サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

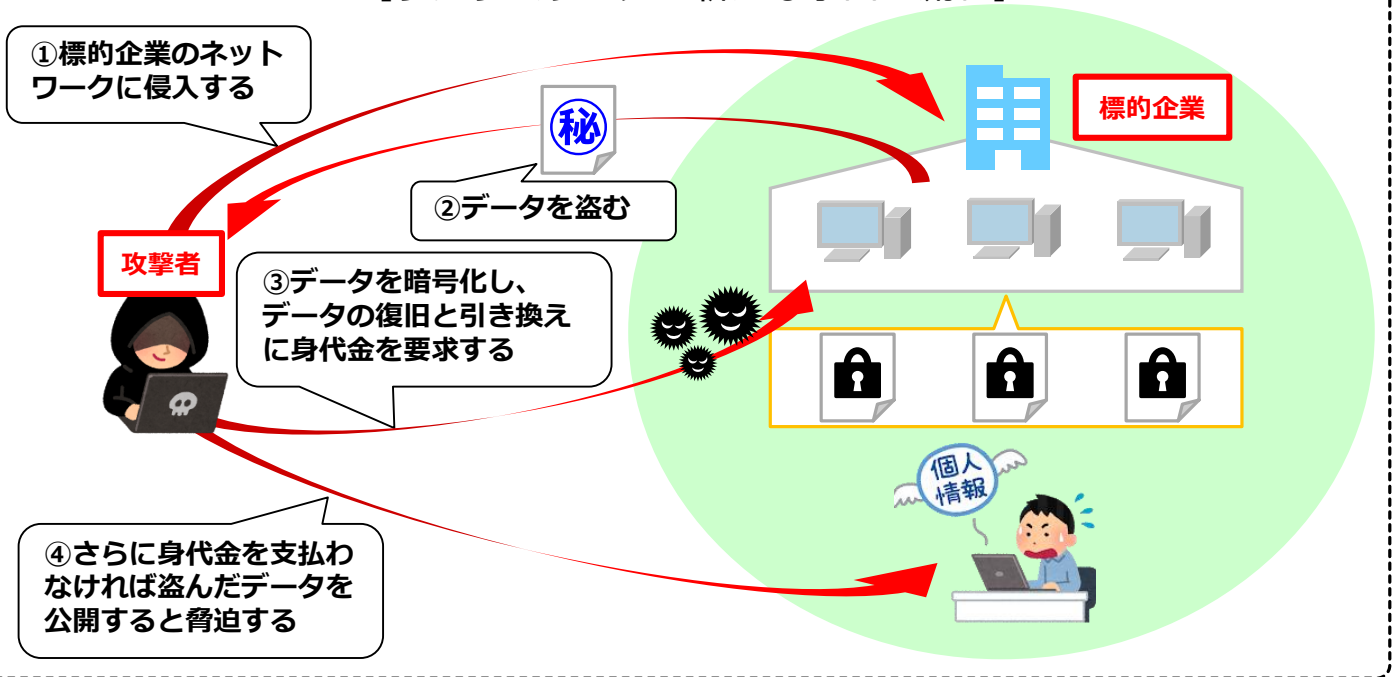
令和3年
11月1日
Vol.67

⚠ ランサムウェアの新たな手口に注意 ⚠

ランサムウェアとは、パソコン等の端末やサーバ上のデータを暗号化等して使用不可にし、それらの復旧と引き換えに身代金を支払うように脅迫メッセージを表示するウイルスの総称です。

これまでは基本的に明確な標的を定めずウイルスメールをばらまくといった方法で広く無差別に攻撃を行っていましたが、近年、明確に標的を企業組織に定め、身代金を支払わざるを得ないような状況を作り出す新たな手口が発生しています。

【ランサムウェアの新たな手口の流れ】



【予防と対策】

企業・組織のネットワークへの侵入対策	リモートデスクトップサービスの認証を突破されたり、VPN装置のアップデートが行われておらず、侵入されたという事例等が多くありますので、インターネットからアクセス可能な装置全体について、**アクセス制御が適切にできているか**、**認証が突破される可能性はないか**、**脆弱性は解消されているか**、といった点を確認しましょう。
データ・システムのバックアップ	ネットワークサーバにバックアップサーバが接続されていると、バックアップサーバも被害に遭う可能性があります。 ファイルは**定期的にバックアップ**し、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**するようにしましょう。

『ランサムウェアの被害に遭ったかもしれない』と思ったら警察に相談してください。

参考：IPA「【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について」(https://www.ipa.go.jp/security/announce/2020-ransom.html)

相談窓口 愛媛県警察本部サイバー犯罪対策課 TEL089-934-0110(代)