

## 長崎県内でランサムウェア被害が発生！

長崎県内の介護施設で、ランサムウェア被害が発生し、サーバ内のデータが暗号化されてしまいました。このほかにも、ランサムウェアの前兆にもなり得るEmotetの被害も散見されています。

自社のシステムのセキュリティ対策を今一度見直すと共に、従業員へのセキュリティ教育の再徹底をお願いします。

### 1 ランサムウェアとは？

感染したパソコンをロックしたり、ファイルを暗号化したりすることによって使用不能にした後、元に戻すことと引き換えに金銭を要求する不正プログラムです。

### 2 どんな点に注意したらいい？

#### (1) 不正アクセス対策

- ・ 多要素認証を活用しましょう。
- ・ 総当たり攻撃の被害に遭わないようパスワード入力上限回数を設定しましょう。

#### (2) アクセス権限の最小化

- ・ システムにアクセスできる人を限定しましょう。
- ・ ユーザーごとに、アクセスできる範囲を必要最小限にしましょう。

#### (3) インターネット接続制御装置の脆弱性の確認

- ・ VPNやゲートウェイなどのインターネットと接続を制御する装置に脆弱性がないか確認しましょう。
- ・ 脆弱性がある場合は、セキュリティパッチを迅速に適用しましょう。

#### (4) 組織内への周知

- ・ メールの添付ファイルを不用意に開かない、URLを不用意にクリックしない、ということを周知しましょう。
- ・ 不審なファイルを開いてしまった場合等には、セキュリティ担当部門に即座に連絡・相談することを周知しましょう。

#### (5) バックアップの取得

- ・ 定期的にバックアップを取っておきましょう。
- ・ バックアップ取得後はバックアップ媒体はネットワークから切り離しましょう。

※ これらのことについて、自組織のシステムを確認してください。システム構築を他社と契約している場合は、契約先に確認してください。

サイバー犯罪被害防止情報について、サイバー犯罪対策課公式LINE (ID: @387ojopi) の中で紹介しています。  
ぜひ、友だち登録 (右記QR) をお願いします。

