

## ランサムウェアに注意してください！

大阪府内の医療機関がランサムウェアに感染し、電子カルテが閲覧できなくなる被害が発生しています。ランサムウェアに感染すると、パソコンやサーバ内のファイルが暗号化され閲覧できなくなり、業務に重大な支障を来すおそれがあり、事業活動の停止に追い込まれるケースがあります。

ランサムウェアの感染経路は、VPN機器等のネットワーク機器の脆弱性やメールの添付ファイルがほとんどです。特に、最近ではVPN機器の脆弱性が突かれて感染するケースが増加していますので、外部からサーバへのアクセスを利用している方は、VPN機器等の脆弱性対策をお願いします。

### ランサムウェア

ランサムウェアとは、パソコン等の端末及びネットワーク接続された共有フォルダ等に保管されたファイルを、暗号化して使用不能にするウイルスです。

このウイルスは、使用不能な状況を復旧することと引き換えに、金銭（仮想通貨）を要求することから「身代金要求型ウイルス」とも呼ばれています。

### ダブルエクストーション

最近のランサムウェアは、データの暗号化のみならずデータを窃取した上、事業者等に対して「対価を支払わなければ、当該データを公開する」などと金銭（仮想通貨）を要求する二重恐喝（ダブルエクストーション）という手口が使われています。実際にリークサイト上で、窃取された個人情報等が公開されています。

### ランサムウェア対策

#### ➤ VPN機器やソフトウェアの脆弱性対策

システム、ソフトウェアの脆弱性を悪用されて侵入されるケースが確認されています。脆弱性情報を確認し、脆弱性がある場合は、速やかにセキュリティパッチを適用しましょう。

#### ➤ バックアップは必ず実施

同一ネットワークのバックアップは、感染する場合があります。危険です。バックアップは、別のシステムまたは外部記録媒体でも実施しましょう。

#### ➤ パスワード管理

パスワードを盗用される場合もあります。初期パスワードは必ず変更して下さい。パスワードは複雑なものにして、外部に流出しないように適切に管理しましょう。



ランサムウェア「LOCKBIT3.0」の画面。感染すると「あなたの重要なファイルは全て盗まれ、暗号化された」と表示される。



脆弱性情報（緊急性、重要性の高い脆弱性情報等をピックアップしてご紹介します。）

#### ～Fortinet製OS等の認証バイパスの脆弱性（2022年10月14日公表）～

Fortinet社が提供する「FortiOS、FortiProxy、FortiSwitchManager」における認証バイパスの脆弱性について、アドバイザリが公表されていますので、当該製品を利用されている場合は、早急に対応をお願いします。

詳細は、必ず、公式サイト及びIPA、JVN、JPCERT/CC等の脆弱性情報提供サイトを確認してください。

サービス名、機器名等 (影響を受けるソフトウェア)	脆弱性の概要 (悪用された場合の影響等)	CVE (共通脆弱性識別子)	対策 (修正プログラムの公開情報等)
<ul style="list-style-type: none"> <li>FortiOS</li> <li>FortiProxy</li> <li>FortiSwitchManager (バージョンは省略)</li> </ul>	認証されていない第三者が、当該製品に細工したHTTP(S)リクエストを送信し、任意の遠隔操作を行うことが可能	CVE-2022-40684 (CVSS v3 9.6) 緊急	脆弱性を修正したバージョンへのアップグレードが推奨されている。

参照：JPCERT/CC「Fortinet製FortiOS等の認証バイパスの脆弱性に関する注意喚起」<https://www.jpCERT.or.jp/at/2022/at220025.html>

「CS情報SHIG@」 キャッシュレス決済の不正利用が発生しています。明細書を確認してください。

滋賀県警察本部 サイバー犯罪対策課 077-522-1231（代表）

県警webページ →

