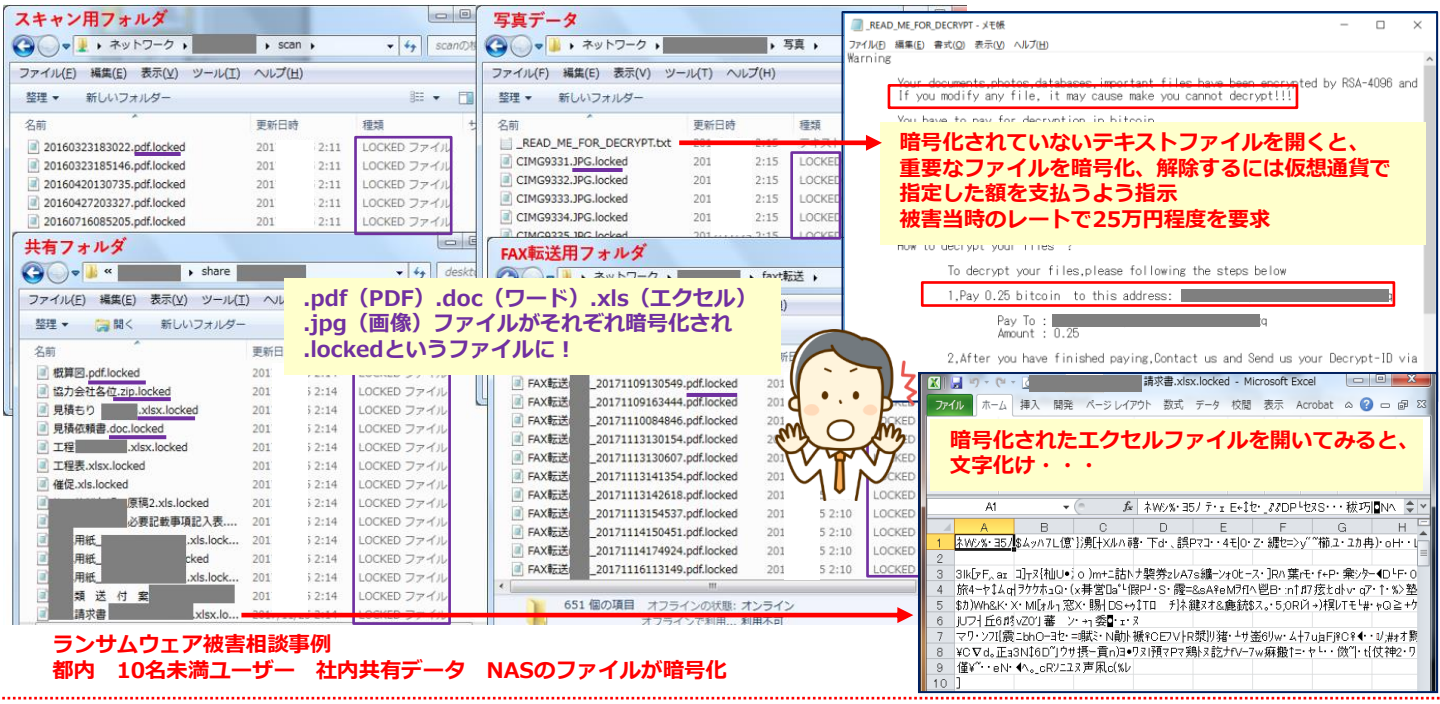
回覧 印 印 印 印 印 印 印 印 印 印 印 印

ASAMA Security Newsletter Vol.80

あさまセキュリティニュースレター

ランサムウェア被害が急増中！！被害にあう前に対策を

（2022年1月11日）



ランサムウェア被害相談事例
都内　10名未満ユーザー　社内共有データ　NASのファイルが暗号化

攻撃のパターン

- VPNやリモートデスクトップサービスの**脆弱性をつく攻撃**（テレワーク時代に合わせた攻撃）、**Emotet**等取引先に成りすました攻撃により、パソコンやサーバをマルウェア感染させる
- 感染したPCを遠隔操作で、**ネットワーク上のサーバや共有データを暗号化するよう命令し、データを暗号化**
- 社内の端末やサーバを一斉に暗号化させる攻撃も（復旧を阻害するため、バックアップ等も同時に）
- **データ暗号化を戻すための金銭要求 ＋ 盗んだデータを公開すると脅迫し、金銭要求（二重の脅迫）**

対策

- **古いネットワーク機器のファームウェアのバージョンアップや見直しはできているか？**
- **外部からのアクセスを利用している場合は、設定が適切か？**
- **ウイルス対策ソフト未導入の端末で、社内データにアクセスしているものはないか？**
- **バックアップは取れているか、何世代か前に戻せる仕組みがあるか？**
- **社員全員でセキュリティに対する意識を高める、情報共有しているか？**

ウイルス対策、不正アクセス対策、脆弱性対策など、基本的な対策を確実かつ多層的に適用することが重要！！

海外ではギフトカードや新型コロナについての情報が入っていると称し、ランサムウェアが仕込まれたUSBメモリを送りつけてくる攻撃が発生！
不審なUSBメモリは接続しないように！

情報源

ESETサイバーセキュリティ情報局　https://eset-info.canon-its.jp/malware_info/special/detail/211102.html

警視庁ランサムウェア被害防止対策　https://www.npa.go.jp/cyber/ransom/index.html

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414