サイバーレジリエンスの獲得：サイバー攻撃対策のコストをZertoで管理、軽減する

サイバー攻撃への備え、対応力、回復力を強化

米国のIT調査会社IDCによるサイバーレジリエンスに関する調査レポート『State of IT Resilience 2019』は、ランサムウェアなど、サイバー攻撃の増加傾向を明確に示しています。特に、データの損失やビジネスの中断につながるサイバー攻撃の脅威が顕著になっています。全500社を対象とした調査結果の概要は以下のとおりです。

- **84%**の企業が過去12か月以内に悪意ある攻撃を受け、そのうち
- **89%**の攻撃が実害をもたらし、さらにその
- **93%**がデータの破損または損失につながっています

このようなサイバー攻撃の被害は収まる気配がありません。それどころか、新しい変異種が現れたり、日々技術的な進化を遂げ、攻撃の深刻さと頻度が増すばかりです。それに比べ、サイバーセキュリティの伝統的な戦略が進化する速度は遅く、24時間年中無休の可用性が求められるビジネスを保護するには十分ではありません。
そのため、サイバーセキュリティの戦略を「サイバーレジリエンス」にシフトする企業が増えています。ネットワークのパラメータを保護することに集中するのではなく、グローバルでハイブリッドなクラウド環境でリスクを軽減する戦略が主流になりつつあります。
サイバーレジリエンスには、サイバー攻撃に対する準備、対応、そして、被害を受けたときの回復が含まれます。サイバーセキュリティ戦略はもはや防止だけにとどまるべきではなく、重要データの整合性を確保するための一貫した対策が必要になります。したがって、サイバーレジリエンスは、人とプロセスと技術の3要素が柱となります。

人とプロセス：サイバーレジリエンスに根差した盤石なプロセスと行動様式

サイバー攻撃への抵抗力を養うには、きちんとした枠組みが必要です。現代のITチームは、NIST（米国国立標準研究所）フレームワークのような特定の枠組みを採用して、サイバーセキュリティのアプローチにおける各ステップに正確性を期しています。これには、脅威に対する防御、検知、識別、リカバリのプロセスや方法論が含まれます。
正しい準備を整えることは非常に大切ですが、正しいデータリカバリ技術を導入し、実践することも同じぐらい重要です。たとえば、継続的データ保護（CDP-Continuous Data Protection）技術を活用したZerto IT Resilience Platform™のような信頼性の高いツールの導入が不可欠です。

注目ポイント

ほんの数秒でリカバリ

サイト全体、アプリケーション、仮想マシン（VM）、ファイルを数秒でリカバリでき、しかも多岐にわたる柔軟な選択が可能。

アプリケーションの整合性を保つ

複数VMアプリケーションをまるごと同じチェックポイントからリストアできる一貫性のあるリカバリ機能。

短期または長期のデータ保持

Zertoの特別なジャーナル技術で短期/長期の柔軟なリテンション設定が可能。

業務を中断しない継続的テスト

本番環境に影響を与えることなく、隔離された環境でリカバリをテスト。テスト環境における補足レポート機能も充実。

データ フォレンジックの徹底

個別のネットワークにデータを隔離して、本番環境へのリストア前に整合性を確認。

Zerto | Climb Inc. Growing to Meet Your Needs

サイバー攻撃の脅威は継続的データ保護（CDP）で撃退

デジタル トランスフォーメーション（DX）に取り組んでいる企業の82%は、データ保護の戦略を進化せることがDXの成功に欠かせない、と考えています。このような傾向がIDCの『State of IT Resilience 2019』によって明らかにされています。これは、従来のリカバリ ソリューションの進化が十分ではない、と考えられていることを意味します。スナップショット バックアップの技術では、時間的なギャップが生じるのを避けられず、データの損失につながる危険性があります。リカバリに時間がかかり、企業全体の業務を中断させるリスクもつきまといます。

ランサムウェアの攻撃を受けたとき、Zertoのおかげで、その攻撃を15分でくい止め、3時間でシステムを再稼働できました。Zertoの力がなければ、身代金を払わなければならなかったし、それでデータが回復できたかどうかも定かではありません。

ClearPath Mutual、システム管理者
Rubyanne O'bryan

Zertoがもたらす違い：継続的データ保護（CDP）の真価

リカバリ ポイントの継続的なストリーム

ZertoのElastic Journalは、精密な設定が可能なジャーナル技術と長期保存リポジトリを組み合わせ、リカバリ ポイントの継続的なストリームを提供します。数秒、数分、数時間、あるいは数年単位で遡れる柔軟性が実現します。

アプリケーションの整合性

Zertoでは、仮想保護グループ（Virtual Protection Group）を通じて完全な整合性を確保し、アプリケーションのスタック全体を保護、リカバリできます。複数VM（仮想マシン）にまたがる整合性を、それらがインフラストラクチャのどこで稼働していようとも保つことができます。

業務を中断させない継続的なテスト

ZertoのIT Resilience Platform™が災害復旧（DR）テストのオーケストレーションと自動化を可能にします。わずか4回のクリックで、いつでも簡単にテストを実行できます。

ランサムウェア攻撃からのリカバリも数秒で

ランサムウェアの攻撃を受けたときも、Zertoの革新的なジャーナル技術で、ファイル、VM、アプリケーション、あるいはサイト全体を安全なチェックポイントに簡単にリカバリできます。ほんの数秒前のチェックポイントへもリカバリ可能です。

Climb Inc. Growing to Meet Your Needs 株式会社クライム
www.climb.co.jp
本　社／〒103-0014 東京都中央区日本橋蛎殻町1-36-7 蛎殻町千葉ビル4F
Tel:03-3660-9336 Fax:03-3660-9337 E-mail:soft@climb.co.jp
大阪営業所／ Tel:06-6147-8201　名古屋営業所／ Tel:052-462-1282
福岡営業所／ Tel:092-686-8637