資料７－３

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

厚生労働省におけるサイバーセキュリティに関する取り組み

Ministry of Health, Labour and Welfare of Japan

医療・水道分野におけるサイバーセキュリティに関する取り組み

課題

近年、重要インフラ事業者のICT化が進むにつれ、サイバー攻撃等のリスクは高まっており、サイバーセキュリティへの取組の必要性が増大している。また、特に医療分野においては、ランサムウェア等の「外部からの攻撃」が年々増加しており、事業者のみでの対策には限界がきている。

医療分野

これまでの対応

- 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実施
- 上記調査を踏まえ、令和5年5月頃に医療情報システムの安全管理に関するガイドラインを改定
- 医療法施行規則第14条第２項を新設し、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じることを追加する。（令和５年４月1日施行）

水道分野

これまでの対応

- 水道分野における情報セキュリティガイドライン（第４版）を平成31年３月に策定
- 水道施設の技術的基準を定める省令を一部改正し、水道施設の施設基準において、サイバーセキュリティ対策を確保するために必要な措置を講じる旨を規定

今後の対応

- 「重要インフラのサイバーセキュリティ対策に係る行動計画」の内容を踏まえ、必要に応じて各種ガイドライン等の改訂を検討する。

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）

第16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（令和５年３月23日）資料２-1

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な有効な対策の実施を促すことが必要。
・　病院が保有する医療情報システムのサイバーセキュリティ対策について実態調査を実施。具体的に令和４年10月に発生した大阪急性期・総合医療センターにおけるサイバー攻撃事案を受けて発出した令和４年11月10日付け事務連絡「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」及び令和４年12月16日付け事務連絡「FortiOSに関する脆弱性情報への対応について（注意喚起）」において周知した対策への取組状況について質問。
・　これを踏まえ、「医療情報システムの安全管理に関するガイドライン第6.0版」に反映を行うこととする。

調査方法・対象

- G-MIS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。（問数は17問）
- 調査対象は、G-MIS IDが付与されている、8,238の病院。
- 有効回答数：4,811施設（回答率：58,4%）

調査期間

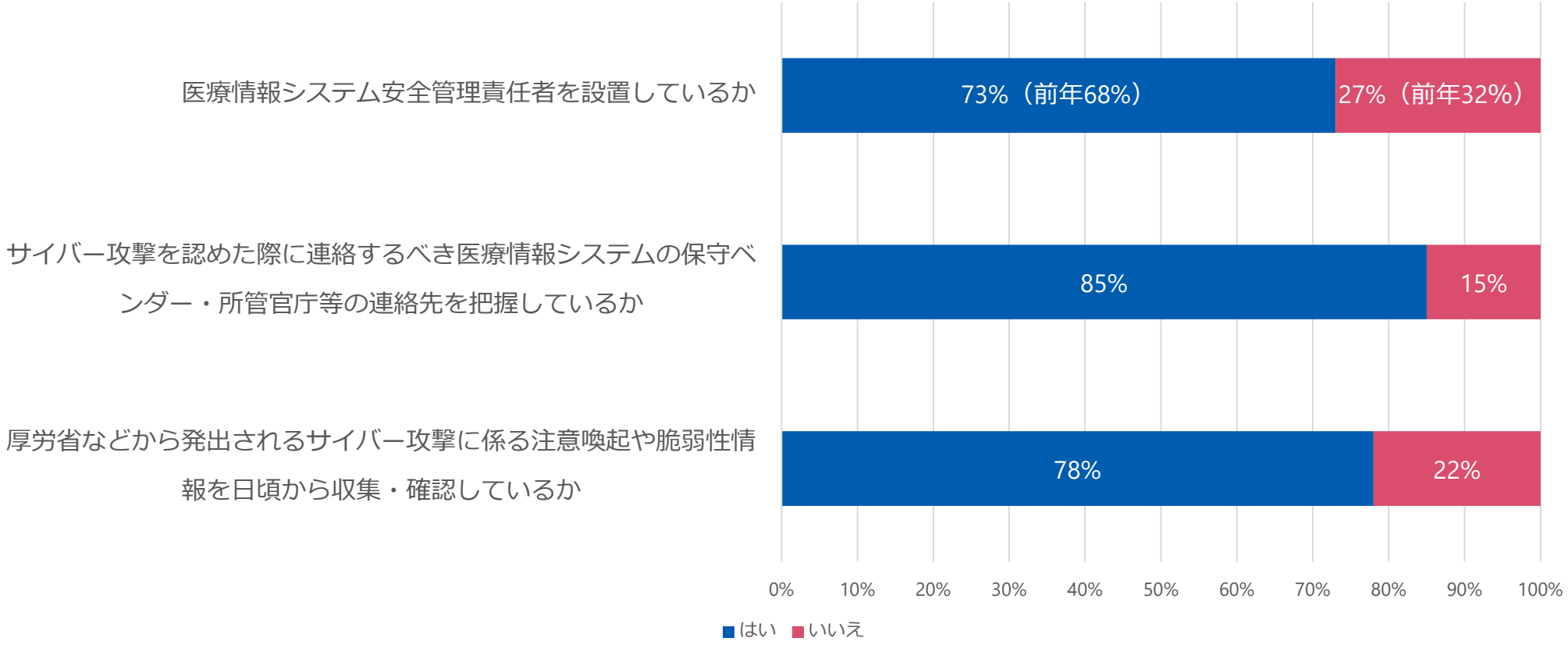
・令和５年１月27日（金）～　令和５年３月15日（水）

第16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（令和５年３月23日）資料２-1

調査結果について（体制構築と連絡体制について）

令和５年３月17日集計（速報値）

調査対象医療機関数：8,238施設　有効回答数：4,811施設（回答率：58,4%）

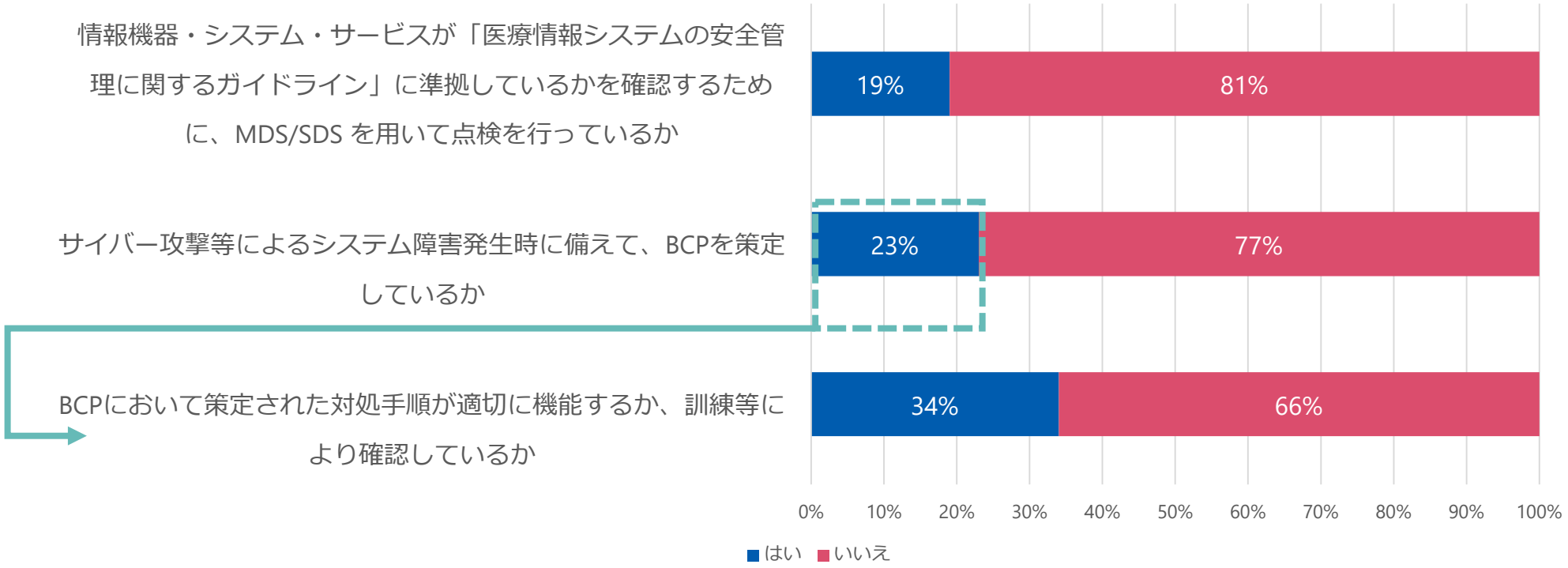


○医療情報システム安全管理責任者の設置、サイバー攻撃を認めた際に連絡すべき所管官庁等の連絡先の把握、サイバー攻撃に係る注意喚起や脆弱性情報の収集・確認は調査対象医療機関の内、70%以上で行っていた。

○医療情報システム安全管理責任者の設置に関しては、前年と同程度以上の設置率であった。

調査結果について（MDS/SDSを用いた点検・BCP策定等について）

令和５年３月17日集計（速報値）



※最後の質問については、2項目でBCPを策定している23%が母数となっている

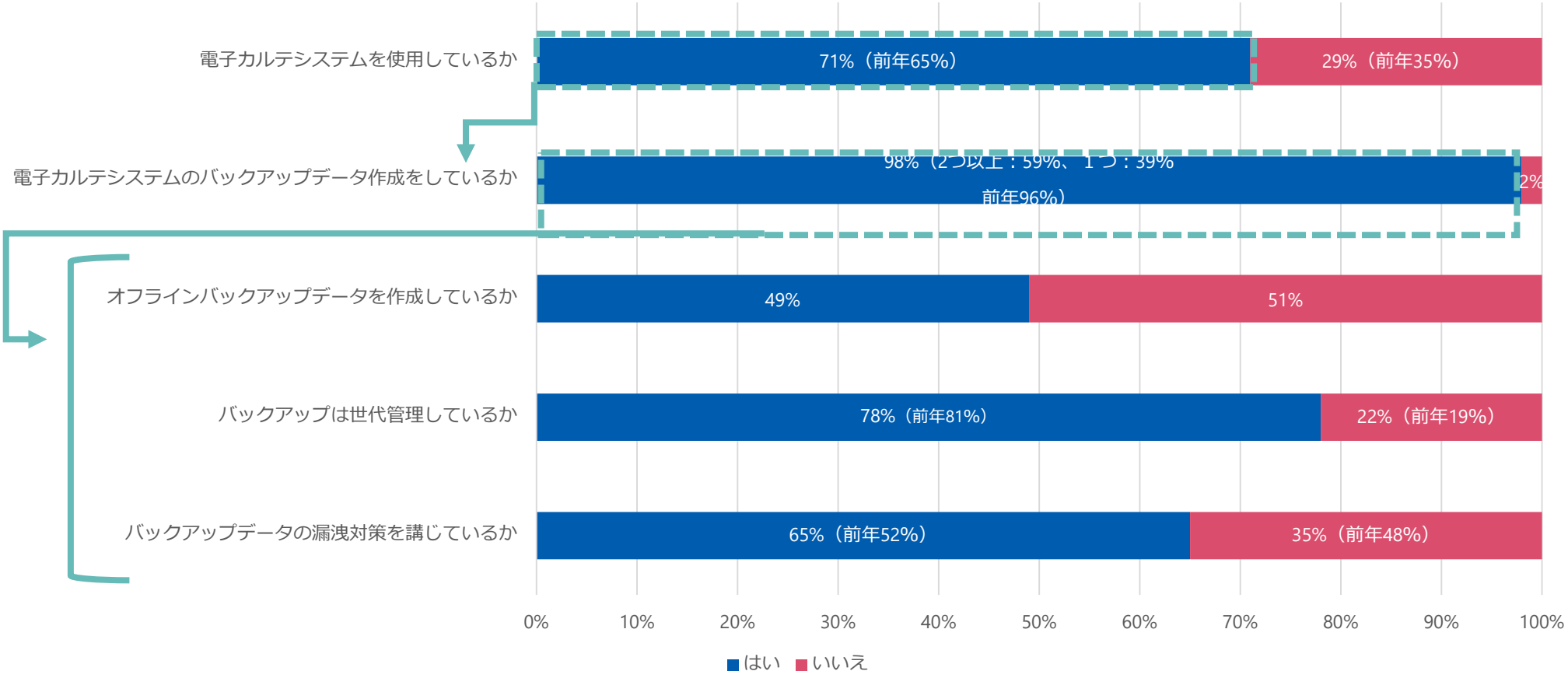
○MDS/SDSを用いて点検を行っている医療機関の割合は、調査対象医療機関の内、19%であった。

○サイバー攻撃等によるシステム障害発生時に備えて、BCPを策定している医療機関の割合は、調査対象医療機関の内、23%であった。その内、BCPを用いて訓練等により確認している医療機関の割合は、34%であった。

第16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（令和５年３月23日）資料２-1

調査結果について（電子カルテシステムのバックアップについて）

令和５年３月17日集計（速報値）



※3項目以降については、2項目でバックアップデータを作成している98%が母数となっている

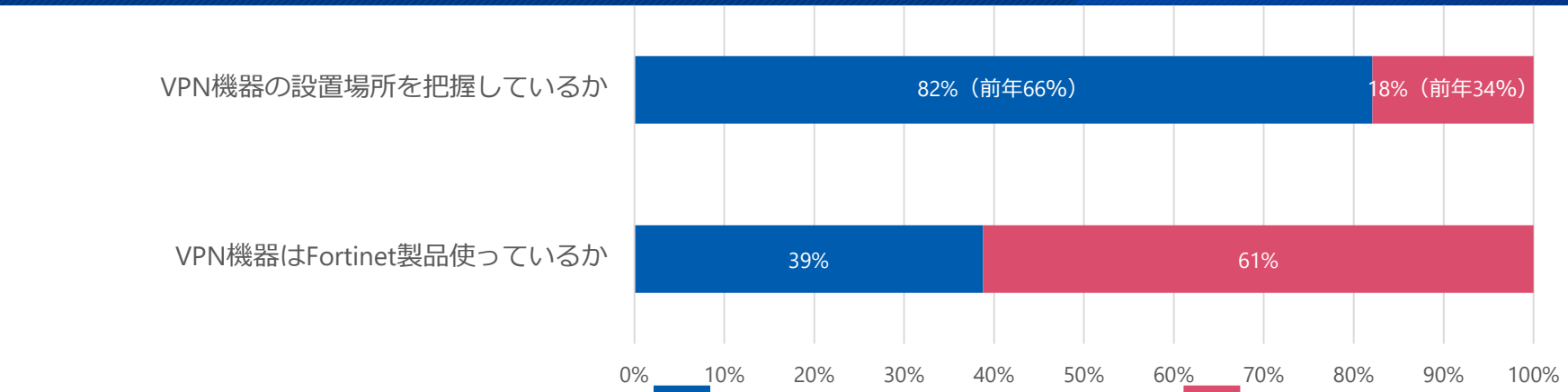
○調査対象医療機関の内、98%の医療機関で、電子カルテシステムのバックアップデータを作成しているが、その内、オフラインのバックアップデータの作成は49%であった。

○また、世代管理をしている医療機関の割合は78%であり、漏洩対策を講じている医療機関の割合は65%であった。

第16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（令和５年３月23日）資料２-1

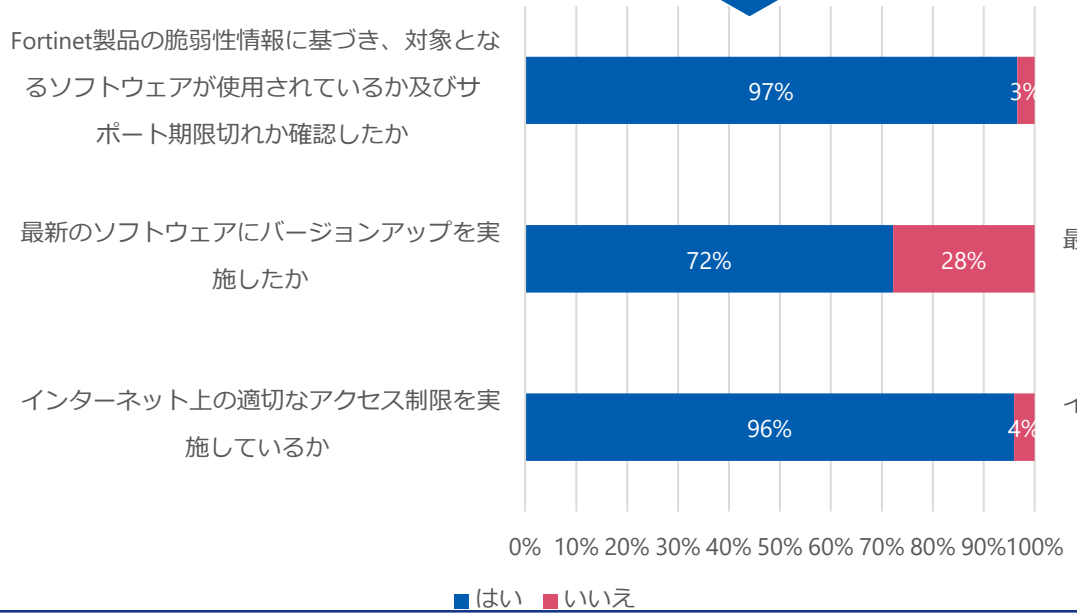
調査結果について（リモートゲートウェイ装置について）

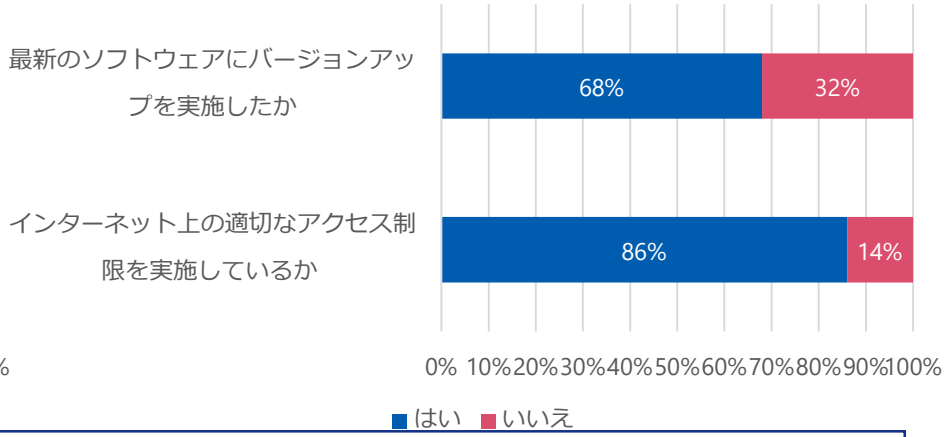
令和５年３月17日集計（速報値）



※以降の質問は39%が母数となっている

※以降の質問は61%が母数となっている



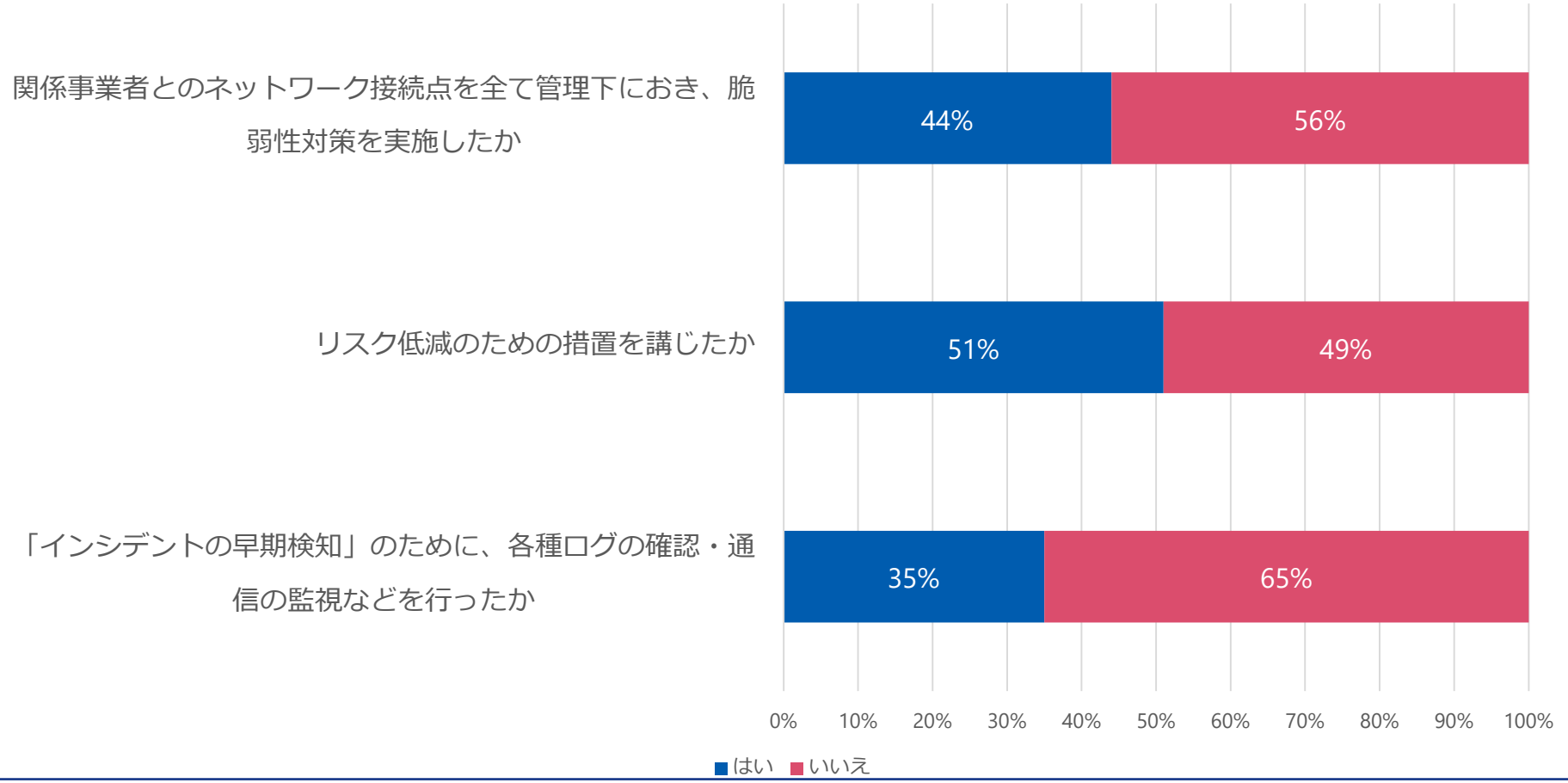


○VPN機器の設置場所把握をしている医療機関は、調査対象医療機関の内、82%であり、その内、Fortinet製品を使用している医療機関は39%であった。最新のソフトウェアにバージョンアップの実施と適切なアクセス制限をしている医療機関は各々、調査対象医療機関の内、Fortinet製品を使用している医療機関で72%、96%、使用していない医療機関で68%、86%であった。

調査結果について（令和４年11月10日「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」）

第16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（令和５年３月23日）資料２-1

令和５年３月17日集計（速報値）



○関係事業者とのネットワーク接続点を全て管理下におき、脆弱性対策を実施した医療機関の割合は、調査対象医療機関の内、44%であった。

○リスク低減のための措置を講じている医療機関の割合は、調査対象医療機関の内、51%であった。

○「インシデントの早期検知」のための、各種ログの確認・通信の監視などを行っている医療機関の割合は、調査対象医療機関の内、35%であった。

厚生労働省ホームページ

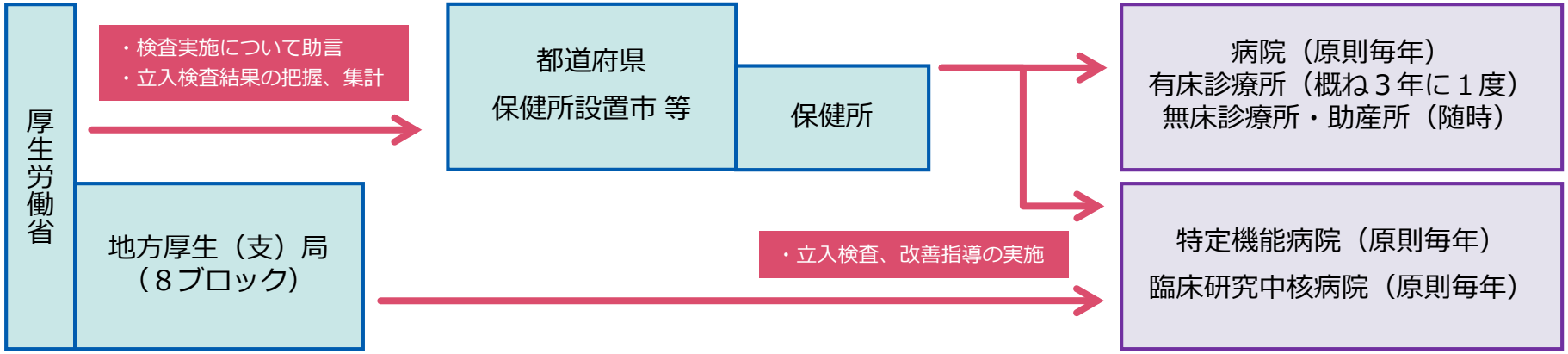
医療法に基づく立入検査の概要

立入検査の目的

・病院、診療所等が法令により規定された人員及び構造設備を有し、かつ、適正な管理を行っているか否かについて検査し、不適正な場合は指導等を通じ改善を図ることにより、病院、診療所等を良質で適正な医療を行う場にふさわしいものとする。

立入検査の実施主体

・**医療法第２５条第１項による立入検査** ・・・ 各病院、診療所等に対し、都道府県等が実施
・**医療法第２５条第３項による立入検査** ・・・ 特定機能病院等に対し、国が実施



主な検査項目

○**病院管理状況**
➢カルテ、処方箋等の管理、保存　➢届出、許可事項等法令の遵守　➢患者入院状況、新生児管理等　➢医薬品等の管理、職員の健康管理
➢安全管理の体制確保　等
○**人員配置の状況**
➢医師、看護婦等について標準数と現員との不足をチェック
○**構造設備、清潔の状況**
➢診察室、手術室、検査施設等　➢給水施設、給食施設等　➢院内感染対策、防災対策　➢廃棄物処理、放射線管理　等

医療機関の管理者が遵守するべき事項への位置づけ

第16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（令和５年３月23日）資料２-2

これまでの本ＷＧでの議論を踏まえ、下記の通り、医療機関の管理者が遵守するべき事項に位置づけた。

これまでのＷＧでの議論

○　医療機関のセキュリティ対策は、「医療情報システムの安全管理に関するガイドライン」に基づき、各医療機関が自主的に取組を進めてきたところ。昨今のサイバー攻撃の増加やサイバー攻撃により長期に診療が停止する事案が発生したことから実施した緊急的な病院への調査では、自主的な取組だけでは不十分と考えられる結果であった。平時の予防対応として、脆弱性が指摘されている機器の確実なアップデートの実施等が必要。（第11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（令和４年５月27日））

○　医療機関がサイバーセキュリティを確保するための具体的な対策を明示し、ペナルティを課すのではなく、支援・助言を行うための検査になるような進め方が望ましい（（第11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（令和４年５月27日））））

○　令和４年度中に医療機関等の管理者が遵守すべき事項に位置付けるための省令改正を行う。（第12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（令和４年９月５日））

改正概要・対応の方向性

○　医療法施行規則第14条第２項を新設し、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じることを追加する。

○　令和５年３月10日公布、４月１日施行（予定）

○　「必要な措置」としては、最新の「医療情報システムの安全管理に関するガイドライン」（以下「安全管理ガイドライン」という。）を参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行うこととする。

○　安全管理ガイドラインに記載されている内容のうち、優先的に取り組むべき事項については、厚生労働省においてチェックリストを作成し、各医療機関で確認できる仕組みとする。

○　また、医療法第25条第１項に規定に基づく立入検査要綱の項目に、サイバーセキュリティ確保のための取組状況を位置づける。

◎医療法施行規則（昭和二十三年厚生省令第五十号）

第十四条　（略）

２　病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保するために必要な措置を講じなければならない。

※　下線部を新設。

参考

（参照条文）

◎医療法（昭和23年法律第205号）（抄）

第25条　都道府県知事、保健所を設置する市の市長又は特別区の区長は、必要があると認めるときは、病院、診療助若しくは助産所の開設者若しくは管理者に対し、必要な報告を命じ、又は当該職員に、病院、診療助に立ち入り、その有する人員若しくは清潔保持の状況、構造設備若しくは診療録、助産録、帳簿書類その他の物件を検査させることができる。

２（略）

３　厚生労働大臣は、必要があると認めるときは、特定機能病院等の開設者若しくは管理者に対し、必要な報告を命じ、又は当該職員に、特定機能病院等に立ち入り、その有する人員若しくは清潔保持の状況、構造設備若しくは診療録、助産録、帳簿書類その他の物件を検査させることができる。

４～５（略）

今後のスケジュール（予定）

令和５年4月1日　改正省令施行

5月末頃　「医療法第25条第１項の規定に基づく立入検査要綱の一部改正について」及び「令和５年度の医療法第 25 条第１項の規定に基づく立入検査の実施について」（通知）発出

6月頃　立入検査開始

サイバーセキュリティの確認のためのチェックリスト

第16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（令和５年３月23日）資料２-3

【医療機関において確認する項目】

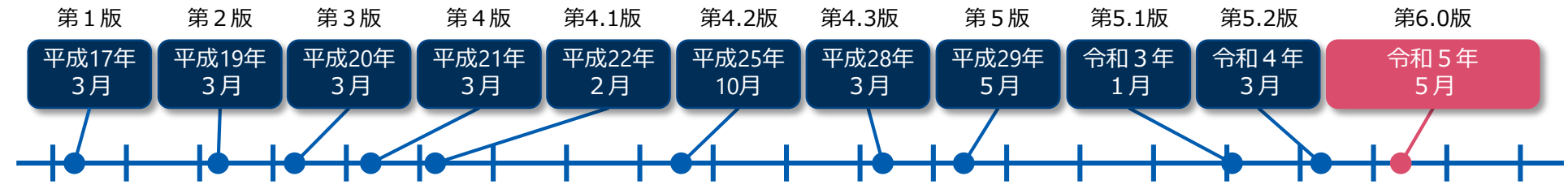
大項目	項番	チェック項目
1 体制構築	１－１	医療機関に医療情報システム安全管理責任者を配置している。
2 情報システムの管理	２－１	医療機関において、以下について把握している。
		① 医療機関で用いる端末の一覧
		② 医療機関で用いるネットワーク機器の一覧
		③ 医療機関で用いる記録媒体の一覧
		④ 医療機関で用いるサーバーの一覧
	２－２	職員の私物や事業者所有の機器等について、診療に関する業務で使用する場合の許可や管理体制が明確になっている。
	２－３	医療機関は、既に報告されている脆弱性について、事業者から最新の安全性に関する確認結果の報告を受けている。
3 情報システムの運用	３－１	退職者のアカウント等、不要なアカウントを削除する管理体制ができている。
	３－２	利用者の職種・担当業務別の情報区分ごとのアクセス管理機能がある。
	３－３	ネットワーク機器（※）にセキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。 （※）VPN機器を含むインターネットとの接続を制御するルータ。
	３－４	サーバーでアクセス記録（アクセスログ）の管理をしている。
	３－５	ネットワーク機器にアクセス制限を実施している。
4 インシデント発生時の対応	４－１	サイバー攻撃を受ける等システムに重大な障害が発生したことを想定した事業継続計画（BCP）を策定済み、又は、令和５年度中に策定予定である。
	４－２	インシデント発生時に備えて、組織内連絡体制と外部関係機関（事業者、厚生労働省及び警察等）への連絡体制を整えている。
	４－３	医療機関において、診療継続のために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。

【事業者において確認する項目】

大項目	項番	チェック項目
1 体制構築	１－１	事業者内に、医療情報システムの管理責任者がいる。
2 情報システムの管理	２－１	事業者は、提供するソフトウェア・機器等の脆弱性に関して、医療機関への導入時、以降適時、求められる安全性に関する状況（初期PWの変更、脆弱性の更新状況）を確認し、医療機関にその結果を報告し、対応している。
3 情報システムの運用	３－１	ネットワーク機器（※）にセキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。 （※）VPN機器を含むインターネットとの接続を制御するルータ。
	３－２	サーバーでアクセス記録（アクセスログ）の管理をしている。
	３－３	ネットワーク機器にアクセス制限を実施している。
4 インシデント発生時の対応	４－１	事業者は、インシデント発生時、事前に明確化している責任分界点に応じて対応できる体制を整えている。
	４－２	事業者は、バックアップについての保管及び取り扱いについて、医療機関に取り扱い説明書等の文書として提供している。

医療情報システムの安全管理に関するガイドライン 策定の背景及び改定の経緯

- 医療情報システムの安全管理に関するガイドラインは、e-文書法、個人情報保護等への対応を行うための情報セキュリティ管理のガイドラインとして、平成17年3月に第１版を策定。
- 以降、各種制度の動向や情報システム技術の進展等に対応して改定。今般、**令和５年５月に第6.0版を策定。**



版	第１版、第２版、第３版	第４版（第4.1版、第4.2版、第4.3版）	第５版（第5.1版、第5.2版）	第6.0版
策定・改定概要	**第１版** • 医療情報システムのセキュリティ管理を目的とて策定 **第２版** • 重要インフラとしての医療情報システムという観点からの対応 **第３版** • 個人情報施策の議論およびモバイル端末普及への対応	**第4版** • 個人情報保護施策の議論およびモバイル端末普及への対応 **第4.1版** • 民間事業者のデータセンターにおける外部保存に関する対応 **第4.2版** • 調剤済み処方せん及び調剤録等の外部保存への対応 **第4.3版** • 「電子処方せんの運用ガイドライン」への対応	**第5版** • 医療機関等の範囲の明確化 • 改正個人情報保護法対応 • サイバー攻撃の動向への対応 **第5.1版** • クラウドサービスへの対応 • 認証・パスワードに関する対応 • サイバー攻撃等による対応 • 外部保存受託事業者の選定基準対応 **第5.2版** • ２省（総務省、経産省）GL等との整合性 • 改正個人情報保護法への対応 等 • 医療機関へのサイバー攻撃の多様化・巧妙化 • 「規制改革実施計画」等への対応 • 電子署名 • 外部ネットワーク 等	**第6.0版** 全体構成の見直し • 概説編、経営管理編、企画管理編、システム運用編の４編に再構成 • Q&Aの充実 等 技術的な動向 • 外部委託、外部サービスの利用に関する整理 • 情報セキュリティに関する考え方の整理 • 新技術、制度・規格の変更への対応 等

第5.2版 から 第6.0版 への改定方針

2023年４月からの保険医療機関・薬局におけるオンライン資格確認導入の原則義務化により、概ねすべての医療機関等において、本ガイドラインに記載されているネットワーク関連のセキュリティ対策が必要となる。これを踏まえ、第6.0版への改定では、第5.2版で中長期的に検討を継続することとした論点を中心に、全体構成の見直しとともに検討した。

○ 外部委託、外部サービスの利用に関する整理

- クラウドサービスの特徴を踏まえたリスクや対策の考え方
- 医療機関等のシステム類型別に対応した責任等の整理　　等

○ 情報セキュリティに関する考え方の整理

- ネットワーク境界防御型思考／ゼロトラストネットワーク型思考
- 災害、サイバー攻撃、システム障害等の非常時に対する対応や対策　　等

○ 新技術、制度・規格の変更への対応

- 本人確認を要する場面での運用（eKYCの活用）
- オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置
- 新たなネットワーク技術（ローカル５G）の利用可能性、利用場面
- 医療情報の共有・提供に関連する法令等の規定や技術・規格の動向

○ 全体構成の見直し

- 概説編（Overview）、経営管理（Governance）編、企画管理（Management）編、システム運用（Control）編の４編構成（各編は数十ページ程度、第5.2版の文章等を全面的に精査）
  - ※ 第5.2版 6.12章（電子署名）は、策定時に詳細な検討・調整を行ったため、原則、現行版を踏襲
- 概要、Q&A、用語集、特集（小規模医療機関等向け、サイバーセキュリティ）等、支援文書の整備