



# 病院におけるサイバー インシデントの共有

市立東大阪医療センター 経営企画課 鈴木 淳

# ランサムウェアの挙動調査

- ▶ 特定したランサムウェアの特徴として、Power Shellを使うということで、Windowsサーバを中心に調査
- ▶ 取得した情報を漏洩させるようなので、ルータのログを確認
- ▶ ルータはインターネット閲覧をしない想定で設定されていたため、送信に失敗したログが大量に発生していた
- ▶ ルータの記憶容量を超えてしまい不正アクセス時の記録は残っていなかった



- ▶ ルータ単体のログ保存期間は短いため、別途ログを保存するサーバか、監視ツールによるログ取得などを検討する必要がある
- ▶ 通信量などを監視しておくだけでも不正アクセスの予兆が見えるかも

# IPA提供、調査ツール



【参考】

サイバーレスキュー隊 (J-CRAT) 技術レポート2017/  
インシデント発生時の初動調査の手引き  
~WindowsOS標準ツールで感染を見つける~

<https://www.ipa.go.jp/security/J-CRAT/report/20180329.html>



# 復号化ツール公開

- ▶ ランサムウェアの復号化ツールまとめサイト「NO MORE RANSOM」

<🔒/>  
**NO MORE RANSOM**

**復号ツール**

パートナー 当プロジェクトについて 日本語

ホーム ランサムウェアの特定 ランサムウェア Q&A 被害防止のアドバイス

**復号ツール** 犯罪を報告する

重要！復号ツールをダウンロードして作業を開始する前に、ガイドをお読みください。システムにマルウェアが存在する限り、システムを繰り返しロックしたりファイルを暗号化したりするので、まず最初にマルウェアを除去してください。マルウェア除去は信頼できるウイルス対策ソフトであれば、どれでも実施が可能です。

🔍 クイック検索...

# 復号化ツール実行

▶ 公開されたツールは、

1. ライセンス同意画面
2. ファイル選択して実行
3. 完了！ と操作はとても簡単



Bitdefender Decryption Utility for REvil ransomware.

**Get the best ransomware protection**  
Bitdefender intercepts any kind of ransomware attack. [BUY NOW](#) **Bitdefender**

**The threat is gone!**  
But there are several things you should be aware of

**脅威は去った！**  
ただし注意すべき点がいくつかある

You should always backup your data.  
You and your files' security is a continuous process. Make sure you keep your data protected at all times.  
Next time we might not be able to help you recover your data.

常にバックアップをしなければならない。  
セキュリティは継続的な取り組みであり、常に保護されていることを確認してください。  
次もデータの復旧を助けられるとは限らないのだから。

[START TOOL](#) [ADVANCED OPTIONS](#)

# 復号化ツールの検証

- ▶ 復号化ツールによる復号化で元に戻ったように見えても本当に画像が元通りなのか？
- ▶ 本系とバックアップでランサムウェアによる被害の進み方が違っていたので、復号化したファイルと本来のファイルと比較して検証。



```
X:¥>certutil -hashfile File004. dcm
SHA1 ハッシュ (ファイル File004. dcm):
ca16ba275d96136caf626c9f684d9b38ec963954
CertUtil: -hashfile コマンドは正常に完了しました。
```

ハッシュ値が完全一致  
→ 内容が一致していると判断

# まとめ

## ▶ まずは現状把握

- ルータ類：使われている機器の場所、役割、接続先、バージョン情報 etc...
- サーバ類：保持してる情報、提供するサービス、連携先 etc..

## ▶ 効率の追求もいいけど、冗長なことで助かることもある

- 医療機器に残ったままのデータ、画像編集用の別サーバ、データベースとは別に保存されたレポートPDF、etc..、残っていたことで助かった
- CD作成のシステム、紹介状用と2系統あったので運用回避

## ▶ 訓練の必要性

- 事前にシステムが動かなかった場合の対応を決めておくと同時に災害訓練などと同様、定期的に訓練しておく