⑥ Emotet（マルウエア：windows のみ感染）220904a

ロシアが発生源、 Office のマクロファイルを添付し
メールアカウント、PWD、アドレス帳 etc をコピーされ
感染メールで送付する（なりすましメール）

⑥ 感染確認方法

まず システム > システムの種類で Win が 64ビット
か 32ビット なのかを確認
> ブラウザ起動 > 上部の検索欄 に
「emocheck」 と入力 > Release - JPCERT CC/
Emocheck v2.1.1 x64 exe.（64ビット）
〃 86 〃 （32ビット）
> いずれかのファイル・ダウンロード完了すれば
> emockeck v2.1.1 64exe の（ファイルを開く）
> これで 黒い画面 で検索が始まり （OK）なら
「検知されませんでした。」 と表示、

---

⑥ 感染してはった場合、「Emotet」検知、と表示、
・インターネット から切断する.（Lan ケーブル外す、or（機内モード）
黒い画面にプロセス ID：1.952（この数値をメモする）
> タスクマネージャー を起動 Shift + ctrl キー + Esc
タスクマネージャー が起動したら 左下の 詳細 > 上部の（詳細）
タブ > PID 項目 ボタン > これで 先程の（1962）
の番号 を探す。