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 3 年度報告　「課題抽出のためのアンケートの設計と試験的実施」

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

医療機関に於けるサイバーセキュリティの実情は深刻であり、一般的な病院がランサムウェアなどの被害を受ける事案が発生している。サイバーセキュリティに関する専門技術を有する人材のニーズは高いが、多くの医療機関では人材確保が不可能である。

ヘルスケア ISAC の設立に関する課題調査、それに留まらない課題抽出について、多数の病院を対象に調査することとなった。その前段階として、小規模な対象にアンケートして、本格的調査の準備を行った。

医療機関に於けるサイバーセキュリティの管理体制を調べるために、組織で実施しているセキュリティ対策、施設内の規定、セキュリティインシデント発生時の対応、侵入対策やウイルス対策の状況、サイバーセキュリティ対策への意識や理解度などを 106 問の設問にまとめた。これだけ設問数が多い、負担感の大きいアンケートにも関わらず全対象者の約 1 割 9%が回答した、サイバーセキュリティに関するリテラシーの高さ存在を感じされた。

A．研究目的

1．研究の背景

医療機関に於けるサイバーセキュリティの実情は深刻であり、既に日常診療にあたる一般的な病院がランサムウェアなどの被害を受ける事案が複数、発生している。サイバーセキュリティに関する専門技術を有する人材のニーズは高いが、人数が非常に限られており、多くの医療機関では人材確保が不可能である。各施設で医療情報システム運営を担当する職員は不安を抱えているが、人材や資金の大きな不足により、十分な対策を打てない。

一方で各施設の実情、詳細な情報が明らかではない。下記の要因により、詳細な調査が行われなかったと考えられる。

① 専門技能を有するスタッフの大幅な不足により、各施設の情報や技能の不足は調べるまでもなく明白であり、対策も実施されていないとの思い込みがある。

② アンケート調査では、回答者の負担を軽減しないと回答率が低下すると恐れて、意図的に設問数が減らす。そのため、サイバーセキュリティへの知識不足、不安などの回答は得られるが、“何の知識が不足しているか”、“何が不安なのか”、具体的情報に調査が踏み込まない。

③ そもそもサイバーセキュリティに関する共通認識が未形成であり、正当な情報源も少なく、専門性の高い人々でも誤解や誤認識が多い。異なる思い込みの集団が併存している。

④ サイバーセキュリティの課題として、何を捉えたいか、調査者も意識が定まっていない。技術的知識のレベルを問いたいのか、マネジメント上の課題を問いたいのか、調査目的が不明確な研究が多い。

先行研究として、2020 年度厚生労働行政推進調査事業で医療分野に於ける情報共有の試み、ヘルスケア ISAC の設立に関する意識調査を医療 ICT の関係者に対して実施した[1]。ISAC 自体が知られていないため、限定的な調査として、日本遠隔医療学会会員を対象として、2021 年 3 月に実施した。その経験を元に、次の研究段階として、本研究を実施して、ISAC に留まらず、医療情報システムやネットワークの管理に関する意識調査を行うこととした。

本研究の初期（2021 年半ば）には、ヘルスケア ISAC の設立に関する課題調査が主要な狙いだったが、年度半ばに 10 月につる

ぎ町立半田病院に対してランサムウェアによる医療情報システム破壊事件が発生して、ISAC 結成に留まらず、医療機関のサイバーセキュリティ能力向上に社会的関心が高まった。そのため本研究も、ISAC 結成に留まらない課題抽出を、日本遠隔医療学会などの限定的対象に留めず、多数の病院を対象に調査することとなった。ただし、いきなり大規模な調査研究を実施できないので、まず調査課題を設計し、小規模な対象にアンケートして、本格的調査の準備を行った。

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ことで、社会的課題を網羅的に把握することが期待される。しかしサイバーセキュリティに関する社会的課題の構造的視点は未確立であり、事件や事故の発生の度に認識を改めている現状がある。半田病院の事件さえ、ウイルス感染やファイアウォール破りに留まった社会的認識を、ランサムウェア犯罪への危機感まで高めたが、制度や政策などサイバーセキュリティに関する社会的課題の構造（許されること・許されないこと、技術評価など）の構築に至っていない。

評価尺度が未確立な中での調査は、探索的調査にならざるを得ず、社会的意義を持つには、公的に重視される対象者集団で、多数の回答を得ることが求められる。ランサムウェア被害の発生などに伴い、問題意識を高く持った一般社団法人日本病院会の協力を得ることとなった。ただし、いきなり日本病院会の会員施設を対象とした調査はできないので、先行研究と同じく、一般社団法人日本遠隔医療学会で試験を続けることとした。2021 年度研究では、日本遠隔医療学会での試験的調査まで行う。

3．調査内容

狙いはサイバー犯罪に対峙する能力の調査である。高度なサイバーセキュリティ対策技術、優れた技能教育手法などの試みの探索などでない。そこで医療機関に於けるサイバーセキュリティの管理体制を調べるために、以下のような課題群を設定して、それらを明かにする設問集を作りこととした。

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

なお,対象施設の“公的見解”としての調査ではなく、あくまで回答者の私見を問うこととした。社会的課題の構造が未確立なので、“公式見解”をまとめにくいと考えた。

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、先行研究［1]と同様に GoogleForm を用いた WEB アンケートとした。

2．設問製作

（1）製作者

近藤博史研究代表者が製作した。研究代表者は日本医療情報学会医療情報技師研修・試験制度担当、鳥取大学医学部附属病院での医療情報部長、鳥取県の地域医療情報連携ネットワーク“おしどりネット”、日本 IHE 協会など、技術的知識と現場マネジメント経験の蓄積に裏打ちされた経験を活かした。

（2）設問数

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）設問の工夫

曖昧に“不安”、“問題意識が高い”などを結論としないために、やむを得ず 106 問を設けたが、たいへん多いと認識している。そこで回答者の意欲が続くように、“クイズの

ように回答する”、“学習になる”などの設問を、「最近のサイバー攻撃に対する理解度」を問う 9 課題を準備した。他にも、設問に回答することが、セキュリティに関する認識の向上につながるように工夫した。

3．アンケート実施
（1）回答依頼の案内
日本遠隔医療学会会員メーリングリストを用いて、アンケートへの協力を依頼した。

⑵調査期間　2022 年 3 月 20 日～25 日
　この間、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発信した。

⑶対象者数は、メーリングリストの有効メールアドレス 506 件

⑷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　46 件（9.1%）

2．回答の概要
⑴先行研究と近い傾向があった。
①医師が最も多い（41.3%）
②医療情報技師やサイバーセキュリティ関連の有資格者は少なかった。(8.6%)
⑶回答者所属機関では、大学が多かった（45.7%以上）。医療機関は 200 床以上の病院と診療所が多かった。

⑵今回から入れた設問について
　組織での対策、規定やインシデント対応、所属機関での技術的対策、技術や管理的事項への理解など、知識や情報の質や量にばらつきはあるが、状況に通じた対策を取っている回答が多かった。
　日本遠隔医療学会の会員は医療 ICT に関する情報が恵まれた環境にあると考えられるが、所属機関全体で技術レベルが高いとは限らない。各施設の状況は、それほど悪くないと考えられる。

3．考察
　アンケートの回答率は、低かった先行研究（106 件、21%）より、更に低下して、46 件で 9.1%である。設問数が先行研究の 21 問から 5 倍になったことで、回答への協力が低下したと考えられる。
　逆に、これだけ設問数が増えて、負担感の大きいアンケートにも関わらず 9%の会員が回答したとの前向きな考え方ができる。特に学会員は、医療情報システムの管理部門の職員が多いと限らない。回答にはサイバーセキュリティに関するリテラシーの存在を感じされ、意識の高さから最後まで回答したと推測される。それだけのリテラシーを有する回答者が 10%弱は存在したと考えられる。逆に回答しなかった 9 割の会員には、同水準のリテラシーを期待できない可能性がある。それが「サイバーセキュリティについて、全体では低水準で、調査するまでもない」との状況の恐れがある。
　回答への負担が大きなアンケートだが、課題抽出には、この形態が必要であり、日本遠隔医療学会会員へのテスト調査でも結果が得られている。この設問群で、次の調査に臨みたい。

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**

Ｄ．健康危険情報
なし

Ｅ．参考文献
[1] 近藤博史、オンライン診療・遠隔医療や「非接触」を念頭に置いた ICT 化の中で医療機関が具備すべきサイバーセキュリティ対策や技術を踏まえたサイバーセキュリティ指針の策定（厚生労働科学研究成果データベース）、https://mhlw-grants.niph.go.jp/project/145932、2023 年 5 月 5 日検索

令和３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4年（2022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 3 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)

（２）研究課題

医療分野の情報化の推進に伴う医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究

（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。

２．事業実施概要

（１）実施体制

・研究代表者

鳥取大学医学部附属病院医療情報部教授　近藤博史

・担当研究者（研究分担者）

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
スタッフ　麦谷由香

（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

日本遠隔医療学会のメーリングリスト登録者全員（学会員：約 600 人）。

（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 3 月 20 日～25 日

（５）設問数

106 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-Q48】
⑤侵入経路の対策として実施している事項等	【Q49-Q61】
⑥ウイルス対策の状況	【Q62-Q65】
⑦サイバーセキュリティ対策への意見	【Q66-Q69】
⑧最近のサイバー攻撃に対する理解度	【Q70-Q78】
⑨重要データの保存について実施している事項	【Q79-Q84】
⑩情報部門の管理について	【Q85-Q89】
⑪ISAC について情報共有したい事項等	【Q90-Q103】
⑫その他意見	【Q104-Q106】

（7）回収者数

回答者数は 46 人である。

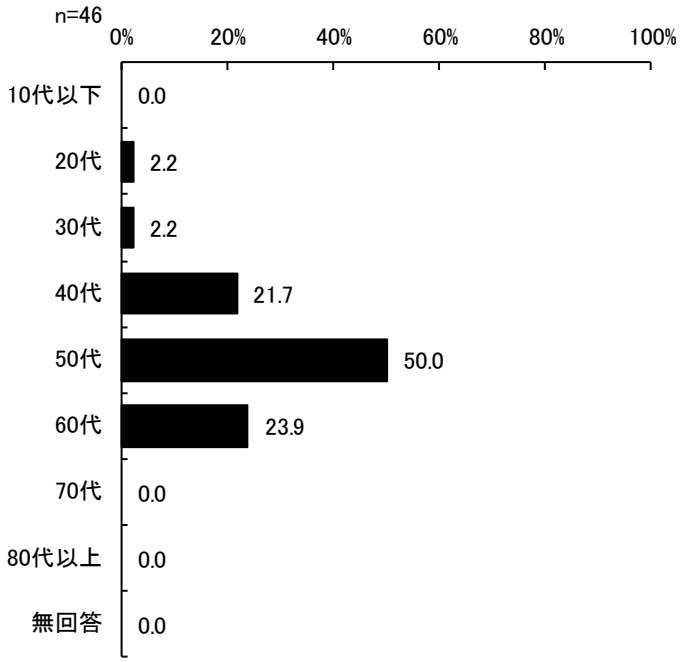
２．調査結果

（１）回答者の基本属性

1）年齢

年齢については、50 代が 50.0％で最も割合が高く、ついで 60 代が 23.9％であった。

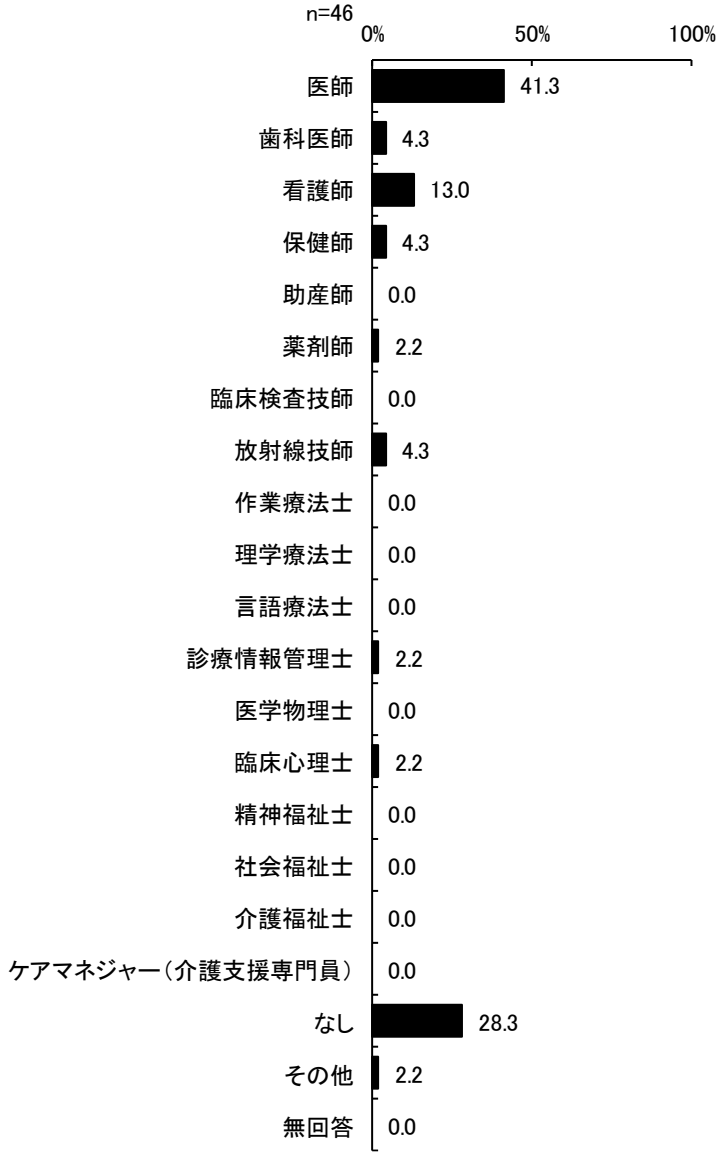
図表１　年齢（Q1）



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、医師が 41.3%で最も割合が高く、ついで「なし」が 28.3%、看護師が 13.0%であった。

図表 2　保有している医療系の資格（Q2）【複数回答】

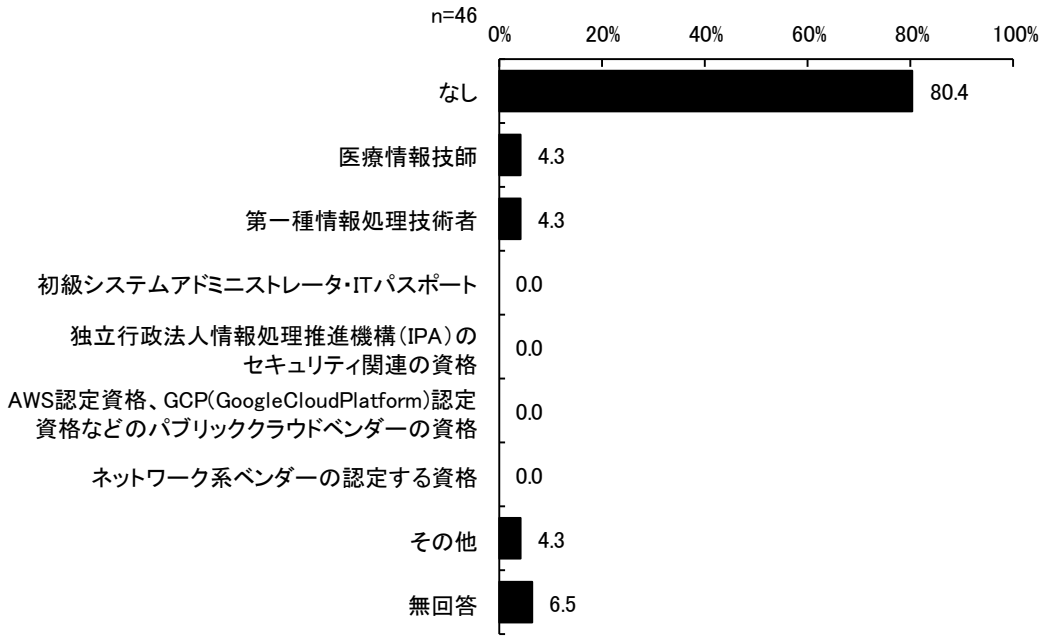


※「その他」の主な回答は以下の通り。
・臨床工学技士

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 80.4%で最も割合が高く、ついで医療情報技師、第一種情報処理技術者、その他がいずれも 4.3%であった。

図表 3　保有している情報系の資格（Q3）【複数回答】

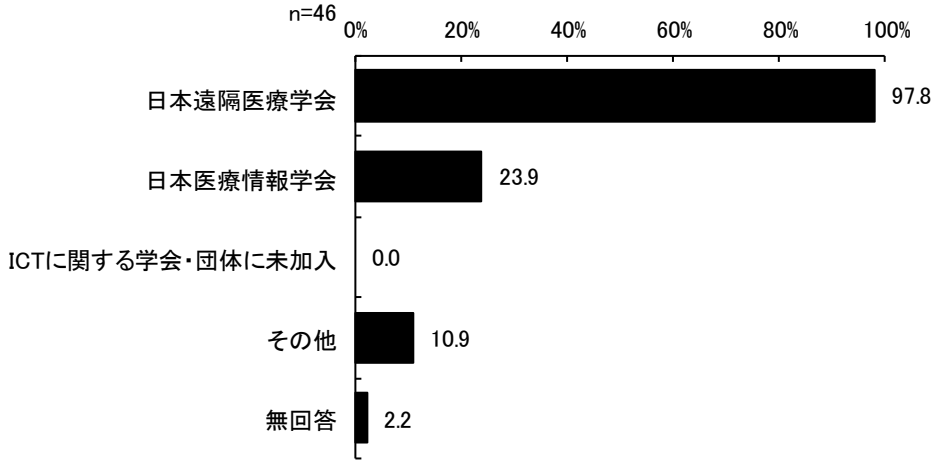


※「その他」の主な回答は以下の通り。
- 診療放射線技師
- IS027001 審査員補

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、日本遠隔医療学会が 97.8％で最も割合が高く、ついで日本医療情報学会が 23.9％であった。

図表 4　ICT に関する所属学会・団体（Q4）【複数回答】



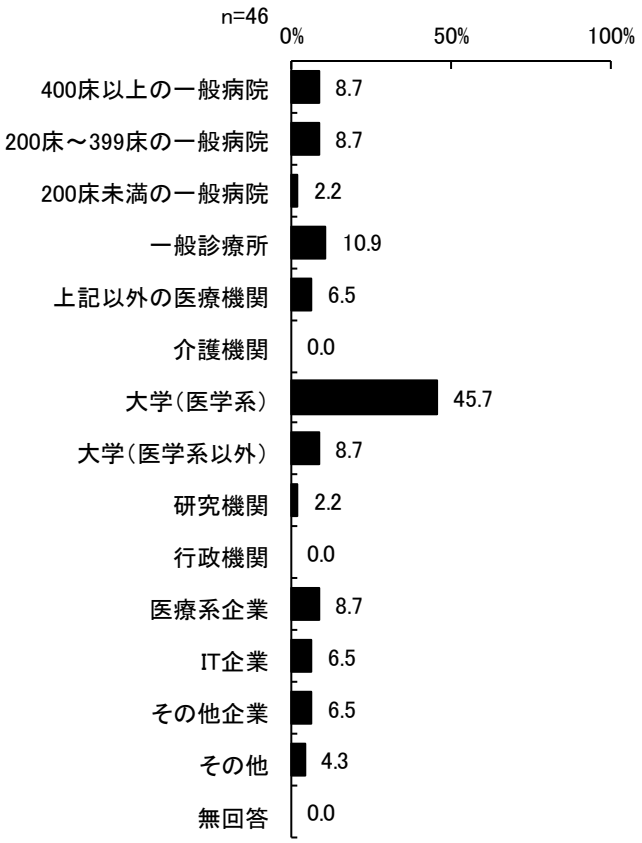
※「その他」の主な回答は以下の通り。

- IEEE
- 情報処理学会
- 電子情報処理学会
- 日本デジタルパソロジー研究会
- 日本診療情報管理学会
- 日本放射線技師会

5）所属機関

所属機関については、大学（医学系）が 45.7%で最も割合が高く、ついで一般診療所が 10.9%であった。

図表 5　所属機関（Q5）【複数回答】

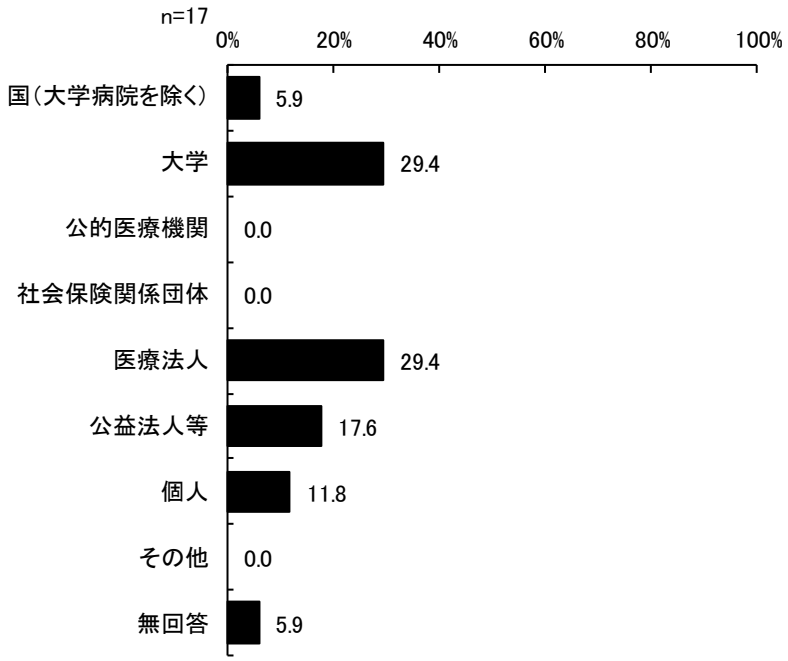


※「その他」の主な回答は以下の通り。
・訪問看護ステーション

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、大学および医療法人がいずれも 29.4%で最も割合が高く、ついで公益法人等が 17.6%であった。

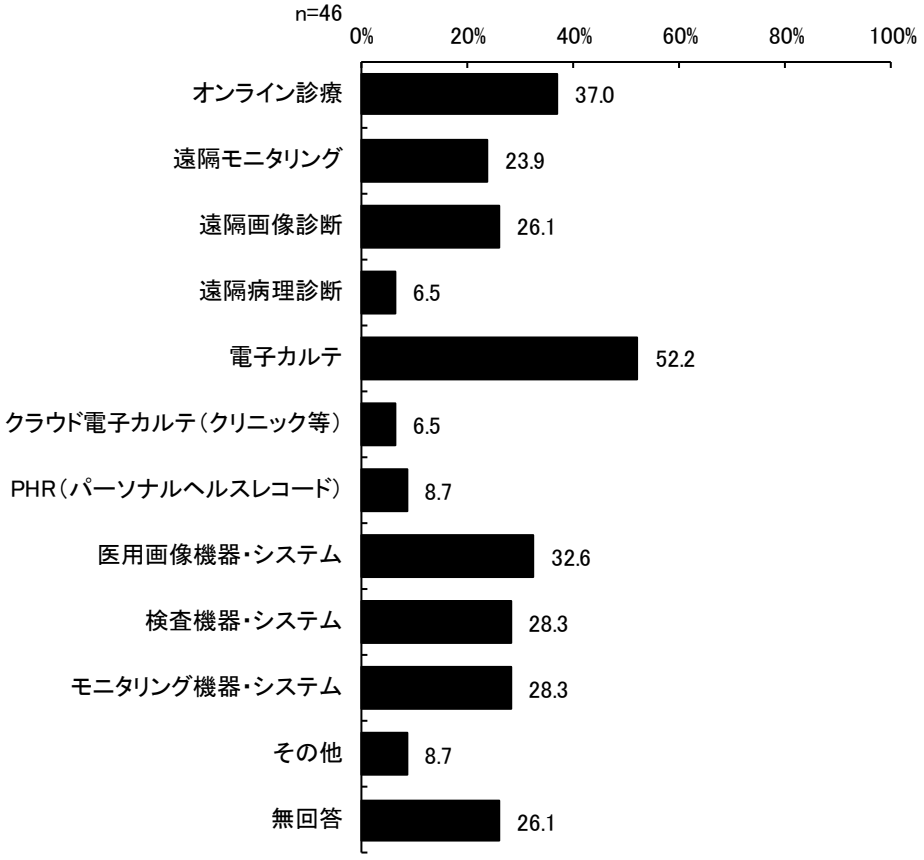
図表 6　施設の開設者（医療機関の場合）（Q6）



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 52.2%で最も割合が高く、ついでオンライン診療が 37.0%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】

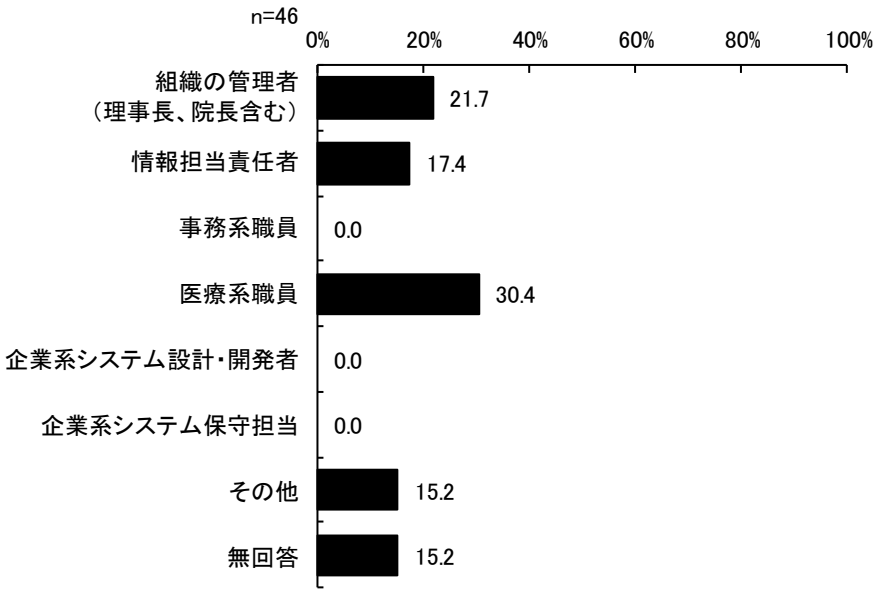


※「その他」の主な回答は以下の通り。
- オンライン授業
- 遠隔看護
- なし

8）職場での立場

職場での立場については、医療系職員が 30.4％で最も割合が高く、ついで組織の管理者（理事長、院長含む）が 21.7％であった。

図表 8　職場での立場（Q8）

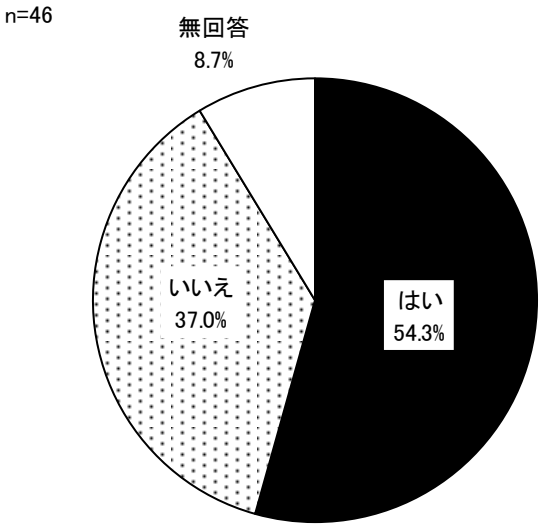


※「その他」の主な回答は以下の通り。
- 機械設計、ソフト設計を担当
- 市場調査を担当
- 大学教授
- 教員
- 講師

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 54.3%であった。

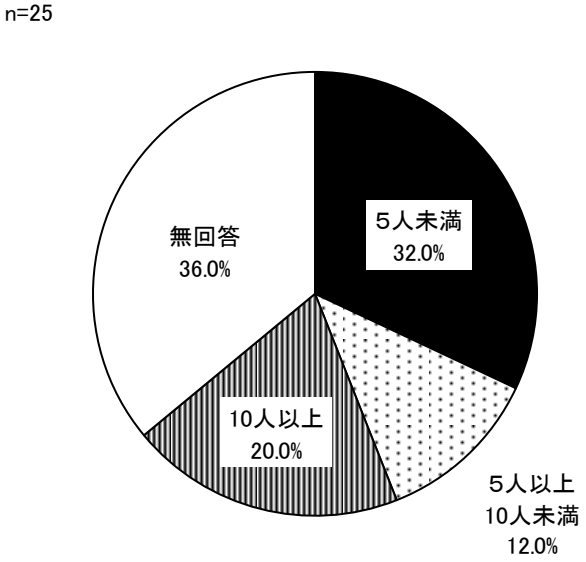
図表 9　情報システムを統括する部署はあるか（Q9）



10）情報システムを統括する部署への所属人数

情報システムを統括する部署への所属人数については、5 人未満が 32.0%で最も割合が高く、ついで 10 人以上が 20.0%であった。

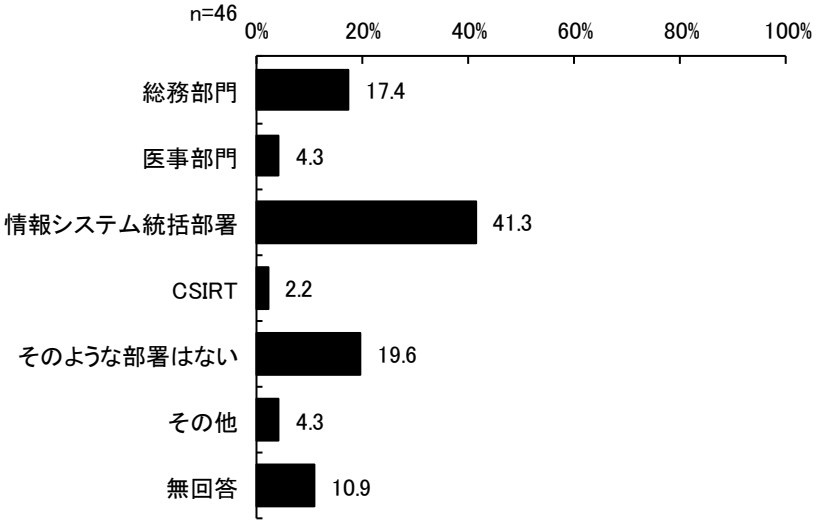
図表 10　情報システムを統括する部署への所属人数（Q10）



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 41.3%で最も割合が高く、ついで「そのような部署はない」が 19.6%、総務部門が 17.4%であった。

図表 11　情報セキュリティ対策を行う担当部署（Q11）

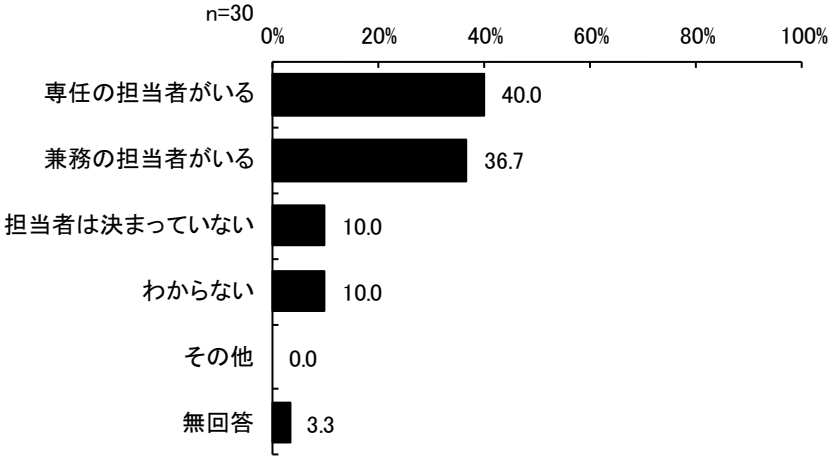


※「その他」の主な回答は以下の通り。
・不明

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、「専任の担当者がいる」が 40.0%で最も割合が高く、ついで「兼務の担当者がいる」が 36.7%であった。

図表 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（Q12）



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、1.5 人であった。

図表 13　情報セキュリティ担当者の常勤の専任者の人数（Q13）

（人）

	調査数	平均値	標準偏差	中央値	最小値	最大値
常勤の専任者の人数	4	1.5	0.5	1.5	1	2

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、2.8 人であった。

図表 14　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
常勤の兼務者の人数	10	2.8	2.36	2	1	9

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、2.0 人であった。

図表 15　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
非常勤の専任者の人数	3	2	2.16	1	0	5

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、0.17 人であった。

図表 16　情報セキュリティ担当者の非常勤の兼務者の人数（Q16）

（人）

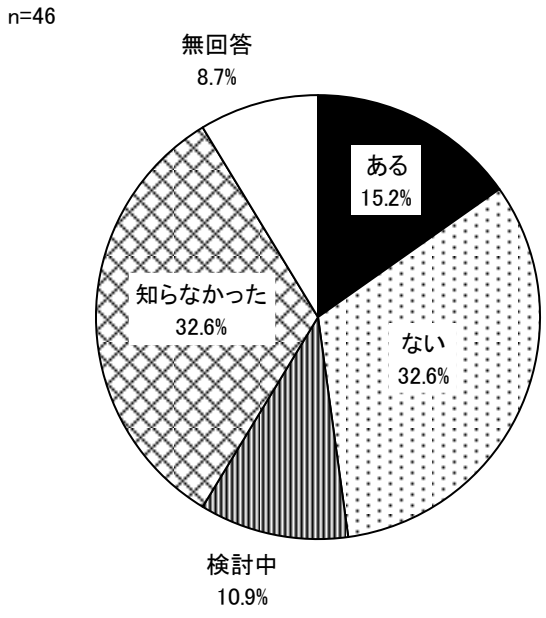
	調査数	平均値	標準偏差	中央値	最小値	最大値
非常勤の兼務者の人数	6	0.17	0.37	0	0	1

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」および「知らなかった」がいずれも 32.6%で最も割合が高かった。

※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

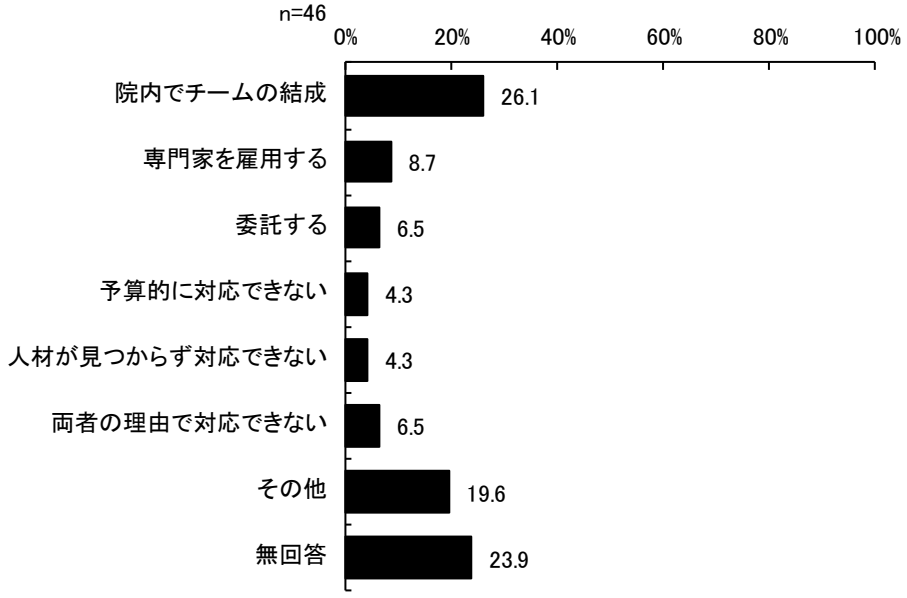
図表 17　所属する組織に CSIRT はあるか（Q17）



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 26.1%で最も割合が高く、ついで「その他」が 19.6%、「専門家を雇用する」が 8.7%であった。

図表 18　CSIRT を組織化する場合どのように作るか（Q18）

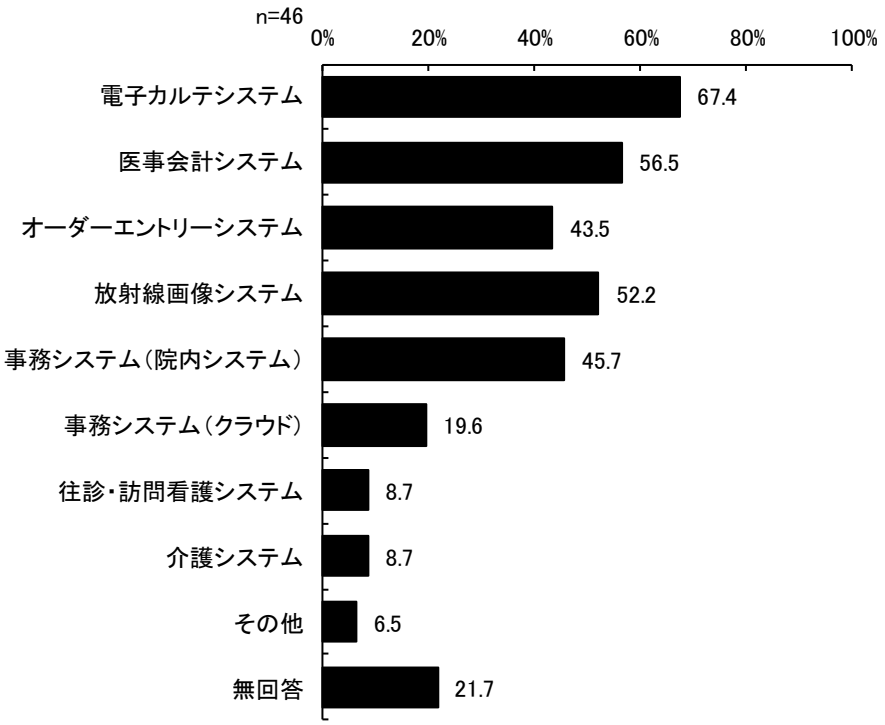


※「その他」の主な回答は以下の通り。
- 学内共通の組織として運用
- 現時点では未定
- これから検討する
- 積極的に習得し普及に努めたい
- 大学側に設置（病院の責任者も構成員として参加）
- 予算も人材も、ノウハウも何もない
- わからない

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、電子カルテシステムが 67.4%で最も割合が高く、ついで医事会計システムが 56.5%、放射線画像システムが 52.2%であった。

図表 19　導入している情報システム（Q19）【複数回答】

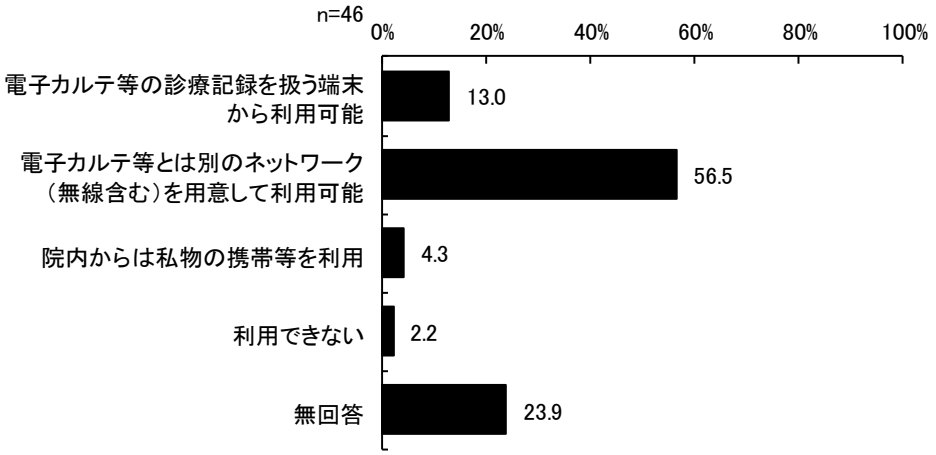


※「その他」の主な回答は以下の通り。
- 遠隔読影システム
- オンライン診療システム
- オンライン服薬指導システム

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 56.5%で最も割合が高く、ついで「電子カルテ等の診療記録を扱う端末から利用可能」が 13.0%であった。

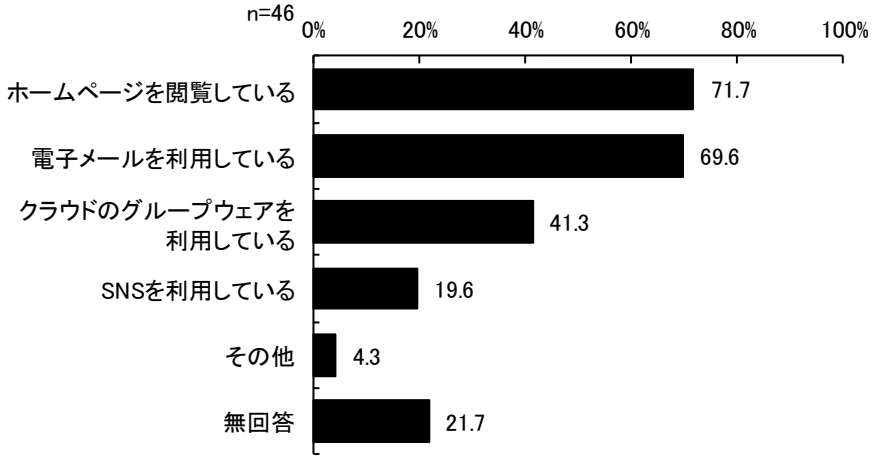
図表 20　院内における職員のインターネットの利用可否（Q20）



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 71.7%で最も割合が高く、ついで「電子メールを利用している」が 69.6%であった。

図表 21　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】

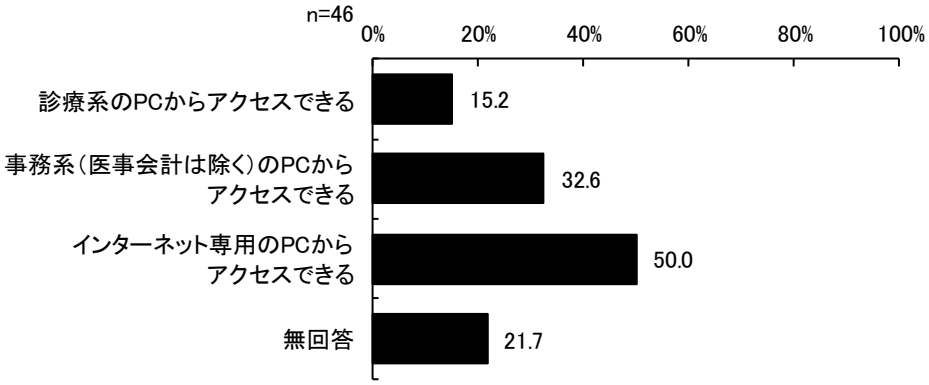


※「その他」の主な回答は以下の通り。
・コンテンツフィルタに抵触しない限り制限はしていない
・帝人バイタルリンク

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50.0%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32.6%であった。

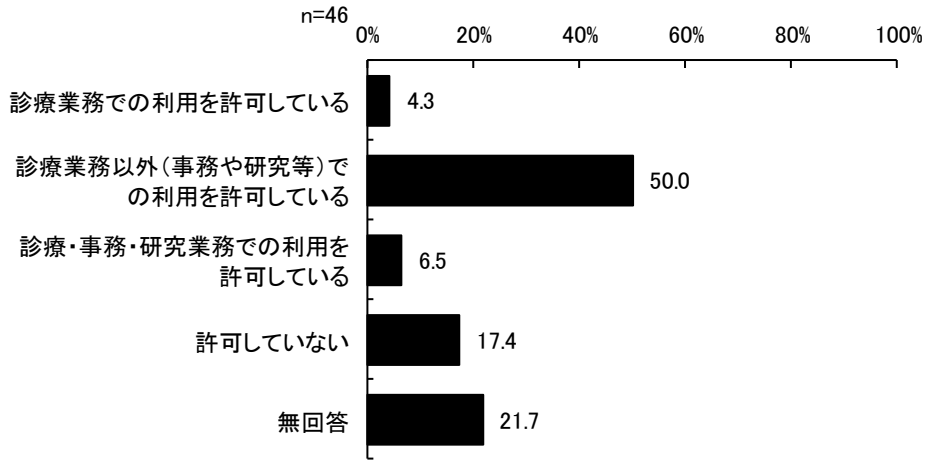
図表22　インターネットにアクセスできるパソコン（PC）について（Q22）【複数回答】



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50.0%で最も割合が高く、ついで「許可していない」が17.4%であった。

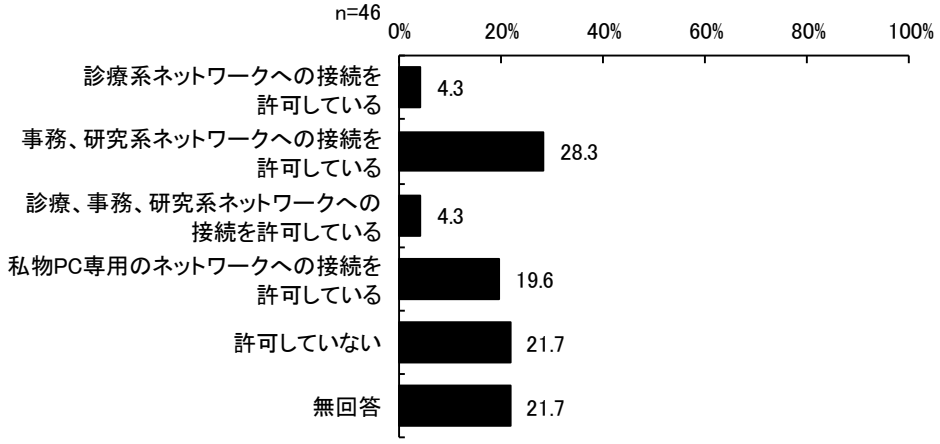
図表23　職員（医師など）の私物のPCを用いて業務を行うことを許可しているか（Q23）



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、「事務、研究系ネットワークへの接続を許可している」が 28.3%で最も割合が高く、ついで「許可していない」が 21.7%であった。

図表 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（Q24）

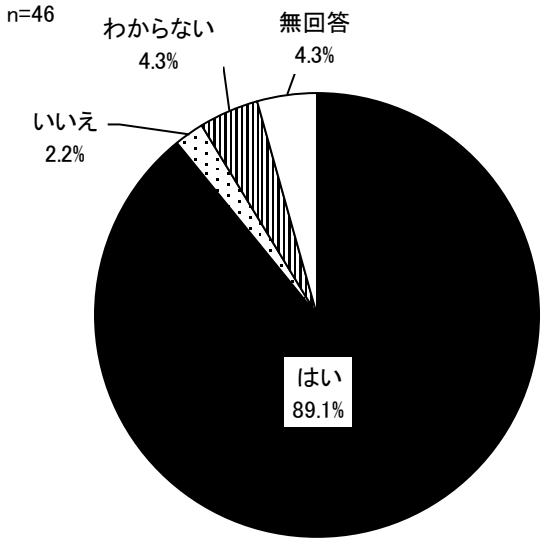


（2）組織で実施しているセキュリティ対策

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 89.1%で最も割合が高く、ついで「わからない」が 4.3%であった。

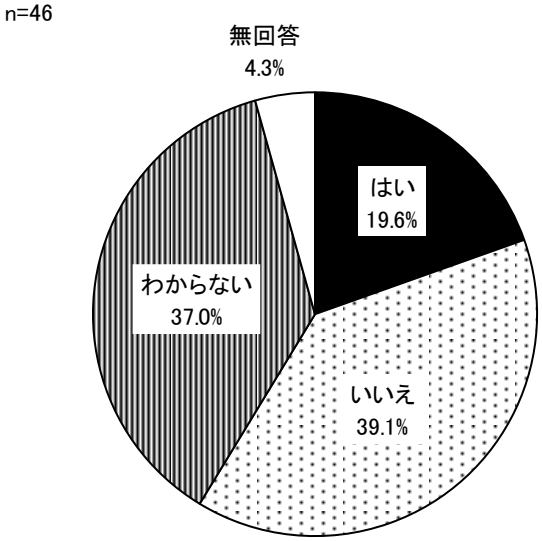
図表 25　ウイルス対策ソフトを導入しているか（Q25）



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、「いいえ」が 39.1%で最も割合が高く、ついで「わからない」が 37.0%であった。

図表 26　資産管理ソフトを導入しているか（Q26）



図表 27　資産管理ソフトを導入しているか（Q26）と情報システムを統括する部署はあるか（Q9）とのクロス集計結果

（表頭）Q26 資産管理ソフトを導入しているか
（表側）Q9　情報システムを統括する部署はあるか

	調査数	はい	いいえ	わからない	無回答
はい	25	5	5	14	1
	100.0	20.0	20.0	56.0	4.0
いいえ	17	3	13	1	－
	100.0	17.6	76.5	5.9	－

図表 28　資産管理ソフトを導入しているか（Q26）と情報セキュリティ対策を行う担当部署（Q11）とのクロス集計結果

（表頭）Q26 資産管理ソフトを導入しているか
（表側）Q11 情報セキュリティ対策を行う担当部署

	調査数	はい	いいえ	わからない	無回答
ある	30	6	9	14	1
	100.0	20.0	30.0	46.7	3.3
ない	9	1	7	1	－
	100.0	11.1	77.8	11.1	－

図表 29　資産管理ソフトを導入しているか（Q26）と「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（Q17）とのクロス集計結果

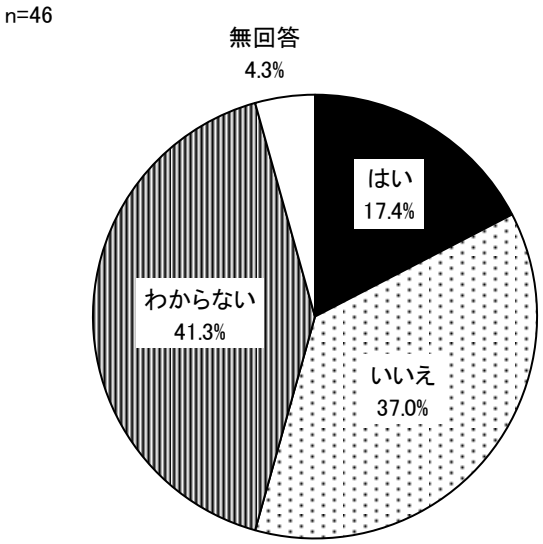
（表頭）Q26 資産管理ソフトを導入しているか
（表側）Q17 「医療情報システムの安全管理ガイドライン」にあるCSIRTはあるか

	調査数	はい	いいえ	わからない	無回答
ある	7	4	－	3	－
	100.0	57.1	－	42.9	－
ない	35	4	18	13	－
	100.0	11.4	51.4	37.1	－

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、「わからない」が 41.3%で最も割合が高く、ついで「いいえ」が 37.0%であった。

図表 30　仮想ブラウザを導入しているか（Q27）



図表 31　仮想ブラウザを導入しているか（Q27）と情報システムを統括する部署はあるか（Q9）とのクロス集計結果

（表頭）Q27 仮想ブラウザを導入しているか
（表側）Q9　情報システムを統括する部署はあるか

	調査数	はい	いいえ	わからない	無回答
はい	25 100.0	5 20.0	7 28.0	12 48.0	1 4.0
いいえ	17 100.0	2 11.8	10 58.8	5 29.4	－ －

図表 32　仮想ブラウザを導入しているか（Q27）と情報セキュリティ対策を行う担当部署（Q11）とのクロス集計結果

（表頭）Q27 仮想ブラウザを導入しているか
（表側）Q11 情報セキュリティ対策を行う担当部署

	調査数	はい	いいえ	わからない	無回答
ある	30 100.0	6 20.0	9 30.0	14 46.7	1 3.3
ない	9 100.0	1 11.1	6 66.7	2 22.2	－ －

図表 33　仮想ブラウザを導入しているか（Q27）と「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（Q17）とのクロス集計結果

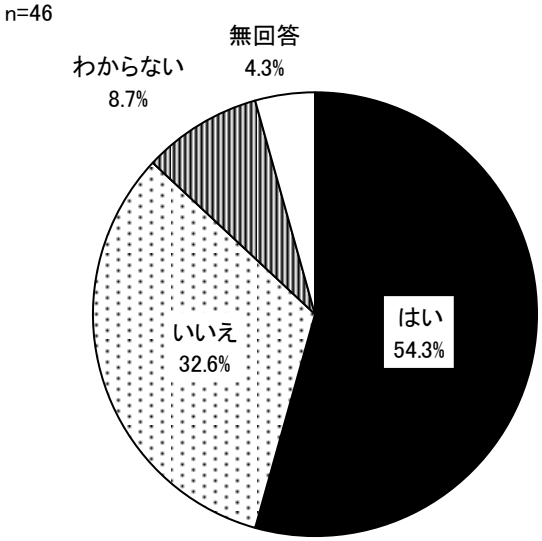
（表頭）Q27 仮想ブラウザを導入しているか
（表側）Q17 「医療情報システムの安全管理ガイドライン」にあるCSIRTはあるか

	調査数	はい	いいえ	わからない	無回答
ある	7 100.0	4 57.1	2 28.6	1 14.3	－ －
ない	35 100.0	3 8.6	15 42.9	17 48.6	－ －

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 54.3%で最も割合が高く、ついで「いいえ」が 32.6%であった。

図表 34　セキュリティ教育を行っているか（Q28）



図表 35　セキュリティ教育を行っているか（Q28）と情報システムを統括する部署はあるか（Q9）とのクロス集計結果

（表頭）Q28 セキュリティ教育を行っているか
（表側）Q9　情報システムを統括する部署はあるか

	調査数	はい	いいえ	わからない	無回答
はい	25	14	7	3	1
	100.0	56.0	28.0	12.0	4.0
いいえ	17	8	8	1	－
	100.0	47.1	47.1	5.9	－

図表 36　セキュリティ教育を行っているか（Q28）と情報セキュリティ対策を行う担当部署（Q11）とのクロス集計結果

（表頭）Q28 セキュリティ教育を行っているか
（表側）Q11 情報セキュリティ対策を行う担当部署

	調査数	はい	いいえ	わからない	無回答
ある	30	18	8	3	1
	100.0	60.0	26.7	10.0	3.3
ない	9	2	6	1	－
	100.0	22.2	66.7	11.1	－

図表 37　セキュリティ教育を行っているか（Q28）と「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（Q17）とのクロス集計結果

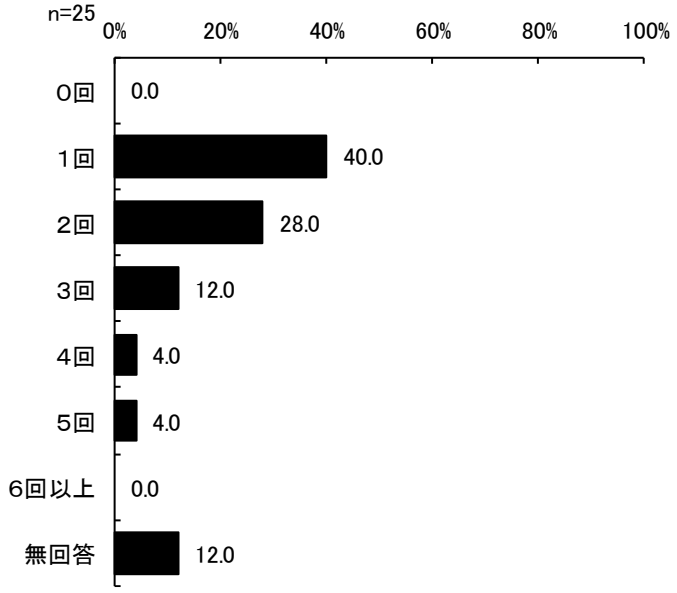
（表頭）Q28 セキュリティ教育を行っているか
（表側）Q17 「医療情報システムの安全管理ガイドライン」にあるCSIRTはあるか

	調査数	はい	いいえ	わからない	無回答
ある	7	6	－	1	－
	100.0	85.7	－	14.3	－
ない	35	17	15	3	－
	100.0	48.6	42.9	8.6	－

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 40.0%で最も割合が高く、ついで 2 回が 28.0%であった。

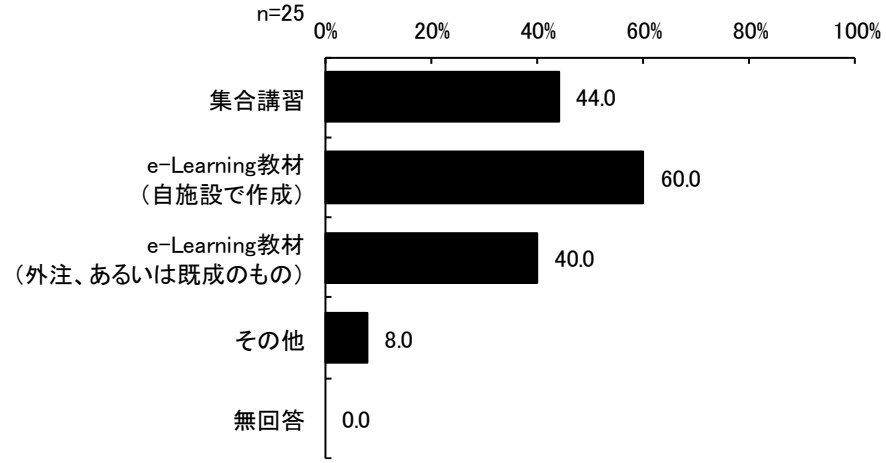
図表 38　セキュリティ教育は年に何回行っているか（Q29）



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、e-Learning 教材（自施設で作成）が 60.0%で最も割合が高く、ついで集合講習が 44.0%であった。

図表 39　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】

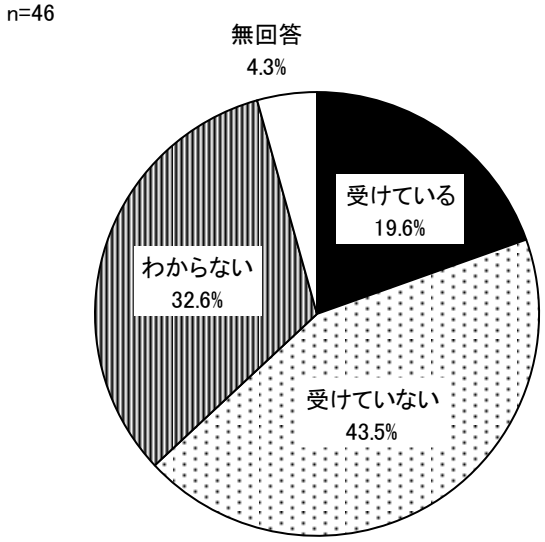


※「その他」の主な回答は以下の通り。
- 個別
- 行っていない

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 43.5%で最も割合が高く、ついで「わからない」が 32.6%であった。

図表 40　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）



図表 41　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）と情報システムを統括する部署はあるか（Q9）とのクロス集計結果

（表頭）Q31 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）
（表側）Q9　情報システムを統括する部署はあるか

	調査数	受けている	受けていない	わからない	無回答
はい	25	7	5	12	1
	100.0	28.0	20.0	48.0	4.0
いいえ	17	1	15	1	－
	100.0	5.9	88.2	5.9	－

図表 42　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）と情報セキュリティ対策を行う担当部署（Q11）とのクロス集計結果

（表頭）Q31 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）
（表側）Q11 情報セキュリティ対策を行う担当部署

	調査数	受けている	受けていない	わからない	無回答
ある	30	7	10	12	1
	100.0	23.3	33.3	40.0	3.3
ない	9	－	9	－	－
	100.0	－	100.0	－	－

図表 43　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）と「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（Q17）とのクロス集計結果

（表頭）Q31 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）
（表側）Q17 「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

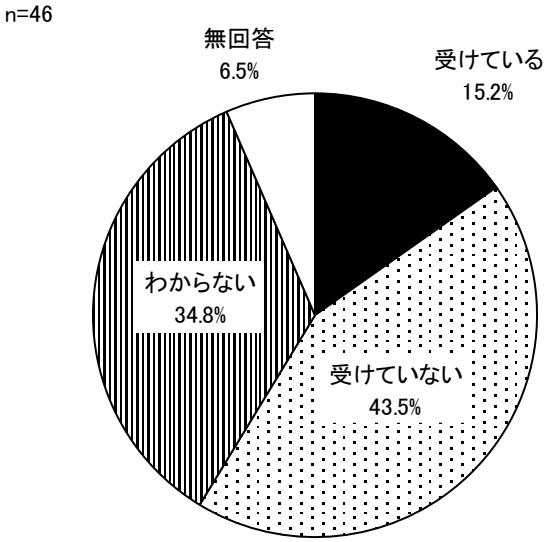
	調査数	受けている	受けていない	わからない	無回答
ある	7	5	－	2	－
	100.0	71.4	－	28.6	－
ない	35	3	20	12	－
	100.0	8.6	57.1	34.3	－

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 43.5%で最も割合が高く、ついで「わからない」が 34.8%であった。

※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 44　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）



図表 45　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）と情報システムを統括する部署はあるか（Q9）とのクロス集計結果

（表頭）Q32 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）
（表側）Q9　情報システムを統括する部署はあるか

	調査数	受けている	受けていない	わからない	無回答
はい	25	7	5	11	2
	100.0	28.0	20.0	44.0	8.0
いいえ	17	－	15	2	－
	100.0	－	88.2	11.8	－

図表 46　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）と情報セキュリティ対策を行う担当部署（Q11）とのクロス集計結果

（表頭）Q32 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）
（表側）Q11 情報セキュリティ対策を行う担当部署

	調査数	受けている	受けていない	わからない	無回答
ある	30	7	10	11	2
	100.0	23.3	33.3	36.7	6.7
ない	9	－	8	1	－
	100.0	－	88.9	11.1	－

図表 47　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）と「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（Q17）とのクロス集計結果

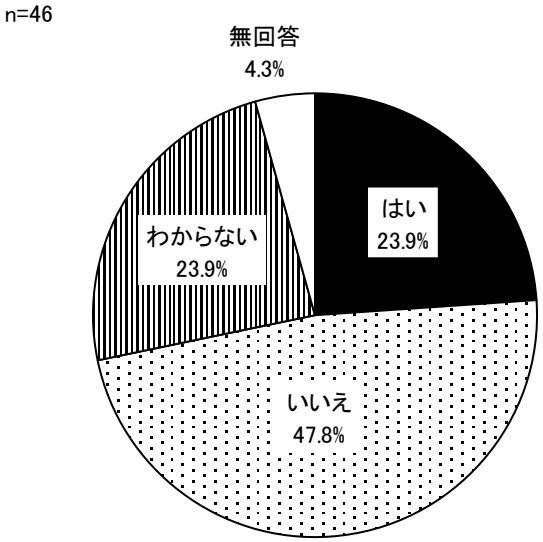
（表頭）Q32 ペネトレーションテストを受けているか（直近３年以内の状況）
（表側）Q17 「医療情報システムの安全管理ガイドライン」にあるCSIRTはあるか

	調査数	受けている	受けていない	わからない	無回答
ある	7	4	1	2	－
	100.0	57.1	14.3	28.6	－
ない	35	3	19	12	1
	100.0	8.6	54.3	34.3	2.9

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 47.8%で最も割合が高く、ついで「はい」および「わからない」がいずれも 23.9%であった。

図表 48　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）



図表 49　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）と情報システムを統括する部署はあるか（Q9）とのクロス集計結果

（表頭）Q33 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）
（表側）Q9　情報システムを統括する部署はあるか

	調査数	はい	いいえ	わからない	無回答
はい	25	9	6	9	1
	100.0	36.0	24.0	36.0	4.0
いいえ	17	1	15	1	－
	100.0	5.9	88.2	5.9	－

図表 50　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）と情報セキュリティ対策を行う担当部署（Q11）とのクロス集計結果

（表頭）Q33 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）
（表側）Q11 情報セキュリティ対策を行う担当部署

	調査数	はい	いいえ	わからない	無回答
ある	30	10	10	9	1
	100.0	33.3	33.3	30.0	3.3
ない	9	－	9	－	－
	100.0	－	100.0	－	－

図表 51　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）と「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（Q17）とのクロス集計結果

（表頭）Q33 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）
（表側）Q17 「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

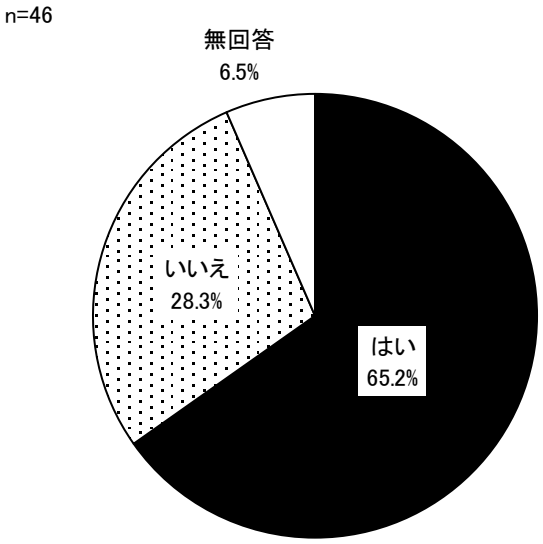
	調査数	はい	いいえ	わからない	無回答
ある	7	6	－	1	－
	100.0	85.7	－	14.3	－
ない	35	4	21	10	－
	100.0	11.4	60.0	28.6	－

（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 65.2%であった。

図表 52　情報セキュリティポリシーを規定しているか（Q34）



図表 53　情報セキュリティポリシーを規定しているか（Q34）と情報システムを統括する部署はあるか（Q9）とのクロス集計結果

（表頭）Q34 情報セキュリティポリシーを規定しているか
（表側）Q9　情報システムを統括する部署はあるか

	調査数	はい	いいえ	無回答
はい	25	20	4	1
	100.0	80.0	16.0	4.0
いいえ	17	8	9	－
	100.0	47.1	52.9	－

図表 54　情報セキュリティポリシーを規定しているか（Q34）と情報セキュリティ対策を行う担当部署（Q11）とのクロス集計結果

（表頭）Q34 情報セキュリティポリシーを規定しているか
（表側）Q11 情報セキュリティ対策を行う担当部署

	調査数	はい	いいえ	無回答
ある	30	25	4	1
	100.0	83.3	13.3	3.3
ない	9	2	7	－
	100.0	22.2	77.8	－

図表 55　情報セキュリティポリシーを規定しているか（Q34）と「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（Q17）とのクロス集計結果

（表頭）Q34 情報セキュリティポリシーを規定しているか
（表側）Q17 「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

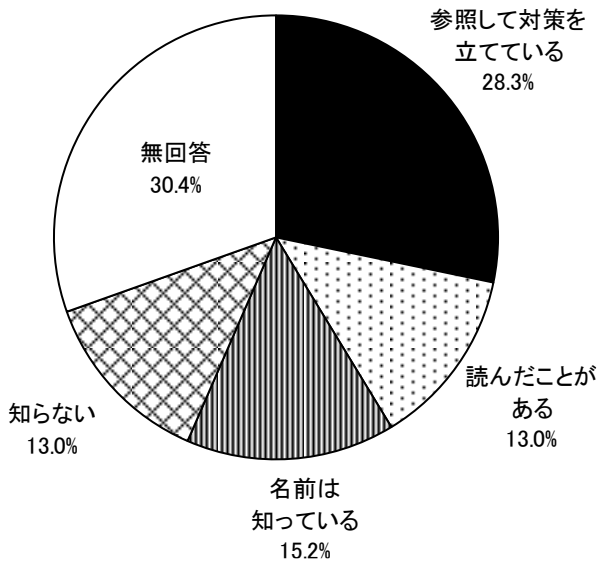
	調査数	はい	いいえ	無回答
ある	7	7	－	－
	100.0	100.0	－	－
ない	35	21	13	1
	100.0	60.0	37.1	2.9

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 28.3%で最も割合が高く、ついで「名前は知っている」が 15.2%であった。

図表 56　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）

n=46

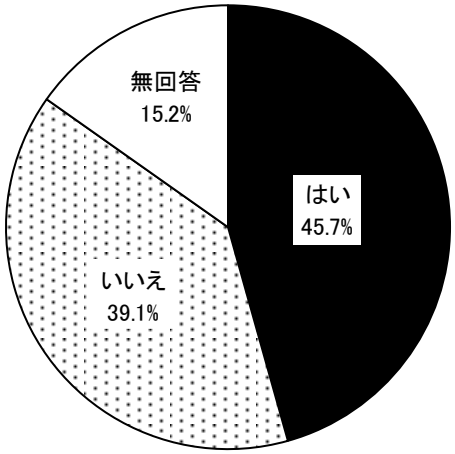


3）セキュリティインシデント発生時の手順が定められているか

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45.7%であった。

図表 57　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）

n=46

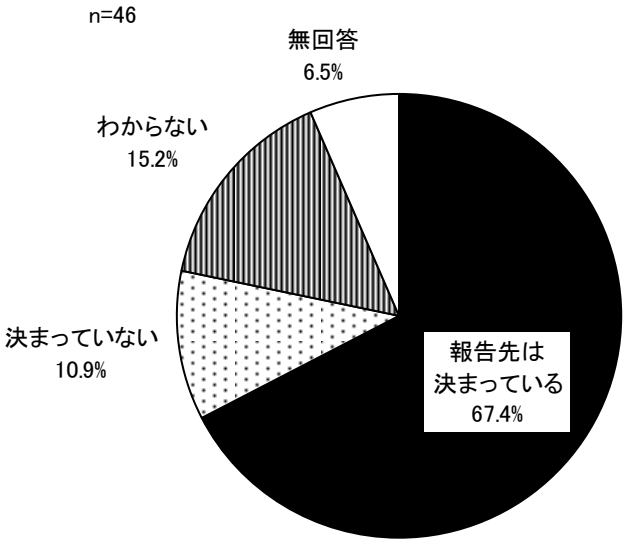


（4）セキュリティインシデント発生時の対応

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 67.4%で最も割合が高く、ついで「わからない」が 15.2%であった。

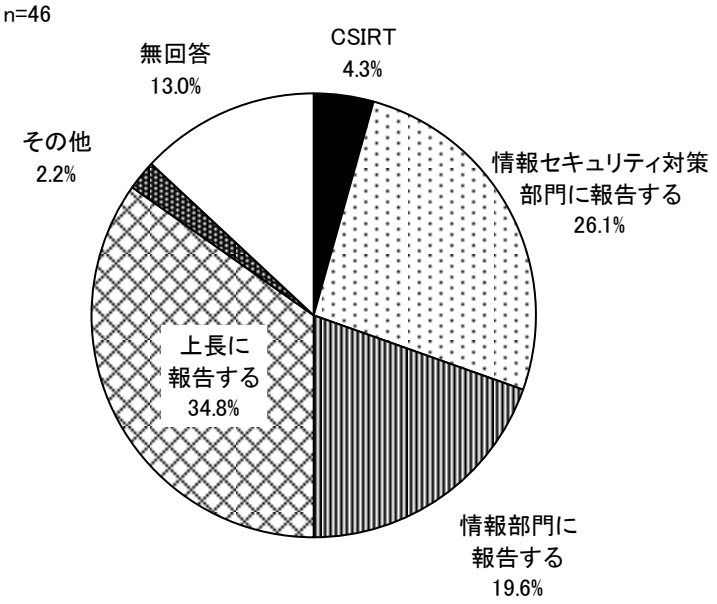
図表 58　職員がセキュリティインシデントを発見したときに報告する部署が決まっているか（Q37）



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、「上長に報告する」が 34.8%で最も割合が高く、ついで「情報セキュリティ対策部門に報告する」が 26.1%であった。

図表 59　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）

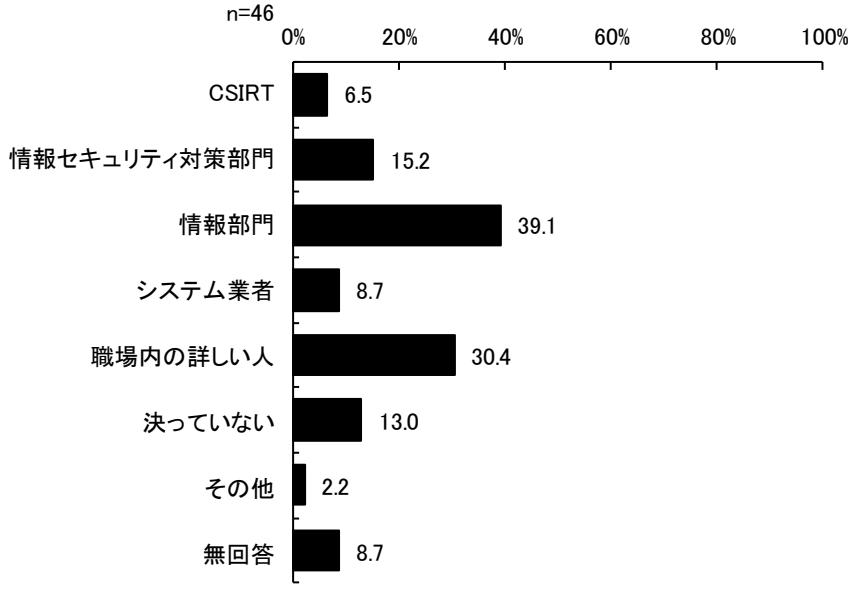


※「その他」の主な回答は以下の通り。
・不明

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 39.1%で最も割合が高く、ついで職場内の詳しい人が 30.4%であった。

図表 60　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】

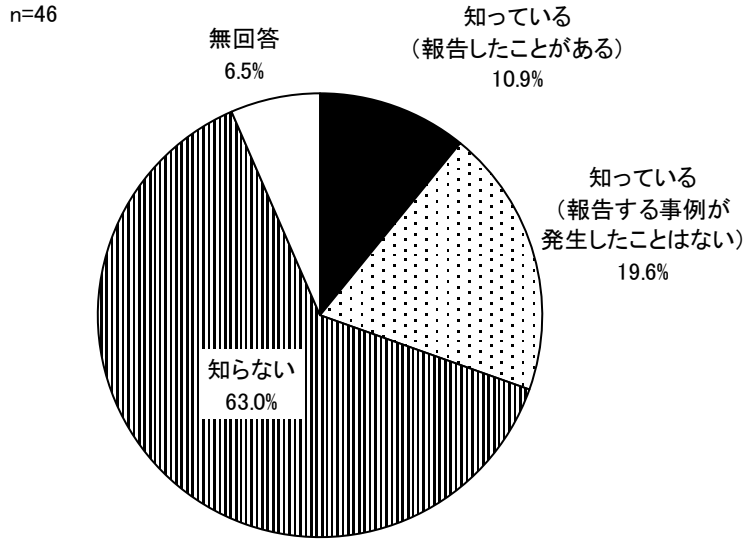


※「その他」の主な回答は以下の通り。
・不明

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、「知らない」が 63.0%で最も割合が高く、ついで「知っている（報告する事例が発生したことはない)」が 19.6%であった。

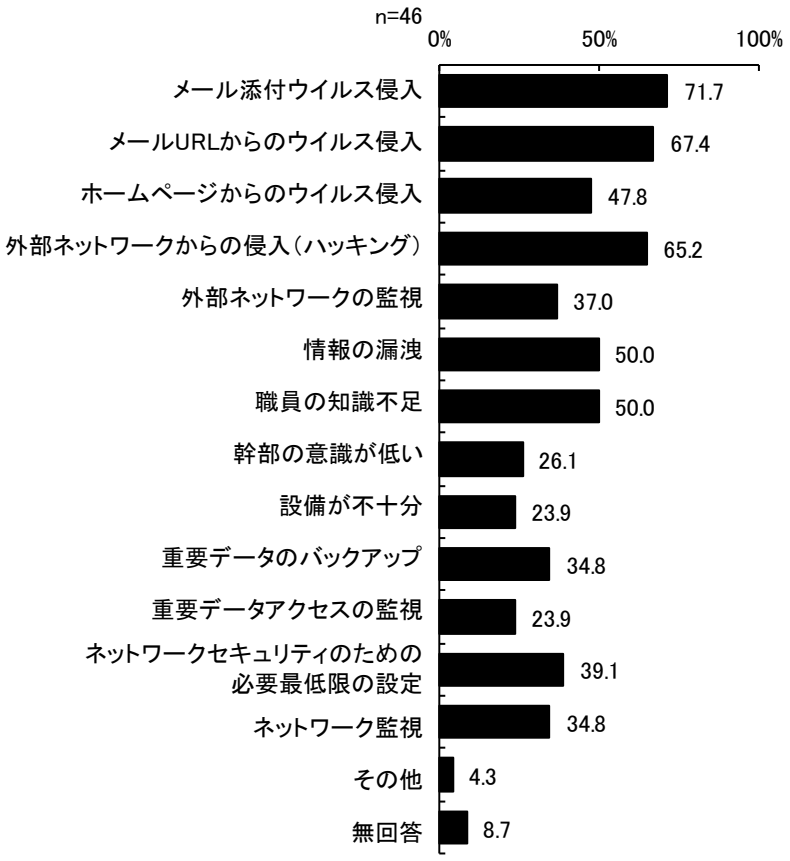
図表 61　情報セキュリティインシデント発生時の厚生労働省の窓口を知っているか（Q40）



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、「メール添付ウイルス侵入」が71.7%で最も割合が高く、ついで「メールURL からのウイルス侵入」が67.4%であった。

図表 62　所属機関のサイバーセキュリティの課題（Q41）【複数回答】

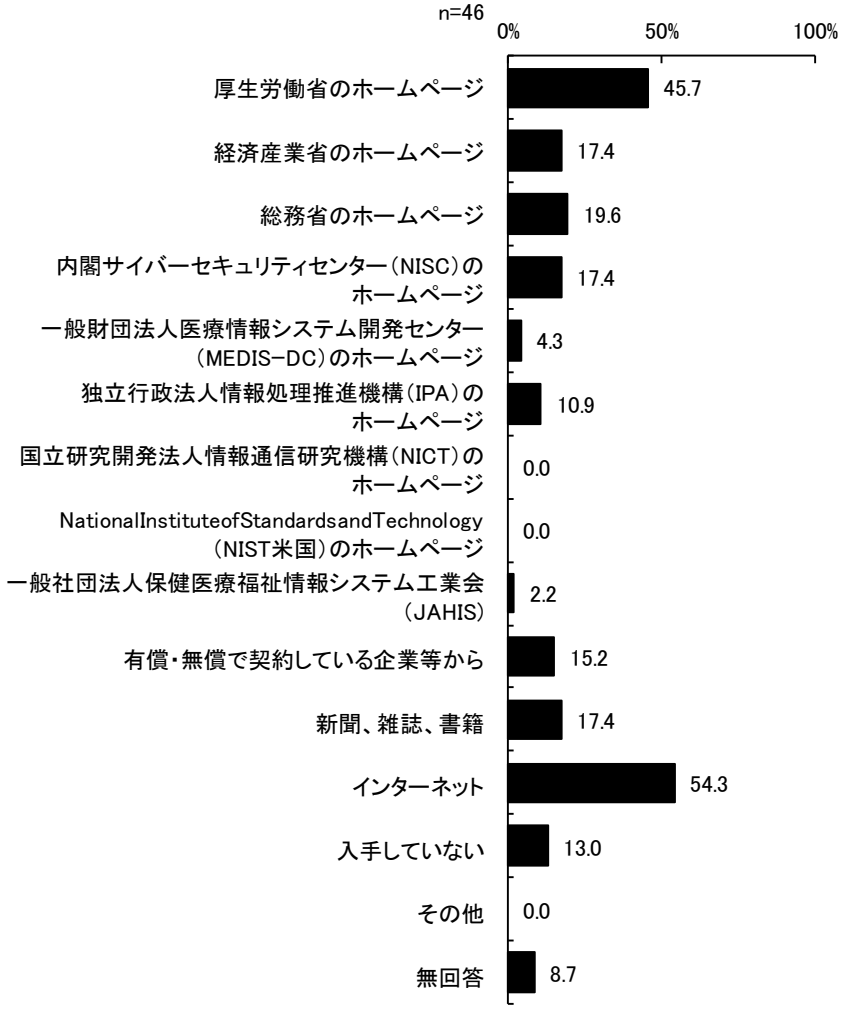


※「その他」の主な回答は以下の通り。
- フィッシング詐欺
- 電話を利用した攻撃
- 予算がない

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 54.3%で最も割合が高く、ついで厚生労働省のホームページが 45.7%であった。

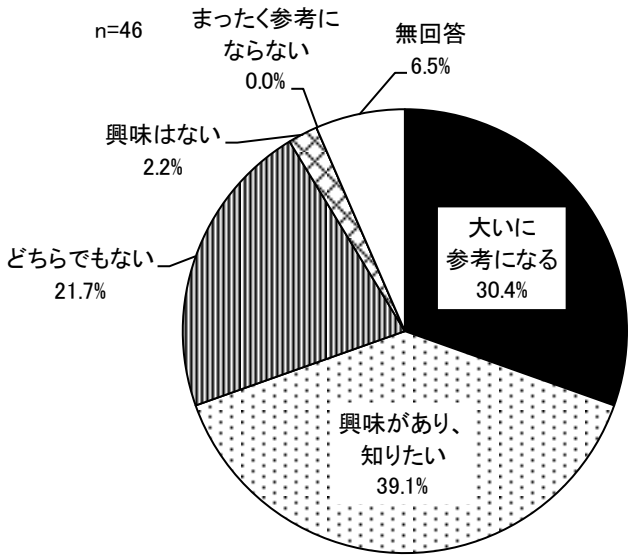
図表 63　情報セキュリティに関する情報源（Q42）【複数回答（3 つまで）】



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 39.1%で最も割合が高く、ついで「大いに参考になる」が 30.4%であった。

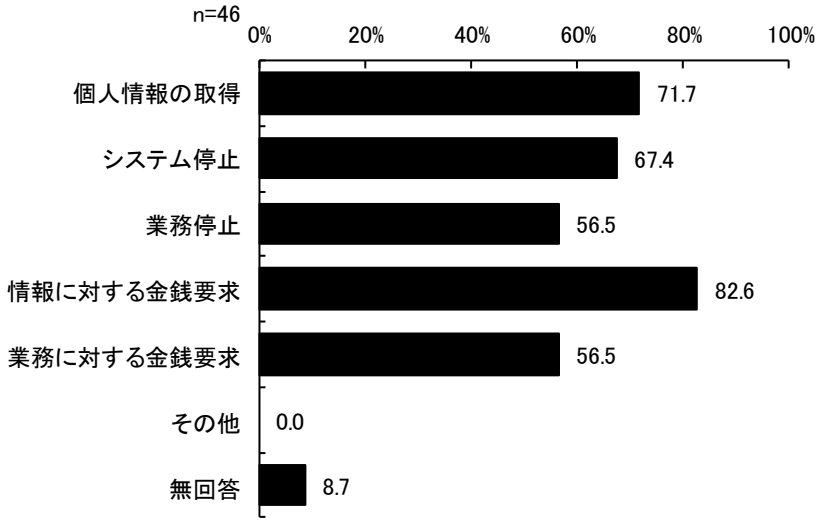
図表 64　他の施設の対策状況は対策を立てる上で参考になるか（Q43）



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 82.6%で最も割合が高く、ついで個人情報の取得が 71.7%であった。

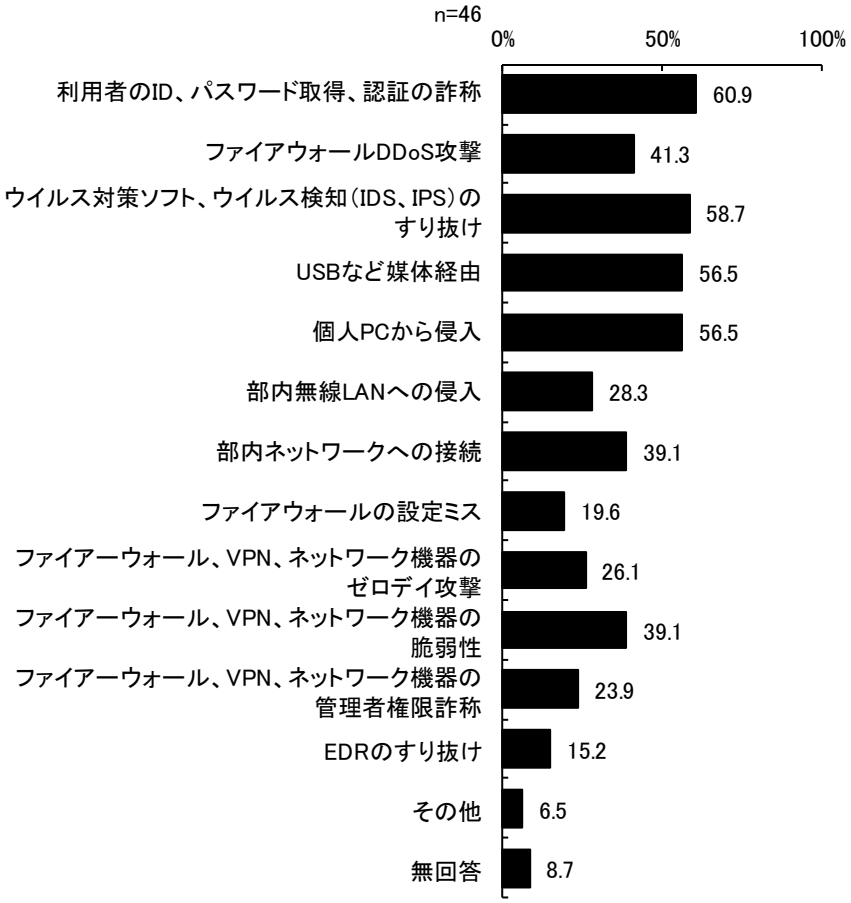
図表 65　最近のサイバーテロの目的（Q44）【複数回答】



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、利用者の ID、パスワード取得、認証の詐称が 60.9%で最も割合が高く、ついでウイルス対策ソフト、ウイルス検知（IDS、IPS）のすり抜けが 58.7%であった。

図表 66　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】

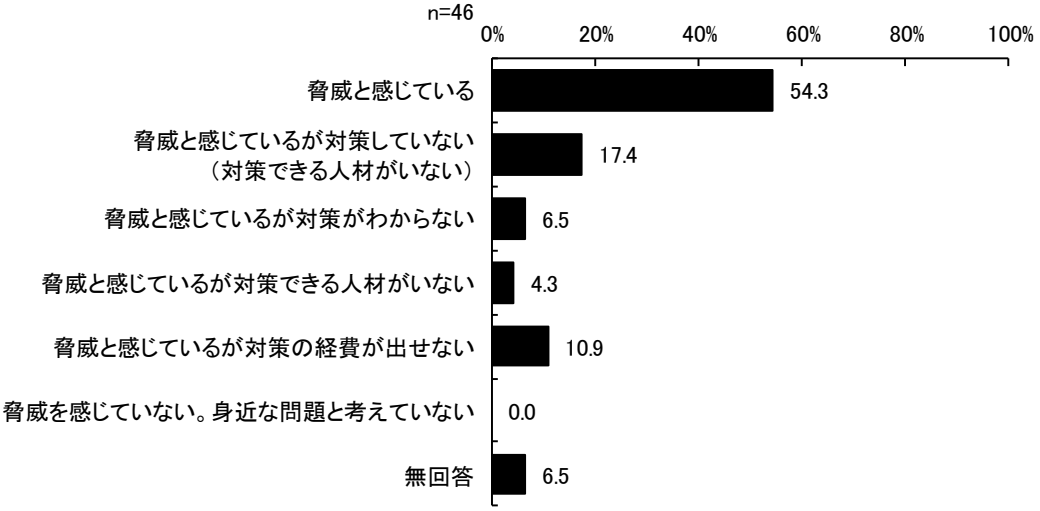


※「その他」の主な回答は以下の通り。
- ランサムウェア
- 個人 PC 売却時にハードディスクの消去情報復元

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 54.3%で最も割合が高く、ついで「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）」が 17.4%であった。

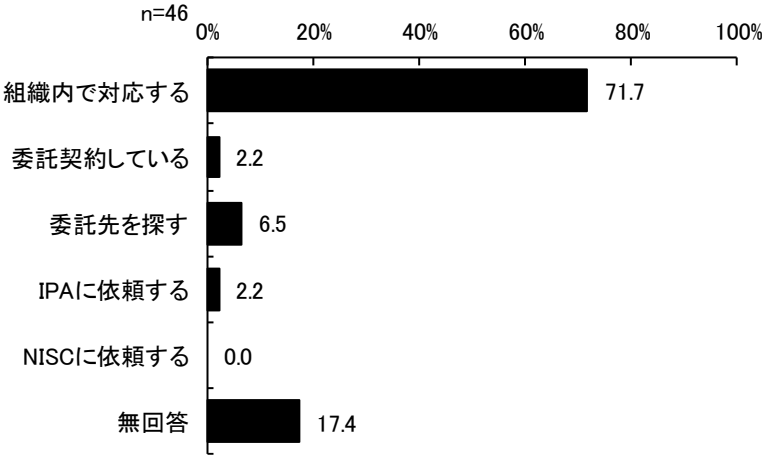
図表 67　サイバーセキュリティを脅威と感じているか、対策を検討しているか、問題は何か（Q46）



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 71.7%で最も割合が高く、ついで「委託先を探す」が 6.5%であった。

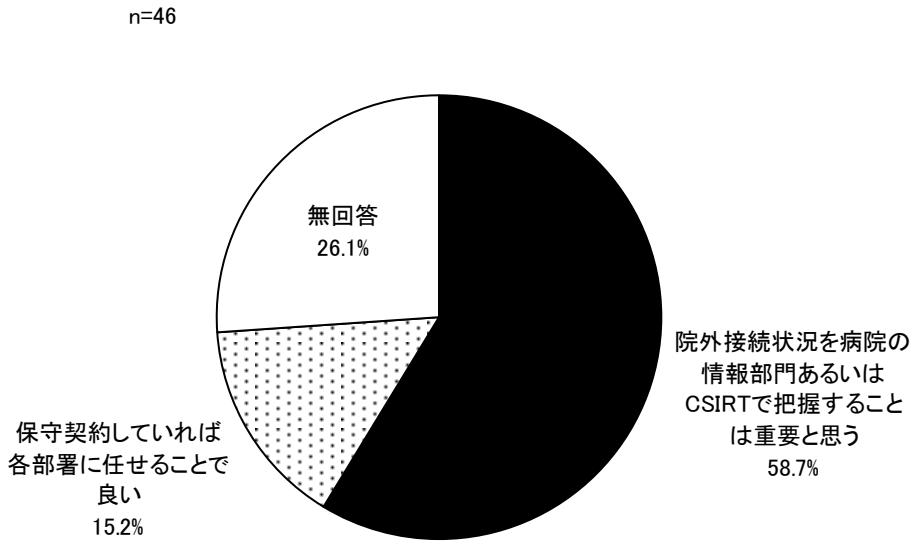
図表 68　インシデント発生時の対応について（Q47）



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58.7%であった。

図表69　インシデント発生以前の事前調査に対する意識（Q48）

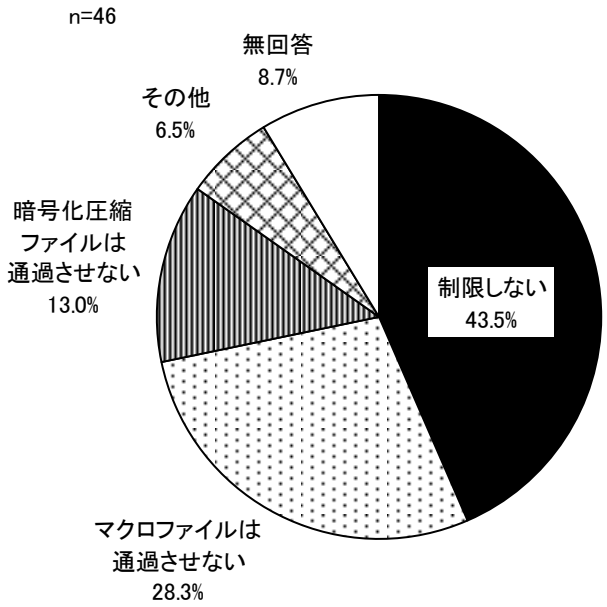


（5）侵入経路の対策として実施している事項等

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 43.5%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 28.3%であった。

図表 70　メール添付ファイルについて（Q49）

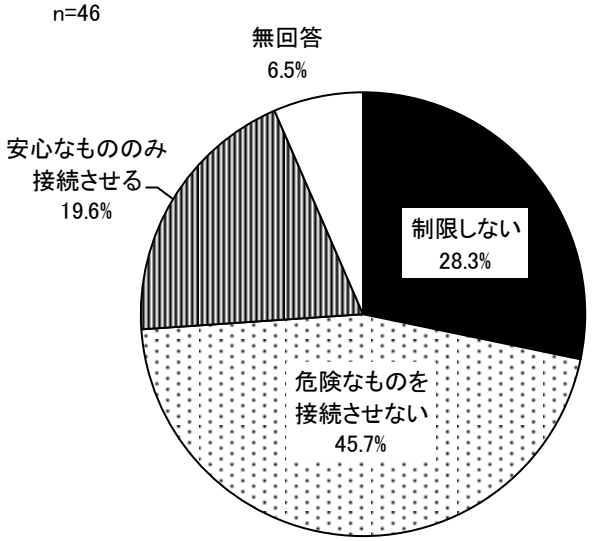


※「その他」の主な回答は以下の通り。
- EXE 等、実行ファイルは通過させない
- サンドボックスを用意している
- 外部メールサービスを利用している
- 知らない

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 45.7%で最も割合が高く、ついで「制限しない」が 28.3%であった。

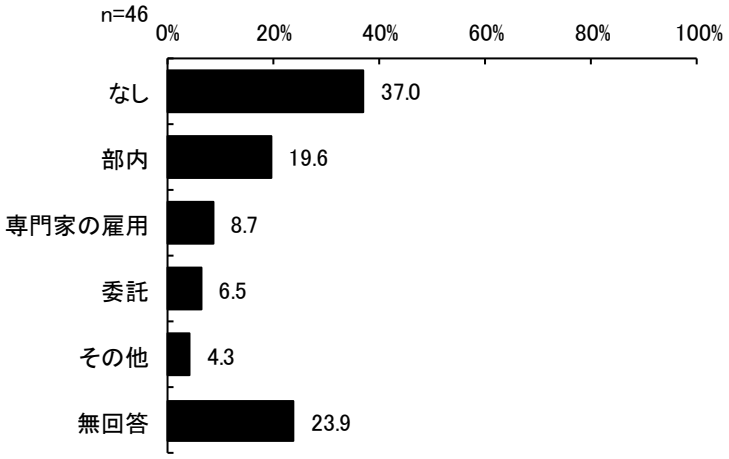
図表 71　ホームページ閲覧に関する対策（Q50）



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 37.0%で最も割合が高く、ついで「部内」が 19.6%であった。

図表 72　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）

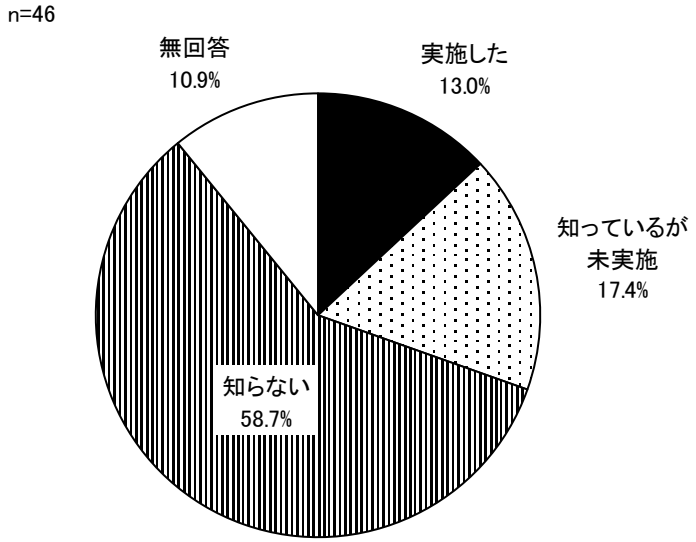


※「その他」の主な回答は以下の通り。
- 大学全体で NISC 基準に沿って組織化
- 不明

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、「知らない」が 58.7%で最も割合が高く、ついで「知っているが未実施」が 17.4%であった。

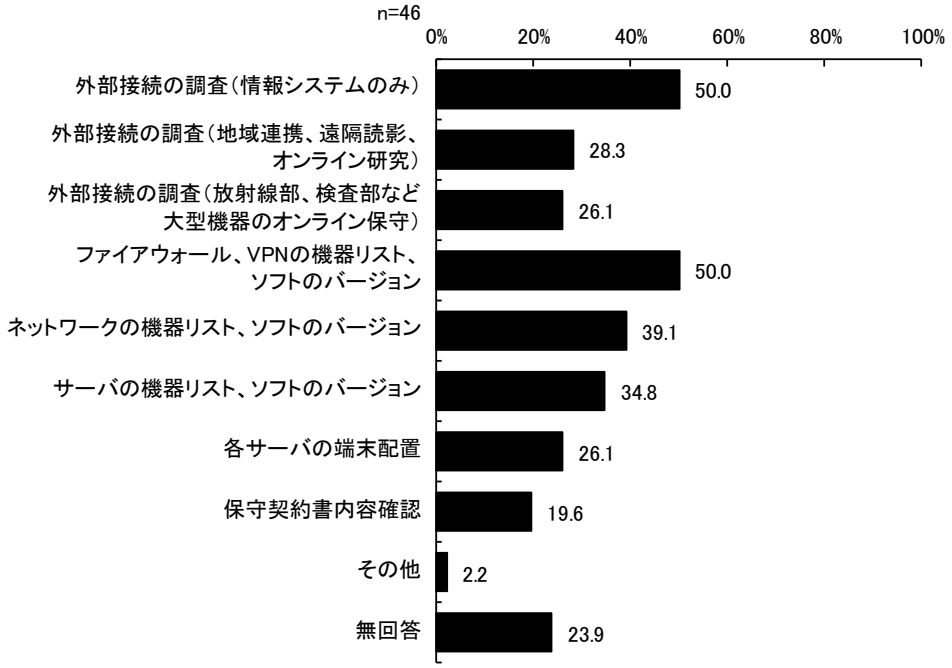
図表 73　医療情報システムの安全管理ガイドラインに添付されたサイバーセキュリティに関するチェックリスト、フローを知っているか（Q52）



5）事前調査、監視の対象

事前調査、監視の対象については、「外部接続の調査（情報システムのみ)」および「ファイアウォール、VPN の機器リスト、ソフトのバージョン」がいずれも 50.0%で最も割合が高く、ついで「ネットワークの機器リスト、ソフトのバージョン」が 39.1%であった。

図表 74　事前調査、監視の対象（Q53）【複数回答】

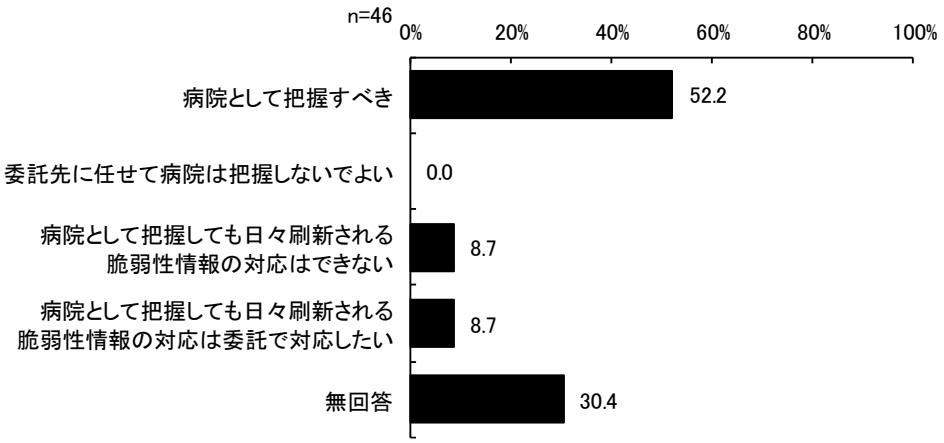


※「その他」の主な回答は以下の通り。
・不明

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 52.2%で最も割合が高かった。

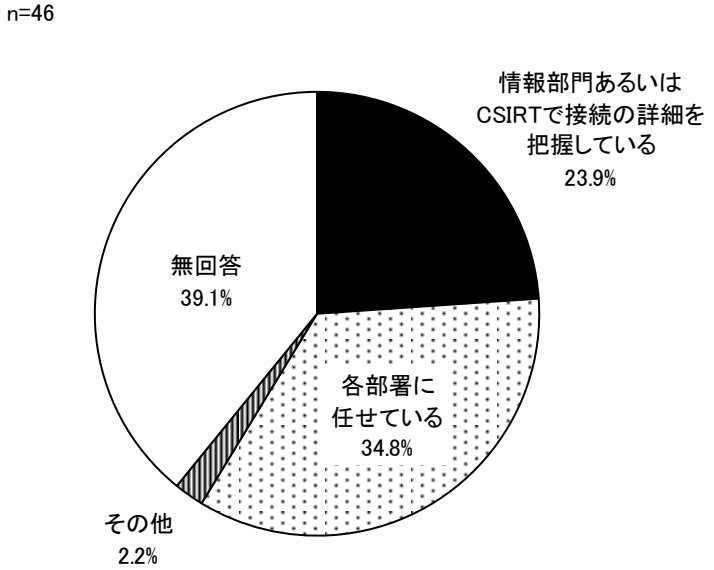
図表 75　システムの保守回線・CT・MRI 等の検査機器の保守回線の詳細（Q54）



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、「各部署に任せている」が 34.8%で最も割合が高く、ついで「情報部門あるいは CSIRT で接続の詳細を把握している」が 23.9%であった。

図表 76　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）

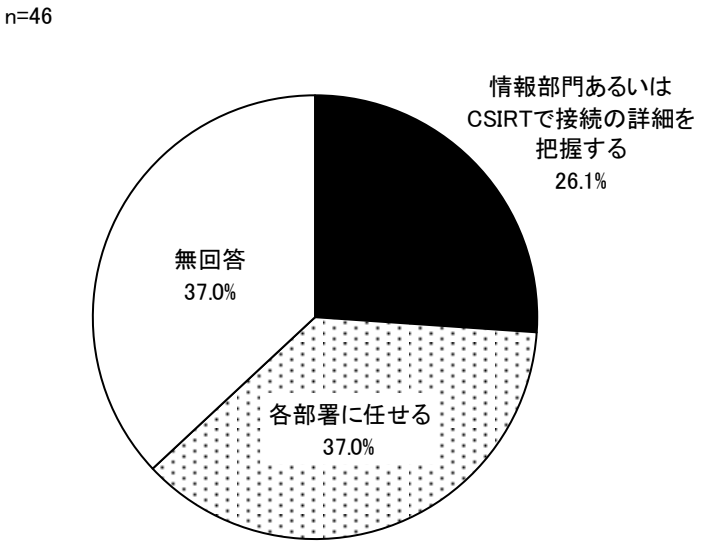


※「その他」の主な回答は以下の通り。
・不明

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、「各部署に任せる」が 37.0%であった。

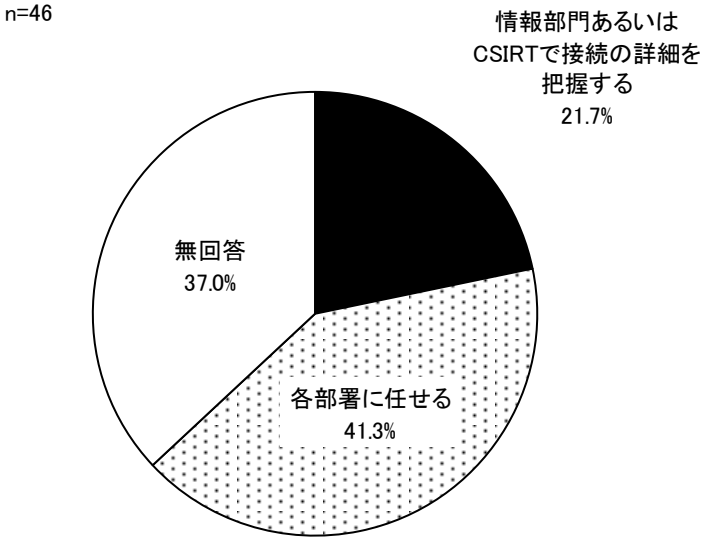
図表 77　オンライン診療・遠隔モニタリング・院内 SNS の接続について（Q56）



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、「各部署に任せる」が 41.3%であった。

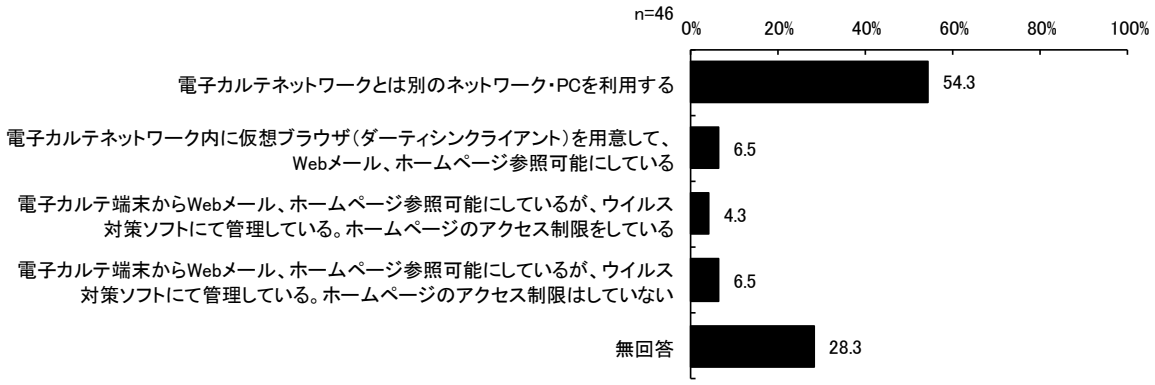
図表 78　匿名化してオンライン接続する遠隔画像診断・匿名化してオンライン接続する調査等の接続について（Q57）



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 54.3%で最も割合が高かった。

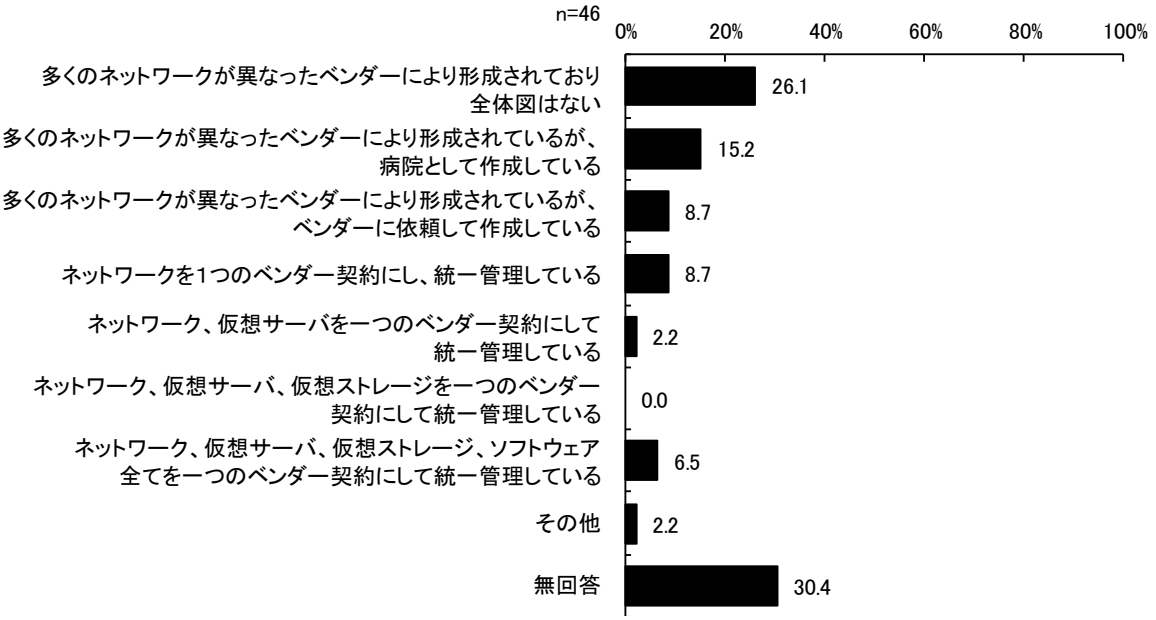
図表 79　利用者のホームページ閲覧、メール受信について（Q58）



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、「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 26.1%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 15.2%であった。

図表 80　院内ネットワーク全体図の作成はされているか（Q59）

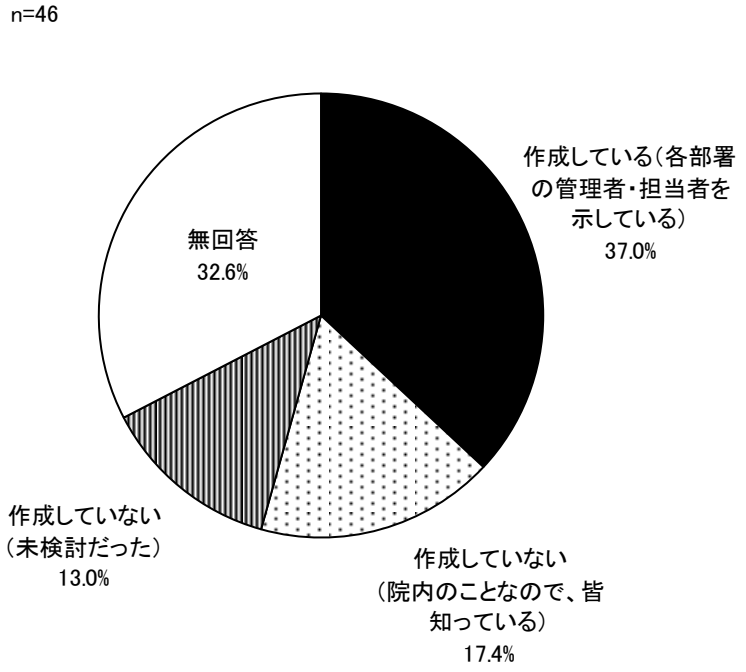


※「その他」の主な回答は以下の通り。
・不明

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 37.0%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 17.4%であった。

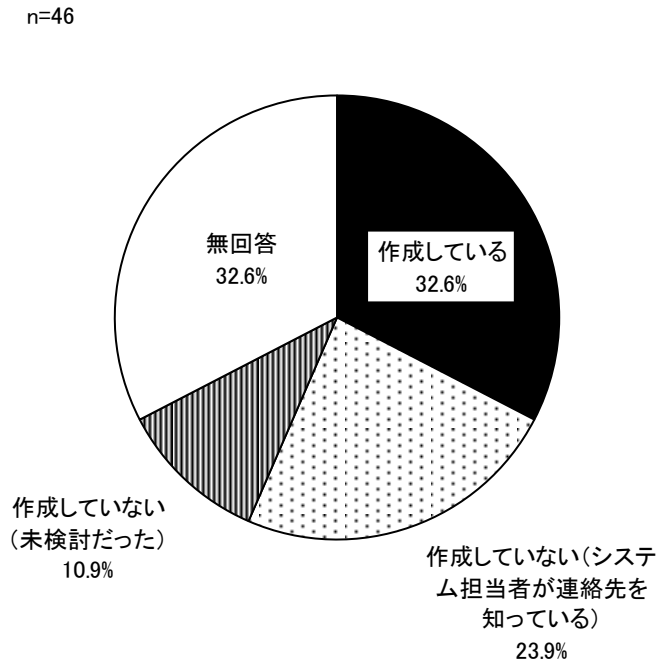
図表 81　電子カルテシステム・部門システムそれぞれについて院内の管理者・担当者一覧を作成しているか（Q60）



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 32.6%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 23.9%であった。

図表 82　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）

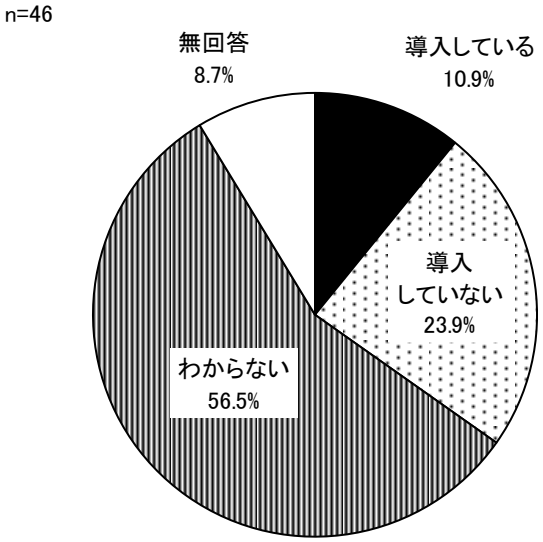


（6）ウイルス対策の状況

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、「わからない」が 56.5%で最も割合が高く、ついで「導入していない」が 23.9%であった。

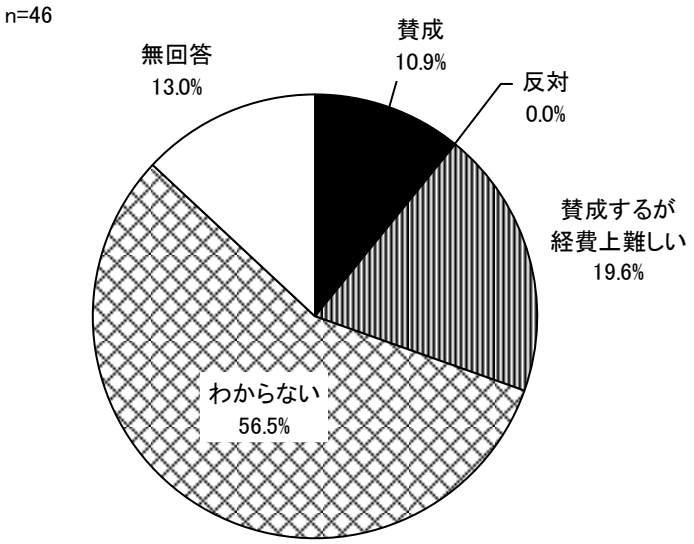
図表 83　端末への EDR（Endpoint Detection and Response）導入状況（Q62）



2）端末への EDR 導入について

端末への EDR 導入については、「わからない」が 56.5%で最も割合が高く、ついで「賛成するが経費上難しい」が 19.6%であった。

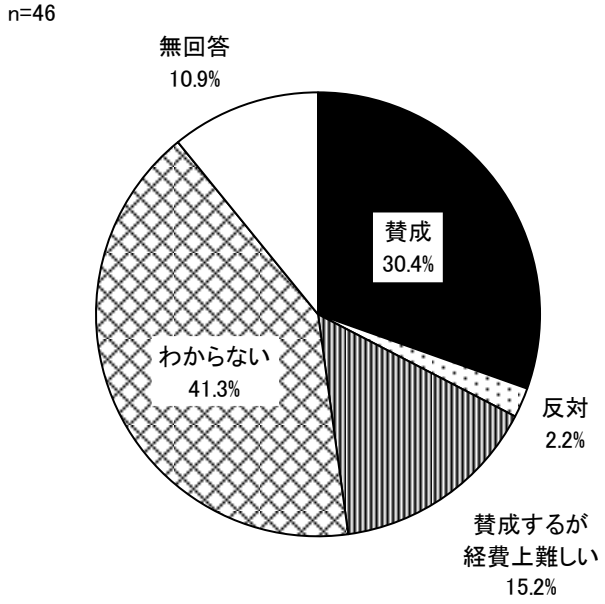
図表 84　端末への EDR 導入について（Q63）



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、「わからない」が 41.3%で最も割合が高く、ついで「賛成」が 30.4%であった。

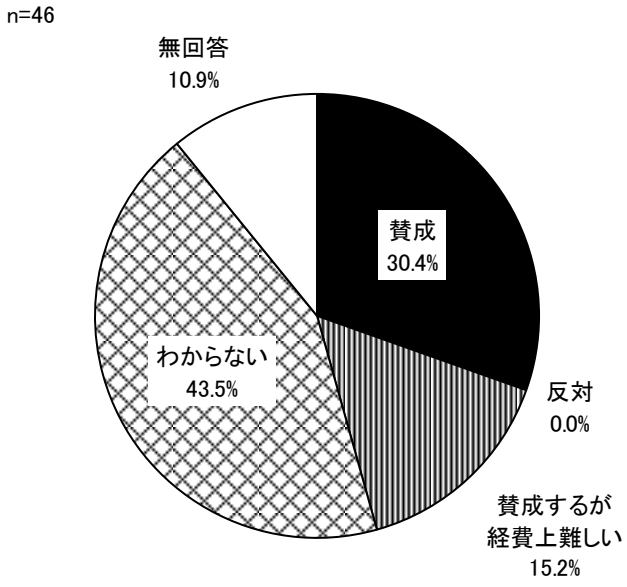
図表 85　内部ネットワークを監視することについて（Q64）



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、「わからない」が 43.5%で最も割合が高く、ついで「賛成」が 30.4%であった。

図表 86　内部サーバーを監視することについて（Q65）

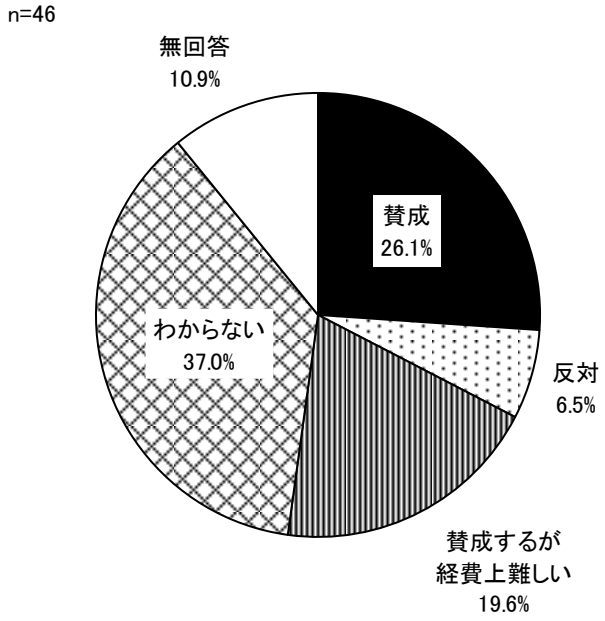


(7)サイバーセキュリティ対策への意見

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、「わからない」が 37.0%で最も割合が高く、ついで「賛成」が 26.1%であった。

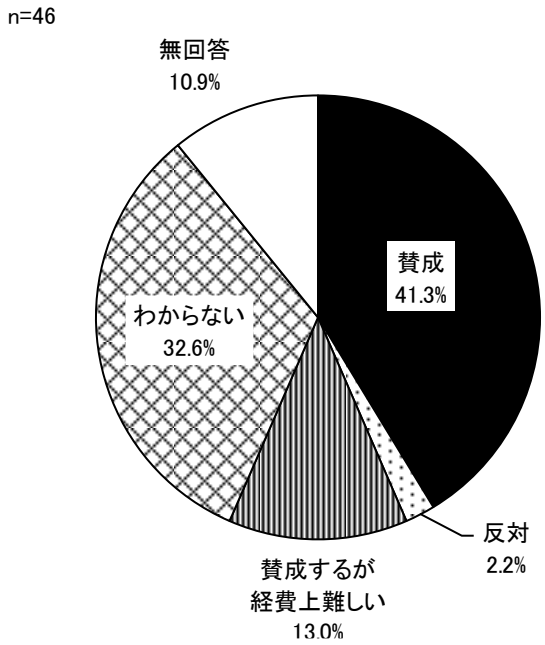
図表 87　端末からサーバーを守るためのシンクライアント基盤の導入（Q66）



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」が 41.3%で最も割合が高く、ついで「わからない」が 32.6%であった。

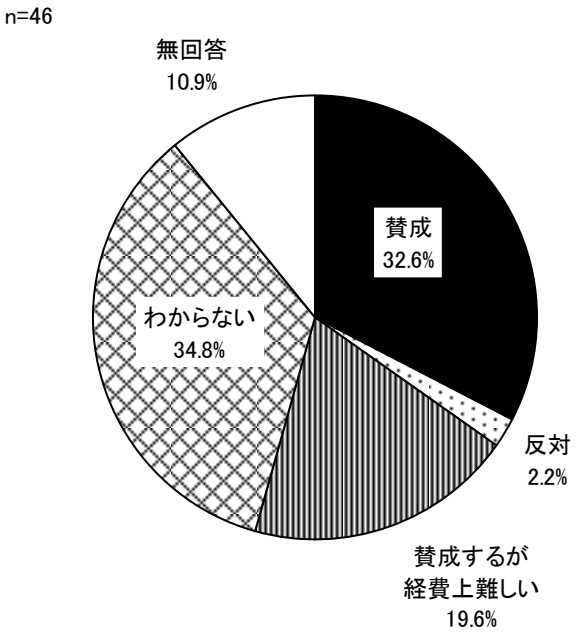
図表 88　仮想ブラウザ（ホームページ、Web メール参照用の仮想サーバーを用意）経由のインターネット参照（Q67）



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、「わからない」が 34.8%で最も割合が高く、ついで「賛成」が 32.6%であった。

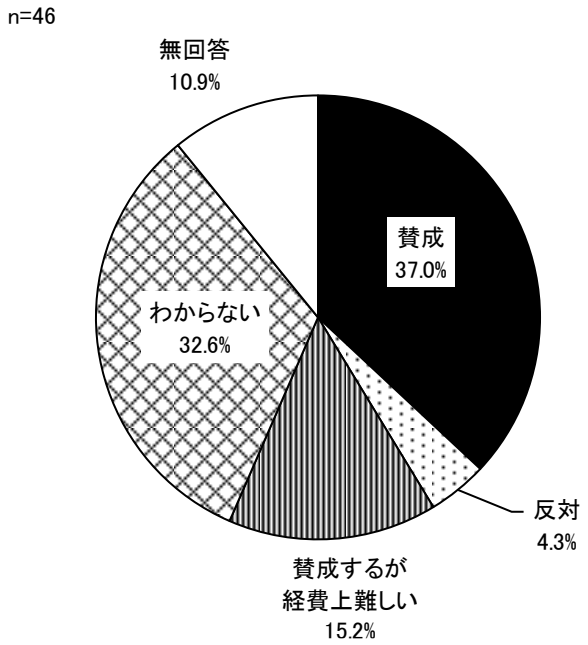
図表 89　組織内のサーバー（ハード系）を仮想サーバー、仮想ストレージ、仮想ネットワーク等を用いて病院あるいは委託契約にて統一的に導入管理を行う（Q68）



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」が 37.0%で最も割合が高く、ついで「わからない」が 32.6%であった。

図表 90　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）

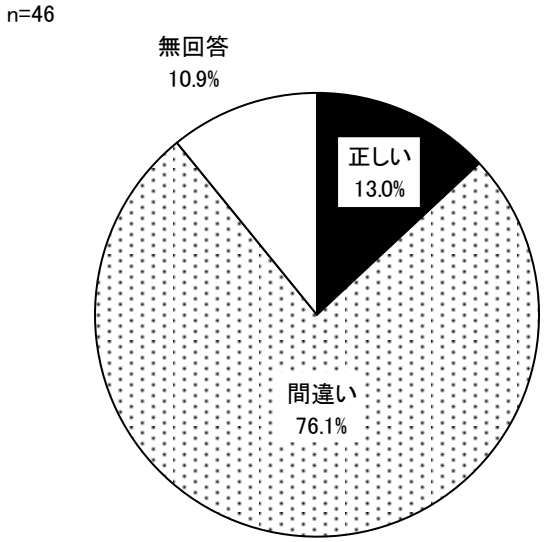


（8）最近のサイバー攻撃に対する理解度

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」

「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」については、「間違い」が76.1%であった。

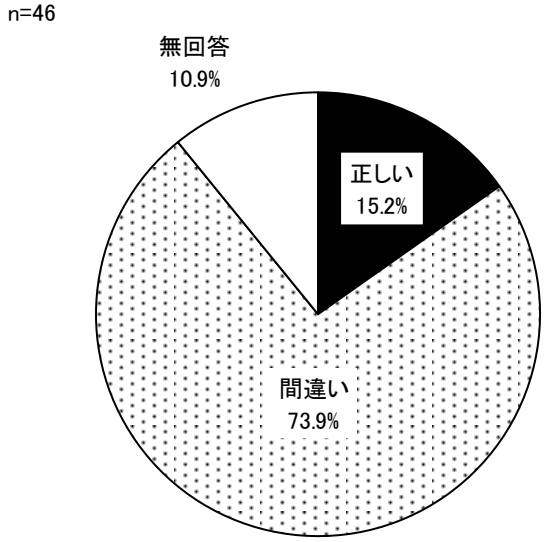
図表91　「データを暗号化されたPC、サーバーに必ずウイルスは見つかる」（Q70）



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」

「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」については、「間違い」が 73.9%であった。

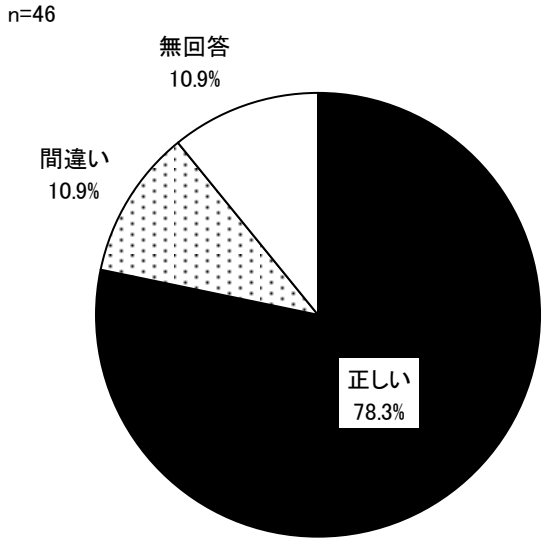
図表 92　「A さんからウイルス添付メールが届いた場合、A さんの PC はコンピュータウイルスに感染している」(Q71)



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」

「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」については、「正しい」が 78.3%であった。

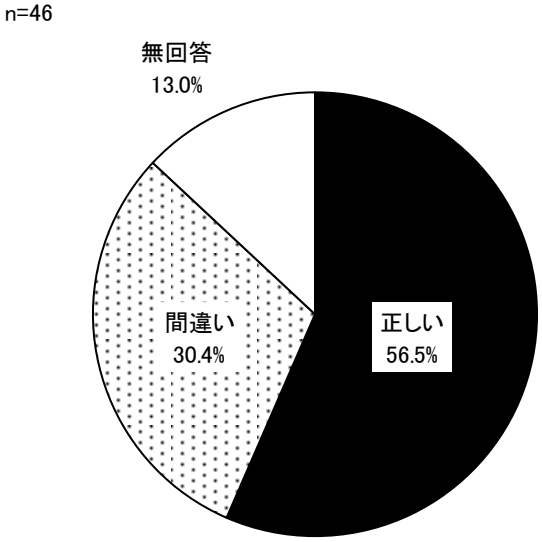
図表 93　「Windows のアクティブディレクトリやバックアップの設定ファイルは攻撃される」(Q72)



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」

「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」については、「正しい」が 56.5%であった。

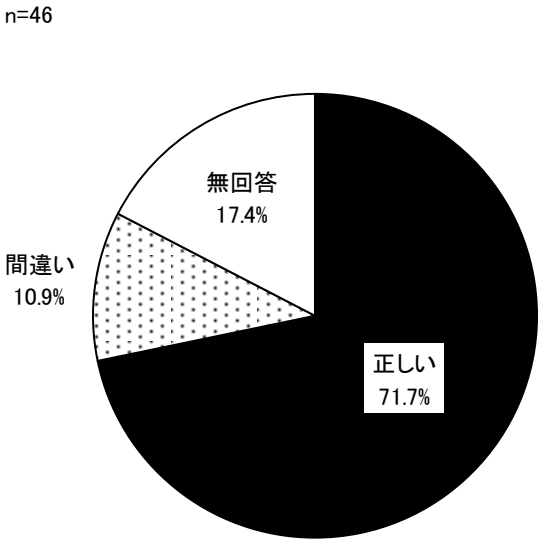
図表 94　「大容量のファイル全体の暗号化は時間がかかるので一部の暗号化をするものもある」(Q73)



5)「攻撃を受けた場合に IPA、NISC に対応、助言する窓口がある」

「攻撃を受けた場合に IPA、NISC に対応、助言する窓口がある」については、「正しい」が 71.7%であった。

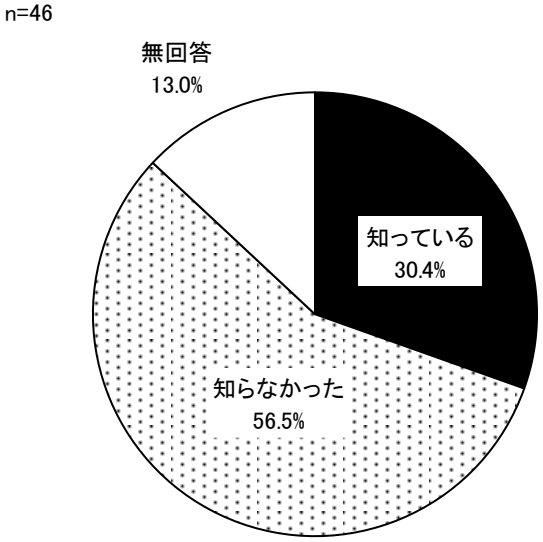
図表 95　「攻撃を受けた場合に IPA、NISC に対応、助言する窓口がある」(Q74)



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」

「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」については、「知らなかった」が 56.5%であった。

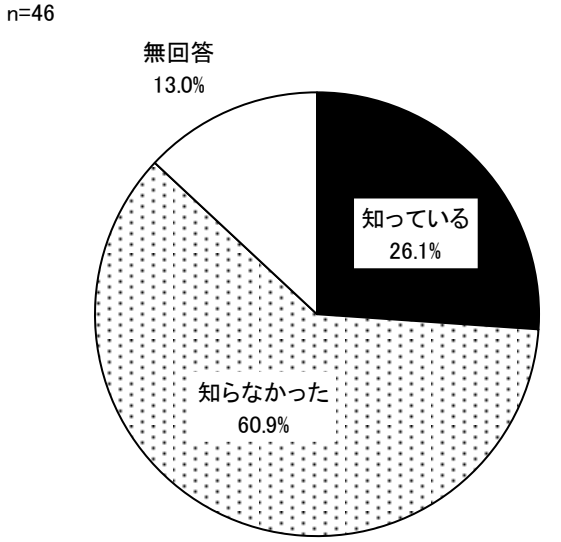
図表 96　「NISC の 3、2、1 ルールでは 3 つのデータ、2 つにバックアップ、1 つのオフラインバックアップが提唱されている」(Q75)



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」

「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」については、「知らなかった」が 60.9%であった。

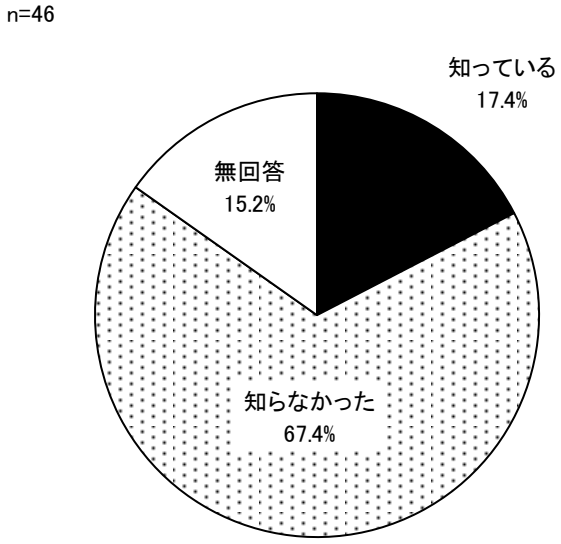
図表 97　「NICT のサイバーセキュリティ研究所のデータでは IoT 機器の攻撃が半数以上である」（Q76）



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」

「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」は、「知らなかった」が 67.4%であった。

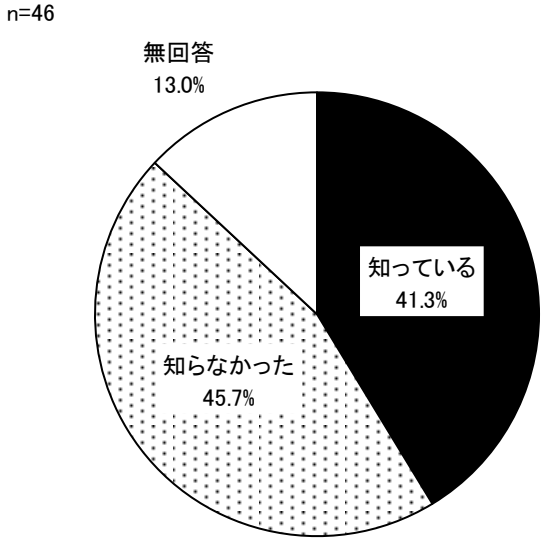
図表 98　「国際医療機器規制当局フォーラム文書におけるサイバー攻撃対策について」（Q77）



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」

「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」については「知らなかった」が 45.7%であった。

図表 99　「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」(Q78)

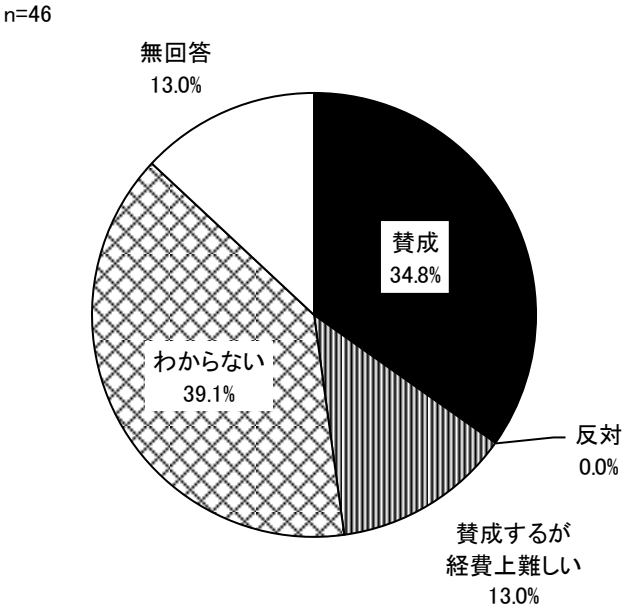


(9)重要データの保存について実施している事項

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、「わからない」が39.1%で最も割合が高く、ついで「賛成」が34.8%であった。

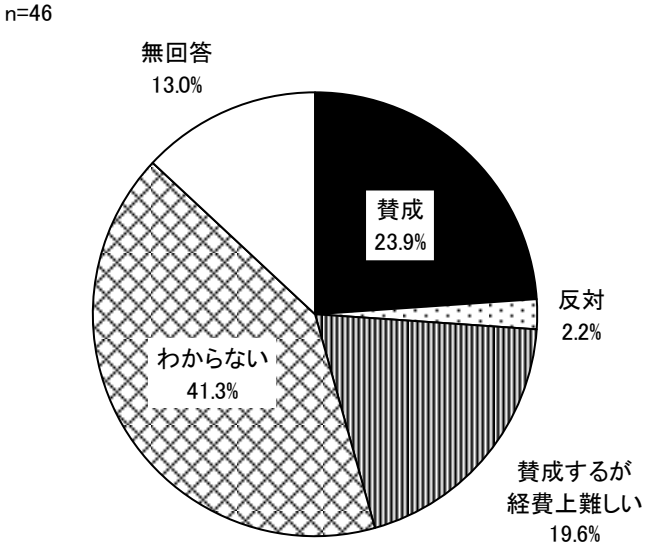
図表100　RAIDによるリアルタイムの保存（Q79）



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、「わからない」が 41.3%で最も割合が高く、ついで「賛成」が 23.9%であった。

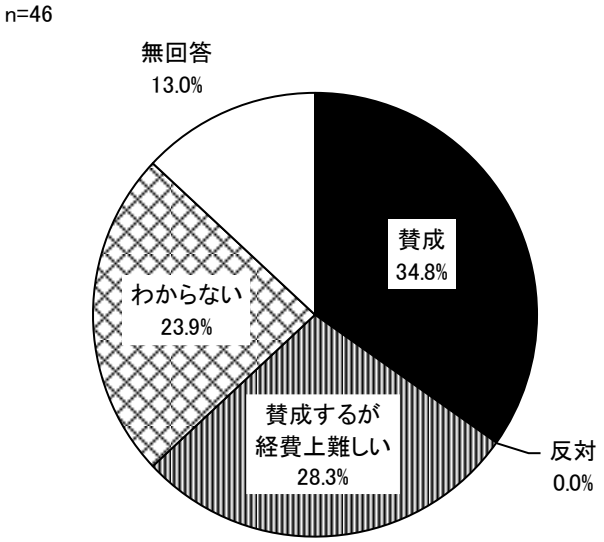
図表 101　RAID 以外にリアルタイムのバックアップを用意する（Q80）



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」が 34.8%で最も割合が高く、ついで「賛成するが経費上難しい」が 28.3%であった。

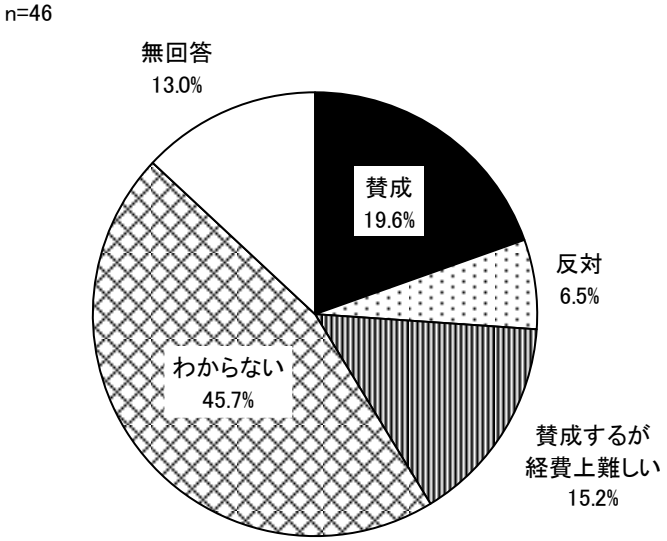
図表 102　遠隔地にリアルタイムのバックアップをする（Q81）



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、「わからない」が 45.7%で最も割合が高く、ついで「賛成」が 19.6%であった。

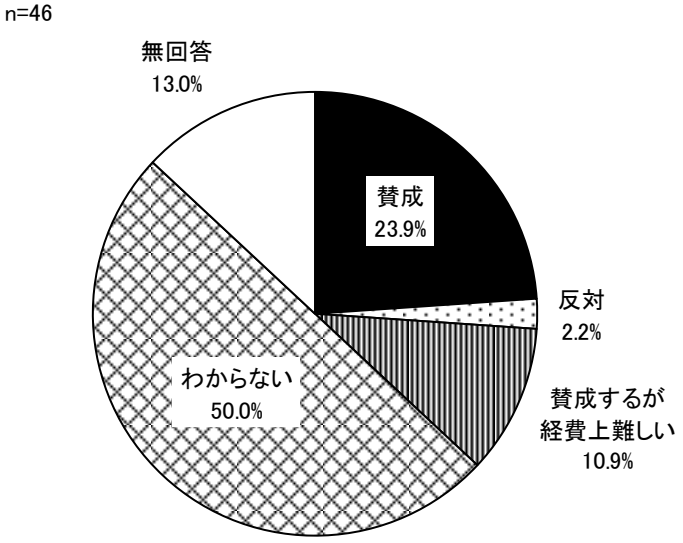
図表 103　ジュークボックス型の磁気テープユニットによる日々のバックアップ（Q82）



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 50.0%で最も割合が高く、ついで「賛成」が 23.9%であった。

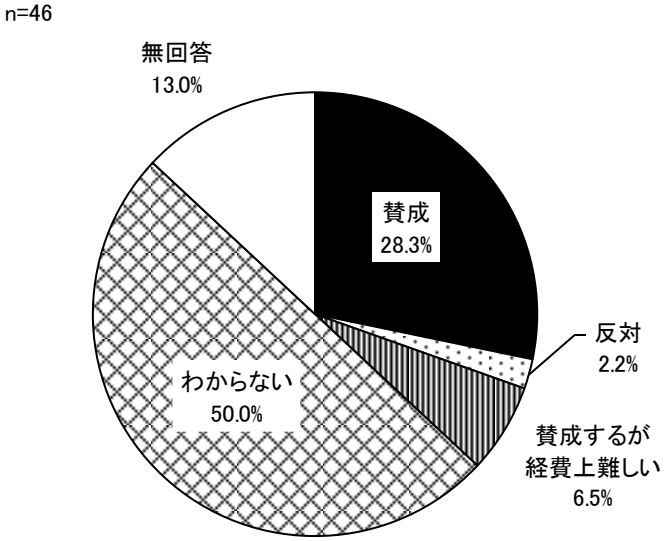
図表 104　SS-MIX フォルダーから地域連携サーバーが pull する仕組みで地域連携側にバックアップできる（Q83）



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、「わからない」が 50.0%で最も割合が高く、ついで「賛成」が 28.3%であった。

図表 105　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）

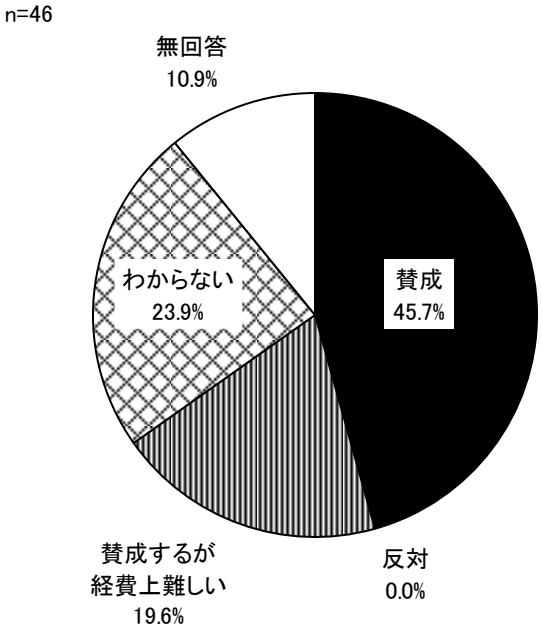


（１０）情報部門の管理について

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45.7%で最も割合が高く、ついで「わからない」が23.9%であった。

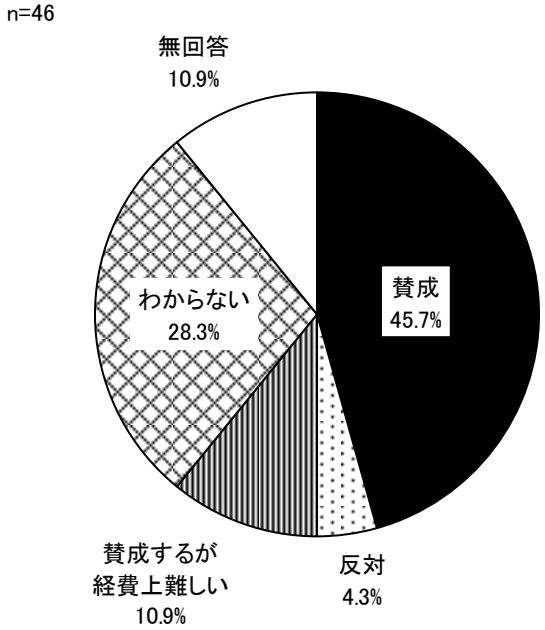
図表106　管理者のサーバー等の管理に用いるPCとメール・ホームページ参照のPCとは別の機器、別のネットワークを用いる（Q85）



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 45.7%で最も割合が高く、ついで「わからない」が 28.3%であった。

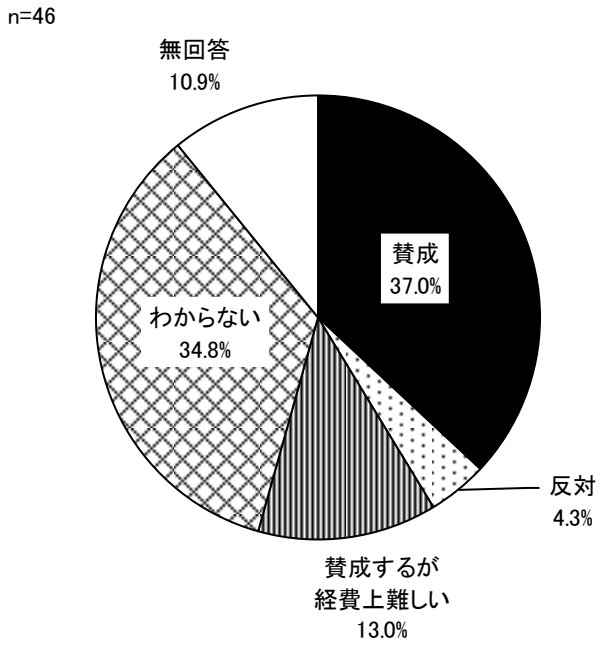
図表 107　委託業者の院外からの接続は事前に時間等を連絡させ、時間、接続先を限定する（Q86）



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 37.0%で最も割合が高く、ついで「わからない」が 34.8%であった。

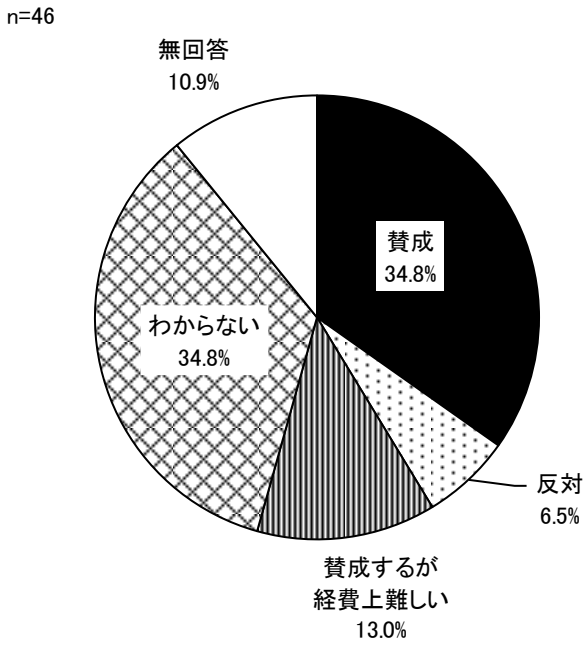
図表 108　委託業者の院外からの接続は事前に時間・接続先等を連絡させファイアウォールの接続を制限する（Q87）



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」および「わからない」がいずれも 34.8%で最も割合が高く、ついで「賛成するが経費上難しい」が 13.0%であった。

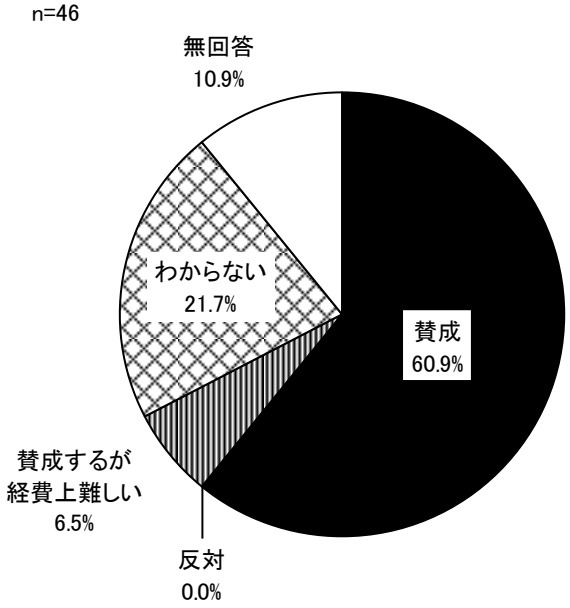
図表 109　委託業者の院外からの接続はリモートアクセス、シンクライアントなどを用いて直接接続させない（Q88）



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 60.9%で最も割合が高く、ついで「わからない」が 21.7%であった。

図表 110　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）

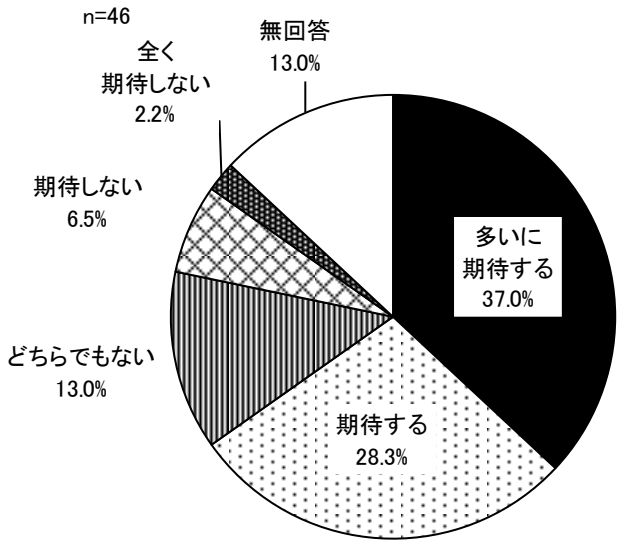


（１１）ISAC※について情報共有したい事項等　※Information Sharing and Analysis Center

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」が 37.0%で最も割合が高く、ついで「期待する」が 28.3%であった。

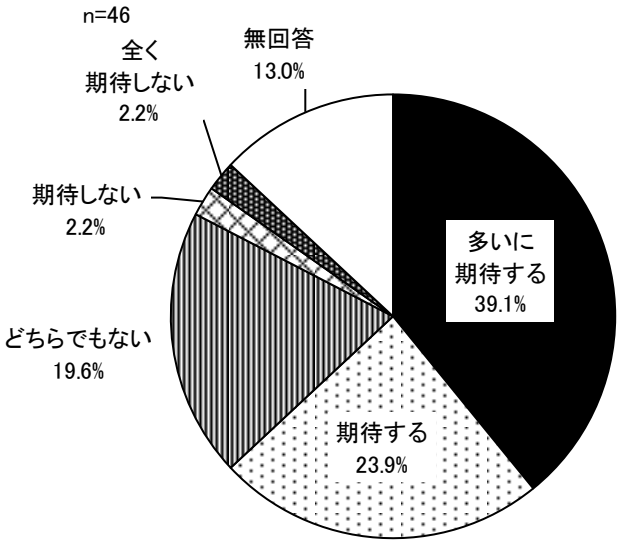
図表 111　流行しているマルウェア（ウイルス）等、リスク関連の情報（Q90）



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 39.1%で最も割合が高く、ついで「期待する」が 23.9%であった。

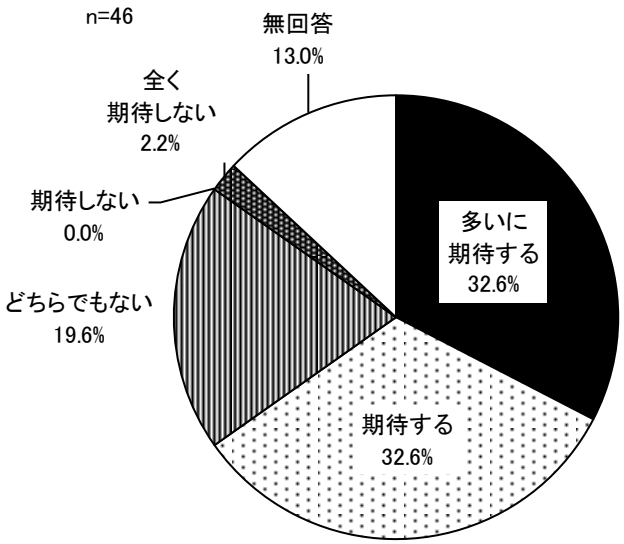
図表 112　セキュリティ対策の具体的な実施方法（Q91）



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」および「期待する」がいずれも32.6%で最も割合が高かった。

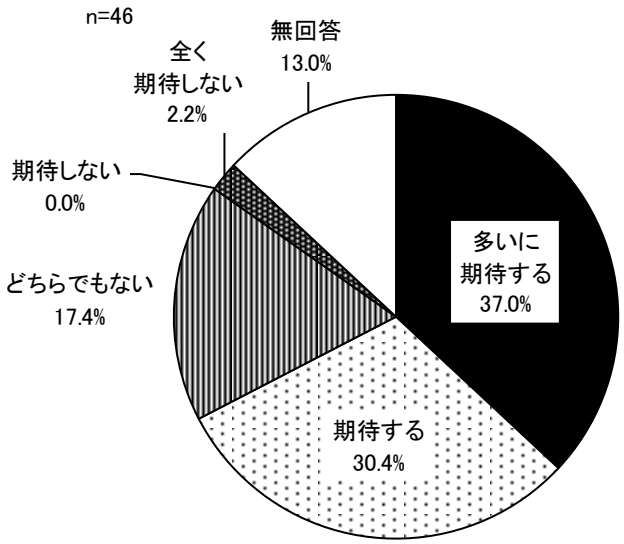
図表 113　マルウェア検体の分析（Q92）



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37.0%で最も割合が高く、ついで「期待する」が30.4%であった。

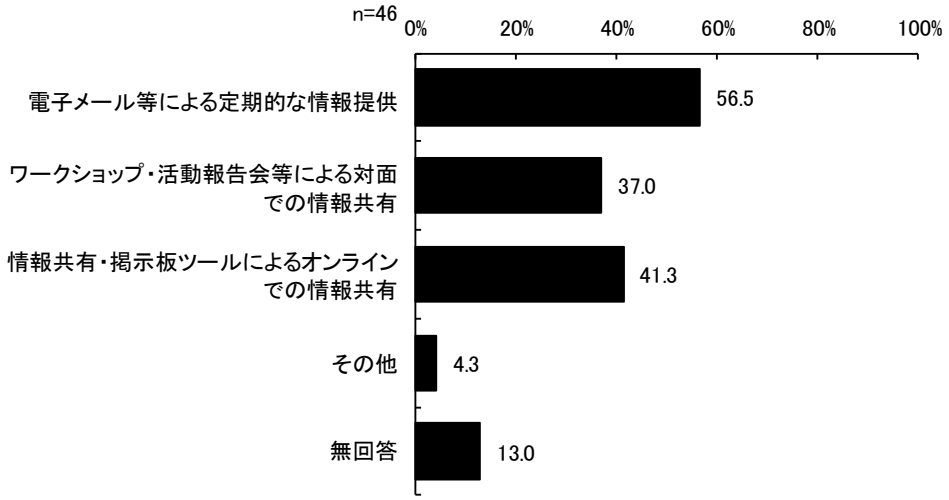
図表 114　セキュリティ教育教材の提供（Q93）



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 56.5%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 41.3%であった。

図表 115　情報共有の手段について（Q94）【複数回答】

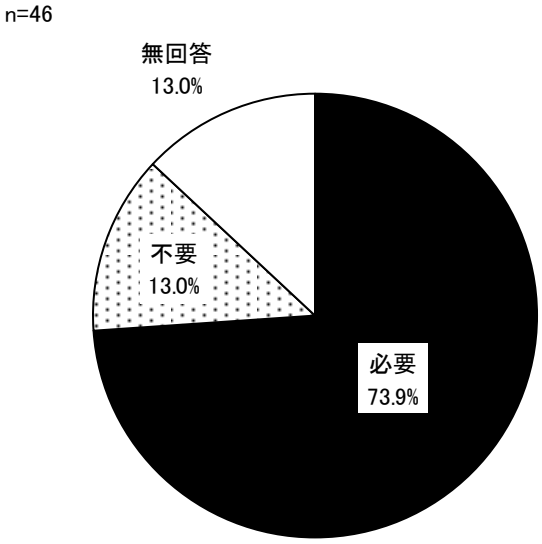


※「その他」の主な回答は以下の通り。
・SNS

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 73.9%であった。

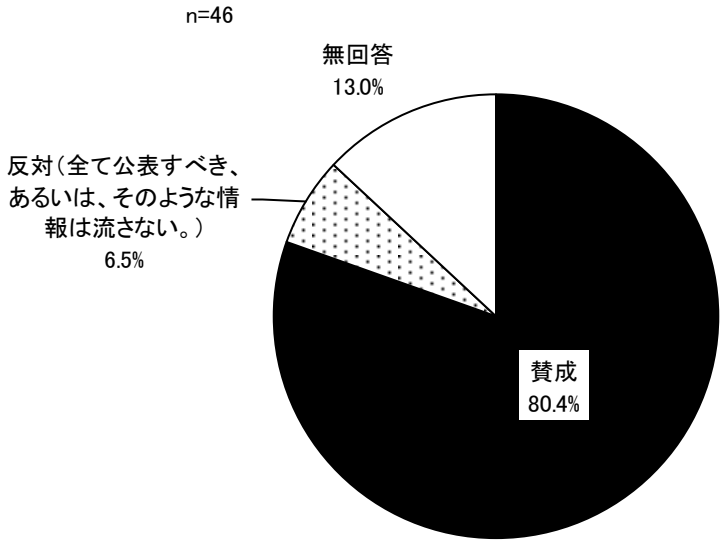
図表 116　知識レベルが同じではないので、技術的指導者が必要（Q95）



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 80.4%であった。

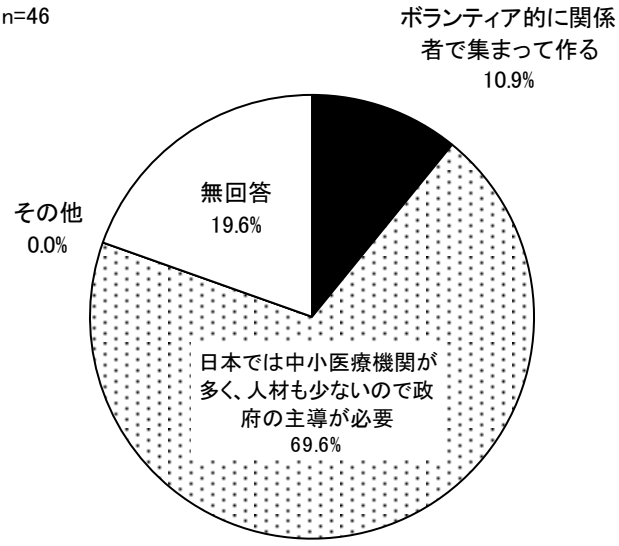
図表 117　共有するべき情報には噂、予想なども含む必要があり、公表しにくいものがあると思う（Q96）



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 69.6%で最も割合が高く、ついで「ボランティア的に関係者で集まって作る」が 10.9%であった。

図表 118　組織のあり方について（Q97）



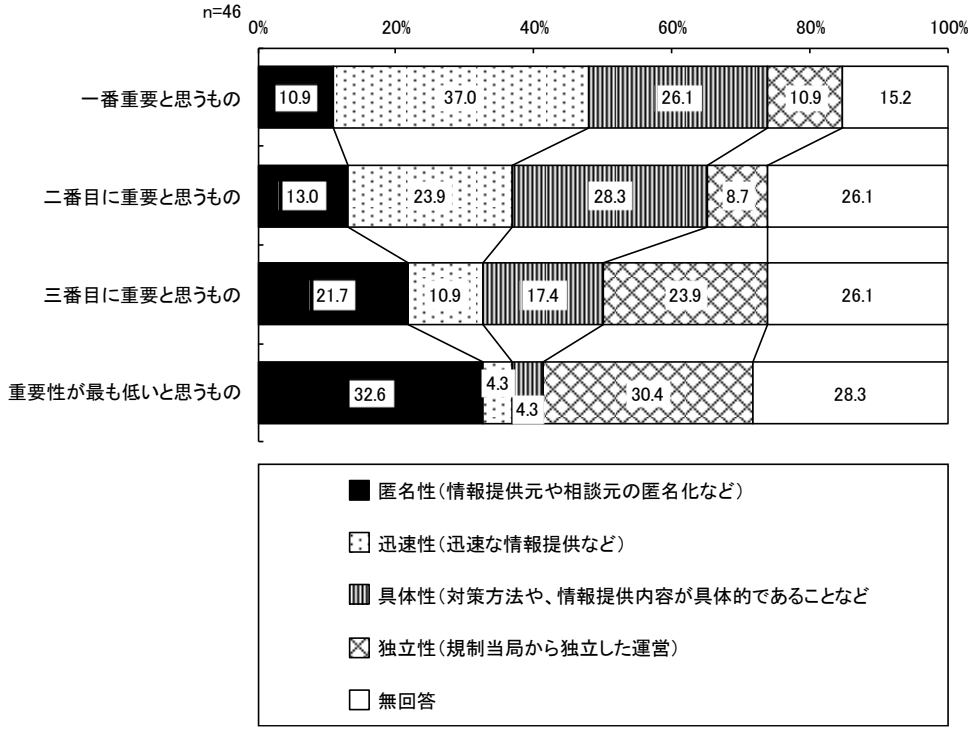
9）サイバーセキュリティ情報の公的共有組織に必要な要素の重要度

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、迅速性（迅速な情報提供など）が 37.0%で最も割合が高く、ついで具体性（対策方法や、情報提供内容が具体的であることなど）が 26.1%であった。

逆に、重要性が最も低いと思うものについては、匿名性（情報提供元や相談元の匿名化など）が 32.6%で最も割合が高く、ついで独立性（規制当局から独立した運営）が 30.4%であった。

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

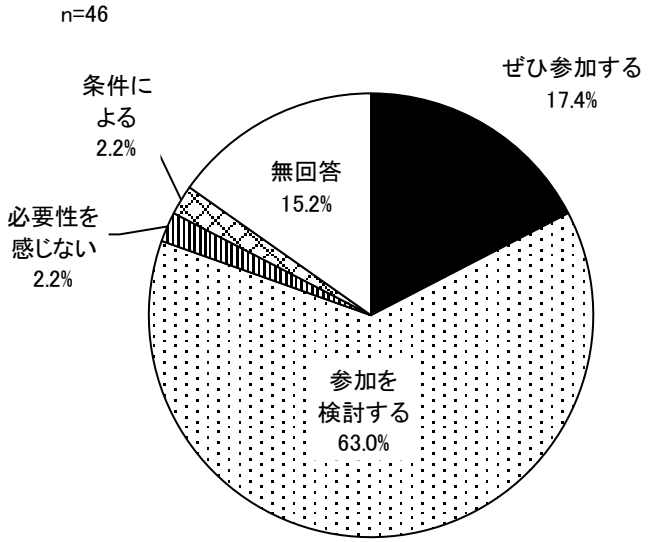
図表 119　サイバーセキュリティ情報の公的共有組織に必要な要素の重要度（Q98～Q101）



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 63.0%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 120　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」の主な回答は以下の通り。
・組織で登録して随時参加可能/必要なメンバが参加できるようにする

（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 121　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

・医療機関は報酬では縛られているが、セキュリティでは縛られているとは思っていない。また、広報が極めて専門的で理解されていないことが多い。例えば、ウイルスの脅威はなんとなく理解されるが、そこから突然“VPN”という言葉を使い理解が吹き飛んでいるように見える。 ・現在の医療関係者の IT リテラシーレベルでは、自主的集まりで ISAC を構成しても、事実上機能しない。NISC 等が主導した設置・運営が適切。

2）本アンケートについて意見や提案など

図表 122　本アンケートについて意見や提案など

・100 問のアンケートにどれだけ皆さんがまじめに答えられているか興味があります。 ・かなりサイバーセキュリティの知識を持っている人しか回答できないと思うので、対象者を限定してはいかがでしょうか。 ・医療機関向けの質問と思われる質問が多かった。(医療機関向けのアンケートだったのか) ・現在医療機関に勤めていないので、あまり参考にならなかったと思います。アンケートに答えてしまい申し訳ございませんでした。 ・質問数が多すぎます。 ・質問内容を予めカテゴリー別にし、勤務機関別や職種別による該当者が答えられるようだと助かります。 ・短い時間で準備なさったので仕方が無いことではあるが、RAID を RAIDS と書かれているなど、質問の詰めが甘い印象がある。また、大学病院のような、組織内組織には必ずしも適切で無い質問形式も多い。遠隔医療学会の構成員を考えると、若干偏りのあるデータ収集となってしまうのではないか。 ・同じような質問を繰り返しされているように見えるところがある。違いがよくわからない設問があった。 ・内容が専門的なので一般の医療従事者として加入している会員には回答不能な点も多くありました。

第３章　まとめ

１．調査結果の概要

（1）サイバー攻撃の脅威や課題への認識

近年、医療等分野及び医療情報システムに対するサイバー攻撃の多様化・巧妙化が一層進み、医療機関等における診療業務等に大きな影響が生じる被害が見られ、特にランサムウェアに代表される攻撃への対策は、喫緊の課題となっていることが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、ガイドラインと表す）[1]で指摘されている。

本調査の回答者においても、最近のサイバーテロの目的（Q44）として「情報に関する金銭要求」（82.6%）、「個人情報の取得」（71.7%）が上位に挙げられており、ガイドラインで指摘されていたものと同様の認識がなされていた。

サイバー攻撃を脅威と感じているか（Q46）については、サイバー攻撃を脅威と感じていないとの回答者はおらず全ての回答者が脅威と感じていた。しかしながら、「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）」（17.4%）、「脅威と感じているが対策の経費が出せない」（10.9%）、「脅威と感じているが対策がわからない」（6.5%）、「脅威と感じているが対策できる人材がいない」（4.3%）（以上４項目合わせて 39.1%）と約４割の回答者の施設では、人材や経費、対策方法のノウハウが不足しているために対策ができていない状況であった。

また、所属機関のサイバーセキュリティの課題（Q41）として、全 13 個の選択肢の回答割合は 20%から 70%と一定割合の回答者が課題として認識しており、中でも上位３位は、「メール添付ウイルス侵入」（71.7%）、「メール URL からのウイルス侵入」（67.4%）、「外部ネットワークからの侵入（ハッキング）」（65.2%）があげられ、外部からのウイルス等の侵入対策を課題と認識する機関の割合が高かった。

（2）サイバーセキュリティに関する知識

本調査では回答者のサイバーセキュリティに関する知識を問う設問を設けた。

まず正誤を問う５つの設問について、サイバー攻撃に関する設問（Q70～Q72）の正答率は 70%代、ファイルの暗号化に関わる設問（Q73）の正答率は 50%代、IPA、NISC の窓口に関する設問（Q74）の正答率は 70%代であり、それぞれの設問において正しく認識できていない回答者が一定程度、認められた。

＜正誤を問う設問＞
・「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」→正解は「間違い」

[1] 「医療情報システムの安全管理に関するガイドライン」第 5.2 版（令和４年３月厚生労働省）

（76.1%）
・「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」→正解は「間違い」（73.9%）
・「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」→正解は「正しい」（78.3%）
・「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」→正解は「正しい」（56.5%）
・「攻撃を受けた場合に IPA、NISC に対応、助言する窓口がある」→正解は「正しい」（71.7%）

また事柄を知っているか否かを問う 4 つの設問（Q75～Q78）について、「知っている」との回答割合は最も高いものでも「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」の 41.3%であり、4 問のいずれについても、「知っている」との回答は半数に満たず、総じてあまり認知されていない状況であった。

＜知っているか否かを問う設問＞
・「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」→「知っている」が 30.4%
・「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」→「知っている」が 26.1%
・「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」が 17.4%
・「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」→「知っている」が 41.3%

（3）サイバーセキュリティへの対応の実態

ガイドラインで規定されている「組織的安全管理」などの安全管理の観点ごとに、関連する調査結果を整理した。

1）組織的安全管理の観点

情報システム統括部署があるかとの問い（Q9）については、「いいえ」との回答が 37.0%であった。CSIRT（Q17）が存在するとの回答は 15.2%であり、「ない」、「検討中」、「知らなかった」の合計は 76.1%であった。

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）について、「担当者は決まっていない」との回答が 10%存在した。

情報セキュリティポリシーを規定しているかとの問い(Q34)については、「いいえ」が 28.3%、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との問い（Q36）については、「いいえ」が 39.1%、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

ているかとの問い（Q37）については、「決まっていない」との回答が 10.9%であった。情報セキュリティに関する職員の組織内の相談先（Q39）については、「決まっていない」との回答が 13.0%であった。

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との問い（Q40）については、「知らない」との回答が 63.0%であった。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との問い（Q52）については、「知らない」との回答が 58.7%であった。

院内ネットワーク全体図の作成がされているかとの問い（Q59）については、「多くの異なったベンダーにより形成されており全体図はない」との回答が 26.1%であった。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との問い（Q60）については、「作成していない（未検討だった）」が 13.0%であった。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との問い（Q61）については、「作成していない（未検討だった）」が 10.9%であった。

2）技術的安全管理の観点

院内における職員のインターネットの利用可否（Q20）については、「電子カルテ等の診療記録を扱う端末から利用可能」との回答が 13.0%あった。インターネットにアクセスできるパソコン（Q22）については、「事務系（医事会計）の PC からアクセスできる」が 32.6%あった、「診療系の PC からアクセスできる」が 15.2%あった。

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）については、「診療系ネットワークへの接続を許可している」（4.3%）、「事務、研究系ネットワークへの接続を許可している」（28.3%）、「診療、事務、研究系ネットワークへの接続を許可している」（4.3%）の合計が 36.9%であった。

「資産管理ソフトを導入しているか」との問い（Q26）に対し、「いいえ」との回答が 39.1%みられた。「仮想ブラウザを導入しているか」との問い（Q27）に対し、「いいえ」との回答が 37.0%みられた。

「外部セキュリティ監査を受けているか」との問い（Q31）に対し、「受けていない」が 43.5%みられた。

「直近 3 年以内にペネトレーションテストを受けているか」との問い（Q32）に対し、「受けていない」が 43.5%みられた。

「侵入経路の対策としての事前調査、監視の対象」（Q53）については、「外部接続の調査（情報システムのみ）」、「ファイアウォール、VPN の機器リスト、ソフトのバージョン」がいずれも 50.0%で最も割合が高かったが、選択肢にあげられた全ての事項がリスクとなりうるため、これらも事前調査、監視の対象とすることが望まれる。

「端末への EDR（Endpoint Detection and Response）導入状況」（Q62）については、「導入していない」が 23.9%あった。

３）人的安全対策の観点

回答者のガイドラインの認知状況等（Q35）について、「名前は知っている」と「知らない」との回答は合計で 28.2%であった。

「セキュリティ教育を行っているか」との問い（Q28）に対し、「はい」が 54.3%あったのに対し、「いいえ」が 32.6%あった。また「セキュリティ訓練を行っているか」との問い（Q33）に対し、「はい」が 23.9%であったのに対し、「いいえ」は 47.8%であった。

４）災害、サイバー攻撃等の非常時の対応の観点

インシデント発生以前の事前調査に対する意識（Q48）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 58.7%であったのに対し、「保守契約していれば各部署に任せることで良い」が 15.2%であった。

５）外部のネットワーク等を通じた情報交換時の対応の観点

ホームページ閲覧に関する対策（Q50）としては、「危険なものを接続させない」（45.7%）、「安心なもののみ接続させる」（19.6%）とのリスクの低い対策にかかる回答が合計 65.3%を占めたが、一方で「制限しない」との回答も 28.3%あった。

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（Q55）について「各部署に任せている」との回答が 34.8%あった。オンライン診療・遠隔モニタリング・院内 SNS の接続（Q56）について「各部署に任せている」との回答が 37.0%あった。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（Q57）について、「各部署に任せている」との回答が 41.3%あった。

（４）属性別の分析

情報システム統括部署（Q9）、情報セキュリティ対策担当部署（Q11）、CSIRT（Q17）の有無が情報セキュリティ対策の実施に影響を及ぼしているかの分析を試みた。なおアンケート調査への回答数が少ないため、参考値とする点に留意が必要である。

情報システム統括部署や情報セキュリティ対策担当部署、CSIRT（以下、情報システム統括部署等）の有無と、資産管理ソフトの導入（Q26）、仮想ブラウザの導入（Q27）、セキュリティ教育の実施状況（Q28）、外部セキュリティ監査を受けているか（Q31）、ペネトレーションテストを受けているか（Q32）、セキュリティ訓練の実施状況（Q33）、情報セキュリティポリシーの規定状況（Q34）の関係についてみた。資産管理ソフト、仮想ブラウザの導入については、情報システム統括部署等が存在する機関では導入されている機関の割合が高かった。セキュリティ教育などその他の事項についても同様に、情報システム統括部署等が存在する機関の方が実施されている割合が高かった。

このことから情報システム統括部署等が機関におけるこれらの情報セキュリティ対策を推進することで、対応が進んでいる可能性がある。

(5)ISAC への要望事項

医療分野の ISAC[2]は現状存在しないが、仮に存在する場合における情報共有の在り方や参加意向（Q90～Q104）について以下に示す。

ISAC による情報共有への期待度についてみる。提示したいくつかの事項に対し「多いに期待する」または「期待する」と回答した割合の合計についてみると、「流行しているマルウェア（ウイルス）等、リスク関連の情報」は 65.3%、「セキュリティ対策の具体的な実施方法」は 63.0%、「マルウェア検体の分析」は 65.2%、「セキュリティ教育教材の提供」は 67.4%と、いずれも 6、70%程度の回答者が期待し、一定のニーズがあることが認められた。

情報共有の手段としては、「電子メール等による定期的な情報提供」が 56.5%と最も割合が高かったが、回答者による定期的に重要な情報を網羅的に把握したいという意識の表れと考えられた。また「知識レベルが同じではないので、技術的指導者が必要か」との問いに対しては、「必要」との回答が 73.9%と高かったが、提供される情報の信頼性を高めてほしいとのニーズの表れと考えられた。

ISAC の組織のあり方への要望としては、「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 69.6%で、「ボランティア的に関係者で集まって作る」（10.9%）の回答割合を上回った。また「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」との問いに対して、「ぜひ参加する」、「参加を検討する」との回答の合計は 80.4%で、回答者の多くが ISAC への参加を前向きにとらえている状況と考えられた。

２．今後に向けた対応

(1)ガイドライン第 5.2 版への対応など個別施設の体制強化

１）組織的安全管理の観点

調査結果から、情報システム統括部署や情報セキュリティ担当部署、CSIRT がある機関においては、ない機関と比べてセキュリティ対策が進んでいる傾向がみられた。

この調査結果から、サイバーセキュリティ対策を推進する上で、担当組織の設置は重要と考えられる。しかしながら回答者の所属する機関には、情報システム統括部署がないところが約 4 割存在した。このような機関ではまずは担当部署の設置することが望まれる。

２）技術的安全管理の観点

診療系システムのネットワークがインターネットに接続され、インターネットを通じた外部からの侵入等の脅威が存在する運用がなされている施設が一部で存在した。このようなシステムの脆弱性を把握する手段として、外部セキュリティ監査やペネトレーションテストを受けることが考えられるが、いずれも受けていないところが約 4 割存在した。必要な対策を

[2] Information Sharing and Analysis Center

講じるため、まずは監査やテストを受けシステムの脆弱性を把握することが望まれる。

３）人的安全対策の観点

セキュリティ教育や訓練が行われていない施設が一定の割合で存在していたが、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減を図るために、教育や訓練を実施することが望まれる。

４）災害、サイバー攻撃等の非常時の対応の観点

サイバー攻撃を脅威と感じていながらも、約 4 割の回答者の施設では、人材や経費、対策方法のノウハウが不足しているために対策ができていない状況であったが、対策方法のノウハウについては外部機関に助言を求めることなどを通じた対応が望まれる。

５）外部のネットワーク等を通じた情報交換時の対応の観点

ホームページ閲覧を制限しない施設が 3 割存在し、地域連携や遠隔病理診断などでの接続について各部署に任せるとの回答が約 3 割存在したが、機関として一元的に管理することがリスク低減につながると考えられる。

（２）施設間連携による体制強化

回答者から所属機関のサイバーセキュリティに関する課題が多く挙げられていたが、この中には、情報セキュリティへの対応が比較的進んでいると考えられる CSIRT を設置する機関に所属する回答者も含まれていたことから、個々の施設においてサイバーセキュリティ対策を十分に行うことは、本調査では具体的に明らかにできていないが何らかの制約があり、難しいのではないかと考えられた。この他、サイバーセキュリティ対策にかかる情報収集や、複数施設で連携して対応することが可能な施策の検討や運用などを効率的に行う観点から、施設間で連携して対策を行うことが有用と考えられた。

この施設間連携の具体的なあり方として、ヘルスケア ISAC を創設・運用することが考えられるが、本調査で ISAC に対する意向をうかがったところ、流行しているマルウエアやセキュリティ対策の具体的な実施方法などの情報提供について ISAC に期待する回答者や、ISAC への参加を希望する医療機関が一定割合でみられたことから、今後は、ISAC の創設に向け、本調査の対象となっていない医療機関においても ISAC へのニーズが一定割合であることを把握することが望まれる。

以上

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）
Q106 ご意見いただいた方で、今後ディスカッションにご協力いただける方は、お名前、ご所属、メールアドレスなどをご記入ください。なお、本欄にご記入いただいても、Q103 以前の分析には用いません。ディスカッションのみに利用いたします。	（自由記述のため、選択肢はなし）