A-3.
ランサムウェアへの感染と対策

青山学院大学
根本　貴弘

このセッションの目的

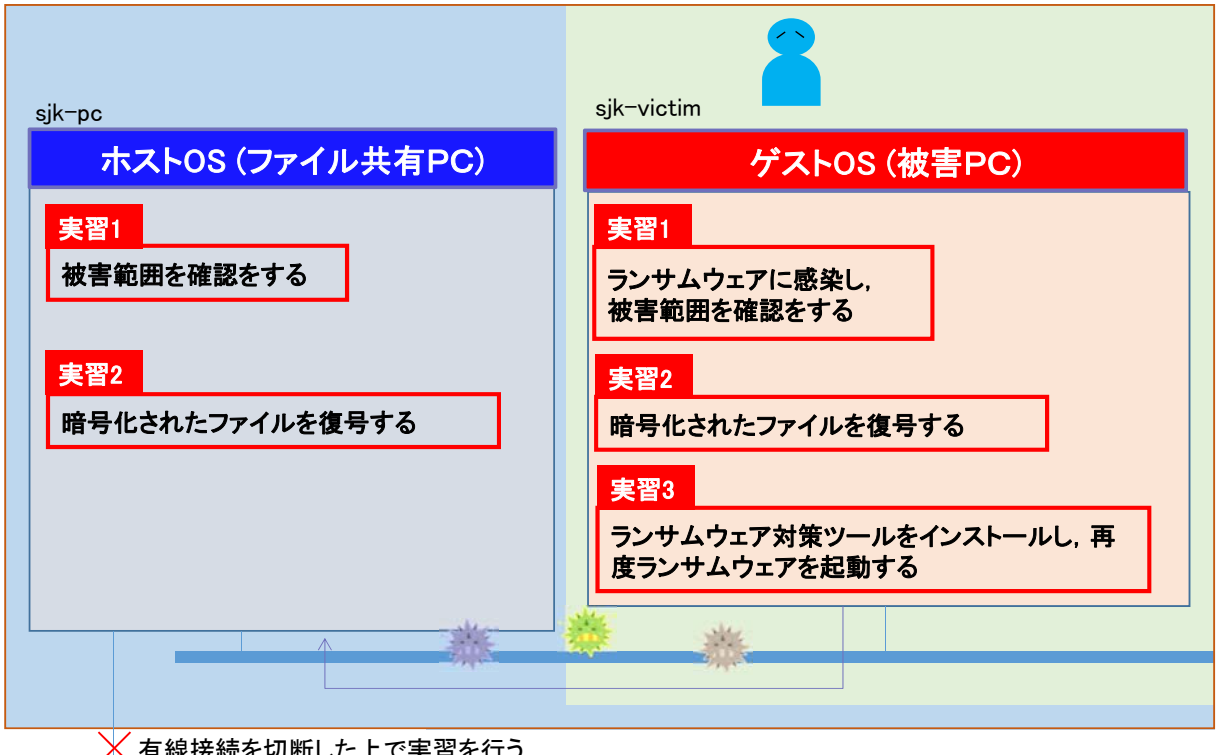
⑩ランサムウェアの感染実習
　⑩被害範囲を確認する
⑩事後対応
⑩事前対策

ランサムウェアに感染したときの被害状況の把握，事後対応が行え，さらに，事前対策を講じることができる

実習

- ランサムウェアの感染実習
  - ランサムウェアに感染し，被害範囲を確認する
    - 暗号化されたファイルの拡張子は？暗号化される前の拡張子は？
    - 暗号化されたファイルの保存場所（ディレクトリ）は？
- 事後対応
  - 暗号化されたファイルを復元する
- 事前対策
  - ランサムウェア対策ツールをインストールし，再度ランサムウェアを起動する

実習概要

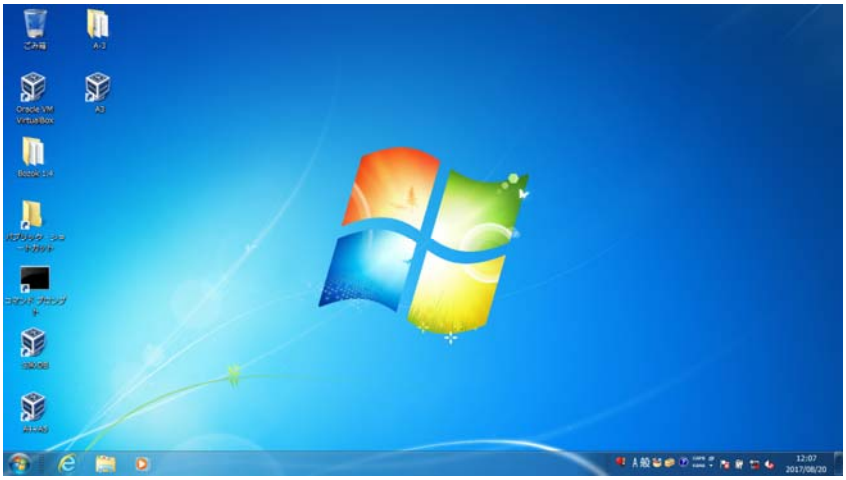


実習をはじめる前に

実習環境の確認

PCへのログイン(ホストOS)

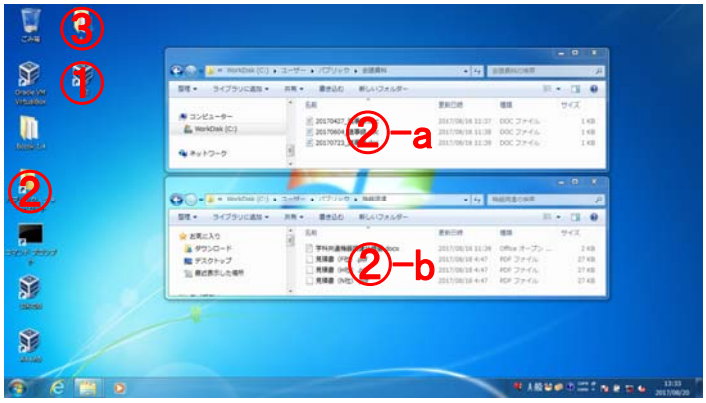
- 電源ボタンを押してPCを起動する
- ログイン画面で以下の情報を入力
  - ID: sjk00
  - PW: sjk2017



ホストOSログイン後画面

本セッションで使用するファイルの確認(ホストOS)

- A3(VirtualBoxを使用したゲストOS)…①
- パブリック-ショートカット(ゲストOSとファイル共有を行うためのパブリックディレクトリ) …②
  - [会議資料]ディレクトリ…②-a
  - [機器調達]ディレクトリ…②-b
- A-3(被害範囲確認用ファイルを保存したディレクトリ) …③



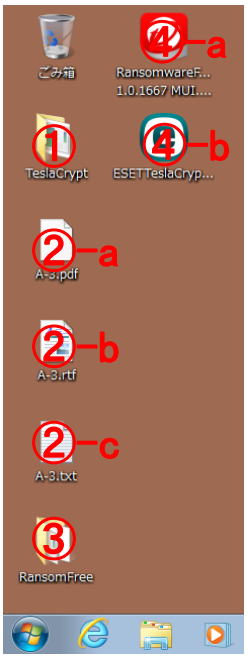
PCへのログイン(ゲストOS)

- [A3]…③をクリックし，ゲストOSを起動する
- ログイン画面で以下の情報を入力
  - ID: sjk-victim
  - PW: sjk2017

ゲストOSログイン後画面

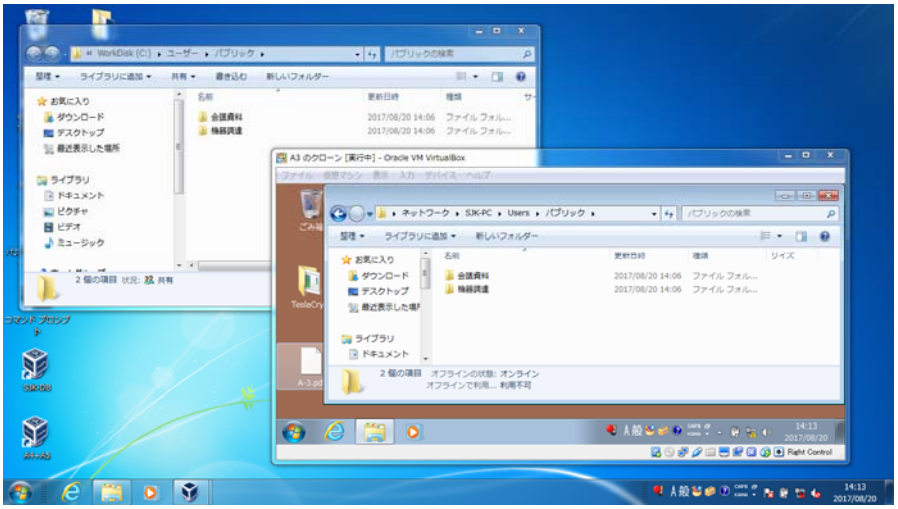
本セッションで使用するファイルの確認(ゲストOS)

- TeslaCrypt(ランサムウェアを保存しているディレクトリ)…①
- 被害範囲確認用ファイル
  - A-3.pdf …②-a
  - A-3.rtf …②-b
  - A-3.txt …②-c
- RansomFree(ランサムウェア対策ツールを保存してるディレクトリ) …③
- 復号ツール
  - Ransomware File Decryptor Tool …④-a
  - ESET TeslaCrypt Decryptor … ④-b



共有ディレクトリの確認

- ホストOSとゲストOSの共有ディレクトリの中身が同じであることを確認する
  - ホストOS側：パブリック-ショートカット
  - ゲストOS側：[ネットワーク]>[SJK-PC]>[Users]>[パブリック]



実習1

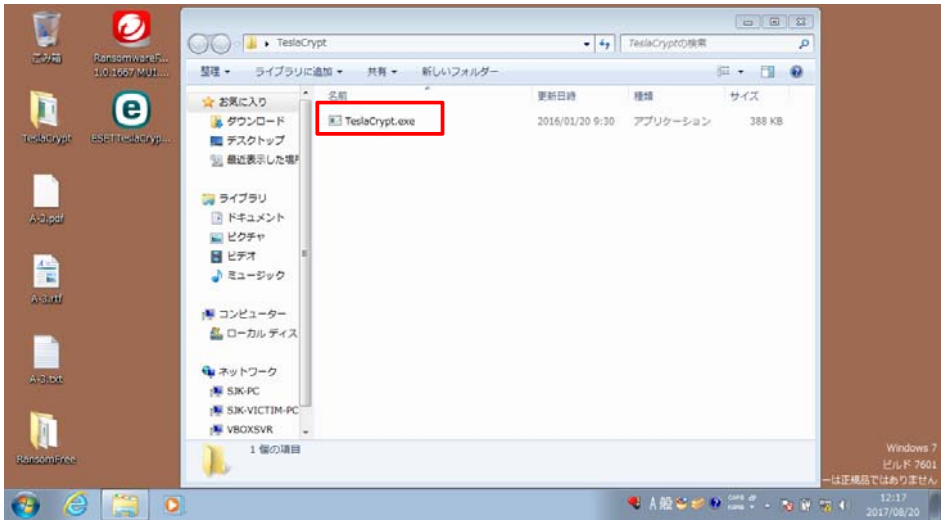
ランサムウェアに感染し，
被害範囲を確認する

1-1　感染前のファイルの状態の調査

- ホストOS及びゲストOSの感染前の各種ファイルの状態を調査する
  - ファイルの拡張子の確認
  - ファイルの更新日時の確認
  - ファイルが閲覧可能か確認(.txt，.rtf，.docのみ)
- ホストOS側の調査
  - 調査対象ディレクトリ
    - 共有ディレクトリ(パブリック-ショートカット)
    - [A-3]ディレクトリ
- ゲストOS側の調査
  - 調査対象ディレクトリ
    - 共有ディレクトリ([ネットワーク]>[SJK-PC]>[Users]>[パブリック])
    - [デスクトップ]ディレクトリ

1-2 ランサムウェアの起動

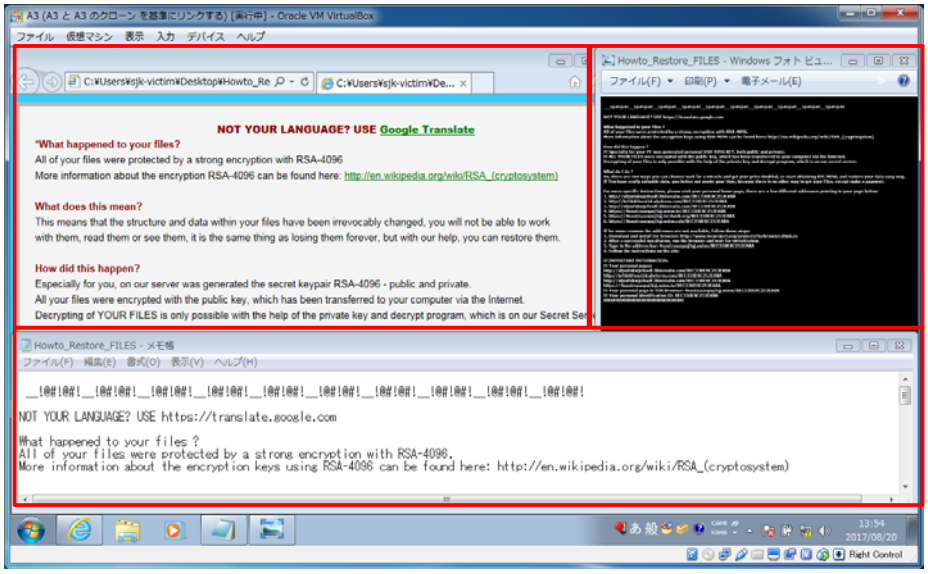
- ゲストOS上でTeslaCrypt.exeを起動する
  - [デスクトップ]>[TeslaCrypt]>[TeslaCrypt.exe]をクリック



  - [ユーザアカウント制御]ウインドウが表示されたら[いいえ]を選択

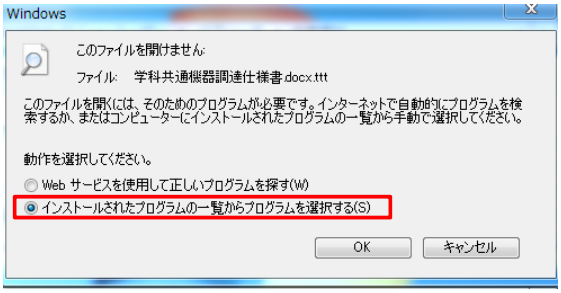
1-3 表示された脅迫文の調査

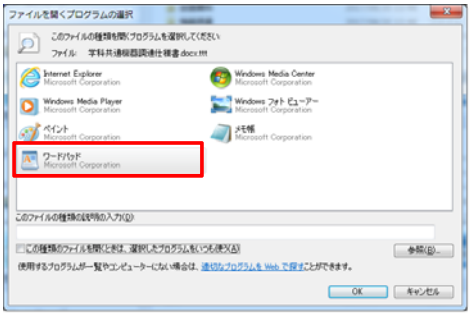
- 表示された脅迫文の種類と内容を調査する
  - 脅迫文ファイルの拡張子の種類の確認
  - 脅迫文の内容の確認



1-4 被害範囲の確認

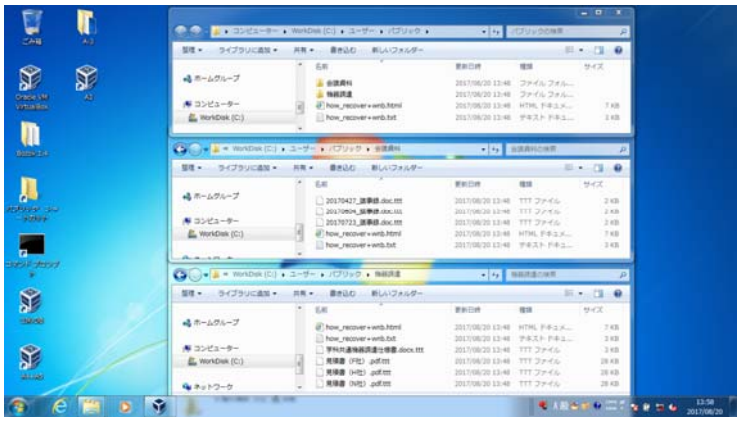
- ホストOS及びゲストOSの感染後の各種ファイルの状態を調査し，被害範囲を調査する
  - ファイルの拡張子の確認
  - ファイルの更新日時の確認
  - ファイルが閲覧可能か確認
    - [ファイルが開けません]ウインドウが表示された場合は，[インストールされたプログラムの一覧からプログラムを選択する(S)]を選択し，[ワードパッド]を選択する

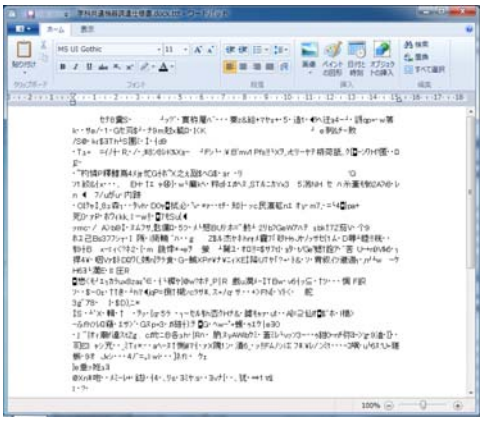




1-4 被害範囲の確認

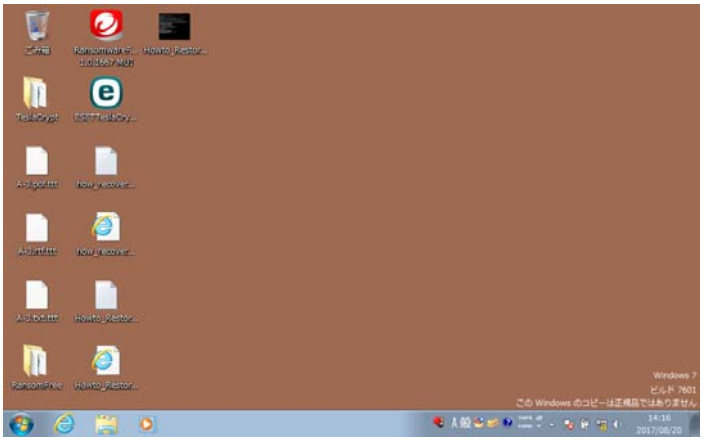
- ホストOS側の調査
  - 以下のディレクトリの中身が暗号化されているか確認
    - 共有ディレクトリ
    - [A-3]ディレクトリ

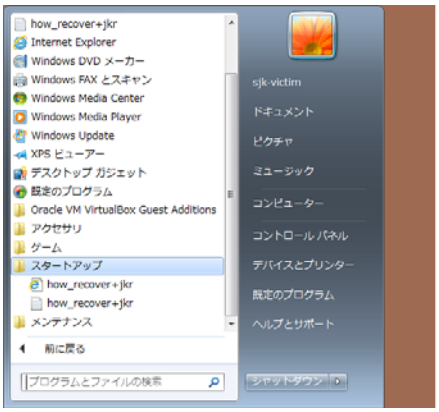




1-4 被害範囲の確認

- ゲストOS側の調査
  - 以下のディレクトリの中身が暗号化されているか確認
    - 共有ディレクトリ
    - [デスクトップ]ディレクトリ
    - [スタートアップ]ディレクトリ
    - [TeslaCrypt]ディレクトリ





1-5 まとめ

- TeslaCryptの被害範囲
  - 被害対象ファイルの拡張子
    - .txt, .rtf, .pdf, .doc, .docx等
    - 本セッションでは扱わないが，.jpegや.wmv等も被害対象となる
  - 被害対象外ファイルの拡張子
    - .exe, .dat, .dll等
  - 被害対象ディレクトリ
    - ゲストOS側：[C:]>[ユーザー]ディレクトリ配下すべて
    - ホストOS側：共有ディレクトリのみ

実習2

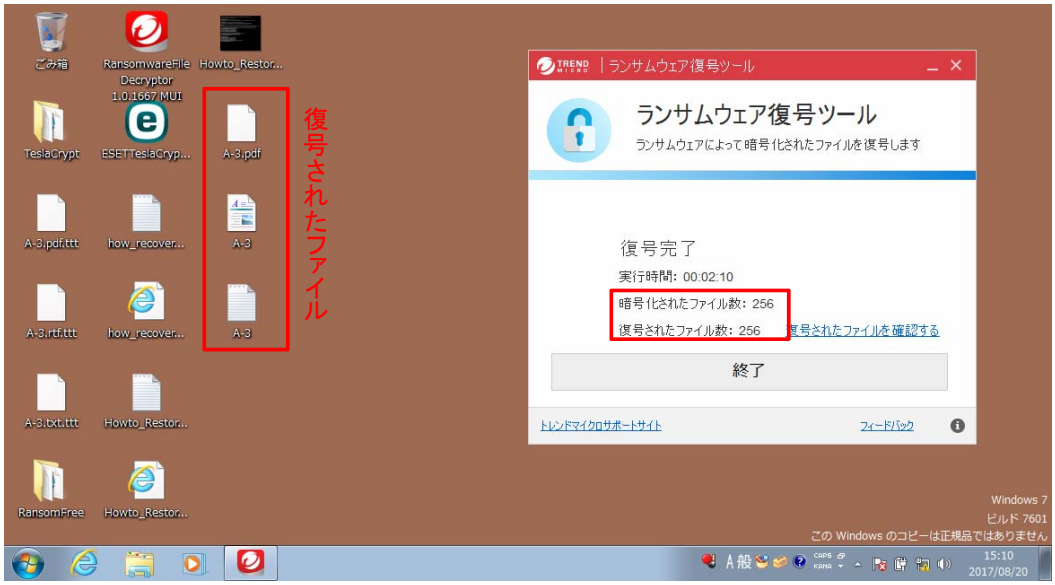
暗号化されたファイルを復元する

2-1　ゲストOS内のファイルを復号する

- Ransomware File Decryptor Toolを使用し，ゲストOS上の暗号化されたファイルを復号する
  - [Ransomware File Decryptor Tool]をクリック
    - [同意する]を選択する
    - [1. ランサムウェア名を選択してください]で，[TeslaCrypt(V3,V4)]を選択する
    - [2. 複合対象のファイルまたはフォルダを選択してください]で，[ローカルディスク(C:)]を選択する

2-2　復号されたファイルを確認する

- Ransomware File Decryptor Toolによって複合されたファイル数とファイルを確認する

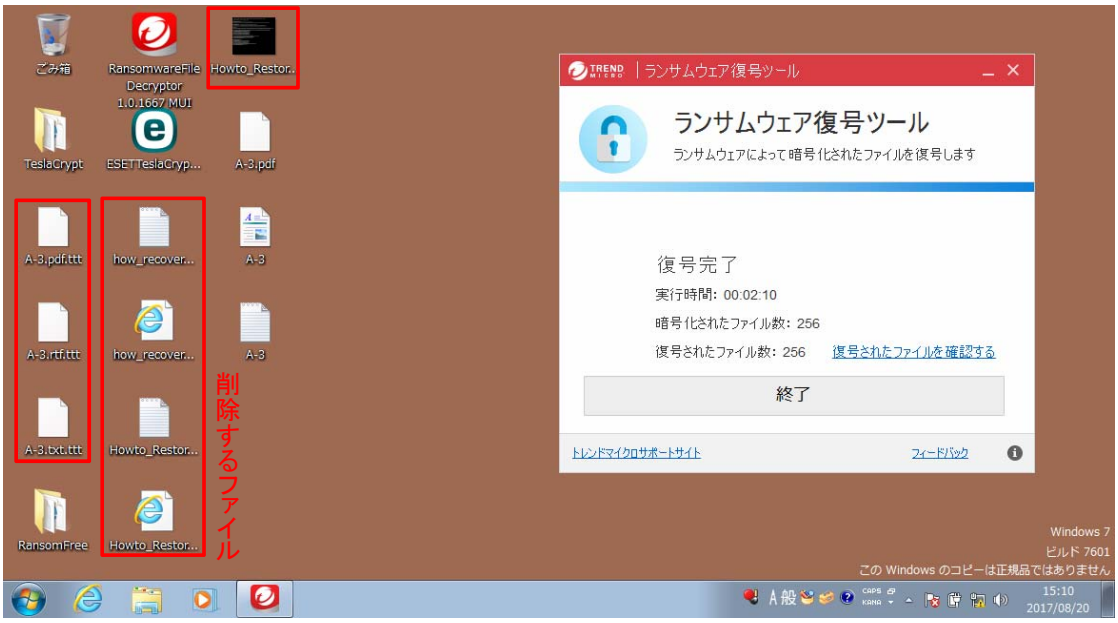


2-3　共有ディレクトリ内のファイルを復号する

- Ransomware File Decryptor Toolを使用し，共有ディレクトリ内の暗号化されたファイルを復号する
  - [Ransomware File Decryptor Tool]をクリック
    - [同意する]を選択する
    - [1. ランサムウェア名を選択してください]で，[TeslaCrypt(V3,V4)]を選択する
    - [2. 複合対象のファイルまたはフォルダを選択してください]で，[ネットワーク]>[SJK-PC]>[Users]>[パブリック]]を選択する
  - 復号が完了したら，復号されたファイル数とファイルを確認する

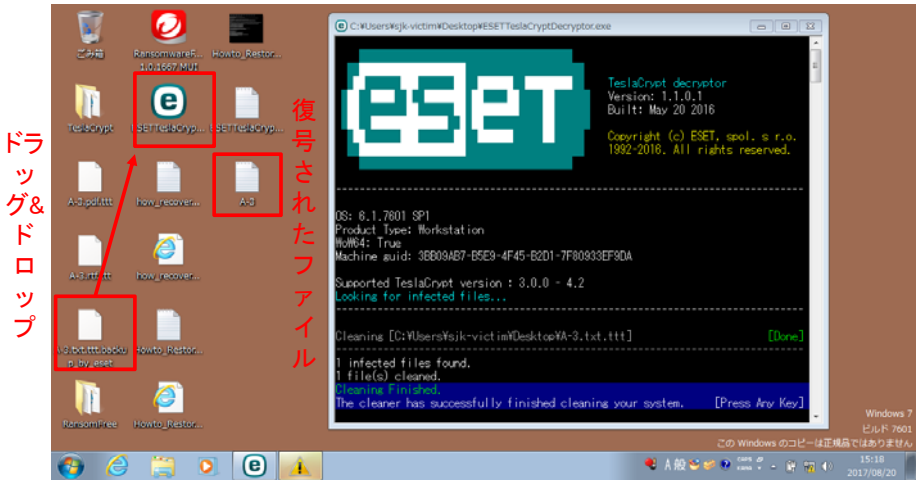
2-4　不要なファイルの削除

- 暗号化されたファイルや脅迫文ファイルを削除する



2-5　ESET TeslaCrypt Decryptorを用いた復号

- ESET TeslaCrypt Decryptorを用いた復号
  - 復号したいファイルを[ESET TeslaCrypt Decryptor]アイコンにドラッグ&ドロップする
  - [ESET TeslaCrypt Decryptor]が起動された後，指示に従い，[Enter]キー等の適当なキーを押す



2-6 まとめ

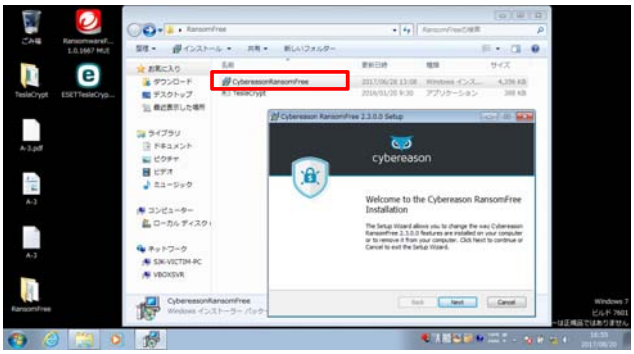
- 事後対応
  - 復元ツールを試す
    - TeslaCryptのようにマスターキーが公開されているものは復元できることもある
    - しかし，復元できない場合もある
- 事前対策
  - バックアップを取る
    - 定期的にバックアップを取る
    - バックアップ用デバイスはバックアップ時のみPCと接続させる
      - USBメモリ，外付けHDD，ネットワークドライブ，クラウド上のストレージ等
    - バックアップ用デバイスは複数用意する
    - 定期的にバックアップから復元できることを確認する
  - ランサムウェア対策ツールを利用する

実習3

ランサムウェア対策ツールをインストールし，再度ランサムウェアを起動する

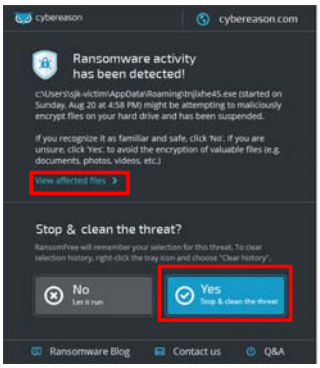
3-1 ランサムウェア対策ツールをインストールする

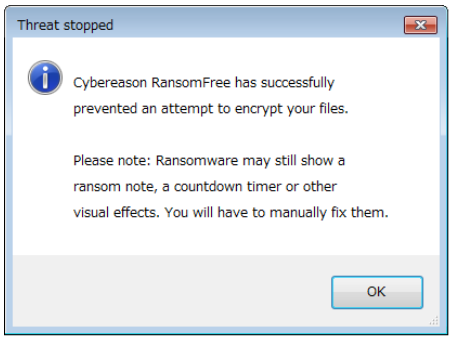
- ゲストOSにCybereasonRansomFreeをインストールする
  - デスクトップ画面にある[RansomFree]ディレクトリをクリック
  - [CybereasonRansomFree]を起動する
    - [Next]をクリックする
    - [I accept the terms in the License Agreement]をチェックし，[Next]をクリックする
    - [Install]をクリックする
    - [ユーザアカウント制御]ウインドウが表示されたら，[はい]をクリックする
    - インストールが完了したら[Finish]をクリックする



3-2 ランサムウェアを起動する

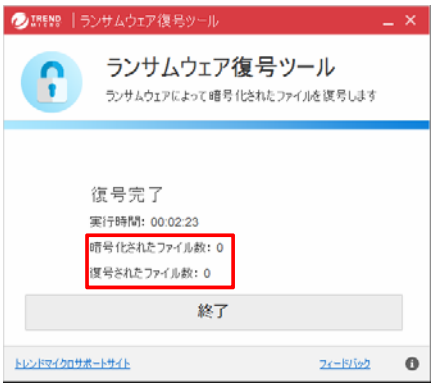
- TeslaCryptを起動し，CybereasonRansomFreeによってTeslaCryptが実行されないことを確認する
  - [RansomFree]ディレクトリ内の[TeslaCrypt.exe]ファイルをクリック
  - CybereasonRansomFreeが起動したら，[View affected files]をクリックし，暗号化された可能性のあるファイルを確認
  - [Yes]を選択を選択し，暗号化を行うプロセスを停止及び除去





3-3 暗号化されていないことを確認する

- Ransomware File Decryptor Toolを使用し，暗号化されたファイルがないことを確認する
  - [Ransomware File Decryptor Tool]をクリック
    - [同意する]を選択する
    - [1. ランサムウェア名を選択してください]で，[TeslaCrypt(V3,V4)]を選択する
    - [2. 複合対象のファイルまたはフォルダを選択してください]で，[デスクトップ]を選択する
  - 復号が完了したら，暗号化されたファイル数とファイルを確認する



3-4 まとめ

- 事前対策
  - ランサムウェア対策ツールをあらかじめインストールしておくことで，ランサムウェア被害に気づく機会を増やすとともに，暗号化を防止する
  - ただし，暗号化された後に検出する場合もあるため，確実に暗号化を防止できるわけではない
  - 2-6で紹介したバックアップによる事前対策や他のセキュリティソフトと組み合わせることが重要