サイバー防犯通信

令和３年１０号
兵庫県警察本部
サイバー犯罪対策課

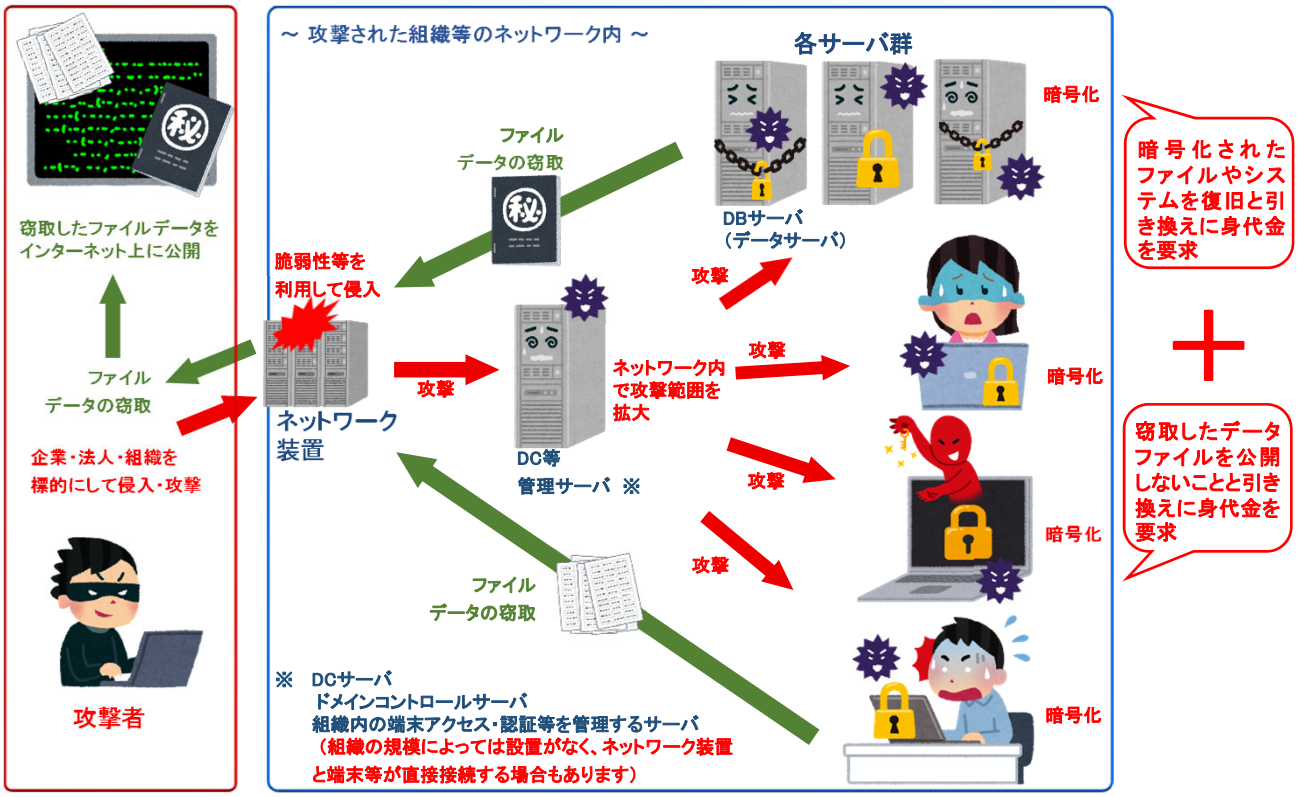
新たなランサムウエア攻撃にご注意

～企業・法人・組織向け～

ランサムウエアとは、感染すると端末などに保存されているファイルを暗号化して使用できない状態にした上で、そのファイルを復号化する対価として金銭を要求する不正プログラムです。

従来の不特定多数に対するばらまき型の攻撃から、新たに企業・法人・組織を標的にした「標的型攻撃」が主流になっています。

～ ランサムウエア被害拡大イメージ図 ～



最近の事例として、ファイルの暗号化のみならず、ファイルを窃取した上に被害法人等に対して「対価を支払わなければ当該ファイルを公開する」などと金銭を要求する二重恐喝（ダブルエクストーション）という手口が認められています。

ネットワーク機器の脆弱性を利用し、組織等のネットワーク内に侵入する攻撃手口に変化しています。また、テレワーク普及を利用して組織等のネットワーク内に侵入する手口が複数認められるため、注意が必要です。

Check! ～～防犯ポイント～～

- リモートデスクトップサービスの不用意な露出の停止・見直し、ネットワーク装置の脆弱性の解消、端末やサーバのOS更新等、必ずしも新たな投資を要しない設定変更や見直しで被害を予防できる可能性があります。
- 定期的にバックアップを取得しましょう。
- 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様にしましょう。
- バックアップ中にマルウエア感染する可能性を考慮し、バックアップに使用する装置・媒体は複数用意しましょう。
- 万が一ランサムウエア攻撃を受けた場合は警察に届出をお願いします。

記事引用元 ： 警察庁資料「令和3年上半期におけるサイバー空間をめぐる脅威の情勢等について」
情報処理推進機構（IPA）ホームページ内「事業継続を脅かす新たなランサムウエア攻撃について」