一般社団法人日本保険薬局協会
セキュリティアンケート調査結果

一般社団法人日本保険薬局協会
/一般社団法人医療ISAC

2023年3月

＜目次＞

1．調査概要

調査目的

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、保険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保険薬局を対象として、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ので、電子薬歴システムや関連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。

なお、ご回答いただいた内容や、企業名、薬局名などを公開することは一切ございませんのでご安心くださいますようお願い申し上げます。

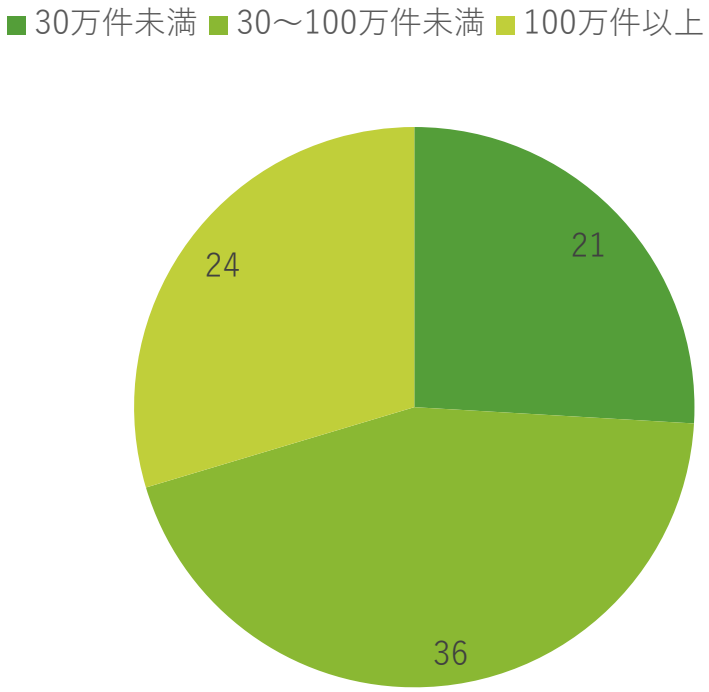
本調査は日本保険薬局協会と医療ISACの共同事業となります。

調査対象

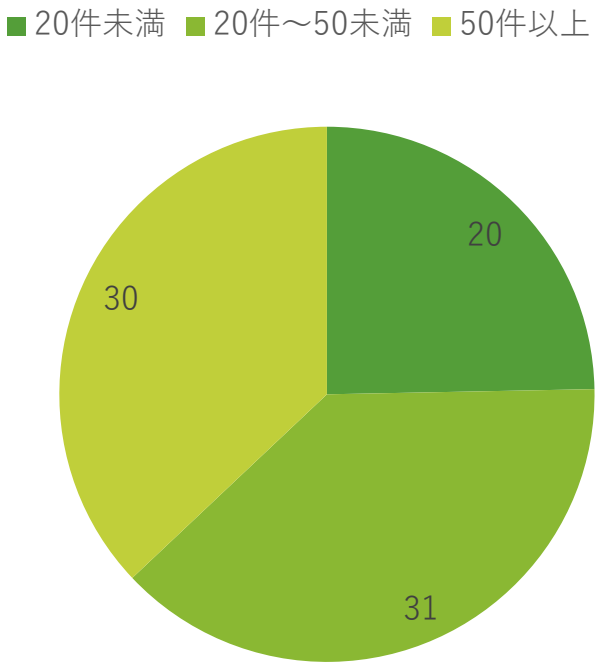
- 実施期間：2023年1月23日～2月18日
- 調査対象全数：567件（正会員/賛助会員全体）
- 回答合計数（回答率）：81件（14%）
- うち調査対象数：81件
- 調査組織：（一社）日本保険薬局協会/（一社） 医療ISAC

＜年間調剤件数別内訳＞

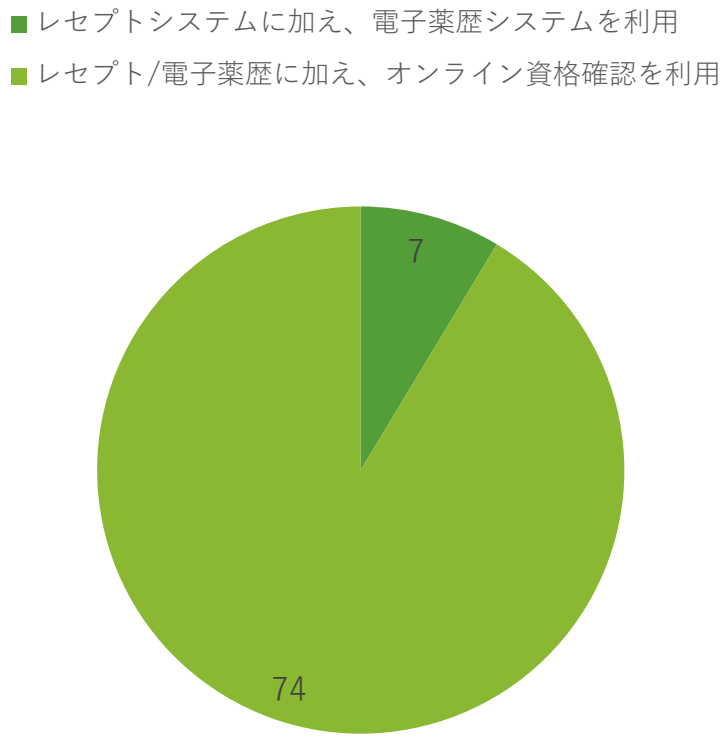
※：令和4年1月1日から令和4年12月31日までの調剤実施件数



＜運営薬局件数別内訳＞



＜IT利用環境別内訳＞



※：「オンラインレセプトシステムのみ利用」
「紙情報で管理」は0件

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？	□ オンラインレセプトシステムのみを利用している □ オンラインレセプトシステムに加え、電子薬歴管理システムを利用している □ オンラインレセプト/電子薬歴管理システムに加え、保険証のオンライン資格確認とも情報連携している □ 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　□わからない
サイバー保険	⑫：サイバー保険に加入しているか？	□システムの復旧費用にも対応したサイバーセキュリティ総合保険に加入している □情報漏えいにの補償などに絞ったサイバー保険に加入している □サイバー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：基幹系システム（ 薬歴システム/レセプトシステム ）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、IT事業者は貴社に対して、検討・実施すべきセキュリティ対策の指示を行っていますか？	□行っている　□行っていない　□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？	□行っている　□行っていない　□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？	□している　□していない　□わからない

２．全体結果

＜アンケート調査結果_全体総評＞

- 今回の調査対象薬局のうち、保険証等のオンライン資格確認との連携という、インターネットとの接続を前提としたIT環境の利用施設数は9割強を占めており、**それ以外も含めた全体平均においても8割以上はサイバー攻撃への脅威**を感じている

- 厚労省から脆弱性が周知されたVPN機器を利用している薬局の全体割合は3割強であり、**9割弱はこれらの脆弱性対応は完了している状況である。**

- **バックアップの取得率はほぼ100%**であり、ランサム感染リスクを低減するための**オフライン取得率は7割**近く、**オフサイト取得率は3割以上**に及んでいる状況である。

- さらに、IT人材数の全体平均も６名弱と医療・介護・健診分野と比較しても多く、厚労省安全管理GLの把握率も８割強に及んでいる。ただし、セキュリティ監査の定期実施率は3割程度であり、未実施率が6割弱を占めており、**IT人材規模に応じた定期的なセキュリティ監査を通したPDCAへの取組率は相対的に低い**といえる。

- 年間セキュリティ予算は500万未満が最も多いが、500万以上の予算確保率は3割弱、さらに**1000万以上の予算を確保できている施設も15%近く存在**している。それにもかかわらず、セキュリティ予算が十分と回答した施設割合は1割強しかなく、**調剤頻度/運営店舗数に応じた適切なセキュリティ対応が十分に行えていない状況がみられる。**

- サイバー保険の加入割合は**3割強にあり、医療・介護・健診等の関連分野と比較した際に高い**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。

- IT事業者によるセキュリティ対策の指示等を確認している組織は全体の半分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（45%)であることが示されており、**一部の施設ではIT事業者への過度な依存が危険であることが認識されている。**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。

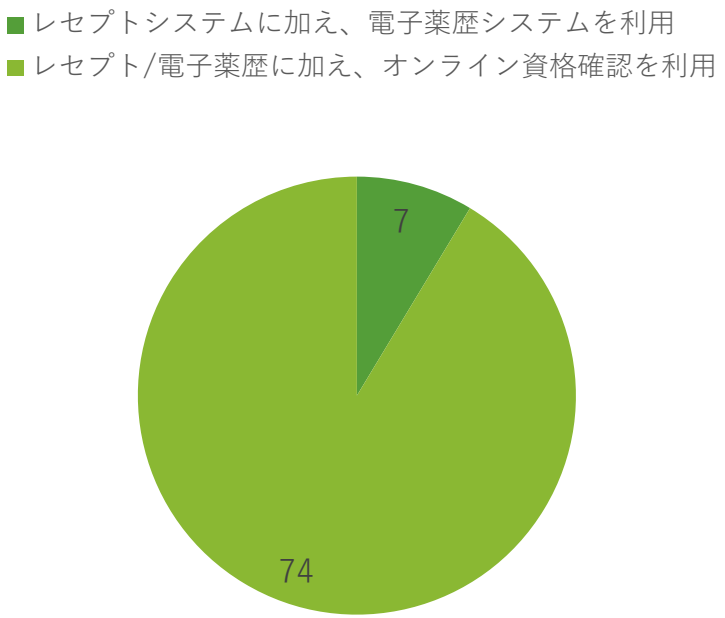
- 総合すると、医療・介護・健診等の他分野同様、薬局においてもサイバー攻撃への脅威の感受率は高く、ランサムウェア攻撃へのリスクに備えたバックアップについてもオフライン/オンサイトでの取得率が高い。特に他分野と比較した際のIT人材配置数は多く、厚労省GLの把握率も高い。年間セキュリティ予算も他分野と比較すると高く確保できているが、運営薬局数等の規模の大きさの問題もあり、監査等を通したセキュリティPDCAを確実に回すことが難しく、クローズネットワークの安全神話の考え方に拘泥する薬局も一定数は存在していると言える。また、IT事業者への盲目的な依存へのリスクは一部薬局では認識されているが、セキュリティ面も含めた明示的な契約率は他分野同様低いため、**今後、IT事業者に対する主体的なマネージメント意識の向上に加え、高いセキュリティ予算を確保し、セキュリティPDCAを回すことのできている薬局の取組事例等を参考に、厚労省GL等も踏まえ、特にオンライン資格確認等、インターネットとの接続に伴い影響のある範囲から薬局内部のセキュリティ対策に着手していくことが重要と考えられる。**

＜アンケート調査結果_全体結果(1/7)＞

【IT利用の形態】

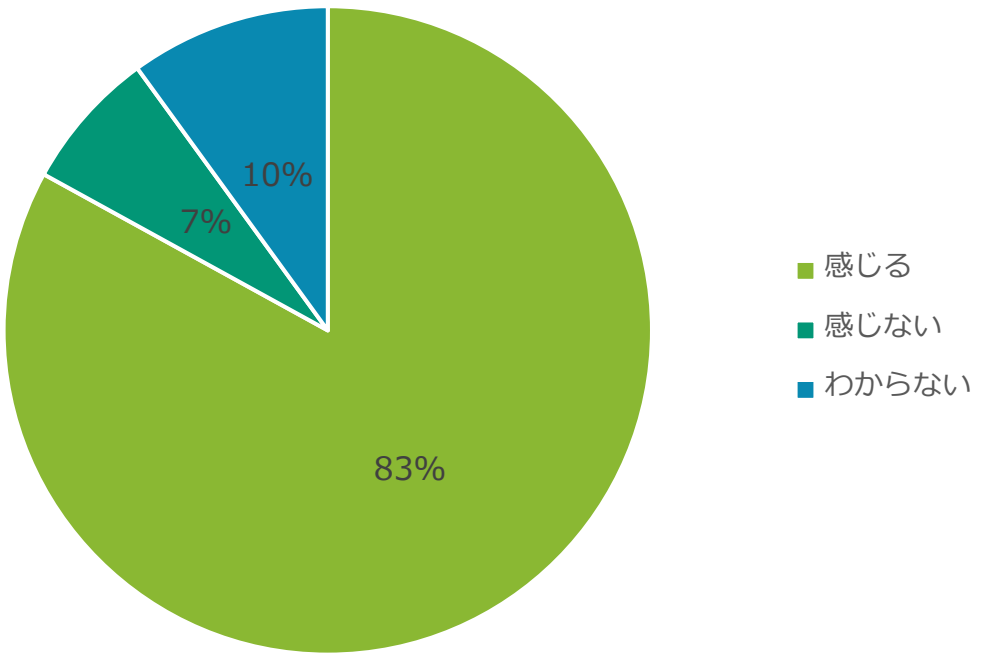
＜①：ITの利用形態は？＞　※N＝81

※：「オンラインレセプトシステムのみ利用」「紙情報で管理」は0件



【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＝81

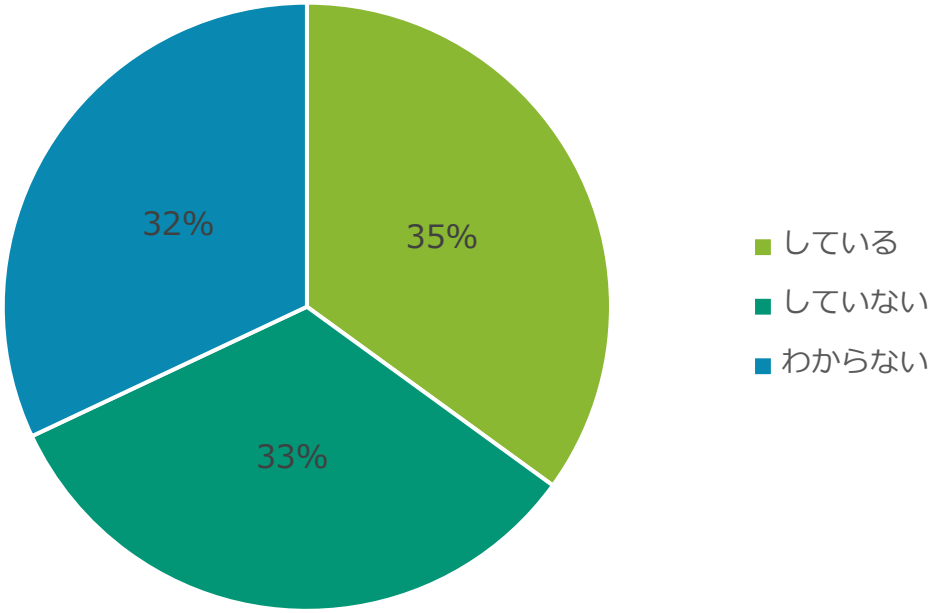


薬局施設におけるオンライン資格確認との連携率という、**インターネットとの接続度は極めて高く**、
かつ、これら施設の**8割以上がサイバー攻撃への脅威を感じている**

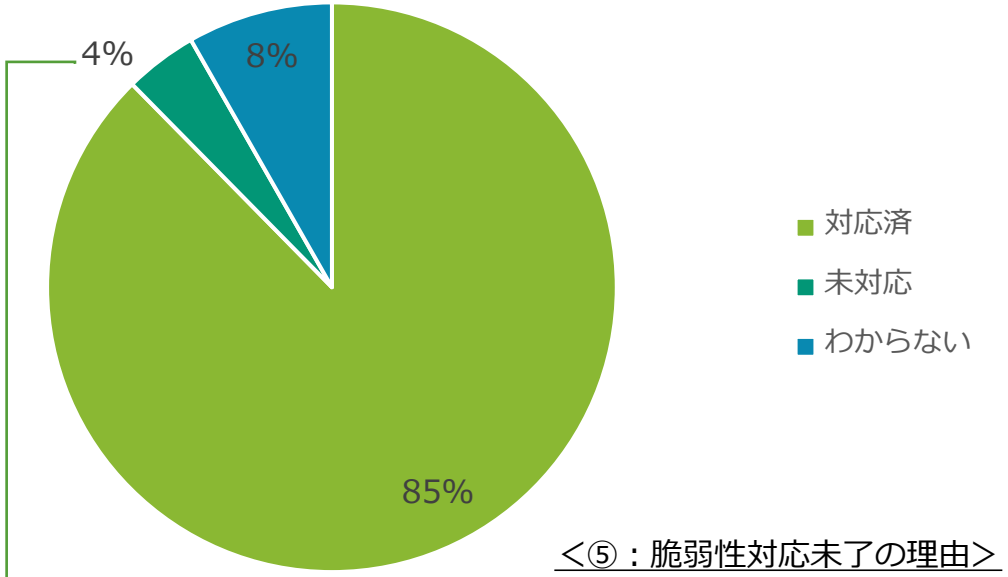
＜アンケート調査結果_全体結果(2/7)＞

【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か？＞　※N＝81



＜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＝26



＜⑤：脆弱性対応未了の理由＞

1件	（理由）脆弱性のあるものは利用していない

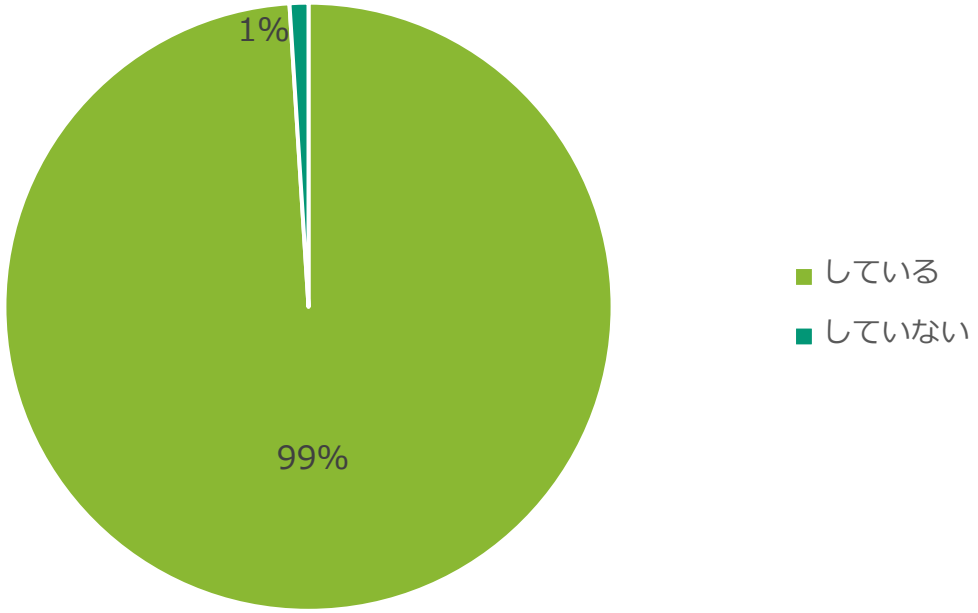
厚労省から脆弱性が周知されたVPN機器を利用している薬局の割合は3割強であり、**9割弱はこれらの脆弱性対応は完了している状況である。**

＜アンケート調査結果_全体結果(3/7)＞

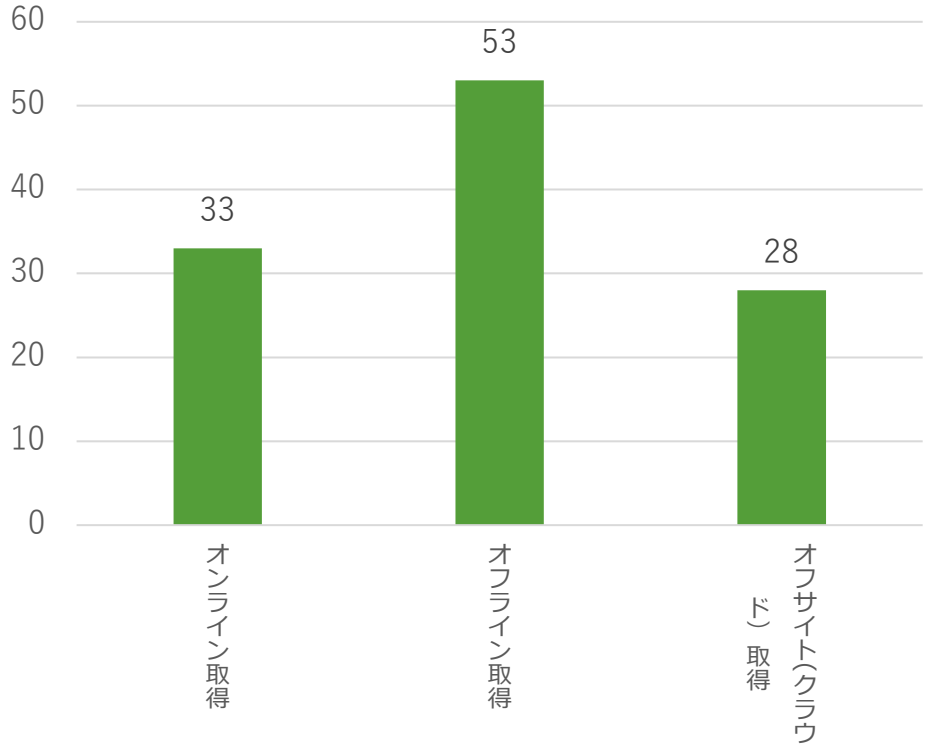
【バックアップ対策】

＜⑥-1：バックアップの取得率＞　※N＝81

※：「わからない」は0件



＜⑥-2：バックアップの取得方式(複数選択式）＞　※N＝80



<u>バックアップの取得率はほぼ100%</u>であり、ランサム感染リスクを低減するための**<u>オフライン取得率は7割</u>**近く、
<u>オフサイト取得率は3割以上</u>に及んでいる状況である。

＜アンケート調査結果_全体結果(4/7)＞

【IT人材】

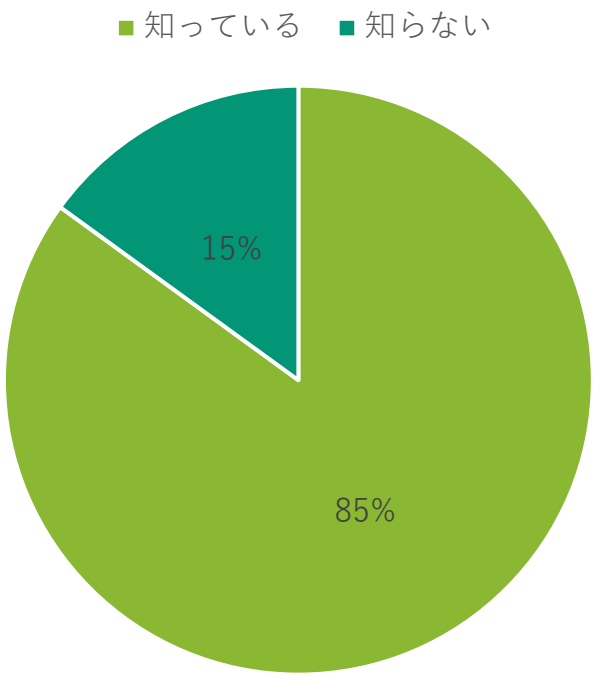
＜⑦：IT人材数＞　※N＝81

種別	平均人数
施設内システム担当者	**5.7人**
うち、常勤数	**4.1人**
常勤率：72%	

【監査】

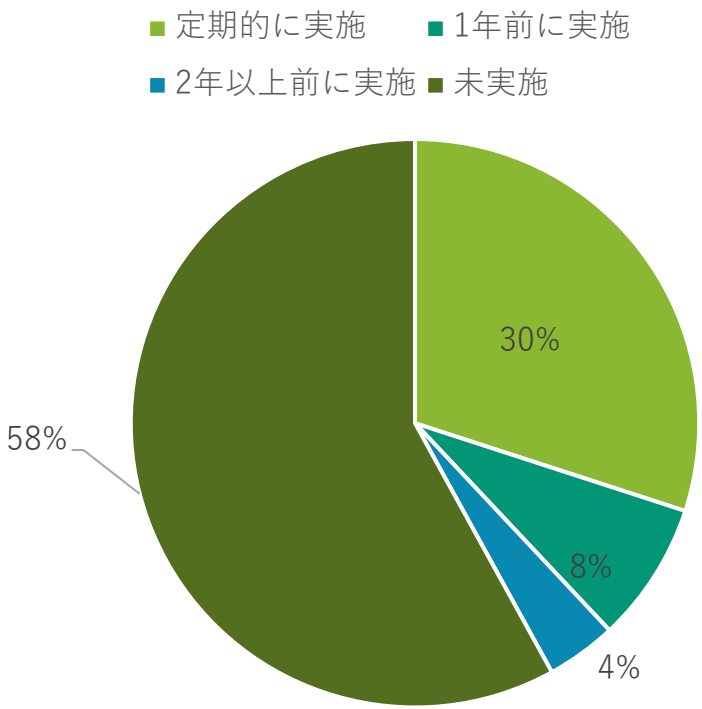
＜⑧：厚労省安全管理GLの認識状況＞

※N＝81



＜⑨：セキュリティ監査の実施状況＞

※N＝81

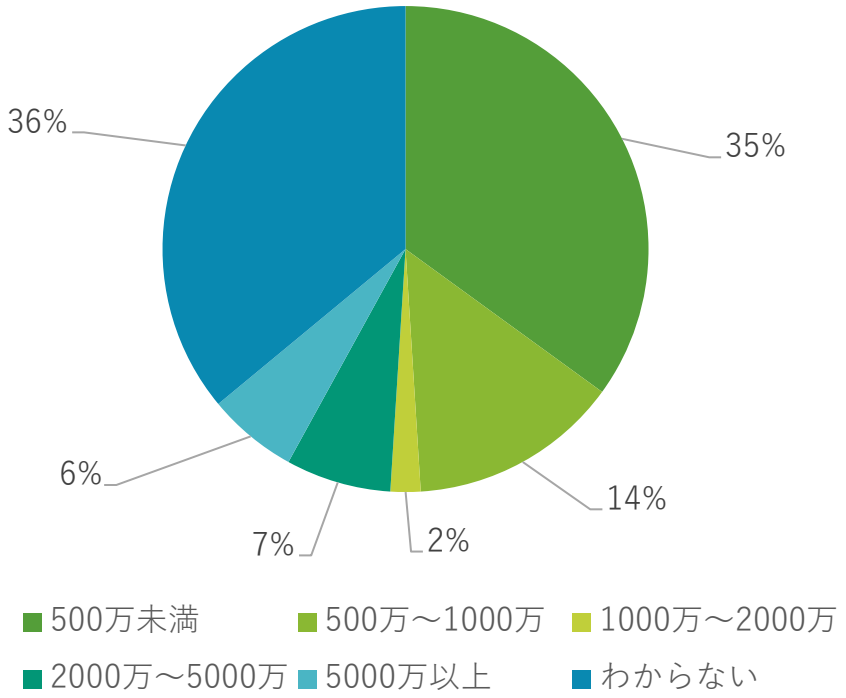


IT人材数は６名弱と多く、厚労省安全管理GLの把握率は８割強に及んでいる。
ただし、セキュリティ監査の定期実施率は3割程度であり、未実施率が6割弱を占めており、**IT人材数に応じた定期的なセキュリティ監査の実施率は相対的に低い**といえる。

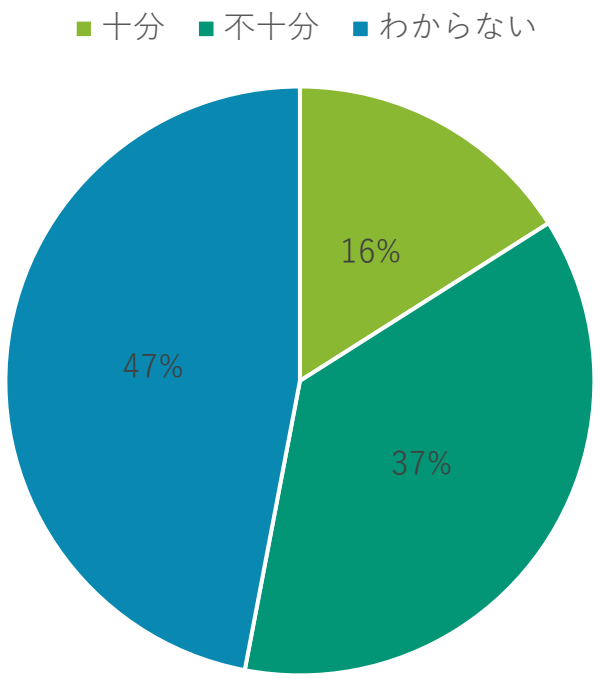
＜アンケート調査結果_全体結果(5/7)＞

【セキュリティ予算】

＜⑩：年間のセキュリティ予算＞　※N＝81



＜⑪：セキュリティ予算の十分性＞　※N＝81

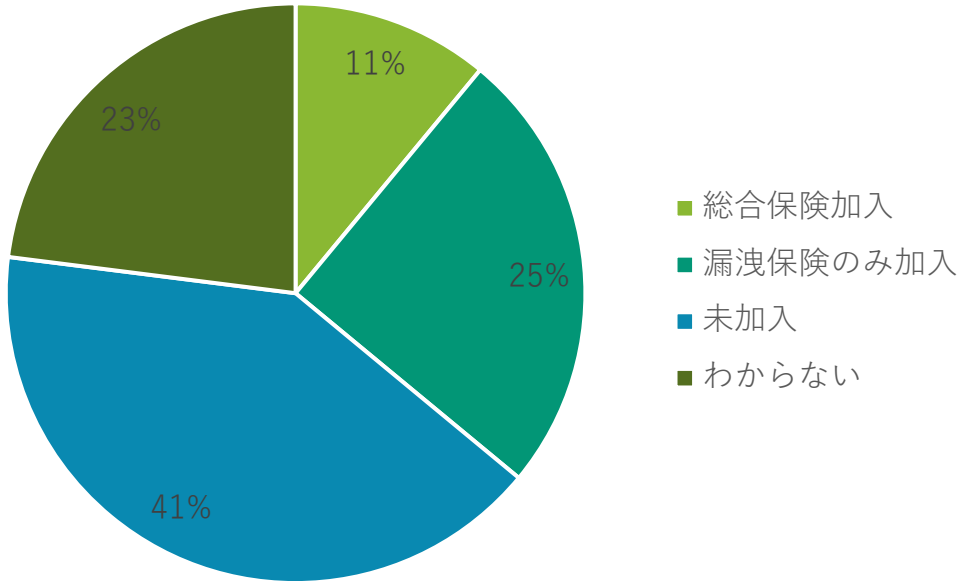


年間セキュリティ予算は500万未満が最も多いが、**1000万以上の予算を確保できている施設も15%近く存在**している。ただし、セキュリティ予算が十分と回答した施設割合は1割強あり、**調剤頻度/運営店舗数に適したセキュリティ対応が十分に行えていない状況がみられる。**

＜アンケート調査結果_全体結果(6/7)＞

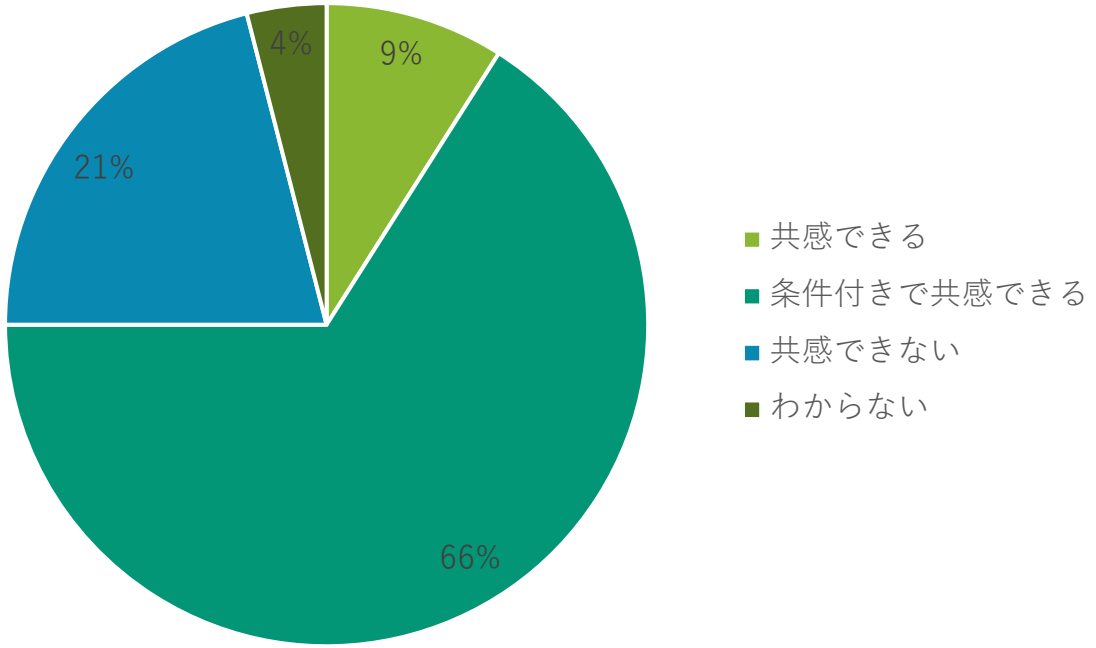
【サイバー保険】

<u>＜⑫：サイバー保険の加入状況＞</u>　※N＝81



【クローズドNWの安全性】

<u>＜⑬：診療系NWは安全という考え方への共感状況＞</u>　※N＝81

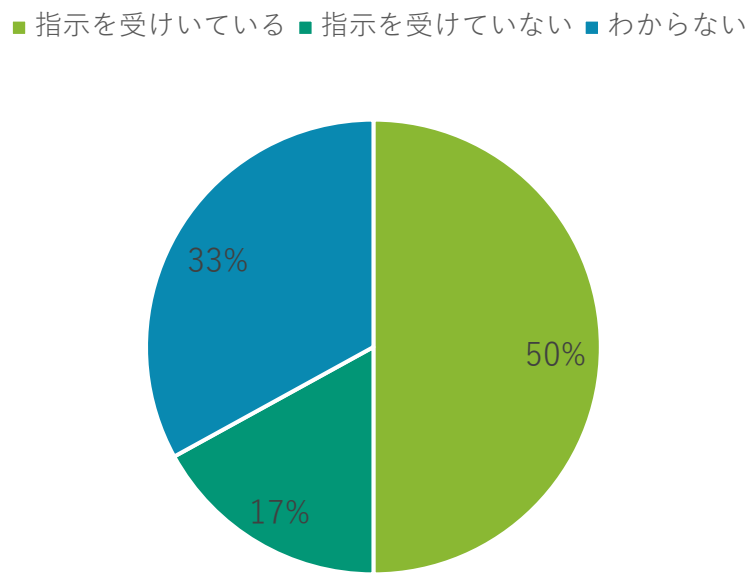


サイバー保険の加入割合は**<u>3割強にあり、医療・介護・健診等の関連分野と比較した際に高い</u>**点が特徴と言える。
ただし、外部との接点を持たない無菌室でシステムセキュリティを考える思考傾向（＝診療系ＮＷはクローズド環境であるため安全と考える傾向）は**<u>他分野同様、高止まりしている</u>**状況である。

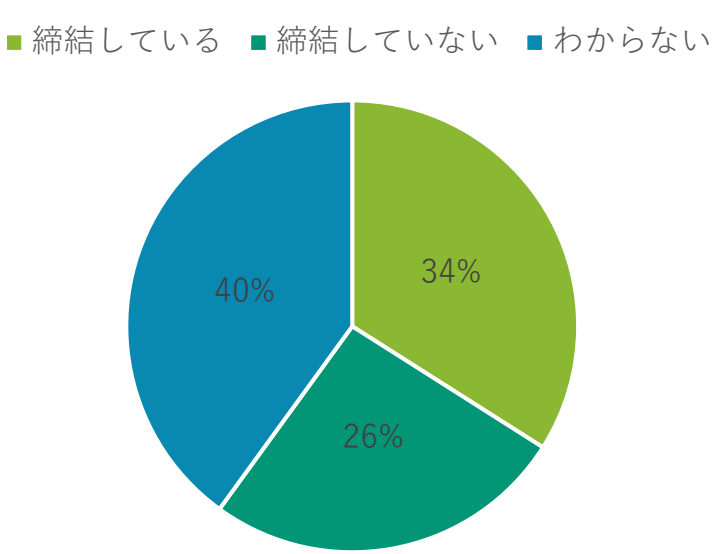
＜アンケート調査結果_全体結果(7/7)＞

【IT事業者とのコミュニケーション状況】　※N＝81

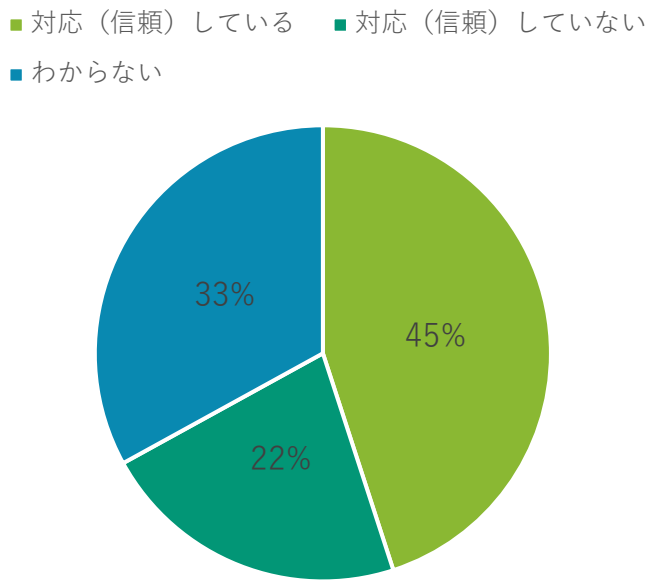
＜⑭：IT事業者によるセキュリティ対策指示状況＞



＜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（50%)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（45%)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．年間調剤件数別結果

＜アンケート調査結果総評_年間調剤件数別＞

- 年間調剤件数別（30万件未満/30万件～100万件未満/100万件以上という3層）でみると、オンライン資格確認との連携も含めた、インターネット接続環境率はいずれの層も高い一方で、サイバー攻撃への脅威感度は年間調剤件数に応じて高まるが、特に30万件未満（小調剤規模）の層は低い傾向がある。

- 年間調剤件数が多いほどVPN機器種別の未把握率（「わからない」率」は低い。ただし、**脆弱性対応率は中調剤規模施設（30万～100万件未満）が相対的にもっとも低い。**

- バックアップ取得率はすべての年間調剤規模において共通的に極めて高い。さらに**どの層においてもオンラインより、オフライン取得率が高いという特徴**が示されている。

- **100万件以上の大規模層は他と比較して突出してIT担当者が多いこと**が分かる。これらの施設は厚労省安全管理GLの把握率やセキュリティ監査実施も高いが、**相対的に、中規模層（30万～100万件未満）ではセキュリティ監査未実施率が低い**状況である。

- **100万件以上の大規模層ではセキュリティ予算が500万以上の割合が高く、2000万以上確保の施設も3割強近く**に及んでいる。一方、セキュリティ予算が十分と回答した施設は30万～100万件未満の中規模層が最も低いが、これらの層も1割強は500万以上のセキュリティ予算を確保していることから、**小規模/大規模の中間に位置する層として、IT規模に応じたセキュリティ施策に苦心していることがわかる。**

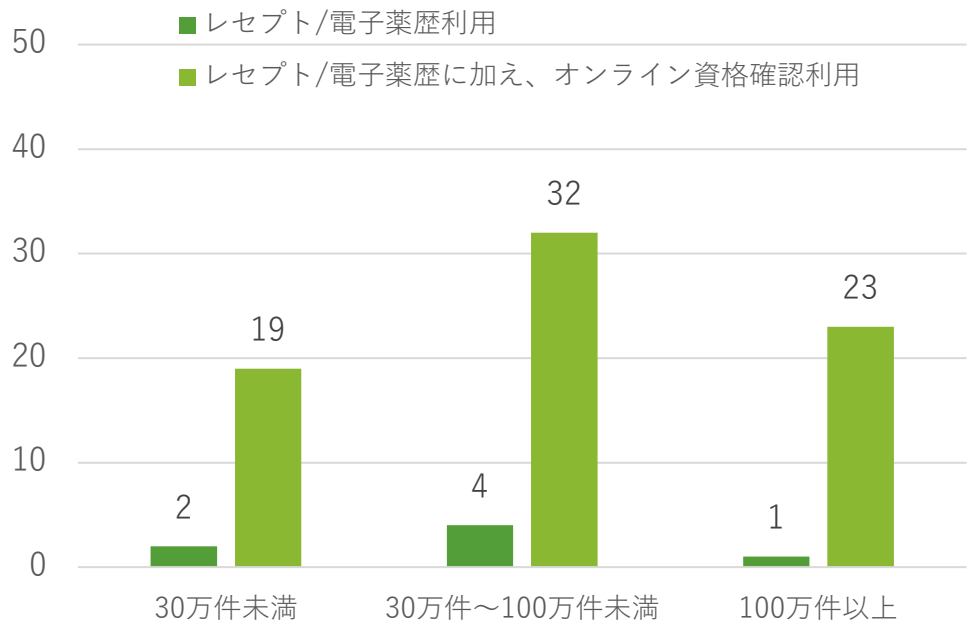
- サイバー保険の未加入率は30万～100万未満の中規模層が高く、**IT規模の拡大に伴うセキュリティへの踏み込みに躊躇する中規模施設の悩みが浮き彫り**になっている。一方で、診療系NWのクローズド神話への共感率は大規模層（100万件以上）が最も高いことから、セキュリティ予算を確保しているが**境界防御的な古い考え方を前提とした対策に陥っている**状況がうかがえる。

- **年間調剤件数が30万～100万件未満の中規模層はIT事業者とのセキュリティ面含めた契約率、IT事業者とのリスクコミュニケーション率も他と比較して高く、そのため業者への信頼度も高い**。
- 他方で、100万件以上の大規模層では契約率は層別でもっとも低いが、**リスクコミュニケーション率は相応に高く、そのため、業者への信頼度も4割強には及んでいる**。**契約締結率にかかわらず、どの層もIT事業者への信頼度が全体的かつ共通的に高いことがこの分野の特徴と言える。**

＜アンケート調査結果_年間調剤件数別(1/7)＞

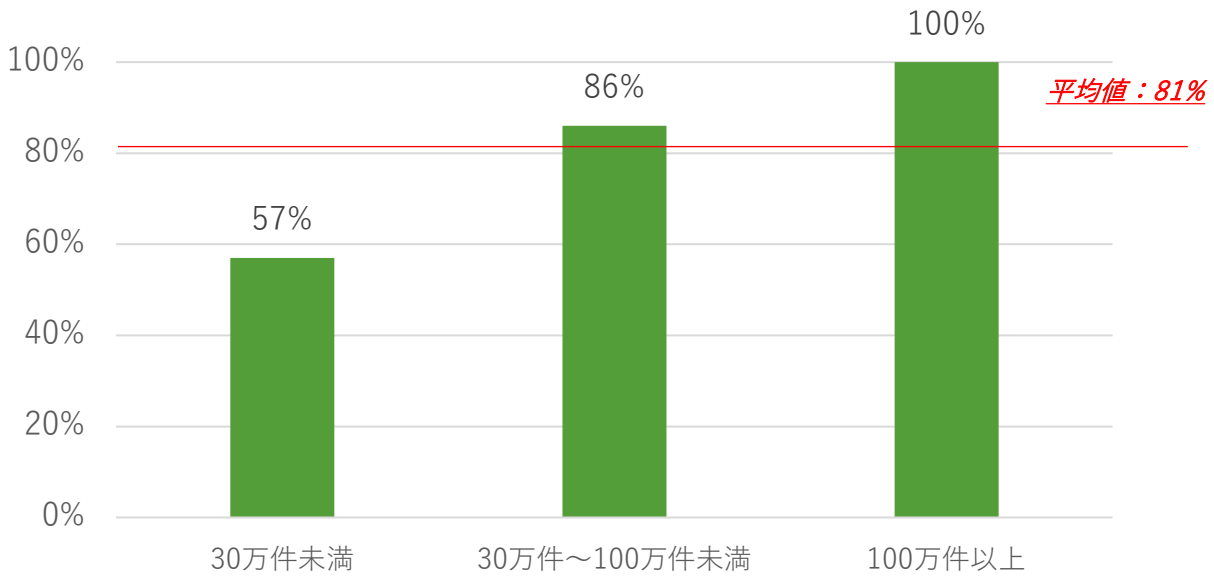
【ITの利用形態】

＜①：ITの利用形態（件数）＞　※N＝81



【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＝81

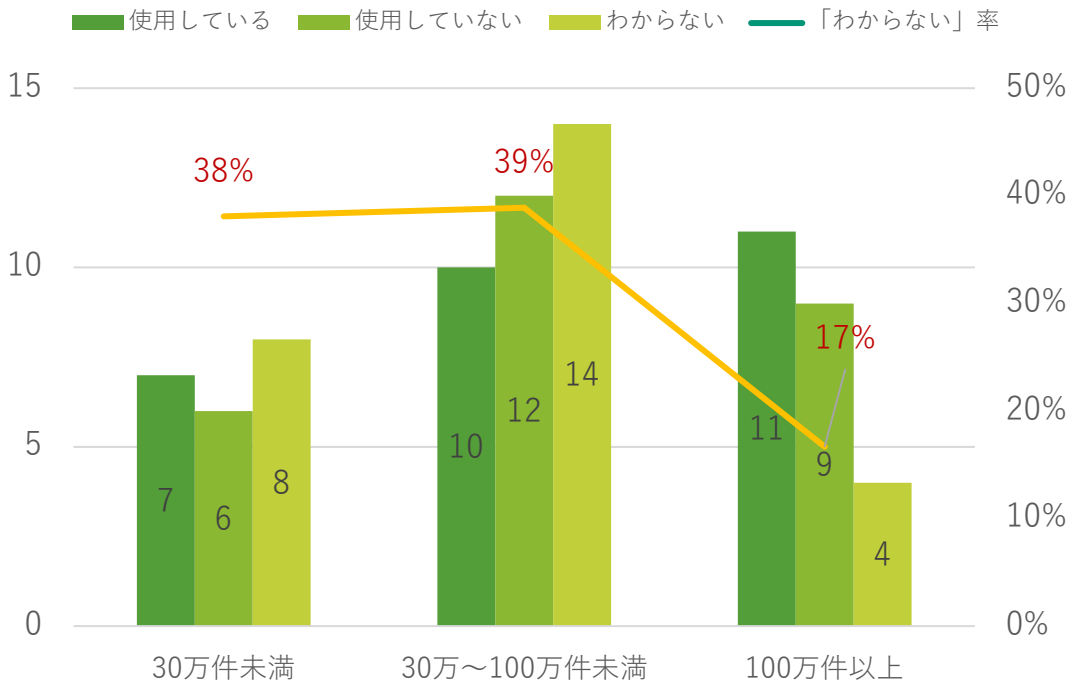


オンライン資格確認との連携も含めた、インターネット接続度はいずれの層も高い。
なお、**サイバー攻撃への脅威感度は年間調剤件数に応じて高まるが、特に30万件未満（小調剤規模）の層は低い傾向**がある。

＜アンケート調査結果_年間調剤件数別(2/7)＞

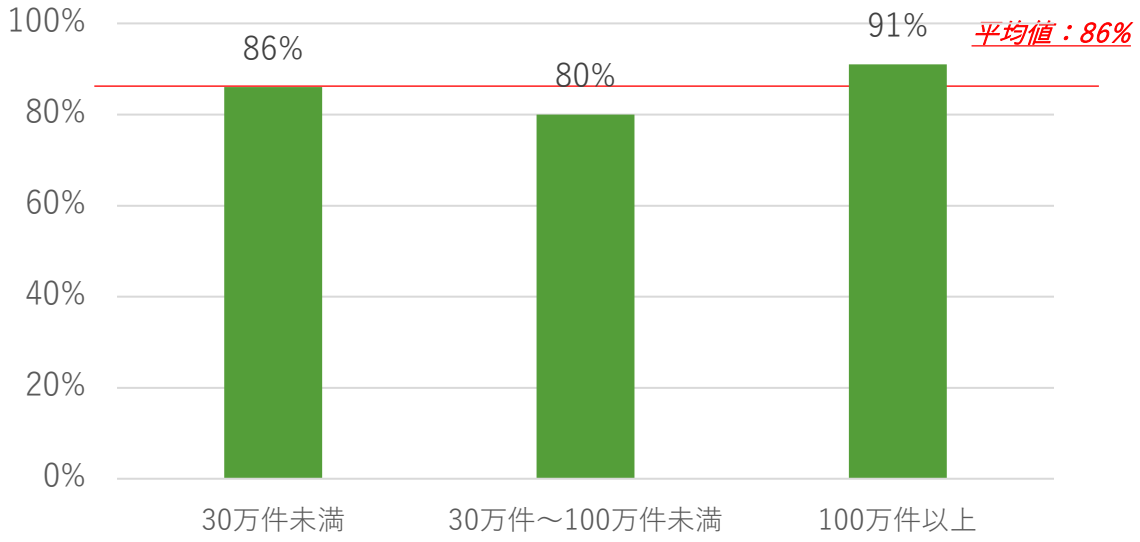
【脆弱性対策】

＜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＝81



＜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＝28



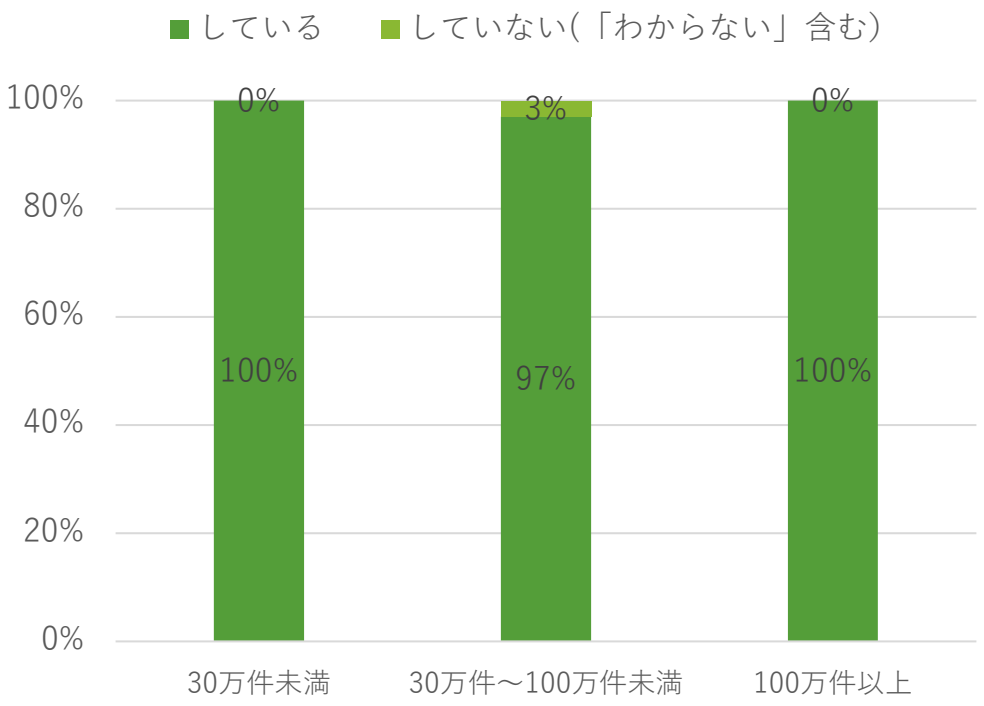
※＜⑤：脆弱性対応未了の理由＞は1件のみが該当するため調査省略

年間調剤件数が多いほどVPN機器種別の未把握率（「わからない」率」は低い。
ただし、**脆弱性対応率は中調剤規模施設（30万～100万件未満）が相対的にもっとも低い。**

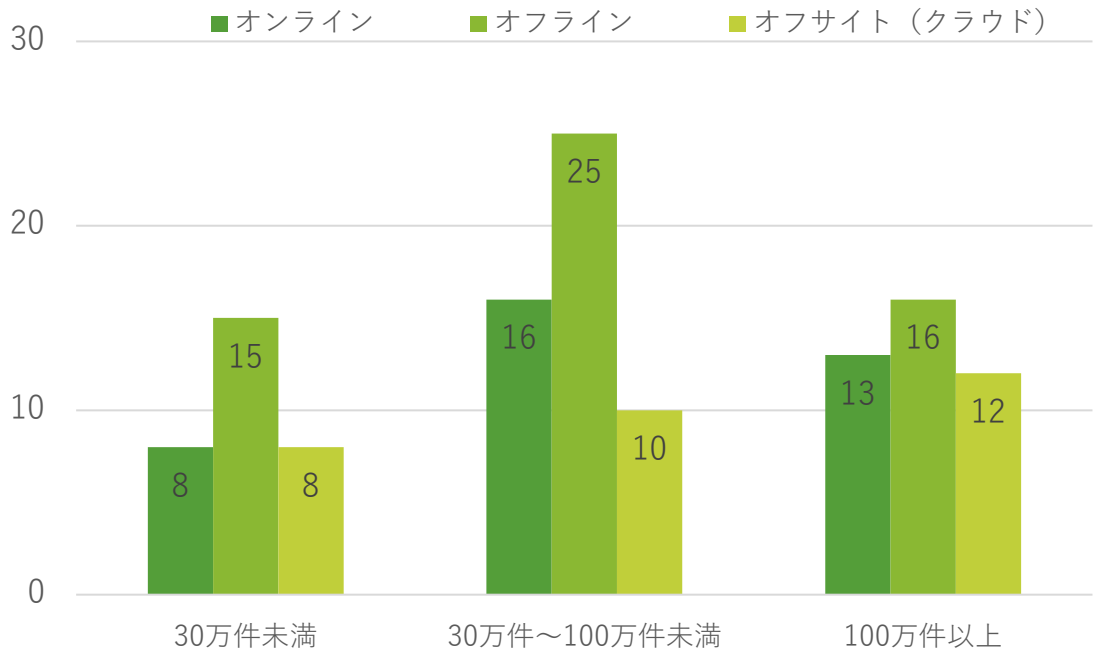
＜アンケート調査結果_年間調剤件数別(3/7)＞

【バックアップ対策】

＜⑥-1：バックアップの取得率＞ ※N＝81



＜⑥-2：バックアップの取得方式（件数：複数選択式）＞ ※N＝80



バックアップ取得率はすべての年間調剤規模において共通的に極めて高い。
さらに**どの層においてもオンラインより、オフライン取得率が高いという特徴**が示されている。

＜アンケート調査結果_年間調剤件数別(4/7)＞

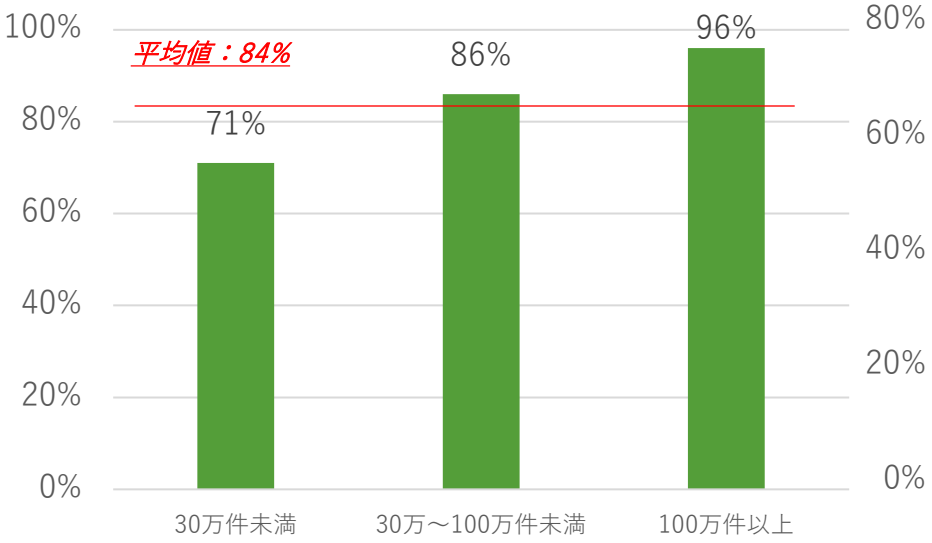
【IT人材】 ※N＝81

＜⑦：IT人材数＞

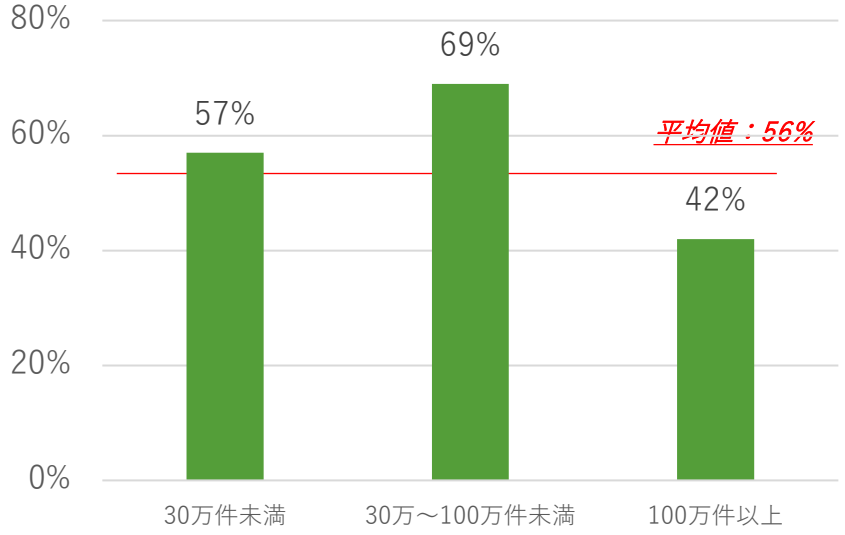
年間調剤件数	施設内システム担当者	うち、常勤数	常勤率
30万件未満	4.0人	4.0人	100%
30万～100万件未満	2.8人	2.2人	78%
100万件以上	11.3人	10.7人	95%

【監査】 ※N＝81

＜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＞

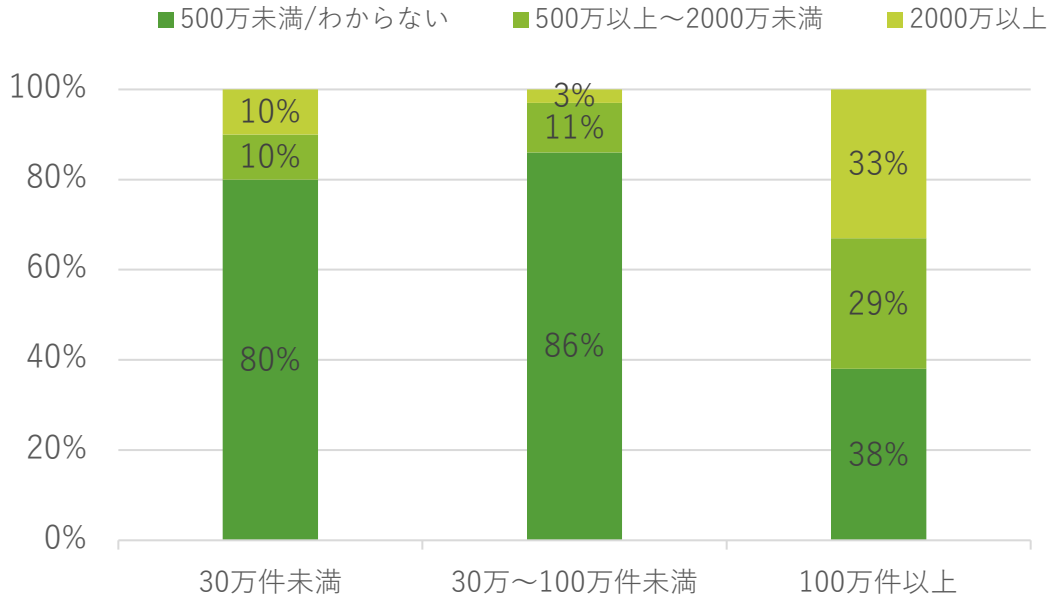


100万件以上の大規模層は他と比較して突出してIT担当者が多いことが分かる。これらの施設は厚労省安全管理GLの把握率やセキュリティ監査実施も高いが、**相対的に、中規模層（30万～100万件未満）ではセキュリティ監査未実施率が低い**状況である。

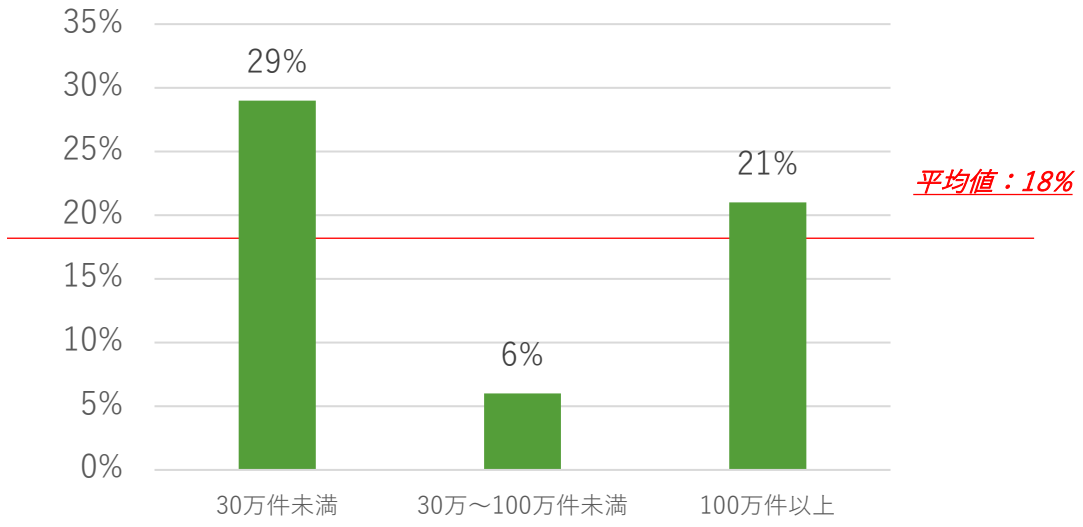
＜アンケート調査結果_年間調剤件数別(5/7)＞

【セキュリティ予算】 ※N＝81

＜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＞

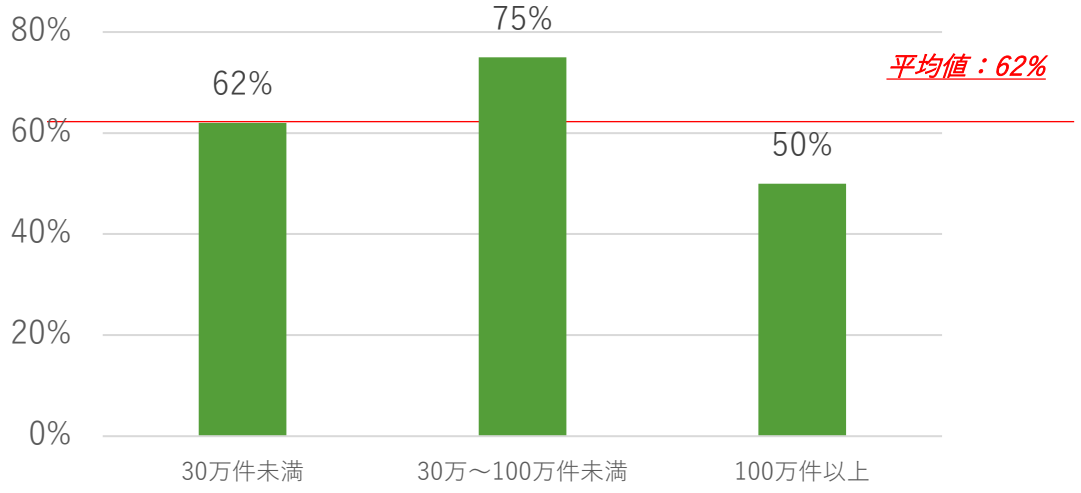


100万件以上の大規模層ではセキュリティ予算が500万以上の割合が高く、2000万以上確保の施設も3割強近くに及んでいる。
一方、セキュリティ予算が十分と回答した施設は30万～100万件未満の中規模層が最も低いが、これらの層も1割強は500万以上のセキュリティ予算を確保していることから、**小規模/大規模の中間に位置する層として、IT規模に応じたセキュリティ施策に苦心していることがわかる。**

＜アンケート調査結果_年間調剤件数別(6/7)＞

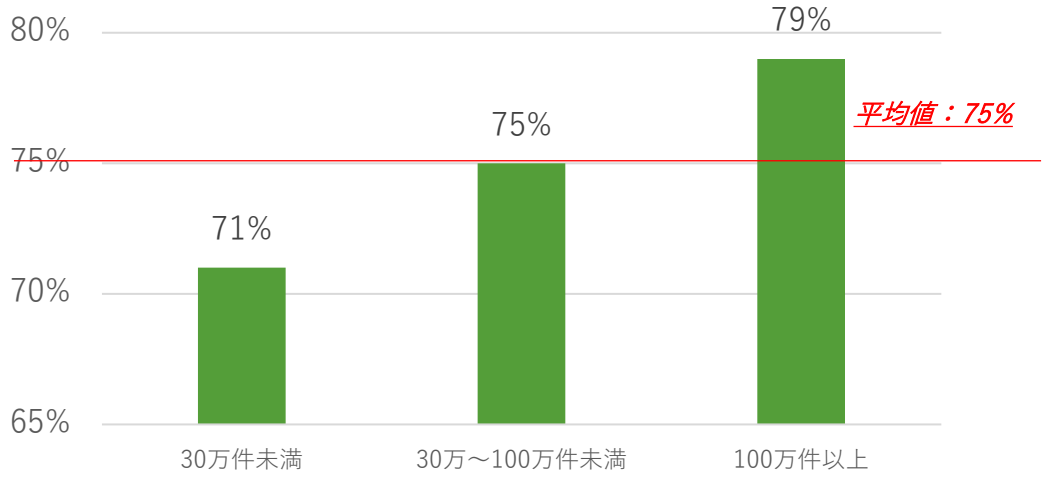
【サイバー保険】 ※N＝81

＜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＝81

＜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＞

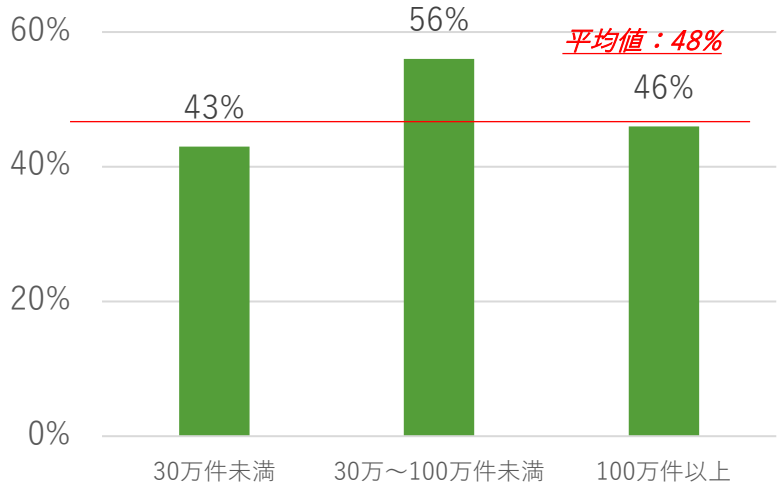


サイバー保険の未加入率は30万～100万未満の中規模層が高く、**IT規模の拡大に伴うセキュリティへの踏み込みに躊躇する中規模施設の悩みが浮き彫り**になっている。一方で、診療系NWのクローズド神話への共感率は大規模層（100万件以上）が最も高いことから、セキュリティ予算を確保しているが**境界防御的な古い考え方を前提とした対策に陥っている**状況がうかがえる。

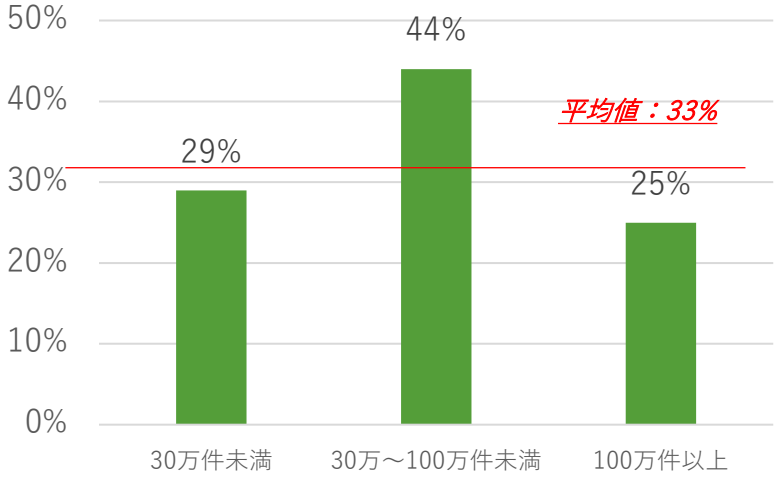
＜アンケート調査結果_年間調剤件数別(7/7)＞

【システム提供事業者とのコミュニケーション状況】 ※N＝81

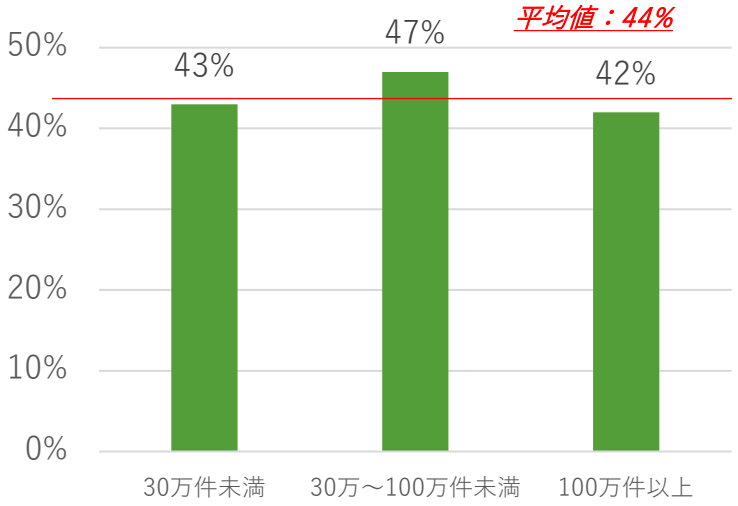
＜⑭：IT事業者によるセキュリティ対策の「指示を受けている」と回答した施設割合＞



＜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＞



年間調剤件数が30万～100万件未満の中規模層はIT事業者とのセキュリティ面含めた契約率、IT事業者とのリスクコミュニケーション率も他と比較して高く、そのため業者への信頼度も高い。
他方で、100万件以上の大規模層では契約率は層別でもっとも低いが、**リスクコミュニケーション率は相応に高く、そのため、業者への信頼度も4割強には及んでいる。**
契約締結率にかかわらず、どの層もIT事業者への信頼度が全体的かつ共通的に高いことがこの分野の特徴と言える。

４．運営薬局件数別結果

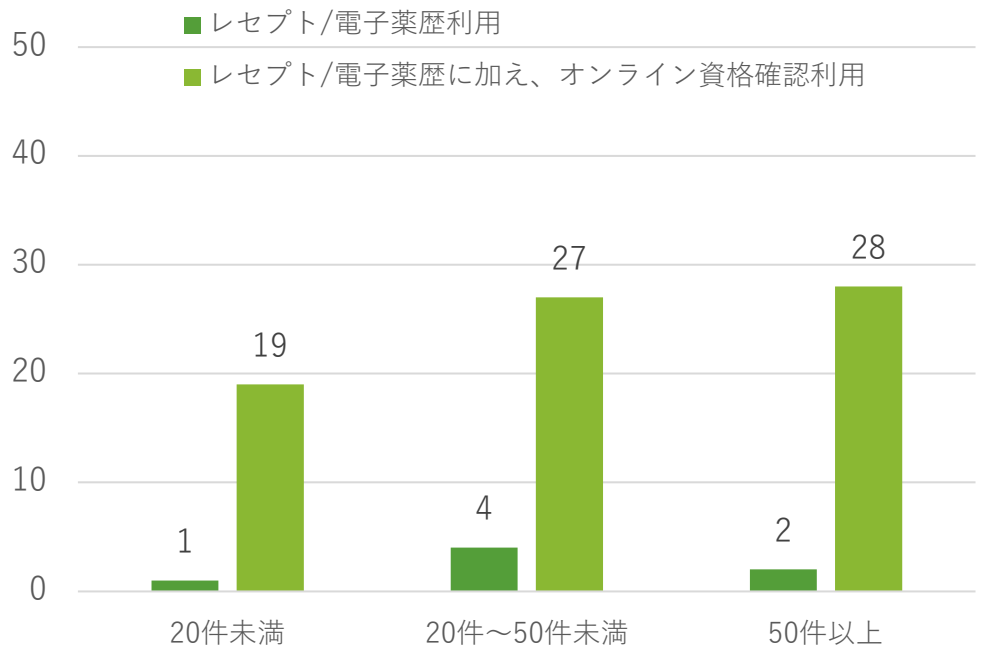
＜アンケート調査結果総評_運営薬局件数別＞

- 運営薬局件数別（20件未満/20件～50件未満/50件以上という3層）でみると、オンライン資格確認というインターネットとの接続度はどの層も高いが、**特に20件未満（小規模）の薬局運営施設ほどサイバー脅威への感度が低い。**
- **薬局運営規模に応じてVPN機器種別の把握率は高まる傾向**があるが、脆弱性対応率は**相対的に20件～50件未満の層が低い**状況である。
- 薬局運営規模にかかわらずバックアップ取得率は高く、**オンラインに対するオフラインバックアップ取得率も全体的に高い状**況である。
- **特に50件以上の大規模薬局層ではIT担当者数が多い**傾向がある**。厚労省安全管理GLの把握率/セキュリティ監査実施率も運営薬局数に応じて高くなる基本傾向**がある。
- **50件以上の運営薬局層（大規模層）は5割弱が500万以上のセキュリティ予算を確保**している一方で、20件未満の小規模層は、 25%以上が500万以上の予算確保を出来ている一方で、**セキュリティ予算に不満を特に強く持っている**ことがうかがえる。
- サイバー保険未加入率は20件～50件未満の中規模層（セキュリティ予算への満足度が最も低い層）が一番高く、**この層は特にサイバー保険へのコスト拠出が困難である**ことが見受けられる。ただし、**クローズドNWの安全神話への共感割合はどの層も共通的に高い**状況である。
- 運営薬局数の多い50件以上（大規模）の層が最もIT事業者とのリスクコミュニケーション率（指示を受けている率）/セキュリティ面を含めた契約率が低く、一方で事業者への信頼度は全体的に高い状況であり、**潤沢なIT人材のもとでベンダ依存でないセキュリティ管理への取組が出来ている**ことが見て取れる。
- それ以外の層でも契約率はコミュニケーション率を下回っているが、**セキュリティ予算面の十分性やIT人材数を考慮し、大規模層と比較した場合、ベンダ独立的なセキュリティ対策が実施できているかには不安が残る**といえる。

＜アンケート調査結果_運営薬局件数別(1/7)＞

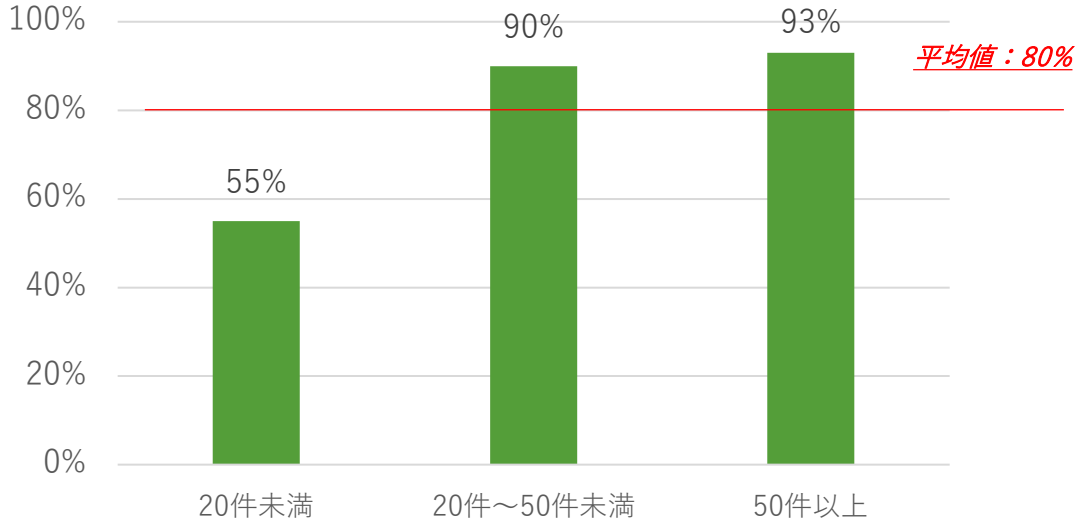
【ITの利用形態】

＜①：ITの利用形態(件数）＞　※N＝81



【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＝81



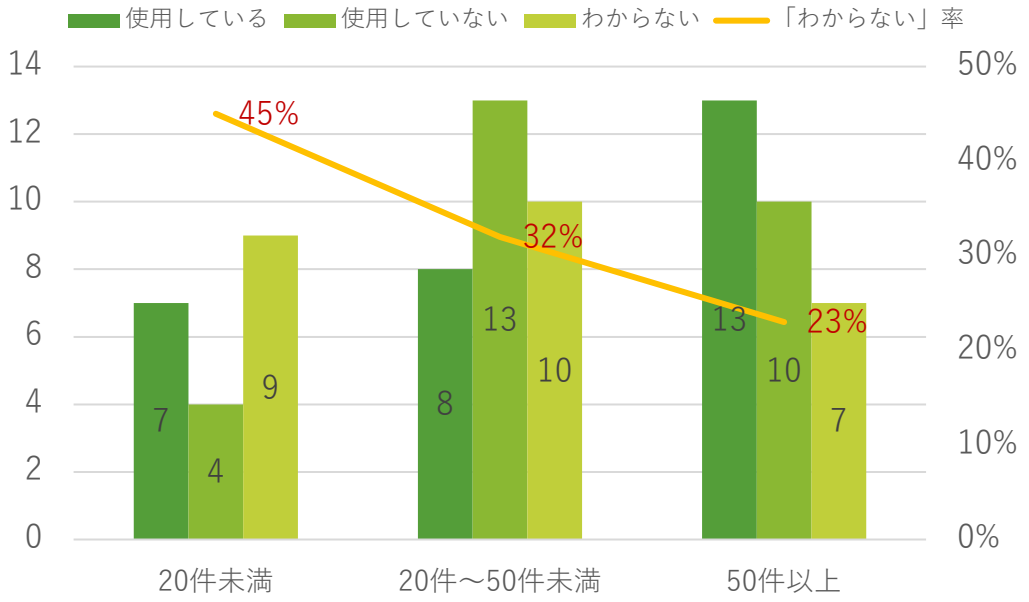
オンライン資格確認というインターネットとの接続度はどの層も高いが、**特に20件未満（小規模）の薬局運営施設ほどサイバー脅威への感度が低い。**

＜アンケート調査結果_運営薬局件数別(2/7)＞

【脆弱性対策】

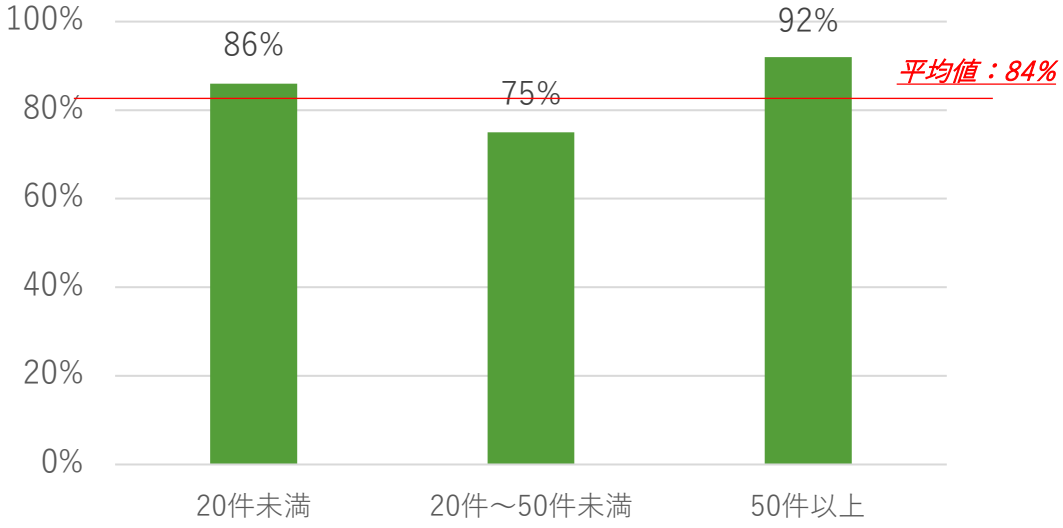
＜③：厚労省等から脆弱性が指摘されたForitnet社製VPN機器を使用している施設件数＞

※N＝81



＜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＝28



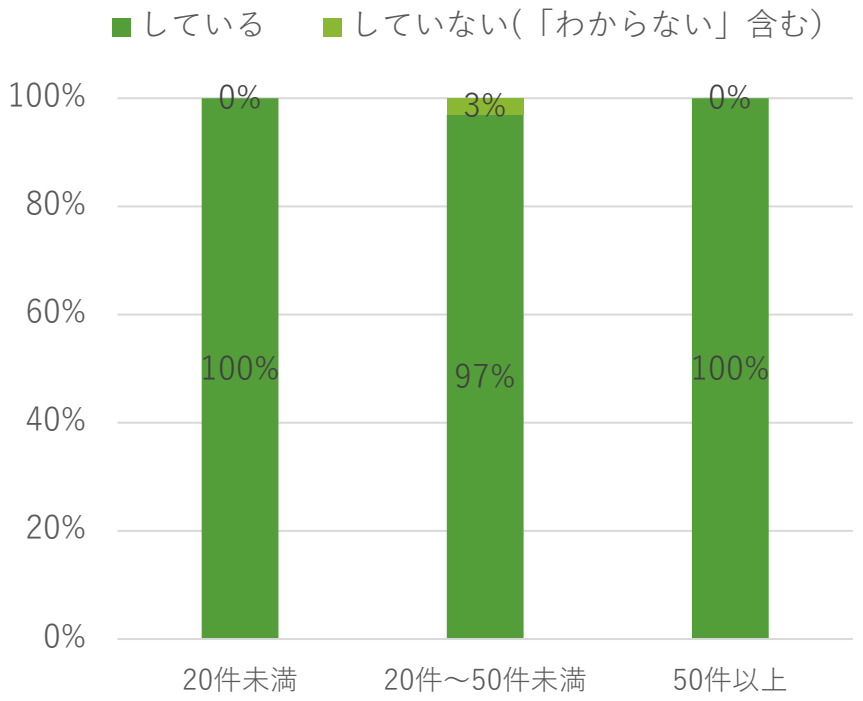
※＜⑤：脆弱性対応未了の理由＞は1件のみのため調査省略

薬局運営規模に応じてVPN機器種別の把握率は高まる傾向があるが、
脆弱性対応率は**相対的に20件～50件未満の層が低い**状況である。

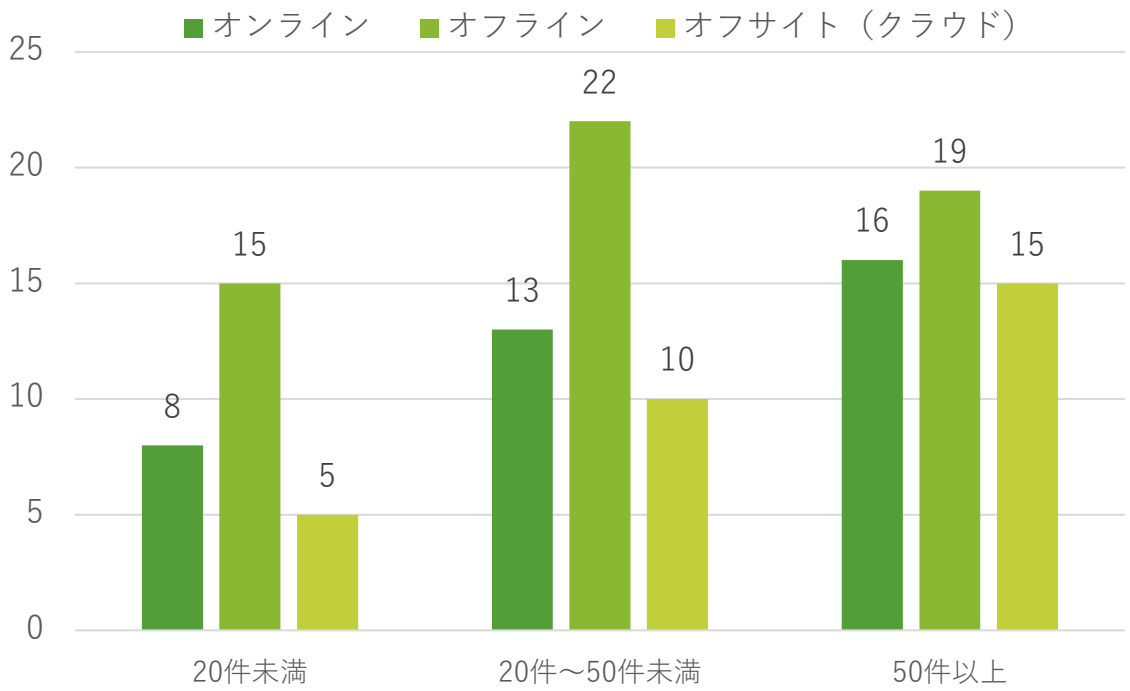
＜アンケート調査結果_運営薬局件数別(3/7)＞

【バックアップ対策】

<⑥-1：バックアップの取得率＞ ※N＝81



<⑥-2：バックアップの取得方式(複数選択式）＞ ※N＝80



薬局運営規模にかかわらずバックアップ取得率は高く、**オンラインに対するオフラインバックアップ取得率も全体的に高い状**況である。

＜アンケート調査結果_運営薬局件数別(4/7)＞

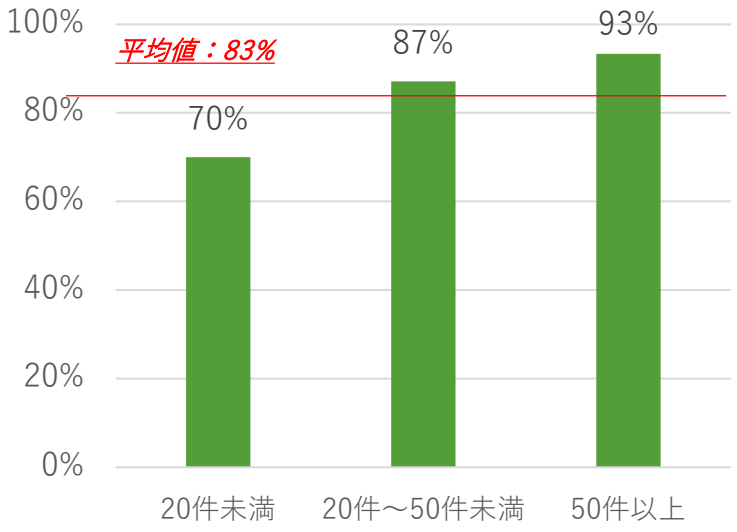
【IT人材】 ※N＝81

＜⑦：IT人材数＞

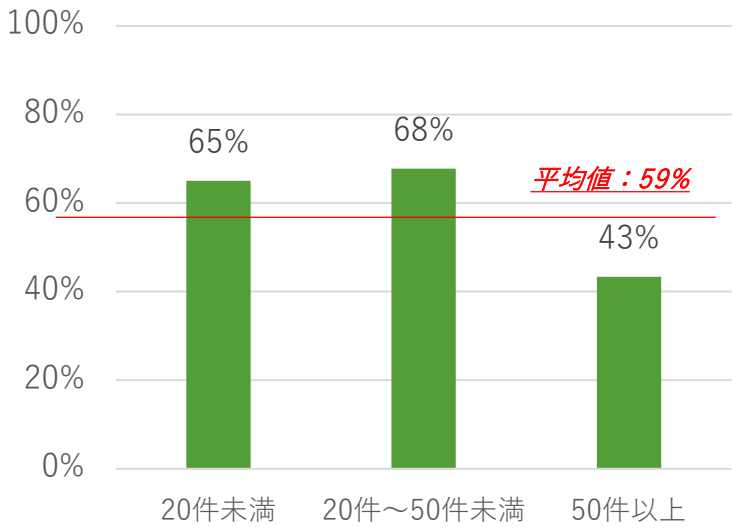
運営薬局件数	施設内システム担当者	うち、常勤数	常勤率
20件未満	4.1人	4.0人	99%
20件～50件未満	1.9人	1.9人	97%
50件以上	10.5人	9.4人	89%

【監査】 ※N＝81

＜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＞

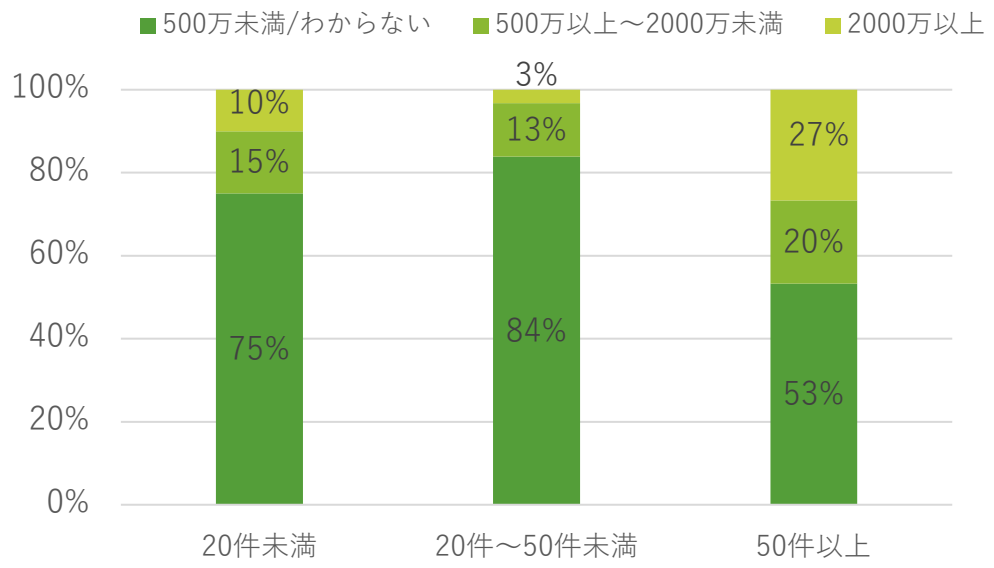


特に50件以上の大規模薬局層ではIT担当者数が多い傾向がある。
厚労省安全管理GLの把握率/セキュリティ監査実施率も運営薬局数に応じて高くなる基本傾向がある。

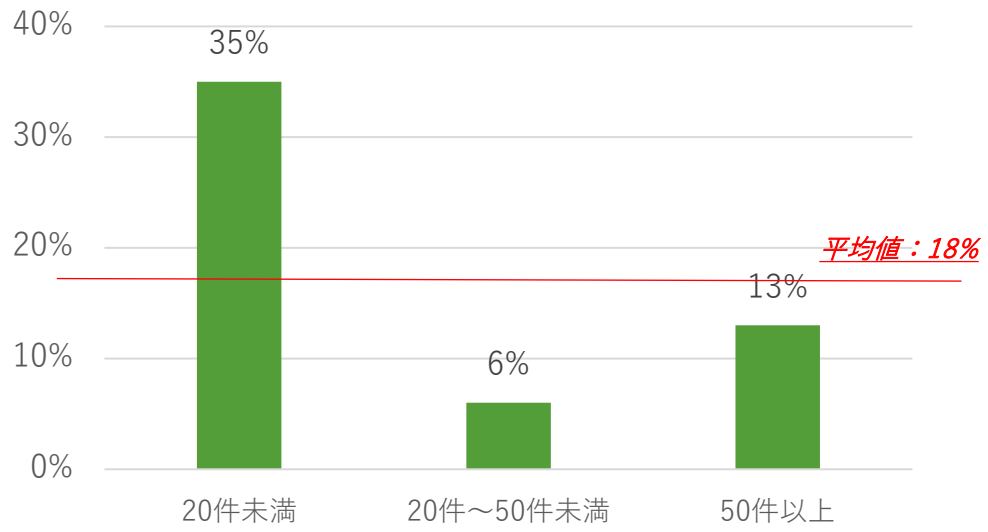
＜アンケート調査結果_運営薬局件数別(5/7)＞

【セキュリティ予算】 ※N＝81

＜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＞

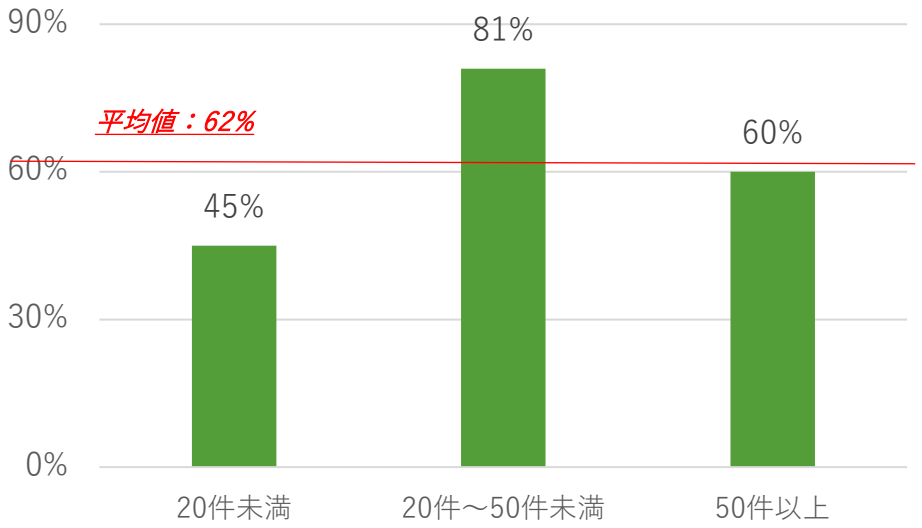


<u>50件以上の運営薬局層（大規模層）は5割弱が500万以上のセキュリティ予算を確保</u>している一方で、20件未満の小規模層は、25%以上が500万以上の予算確保を出来ている一方で、**<u>セキュリティ予算に不満を特に強く持っている</u>**ことがうかがえる。

＜アンケート調査結果_運営薬局件数別(6/7)＞

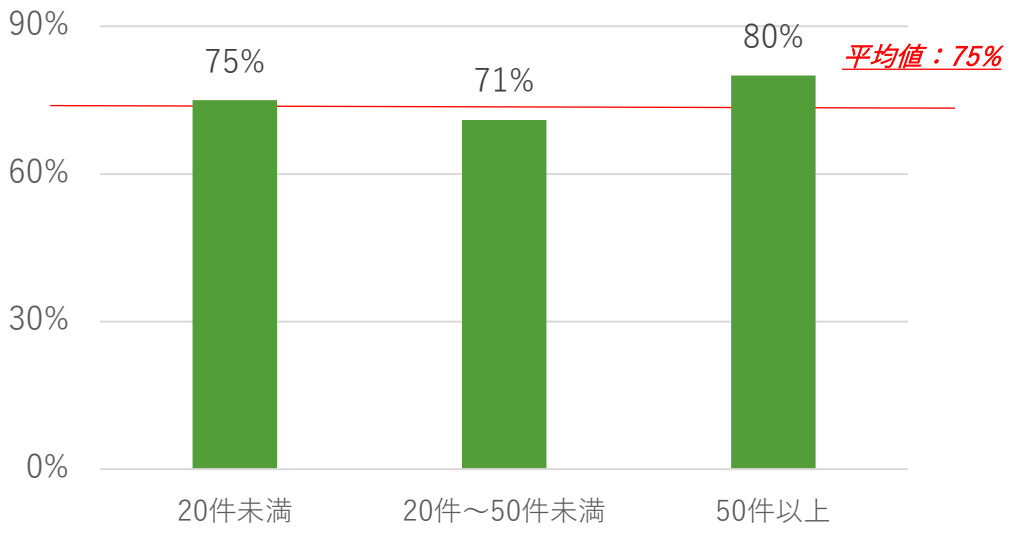
【サイバー保険】 ※N＝81

＜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＝81

＜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＞

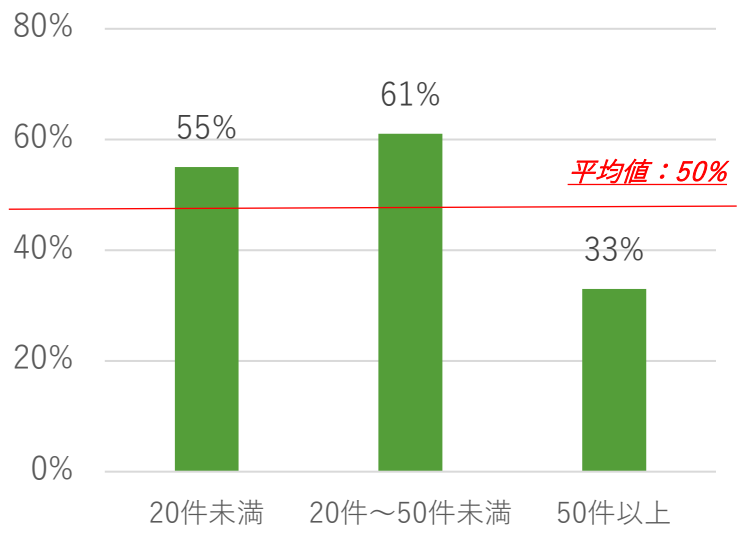


サイバー保険未加入率は20件～50件未満の中規模層（セキュリティ予算への満足度が最も低い層）が一番高く、**この層は特にサイバー保険へのコスト拠出が困難である**ことが見受けられる。ただし、**クローズドNWの安全神話への共感割合はどの層も共通的に高い**状況である。

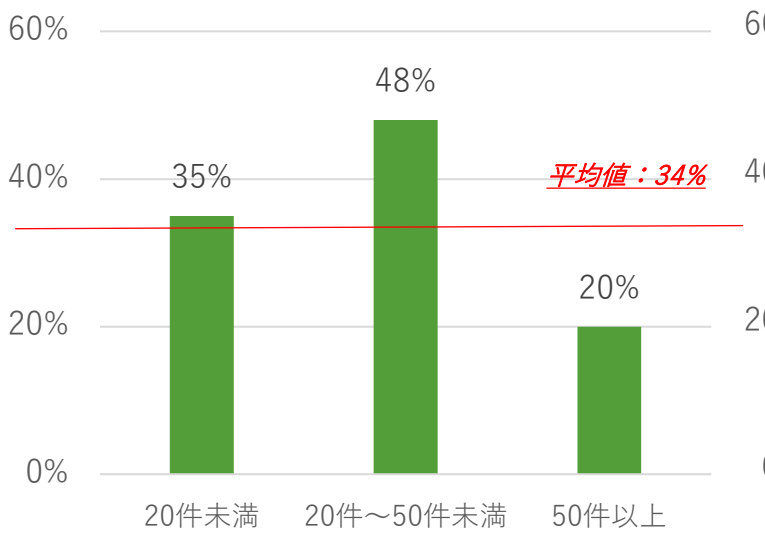
＜アンケート調査結果_運営薬局件数別(7/7)＞

【システム提供事業者とのコミュニケーション状況】 ※N＝81

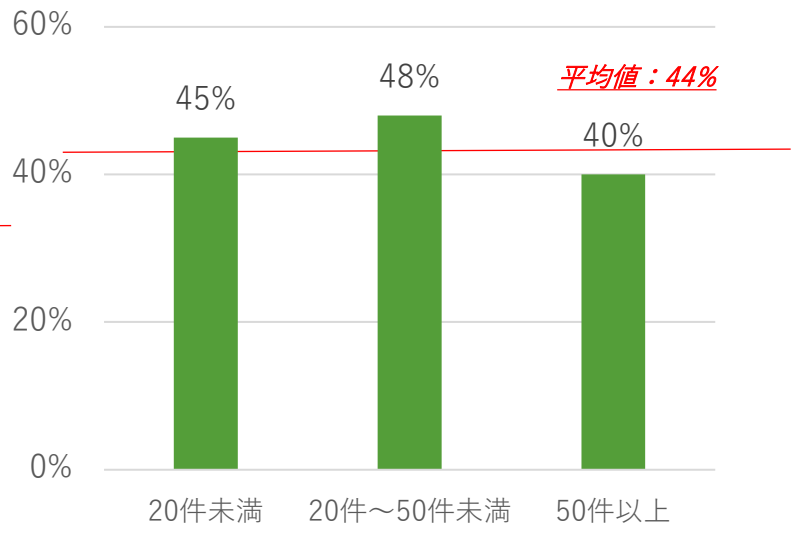
＜⑭：IT事業者によるセキュリティ対策の「指示を受けている」と回答した施設割合＞



＜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＞



運営薬局数の多い50件以上（大規模）の層が最もIT事業者とのリスクコミュニケーション率（指示を受けている率）/セキュリティ面を含めた契約率が低く、一方で事業者への信頼度は全体的に高い状況であり、**潤沢なIT人材のもとでベンダ依存でないセキュリティ管理への取組が出来ている**ことが見て取れる。
それ以外の層でも契約率はコミュニケーション率を下回っているが、**セキュリティ予算面の十分性やIT人材数を考慮し、大規模層と比較した場合、ベンダ独立的なセキュリティ対策が実施できているかには不安が残る**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＞

- 調査対象薬局におけるIT利用環境別（「オンラインレセプトシステムのみを利用している」、「オンラインレセプトシステムに加え、電子薬歴管理システムを利用している」、「 オンラインレセプト/電子薬歴管理システムに加え、保険証のオンライン資格確認とも情報連携している」、「 紙情報で管理している 」という4層）にみると、今回のアンケート回答組織には、 「オンラインレセプトシステムのみを利用している」、 「 紙情報で管理している」に該当する施設は存在しなかった。
- そのため、 「オンラインレセプトシステムに加え、電子薬歴管理システムを利用している」**（レセ/電子薬歴利用）**、「 オンラインレセプト/電子薬歴管理システムに加え、保険証のオンライン資格確認とも情報連携している」**（レセ/電子薬歴利用＋オン資利用）**という2つの層で調査を行った。

- **保険証等のオンライン資格確認（オン資）との連携といった、インターネットとの接続環境を業務上有する施設ほど、サイバー攻撃への脅威感度は高い**

- VPN機器種別の把握率はほぼ変わらないが、**インターネット接続度の高いオン資利用施設ほど脆弱性対応の完了率は高い**。

- **オンライン資格確認利用施設では、オフラインバックアップ取得率が高い**

- 施設内のIT人材における厚労省GLの把握率、セキュリティ監査の実施率自体等、**セキュリティ成熟度にほぼ差はない**が、（一部の外れ値を除いた）レセ/電子薬歴のみ利用施設層/オン資も利用している施設層を比較すると、**後者のほうがIT担当者の配置数が多い傾向**がある。

- **オン資利用施設層は500万以上のセキュリティ予算を確保する施設が3割強**に及ぶが、**オン資未利用施設層では全ての施設で該当予算が500万以下**との回答であった。そのため、**オン資未利用施設ではセキュリティ予算が十分と回答した施設はゼロ件**である。

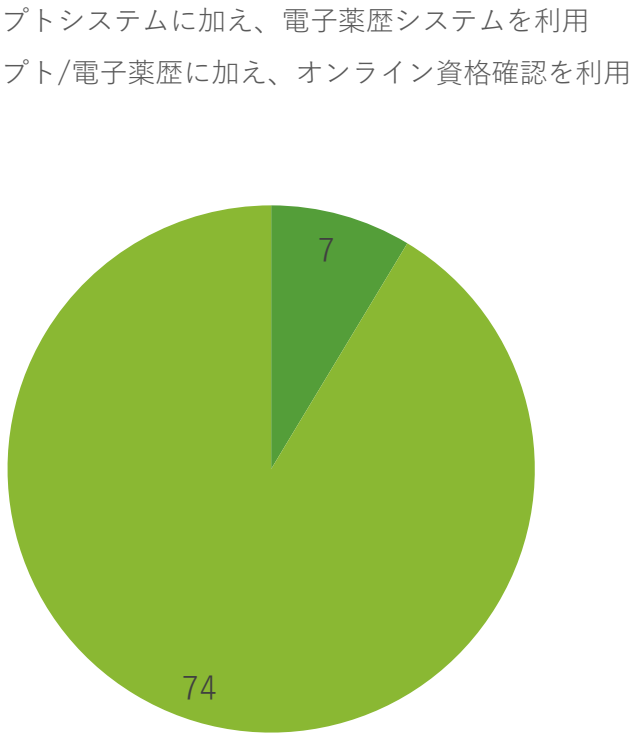
- オン資未利用施設層ではサイバー保険の加入施設はゼロであり、さらに診療系NWはクローズドなため安心であるという考え方への共感率（共感/部分共感）は100%に至っている。**こうした施設層ではセキュリティ予算が不十分であるため、保険加入も困難であり、そのため無意識的に古い安全神話へ依拠せざるを得ない構造が浮き彫り**になっている。一方、インターネットとの接点を業務上有さざるを得ない**オン資利用施設層でも7割強はそうした考え方**を持っており、**薬局分野でも根拠のない安全神話の根深さが示されている**。

- オン資利用有無にかかわらず、IT業者によるユーザセキュリティ確認を行っている施設群のうち、**15%前後は、セキュリティ面の契約を行っていない状況**である。他方、オン資未利用施設層は、利用施設層と比較すると、ユーザセキュリティ確認率/契約率/事業者への信頼率も高い。この事実は、オン資というインターネットとの接続を明示的に前提とする、**新しい薬局IT環境において、業者とのセキュリティコミュニケーションを通して適切な安全管理水準を維持する取組に踏み込めないオン資利用施設が一定数は存在する**ことを示しているともいえる。

＜アンケート調査結果_ IT利用環境別(1/7)＞

【ITの利用形態】

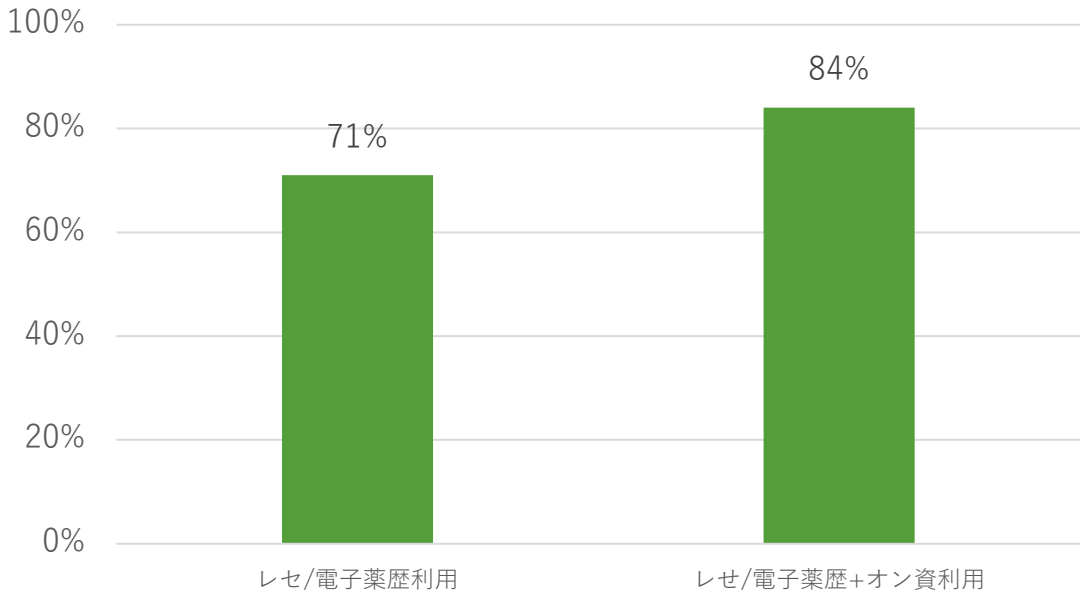
＜①：ITの利用形態(件数）＞　※N=81



※：「オンラインレセプトシステムのみ利用」「紙情報で管理」は0件

【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＝81



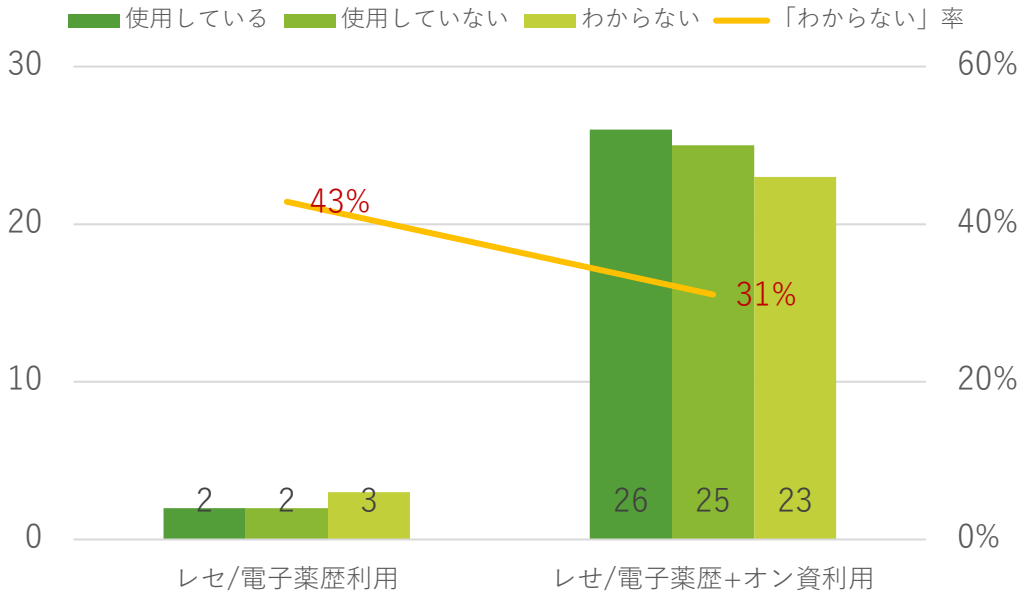
保険証等のオンライン資格確認（オン資）との連携といった、インターネットとの接続環境を業務上有する施設ほど、サイバー攻撃への脅威感度は高い

＜アンケート調査結果_ IT利用環境別(2/7)＞

【脆弱性対策】

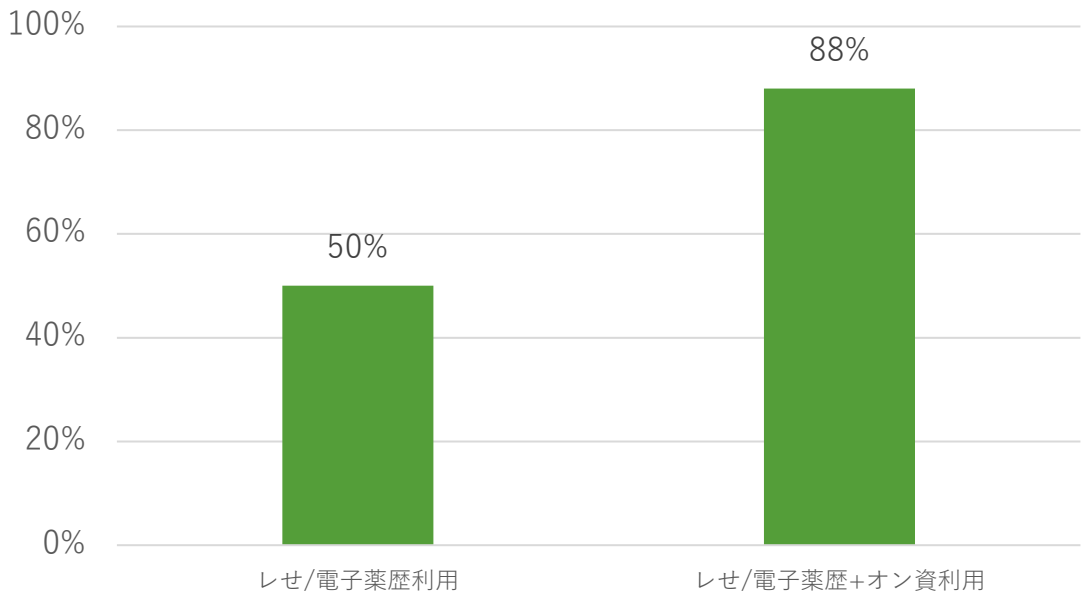
＜③：厚労省等から脆弱性が指摘されたForitnet社製VPN機器を使用している施設件数＞

※N＝81



＜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＝28



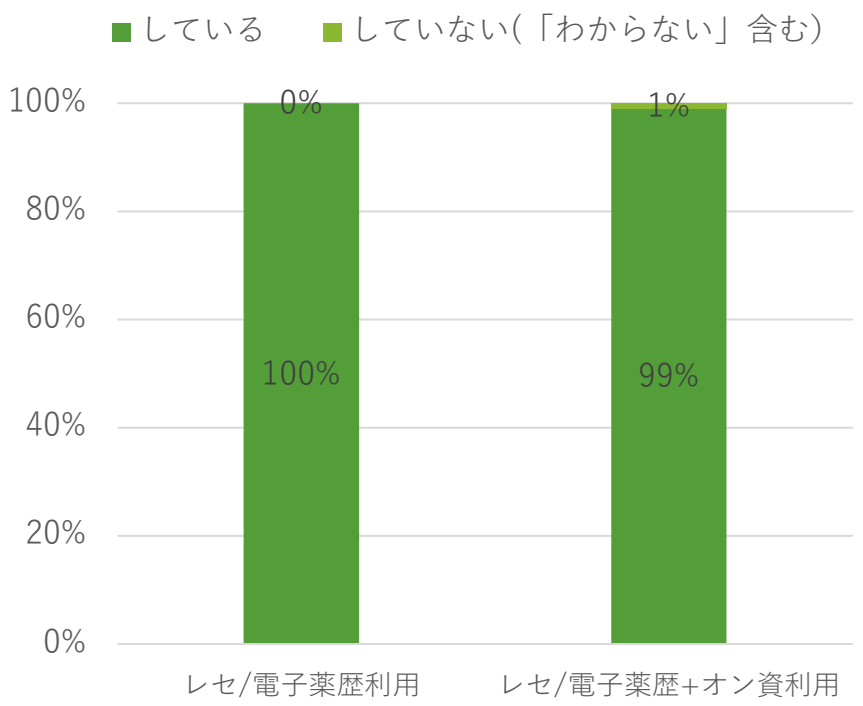
※＜⑤：脆弱性対応未了の理由＞は1件のみのため調査省略

IT利用環境別でみると、VPN機器種別の把握率はほぼ変わらないが、**インターネット接続度の高いオン資利用施設ほど脆弱性対応の完了率は高い**。

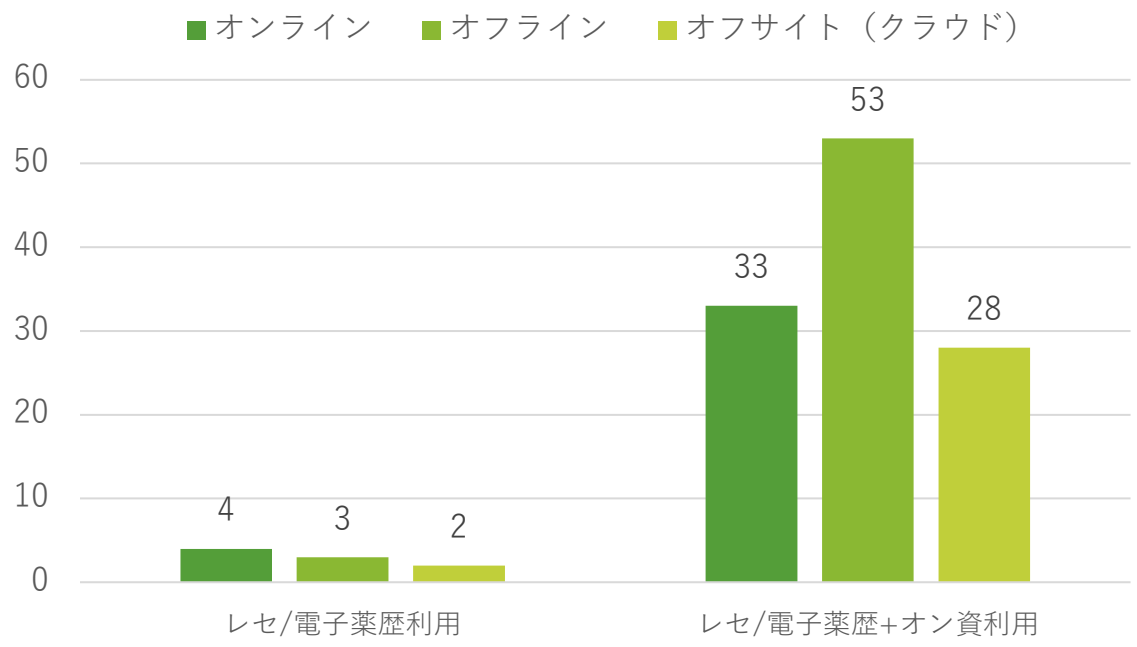
＜アンケート調査結果_ IT利用環境別（3/7）＞

【バックアップ対策】

＜⑥-1：バックアップの取得率＞ ※N＝81



＜⑥-2：バックアップの取得方式(件数/複数選択式）＞ ※N＝80



オンライン資格確認利用施設では、オフラインバックアップ取得率が高い

＜アンケート調査結果_ IT利用環境別(4/7)＞

【IT人材】 ※N＝81

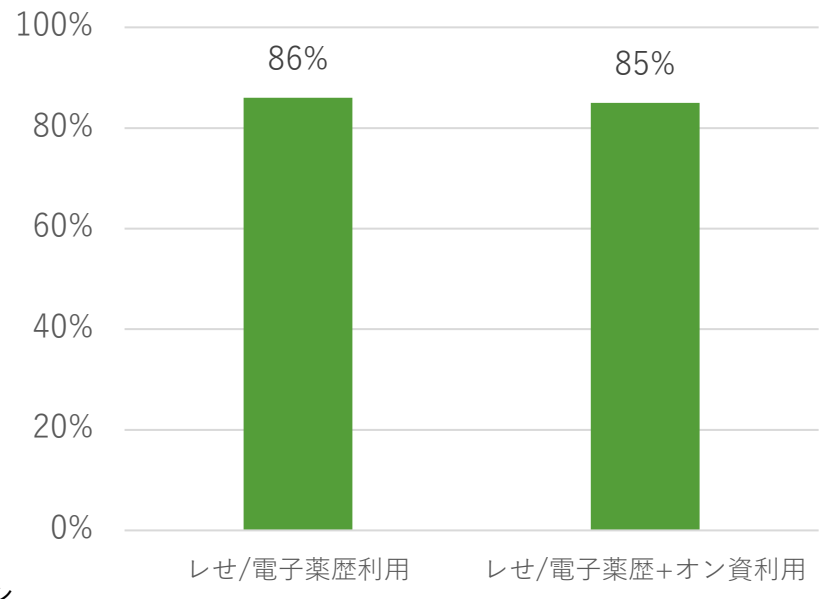
＜⑦：IT人材数＞

IT利用環境別		施設内システム担当者	うち、常勤数	常勤率
レセ/電子薬歴利用	全平均	5.7人	2.9人	50%
	外れ値除く平均（※）	**1.6人**	**1.6人**	**100%**
レセ/電子薬歴＋オン資利用	全平均	5.6人	5.4人	96%

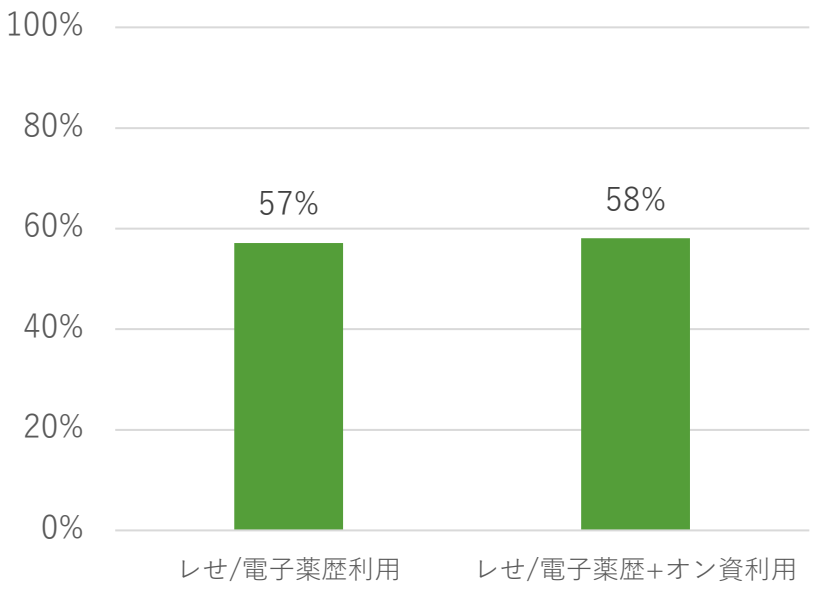
※：1件のサンプルの施設内システム担当者/常勤数が他サンプルと比較して著しく高かったため、そのサンプルを外れ値として除外した場合の平均値

【監査】 ※N＝81

＜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＞

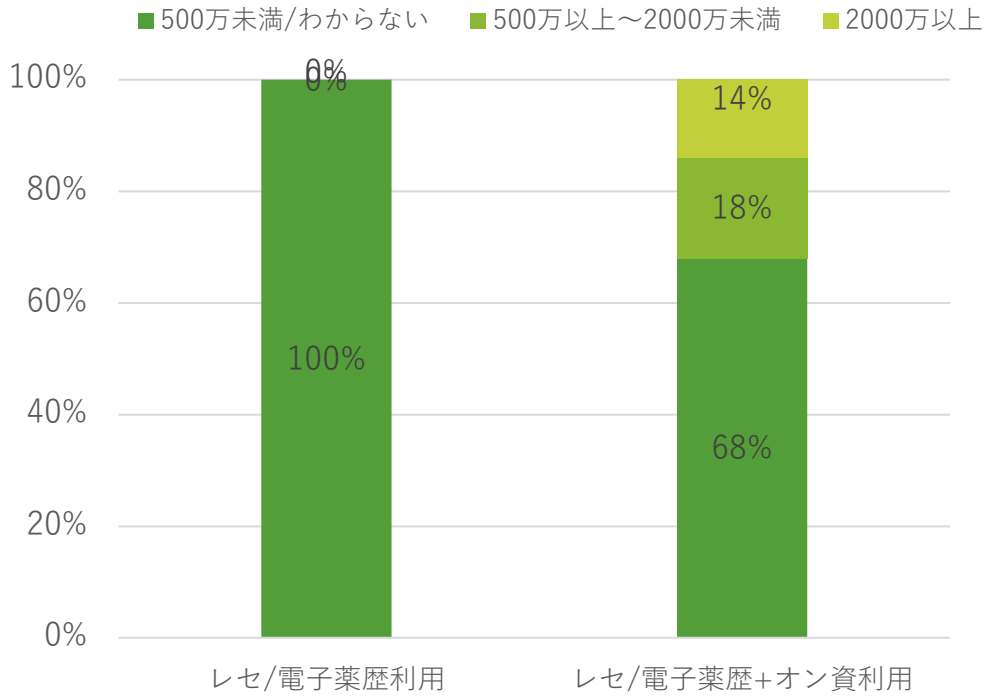


施設内のIT人材における厚労省GLの把握率、セキュリティ監査の実施率自体等、**セキュリティ成熟度にほぼ差はない**が、（一部の外れ値を除いた）レセ/電子薬歴のみ利用施設層/オン資も利用している施設層を比較すると、**後者のほうがIT担当者の配置数が多い傾向**がある。

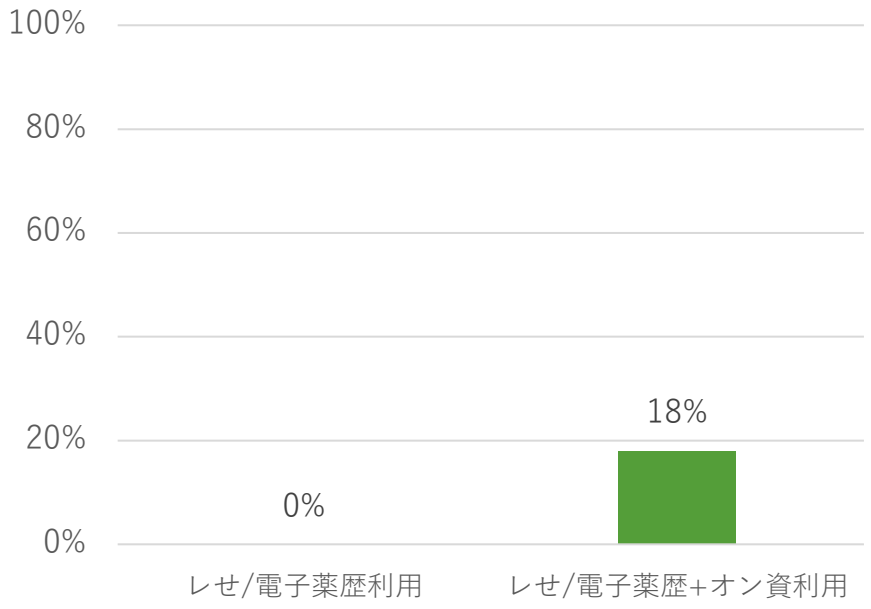
＜アンケート調査結果_ IT利用環境別(5/7)＞

【セキュリティ予算】 ※N＝81

＜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＞

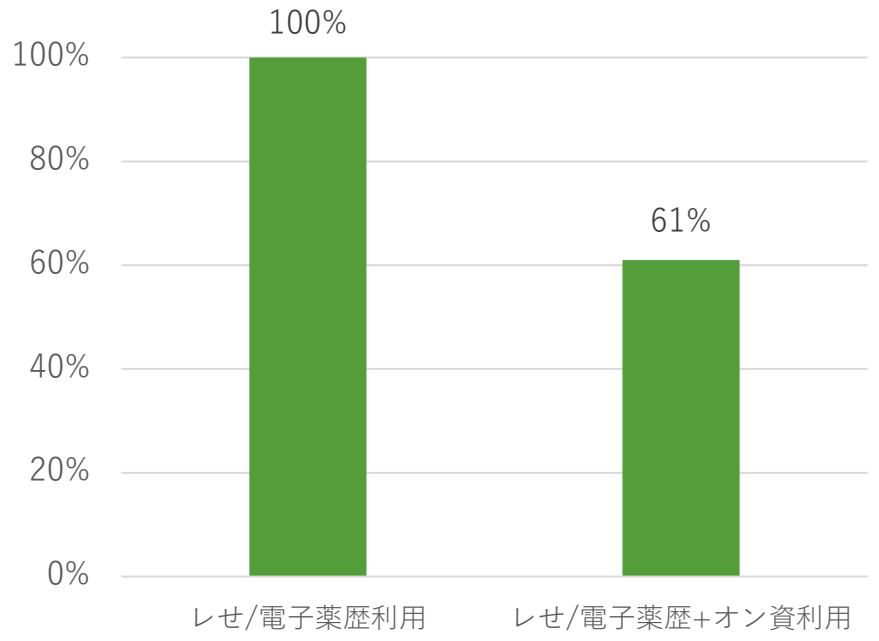


オン資利用施設層は500万以上のセキュリティ予算を確保する施設が3割強に及ぶが、**オン資未利用施設層では全ての施設で該当予算が500万以下**との回答であった。そのため、**オン資未利用施設ではセキュリティ予算が十分と回答した施設はゼロ件**である。

＜アンケート調査結果_ IT利用環境別(6/7)＞

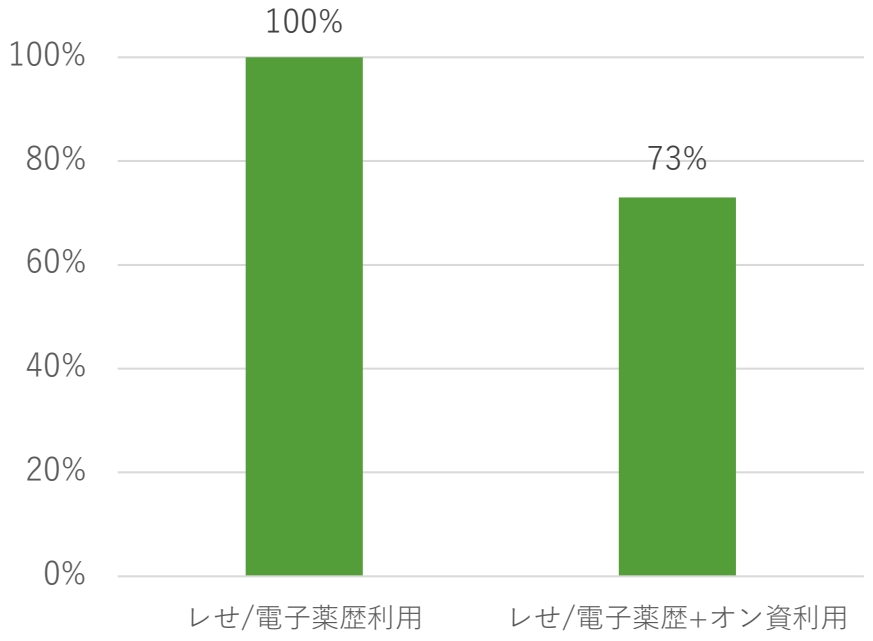
【サイバー保険】 ※N＝81

＜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＝81

＜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＞

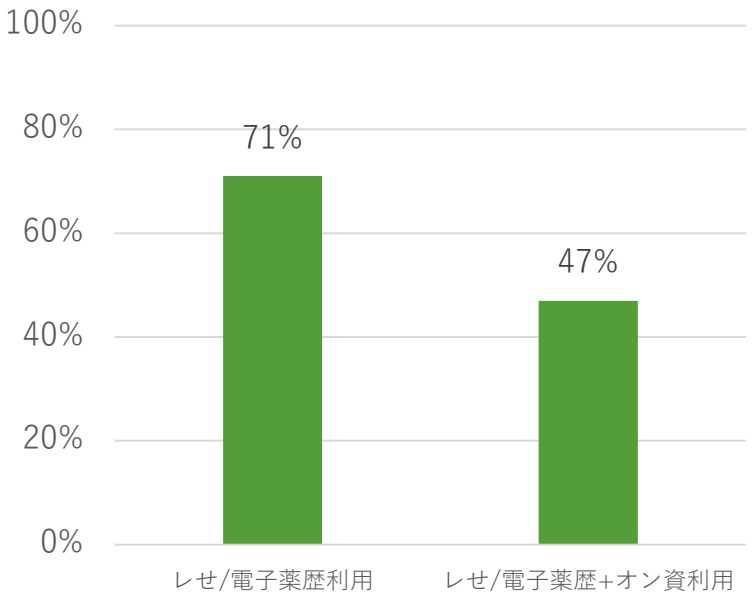


オン資未利用施設層ではサイバー保険の加入施設はゼロであり、さらに診療系NWはクローズドなため安心であるという考え方への共感率（共感/部分共感）は100%に至っている。**こうした施設層ではセキュリティ予算が不十分であるため、保険加入も困難であり、そのため無意識的に古い安全神話へ依拠せざるを得ない構造が浮き彫り**になっている。
一方、インターネットとの接点を業務上有さざるを得ない**オン資利用施設層でも7割強はそうした考え方**を持っており、**薬局分野でも根拠のない安全神話の根深さが示されている**。

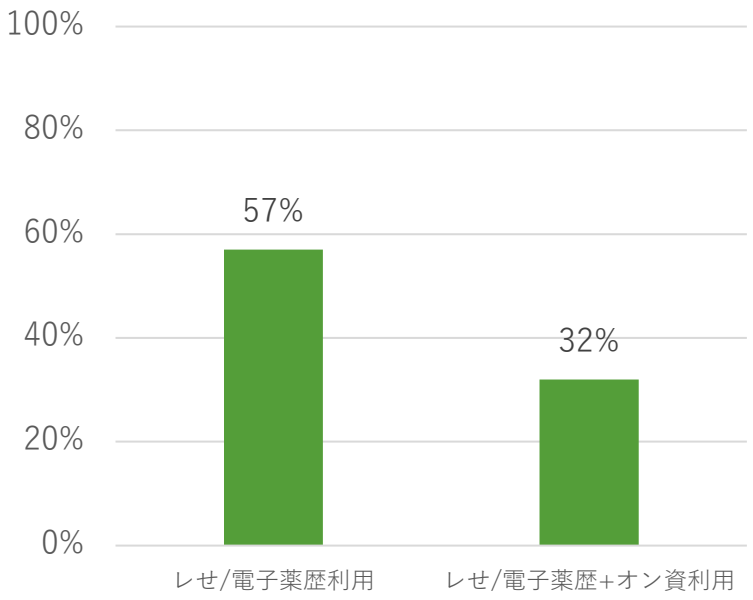
＜アンケート調査結果_ IT利用環境別(7/7)＞

【システム提供事業者とのコミュニケーション状況】 ※N＝81

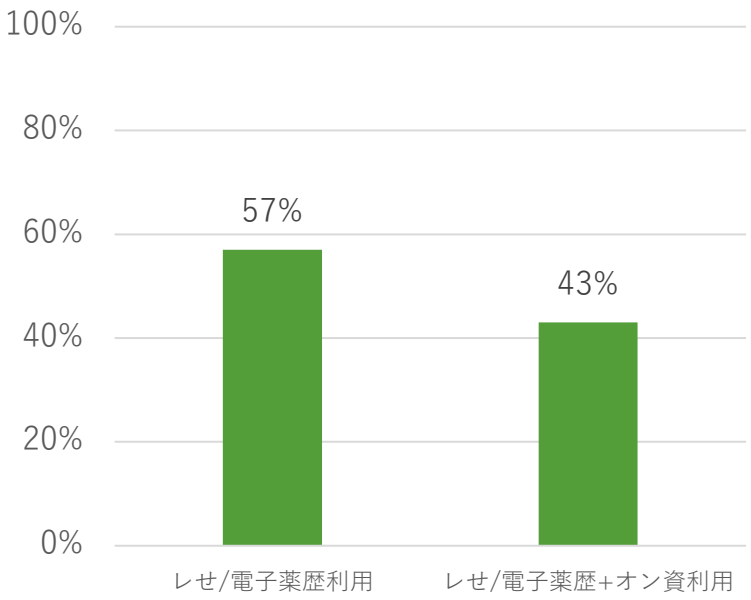
＜⑭：IT事業者によるセキュリティ対策の「指示を受けている」と回答した施設割合＞



＜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＞



オン資利用有無にかかわらず、IT業者によるユーザセキュリティ確認を行っている施設群のうち、**15%前後は、セキュリティ面の契約を行っていない状況**である。他方、オン資未利用施設層は、利用施設層と比較すると、ユーザセキュリティ確認率/契約率/事業者への信頼率も高い。この事実は、オン資というインターネットとの接続を明示的に前提とする、**新しい薬局IT環境において、業者とのセキュリティコミュニケーションを通して適切な安全管理水準を維持する取組に踏み込めないオン資利用施設が一定数は存在する**ことを示しているともいえる。


Medical Information Sharing and Analysis Center