

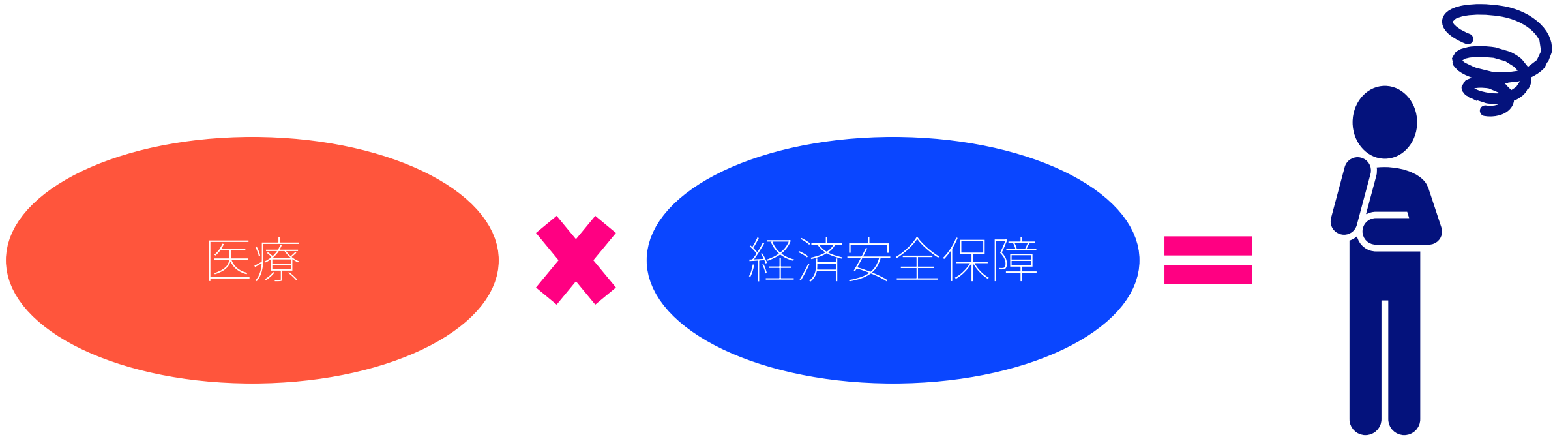
IISEシンポジウム「高品質なヘルスケアデータとエコシステムの構築」

# 医療分野と経済安全保障法改正

2026年3月16日

株式会社国際社会経済研究所  
経済安全保障・デジタル社会研究部 遊間 和子

# 1.なぜ「経済安全保障」？

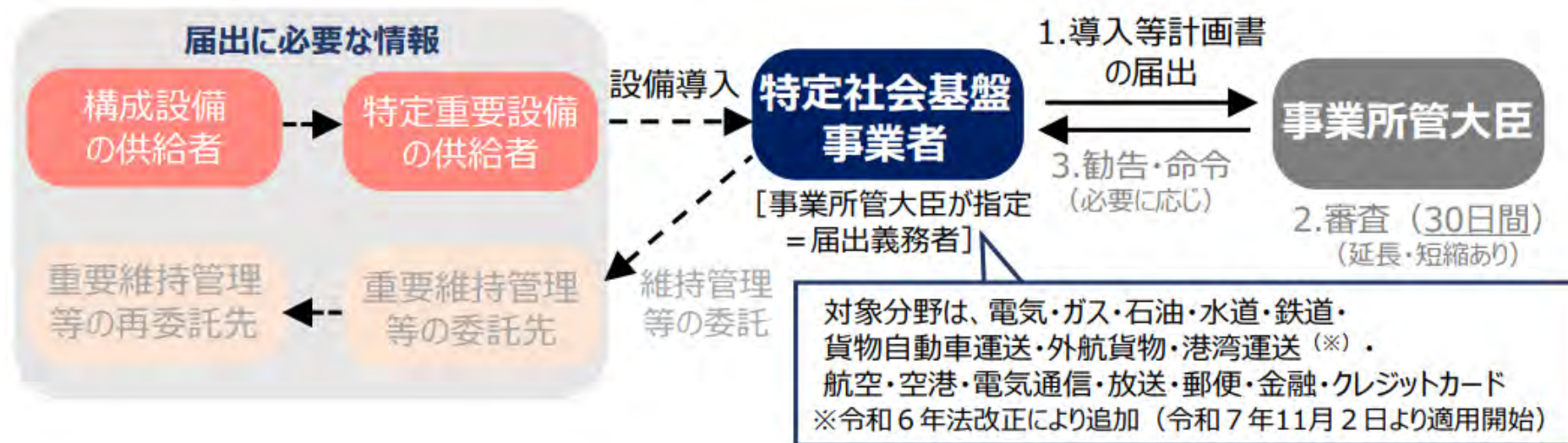


経済安全保障とは、国際情勢の複雑化、社会経済構造の変化等により、安全保障の裾野が経済分野に急速に拡大する中、**国家・国民の安全を経済面から確保するための取組**を強化・推進すること

- 国際情勢の複雑化、社会経済構造の変化等により、安全保障の裾野が経済分野に急速に拡大する中、**国家・国民の安全を経済面から確保するための取組を強化・推進**することが重要となり、**2つの法律が制定**。
- **経済安全保障推進法**（2022年5月11日成立、5月18日公布）にて4つの制度を運用
  - (1)重要物資の安定的な供給の確保、**(2)基幹インフラ役務の安定的な提供の確保**、(3)先端的な重要技術の開発支援、(4)特許出願の非公開 を段階的にスタート
- **重要経済安保情報保護活用法**（2024年5月10日成立、5月17日公布）
  - 重要経済基盤（重要なインフラや物資のサプライチェーン）に関する一定の情報であって、公になっていないもののうち、その漏えいが我が国の安全保障に支障を与えるおそれがあるため、特に秘匿する必要があるもの（具体例：サイバー脅威・対策等に関する情報、サプライチェーン上の脆弱性関連情報）
  - 「セキュリティ・クリアランス」とは、国家における情報保全措置の一環として、政府が保有する安全保障上重要な情報として指定された情報に対して、アクセスする必要がある者のうち、情報を漏らすおそれがないという信頼性を確認した者の中で取り扱うとする制度

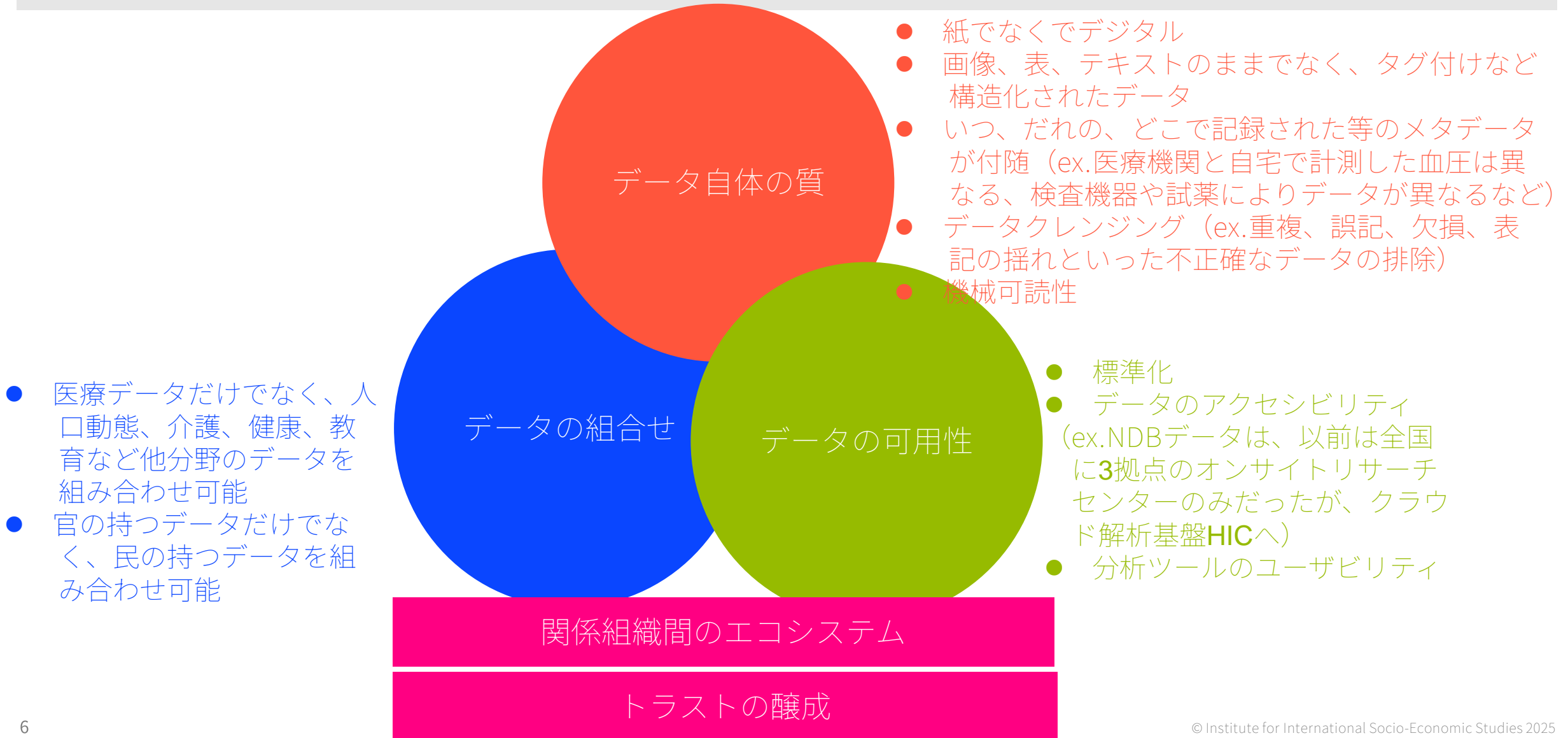
### 3. 経済安全保障推進法：基幹インフラ役務の安定的な提供の確保に関する制度 I I S E

- 基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、国が**基幹インフラ事業（特定社会基盤事業）**を定め、**一定の基準に該当する事業者（特定社会基盤事業者）**を指定し、国が定めた重要設備（特定重要設備）の導入・維持管理等の委託をしようとする際に、**事前に届出を行い、審査を受ける制度**（2024年5月17日から運用開始）
- 対象分野は、電気・ガス・石油・水道・鉄道・貨物自動車運送・外航貨物・港湾運送※・航空・空港・電気通信・放送・郵便・金融・クレジットカード



- 国民のQOL・QOD維持・向上には、データ保護やセキュリティに配慮した上で、患者ジャーニーを含む生涯にわたる一人ひとりの高品質のヘルスケアデータを収集・活用していくべきといえる。
- そのためには、健康・医療・介護分野だけでなく、行政や教育機関などが持つデータと連携して活用していく分野的ボーダレス、ひとつの自治体・地域の中だけで完結するのではない地理的なボーダレス、公的機関と民間組織との垣根を超える官民のボーダレスを実現していくことが必要である。
- それぞれの組織が相互に連携し、共存共栄しながら大きな価値を創出するエコシステムを構築していくには、いかにトラストを醸成していくかも重要となる。

# 5. 高品質なヘルスケアデータとは



## 6. トラストを揺るがす医療機関へのサイバー攻撃

発生年月	機関	概要
2017年8月	福島県立医科大学付属病院	ランサムウェア「WannaCry（ワナクライ）」の亜種に感染し、PCや医療機器がロックされ使用できない状態に。「身代金」の要求には応じず、データの復元を断念。災害拠点病院の一つで、県北部の救命救急センターとしての役割を担う。
2018年10月	宇陀市立病院（奈良県）	ランサムウェア「GandCrab（ガンクラブ）」によって1133人分の患者データが暗号化されアクセス不能に。全データの復元には2019年3月までかかった。
2021年10月	つるぎ町立半田病院（徳島県）	ランサムウェアに感染し、犯罪者集団「LockBit（ロックビット）」からの身代金要求。電子カルテシステムに登録された約8万5000件の患者情報を閲覧できなくなり、診療報酬の請求も停止。2022年1月に電子カルテシステムを復旧。
2022年10月	大阪急性期・総合医療センター	ランサムウェアによるサイバー攻撃で、電子カルテシステムが停止。身代金要求される。高度救命救急センターも設置している大阪市南部の中核的な医療機関で、大阪府で唯一指定されている基幹災害医療センターでもある。診療の完全復旧は1月までかかった。
2025年2月	宇都宮セントラルクリニック	ランサムウェア「Qilin（麒麟）」により約30万人分の個人情報暗号化され、流出の可能性があるとして、診療・健診業務も一部停止となった。停止していた業務の一部が復旧したのは3月初旬。
2026年2月	日本医科大学武蔵小杉病院	ナースコールシステムのサーバー3台がランサムウェア感染約1万人分の個人情報（氏名・住所・電話番号等）が流出し、身代金要求される。電子カルテの情報には影響なく、復旧は約2週間。

## 7. 医療情報システムの安全対策

- 医療情報の安全管理に関しては、「医療情報システムの安全管理に関するガイドライン（略称：厚労省ガイドライン）」及び「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（略称：2省ガイドライン）」に、必要な対策が規定。
- 厚生労働省では、2023年4月から医療法に基づく医療機関に対する立入検査の項目に、サイバーセキュリティ対策の項目を位置付け
  - 厚労省ガイドラインから特に取り組むべき重要な項目を抽出し、「医療機関におけるサイバーセキュリティ対策チェックリスト」を公表
- 厚生労働省 健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループにおいて、2023年5月に策定された厚労省ガイドライン第6.0版の改定が検討中。
  - 想定される論点は、8つ

- 総務省、厚生労働省、経済産業省「医療情報システムの契約における当事者間の役割分担等に関する確認表」が2024年6月に公表される。
  - 医療機関における情報セキュリティインシデントでは、契約の際に、医療機関と医療情報システム・サービス事業との役割分担等が適切に協議されていないことが課題の一つで、契約上の役割分担等が曖昧な点は、事業者対応において責任の所在が問題となる等のケースがある。
  - 可能な限り、事前に双方の役割分担等を取り決め、有事の際に即座に対応できるよう、契約の段階で合意形成文書（契約書やサービス・レベル合意書（SLA）等）に落とし込むことが重要
- 厚生労働省「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」も2024年6月に公表さえる。
  - 昨今の巧妙化したサイバー攻撃においては完全にリスクを排除できない。
  - サイバー攻撃を「どのように防ぐか」だけでなく「発生時にどのように対応するか」という意識で、非常時に診療への影響を最低限に抑えるための対応を、あらかじめ「サイバー攻撃を想定した事業継続計画（BCP）」を策定しておくことで、適切な復旧対応等を行うことが可能。
  - BCP の策定に際の参考となるように作成。

## 医療情報システムの契約における当事者間の役割分担等に関する確認表

### Part 1 主に医療機関が実施する項目

(契約を締結する上で医療機関が主体となって、必要に応じてシステム関連業者の協力を得ながら実施することが望ましい項目の例)

\*が付けられている用語については、別添の「用語の解説」を適宜参照すること。

項番	項目	内容	初回確認 ( / )	完了日 (日付)	備考欄
<b>A 事業者選定・事業者管理</b>					
1	事業者からの開示資料の確認	事業者から開示を受けたサービス仕様適合開示書 <sup>*1</sup> 等 (MDS/SDS <sup>*2</sup> 、MDS2 <sup>*3</sup> 等)を確認しているか。	はい・いいえ	( / )	
2	事業者管理	①事業者との契約・協働体制を把握・管理できているか。	はい・いいえ	( / )	
		②医療情報を第三者提供する場合の管理体制が整備されているか。	はい・いいえ	( / )	
<b>B 医療機関の内部体制</b>					
1	「医療情報システムの安全管理に関するガイドライン」の確認	「医療情報システムの安全管理に関するガイドライン」を確認したか。	はい・いいえ	( / )	
2	「医療機関におけるサイバーセキュリティ対策チェックリスト」に基づく契約時での現状把握及び対応	「医療機関におけるサイバーセキュリティ対策チェックリスト」を用いて、契約時に医療情報システムの現状把握及び対応を実施しているか。	はい・いいえ	( / )	
		①医療情報を取り扱う職員に関して人的安全管理対策を実施してい			

資料出所：総務省、厚生労働省、経済産業省「医療情報システムの契約における当事者間の役割分担等に関する確認表」(2024年6月)

## サイバー攻撃を想定した事業継続計画（BCP）策定の確認表

※医療機関がBCPを策定する際、最低限必要な事項を網羅しているか、確認のために使用するものです

※BCP策定や見直しの際にご活用ください

項番	大項目	確認項目	確認欄
1	平時（平時において、非常時に備え、サイバーセキュリティの体制整備を行う。）		
1-1	情報機器等の把握と適切な管理、全体構成図の作成	サーバ、端末PC、ネットワーク機器を把握できているか。	
		ネットワーク構成図・システム構成図が整備できているか。	
		システム停止が事業継続に与える影響を把握できているか。	
		サーバ、端末PC、ネットワーク機器の脆弱性への対応ができているか。	
1-2	非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集	インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図が整備できているか。	
		リスク検知のための情報収集体制が整備できているか。	
		教育訓練が実施できているか。	
		バックアップの実施と復旧手順が確認できているか。	
2	検知（医療情報システム等の障害が見受けられる場合は、早期に医療情報システム部門へ報告し、異常内容の事実確認を行う。）		

資料出所：厚生労働省「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」（2024年6月）

### ■ 目的

- 病院に対するランサムウェア等のサイバー攻撃が増加し、長期にわたり診療が停止した事例が確認されていることから、病院におけるランサムウェアのリスクを把握するとともに、長期に診療が停止することがないよう早急に有効な対策の実施を促すことが必要。
- 病院が保有する電子カルテシステム等の医療情報システムのサイバーセキュリティ対策の実態を、昨年に引き続き調査する。

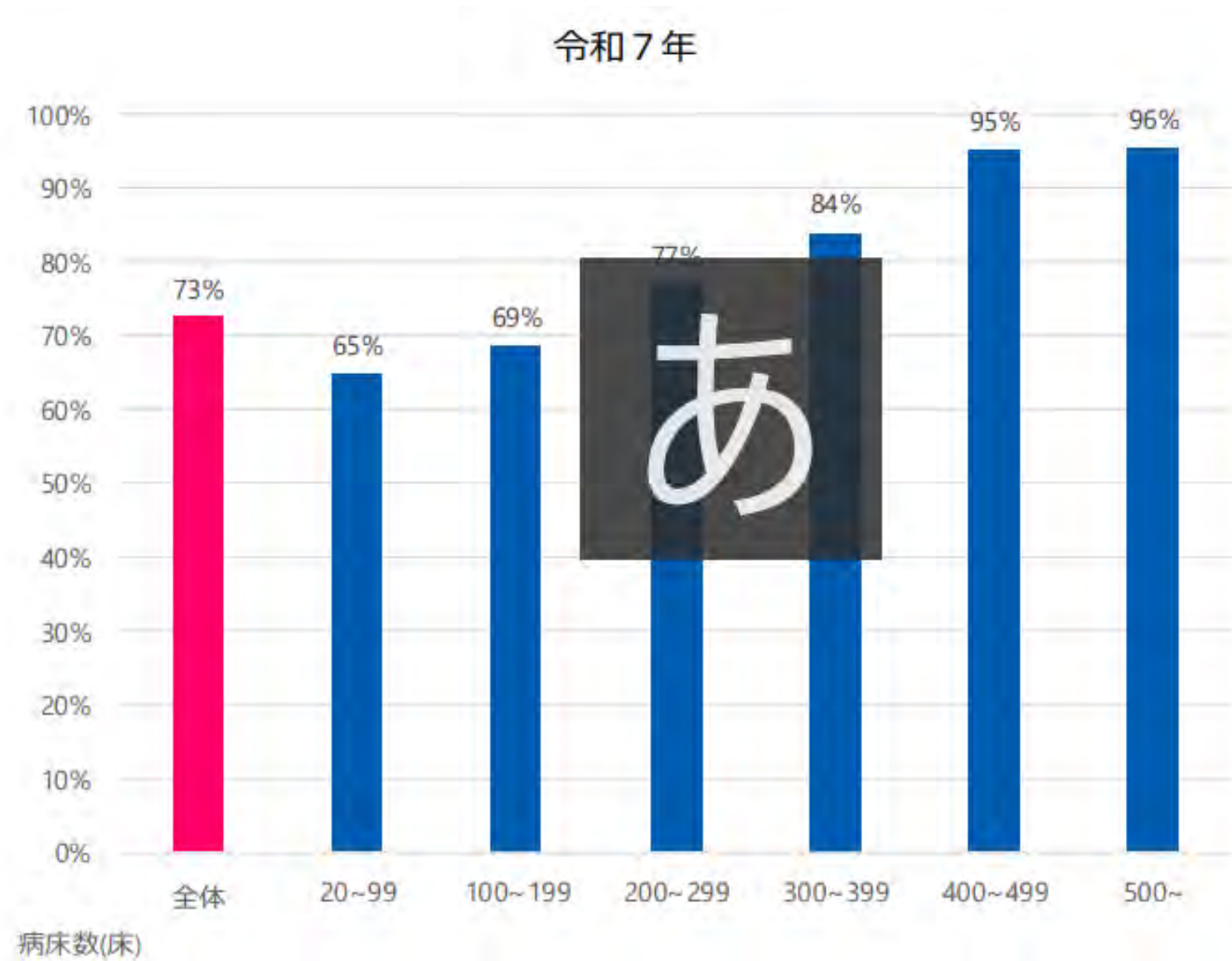
### ■ 調査対象

- 調査対象は、G-MIS IDが付与されている病床数20床以上の8,117の病院
- 有効回答数：5,842施設（回答率：72.0%）

### ■ 調査期間

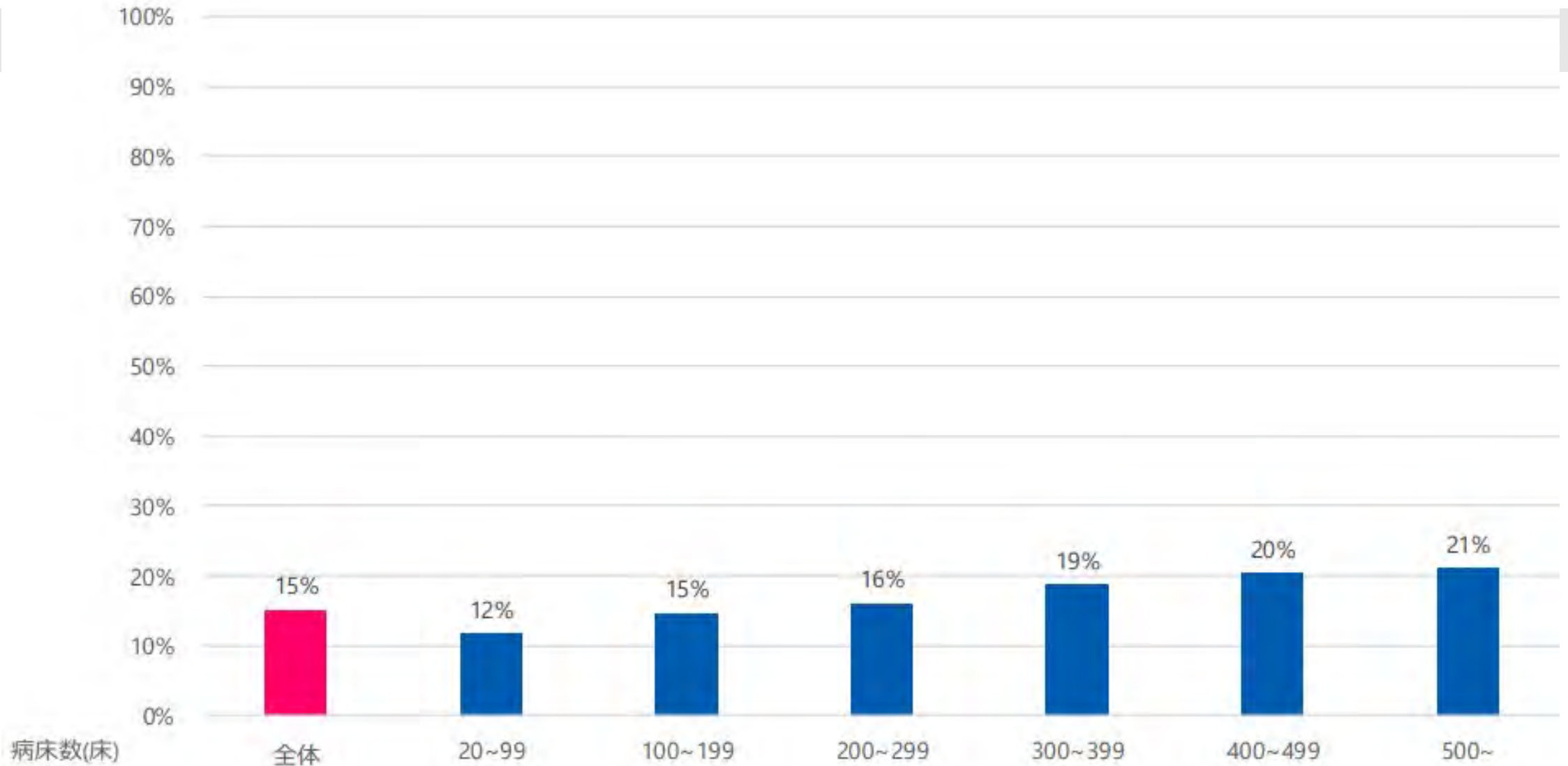
- 2025年1月27日（月）～2025年3月7日（金）

資料出所：第25回 健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ（2025年7月24日）  
厚生労働省「病院における医療情報システムのサイバーセキュリティ対策に係る調査の結果について」



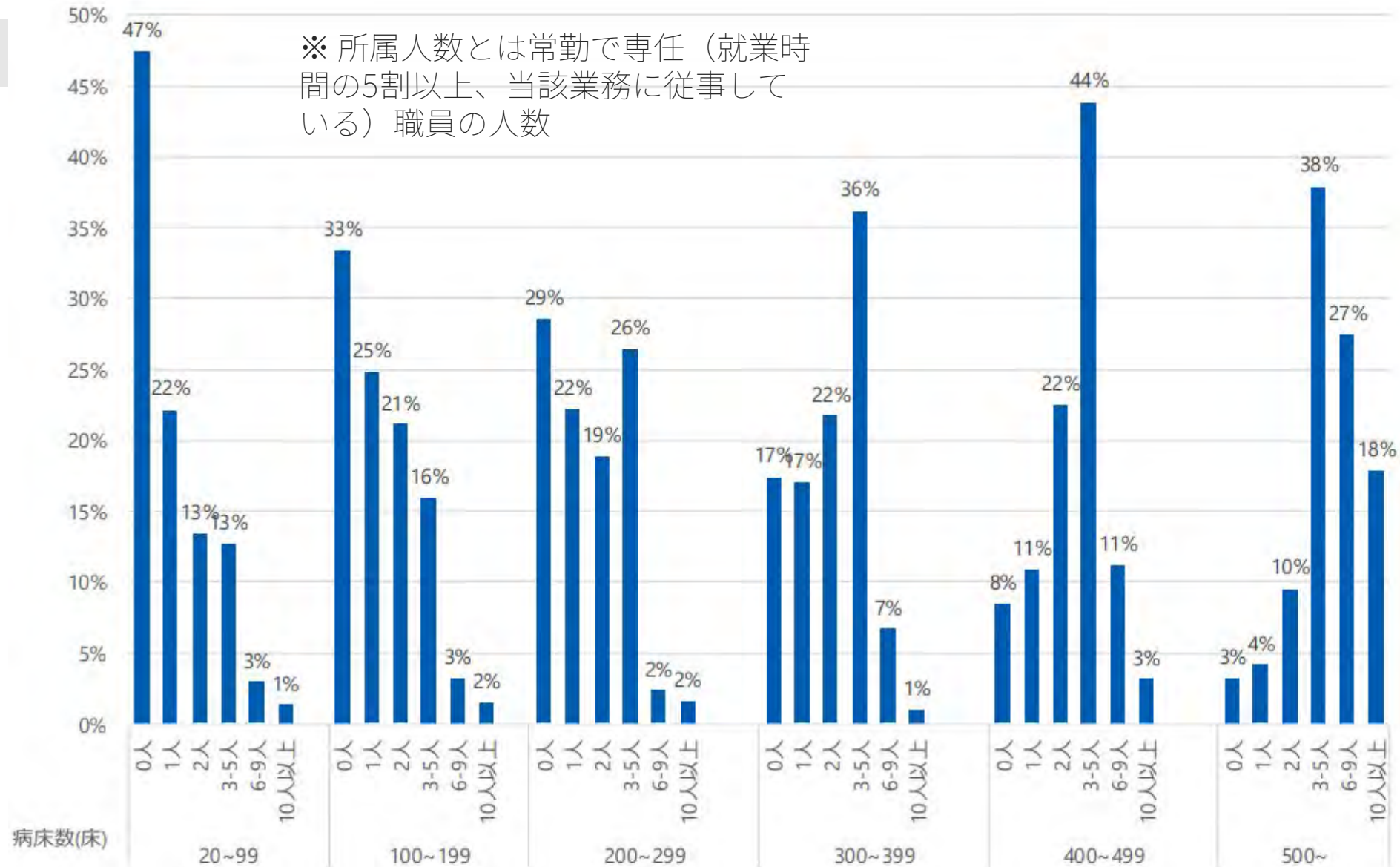
資料出所：第25回 健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ（2025年7月24日）  
厚生労働省「病院における医療情報システムのサイバーセキュリティ対策に係る調査の結果について」

## 8-2. CISOは医療情報に関連した資格を保持している



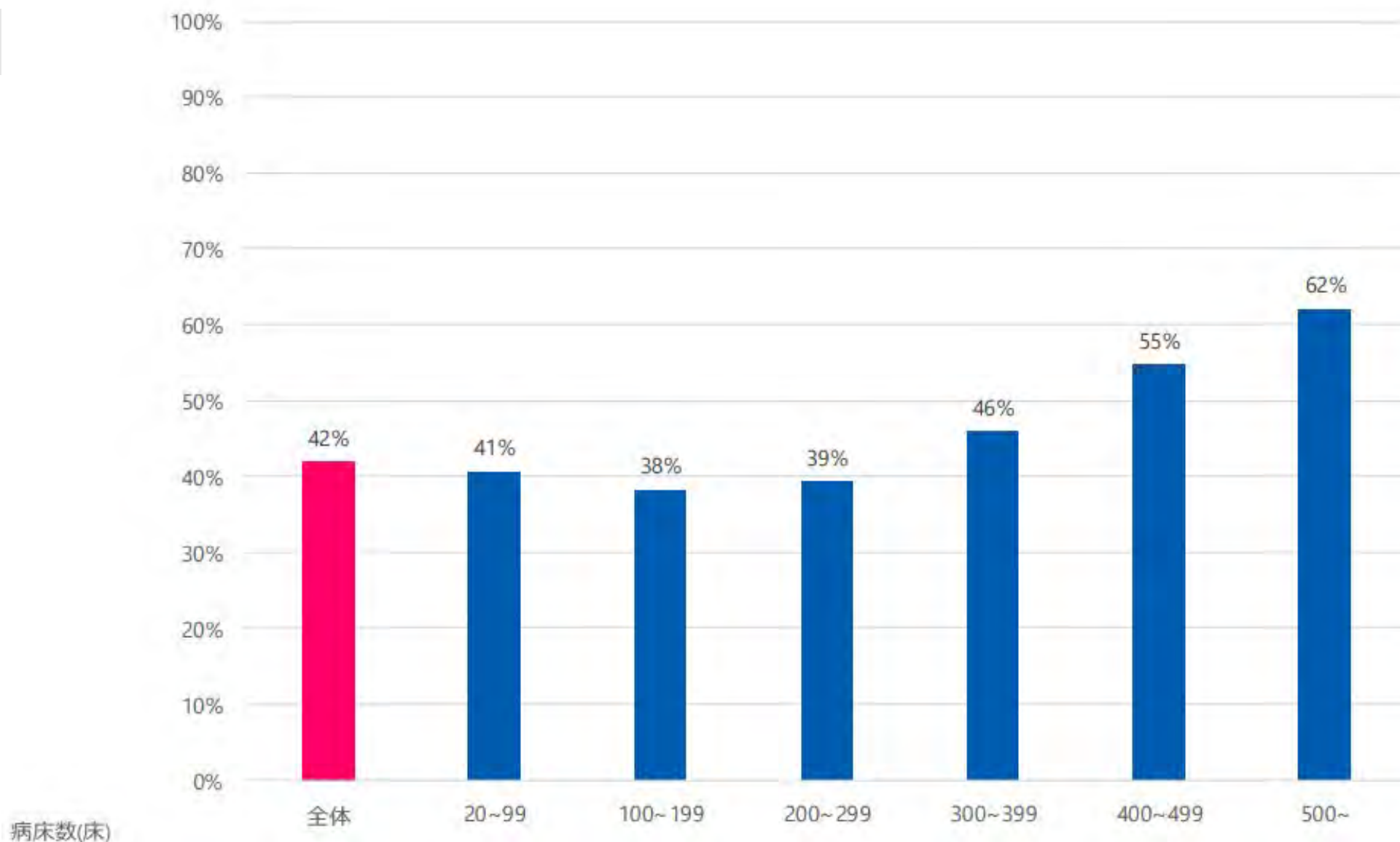
資料出所：第25回 健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ（2025年7月24日）  
厚生労働省「病院における医療情報システムのサイバーセキュリティ対策に係る調査の結果について」

### 8-3.情報システム部門の所属人数



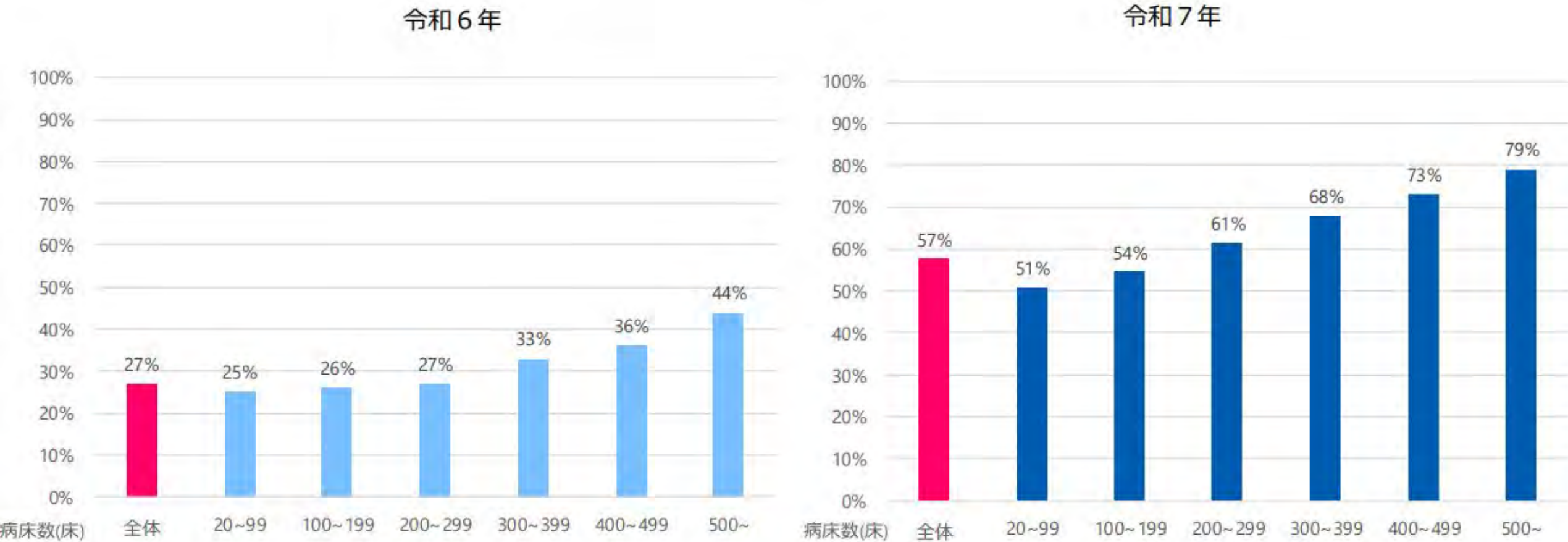
資料出所：第25回 健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ（2025年7月24日）  
厚生労働省「病院における医療情報システムのサイバーセキュリティ対策に係る調査の結果について」

## 8-4. インシデント発生時の対策チーム（組織内CSIRT）を設置している



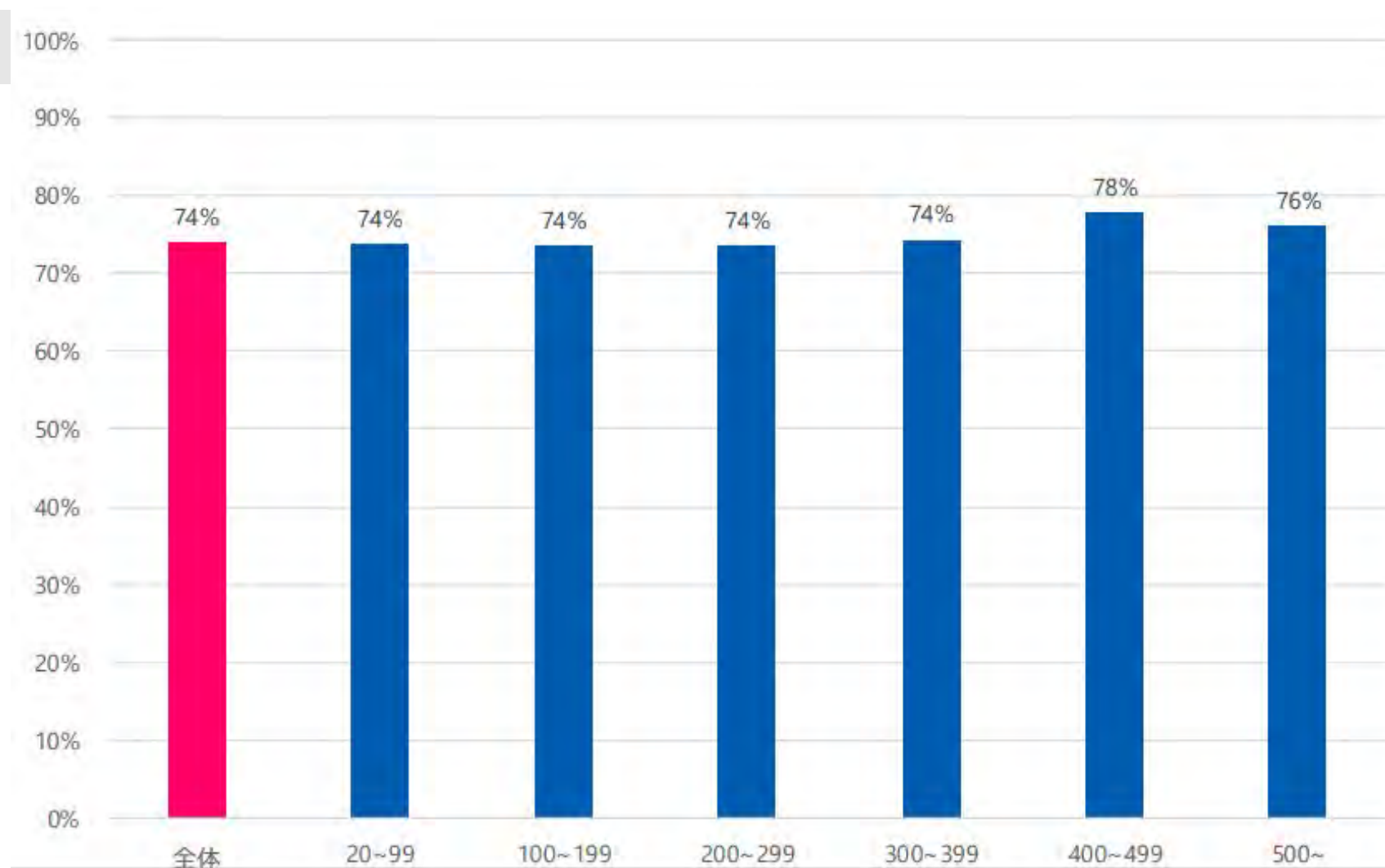
資料出所：第25回 健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ（2025年7月24日）  
厚生労働省「病院における医療情報システムのサイバーセキュリティ対策に係る調査の結果について」

## 8-5.事業継続計画（BCP）を策定している



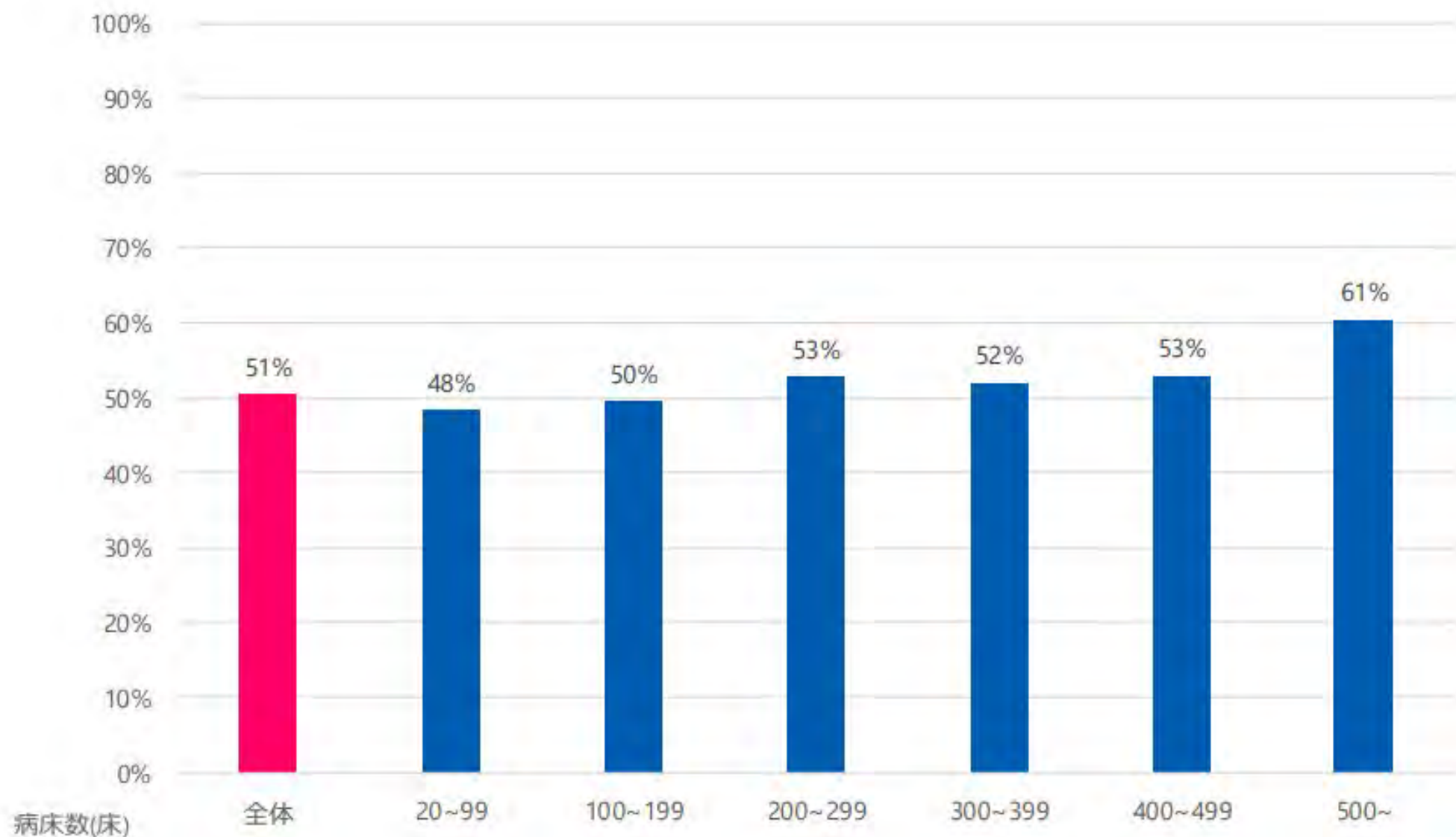
資料出所：第25回 健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ（2025年7月24日）  
厚生労働省「病院における医療情報システムのサイバーセキュリティ対策に係る調査の結果について」

## 8-6. ネットワーク機器に定期的にセキュリティパッチを適用している



資料出所：第25回 健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ（2025年7月24日）  
厚生労働省「病院における医療情報システムのサイバーセキュリティ対策に係る調査の結果について」

## 8-7. 医療機関とシステム事業者等の役割を契約書やサービスレベル合意書に落とし込んでいる



資料出所：第25回 健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ（2025年7月24日）

- 医療機関におけるサイバー攻撃が顕在化したことで、**基幹インフラ制度への医療分野の追加を検討することが言及される**ようになる。
  - 2024年の経済安全保障法改正法案に対する衆参内閣委員会の附帯決議
  - 「経済財政運営と改革の基本方針2024」（2024年6月21日閣議決定）
- **第11回経済安全保障法制に関する有識者会議（2024年12月24日）**において、今後、医療DXの推進やそれに伴う医療機関のシステム環境の変化が見込まれることやサイバー安全保障に関する有識者会議で、基幹インフラ等に関する情報共有の促進等が提言されたことも踏まえ、**以下の方針で検討を進め、速やかに必要な対応を行う**とされた。
  - ① 個別の**医療機関**については、基幹インフラ制度の対象となり得る医療機関や特定重要設備等の検討を行い、2025年度夏までに結論を得る。
  - ② **社会保険診療報酬支払基金**については、基幹インフラ制度の対象となり得る特定重要設備等の検討を行い、2025年度夏までに結論を得る。（厚生労働省は、医療DXの推進に当たり、同基金を改組し、診療報酬等の審査支払機能に加え、医療DXに係るシステムの開発・運用主体とする予定）

## ■ 第121回「社会保障審議会医療部会」（2025年11月25日）が開催

- 経済安全保障推進法の枠組みは、法律で対象となる分野を外縁として規定。それぞれの分野について、必要な範囲に細分化し政令で絞り込み。
- 検討項目は、①対象医療機関の範囲と②医療機関における特定重要設備
- 対象医療機関の範囲については、特定社会基盤事業者の指定基準の考え方である事業規模（病床数等）及び代替可能性（地域医療において果たす役割や医療提供能力、広域な観点の医療機関機能等）のほか、救急医療や災害医療の拠点及びそれらのバックアップとしての役割などの観点から総合的に検討を行った結果、地域における最後の砦としての機能を有する特定機能病院を念頭に指定することとする。地域性を考慮しつつ、段階的に指定範囲を拡大。
- 特定機能病院の特定重要設備は、設備が停止した場合の社会的混乱の規模や、患者の生命に直結するか否か等の観点を踏まえ、電子カルテ、手術部門、集中治療部門に関連する設備から選定する方向で検討。
- 社会保険診療報酬支払基金を特定社会基盤事業者とし、電子カルテ情報共有サービス、電子処方箋管理サービス、オンライン資格確認等システムに係る設備を特定重要設備とすることを念頭に制度改正に向けた検討を進める

# (参考) 特定機能病院の一覧 (令和7年4月1日現在)

北海道	札幌医科大学附属病院	853
	北海道大学病院	944
	旭川医科大学病院	602
青森県	弘前大学医学部附属病院	636
岩手県	岩手医科大学附属病院	1,000
宮城県	東北大学病院	1,160
秋田県	秋田大学医学部附属病院	615
山形県	山形大学医学部附属病院	637
福島県	福島県立医科大学附属病院	778
茨城県	筑波大学附属病院	809
栃木県	自治医科大学附属病院	1,132
	獨協医科大学病院	1,195
群馬県	群馬大学医学部附属病院	731
埼玉県	埼玉医科大学病院	961
	防衛医科大学校病院	800
千葉県	千葉大学医学部附属病院	850
	国立がん研究センター東病院	427
東京都	国立がん研究センター中央病院	578
	聖路加国際病院	520
	東京慈恵会医科大学附属病院	1,075
	順天堂大学医学部附属順天堂医院	1,051
	東京科学大学病院	813
	東京大学医学部附属病院	1,226
	日本医科大学付属病院	877
	昭和医科大学病院	815
	東邦大学医療センター大森病院	916
	東京医科大学病院	904
	慶應義塾大学病院	950
	国立健康危機管理研究機構国立国際医療センター	716
	帝京大学医学部附属病院	1,068
	日本大学医学部附属板橋病院	990
	がん研究会有明病院	686
	杏林大学医学部附属病院	1,137

神奈川県	横浜市立大学附属病院	671
	聖マリアンナ医科大学病院	955
	東海大学医学部附属病院	804
	北里大学病院	1,135
新潟県	新潟大学医歯学総合病院	827
富山県	富山大学附属病院	612
石川県	金沢大学附属病院	830
	金沢医科大学病院	817
福井県	福井大学医学部附属病院	600
山梨県	山梨大学医学部附属病院	618
長野県	信州大学医学部附属病院	717
岐阜県	岐阜大学医学部附属病院	614
静岡県	静岡県立静岡がんセンター	615
	浜松医科大学医学部附属病院	613
愛知県	愛知県がんセンター	500
	名古屋大学医学部附属病院	1,080
	名古屋市立大学病院	800
	藤田医科大学病院	1,376
	愛知医科大学病院	900
三重県	三重大学医学部附属病院	685
滋賀県	滋賀医科大学医学部附属病院	603
京都府	京都府立医科大学附属病院	1,065
	京都大学医学部附属病院	1,131
大阪府	大阪大学医学部附属病院	1,086
	国立循環器病研究センター	550
	大阪医科薬科大学病院	903
	関西医科大学附属病院	797
	近畿大学病院	919
	大阪公立大学医学部附属病院	965
	大阪国際がんセンター	500
兵庫県	兵庫医科大学病院	963
	神戸大学医学部附属病院	934

奈良県	奈良県立医科大学附属病院	992
和歌山県	和歌山県立医科大学附属病院	800
鳥取県	鳥取大学医学部附属病院	697
島根県	島根大学医学部附属病院	600
岡山県	岡山大学病院	853
	川崎医科大学附属病院	1,182
広島県	広島大学病院	742
山口県	山口大学医学部附属病院	754
徳島県	徳島大学病院	692
香川県	香川大学医学部附属病院	613
愛媛県	愛媛大学医学部附属病院	644
高知県	高知大学医学部附属病院	613
福岡県	九州大学病院	1,252
	福岡大学病院	771
	久留米大学病院	1,018
	産業医科大学病院	674
佐賀県	佐賀大学医学部附属病院	602
長崎県	長崎大学病院	874
熊本県	熊本大学病院	845
大分県	大分大学医学部附属病院	618
宮崎県	宮崎大学医学部附属病院	604
鹿児島県	鹿児島大学病院	653
沖縄県	琉球大学病院	600

○47都道府県に88病院が存在。  
 (多い順に、東京都16、大阪府7、愛知県5、神奈川県4、福岡県4、等)  
 ○そのうち、大学附属病院は79病院。  
 ○右欄の数字は病床数 (R6.10厚生局)

資料出所：  
 令和7年11月25日  
 第121回社会保障審  
 議会医療部会資料

- 経済安全保障法制に関する有識者会議 推進法改正に関する検討会合での議論を経て、第14回（2026年1月16日）に「経済安全保障の更なる推進に向けた提言」が公表
- 提言の骨子は5つ
  - サプライチェーン強靱化
  - 基幹インフラ役務の安定提供・特定重要技術の研究開発等
  - 海外事業の展開支援
  - 総合的な経済安全保障シンクタンク及び官民協議会
  - データセキュリティ → 個人に関する機微なデータ（例えば、ゲノムデータ、医療情報、金融情報、生体認証情報、位置情報等）の漏洩リスクとそのための方策の検討
- 提言を踏まえた経済安全保障推進法の改正案が、自民党の経済安全保障推進本部において2026年3月12日に了承、今週（3月16日～）には、政府での閣議決定され、今国会に提出予定。

- 医療DXの推進に関する工程表の基づき、「全国医療情報プラットフォーム」の創設、電子カルテの標準化等、診療報酬改定DXその他関連する医療DX施策が推進されている。データの一次利用および二次利用のために、**医療機関をはじめとして、関係機関がネットワーク化し、データ連携**していく社会を見据えている。
- 一方で、サイバー攻撃などのインシデントが発生した際の**リスクは拡大し、影響は甚大**となる。
- 「病院における医療情報システムのサイバーセキュリティ対策に係る調査」からも明らかのように、**ネットワーク化が進む現状**に対して、医療機関のセキュリティ対策は十分とはいえる状況ではなく、特に、**規模の小さい医療機関の対応が遅れている**。
- 経済安全保障法改正による直接的な影響は医療情報基盤・診療報酬審査支払機構（旧社会保険診療報酬支払基金）と特定機能病院ということになるが、ネットワーク化が進む中で、**結果的にそこに連なるすべての機関のセキュリティ向上**が求められる。
- セキュリティ向上＝アクセシビリティ・ユーザビリティの低下とならないよう、**セキュリティ・バイ・デザイン**（システムやソフトウェアの企画・設計段階からセキュリティを組み込む開発アプローチ）と**ユーザ中心設計**（ユーザーのニーズや行動を理解し、それに基づいた設計）を組み合わせていくべき。

- ヘルスケアデータを流通させるためには、**トラストの醸成が重要**であり、データをやりとりする相手の情報システムのセキュリティが担保され、安全なデータ交換ができることが**データ流通を促進**させる。経済安全保障法改正による医療分野の追加はその**底上げに大きく貢献**すると期待される。
- また、デジタルの世界の話であっても、人は信頼できる相手でなければ連携を進めることはできない。**アナログの世界でのトラストの醸成も併せて検討すべき**である。
- 自分自身のデータや自組織が保有するデータを提供するためのインセンティブも必要となる。**インセンティブは、金銭的なものだけでなく、社会を良くしたい、未来を良くしたいという思いも含まれる**。
- また、ヘルスケアデータの提供を法律で定め「**デジタル公共財**」とすることで、**流通を促進**することもできるかもしれない。
- トラストの醸成を前提として、ヘルスケアに関わるステークホルダーがお互いwin-winとなるような**データ流通のエコシステム**を構築することで、DXを加速化させていくべきといえる。

**I I S E**