

「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（病床別分析結果）

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に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

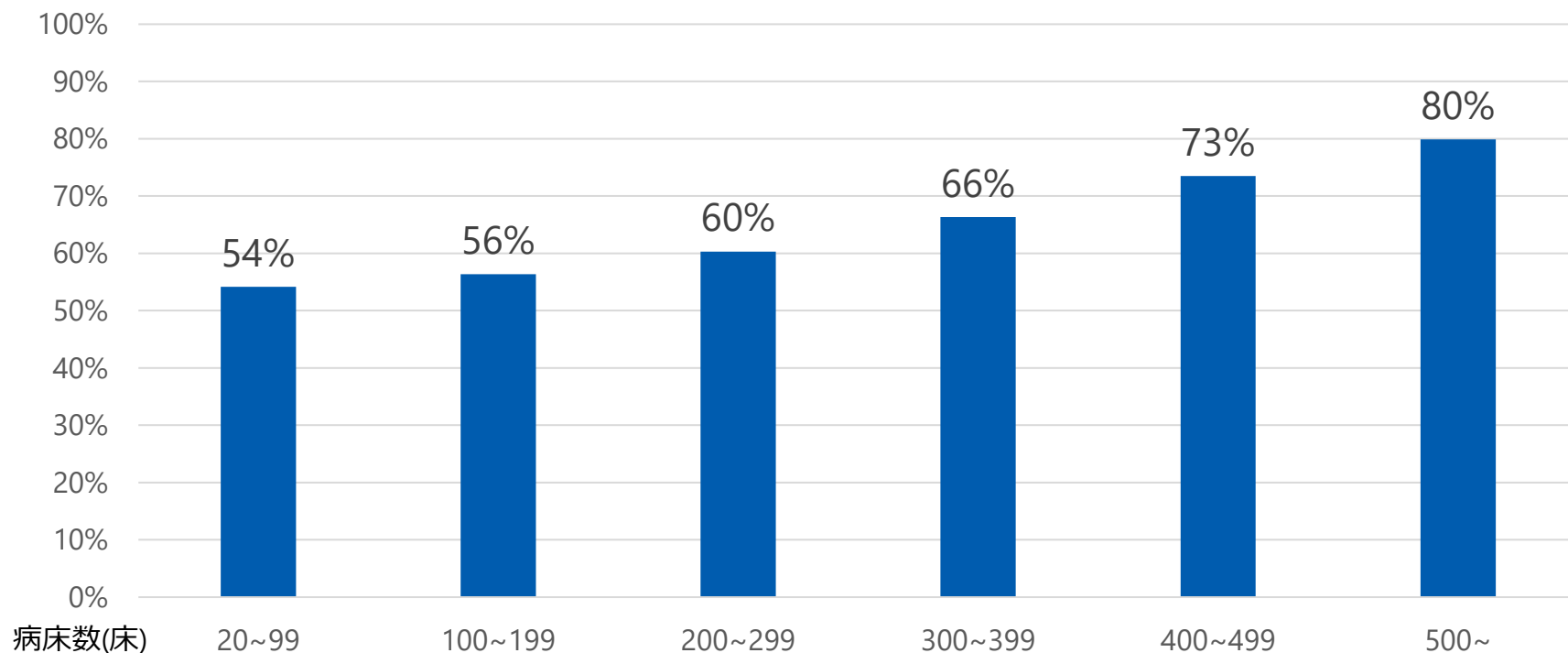
- ・ 令和5年1月27日（金）～ 令和5年3月15日（水）

今回の分析対象

分析対象医療機関数：8,172施設 有効回答数：4,801施設（回答率：58,7%）

※分析対象医療機関は、G-MIS IDが付与されており、かつ、病床数が判明している医療機関。

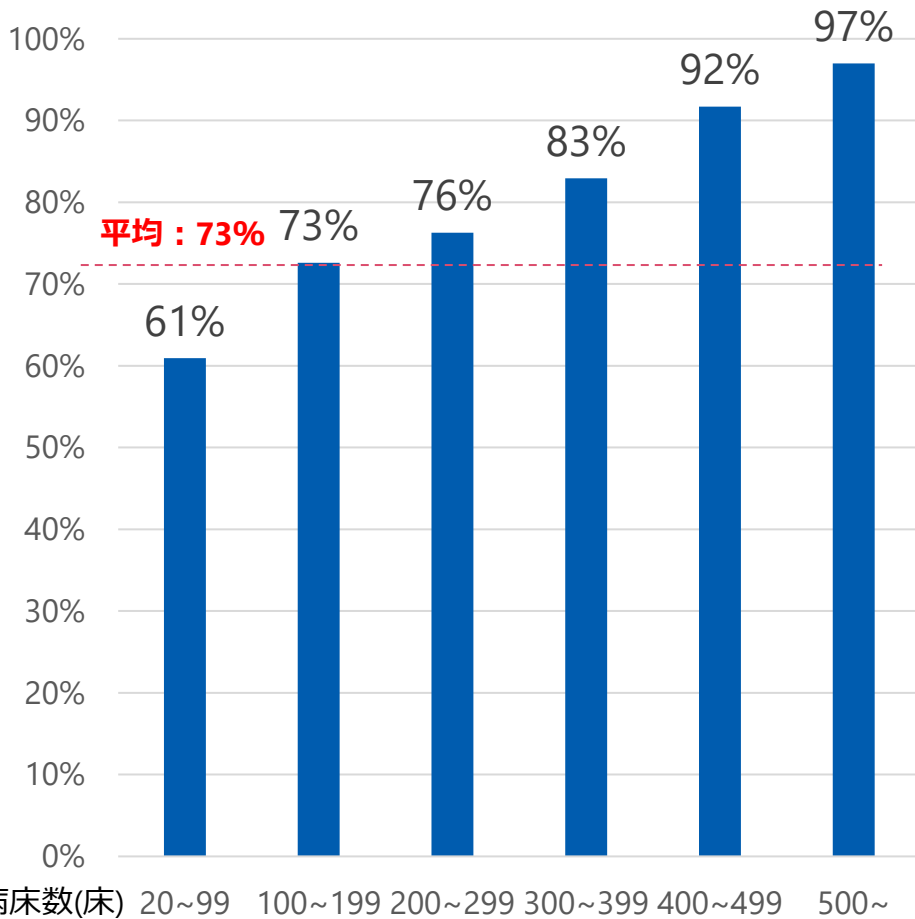
回答率



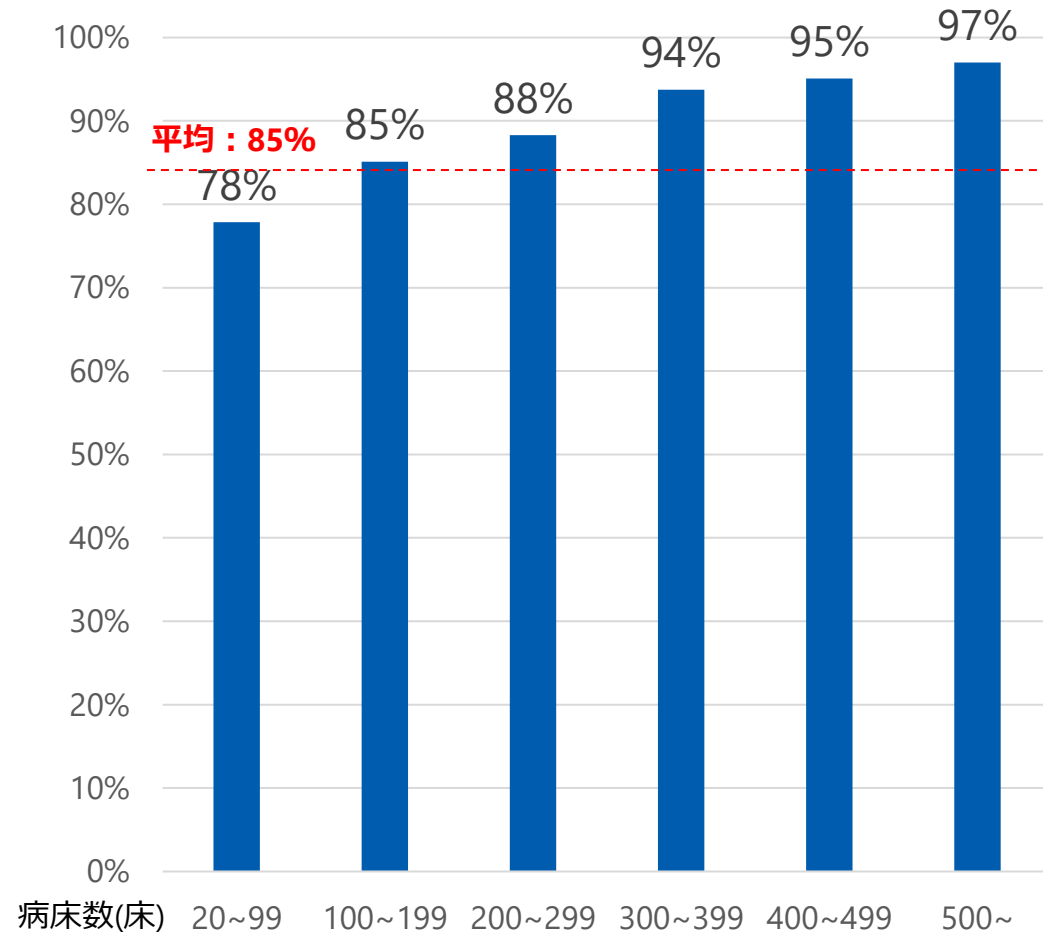
病床数（床）	20~99	100~199	200~299	300~399	400~499	500~	合計
調査対象医療機関数	2910	2821	1022	674	362	383	8172
有効回答数	1576	1590	616	447	266	306	4801

調査結果について（体制構築と連絡体制について）

医療情報システム安全管理責任者を
設置しているか



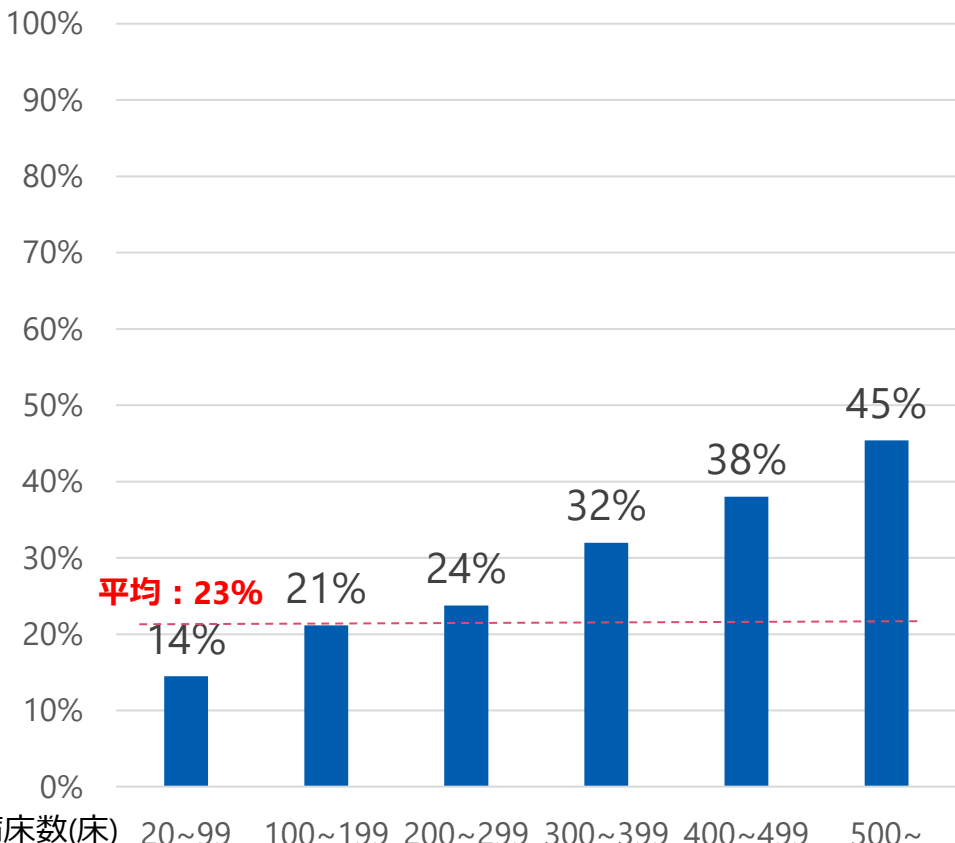
サイバー攻撃を認めた際に連絡すべき医療情報システムの
保守ベンダー・所管官庁等の連絡先を把握しているか



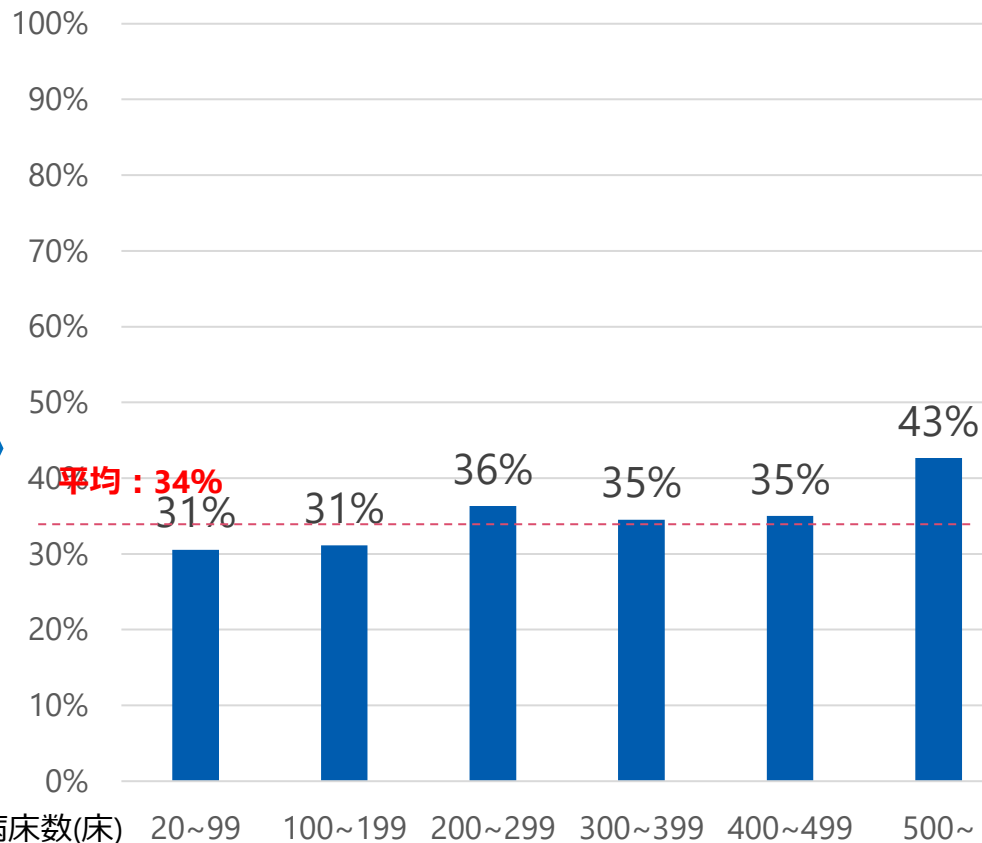
- 医療安全管理責任者を設置している医療機関の割合は、400~499床で92%、500床以上で97%であった。
- サイバー攻撃を認めた際に連絡すべき医療情報システムの保守ベンダー・所管官庁等の連絡先を把握している医療機関の割合は、すべての病床数区分において、約80%以上であった。

調査結果について（BCP策定・訓練について）

サイバー攻撃等によるシステム障害発生時に
備えて、BCPを策定しているか



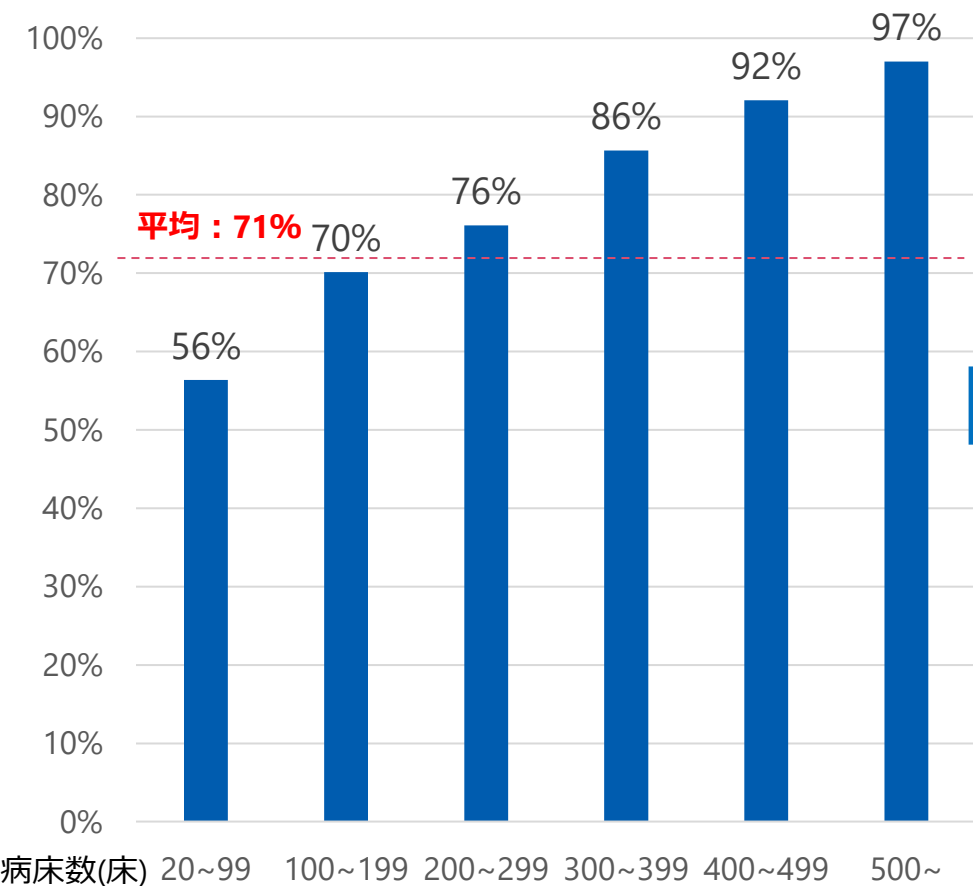
BCPにおいて策定された対処手順が適切に機能す
るか、訓練等により確認しているか



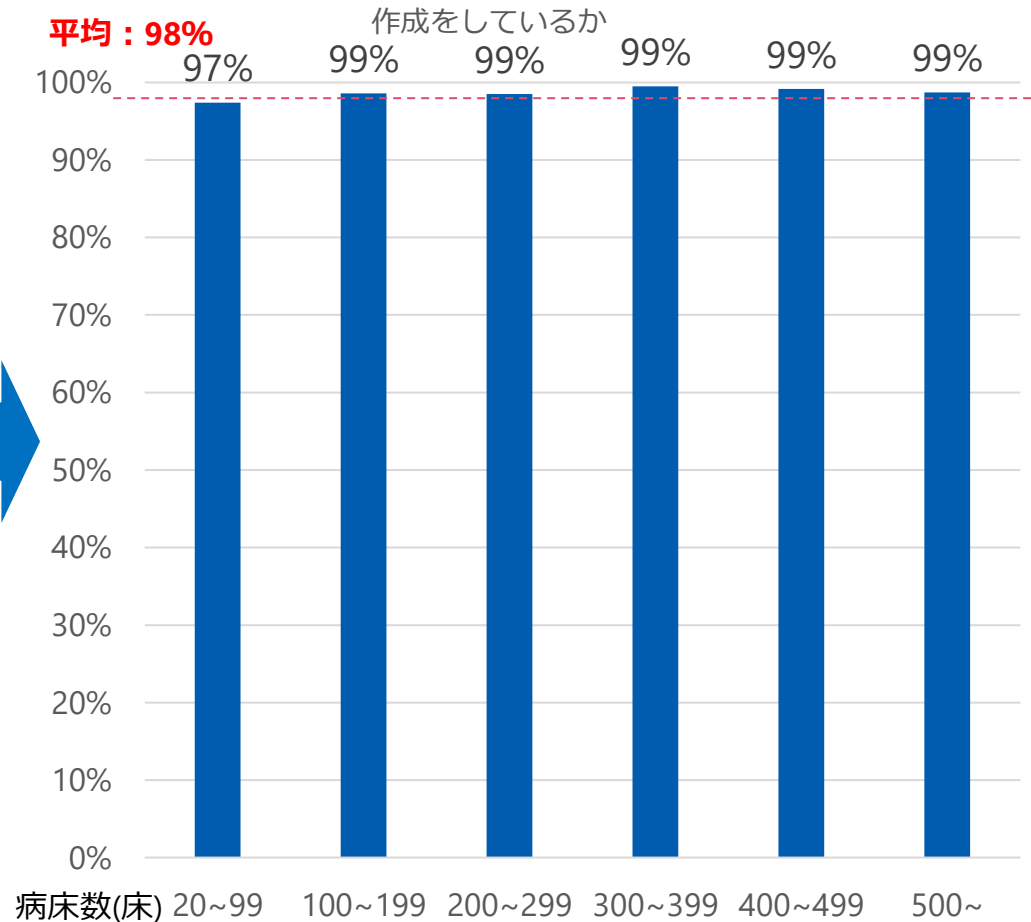
- サイバー攻撃等によるシステム障害発生時に備えて、BCPを策定している医療機関の割合は、病床数が多い医療機関ほど高くなる傾向にあった。
- BCPを策定している医療機関のうち、BCPにおいて策定された対処手順が適切に機能するか、訓練等により確認している医療機関の割合は、すべての病床数区分において、約30%~40%であった。

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①）

電子カルテシステムを使用しているか



電子カルテシステムのバックアップデータ

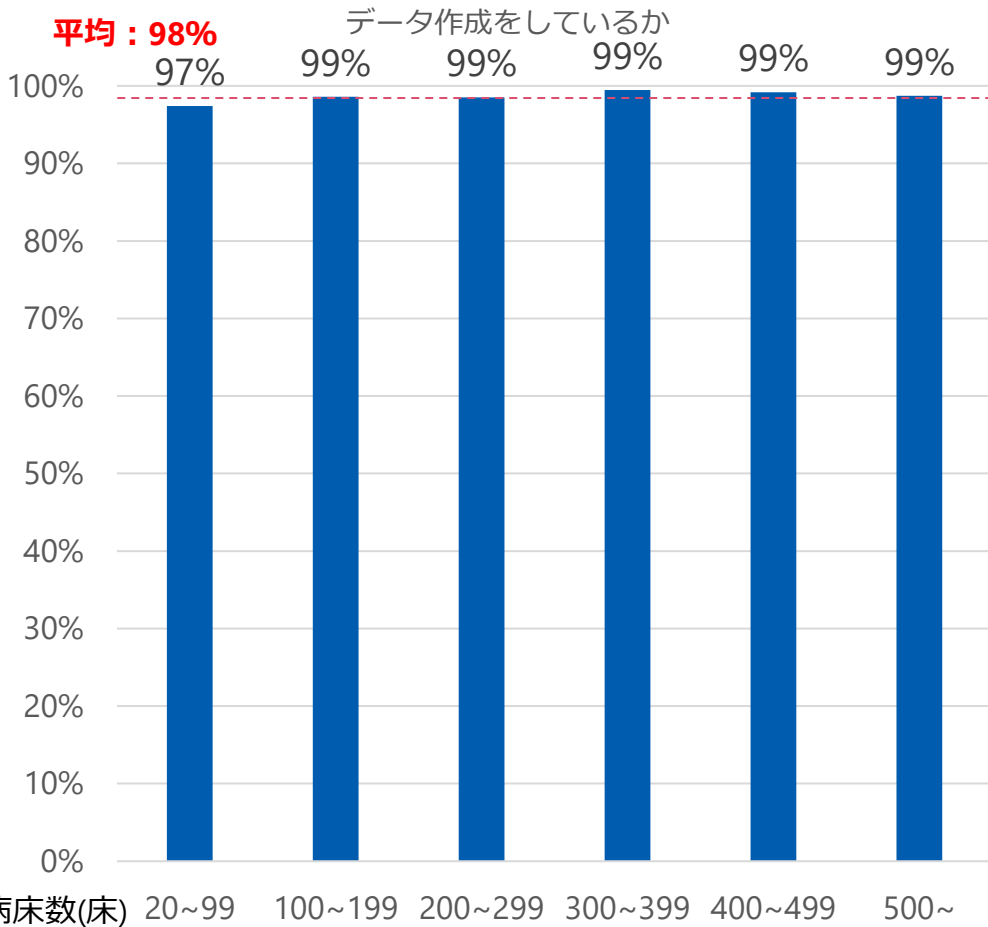


※電子カルテシステムを使用している医療機関数が母数となっている

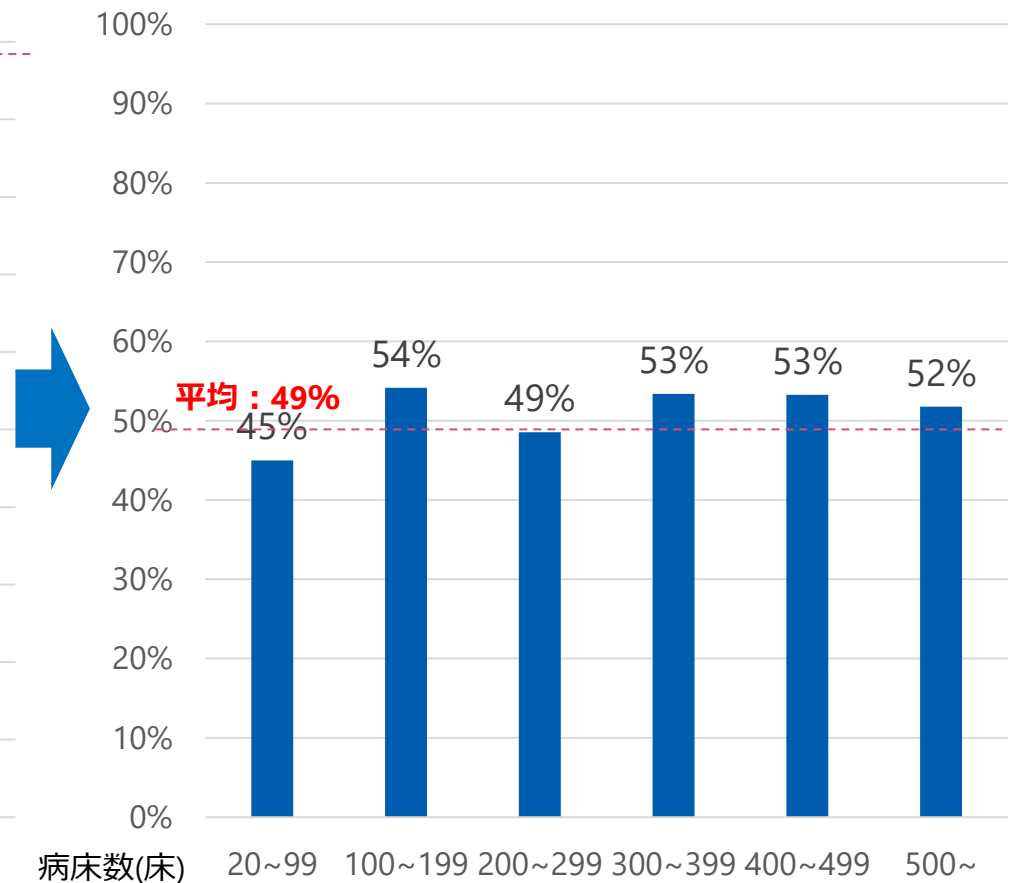
- 電子カルテシステムを使用している医療機関の割合は、病床数が多い医療機関ほど高くなる一方で、20~99床では56%であった。
- 電子カルテシステムを使用している医療機関のうち、電子カルテシステムのバックアップデータを作成している医療機関の割合は、すべての病床数区分において、約100%であった。

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②）

電子カルテシステムのバックアップ



オフラインバックアップデータを作成しているか



※バックアップデータ作成をしている医療機関数が母数となっている

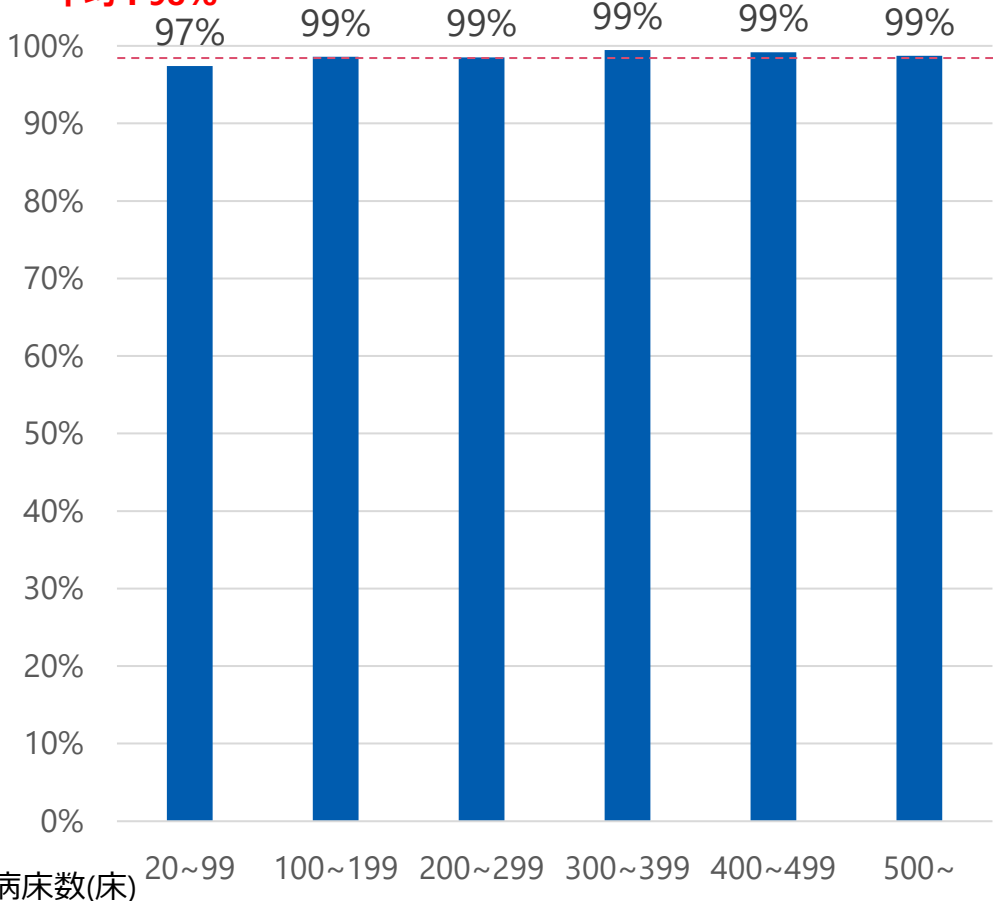
○電子カルテシステムのバックアップデータを作成している医療機関のうち、オフラインバックアップデータを作成している医療機関の割合は、すべての病床数区分において、約50%であった。

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③）

電子カルテシステムのバックアップ

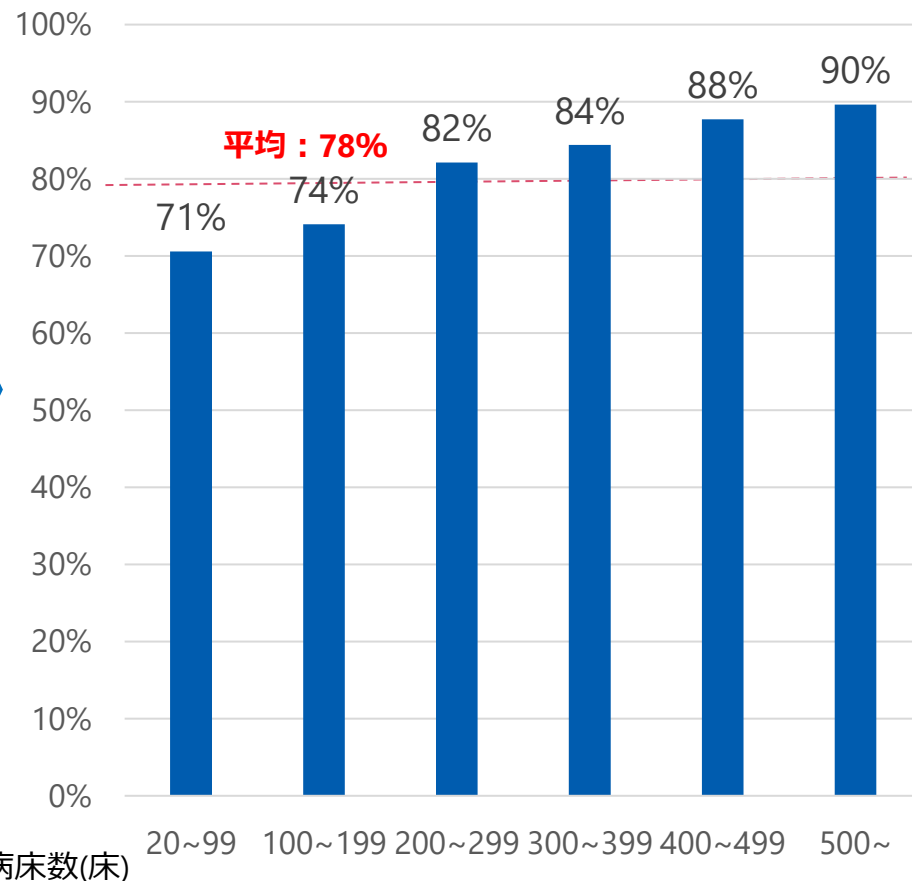
平均：98%

データ作成をしているか



バックアップは世代管理しているか

平均：78%

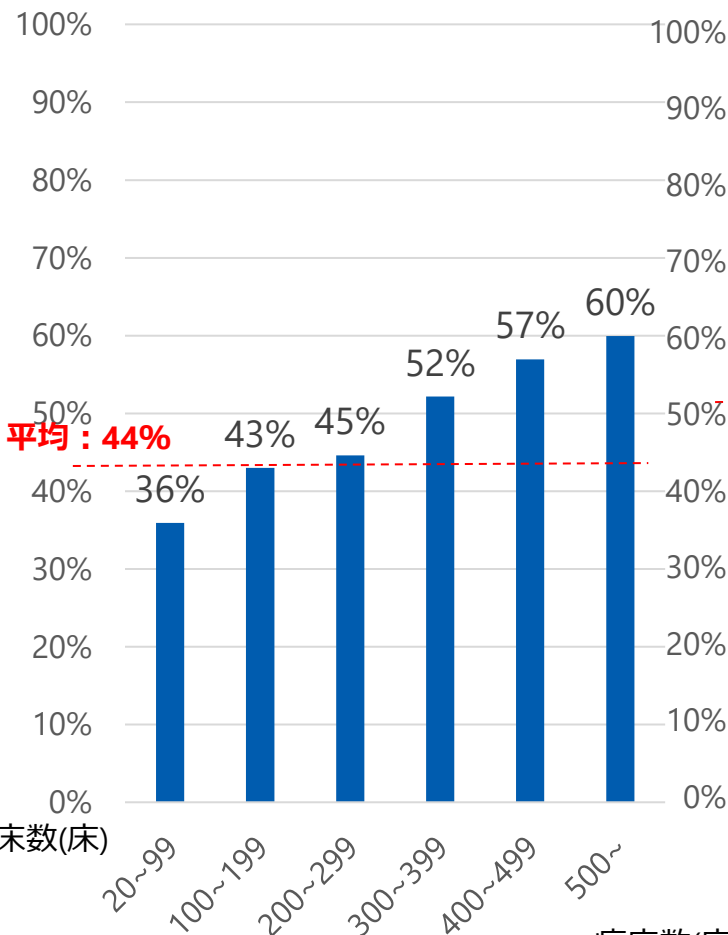


※バックアップデータ作成をしている医療機関数が母数となっている

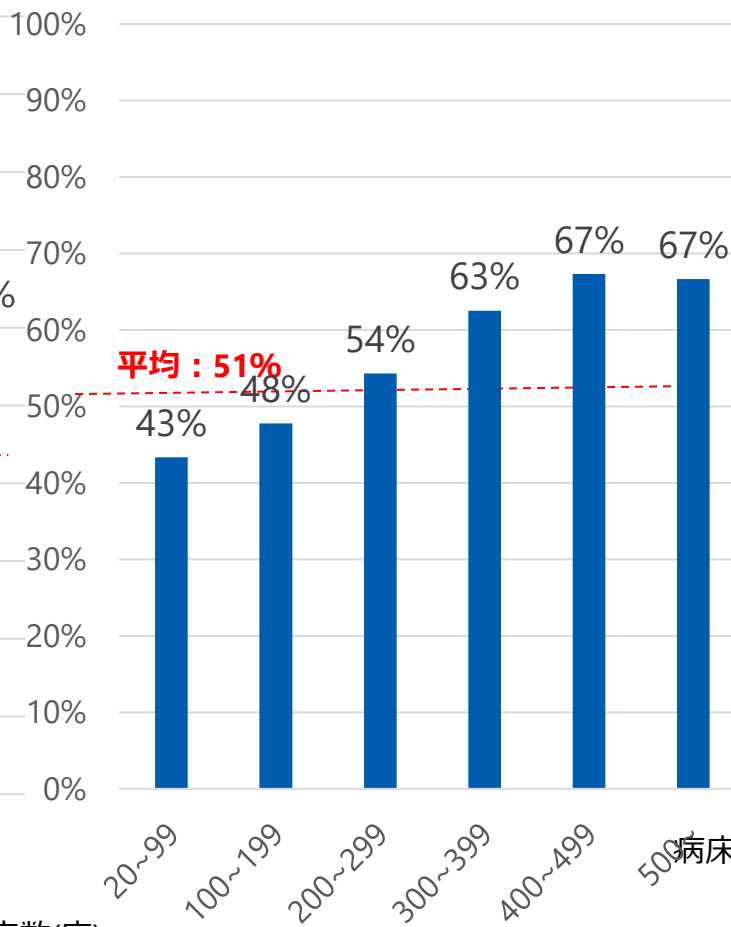
○電子カルテシステムのバックアップデータを作成している医療機関のうち、バックアップを世代管理している医療機関の割合は、病床数が多い医療機関ほど高くなる傾向にあった。

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）」）

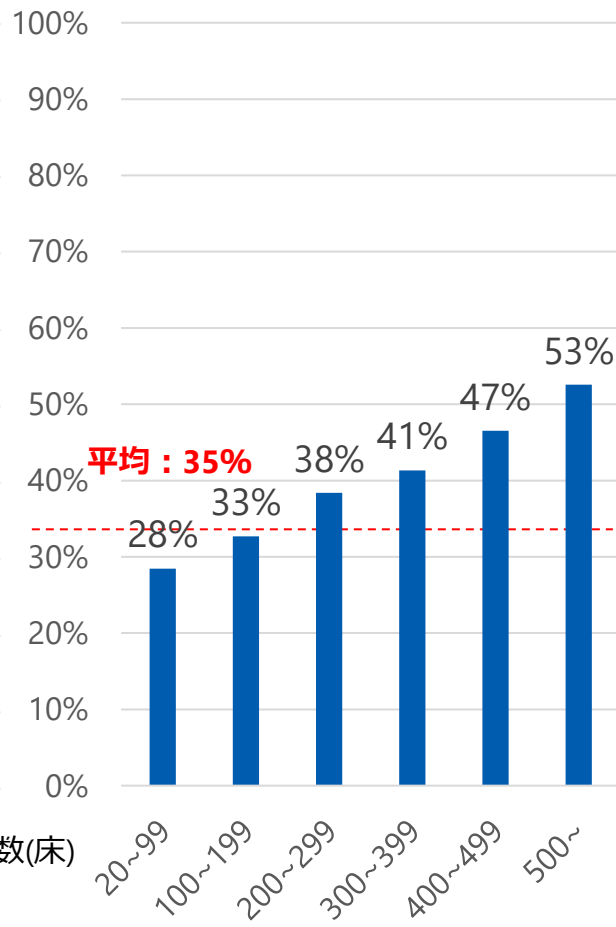
関係事業者とのネットワーク接続点を全て管理下におき、脆弱性対策を実施したか



リスク低減のための措置を講じたか



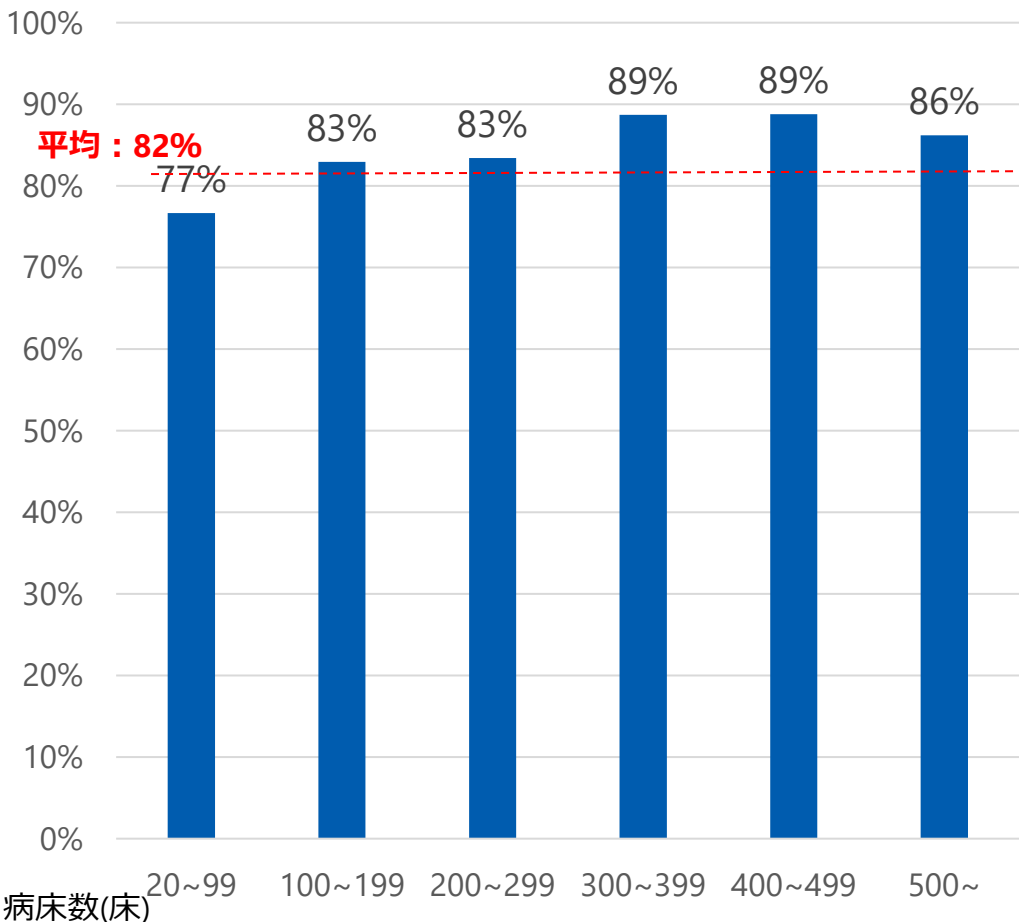
「インシデントの早期検知」のために、各種ログの確認・通信の監視などを行ったか



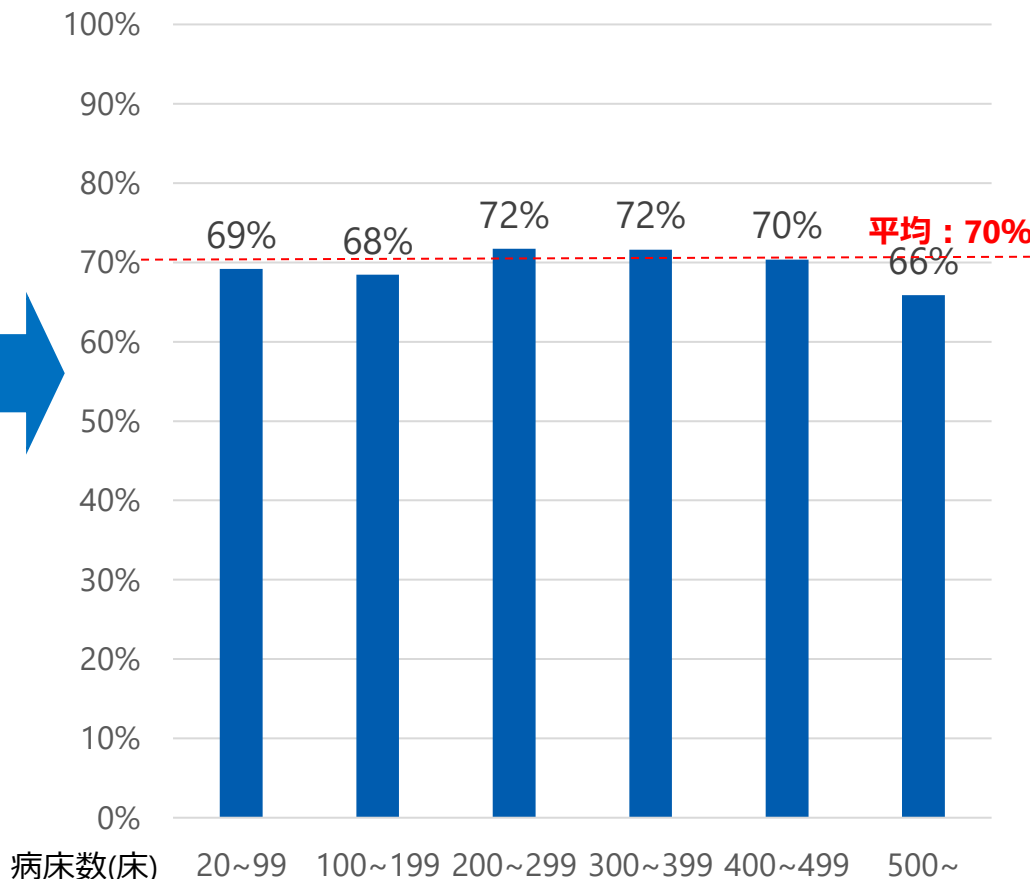
○関係事業者とのネットワーク接続点を全て管理下におき、脆弱性対策を実施した医療機関や、リスク低減のための措置を講じた医療機関、「インシデントの早期検知」のために各種ログの確認・通信の監視などを行った医療機関の割合は、いずれも病床数が多い医療機関ほど高くなる傾向にあった。

調査結果について（リモートゲートウェイ装置について①）

VPN機器の設置場所を把握しているか



最新のソフトウェアにバージョンアップを実施したか

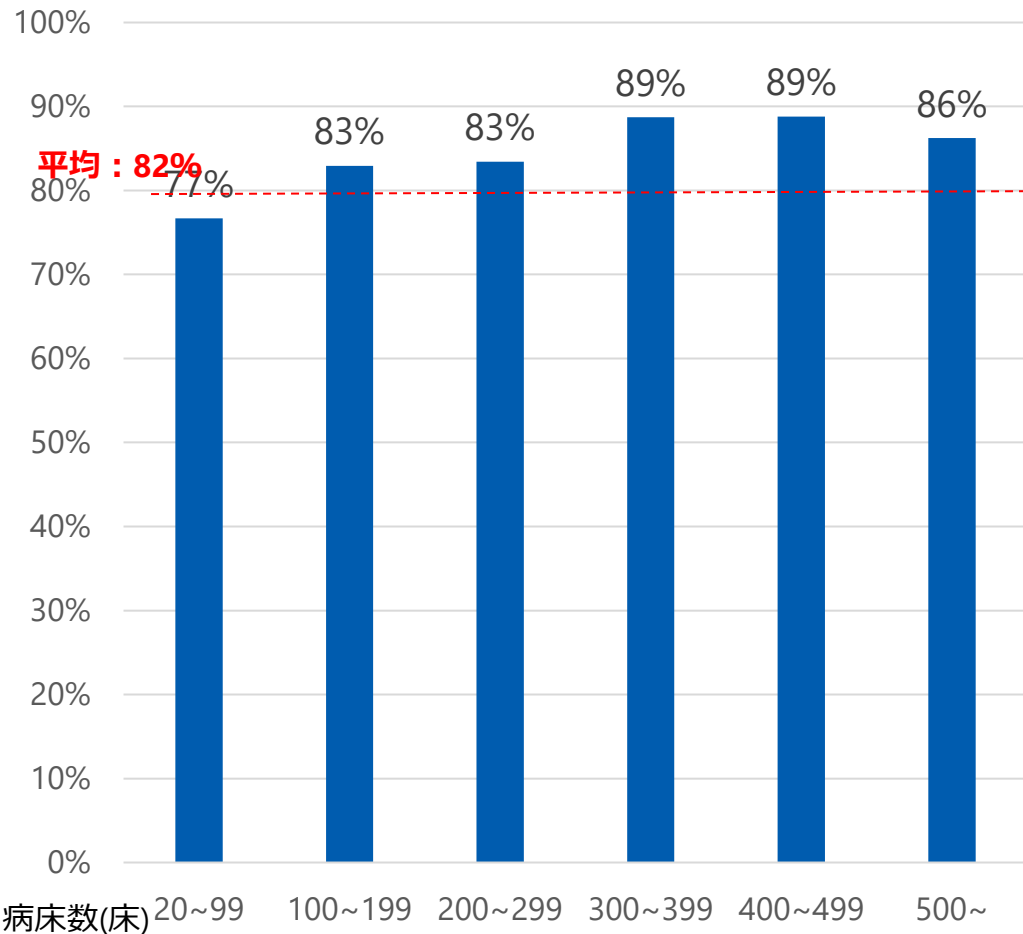


※VPN機器の設置場所を把握している医療機関数が母数となっている

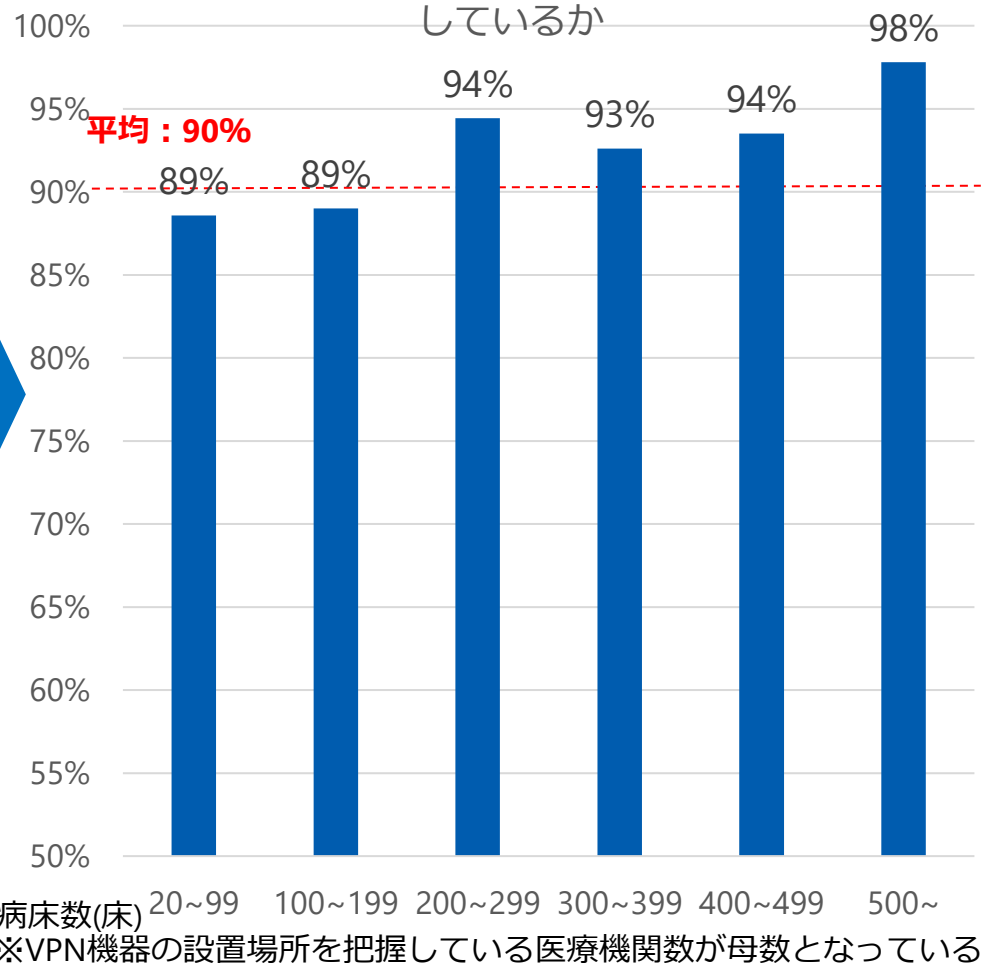
- VPN機器の設置場所を把握している医療機関の割合は、すべての病床数区分において、80%~90%であった。
- VPN機器の設置場所を把握している医療機関のうち、VPN機器について最新のソフトウェアへのバージョンアップを実施した医療機関の割合は、すべての病床数区分において、約70%であった。

調査結果について（リモートゲートウェイ装置について②）

VPN機器の設置場所を把握しているか



インターネット上の適切なアクセス制限を実施



○VPN機器の設置場所を把握している医療機関のうち、インターネット上の適切なアクセス制限を実施している医療機関の割合は、すべての病床数区分において、約90%以上であった。