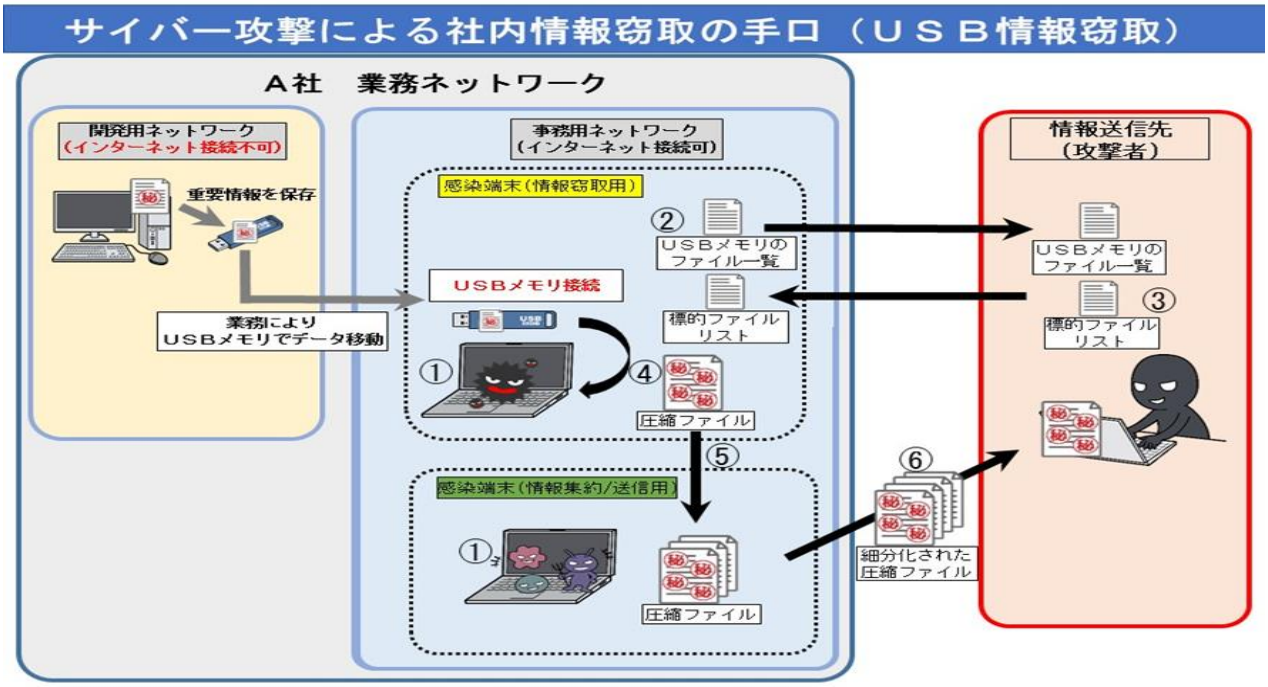
モノづくりプリザーブ
Preservation for Industries in kyoto

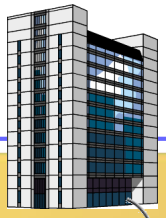
モノプリ・ニュース / 第18号

クローズド環境からの情報窃取事案発生！

USBメモリを標的とした新たな情報窃取事案が発生しています。重要情報をUSBメモリで移動している場合は、被害防止対策を実施してください。



① インターネット端末に重要情報が保存されたUSBメモリを接続すると、不正プログラムが起動
② USBメモリ内のファイル一覧を攻撃者に送信
③ 攻撃者は窃取するファイルを標的ファイルリストとして送信
④ 標的ファイルリストに基づいて圧縮ファイルを作成
⑤ 不正プログラムに感染した情報集約/送信用端末に圧縮ファイルを送信
⑥ 情報集約/送信用端末で、データを加工、細分化し、攻撃者に送信



～ 被害防止対策 ～

- **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必ず暗号化する。**
- **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し、不要な端末間送信を無効にする。**

＊ **今回確認された攻撃の感染端末には、正規の実行ファイルに似せたもの（例：「intelUPD.exe」「intelu.exe」「IgfxService.exe」等）や、「interad.log」「slog.log」といった不正なファイル、持ち出しに利用された「RAR」形式の圧縮ファイルが発見されていますので、再度確認をお願いします。**

異常を検知した場合は、警察への速報をお願いします！

京都府警察本部モノづくりプリザーブ事務局　075-451-9111（内線 5821）