CyberCrime Control Project

令和２年12月

広島県警察本部
サイバー犯罪対策課
082-228-0110
（内線　705-586）

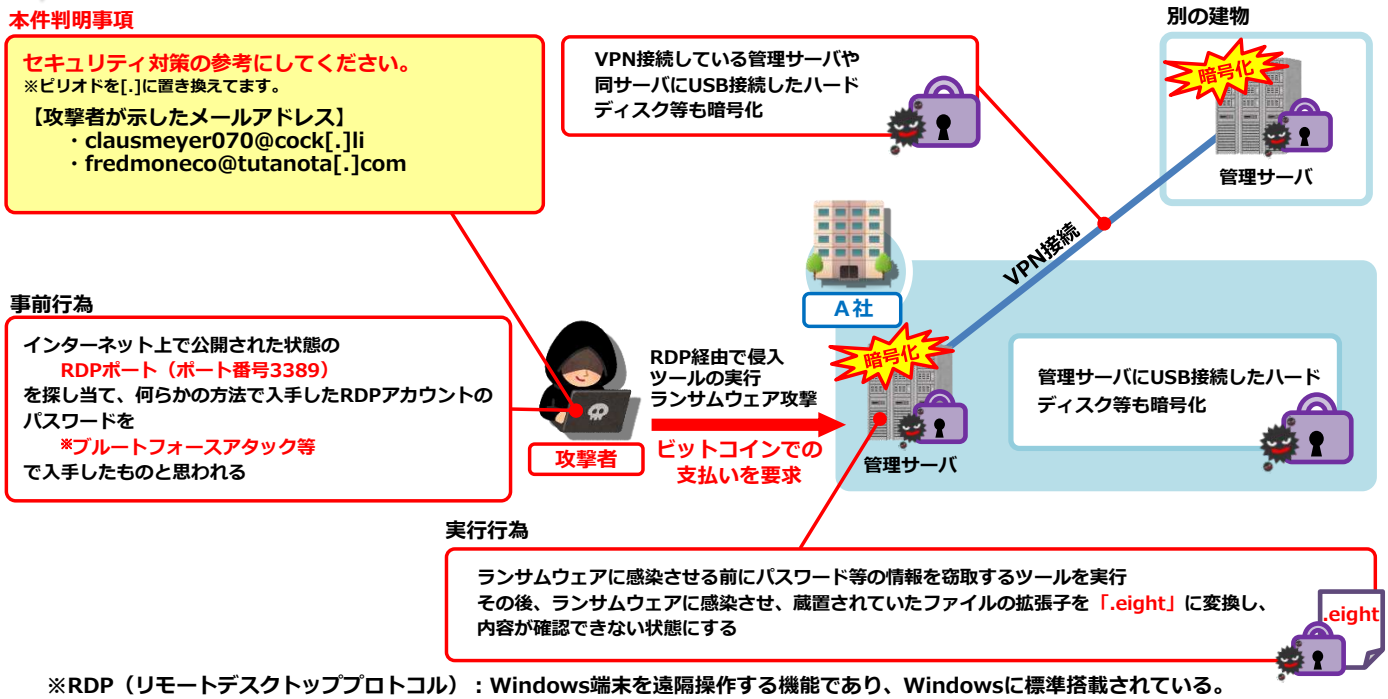
ー 県内でもランサムウェアによる攻撃が発生！！ ー

本年11月に県内企業でランサムウェアの感染が確認されました。
ランサムウェアとは、パソコンやサーバ等のデータを暗号化する等して使用不可にし、暗号化したデータの復旧と引き換えに身代金を要求するメッセージを表示するウイルスの総称です。

県内で確認されたもの　ー「Phobos（フォボス）」の亜種と推認されるランサムウェアに感染 ー

Phobos（フォボス）

※RDP経由で攻撃対象に侵入し、感染すると端末内に保存されているファイルを暗号化して、脅迫メッセージを表示する。
メッセージには、攻撃者のメールアドレス宛にメールを送るように要求するとともに、ビットコインで身代金を支払えば、ファイルを復号できる旨が記されていることが多い。



※RDP（リモートデスクトッププロトコル）：Windows端末を遠隔操作する機能であり、Windowsに標準搭載されている。
※ブルートフォースアタック（総当たり攻撃）：パスワード等を解読するために可能な組み合わせをすべて試す攻撃手法のこと。

対策

ネットワークへの侵入対策

- RDPの利用を止めて、他のアクセス手段（VPN導入等）を検討する
- RDPの利用を続けざるを得ない場合は
  - 管理者のユーザ名やパスワードをデフォルトのままや安易なものにせず、複雑なものにする
  - パスワード認証のほかに、生体認証や端末認証等の異なる認証手段を追加し「多要素認証」を導入する
- ネットワーク機器等の脆弱性を確認し、解消する

データ・システムのバックアップ

- バックアップに使用する装置・媒体は、バックアップ時のみ対象機器と接続する
- 重要なファイルは定期的にバックアップを取得する
- データのみならず、システムの再構築を含めた復旧計画を策定する

（引用）　cybereason　https://www.cybereason.co.jp/blog/ransomware/5436
（引用）　独立行政法人情報処理推進機構（IPA）　https://www.ipa.go.jp/files/000084974.pdf

平成28年～令和２年
「めざそう！安全・安心・日本一」
ひろしまアクション・プラン

運動目標　県民だれもが穏やかで幸せな暮らしを実感できる
日本一安全・安心な広島県の実現

重点項目
- 身近な犯罪被害の抑止
- 子供・女性・高齢者等の安全確保
- 新たな犯罪脅威への対応

なくそう特殊詐欺被害　アンダー5作戦
なくそう交通死亡事故　アンダー75作戦