the GORILLA GUIDE® to...

クラウドサイバーレジリエンス

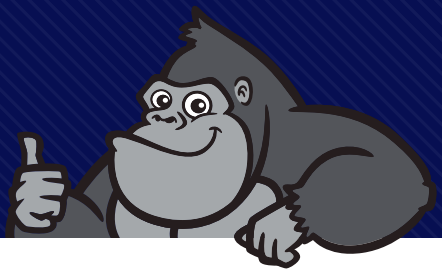
マルチクラウド / ハイブリッド環境で組織のデータを保護する方法

LAWRENCE MILLER

rubrik

POWERED BY ActualTech MEDIA

the GORILLA GUIDE® to...



クラウドサイバーレジリエンス

マルチクラウド / ハイブリッド環境で組織のデータを保護する方法

著者 ： Lawrence Miller

POWERED BY ActualTech MEDIA

Copyright © 2024 by Future US LLC
Full 7th Floor
130 West 42nd Street
New York, NY 10036

無断転載を禁じます。 本書または本書のいかなる部分も、 書評で簡単に引用する場合を除き、 出版社の書面による明示的な許可なく、 いかなる方法においても複製または使用することを禁止します。 アメリカ合衆国で印刷。

www.actualtechmedia.com

謝辞

コンテンツ配信ディレクター
Wendy Hernandez

グラフィックデザイナー
Olivia Thomson

スマートスタジオ責任者
Katie Mohr

特別寄稿社 ： RUBRIK
Daniel Lu
クラウド製品マーケティング

Amanda O’ Callaghan
コンテンツマーケティング責任者

著者について

Lawrence Miller （CISSP） はさまざまな業界で 20 年以上の経験を持つ情報セキュリティのプロフェッショナルです。 情報技術やセキュリティに関する多様なテーマで 200 冊以上の著作があります。

ジャングルへの入口

Chapter 1: 防御だけでは不十分な理由 7

サイバー攻撃の普及 7

サイバーレジリエンスの説明と重要な理由 10

攻撃下でも事業運営を可能にする新戦略の必要性 11

Chapter 2: クラウド内のデータ保護に関する課題の認識 12

クラウドスプロールによる攻撃対象領域の拡大 12

クラウドを標的にする攻撃の増加 13

Chapter 3: 他の組織で現在実践しているサイバーレジリエンス 15

無為無策 15

DIYで対応 17

レガシーなオンプレミスツールへのリフト＆シフト 18

クラウドベンダーのネイティブバックアップツール 20

Chapter 4: クラウドサイバーレジリエンス向けのより良いソリューション 23

シンプルで一元化された保護 24

包括的なサイバーレジリエンス 25

クラウド向けに構築 25

迅速な復元 26

TCOの削減 27

まとめ 27

本書で使用されているアイコン

SCHOOL HOUSE
「コールアウト」では主要テーマからは外れるとしても、重要ポイントについて有益な情報を記載しています。

FOOD FOR THOUGHT
ここは特別なコーナーで、本書内で紹介される補助的な話題について、少し詳しく説明しています。

BRIGHT IDEA
すばらしい思い付きがある場合には、名案コーナーに目印の電球を示してお知らせします。

DEEP DIVE
特定のテーマについて、深く掘り下げます。

EXECUTIVE CORNER
ビジネスリーダーにとって戦略的に関心の高い事柄について考察しています。

定義
用語、フレーズ、概念について定義しています。

GPS
正しい認識へと導くお手伝いをします。

ナレッジチェック
読み終わった箇所についての知識をテストします。

注意
重大なミスをしないよう必ずお読みください。

重要
必ず確認していただきたい箇所です。

ヒント
読んだ箇所に基づいたお役立ちアドバイスです。

はじめに

ゴリラガイド®「クラウドサイバーレジリエンス」へようこそ。 本書では、 急速に進化を遂げている脅威の状況と、 防御のみに頼ったサイバーレジリエンス戦略ではクラウド内にある組織のデータを十分に保護することができない理由についてご説明します。

今日のクラウドサイバーレジリエンスに対する一般的なアプローチを一部ご説明し、クラウド内の組織データを保護し、 真のクラウドサイバーレジリエンスを実現するためのより良いソリューションをご紹介します。

それでは、 さっそくページをめくって始めましょう。

CHAPTER 1

防御だけでは不十分な理由

重要なアプリケーションやデータをクラウドに移行する組織が増えるにつれ、サイバー犯罪者は戦術を変え、 クラウド内の「標的が豊富な環境」に焦点をあてています。 この変化の激しい脅威に満ちた環境を考慮すると、 組織は「侵害を想定する」という考え方を採用する必要があります。 したがって、 データのセキュリティと事業の存続を確保するには、 防御のみに焦点をあてたサイバーセキュリティ戦略ではもはや十分ではありません。 代わりに、 サイバーセキュリティとクラウドサイバーレジリエンスに対するより包括的なアプローチが必要になります。

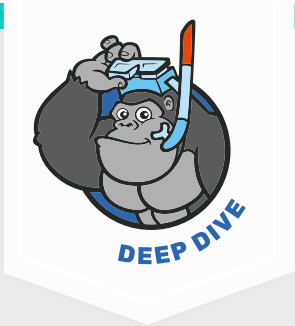
サイバー攻撃の普及

攻撃者は、 企業の貴重なデータを盗み出そうとますます執拗で巧妙になっています。 先ごろの Rubrik Zero Labs のレポートでは、 この問題の規模を明確に示しており、 94% の組織がサイバー攻撃の標的になっています。 これらの攻撃は、 ある一か所だけの脆弱性に限定されるものではありません。 同レポートでは、 多くの組織が SaaS （67%）、 クラウド （66%）、 オンプレミス （51%） など、 複数の環境にわたって攻撃を受けていたことが明らかになりました。

近年のクラウドインフラの複雑さにより、 この問題はさらに深刻になり、 クラウドスプロール （クラウド環境の無秩序な増大） により、 攻撃対象領域は大幅に拡大しました。 このような拡大に伴い、 データを保護することはさらに難しくなっています。 セキュリティの専門知識が必要ですが、 多くの組織においては現在、 それが足りていません。

近年、 ランサムウェアは攻撃力を増しています。 ランサムウェアに関する世界的なコストは 2021 年に 200 億ドルに達すると予測されましたが、 専門家は 2031 年までに 2,650 億ドルに急増すると予測しています。

DORA （キャラクター名ではありません）



デジタルオペレーションレジリエンス法（DORA）は、金融サービス機関のサイバーレジリエンス機能を促進する目的で制定された欧州連合（EU）の規制です。この法律は、EU 加盟国の金融サービス組織、 および EU と取引を行う金融サービス組織に対し、 従来の検出と保護のアプローチではなくレジリエンスと復元を重視することで、 サイバー攻撃などの業務中断への対応を改善するよう求めるものです。

対象の金融機関に重要なサービスを提供する組織も、 DORA 規制に準拠する必要があります。 準拠しない場合、 全世界の年間総売上 （商品またはサービスの販売による収益） の最大 2% に相当する罰金が科せられる可能性があります。

実際に攻撃を受けると、 身代金の金額だけではなく、 ダウンタイム、 収益の損失、 復旧の費用、 風評被害、 法規制順守の罰則などが必然的に発生します。 注意しておきたいのは、「サイバー犯罪者に仁義なし」ということです。 たとえ攻撃者がデータを復元するための復号ツールを提供したとしても、 機密データがダークウェブで販売されないという保証はありません。

サイバー攻撃を受けた場合の総コストは多くの場合、 数百万ドルになります。 完全に復旧ができたとしても、 数週間から数か月かかり、 影響を受けた組織には長期的な影響が残ります。

世界規模で見ると、 今年はサイバーセキュリティに 2,000 億ドル以上が投じられる見通しで、 企業のセキュリティチームの中には対策のために 75 以上のツールを使用しているところもあります。 これほど多額の投資をしていても、 攻撃者は依然として侵入しては大損害を与え、 事業や評判、 キャリアを脅かしています。

- UnitedHealth Group （UHG） 社は 2024 年 2 月のランサムウェア攻撃で 8 億 7,200 万ドル以上のコストがかかり、 直接コストは総額 10 億ドルを超えると報告されています。
- MGM Resorts International 社は 2023 年 9 月のデータ流出で 10 日間のダウンタイムが発生、 その結果、 第 3 四半期の業績に 1 億ドルの打撃を受けました。
- Clorox 社がサイバー攻撃を受けたことが 2023 年 8 月に公表され、 結果として約 5 億ドルの収益損失、 30 億ドル以上の評価損失、 サプライチェーンの不足が生じ、 最高情報セキュリティ責任者 （CISO） が退任しました。

これらの例は、 企業が通常の業務を迅速に再開できない場合、 サイバー攻撃のコストが指数関数的に増加することを示しており、「常時接続」のデジタル世界においてサイバーレジリエンスの重要性が高まっていることを如実に示しています。

サイバーレジリエンスの説明と重要な理由

サイバーレジリエンスとは、 運用を効率的に継続しながらサイバー攻撃やデータ侵害に対して対策・対応・復旧できるようにする組織の能力です。 米国立標準技術研究所（NIST） はサイバーレジリエンスの定義を「サイバーリソースを使用する、 あるいはサイバーリソースで機能するシステムに影響を及ぼす悪条件、 ストレス、 攻撃、 または侵害を予測・対処し、 そこから復旧、 適応する能力」としています。

今日の脅威をめぐる環境において、 強固なサイバーレジリエンス能力を備えることは、企業や組織にとって必須です。 防御でサイバー攻撃を阻止できなかった場合、 迅速に対応して復旧する能力が、 事業を存続させるうえで不可欠です。

Information Technology Intelligence Consulting（ITIC）の『2024 Hourly Cost of Downtime Survey』によると、中～大規模の企業の90%以上で、ダウンタイム1時間の平均コストが30万ドルを超えていることが明らかになりました。

被害は攻撃自体によるものだけではありません。 攻撃 （ランサムウェア攻撃やサービス拒否攻撃など） によるものであれ、 組織のインシデント対応作業 （封じ込めや根絶） によるものであれ、 それらいずれか一方、 あるいはその両方が組み合わさって直接的な被害を及ぼすため、 コストがかかるダウンタイムは免れません。 例を挙げると、Colonial Pipeline 社は 2021 年 5 月にランサムウェア攻撃を受けた際、 同社の CEO はランサムウェアの拡散を阻止するために、 攻撃の影響を受けた重大なシステムをシャットダウンする決断を迅速かつ的確に下しました。 迅速で効果的な対応をして、身代金 440 万ドルの支払いを決定したにもかかわらず、 通常運用の再開までには数日かかり、 米国東湾岸の燃料供給が途絶えて米国の 4 州 （バージニア州、 ノースカロライナ州、 ジョージア州、 フロリダ州） に非常事態宣言が発令されました。

つまり、 停止期間が長いほど収益への影響が大きくなるということです。 ダウンタイムは事業や顧客にマイナスの影響を及ぼし、 Colonial Pipeline 社のようにサプライチェーン全体に影響を与えることもあります。 **すなわち、 サイバーレジリエンスはビジネスのレジリエンスなのです。**

攻撃下でも事業運営を可能にする新戦略の必要性

従来のサイバーセキュリティ業界では、 攻撃を防ごうと、 エンドポイントやネットワーク、アプリケーションなどのさまざまなレイヤーで高い壁や広い堀を建設することに追われてきました。 そして新種の攻撃が出現するたびに、 それに対する新しい「必須の」防御ツールが登場します。防御は必要ですが、それだけでは攻撃に対抗できません。現在のクラウドアプリケーションは一極集中型ではなく、 マルチクラウドやハイブリッド環境に分散しているため、 従来の防御方法でセキュリティを確保することが難しくなっています。サイバー攻撃から復旧するために組織は、 インフラのセキュリティよりもサイバーレジリエンスを優先する必要があります。データが安全で利用できる状態であれば事業を継続できるため、組織はデータそのものの安全性を確保しなければなりません。

CHAPTER 2

クラウド内のデータ保護に関する課題の認識

クラウド内のデータを保護するには、 クラウド特有の課題が伴います。 クラウドを使用するメリットの 1 つは、 リソースを簡単にスピンアップ （実際に準備できるために準備） できることです。 その柔軟さから、 データは複数のアカウント、 リージョン、 サービス、 クラウドにまたがって容易に広がります。 この挙動により、 何がどのように保護されているのかを追跡することが困難になります。 それ以上に重要なことは、 何が保護されていないのかを特定するのが難しいことです。 攻撃者はこのことをよく知っているため、 結果的にますますクラウド内のデータを標的にしているのです。

クラウドスプロールによる攻撃対象領域の拡大

クラウドに関して言えば、「良いものも度が過ぎると問題である」 と思うことがあるでしょう。 クラウドは利用している顧客にとっては多くのメリットがありますが、 クラウドスプロール （無秩序な増大） は現在、 組織にとって深刻な問題となっています。 クラウドスプロールによってコストがかさむだけでなく、 攻撃対象領域が大幅に拡大したり、 設定ミスのリスクが増加したりすることから、 データ流出につながる可能性があります。

クラウドスプロールはたいていシャドウデータが原因です。 シャドウデータとはつまり、 IT 部門やセキュリティ部門にきちんと管理・保護されていないまま作成・保管・共有されたものを意味します。 多くの場合、 同じ組織内のさまざまな事業部や部門が、

個々のニーズに合わせて異なるクラウドプロバイダーから独自のクラウドサービスを調達します。 たとえば、 ある組織の開発者は強力な開発エコシステムを決め手として Google Cloud Platform （GCP） を利用し、同じ組織のマーケティングチームは使い勝手の良さと Amazon Marketplace との相性の良さから Amazon Web Services （AWS） を選択し、さらに同組織のインフラ＆オペレーション （I&O） チームは広範な Windows サービスを利用するためにシステムを Microsoft Azure へ展開する、 といった具合です。

このような状況では、 アカウント / テナント / サブスクリプションのサイロ化を招くだけでなく、ユーザーのアクセス制御やセキュリティポリシーも別々になります。 すべてのクラウドサービスにまたがる、 明確で一貫したセキュリティ体制の見通しがなければ、 防御の隙間が必ず生じます。 こういった可視性と制御能力の欠如は、 データを危険にさらすだけでなく、コンプライアンス要件を満たすことも困難にします。

クラウドを標的にする攻撃の増加

残念な現実ですが今日では、 自分の組織がサイバー攻撃の標的にされるかどうかではなく、「いつ標的にされるか」が問題になっています。 クラウドはこれらの問題を魔法のように解決してくれるわけではありません。 実際、 2022 年には毎月 94% のクラウドテナントが標的になっており、これらのテナントのうち 62% が現実に侵害を受けています。 特にランサムウェア攻撃はますます一般的になっています。 ガートナー社の報告によると、2025 年までに 75% の組織がランサムウェア攻撃に直面する、 と言われています。

また、 攻撃者が「二重脅迫型」ランサムウェア攻撃で組織を標的にするケースも増えています。 これは、 追加の支払いに応じないと組織の機密データを公開する、と脅迫する手口です。 さらに進んだ「三重脅迫型」ランサムウェア攻撃も登場しています。 この攻撃では、 攻撃者が標的の組織に対して DoS （サービス拒否） 攻撃を仕掛けたり、 最初のランサムウェア攻撃で侵害された個人データの各被害者に対して身代金の支払いを強要したりします。

また、 サービスとしてのランサムウェア （RaaS） の拡がりで、 技術的な専門知識が限られている攻撃者でも、 料金または手数料を支払って、 他人が構築および / または管理するランサムウェア攻撃のライセンスを取得し、 攻撃を仕掛けることも容易になりました。 RaaS の多くのプロバイダーは、 ライセンスを取得した攻撃者に対し、 技術サポート、収集サービス、その他の「付加価値のある」管理サービスも用意しています。

データを復元するために身代金の支払いを決断した組織は、自らの責任でリスクを負うことになります。身代金を支払ったとしても、データが復元できるとは限りません。実際、2023年のRubrik Zero Labsのレポートによると、身代金を支払った組織のうちデータをすべて復元できたのはわずか16%で、46%は半分以下のデータしか復元できませんでした。組織は身代金を支払う決断をする前に、法執行機関と弁護士の両方に相談するべきです。

こうした不可避の攻撃に対策するために今、 何をするかによって、 実際に攻撃を受けてしまうのか、 そして攻撃を受けたとしてもビジネスがどのような損害を受けるのか、 が決まってきます。 サイバー攻撃の被害からビジネスを守るための最善策の 1 つは、 サイバーレジリエンスの戦略を立てることです。

CHAPTER 3

他の組織で現在実践しているサイバーレジリエンス

防御だけでは不十分であることや、 クラウド内のデータ保護がますます困難になっていることを理解すると、 ほかの組織が現在実施しているサイバーレジリエンスについて興味が湧いてくることでしょう。 この章では、 現在のサイバーレジリエンスに対して最も一般的な 4 つのアプローチについてご説明します。

無為無策

バックアップと復元に対するこの最初の選択肢は、 実際には選択肢ではありません。 しかし多くの組織は、 データをクラウドへ移行すればデータ保護とサイバーレジリエンスのニーズにも対処できるという誤った認識を持っています。 その結果、 これらの組織は基本的に何もしません。 このような危険な思い込みは、 以下のような一般的な誤解から生じています。

- **責任共有モデル。** すべてのパブリッククラウドプロバイダーには責任共有モデルがあります （**図 1** 参照）。 このモデルは技術スタックのコンポーネント （物理的なインフラ、 ネットワーク、 仮想化、 オペレーティングシステム、 アプリケーション、 データなど） のうち、 どれがクラウドプロバイダーの責任で、 どれが顧客の責任かを示すものです。 責任共有モデルは、 クラウドプロバイダーやサービスモデルによって、 サービスとしてのソフトウェア （SaaS）、 サービスとしてのプラットフォーム

（PaaS）、サービスとしてのインフラ （IaaS） など若干異なります。ただし、 これらのすべてに共通することは「顧客は必ず自分のデータに責任を持つ」ということです。

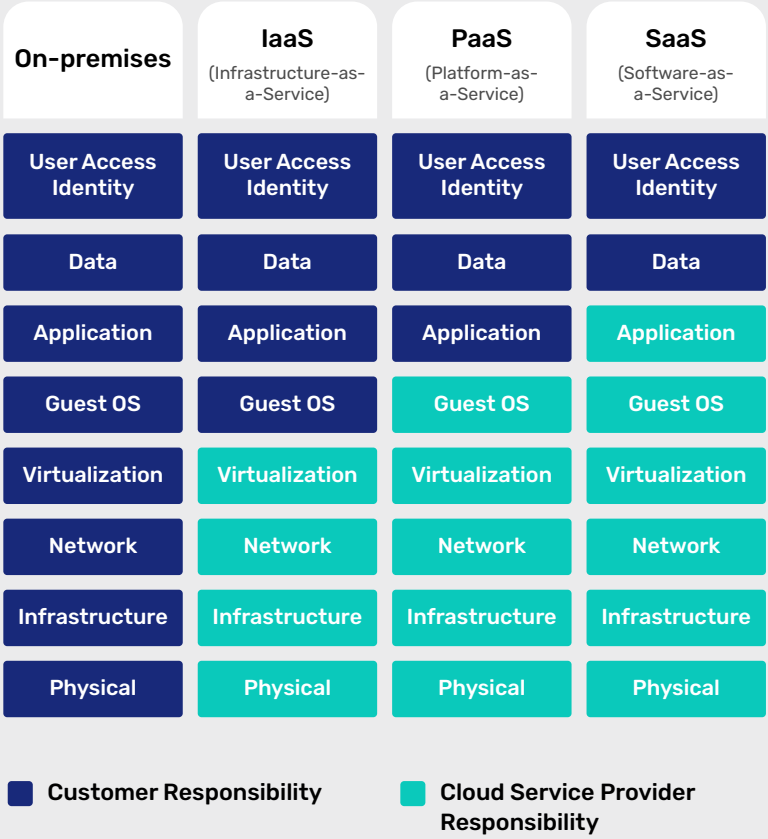


FIGURE 1: 責任共有モデルの例

- **高い信頼性。** 主要なクラウドプロバイダーはすべて、 鉄壁の「99.999% （またはそれ以上）」の可用性 （稼動時間） と「99.999999999%」の耐用性 （データ完全性） を備えた強固なインフラとサービスを提供しています。 確かに、 そのレベルの信頼性があればデータを失うことはないでしょう。 ただし、 高い信頼性とサイバーレジリエンスは同じものではありません。 高い信頼性は、 ハードドライブやサーバーといったハードウェアの障害に起因する重要システムのダウンタイムを最小限にするものであり、 サイバーレジリエンスはサイバーセキュリティのインシデントを迅速に検出し、 対応して復旧できるようにするものです。

- **顧客側の計画不足は、 クラウドプロバイダー側の緊急事態には該当しません。** クラウドプロバイダーはデータをバックアップし、 他のデータセンターやリージョンへ複製しますが、 これはサービスレベル契約 （SLA） を満たすためであり、 顧客のサイバーレジリエンスを確保するためではなく、 彼ら自身のサイバーレジリエンスを確保するためです。 また、 クラウドプロバイダーはデータが有効であることを保証するために何かをするわけではありません。 元のデータがサイバー攻撃ですでに暗号化されている場合、 複製したバックアップコピーも暗号化されています。 悪意のある内部関係者が、 ランサムウェア攻撃で重要なファイルを削除したり、 特権アカウントを侵害し、 それを使用してデータを暗号化したりした場合、 クラウドプロバイダーはデータを復元しません。

DIY で対応

一部の組織では、バックアップと復元のニーズに対応するためにDIY(自社で作り上げる) という方法を選択します。 自社製のバックアップツールには通常、 カスタム開発されたソフトウェアやスクリプトベースのソリューションが含まれており、 組織特有の要件に対応するように特別に作成されています。 ただし、 このようなツールは複雑さと機能の点でかなりばらつきがあります。自社製ツールはきめ細かなカスタマイズと制御を可能にしますが、以下の点においていくつか重要な問題があります。

- **コスト （実費と機会コスト）。** 自社製ツールはデータのライフサイクル全体にわたって開発・管理・更新に多大なリソースを必要とします。これは、 希少で価値の高いリソース、 つまりアプリケーション開発者が、事業の中核を支える戦略的で付加価値の高いプロジェクトに携わる機会を奪うことになります。

- **拡張性。** 自社製ソリューションはたいてい、 特定の環境において、特定の種類のデータをバックアップするなどといった、 限られた問題を解決するために構築されます。 アプリケーションのアーキテクチャが進化すると、 おそらく別のクラウドに移行しますが、 その場合にはこれらのツールやスクリプトをそれぞれのクラウドのアカウント、 テナント、 サブスクリプションに合わせて調整する必要があります。 そのため、 データ量が増加し、 インフラがますます複雑になり、 拡張が困難になります。最後に、 データのバックアップは比較的簡単なことです。 留意すべき大変な点は、 バックアップの期限を切らさないように注意することや、バックアップの保存に対する無期限の支払いを避けることです。

- **セキュリティとコンプライアンス。** 自社製ソリューションには、 リスクを最小限に抑え、 規制コンプライアンスに確実に準拠するために必要な高度なセキュリティ機能が欠けていることがよくあります。

レガシーなオンプレミスツールへのリフト＆シフト

一部の組織は、 既存のオンプレミスのバックアップおよび復元ツールを （自社製か既製品かを問わず） クラウドへ単純にリフト＆シフトしようとします。 残念ながらこのアプローチはたいてい、 クラウド戦略を採用する際に組織が求める俊敏性や弾力性を妨げます。 なぜなら、 これらのレガシーツールはクラウド向けに設計または最適化されたわけではないからです。 これらのツールはクラウドネイティブなサービスを利用できないため効率が悪く、 パフォーマンスが低下し、 コスト上昇につながります。 また、 このようなリフト＆シフトでは、 さまざまなアプリケーションやクラウドのデータを保護する別々のツールが必要となり、 分断された環境が生じることになります。 そのため、 データの場所に

関わらず組織のすべてのデータに対して一貫した保護を提供することは、 IT 部門にとって難しくなります。 レガシーなオンプレミスバックアップツールをクラウドに後付けする場合には、そのほかにも次のような課題が生じます。

- **レガシーバックアップはサイバー攻撃に対して脆弱です。** レガシーバックアップは、 書き換え不可の特性を備えたゼロトラストアーキテクチャに基づく適切な認証とアクセス制御がないことが多いため、攻撃者は脆弱性を悪用して機密データに不正アクセスできるようになり、 組織のセキュリティ体制が危険にさらされます。 また、 これらのシステムではオープンストレージプロトコルを頻繁に利用しているため、悪意のある攻撃者による不正アクセスや不正操作にデータがさらされることになります。

- **レガシーバックアップは、 サイバー攻撃中にどのデータが危険にさらされているか、 または何が侵害されたかについて、 重要なインサイトや可視化を提供していません。** レガシーバックアップおよび復元ツールを使用して、 何を復旧すべきか、 攻撃がいつ起こったのか、 悪意のあるアクターがどこまで侵入したのか、 それによる被害の範囲がどの程度かを特定するのは、 非常に困難な作業になりえます。 このばらばらな情報をつなぎ合わせるのは非常に時間がかかり、 復旧プロセスを著しく遅らせる可能性があります。 また、 明確なポイントインタイム（特定の時点の） バックアップを指定する機能がなければ、 組織は侵害されたバックアップから再感染するリスクを負うことになります。

- **レガシーバックアップツールはクラウド向けに構築されていません。** オンプレミス環境は、 動的性質が高いクラウドに比べると、 比較的静的です。 レガシーバックアップツールは通常、API を利用したオペレーションや IaC （コードとしてのインフラ） の原理をほとんど、 あるいはまったくサポートしておらず、 クラウドネイティブな構成、 メタデータ、ステートレスコンポーネントを取得できず、 クラウドネットワークのレイテンシと帯域幅の制約に対して最適化されていません。 そのため、クラウドには適していません。

クラウドベンダーの ネイティブバックアップツール

これは最後の選択肢ですが、多くの組織はバックアップと復元のニーズに対応するために、クラウドプロバイダーのネイティブツールを利用しています。 クラウドネイティブなバックアップツールは、 クラウドプロバイダーそれぞれのクラウド環境のデータをバックアップするために特別に設計・最適化されたサービスです。 これらのツールは、 クラウドプロバイダーが提供する他のサービスとシームレスに連携し、 基本的な （場合によっては高度な）バックアップと復元機能を提供するため、 クラウドで基本的なバックアップ機能を必要とする顧客の間で人気のある選択肢となっています。 組織がクラウドプロバイダーのネイティブツールを使用する主な理由は、「簡単だから」 時間を節約できると感じているからです。ただし、「簡単」は必ずしも「正しい」という意味ではありません。

一部の組織はネイティブバックアップおよび復元ツールがあれば「十分である」と考えていますが、クラウドサイバーレジリエンスに対して「十分である」というアプローチでは、最新の脅威から重要なデータや事業を守ることはできません。

すでに特定のクラウドプラットフォームに投資している企業にとっては、 ネイティブのクラウドバックアップソリューションを採用することは便利に思えるかもしれませんが、 ネイティブのバックアップツールは一般的に、 クラウド上で組織の重要なデータのサイバーレジリエンスを実現するために必要な柔軟性・拡張性・能力・機能が不足しています。 また、 ネイティブツールは複雑で使いにくいこともあります。 そしてもちろん、 ネイティブツールはクラウドプロバイダーの環境内にあるデータのみを保護することに重点を置いているため、 ほかのクラウドやオンプレミスのデータセンター内のデータを保護することは意図していません。そのほかにも、 ネイティブバックアップツールに関連して次の課題が挙げられます。

- **マルチクラウドやハイブリッドに対応していない。** 多くの場合、 クラウドネイティブツールは AWS や GCP、 Microsoft Azure などの単一のクラウド環境向けに構築・最適化されています。 この制約により、 複数のクラウド、 SaaS アプリケーション、 オンプレミスのインフラにまたがってバックアップと復元を管理することは困難になります。 これらは基本的に専用ツールであり、 他のクラウド環境をサポートしているとしてもその機能は限られており、 顧客はデータエグレス料金 （データ通信料） を請求される可能性があります。

- **管理が分断される。** 同じクラウド環境内でも、 これらのツールはワークロードごとに管理アプローチが分断されている可能性があり、 包括的なデータ保護を実現することは難しく、 クラウドアカウントごとに個別の管理と設定が必要になります。 また、 これらのツールではワークロードごとに異なるアプローチを採用している場合があります。 スナップショットのようなもの、 ベーシックなバックアップのようなもの、 書き換え不可に対応しているもの / していないもの、 長期保存できるもの / できないものなどさまざまで、非常に複雑になっている可能性があります。

- **セキュリティに関するインサイトが限定的。** クラウドネイティブなバックアップツールは、 データ脅威分析およびセキュリティ体制管理の機能を備えていないことが多いため、 環境を監視して不審な活動を見つけたり、 潜在的なサイバー攻撃を検出したり、 機密データのリスクを特定することは困難です。

- **バックアップストレージにコストがかかる。** クラウドネイティブなツールでは一般的に、 バックアップデータを保存するためのコストが最適化されていません。 そのため、 バックアップデータの保存にかかるコストが元のデータ自体の保存コストよりも高くなることがあります。 たとえば AWS Backup では、 S3 バックアップデータの保存コストは 0.05 ドル /GB/ 月で、元のデータの保存コスト（0.022 ドル /GB/ 月）よりも高くなります。

CHAPTER 4

クラウドサイバーレジリエンス向けのより良いソリューション

データ保護に対する従来のアプローチ （何もしない、 DIY での対応、レガシーなオンプレミスツールのリフト＆シフト、 クラウドプロバイダーのネイティブツールの使用） には、 いずれも真のクラウドサイバーレジリエンスに必要なエンタープライズレベルの機能 （検索やファイルレベルの復元、論理的に隔離されたバックアップ、機密データの検出などの高度なセキュリティ機能） が欠如していることがよくあります。 クラウドサイバーレジリエンスにとって、より良いアプローチが必要なのは明らかです。 しかし、 クラウドサイバーレジリエンスのソリューションに対して一体何を求めればよいのでしょうか？ 理想的には、クラウドサイバーレジリエンスのソリューションは以下の機能と特徴を念頭において構築するべきです。

- シンプルで一元化された保護
- 包括的なサイバーレジリエンス
- 迅速な復元
- 総保有コスト （TCO） の削減

シンプルで一元化された保護

企業はパブリッククラウドサービスを継続して使用するにつれて、 サイバーレジリエンスを保証し、 コンプライアンスを証明するために、 何十・何百ものクラウドのアカウントとサブスクリプションにおいて基準のバックアップを取得することが難しくなっています。 一貫したポリシーを大規模に実装するには、 手動でのジョブのスケジュール管理や手間のかかるスクリプト作成が必要になり、 IT の生産性が低下します。 組織は、 独自のビジネス要件に対応する最善の組み合せのソリューションを選択するため、 マルチクラウドやハイブリッド環境は、 ますます一般的になっています。 しかし、 マルチクラウドやハイブリッドの戦略では、 ばらばらなクラウドリソースやツールを設定・管理するために、 さまざまな環境にまたがる専門的なスキルを必要とするため、 リスクの高い設定ミス、 運用の非効率性、 一貫性のないデータ保護につながることが多くなります。

そのため、 求められるクラウドサイバーレジリエンスのソリューションは、 SaaS アプリケーションやオンプレミスのデータセンターといったマルチクラウドやハイブリッドクラウド環境を対象とする単一のプラットフォームを提供するものになります。 その際に、 AWS、 GCP、 Microsoft Azure などの主要なパブリッククラウドプロバイダーをすべてサポートしていることが必須です。 このソリューションは、 SaaS やオンプレミスのアプリケーションだけでなく、 クラウドのワークロードを自動で検出・保護し、 データ保護ポリシーの設定、 バックアップの可視化、 データの復元、 コンプライアンスと可監査性を実現するための中心的な制御ポイントにする必要があります。 最後に、 このソリューションでは、 アウトオブバンド方式の管理 （通常とは別の管理） を提供して、 データ保護スタックが本番用スタックとは独立して実行されるようにします。

2023 年の Rubrik Zero Labs のレポートによると、 10 社中 9 社が「サイバー攻撃中に、 悪意のある攻撃者がデータのバックアップにアクセスしようとして、 その 73% が部分的に成功した」と報告しています。

包括的なサイバーレジリエンス

求められるクラウドサイバーレジリエンスのソリューションは、 すべてのデータソースについてサイバー攻撃、悪意のある内部関係者、および運用の中断に対抗できるように設計され、自動化・完全隔離・書き換え不可・アクセス制御可能の特性を備えたバックアップによって、クラウドデータの整合性と可用性を保証できるものになります。 このソリューションは、機密データを正確に特定し、 異常や脅威 （ランサムウェア、 データ破壊、 侵害の兆候など） に対してデータを継続的に監視し、 保護されていないデータや危険にさらされているデータについてインテリジェントなインサイトを提供して、 データのセキュリティ体制を最大化できるようにする必要があります。 個人を特定できる機密情報 （PII） が侵害された場合に迅速な通知が必要とされる規制 （EU 一般データ保護規則 （GDPR） やカリフォルニア州消費者プライバシー法 （CCPA）） の対象となっている組織にとって、攻撃の範囲と潜在的な機密データの暴露を判断することは特に重要です。

クラウド向けに構築

クラウドサイバーレジリエンスのソリューションはクラウドネイティブで、 かつ次のような優れた設計原理に基づいて構築する必要があります。

- **ソフトウェア定義 ：** 異なるハードウェアおよびソフトウェアのコンポーネント （オンプレミスのプラグアンドプレイアプライアンス、 サードパーティのハードウェア上のソフトウェア、 クラウド上のソフトウェアなど） を、展開の柔軟性を備えた 1 つのソフトウェアファブリックに統合します。
- **スケールに応じてシンプルに対応 ：** 管理の複雑さを解消するリニアスケールアーキテクチャにより、 急激に増加する情報量を簡単に処理します。
- **クラウドモビリティ ：** オンプレミスまたはパブリッククラウドのどちらに展開されている場合でも、 クラウドおよびアプリケーションのモビリティによって、クラウドネイティブなアプリケーションの保護、 アプリケーションおよびファイル間の検索、 テスト / 開発用または災害復旧用のインスタンスの迅速なスピンアップを実現します。

- **API（アプリケーションプログラミングインターフェイス）ファースト：** 業界標準の OpenAPI ドキュメント、 サンプルコード、 さまざまな自動化ツールとの事前構築済みの統合により、 ユーザーの API 利用をサポートするような、簡単に拡張できるデータ管理ソリューションにします。
- **エンドツーエンドのセキュリティ：** 転送時および保存時のデータ暗号化、書き換え不可の無制限のスナップショット、 きめ細かなアクセス制御など、包括的で多面的なセキュリティアプローチにより、 ライフサイクル全体にわたってデータを保護します。

迅速な復元

クラウドで 1 つのワークロードインスタンスを復元することは、 多くの場合、 手動による複数ステップのプロセスです。 このプロセスはクラウドサービスやプロバイダーによって異なります。 組織で実施しなければならない手動のステップが多いほど人為的なミスが生じる可能性が高くなり、 データを復元して通常の運用を再開するまでにかかる時間も長くなります。

そのため、 求められるクラウドサイバーレジリエンスのソリューションは、 クラウドバックアップデータ全体でグローバルな検索とファイルレベルの復元が可能で、 マウスを数回クリックするだけで、 アプリやファイル、 オブジェクトをきめ細かく復元することで目標復旧時間（RTO） をほぼゼロにできるものになります。 インシデント対応担当者は、 個々のワークロードを手動で検証せずに適切なバックアップを迅速に特定し、 本番環境が再感染するリスクなしで個々のワークロードを確実に復元できるようにする必要があります。

総保有コスト （TCO） を削減

パブリッククラウドの急激な導入に伴い、 クラウドスプロールは組織にとって大きな課題となっており、 クラウドストレージに関するコストが高騰しています。 クラウドコストが高騰する中、企業はクラウドの利用を最適化することによって、データのバックアップ、インデックス作成、 アーカイブ、 復元に必要なコンピュータのリソースなど、 ハードバックアップのコストを含め、 コスト全体を制御する方法を模索しています。 そのため、 求められるクラウドサイバーレジリエンスのソリューションは、 低コストのオブジェクトストア AWS S3 Glacier や Azure Blob Archive Tier にバックアップを保存する、 完全なバックアップの代わりに増分バックアップを実行する、 圧縮や重複排除などのデータ整理機能を利用する、 といったことが可能なものになります。

セキュリティポリシーの設定、 データ復元の管理、 脅威の監視、 コンプライアンスの報告を合理化することで、 企業はソフトバックアップのコストを削減し、 ビジネスにおいて他の重要な優先事項に注力できるようにすることで時間とリソースの節約が可能になります。

まとめ

本書では、 マルチクラウドやハイブリッド環境において組織のデータを保護するためのクラウドサイバーレジリエンスの必要性について説明しました。 現在の脅威の状況は急速に進化しており、 企業の攻撃対象領域は大幅に拡大し、 攻撃者にとっては理想的な状況を作り出しています。 真のクラウドサイバーレジリエンスを実現するには、 データ保護に対するより良いアプローチが必要です。 それは、 クラウド関連の支出削減に貢献し、 包括的なサイバーレジリエンスや迅速な復元などの機能も備えた、 シンプルで一元化されたクラウドネイティブなプラットフォーム上に構築されるものです。

クラウドサイバーレジリエンスに関する Rubrik の詳しい見解については、 https://www.rubrik.com/solutions/cloud-solutions でコンテンツ、 ウェビナー、 デモなどをご確認ください。

RUBRIKについて

Rubrikは、企業がビジネスレジリエンス、クラウドモビリティ、規制コンプライアンスを推進できるよう、データコントロールを支援しています。Rubrikは、ソフトウェア定義のファブリックを通じてデータセンターとデータを分離し、オンプレミス/クラウドなどすべてのデータに対して1つの管理プレーンを提供することで、企業固有のオンプレミスインフラとクラウドの間を橋渡しします。迅速なアクセス、自動化された連携、エンタープライズクラスのデータ保護とレジリエンスによって、包括的なデータ管理を提供しています。

ACTUALTECH MEDIAについて

ActualTech Mediaは、Future PLCのB2Bファミリーに属するB2Bのテックマーケティング企業で、革新的なリード創出プログラムと魅力的なカスタムコンテンツサービスを通じて、企業のITベンダーとITバイヤーを結び付けています。

ActualTech Mediaのチームは、企業のIT担当者に向けて発信しています。なぜなら、私たちもかつてはIT担当者だったからです。

当社の経営陣には元CIO、IT責任者、アーキテクト、特定領域の専門家、マーケティング専門家が多数在席しており、お客様がテクノロジーの状況説明にかける時間を短縮し、成果につながる戦略の策定に多くの時間をかけるようにしています。

ITマーケティングの担当者の方で、独自のGorilla Guide®をご希望の場合は、actualtechmedia.comをご確認ください。