DELL Technologies

突発的なサイバー インシデントに備えていますか？

サイバー攻撃に伴うリスクとコストは増加し続けています。その中でも、ランサムウェア攻撃は企業運営にとって多大な損害が生じる攻撃の1つです。数週間または場合によっては数か月間という長期にわたって事業運営を行えないことは、組織が長期的な成功を収める上で大打撃となる可能性があります。

リカバリーは非常に重要であり、通常の運営に戻るための取り組みは極めて困難なものとなります。サーバーや大量のデータとアプリケーションをリストアし、最も重要なアプリケーションをできるだけ早くオンラインにして、目標リカバリー時間（RTO）を達成するには多大な労力が必要となります。

72%

の企業が、ITセキュリティとリスクの要件をすべて確実に満たすために外部の支援を必要とすると報告しています。[5]

ビジネスを戻すために必要不可欠な支援を提供

インシデント対応およびリカバリーサービス

業界が認めた当社のサイバーセキュリティ専門家チームがあらゆる段階でお客様と連携します。デル・テクノロジーズのグローバル ネットワーク規模によって支えられているため、すばやく対応して脅威を排除し、迅速かつ中断を最小限に抑えながら事業運営をリストアできます。

サイバー脅威は増え続け、その影響は甚大になる可能性がある

間隔にして 11 秒おきに サイバー攻撃またはランサムウェア攻撃の被害に見舞われている[1]

16 日間 ランサムウェア攻撃後の平均ダウンタイム[2]

75% の組織が2025年までに1回以上攻撃を受ける[3]

数にして 60% 以上 の企業が脆弱性の悪用によるデータ侵害を経験している[4]

インシデント対応およびリカバリー サービス

Dell Technologies Servicesには、サイバー事件の被害に遭ったお客様のリカバリーにおいて実績があります

⚠ インシデントが発生。何をすべきでしょうか？

事業運営が影響を受けると、次の問題が発生する可能性があります。

- Eメールが停止する
- データにアクセスできない
- マルウェア
- ネットワークが停止する
- **Active Directory**が停止する
- トランザクションを処理できない
- 身代金を要求されている

支援を受ける

支援を受ける

当社の専門家チームが迅速に対応いたします。お客様に行っていただくのは次の連絡先までお問い合わせいただくことだけです。
Incident.Recovery@dell.com

リカバリー

インシデント対応およびリカバリー（IRR）チーム

あらゆる段階で専門家がお客様をサポート

信頼できるエキスパート

業界が認めたサイバーセキュリティ専門家で構成された専属チームが、幅広い人材とドメインにわたって広範な専門技術とベスト プラクティスを提供します。

状況に関係なく必要なサポートを提供

当社のサービスは、お客様が直面している状況や何が影響を受けているのかに関係なくお客様のニーズに対応します。まずはお客様の状況を評価し、最適なリソースを手配してお客様が迅速にリカバリーできるようにします。

当社の取り組み

攻撃を受けて間もない場合でも、すでに着手しているリカバリー作業をさらに早く進めるための支援を必要としている場合でも、当社の専門家が次の対応を行います。

- 適切なリソースを評価し導入する
- 脅威を排除しセキュリティ リスクを軽減する
- ビジネス アプリケーションをインシデント発生前の運用状態に戻す
- 従業員が業務に戻れるようにワークステーションを再導入する
- エキスパートによるデータ フォレンジック サービスを提供する
- セキュリティの向上を支援する

支援を受ける

- 数分/数時間以内に電話で手配し、通常は48時間以内にチームをオンサイトに派遣
- さまざまな場所と言語に対応した複数のワークストリームを使用して100以上のリソースを拡張し、必要に応じて柔軟に調整
- 大半が10年以上の経験を持つ業界認定のサイバーセキュリティ専門家を派遣
- Dell製およびDell製以外のインフラストラクチャとエンドポイント デバイスに関する専門技術を提供
- エッジ、クラウド、法務、保険などに関する知識と経験を提供
- 170以上の市場にグローバルに対応
- 革新的な従量制課金ソリューションを活用することで、ITソリューションのコストをテクノロジーの利用と投入可能な予算に合わせて調整および拡張可能**

リカバリー

- 脅威を与える存在を排除する
- 通常の運営に迅速に戻れるようにする
- 既存のITスタッフを拡充してワークロードの増加に対応できるようにする
- 強化されたネットワーク環境を再構築する
- 繰り返し発生するサイバー攻撃を防ぐためのセキュリティ戦略を策定し実施することで、セキュリティ体制を強化する
- ベスト プラクティスの教育と共有

詳細については、こちらにアクセスしてください：**Delltechnologies.com/incident-response-and-recovery**

** Payment solutions provided to qualified commercial customers by Dell Financial Services (DFS) or through Dell Technologies group companies and/or through Dell's authorized business partners (together with DFS "Dell"). Offers may not be available or may vary by country. Offers may be changed without notice and are subject to product availability, eligibility, credit approval and execution of documentation provided by and acceptable to Dell or Dell's authorized business partners. In Spain, services are provided by Dell Bank International d.a.c branch in Spain and in remainder of the EU by Dell Bank International d.a.c, trading as Dell Financial Services which is regulated by the Central Bank of Ireland. Dell Technologies, DellEMC and Dell logos are trademarks of Dell Inc.

[1] 2021年度の推定値、Cybersecurity Ventures：https://cybersecurityventures.com
[2] 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
[3] Detect, Protect, Recover: How Modern Backup Applications can protect you from ransomware」、Nik Simpson、Gartner（2021年1月6日）https://www.gartner.com/doc/reprints?id=1-258HHK51&ct=210217&st=sb

[4] デルの委託によりForrester Consultingが作成したソート リーダーシップ ペーパー「BIOS Security – The Next Frontier for Endpoint Protection」（2019年6月）
[5] Forrester Consultingがデル・テクノロジーズに代わって実施した委託調査（2020年12月）