

# ランサムウェア被害防止対策

ランサムウェアに、感染すると**自社だけにとどまらず、サプライチェーン**等で結びついた他の事業者・団体へ**多大な影響**が生じます。決して**自社は無関係と思わず、社内での未然防止対策、注意喚起のほか、サプライチェーン全体への目配り**をお願いします。

## ○ 感染を防ぐポイント

### ● VPN機器等の脆弱性対策

VPN機器等のネットワーク機器の脆弱性が狙われています。

日頃から使用機器の脆弱性情報を把握し、機器を最新の状態に保ってください。

(「注意喚起 JPCERT」で検索して確認)

### ● リモートデスクトップの脆弱性対策とパスワード管理

公開されているリモートデスクトップ (RDP) や脆弱性のあるRDPなどが狙われています。

脆弱性を放置せず、パスワードは強固にしましょう。

### ● 電子メール等への警戒

添付ファイルは、送信元に確認してから開く。メールのリンクは開かない。

脆弱性情報が出ている場合は、パスワードが漏えいしたものと考え、脆弱性対策をしたタイミングでパスワードを変更してください。パスワードは、大文字・小文字・数字・記号の組合せによる10文字以上を設定して、使い回さず、多要素認証、IPアドレス等によるアクセス制限と組み合わせてください。

Check Point



サイバー捜査官 ウルミー

## ○ 感染してしまった（疑いがある）際の対応

### ● インターネット・社内ネットワークからの隔離

感染した（疑いがある）際は、有線LANならケーブルを抜き、無線LANなら通信をオフにするなどインターネットや社内のネットワークから遮断してください。

### ● シャットダウン・再起動をしない

気付いたら感染していた（使えなくなっていた）場合は、感染経路調査のため電源を落とさないでください。（目の前で感染が始まった場合に限り、例外的にシャットダウンしてください。暗号化にはある程度時間がかかるため）

### ● 関係機関や警察への通報

事業を所轄する関係機関や警察へ通報してください。

Check Point



サイバー捜査官 ウルミー