5分でわかる
シリーズ

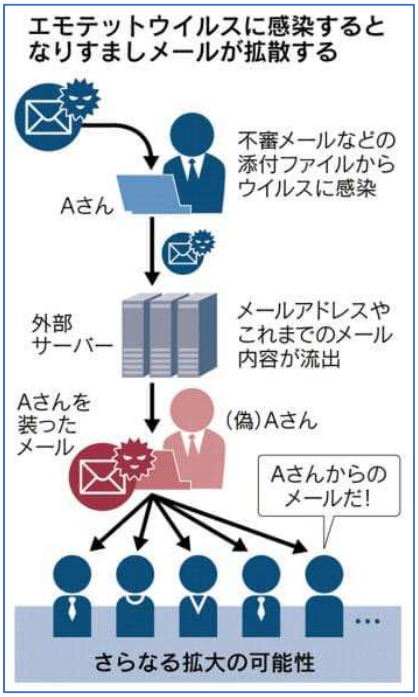
なりすましメール拡散ウイルス国内本格上陸
マルウェア「Emotet（エモテット）」について

RICOH
imagine. change.

欧米で流行しているコンピューターウイルス「Emotet（エモテット）」が日本に本格上陸し、被害が拡大しています。
感染すると**メールアドレスや本文を盗まれ、本人になりすましたメールが次々と関係者に送られる被害が多数報告されています。**
少なくとも400以上の団体・企業で被害が出ているとされ、民間団体などが注意を呼びかけています。

○「Emotet（エモテット）」はどんなマルウェア？

2014年にバンキングマルウェアとして確認されたマルウェア「Emotet」がボットネットとして進化し、2018年以降、世界中で猛威を振るっています。
感染したコンピューター内で所有者に気付かれることなく、様々な悪質なタスクを実行しています。**日本でも感染被害が増加**しております。



日本経済新聞　2019/11/29

【これまでのマルウェアとEmotetとの違いの特長】
実在の組織や人物になりすましたメールに添付されたファイルから**感染メールそのものが盗まれる**点

<侵入経路>
ほとんどがメール経由
（細工された**Wordファイル**によってEmotetに感染するケースが多い）

<感染により発生する被害>
- **取引先や顧客の連絡先とメールの内容が窃取され外部に送信される**
- **（取引先以外の）外部の組織に大量の不審メールを送信してしまう**
- **他のマルウエアがダウンロードされ感染する恐れ**
- **感染した端末内の資格情報やシステム上の脆弱点を利用した、ネットワーク内の別の端末への感染拡大**

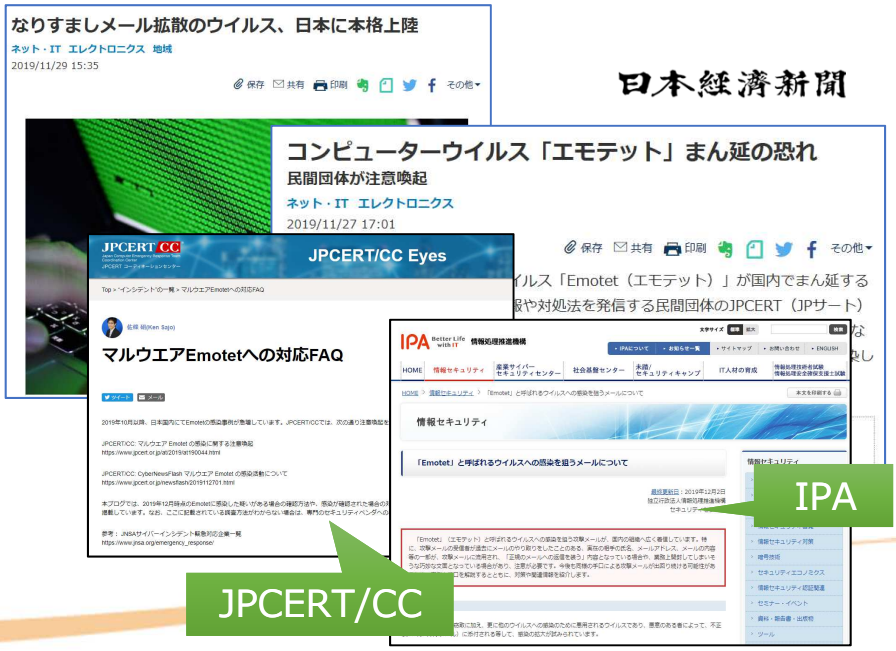
<感染被害が拡大している理由>
- コマンドプロンプトやPowerShellなど正規のプロセスを悪用しているため検出が困難
- 自身が頻繁に更新されるため、シグネチャによる検出が難しい。
- 本体に悪意のあるコードをできるだけ持たず、シグネチャによる検出が難しい。
- 解析環境であることを確認すると活動しないため、サンドボックスによる検出や、マルウェアの解析が難しい（シグネチャの作成が難しい）。

エモテットの感染被害

首都大学東京 (11/1)	教員が受信したメールの添付ファイルを開封しＰＣが感染。相次いで教職員などへ不審メールが届いた。
双葉電子工業 (11/8)	フィリピン子会社のＰＣがウイルスに感染。子会社の従業員とメールでやりとりした一部のアドレスが盗まれた。
京都市観光協会 (11/25)	同協会の職員のＰＣがウイルスに感染。職員を装ったメールが相次いで送信された。

(注)日付はウイルスへの感染を発表した日

日本経済新聞　2019/11/29



AppGuradならEMOTETからPCを守れます！

#	公表時期	国・地域	組織名	金銭影響	インシデント種別	説明
1	2014/7/9	日本	教育	260億円	内部犯行	約3504万件の情報漏えいが発生
2	2015/6/1	日本	公共機関	10億円	マルウェア感染	約125万件の個人情報の漏えいが発生
3	2017/6/28	ドイツ	製薬	360億円	ランサムウェア	ランサムウェアに感染し、ネットワークが優害
4	2017/8/16	デンマーク	運輸	330億円	ランサムウェア	数週間にわたり輸送の遅延などの混乱
5	2017/12/10	米国	運輸	440億円	ランサムウェア	運送システムに大規模な影響が発生した
6	2018/1/26	日本	仮想通貨取引所	580億円	不正アクセス	サイバー攻撃により仮想通貨NEMが流出
7	2018/4/25	米国	信用調査	260億円	不正アクセス	1.4億人分の情報が流出し、同社のCEOらが辞職
8	2018/8/6	台湾	製造業	275億円	ランサムウェア	製造システムが3日間停止し、納品が遅延
9	2018/10/26	香港	航空	226億円	不正アクセス	株価が3.8%安、時価総額を約226億円を失う
10	2019/3/18	ノルウェー	製造	45億円	ランサムウェア	手動操作に切り替えたことから、生産量が減少
11	2019/7/8	英国	航空	248億円	不正アクセス	個人情報漏えいでGDPR制裁金
12	2019/7/9	英国	ホテル	135億円	不正アクセス	個人情報漏えいでGDPR制裁金
13	2019/7/12	米国	SNS	5400億円	個人情報不正流出	利用者情報の不正流出に対するFTC制裁金

一般社団法人　日本サイバーセキュリティ・イノベーション委員会資料より抜粋

標的型攻撃メールによるコンピューターウイルス感染で
生徒など100名分の個人情報が漏えい。

想定被害額 890万円　　**年間売上の約18%の損害**

賠償損害		費用損害	
損害賠償	100万円	調査・復旧費用	500万円
訴訟費用	300万円	お客様対応費用（お詫び・お見舞金など）	10万円
		法律相談	20万円

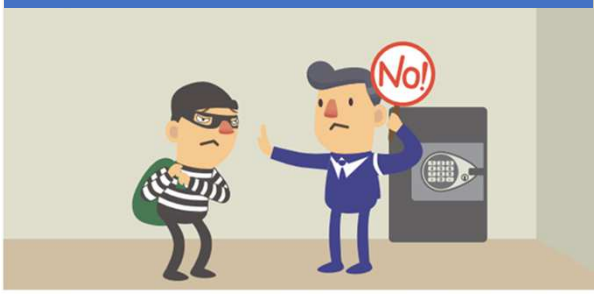
一般社団法人 日本損害保険協会HPより抜粋

サイバーセキュリティはITだけの問題ではなく、企業経営を脅かす問題になっています。

従来型アンチウイルスソフトは入れないようにして防御する

「未知のマルウェア」や「ゼロデイ攻撃」は防御できない

AppGuardは入られても悪さをさせない



「未知のマルウェア」や「ゼロデイ攻撃」への対策にも有効

APPGUARD

- レジストリに自動起動設定 → **レジストリの変更をブロック**
- メモリ読み込み/書き込み（ファイルレスマルウェア） → **メモリの読み書きをブロック**
- 最新バージョンにアップデート 攻撃モジュールダウンロード → **ダウンロードされたEmotetの実行をブロック**
- 同じネットワーク内の他PCに横展開 → **他PCでのEmotetの実行をブロック**

AppGuardは、これらの脅威からPCを守ることができます。
さらに言うと、お客様の事業そのものを守ることができる製品です。

お困りごとがありましたらお気軽にご連絡下さい。
提案ご支援いたします。

※記載の効果はあくまでも一例であり、すべてのお客様について同様の効果があることを保証するものではありません。
※記載の内容は予告なく変更になる場合があります。あらかじめご了承ください。
※記載の会社名および製品名は、各社の商号、商標または登録商標です。

RICOH imagine. change.
リコージャパン株式会社
東京都港区芝3-8-2 芝公園ファーストビル
お問い合わせ先：ricoh_scrumpackage@ricoh-japan.co.jp

●お問い合わせ・ご用命は・・・
株式会社 信交社　TEL 0263-25-9860
TAX 0263-72-7890

このチラシの記載内容は、2019年12月現在のものです。－Ver.1.2－