DELL Technologies

サービス概要

# Cyber Recovery サービス

サイバー リカバリー戦略を策定し、リカバリー プログラムを実装する

## 基本情報

**Dell Technologies Cyber Recovery サービス：**

- サイバー攻撃後に中核的なビジネス機能を復旧できる信頼性の高いサイバー リカバリー ヴォールトに、必要最小限の企業体制を構築します
- リカバリー戦略と、組織全体のインシデント対応計画との統合ポイントについて助言を提供します
- NIST サイバーセキュリティ フレームワークに合致したリカバリー ソリューションを統合し、多様な脅威ベクトルに対応する計画を策定します
- リカバリー計画および手順を作成し、テストします

## ビジネスの課題

サイバー攻撃が頻発しています。その結果、ダウンタイムが長くなり、ビジネス オペレーションが数日から数週間にわたって中断され、膨大な損失が発生する場合があります。機密情報や専有データの露出の懸念にとどまらず、データ破壊やデータ暗号化による身代金要求に特化したサイバー攻撃がますます増えているのが現実です。最近のランサムウェア攻撃の多くは、特に製造システム、病院の情報システム、銀行システム、地方自治体に大きな損害を与えています。こうした攻撃は従来の境界セキュリティ制御を擦り抜けることができます。攻撃者は数か月、時には数年にもわたり検出されないまま、可能な限り多くのシステムに影響を及ぼし、ビジネスの復旧をますます困難にします。組織外の攻撃者に加え、残念なことに、内部関係者が関与するサイバー攻撃が増加しており、経営幹部は、あらゆるタイプの脅威に対してビジネスを保護するために備える必要があります。こうした要因により、あらゆる業界のビジネス リーダーが、サイバー攻撃が発生した場合に復旧できるという保証を求めています。

サイバー攻撃は巧妙化が進み、より破壊的になっています。このため企業は、破壊的なサイバー攻撃に確実に対処できるようにするための「最後の防御線」となる新しいデータ保護とサイバー セキュリティのユース ケースを検討する必要があります。

## サービスの内容

最新のアプローチでは、最も重要なデータ（必要不可欠なアプリケーション、データ、知的財産など）のコピーを本番ネットワークから分離された場所で保管し、本番バックアップ システムからも分離しておくことに重点が置かれています。ネットワークに直接接続しないようにして、複数のロールバック ポイントを用意することで、セキュリティ侵害を受けていない「ゴールド コピー」をリカバリーに利用することができます。

Dell EMC PowerProtect Cyber Recovery は、エアギャップ型のデータ保護ヴォールトの実現をサポートします。また、Dell Technologies Services との連携により、テクノロジーとプロセスの採用を加速し、サイバー攻撃からの復旧に対する安心感を向上させることができます。当社のサービスは、アドバイザリーと実装という 2 つの主要分野に重点を置いています。

アドバイザリー フェーズでは、お客様のデータ保護環境に Cyber Recovery を統合して最適化するための推奨事項の提供に重点を置いています。お客様の現在および将来の状態を分析して、サイバー リカバリーの準備を整えるための独自の戦略を、保護とリカバリーに対するビジネス ニーズと緊密に合致させつつ構築します。

アドバイザリー フェーズの主要な要素として、ワークショップと情報セッションがあります。この目的は、お客様のアプリケーションに関するデータを収集し、通常業務に対する重要性を理解することです。こうした考察をもとに、Cyber Recovery Vault で何を保護すべきかについての助言を行い、必要最小限の企業体制、つまり中核的な機能を再構築し事業運営を再開するために最も重要なデータとアプリケーションを集めたものを作り上げます。

実装フェーズでは、Cyber Recovery Solution をデータ保護環境に統合します。このフェーズでは、アドバイザリー フェーズを通じて収集した情報を使用して、お客様の具体的なニーズに合わせてソリューションを調整できます。また、Cyber Recovery 環境に、次のように追加のテクノロジーと機能を統合することもできます。

- ヴォールト インフラストラクチャを導入する
- CyberSense 分析を導入してデータを分析し、侵害の早期兆候を特定する
- Cyber Recovery Vault 要件をサポートするために本番バックアップを変更する
- 追加の本番環境のデル・テクノロジーズ インフラストラクチャを強化する
- Cyber Recovery Vault と機能をメインフレーム環境と統合する
- 複数のプラットフォーム、異機種混在テクノロジー、保存ポリシー、アプリケーションを含む Cyber Recovery Vault を作成する
- ヴォールトからのリカバリーを実行するための、詳細な運用手順書（リカバリー ランブック）を作成する
- 詳細なリカバリー ランブックや追加のテスト シナリオの作成をサポートする

## メリットの概要

サイバー攻撃が急増するなか、今や問題は組織が影響を受けるかどうかではなく、いつ影響を受けるかになっています。どの企業においても自社のサイバー インシデント対応やサイバー リカバリー戦略によって達成する必要がある独自の目標、目的、IT 要件があります。当社のコンサルティング エキスパートがお客様と協力して、破壊的なサイバー攻撃が発生した場合でも、ビジネスを保護し、復旧できるようにするプロセスと処理手順を開発します。

Dell Technologies Services は以下を実現します。

- エアギャップ型の Cyber Recovery Vault ソリューションと推奨事項により、ヴォールト内に必要最小限の企業体制を作成し、サイバー攻撃が発生した場合にリカバリーを可能にします。
- 特定のコア アプリケーションを保護し、そのリカバリー機能を証明することで、規制圧力が厳しさを増すなかでのコンプライアンス目標の達成を支援します。
- NIST サイバーセキュリティ フレームワークに合致したリカバリー戦略をインシデント対応準備に盛り込みます。

Dell Technologies Services の詳細はこちら

デル・テクノロジーズのエキスパートへのお問い合わせはこちら

他の関連資料を見る

#DellTechnologies で会話に参加する