RANSOMWARE インシデントレスポンス

1 感染したマシンを隔離する

感染したマシンを物理的にネットワークから切り離します。

2 ランサムウェアのファミリーを特定する

いくつかのランサムウェアファミリーについては、オンラインで復号化ツールを見つけることができ、対応のための時間、コスト、手間を削減できます。

3 バックアップとレプリケーションを停止する

感染を発見したら、すぐに定期的なバックアップジョブを停止し、直前のバックアップデータが上書きされないようにします。適正なバックアップデータは、復旧のために最も重要です。

4 リストアするデータを優先度付けする

リストアを始める前に、通常業務に戻すためにどのファイル/フォルダが重要かを優先度付けします。

5 リストア先を確認する

データをどこにリストアするか?
同じ場所か違う場所か?
データをリストアするための
十分な容量があるかどうか?

6 感染したファイル及びフォルダをソートする

感染したファイルをソートして
おくことで、リストアプロセスを
高速化できます。
感染していないファイルは
リストアする必要が無いからです。

7 リストアするデータを選択する

重要なデータのみリストア
するか、全てのデータを
リストアするかを決めることで、
迅速にリカバリできます。.

8 データをリストアする

目標は、できるだけ早く通常業務を
再開することです。
上のシンプルなステップに従い、
適正にデータをリストアしてください。