



サイバーセキュリティ ニュース

平成29年
第2号

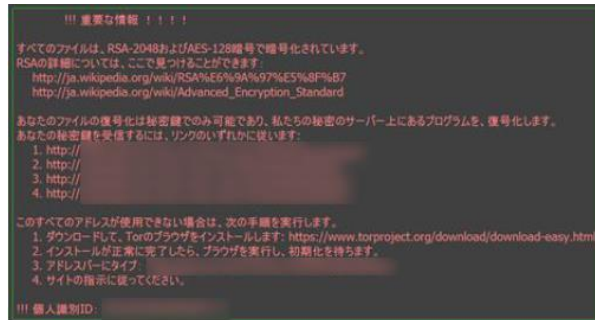
ランサムウェアへの対策について

1 ランサムウェアとは

ランサムウェア (Ransomware) とは、コンピュータウイルスの一種であり、「身代金 (Ransom)」と「ソフトウェア (Software)」を組み合わせた造語です。ランサムウェアに感染すると、強制的に「ファイルの暗号化」や「端末のロック」が行われ、その解除と引き換えに金銭を要求されます。

2015年頃からランサムウェアの被害が増加しており、トレンドマイクロの調査では、調査対象の国内法人ユーザの25.1%が「ランサムウェアの攻撃にあったことがある」と回答しています。(※1)

感染経路としては、従来のウイルスと同様に、メールの添付ファイルや悪意のあるウェブサイトからの感染が考えられます。



(左) PCのファイルが暗号化された場合の脅迫画面例(※2)

(右) スマートフォンがロックされた場合の脅迫画面例(愛知県警HPより)

※1 トレンドマイクロ プレスリリース 企業におけるランサムウェア実態調査2016

<http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20160727064652.html>

※2 情報処理推進機構 ランサムウェアの脅威と対策 <https://www.ipa.go.jp/security/technicalwatch/20170123.html>

2 ランサムウェアによる主な被害事例

○ 病院のデータ共有システムが感染

平成28年2月5日、米国ロサンゼルス市の病院のシステムがランサムウェアに感染していることが発覚。電子カルテなどのシステムがロックされ、電子的な情報共有ができなくなった。

○ 交通関係機関の複数の端末が感染

平成28年11月25日、米国サンフランシスコ市の交通当局の複数のコンピュータ端末がランサムウェアに感染していることが発覚。金銭関係システムへの影響が懸念されたことから、25日から27日にかけて駅の券売機などを停止して、被害の調査などを実施した。

○ ホテルの施錠管理システムが感染

平成29年1月、オーストリアの高級ホテルにおいて、カードキーのシステムなどがランサムウェアに感染していることが発覚。客室の施錠と開錠を行うシステムがダウンし、宿泊客が部屋に入れなくなった。

3 対策

ファイル暗号化型のランサムウェアへの対策として、次のものがあります。

攻撃を受けないための対策		被害を低減するための対策	
ウイルス対策製品の導入	各端末やネットワーク上の機器においてウイルス対策製品を導入し、ウイルスを検知・ブロックする	データのバックアップ	重要なデータについては、定期的なバックアップを行う
ぜい弱性対策	ぜい弱性を修正するアップデートを行う	適切なアクセス制限	ネットワークの分離、ファイルの編集、書込みの制限等を適切に行い、個々のユーザによる共有データへのアクセスを必要最小限にする
職員へのセキュリティ教育	メールの添付ファイルを安易に開かない等、職員への教育を行う		



被害を受けたらまずは警察へ御相談ください

茨城県警察サイバー攻撃特別捜査隊

TEL.029-301-0110 (内線5691)

