サイバー攻撃から迅速にリカバリーするための専門知識とリソース

業務の妨げとなるサイバー インシデントに対し十分な準備を整え、自信を持って運用

Dell Incident Recovery Retainer Service

サイバー攻撃のリスクとコストは増大の一途をたどっています。ビジネスを遂行できなくなれば、財務実績、顧客関係、法令遵守、企業の評判に悪影響が及びます。

攻撃が発生した場合、リカバリーの成功に最も重要なのは対応スピードです。しかし、通常のオペレーションを再開する作業は非常に困難なことがあります。インシデントの封じ込めに加えて、遅延を最小限に押さえ、重要なアプリケーションをオンラインに復帰させるには、IT環境と大量のデータをリストアする必要があります。

75%
2025年までに1回以上攻撃を受けると予想される組織の割合[1]

97%
サイバー イベントを経験したお客様のリカバリーの成功率[2]

16日
ランサムウェア攻撃後の平均ダウンタイム[3]

多くのITチームには、サイバー攻撃からのリカバリーに必要な能力やスキルの組み合わせが不足しています。**Dell Incident Recovery Retainer Service**では、業界認定を受けたサイバーセキュリティおよびインフラストラクチャ専門スタッフのチームが、お客様と緊密に協力して環境を復旧します。このサービスには**120～240**時間のリカバリー支援が含まれているため、注文の承認を待つ必要がありません。当社のチームがすぐにリカバリーに取りかかります。

リカバリー準備状況の評価を実施します。当社は、サービス開始時にお客様の組織の現在のリカバリーおよびリストア戦略を把握することが重要であると考えています。当社の経験豊富なチームが既存のリカバリー計画、ネットワークおよびインフラストラクチャ、バックアップ プロセスなどをレビューします。このチームが作成する評価および計画サマリー レポートを通じて、インシデント準備状況とリカバリー態勢の強化に向けたロードマップをお客様に提供します。

主なメリット

- インシデントが発生した場合：
  - 高度なスキルと経験を持つDellのサイバーセキュリティ エキスパートが迅速に対処
  - 当社のチームがお客様の状況を迅速に評価し、ビジネスの中断を最小限に抑えるための最適な対処方法を判断
  - 脅威を取り除き、悪用された脆弱性を解消[4]
- リテーナー モデルで年間**120～240**時間のリカバリー支援を提供
- デル・テクノロジーズのサイバーセキュリティ チームが、お客様固有の状況に対応できる豊富な経験、スキル、ツールを提供
- 既存のリカバリー機能および範囲についてリカバリー準備状況の初期評価を実施し、サマリー レポートを通じて改善のための優先事項を提案
- Dellチームは初期評価を通じてお客様の環境を把握しているため、リカバリー プロセスがより効率的に

主要機能

年間120～240時間のインシデント リカバリー アクティビティー

- リモートでの実施（地域によってはオンサイトでの実施も可能。追加料金がかかります）
- プロジェクト マネージャーによるアクティビティーの監視
- インシデントおよび状況の評価
- リソースの割り当てと導入
- フォレンジック分析 - デジタル、マルウェア、データ
- 脅威の除去
- データ サニタイゼーション、リカバリー、保全
- 環境およびアプリケーションの復元

インシデント リカバリー機能の評価

- エンゲージメント開始時に実施
- サイバーセキュリティ インシデント発生時の対応準備として、お客様のネットワーク、インフラストラクチャ、および設備を把握
- インシデント リカバリー計画、データ バックアップ、およびリストア機能をレビュー
- **Dell**が作成するサマリー レポートを通じて、準備状況およびリカバリー態勢の強化に向けた提案事項を提示

サービス レベル：

- お客様の最初のリクエストから**2**時間以内にお客様とのサービス開始ミーティングのスケジュールを設定（平均初動時間）
- サービス開始ミーティング後**6**時間以内にリモート対応を開始（平均対応時間）
- オンサイト対応について合意を得ている場合は、サービス開始ミーティング後**24**時間以内に開始（平均対応時間）

利用時間と残り時間について、四半期ごとにお客様と確認

- リカバリーおよびリストア時間をすべて使い切らなかった場合は、残り時間を専門スタッフによるインシデント リカバリー計画作成、サイバーセキュリティに関する改善、および関連領域での支援に振り向けることが可能

さまざまな利用状況に対応

サイバーセキュリティ インシデントがいつ発生するかを正確に知ることは不可能です。**Dell Incident Recovery Retainer Service**で不測の事態に備えましょう。高度なスキルを持つ経験豊富なサイバーセキュリティ プロフェッショナルが速やかに対応し、脅威を取り除いて重要なオペレーションの再開に向けて活動するため、お客様は安心してシステムを運用できます。

ぜひセールス担当者にお問い合わせください

[1] 『Detect, Protect, Recover: How modern backup applications can protect you from ransomware』、Nik Simpson、Gartner（2021年1月6日）、GartnerドキュメントID G00733304 https://www.gartner.com/en/documents/3995229

[2] 北米における2019年6月～2021年7月のサービス リクエストに関するDellの分析に基づきます。

[3] 『Why Ransomware Costs Businesses Much More than Money』、Forbes（2021年4月30日）https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=469c541a71c6

[4] サービスに含まれる年間120～240時間を超えるリカバリー作業が必要な場合、追加時間をご購入いただけます。