

# インターネットセキュリティ

インフラセクション 中道

## ■ 骨子

- ランサムウェアによる実害例
- 原因考察
- 被害防止例

## ■ランサムウェアによる実害例

- 発生日時：2020年9月10日
- 場所：ドイツデュッセルドルフ  
大学病院のサーバ30台
- 被害状況：データアクセス不能による医療中断

## ■原因考察

- ・ 侵入手段は添付ファイル付きのなりすましメール
- ・ VPNソフトウェアの脆弱性を突いたもの

# ■被害防止

- ・ 侵入手段は添付ファイル付きのなりすましメール対策としてはメールのフィルタリングとスキャンが有効。
- ・ ソフト脆弱性の修正プログラムは早急に対処する。しかし修正プログラムを適用しても既にITネットワークに侵入可能な状態になっていた場合は、別手段をとる必要あり。
- ・ 患者データのまめなバックアップ
- ・ 多層防御

## ■ 多層防御

- ・ 侵入されるなどの被害が発生したとしても、すぐに検知し、被害の最小化を図れるように何重にも対応策を張り巡らすこと

## ■ 多層防御

- ・ 侵入されるなどの被害が発生したとしても、すぐに検知し、被害の最小化を図れるように何重にも対応策を張り巡らすこと

# ■まずは自身の足元から

- ・ こまめにwindowsupdateを！
- ・ 不審メールを見極める眼力をつけましょう
- ・ ウィルスセキュリティソフトのレポートも確認しよう



# ■今回は序章

- ・被害は身近にも起きてます
- ・常日頃から関心、慎重な判断をしていきましょう
- ・今後、自分が関心を持った技術などを深掘りし、発表していきます