White Paper

身代金を払うよりも迅速な復元の方が安全な理由

Sponsored by: Veeam

Johnny Yu　　Jennifer Glenn　　Phil Goodwin
June 2022

はじめに

ダウンタイムが生じるたびに、数千ドルものビジネスが失われ得る。ランサムウェアの攻撃を受けてしまうと、身代金支払いへの誘惑にかられることもあるであろうが、これは攻撃を受けた企業が望むような応急処置ではない。

身代金の支払いは、必ずしも復元を、ましてやタイムリーな復元を保証するわけでもない。IDCのユーザー調査「*Worldwide Future Enterprise Resiliency and Spending Survey*」では、身代金を支払った後に復元できた企業は、調査に回答した企業の 28%未満である（Figure 1 を参照）。

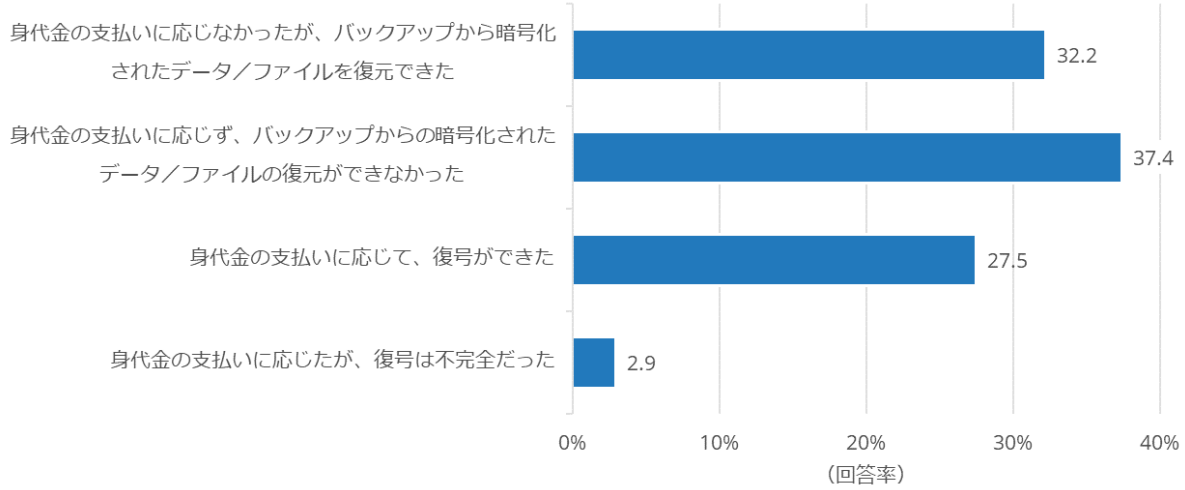
さらに、身代金を支払う選択に決まった手順はない。身代金の支払いに応じると選択する企業のリーダーは、まず、法務チームおよび関連するチームと、この選択に関して時間をかけて検討しなければならない。次いで、ランサムウェア対応チームは、時間をかけて攻撃者と交渉することになるであろう。その後の復号化プロセス自体にさらに長い時間がかかってしまう上、前述の調査報告で指摘されているように、復号化プロセスが機能しない場合もある。

身代金の支払いに応じない場合も、それなりのリスクがある。前述の調査報告では、バックアップファイルから暗号化されたデータを復元できた企業は、調査対象企業の 3 分の 1 未満であったことが分かっている。しかし、データ復元計画を確実かつ迅速に構築するためのツールや技法が確立されてきているため、今後この割合は増やしていけるはずである。こうしたツールや技法を利用すれば、企業は身代金の支払いに応じるか否かを検討するステップに貴重な時間を費やすことなく、自信を持って復元に専念できる。

FIGURE 1

ランサムウェア攻撃を受けた企業で、自社だけで復元できるのは３分の１未満

Q.　システムまたはデータへのアクセスをブロックした最近のランサムウェアインシデントに対する貴社の対応とその結果は、次のうちのどれでしたか？



n = 444

Notes:

- データは IDC の Quantitative Research Group によって管理されている
- データには重み付けがなされていない
- サンプルサイズが小さいデータは参考値

Source: IDC's *Worldwide Future Enterprise Resiliency and Spending Survey*（2021 年 12 月実施）

迅速かつ確実な復元計画の構築

ランサムウェアとは、セキュリティ防御を破って侵入し、重要な情報にアクセスして人質にとる、多くの場合は一連の攻撃ソフトウェアである。ランサムウェア攻撃をまとめて阻止するのがデータ保護のための最良の解決策であることは明らかであるが、これは常に実現可能とは限らない。デジタルビジネスでは、機敏なサービス、革新的なソリューションおよび常時接続の可用性が求められており、セキュリティによって業務が妨げられてはいけない。これはまた、保護に頼るだけでは不十分であることを意味している。

むしろ、対策に成功した企業は、オペレーションが継続され、情報のセキュリティが維持されるように、迅速かつ確実な復元に焦点を合わせたデータ保護の取り組みを拡大している。データ保護の取り組みには、以下が含まれる。

- **検知**：異常およびセキュリティ侵入を迅速に識別し、対応する。
- **防御**：重要なデータのクリーンでイミュータブルなコピーを作成し、維持する。
- **復元**：重要なデータやアプリケーションを、素早くビジネスに戻す。

迅速で確実な復元の第一ステップは、セキュリティインシデントの発生を即座に検知して阻止することである。そのために、企業は、自社のデータの所在やその特性、誰または何がそのデータにアクセスできるか、そしてそのデータがどのように使用され得るかを知っていなければならない。この情報を手にすれば、IT チームとセキュリティオペレーションチームは、どのユーザーまたはデバイスが特定のタイプのデータにアクセスできるか、また、いつどのように使用できるかを指示するポリシーを確立できる。

確立されたポリシーは、機密情報の不正アクセス、誤使用、または漏洩／盗難を防止するために、複数のセキュリティおよびデータ管理のコントロールポイントに適用できる。これらのポリシーは、新たなリスクの出現や企業運営の変化に応じて、変更や調整ができる。また、今後発生する恐れのあるランサムウェア攻撃に対抗するインシデント対応プロセスおよびプレイブックを指定できるデータ保護の基盤も提供する。

ランサムウェアから迅速に復元するための防御コンポーネントには、クリーンで迅速にアクセス可能なデータのバックアップコピーを有することが含まれる。このバックアップコピーからデータの復元がなされる。暗号化、イミュータブルなストレージ、およびエアギャッピングなどのように、バックアップへの不正侵入を困難にするツールは、これまで数年間に渡って販売されており、データ保護の実務担当者には使い慣れたものであろう。

ツール自体とは別に、データ保護のベストプラクティスも実装する必要がある。これには、バックアップデータの複数のコピーを複数の場所に保存することや、誰がバックアップの削除や上書き、復元開始ができるのか、アクセスを制限することが含まれる。

ランサムウェア攻撃からの迅速な復元／修復コンポーネントは、計画外の停止からの復元プロセスに似ているが、いくつかのステップが追加されている。ランサムウェアに対する総体的な対策では、復元プロセスにセキュリティを含める必要がある。復元の最初のステップは、セキュリティチームがマルウェアや侵入の兆候を捜すためにフォレンジックを実行しバックアップコピーをスキャンできるよう、隔離されたサンドボックス環境内で行われるべきである。

いったん復元方法が確立されたら、その方法は定期的にテストされなければならない。テストによってバックアップコピーの復元可能性が保証され、インシデント対応に関与するすべての関係者に復元方法を試す機会が提供される。テストを繰り返すことで、企業はランサムウェア攻撃からの復元のタイミングを計り、改善し、自信を持って身代金の支払いを拒否できるようになる。

セキュリティチームを実質的に通常のディザスターリカバリー（DR：Disaster Recovery）プロセスに関与させることによって、企業はサイバー攻撃の残滓を発見、除去し、バックアップデータを本番環境に戻される前にクリーンな状態にできる。

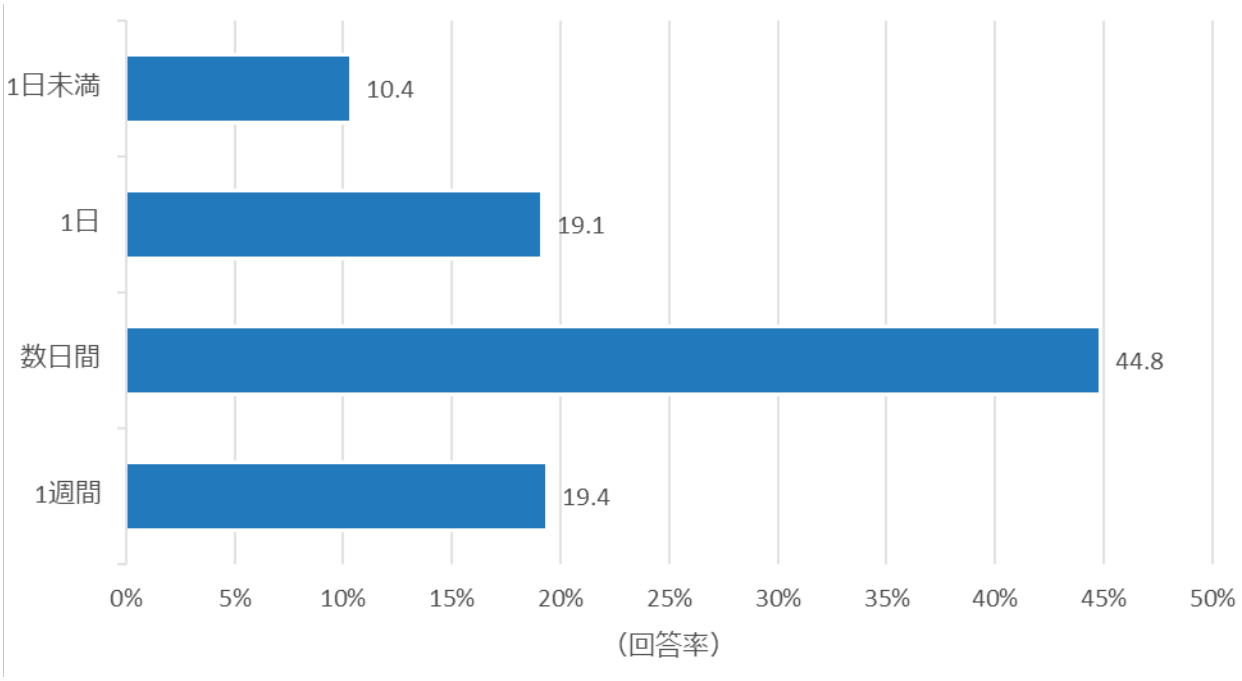
身代金の支払いと迅速な復元の比較

2021 年 12 月の IDC のユーザー調査「*Worldwide Future Enterprise Resiliency and Spending Survey*」では、ランサムウェアの影響を受けた調査対象企業の 45%近くが、数日間ビジネスを混乱させられたと回答している。そのほぼ 5 分の 1（19.4%）が、1 週間に渡ってビジネスの混乱が続いたと回答している（Figure 2 を参照）。

FIGURE 2

ほとんどの企業は、ランサムウェア攻撃を受けて 1 日以上のダウンタイムを経験

Q.　システムまたはデータへのアクセスをブロックした最近のランサムウェアインシデントにおいて、貴社のビジネスは何日間混乱しましたか？



n = 444

Notes:

- データは IDC の Quantitative Research Group によって管理されている
- データには重み付けがなされていない
- サンプルサイズが小さいデータは参考値

Source: IDC's *Worldwide Future Enterprise Resiliency and Spending Survey*（2021 年 12 月実施）

ダウンタイムの最小化はランサムウェア対策の主要な目標の一つであるため、身代金の支払いに応じる選択をした企業もある（Figure 3 を参照）。しかし、身代金を支払えば直ちに企業が復元を開始できるという認識は迷信にすぎない。

通常、身代金の支払いに応じるという決定は、即時にはなされない。ほとんどの企業は、支払いに応じるかの検討に先立って上層部の意思決定者と法務チームが議論している間に、自社で可能なあらゆるデータ復元方法を試みる。文書化され、テストされたディザスターリカバリー計画があれば、このステップが短縮でき、企業の復元機能が不十分であると判明した場合は、次のステップにエスカレーションする必要がある。

企業が身代金の支払いを決定すると、攻撃者だけではなく、サイバー保険会社および政府機関が議論に加わってくる。保険請求を問題なく手にするべくベストプラクティスが守られていると主張し、自社が法規を遵守している証明を行い、犯罪者の要求する金額を下げるために、企業は、こうした関係者のすべてと交渉しなければならない。検討に要した日々もまた、ダウンタイムとなってしまう。

支払いがなされ、犯罪者から復号化キーが配信されても、暗号化されたデータが復号化されるまでは、復元プロセスは開始できない。多くの場合復号ソフトウェアは最適化されていないため、

復号処理には長い時間がかかる。また、復号ソフトウェア自体が損なわれていない保証も、実際に機能する保証もない。

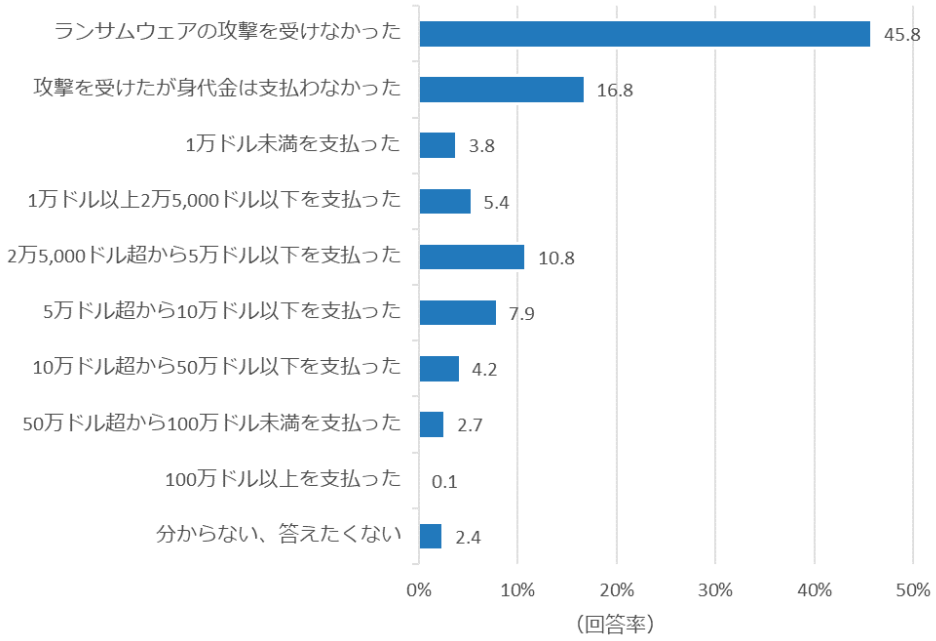
さらに、身代金を支払っても、犯罪者が最初に侵入した手段は阻止できていないため、企業は、まったく同じタイプの攻撃に対して、今後も脆弱なままであろう。その上、身代金の支払いに応じることは、犯罪のビジネスモデルを提供し、それが利益をもたらすと攻撃者に教えることになり、今後の攻撃を保証したも同然である。

そうではなく、データバックアップのためのテクノロジーとプロセスを強化することが、迅速で確実な復元の助けとなる。IDC のユーザー調査「*Worldwide Future Enterprise Resiliency and Spending Survey*」では、ランサムウェアの被害を受けた調査対象企業の 32.2%が、身代金の支払いに応じずに、バックアップからファイルを正常に復元できたと回答している（前出の Figure 1 を参照）。

FIGURE 3

身代金の金額は、数万ドル以上となる可能性がある

Q.　システムやデータへのアクセスを取り戻すためにこの 12 か月間に身代金を支払った場合、その額はどのくらいでしたか？



n = 858

Notes:

- データは IDC の Quantitative Research Group によって管理されている
- データには重み付けがなされていない
- サンプルサイズが小さいデータは参考値

Source: IDC's *Worldwide Future Enterprise Resiliency and Spending Survey*（2021 年 12 月実施）

迅速で信頼性の高い復元システムはディザスターリカバリー計画に基づいているため、数時間以内に企業を正常な状態に戻すのに適している。セキュリティスキャンとフォレンジックに追加の時間をかけたとしても、身代金の支払いなしに、企業にとってより迅速な復元をもたらすはずである。

さらに、復元システムの強度と信頼性が自社の管理下にあるため、ランサムウェア攻撃からの迅速な復元によって、企業は積極的に先手を打てる。自社の復元システムを定期的に検証している企業は、ランサムウェアインシデント中のタイムテーブルを十分に把握しており、身代金の支払い後に犯罪者がその取引を約束通り果たすかどうかを心配する必要はない。

コストの観点からは、攻撃を受けるたびに身代金を支払うよりも、迅速で信頼できる復元の方が持続可能である（前出の Figure 3 を参照）。また、企業は、自社に既存のバックアップ、ディザスターリカバリー、およびセキュリティ資産を一体化できるため、迅速な復元システムを構築するための新しいツールに投資する必要は必ずしもない。

ダウンタイムのコストは、大幅に増加する可能性がある。2020 年の IDC のユーザー調査「*Cost of Downtime and the Importance of Support Survey*」では、オンプレミスのワークロードのダウンタイムの平均コストは 1 時間当たり 2,800 ドルであり、クラウドで実行されるワークロードの場合は 1 時間当たり 3,275 ドルである。これらのメトリクスは、生産性喪失に関連するコスト、潜在的な収益の喪失、復元に要するコスト、ペナルティ、および他の料金が含まれる。さらに警戒すべきは、これらはワークロード当たりの平均コストであり、ランサムウェア攻撃では一度に複数のシステムがダウンさせられる可能性があることである。

この調査の回答者は、ダウンタイムに起因する非財務的要因の重要性も評価していた。つまり、回答者は、長期のダウンタイムが従業員のモラル、生産性、および企業の評判に悪影響を及ぼすことを懸念している。ランサムウェアに起因するダウンタイムは、規制措置および企業の株主によってもたらされる法的措置の可能性などの追加費用をもたらす。

将来の展望

データ保護とデータセキュリティは密接に関連しており、現在、企業は、防御、検知、および修復に対する全体的なアプローチを提供するソリューションを探している。ランサムウェアは絶えず進化しているため、まだ遭遇していない攻撃手法に対する防御策の開発は不可能である。

この刻々と変化する脅威に対応するため、企業はランサムウェアの復元にグループとして取り組むことになる。データ保護ソフトウェアによって検出された異常なバックアップまたは暗号化活動、ファイル名の変更、およびデータの削除はセキュリティチームおよびインシデント対応チームと共有され、侵害の可能性を警告する。同様に、脅威や異常なデータアクセスは、バックアップ管理者が、最後の正常なバックアップコピーがいつなされたかを絞り込む上で役立つ。

やがて企業は、ランサムウェアに対してリアクティブな対応よりもプロアクティブな対応を確立していく。十分に練られた対応に加えて、セキュリティに関するベストプラクティスが遵守され、新しいインフラストラクチャが導入されるたびにポリシーが更新され、潜在的な攻撃の影響範囲も抑制されていく。セキュリティサイドとデータ保護サイドの両方のベンダーツールは、こうした取り組みを支援するために情報を共有できるであろう。

Veeam の検討

Veeam プラットフォームは、オンプレミスのコア、クラウド、およびエッジリポジトリーに渡ってデータ保護機能を提供している。同社は仮想環境でのデータの処理の分野で最もよく知られている企業で、その機能は物理インフラストラクチャや UNIX 環境にも拡張されている。Veeam プラットフォームは、以下の主要モジュールを有している。

- **バックアップと復元**：Veeam を使用してオンプレミスおよびクラウド内のデータを保護するに当たり、その特質はシンプルさである。Veeam Backup & Replication は、最も厳しいサービスレベルを提供すると同時に、その管理に必要な人的労働を削減するように設計されている。

- **オーケストレーション**：ディザスターリカバリー、文書化、テスト、およびコンプライアンスを自動化する。多くの企業にはディザスターリカバリー計画がないか、部分的なディザスターリカバリー計画しかないが、これは主に、完全な計画の実施は複雑でコストがかかるためである。オーケストレーションは、復元に関連する多くの共通タスクを自動化することによって、災害からの復元プロセスを単純化するように設計されている。
- **監視と分析**：Veeam ONE を使用すると、企業は、インフラストラクチャ全体を一元的に監視できる。Veeam ONE は、インフラストラクチャの最適化、データ保護の抜け穴の迅速な識別、および復元の成功の保証についてのインサイトを提供する。

課題と機会

ランサムウェア攻撃は絶えず進化しているが、対抗する防衛はほとんど後追いのリアクションであった。IT リーダーは攻撃に対して可能な限りプロアクティブである必要があり、これを実現するテクノロジーが利用できる必要があると、IDC は考える。

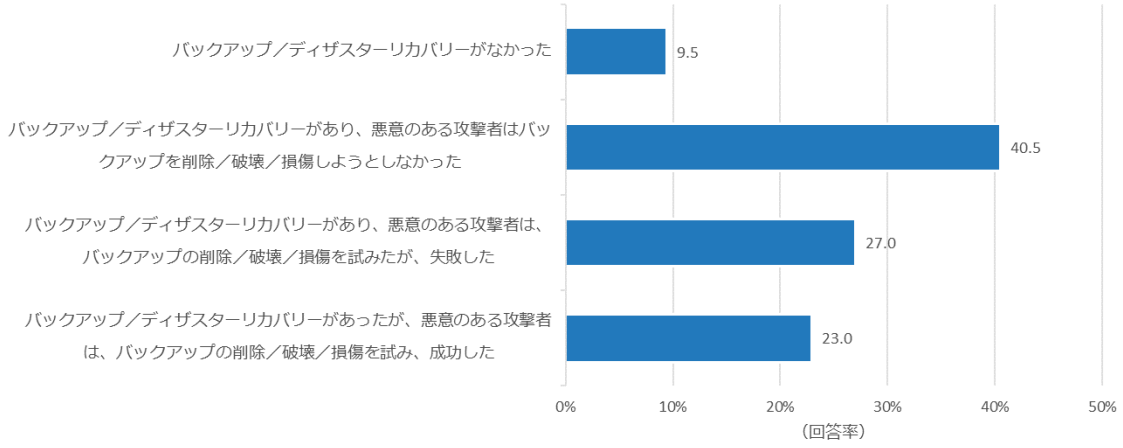
市場には従来、ランサムウェア対策に限定されたソリューションとして単一の製品が提供されてきたが、単一のソリューションではマルウェア攻撃およびランサムウェア攻撃のすべての面には対処できない。したがって、IT 企業はトータルソリューションを構築する必要があり、データ保護とセキュリティの両方からの製品を常に必要としている。

バックアップデータを削除しようとする攻撃方法は依然としてよく試みられているため、データ保護ベンダーは、引き続きバックアップデータの保護に注力する必要がある。IDC のユーザー調査「*Worldwide Future Enterprise Resiliency and Spending Survey*」では、調査対象企業の半数が、悪意のある攻撃者がバックアップをターゲットにしており、そのうち約半数が成功したと回答している（Figure 4 を参照）。

FIGURE 4

ランサムウェアの攻撃者の多くは、バックアップを無効化しようとする

Q.　システムまたはデータへのアクセスをブロックした最近のランサムウェアインシデントにおいて、バックアップ／ディザスターリカバリーに関する貴社のスタンスは何でしたか？



n = 444

Notes:

- データは IDC の Quantitative Research Group によって管理されている
- データには重み付けがなされていない
- サンプルサイズが少ないデータは参考値

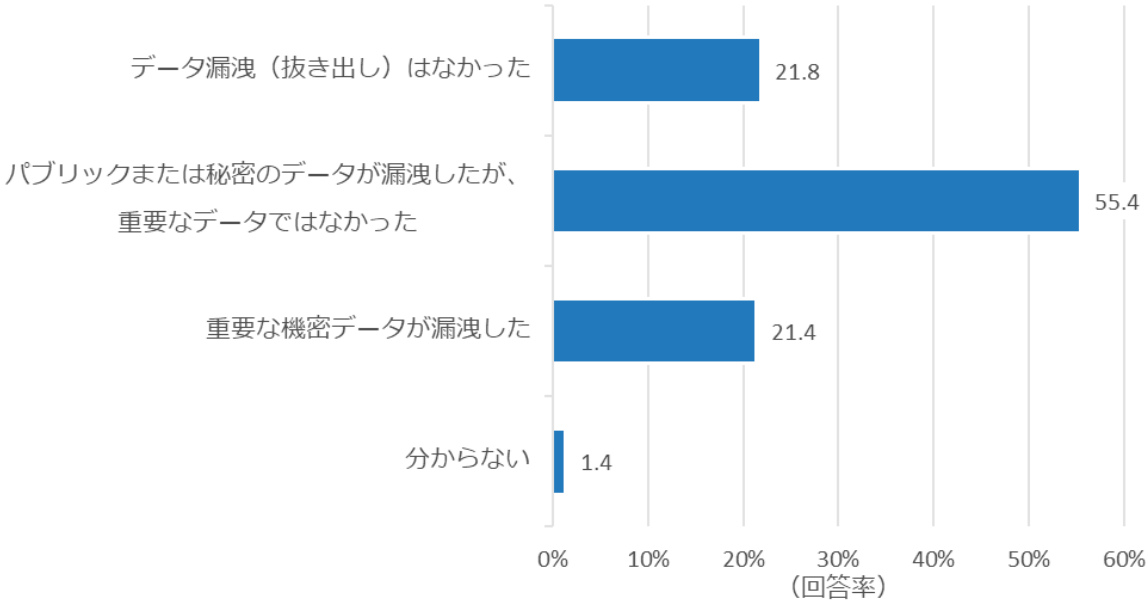
Source: IDC's *Worldwide Future Enterprise Resiliency and Spending Survey*（2021 年 12 月実施）

データ漏洩の増加によって、セキュリティの必要性がさらに高まる。ランサムウェアインシデントに遭遇した調査対象企業の 4 分の 3 近くが、直近の攻撃でデータが盗まれたと回答した（Figure 5 を参照）。データの復元と修復のプロセスにセキュリティを含めることは、盗まれたデータが暗号化されていて犯罪者にとって無意味であることを確実にしたり、少なくとも重要なデータや機密性の高いデータが盗まれたかどうかを判断したりする上で助けになるであろう。

FIGURE 5

ランサムウェアインシデントの 75%以上でデータが盗まれている

Q. *システムまたはデータへのアクセスをブロックした最近のランサムウェアインシデントで、次のうちのどのようなことが起こりましたか？*



n = 444

Notes:

- データは IDC の Quantitative Research Group によって管理されている
- データには重み付けがなされていない
- サンプルサイズが小さいデータは参考値

Source: IDC's *Worldwide Future Enterprise Resiliency and Spending Survey*（2021 年 12 月実施）

ランサムウェアは絶えず進化し、IT 企業は常に守勢にまわるため、避けられないランサムウェアの攻撃に対して、企業はより積極的なスタンスをとらなければならない。IT 企業は、ゼロトラスト、脅威の封じ込め、およびその他の対策を実施しようとしており、IT サプライヤーには、企業のこうした施策を支援するビジネスチャンスがある。

結論

身代金の支払いに応じずにランサムウェア攻撃から完全に復元できる企業は少なく、身代金の支払いは、企業運営を早く正常に復元させるための手段とみなされることが多い。しかしながら、

身代金の支払いに応じるだけで、企業が直ちに復元を開始できることにはならず、また、データの完全復元が保証されるわけでもない。

多くの場合、復号アルゴリズムの処理は遅く、弁護士や政府機関とのコンサルティングおよび攻撃者との交渉に、すでに時間が費やされてしまっている。企業が確信を持ってデータ復元プロセスを即座に開始すれば、この時間はすべて節約できるはずである。

企業は、検知、防護、復元の原則に基づいて、確実なデータ復元システムを構築する必要がある。セキュリティをデータ保護および復元プロセスに織り込むと、完全性が確保され、ランサムウェア攻撃を受けてもダウンタイムを最小限に抑えられる。

IDC 社 概要

International Data Corporation（IDC）は、IT および通信分野に関する調査・分析、アドバイザリーサービス、イベントを提供するグローバル企業です。50 年にわたり、IDC は、世界中の企業経営者、IT 専門家、機関投資家に、テクノロジー導入や経営戦略策定などの意思決定を行う上で不可欠な、客観的な情報やコンサルティングを提供してきました。

現在、110 か国以上を対象として、1,100 人を超えるアナリストが、世界規模、地域別、国別での市場動向の調査・分析および市場予測を行っています。

IDC は世界をリードするテクノロジーメディア（出版）、調査会社、イベントを擁する IDG（インターナショナル・データ・グループ）の系列会社です。

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com