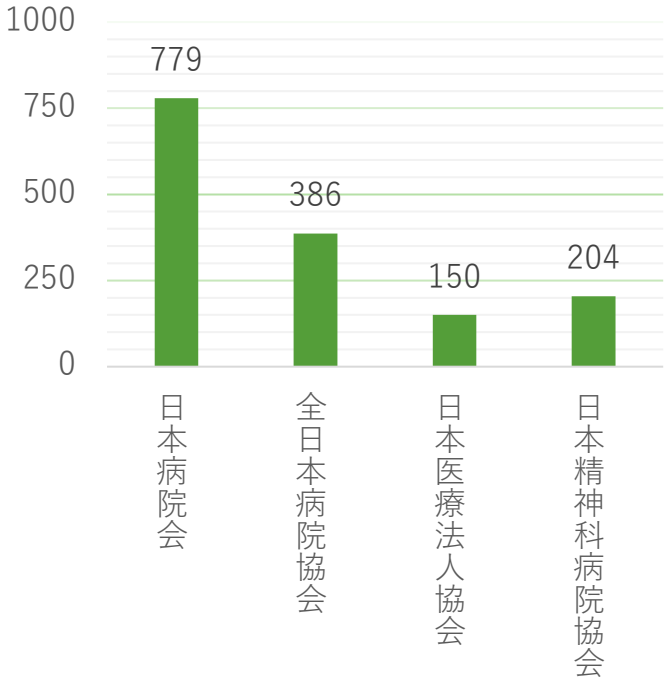
一般社団法人医療ISAC

四病院団体協議会
セキュリティアンケート調査結果

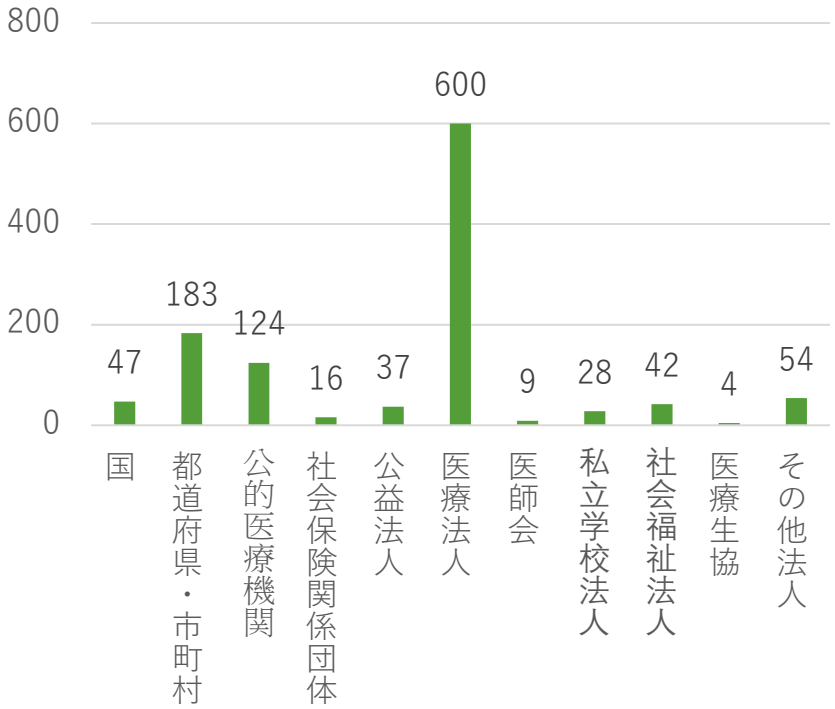
調査対象

- 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%

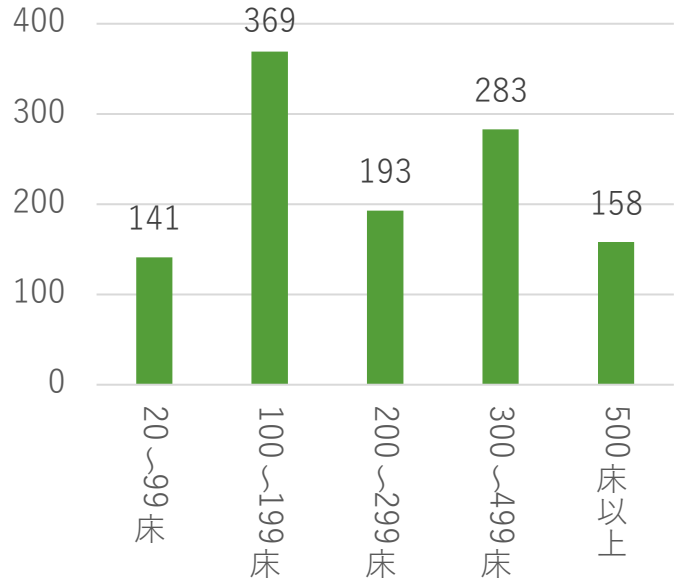
＜団体別内訳＞



＜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。

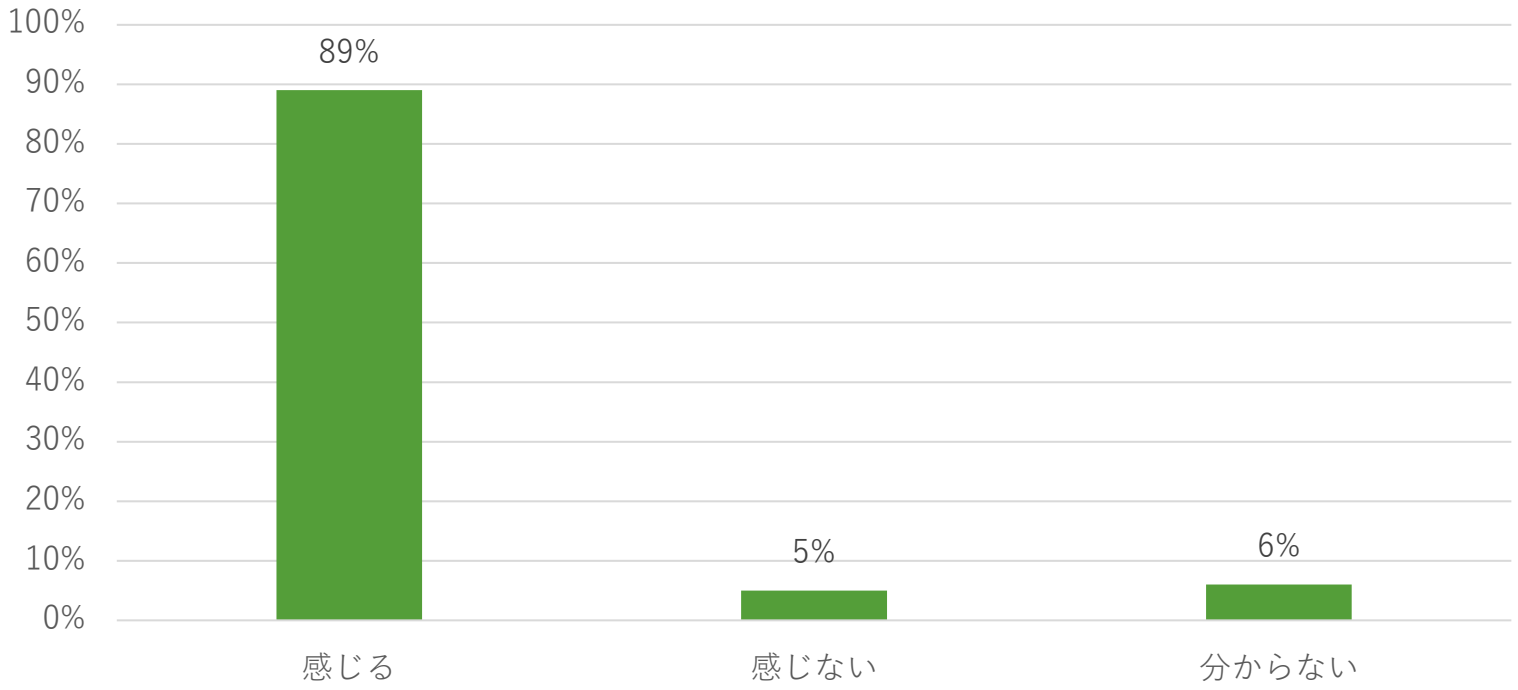
- セキュリティ事故発生時のインシデントレスポンスはUSBメモリ紛失等、情報漏えい等への対応を通して病院として習熟度が高まっている。
- しかしながら、患者診療の前提となる医療情報システムが利用不可になった場合の業務継続計画、つまりランサムウェアの被害を受け、**診療系の医療情報システムが利用不可になった場合に患者診療を適切な水準で維持するための計画・態勢整備を行えている回答病院は3割程度**であった。

＜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＞

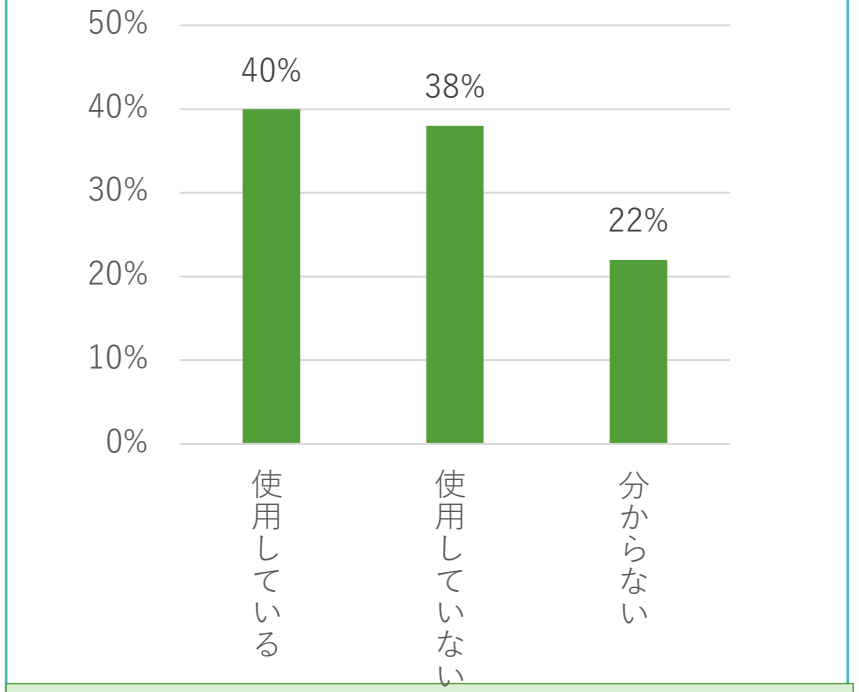


＜アンケート調査内容_全体結果(2/7)＞

＜脆弱性への対応＞

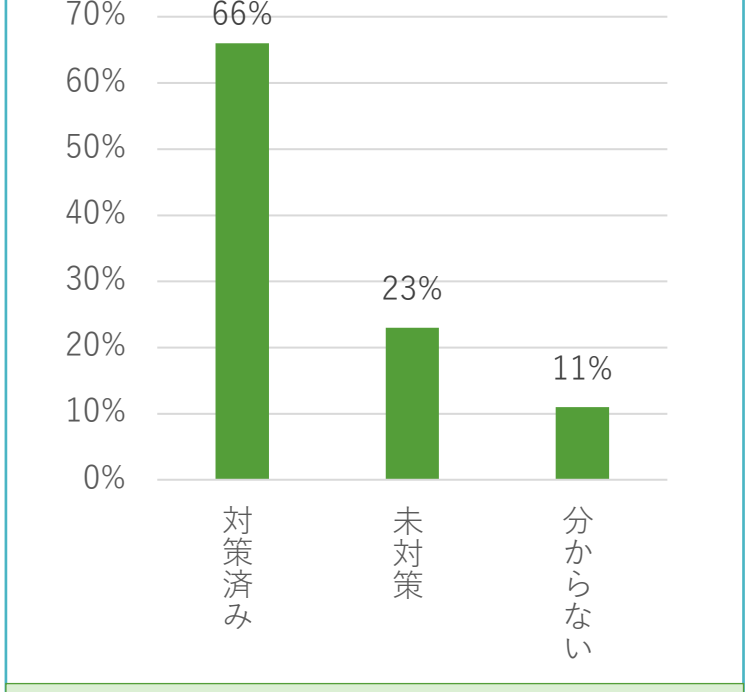
・NISCや厚労省が脆弱性を指摘したVPN製品・ソリューションを使用する病院は4割程度。
・そのうちの6割以上は脆弱性への対応を行っているが、状況不明も含めれば**未対応が3割強以上**を占めている。
・未対応の理由としては、**情報が届いていないこと（知らなかった）、予算不足であったことが回答の半分弱**を占め、さらにその他の理由には「外部と接続していない」「クローズドネットワークで運用しているため」「パッチ適用による不具合が懸念されるため」等が多く見受けられた。

Q1



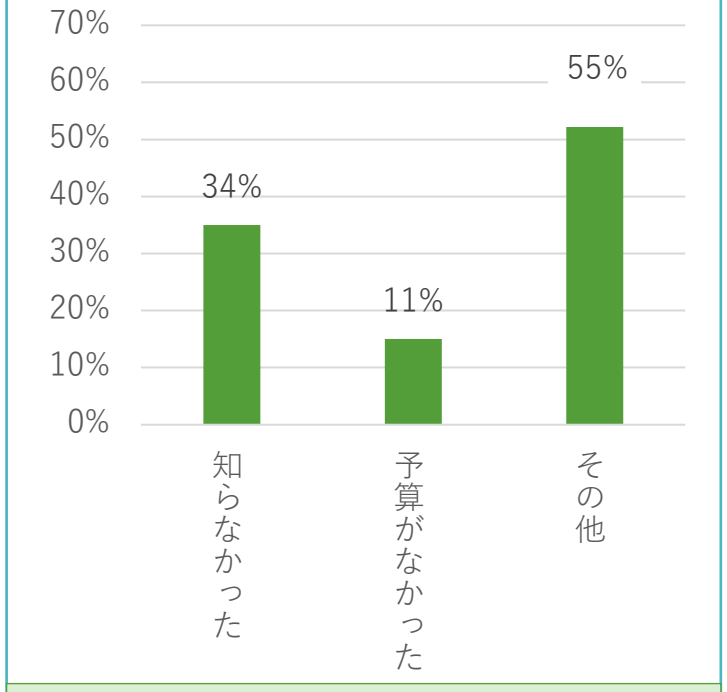
脆弱性指摘のあったVPN使用状況

Q２



Q1で「使用している」場合の脆弱性対応状況

Q３



Q2で「未対応」とした場合の理由

＜アンケート調査内容_全体結果(3/7)＞

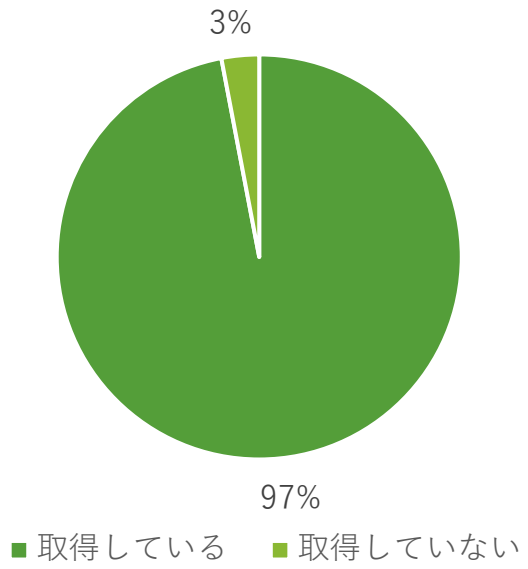
＜バックアップへの対応＞

・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。

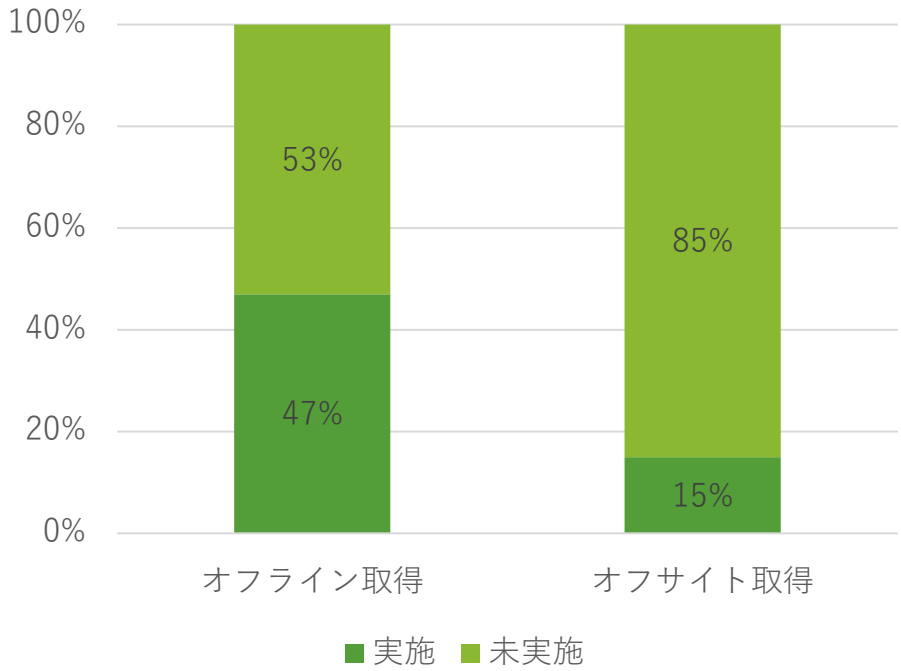
・そのうち、**バックアップをオフライン取得している割合は5割を少し下回り、オフサイト（外部施設）へ保管している割合は1割強程度**である。

・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＞

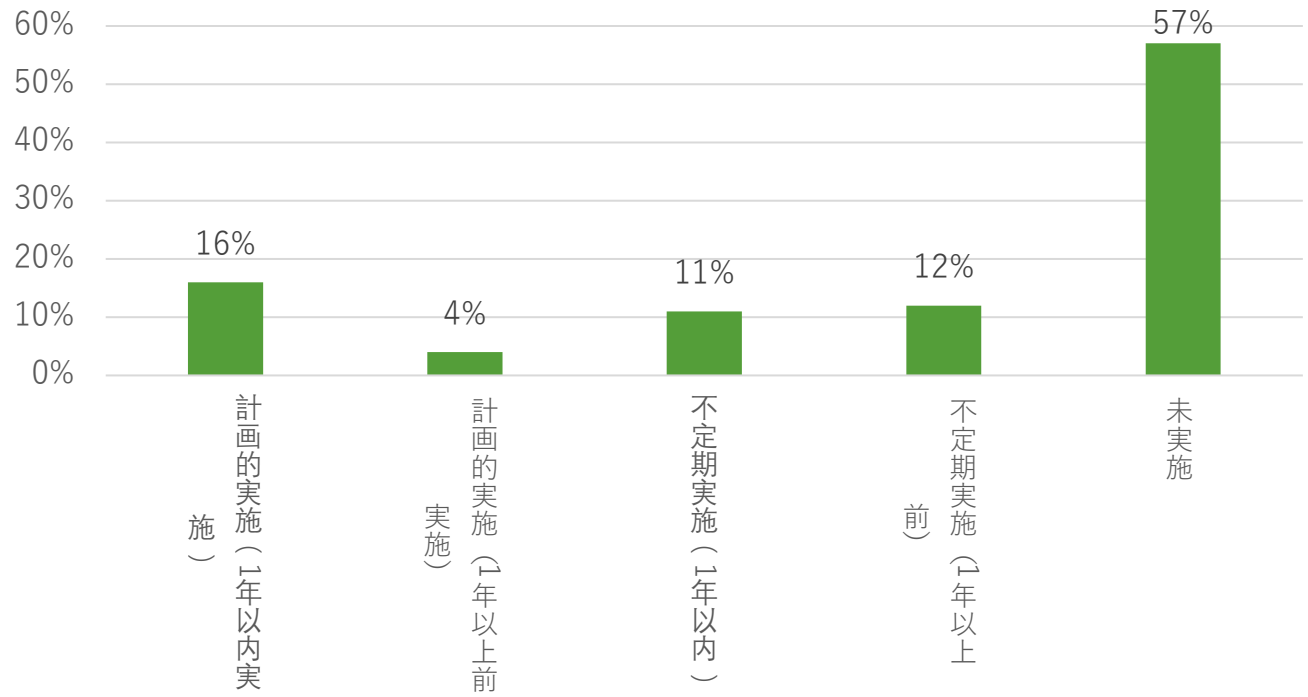
・院内システム担当者数は全体平均で3人弱で、そのうち常勤者もほぼ同水準であるため、専門的なセキュリティ知見のある外部企業からの要員派遣等、**外部の目線の導入による環境見直し等が発生しづらい**体制でシステム管理が行われていることが推測される。

・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＞



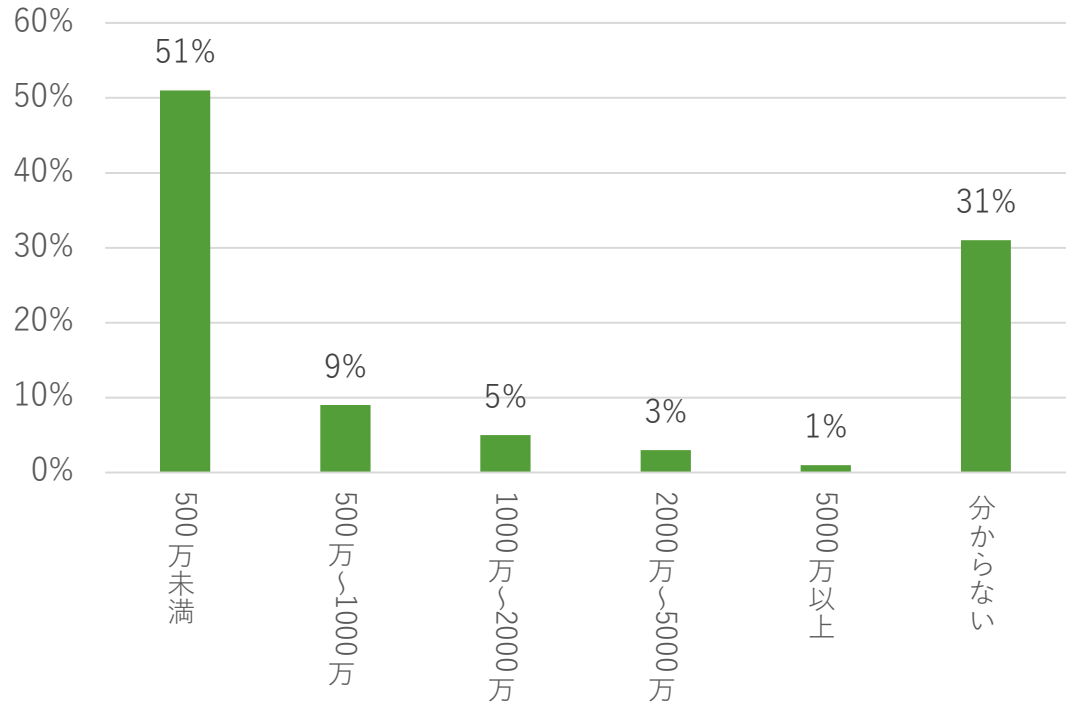
＜アンケート調査内容_全体結果(5/7)＞

＜セキュリティ管理～その２＞

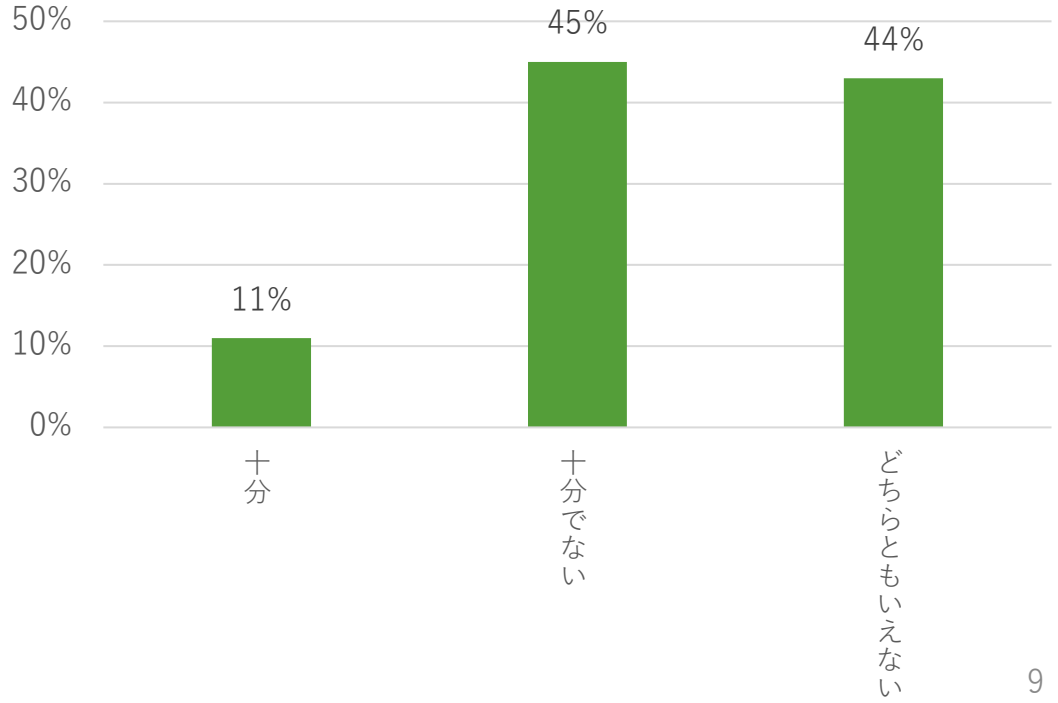
・年間のセキュリティ予算が500万円未満と回答した病院の割合は5割強、セキュリティ予算が十分でないと回答する割合もほぼ5割弱であり、**半数程度の病院は現在のセキュリティ予算が十分でない**と考えている。

・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)＞

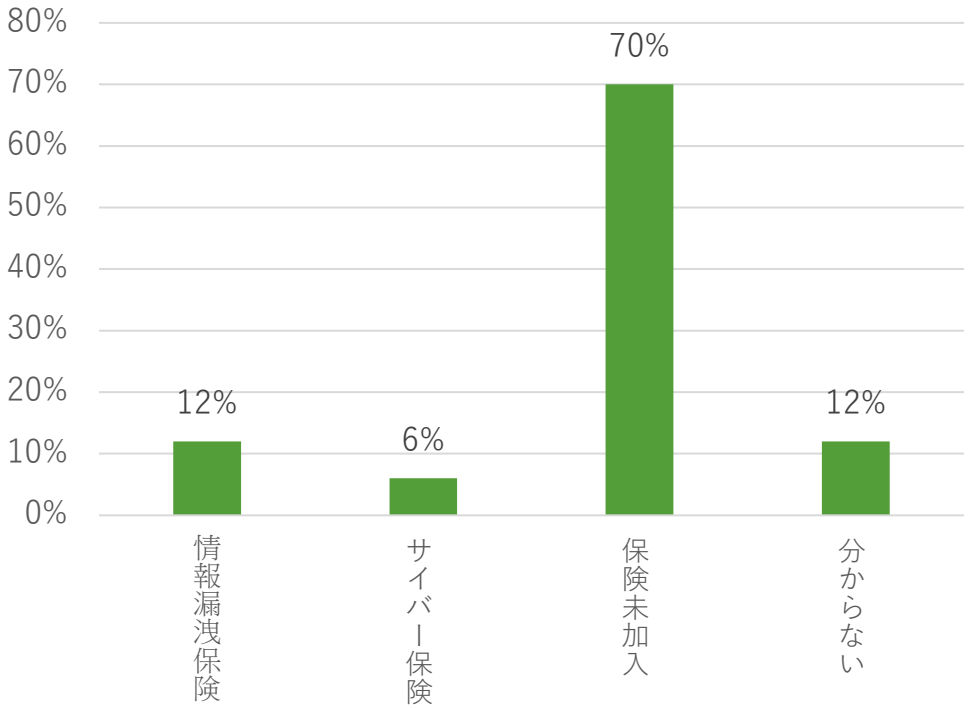
＜セキュリティ管理～その３＞

・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。

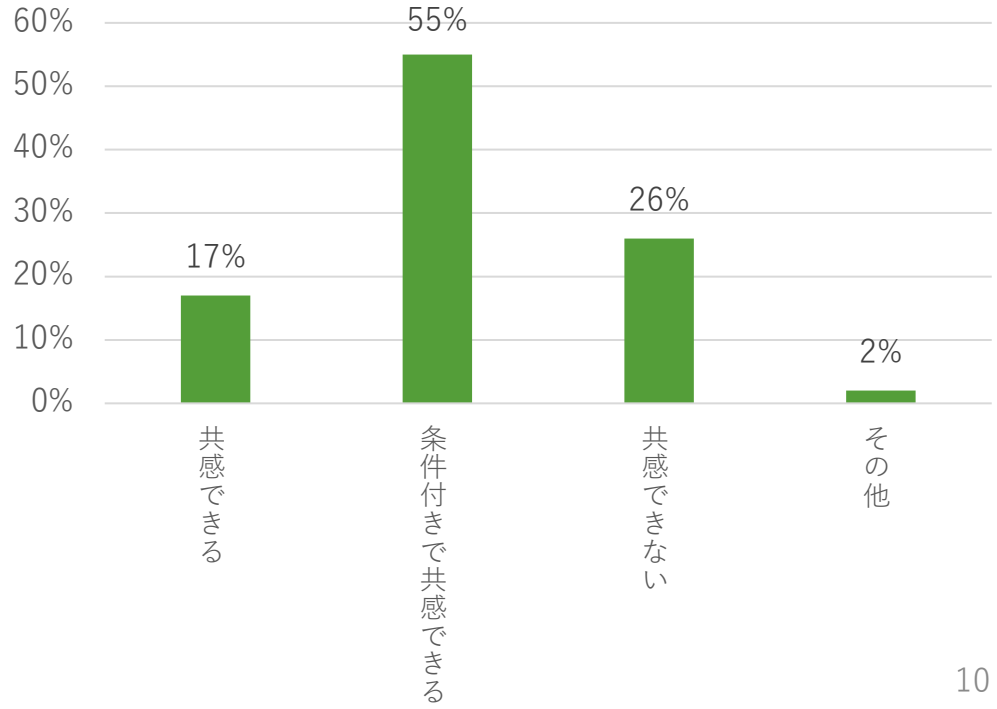
・また、「診療系ネットワークは外部ネットワークと遮断されているため安全である」という考えに何らかの形で**共感すると回答した病院の割合も7割以上**にのぼっている。

・**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＞



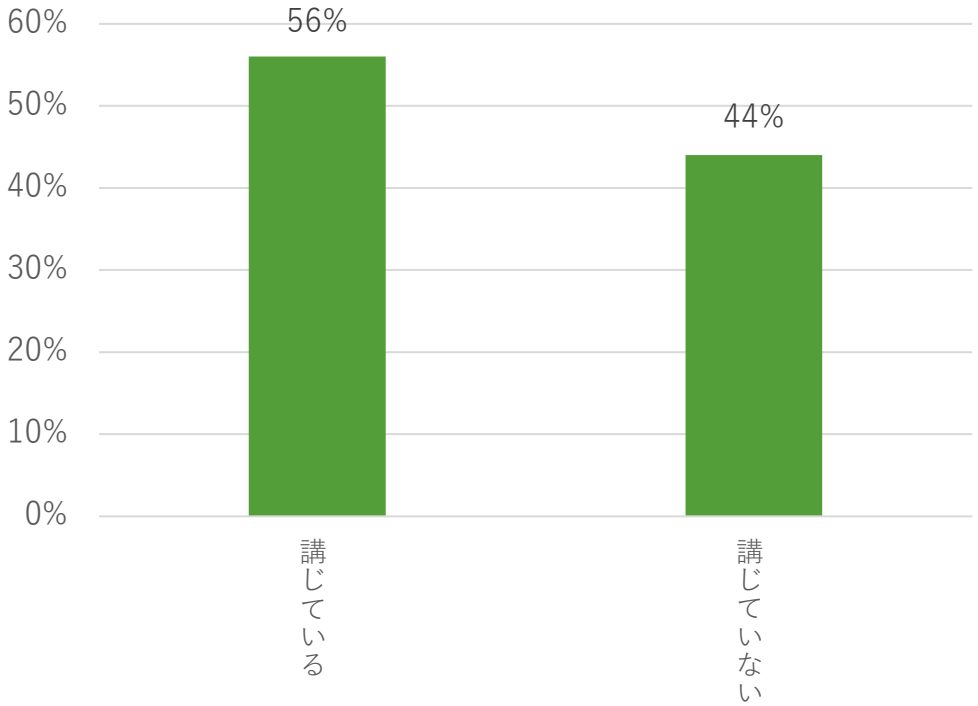
＜アンケート調査内容_全体結果(7/7)＞

＜インシデントレスポンス・BCP＞

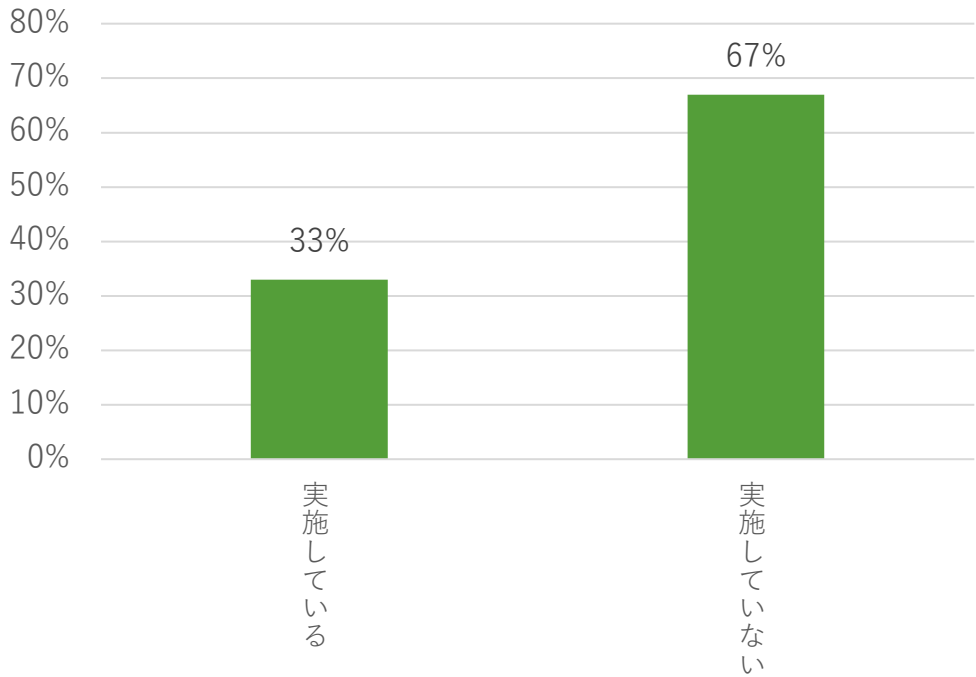
・セキュリティインシデントの被害最小化プロセスを整備している病院の回答割合は6割弱である一方、患者診療等の院内業務の前提となる医療情報システムが利用不可になる事態への対応プロセスを整備している病院は3割強であった。

・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。**

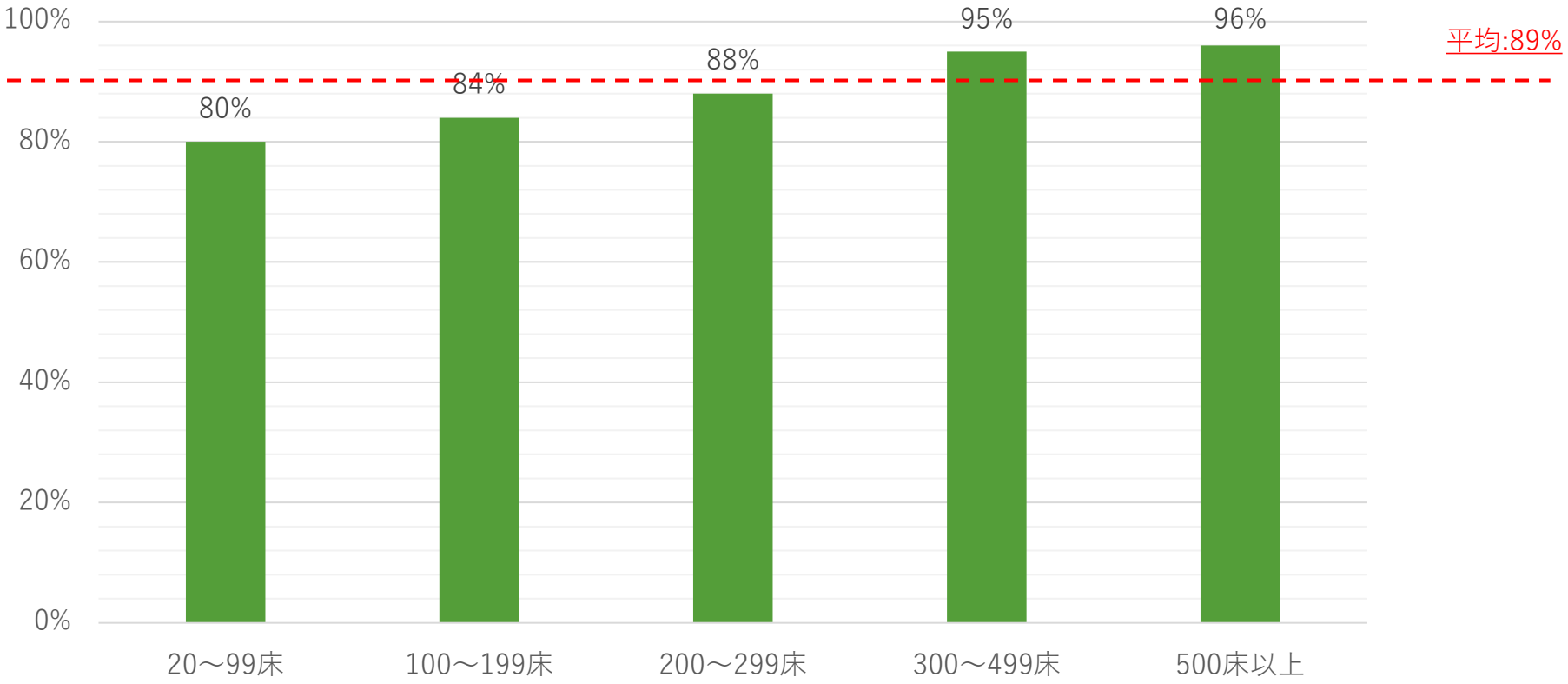
- 主な要因としては、500床未満の病院全てにおいて、年間セキュリテイ予算が500万円未満と回答した病院がほぼ半数を占めていること、また同様の事態にある500床以上の大規模病院が3割強も存在している等、**セキュリティ予算の全般的な不足にある**と考えられる。
- セキュリテイ予算が十分でないと考える病院も平均で4割強に達しており、そのなかでも**病床規模が大きい病院ほど予算の不足を訴える傾向が強い**。

- 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＞



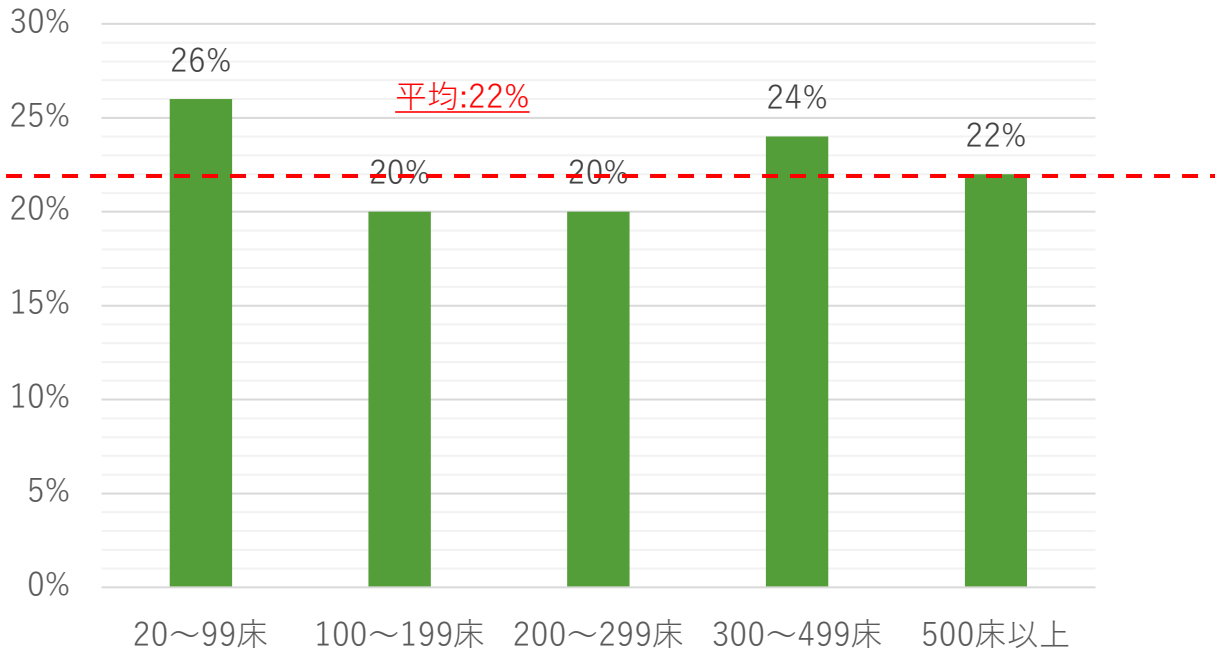
＜アンケート調査内容_病床規模別(2/7)＞

＜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・・・

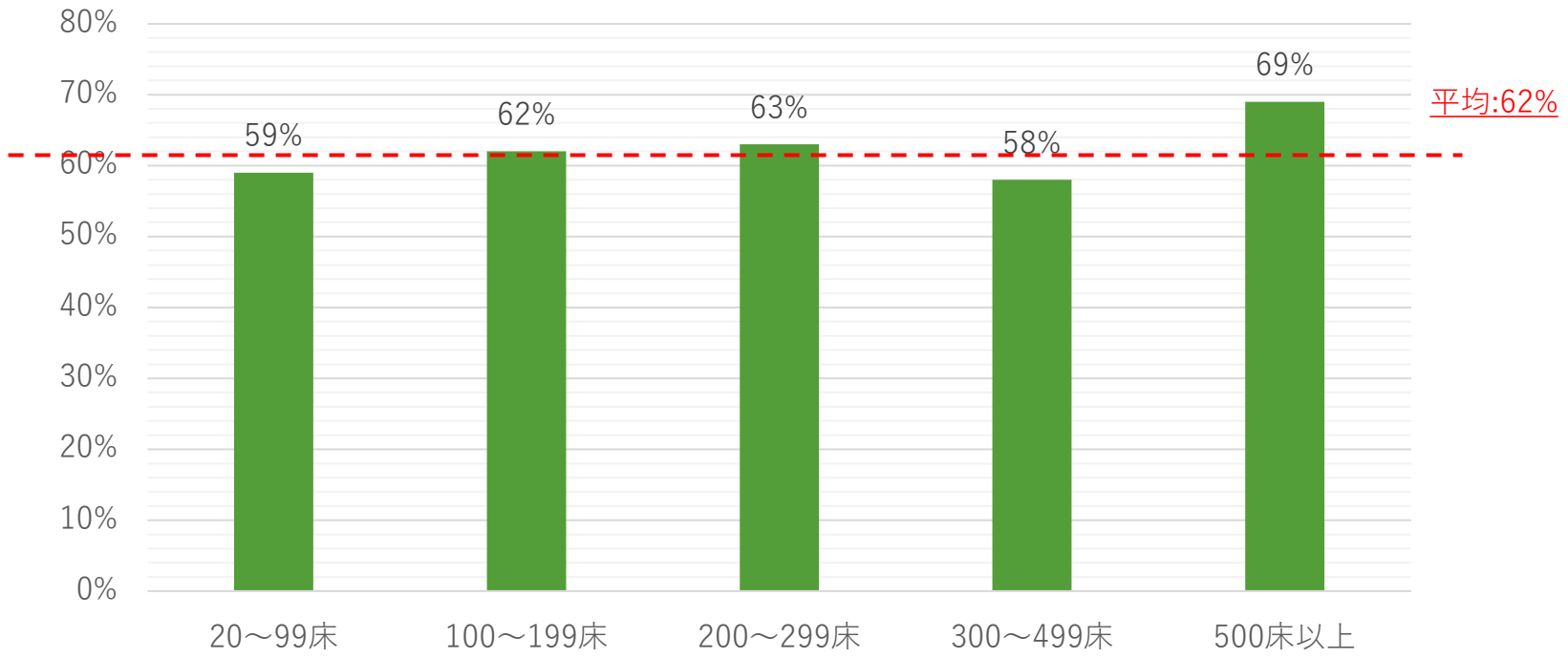
＜アンケート調査内容_病床規模別(3/7)＞

＜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＞



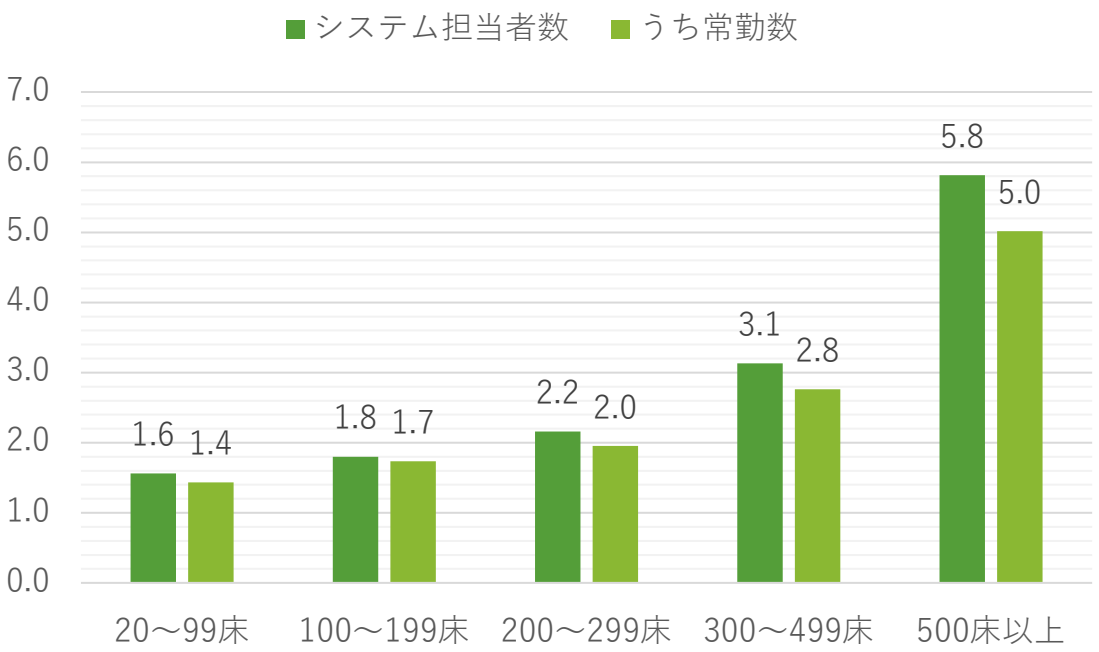
＜アンケート調査内容_病床規模別(4/7)＞

＜セキュリティ管理～その１＞

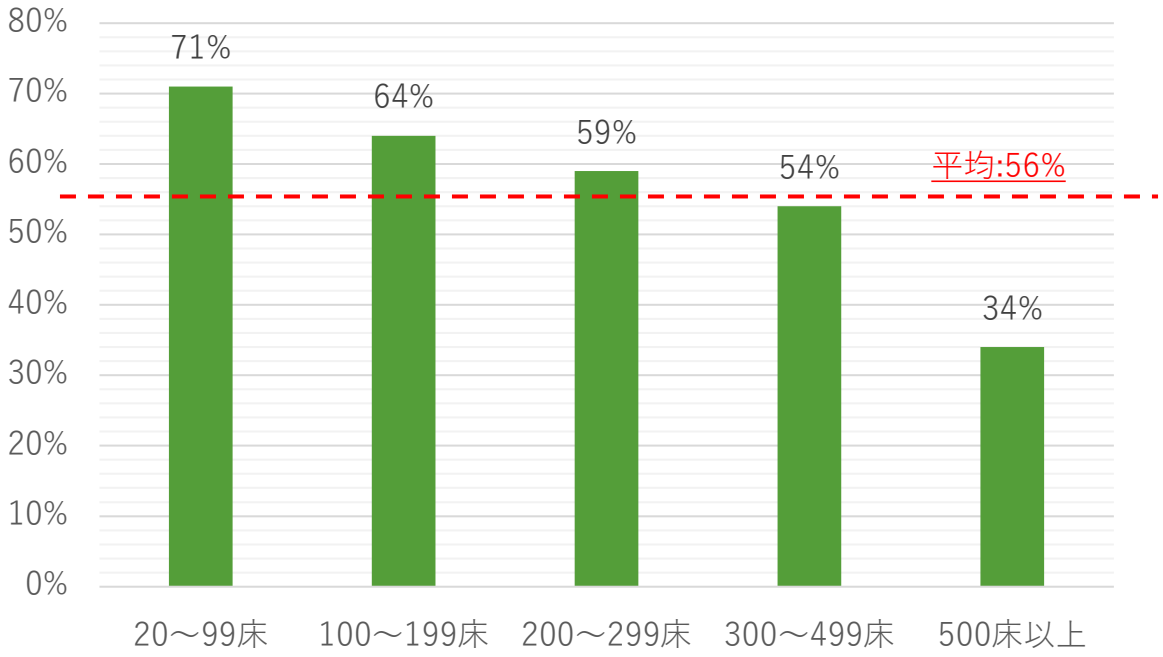
・病床規模が大きくなるにしたがい**院内システム担当者の配置人員数も増加**するが、いずれの規模でも**ほぼ常勤者により構成**されている。

・**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＞



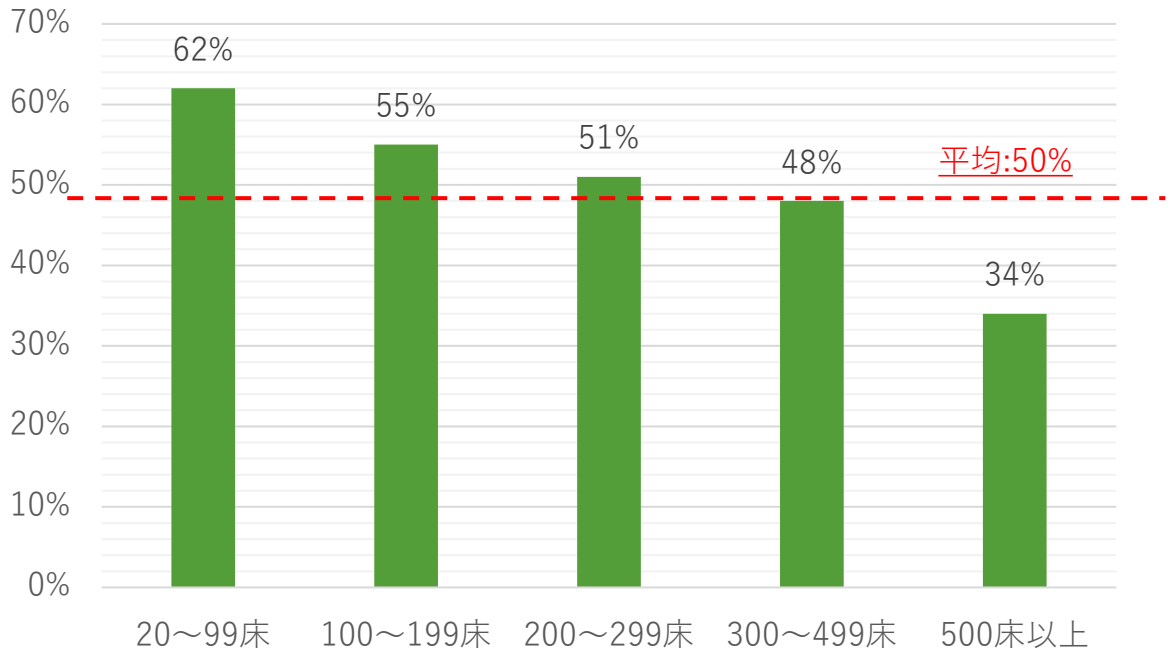
＜アンケート調査内容_病床規模別(5/7)＞

＜セキュリティ管理～その２＞

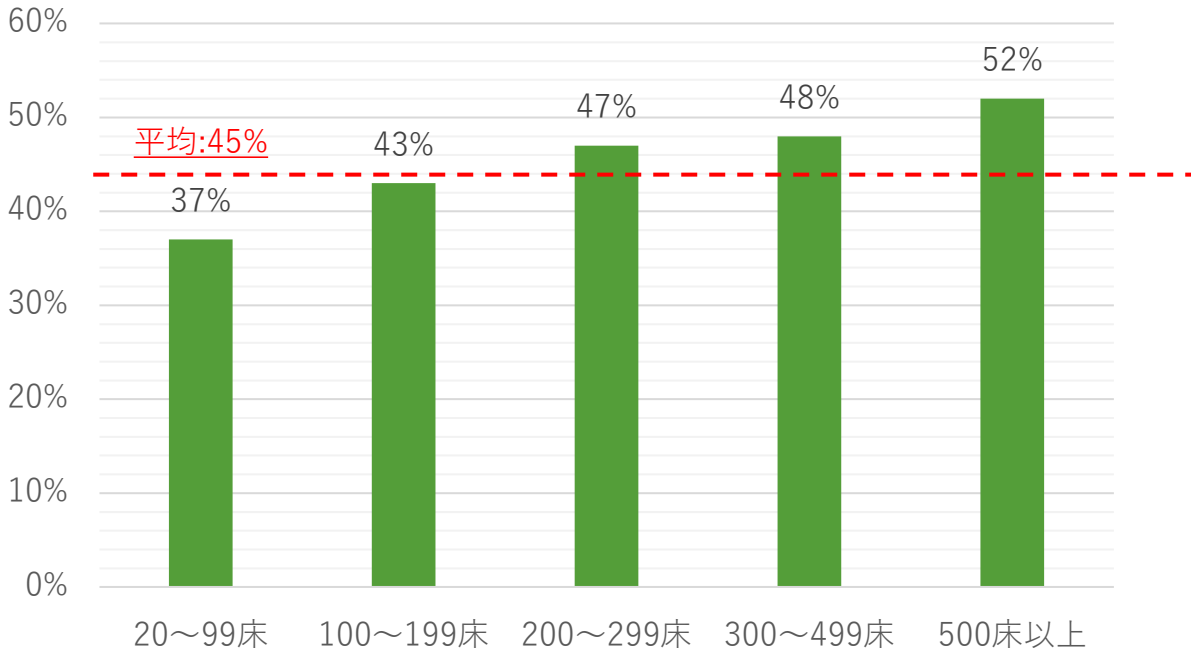
・年間セキュリティ予算が500万円未満と回答した割合は**500床未満の病床規模においてほぼ半数以上**を占めており、さらに**500床以上でも同等の回答率は3割以上**に達している。

・**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＞



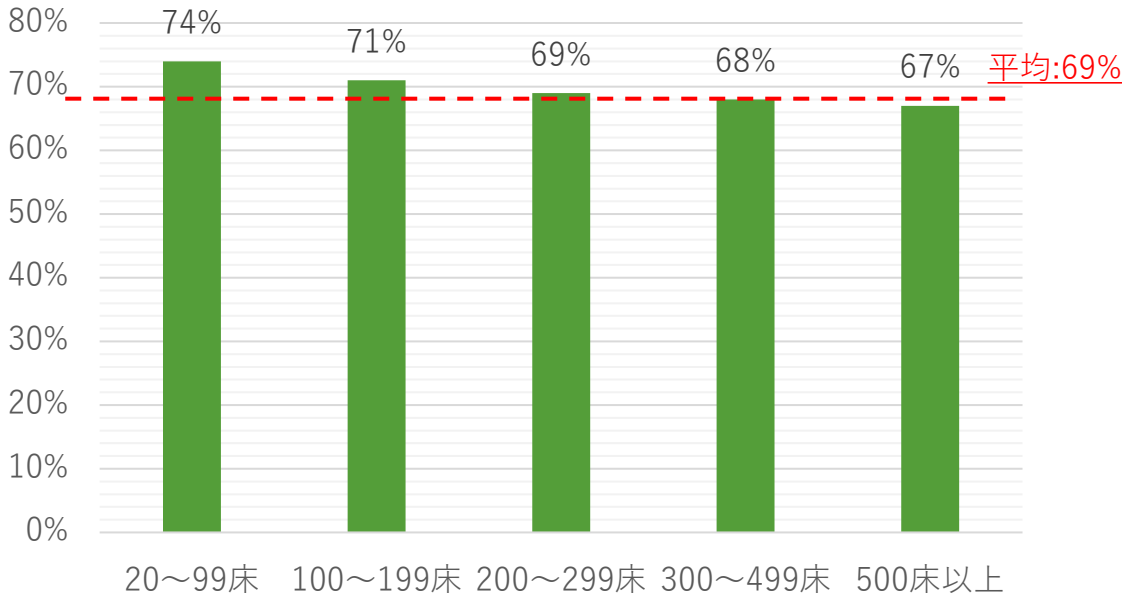
＜アンケート調査内容_病床規模別(6/7)＞

＜セキュリティ管理～その３＞

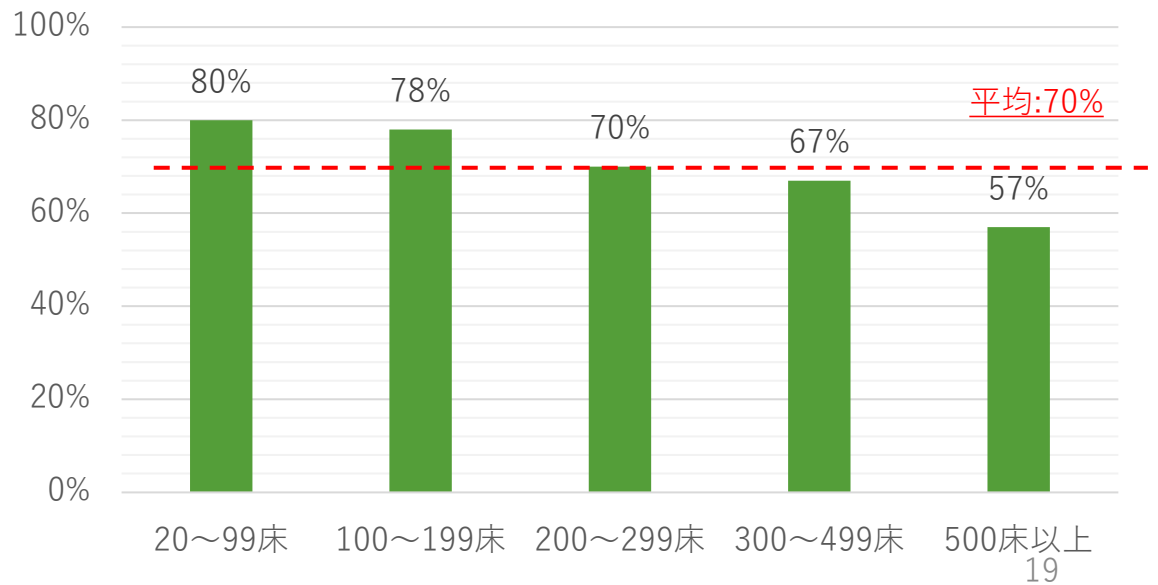
・**サイバー保険の未加入比率は病床規模が小さいほど高まる**傾向が見られる。院内システム（セキュリティ）担当者もセキュリティ予算も少ない病院ほど、サイバー保険という有事の事態への備えの検討が劣後する事態を示していると推測される。

・**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＞



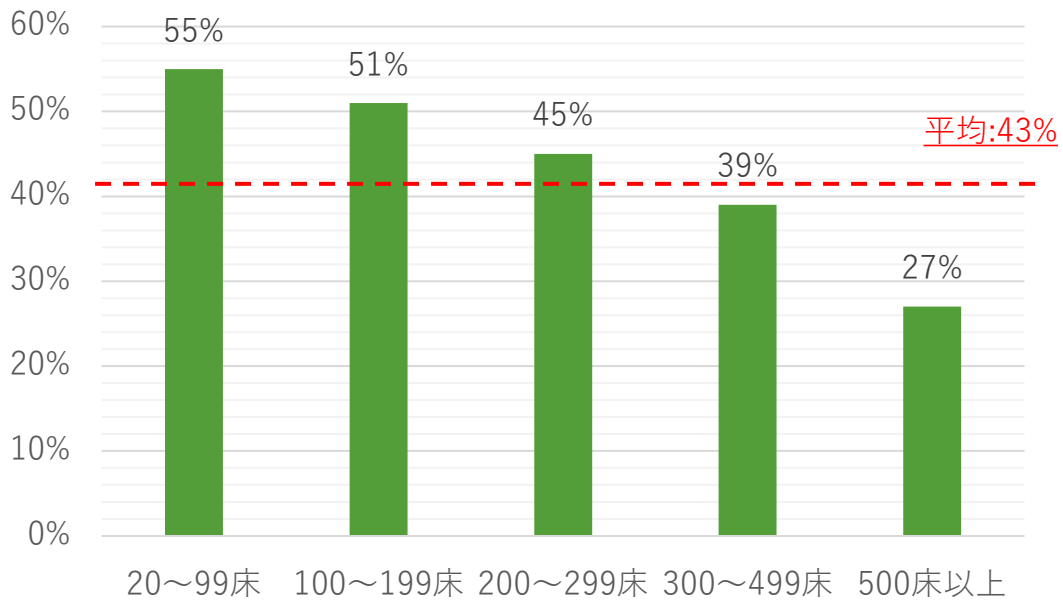
＜アンケート調査内容_病床規模別(7/7)＞

＜インシデントレスポンス・BCP＞

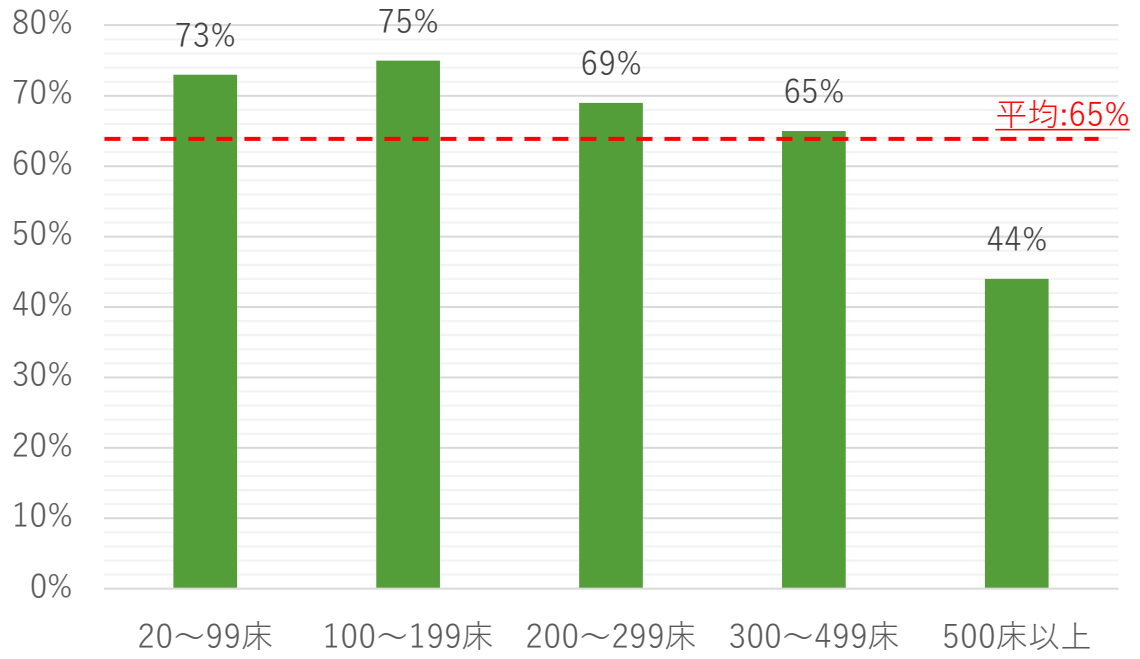
・基本的に**病床規模が小さいほど、インシデントレスポンス、BCPともに未対応率は増加**する傾向である。

・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。

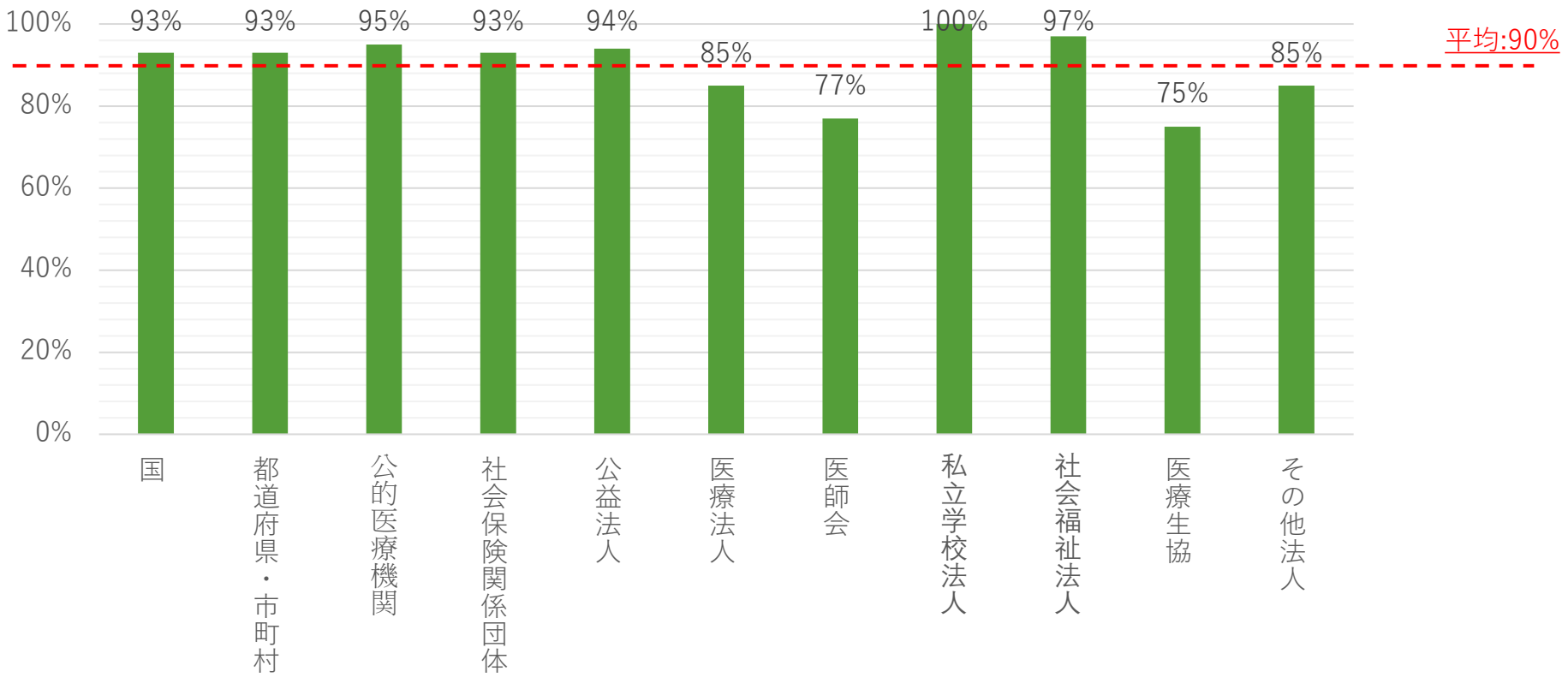
- インシデントレスポンス・BCPともに未対応率の高い開設者は、**医師会、医療法人、医療生協の順**となる。全体的にシステムがサイバー攻撃で利用不可となった場合のBCP（サイバーBCP)の未対応率は開設者平均で7割弱に達しているが、医師会、医療生協の未対応率は平均値を大きく上回っている。

- 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＞



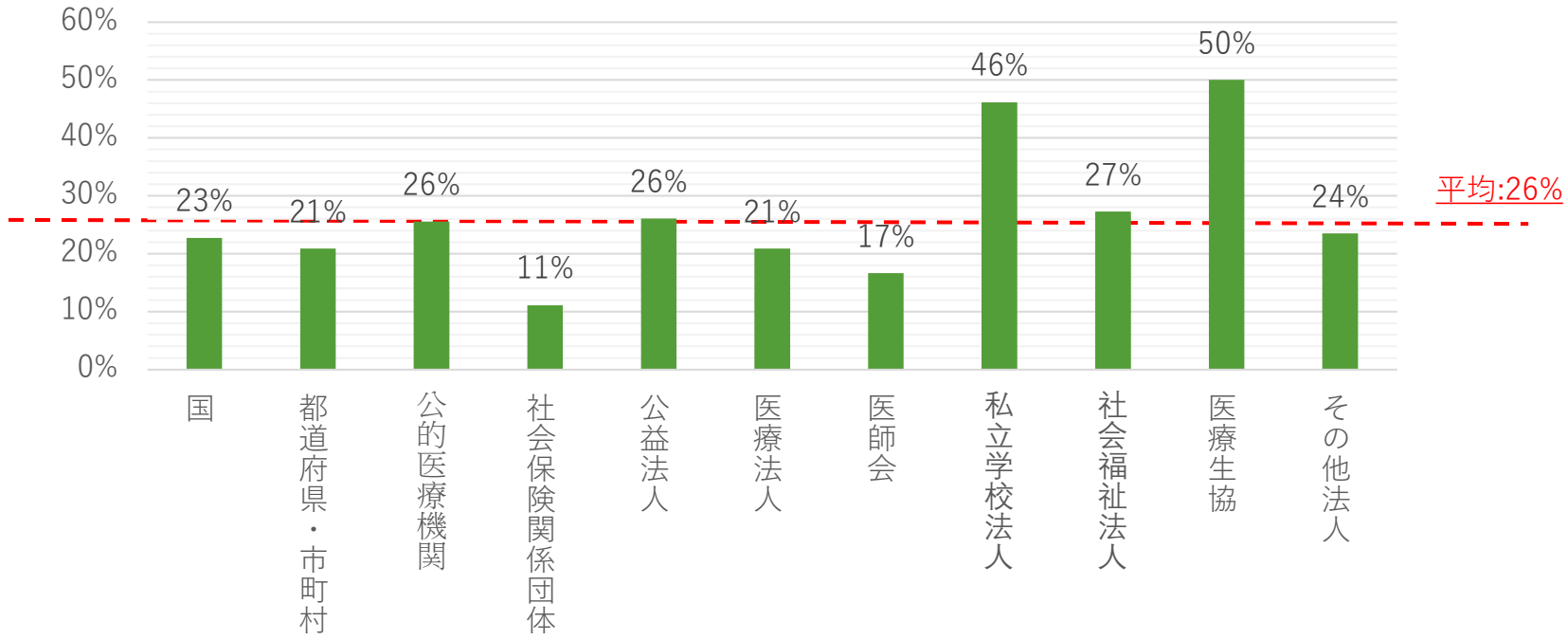
＜アンケート調査内容_開設者別(2/7)＞

＜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＞



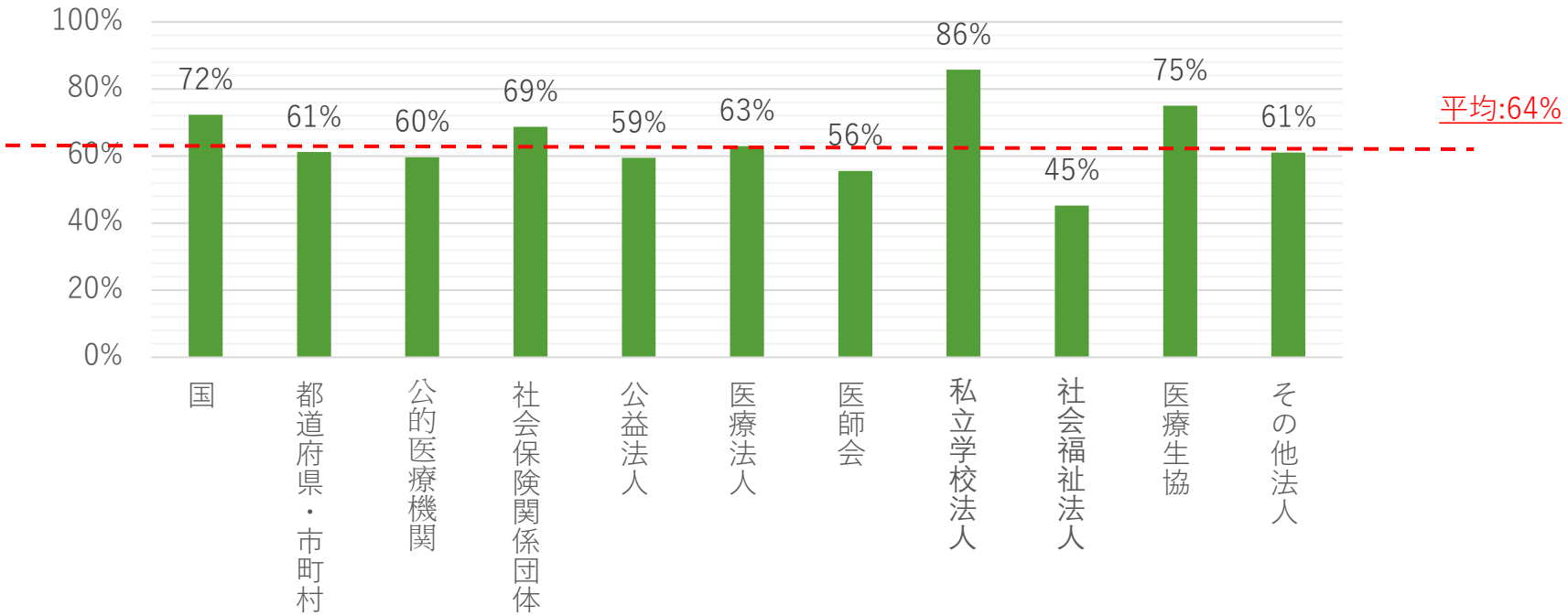
＜アンケート調査内容_開設者別(3/7)＞

＜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/オンサイト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)＞

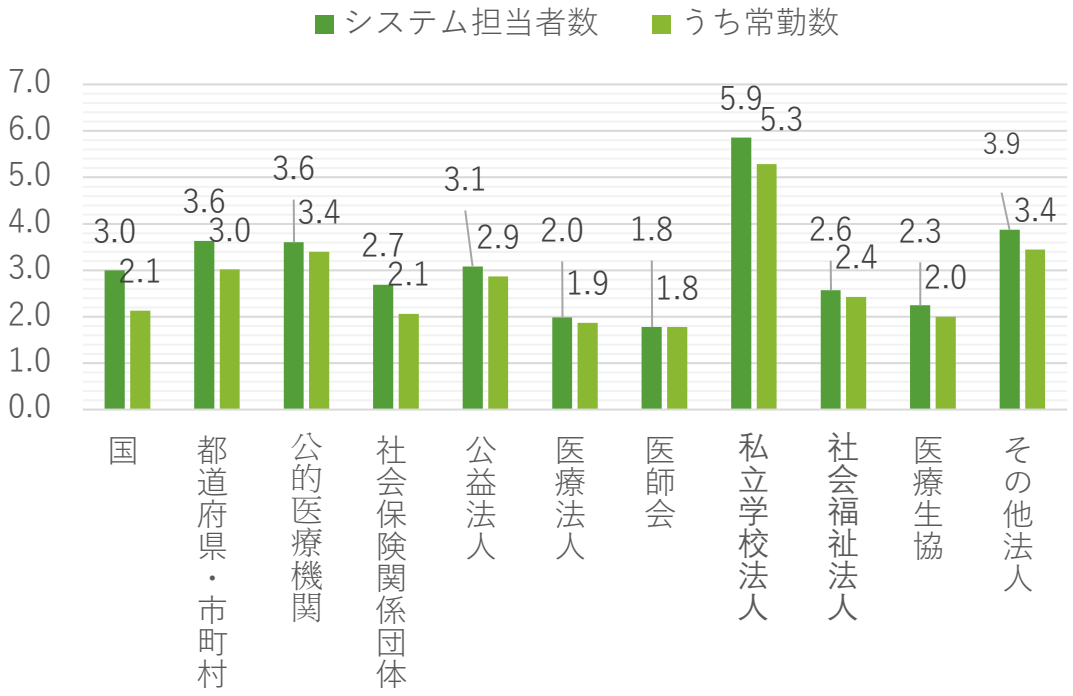
＜セキュリティ管理～その１＞

・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。

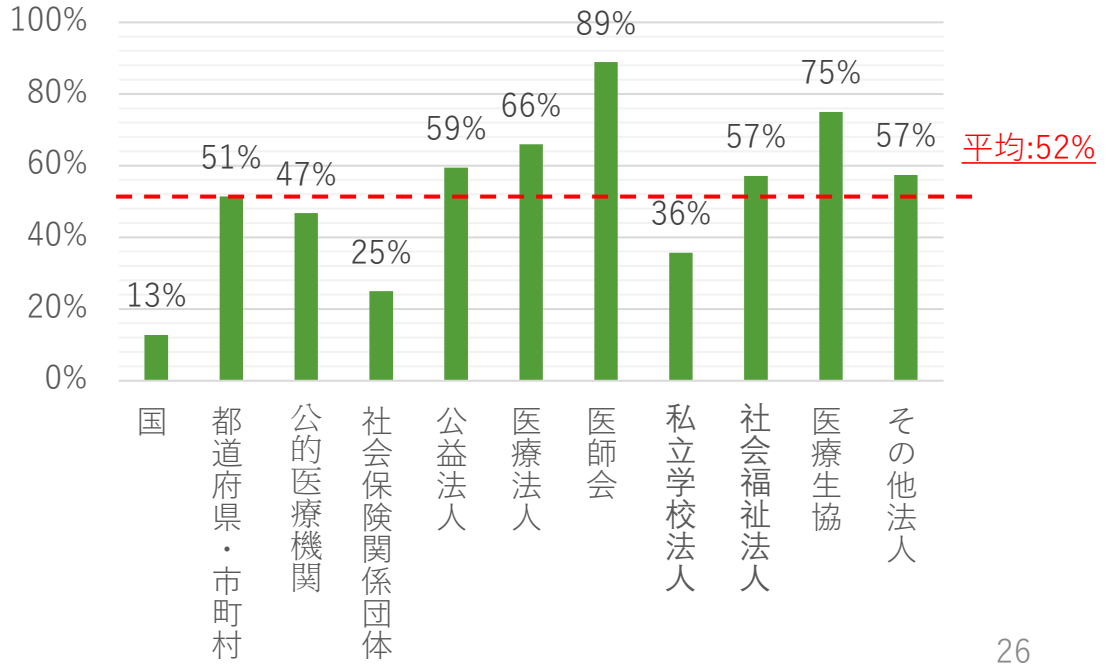
・セキュリティ監査未実施率は**医師会（89%）、医療生協（75%）**が特に平均値を上回る状況である。国や社保、私大等は法定監査の一環としてセキュリティ監査を実施するため、実施率が相対的に高いと思われる。

・なお、システム担当者はどの開設者でも**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＞



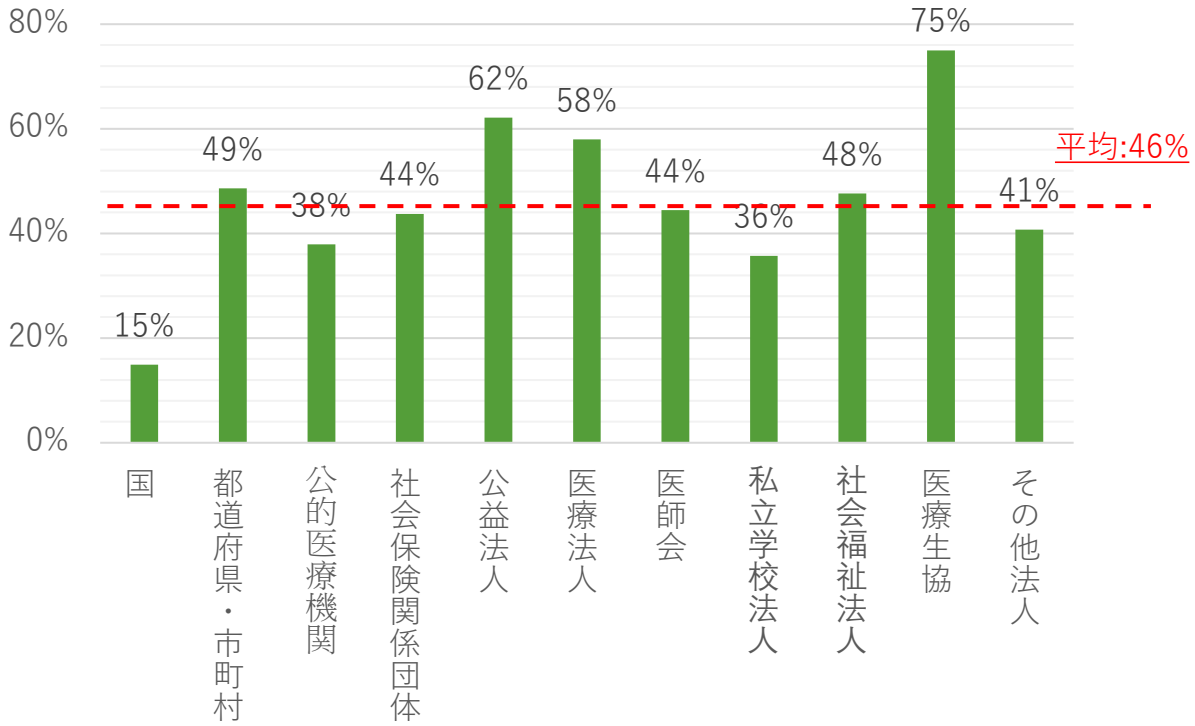
＜アンケート調査内容_開設者別(5/7)＞

＜セキュリティ管理～その２＞

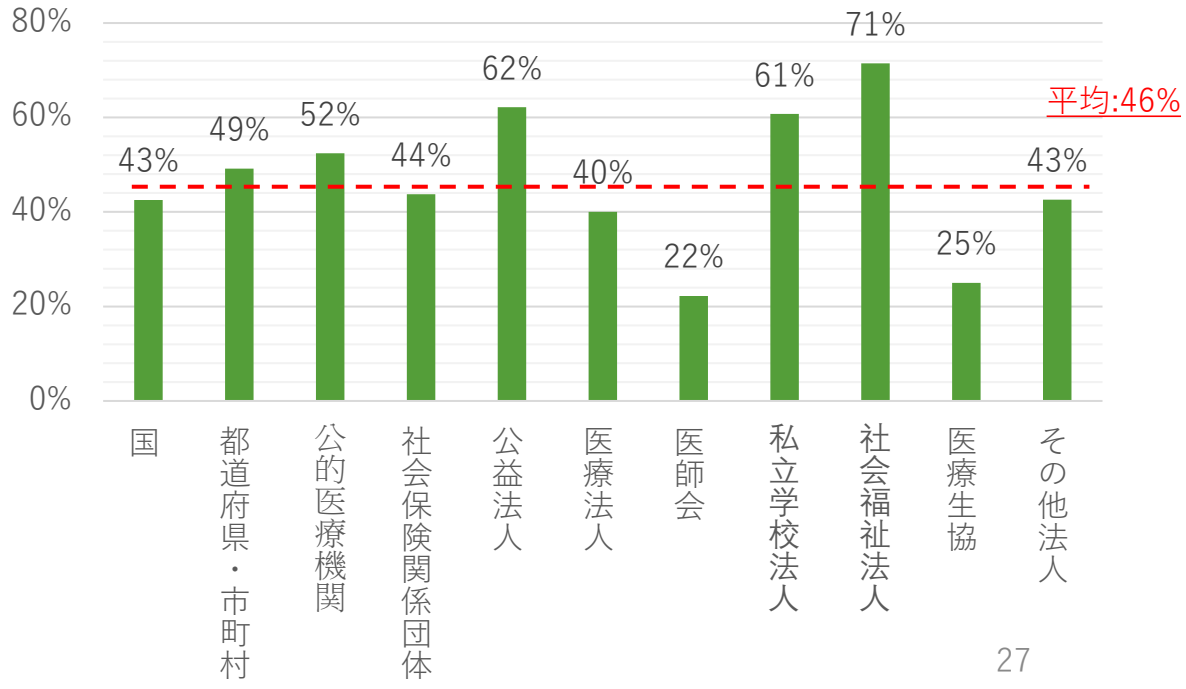
・開設者平均で見ると、特に**医療生協(75%)、公益法人（62%)、医療法人（58%)**の病院ではセキュリティ予算額が全体的に小さい傾向にあることがわかる。

・セキュリテイ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)＞

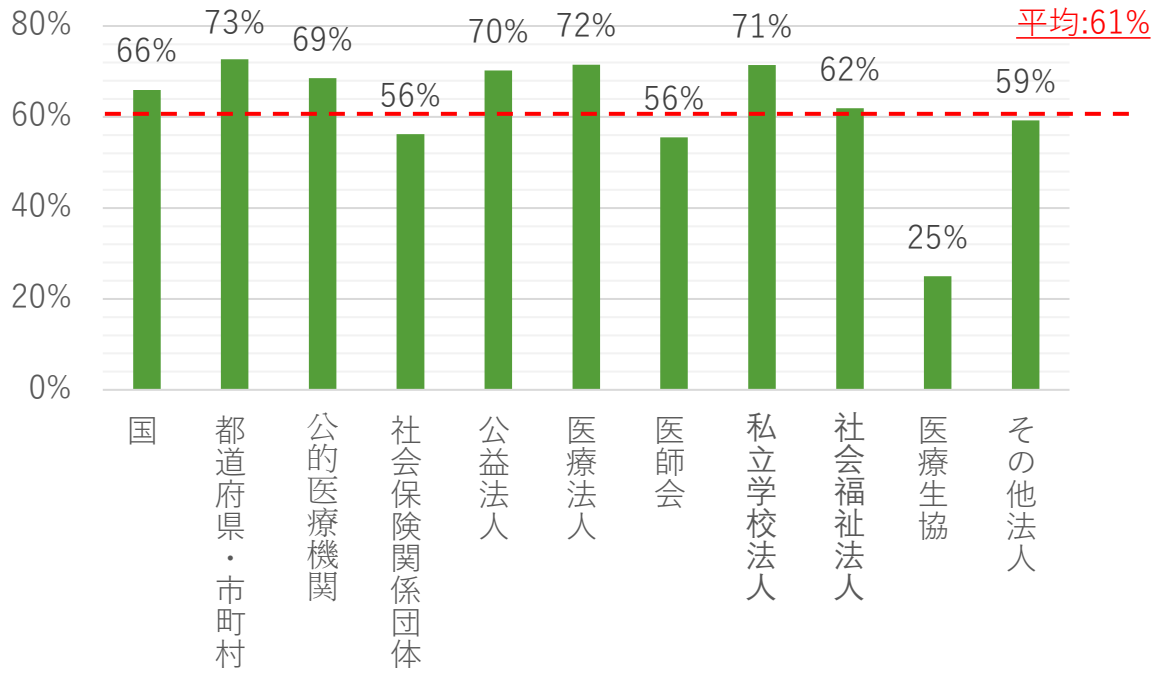
＜セキュリティ管理～その３＞

・**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。

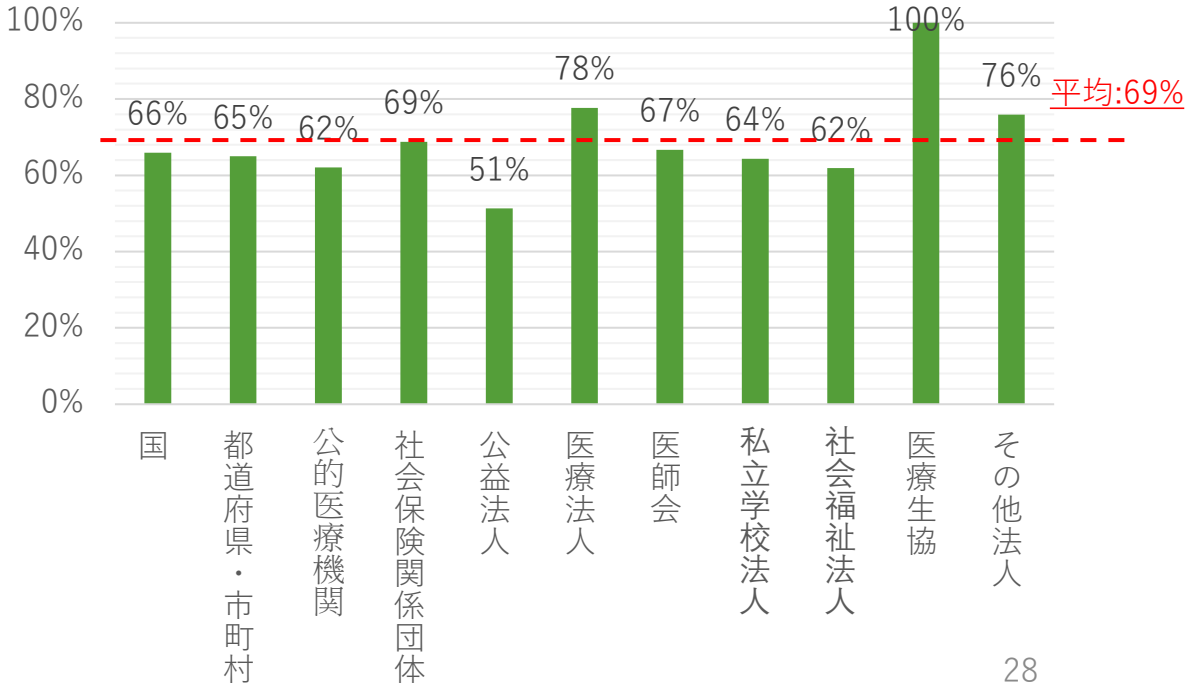
・社保（56%)、医師会（56%)、医療生協（25%) の未加入率は平均値を下回っている。このうち、**社保はサイバー保険加入率が高い（24%）**ことによるが、ほかは「わからない」（医療生協：75%、医師会：33%)という回答結果が多いためとなる。なお、**開設者全体平均で、サイバー保険に加入していると回答した割合自体は7%**である。

・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＞



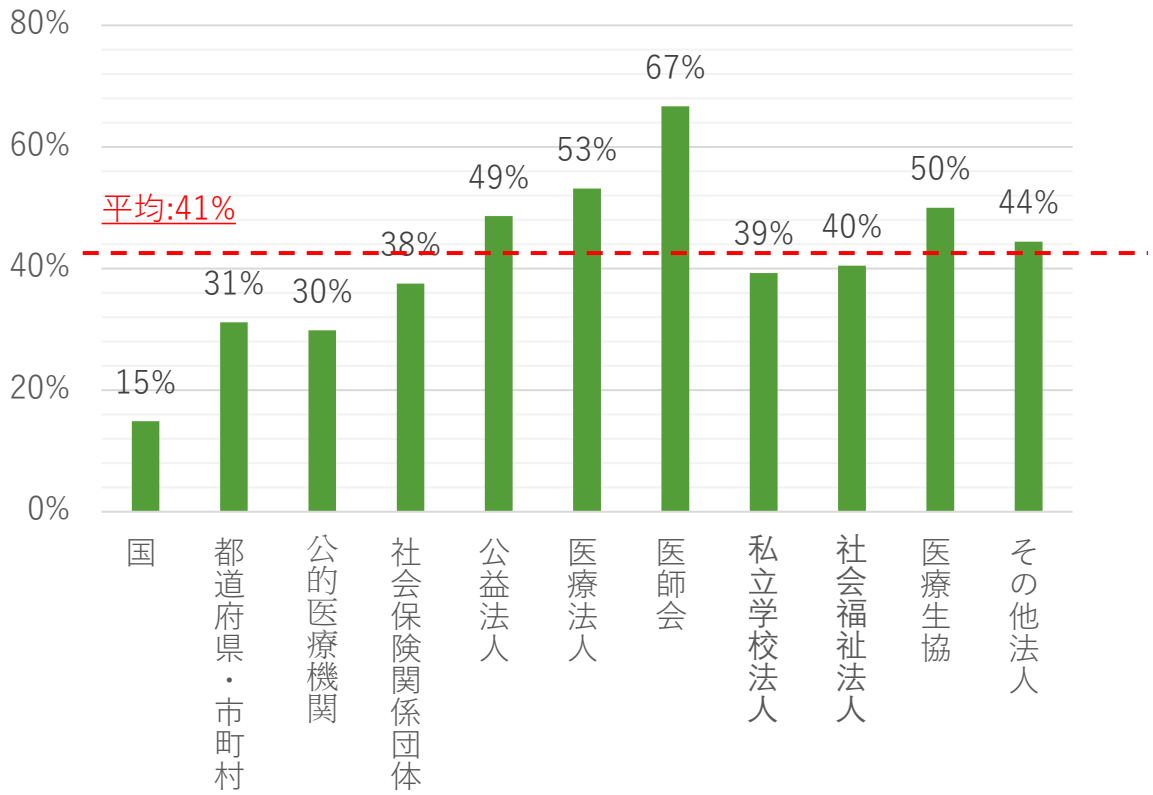
＜アンケート調査内容_開設者別(7/7)＞

＜インシデントレスポンス・BCP＞

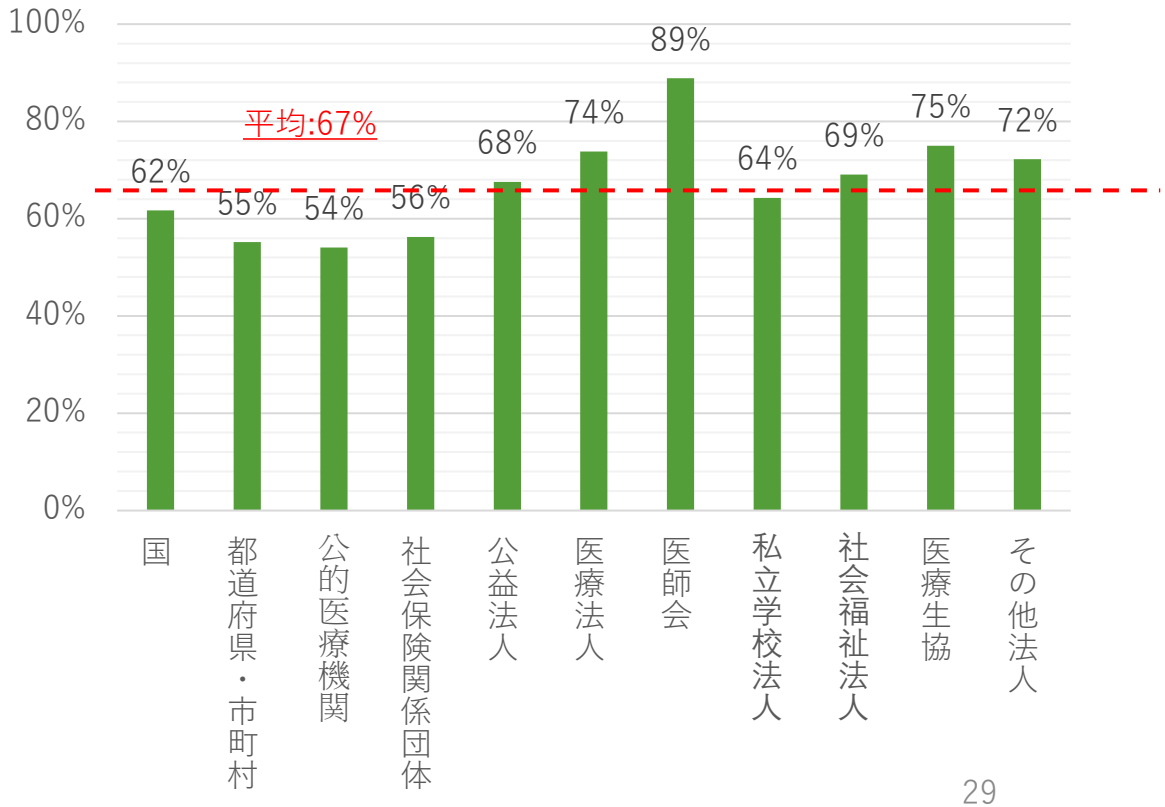
・インシデントレスポンス・BCPともに未対応率の高い開設者は、**医師会（67%/89%)、ついで医療法人（53%/74%)**となる。

・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＞



4. 提言

提言～概要

予算面の措置

1

診療報酬という公定価格の世界のなかで、収支差益率はほぼなく、セキュリティ予算も計画的に確保できない国内病院業界に対して、高度化/巧妙化するサイバー脅威への対策として、**他産業平均で見た合理的なセキュリティ予算を官公庁が公的に補助することで、患者診療の継続性・安全性を担保すべきではないか**

ガイドライン面の措置

2

国内医療情報セキュリティの典拠である厚生労働省**「医療情報システムの安全管理に関するガイドライン」**を、現行のサイバー脅威や経産省・総務省安全管理GLの変更経緯等も勘案した観点より、リスクベースアプローチのコンセプトの下でアップデートし、医療機関が主体的にリスク評価・検討し、IT事業者と対等にコミュニケーションするための共通の物差しの整備--- つまり、**患者の診療継続性（患者ファースト）を確保するため、病院・IT事業者が一体となり、共通のリスク認識のもとで医療情報システムを守るという観点より、厚労省ガイドラインの内容を見直すべきではないか**

提言１～前提

【前提】

- 前述の調査結果からは、**病院でもサイバー対策の重要性は理解しているが、予算制約上、本来実施すべき対策が行えない状況**が見受けられる。
- また、外部のセキュリティ専門企業からの派遣受け入れ、あるいはセキュリティ監査による態勢改善等、**外部のセキュリティ専門家の導入を行うにも、セキュリティ面の予算を確保しなければ実施できない**。
- 診療報酬という公定価格に基づき収支管理を行わざるを得ず、且つ、収支差益も報酬改定に伴い変動・低減していく国内の病院にとって、**サイバーセキュリティへの投資を「自助」で行いつづけることは困難**であると言える。

- ＜医療＞はNISCが指定する重要インフラの一つに指定される通り、その他一般以上のサイバー水準が求められるものの、それに対応できるほどの**リソース・予算を持つ病院は非常に限られている**といえる。
- そのため、各病院の規模に応じたセキュリテイ予算の実態を踏まえつつ、**「公助」、つまり公的な補助金支給は不可欠**と考えられる。

- **上記前提のもと、他産業平均で見て、＜医療＞いう公的インフラに対して、本来求められるべきセキュリティ予算の具体的な金額を病床規模区分に応じて試算する。**

提言１～試算方法（概要）

・他産業では、収益（売上）に占める**IT予算比率は平均２％程度**と言われており、さらにそのIT予算の中で**セキュリティ関連費用は１５％以上が計上される傾向**が高い。
・そのため、国内の病院の収益を算出し、その収益に対して2%程度のIT予算費を試算し、さらに**そのIT予算費のうち15%（他産業平均で見た必要最低水準）を病院が本来有するべき必要なセキュリティ予算（①）**として算出する。
・なお、国内の病院のIT普及率は病床規模が小さいほど低くなる傾向がある。そのため、IT導入の初期費用の必要性も勘案し、規模の小さい病院についてはIT予算費率を一部補正している。

・アンケート回答項目におけるセキュリティ予算の回答結果を踏まえ、**1病院あたりどの程度のセキュリティ予算を実態的に確保しているかについての推定計算**を行い、病床規模別に整理を行う（②）

・**①と②のギャップを分析**し、他産業平均から考慮した場合、1病院あたり確保すべきセキュリティ予算の不足状況を病床規模別に整理する。

・他産業では従前よりセキュリティ投資が長年行われており、その結果も踏まえ15％以上のセキュリティ投資に留まっている。
・セキュリティ投資が従来まで困難であった病院業界ではこの必要最低水準（15%)でなく、その2倍程度（30%)の投資を十分水準として数年は行うことで、他産業より劣後するセキュリティ水準の急速な底上げが必要であると考えられる。
・そのため、対IT予算費30%で見た、公的補助（公助）の金額水準もあわせて整理する。

提言～セキュリティ予算の必要公的補助金額

・試算の結果、病床規模別に、１病院あたりのセキュリティ予算として以下の＜公助＞＝公的補助金が必要と考えられる。
・**はじめ数年は十分水準（対IT予算費30%)程度の補助金を支給し、セキュリティ水準の底上げが図られたのちに、必要最低水準（対IT予算費15%)の補助金支給に変更していく段階的なアプローチ**が期待される。

病床規模	対IT予算費15%試算 （公助の必要最低水準）	対IT予算費30%試算 （公助の十分水準）
20床~99床	**300万程度**	**980万程度**
100床～199床	**1200万程度**	**2900万程度**
200床～299床	**1800万程度**	**4200万程度**
300床～499床	**2100万程度**	**5000万程度**
500床～	**5900万程度**	**1億3000万程度**

提言２～前提

【前提】

- 国内の医療情報システムは3省2ガイドライン、つまり病院は厚生労働省「医療情報システムの安全管理に関するガイドライン」、IT事業者は経産省・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」に準拠することで、セキュリティ管理を行うことが求められている。
- 高度化・巧妙化するサイバーリスクの高まり、病院業務における新たなテクノロジー導入等の外部背景も踏まえ、IT事業者向けの経産省・総務省ガイドラインは20年8月に従前のルールベースアプローチから、リスクベースアプローチへの変更が行われた。これにより、**病院/IT事業者それぞれがどのような対策を講じることで医療情報システム全体のセキュリティ -- 患者を守るためのセキュリティ --- を確保していくかについてIT事業者は病院へ能動的にコミュニケーションを行うこと**が求められるようになった。

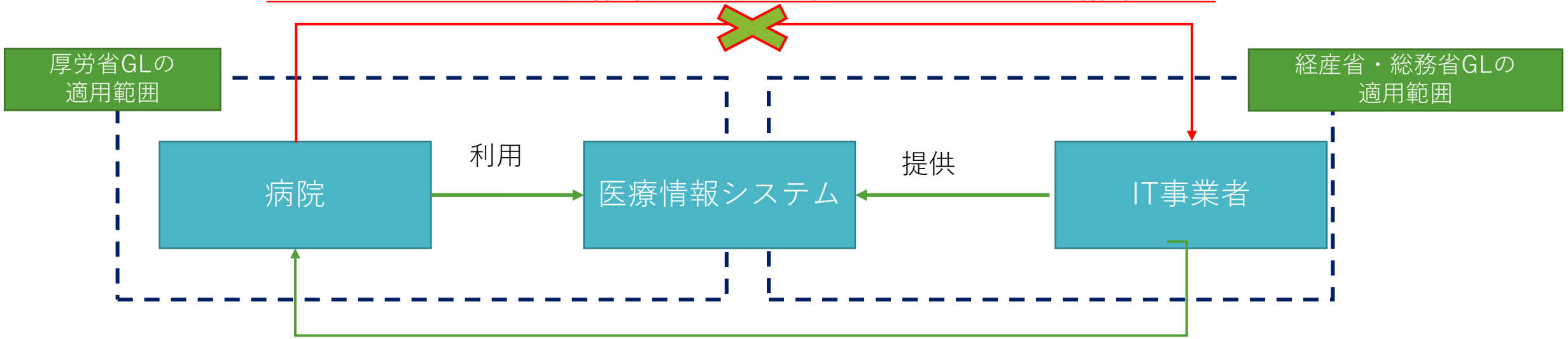
- 一方、仮にIT事業者が病院の院内システム担当者へコミュニケーションを行ったとしても、現行の厚労省GLではそのコミュニケーションを受けて、病院としてどのような技術・運用対策を講じるべきかについてのインストラクションが存在せず、対応自体が困難になると想定される。**つまり、事業者向けGL/病院向けGL一体とした目線のもとで、患者診療の継続性を守るためのセキュリティを考えること自体が現行の3省2ガイドラインの立て付け上、難しいといえる。**
- 今後、セキュリティ予算の公的補助が各病院に付き、セキュリティ対策・運用をIT事業者とともに行うに際しても、**こうしたIT事業者とのサイバーリスクに関するコミュニケーションを行うための一定の準拠枠（何をどう指示すべきか等）が存在しなければ、IT事業者の言いなりになって終わりとなるリスクが高い。**

- 上述のリスクを回避するために、病院向けの厚労省GL自体にそのようなエッセンスが含まれるべきであるが、現行の多くは、**病院が＜システムユーザとして何をなすべきか＞に軸足を置いた内容**となっている。そのため、**IT事業者を管理監督する＜システムオーナーとして病院がIT事業者と対等の立場に立って、何をなすべきか＞の整理が不十分**である。
- 患者の命は病院が守る責任があり、患者診療の継続性を確保するために医療情報システムのセキュリティ改善を行うシステムオーナーとしての責任は一義的には病院にある。しかし、現行のガイドラインにはそのような視点が十分でない。
- セキュリティ管理も含めた医療情報システムの継続性を確保するために病院がIT事業者と連携して、どのような確認や指示を行うべきなのか（バックアップの退避、VPN機器の脆弱性対応等）について、院内システム担当者の意識向上が図られないのも仕方がない状況である。（IT事業者へのシステム管理の丸投げ体質の一因にもなっていると思料）

- **そのため、現行の厚労省GLを経産省・総務省GLと一体化して、病院/IT事業者が一体となり、＜患者を守る＞ために、医療情報システムのサイバーセキュリティをどのように検討・対応すべきかという観点より、3省2ガイドラインを一本化・見直すことが重要である。**

提言２～改善すべき状況（イメージ）

厚労省GLには、病院がシステムオーナーの意識を持ち、ITベンダーとサイバーリスクに関するコミュニケーションを具体的にどのように行うべきかについての指針がない



経産省・総務省GL（20/8)には、病院を単なるシステムユーザでなく、システムオーナーとして同じ共通理解のもとで、セキュリティの合意形成を行うことが求められており、IT事業者⇒病院のサイバーリスクに関するコミュニケーションが求められている。

結果

・IT事業者がセキュリティの合意形成を病院と行おうにも、**病院側がどのようにそれに対応すべきなのかのリスク/対策を検討するための準拠枠が存在しないため、IT事業者と対等の目線（共通の物差し）で、医療情報システムのセキュリティ – 患者安全 – を検討することが困難**

提言２～厚労省GL/経産省・総務省GLの一体化

現行の厚労省GLと経産省・総務省GLの一体化（あるいは、厚労省GLの見直し）は、少なくとも以下の観点より行われるべき。

【①：病院＝システムオーナーの明確化】

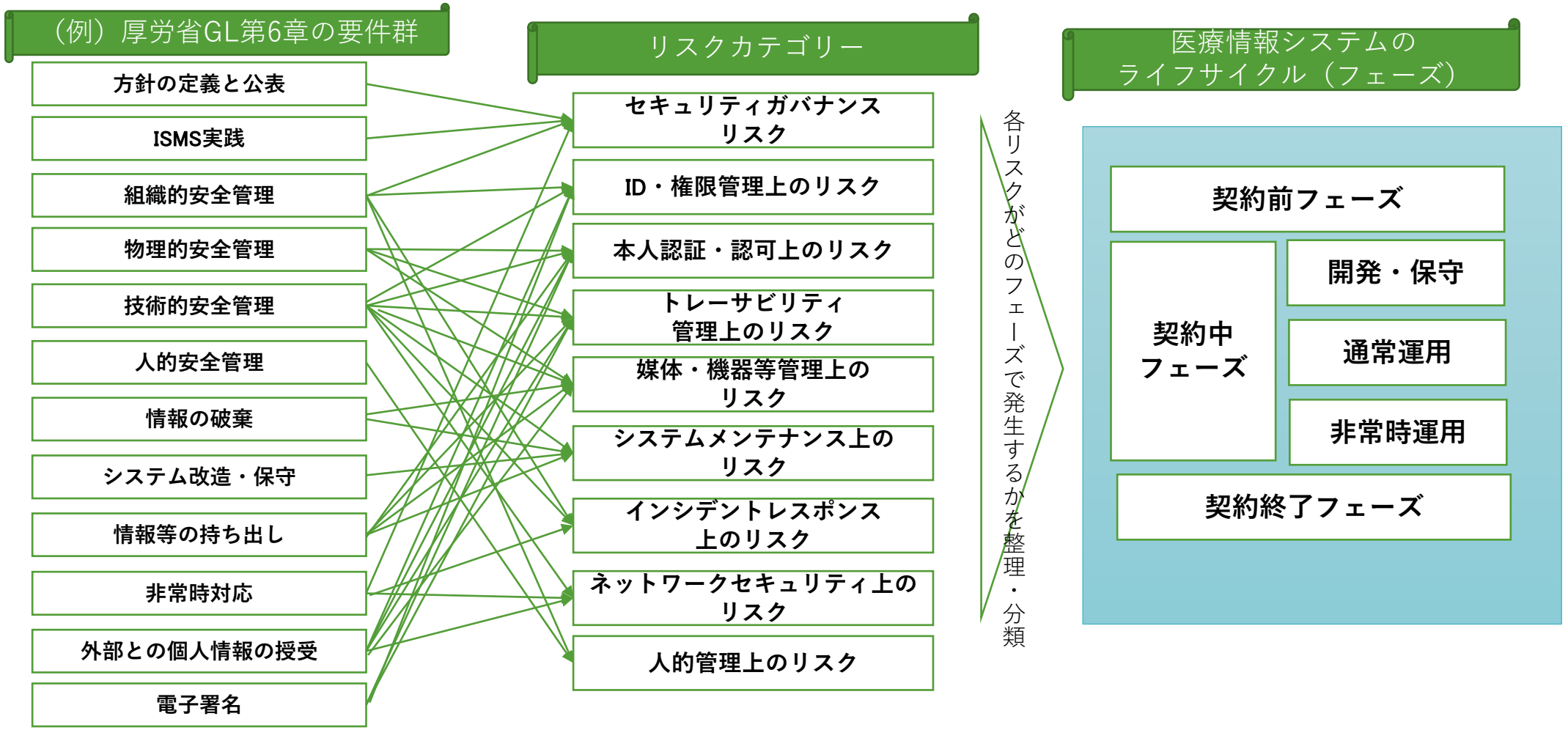
- 病院は医療情報システムの＜システムユーザ＞でなく、**＜システムオーナー＞**であること
- ＜システムオーナ＞としての責任は、第一義的には、**医療情報システムを用いた患者診療の継続性を維持すること、つまり患者安全の確保**であること

【②：病院・IT事業者一体型のリスクベースアプローチ】※　具体的なイメージは後続頁参照

- 経産省・総務省GLを踏まえた観点より、医療情報システムを取り巻く情報流を整理し、そこに潜むリスクを特定した上で、合理的なサイバー対策を**病院・IT事業者が一体となって行うことが重要**であること
- ＜システムオーナ＞としてIT事業者（システム委託先）に対して、確認、依頼、協力申出すべき事項がなんであるのかについて、**想定されるリスク別に整理・体系化する**こと（例えば、リモートメンテ接続口を講じる場合、メンテ機器や環境の脆弱性が発生するリスクがあるため、その対応についてITベンダに確実に指示することなど）
- ＜システムユーザ＞の目線のもとで整理されている現行の主要対策についても、想定されるリスクを洗い出し、「このようなリスクがある場合は、ｘｘｘという対策を講じるべき」という観点で再整理すること

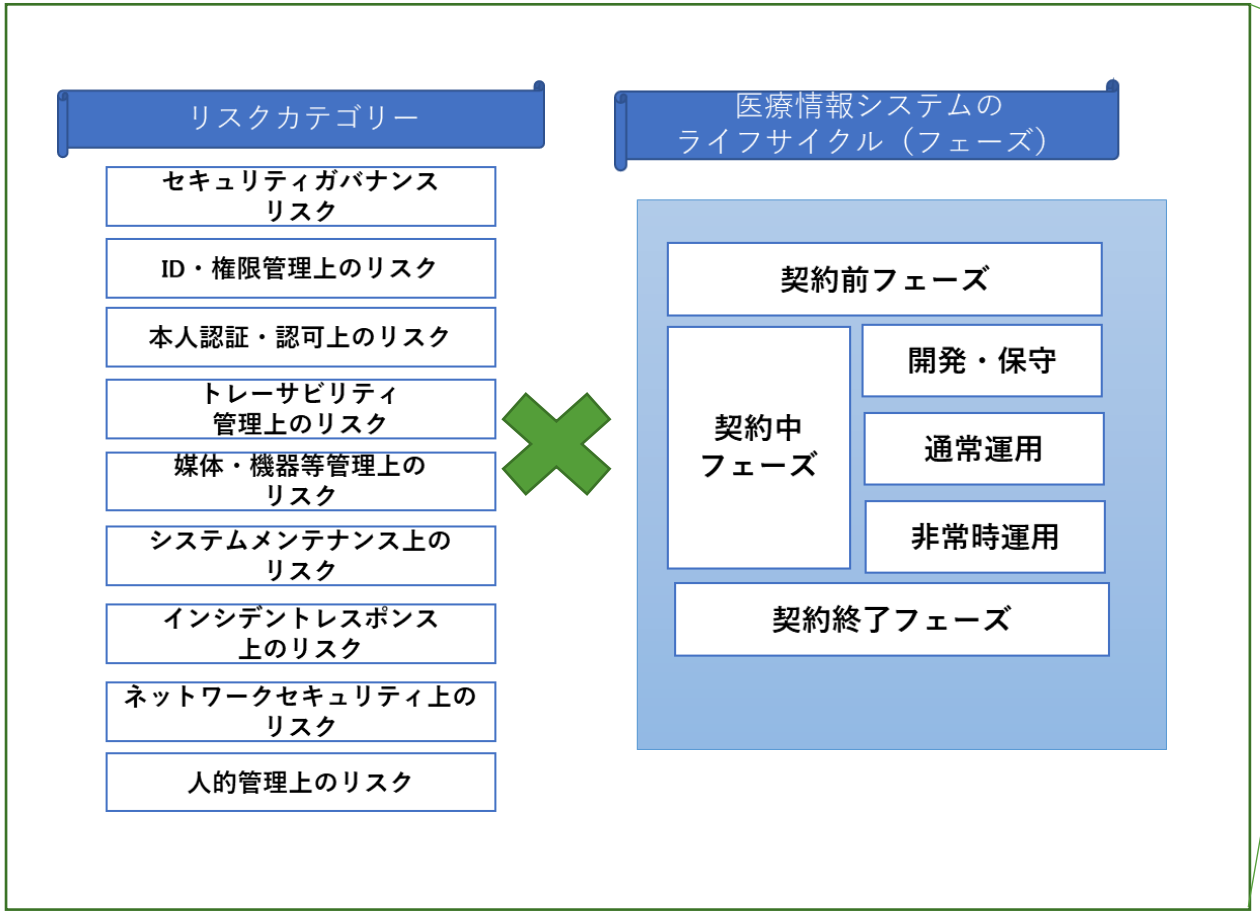
（参考）病院・IT事業者一体型のリスクベースアプローチイメージ図(1/3)

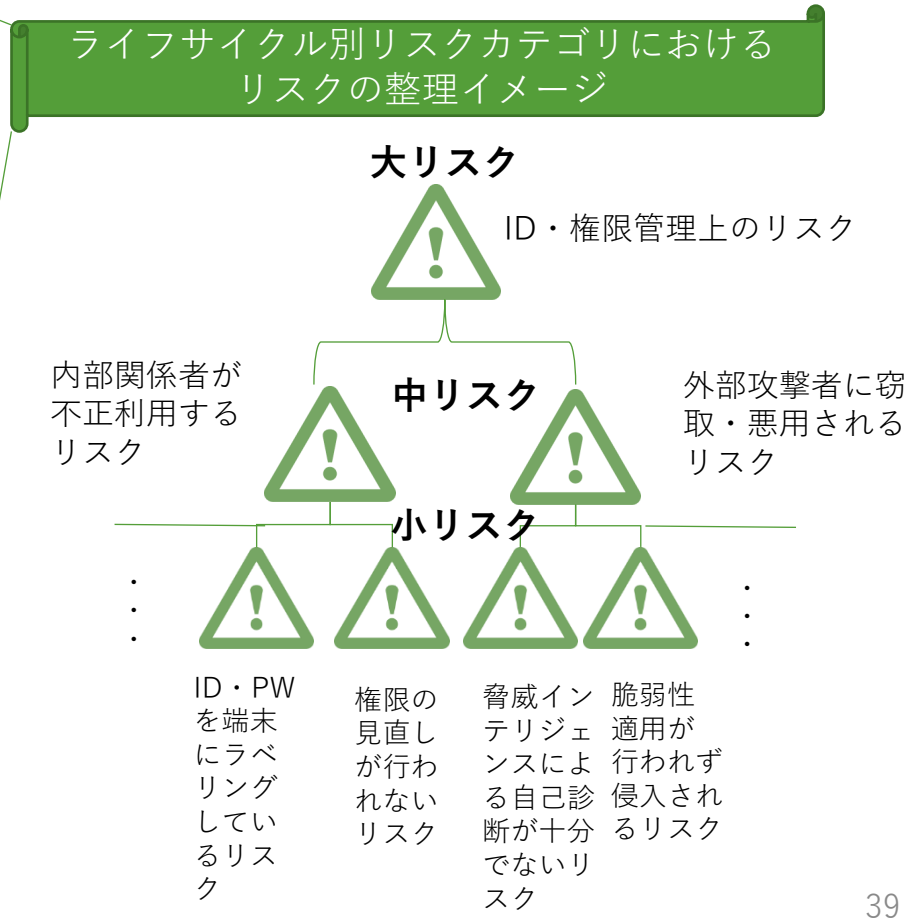
<u>厚労省GLの各種対策要件群（第6章～第9章）を、想定されるリスクのカテゴリーと紐づけていく</u>。
さらにこれらカテゴリーにおける各リスクが、経産省・総務省GLが前提とする医療情報システムのどのライフサイクル（フェーズ）で対策検討すべきものかについて分類・整理する。



（参考）病院・IT事業者一体型のリスクベースアプローチイメージ図(2/3)

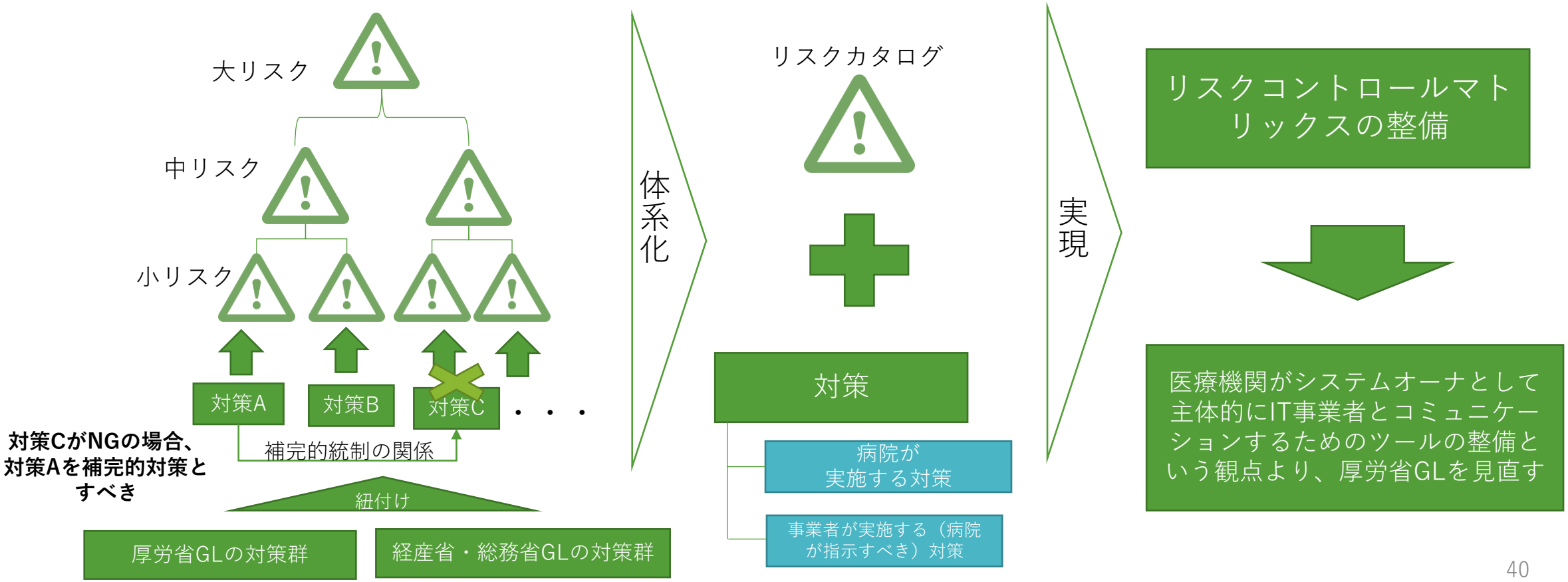
医療情報システムのライフサイクル別に整理されたリスクカテゴリでは、**各リスクが顕在化するシナリオ（リスクシナリオ）を階層的に整理**していく。これにより、想定されるリスクが顕在化する標準的なリスクシナリオに基づき、医療機関において合理的なセキュリティ対策の要否を検討することを可能とする。





（参考）病院・IT事業者一体型のリスクベースアプローチイメージ図(3/3)

さらに現行の厚労省GLの諸対策のみでなく、経産省・総務省GLの対策（IT事業者に守らせるべき対策）も踏まえ、各リスクシナリオにおいて、**リスクが顕在化しないため講じるべき対策を紐づける**とともに、ある対策がNGの場合、どの対策を補完的対策とすべきかという**対策間の関係性（補完性）をあわせて整理していく**。
これにより、特定の対策がNGの場合、どの対策をもってセキュリティリスク低減を補完的に図るべきか、あるいはどの対策が十分でないとどのようなセキュリティリスクが想定されるのか等について、**病院が主体的に検討・評価し、必要に応じてIT事業者への指示・依頼を行うことに活用できるリスクコントロールマトリックス（リスク/対策の一覧表）**を整備する。




Medical Information
Sharing and Analysis Center