Enterprise Strategy Group | Getting to the bigger truth.™

ESGホワイトペーパー

サイバーレジリエンスを確保するためのストレージの役割

著者：スコット・シンクレア（Scott Sinclair）ESG プラクティスディレクター・シニアアナリスト、
モニャ・キーン（Monya Keane）ESG シニアリサーチアナリスト

2022 年 1 月

この ESG ホワイトペーパーは IBM の委託により作成され、

目次

エグゼクティブサマリー

変革がもたらすビジネス資産としてのデータの役割は、ますます大きくなっています。アプリケーション開発への投資の増加や最新の DevOps への移行、およびビジネスインテリジェンス、分析、機械学習の需要の高まりにより、ほぼすべての企業がデータの作成と利用を加速しています。また、データを活用する場所の数も拡大しています。このようなデータの急増と、運用を加速させる圧力の高まりが重なり、IT インフラストラクチャーと IT 運用の両方がますます複雑になっています。

このようなことから、組織やそのインフラストラクチャーは、悪意ある攻撃、人為的なミス、不注意な行為に遭う大きなリスクにさらされています。残念ながら、レガシーな戦略では、このようなインシデントの発生時および発生後の事業運用を適切に継続することはできません。企業は、攻撃やその他の侵害を防ぐために機能を組み合わせようとすることはできますが、機能ギャップ、不十分な統合、複雑な管理により、セキュリティー目標の達成は、時間がかかり、難しくなっています。

組織の考え方を予防からインシデントへの準備に変えること（たとえば、サイバーレジリエンスを備えたストレージソリューションの実装など）は、重要なデータ資産を保護し、ランサムウェアやその他のサイバー攻撃に迅速に対応し、そこから復旧する上での鍵となります。

はじめに

IT は新たな課題に直面しています。ESG が実施した調査では、回答者の約半数（46%）が、現在の IT は 2 年前よりも複雑になっていると回答しています。このような複雑化の要因は、デジタル変革への取り組み（29%）、データ量の増加（35%）、サイバーセキュリティー環境の急速な進化（37%）、新しいデータセキュリティーおよびプライバシー規制への対応（32%）が考えられます。[1]

これだけでなく、組織は重要な IT スキルが不足しているという問題にも直面しています。実際、調査対象組織の 48%が、サイバーセキュリティーの専門家が不足していると回答していて、これは不足している項目の中で最も多く挙げられた項目でした。さらに、これらの組織では、アプリケーション、デバイス、リモート/モバイルワーカーが無秩序に拡大していて、IT が保護すべきセキュリティー境界の規模と範囲が拡大しています。[2]

最新の IT は複雑であり、データは急増し、サイバー攻撃の脅威は増加し続けることから、IT チームはこれらに対応しきれないことがよくあります。社内の人材だけでこの複雑性に対応しようとしても、勝ち目はありません。成功するためには、基盤となるインフラストラクチャーそのものを最新化する必要があります。しかし、ここで IT の意思決定者が必要とするテクノロジーには、アプリケーションのニーズを満たすだけ、または運用を簡素化するだけではなく、それ以上が求められます。真の成功を収めるには、これらの目標を達成し、アプリケーション環境のサイバーレジリエンシーを向上できるテクノロジーが必要です。

急増するサイバー攻撃とランサムウェアの脅威

組織が直面するサイバーセキュリティーの脅威が増加している背景として、サイバー犯罪者が得られる報酬が増加していることが考えられます。たとえば、2020 年に FBI のインターネット犯罪苦情センター（IC3）に米国民から寄せられた苦情は、2019 年から 69%増加し、41 億ドル(120 円換算で約 4920 億円)を超える被害額が報告されています。[3]さらに、過去 5 年間で、IC3 は合計 133 億ドル(120 円換算で約 1 兆 5960 億円)の被害額を報告し

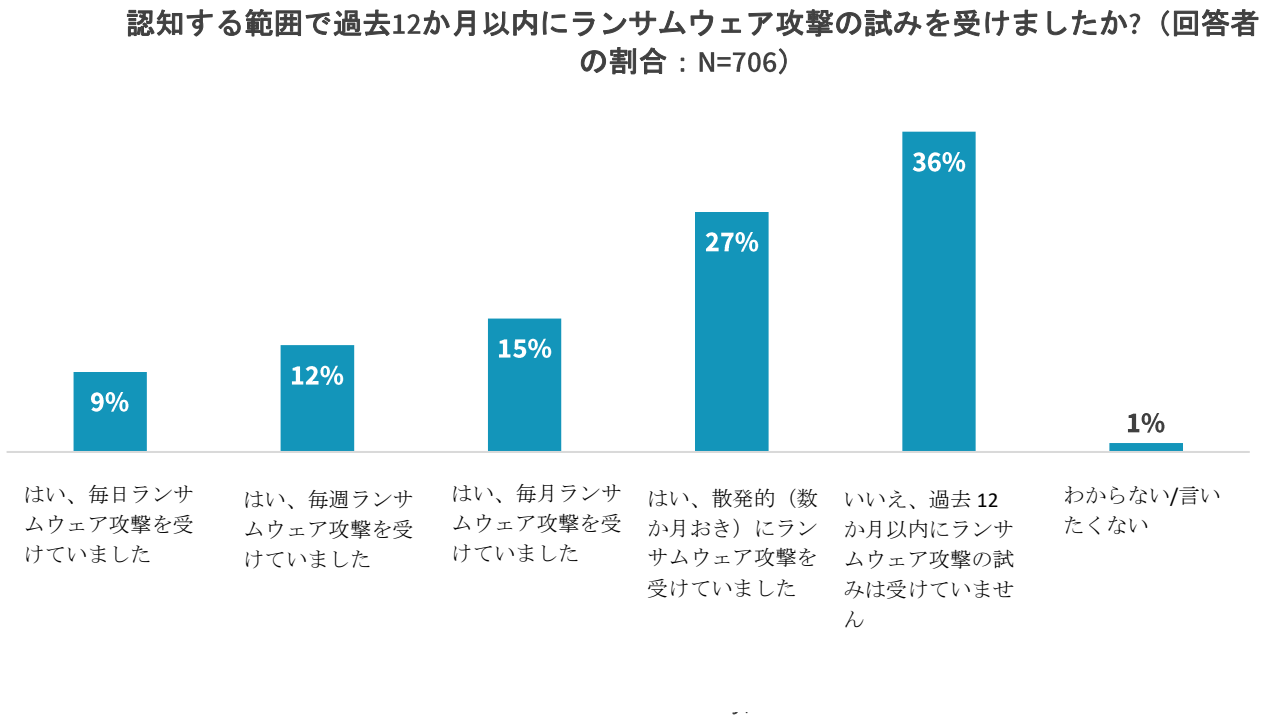
[1] 出典：ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*（2021 年 11 月）
[2] Ibid.
[3] 出典：Federal Bureau of Investigation Internet Crime Complaint Center, *Internet Crime Report 2020*.

ています。[4]米国では、2020 年第 4 四半期における、企業に対するランサムウェア攻撃後の平均中断期間は 21 日でした。[5]ランサムウェアが事業運営にかなりの悪影響を与えていることは明らかです。

IT の複雑さとサイバー攻撃への脆弱性には強い相関関係が存在します。IT が複雑化すればするほど、サイバー攻撃の頻度は高くなり、そのコストも高くなります。

ランサムウェアは、企業の最も価値のある資産であるデータを攻撃する、一般的な脅威です。IC3 は、2020 年に 2,474 件のランサムウェアのインシデントが報告されたことを明らかにしています。また、ESG の調査では、

図 1：回答者の 63%が過去 12 か月にランサムウェア攻撃を経験



出典：ESG, a division of TechTarget, Inc.

ESG-WP-IBM-Cyber-Resiliency-Jan-2022_Figures 1 and 2.xlsx

調査対象組織の 63%が過去 1 年間にランサムウェア攻撃を経験していました。実際、9%が日常的にランサムウェア攻撃を経験しています（図 1 参照）。[6]

ランサムウェア対策に必要なテクノロジー戦略は、従来のサイバーセキュリティーの領域を超えて展開するだけでなく、データストレージとデータ保護の進歩も活用しなければなりません。

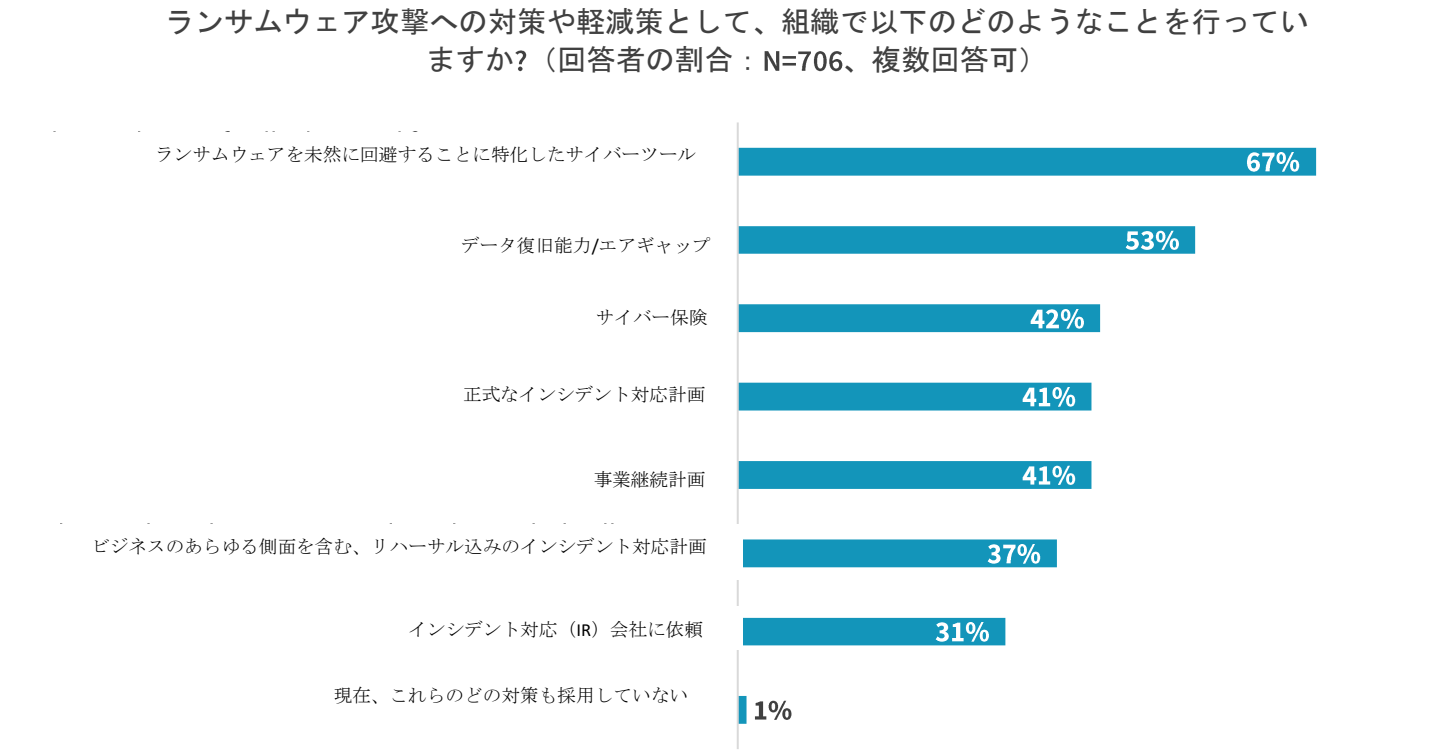
サイバーレジリエンスにおけるデータストレージの役割

ストレージシステムとストレージ管理者はいずれもランサムウェア対策で大きな役割を果たします。ESG が IT 意思決定者に組織で採用しているランサムウェア攻撃への対策や軽減策を尋ねたところ、回答者の 67%は、プロアクティブなランサムウェア回避のためにサイバーツールを使用していると回答し、53%は、エアギャップ

[4] Ibid.
[5] 出典：Coveware ブログ、*Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands*（2021 年 2 月）
[6] 出典：ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*（2021 年 11 月）

などのデータ復旧機能を挙げていました（図 2 参照）。[7]これら 2 つの回答が多く挙げられたことで、攻撃を避けるための対策を実施することの重要性だけでなく、否応なく攻撃が発生してしまった場合に事業を復旧できるソリューションに投資することの重要性も明らかになりました。ランサムウェアの対策や軽減のためのポリシーを設定するだけでは不十分です。このような「部分的」なアプローチでは、攻撃を軽減するための努力は行われていても、効果的なデータ復旧計画が実際に必要になる前に確立する努力はほとんど、あるいはまったく行われていないため、誤った安心感を生み出します。

図 2：一般的に実施されているランサムウェアへの対策または軽減策



出典：ESG, a division of TechTarget, Inc.

ESG-WP-IBM-Cyber-Resiliency-Jan-2022_Figures 1 and 2.xlsx

攻撃への対策は、従来のデータ復旧とはまったく異なるので注意してください。通常、組織はほとんどの場合、最新のコピーを使用してデータを復旧させたいと考えます。しかし、ランサムウェアの場合、通常、IT は使用すべき「正常な」コピーがわからないため、復旧はより高リスク、より長時間になる可能性があります。一部のランサムウェア攻撃は、データだけでなく、バックアップインフラストラクチャーそのものを狙います。このため、高度なストレージ機能は、ランサムウェアからの効果的な復旧の基礎となります。

図 2 に挙げられた対策を採用することは賢明であり、増加する必要はありますが、ランサムウェアからの復旧に 100%有効な単一の防御策はないということを理解しておく必要があります。データの復旧だけでなく、ランサムウェアの特定と回避に特化したツールを検討することは重要ですが、それだけでは不十分です。最良の防御策を講じても、攻撃により破られる可能性はあります。組織は、そのような事態に備え、可能な限り迅速に復旧することでビジネスへの影響を最小限に抑える方法を評価しておく必要があります。ランサムウェアによ

[7] Ibid.

る全体的な被害を最小限に抑えるために、組織は、いかに早く攻撃を特定し、いかに早く被害を軽減し、いかに早く正常なコピーで復旧できるかを追い求める必要があります。

そこで重要になるのが、ハードウェア、ソフトウェア、人、プロセスなど、データにかかわるすべての要素を考慮した、強力なサイバーレジリエンシー戦略です。サイバーレジリエンス体制を構築する組織は、「*どのように保護するか*」という考えから、「*ランサムウェアからどれだけ早く復旧し、どれだけ早くビジネスを正常な状態に戻せるか*」という考えに変える必要があります。

データストレージとデータ保護：ランサムウェアのリスクを最小限に抑えるために重視すべきこと

ランサムウェアからの復旧は、災害復旧の一種ですが、その影響は火災や水害のものとはまったく異なります。火災の場合、完全に鎮火したかどうかを判断できます。ランサムウェアは、壁の中に隠れた火種からいつ再出火してもおかしくないような状況です。ストレージ管理者は、ランサムウェアに関連するリスクを軽減するために特定の分野に注目する必要があります。スピードが重要なので、組織は以下のことをどれだけ早くできるかを判断する必要があります。

- リスクを特定する
- 発生した被害を定量化する
- 既知の正常なコピーを特定し、その正常なコピーを使用し復旧して、最終的に業務を復旧することで被害を軽減する

「自分たちには関係ない」と考えるのは危険です。組織は先回りして、実際に必要になる前に、効果的なデータストレージとデータ保護ソリューションを導入しなければなりません。

IBM によるサイバーセキュリティーからサイバーレジリエンスへの移行

サイバーセキュリティーとリスク管理における豊富な経験があり、サイバーレジリエンスのリーダー的存在として認められている IBM は、以下のような高度なストレージおよびデータ保護ソリューションの包括的なスイートを提供しています。

- IBM FlashSystem、IBM Cloud Object Storage **および** IBM Spectrum Scale：データイミュータビリティと暗号化機能を備えたプライマリストレージソリューションです。
- IBM Tape Storage：データイミュータビリティと暗号化をサポートし、エアギャップによる保護を提供します。
- IBM Spectrum Copy Data Management ソフトウェア：データのコピーを管理および保護します。
- IBM Spectrum Protect Suite による追加保護：Spectrum Protect ソフトウェア定義ストレージは、フラッシュ、ディスク、オブジェクトストレージ、物理テープまたは仮想テープにデータを配置できます。これにより、通常のアクセスパターンからの大きな逸脱を特定することで、マルウェアやランサムウェアの活動を検出します。

- QRadar と Storage Insights のソリューション：AI で強化された機能を使用して潜在的な脅威の検出を加速させます。

IBM Cyber Vault によるサイバーレジリエンス

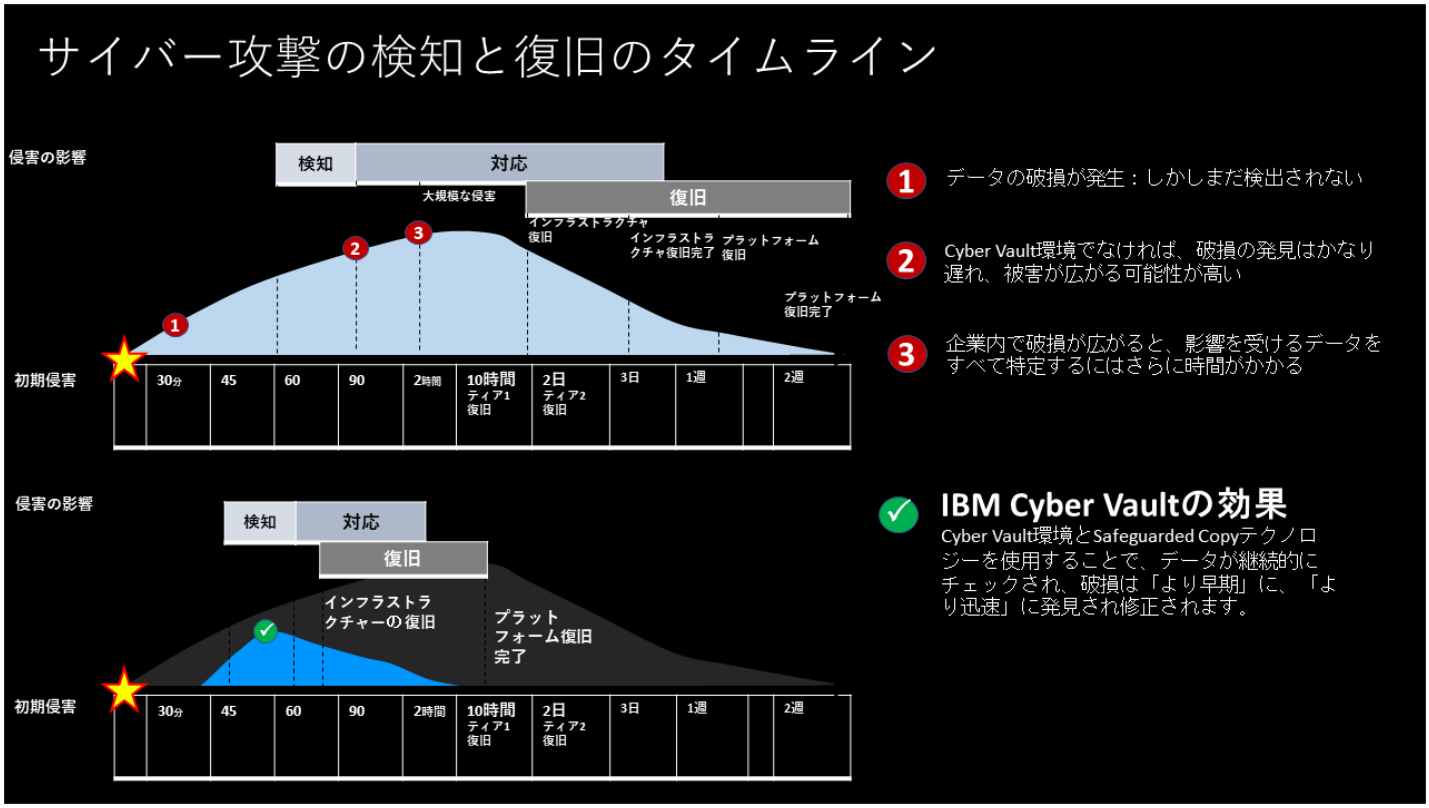
ランサムウェアから保護するためのストレージの役割は、強調してもし過ぎることはありません。プライマリデータに加えられた変更を監視するストレージソフトウェアは、攻撃の開始を特定できる絶好の位置にあります。また、セカンダリコピーを作成および保護するテクノロジーとして、復旧を支援するストレージの役割を極めて重要にします。これらの事実を考慮すると、IBM のサイバーレジリエンシーツールボックスの中で最も有用なツールの 1 つは IBM Cyber Vault です。

IBM Cyber Vault は、サイバー攻撃から迅速に復旧するためのセキュリティー手法です。これは、分離されたイミュータブルなスナップショットを定期的に作成するテクノロジーである IBM Safeguarded Copy の上に構築されています。Cyber Vault は、これらのスナップショットを分析し、ランサムウェアの存在を示す可能性のある悪意ある変更を探します。IBM Cyber Vault は、IBM QRadar および IBM Storage Insights と統合して、さらに迅速な検出を実現します。そのイミュータブルなコピーの検証により、管理者は、正常なコピーを素早く特定し、テストして、それから復元できます。

特に速さを強化するという点では、IBM Cyber Vault は、ストレージ管理者が以下のことを迅速に行えるように支援します。

- **特定**：QRadar および Storage Insights との統合により、検出と監視が強化されます。
- **被害の軽減と定量化**：これは自動化されたプロセスです。攻撃を早期に自動検知することで、攻撃からの迅速な復旧が可能になることは明らかです。
- **既知の正常なコピーの特定**：脅威が検知された場合、データのイミュータブルなコピーの自動化が発生します。
- **業務の復元**：数日や数週間単位ではなく、数時間単位での復旧が可能です（図 3 参照）。

図 3：IBM Cyber Vault によるサイバー復旧の加速



出典：IBM

より大きな真実

IT インフラストラクチャーは、これからもさらに複雑になり、人為的なミス、システム障害、不注意な行為が発生する機会は増えます。同時に、組織の内外を問わず、悪意あるアクターが弱点を探し、それを悪用しようとする努力も絶え間なく続きます。

間違いなく、セキュリティーインシデントは発生します。この事実により、組織は、考え方を「リアクティブ」から「プロアクティブ」に変え、攻撃を防ぐことに集中するのではなく、セキュリティー障害が発生した場合に備え、それに対応することが求められています。これこそが、組織がサイバーセキュリティーからサイバーレジリエンスへと移行するときにやるべき変革なのです。

多くの組織は、NIST Cybersecurity Framework が提供するガイダンスを参考にしてサイバーレジリエンス戦略を作成しています。このガイダンスでは、組織が重要なリソースを特定し、それらのリソースを保護し、障害や侵害を検出し、サイバーインシデントへの対応とそこからの復旧を計画するよう推奨しています。先進的な組織は、複数のデータ復旧オプションを維持しながら、データ発見、コピー管理、暗号化、アクセス制御、イミュータブルなストレージなどの機能によりサイバーレジリエンスを強化できる IT インフラストラクチャー機能に特に注目しています。

IT およびビジネスリーダーにとって、サイバーレジリエンスとは、事業運用を維持するためにテクノロジーとビジネスについて正しい意思決定をすることです。

Enterprise Strategy Group は、テクノロジー分析、リサーチ、戦略を統合した会社であり、マーケットインテリジェンス、実用的なインサイト、Go-to-Market コンテンツサービスをグローバル IT コミュニティに提供しています。

www.esg-global.com contact@esg-global.com 508.482.0188