



ランサムウェア、あなたの会社も標的に？ 被害を防ぐためにやるべきこと



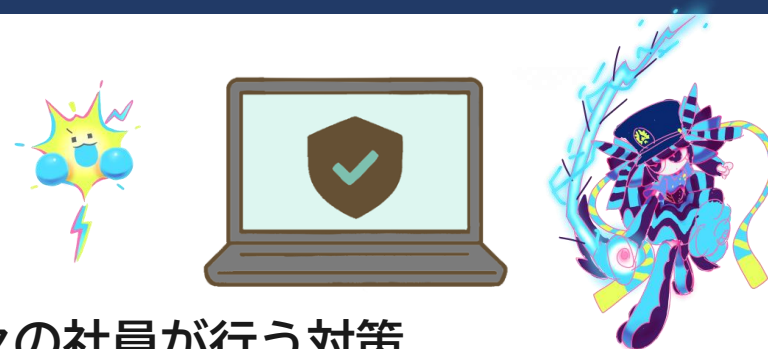
「ランサムウェア」とは、「身代金」を意味する英語「ランサム(Ransom)」と「ソフトウェア(Software)」とを組み合わせた言葉です。パソコンやサーバをウイルスに感染させて、保存されているファイル等のデータを勝手に暗号化することで使用できない状態にした後、それを元に戻すことと引き換えに「身代金」を要求する不正プログラムです。

ランサムウェアに感染すると

- ・ ファイルが暗号化されて使用できなくなる
- ・ ファイルの復号のための金銭の支払いを要求される
- ・ 会社の業務システムやオンラインシステムなどが感染すると、通常の業務運営ができなくなる

国内の大手メーカーで工場
の操業を一時停止せざるを得
なくなった事案も発生！

ランサムウェア被害の未然防止や 軽減のために企業ができる対策は？



個々の社員が行う対策

- ・ メールのリンク、添付ファイルを開く際は慎重に行う
- ・ パスワードは複雑にし、使い回さない、多要素認証を利用するなどアカウントを適切に管理する
- ・ 管理者の許可を得ずソフトウェアをインストールしない
- ・ セキュリティ教育を受けリテラシーを高める

企業・団体全体で行う対策

- ・ OS等を最新の状態にする
- ・ ウイルス対策ソフト等を導入する
- ・ 認証機能を強化する
- ・ ファイアウォール等を設定して不審な通信をブロックする
- ・ 不要なユーザーの削除や権限を最小化するなどアクセス権を適切に管理する
- ・ データの定期的なバックアップとネットワークから切り離してバックアップを保管する
- ・ セキュリティ教育と業務継続計画(BCP)

被害に遭ったときの対応は？

- ・ 感染した端末をネットワークから隔離
- ・ 感染した端末の電源を切らない
- ・ 組織全体で対応する
- ・ 警察に相談・通報する

企業の皆様からの情報提供がサイバー空間の安全につながります。

茨城県警察ホームページ>サイバーコンテンツにアクセス
・ 専門用語を使わず15分で学べる「サイバー衛生研修」
・ ランサムウェアを動画(政府広報オンライン動画)で解説

