

デジタルテクノロジー

ランサムウェア対策 バックアップ



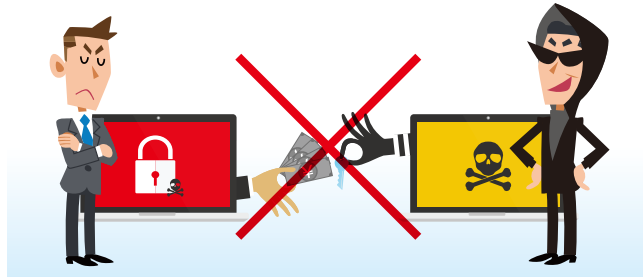
被害が拡大し続けているランサムウェア、すべての企業・組織がそのターゲットです

ランサムウェアの猛威はとどまるところを知りません。日本情報処理推進機構 (IPA) が発表した「情報セキュリティ10大脅威2023」でも、ランサムウェアがトップにランキングされています。実際にランサムウェア被害の報告件数は増加傾向にあり、警察庁の資料によればその半数以上が中小企業であることがわかっています。つまり規模や知名度に関わらず、すべての企業・組織がターゲットになり得るのです。

ランサムウェア攻撃者に屈しないためには**4つの事前対策**が必要です

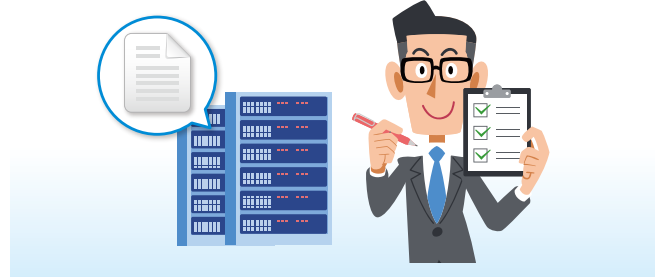
事前対策 1 絶対に身代金は支払わないと組織として定めておく

データが暗号化されて業務が止まってしまった状況では、相手(反社会的勢力)の言いなりにならざるを得ません。万が一身代金を払ったことが発覚すれば、社会的信用は失墜し、事業継続は困難になります。従って、絶対に身代金は支払わないと組織として定めておく必要があります。



事前対策 2 復旧手順と被害想定洗い出しを事前に実施

バックアップデータが存在しても、それを適切にリストアできなければ意味がありません。実際に攻撃を受けた際に確実に復旧できるよう、復旧手順や影響範囲などを事前に洗い出しておきましょう。



事前対策 3 しかるべきシステムでバックアップを取得する

ランサムウェアでデータを暗号化・破壊された場合でも、もとのデータが存在すればそこから復旧を行うことができ、身代金を支払う必要はありません。しかしこのようなデータを確保し続けるには、バックアップデータの隔離やWORM、振る舞い検知などが適切に考慮されている必要があります。



事前対策 4 エンドポイントのセキュリティを強化する

警察庁の調査によれば、多くの攻撃でVPN機器の脆弱性が悪用されていることがわかっています。しかし攻撃箇所はこれだけではなく、セキュリティ対策が十分ではない端末もランサムウェアの温床になっています。これらのセキュリティ強化はデジタルテクノロジーにおまかせください。



バックアップによるデータプロテクションに必要な**3つの条件**

条件 1 攻撃者の手の届くところから隔離されていること

攻撃者の標的となるシステムは主に「ファイルサーバー」「AD*サーバー」「バックアップサーバー」です。その中でもWindowsベースのバックアップシステムは、サーバー攻撃と同時にデータも被害を受けることが一般的で、この問題を回避するために必要なのが、サーバーからデータを物理的もしくは論理的に隔離することです。たとえば、重複排除ストレージやテープ装置、パブリッククラウドを活用し、二次バックアップ環境を構築することなどが考えられます。またデータ復旧時は、安全性を確保するためにどのような手順でアクセスするか、明確に決めておく必要があります。

*AD: Active Directory



条件 2 WORM機能を実装していること

WORMとは「Write Once, Read Many」の略称です。これは、一度書き込んでしまえば上書きや削除は一切できない、という概念を指します。バックアップシステムがこの機能を備えていれば、ランサムウェアが元データを暗号化しても、別データとして保存されるため元データは安全に残り続けます。そのため万が一の攻撃を受けても復旧が可能です。



条件 3 振る舞い検知機能を実装していること

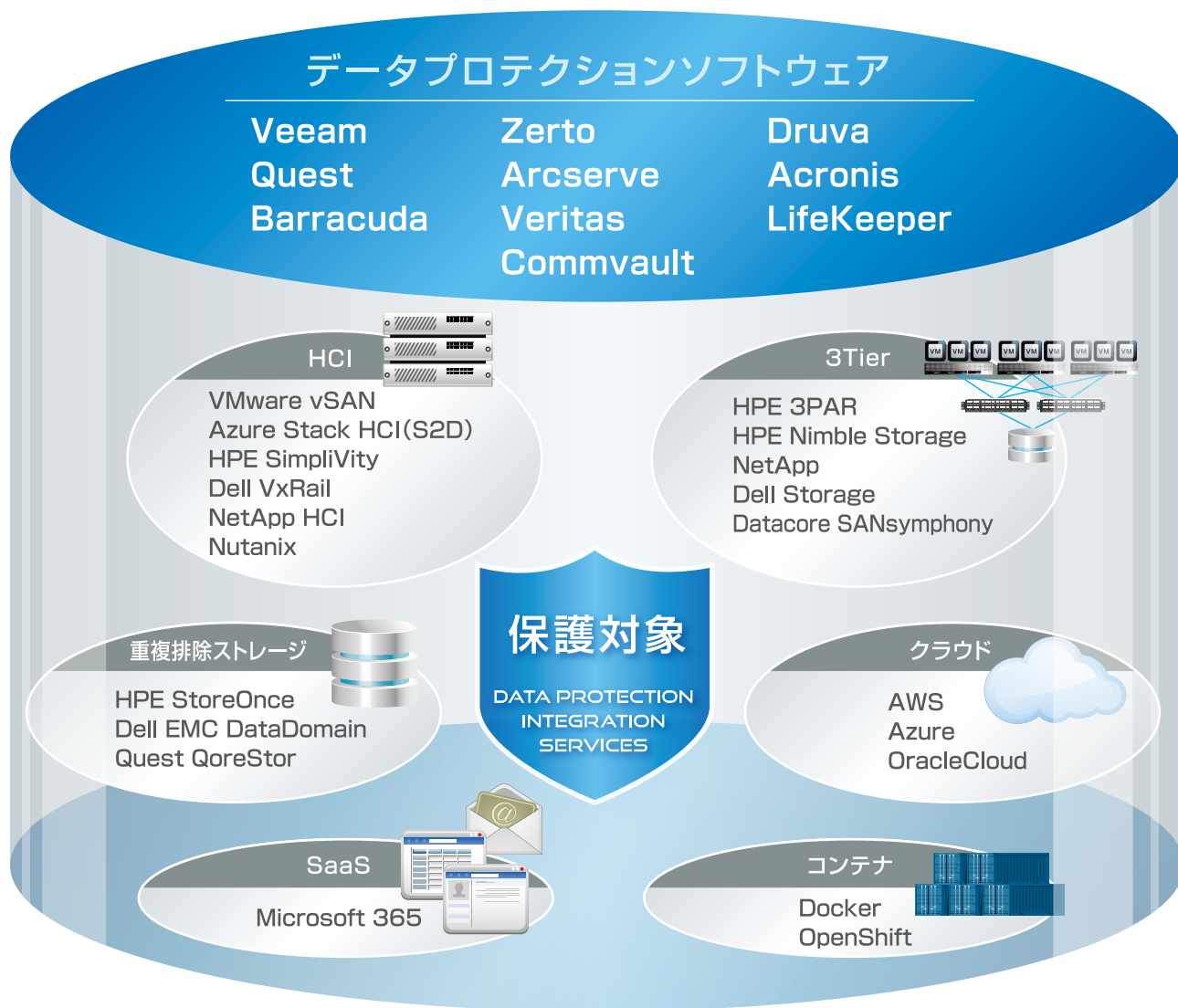
バックアップシステムにおける振る舞い検知とは、常にファイルのバックアップの変化量をモニタリングしておき、ファイルの急激な増減を検知した場合、アラートを通知する機能です。この機能を保有することにより、ランサムウェア攻撃の初期段階で発見し、感染前のファイルを特定・復旧することが可能になります。



ランサムウェア対策で重要なデータプロテクション
そのソリューションはデジタルテクノロジーにお任せください

デジタルテクノロジーの取り扱い製品

3Tierの仮想化環境やHCIといったオンプレミスシステムはもちろんのこと、各種クラウドサービスや、コンテナ環境までカバー。幅広い環境に対応できるデータプロテクションソフトウェアをラインアップしています。



スピード対応

お問い合わせ対応の所要時間を徹底的に削減。対応開始までお待ちいたしません。

構築・テストのみでも対応OK

既に製品選定、設計が完了している場合、構築のみで請け負うことも可能です。

プロアクティブトータルサポート

データ保護単体ではなくシステム全体のサポートも可能です。トラブル対応はもちろんのこと、ファームアップや運用支援など、お客様の快適な運用を支えるサポートを行います。

ランサムウェア対策のための データプロテクションソリューションは、 デジタルテクノロジーにお任せください。



デジタルテクノロジー株式会社

<https://www.dtc.co.jp/>

[東京] 〒104-0032 東京都中央区八丁堀 2-23-1 エンパイヤビル
MAIL: sales@dtc.co.jp

[大阪] 〒530-0001 大阪市北区梅田1-13-1
大阪梅田ツインタワーズ・サウス 15F
MAIL: osaka@dtc.co.jp