# EMOTET（エモテット）の脅威

IPA（情報処理推進機構）、JPCERT/CC（日本コンピュータ緊急対応センター）が相次いで注意喚起を発し、最恐のマルウェアと言われるEMOTET とは！？

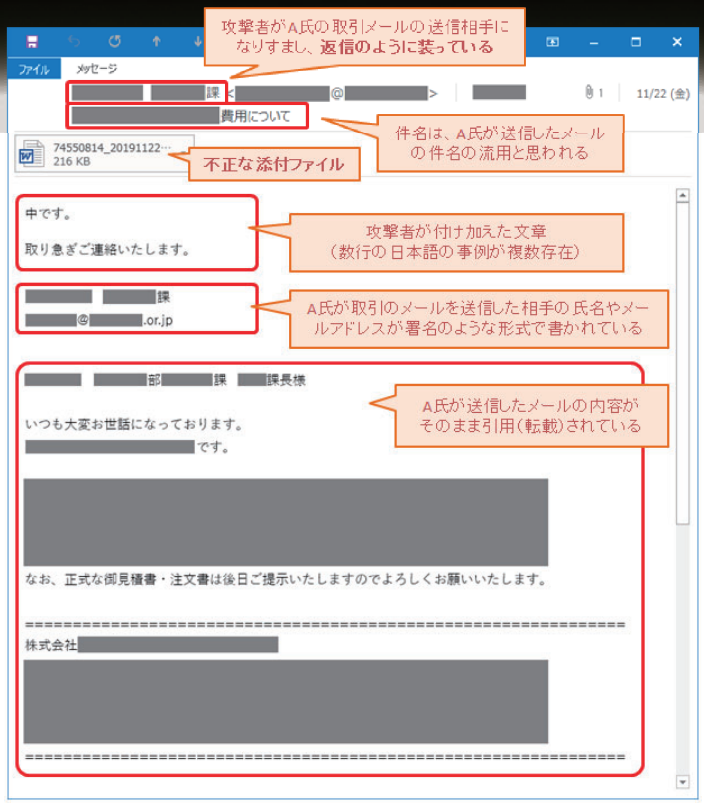
## 巧妙な拡散手法

感染 PC のメール履歴を含む情報を抜き取り巧妙な拡散メールを取引先に送信

マルウェアの「被害者」だが、同時に「加害者」的な立場に陥る

⬇

**信用の失墜・賠償責任**




Emotet 拡散メールサンプル参照元：独立行政法人 情報処理推進機構

## セキュリティの網を抜ける数々の機能

①本機能稼働前に環境をチェック

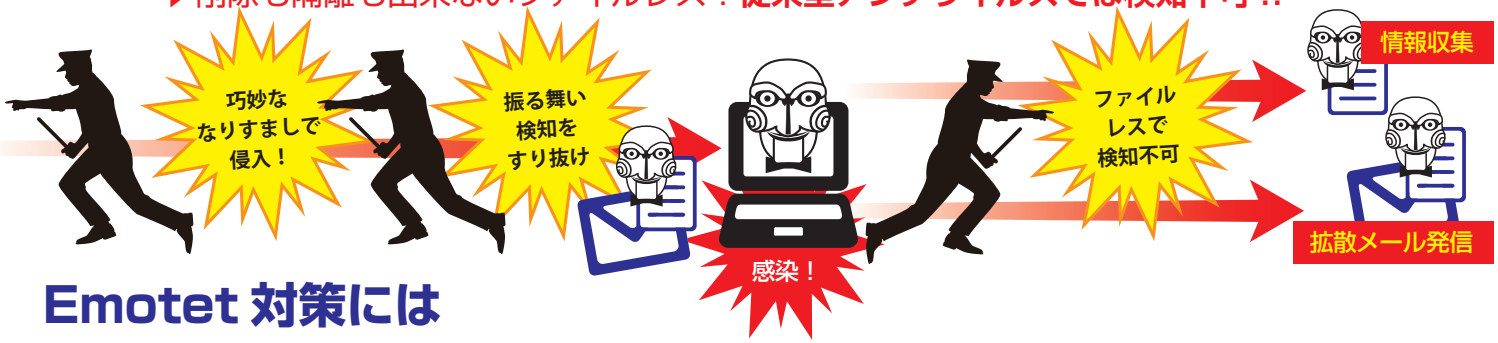
▶sandbox など仮想環境だと動作しない

▶振る舞い検知をすり抜け

②本体に不正なコードをほとんど含まない

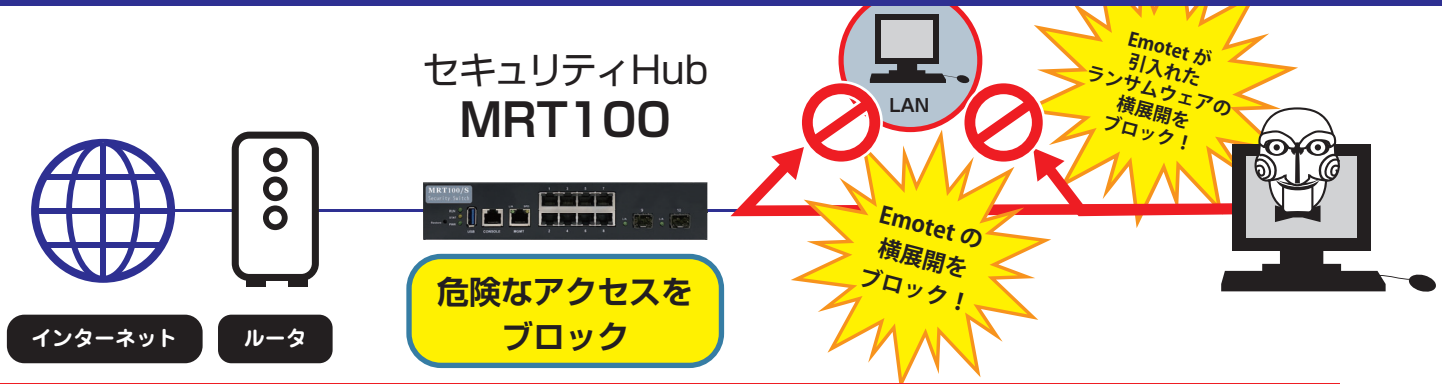
▶不正コードは攻撃者の用意する C&C サーバから最新のマルウェア（ランサムウェアを含む数々の攻撃ツール）をダウンロードし、保存せずメモリ上で作動

▶削除も隔離も出来ないファイルレス！**従来型アンチウイルスでは検知不可 !!**




## Emotet 対策には

### 不正通信を検知する MRT100 で Emotet の LAN 内感染を遮断！




MRTは内部対策です。出入口対策であるUTM等との併用による多層防御および不審なメールは開かないなどの意識づけも重要です。

株式会社 アレクソン