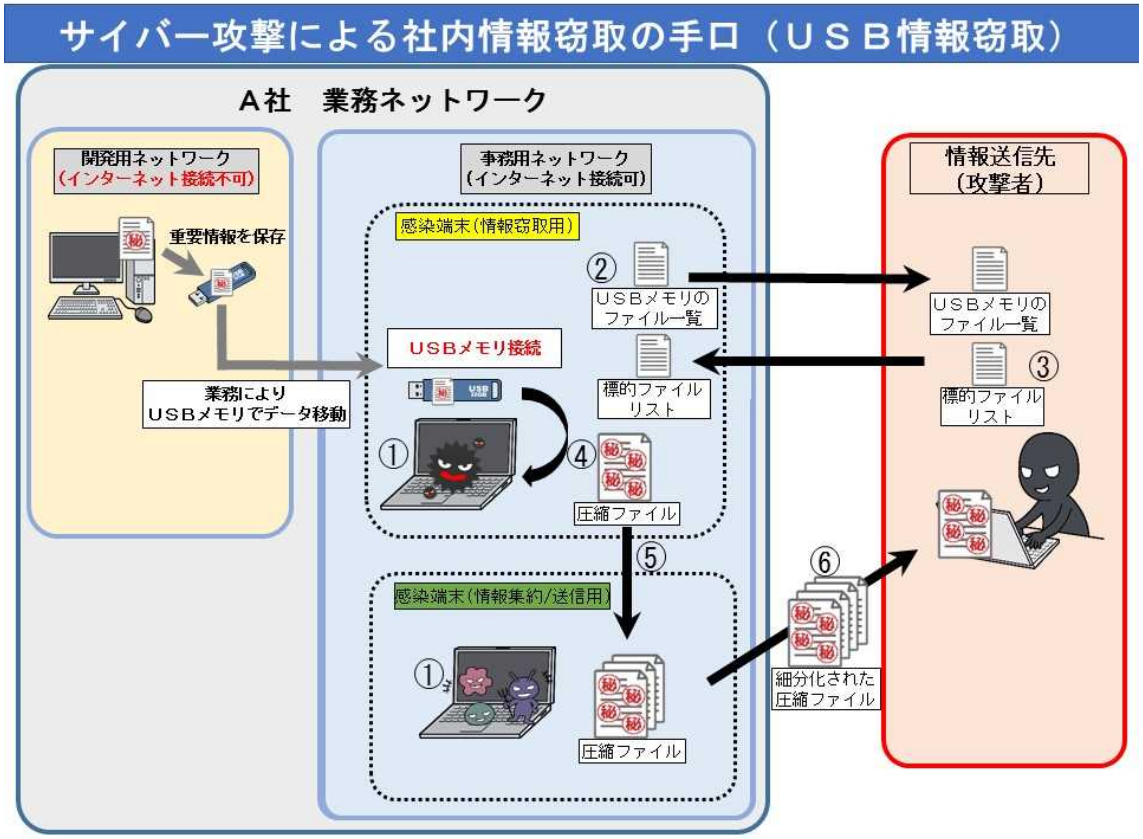
Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 29 年3月 30 日

Topic

サイバー攻撃に関する注意喚起について

クローズドネットワーク環境のパソコンに保存された重要情報を窃取し得る新たなサイバー攻撃の手口（USB 情報窃取）を確認しました。
ネットワーク管理者は、不正アクセスや情報漏えいのリスク低減を図るなど、早急に被害防止対策を実施することを推奨します。



1　情報窃取の手口について

企業等が保有する機密情報等の重要情報については、独立したクローズドネットワークで保存・運用する方法が普及しています。この度、このように外部と隔離されたネットワークに保存された情報であっても、インターネット接続された事務用ネットワークの端末と外部記録媒体（USB メモリ等）を用いて窃取することが可能となる新たなサイバー攻撃の手口を確認しました。

①　攻撃者は、インターネット接続された事務用ネットワーク端末を不正プログラムに感染させる。

② 外部記録媒体（USB メモリ等）が感染端末（情報窃取用）の USB ポートに接続されると不正プログラムが自動起動し、外部記録媒体に保存されている情報の「ファイル一覧」を作成し、端末に保存する。

③ 攻撃者は、インターネットを通じて「ファイル一覧」を取得し、「ファイル一覧」の中から窃取したい「標的ファイルリスト」を作成の上、感染端末（情報窃取用）に送信する。

④ 感染端末（情報窃取用）の不正プログラムは、外部記録媒体に保存されている情報のうち「標的ファイルリスト」で指定されたファイルを圧縮して端末に保存する。

⑤ 圧縮されたファイルは、事務用ネットワークの感染端末（情報集約／送信用）に送信される。社内に感染端末（情報窃取用）が複数存在する場合、各端末で保存された圧縮ファイルが感染端末（情報集約／送信用）に集約される。

⑥ 感染端末（情報集約／送信用）の不正プログラムは、同圧縮ファイルを端末内で加工・細分化し、外部へ送信する。

2 推奨する対策

(1) 調査の一例

パソコンの「C:¥intel¥logs」や「C:¥Windows¥system32」の下に、

- 正規の実行ファイルに似た名前の実行ファイル（例：「intelUPD.exe」、「intelu.exe」、「IgfxService.exe」等）
- 「interad.log」や「slog.log」といった不正なファイル
- 使用していない「RAR」形式のファイル

がないか確認してください。

※ 具体名は現在判明している一例であり、ファイル名やパスは異なる場合があります。

(2) 情報漏えい防止対策

○ 機密性が高い情報を扱うネットワークからデータを持ち出す際は、暗号化を行う。

○ インターネットに接続したネットワークに USB メモリを接続し、当該データをメール等を利用し外部に送信する場合は、当該データを暗号化したままの状態で送信する。

○ USB メモリ内のデータは速やかに消去する。

○ 不要な端末間通信を無効にする。

(3) その他一般的な措置

プロキシログの監視、ファイアウォールの設定や侵入検知システム(IDS)、侵入予防システム(IPS)の導入、ウイルス対策、ＯＳやアプリケーションの最新版への更新を行うとともに、脆弱性診断を定期的に行うなどの対策を実施してください。