資料２－１

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

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

2023（令和５）年３月23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

医政局特定医薬品開発支援・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）

## 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%）

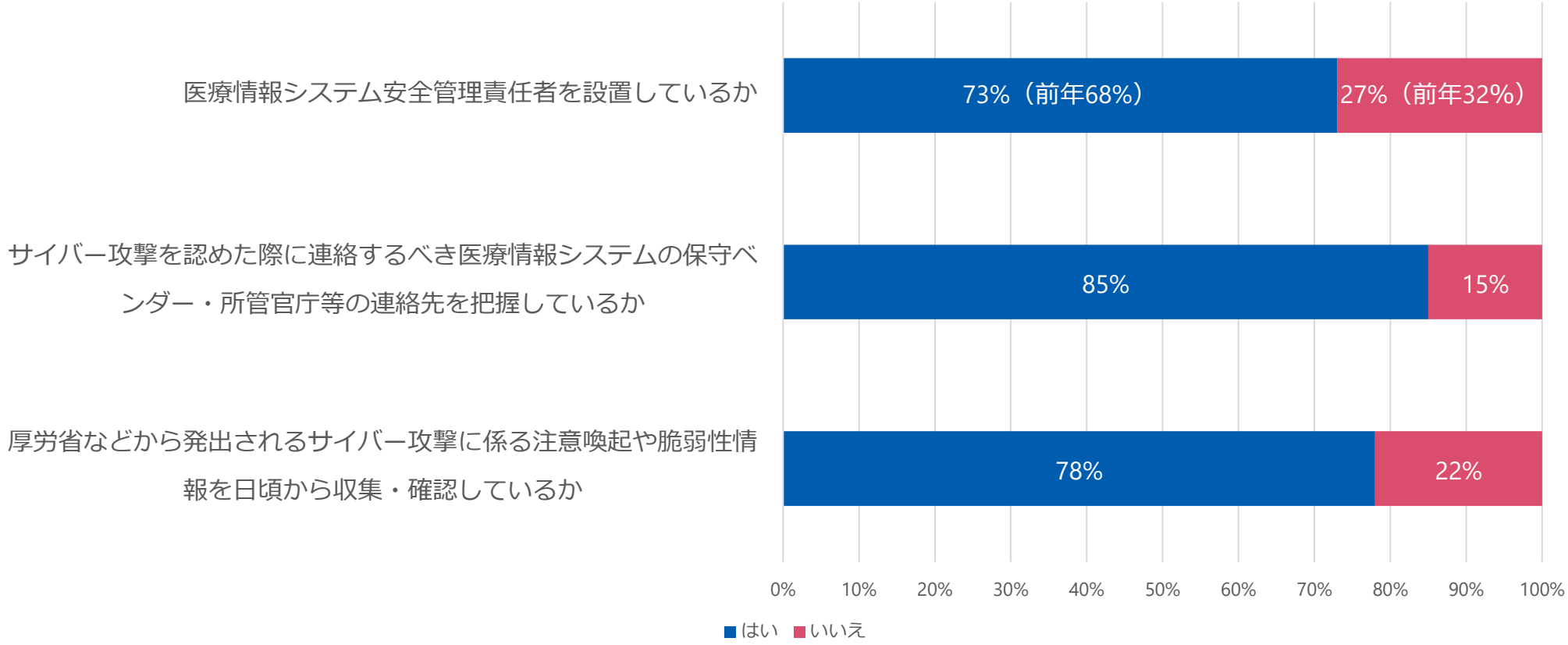
## 調査期間

・令和５年１月27日（金）～　令和５年３月15日（水）

# 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%）

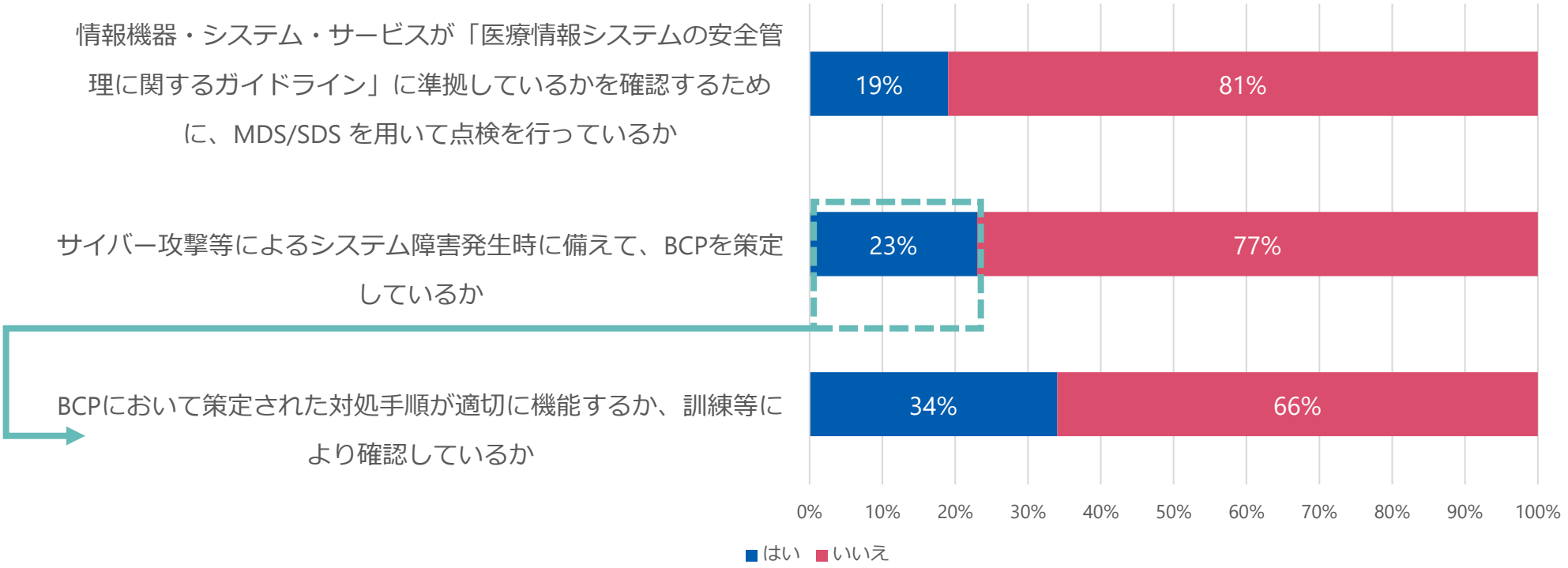



○医療情報システム安全管理責任者の設置、サイバー攻撃を認めた際に連絡すべき所管官庁等の連絡先の把握、サイバー攻撃に係る注意喚起や脆弱性情報の収集・確認は調査対象医療機関の内、70%以上で行っていた。

○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）



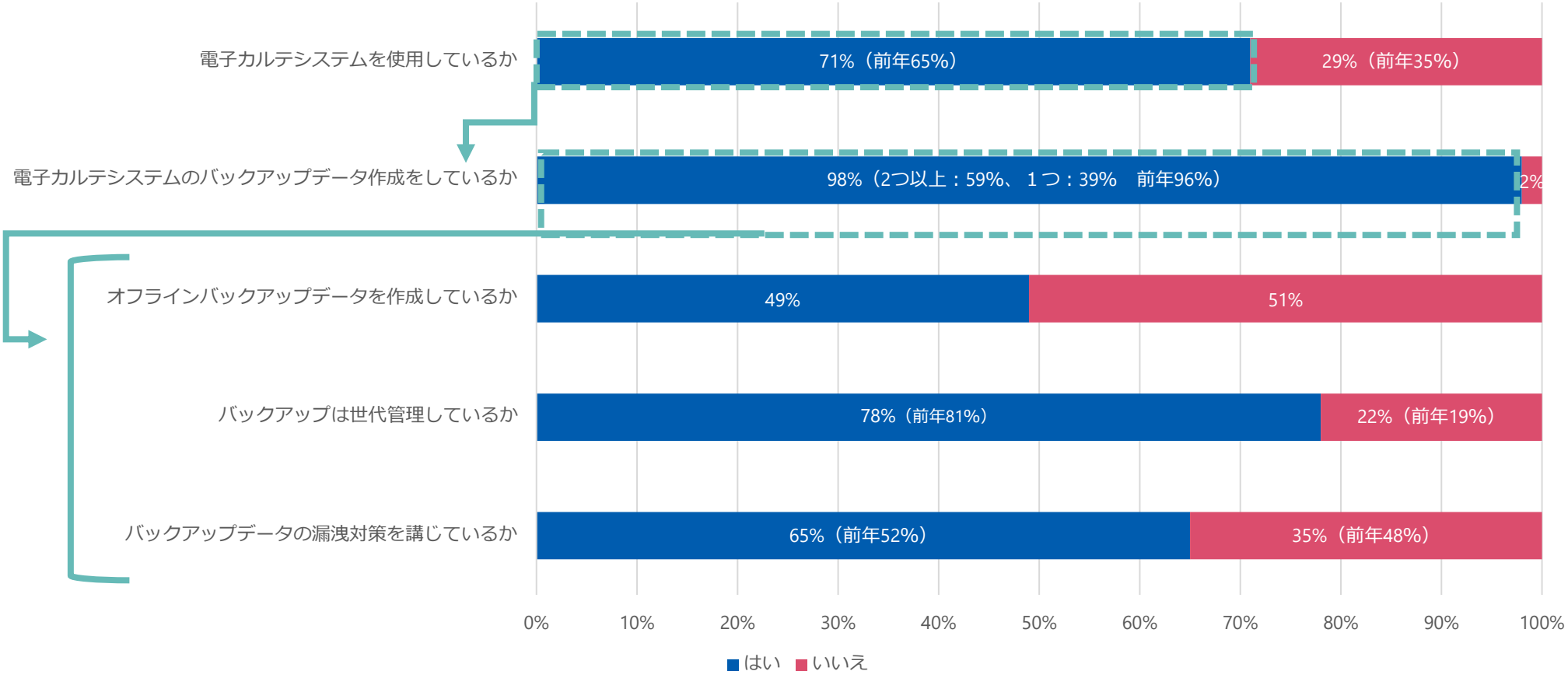

※最後の質問については、2項目でBCPを策定している23%が母数となっている

○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。

# 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）



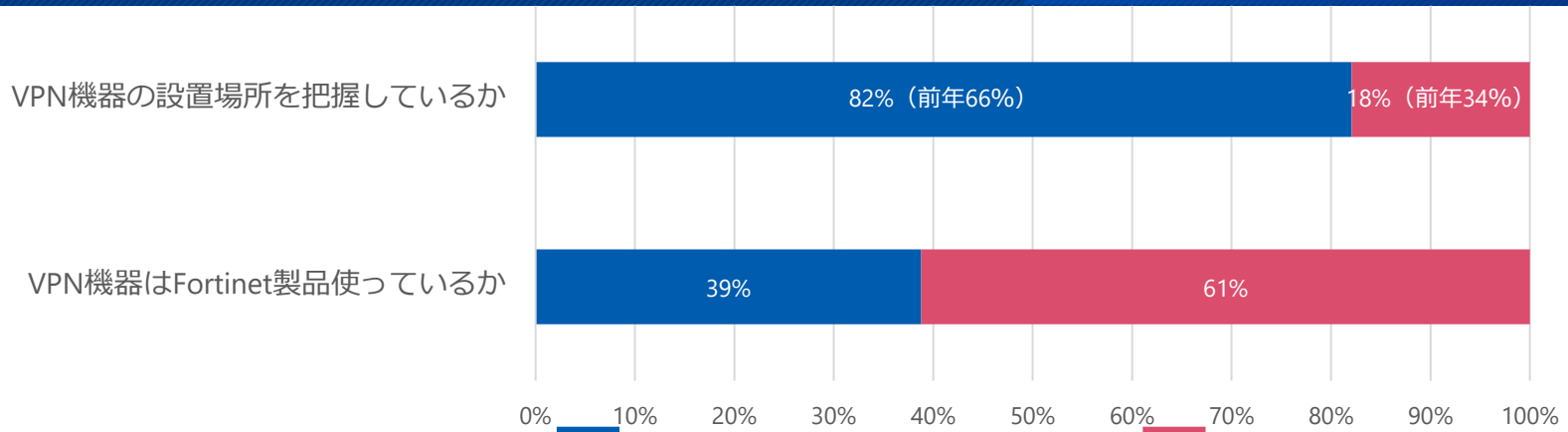

※3項目以降については、2項目でバックアップデータを作成している98%が母数となっている

○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。

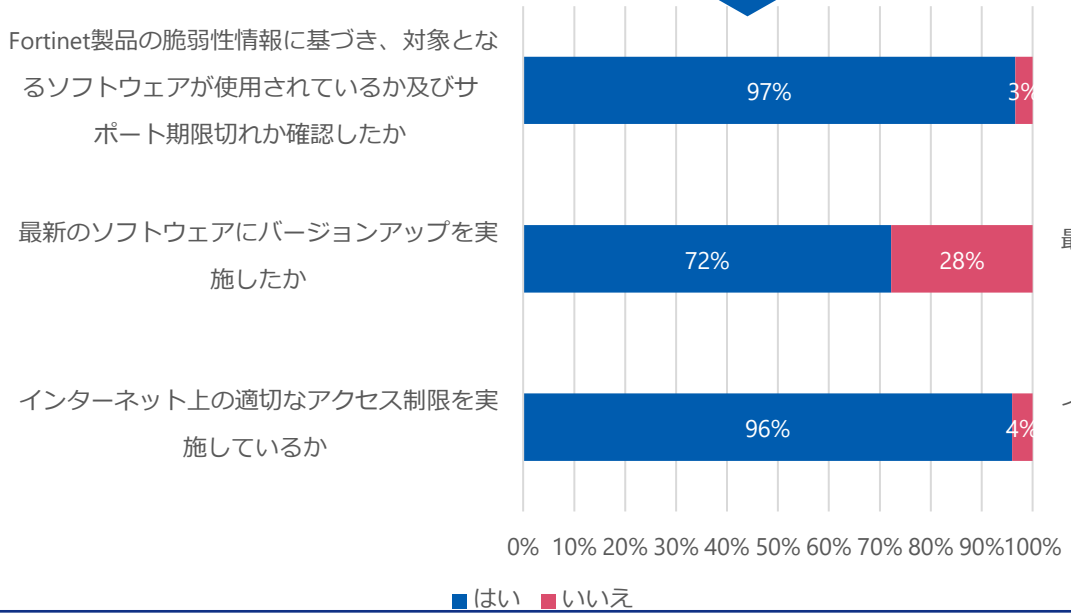
# 調査結果について（リモートゲートウェイ装置について）

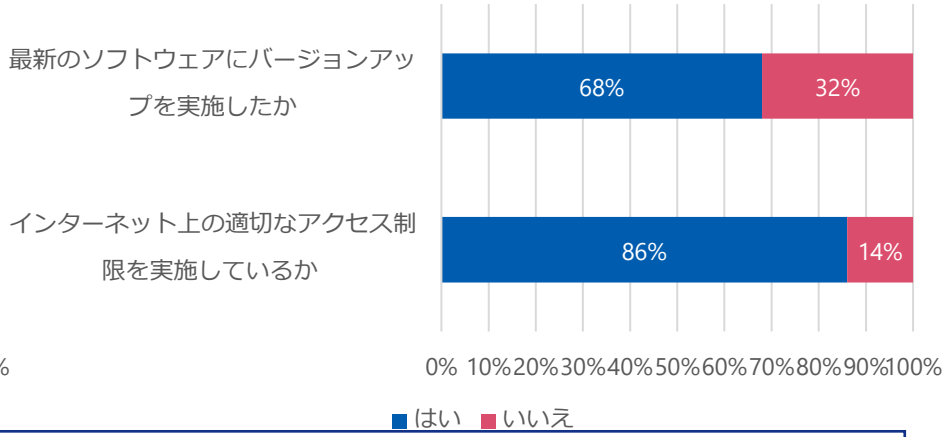
令和５年３月17日集計（速報値）




※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

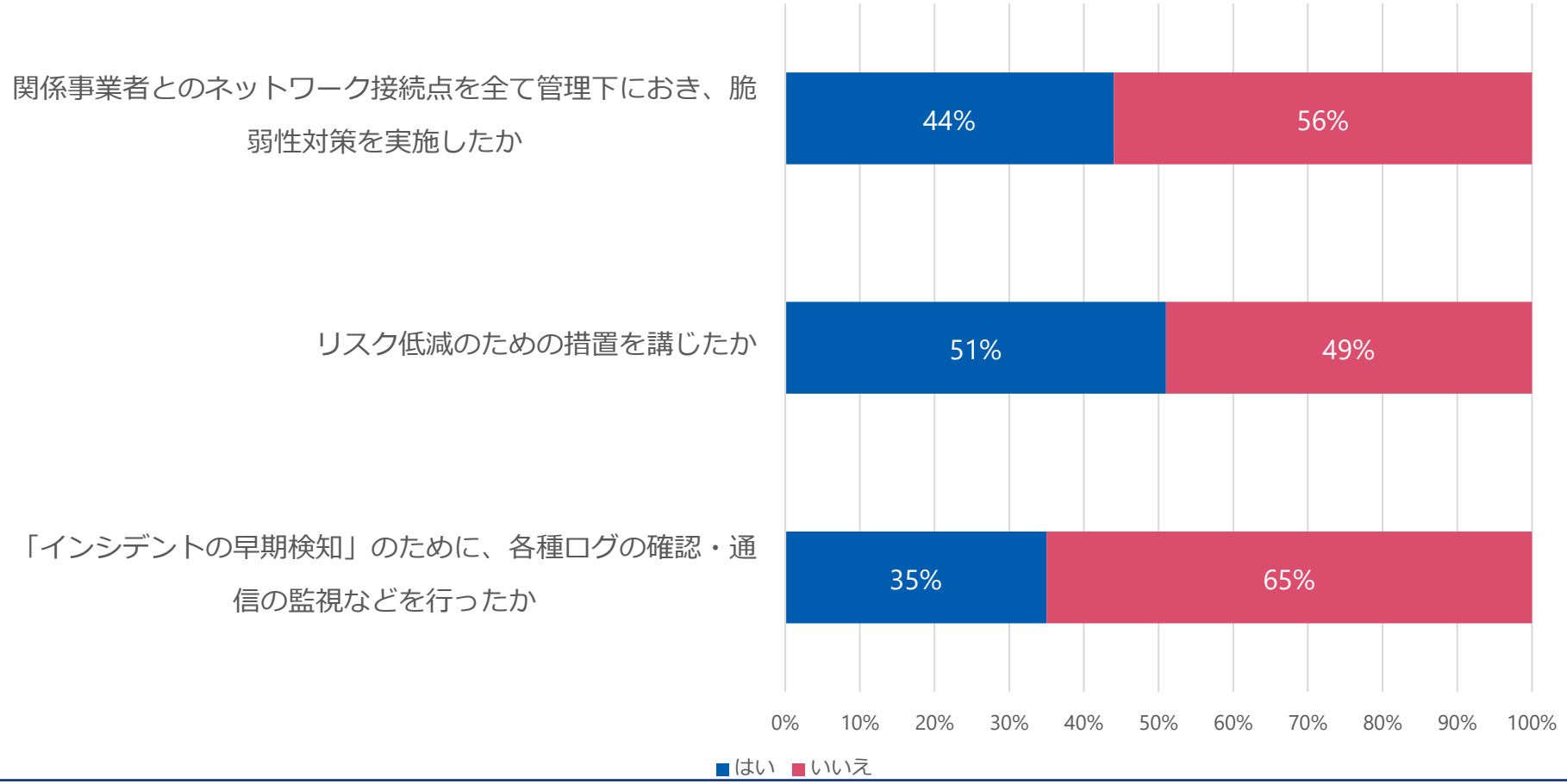



○VPN機器の設置場所把握をしている医療機関は、調査対象医療機関の内、82%であり、その内、Fortinet製品を使用している医療機関は39%であった。最新のソフトウェアにバージョンアップの実施と適切なアクセス制限をしている医療機関は各々、調査対象医療機関の内、Fortinet製品を使用している医療機関で72%、96%、使用していない医療機関で68%、86%であった。

# 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）」）

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。