一般社団法人遠隔画像診断サービス連合
セキュリティアンケート調査結果

一般社団法人遠隔画像診断サービス連合会
/一般社団法人医療ISAC

2023年11月

＜目次＞

1．調査概要

1．調査目的

近年、国内の医療機関におけるランサムウェア被害事例が多く報告されている。21年10月の徳島県つるぎ町立半田病院に続き、22年1月から複数の医療機関が攻撃を受け、最近では22年10月の大阪急性期・総合医療センターでも同種の被害が発生したことは記憶に新しい。

これらの感染事案の大半は、半田病院の事例が示すように、外部事業者とインターネットを経由して医療機関の院内ネットワークを結びつけるために設置していたVPN機器の脆弱性が原因で発生している。
また、大阪急性期・総合医療センターの事例は、給食関連業務を事業者/医療機関間の拠点間接続を介して提供していた状況下にて、当該事業者の一般業務用ネットワークに設置していたVPN機器の脆弱性が悪用され、委託元である医療センターの内部ネットワークにまで感染拡大が発生しており、いわゆる、「サプライチェーン攻撃」と呼ばれるものに該当するものとなる。

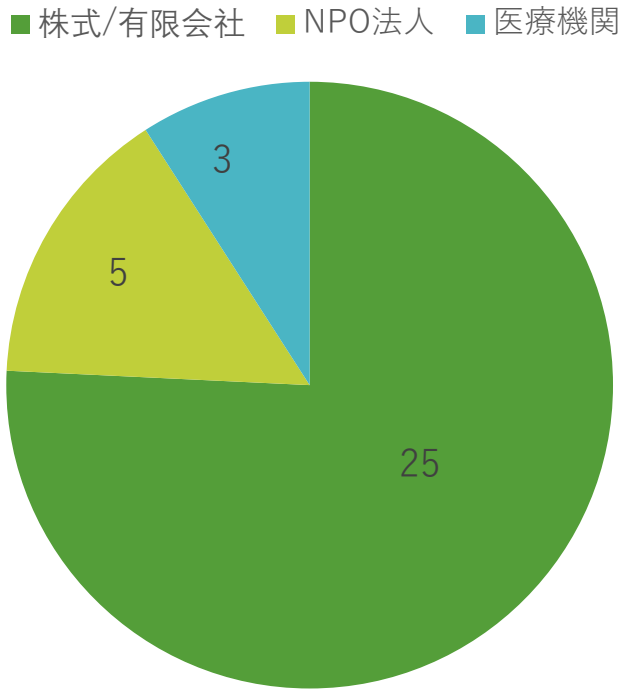
こうした事案の続発を受け、厚生労働省は22年11月に医療機関に対して院内ネットワークと結びつく外部との接続点の棚卸しの必要性を通知しているが、いまだにこうした外部ネットワークとの接続点の脆弱性を悪用したサイバー攻撃事案は報道に上がらないものも含め多くの医療機関で発生している状況である。

このような状況を受け、高度化・巧妙化するサイバー攻撃に対して、遠隔診断サービスを提供する業界のセキュリティ現状の課題を探るべく、（一社）医療ISAC/一般社団法人遠隔画像診断サービス連合会(ATS)は、遠隔画像診断サービス・遠隔読影サービス（以下、『遠隔診断サービス』と略記）を医療機関等に対して外部から提供する事業者のセキュリティ管理状況を共同調査した。

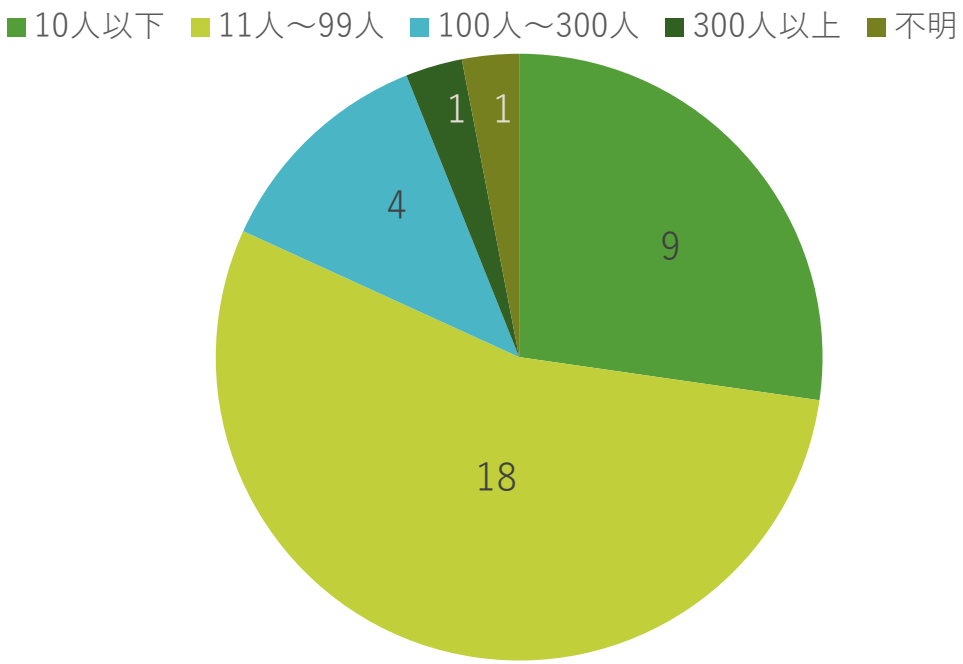
1．調査対象(1/2)

- 調査期間：2023年10月18日～11月9日
- 対象組織：ATS正会員組織（57組織）
- 回答率：58% (33組織)
- 調査組織：（一社）遠隔画像診断サービス連合会（ATS)/ （一社）医療ISAC

＜組織種別内訳＞

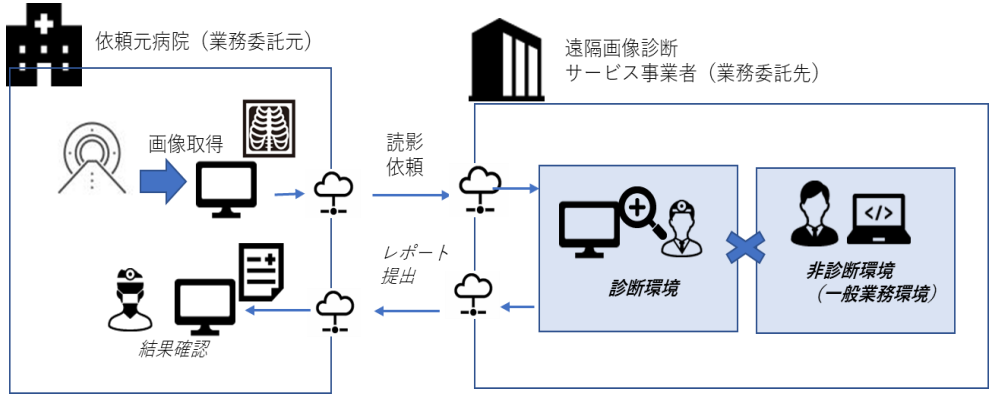


＜従業員数（組織規模）別内訳＞

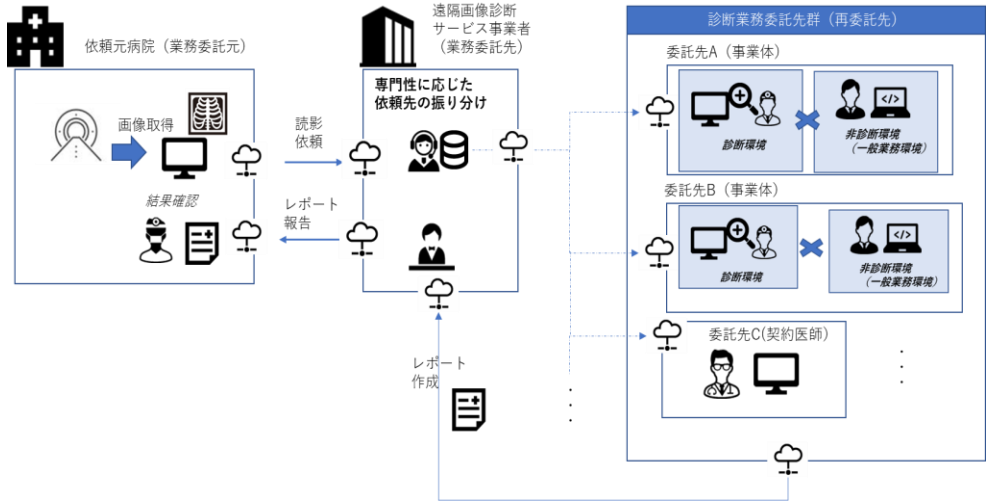


1．調査対象(2/2)

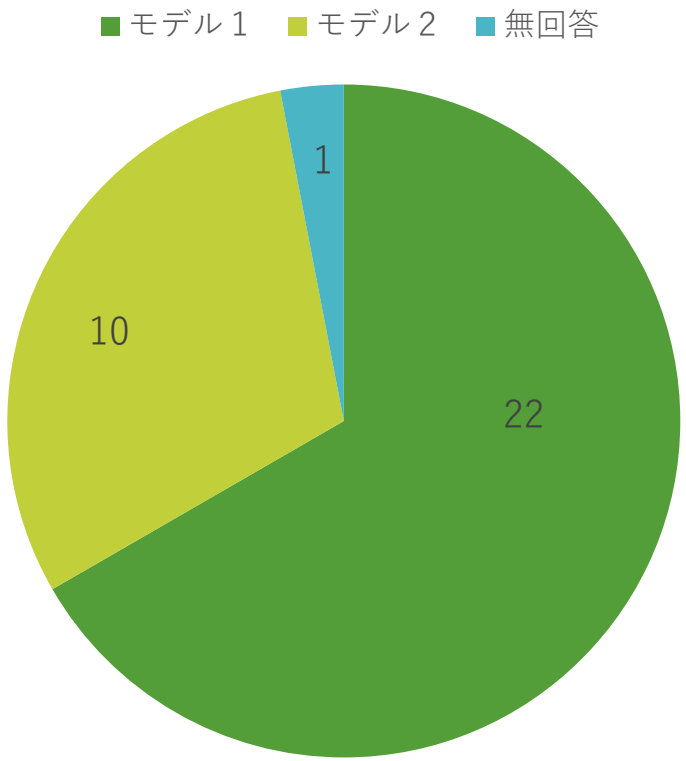
サービス提供モデル１：病院（委託元）/事業者（委託先）の二社間モデル(1対1型)



サービス提供モデル２：病院（委託元）/事業者（委託先）/事業者委託先（再委託先）の多数間モデル(1対N型)



<サービス提供モデル別内訳>



1．調査項目(1/4)

調査項目は以下の13項目のうち、回答結果に応じて回答対象項目が分岐する方式となる。

カテゴリ		調査項目		回答項目
No.1	ガイドラインへの対応・認識状況	No.1-1	医療機関への遠隔画像診断サービス、または遠隔読影サービス（以下、『遠隔診断サービス』と略記）を提供する事業者として、経済産業省・総務省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」(以下、『2省ガイドライン』)に基づくセキュリティ対応を行っていますか？	□ はい　□ いいえ（「不明」含む） *※回答が「はい」の場合はNo.2の設問、「いいえ」の場合はNo.1-2に進んでください*
		No.1-2	2省ガイドラインの存在を知っていますか？	□ はい　□ いいえ（「不明」含む） *※回答が「はい」の場合はNo.1-3、「いいえ」の場合はNo.2の設問に進んでください*
		No.1-3	2省ガイドラインに基づく対応を行っていない理由の中で、該当するものをすべてご回答ください。	□ 2省ガイドラインは適用されず、対応の必要がないと考えていたため □ 対応のコスト・リソースが確保できないため □ 依頼元の医療機関から2省ガイドラインの対応を求められなかったため □ それ以外の理由　（自由記述） *※回答にかかわらず、そのままNo.2の設問に進んでください*

1．調査項目(2/4)

カテゴリ		調査項目		回答項目
No.2	自社内部のセキュリティ管理状況	No.2-1	貴社では依頼元の医療機関との間で画像診断対象となるデータ等をやり取りする場合、どのようなネットワークセキュリティを採用していますか？ 最も近しいものを一つご回答ください。	□　インターネット回線を利用したVPNを採用 □　閉域網の回線を利用したVPNを採用 □　専用線の採用 □　データ授受用のクラウドサービスの採用 □ 特段のネットワークセキュリティは実施していない（「わからない」を含む） □　その他 *※回答にかかわらず、No2-2に進んでください*
		No.2-2	依頼元の医療機関とネットワーク接続するための自社管理の機器（VPN機器やルータ等）について、メーカが公表した新たなファームウェアやセキュリティパッチの適用（脆弱性対応）を実施していますか？	□ メーカが公表した時点から5営業日以内に都度実施している □ メーカ公表に応じた都度の頻度ではなく、一定の頻度で情報収集し、実施している □ 特に実施していない（「わからない」を含む） *※回答内容にかかわらず、No2-3に進んでください*
		No.2-3	依頼元の医療機関とネットワーク接続するための自社管理の機器（VPN機器やルータ等）について、ログインパスワードを定期的に変更していますか？	□　変更している □　変更していない（「わからない」を含む） *※回答内容にかかわらず、No2-4に進んでください*
		No.2-4	医療機関から提供された画像を診断するための環境（以下、『画像診断環境』）は、貴社内部の業務ネットワークから独立していますか？	□はい　□いいえ *※回答が「はい」の場合はNo.2-5、「いいえ」の場合はNo.2-6に進んでください。*

1．調査項目(3/4)

カテゴリ		調査項目		回答項目
No.2	自社内部のセキュリティ管理状況	No.2-5	社内の業務ネットワークから独立した画像診断環境には、ウイルス対策ソフトの導入やセキュリティパッチの適用等、セキュリティ対策を実施していますか？	□ 実施している　□ 実施していない *※回答が「実施している」の場合は、No2-7、「実施していない」の場合はNo2-6へ進んでください。*
		No.2-6	社内の業務ネットワークにおける、インターネット等の外部ネットワークとの接続点に設置されているネットワーク機器に対して、新たなファームウェアやセキュリティパッチの適用（脆弱性対応）を実施していますか？	□ 全ての機器を対象にして、のファームウェア/セキュリティパッチ適用について、メーカが公表した時点から5営業日以内に、都度実施している □ 一部の機器（重要度の高い機器）については、ファームウェア/セキュリティパッチ適用を、メーカが公表した時点から５営業日以内に都度実施している □ ファームウェア/セキュリティパッチの適用は、メーカ公表に応じた都度の頻度ではなく、一定の頻度で情報収集し、実施している □　特に実施していない *※回答内容にかかわらず、そのままNo2-7に進んでください。*
		No2-7	貴社の画像診断環境とネットワークで接続する医療機関、または遠隔診断業務を委託する外部事業者において仮にマルウェア感染等が発生した場合、貴社の画像診断環境へのネットワークを介した二次感染を予防/検知するために、何らかのセキュリティ対策を講じていますか？	□　実施している（セキュリティ対策の実施概要を記入ください） □　実施していない *※＜サービス提供モデル＞が「モデル1」とご回答いただいた方はここでアンケート回答は終了です。* *「モデル2」とご回答頂いた方のみ、No3に進んでください。*

1．調査項目(4/4)

サービス提供モデル２：病院（委託元）/事業者（委託先）/事業者委託先（再委託先）の多数間（1対N）モデルに該当する場合のみ回答

カテゴリ		調査項目		回答項目
No.3	自社サービスサプライチェーン上のセキュリティ管理状況	No.3-1	依頼元の医療機関から提供された画像診断対象データを、業務委託（医療機関にとっては再委託）している事業者、または個人（医師）とやり取りする場合、どのようなネットワークセキュリティを採用していますか？ 最も近しいものを一つご回答ください。	□　インターネット回線を利用したVPNを採用 □　閉域網の回線を利用したVPNを採用 □　専用線の採用 □　データ授受用のクラウドサービスの採用 □ 特段のネットワークセキュリティは実施していない（「わからない」を含む） □　その他 *※回答内容にかかわらず、そのままNo3-2へ進んでください。*
		No.3-2	遠隔診断を業務委託（医療機関にとっては再委託）している事業者、または個人（医師）が、貴社からの依頼に基づき画像診断を行う際のIT環境に対して、セキュリティ対策の実施を指示・依頼していますか？	□　実施している　（実施依頼している対策の概要を記入ください） □　実施していない *※回答が「実施している」の場合はここでアンケート回答は終了です。「実施していない」の場合はNo3-3へ進んでください。*
		No.3-3	業務委託先の事業者/個人（医師）の画像診断環境に対して、セキュリティ対策の実施を指示・依頼していない理由のうち、該当するものをすべてご回答ください。（複数回答式）	□　VPN等の自社主導で設定したネットワークセキュリティによって、委託先のセキュリティ対応も図れていると考えているため □　委託先が主体的に実施しており、あえて指示・依頼する必要がないと考えているため □　特段の理由はない □　その他

２．全体結果

＜２．全体総評＞

- 今回の調査対象組織のうち、遠隔診断サービスを提供する上でコンプライアンスとして求められる２省ガイドラインについて、７割以上が対応済みではあるが、**3割近くが未対応で、そのうち半数は2省ガイドライン自体の存在を把握しているが、対応未着手である状況**であった。
- 未実施の理由のなかで、一番大きい理由は、医療機関等から、こうした依頼が届いていないという点であり、**医療機関等を起点としたリスクコミュニケーションが十分でない**といえる。

- 事業者の多くは医療機関との画像データ等を取り交わすに際して、それぞれの観点より適したと判断するネットワークセキュリティを講じている。ただし、医療機関とのネットワーク接続点となる機器における**パッチ適用頻度は十分ではない傾向が強いといえる**。
- 例えば、適用前のセキュリティ脆弱性を悪用された場合、ネットワーク機器におけるログインPWの漏洩リスクが想定されるため、こうした**PWの変更には、より意識的に取り組むことが必要である**。

- さらに、複数の接続先への接触を前提とする遠隔診断サービス提供主体においては自社では然るべきセキュリティ対応は行っている一方で、**接続先の諸組織に自社として＜責任共有/分界＞モデルにおいてどのような事項を共有・依頼するかを整理する取組が十分とは言えない組織も見受けられている**。

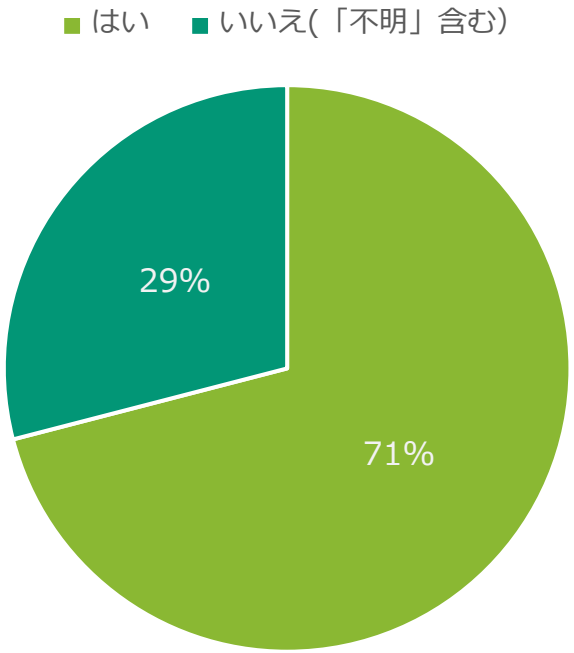
- こうした取り組みは、遠隔診断サービス以外も含めた、医療機関・事業者間のサイバーリスクにかかわるコミュニケーションの基底部を形成するものである。**MDS/SDSを提出すれば良いという安易に流されることなく、医療機関、ひいては接続先のステークホルダーとのサイバーリスクコミュニケーションを確実に行うことが必要**といえる。

＜２．アンケート調査結果_全体結果(1/4)＞

【１．ガイドラインへの対応・認識状況】

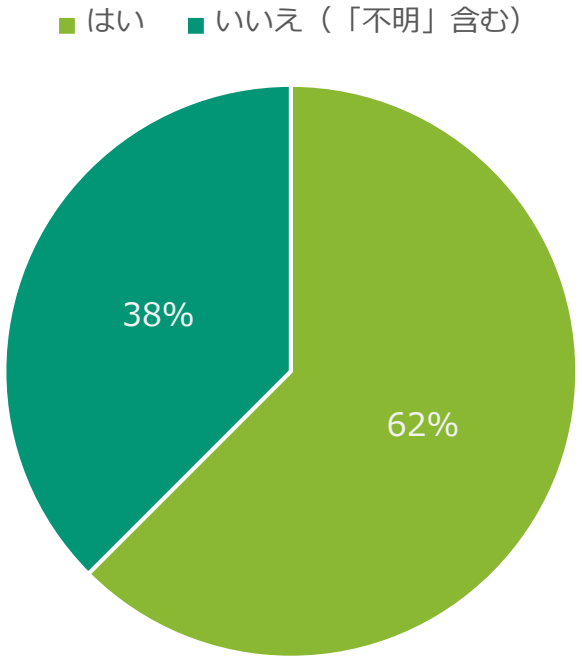
＜1-1：2省GLへの対応状況＞　※n=31

(無回答２件除く)

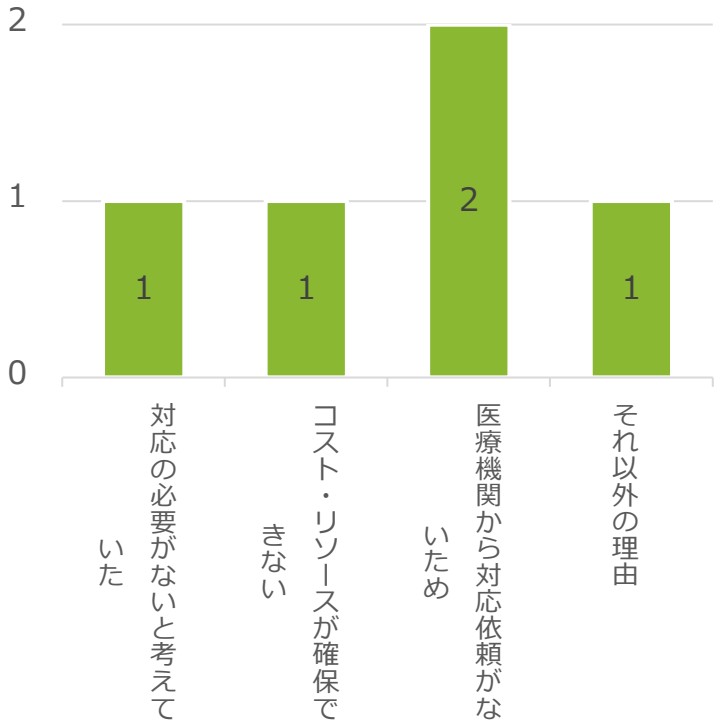


＜1-2：1.1が＜いいえ＞の場合の２省GLの存在の認識有無＞　※n= 8

(無回答1件除く)



＜1-３：1.２が＜はい＞（認識している）の場合の未対応理由（複数回答）＞　※n=5

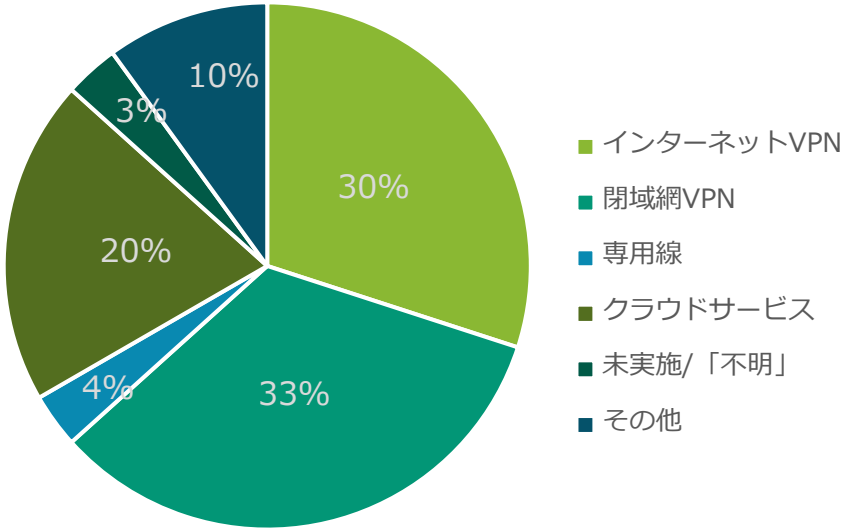


遠隔診断サービスを提供する外部事業者の７割以上は経産省・総務省安全管理GLに対応する取組を行っている。
一方で、３割程度の組織は、GLの存在を認識しているものの、対応の喫緊性を認識していない状況である。

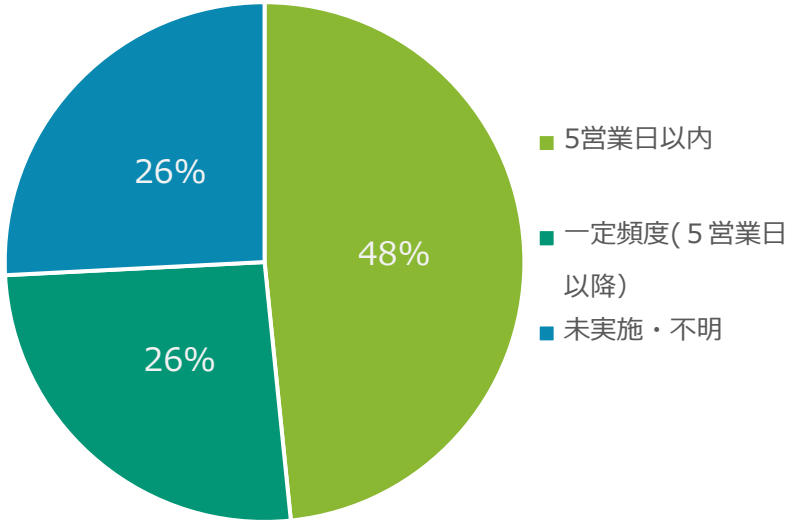
＜２．アンケート調査結果_全体結果(2/4)＞

【２．自社内部のセキュリティ対応状況】

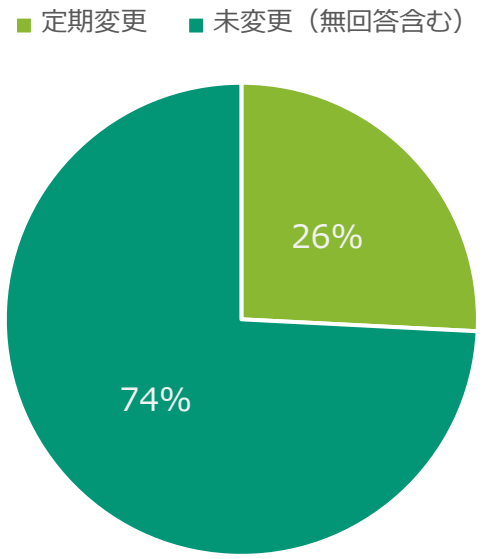
＜2-1：医療機関とデータ授受する場合のネットワークセキュリティ＞ ※n=30 (無回答3件除く)



＜2-2：対医療機関接続用のNW機器のパッチ適用＞ ※n=31 (無回答２件除く)



＜2-3：対医療機関接続用のNW機器のログインPWの定期変更＞ ※n=31 (無回答２件除く)



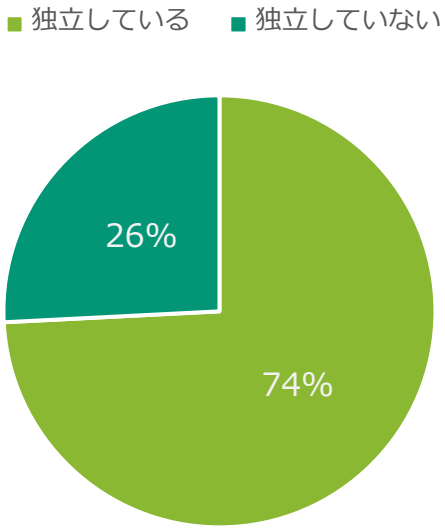
遠隔診断サービス提供事業者の多くは医療機関との画像データ等を取り交わすに際したネットワークセキュリティを講じているものの、**パッチ適用頻度は半数でタイムリー性を欠いている**。
さらに他業種ではセキュリティ慣習として一般化している、**適用前の脆弱性を悪用された場合、流出する可能性のあるログインPWの変更を行う取組の実施率は３割未満**に留まっている。

＜２．アンケート調査結果_全体結果(3/4)＞

＜2-4：画像診断環境/業務ネットワーク間の独立性＞

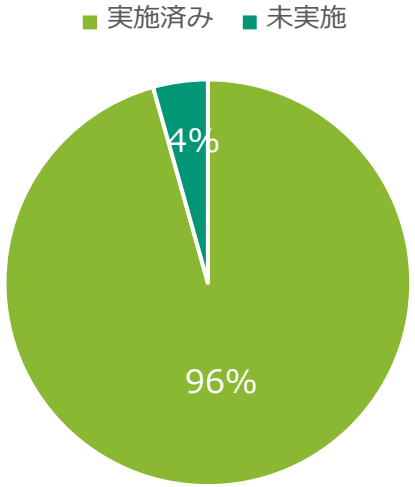
※n=31

(無回答２件除く)



＜2-5：業務NWから独立した画像診断環境におけるセキュリティ実施有無＞

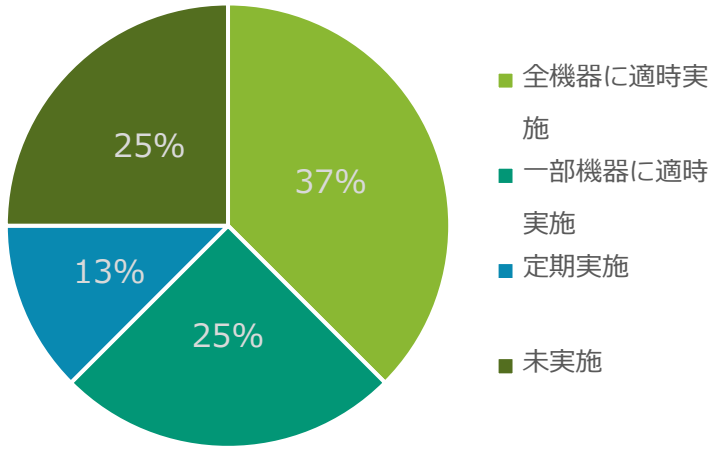
※n=23



＜2-6：画像診断環境と独立していない業務NWが外部接続する機器におけるセキュリティパッチ対応状況＞

※n=8

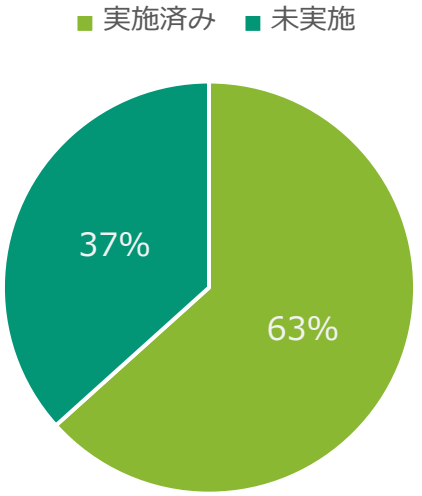
(無回答1件除く)



＜2-7：二次感染被害対策の実施有無＞

※n=30

(無回答3件除く)

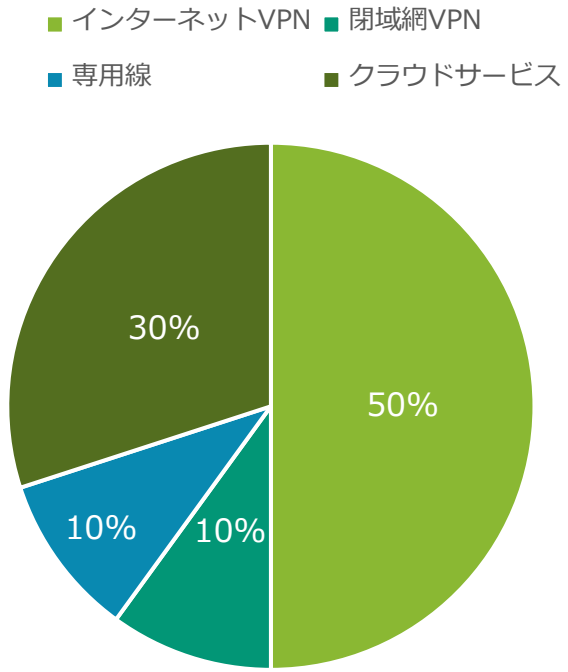


対顧客（医療機関）業務/社内業務の環境分離率は高く、セキュリティ対策も進んでいるものの、**環境分離のできていない企業の一部は対外接続用機器に係るセキュリティパッチ適用が進んでいない状況**である。二次被害感染対策を講じているとの回答自体は多いものの、**対外接点に係る脆弱性リスクに備えた予防的な取組の弱さ**が浮き彫りになっているといえる。

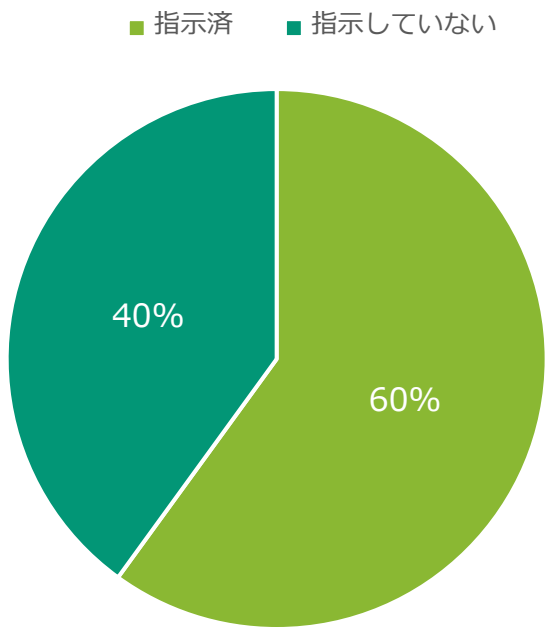
＜２．アンケート調査結果_全体結果(4/4)＞

【３．自社サービスサプライチェーン上のセキュリティ管理状況】

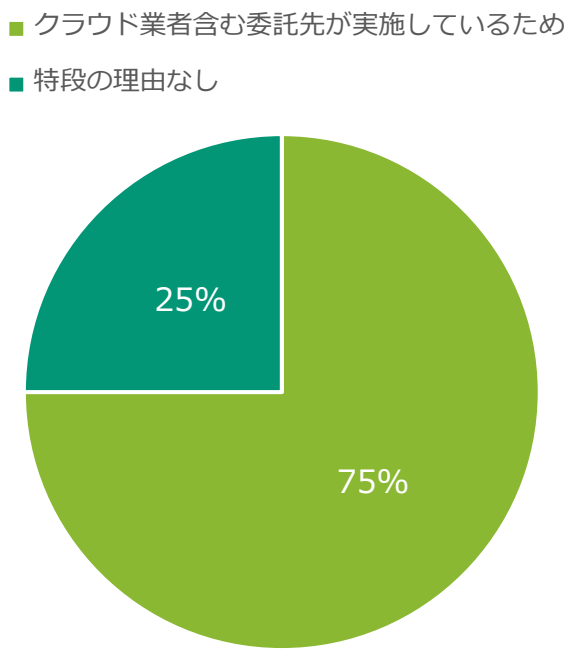
＜3-1：外部とデータ授受する場合のネットワークセキュリティ＞　※n=10



＜3-2：業務委託先へのセキュリティ依頼事項の指示有無＞　※n=10



＜3-3：3-2が「指示していない」場合の理由＞（複数回答）　※n=4



医療機関以外の接続組織も想定したサプライチェーン上のサイバーリスクを想定した自社内部のリスクマネジメント（ネットワークセキュリティ）の取組は様々に行われている。しかしながら、相手先組織へ適切なセキュリティ依頼事項を伝達・共有する**リスクコミュニケーションの取組は４割ほどで未実施**であり、その理由の多くも委託先が実施しているはずという、**根拠のない楽観**に陥っている点には留意すべきである。

３．従業員数（規模）別内訳

＜３．従業員数別総評＞

- 従業員数別(規模別）で見た場合、**規模の小さい組織体ほど、GLへの対応状況、ひいてはGLの認識率も低くなる**傾向が見受けられる。
- 従業員数の多い組織体ほどネットワークセキュリティの選択肢が洗練され、特定の方式へ収れんする傾向がある。
- 医療機関と接続するためのNW機器については(一部例外を除き）半数の割合が適時に実施しているが、**規模の小さな組織体のほうがログインPWの定期変更率が高いという、逆説的な傾向**も見受けられる。
- 業務ネットワークから独立した画像診断環境を有する組織体はいずれの規模でもセキュリティ対策を講じている。
- 一方で**業務NWと接続した診断環境を有する組織体ではインターネット等との接続機器に係るパッチ適用を適時に行えていないケース**が一部に見受けられる。
- なお、**接続先からの二次感染被害対策は規模が小さいほど未実施率が高く**なっている。
- 1対N型の多数間モデルを採用する組織体はいずれも然るべきネットワークセキュリティを実施しているが、**100人以下の規模の場合、委託先へのセキュリティ実施事項の依頼率は低い状況**である。なお、その理由の多くは委託先が実施しているはずという楽観に依拠しており、その意味でリスクを抱えているといえる。

＜３．前提＞

- 今回の調査対象の母集団（33件）のうち、組織種別の観点からは、約8割近く（25件）が「株式会社(有限会社を含む」となっている。

- また、従業員数（規模別）の観点でみると、「NPO法人」（5件）はすべて「11人～99人」の層に分類され、「医療機関」（3件）はすべて従業員数の層が異なる結果となっている。

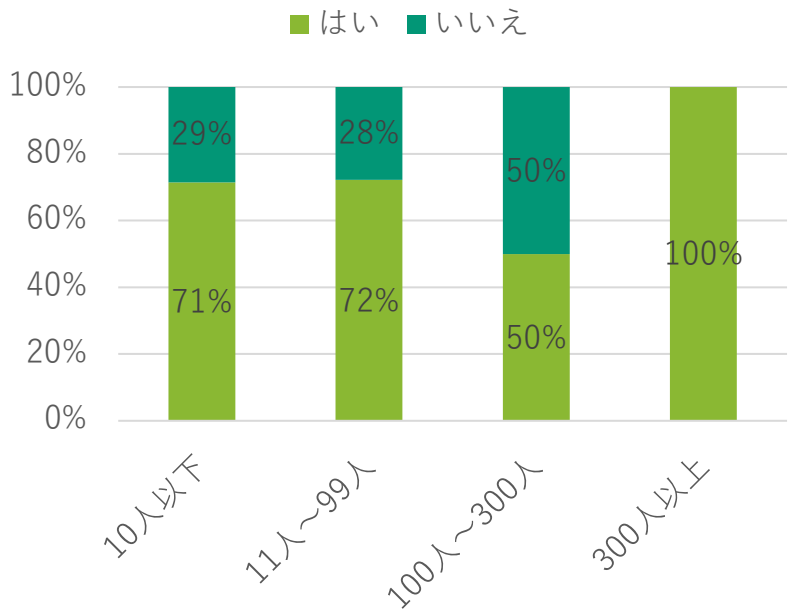
- 仮に組織種別と従業員数それぞれの観点から分析を行っても、有意な差を識別することが難しいため、今回の本レポートでは、従業員数の着観点からアンケート結果を分析することとする。

- 母集団は、従業員数不明回答(1件）を除いた、**32件のサンプル**となる。なお、設問によっては、これ以外の無回答のサンプルが一部含まれているため、各結果別に示している。

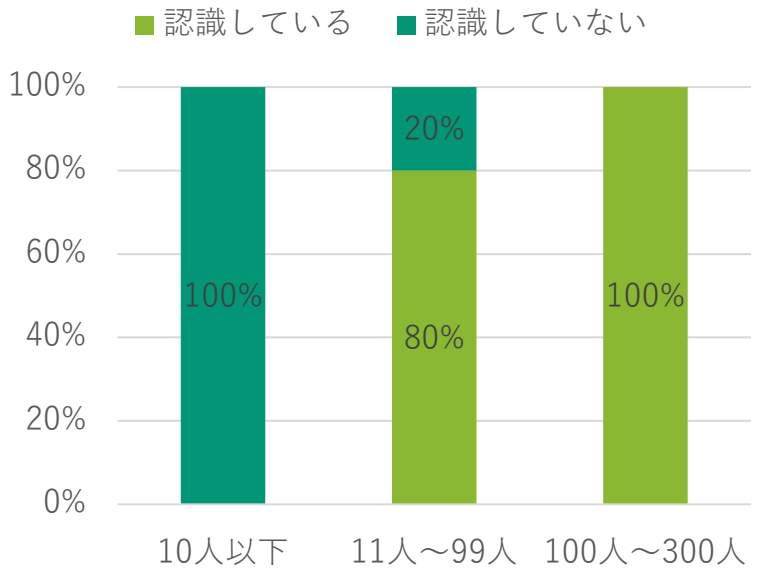
＜３．アンケート調査結果_従業員数別結果(1/4)＞

【１．ガイドラインへの対応・認識状況】

＜1-1：2省GLへの対応状況＞　※n=30
（無回答2件除く）



＜1-2：1.1が＜いいえ＞の場合の２省GLの存在の認識有無＞　※n= 8
（無回答1件除く）



＜1-３：1.２が＜はい＞（認識している）の場合の未対応理由（複数回答）＞　※n=5

理由	11人～９９人	１００人～３００人
依頼元の医療機関から2省ガイドラインの対応を求められなかったため	１件	１件
対応のコスト・リソースが確保できないため	１件	-
対応の必要がないと考えていたため	１件	-
それ以外の理由	１件	-

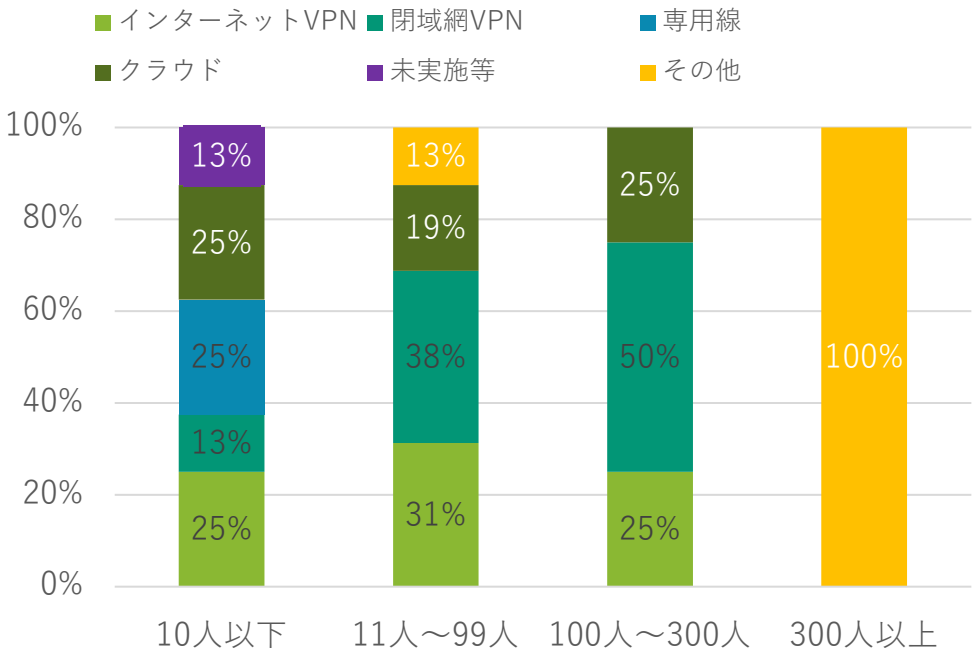
※10人以下、及び300人以上の該当データはなし

相対的に**規模の小さい組織体ほど、GLへの対応状況、ひいてはGLの認識率も低くなる**傾向が見受けられる。

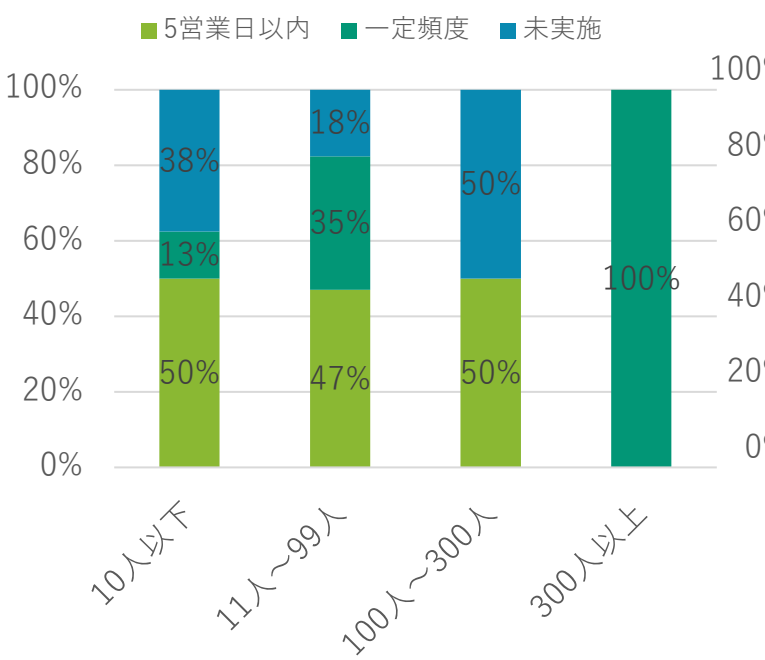
＜３．アンケート調査結果_従業員数別結果(2/4)＞

【２．自社内部のセキュリティ対応状況】

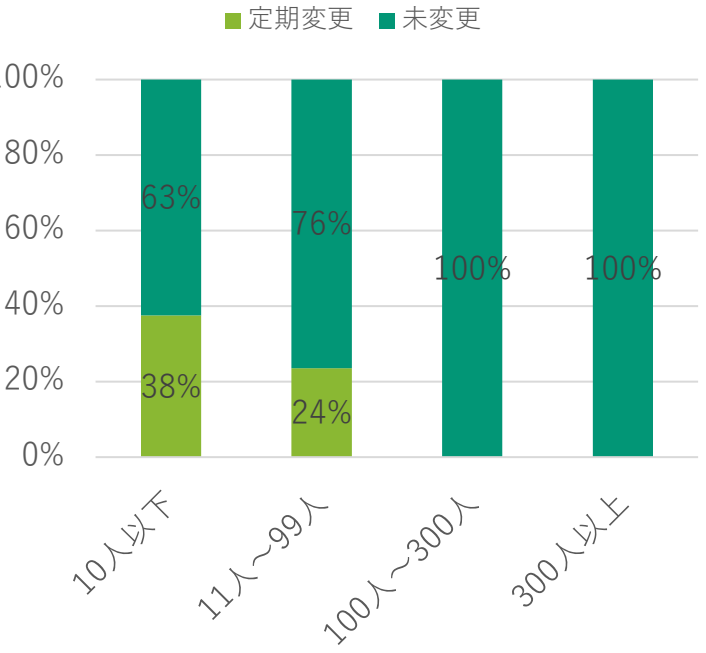
＜２-１：医療機関とデータ授受する場合のネットワークセキュリティ＞ ※n=29 (無回答3件除く)



＜２-２：対医療機関接続用のNW機器のパッチ適用＞ ※n=30 (無回答2件除く)



＜２-３：対医療機関接続用のNW機器のログインPWの定期変更＞ ※n=30 (無回答2件除く)



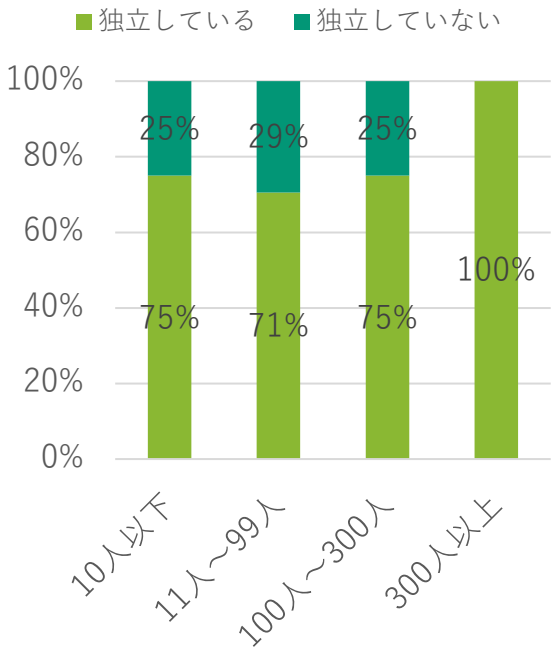
従業員数の多い組織体ほどネットワークセキュリティの選択肢が洗練され、特定の方式へ収れんする傾向がある。
医療機関と接続するためのNW機器については(一部例外を除き）半数の割合が適時に実施しているが、**規模の小さな組織体のほうがログインPWの定期変更率が高いという逆説的な傾向**が見受けられる。

＜３．アンケート調査結果_従業員数別結果(3/4)＞

＜2-4：画像診断環境/業務ネットワーク間の独立性＞

※n=30

(無回答2件除く)



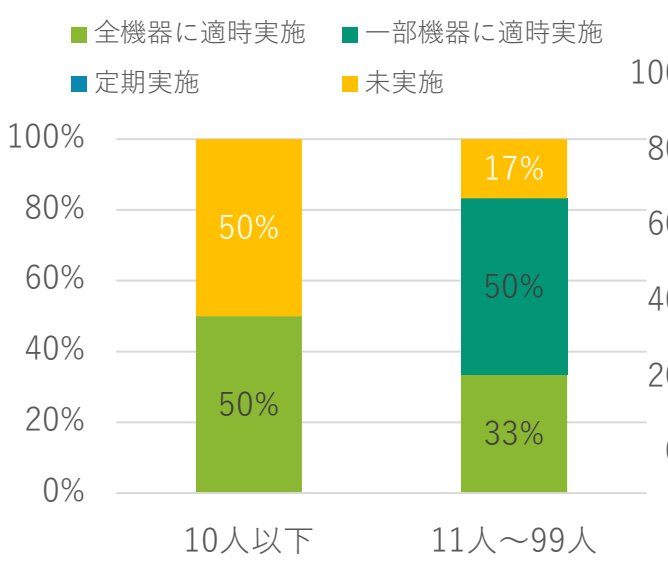
＜2-5：業務NWから独立した画像診断環境におけるセキュリティ実施有無＞

※n=22

＜2-6：画像診断環境と独立していない業務NWが外部接続する機器におけるセキュリティパッチ対応状況＞

※n=8

(無回答1件除く)



※100人～300人、300人以上の該当データはなし

＜2-7：二次感染被害対策の実施有無＞

※n=29

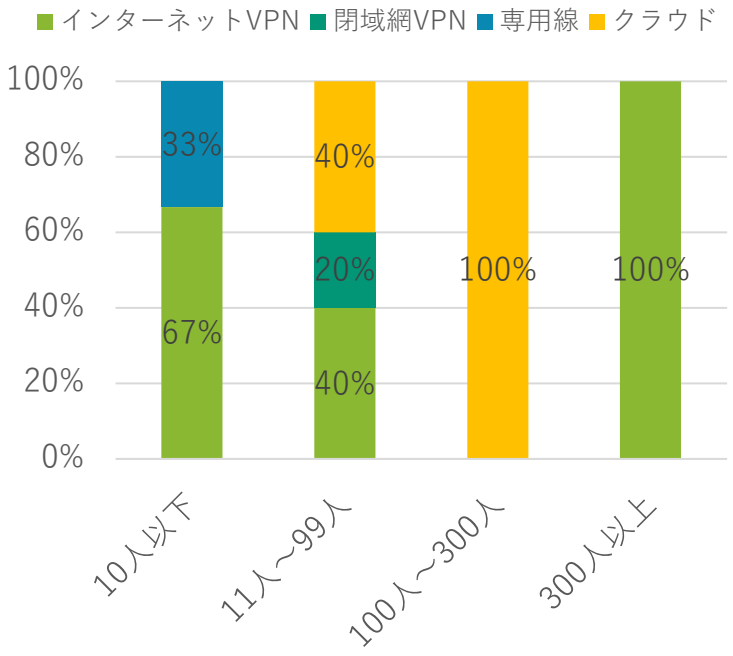
(無回答3件除く)

業務ネットワークから独立した画像診断環境を有する組織体はいずれの規模でもセキュリティ対策を講じているが、一方で**業務NWと接続した診断環境を有する組織体ではインターネット等との接続機器に係るパッチ適用を適時に行えていないケース**が見受けられる。
なお、**接続先からの二次感染被害対策は規模が小さいほど未実施率が高く**なっている

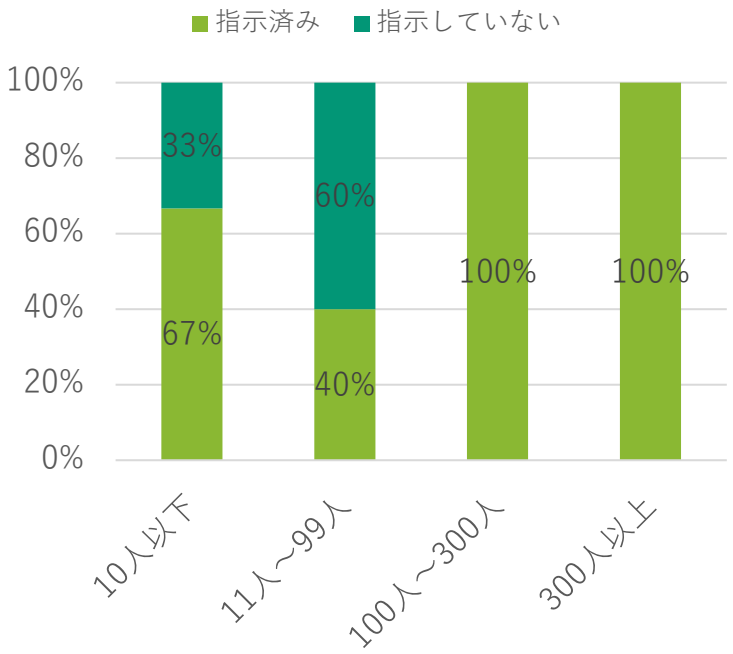
＜３．アンケート調査結果_従業員数別結果(4/4)＞

【３．自社サービスサプライチェーン上のセキュリティ管理状況】

＜3-1：外部とデータ授受する場合のネットワークセキュリティ＞　※n=10



＜3-2：業務委託先へのセキュリティ依頼事項の指示有無＞　※n=10



＜3-3：3-2が「指示していない」の場合の理由＞（複数回答）　※n=4

理由	10人以下	11人～99人
クラウド業者を含む委託先が実施しているため	1件	2件
特段の理由はない	-	1件

※100人～300人/300人以上の該当データはなし

1対N型の多数間モデルを採用する組織体はいずれも然るべきネットワークセキュリティを実施しているが、**100人以下の規模の場合、委託先へのセキュリティ実施事項の依頼率は低い状況**である。なお、その理由の多くは委託先が実施しているはずという楽観に依拠しており、その意味でリスクを抱えているといえる。

４．サービスモデル別

＜４．サービスモデル別総評＞

- 1対1型（モデル1)/1対N型(モデル2)ともに、**GLへの対応状況/認識率ともにほぼ同水準**であり、大きな差異はない。

- さらに、両モデル共にネットワークセキュリティは相応に実施しており、**医療機関接続用のNW機器のパッチ適用率、ログインPW定期変更率もほぼ同水準**である。

- 接続先からの二次感染対策率は両モデルとも同程度である。

- 一方で、**1対1型（モデル１）は画像診断環境/業務NWの分離率は相対的に低いが、業務NWから独立した環境のセキュリティ実施率自体は高い**状況である。
- さらに、未分離環境における業務NWがインターネット等、外部ネットワークと接続するための**機器のセキュリティパッチ適用頻度も高く、1対N型よりもセキュアな取組が実施されている可能性**が見受けられる。

- **1対N型（モデル２）の場合、セキュリティ対応事項の調整等が接続先との様々なIT環境要因によって個々に変動することもあり、それが上記の結果に表れていると想定できる。**

＜４．前提＞

- 今回の調査項目のカテゴリーである【No１．ガイドラインへの対応・認識状況】、【No２．自社内部のセキュリティ対応状況】、【No３．自社サービスサプライチェーン上のセキュリティ管理状況】のうち、【No3】はサービス提供モデル２：病院（委託元）/事業者（委託先）/事業者委託先（再委託先）の多数間モデルを提供する事業体のみの設問としている。サービス提供モデル２に係るNo3の管理状況についての分析は、前頁に記載の全体結果/従業員数別結果にてすでに実施しているため、本章では割愛する。

- 上記の前提のもと、次頁以降の分析内容は、サービス提供モデル別の、【No1】/【No２】の調査項目カテゴリーを対象とする。

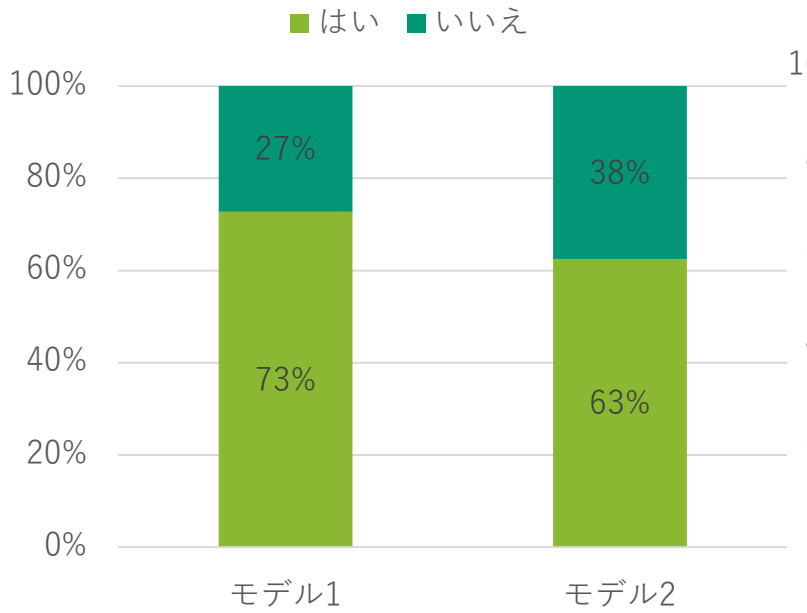
- サービス提供モデル未回答(1件）を除いた、**32件のサンプルが母集団全体**となる。なお、設問によっては、これ以外の無回答のサンプルが一部含まれているため、各結果別に示している。

＜４．アンケート調査結果_サービスモデル別結果(1/3)＞

【１．ガイドラインへの対応・認識状況】

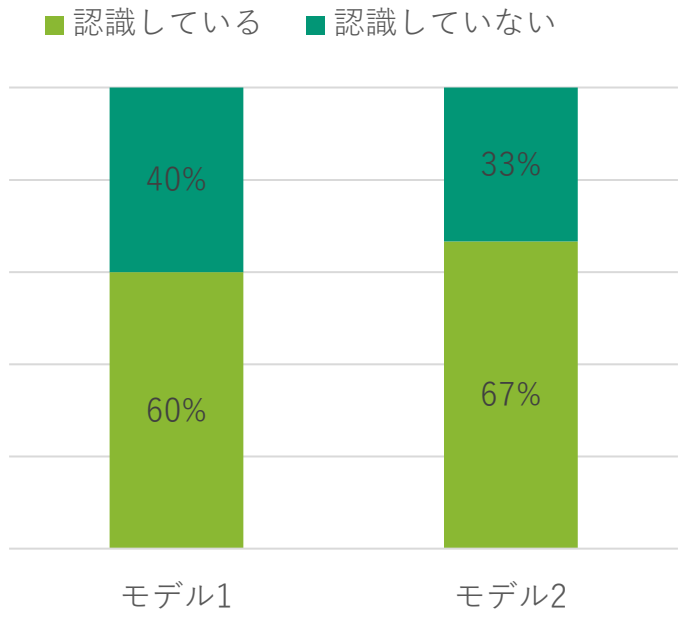
＜1-1：2省GLへの対応状況＞　※n=30

（無回答2件除く）



＜1-2：1.1が＜いいえ＞の場合の２省GLの存在の認識有無＞　※n= 8

（無回答1件除く）



＜1-３：1.２が＜はい＞（認識している）の場合の未対応理由（複数回答）＞　※n=5

理由	モデル1	モデル２
依頼元の医療機関から2省ガイドラインの対応を求められなかったため	１件	１件
対応のコスト・リソースが確保できないため	１件	-
対応の必要がないと考えていたため	１件	-
それ以外の理由	-	1件

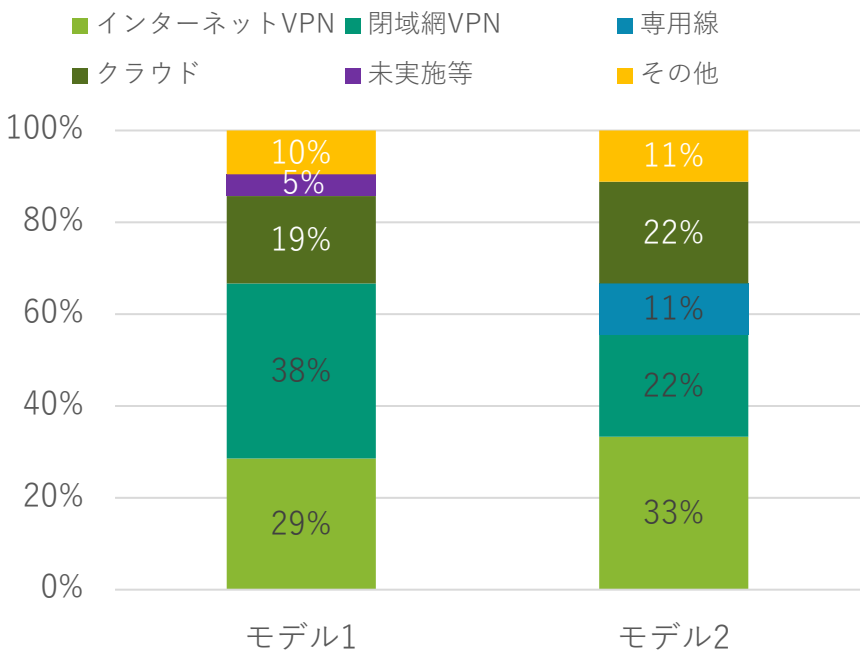
※10人以下/300人以上の該当データはなし

1対1型（モデル1)/1対N型(モデル2)ともに、GLへの対応状況/認識率ともにほぼ同水準であり、大きな差異はない。

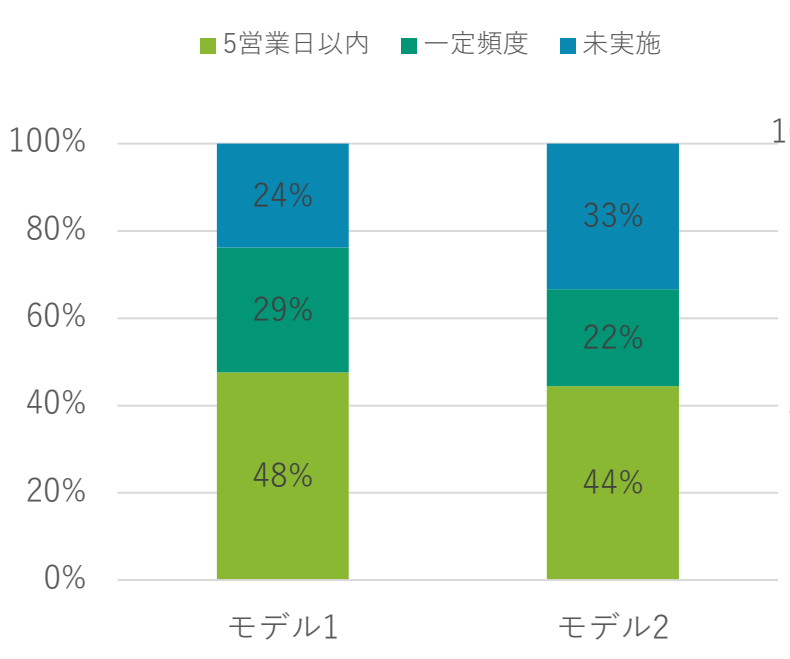
＜４．アンケート調査結果_サービスモデル別結果(2/3)＞

【２．自社内部のセキュリティ対応状況】

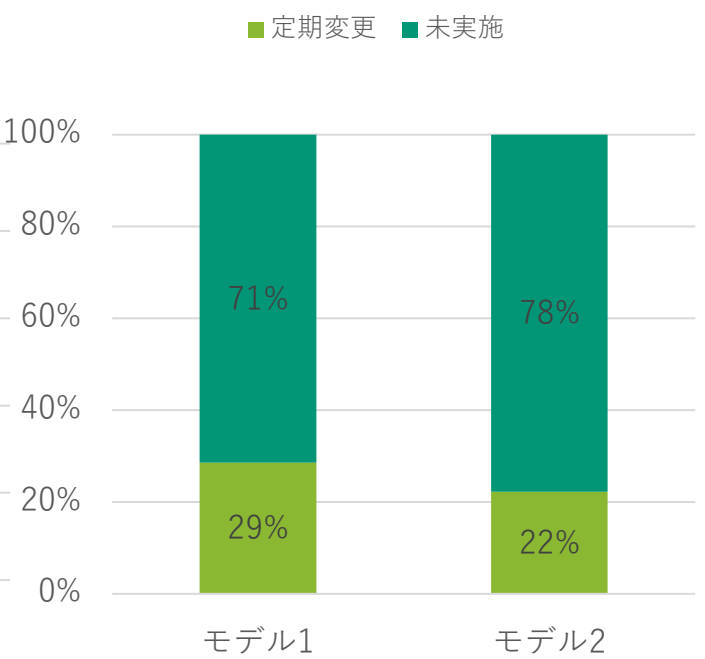
＜２-１：医療機関とデータ授受する場合のネットワークセキュリティ＞ ※n=29 (無回答3件除く)



＜２-２：対医療機関接続用のNW機器のパッチ適用＞ ※n=30 (無回答2件除く)



＜２-３：対医療機関接続用のNW機器のログインPWの定期変更＞ ※n=30 (無回答2件除く)



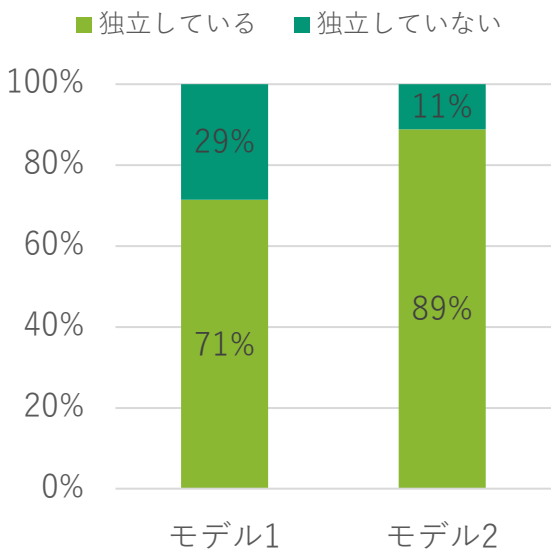
両モデル共にネットワークセキュリティは相応に実施しており、
医療機関接続用のNW機器のパッチ適用率、ログインPW定期変更率もほぼ同水準である。

＜４．アンケート調査結果_サービスモデル別結果(3/3)＞

＜2-4：画像診断環境/業務ネットワーク間の独立性＞

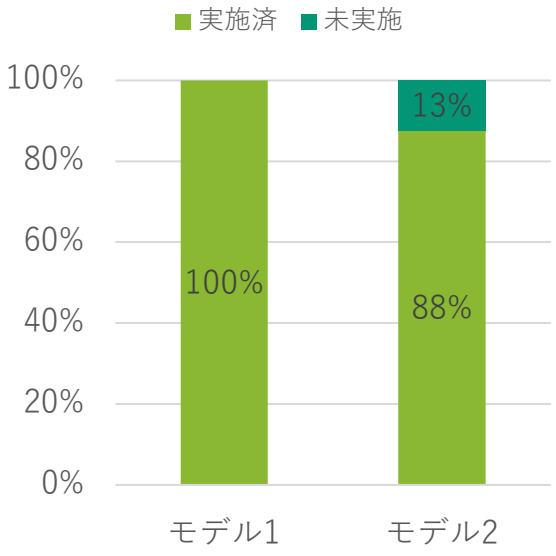
※n=30

(無回答2件除く)



＜2-5：業務NWから独立した画像診断環境におけるセキュリティ実施有無＞

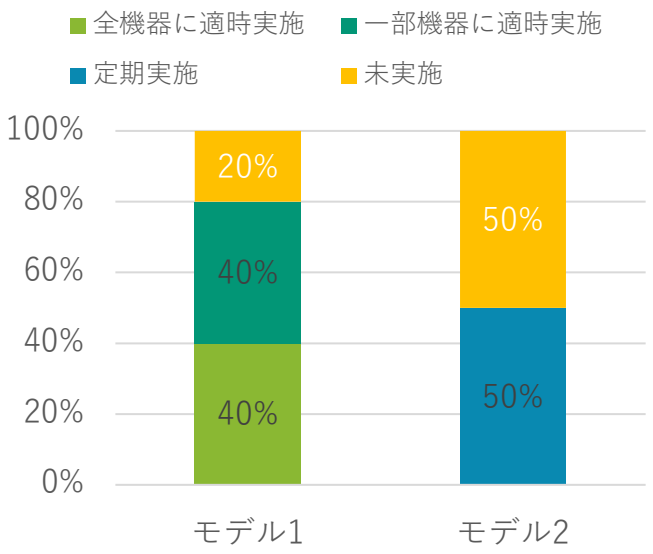
※n=22



＜2-6：画像診断環境と独立していない業務NWが外部接続する機器におけるセキュリティパッチ対応状況＞

※n=8

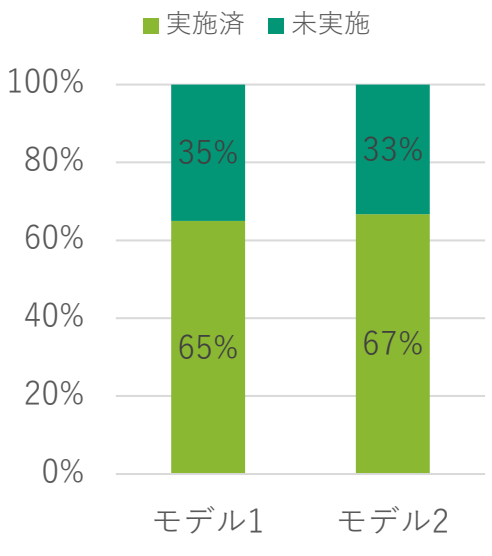
(無回答1件除く)



＜2-7：二次感染被害対策の実施有無＞

※n=29

(無回答3件除く)



接続先からの二次感染対策率は両モデルとも同程度である。
一方で、**1対1型（モデル１）は画像診断環境/業務NWの分離率は相対的に低いが、業務NWから独立した環境のセキュリティ実施率は高い**。さらに、未分離環境における業務NWが外部ネットワークと接続するための**機器のセキュリティパッチ適用頻度も高く、1対N型よりもセキュアな取組が実施されている可能性**が見受けられる。


Medical Information
Sharing and Analysis Center