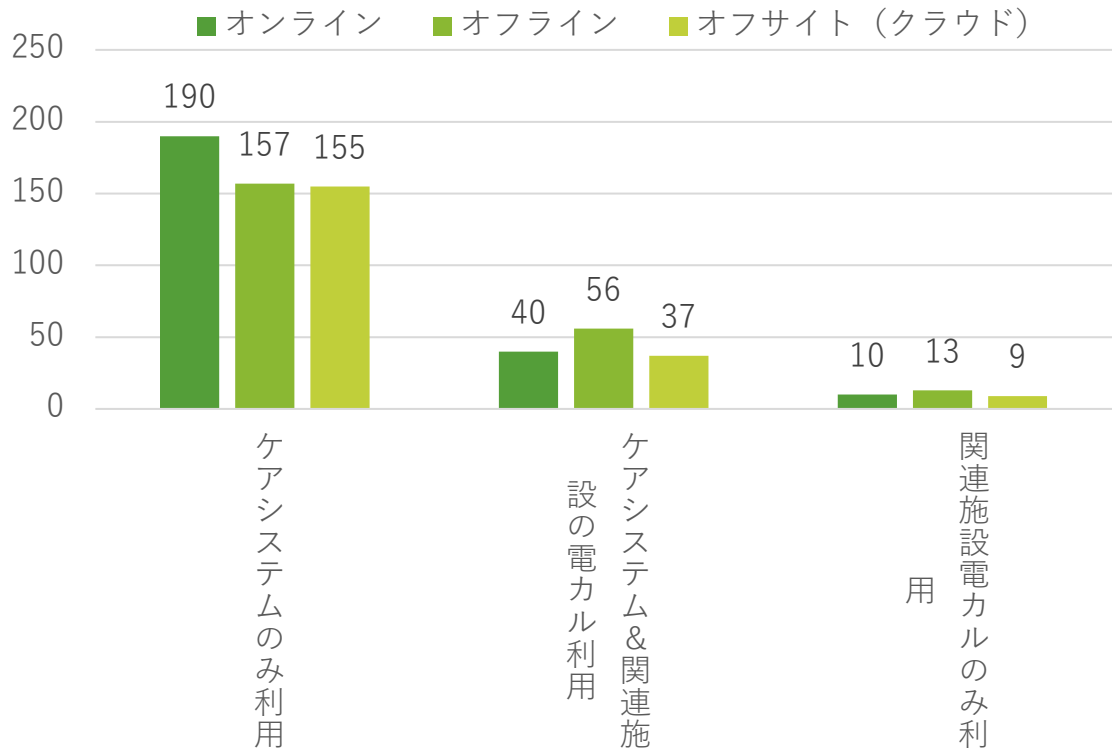
＜アンケート調査結果_ IT利用環境別結果(3/7) ＞

【バックアップ対策】

＜⑥-1：バックアップの取得率＞ ※N＝657



＜⑥-2：バックアップの保管方式(複数選択式）＞ ※N＝563



IT利用環境にかかわらず、バックアップの取得率は概ね９割前後であり、
ランサム感染に備えたオフライン/オフサイト型の保管方式もいずれも高い傾向が示されている。

＜アンケート調査結果_ IT利用環境別結果(4/7) ＞

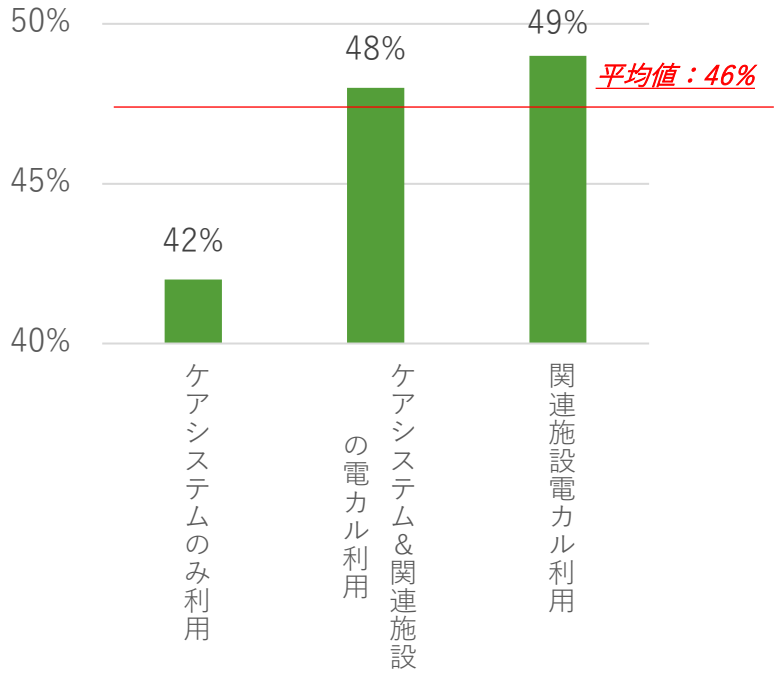
【IT人材】 ※N＝657

＜⑦：IT人材数＞

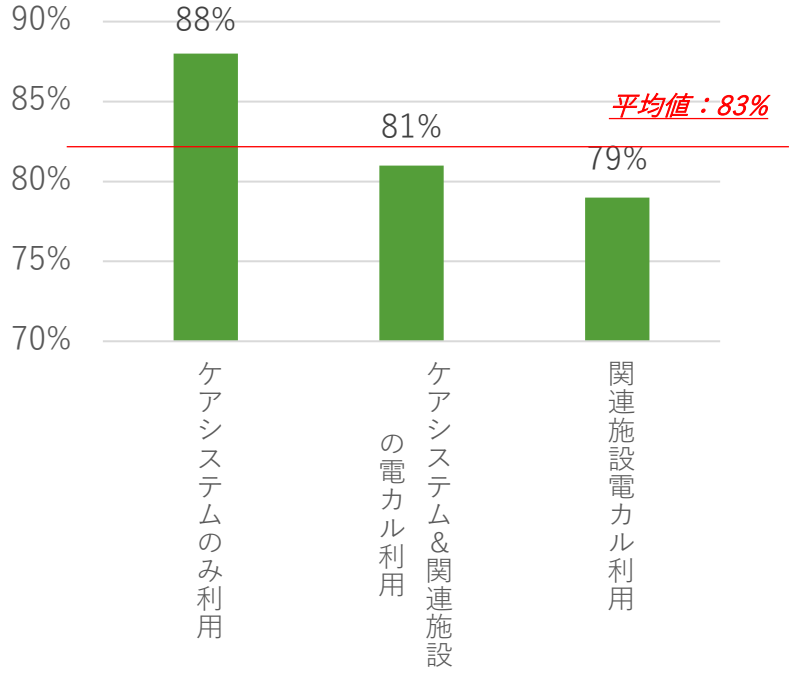
IT利用環境別	施設内システム担当者	うち、常勤数
ケアシステムのみ利用	2.3人	2.3人
ケアシステム＆関連施設の電カル利用	1.1人	1.1人
関連施設電カルのみ利用	0.9人	0.9人

【監査】 ※N＝657

＜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＞

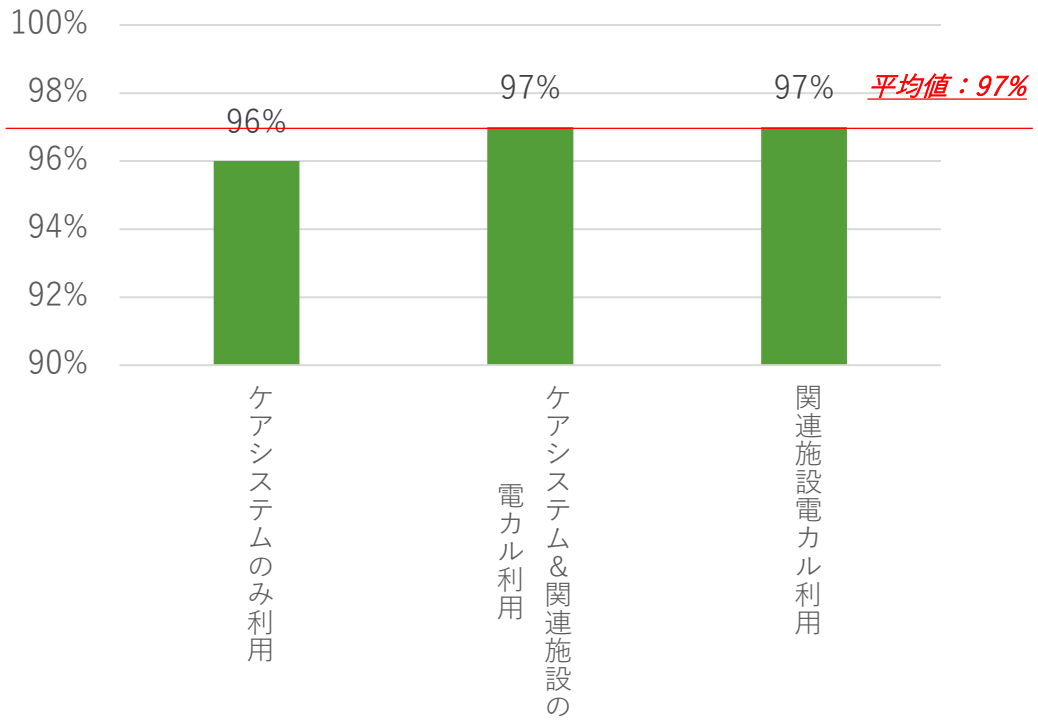


今回の調査結果からは、ケアシステムのみ利用施設が最もIT人材数が高いことが示されたが、
厚労省GLの把握率/セキュリティ監査実施率は他のIT利用環境組織と比較すると低い状況であった。
ケアシステムのみ利用組織では、**人はいても、知識/ノウハウが不足している**状況にあると言える。

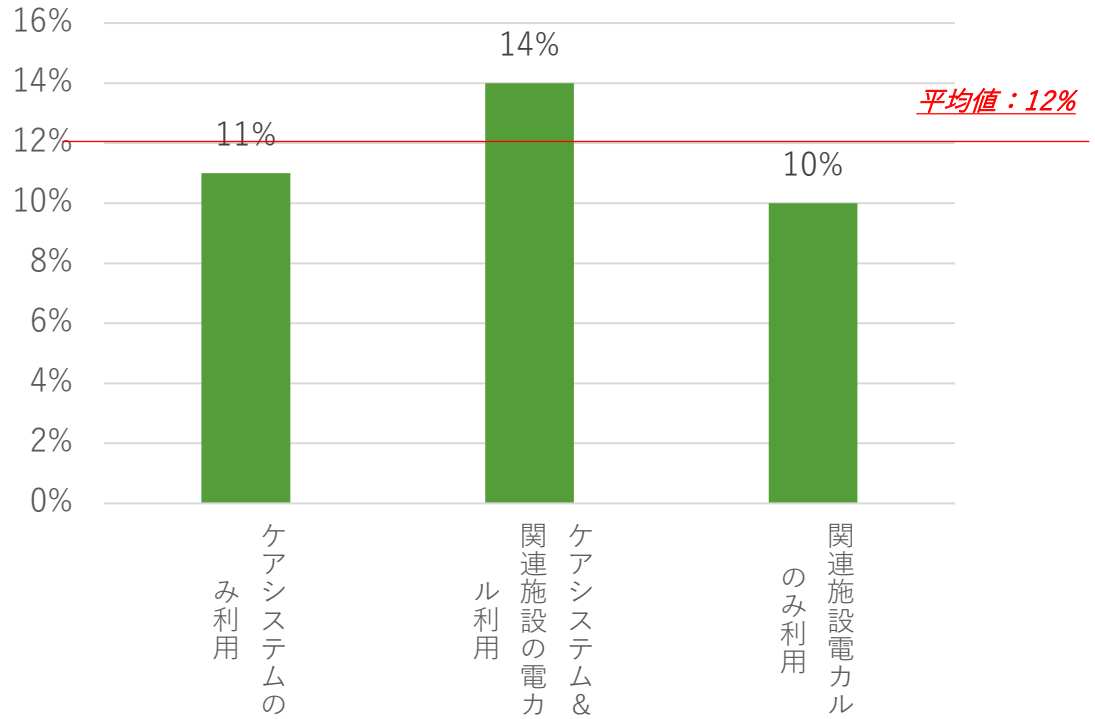
＜アンケート調査結果_ IT利用環境別結果(5/7)＞

【セキュリティ予算】 ※N＝657

＜⑩：年間のセキュリティ予算のうち、「500万未満」及び「分からない」と回答した（「500万以上」以外で回答した）施設割合＞



＜⑪：セキュリティ予算が十分と回答した施設の割合＞

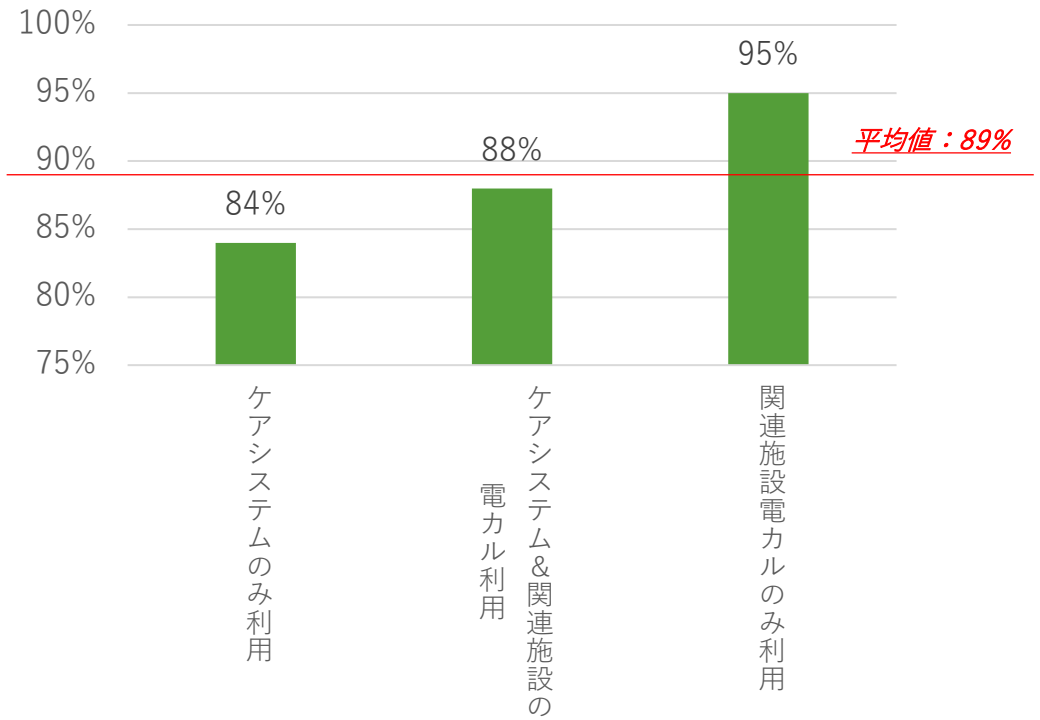


IT利用環境別の観点においても、年間セキュリティ予算は一律低く、かつ、
それで十分と考える施設は１割前後にとどまることが示されている。

＜アンケート調査結果_ IT利用環境別結果(6/7)＞

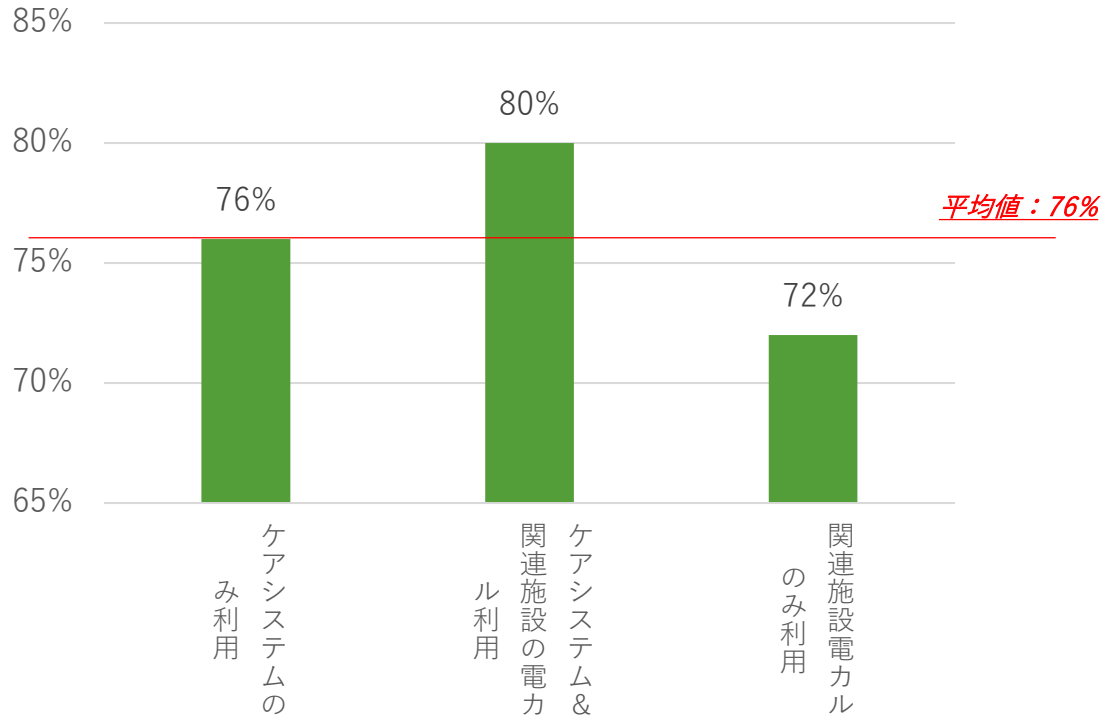
【サイバー保険】 ※N＝657

＜⑫：サイバー保険を「加入」以外で回答した（「未加入」/「分からない」と回答した）施設割合＞



【クローズドNWの安全性】 ※N＝657

＜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＞

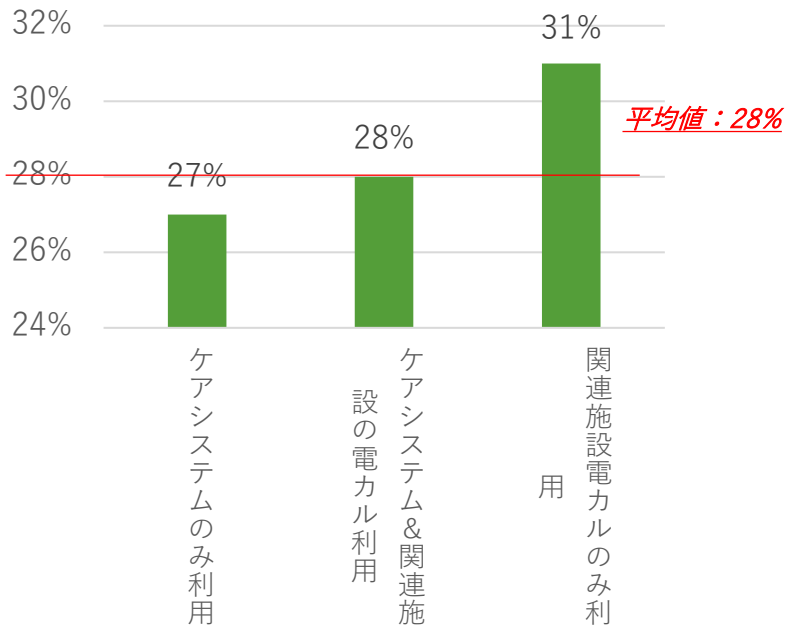


<u>電カルを利用する組織では、サイバー保険の加入率が高まる</u>傾向にある。一方で、クローズドNWの安全神話への共感度自体はどのIT利用環境組織においても大きな差異はなく、**<u>老健施設共通で８割弱はそうした考えに陥っている</u>**と言える。

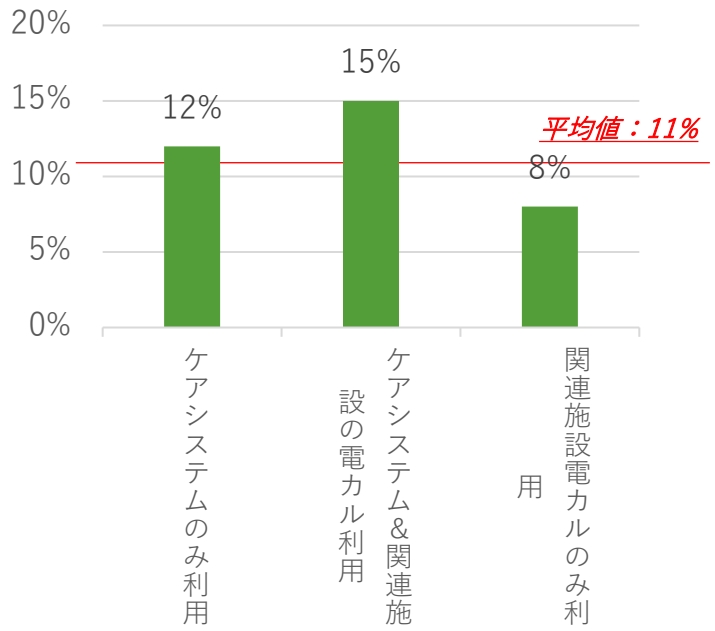
＜アンケート調査結果_ IT利用環境別結果(7/7)＞

【システム提供事業者とのコミュニケーション状況】 ※N＝657

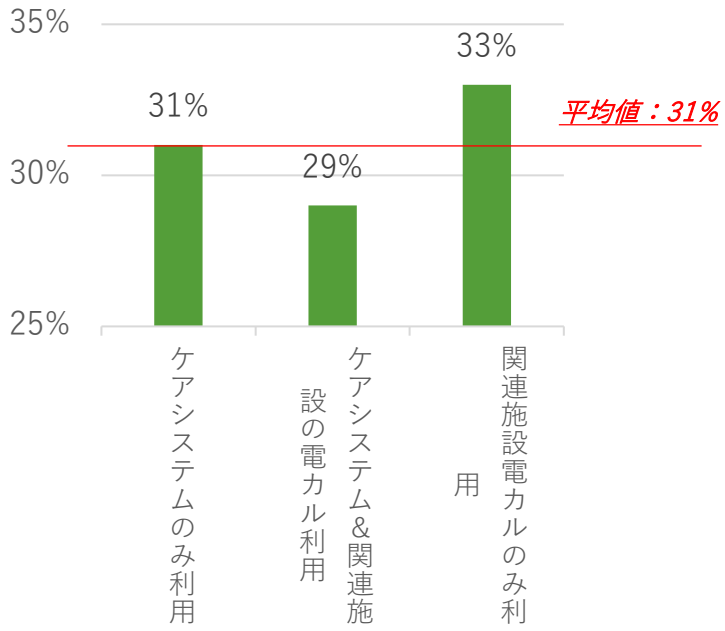
＜⑭：IT事業者によるセキュリティ対策の「指示を受けている」と回答した施設割合＞



＜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＞



電カルシステムを利用している組織は、ケアシステムのみ利用の組織と比較して、IT事業者によるセキュリティ指示率が高い。
相対的に、IT事業者とのセキュリティ契約率はケアシステム/電カルの双方を利用する組織が高く、そうした組織におけるセキュリティ対応報告への信頼率は他と比較しても低い。**IT化の成熟度が高いほど、セキュリティ面の契約を結び、かつ、一定の不満をIT事業者に抱いていることがわかる。**


Medical Information
Sharing and Analysis Center