

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

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。

Q「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。

【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

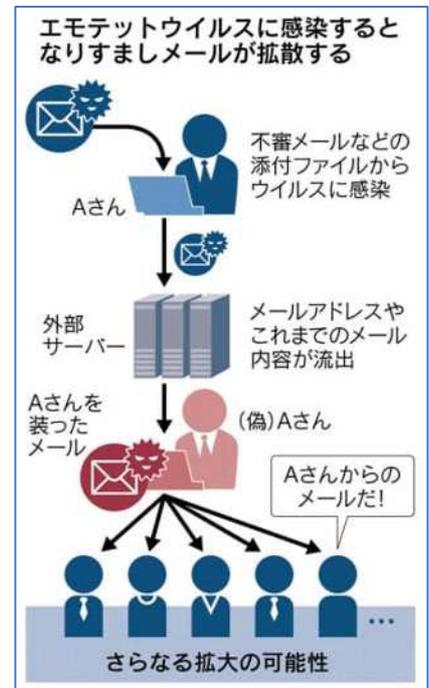
(細工されたWordファイルによってEmotetに感染するケースが多い)

<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
- ・他のマルウェ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)。



日本経済新聞 2019/11/29

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

なりすましメール拡散のウイルス、日本に本格上陸
ネット・IT エレクトロニクス 地球
2019/11/29 15:35

日本経済新聞

コンピューターウイルス「エモテット」まん延の恐れ
民間団体が注意喚起
ネット・IT エレクトロニクス
2019/11/27 17:01

JPCERT/CC Eyes

マルウェアEmotetへの対応FAQ

IPSA

IPSA

JPCERT/CC

○サイバー攻撃により多大なビジネス影響が発生

感染後の事後対応策も大事ですが、そもそも感染を予防する対策は十分ですか？

#	発症時期	国・地域	組織名	金額影響	インシデント種別	説明
1	2014/7/9	日本	教育	260億円	内部取引	約3504万円の債権差入りが発生
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、ネットワークが被害
4	2017/8/16	デンマーク	運輸	330億円	ランサムウェア	鉄道線におよび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	14億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	台湾	航空	226億円	不正アクセス	稼働が3.8%減、時限稼働を約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	米国	航空	248億円	不正アクセス	個人情報漏えいでGDP削減
12	2019/7/9	米国	ホテル	135億円	不正アクセス	個人情報漏えいでGDP削減
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罰金

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名分の個人情報情報が漏えい。

想定被害額 890万円

年間売上上の約18%の損害

賠償損害

損害賠償 100万円
訴訟費用 300万円

費用損害

調査・復旧費用 500万円
お客様対応費用 (お詫言・お礼資金など) 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。

AppGuard Marketing, Inc.
Safety and Smile with AppGuard

〒162-8565 東京都新宿区揚場町2-1
軽子坂MNビル 8階
TEL: 03-5989-0855
<https://appguard-m.com/>

お問合せ

システム・アルファ株式会社

第3ソリューション部 担当 中島 矢端

〒371-0847 群馬県前橋市大友町2-23-5
TEL: 027-210-7600 FAX: 027-252-7330