資料７

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

第32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

2026（令和8）年5月29日

「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

厚生労働省　医政局

医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

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（概要）

背景・目的

○　病院に対するランサムウェア等のサイバー攻撃が継続して発生しており、長期にわたり診療が停止した事例も確認されている。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である。

○　本調査の目的は、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調査し、これまでの政策の効果確認に加え、今後の政策方針の決定に資するものとして、令和５年度以降、毎年定期的に調査を実施しているもの。

調査方法・対象・条件

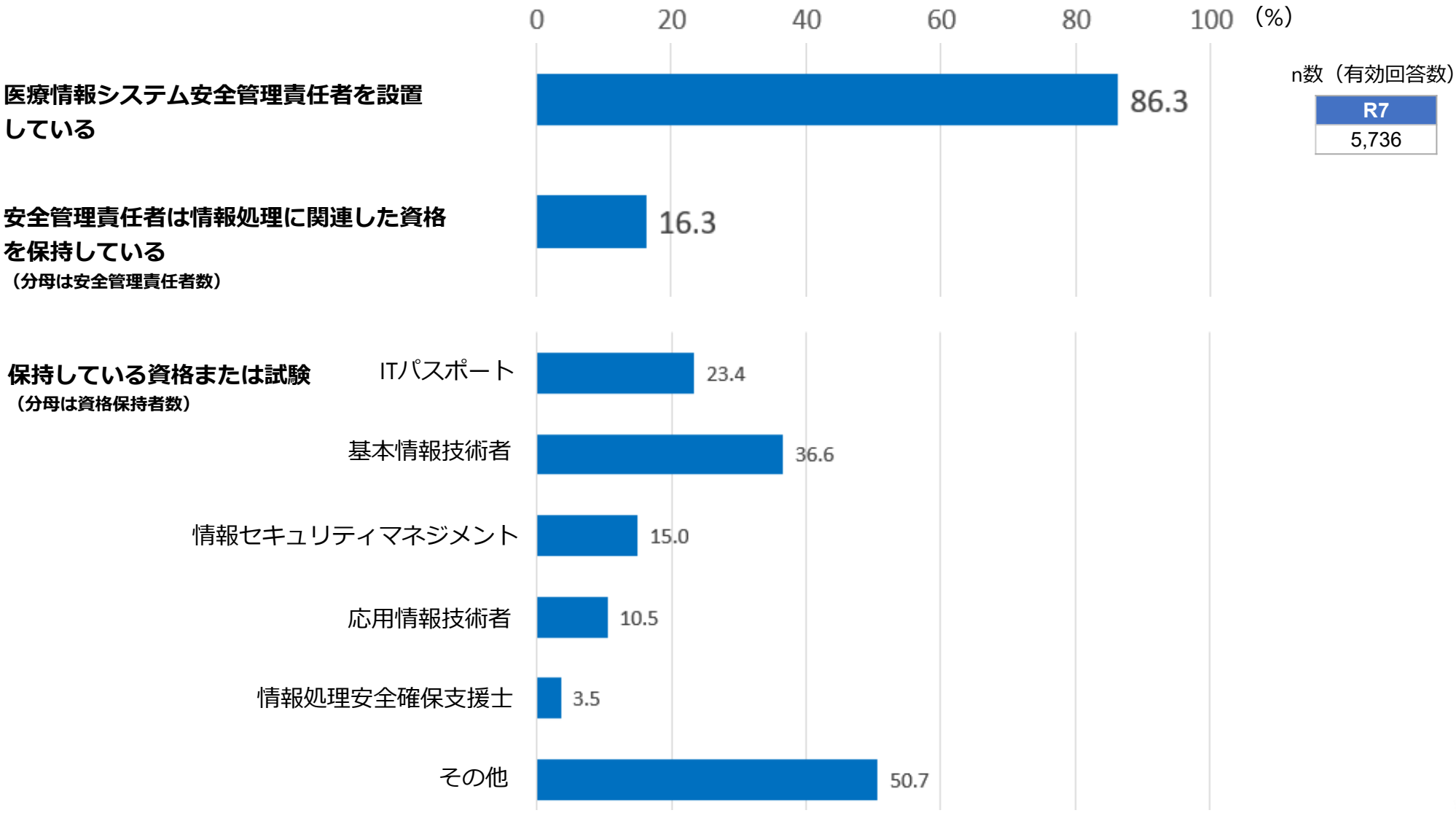
- G-MIS（Gathering Medical Information System）を用いて、病院のサイバーセキュリティ対策の実態に関するアンケート調査を実施。
- 調査対象は、G-MIS IDが付与されている病院（**8,102施設**）
- 令和8年3月末時点の情報について回答を依頼した。
- 有効回答数：**5,736（70.8%）**施設 （令和７年：72.0%）
- 令 和５年５月31 日に発出された「医療情報システムの安全管理に関するガイドライン（6.0 版）」、令和７ 年５月に発出された「医療機関におけるサイバーセキュリティ対策チェックリスト」及び厚生労働省等から発出された通知・事務連絡等において周知した対策への取組状況について質問した。

調査期間

・令和8年3月9日（月）～　令和8年4月24日（金）

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（概要）
－ 医療情報システム安全管理責任者 －

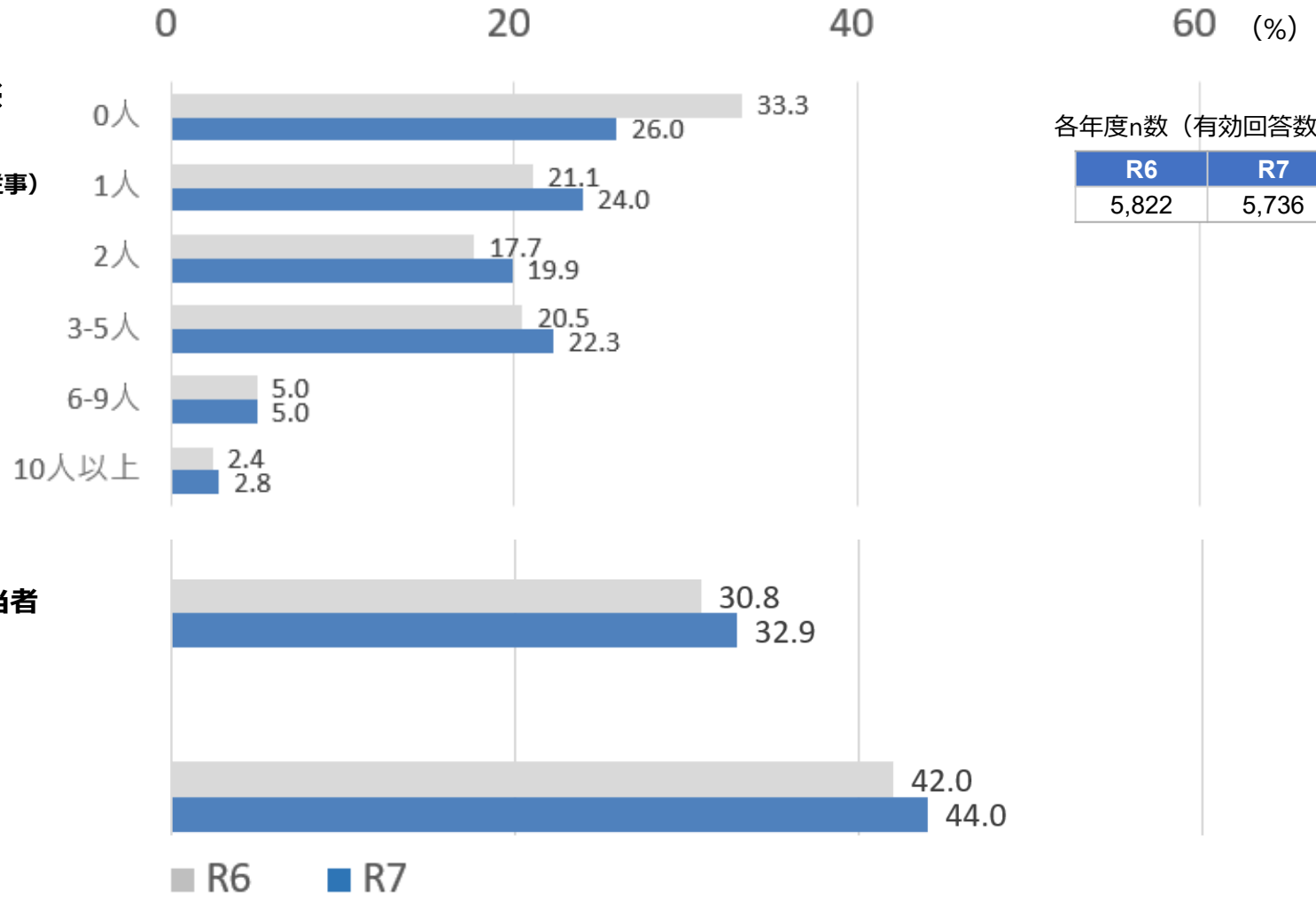
○　医療情報システム安全管理責任者の情報処理資格の保持割合は16%であり、その資格はITSSレベル２※の基本情報技術者が最も多い。
※IT Skill Standard：経産省の策定するITプロフェッショナルに求められるスキルを体系化した指標



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（概要）
－ 院内セキュリティ体制 －

○　院内システム部門の所属人数は0人が最頻値であるものの、その割合は減少している。各部門におけるセキュリティ担当者の配置割合やCSIRT※の設置割合も微増している。

※CSIRT：Computer Security Incident Response Team。サイバー攻撃発生時などに被害の最小化や迅速な復旧を図る専門チーム。

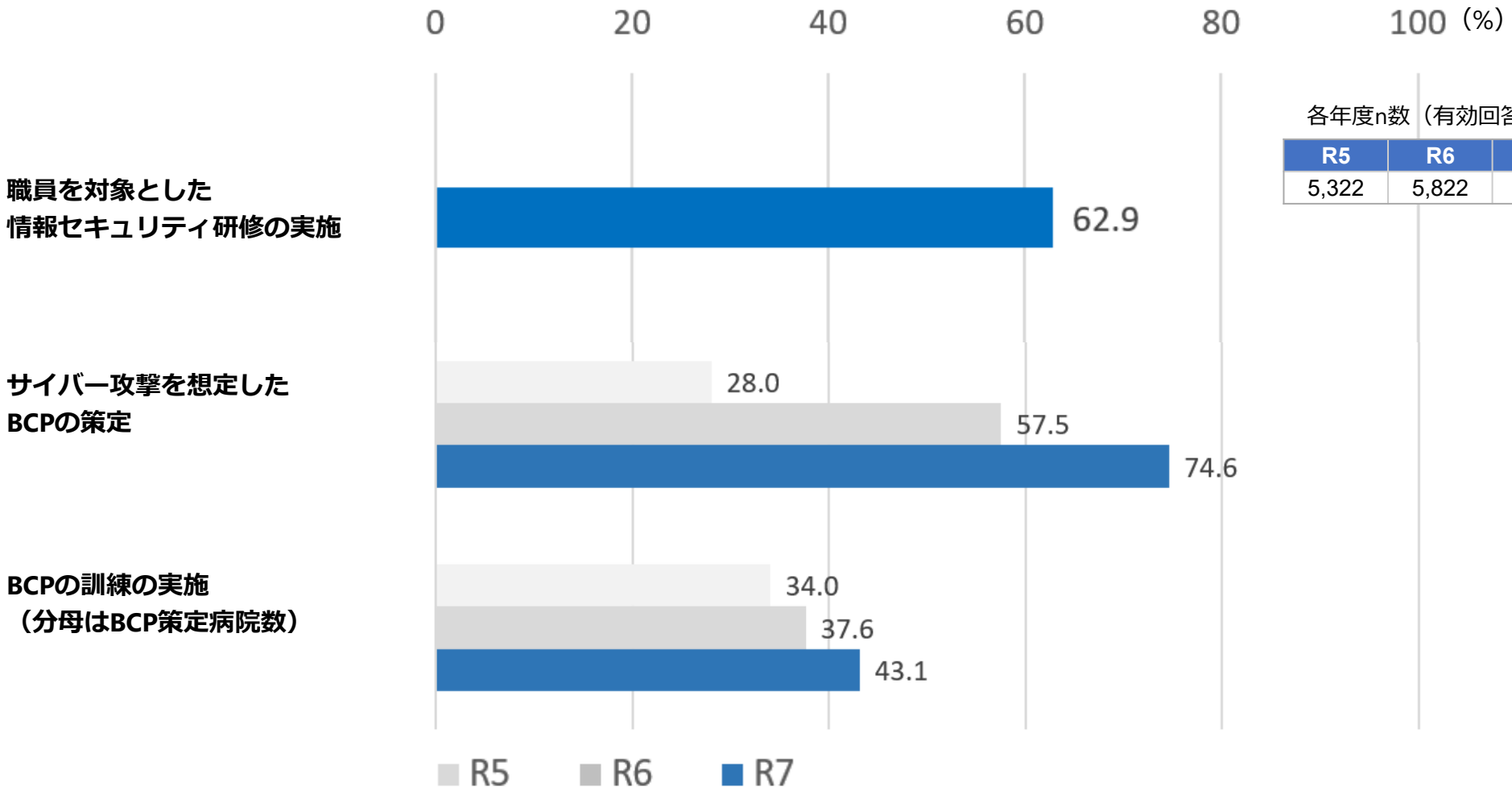


各年度n数（有効回答数）

R6	R7
5,822	5,736

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（概要）
－ 研修・訓練とBCP策定 －

○ セキュリティ研修の実施割合は63%であった。
○ BCPの策定と訓練の実施割合は令和6年度のチェックリスト項目化以降、年々増加している。

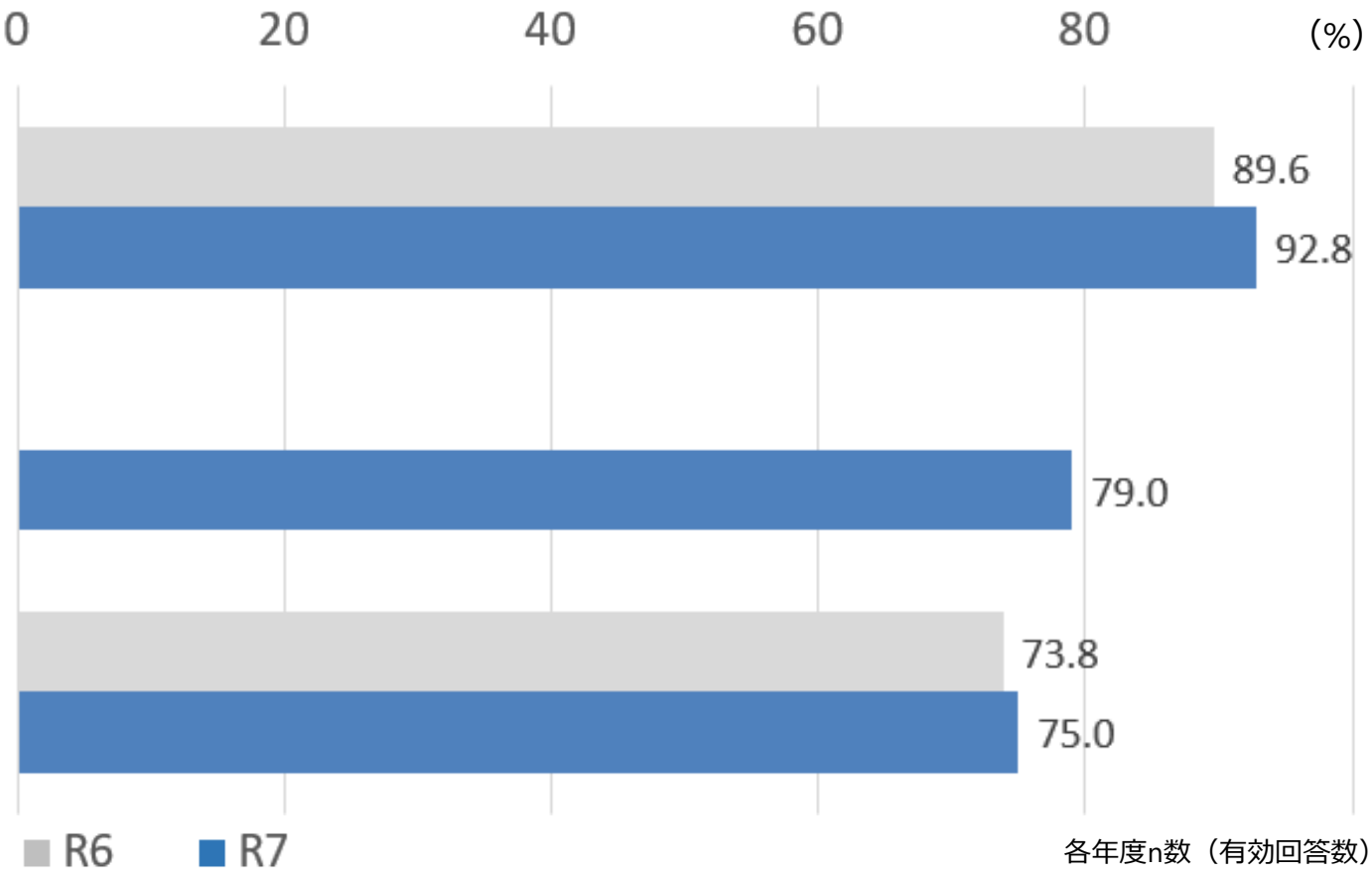


各年度n数（有効回答数）

R5	R6	R7
5,322	5,822	5,736

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（概要）
－ 資産管理 －

○　情報機器の台帳管理をしている病院の割合は高い水準からさらに増加したが、ネットワークに接続する医療機器の台帳管理を実施している病院の割合はそれよりも低かった。ネットワーク構成図を定期的に更新し、外部接続点数を把握できている病院の割合はさらに低いが、令和6年と比較して若干増加している。

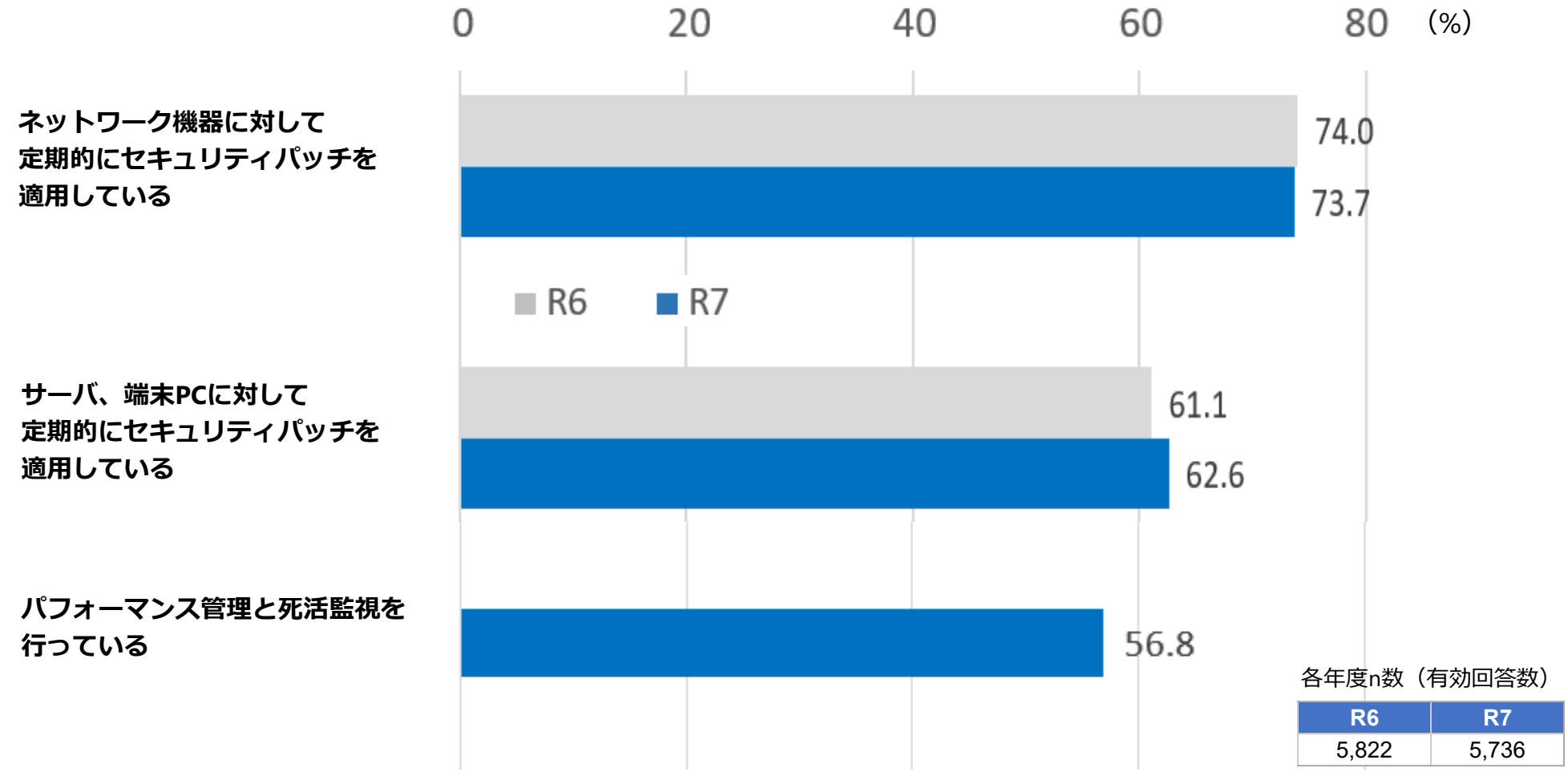


各年度n数（有効回答数）

R6	R7
5,822	5,736

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（概要）
－ 脆弱性管理と監視 －

○　ネットワーク機器とサーバ、定期的な端末PCのパッチ適用割合はほぼ横ばいであった。ネットワーク機器については外部接続点数を把握している病院割合と同程度となっているが、サーバ、端末PCのに対してセキュリティパッチを適用できている病院の割合は、台帳管理できている病院の割合よりも大幅に低い。また適切にシステムが稼働しているかのパフォーマンス管理や死活監視を実施できている医療機関はさらに少なかった。

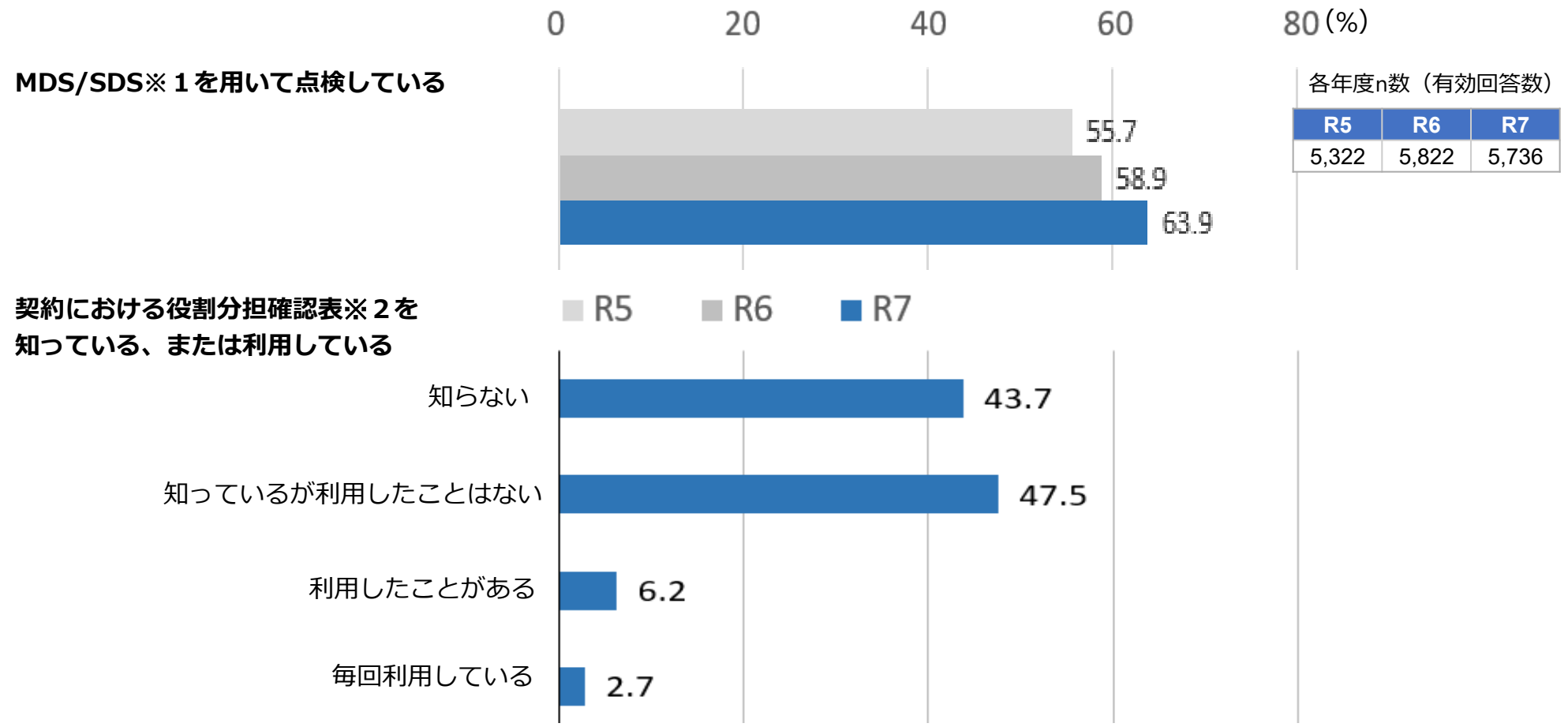


各年度n数（有効回答数）

R6	R7
5,822	5,736

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（概要）
– 契約における安全管理 –

○　MDS/SDS※1を用いた点検の実施割合は年々増加している。契約における役割分担確認表※2については知名度も44%程度であり、利用経験のある病院が10%未満となっている。



各年度n数（有効回答数）

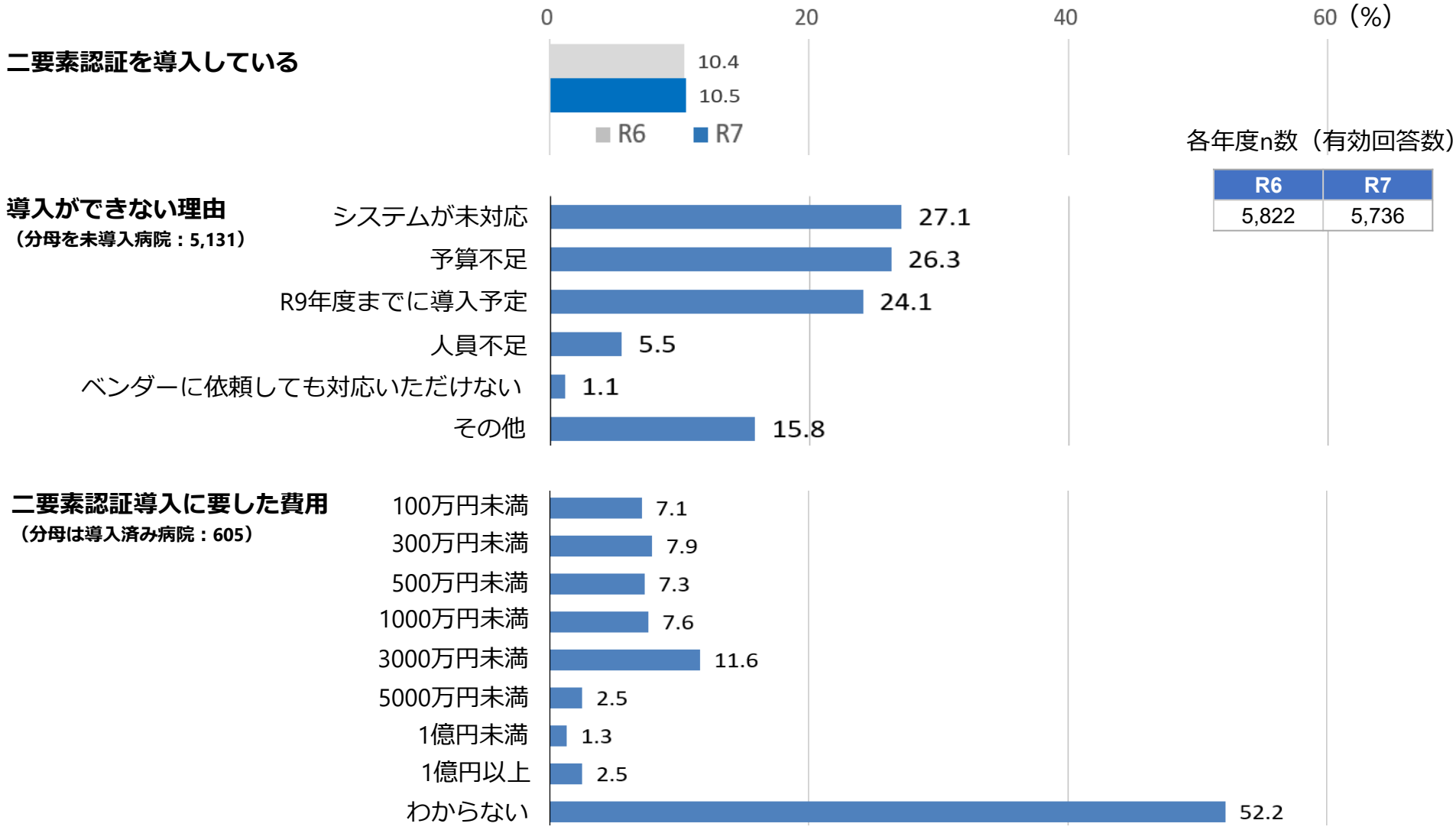
R5	R6	R7
5,322	5,822	5,736

※１：MDS/SDS（Manufacturer / Service Provider Disclosure Statment for Medical Information Security）自組織の情報機器・システムが「医療情報の安全管理に関するガイドライン」への準拠しているかを確認するための医療情報セキュリティ開示書

※２：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：総務省・厚生労働省・経済産業省においてとりまとめた、医療情報システムの契約時に医療機関と事業者の責任・役割分担をすりあわせ、契約書やサービスレベル合意書に落とし込むための確認表。

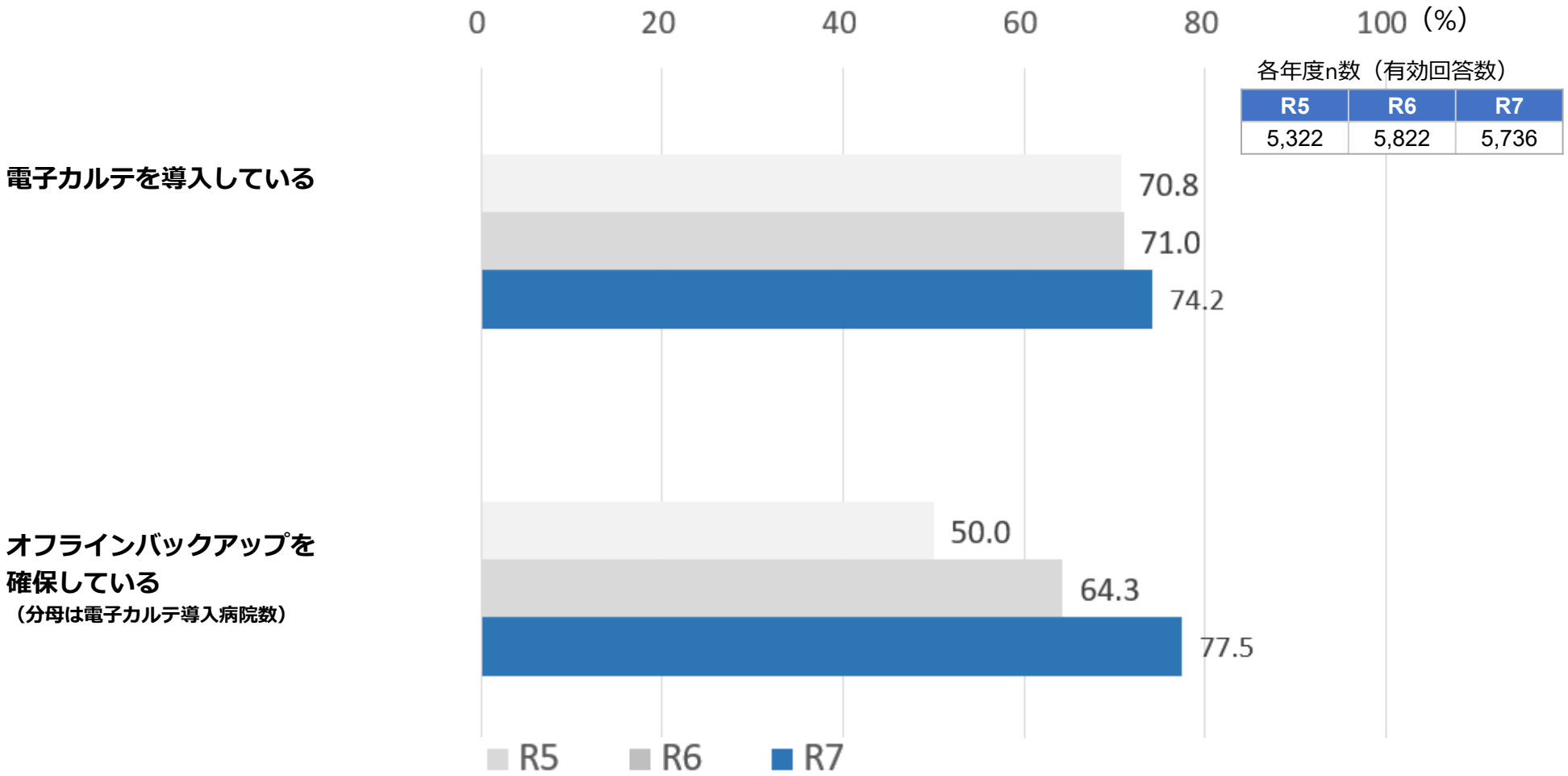
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）
－ 二要素認証の導入 －

○　二要素認証導入割合は昨年の10%程度と同様であった。一方で、R9年度までに導入予定の医療機関が24%存在する。システム自体が未対応であることと、病院の予算不足が原因として大きいことが今回の調査で明らかとなった。また、導入済の病院の中で導入費用を把握している病院において1000万円から3000万円程度が最頻値であった。



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（概要）
– 電子カルテとオフライン保存 –

○　電子カルテの導入割合は、74%と増加している。オフラインバックアップの確保割合についても令和6年度の診療報酬改定で、診療録管理体制加算の要件となった。その後年々増加している。



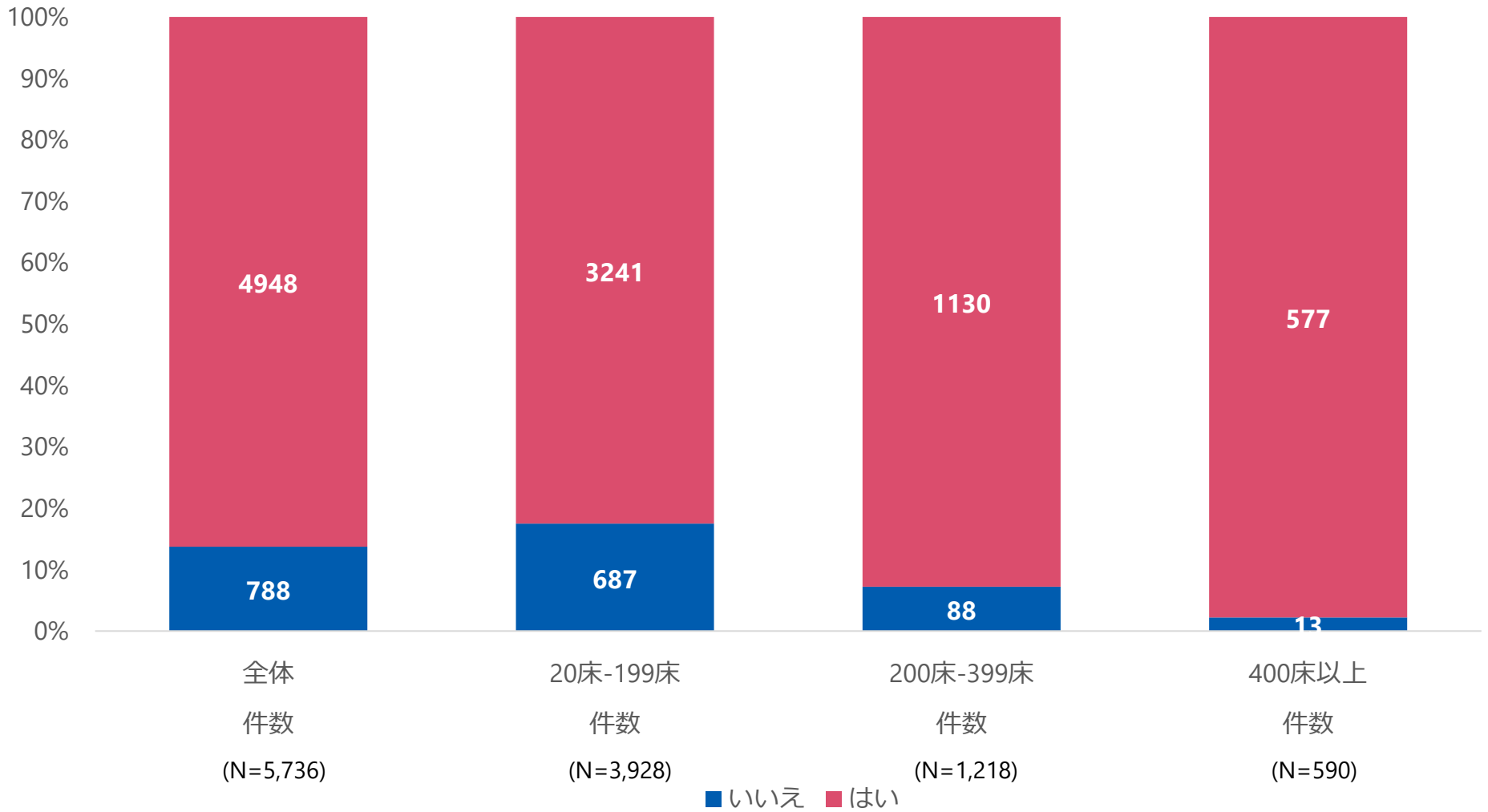
各年度n数（有効回答数）

R5	R6	R7
5,322	5,822	5,736

参考資料：病床規模別集計

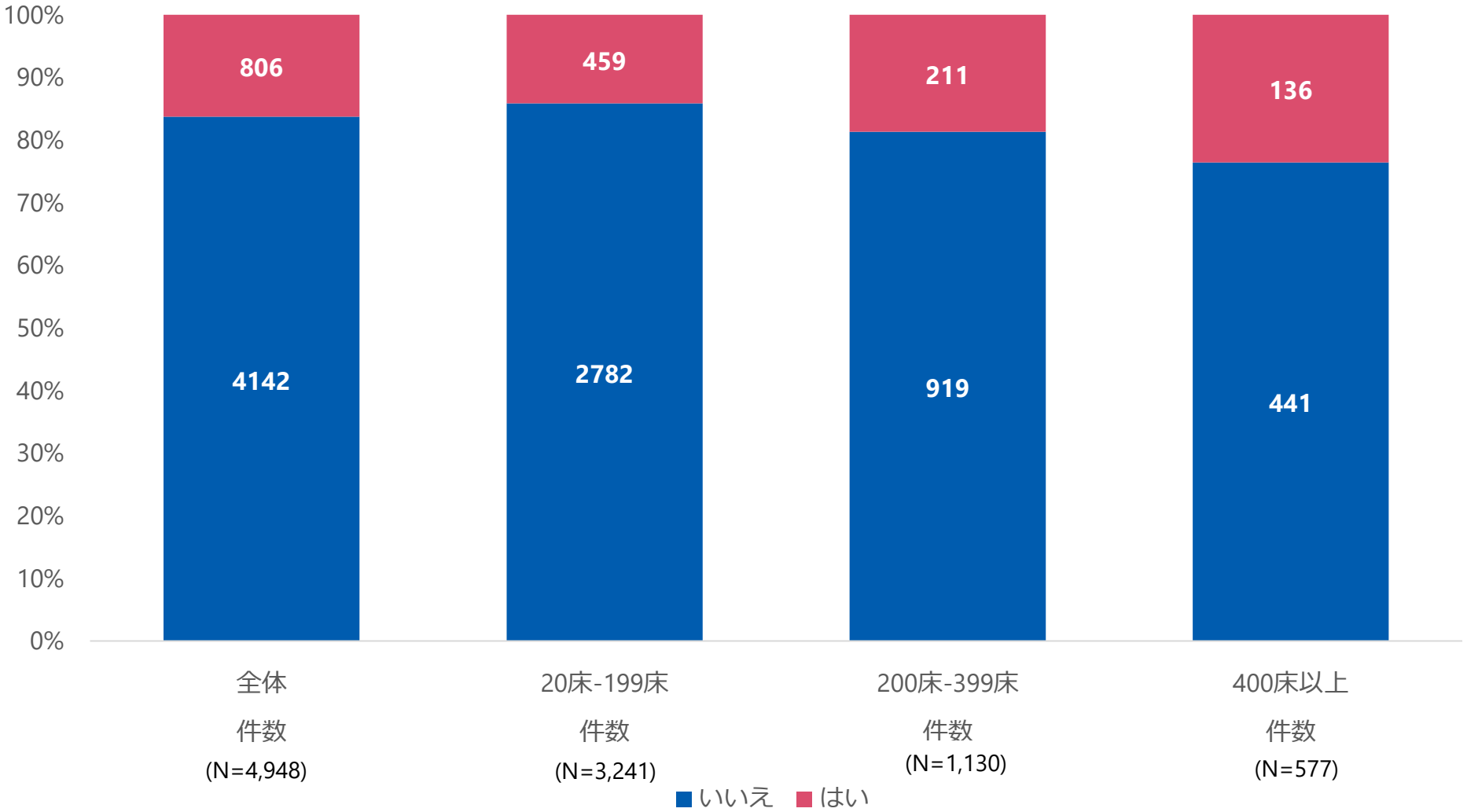
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

医療情報システム安全管理責任者を設置している



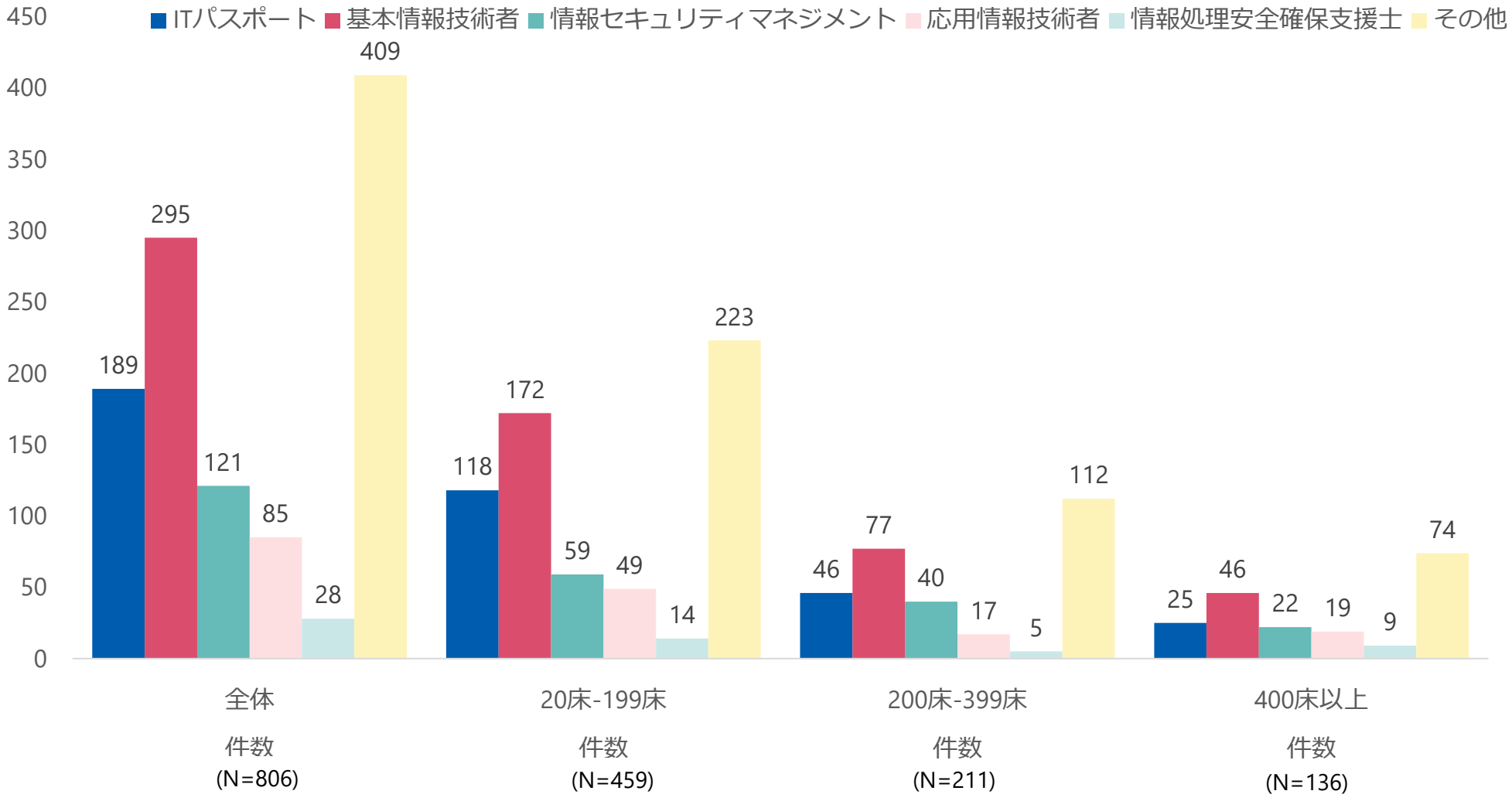
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

安全管理責任者は情報処理に関連した資格を保持している



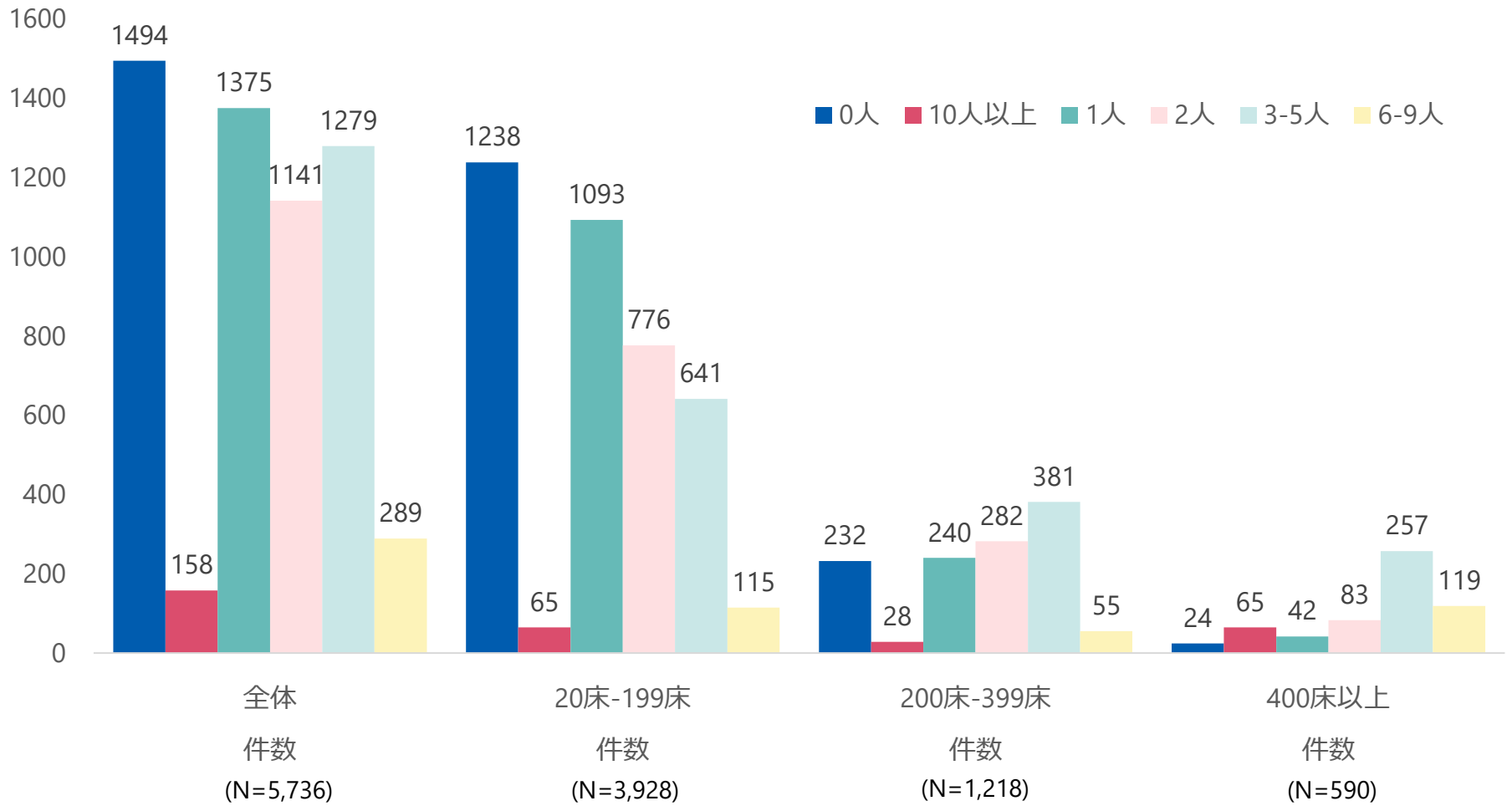
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

保持している資格または試験



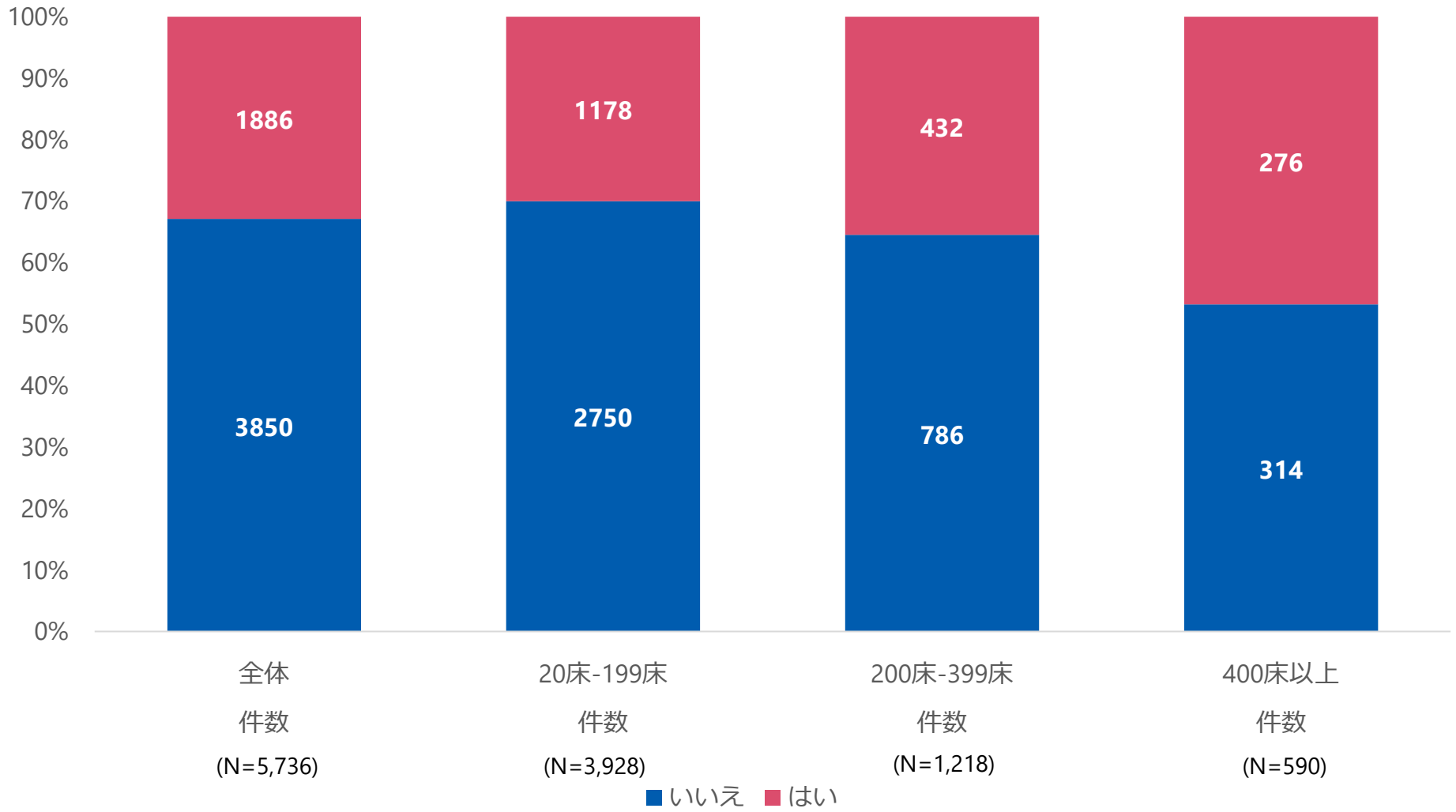
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

情報システム部門の所属人数



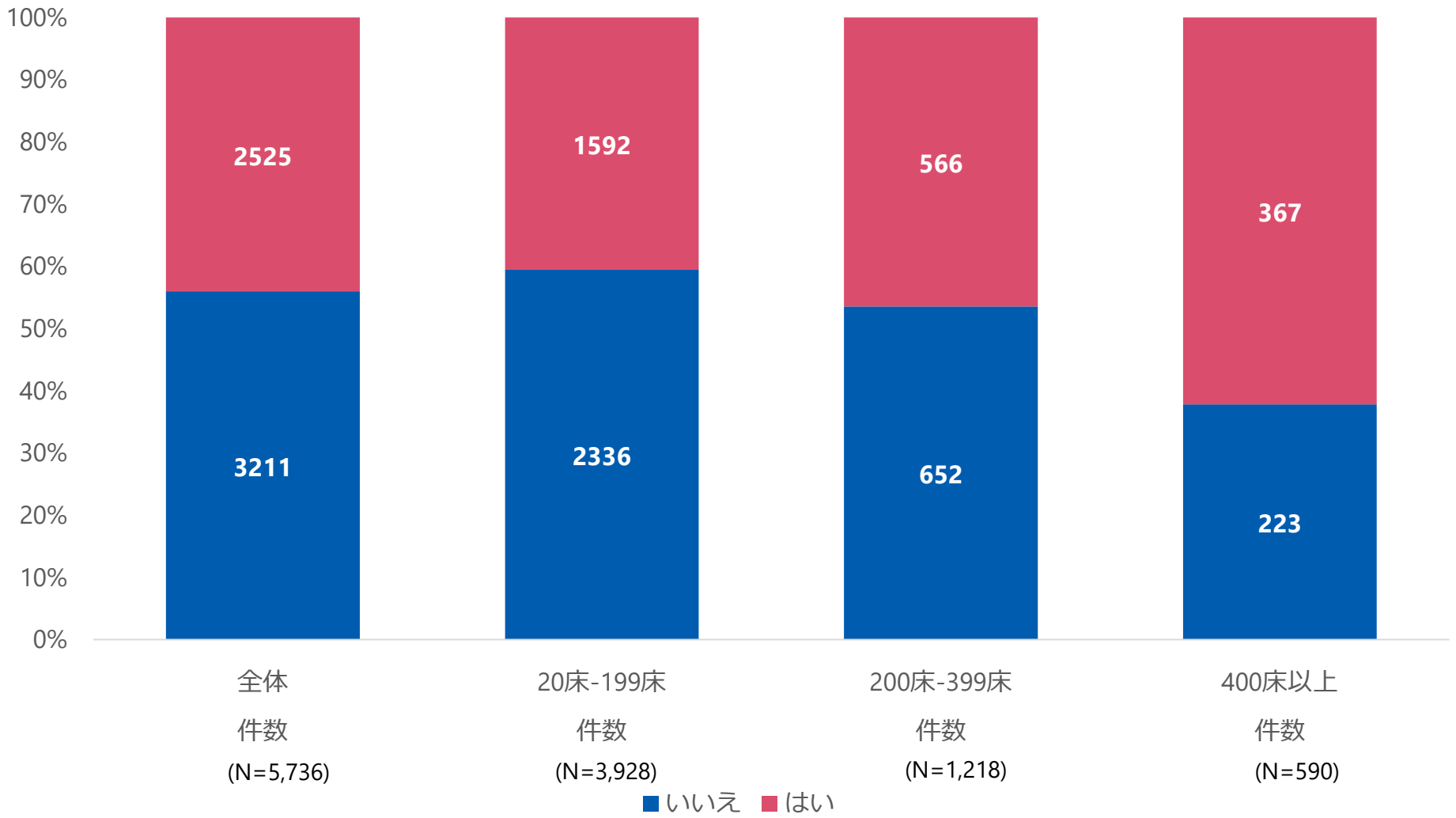
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

各部門に情報セキュリティ担当者を配置している



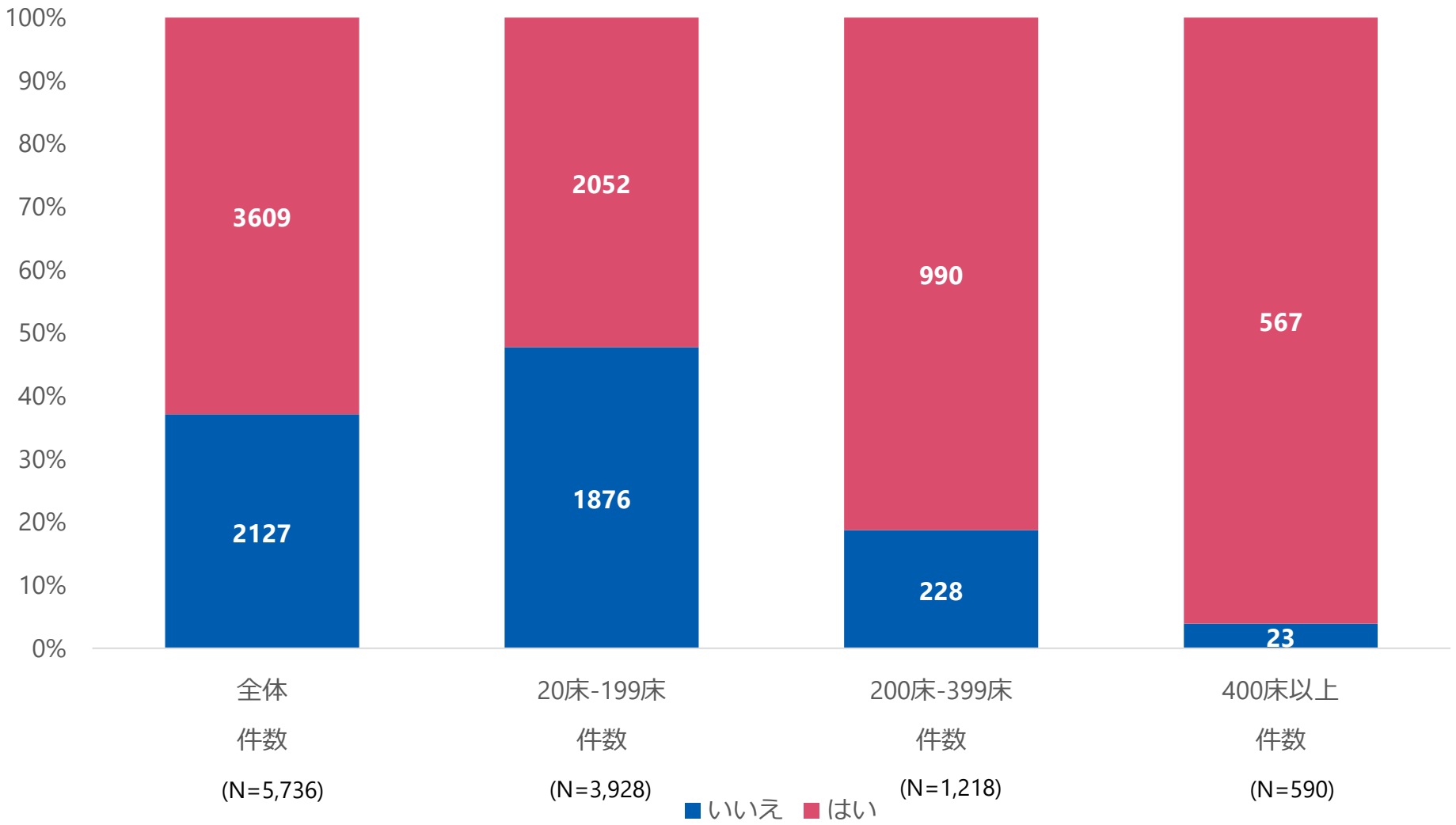
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

CSIRTを設置している



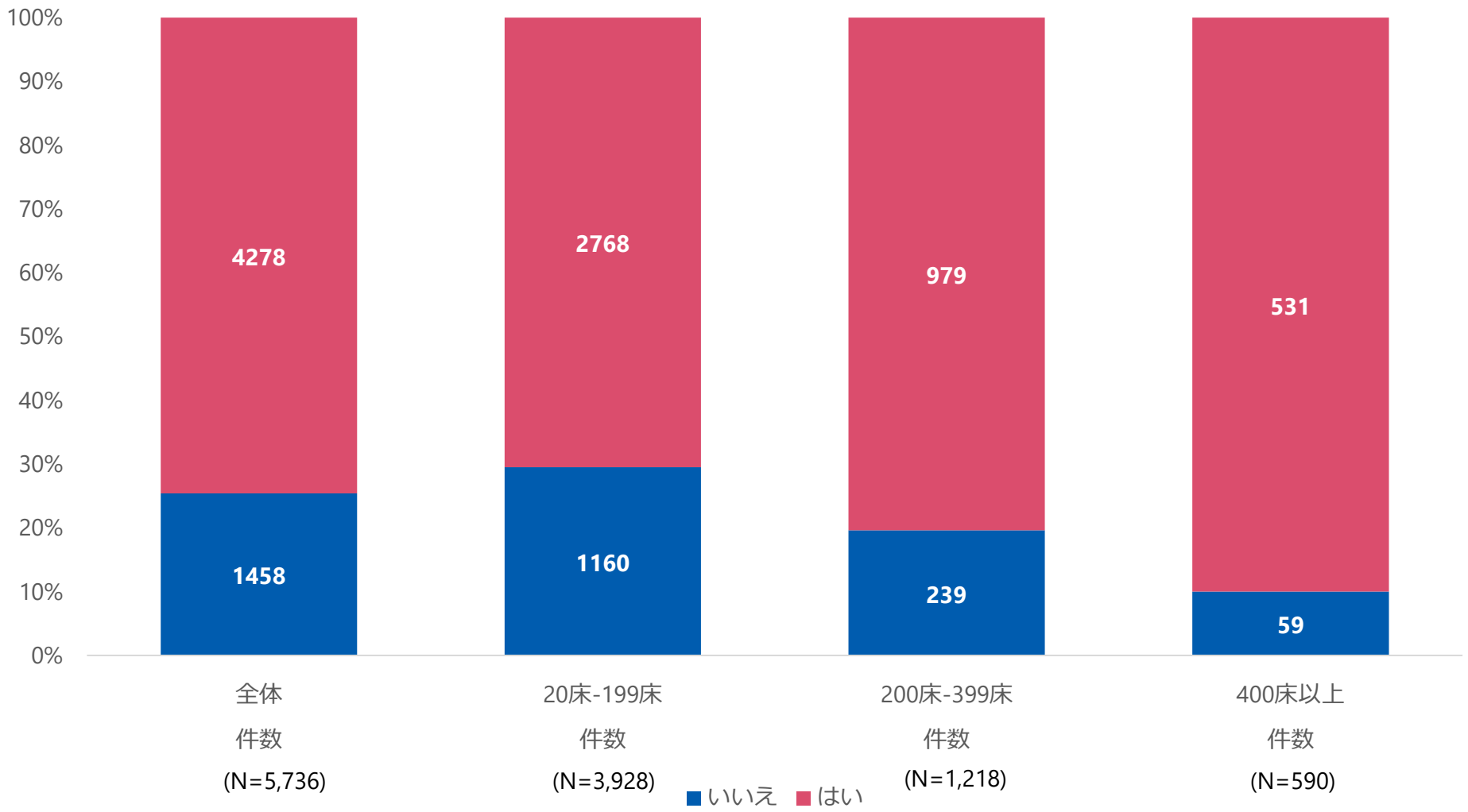
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

職員を対象とした情報セキュリティ研修の実施



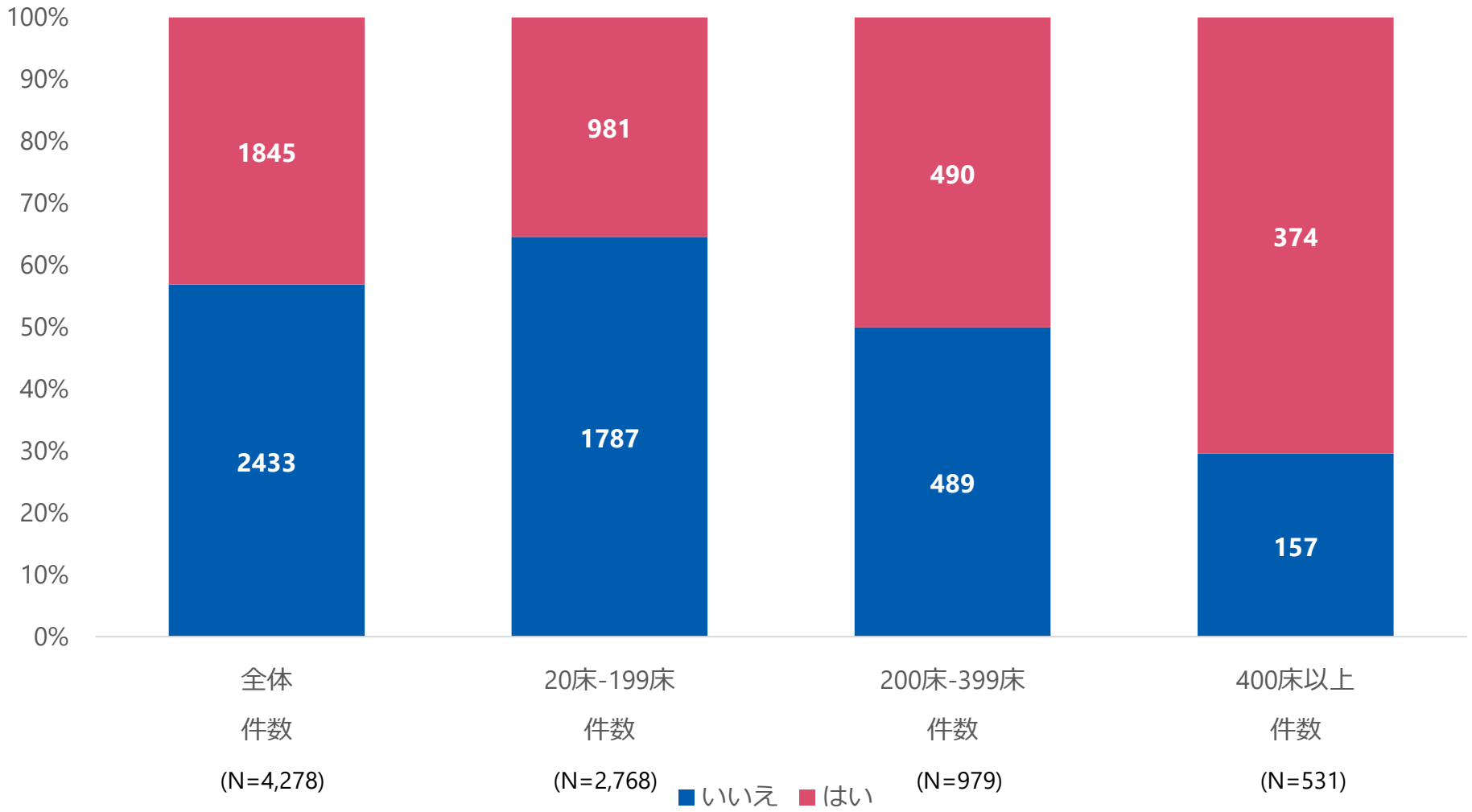
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

サイバー攻撃を想定したBCPの策定



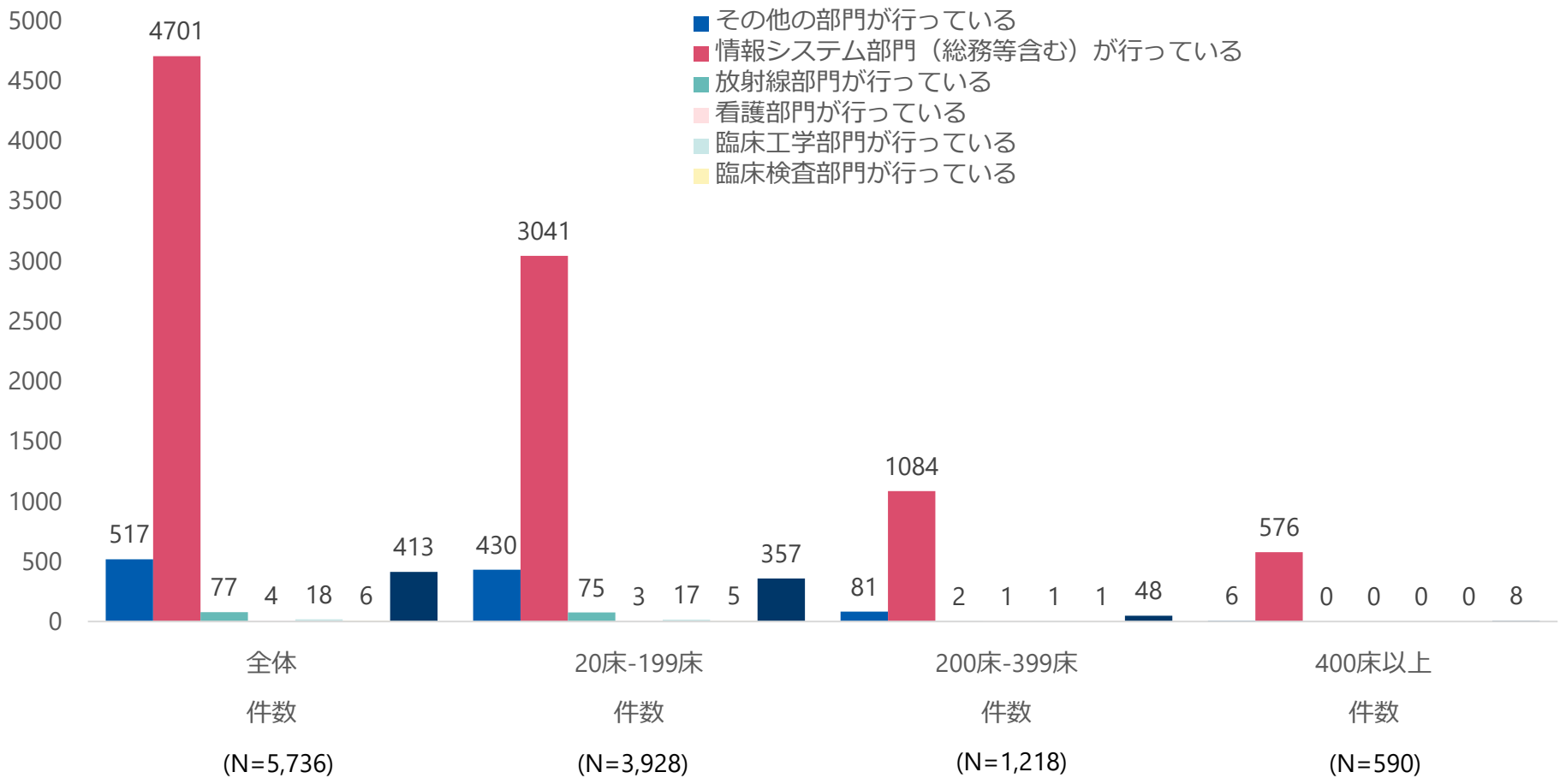
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

BCPの訓練の実施



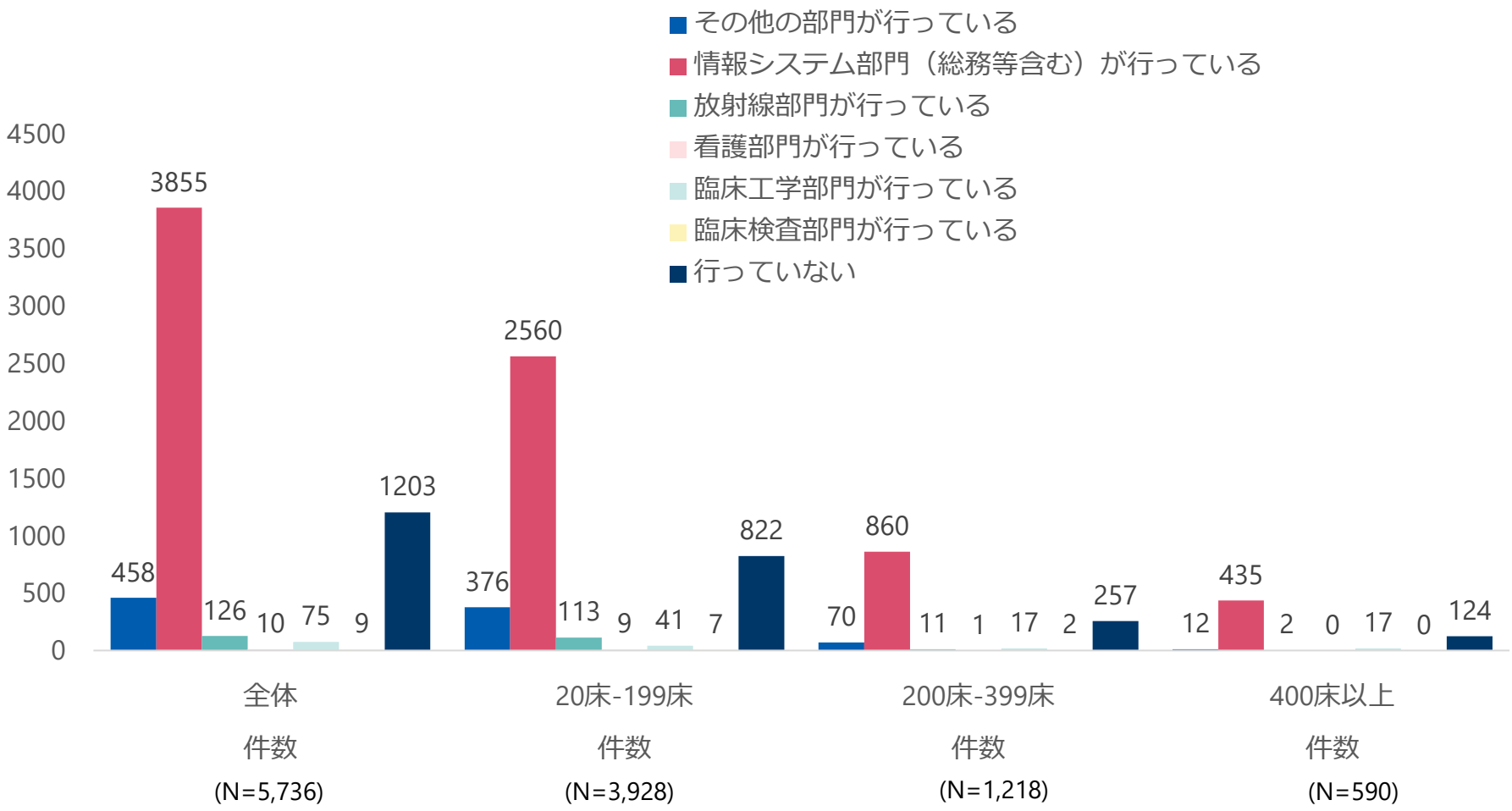
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

サーバ、端末PC、ネットワーク機器の台帳管理を実施している（医療機器を除く）



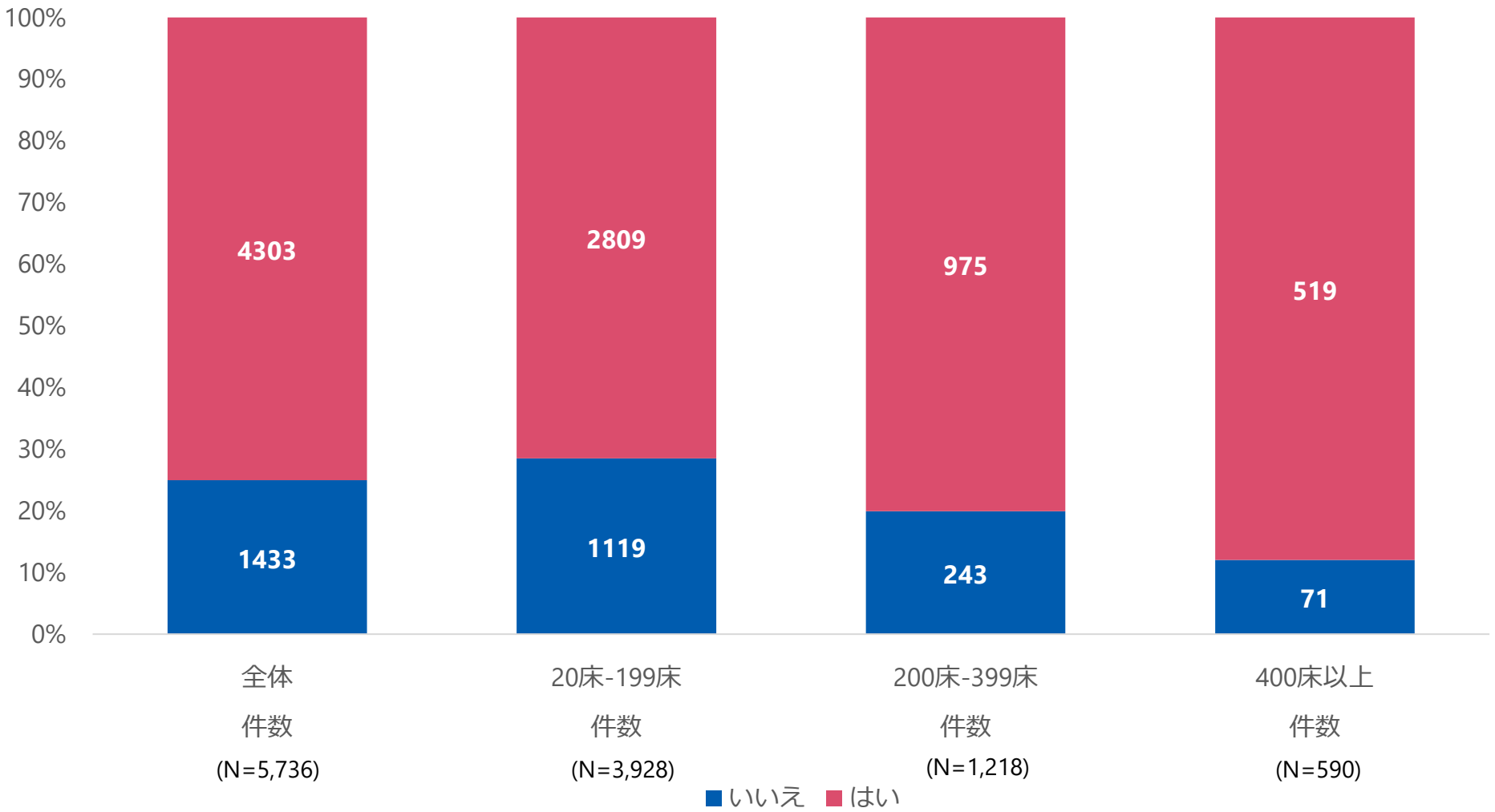
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

ネットワークに接続する医療機器の一元的な台帳管理を実施している



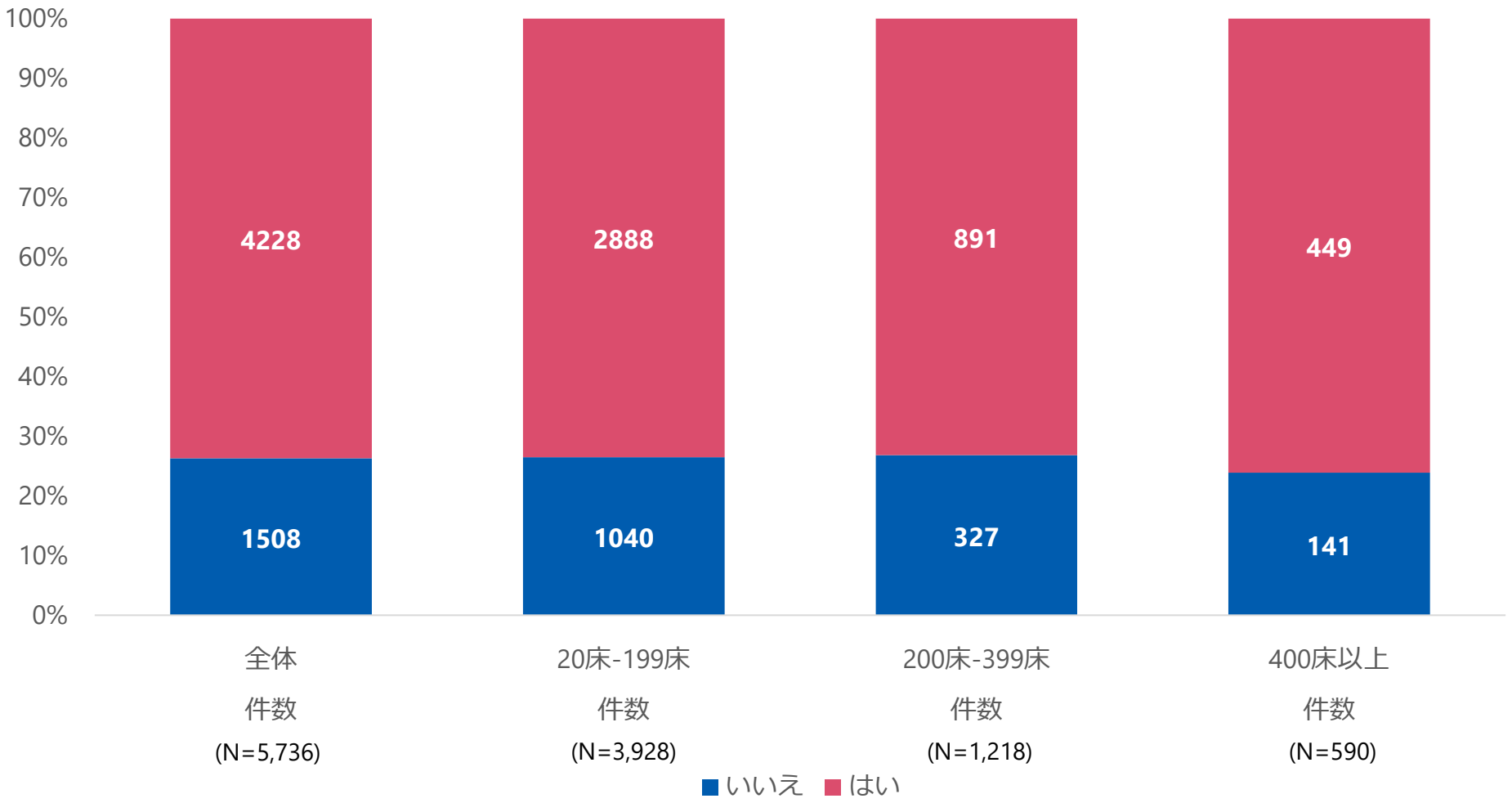
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

ネットワーク構成図を定期的に更新し、各部門の外部接続点数を把握している



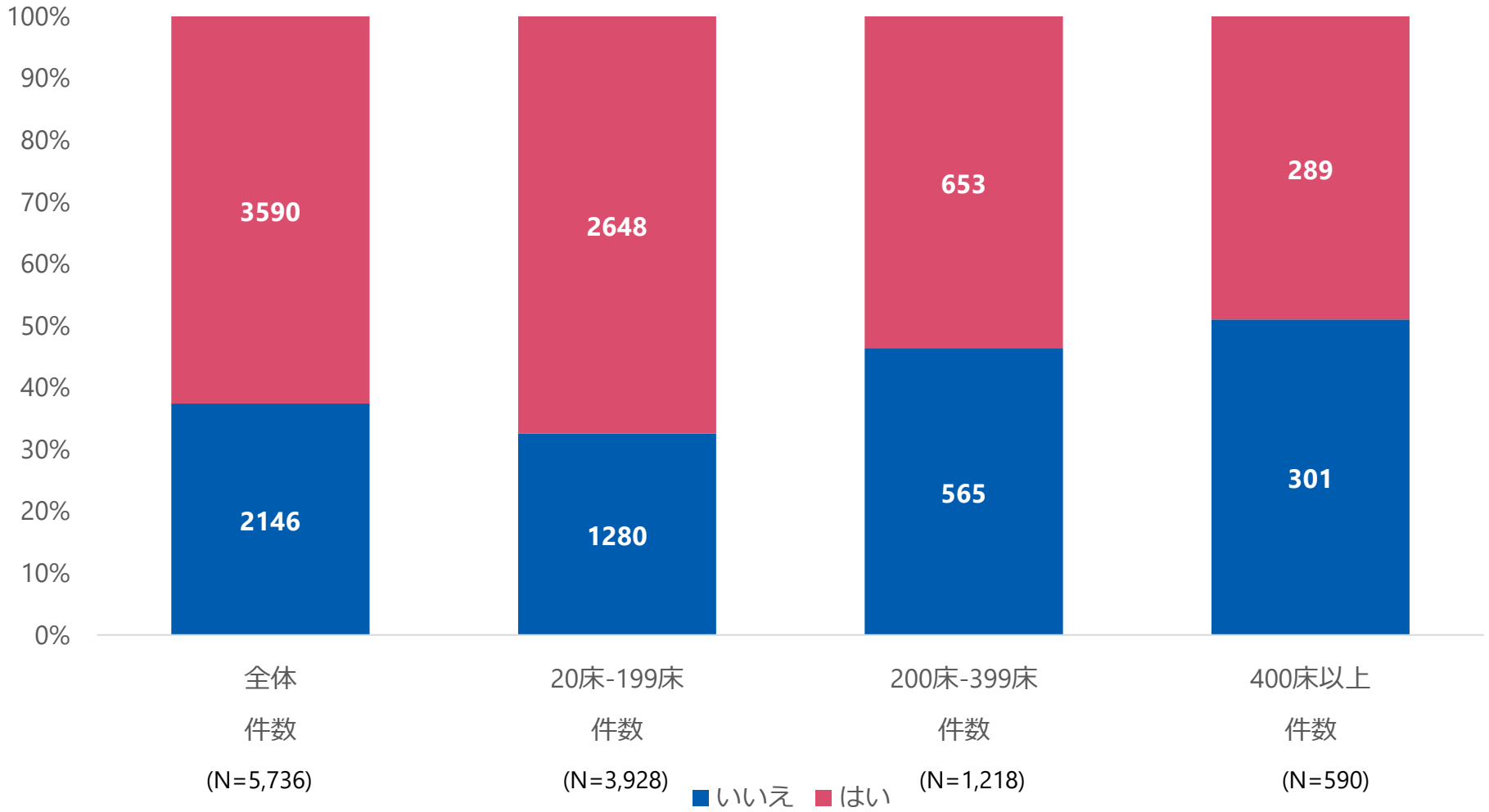
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

ネットワーク機器に対して定期的にセキュリティパッチを適用している



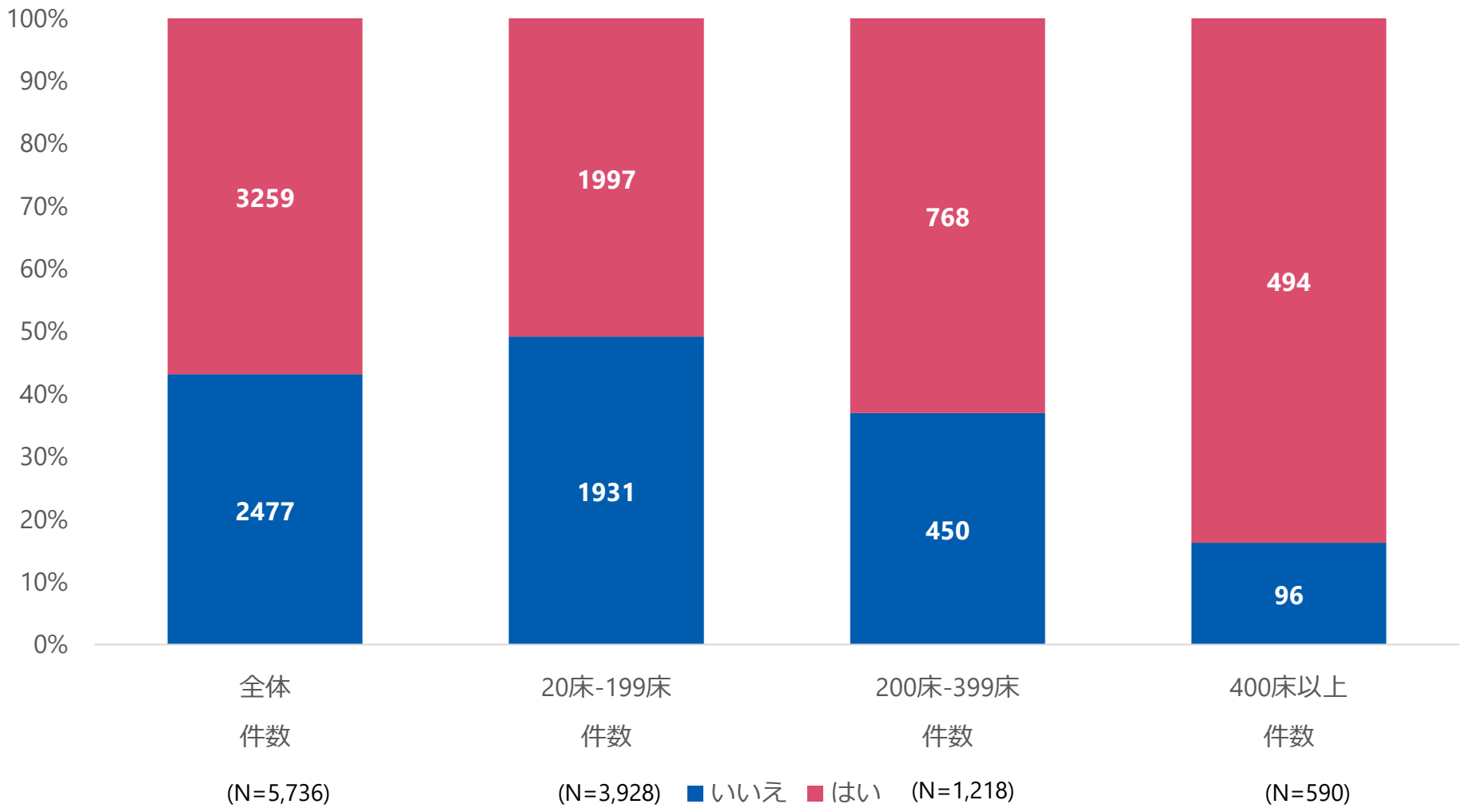
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

サーバ、端末PCに対して定期的にセキュリティパッチを適用している



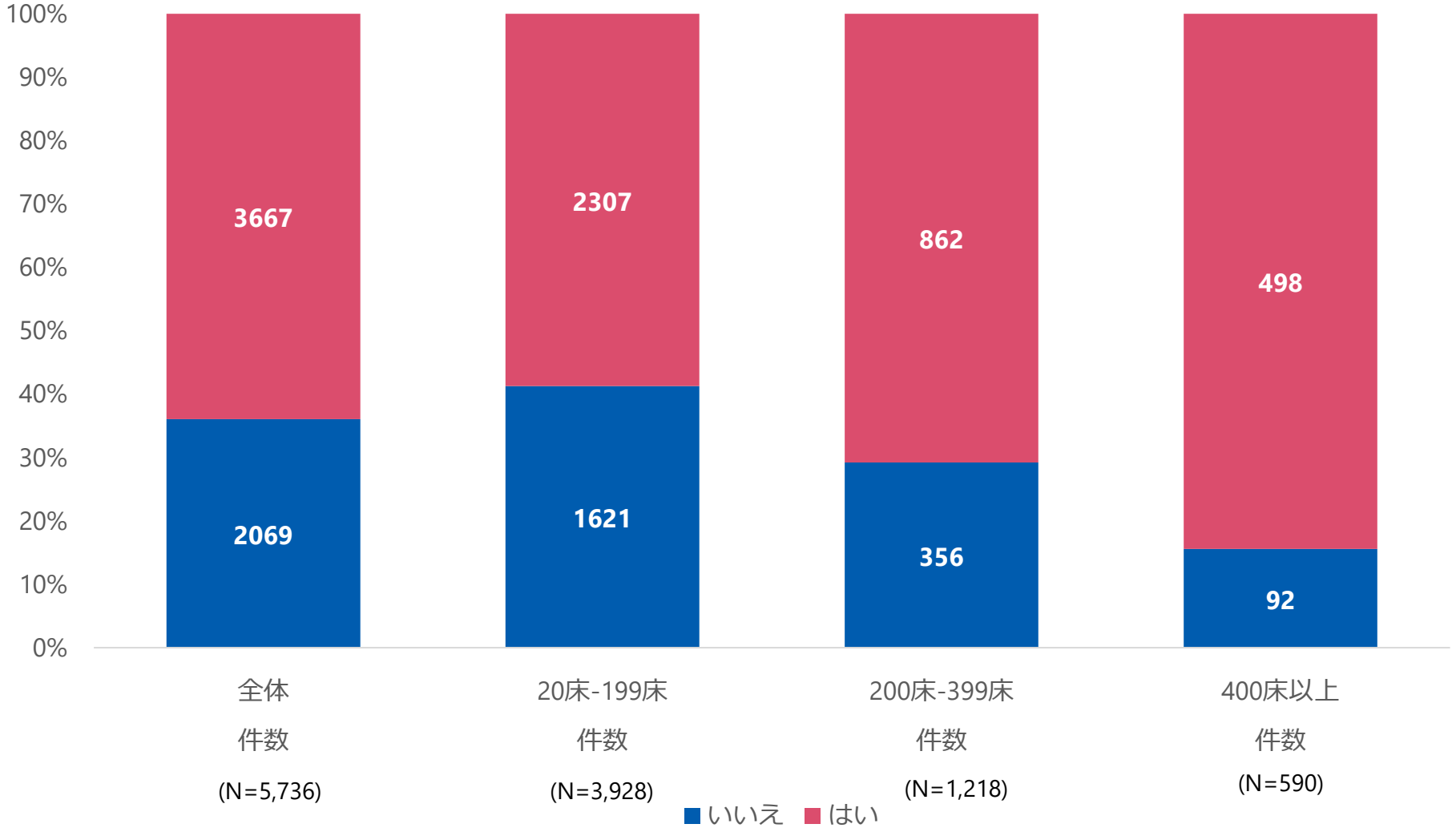
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

パフォーマンス管理と死活監視を行っている



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（概要）

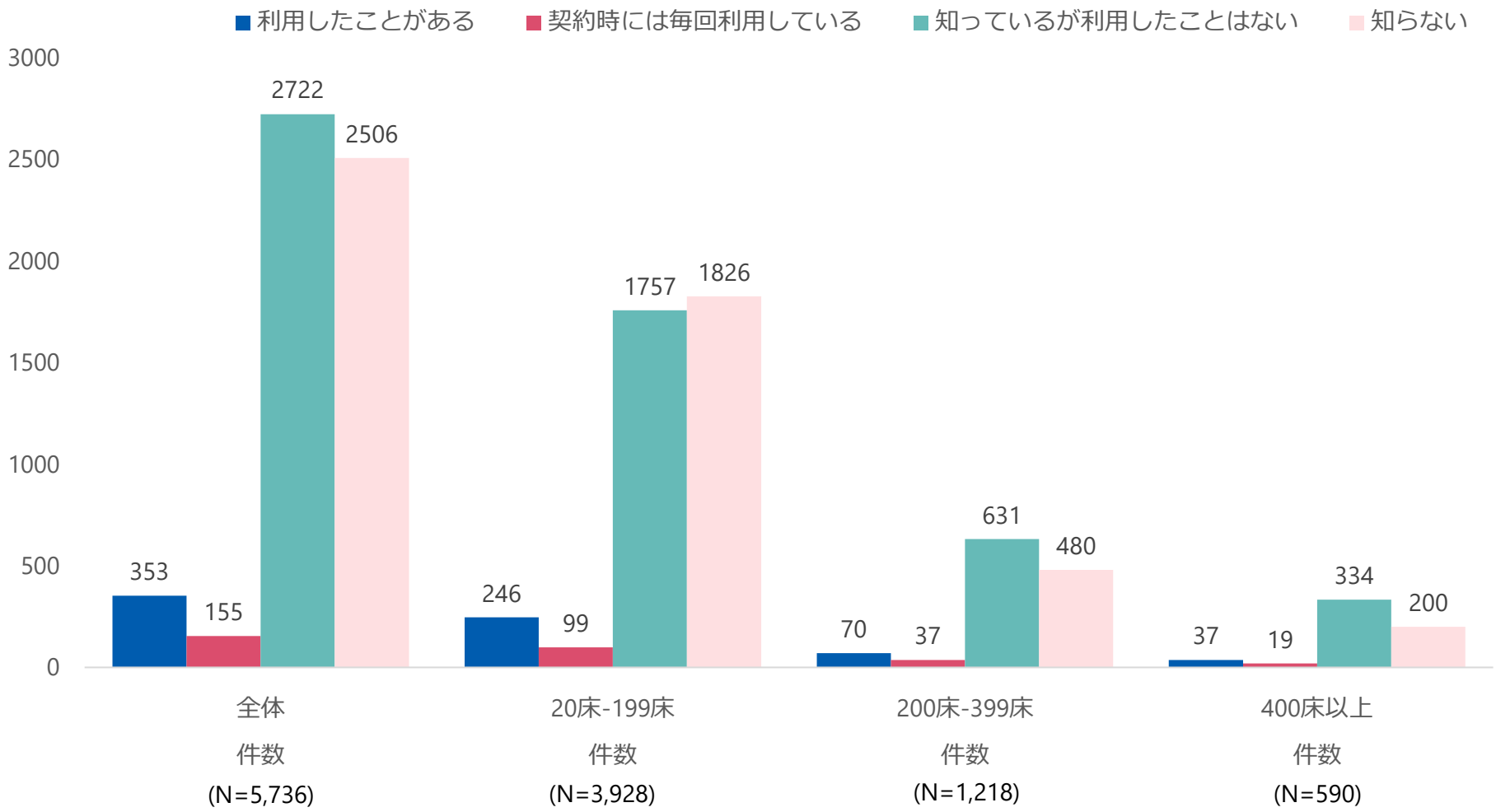
MDS/SDS※を用いて点検している



※：MDS/SDS（Manufacturer / Service Provider Disclosure Statment for Medical Information Security）自組織の情報機器・システムが「医療情報の安全管理に関するガイドライン」への準拠しているかを確認するための医療情報セキュリティ開示書

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（概要）

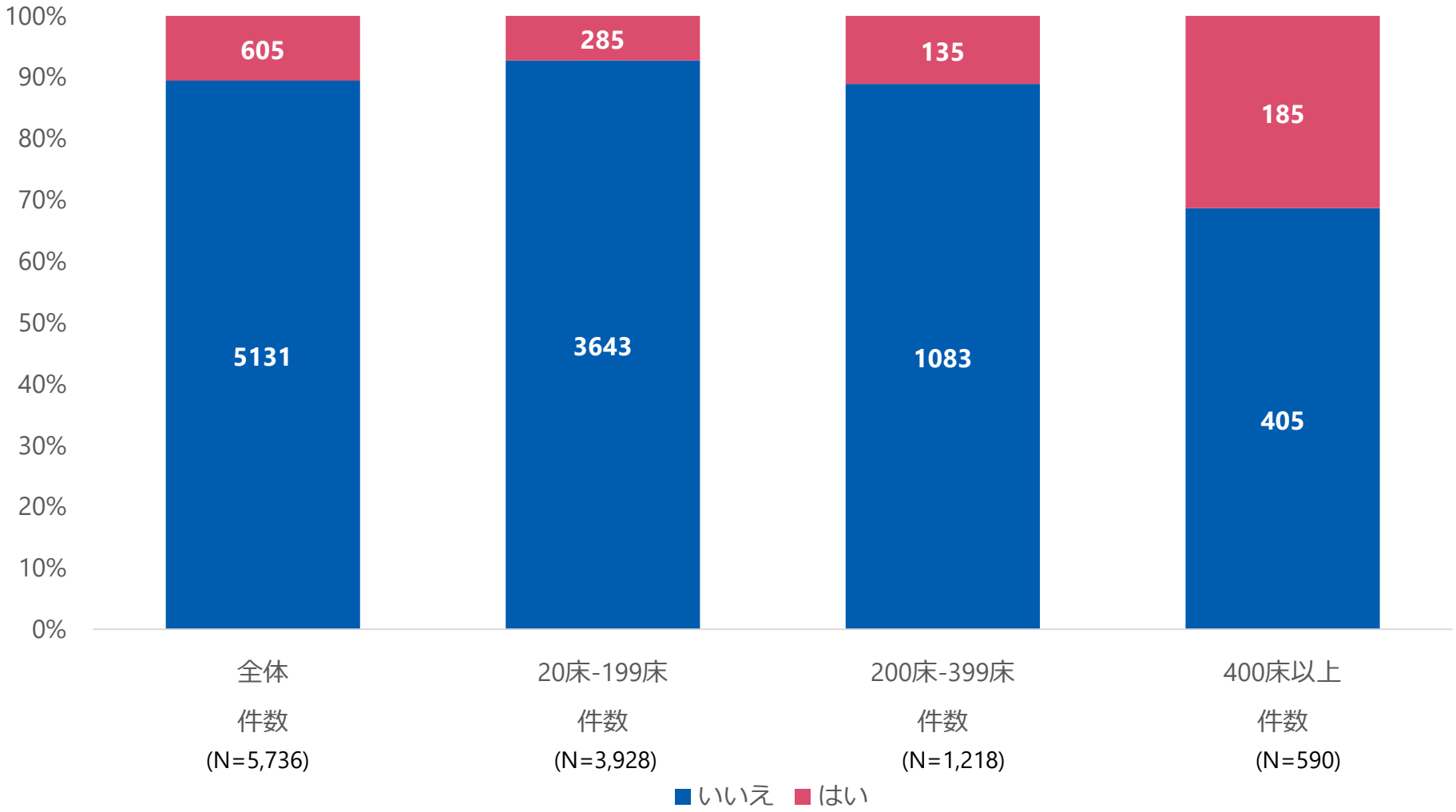
契約における役割分担確認表※を知っている、または利用している



※：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：総務省・厚生労働省・経済産業省においてとりまとめた、医療情報システムの契約時に医療機関と事業者の責任・役割分担をすりあわせ、契約書やサービスレベル合意書に落とし込むための確認表。

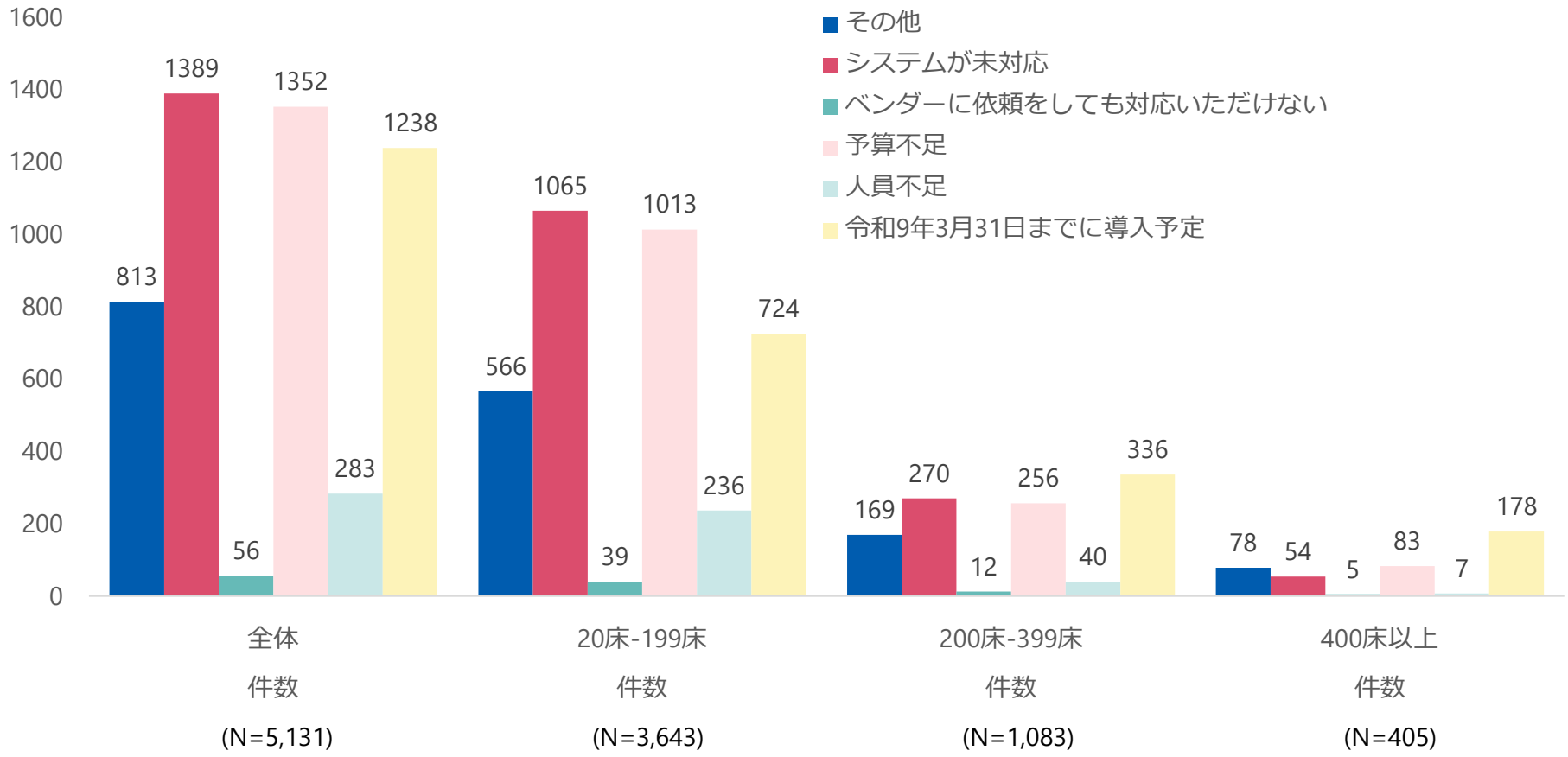
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

二要素認証を導入している



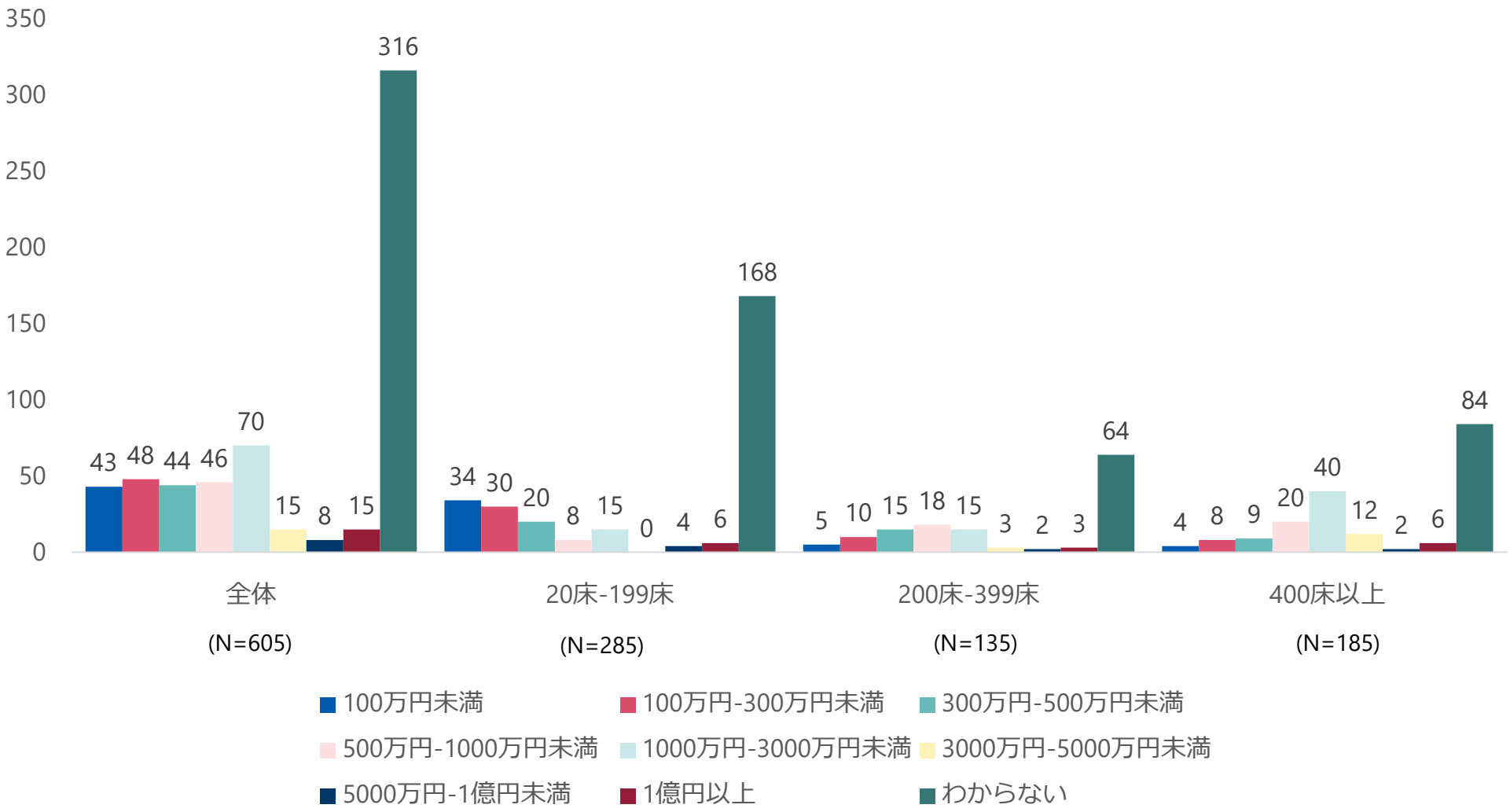
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

二要素認証の導入ができない理由



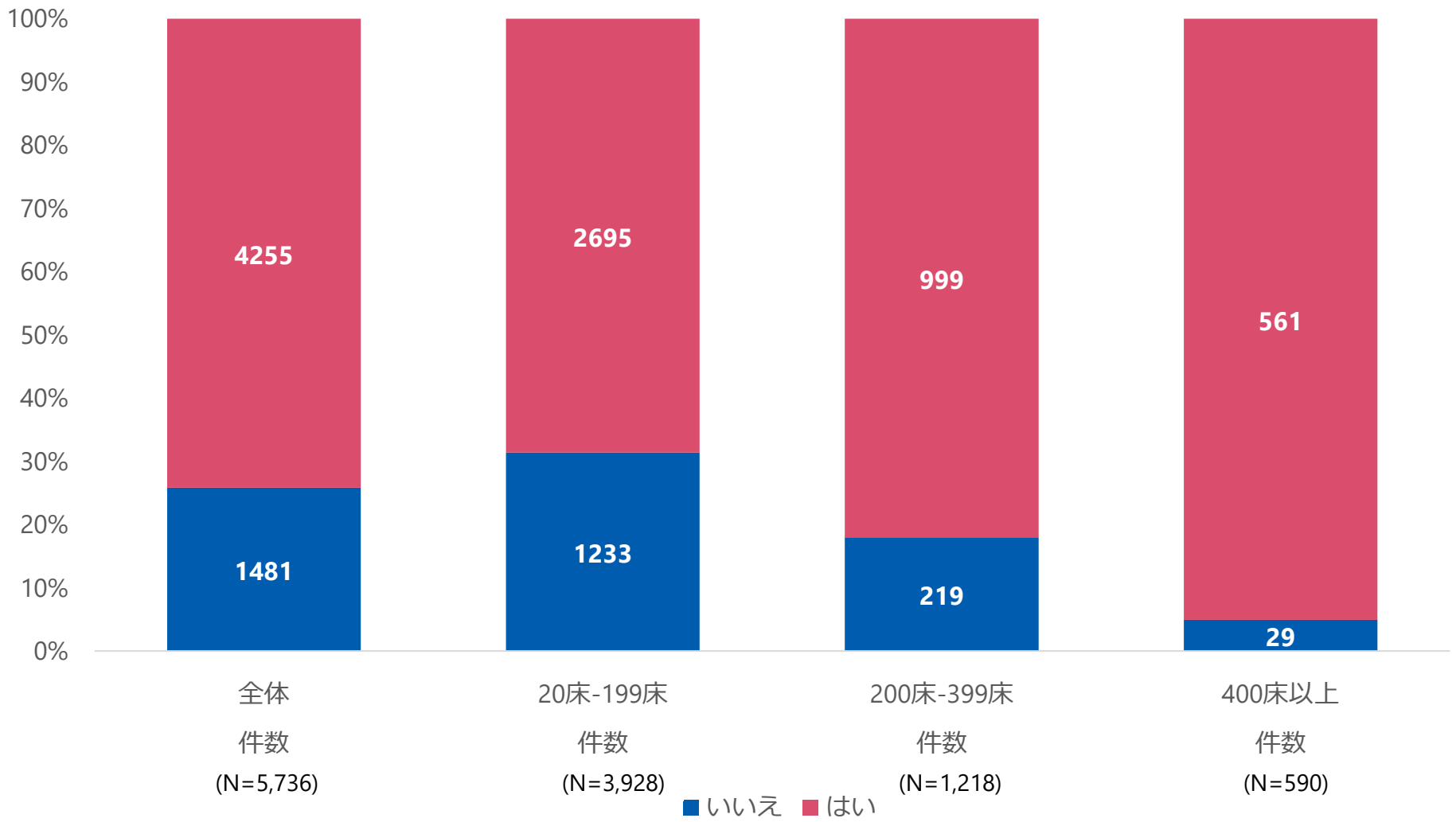
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

二要素認証導入に要した費用



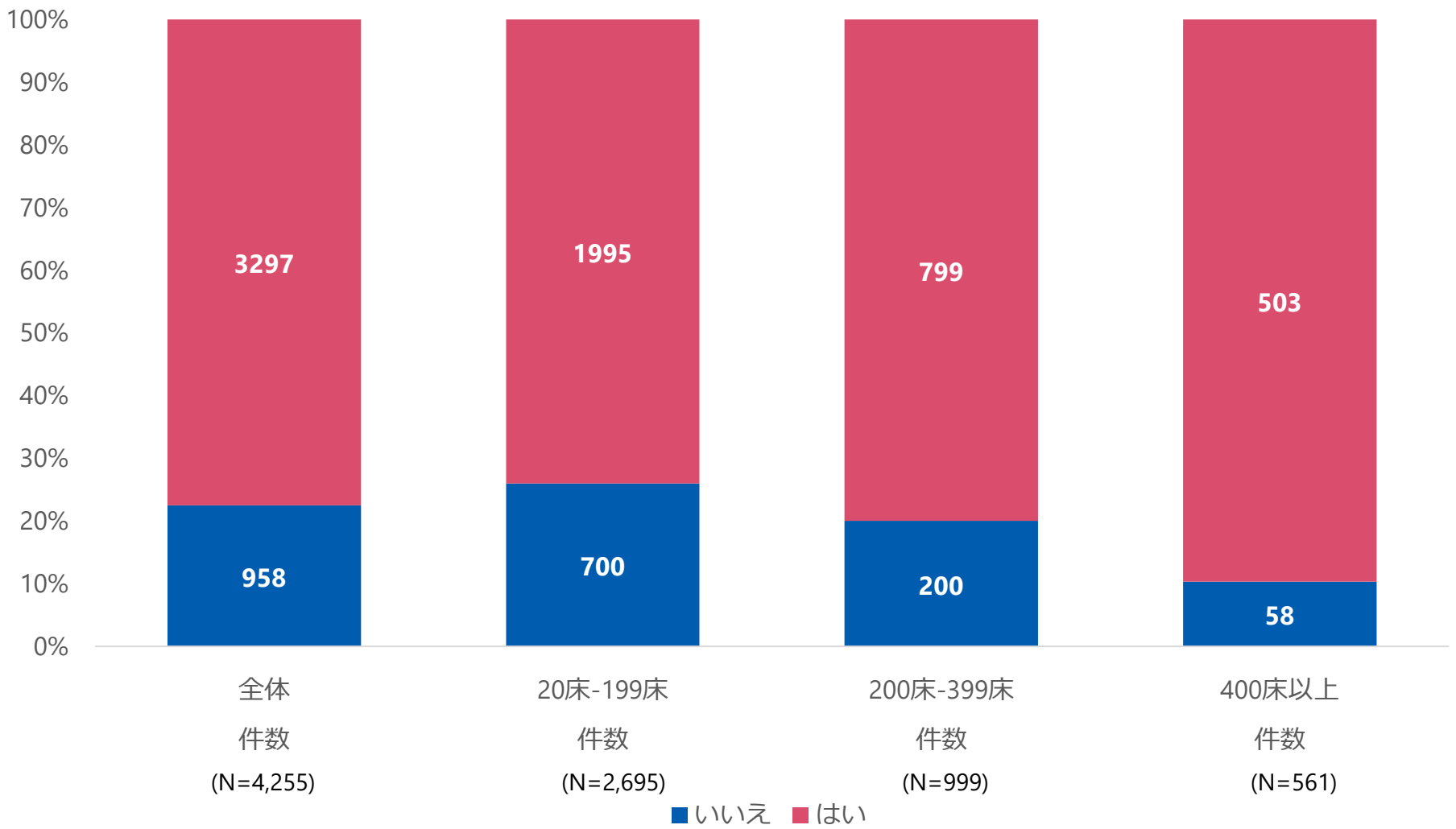
病院における医療情報システムのサイバーセキュリティ対策に係る調査（概要）

電子カルテを導入している



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（概要）

オフラインバックアップを確保している



参考

電子的診療情報連携体制整備加算の新設③

電子的診療情報連携体制整備加算の新設③

➢ 医療DX関連施策の進捗状況を踏まえ、普及した関連サービスの活用を基本としつつ、更なる関連サービスの活用による質の高い医療の提供を評価する観点から、診療録管理体制加算の評価を見直し、電子的診療情報連携体制整備加算を新設する。

現行	改定後
【診療録管理体制加算１】　140点 【診療録管理体制加算２】　100点 ・区分の見直し（診療録管理体制加算２→１） ・許可病床数200床以上の保険医療機関については、専任の医療情報システム安全管理責任者を配置すること。 【診療録管理体制加算３】　30点 ・区分の見直し（診療録管理体制加算３→２）	（削除） 【診療録管理体制加算**１**】　100点 （削除） 【診療録管理体制加算**２**】　30点

入院基本料等加算

（新）	**電子的診療情報連携体制整備加算１**	**160点（入院初日）**
（新）	**電子的診療情報連携体制整備加算２**	**80点（入院初日）**

［施設基準（電子的診療情報連携体制整備加算１）］

（１）　オンライン請求を行っていること。　（２）　明細書を患者に無償で交付していること。
（３）　オンライン資格確認を行う体制を有していること。　（５）　マイナ保険証利用率が、30%以上であること。
（４）　オンライン資格確認等システムを利用して取得した診療情報を、診療を行う診察室等において、閲覧又は活用できる体制を有していること。
（６）　マイナポータルの医療情報等に基づき、患者からの健康管理に係る相談に応じる体制を有していること。
（７）　明細書発行に関する事項、医療DX推進の体制に関する事項等について、当該保険医療機関及びウェブサイトに掲載していること。
（８）　厚生労働省「安全管理ガイドライン」に準拠した体制であること。
（９）　**「安全管理ガイドライン」に基づき、専任の医療情報システム安全管理責任者を配置すること**。また、当該責任者は、職員を対象として、少なくとも年１回程度、定期的に必要な情報セキュリティに関する研修を行っていること。
(10)　専任の医療情報システム安全管理責任者は、情報セキュリティマネジメントや情報処理安全確保支援士の資格を有していることが望ましい。
(11)　非常時に備えた医療情報システムの**バックアップを複数の方式で確保**し、その一部はネットワークから切り離した**オフラインで保管**していること。
(12)　非常時を想定した医療情報システムの利用が困難な場合の対応や復旧に至るまでの対応についての**業務継続計画（ＢＣＰ）を策定**し、少なくとも**年１回程度、定期的に訓練・演習を実施**すること。また、その結果を踏まえ、必要に応じて改善に向けた対応を行っていること。