データセキュリティの現状

データリスクの測定

Rubrik Zero Labs

目次

本書のキーワードは、

組織が所有しているデータの種類や、データの変化の実態、
そしてデータ脅威の実践的視点を取り上げます。

もう一つ、取り上げるのがリスクです。リスクの測定方法、リスクに備える
能力、リスクの変容の実態、永続する存在としてのリスクを紹介します。

とはいえまずは、***今回の結論に至った経緯から説明しましょう。***

データおよび調査手法

Rubrik Zero Labsは、データセキュリティのリスク軽減に向けた、ベンダーに依存しない実用的な情報提供に取り組んでいます。
その目的のために、今回、4つの主要ソースによる調査成果を統合活用しました。

RUBRiK テレメトリー = ◆
Rubrikテレメトリーの活用により、一般的な企業のデータエステートおよびリスクの実態把握を行いました。

WAKEFiELD RESEARCH = ▲
1,600人以上のIT/セキュリティチームのリーダーの視点

RUBRiK パートナー = ●
Rubrikパートナー2社による研究と手引き

支援提供企業各社 = ■
定評あるサイバーセキュリティ企業および機関による研究

RUBRiKテレメトリー ◆

Rubrik Zero Labsは、各企業が自社データについて弊社を信頼してくれるのであれば、そのデータから分かる内容に関して透明性を確保しなければならないと考えています。透明性という点では、以下に、弊社が用いた測定方法の構成要素と、それが弊社の見解にどう影響しているのかを記載しています。

注：本調査には、今回が初の利用となったLaminar由来のデータが含まれます。Laminarはデータセキュリティ態勢管理用プラットフォームで業界をリードする企業で、2023年にRubrikが買収しました。

RUBRIKテレメトリーの対象：

6,000以上 のクライアント

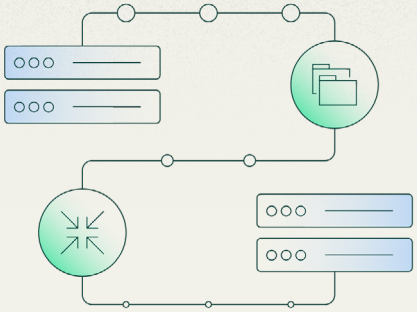
68 か国

42 EB の保護対象データと384億以上の機密データレコード

保護対象のデータ総量：
- 42エクサバイトの論理ストレージ
- 963バックエンドペタバイト（BEPB）の物理ストレージ

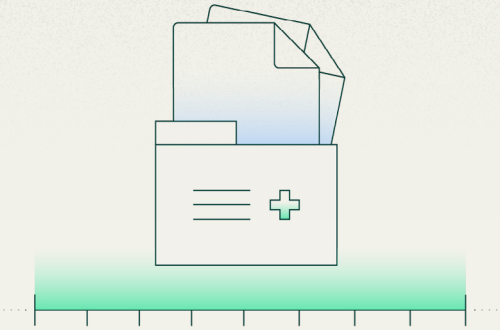
384億以上の機密データレコード

対象データは2023年1月1日から2023年12月31日までの分



EB vs BEPB

ご存知ですか？世界中の大抵の人々は、「データ」と聞くと、論理ストレージ（*フロントエンドストレージ*とも呼ばれます）を思い浮かべます。一方、データビジネスに従事する私たちが扱うのは、主に*バックエンドストレージ*です。Rubrikは、組織のデータを全体的に捉え、重複排除や圧縮などの複数の異なる技術を実行し、*バックエンドストレージ*に格納される*フロントエンド*データの量を削減しています。本レポートでは、全体を通して*バックエンド*ストレージを取り上げます。



42 EBとはどれくらいのデータ量なのか

医療記録を例にすると各種画像（X線やMRIなど）、カルテ情報、などが含まれます。平均的な人では、医療記録の容量はおよそ80MBです。

仮にRubrikが保護する42 EBのデータのすべてが医療記録のみだったとすると、その中身は、人類の歴史上に存在した延べ人数1,170億人全員の一人ひとりの医療記録5つ分に相当します。すさまじい容量です。

WAKEFiELD RESEARCH

弊社はWakefield Researchと共に、ITとセキュリティの両分野のリーダーを対象とする共同調査を実施し、さらなるインサイトを収集しました。このデータは、Rubrikテレメトリーを補完し、リーダーたちの視点とリーダーたちの現場感の両方に関するインサイトを提供してくれるものです。客観性確保のため、Rubrikの顧客の持つデータはWakefield Researchのデータセットからは対象外としています。

1,600人以上 のIT/セキュリティのリーダー

10 か国

50%超 のCIOまたはCISO

1,625

人の意思決定者を対象とし、その勤務先については3つの地域（南北アメリカ、EMEA、APAC）の10か国（米国、英国、フランス、ドイツ、イタリア、オランダ、日本、オーストラリア、シンガポール、インド）に所在する従業員500名以上の企業

50% がCIOまたはCISO

50% がIT担当の意思決定者

50% がディレクターまたはVP

50% がセキュリティ担当の意思決定者

RUBRiKパートナー

弊社では、データレジリエンスの改善に向けた継続的な取り組みにおいて、データセットを活用するとともに、Rubrikパートナー2社からのサポートを受けました。

Microsoft

Microsoftからは、データ流出率およびレジリエンスの推奨事項を中心に、2023 Microsoft Digital Defense Report[1]のデータを提供していただきました。

AON

Aonからは、データバックアップの現実および侵入被害後の成果を中心に、2023 Aon Cyber Resilience Report[2]のデータを提供していただきました。

支援提供企業各社

Rubrikとして可能な限り客観的な視点の提示につとめるため、Rubrikテレメトリーとは異なった独自の可視化を行っているさまざまな組織から提供を受けたデータを取り入れました。

MANDIANT NOW PART OF Google Cloud

Mandiantからは、同社での2023年の年間[3]インシデントレスポンス/MDRイベントにおいて確認されたデータの取り込み時間（Dwell time）を提供していただきました。

UNIT 42 BY PALO ALTO NETWORKS

Palo Alto Networks Unit 42からは、同社での2023年の年間インシデントレスポンス/MDRイベントに基づく、ランサムウェア要求と支払いに関する調査結果を提供していただきました。

proofpoint

Proofpointからは、同社の2023 Human Factors Threat Report[4]に基づく、クラウドの標的化に関する情報を提供していただきました。

Recorded Future®

Recorded Futureからは、レポートとして公開されている2023年のランサムウェア年間トレンド[5]を提供していただきました。

UNIVERSITY OF MINNESOTA

ミネソタ大学ツインシティー校公衆衛生学部からは、同学部の研究「Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients[6]」（発表済み、現在最終査読中）に基づく、公衆衛生機関へのランサムウェアの影響について提供していただきました。

1 https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
2 https://www.aon.com/2023-cyber-resilience-report/
3 https://www.mandiant.com/m-trends
4 https://www.proofpoint.com/us/resources/threat-reports/human-factor
5 https://therecord.media/ransomware-tracker-the-latest-figures
6 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292

リスクについての話

本調査での、リスクへのアプローチ方法の
基本原則をご紹介します。

はじめに

次の式で「リスク」の算出を簡易化します。

データが外部エンティティによって感染させられる可能性 ＋ 今現在データ内に存在するリスク ＋ 今後可能性のある影響 ＋ その影響への対応における判断 ＝ リスク

何と大きな数値でしょうか

次に

今回はデータに焦点をあてていきます。
データセキュリティ企業として、弊社が最も得意としている分野は、インフラストラクチャやアーキテクチャではなくデータに関するものであり、データ内のリスク、そしてデータに対するリスクを対象としています。

具体的な重点分野
率直に言って、今、だれもが忙しくしています。データセキュリティに関し、全面的にくまなく目を通す時間がある人などいません。そこで弊社では、今回の調査対象を意図的にいくつかの重要トピックに絞りました。

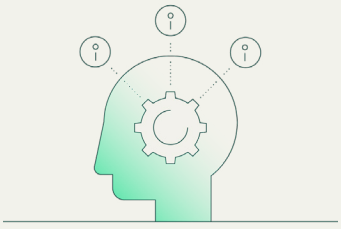
クラウド
商用利用可能なクラウドの存在は今や、10年単位で語れるものとなりました。とはいえ、クラウドデータのセキュリティに関する混乱はいまだに存在します。クラウドが標的となる頻度、そしてその成功率は、オンプレミスよりも高くなっています。また、防御も完璧ではないため、完全な防御も困難です。

ランサムウェア
それほど遠くない昔に、専門家たちはランサムウェアの減退を予測していました。しかし実際にはそうならず、ランサムウェアはあらゆる種類の組織に大きな混乱をもたらし続けています。

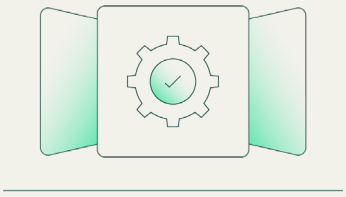
医療
ほぼ例外なく、医療機関は他の業界に比べて生成および保管される機密データが多く、規制面での監督もより厳しいものとなっています。医療分野における規制圧力の副次的な利点は、調査に利用できる公開データが多いことです。

最後に

この調査報告の対象者



インテリジェンスによって情報が適切な意思決定者に伝わらなくてはならず、リスク関連の意思決定は通常、経営層が行います。



本調査の目的は、そうした経営層が事業、サイバーセキュリティ、ITの各部門を横断する形でディスカッションを行ううえでの情報を提供し、支援することです。

共通の出発点を用意することで、一丸となってリスクに立ち向かうための準備を意思決定層が円滑に行えるようになります。

それでは、リスクがどのように受け止められているのかを見てみることにしましょう。

人間は、不確実性を扱うのがあまり得意ではありません。
何かが起きそうな可能性に直面すると、私たちは
次のいずれかの考えを抱きがちです。

気象学者は、地域の降水確率が52%の場合、
「雨が降ります」、あるいは「雨は降りません」と
断言したりはしません。

その際に、私たちが本当に知りたい具体的な内容は、どの程度の雨なのか、です。
小雨なのか、土砂降りなのか 家から出ない方がいい？ だって、いずれにしても出勤したくなかったから。

判断するのは自分であり、自分以外にはいません。

一度きりしか判断しなくてもいいのなら、楽でしょう。

しかし、そんなわけにはいきません。

雨に対する今日の反応は、明日の天気予報の捉え方に影響を及ぼすと同時に、雨への対処における教訓ももたらします。

これらの要因が組み合わさって、次回、嵐に対峙しなくてはならない際の新たな条件ができあがります。このことは、雨についても、そしてサイバーリスクについても当てはまります。

それでは、考慮すべき
外部の脅威から見ていきましょう。

貴社のデータは攻撃者からのリスクにさらされているか？

まずは基本的な疑問から。

攻撃者が**当社のデータ**を標的にする可能性があるのでしょうか？

インターネット接続された
冷蔵庫に命を狙われる？

ランサムウェアのESXiへの
標的シフトは
非常に大きな進化

攻撃者のリアルな
AI活用方法

貴社のニュースフィードの、事実とFUDの度合いはどれくらいですか？

次なる
SolarWinds事件か？

（FUD＝不安、疑念、不信）

最悪のデータ漏洩：
史上最大規模のデータ損失

Strawberry TempestがLapsus$よりも悪い理由

貴社がサイバー攻撃を受けるかどうかについて、
100%の確度で言い切ることは不可能ですが、
昨年、同業者に何があったのかはお伝えできます。

ほぼすべての業界で、約2週間間隔でサイバー攻撃を受けています。

IT/セキュリティ担当リーダー全体での昨年の概況：▲

94% のITおよびセキュリティリーダーは昨年、自社組織が大規模なサイバー攻撃を経験したと報告しています。

30 2023年の年間平均として、上長の判断が必要となった悪意あるイベント数は30でした。

93% の外部組織が、管理組織に正式なデータ損失を通知しています。

サイバー攻撃は、***物理的な窃盗や火事***よりもはるかに高い確率で発生します。

サイバー攻撃の可能性を総体的に捉えるため、ある欧州の保険会社[1]が同一期間におけるサイバー攻撃と昔ながらの脅威とを比較したところ、次のようなことが判明しました。

67% 各組織で発生する可能性としてサイバー攻撃の方が物理的な窃盗よりも67%高い。

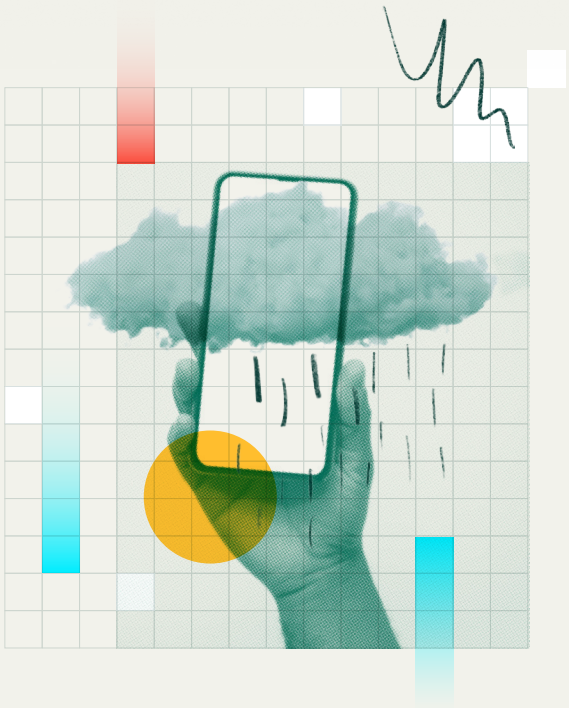
5倍 各組織で発生する可能性としてサイバー攻撃の方が火事の5倍高い。

20% の組織が、サイバー攻撃の発生時にどうすればいいのか把握していない。

1 https://www.aviva.com/newsroom/news-releases/2023/12/One-in-five-businesses-have-been-victims-of-cyber-attack-in-the-last-year/

攻撃者にとっては***ハイブリッド環境***の方が標的として手軽です。

標的になる可能性が高いのであれば、どこにどんな攻撃が行われそうなのかを知っておくことが有用となります。サイバー攻撃の被害に遭った94%の外部組織のうち、多くにおいて攻撃は複数の環境にまたがる形で発生しました。▲



67% SaaS

66% クラウド

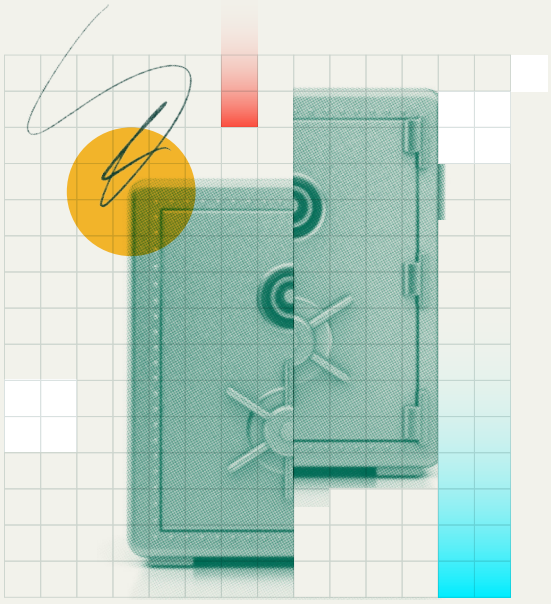
51% オンプレミス

さらに、上記の環境における攻撃の主要な2タイプに関する視点もご紹介します。▲

38%
の被害組織で、1回のサイバー攻撃で1件以上のデータ侵害がありました。

33%
の被害組織で、1回以上のランサムウェア攻撃を経験しました。

ほぼすべてのクラウドテナントが標的となっており、2023年には3分の2が侵入を許しています。



これについては弊社の独自調査の結果ではありません。Proofpointの報告によるものです[1]：■

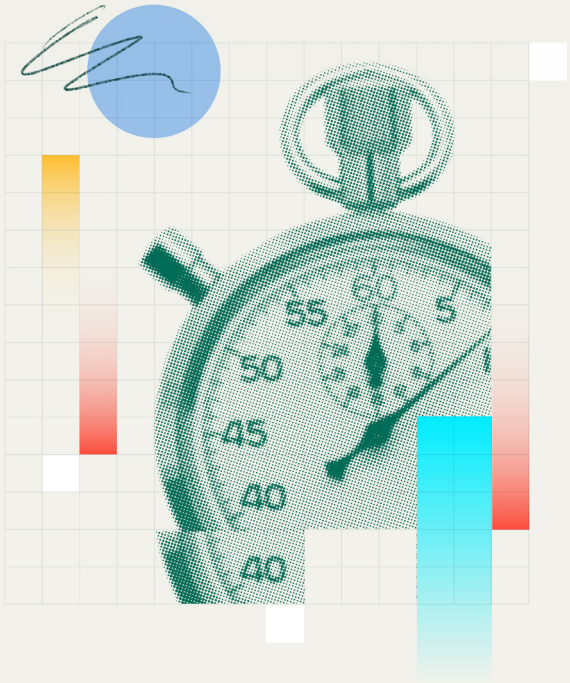
94%
のクラウドテナントが昨年、毎月標的となりました。

62%
の標的化されたクラウドテナントで、侵害が成功しました。

1 https://www.proofpoint.com/us/resources/threat-reports/human-factor

攻撃者は、発見される何日も前から***データにアクセス***しています

検知前に攻撃者が被害者の環境内に存在している日数として、**Mandiantが測定したデータの取り込み時間[1]は以下のとおりです。**



10日間

すべてのイベントにおける昨年の全世界のデータ取り込み時間の中央値は10日間でした。

5日間

ランサムウェアイベントでの全世界のデータ取り込み時間の中央値は5日間です。

良いニュース：

これらはMandiantがこれまでに観測したなかでの史上最短のデータ取り込み時間でした。

悪いニュース：

これでも、悪意ある攻撃者が目的を達するには十分な長さです。

想像を超える実態。ランサムウェアは増加しています（70%の伸び）。

Recorded Futureでは、昨年公表されたランサムウェア攻撃が大幅に増加していたことを確認しました。

46%

358件の医療分野へのランサムウェア攻撃が報告されました（前年比46%の増加）。

70%

4,399件の全業界への攻撃が報告されました（前年比70%の増加）。

続いて、視点を組織のデータへと移しましょう。

1 https://www.mandiant.com/m-trends

貴社のデータ内に
リスクは存在するか？

攻撃を受ける確率を把握しているのなら（実際のところ、非常に高いわけではありませんが）、軽減策によるリスクの最小化に万全を期すことは理にかなっています。

攻撃が成功する可能性

攻撃による フォールアウト 副産物

結局のところ、やろうとすることは（机上では）驚くほどシンプルです。
保護の図式は、

この等式の両方の側を精査しなくてはなりません。
組織側として、防御者に期待している保全対象を
見ていきましょう。

データ

は今、急速に増加し、防御境界を
拡大させています。

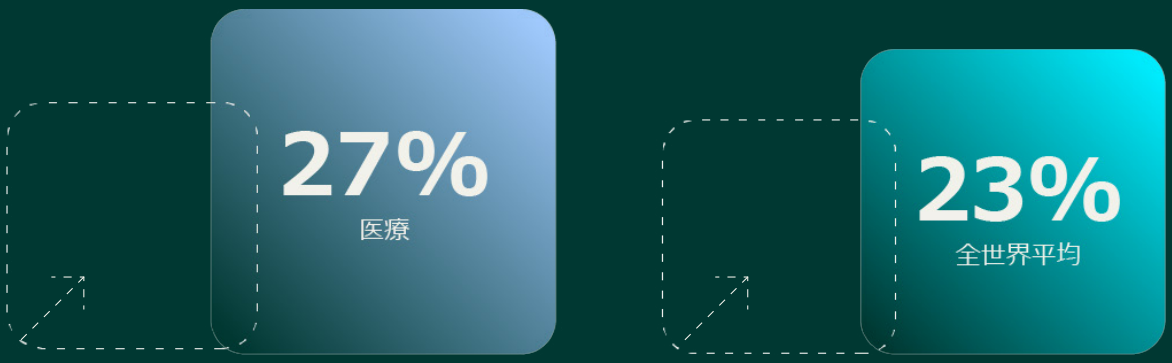
医療分野の防御者は、全世界平均よりも大規模で機密データの数も多いうえ、成長速度を増しているデータ対象領域の保全に責任を負っています。◆

医療機関は全世界平均より22%も多くのデータを保全しています。

BETBについておさらい

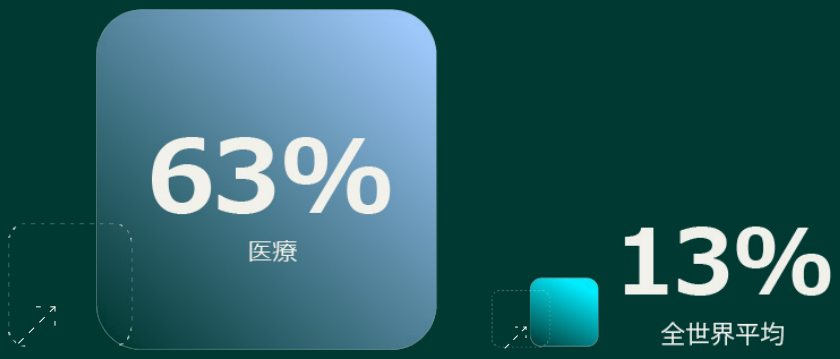
EB vs BEBP
ご存知ですか？世界中の大抵の人々は、「データ」と聞くと、論理ストレージ（*フロントエンドストレージ*とも呼ばれます）を思い浮かべます。一方、データビジネスに従事する私たちが扱うのは、主に*バックエンドストレージ*です。Rubrikは、組織のデータを全体的に捉え、重複排除や圧縮などの複数の異なる技術を実行し、*バックエンドストレージ*に格納される*フロントエンドデータ*の量を削減しています。本レポートでは、全体を通して*バックエンドストレージ*を取り上げます。

標準的な医療機関では昨年、データエステートが27%増加しました（グローバル組織では23%）。



標準的な医療機関は、全世界平均よりも50%多くの機密データを保持しています。

医療分野の機密データレコード数は2023年に63%以上増加しています。他のどの業界をもはるかに上回り、全世界平均（13%）の5倍です。



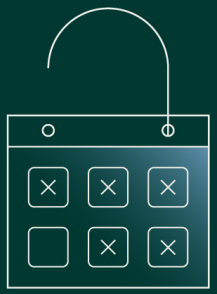
各組織では昨年、対処すべき問題の数が史上最高となりました。

脆弱性は漏洩の尺度として完璧とは言えませんが、ベンダー由来の固有リスクの範囲と規模についての確かな見解を提供してくれるものではあります。

2022年は脆弱性に関する記録更新の年となり、報告された脆弱性の数は史上最多でした。

25,083
件の脆弱性発見

2023年、記録はさらに更新され、前年を16%も上回ることとなりました。



29,065
件の脆弱性発見

各組織はますます、クラウドとSAASへの依存度を高めています

モダンなビジネスへの需要が、クラウドに対する集中増加を余儀なくさせているのです。
ハイブリッド環境の実態が一貫してクラウドとSaaSへと向かっている一方、
オンプレミスのアーキテクチャ拡張は優先順位が下がっている状況です。

2022：

2023：

クラウドにはセキュリティ面の盲点が存在する

クラウドデータのセキュリティ
盲点その1：

標準的なクラウドインスタンス内の全データの70%がオブジェクトストレージです。[1]

オブジェクトストレージは、大半のセキュリティアプライアンスにとっての共通する盲点となります。通常は自己での機械判読ができないためです。

クラウドデータのセキュリティ
盲点その2：

オブジェクトストレージ内の全データの88%が、CSV、JSON、XMLといった、テキストファイルまたは半構造化ファイルのいずれかです。◆

仮に、手元のツールやプロセスがオブジェクトストレージ内部を視認できるとしましょう。すると別の問題が出てきます。非構造化データ（テキストファイルなど）と半構造化データがセキュリティ面での別の盲点となるのです。なぜならそうしたデータタイプは、機械判読の可否や、主要なセキュリティ技術およびサービスの対象かどうかの点において、まったく統一性がないからです。

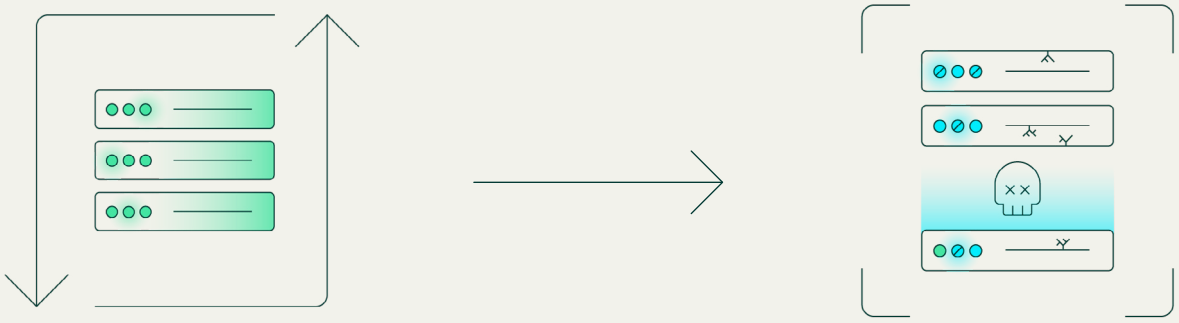
クラウドデータのセキュリティ
盲点その3：

全オブジェクトストアの25%以上に、保護対象保健情報（PHI）や個人識別情報（PII）といった、規制または法的要件の対象データが含まれています。◆

簡単に言うと、クラウドには固有のリスクが付き物です。組織として機能するためにクラウドが必要である一方、オンプレミス資産よりもセキュリティ面や可視性が劣る環境に規制データが保管されている状況では、リスクを切り離せないのです。

ほとんどのバックアップソリューションはタスクに対応しきれていません。

バックアップや復元の技術は、ほぼすべての組織において不可欠の要素です。それらの技術は数十年にわたり、ディザスタリカバリやビジネスコンプライアンスに用いられてきました。
とはいえ、多くの企業がそうしたソリューションをうまく機能させられず、苦心しています。



99%

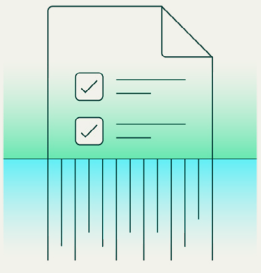
Rubrik Zero Labsの以前の調査[1]では、99%以上の外部組織がバックアップソリューションをすでに導入していると回答していました。◆

93%以上

とはいえ、そのうち93%以上の組織が既存ソリューションでの重大な問題に直面しました。◆

70%

Aonのレポート[2]では、70%の組織がバックアップをオフサイトに保管していない、またはバックアップが書き換え不可ではない状態でした。●



40%

Rubrikが確認した組織のほぼ40%が、自社のデータバックアップに関するコンプライアンスポリシーを未策定です。◆

1 https://www.rubrik.com/zero-labs/2023-spring
2 https://www.aon.com/2023-cyber-resilience-report/

悪いニュース：

サイバー犯罪者はバックアップに関する玄人であり、日常業務のごとくバックアップを標的としています。

攻撃者はほぼ全世界的に、防御担当者の手からバックアップと復元の選択肢を取り上げようと試みていました。
攻撃に成功されてしまったことを報告した外部組織：▲

96%

攻撃者は攻撃の96%においてバックアップを感染させようと試みました。

74%

そして、その試みの74%は、少なくとも部分的に成功しました。

サイバー犯罪者は、効果的なリストアに対する保険策を講じています

攻撃者は、防御側の措置に応じる形でランサムウェアへのアプローチを進化させています。単なるデータ暗号化の代わりに、サイバー犯罪者たちはデータを盗み出したうえで、それを公開すると脅す手段にも出ているのです。仮に標的が迅速な復旧で暗号化攻撃を阻止しても、ランサムウェア攻撃者には身代金の額を釣り上げる別の方策があります。

2倍

Microsoftでは、最初の侵害後に脅威アクターがデータを流出させたと思われる回数が2022年11月以降、倍増していると結論付けました。●

12%

Aonの調べでは、データ侵害はランサムウェア単独の場合と比べて組織への全体的な影響度が12%高くなっています。●

93%

ランサムウェア攻撃に成功されてしまった外部組織の93%が身代金要求への支払いを行い、うち58%が支払いの動機は盗まれたデータの漏洩のおそれだったと回答しました。▲

ここまでで危険性は把握できましたので、続いて影響について見ていきましょう。

その後に
どれほど悪い事態が待っているのか

サイバー攻撃は物語の終わりだと考える人が多くいます。

しかし、実際には終わりではなく、物語の中盤です。

再度、天気予報の例に戻ると、***雨が降ったからといって話がそこで終わるわけではありません。***

人生はまだ続くのです。しかし今度は、条件への適応が必要です。濡れないようにするには？ 雨の中でも犬は散歩するか？ 避けられない状況で雨に降られたらどうなるか？

同じように、サイバー攻撃は、修復、復旧、レポートの手間を大量にもたらすことになります。

その手間がどれだけ骨の折れるものとなるかは、そうした結果に対し、当初からいかに首尾よく備えていたのかに左右されます。

サイバー攻撃、特にランサムウェアによる副産物について、昨年起きた医療機関に対する攻撃を題材に詳しく見ていきましょう。

これが、サイバー攻撃後に起きることの実態です。

米国人のおよそ3人に1人の個人記録が、昨年起きた医療機関への侵入において侵害されました[1]。

24万4千以上

人（平均人数）が、昨年起きた医療機関への1回のサイバー攻撃において影響を受けました。

186%

2022年から増加

1億3,300万以上

昨年の米国医療組織に対するサイバー攻撃によりレコードの侵害を受けた人

1 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

医療機関を対象とするランサムウェア攻撃では、全世界平均に比べておよそ5倍も多くの機密データが影響を受けます。◆

Rubrikは、ランサムウェア暗号化による攻撃範囲と、その範囲内で影響を受ける機密データの両方を測定しています。
影響を受けるファイルは、暗号化されるファイル、削除されるファイル、流出するファイルなどです。

典型的な対医療機関ランサムウェア暗号化攻撃で影響を受ける本番環境内のデータは次のとおりです。

医療機関：

1,680万

1回の暗号化攻撃で
影響を受けるファイルの総数。

840万

左記のファイル内の
機密データレコード数。

20%

標準的な医療組織が保有する総機密データのうち、ランサムウェア暗号化攻撃が行われるたびに影響を受けている割合。

平均的な大規模グローバル組織では通常、機密データへの影響ははるかに少ない状況です。

13.7M

total impacted
files per event

170万

1回の暗号化攻撃で影響を
受ける機密データレコード数

6%

組織の機密データ全体に
占める割合

仮想化が医療とランサムウェアにとって重要な位置付けとなっています。◆

次に、ランサムウェア暗号化の発生場所を見てみましょう。

97%

の医療関連の暗号化データの保管先が
仮想化アーキテクチャ内です。

83%

の全産業の暗号化データの保管先が
仮想化アーキテクチャ内です。

このことの主要因と思われるのは次の2点です。

1 : 仮想化アーキテクチャは通常、従来型のエンドポイントと比べてセキュリティ範囲が手薄です。それによってセキュリティの死角が生まれ、同時に攻撃者の自由なアクセスを許すことになります。

2 : 攻撃者は、ひとたび仮想化制御パネルへのアクセス権を取得すると、侵害された資格情報のみですばやく大規模に動くことが往々にしてあります。

身代金の支払額はまちまちです。

当初の要求額は大抵、実際の支払額より多くなっています。Palo Alto Networks Unit 42は、昨年1年間の身代金支払いにおける以下の傾向に着目しました。▪

	全業界：	医療：
要求額の中央値	80万ドル	20万ドル
支払額の中央値	27.5万ドル	10万ドル
支払額上位5件の中央値	2,500万ドル	29.7万ドル

バックアップとデータ窃取が、被害者の身代金支払いの可能性に大きく影響します。

トゥウェンテ大学[1]は、被害者に身代金を支払わせることになった要因と、それとは別に何が実際の身代金の支払額の多寡に影響したのかを調査しました。調査結果が示す内容は以下のとおりです。

復元可能なバックアップを保持していた組織は

27.5倍
身代金を支払う可能性が低い

1 https://databreaches.net/university-of-twente-maps-decision-making-process-for-ransomware-victims/#:~:text=for%20the%20best-,article,-.

データ流出が、身代金を支払う可能性と支払額の引き上げにつながっていました。

40%

データ流出を伴う状況で身代金を支払った割合。

25%

データ流出を伴わない状況で身代金を支払った割合。

5.5倍

暗号化のみだった場合と比較しての、データ流出を伴う攻撃で支払った身代金の額。

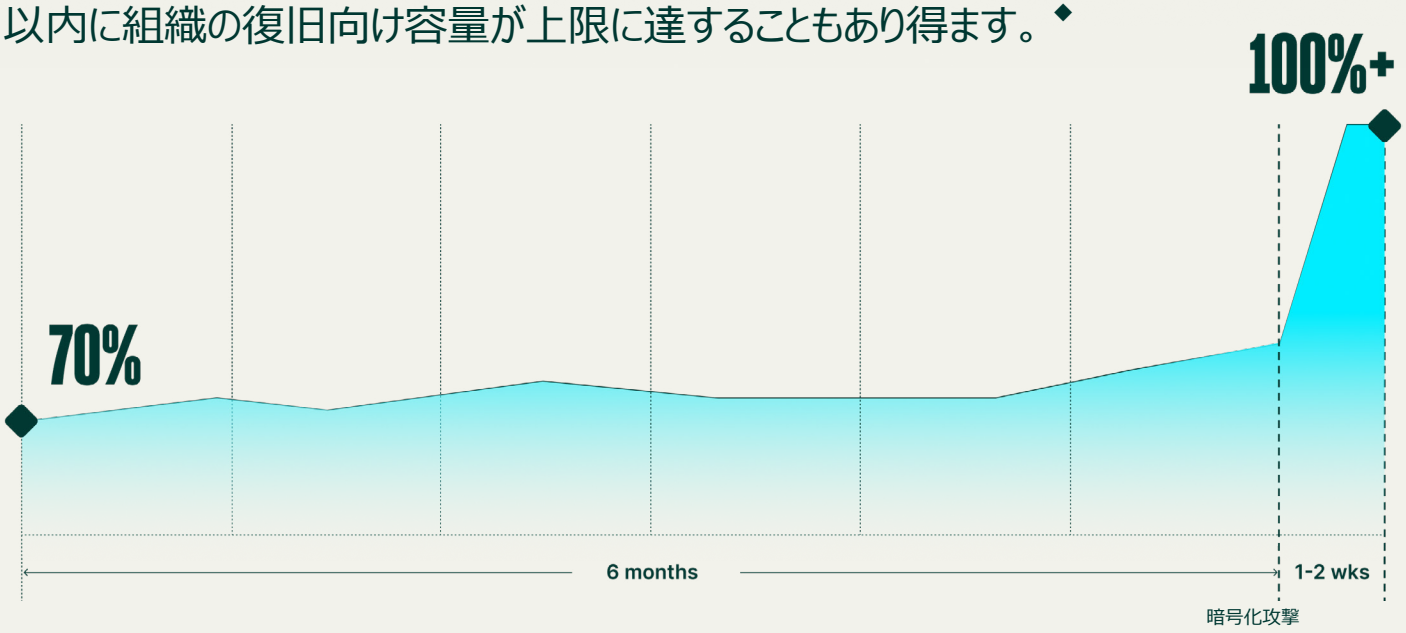
ストレージの過負荷：誰にも予測できない復旧の盲点

雨の日に水が降り注ぐことは誰でも知っています。しかし、ランサムウェアによって引き起こされるデータの大洪水（Data deluge）に備えている組織はほぼありません。

仮に、医療機関への1回のランサムウェア攻撃で1,680万個のファイルが暗号化または変更されたなら、それは基本的に、その暗号化攻撃によって被害者の手元に1,680万個の「新規」ファイルが作成されたということです（標準的なグローバル組織では新規ファイル数は1,370万個）。◆

それらのファイルは新規ファイルとしてバックアップされ、暗号化攻撃の際に膨大なストレージ容量を消費します。

もし、ランサムウェア攻撃前の被害者のストレージ使用容量が70%以上だったとすると、今回の「新規」データによって1～2週間以内に組織の復旧向け容量が上限に達することもあり得ます。◆



この問題をさらに深刻化するのが、被害者は往々にしてさらなる「新規データ」を作成しなくてはならないことです。たとえば、分析用のフォレンジックイメージや、法律面の目的での書き換え不可のコピーなどが必要となります。また多くの場合、対応や復旧のワークフローでは複製データも必要です。簡単に言うと被害者は、攻撃者が膨大な新規データを作成した直後に、対応プロセスの一環としてさらに多くの新規データを作成しなくてはならないのです。

Rubrikのランサムウェア対応チームが過去に手がけた200件以上の復旧業務では、この問題は、2つの結果のうちどちらか1つになることがわかりました。組織は次のいずれかを実行しなくてはなりません。

1： データ容量を迅速に拡張する。これには財務投資と従業員へのプレッシャーが必ず伴う。

2： 復旧能力を低下させてデータの増加を遅らせる。これは結果として、時間的に厳しいなかで復旧の選択肢を狭めることになる。

ランサムウェアの副産物が、少なくとも42人の米国人の死亡の直接要因となりました。

どのランサムウェア攻撃でもデータ面での影響が発生します。実際のリスク、特に医療分野におけるリスクについては、運営面での影響や人の命によっても測定されます。

ミネソタ大学ツインシティー校公衆衛生学部では、2016年から2021年の間に起きたランサムウェア攻撃[1]による病院と患者処置への現実の影響を調査しました。その結果は以下のとおりです。

20%

ランサムウェア攻撃の最初の1週間全体で、患者への処置対応能力が20%低下しました。

こうした攻撃はもはや、単にデータや事業、個々のプライバシーだけに影響しているわけではありません。サイバー攻撃が生死の問題であるという直接的な証拠があります。

4分の1

調査対象期間にランサムウェアの直接的な影響があった米国の病院はわずか5%だったものの、別途、20%の病院では、被害を受けた病院から周辺病院への患者の移送や転院に際して波及効果の影響を被りました。

0.5～1%

標準的な病院では、1回のランサムウェア攻撃の直接的な結果として年間総収入の0.5～1%の損失を被りました。

2～3週間

各病院では、ランサムウェア攻撃後に通常の患者処置水準に戻るまでに平均で2～3週間を要しました。

42～67人の死者

ランサムウェア攻撃の副産物が、42～67人の患者[2]の死の直接的な要因となっています。

1 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292
2 https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/

復旧
による初期化

初期対応が実行され、組織が比較的通常の業務に戻った後も、
ランサムウェア攻撃の副産物はリスク面の影響を生み出し続けます。

悪いニュースと良いニュースがあります。

サイバー攻撃は、組織と社員に***影響***を及ぼします。

Aonによると、大規模なサイバーインシデントにより、●

9%

の株主価値下落が1回の攻撃でもたらされます。

外部組織ではサイバー攻撃による以下のような直接的影響がありました。▲

44%
リーダーの交代を余儀なくされた

43%
否定的な報道やイメージの悪化

37%
収益の損失

36%
失った顧客

ITおよびセキュリティ担当の上級リーダーの96%が、サイバー攻撃の直接的な結果として、感情面や精神面での変化があったと回答しました。▲

53%
現在の職務に関する不安の高まり

41%
同僚やチームメンバーの信頼を失う

38%
雇用の確保に対する不安

33%
睡眠不足または睡眠の問題

経営幹部は自社が***次回の攻撃から復旧できる***という
確信を持つことが必要になります。

60%

のITおよびセキュリティ担当のリーダーが、サイバー攻撃の際の自社の事業継続維持能力に対し、極めて、あるいは非常に不安を感じています。▲

28%

の外部組織が、サイバー攻撃の際に重要なデータやアプリケーションを回復させる組織としての能力について、取締役や経営幹部はほとんど、あるいはまったく自信をもっていないと考えています。▲

サイバー攻撃は、予測が可能な解決すべき問題を生み出します。

以下は、サイバー攻撃の際に最もよく確認される問題と、組織としてサイバー攻撃後に直面することを覚悟しておくべき最も一般的な変化です。

外部組織から回答のあった、サイバー攻撃の際に直面した最も大きな制約です。▲

19%	18%	18%	17%	16%
ハイブリッド環境全体での横断作業の問題	チーム間での連携の欠如	実効性のないバックアップおよび復旧ソリューション	経営陣の関与の欠如	可視性の課題

以下は、外部組織がサイバー攻撃によって直面した最も一般的な変化です。▲

24%	20%	19%	19%	18%
上級リーダーによる監視強化	サイバーセキュリティ技術の変化	サイバーセキュリティの計画と手順の見直し	説明責任を果たす機会の増加	ITやサイバーセキュリティ担当チームの士気低下

サイバー攻撃が肯定的な結果を
促進する場合もあります。

そうした危機の時を生かすための準備を整えている
組織は、未来を再構築することができます。

Aonによると、サイバー攻撃をうまく乗り切った企業では、
同業他社と比較して

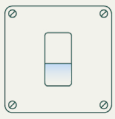
18%の株主

価値上昇が起きました。

サイバー攻撃後、外部組織の▲

55%

で新しいテクノロジーまたは
サービスへの支出が増加



42%

でベンダーまたは
サードパーティとの関係を切り替え

37%

でスタッフを追加雇用

リスクの根絶は不可能ですが、リスクサイクルに影響を与え、
リスク基準の組み直しに関与することはできます。

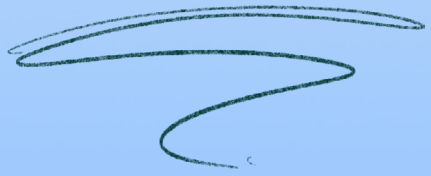
データリスクの
初期化

最終的な結果をお伝えして
締めくくりにしたいと思いますが、

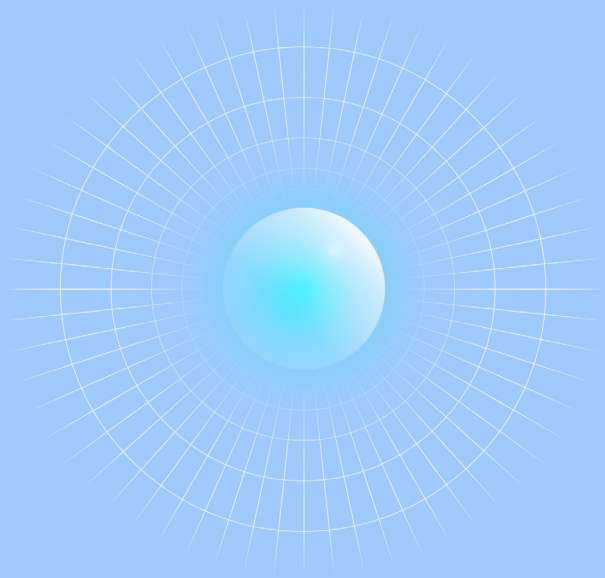
実際には、それがまた
新たな章の始まりと
なります。

一度、嵐を切り抜けたからと言って、今後はもう二度と嵐に遭遇しないということはありません。

実際には、ほぼ間違いなく別の嵐に見舞われますし、
その時にはまた新たな、そしておそらくは初めて経験するリスクが
もたらされ、不意をつかれることもあり得るでしょう。



攻撃者が主導権を握っているリスク要因を変化させるための複数の選択肢があるとお伝えしたいのはやまやまですが、残念ながら弊社の分析によれば、それを追い求めるのは天気を操ろうとするのと同じくらいに無意味です。

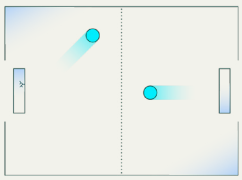


人生における大半の物事と同様に、自分の身に起きることはコントロールできません。ただし良いニュースとして、リスクの初期化と、その後の影響はコントロール可能です。

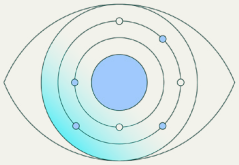
では、リスクの初期化をうまく実行する方法に関するデータを詳しく見ていきましょう。リスクについての各推奨事項は、サイバー攻撃、データ面の影響、想定結果に関する調査成果に基づくものです。

新たなデータリスクに対して実際に何が影響するのか

データリスクの大幅改善のために
利用できる最も影響力の強い手段：

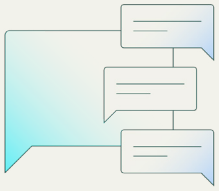


ハイブリッド環境全体で全面的に攻撃者に挑む準備を整えます。攻撃者たちはすでにハイブリッド環境を対象とした活動で成功を収めており、各組織も同じ方向へと動いています。

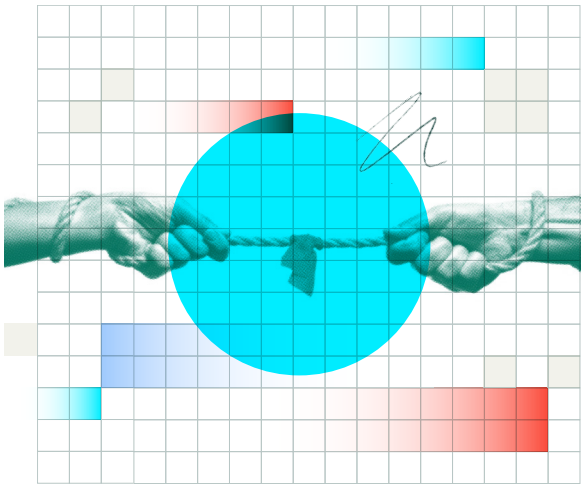


データの可視性を向上させます。特に、

- ハイブリッド環境全体で全面的に視野を拡張します。
- 機密データの保管先や、特定のデータ要素に適用される規制内容の種類を把握します。
- リーダーによる新たな監視への対応準備を行い、最近の投資がいかに期待する成果へと結びつくのかを説明します。



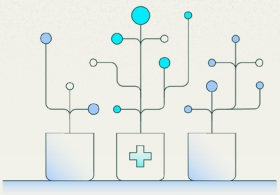
上層部による監視の増加を見越して、サイバー攻撃後の作業内容を事前に伝えます。



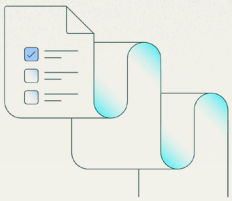
復旧への準備を整え、攻撃者からの***復旧作業への挑戦状***に備えます。

具体的には、

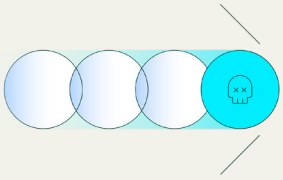
- バックアップが完全に書き換え不可で、サイバー攻撃中も利用できるようになっている状態を確保します。
- 可能な限り、復旧手順を自動化します。
- ハイブリッド環境全体での復旧結果をテストします。
- 既存のセキュリティサービスおよび技術を活用して、バックアップ技術の書き換え不可性と統合化をテストします。



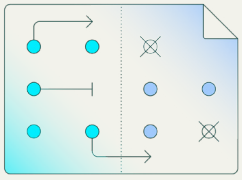
手元のデータ（特に機密データ）が増加していることを認識します。増加を制御し、重要データの保護を優先化することを学んでください。



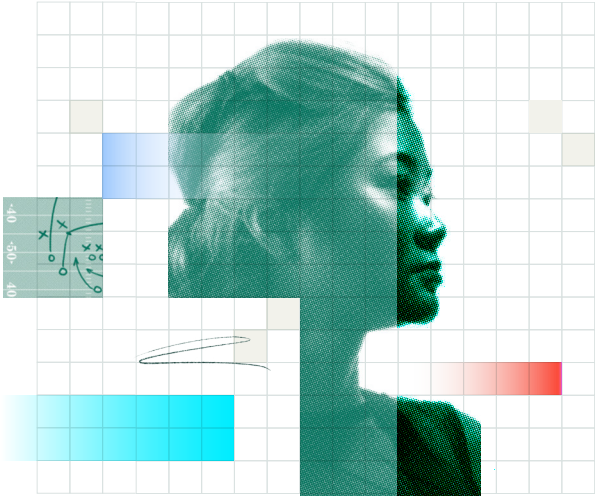
現に暗号化が進行し、攻撃者が窃取データの漏洩を脅迫してきているという状況でのランサムウェア攻撃の真っ最中に、規制当局からの質問や法的な質問に答えるための準備をします。



サイバー攻撃は多くの場合、新技術、スタッフの増員、ベンダーやパートナーの切り替えにつながることを認識します。そうした変更期間を利用してインパクトを最大化するための準備をしてください。



計画や成果を組織全体に定期的に知らせ、サイバー攻撃による士気低下に対処するとともに、チーム全体に再度、自信を植えつけます。



サイバー攻撃の前、最中、後に ***別々のチームを統合***するための方法を見つけます。

具体的には、

- 統合プレイブックを作成して訓練や演習を行います。
- 各々の具体的なリスク判断に最も適しているのはどのチームかを見極めます。
- 職務を割り当てられたリスク責任者に適切なデータを渡すための最善の方法を確立します。
- 迅速な判断を可能とし、競合する視点からの抵抗の可能性を抑えるため、全チームが同じデータ視点を持った状態を確保します。

別の視点から

事実として、Rubrik Zero Labsのリスクへのアプローチはデータ主導の視点に基づくものです。ここで視点を広げ、Microsoftの2023 Digital Defense Report[1]のレジリエンスに関する主要推奨事項にも目を向けましょう。Microsoftの立場はRubrikの立場とは明確に異なりますが、それゆえに、同社の推奨事項がリスク軽減の取り組みを強化するものになればと思います。

99% Microsoftでは、データの基本的なセキュリティ対策で全攻撃の99%を防げると判断しています。

具体的な推奨事項：

- 多要素認証を有効化する
- 最重要データや機能を保護する資産については特に、ゼロトラスト原則を適用する
- 拡張型検知とマルウェア対策を用いてハイブリッド環境の重要箇所をカバーする
- 重要なシステムとアプリケーションに常に最新版のパッチを適用する
- データ保護のため、どのデータが最重要なのか、その保管先はどこなのかを把握して、それらのエンクレーブの適切な保護策を実行する

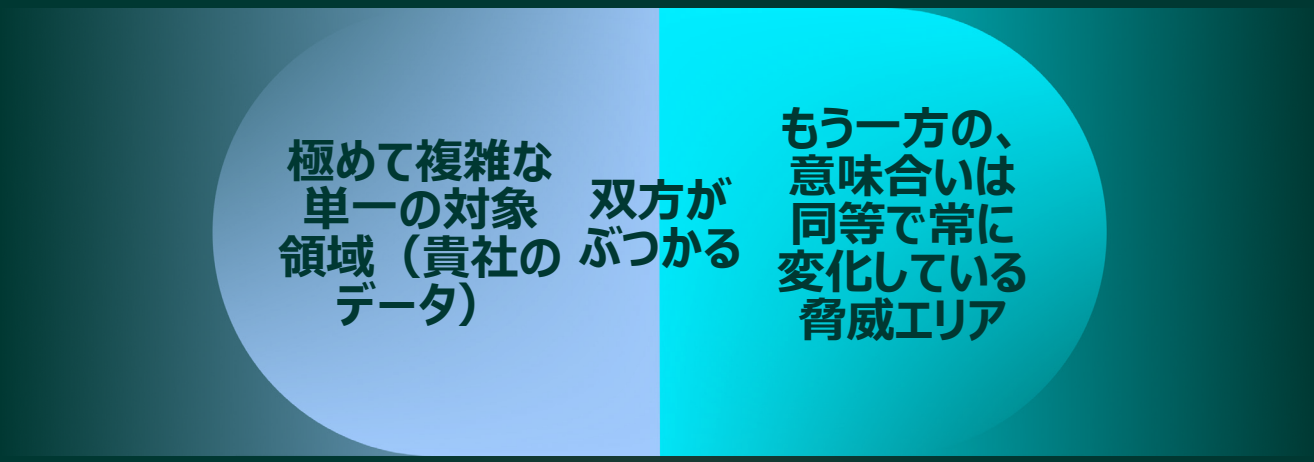
ランサムウェアに関するMicrosoftの視点をもう一段掘り下げてみると、同社では「The Foundational Five（基本の5）」を、ランサムウェアの影響を排除するための最適なやり方として提唱しています。

1. フィッシングに強い資格情報によるモダン認証
2. テクノロジースタック全体への最低限の特権アクセスの適用
3. 脅威やリスクと無縁の環境
4. コンプライアンスに関する、およびデバイス、サービス、アセットの健全性に関する態勢管理
5. ユーザーとビジネスクリティカルなデータの自動クラウドバックアップおよびファイル同期

1 https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

このレポートでは、リスク数値算出の簡易化から話を始めました。
「これ」を「あれ」から守る必要がある、です。

実際上は、リスクは驚くほど複雑なトピックです



リスク

文字どおりの数百万もの変数が関わるため、リスクを完全に特定する、あるいは完全に排除することは不可能です。可能なのは、最も影響力の大きい手段を操り、予測可能な結果への対処に取り組んで、リスク計算を有利に変えるための明確な行動を取ることです。

本調査によって、データリスクの軽減に関するインサイトを手に入れ、
進化するリスクサイクルに備えていただければ幸いです。

謝意

多大な労力をかけて獲得したデータ知見を本調査に提供していただいた各組織に対し、Rubrikとしてさらなる感謝を伝えたく思います。

- MicrosoftとAonのパートナーの皆様には、戦略的な方向性、そして裏付けとなるデータの両方を提供していただきました。

- 以下の各組織には、独自の分析の使用を許可していただくとともに、適切な分類を確実に行うための分かりやすい素材をご提供いただきました。
  - Proofpoint
  - Recorded Future（Allan “Ransomware Sommelier” Liska氏）
  - Mandiant（Kirstie “Swiftie” Failey氏）
  - Palo Alto Networks Unit 42（Ingrid Parker氏）

- ミネソタ大学ツインシティー校公衆衛生学部（Hannah Neprash氏、Claire McGlave氏、Sayeh Nikpay氏）には、独自の研究成果の使用許可と、研究内容の詳細の提供をいただくとともに、同学部の学術調査とRubrik Zero Labsの業界調査の足並みを揃えるためのRubrik Zero Labsとの連携へのご協力を賜りました。

Rubrik Zero Labsの研究は、多くの人々の協力によって成り立っています。Wakefield Researchには、この研究を可能な限り客観的なものとするための外部データを提供していただきました。Shaped Byには、データを意味づけするためのすばらしい方法を見つけていただきました。最後に、多くのRubrik関係者が多大な労力によって、能力、コンテキスト、ガイダンスを提供してくれました。Amanda “Danger” O’Callaghan、Linda “Taskmaster” Nguyen、Lynda “Go Niners” Hall、Ben Long、Peter “I’m the Law” Chang、Ajay Kumar Gaddam、Ryan Goss、Derek Morefield、Josh Burns、Gunakar Goswami、Prasath Mani、Ethan Hagan、Kevin Nguyen、Caleb “Social King” Tolin、Kelly Cooper、Hannah Battillo、Sindhu Nagendra、Caitlin “Plz stop letting Steve talk to reporters” O’Malley、Fareed Fityanの各氏に対し、格別の感謝を申し上げます。