国内ヘルスケア分野の
セキュリティ実態の比較調査分析

目次

１．調査概要
２．比較調査項目
３．比較調査結果
４．総評

調査概要～前提(1/2)

医療ISACでは2022年１～2月にかけて**四病院団体協議会**、2022年11月～12月には**全国保険医団体連合会/日本病院会**、23年1月に**全国老人保健施設協会**、23年2月に**人間ドック学会、日本保険薬局協会(NPhA)**と共同で、加盟組織におけるセキュリティ実態を把握するためのアンケート調査を行った。

病院

四病院団体協議会
日本病院会・全日本病院協会・日本精神科病院協会・日本医療法人協会

2022年1月～2月

診療所
病院

全国保険医団体連合会（保団連）
一般社団法人日本病院会（日病）

2022年11月～12月

介護

公益社団法人全国老人保健施設協会（全老健）

2023年1月

健診
薬局

公益社団法人日本人間ドック学会（ドック学会）
一般社団法人日本保険薬局協会(NPhA)

2023年2月

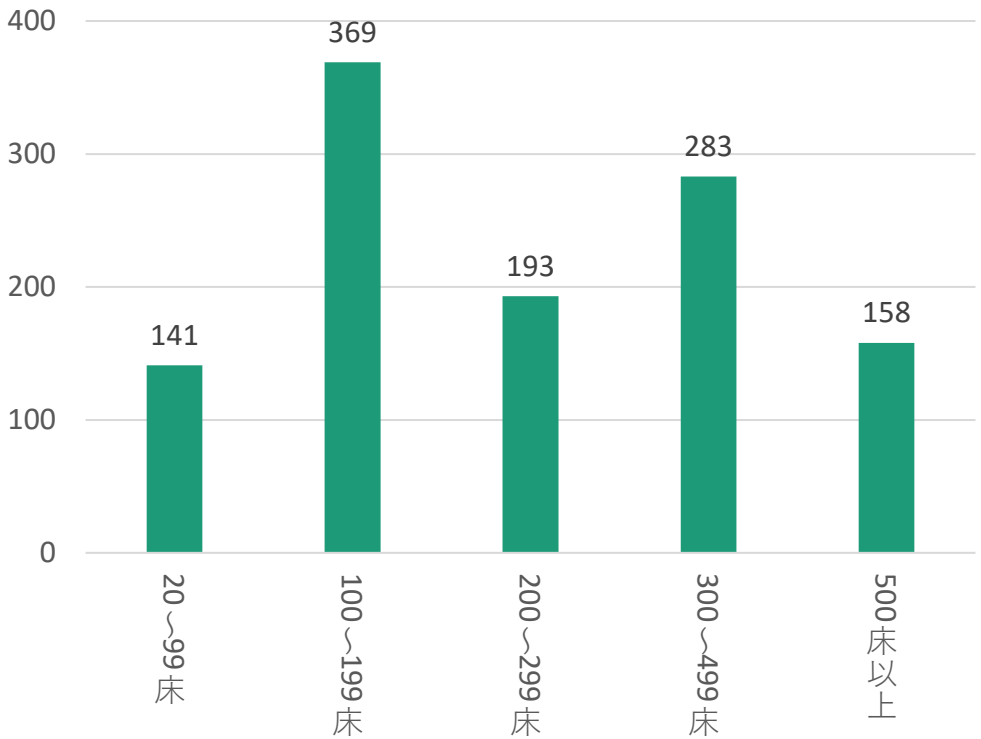
調査概要～前提(2/2)

	調査組織対象	回答組織（者）件数	団体加盟（会員）数（回答当時）	回答割合率
1	四病院団体協議会	1144件	5596病院	約21%
2	全国保険医団体連合会	897件	10万7000人	-
3	一般社団法人 日本病院会	382件	約2500病院	約15%
4	公益社団法人 全国老人保健施設協会	788件	3570施設	約22%
5	公益社団法人 日本人間ドック学会	318件	1788施設	約18%
6	一般社団法人 日本保険薬局協会	81件	383施設	約21%

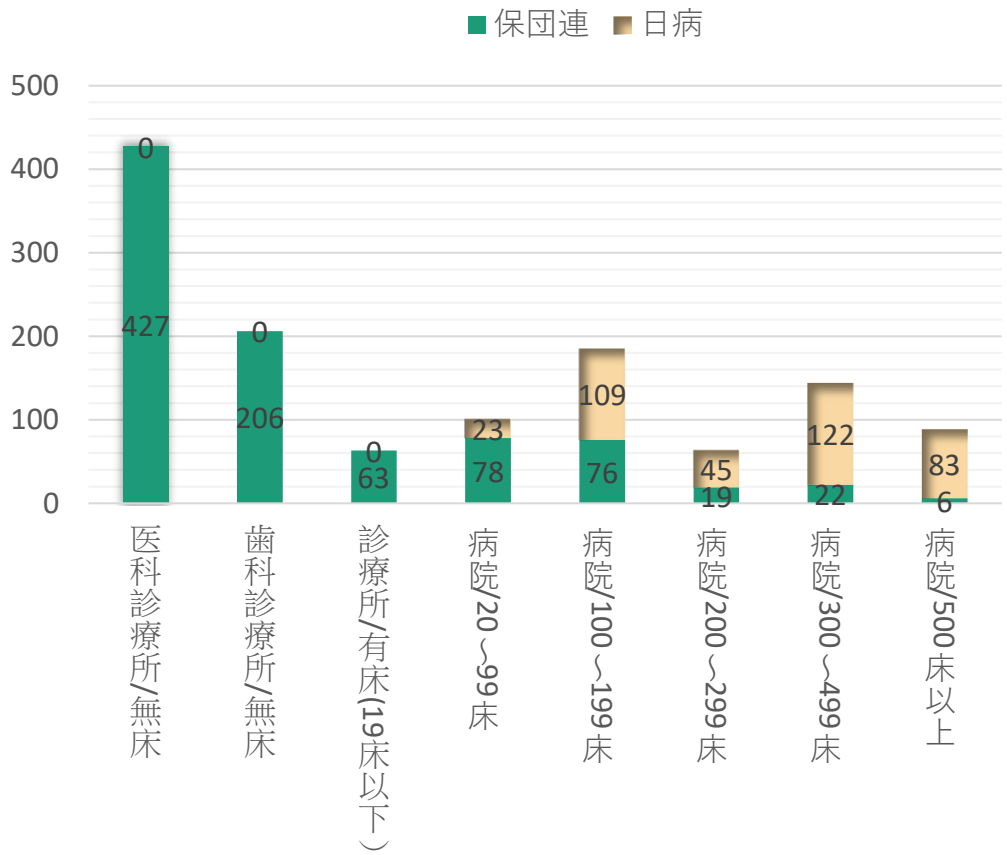
調査概要～調査対象組織内訳(1/2)

各団体別レポートは様々な属性より分析を行っているが、ここでは規模に着眼した組織内訳を示す。

1 ＜四病協：病床規模別＞



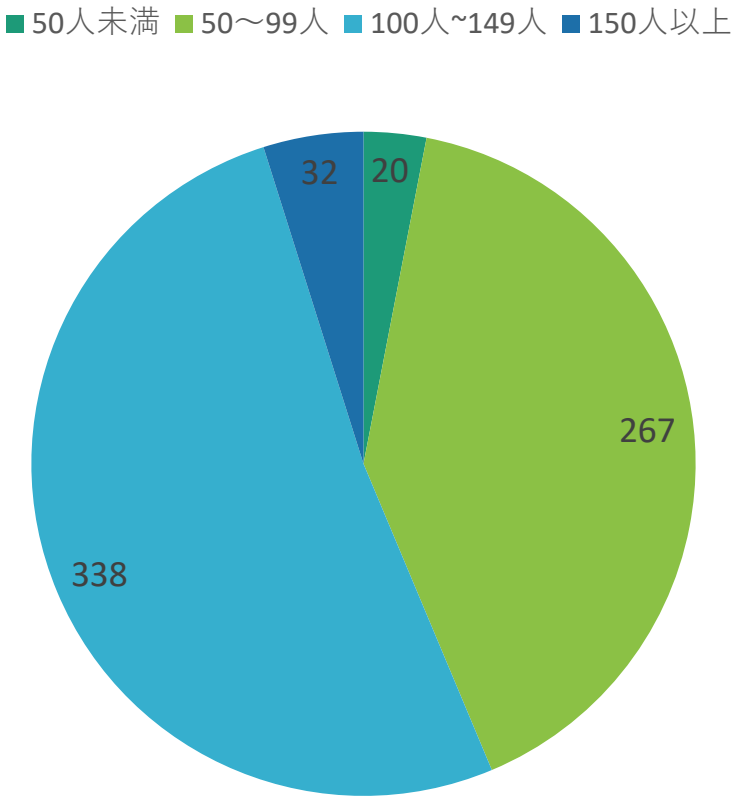
2 3 ＜保団連/日病：病床規模別＞



調査概要～調査対象組織内訳(2/2)

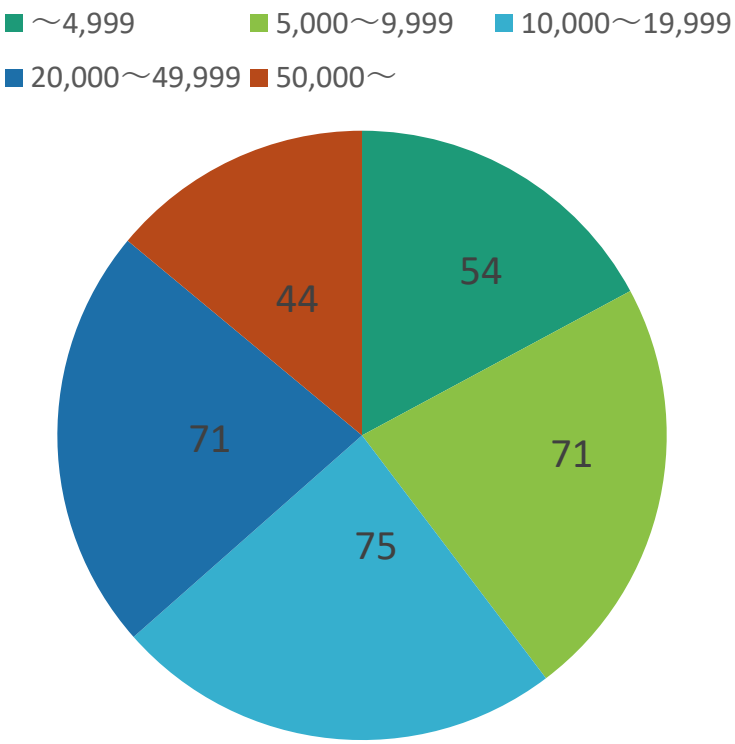
4

＜全老健：入居定員規模別＞



5

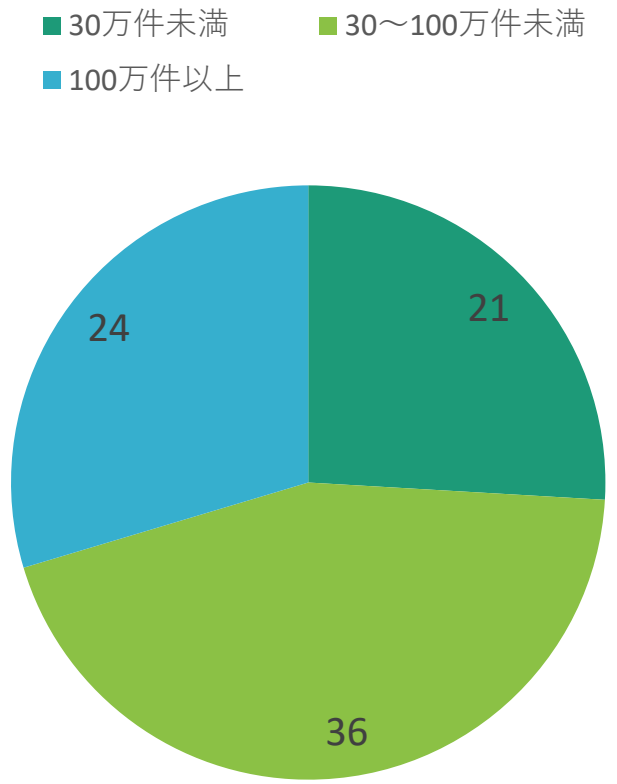
＜人間ドック学会：年間健診実施数別＞



※：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

6

＜NPhA:年間調剤件数別＞



※：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

2．比較調査項目

比較調査項目(1/2)

調査項目は調査時期によって一部異なるものもある。そのため、共通する調査項目に着眼した分析を行う。

カテゴリ	調査項目	調査対象組織					
		1 四病協	2 保団連	3 日病	4 全老健	5 ドック学会	6 NPhA
（1）： サイバー攻撃への脅威	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？	○	-	-	○	○	○
（2）： バックアップ対策	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）	○	-	-	○	○	○
（3）：脆弱性対策 （資産管理）	外部からのリモートメンテナンス用のVPN機器の種別を把握しているか？	-	○	○	○	○	○
（4）：IT人材	施設内のシステム担当者は何人いるか？ うち常勤の担当者は何人いるか？	○	-	-	○	○	○
（5）：監査	(a)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？	-	-	-	○	○	○
	(b)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？ （定期/不定期/未実施）	○	-	-	○	○	○

比較調査項目(2/2)

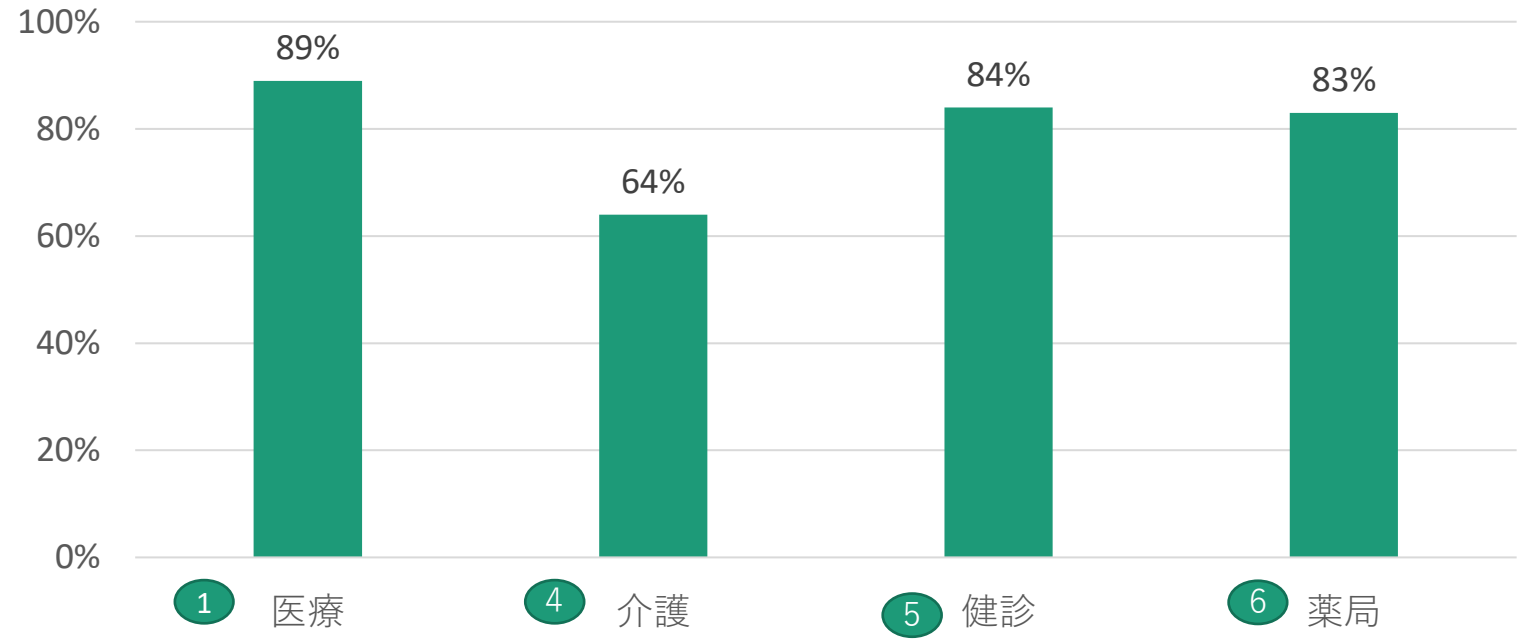
カテゴリ	調査項目	調査対象組織					
		1 四病協	2 保団連	3 日病	4 全老健	5 ドック学会	6 NPhA
（6）： セキュリティ予算	(a) セキュリティに関する概算年間予算（人件費・委託費を含む）はどの程度か？	○	-	-	○	○	○
	(b) セキュリティ予算は十分か？	○	-	-	○	○	○
（7）： セキュリティ保険加入	サイバー保険/情報漏洩保険等、何らかのセキュリティ保険に加入しているか？		-	-			
（8）： クローズドネットワークの安全性への共感	診療系ネットワークに設置された基幹系システムのセキュリティは安全であるという考え方に共感できるか？（共感・条件付共感）	○	-	-	○	○	○
（9）： IT事業者とのリスクコミュニケーション	(a)IT事業者は、基幹系システムについて、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、自組織が行うべきセキュリティ対策を指示しているか？	-	-	-	○	○	○
	(b)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」に基づき、セキュリティ面の責任分界を条項として明示的に定め、取り交わしを行っているか？	-	○	○	○	○	○
	（C)基幹系システムのセキュリティ対応について、IT事業者は十分に対応していると思うか？	-	-	-	○	○	○

3．比較調査結果

比較調査結果～(1) サイバー攻撃への感受性

国内の医療/介護/健診/薬局といった、患者ケアに直接関係のあるヘルスケアサプライチェーンの観点から見た場合、**ランサムウェアの実害を受けている医療層（病院）が最もサイバーリスクへの感受性が高い一方で、未だIT化が十分でない介護分野ではそうした意識が低い**ことが示されている。
なお、健診や薬局も医療分野と同水準のサイバーリスク認識を有している。

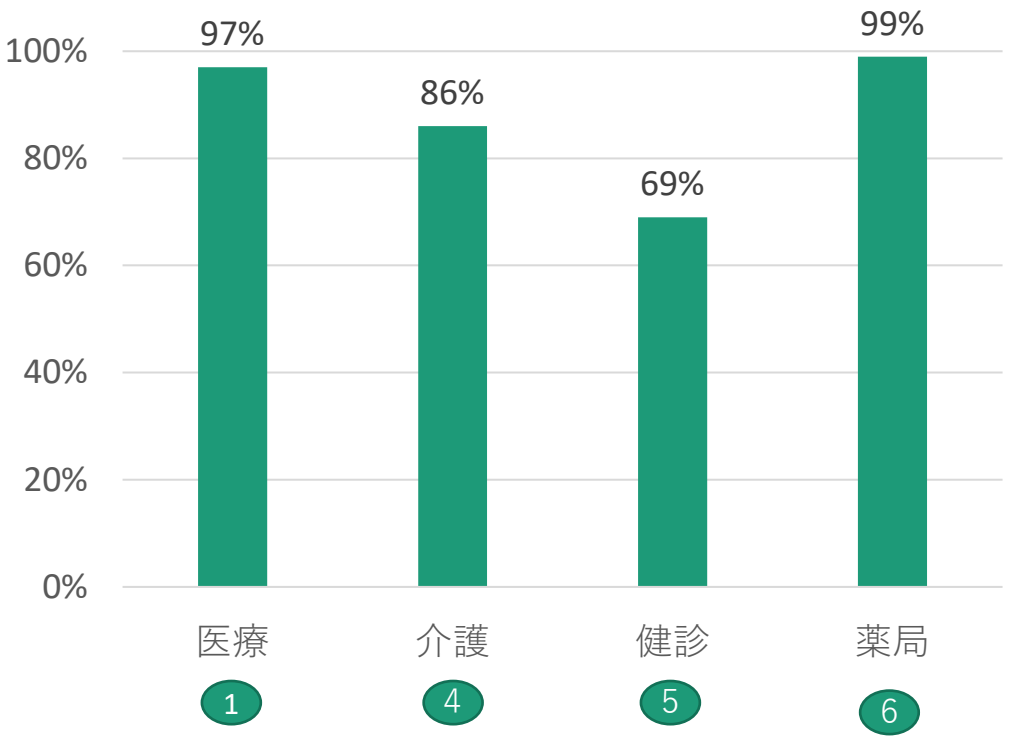
＜サイバー攻撃への脅威を感じる割合＞



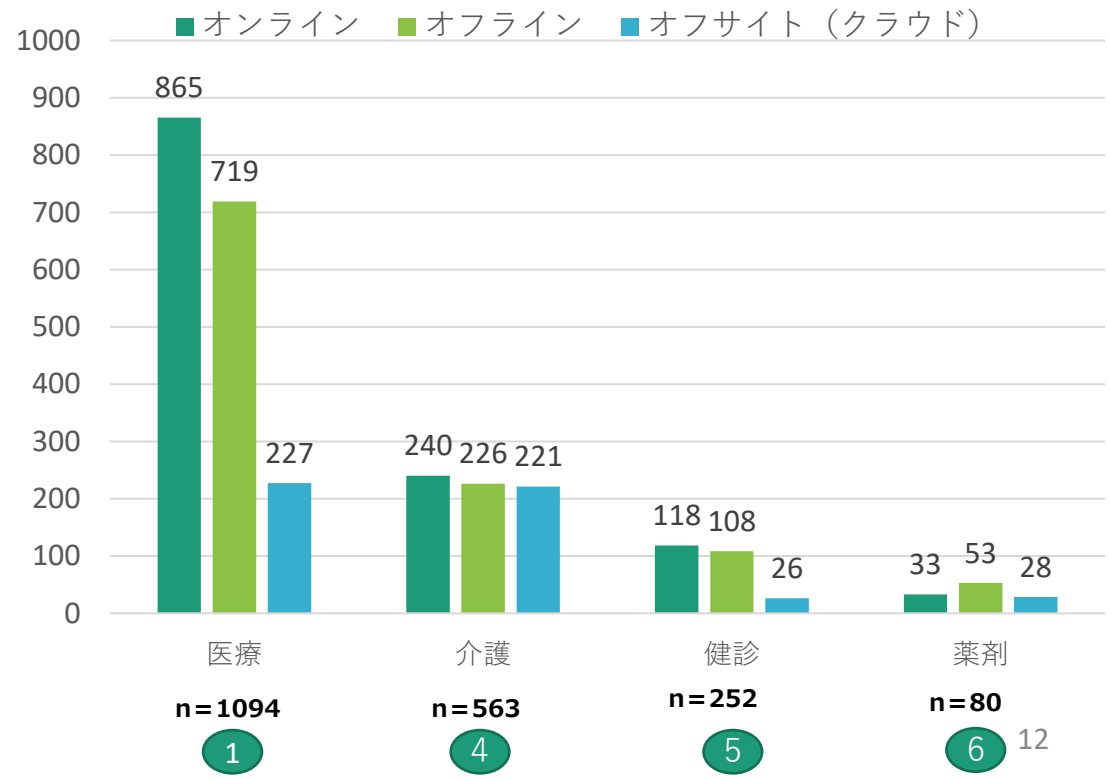
比較調査結果～(2) バックアップ対策

ランサムウェアリスクに備えたバックアップの取得率は健診層が最も低く、薬局、医療（病院）の順に高い状況である。健診層のバックアップ取得率の低さは、国内健診事業モデルのスポット性（非継続性）と影響がある可能性が推測される。
なお、どの分野においてもオンライン以外のバックアップ取得は行われているが、**ランサム被害報道の強い医療層（病院）においてそうした取組率が高い状況**が示されている。

＜バックアップを取得している割合＞



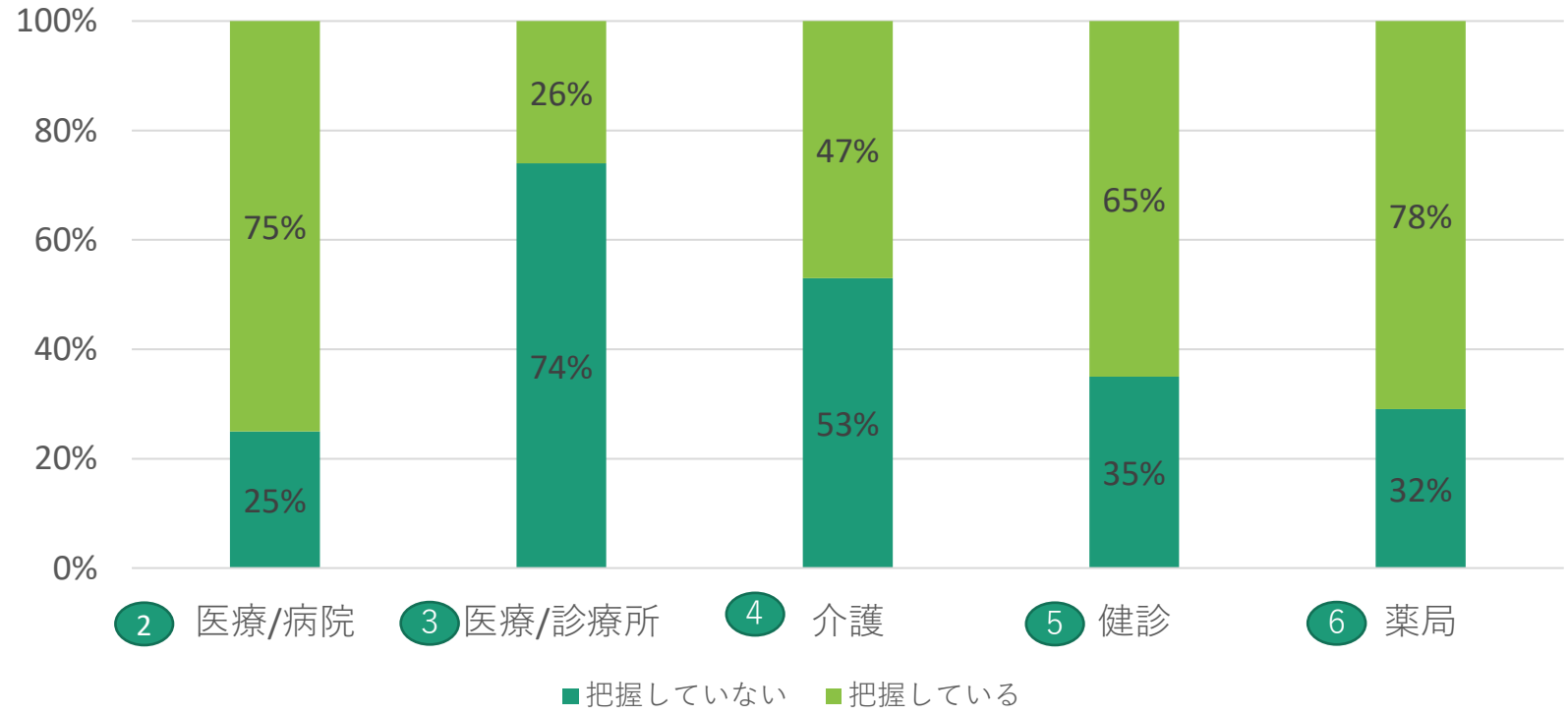
＜バックアップ取得方法/複数選択式＞



比較調査結果～(3)脆弱性対策(資産管理)

施設内に設置された機器等の把握は、サイバー攻撃の標的になるIT資産を正しく管理するという点で極めて重要だが、IT事業者が設置した施設内システムへの**リモートメンテナンス用VPN機器の製品種別を把握していない割合は診療所では7割強、介護では5割以上**を占めている。
一方、薬局層、VPN機器の脆弱性を悪用された攻撃の被害率/報道率の高い病院層ではこうした資産管理の取組が進んでいることがわかる。

<外部からのリモートメンテ機器の種別等の情報把握（資産管理）状況>



比較調査結果～(4) IT人材配置数

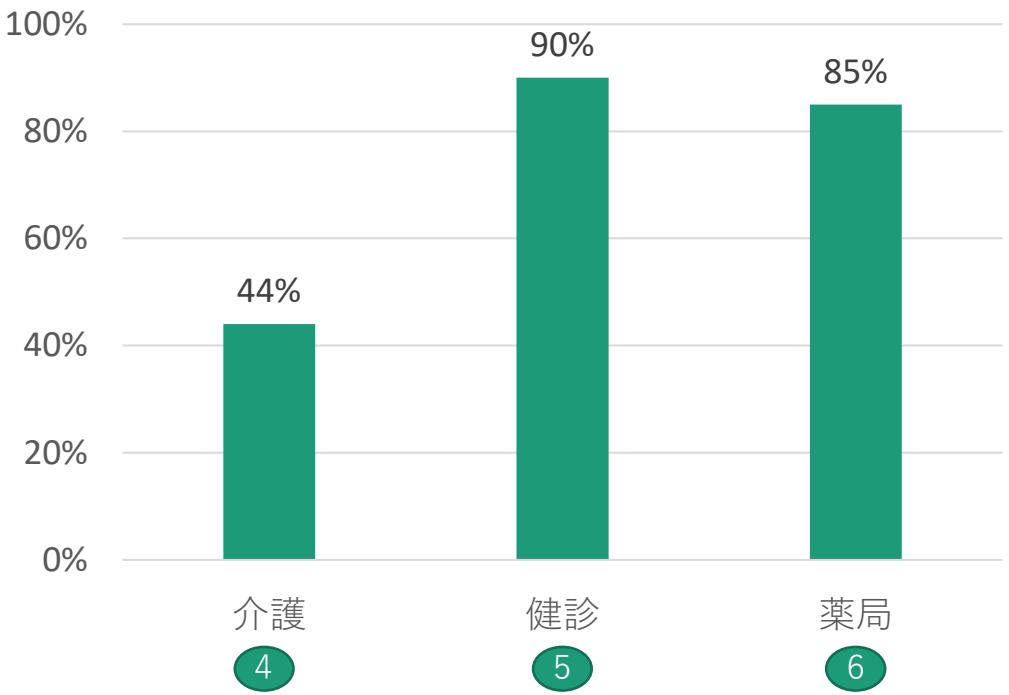
施設内のシステム担当者数配置数は薬局層が突出して多い。薬局の場合、チェーン展開で各エリア別にIT担当者を外部要員も含め適宜配置する等、規模に見合ったIT人材配置が機動的に行われていることが配置数の高さ及び常勤率の低さに影響していると想定される。
また、**介護層は最もシステム担当者配置数が少ない。**医療報酬水準より厳しい、介護報酬制度に規定された経営モデルにおいて、IT等のバックオフィス人材を継続的に定着・確保することの構造的な困難さが見て取れる。

	分野	施設内システム担当者	うち、常勤者	常勤割合率
1	医療	2.5人	2.4人	96%
4	介護	1.6人	1.5人	94%
5	健診	2.9人	2.6人	90%
6	薬局	5.7人	4.1人	72%
	全体平均	3.2人	2.7人	88%

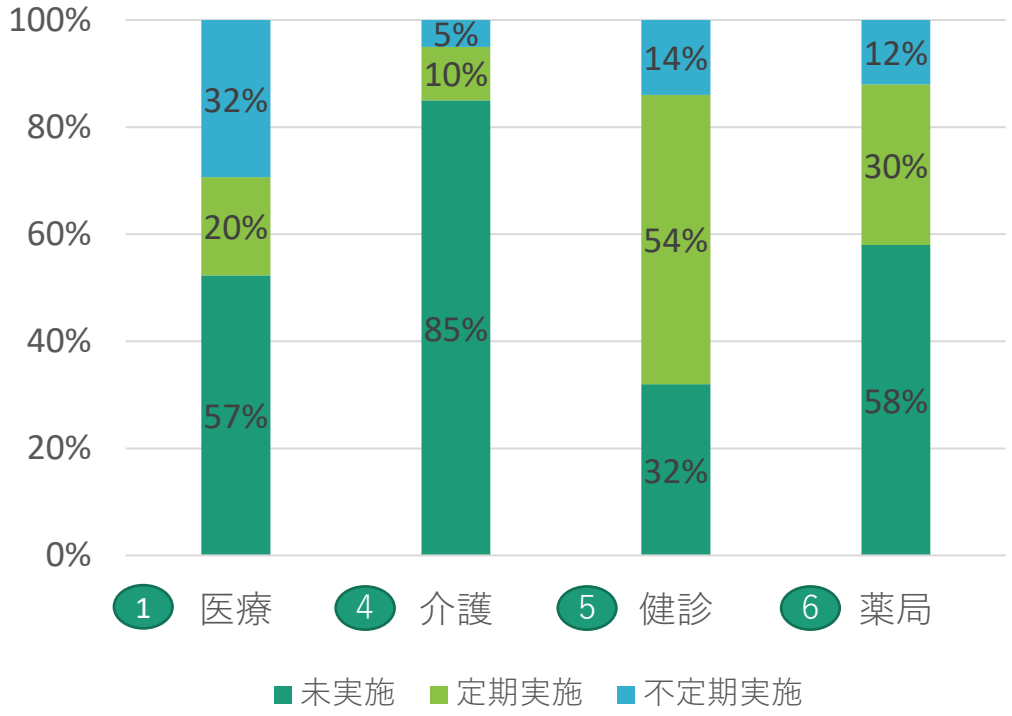
比較調査結果～(5) 監査

健診層では、特に厚労省安全管理GLの把握率が高く、かつ、セキュリティ監査の定期実施率も高いため、GLに基づくセキュリティPDCAの取組水準も高いと考えられる。続いて、薬局分野が同種の取組率が高い状況ではある。
他方、**介護層では、安全管理GLの把握率の低さ/セキュリティ監査の未実施率の高さが顕著**であり、IT人材配置数の少なさ・セキュリティ予算の確保の難しさがこうした事態を招いていると言える。

<(a) 厚労省安全管理GLを把握している割合>



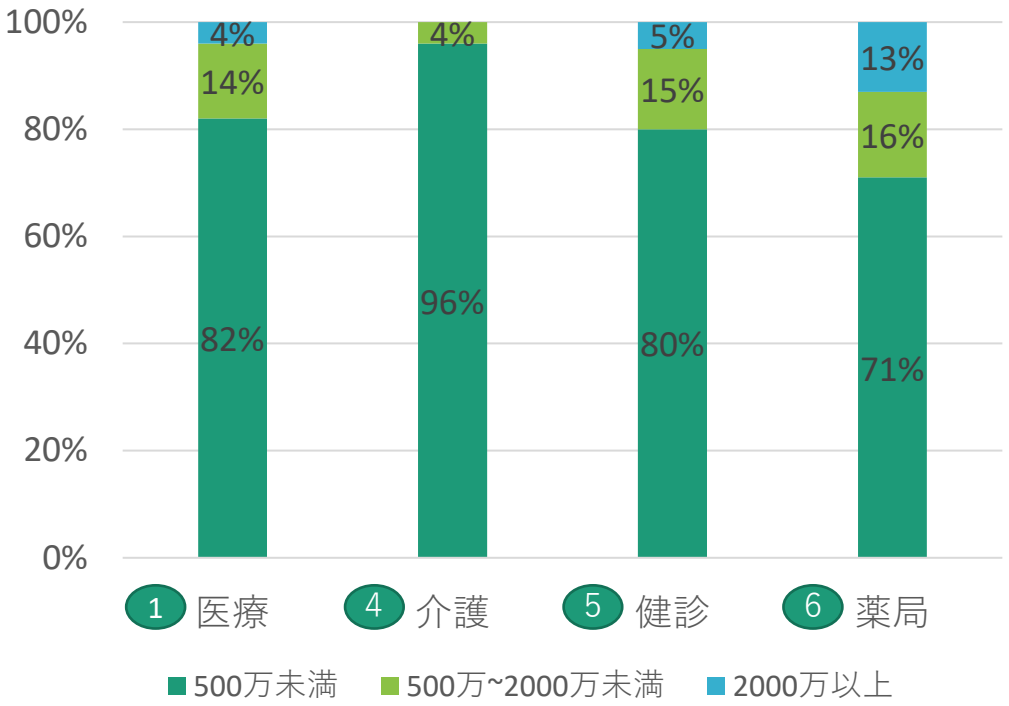
<(b) セキュリティ監査の実施状況>



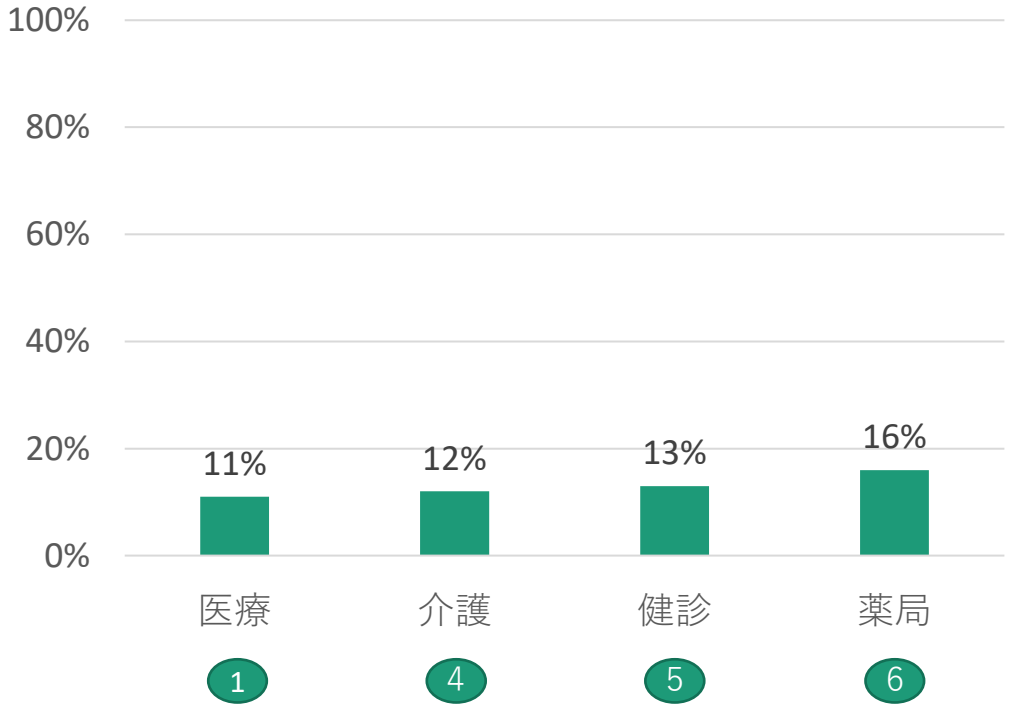
比較調査結果～(6) セキュリティ予算

健診・薬局層ではセキュリティ予算が500万以上確保できている割合が高い一方で、予算に不十分と回答した割合も相対的に多い。
特に薬局層では、運営がチェーン展開型で推進されるため、エリア単位のセキュリティ予算の確保が必要になることが原因の一つと考えられる。
なお、**介護分野ではセキュリティ予算（ひいてはIT予算というべきか）が他分野と比較して大きく下回っている**状況が浮き彫りになっている。

＜(a) セキュリティ予算確保状況＞



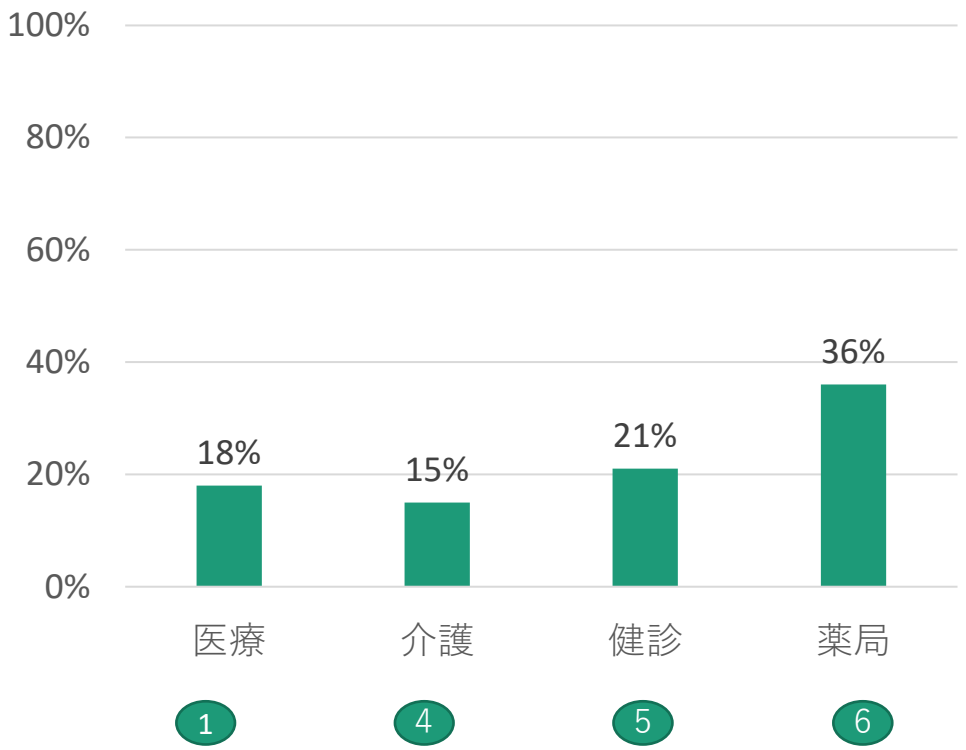
＜(b) セキュリティ予算が十分と回答した割合＞



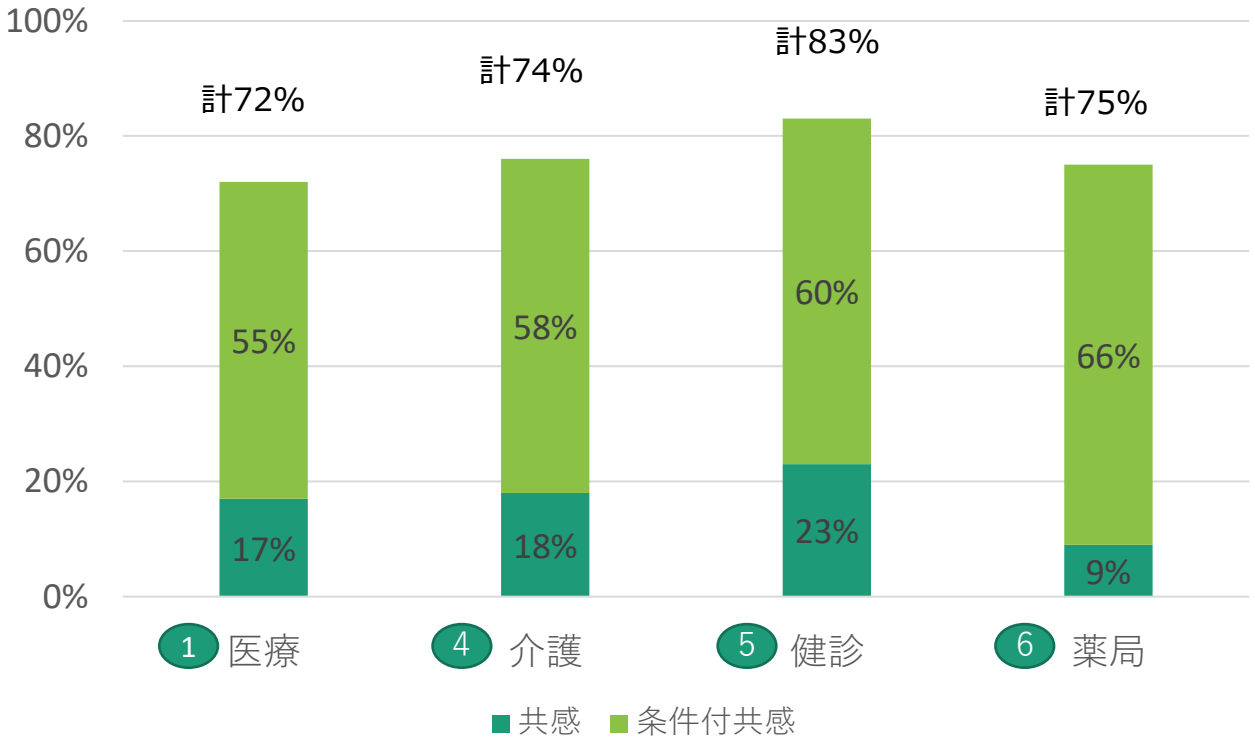
比較調査結果～（7）サイバー保険/（8)クローズドNWの安全神話への共感

何らかのセキュリティ保険に加入している割合は**薬局、健診の順に高い**一方、クローズドNWの安全神話への共感率も**健診、薬局の順**に高い。薬局・健診層では、安全神話という無根拠な空想への共感度は高いが、しっかりとセキュリティ保険にも加入するといった、**現実的なリスク管理意識が強い**と言える。
なお、クローズドNWの安全神話への共感率のうち、**薬局層においては完全共感率が最も低いことからも、この層におけるセキュリティ意識の高さ**がうかがえる。

＜何らかのセキュリティ保険に加入している割合＞



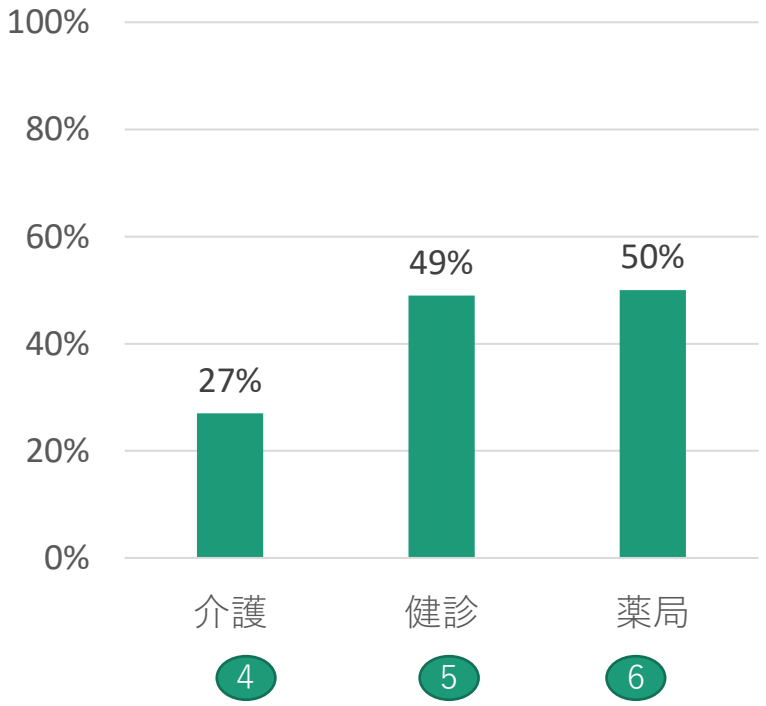
＜クローズドNWの安全神話へ共感する割合＞



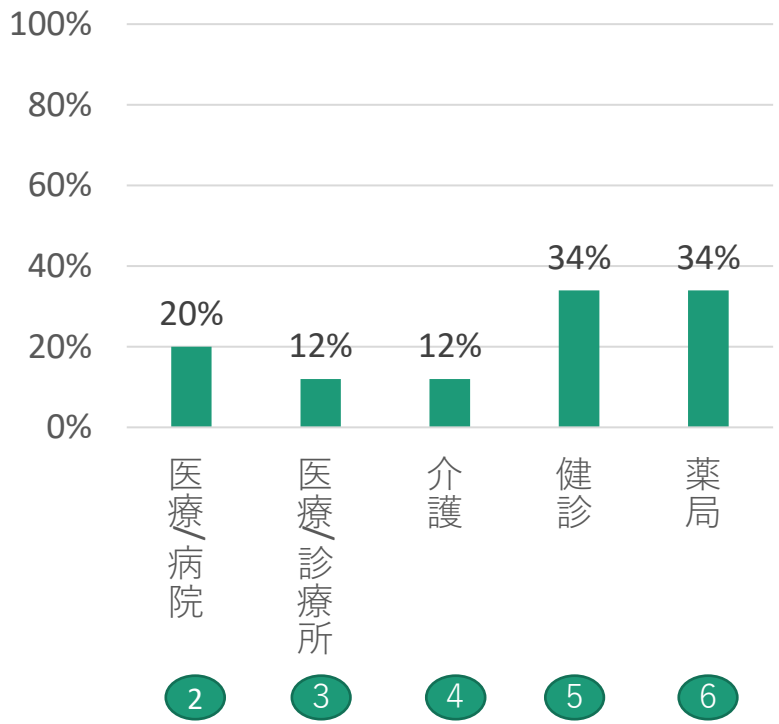
比較調査結果～(9) IT事業者とのリスクコミュニケーション

3省2ガイドラインが求めるIT事業者とのセキュリティも含めた責任分界を契約等で定めている施設割合は**診療所、介護がともに最も低い。**また、介護/健診/薬局という層で見た場合、**契約の取り決めをしていないにも関わらず、IT事業者への信頼度が全体的に高いことがうかがえる**。実務的には事業者によるユーザセキュリティの指示等がある状況に起因すると思われるが、サイバー被害の発生等の想定外の異常事態においては契約/法律が優先することは言うまでもないため、**自主防衛のためにも適切なセキュリティ面も含めた契約を取り交わすことが喫緊の対応事項と言える。**

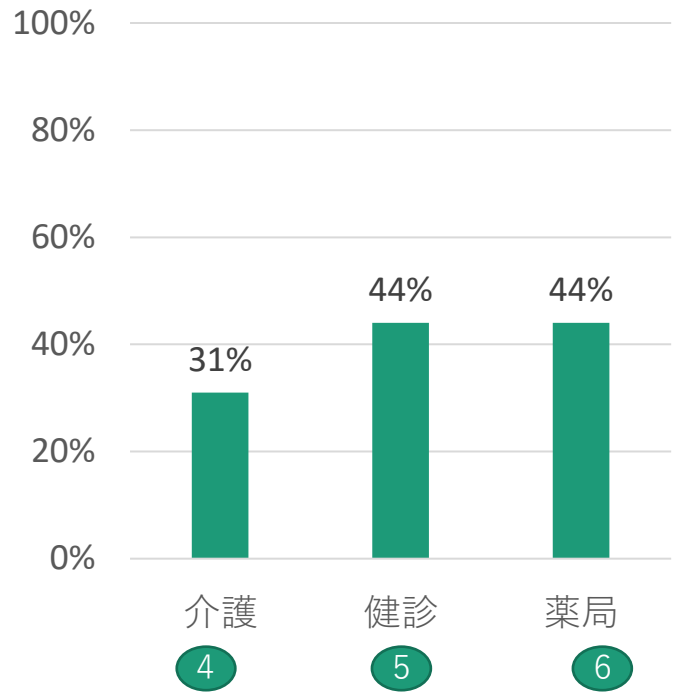
<(a)IT事業者によるユーザセキュリティ支持を受けている割合>



<(b)IT事業者とセキュリティ上の責任分界を含めた契約を取り交わしている割合>



<(c)IT事業者を信頼している割合>



４．総評

総評

- 医療（病院・診療所）/介護/健診/薬局という観点でサイバー攻撃への対策状況（ヒト・カネ・モノ）を比較分析すると、**特に介護層のセキュリティへの取組が劣後している**点が見受けられる。介護報酬上の制約やIT化の遅れ等の問題もあるものの、患者ケアを目的としたヘルスケアサプライチェーンの観点からは、**介護層におけるセキュリティの脆弱点からその他の分野・層への攻撃波及のリスクは否定できない**状況である。

- また、サイバー攻撃対策を考えるうえで基本的なIT資産管理（どのような機器が院内・施設内で利用されているかの把握）の取組において、**IT業者が院内に持ち込んでいる機器を把握していない割合は介護層に加え、診療所層が最も高い**状況である。**介護層/診療所層は契約におけるセキュリティ上の合意形成率も最も低い**割合であり、ナレッジ・ノウハウ自体が不足していることが推測される。
- そのため、**こうした層も含め、より幅広に、セキュリティ面を含むIT事業者との契約交渉力をいかに底上げするかを、多面的に考えていく必要があると言える。**

- 一方、IT人材数の配置数やセキュリティ予算確保、またはセキュリティPDCA等において、**健診や薬局層ではランサムウェア等の実被害の多い医療層以上に充実した取組**が行われており、**国内ヘルスケア分野のセキュリティ上のベタープラクティスが潜在**していると考えられる。
- 健診や薬局層とその他の層では事業・経営モデルの前提が異なる点もあるが、患者ケアを目的とする意味では同じ方向を向いている、国内のヘルスケアサプライチェーンにおける各層・分野が、自分野のみならず、**他の分野のベタープラクティス（まずは低コストでも着手できるリテラシー向上等）を横断的に共有しあえる仕組み作りの検討**が重要になるといえる。


Medical Information
Sharing and Analysis Center