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

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
(21IA2013)

令和３～４年度　総合研究報告書
研究代表者　近藤　博史

令和５年　３月

目次

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
総合報告

研究代表者　近藤博史
特定非営利活動法人日本遠隔医療協会
研究分担者
山本隆一　財団法人医療情報システム開発センター
美代賢吾、　国際医療研究センター
星本弘之、辻岡和孝
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として、技術状況や課題の総合的検討、複数の病院のセキュリティ管理状況調査、日本病院会会員施設へのセキュリティ管理状況に関するアンケート調査、医療情報システムの安全管理ガイドラインへ反映すべき課題の調査、院内へのサイバーセキュリティ訓練の手法の調査等を行った。

1．総合報告

（1）目的

重要インフラに該当する医療分野において、医療機関等のサイバーセキュリティに対する取り組みを強化することは喫緊の課題である。病院情報システムは、これまで外部と隔絶した情報ネットワークであった状況に対し、データヘルス改革、働き方改革、オンライン診療、モバイルヘルス(m-Health)等の導入で外部ネットワークへの接続が始まっている。情報化が進んでいなかった小規模病院、診療所における電子カルテの導入・普及も進みつつある。また、今後、拡大する m-Health 機器（携帯に連携した継続的なモニタリングと適時な介入をする治療アプリを含む。）は病院、診療所のシステムと連携され、研究基盤として活用されることも考慮する必要がある。同時に、進化するクラウド技術により、医療機関内にあったサーバをクラウド上に移行することも現実的になりつつある。

一方、サイバーセキュリティ対策も閉じたネットワークの出入口監査から、エンドポイント検知、ゼロトラストと言われるような内外の区別が無く直接個々の端末を対策する取組が重視されるようになってきた。このように変化と対策の将来像は双方合致した状況に見えるが、正反対の現状から理想の将来像に如何に安全に効率的に移行するかが喫緊の課題と言える。

本研究では、国内及び諸外国の EMR、EHR、PHR、m Health および臨床研究ネットワークも含めた対象について調査を行い、医療機関等の現場に即したサイバーセキュリティ対策を次世代技術や他分野の手法も踏まえて整理し、現在および今後の状況に即した対策のあり方を教育・情報共有も含め検討する。

具体的には、医療分野におけるサイバーセキュリティ対策と課題について医療機関の規模・ユースケース等ごとに整理するとともに、医療機関同士が相互にサイバーセキュリティ対策に関する情報共有・相談を行う体制のあり方等を検討し、医療機関等への対策強化の普及・促進策等を検討する。さらに、諸外国の先進的な医療クラウドの事例調査と、国内における医療情報システムのクラウド化などの先例調査と現場意向調査を行い、日本のニーズから近未来化を効率的かつ迅速に進めるためのクラウド化の方向性を検討する。最後に現状の医療機関のサイバーセキュリティ対策の強化を迅速に広範囲に適合するための方策について、クラウド化を含めて提案し、その手引き等の作成を行う。

（2）研究結果の概要

医療のクラウド利用への変化は診療所用クラウド型電子カルテと、歩数、脈拍、体重、血糖値などの計測モバイルヘルス系のクラウド利用が進んでいる。一方、大規模病院のクラウド移行については鳥取大学が 2020 年にクラウドサーバのオンプレミス構築がクラウドサーバ移行の技術的可能性は明確にした。同時に、シンクライアントによる地域連携システムのスマートフォン通信を介した高速表示は専用回線と共に利用して通信切断時の予備通信回線の技術的課題をクリアしたと言える。2021 年には福井大学病院のクラウドサーバ移行が具体的な実現を示した。ただ、そのコストはオンプレミスと同程度であったので、今後のクラウドサービス利用の増加によるスケールベネフィット効率化を待つ必要があることがわかった。クラウドサービスにおけるセキュリティに関しては AWS から 2 回聴取し、クラウドサービスにおけるセキュリティの責任分界点と利用者の設定ミス時の利用者責任部分の課題が明確になり、その対策として十分な説明資料のサービスの充実が図られていた。一方、シンポジウムにおいて医療情報システムの安全管理ガイドラインに掲載された CSIRT 組織化については、医療機関からの困難な状況の指摘があり、具体的要件情報の収集のため、金融系 CSIRT 委託事業者と IPA から事情を聴取し、攻撃後ではなく、攻撃前の調査の重要性が明確となった。具体的には外部接続の確認、これには接続の FW, VPN ルータの機種、ソフトウェアのバージョン、設定内容、保守体制を含む。また、外部接続と内部ネットワーク全体図、そこにおけるサーバとクライアント端末の関係も資料作成が必須であった。ただ、医療機関の場合は種々のネットワーク、機器が次期と部署が異なり統合管理部署がないことも明確になった。例えば、情報システムと放射線部門の購入するＣＴ、ＭＲＩなどの検査機器とそのオンライン保守回線があげられる。現地保守契約でもコロナ禍でいつの間にかオンライン保守化した事例もあった。事前調査の困難さが明確になった。また、NHK のインタビュー体験から一般への説明の困難さ、これは ISAC 内での情報共有の困難さにも関係するが、知識のある専門家間では相対的安全性の議論がされることの理解の重要性が明確になった。令和 3 年度、4 年度のアンケート調査では既存技術でセキュリティレベルを上げる仕組みの理解度を聞くことにした。

医療機関内にあるサーバをクラウド上に移行する方法についてはオンプレミスでクラウドサーバ類似のサーバを導入した鳥取大学医学部附属病院の事例や実際に現状でクラウドサーバの利用を開始した福井大学医学部附属病院の事例の情報収集をしていたが、2021 年度に発生した VPN と FW の複合機の脆弱性をついたサイバー攻撃事例の頻発により、シンポジウム等を介した情報収集は IPA の CSIRT 活動を中心に始めた。日本医療情報学会春季学術大会では事前の①事前のネットワーク調査、②ネットワーク・サーバ機器の資産台帳の整備、③脆弱性が判明した場合の医療機関の知るタイミング、知った後の対応の問題。攻撃後では③ネットワーク、機器の情報収集の時間の必要性、④ハッカーの潜入機関が 100 日以上になる場合がある。⑤画像のような大容量データも一部の暗号化の場合がある。⑥暗号化されたデータの複合化をしても前の状態と同じかの証明ができない問題。などが明確になった。これによりデータバックアップと BCP の問題が明確になったため、日本遠隔医療学会総会ではストレージに絞って情報収集し、①フラッシュ系ストレージ会社から、ハードウェア依存型バックアップやストレージ専用 OS によるバックアップにより OS に依存しないバックアップの提案があり、これらはテープよりも高速に利用可能であるメリットが示された。また、②ネットワーク系ベンダーからの提案で接続時間を書き込み時のみに制御し暗号化を免れる方法の提案があった。一方、③テープバックアップからは垂直磁場の利用で 5TB が 5 万円のテープが近い将来 500TB になり、一回書き込み（WriteOnce）の実現性が指摘された。これは上述の④ハッカーの潜入機関が 100 日以上への対応を可能にする方法であり期待できる。鳥取大学病院で 1 年間の電子カルテデータ SS-MIX2 で 1 TB であるが、地域医療ネットワークの公立病院では 5 年で 1 TB 未満であり、地域でのバッ

クアップサービスの利用の可能性も考えられた。日本医療情報学連合大会では①大阪府急性期医療センターのサプライチェーン経由型の攻撃を話題にしたが、企業と医療機関が基本的な情報公開とリスク分析を行っていなかったからと言った議論になり、具体的な対策を参加者に提示できなかった。しかし、日本遠隔医療学会春季学術大会では現場調査の CISCO を含めたネットワーク会社を中心に議論した。①攻撃後も前も NDR の必要性が明確になった。②システム導入時の管理者権限のわかりやすい ID, パスワードの利用が指摘された、筆者も③NIST が言うゼロトラストアーキテクチャーにおける端末と人の Authentication Authorization の後者、権限付与が日本では配慮が薄いと考えていた。つまり「閉じたネットワーク神話」もあり、これまで保守ベンダーは管理者権限のわかりやすい ID, パスワードを利用し、病院や関連ベンダーに簡単に情報共有してきた。このことはソフトのインストールなど対応が容易なこと、逆に言えば、ソフトの管理などあまり重視していなかったことと共通する。実際、サプライチェーン経由でハッカーが侵入しても管理者権限が容易に取得できなければ攻撃は難しいものであり今後この部分の教育、管理の徹底が必要である。

別途、放射線機器のオンライン保守中心に安価な携帯デジタル通信①LTE による専用回線接続の増加を聞いた。携帯電話の大きさで USB 接続できる機器が、ネットワーク機器、PC, 画像検査機器に直結して多くの保守がされている。また、②https サーバに接続する PC 等を用いて遠隔保守や遠隔画像診断をするサービスも増加している。DICOM 画像の取得、レポートの返信、検査機器のログ情報の取得などほとんどの通信が PC 経由でできる状況になっている。現状この医療機関内の PC の内容はブラックボックス化されている。外部接続する内部ネットワーク内の PC について病院は①通信内容の情報を知る必要があり、②モニタリング、監視するべき、あるいはモニタリング情報を知らされるべきである。また、③この PC が乗っ取られることを想定して DMZ など同 PC から病院内ネットワークに自由に通信できる環境におくべきではないと考えられる

複数病院のサイバーセキュリティ実態調査が最後になったが、現状の攻撃と対策技術の調査の後の現場の実態調査は順序として適切であったと考える。ベンダーが情報を公開し医療機関と共にリスク分析をして対応する新たな手法は始まったばかりで、理解されていない状況がわかり、具体的な病院管理者の対応の指導が必要であった。実際の医療機関の外部接続は数個の FW に集約された理想系から、部門システム、検査機器毎の保守回線が多数存在する病院が多かった。一度にまとめて導入されることのない中小病院では専門の技術者もおらず、全体のリスク想定と対策は難しいと考えられた。特に放射線機器の保守回線を LTE で導入する場合、無線のため病院のネットワーク管理者と協議する必要もなく接続できるので情報部門が放射線部門や検査部門の機器の保守契約に関与する体制が必須になっている。

（3）研究の実施経過

医療システムのクラウド移行については鳥取大学病院、福井大学病院の情報収集を行い、診療所電子カルテ、医療 D X に関係するモバイルヘルス系システムは遠隔医療学会、医療情報部長会からの情報収集から得た。一方、クラウドサービスにおけるセキュリティ、医療関係者等の意見を聞く場として分担者である山本隆一氏に「医療情報システムの安全管理ガイドライン」の解説を加えて、2021 年 6 月の医療情報学会、2021 年 10 月の遠隔医療学会、2021 年 11 月の医療情報学連合大会、2022 年 2 月の遠隔医療学会スプリングカンファレンスでシンポジウムを企画した。ここではセキュリティベンダー、クラウド事業者、CSIRT 事業者、IPA, 医療機器工業会にも発表頂きそれぞれの情報収集と同時に視聴者の医療関係者の意見を聞いた。CSIRT 委託事業者、I P A からの CSIRT の事前情報収集としての医療機関内のネットワークと外部接続の把握に関して、代表近藤はデータ調査会社のオンラインデータ取得における事業者の「匿名保存する」の説明に対して名寄せ可能性から「匿名化されていない」接続をしていることを指摘した。また、別途、「遠隔画

像診断サービス」においても「匿名化保存」の説明の下で画像サーバにオンライン接続している実態を発見した。研究班内で検討し危険な接続の可能性として扱うこととした。また、美代、星本は画像検査機器等の保守契約においてコロナ禍でオンライン保守に移行され、詳細が情報担当部門に連絡されない実態を報告した。類似の情報は医療情報部長会でも愛媛大学の木村教授からも指摘があり、契約において責任取らない旨の内容を見つけ報告した。6 月の東大阪病院、徳島県半田病院の事例もあり、データの安全な保存技術について、昔の磁気テープ保存の見直し、販売の増加情報を得たが、直接ストレージ機器ベンダー、ネットワーク機器ベンダーに聴取しハードウェアに暗号化されない、消されないバックアップ機器の開発がされている情報を得た。また、ＮＨＫ からのインタビューは情報機器を知らない一般人への説明の困難さも明確になり医療系 ISAC 立ち上げ時に参加者への説明に問題になることがわかり、ICT の安全性は繋がっていること自体は危険であり、相対的に安全になる技術を推奨する立場であることの教育の重要性が明確になった。これを踏まえて、今年度のアンケート調査は「相対的に安全になる技術、推奨される技術」に関する知識を問うことにすることを研究班内で協議した。最新の「医療情報システムの安全管理ガイドライン」にも仮想ブラウザなど技術の名称が記載されるようになった。シンポジウム開催による専門家からの情報収集と参加者への情報提供では、2021 年に増加し、電子カルテ、病院の機能停止の大問題から脆弱性をつくサイバー攻撃対策として CSIRT 活動を実際に行なっている IPA の担当者の話を日本医療情報学会春季学術大会で企画した。また、日本遠隔医療学会総会では診療データのバックアップに焦点を当てた。2022 年 11 月の日本医療情報学連合大会、2023 年の日本遠隔医療学会スプリングカンファレンスでは 2022 年に発生したサプライチェーン経由の攻撃に焦点を当て、ネットワーク会社 2 社に講演をして頂いた。また、別途、現場から聴取した情報を元に ISDN のサービス終了に変わる安価で簡単な携帯デジタル通信を用いた LTE 専用回線利用の保守契約の増加を確認した。

また、遠隔画像診断サービスについて https 接続を使った DICOM 画像と診断レポートの通信のセキュリティも積極的調査対象にした。どちらも放射線機器、放射線遠隔画像診断に関係するため、日本医療画像システム工業会 JIRA の DICOM 委員会、日本医学放射線学会の電子情報・AI 委員会の遠隔画像診断ガイドライン更新の小委員会の委員として現場で情報収集した。また、現場の状況を取得するため放射線技師学会での招待講演時にシンポジウムに参加し、ベンダーと放射線技師の考えを聞いた。

複数病院のサイバーセキュリティ実態調査では、病院会から紹介された病院を中心に１１病院を選択し調査した。経営者、システム管理者、利用者のチェエクリストのチェックから始めた。１１病院のデータを並べ、〇の多い項目、少ない項目について項目内容と病院の状況を想定して検討した。経営者では、予算化や組織の作成などは多くの医療機関で〇がつくが、具体的な体制、管理規則は個人情報保護対応ほどはされていない状況が見える。また、具体的方法の明示のない監査の実施、現状調査は丸が少ない。ただ、セキュリティ対策の公表はリスクもあり意見の別れるところであり、何らかの提案が必要と思われた。システム管理者では、これまでの個人情報保護法に基づいた医療情報システムの安全管理ガイドラインの内容についてはほとんど〇の状況だが、監査の実施については詳細の提案がないためやや数字は落ちる、契約内容についても担当部署でない可能性もあり数字が低くなる。医療情報システム系でもベンダーへの規則の改定部分の MDS の医療側対応はまだ普及しておらず、医療側の具体的対応も指導が必要と感じる。IoT 関係も同様でベンダー側の規則が成立したのが昨年度であり、医療者側の対応の具体的指導は今後のことであり、これから整備される ISAC も成績は悪い。外部への Web サービスがほとんどされていない日本の医療機関では答えられないものも多い。利用者では、個人情報保護のガイドラインに従って教育されている結果で〇が大半だいが、医療機関で導入されているシステムに依存した部分は X も存在する。

外部通信を含んだネットワーク全体図、

情報系機器の資産台帳の作成は日々の脆弱性対策にも、攻撃発生時の CSIRT 活動に必須のことであり、各病院が個別に作成し、更新すべきものである。しかし、業者任せで全体を把握していない病院にとっては手立てもわからず、その作成に協力することは重要である。また、本研究において作成のノウハウを作ることも重視した。そのため、2022 年度の調査を実施したセコム山陰に協力して頂き、新たな調査ベンダーにはセコム山陰の指導のものとに調査することにした。また、情報担当で管理されていない外部接続を探す、一定期間内に機器の事実を調査することは、定番の方法が無く、コスト計算も大小なることが予想されたので、厳密に人数と時間の記録をとり、人員の単価はベンダーに依存することで調査を実施した。情報管理の契約については、病院と遠隔医療協会、遠隔医療協会と各ベンダーで契約した。各病院の情報は、研究代表、分担者とセコム山陰で共有した。
作成された外部接続を含むネットワークの全体像、と資産台帳からは、7 つの外部接続に集約した病院から、最大 47 の外部接続を有する病院まで存在した。サブシステムや検査機器の保守に https サーバに接続する SSL-VPN 接続が見られた。放射線機器の保守系で LTE 回線も見られた。また、サービス終了が近い ISDN 接続も残っていた。放射線機器の保守回線が見られない医療機関が一つあり、放射線機器の保守回線が忘れられている可能性があった。

2. 病院調査の管理方式
（担当　研究分担者　長谷川高志）
　各病院の調査は、サイバーセキュリティに関する技術を有するシステム技術系企業６社に委託した。その調査結果を研究代表者、研究分担者が統括する視点から整理、分析した。５社で１１病院の調査を実施するにあたり、各社・各施設が公平かつ共通・一定に作業するべく、各社との情報保護や業務方式のルールや手続や文書類を共通化した。各施設とも依頼書、作業手順書、情報保護の誓約書等を共通の書式や方式で実施した。また調査内容の技術レベルを均質にするために、調査会社中の一社で令和４年２～３月に一施設でパイロット調査を担当した企業が、技術および工程の共通管理やレビューを担当した。これにより、具体的な調査事項のブレの抑制が抑制された。この管理方式は、本研究のみならず、今後サイバーセキュリティに関する施設調査を実施する際の“調査結果の質の安定化”に資する手法となった。なお調査対象施設は研究班による個別選別と、一般社団法人日本病院会での募集の二系統から選んだ。この募集および令和４年度研究での調査活動について、一般社団法人日本病院会からの支援は大変有益だった。

3. サイバーセキュリティに関する意識調査
（担当　研究分担者　長谷川高志）
（1）目的
　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アンケート調査する。単なる意識調査ではなく、回答者の知識水準などを具体的に抽出する設問を作った。日本病院会の会員施設を対象として、各施設の現実の状況を捉えた。プレ調査として、令和 3 年度に日本遠隔医療学会会員にパイロット調査を行った。
（2）結果概要
　詳細を把握するために、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存在を感じされた。令和 4 年度に本格的に実施した。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。
実施経過：アンケート用紙は昨年度研究と同じ書式を用いた。一般社団法人日本病院会殿に協力いただき、会員施設にインターネット経由で 9 月 21 日～11 月 7 日にアン

ケートを実施した。結果はNTTデータ経営研究所に一次分析を依頼した。
研究成果の刊行に関する一覧表：　特になし
（3）成果の今後の展開
日本病院会殿を通して、各施設に結果を知らせる。この結果から、対策技術の方向性を整理すべきことを様々な場に提唱する。

4. 医療情報システムの安全管理ガイドラインの調査・精査および患者を対象としたオンライン診療の現状把握や調査
（担当　研究分担者　山本隆一）：
（1）目的
医療分野における喫緊の課題であるサイバーセキュリティ対策と課題について、迅速かつ効果的な解決の方策を検討、提言を行う。
（2）結果の概要
昨年度に引き続き、山本本人が改定作業班の主査として主導し、取り纏めを行った「医療情報システムの安全管理ガイドライン 5.2 版」に対する医療機関やシステムベンダーからの質疑、意見等から社会の反応とその対応を検討し、今後のガイドラインからのアプローチの現状と可能性、今後の方策について調査を行った。また、随時、関係各位からの聴取を行ない、方策を検討して、新たに発出予定である第 6.0 版への提言を行った。また、患者を対象としたオンライン診療の現状把握や調査を行い、前年度結果との比較分析をし、研究期間中の状況の変化の把握、患者の意識の変化や、社会情勢の影響の有無など検討を行った。
（3）実施経過
改定作業班の主査として改定を主導した「医療情報システムの安全管理ガイドライン 5.2 版」に対しての社会の反応や対応を検討し、今後のガイドラインからのアプローチの現状と可能性、今後の方策について調査を行い、新たに発出予定である第6.0版への提言を行った。また、患者を対象としたオンライン診療の現状把握や調査を行い、前年度結果との比較分析をし、研究期間中の状況の変化の把握、患者の意識の変化や、社会情勢の影響の有無など検討を行った。
（4）研究により得られた成果の今後の活用・提供
今後も適宜見直し改定が予定されている「厚労省医療情報システムの安全管理に関するガイドライン」に関して、今後検討を行うにあたり重要なポイントを複数掲げられたこと、並びに「オンライン診療の適切な実施のためのガイドライン」に関しても、アンケート調査により受診した患者側の状況や意見など今後の改定等の参考となりえる提言が出来た。

5. 医療機器等に関連した調査と対策および医療機関のセキュリティ対応状況と教育等の対策の整理
（担当　研究分担者　美代賢吾、星本弘之、辻岡和孝）
（1）目的
医療機関、とくに中小規模の民間医療機関などにおいては情報システムや情報セキュリティの担当者が適切に設置されておらず、システム管理やセキュリティ対応において様々な問題を抱えている。さらに、近年多発している医療機関に対するサイバー攻撃に適切に対応を行うには、医療機関の情報システムを適切に管理運用する体制の整備に加え、一般の職員などのITおよびセキュリティリテラシーの向上が必要と考えられる。以上から、本分担研究としては、一般職員等に対するセキュリティ訓練プラットフォームの検討とリファレンスシステムの開発を行うことを目的として研究を実施した。
（2）結果概要
医療機関におけるサイバーセキュリティ対策調査として、日本国内4000の病院（精神科を含む）に調査票を送付し、用意したWeb上の回答フォームに508の医療機関から回答があった（回答率12.7%）。その結果、IoT 機器の利用が進む状況の中、現在IMDRF 文書に記載されるサイバーセキュリティリスクへの対応については、多くの医療機関が十分に対応できていないことが明らかになった。今後の対応として、IoT機器に対するサイバー攻撃のリスク評価と対応基準の検討、IMDRF文書のセキュリティ要件に対応するための医療機関を支援する組織の必要性、日々進化するサイバー攻撃に対応し、的確な教育を行う仕組みの組織的な提供により、日本の医療機関全体のサ

イバー攻撃への対処能力の向上につなげる必要性が示唆された。

令和 3 年度に開発検証したプロトタイプシステムを元に、実運用が可能な迷惑メール対応訓練システムを開発した。本システムにより、一般的な迷惑メール（マルウェア添付、URL 記載）に類似した訓練メールの発信とそのメールの開封・URL アクセス・添付ファイル参照などに関する受信者の行動把握が可能となり、適切なセキュリティ対応に関する訓練を実施するシステムの実現が可能となった。今後は、このシステムを用いたセキュリティ訓練サービスの提供などについて検討を行っていく予定であるが、それと合わせて中小医療機関を適切に支援する体制の整備が必要である。

4．健康被害情報

なし

5．謝辞

本研究にあたり、一般社団法人日本病院会殿および会員施設の皆様、調査にご協力いただいた全ての病院、関係者の皆様にたいへんお世話になりました。ここに深く感謝を述べさせていただきます。

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

病院サイバーセキュリティ調査の管理方式

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
各施設サイバーセキュリティ調査では、調査項目・調査水準・秘密保持や質管理などのために、文書や手順の共通化、監督企業の設置など、管理方式を構築した。　構築に時間を要したが、構築後は調査が効率的かつ均質に進み、短期間に調査作業が進んだ。

A．研究目的

病院のサイバーセキュリティ調査は、調査内容と別に対象先病院の募集と選定、調査実施に至るまでの調整業務があった。また調査担当各社の実施項目の準備、実施時の監督や調査の質のすりあわせ等、様々な運営の努力を集結して、管理方式を構築した。

管理方式には以下の質保証や手順の効率化の利点がある。

1，同時に複数の病院･企業で共通の手順で作業を進め、業務の質を安定できる。
2，各施設･各社同じ手順を進めるので、組織内部の説明や意思決定が円滑になる。
3，秘密保持等の誓約が均質に管理できる。
4，調査の質を安定できる。

B．研究方法

1．手順、秘密保持契約、工数管理などのドキュメントを共通化した。
2．担当組織を一本化した。

C．研究結果

1．共通ドキュメント
① 病院向け調査手順
② 日本遠隔医療協会から病院への依頼状
③ 病院・協会間秘密保持誓約書
④ 調査担当企業向け調査手順
⑤ 調査担当企業・協会間秘密保持契約
⑥ 調査工数確認票
【資料1～6】

2．手順
① 企業募集
② 企業・研究班会議
③ 企業向け書式（資料①～⑥）提供
④ 病院募集
⑤ 応募病院への依頼（意向確認）
⑥ 誓約等手続
⑦ （各社調査）
⑧ 各社に途中の工数確認およびドキュメントチェック

3．監督企業の設置

セコム山陰株式会社を監督企業とした。監督企業と調査各社はシステム開発の工程管理システムで工程、ドキュメントの提出等を管理した。また調査内容の確認を随時行った。

3．考察

（1）業務の質と効率

手順構築の時間を要したが、調査開始以降は効率的に作業が進んだ。そのため調査が2023年1月～3月に集中したが、調査は短期間で終了し、複数調査が同時並行して進行した。

（2）調査内容のレベル統一

サイバーセキュリティは、皆の意識がバラバラだが、調査手順書の作成･配布および監督企業の業務により、調査レベルの平準化が進んだ。

（3）総論として

ネットワーク接続図などの重要情報を調査対象とした。各社で秘匿レベルの意識差があり、当初、曖昧な情報に留めたケースと詳細なケースが混在した。しかし曖昧な情報では、問題点を絞れないので、監督企業として詳細調査を指導できた。

サイバーセキュリティは、まだしばらく、意識差が大きいと考えられるが、質をコン

トロールした調査が可能であることを実証
した。

D．健康危険情報
なし

厚生労働行政推進調査事業

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

【資料１　病院向け説明書】

病院に対するサイバーセキュリティに関する調査・報告書作成業務

各病院調査等手順

特定非営利活動法人日本遠隔医療協会

第 1.1 版　2022 年 11 月 21 日

【調査の基本構想】

日本国内の複数の医療機関で、サイバー犯罪者による破壊行為の被害（ランサムウェアの攻撃）が多発している。被害（アクシデント）に至らずとも、インシデントも多数発生していると考えられる。その対策が急務であるが、サイバー犯罪自体が急速に進化していること、元々の日本の医療機関の情報化の弱さや要員不足から、この事態への対応が進んでいない。そこで厚生労働省の調査研究（厚生労働行政推進調査事業）により、医療機関のサイバーセキュリティに関する調査を進めている。

本研究班は、日本の医療分野のサイバーセキュリティの専門家を結集して（参考資料　研究班体制）、複数の病院に訪問調査を実施している。

セキュリティインシデント発生時の対応として CSIRT の組織化が医療機関に求められているが、CSIRT の対応ができる人材は日本では限られている現状がある。CSIRT の対応には米国の NIST の SP－800 が参考にされており、日本では IPA, JPSIRT での議論資料があり、これらをフォローしている必要がある。しかし、日本の電子カルテベンダー等医療情報システム関連の大企業の医療部隊で、これらをフォローされていたとは言えない状況である。一方、攻撃は組織化しており迅速な対応が要求されているにも関わらず、これを医療機関側に求めることはかなり厳しい状況と言える。全国的に委託業者の育成が必要と判断する。

具体的には CSIRT の対応は 3 つのステップからなる。

① 事前にネットワーク全体像、外部接続全体像、内部の通信全体像の把握が各医療機関に求められる。

② この資料に応じて脆弱性が明確になった場合に迅速に対応することが必要である。

③ 何らかの異常を察知した場合に対応する。

このうち、**①事前調査**について、日本の医療機関ではシステムの構築に多数のベンダーがネットワークとサーバ、端末を導入し接続しており、全体像が掴み難い現状がある。これは電子カルテベンダーが全体を入札していても部門については部門システムに任せていることが多く、全体像は十分把握されているとは言えない。ネットワークとサーバ等のハードウェアを一括管理し、その上に幾つかのソフトウェアを載せる方法が管理上理想であり、その方向を進める必要はあるが、現状では全体把握は難しい状況である。2022 年 3 月に行った先行調査（A 病院調査）でも調査結果に現れたが、コロナ禍で現地保守がいつの間にか、オンライン保守になり、外部接続がされている状況もあり、病院は病院資産でない機器（ベンダー資産の保守用機器）の管理状況を把握する必要がある。CT など検査機器は院内の管理も情報担当ではなく、遠隔読影、地域連携なども存在する。中小病院ではこれらの把握に人材もおらず、専門業者に委託する必要がある。**②脆弱性への対応**のステップは既にネットワーク管理事業者等では各施設の機器のリストを保持し、脆弱性が発表されるとシステム上で対応すべき医療機関等を検索し、担当部署に連絡する体制を作っている事例がある。中小病院ではこれらの部分も委託が望ましいと言える。**③異常検知時の対応**のステップは、事前調査がされていると容易であり、これらの委託事業者の負荷も抑えられる。

人材豊富な大病院では**①事前調査**、**②脆弱性への対応**のステップは可能かもしれないが、情報管理の人材の少ない中小病院では難しい。

本調査は、**①事前調査**に関する、調査手法開発の試みである。2022 年 3 月に一施設で先行調査を行い、様々な事柄がわかった。しかしながら、本研究班とコミュニケーションがある施設や企業で行ったもので、その調査結果が多くの施設に共通的普遍的と言えるか、調査手法をそのまま多くの施設に適用できるか、不明である。そこで 2022 年度に全国各地の複数の施設でトライアルを行うこととした。

1．　本文書について

本文書は調査に協力いただく病院向けの説明および手続の解説であり、以下事項が記載されている。

① 調査協力施設の役割、負担
② 調査事項と手順
③ 手続および工程（スケジュール観）
④ 書式類

2．　調査協力施設の役割、負担

① 責務

- 調査担当会社よりの要請に基づく、調査協力施設の関係者（病院長、職員、システム担当者）へのヒヤリングの日程調整
- 調査担当会社よりの要請に基づく、調査協力施設内の設備の調査（同行、案内）
- 調査担当会社よりの要請に基づく、調査協力施設内の設備業者との情報提供に関する仲介
- 調査担当会社よりの質問への対応

② 調査目的

まだ日本国内の病院のサイバーセキュリティの状況に関する実態情報が無く、日本国内の多くの病院がどのような状況にあり、国家レベルの対策として何を打ち出すべきか、厚生労働省に伝え政策立案の情報収集が本調査研究の目的である。

調査結果の詳細情報を秘密保持すべき厚生労働省に報告する。また統計的処理等を経て、対象施設との関係を全くたどれない情報を学術的に公開（論文投稿、学会等の講演、図書出版）することがある。

調査により、施設内のサイバーセキュリティ上の不足や不備が見いだされるかもしれないが、その責任追及や処罰のための報告などは研究目的ではない。不備や不足な状況も、受け止めるべき現実として明らかにしてゆく。調査結果を整理した段階で指摘できる問題点や対策について、報告書に記す。

③ 調査に関する秘密保持

調査担当企業は厚生労働行政推進調査事業研究班の受託機関（事務局）の特定非営利活動法人日本遠隔医療協会との契約に基づき、担当する。各企業は、調査対象病院に対して日本遠隔医療協会が誓約する秘密情報保持の諸条項を遵守して調査する。

④ 調査に関する負担

調査に係わる対象施設職員への謝金（日本遠隔医療協会規定に基づく）、調査に於いて対象施設が支払う必要がある費用を、日本遠隔医療協会は対象施設に支払う。支払については、日本遠隔医療協会研究事務局が調整する。

3．　調査事項と手順

3.1　概要

今回の調査は**①事前調査**のステップとして、病院担当者あるいは調査各社が効率的に実施できる手

法の開発を狙っている。ただし開発途上の手法なので、不明点や過不足は、調査途上で適宜修正しながら進める。

3.2　チェックリストによるヒヤリング

① 医療情報システムの安全管理のガイドラインにあるチェックリスト（経営層向け、システム管理者向け、利用者向け）を訪問調査で聞き取り、作成する。

② チェックリストは下記 URL よりダウンロードできる。

「医療機関のサイバーセキュリティ対策チェックリスト」　Excel 版
（経営層向け、システム管理者向け、利用者向けがこの Book 内に含まれる）
https://www.mhlw.go.jp/content/10808000/000936169.xlsx
https://www.mhlw.go.jp/content/10808000/000936167.pdf　（PDF 版）

③ 病院長、システム管理者、利用者（1、2 名）の 3−4 人に、訪問調査前に予め上記チェックリストをダウンロードいただき、内容を確認いただき、第一回訪問に備えていただきたい。そこで結果を調査員と付き合わせる。

- 分からないことは、何が分からないか、記載して頂き、○×を記載して頂く。
- 理解が困難であった部分は記録し、今後の検討材料にする。ヒヤリングは一人 30 分ほどで終える。**（病院長、利用者で最大で 1.5 時間×2）**

④ システム管理者にも同様に対面での調査を行う。**2 時間以上、半日程度の調査にする。**資料が病院にあってすぐに出ない場合は、その場では宿題として、一週間の期間に提出を求める。提出されなかった場合、出されなかったとして記録する。（提出が必須ではなく、1 週間掛けても提出できないことも、実態の情報となる）資料が保守業者にある場合には業者の担当者、連絡先を聞き、病院の了解の下、直接ベンダーに聞く。ベンダーに聞く場合も、1 週間以内に情報が出されない場合には、出せなかったとして記録する。

- 分からないことの説明、帳票など具体的なものがあるのかなど、詳細を質問し完成させる。
- この調査は第一回訪問だけでは終わらない。二回目訪問などが必要である。

3.3　院内設備の巡回調査

① 外部接続、サーバ、ネットワーク機器等は調査会社、システム管理者、病院からの委託事業者が直接院内巡回して機種等を確認する。

- システム管理者と委託事業者担当者の技術的な詳細確認は 1 時間を 2 回ほど必要

② 必要な場合、調査施設の了解の下、ベンダーに問合せていただく。

③ 外部接続の状況調査（管理者の知らない接続なども洗い出す）の対象は以下の通り。

[1] 各システム
[2] ネットワーク保守
[3] ＣＴ、ＭＲＩ等ネットワーク接続検査等の機器の保守
[4] マイナカード関係接続
[5] 地域医療連携接続
[6] 遠隔読影サービス接続
[7] 研究ネットワーク接続
[8] 各種遠隔サービス接続など

3.4　追加ヒヤリング等

① 本調査開始後も、サイバー犯罪状況は刻々と変化している。調査項目や内容を追加する場合がある。

② 脆弱な機器からの侵入だけでなく、サプライチェーン経由の侵入が発生しており、それに関する質問などを検討中である。まとまり次第、各社に連絡する。

3.5　作成する図面、表、図書

以下のドキュメントを作成、提出いただく。

① チェックリストによる調査結果（経営層向け）
② チェックリストによる調査結果（システム管理者向け）
③ チェックリストによる調査結果（利用者向け）
④ 病院情報システムのバックアップ状況（表）
⑤ 外部接続先一覧　および　外部接続先調査履歴
⑥ ネットワーク概要図
⑦ 情報システム管理体制図

3.6　調査対象病院への報告

① 現状の詳細資料（前項①～⑦）を提出し、脆弱性、管理上の必要性など指摘する。

② 既存のファイアウォール,VPN の脆弱性が公開された時に、自院に同様の状況がないか判断するためにも、事前に作成すべき資料である。

③ サーバーセキュリティ対策、事故発生時に 各病院が保持し、更新していくことが重要である。

④ ここで作成された資料は、脆弱性が公開された場合に自院に同様の脆弱性がないか確認し、脆弱性がある場合の対応を可能にする。脆弱性情報は日本国内では IPA、JPSIRT 等で公開されるので、今後その部分の委託が可能になると期待する。

⑤ これら資料（詳細情報）は、厚生労働省担当室（特定医薬品開発支援・医療情報担当参事官室）に提出する。ただし、厚生労働省からの公開（政策検討の会議資料、各種規則や指針）および当研究班での公開（学会等への報告）では、個別施設名を示す事や特定のセキュリティ上の弱点を晒すこと（サイバー犯罪者に資する情報の公開）はせず、統計的情報などに限定する。調査担当各社も日本遠隔医療協会との秘密保持協定で、本項の遵守が義務づけられる。

4．調査手順

① 日本遠隔医療協会からの意向確認
- 調査に協力いただけるか、研究班事務局（日本遠隔医療協会）が確認する。
- 日本遠隔医療協会から秘密保持に関する誓約書を提出する。
- 確認次第、調査担当社が引き継ぐ。

② 意向確認後、一ヶ月以内
- 調査担当社から連絡
- 訪問調査日程等の調整

③ 調査

- チェックリストヒヤリング　1～2 回（一回半日程度）
- 施設内巡回調査　　1～2 回訪問（一回半日程度）

④ 調査報告提出

- 調査後一ヶ月以降、2023 年 5 月末日までにお送りする。

5．誓約書

① 調査対象施設（病院）と研究班（日本遠隔医療協会）で情報に関する取決を行う。

② 情報管理に関する誓約書を日本遠隔医療協会から各施設に提出する。

③ 研究班と調査各社は誓約書に沿った秘密保持契約を締結してから、調査に入る。

【資料２　病院向け依頼状】

令和５年１月＊日

貴院名
院長先生名　御侍史

厚生労働行政推進調査事業
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
研究代表者　近藤博史

サイバーセキュリティに関する病院調査への協力のお願い

日頃より厚生労働行政推進調査事業でお世話になっております。一般社団法人日本病院会様より、サイバーセキュリティに関するご意向調査を行いましたところ、貴院よりご協力をお申し出いただき、深く感謝申し上げます。研究班で検討の結果、貴院にて調査を進めたく、ご依頼いたします。以下は日本病院会殿よりの意向調査の説明の繰り返しですが、趣旨と今後の手順をお示しいたします。

1. 背景と目的

ランサムウェア等の被害で、複数の病院が狙われ、医療情報システムを破壊され、診療に支障を来す事態が発生しております。厚生労働省では、その対策を立案すべく、厚生労働行政推進調査事業で複数の病院について、サイバーセキュリティの現状に関する調査を進めております。

サイバーセキュリティに関する各病院の技術水準を高めることや、人材を揃えることはたいへん困難です。一方でサイバーセキュリティ上のリスクは高く、今後さらに高まります。今後の政策立案に活かすため、日本病院会様の会員施設から選ばれた約 10 施設で詳細に調べ、リスクと管理状況を明らかにすることが調査目的です。そこで各施設の医療情報システムの管理状況を後述の手法で調査します。ご協力いただいた施設には、サイバーセキュリティ上の防衛に欠かせない情報設備の管理状況データ（資産管理台帳に相当）をご報告します。今後、このような資産管理台帳は各施設で導入が進むので、パイロットスタディとして、いち早くセキュリティ対策に着手でき、台帳も少ない負担で入手できます。そのような背景をご理解の上で、ご協力いただけますよう、よろしくお願い申し上げます。

2. 調査手法

(1) 厚生労働省の「医療情報システムの安全管理ガイドライン 5.2 版」に基づく調査
以下がホームページの URL です。　参考となる情報が多々掲載されています。このような調査は、今後各施設で必要となります。いち早く手法を習得できる機会となります。

https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html
ガイドライン本体は以下の URL です。
https://www.mhlw.go.jp/content/10808000/000936160.pdf

調査に用いるチェックリストの URL は以下です。
（Excel 版）　https://www.mhlw.go.jp/content/10808000/000936169.xlsx

（PDF 版）　https://www.mhlw.go.jp/content/10808000/000936167.pdf

参考資料として、以下が医療情報システム等の障害発生時の対応フローチャートです。
（Excel 版）　https://www.mhlw.go.jp/content/10808000/000936170.xlsx
（PDF 版）　https://www.mhlw.go.jp/content/10808000/000936168.pdf

調査員（研究班が委託する企業社員）が訪問して、病院長様、システム管理者様、利用者様（職員１、２名）の 3～4 人にヒヤリングいたします。上記チェックリストを用いて、チェックしていただきます。分からないことは、何が分からないか、記載して頂き、○×を記載して頂きます。　所要時間は各 15 分ほどです。

(2) 貴院の情報システムに関する委託事業者に 1 時間程度の面談調査
調査員が訪問して、帳票など具体的な管理文書の有無など、詳細を質問して情報を整理します。

(3) 貴院システム管理者様および貴院委託事業者担当者様の技術的な詳細確認
1 時間ほどの調査を 2 回ほど行い、以下の情報をまとめます。

① 外部接続の状況調査（管理者の知らない接続なども洗い出します。）
- 各システム、ネットワーク保守
- ＣＴ、ＭＲＩ等ネットワーク接続検査等の機器の保守
- マイナカード関係接続
- 地域医療連携接続
- 遠隔読影サービス接続
- 研究ネットワーク接続
- 各種遠隔サービス接続など

② 内部の全体ネットワーク図
- システム名称、DB の名称とサーバと端末、バックアップ等の配置など
- 場合により、病院様の了解の下、委託事業者からベンダーに調査いたします。

③ システム管理台帳

④ 院内各システムのデータバックアップ状況

⑤ 管理体制図

(4) 個人情報について
職員や患者の個人情報は収集しません。

3. 調査結果について
(1) 複数施設を調査するので、それらをまとめて厚生省の政策立案もしくは、学術的な場での公表（論

文、書籍、学会発表）に用います。個別の施設に関する情報やシステム上の詳しい情報を外部に公開することはありません。これについて、後日　日本遠隔医療協会より情報保護に関する誓約書を提出いたします。

(2) ご協力いただいた施設には、調査結果（詳細報告資料）を提出し、管理上の課題など指摘します。

- これまでに攻撃を受けた施設事例のように既存のファイアウォールや VPN の脆弱性が公開された時に、自院に同様の状況がないか判断するためにも、事前に作成すべき資料です。
- ここで作成された資料は、脆弱性が公開された場合に自院に同様の脆弱性がないか、確認し、あった場合の対応することを可能にします。脆弱性の公開については日本国内では独立行政法人情報処理推進機構(IPA), Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) 等に発表されます。今後その部分は委託することも可能になると思います。
- これらの資料は、サーバーセキュリティ対策、事故発生時に 各病院が保持し、更新していくことが重要です。

5. 調査の進め方

今後の調査の窓口を、貴院よりのご協力申出で記されました、以下のご担当者様にお願いしたく存じます。

＜部署名＞　＜役職名＞　＜お名前＞ 様

6. 謝礼について

ヒヤリング等に要した時間ついて、本研究班の規定により謝金をお支払いいたします。また各施設から委託している会社等への調査費用が発生する場合、ご相談の上、お支払いいたします。

7. お問い合わせについて

調査の詳細なご連絡は調査員（研究班が委託する企業社員）が務めます。それ以外の事柄について、下記の研究事務局がご連絡や調整を担当いたします。

特定非営利活動法人日本遠隔医療協会
厚生労働行政推進調査事業、研究運営担当（研究分担者　長谷川高志）
telemedicine-research@j-telemed-s.jp

日本遠隔医療協会事務局
〒370-0033　群馬県高崎市中大類町 37-1
高崎健康福祉大学健康福祉学部 医療情報学科内
http://http://j-telemed-s.jp/

以上

【資料３　病院向け誓約書】

【調査対象施設・日本遠隔医療協会間の秘密保持誓約書（ひな形)】

＊＊病院　殿

この度、特定非営利活動法人日本遠隔医療協会(以下、協会)は、＊＊病院殿(以下、貴院)の第1条に定める本件業務を遂行するにあたり、情報の取扱いに関し以下のとおり誓約する。

第1条(本件業務)

1 本誓約は、貴院のサイバーセキュリティに関する調査に際し、調査で収集する情報について、その秘密保持に関する取扱いを定めることを目的とする。

2 調査により収集する情報は、調査研究の委託者である厚生労働省に、秘密情報(非公開対象)として提出する。

3 調査により収集する情報について、統計的処理等を施して、貴院との関係性を消失したものを、学術的に公開(論文、講演、書籍執筆)することは本件業務の一部に含まれる。

第2条(秘密情報)

1 本誓約において秘密情報とは、文書、口頭、物品および電子媒体等形態を問わず、本件業務の実施に伴い収集する情報のうち、次の各号に定める情報をいう。

　1 秘密である旨が明記された文書、図面、写真またはその他有体物(電子的手段による場合を含む。)として開示された情報。

　2 貴院の施設運営に関する情報で、調査の際に収集された聞き取り結果、文書、図面、写真またはその他有体物(電子的手段による場合を含む。)。

2 前項の規定にかかわらず、次の各号に該当することを協会が証明し得るものは秘密情報には含まれないものとする。

　① 貴院より開示を受ける前に、既に所有または取得していたもの

　② 貴院より開示を受ける前に、既に公知公用となっているもの

　③ 貴院より開示を受けた後に、協会が本契約の規定に違反することなく公知公用となったもの

　④ 開示の権限を有する第三者から、秘密保持の義務を負うことなく、適法に知得したもの

第3条(秘密保持)

1 協会は、貴院の事前の書面(電磁的措置を含。)による承諾なしに、秘密情報を本件業務以外の目的のためには一切使用しない。

2 協会は、本件業務の遂行上知る必要のある自己の従業者および本件業務の一部を委託する他団体の従業者(以下「関係者」という)に対してのみ、秘密情報を開示および共有することとし、合理的かつ善良と認められる注意をもって管理するものとする。

3 協会は、秘密情報を関係者および本件業務で定義した開示先以外の第三者に開示しない。

第4条(秘密情報の管理)

協会は、本件業務を遂行するために合理的に必要な範囲内で、秘密情報を複写および複製することができるものとし、その範囲を超えて複写・複製してはならない。また、秘密情報の複写物および複製物も秘密情報とみなすものとする。

第5条(秘密情報の返還)

協会は、貴院の要請があり次第、速やかに秘密情報(複写物、複製物を含む)を返還し、返還が不可能な場合には、貴院の指示に従って、当該資料を消去または廃棄するものとする。

第6条（秘密情報の権利）

1　秘密情報に関する一切の権利は、貴院に帰属するものとする。また、当事者間で別途合意した場合を除き、秘密情報の開示は、協会に対していかなる権利も付与しないものとして解釈する。

第 7 条（損害賠償）

貴院は、協会が本誓約の規定に違反した場合、当該違反を是正するために必要な措置をとることを求めることができるとともに、当該違反によって被った損害の賠償を請求することができる。

第 8 条（有効期間）

本誓約の有効期間は、202＊年＊月＊日から2023年 3 月 31 日までとする。ただし、第3条、第4条および第5条、第6条、第 7 条はそれぞれの対象事項が存続する限り、本誓約の有効期間終了後も有効に存続する。

2022 年　　＊月　　＊日

群馬県高崎市新後閑町 4-2
特定非営利活動法人　日本遠隔医療協会
理事長　酒巻　哲夫　（押印）

【資料４　調査担当企業向け説明書】

調査担当企業向け資料

調査に当たる企業ご担当者向けの調査業務概説

1．　本文書について

本文書は調査に従事する企業向けの説明文書および手続の解説であり、以下の事項が列記されている。

① 調査企業の責務と役割
② 調査事項と手順
③ 調査事例
④ 手続および工程（スケジュール観）
⑤ 書式類

2．　調査企業の責務と役割

① 調査企業の条件

医療 ICT に関する事業実績が有り、病院内の情報システムに詳しい企業に調査を委託する。厚生労働省発行の医療情報システムの安全管理のためのガイドラインを読み込んでいれば、後述の手順の難度は高くない。調査対象施設でのシステム構築や運用に携わっている企業であれば、円滑な調査の遂行を期待できる。

② 調査企業への支援

研究代表者と協力して、A 病院の調査を担当し、調査手順を開発したセコム山陰株式会社が、手順実施の支援や質問対応、レポートの確認、情報共有支援、工数モニタリングなどの調査支援を担当する。その指導や支援に沿って調査されたい。

③ 調査目的

まだ日本国内の病院のサイバーセキュリティの状況に関する実態情報が無く、日本国内の多くの病院がどのような状況にあり、国家レベルの対策として何を打ち出すべきか、厚生労働省に伝え政策立案の情報収集が本調査研究の目的である。個別施設の課題解決は重要だが、大方針が立たないうちに個別課題に没入することは全ての病院に取り、好ましい状況ではない。そこで調査対象施設のサイバーセキュリティに関する能力向上、問題点の詳細調査や指導、監査は範囲外である。調査を担当する各社は、現状調査に徹していただきたい。

調査により、サイバーセキュリティ上の不足や不備が見いだされるかもしれないが、その責任追及や処罰のための報告なども研究目的ではない。不備や不足な状況も、受け止めるべき現実として明らかにしてゆく。監査や改正に要する研究予算も有していない。

後述の調査結果を整理した段階で指摘できる問題点や対策について、報告書に記す。

④ 調査に関する契約

調査各社との契約者は各病院でなく、厚生労働行政推進調査事業研究班の受託機関（事務局）の特定非営利活動法人日本遠隔医療協会である。各企業は日本遠隔医療協会との間で、見積・発注・秘密保持等の契約を結ぶ。秘密保持契約の対象には、調査各社と日本遠隔医療協会の知財だけでなく、調査対象病院から得た調査結果情報が含まれる。知財と言えない情報でも、調査各社で許可なく利用や公開することは認められない。

3．　調査事項と手順

3.1　概要

今回の調査は**①事前調査**のステップとして、病院担当者あるいは調査各社が効率的に実施できる手法の開発を狙っている。ただし開発途上の手法なので、不明点や過不足は、調査途上で適宜修正しながら進める。調査手順に関する不明点、過不足について、調査各社はセコム山陰株式会社に報告、相談しながら、調査を進められたい。

3.2　チェックリストによるヒヤリング

① 医療情報システムの安全管理のガイドラインにあるチェックリスト（経営層向け、システム管理者向け、利用者向け）を訪問調査で聞き取り、作成する。

② チェックリストは下記 URL よりダウンロードできる。

「医療機関のサイバーセキュリティ対策チェックリスト」　Excel 版
（経営層向け、システム管理者向け、利用者向けがこの Book 内に含まれる）
https://www.mhlw.go.jp/content/10808000/000936169.xlsx
https://www.mhlw.go.jp/content/10808000/000936167.pdf　（PDF 版）

③ 病院長、システム管理者、利用者（1、2 名）の 3−4 人に、訪問調査前に予め上記チェックリストをダウンロードいただき、内容を確認いただき、第一回訪問に備えていただきたい。そこで結果を調査員と付き合わせる。

- 分からないことは、何が分からないか、記載して頂き、○×を記載して頂く。
- 理解が困難であった部分は記録し、今後の検討材料にする。ヒヤリングは一人 30 分ほどで終える。**（病院長、利用者で最大で 1.5 時間×2）**

④ システム管理者にも同様に対面での調査を行う。**2 時間以上、半日程度の調査にする。**資料が病院にあってすぐに出ない場合は、その場では宿題として、一週間の期間に提出を求める。提出されなかった場合、出されなかったとして記録する。（提出が必須ではなく、1 週間掛けても提出できないことも、実態の情報となる）資料が保守業者にある場合には業者の担当者、連絡先を聞き、病院の了解の下、直接ベンダーに聞く。ベンダーに聞く場合も、1 週間以内に情報が出されない場合には、出せなかったとして記録する。

- 分からないことの説明、帳票など具体的なものがあるのかなど、詳細を質問し完成させる。
- この調査は第一回訪問だけでは終わらない。二回目訪問などが必要である。

3.3　院内設備の巡回調査

① 外部接続、サーバ、ネットワーク機器等は調査会社、システム管理者、病院からの委託事業者が直接院内巡回して機種等を確認する。

- システム管理者と委託事業者担当者の技術的な詳細確認は 1 時間を 2 回ほど必要

② 必要な場合、調査施設の了解の下、ベンダーに問合せていただく。

③ 外部接続の状況調査（管理者の知らない接続なども洗い出す）の対象は以下の通り。

[1] 各システム
[2] ネットワーク保守
[3] ＣＴ、ＭＲＩ等ネットワーク接続検査等の機器の保守
[4] マイナカード関係接続
[5] 地域医療連携接続

[6] 遠隔読影サービス接続
[7] 研究ネットワーク接続
[8] 各種遠隔サービス接続など

3.4 追加ヒヤリング等

① 本調査開始後も、サイバー犯罪状況は刻々と変化している。調査項目や内容を追加する場合がある。
② 脆弱な機器からの侵入だけでなく、サプライチェーン経由の侵入が発生しており、それに関する質問などを検討中である。まとまり次第、各社に連絡する。

3.5 作成する図面、表、図書

以下のドキュメントを作成、提出いただく。

① チェックリストによる調査結果（経営層向け）
② チェックリストによる調査結果（システム管理者向け）
③ チェックリストによる調査結果（利用者向け）
④ 病院情報システムのバックアップ状況（表）
⑤ 外部接続先一覧　および　外部接続先調査履歴
⑥ ネットワーク概要図
⑦ 情報システム管理体制図

3.6 調査対象病院への報告

① 現状の詳細資料（前項①～⑦）を提出し、必要に応じて、脆弱性、管理上の必要性など指摘する。
② 既存のファイアウォール,VPN の脆弱性が公開された時に、自院に同様の状況がないか判断するためにも、事前に作成すべき資料である。
③ サイバーセキュリティ対策、事故発生時に 各病院が保持し、更新していくことが重要である。
④ ここで作成された資料は、脆弱性が公開された場合に自院に同様の脆弱性がないか確認し、脆弱性がある場合の対応を可能にする。脆弱性情報は日本国内では IPA、JPCERT 等で公開されるので、今後その部分の委託が可能になると期待する。
⑤ これら資料（詳細情報）は、厚生労働省担当室（特定医薬品開発支援・医療情報担当参事官室）に提出する。ただし、厚生労働省からの公開（政策検討の会議資料、各種規則や指針）および当研究班での公開（学会等への報告）では、個別施設名を示す事や特定のセキュリティ上の弱点を晒すこと（サイバー犯罪者に資する情報の公開）はせず、統計的情報などに限定する。調査担当各社も日本遠隔医療協会との秘密保持協定で、本項の遵守が義務づけられる。
⑥ 病院への報告書は日本遠隔医療協会を通じて提出する。

4．調査の作業量の目安

① 2022 年 3 月に実施した A 病院で要した作業概要を以下に示す。
- 詳細工数内訳を参考資料 1 に示す。

② 総工数としては約 300 時間（参考資料 1　参照）

- A 病院は、研究代表者（近藤博史）と人間関係がある施設である。
- セコム山陰と同院技術担当者とコミュニケーションがとり易い状況だった
- 初めてコンタクトする病院の場合は、調整などで工数が増える可能性がある。
- 訪問人数　2 名又は 3 名で訪問。　1 名で訪問の場合、工数削減可能。

③ 工数変動要因

- 病床数、情報系担当の人的体制（スキル)、ベンダーに対する保守の委託内容など
- 移動に関わる交通費・工数、宿泊費が追加になる

④ 今後の打合せ

- 全体キックオフ
- 各社スタート時の小キックオフ（各社、セコム山陰、日本遠隔運動療法協会）を行う。

5．調査対象病院

① 日本病院会会員の候補施設

- 長谷川から、意向確認して、その後、担当社との手順に入っていただく。
- その病院に出入りのシステム会社を紹介してもらう施設がいくつかあるので、日本遠隔医療協会から会社にも連絡を入れて、「本当に調査を担当するか？」を確認する。

② おしどりネット内の対象候補病院（研究代表者から各施設に依頼する）

③ 各病院への訪問の連絡は、担当各社より実施する。

- その際に病院向け説明書（本書前部、別途独立版あり）を各社より渡して説明する。
- 訪問に関する諸業務は各社で調整の上で実施する。
- 後述の情報共有システムで、訪問日程などを報告する。
- 各病院と日本遠隔医療協会（研究事務局）での調整すべき事項は、必要時に研究事務局まで連絡する。

6．全工程のスケジュール観

このスケジュール観を目安とするが、遅れ気味なので早めるよう努力する。早く調査が進む施設は以下のスケジュールに囚われず、早々に報告書作成まで終える。

① ～11 月中旬

- ターゲット病院の決定
- 並行して作業内容、工数、費用などの算定

② ～11 月下旬

- 契約
- 日本遠隔医療協会から各調査会社への発注

③ 12 月初

- 訪問・メール・電話等での調査開始
- 途中調査会社～セコム山陰との間で調整、フォローを実施

④ ～1 月中旬　調査会社は途中経過をセコム山陰に報告し、レビューを受ける。
追加で必要な調査を実施頂く（深掘りして欲しい部分）

⑤ ～2 月上旬　調査会社～セコム山陰の間で報告書、ドキュメントの調整
この段階のとりまとめ前報告書も、研究班で参照し、まとめ方を改良する。

⑥　～2 月下旬　　調査会社から日本遠隔医療協会に報告書提出と検収

7．調査各社間の情報共有体制

セコム山陰により、各社・研究班間の効率的な情報共有システムを準備するので、各社もこれを用いてデータ共有や報告など行う。詳細説明および ID,パスワード等は別途、セコム山陰より連絡する。

8．契約関連事項

① 見積予算。

- 人件費で300万円を上限として､見積いただく｡出張回数見通しも見積に含めていただく。見積は概算でかまわない。実績時に調整する。

② セコム山陰による「調査会社に対する調査・報告書作成業務の支援、監修」

- 別途　研究班とセコム山陰で、調査各社への支援に際しての秘密保持契約を結ぶ。
  - 両者の知財保護だけでなく、「調査時に調査対象施設で得た情報を秘密保持対象とすること、秘密保持期間は無期限」との条項を盛り込む。
- 複数施設調査への支援業務として契約を協議して内容を決定して、終了時に精算する。
- 作業途中で、セコム山陰が工数モニタリングして、日本遠隔医療協会に報告する。

③ 個別病院と研究班の秘密保持（各施設～日本遠隔医療協会）

- 調査対象施設（病院）と研究班（日本遠隔医療協会）で情報に関する取決を行う。
  - 情報管理に関する誓約書を日本遠隔医療協会から各施設に提出する。
  - 研究班と調査各社は発注契約と秘密保持契約を結ぶ。(対象病院別の締結)
- 調査病院のリスクを“調査した内容が外部に漏洩すること”として、防衛する。
- 研究班の秘密保持の誓約の元で、委託する調査会社に対しても同様に遵守させる

④ 調査各社の病院別調査契約（各社～日本遠隔医療協会）

- 日本遠隔医療協会と各社で締結する。
- 各社は日本遠隔医療協会に見積書を提出する。
- 日本遠隔医療協会は各社に発注書を渡す。これを契約とする。
- 秘密保持契約を別に締結する。
  - 両者の知財保護だけでなく、「調査時に調査対象施設で得た情報を秘密保持対象とすること、秘密保持期間は無期限」との条項を盛り込む。
  - 秘密保持契約のサンプルは日本遠隔医療協会から提供する。
- 調査担当各社には､秘密保持を前提として､A 病院調査報告書をサンプルとして開示する。この報告書も秘密保持対象とする。

⑤ 見積と契約の手続について

- 以下の条件で見積書を作成して、研究事務局（takahasegawa@j-telemed-s.jp）に PDF で提出する。
  - 本資料に定める調査を行う。
  - 人件費 300 万円に収まる範囲での作業を計画する。
  - 工数（調査、図書作成)、出張旅費、必要経費（消耗品等）を示す。

- 週一回、工数実績を報告いただく（セコム山陰でモニタリング、集計する）
- 担当窓口を定めて、日本遠隔医療協会およびセコム山陰との連絡を一本化する。
- 終了時に工数等実績を見て、必要な調整を行う。

● セコム山陰のアシスト下で調査、報告を作成する。

- セコム山陰の情報共有システムを用いて、情報共有、データ共有を行う。
- 前述の工数報告は、同システムを用いて行う。

⑥

付属資料

参考資料１　２０２２年２月～２０２２年５月に於いてＡ病院に対して行った調査業務での工数内訳

【研究班情報】

1. 研究代表者　近藤博史
   ① 鳥取大学名誉教授（元鳥取大学医学部附属病院医療情報部　部長・教授）
   ② 協立温泉病院　院長
   ③ 特定非営利活動法人日本遠隔医療協会　特任主席研究員

2. 研究分担者　山本隆一
   ① 一般社団法人医療情報システム開発センター　理事長

3. 研究分担者　美代賢吾
   ① 国立研究開発法人　国立国際医療研究センター　医療情報基盤センター　センター長

4. 研究分担者　星本弘之
   ① 国立研究開発法人　国立国際医療研究センター　医療情報基盤センター

5. 研究分担者　長谷川高志
   ① 特定非営利活動法人日本遠隔医療協会　特任上席研究員
   ② 本調査の事務局

6. 調査事務局

特定非営利活動法人日本遠隔医療協会
厚生労働行政推進調査事業、研究運営担当（研究分担者　長谷川高志）
telemedicine-research@j-telemed-s.jp

日本遠隔医療協会事務局
〒370-0033　群馬県高崎市中大類町 37-1
高崎健康福祉大学健康福祉学部 医療情報学科内
http://http://j-telemed-s.jp/

【資料５　調査担当企業・日本遠隔医療協会間秘密保持契約】

【日本遠隔医療協会・調査担当企業間の秘密保持契約書（ひな形)】

秘密保持契約書

特定非営利活動法人日本遠隔医療協会（以下「甲」という）と＊＊＊＊＊＊＊＊＊株式会社（以下「乙」という）は、甲乙間で第１条に定める本件業務の遂行するにあたり、互いに開示又は提供する情報の秘密保持に関して、以下のとおり秘密保持契約（以下「本契約」という）を締結する。

第1条（本件業務）

1 本契約は、調査対象病院のサイバーセキュリティに関する調査に際し、調査で収集する情報について、その秘密保持に関する取扱いを定めることを目的とする。

2 調査により収集する情報は、調査研究の委託者である厚生労働省に、秘密情報（非公開対象）として提出する。

3 調査により収集する情報について、統計的処理等を施して、調査対象病院との関係性を消失したものを、学術的に公開（論文、講演、書籍執筆）することは本件業務の一部に含まれる。

第2条（秘密情報）

1 本契約において秘密情報とは、文書、口頭、物品および電子媒体等形態を問わず、本件業務の実施に伴い収集する情報のうち、次の各号に定める情報をいう。

　1　秘密である旨が明記された文書、図面、写真またはその他有体物（電子的手段による場合を含む。）として開示された情報。

　2　調査対象病院の施設運営に関する情報で、調査の際に収集された聞き取り結果、文書、図面、写真またはその他有体物（電子的手段による場合を含む。）。

2 前項の規定にかかわらず、次の各号に該当することを乙が証明し得るものは秘密情報には含まれないものとする。

　① 調査対象病院より開示を受ける前に、既に所有または取得していたもの

　② 調査対象病院より開示を受ける前に、既に公知公用となっているもの

　③ 調査対象病院より開示を受けた後に、乙が本契約の規定に違反することなく公知公用となったもの

　④ 開示の権限を有する第三者から、秘密保持の義務を負うことなく、適法に知得したもの

第3条（秘密保持）

1 乙は、甲の事前の書面（電磁的措置を含む。）による承諾なしに、秘密情報を本件業務以外の目的のためには一切使用しない。

2 乙は、本件業務の遂行上知る必要のある自己の従業者および本件業務の一部を委託する他団体の従業者（以下「関係者」という）に対してのみ、秘密情報を開示および共有することとし、合理的かつ善良と認められる注意をもって管理するものとする。

3 乙は、秘密情報を関係者および本件業務で定義した開示先以外の第三者に開示しない。

第4条（秘密情報の管理）

乙は、本件業務を遂行するために合理的に必要な範囲内で、秘密情報を複写および複製することができるものとし、その範囲を超えて複写・複製してはならない。また、秘密情報の複写物および複製物も秘密情報とみなすものとする。

第5条（秘密情報の返還）

乙は、甲の要請があり次第、速やかに秘密情報（複写物、複製物を含む）を返還し、返還が不可能な場合には、甲の指示に従って、当該資料を消去または廃棄するものとする。

第6条（秘密情報の権利）

1　秘密情報に関する一切の権利は、調査対象病院に帰属するものとする。また、当事者間で別途合意した場合を除き、秘密情報の開示は、乙に対していかなる権利も付与しないものとして解釈する。

第7条（損害賠償）

甲は、乙が本契約の規定に違反した場合、当該違反を是正するために必要な措置をとることを求めることができるとともに、当該違反によって被った損害の賠償を請求することができる。

第8条（有効期間）

本契約の有効期間は、202＊年＊月＊日から2023年 3 月 31 日までとする。ただし、第3条、第4条、第5条、第6条および第7条はそれぞれの対象事項が存続する限り、本契約の有効期間終了後も有効に存続する。

第9条（協議事項）

甲及び乙は、本契約に定めのない事項及び本契約の履行又は解釈にあたって生じた疑義について、信義誠実の原則に従い、その都度協議により定めるものとする。

本契約締結の証として、本書２通を作成し、甲及び乙は記名押印のうえ、各自その１通を保有する。

２０２＊年　＊＊月　＊＊日

甲：群馬県高崎市新後閑町4-2
特定非営利活動法人日本遠隔医療協会
理事長　　酒巻　哲夫　（押印）

乙：

【資料６　調査担当企業工数確認票】

病院に対するサイバーセキュリティに関する調査・報告書作成業務

対象病院	
調査企業	

	項目		予定工数（時間）	実績工数（時間）
1	①チェックリストによるヒアリング（経営層向け）	調査	16.00	
2	①チェックリストによる調査結果（経営層向け）	図書作成	16.00	
3	②チェックリストによるヒアリング（システム管理者向け）	調査	16.00	
4	②チェックリストによる調査結果（システム管理者向け）	図書作成	16.00	
5	③チェックリストによるヒアリング（医療従事者・一般のシステム利用者向け）	調査	16.00	
6	③チェックリストによる調査結果（医療従事者・一般のシステム利用者向け）	図書作成	16.00	
7	④病院情報システムのバックアップ状況（表）	調査	4.00	
8	④病院情報システムのバックアップ状況（表）	図書作成	16.00	
9	⑤外部接続先一覧　および　外部接続先調査履歴	調査	4.00	
10	⑤外部接続先一覧　および　外部接続先調査履歴	図書作成	16.00	
11	⑥ネットワーク概要図	調査	4.00	
12	⑥ネットワーク概要図	図書作成	16.00	
13	⑦情報システム管理体制図	調査	4.00	
14	⑦情報システム管理体制図	図書作成	16.00	
15	移動			
16	打合せ			
17	その他（事前調査、進捗報告など）		24.00	
		合計	200.00	

（調査会社）　→　セコム山陰（取り纏め）　→　日本遠隔医療協会

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。

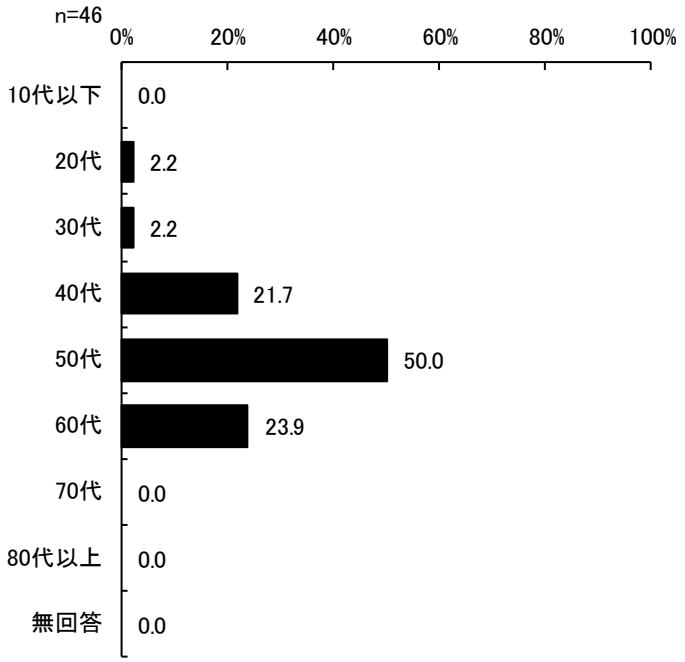
２．調査結果

（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。

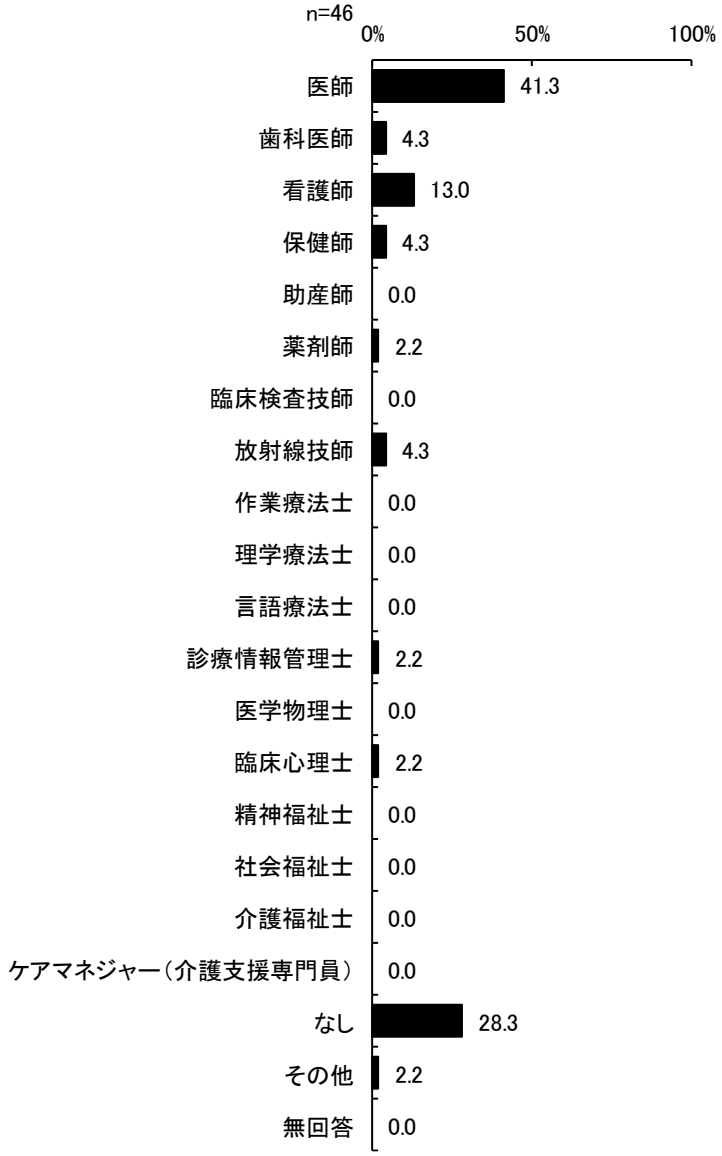
図表１　年齢（Q1）



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】

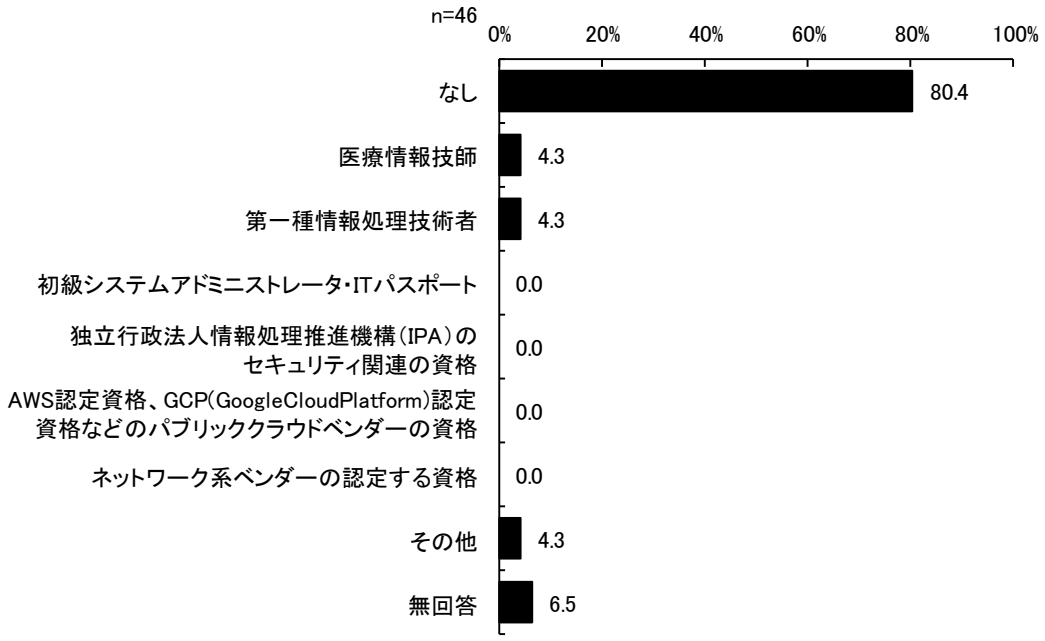


※「その他」の主な回答は以下の通り。
・臨床工学技士

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】

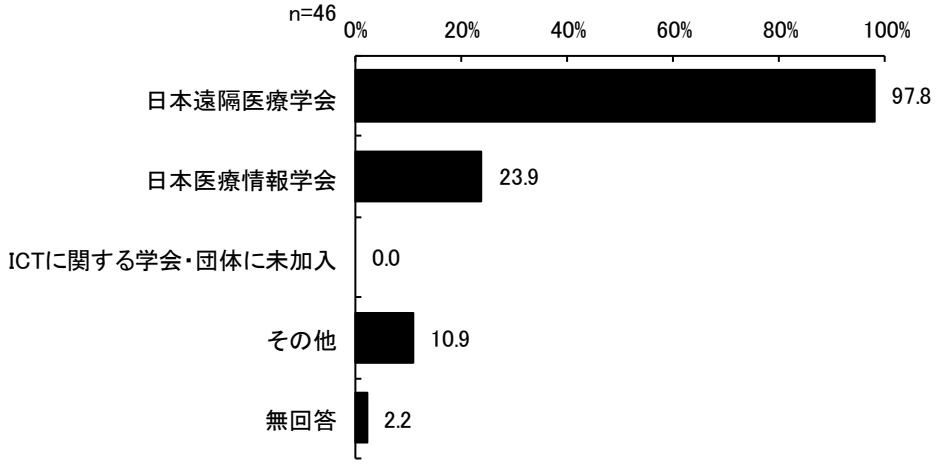


※「その他」の主な回答は以下の通り。
- 診療放射線技師
- IS027001 審査員補

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】



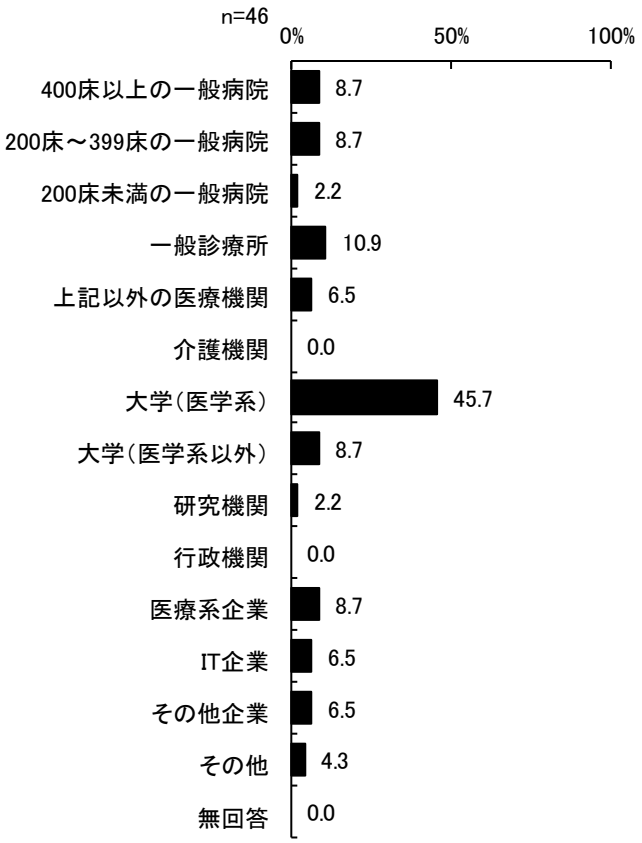
※「その他」の主な回答は以下の通り。

- 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】

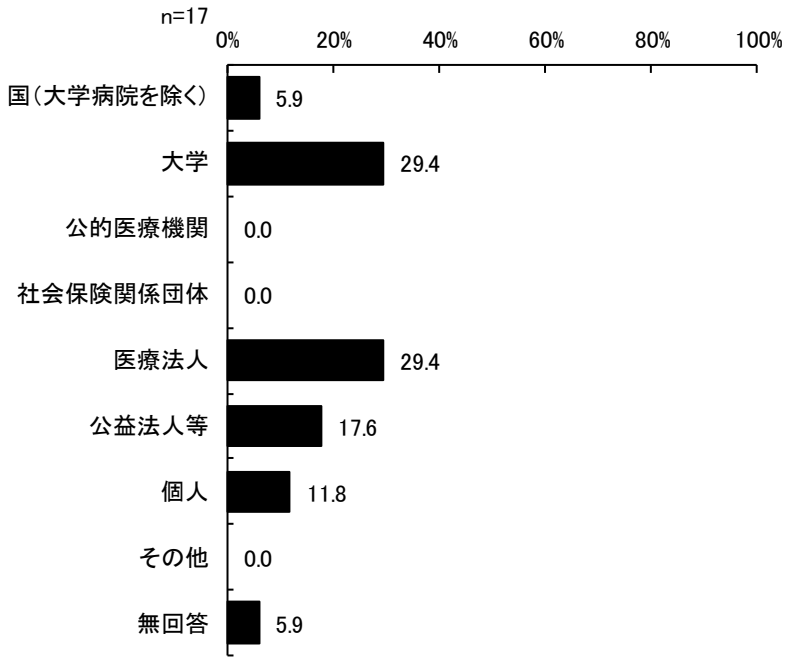


※「その他」の主な回答は以下の通り。
・訪問看護ステーション

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。

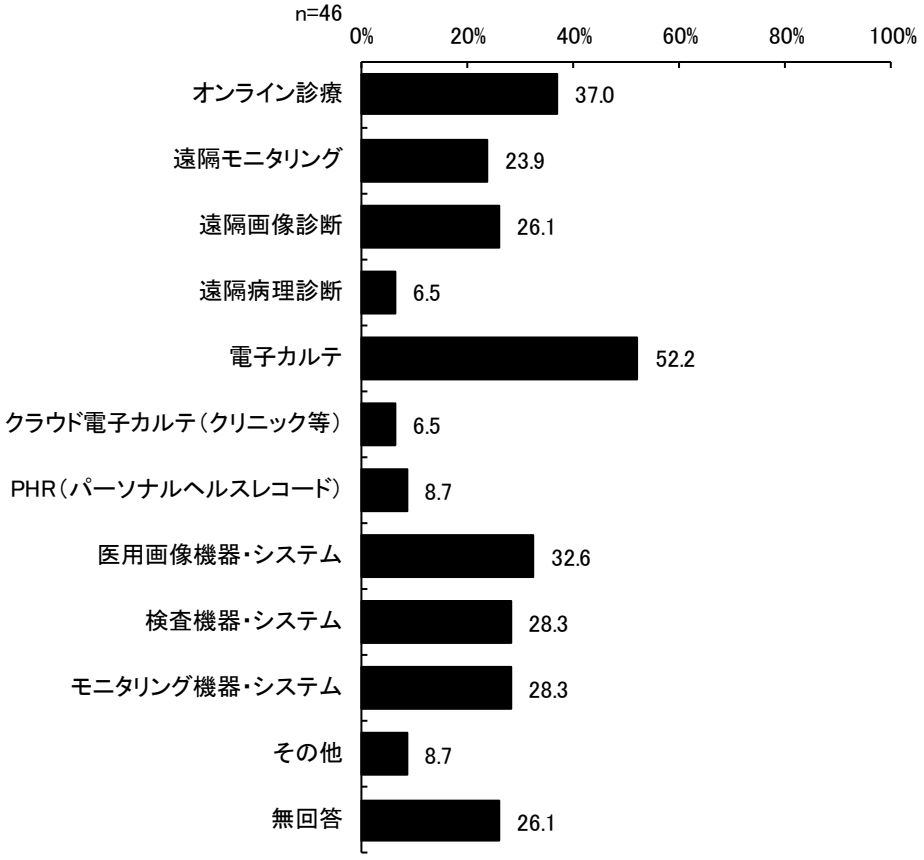
図表 6　施設の開設者（医療機関の場合）（Q6）



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】

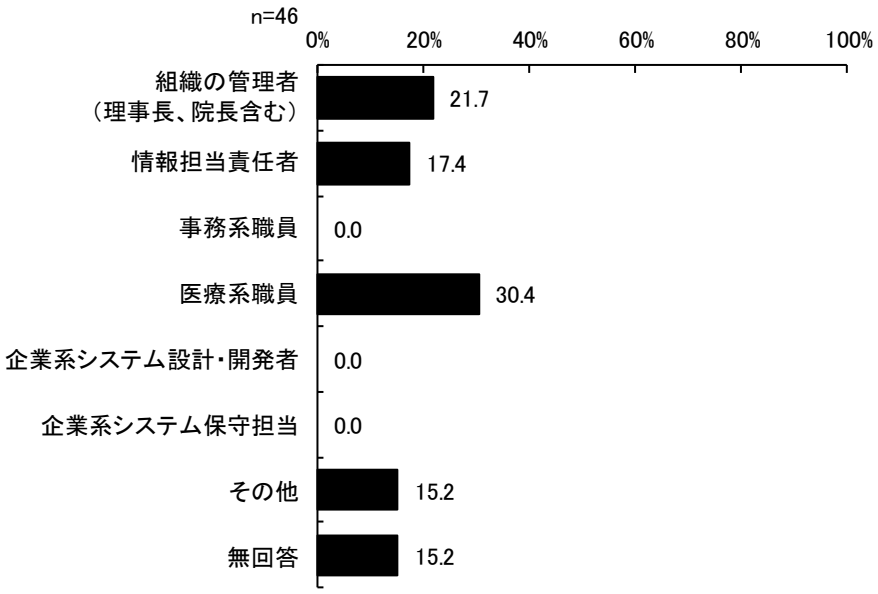


※「その他」の主な回答は以下の通り。
- オンライン授業
- 遠隔看護
- なし

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）

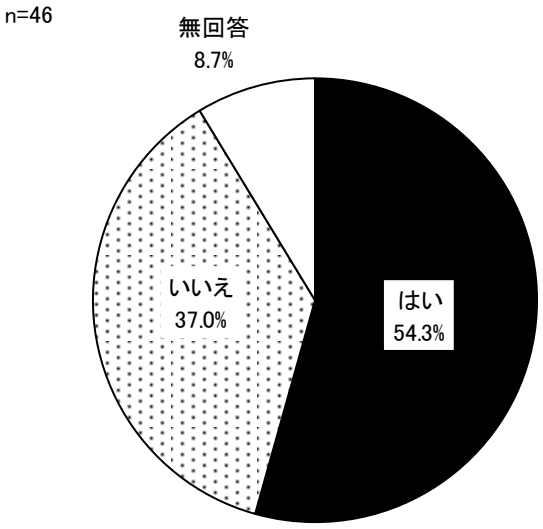


※「その他」の主な回答は以下の通り。
- 機械設計、ソフト設計を担当
- 市場調査を担当
- 大学教授
- 教員
- 講師

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。

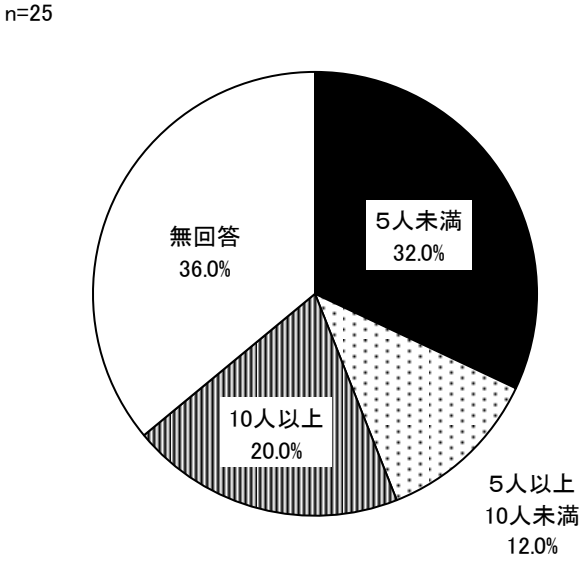
図表 9　情報システムを統括する部署はあるか（Q9）



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。

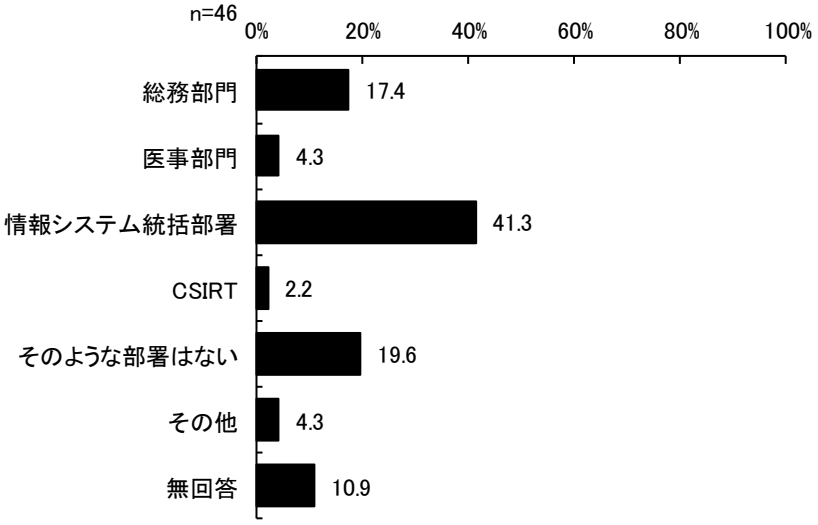
図表 10　情報システムを統括する部署への所属人数（Q10）



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）

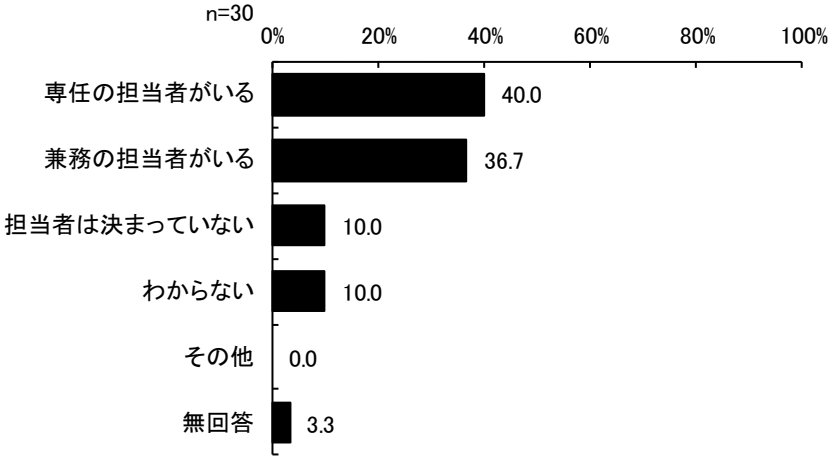


※「その他」の主な回答は以下の通り。
・不明

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）

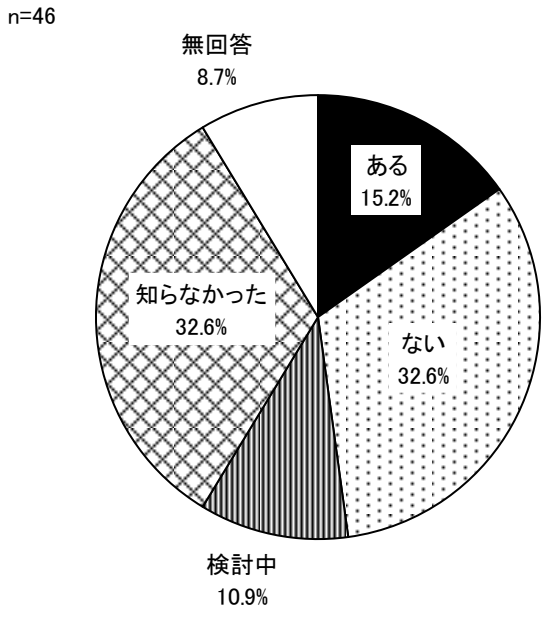
	調査数	平均値	標準偏差	中央値	最小値	最大値
非常勤の兼務者の人数	6	0.17	0.37	0	0	1

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

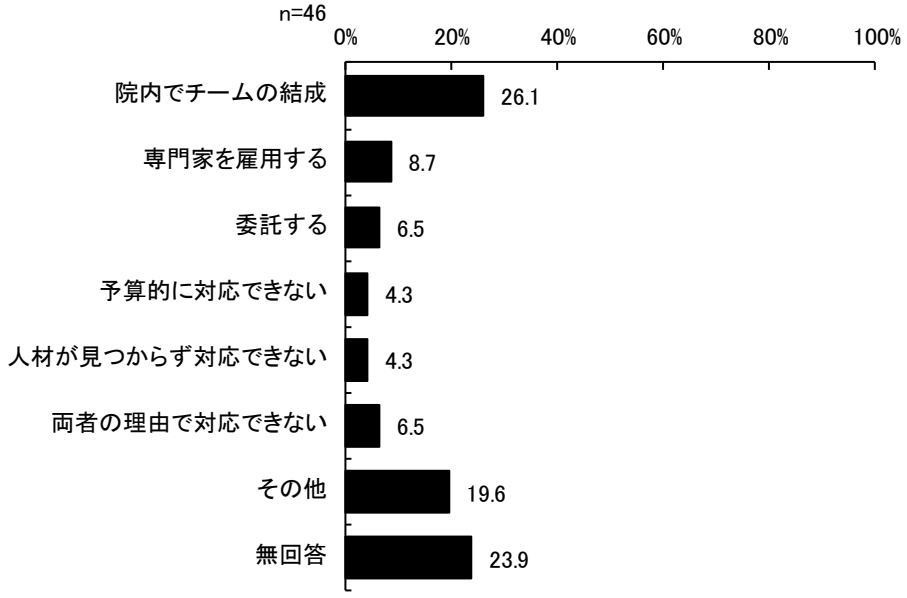
図表 17　所属する組織に CSIRT はあるか（Q17）



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）

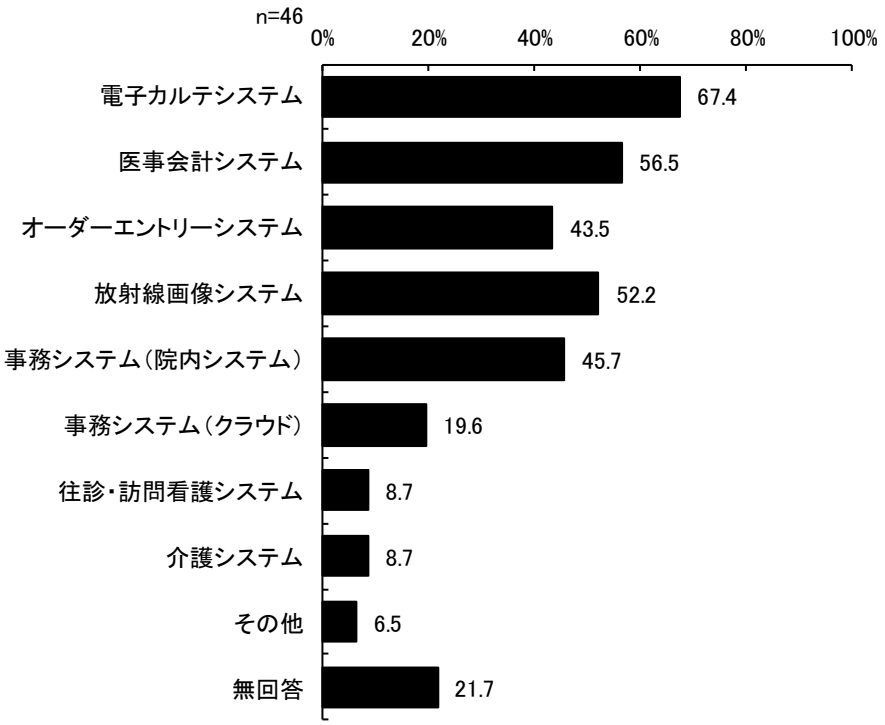


※「その他」の主な回答は以下の通り。
- 学内共通の組織として運用
- 現時点では未定
- これから検討する
- 積極的に習得し普及に努めたい
- 大学側に設置（病院の責任者も構成員として参加）
- 予算も人材も、ノウハウも何もない
- わからない

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】

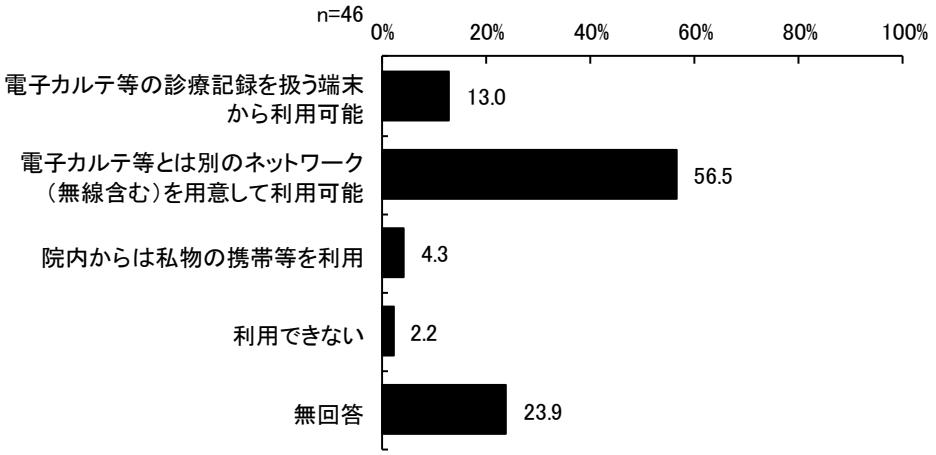


※「その他」の主な回答は以下の通り。
- 遠隔読影システム
- オンライン診療システム
- オンライン服薬指導システム

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。

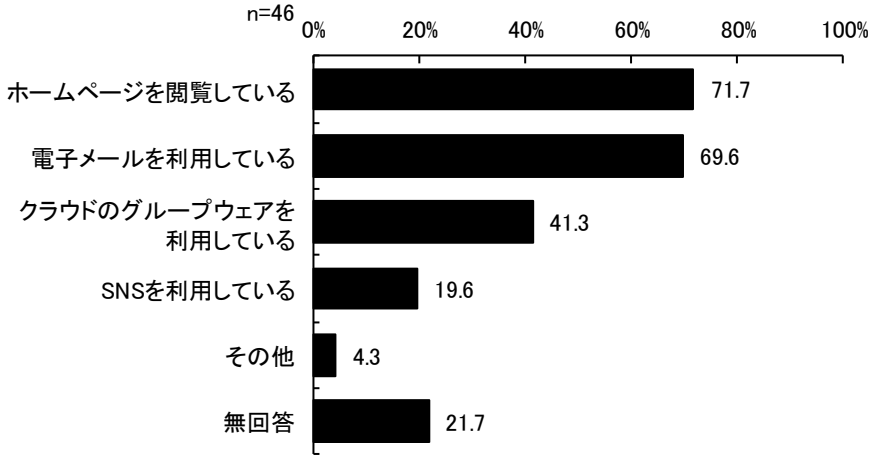
図表 20　院内における職員のインターネットの利用可否（Q20）



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】

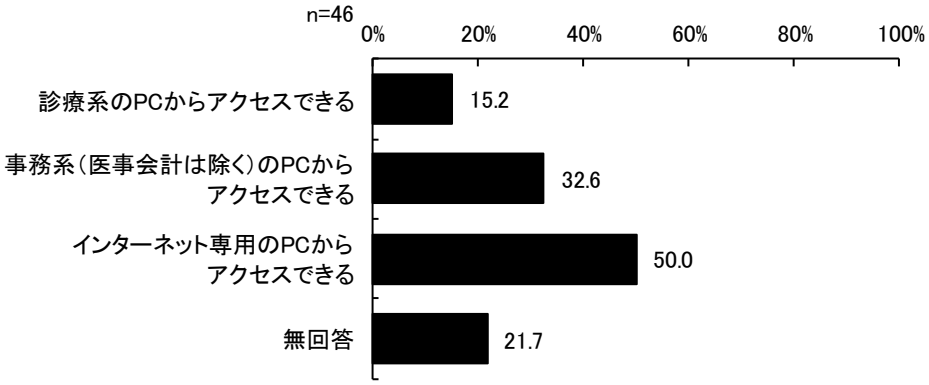


※「その他」の主な回答は以下の通り。
・コンテンツフィルタに抵触しない限り制限はしていない
・帝人バイタルリンク

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。

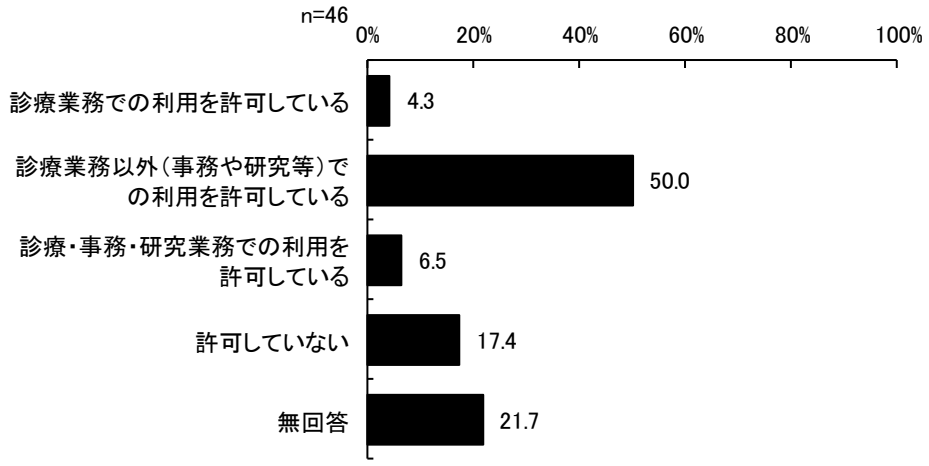
図表22　インターネットにアクセスできるパソコン（PC）について（Q22）【複数回答】



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。

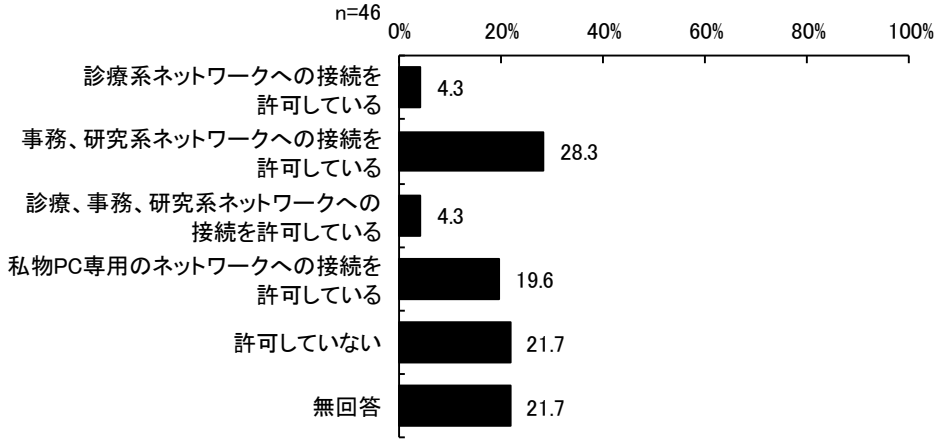
図表23　職員（医師など）の私物のPCを用いて業務を行うことを許可しているか（Q23）



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）

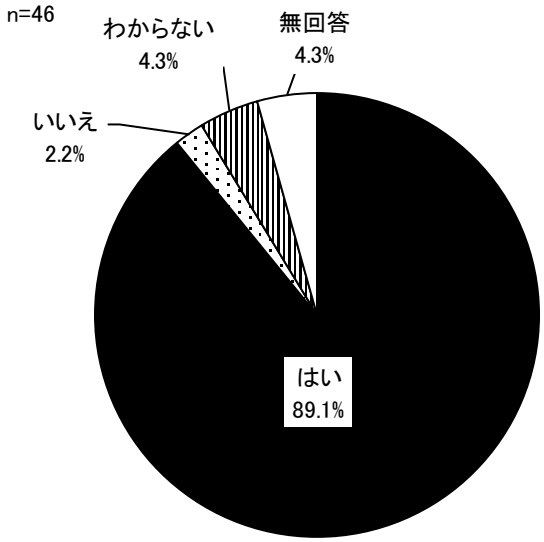


（2）組織で実施しているセキュリティ対策

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。

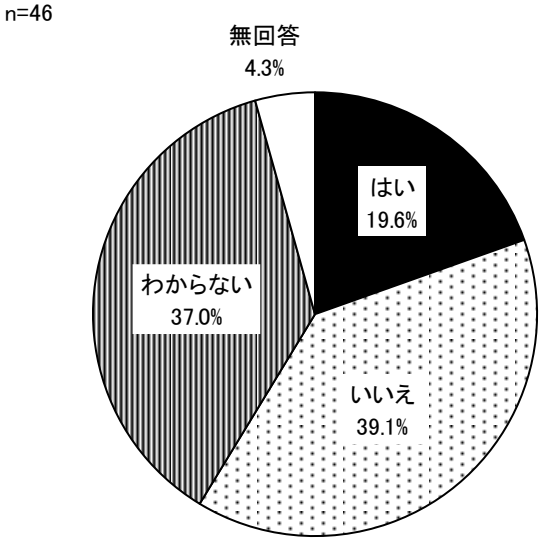
図表 25　ウイルス対策ソフトを導入しているか（Q25）



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

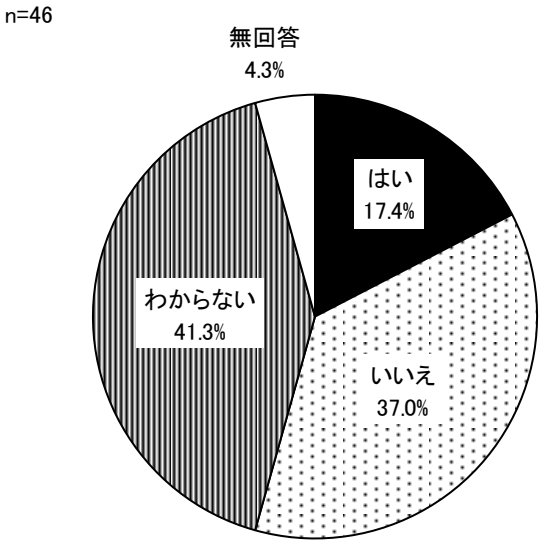
（表頭）Q26 資産管理ソフトを導入しているか
（表側）Q17 「医療情報システムの安全管理ガイドライン」にあるCSIRTはあるか

	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

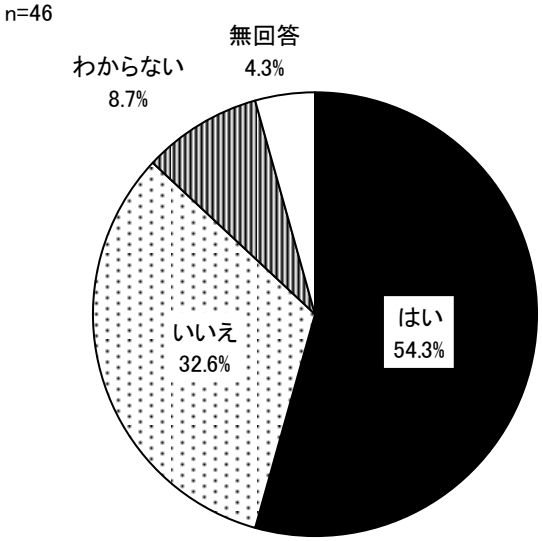
（表頭）Q27 仮想ブラウザを導入しているか
（表側）Q17 「医療情報システムの安全管理ガイドライン」にあるCSIRTはあるか

	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

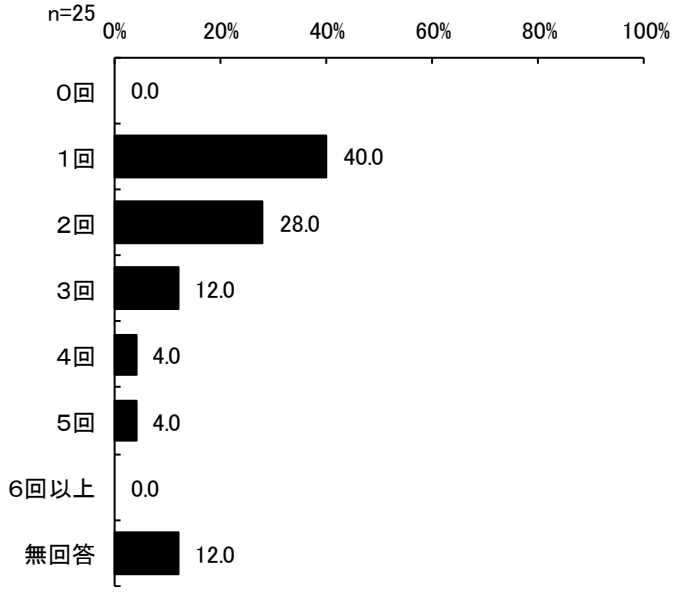
（表頭）Q28 セキュリティ教育を行っているか
（表側）Q17 「医療情報システムの安全管理ガイドライン」にあるCSIRTはあるか

	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。

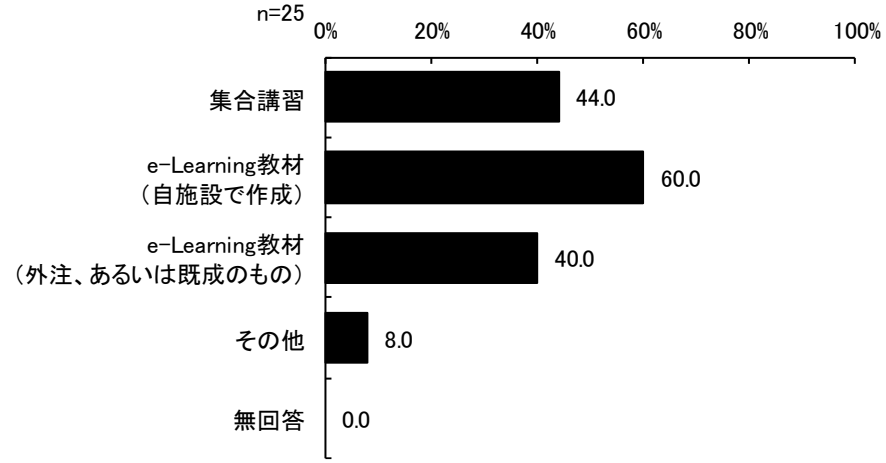
図表 38　セキュリティ教育は年に何回行っているか（Q29）



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】

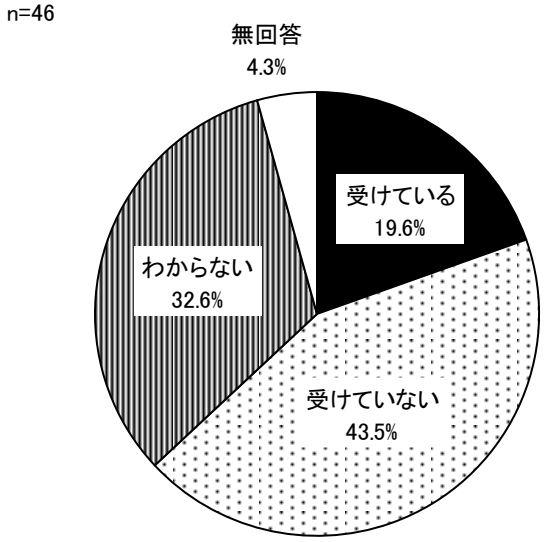


※「その他」の主な回答は以下の通り。
- 個別
- 行っていない

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

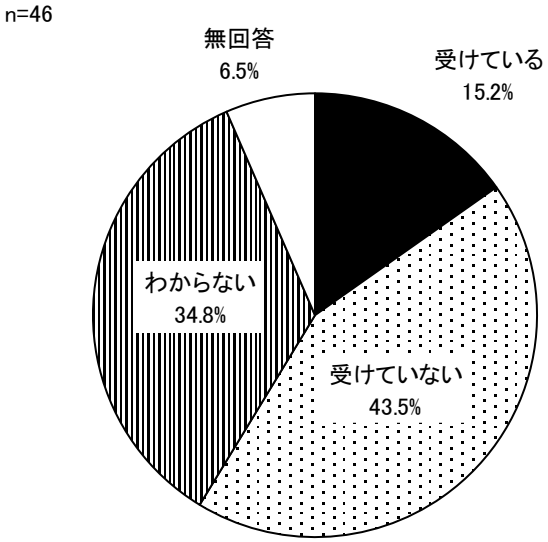
	調査数	受けている	受けていない	わからない	無回答
ある	7	5	－	2	－
	100.0	71.4	－	28.6	－
ない	35	3	20	12	－
	100.0	8.6	57.1	34.3	－

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

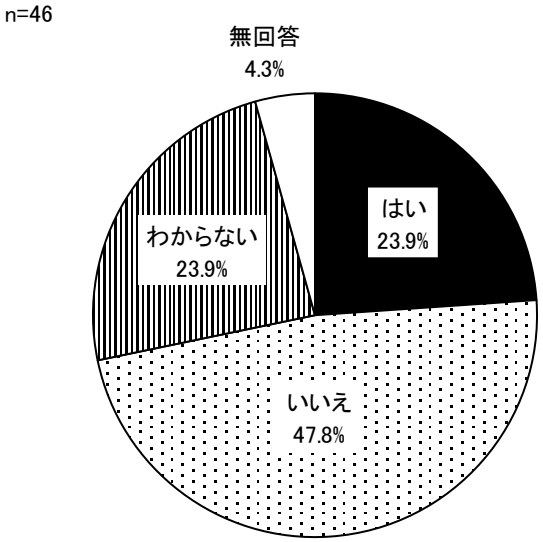
（表頭）Q32 ペネトレーションテストを受けているか（直近３年以内の状況）
（表側）Q17 「医療情報システムの安全管理ガイドライン」にあるCSIRTはあるか

	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

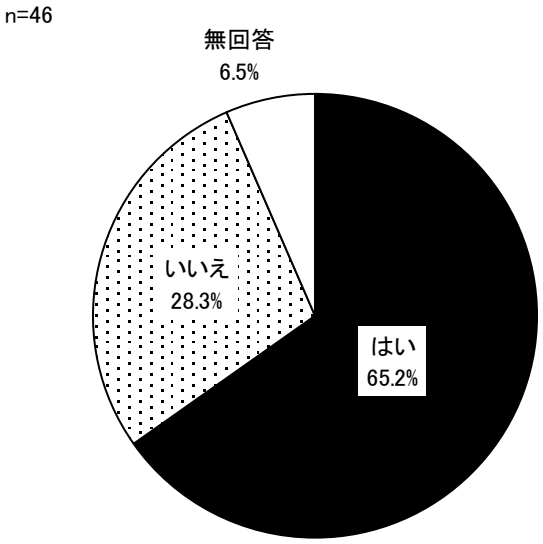
	調査数	はい	いいえ	わからない	無回答
ある	7	6	－	1	－
	100.0	85.7	－	14.3	－
ない	35	4	21	10	－
	100.0	11.4	60.0	28.6	－

（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

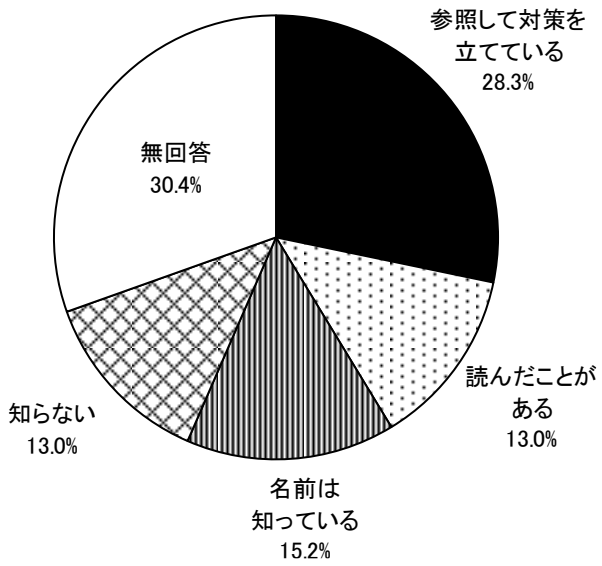
	調査数	はい	いいえ	無回答
ある	7	7	－	－
	100.0	100.0	－	－
ない	35	21	13	1
	100.0	60.0	37.1	2.9

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

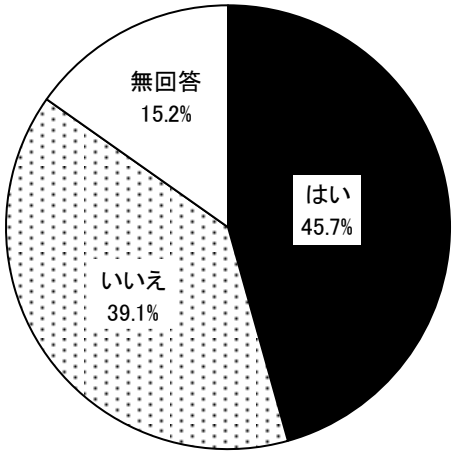


3）セキュリティインシデント発生時の手順が定められているか

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

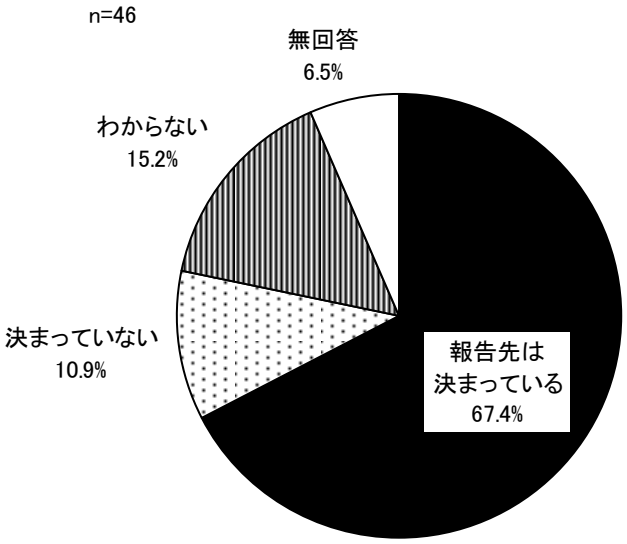


（4）セキュリティインシデント発生時の対応

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。

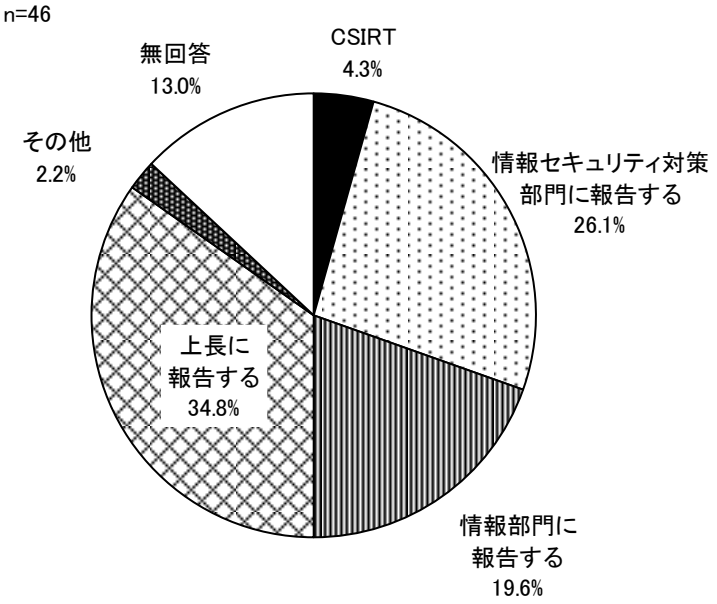
図表 58　職員がセキュリティインシデントを発見したときに報告する部署が決まっているか（Q37）



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）

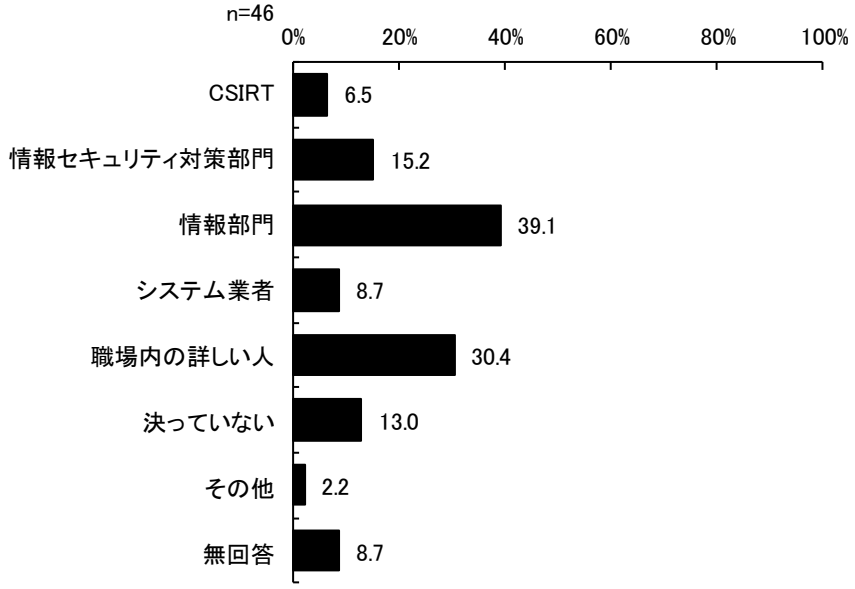


※「その他」の主な回答は以下の通り。
・不明

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】

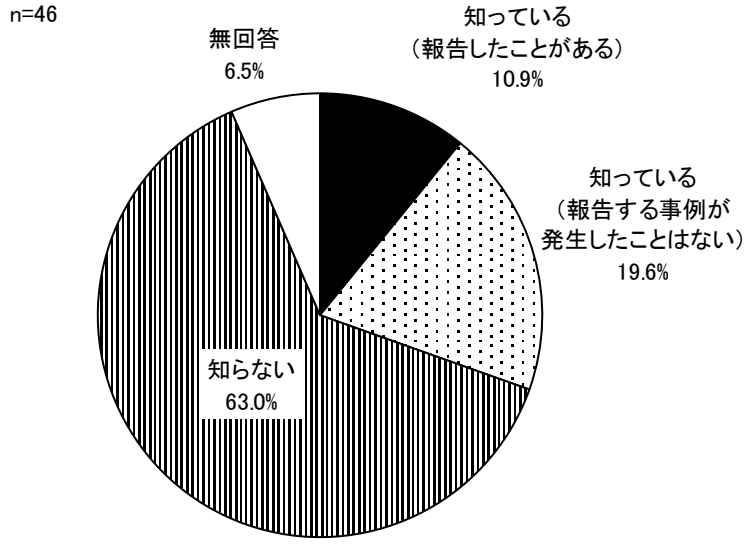


※「その他」の主な回答は以下の通り。
・不明

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。

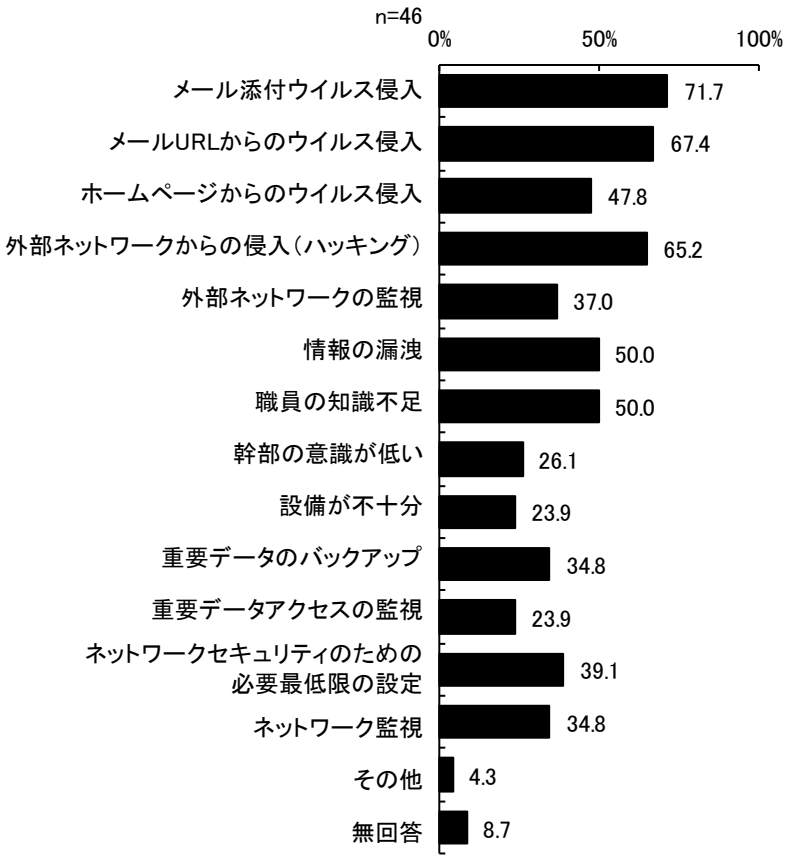
図表 61　情報セキュリティインシデント発生時の厚生労働省の窓口を知っているか（Q40）



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】

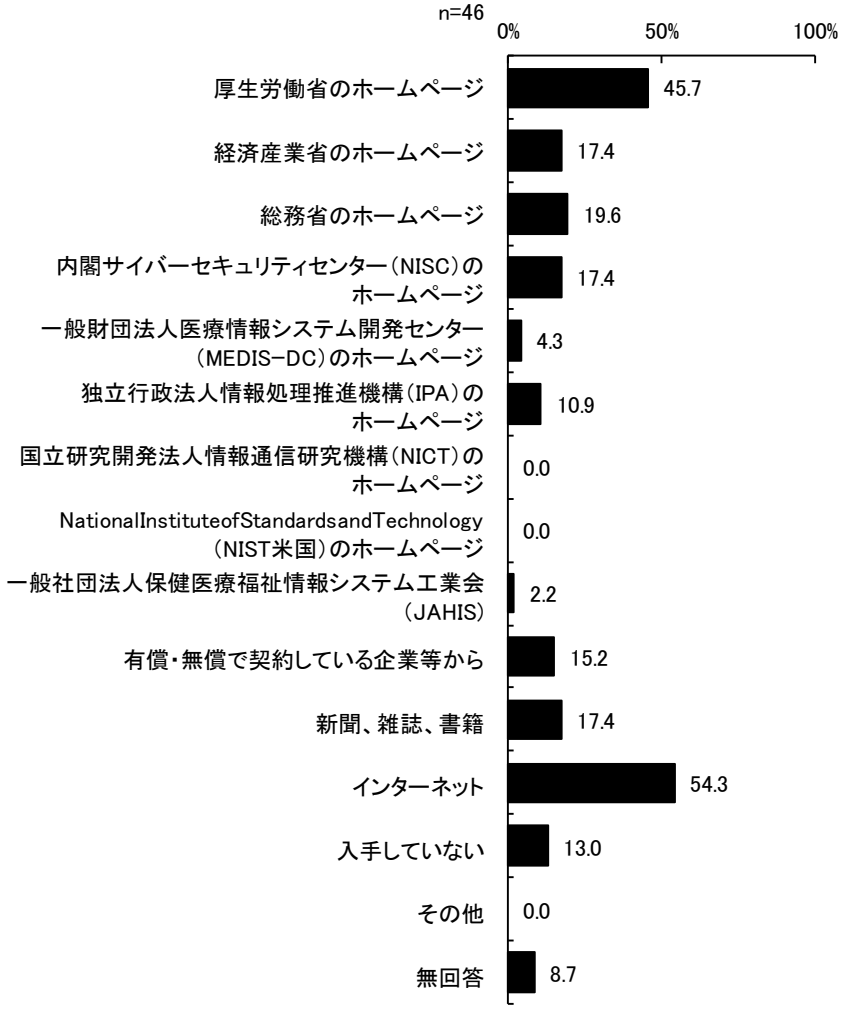


※「その他」の主な回答は以下の通り。
- フィッシング詐欺
- 電話を利用した攻撃
- 予算がない

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。

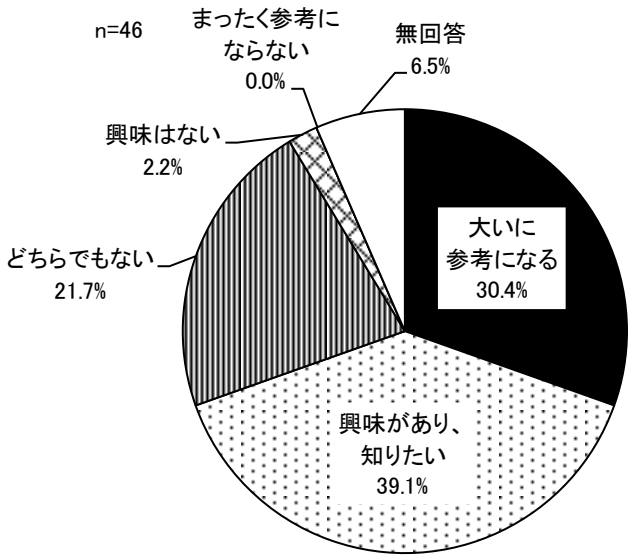
図表 63　情報セキュリティに関する情報源（Q42）【複数回答（3 つまで）】



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。

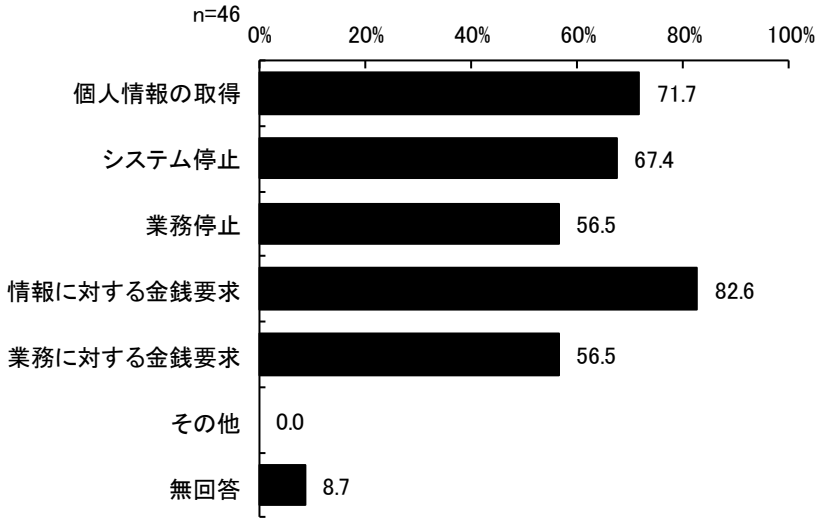
図表 64　他の施設の対策状況は対策を立てる上で参考になるか（Q43）



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。

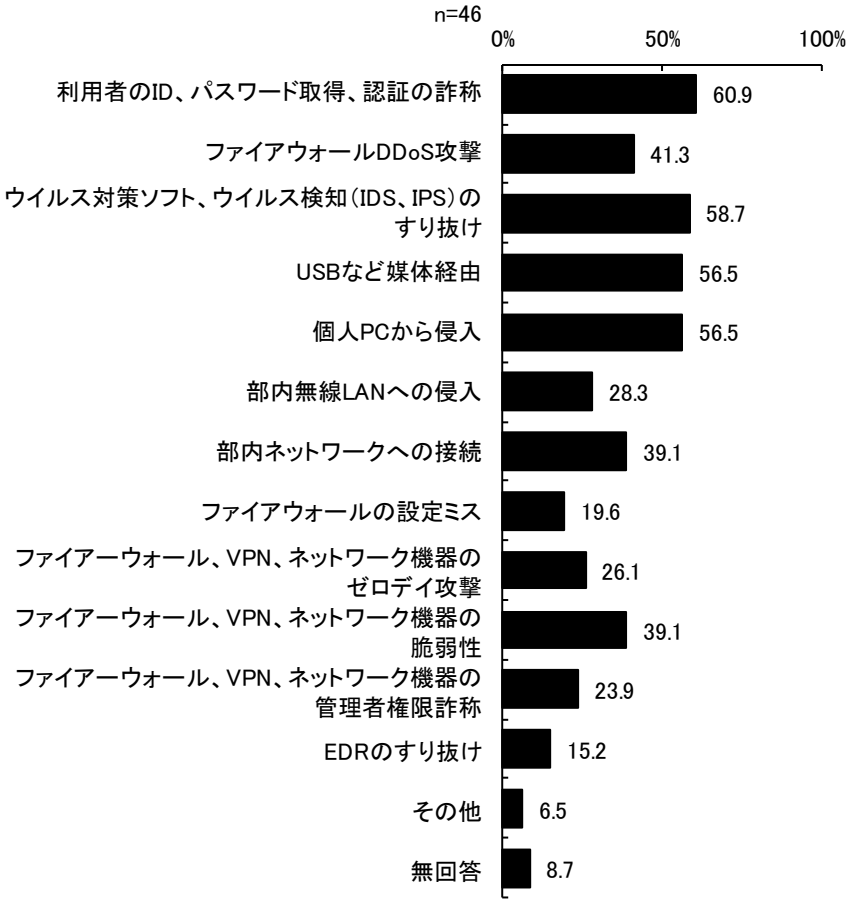
図表 65　最近のサイバーテロの目的（Q44）【複数回答】



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】

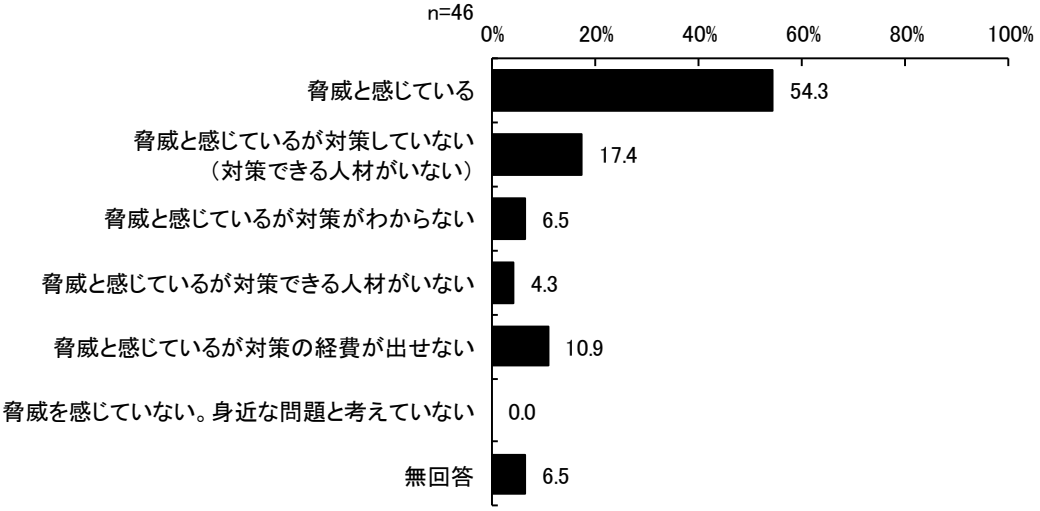


※「その他」の主な回答は以下の通り。
- ランサムウェア
- 個人 PC 売却時にハードディスクの消去情報復元

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。

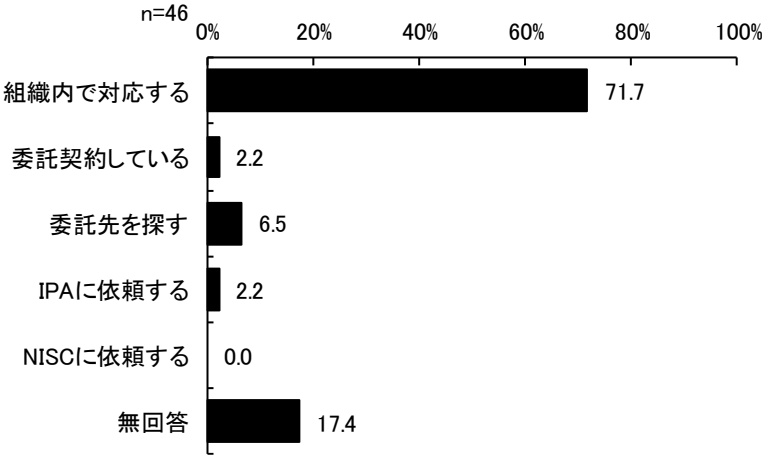
図表 67　サイバーセキュリティを脅威と感じているか、対策を検討しているか、問題は何か（Q46）



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。

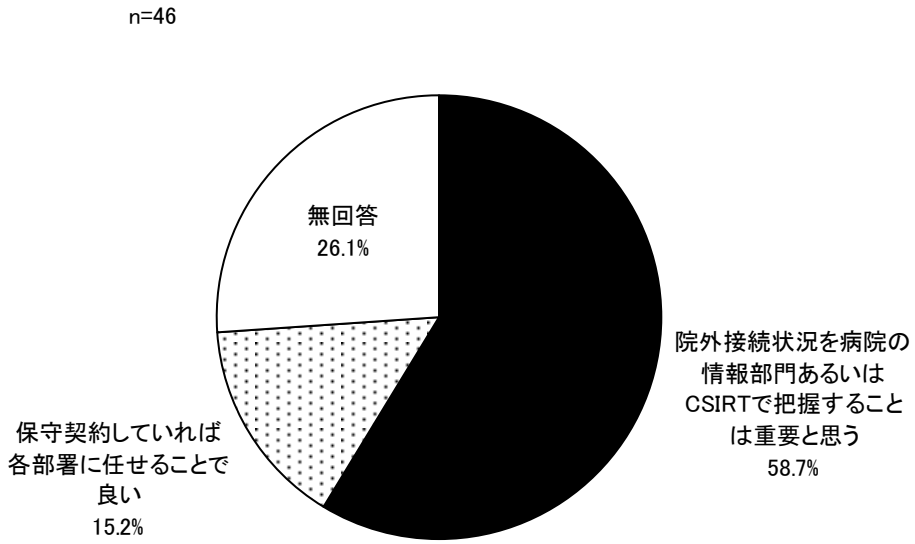
図表 68　インシデント発生時の対応について（Q47）



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）

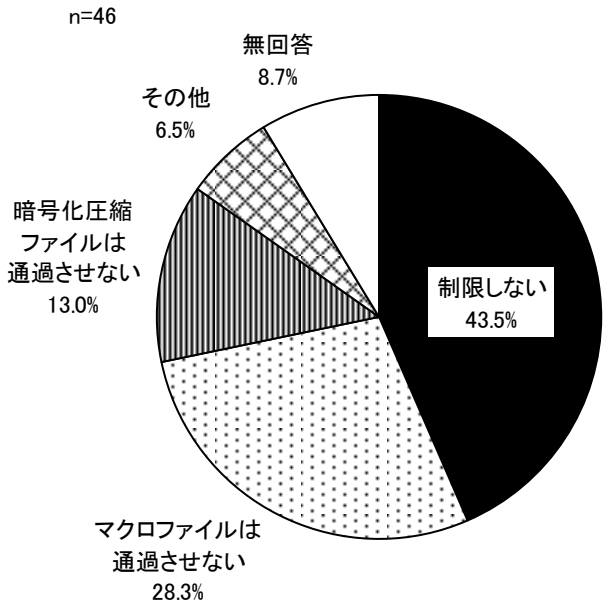


（5）侵入経路の対策として実施している事項等

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）

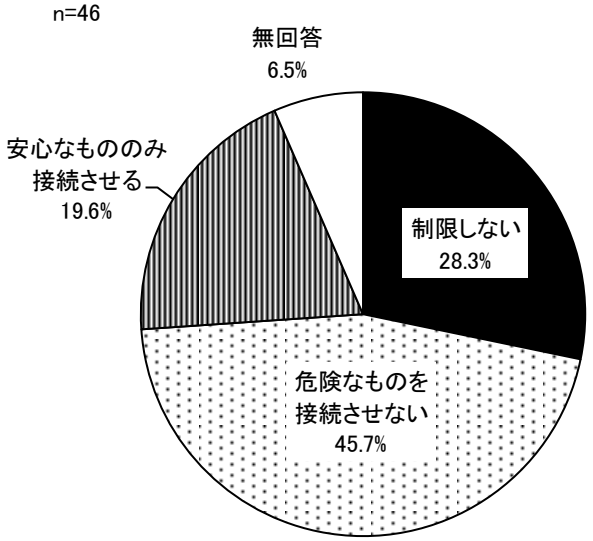


※「その他」の主な回答は以下の通り。
- EXE 等、実行ファイルは通過させない
- サンドボックスを用意している
- 外部メールサービスを利用している
- 知らない

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。

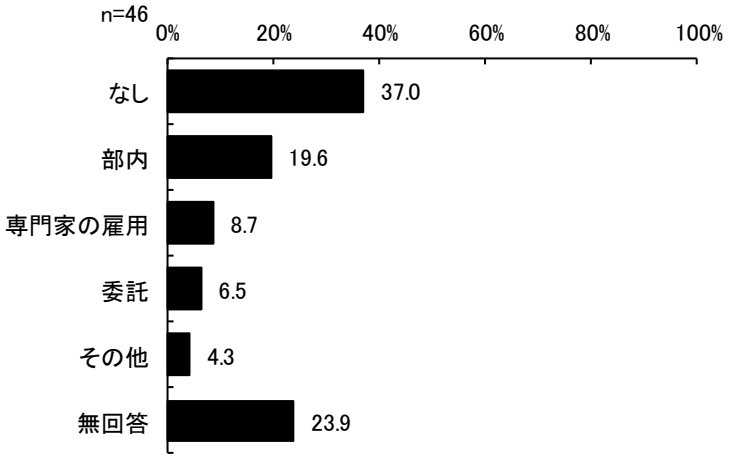
図表 71　ホームページ閲覧に関する対策（Q50）



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）

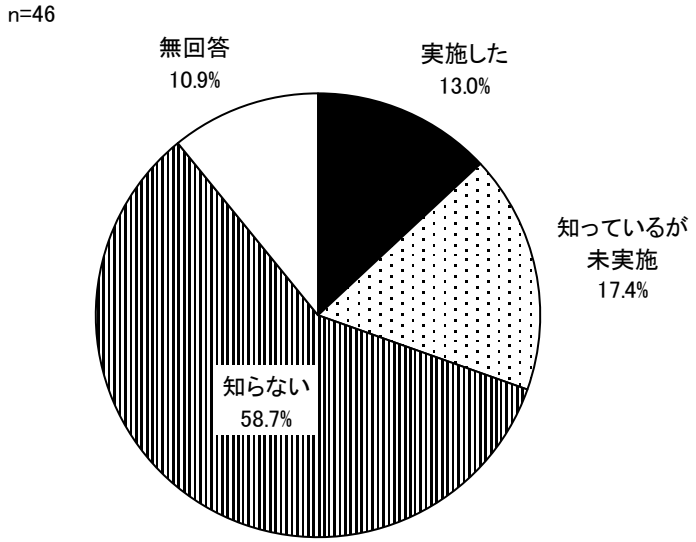


※「その他」の主な回答は以下の通り。
- 大学全体で NISC 基準に沿って組織化
- 不明

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。

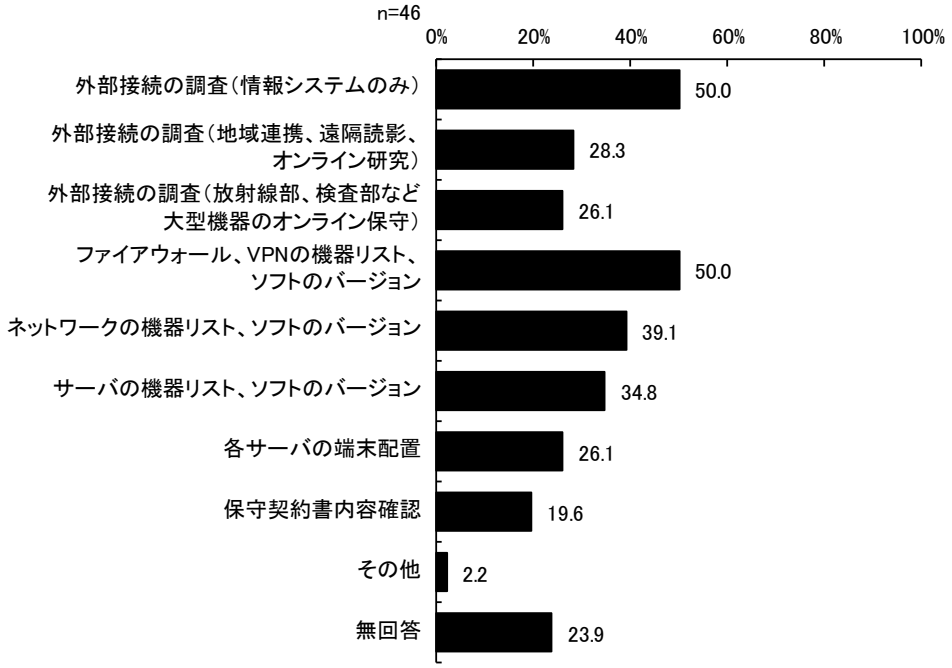
図表 73　医療情報システムの安全管理ガイドラインに添付されたサイバーセキュリティに関するチェックリスト、フローを知っているか（Q52）



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】

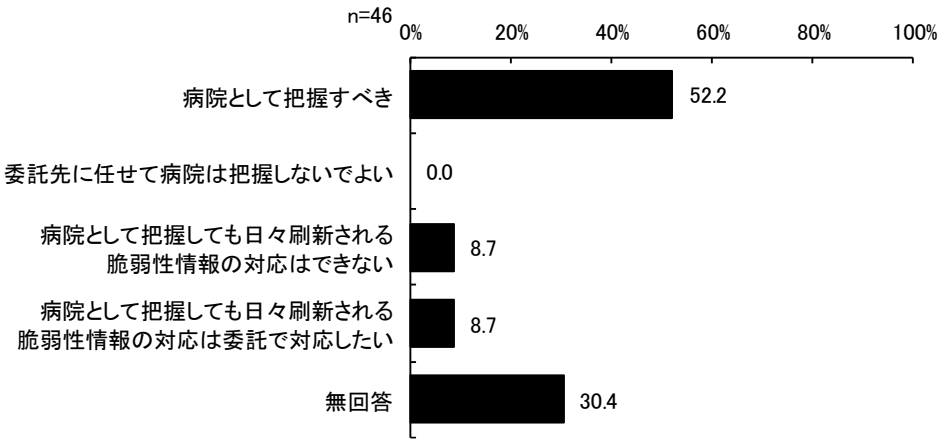


※「その他」の主な回答は以下の通り。
・不明

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。

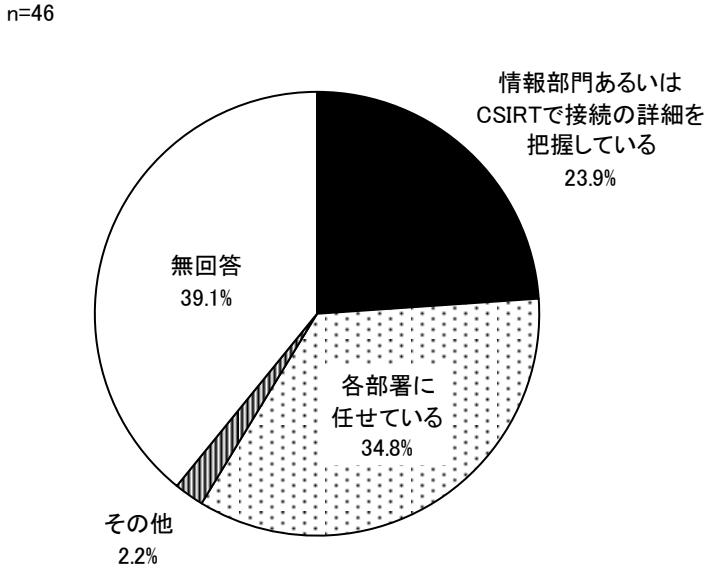
図表 75　システムの保守回線・CT・MRI 等の検査機器の保守回線の詳細（Q54）



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）

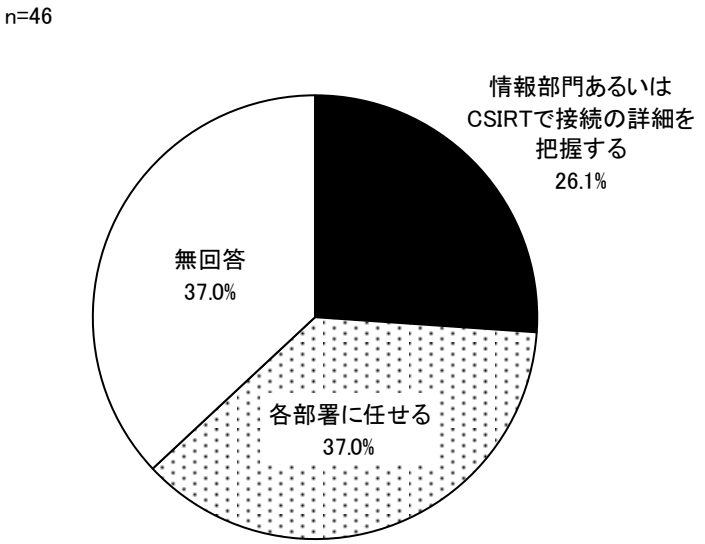


※「その他」の主な回答は以下の通り。
・不明

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。

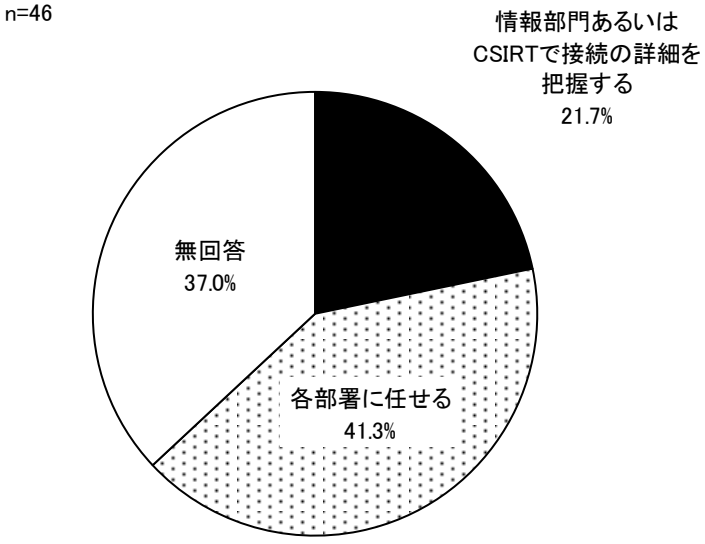
図表 77　オンライン診療・遠隔モニタリング・院内 SNS の接続について（Q56）



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。

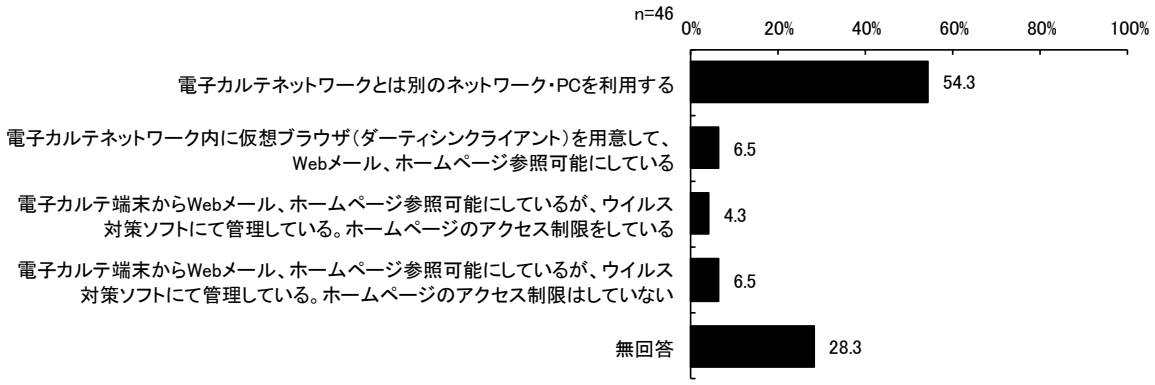
図表 78　匿名化してオンライン接続する遠隔画像診断・匿名化してオンライン接続する調査等の接続について（Q57）



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。

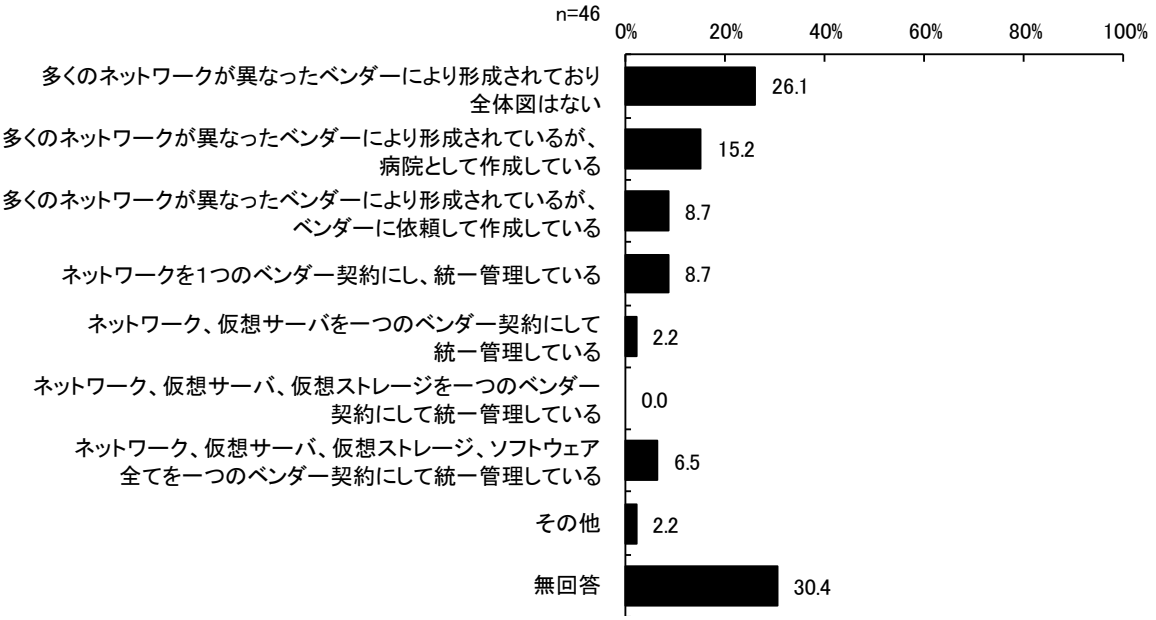
図表 79　利用者のホームページ閲覧、メール受信について（Q58）



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）

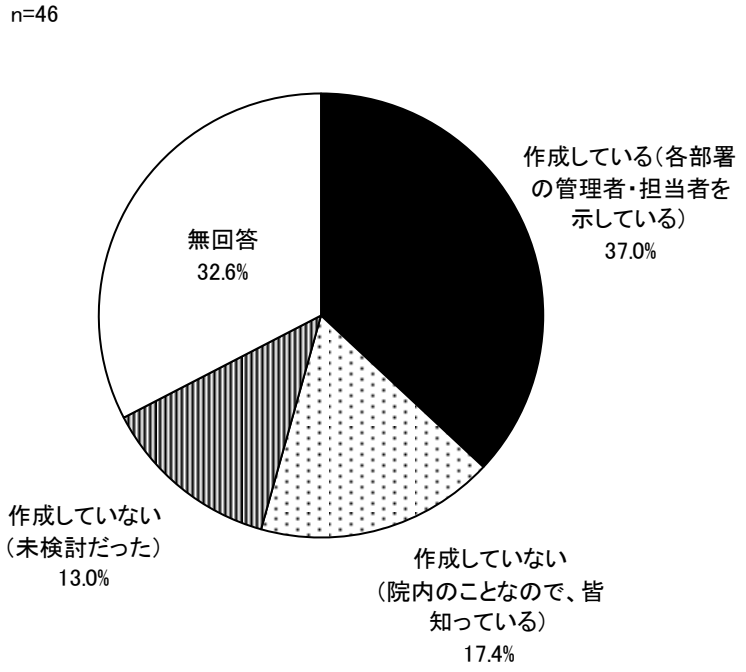


※「その他」の主な回答は以下の通り。
・不明

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。

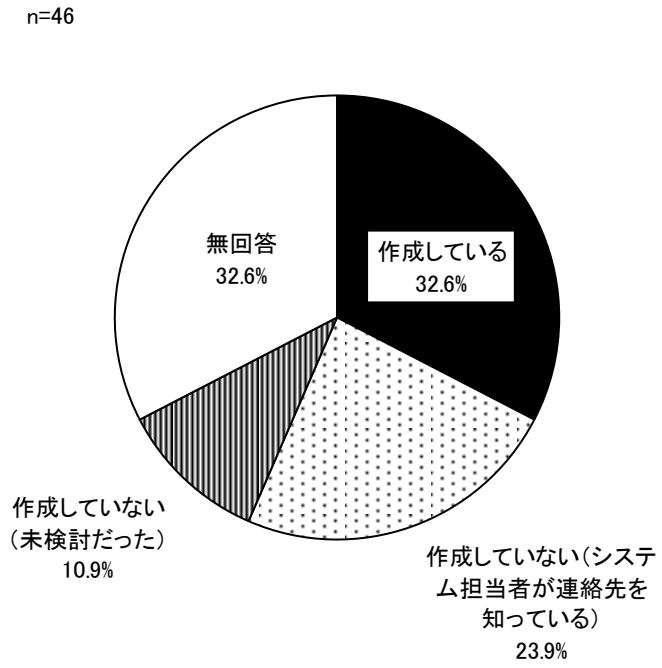
図表 81　電子カルテシステム・部門システムそれぞれについて院内の管理者・担当者一覧を作成しているか（Q60）



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）

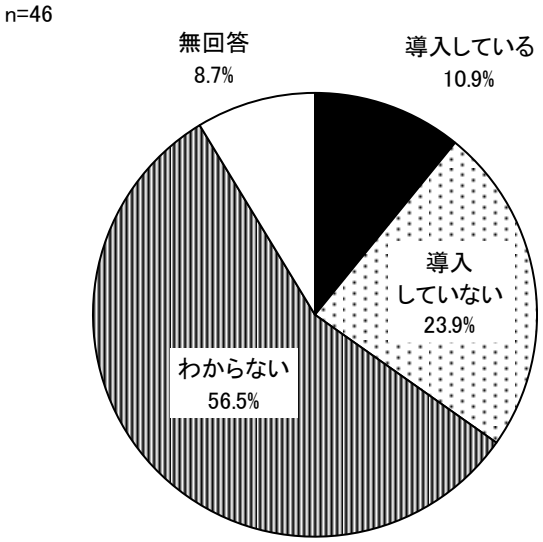


（6）ウイルス対策の状況

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。

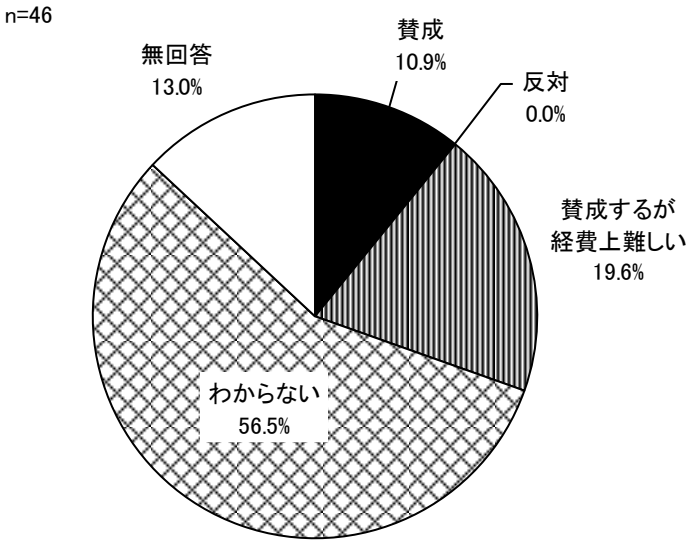
図表 83　端末への EDR（Endpoint Detection and Response）導入状況（Q62）



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。

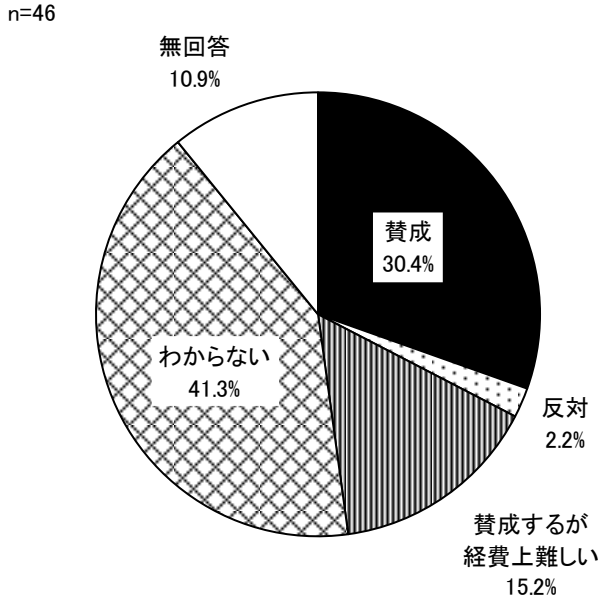
図表 84　端末への EDR 導入について（Q63）



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。

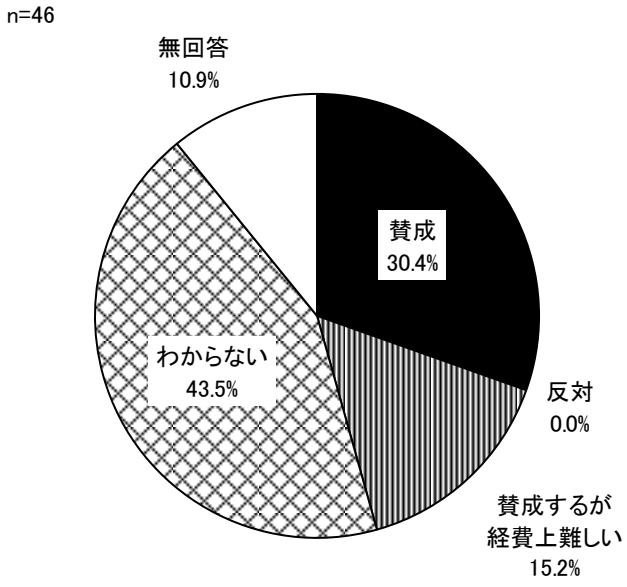
図表 85　内部ネットワークを監視することについて（Q64）



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）

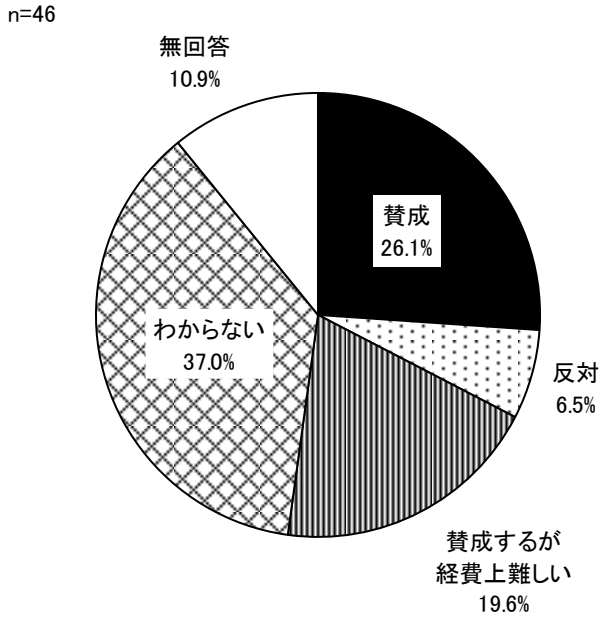


(7)サイバーセキュリティ対策への意見

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。

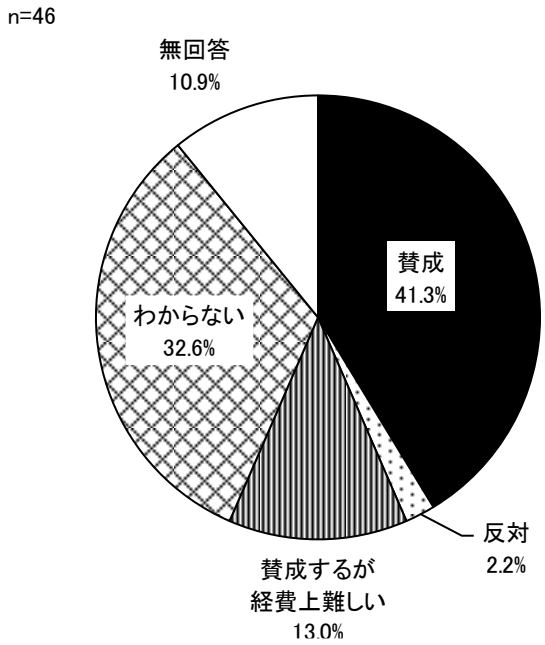
図表 87　端末からサーバーを守るためのシンクライアント基盤の導入（Q66）



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。

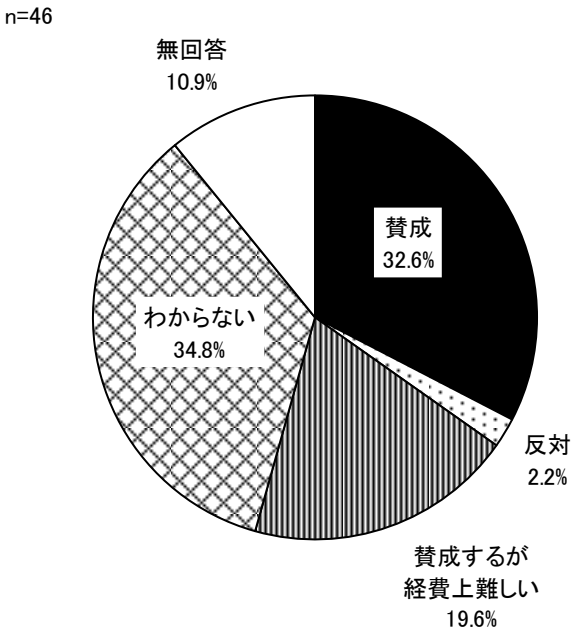
図表 88　仮想ブラウザ（ホームページ、Web メール参照用の仮想サーバーを用意）経由のインターネット参照（Q67）



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。

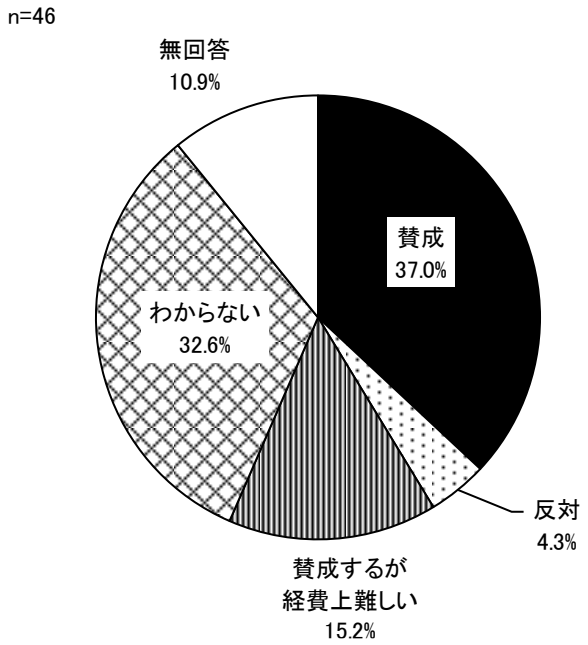
図表 89　組織内のサーバー（ハード系）を仮想サーバー、仮想ストレージ、仮想ネットワーク等を用いて病院あるいは委託契約にて統一的に導入管理を行う（Q68）



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）

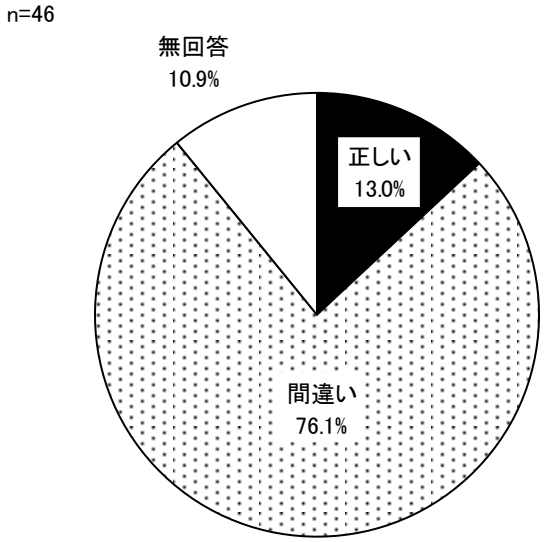


（8）最近のサイバー攻撃に対する理解度

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。

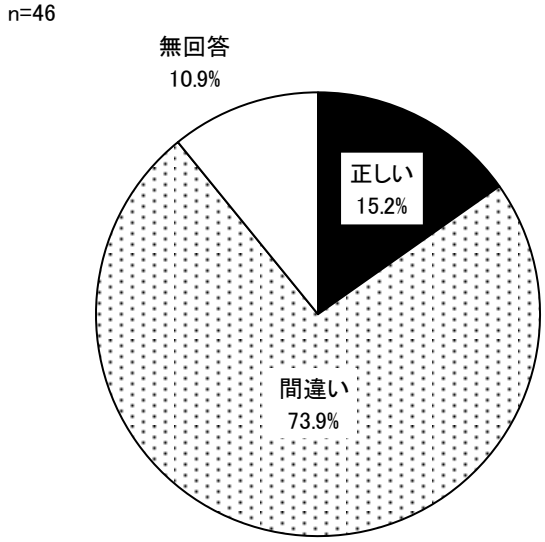
図表91　「データを暗号化されたPC、サーバーに必ずウイルスは見つかる」（Q70）



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。

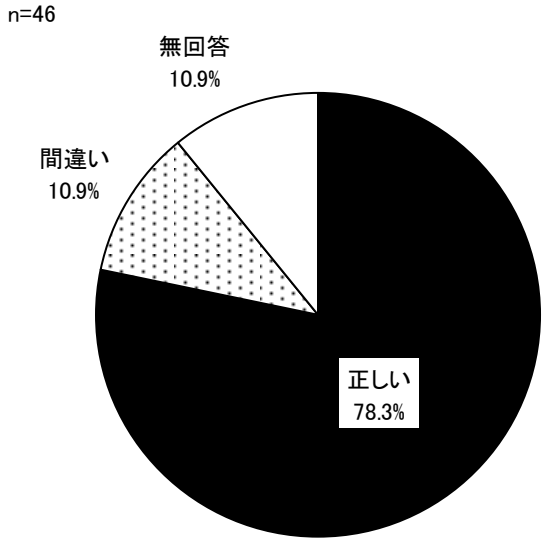
図表 92　「A さんからウイルス添付メールが届いた場合、A さんの PC はコンピュータウイルスに感染している」(Q71)



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。

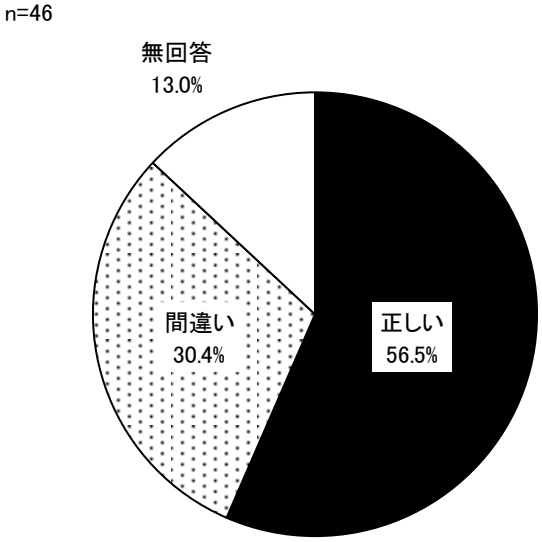
図表 93　「Windows のアクティブディレクトリやバックアップの設定ファイルは攻撃される」(Q72)



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。

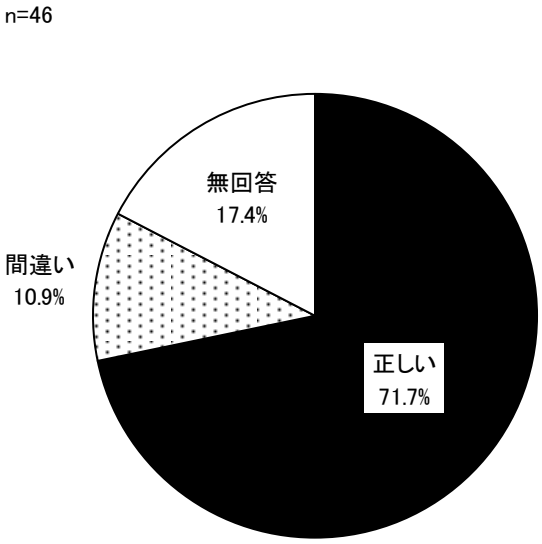
図表 94　「大容量のファイル全体の暗号化は時間がかかるので一部の暗号化をするものもある」(Q73)



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。

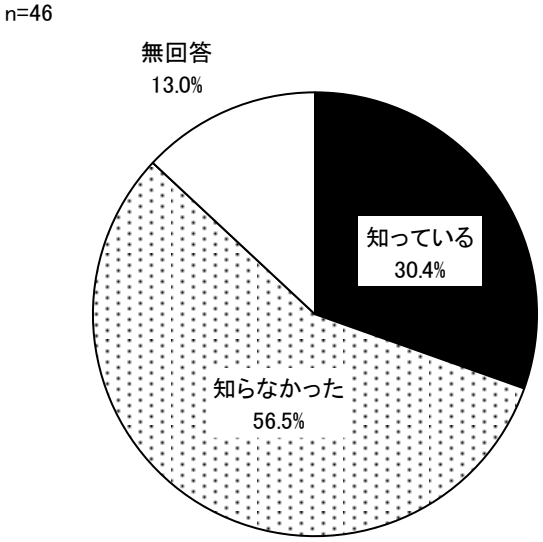
図表 95　「攻撃を受けた場合に IPA、NISC に対応、助言する窓口がある」(Q74)



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。

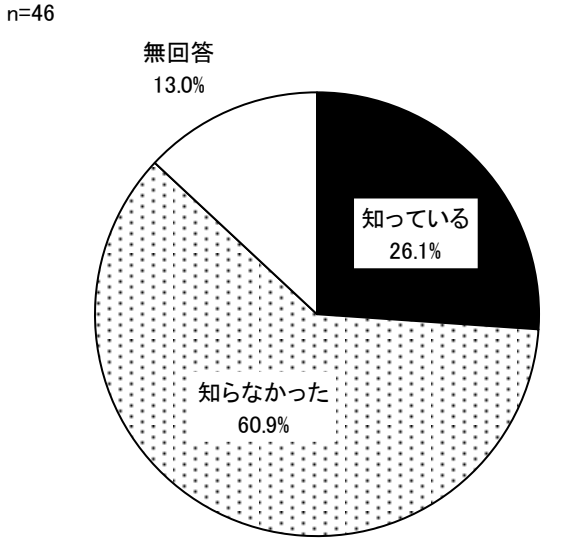
図表 96　「NISC の 3、2、1 ルールでは 3 つのデータ、2 つにバックアップ、1 つのオフラインバックアップが提唱されている」(Q75)



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。

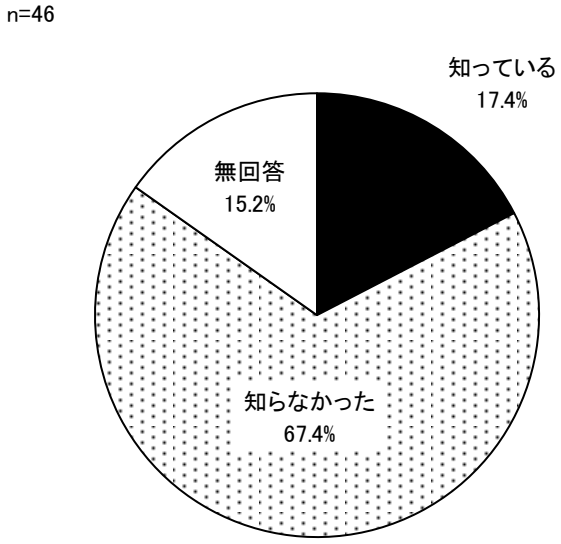
図表 97　「NICT のサイバーセキュリティ研究所のデータでは IoT 機器の攻撃が半数以上である」（Q76）



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。

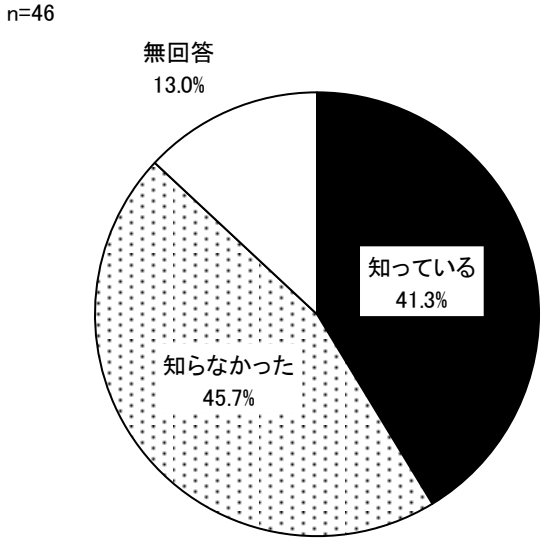
図表 98　「国際医療機器規制当局フォーラム文書におけるサイバー攻撃対策について」（Q77）



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)

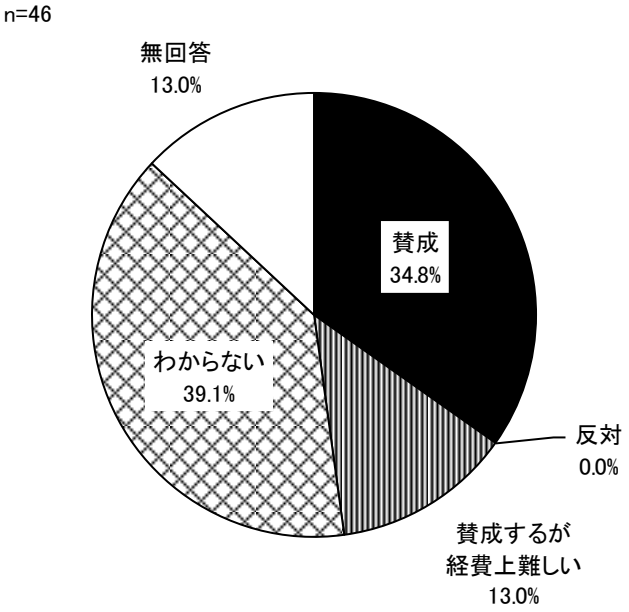


(9)重要データの保存について実施している事項

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。

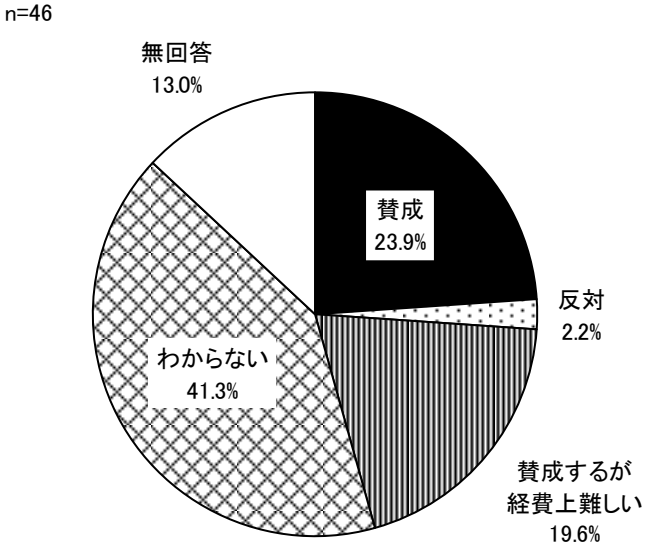
図表100　RAIDによるリアルタイムの保存（Q79）



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。

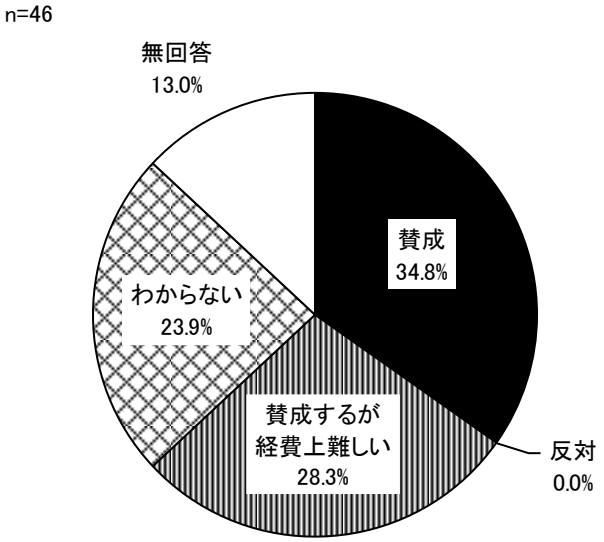
図表 101　RAID 以外にリアルタイムのバックアップを用意する（Q80）



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。

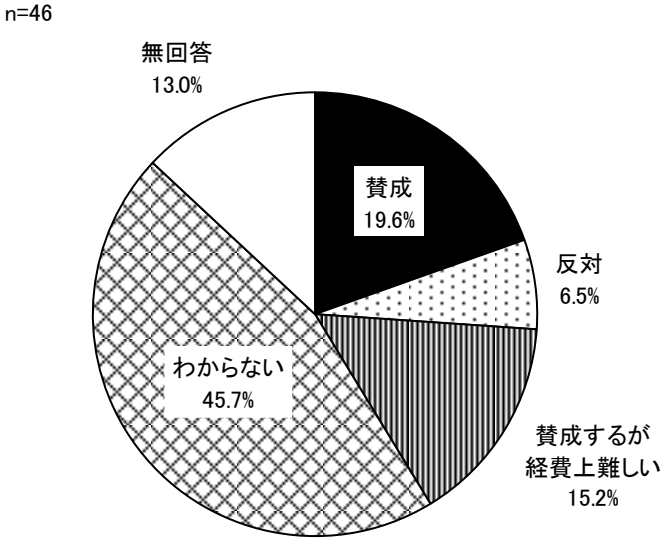
図表 102　遠隔地にリアルタイムのバックアップをする（Q81）



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。

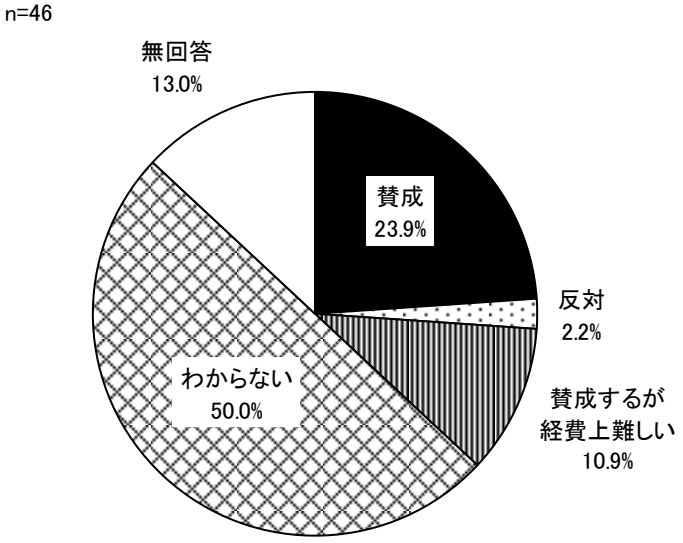
図表 103　ジュークボックス型の磁気テープユニットによる日々のバックアップ（Q82）



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。

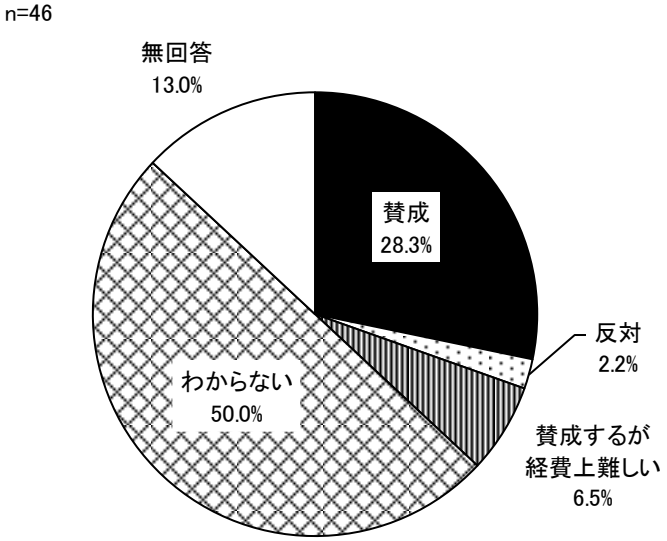
図表 104　SS-MIX フォルダーから地域連携サーバーが pull する仕組みで地域連携側にバックアップできる（Q83）



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）

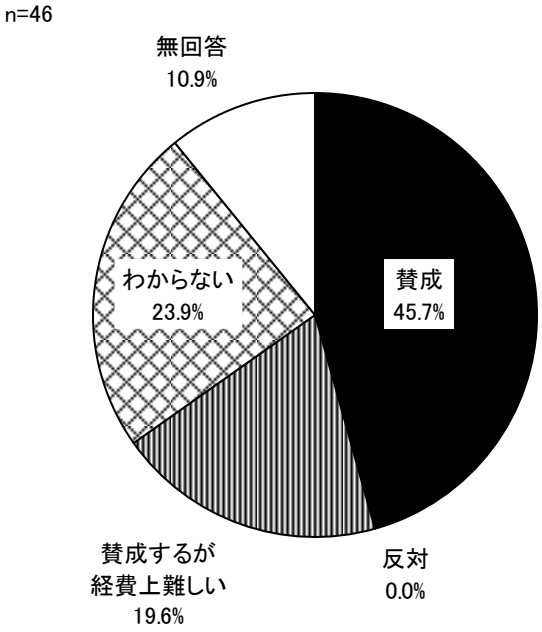


（１０）情報部門の管理について

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。

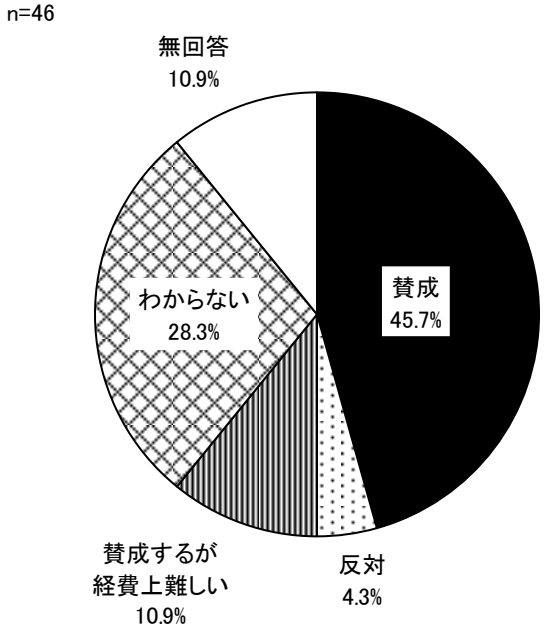
図表106　管理者のサーバー等の管理に用いるPCとメール・ホームページ参照のPCとは別の機器、別のネットワークを用いる（Q85）



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。

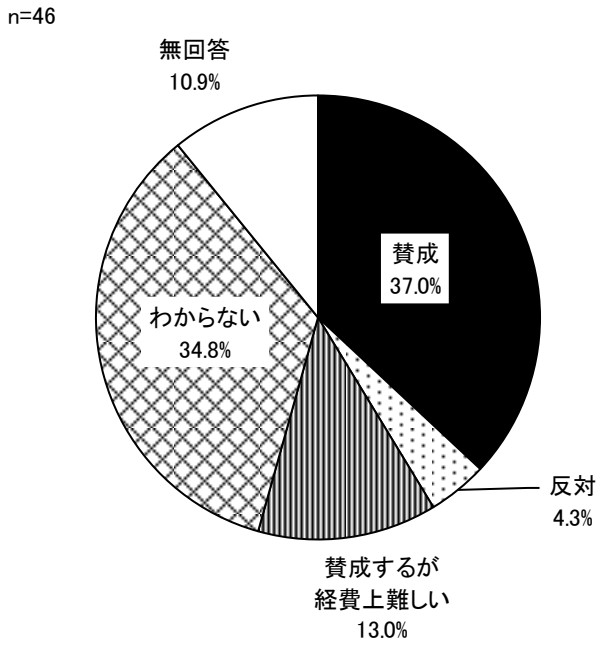
図表 107　委託業者の院外からの接続は事前に時間等を連絡させ、時間、接続先を限定する（Q86）



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。

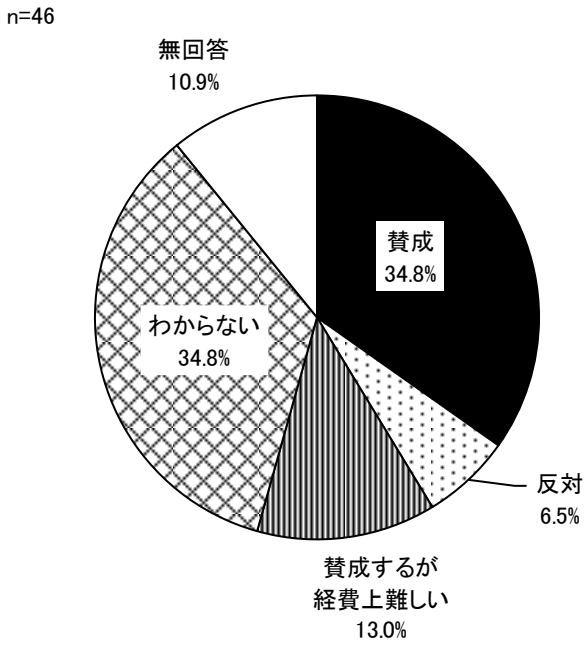
図表 108　委託業者の院外からの接続は事前に時間・接続先等を連絡させファイアウォールの接続を制限する（Q87）



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。

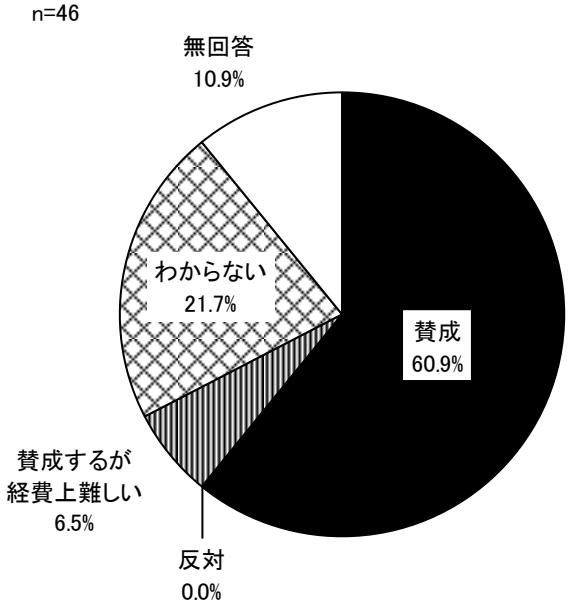
図表 109　委託業者の院外からの接続はリモートアクセス、シンクライアントなどを用いて直接接続させない（Q88）



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）

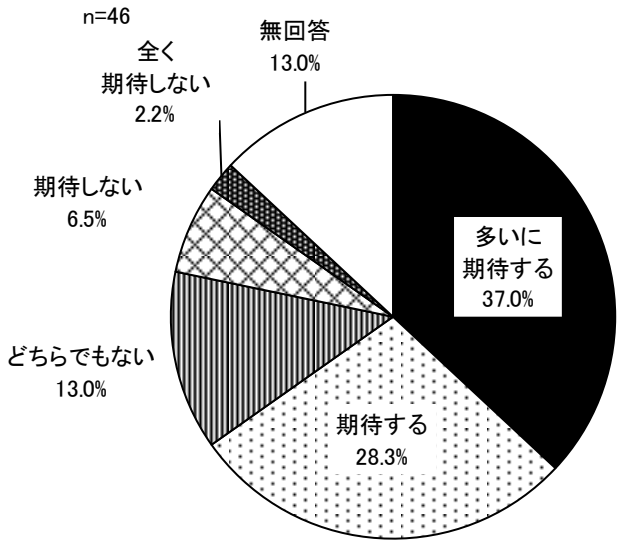


（１１）ISAC※について情報共有したい事項等　※Information Sharing and Analysis Center

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。

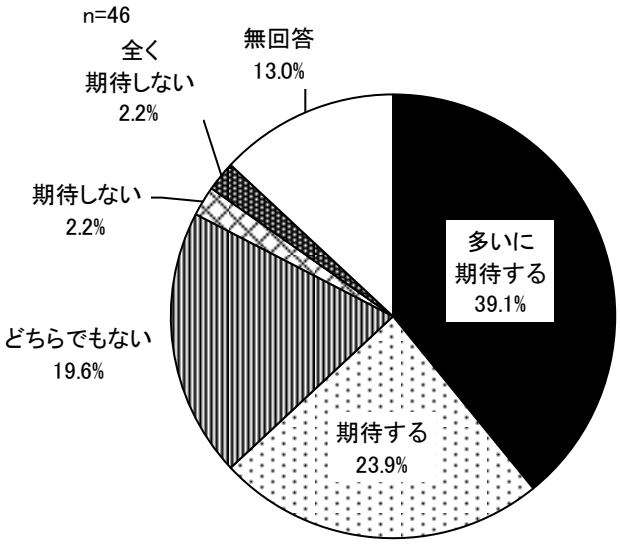
図表 111　流行しているマルウェア（ウイルス）等、リスク関連の情報（Q90）



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。

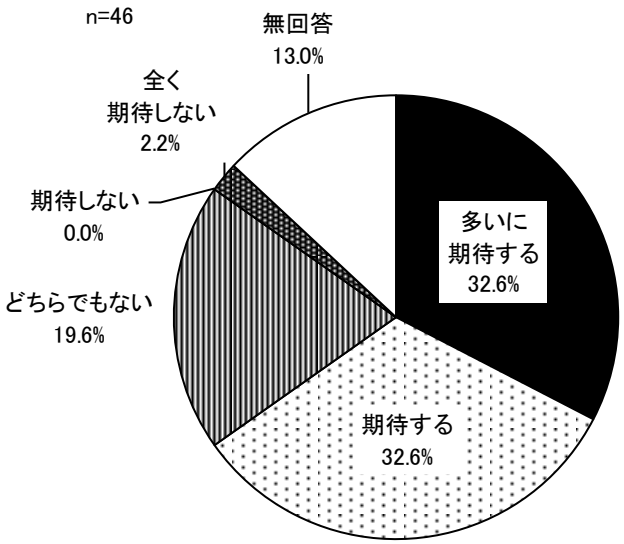
図表 112　セキュリティ対策の具体的な実施方法（Q91）



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。

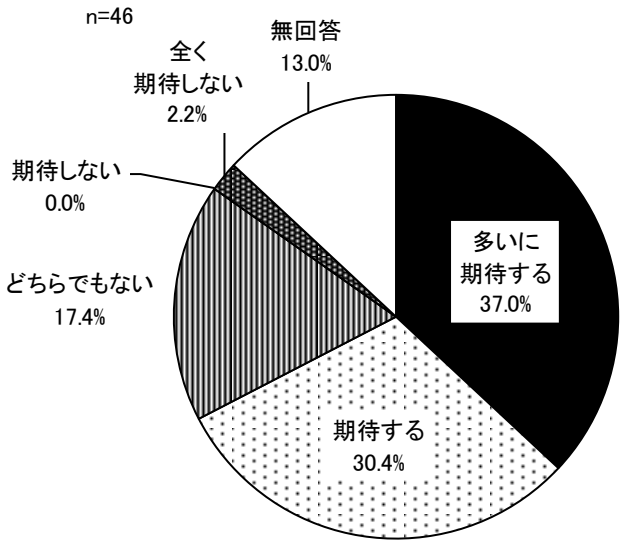
図表 113　マルウェア検体の分析（Q92）



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。

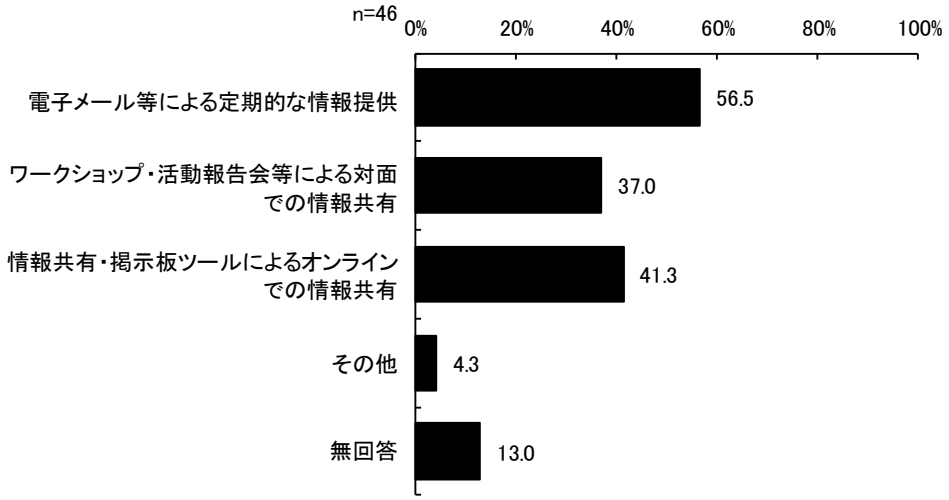
図表 114　セキュリティ教育教材の提供（Q93）



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】

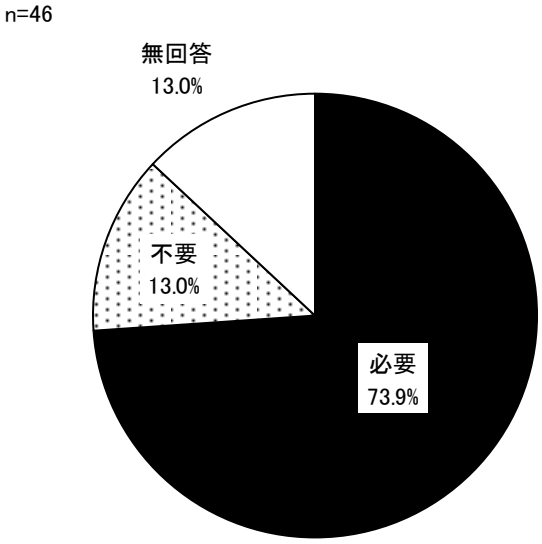


※「その他」の主な回答は以下の通り。
・SNS

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。

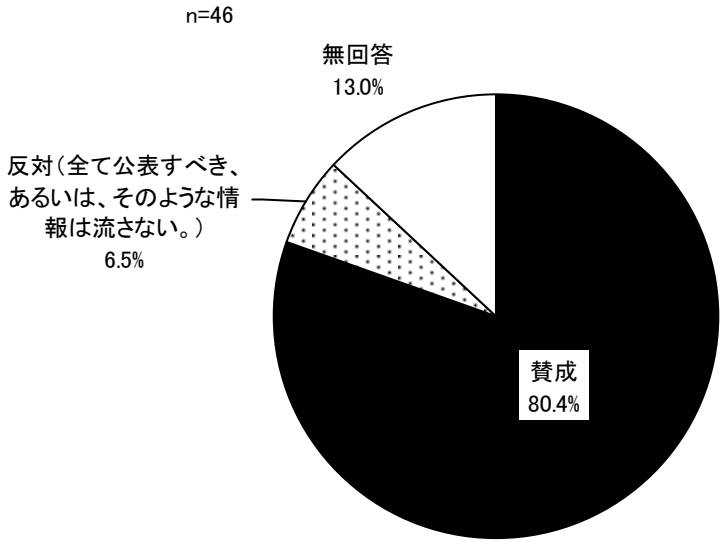
図表 116　知識レベルが同じではないので、技術的指導者が必要（Q95）



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。

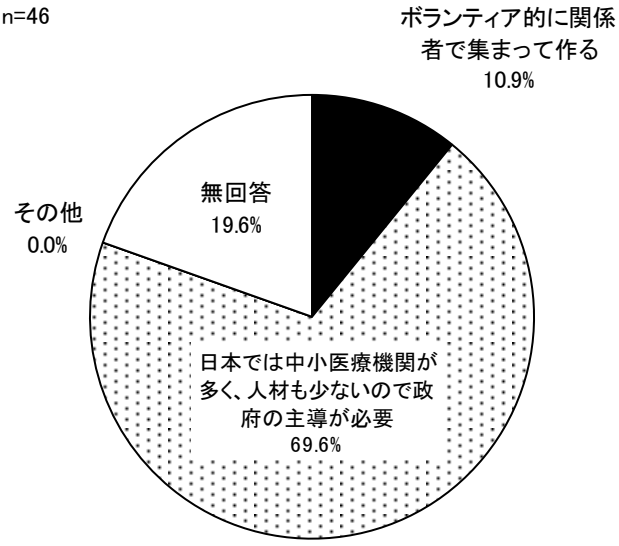
図表 117　共有するべき情報には噂、予想なども含む必要があり、公表しにくいものがあると思う（Q96）



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）



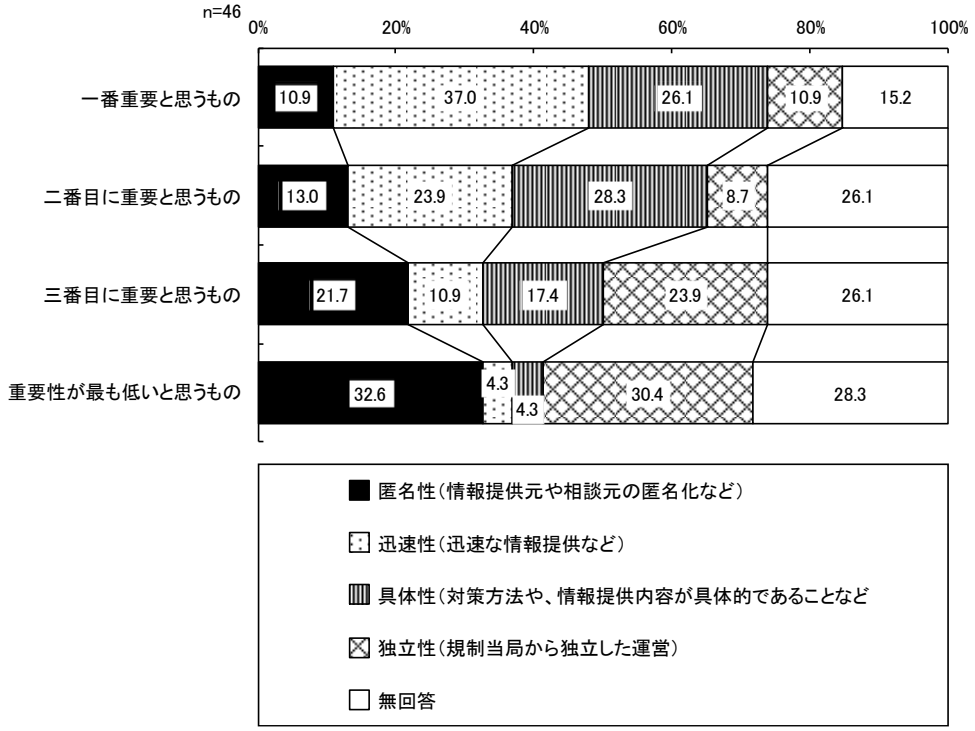
9）サイバーセキュリティ情報の公的共有組織に必要な要素の重要度

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。

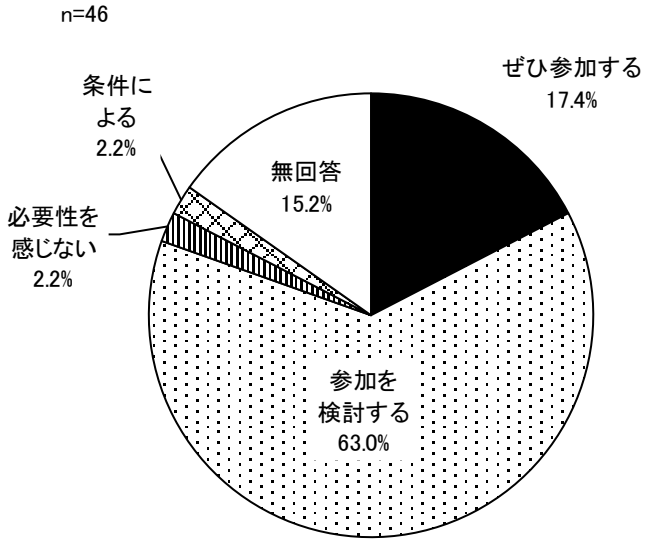
図表 119　サイバーセキュリティ情報の公的共有組織に必要な要素の重要度（Q98～Q101）



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）

令和 3 年度厚生労働行政推進調査事業費補助金（地域医療研究基盤開発推進事業）
「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」

2021年度（令和3年度）分担研究報告書

山本　隆一　（一財）医療情報システム開発センター・理事長
研究協力者：吉田真弓　（一財）医療情報システム開発センター・主任研究員

A. 研究目的

医療機関における感染拡大防止の進む現状と、今後ポスト・コロナのニュー・ノーマルとして定着する種々の遠隔システムに的確に対応し後押ししていくことができるよう、オンライン診療・遠隔医療や「非接触」を念頭に置いた ICT 化、医療機器の IoT 化が進む中で求められる医療機関のサイバーセキュリティ対策や技術について、既存のガイドライン等で各所にばらばらに記載された内容を整理・精査しつつ、医療現場の実態や最新の技術動向を踏まえたサイバーセキュリティ指針案を新たに策定することを目的とする。山本の担当部分は、サイバーセキュリティ指針案を策定するにあたって、安全管理ガイドラインの作成者としての視点からの課題提議、および患者を対象としたオンライン診療の普及と現状の把握、患者の意向や普及に当たってのセキュリティ面の課題と対応方法を見出し、厚労省の安全管理GL第 6 版の改定に向けて提言を行う。

B. 研究方法

山本は医療分野におけるガイドライン作成者の視点から、各ガイドラインの作成時の状況、その後について医療情報システム開発センターの立場から国、企業系の意見を聴取する。また、COVID-19（以下、「新型コロナウィルス」と記載）感染の影響により急速に拡がったオンライン診療等について、患者側の視点を Web アンケート調査により現状を把握し、昨年度、同様の手法で行った調査結果との比較を行い、認知度や意識の変化、傾向や課題点など洗い出しを行う。

B－1. 患者への Web アンケート調査

患者を対象としたオンライン診療に関するWebアンケート調査については、リサーチ会社（マクロミル）を利用して実施した。アンケート対象者の絞り込みは、マクロミルのモニター会員で、1年以内に特定健診など定期健康診断や歯科のメンテナンス以外で医療機関を受診し、医師等からの病状や治療に関する説明を理解できた 18 歳以上の国内在住者 1000 名程度として実施した。

質問については、医療機関において電子化が進むことに関しての意識、オンライン診療の認知・経験の有無、また、経験者のみにオンライン診療を受診した際の状況、疾患の状態（定期的な受診、急な症状等）、継続の希望や、オンライン診療への要望・必要性などを確認した。また、全員を対象としてオンライン診療への意見感触、対面受診以外の必要性などを質問した。

なお、本調査と昨年度調査の結果の比較を行うため、アンケート調査票や回答は昨年度分を踏襲し、対象者の選定条件も同じとする調査を行った。質問項目は、以下 B-2 に記す。

B－2. 質問項目

質問数は、計 30 問(マクロミルが設定しているプロファイル関連の質問、我々がスクリーニング用に設定した質問2問を除く)で、内訳は次の通り。本人の生活環境(居住環境・最寄りの医療機関へのアクセス)や受診の頻度、マイナンバーカードの取得やスマホ所持の有無などの基本情報 8 問、医療機関の ICT 化に関する質問1項目(8問)、オンライン診療に関する質問、オンライン診療の認知や経験、受診した感想、希望、意見など21問、計 30 問。

なお、オンライン診療の実施の感触や実施した課題などは経験者のみに質問を行ったが、オンライン診療を知らない患者に対しても細かく解説を行った上で、全回答者に対してオンライン診療の必要性やあり方を尋ねた。

＜基本情報関連質問～マクロミルデフォルト設定～＞　計9問
1. 性別　2. 年齢　3. 居住地　4. 婚姻状況　5. 子供の有無　6. 世代年収　7. 個人年収
8. 職業　9. 学生区分(8で「学生」を選択した場合のみ)

＜スクリーニング質問＞　計2問
1.　1年以内に医療機関を受診したか。(歯科のクリーニングや健康診断などを除く。オンライン診療、外来診療、訪問診療など、受診の形態は問わない。)
2.　受診した際に自身の病状や治療に関して医師や看護師からの説明を理解できたか。
(上記2問ともに「はい」を選択した人が、以下のアンケートの回答者対象となる。)

＜基本情報関連質問＞Q1～Q8　計8問
Q1. 生活状況(同居家族や独居など)　**Q2.** 医療機関の受診頻度
Q3. 最寄りの医療機関へのアクセス方法(交通手段、時間など)
Q4. 受診中もしくは受診した診療科　**Q5.** 手術歴の有無(過去2年以内)
Q6. スマートフォンの所持　**Q7.** 自身のマイナンバーカードの取得状況
Q8. マイナンバーカードの非取得(非申請)の理由

＜医療の ICT 化に関する質問＞Q9(q1～q8)　計1問
Q9. 以下の8項目(q1～q8)について、「そう思う」「そう思わない」「どちらでもない」で回答。
q1. ワクチン開発等に使えるよう、診療情報の電子化を進めてほしい。
q2. スマートフォンに PHR の機能を持たせて自分の過去の予防接種履歴や、受診時の検査結果データを蓄積した上で、将来の手術や緊急時に利用できることが必要だ。
q3. 医療機関で持つカルテ情報は非常に重要な個人情報であり、現状の医療機関の体制のままで電子化が進むのにはセキュリティ面で不安だ。
q4. 医療機関で電子カルテを導入したりシステムの電子化が進んでいるのであれば、電子データの取り扱いについては、特に HP や院内掲示などで丁寧に説明が必要だ。
q5. 医療機関を選択する基準には、電子化が進んでいることは必要だ。
q6. 医療機関を選択する際に、口コミのサイトを参考に選ぶ。
q7. マイナンバーカードやスマホが健康保険証やお薬手帳の代わりとして利用できるのは便利だし利用した

い。
q8. マイナンバーカードやスマホが健康保険証やお薬手帳の代わりとして利用するのはセキュリティ面での不安がある。

＜オンライン診療に関する質問＞　Q10～Q30　計21問
Q10.オンライン診療の認知
　以下の質問は、回答について、対象者を限定する場合も含む。
　対象者を限定した場合は、冒頭に＊を付与。何もない場合は全員が対象。
＊Q11.（Q10 で知っていると回答した人のみ）オンライン診療の経験
＊Q12.（Q11 で経験ありと回答した人のみ）オンライン診療を受けた医療機関
＊Q13.病状・症状　　**Q14.** 症状の程度（急病や急変、または定期的受診）
＊Q15. 自身の環境（自宅・職場等）　**＊Q16.** 立会いの有無
＊Q17. 本人確認の方法（医師→患者）　**＊Q18.** 利用した端末や機器の種類
＊Q19. 利用した機器や端末のセキュリティ面の措置（ウィルスソフトやパッチ適用等）
＊Q20. オンライン診療を受けた理由　**＊Q21.**頻度　**＊Q22.**満足・不満足度
＊Q23. 感想　**＊Q24.** 今後の継続希望　　**＊Q25.** Q24回答の理由
Q26.（オンライン診療の説明を読み理解した上で）オンライン診療での受診の希望
＊Q27.（Q26 で「受けたくない」と回答した人のみ）その理由
＊Q28.（Q12 でのオンライン診療未経験者が対象）オンライン診療を受けていない、もしくは望まない理由
Q29. オンライン診療の必要性（対面診療以外が必要か）
Q30. オンライン診療と対面診療に関する考え

<u>倫理面への配慮</u>
　本研究は、リサーチ会社を利用して Web アンケートを実施しており、対象者すべてにアンケート回答時に同意取得を行っている。また、アンケートにおいて氏名や生年月日等の個人を特定されるような質問はなく、結果に対しても個人を特定する行為は行わない。そのため、倫理面の問題がないと判断した。

C.　研究結果
1. アンケート結果概要
　2022 年 3 月 28 日～29 日に調査を実施し、その結果を以下に概要を記載した上で、本報告書の後半に結果グラフを載せる。

1-2. 回答者プロファイル
　回答者数は 1111 名、回答者の年齢は、18 歳以上で、最高年齢が 85 歳。年齢 10 歳区切りで最も多い年齢層が 50 歳代 25.3%、40 歳代 22.9%、60 歳代 18.5%、30 歳代、70 歳代、20 歳代 7.7%の順だった。なお、18・19 歳が 1.1%、80 歳以上が 0.5%で実数にして 6 名だった。
居住地は、東京都が最も多く 14.3%で、続いて大阪府が 9.7%、神奈川県、千葉県、愛知県の順で多かった。

婚姻状況に関しては、既婚が多く 64.8%、子供の有無については、子供有が 58.7%だった。世帯年収では、400 万～600 万円が最も多く 20.3%、続いて 600 万～800 万円で 17.2%、200 万～400 万円が 16.8%で、職業は会社員（事務系、技術系、その他）が最も多く 41.1%、続いて、無職 15.4%、専業主婦（主夫）14.3%、パートアルバイトが 13.0% の順だった。
生活の状況は、配偶者と子供との同居が 33.9%で最も多く、配偶者との同居が 28.1%、独居が 16.9%、両親との同居が 13.0% という結果だった。

1-3. 回答者の受診頻度やマイナンバーカードの所持について

医療機関への受診の頻度は、月に1, 2回が最も多く 37.9%、2.3 か月に1回が 30.8%、半年に1回が 14.9%、年1回が 10.4%で、最寄りの医療機関（かかりつけの医療機関）へのアクセス環境については、「車で 30 分未満」が最も多く 37.3%、続いて多いのが「徒歩で 15 分未満」で 35.5%だった。
受診しているもしくは、受診した医療機関の診療科（複数回答）は、内科が多く 54.8%，歯科が 30%，皮膚科 19.1%，眼科が 18.8%、整形外科、婦人科、泌尿器科、循環器内科、心療内科、精神科の順で多かった。2年以内の手術歴では、有が 10.8%，無が 88.4%だった。スマホの所有ありは 94.6%。マイナンバーカードの所有あり（申請済で受取待ちを含め）が 68.1%。マイナンバーカードを持っていない人（n=338）にその理由を尋ねると「交付手続きが面倒だから」が最も多く 27.2%で、「用途がない、使い道が分からない」20.4%，「近々申請予定」が 17.8%、「自身の個人情報の漏洩が怖い」が 16.9%だった。

1-4. 医療機関での電子化について

医療機関での電子化が進むことについては、8項目のうち、「電子カルテやオンライン診療システムを導入している場合は、患者がちゃんと理解できるように、HP や院内掲示で説明が必要である」が「そう思う」という意見が 63%で、他の項目（PHR の推進や、マイナンバーカードの診察券としての利用の推進、スマホでの受診予約やリマインドなど医療機関での電子化対応）と比較すると、関心の高さが見られた。

1-5. オンライン診療に関する認知と経験

オンライン診療を知っているかは、最も多いのが「名前は知っているが内容をよく知らない」53.4%で、オンライン診療を知っている人が 41.3%、聞いたことがないが、5.3%。オンライン診療を知っている人（n=459）に、オンライン診療の経験の有無を聞いたところ、オンライン診療の経験があるが 13.1% （60 名）だった。

1-6. オンライン診療での症状や状況

オンライン診療の受診経験者（60 名）に、オンライン診療の受診先を尋ねたところ、71.7%（43 名）が「かかりつけの医療機関」と回答し、「初めての医療機関（インターネット等で検索）」が 16.7%（10 名）、「初診の医療機関で、かかりつけ医や関連の医療機関」が 8.3%（5 名）、「過去に受診した医療機関（オンライン受診では初めて）」が 3.3%（2 名）だった。オンライン診療を受診した際の症状は、発熱が最も多く 31.7%（19 名）、咳や喉の痛みが 13.3% （8 名）、身体のだるさ・不調が 18.3%（11 名）の順で多かった。その他が 16 名で、内訳は低用量ピルの処方、持病の定期検診、泌尿器科や ED,皮膚疾患の処方等での受診だった。その時の症状の現れ方（n=60）は、急な症状が 53.3%、定期的な受診で自身がオンライン診療を希望が 40%、

定期的な受診で主治医等に勧められたが 5%。オンライン診療の受診の自身の場所は、自宅が最も多く 98.3%(59 名)、入院施設で、1.7% (1 名)。立会い等の有無は、本人のみが最も多く 86.7%(52 名)、家族や友人の同席が 13.3%(8 名)。

オンライン診療の際の患者本人確認(n=60)については、「かかりつけ医のため、顔の確認のみ」が最も多く 40%(24 名)、「診察券番号もしくは健康保険証の番号を口頭で伝えた」が 25%(15 名)で次に多かった。オンライン診療で患者が利用した端末については、自身のスマホ・タブレット」が 66.7%(40 名)、「自身のPC」が 23.3% (14 名)、「電話・テレビ電話」が 8.3%(5 名)だった。その端末へのセキュリティ面の措置については(複数回答)、OS のセキュリティパッチの適用(月次アップデート実施や Windows Defender の更新)が最も多く 73.3% (44 名)、「ドコモ光など光回線を自宅や職場で契約して利用している。」が 25% (15 名)、「ウィルスソフトを購入しインストールしている」 23.3% (14 名)が続いて多かった。他に「TV 電話で何もしていない」は 8.3%(5 名)、「家族等に任せていてわからない」「公共施設や駅などで無料の無線 LAN を使っている」が同数で 1.7%(1 名)だった。

オンライン診療を受けた理由は、「新型コロナウィルスの感染拡大で外来受診の不安があった」「通院する医療機関での勧め」が同数で、33.3%(20 名)で最も多く、オンライン診療が便利なので(通院の手間や時間短縮)も 16.7.% (10 名) だった。また、興味があったから(ニュースや新聞などの話題)も 8.3% (5 名) あった。

オンライン診療を受けた回数は、初診で1回が 48.3% (29 名)、過去に1・2回(緊急時対応)が 26.7.% (16 名)で、毎月～3か月に1度の定期的受診が 15%(9 名)、毎回(検査や注射以外の受診)も 8.3%(5 名)いた。オンライン診療を受けた感想で、「満足」「多少問題はあったが満足した」を併せて満足という好意的な意見が 96.7%(58 名)で、オンライン診療の経験者のほとんどが好意的な意見だった。

また、具体的な感想について(複数回答)は、安心して診察が受けられたが 68.3%(41 名)、「医師等の説明が聞き取れない、もしくは疾患の状態を見せたり伝えたりできなかった。」が 23.3%(14 名)、接続や機器操作に手間取ったが 3.3%(2 名)、自宅などの接続環境や操作方法がうまくいかなかった」が 5.0%(3 名)で、オンライン診療特有の課題点も見られた。

今後のオンライン診療の継続については、場合によっては受けたいを含め、「今度も継続して受けたい」が 91.7%(55 名)だった。具体的な理由や条件としては、「検査以外はオンライン診療を受けたい」が 60% (33 名)、「新型コロナウィルの感染拡大によってはオンライン診療を受けたい」が 21.8%(12 名)、「自分でオンライン診療と通院を選択したい」「オンライン診療の医療機関が増えれば」「受診料が安くなれば」は各々 5.5% (3 名)で少なかった。

1-7. オンライン診療と対面受診への意識

オンライン診療を知っていて、受けたことがない回答者(n=399)に、その理由を確認したところ、「通院先がオンライン診療に未対応だから」が最も多く 46.1% (184 名)、「対面での診療を希望するため」が 22.6%(90 名)、「検査等で対面でないと対応不可のため」が 15.8%だった。

最後に全回答者(n=1111)に、対面診療以外に、オンライン診療が必要かどうかを確認した。オンライン診療も必要とする意見が 55.3%で、オンライン診療は不要とする意見は 18.5%だった。

同様に全回答者にオンライン診療と対面診療についての意見を尋ねた(n=1111)。「オンライン診療は不要(対面診療が基本)」が 8.3%で、近年の新型コロナの蔓延など緊急事態の場合、もしくは通常時から本人が

選択するを含め、「オンライン診療が必要」という意見は 80.4%だった。また、「オンライン診療の環境を国や自治体が整えたうえでオンライン診療が必要」という意見は 10.2.%だった。

2. 結果のまとめ

本調査は、割付はせずランダムな調査依頼ではあるものの、回答者は満遍なくどの年代も含まれており、年代の構成は 50 歳代が最も多く回答者の約 25%で、60 歳代も約 19%だった。回答者の職業は会社員が半数を占め、無職や学生が約 17%、専業主婦(主夫)が約 3 割。

生活状況は、独居が約 17%で、それ以外は同居者有であった。回答者の 75%が少なくとも3か月に1度以上は受診しており、週に1回以上の受診も5%程度であった。最寄りの医療機関へのアクセスは、半数が徒歩で 30 分以内にアクセス可能で、4割が車や公共交通機関を使い 30 分以内でアクセスが可能で、殆どの回答者が概ね 30 分以内に医療機関へのアクセスが可能であった。

医療機関の電子化の推進については安全面を危惧するような意見や否定的な意見は多くはないが、他の項目と比較して「医療機関に求める」とする回答が多かったものが、「安全管理についてはHPや院内掲示で丁寧に患者への理解を得られるような対応をするべき」という項目であった。

オンライン診療は、ほとんどの人が新聞やニュース報道で見聞きしていたが、内容まで理解しているのは約 41%だった。そのうち実際にオンライン診療を経験した人が約 13%、実数で60名だった。

オンライン診療の受診時の症状は、急な症状が約 53%で、定期的な受診が 45%だった。オンライン診療を受けた場所は医療機関や介護施設が 1 名で、残り全員が「自宅」だった。立会者なし自身のみが約 87%だった。オンライン診療に利用した端末は約 67%がスマホやタブレット、約 23%が PC で、セキュリティの措置については、TV 電話なので何もしていないが約8%で、約 73%が OS のアップデート等の基本的な措置は行っており、ウィルスソフトを購入して利用している人も約 23%だった。オンライン診療を受けた回数は、初診でオンライン診療を受けた人が約 48%、対面受診が出来なかったので過去に1, 2回が約 28%。定期的に受けている人は約 23%だった。

満足度については、オンライン診療を受けた人の殆どが受けた診療に満足し、7割弱が安心して診療を受けることができたと回答した。しかし、自身の症状の説明や傷病の状態を上手く映せなかった、または自身の接続環境や機器操作に問題があったなどが4割程度、オンライン故の問題点があり、この点は患者側の経験値の部分が大きいが、「処方箋の発行や送付に時間を要した」が 5%で、今後は、医療機関内の手順やシステム上の課題の検討、患者が増えた場合への対応など課題も見られた。しかし、いくつかの課題点は見られるものの、オンライン診療の経験者の殆どがオンライン診療の継続を望んでいた。

また、全体の回答者の中でオンライン診療の内容を知らないと回答した 652 名の人の内、約4割がオンライン診療を受けたいと思わないと回答し、理由としては8割がオンラインで診察や処置に不安があると回答していた。

オンライン診療の未経験者 399 名は、その未経験の理由として 6 割が自身の疾病や処置の方法、受診する医療機関でのオンライン診療に未対応だからといった、本人の意見や希望とは無関係の理由で受けられない状況であり、オンライン診療そのものを否定した意見は約 23%であった。

回答者全体のオンライン診療の受け止め方は、回答者の殆どが、医療サービスの選択肢の1つとして誰でもオンライン診療を受けられる環境を求めているという傾向が見られた。

3.　前回との比較

Web アンケートのため、回答者には一定のバイアスはあるが、オンライン診療や医療機関の ICT 化についての患者への調査であり、回答者の選定基準や調査方法については適切と考えた。1年前に同じ調査票を利用して実施したアンケート調査の回答者との相違点は、前回から女性が1割弱少なく、男性 55.6%、女性 44.4%で、結果として性別の割合が逆になった点で、その他の年齢階層や職業などは前回とほぼ同じ割合だった。

オンライン診療の認知率については、「知っている」が 41%で、前回結果から 1.5%ではあるが増えていた。また、オンライン診療の経験者は全回答者の5%で、でもほぼ同じ割合だが、オンライン診療を知っている人のうち経験者は、今回が 13.1%で、前回の 12.7%から僅かではあるが増えてはいた。

比較的差が見られたものは、マイナンバーカードの所持（申請済み含む）が1割近く増え 68%となった点である。また、オンライン診療の受診に関する項目では、オンライン診療を受けた切掛けが、「急な症状での受診（発熱等）」が前回から1割以上増え、経験者の半数を占めた。

また、オンライン診療を受けた場所については、前回は自宅が8割程度で職場や宿泊施設が 1 割以上あったが、今回の調査では殆どが自宅であった。また、オンライン診療に使う端末については、前回から15%増えて 67%が「自身のスマートフォンもしくはタブレット」であった。

また、オンライン診療の回数は、「初診で1回」が前回より 2 割近く増えて半数近くあった。オンライン診療を受けた感想については、「多少問題があった」が前回から 7%程度減り、「満足だった」が 10%増えて 72%であった。オンライン診療を今後も受けたいと思う人が 55 名で、前回から1割以上増えたが、継続して受けたいと思う理由としては、「検査など対面の必要がなければオンライン診療を受けたい」が前回から15%増えて 60%という結果だった。

上記に述べた以外には、1年での変化は殆ど見られず、新型コロナウィルス感染症での様々な対応や感染状況の増減、ワクチン接種完了者の増加などは、患者のオンライン診療に関する意識や受診の状況にはあまり影響はなく、意識自体は一定で、状況には左右されない傾向が見られた。

D. 考察

オンライン診療の経験者はわずかに増えており、初診での受診も昨年度と比較して多かった点は新型コロナウィルスの感染症の影響が要因と考えられる。また、オンライン診療で利用する端末も、スマートフォンやタブレットが増えたが、この点は、オンライン診療システムが少しずつ医療機関に普及し、大手のベンダーによりオンライン診療アプリが患者側に提供され、特に患者側で環境整備の必要もなく、オンライン診療を受診するにあたってのハードルが下がった点、また、新型コロナウィルス感染症の罹患者の殆どが自宅での療養となった点も関係すると考えられる。

結果に記載した通り、本調査の回答者は最低限の IT リテラシーは備えており、その上でオンライン診療を受けた経験者のため情報通信機器へのセキュリティ対策についての知識も備えていると考えられ、オンライン診療で利用した機器への対策結果でも裏付けがなされた。

しかし、今後オンライン診療に対応できる医療機関が増え、オンライン診療がもっと身近な存在となった場合に、患者はタブレットやスマホで気軽に接続が可能である半面、やはりセキュリティ面での措置も疎かになる可能性が高く、今後はこれらの通信機器も攻撃の対象ともなり得る。

患者側は年齢、生活環境等様々で、患者の通信機器に対して一律に適切な措置を求めることは難しいた

め、オンライン診療で利用する医療機器側の端末は、電子カルテシステムとは切り離すなど、医療機関側に適切な措置が必要と考えられる。

現状のオンライン診療の適切な実施に関するガイドラインではオンライン診療システムが電子カルテ等の診療情報システムに接続する場合とそうでない場合に分けて、接続する場合には医療情報システムの安全管理に関するガイドラインに準拠することを求めている。当面安全を担保するためには診療情報システムと切り離すことも対策としては有効ではあるが、今後は対面診療とオンライン診療の有機的な結合が求められることは明白で、IT リテラシーを一律には期待できない患者端末を用いるオンライン診療システムとの接続を前提にする必要がある。この場合、リスクの大部分はサイバーセキュリティであり、十分な対策が求められる。

今年3月にリリースされた医療情報システムの安全管理に関するガイドライン5.2 版は、サイバーセキュリティに関しても一定の記載があり、対応策も述べられている。しかし、ネットワークセキュリティに関しては、2007 年にレセプトオンラインの開始に際して強化されたものの、現状のクラウド化の流れや、オンライン診療の急速な普及、あるいは保険資格のオンライン確認システムの導入やそれに伴うデータヘルス集中改革で導入が進められている様々なシステムに対応可能かどうかは十分に検証されていないと考えられる。ネットワークセキュリティ、サイバーセキュリティを中心に速やかに検証を進め必要に応じた改訂を進めることが望まれる。

E.結論

オンライン診療に焦点をあててアンケート調査を行った。WEB アンケートのバイアスはあるものの、昨年度に比べて経験者はわずかに増加しており、21年度のオンライン診療指針の見直しもあり、今後は漸増するものと推測される。オンライン保険資格確認、電子処方箋、オンライン診療と様々な意味で、医療機関にとって外部ネットワークへの依存は避けがたく、サイバーセキュリティ対策の重要性はますます増加している。ただ一般に言われているサイバーセキュリティ対策は医療機関に固有のものではなく、対策も一般的に述べられていることが多い。医療機関の IT 化やネットワーク依存は進んでいるものの、IT 化自体は目的ではなく、あくまでもツールであり、また制度的に促進されたものもあり、サイバーセキュリティ対策も自らリスク分析を行う積極的対応ではなく、モデル対策をつまみ食いしている医療機関もあると思われる。安全管理ガイドライン次版では、このような医療機関の特性にも配慮し、みずからリスク分析を行う積極的対策を誘導するような工夫も必要と思われる。

F.研究発表

1. 吉田　真弓, 山本隆一, オンライン診療の普及および医療機関の電子化についての患者への意識調査研究,第 23 回日本医療情報学会春期学術大会ポスター発表, 米子市・WEB 開催, 2021 年 6 月
2. 吉田　真弓, 山本隆一, 患者への Web アンケート調査に基づいた、オンライン診療および医療機関の電子化の在り方に関する調査研究, 第41回医療情報学連合大会, 口演発表, 2021 年 11 月
3. 吉田　真弓, 患者への Web アンケート調査に基づいたオンライン診療および医療機関の電子化のあり方に関する調査研究, CPA EXPO2021-2022, 口演発表(WEB), 2022 年 2 月

＜参考１＞グラフ表示※

※人数表記がない場合は、回答者数は 1111 名（n=1111）、単一回答とする。

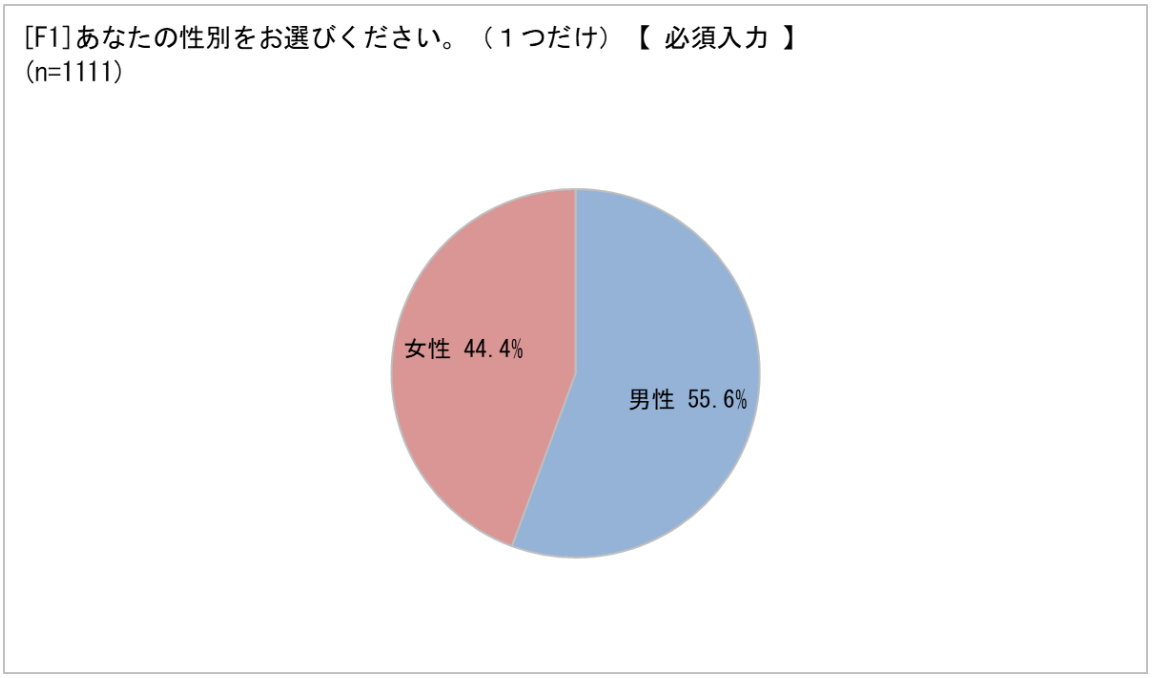


Figure1.性別

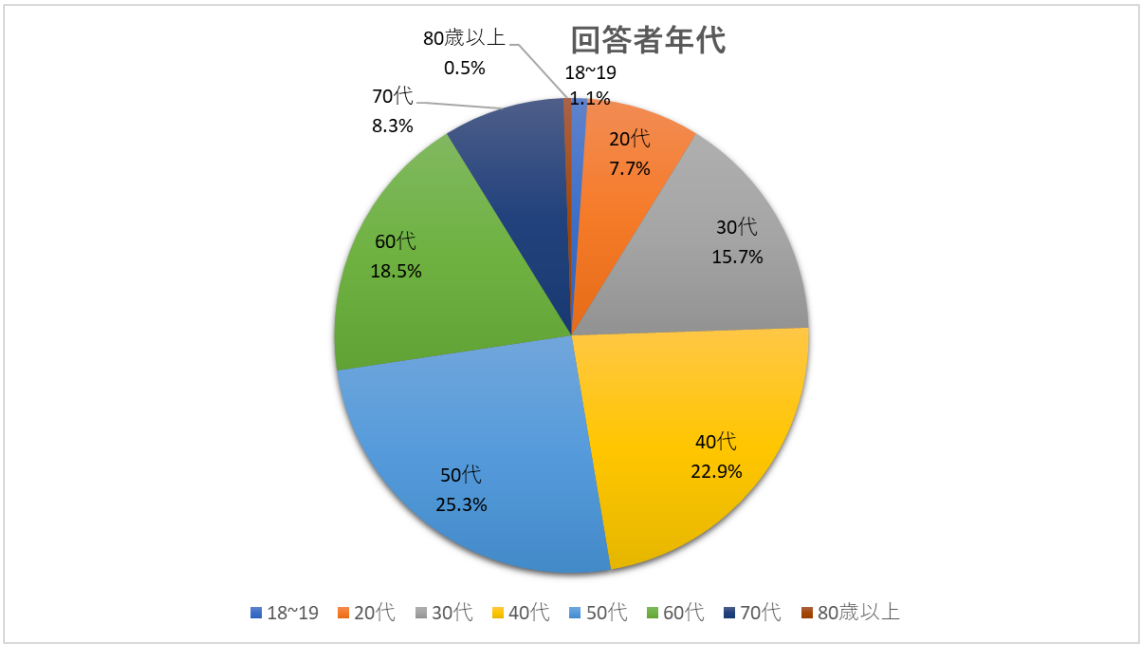


Figure2. 回答者年代別

	単一回答	%
	全体	(1111)
1	北海道	4.2
2	青森県	0.6
3	岩手県	1.0
4	宮城県	1.4
5	秋田県	0.9
6	山形県	0.9
7	福島県	0.5
8	茨城県	1.6
9	栃木県	1.4
10	群馬県	1.8
11	埼玉県	5.4
12	千葉県	6.9
13	東京都	14.3
14	神奈川県	9.3
15	新潟県	2.0
16	富山県	0.9
17	石川県	0.5
18	福井県	0.4
19	山梨県	0.4
20	長野県	1.0
21	岐阜県	1.8
22	静岡県	2.3
23	愛知県	6.3
24	三重県	1.3
25	滋賀県	0.8
26	京都府	2.1
27	大阪府	9.7
28	兵庫県	5.1
29	奈良県	1.0
30	和歌山県	0.8
31	鳥取県	0.0
32	島根県	0.4
33	岡山県	2.0
34	広島県	1.4
35	山口県	1.1

36	徳島県	0.3
37	香川県	0.5
38	愛媛県	1.4
39	高知県	0.0
40	福岡県	2.8
41	佐賀県	0.3
42	長崎県	0.8
43	熊本県	0.6
44	大分県	0.4
45	宮崎県	0.3
46	鹿児島県	0.6
47	沖縄県	0.7

Table1. 回答者居住地

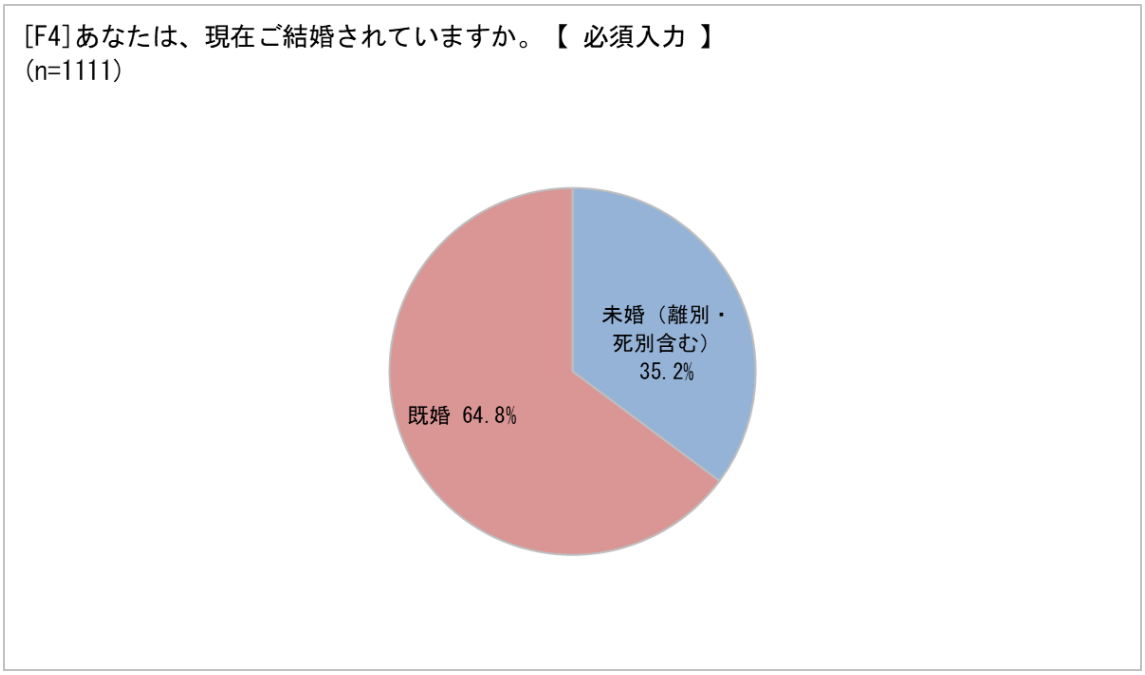


Figure3. 婚姻状況

[F5]あなたには、現在お子様がいらっしゃいますか。【 必須入力 】
(n=1111)

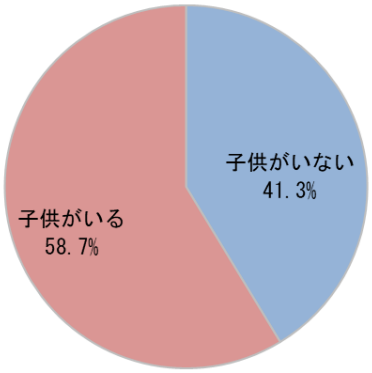


Figure4. 子供の有無

[F8]あなたの現在のご職業をお答えください。【 必須入力 】
(n=1111)

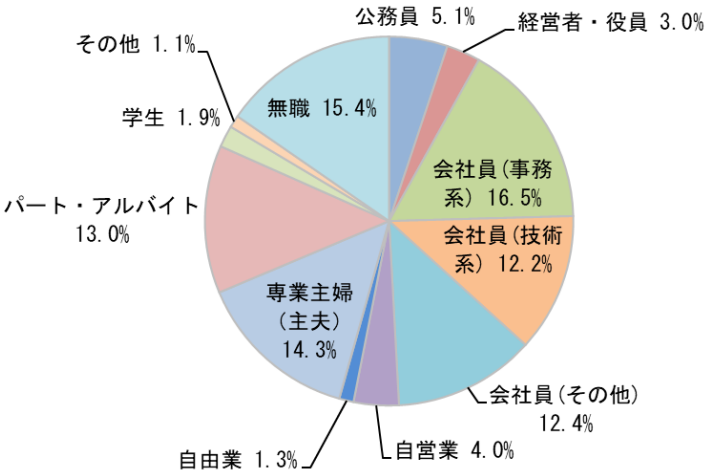


Figure5. 職業

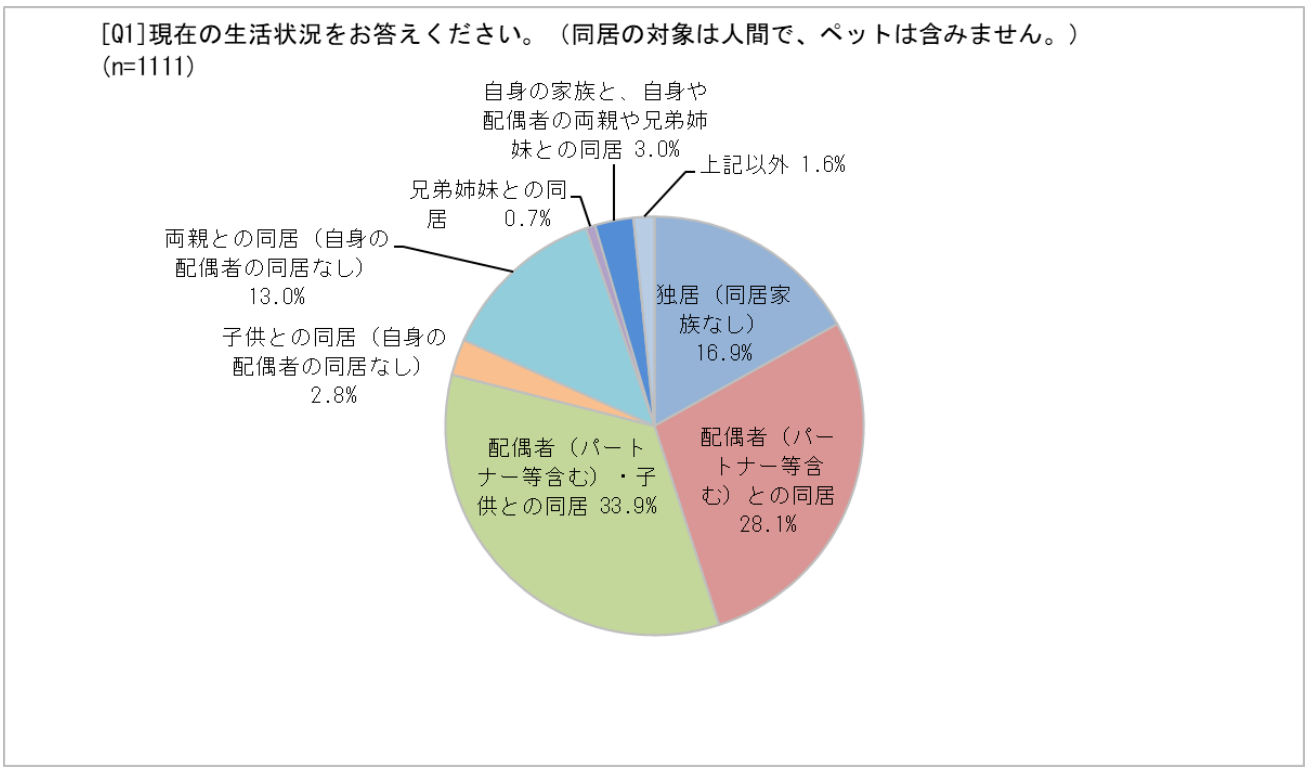


Figure6.生活状況

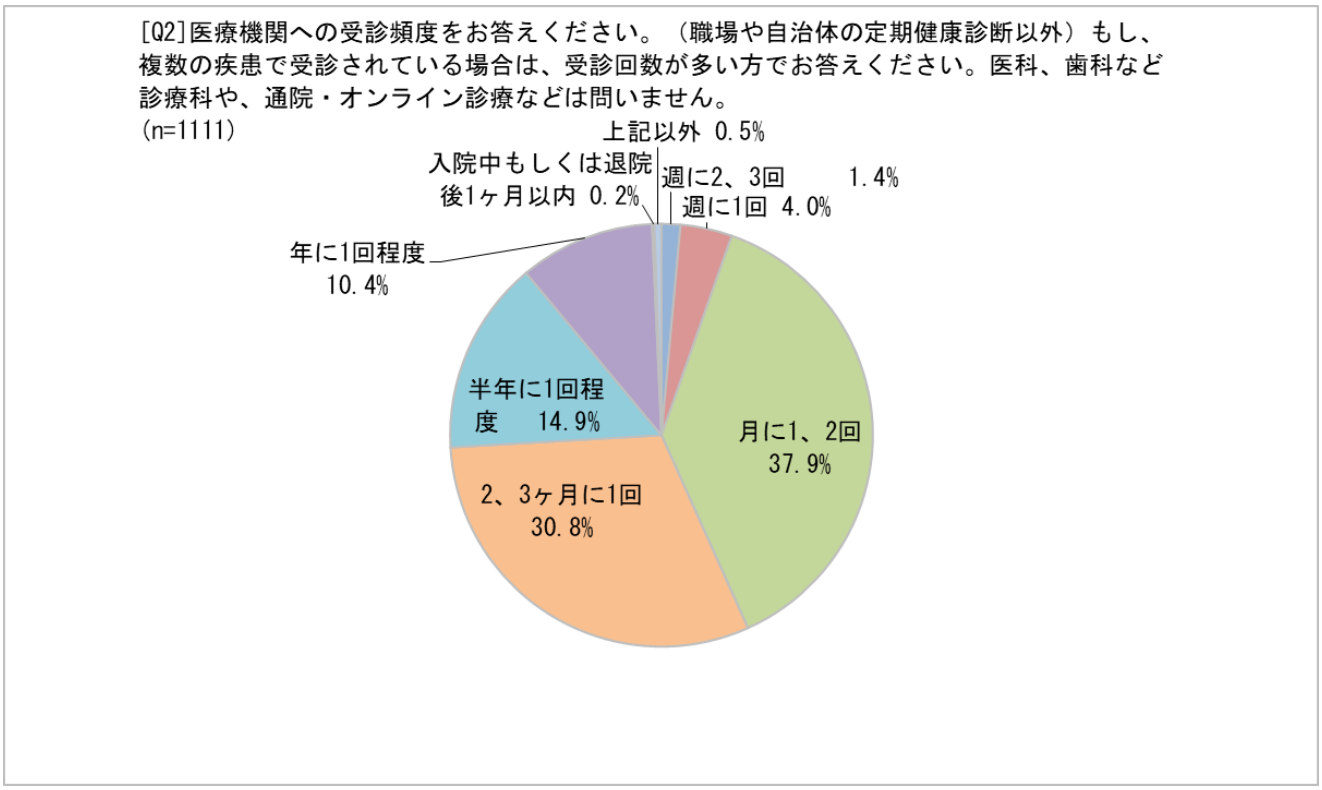


Figure7. 受診の頻度

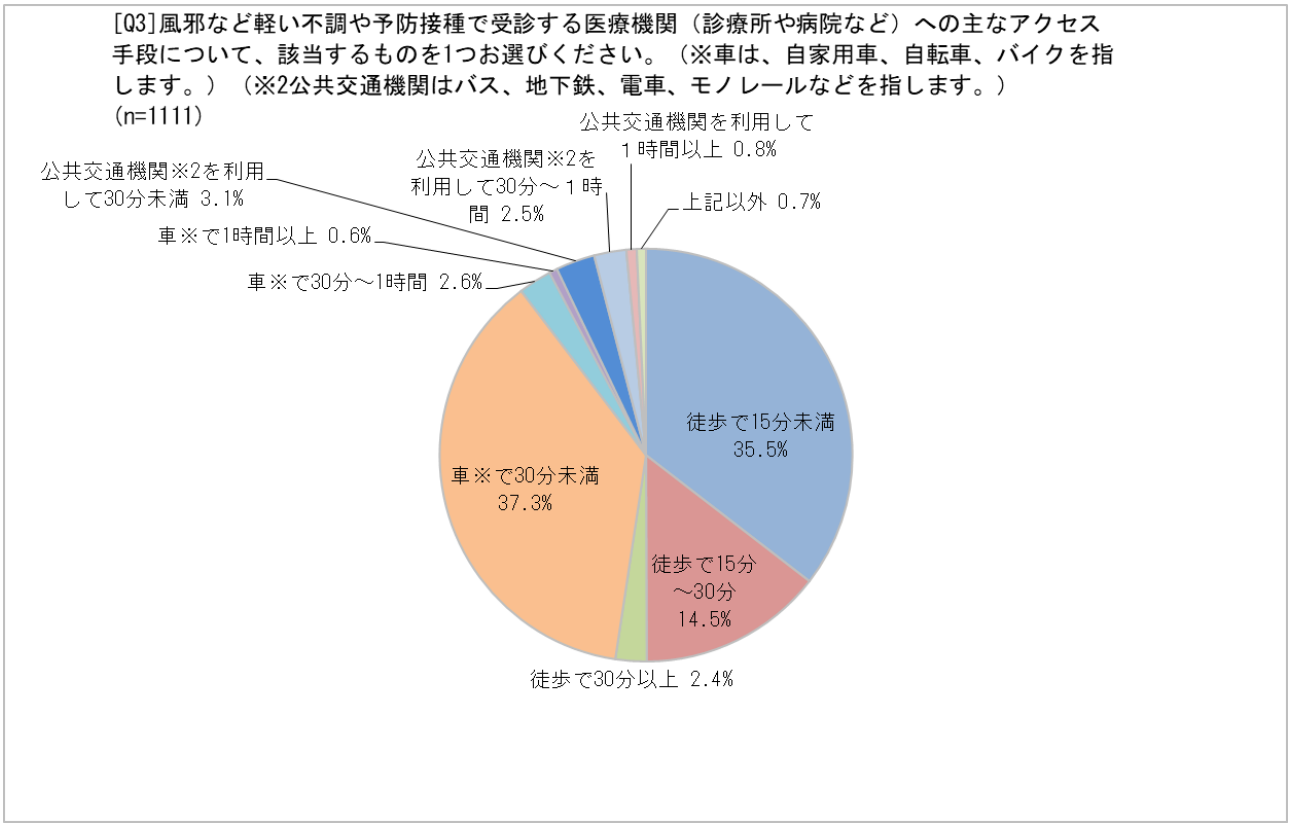


Figure8.受診する医療機関へのアクセス状況

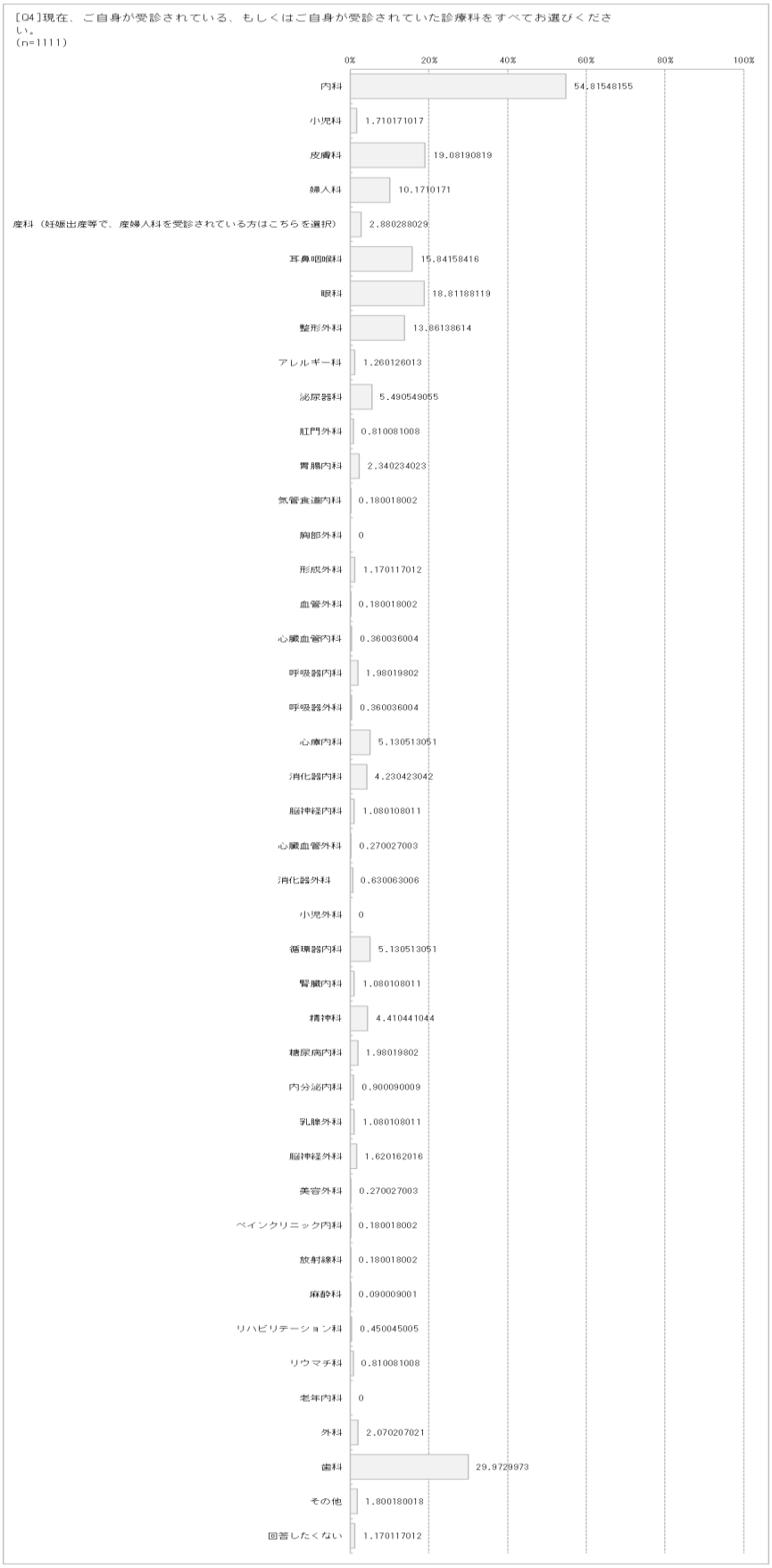


Figure9. 受診する(した)診療科（複数回答）

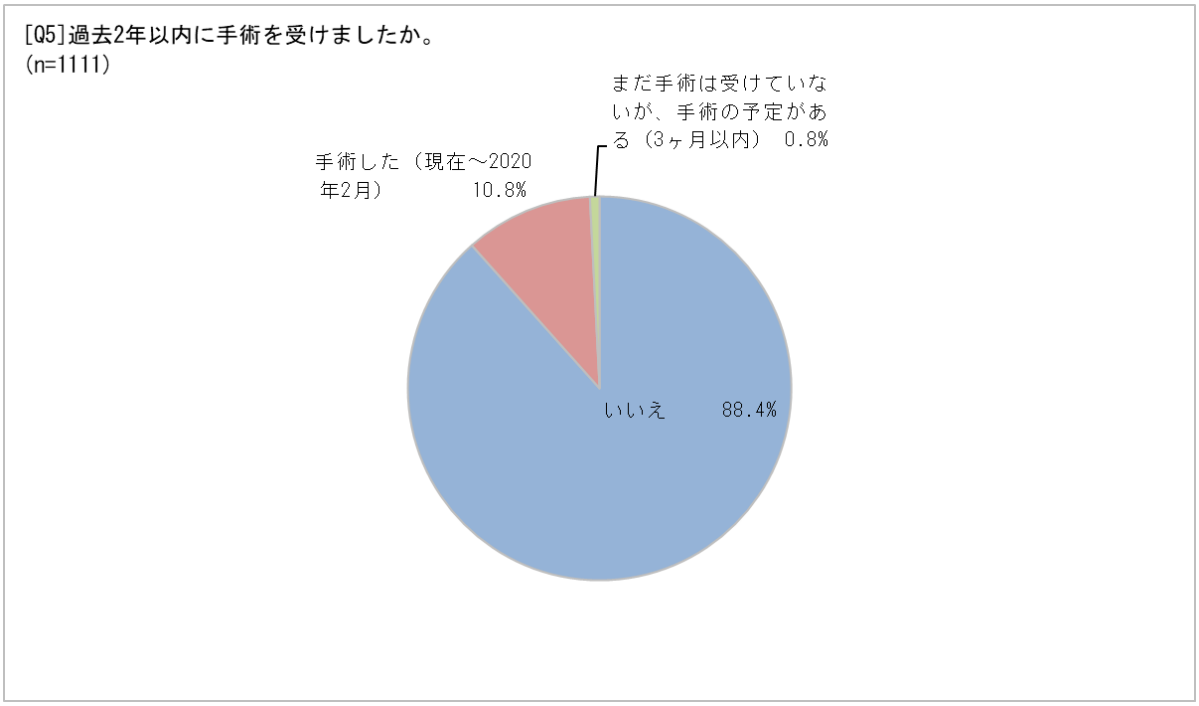


Figure10.過去2年間の手術歴

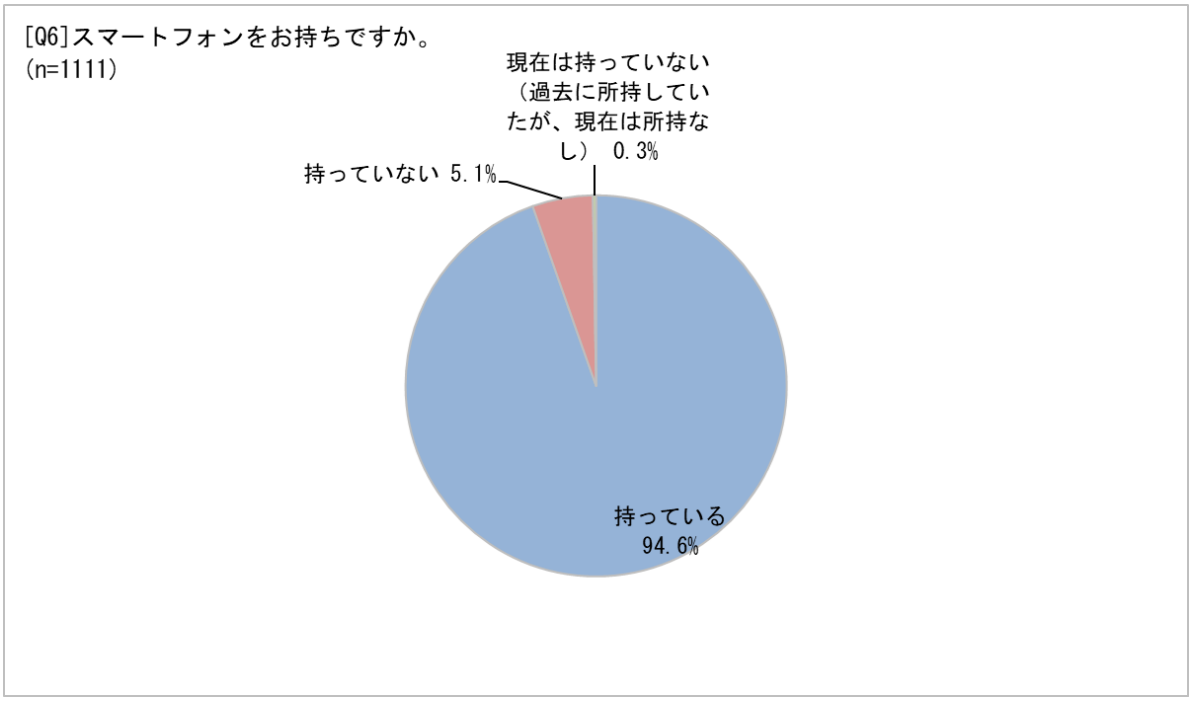


Figure11.スマートフォンの所持

[Q7]ご自身のマイナンバーカードを持っているか教えてください。（お住まいの自治体にてマイナンバーカードの交付申請手続き中、もしくはカードの受取り予定の方も含みます。）
(n=1111)

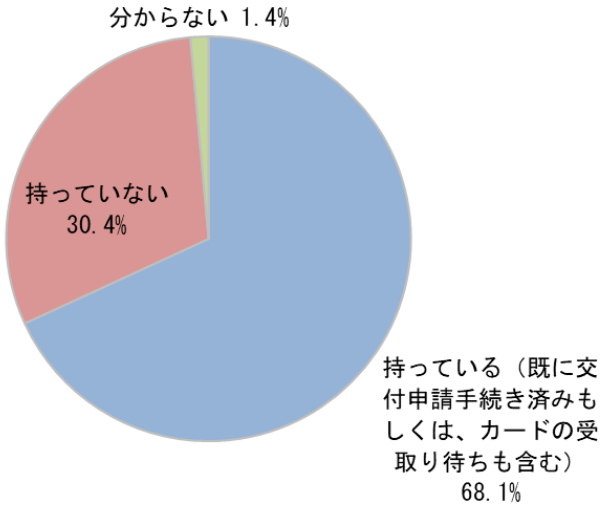


Figure12.マイナンバーカードの所有

[Q8]マイナンバーカードを持っていないと回答された方にお尋ねします。マイナンバーカードを持っていない理由を教えてください。当てはまるものが複数ある場合は、最も強い理由をお選びください。
(n=338)

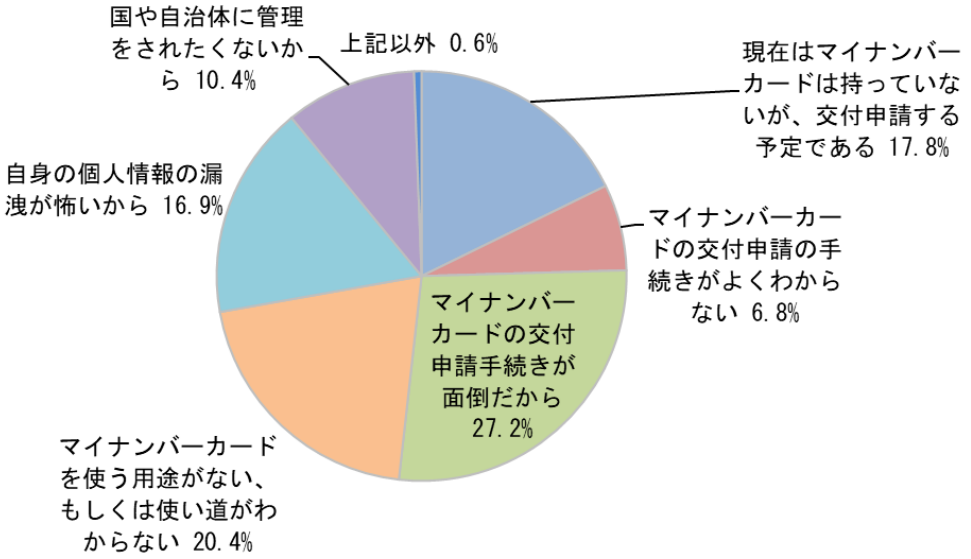


Figure13.マイナンバーカードを所有していない理由

[Q9]最近、医療機関(病院や診療所)では電子カルテやオンライン診療を導入するなど、電子化が進められています。また、日本政府によりマイナンバーカードの利用促進が行われており、マイナンバーカードが健康保険証として利用できるようになり、マイナンバーカードとマイナポータルを使えば、自分のスマートフォンで健診結果や薬剤情報が確認できたり、医療費控除も便利に行えるようになりました。将来的には PHR(Personal Health Records)という、健康医療データの個人口座の中に、乳幼児期の予防接種情報や医療機関での検査結果、健診の結果、お薬手帳の情報などが保管されることになります。PHR は、自分がケガや病気で受診した時に医師や看護師への説明に使ったり、自分の健康維持にも使えます。あなたのもしもの時、例えば意識不明で救急搬送されたり大規模災害の時でも、あなたの記憶やカルテの代わりに使えます。このように医療制度や生活環境が電子化の推進で便利になる一方、コンピュータウイルスの蔓延やハッカーによる侵入などの危険性について、セキュリティの専門家などから指摘されています。以下のそれぞれの項目について、ご自身の感覚にもっとも近いものを 1 つ選んでください。

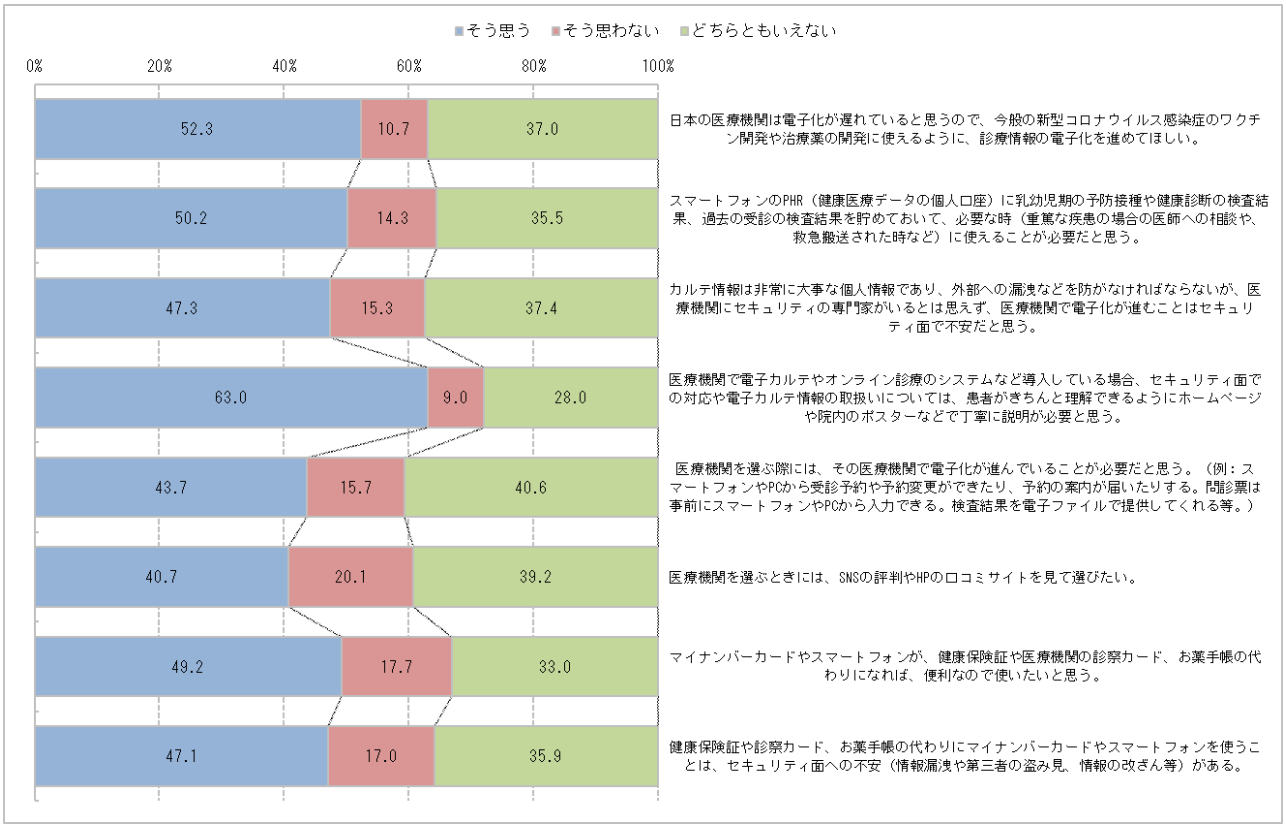


Figure14.医療機関の電子化への感想

[Q10]「オンライン診療」を知っているか教えてください。
(n=1111)

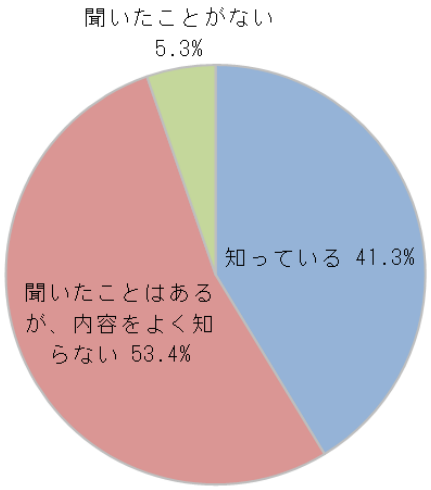


Figure15.オンライン診療の認知

[Q11]「オンライン診療を知っている」と回答された方にお尋ねします。ご自身がオンライン診療を受けたことがあるかを教えてください。
(n=459)

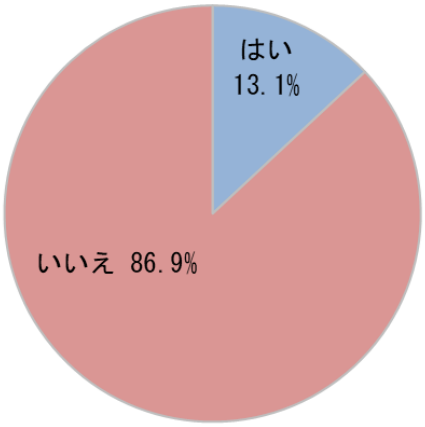


Figure16.オンライン診療の受診経験（対象:「オンライン診療」既知の回答者）

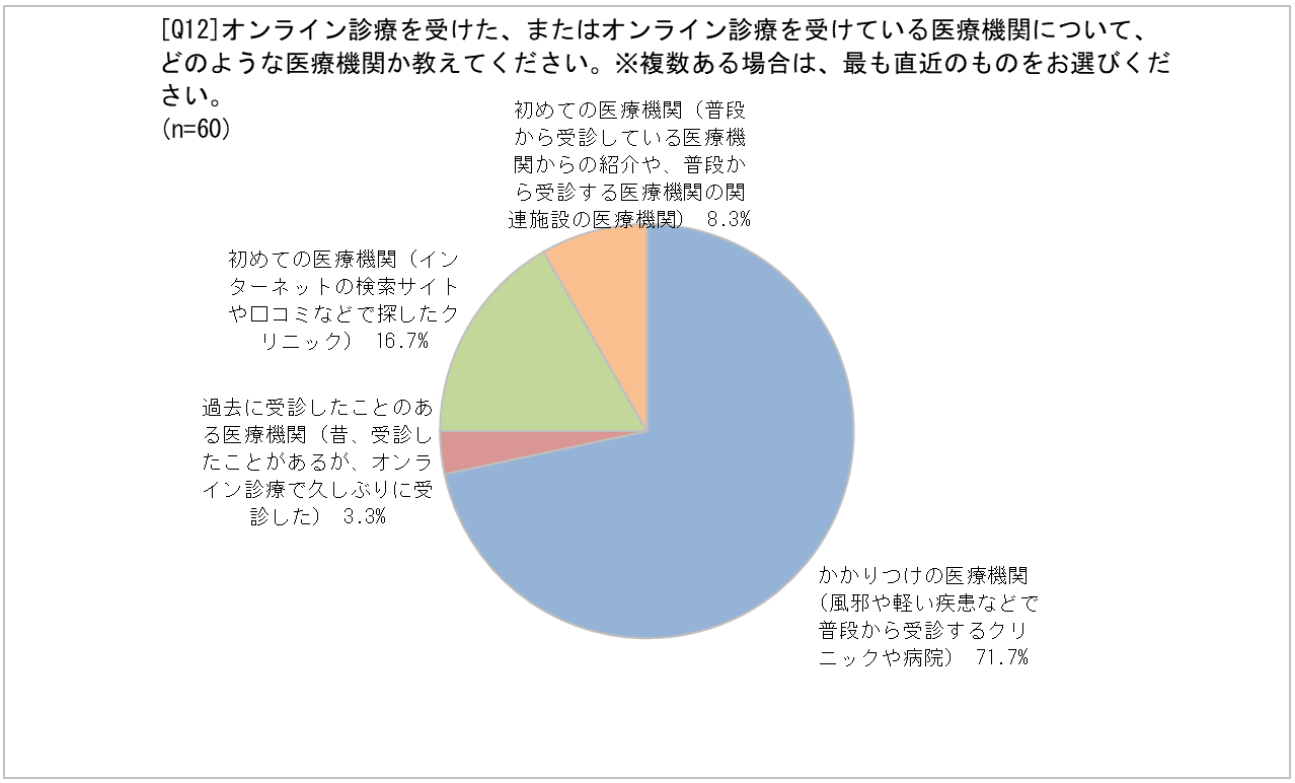


Figure17.（対象：経験者）オンライン診療を受けた医療機関について

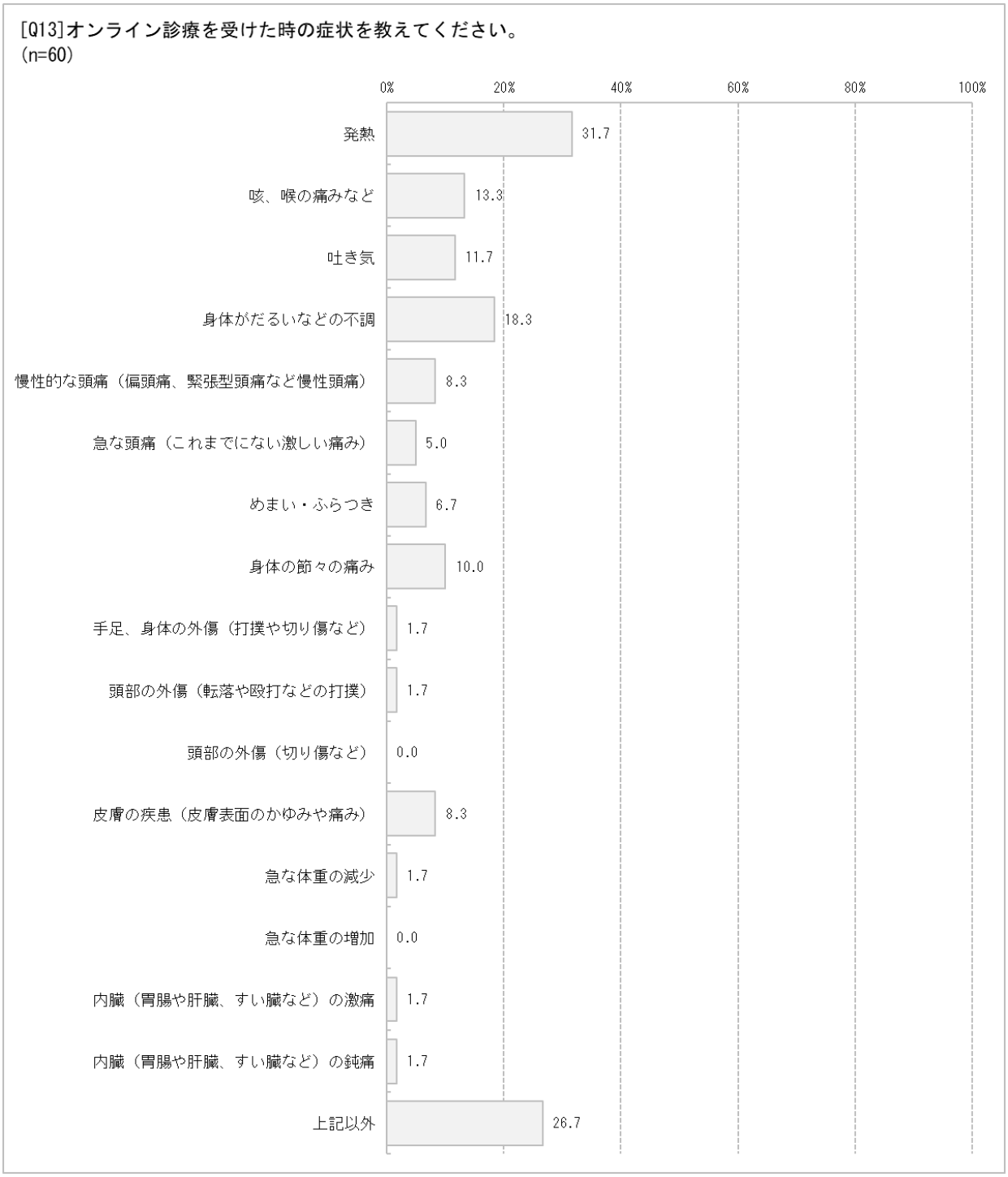


Figure18.（対象:経験者）オンライン診療を受けた際の症状＜疾患傷病等＞（複数回答）

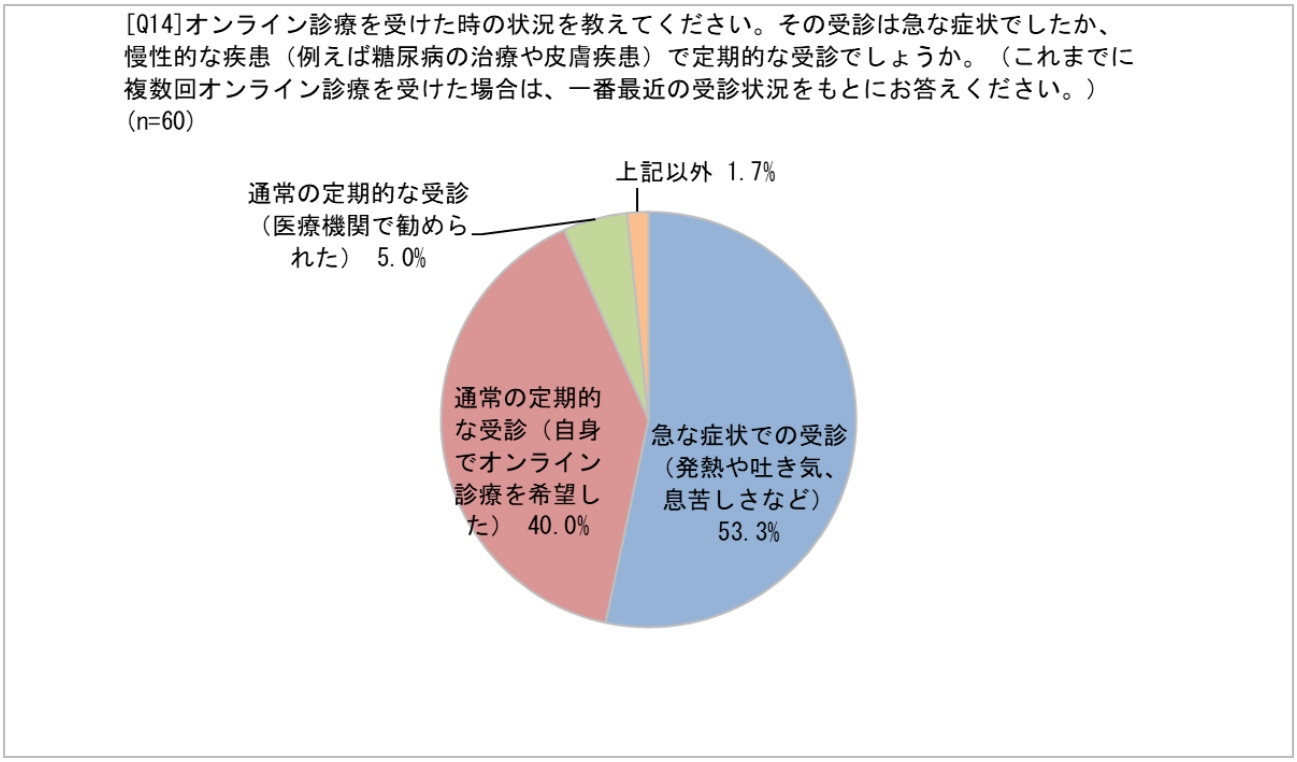


Figure19.（対象:経験者）オンライン診療を受けた際の状況＜発症＞

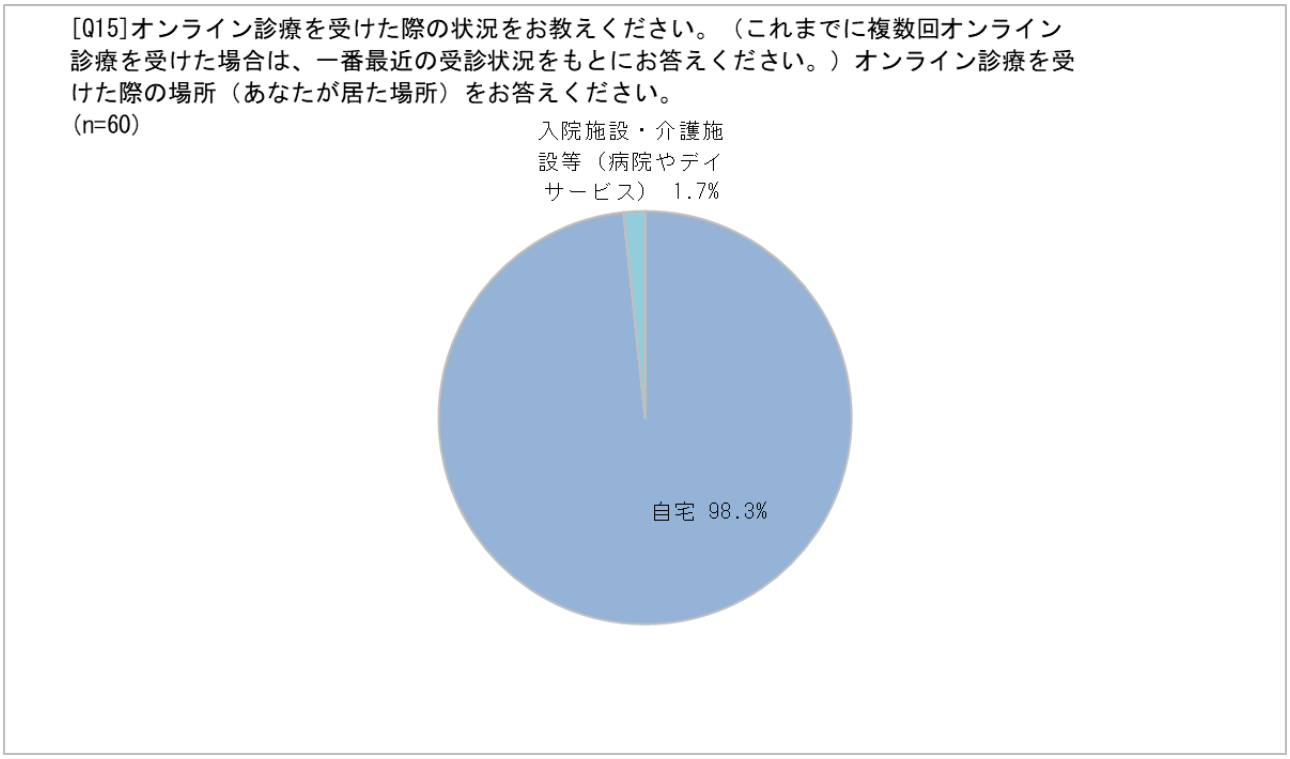


Figure20.（対象:経験者）オンライン診療を受けた際の状況＜場所＞

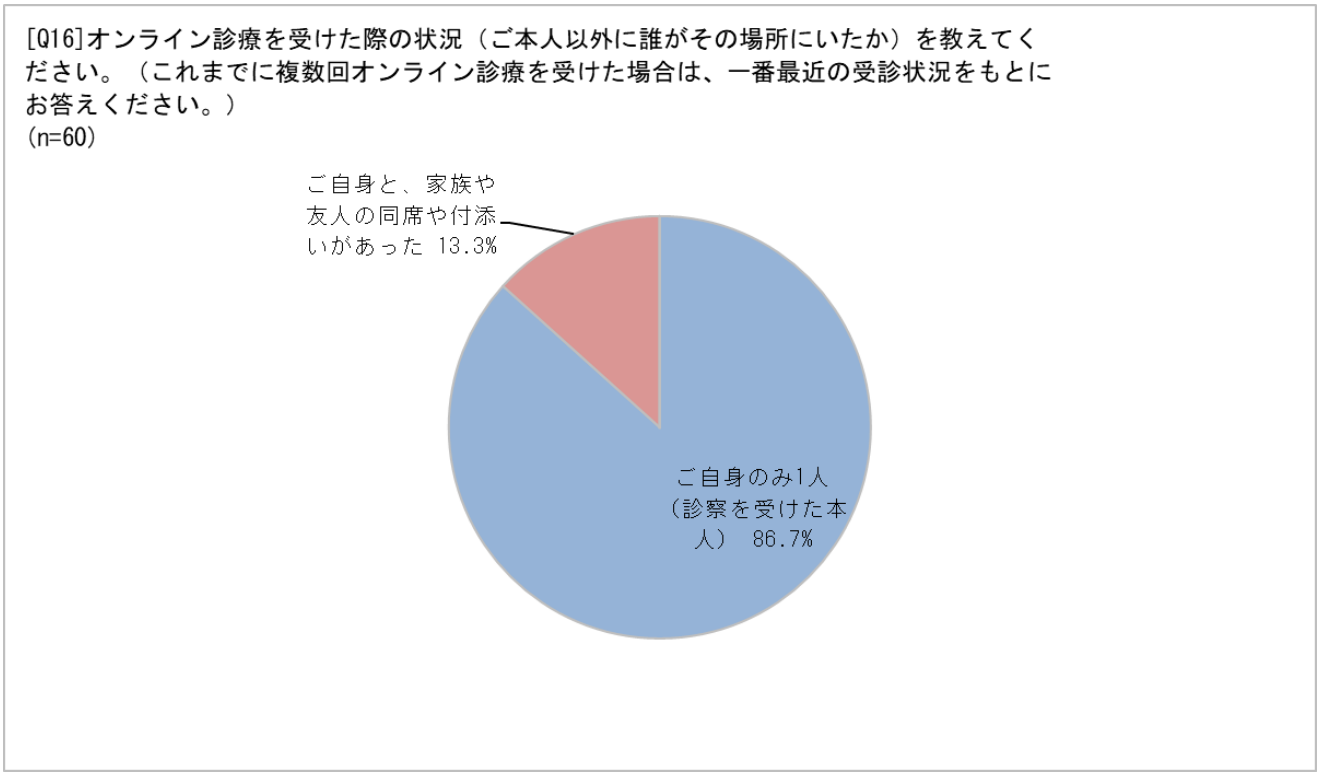


Figure21.（対象:経験者)オンライン診療の状況＜立会者等の有無＞

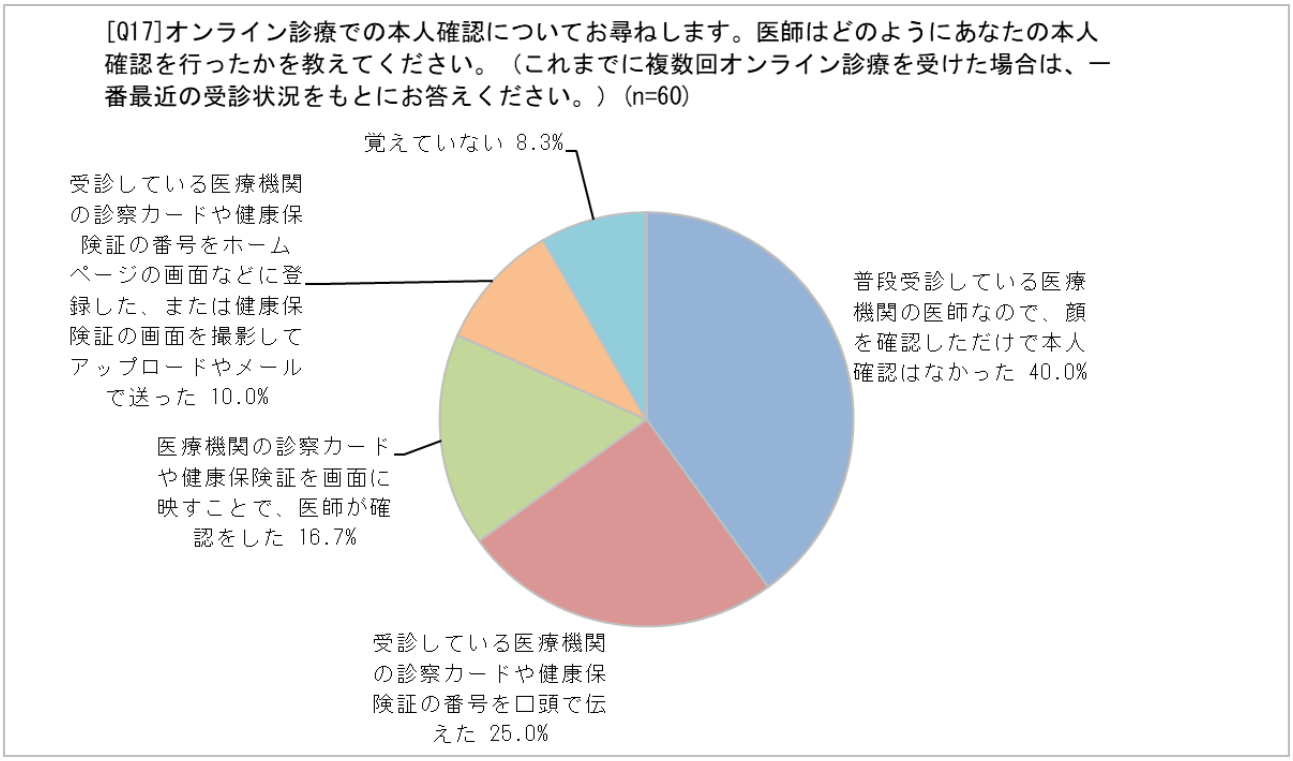


Figure22.（対象:経験者)オンライン診療での本人確認の方法

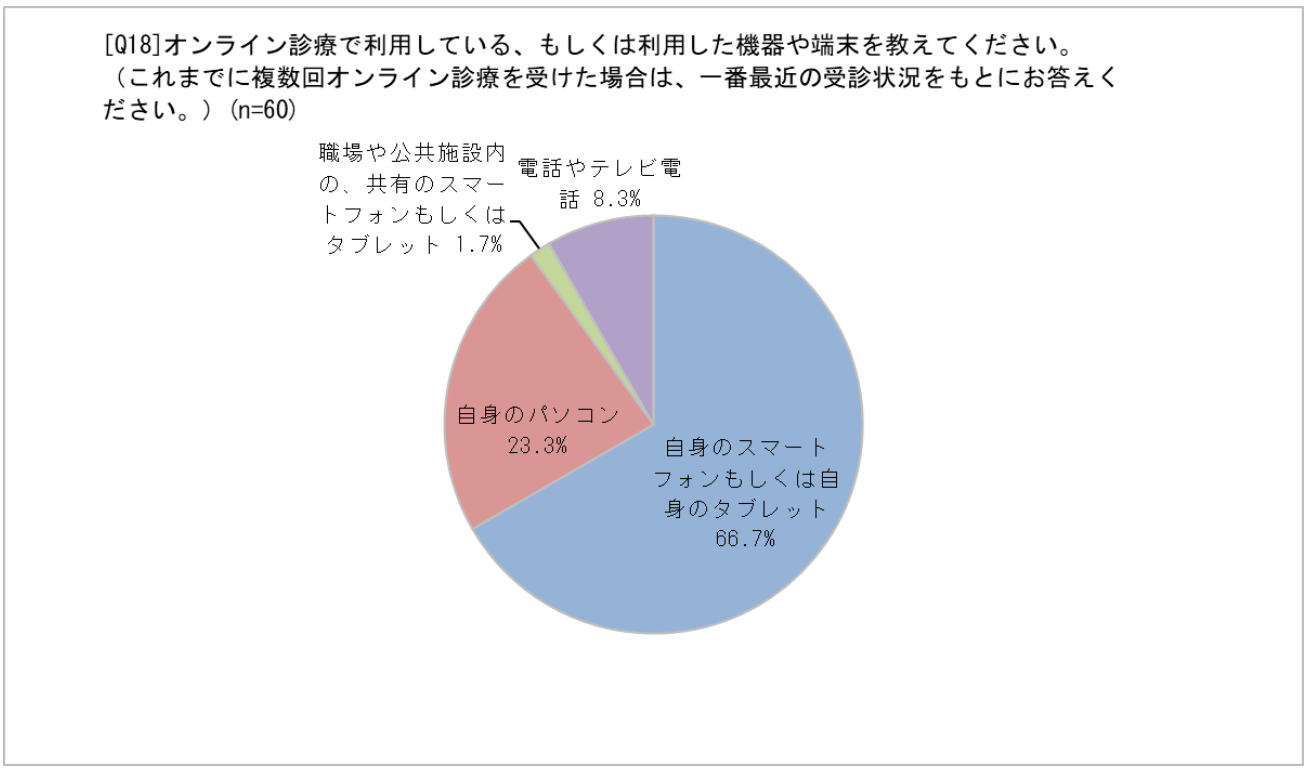


Figure23.（対象：経験者）オンライン診療で利用している機器・端末の種類

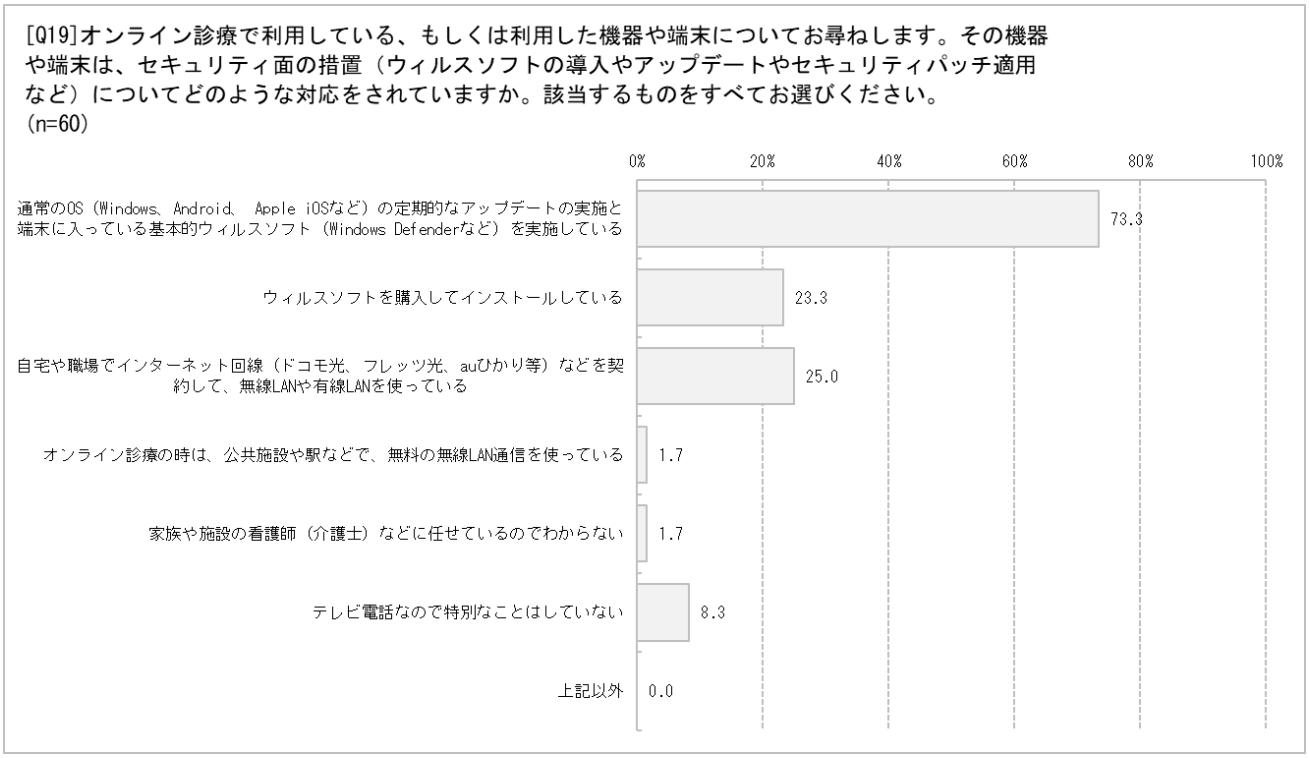


Figure24.（対象：経験者）オンライン診療で利用する端末のセキュリティ措置

[Q20]オンライン診療を受けた、もしくは受けている理由を教えてください。（複数当てはまる場合は、最も強い理由を1つお選びください。）(n=60)

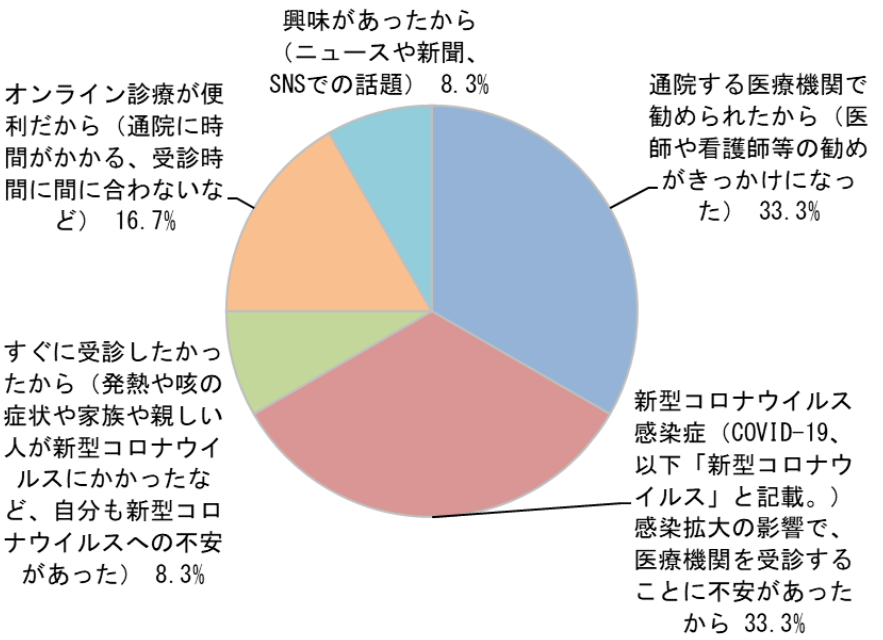


Figure25.（対象:経験者)オンライン診療を受けた理由

[Q21]オンライン診療を受けた、または受けている頻度を教えてください。(n=60)

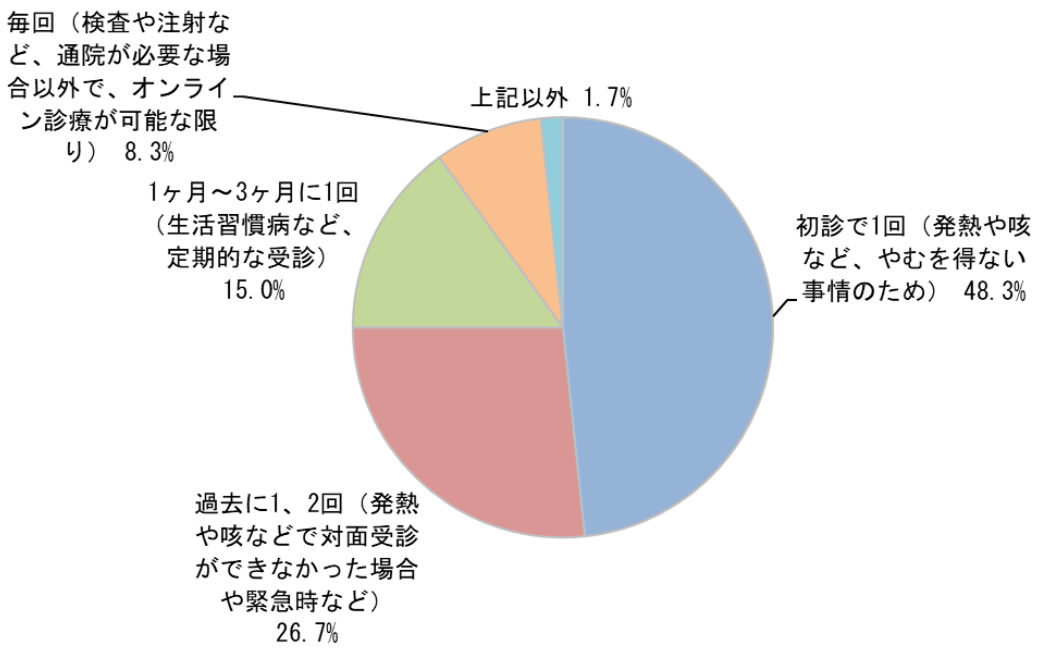


Figure26.（対象:経験者)オンライン診療の受診の頻度

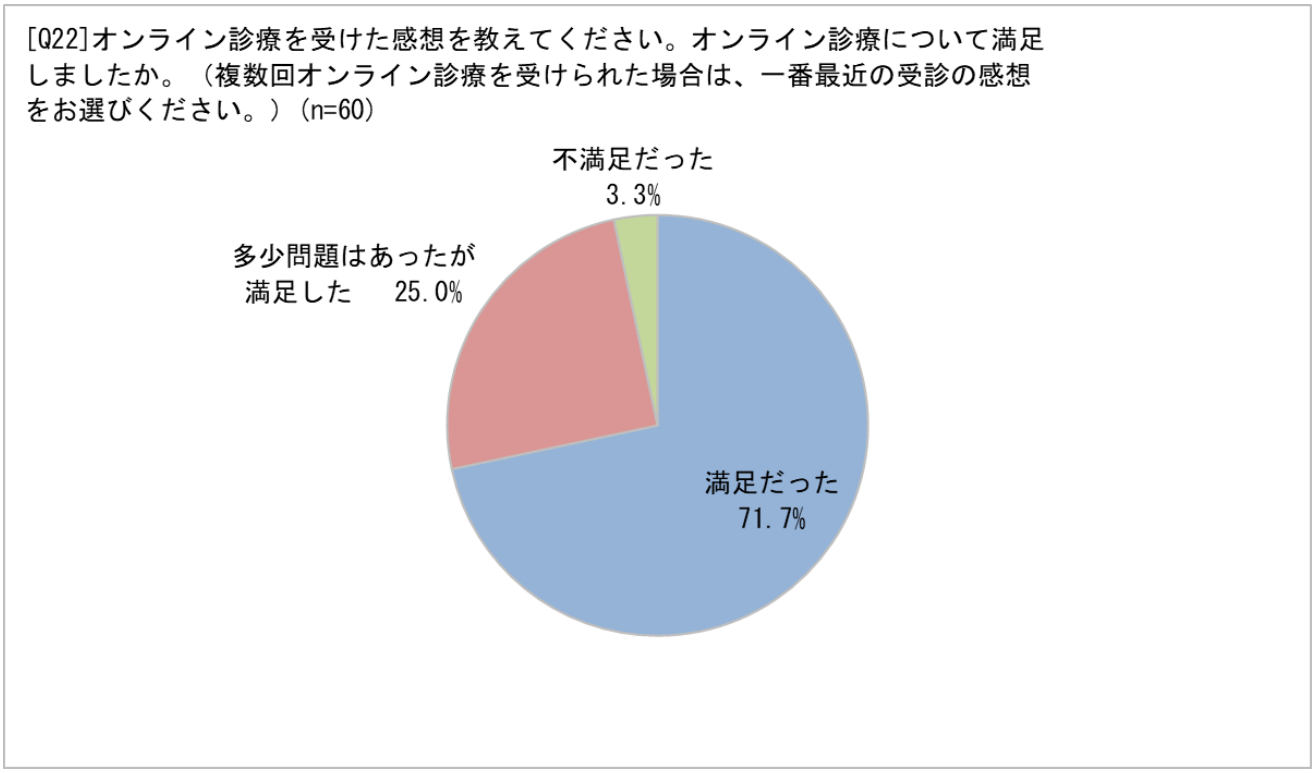


Figure27.（対象:経験者）オンライン診療を受けた感想

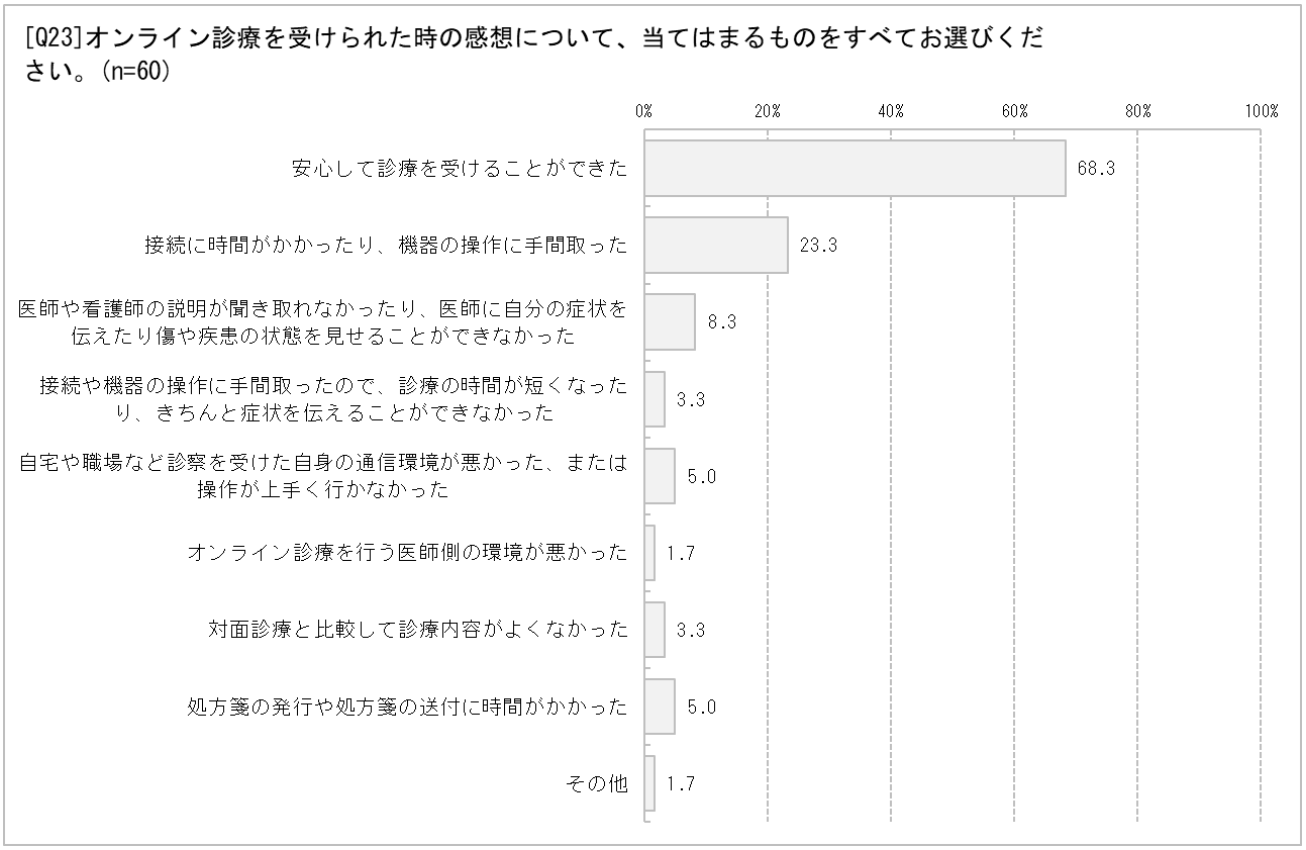


Figure28.（対象:経験者）オンライン診療の受診への感想

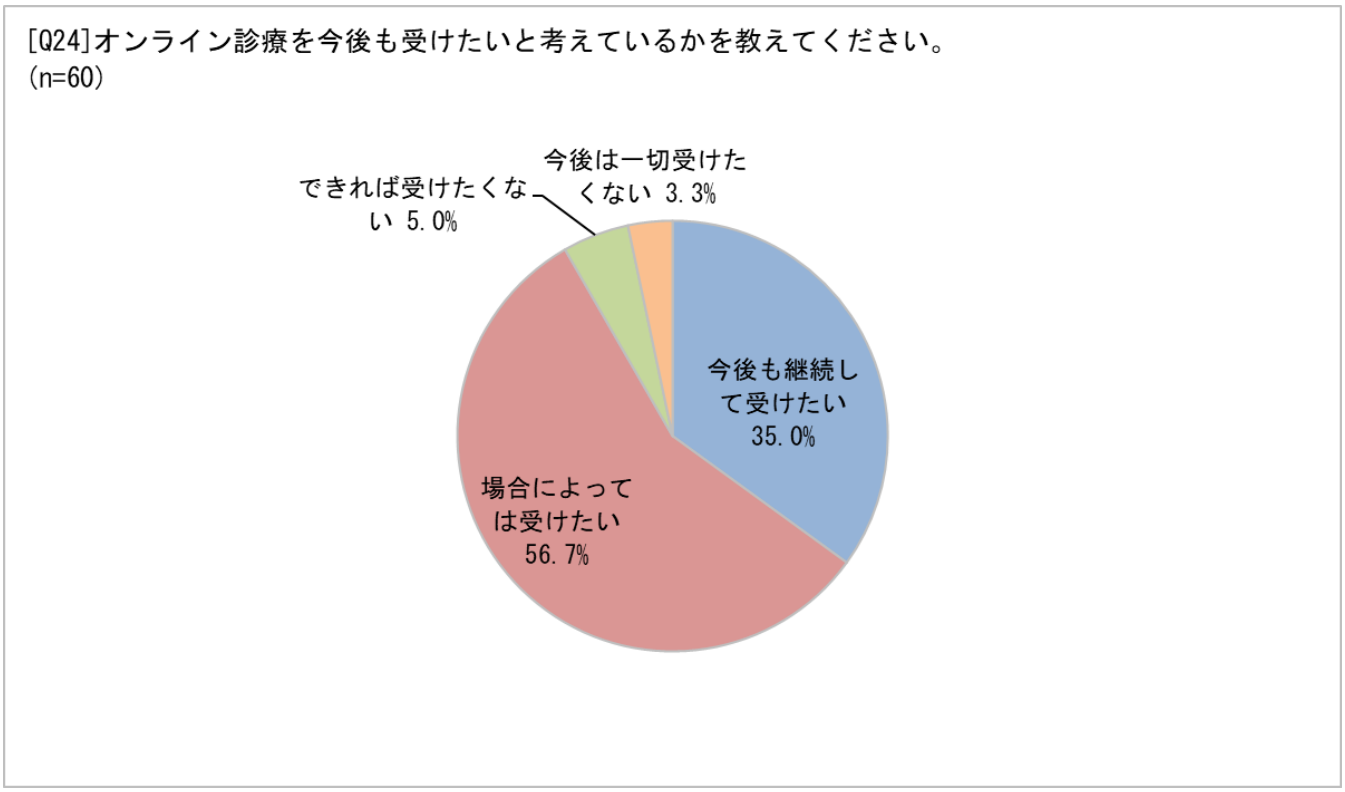


Figure29.（対象:経験者)オンライン診療の受診の希望

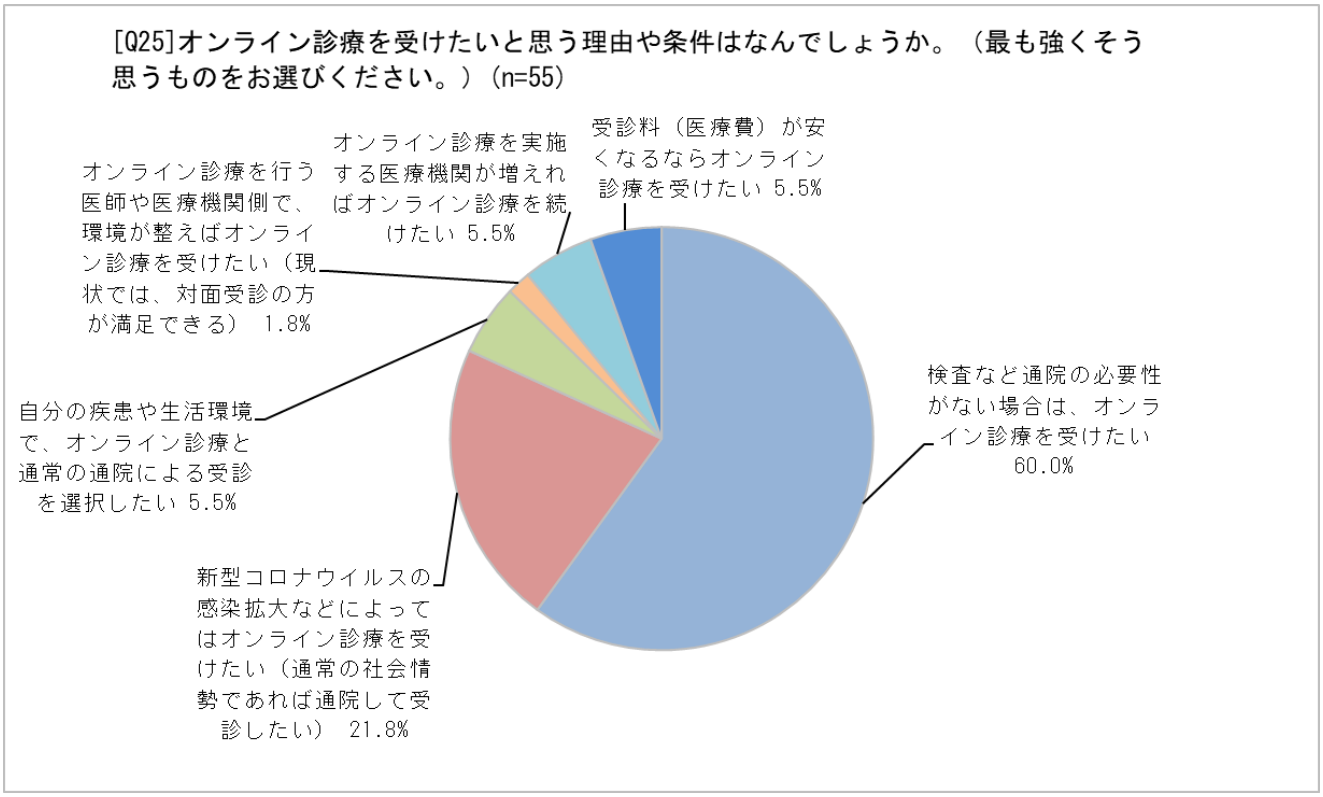


Figure30.（対象:経験者)オンライン診療を受けたいと思う理由

「オンライン診療」とは、患者が医療機関に赴いて医師の診療を受ける代わりに、スマートフォンなどの情報通信機器※を患者と医師が利活用した上で、医師が患者の診察や診断を行い診断結果の説明や処方等の診療行為を行うことです。通常は、医療機関を受診している患者のうち、症状が落ち着いており医師がオンライン診療で問題ないと判断される患者の場合は、その医療機関のオンライン診療を受けることが可能ですが、今般の新型コロナウイルスの感染拡大を受け、問題がないと医師が判断した場合ややむを得ない場合は、診療前相談などを行った上で、初診からでもオンライン診療を受けることができます。(初診からのオンライン診療は、原則として「かかりつけの医師」や健康診断の結果を医師が持っている場合など、限られます。)※情報通信機器・・・テレビ電話、スマートフォン、タブレット、パソコン等で撮影や通話、インターネット・無線 LAN 通信等が可能な機器

上記の「オンライン診療」の説明を読んで、オンライン診療についてお尋ねします。オンライン診療を受けたいと思いますか。(n=652)

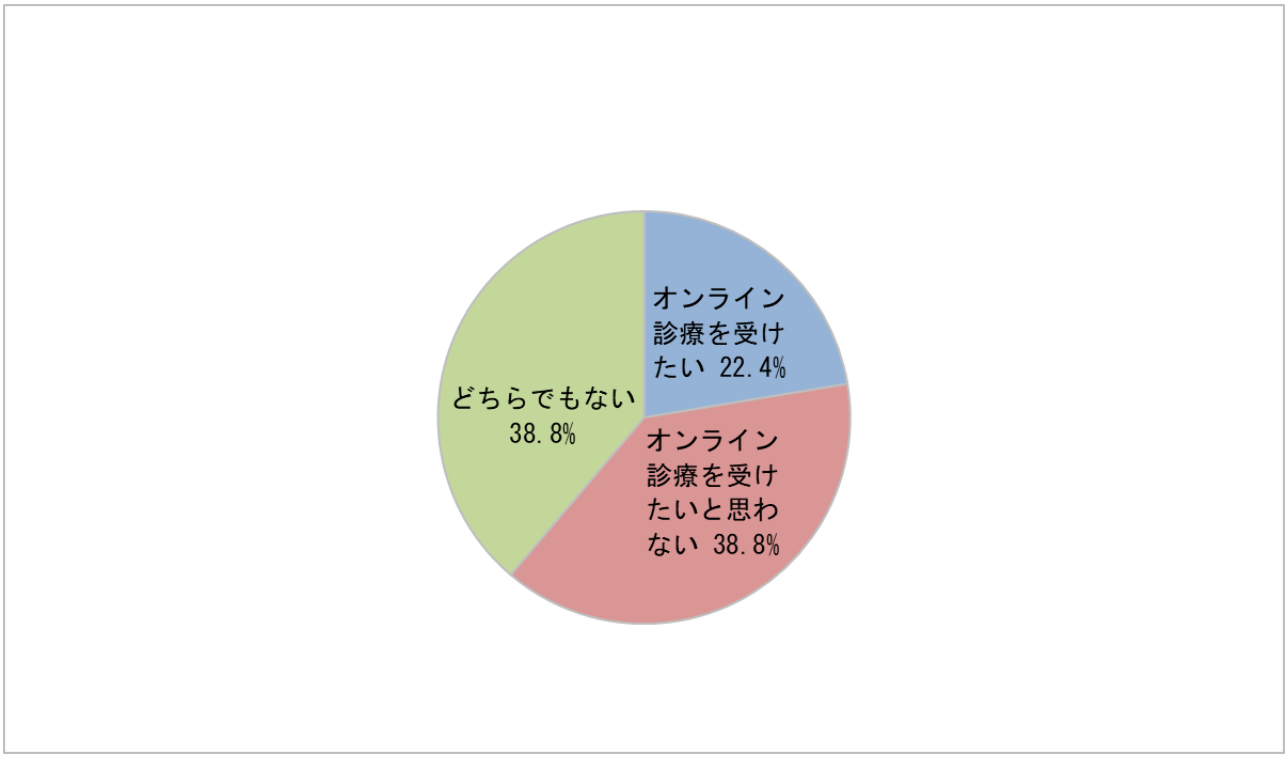


Figure31.オンライン診療での受診の希望

[Q27]前問で、「オンライン診療を受けたいと思わない」と回答された方に伺います。「オンライン診療を受けたいと思わない」理由は何でしょうか。（最も強くそう思うものをお選びください。）（n=253）

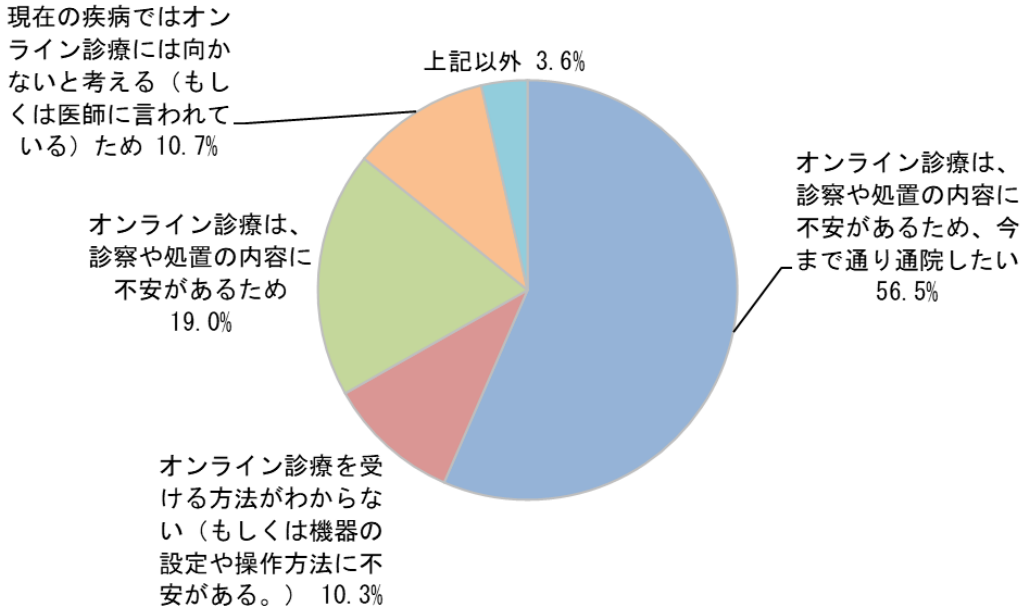


Figure32.オンライン診療を受けたいと思わない理由

[Q28]「オンライン診療を受けたことがない」と回答した方へお尋ねします。オンライン診療を受けていない、またはオンライン診療を受けることができない理由をお教えください。（該当が複数ある場合は、最も強い理由をお選びください。）（n=399）

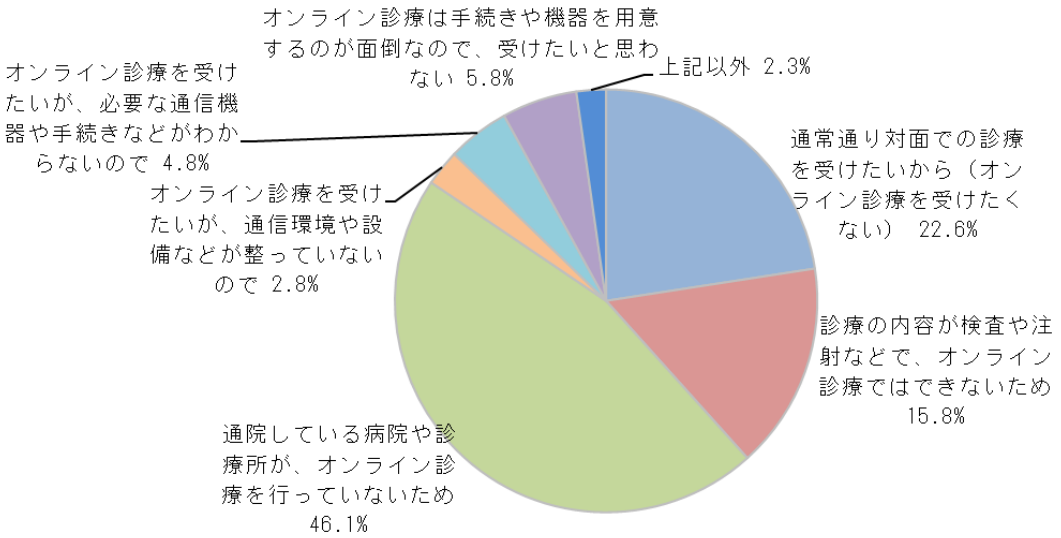


Figure33.オンライン診療を受けた経験がない理由

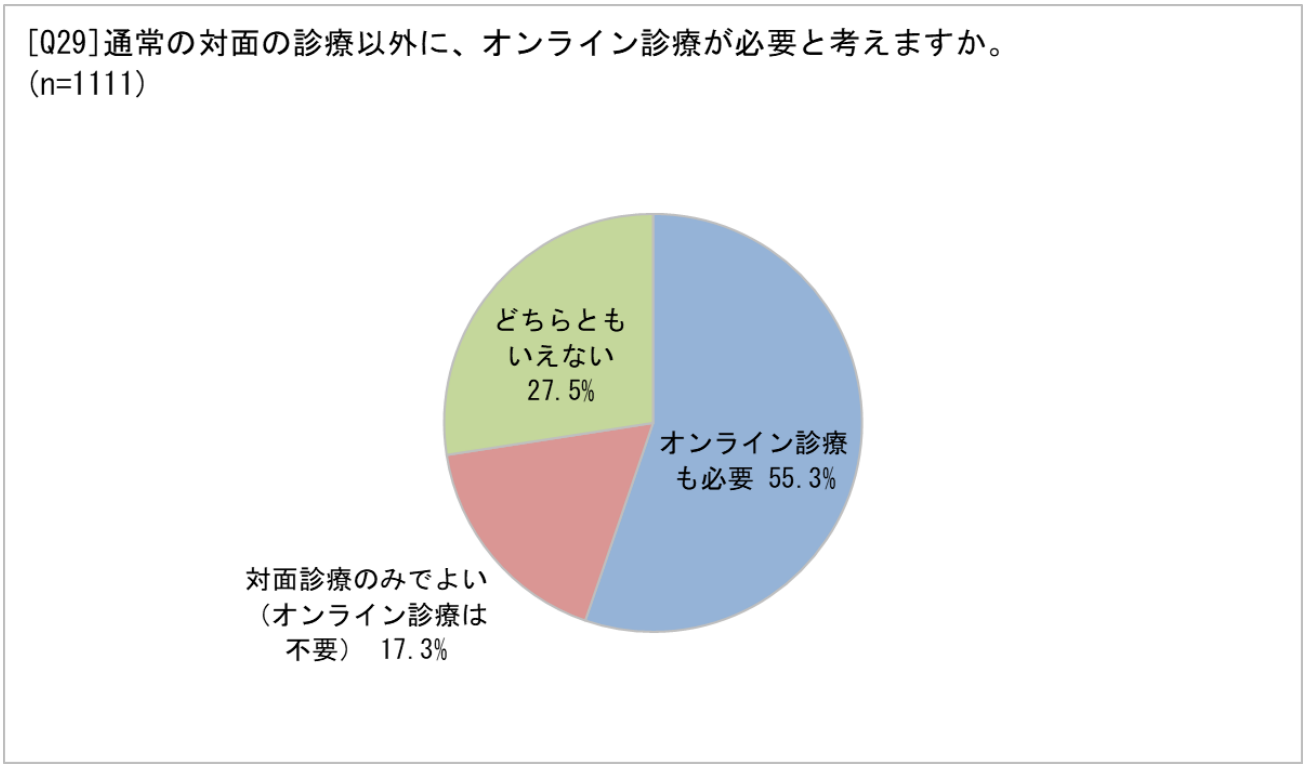


Figure34.オンライン診療の必要性(全回答者)

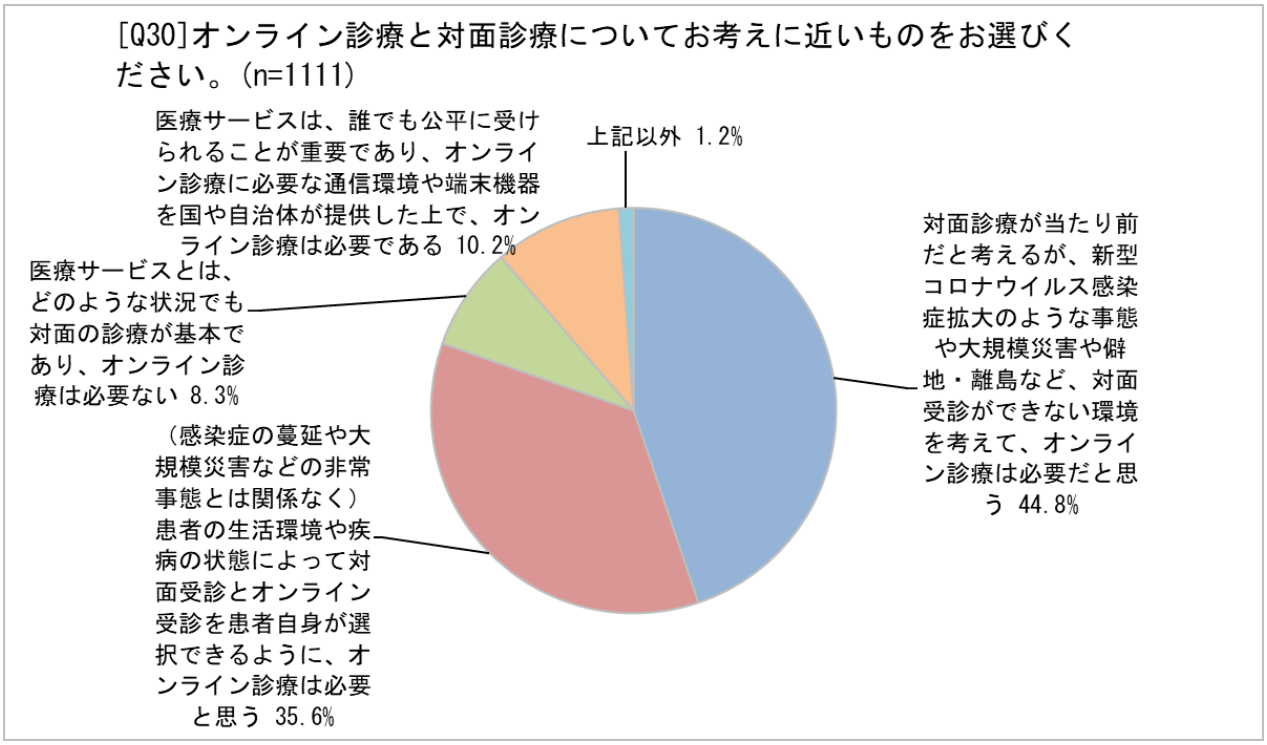
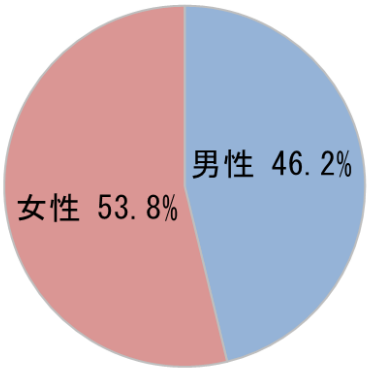


Figure35.オンライン診療と対面診療に対する考え(全回答者)

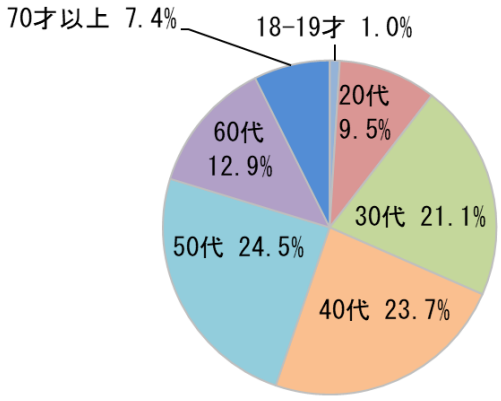
＜参考 2＞前回調査結果(2021 年 3 月実施分)

前回の調査は 2021 年 3 月 26 日～29 日、対象者:患者 1030 名。対象者の選定方法、調査票はほぼ同じものとなる。前回の調査結果を下に記す。

[F1]あなたの性別をお選びください。（１つだけ） 【必須入力 】(n=1030)



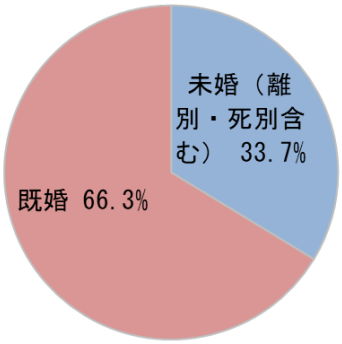
[NF2S1N]あなたの年齢をお答えください。 【必須入力 】(n=1030)



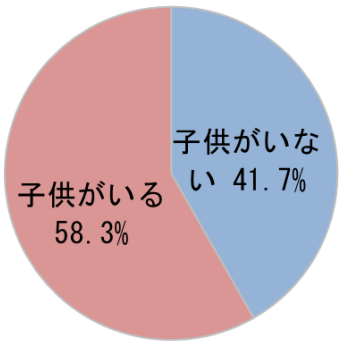
F3 あなたのお住まいをお選びください。(1つだけ)【 必須入力 】

	単一回答	n	%
	全体	(1030)	
1	北海道	38	3.7
2	青森県	10	1.0
3	岩手県	12	1.2
4	宮城県	14	1.4
5	秋田県	12	1.2
6	山形県	4	0.4
7	福島県	13	1.3
8	茨城県	23	2.2
9	栃木県	13	1.3
10	群馬県	9	0.9
11	埼玉県	58	5.6
12	千葉県	59	5.7
13	東京都	143	13.9
14	神奈川県	98	9.5
15	新潟県	13	1.3
16	富山県	9	0.9
17	石川県	8	0.8
18	福井県	3	0.3
19	山梨県	3	0.3
20	長野県	19	1.8
21	岐阜県	13	1.3
22	静岡県	34	3.3
23	愛知県	72	7.0
24	三重県	16	1.6
25	滋賀県	11	1.1
26	京都府	16	1.6
27	大阪府	76	7.4
28	兵庫県	54	5.2
29	奈良県	14	1.4
30	和歌山県	5	0.5
31	鳥取県	6	0.6
32	島根県	3	0.3
33	岡山県	17	1.7
34	広島県	24	2.3
35	山口県	7	0.7
36	徳島県	5	0.5
37	香川県	6	0.6
38	愛媛県	10	1.0
39	高知県	2	0.2
40	福岡県	37	3.6
41	佐賀県	2	0.2
42	長崎県	6	0.6
43	熊本県	7	0.7
44	大分県	9	0.9
45	宮崎県	3	0.3
46	鹿児島県	8	0.8
47	沖縄県	6	0.6

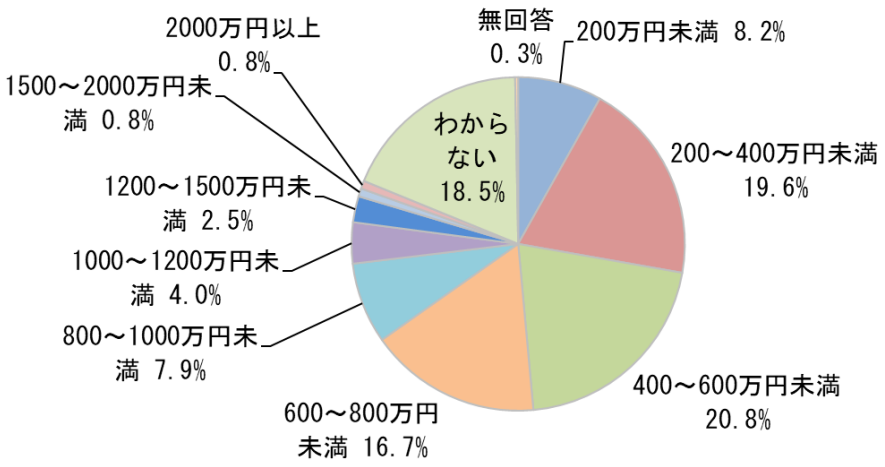
[F4]あなたは、現在ご結婚されていますか。 【必須入力 】
(n=1030)



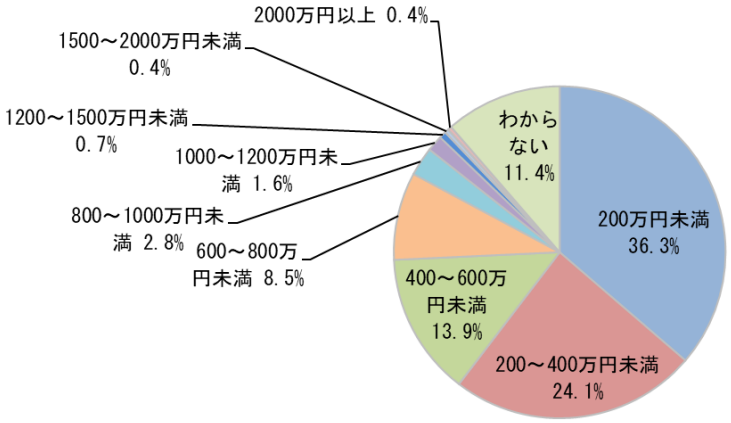
[F5]あなたには、現在お子様がいらっしゃいますか。【必須入力 】(n=1030)



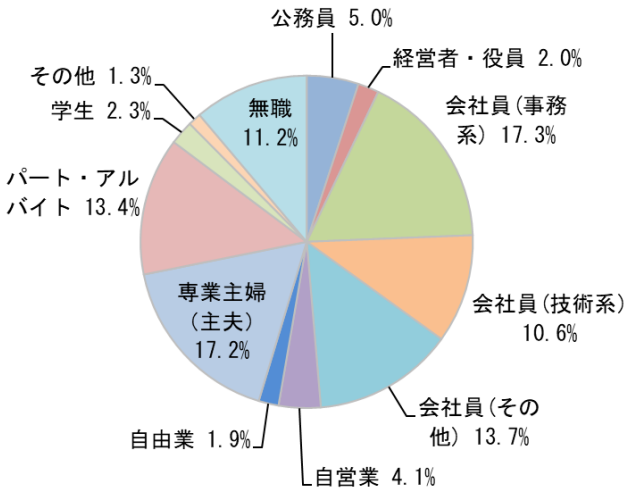
[F6]あなたの世帯年収（税込）を教えてください。（ひとつだけ）
(n=1030)



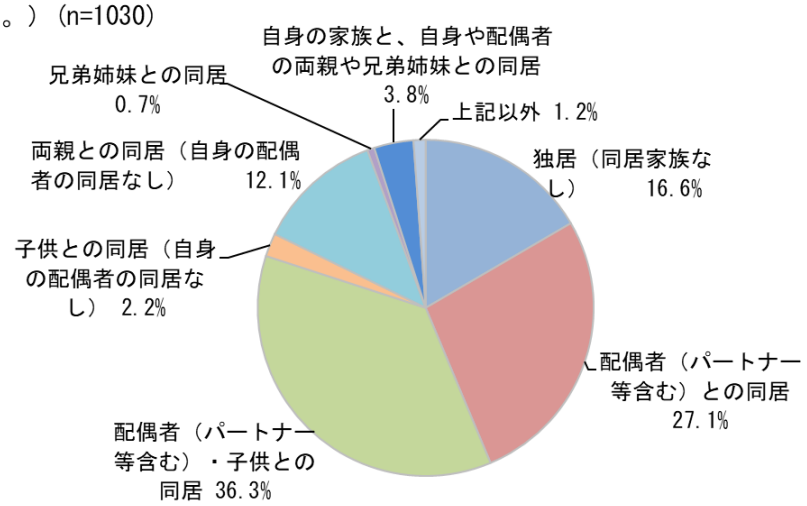
[F7]あなたの個人年収（税込）をお答えください。（ひとつだけ）
(n=1030)



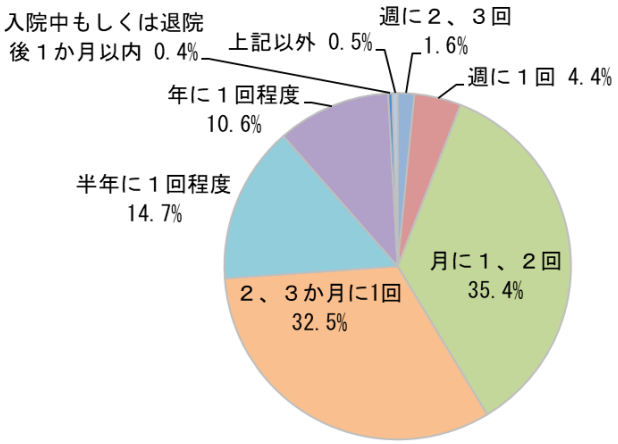
[F8]あなたの現在のご職業をお答えください。 【必須入力 】
(n=1030)



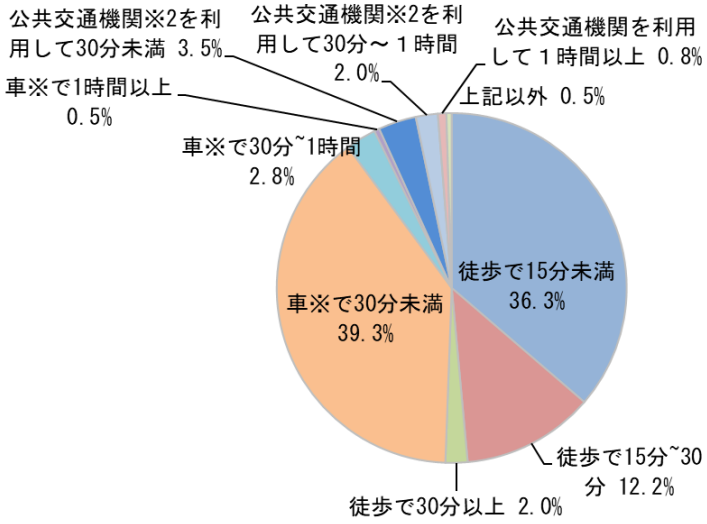
[Q1]現在の生活状況をお答えください。（同居の対象は人間で、ペットは含みません。）(n=1030)

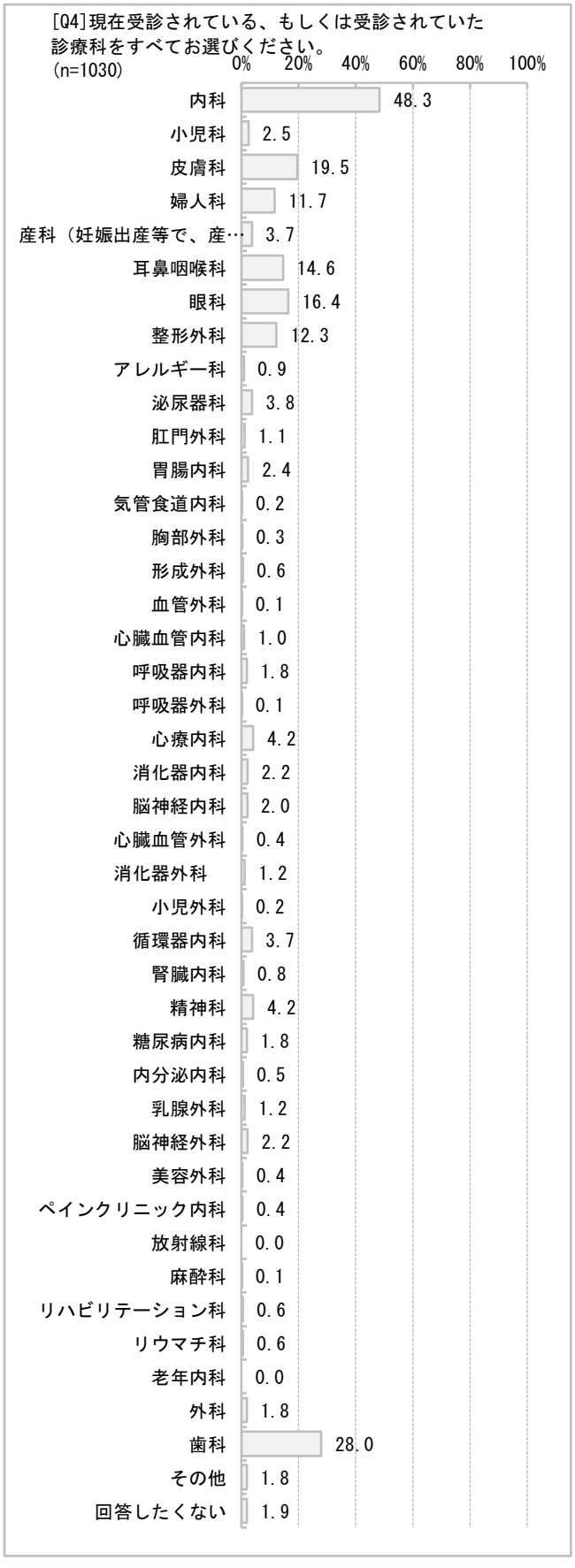


[Q2]医療機関への受診頻度をお答えください。（職場や自治体の定期健康診断以外）もし、複数の疾患で受診されている場合は、受診回数が多い方でお答えください。医科、歯科など診療科や、通院・オンライン診療などは問いません。(n=1030)

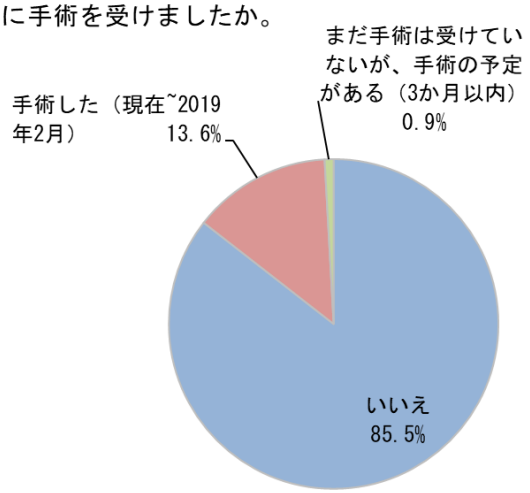


[Q3]風邪など軽い不調や予防接種で受診する医療機関（診療所や病院など）への主なアクセス方法について、該当するものを１つお選びください。（※車は、自家用車、自転車、バイクを指します。）（※2公共交通機関はバス、地下鉄、電車、モノレールなどを指します。）(n=1030)

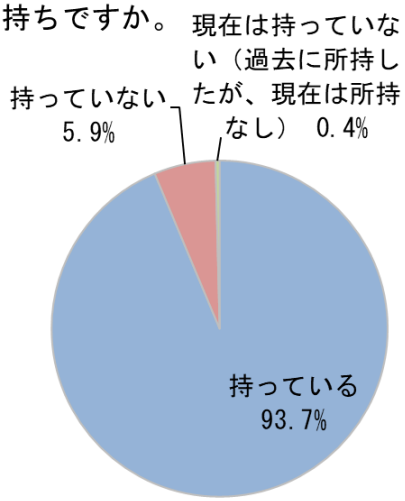



[Q4]現在受診されている、もしくは受診されていた
診療科をすべてお選びください。
(n=1030)
0%
20%
40%
60%
80%
100%
内科 48.3
小児科 2.5
皮膚科 19.5
婦人科 11.7
産科（妊娠出産等で、産… 3.7
耳鼻咽喉科 14.6
眼科 16.4
整形外科 12.3
アレルギー科 0.9
泌尿器科 3.8
肛門外科 1.1
胃腸内科 2.4
気管食道内科 0.2
胸部外科 0.3
形成外科 0.6
血管外科 0.1
心臓血管内科 1.0
呼吸器内科 1.8
呼吸器外科 0.1
心療内科 4.2
消化器内科 2.2
脳神経内科 2.0
心臓血管外科 0.4
消化器外科 1.2
小児外科 0.2
循環器内科 3.7
腎臓内科 0.8
精神科 4.2
糖尿病内科 1.8
内分泌内科 0.5
乳腺外科 1.2
脳神経外科 2.2
美容外科 0.4
ペインクリニック内科 0.4
放射線科 0.0
麻酔科 0.1
リハビリテーション科 0.6
リウマチ科 0.6
老年内科 0.0
外科 1.8
歯科 28.0
その他 1.8
回答したくない 1.9

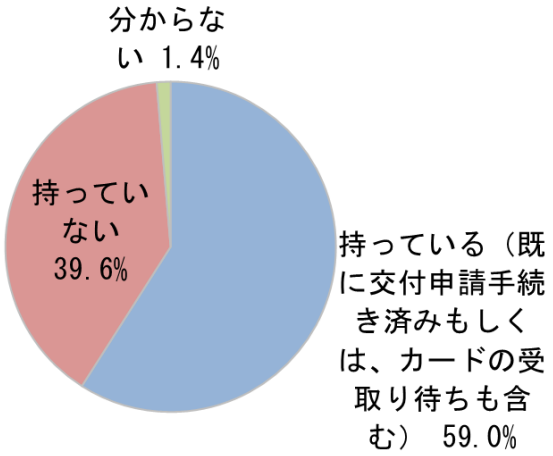
[Q5]過去２年以内に手術を受けましたか。
(n=1030)



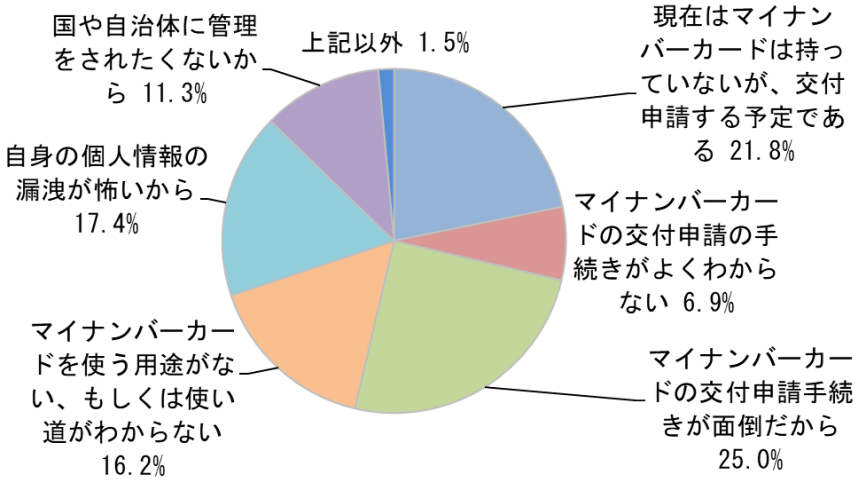
[Q6]スマートフォンをお持ちですか。
(n=1030)



[Q7]ご自身のマイナンバーカードを持っているか教えてください。（お住まいの自治体にてマイナンバーカードの交付申請手続き中、もしくはカードの受取り予定の方も含みます。）(n=1030)



[Q8]マイナンバーカードを持っていないと回答された方にお尋ねします。マイナンバーカードを持っていない理由を教えてください。当てはまるものが複数ある場合は、最も強い理由をお選びください。(n=408)

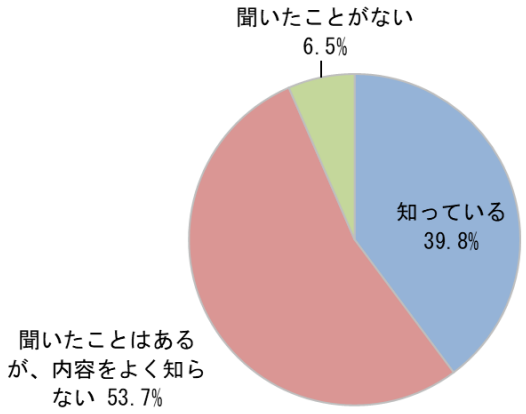


Q9 最近、医療機関（病院や診療所）では電子カルテの導入やオンライン診療を導入するなど、電子化が進められています。また、日本政府ではマイナンバーカードの利用促進が行われており、健康保険証としての利用や運転免許証と一体化も進められています。マイナンバーの仕組みを使って、自分のスマートフォンで健診結果や薬剤情報が確認できたり、医療費控除も便利に行えるようになります。将来的にはPHR（Personal Health Records）という、健康医療データの個人口座の中に、乳幼児期の予防接種情報や医療機関での検査結果、健診の結果、お薬手帳の情報などが保管されることになります。PHRは、自分がケガや病気で受診した時に医師や看護師への説明に使ったり、自分の健康維持にも使えます。あなたのもしもの時、例えば意識不明で救急搬送されたり大規模災害の時でも、あなたの記憶やカルテの代わりに使えます。このように医療制度や生活環境が電子化の推進で便利になる一方、コンピュータウイルスの蔓延やハッカーによる侵入などのセキュリティの専門家などから指摘されています。以下のそれぞれの項目について、ご自身の感覚にもっとも近いものを１つ選んでください。

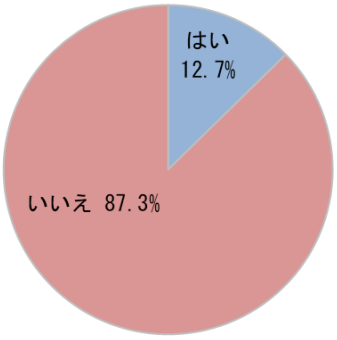
単一回答マトリクス

			1	2	3
		全体	そう思う	そう思わない	どちらともいえない
1	日本の医療機関は電子化が遅れていると思うので、今般の新型コロナウイルス感染症のワクチン開発や治療薬の開発に使えるように、診療情報の電子化を進めてほしい。	(1030)	553 53.7	97 9.4	380 36.9
2	スマートフォンのPHR（健康医療データの個人口座）に乳幼児期の予防接種や健康診断の検査結果、過去の受診の検査結果を貯めておいて、必要な時（重篤な疾患の場合の医師への相談や、救急搬送された時など）に使えることが必要だと思う。	(1030)	524 50.9	147 14.3	359 34.9
3	カルテ情報は非常に大事な個人情報であり、外部への漏洩などを防がなければならないが、医療機関にセキュリティの専門家がいるとは思えず、医療機関で電子化が進むことはセキュリティ面で不安だと思う。	(1030)	507 49.2	169 16.4	354 34.4
4	医療機関で電子カルテやオンライン診療のシステムなど導入している場合、セキュリティ面での対応や電子カルテ情報の取扱いについては、患者がきちんと理解できるようにホームページや院内のポスターなどで丁寧に説明が必要と思う。	(1030)	683 66.3	77 7.5	270 26.2
5	医療機関を選ぶ際には、その医療機関で電子化が進んでいることが必要だと思う。（例：スマートフォンやPCから受診予約や予約変更ができたり、予約の案内が届いたりする。問診票は事前にスマートフォンやPCから入力できる。検査結果を電子ファイルで提供してくれる等。）	(1030)	482 46.8	147 14.3	401 38.9
6	医療機関を選ぶときには、SNSの評判やHPの口コミサイトの見て選びたい。	(1030)	405 39.3	224 21.7	401 38.9
7	マイナンバーカードやスマートフォンが、健康保険証や医療機関の診察カード、お薬手帳代わりになるとすれば、便利なので使いたいと思う。	(1030)	497 48.3	181 17.6	352 34.2
8	健康保険証や診察カード、お薬手帳の代わりにマイナンバーカードやスマートフォンを使うことは、セキュリティ面への不安（情報漏洩や第三者の盗み見、情報の改ざん等）がある。	(1030)	524 50.9	157 15.2	349 33.9

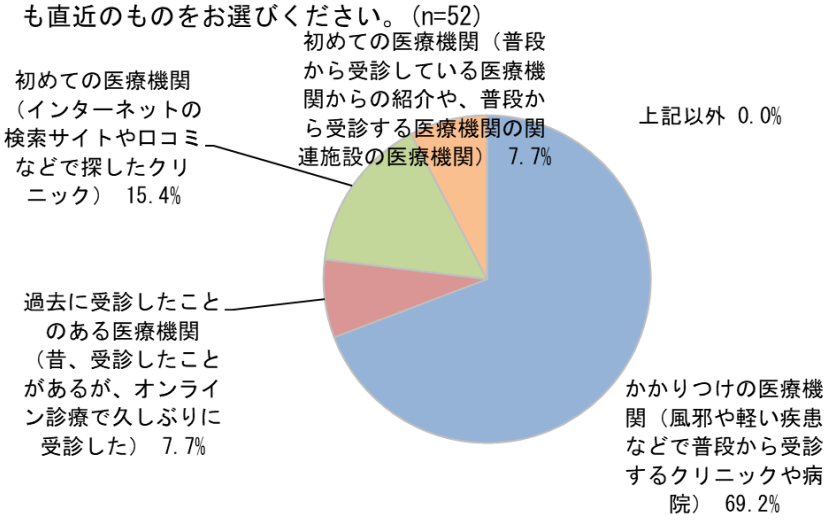
[Q10]「オンライン診療」を知っているか教えてください。
(n=1030)



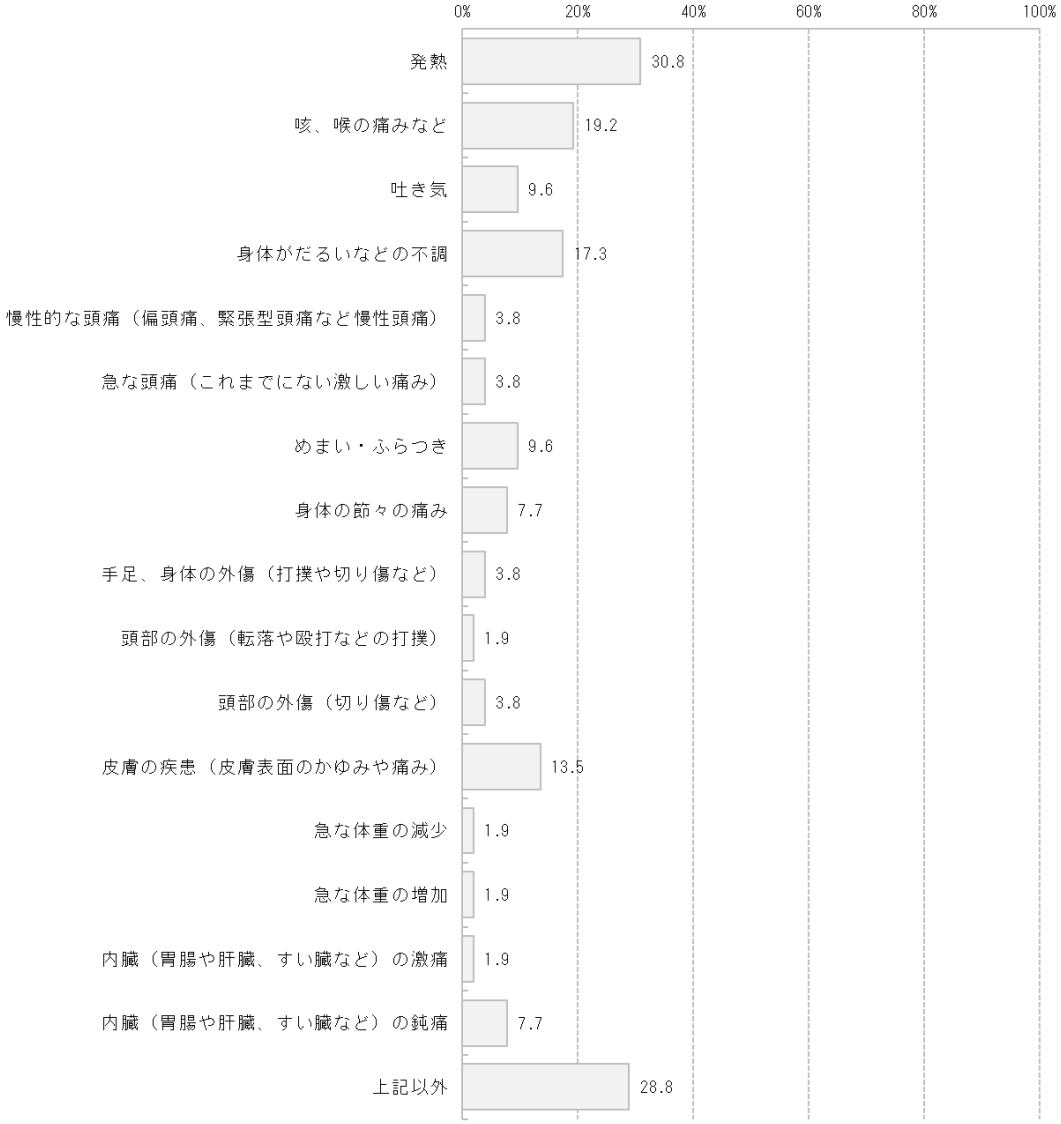
[Q11]「オンライン診療を知っている」と回答された方にお尋ねします。ご自身がオンライン診療を受けたことがあるかを教えてください。(n=410)



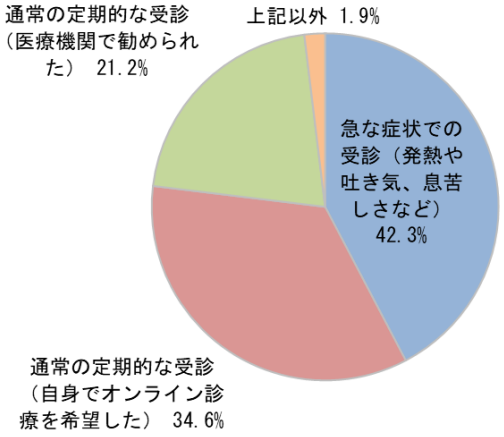
[Q12]オンライン診療を受けた、またはオンライン診療を受けている医療機関について、どのような医療機関か教えてください。※複数ある場合は、最も直近のものをお選びください。(n=52)

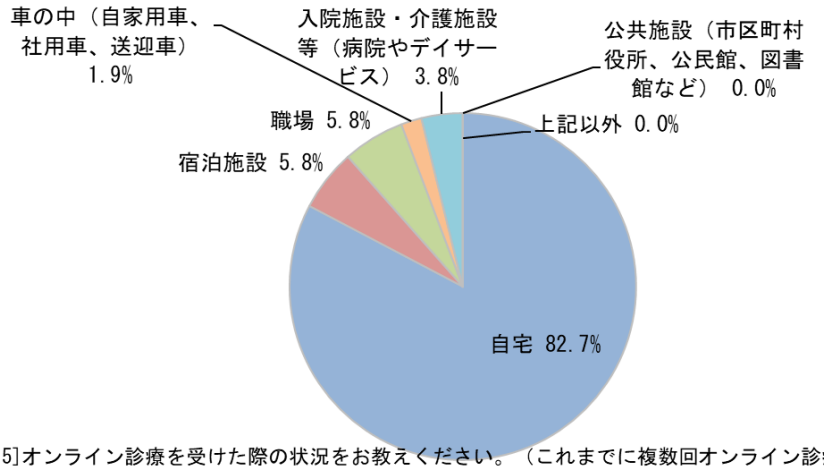


[Q13]オンライン診療を受けた時の症状を教えてください。
(n=52)



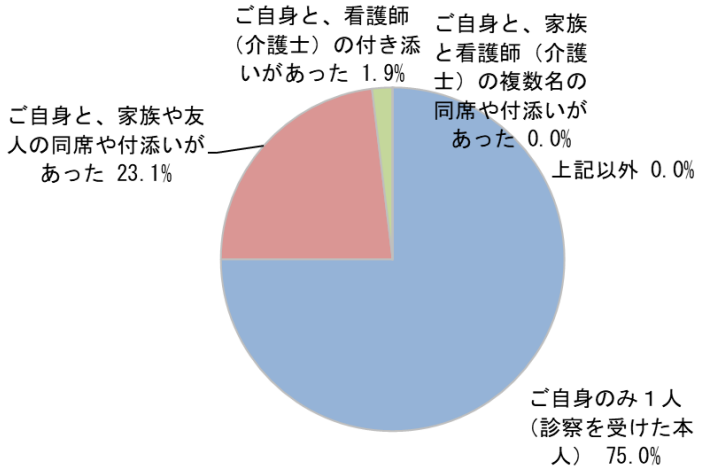
[Q14]オンライン診療を受けた時の状況を教えてください。その受診は急な症状でしたか、慢性的な疾患（例えば糖尿病の治療や皮膚疾患）で定期的な受診でしょうか。（これまでに複数回オンライン診療を受けた場合は、一番最近の受診状況をもとにお答えください。）(n=52)



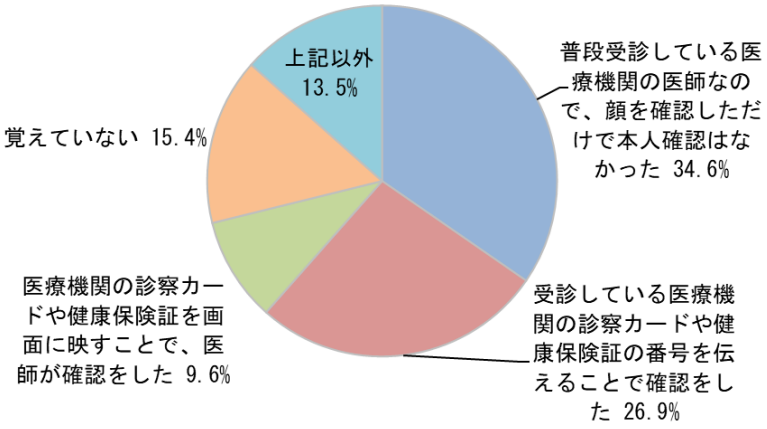


[Q15]オンライン診療を受けた際の状況をお教えください。（これまでに複数回オンライン診療を受けた場合は、一番最近の受診状況をもとにお答えください。）オンライン診療を受けた際の場所（あなたが居た場所）をお答えください。(n=52)

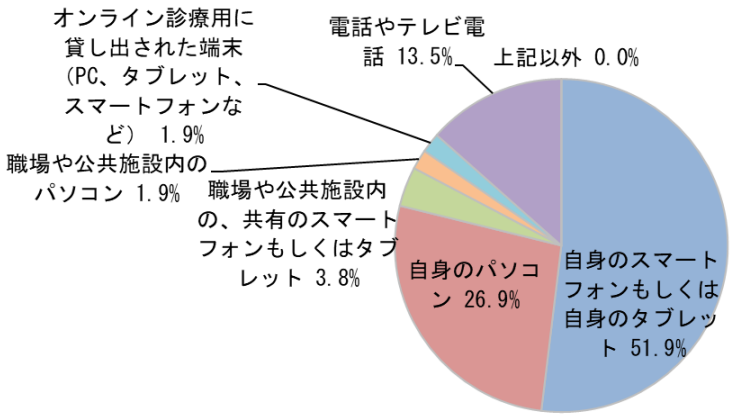
[Q16]オンライン診療を受けた際の状況（ご本人以外に誰がその場所にいたか）を教えてください。（これまでに複数回オンライン診療を受けた場合は、一番最近の受診状況をもとにお答えください。）(n=52)



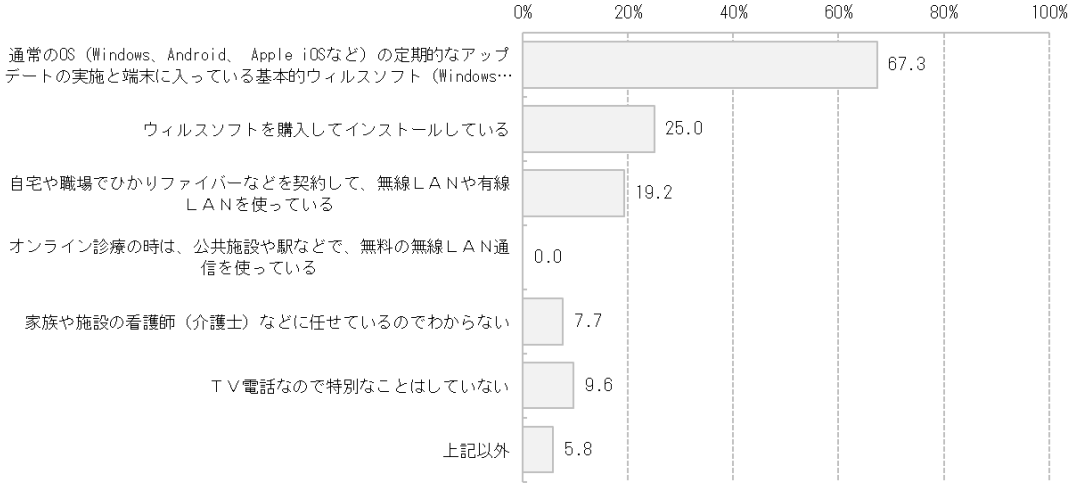
[Q17]オンライン診療での本人確認についてお尋ねします。医師はどのようにあなたの本人確認を行ったかを教えてください。（これまでに複数回オンライン診療を受けた場合は、一番最近の受診状況をもとにお答えください。）(n=52)



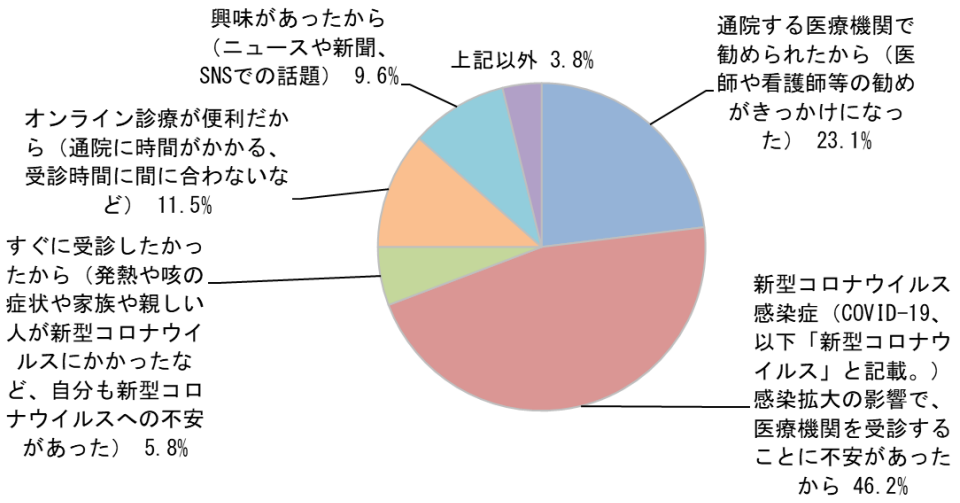
[Q18]オンライン診療で利用している、もしくは利用した機器や端末を教えてください。（これまでに複数回オンライン診療を受けた場合は、一番最近の受診状況をもとにお答えください。）(n=52)



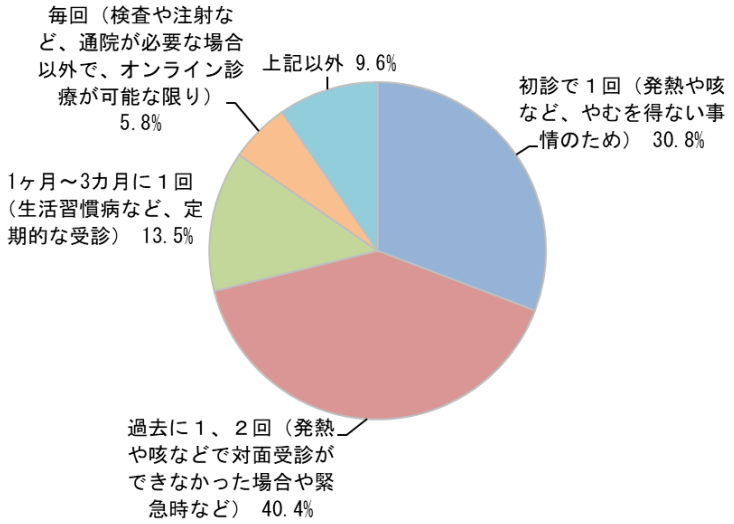
[Q19]オンライン診療で利用している、もしくは利用した機器や端末についてお尋ねします。その機器や端末は、セキュリティ面の措置（ウィルスソフトの導入やアップデートやセキュリティパッチ適用など）についてどのような対応をされていますか。該当するものをすべてお選びください。 (n=52)



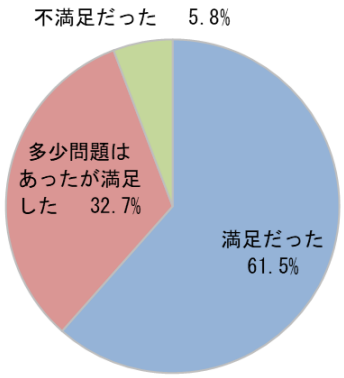
[Q20]オンライン診療を受けた、もしくは受けている理由を教えてください。（複数当てはまる場合は、最も強い理由を１つお選びください。）
(n=52)



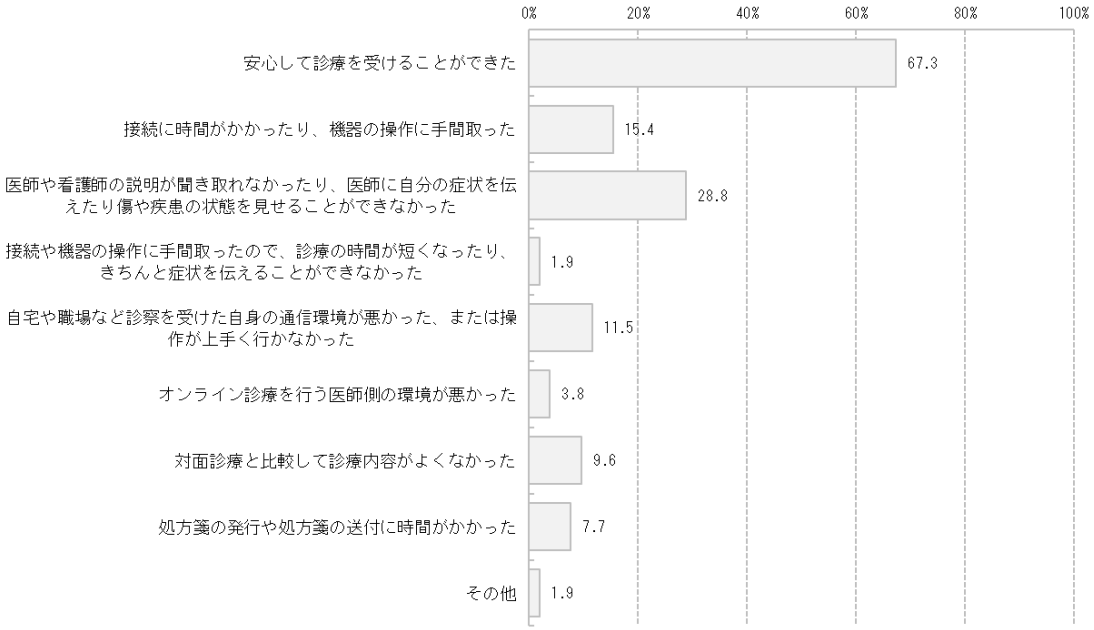
[Q21]オンライン診療を受けた、または受けている頻度を教えてください。
(n=52)



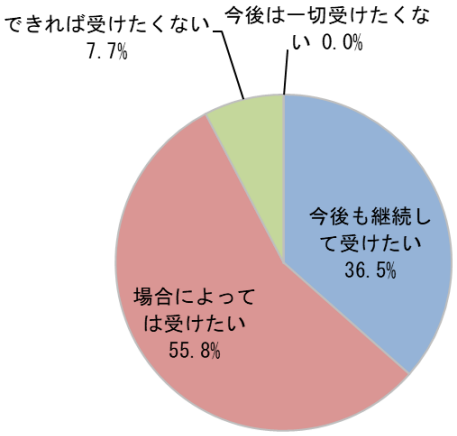
[Q22]オンライン診療を受けた感想を教えてください。オンライン診療について満足しましたか。（複数回オンライン診療を受けられた場合は、一番最近の受診の感想をお選びください。）
(n=52)



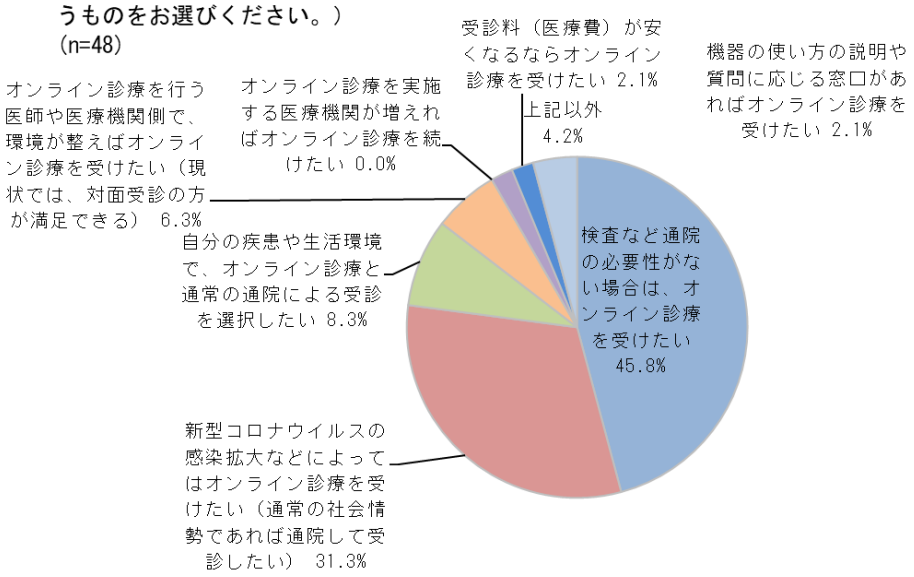
[Q23]オンライン診療を受けられた時の感想について、当てはまるものをすべてお選びください。(n=52)



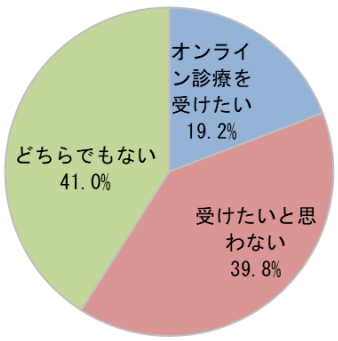
[Q24]オンライン診療を今後も受けたいと考えているかを教えてください。
(n=52)



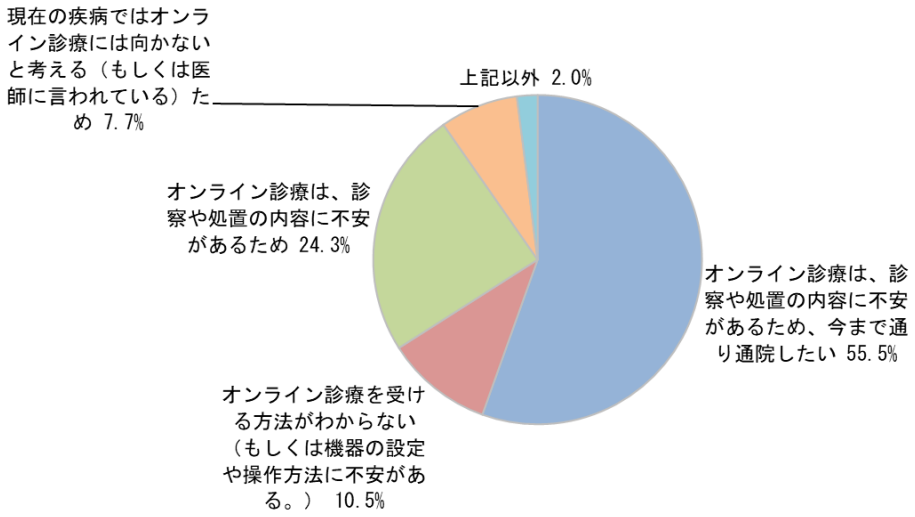
[Q25]オンライン診療を受けたいと思う理由や条件はなんでしょうか。（最も強くそう思うものをお選びください。）
(n=48)



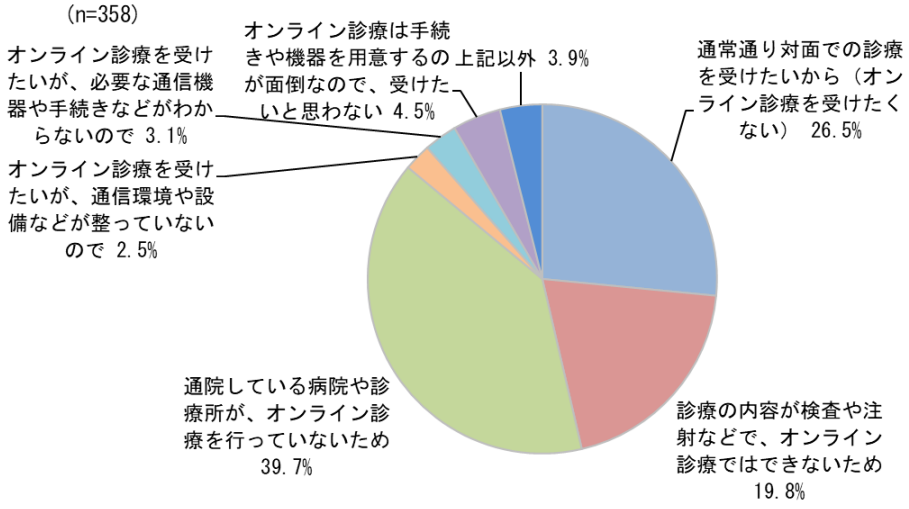
[Q26]「オンライン診療とは」オンライン診療とは、患者が医療機関に赴いて医師の診療を受ける代わりに、スマートフォンなどの情報通信機器※を患者と医師が利活用した上で、医師が患者の診察や診断を行い診断結果の説明や処方等の診療行為を行うことです。通常は、医療機関を受診している患者のうち、症状が落ち着いており医師がオンライン診療で問題ないと判断される患者の場合は、その医療機関のオンライン診療を受けることが可能ですが、今般の新型コロナウイルスの感染拡大を受け、問題がないと医師が判断した場合や...
(n=620)



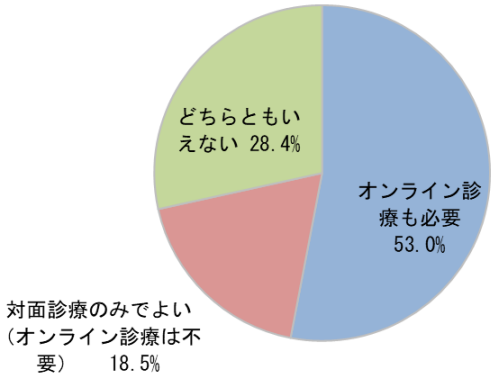
[Q27]前問で、「オンライン診療を受けたいと思わない」と回答された方に伺います。「オンライン診療を受けたいと思わない」理由は何でしょうか。（最も強くそう思うものをお選びください。）(n=247)

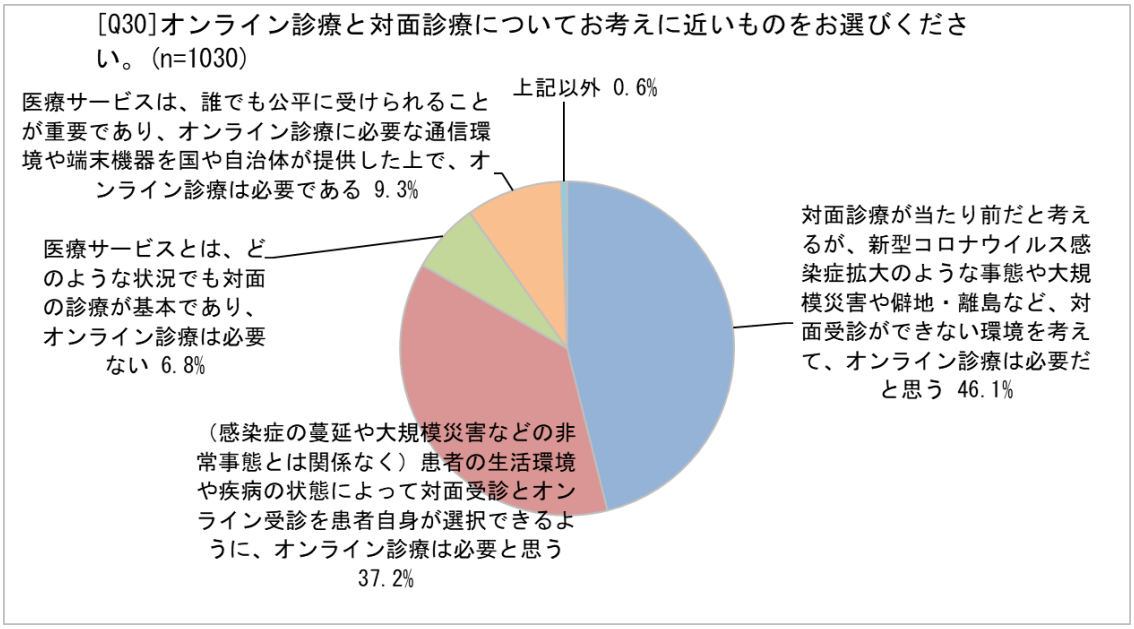


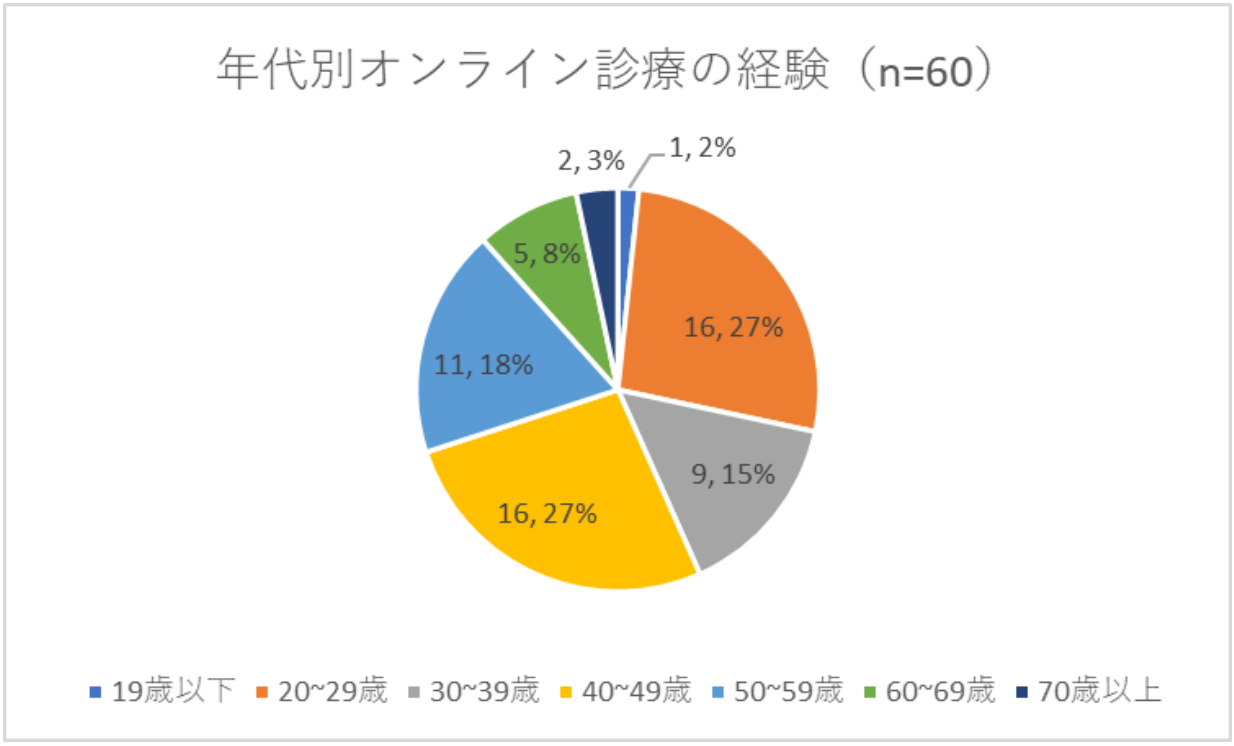
[Q28]「オンライン診療を受けたことがない」と回答した方へお尋ねします。オンライン診療を受けていない、またはオンライン診療を受けることができない理由をお教えください。（該当が複数ある場合は、最も強い理由をお選びください。）
(n=358)



[Q29]通常の対面の診療以外に、オンライン診療が必要と考えますか。(n=1030)







年代別のオンライン診療の経験（n=60）

令和３年度　厚生労働行政推進調査事業費補助金
地域医療基盤開発推進研究事業

分担研究報告書

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（21IA2013）

研究分担者　美代 賢吾
（国立研究開発法人国立国際医療研究センター医療情報基盤センター長）
研究分担者　星本 弘之
（国立研究開発法人国立国際医療研究センター医療情報基盤センター専門職）

研究要旨
令和 2 年度の厚生労働科学研究での調査結果に基づき、医療機関に求められるサイバーセキュリティ対策教育のあり方について検討し、標的型メール対応訓練の実施基盤の開発を行った。開発の結果、標的型メールを模した訓練メールの送信とその開封状況（開封、添付ファイル開封、URL クリック）などの検出機能の実装を行った。次年度以降、多施設対応機能やより有効な訓練メール作成機能の追加実装を行い、医療機関に対する訓練サービスの提供について検討を行う。

A.研究目的

重要インフラに該当する医療分野において、医療機関等のサイバーセキュリティに対する取り組みを強化することは喫緊の課題である。病院情報システムは、これまで外部と隔絶した情報ネットワークであった状況に対し、データヘルス改革、働き方改革、オンライン診療、モバイルヘルス(m-Health)等の導入で外部ネットワークへの接続が始まっている。情報化が進んでいなかった小規模病院、診療所における電子カルテの導入・普及も進みつつある。また、今後、拡大する m-Health 機器（携帯に連携した継続的なモニタリングと適時な介入をする治療アプリを含む。）は病院、診療所のシステムと連携され、研究基盤として活用されることも考慮する必要がある。同時に、進化するクラウド技術により、医療機関内にあったサーバをクラウド上に移行することも現実的になりつつある。

このように急速にネットワーク化され外部との接点が増す医療機関へのサイバーセキュリティ対策への取り組み、適切な教育は喫緊の課題である。主任研究者がおこなう、医療分野におけるサイバーセキュリティ対策と課題についての整理、および医療機関同士が相互にサイバーセキュリティ対策に関する情報共有・相談を行う体制のあり方等の検討状況を参考にしつつ、分担研究者は、医療機関に対する情報セキュリティ教育の方法論や、医療機関が求めるサービスについての検討をおこなう。

B.研究方法

２０２１年度

1. 2020 年度に実施した厚生労働科学特別研究事業「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に関する研究（研究代表者：国立大学法人鳥取大学 近藤博史教授)」で分担研究者が実施した、医療機関のサイバーセキュリティ実態調査を参考に、医療機関の体制にあった教育方法、ニーズの検討をおこなう。
2. 検討した教育方法、ニーズに基づき、医療機関への教育・対策につながる、オンラインサービスのプロトタイプ的なシステムの構築をおこなう。
3. 必要に応じて、国内での実際の医療機関の状況についてヒアリングとともに情報セキュリ

ティ対策のニーズ等について情報収集をおこなう。
4. 得られた知見及び成果について、関連学会で報告する

２０２２年度
1. 2021 年度に構築したプロトタイプシステムの評価をおこない、医療機関が求めるサービスのニーズについて、考察をおこなう
2. 必要に応じて、国内での実際の医療機関の状況についてヒアリングとともに情報セキュリティ対策のニーズ等について、追加の情報収集をおこなう。
3. 医療機関の求める、教育ニーズ、対策ニーズについて、全体の手順書の一部としてまとめる。
4. 得られた知見及び成果について、関連学会で報告する

C．研究結果

1. 方法

2021 年度の研究では、2020 年度に分担研究者が実施した医療機関のサイバーセキュリティ実態調査の結果に基づき、医療機関に必要と考えられるサイバーセキュリティ教育のあり方について検討を行った。

実態調査は 4000 病院に対して回答を依頼し、508 病院より回答を得た。結果の詳細については、文献 1 にまとまっているが、概要としては、サイバーセキュリティ教育は全体の約 39%（198/508）の病院で実施しているが、サイバーセキュリティ訓練は約 7.7%（39/508）の実施率と大幅に実施率が下がっていること、さらに開設主体別の分析では、国・大学が開設した施設では 42.9%(12/28)

がサイバーセキュリティ訓練を実施しているが、民間では 3.6%（11/304）と大幅に実施率が下がっていることから、セキュリティ訓練を容易に実施できる基盤の整備が有効であると考えられた。また、分担研究者の所属機関におけるサイバーセキュリティ事案のヒアリングの結果、標的型メールなどの情報提供はその他の業務上のメールなどに紛れて、きちんと読まれていない実態が明らかとなっており、情報提供以外に実際のメールでの訓練が有効であると考えられたこと。また、昨今のサイバー攻撃の事案を考慮し、emotet などの標的型メール攻撃に分類されるものが事例としても多く見られたことから、標的型メール対応訓練の実施基盤を開発することとし、必要な機能についての整理を行った。

2. 標的型メール対応訓練の実施基盤の仕様

標的型メール対応訓練基盤としては、必要な機能について調査と検討を行った結果、以下の機能が必要と判断された。

■メール送信機能
1）登録した複数のメールアドレスに対して、訓練メールを送信する機能
2）メールの内容（本文、フィッシングを模したＵＲＬ情報、題名、発信元メールアドレス、発信元メールアドレス表示名）を任意に設定可能であること

■メールの扱いの検知機能
以下、送信したメールアドレスごとに
3）送信したメールの開封の有無の検知機能
4）フィッシングを想定した URL へのアクセスの有無の検知機能
5）マルウェアを模した添付ファイルの開封検知機能

■管理機能
6）訓練結果の集計・表示機能（開封率、URL アクセス率、添付ファイル開封率、など）
7）複数施設で並行して訓練実施可能であること
8）参加施設ごとに訓練結果の集計表が出力可能であること

3. 開発結果

2021 年度は、開発工数の関係から 1）,3）～6）までについて開発と検証を行うこととした。2）については、本文テキストは手動で設定することとし、メール本文に埋め込むＵＲＬについては検出機能との連携の関係からシステムが自動的に作成することとした。また、メールアドレス表示名の任意設定については、プロトタイプでは省略することとした。

メール開封、URL アクセス、添付ファイル開封の判定については、HTML メールおよび HTML 形式の添付ファイルを用い、Web サーバにアクセスが行われたかによって判定することとした。

以下、図 1 にメール作成画面のキャプチャ、図 2 に送信されたメールのイメージ、図 3 に管理画面のキャプチャを示す。

図 1 : メール作成画面 :　件名と本文は任意に設定可能。埋め込み URL と添付ファイル名は自動生成されるため、表示されていない。

図 2：送信されたスパムメール（仮）：本文や送信アドレス、URL などの偽装については機能検証のため省略している。また、HTML 形式メールのため、開封判定のために外部参照している画像の表示がメールクライアントの機能でブロックされている。

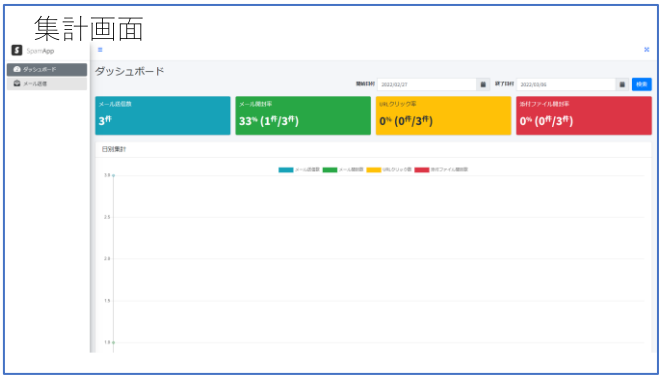


図 3：集計画面：メール送信数、開封率、ＵＲＬクリック率、添付ファイル開封率が集計可能。多施設対応は未実装。

D．考察

開発したシステムの試験運用の結果、メール開封、URL クリック、添付ファイル開封の検出は可能であった。但し、メール開封判定が HTML メールに埋め込んだ特定の画像が表示されたかで行っているため、プレビュー表示が無効に設定されている電子メールクライアントの場合、開封して本文の文字情報を表示しても Web サーバ上の画像へのアクセスがプレビュー抑止のため作動せず、開封の検出ができない場合があることが明らかとなった(結果図 2 参照)。

これについては、セキュリティ上の理由からプレビュー機能が初期段階では無効とされていることから、セキュリティ的にはより安全側になる設定であるため、この環境にも関わらず開封が検出されたケースはよりセキュリティ上の問題につながる可能性があることから、より対応に注意が必要であると考えられる。

なお、現時点の評価システムでは、以下の機能が未実装であることから、より訓練効果の高いダミーメール送信を実現するため、以下の点の追加開発が必要であると考えられる。

1）メール送信アドレスの表示名部分を任意に設定：標的型メールの多くの事例では、表示名が知人（上司、同僚、取引先関係者、など）となっているケースが多いため。

2）埋め込みＵＲＬ表示名を任意に設定：　同じく、認証画面や資料入手画面などへのリンクが設定されているケースが多いため。

3）添付ファイルを html 以外にＷｏｒｄ形式なども可能に：　同じく、Word のマクロによりマルウェア本体のダウンロードを行うものも存在するため。

本システムの実装とサービスの提供により、中小規模医療機関などにおける標的型メール対応訓練の実施率向上が期待できることから、医療機関のサイバーセキュリティレベルの向上が期待される。

E．結論

本システムの開発により、標的型メール対応訓練の実施基盤のプロトタイプ開発と検証を行った。その結果、開封判定には一部不可能なケースが存在することが明らかとなったが、これはセキュリティ的にはより安全な側の設定であり問題とはならないと考えられた。今後は、実際に多施設での訓練に適用し、その効果や訓練メールのあり方についての検討を進める。

F．健康危険情報

特になし

G．研究発表

1．論文発表

特になし

2．学会発表

特になし

3．その他

(1) 美代賢吾. 医療機関とサイバー攻撃標的型攻撃とランサムウェアを中心に. 週刊医学界新聞, 3411. 医学書院, 2021.

(2) 美代賢吾. 医療情報システムと新興感染症・災害・サイバー攻撃を考える；医療者・患者を支援し、診療を継続するために. IT Vision, 43：42-43, 2021.

H．知的財産権の出願・登録状況（予定を含む。）

特になし

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。

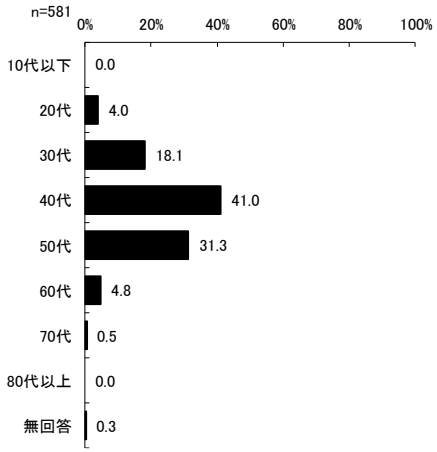
２．調査結果

（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。

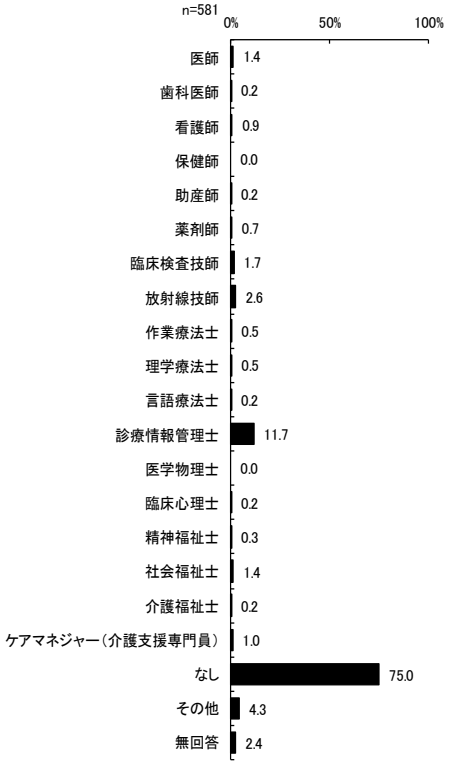
図表 1　年齢（Q1）



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。

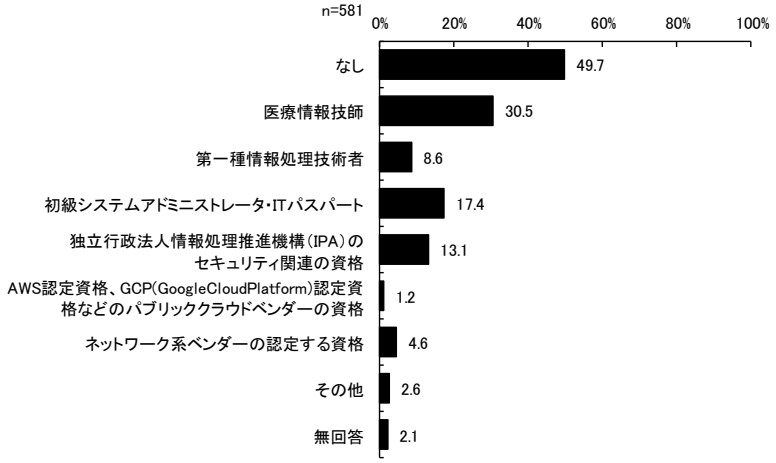
図表 2　保有している医療系の資格（Q2）【複数回答】



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】



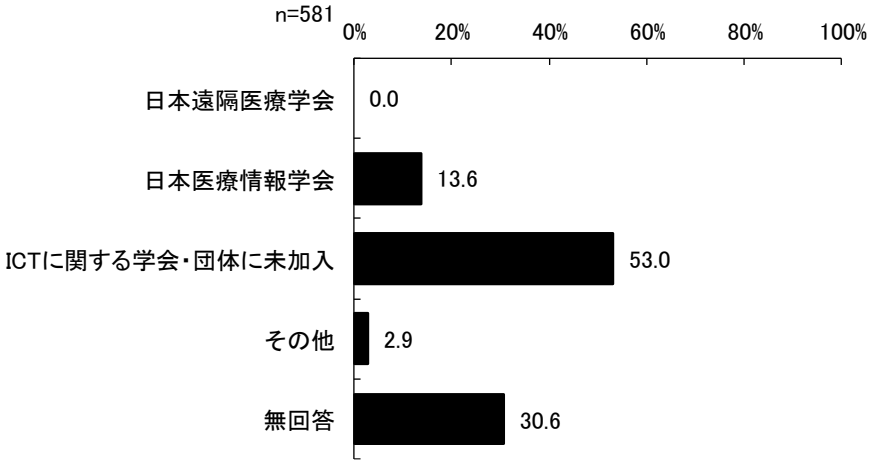
※「その他」の主な回答は以下の通り。

- 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】

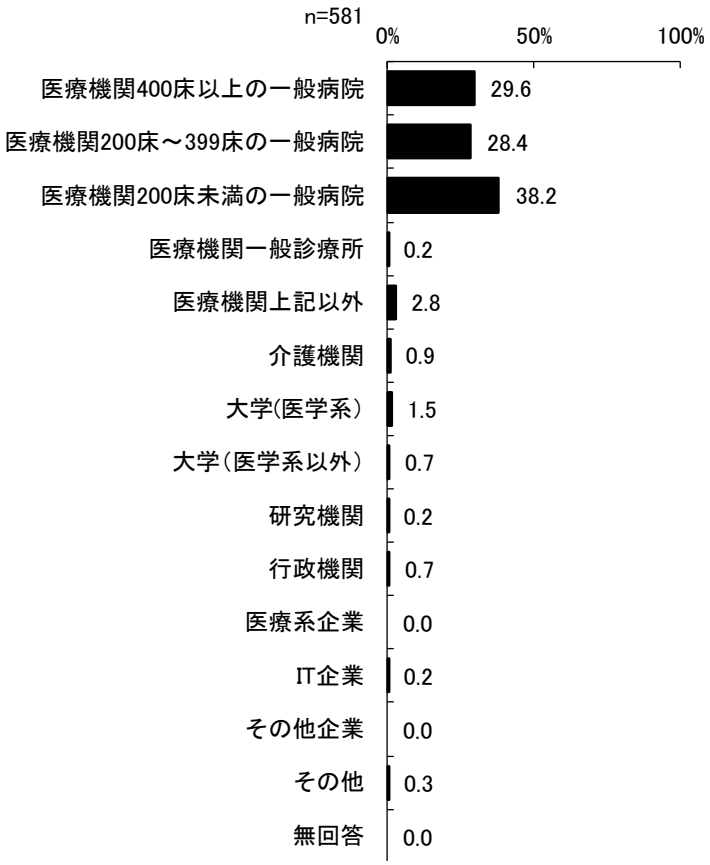


※「その他」の主な回答は以下の通り。
- ユーザー会内 セキュリティ分科会
- 医療情報技師育成部会
- 医療情報技師会
- 九州沖縄医療情報技師会
- 熊本県医療情報システム研究会
- 電子通信情報学会
- 日本医療情報学会

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。

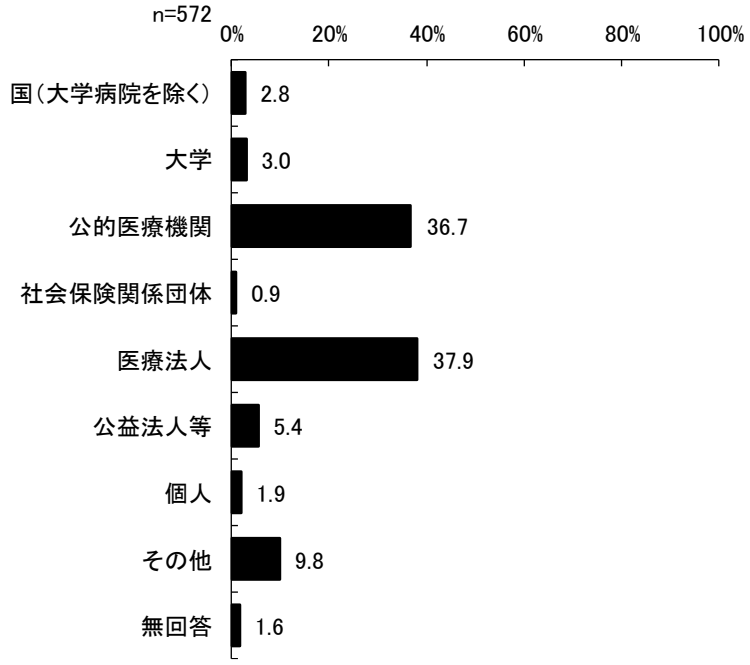
図表 5　所属機関（Q5）【複数回答】



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）



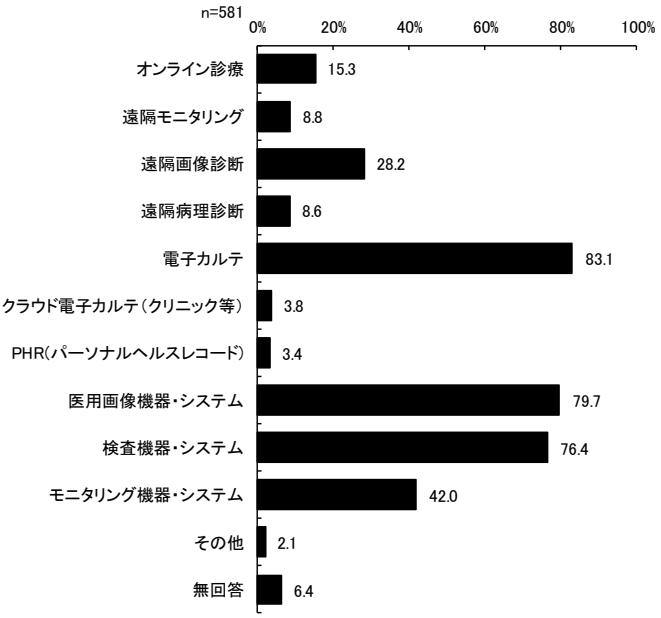
※「その他」の主な回答は以下の通り。

- 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】

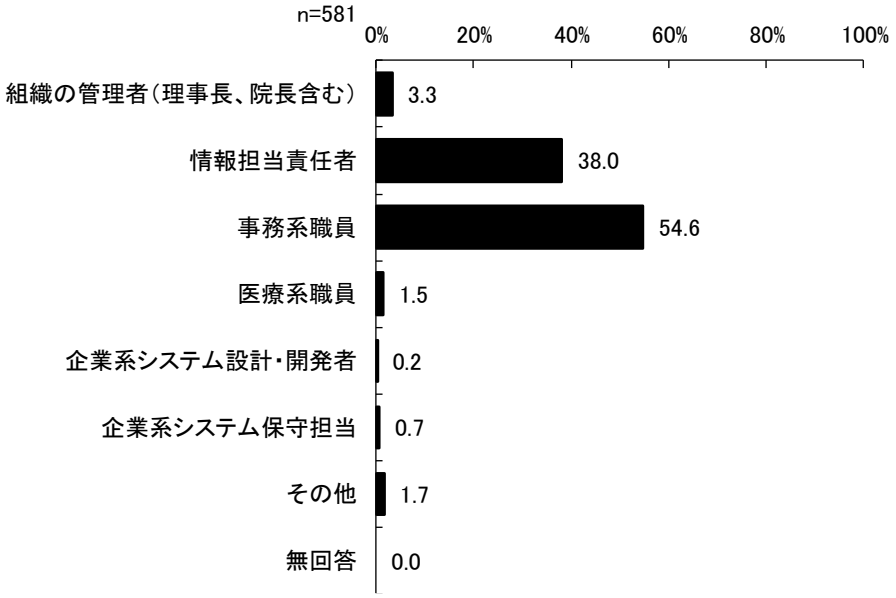


※「その他」の主な回答は以下の通り。
- オーダリングシステム
- オンラインセカンドオピニオン
- リモート面会
- 医事会計
- 医療情報共有システム
- 画像検査 Web 予約システム
- 外注検査受託システム
- 紹介 Web 予約システム
- 地域医療連携システム
- 転院調整システム
- 文書管理システム

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）

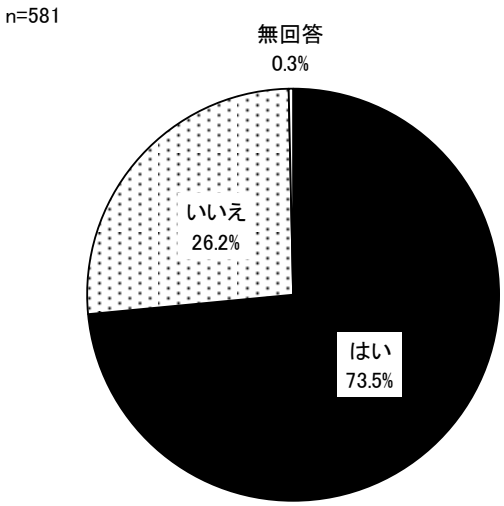


※「その他」の主な回答は以下の通り。
- 医事系部門責任者
- 医療系職員と情報担当の兼務
- 医療情報技師
- 医療情報担当
- 情報システム担当者
- 情報管理係
- 情報担当者

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）



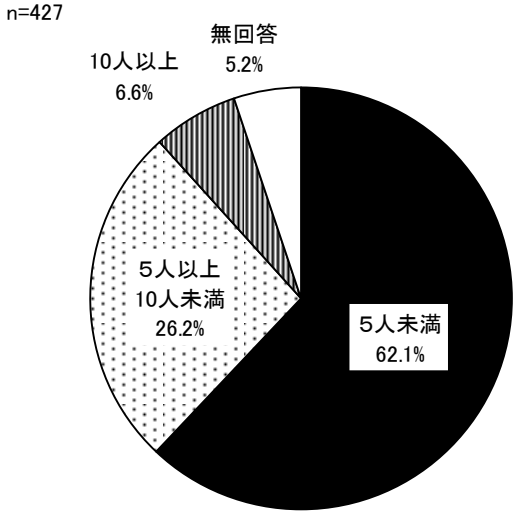
図表 10　情報システムを統括する部署はあるか（Q9）と所属機関（Q5）のクロス集計結果

	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。

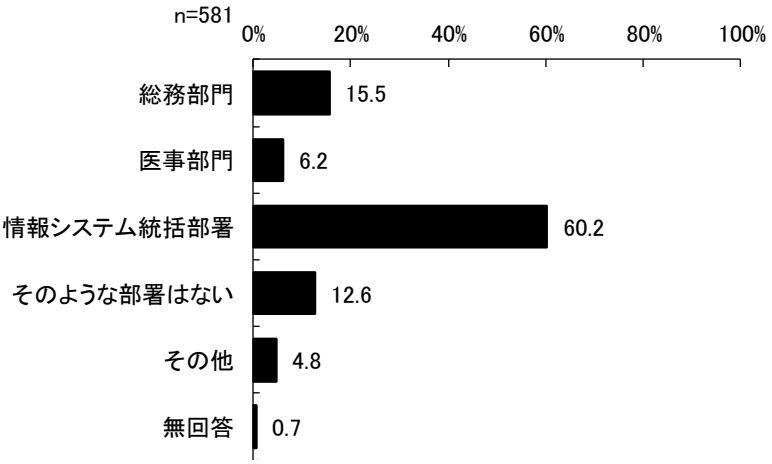
図表 11　情報システムを統括する部署の所属人数（Q10）



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）



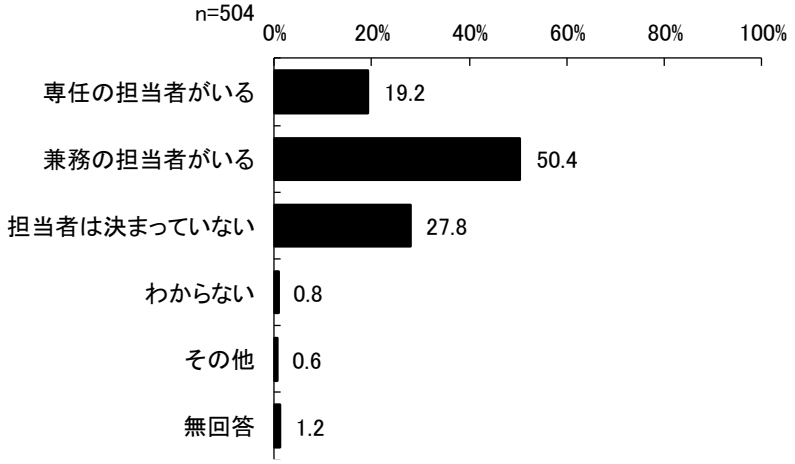
※「その他」の主な回答は以下の通り。

- 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）

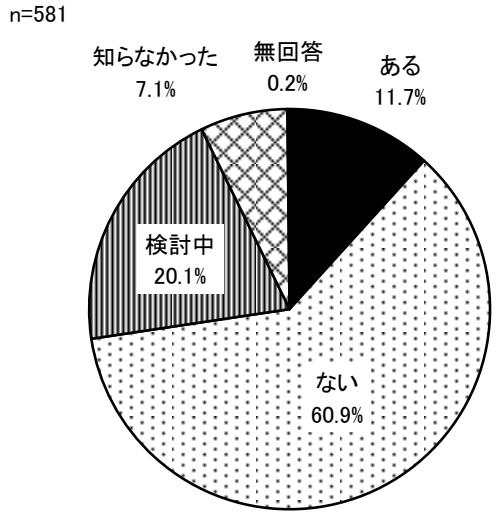
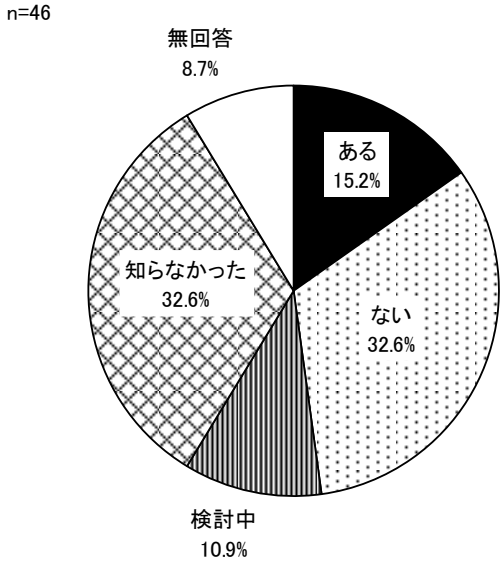
	調査数	平均値	標準偏差	中央値	最小値	最大値
非常勤の兼務者(今年度)	133	0.2	0.74	0.00	0.00	7.00
非常勤の兼務者(昨年度)	6	0.17	0.37	0.00	0.00	1.00

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

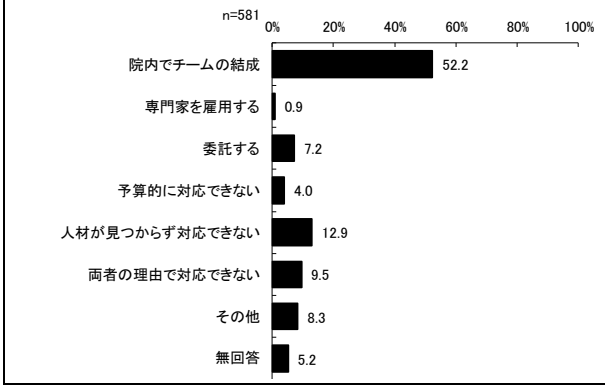
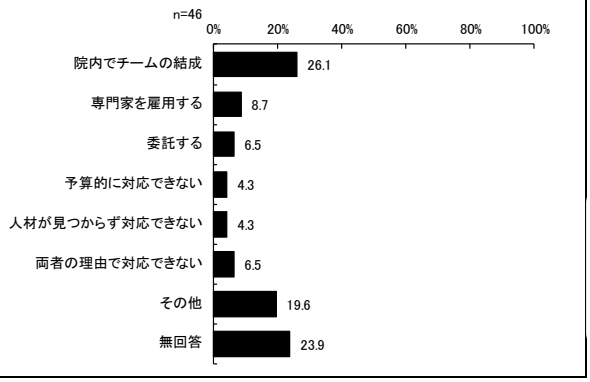
図表 18　所属する組織にCSIRTはあるか（Q17）

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）

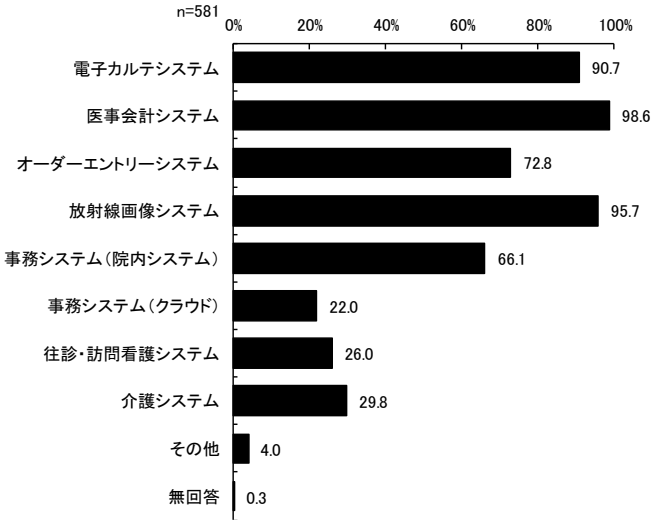
今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

※「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】

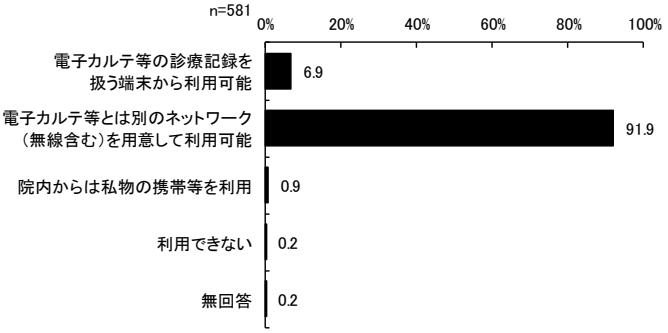


※「その他」の主な回答は以下の通り。
・医療情報部門系システムが多数
・遠隔読影システム
・患者向けスマートフォン用アプリケーション
・給食システム
・健診システム
・検査システム
・検体検査システム
・材料管理
・歯科技工
・手術部門システム
・生理検査システム
・地域医療連携に関するシステム
・調剤管理システム
・透析システム
・入退室管理システム
・病歴管理システム等
・予約管理
・臨床検査

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。

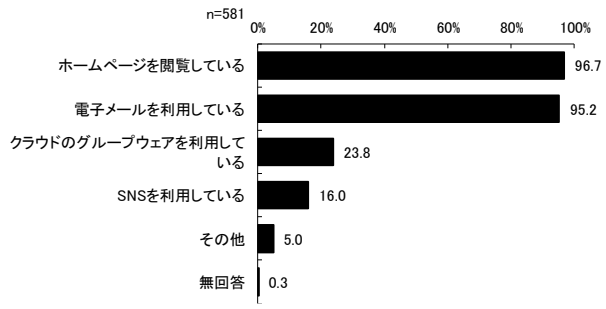
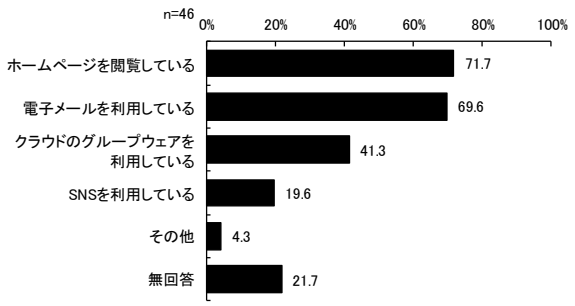
図表 21　院内における職員のインターネットの利用可否（Q20）



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
	

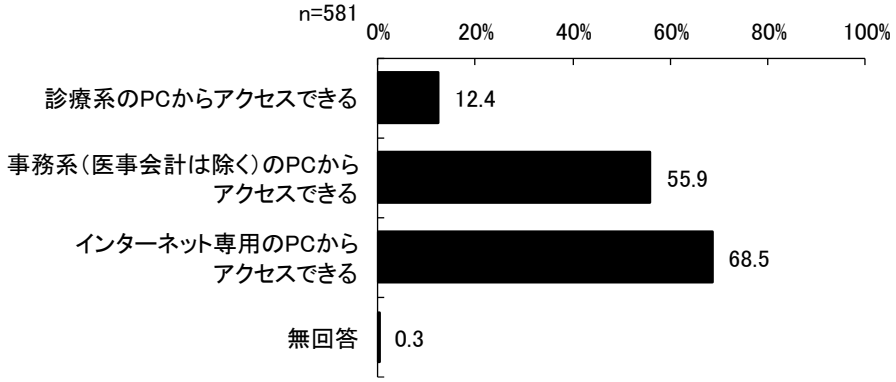
※「その他」の主な回答は以下の通り。
・NCD 登録等
・Office365
・SNS に関しては病院情報公開用アカウント
・UTM で防御されるもの以外は特にフィルタしていない
・WEB 会議
・オンプレのグループウェアを利用している
・オンライン講習等の受講
・クラウドの業務システムを利用（訪問・居宅）
・レセプトデータの送信、健康保険証のオンライン資格確認
・医薬品発注

・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。

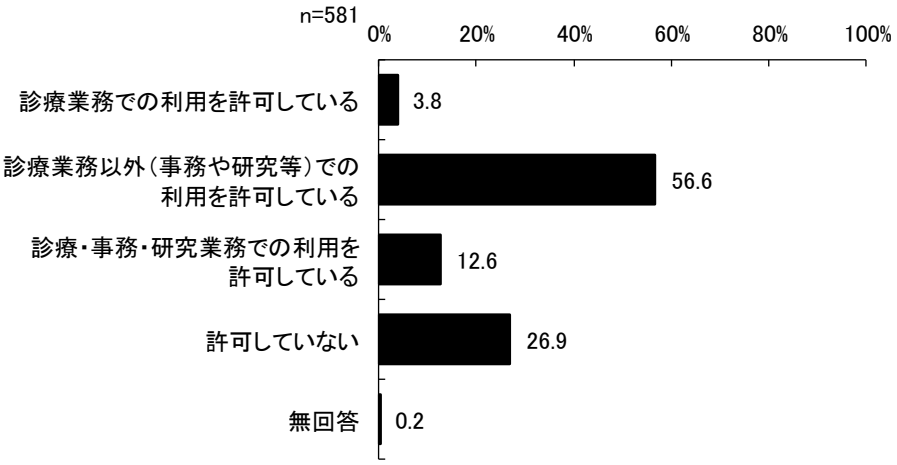
図表23　インターネットにアクセスできるパソコン（PC）について（Q22）【複数回答】



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。

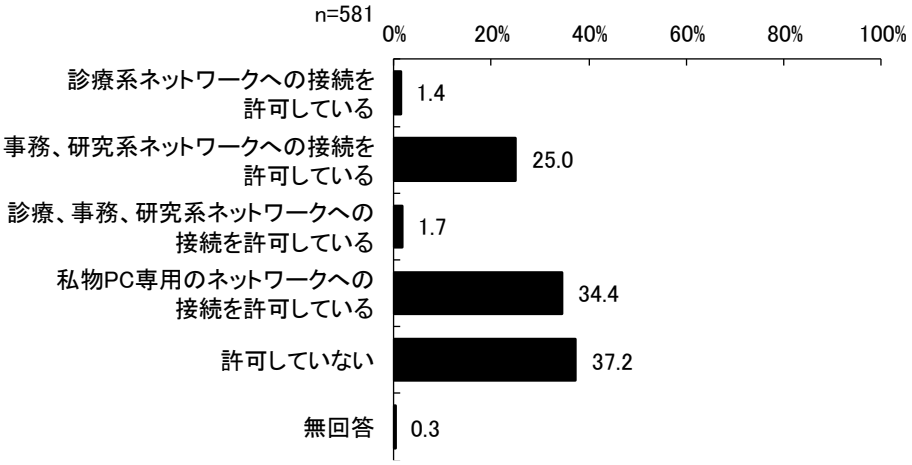
図表24　職員（医師など）の私物のPCを用いて業務を行うことを許可しているか（Q23）



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）

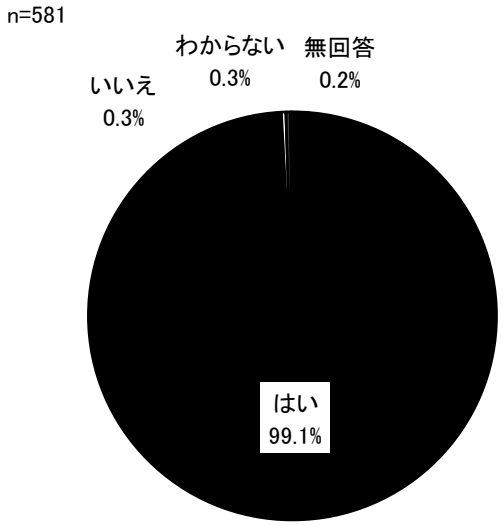


(2)組織で実施しているセキュリティ対策

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。

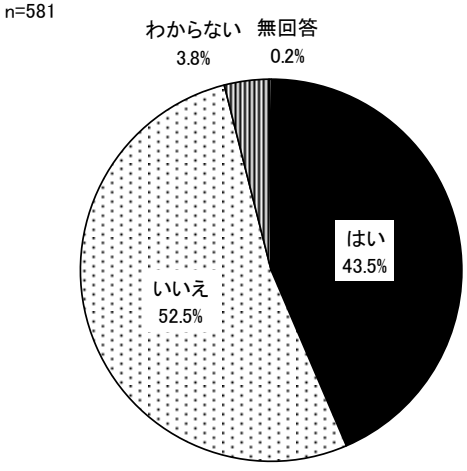
図表 26　ウイルス対策ソフトを導入しているか（Q25）



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）



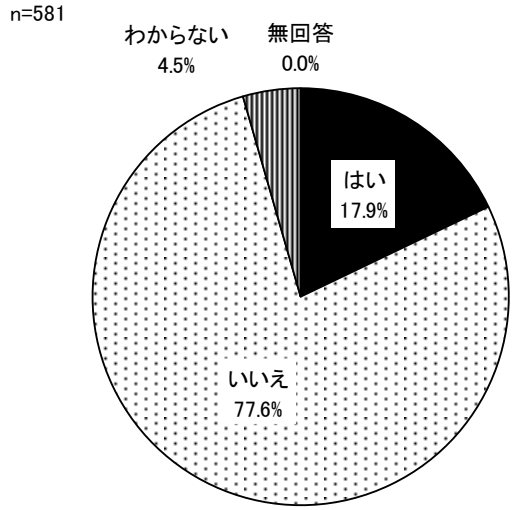
図表 28　資産管理ソフトを導入しているか（Q26）と所属機関（Q5）のクロス集計結果

	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。

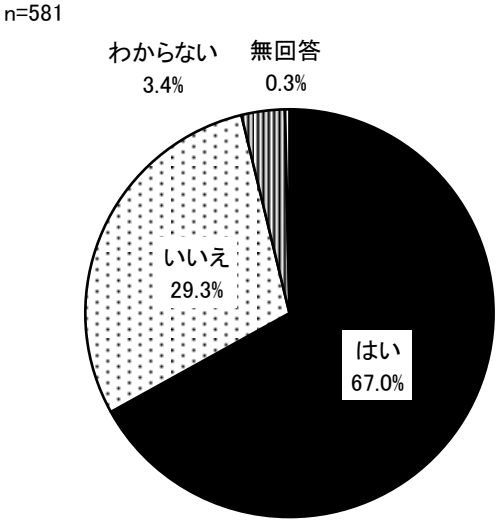
図表 29　仮想ブラウザを導入しているか（Q27）



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）



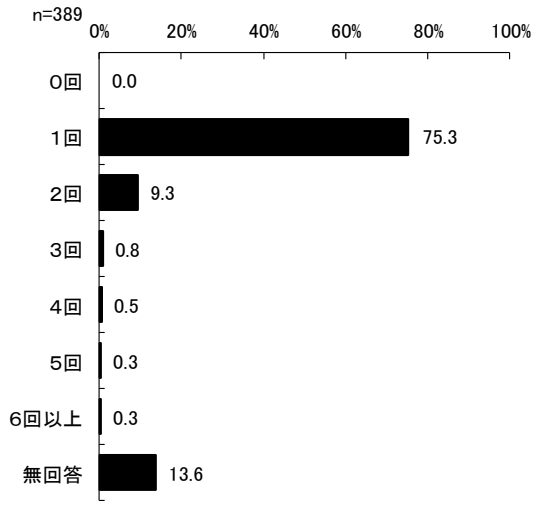
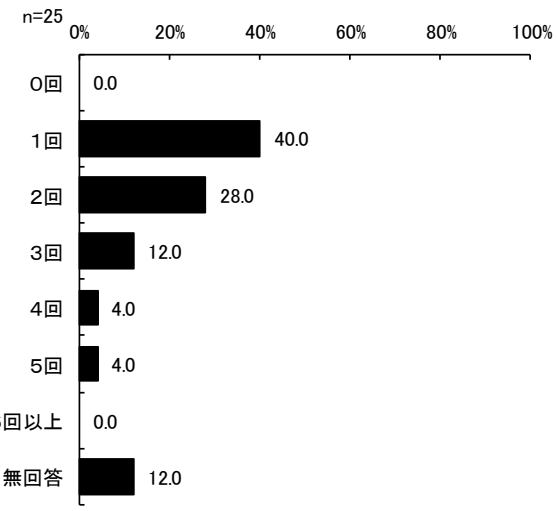
図表 31　セキュリティ教育を行っているか（Q28）と所属機関（Q5）のクロス集計結果

	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。

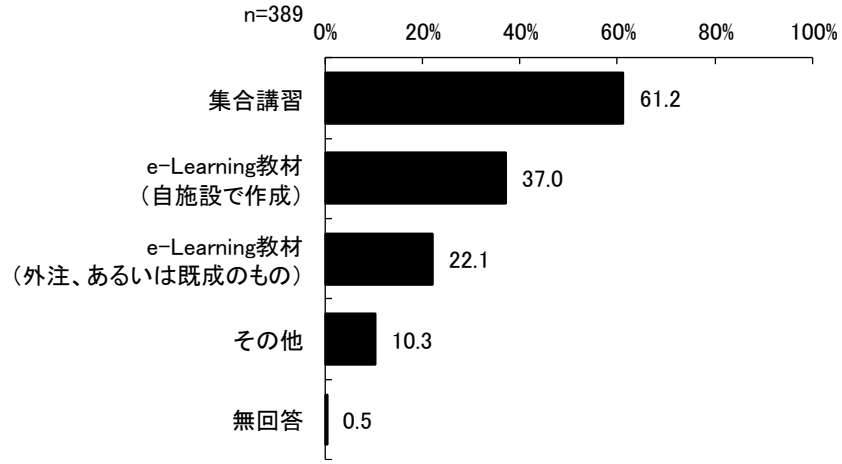
図表 32　セキュリティ教育は年に何回行っているか（Q29）

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】

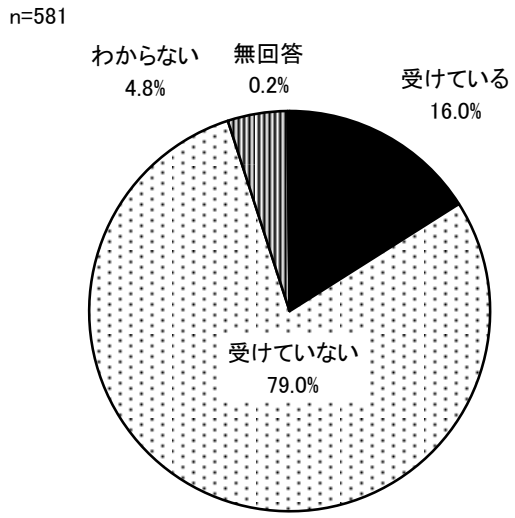
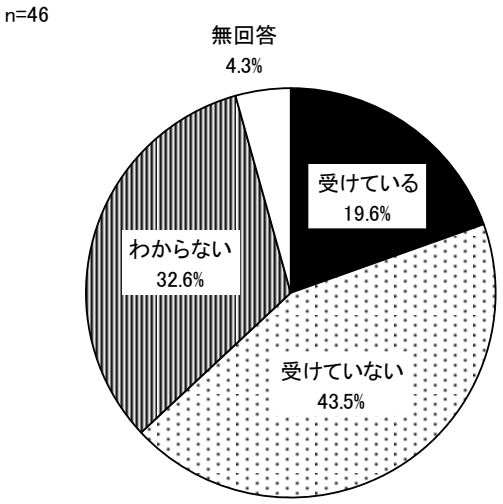


※「その他」の主な回答は以下の通り。
・DVDを各部署に配布
・e-Learning（自施設作成と外注のハイブリッド）
・e-Learning教材（本部が作成）
・WEB動画
・WEB配信形式
・イントラネット内メールと添付ファイル
・コロナ禍のため資料掲載
・ニュース発行
・グループウェアでの院内資料配布
・メールなどによる模擬訓練等
・院内メールで事例共有
・院内メッセンジャーを使った、自己作成コンテンツ
・会議資料
・会議等で口頭説明
・研修資料配布と理解度テスト
・個人での研修動画視聴による研修
・厚生労働省が作成している医療機関等向けサイバーセキュリティ研修
・厚生労働省作成の研修素材
・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）

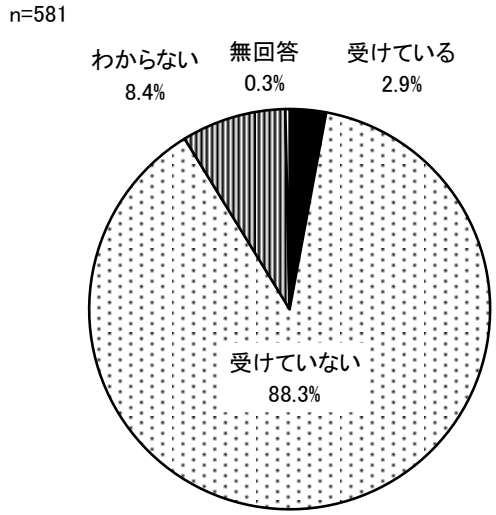
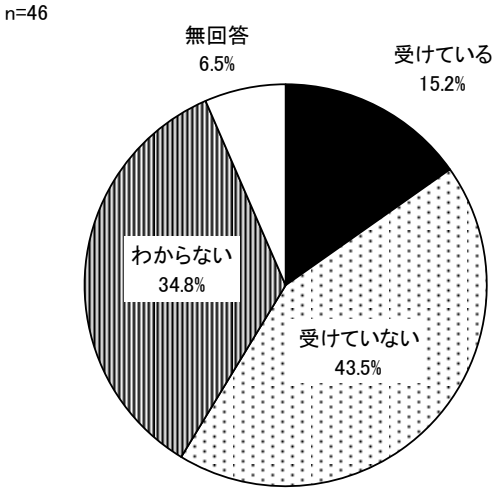
今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

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

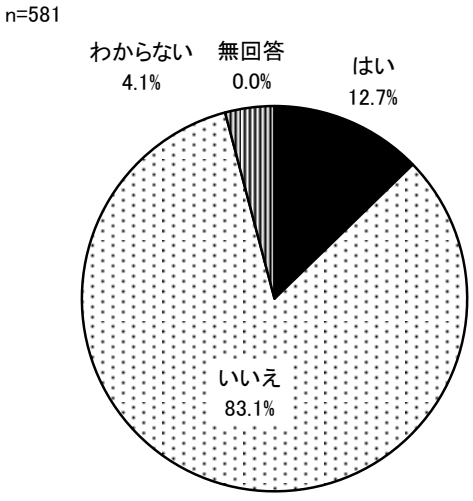
図表 35　ペネトレーションテストを受けているか（直近 3 年以内の状況）（Q32）

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）

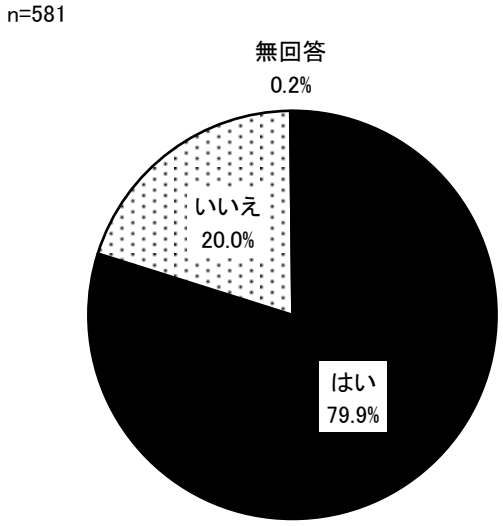


（3）施設内での規定の有無等

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。

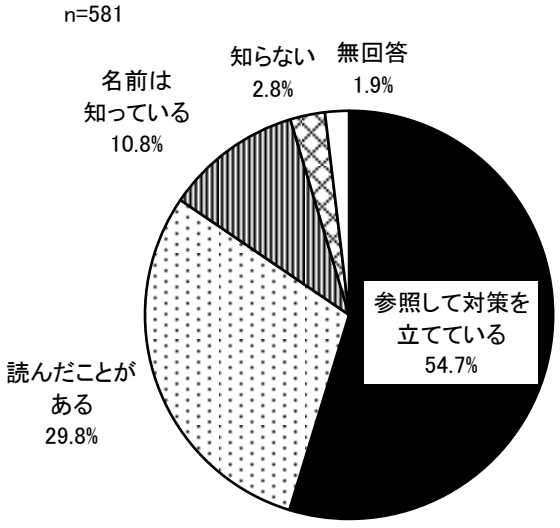
図表 37　情報セキュリティポリシーを規定しているか（Q34）



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。

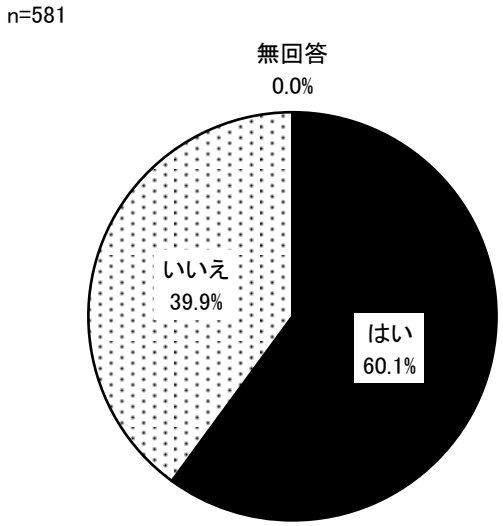
図表 38　厚生労働省の「医療情報システムの安全管理に関するガイドライン」の認知状況等（Q35）



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

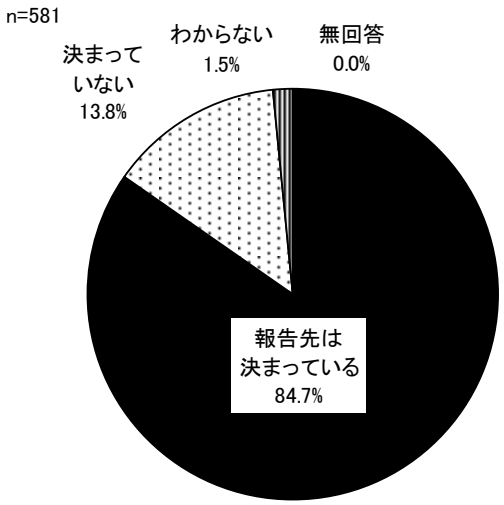
	調査数	はい	いいえ
医療機関 400床以上の一般病院	172	128	44
	100.0	74.4	25.6
医療機関 200床～399床の一般病院	165	93	72
	100.0	56.4	43.6
医療機関 200床未満の一般病院	222	118	104
	100.0	53.2	46.8
医療機関 一般診療所	1	－	1
	100.0	－	100.0
医療機関 上記以外	16	6	10
	100.0	37.5	62.5
介護機関	5	3	2
	100.0	60.0	40.0
大学(医学系)	9	7	2
	100.0	77.8	22.2
大学（医学系以外）	4	4	－
	100.0	100.0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

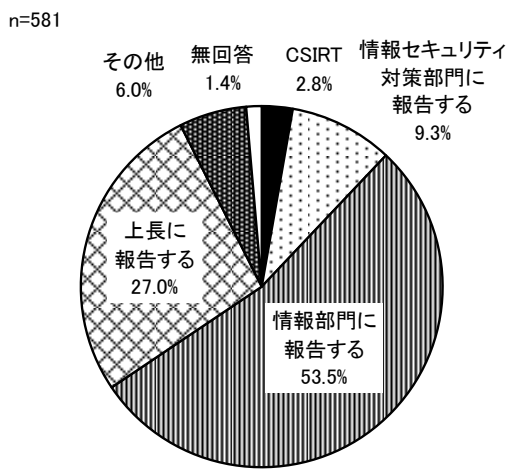
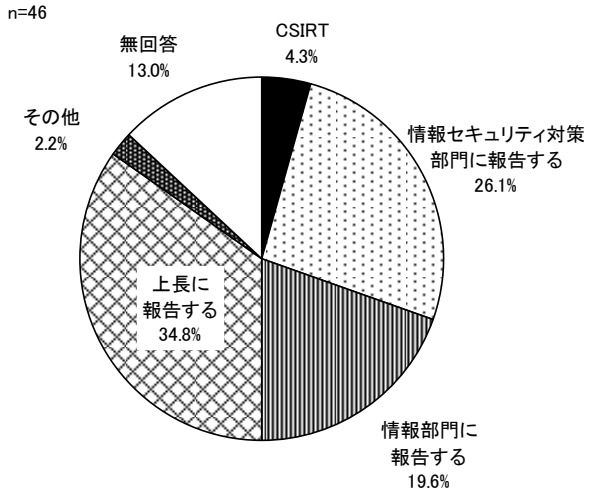
図表 41　職員がセキュリティインシデントを発見したときに報告する部署が決まっているか（Q37）



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）

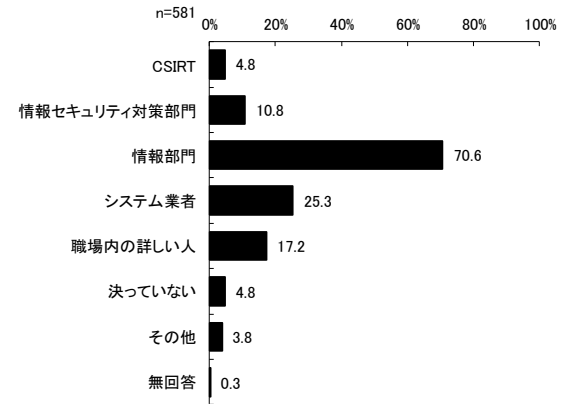
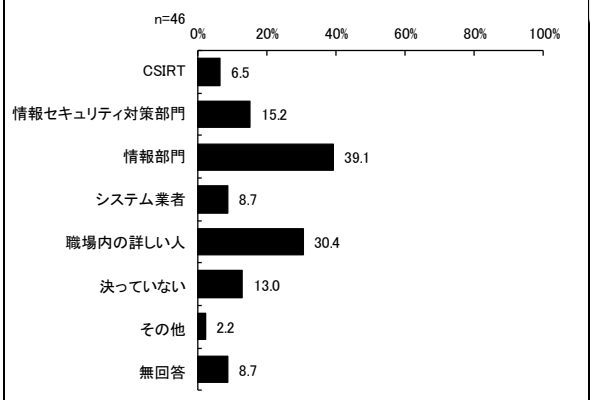
今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

※「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】

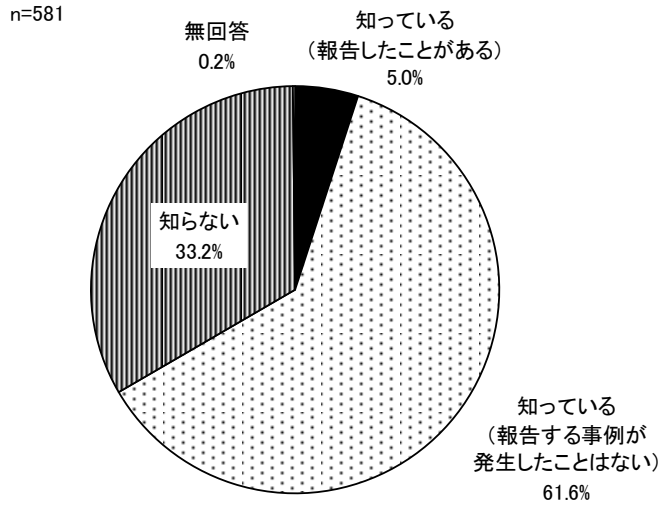
今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

※「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。

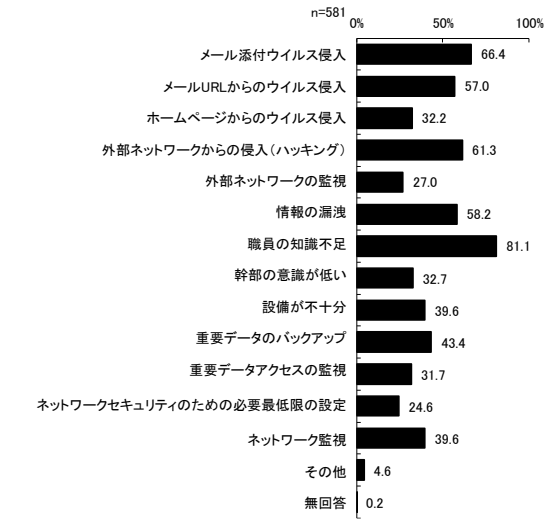
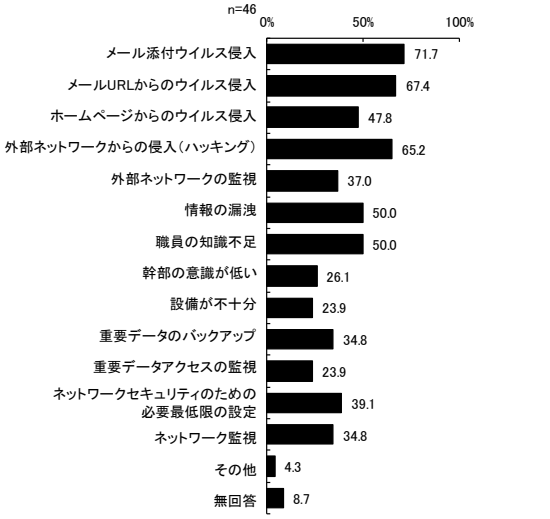
図表 44　情報セキュリティインシデント発生時の厚生労働省の窓口を知っているか（Q40）



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】

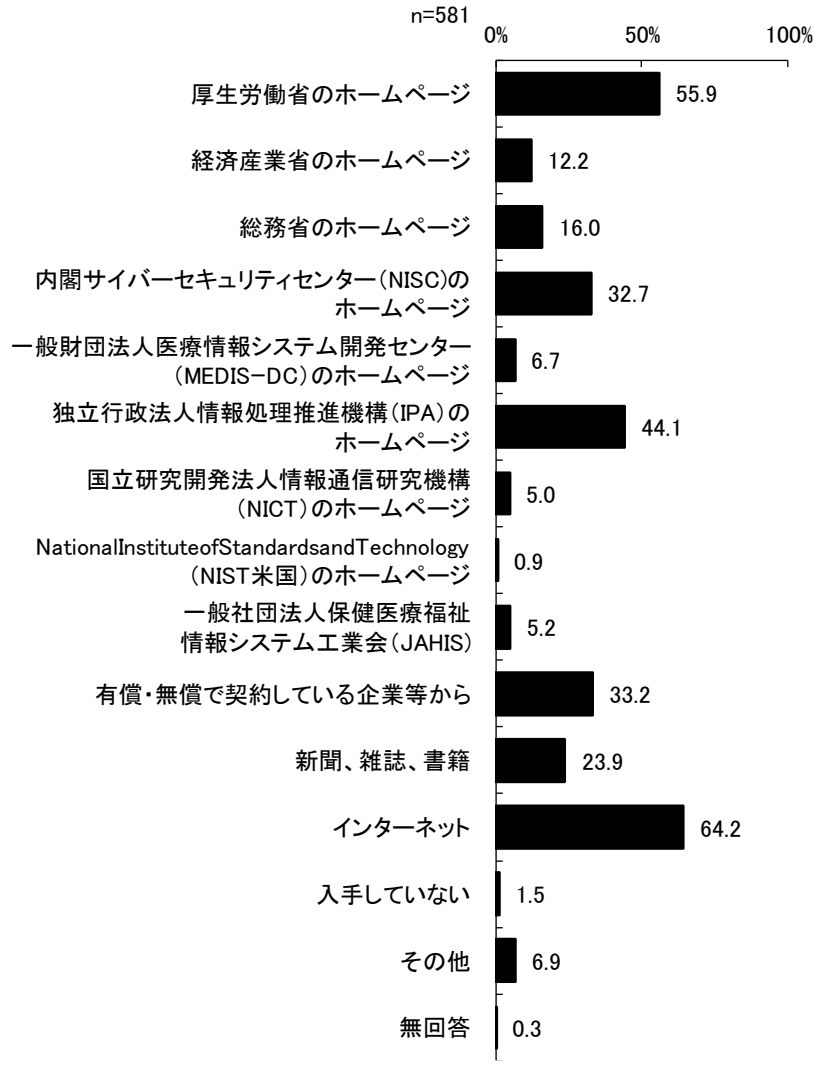
今年度（日本病院会）調査結果	昨年度（令和 3 年度）（日本遠隔医療学会）調査結果
	

※「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）】



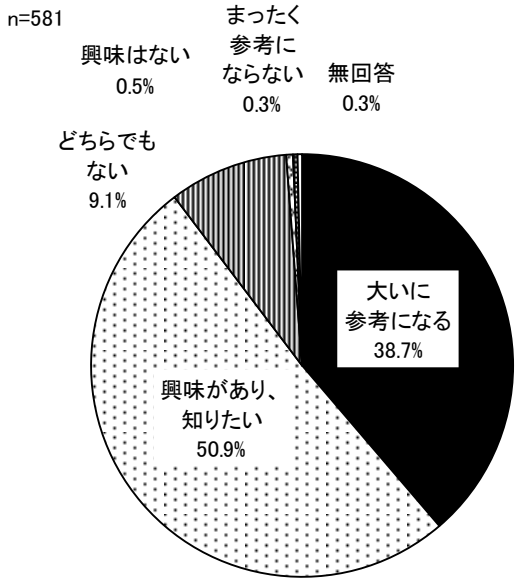
※「その他」の主な回答は以下の通り。
・本部からの情報
・JPCERT のホームページ
・システム業者
・システム提供業者
・セキュリティ関連会社からの情報提供
・医療 ISAC
・医療系の雑誌
・医療情報技師会
・一般社団法人日本病院会
・都道府県の警察公安課サイバー攻撃対策係
・加入団体からの情報提供
・各種セミナー

・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。

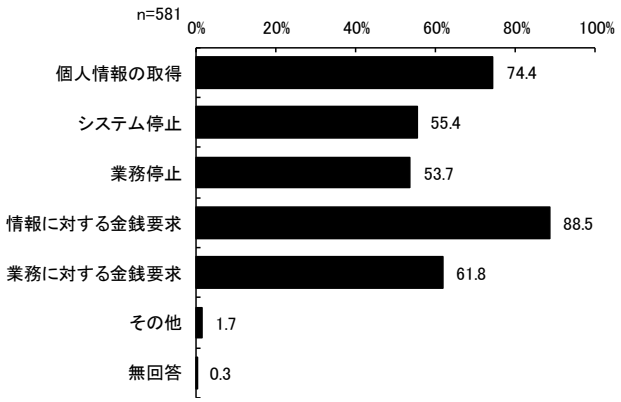
図表 47　他の施設の対策状況は対策を立てる上で参考になるか（Q43）



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】

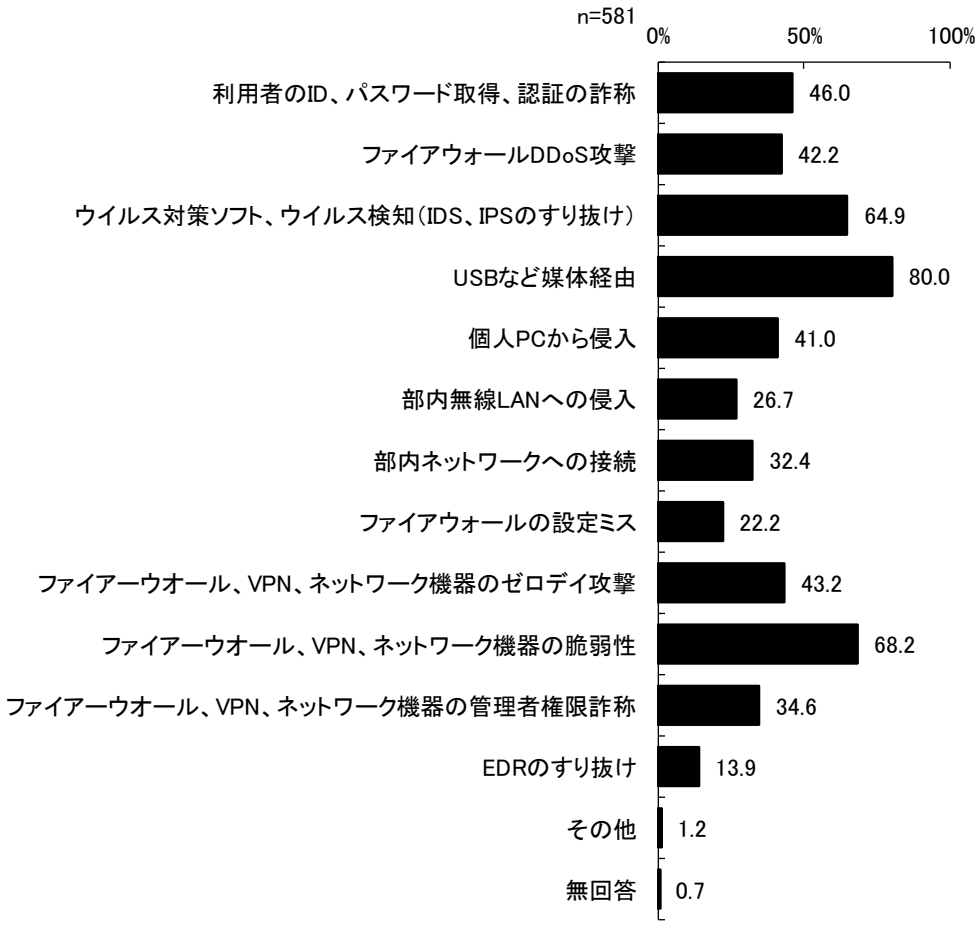


※「その他」の主な回答は以下の通り。業務停止による社会不安醸成
・国家間テロ、国家間戦争
・社会的信用の失墜
・敵性国家の生産性低下
・愉快犯

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】

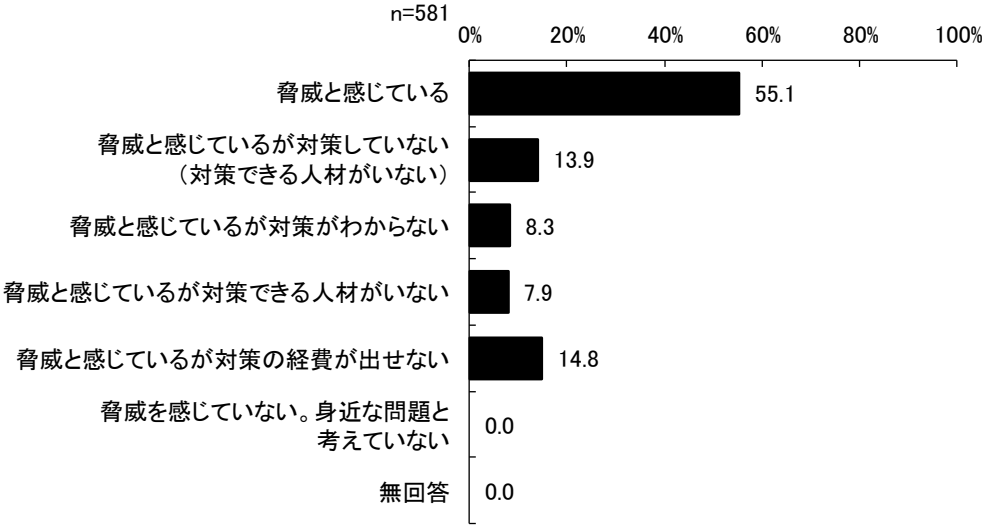


※「その他」の主な回答は以下の通り。
・メールに添付されたウイルスの展開
・サイバー攻撃であれば導入の無い EDR 以外は全てチェックとする
・メール添付ファイルからの端末の RAT 感染からのラテラルムーブメント
・外部公開系サーバのプラットフォーム脆弱性
・リモートメンテナンス環境を踏み台にした侵入
・レガシー機器、アップデートされていない機器からの侵入
・個人 PC から侵入
・悪意ある故意
・職員による規程違反作業による、脆弱性露見、情報漏洩

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。

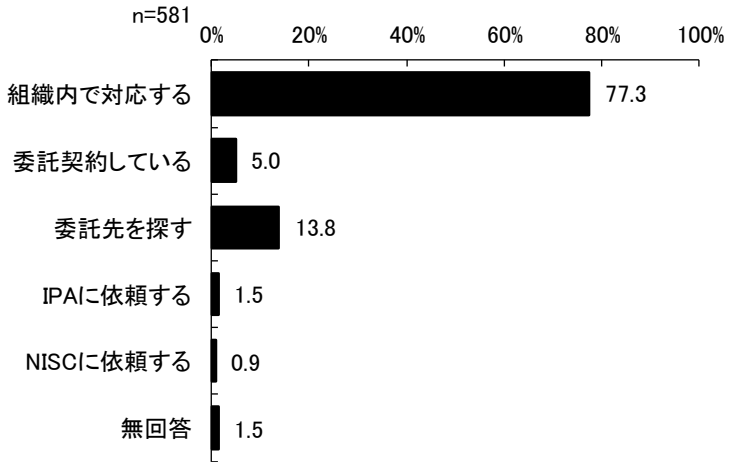
図表 50　サイバーセキュリティを脅威と感じているか、対策を検討しているか、問題は何か（Q46）



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。

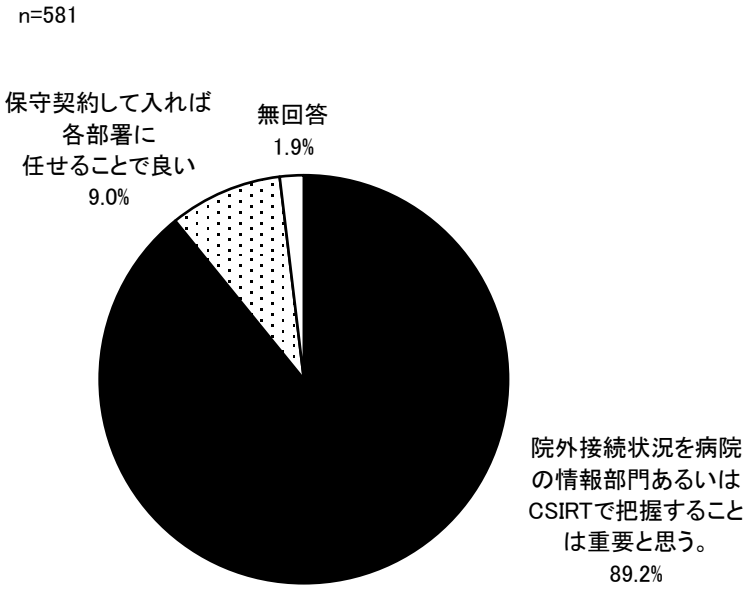
図表 51　インシデント発生時の対応について（Q47）



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）

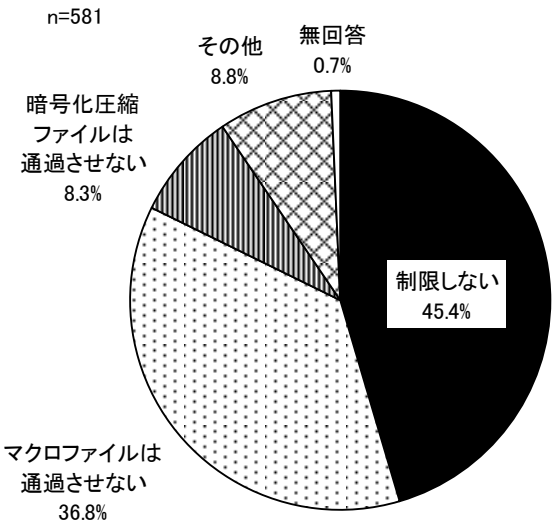


（5）侵入経路の対策として実施している事項等

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）



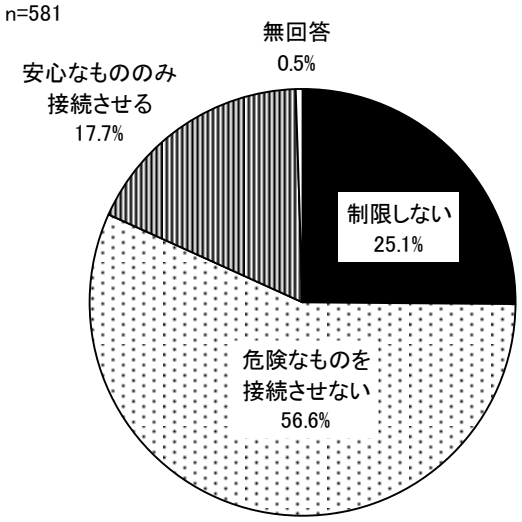
「その他」の主な回答は以下の通り。
・.xls .doc の添付ファイルは削除する
・「.exe」ファイルが添付されたメール及びウィルス対策ソフトでのチェックで不正なファイルと判断されたものは通過させない
・ESET(ウイルス対策ソフトでの制御)
・UTM によるウイルスブロック機能を有している
・Windows 実行ファイル、Windows スクリプトは通過させない
・ウィルスチェック
・ウイルス対策ソフトのセキュリティ設定
・システム部門は制限したいが、業務の都合上、制限出来ない状況
・セキュリティソフトで設定（初期から変更していない）
・ファイアウォールでポートの限定、添付ファイルの容量制限を設けている
・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。

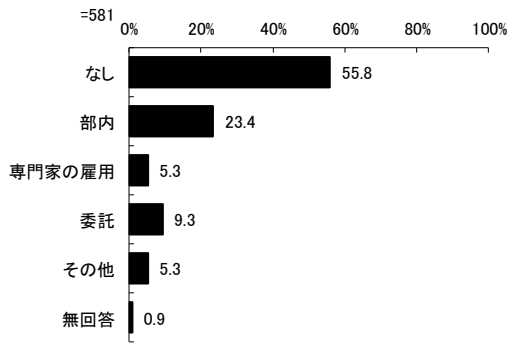
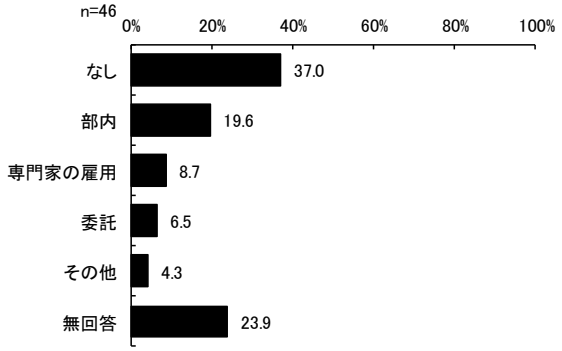
図表 54　ホームページ閲覧に関する対策（Q50）



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
	

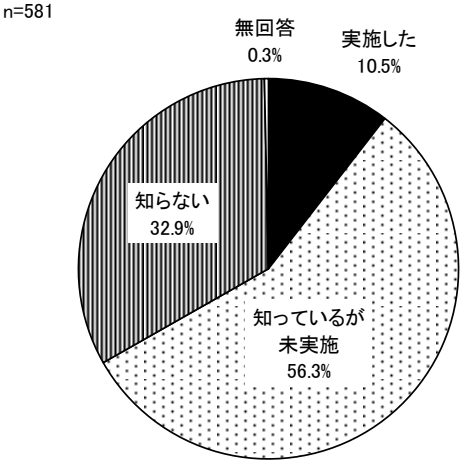
※「その他」の主な回答は以下の通り。
・院内の委員会にて対応
・上部機関が設置している
・機構にて組織化されている
・情報セキュリティポリシーにより規定
・対策専門部署の設立

・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。

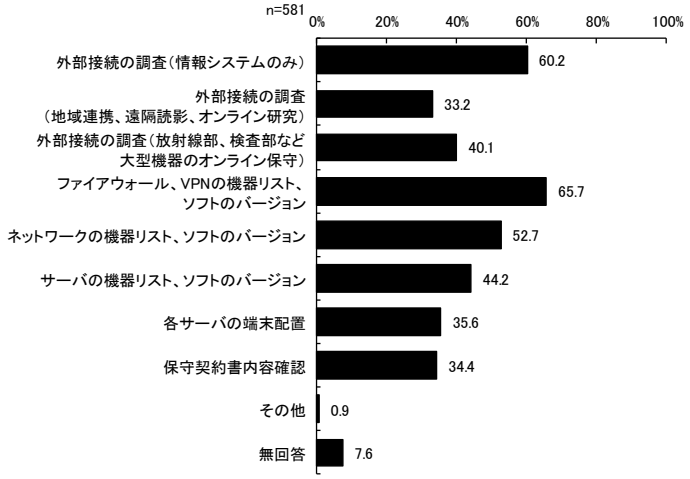
図表 56　医療情報システムの安全管理ガイドラインに添付されたサイバーセキュリティに関するチェックリスト、フローを知っているか（Q52）



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】

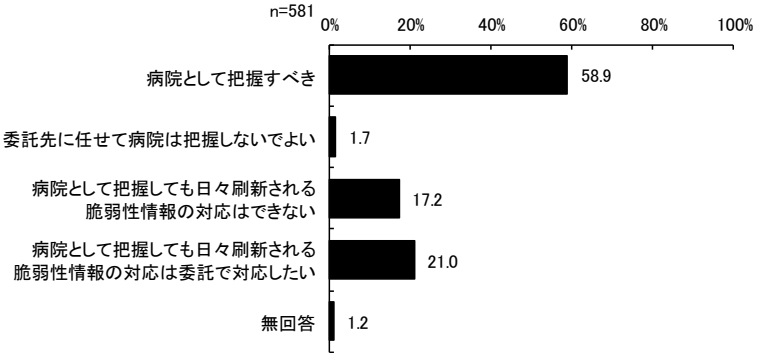


※「その他」の主な回答は以下の通り。
・各システムに格納されている DB とデータレイアウトの把握

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。

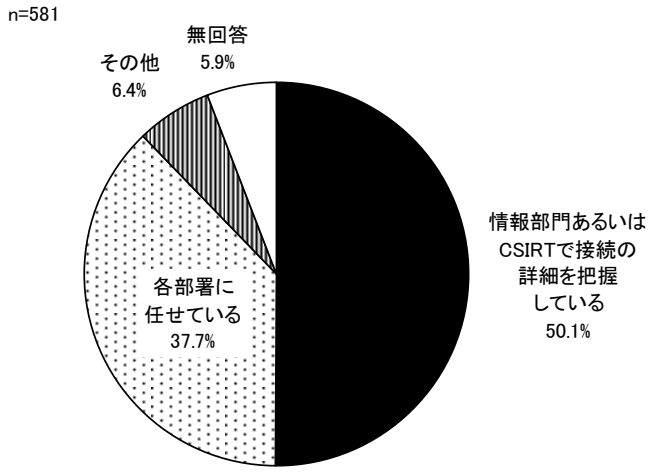
図表 58　システムの保守回線・CT・MRI 等の検査機器の保守回線の詳細（Q54）



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）

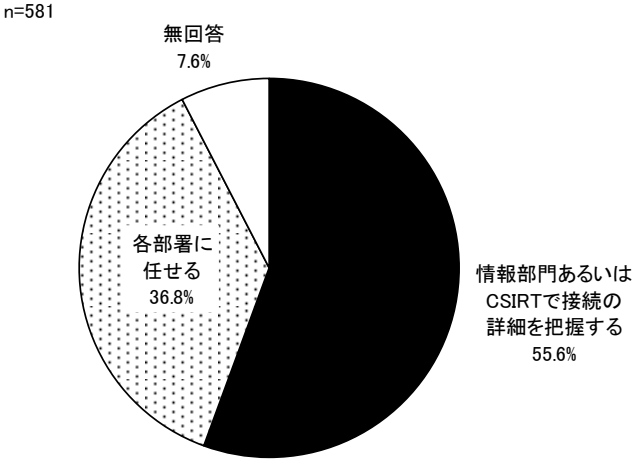


※「その他」の主な回答は以下の通り。
・ケースによって異なる
・システム管理部門で対応
・リアル接続はしていない。必要に応じてｅメール等で連携する
・兼任システム担当者が把握している
・外部接続は一切遮断している
・各部署に任せ、報告・管理先を情報部としている
・地域連携、遠隔病理診断等を導入していない
・導入時に情報部門が関わりセキュリティ対策を施す。導入後の運用は担当部署が担う
・把握しているが、通信技術等の知識がなく詳しくわからない
・病院として把握しても日々刷新される脆弱性情報の対応はできない

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。

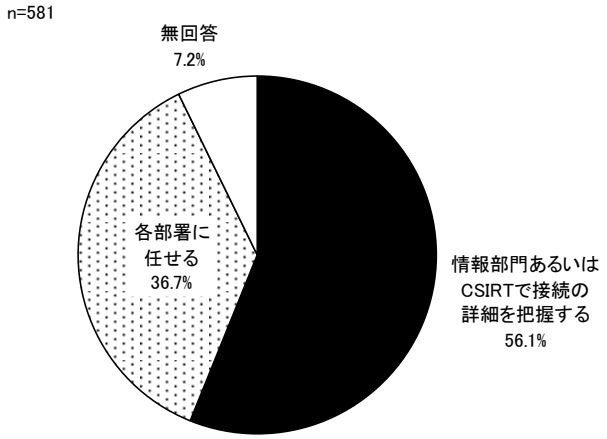
図表 60　オンライン診療・遠隔モニタリング・院内 SNS の接続について（Q56）



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。

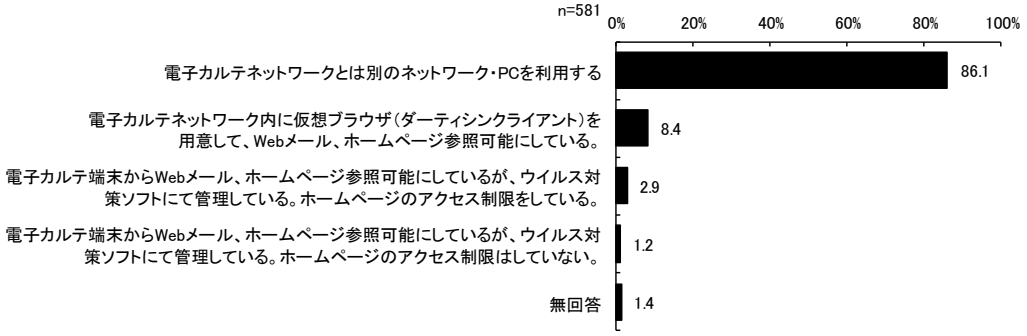
図表61　匿名化してオンライン接続する遠隔画像診断・匿名化してオンライン接続する調査等の接続について（Q57）



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。

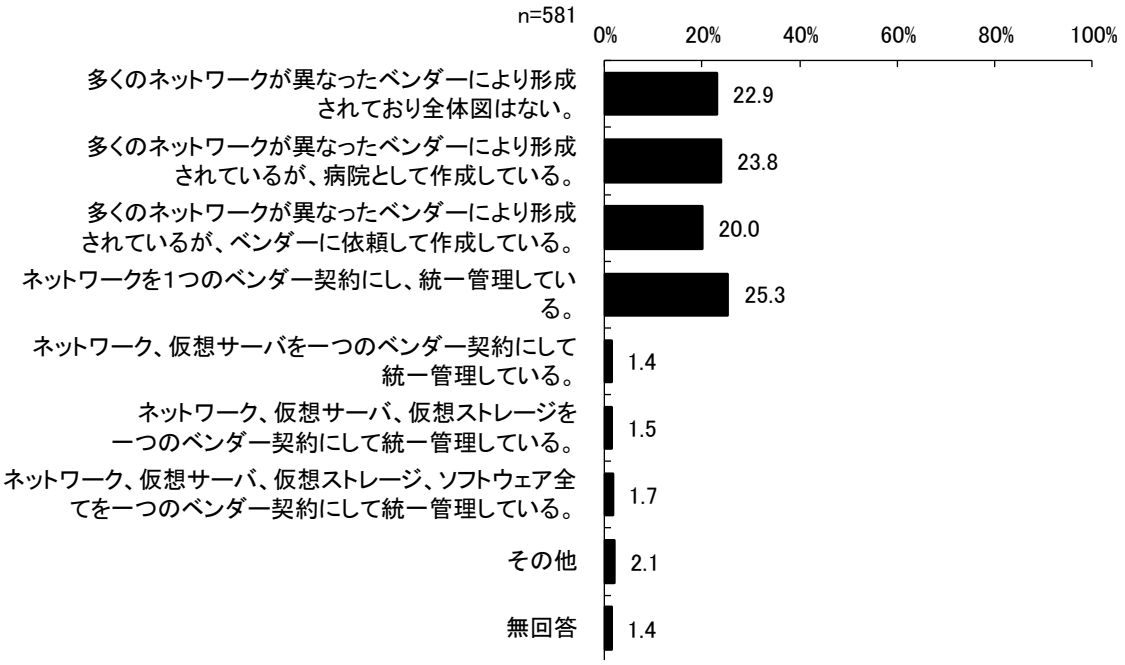
図表 62　利用者のホームページ閲覧、メール受信について（Q58）



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）

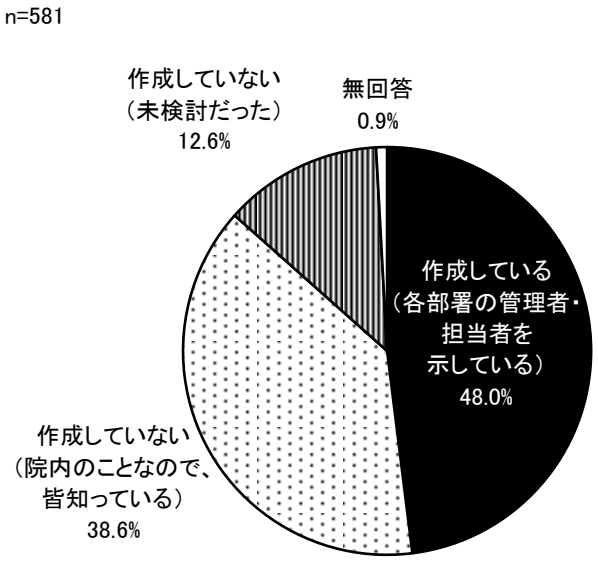


※「その他」の主な回答は以下の通り。
・office365 を利用
・オンプレ環境自体が大規模(5000 ホスト規模)なこと、近年は外部 DC やクラウドの活用も進み、規模が大きくなり過ぎたため一元的に描画できないが、ネットワーク管理者の頭の中にはある
・一部使用していない系統の削除ができていない
・ネットワークを１つのベンダー契約にしているが、管理が徹底されておらず病院に情報提供されない
・ほぼ統一された全体図があるが、一部異なるベンダーにより形成された部分があり、その部分については管理できていない
・一つのベンダーにお願いしているが、接続端末等の情報は管理できていない
・統一管理のため調査中（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。

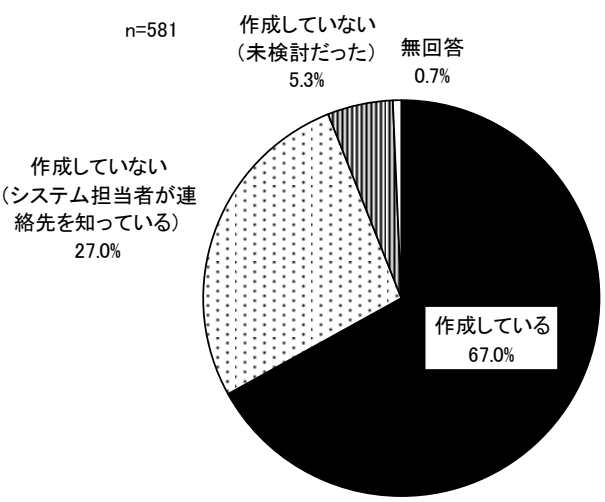
図表 64　電子カルテシステム・部門システムそれぞれについて院内の管理者・担当者一覧を作成しているか（Q60）



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）

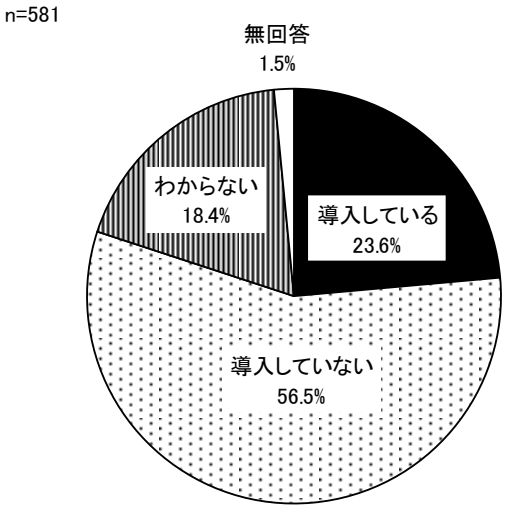


（6）ウイルス対策の状況

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。

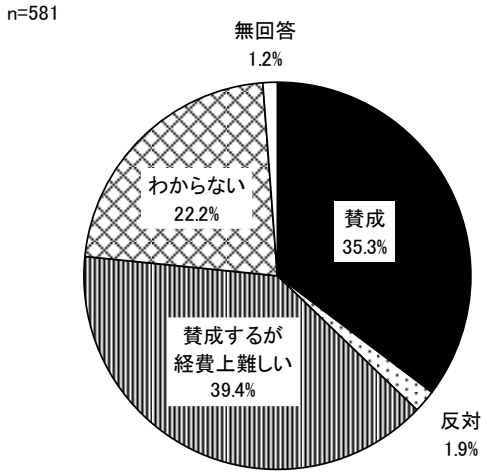
図表66　端末へのEDR（Endpoint Detection and Response）導入状況（Q62）



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。

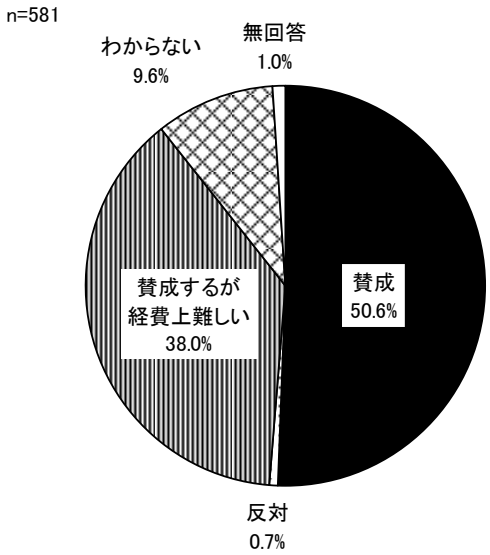
図表 67　端末への EDR 導入について（Q63）



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。

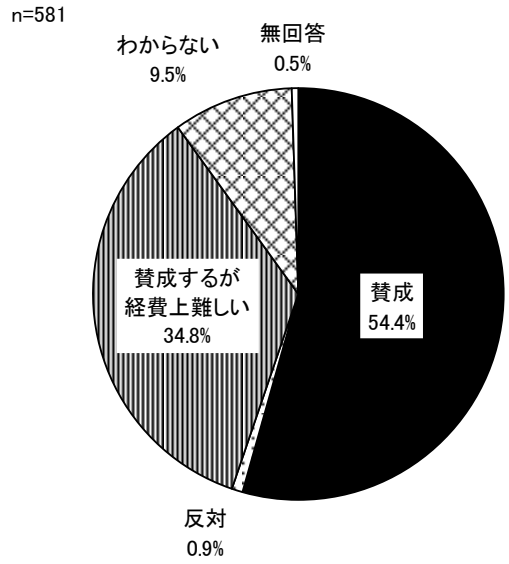
図表 68　内部ネットワークを監視することについて（Q64）



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）

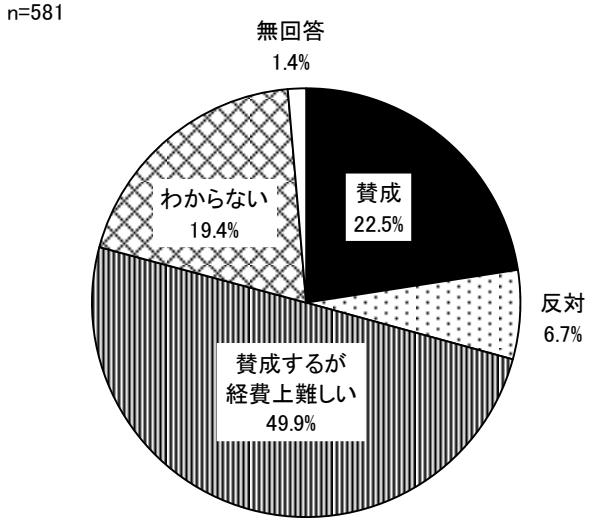


（7）サイバーセキュリティ対策への意見

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。

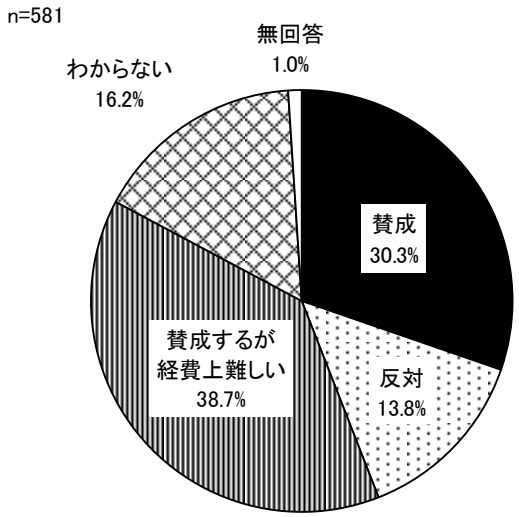
図表 70　端末からサーバーを守るためのシンクライアント基盤の導入（Q66）



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。

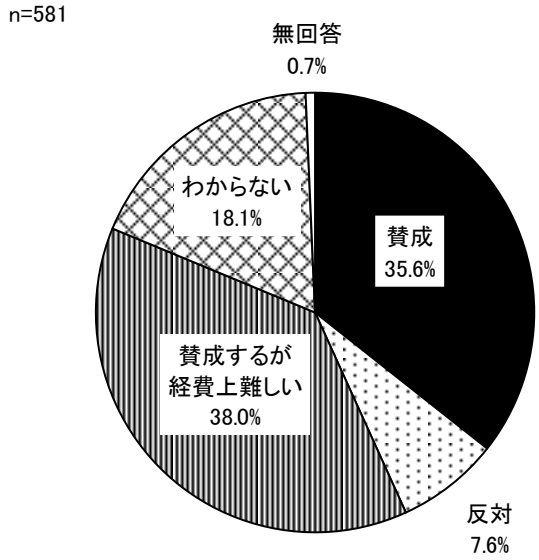
図表 71　仮想ブラウザ（ホームページ、Web メール参照用の仮想サーバーを用意）経由のインターネット参照（Q67）



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。

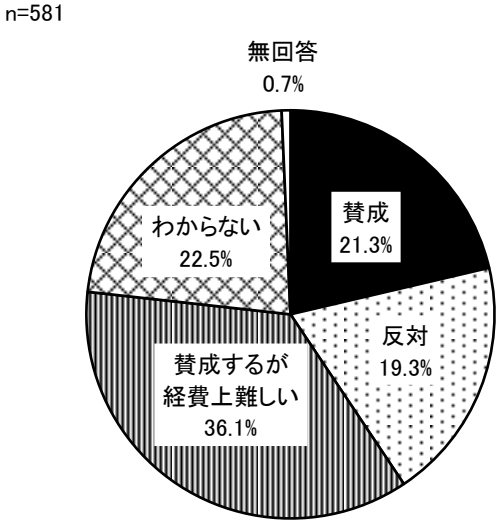
図表 72　組織内のサーバー（ハード系）を仮想サーバー、仮想ストレージ、仮想ネットワーク等を用いて病院あるいは委託契約にて統一的に導入管理を行う（Q68）



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）

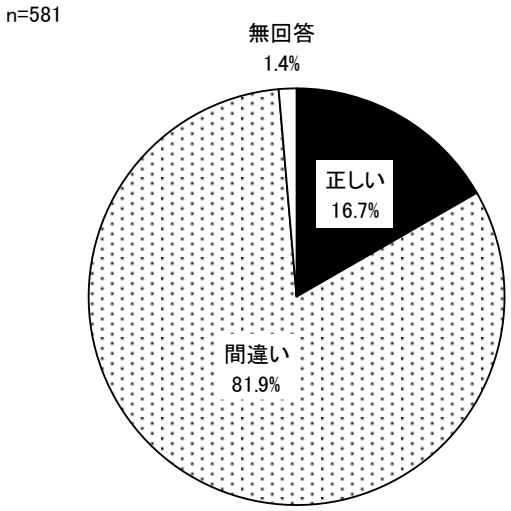


（8）最近のサイバー攻撃に対する理解度

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。

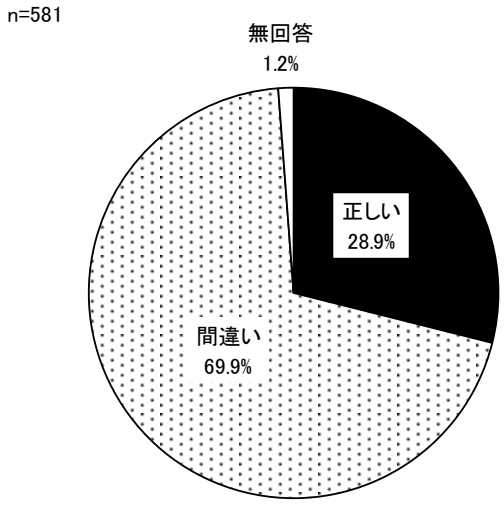
図表74　「データを暗号化されたPC、サーバーに必ずウイルスは見つかる」ことは正しいか（Q70）



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。

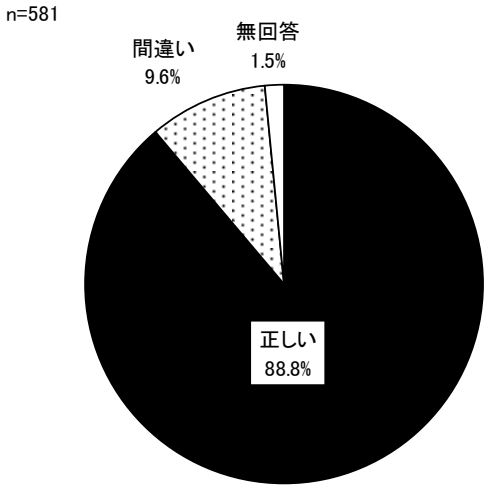
図表 75　「A さんからウイルス添付メールが届いた場合、A さんの PC はコンピュータウイルスに感染している」ことは正しいか（Q71）



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。

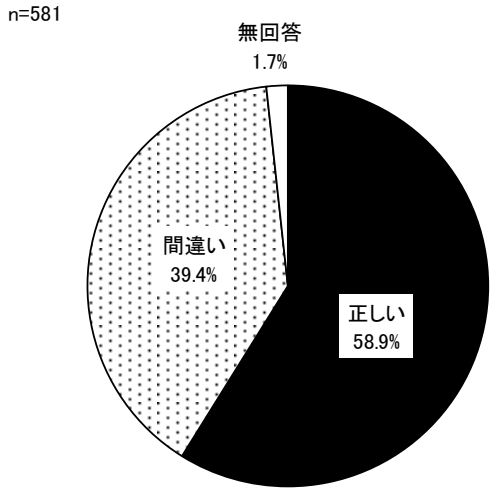
図表 76　「Windows のアクティブディレクトリやバックアップの設定ファイルは攻撃される」ことは正しいか（Q72）



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。

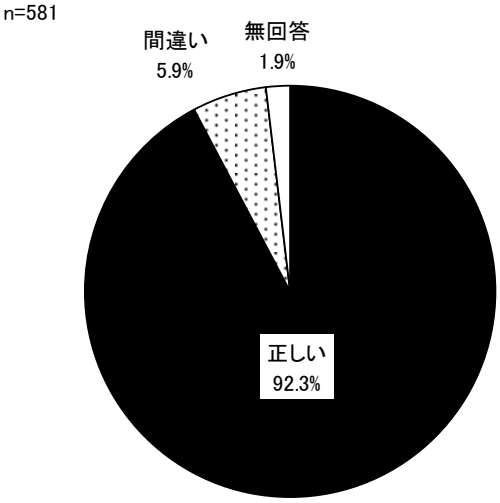
図表 77　「大容量のファイル全体の暗号化は時間がかかるので一部の暗号化をするものもある」ことは正しいか（Q73）



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。

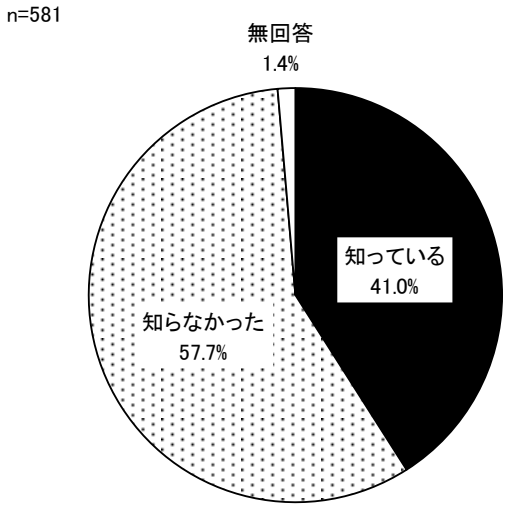
図表 78　「攻撃を受けた場合に IPA、NISC に対応、助言する窓口がある」ことは正しいか（Q74）



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）



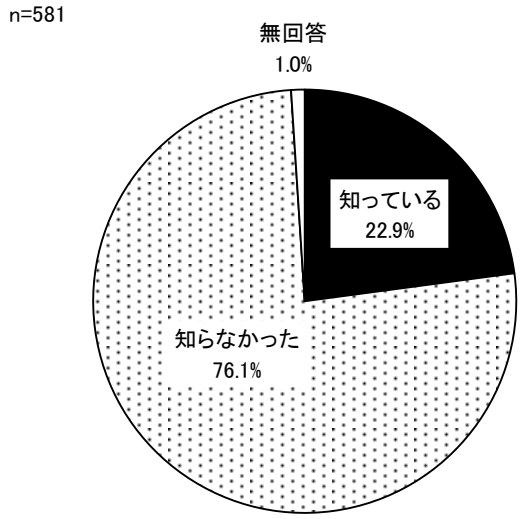
図表 80　「NISC の 3、2、1 ルールでは 3 つのデータ、2 つにバックアップ、1 つのオフラインバックアップが提唱されている」ことを知っているか（Q75）とセキュリティ教育を行っているか（Q28）、セキュリティ教育は年に何回行っているか（Q29）、セキュリティ教育のためにどのような研修を行っているか（Q30）のクロス集計結果

		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）



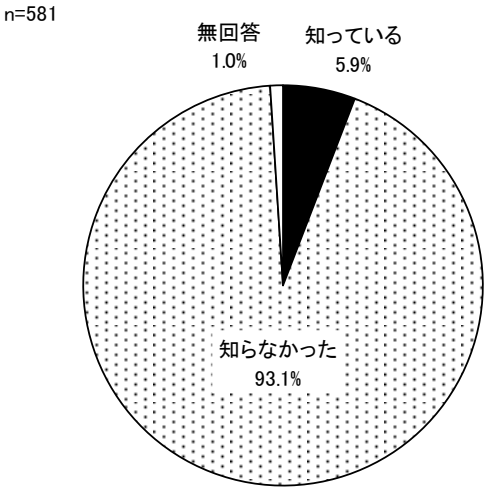
図表 82　「NICT のサイバーセキュリティ研究所のデータでは IoT 機器の攻撃が半数以上である」ことを知っているか（Q76）とセキュリティ教育を行っているか（Q28）、セキュリティ教育は年に何回行っているか（Q29）、セキュリティ教育のためにどのような研修を行っているか（Q30）のクロス集計結果

		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）



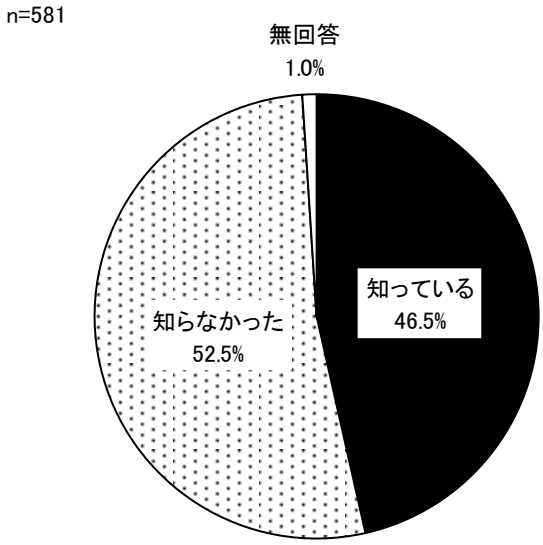
図表 84　「国際医療機器規制当局フォーラム文書におけるサイバー攻撃対策について」知っているか（Q77）とセキュリティ教育を行っているか（Q28）、セキュリティ教育は年に何回行っているか（Q29）、セキュリティ教育のためにどのような研修を行っているか（Q30）のクロス集計結果

		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

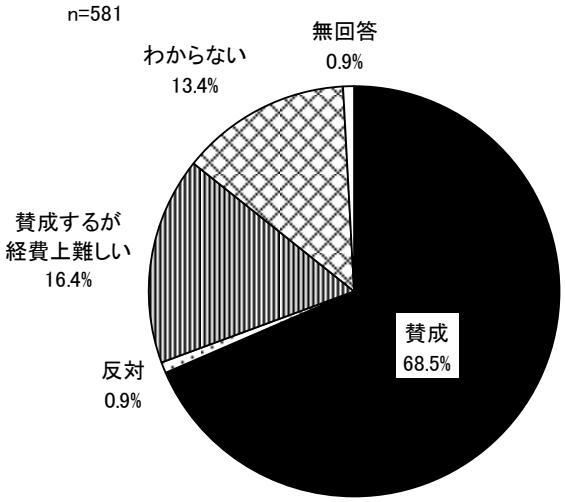
		調査数	知っている	知らなかった	無回答
Q28 セキュリティ教育を行っているか	はい	389 100.0	206 53.0	179 46.0	4 1.0
	いいえ	170 100.0	58 34.1	111 65.3	1 0.6
	わからない	20 100.0	4 20.0	15 75.0	1 5.0
Q29 セキュリティ教育の1年あたりの実施回数	1回	293 100.0	155 52.9	136 46.4	2 0.7
	2回	36 100.0	17 47.2	17 47.2	2 5.6
	3回	3 100.0	1 33.3	2 66.7	－ －
	4回	2 100.0	2 100.0	－ －	－ －
	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。

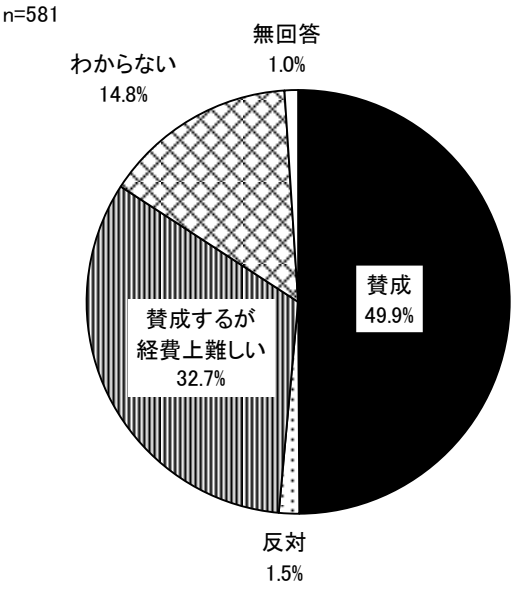
図表87　RAIDによるリアルタイムの保存（Q79）



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。

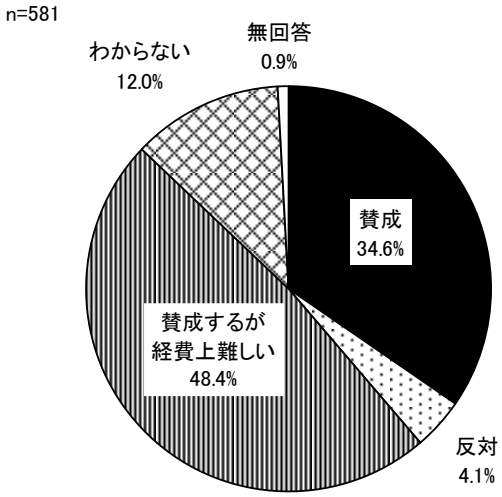
図表 88　RAID 以外にリアルタイムのバックアップを用意する（Q80）



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。

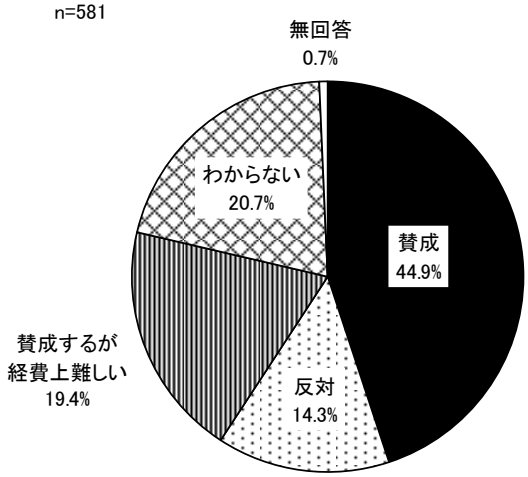
図表 89　遠隔地にリアルタイムのバックアップをする（Q81）



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。

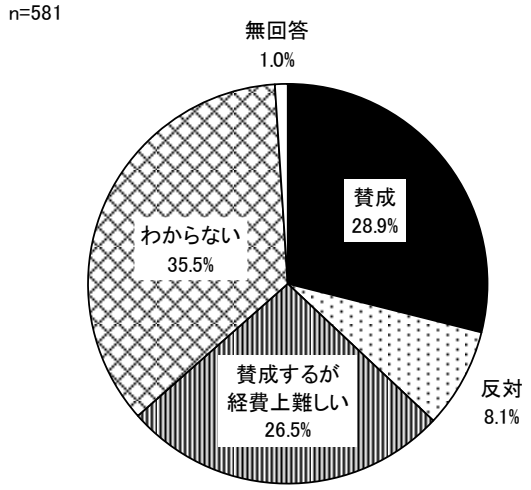
図表 90　ジュークボックス型の磁気テープユニットによる日々のバックアップ（Q82）



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。

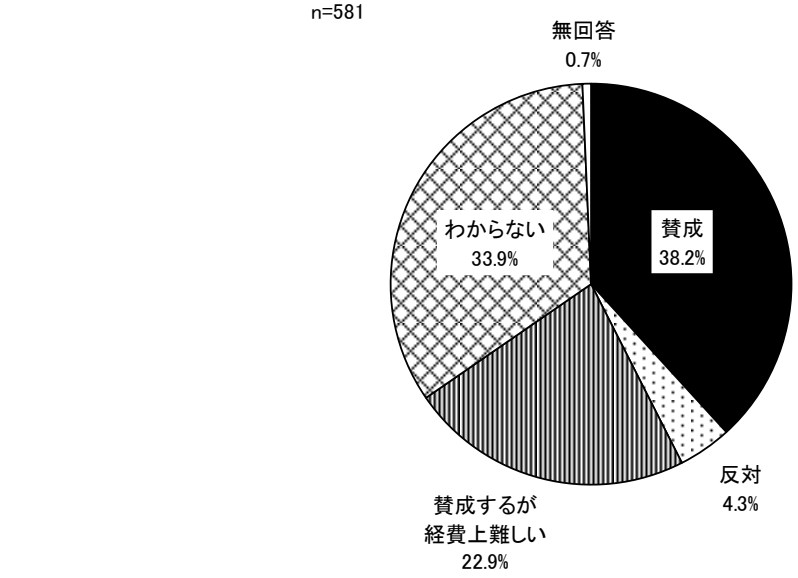
図表 91　SS-MIX フォルダーから地域連携サーバーが pull する仕組みで地域連携側にバックアップできる（Q83）



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）

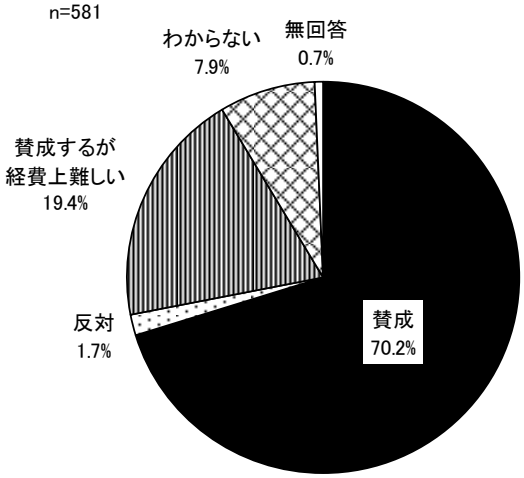


（１０）情報部門の管理について

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。

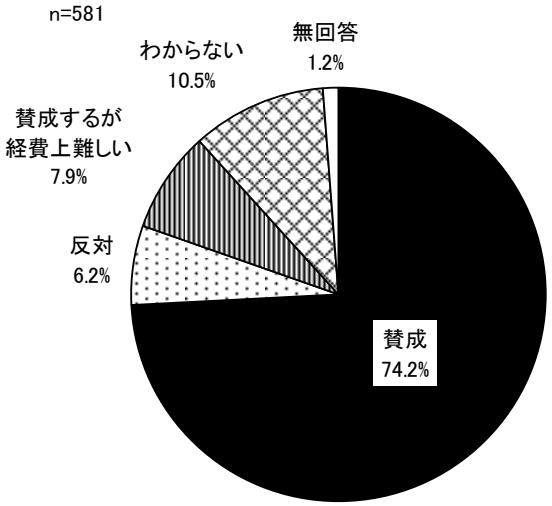
図表93　管理者のサーバー等の管理に用いるPCとメール・ホームページ参照のPCとは別の機器、別のネットワークを用いる（Q85）



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。

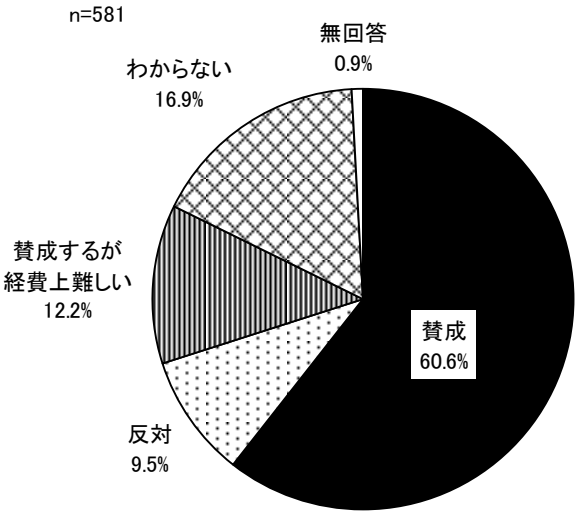
図表 94　委託業者の院外からの接続は事前に時間等を連絡させ、時間、接続先を限定する（Q86）



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。

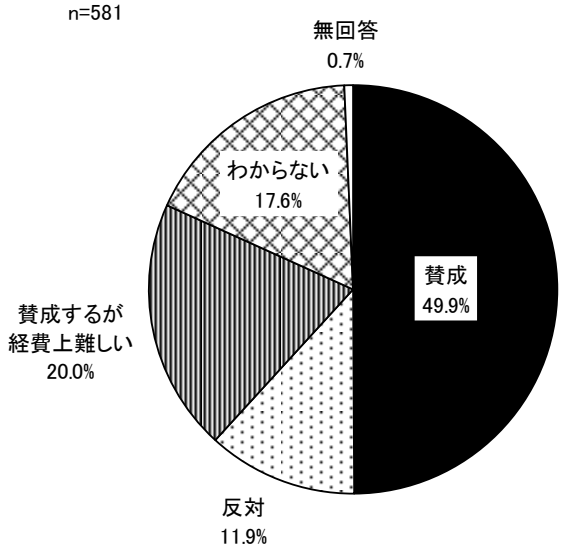
図表 95　委託業者の院外からの接続は事前に時間・接続先等を連絡させファイアウォールの接続を制限する（Q87）



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。

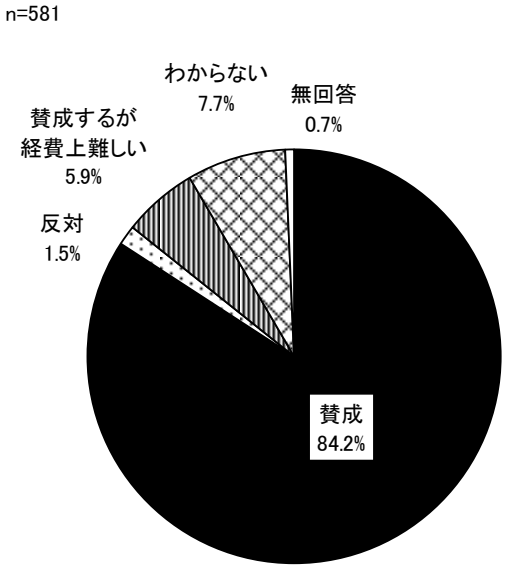
図表 96　委託業者の院外からの接続はリモートアクセス、シンクライアントなどを用いて直接接続させない（Q88）



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）

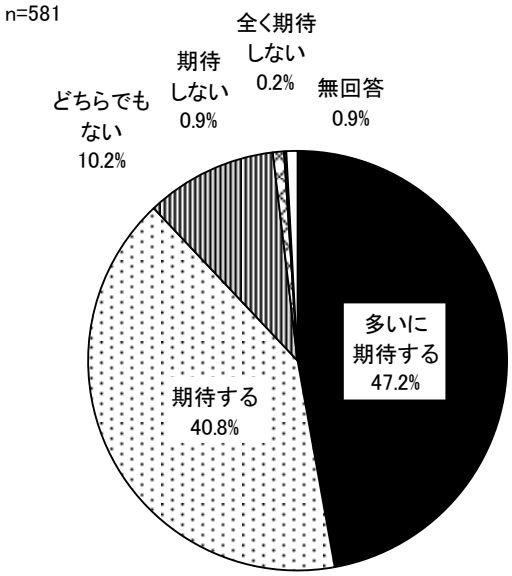


（１１）ISAC※について情報共有したい事項等　※Information Sharing and Analysis Center

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。

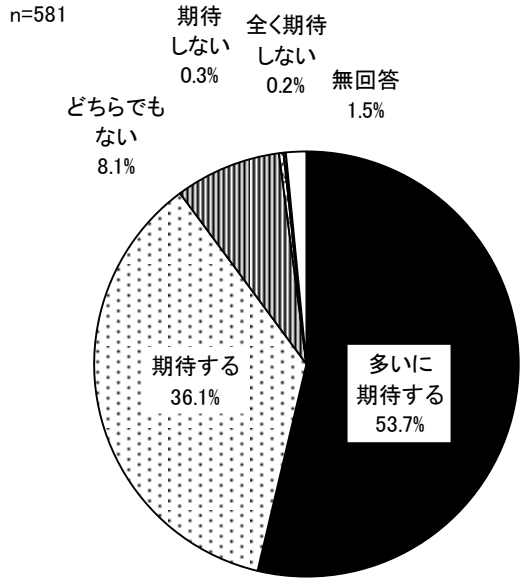
図表 98　流行しているマルウェア（ウイルス）等、リスク関連の情報（Q90）



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。

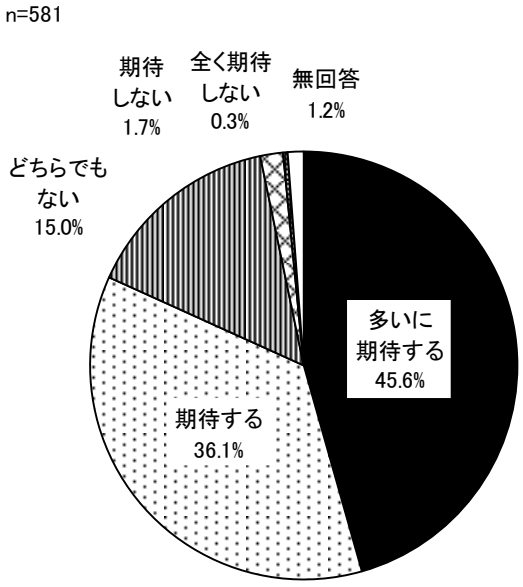
図表 99　セキュリティ対策の具体的な実施方法（Q91）



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。

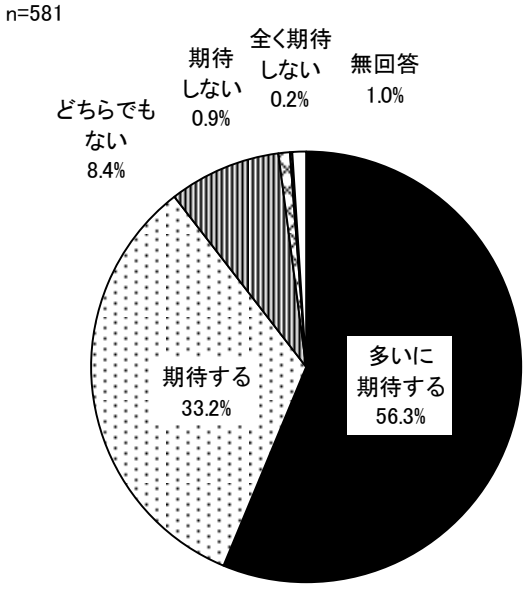
図表 100　マルウェア検体の分析（Q92）



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。

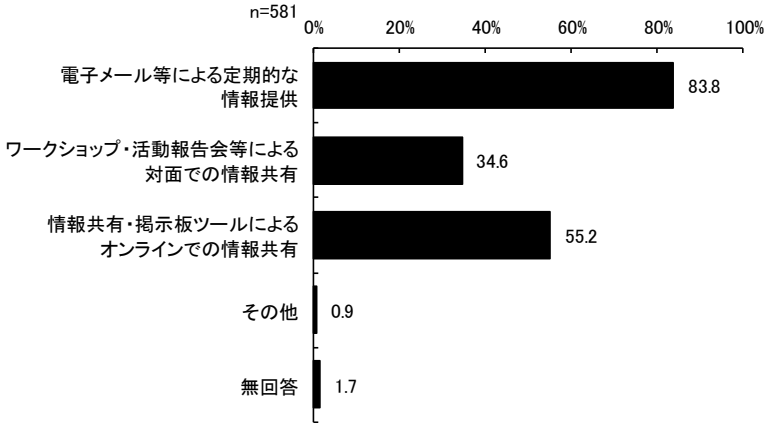
図表 101　セキュリティ教育教材の提供（Q93）



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】

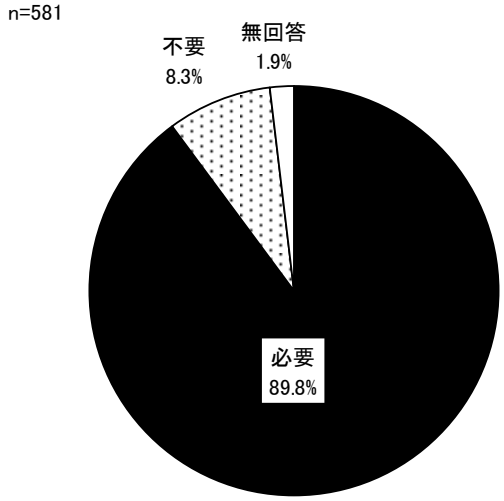


※「その他」の主な回答は以下の通り。
・FAX
・WEB による迅速な情報提供（固定的ではなく多岐にわたる情報）
・Youtube
・オンラインでのワークショップ
・活動報告会
・事例発表会の開催

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。

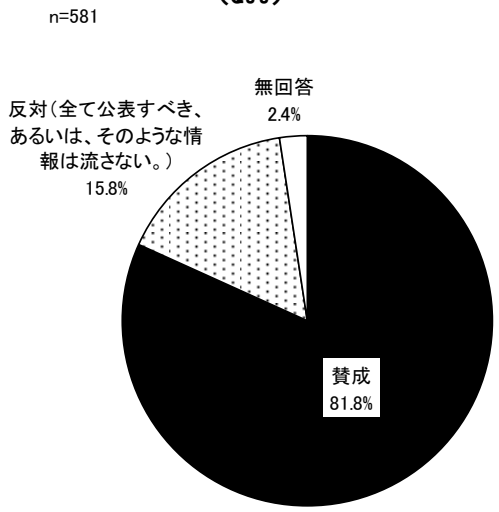
図表 103　知識レベルが同じではないので、技術的指導者が必要（Q95）



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。

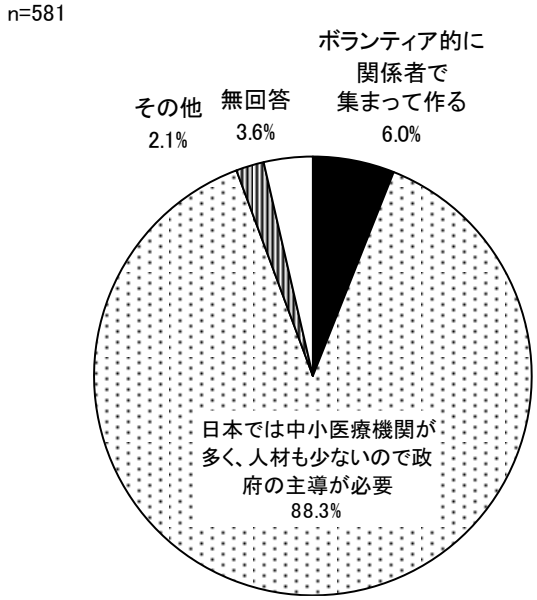
図表 104　共有するべき情報には噂、予想なども含む必要があり、公表しにくいものがあると思う（Q96）



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）



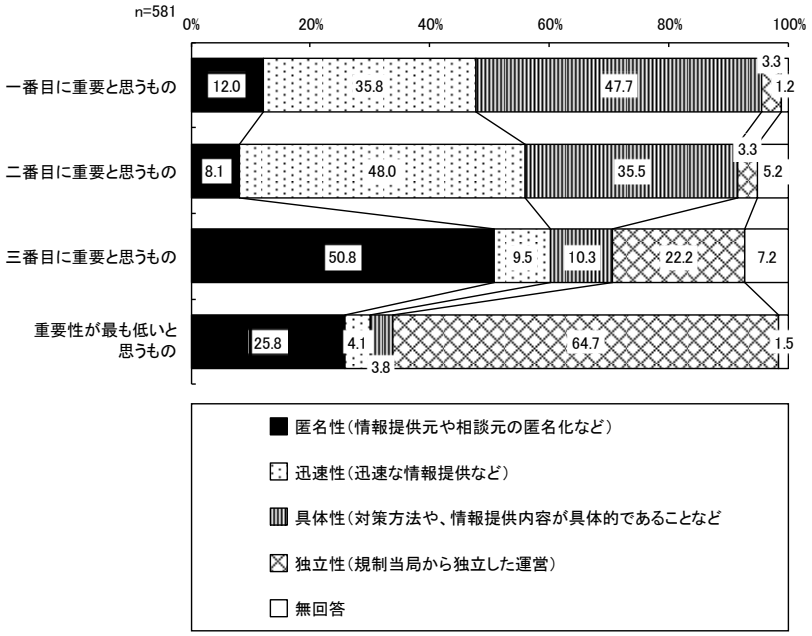
※「その他」の主な回答は以下の通り。
・アドバイザー的に政府が一般企業から選択した技術的指導者を配置し、医療系の関係者で組織化する
・全ての企業で問題と成るセキュリティに掛るコストを法制化するしか予算確保は出来ない
・日本で医療 ISAC と呼ばれるものが 2 つあるが、どちらも存在に疑問。悪徳系のほうは悪戯に不安を煽るだけ、NISC セプターカウンシルに設置された役所形骸系(日本医師会事務局内)のほうは活動実態が聞こえてこない
・日本に人材はいない
・本社・本部で対応

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。

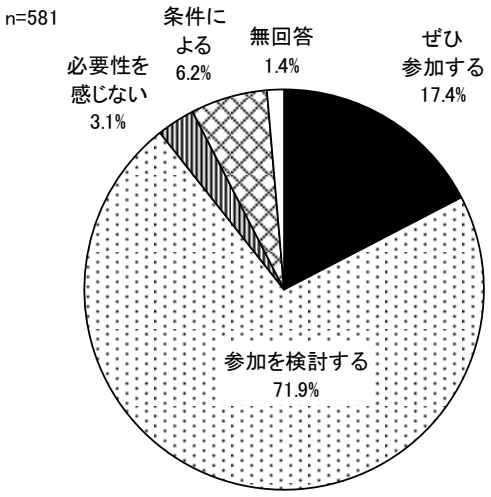
図表 106　サイバーセキュリティ情報の公的共有組織に必要な要素の重要度（Q98～Q101）



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）

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」

分担研究者：山本　隆一（一財）医療情報システム開発センター・理事長
研究協力者：吉田真弓（一財）医療情報システム開発センター・主任研究員

研究要旨

重要インフラに該当する医療分野において、医療機関等のサイバーセキュリティに対する取り組みを強化することは喫緊の課題である。病院情報システムは、これまで外部と隔絶した情報ネットワークであった状況に対し、データヘルス改革、働き方改革、オンライン診療、モバイルヘルス(m-Health)等の展開で外部ネットワークへの接続が進み、患者等にまで利用が拡大する方向性にある。情報化が遅れていた小規模病院、診療所における電子カルテの普及も進みつつある。また、拡大する m-Health 機器（携帯に連携した継続的なモニタリングと適時な介入をする治療アプリを含む。）は病院、診療所のシステムと連携され、研究基盤として活用される状況もある。同時に、進化するクラウド技術により、医療機関内にあったサーバをクラウド上に移行することも現実的になりつつある。

一方、サイバーセキュリティ対策も閉じたネットワークの出入口監査から、エンドポイント検知、ゼロトラストと言われる内外の区別が無く直接個々の端末を対策する取組が重視されるようになってきた。変化と対策の将来像は双方合致した状況に見えるが、現状から理想の将来像に安全に移行できるかが喫緊の課題である。

これらの状況を踏まえ、本研究では医療分野におけるサイバーセキュリティ対策と課題について医療機関の規模・ユースケース等ごとに整理し、医療機関同士が相互にサイバーセキュリティ対策に関する情報共有・相談を行う体制のあり方や、医療機関等への対策強化の普及・促進策等を検討する。

A．研究目的

重要インフラに該当する医療分野において、医療機関等のサイバーセキュリティに対する取り組みを強化することは喫緊の課題である。病院情報システムは、これまで外部と隔絶した情報ネットワークであった状況に対し、データヘルス改革、働き方改革、オンライン診療、モバイルヘルス(m-Health)等の展開で外部ネットワークへの接続が進み、患者等にまで利用が拡大する方向性にある。情報化が遅れていた小規模病院、診療所における電子カルテの普及も進みつつある。また、拡大する m-Health 機器（携帯に連携した継続的なモニタリングと適時な介入をする治療アプリを含む。）は病院、診療所のシステムと連携され、研究基盤として活用される状況もある。同時に、進化するクラウド技術により、医療機関内にあったサーバをクラウド上に移行することも現実的になりつつある。

一方、サイバーセキュリティ対策も閉じたネットワークの出入口監査から、エンドポイント検知、ゼロトラストと言われる内外の区別が無く直接個々の端末を対策する取組が重視されるようになってきた。変化と対策の将来像は双方合致した状況に見えるが、現状から理想の将来像に安全に移行できるかが喫緊の課題である。

これらの状況を踏まえ、本研究では医療分野におけるサイバーセキュリティ対策と課題について医療機関の規模・ユースケース等ごとに整理し、医療機関同士が相互にサイバーセキュリティ対策に関する情報共有・相談を行う体制のあり方や、医療機関等への対策強化の普及・促進策等を検討する。

B．研究方法

b１．分担研究内容

山本研究班では、山本が改定作業班主査として主導し取り纏めを行った「医療情報システムの安全管理ガイドライン 5.2 版」について、主導者の視点から、作成時の状

況、その後について医療情報システム開発センターの立場から国、企業系の意見を聴取し今後の方策を検討した。
COVID-19（以下、「新型コロナウィルス」と記載）感染拡大の影響もあって、オンライン診療は世の中に急速に拡がり制度としてほぼ定着していると言える。研究代表者の方で、オンライン診療の提供側である医療機関についてはサイバーセキュリティへの予防や対策や、組織の安全管理体制などの調査を実施するため、我々は、提供を受ける側の患者に対して、昨年度に引き続きオンライン診療およびセキュリティ面の意識調査を実施した。Web アンケート調査により現状を把握し、昨年度、同様の手法で行った調査結果との比較を行い、認知度や意識の変化、傾向や課題点など洗い出しを行った。またこの調査とは別に医療情報システムの安全管理に関するガイドライン改定作業班と標準的セキュリティポリシーの検討をおこなった。

ｂ２．意識調査概要

患者を対象としたオンライン診療およびセキュリティに関する意識調査は、リサーチ会社（マクロミル）を利用して Web アンケートを実施した。アンケート対象者の絞り込みは、マクロミルのモニター会員で、1 年以内に特定健診など定期健康診断や歯科のメンテナンス以外で医療機関を受診し、医師等からの病状や治療に関する説明を理解できた 18 歳以上の国内在住者 600 名程度とした。質問内容は、医療機関において電子化が進むことに関しての意識、オンライン診療の認知・経験の有無、また、オンライン診療の経験者に対して、受診した際の状況、疾患の状態（定期的な受診、急な症状等）、継続の希望やオンライン診療への要望・必要性などを確認した。また、全員を対象にオンライン診療への意見や感触、対面受診以外の必要性などを質問した。
なお、本調査と昨年度調査の結果の比較を行うため、アンケート調査票や回答は昨年度分を踏襲し、対象者の選定条件も同じとする調査を行った。質問項目は、以下 b-3 に記す。

ｂ３．質問項目

質問数は、計 30 問（マクロミルが設定しているプロファイル関連の質問、我々がスクリーニング用に設定した質問２問を除く）で、内訳は次の通り。本人の生活環境（居住環境・最寄りの医療機関へのアクセス）や受診の頻度、マイナンバーカードの取得やスマホ所持の有無などの基本情報 8 問、医療機関の ICT 化に関する質問１項目（8 問）、オンライン診療に関する質問、オンライン診療の認知や経験、受診した感想、希望、意見など 21 問、計 30 問。なお、オンライン診療の受診の感触や実施した際の課題などは経験者のみに質問を行ったが、オンライン診療を知らない患者に対しても細かく解説を行った上で、全回答者に対してオンライン診療の必要性やあり方を尋ねた。

ｂ４．アンケート内容

前述の通り、調査の対象者は各群 900 名、計 2,700 名で、全員に同じアンケート調査票を使用した。スクリーニング調査 3 問、本調査 19 問。アンケート調査項目の概要は以下の通り。
＜基本情報関連質問～マクロミルデフォルト設定～＞　計 9 問
1. 性別　2. 年齢　3. 居住地　4. 婚姻状況　5. 子供の有無　6. 世代年収　7. 個人年収
8. 職業　9. 学生区分（8 で「学生」を選択した場合のみ）
＜スクリーニング質問＞　計 2 問
1. 1 年以内に医療機関を受診したか。（歯科のクリーニングや健康診断などを除く。オンライン診療、外来診療、訪問診療など、受診の形態は問わない。）
2. 受診した際に自身の病状や治療に関して医師や看護師からの説明を理解できたか。
（上記 2 問ともに「はい」を選択した人が、以下のアンケートの回答者対象となる。）
＜基本情報関連質問＞Q1～Q8　　計 8 問
Q1. 生活状況（同居家族や独居など）
Q2. 医療機関の受診頻度
Q3. 最寄りの医療機関へのアクセス方法（交通手段、時間など）
Q4. 受診中もしくは受診した診療科
Q5. 手術歴の有無（過去２年以内）
Q6. スマートフォンの所持
Q7. 自身のマイナンバーカードの取得状況
Q8. マイナンバーカードの非取得（非申請）

の理由
＜医療の ICT 化に関する質問＞Q9（q1～q8）計 1 問
Q9. 以下の 8 項目（q1～q8）について、「そう思う」「そう思わない」「どちらでもない」で回答。
q1. ワクチン開発等に使えるよう、診療情報の電子化を進めてほしい。
q2. スマートフォンに PHR の機能を持たせて自分の過去の予防接種履歴や、受診時の検査結果データを蓄積した上で、将来の手術や緊急時に利用できることが必要だ。
q3. 医療機関で持つカルテ情報は非常に重要な個人情報であり、現状の医療機関の体制のままで電子化が進むのにはセキュリティ面で不安だ。
q4. 医療機関で電子カルテを導入したりシステムの電子化が進んでいるのであれば、電子データの取り扱いについては、特に HP や院内掲示などで丁寧に説明が必要だ。
q5. 医療機関を選択する基準には、電子化が進んでいることは必要だ。
q6. 医療機関を選択する際に、口コミのサイトを参考に選ぶ。
q7. マイナンバーカードやスマホが健康保険証やお薬手帳の代わりとして利用できるのは便利だし利用したい。
q8. マイナンバーカードやスマホが健康保険証やお薬手帳の代わりとして利用するのはセキュリティ面での不安がある。

＜オンライン診療に関する質問＞ Q10~Q30　計 21 問
Q10. オンライン診療の認知
以下の質問は、回答について、対象者を限定する場合も含む。対象者を限定した場合は、冒頭に＊を付与。何もない場合は全員が対象。
＊Q11.（Q10 で知っていると回答した人のみ）オンライン診療の経験
＊Q12.（Q11 で経験ありと回答した人のみ）オンライン診療を受けた医療機関
＊Q13. 病状・症状　　Q14.症状の程度（急病や急変、または定期的受診）
＊Q15. 自身の環境（自宅・職場等）
＊Q16. 立会いの有無
＊Q17. 本人確認の方法（医師→患者）
＊Q18. 利用した端末や機器の種類
＊Q19. 利用した機器や端末のセキュリティ面の措置（ウィルスソフトやパッチ適用等）
＊Q20．オンライン診療を受けた理由
＊Q21.頻度　　＊Q22.満足・不満足度
＊Q23. 感想　　＊Q24．今後の継続希望
＊Q25.　前問 Q24 回答の理由
Q26.（オンライン診療の説明を読み理解した上で）オンライン診療での受診の希望
＊Q27.（Q26 で「受けたくない」と回答した人のみ）その理由
＊Q28.（Q12 でのオンライン診療未経験者が対象）オンライン診療を受けていない、もしくは望まない理由
Q29.　オンライン診療の必要性（対面診療以外が必要か）
Q30. オンライン診療と対面診療に関する考え

ｂ５．医療機関における情報ガバナンス確立のためのセキュリティポリシーの検討
本来モデルポリシーを策定してできるだけ多数の医療機関においてフィージビリティの確認を行う予定であったが、医療情報システムの安全管理に関するガイドライン第 6 版の改訂と並行して検討することになり、作業班での意見交換を中心に検討を進めた。
＜倫理面への配慮＞
本研究は、リサーチ会社を利用して Web アンケートを実施しており、対象者すべてにアンケート回答時に同意取得を行っている。また、アンケートにおいて氏名や生年月日等の個人を特定されるような質問はなく、結果に対しても個人を特定する行為は行わない。そのため、倫理面の問題がないと考える。

Ｃ．研究結果
2023 年 3 月 28 日～30 日に調査を実施し、その結果は以下に概要を記載し、本報告書の後半に結果グラフを記載する。最後にセキュリティポリシーの検討の結果を示す。

ｃ-１．回答者プロファイル
回答者数は 663 名、男女比は女性 48.4%、男性 51.6%でわずかに男性が多い。回答者の年齢は、18 歳以上で、年齢 10 歳区切り

で最も多い年齢層が 50 歳代 24.4%、60 歳代 21.1%、40 歳代 17.2%、30 歳代 17.2%、70 歳代 10.3%、20 歳代 8.1%の順だった。なお、18・19 歳が 0.3%2 名、80 歳以上が 1.4%で 9 名だった。
居住地は、東京都が最も多く 14.8%で、続いて大阪府が 9.5%、神奈川県 8.9%、北海道、愛知県の順で多かった。
婚姻状況に関しては、既婚が多く 67.7%、子供の有無については、子供有が 63.0%だった。世帯年収では、分からない・無回答を除くと、400 万～600 万円が最も多く 22.0%、続いて 200 万～400 万円の 18.7%、600 万～800 万円が 17.2%で、職業は会社員（事務系、技術系、その他）が 38.4%で最も多く、続いて、無職 15.5%、専業主婦（主夫）16.0%、パートアルバイトが 14.3% の順だった。
生活の状況は、配偶者と子供との同居が 34.7％で最も多く、配偶者との同居が 28.7%、独居が 15.7%、両親との同居が 12.4% という結果だった。昨年度の回答者プロファイルとの目立った差は見られなかった。
＜参考＞昨年度の結果では、回答者は 1111 名、男女比は女性 44.4%、男性 55.6%、最も多い年齢層が 50 歳代 25.3%、40 歳代 22.9%、60 歳代 18.5%、30 歳代、70 歳代、20 歳代 7.7%の順だった。なお、18・19 歳が 1.1%、80 歳以上が 0.5%で実数にして 6 名。
居住地は、東京都が最も多く 14.3%で、続いて大阪府が 9.7%、神奈川県、千葉県、愛知県の順で多かった。
婚姻状況に関しては、既婚が多く 64.8%、子供の有無については、子供有が 58.7%だった。世帯年収では、400 万～600 万円が最も多く 20.3%、続いて 600 万～800 万円で 17.2%、200 万～400 万円が 16.8%で、職業は会社員（事務系、技術系、その他）が最も多く 41.1%、続いて、無職 15.4%、専業主婦（主夫）14.3%、パートアルバイトが 13.0% の順だった。生活の状況は、配偶者と子供との同居が 33.9%で最も多く、配偶者との同居が 28.1%、独居が 16.9%、両親との同居が 13.0% という結果だった。

ｃ－２．回答者の受診頻度やマイナンバーカードの所持について

医療機関への受診の頻度は、月に１，２回が最も多く 35.7%、2.3 か月に１回が 32.9%、半年に１回が 14.0%、年１回が 11.6%で、最寄りの医療機関（かかりつけの医療機関）へのアクセス環境については、「車で 30 分未満」が最も多く 41.2%、続いて多いのが「徒歩で 15 分未満」で 33.2%だった。
受診している、もしくは受診した医療機関の診療科（複数回答）は、内科が多く 52.6%, 歯科が 31.7%, 皮膚科 20.2%, 眼科が 18.1%、耳鼻咽喉科、整形外科、婦人科、循環器内科、精神科、泌尿器科、心療内科の順で多かった。
２年以内の手術歴では、有が 11.0%, 無が 87.8%だった。スマホの所有ありは 96.7%。マイナンバーカードの所有あり（申請済で受取待ちを含め）が 87.5%。マイナンバーカードを持っていない人（n=78）にその理由を尋ねると「近々申請予定」が 24.1%で最も多く、次に「自身の個人情報の漏洩が怖い」で 25.3%、「国や自治体に管理されたくない」が 21.5%、「用途がない、使い道が分からない」13.9%で、「手続きが面倒だから」は 10.1%だった。
昨年度の結果と比較して、受診歴や受診状況に関しては、ほぼ傾向は同じだった。ただ、マイナンバーカードの所持が、昨年度の 68.1%から 87.5%で所持有が２０%増えたこと、また、所持していない人の内、24%は近いうちに申請予定で、それ以外 76%の人の未申請の理由として、昨年度最も多かった「手続きが面倒」が大幅に減ったこと、「個人情報の漏洩が怖い」「国自治体に管理されたくない」という理由が半数近くあったことなど、昨年度と大きな差がみられた。

ｃ－３．医療機関での電子化について

医療機関での電子化が進むことについては、制度の変化に伴い、昨年度の８項目に追加して、「マイナンバーカードが健康保険証の代わりになると、医療費が安くなるなどメリットがあれば使いたい」を入れ９項目で質問した。
その内、「電子カルテやオンライン診療システムを導入している場合は、患者がちゃんと理解できるように、HP や院内掲示で説明が必要である」が「そう思う」という意見が

67.9%で他の項目と比較してかなり高く、昨年度も同様だった。次に「そう思う」が多かったものが、追加した１項目「マイナンバーカードを保険証として利用すると医療費が安くなるなら使いたい。」が 61.5%で他の項目（PHR の推進や、マイナンバーカードの診察券としての利用の推進、スマホでの受診予約やリマインドなど医療機関での電子化対応）と比較してかなり高く、関心の高さが見られた。また、昨年度は 47.3%だった「医療機関ではセキュリティの専門家がいると思えないので個人情報の漏洩など心配」が、54.8%に上がっており、昨年度起きた医療機関のサイバー攻撃被害やその報道の影響によるものと考えられる。

c-4.　オンライン診療に関する認知と経験

オンライン診療を知っているかは、最も多いのが「名前は知っているが内容をよく知らない」52.8%で、オンライン診療を知っている人が 43.9%、聞いたことがないが、3.3％。オンライン診療を知っている人（n=291）に、オンライン診療の経験の有無を聞いたところ、オンライン診療の経験があるが 15.1% （44 名）だった。

＜参考＞昨年度の結果（n=1111）は、聞いたことはあるが内容を知らないが 41.3%、聞いたことがないが、5.3%。オンライン診療を知っている人（n=459）に、オンライン診療の経験の有無を聞いたところ、オンライン診療の経験があるが 13.1% （60 名）だった。

ｃ－５．オンライン診療での症状や状況

オンライン診療の受診経験者（44 名）にオンライン診療の受診先を尋ねたところ、「初めての医療機関で、インターネット等での検索や口コミサイトで探した」が 45.5%（20 名）、「かかりつけの医療機関」が 27.3%（12 名）、「過去に受診した医療機関（オンライン受診では初めて）」が 15.9%（7 名）、「初診の医療機関で、かかりつけ医や関連の医療機関」が 9.1%（4 名）、だった。昨年度の結果は、71.7%（43 名）が「かかりつけの医療機関」と回答し、「初めての医療機関（インターネット等で検索）」が 16.7%（10 名）、「初診の医療機関で、かかりつけ医や関連の医療機関」が 8.3%（5 名）、「過去に受診した医療機関（オンライン受診では初めて）」が 3.3%（2 名）だった。

オンライン診療を受診した際の症状（n=44）は、発熱が最も多く 38.6%（17 名）、咳や喉の痛みが 34.1%（15 名）、身体のだるさ・不調が 20.5%（9 名）の順で多かった。その時の症状の現れ方は、急な症状が 47.7%、定期的な受診で自身がオンライン診療を希望が 34.1%、定期的な受診で主治医等に勧められたが 13.6%。オンライン診療を受診した場所は、自宅が最も多く 93.2%（41 名）、職場が 4.5%、車の中 2.3%だった。立会い等の有無は、本人のみが最も多く 84.1%（37 名）、家族や友人の同席が 13.3%（8 名）。

＜参考＞昨年度の結果は、オンライン診療を受診した際の症状は、発熱が最も多く 31.7%（19 名）、咳や喉の痛みが 13.3%（8 名）、身体のだるさ・不調が 18.3%（11 名）の順で多かった。その他が 16 名で、内訳は低用量ピルの処方、持病の定期検診、泌尿器科や ED,皮膚疾患の処方等での受診だった。その時の症状の現れ方（n=60）は、急な症状が 53.3%、定期的な受診で自身がオンライン診療を希望が 40%、定期的な受診で主治医等に勧められたが 5%。オンライン診療の受診の自身の場所は、自宅が最も多く 98.3%（59 名）、入院施設で、1.7%（1 名）。立会い等の有無は、本人のみが最も多く 86.7%（52 名）、家族や友人の同席が 13.3%（8 名）。

ｃ－６．オンライン診療での本人確認、利用端末機器の種類

オンライン診療の際の患者本人確認（n=44）については、「その医療機関の診察券や健康保険証を WEB で登録したり、スマホで撮影して画像をアップロードした」が最も多く 31.8%(14 名)、「かかりつけの医療機関のため、顔の確認のみ」が 29.5%で次に多く、「診察券番号もしくは健康保険証の番号を口頭で伝えた」は 18.2%（8 名）だった。オンライン診療で患者が利用した端末については、自身のスマホ・タブレット」が 84.1%（37 名）、「自身のＰＣ」が 9.1%(4 名)、「電話・テレビ電話」が 4.5%（２名）だった。その端末へのセキュリティ面の措置については（複数回答）、OS のセキュリティパッチの適用（月次アップデート実施や Windows Defender の更新）が最も多く

75.0%(33 名)、「ドコモ光など光回線を自宅や職場で契約して利用している。」が 31.8%(14 名)、「ウィルスソフトを購入しインストールしている」 20.5% (9 名)が続いて多かった。他に「TV 電話で何もしていない」は 4.5%（2 名）、「家族等に任せていてわからない」は 1.7%（1 名）だった。
＜参考＞昨年度の結果は、オンライン診療の際の患者本人確認（n=60）については、「かかりつけ医のため、顔の確認のみ」が最も多く 40%(24 名)、「診察券番号もしくは健康保険証の番号を口頭で伝えた」が 25%（15 名）で次に多かった。オンライン診療で患者が利用した端末については、自身のスマホ・タブレット」が 66.7%（40 名）、「自身のＰＣ」が 23.3%(14 名)、「電話・テレビ電話」が 8.3%（5 名）だった。その端末へのセキュリティ面の措置については（複数回答）、OS のセキュリティパッチの適用（月次アップデート実施や Windows Defender の更新）が最も多く 73.3%(44 名)、「ドコモ光など光回線を自宅や職場で契約して利用している。」が 25%(15 名)、「ウィルスソフトを購入しインストールしている」23.3%(14 名)が続いて多かった。他に「TV 電話で何もしていない」は 8.3%（5 名）、「家族等に任せていてわからない」「公共施設や駅などで無料の無線 LAN を使っている」が同数で 1.7%（1 名）だった。

ｃ－７.オンライン診療を受けた理由
オンライン診療を受けた理由は、「新型コロナウィルスの感染拡大で外来受診の不安があった」が最も多く 36.4%（16 名）、オンライン診療が便利なので（通院の手間や時間短縮）が 20.5%(9 名）だった。「通院する医療機関での勧め」は 18.2%、すぐに受診したかった（コロナ感染の疑いなど）が 15.9%、「興味があったから」は 4.5%（２名）だった。
<参考>昨年度の結果は、オンライン診療を受けた理由は、「新型コロナウィルスの感染拡大で外来受診の不安があった」「通院する医療機関での勧め」が同数で、33.3%（20 名）で最も多く、オンライン診療が便利なので（通院の手間や時間短縮）も 16.7.% (10 名）だった。また、興味があったから（ニュースや新聞などの話題）も 8.3%(5 名）あった。

ｃ－８.オンライン診療を受けた回数、受診の感想、継続の希望
オンライン診療を受けた回数は、初診で１回が 56.8%(25 名)、過去に１・２回（緊急時対応）が 34.1.%（15 名）で、毎月～３か月に１度の定期的受診（生活習慣病等）が 4.5%（2 名）だった。オンライン診療を受けた感想で、「満足」「多少問題はあったが満足した」を併せて満足という好意的な意見が 97.7%（43 名）で、不満足は実数にして１名であり、オンライン診療の経験者の大多数が好意的な意見だった。
また、具体的な感想について（複数回答）は、安心して診察が受けられたが 56.8%（25 名）、「医師等の説明が聞き取れない、もしくは疾患の状態を見せたり伝えたりできなかった。」が 22.7%（10 名）、接続や機器操作に手間取ったが 18.2%（8 名）、「処方箋の発行や処方箋の送付に時間がかかった」が 15.9%（7 名）で、オンライン診療特有の課題点も見られた。
今後のオンライン診療の継続については、場合によっては受けたいを含め、「今度も継続して受けたい」が 97.7%(43 名)だった。具体的な理由や条件としては、「検査以外はオンライン診療を受けたい」が 51.2%（22 名）、「新型コロナウィルの感染拡大によってはオンライン診療を受けたい」が 30.2%（13 名）、「自分でオンライン診療と通院を選択したい」「オンライン診療の医療機関が増えれば」は、各々7.0% （3 名）だった。
＜参考＞昨年度の結果は、オンライン診療を受けた回数は、初診で１回が 48.3% (29 名)、過去に１・２回（緊急時対応）が 26.7.%（16 名）で、毎月～３か月に１度の定期的受診が 15%（9 名）、毎回（検査や注射以外の受診）も 8.3%（5 名）いた。オンライン診療を受けた感想で、「満足」「多少問題はあったが満足した」を併せて満足という好意的な意見が 96.7%（58 名）で、オンライン診療の経験者のほとんどが好意的な意見だった。また、具体的な感想について（複数回答）は、安心して診察が受けられたが 68.3%（41 名）、「医師等の説明が聞き取れない、もしくは疾患の状態を見せたり伝えたりできなかった。」が 23.3%（14 名）、接続や機

器操作に手間取ったが 3.3%（2 名）、自宅などの接続環境や操作方法がうまくいかなかった」が 5.0%（3 名）だった。

今後のオンライン診療の継続については、場合によっては受けたいを含め、「今度も継続して受けたい」が 91.7%（55 名）だった。具体的な理由や条件としては、「検査以外はオンライン診療を受けたい」が 60%（33 名）、「新型コロナウィルの感染拡大によってはオンライン診療を受けたい」が 21.8%（12 名）、「自分でオンライン診療と通院を選択したい」「オンライン診療の医療機関が増えれば」「受診料が安くなれば」は各々5.5%（3 名）で少なかった。

ｃ－９.オンライン診療と対面受診への意識

オンライン診療を知っていて受けたことがない回答者（n=247）に、その理由を確認したところ、「通院先がオンライン診療に未対応だから」が最も多く 38.5%、「対面での診療を希望するため」が 23.9%、「検査等で対面でないと対応不可のため」が 17.4%だった。

最後に、全回答者（n=663）に「対面診療以外にオンライン診療が必要と思うか」を確認した。オンライン診療も必要とする意見が 54.4%で、オンライン診療は不要とする意見は 15.8%だった。
同様に全回答者に「オンライン診療と対面診療について」の意見を尋ねた（n=663）。「オンライン診療は不要（対面診療が基本）」が 8.1%で昨年度が 8.3%で、ほぼ変わりがなかった。また、新型コロナの蔓延など緊急事態の場合もしくは通常時から本人が選択を含め、「オンライン診療が必要」という意見は 77.6%で、「オンライン診療の環境を国や自治体が整えたうえでオンライン診療が必要」という意見は 13.7.%だった。昨年度は、前者が 80.4%、後者が 10.2%でほぼ同じ傾向が見られた。

ｃ－１０．標準的セキュリティポリシーの検討

従来のガイドラインの構成では情報ガバナンスは６．１章の方針の制定のみに記載があり、具体性にかけていたが、改定作業班の議論において、本来情報の安全管理は、ガバナンス、マネージメント、コントロールという三層構造の対策が必要で、指針自体を大幅に改訂し、この三層構造を基本とすることになった。最上位層であるガバナンスは経営管理編であるが、その内容のかなりの部分は実質的にセキュリティポリシーの内容に関するもので、体制の整備から asset classification、さらには持続的改善に関する事項も含まれることになった。したがってここで指針とは別に標準的セキュリティポリシーを策定するより、指針第６版の公表を経て、その普及度合いをあらためて検証することが適切と考えられた。

Ｄ．考察

昨年度の結果と比較して、回答者のプロファイルには目立った違いはなく、受診歴や受診状況に関しても、ほぼ傾向は同じだった。ただ、マイナンバーカードの所持が、昨年度の 68.1%から 87.5%で所持有が２０%増えたこと、また、所持していない人の内、24%は近いうちに申請予定で、それ以外 76%の人の未申請の理由として、昨年度最も多かった「手続きが面倒」が大幅に減ったこと、「個人情報の漏洩が怖い」「国自治体に管理されたくない」という理由が半数近くあったことなど、昨年度と大きな差がみられた。

医療機関の電子化については、「電子カルテやオンライン診療システムを導入している場合は、患者がちゃんと理解できるように、HP や院内掲示で説明が必要である」が「そう思う」という意見が 67.9%で高く、昨年度の 63%に続いてやはり高い傾向が見られた。今回、唯一追加した「マイナンバーカードを保険証として利用すると医療費が安くなるなら使いたい。」については、61.5%で他の項目と比較すると 20%程高く、昨年度のマイナンバーカードの普及促進の効果と関心の高さが見られた。また、昨年度は 47.3%だった「医療機関ではセキュリティの専門家がいると思えないので個人情報の漏洩など心配」が、54.8%に上がっており、昨年度起きた医療機関のサイバー攻撃被害やその報道の影響によるものと考えられる。オンライン診療の認知は、「聞いたことはあるが内容を知らない」が昨年度と同様に 50%程度で、３%程度ではあるが「知って

いる」が増えていた。

オンライン診療の経験者は 15.1%で、昨年度から２%ではあるが増えていた。大きな差が見られたのがオンライン診療の受診先医療機関で、昨年度は「かかりつけの医療機関」が 71.7%で受診先の殆どを占めていたが、今回は、「初診の医療機関でインターネットで検索したクリニック等」が 45.5%で最も多く、かかりつけの医療機関が 27.3%でかなり開きが見られた。これも、新型コロナウィルス感染症の変化や制度の見直しが要因の一つとも考えられる。

また、オンライン診療で利用する端末はスマーフォン・タブレットが増え、昨年度の 66.7%から 84.1%に一気に増加した。この点は、オンライン診療システムが医療機関に普及し、大手のベンダーによりオンライン診療アプリが患者側に提供され、スマホのポップアップ広告や TVCM 等でも頻繁に目にする機会が増えたこと、患者側でオンライン診療に対する構えが軽くなり、新型コロナウィルス感染症への対応も、個人で判断する場面が多くなったことも関係すると考えられる。オンライン診療で利用した端末においては、PC は減っていたが、機器端末のセキュリティ措置については、「家族に任せていてわからない」は１名しかおらず、殆どが月次アップデートの実施や、ウィルスソフトを購入して利用、光回線を契約しているなど、ＩＴリテラシーに関してもある程度は備えていることが伺える。

また、オンライン診療に関しては、昨年度と同様、受診を経験した人の大多数は満足と回答していた。受診時には、機器の接続の問題やコミュニケーションの取り方などの課題が上げられたが、これについては、オンライン診療サービス自体の問題というより、経験者の殆どが初めてもしくはそれに近く、不慣れなために起きた事象と推測される。

今後、マイナンバーカードの普及や電子処方箋サービスの普及により、オンライン診療に対応できる医療機関が増え、これまでハードルの高かった患者にとってもオンライン診療が身近な存在になると想定される。患者はタブレットやスマホで気軽に接続が可能である半面、やはりセキュリティ面での措置も疎かになる可能性が高く、今後はこれらの通信機器も攻撃の対象ともなり得る。患者側は年齢、生活環境等様々で、患者の通信機器に対して一律に適切な措置を求めることは難しいため、オンライン診療で利用する医療機器側の端末は、電子カルテシステムとは切り離すなど、医療機関側に適切な措置が必要と考えられる。

医療ＤＸの動きを鑑みると、今後は対面診療とオンライン診療の有機的な結合が求められることは明白で、IT リテラシーを一律には期待できない患者端末を用いるオンライン診療システムとの接続を前提にする必要がある。この場合、リスクの大部分はサイバーセキュリティであり、十分な対策が求められる。

令和５年度の前半にリリース予定である医療情報システムの安全管理に関するガイドライン 6.0 版は、サイバーセキュリティに関しても一定の記載があり、対応策も述べられている。しかし、ネットワークセキュリティに関しては、2007 年にレセプトオンラインの開始に際して強化されたものの、現状のクラウド化の流れや、オンライン診療の急速な普及、あるいは保険資格のオンライン確認システムの導入やそれに伴うデータヘルス集中改革で導入が進められている様々なシステムに対応可能かどうかは十分に検証されていないと考えられる。ネットワークセキュリティ、サイバーセキュリティを中心に速やかに検証を進め必要に応じた改訂を進めることが望まれる。

Ｅ．結論

計３年に渡ってオンライン診療に焦点をあててアンケート調査を行った。調査の方法が WEB アンケートであるため一定程度のバイアスはあるものの、オンライン診療の認知も経験者も僅かではあるが年々増加しており、マイナンバーカードの普及や健康保険証としての利用や、マイナポータルの利用用途の広がりなど、医療健康サービスを受ける側の患者の環境や意識も大きく変わりつつある。

また、医療機関においても、オンライン保険資格確認、電子処方箋、オンライン診療と様々な意味で、医療機関にとって外部ネットワークへの依存は避けがたく、サイバーセキュリティ対策の重要性はますます増加している。ただ一般に言われているサイバ

ーセキュリティ対策は医療機関に固有のものではなく、対策も一般的に述べられていることが多い。医療機関の IT 化やネットワーク依存は進んでいるものの、IT 化自体は目的ではなく、あくまでもツールであり、また制度的に促進されたものもあり、サイバーセキュリティ対策も自らリスク分析を行う積極的対応ではなく、モデル対策の一部だけ対応するといった医療機関もあると思われる。まもなく発出される「安全管理ガイドライン第 6 版」では、このような医療機関の特性にも配慮し、みずからリスク分析を行う積極的対策を誘導するような工夫が施されており、少しでも早く医療機関へ浸透することが望まれる。

Ｆ．研究発表

吉田　真弓，山本 隆一，患者への意識調査に基づいたオンライン診療および医療機関の電子化に関する調査研究,第４２ 回医療情報学連合大会，札幌市，口演発表， 2022 年 11 月

Ｇ．添付資料：

参考資料１．2022 年度アンケート調査結果グラフ

参考資料２．2021 年度アンケート調査結果グラフ

＜参考 1＞アンケート調査結果（2023 年 3 月実施） グラフ表示※

※人数表記がない場合は、回答者数は 663 名（n=663）、単一回答とする。

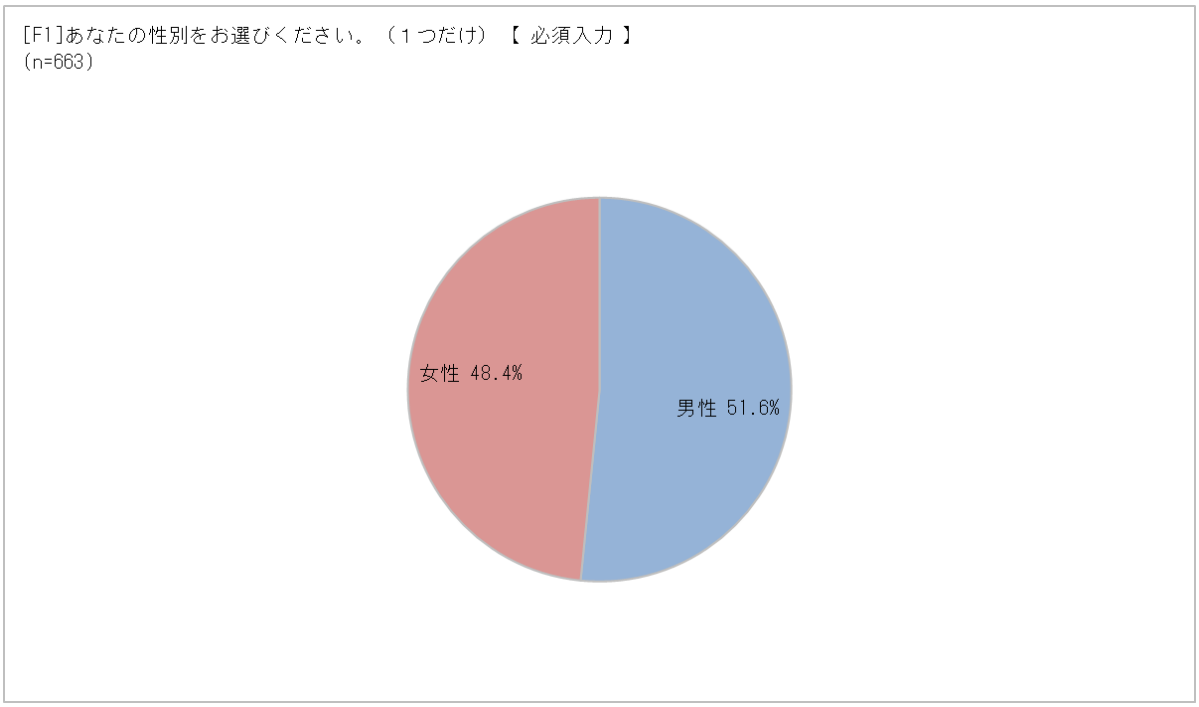


Figure1.性別

	全体	(663)
1	北海道	6.0
2	青森県	0.8
3	岩手県	0.3
4	宮城県	1.5
5	秋田県	0.3
6	山形県	0.6
7	福島県	0.9
8	茨城県	1.4
9	栃木県	1.2
10	群馬県	0.3
11	埼玉県	4.5
12	千葉県	5.1
13	東京都	14.8
14	神奈川県	8.9
15	新潟県	1.5

16	富山県	0.8
17	石川県	0.6
18	福井県	0.3
19	山梨県	0.3
20	長野県	0.9
21	岐阜県	1.5
22	静岡県	3.5
23	愛知県	6.3
24	三重県	1.2
25	滋賀県	1.2
26	京都府	1.5
27	大阪府	9.5
28	兵庫県	6.0
29	奈良県	1.4
30	和歌山県	0.2
31	鳥取県	0.9
32	島根県	0.2
33	岡山県	1.4
34	広島県	2.7
35	山口県	0.5
36	徳島県	0.8
37	香川県	0.3
38	愛媛県	1.7
39	高知県	0.2
40	福岡県	4.1
41	佐賀県	0.5
42	長崎県	1.1
43	熊本県	1.4
44	大分県	0.3
45	宮崎県	0.3
46	鹿児島県	0.6
47	沖縄県	0.2

Table1. 回答者居住地

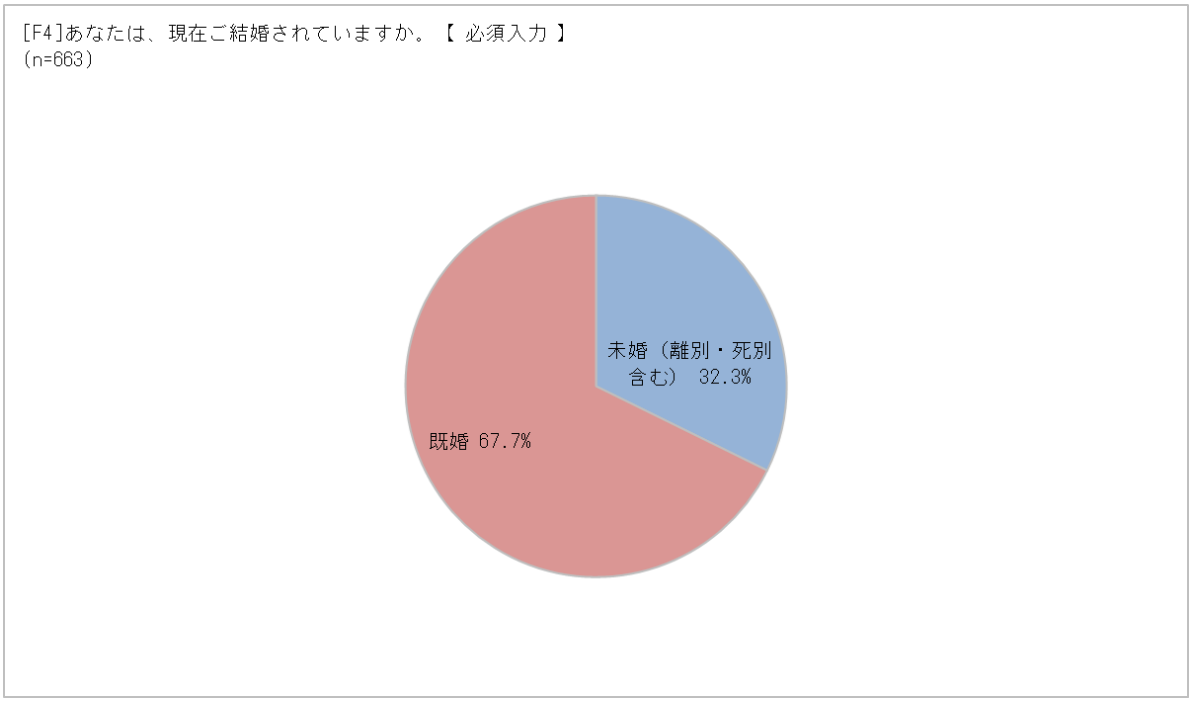


Figure3. 婚姻状況

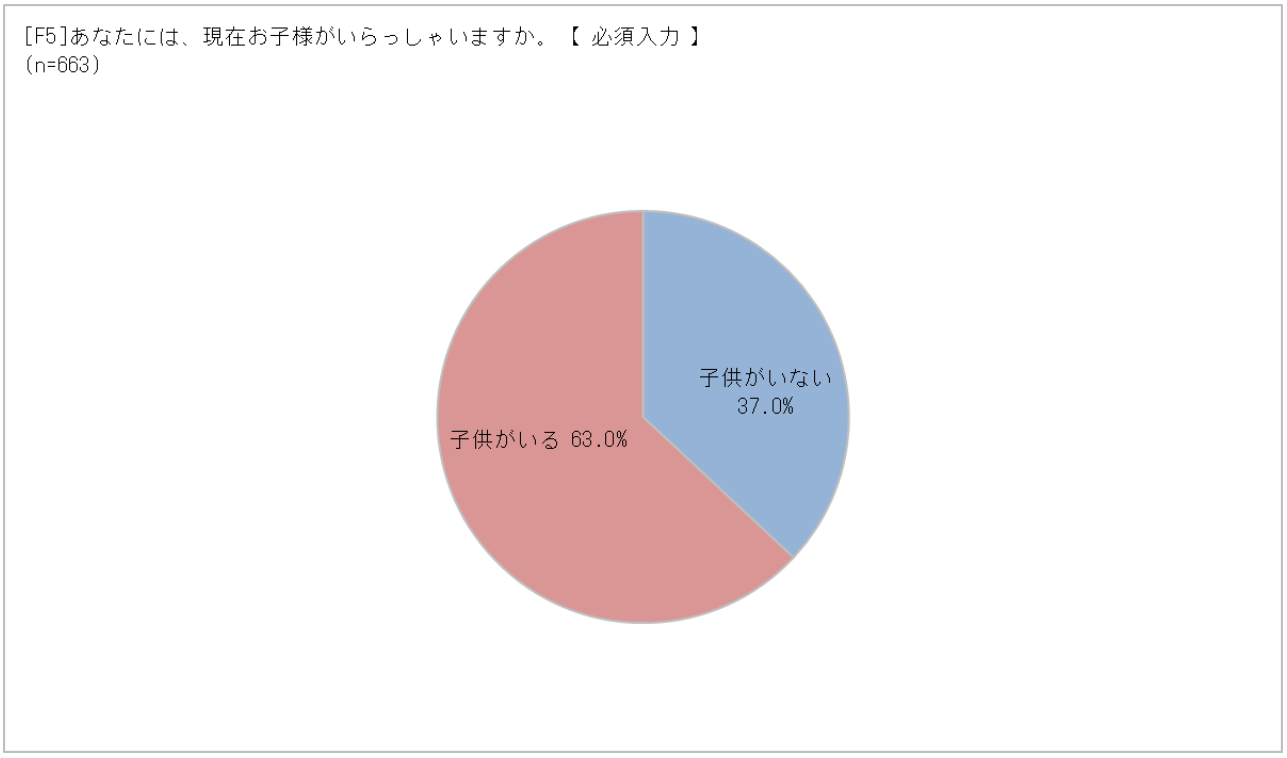


Figure4. 子供の有無

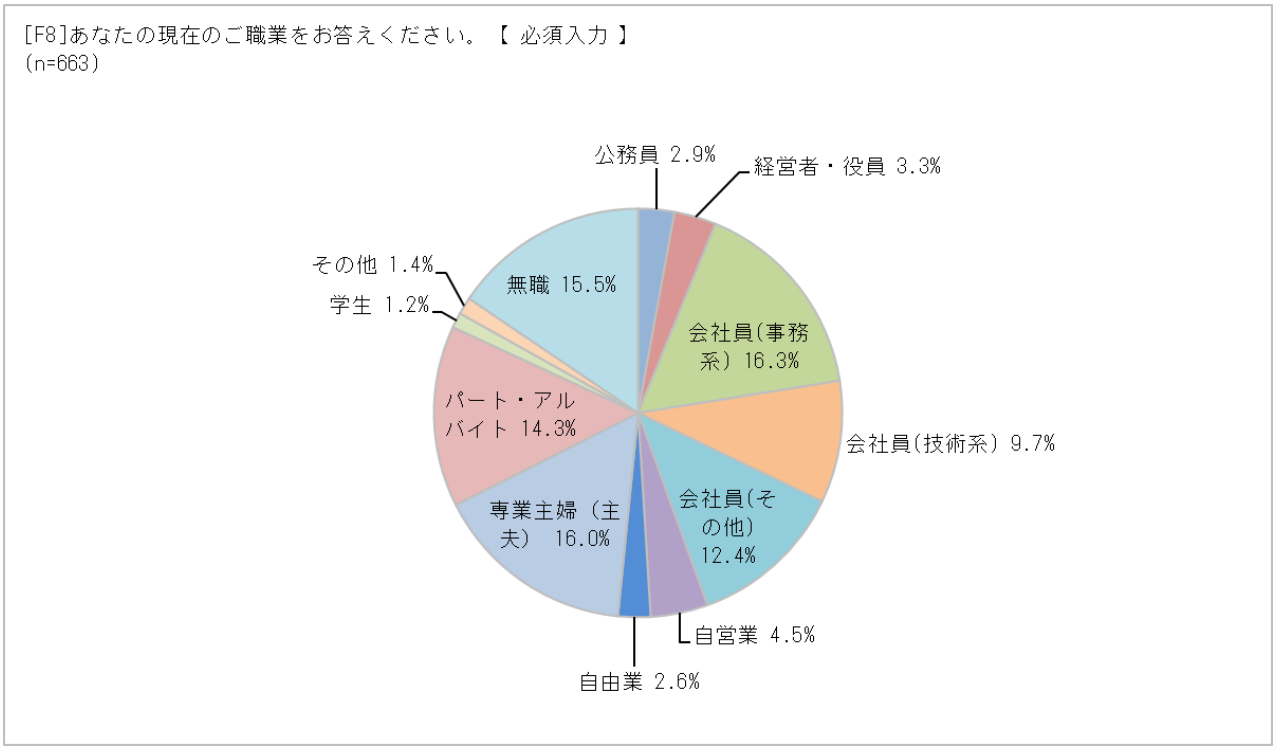


Figure5. 職業

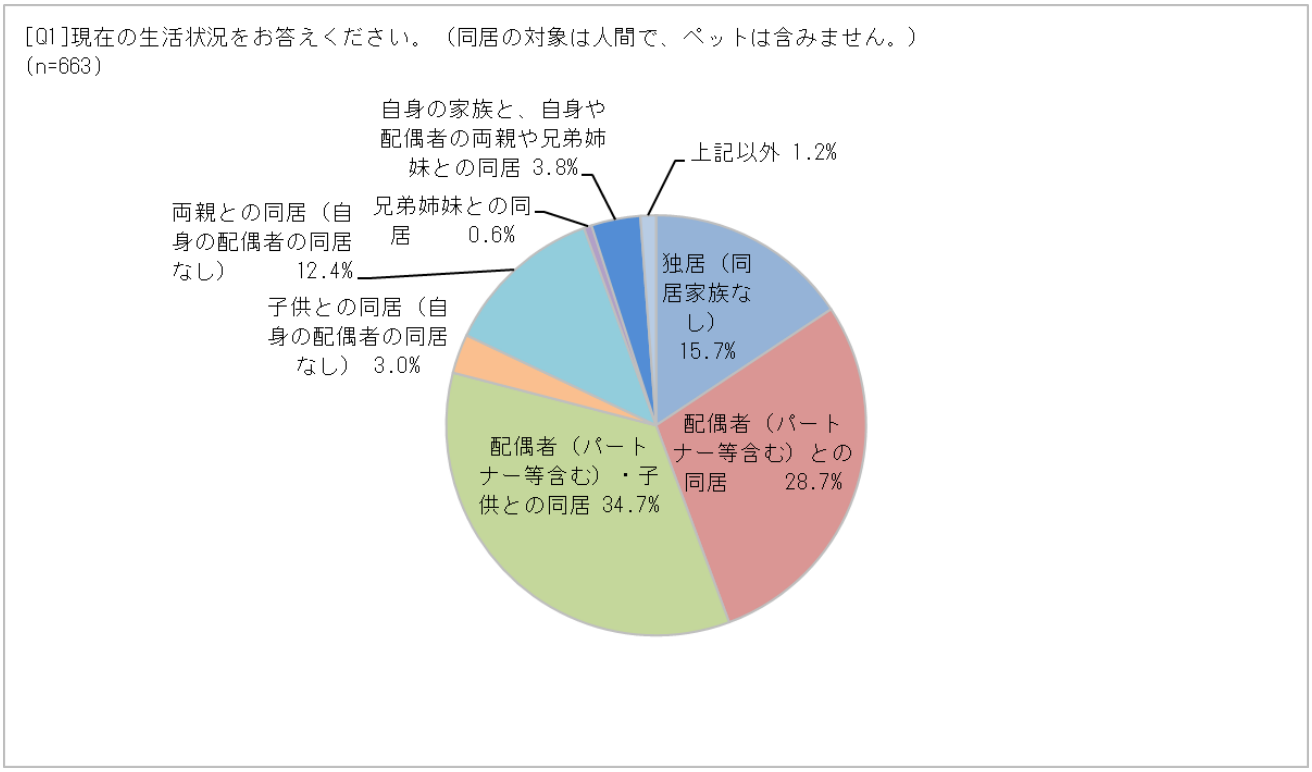


Figure6.生活状況

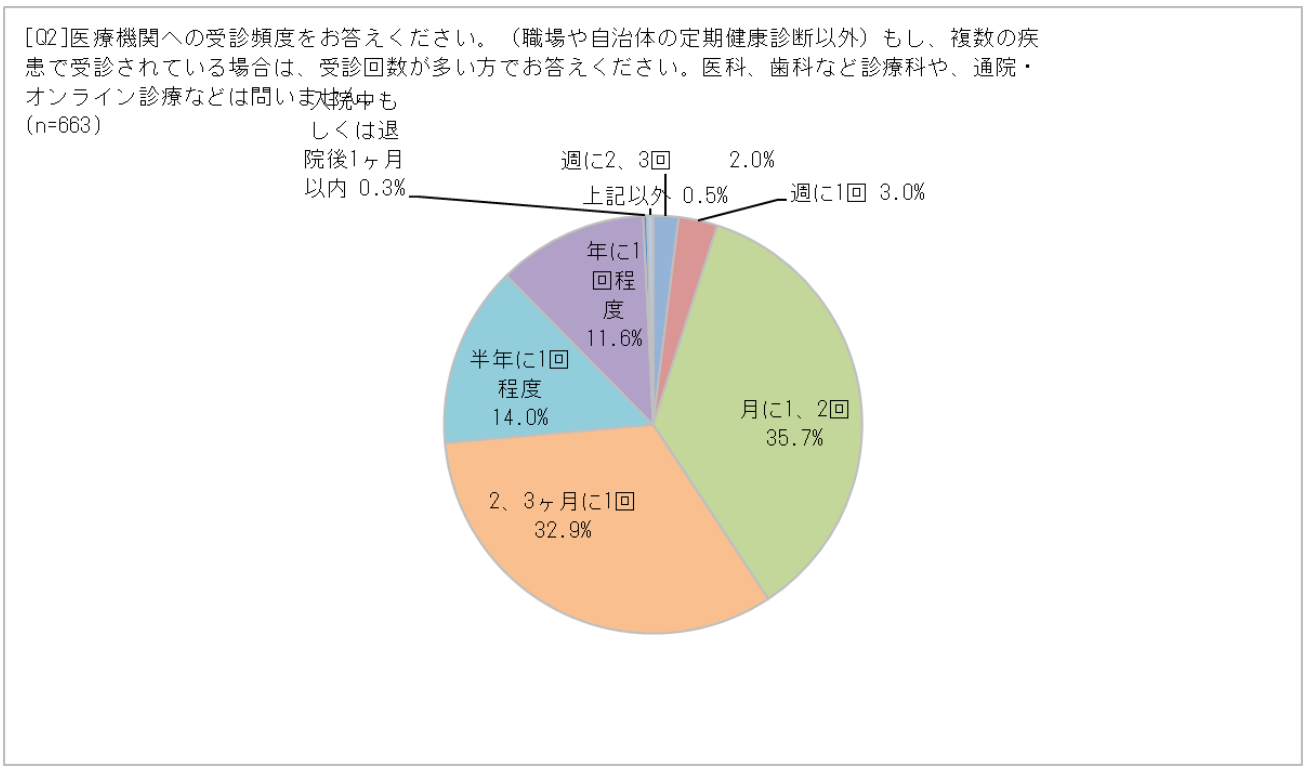


Figure7. 受診の頻度

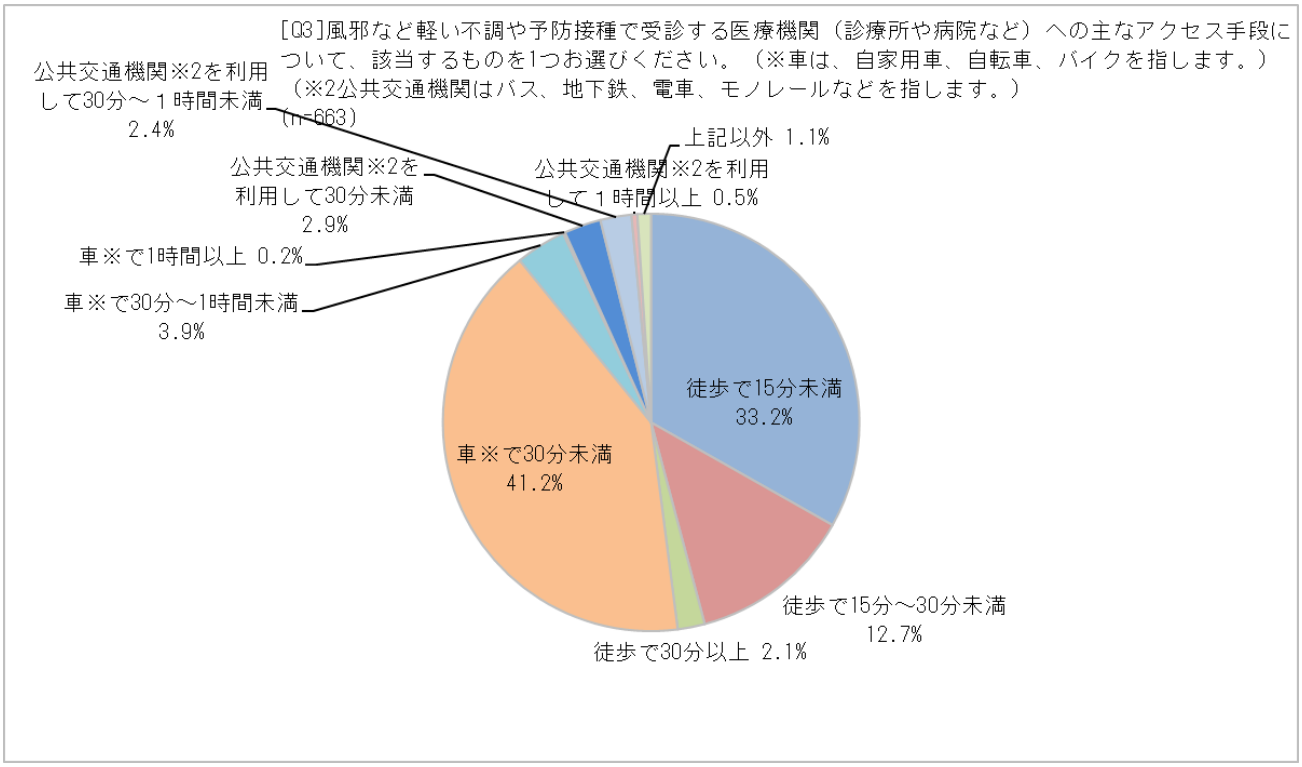


Figure8.受診する医療機関へのアクセス状況

	全体	(663)
1	内科	52.6
2	小児科	1.5
3	皮膚科	20.2
4	婦人科	10.1
5	産科（妊娠出産等で、産婦人科を受診されている方はこちらを選択）	2.9
6	耳鼻咽喉科	15.4
7	眼科	18.1
8	整形外科	12.5
9	アレルギー科	0.8
10	泌尿器科	4.2
11	肛門外科	1.4
12	胃腸内科	2.4
13	気管食道内科	0.2
14	胸部外科	0.0
15	形成外科	1.2
16	血管外科	0.0
17	心臓血管内科	0.6
18	呼吸器内科	2.1
19	呼吸器外科	0.5
20	心療内科	3.9
21	消化器内科	2.1
22	脳神経内科	1.7
23	心臓血管外科	0.9
24	消化器外科	1.4
25	小児外科	0.3
26	循環器内科	5.6
27	腎臓内科	1.2
28	精神科	4.5
29	糖尿病内科	1.4
30	内分泌内科	0.8
31	乳腺外科	1.4
32	脳神経外科	2.6
33	美容外科	0.8
34	ペインクリニック	0.6
35	放射線科	0.2
36	麻酔科	0.2
37	リハビリテーション科	0.5
38	リウマチ科	0.9
39	老年内科	0.0
40	外科	3.2
41	歯科	31.7
42	その他	1.5
43	回答したくない	1.7

Graph 9. 受診する(した)診療科（複数回答）

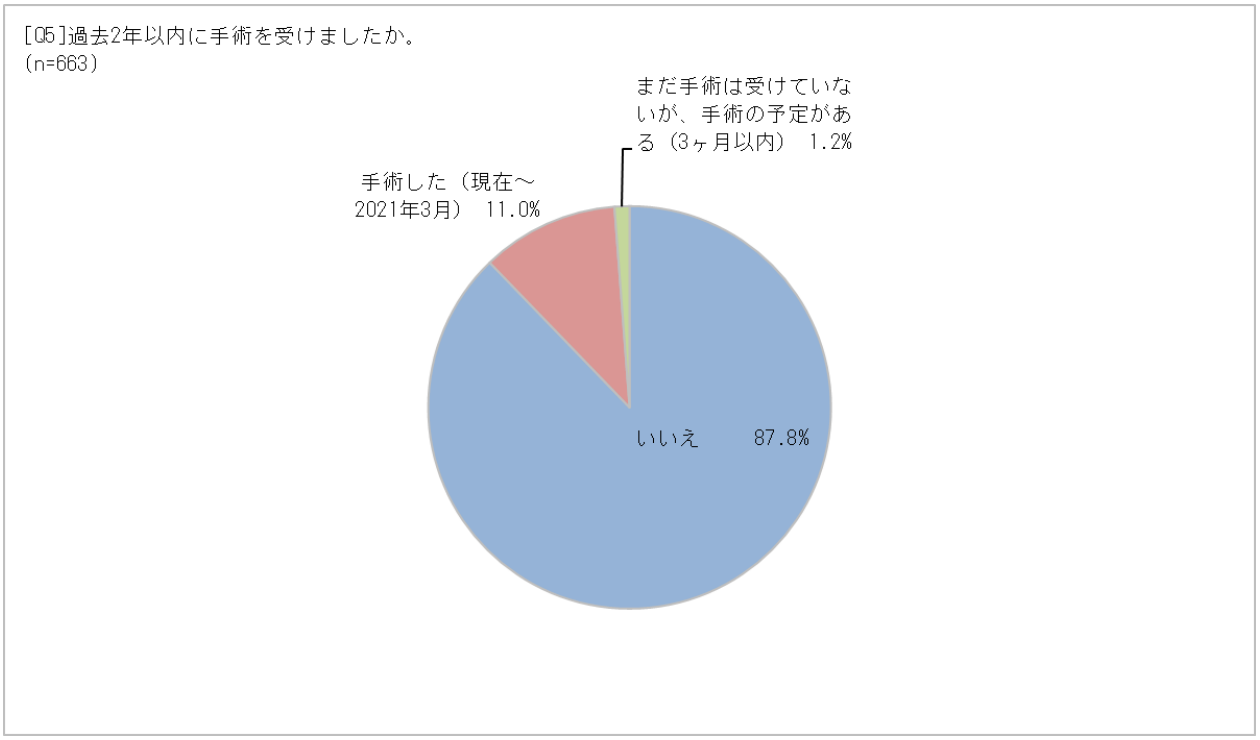


Figure10.過去2年間の手術歴

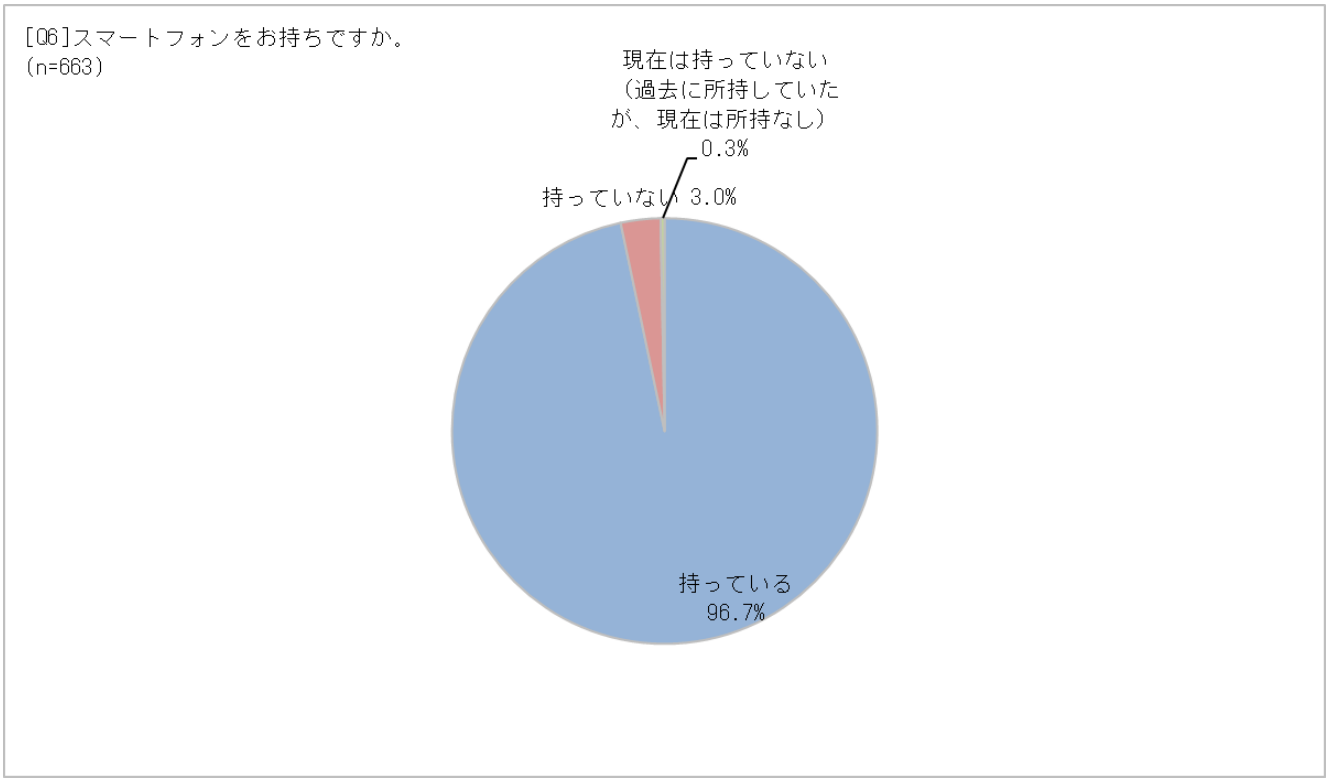


Figure11.スマートフォンの所持

[Q7]ご自身のマイナンバーカードを持っているか教えてください。（お住まいの自治体にてマイナンバーカードの交付申請手続き中、もしくはカードの受取り予定の方も含みます。）
(n=663)

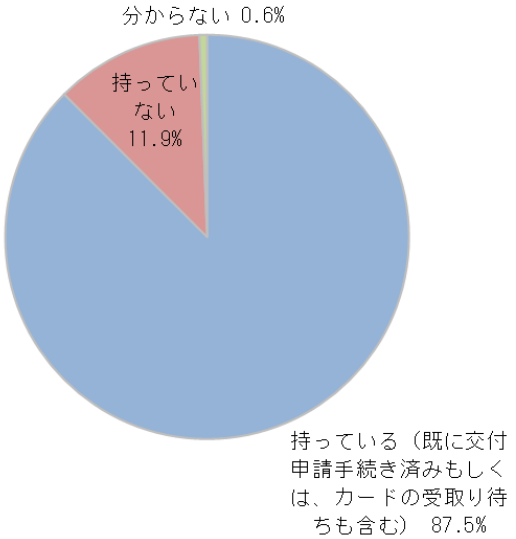


Figure12.マイナンバーカードの所有

[Q8]マイナンバーカードを持っていないと回答された方にお尋ねします。マイナンバーカードを持っていない理由を教えてください。当てはまるものが複数ある場合は、最も強い理由をお選びください。
(n=79)

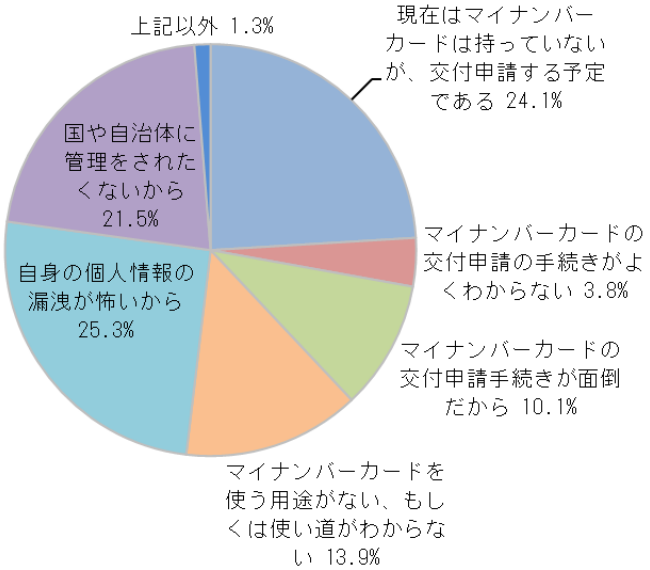


Figure13.マイナンバーカードを所有していない理由

［Q9］ 最近、医療機関（病院や診療所）では電子カルテのオンライン診療を導入するなど、電子化が進められています。また、日本政府によりマイナンバーカードの利用促進が行われており、マイナンバーカードが健康保険証として利用できるようになり、マイナンバーカードとマイナポータルを使えば、自分のスマートフォンで健診結果や薬剤情報が確認できたり、医療費控除も便利に行えるようになりました。将来的には PHR（Personal Health Records）という、健康医療データの個人口座の中に、乳幼児期の予防接種情報や医療機関での検査結果、健診の結果、お薬手帳の情報などが保管されることになります。PHR は、自分がケガや病気で受診した時に医師や看護師への説明に使ったり、自分の健康維持にも使えます。あなたのもしもの時、例えば意識不明で救急搬送されたり大規模災害の時でも、あなたの記憶やカルテの代わりに使えます。このように医療制度や生活環境が電子化の推進で便利になる一方、コンピュータウイルスの蔓延やハッカーによる侵入などの危険性について、セキュリティの専門家などから指摘されています。以下のそれぞれの項目について、ご自身の感覚にもっとも近いものを 1 つ選んでください。

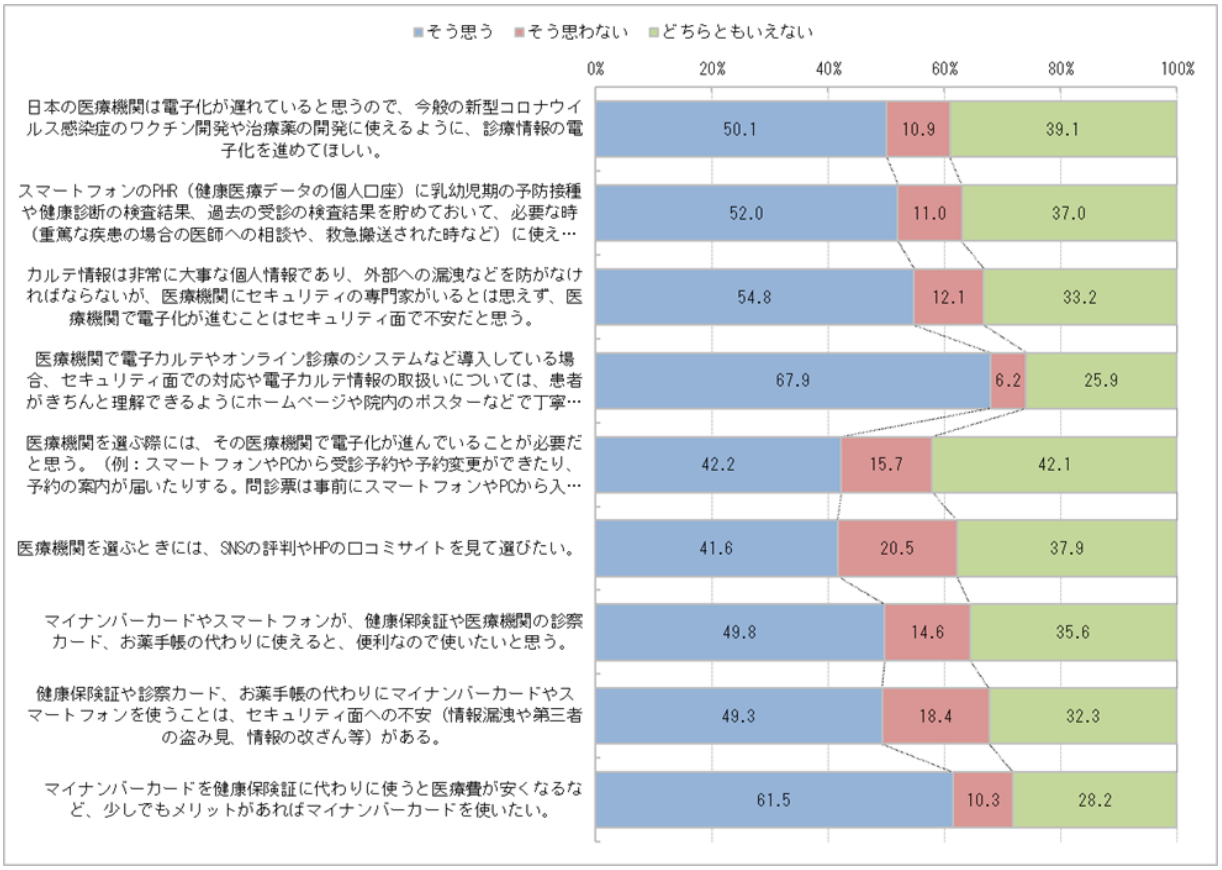


Figure14.医療機関の電子化への感想

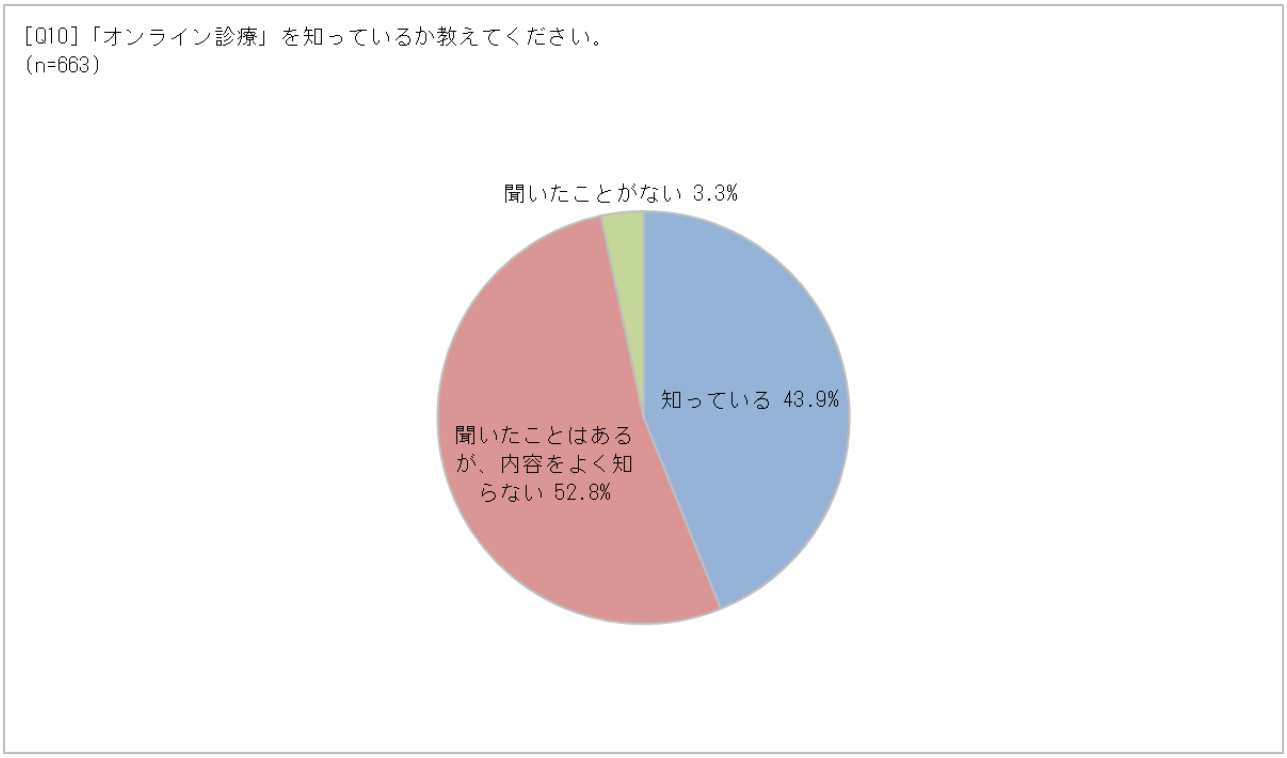


Figure15.オンライン診療の認知

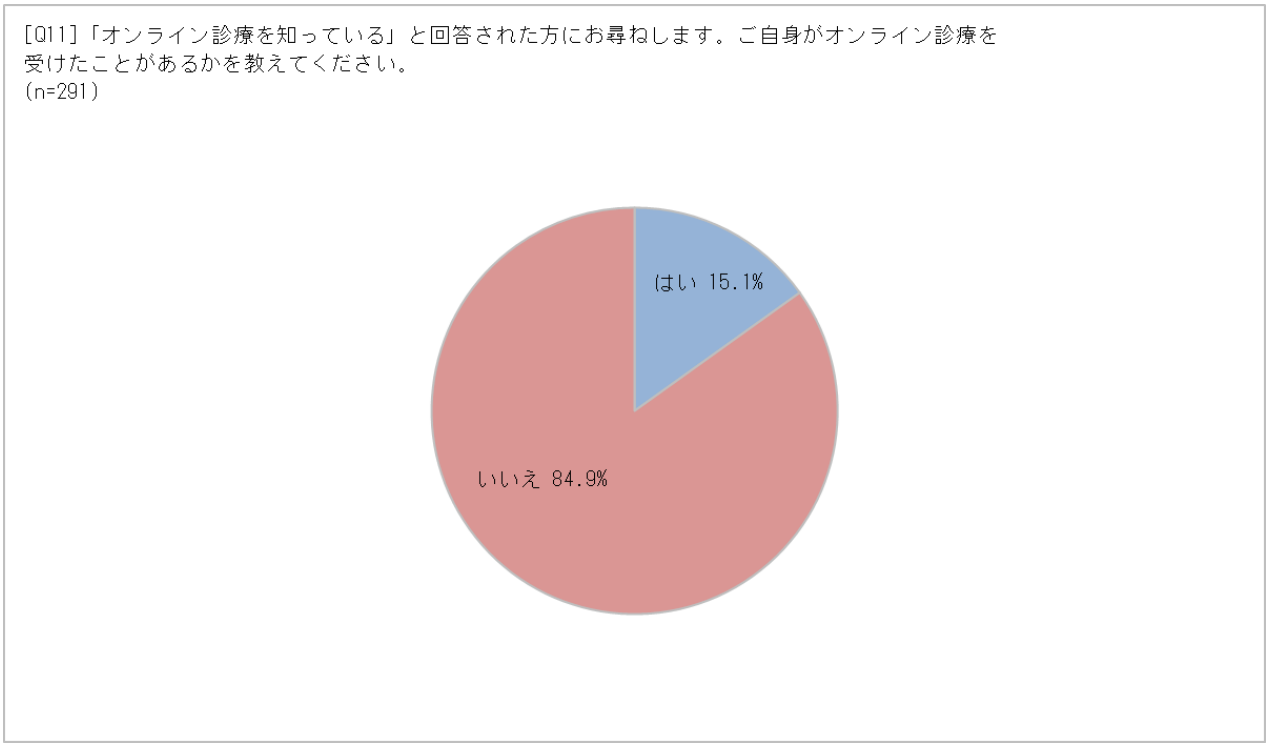


Figure16.オンライン診療の受診経験（対象:「オンライン診療」既知の回答者）

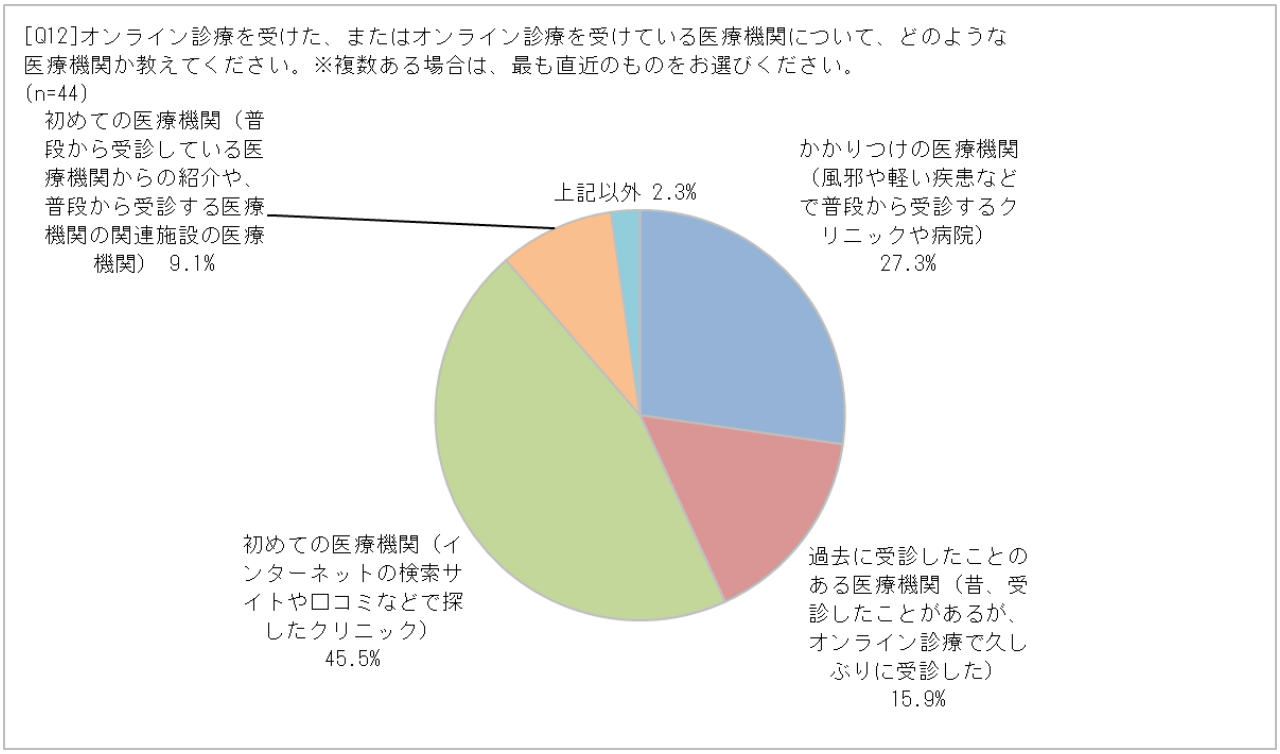


Figure17.（対象：経験者）オンライン診療を受けた医療機関について

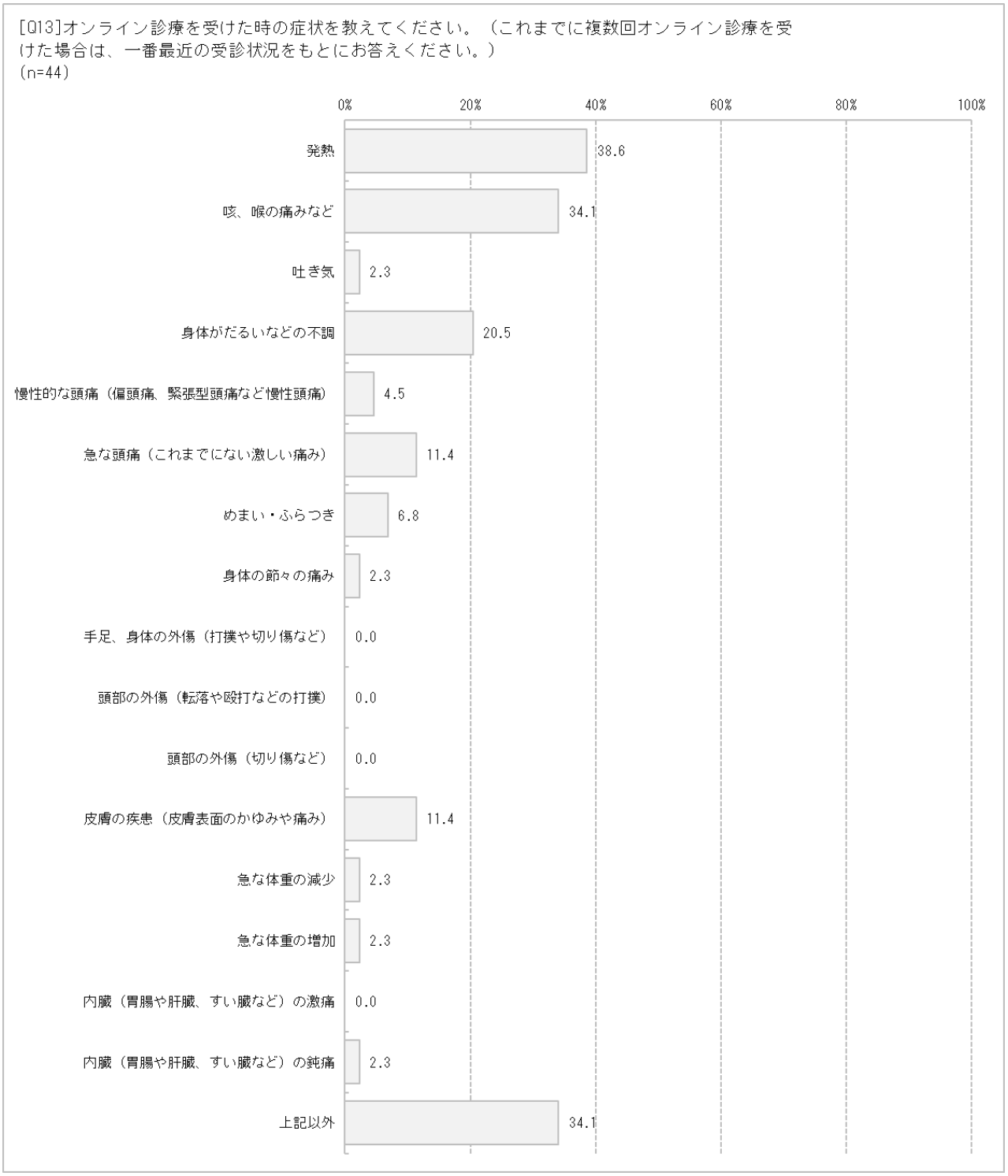


Figure18.（対象:経験者)オンライン診療を受けた際の症状＜疾患傷病等＞（複数回答）

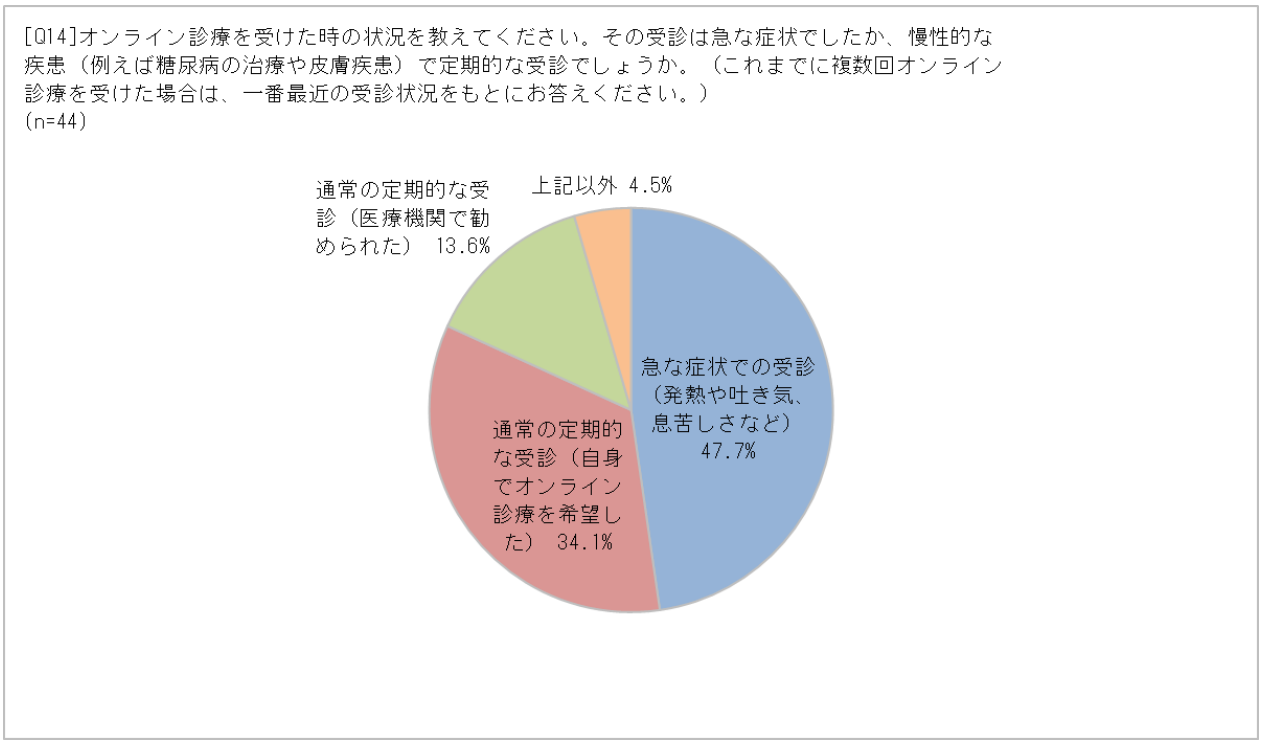


Figure19.（対象:経験者)オンライン診療を受けた際の状況＜発症＞

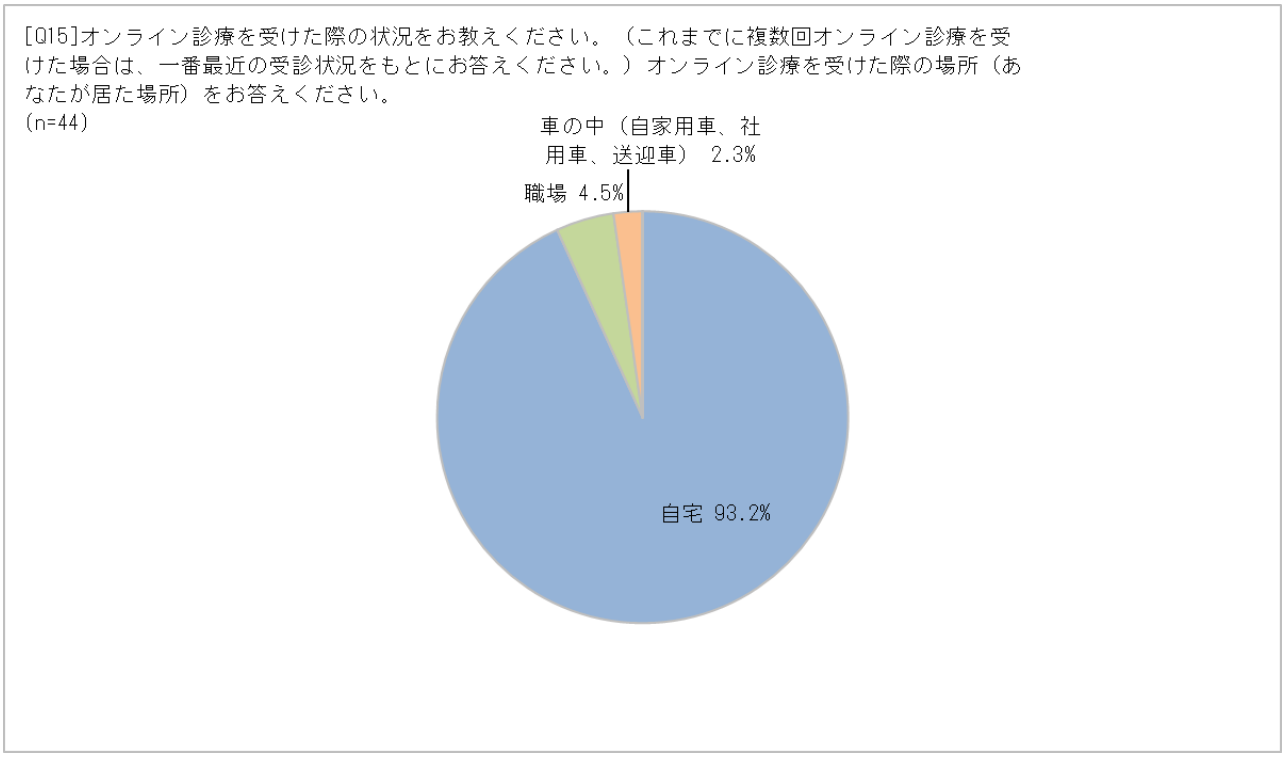


Figure20.（対象:経験者)オンライン診療を受けた際の状況＜場所＞

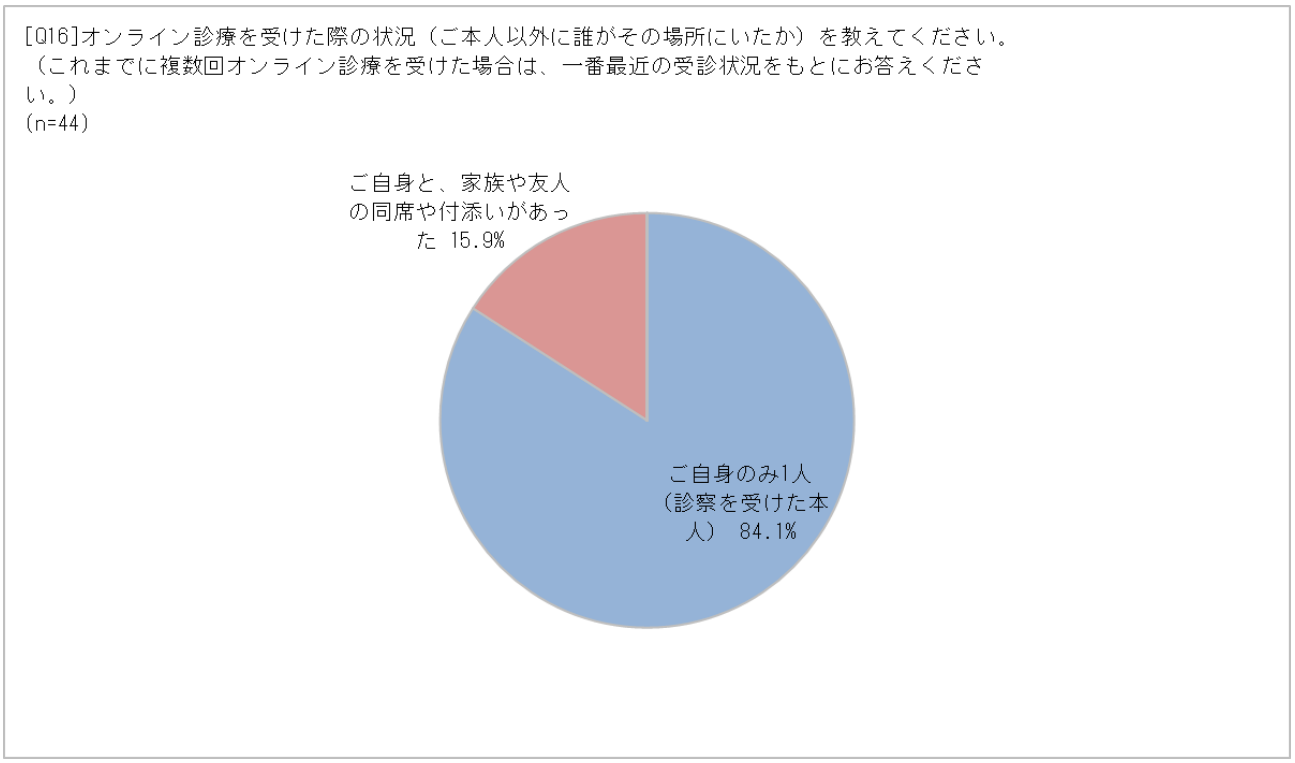


Figure21.（対象：経験者）オンライン診療の状況＜立会者等の有無＞

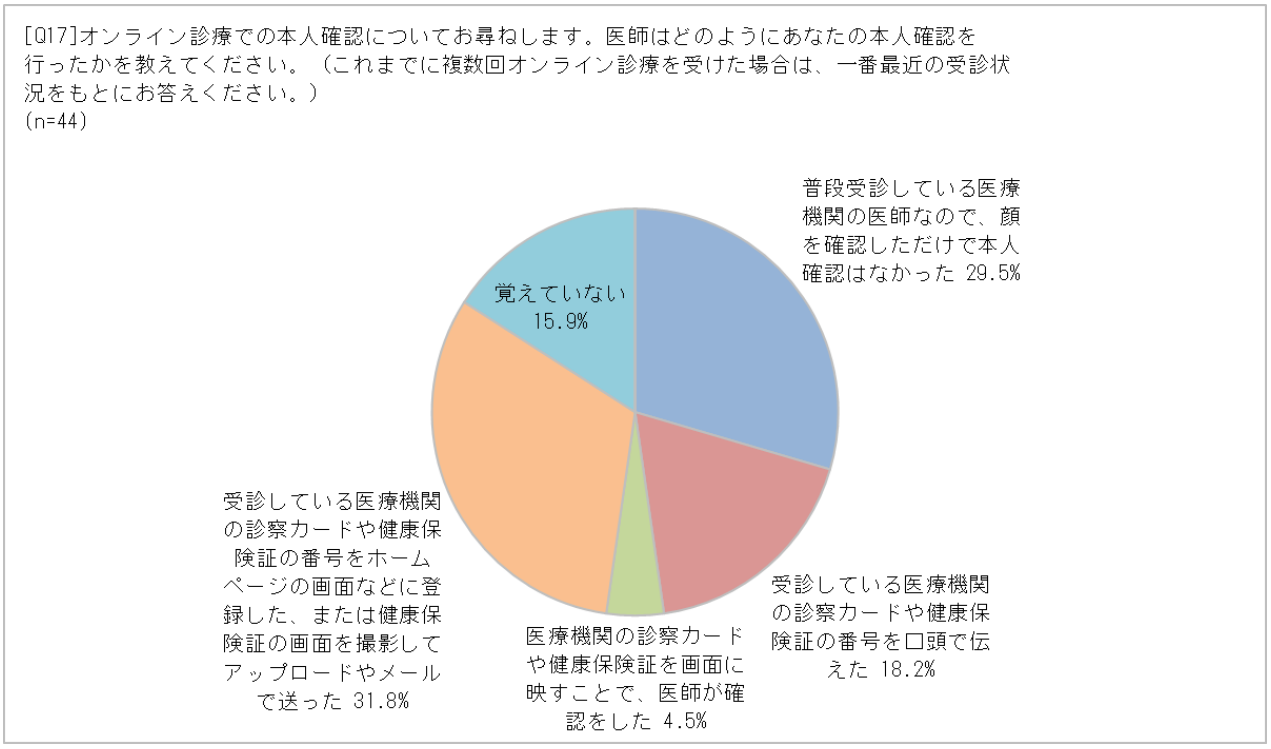


Figure22.（対象：経験者）オンライン診療での本人確認の方法

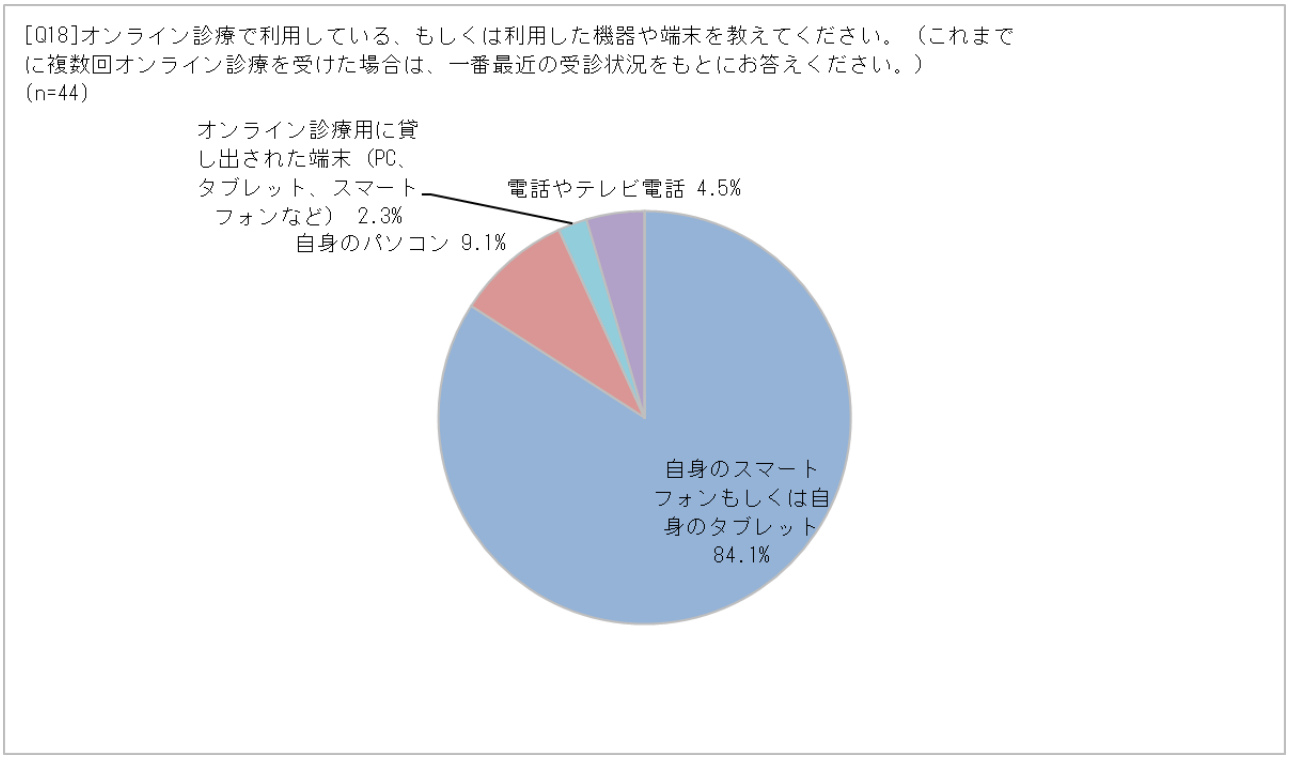


Figure23.（対象：経験者）オンライン診療で利用している機器・端末の種類

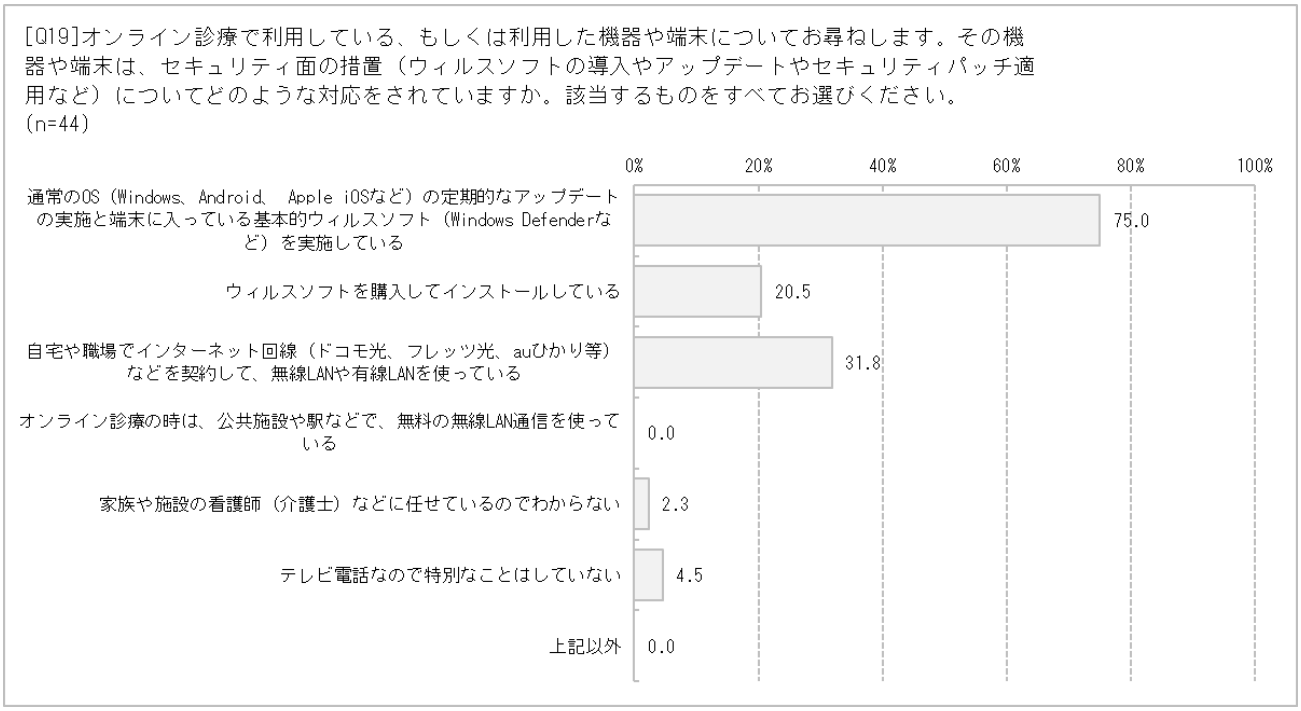


Figure24.（対象：経験者）オンライン診療で利用する端末のセキュリティ措置

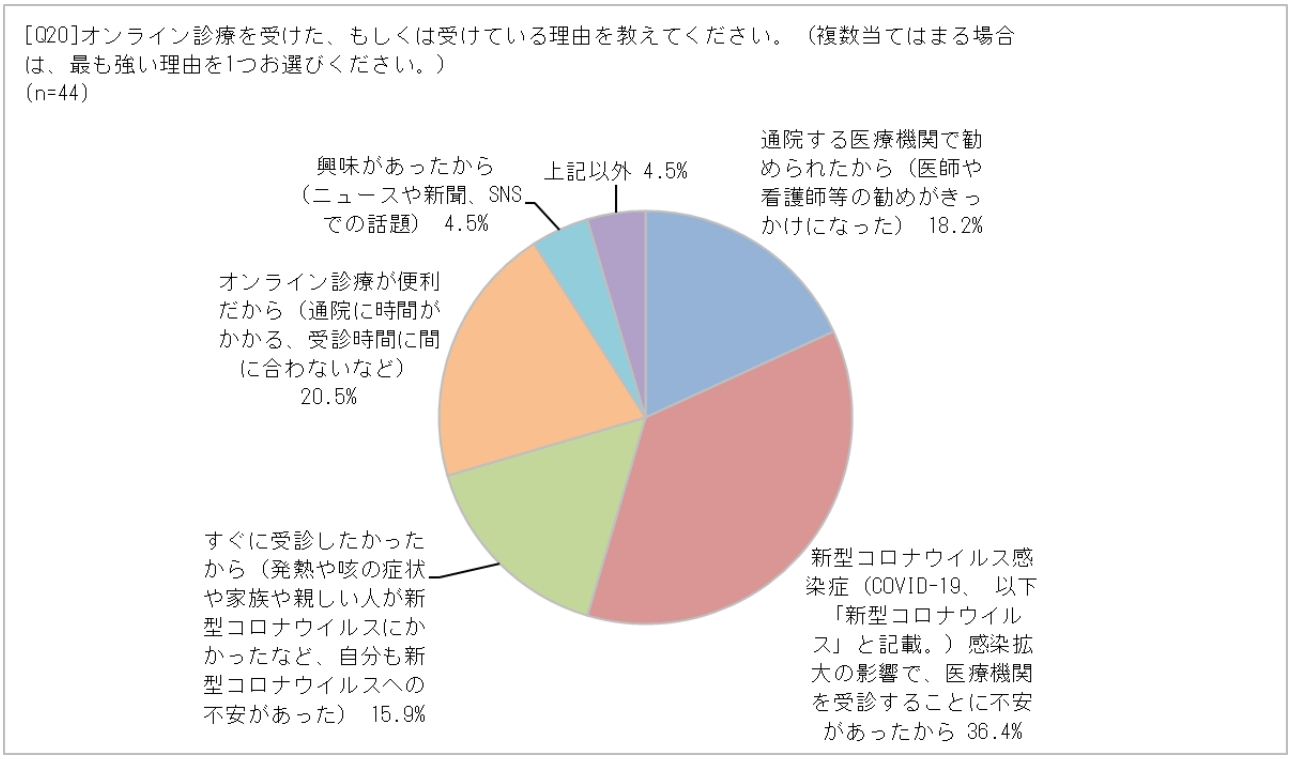


Figure25.（対象:経験者）オンライン診療を受けた理由

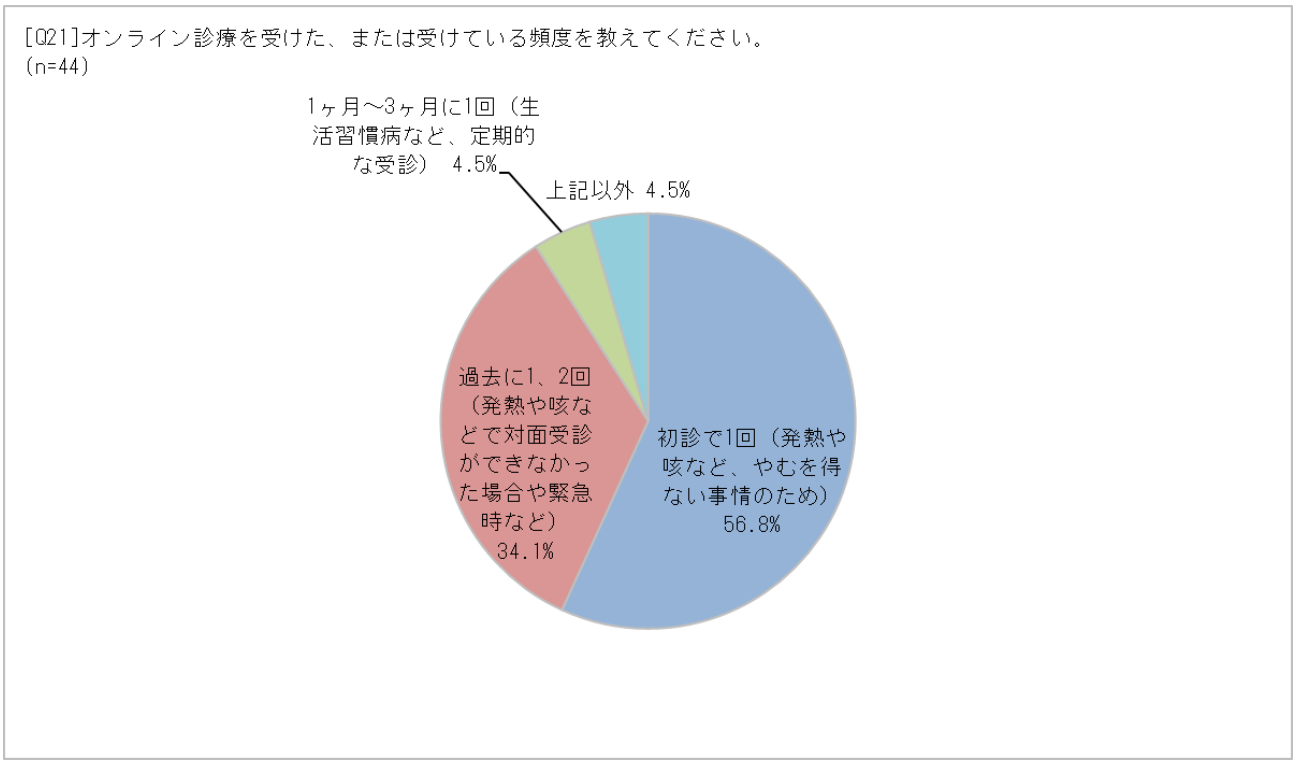


Figure26.（対象:経験者）オンライン診療の受診の頻度

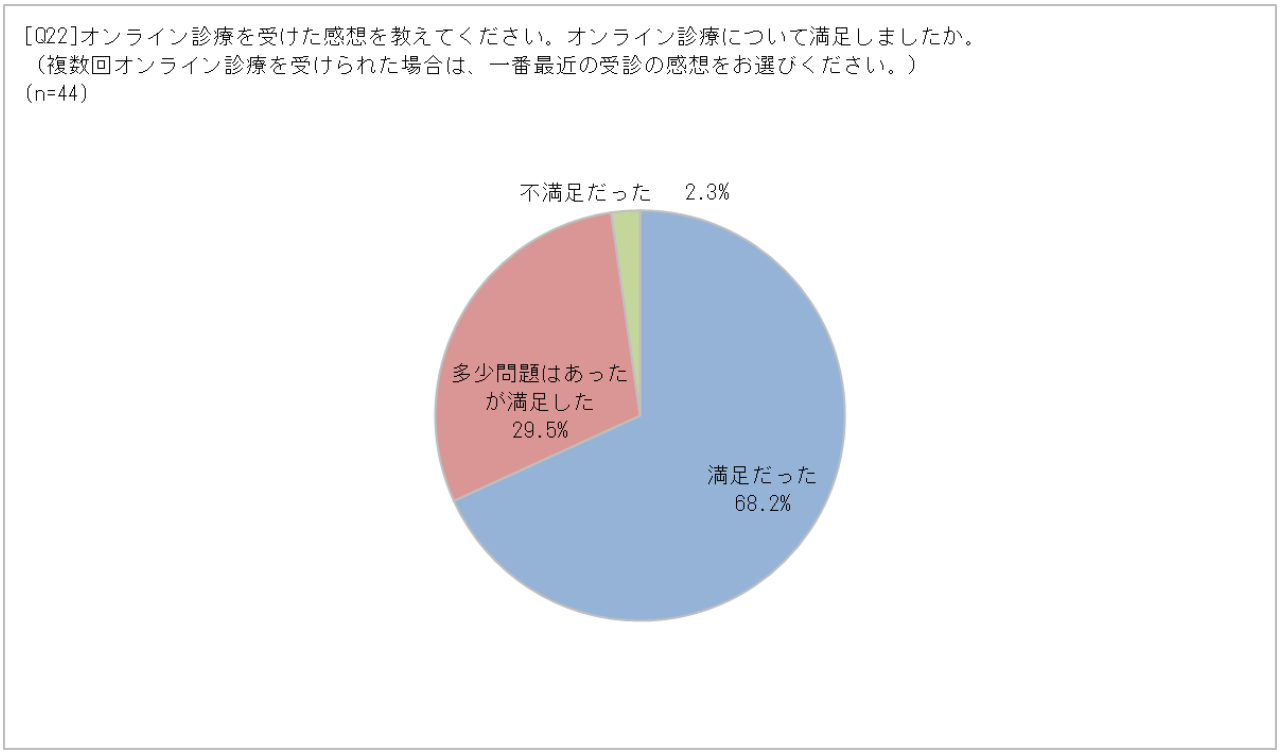


Figure27.（対象：経験者）オンライン診療を受けた感想

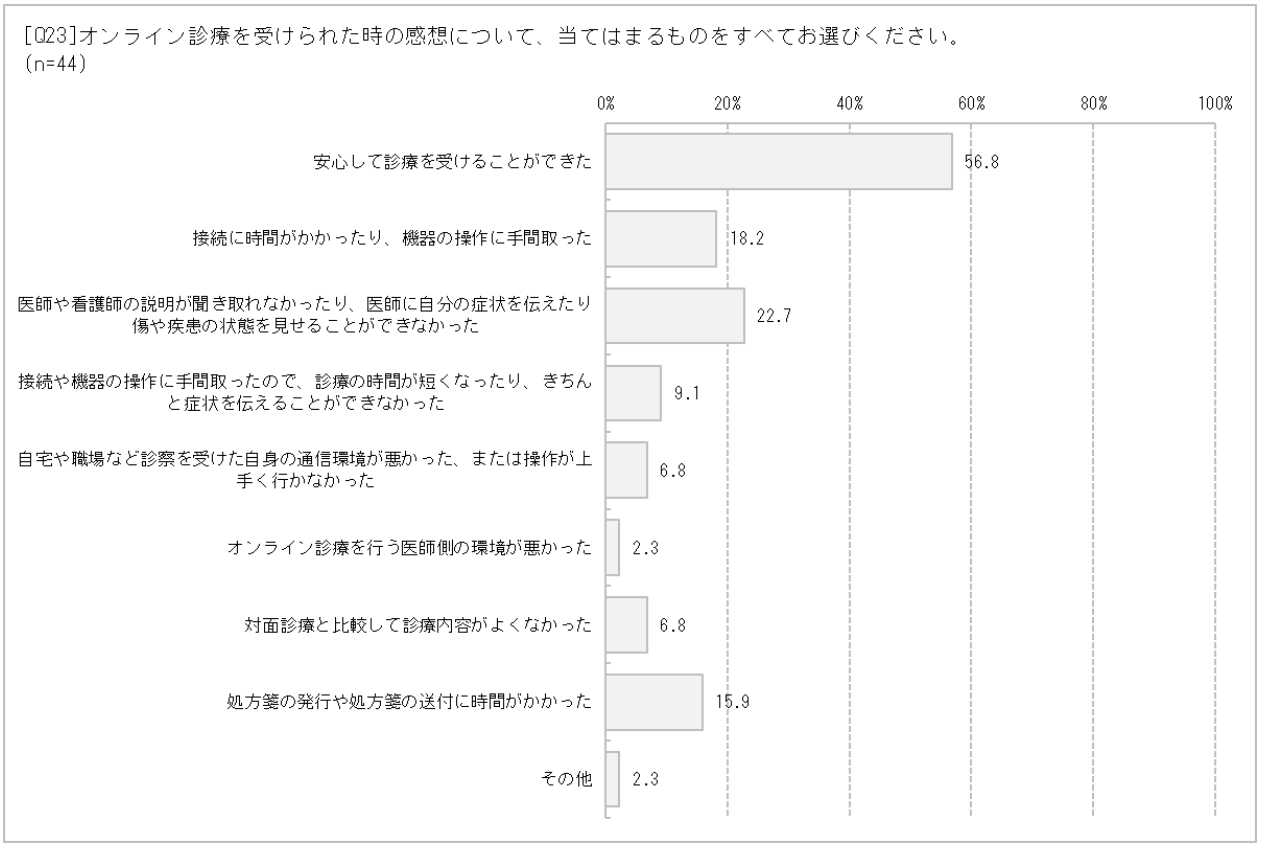


Figure28.（対象：経験者）オンライン診療の受診への感想

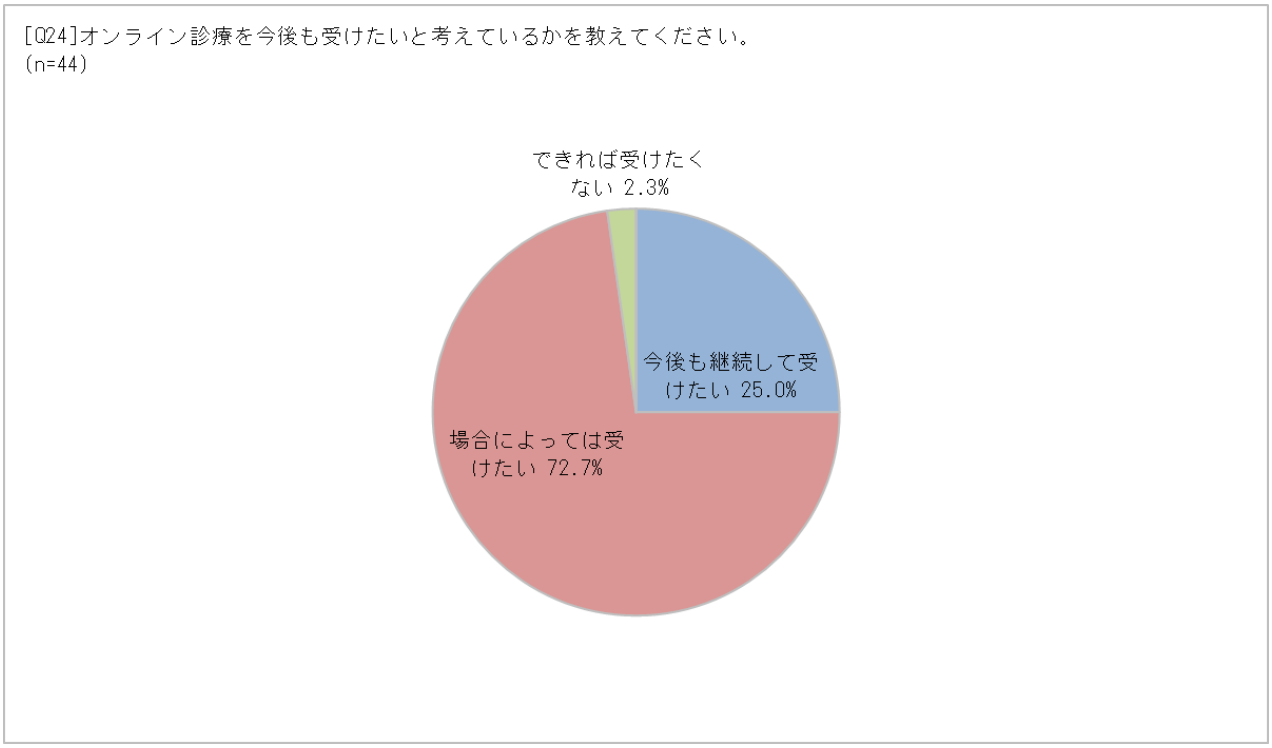


Figure29.（対象：経験者）オンライン診療の受診の希望

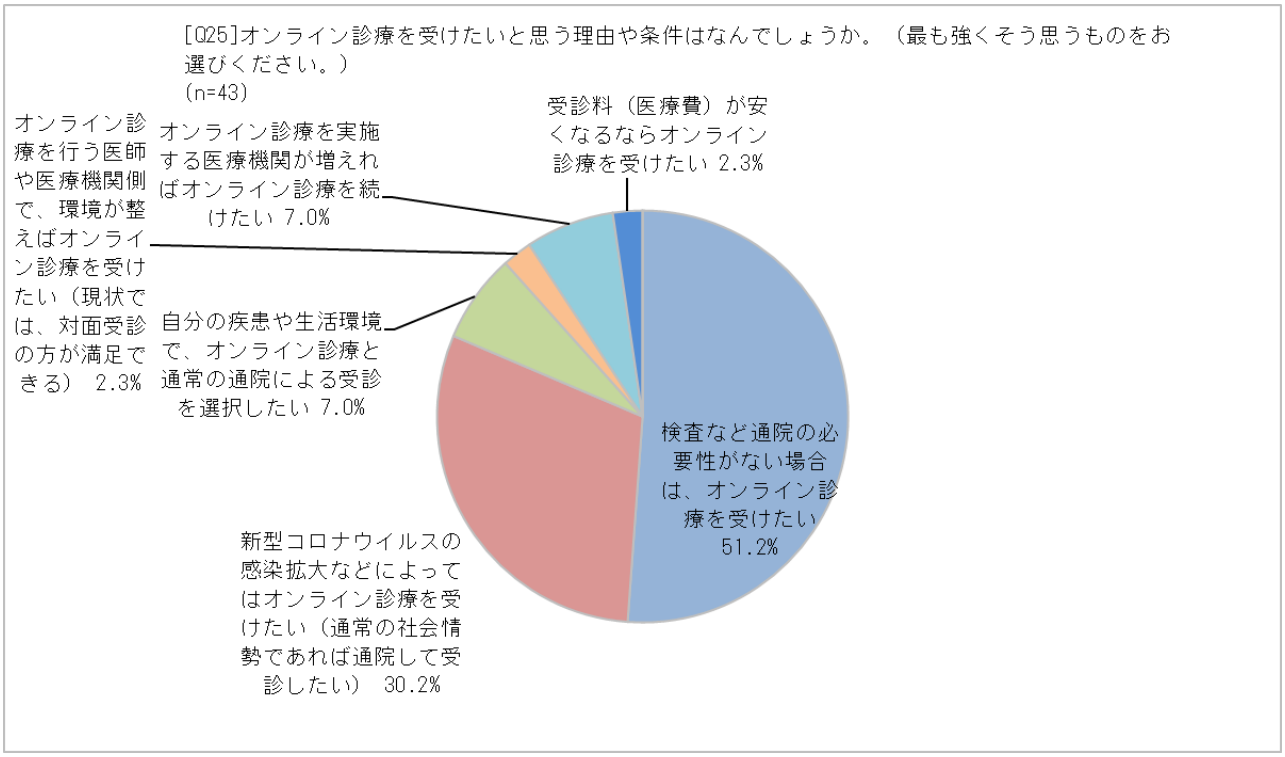


Figure30.（対象：経験者）オンライン診療を受けたいと思う理由

「オンライン診療」とは、患者が医療機関に赴いて医師の診療を受ける代わりに、スマートフォンなどの情報通信機器※を患者と医師が利活用した上で、医師が患者の診察や診断を行い診断結果の説明や処方等の診療行為を行うことです。通常は、医療機関を受診している患者のうち、症状が落ち着いており医師がオンライン診療で問題ないと判断される患者の場合は、その医療機関のオンライン診療を受けることが可能ですが、今般の新型コロナウイルスの感染拡大を受け、問題がないと医師が判断した場合ややむを得ない場合は、診療前相談などを行った上で、初診からでもオンライン診療を受けることができます。(初診からのオンライン診療は、原則として「かかりつけの医師」や健康診断の結果を医師が持っている場合など、限られます。)※情報通信機器・・・テレビ電話、スマートフォン、タブレット、パソコン等で撮影や通話、インターネット・無線 LAN 通信等が可能な機器

上記の「オンライン診療」の説明を読んで、オンライン診療についてお尋ねします。オンライン診療を受けたいと思いますか。(n=652)

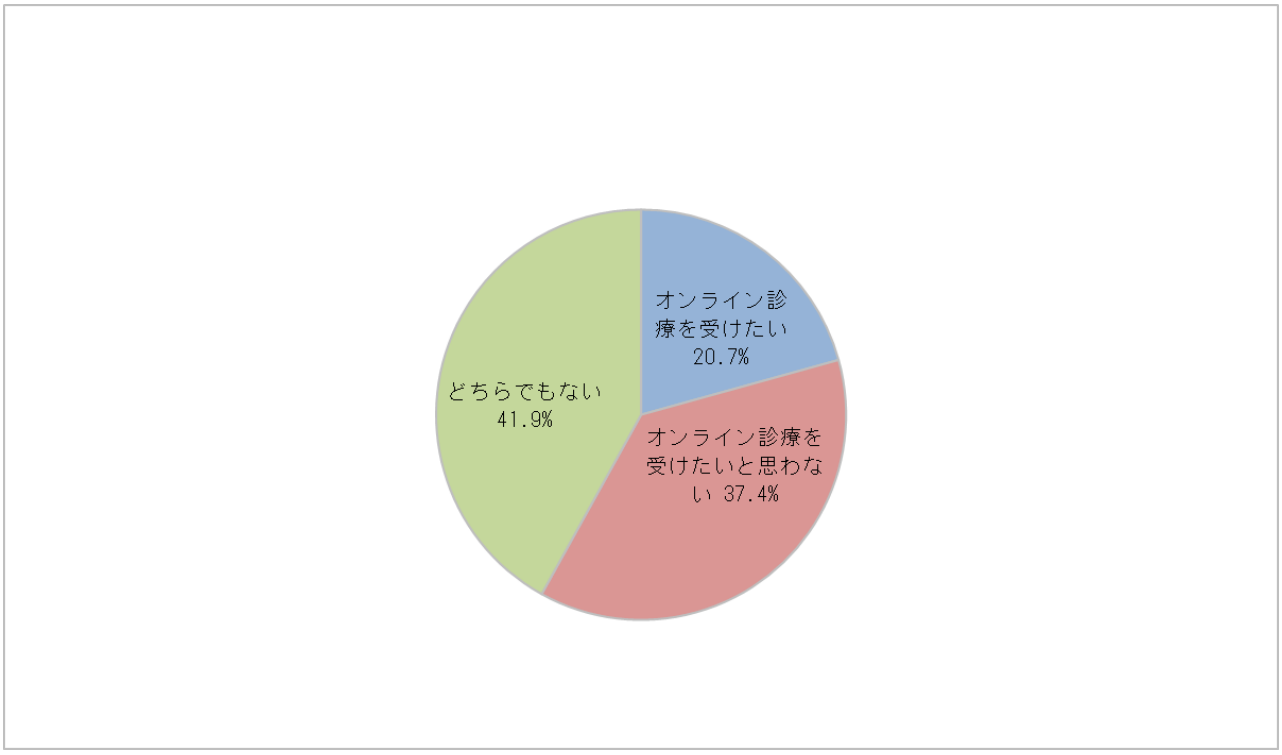


Figure31.オンライン診療での受診の希望

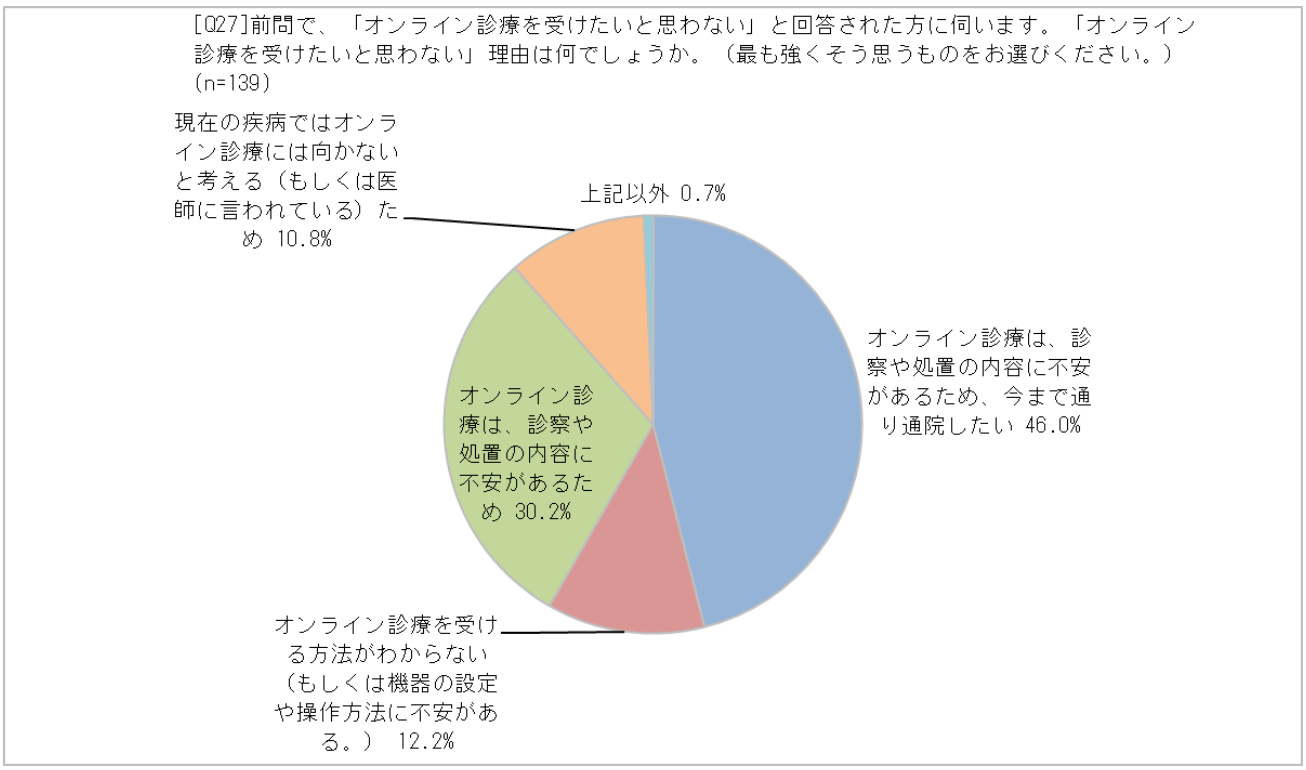


Figure32.オンライン診療を受けたいと思わない理由

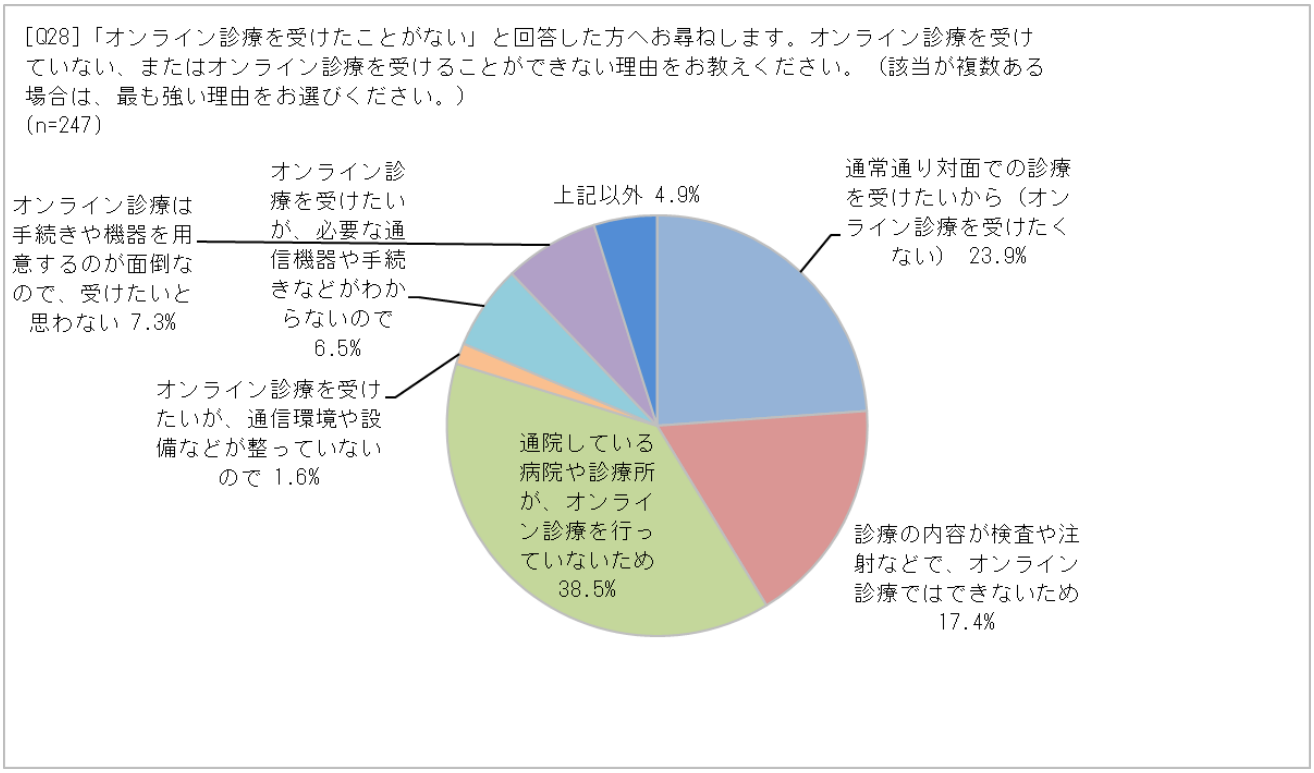


Figure33.オンライン診療を受けた経験がない理由

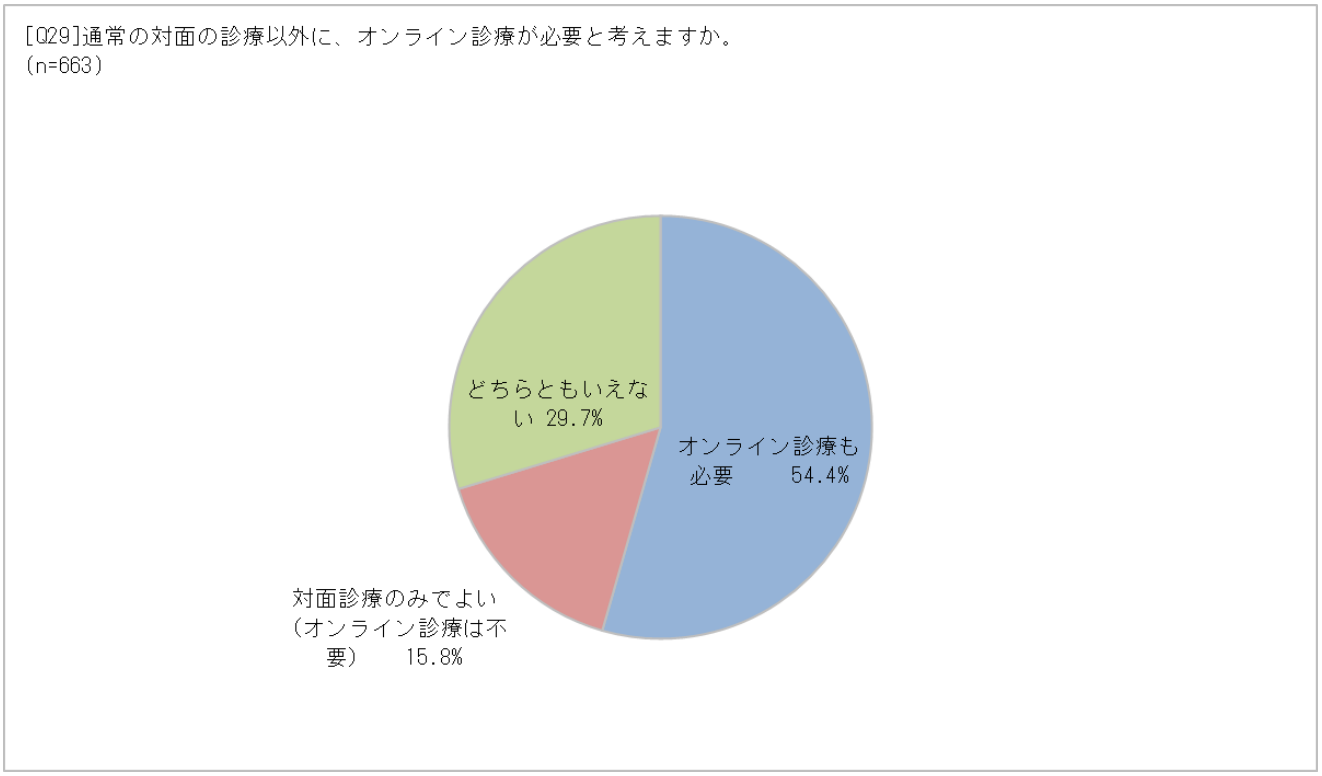


Figure34.オンライン診療の必要性(全回答者)

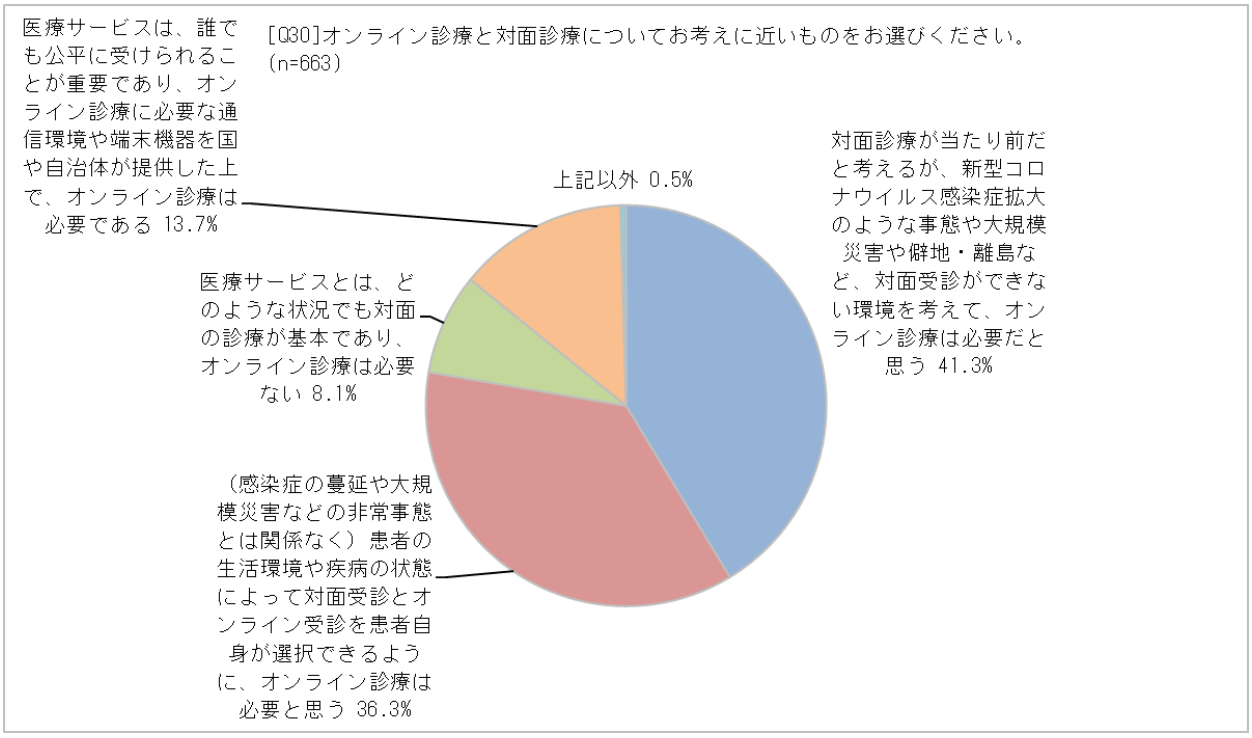


Figure35.オンライン診療と対面診療に対する考え(全回答者)

＜参考1＞前回調査結果（2022 年 3 月実施分）

前回の調査は 2022 年 3 月 28 日～29 日、対象者：患者 1111 名。対象者の選定方法、調査票はほぼ同じものとなる。前回の調査結果を下に記す。

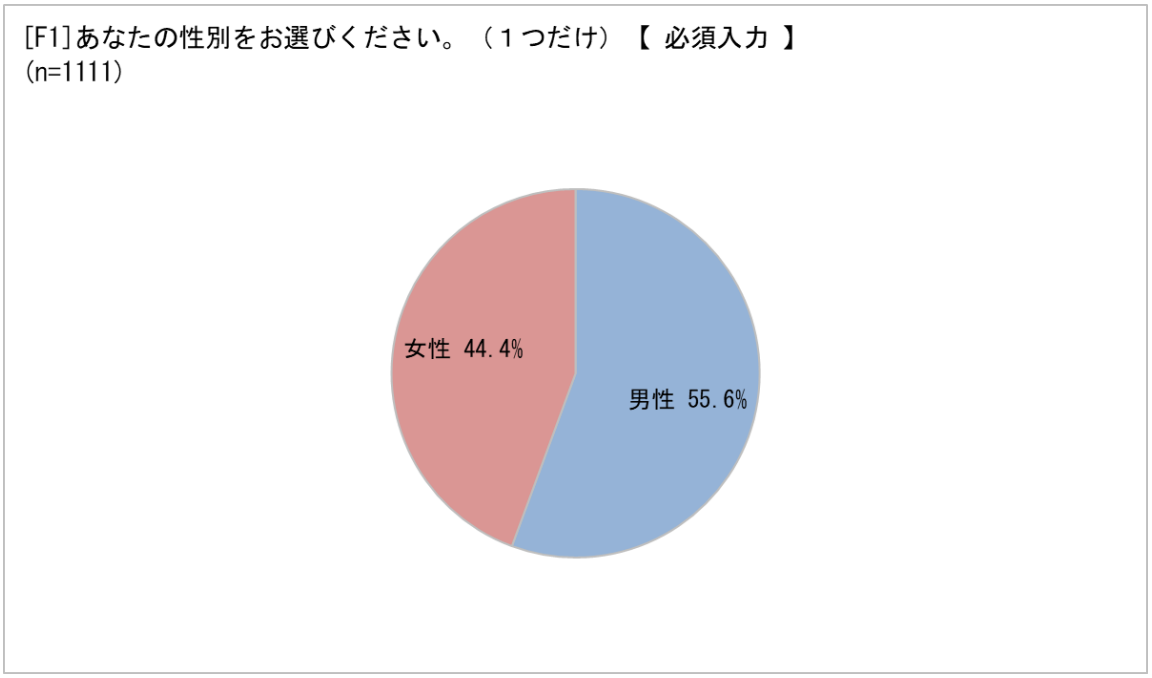


Figure1.性別

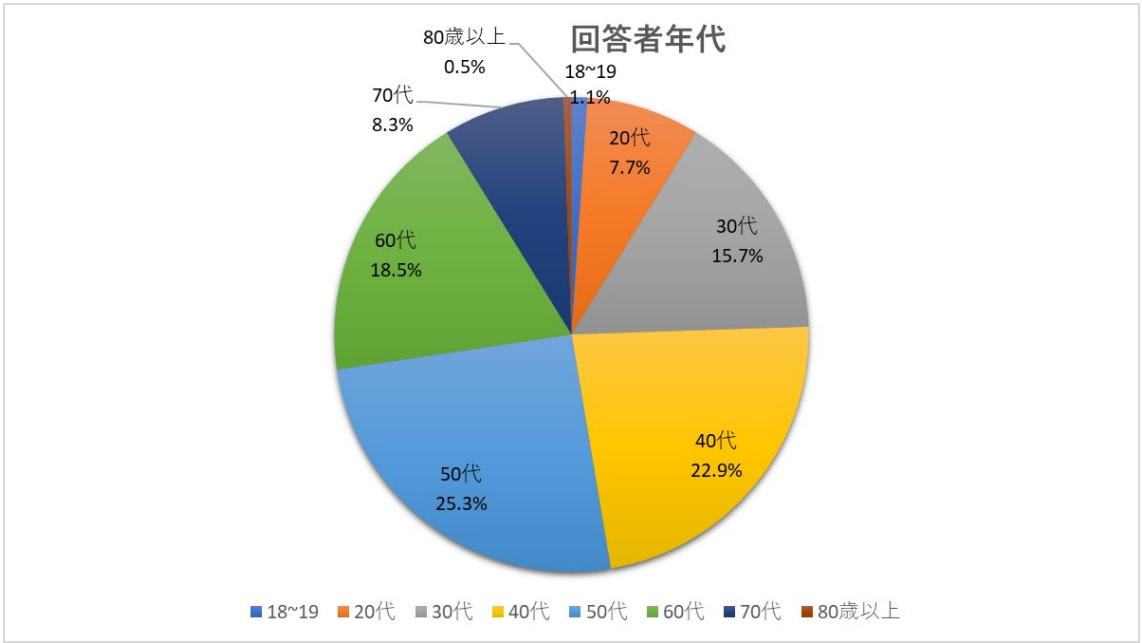


Figure2. 回答者年代別

	単一回答	%
	全体	(1111)
1	北海道	4.2
2	青森県	0.6
3	岩手県	1.0
4	宮城県	1.4
5	秋田県	0.9
6	山形県	0.9
7	福島県	0.5
8	茨城県	1.6
9	栃木県	1.4
10	群馬県	1.8
11	埼玉県	5.4
12	千葉県	6.9
13	東京都	14.3
14	神奈川県	9.3
15	新潟県	2.0
16	富山県	0.9
17	石川県	0.5
18	福井県	0.4
19	山梨県	0.4
20	長野県	1.0
21	岐阜県	1.8
22	静岡県	2.3
23	愛知県	6.3
24	三重県	1.3
25	滋賀県	0.8
26	京都府	2.1
27	大阪府	9.7
28	兵庫県	5.1
29	奈良県	1.0
30	和歌山県	0.8
31	鳥取県	0.0
32	島根県	0.4
33	岡山県	2.0

34	広島県	1.4
35	山口県	1.1
36	徳島県	0.3
37	香川県	0.5
38	愛媛県	1.4
39	高知県	0.0
40	福岡県	2.8
41	佐賀県	0.3
42	長崎県	0.8
43	熊本県	0.6
44	大分県	0.4
45	宮崎県	0.3
46	鹿児島県	0.6
47	沖縄県	0.7

Table1. 回答者居住地

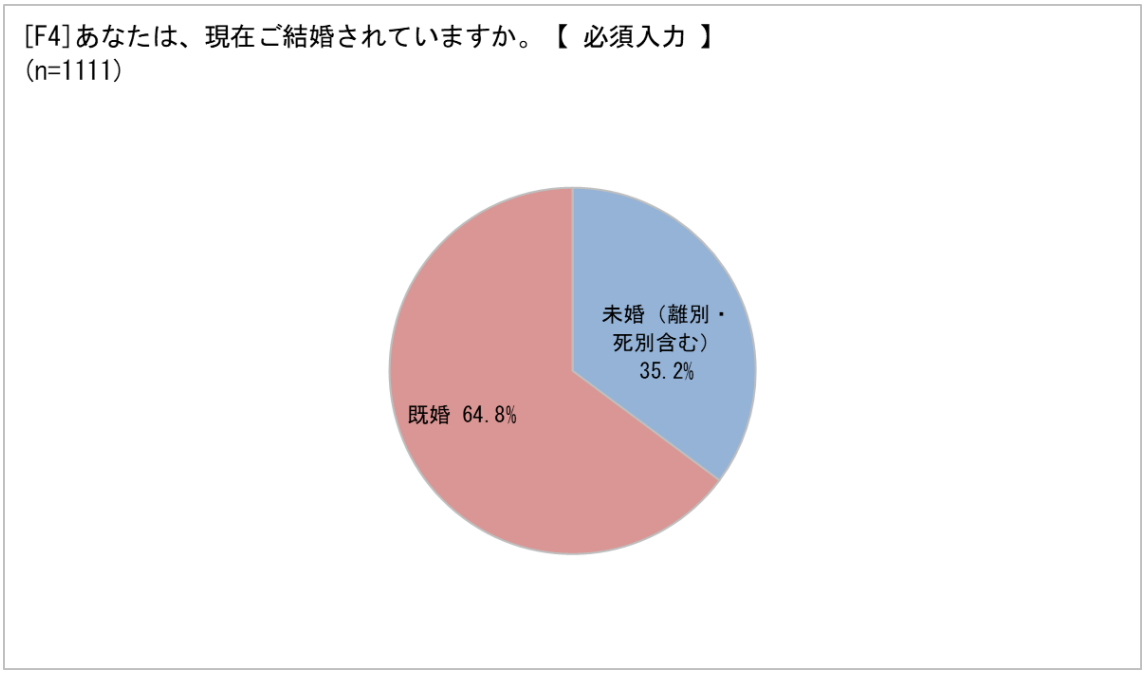


Figure3. 婚姻状況

[F5]あなたには、現在お子様がいらっしゃいますか。【 必須入力 】
(n=1111)

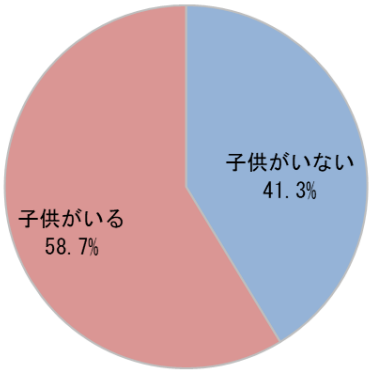


Figure4. 子供の有無

[F8]あなたの現在のご職業をお答えください。【 必須入力 】
(n=1111)

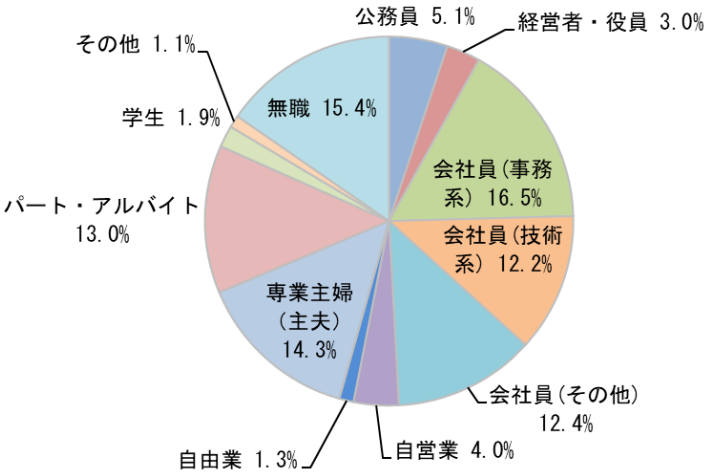


Figure5. 職業

[Q1]現在の生活状況をお答えください。（同居の対象は人間で、ペットは含みません。）
(n=1111)

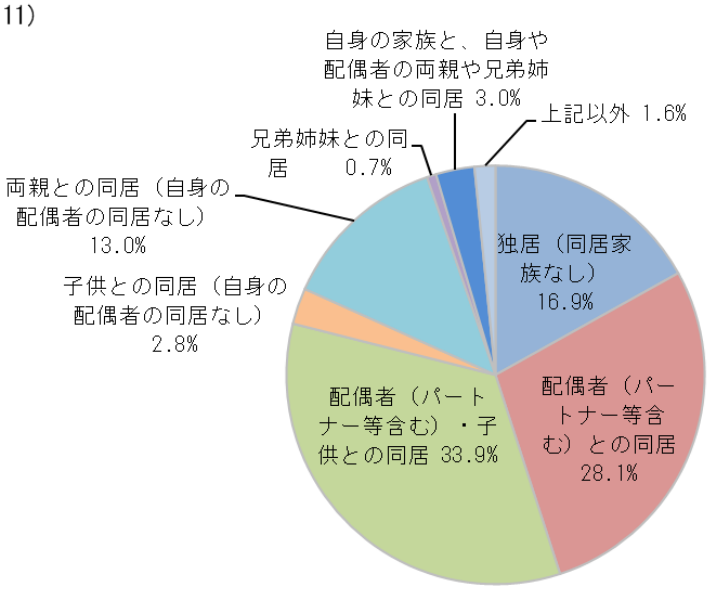


Figure6.生活状況

[Q2]医療機関への受診頻度をお答えください。（職場や自治体の定期健康診断以外）もし、複数の疾患で受診されている場合は、受診回数が多い方でお答えください。医科、歯科など診療科や、通院・オンライン診療などは問いません。
(n=1111)

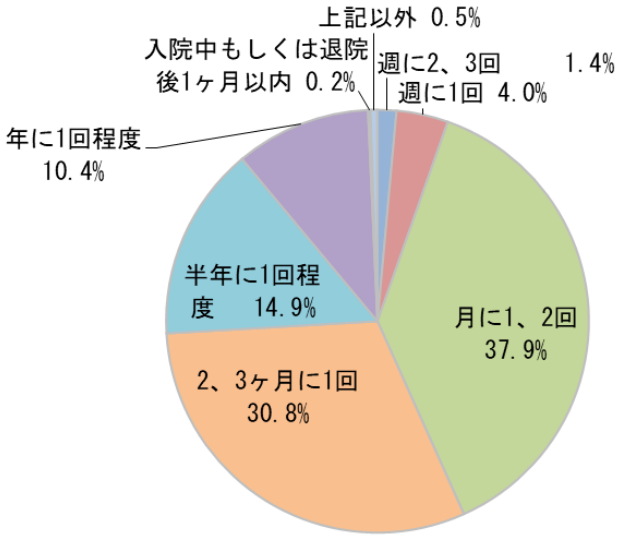


Figure7. 受診の頻度

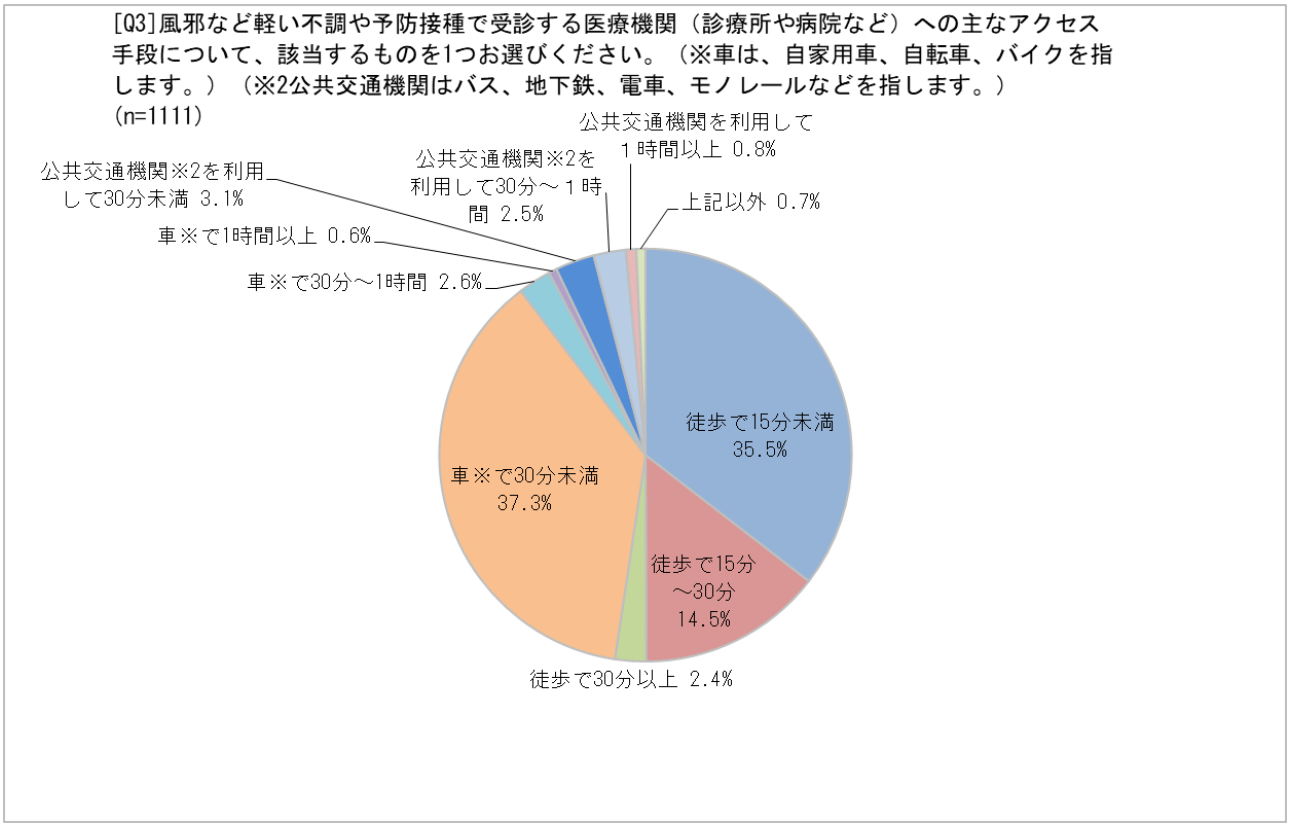


Figure8.受診する医療機関へのアクセス状況

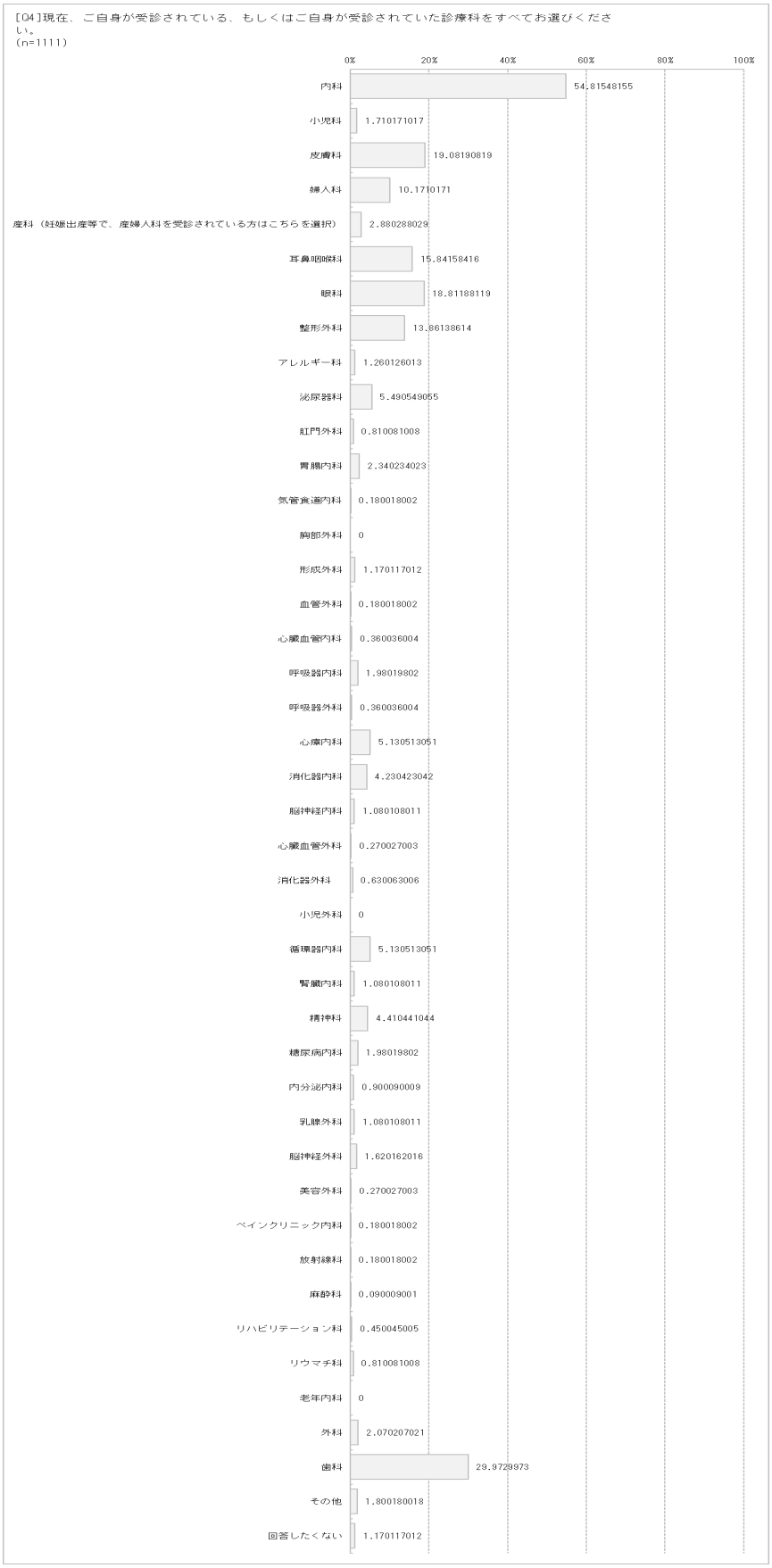


Figure9. 受診する(した)診療科（複数回答）

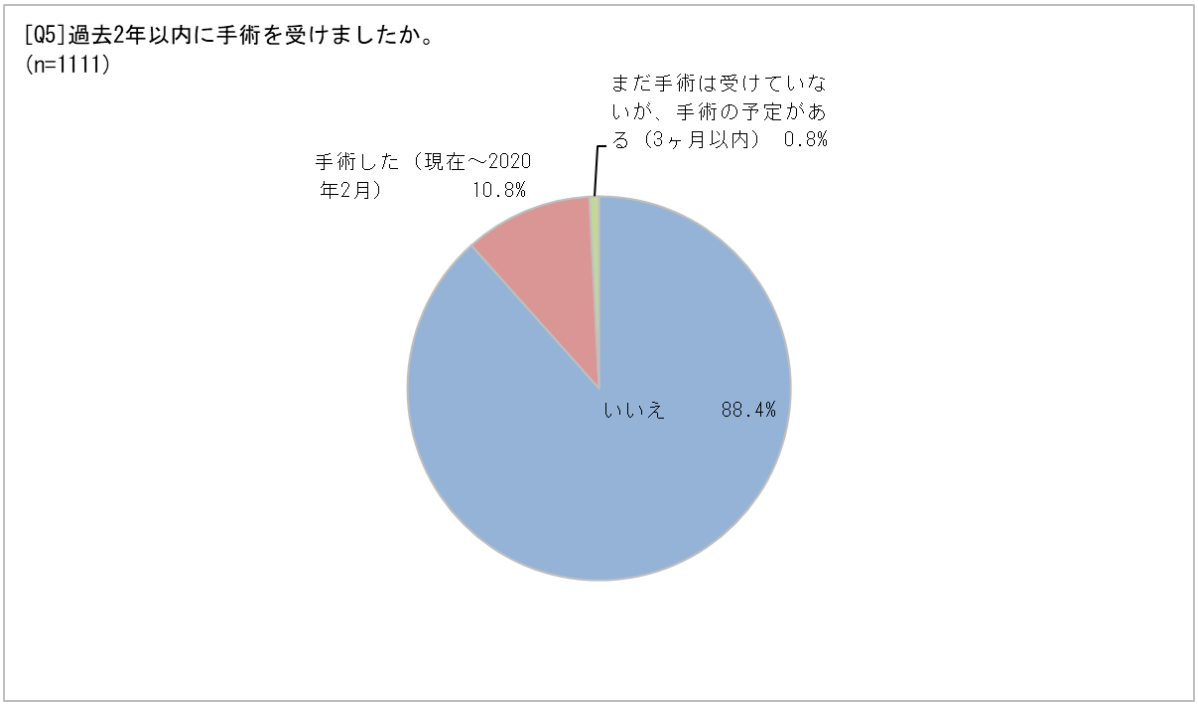


Figure10.過去2年間の手術歴

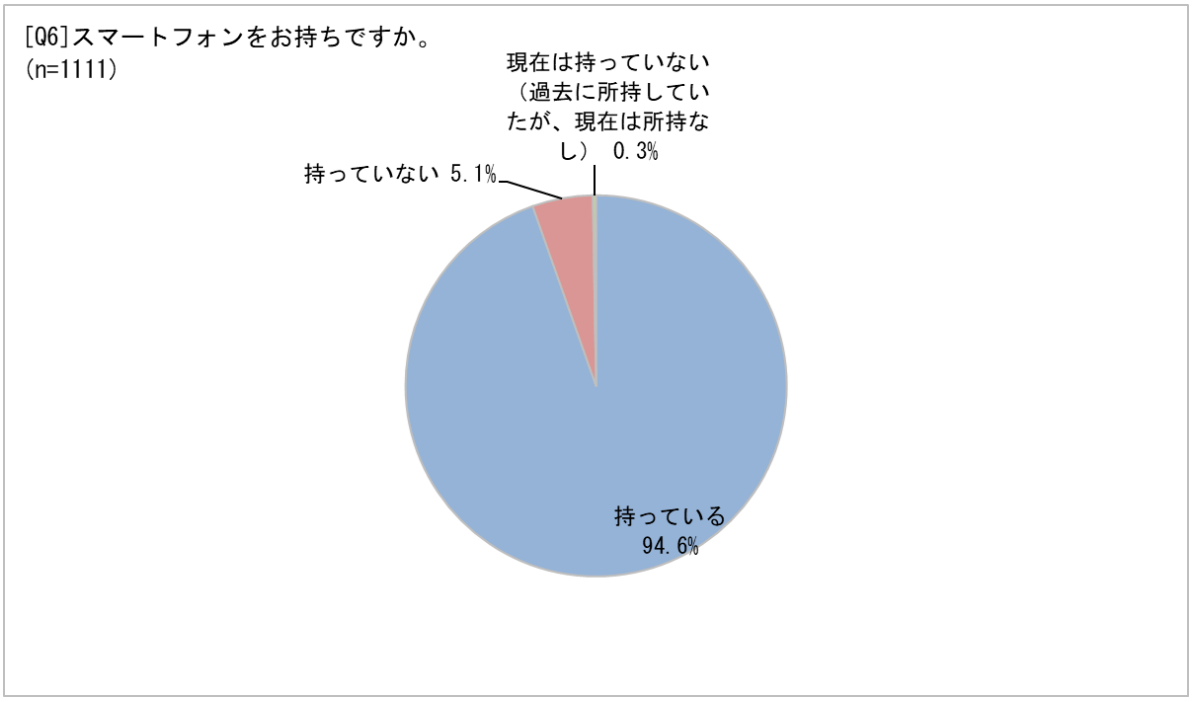


Figure11.スマートフォンの所持

[Q7]ご自身のマイナンバーカードを持っているか教えてください。（お住まいの自治体にてマイナンバーカードの交付申請手続き中、もしくはカードの受取り予定の方も含みます。）
(n=1111)

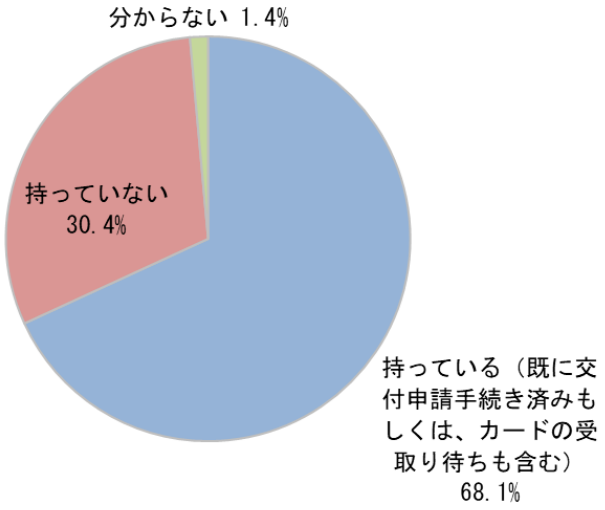


Figure12.マイナンバーカードの所有

[Q8]マイナンバーカードを持っていないと回答された方にお尋ねします。マイナンバーカードを持っていない理由を教えてください。当てはまるものが複数ある場合は、最も強い理由をお選びください。
(n=338)

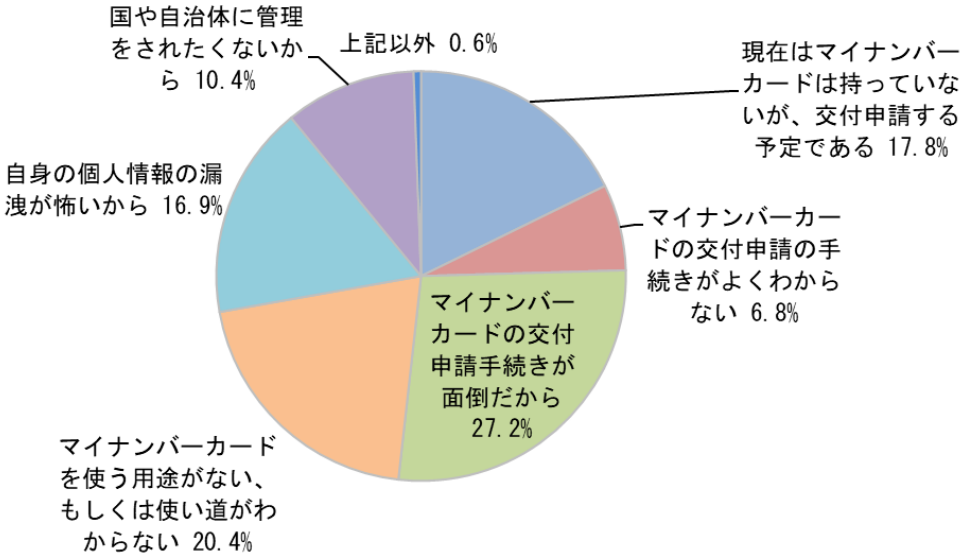


Figure13.マイナンバーカードを所有していない理由

[Q9]最近、医療機関(病院や診療所)では電子カルテやオンライン診療を導入するなど、電子化が進められています。また、日本政府によりマイナンバーカードの利用促進が行われており、マイナンバーカードが健康保険証として利用できるようになり、マイナンバーカードとマイナポータルを使えば、自分のスマートフォンで健診結果や薬剤情報が確認できたり、医療費控除も便利に行えるようになりました。将来的には PHR(Personal Health Records)という、健康医療データの個人口座の中に、乳幼児期の予防接種情報や医療機関での検査結果、健診の結果、お薬手帳の情報などが保管されることになります。PHR は、自分がケガや病気で受診した時に医師や看護師への説明に使ったり、自分の健康維持にも使えます。あなたのもしもの時、例えば意識不明で救急搬送されたり大規模災害の時でも、あなたの記憶やカルテの代わりに使えます。このように医療制度や生活環境が電子化の推進で便利になる一方、コンピュータウイルスの蔓延やハッカーによる侵入などの危険性について、セキュリティの専門家などから指摘されています。以下のそれぞれの項目について、ご自身の感覚にもっとも近いものを 1 つ選んでください。

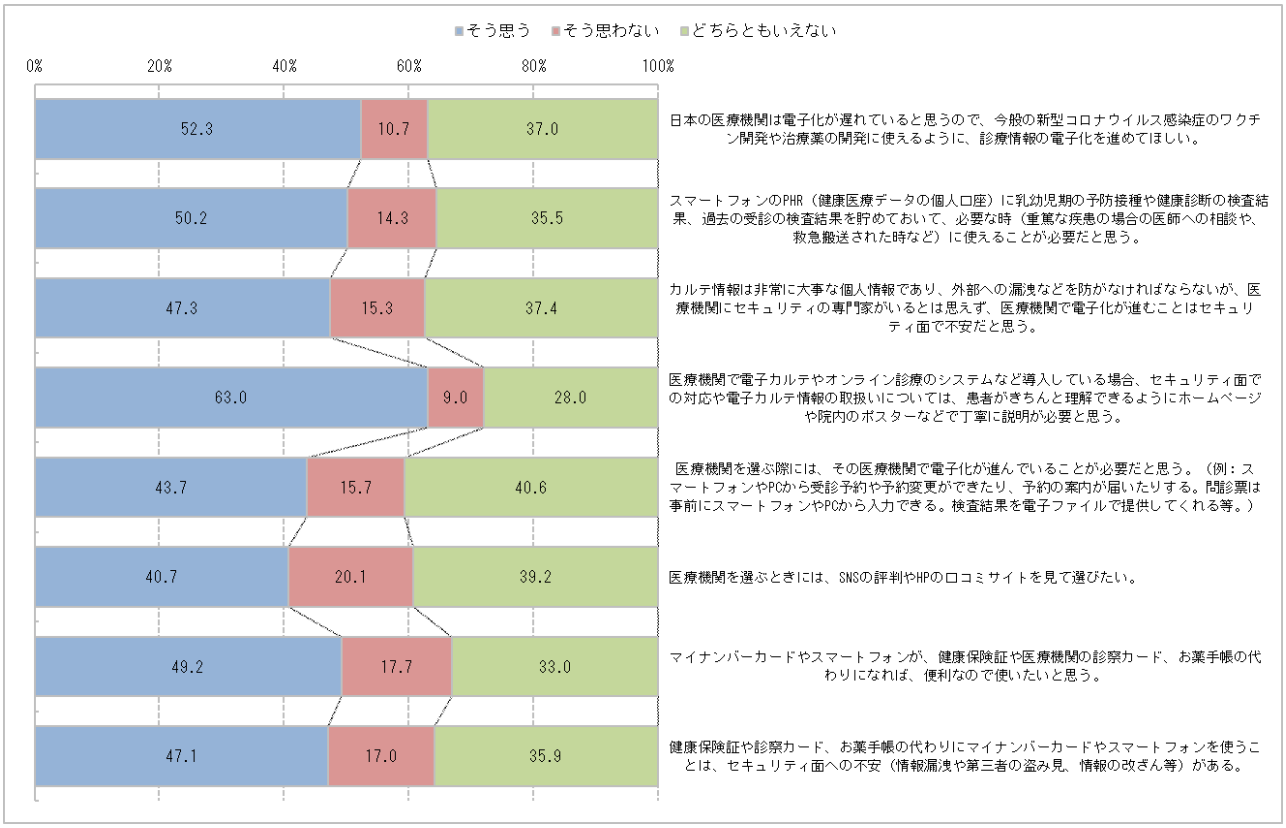


Figure14.医療機関の電子化への感想

[Q10]「オンライン診療」を知っているか教えてください。
(n=1111)

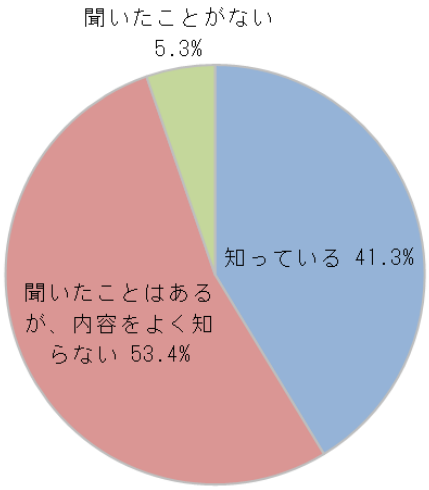


Figure15.オンライン診療の認知

[Q11]「オンライン診療を知っている」と回答された方にお尋ねします。ご自身がオンライン診療を受けたことがあるかを教えてください。
(n=459)

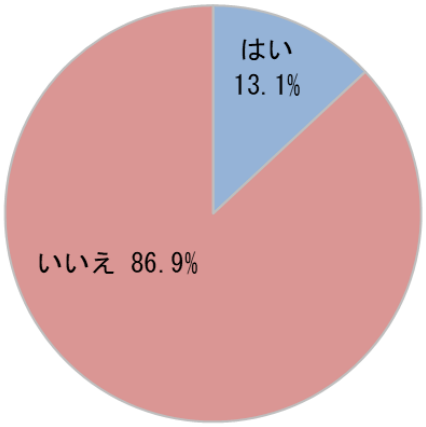


Figure16.オンライン診療の受診経験（対象:「オンライン診療」既知の回答者）

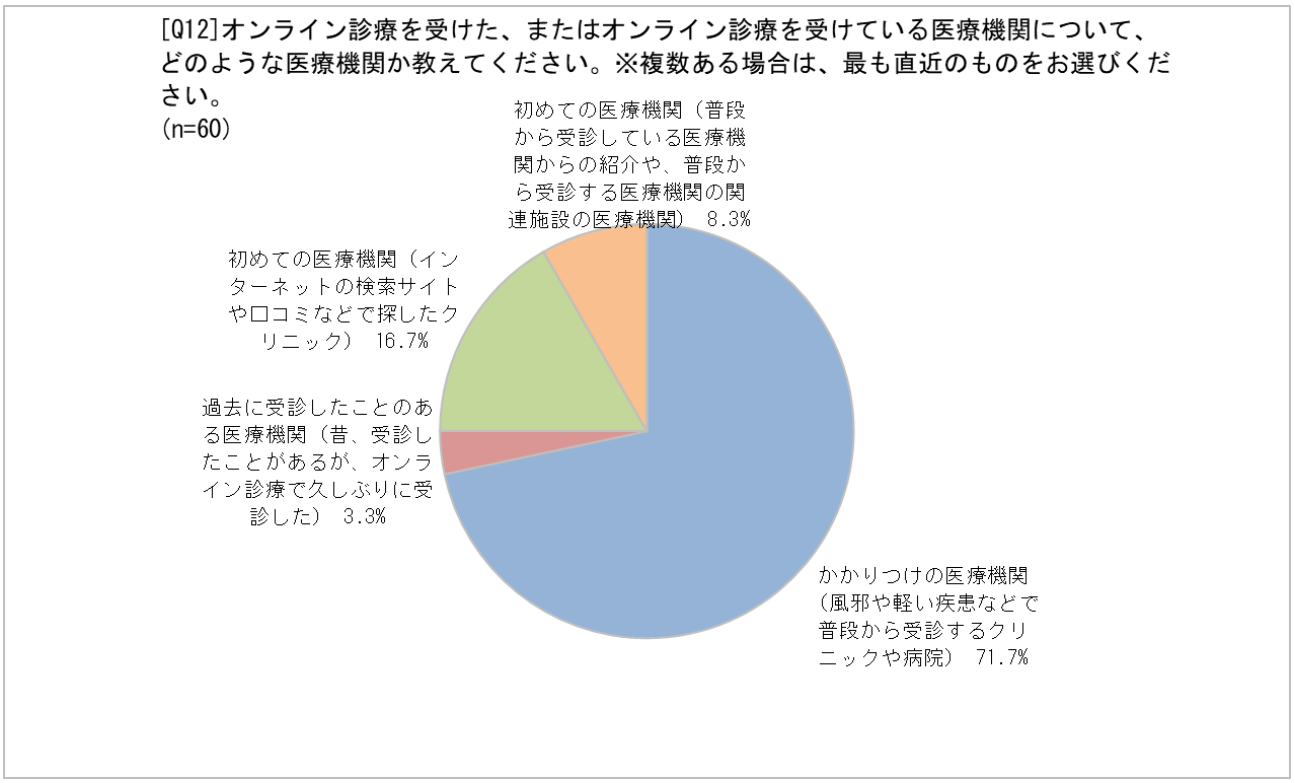


Figure17.（対象：経験者）オンライン診療を受けた医療機関について

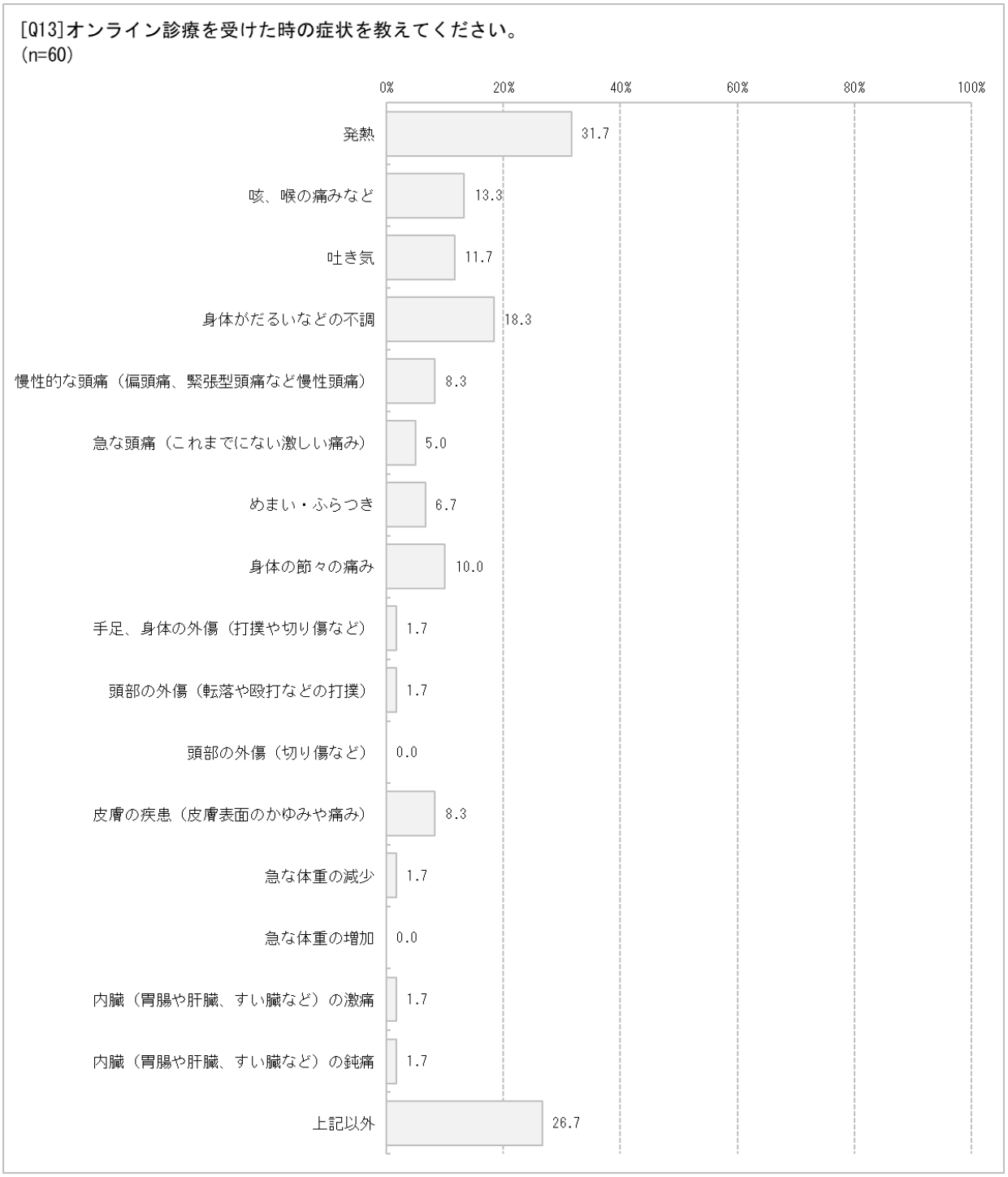


Figure18.（対象:経験者)オンライン診療を受けた際の症状＜疾患傷病等＞（複数回答）

[Q14]オンライン診療を受けた時の状況を教えてください。その受診は急な症状でしたか、慢性的な疾患（例えば糖尿病の治療や皮膚疾患）で定期的な受診でしょうか。（これまでに複数回オンライン診療を受けた場合は、一番最近の受診状況をもとにお答えください。）
(n=60)

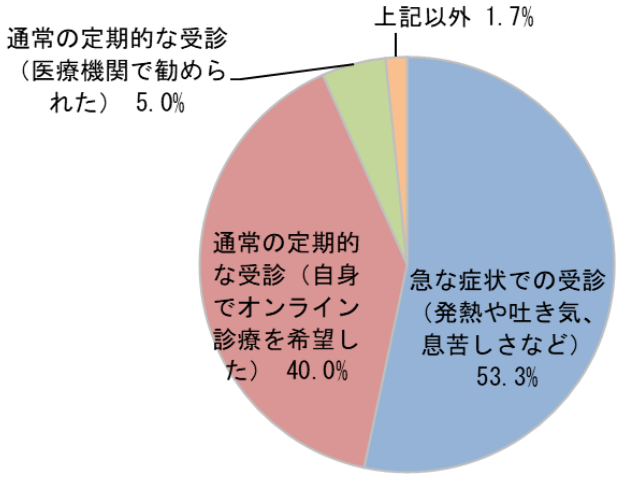


Figure19.（対象:経験者）オンライン診療を受けた際の状況＜発症＞

[Q15]オンライン診療を受けた際の状況をお教えください。（これまでに複数回オンライン診療を受けた場合は、一番最近の受診状況をもとにお答えください。）オンライン診療を受けた際の場所（あなたが居た場所）をお答えください。
(n=60)

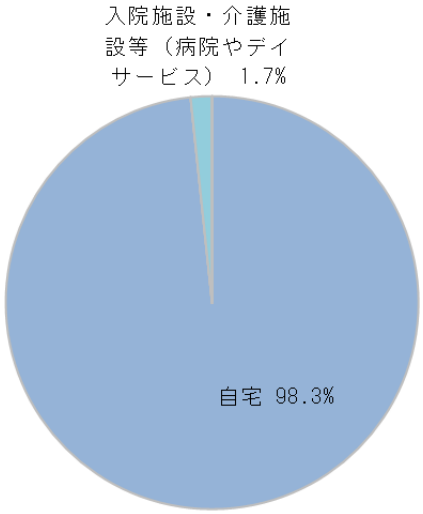


Figure20.（対象:経験者）オンライン診療を受けた際の状況＜場所＞

[Q16]オンライン診療を受けた際の状況（ご本人以外に誰がその場所にいたか）を教えてください。（これまでに複数回オンライン診療を受けた場合は、一番最近の受診状況をもとにお答えください。）
(n=60)

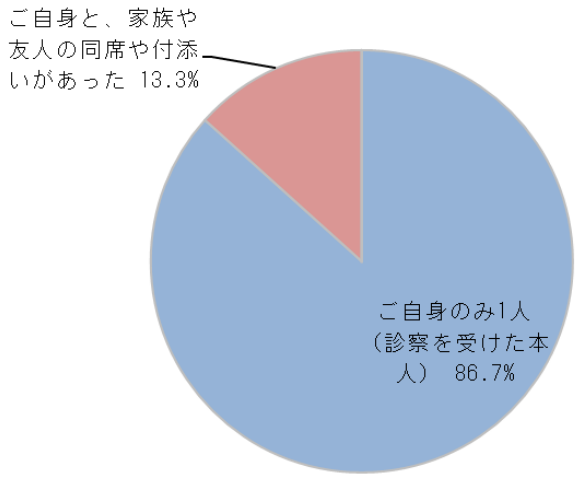


Figure21.（対象：経験者）オンライン診療の状況＜立会者等の有無＞

[Q17]オンライン診療での本人確認についてお尋ねします。医師はどのようにあなたの本人確認を行ったかを教えてください。（これまでに複数回オンライン診療を受けた場合は、一番最近の受診状況をもとにお答えください。）(n=60)

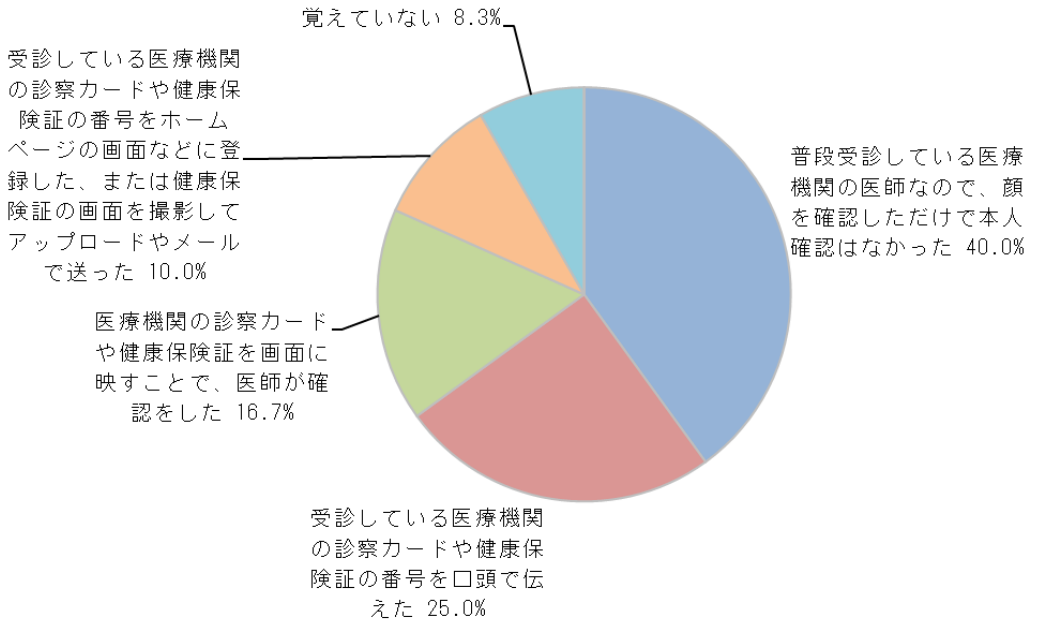


Figure22.（対象：経験者）オンライン診療での本人確認の方法

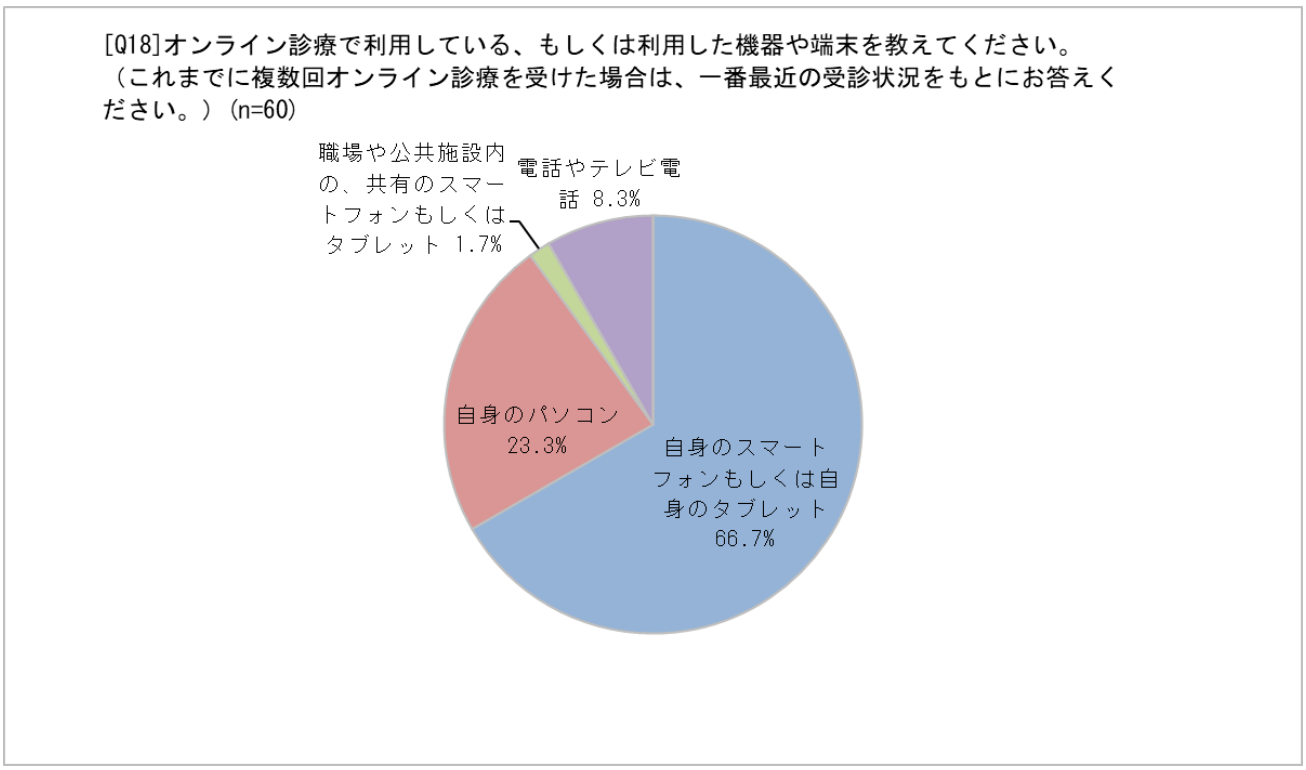


Figure23.（対象：経験者）オンライン診療で利用している機器・端末の種類

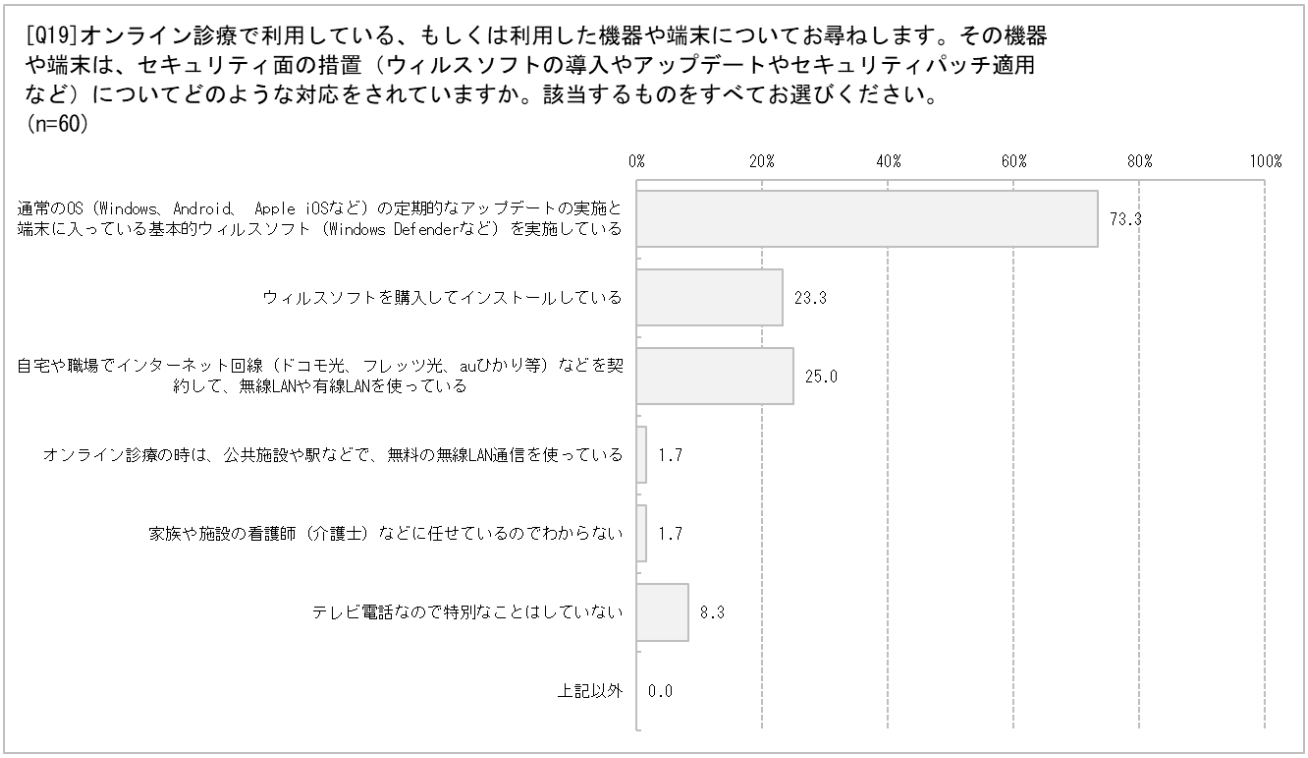


Figure24.（対象：経験者）オンライン診療で利用する端末のセキュリティ措置

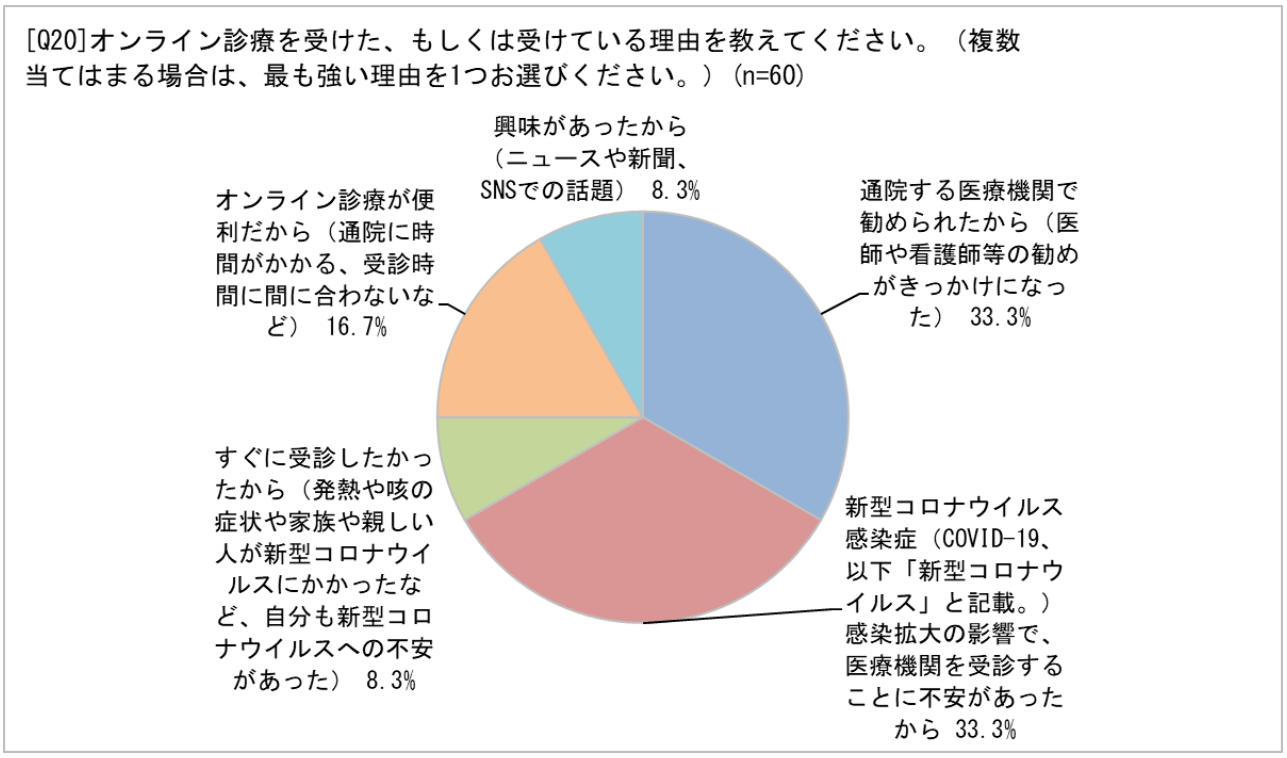


Figure25.（対象:経験者)オンライン診療を受けた理由

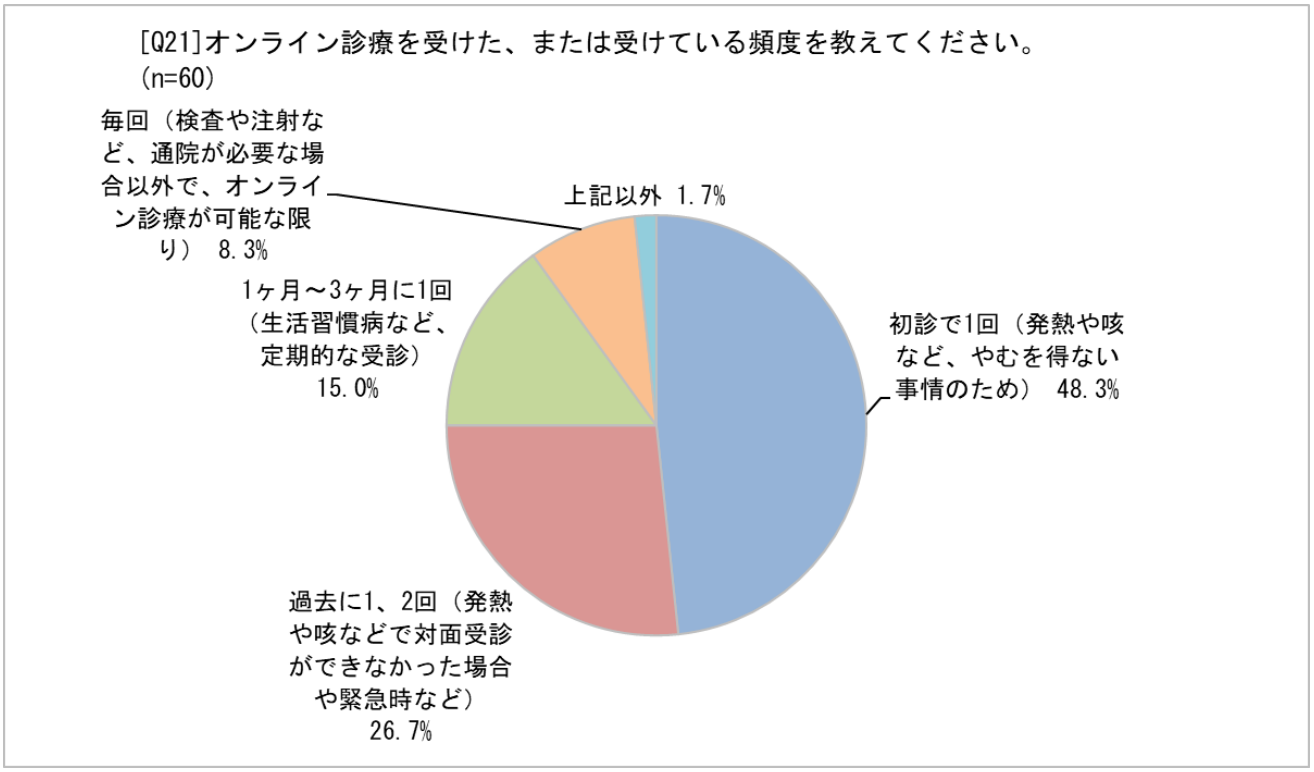


Figure26.（対象:経験者)オンライン診療の受診の頻度

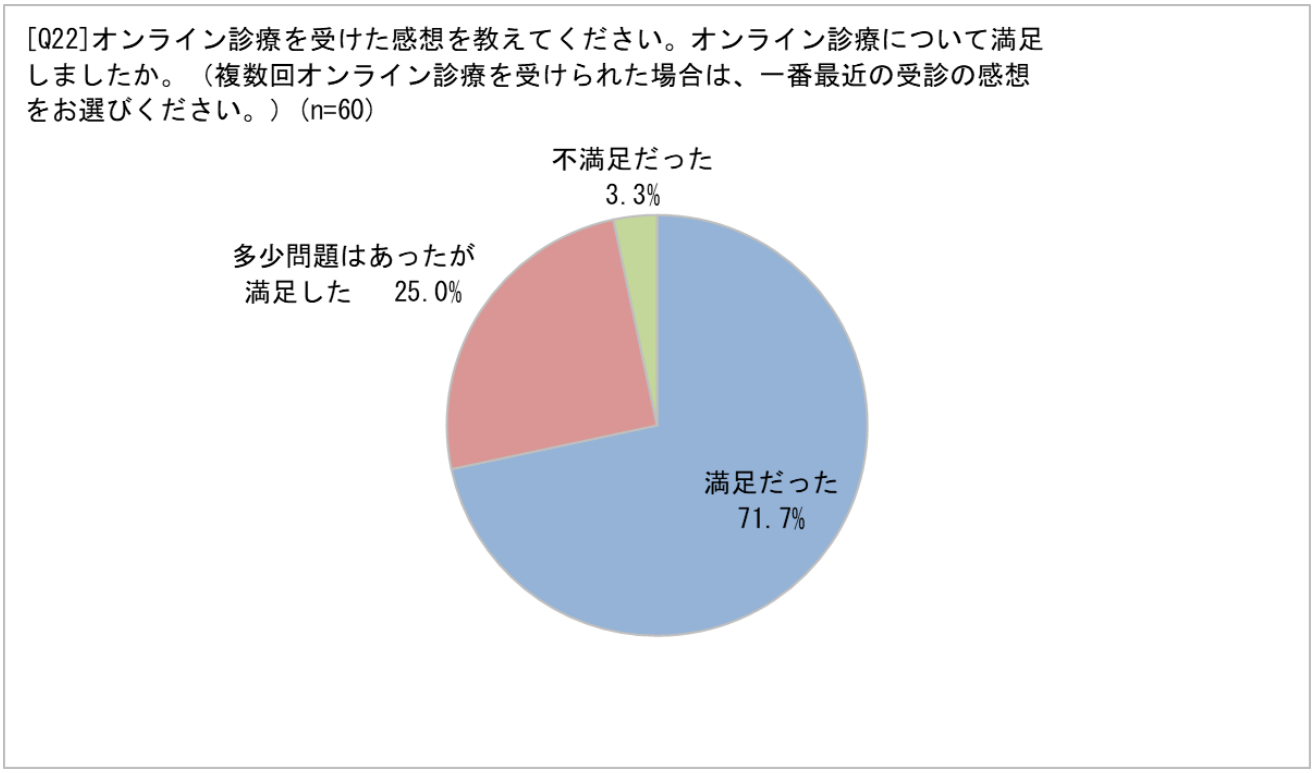


Figure27.（対象:経験者)オンライン診療を受けた感想

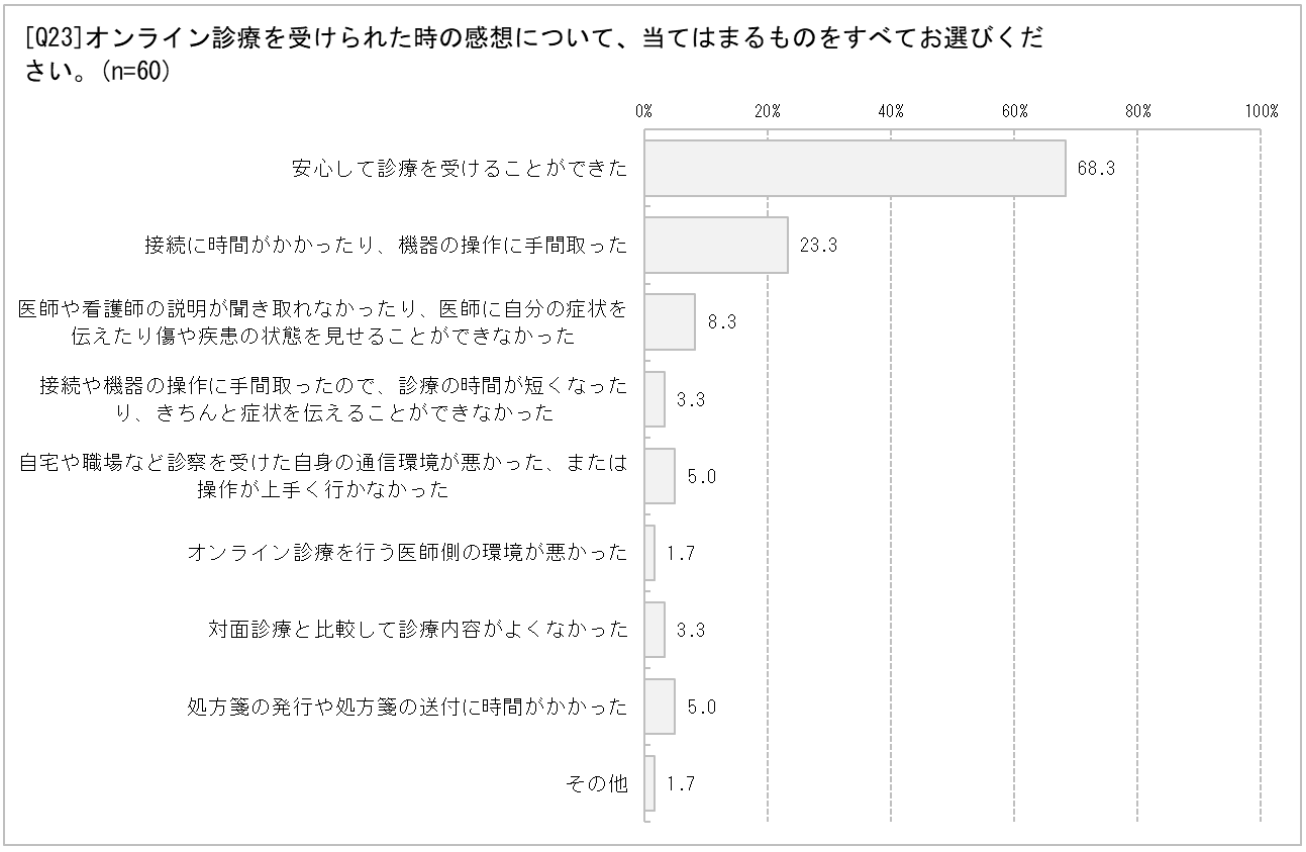


Figure28.（対象:経験者)オンライン診療の受診への感想

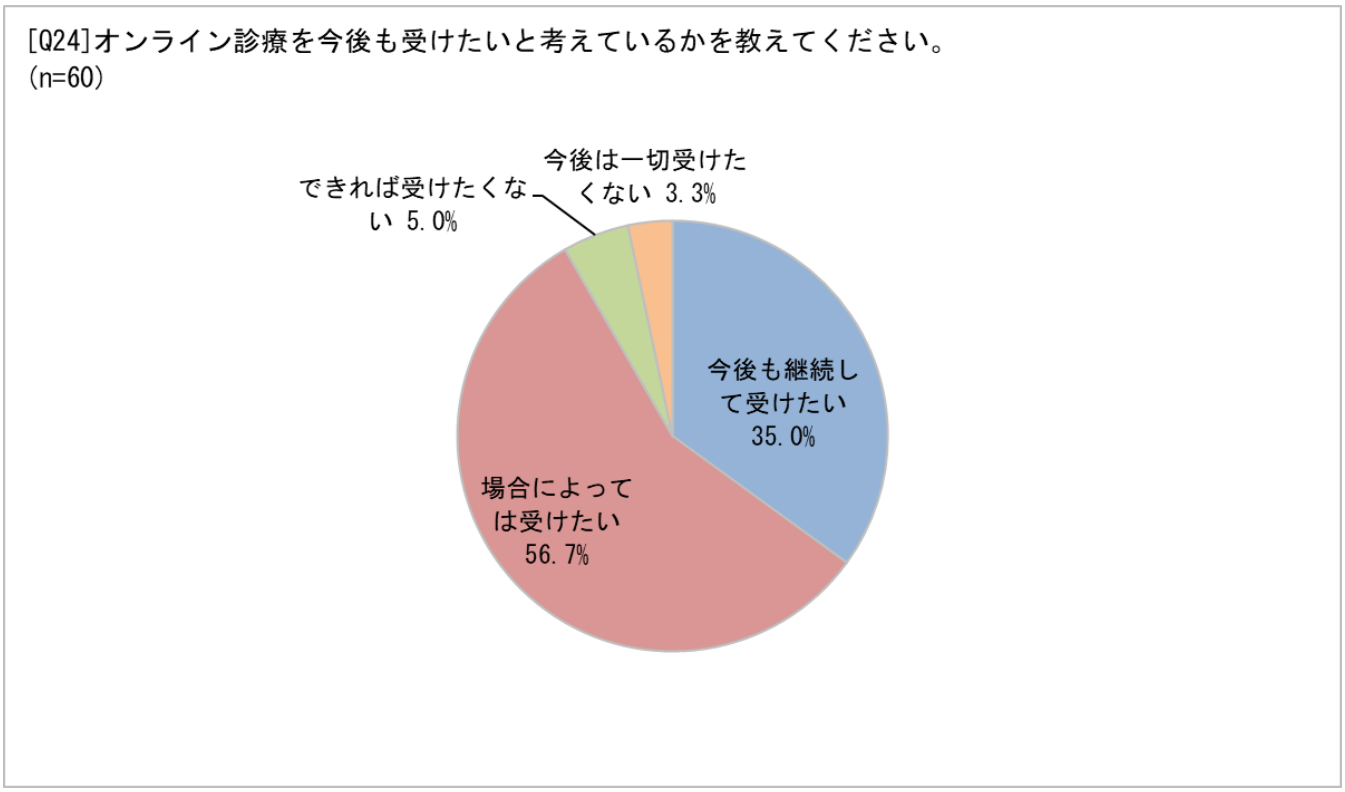


Figure29.（対象:経験者)オンライン診療の受診の希望

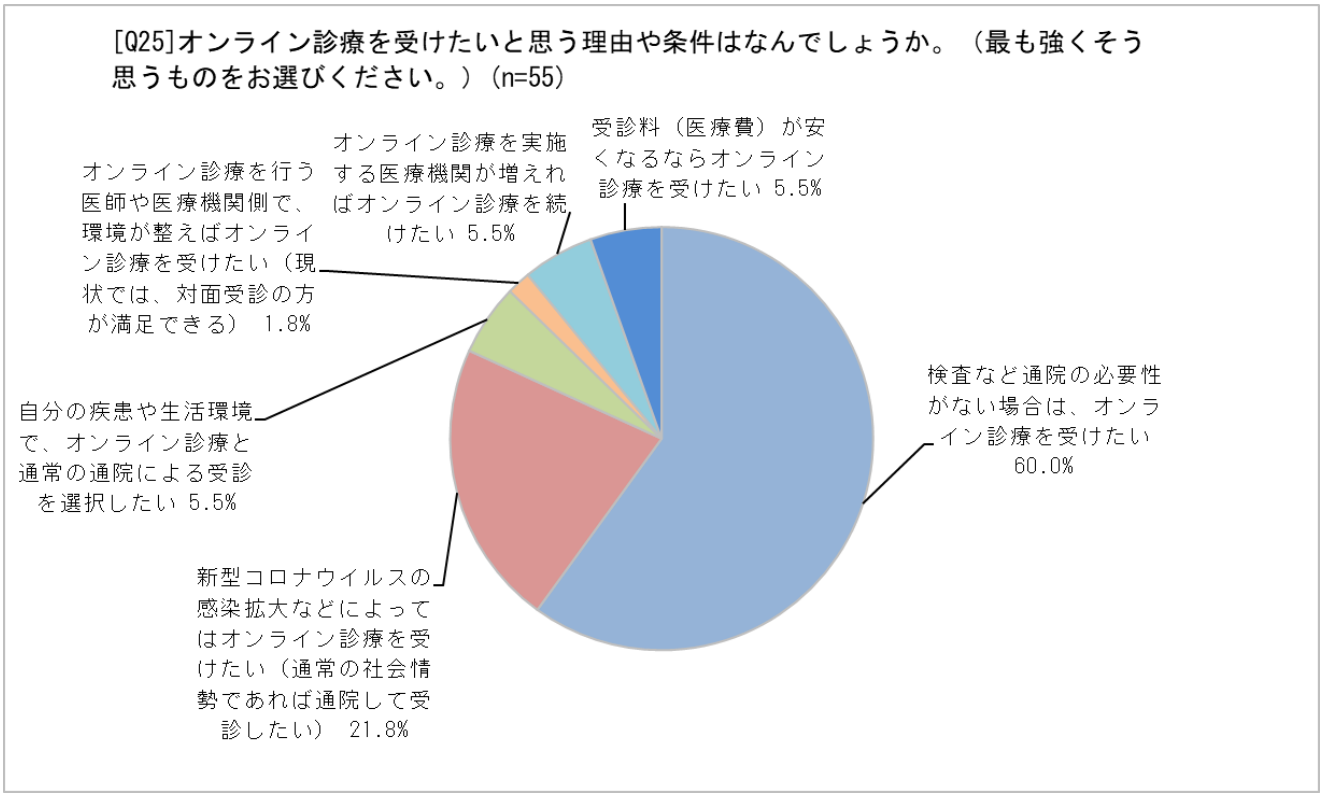


Figure30.（対象:経験者)オンライン診療を受けたいと思う理由

「オンライン診療」とは、患者が医療機関に赴いて医師の診療を受ける代わりに、スマートフォンなどの情報通信機器※を患者と医師が利活用した上で、医師が患者の診察や診断を行い診断結果の説明や処方等の診療行為を行うことです。通常は、医療機関を受診している患者のうち、症状が落ち着いており医師がオンライン診療で問題ないと判断される患者の場合は、その医療機関のオンライン診療を受けることが可能ですが、今般の新型コロナウイルスの感染拡大を受け、問題がないと医師が判断した場合ややむを得ない場合は、診療前相談などを行った上で、初診からでもオンライン診療を受けることができます。(初診からのオンライン診療は、原則として「かかりつけの医師」や健康診断の結果を医師が持っている場合など、限られます。)※情報通信機器・・・テレビ電話、スマートフォン、タブレット、パソコン等で撮影や通話、インターネット・無線 LAN 通信等が可能な機器

上記の「オンライン診療」の説明を読んで、オンライン診療についてお尋ねします。オンライン診療を受けたいと思いますか。(n=652)

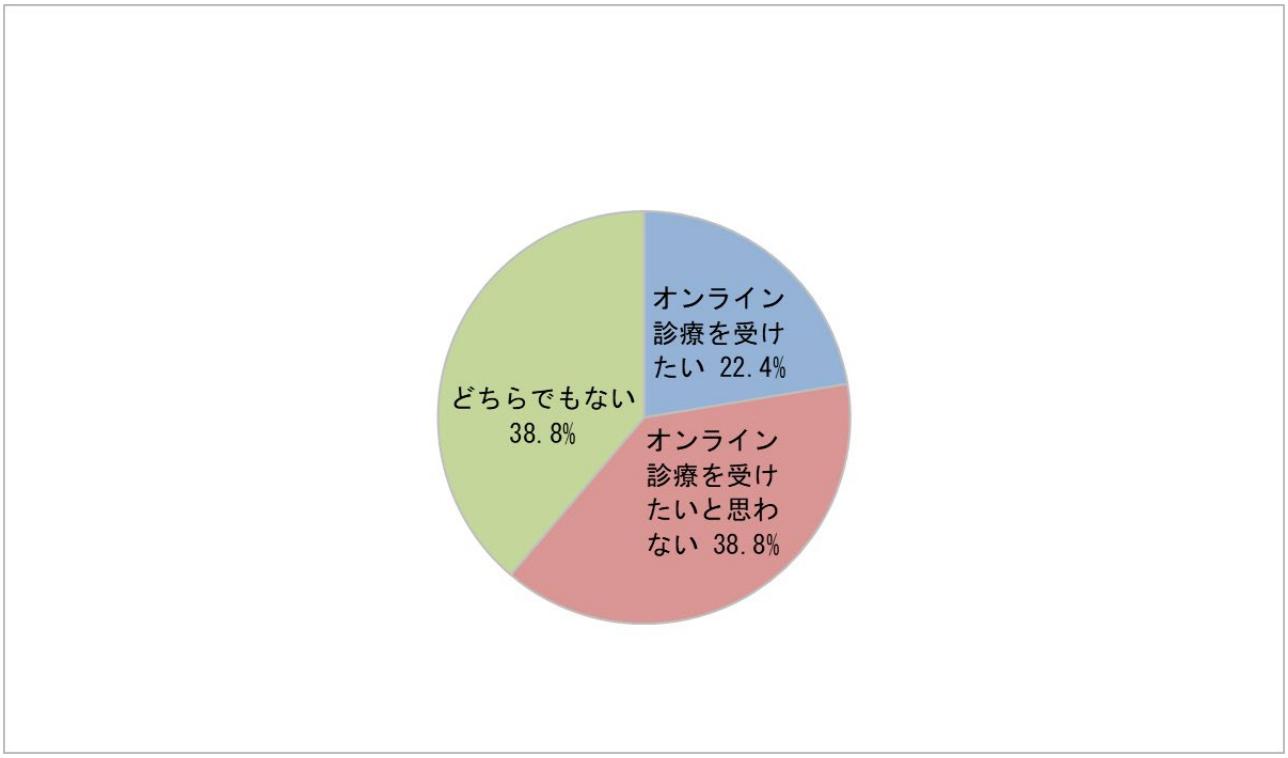


Figure31.オンライン診療での受診の希望

[Q27]前問で、「オンライン診療を受けたいと思わない」と回答された方に伺います。「オンライン診療を受けたいと思わない」理由は何でしょうか。（最も強くそう思うものをお選びください。）（n=253）

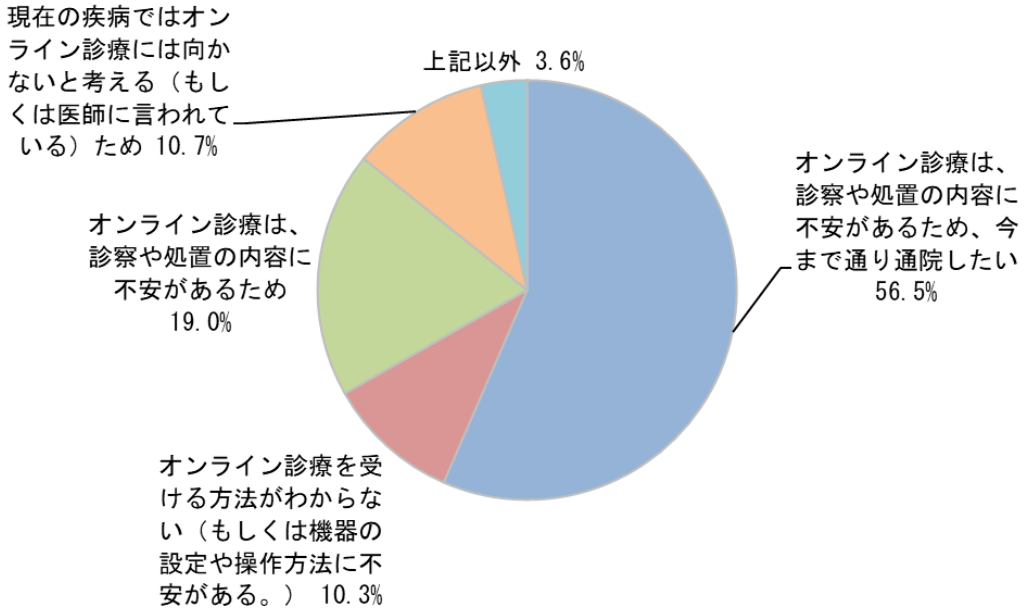


Figure32.オンライン診療を受けたいと思わない理由

[Q28]「オンライン診療を受けたことがない」と回答した方へお尋ねします。オンライン診療を受けていない、またはオンライン診療を受けることができない理由をお教えください。（該当が複数ある場合は、最も強い理由をお選びください。）（n=399）

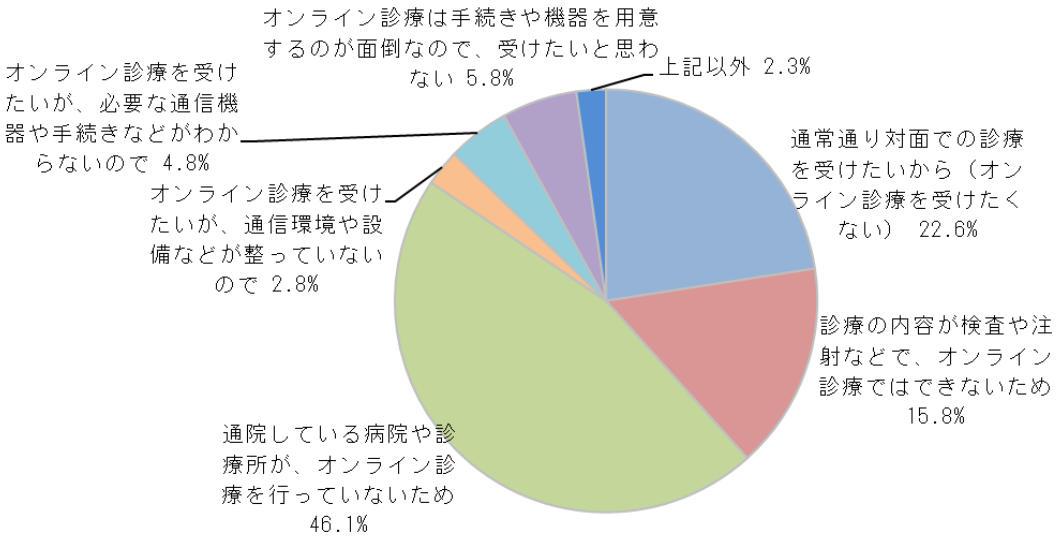


Figure33.オンライン診療を受けた経験がない理由

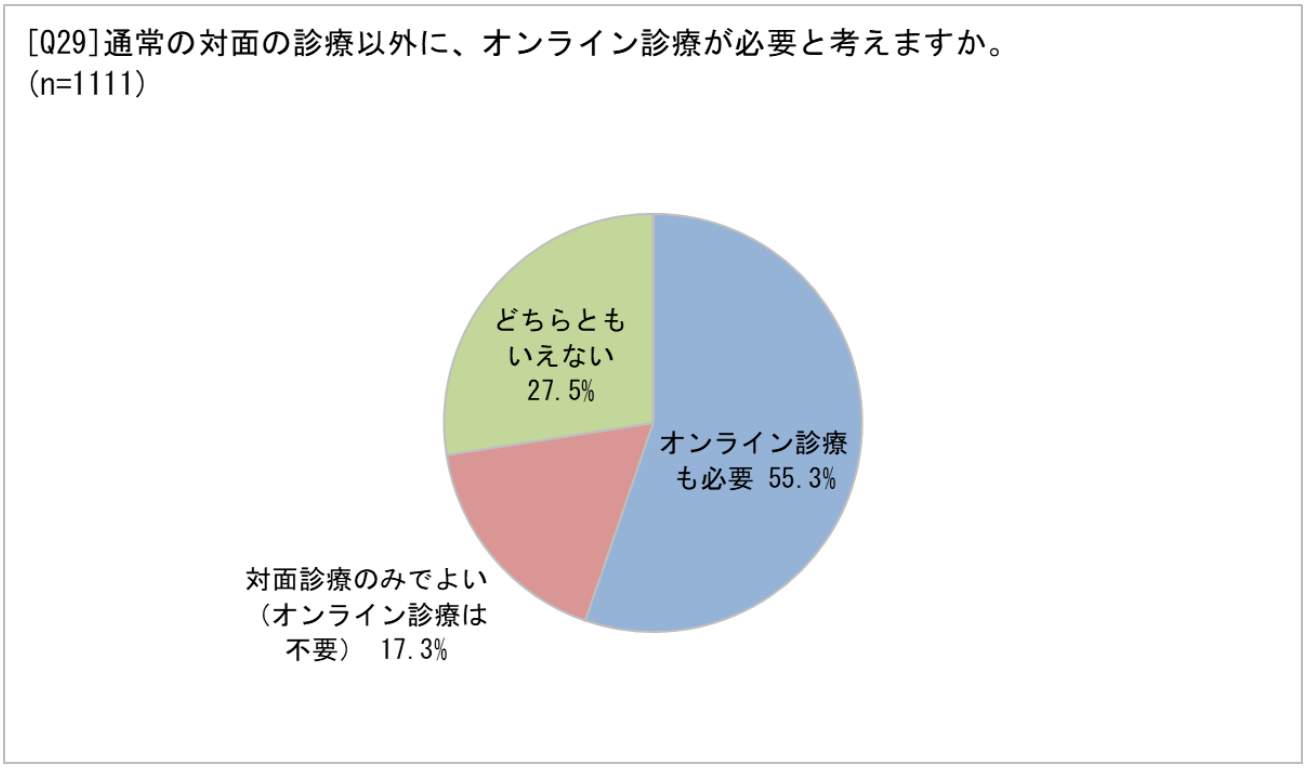


Figure34.オンライン診療の必要性(全回答者)

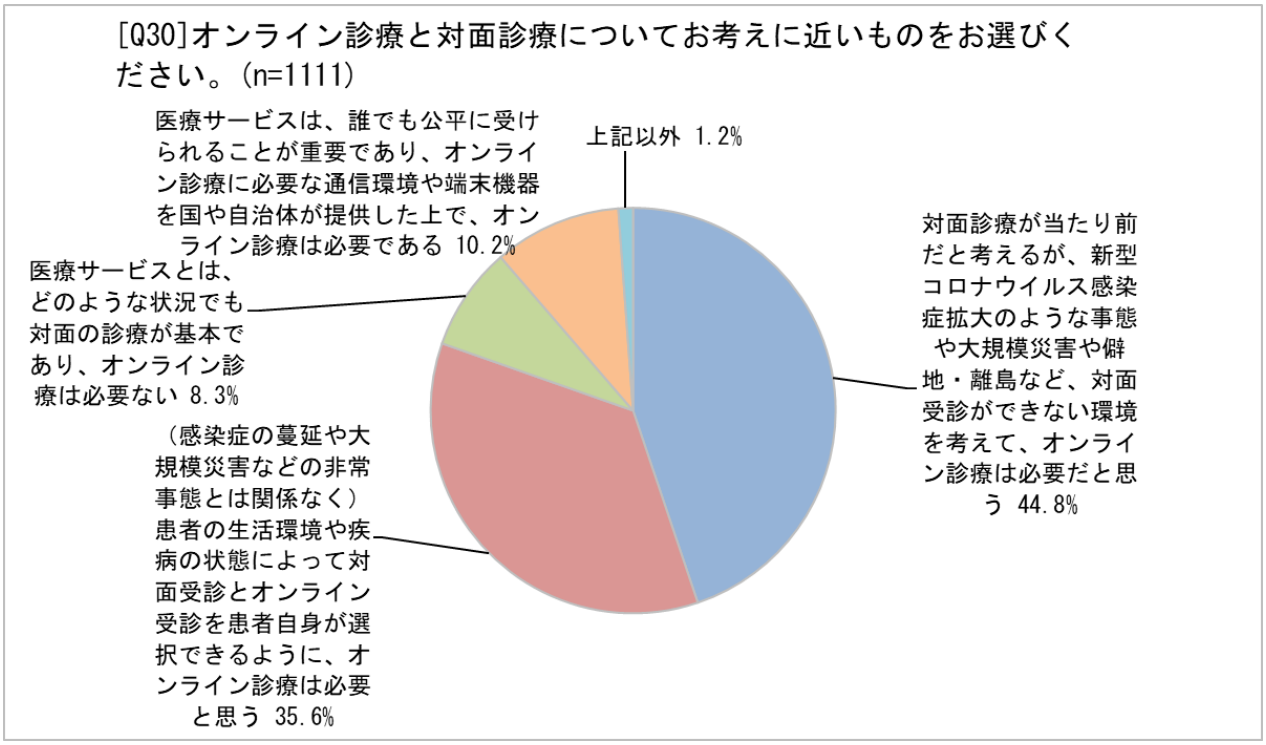


Figure35.オンライン診療と対面診療に対する考え(全回答者)

令和４年度　厚生労働行政推進調査事業費補助金
地域医療基盤開発推進研究事業

分担研究報告書

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（２１ＩＡ２０１３）

研究分担者　美代 賢吾
（国立研究開発法人国立国際医療研究センター医療情報基盤センター長）
研究分担者　星本 弘之
（国立研究開発法人国立国際医療研究センター医療情報基盤センター専門職）
研究分担者　辻岡 和孝
（国立研究開発法人国立国際医療研究センター医療情報基盤センター上級研究員）

研究要旨
令和 2 年度の厚生労働科学研究での調査結果に基づき、医療機関、特に中小規模医療機関など IT に関する専門職員が不在の組織に求められるサイバーセキュリティ対策教育のあり方について検討し、令和 3 年度に標的型メール対応訓練の実施基盤の要素技術開発を行った。令和 4 年度については、令和 3 年度の成果を拡張し、実用的な迷惑メール対応訓練システムの構築を行った。本システムにより、一般的な迷惑メール対応訓練のためのメール配信および配信された訓練メールに対する反応結果の把握が可能となった。今後は、このシステムを用いることにより、民間病院において実施率が著しく低いサイバーセキュリティ対応訓練の普及につながることが期待される。一方、訓練サービスの提供と合わせて、訓練結果などに基づく支援のあり方について検討する必要がある。

A. 研究目的

重要インフラに該当する医療分野において、医療機関等のサイバーセキュリティに対する取り組みを強化することは喫緊の課題である。病院情報システムは、これまで外部と隔絶した情報ネットワークであった状況に対し、データヘルス改革、働き方改革、オンライン診療、モバイルヘルス(m-Health)等の導入で外部ネットワークへの接続が始まっており、情報化が進んでいなかった小規模病院、診療所における電子カルテの導入・普及も進みつつある。さらに、CT や MRI、検体検査機器などが高度化し、開発ベンダーによる常時リモートメンテナンスの体制も一般的となっているほか、進化するクラウド技術により、医療機関内にあったサーバをクラウド上に移行することも現実的になりつつある。

このように急速にネットワーク化され外部との接点が増す医療機関において、近年多発しているランサムウェア攻撃などの事例においては、不適切に構築・管理運用されたシステムにより医療機関内部に侵入されていることが明らかになっていることから、組織としてのサイバーセキュリティ対策への取り組みにくわえ、一般利用者等への適切な教育は喫緊の課題である。しかしながら、令和 2 年度に分担研究者らが実施した医療機関のサイバーセキュリティ実態調査の結果、サイバーセキュリティに関する教育は全体の約 39%（198/508）の病院で実施されているが、より実践的なサイバーセキュリティ対応訓練を実施している医療機関は約 7.7%(39/508)であり、特に、民間医療機関では 3.6%（11/304）のみが実施と大幅に実施率が下がっていることから、セキュリティ訓練を容易に実施できる基盤の整備が有効であると考えられた。

このような背景のもと、主任研究者がおこなう、医療分野におけるサイバーセキュリティ対策と課題についての整理、および医療機関同士が相互にサイバーセキュリティ対策に関する情報共有・相談を行う体制のあり方等の検討状況を参考に、分担研究者らは、医療機関に対する情報セキュリティ教育の方法や、その実施に必要なサービスについての検討し、実用性評価のためのリファレンスシステムについて開発を目的として本研究を行った。

B. 研究方法

令和 4 年度は、令和 3 年度に開発した要素技術検証用のプロトタイプシステムの評価に基づき、以下の内容についての検討と開発評価を行った。

1. 令和 3 年度に構築したプロトタイプシステムの評価にもとづき、実用可能な訓練システムの要件について検討整理した。

2. 1）の検討結果に基づき、評価用のリファレンスシステムについての開発を行った。

C．結果

1. 要件検討

分担研究者らの所属機関におけるサイバーセキュリティ事案分析の結果、令和 4 年度上半期においては、メールシステムによりブロックされた者を含め、受信したメールの 14～16%が迷惑メールであり、システムが検知しなかったものを考えると、一般職員に対する情報セキュリティの脅威としては電子メールによるものが大きな割合を占めると考えられた。これに対して、標的型メールへの対応方法などについて、電子メールなどによる情報提供都度行っているが、これはその他の業務上のメールなどに紛れて、きちんと読まれていない実態が明らかとなっているため、情報提供以外に実際のメールでの訓練については依然有効であると考えられた。そのため、令和 4 年度の開発では、令和 3 年度に評価を実施した要素技術を用いて実運用を行うために必要な以下の機能についての追加開発と検証を行った。

2. 標的型メール対応訓練のリファレンスシステムの仕様

標的型メール対応訓練システムとしては、実運用においては、以下の機能が必要と判断された。

■メールの扱いの検知機能

以下、送信した対象メールアドレスごとに

1）送信したメールの開封の有無の検知機能

2）フィッシングを想定した URL へのアクセスの有無の検知機能

3）マルウェアを模した添付ファイルの開封検知機能

■管理機能

4）訓練結果の集計・表示機能（開封率、URL アクセス率、添付ファイル開封率、など）

5）送信アドレスごとの反応状況（開封、URL アクセス、添付ファイル開封）一覧表示

特に、管理機能のうち送信先アドレスごとの振る舞い状況一覧確認機能は、訓練参加者に対する事後のフィードバックを行う上で必須となることから、今回実装を行った。

3. 開発結果

令和 4 年度の開発の結果を以下に示す。

1） 管理画面

図 1 に示す管理画面では、発信した訓練メール数およびそれらのメールに対する受信者（訓練参加者）による①メール開封、②メール内に記載の URL へのアクセス、③メールに添付されたファイルの開封（閲覧）の各イベントの発生数の集計値を確認可能である。表示期間は任意に設定可能としている。

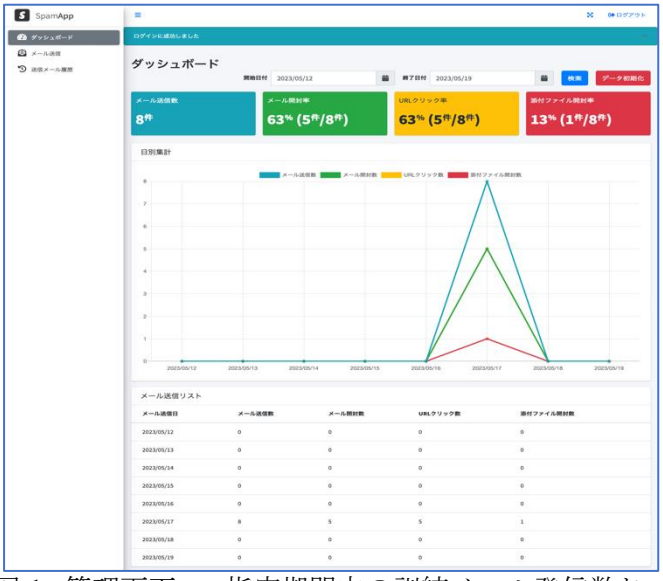


図 1：管理画面： 指定期間内の訓練メール発信数およびそれらのメールに対する受信者の反応状況を集約表示し、一覧で把握可能としている。

2） 訓練メール作成・発信画面

図 2 に訓練メールの作成画面を示す。この画面において、訓練メールの送信先アドレス、件名・本文と URL や添付ファイルの有無などを設定可能である。添付ファイル名については任意に設定可能であるが、現時点ではファイル形式は html 形式のみとなっている。

図 2：訓練メール作成及び発信画面。任意の宛先アドレスに対して、入力された件名・本文および添付ファイルなど設定して送信する。

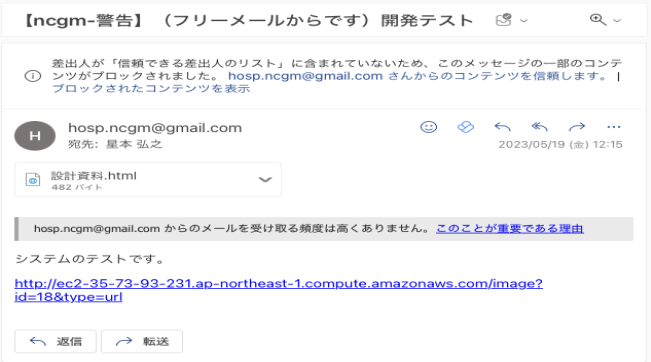


図 2-2：実際に受信された訓練メールの例。コンテンツブロックにより、この時点ではメール開封の検知はできていない。

3） 各受信者の反応状況確認画面
図３に訓練メールを送信したアドレスごとの訓練メールに対する反応状況の確認画面を示す。この画面では、送信先アドレスごとに①メール開封、②メール本文中の URL へのアクセス有無、③添付したファイルの開封・閲覧の有無、の各イベントの発生状況についてそれぞれ確認可能である。また、それぞれのイベントごとに表寿の有無を設定可能である。

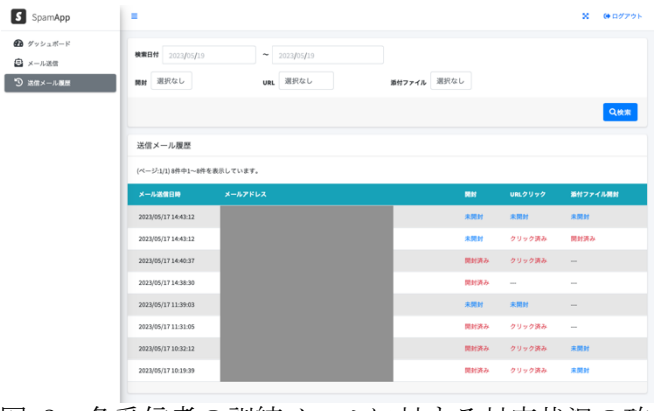


図 3：各受信者の訓練メールに対する対応状況の確認画面。開封、ＵＲＬクリック、添付ファイル開封について確認可能なほか、表示するイベントの絞り込みが可能。

D．評価と考察

今年度開発したシステムにより、迷惑メール対応訓練の実施に向けて必要となる機能の実装はほぼ完了したと考えられる。一方、本システムを用いて分担研究者らの所属組織のメールシステム（Microsoft 社の Office365）に対して訓練メールを試験送信したところ、一部受信者において訓練メールが本物の迷惑メールと判定され、検疫処理が行われるという事象が見られた。これはメールシステム自体のセキュリティ機能の高さを示すと考えられるが、一方では円滑に訓練を実施する上では若干の障害になると考えられるため、訓練の実施においては注意が必要である。しかし、当センターにおいても、度重なる注意喚起にもかかわらず、検疫処理されたメールに対してわざわざ検疫を解除して開封し、さらに添付ファイルや本文中の URL にアクセスを行い、マルウェア感染などに至った事例もあることから、一般利用者に対する訓練としてはこのようなケースもあるいは有効である可能性もある。さらに、セキュリティ訓練を円滑に実施する上では、メールシステム自体にそのような訓練機能を組み込むことも有効と考えられるため、その点についてはメールシステム運用事業者などの意見を今後確認したいと考えている。
本システムの実装とサービスの提供により、中小規模医療機関などにおける標的型メール対応訓練の実施率向上が期待できることから、医療機関のサイバーセキュリティレベルの向上が期待される。

なお、分担研究者らの所属組織においても、一般職員からの不審メールに関する通報・相談に加え、不審サイトなどに実際にアクセスしてしまったケースが日々発生しており、それらの対処には複数の専任職員やオペレータなどがあたっているが、業務上かなりの負荷となっている。これに対し、中小規模の医療機関においては情報システムの専任担当者が置かれていないケースが非常に多く見られることから、本システムなどによる訓練の実施と合わせ、その結果の分析や対応方法に関する情報提供、教育の実施などについて支援する組織が必要と考えられることから、教材作成と提供や支援のあり方について早急に整理し、体制を構築する必要があると考えられる。

E．結論

本システムの開発により、標的型メール対応訓練の実施基盤の実用に向けた開発と検証を行った。今回の開発により、必要な機能についての開発と評価が行えたと考えられる。一方、本システムなどの外部システムなどによる訓練メールは実際のメールシステムにおいて検疫対象と判定される場合もあることから、実際の訓練実施においては、その点も考慮した計画が必要と考えられる。

F．健康危険情報

特になし

G．研究発表

１．論文発表
特になし

２．学会発表
特になし

３．その他
(1) 美代 賢吾. 医療機関のための情報セキュリティ対策　サイバー攻撃から守る、情報漏えいを防ぐためのノウハウ】病院管理者・医療情報部門に求められる情報セキュリティ対策 医療情報システム・医療機器のリモート保守をめぐって. IT Vision 37:2-43, 2022.
(2) 美代 賢吾. ランサムウェアって知っていますか−医療機関を狙うサイバー攻撃への防御と対策. LiSA 29 巻 8 号:739-746, 2022,
(3) 菅沼景子, 星本弘之, 美代賢吾. 医療情報システムにおける二要素認証技術の現況と課題―効果的導入法を含め―. 新医療 50 号:62-66, 2023.

H．知的財産権の出願・登録状況（予定を含む。）

特になし

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

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

記録類

1. 成果一覧
2. 研究組織

研究成果の刊行に関する一覧表（総括報告）

番号	発表者	論文題目	大会名	ページ	年度
1	近藤博史	コロナ禍におけるIoTを含めたサイバーセキュリティの現状と対策、および対策としてのISAC	第41回医療情報学連合大会 41st JCMI	p.434-435	2021
2	近藤博史	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	第41回医療情報学連合大会 41st JCMI	p.436-439	2021
3	林 薫	サイバー攻撃の現状から考える医療分野のセキュリティ対策	第41回医療情報学連合大会 41st JCMI	p.440-442	2021
4	松元 恒一郎	IoT機器としての医療機器、モバイルヘルスにおけるセキュリティ対策の現状	第41回医療情報学連合大会 41st JCMI	p.443-446	2021
5	田中 彰子	医療分野におけるサイバーセキュリティ対策と情報共有・相談体制の試行	第41回医療情報学連合大会 41st JCMI	p.447-448	2021
6	近藤 博史	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.	日本遠隔医療学会雑誌,17(Suppl.),	24	2022
7	近藤 博史.,松山 征嗣	最近のサイバー攻撃の特徴	日本遠隔医療学会雑誌,17(Suppl.),	25	2022
8	美代賢吾	医療機関とサイバー攻撃標的型攻撃とランサムウェアを中心に	週刊医学界新聞	3月8日号	2021
9	美代賢吾	医療情報システムと新興感染症・災害・サイバー攻撃を考える；医療者・患者を支援し、診療を継続するために	IT Vision, 43	42-43	2021

番号	発表者	論文題目	大会名	ページ	年度
1	近藤 博史	厚生労働省調査事業等から分かった保険医療分野の サイバーセキュリティの現状と対策	第42回医療情報学連合大会 42nd JCMI	p.364-367	2022
2	長谷川高志	サイバー攻撃から診療記録を守るために何をするべきか？　－ストレージからの検討－	第42回医療情報学連合大会 42nd JCMI	p.368-370	2022
3	山本 隆一	医療情報システムの安全管理に関するガイドライン- サイバーセキュリティの観点から -	第42回医療情報学連合大会 42nd JCMI	p.368-373	2022
4	田中 彰子	医療分野におけるサイバーセキュリティ対策の取組みについて	第42回医療情報学連合大会 42nd JCMI	p.374-375	2022
5	美代賢吾	医療機関のための情報セキュリティ対策 サイバー攻撃から守る、情報漏えいを防ぐためのノウハウ】病院管理者・医療情報部門に求められる情報セキュリティ対策　医療情報システム・医療機器のリモート保守をめぐって	INNERVISION 37巻7付録	Page42-43	2022
6	美代賢吾	ランサムウェアって知っていますか-医療機関を狙うサイバー攻撃への防御と対策	LiSA 29巻8号	Page739-746	2022
7	近藤博史 山本隆一 長谷川高志 美代賢吾 星本弘之 持田真樹 西村元宏	サイバー攻撃から診療記録を守るために何をするべきか? 厚生労働省調査事業等から分かった保険医療分野のサイバーセキュリティの現状と対策	第42回医療情報学連合大会論文集	Page364-367	2022
8	菅沼景子 星本弘之 美代賢吾	医療情報システムにおける二要素認証技術の現況と課題―効果的導入法を含め―	新医療 50(1)	62-66	2023
9	近藤博史 長谷川高志 山本隆一 美代賢吾 星本弘之	新たに発見された脆弱性対応の組織的対策の必要性	日本遠隔医療学会雑誌18巻補刊号	Page63	2023

研究組織

所属機関・部署・職名	氏名	分担した研究項目及び研究成果の概要	研究実施期間	配分を受けた研究費	間接経費
特定非営利活動法人日本遠隔医療協会・特任上席研究員	近藤博史	代表および研究統括 成果 ・　サイバーセキュリティ技術の調査 ・　中小病院のサイバーセキュリティ実態調査	令和３年４月１日～令和５年３月３１日	63,323,000円	19,107,000円
特定非営利活動法人日本遠隔医療協会・特任上席研究員	長谷川高志	分担した研究項目 ・医療者向けサイバーセキュリティアンケート ・中小病院の調査手法開発と実施管理 成果 ・病院調査の管理完了 ・アンケート終了、集計	令和３年４月１日～令和５年３月３１日	0円	0円
医療情報システム開発センター・理事長	山本隆一	分担 ・医療分野のガイドラインの調査・精査 成果 ガイドラインの検討や改定すべき課題を見いだした。	令和３年４月１日～令和４年３月３１日	1,000,000円	300,000円
国立研究開発法人国立国際医療研究センター・医療情報基盤センター・医療情報基盤センター長	美代賢吾	分担 ・効果的なセキュリティ教育 ・情報共有の検討 成果 教育手法の評価	令和３年４月１日～令和４年３月３１日	1,000,000円	300,000円
国立研究開発法人国立国際医療研究センター・医療情報基盤センター・副医療情報管理部門長	星本弘之	分担 ・医療機器等に関連した調査と対策の整理 成果 教育手法の評価	令和３年４月１日～令和４年３月３１日	0円	0円
国立研究開発法人国立国際医療研究センター・医療情報基盤センター・上級研究員	辻岡和孝	効果的なセキュリティ教育・情報共有の検討	令和4年4月1日～令和5年3月31日	0円	0円

厚生労働科学研究費補助金地域医療基盤開発推進研究事業
「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」（21IA2013）

研究班 事務局
〒370-0033
群馬県高崎市中大類町37-1　高崎健康福祉大学健康福祉学部医療情報学科内
特定非営利活動法人日本遠隔医療協会
TEL / FAX：027-350-7475
e-mail: telemedicine-research@j-telemed-s.jp