歯科ITベンダ向け
セキュリティアンケート分析結果

2024年1月

目次

1．調査概要

1．調査概要～目的・背景

（一社）医療ISACでは、医療機関、介護施設、薬局、健診施設等、国内の医療サービスを提供する組織を対象としたセキュリティアンケート調査を様々に実施しており、その結果を公表してきました。

一方、医療サービスの提供組織が利用する医療情報システムの大半は、医療情報システム・サービスを提供する外部のIT事業者により担われています。

当法人のセキュリティアンケートでも、医療情報システム・サービスの開発・運用を外部委託しているIT事業者に対して、医療サービスの提供組織が委託元としての責任の観点でどのようなセキュリティ管理を行っているかについては調査は行ってきましたが、実際に該当する各種事業者の具体的なセキュリティへの取り組みを正面から調査することは少ない状況でした。

国内医療分野のセキュリティ実態を正確に把握するためには、IT事業者によるセキュリティへの取組状況を理解することも重要です。

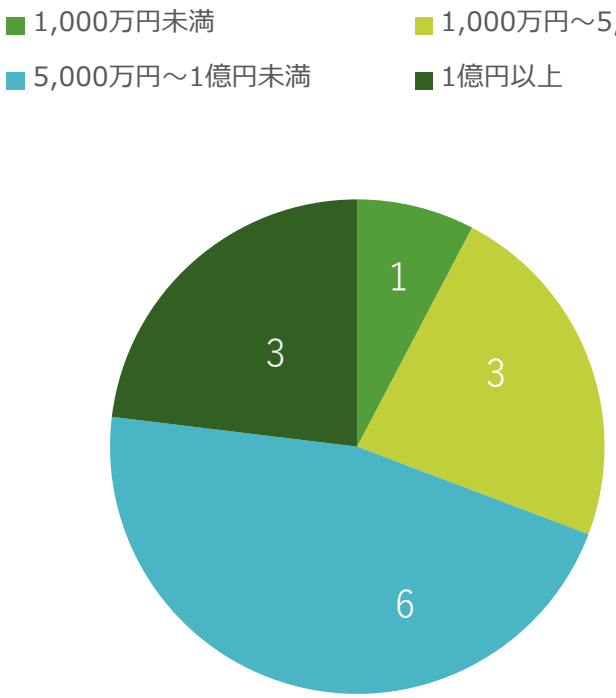
本レポートは、上記の目的・背景のもと、歯科系の医療機関・クリニック（以下、『歯科施設』）に対して、医療情報システム・サービスを提供するIT事業者（以下、『歯科ITベンダ』）を対象に、セキュリティアンケートを実施し、その結果を分析・整理したものとなります。

1．調査概要～アンケート調査/分析対象

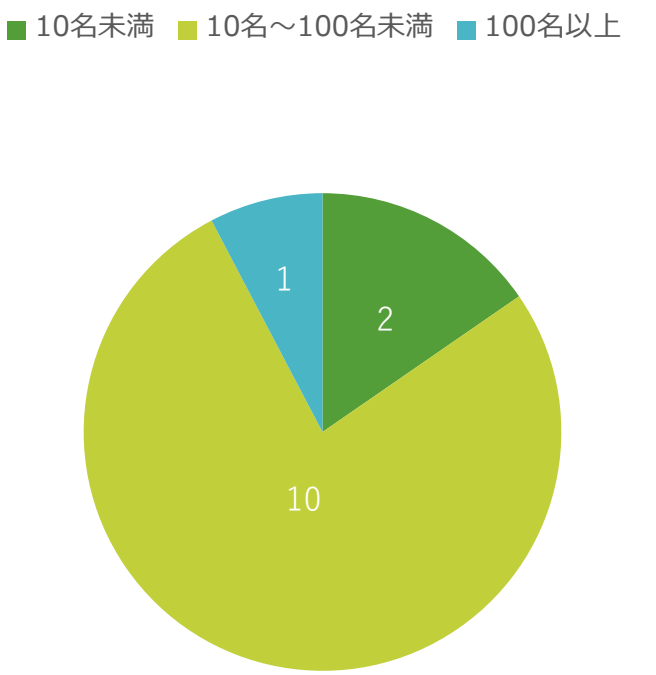
- アンケート調査期間：２０２３年１１月～１２月
- アンケート回答組織数：２３件

- **分析対象：歯科施設の院内ネットワーク環境とオンライン接続を行っている医療情報システム・サービスを提供する歯科ITベンダ**
- **分析対象とした組織数：１３件**

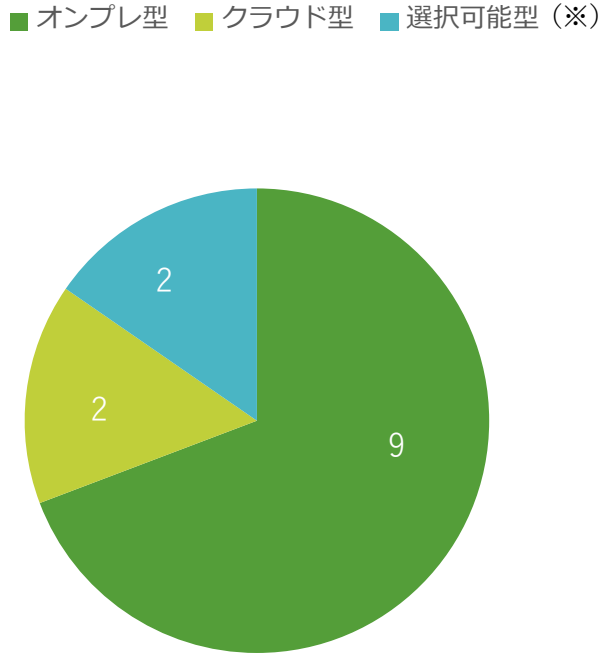
<資本金別>



<医療システム等を開発、運用・保守する従業員数（目安）別>



<システム提供方式>



※：選択可能型＝ユーザがオンプレ・クラウドの方式を選択可能なシステム提供方式を指す

1．調査概要～アンケート項目(1/6)

調査に際したアンケート項目は以下の通り。

カテゴリ	アンケート項目		回答項目
1．ガイドラインへの対応・認識状況	(1)	歯科向け医療システム提供事業者として、以下のガイドライン・ガイダンス、あるいはそれに類する公知の基準を考慮された上で、自社のシステム、およびサービスにおけるセキュリティ対応を実施されていますか？ ・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】 ・個人情報保護委員会／厚生労働省【医療・介護関係事業者における個人情報の適切な取り扱いのためのガイダンス】	□ はい　□ いいえ（「不明」含む） *※回答が「はい」の場合は2の設問、「いいえ」の場合はNo.1-(2)に進んでください*
	(2)	歯科向け医療システム提供事業者として、特に公知のガイドライン・ガイダンス等を参考にしたセキュリティ対策を実施していない理由のなかで、該当するものをすべてご回答ください。（複数回答可能）	□ 歯科向け医療システム提供事業者としてそうした取り組みは特に必要ないと考えていたため（認識上の課題） □ 対応のコスト・リソースが確保できないため（リソース上の課題） □ 依頼元の医療機関からセキュリティ対応を求められなかったため（先方との関係性） □ それ以外の理由　（自由記述）

1．調査概要～アンケート項目(2/6)

カテゴリ	アンケート項目		回答項目
2．事業者としてのシステム・サービスセキュリティへの取組	**ネットワークセキュリティ管理状況**		
	(1)	貴社では歯科向け医療システムを提供する場合、委託元の歯科施設との間で、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　（自由記述）
	(2)	委託元の歯科施設とオンライン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、自社として、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） *※回答が「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」「特に実施していない（「わからない」を含む）」の場合、2-(4)に進んでください。* *「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 」の場合、2-(3)に進んでください。*
	(3)	*2-(2)で「一定の頻度で情報収集し実施している」を選択された方に伺います。* どのくらいの頻度で情報収集されていますか？	□ ほぼ毎月行う □ 四半期に1回行う □ 半年に1回行う □ 1年に1回行う □その他（自由記述）

1．調査概要～アンケート項目(3/6)

カテゴリ	アンケート項目		回答項目
２．事業者としてのシステム・サービスセキュリティへの取組	(4)	委託元の歯科施設とオンライン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） *※回答が「変更している」の場合、2-(5)、「変更していない（わからないを含む）」の場合、2-(6)に進んでください。*
	(5)	*2-(4)で「変更している」と回答した方に伺います。* どのくらいの頻度でログインパスワードを変更されていますか？	□ ほぼ毎月行う □ 四半期に1回行う □ 半年に1回行う □ 1年に1回行う □その他（自由記述）
	サプライチェーンリスク管理		
	(6)	歯科施設と貴社間で歯科向け医療システムに係るやり取り（遠隔保守等のサービスを含む）を行う際の企業内部のIT環境（歯科施設向けサービス提供環境）は、その他の業務ネットワークから独立していますか？	□　している □　していない（わからないを含む） *※回答が「している」の場合、2-(7)、「していない（わからないを含む）」の場合、2-(8)に進んでください。*

1．調査概要～アンケート項目(4/6)

カテゴリ	アンケート項目		回答項目
2．事業者としてのシステム・サービスセキュリティへの取組	(7)	*2-(6)で「している」と回答した方に伺います。* 社内の業務ネットワークから独立した、歯科施設向けサービス提供環境には、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（わからないを含む）
	(8)	*2-(6)で「していない（不明）」と回答した方に伺います。* 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 *※回答が「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」の場合、2-(9)、それ以外は2-(10)へ進んでください。*

1．調査概要～アンケート項目(5/6)

カテゴリ	アンケート項目		回答項目
2．事業者としてのシステム・サービスセキュリティへの取組	(9)	*2-(8)で「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」と回答した方に伺います。* どのくらいの頻度で情報収集/適用されていますか？	□ ほぼ毎月行う □ 四半期に1回行う □ 半年に1回行う □ 1年に1回行う □その他（自由記述）
	(10)	歯科施設向けサービス提供環境とネットワークで接続する歯科施設側でマルウェア感染等が発生した場合、貴社のサービス提供環境に対して仮にネットワークを介した二次感染が発生するシナリオを予防／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 □　実施していない（わからないを含む） *※回答が「実施している」の場合、2-(11)に進んでください。それ以外は2-(12)に進んでください。*
	(11)	*2-(10)で「実施している」と回答した方に伺います。* 二次感染を予防／検知するために実施しているセキュリティ対策は何ですか？概要をご記入ください	*（自由記述型）*

1．調査概要～アンケート項目(6/6)

カテゴリ	アンケート項目		回答項目
２．事業者としてのシステム・サービスセキュリティへの取組	**リスクコミュニケーションの取組**		
	(12)	歯科向け医療システム提供事業者として、歯科施設との間でセキュリティ面の責任分界を明確に定義し、歯科施設が自社サービスを利用する上で行うべきセキュリティ対策の合意形成が図られることは、歯科施設/サービス事業者双方が為すべきセキュリティ範囲を明確化する上で重要となります。 こうした考え方は経済産業省・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」が求めるアプローチですが、こうしたアプローチは貴社で検討・実施されていますか？	□ している □ していない
3.その他	(1)	貴社ではサイバーセキュリティ保険に加入していますか？	□ している □ していない

２．総評

２．総評(1/2)

- 今回の分析対象となる歯科ITベンダ（１３件）のうち、７割近くは２省GL、個人情報保護ガイダンス等を考慮したセキュリティ対応を進めているものの、**３割強は特にコスト・リソース面の課題によって、対応が十分に行えていない状況**が示されている。
- なお、セキュリティ対応を進めていると回答した歯科ITベンダの中の**３割近くは２省GLが求めるリスクコミュニケーションに着手できていない**との回答が見受けられており、国内医療分野固有のセキュリティへの配慮が一部の歯科ITベンダには十分に浸透していない状況がみられる。

- 歯科ITベンダが歯科施設とオンライン接続するためのネットワーク機器に５営業日以内にセキュリティパッチを適用する割合は全体で２割前後、重要度が高いパッチが配布された場合は適用すると回答した割合も２割前後にとどまっている。そのため、**６割近くの歯科ITベンダでは脆弱性情報の公開から対応までの期間における攻撃リスクが相対的に高い傾向**にあるといえる。

- 加えて、該当するネットワーク機器の認証情報、つまり**ログインパスワードの変更を定期的に行っている歯科ITベンダは２割弱**であり、その頻度自体も決して高いとは言えない状況である。そのため、歯科ITベンダにおいては、対歯科施設とのネットワーク機器の脆弱性パッチが適用されたとしても、**仮に脆弱性公表から早期の攻撃により、パッチ適用前の時点でログイン情報が漏洩するリスクシナリオを想定した場合、十分な対応が行えているとは言い難い**状況である。

- 自社業務と歯科施設向け業務のネットワーク環境を独立させている歯科ITベンダのうち、**独立したセキュリティ対策の施策を講じているケースは８割近くに及んでいる**。一方、ネットワーク環境を独立させていない歯科ITベンダのうち、６割弱は自社業務環境におけるネットワーク機器へのパッチ適用は一定頻度と回答があった。その中でも適用頻度が低い組織は**相対的に業務環境から歯科施設向け環境へのマルウェア感染リスク、つまりサプライチェーンリスクが高い状況にあると想定される。**

- 歯科施設側のマルウェア感染による自社のサービス環境が二次感染を受けるリスクに対する対策の実施率は５割強であり、**未実施の４割強の歯科ITベンダにおいては医療機関からの二次感染リスクが相対的に高い**状況にあると考えられる。

（次頁に続く）

２．総評(2/2)

（前頁から続く）

- **２省GLが事業者に求めるリスクコミュニケーションの取組率は４割強**に留まっており、歯科施設/歯科ITベンダ間のセキュリティに関する責任共有の取組はまだ途上にある。

- なお、サイバー保険の加入率自体は、医療ISACが他組織と共同で実施した様々な分析結果と比べて、**一定の高い割合**を示している。特に対歯科施設向けサービス提供環境と自社のその他業務環境を分離していない組織、または歯科施設からオンライン経由でマルウェアに二次感染するリスクへの対策が未実施と回答した組織の半数近くがサイバー保険に加入しており、**技術的な未然防止対策でなく、サイバー保険による事後的な損失対応を見込んだリスク移転が図られている**とも考えられる。

- 総合すると、今回の調査対象とした歯科ITベンダでは、２省GLが求めるリスクマネジメントの一環としての**ネットワークセキュリティ、ひいては複数施設へサービス提供を行うための対歯科施設向け業務環境を取り巻くサプライチェーンリスクへの取組状況にバラつきがかなりある**ことが示されている。合理的/適切な対策を講じるものもあれば、そうでないものも散見されている。
- 医科/歯科/調剤は国内では大きく「医療」分野とまとめられるが、そのシステム/セキュリティ管理の成熟度には隔たりがあるため、**国内の歯科IT向けに適した等身大の合理的な対策検討のスキーム**こそが求められる。よって、サイバーセキュリティという、**歯科ITベンダから見れば、ある種の＜非競争領域＞についての情報収集・共有を図る仕組み**を設けることで、**歯科IT業界全体のセキュリティの底上げを図ること**が一案として考えられる。

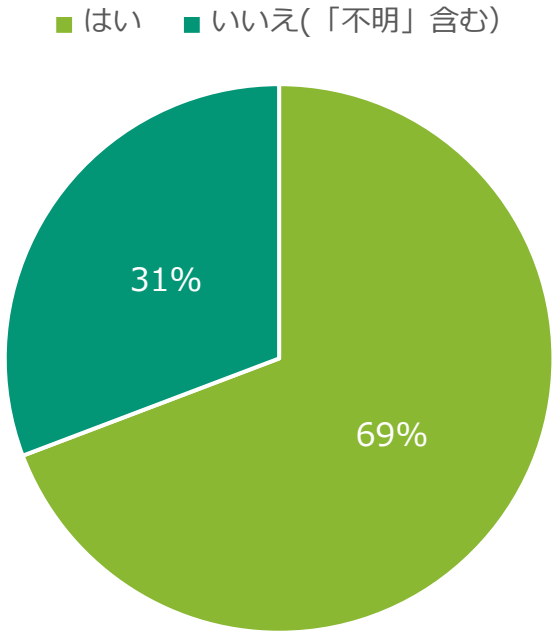
- また、今回の調査項目に直接的には含めていないが、常に高度化/巧妙化するサイバー攻撃の被害を明日にでも自社が受けるかもしれないというリスクシナリオに立った場合、サイバー攻撃を水際で防御し続ける『未然防止策』への投資には限界がある。今後は『**復旧・拡大防止策**』、つまり**早急にサイバー被害から復旧し、ステークホルダー（医療機関/患者）へのダメージ率を最小限化するためのBCPへの注力こそが重要になる**ため、その点についても歯科IT業界全体でナレッジシェアを図っていくことが望ましいといえる。

3．調査結果

3．調査結果(1/6)～２省GL等への対応

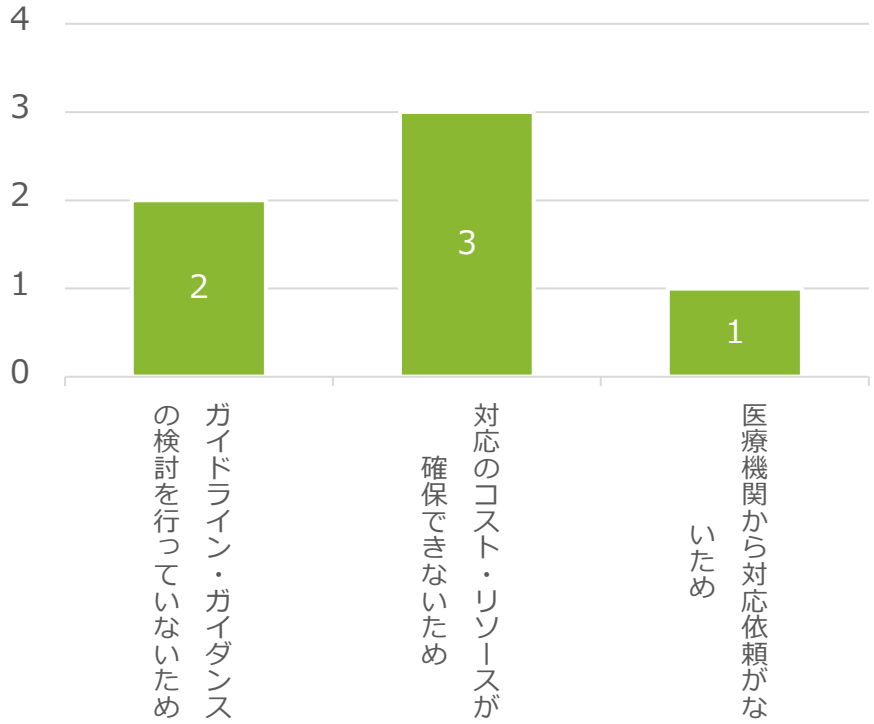
【１．ガイドライン等への対応・認識状況】

<1-(1)：2省GLや個人情報保護ガイダンス等への対応状況>　※n=13



<1-(２)：1-(1)が<いいえ(不明含む）>の場合の理由（複数回答）>

※n=4

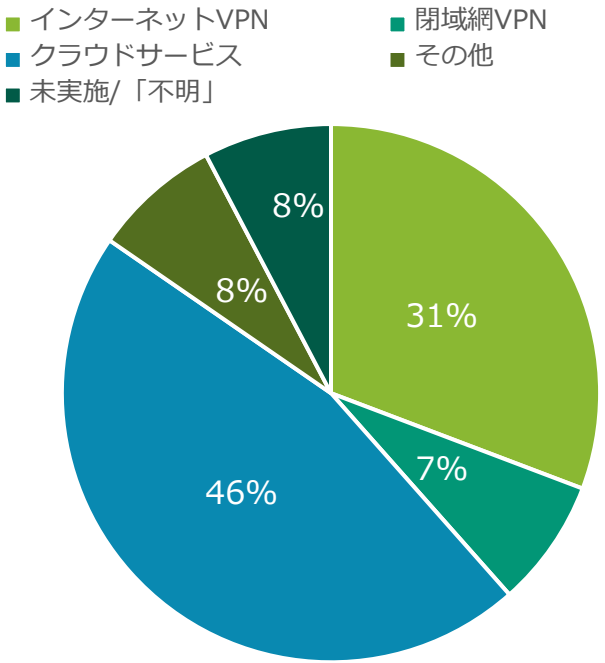


歯科ITベンダの**7割近くが2省GL等のデータコンプライアンスへの対応**を進めているものの、
３割程度は主にコスト・リソース面の課題によって、対応が十分に行えていない状況が示されている。

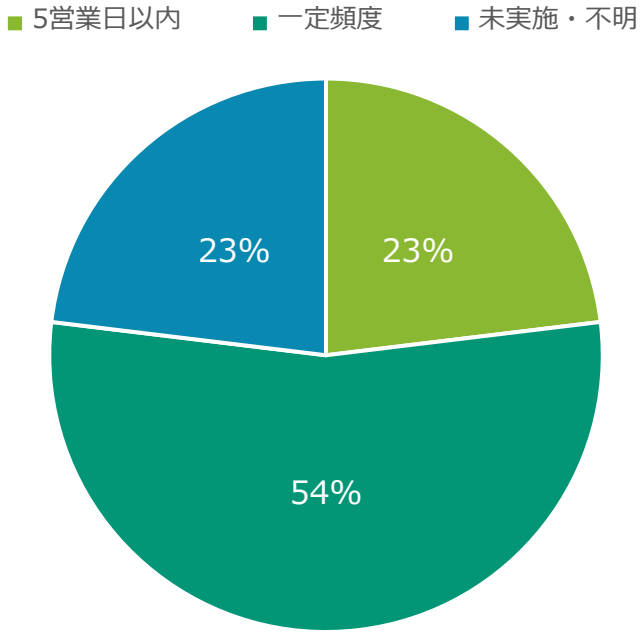
3．調査結果(2/6)～ネットワーク機器のセキュリティ管理

【2．事業者としてのシステム・サービスセキュリティへの取組】

＜2-(1)：歯科施設とデータ授受する場合のネットワークセキュリティ＞ ※n=13



＜2-(2)：対歯科施設接続用の自社NW機器のパッチ適用頻度＞ ※n=13



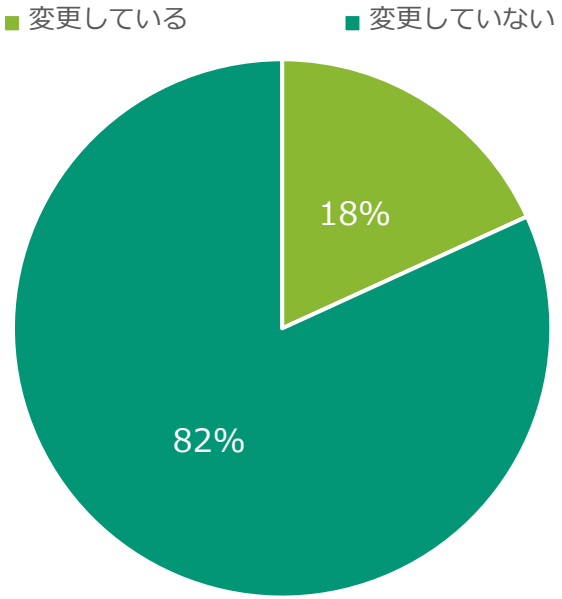
＜2-(3)：2-(2)のうち、一定頻度と回答した場合の、具体的な頻度＞ ※n=7

具体的な頻度	対象件数
ほぼ毎月行う	4件
重要/必要と自社判断した場合	3件

歯科ITベンダ/歯科施設間のデータ授受の方式のうち、5割弱が外部クラウド、３割程度がインターネットVPNによるセキュリティ対応を図っている。
データ授受を行うための自社ネットワーク機器に５営業日以内にセキュリティパッチを適用する割合は２割前後、重要度が高い場合は適用する割合も２割前後にとどまっているため、**６割近くの歯科ITベンダでは脆弱性情報の公開から対応までの期間における攻撃リスクが相対的に高い傾向**にあるといえる。

3．調査結果(3/6)～ネットワーク機器のセキュリティ管理

＜2-(4)：ネットワーク機器のログインPWの定期変更有無＞ ※n=13



＜2-(5)：定期変更実施率の割合＞

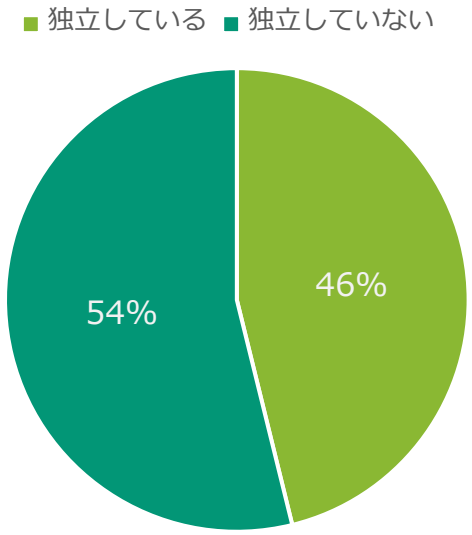
※n=2

定期変更頻度	対象件数
隔月で行う	1件
四半期に1回行う	1件

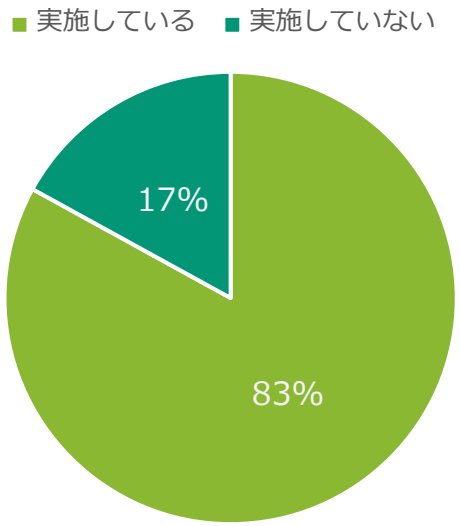
歯科施設との接続ポイントに係るネットワーク機器の認証情報、つまり**ログインパスワードの変更を定期的に行っている歯科ITベンダは２割弱であり**、さらにその頻度自体も決して高いとは言えない状況である。
そのため、歯科ITベンダにおいては、対歯科施設とのネットワーク機器の脆弱性パッチが適用されたとしても、**仮にゼロデイ攻撃により、パッチ適用前の時点でログイン情報が漏洩するリスクシナリオを想定した場合、十分なセキュリティ対応が行えているとは言い難い**状況である。

3．調査結果(4/6)～サプライチェーンリスク管理

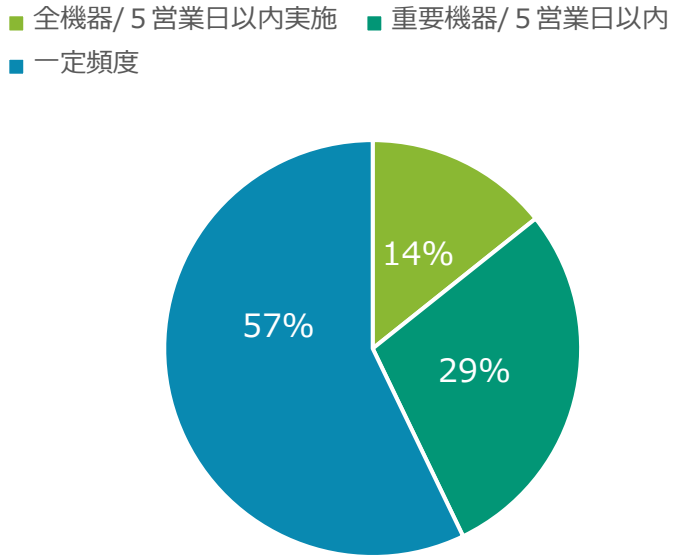
＜2-(6)：自社業務/歯科施設向け業務ネットワーク（NW)間の独立・分離＞ ※n=13



＜2-(7)：2-(6)が【独立している】の場合、業務NWから独立した歯科施設向けNW環境のセキュリティ実施有無＞ ※n= 6



＜2-(8)：＜2.6＞が【独立していない】の場合、業務NWにおいて外部との接続を行うためのNW機器のパッチ適用頻度＞ ※n= 7



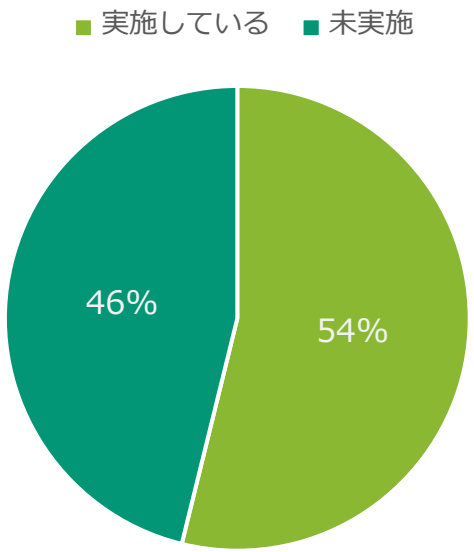
＜2-(9)：2-(8)で、一定頻度と回答した場合の、具体的な頻度＞ ※n=4

具体的な頻度	対象件数
ほぼ毎月行う	1件
重要/必要と自社判断した場合	2件
1年に１回行う	1件

自社業務と歯科施設向け業務のネットワーク環境を独立させている歯科ITベンダのうち、**独立したセキュリティ対策の施策を講じているケースは８割近くに及んでいる**。
一方、ネットワーク環境を独立させていない歯科ITベンダのうち、６割弱は自社業務環境におけるネットワーク機器へのパッチ適用は一定頻度と回答があり、その中でも頻度が低い歯科ITベンダは**相対的に業務環境から歯科施設向け環境へのマルウェア感染リスク、つまりサプライチェーンリスクが高いといえる。**

3．調査結果 (5/6)～サプライチェーンリスク管理

＜2-(10)：歯科施設側の感染に伴う、自社環境への二次感染被害対策の実施有無＞　※n=13



＜2-(11)：2-(10)が実施している」の場合の対策概要＞

※n=7

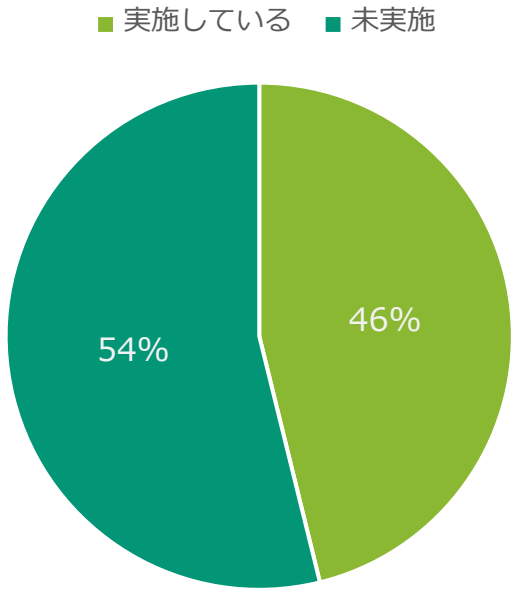
実施している対策概要	対象件数
ウイルス/脅威検出対策ソフト・サービスの導入	4件
ネットワークセキュリティ製品の導入	1件
ネットワーク機器による通信制御	1件
非公開	1件

歯科施設側のマルウェア感染による自社のサービス環境が二次感染を受けるリスクに対する対策の実施率は5割強だが、**<u>未実施の4割強の歯科ITベンダにおいては医療機関からの二次感染リスクが相対的に高い</u>**状況にある。なお、二次感染対策のうち、最も多いものはウイルス対策ソフト・サービスの導入であった。

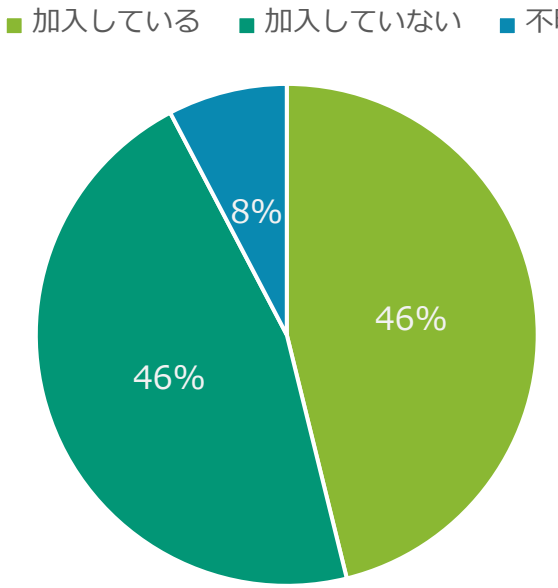
3．調査結果 (6/6)～リスクコミュニケーションの取組率等

【3．その他】

＜2-(12)：2省GLが求めるリスクコミュニケーションの実施有無＞　※n=13



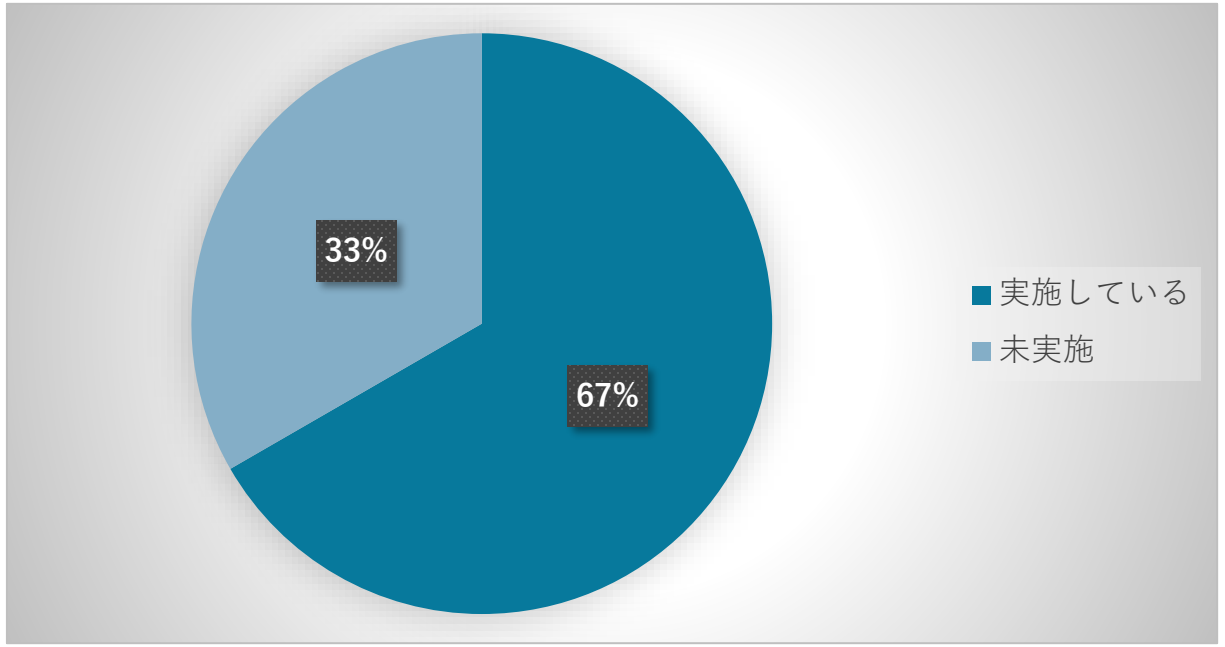
<3-(1)：サイバー保険加入有無>　※n=13



<u>2省GLが事業者に求めるリスクコミュニケーションの取組率は4割強</u>に留まっている。
なお、サイバー保険の加入率自体は、システム・サービスの提供先である医療サービスの提供主体（歯科系医療機関やクリニック等）と比較しても**<u>比較的高い割合</u>**を示している。なお、**<u>2-(10)で歯科施設をオンライン経由したマルウェアの二次感染被害対策が未実施と回答した歯科ITベンダの半数がサイバー保険に加入</u>**しており、技術的な未然防止対策でなく、サイバー保険による事後的な損失対応を見込んだリスク移転が図られている点は特徴的といえる。

（補足）特定の着眼点からの調査結果の補足(1/3)

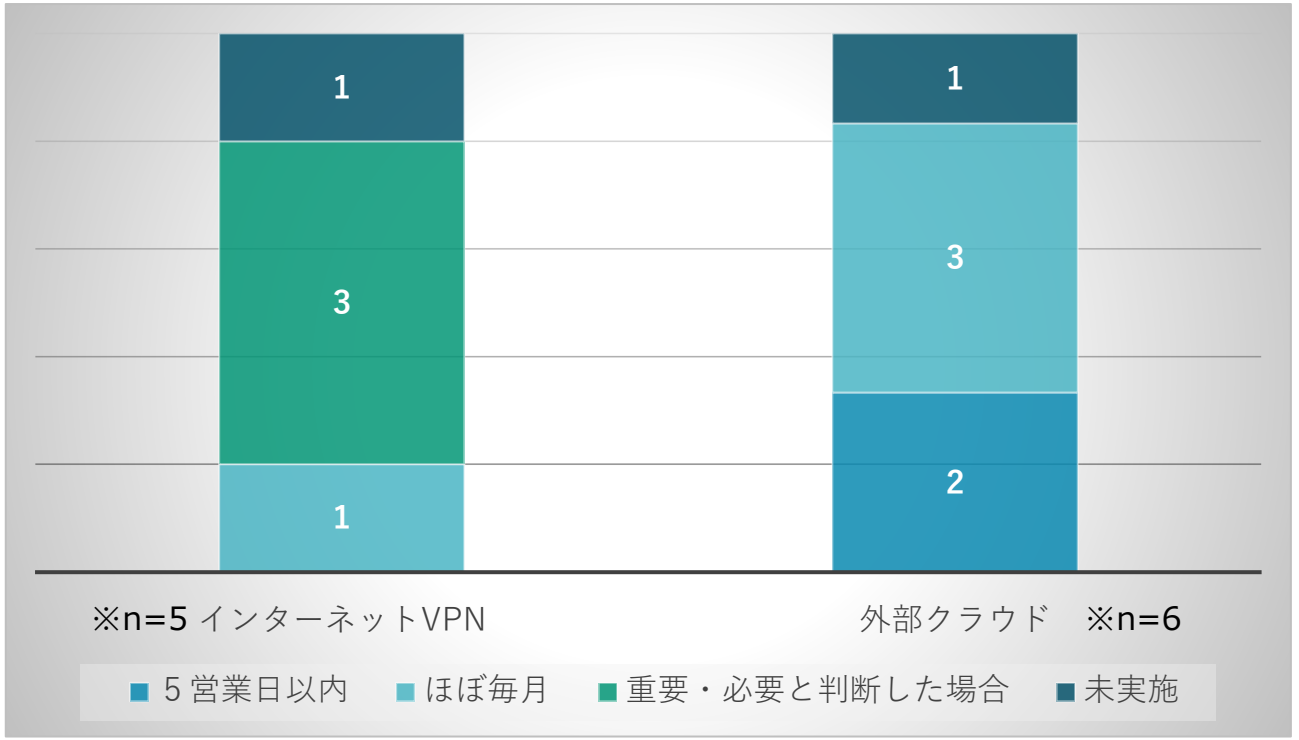
テーマ１	＜1-(1)：2省GLや個人情報保護ガイダンス等への対応状況＞で**「はい」**と回答した歯科ITベンダのうち、 ＜２-(12)：２省GLが求めるリスクコミュニケーションの実施有無＞で**「未実施」**と回答した組織の割合



必ずしも２省GLや個人情報保護ガイダンスを考慮したセキュリティ設計が行われていたとしても、一部の歯科ITベンダでは、**歯科施設がシステム・サービスを利用する際に、コンプライアンスとして事業者に求められる２省GLにおけるリスクコミュニケーションの必要性が十分に理解されていない**ことが示されている。

（補足）特定の着眼点からの調査結果の補足(2/3)

テーマ２	＜２-(1)：歯科施設とデータ授受する場合のネットワークセキュリティ＞で**「インターネットVPN」**（５件）、または**「外部クラウド」**（６件）と回答した組織における、＜２-(2)：対歯科施設接続用の自社NW機器のパッチ適用頻度＞の内訳

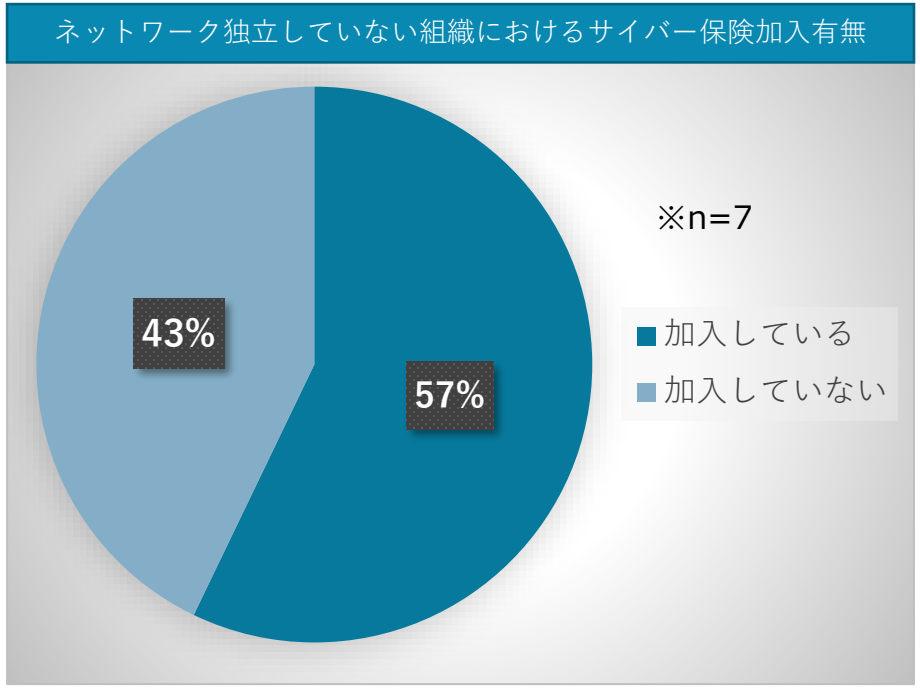


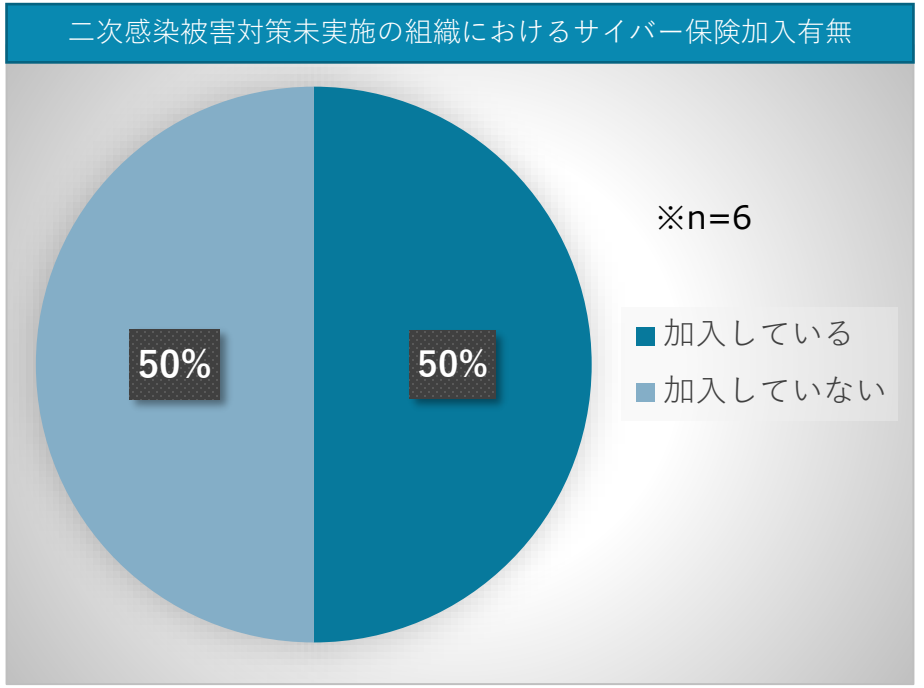
インターネットVPN型のITベンダより、**外部クラウドを用いてデータ授受を行う歯科ITベンダのほうが歯科施設とのネットワーク接続機器におけるセキュリティパッチ適用の実施率が相対的に高い**ことが示されている。

（補足）特定の着眼点からの調査結果の補足(3/3)

テーマ３

＜2-(6)：自社業務/歯科施設向け業務ネットワーク（NW)間の独立・分離＞で**「独立していない」**と回答した組織（７件）、及び＜2-(10)：歯科施設側の感染に伴う自社環境への二次感染被害対策の実施有無＞で**「実施していない」**と回答した組織（6件）における、＜3-(1)：サイバー保険加入有無＞の割合





対歯科施設向けのIT環境とその他自社業務環境をネットワーク独立させない組織、あるいは歯科施設からの二次感染被害対策を特に実施していない組織の**半分程度はサイバー保険に加入している**ことが示されている。


Medical Information
Sharing and Analysis Center