KEEPER
Cybersecurity Starts Here

2021

ランサムウェア影響レポート

目次

序論と方法論

2021年はランサムウェアの年となるでしょう。攻撃の頻度が急速に増加するにつれて、桁違いに高額になっていく身代金の要求がマスコミに大きく取り上げられています。消費者は、かつて影響から比較的遮断されていましたが、利用する組織が攻撃によりオフライン状態になってしまうため、今では製品不足やサービスにアクセスできない状況を経験しているのです。

しかし、攻撃後の組織内には何が起こるのでしょうか？内部プロセスはどのような影響を受けているのでしょう？従業員の効率性と生産性への影響はどのようなものでしょうか？それらを突き止めるために、Keeperは、雇用主が過去12ヶ月間にランサムウェア攻撃を受けたことがある米国内の従業員2,000人を対象に調査を行いました。

Keeper SecurityはPollfishと提携し、米国内のフルタイム従業員2,000人を対象とした本調査を実施しました。過去12ヶ月間にランサムウェア攻撃の被害に遭った企業でフルタイムで働く個人のみを対象としました。調査は2021年6月に完了しました。

サイバーセキュリティトレーニング不足による影響

従業員の3分の1近くが、攻撃前に十分なサイバーセキュリティトレーニングを受けていなかったことがわかりました。

従業員のサイバーセキュリティ意識向上トレーニングは、ランサムウェア攻撃を防ぐ上で不可欠です。ランサムウェア攻撃には特にソーシャルエンジニアリングが関与したものが非常に多いためです。

- 回答者は、ランサムウェア攻撃の42%はフィッシングメールが原因だったと報告
- 悪意のあるウェブサイトが別の23%を構成
- 21%は漏洩したパスワードが原因

しかし、回答者の29%が、雇用主が被害に遭うまでランサムウェアとは何なのかを知らなかったとKeeperに回答しています。これは、ランサムウェア攻撃の大半とまでは言わずとも、多くの攻撃を以下のような方法で防ぐことができた可能性があることを示しています。

- サイバーセキュリティに対する意識向上、特にフィッシングやその他のソーシャルエンジニアリング手法を避ける方法について、従業員を適切かつ定期的にトレーニングする
- すべてのアカウントに強力でユニークなパスワードの使用を従業員に要求し、多要素認証に対応している場合は常にそれを有効にする

1日遅れると1ドル足りなくなる？

回答者は、攻撃後、組織の87%がセキュリティプロトコルをより厳格なものに制定、90%が従業員にサイバーセキュリティトレーニングを追加で提供、67%がサイバーセキュリティへの支出を増やしたと回答しています。

支払うべきか、支払わざるべきか

身代金を支払えば更なる攻撃が助長されることは誰もが同意しています。ただ、組織がランサムウェアの要求に屈するべきかどうかは、セキュリティコミュニティ内でも大きな議論の余地があります。これは、組織が活発な攻撃を受けると、組織の上層部は、問題を解決し一刻も早くオンライン状態に戻るよう求める顧客や企業の利害関係者、さらにはサイバー保険会社からの途方もないプレッシャーに直面するからです。このプレッシャーは、システムがダウンタイムとなることで人の健康や生命を危険にさらす可能性がある、医療施設や公共部門で特に強いものとなってます。

結果として、回答者の49%が、自分の雇用主が身代金を支払ったとKeeperに答えています。しかし、このお金は天から降ってきたものではありません。93%が、身代金を支払った後、雇用主が他の分野で予算の引き締めを行ったと回答しています。

ランサムウェアがもたらす高額な間接的コスト

ランサムウェアからの回復には、高額な間接的コストが発生します。

SNSでは非常に高額な身代金を要求される傾向が発信されていますが、組織は攻撃後に多額の間接的コスト（特にシステムの停止など）の負担を被ります。こうした障害は顧客やパートナーの不満を募らせるだけでなく、従業員が仕事を遂行する妨げにもなるのです。

- 7%の回答者は、攻撃の後にシステムやネットワークに一時的にアクセスできなかった
- システム停止状態の28%は、1週間以上続いた
- 回答者の26%は、少なくとも1週間以上職務を遂行できなかった

たとえシステムがオンラインに戻ったとしても、組織はさらなる攻撃を防ぐために変更を加える必要があります。回答者の圧倒的多数（83%）は、自分の組織が新しいソフトウェアをインストールしたり、他の主要なアップデート（一部の資産をクラウドに移行するなど）を行ったりしたと回答しています。

ほとんどの場合、このような変更を順次実施することで生産性がさらに低下し、間接的な回復コストの集計に加算されていったのです。回答者の71%が、新しいソフトウェアやアップデートをインストールするプロセスは不便であった、あるいは生産性が損なわれたと回答しています。

- 答者の64%がログイン認証情報や文書を紛失した
- 8%がプログラムやアプリケーションの不具合を経験したと報告した
- 33%が新しいプロトコルを習得する困難さに直面した
- 40%がコンピューターの再起動やアップデートで時間を損失した
- 3%が、プログラムやアカウントへのログイン状態が継続されず、ログインを続ける必要があった
- 21%が、通常のオンラインツールやアプリケーションが利用できなくなったと回答した

残念ながら、従業員がパスワードをリセットしたり、失われた文書の回復を試みたり、新しいアプリケーションやプロトコルでサポートを受けたりするためにIT担当者からの助けを最も必要としていた際、IT部門は多くの場合多忙を極めていたのです。回答者の3分の1以上（36%）が、セキュリティ以外の問題に対するITサポートへのアクセスが、攻撃を受けた後は制限されたと回答しています。

公表されていない攻撃の割合

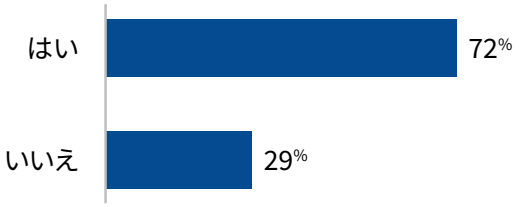
ランサムウェア攻撃は、その多くが公表されていないために広く蔓延しています 。

身代金を支払って先に進まなければならないという組織のリーダーが感じるプレッシャーに加えて、回答者の64%が、ランサムウェア攻撃を受けたことで組織の評判が損なわれたと感じています。さらに、従業員の63%が、自分の組織が攻撃を受けたことにより、自分が組織に対して寄せていた信頼が失われたと報告しています。

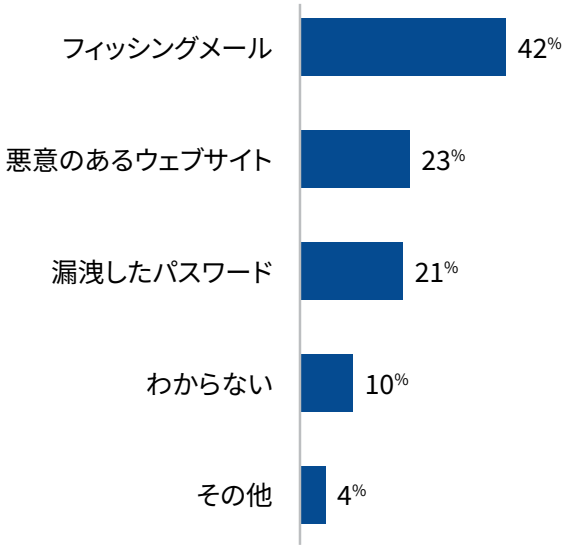
このことを念頭に置くと、雇用主がパートナーや顧客（一般市民ではない）だけに攻撃について公表したと回答したのは回答者の26%であり、15%は誰にも話さなかったということは、驚くには当たりません。これは、ランサムウェア攻撃が、認識されている以上に広範囲に蔓延している可能性が高いことを示しています。

完全データ

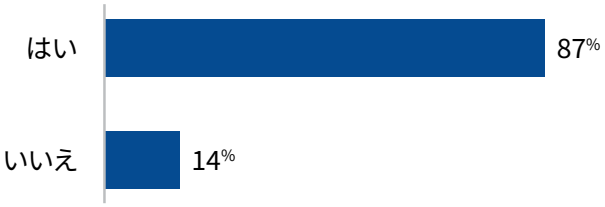
Q1. あなたは、攻撃を受ける以前からランサムウェアについて知っていましたか?



Q2. あなたの会社に対するランサムウェア攻撃の根本原因は何でしたか?

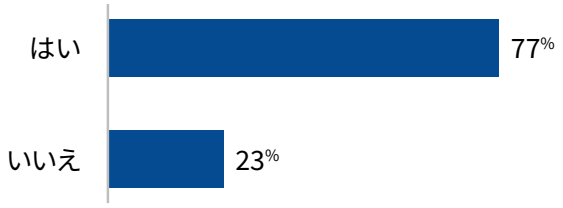


Q3. ランサムウェア攻撃を受けたことで、あなたの会社はセキュリティプロトコルを厳格化しましたか?

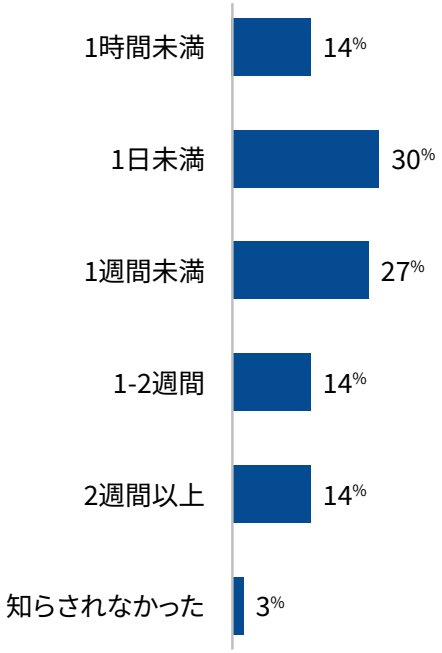


回答調査結果は、四捨五入により100%を超えるものもあります

Q4. あなたの会社は、ランサムウェア攻撃を受けたことでオフライン状態（システムやネットワークにアクセスできなかったなど）になった時期はありましたか？

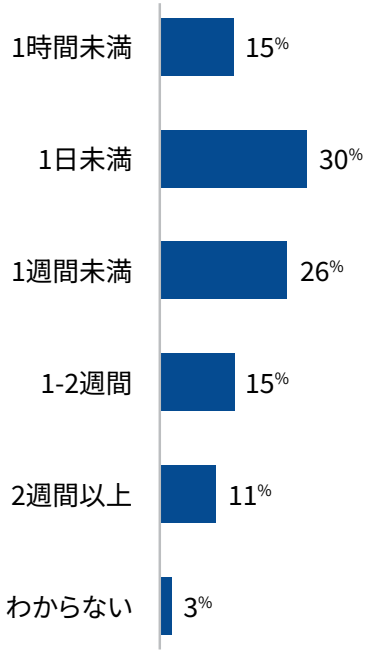


Q5.「はい」と答えた方は、会社はどれほどの期間ダウンしていましたか？

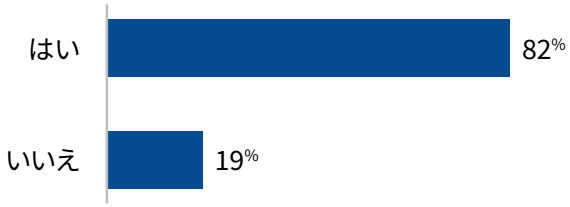


回答調査結果は、四捨五入により100%を超えるものもあります

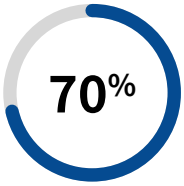
Q6.「はい」と答えた方は、完全に働くことができなかった期間はどのくらいでしたか？



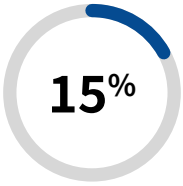
Q7. ランサムウェア攻撃を受けた後、あなたの組織の上層部は従業員と効果的にコミュニケーションを取っていたと思いますか？



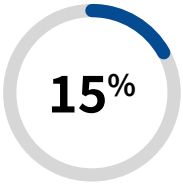
Q8. あなたの会社は、顧客やパートナーに攻撃についての注意を喚起しましたか？



はい



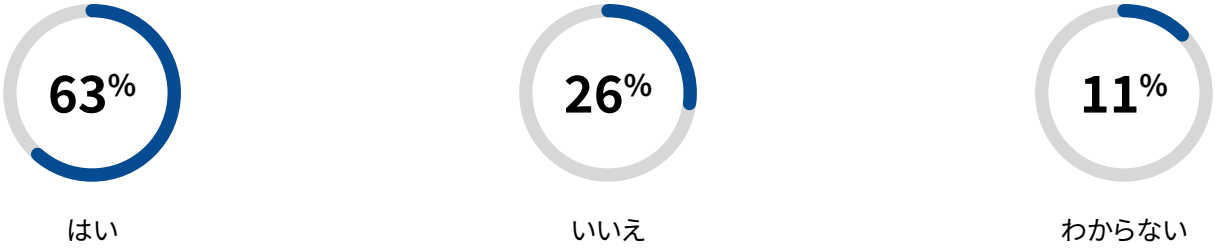
いいえ



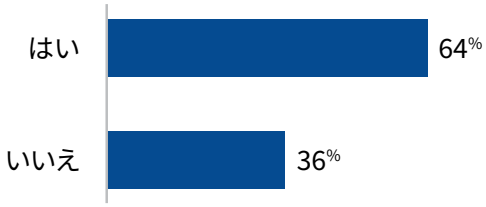
わからない

回答調査結果は、四捨五入により100%を超えるものもあります

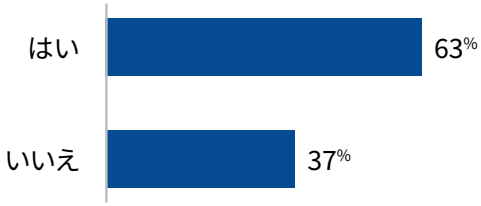
Q9. あなたの会社は、攻撃について反応する声明を一般に公表しましたか？



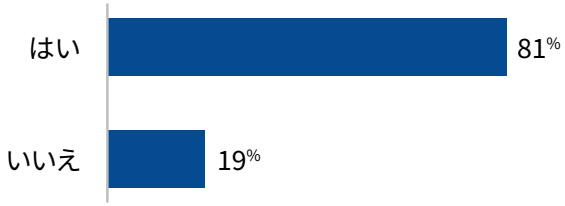
Q10. あなたは、ランサムウェア攻撃が会社の評判に悪影響を及ぼしたと感じますか？



Q11. ランサムウェア攻撃は、自分の組織に対するあなた自身の信頼に影響を与えましたか？

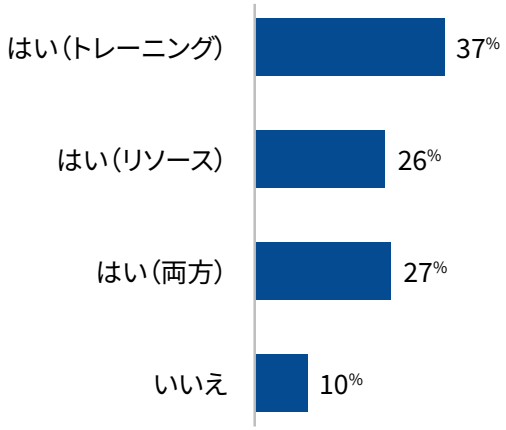


Q12. ランサムウェア攻撃を受ける前、あなたはソフトウェアアップデートの通知が来たら定期的にインストールしましたか？

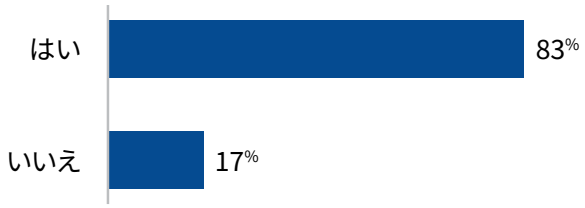


回答調査結果は、四捨五入により100%を超えるものもあります

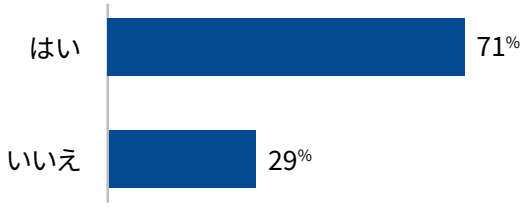
Q13. 攻撃後、あなたの会社はサイバーセキュリティのトレーニングやリソースを提供しましたか?



Q14. 攻撃後、あなたの会社は、ソフトウェアのインストールや他の主要な技術アップデート(資産をクラウドに移行するなど)を実行しましたか?

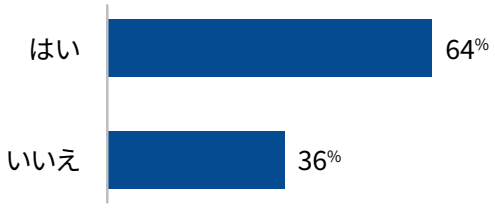


Q15. 「はい」と答えた方は、新しいソフトウェアやアップデートをインストールするプロセスが原因で、支障が出たり生産性が損なわれたりしたと感じますか?

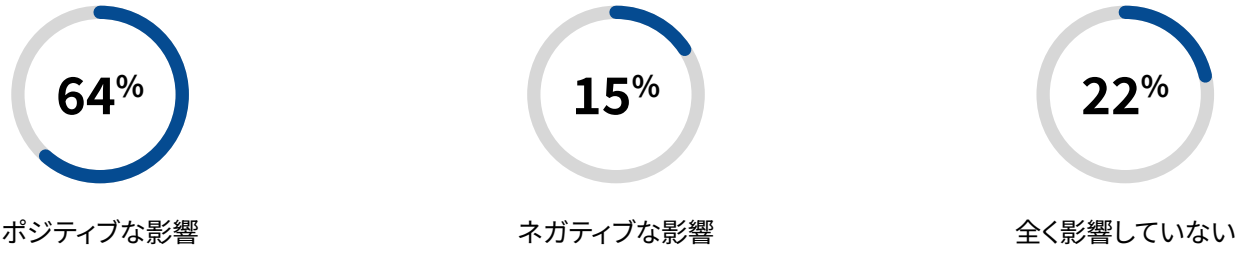


回答調査結果は、四捨五入により100%を超えるものもあります

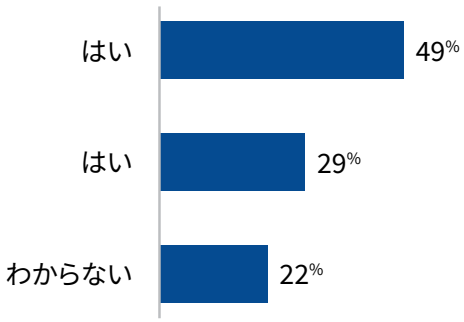
Q16.「はい」と答えた方は、デバイスを更新する過程でログイン認証情報や文書などの情報をひとつでも紛失しましたか?



Q17.「はい」と答えた方は、アップデートが日常業務にどのような影響を及ぼしたと感じていますか?

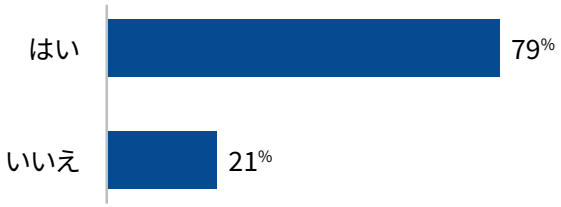


Q18. あなたの会社は身代金を支払いましたか?



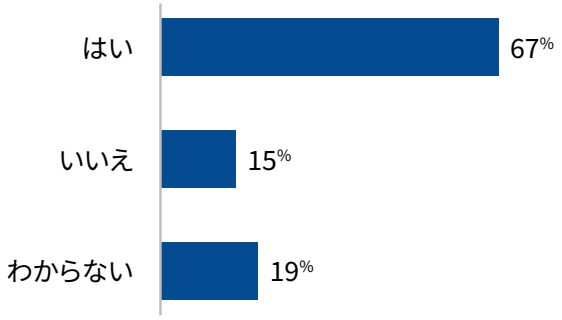
回答調査結果は、四捨五入により100%を超えるものもあります

Q19.「はい」と答えた方は、その金額は従業員に開示されましたか？



Q20.「はい」と答えた方は、自分の組織が身代金を支払った後、他の分野で予算を引き締めていることに気づいたことはありますか？

Q21. 攻撃後、あなたの会社でサイバーセキュリティ分野への支出は増加しましたか？



回答調査結果は、四捨五入により100%を超えるものもあります

Keeperについて

Keeperは、堅牢な管理、制御、強力なパスワードセキュリティに対する可視性、リアルタイムのダークウェブ監視を提供し、ランサムウェア攻撃から組織を保護します。

Keeperが提供するゼロ知識、エンタープライズグレードのパスワードセキュリティ、そして暗号化プラットフォームは、世界中の何千もの企業がパスワード関連のサイバー攻撃を防ぎ、生産性を向上させ、コンプライアンスを強化するのに役立っています。

Keeperは、IT管理者が従業員のパスワード慣行を完全に可視化できるようにするため、パスワード要件が実施されていることを監視し、強力でユニークなパスワードや多要素認証（2FA）などのパスワードセキュリティポリシーを組織全体で強制することが可能になります。きめ細かなアクセス制御により、管理者は役割や責任に基づいて従業員の権限を設定したり、職務分類やプロジェクトチームなど、個々のグループ向けの共有フォルダを設定したりすることができます。

組織は、パスワードの保護を強化するためにKeeper ファイルストレージやBreachWatch™といった高性能なアドオンを導入できます。Keeper ファイルストレージは、従業員が文書や画像、動画、さらにはデジタル認証やSSHキーといった重要なデータを安全に保存することを可能にし、BreachWatch™はダークウェブフォーラムをスキャンし、従業員のパスワードがひとつでも公的データ漏洩で流出した場合、IT管理者に通知します。

KeeperはSOC-2、FIPS 140-2、およびISO 27001認証を取得しており、米国連邦政府による賞管理システム (SAM) の使用にも指定されています。Keeperは、あらゆる主要産業部門において、規模を問わず全ての企業を保護しています。

詳細については、**keeper.io/ransomware-impact** をご覧ください。