COHESITY

データセキュリティとデータ管理の現状レポート 2023

2023年7月

概要

第2回目となる「データセキュリティとデータ管理の現状レポート」は、Cohesity社、Tenable社、BigID社の委託によりCensuswide社が実施した2023年の調査に基づくもので、ITおよびセキュリティ運用 (SecOps) の意思決定者3,400人以上 (両者の割合はほぼ半々です) を対象としています。この調査は、2023年4月にオーストラリア、フランス、ドイツ、日本、ニュージーランド、英国、米国の企業や組織を対象に実施されました。[1]

サイバー攻撃が深刻化し、頻発している現在、特筆すべき調査結果は下記の3点です:

- **ほとんどの組織は、脅威に対処し事業継続性を維持するために必要なサイバーレジリエンス戦略やデータセキュリティ能力を有していない。**
- **2022年と比較して、攻撃された後に自分の組織がデータを迅速に復旧できると確信している回答者が減少した。**
- **サイバー保険の加入が難しくなっている。**

増加するサイバー攻撃でランサムウェアへの懸念が続く

私たちが2022年に第1回目の「データセキュリティとデータ管理の現状レポート」を発表した際、ランサムウェアの脅威はすでに最重要課題でした。実際、昨年の調査回答者の74%が、その年に自分の業界でランサムウェア攻撃の脅威が高まっていると感じると回答していました。

今年の調査でも同じ質問をしたところ、その割合は大幅に上昇しました。回答者の実に93%が、昨年の同時期と比べて、今年はランサムウェア攻撃の脅威が高まっていると回答しています。

そして、この懸念は単なる脅しではなく、実際に攻撃されています。2年連続で、回答者の半数近くが、過去6ヶ月間にランサムウェアの被害に遭ったと回答してます。

1. Censuswide社は、ESOMARの原則に基づき、Market Research Societyを遵守し、その会員を雇用しています。

ランサムウェアやその他のサイバー攻撃が、あなたのビジネスや世界中の企業にとって依然として現実的な脅威となっているのかどうか疑問に思っているのであれば、このグローバル調査が、その答えはイエスであると教えてくれます。

93%が、2023年はランサムウェア攻撃の脅威が高まっていると感じていると回答ました。

45%が、自分の組織が過去6ヶ月間にランサムウェアの被害に遭ったと回答しました。

COHESITY

課題 1

ほとんどの組織は、脅威に対処し事業継続性を維持するための強力なサイバーレジリエンス戦略やデータセキュリティ能力を欠いている。

脅威の増加にもかかわらず、また、最近攻撃を受けたと回答した組織の割合が高いにもかかわらず、サイ バーレジリエンスを強化するための戦略的対策が進んでいません。実際、調査回答者の5人に4人近くが、自社が今日の深刻化するサイバー上の課題や脅威に対処するためのサイバーレジリエンス戦略を策定し有していることに自信がありません。

そして、それは自信の問題だけではありません。組織は、サイバーレジリエンスとデータセキュリティ能力も必要です。これはデータ復旧と業務オペレーションの回復を迅速に行うためです。

NISTサイバーセキュリティフレームワークは、サイバーセキュリティとサイバーリカバリのための参照フレームワークとして、企業から頻繁に引用されています。識別、防御、検知、対応、復旧の機能を通じて、このフレームワークは、リスクと業務の優先順位に基づいて投資の優先順位を決定する方法をシンプルにします。また、これらのフレームワークは、適切なコントロールとプロセスの導入を導き、セキュリティ、IT、ビジネスの整合性を図るために組織に共通参照ポイントを作成するので、このスタンダードに合わせることは、いくつもの利点をもたらします。

80%が、組織のサイバーレジリエンス戦略と、それが今日のサイバー上の課題や脅威に対処できるかどうかについて懸念があると回答しました。

(回答者には、調査の開始時に、この NIST による サイバーレジリエンスの定義が提供されました)

「サイバーレジリエンスは、特にデータに関する基本を正しく
理解することから始まります。機密データがどこにあるのか、
それは何なのか、誰がアクセスできるのか、
そしてそれに関連するリスクを理解することが不可欠です。
セキュリティコミュニティとして、私たちはデータを
セキュリティ戦略の中心に置く必要があります」

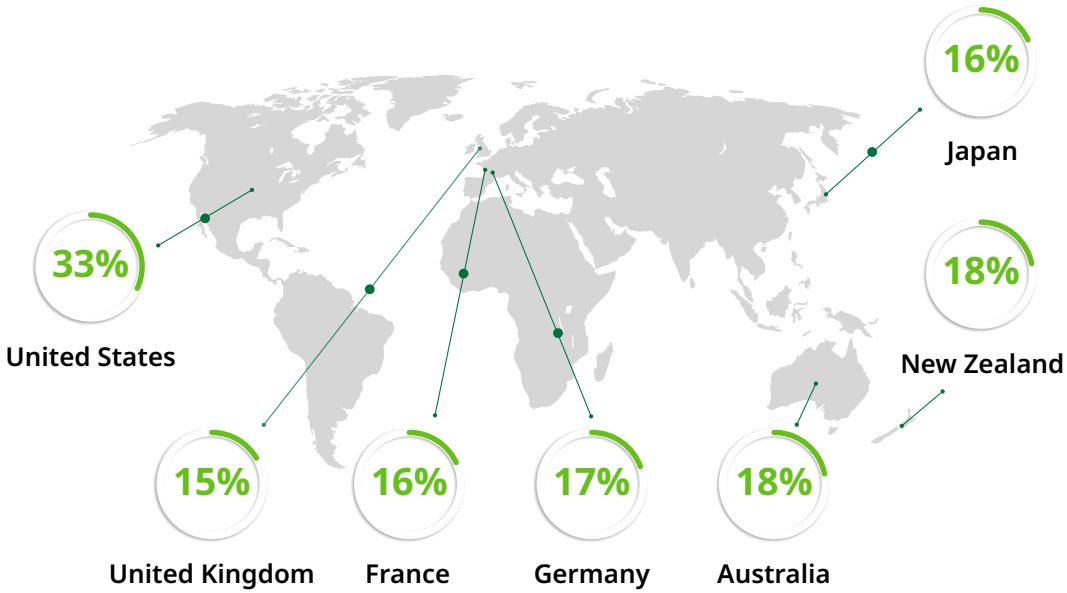
TYLER YOUNG氏、チーフインフォメーションセキュリティオフィス、BIGID社

課題 2

回答者は、攻撃後に自分の組織が復旧できないことを心配している。

ランサムウェアの脅威について尋ねたところ、昨年の回答者の40%が、たとえデータがバックアップされていたとしても、”データ復旧の失敗”が心配であると回答しました。今年は、67%が、システム全体がサイバー攻撃を受けた場合に、自社がデータや重要なビジネスプロセスを復旧できる完全な確信がないと回答しました。

サイバー攻撃後にマルウェアに再感染するリスクなしに復旧できることに”絶対の自信がある”と回答した世界の少ない割合 (21%) の中で、米国は他の地域の国々よりもはるかに自信を持っていました。



復旧と再稼働することを非常に難しくしている障壁は何ですか? 調査によると、上位3つの課題は次のとおりです:

34% ITシステムとセキュリティシステムの統合の欠如

33% IT専門家とセキュリティ専門家の間の連携不足

32% 時代遅れのバックアップとリカバリシステム

COHESITY

…そして、復旧が可能だとしても、それが必ずしも高速だとは限らない。

復旧の遅れは予測不能性をもたらし、ビジネスに悪影響を及ぼします。また、多くの質問を生じさせます。

仮想マシン、データベース、NASデータはいつオンラインに戻り、アクセスできるようになるのか? それらはクリーンに復旧できるのか? それとも、リカバリによってマルウェアが再導入され、システムに再感染しないのか? ミッションクリティカルなデータを、時間や場所を問わずに復旧できるのか? 可能なら、いつ?不可能なら、どうなるのか?

サイバー攻撃が発生した場合、自分の会社がデータやビジネスプロセスを復旧させるのに、平均でどれくらいの時間がかかるると思うか質問しました:

95%が24時間以上かかると回答

74%が4日以上かかると回答

41%が1週間以上かかると回答

そしてランサムウェア攻撃では、1分1秒が重要です。ビジネスが停止し、データにアクセスできなくなる時間が長ければ長いほど、事態は深刻化し、多くの場合直ちに下流に影響を及ぼすリスクが高まります。

「組織は、特に1日以上になると、オフラインで業務を維持することができません。しかし、多くの組織がサイバー犯罪者に対して脆弱なのは、必要なとき、データやビジネスプロセスを迅速に復旧できないからという厳しい現実があります」

BRIAN SPANSWICK、最高情報セキュリティ責任者兼IT部門長、COHESITY

95%が24時間以内にデータやビジネスプロセスを復旧できない場合、組織は脆弱であるだけでなく、将来的に業界の攻撃を誘発する選択をする可能性があります。身代金の支払いもそのひとつです。

ほとんどの人が身代金の支払いを検討

身代金の支払いは一般的に最後の手段であると考えられていますが、グローバル調査の回答者の90%が、(間違いなく支払う国もあれば、コスト次第で支払う国もありますが) データやビジネスプロセスを復旧できる、あるいは復旧が早まるのであれば、身代金の支払いを検討すると回答しています。この判断をする可能性が最も高い国は以下の通りです:

- **オーストラリアとニュージーランド (95%)**
- **米国 (94%)**
- **フランス (93%)**
- **イギリス (91%)**

ドイツ **(87%)** と日本 **(78%)** は依然として支払いを検討する可能性が高いですが、全体としてはそこまで高くありません。

サイバー犯罪者と取引する場合、善意の行為者と取引するわけではないので、身代金を支払ってもデータが復旧できる保証はないこと、あるいは復旧できたとしても、そのデータがクリーンでマルウェアに感染していない保証はないことを常に念頭に置いておく必要があります。

課題 3

サイバー保険の加入が難しくなっている。

サイバー犯罪の被害額は世界で年間8兆ドル (2025年には10兆5,000億ドル) に上ると予測されており、サイバー攻撃やデータ侵害、その他のサイバー関連インシデントによる損失から金銭的な保護を図ろうとする企業が増えています。こうした企業は、保護戦略のひとつとしてサイバー保険に注目しています。

今年の調査回答者は、74%が現在自社がサイバー保険に加入していると回答しました (日本は61%に過ぎません)。しかし、保険契約を確保するのは容易ではなく、調査回答者のほぼ半数 (46%) が、3年前よりもサイバー保険の加入が難しくなっていると回答しています。

回答者が、企業がサイバー保険を確保しようとする際に重要と判断される技術や能力の項目は多く、その中には下記が含まれます:

- 40% 強力な暗号化
- 38% バックアップの完全性を検証する能力
- 37% 多要素認証 (MFA)
- 34% 異常検知
- 33% データ隔離 / エアギャップ
- 29% イミュータビリティ (不変性)

重要な能力を満たすことは、加入が困難なサイバー保険の確保に役立つだけでなく、保険料の引き下げにもつながる可能性があります。

ランサムウェアやより広範なサイバー攻撃に打ち勝つための多層的なセキュリティアプローチにおいて、サイバー保険でもうひとつの層を追加することができます。

問題は山積み。しかし解決策もある。

サイバーレジリエンスを強化することは可能です。

本レポートに記載した通り問題は深刻ですが、ここで取り上げたランサムウェアやその他のサイバーインシデントであれ、地震、洪水、システム障害、人為的ミスなどの災害であれ、脅威が深刻化する中で、組織がサイバーレジリエンスを強化する方法はあります。

サイバーレジリエンスを推進するための具体的な2つの方法は、コラボレーションの強化と洞察の深化です。

コラボレーションの強化

回答者の87%が、データベンダーとサイバーセキュリティベンダーは、完全かつ統合されたランサムウェア対策ソリューションを提供するために協力する必要があると考えています[2]。ベンダーがランサムウェアの撃退という共通の目標に向かって取り組み、クリーンな復旧作業を支援する統合ソリューションを構築することで、組織はそのメリットを享受することができます。サイバー耐性を高めることは、組織にとって、またサービスを提供する顧客にとって、そして業界にとって、より良いことです。国家主体のサイバー犯罪がますます増加する中、これらの攻撃を阻止し、それらに対する回復力を確立することは、世界にとって有益です。

洞察の深化

ベンダー間の協業によるメリットに加え、回答者の90%は、自社のセキュリティ体制とサイバーレジリエンスに関する総合的な洞察を提供するデータセキュリティとデータ管理プラットフォームは、自社にとって有益であると感じています。この洞察により、組織は業務中断のリスクを低減し、サイバー攻撃に耐える能力を向上させることができます。さらに、こうした洞察は、業界規制やプライバシー規制を遵守するための監査を迅速かつ容易にするのに役立ちます。

“今日の巧妙なサイバー脅威の状況において、最新のデータセキュリティ機能を持たない従来型のバックアップとリカバリとシステムに依存することは、災難の元となります。代わりに、組織は既存のサイバーセキュリティソリューションと連携し、セキュリティ体制を可視化し、サイバーレジリエンスを向上させるデータセキュリティとデータ管理プラットフォームを探し求めることが必要です”

BRIAN SPANSWICK、最高情報セキュリティ責任者兼IT部門長、COHESITY

2. この統計は、”非常に重要 “または “やや重要 “のいずれかを選択した回答者の結果を組み合わせたものです。

「身代金を支払うことは、単に金銭的な損失を被るだけでなく、サイバー犯罪者が脆弱な組織を標的にし続けることを助長するという悪循環につながります。Tenable の最近の調査によると、日本の大手企業の外部アタックサーフェスには、サイバー犯罪に悪用される可能性のある資産が12万件以上もあります。企業や組織は、先行的なセキュリティ対策を優先的に実行して機密データや重要システムを保護し、身代金の支払いがもたらす最悪の事態を防ぐ必要があることは明白です」

TENABLE NETWORK SECURITY JAPAN株式会社 カントリーマネージャー、貴島直也氏

データセキュリティと
データ管理の現状レポート 2023

まとめ

組織がランサムウェアに襲われ、データが盗まれたり、消去されたり、感染したり、あるいはその他の方法で侵害されたりした場合、その組織はデータ、プロセス、オペレーション、アプリケーションが復旧するまでうまく機能することができません。この復旧をクリーンかつ迅速に行うことは、ビジネスレジリエンスにとって極めて重要です。

このような現実を踏まえると、データセキュリティとデータ管理に対する包括的なアプローチは、今後も続く世界的な脅威に対する最良の対抗手段です。

今年のグローバル調査では、以下のことが明らかになりました:

1. **ほとんどの組織では、こうした脅威に対処し、事業継続性を維持するために必要なサイバーレジリエンス戦略やデータセキュリティ機能がまだ整備されていない。**
2. **自社の組織がサイバー攻撃後に効果的かつ迅速に復旧できると確信しているITおよびSecOpsの専門家はより少ない。**
3. **サイバー保険は普及しているにもかかわらず、加入が難しく、加入資格に必要となるテクノロジーや重要な能力の項目が多い。**

最終的には、サイバーセキュリティとデータセキュリティおよびデータ管理のためのソリューションを連携、提携、統合できるベンダーと協働する組織が、サイバーインシデントに対する耐性を持ち、そこから復旧し、全体的な事業リスクを低減するために、より優位な立場に立つことができます。さらに、全体的なセキュリティ体制に関する洞察を提供するデータセキュリティとデータ管理プラットフォームを持つ組織は、脅威に耐え、自信を持って復旧することができます。

今日の組織に、準備不足は許されません。

6100022-001 JP 7-2023

COHESITY

COHESITY