小規模組織向けサイバーセキュリティ

# ランサムウェアチェックリスト

## ランサムウェアに関するレディネス

☐ **ランサムウェアの防止および保護対策を策定する中で、以下の点を定期的に評価する:**

- 貴組織では、定期的なスケジュールバックアップを実施しているだろうか？
- 貴組織のネットワークには、必須でないデバイスが接続されているだろうか？
- 貴組織は、身代金の支払いに伴う法規上のリスクについて把握しているだろうか？
- 貴組織では、ソフトウェアシステムを定期的にアップデートしているだろうか？ こうしたアップデートは自動化されているだろうか？
- 貴組織は、ランサムウェア攻撃およびデータ損失に対処するための計画を抱えているだろうか？
- システムにはサイバー保険のポリシーがあるだろうか？ ポリシーがある場合、ランサムウェア攻撃はどのように補償されるだろうか？

## リアルタイム保護

☐ **新たな脅威インテリジェンスにリアルタイムで適応できるアンチマルウェア保護システムに投資する。**

☐ **機密または必須情報を収容したネットワークに接続した全てのデバイスのセキュリティを評価する。**

- ☐ 必須ではない全てのシステムを別のネットワークに接続する。
- ☐ リモートワークセットアップのセキュリティを考慮する。セキュリティツールがオフネットワークでも動作し、全てのWebトラフィックを監視できるようにする。

☐ **フィッシング攻撃および強力なパスワード保護の必要性に関して従業員教育を推進する。**

☐ **実行可能であれば、組織全土における多要素認証の実装を検討する。**

☐ **全てのソフトウェアおよびシステムを定期的にアップデートする。**

- ☐ 可能であれば、自動アップデートに設定を変更する。

☐ **ランサムウェア攻撃および貴重なデータの損失に対処するためのインシデントレスポンスおよび危機管理計画を策定する。**

- ☐ ランサムウェア攻撃が発生した場合に備えて外部コミュニケーション計画を準備する。

## データバックアップ

- ☐ データを常に保護する、セキュアかつ定期的にアップデートされるバックアップシステムに投資する。
  - ☐ USB またはハードドライブを利用する場合は、バックアップの終了後にネットワークコンピューターからこうしたデバイスの接続を物理的に切断する。
  - ☐ クラウドストレージを利用する場合は、サーバーに高レベルな暗号化と多要素認証を配備する。
- ☐ 最悪の場合のディザスタリカバリに備えて、総勘定元帳の読み取り専用コピーを作成しておく。
- ☐ 自動データリカバリおよび修復を実行するシステムを開発する。
- ☐ 重要データおよびビジネスサービスの復元にどの程度の時間を要するか、シナリオを策定する。

## 規制環境

- ☐ 運用環境におけるランサムウェアに関する法規ガイダンスを評価する。
  - ☐ 各国ごとのガイダンスを考慮する。
  - ☐ 金融セクター固有のガイダンスを考慮する。
  - ☐ 国際的な法規要件を考慮する。
  - ☐ 変更されたガイダンスの定期的な評価計画を策定する。
- ☐ 身代金を支払う場合のリスクを評価する。
- ☐ 現地法執行機関と連絡を取る。
- ☐ 攻撃が発生した場合の迅速な情報共有のつながりを築く。
- ☐ ランサムウェアに関するサイバー保険ポリシーのメリットとデメリットを評価する。

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org