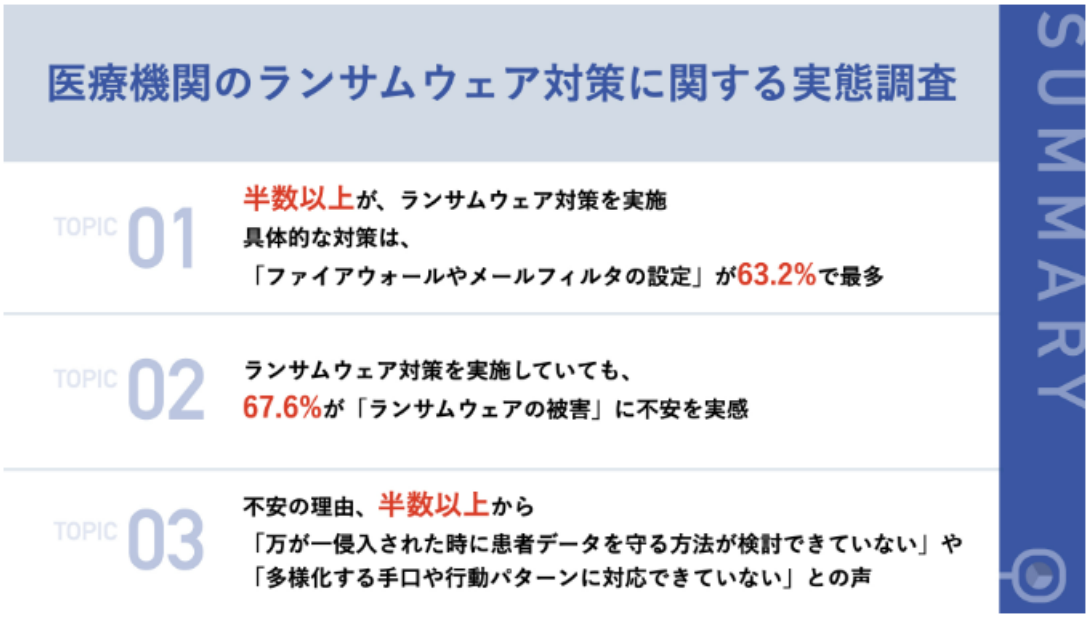
医療機関におけるランサムウェア対策への意識調査

54.3%が対策を実施、それでも約 7 割が「ランサムウェア被害」を不安視
～「病院としての信用が薄くなる」「患者の不安を煽ることになる」などの声～

東京、日本、2023 年 3 月 11 日 - ネットワーク監視ソフトウェア、ファイル共有・転送ソフトウェア等の販売およびサポートを行うプログレス・ソフトウェア・ジャパン株式会社（本社：東京都港区、代表取締役：ユファン・ステファニー・ワン）は、医療機関のネットワーク/システム管理に携わる方 105 名を対象に、医療機関のランサムウェア対策に関する実態調査を実施いたしましたので、お知らせいたします。

調査サマリー



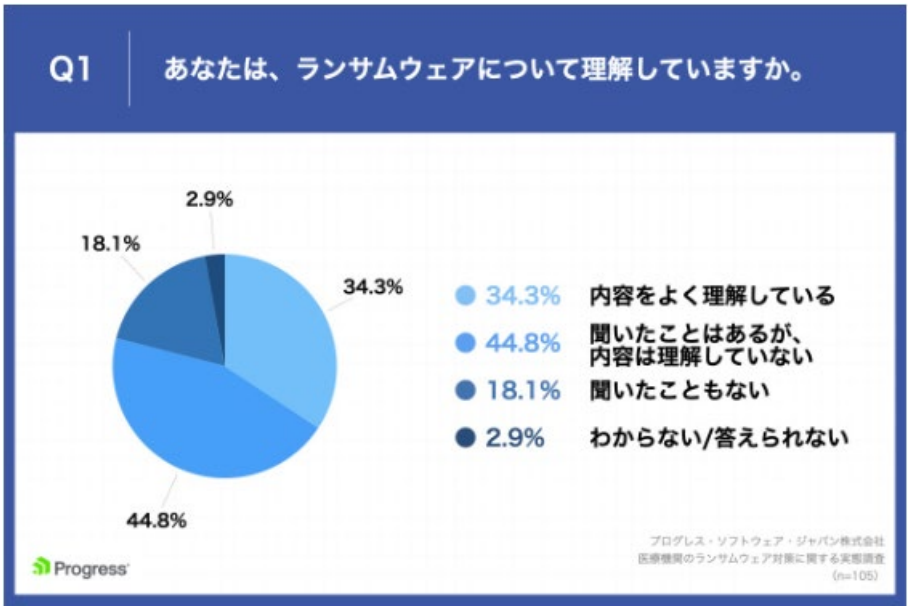
調査概要

調査概要：医療機関のランサムウェア対策に関する実態調査
調査方法：IDEATECH が提供するリサーチ PR「リサピー®」の企画によるインターネット調査
調査期間：2023 年 2 月 21 日～同年 2 月 22 日
有効回答：医療機関のネットワーク/システム管理に携わる方 105 名
※構成比は小数点以下第 2 位を四捨五入しているため、合計しても必ずしも 100 とはなりません。

ランサムウェアについて、内容を理解できているのは 34.3%

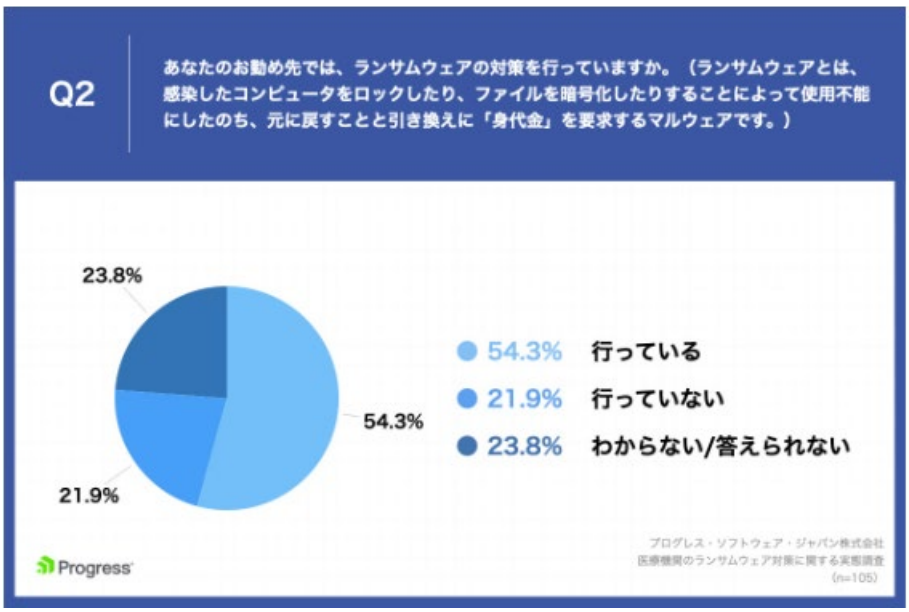
「Q1.あなたは、ランサムウェアについて理解していますか。」（n=105）と質問したところ、「内容をよく理解している」が 34.3%、「聞いたことはあるが、内容は理解していない」が 44.8%という回答となりました。

Q1.あなたは、ランサムウェアについて理解していますか。
・内容をよく理解している：34.3%
・聞いたことはあるが、内容は理解していない：44.8%
・聞いたこともない：18.1%
・わからない/答えられない：2.9%



ランサムウェアの対策、半数以上が実施

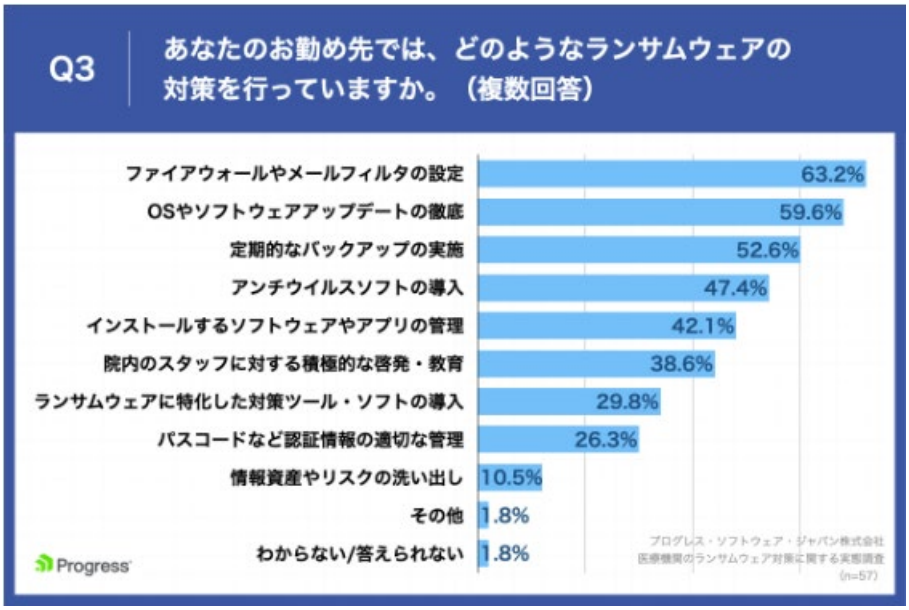
「Q2.あなたのお勤め先では、ランサムウェアの対策を行っていますか。（ランサムウェアとは、感染したコンピュータをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求するマルウェアです。）」（n=105）と質問したところ、「行っている」が 54.3%、「行っていない」が 21.9%という回答となりました。



Q2.あなたのお勤め先では、ランサムウェアの対策を行っていますか。
・行っている：54.3%
・行っていない：21.9%
・わからない/答えられない：23.8%

具体的なランサムウェア対策、「ファイアウォールやメールフィルタの設定」が 63.2%で最多

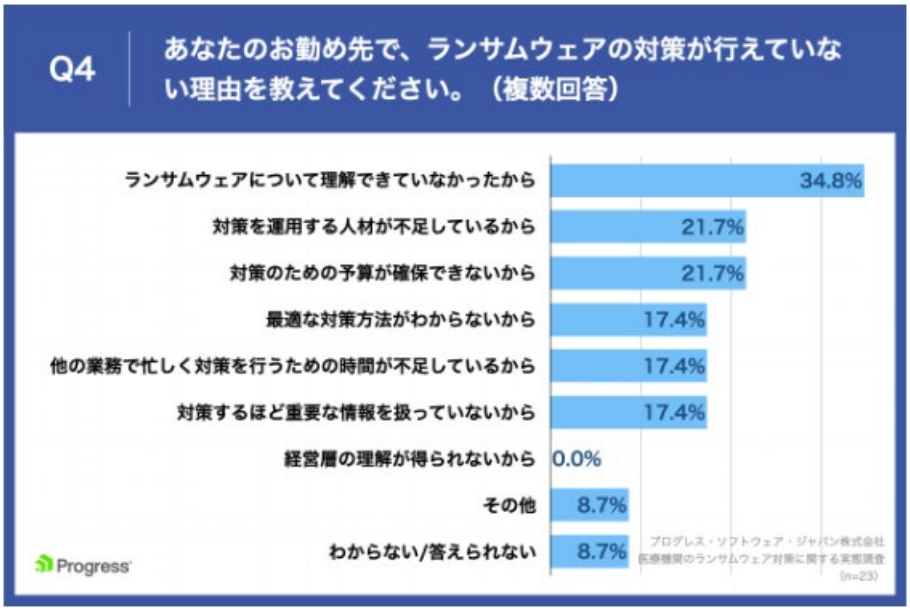
Q2 で「行っている」と回答した方に、「Q3.あなたのお勤め先では、どのようなランサムウェアの対策を行っていますか。（複数回答）」（n=57）と質問したところ、「ファイアウォールやメールフィルタの設定」が 63.2%、「OS やソフトウェアアップデートの徹底」が 59.6%、「定期的なバックアップの実施」が 52.6%という回答となりました。



Q3.あなたのお勤め先では、どのようなランサムウェアの対策を行っていますか。（複数回答）
・ファイアウォールやメールフィルタの設定：63.2%
・OS やソフトウェアアップデートの徹底：59.6%
・定期的なバックアップの実施：52.6%
・アンチウイルスソフトの導入 ：47.4%
・インストールするソフトウェアやアプリの管理：42.1%
・院内のスタッフに対する積極的な啓発・教育：38.6%
・ランサムウェアに特化した対策ツール・ソフトの導入：29.8%
・パスコードなど認証情報の適切な管理：26.3%
・情報資産やリスクの洗い出し：10.5%
・その他：1.8%
・わからない/答えられない：1.8%

ランサムウェアの対策が行えていない理由、「ランサムウェアについて理解できていなかったから」が 34.8%で最多
Q2 で「行っていない」と回答した方に、「Q4.あなたのお勤め先で、ランサムウェアの対策が行えていない理由を教えてください。（複数回答）」（n=23）と質問したところ、「ランサムウェアについて理解できていなかったから」が 34.8%、「対策を運用する人材が不足しているから」が 21.7%、「対策のための予算が確保できないから」が 21.7%という回答となりました。

Q4.あなたのお勤め先で、ランサムウェアの対策が行えていない理由を教えてください。（複数回答）
・ランサムウェアについて理解できていなかったから：34.8%
・対策を運用する人材が不足しているから：21.7%
・対策のための予算が確保できないから：21.7%
・最適な対策方法がわからないから：17.4%
・他の業務で忙しく対策を行うための時間が不足しているから：17.4%
・対策するほど重要な情報を扱っていないから：17.4%
・経営層の理解が得られないから：0.0%
・その他：8.7%
・わからない/答えられない：8.7%



「時間がない」や「危機感不足」などの理由も

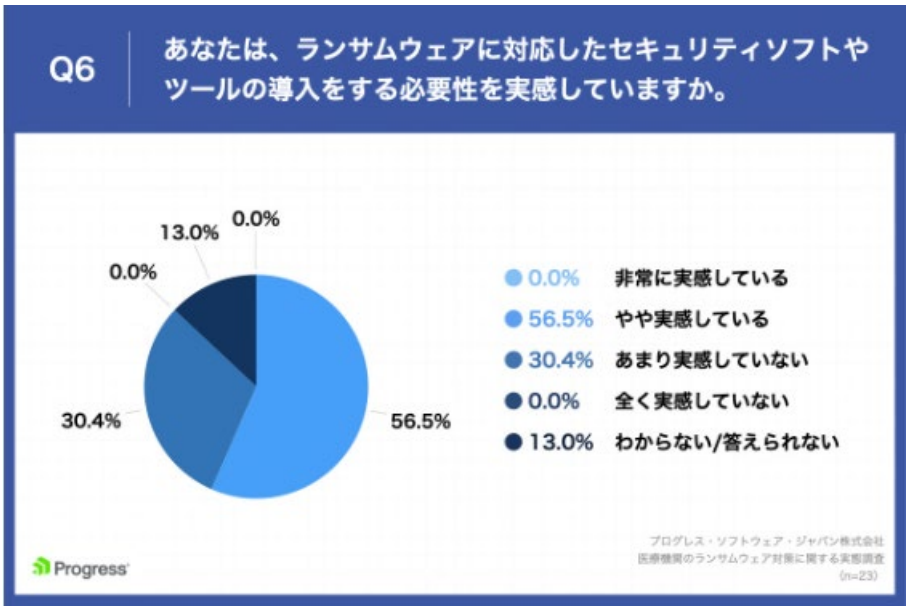
Q4 で「わからない/答えられない」以外を回答した方に、「Q5.Q4 で回答した以外に、ランサムウェアの対策が行えていない理由があれば、自由に教えてください。（自由回答）」（n=21）と質問したところ、「時間がない」や「危機感不足」など 12 の回答を得ることができました。

＜自由回答・一部抜粋＞
・50 歳：時間がない。
・55 歳：危機感不足。
・41 歳：ウイルスについての危機管理ができていない。
・26 歳：知識がないため。

ランサムウェア対策をしていない回答者のうち、56.6%がセキュリティソフトやツール導入の必要性を実感

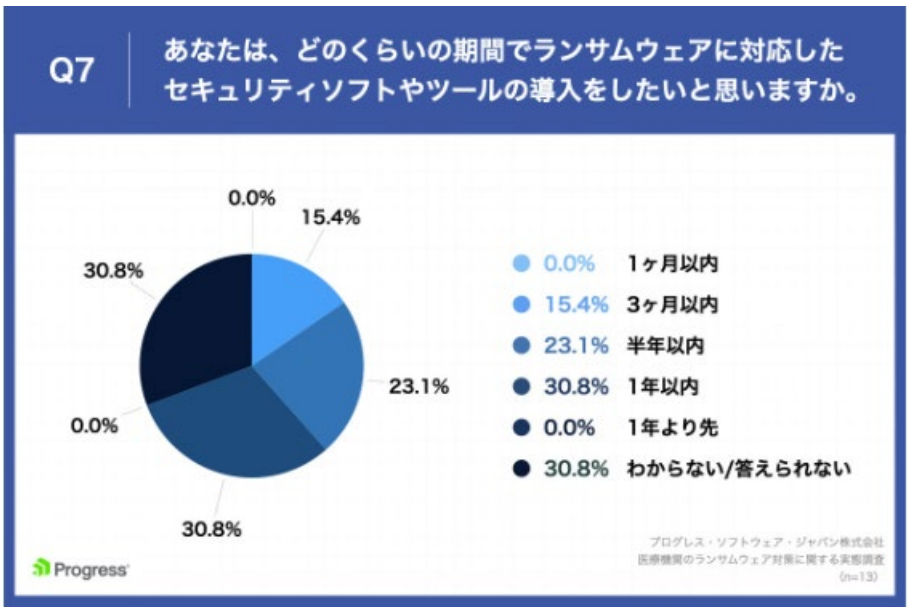
Q2 で「行っていない」と回答した方に、「Q6.あなたは、ランサムウェアに対応したセキュリティソフトやツールの導入をする必要性を実感していますか。」（n=23）と質問したところ、「やや実感している」が 56.5%、「あまり実感していない」が 30.4%という回答となりました。

Q6.あなたは、ランサムウェアに対応したセキュリティソフトやツールの導入をする必要性を実感していますか。
・非常に実感している：0.0%
・やや実感している：56.5%
・あまり実感していない：30.4%
・全く実感していない：0.0%
・わからない/答えられない：13.0%



3 割以上が、「1 年以内にランサムウェアに対応したセキュリティソフトやツールの導入をしたい」と回答

Q6 で「非常に実感している」「やや実感している」と回答した方に、「Q7.あなたは、どのくらいの期間でランサムウェアに対応したセキュリティソフトやツールの導入をしたいと思いますか。」（n=13）と質問したところ、「1 年以内」が 30.8%、「半年以内」が 23.1%という回答となりました。

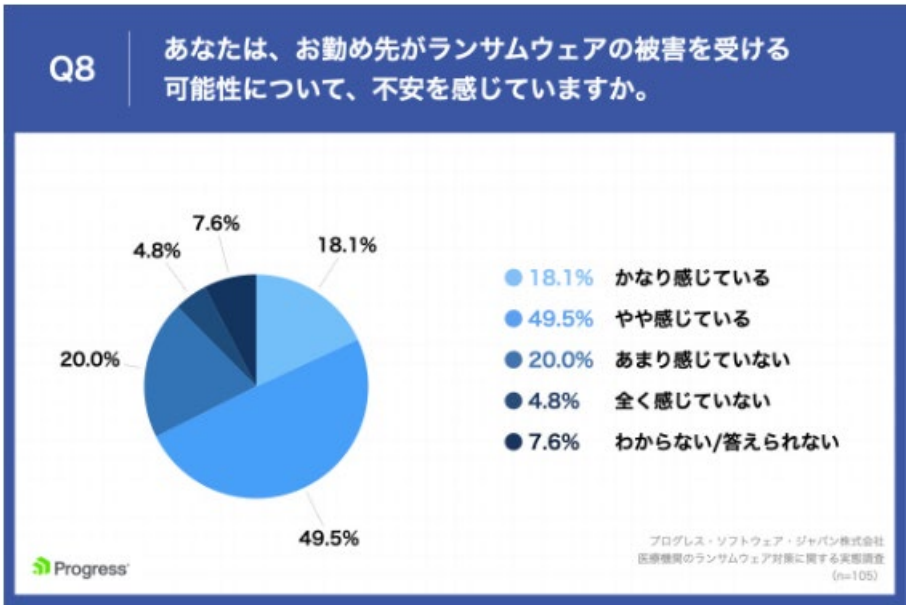


Q7.あなたは、どのくらいの期間でランサムウェアに対応したセキュリティソフトやツールの導入をしたいと思いますか。

・1 ヶ月以内：0.0%
・3 ヶ月以内：15.4%
・半年以内：23.1%
・1 年以内：30.8%
・1 年より先：0.0%
・わからない/答えられない：30.8%

67.6%が、勤め先がランサムウェアの被害を不安視

「Q8.あなたは、お勤め先がランサムウェアの被害を受ける可能性について、不安を感じていますか。」（n=105）と質問したところ、「かなり感じている」が 18.1%、「やや感じている」が 49.5%という回答となりました。

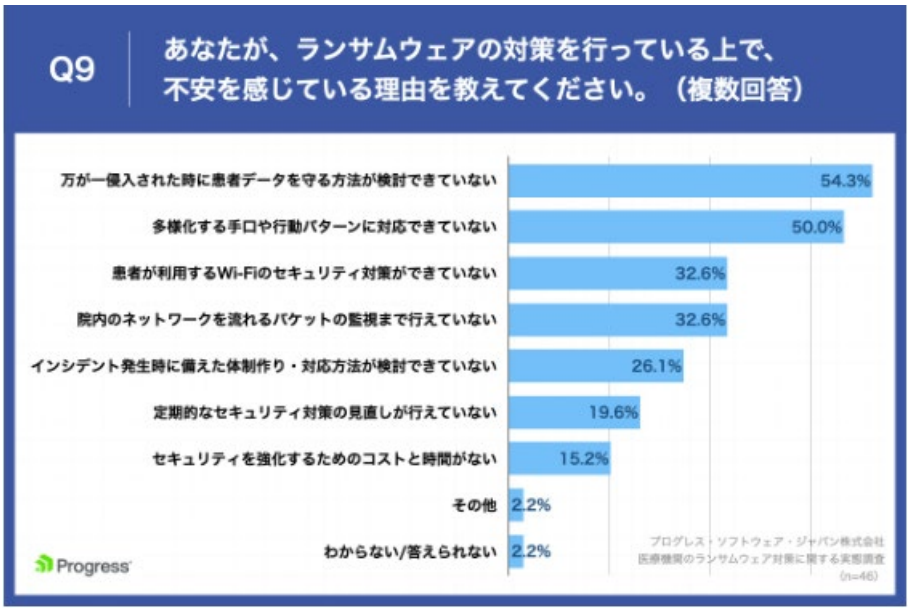


Q8.あなたは、お勤め先がランサムウェアの被害を受ける可能性について、不安を感じていますか。
・かなり感じている：18.1%
・やや感じている：49.5%
・あまり感じていない：20.0%
・全く感じていない：4.8%
・わからない/答えられない：7.6%

ランサムウェアの対策で不安を感じている理由、「万が一侵入された時に患者データを守る方法が検討できていない」が 54.3%で最多

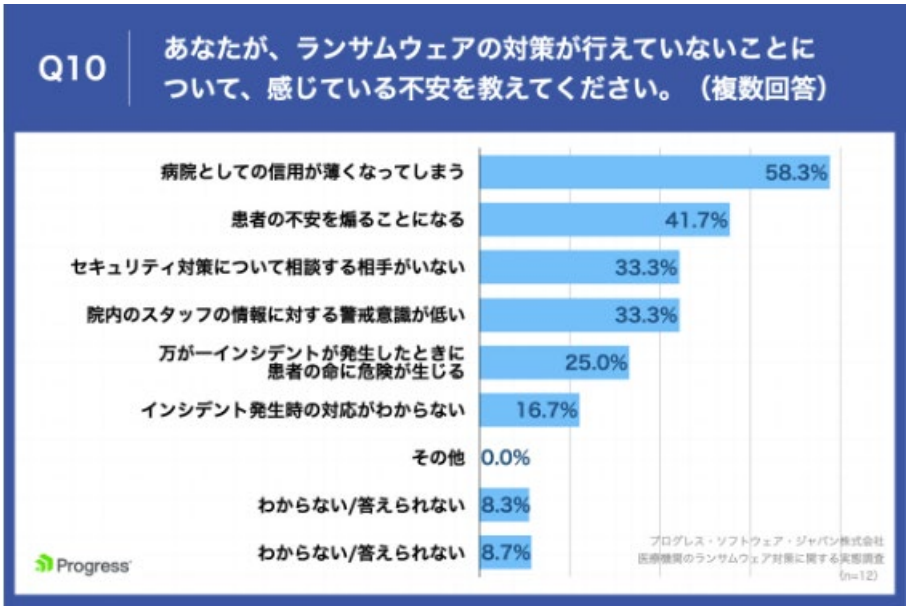
Q2 で「行っている」かつ Q8 で「かなり感じている」「やや感じている」と回答した方に、「Q9.あなたが、ランサムウェアの対策を行っている上で、不安を感じている理由を教えてください。（複数回答）」（n=46）と質問したところ、「万が一侵入された時に患者データを守る方法が検討できていない」が 54.3%、「多様化する手口や行動パターンに対応できていない」が 50.0%、「患者が利用する Wi-Fi のセキュリティ対策ができていない」が 32.6%という回答となりました。

Q9.あなたが、ランサムウェアの対策を行っている上で、不安を感じている理由を教えてください。（複数回答）
・万が一侵入された時に患者データを守る方法が検討できていない：54.3%
・多様化する手口や行動パターンに対応できていない：50.0%
・患者が利用する Wi-Fi のセキュリティ対策ができていない：32.6%
・院内のネットワークを流れるパケットの監視まで行えていない：32.6%
・インシデント発生時に備えた体制作り・対応方法が検討できていない：26.1%
・定期的なセキュリティ対策の見直しが行えていない：19.6%
・セキュリティを強化するためのコストと時間がない：15.2%
・その他：2.2%
・わからない/答えられない：2.2%



具体的な不安、「病院としての信用が薄くなってしまう」が 58.3%で不安

Q2 で「行っていない」かつ Q9 で「かなり感じている」「やや感じている」と回答した方に、「Q10.あなたが、ランサムウェアの対策が行えていないことについて、感じている不安を教えてください。（複数回答）」（n=12）と質問したところ、「病院としての信用が薄くなってしまう」が 58.3%、「患者の不安を煽ることになる」が 41.7%、「セキュリティ対策について相談する相手がいない」が 33.3%という回答となりました。



Q10.あなたが、ランサムウェアの対策が行えていないことについて、感じている不安を教えてください。（複数回答）

・病院としての信用が薄くなってしまう：58.3%
・患者の不安を煽ることになる：41.7%
・セキュリティ対策について相談する相手がいない：33.3%
・院内のスタッフの情報に対する警戒意識が低い：33.3%
・万が一インシデントが発生したときに患者の命に危険が生じる：25.0%
・インシデント発生時の対応がわからない：16.7%
・その他：0.0%
・わからない/答えられない：8.3%

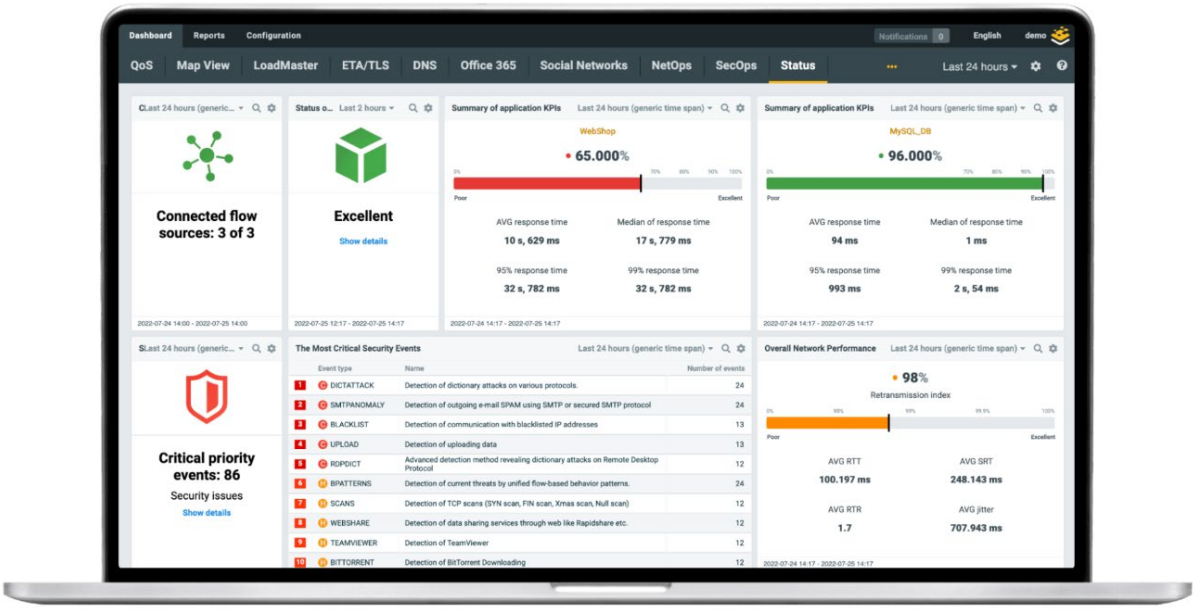
まとめ

今回は、医療機関のネットワーク/システム管理に携わる方 105 名を対象に、医療機関のランサムウェア対策に関する実態調査を実施しました。

まず、ランサムウェアについて理解している医療機関のシステム担当者は、3 割程度に留まっていることが分かりました。一方で、対策自体は半数以上が実施しており、具体的には「ファイアウォールやメールフィルタの設定」や「OS やソフトウェアアップデートの徹底」、「定期的なバックアップの実施」などの対策が行われていることが分かりました。ランサムウェア対策を実施していない場合の理由としては、「ランサムウェアについて理解できていなかったから」が 34.8%で最多となり、認知度が対策に踏み切るかどうかの分かれ道になっていることが判明しました。対策をしていない場合でも、半数以上がセキュリティソフトやツール導入の必要性を実感しており、勤め先の被害を不安に感じるとの声が多数寄せられました。

今回の調査では、医療機関のネットワーク担当者が、日頃からシステムのセキュリティーを重要視しており、セキュリティソフトやツールを導入して、患者の大切なデータを守る必要性を感じていることが分かりました。一方で、ランサムウェアに対する理解が深まっているとは言えない現状となっており、患者から信頼される医療機関になるためには、まずはランサムウェアについてしっかりと理解した上で、適切な対策を取る必要があると言えるでしょう。

ランサムウェア対策には「Flowmon」



Flowmon は、ネットフローデータを元に自社のネットワーク内での事象を把握、監視できるネットワークトラフィック監視およびセキュリティソリューションです。蓄積したデータを AI エンジンが分析、解析、関連付けをおこない、分析結果を表示します。これにより、これまでの事後処理的なトラブルシューティングから事前対策型に移行できます。また、振る舞い検知機能は 200 以上のハッカーの振る舞いパターンを登録しており、新しいパターンが発見されると自動的に更新します。これにより迅速にランサムウェア、マルウェアなどの事象を素早く検知し、対応することが可能です。

Flowmon の詳細については、https://www.flowmon.com/jp をご参照ください。

プログレスについて

プログレス（Nasdaq：PRGS）は、テクノロジーが牽引する世界において専心的にビジネスを推進し、多くの企業がイノベーションのサイクルを加速し、躍進して業績を向上させていくプロセスを支援します。プログレスは信頼できるプロバイダーとして、インパクトが大きいアプリケーションを開発、展開、管理するための最高の製品を提供し、お客様は必要なアプリケーションとエクスペリエンスを開発し、適切な手法で展開し、すべてを安全かつ確実に管理することが可能になります。1,700 のソフトウェア

会社と 350 万の開発者を含め何十万もの企業が目標達成のために確信を持ってプログレス製品を利用しています。詳細については www.progress.com をご覧ください。

お問い合わせ先：
プログレス・ソフトウェア・ジャパン株式会社
高田美奈（たかたみな）
sales_japan@progress.com