厚生労働行政推進調査事業（地域医療基盤開発推進研究事業）
研究報告書

医療分野のサイバーセキュリティに関する意識調査
令和 4 年度報告　日本病院会会員施設へのアンケートの実施と速報

研究分担者　長谷川高志
特定非営利活動法人日本遠隔医療協会

研究要旨

昨年度の小規模集団にパイロット調査を行ったアンケートについて、本格的に実施した。日本病院会の会員を対象として、2489 会員に案内して、581 件（23.3%）の回答を得た。昨年度の小規模集団での回答率の 2 倍以上を得た。多忙な病院現場にも関わらず、設問数の多いアンケートへの積極的な対応と受け止めた。

回答は学会実施と比べて、知識水準等に差異は無かった。コストや人員不足、対策技術の方向性の不統一など現場の厳しい状況が明らかとなった。

A．研究目的

1．研究の背景

令和 3 年度に病院に於けるサイバーセキュリティの管理状況のアンケートを設計して、日本遠隔医療学会会員に試験的に実施した。その結果として、回答率は低かったが、サイバーセキュリティに高い意識を持つ回答者による調査結果が得られた。そこで本格的に多数の病院のサイバーセキュリティに関する状況を調査することとなった。

本調査の実施中の 2022 年秋には、大阪府の大阪急性期医療センターがランサムウェア攻撃を受け、サプライチェーン経由の攻撃への懸念が高まった。深刻な案件発生と並行したアンケート実施となった。

2．研究の対象

所在地域、規模や運営形態の異なる多数の病院を調査するために、一般社団法人日本病院会の協力を得て、会員施設を対象にアンケートを実施した。

3．調査内容

サイバー犯罪に対峙する各施設の管理に対する意識や状況を調査した。アンケートの内容は令和 3 年度研究で日本遠隔医療学会会員に行ったものと同じである。

4．研究の運営

令和 4 年度のアンケート調査では、日本病院会を介した調査なので、本研究班と近しい日本遠隔医療学会会員を対象とした際よりも、丁寧に依頼や説明の手続を踏んで進めた。

B．研究方法

1．アンケートシステム

低コスト、低負担、短期実施が欠かせないため、令和 3 年度研究と同じく GoogleForm を用いた WEB アンケートとした。

2．設問

前年度に近藤博史研究代表者が作成した、以下の設問群と設問数のアンケートを実施した。

①回答者の基本属性	24 問
②組織で実施しているセキュリティ対策	9 問
③施設内での規定の有無等	3 問
④セキュリティインシデント発生時の対応	12 問
⑤侵入経路の対策として実施している事項等	13 問
⑥ウイルス対策の状況	4 問
⑦サイバーセキュリティ対策への意見	4 問
⑧最近のサイバー攻撃に対する理解度	9 問
⑨重要データ保存について実施している事項	6 問
⑩情報部門の管理について	5 問
⑪ISAC について情報共有したい事項等	14 問
⑫その他意見	3 問

合計　106 問

3．アンケート実施管理

（1）日本病院会への依頼

日本病院会には 2022 年 5 月から、の大道道久副会長と相談を開始して、アンケートへの協力依頼文章の送付などの手続を進めた。日本病院会殿向けの依頼文書を資料 1, 病院会会員各施設向けの依頼文書を資料 2 に示す。

（2）調査期間

2022 年 9 月 20 日～11 月 7 日に実施した。 日本病院会を通じて、会員各施設に案内を送り、この期間にアンケートの回答を得た。日本病院会本部より、多くの回答を得るため、複数回にわたり、アンケート協力依頼のメールを各施設に発信した。

（3）対象者数は、日本病院会参加施設数の 2489 だった。

(4)解析は、株式会社エヌ・ティー・ティ・データ経営研究所に委託した。

C．研究結果
1．回答件数　581 件（23.3%）

2．回答の概要
（1）回答者は職種なし（一般職）が大半となった。
（2）ICT 関連学会に所属しない回答者が大半となった。
（3）日本遠隔医療学会でのアンケート（令和 3 年度）と知識や情報について、傾向として差異は小さかった。情報システム管理などを担当する職員が回答者に多いと推測され、日本遠隔医療学会員の回答より、具体的な状況の回答が多く得られた。
（4）大きな傾向には、以下がある。
①技術的知識や価値感は適正と考えられる。
②現状に高い危機感を持っている。
③サイバーセキュリティのためのコストは限られ、組織・体制は十分と言えない。

3．考察
（1）アンケートの回答率は、日本遠隔医療学会より高く、581 件、23％であった。一般的なアンケートとしては低い回答率だが、設問数が非常に多く、設問も難度が高く、負担感の大きいアンケートに 23％の回答率を得たことは、社会的課題としての重要性を感じる施設が多かったと推測する。
（2）日本遠隔医療学会向けよりも、システム管理担当者としての立場の回答者が多いと考えられる。より実務的か回答の傾向と考えられる。
（3）75％強の施設が回答しなかったが、以下の懸念がある。
①　本調査の回答は、“意識が高い”、“知識や情報を収集している”施設に偏っている。
②回答しなかった施設を含め、多くの病院が、知識・情報・現状の管理体制で、本回答より深刻な状況にある。
（4）本アンケートへの不満として、まとまりがない、意図がわからないなどの指摘が少なくなかった。本アンケートの欠点以前の課題として、令和 3 年度総括報告中の分担報告でも指摘した通り、サイバーセキュリティに関する社会的課題の構造（制度、製作、許されること・許されないこと、技術評価など）の共通認識の不足から、回答者のちてき水準が高くとも、意識付けに方向性がないことを示唆している。
社会的課題の構造的捉え方の共有、社会的評価尺度の確立を行わないと、各施設が、各々の思い込みでバラバラな方向への対策を取る懸念がある。比喩だが、社会として共通する交通ルールの無い世の中で、交通安全を守るための意識作りをボトムアップで進めることに近い。例え意識と技能が高い運転者が多くとも、共通ルールがなければ交通安全は保てないし、交通犯罪も抑止できない。方向性を近いものとするためにも、ISAC などの取り組みを“社会的評価視点”の下で進める必要性も示唆している。
（5）各施設の技術水準を比較可能なデータとして捉えるには、設問数の多い調査が不可欠である。設問数を減らすと“技術への自己認識”を把握できるが、具体的な技術水準を比較可能な情報として捉えられない。それにより、今回調査で回答施設の技術や知識水準が低くないことを捉えることができた。

4．詳細な調査結果と分析結果について
株式会社エヌ・ティー・ティ・データ経営研究所により分析結果の報告書を添付する。

添付資料
医療分野のサイバーセキュリティに関する意識調査　**報告書（資料 3）**

D．健康危険情報
なし

令和４年度厚生労働行政推進調査事業補助金（地域医療基盤開発推進研究事業）

医療分野のサイバーセキュリティに関する意識調査

報 告 書

令和5年（2023年）3月

株式会社エヌ・ティ・ティ・データ経営研究所

目次

第１章　事業の概要

１．事業の目的等

（１）事業名

令和 4 年度厚生労働行政推進調査事業

（２）研究課題

ヘルスケア分野のサイバーセキュリティに関する調査

（３）目的

上記課題の研究活動において、遠隔医療、医療 ICT に関連する業務に従事する医療者、技術者に医療分野のサイバーセキュリティに関する意識調査（アンケート）を行う。

アンケート調査の対象は、一般社団法人日本遠隔医療学会の学会員、日本病院会の会員施設などである。なお今年度は日本病院会の会員施設を対象として調査を行ったが、令和 3 年度における日本遠隔医療学会の会員を対象とした調査結果を比較対象とした。

２．事業実施概要

（１）実施体制

・研究代表者

特定非営利活動法人日本遠隔医療協会　近藤博史

・研究分担者（本調査担当）

特定非営利活動法人日本遠隔医療協会　長谷川高志

・アンケート調査結果の集計分析・報告書作成担当者

ＮＴＴデータ経営研究所　ライフ・バリュー・クリエイションユニット
アソシエイト・パートナー　米澤麻子
マネージャー　西尾文孝
シニアコンサルタント　有賀理瑛
スタッフ　篠田珠絵

（２）アンケート調査

遠隔医療、医療 ICT に関連する業務に従事する医療者、技術者に医療分野のサイバーセキュリティに関する意識調査（アンケート）を行った。

アンケート対象は、一般社団法人日本遠隔医療学会の学会員、日本病院会の会員施設などである。

第２章　アンケート調査

１．調査概要

（１）調査の目的

医療機関等におけるサイバーセキュリティ対策の実態等を把握すること。

（２）調査対象

日本病院会会員施設（約 2489 施設）。

（３）調査方法

調査対象にメールで調査実施の案内をし、WEB 調査画面（Google フォーム）で回答してもらう方法とした。

（４）調査期間

令和 4 年 9 月 21 日～11 月 7 日

（５）設問数

105 問

（６）主な調査項目

①回答者の基本属性	【Q1-Q24】
②組織で実施しているセキュリティ対策	【Q25-Q33】
③施設内での規定の有無等	【Q34-Q36】
④セキュリティインシデント発生時の対応	【Q37-Q46】
⑤CSIRT の活動に関して	【Q47-Q48】
⑥侵入経路の対策として実施している事項等	【Q49-Q61】
⑦ウイルス対策の状況	【Q62-Q65】
⑧サイバーセキュリティ対策への意見	【Q66-Q69】
⑨最近のサイバー攻撃に対する理解度	【Q70-Q78】
⑩重要データの保存について実施している事項	【Q79-Q84】
⑪情報部門の管理について	【Q85-Q89】
⑫ISAC について情報共有したい事項等	【Q90-Q103】
⑬その他意見	【Q104-Q105】

（7）回収者数

回答者数は 581 施設である。

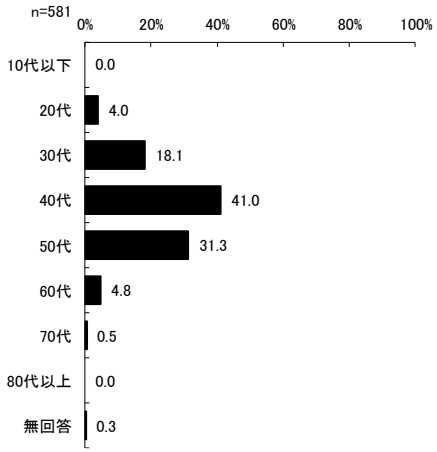
２．調査結果

（１）回答者の基本属性

1）年齢

年齢については、40 代が 41.0％で最も割合が高く、ついで 50 代が 31.3％であった。

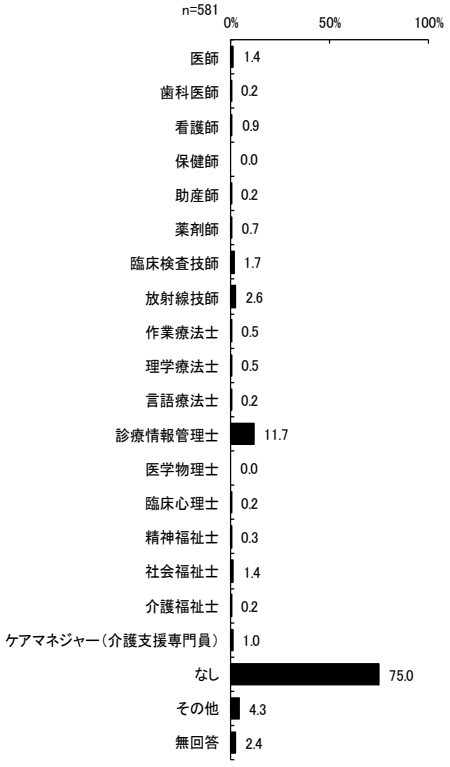
図表 1　年齢（Q1）



2）保有している医療系の資格

保有している医療系の資格については、「なし」が 75.0％で最も割合が高かった。

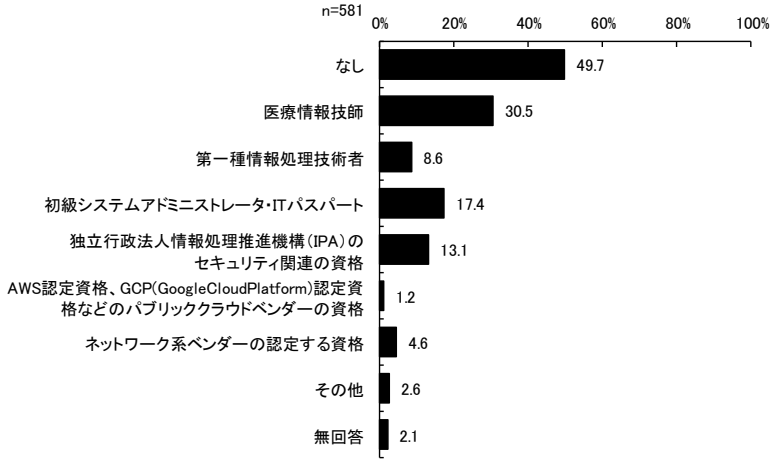
図表 2　保有している医療系の資格（Q2）【複数回答】



3）保有している情報系の資格

保有している情報系の資格については、「なし」が 49.7％で最も割合が高く、ついで医療情報技師が 30.5％であった。

図表 3　保有している情報系の資格（Q3）【複数回答】



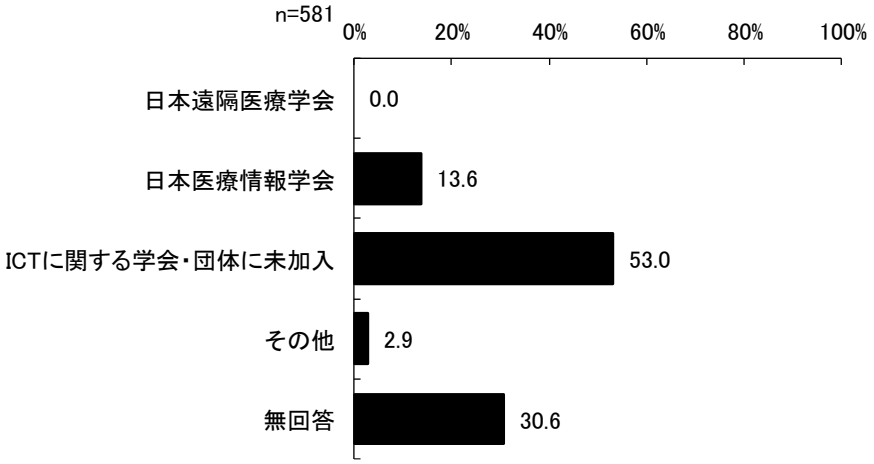
※「その他」の主な回答は以下の通り。

- ITIL
- AZ-104
- ISO27001 審査員
- IT ストラテジスト
- LPI LPIC Level1
- LPIC/MS/Oracle7
- MCSE6:Desktop Infrastructure
- MCSE6:Server Infrastructure
- Microsoft Azure Administrator
- Microsoft 認定資格 6（MCP：Windows10、Active Directory）
- ORACLE MASTER(BRONZE)
- XML MASTER(BASIC)
- データベーススペシャリスト
- テクニカルエンジニア（システム管理）
- ネットワークスペシャリスト
- 医用画像情報専門技師
- 医療情報システム監査人
- 医療情報システム監査人補
- 応用情報技術者
- 基本情報技術者（第二種）
- 第一種情報処理技術者
- 公認医療情報システム監査人補
- 上級医療情報技師
- 上級個人情報保護士
- 情報処理安全確保支援士
- 情報処理検定２級
- 診療情報管理士

4）ICT に関する所属学会・団体

ICT に関する所属学会・団体については、未加入が 53.0％で最も割合が高かった。

図表 4　ICT に関する所属学会・団体（Q4）【複数回答】

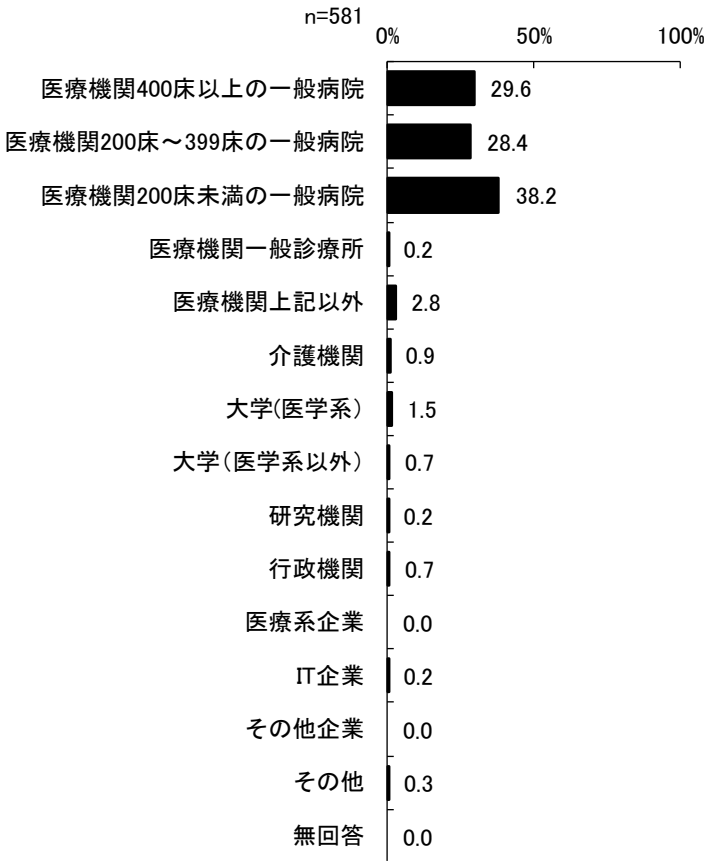


※「その他」の主な回答は以下の通り。
- ユーザー会内 セキュリティ分科会
- 医療情報技師育成部会
- 医療情報技師会
- 九州沖縄医療情報技師会
- 熊本県医療情報システム研究会
- 電子通信情報学会
- 日本医療情報学会

5）所属機関

所属機関については、200 床未満の一般病院が 38.2％で最も割合が高かった。

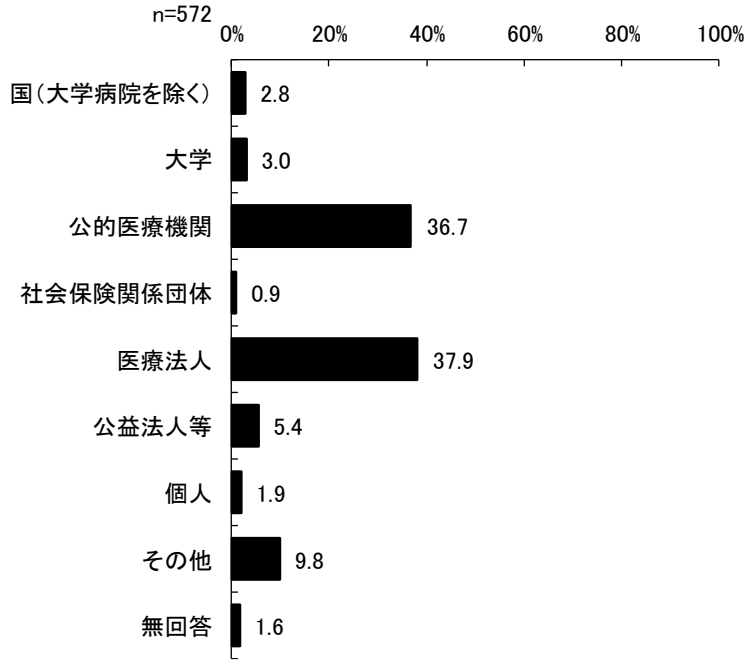
図表 5　所属機関（Q5）【複数回答】



6）施設の開設者（医療機関の場合）

施設の開設者については、医療法人が 37.9％で最も割合が高く、ついで公益医療機関が 36.7％であった。

図表 6　施設の開設者（医療機関の場合）（Q6）



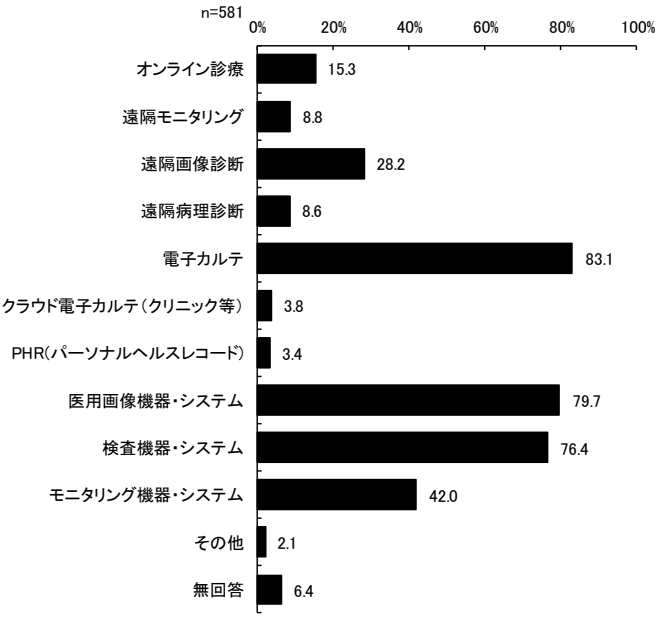
※「その他」の主な回答は以下の通り。

- 医療生活協同組合
- 一般社団法人
- 一部事務組合
- 株式会社
- 健康保険組合
- 公立学校共済組合
- 厚生連
- 国家公務員共済組合連合会
- 社会福祉法人
- 宗教法人
- 新潟県
- 生活協同組合
- 地方公共団体
- 地方独立行政法人
- 自治体
- 独立行政法人
- 日本赤十字社

7）所属機関が提供している医療 ICT に関するサービスや業務、製品

所属機関が提供している医療 ICT に関するサービスや業務、製品については、電子カルテが 83.1％で最も割合が高く、ついで医用画像機器・システムが 79.7％であった。

図表 7　所属機関が提供している医療 ICT に関するサービスや業務、製品（Q7）【複数回答】

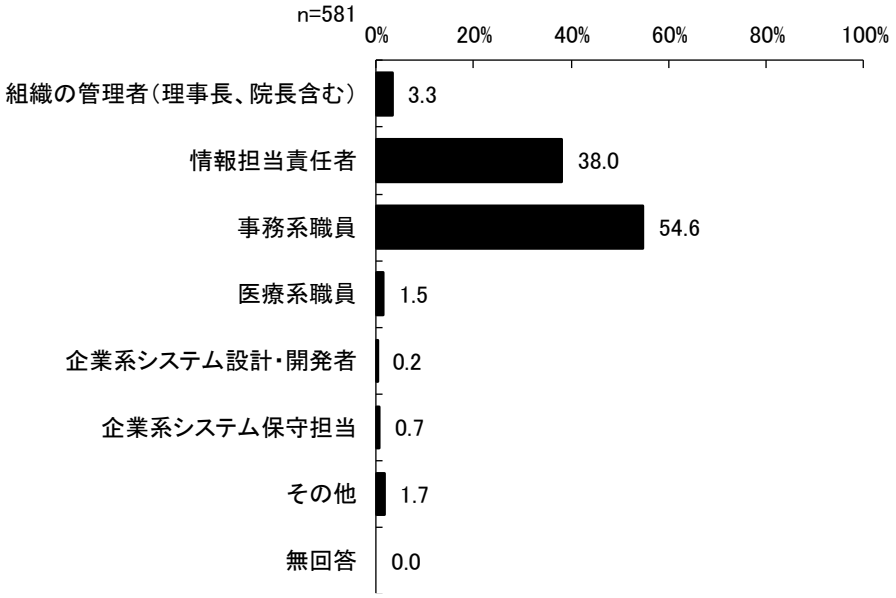


※「その他」の主な回答は以下の通り。
- オーダリングシステム
- オンラインセカンドオピニオン
- リモート面会
- 医事会計
- 医療情報共有システム
- 画像検査 Web 予約システム
- 外注検査受託システム
- 紹介 Web 予約システム
- 地域医療連携システム
- 転院調整システム
- 文書管理システム

8）職場での立場

職場での立場については、事務系職員が 54.6％で最も割合が高く、ついで情報担当責任者が 38.0％であった。

図表 8　職場での立場（Q8）

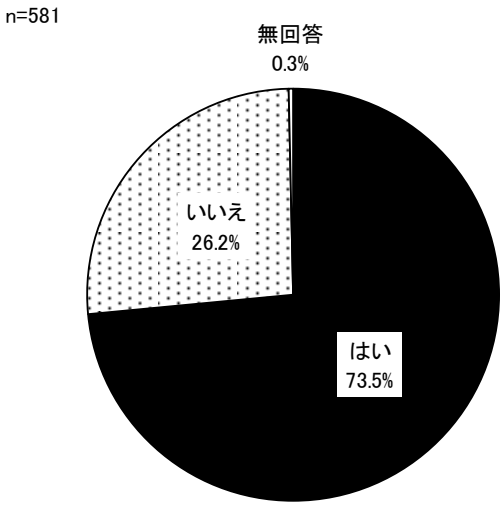


※「その他」の主な回答は以下の通り。
- 医事系部門責任者
- 医療系職員と情報担当の兼務
- 医療情報技師
- 医療情報担当
- 情報システム担当者
- 情報管理係
- 情報担当者

9）情報システムを統括する部署はあるか

情報システムを統括する部署はあるかについては、「はい」が 73.5%であった。

図表 9　情報システムを統括する部署はあるか（Q9）



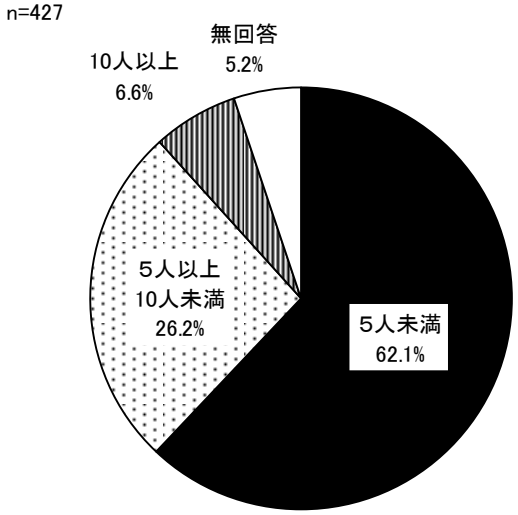
図表 10　情報システムを統括する部署はあるか（Q9）と所属機関（Q5）のクロス集計結果

	調査数	はい	いいえ
医療機関 400床以上の一般病院	171	159	12
	100.0	93.0	7.0
医療機関 200床～399床の一般病院	165	131	34
	100.0	79.4	20.6
医療機関 200床未満の一般病院	222	123	99
	100.0	55.4	44.6
医療機関 一般診療所	1	－	1
	100.0	－	100.0
医療機関 上記以外	16	10	6
	100.0	62.5	37.5
介護機関	5	1	4
	100.0	20.0	80.0
大学(医学系)	8	8	－
	100.0	100.0	－
大学（医学系以外）	4	4	－
	100.0	100.0	－
研究機関	1	1	－
	100.0	100.0	－
行政機関	4	3	1
	100.0	75.0	25.0
医療系企業	－	－	－
	－	－	－
IT企業	1	1	－
	100.0	100.0	－
その他企業	－	－	－
	－	－	－
その他	2	2	－
	100.0	100.0	－

10）情報システムを統括する部署の所属人数

情報システムを統括する部署の所属人数については、5 人未満が 62.1%で最も割合が高く、ついで 5 人以上 10 人未満が 26.2%であった。

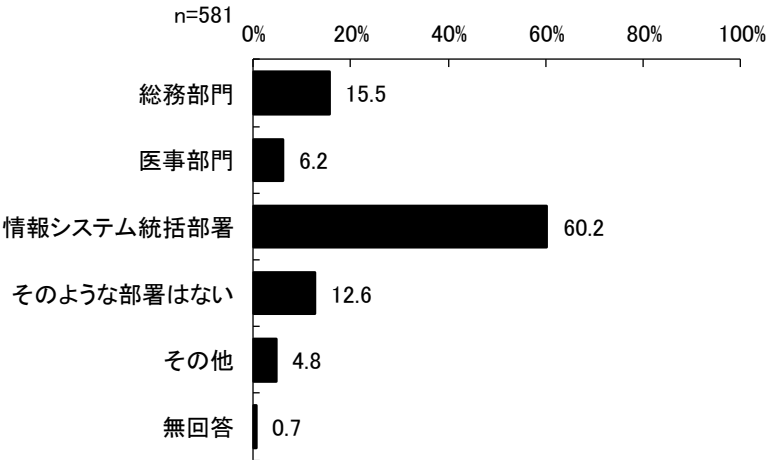
図表 11　情報システムを統括する部署の所属人数（Q10）



11）情報セキュリティ対策を行う担当部署

情報セキュリティ対策を行う担当部署については、情報システム統括部署が 60.2%で最も割合が高く、ついで総務部門が 15.5%であった。

図表 12　情報セキュリティ対策を行う担当部署（Q11）



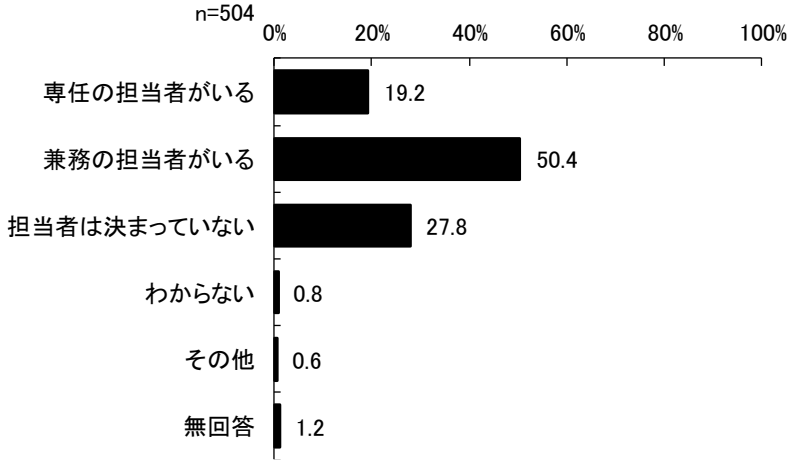
※「その他」の主な回答は以下の通り。

- IT 推進室
- 医事部門と総務部門（電子カルテ系とそれ以外で分かれる）
- 医療情報システム委員会
- 会計課
- 管理課
- 企画管理課
- 企画情報課
- 企画部門
- 経営課
- 経営企画課、経営企画室
- 経営企画情報課
- 施設課
- 事務部の情報システム課
- 事務部門
- 情報システムを統括する部署の人間が行っている
- 情報セキュリティ委員会
- 診療情報管理
- 診療情報管理部門
- 総務部門と情報システム部署
- 統括部署ではない「システム委員会」

12）情報セキュリティの担当部署がある場合における情報セキュリティ担当者の有無

情報セキュリティの担当部署がある場合における情報セキュリティ担当者の有無については、「兼務の担当者がいる」が 50.4%で最も割合が高く、ついで「担当者は決まっていない」が 27.8%であった。

図表 13　情報セキュリティの担当部署がある場合における情報セキュリティ担当者の有無（Q12）



※「その他」の主な回答は以下の通り。
・各部署にセキュリティ管理担当者を配置
・非常勤顧問

13）情報セキュリティ担当者の常勤の専任者の人数

情報セキュリティ担当者の常勤の専任者の平均人数は、2.28 人であった。

図表 14　情報セキュリティ担当者の常勤の専任者の人数（Q13）

（人）

	n数	平均値	標準偏差	中央値	最小値	最大値
常勤の専従者(今年度)	96	2.28	1.75	2.00	0.00	9.00
常勤の専従者(昨年度)	4	1.50	0.50	1.50	1.00	2.00

14）情報セキュリティ担当者の常勤の兼務者の人数

情報セキュリティ担当者の常勤の兼務者の平均人数は、1.97 人であった。

図表 15　情報セキュリティ担当者の常勤の兼務者の人数（Q14）

（人）

	調査数	平均値	標準偏差	中央値	最小値	最大値
常勤の兼務者(今年度)	247	1.97	1.76	2.00	0.00	18.00
常勤の兼務者(昨年度)	10	2.80	2.36	2.00	1.00	9.00

15）情報セキュリティ担当者の非常勤の専任者の人数

情報セキュリティ担当者の非常勤の専任者の平均人数は、0.22 人であった。

図表 16　情報セキュリティ担当者の非常勤の専任者の人数（Q15）

（人）

	調査数	平均値	標準偏差	中央値	最小値	最大値
非常勤の専従者(今年度)	58	0.22	0.59	0.00	0.00	3.00
非常勤の専従者(昨年度)	3	2.00	2.16	1.00	0.00	5.00

16）情報セキュリティ担当者の非常勤の兼務者の人数

情報セキュリティ担当者の非常勤の兼務者の平均人数は、0.2 人であった。

図表 17　情報セキュリティ担当者の非常勤の兼務者の人数（Q16）

（人）

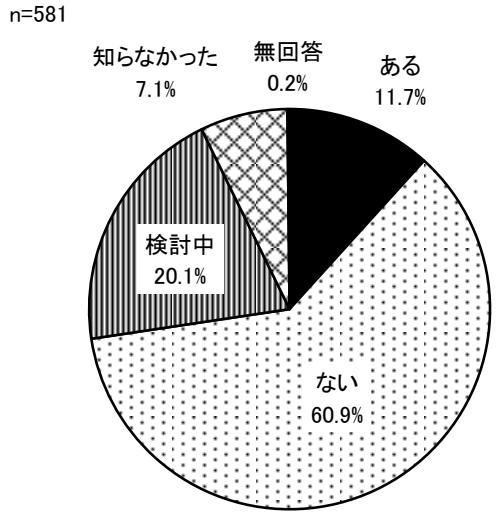
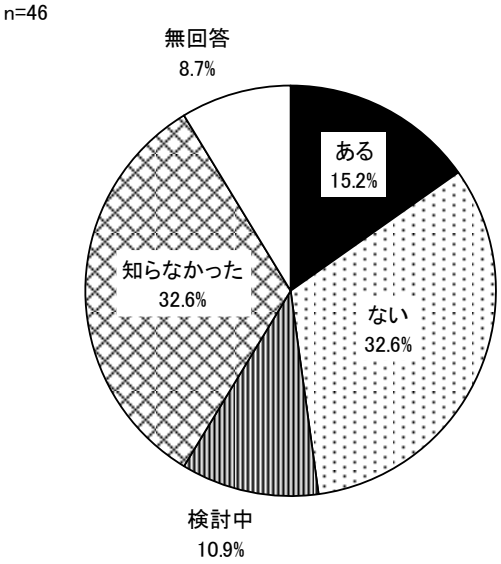
	調査数	平均値	標準偏差	中央値	最小値	最大値
非常勤の兼務者(今年度)	133	0.2	0.74	0.00	0.00	7.00
非常勤の兼務者(昨年度)	6	0.17	0.37	0.00	0.00	1.00

17）所属する組織にCSIRTはあるか

所属する組織に「医療情報システムの安全管理ガイドライン」にある CSIRT※はあるかについては、「ない」が 60.9%で最も割合が高く、ついで「検討中」が 20.1%であった。

※Computer Security Incident Response Team＝セキュリティインシデント発生時に対応する専門チーム

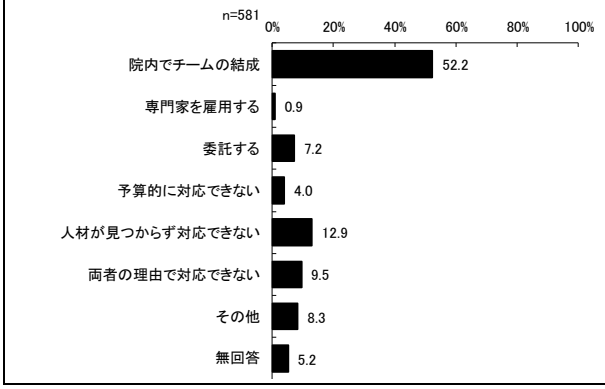
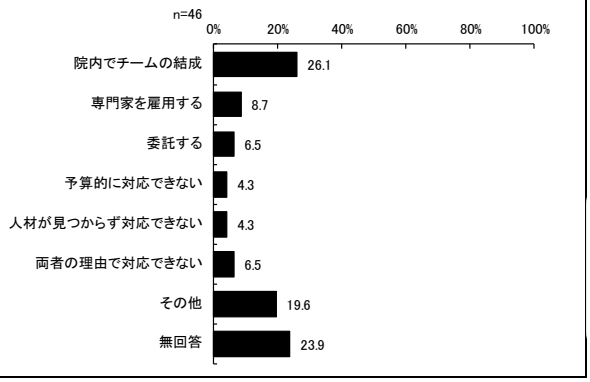
図表 18　所属する組織にCSIRTはあるか（Q17）

今年度（日本病院会）調査結果	昨年度（令和3年度）（日本遠隔医療学会）調査結果
	

18）CSIRT を組織化する場合どのように作るか

CSIRT を組織化する場合どのように作るかについては、「院内でチームの結成」が 52.2%で最も割合が高かった。

図表 19　CSIRT を組織化する場合どのように作るか（Q18）

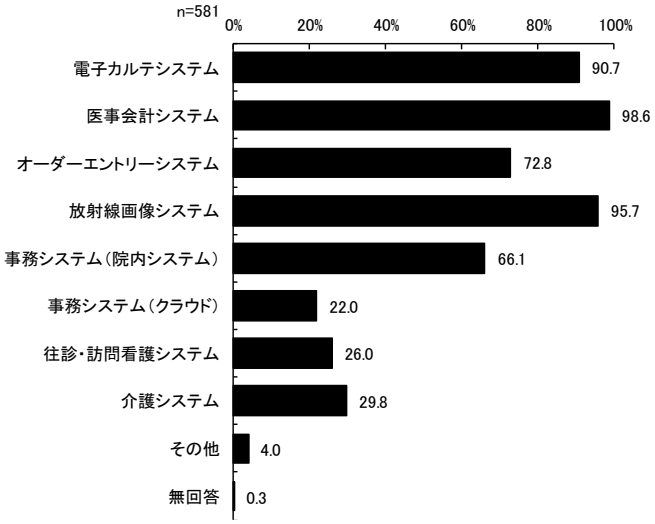
今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

※「その他」の主な回答は以下の通り。
・院内＋外注
・院内でチームを結成する及び外部専門家を招聘（委託）
・院内で検討する
・機構本部が主体で構築
・上位組織の指導のもと
・病院だけでなく、法人全体での組織を運営している
・市の情報政策課の協力を得て、チームを結成
・情報担当部署にてチームの結成
・大学側に設置されており、病院側では詳細は把握なし

19）導入している情報システム

導入している情報システムについては、医事会計システムが 98.6%、放射線画像システムが 95.7%であった。

図表 20　導入している情報システム（Q19）【複数回答】

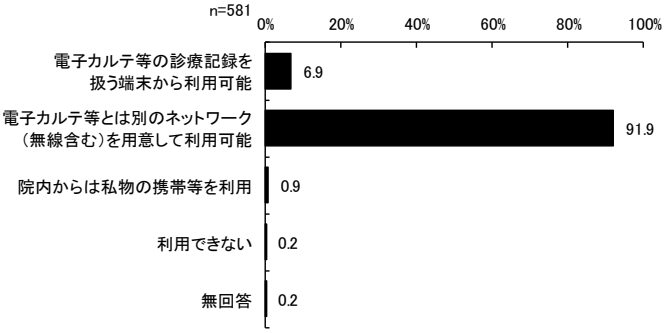


※「その他」の主な回答は以下の通り。
・医療情報部門系システムが多数
・遠隔読影システム
・患者向けスマートフォン用アプリケーション
・給食システム
・健診システム
・検査システム
・検体検査システム
・材料管理
・歯科技工
・手術部門システム
・生理検査システム
・地域医療連携に関するシステム
・調剤管理システム
・透析システム
・入退室管理システム
・病歴管理システム等
・予約管理
・臨床検査

20）院内における職員のインターネットの利用可否

院内における職員のインターネットの利用可否については、「電子カルテ等とは別のネットワーク（無線含む）を用意して利用可能」が 91.9%で最も割合が高かった。

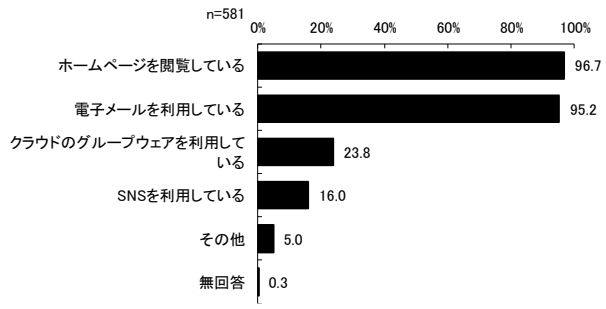
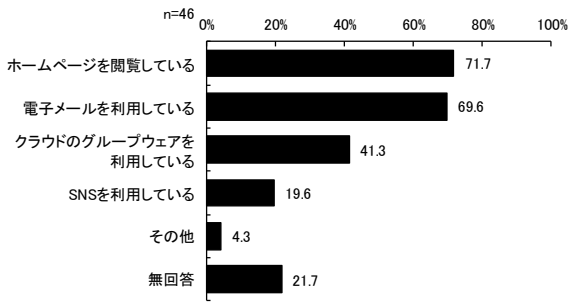
図表 21　院内における職員のインターネットの利用可否（Q20）



21）院内からインターネットで利用しているサービス

院内からインターネットで利用しているサービスについては、「ホームページを閲覧している」が 96.7%で最も割合が高く、ついで「電子メールを利用している」が 95.2%であった。

図表 22　院内からインターネットで利用しているサービス（Q21）【複数回答】

今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

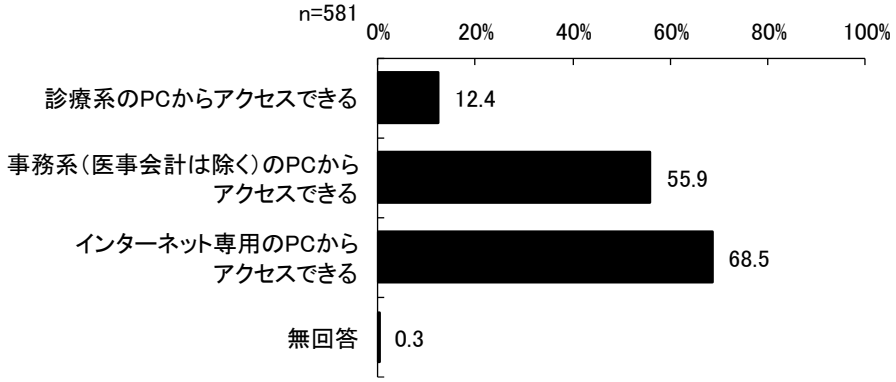
※「その他」の主な回答は以下の通り。
・NCD 登録等
・Office365
・SNS に関しては病院情報公開用アカウント
・UTM で防御されるもの以外は特にフィルタしていない
・WEB 会議
・オンプレのグループウェアを利用している
・オンライン講習等の受講
・クラウドの業務システムを利用（訪問・居宅）
・レセプトデータの送信、健康保険証のオンライン資格確認
・医薬品発注

・医療に関する情報検索、購入機器情報検索等
・院内ファイルサーバへのアクセス
・遠隔読影、遠隔画像参照
・各種クラウドサービス（税申請、国や県への報告など）
・学会等のデータ登録
・看護や専門部署の、関連する団体等のサイトを閲覧
・勤怠システムを利用している
・事務系システム（クラウド）
・人事・財務、地域連携、統計、入退院支援クラウド

22）インターネットにアクセスできるパソコン（PC）

インターネットにアクセスできるパソコン（PC）については、「インターネット専用のPCからアクセスできる」が68.5%で最も割合が高く、ついで「事務系（医事会計は除く）のPCからアクセスできる」が55.9%であった。

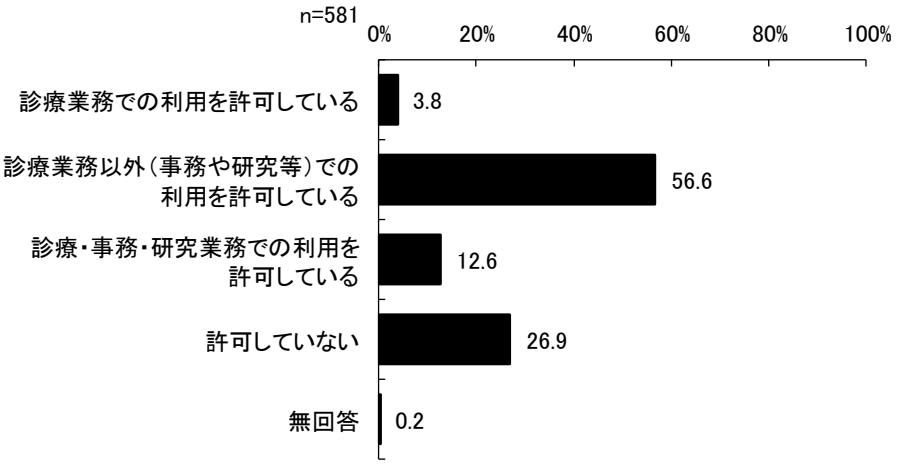
図表23　インターネットにアクセスできるパソコン（PC）について（Q22）【複数回答】



23）職員（医師など）の私物のPCを用いて業務を行うことを許可しているか

職員（医師など）の私物のPCを用いて業務を行うことを許可しているかについては、「診療業務以外（事務や研究等）での利用を許可している」が56.6%で最も割合が高く、ついで「許可していない」が26.9%であった。

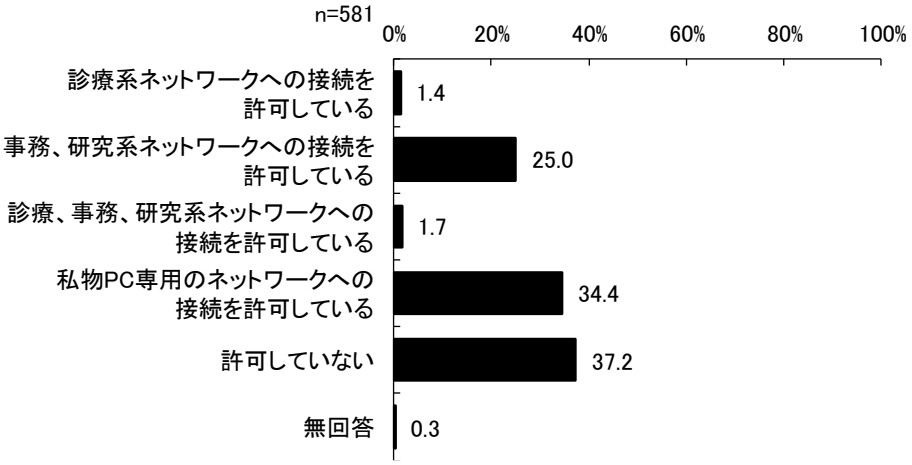
図表24　職員（医師など）の私物のPCを用いて業務を行うことを許可しているか（Q23）



24）職員の私物の PC のネットワーク接続を許可しているか

職員の私物の PC のネットワーク接続を許可しているかについては、「許可していない」が 37.2%で最も割合が高く、ついで「私物 PC 専用のネットワークへの接続を許可している」が 34.4%であった。

図表 25　職員の私物の PC のネットワーク接続を許可しているか（Q24）

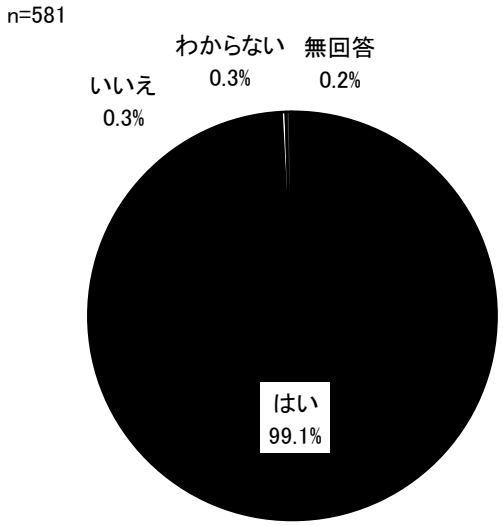


(2)組織で実施しているセキュリティ対策

1) ウイルス対策ソフトを導入しているか

ウイルス対策ソフトを導入しているかについては、「はい」が 99.1%で最も割合が高かった。

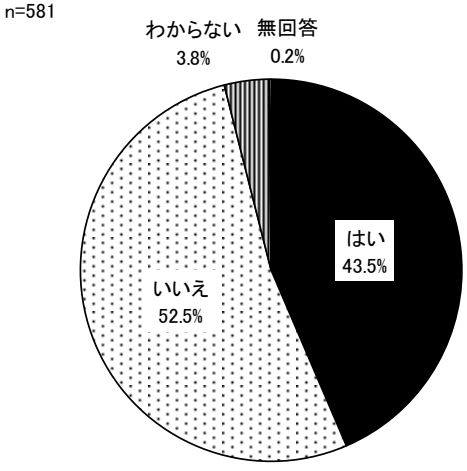
図表 26　ウイルス対策ソフトを導入しているか（Q25）



2) 資産管理ソフトを導入しているか

資産管理ソフトを導入しているかについては、「はい」が 43.5%であった。

図表 27　資産管理ソフトを導入しているか（Q26）



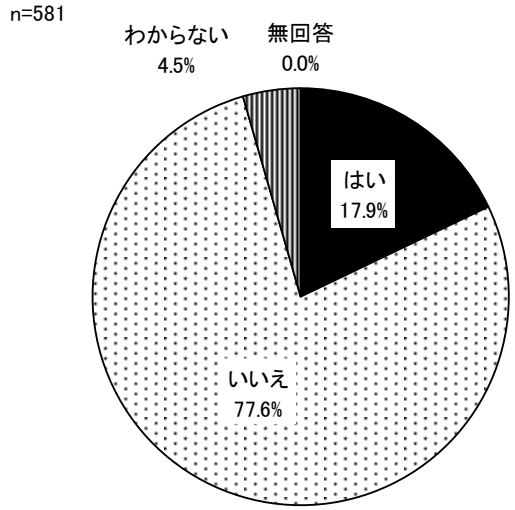
図表 28　資産管理ソフトを導入しているか（Q26）と所属機関（Q5）のクロス集計結果

	調査数	はい	いいえ	わからない
医療機関 400床以上の一般病院	172	113	55	4
	100.0	65.7	32.0	2.3
医療機関 200床～399床の一般病院	164	78	78	8
	100.0	47.6	47.6	4.9
医療機関 200床未満の一般病院	222	57	157	8
	100.0	25.7	70.7	3.6
医療機関 一般診療所	1	－	－	1
	100.0	－	－	100.0
医療機関 上記以外	16	3	12	1
	100.0	18.8	75.0	6.3
介護機関	5	1	4	－
	100.0	20.0	80.0	－
大学(医学系)	9	5	4	－
	100.0	55.6	44.4	－
大学（医学系以外）	4	－	4	－
	100.0	－	100.0	－
研究機関	1	－	1	－
	100.0	－	100.0	－
行政機関	4	4	－	－
	100.0	100.0	－	－
医療系企業	－	－	－	－
	－	－	－	－
IT企業	1	－	1	－
	100.0	－	100.0	－
その他企業	－	－	－	－
	－	－	－	－
その他	2	2	－	－
	100.0	100.0	－	－

3）仮想ブラウザを導入しているか

仮想ブラウザを導入しているかについては、「いいえ」が 77.6%で最も割合が高かった。

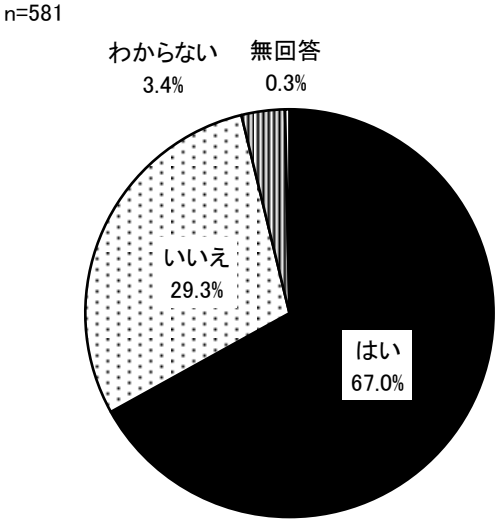
図表 29　仮想ブラウザを導入しているか（Q27）



4）セキュリティ教育を行っているか

セキュリティ教育を行っているかについては、「はい」が 67.0%で最も割合が高く、ついで「いいえ」が 29.3%であった。

図表 30　セキュリティ教育を行っているか（Q28）



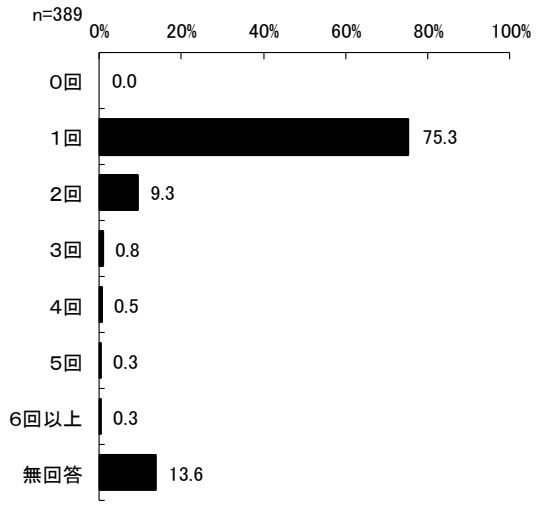
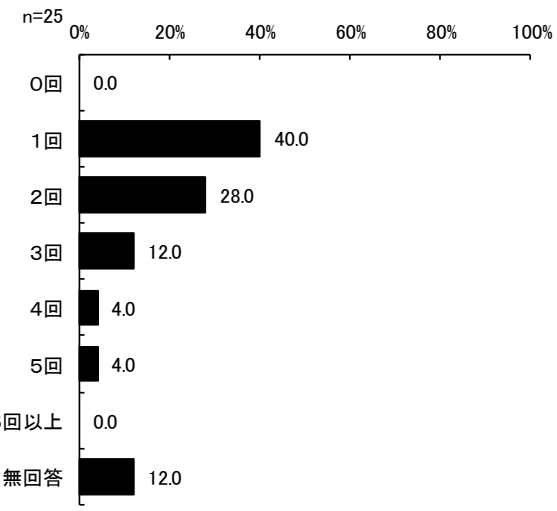
図表 31　セキュリティ教育を行っているか（Q28）と所属機関（Q5）のクロス集計結果

	調査数	はい	いいえ	わからない
医療機関 400床以上の一般病院	172	140	29	3
	100.0	81.4	16.9	1.7
医療機関 200床～399床の一般病院	165	107	53	5
	100.0	64.8	32.1	3.0
医療機関 200床未満の一般病院	220	131	80	9
	100.0	59.5	36.4	4.1
医療機関 一般診療所	1	－	1	－
	100.0	－	100.0	－
医療機関 上記以外	16	7	6	3
	100.0	43.8	37.5	18.8
介護機関	5	2	3	－
	100.0	40.0	60.0	－
大学(医学系)	9	6	3	－
	100.0	66.7	33.3	－
大学（医学系以外）	4	4	－	－
	100.0	100.0	－	－
研究機関	1	1	－	－
	100.0	100.0	－	－
行政機関	4	4	－	－
	100.0	100.0	－	－
医療系企業	－	－	－	－
	－	－	－	－
IT企業	1	1	－	－
	100.0	100.0	－	－
その他企業	－	－	－	－
	－	－	－	－
その他	2	2	－	－
	100.0	100.0	－	－

5）セキュリティ教育は年に何回行っているか

セキュリティ教育は年に何回行っているかについては、1 回が 75.3%で最も割合が高く、ついで 2 回が 9.3%であった。

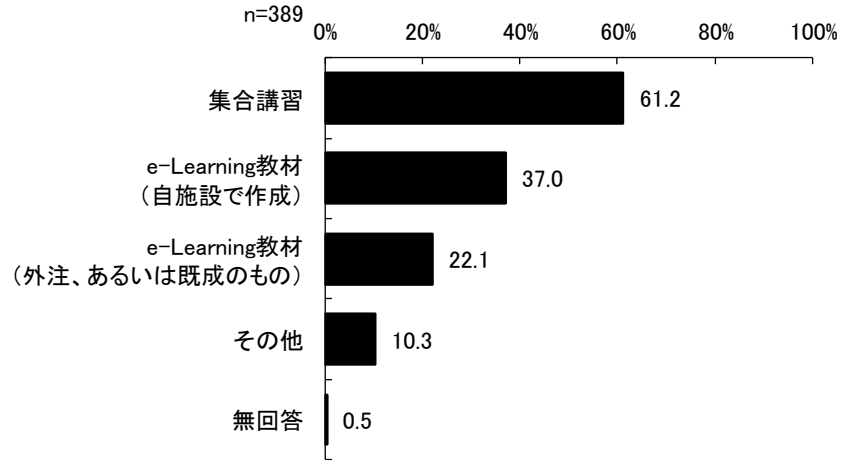
図表 32　セキュリティ教育は年に何回行っているか（Q29）

今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

6）セキュリティ教育のためにどのような研修を行っているか

セキュリティ教育のためにどのような研修を行っているかについては、集合研修が61.2%で最も割合が高く、ついでe-Learning教材（自施設で作成）37.0%であった。

図表33　セキュリティ教育のためにどのような研修を行っているか（Q30）【複数回答】

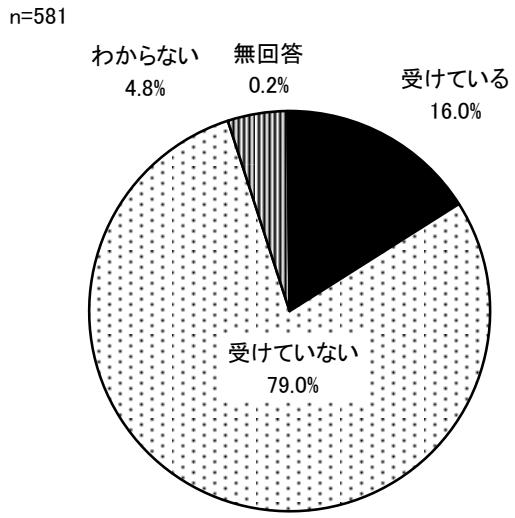
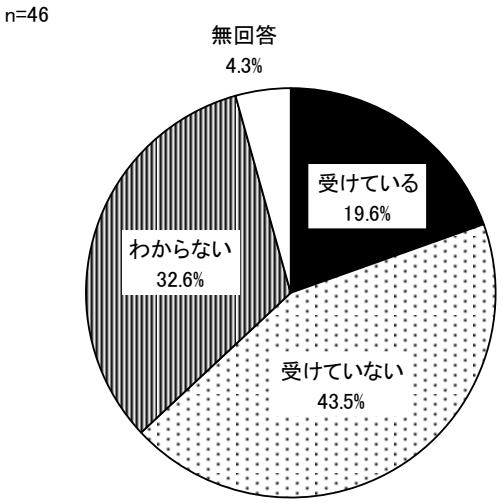


※「その他」の主な回答は以下の通り。
・DVDを各部署に配布
・e-Learning（自施設作成と外注のハイブリッド）
・e-Learning教材（本部が作成）
・WEB動画
・WEB配信形式
・イントラネット内メールと添付ファイル
・コロナ禍のため資料掲載
・ニュース発行
・グループウェアでの院内資料配布
・メールなどによる模擬訓練等
・院内メールで事例共有
・院内メッセンジャーを使った、自己作成コンテンツ
・会議資料
・会議等で口頭説明
・研修資料配布と理解度テスト
・個人での研修動画視聴による研修
・厚生労働省が作成している医療機関等向けサイバーセキュリティ研修
・厚生労働省作成の研修素材
・厚労省の情報セキュリティのYoutube
・資料を院内掲示版へ掲示
・資料配布と理解度テスト
・資料配布や動画研修
・自施設作成のものをWEBにて閲覧
・所属長が研修後、部下へ伝達研修実施
・情報系委員会などでの啓蒙活動
・新規入職者に対して、外部デバイス取り扱いなど
・新人研修
・新人職員に対して行う
・通常は集合講習、現在は資料通知
・入職研修時に実施

7）外部セキュリティ監査を受けているか（直近 3 年以内の状況）

外部セキュリティ監査を受けているか（直近 3 年以内の状況）については、「受けていない」が 79.0%で最も割合が高かった。

図表 34　外部セキュリティ監査を受けているか（直近 3 年以内の状況）（Q31）

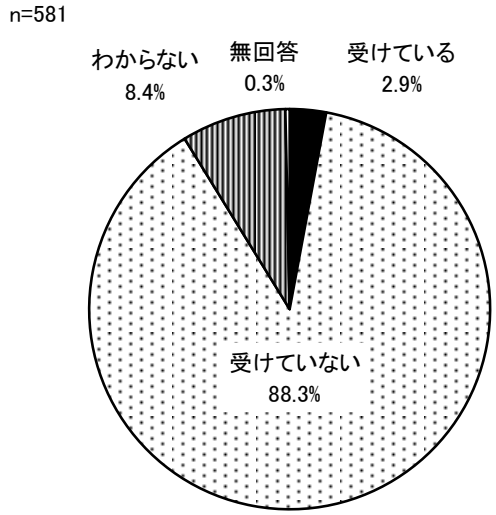
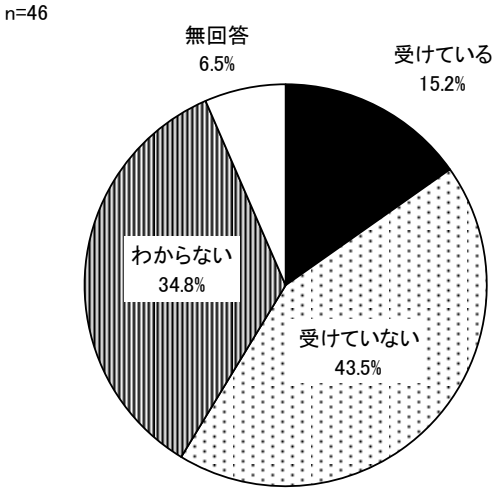
今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

8）ペネトレーションテストを受けているか（直近 3 年以内の状況）

ペネトレーションテスト※を受けているか（直近 3 年以内の状況）については、「受けていない」が 88.3%で最も割合が高かった。

※インターネット接続を通じた施設内ネットワークへの侵入テスト

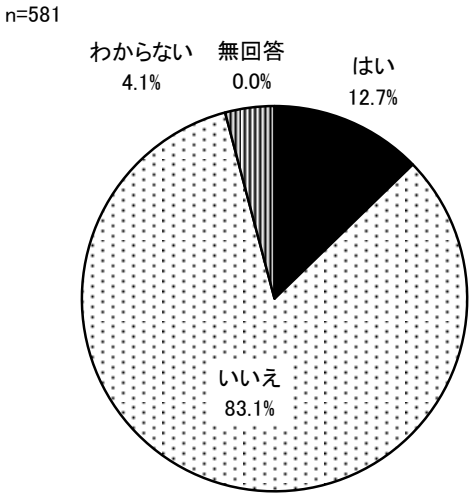
図表 35　ペネトレーションテストを受けているか（直近 3 年以内の状況）（Q32）

今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

9）セキュリティ訓練を実施しているか（直近 3 年以内の状況）

セキュリティ訓練を実施しているか（直近 3 年以内の状況）については、「いいえ」が 83.1%で最も割合が高かった。

図表 36　セキュリティ訓練を実施しているか（直近 3 年以内の状況）（Q33）

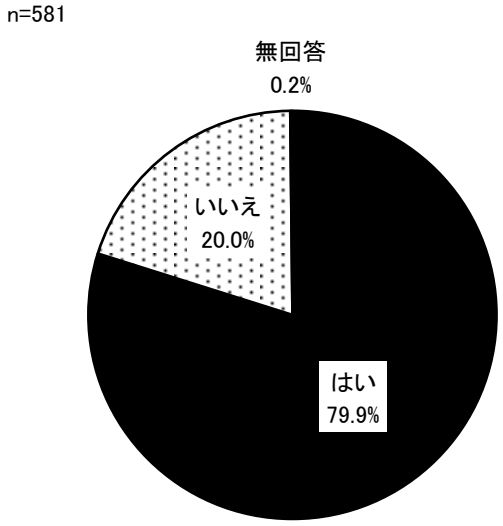


（3）施設内での規定の有無等

1）情報セキュリティポリシーを規定しているか

情報セキュリティポリシーを規定しているかについては、「はい」が 79.9%であった。

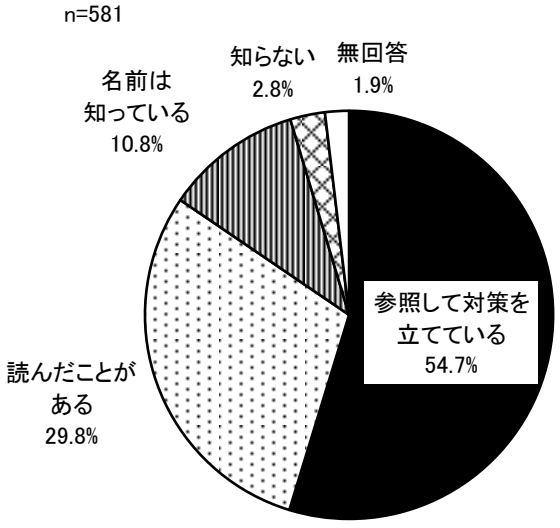
図表 37　情報セキュリティポリシーを規定しているか（Q34）



2）厚生労働省の「医療情報システムの安全管理に関するガイドライン」の認知状況等

厚生労働省の「医療情報システムの安全管理に関するガイドライン」の認知状況等については、「参照して対策を立てている」が 54.7%で最も割合が高く、ついで「読んだことがある」が 29.8%であった。

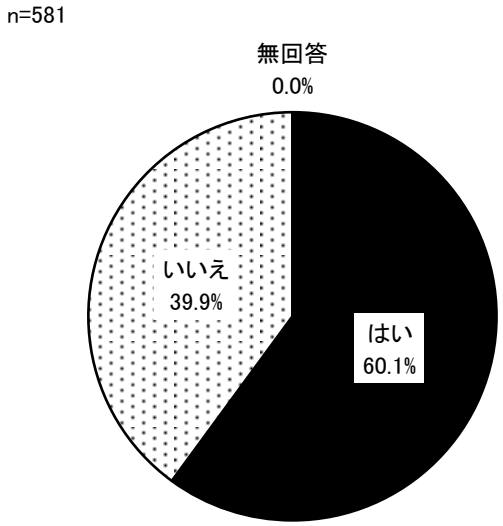
図表 38　厚生労働省の「医療情報システムの安全管理に関するガイドライン」の認知状況等（Q35）



3）セキュリティインシデント発生時の手順が定められているか

セキュリティインシデント発生時の手順が定められているかについては、「はい」が60.1%であった。

図表 39　セキュリティインシデント発生時の手順が定められているか（Q36）



図表 40　セキュリティインシデント発生時の手順が定められているか（Q36）と所属機関（Q5）のクロス集計結果

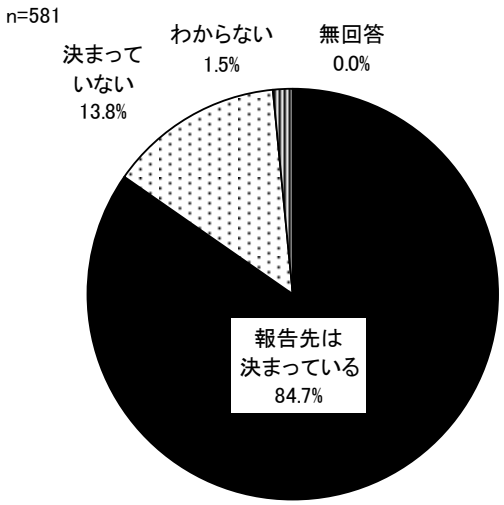
	調査数	はい	いいえ
医療機関 400床以上の一般病院	172	128	44
	100.0	74.4	25.6
医療機関 200床～399床の一般病院	165	93	72
	100.0	56.4	43.6
医療機関 200床未満の一般病院	222	118	104
	100.0	53.2	46.8
医療機関 一般診療所	1	－	1
	100.0	－	100.0
医療機関 上記以外	16	6	10
	100.0	37.5	62.5
介護機関	5	3	2
	100.0	60.0	40.0
大学(医学系)	9	7	2
	100.0	77.8	22.2
大学（医学系以外）	4	4	－
	100.0	100.0	－
研究機関	1	1	－
	100.0	100.0	－
行政機関	4	3	1
	100.0	75.0	25.0
医療系企業	－	－	－
	－	－	－
IT企業	1	1	－
	100.0	100.0	－
その他企業	－	－	－
	－	－	－
その他	2	2	－
	100.0	100.0	－

（4）セキュリティインシデント発生時の対応

1）職員がセキュリティインシデントを発見したときに報告する部署が決まっているか

職員がセキュリティインシデントを発見したときに報告する部署が決まっているかについては、「報告先は決まっている」が 84.7%で最も割合が高く、ついで「決まっていない」が 13.8%であった。

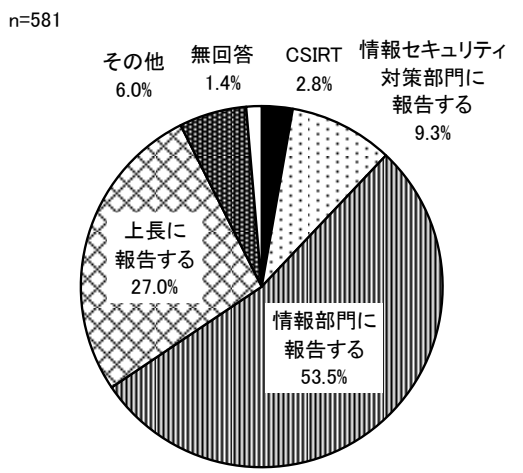
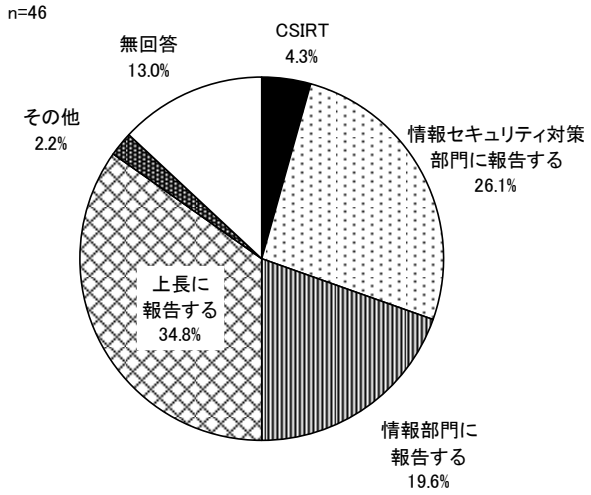
図表 41　職員がセキュリティインシデントを発見したときに報告する部署が決まっているか（Q37）



2）情報セキュリティインシデント発生時における報告先

情報セキュリティインシデント発生時における報告先については、「情報部門に報告する」が 53.5%で最も割合が高く、ついで「上長に報告する」が 27.0%であった。

図表 42　情報セキュリティインシデント発生時における報告先（Q38）

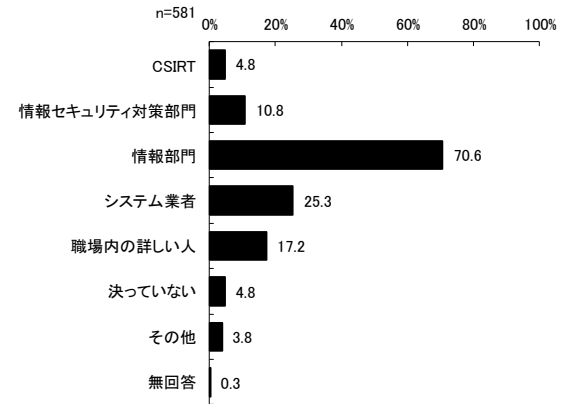
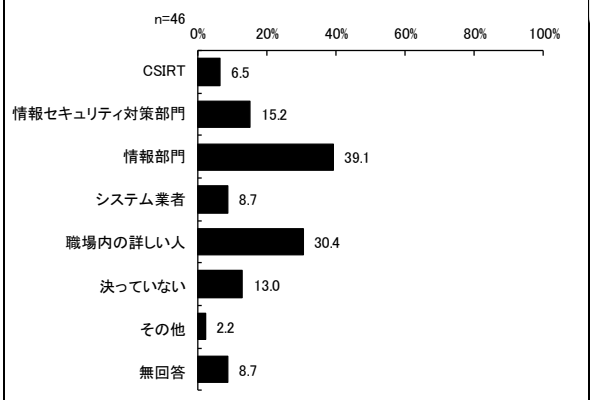
今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

※「その他」の主な回答は以下の通り。
・ケースによる
・システム管理者
・システム担当者
・セキュリティ責任者
・まず院内の上長に報告し、本部 CSIRT へ報告
・一旦、医療安全管理課に報告する
・院長（情報システム管理者）
・契約先 IT 企業
・経営幹部
・上長、個人情報管理者、切り分けしフローチャートに則って報告
・事務長
・上位組織の情報セキュリティ対策室
・上長、情報部門、安全管理室
・上長および連絡網あり
・上長と総務課
・上長に報告の上、システム担当へ報告
・上長に報告後、上長より総務課長へ報告する
・情報担当者に報告する
・情報部門と上長に報告
・総務課
・総務課システム担当
・総務課職員
・総務部門
・法人本部
・決まっていない

3）情報セキュリティに関する職員の相談先（組織内）

情報セキュリティに関する職員の相談先（組織内）については、情報部門が 70.6%で最も割合が高く、ついでシステム業者が 25.3%であった。

図表 43　情報セキュリティに関する職員の相談先（組織内）（Q39）【複数回答】

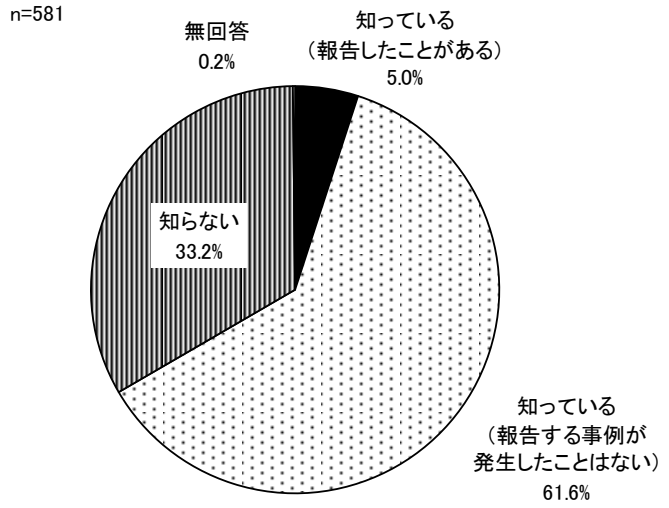
今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

※「その他」の主な回答は以下の通り。
・事務部門
・システム担当者
・企画情報課
・事務責任者
・社内（病院外）情報システム部門
・情報システム担当者へ報告
・総務担当
・同一法人別病院のシステム係
・法人本部 ICT 推進センター
・診療情報管理室
・総務課・電子カルテチーム
・総務課職員
・総務課内のシステム担当者
・電算担当（兼務）
・有資格契約アドバイザー

4）情報セキュリティインシデント発生時の厚生労働省の窓口を知っているか

情報セキュリティインシデント発生時の厚生労働省の窓口を知っているかについては、「知っている（報告する事例が発生したことはない)」が 61.6%で最も割合が高く、ついで「知らない」が 33.2%であった。

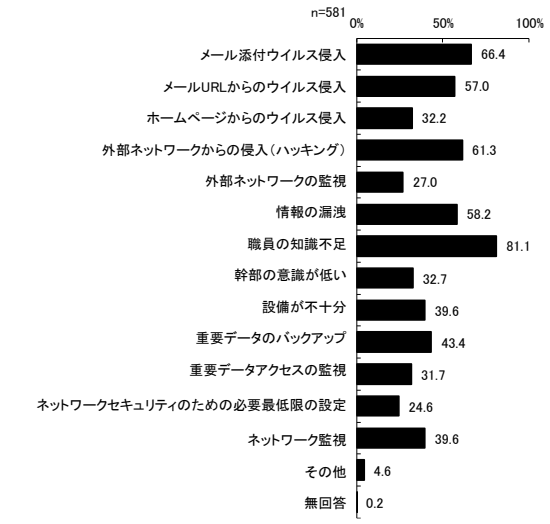
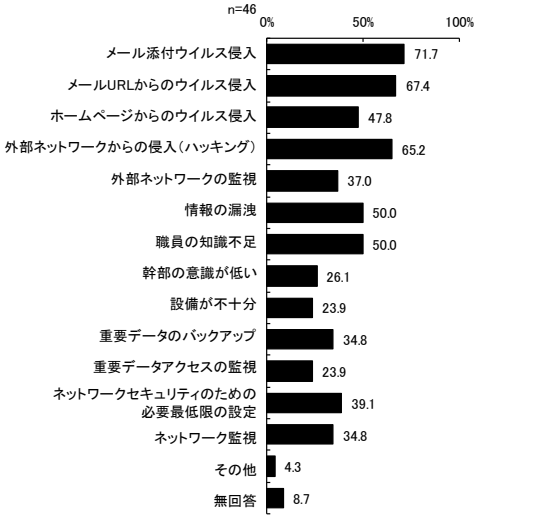
図表 44　情報セキュリティインシデント発生時の厚生労働省の窓口を知っているか（Q40）



5）所属機関のサイバーセキュリティの課題

所属機関のサイバーセキュリティの課題については、「職員の知識不足」が 81.1％で最も割合が高く、ついで「メール添付ウイルス侵入」が 66.4％であった。

図表 45　所属機関のサイバーセキュリティの課題（Q41）【複数回答】

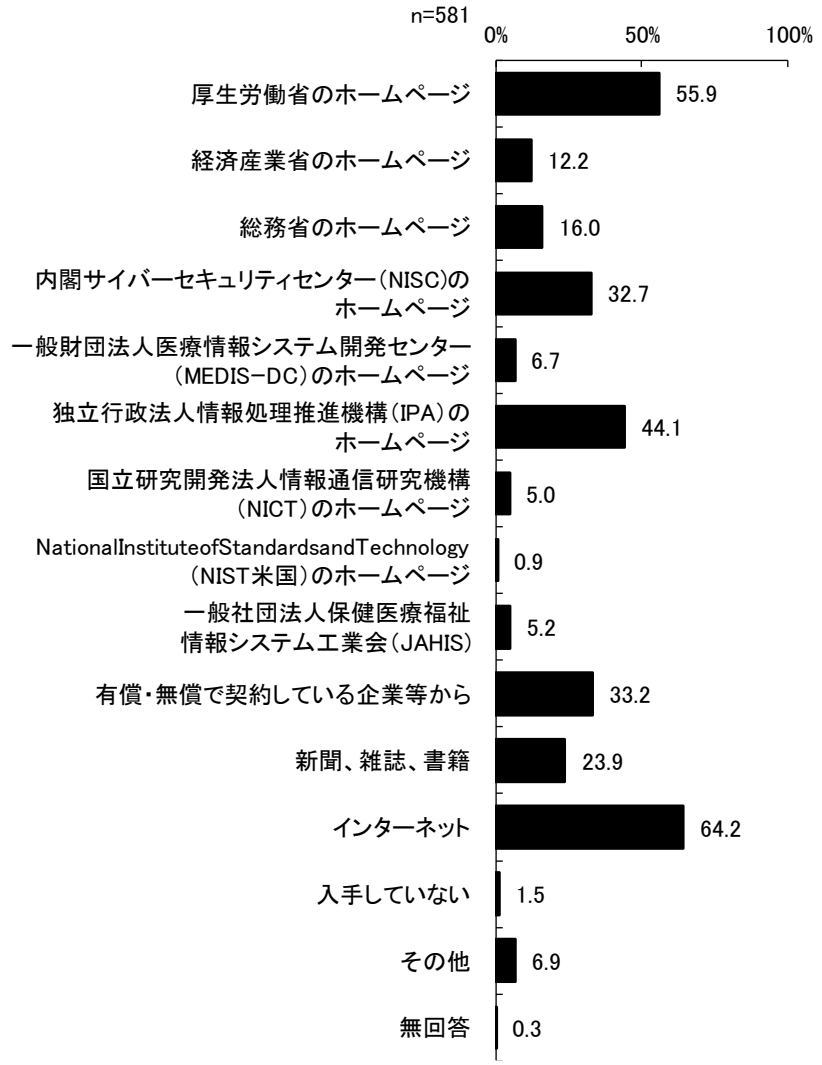
今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

※「その他」の主な回答は以下の通り。
・PPAP
・ICT 利用上、必須な保守契約を結んでいないケースが多々ある
・IT に対応するポジションの職員が専門職ではなく普通の事務職、医療機器に対するセキュリティ対策が部門任せになっている。
・BCP プランがない
・USB メモリ等記録媒体の管理徹底
・USB メモリ等による診療情報持ち出しの体制整備
・外部記憶装置（USB 等）からのウイルス感染
・私物の USB 使用
・インターネット系の SKYSEA の導入（イントラ系は導入済み）
・ウイルス対策ソフトで対応できなかったウイルス侵入の脅威。既存通信網の整理
・ウイルス対策ソフトの検疫を突破したウイスルの脅威
・ハードウェア全般の老朽化
・リモートアクセスのセキュリティ
・リモートメンテナンス用ネットワークの脆弱性の有無
・可搬記録媒体の接続設定
・患者紹介等で持ち込まれる情報・記憶媒体、研究・教育用データのセキュリティ管理
・個人 PC 端末のセキュリティ対策
・最低限の設備の基準の不透明とそれに掛るコスト
・情シス部門のセキュリティ知識向上
・情報システム部門の設置
・人材不足
・担当職員数不足、統括部署が無いこと
・対策をするとなった場合に多額の費用が発生すること
・必要な予算を確保できない

6）情報セキュリティに関する情報源

情報セキュリティに関する情報源については、インターネットが 64.2%で最も割合が高く、ついで厚生労働省のホームページが 55.9%であった。

図表 46　情報セキュリティに関する情報源（Q42）【複数回答（3 つまで）】



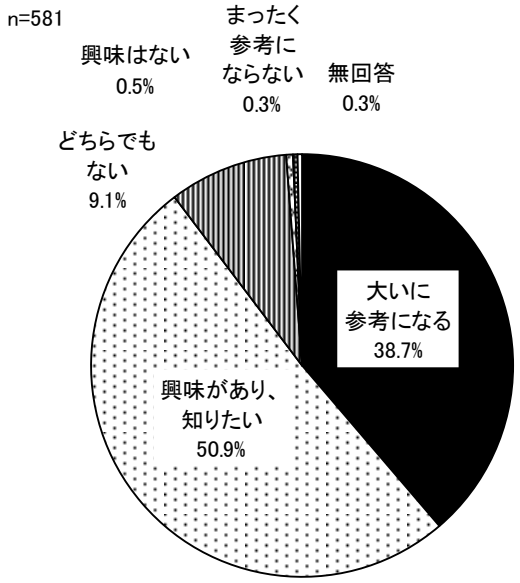
※「その他」の主な回答は以下の通り。
・本部からの情報
・JPCERT のホームページ
・システム業者
・システム提供業者
・セキュリティ関連会社からの情報提供
・医療 ISAC
・医療系の雑誌
・医療情報技師会
・一般社団法人日本病院会
・都道府県の警察公安課サイバー攻撃対策係
・加入団体からの情報提供
・各種セミナー

・業者
・警察署
・警視庁
・研修会
・県庁や病院局からの情報提供
・私立医科大学協会
・社内（病院外）情報システム部門
・所属している医療団体等からの情報
・脆弱性対策情報データベース
・他グループ病院の人脈
・他医療機関との情報共有
・地元警察署
・適切な時期に上記複数から情報を得ている
・電子カルテベンダー
・日本医療情報学会
・保守ベンダーから情報提供 10
・法人本部 ICT 推進センターからの通知
・本部より

7）他の施設の対策状況は対策を立てる上で参考になるか

他の施設の対策状況は対策を立てる上で参考になるかについては、「興味があり、知りたい」が 50.9%で最も割合が高く、ついで「大いに参考になる」が 38.7%であった。

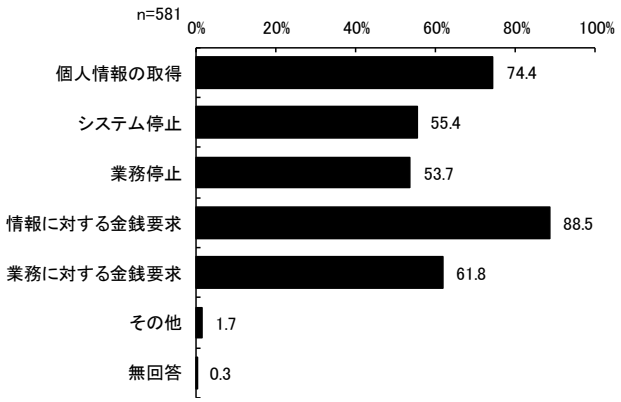
図表 47　他の施設の対策状況は対策を立てる上で参考になるか（Q43）



8）最近のサイバーテロの目的

最近のサイバーテロの目的については、情報に対する金銭要求が 88.5%で最も割合が高く、ついで個人情報の取得が 74.4%であった。

図表 48　最近のサイバーテロの目的（Q44）【複数回答】

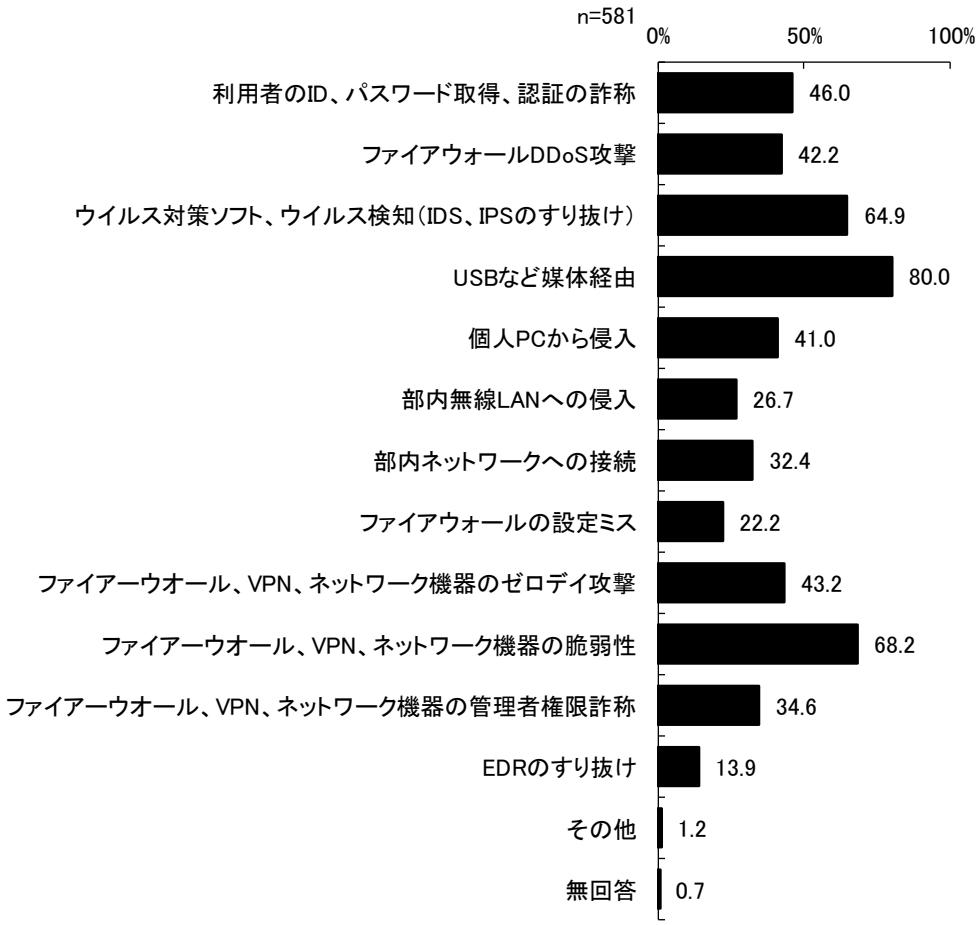


※「その他」の主な回答は以下の通り。業務停止による社会不安醸成
・国家間テロ、国家間戦争
・社会的信用の失墜
・敵性国家の生産性低下
・愉快犯

9）どのようなサーバー攻撃方法の侵入経路を想定しているか

どのようなサーバー攻撃方法の侵入経路を想定しているかについては、USB など媒体経由が 80.0%で最も割合が高く、「ファイアーウオール、VPN、ネットワーク機器の脆弱性」が 68.2%であった。

図表 49　どのようなサーバー攻撃方法の侵入経路を想定しているか（Q45）【複数回答】

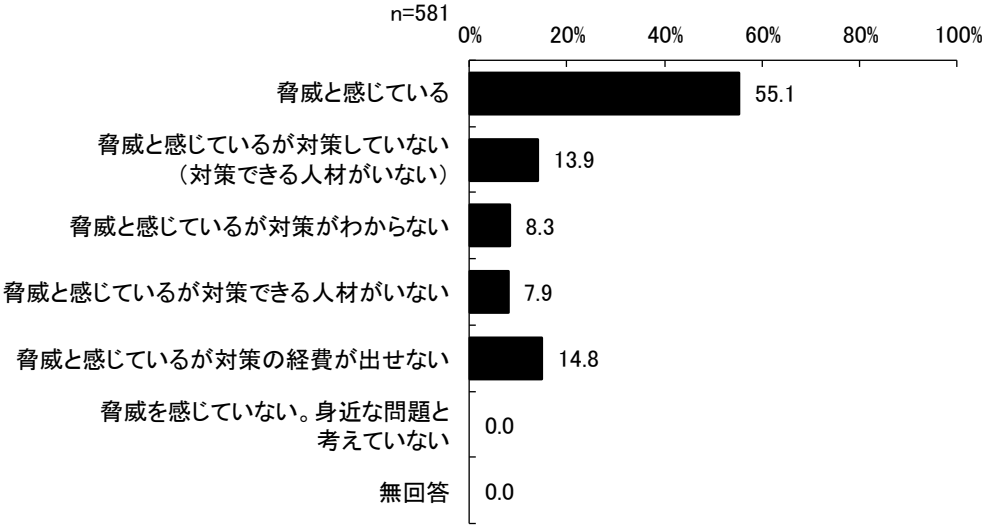


※「その他」の主な回答は以下の通り。
・メールに添付されたウイルスの展開
・サイバー攻撃であれば導入の無い EDR 以外は全てチェックとする
・メール添付ファイルからの端末の RAT 感染からのラテラルムーブメント
・外部公開系サーバのプラットフォーム脆弱性
・リモートメンテナンス環境を踏み台にした侵入
・レガシー機器、アップデートされていない機器からの侵入
・個人 PC から侵入
・悪意ある故意
・職員による規程違反作業による、脆弱性露見、情報漏洩

10）サイバーセキュリティを脅威と感じているか、対策を検討しているか、問題は何か

サイバーセキュリティを脅威と感じているか、対策を検討しているか、問題は何かについては、「脅威と感じている」が 55.1%で最も割合が高かった。

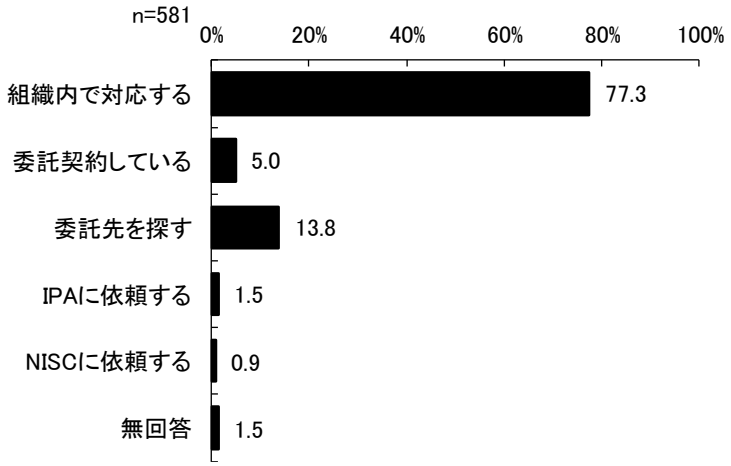
図表 50　サイバーセキュリティを脅威と感じているか、対策を検討しているか、問題は何か（Q46）



11）インシデント発生時の対応について

インシデント発生時の対応については、「組織内で対応する」が 77.3%で最も割合が高かった。

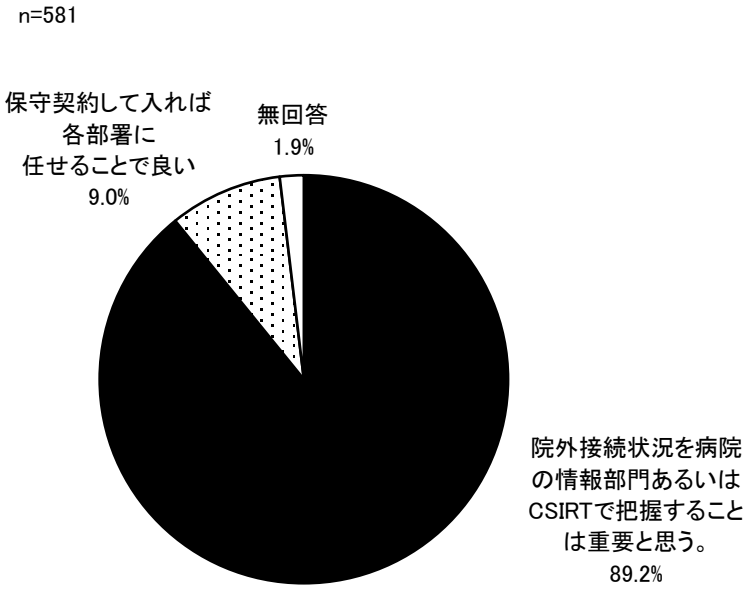
図表 51　インシデント発生時の対応について（Q47）



12）インシデント発生以前の事前調査に対する意識

インシデント発生以前の事前調査に対する意識については、「院外接続状況を病院の情報部門あるいはCSIRTで把握することは重要と思う」が89.2%であった。

図表52　インシデント発生以前の事前調査に対する意識（Q48）

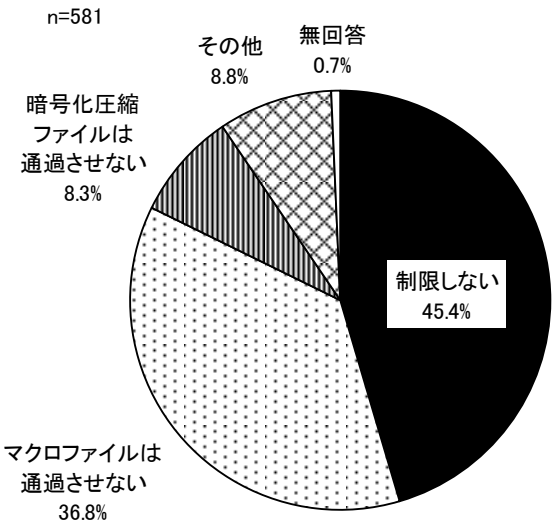


（5）侵入経路の対策として実施している事項等

1）メール添付ファイルに関する対策

メール添付ファイルについては、「制限しない」が 45.4%で最も割合が高く、ついで「マクロファイルは通過させない」が 36.8%であった。

図表 53　メール添付ファイルについて（Q49）



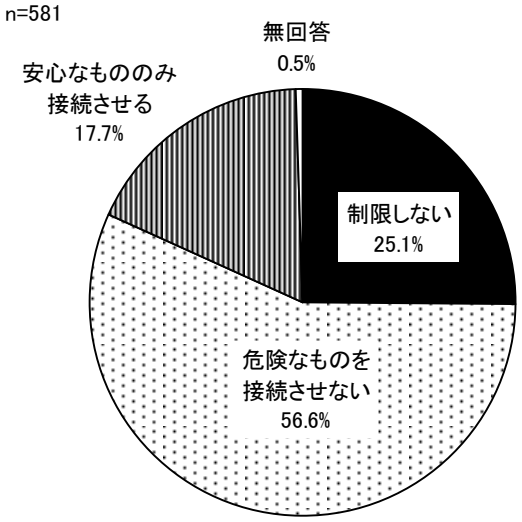
「その他」の主な回答は以下の通り。
・.xls .doc の添付ファイルは削除する
・「.exe」ファイルが添付されたメール及びウィルス対策ソフトでのチェックで不正なファイルと判断されたものは通過させない
・ESET(ウイルス対策ソフトでの制御)
・UTM によるウイルスブロック機能を有している
・Windows 実行ファイル、Windows スクリプトは通過させない
・ウィルスチェック
・ウイルス対策ソフトのセキュリティ設定
・システム部門は制限したいが、業務の都合上、制限出来ない状況
・セキュリティソフトで設定（初期から変更していない）
・ファイアウォールでポートの限定、添付ファイルの容量制限を設けている
・プロバイダのセキュリティチェック
・ヘルプデスクによるデータ移動対応
・メールサーバーのセキュリティ機能による監査
・メールは病院管理ではなく、詳細不明
・メール監視のソフトによるフィルタリング
・圧縮ファイルのみ通過
・圧縮ファイルや URL 付きのメール・フリーアドレスには SPAM と表示させる
・可能な限りスキャンニングやサンドボックスでの検証実施
・外部からのファイルのマクロは無効化し、暗号化圧縮ファイルは送受信を禁止し、WEB ダウンロードなどを使用する。
・外部委託のゲートウェイの設定で危険と判定されたものを通さない
・検疫を実施している
・現在はマクロ・ファイルを弾いているが、弊害が大きい
・古い office ファイルは通過させない
・古いソフト等、セキュリティに問題があるファイルは通さない（本社側で設定されている）
・職員周知

・身に覚えのない添付ファイルは開かない啓蒙
・制限していないがセキュリティソフトを導入している
・制限はしていないがウイルス対策ソフトのフィルタで検疫している
・送信元が確かなもの以外は DL しないようにしている
・対策は実施しているが詳細は他部署管理のため不明
・配信前のウイルスチェックサービスを利用
・不審なメールの添付ファイルは開かないよう周知
・不明な宛先・文字化けは開かない、閲覧ウィンドウ OFF

2）ホームページ閲覧に関する対策

ホームページ閲覧に関する対策については、「危険なものを接続させない」が 56.6%で最も割合が高く、ついで「制限しない」が 25.1%であった。

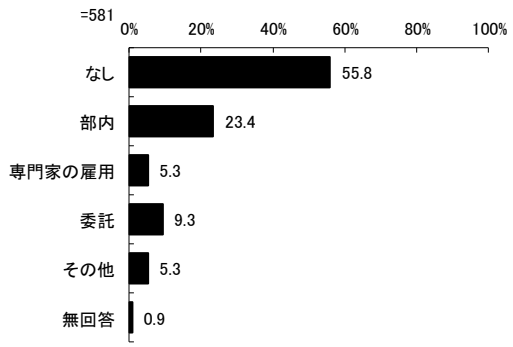
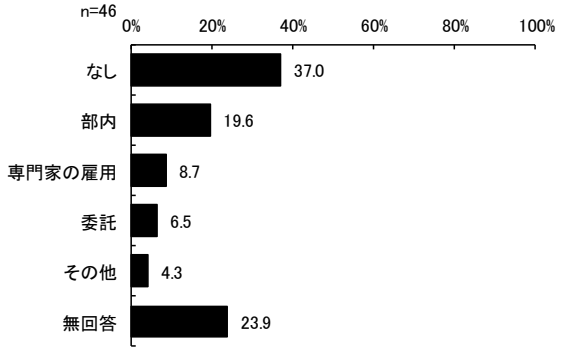
図表 54　ホームページ閲覧に関する対策（Q50）



3）医療情報システムの安全管理ガイドラインに記載の CSIRT 組織化について

医療情報システムの安全管理ガイドラインに記載の CSIRT 組織化については、「なし」が 55.8%で最も割合が高く、ついで「部内」が 23.4%であった。

図表 55　医療情報システムの安全管理ガイドラインに記載の CSIRT 組織化について（Q51）

今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

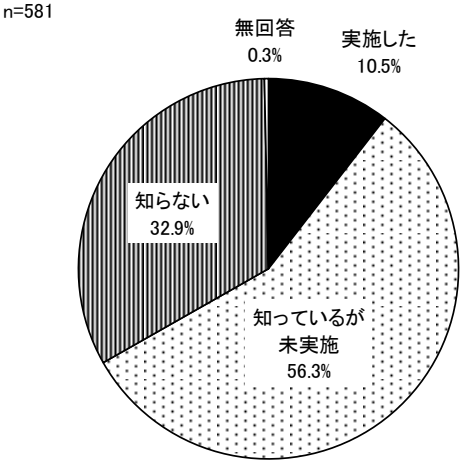
※「その他」の主な回答は以下の通り。
・院内の委員会にて対応
・上部機関が設置している
・機構にて組織化されている
・情報セキュリティポリシーにより規定
・対策専門部署の設立

・団体本部
・病院だけでなく法人全体として運用している
・法人内職員で検討
・本部が管理している

4）医療情報システムの安全管理ガイドラインに添付されたサイバーセキュリティに関するチェックリスト、フローを知っているか

医療情報システムの安全管理ガイドラインに添付されたサイバーセキュリティに関するチェックリスト、フローを知っているかについては、「知っているが未実施」が 56.3%で最も割合が高く、「知らない」が 32.9%であった。

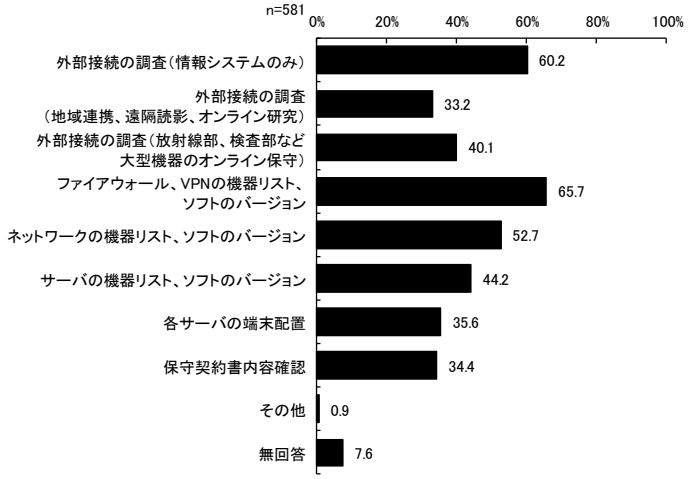
図表 56　医療情報システムの安全管理ガイドラインに添付されたサイバーセキュリティに関するチェックリスト、フローを知っているか（Q52）



5）事前調査、監視の対象

事前調査、監視の対象については、ファイアウォール、VPN の機器リスト、ソフトのバージョン」が 65.7%で最も割合が高く、ついで「外部接続の調査（情報システムのみ)」が 60.2%であった。

図表 57　事前調査、監視の対象（Q53）【複数回答】

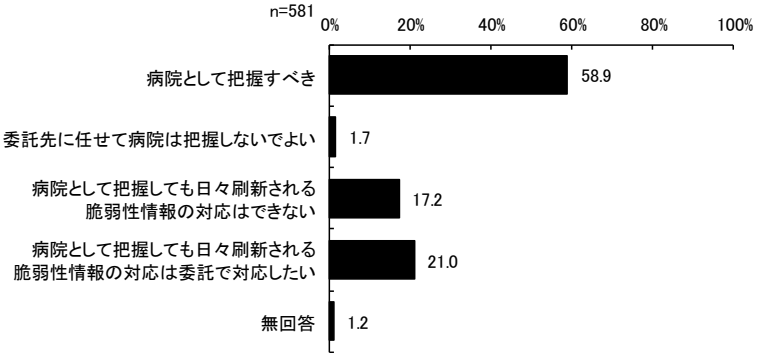


※「その他」の主な回答は以下の通り。
・各システムに格納されている DB とデータレイアウトの把握

6）システムの保守回線・CT・MRI 等の検査機器の保守回線の詳細

システムの保守回線・CT・MRI 等の検査機器の保守回線の詳細については、「病院として把握すべき」が 58.9%で最も割合が高かった。

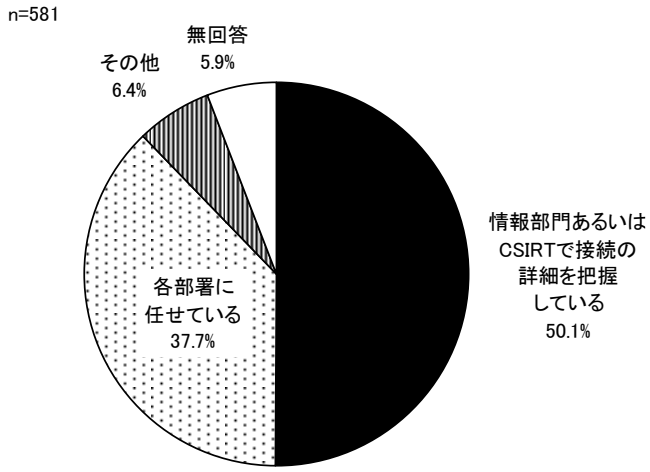
図表 58　システムの保守回線・CT・MRI 等の検査機器の保守回線の詳細（Q54）



7）地域連携・遠隔病理診断・遠隔画像診断・オンライン治験接続について

地域連携・遠隔病理診断・遠隔画像診断・オンライン治験接続については、「情報部門あるいはCSIRTで接続の詳細を把握している」が50.1%で最も割合が高く、「各部署に任せている」が37.7%であった。

図表59　地域連携・遠隔病理診断・遠隔画像診断・オンライン治験接続について（Q55）

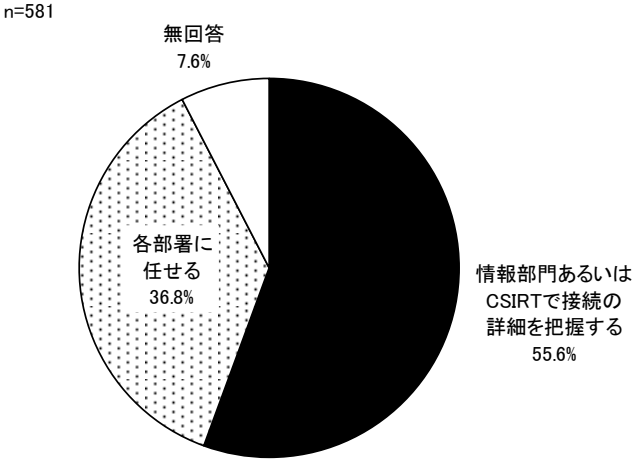


※「その他」の主な回答は以下の通り。
・ケースによって異なる
・システム管理部門で対応
・リアル接続はしていない。必要に応じてｅメール等で連携する
・兼任システム担当者が把握している
・外部接続は一切遮断している
・各部署に任せ、報告・管理先を情報部としている
・地域連携、遠隔病理診断等を導入していない
・導入時に情報部門が関わりセキュリティ対策を施す。導入後の運用は担当部署が担う
・把握しているが、通信技術等の知識がなく詳しくわからない
・病院として把握しても日々刷新される脆弱性情報の対応はできない

8）オンライン診療・遠隔モニタリング・院内 SNS の接続について

オンライン診療・遠隔モニタリング・院内 SNS の接続については、「情報部門あるいは CSIRT で接続の詳細を把握する」が 55.6%で最も割合が高く、ついで「各部署に任せる」が 36.8%であった。

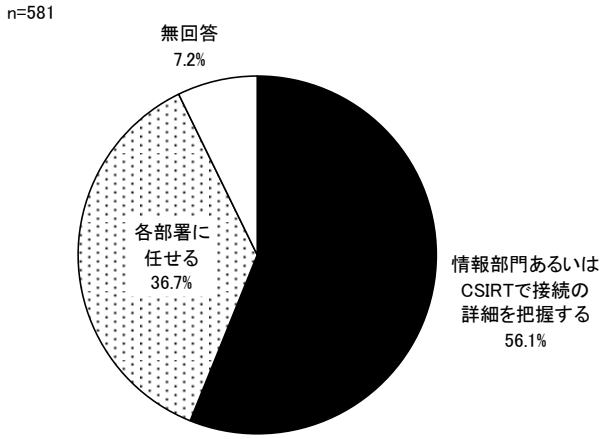
図表 60　オンライン診療・遠隔モニタリング・院内 SNS の接続について（Q56）



9）匿名化してオンライン接続する遠隔画像診断・匿名化してオンライン接続する調査等の接続について

匿名化してオンライン接続する遠隔画像診断・匿名化してオンライン接続する調査等の接続については、「情報部門あるいはCSIRTで接続の詳細を把握する」が56.1%で最も割合が高く、ついで「各部署に任せる」が36.7%であった。

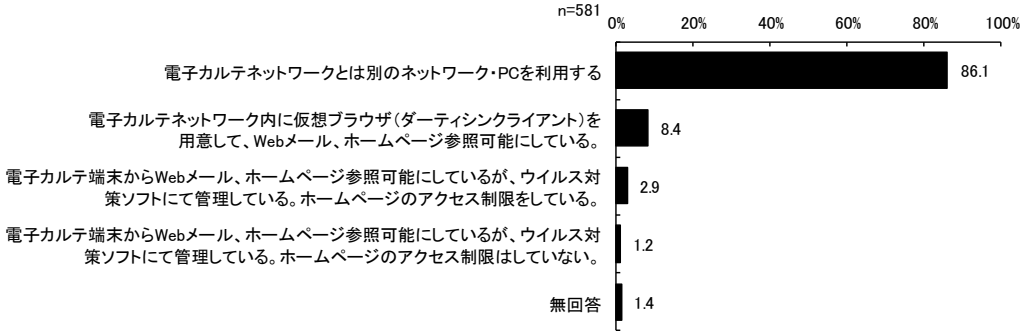
図表61　匿名化してオンライン接続する遠隔画像診断・匿名化してオンライン接続する調査等の接続について（Q57）



10）利用者のホームページ閲覧、メール受信について

利用者のホームページ閲覧、メール受信については、「電子カルテネットワークとは別のネットワーク・PC を利用する」が 86.1%で最も割合が高かった。

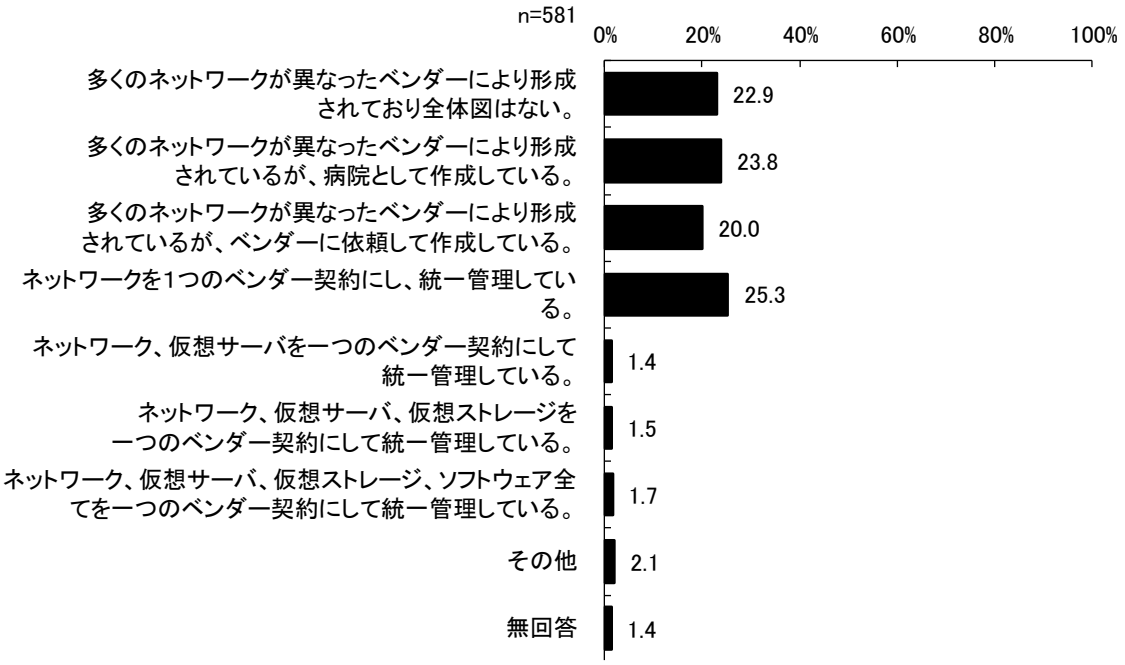
図表 62　利用者のホームページ閲覧、メール受信について（Q58）



11）院内ネットワーク全体図の作成はされているか

院内ネットワーク全体図の作成はされているかについては、「ネットワークを１つのベンダー契約にし、統一管理している」が 25.3%で最も割合が高く、ついで「多くのネットワークが異なったベンダーにより形成されているが､病院として作成している」が 23.8%、「多くのネットワークが異なったベンダーにより形成されており全体図はない」が 22.9%であった。

図表 63　院内ネットワーク全体図の作成はされているか（Q59）

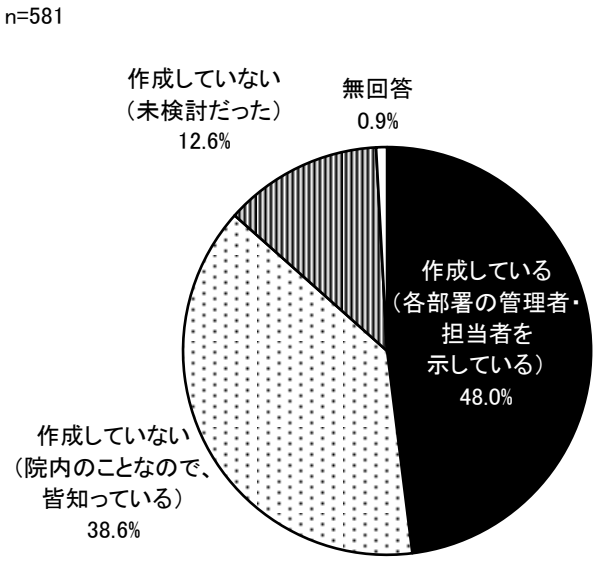


※「その他」の主な回答は以下の通り。
・office365 を利用
・オンプレ環境自体が大規模(5000 ホスト規模)なこと、近年は外部 DC やクラウドの活用も進み、規模が大きくなり過ぎたため一元的に描画できないが、ネットワーク管理者の頭の中にはある
・一部使用していない系統の削除ができていない
・ネットワークを１つのベンダー契約にしているが、管理が徹底されておらず病院に情報提供されない
・ほぼ統一された全体図があるが、一部異なるベンダーにより形成された部分があり、その部分については管理できていない
・一つのベンダーにお願いしているが、接続端末等の情報は管理できていない
・統一管理のため調査中（現在はシステムごとの個別管理）
・複数のネットワークがあるが敷設時の担当者が退職のため一部の図面しかなく障害時の都度に現場確認を行なっている
・複数ベンダーのネットワーク構成図を一元管理している
・分かる範囲で作成

12）電子カルテシステム・部門システムそれぞれについて院内の管理者・担当者一覧を作成しているか

電子カルテシステム・部門システムそれぞれについて院内の管理者・担当者一覧を作成しているかについては、「作成している（各部署の管理者・担当者を示している）」が 48.0%で最も割合が高く、ついで「作成していない（院内のことなので、皆知っている）」が 38.6%であった。

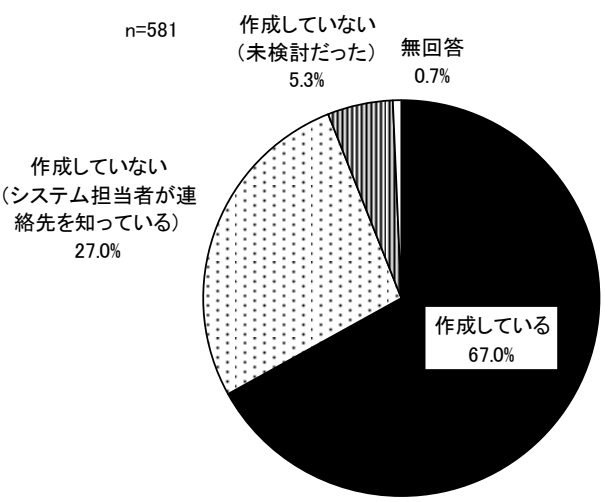
図表 64　電子カルテシステム・部門システムそれぞれについて院内の管理者・担当者一覧を作成しているか（Q60）



13）電子カルテシステム・部門システムの構築・運用事業者の連絡先一覧を作成しているか

電子カルテシステム・部門システムの構築・運用事業者の連絡先一覧を作成しているかについては、「作成している」が 67.0%で最も割合が高く、ついで「作成していない（システム担当者が連絡先を知っている)」が 27.0%であった。

図表 65　電子カルテシステム・部門システムの構築・運用事業者の連絡先一覧を作成しているか（Q61）

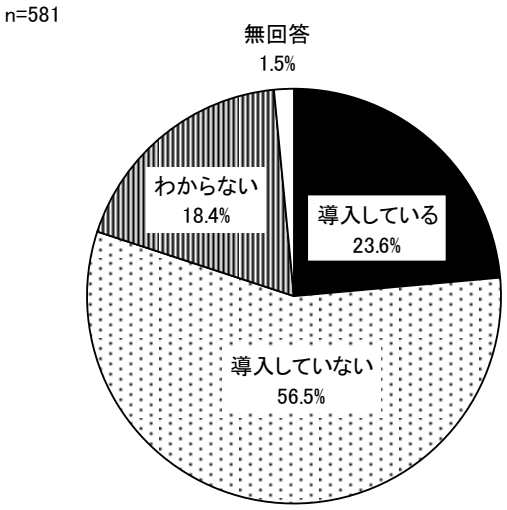


（6）ウイルス対策の状況

1）端末へのEDR（Endpoint Detection and Response）導入状況

端末へのEDR（Endpoint Detection and Response）導入状況については、「導入していない」が56.5%で最も割合が高く、ついで「導入している」が23.6%であった。

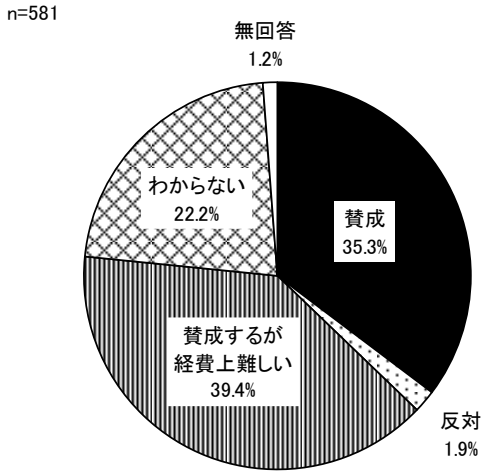
図表66　端末へのEDR（Endpoint Detection and Response）導入状況（Q62）



2）端末への EDR 導入について

端末への EDR 導入については、「賛成するが経費上難しい」が 39.4％で最も割合が高く、ついで「賛成」が 35.3％であった。

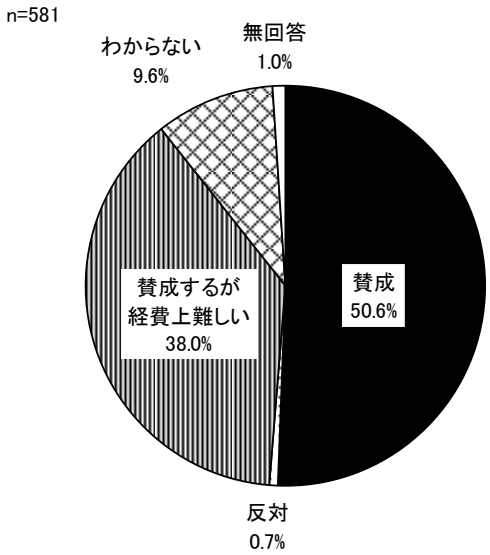
図表 67　端末への EDR 導入について（Q63）



3）内部ネットワークを監視することについて

内部ネットワークを監視することについては、「賛成」が 50.6%で最も割合が高く、ついで「賛成するが経費上難しい」が 38.0%であった。

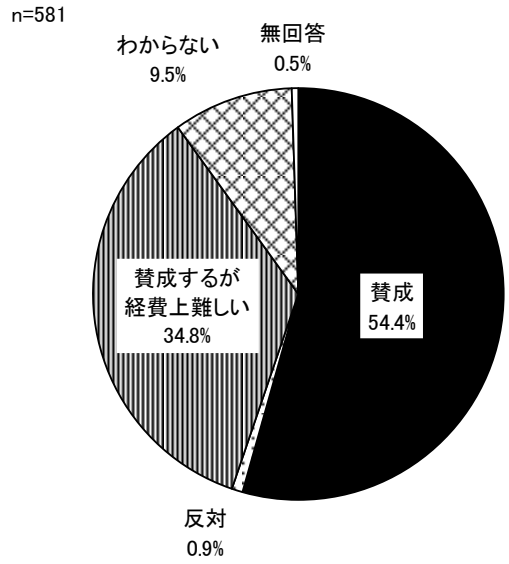
図表 68　内部ネットワークを監視することについて（Q64）



4）内部サーバーを監視することについて

内部サーバーを監視することについては、「賛成」が 54.4%で最も割合が高く、ついで「賛成するが経費上難しい」が 34.8%であった。

図表 69　内部サーバーを監視することについて（Q65）

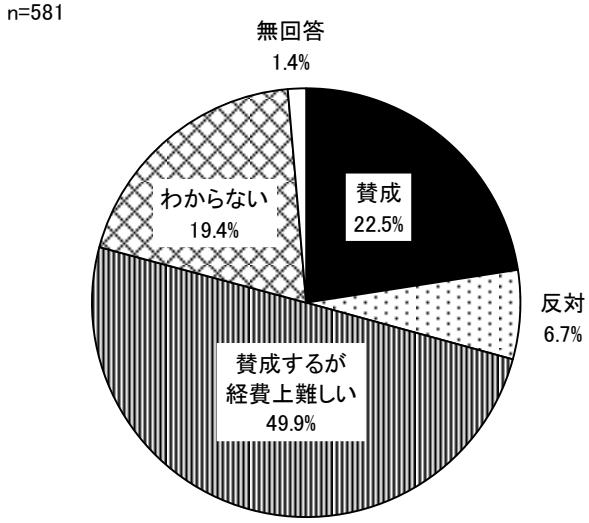


（7）サイバーセキュリティ対策への意見

1）端末からサーバーを守るためのシンクライアント基盤の導入

端末からサーバーを守るためのシンクライアント基盤の導入については、「賛成するが経費上の難しい」が 49.9%で最も割合が高く、ついで「賛成」が 22.5%であった。

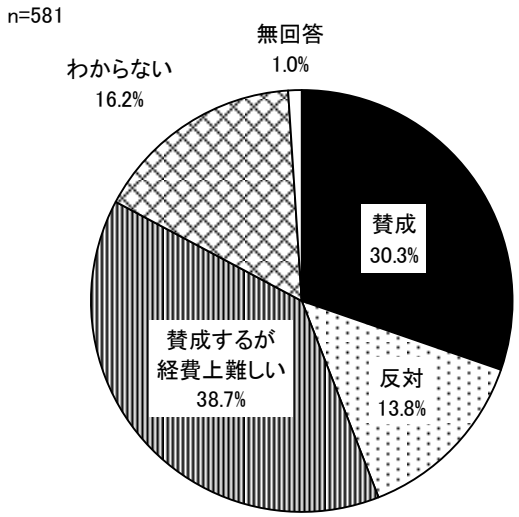
図表 70　端末からサーバーを守るためのシンクライアント基盤の導入（Q66）



2）仮想ブラウザ（ホームページ、Web メール参照用の仮想サーバーを用意）経由のインターネット参照

仮想ブラウザ（ホームページ、Web メール参照用の仮想サーバーを用意）経由のインターネット参照については、「賛成するが経費上難しい」が 38.7%で最も割合が高く、ついで「賛成」が 30.3%であった。

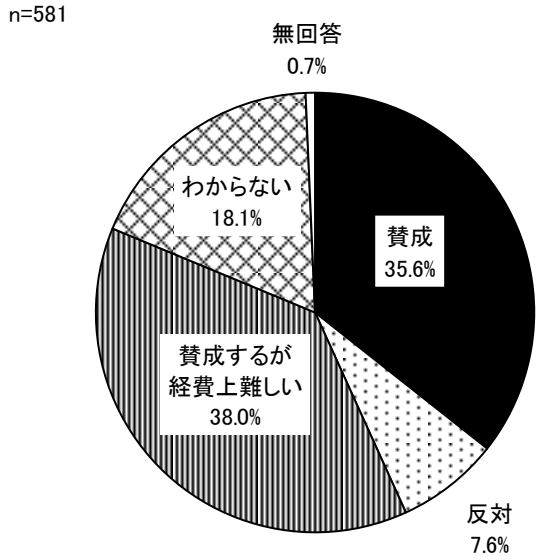
図表 71　仮想ブラウザ（ホームページ、Web メール参照用の仮想サーバーを用意）経由のインターネット参照（Q67）



3）組織内のサーバー（ハード系）を仮想サーバー、仮想ストレージ、仮想ネットワーク等を用いて病院あるいは委託契約にて統一的に導入管理を行う

組織内のサーバー（ハード系）を仮想サーバー、仮想ストレージ、仮想ネットワーク等を用いて病院あるいは委託契約にて統一的に導入管理を行うことについては、「賛成するが経費上難しい」が 38.0%で最も割合が高く、ついで「賛成」が 35.6%であった。

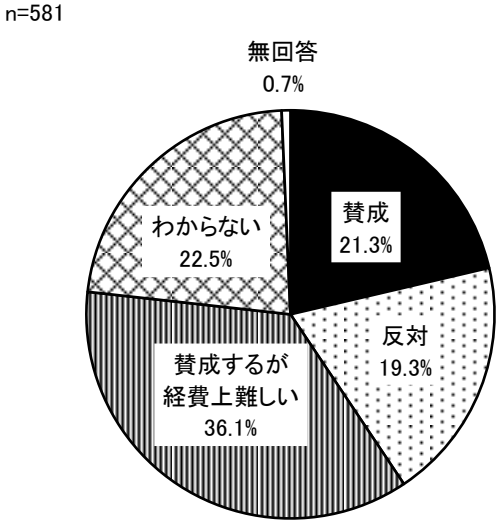
図表 72　組織内のサーバー（ハード系）を仮想サーバー、仮想ストレージ、仮想ネットワーク等を用いて病院あるいは委託契約にて統一的に導入管理を行う（Q68）



4）組織内のサーバー（ハード系）をクラウドサーバー等を用いて病院あるいは委託契約にて統一的に導入管理を行う

組織内のサーバー（ハード系）をクラウドサーバー等を用いて病院あるいは委託契約にて統一的に導入管理を行うことについては、「賛成するが経費上難しい」が 36.1%で最も割合が高く、ついで「わからない」が 22.5%であった。

図表 73　組織内のサーバー（ハード系）をクラウドサーバー等を用いて病院あるいは委託契約にて統一的に導入管理を行う（Q69）

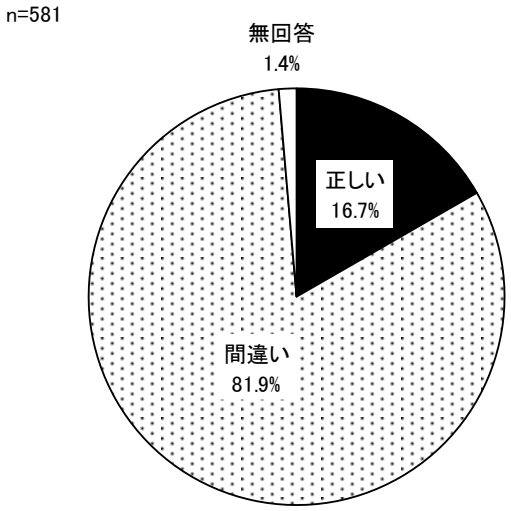


（8）最近のサイバー攻撃に対する理解度

1）「データを暗号化されたPC、サーバーに必ずウイルスは見つかる」ことは正しいか

「データを暗号化されたPC、サーバーに必ずウイルスは見つかる」ことは正しいかについては、「間違い」が81.9%であった。

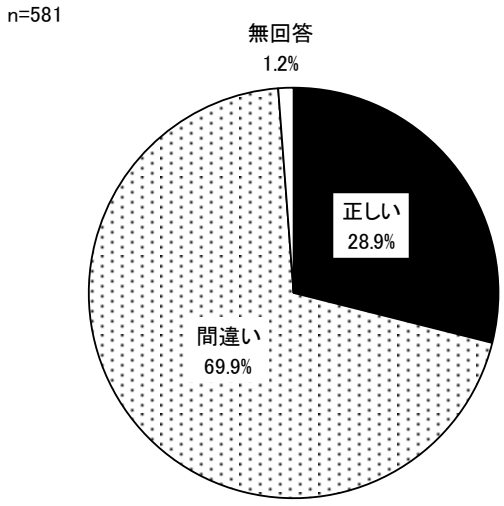
図表74　「データを暗号化されたPC、サーバーに必ずウイルスは見つかる」ことは正しいか（Q70）



2)「A さんからウイルス添付メールが届いた場合、A さんの PC はコンピュータウイルスに感染している」ことは正しいか

「A さんからウイルス添付メールが届いた場合、A さんの PC はコンピュータウイルスに感染している」ことは正しいかについては、「間違い」が 69.9%であった。

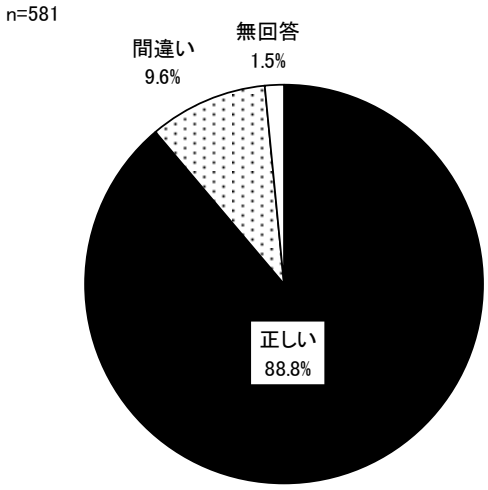
図表 75　「A さんからウイルス添付メールが届いた場合、A さんの PC はコンピュータウイルスに感染している」ことは正しいか（Q71）



3)「Windows のアクティブディレクトリやバックアップの設定ファイルは攻撃される」ことは正しいか

「Windows のアクティブディレクトリやバックアップの設定ファイルは攻撃される」ことは正しいかについては、「正しい」が 88.8%であった。

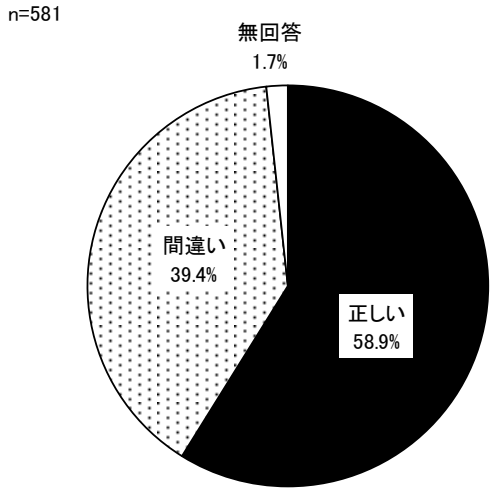
図表 76　「Windows のアクティブディレクトリやバックアップの設定ファイルは攻撃される」ことは正しいか（Q72）



4)「大容量のファイル全体の暗号化は時間がかかるので一部の暗号化をするものもある」ことは正しいか

「大容量のファイル全体の暗号化は時間がかかるので一部の暗号化をするものもある」ことは正しいかについては、「正しい」が 58.9%であった。

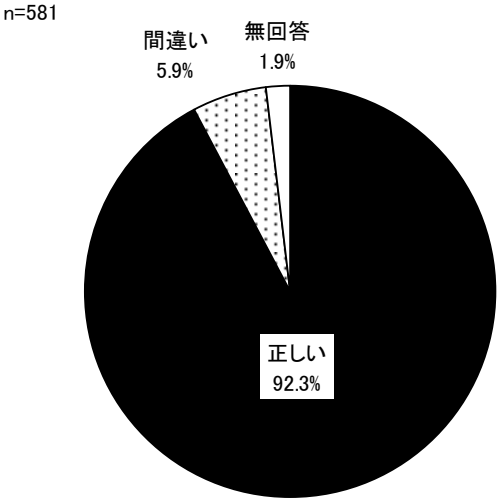
図表 77　「大容量のファイル全体の暗号化は時間がかかるので一部の暗号化をするものもある」ことは正しいか（Q73）



5)「攻撃を受けた場合に IPA、NISC に対応、助言する窓口がある」ことは正しいか

「攻撃を受けた場合に IPA、NISC に対応、助言する窓口がある」ことは正しいかについては、「正しい」が 92.3%であった。

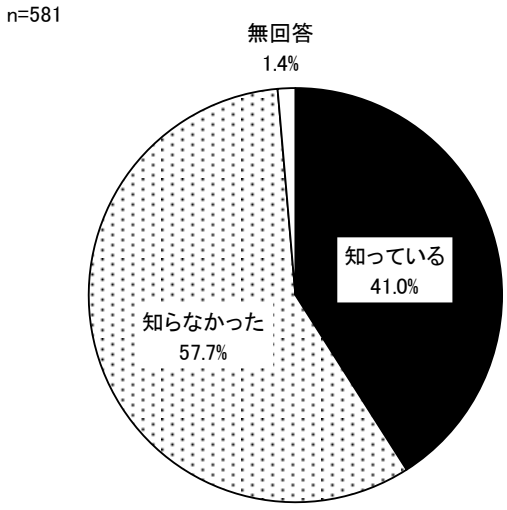
図表 78　「攻撃を受けた場合に IPA、NISC に対応、助言する窓口がある」ことは正しいか（Q74）



6)「NISC の 3、2、1 ルールでは 3 つのデータ、2 つにバックアップ、1 つのオフラインバックアップが提唱されている」ことを知っているか

「NISC の 3、2、1 ルールでは 3 つのデータ、2 つにバックアップ、1 つのオフラインバックアップが提唱されている」ことを知っているかについては、「知らなかった」が 57.7%であった。

図表 79　「NISC の 3、2、1 ルールでは 3 つのデータ、2 つにバックアップ、1 つのオフラインバックアップが提唱されている」ことを知っているか（Q75）



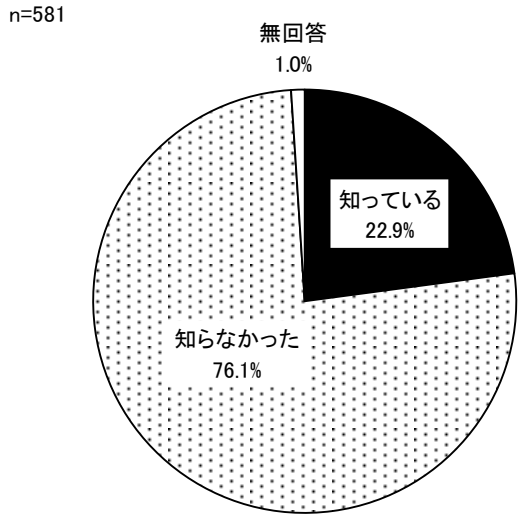
図表 80　「NISC の 3、2、1 ルールでは 3 つのデータ、2 つにバックアップ、1 つのオフラインバックアップが提唱されている」ことを知っているか（Q75）とセキュリティ教育を行っているか（Q28）、セキュリティ教育は年に何回行っているか（Q29）、セキュリティ教育のためにどのような研修を行っているか（Q30）のクロス集計結果

		調査数	知っている	知らなかった	無回答
Q28 セキュリティ教育を行っているか	はい	389 100.0	174 44.7	210 54.0	5 1.3
	いいえ	170 100.0	57 33.5	111 65.3	2 1.2
	わからない	20 100.0	5 25.0	14 70.0	1 5.0
Q29 セキュリティ教育の1年あたりの実施回数	1回	293 100.0	127 43.3	163 55.6	3 1.0
	2回	36 100.0	17 47.2	19 52.8	－ －
	3回	3 100.0	1 33.3	2 66.7	－ －
	4回	2 100.0	1 50.0	1 50.0	－ －
	5回以上	2 100.0	－ －	2 100.0	－ －
Q30 研修の形式	集合講習	238 100.0	112 47.1	122 51.3	4 1.7
	e-Learning教材（自施設で作成）	144 100.0	70 48.6	74 51.4	－ －
	e-Learning教材（外注、あるいは既成のもの）	86 100.0	40 46.5	45 52.3	1 1.2
	その他	40 100.0	20 50.0	20 50.0	－ －

7)「NICT のサイバーセキュリティ研究所のデータでは IoT 機器の攻撃が半数以上である」ことを知っているか

「NICT のサイバーセキュリティ研究所のデータでは IoT 機器の攻撃が半数以上である」ことを知っているかについては、「知らなかった」が 76.1%であった。

図表 81　「NICT のサイバーセキュリティ研究所のデータでは IoT 機器の攻撃が半数以上である」ことを知っているか（Q76）



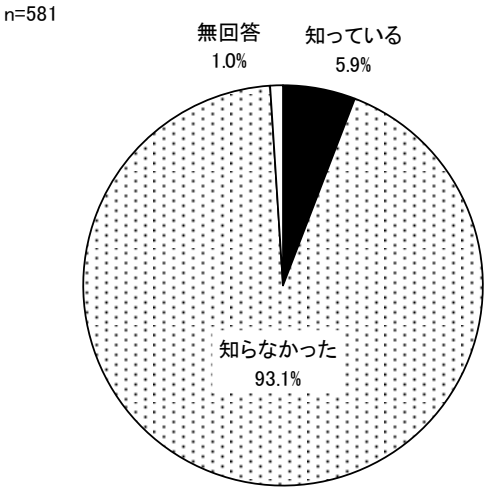
図表 82　「NICT のサイバーセキュリティ研究所のデータでは IoT 機器の攻撃が半数以上である」ことを知っているか（Q76）とセキュリティ教育を行っているか（Q28）、セキュリティ教育は年に何回行っているか（Q29）、セキュリティ教育のためにどのような研修を行っているか（Q30）のクロス集計結果

		調査数	知っている	知らなかった	無回答
Q28 セキュリティ教育を行っているか	はい	389 100.0	98 25.2	287 73.8	4 1.0
	いいえ	170 100.0	31 18.2	138 81.2	1 0.6
	わからない	20 100.0	4 20.0	15 75.0	1 5.0
Q29 セキュリティ教育の1年あたりの実施回数	1回	293 100.0	65 22.2	224 76.5	4 1.4
	2回	36 100.0	12 33.3	24 66.7	－ －
	3回	3 100.0	2 66.7	1 33.3	－ －
	4回	2 100.0	1 50.0	1 50.0	－ －
	5回以上	2 100.0	－ －	2 100.0	－ －
Q30 研修の形式	集合講習	238 100.0	60 25.2	175 73.5	3 1.3
	e-Learning教材（自施設で作成）	144 100.0	43 29.9	101 70.1	－ －
	e-Learning教材（外注、あるいは既成のもの）	86 100.0	19 22.1	66 76.7	1 1.2
	その他	40 100.0	8 20.0	32 80.0	－ －

8）「国際医療機器規制当局フォーラム文書におけるサイバー攻撃対策について」知っているか

「国際医療機器規制当局フォーラム文書におけるサイバー攻撃対策について」知っているかは、「知らなかった」が 93.1%であった。

図表 83　「国際医療機器規制当局フォーラム文書におけるサイバー攻撃対策について」知っているか（Q77）



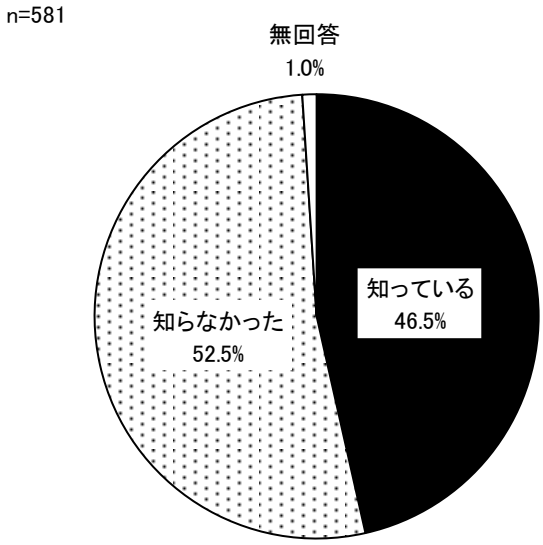
図表 84　「国際医療機器規制当局フォーラム文書におけるサイバー攻撃対策について」知っているか（Q77）とセキュリティ教育を行っているか（Q28）、セキュリティ教育は年に何回行っているか（Q29）、セキュリティ教育のためにどのような研修を行っているか（Q30）のクロス集計結果

		調査数	知っている	知らなかった	無回答
Q28 セキュリティ教育を行っているか	はい	389	26	359	4
		100.0	6.7	92.3	1.0
	いいえ	170	7	162	1
		100.0	4.1	95.3	0.6
	わからない	20	1	18	1
		100.0	5.0	90.0	5.0
Q29 セキュリティ教育の1年あたりの実施回数	1回	293	19	271	3
		100.0	6.5	92.5	1.0
	2回	36	1	35	−
		100.0	2.8	97.2	−
	3回	3	1	2	−
		100.0	33.3	66.7	−
	4回	2	−	2	−
		100.0	−	100.0	−
	5回以上	2	−	2	−
		100.0	−	100.0	−
Q30 研修の形式	集合講習	238	18	218	2
		100.0	7.6	91.6	0.8
	e-Learning教材（自施設で作成）	144	8	135	1
		100.0	5.6	93.8	0.7
	e-Learning教材（外注、あるいは既成のもの）	86	7	77	2
		100.0	8.1	89.5	2.3
	その他	40	2	38	−
		100.0	5.0	95.0	−

9)「医療用 IoT 機器は、5、6 年のシステム更新後も使われるので設定変更忘れが危惧される」ことを知っているか

「医療用 IoT 機器は、5、6 年のシステム更新後も使われるので設定変更忘れが危惧される」ことを知っているかについては「知らなかった」52.5%であった。

図表 85　「医療用 IoT 機器は、5、6 年のシステム更新後も使われるので設定変更忘れが危惧される」ことを知っているか（Q78）



図表 86　「医療用 IoT 機器は、5、6 年のシステム更新後も使われるので設定変更忘れが危惧される」ことを知っているか（Q78）とセキュリティ教育を行っているか（Q28）、セキュリティ教育は年に何回行っているか（Q29）、セキュリティ教育のためにどのような研修を行っているか（Q30）のクロス集計結果

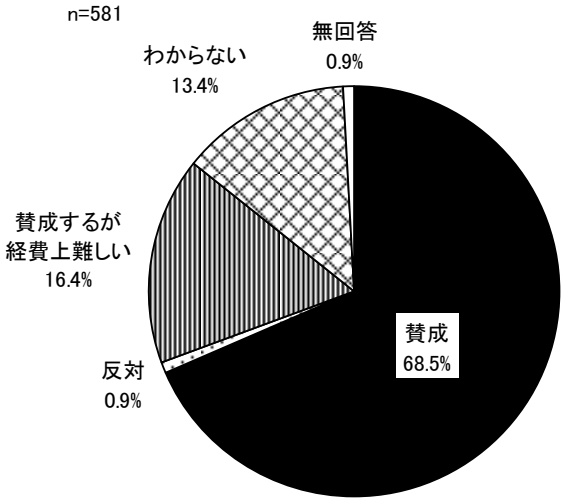
		調査数	知っている	知らなかった	無回答
Q28 セキュリティ教育を行っているか	はい	389 100.0	206 53.0	179 46.0	4 1.0
	いいえ	170 100.0	58 34.1	111 65.3	1 0.6
	わからない	20 100.0	4 20.0	15 75.0	1 5.0
Q29 セキュリティ教育の1年あたりの実施回数	1回	293 100.0	155 52.9	136 46.4	2 0.7
	2回	36 100.0	17 47.2	17 47.2	2 5.6
	3回	3 100.0	1 33.3	2 66.7	－ －
	4回	2 100.0	2 100.0	－ －	－ －
	5回以上	2 100.0	1 50.0	1 50.0	－ －
Q30 研修の形式	集合講習	238 100.0	127 53.4	109 45.8	2 0.8
	e-Learning教材（自施設で作成）	144 100.0	81 56.3	62 43.1	1 0.7
	e-Learning教材（外注、あるいは既成のもの）	86 100.0	48 55.8	37 43.0	1 1.2
	その他	40 100.0	18 45.0	22 55.0	－ －

(9)重要データの保存について実施している事項

1) RAIDによるリアルタイムの保存

RAIDによるリアルタイムの保存については、「賛成」が68.5%であった。

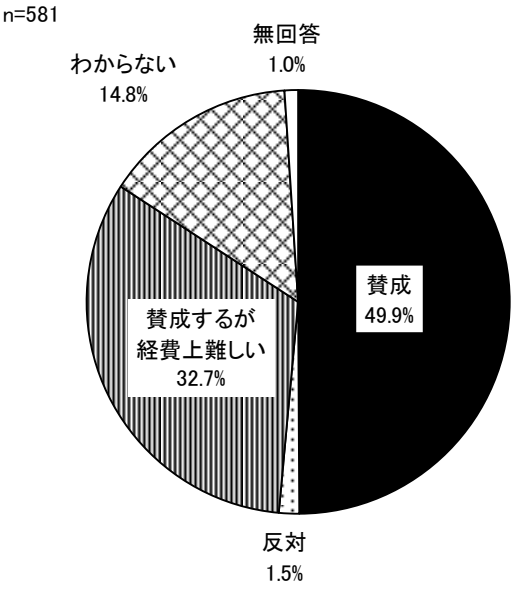
図表87　RAIDによるリアルタイムの保存（Q79）



2）RAID 以外にリアルタイムのバックアップを用意する

RAID 以外にリアルタイムのバックアップを用意するについては、「賛成」が 49.9%で最も割合が高く、ついで「賛成するが経費上難しい」が 32.7%であった。

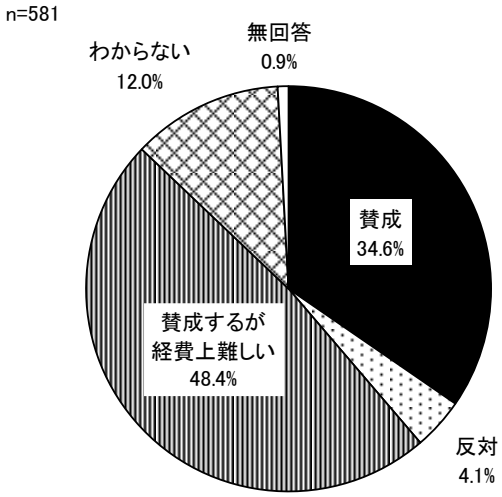
図表 88　RAID 以外にリアルタイムのバックアップを用意する（Q80）



3）遠隔地にリアルタイムのバックアップをする

遠隔地にリアルタイムのバックアップをするについては、「賛成するが経費上難しい」が 48.4%で最も割合が高く、ついで「賛成」が 34.6%であった。

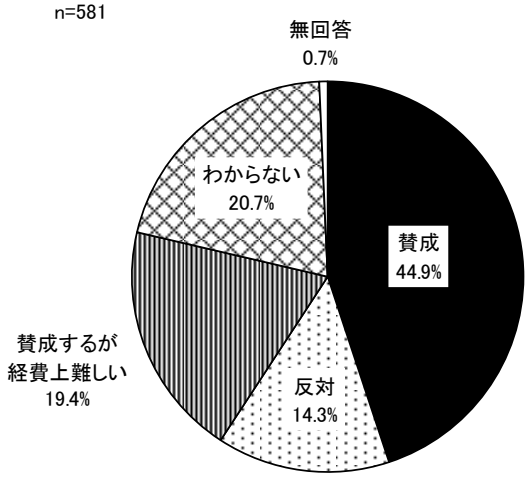
図表 89　遠隔地にリアルタイムのバックアップをする（Q81）



4）ジュークボックス型の磁気テープユニットによる日々のバックアップ

ジュークボックス型の磁気テープユニットによる日々のバックアップについては、「賛成」が 44.9%で最も割合が高く、ついで「わからない」が 20.7%であった。

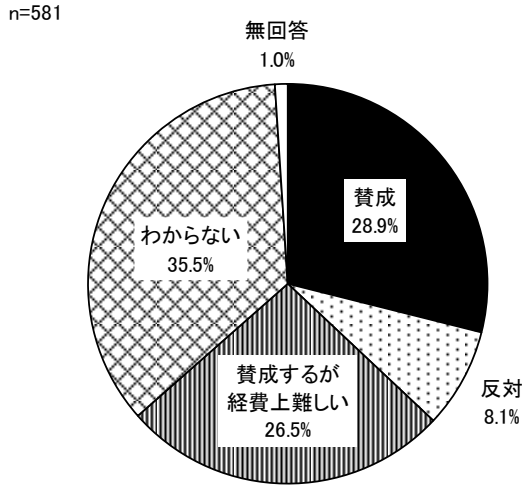
図表 90　ジュークボックス型の磁気テープユニットによる日々のバックアップ（Q82）



5）SS-MIX フォルダーから地域連携サーバーが pull する仕組みで地域連携側にバックアップできる

SS-MIX フォルダーから地域連携サーバーが pull する仕組みで地域連携側にバックアップできるについては、「わからない」が 35.5%で最も割合が高く、ついで「賛成」が 28.9%であった。

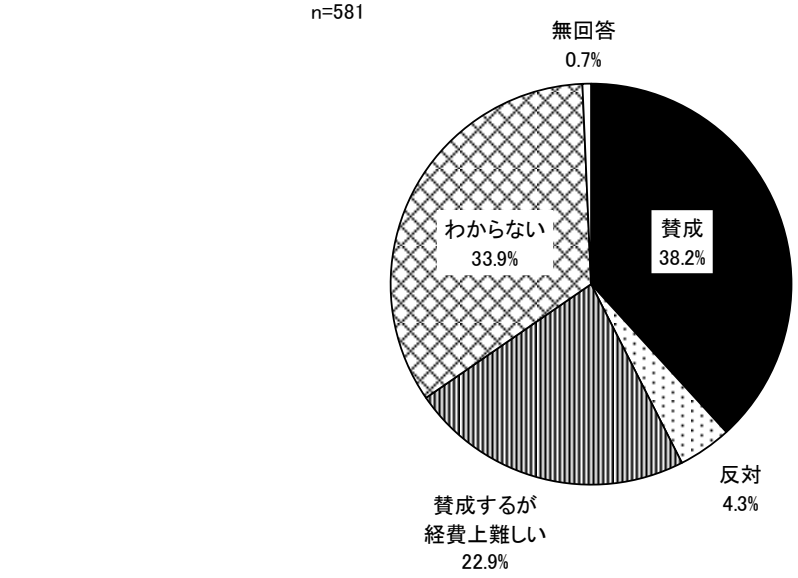
図表 91　SS-MIX フォルダーから地域連携サーバーが pull する仕組みで地域連携側にバックアップできる（Q83）



6）ストレージベンダーが用意するバックアップで削除等は特別な方法を用いる

ストレージベンダーが用意するバックアップで削除等は特別な方法を用いるについては、「賛成」が 38.2%で最も割合が高く、ついで「わからない」が 33.9%であった。

図表 92　ストレージベンダーが用意するバックアップで削除等は特別な方法を用いる（Q84）

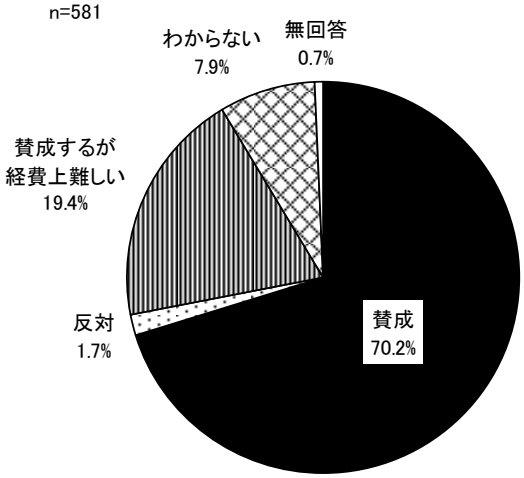


（１０）情報部門の管理について

1）管理者のサーバー等の管理に用いるPCとメール・ホームページ参照のPCとは別の機器、別のネットワークを用いる

管理者のサーバー等の管理に用いるPCとメール・ホームページ参照のPCとは別の機器、別のネットワークを用いるについては、「賛成」が70.2%で最も割合が高く、ついで「賛成するが経費上難しい」が19.4%であった。

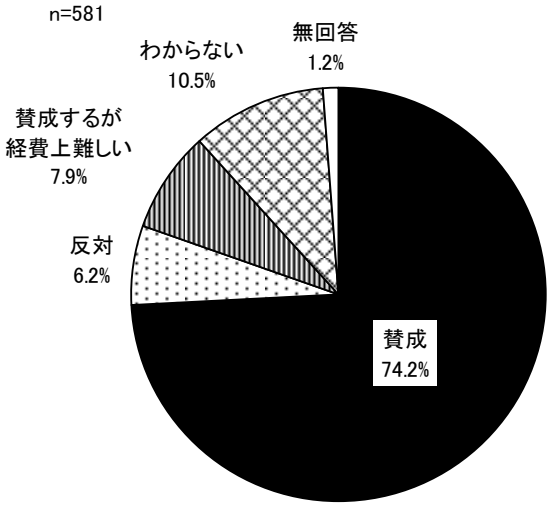
図表93　管理者のサーバー等の管理に用いるPCとメール・ホームページ参照のPCとは別の機器、別のネットワークを用いる（Q85）



2）委託業者の院外からの接続は事前に時間等を連絡させ、時間、接続先を限定する

委託業者の院外からの接続は事前に時間等を連絡させ、時間、接続先を限定するについては、「賛成」が 74.2%で最も割合が高かった。

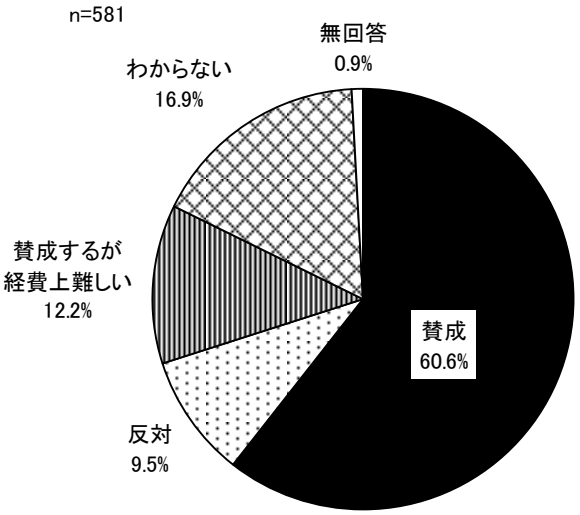
図表 94　委託業者の院外からの接続は事前に時間等を連絡させ、時間、接続先を限定する（Q86）



3）委託業者の院外からの接続は事前に時間・接続先等を連絡させファイアウォールの接続を制限する

委託業者の院外からの接続は事前に時間・接続先等を連絡させファイアウォールの接続を制限するについては、「賛成」が 60.6%で最も割合が高く、ついで「わからない」が 16.9%であった。

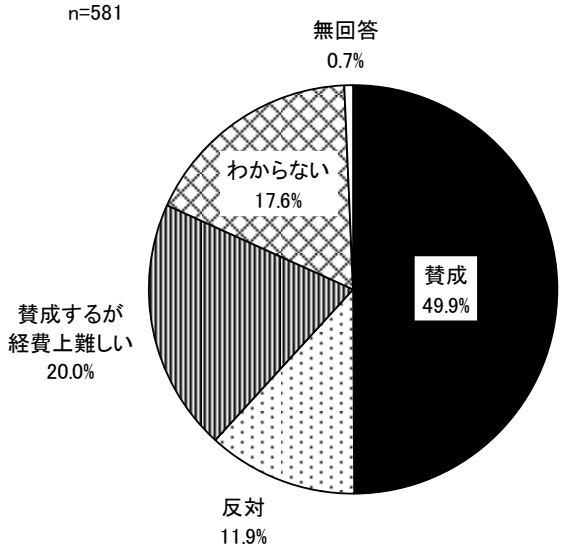
図表 95　委託業者の院外からの接続は事前に時間・接続先等を連絡させファイアウォールの接続を制限する（Q87）



4）委託業者の院外からの接続はリモートアクセス、シンクライアントなどを用いて直接接続させない

委託業者の院外からの接続はリモートアクセス、シンクライアントなどを用いて直接接続させないについては、「賛成」が 49.9%で最も割合が高く、ついで「賛成するが経費上難しい」が 20.0%であった。

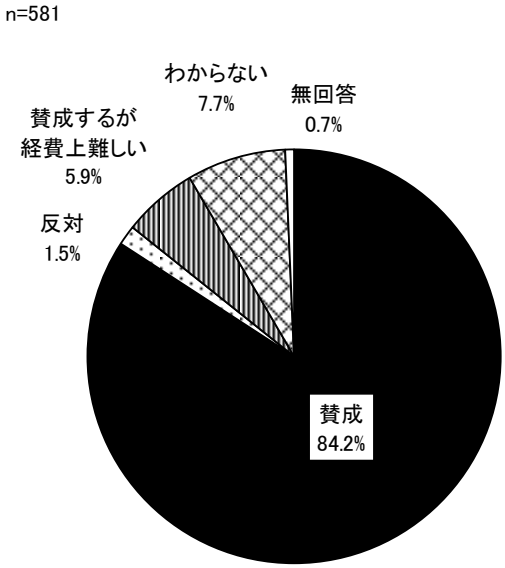
図表 96　委託業者の院外からの接続はリモートアクセス、シンクライアントなどを用いて直接接続させない（Q88）



5）委託業者が、院内にファイルを取り込む場合や院内から取り出す場合に記録を残す

委託業社が、院内にファイルを取り込む場合や院内から取り出す場合に記録を残すについては、「賛成」が 84.2%で最も割合が高かった。

図表 97　委託業者が、院内にファイルを取り込む場合や院内から取り出す場合に記録を残す（Q89）

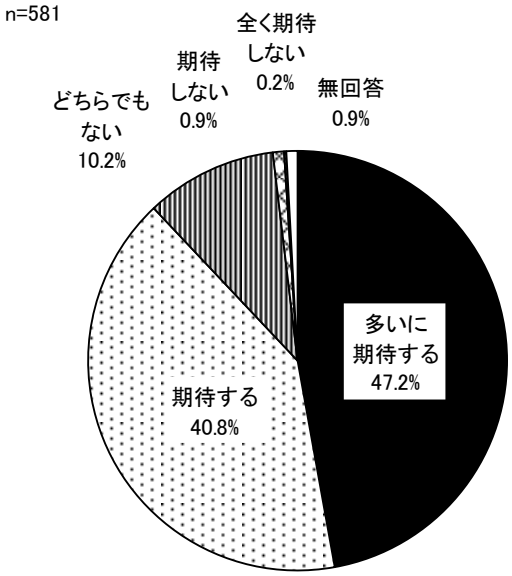


（１１）ISAC※について情報共有したい事項等　※Information Sharing and Analysis Center

1）流行しているマルウェア（ウイルス）等、リスク関連の情報

流行しているマルウェア（ウイルス）等、リスク関連の情報については、「多いに期待する」47.2%で最も割合が高く、ついで「期待する」が 40.8%であった。

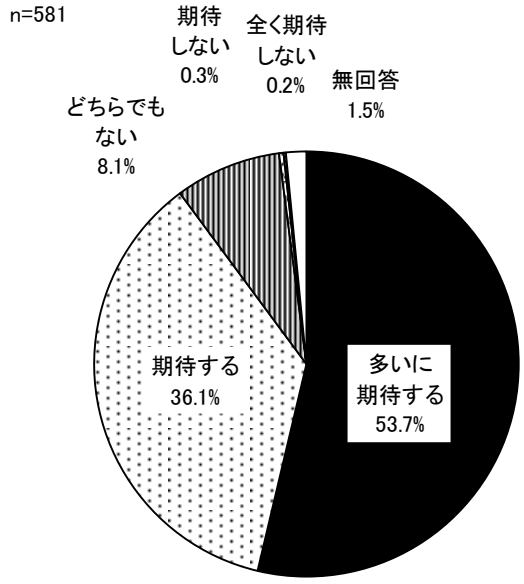
図表 98　流行しているマルウェア（ウイルス）等、リスク関連の情報（Q90）



2）セキュリティ対策の具体的な実施方法

セキュリティ対策の具体的な実施方法については、「多いに期待する」が 53.7%で最も割合が高く、ついで「期待する」が 36.1%であった。

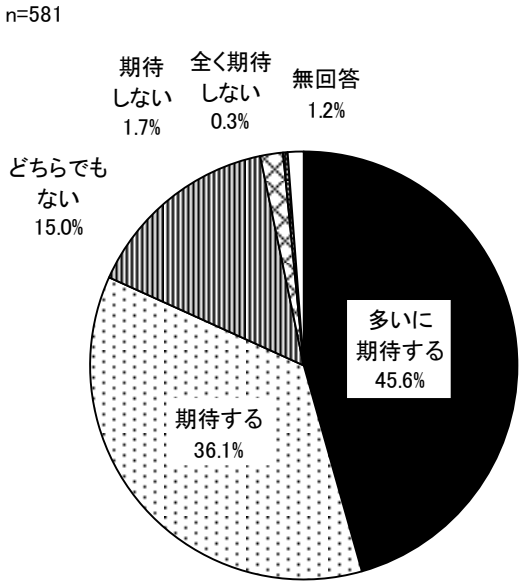
図表 99　セキュリティ対策の具体的な実施方法（Q91）



3）マルウェア検体の分析

マルウェア検体の分析については、「多いに期待する」が 45.6%で最も割合が高く、ついで「期待する」が 36.1%であった。

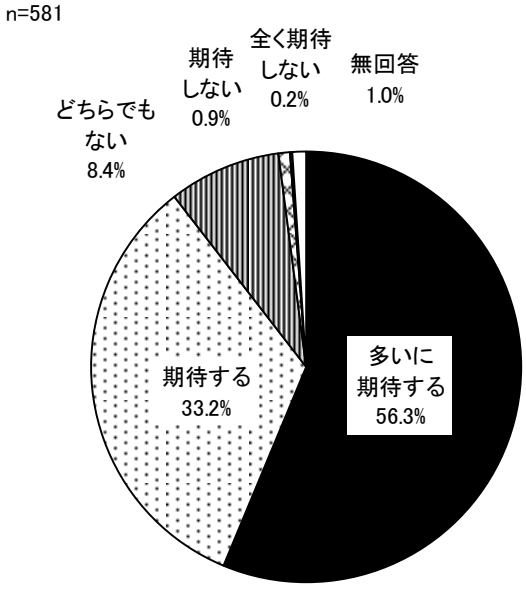
図表 100　マルウェア検体の分析（Q92）



4）セキュリティ教育教材の提供

セキュリティ教育教材の提供については、「多いに期待する」が 56.3%で最も割合が高く、ついで「期待する」が 33.2%であった。

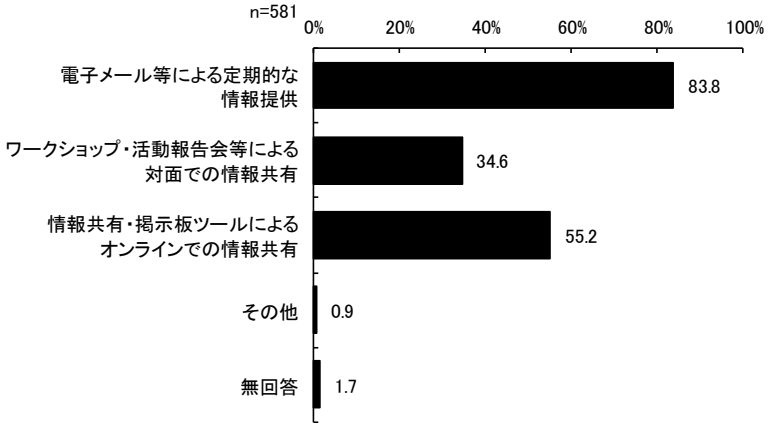
図表 101　セキュリティ教育教材の提供（Q93）



5）情報共有の手段について

情報共有の手段については、「電子メール等による定期的な情報提供」が 83.8%で最も割合が高く、ついで「情報共有・掲示板ツールによるオンラインでの情報共有」が 55.2%であった。

図表 102　情報共有の手段について（Q94）【複数回答】

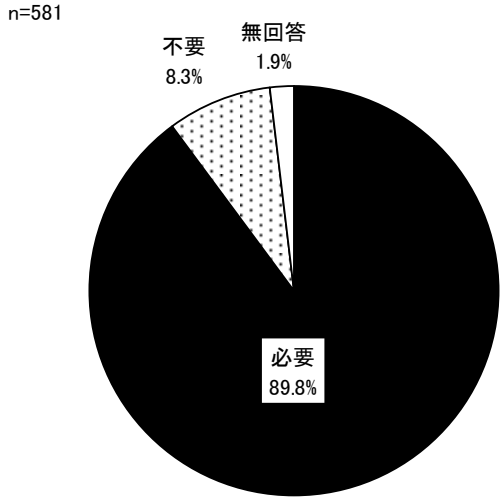


※「その他」の主な回答は以下の通り。
・FAX
・WEB による迅速な情報提供（固定的ではなく多岐にわたる情報）
・Youtube
・オンラインでのワークショップ
・活動報告会
・事例発表会の開催

6）知識レベルが同じではないので、技術的指導者が必要

知識レベルが同じではないので、技術的指導者が必要については、「必要」が 89.8%であった。

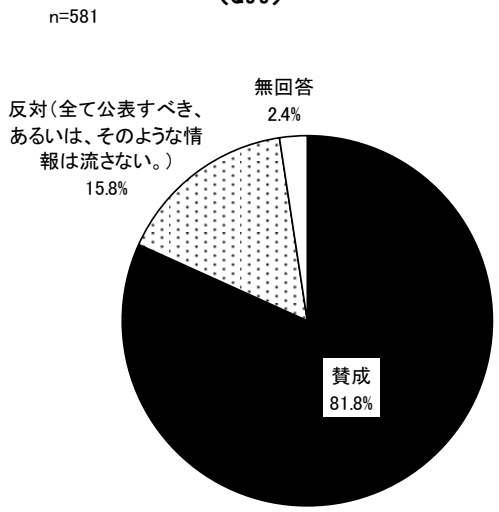
図表 103　知識レベルが同じではないので、技術的指導者が必要（Q95）



7）共有するべき情報には噂、予想なども含む必要があり、公表しにくいものがあると思う

共有するべき情報には噂、予想なども含む必要があり、公表しにくいものがあると思うについては、「賛成」が 81.8%であった。

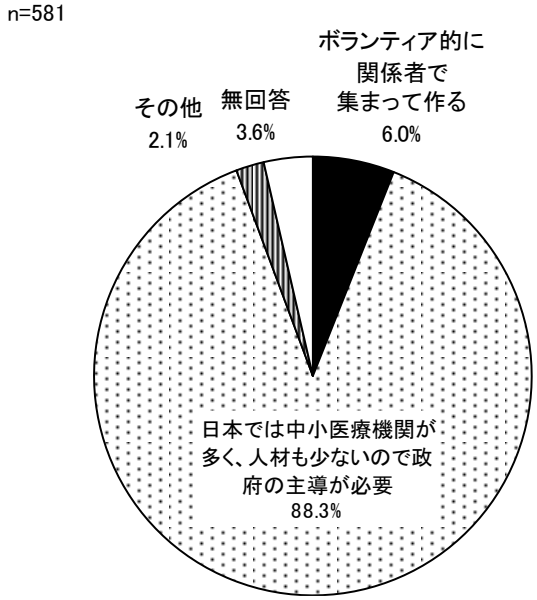
図表 104　共有するべき情報には噂、予想なども含む必要があり、公表しにくいものがあると思う（Q96）



8）組織のあり方について

組織のあり方については、「日本では中小医療機関が多く、人材も少ないので政府の主導が必要」が 88.3%で最も割合が高かった。

図表 105　組織のあり方について（Q97）



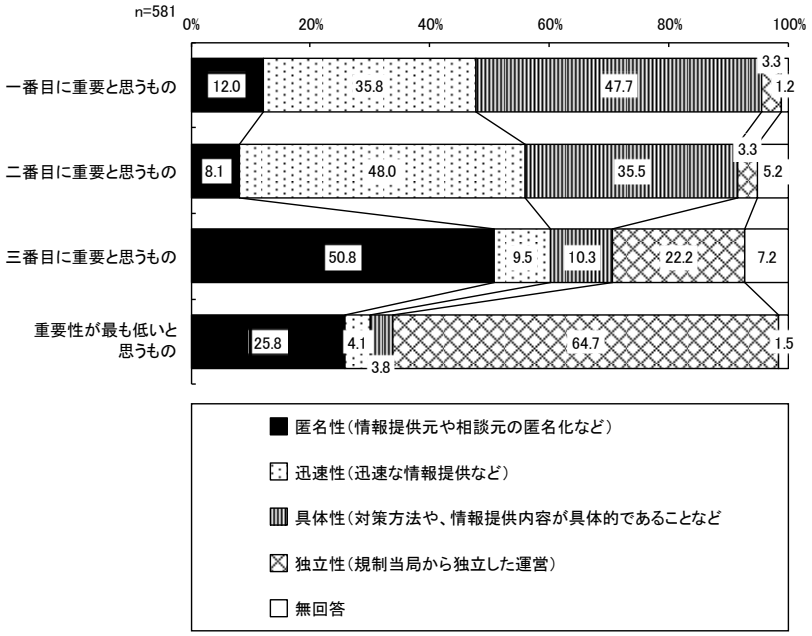
※「その他」の主な回答は以下の通り。
・アドバイザー的に政府が一般企業から選択した技術的指導者を配置し、医療系の関係者で組織化する
・全ての企業で問題と成るセキュリティに掛るコストを法制化するしか予算確保は出来ない
・日本で医療 ISAC と呼ばれるものが 2 つあるが、どちらも存在に疑問。悪徳系のほうは悪戯に不安を煽るだけ、NISC セプターカウンシルに設置された役所形骸系(日本医師会事務局内)のほうは活動実態が聞こえてこない
・日本に人材はいない
・本社・本部で対応

9）サイバーセキュリティ情報の公的共有組織に必要な要素の重要度

サイバーセキュリティ情報の公的共有組織に必要な要素で一番重要と思うものについては、具体性が 47.7%で最も割合が高く、二番目に重要と思うものについては迅速性が48.0%で最も割合が高く、三番目に重要と思うものについては、匿名性が 50.8%で最も割合が高く、重要性が最も低いと思うものについては、独立性（規制当局から独立した運営）が 64.7%であった。

この結果から重要性は「具体性」、「迅速性」、「匿名性」、「独立性」の順に高いと言える。

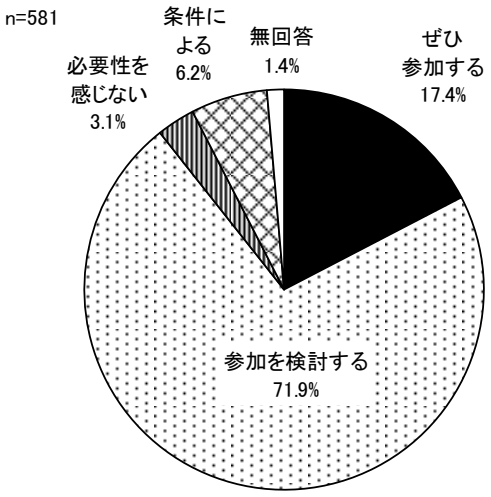
図表 106　サイバーセキュリティ情報の公的共有組織に必要な要素の重要度（Q98～Q101）



10）サイバーセキュリティ情報を共有するサービスを提供する公的組織があれば参加するか

サイバーセキュリティ情報を共有するサービスを提供する公的組織があれば参加するかについては、「参加を検討する」が 71.9%で最も割合が高く、ついで「ぜひ参加する」が 17.4%であった。

図表 107　サイバーセキュリティ情報を共有するサービスを提供する公的組織があれば参加するか（Q102～Q103）



※「条件による」と回答した場合の具体的な条件の主な回答は以下の通り。
・コスト、役に立つか
・サービス内容を確認した上で判断する
・できれば費用負担なし
・医療業界に特化しているか
・運営主体が正しく運営できる組織かどうか判断してから参加する
・活動内容等
・共有方法
・行政からの依頼文があること
・国の関与がどれくらいか（関与しすぎるものには参加しない）
・参加する際の費用、業務上病院の許可を得られるメリットの有無
・参加の是非が診療報酬に影響ないことと、参加・離脱が容易であること、更に不参加でも参加組織と同様に情報提供がなされること
・参加費用が無償か低額であること
・所属組織が公認の上、職務による参加
・信頼できる組織かどうか
・組織に加わるメリットと組織に入ることによる業務負荷の増加
・組織の許可とついていけるレベルなのか
・担当者や担当部署について組織内で要検討
・内容による
・スタッフの拘束時間
・費用面と人材確保の問題がクリアできれば
・非公開であること

（１２）その他意見

1）医療分野のサイバーセキュリティやヘルスケア ISAC に関する意見

図表 108　医療分野のサイバーセキュリティやヘルスケア ISAC に関する意見（Q104）

- １つ病院が個別に情報収集、対策の検討には限界があり、医療分野業界で広く共有できることが望ましい
- ISAC の早期の立ち上げを望む
- WEB セミナーなどがあれば、案内をいただけると幸いです
- ガイドラインに沿ったものをパッケージ化してほしい。また費用面でのサポートもお願いしたい
- サイバーセキュリティについて具体的な対策が知りたい。(最低限必要なものから優先順位をつけてどんな対策が必要か) 費用対効果など示されるとなお分かりやすい
- サイバーセキュリティ対策は費用ばかりかかるので、経営幹部がまったく乗り気にならない。医療機関の事務系の幹部職員はサイバーセキュリティ（ICT）の知識が全くないので全く話がすすまない。なので、医療機関でサイバーセキュリティ対策が進むことは難しいと思う
- セキュリティポリシーや情報セキュリティ規定のサンプルを提供してほしい
- セキュリティ対策（人材や対策措置）に対する公的な支援が必要だと考えています
- セキュリティ対策は重要であるが、費用や人員のコスト増が課題と感じる
- セキュリティ予算の必要性を確立いただきたい
- ぜひ進めて欲しい
- ランサムウェアへの具体的な対策、感染してしまった場合の具体的な対処例等動画を使った教材等提供してほしい
- 医療が国の当該重要項目であるので、どの医療機関でも同じ水準になるよう対応して欲しい
- 医療監視など、定期立入検査や監査でも意見がほしい
- 医療機関に情報システム、ネットワークなどを専門に取り扱う部門と、技術者が必要と感じています。医療情報部が存在する病院でも中身はそういった部署ではなく、診療情報管理士を中心とした点数を取るための医療系部署である場合が多いのではないでしょうか。医療情報システムは情報統括部門で管理し、正しく運用すべきと思います
- 医療機器メーカーのサイバーセキュリティに対する意識を高めることは重要と思います
- 医療機器系は安定稼働重視であるため、枯れた技術を使う事を優先し、セキュリティ担保は二の次になりがちであると思う。コスト的に見合った形で彼ら医療系ベンダーが適切にセキュリティ対応が取れる様な施策をアドバイスして頂きたい
- 医療業界ではセキュリティー対策が一般企業に比べてかなり遅れている。理由は様々あるが費用面が大きい。医療収入の中にセキュリティーの診療報酬もない為どうしても上層部の理解が得られない。もっと医療業界全体としてセキュリティー対策する方法を検

討して頂きたいです
・医療分野のサイバーセキュリティに対する窓口を一本化してほしい
・一方的な提供だと受け手側の問題もあるため双方向のものであるとよい
・院内業務に注力しなければならない担当者は多く、外部からの情報を入手、精査することが難しい。人員のレベルにも大きな差があり、情報発信や規程づくりが後手に回ってしまう。
・各病院のレベルが様々なのでわかりやすい説明と対策を求めます
・管理を医療機関に任せるのではなく、具体的な国の支援が必要だと感じます。
・厚労省主体で書く医療機関の情報セキュリティ専任者もしくはアドバイザーをリーズナブルな価格（月額1万円以内くらい）で外部委託できる仕組みを作って欲しい
・国が主導し、費用がかからない方式検討が望ましい
・社会情勢上、セキュリティ担当者に求められるレベルが急激に高くなっているが施設によっては難しく担当者の格差が大きくなっている。セキュリティ担当者研修をレベル別に実施していただきたい。
・情報提供団体が多すぎて、見るだけで疲れる。信頼がおける団体にて統合してほしい。
・情報発信や参加する人などオープンで広く参加できるような組織になると良いと思います。
・情報部門は日々忙しいため、各組織とも担当者の技術・意識レベルによりセキュリティ強度が大きく変わってしまいます。それらを均等化すべく、教育・情報提供体制の構築があれば有り難いです。
・人材に対するポストや給与体型が評価整備されていない
・先の質問に回答した通り「医療ISAC」と言われるものがバラバラ。以前からあった悪徳系と役所形骸系に続き、少し前に厚労省が医療ISAC設立の発表を行っていた。日本では医療ISACと呼ばれる組織が3つになるのか？業界関係者からしてもややこしいし、リテラシーの低い医療機関であれば尚更混乱するのではないか。「医療ISAC」を標榜する組織は一つにしてもらいたい。
・専門知識がないままにシステムを運用している当院のような環境でも、無料または格安に（市井のサイバーコンサル等に依頼せずとも）最低限のセイバーセキュリティ基盤を整備できるよう、規定やマニュアル作成支援ツールなどを提供されてはどうでしょうか。
・全員とは言わないが、田舎の50代以上の経営層の方々にセキュリティの概念が皆無に等しい。教育ターゲットとして重点的に行って欲しい。
・他分野の情報も共有した上で、医療分野での予測も含めて情報共有
・対策を病院の自由意志に任せていると、様々な理由をつけて結局やらずじまいになるので、法律で縛ったほうが良い
・大病院であれば人材も集められ、それなりに対策が取れると思うが、小さい病院では予算も限られる。また、医療分野で働いている方たちは元々ITリテラシーが低いと感じる。
・病院規模問わず医療分野に必要な情報共有ができることが必要だと感じています。

・流行すると慌てふためき対策が十分に練られないまま、決定されないようにしてほしい。また、費用補助を活用できるノウハウを合わせて提案してほしい。

2）本アンケートについて意見や提案など

図表 109　本アンケートについて意見や提案など（Q105）

・EDR については、システムに影響が無いなら賛成という項目が欲しい
・Q49～Q58 について　当院で実際に運用していることを回答するのか、望ましいと考える運用を回答するのかがわかりにくかった
・WEB アンケートの安全性が気になりました。脆弱性の漏えいにつながるのではないかと危惧しています
・アンケートの回答に病院名と所属部署ぐらいはいれたほうがいいのではないのでしょうか？あとアンケート項目が多い
・アンケート調査の集計結果を提示していただきたいです。セキュリティ教育を上層部に働きかけるためにも、根拠となる資料になり得ると考えますので、提示していただければと思います
・おそらくこのアンケートを作成した担当者はサイバーセキュリティに関する実務経験に乏しいか、教科書で勉強しただけで分かっているつもりの頭でっかちだと感じた。どうせやるのであれば、もう少し実務経験値のある人間が作成したほうが良い。またあちこち質問の日本語がおかしく、読んでいて頭が痛くなった。設問分の推敲不足
・このようなアンケートに答えるのが不安である
・この回答ができる知識を持つ病院スタッフは数少ないと思うので、このアンケートの目的不明
・サイバーセキュリティに関する調査が各団体からあり、同じような回答をしている。どこかで一本化して頂きたい
・システムの標準化が国の目標としてあるとはいえ、まだ各医療機関でそれぞれ異なった環境です。各選択肢でそれを選んだ理由など掘り下げてみてはいかがでしょうか。
・セキュリティをレベル分けして段階的に対策を説明していただくとわかりやすいと思います
・はい or いいえ方式の方が助かる
・よくあるアンケートと異なり、実のあるよい内容であった。
・ただ、質問数が多いので、あらかじめ何問あるとか、何パーセント進んでいるとか分からないため、途中からしんどくなりますし、業務的にも支障をきたします。少なくとも、30 分では終わらない内容かと思います。
・あらためて、サイバーセキュリティについて見直しする機会をいただき、ありがとうございました。
・医療組織と言っても規模や提供サービスが様々なので、当院には合ってない事柄も多い

・一部アンケートに関して所属における現状確認なのか、アンケート回答者の意見確認なのか、知識レベル確認テストなのかはっきりしないので回答が難しかった。(そうすべきなのは知っているが、今の所属ではそうなっていない時に　YES/NO どちらを答えるのか等)
・一部質問に関して、解釈によって選択が変わるようなものがあったので、具体例を付けていただければ嬉しいものがありました。
・何を聞こうとしているのか分からない質問が多数見受けられた。
・回答に苦慮するものが多く、実際の現場で対応すべきものに対する実施状況などについて回答させるような質問形式となっていたほうが回答しやすいのではないか？また、選択肢についても、当てはまらないことがある場合など、選択しないという方法で回答をすればよいのかわからなかったため、適当な回答となっているものが多い。さらに回答内容について事前に全質問を提示して、回答を準備させる必要があるのではないでしょうか。記載内容について、確認できる画面がないと思います。戻るボタンを押したときの動作がわからないので、そのまま入力を続けました。最後に、サイバーセキュリティにかかわるアンケートをＵＲＬメールで依頼していることについて、標的型攻撃ととらえてしまい回答を拒否することも検討していました。ご検討ください。
・回答選択肢を増やしてほしい（例：「賛成するが運用上難しい」など）
・該当する選択肢がない場合も多いので、その場合に選択する回答を用意してほしい
・各質問に対して各病院がどのような回答をしたかのフィードバック資料を見たい
・確認テストのような項目は不要ではないか。この調査がどのように役立てられるのか、質問内容から不明。趣味ですか？
・賛成反対の意見を集めるのはいいが、それよりも実際の状況も併せて情報収集すべきでは
・質問がわかりにくく、回答想定も不十分な印象であった為、十分な回答が出来なかったと思う。
・質問が多すぎる。専門的な質問が多く正しく答えられているかわからないため、もっと簡潔にしてもらいたい。
・質問が非常に多く、意図を図りかねる質問もあります。とくに設問の多さは途中で回答を辞めるケースが多くなるように思います。
・質問でわからない言葉を調べたり、回答すること自体が勉強になりました。
・質問の意図が明確ではない設問がある上に、質問が多すぎる
・質問の意味や意図がわからないのが多い。
・質問の質を向上して欲しい。意味不明も多い。
・質問の内容が理解しにくい
・質問の内容について認識間違いの物があった
・質問の内容的に対して適切な選択肢がない、理解しにくい等の項目があり回答に困るものがありました。また質問の数が多く、もう少し項目を絞ってほしい

・質問件数が多いので大変ですが、勉強になった点もあります
・質問内容がとても曖昧だと感じました。集計結果にどれ程の意味があるのか疑問です。
・また全てラジオボタンでなくチェックボックスなどでまとめる等して、見た目だけでもわかり易くして欲しい
・質問内容の意図が伝わらない設問が散見されます。中小医療機関で標準レベルのセキュリティ施策がどう言う物なのかをシステム・ネットワークの知識が無い経営者へ理解させる事は困難ですしそこから費用を捻出する事は、不可能です。複数の省庁で複数の施策拠点に予算を投下するならば統一した機器の提供と監視サービスの実作業拠点を業界団体別に構築する方が国内のセキュリティレベルの底上げの近道であり知識の無い経営者層に最低限のコストがこれくらい必要であると言う認識を持たせる近道だと考えます
・正解がある質問(Q)については、正解と解説を公表してほしい
・設問が○○についてで小項目で賛成・反対とあるが、○○を導入状況なのかあるべき姿としてなのか、詳細がわからないものがあった
・設問が短く回答の選択に悩むケースがあった。Q7、Q53、Q83、Q49～は「実施している」と「賛成」の回答が混在するが、結果が大きく変わってしまうと思う。選択肢自体もニュアンスが混じっている
・設問はたいへん分かり易かったです。
・専任ではなく知識もあまりないため難しい質問もある。また、質問内容が本部管理のものも多いため現場レベルではわからないこともある
・専門性が高いのではないか
・専門的知識が無い為に質問の意図がくみ取れない部分があるのかもしれませんが、この類のアンケートでしばしば感じるのは、質問の文章そのものや、質問と回答の組み合わせなど、日本語として不自然な点です。もしかしたらコンピューターリテラシーと日本語リテラシーのギャップが、一般の人がコンピューターの専門家の言ってる意味がわからない原因ではないかと感じたりもします。厚生労働省のアンケートでさえこれですから、他は推して知るべしと思いました。その点の改善をご提案致します
・専門用語への解説があれば助かります
・選びにくい選択肢があった
・選択肢に『わからない』があったが『どちらでもない』の選択肢がほしい箇所があった
・全体を通してアンケートの意図がわかりにくい
・誰が担当してもわかるような初歩的な対策なども盛り込んでほしい。
・知識を問う設問は、参考 URL 等を付けて頂くと、理解が深まってよかったと思います。
・中立的な回答が無い。
・質問項目が多すぎる。質問の内容が、曖昧な部分もあり回答に困った。
・同じような項目が幾つもあり、簡潔明瞭なアンケートにしていただきたいと感じた。
・調査と教育的な面を別で実施していただけるとありがたいです。
・長すぎる！

・当方の知識を試されているようで、答えたくない部分も多かった　答えがない（はいでもいいえでもない）ものも多かった　病院会として取り組むべき喫緊の課題です
・同じような質問がありました。また、選択肢として選べないものも複数ありました。
・内容のわかりにくい設問がいくつかあった。知識レベルの低い担当者でもわかりやすい文面にしていただきたいと感じました。
・病院規模による管理レベルをわかりやすく解説してあるガイドラインをまとめてほしい。
・理想を答えればよいのか、現実を答えればよいのか、迷う質問があった。
・略語についての日本語による説明をお願いします。

第３章　まとめ

日本病院会会員施設におけるサイバーセキュリティへの意識や体制、対応事項について把握したが、このうち施設のセキュリティ対応に影響が大きいと考えられた施設規模、セキュリティ教育に着目して分析するとともに、今後の方向性を述べる。

１．病院規模別のセキュリティに対する意識や体制の違い

病院の病床規模別に、セキュリティに対する意識や体制の違いについて分析を行ったところ、規模が小さい病院ほど対応が進んでいない実態が把握された。

図表 110　病院の病床規模別のセキュリティ意識や体制の違い

①情報システム統括部署がない施設の割合
400 床以上の一般病院　7.0%
200 床～399 床の一般病院　20.6%
200 床未満の一般病院　44.6%

②資産管理ソフトを導入していない施設の割合
400 床以上の一般病院　32.0%
200 床～399 床の一般病院　47.6%
200 床未満の一般病院　70.7%

③セキュリティ教育を行っていない施設の割合
400 床以上の一般病院　16.9%
200 床～399 床の一般病院　32.1%
200 床未満の一般病院　36.4%

④セキュリティインシデント発生時の手順が定められていない施設の割合
400 床以上の一般病院　25.6%
200 床～399 床の一般病院　43.6%
200 床未満の一般病院　46.8%

＜今後の方向性＞

病院規模が小さいほどセキュリティ対応が進んでいない状況が把握されたが、部署の設置には担当する人材が必要であり、またソフト導入には費用がかかるなど、対応コストの負担がこれらの要因の一つとして考えられた。一方で、セキュリティ教育の実施やセキュリティインシデント発生時の手順を定めることについては、コストを抑えて取組むことも

できるのではないかと考えられた。このことから、病院の規模が小さいほどセキュリティ対応が進んでいない要因には、コスト負担という観点もあるが、根底には大規模病院と比べてセキュリティ対策の必要性に対する意識が低いことや、対応を進める上での知識が欠如していることが考えられた。

上記を踏まえた今後の方向性としては、中小病院におけるサイバーセキュリティに対する意識を向上させる施策が必要と考えられた。またコスト負担によらず実施可能な取組はあると考えられることから、対応を進める上で必要な知識を向上させる施策が必要と考えられた。

2．セキュリティ教育の効果と方向性

回答のあった施設全体について、セキュリティ教育の実施状況別に、セキュリティに関する４つの事項（以下の図表の①～④として記載の事項）への認知度について分析を行ったところ、セキュリティ教育を行っているところの方が、行っていないところよりもいずれの事項への認知度が高かったが、研修の実施回数と研修の形式については、４つの事項への認知度との関係において何らかの傾向はみられなかった。

図表 111　セキュリティ教育の実施状況とセキュリティに関する事項への認知度の関係

①Q75 NISC の３、２、１ルールでは３つのデータ、２つにバックアップ、１つのオフラインバックアップが提唱されていることについて知っている割合

- セキュリティ教育を行っている主体　44.7%
- セキュリティ教育を行っていない主体　33.5%
- セキュリティ教育の１年あたりの実施回数が１回　43.3%
- セキュリティ教育の１年あたりの実施回数が２回　47.3%
- 研修の形式が集合研修　47.1%
- 研修の形式が e-Learning 教材（自施設で作成）　48.6%
- 研修の形式が e-Learning 教材（外注、あるいは既成のもの）　46.5%

②Q76 NICT のサイバーセキュリティ研究所のデータでは IoT 機器の攻撃が半数以上であることについて知っている割合

- セキュリティ教育を行っている主体　25.2%
- セキュリティ教育を行っていない主体　18.2%
- セキュリティ教育の１年あたりの実施回数が１回　22.2%
- セキュリティ教育の１年あたりの実施回数が２回　33.3%
- 研修の形式が集合研修　25.2%
- 研修の形式が e-Learning 教材（自施設で作成）　29.9%

・　研修の形式が e-Learning 教材（外注、あるいは既成のもの）　22.1%

③Q77　国際医療機器規制当局フォーラム文書におけるサイバー攻撃対策について知っている割合

・　セキュリティ教育を行っている主体　6.7%
・　セキュリティ教育を行っていない主体　4.1%
・　セキュリティ教育の１年あたりの実施回数が１回　6.5%
・　セキュリティ教育の１年あたりの実施回数が２回　2.8%
・　研修の形式が集合研修　7.6%
・　研修の形式が e-Learning 教材（自施設で作成）　5.6%
・　研修の形式が e-Learning 教材（外注、あるいは既成のもの）　8.1%

④Q78 医療用 IoT 機器（モニター系機器が多い）は、５、６年のシステム更新後も使われるので設定変更忘れが危惧されることについて知っている割合

・　セキュリティ教育を行っている主体　53.0%
・　セキュリティ教育を行っていない主体　34.1%
・　セキュリティ教育の１年あたりの実施回数が１回　52.9%
・　セキュリティ教育の１年あたりの実施回数が２回　47.2%
・　研修の形式が集合研修　53.4%
・　研修の形式が e-Learning 教材（自施設で作成）　56.3%
・　研修の形式が e-Learning 教材（外注、あるいは既成のもの）　55.8%

＜今後の方向性＞

調査票で設定した 4 つの事項のみの認知度という前提であるが、セキュリティ教育を行っている施設の方が行っていない施設より認知度は高いが、セキュリティ教育の回数については多ければ認知度が必ず高くなるというものではなく、また研修の形式による認知度の違いは把握されなかった。

上記を踏まえた今後の方向性としては、セキュリティ教育を行うことで認知度が高まると考えられることから、セキュリティ教育を推進する施策が必要である。またセキュリティ教育の頻度については年間に１回は実施することが望まれるが、研修の形式についてはコスト面や職員の時間の拘束などの観点から、施設において対応しやすいものを選択することが良いと考えられる。

調　査　項　目

設問項目	選択肢
Q1　年齢	・10 代以下　・20 代　・30 代　・40 代　・50 代　・60 代　・70 代 ・80 代以上
Q2　あなたの保有している医療系の資格を選んでください。(複数回答可)	・医師　・歯科医師　・看護師　・保健師　・助産師　・薬剤師 ・臨床検査技師　・放射線技師　・作業療法士　・理学療法士　・言語療法士 ・診療情報管理士　・医学物理士　・臨床心理士　・精神福祉士 ・社会福祉士　・介護福祉士　・ケアマネージャー（介護支援専門員） ・なし　・その他
Q3　あなたの保有している情報系の資格を選んでください。(複数回答可)	・なし　・医療情報技師　・第一種情報処理技術者 ・初級システムアドミニストレータ・IT パスポート ・独立行政法人 情報処理推進機構（IPA）のセキュリティ関連の資格 ・AWS 認定資格、GCP(Google Cloud Platform)認定資格などのパブリッククラウドベンダーの資格 ・ネットワーク系ベンダーの認定する資格　・その他
Q4　ICT に関する所属学会・団体をお答え下さい（複数回答可）	・日本遠隔医療学会　・日本医療情報学会 ・ICT に関する学会・団体に未加入　・その他
Q5　所属機関をお答え下さい（複数回答可）	・医療機関 400 床以上の一般病院　・医療機関 399 床～200 床の一般病院 ・医療機関 200 床未満の一般病院　・医療機関 一般診療所 ・医療機関 上記以外　・介護機関　・大学（医学系）　・大学（医学系以外） ・研究機関　・行政機関　・医療系企業　・IT 企業　・その他企業　・その他
Q6　医療機関にお勤めの方は、施設の開設者についてお答え下さい	・国（大学病院を除く）　・大学　・公的医療機関　・社会保険関係団体 ・医療法人　・公益法人等　・個人　・その他
Q7　所属機関が提供している医療 ICT に関するサービスや業務、製品（複数回答可）	・オンライン診療　・遠隔モニタリング　・遠隔画像診断　・遠隔病理診断 ・電子カルテ　・クラウド電子カルテ（クリニック等） ・PHR（パーソナルヘルスレコード）　・医用画像機器・システム ・検査機器・システム　・モニタリング機器・システム　・その他
Q8　職場での立場	・組織の管理者（理事長、院長含む）　・情報担当責任者　・事務系職員 ・医療系職員　・企業系システム設計・開発者　・企業系システム保守担当 ・その他
Q9　情報システムを統括する部署はありますか	・はい　・いいえ
Q10 情報システムを統括する部署がある場合、部署には何人所属していますか？人数を答えて下さい。(非常勤・派遣も含む。トナーや端末交換などの単純作業の請負職員は除く)	（数値入力のため、選択肢はなし）
Q11 情報セキュリティ対策を行う担当部署があれば教えてください	・総務部門　・医事部門　・情報システム統括部署 ・そのような部署はない　・その他
Q12 担当部署がある場合、情報セキュリティの担当者はいますか	・専任の担当者がいる　・兼務の担当者がいる　・担当者は決まっていない ・わからない　・その他
Q13 担当者がいる場合、何人いますか　(1) 常勤の専任者の人数をお答え下さい	（数値入力のため、選択肢はなし）
Q14 担当者がいる場合、何人いますか　(2)常勤の兼務者の人数をお答え下さい	（数値入力のため、選択肢はなし）

設問項目	選択肢
Q15 担当者がいる場合、何人いますか (3)非常勤の専任者の人数をお答え下さい	（数値入力のため、選択肢はなし）
Q16 担当者がいる場合、何人いますか (4)非常勤の兼務者の人数をお答え下さい	（数値入力のため、選択肢はなし）
Q17 「医療情報システムの安全管理ガイドライン」にある CSIRT（Computer Security Incident Response Team＝セキュリティインシデント発生時に対応する専門チーム）はありますか	・ある　・ない　・検討中　・知らなかった
Q18 CSIRT を組織化する場合どのように作りますか	・院内でチームの結成　・専門家を雇用する　・委託する ・予算的に対応できない　・人材が見つからず対応できない ・両者の理由で対応できない　・その他
Q19 導入している情報システムについて教えてください（複数回答可）	・電子カルテシステム　・医事会計システム ・オーダーエントリーシステム　・放射線画像システム ・事務システム（院内システム）　・事務システム（クラウド） ・往診・訪問看護システム　・介護システム　・その他
Q20 院内から職員がインターネットを利用していますか	・電子カルテ等の診療記録を扱う端末から利用可能 ・電子カルテ等とは別のネットワーク（無線含む）を用意して利用可能 ・院内からは私物の携帯等を利用　・利用できない
Q21 院内から、インターネットで、どのようなサービスを利用していますか（複数回答可）	・ホームページを閲覧している　・電子メールを利用している ・クラウドのグループウェアを利用している　・SNS を利用している ・その他
Q22 インターネットにアクセスするパソコン（PC）について（複数回答可）	・診療系の PC からアクセスできる ・事務系（医事会計は除く）の PC からアクセスできる ・インターネット専用の PC からアクセスできる
Q23 職員（医師など）の私物の PC を用いての業務は許可していますか	・診療業務での利用を許可している ・診療業務以外（事務や研究等）での利用を許可している ・診療・事務・研究業務での利用を許可している　・許可していない
Q24 職員の私物の PC のネットワーク接続を許可していますか	・診療系ネットワークへの接続を許可している ・事務、研究系ネットワークへの接続を許可している ・診療、事務、研究系ネットワークへの接続を許可している ・私物 PC 専用のネットワークへの接続を許可している ・許可していない
Q25 ウィルス対策ソフトを導入していますか	・はい　・いいえ　・わからない
Q26 資産管理ソフトを導入していますか（組織内の PC を一元的に管理するソフト（例：SKYSEA など))	・はい　・いいえ　・わからない
Q27 仮想ブラウザを導入していますか（仮想環境でインターネットに接続する仕組み）	・はい　・いいえ　・わからない

設問項目	選択肢
Q28 セキュリティ教育を行っていますか	・はい　・いいえ　・わからない
Q29 セキュリティ教育を行っていると回答された方へ、年に何回行っていますか	（数値入力のため、選択肢はなし）
Q30 セキュリティ教育を行っている場合、どのような研修を行っていますか（複数回答可）	・集合講習　・e-Learning 教材（自施設で作成） ・e-Learning 教材（外注、あるいは既成のもの）　・その他
Q31 外部セキュリティ監査を受けていますか　直近 3 年以内の状況をお聞かせください	・受けている　・受けていない　・わからない
Q32 ペネトレーションテストを受けていますか（インターネット接続を通じた施設内ネットワークへの侵入テスト）直近 3 年以内の状況をお聞かせください	・受けている　・受けていない　・わからない
Q33 セキュリティ訓練を実施していますか（標的型メール訓練等）直近 3 年以内の状況をお聞かせください	・はい　・いいえ　・わからない
Q34 情報セキュリティポリシーを規定していますか	・はい　・いいえ
Q35 医療機関の場合だけ、お聞きします。厚生労働省の「医療情報システムの安全管理に関するガイドライン」についてお聞きします	・参照して対策を立てている　・読んだことがある　・名前は知っている ・知らない
Q36 セキュリティインシデント発生時の手順がありますか	・はい　・いいえ
Q37 職員がセキュリティインシデントを発見したときに報告する部署はありますか	・報告先は決まっている　・決まっていない　・わからない
Q38 情報セキュリティインシデント発生時はどこに報告しますか	・CSIRT　・情報セキュリティ対策部門に報告する　・情報部門に報告する ・上長に報告する　・その他
Q39 情報セキュリティに関する職員の相談先（組織内）について教えてください（複数回答可）	・CSIRT　・情報セキュリティ対策部門　・情報部門　・システム業者 ・職場内の詳しい人　・決っていない　・その他
Q40 情報セキュリティインシデント発生時の厚生労働省の窓口を知っていますか	・知っている（報告したことがある） ・知っている（報告する事例が発生したことはない）　・知らない

設問項目	選択肢
Q41 所属機関のサイバーセキュリティの課題は何ですか（複数回答可）	・メール添付ウイルス侵入　・メール URL からのウイルス侵入 ・ホームページからのウイルス侵入 ・外部ネットワークからの侵入（ハッキング） ・外部ネットワークの監視　・情報の漏洩　・職員の知識不足 ・幹部の意識が低い　・設備が不十分　・重要データのバックアップ ・重要データアクセスの監視 ・ネットワークセキュリティのための必要最低限の設定 ・ネットワーク監視　・その他
Q42 情報セキュリティに関する情報源をお答え下さい（主要なもの　3 つ以内）	・厚生労働省のホームページ　・経済産業省のホームページ ・総務省のホームページ ・内閣サイバーセキュリティセンター（NISC）のホームページ ・一般財団法人 医療情報システム開発センター（MEDIS-DC）のホームページ ・独立行政法人 情報処理推進機構（IPA）のホームページ ・国立研究開発法人 情報通信研究機構（NICT）のホームページ ・National Institute of Standards and Technology（NIST 米国）のホームページ ・一般社団法人保健医療福祉情報システム工業会（JAHIS） ・有償・無償で契約している企業等から　・新聞、雑誌、書籍 ・インターネット　・入手していない　・その他
Q43 他の施設の対策状況は、貴施設が対策を立てる上で参考になりますか	・大いに参考になる　・興味があり、知りたい　・どちらでもない ・興味はない　・まったく参考にならない
Q44 最近のサイバーテロの目的について、どのようなものがあるでしょうか（複数回答可）	・個人情報の取得　・システム停止　・業務停止　・情報に対する金銭要求 ・業務に対する金銭要求　・その他
Q45 どのようなサーバー攻撃方法の侵入経路を想定しているでしょうか（複数回答可）	・利用者の ID、パスワード取得、認証の詐称　・ファイアウォール DDoS 攻撃 ・ウイルス対策ソフト、ウイルス検知（IDS、IPS）のすり抜け ・USB など媒体経由　・個人 PC から侵入　・部内無線 LAN への侵入 ・部内ネットワークへの接続　・ファイアウォールの設定ミス ・ファイアーウオール、VPN、ネットワーク機器のゼロデイ攻撃 ・ファイアーウオール、VPN、ネットワーク機器の脆弱性 ・ファイアーウオール、VPN、ネットワーク機器の管理者権限詐称 ・EDR のすり抜け　・その他
Q46 サイバーセキュリティを脅威と感じているか、対策を検討しているか、問題は何か？（最も当てはまるものを選んで下さい）	・脅威と感じている ・脅威と感じているが対策していない（対策できる人材がいない） ・脅威と感じているが対策がわからない ・脅威と感じているが対策できる人材がいない ・脅威と感じているが対策の経費が出せない ・脅威を感じていない。身近な問題と考えていない
Q47 インシデント発生時の対応について	・組織内で対応する　・委託契約している　・委託先を探す ・IPA に依頼する　・NISC に依頼する
Q48 インシデント発生以前の事前調査として	・院外接続状況を病院の情報部門あるいは CSIRT で把握することは重要と思う ・保守契約して入れば各部署に任せることで良い
Q49 メール添付ファイルについて	・制限しない　・マクロファイルは通過させない ・暗号化圧縮ファイルは通過させない　・その他
Q50 ホームページ閲覧	・制限しない　・危険なものを接続させない　・安心なもののみ接続させる
Q51 医療情報システムの安全管理ガイドラインの記載の CSIRT 組織化について	・なし　・部内　・専門家の雇用　・委託　・その他

設問項目	選択肢
Q52 医療情報システムの安全管理ガイドラインの添付されたサイバーセキュリティに関するチェックリスト、フローをご存じですか	・実施した　・知っているが未実施　・知らない
Q53 事前調査、監視（複数回答可）	・外部接続の調査（情報システムのみ） ・外部接続の調査（地域連携、遠隔読影、オンライン研究） ・外部接続の調査（放射線部、検査部など大型機器のオンライン保守） ・ファイアウォール、VPN の機器リスト、ソフトのバージョン ・ネットワークの機器リスト、ソフトのバージョン ・サーバの機器リスト、ソフトのバージョン　・各サーバの端末配置 ・保守契約書内容確認　・その他
Q54 システムの保守回線・CT・MRI 等の検査機器の保守回線の詳細（機種名、ソフトバージョン）	・病院として把握すべき　・委託先に任せて病院は把握しないでよい ・病院として把握しても日々刷新される脆弱性情報の対応はできない ・病院として把握しても日々刷新される脆弱性情報の対応は委託で対応したい
Q55 地域連携・遠隔病理診断・遠隔画像診断・オンライン治験接続について	・情報部門あるいは CSIRT で接続の詳細を把握している ・各部署に任せている　・その他
Q56 オンライン診療・遠隔モニタリング・院内 SNS の接続について	・情報部門あるいは CSIRT で接続の詳細を把握する　・各部署に任せる
Q57 匿名化してオンライン接続する遠隔画像診断・匿名化してオンライン接続する調査等の接続について	・情報部門あるいは CSIRT で接続の詳細を把握する　・各部署に任せる
Q58 利用者のホームページ閲覧、メール受信について	・電子カルテネットワークとは別のネットワーク・PC を利用する ・電子カルテネットワーク内に仮想ブラウザ（ダーティシンクライアント）を用意して、Web メール、ホームページ参照可能にしている ・電子カルテ端末から Web メール、ホームページ参照可能にしているが、ウイルス対策ソフトにて管理している。ホームページのアクセス制限をしている ・電子カルテ端末から Web メール、ホームページ参照可能にしているが、ウイルス対策ソフトにて管理している。ホームページのアクセス制限はしていない
Q59 院内ネットワーク全体図の作成はされているか	・多くのネットワークが異なったベンダーにより形成されており全体図はない ・多くのネットワークが異なったベンダーにより形成されているが、病院として作成している ・多くのネットワークが異なったベンダーにより形成されているが、ベンダーに依頼して作成している ・ネットワークを 1 つのベンダー契約にし、統一管理している ・ネットワーク、仮想サーバを一つのベンダー契約にして統一管理している ・ネットワーク、仮想サーバ、仮想ストレージを一つのベンダー契約にして統一管理している ・ネットワーク、仮想サーバ、仮想ストレージ、ソフトウェア全てを一つのベンダー契約にして統一管理している　・その他
Q60 電子カルテシステム・部門システムそれぞれについて院内の管理者・担当者一覧を作成しているか	・作成している（各部署の管理者・担当者を示している） ・作成していない（院内のことなので、皆知っている） ・作成していない（未検討だった）

設問項目	選択肢
Q61 電子カルテシステム・部門システムの構築・運用事業者の連絡先一覧を作成しているか	・作成している　・作成していない（システム担当者が連絡先を知っている） ・作成していない（未検討だった）
Q62 端末への EDR（Endpoint Detection and Response）	・導入している　・導入していない　・わからない
Q63 端末への EDR について	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q64 内部ネットワーク監視する	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q65 内部サーバーを監視する	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q66 端末からサーバを守るためにシンクライアント基盤の導入	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q67 仮想ブラウザ（ホームページ、Web メール参照用の仮想サーバを用意）経由のインターネット参照	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q68 組織内のサーバハード系を仮想サーバ、仮想ストレージ、仮想ネットワーク等を用いて病院あるいは委託契約にて統一導入管理を行う	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q69 組織内のサーバハード系をクラウドサーバ等を用いて病院あるいは委託契約にて統一導入管理を行う	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q70 データを暗号化された PC、サーバに必ずウイルスは見つかる	・正しい　・間違い
Q71 A さんからウイルス添付メールが届いた場合、A さんの PC はコンピュータウイルスに感染している	・正しい　・間違い
Q72 Windows のアクティブディレクトリやバックアップの設定ファイルは攻撃される	・正しい　・間違い
Q73 大容量のファイル全体の暗号化は時間がかかるので一部の暗号化をするものもある	・正しい　・間違い
Q74 攻撃を受けた場合に IPA、NISC に対応、助言する窓口がある	・正しい　・間違い

設問項目	選択肢
Q75 NISC の 3、2、1 ルールでは 3 つのデータ、2 つにバックアップ、一つのオフラインバックアップが提唱されている	・知っている　・知らなかった
Q76 NICT（情報通信機構）のサイバーセキュリティ研究所のデータでは IoT 機器の攻撃が半数以上である	・知っている　・知らなかった
Q77 国際医療機器規制当局フォーラム（IMDRF）文書におけるサイバー攻撃対策について	・知っている　・知らなかった
Q78 医療用 IoT 機器（モニター系機器が多い）は、5、6 年のシステム更新後も使われるので設定変更忘れが危惧される	・知っている　・知らなかった
Q79 RAID によるリアルタイムの保存	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q80 RAID 以外にリアルタイムのバックアップを用意する	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q81 遠隔地にリアルタイムのバックアップをする	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q82 ジュークボックス型の磁気テープユニットによる日々のバックアップ	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q83 SS-MIX フォルダーから地域連携サーバが pull する仕組みで地域連携側にバックアップできる	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q84 ストレージベンダーが用意するバックアップで、削除等は特別な方法を用いる	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q85 管理者のサーバ等の管理に用いる PC とメール・ホームページ参照の PC とは別の機器、別のネットワークを用いる	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q86 委託業者の院外からの接続は事前に時間等を連絡させ、時間、接続先を限定する	・賛成　・反対　・賛成するが経費上難しい　・わからない

設問項目	選択肢
Q87 委託業者の院外からの接続は事前に時間・接続先等を連絡させファイアウォールの接続を制限する	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q88 委託業者の院外からの接続はリモートアクセス、シンクライアントなどを用いて直接接続させない	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q89 委託業者が、院内にファイルを取り込む場合、院内から取り出す場合に記録を残す	・賛成　・反対　・賛成するが経費上難しい　・わからない
Q90 流行しているマルウェア（ウィルス）等、リスク関連の情報	・多いに期待する　・期待する　・どちらでもない　・期待しない ・全く期待しない
Q91 セキュリティ対策の具体的な実施方法	・多いに期待する　・期待する　・どちらでもない　・期待しない ・全く期待しない
Q92 マルウェア検体の分析	・多いに期待する　・期待する　・どちらでもない　・期待しない ・全く期待しない
Q93 セキュリティ教育教材の提供	・多いに期待する　・期待する　・どちらでもない　・期待しない ・全く期待しない
Q94 情報共有の手段について	・電子メール等による定期的な情報提供 ・ワークショップ・活動報告会等による対面での情報共有 ・情報共有・掲示板ツールによるオンラインでの情報共有　・その他
Q95 知識レベルが同じではないので、技術的指導者が必要（誰でも参加できるか、一定以上の知識レベルの人に限るか）	・必要　・不要
Q96 共有するべき情報には噂、予想なども含む必要があり、公表できにくいものがあると思う（サイバーセキュリティは繋がっている限り絶対に安全と言えるものはないので技術の理解が必要との意見もある）	・賛成　・反対（全て公表すべき、あるいは、そのような情報は流さない）
Q97 組織のあり方について（米国に医療系 ISAC は関係者が集まって組織化された。韓国の医療系 ISAC は政府が主導している）	・ボランティア的に関係者で集まって作る ・日本では中小医療機関が多く、人材も少ないので政府の主導が必要 ・その他
Q98 サイバーセキュリティ情報の公的共有組織に必要な要素についてのお考えを教えてください。一番重要と思うものはどれでしょうか？	・匿名性（情報提供元や相談元の匿名化など） ・迅速性（迅速な情報提供など） ・具体性（対策方法や、情報提供内容が具体的であることなど） ・独立性（規制当局から独立した運営）

設問項目	選択肢
Q99 サイバーセキュリティ情報の公的共有組織に必要な要素についてのお考えを教えてください。二番目に重要と思うものはどれでしょうか？	・匿名性（情報提供元や相談元の匿名化など） ・迅速性（迅速な情報提供など） ・具体性（対策方法や、情報提供内容が具体的であることなど） ・独立性（規制当局から独立した運営）
Q100 サイバーセキュリティ情報の公的共有組織に必要な要素についてのお考えを教えてください。三番目に重要と思うものはどれでしょうか？	・匿名性（情報提供元や相談元の匿名化など） ・迅速性（迅速な情報提供など） ・具体性（対策方法や、情報提供内容が具体的であることなど） ・独立性（規制当局から独立した運営）
Q101 サイバーセキュリティ情報の公的共有組織に必要な要素についてのお考えを教えてください。重要性が最も低い（四番目）と思うものはどれでしょうか？	・匿名性（情報提供元や相談元の匿名化など） ・迅速性（迅速な情報提供など） ・具体性（対策方法や、情報提供内容が具体的であることなど） ・独立性（規制当局から独立した運営）
Q102 サイバーセキュリティ情報を共有するサービスを提供する公的組織がありましたら、参加しますか	・ぜひ参加する　・参加を検討する　・必要性を感じない　・条件による
Q103 上の質問で条件によると回答した方は、具体的な条件を記載下さい	（自由記述のため、選択肢はなし）
Q104 医療分野のサイバーセキュリティやヘルスケア ISAC に関する意見がありますか（自由記述）	（自由記述のため、選択肢はなし）
Q105 本アンケートについて意見や提案などありますか（自由記述）？ 例えば質問内容の改善等のご提案をお願いします。	（自由記述のため、選択肢はなし）