IBM レジリエンシー・オーケストレーションによるサイバー攻撃からの復旧

サイバー攻撃から短時間で復旧を可能にする、信頼性が高く拡張が容易な復旧機能により、データおよびITプラットフォームを保護

ハイライト

- データ・ファイルおよびプラットフォーム構成ファイル用のエアギャップで保護されたイミュータブル・ストレージ(不変ストレージ)。
- Windows やLinux のシステム構成内の異常を即時に検出(Windows レジストリー、アプリケーション構成、デバイス構成など)。
- データやプラットフォーム構成を短時間で統合的にに復旧することにより、サイバー攻撃などにより生じる障害の影響を低減。
- テストの自動化と検証プラットフォームを活用し、ビジネス・システムに影響なくテストを実施可能。
- プロセスに対する可視性とレポート作成により、コンプライアンス要件に対応。

サイバー攻撃は、どの企業にとっても大きな課題となっています。IT 部門やセキュリティー部門の対策によりサイバー攻撃への対応は進んでいるものの、依然として、攻撃は万が一起こったら(「もしも」)ではなく、いつ起きてもおかしくない(「いつも」)考えておくべき問題です。サイバー攻撃による重要なデータやシステム構成の破壊による業務の混乱は、データの漏えいや 全てのIT の機能停止に匹敵し、企業の財務状況や評判に打撃を与える恐れがあります。

これは、データ暗号化や、データ・バックアップを狙ったマルウェアに関わるサイバー攻撃に特に言えることです。バックアップや災害復旧 (DR) のロケーションがネットワークに公開され続けると、これらのデータがマルウェアによって破壊されたり暗号化されたりして、本番データもバックアップ・データも使用できなくなる危険性があります。そうなった場合、本来の業務再開が大幅に遅れてしまいます。

多くの場合、既存の DR ソリューションがサイバー攻撃からの復旧まで想定していなかったり、復旧作業がほとんど手動であったり、手順書が古かったり、テストが不十分だったりといった、DR 機能が常に抱えるような問題が、こうした損害の発生につながっています。その結果、復旧に時間がかかり過ぎたり、データのリカバリー・ポイントが古過ぎたり、さらに復旧そのものが失敗したりすることもあります。

サイバー・レジリエンスに対応するための機能

IBM レジリエンシー ・オーケストレーションのサイバー・インシデント・リカバリー機能は、サイバー攻撃によりシステムが停止した際に、データやプラットフォーム構成を短時間で復旧することを目的に設計されています。このサイバー・インシデント・リカバリー機能には、主に以下のような機能があります。

- 本番環境に影響を及ぼさない、簡単なテスト機能。
- ダウン時間の最小化につながる、データ破損の迅速な検出と迅速な対応。
- リカバリー・ポイント目標 (RPO) を最適化する、効率的なポイント・イン・タイム・リカバリー。
- 大規模なサイト・レベルでの検出とリカバリーを数分で行える、拡張の容易性。
- シンプルな可視化機能と、レポート機能により、各種法規制への対応をサポート。

サイバー・インシデント・リカバリー機能を構成するテクノロジー・ビルディング・ブロックは、本番環境と DR 環境のコンピュート・レイヤーとデータ・レイヤーにわたってプラットフォームを提供し、サイバー攻撃による障害からの迅速な復旧をサポートします。このアーキテクチャーには以下のようなものがあります。

イミュータブル・ストレージ(不変ストレージ)。 構成データにイミュータブル・ストレージ(不変ストレージ)技術を使用し、アプリケーション・データに WORM(*)ストレージを使用することにより、一度保存されたバックアップの破損を防止し、確実なリカバリーを行うことができます。WORM(*):Write Once Read Manyアプリケーション・データについては、この方法を使用することで、ストレージ・コストの削減にもつながります。

エア・ギャップによる保護。 ネットワークを隔離することで、本番環境をリモートまたは DR サイトで保護されているWORM ストレージのバックアップ・データと分離できます。また、WORM ストレージへのアクセスも、データのバックアップ時のみに制限されます。この方法をイミュータブル・ストレージ(不変ストレージ)と組み合わせることで、ネットワークをトラバースしたり、バックアップ・データを狙うマルウェアによる保護データの破壊を防止します。

構成データの検証。 このコンポーネントは、保護対象の構成やデータがクリーンで復旧可能なものになるよう、サポートします。レジリエンシー・オーケストレーションに組み込まれたこのプロセスは、システム構成が変更され、それが「ゴールデン」バージョンと一致しないと、それを自動的に検出します。レジリエンシー・オーケストレーション をお客様のアプリケーション妥当性検証スクリプトと統合して、アプリケーション・レベルとデータ・レベルでのテストを行うこともできます。

オートメーションとオーケストレーション。 レジリエンシー・オーケストレーション では、データ、アプリケーション、スイッチ、およびコンピュート・インフラストラクチャーの復旧プロセスをエンド・ツー・エンド (E2E) で自動化し、IT 環境の迅速な回復を実現します。レジリエンシー・オーケストレーション は、従来の手動のプロセスを、テスト・検証済みの事前定義されたワークフローに置き換えます。これにより、ボタンをクリックするだけで、ビジネス・プロセス全体、アプリケーション、データベース、または個別のシステムを復旧できます。これらのワークフローは、相互接続されたシステムやデータの復旧に必要な複数の手順を統合したもので、人的ミスを防ぎます。レジリエンシー・オーケストレーションは、ワークフロー定義に使える部品(事前に定義されたパターン) を450種異常ライブラリーとして用意しているので、ソリューション実装までの時間の短縮を実現します。

プラットフォーム構成用の サイバー・インシデント・リカバリー

常時業務を行うためには、物理サーバー、VM インスタンス、ストレージ・システムおよびネットワーク・デバイスといったビジネスに不可欠なアプリケーションの基礎となる IT インフラストラクチャーの継続的な可用性が必要となります。サイバー攻撃の攻撃者は、これらのプラットフォームの構成データを破壊することで、業務を停止させます。

サイバー・インシデント・リカバリー のプラットフォーム構成機能 (図 1) は、サーバーやデバイス構成データの「ゴールデン・コピー」を、クラウド・オブジェクト・ストレージまたはIBM データ・センターにエアギャップで保護されたイミュータブル・ストレージ(不変ストレージ)に複製することで、短時間でサービス回復を実現します。本番稼働デバイスは検査され、構成データに加えられた変更が検出されます。システムは変更を分析し、その変更が適切なものであるかどうかを判別し、構成データに疑わしい変更が検出されるとアラートを出します。また、このアラートによって、変更制御管理ソフトウェアから関連するチケットが発行されます。

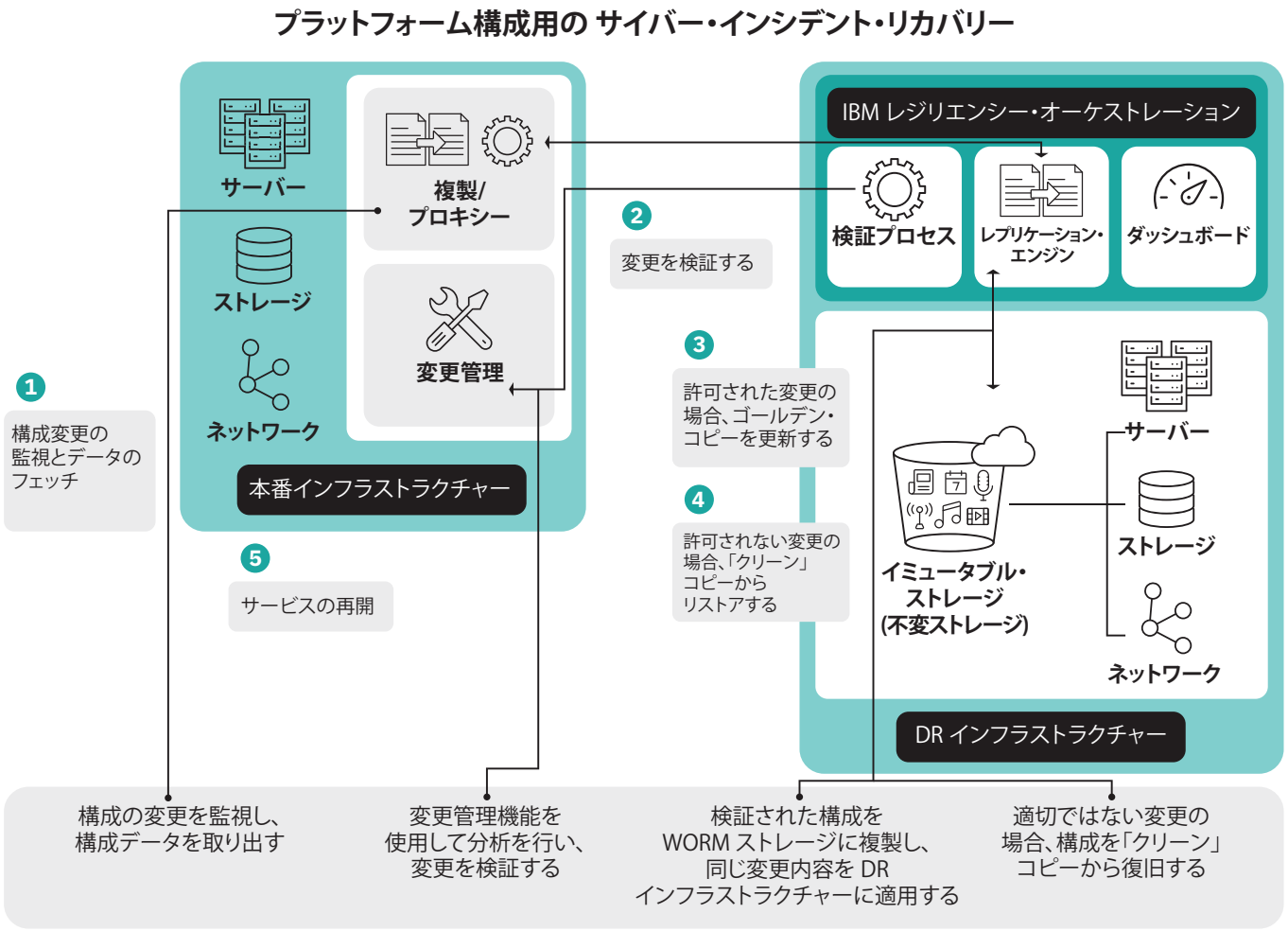

図 1. プラットフォーム構成用の サイバー・インシデント・リカバリー は、ストレージやネットワーク・デバイスだけでなく、物理サーバーおよび仮想サーバーの構成データも保護します。

有効な変更であった場合、構成データは新しい「ゴールデン・コピー」をイミュータブル・ストレージ(不変ストレージ)に複製することで保護されます。適切ではない変更が検知された場合、レジリエンシー ・オーケストレーションが事前準備されたポリシーと適切な承認に基づいて、デバイス構成の最新のクリーン・コピーを本番環境に即時に復旧します。専用の仮想マシン構成は、クリーンな本番環境に復旧されます。

データ用の サイバー・インシデント・リカバリー

サイバー・インシデント・リカバリーのデータ機能は、データそのものを破壊するサイバー攻撃に対して、信頼性の高い、短時間での復旧を実現します。この機能は、エア・ギャップによる保護およびイミュータブル・ストレージ(不変ストレージ)を使用することでデータを保護しながら、お客様のDR サイトで迅速に復旧します。

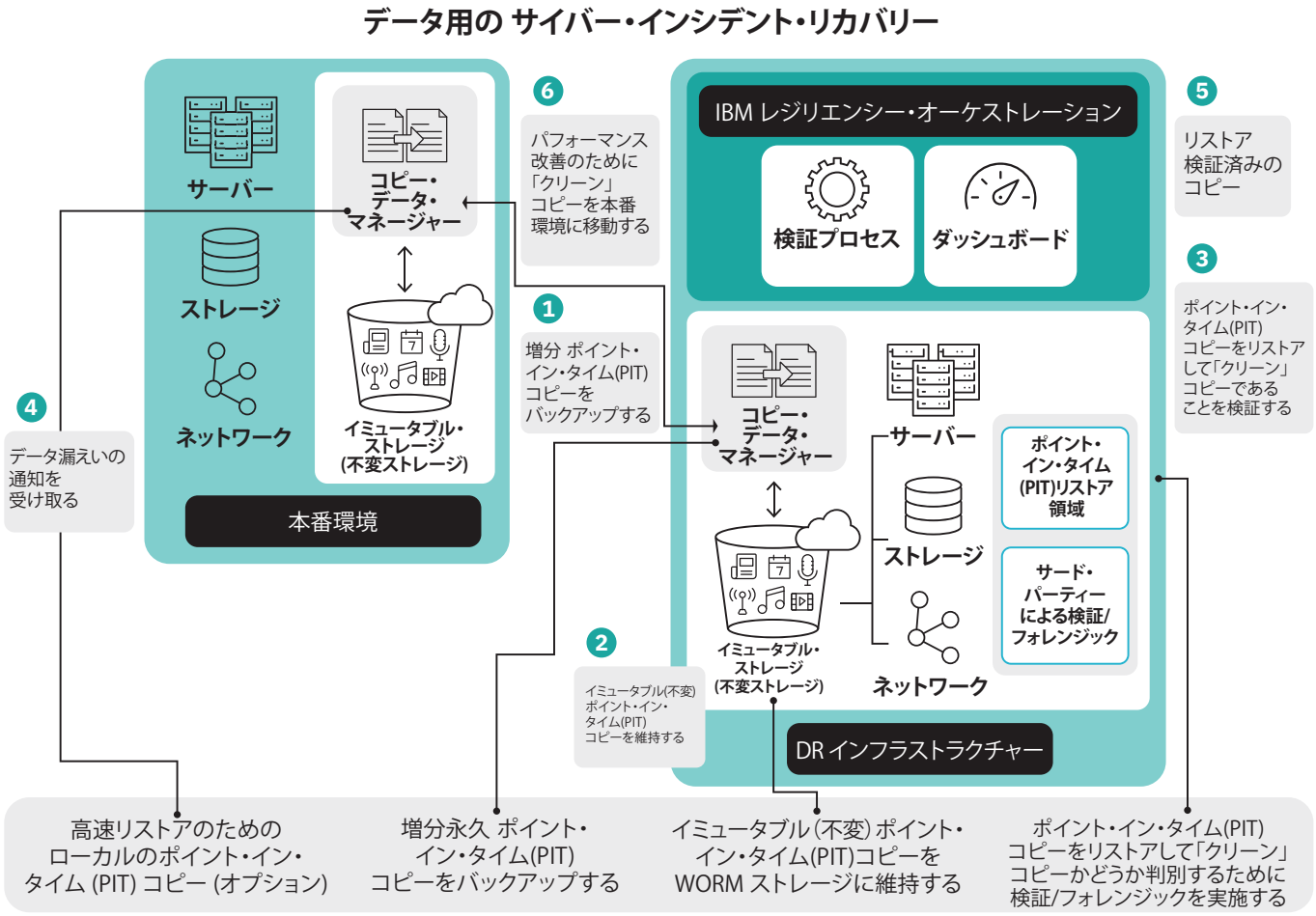

図 2. データ用の サイバー・インシデント・リカバリー は、大規模なデータの効率的なバックアップと、中断を伴わないテストおよび短時間での復旧を可能にします。

サイバー・インシデント・リカバリーは、大規模なアプリケーション・データを扱うことを想定して設計されています。コピー・データ管理テクノロジーを採用し、データの増分ポイント・イン・タイム (PIT) コピーを作成して保持します。クラウド・オブジェクト・ストレージまたは WORMストレージなどのイミュータブル・ストレージ(不変ストレージ)に保持されるこれらのコピーは、変更ができない「永久」コピー です。図2に示すように、コピー・データ管理ソフトウェアは、データを DR サイト (代替サイト) に複製し、ポイント・イン・タイム(PIT) コピーを作成します。オプションで、ポイント・イン・タイム(PIT)コピーを本番サイトに保管することで、迅速な復旧を実現することもできます。

データ・ブリーチや暗号化のマルウェア感染が検出されたという通知を災害復旧管理者が受け取ると、DR サイトで ポイント・イン・タイム(PIT)コピーの自動テストが実行され、データの復旧の可能性を検証します。テストや検証のプロセスで最新の「クリーン」コピーとして判別されると、そのコピーはコピー・データ管理ソフトウェアの高速復旧プロセスによって DR インフラストラクチャー上で復旧されます。DR サイトでテストを頻繁に実施することで、ビジネス・オペレーションに影響を与えることなく、データの復旧の可能性を確認することもできます。レジリエンシー・オーケストレーション は、プラットフォームを短時間で並行して　復旧できるようサポートします。

ダッシュボードとレポート作成機能が管理をシンプルに

サイバー・インシデント・リカバリーには、プラットフォーム構成の変更やデータの変更のモニターをサポートするダッシュボード機能 (図 3) があります。また、サイバー攻撃に対する重要な復旧情報を経営陣や取締役会にリアルタイムで提供することもできるため、詳細な情報を得た上で迅速な判断を下すことが可能になります。

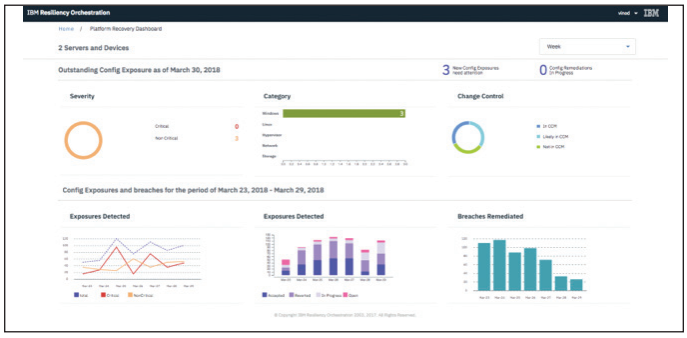

図 3. 総合ダッシュボード

サイバー・インシデント・ダッシュボードは、脆弱性の数や重大度レベルといった詳細情報を提供するため、未解決の脆弱性を追跡することができます。サイバー・データのダッシュボードは、CR RPO、CR RTO、スナップショット検証状況、サイバー攻撃に対する現在の準備状況を可視化します。

レポート作成機能を活用すれば、サイバー・レジリエンスや DR 体制などの豊富なレポートを活用して、通常のオペレーションで作成したグラフと併せて、規制当局に提出し、コンプライアンス対応を容易に実施することができます。

IBM をお勧めする理由

IBM レジリエンシー ・サービスは、世界中のお客様のバックアップや復旧の各種ご要望に60年近くにわたって対応してきた豊富な経験があります。今日では、9,000 社以上のお客様に弊社の災害復旧サービスおよびデータ管理サービスをご利用いただいており、年間およそ 3.5 エクサバイト以上のデータのバックアップをサポートしています。世界 60 カ国以上にある 300 カ所以上の IBM レジリエンシー ・センターで災害復旧やデータ保護を提供し、6,000 名以上のスペシャリストが対応しています。

詳細情報

サイバー・インシデント・リカバリー の詳細については、日本 IBM の営業担当員にお問い合わせいただくか、次の Web サイトをご覧ください。
ibm.com/jp/services/business-continuity/cyber-resilience

IBM グローバル・ファイナンシングは、さまざまな選択肢をご用意して、お客様のビジネス成長に必要なテクノロジーのご利用を支援しています。IBMはIT 製品とサービスのライフサイクル全体を管理をお手伝いします。詳細については、次の Web サイトをご覧ください。**ibm.com**/jp/financing/jp/

日本アイ･ビー･エム株式会社
〒103-8510
東京都中央区日本橋箱崎町19-21

IBM のホーム・ページ:
ibm.com


Please Recycle

89017289-JPJA-02