

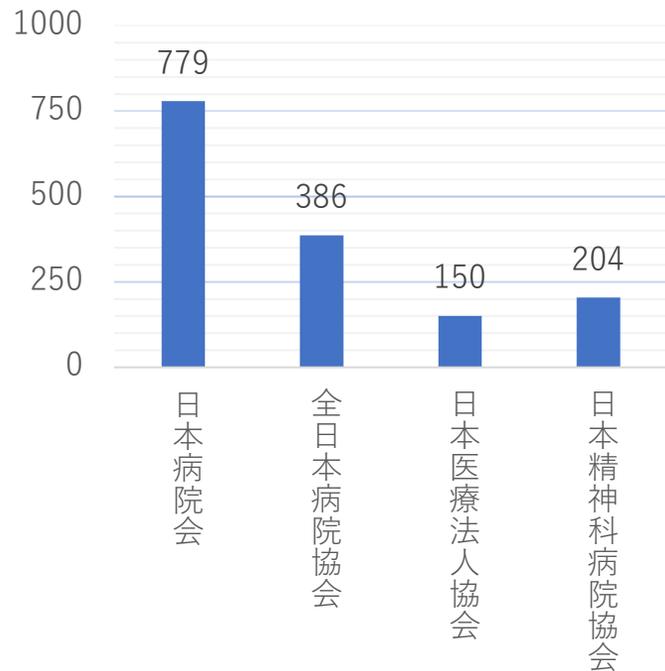
**四病院団体協議会
セキュリティアンケート調査結果
(最終報告)**

- 1.全体結果 (p3~p11)**
- 2.病床規模別調査結果 (p12~p20)**
- 3.開設者別調査結果 (p21~p29)**

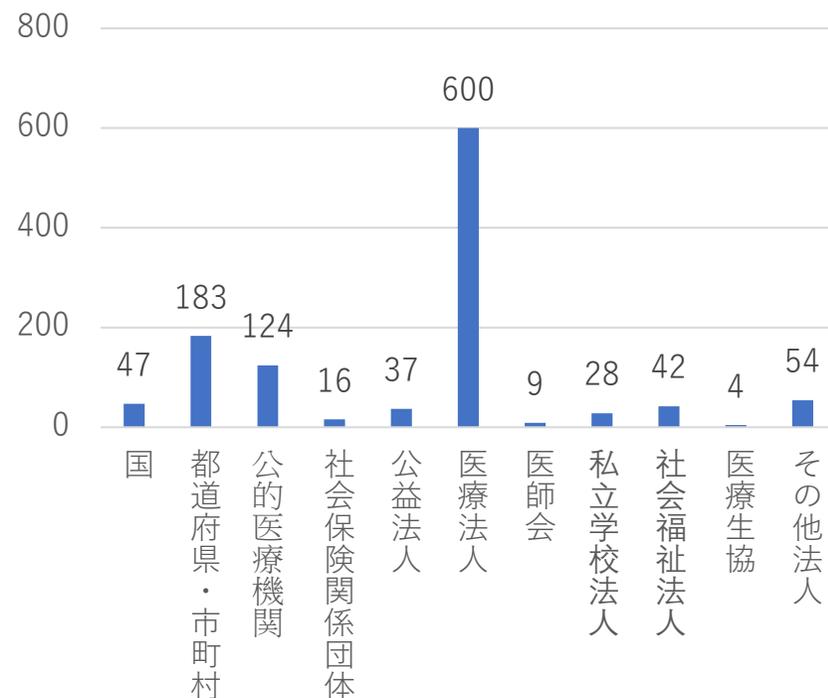
調査対象

- 実施期間：2022年1月31日～2月28日
- 調査対象病院数：5596件（四病院団体協議会加盟病院）
- 回答病院数：1144病院
- 回答率：20.4%
- 実施団体：（一社）医療ISAC

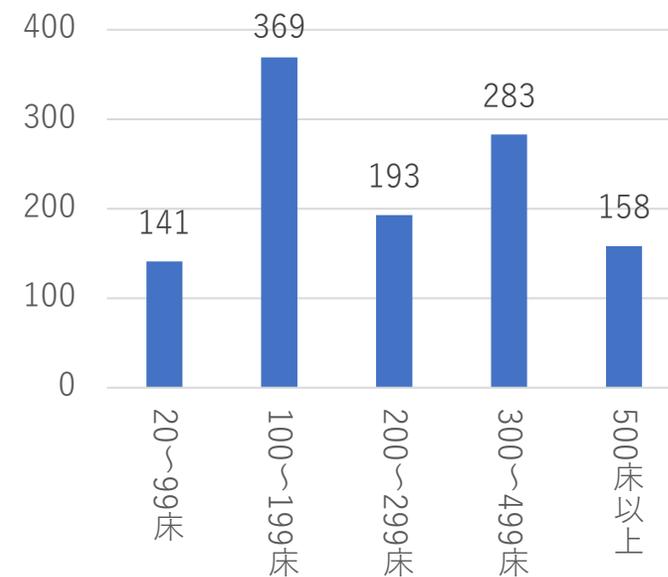
< 団体別内訳 >



< 開設者別内訳 >



< 病床規模別内訳 >



※複数団体加盟病院が存在するため、総合計数は1519件

1. 全体結果

< 全体結果総評 >

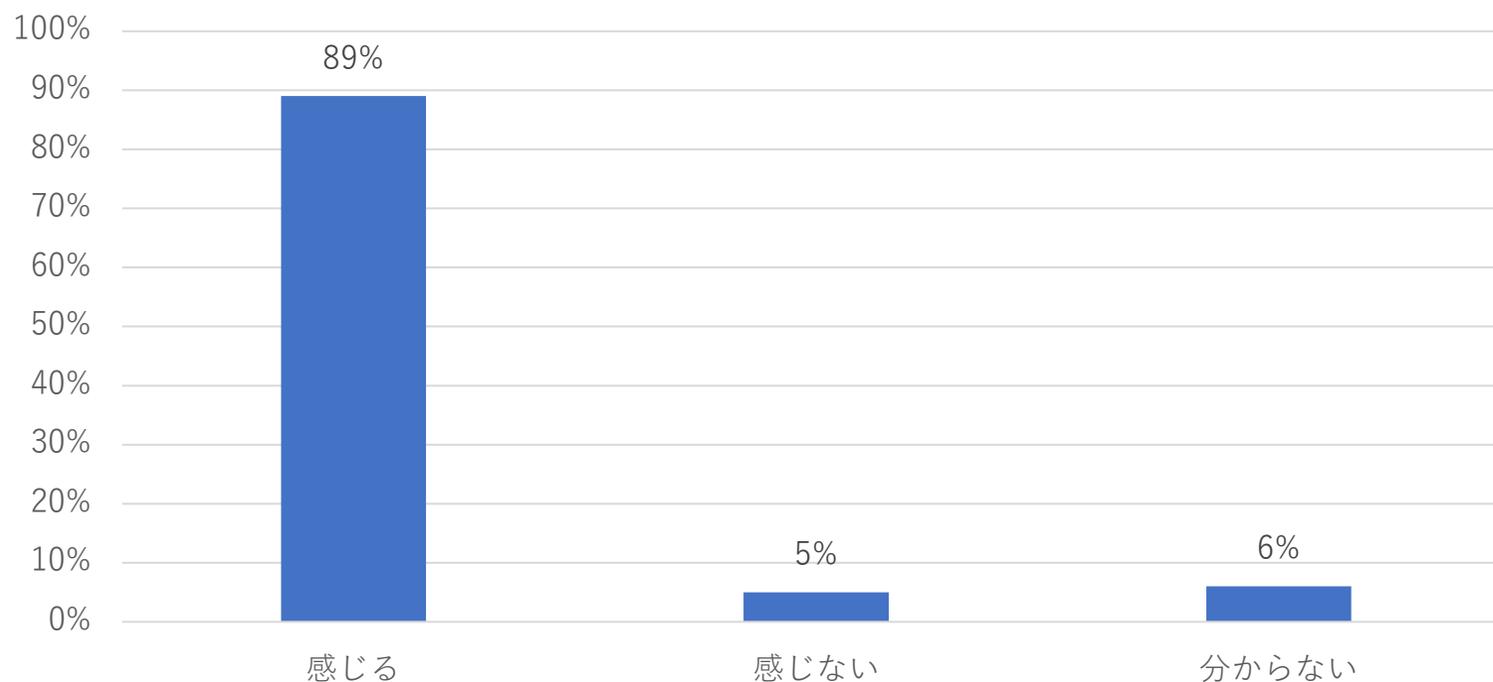
- 当今のサイバー脅威の高まりに対して**ほとんどの回答病院は危機感をもっており**、サイバー対策を講じることの必要性を理解している。
- 一方、NISCや厚労省が指摘したVPN機器の脆弱性への対応を行っていないと回答した病院が3割程度存在しており、**その半数以上が理由を「情報をキャッチできていなかったため」「予算がなかったため」としている。**
- これらの原因として考えられるのが**病院のシステム/セキュリティ管理体制自体の脆弱さ**である。院内システム担当者は常勤で固定化され、セキュリティ専門会社等からの要員派遣等はほぼ行われていない。さらにセキュリティ監査は多くの回答病院で未実施であった。
- つまり、外部の専門家が現在のセキュリティ上の課題を指摘すること、あるいはセキュリティの最新情報を現場へ持ち込むといった、**外の空気を入れることで足元の見直しを行うことが困難**な事態に陥っていると考えられる。
- **こうした事態は、病院のセキュリティ予算不足に起因しているといえる。**
- **何故なら、半数以上の回答病院が年間セキュリティ予算が500万円未満であり、且つ、予算が少ないと感じている。**病院としてサイバー対策を講じなければならないことは理解しているものの、セキュリティ予算がなく、適切なソリューションの導入、外部からの知識提供の機会を確保することができない状況が推測される。
- 加えて、「診療系ネットワークは外部ネットワークと遮断されており安全である」という従前の考えの根強さも見受けられる。外部のセキュリティ専門家による指摘が受けられないことのみでなく、**セキュリティ予算の制約による対策不足を（無意識に）正当化するため、あえてこうした根拠薄弱な安全神話に依存せざるを得なくなっていること**もこの原因の一つと考えられる。
- このような考えが根強く残るなかでは、サイバー保険の加入検討自体にも積極的でない病院が多いことは当然と考えられる。
- セキュリティ事故発生時のインシデントレスポンスはUSBメモリ紛失等、情報漏えい等への対応を通して病院として習熟度が高まっている。
- しかしながら、患者診療の前提となる医療情報システムが利用不可になった場合の業務継続計画、つまりランサムウェアの被害を受け、**診療系の医療情報システムが利用不可になった場合に患者診療を適切な水準で維持するための計画・態勢整備を行えている回答病院は3割程度**であった。

<アンケート調査内容_全体結果(1/7)>

<サイバー攻撃への脅威>

・昨年来の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ている医療機関はほぼ全体の9割に及んでおり、既に医療機関においてもサイバー脅威への対応の必要性の理解は一般化していることが見受けられる。

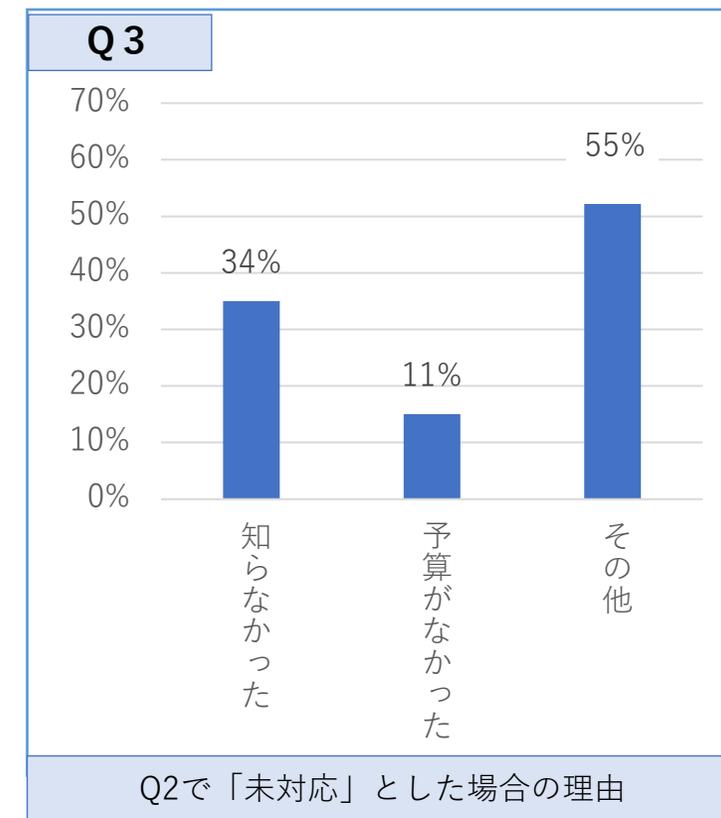
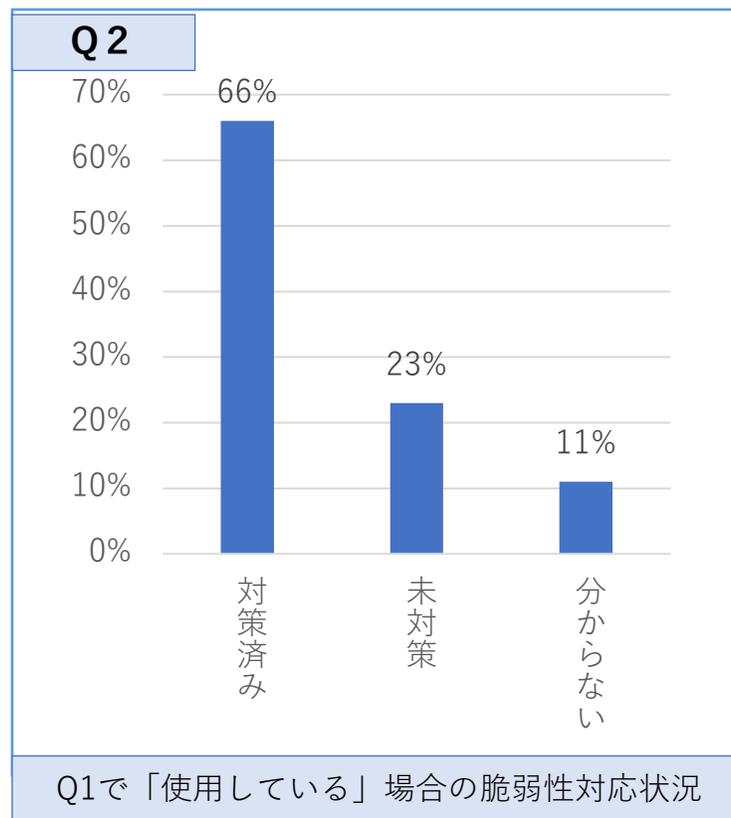
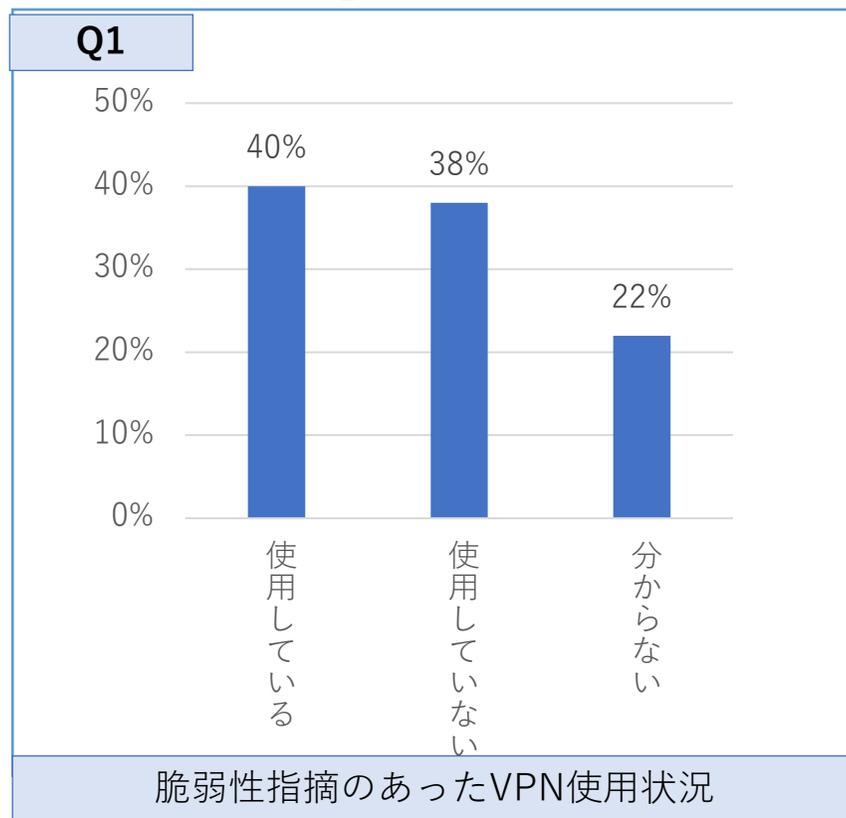
<サイバー脅威への感度>



<アンケート調査内容_全体結果(2/7)>

<脆弱性への対応>

- ・ NISCや厚労省が脆弱性を指摘したVPN製品・ソリューションを使用する病院は4割程度。
- ・ そのうちの6割以上は脆弱性への対応を行っているが、状況不明も含めれば**未対応が3割強以上**を占めている。
- ・ 未対応の理由としては、**情報が届いていないこと（知らなかった）、予算不足であったことが回答の半分弱**を占め、さらにその他の理由には「外部と接続していない」「クローズドネットワークで運用しているため」「パッチ適用による不具合が懸念されるため」等が多く見受けられた。

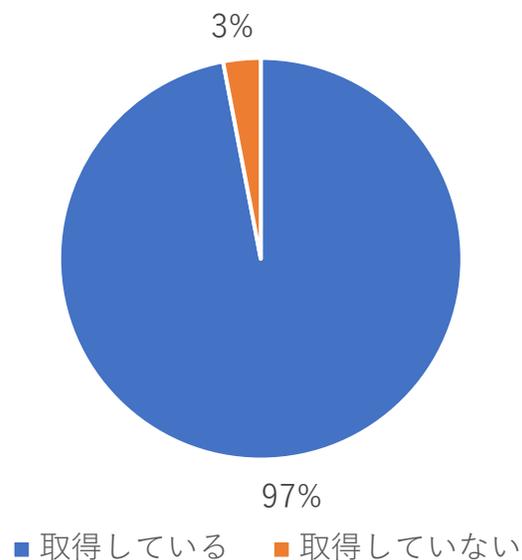


<アンケート調査内容_全体結果(3/7)>

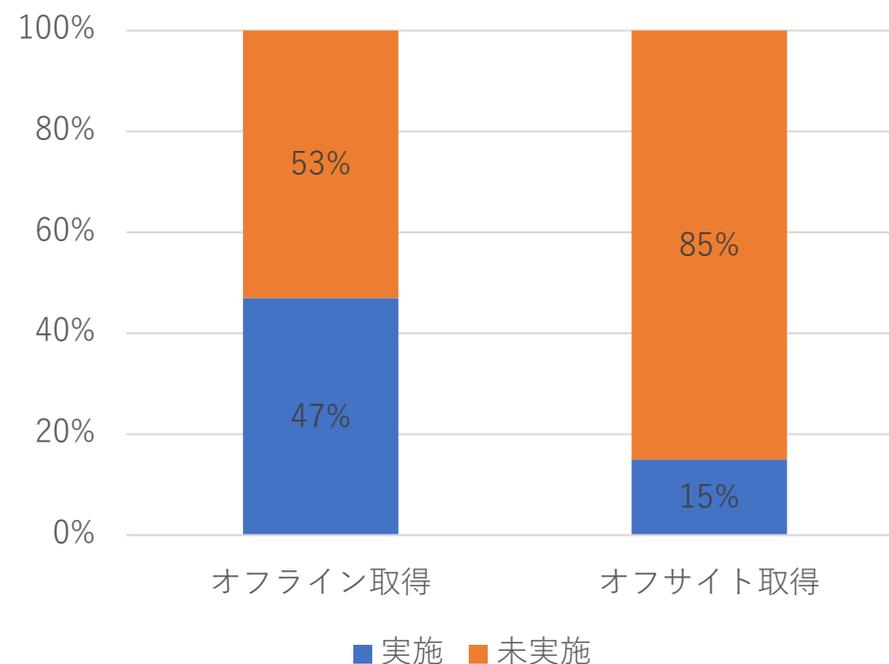
<バックアップへの対応>

- ・回答病院のうち、97%がバックアップを取得していると回答あり。
- ・そのうち、バックアップをオフライン取得している割合は5割を少し下回り、オフサイト（外部施設）へ保管している割合は1割強程度である。
- ・ランサムウェアの感染被害への対応策としてバックアップ退避を行えている病院は未だ十分でない状況と言える。

<バックアップ取得率>



<オフライン/オフサイトバックアップ取得有無率>



<アンケート調査内容_全体結果(4/7)>

<セキュリティ管理～その1>

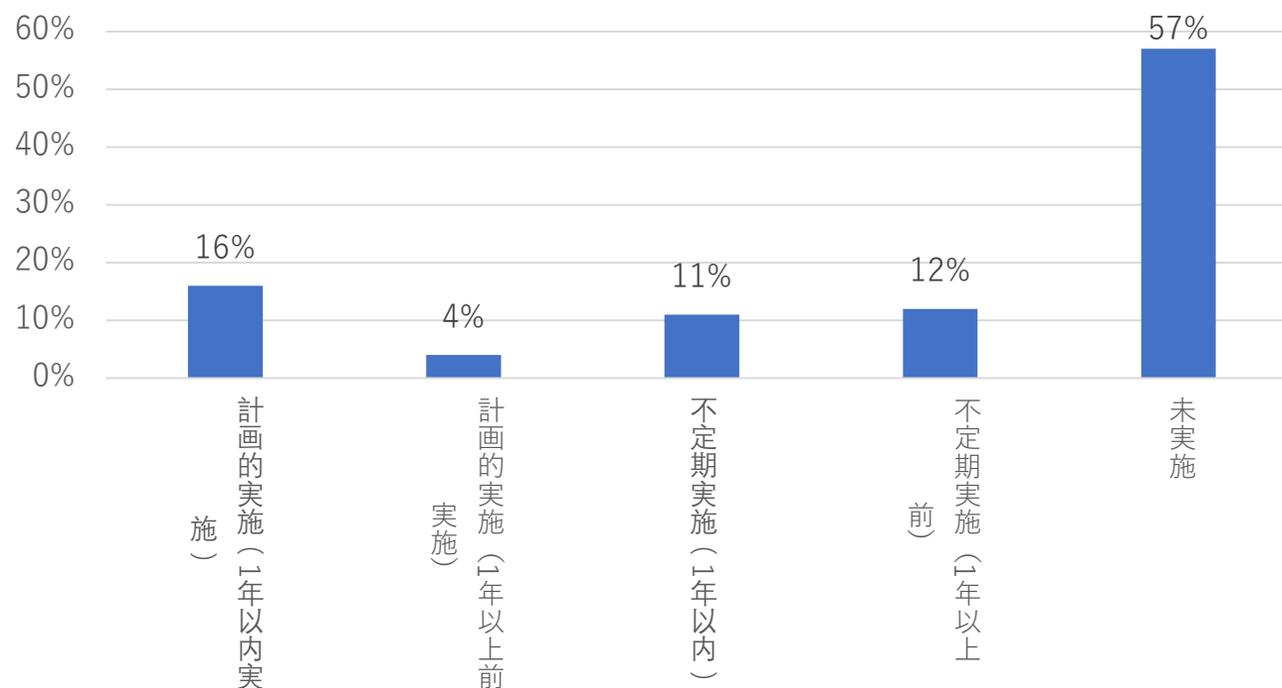
・院内システム担当者数は全体平均で3人弱で、そのうち常勤者もほぼ同水準であるため、専門的なセキュリティ知見のある外部企業からの要員派遣等、外部の目線の導入による環境見直し等が発生しづらい体制でシステム管理が行われていることが推測される。

・セキュリティ監査という外部の目線によるチェックを実施していない病院の回答割合も5割以上を占めており、全体的にセキュリティに通じた外部専門家からの適時/適切なアドバイスが受けにくい状況が見受けられる。

<院内システム担当者数/常勤者数>

全体平均	
院内システム担当者数	2.9人
うち、常勤者数	2.6人

<セキュリティ監査実施状況>



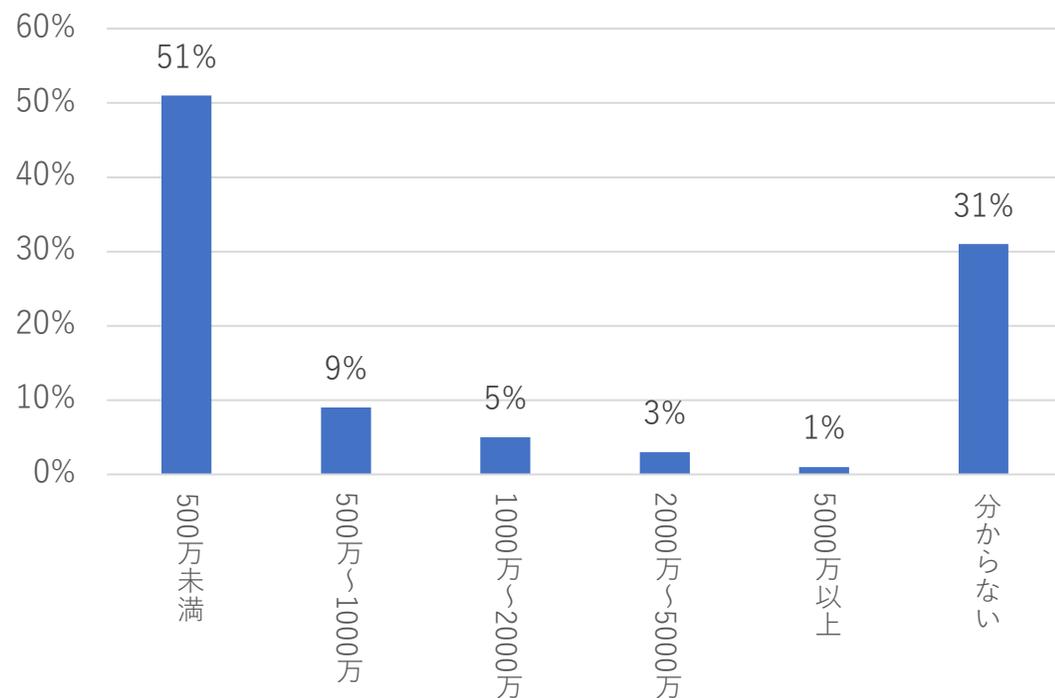
<アンケート調査内容_全体結果(5/7)>

<セキュリティ管理～その2>

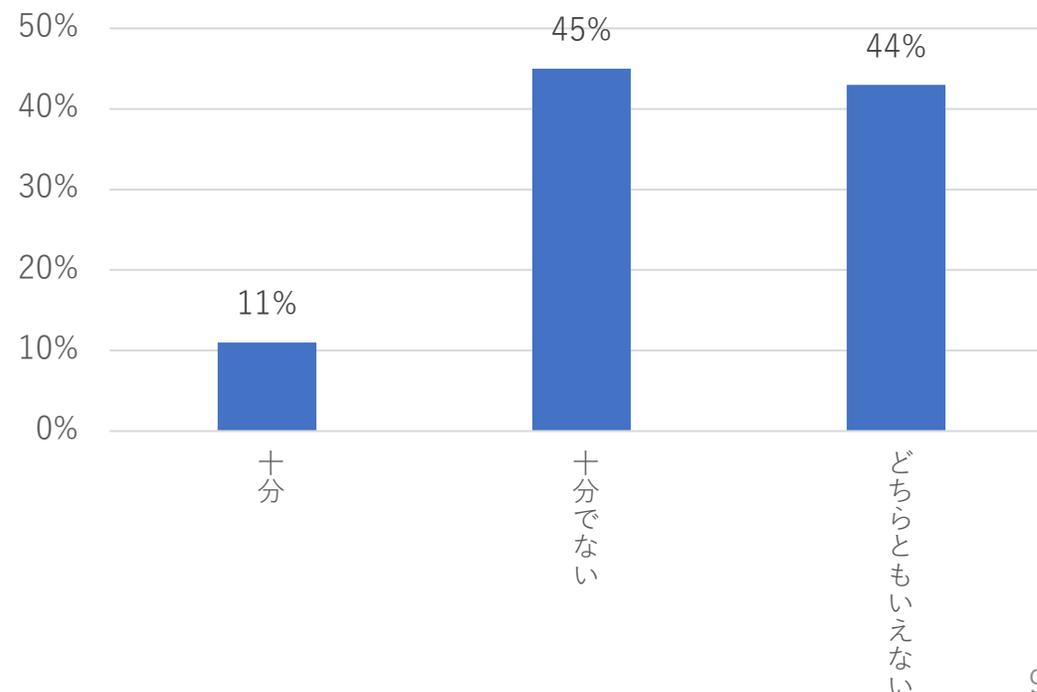
・年間のセキュリティ予算が500万円未満と回答した病院の割合は5割強、セキュリティ予算が十分でないと回答する割合もほぼ5割弱であり、**半数程度の病院は現在のセキュリティ予算が十分でない**と考えている。

・診療報酬という公定価格に基づく病院の収支構造上、十分なセキュリティ予算を計画的に捻出することが困難であり、**予算の制約上、本来病院として実施すべきと考えるセキュリティ対応も結果的に行えなくなっている**状況が推測される。

<年間セキュリティ予算>



<セキュリティ予算を十分と感じているか>

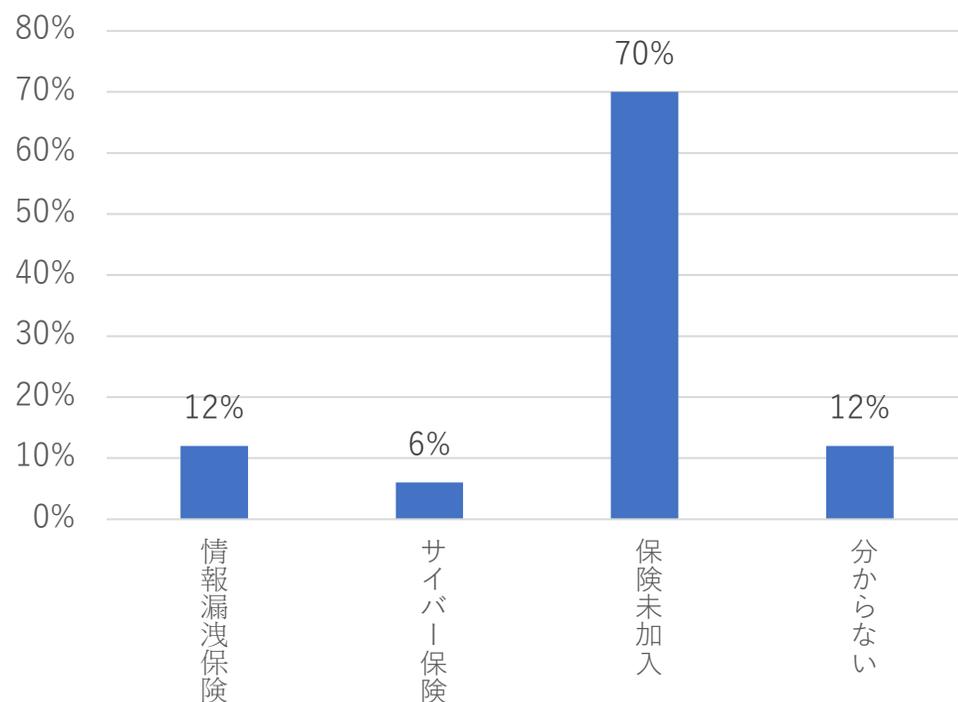


<アンケート調査内容_全体結果(6/7)>

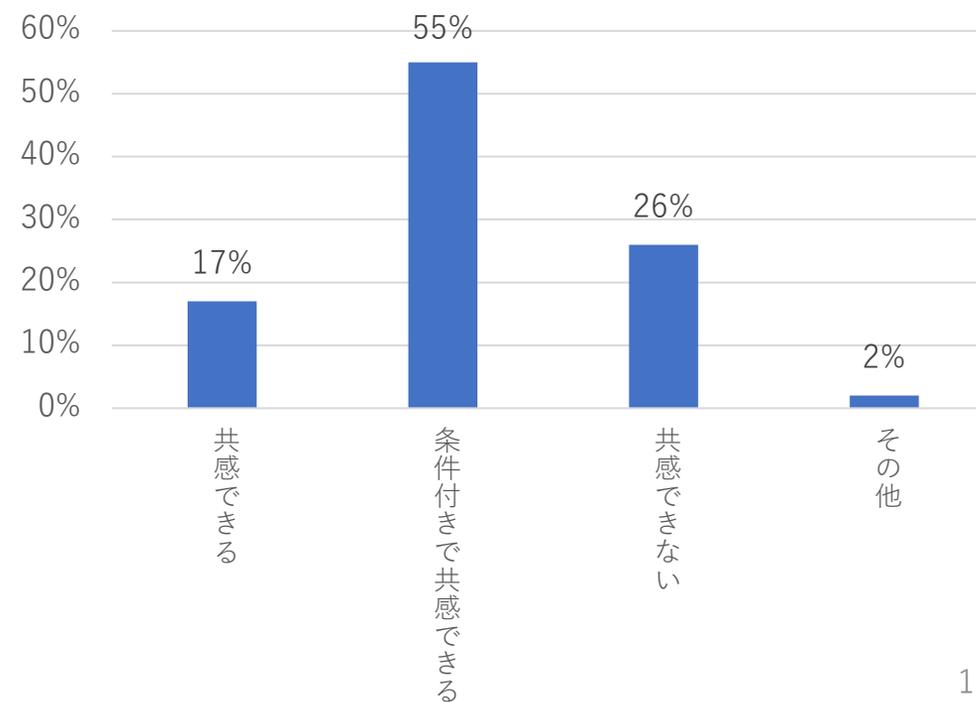
<セキュリティ管理～その3>

- ・インシデント発生に伴う費用負担を行うサイバー保険に未加入であると回答した病院が7割を占めている。
- ・また、「診療系ネットワークは外部ネットワークと遮断されているため安全である」という考えに何らかの形で共感すると回答した病院の割合も7割以上にのぼっている。
- ・診療系ネットワークの安全神話（狭小な境界防御）に依存したセキュリティリテラシーが色濃く残る環境において、サイバー保険に加入するという選択自体、院内で十分な合意を得ることが困難であることが推測される。

<セキュリティ関連保険の加入状況>



<「診療系ネットワークは安全であるという考え」への共感度>



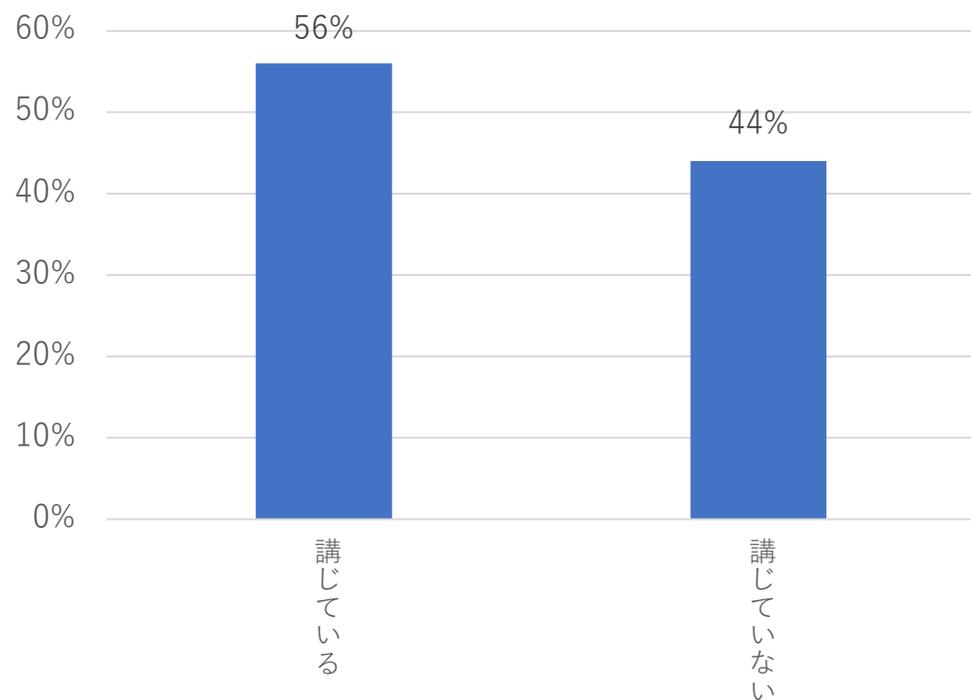
<アンケート調査内容_全体結果(7/7)>

<インシデントレスポンス・BCP>

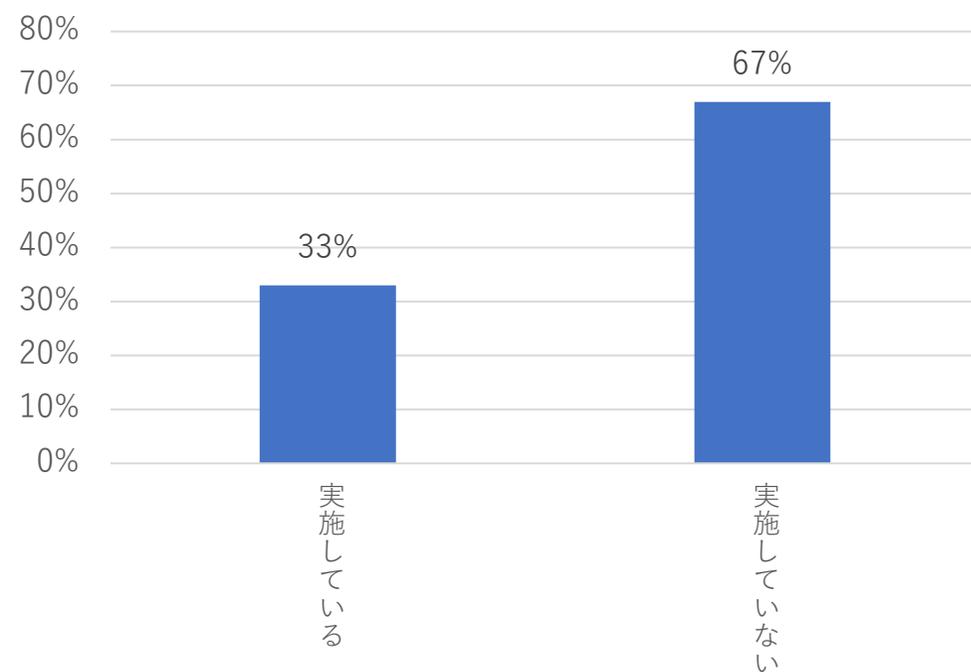
・セキュリティインシデントの被害最小化プロセスを整備している病院の回答割合は6割弱である一方、患者診療等の院内業務の前提となる医療情報システムが利用不可になる事態への対応プロセスを整備している病院は3割強であった。

・USBメモリ・PCの紛失といった、情報漏洩等に伴うインシデント対応プロセスは習熟度が高まっているものの、院内の医療情報システムがランサムウェア等で利用不可になった場合においても、通常通りの患者診療の継続性を担保するための態勢・計画には着手出来ていない状況が浮き彫りになっている。

<インシデントレスポンス対策の実施状況>



<業務継続計画の整備・運用、訓練・見直しの実施状況>



2. 病床規模別調査結果

< 病床規模別総評 >

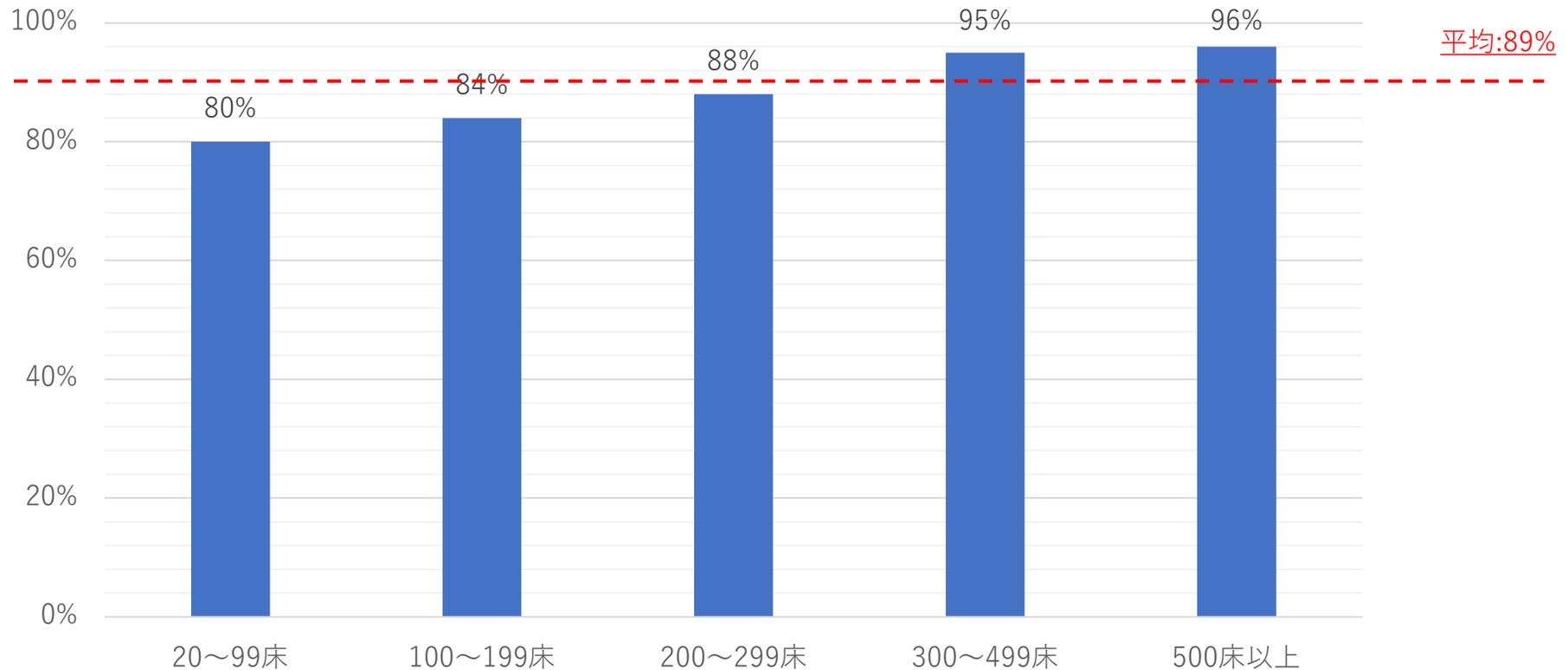
- 病床数が多い病院ほどサイバー脅威への感度が高い傾向がある。
- 厚労省やNISCが指摘したVPN製品の脆弱性対応状況、またはオフライン・オフサイトによるバックアップ取得率には、病床規模の観点より特筆すべき水準の大きな差異は見受けられない。つまり、病床規模に関係なく、いずれの病院においても脆弱性対応やバックアップ退避等、セキュリティに係る共通的な課題が存在すると考えられる。
- 院内システム担当者の配置人員数の大小は病床規模に依存しており、さらにセキュリティ監査の実施率も病床数の多い病院ほど高い傾向がある。病床数が多いほど、相対的に多くシステム担当者が在籍し、セキュリティ監査によるPDCAサイクルも機能していることがうかがえる。
- 他方で、診療系NW＝安全と考えず、サイバー保険への加入や、患者診療の継続性に影響を及ぼすサイバー攻撃による医療情報システムの利用不可を前提とした業務継続計画の整備等、予防的/復旧的な対策を適切なサイバーリスクの認識のもとで講じている病院の比率は、病床規模が小さいほど、低くなる傾向にある。
- 主な要因としては、500床未満の病院全てにおいて、年間セキュリティ予算が500万円未満と回答した病院がほぼ半数を占めていること、また同様の事態にある500床以上の大規模病院が3割強も存在している等、セキュリティ予算の一般的な不足にあると考えられる。
- セキュリティ予算が十分でないと考える病院も平均で4割強に達しており、そのなかでも病床規模が大きい病院ほど予算の不足を訴える傾向が強い。
- これらの結果を総括すると、病床の規模に関係なく、本来講じるべきサイバー対策上の共通的な課題があるにもかかわらず、予算上の制約で十分な実施が図れないことに苦悩する病院の実態が浮き彫りになっていると考えられる。

<アンケート調査内容_病床規模別(1/7)>

<サイバー攻撃への脅威>

- ・いずれの病床規模でもサイバー攻撃への脅威を感じている病院の比率は高い。
- ・病床規模が大きくなるにしたがって、サイバー脅威に危機感を感じている傾向が高くなっている。

<「サイバー脅威を感じている」と回答した病院の病床規模別割合>



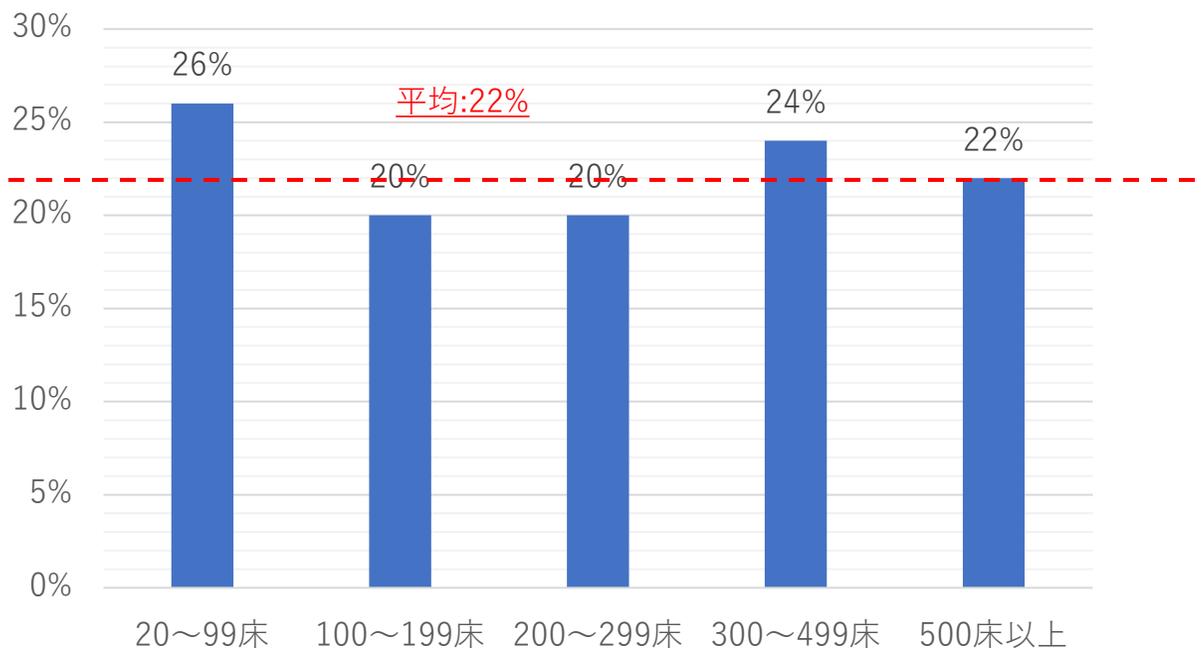
<アンケート調査内容_病床規模別(2/7)>

<脆弱性への対応>

・病床規模に関わらず、**2割程度の病院**は脆弱性が指摘されたVPN製品に対する対策を行わずに、そのまま利用を続けていることがわかる。

・未対応の理由として、一部でベンダーと対応に向けて調整中のため現時点で未実施の回答も見られたが、基本的に、**ベンダーへの依存度の高さ、診療系=安全という神話への依拠、不具合による可用性低下懸念**が主だったものとなる。

<「脆弱性が指摘されたVPN製品を利用しているが、脆弱性対応未実施と回答した病院の病床規模別割合」>



<「情報が届かない」「予算がない」以外の「未対策」の主な理由>

- ✓ ベンダー任せのため、把握していない
- ✓ ベンダーに確認したところ、問題なしと言われた
- ✓ クローズドネットワーク内で運用しているため対策不要と判断
- ✓ 現在ベンダーと調整しており、対応する予定
- ✓ 脆弱性対応により不具合が発生するリスクがあるため（可用性を重視するため）

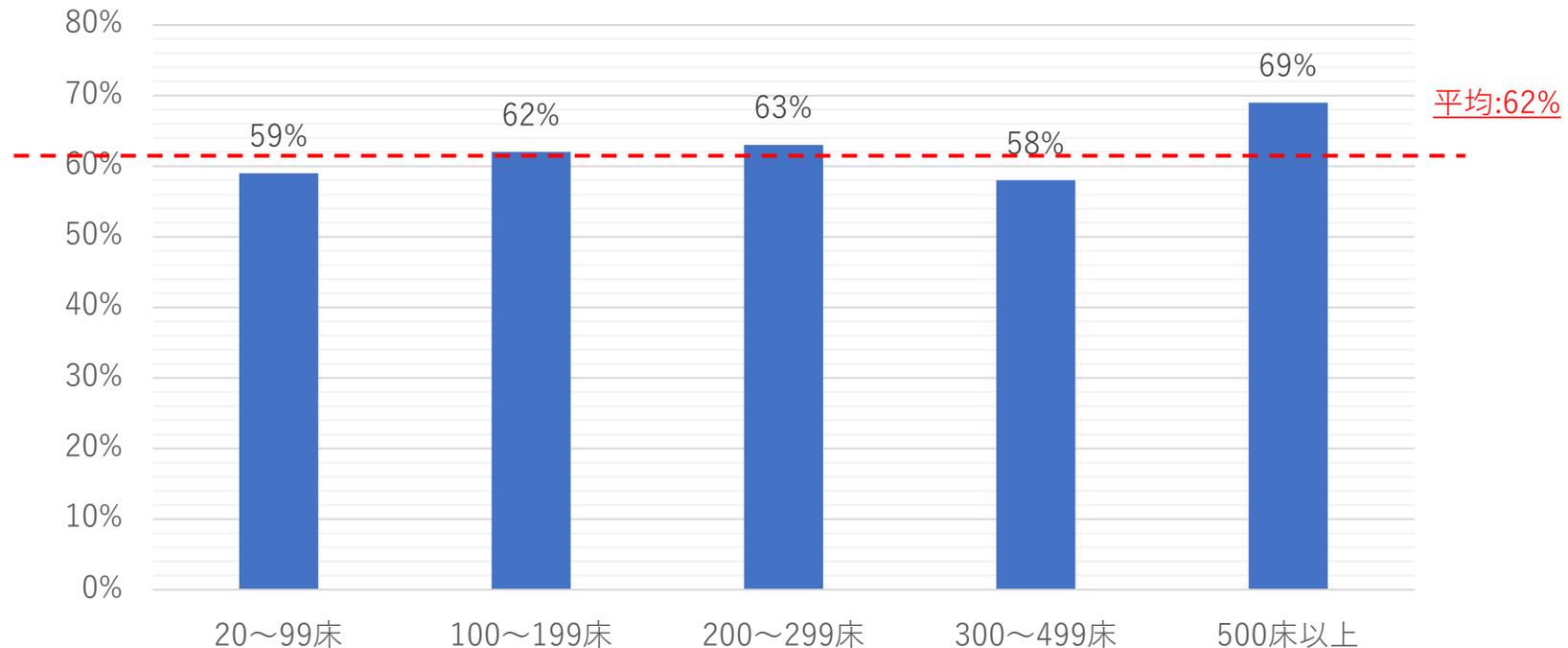
等・・・

<アンケート調査内容_病床規模別(3/7)>

<バックアップへの対応>

- ・病床規模別平均で見ると、いずれの病床でも6割前後はオフライン/オフサイトいずれかによるバックアップ退避を行っているものの、逆にいえば、3~4割前後の病院ではそのような取組が行われていないことが把握できる。
- ・500床以上の病院は相対的にIT予算があるため実施率が高いと考えられる。

<バックアップをオフライン且つ/またはオフサイトに保管していると回答した病院の病床規模別割合>



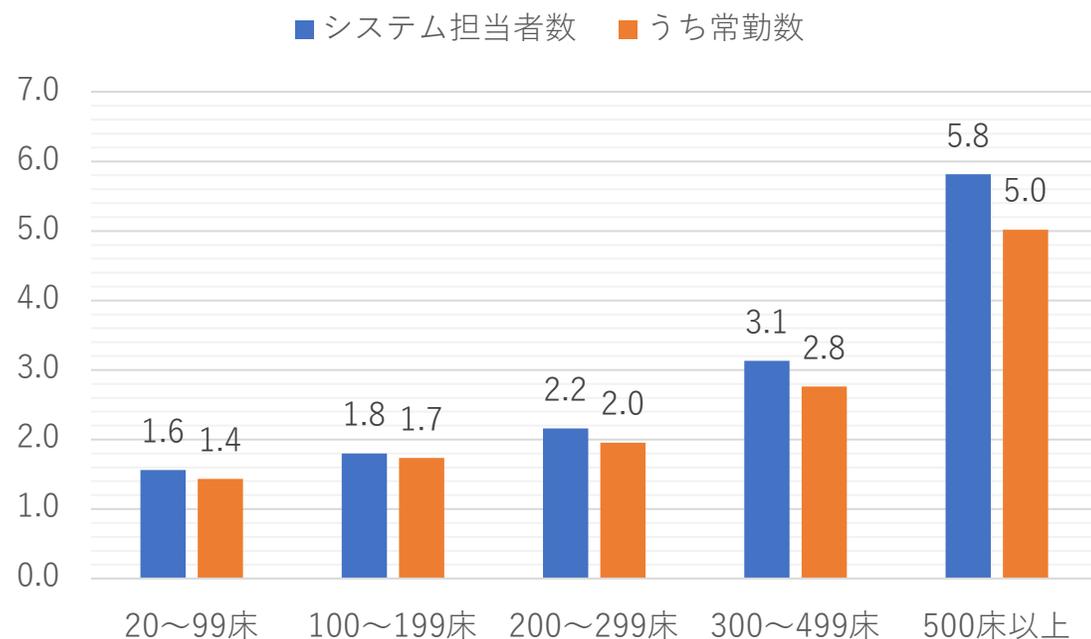
<アンケート調査内容_病床規模別(4/7)>

<セキュリティ管理～その1>

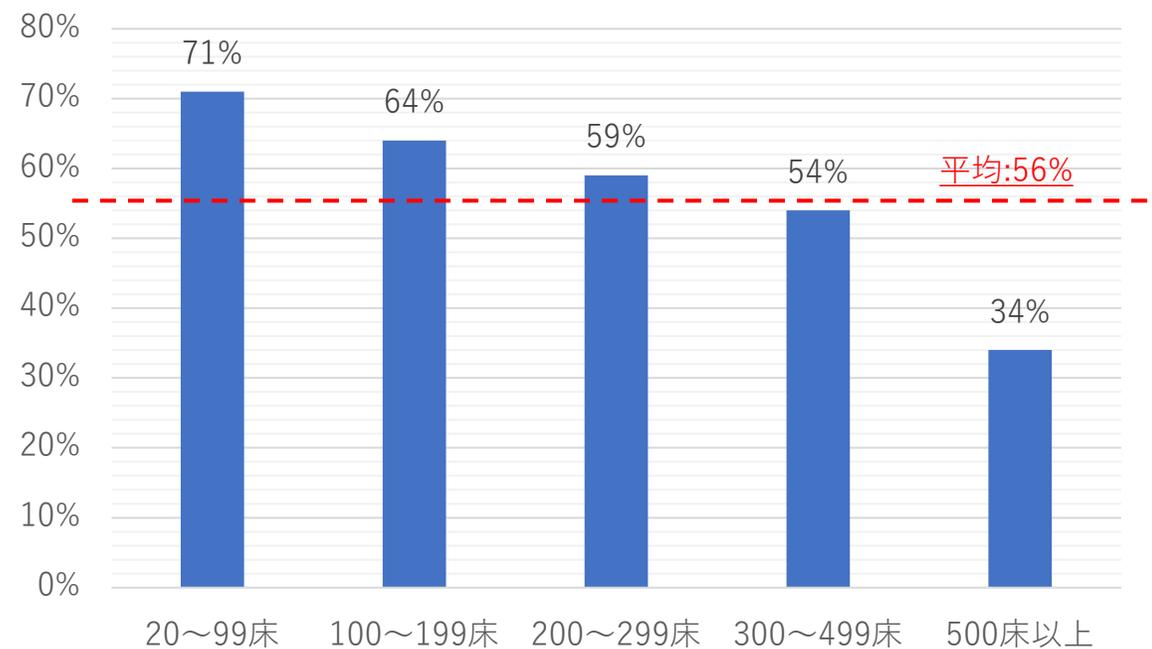
・病床規模が大きくなるにしたがい**院内システム担当者の配置人員数も増加**するが、いずれの規模でも**ほぼ常勤者により構成**されている。

・**セキュリティ監査を一度も実施したことがない病院の割合は、病床規模が小さくなるにつれて、段階的に高くなる傾向**にある。

<院内システム担当者/うち常勤者の病床規模別平均人数>



<セキュリティ監査を一度も実施したことがないと回答した病院の病床規模別割合>



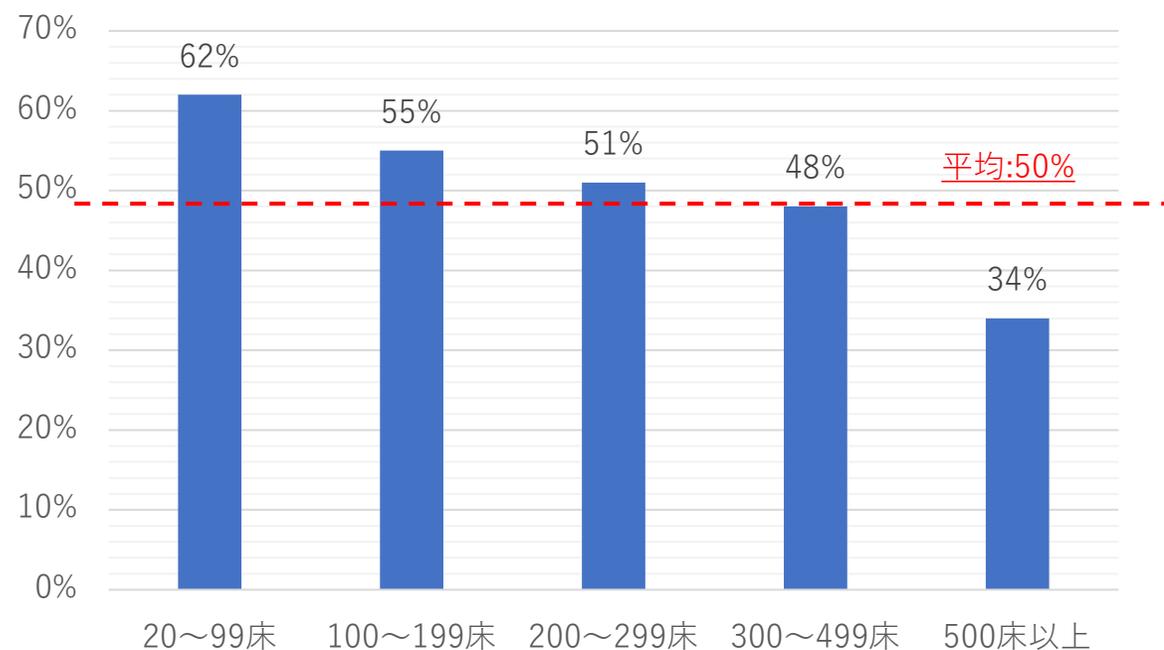
<アンケート調査内容_病床規模別(5/7)>

<セキュリティ管理～その2>

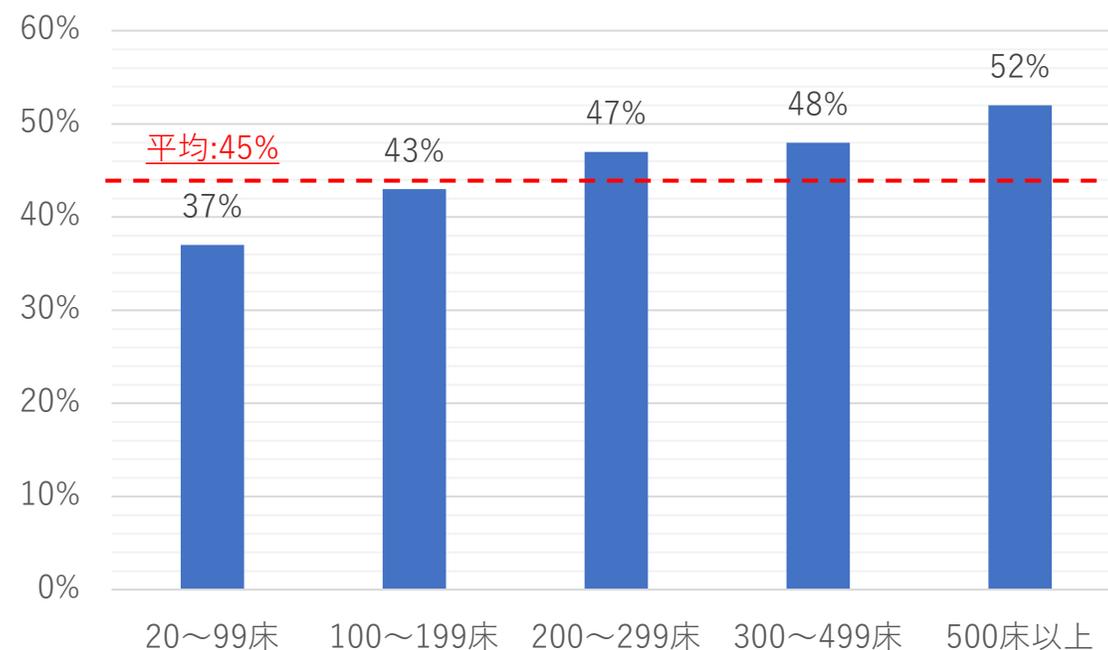
・年間セキュリティ予算が500万円未満と回答した割合は**500床未満の病床規模においてほぼ半数以上**を占めており、さらに**500床以上でも同等の回答率は3割以上**に達している。

・**セキュリティ予算の不足感は病床規模の大きさに応じて比率が高まる傾向**がみられ、特に大規模病床病院ほどその不足感が強い。

<年間セキュリティ予算を「500万未満」と回答した病院の病床規模別割合>



<セキュリティ予算が「十分でない」と回答した病院の病床規模別割合>

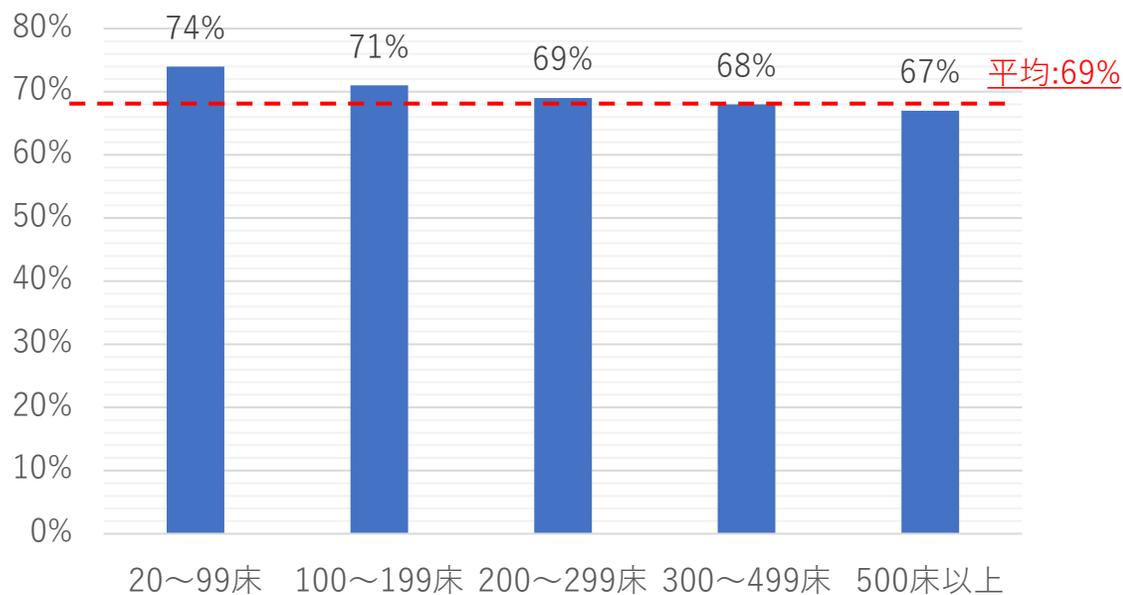


<アンケート調査内容_病床規模別(6/7)>

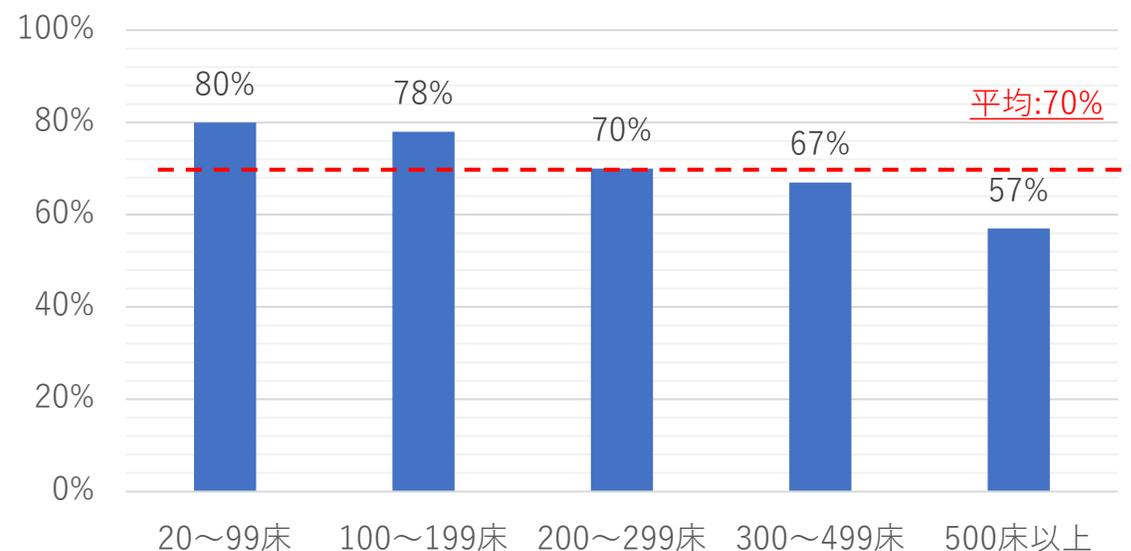
<セキュリティ管理～その3>

- ・サイバー保険の未加入比率は病床規模が小さいほど高まる傾向が見られる。院内システム（セキュリティ）担当者もセキュリティ予算も少ない病院ほど、サイバー保険という有事の事態への備えの検討が劣化する事態を示していると推測される。
- ・診療系NWの安全神話に一定以上の共感を示す病院の比率も同様に病床規模が小さいほど上昇しており、限られた人材・予算でサイバー対応を行うことの無意識の正当化のインセンティブは病床規模に応じて強まっていく傾向がうかがえる。

<サイバー保険が「未加入」病院の病床規模別割合>



<「診療系NW=安全であるという考え」に共感または条件付きで共感可能と回答した病院の規模別割合>

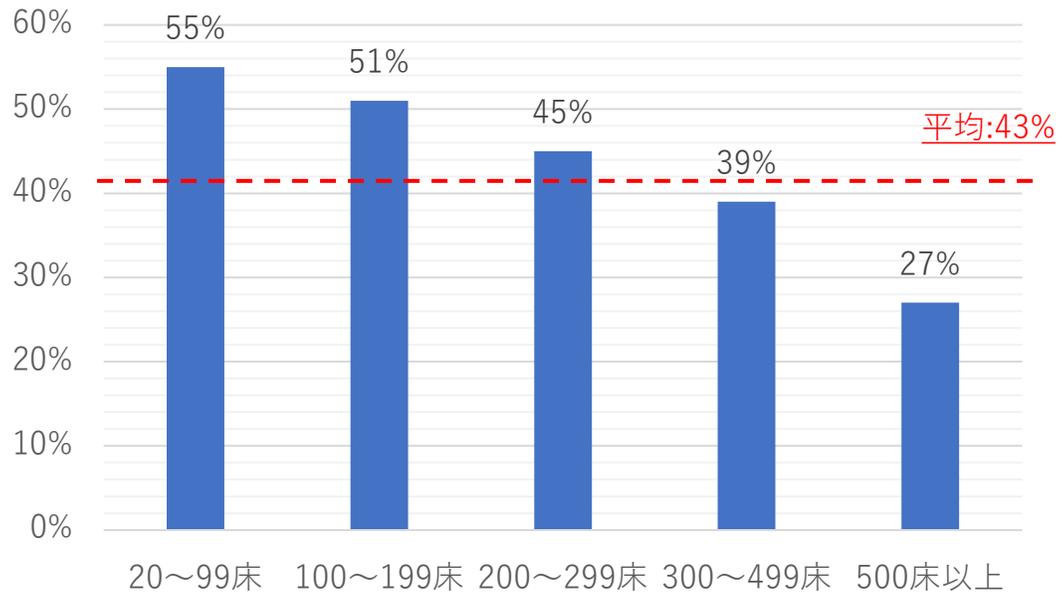


<アンケート調査内容_病床規模別(7/7)>

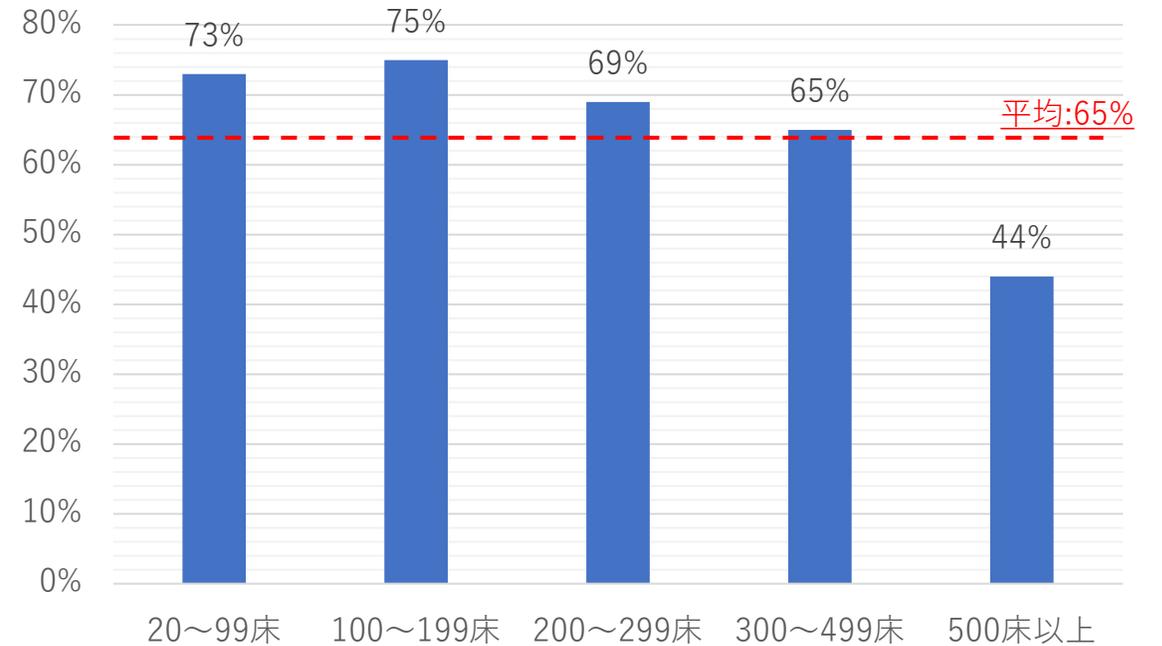
<インシデントレスポンス・BCP>

- ・基本的に**病床規模が小さいほど、インシデントレスポンス、BCPともに未対応率は増加**する傾向である。
- ・特にBCPでは、病床規模が500床未満と500床以上とで大きな懸隔がある状況である。

<インシデントレスポンス対策が「未実施」と回答した病院の病床規模別割合>



<BCPが「未対応」病院の病床規模割合>



3. 開設者別調査結果

< 開設者別総評 >

- 開設者別では、医師会、医療生協が開設者となる病院群のサイバー脅威への感度が低い傾向がある。
- 一方、厚労省やNISCが指摘したVPN製品の脆弱性未対応率は医療生協が特に高く、サイバー脅威への感度の高い私大病院でも多い状況であった。
- バックアップ退避は社福で実施率が低いが、私大法人、医療生協では対応率が高く、バックアップという復旧対策に限られたリソースを注入することで、脆弱性対応の優先度を下げている可能性がうかがえる。なお、社福は開設者平均で見た場合、サイバー保険加入率が開設者の中で最も大きく、それがバックアップオペレーションの省力化につながっている可能性も考えられる。
- セキュリティ予算が500万未満とした回答した高割合は医療生協、公益法人、医療法人の順であるが、これらの病院のうち、予算不足感を強く訴える開設者は公益法人である。一方、医療生協、医師会は500万未満の予算率が多いが、予算の不足感へ不満を覚える割合は全体平均から見ても低く、上述のサイバー脅威への感度の低さがセキュリティ投資の必要性への意識のなかに表れているともいえる。
- 診療系NWはクローズドなため安全と考える開設者病院の割合は医療生協、医療法人が高いが、公益法人は最も低い状況である。公益法人は、クローズドNWの安全性への不信の考えを持ちながらも、セキュリティ予算の不足感に悩む病院の代表例と言える。
- インシデントレスポンス・BCPともに未対応率の高い開設者は、医師会、医療法人、医療生協の順となる。全体的にシステムがサイバー攻撃で利用不可となった場合のBCP（サイバーBCP）の未対応率は開設者平均で7割弱に達しているが、医師会、医療生協の未対応率は平均値を大きく上回っている。
- 以上より、開設者別で総括すると、（医療生協はバックアップ退避率が高くはあるものの）医師会/医療生協のサイバー対応への必要性の認識および対応率が相対的に低い状況と整理できる。他方、公益法人はセキュリティ予算が少ないなかで、「診療系NWは安全である」という考えを排して、サイバー対応に取り組もうとする傾向性が高いと考えられる。

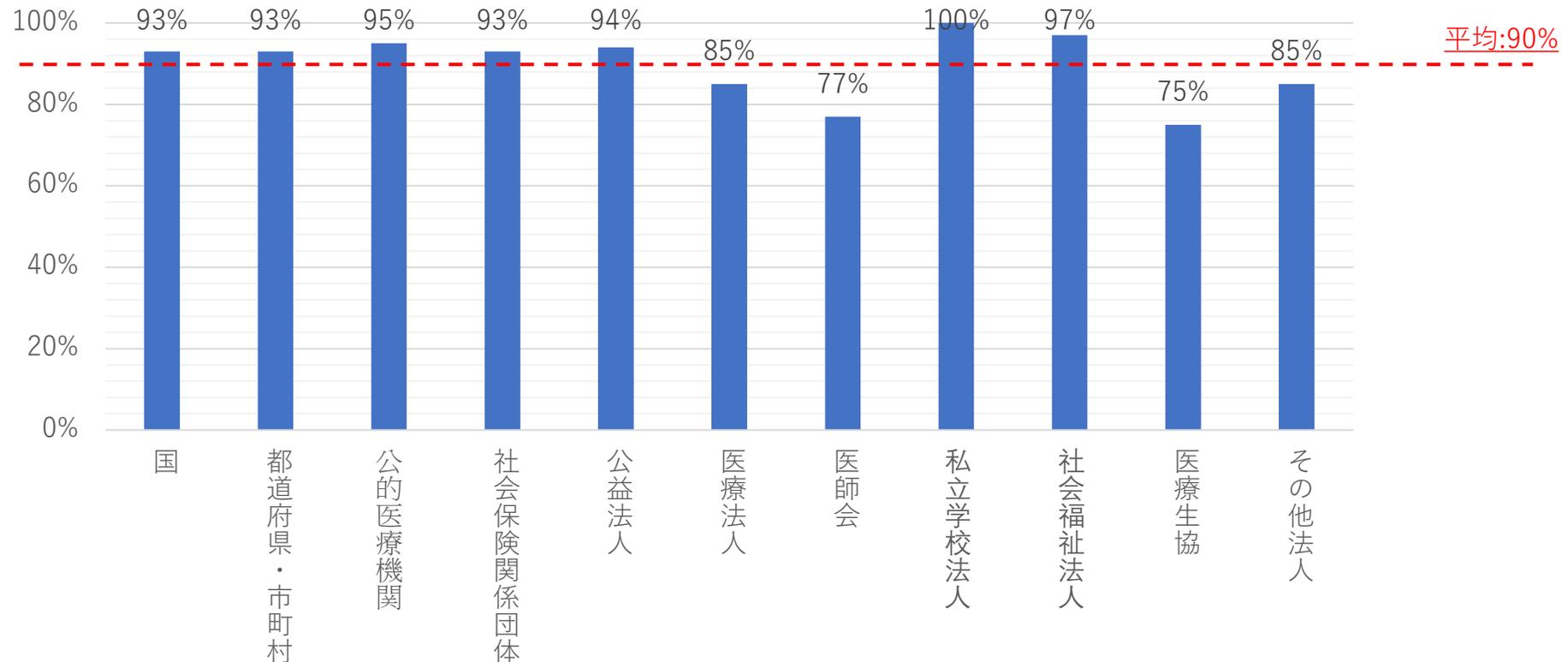
<アンケート調査内容_開設者別(1/7)>

<サイバー攻撃への脅威>

・全体平均の9割程度がサイバー脅威を感じていると回答しており、その中でも**私立大学法人は全ての回答病院(100%)が脅威ありと判断**している。

・ただし、一部の開設者（**医師会 (77%)、医療生協(75%)**）の病院では相対的にサイバー脅威への危機感が低いと言える。

<「サイバー脅威を感じている」と回答した病院の開設者別割合>



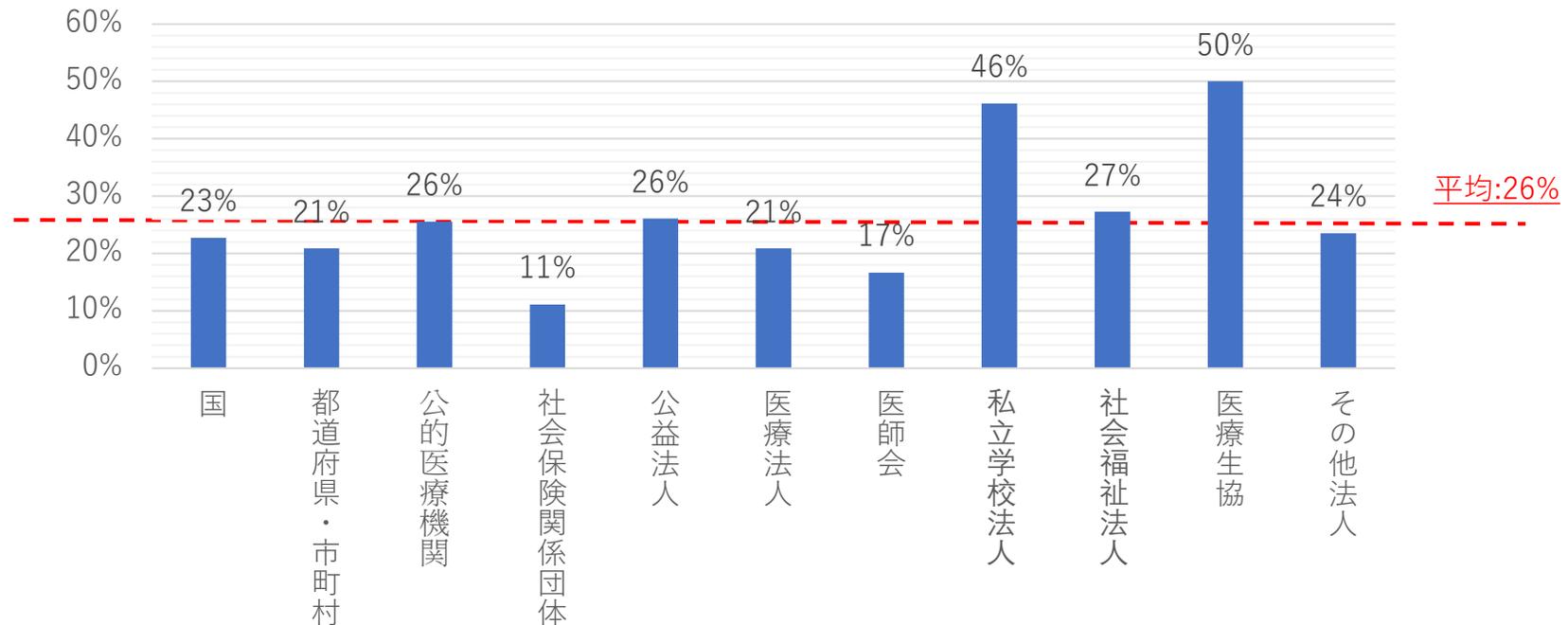
<アンケート調査内容_開設者別(2/7)>

<脆弱性への対応>

・開設者別で見ると、脆弱性が指摘されたVPN製品に対する対策を実施せず、そのまま利用を続けている割合は、**医療生協(50%)、私立大学法人(46%)**が相対的に高い。

・それ以外の開設者区分でも**平均的に2割前後は脆弱性未済のVPN製品が利用され続けている**状況である。

<「脆弱性が指摘されたVPN製品を利用しているが、脆弱性対応を実施していないと回答した病院の開設者別割合」>

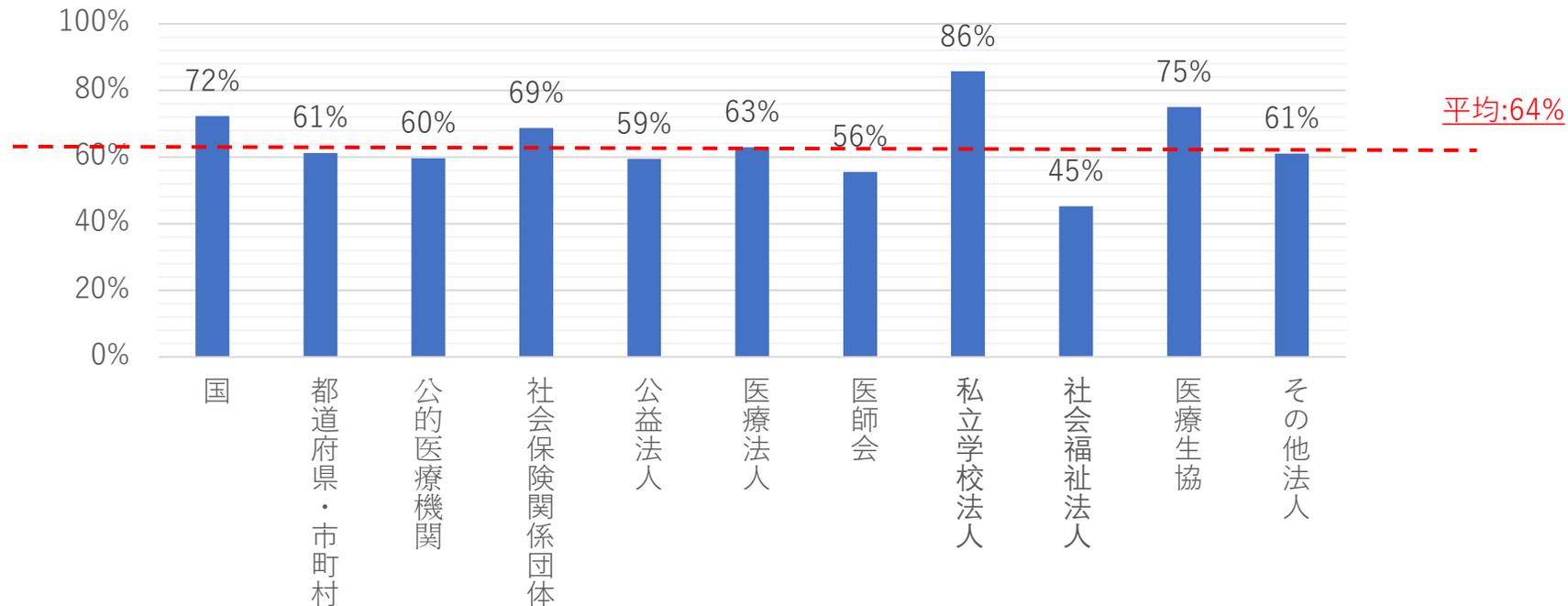


<アンケート調査内容_開設者別(3/7)>

<バックアップへの対応>

- ・開設者別平均で見ると、6割程度がバックアップ退避を行っているものの、社会福祉法人(45%)での対応率が低い状況。
- ・一方、私立大学法人(86%)、医療生協(75%)、国(72%)の開設者病院は平均値以上であり、バックアップのオフライン/オンライン対応が進んでいると言える。

<バックアップをオフライン且つ/またはオフサイトに保管していると回答した病院の開設者別割合>

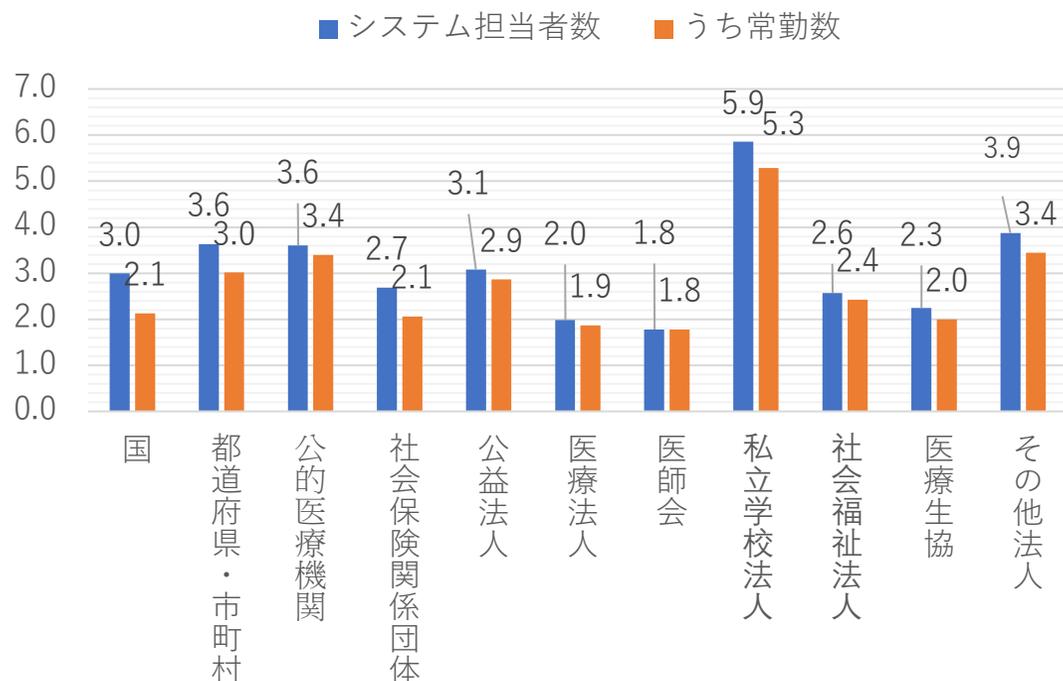


<アンケート調査内容_開設者別(4/7)>

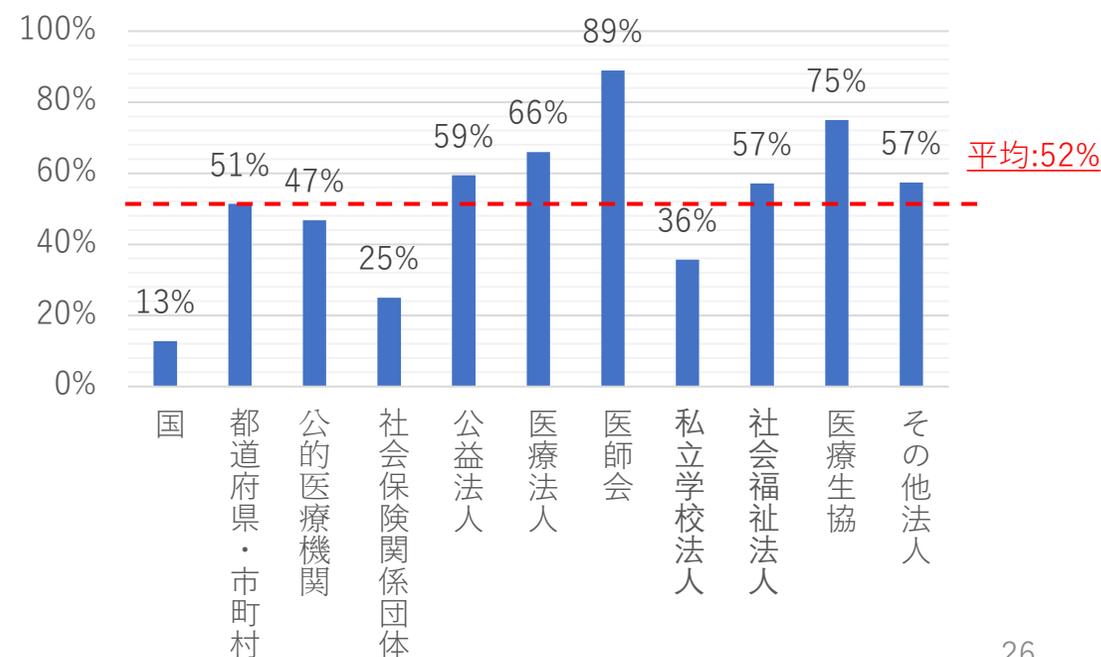
<セキュリティ管理～その1>

- ・開設者別で見ると、**私立大学法人の院内システム担当者の配置数が特に多い**。病院のみでなく大学のシステム管理も同部隊で担うことから配置人員数が多いことが理由として想定される。
- ・セキュリティ監査未実施率は**医師会 (89%)、医療生協 (75%)**が特に平均値を上回る状況である。国や社保、私大等は法定監査の一環としてセキュリティ監査を実施するため、実施率が相対的に高いと思われる。
- ・なお、システム担当者ほどの開設者でも**ほぼ常勤職員で構成**されており、**外部の専門人材のスポット受入等による、セキュリティ強化等の取組率はいずれの開設者でも低い**ことが推測される。

<院内システム担当者/うち常勤者の開設者別平均人数>



<セキュリティ監査を一度も実施したことがないと回答した病院の開設者別割合>



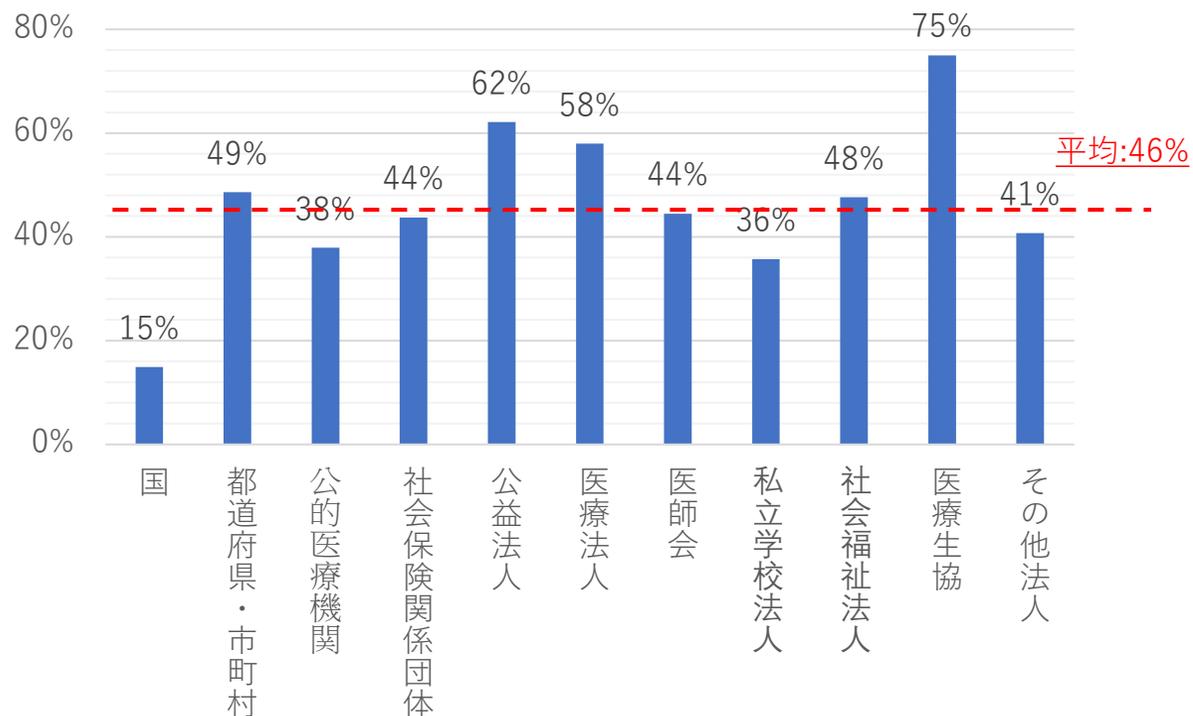
<アンケート調査内容_開設者別(5/7)>

<セキュリティ管理～その2>

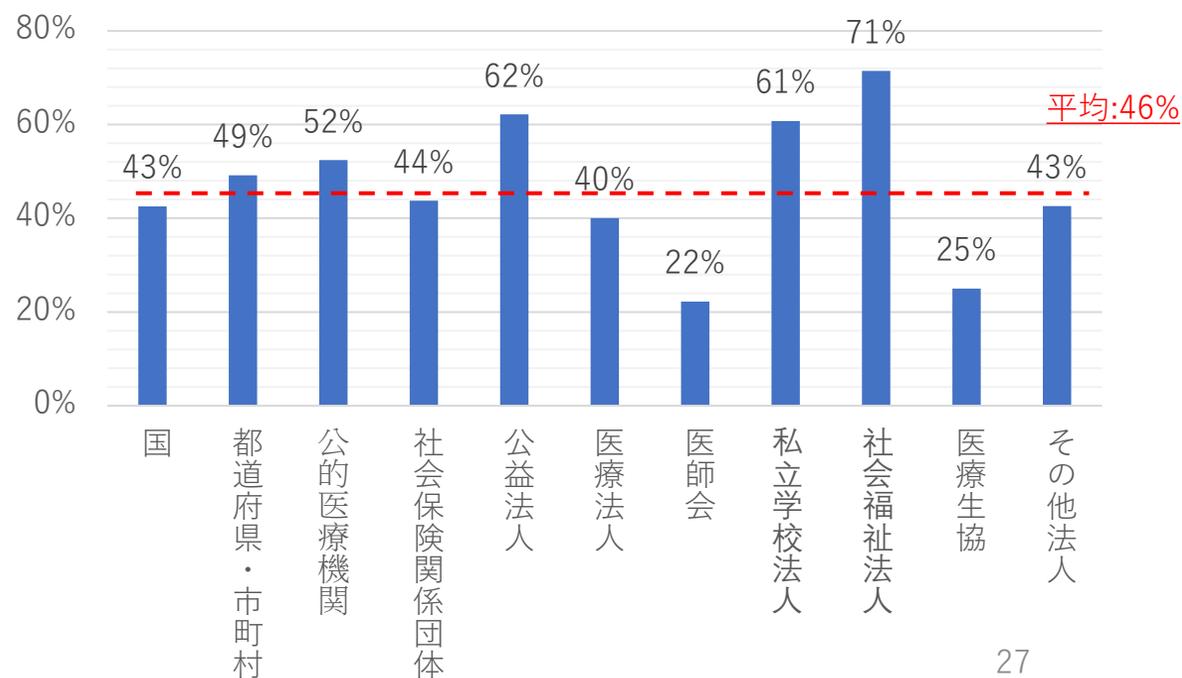
・開設者平均で見ると、特に医療生協(75%)、公益法人(62%)、医療法人(58%)の病院ではセキュリティ予算額が全体的に小さい傾向にあることがわかる。

・セキュリティ予算の不足感については、社会福祉法人(71%)、公益法人(62%)、私立大学法人(61%)の開設者病院で不十分を訴える回答率が高い。なお、医療生協(25%)、医師会(22%)では「どちらともいえない」という回答(医療生協:75%、医師会:67%)が多いため平均値を下回っており、必ずしも予算が十分と判断しているものではないと推察される。

<年間セキュリティ予算を「500万未満」と回答した病院の開設者別割合>



<セキュリティ予算が「十分でない」と回答した病院の開設者別割合>



<アンケート調査内容_開設者別(6/7)>

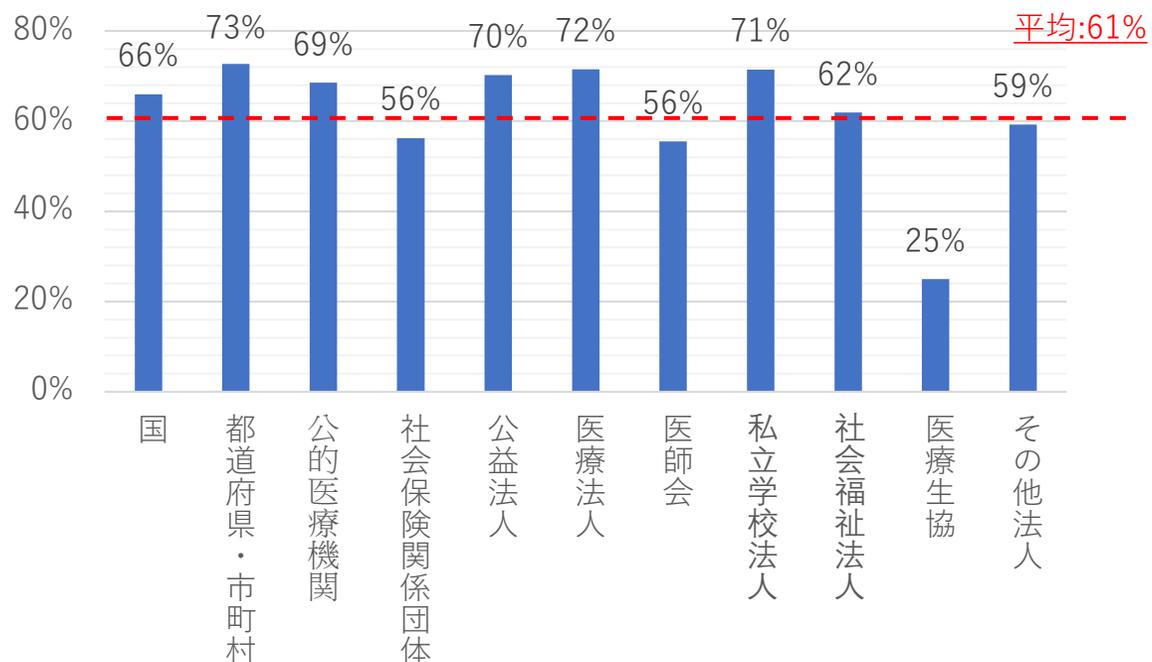
<セキュリティ管理~その3>

・都道府県・市町村 (73%)、医療法人 (72%)、私立大学法人(71%)、公益法人 (70%)のサイバー保険の未加入率が開設者平均から見ると高い。

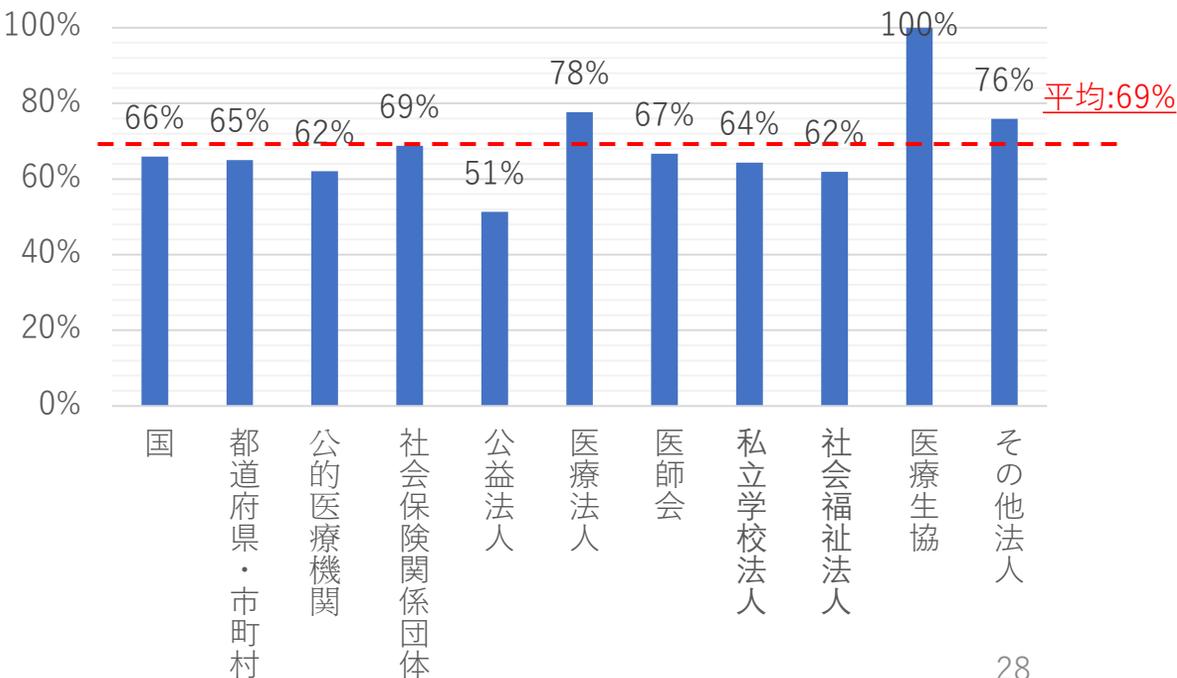
・社保 (56%)、医師会 (56%)、医療生協 (25%)の未加入率は平均値を下回っている。このうち、社保はサイバー保険加入率が高い (24%)ことによるが、ほかは「わからない」(医療生協:75%、医師会:33%)という回答結果が多いためとなる。なお、開設者全体平均で、サイバー保険に加入していると回答した割合自体は7%である。

・診療系NWはクローズドなため安全と考える開設者病院は医療生協(100%)、医療法人(78%)と高く続き、一方、公益法人 (51%)はそのような考え型が希薄であると考えられる。

<サイバー保険が「未加入」病院の開設者別割合>



<「診療系NW = 安全であるという考え」に共感または条件付きで共感可能と回答した病院の開設者別割合>

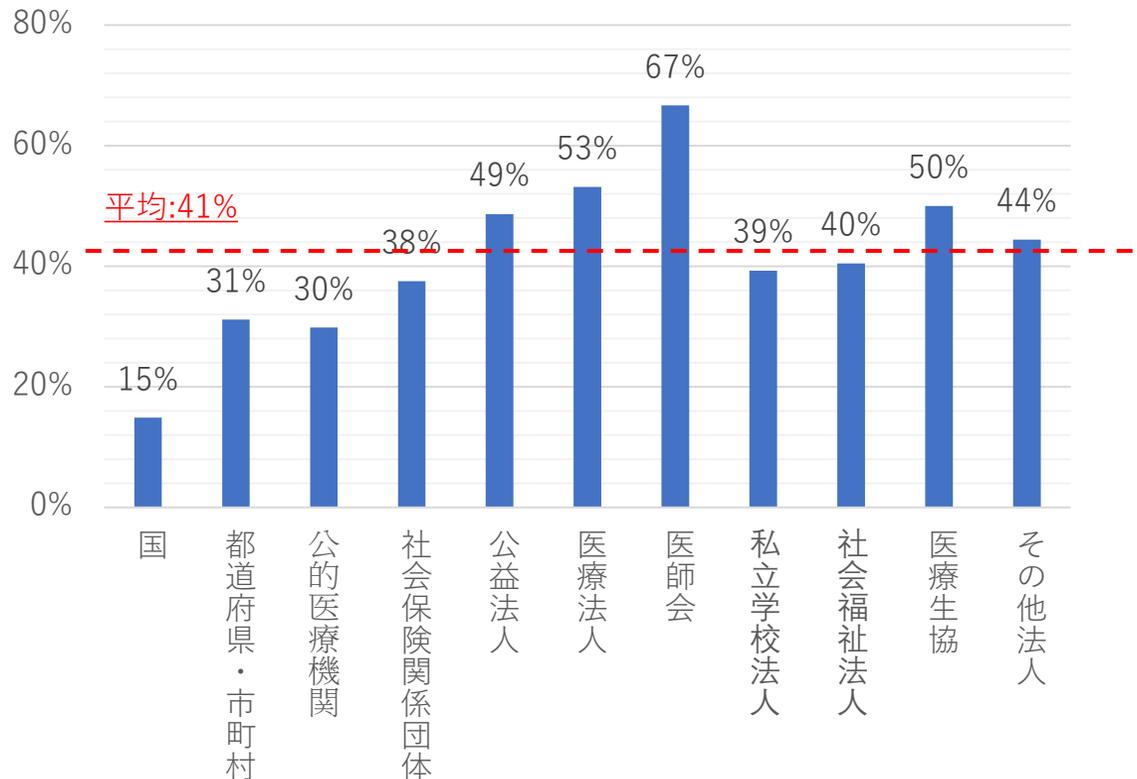


<アンケート調査内容_開設者別(7/7)>

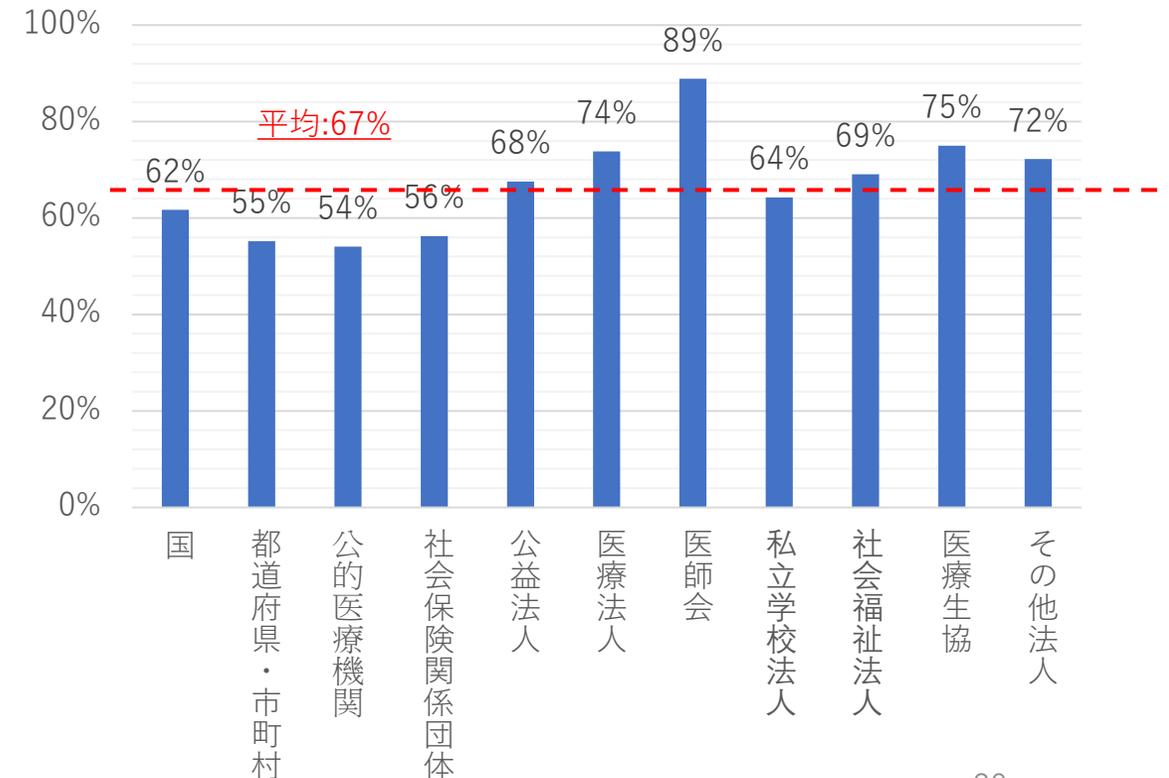
<インシデントレスポンス・BCP>

- ・インシデントレスポンス・BCPともに未対応率の高い開設者は、**医師会 (67%/89%)**、**ついで医療法人 (53%/74%)**となる。
- ・インシデントレスポンス対応率が高い開設者でも、**BCP未対応率は平均的に半数以上**を占めており、医療情報システムが利用不可になった場合の診療継続計画の整備は全体的に十分でない。

<インシデントレスポンス対策が「未実施」と回答した病院の開設者別割合>



<BCPが「未対応」病院の開設者別割合>



END