ストレージ活用の秘訣:
効果的なサイバー・レジリエンス戦略の立て方

グローバル・ビジネスに対する現在の脅威

人的ミス、システム障害、あるいは悪意のある犯罪的行為と原因が何であろうと、データ漏洩は今日の企業にとって最も重大で経済的損失が大きい脅威です。Ponemon Institute の2018年度の調査によると、過去12カ月におよぶ世界における情報漏洩の平均コストは386万ドルでした。データ漏洩によって、企業は通常業務が中断したり、顧客や企業の信用を失うことになりかねません。

同様に人的な被害もあります。世界経済フォーラム (WEF) の2019年グローバル・リスク・レポートでは、サイバー攻撃を人間の福祉に対する最大リスクの１つとして判断しています。WEFの調査対象者の 82% は、サイバー攻撃によるデータや金銭の盗難リスクが増加するだろうと回答しており、80% は業務やIT基盤自体が中断するリスクも高まると回答しています。

情報システム部門が、幅広い脅威がもたらす新しい課題に対処するには、セキュリティーへの体系的なアプローチが必要です。

情報システム部門が、複雑化するセキュリティーの脅威がもたらす新しい課題に対処するには、最新のセキュリティーへの体系的なアプローチが必要です。先進的な企業は、セーフガード・コピーなど、革新的なストレージ技術を採用しています。また、非常に効果的な既存の物理エア・ギャップ手法を利用して脅威を食い止め、ビジネスへの期待に応えています。このようなアプローチを実施する上でカギとなるのは、適切なリスク管理です。

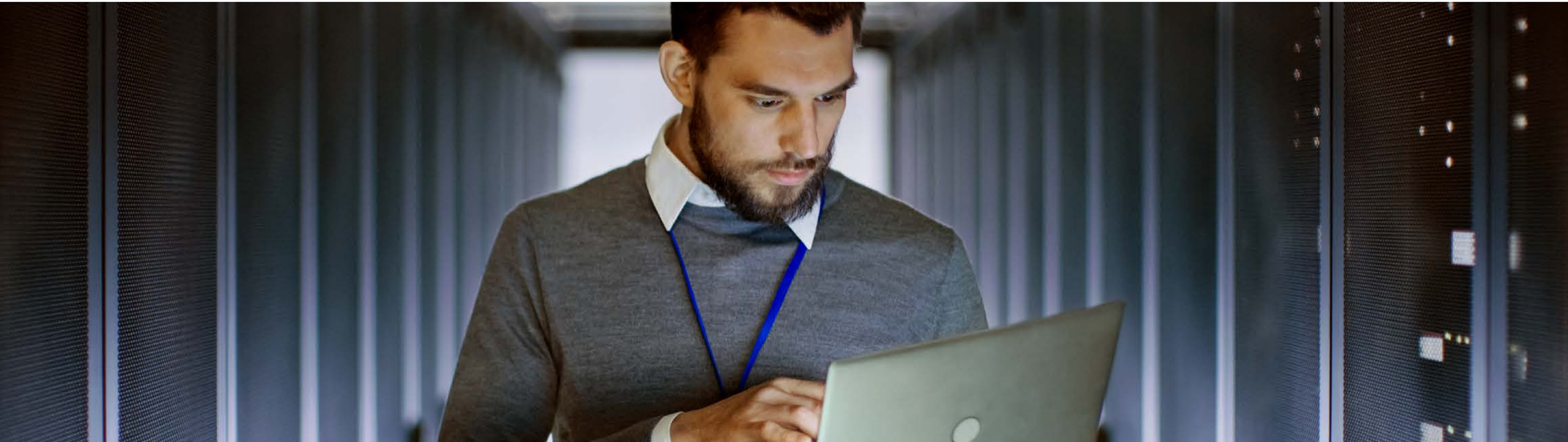
サイバー・セキュリティーとリスク管理

組織が業務の中断を防いだりコストを最小限に抑えたりする方法はすでに多くあります。Ponemon Institute は、データ漏洩のコストを低減するための 4 つの戦略を提案しています。[1]

- インシデント対応チームを作る
- 広範囲の暗号化を使用する
- ビジネス継続性に関して管理する
- 従業員研修を改善する

強固なサイバー・セキュリティー戦略を確立し、維持するには、手続き的アプローチを採用して、所有しているデータとシステム資産、その価値、被るリスクを理解する必要があります。リスク管理の原則を採用して組織の現在および望ましいセキュリティーの状態をプロファイリングすることで、可能な限り幅広い層でサイバー・レジリエンス戦略を実装することを検討できるようになります。サイバー・レジリエンス戦略の評価と実装には、強力なフレームワークが極めて重要です。

サイバー・レジリエンス戦略の評価と実装には、強力なフレームワークが極めて重要です。



NIST フレームワーク: IBM サイバー・レジリエンス・ライフサイクル

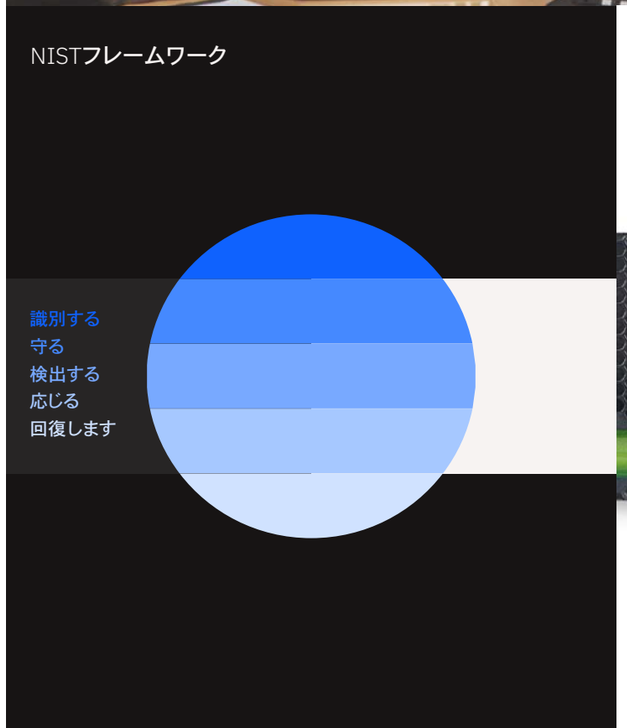
2018 年、米国標準技術局 (NIST) は、*重要インフラのサイバー・セキュリティーを改善するためのフレームワーク。*を公開しました。このフレームワークは、フレームワーク・コア、フレームワーク・インプリメンテーション・ティア、フレームワーク・プロファイルの 3 つのパートが特徴です。[3]

フレームワーク・コア内には一連のサイバー・セキュリティーの機能が存在します。これらの対策はどの企業にも必要であり対応可能です。:

- **特定:** システム、人、資産、データ、機能にもたらされるサイバー・セキュリティーの脅威に関する組織的な理解を促進します。
- **保護:** 適切な保護対策を講じて重要なサービスを確実に提供する。
- **発見:** サイバー・セキュリティーの事象を発見する。
- **対応:** サイバー・セキュリティー・インシデントに対して対策を取る。
- **回復:** サイバー・セキュリティー・インシデントによって損なわれた機能またはサービスを復元させる。

これらの役割を連携させることで、組織のサイバー・セキュリティー・リスクをもっとよく把握できるようになります。はっきりと理解することで、適切なストレージ・ソリューションが何かを見定めることができるようになります。

これらの機能を連携させることで、組織のサイバー・セキュリティー・リスクをもっとよく把握できるようになります。



ストレージ・インフラストラクチャーの役割

ストレージはこれまで長きにわたって、企業運営における「データ管理者」の役割を担ってきました。システム・ストレージ層は、データをメイン・メモリーからの保管場所としてコンテナーを提供するほか、組織が異常な事態から回復するのを支援する保護機能を提供してきました。時間の経過とともに、これらの機能の範囲は拡大しました。

- **バックアップ:** 1960 年代以降、データの誤削除、破損、もしくはプライマリー・デバイスの故障からデータを守るために、アプリケーション・ユーザーがある時点でのデータを別のメディアに保管できるようにしてきました。
- **高可用性:** 約 20 年間、ストレージはマルチパス・アクセス、マルチサーバー・アクセス、およびマシン・ルーム内でのデータのオンライン・コピーの複製を作成する設計を提供してきました。
- **災害対策:** 1990 年代後半以降、ストレージは停電や自然災害から保護するのに十分な、アクティブ・データのコピーを遠隔地で作成する仕組みを提供してきました。
- **高速オンライン・データの高速復旧:** 2010 年代の初頭から、ストレージは誤削除やデータ破損からの迅速な復旧を実現するデータのスナップショット・コピーを提供してきました。

いずれの場合も、リスク事例のさまざまな問題に対処するために、ストレージ・システム、管理ソフトウェア、および業務プロセスに新機能が導入されました。

一般的なストレージ機能から、特にサイバー・レジリエンス関連の機能へとシフトする中、ブロック、ファイル、オブジェクト、テープ、ソフトウェア・デファイン・ストレージ、およびクラウドにまたがって提供される 4 つの主要機能があります。

- **隔離**とは、ネットワークの残りの部分からスナップショットまたはバックアップ・データをネットワークの他の部分から分離する度合いです。隔離は、保護されたコピー、クラウド・オブジェクト・ストレージを利用した論理的手段、または物理的なエア・ギャップを通じて達成できます。
- **改ざん不能機能、**または改ざん防止ストレージ によって、内外の攻撃者によるデータの改ざんや削除を防止します。
- **パフォーマンス** は、サイバー・レジリエンス・フレームワークの重要な能力です。組織はどのくらい迅速にサイバー攻撃から回復できますか? テープはバックアップ・データの分離と改ざん防止に優れていますが、復旧には数時間かかることがあります。
- **再使用のしやすさ**、またはバックアップ・データへのアクセスのしやすさは、復旧手順をテストし、バックアップを検証、サンドボックス環境にデータを復元して、ランサムウェアのインシデントが発生した場合に有効な復旧ポイントを見つけるために重要です。

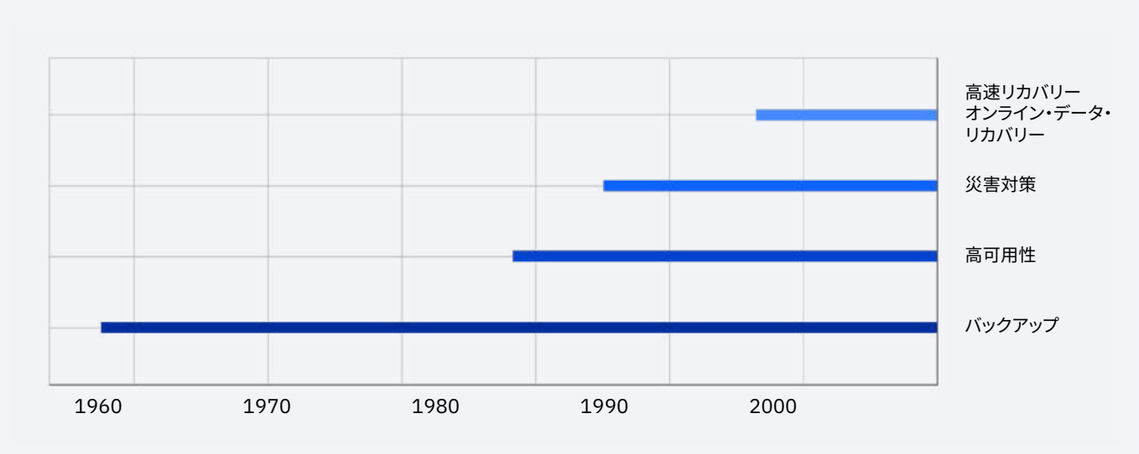


図 1: 長期にわたって変化してきたストレージ保護機能

サイバー攻撃、特にランサムウェアやワイパー攻撃による論理データ破損 (LDC) の脅威により、一連の新しい保護方法を検討する必要が生じています。ソリューション・プロバイダーが、必要とされるレベルの回復力を達成したい場合には、バックアップや災害対策用にすでに存在するストレージ・ツールの一部を借りることができるでしょう。ただし、新しい脅威に対処するには、新しいストレージ機能も必要です。

ストレージ機能と業務プロセスを組み合わせて、高度なマルウェア攻撃に直面した場合でもデータの最新のリカバリ・コピーを保持するメカニズムが必要です。攻撃が検出されて対策が開始されたら、これらの保存されたコピーを使ってアプリケーションを再起動し、通常のサービスを再開することができます。

IBM® Safeguarded Copyは、ユーザーのエラー、悪意のある破壊、マルウェア、ランサムウェア攻撃によるデータの変更または削除を、本データの改ざん不能なポイント・インタイムコピーとデュアル・コントロール・セキュリティーにより防止します。

IBM Redpaper *DS8000® Safeguarded Copy* では、保存されたコピーを作成するために必要な新しい 3 つの機能を識別します。

- **精度:** 組織は、破損事故の場合のデータ損失を最小限に抑えるために、複数の保護コピーを作成できなければなりません。
- **隔離:** 保護コピーは本番データから分離して、ウィルス感染したホスト・システムによって破損されないようにする必要があります。(これは、「エア・ギャップ」ともいいます)。
- **改ざん不能機能:** コピーを不正操作から保護する必要があります。[4]

IDC は『Five Key Technologies for Enabling a Cyber-Resilience Framework』で 自動化とオーケストレーション、および規制レポートと遵守の2つの考慮事項を追加しています。[3] これらは LDC への攻撃耐性に特化した事項ではありませんが、ベスト・プラクティスに組み込むことをお奨めします。

ストレージ・インフラストラクチャー・ソリューション

優れたストレージ・ソリューションは、LDC 攻撃や偶発的な混乱に直面した場合に回復力のある IT 運用を構築するための幅広い機能を提供します。包括的なソリューションは、ストレージの機能、ネットワーク構成、管理制御、物理的セキュリティーを組み合わせたものです。

スナップショット、WORM (追記型光ディスク) メディアで保護されたバックアップ、テープによるエア・ギャップ保護、クラウド・オブジェクト・ストレージなど、現在提供されている主要なサイバー・レジリエンス・ソリューションとテクノロジーをいくつか見てみましょう。

従来のスナップ・ショット・ベースのバックアップとリカバリー
スナップショットは、従来のバックアップの要件に対処する最もパフォーマンスが高くコスト効率の高い方法の 1 つになりました。スペース効率に優れた読み取り専用のデータコピーは、コスト効果の高いリカバリー・ポイントを提供し、前のバージョンのデータの迅速な復元に使用できます。スナップショットを使用して、誤削除や破損から回復することは広く行われています。

保護されたスナップショット
スナップショットを保護する最善の方法は何でしょうか? 1つのアプローチは、本番システムから同じタイプのセカンダリー・ストレージ・システムにストレージ・ボリュームを複製することです。その後、定期的なスナップ・ショットをセカンダリー・アレイのリカバリー・コピーとして使用することができます。複製とスナップショット機能はソフトウェアで自動化する必要があります。非本番環境のストレージ・システムをアプリケーション・サーバーに直接接続することは避けください。アクティブなストレージ・データ接続は、バックアップ・コピーを受信するポートのみにします。

LDC マルウェア攻撃が発生した場合、またはリカバリー操作のテストを実施する場合は、非本番システムに保存したデータ・コピーを、本番ストレージ・システムに戻すことができるリカバリー・コピーのソースとして使用する必要があります。非本番環境のストレージ・システムを使用することで、本番データのコピーと保護コピーの間に論理的なエア・ギャップができます。システム間の物理的な分離では、実装設計が重要になります。同じデータセンター内であっても、距離が近いほどパフォーマンスが高く、ネットワーク・コストが低減します。非本番ストレージ・ソリューションを 災害対策 向けリモート施設に含めるといいでしょう。

WORM メディアで保護したバックアップ
機能的なバックアップおよびアーカイブ・ソフトウェア・システムは、データの完全コピーを管理されたストレージ領域に移し、変更されたデータを保存することでバックアップ・バージョンを維持できます。リカバリー・コピーの保護には、WORM メディアが役立ちます。テープ・カートリッジは WORM として識別され、テープ・ドライブによる上書きから保護されたリカバリー・コピーの書き込みに使用できます。WORM カートリッジへの格納後、アプリケーションまたは管理サーバー内のどのタイプのマルウェアもバックアップ・コピーを破壊することはできません。

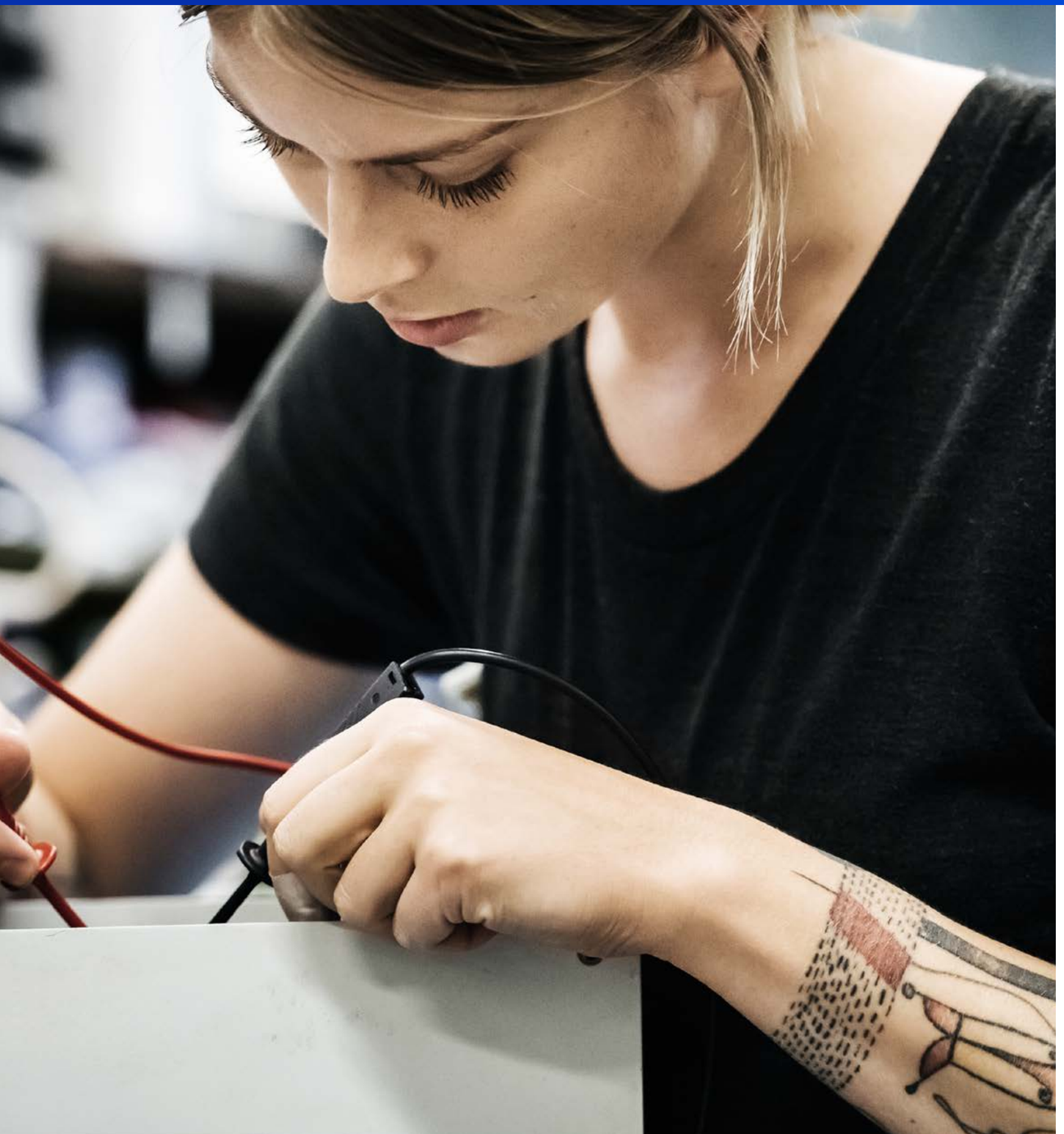
スペース効率に優れたスナップショットとは違い、テープに書き込まれたフル・コピーの場合、データの移動に時間がかかります。リストアも、スナップショットで達成できるよりもはるか遅くなります。ビジネス・ニーズに応じて設計をカスタマイズする必要がありますが、スナップ・ショット・ベースのリカバリーを構築して、データをオフライン・メディアに配置するバックアップで補強する方法が望ましいかもしれません。

強力なテープ・エア・ギャップ保護
「エア・ギャップ」という用語は、マルウェア感染、システム障害、または人的ミスによるデータ破損の広がりを防ぐために、システムまたはネットワークの物理的または仮想的な隔離を意味します。エア・ギャップの基本概念は、セカンダリー・ストレージ・システムを定期的にオンラインにして、最新の変更内容を取り込んだあと、再びオフラインにすることです。スナップショット機能を使用してコピーを作成するアプローチをすばやくマウントして、破損したアプリケーションを回復できます。

ただし、コピーされたデータの完全な保護にはいくつか制約があります。ネットワークまたは保護されたコピーへのソフトウェア・アクセスを行わない最も完全な保護手法は、テープ・ライブラリーを使って実装できます。テープの「オフライン設計」の特徴は真の物理的エア・ギャップを実現し、サイバー攻撃に対処する最もセキュアな保護の 1 つとなります。

エア・ギャップ手法、WORM、他のセキュリティー機能の使用など、テープによるデータ保護の詳細については、IBM テープ・ソリューションによる強力な最新のデータ保護ソリューション・ブリーフをご覧ください。

クラウド・オブジェクト・ストレージによるデータ保護
クラウド・オブジェクト・ストレージは、データをアーカイブし保護するための、耐久性が高くセキュアで費用対効果に優れた手段です。ポリシーを定義することで、デフォルト、最小、最大の保存期間を柔軟に指定できます。これらの保管期間およびその他のリーガル・ホールドは、データがクラウドに保存するたびに、1 つまたは複数のオブジェクトに適用できます。そのため、保管期間が終了し、すべてのリーガル・ホールドがなくなるまでオブジェクトを削除することはできません。



セキュリティーの最適なバランスを両立させる

データへのアクセスを拒否したりデータを破壊したりするサイバー攻撃は、決してなくなりません。それどころか、さらに高度化しています。だからこそ、組織が使用しているテクノロジーとデータ保護に採用している哲学のバランスを両立させることが、効果的なセキュリティー戦略の策定には必要不可欠です。攻撃の成功から回復するための対策も、適切に設計されたセキュリティー体制の重要な部分になります。

いずれの場合も、主要なセキュリティー機能を備えた多くのストレージ・ソリューションは、組織のシステムを「害を及ぼすように設計された一連の脅威」から保護する上で重要な役割を果たします。ただし、今日の脅威の状況および保護する必要がある情報をしっかり理解しないと、バランスを両立させる作業は、大変なことのように思えるかもしれません。

現代の企業は、NIST フレームワークやリスク管理の規則などのアプローチを利用して、包括的なストレージ戦略を構築することができます。スナップショット、テープのエア・ギャップ保護、クラウド・オブジェクト・ストレージのようなテクノロジーを使用してサイバー・レジリエンス・ソリューションを構築し、実装することができ、増大する脅威に直面して組織の安全を維持することができます。

準備不足の状態に陥らないようにしてください。サイバー・レジリエンス戦略の策定に関する詳細情報については以下をご覧ください: https://www.ibm.com/jp-ja/it-infrastructure/storage/mainframe.

参照情報

1. “2018 Cost of a Data Breach Study: Global Overview.” Ponemon Institute、2018 年 7 月
2. “Global Risks Report 2019, 14th Edition.” 2019 年の世界経済フォーラム、スイス・ジェノバ
3. Phil Goodwin and Sean Pike, “Five key technologies for enabling a cyber resilience framework.” IDC、2018 年 7 月
4. Bert Dufrasne、Francesco Anderloni、Roger Eriksson、および Lisa Martinez “IBM FlashSystem A9000 and A9000R Business Continuity Solutions, A draft IBM Redpaper publication.” IBM Corp.、2018 年 11 月