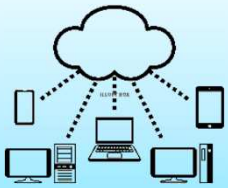
SUNSYSTEM
創業1991年
2026年1月号



クラウドサービスも
サンシステムへ

オフィスのパートナー
有限会社サンシステム
三田市東本庄2070番地の5
TEL079-556-7663 FAX079-556-7664
E-mail:oa-shop@oa-sunsystem.co.jp
URL:www.oa-sunsystem.co.jp

重要なお知らせ

ランサムウエアについての対策

アサヒGHD、アスクルが甚大な被害に遭遇した、ランサムウエアについての対策を考えてみましょう。

中小企業が今すぐやるべき「感染しない」ための基本対策

ランサムウェア対策というと、高額なセキュリティ製品や専門人材が必要だと思われがちですが、実際には今すぐ・低コストで始められる基本対策が被害防止に大きく効きます。重要なのは「特別なこと」ではなく、「当たり前を確実に続けること」です。

①OSや業務ソフトのアップデートを後回しにしないこと

更新通知が出ても「業務が忙しい」「止まると困る」と放置されがちですが、攻撃者はその“更新されていない隙”を狙って侵入します。実際、多くの被害は既に修正済みの脆弱性を放置していたことが原因です。月に一度でもよいので、アップデートを確認・適用する日を決め、習慣化しましょう。

②次に重要なのが、IDとパスワードの管理

同じパスワードを複数のサービスで使い回していると、ひとつ漏れただけで被害が連鎖します。特にVPNやクラウドサービスでは、パスワードに加えて「追加の確認」を行う多要素認証（MFA）を必ず有効にしましょう。スマートフォンで確認するだけでも、不正ログインの多くを防げます。

③セキュリティソフトについても見直しが必要

従来のウイルス対策ソフトは、既知のウイルスを防ぐことには有効ですが、侵入後の不審な動きを見逃すことがあるからです。最近では、端末の挙動を監視する仕組みを備えた製品も登場しており、予算に応じて段階的に検討する価値があります。すべてを一度に導入する必要はなく、重要な端末から始めるだけでも効果的です。

④従業員への基本的なルール共有

ランサムウェアの多くはメールをきっかけに侵入します。「心当たりのない添付ファイルは開かない」「マクロを有効にしない」「少しでも怪しいと感じたら確認する」といったシンプルなルールを、口頭だけでなく文書で共有し、定期的に注意喚起することが重要です。

基本を徹底するだけで、ランサムウェアに「狙われにくい企業」になることができます。

次に侵入されても事業を止めない「バックアップ」について考えましょう

ランサムウェア対策では「侵入を防ぐこと」が注目されがちですが、現実にはそれだけでは不十分です。どれほど対策を重ねても、未知の攻撃手法や設定ミス、取引先を起点とした侵入など、すべてを防ぎ切ることはできません。だからこそ今、多くの企業で重視されているのが、「侵入される前提」で事業を止めないための考え方、すなわちサイバーレジリエンスです。その中心にあるのが、本当に機能するバックアップです。

バックアップの基本として、まず「3-2-1ルール」

①データを3つ持つこと
②本番データに加えて2つのバックアップを用意すること
③保存先は2種類以上の異なる媒体に分けること
④そしてそのうち1つはクラウドなどの遠隔地に保管すること
を意味します。このルールの本質は、「1箇所に依存しない」ことです。
どこか1つが攻撃や障害で使えなくなっても、必ず復旧できる逃げ道を残しておく–この設計思想こそが、ランサムウェア時代のバックアップには欠かせません。

外付けHDDやNASを社内ネットワークに常時接続したままバックアップ先として使っていると、
ランサムウェアに感染した瞬間、そのバックアップ先までまとめて暗号化されてしまいます。
攻撃者にとっては、本番データもバックアップも区別はありません。ネットワーク上に見えるものは、
すべて標的になります。この状態では、バックアップは「保険」ではなく「一緒に壊れる部品」になってしまうのです。

ランサムウェアは、事前対策を講じていても完全に防ぎ切れるとは限りません。
だからこそ重要なのが、「感染に気づいた直後に何をするか」です。
初動対応を誤ると、被害が拡大し、復旧の選択肢を自ら狭めてしまいます。
初動対応の流れを順を追って整理します。

①感染が疑われる端末をネットワークから切断すること

LANケーブルを抜く、Wi-Fiをオフにするなど、物理的・論理的に通信を遮断します。
社内全体が止まる事態を避けるためにも、迷わず実行する必要があります。

②電源を切らないこと

慌ててシャットダウンしてしまうと、メモリ上に残っている攻撃の痕跡が消えたり、復旧や調査に必要な情報が失われたりする可能性があるからです。また、種類によっては暗号化処理が途中で暴走し、被害を悪化させるリスクもあります。専門家の指示を仰ぐまでは、現状を維持することが原則です。

③速やかに専門機関や警察に相談します

社内だけで判断しようとすると、対応が遅れたり誤った選択をしがちです。
なお、身代金の支払いは原則として推奨されていません。支払ってもデータが復号される保証はなく、結果的に犯罪組織への資金提供につながってしまいます。
公的機関や専門事業者と連携し、冷静に対応することが重要です。

最後に行うのが、バックアップからの復旧です。
攻撃前の状態に戻せるバックアップがあれば、事業停止を最小限に抑えることができるからです。逆に、バックアップが使えなければ、復旧までに長期間を要し、経営そのものに深刻な影響を及ぼします。

ランサムウェアは、特別な企業だけに起こる事件ではありません。
地震や台風と同じように、「いつか必ず起こり得る災害」として考えるべき時代に入っています。そして災害と同じく、事前に備えがあれば、過度に恐れる必要はありません。
被害の大小を分けるのは、運や規模ではなく「準備の有無」です。

来月はバックアップについて考えてみましょう！