歴史とともに振り返る、バンキングマルウェアの脅威

調査レポート

2018

安全なネット活用のための

セキュリティ情報

はじめに

バンキングマルウェアは、インターネットバンキングの認証情報（ユーザーIDやパスワード等）やクレジットカード情報を窃取するマルウェアです。バンキングマルウェアに感染すると銀行口座からの不正送金やクレジットカードの不正利用などの被害に遭う可能性があり、日本国内でも大きな被害が出ています。

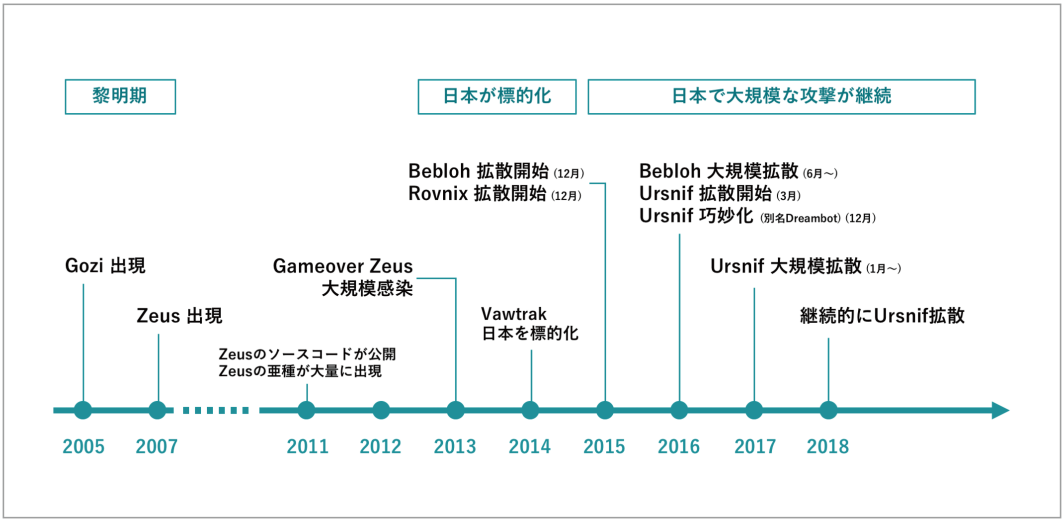
本レポートでは、これまでキヤノンマーケティングジャパンのマルウェアラボより公開している「マルウェアレポート」でもお伝えしてきたバンキングマルウェアについて、国内を中心に2018年までの主なイベントや感染時の動作、対策について解説しています。

歴史とともに振り返る、バンキングマルウェアの脅威

contents

歴史とともに振り返る、バンキングマルウェアの脅威

バンキングマルウェアの歴史



国内の主なバンキングマルウェア関連イベント[1]

[1] マルウェア情報局：2018年上半期のマルウェアレポート https://eset-info.canon-its.jp/malware_info/trend/detail/180824.html

2000年代後半：バンキングマルウェアの黎明期

バンキングマルウェアは、2005年ごろから存在が確認され始めました。最初期の代表的なバンキングマルウェアには、2005年に確認されたGozi、および2007年に確認されたZeusがあります。これらは本来、さまざまなマルウェアを作成するための商業的目的を持ったツールキット[2]でしたが、これらの持つバックドア機能、キーロギング機能、Webインジェクション機能などがオンラインバンキングを狙った攻撃に転用されています。

GoziとZeusの機能は多数のマルウェアに取り込まれました。2009年に登場したSpyeyeはZeusの対抗馬として活動していました[3]が、2010年にZeusの作者がソースコードをSpyeyeの作者に提供したことで、ZeusとSpyeyeが統合されました。また、2010年にGozi、2011年にZeusのソースコードがそれぞれ流出したことをきっかけに大量の亜種が作成され、後に紹介するさまざまなバンキングマルウェアのほか、Ramnit、Citadel、Dyre（別名：Trickbot）などのバンキングマルウェアが誕生しました。

2010年代前半：日本が標的とされ始める

バンキングマルウェアが現れ始めた2000年代後半は主に日本国外のインターネットバンキングが標的とされていましたが、2011年ごろから日本も主要な標的とされています。

Zeusの亜種であり2011年に登場したGameover Zeus（GOZ）はP2P技術を悪用して各国で大量感染を引き起こしました。警察庁によると[4]、世界中で50万～100万台の端末がGOZに感染し、そのうち約25%が米国、約20%が日本に所在していたと推定されています。GOZはその感染規模の大きさから、2014年、FBIとユーロポールを中心とした各国の法執行機関が協力し、テイクダウン作戦が行われました。

2012年に出現したCridex（別名：Bugat, Feodo, Dapato）はZeusをもとにしたワーム[5]型のバンキングマルウェアで、バックドア機能や他端末への感染拡大機能を持ち、日本を中心に感染を広げました。

2014年にはCridexの後継であるDridexが出現し、Office製品の脆弱性を狙ったり、複合機から送信されたメールのように見せかけるソーシャル・エンジニアリング[6]手法を用いたりするなど、手口が巧妙化しました[7]。同じく2014年には

[2] 現在はこのような形態に対してMalware as a Serviceという表現（レトロニム）が用いられることがあります。
[3] Zeusの駆除機能すら搭載されていました。
[4] 警察庁：インターネットバンキングに係る不正送金事犯に関連する不正プログラム等の感染端末の特定及び駆除について
～国際的なボットネットのテイクダウン作戦～（リンク切れ）
[5] マルウェア情報局：ワーム https://eset-info.canon-its.jp/malware_info/term/detail/00107.html
[6] マルウェア情報局：ソーシャル・エンジニアリング https://eset-info.canon-its.jp/malware_info/term/detail/00069.html
[7] マルウェア情報局：複合機からの通知メールを装うDridex、その傾向と対策策 https://eset-info.canon-its.jp/malware_info/trend/detail/150819.html

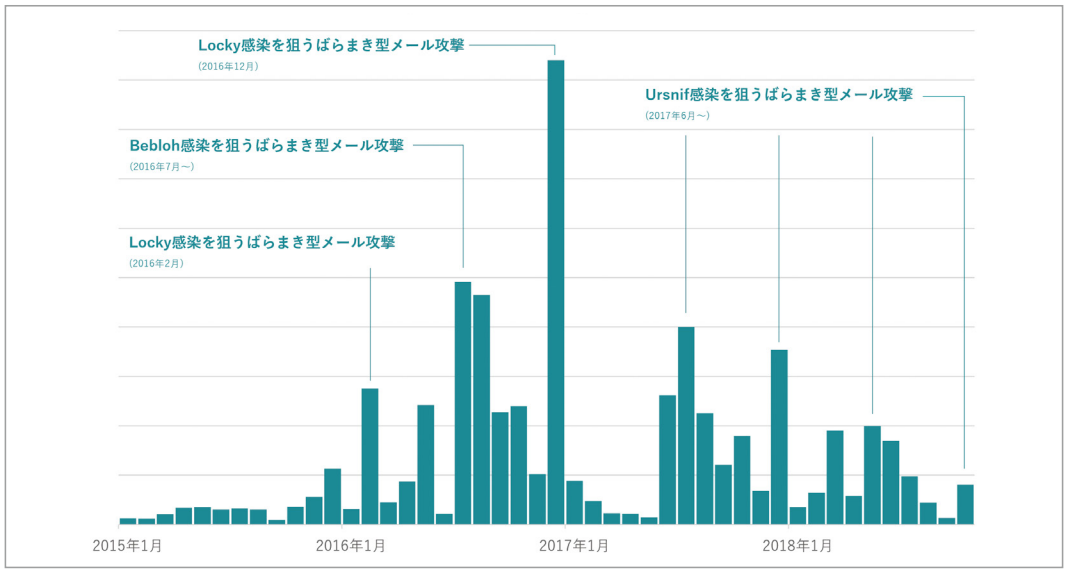
Goziをもとに作成されたVawtrakが日本を標的としました。2015年に警視庁主導のもとVawtrakを対象にテイクダウン作戦が行われ[8]、少なくとも世界で約8万2,000台、うち国内で約4万4,000台の感染端末が特定されました。ほかにも、Neverquest、Shifu、Tsukuba、Brolux、Rovnixといったマルウェアが続々と日本の金融機関を標的とするようになりました。

日本での不正送金被害は2014年～2015年がピークであり、警察庁によると[9] [10]、年間約1500～1900件、金額にしておよそ30億円の不正送金被害が確認されています。

2010年代中盤～現在：日本への大規模な攻撃が継続的に行われる

2015年12月のRovnix 、Bebloh（別名：URLZone, Shiotob）の大量拡散を皮切りに攻撃の規模が拡大し、その頻度も増加しました。2016年6月にはBeblohへの感染を狙う過去最大規模のばらまき型メールが確認されました[11]。Beblohは2009年に初めて登場したバンキングマルウェアで、強力な耐解析機能やプロセス秘匿機能を持ちます。2010年代中盤になってから大規模な攻撃キャンペーンで使用されるようになり、欧州で猛威を振るっていました。

以下のグラフは、ESET製品がマクロウイルス型ダウンローダー（ESET検出名：VBA/TrojanDownloader.Agent）を国内で検出した件数です。あくまでもダウンローダーの統計のため、バンキングマルウェア以外のマルウェアへの感染を狙った攻撃が含まれ、一方でバンキングマルウェアを直接メールに添付したケースなどは含まれていませんが、定期的に攻撃が発生している様子が見て取れます。



VBA/TrojanDownloader.Agent検出数の推移 [12]

[8] 警視庁：ネットバンキングウイルス無力化作戦の実施について（リンク切れ）
[9] 警察庁：平成26年中のインターネットバンキングに係る不正送金事犯の発生状況等について http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf
[10] 警察庁：平成27年中のインターネットバンキングに係る不正送金事犯の発生状況等について http://www.npa.go.jp/cyber/pdf/H280303_banking.pdf
[11] マルウェア情報局：バンキングトロージャン「Bebloh」感染を狙った日本への攻撃が急増 https://eset-info.canon-its.jp/malware_info/news/detail/160617.html
[12] 図中のLockyはランサムウェアの一種

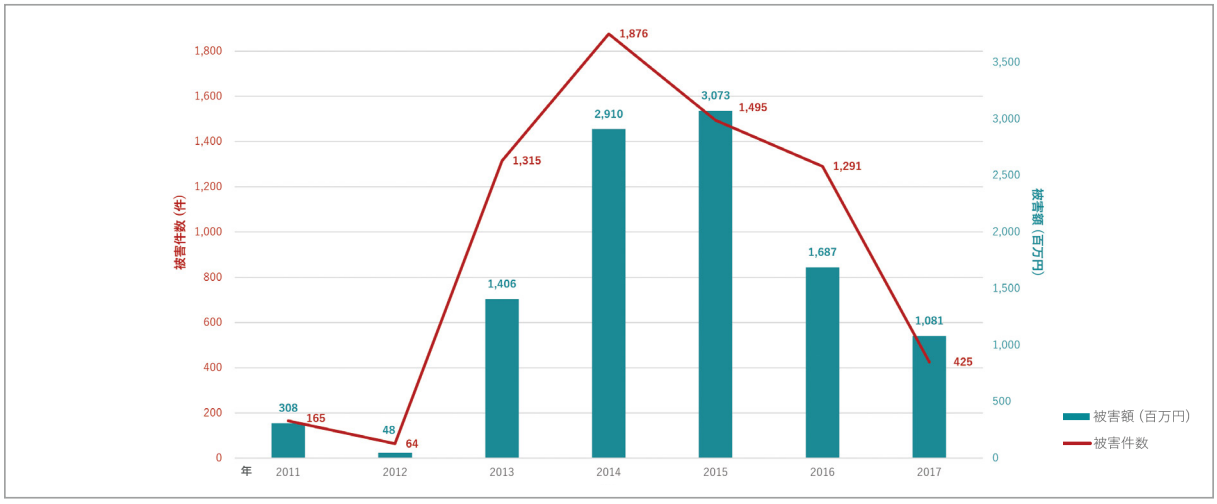
2016年3月ごろからはBeblohに代わりUrsnif（別名：Gozi, Papras, Snifula, DreamBot）が情報窃取のメインコンポーネントとして利用されるようになりました。UrsnifはGoziの流れを汲み、Bebloh同様に強力な耐解析機能と多様な情報窃取機能を持ちます。現在はUrsnifを単独で用いるのではなく、Ursnifに感染させるためのダウンローダーとしてBeblohを利用しているケースが多く観測されており、マルウェアの利用方法にも変化がみられます。

被害状況

＜本章は特に記載のない限り、警察庁発表のデータ[13] [14] [15] [16] [17] [18] をもとに作成しています。＞

インターネットバンキングに係る国内の不正送金事犯は、2011年、2012年は200件に満たない件数でした。しかし、2013年から件数も被害額も急増し、2014年には1,876件、その被害額は約29億1000万円に到達し、過去最悪を記録しています。2015年は1,495件と件数は減少していますが、被害額はさらに増加し約30億7300万円となっています。

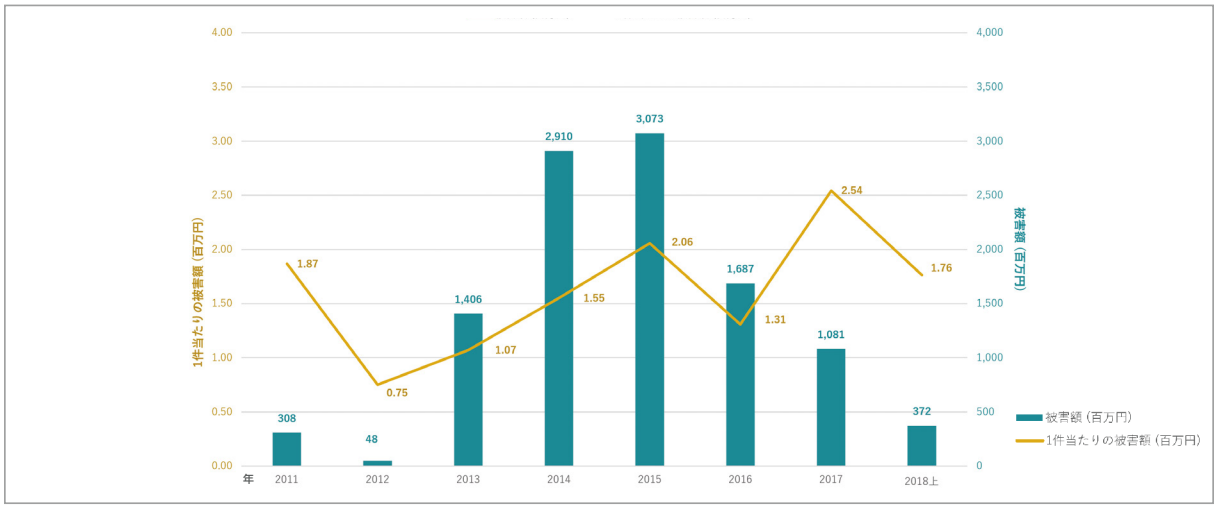
2016年になると国内の不正送金被害は落ち着きを見せ、件数は1,291件、その被害額は約16億8700万円と急減しました。2017年は425件、被害額は約10億8100万円とさらに減少しています。その理由としては、マルウェア検知対策の向上、不正送金に使用されたIPアドレス等に対する金融機関の監視強化、ワンタイムパスワードの導入などの対策が進んでいることが挙げられています。



インターネットバンキングに係る国内の不正送金事犯の件数と被害額の推移

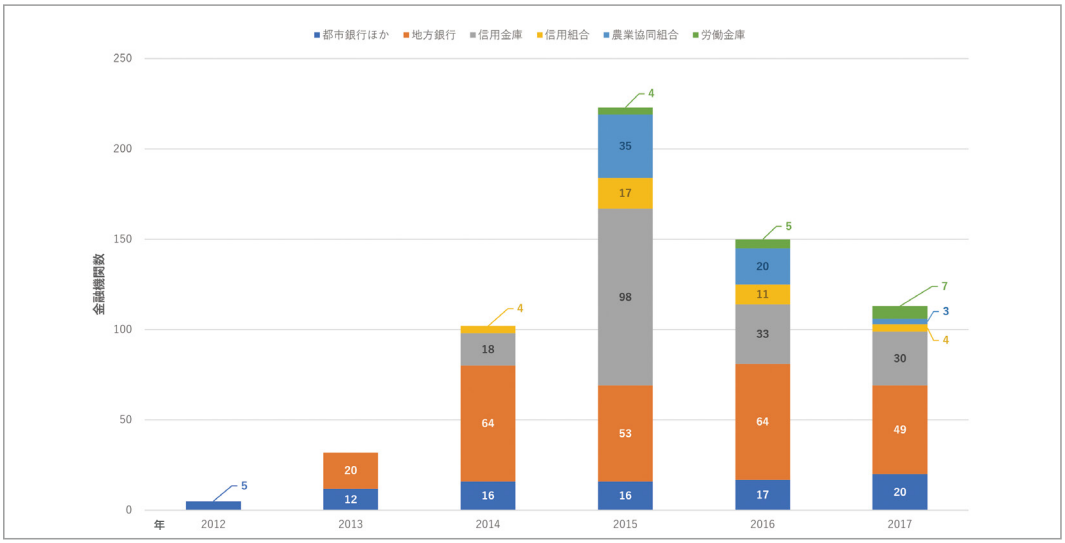
[13] 警察庁：インターネットバンキングに係る不正送金事犯被害の実態と防止策 https://www.antiphishing.jp/news/pdf/apcseminar2014npa.pdf
[14] 警察庁：平成26年中のインターネットバンキングに係る不正送金事犯の発生状況等について http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf
[15] 警察庁：平成27年中のインターネットバンキングに係る不正送金事犯の発生状況等について http://www.npa.go.jp/cyber/pdf/H280303_banking.pdf
[16] 警察庁：平成28年中におけるサイバー空間をめぐる脅威の情勢等について http://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf
[17] 警察庁：平成29年中におけるサイバー空間をめぐる脅威の情勢等について http://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf
[18] 警察庁：平成30年上半期におけるサイバー空間をめぐる脅威の情勢等について http://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_kami_cyber_jousei.pdf

しかしながら、1件あたりの被害額は全体的に増加傾向にあり、2017年は過去最高の254万円となっています。2018年上半期は1件あたり176万円と減少がみられたものの、なお高い水準にあります。ここから、バンキングマルウェアの1件あたりの収益性は徐々に向上してきていると考えられます。



インターネットバンキングに係る国内の不正送金事犯の被害額の推移

バンキングマルウェアの標的となった国内の金融機関は、都市銀行、信託銀行、地方銀行などから労働金庫に至るまで多岐にわたり、少なくとも223の金融機関が標的となったことが報告されています。金融庁によると[19]、2018年11月27日現在で金融庁に登録されている金融機関の数は、都市・信託・その他銀行が34、地方銀行（第二地方銀行を含む）が104、信用金庫が261、信用組合が148、労働金庫が13となっています。銀行や金庫を中心に高いカバレッジで攻撃が行われていた様子が窺えます。



被害金融機関数の推移

[19] 金融庁：免許・許可・登録等を受けている業者一覧 https://www.fsa.go.jp/menkyo/menkyo.html

主な侵入経路

バンキングマルウェアは、大部分のケースにおいて、不特定多数に一斉配信されるメール(ばらまき型メール)によって配布されています。水飲み場型攻撃(攻撃対象とする特定分野の組織やユーザーがよく利用するWebサイトを改ざんし、マルウェアに感染させる標的型攻撃の一種)でのWeb経由の感染も報告されていますが、割合としては少数とみられます。

当社では、ばらまき型メールについて、以下のようなパターンを観測しています。

1. **添付ファイルとしてダウンローダーやバンキングマルウェア本体が添付されているパターン**
   - Microsoft Officeファイル(Wordファイル、Excelファイルなど)
   - スクリプトファイル(VBScript、JavaScriptなど)
   - PDFファイル
   - 実行ファイル(.exe、.srcなど)
   - その他のファイル(.iqyなど)

2. **本文にダウンロードリンクが記載されているパターン**

それぞれについて説明します。

1. 添付ファイルとしてダウンローダーやバンキングマルウェア本体が添付されているパターン

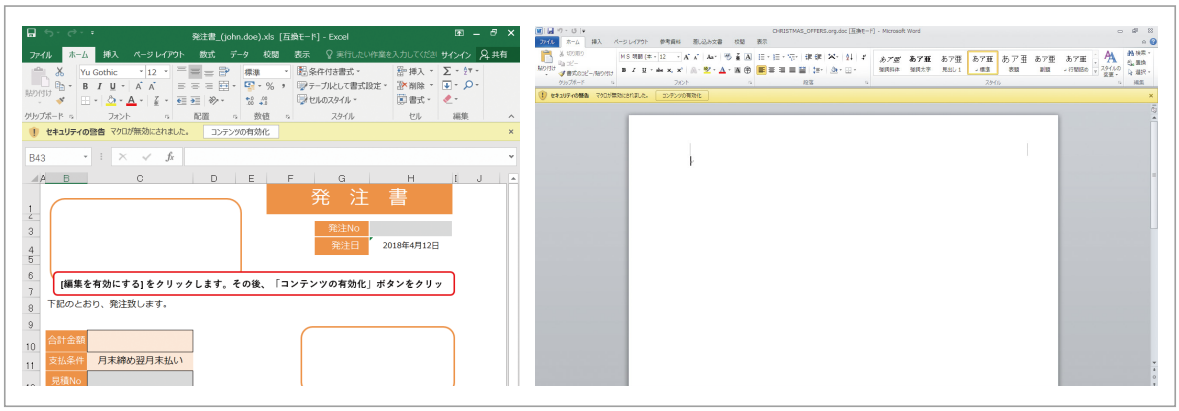
添付ファイルとしてダウンローダーやバンキングマルウェア本体が添付されているパターンの例を以下に示します。

ダウンローダーが添付されたばらまき型メール [20] [21] [22]

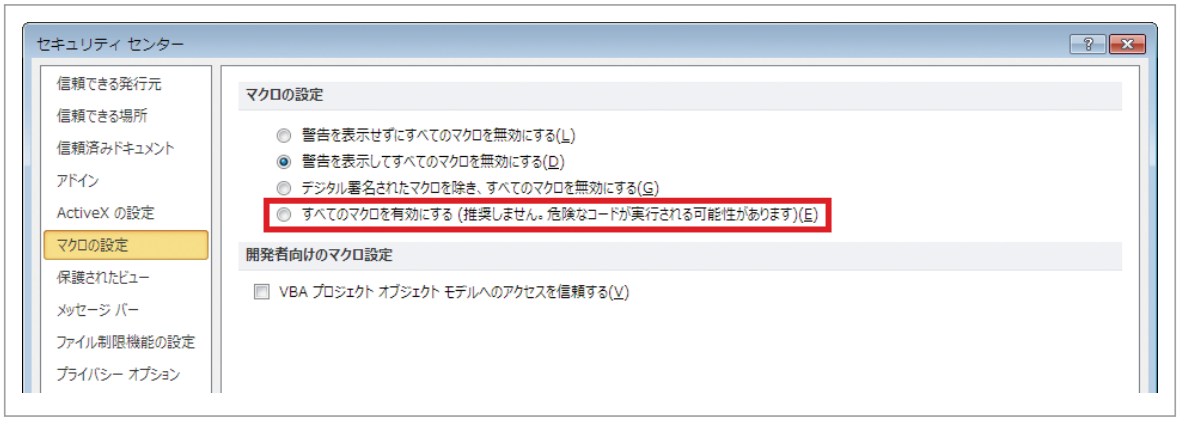
[20] マルウェア情報局:2018年7月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1807.html
[21] マルウェア情報局:2018年8月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1808.html
[22] マルウェア情報局:2018年10月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1810.html

ダウンローダーが添付されているパターンでは、主に数KB～数百KB程度のサイズの小さなファイルが添付されており、何らかの方法でWeb上から次段のダウンローダーやバンキングマルウェア本体をダウンロード・実行します。この大まかな流れは、どの種類の添付ファイルでもおおむね同様です。

近年もっとも頻繁に観測されるダウンローダーはMicrosoft Officeファイルです。Microsoft Officeファイルを悪用して次段のマルウェアをダウンロード・実行するための手段としては、マクロとしてダウンロード処理を記述しファイル開封時に実行させる、DDE（Dynamic Data Exchange）経由でPowerShellなどの外部プログラムにダウンロード処理を実行させる、OfficeやWindowsの脆弱性を用いてダウンロード処理を実行する、などが挙げられます。前述のVBA/TrojanDownloader.Agentでは、次段のマルウェアをダウンロード・実行するコードがマクロとしてファイル内に記述されています。ユーザーがマクロの実行を許可したり、あるいは許可なくマクロを実行する設定になっていたりするとこのコードが実行されます。



VBA/TrojanDownloader.AgentをMicrosoft Officeで開いた画面[23]
（画面上部の「コンテンツの有効化」をクリックするとマクロが実行される）



確認なくマクロを実行するMicrosoft Wordの設定
（本設定項目有効化は推奨しません）

[23] マルウェア情報局：2018年3月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1803.html

また、スクリプトファイル（JavaScript、VBScriptなど）を添付したパターンもみられました[24]。これらのスクリプトはWebブラウザー上で実行されるわけではなく、バッチファイルのようにダブルクリックすると、WSH（Windows Script Host）によって実行されます。基本的な流れは次項「本文にダウンロードリンクが記載されているパターン」と同様ですが、Webブラウザーでダウンロードしたjavascriptファイルを実行するのではなく、メールに添付されたJavaScriptファイルを実行する点が異なります。

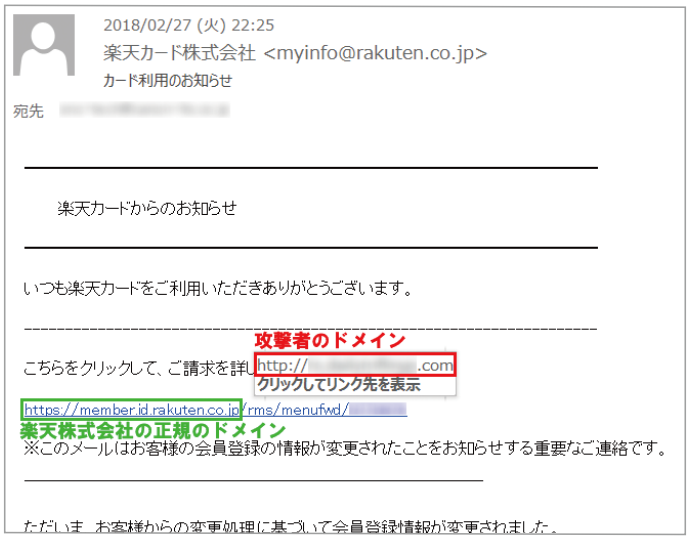
バンキングマルウェア本体が添付されているパターンでは、二重拡張子やRLO[25]などを用いて文書ファイルなどに偽装した実行ファイルが添付されています。2010年代中盤まではこの方法が時折見られましたが、対策が進んだためか、最近はあまり見られなくなりました。

上記方法のほかにも、Webクエリファイル（IQYファイル）を用いた方法[26]、判読不能な画像とVBScriptを用いた方法[27]、ステガノグラフィーを用いて画像ファイル内にダウンロードコードを隠す方法[28]などが観測されています。

2. 本文にダウンロードリンクが記載されているパターン

次に、本文にダウンロードリンクが記載されているパターンの例を以下に示します。

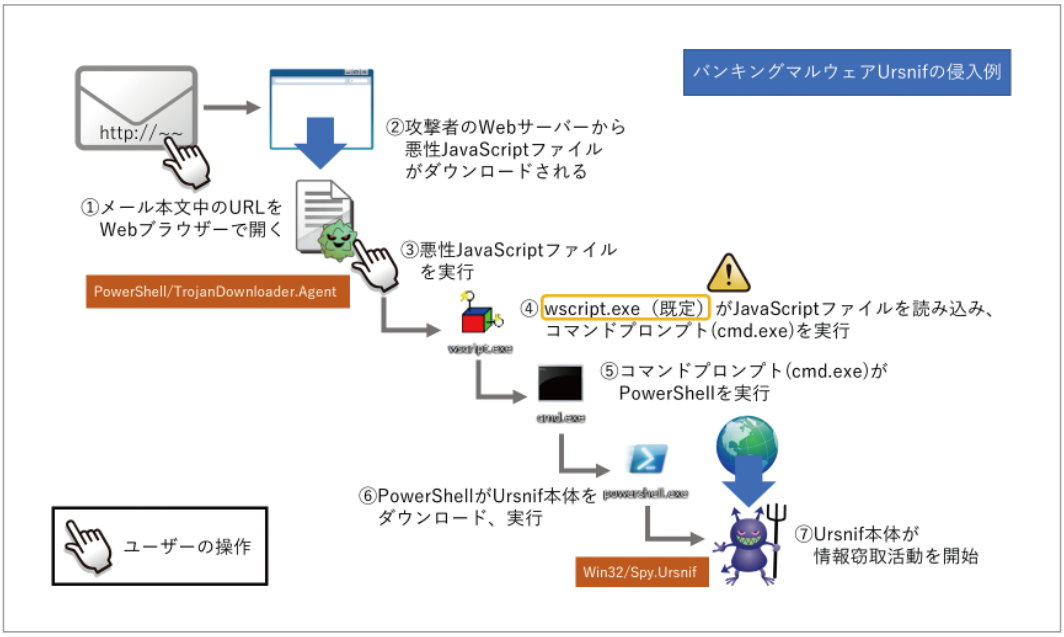
以下の例は、2018年2月に確認された、楽天カードを騙るばらまき型メールです[29]。



楽天カードを騙るばらまき型メールの例

[24] JavaScriptを添付したケースでは、Lockyなどのランサムウェアがダウンロードされる場合も多く観測されました。
[25] Right-to-Left Override。表示上の文字の流れを右から左に変更する制御文字で、これをファイル名に挿入することにより、表示上の拡張子を偽装することができる。 例）example[RLO]fdp.exe => exampleexe.pdf
[26] マルウェア情報局：2018年7月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1807.html
[27] マルウェア情報局：2018年8月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1808.html
[28] マルウェア情報局：2018年10月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1810.html
[29] マルウェア情報局：2018年2月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1802.html

次段のマルウェアのダウンロードリンクがそのまま本文中に記載されている場合もありますが、このケースでは、見た目のURLは正規のドメインでありながら、実際のリンク先は攻撃者のドメインになっていました。こうして攻撃者の用意したURLにアクセスすると次段のマルウェアがダウンロードされます。ダウンロードされたマルウェアをユーザーが手動で実行してしまうと[30]最終的にバンキングマルウェアに感染することになります。



楽天カードを騙るばらまき型メールからバンキングマルウェアに感染するまでの流れ

また、偽アプリを用いてAndroid端末をバンキングマルウェアに感染させる[31] [32] [33]といった、Windowsやメールを対象としない攻撃も確認されています。

このように、攻撃者はバンキングマルウェアに感染させようとさまざまな方法を試みており、特に2010年代後半はばらまき型メールを中心にさまざま攻撃手法が観測されています。これは、前章で解説したようにバンキングマルウェアに対する対策が進み、収益性が低下していることも関係しているかもしれません。

[30] 水飲み場型攻撃によって自動的にダウンロード・実行が行われる可能性もあります。
[31] マルウェア情報局：オンラインバンクを襲うトロイの木馬がAndroid機器に出現 https://eset-info.canon-its.jp/malware_info/news/detail/160329.html
[32] マルウェア情報局：世界中のユーザーを狙った不正ファイナンスアプリがGoogle Play上に https://eset-info.canon-its.jp/malware_info/special/detail/181106.html
[33] マルウェア情報局：Google Playに今なお潜伏し続けるバンキングトロージャン https://eset-info.canon-its.jp/malware_info/special/detail/181122.html

バンキングマルウェアが窃取する情報

バンキングマルウェアが窃取しようとする情報には、以下のものがあります。

- 特定のWebサービス（特にインターネットバンキング、クレジットカードの会員サイト、ECサイト、仮想通貨取引所、Webメール）の認証情報（ID、パスワードなど）
- 特定のアプリケーション（特にWebブラウザー、メールクライアント、FTPクライアント）の認証情報（ID、パスワードなど）
- Webブラウザー上でHTMLフォームに入力した内容
- WebブラウザーのCookie
- Webカメラやマイクから入力された動画や音声
- OSやWebブラウザーの情報
- メールアドレス
- デジタル証明書　　など

攻撃手法

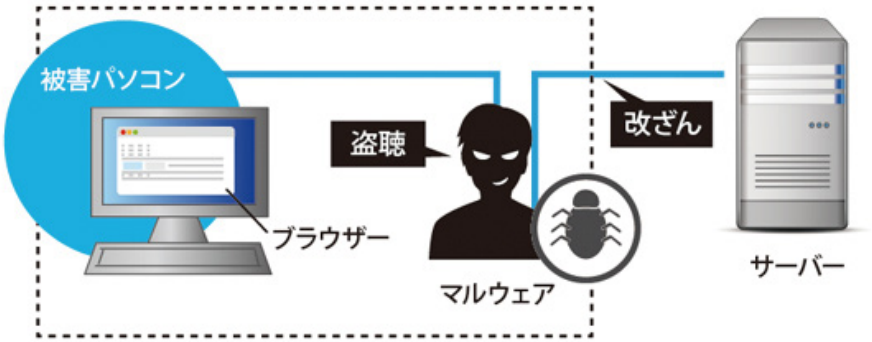
バンキングマルウェアは、前述の情報を窃取するために、一般的なマルウェアに共通する動作に加え、以下のような動作を行います。

- Webインジェクションを用いたMitB、リダイレクション
- Webプロキシを用いたMitM
- キーロギング
- スクリーンショット撮影

各攻撃手法について解説します。

Webインジェクションを用いたMitB、リダイレクション

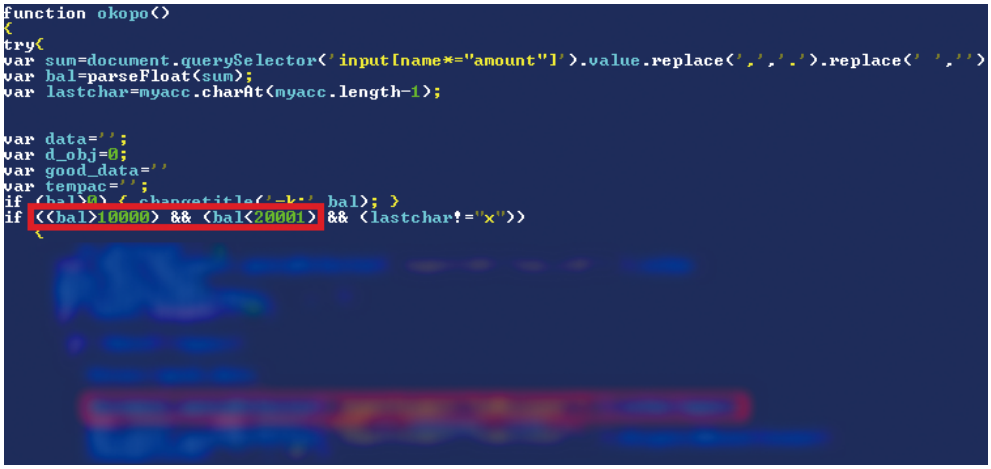
MitB（Man in the Browser）[34]はMitM（Man in the Middle; 中間者攻撃）[35]の一種で、Webブラウザー上で不正コードを実行することで、インターネットバンキングサービスを提供するWebサーバーとWebブラウザー間の通信を傍受、改変する攻撃です。この攻撃はPC上で行われるため、通信先のWebサーバーは正規のサーバーのままであり、通信先ドメインやIPアドレスで通信を遮断することはできません。



MitB攻撃のイメージ図

Webインジェクションでは、Webブラウザー上で表示されるWebページに対して不正なHTMLやJavaScriptを挿入します。その手法としては、Webブラウザーのプロセスに対してコードインジェクションを行い、HttpOpen/SendRequest、InternetRead/WriteFile、PR_Read/Write、ssl_read/write_app_dataといった通信に関わる関数をフックする方法が主に用いられます。また、BackSwap[36] [37]のような新しい攻撃手法も確認されています。BackSwapでは、SetWinEventHook関数でいくつかのWindowsメッセージをフックし、Webブラウザーのウィンドウと閲覧中のURLを特定します。続いて、SendMesssage関数でユーザーのキー入力をエミュレートすることで開発者ツールやアドレスバーを操作し、不正なJavaScriptをWebページに対してインジェクトします。

[34] マルウェア情報局：MITB攻撃 https://eset-info.canon-its.jp/malware_info/term/detail/00051.html
[35] マルウェア情報局：MITM攻撃 https://eset-info.canon-its.jp/malware_info/term/detail/00049.html
[36] マルウェア情報局：2018年5月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1805.html
[37] ESET : BackSwap malware finds innovative ways to empty bank accounts https://www.welivesecurity.com/2018/05/25/backswap-malware-empty-bank-accounts/



```
function okopo()
{
try{
var sum=document.querySelector('input[name*="amount"]').value.replace(',','.').replace(' ','')
var bal=parseFloat(sum);
var lastchar=myacc.charAt(myacc.length-1);


var data='';
var d_obj=0;
var good_data=''
var tempac='';
if (bal>0) { changetitle('-k-' bal); }
if ((bal>10000) && (bal<20001) && (lastchar!="x"))
   {
```

Webページにインジェクトされた不正なJavaScriptの例

```
1  http://
2  https://
3  https://
4  https://
5  https://
6  https://
7  https://
8  https://
9  https://
10 https://
11 https://
12 https://
13 https://
14 https://
15 https://
16 https://
17 https://
18 https://
19 https://
20 https://
21 https://
22 https://
23 https://
24 https://
25 https://
```

Webインジェクションのターゲットとなるurlの一例

こうしてインジェクトされた不正なJavaScriptは、以下のような動作を行います。

- オンラインバンキングのアカウント情報を攻撃者が用意したサーバー（マニピュレーションサーバー）へ送信する
- 送金先の口座を攻撃者の口座に書き換える
- 不正送金に気づかせないように、表示される送金先を書き換える
- 正規のサービスには存在しない偽の認証画面を割り込ませる
- 閲覧中に正規のWebページから攻撃者のWebページに強制的にリダイレクトする

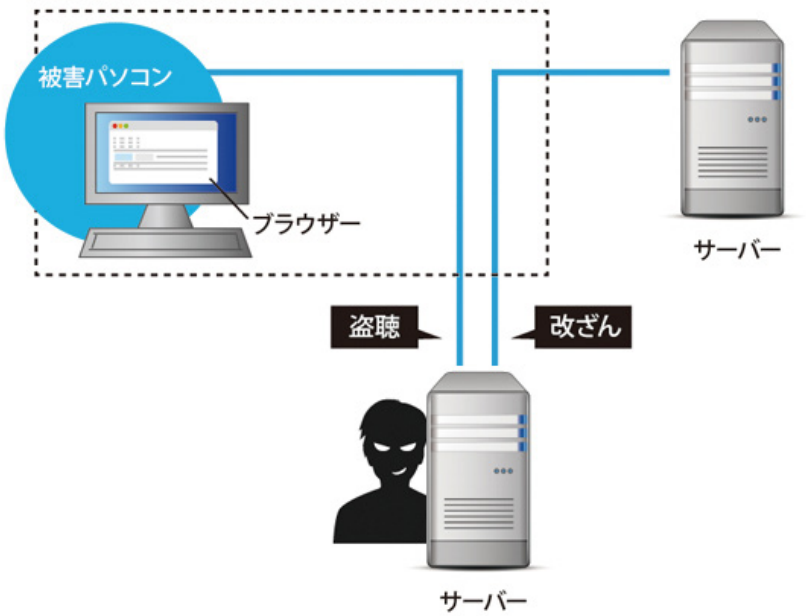
また、Webブラウザーで訪問したWebサイトの情報も記録される場合があります。

```
08-05-2017 11:15:38
USER: User01
URL: https://accounts.firefox.com/metrics
REF: https://accounts.firefox.com/
LANG: ja,en-US;q=0.7,en;q=0.3
AGENT: Mozilla/5.0 (Windows NT 6.1; rv:53.0) Gecko/20100101 Firefox/53.0
COOKIE:
POST: {"broker":"fx-firstrun-v2","context":"fx_firstrun_v2","duration":1672,"entrypoint":"firstrun",
,"screen":{"clientHeight":300,"clientWidth":400,"devicePixelRatio":1,"height":1440,"width":2560},"se
```

バンキングマルウェアによってWebサイト閲覧時に記録された内容

Webプロキシを用いたMitM

Webプロキシを用いたMitMでは、WindowsやWebブラウザーのプロキシ設定、hostsファイル、DNS設定などを変更し、WebブラウザーとWebサーバーとの間に不正なWebプロキシサーバーを割り込ませます。このWebプロキシサーバーではSSL/TLSの復号を行い、WebブラウザーとWebサーバーとの間で本来暗号化されているはずの認証情報や表示内容の窃取、改ざんを行います。



Webプロキシを用いたMitMのイメージ図

その場合、Webブラウザーから確認できるサーバー証明書は攻撃者のWebプロキシサーバーの(つまり不正な)証明書になるため、Webブラウザー上で警告が発生します。それを回避するため、WindowsやWebブラウザーの証明書ストアに攻撃者の証明書がインストールされることが一般的です。

Class 3 Public Primary Certif...	Class 3 Public Primary Certific...	2028/08/02	電子メールの保護,...	VeriSign Class 3 ...
Class 3 Public Primary Certif...	Class 3 Public Primary Certific...	2004/01/08	電子メールの保護,...	VeriSign Class 3 ...
Copyright (c) 1997 Microsof...	Copyright (c) 1997 Microsoft ...	1999/12/31	タイム スタンプ	Microsoft Timest...
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	2031/11/10	サーバー認証, ク...	DigiCert
Erenvob Aband	Erenvob Aband	2025/07/27	<すべて>	<なし>
Eyeixoon Lauvr	Erenvob Aband	2018/07/29	<すべて>	<なし>
GlobalSign Root CA	GlobalSign Root CA	2028/01/28	サーバー認証, ク...	GlobalSign
Goqq Ohedt	Juw Laonce	2018/08/08	<すべて>	<なし>
Itoimha Dafak	Qosmabj Zitmuy	2018/07/28	<すべて>	<なし>
Juw Laonce	Juw Laonce	2025/08/06	<すべて>	<なし>
Microsoft Authenticode(tm) ...	Microsoft Authenticode(tm) R...	2000/01/01	電子メールの保護,...	Microsoft Authen...
Microsoft Root Authority	Microsoft Root Authority	2020/12/31	<すべて>	Microsoft Root A...
Microsoft Root Certificate A...	Microsoft Root Certificate Aut...	2021/05/10	<すべて>	Microsoft Root C...
NO LIABILITY ACCEPTED, (...	NO LIABILITY ACCEPTED, (c)...	2004/01/08	タイム スタンプ	VeriSign Time St...
Qosmabj Zitmuy	Qosmabj Zitmuy	2025/07/26	<すべて>	<なし>
Thawte Timestamping CA	Thawte Timestamping CA	2021/01/01	タイム スタンプ	Thawte Timesta...
UTN-USERFirst-Object	UTN-USERFirst-Object	2019/07/10	タイム スタンプ, ...	USERTrust
VeriSign Class 3 Public Prim...	VeriSign Class 3 Public Primar...	2036/07/17	サーバー認証, ク...	VeriSign

マルウェアによってインストールされた不正なルート証明書の例

キーロギング

バンキングマルウェアは、Webブラウザー上でHTTPリクエストやレスポンスを窃取、改ざんするだけでなく、キー入力の履歴を保存する場合があります。ここにはオンラインバンキングでログインや送金を行った時のキー入力内容も含まれており、ユーザー名やパスワード、第二暗証番号などが窃取されるおそれがあります。また、記録される内容には、送金先をはじめとするさまざまな機密情報も含まれる可能性があります。

```
02-05-2017 18:10:55
C:¥Program Files¥Internet Explorer¥IEXPLORE.EXE
http://www.bing.com/search?q=test&src=IE-SearchBox&FORM=IE8SRC - Windows Internet Explorer

hogehoge
```

バンキングマルウェアによって記録されたキー入力

スクリーンショット撮影

これまで説明した方法に加え、スクリーンショットを動画で撮影し、入力内容を窃取しようとするバンキングマルウェアも確認されています。スクリーンショットの撮影が行われると、Webブラウザー上で利用できるソフトウェアキーボード（スクリーンキーボード）の入力状況を確認することができるため、キーボードから入力をしていなくてもオンラインバンキングのアカウント情報が窃取される可能性があります。

バンキングマルウェアによって記録されたスクリーンショット

その他の特徴

前述の特徴に加え、多くのバンキングマルウェアは以下の特徴を持ちます。

- さまざまな解析妨害機能
- ステルス性
- 感染、攻撃の永続性

各特徴について解説します。

さまざまな解析妨害機能

バンキングマルウェアは、解析技術者や自動解析ソフトウェアなどによって解析されるのを防ぐ（時間稼ぎを行う）ため、さまざまな解析妨害機能を搭載しています。
以下に、その代表例を示します。

- SetupDi関数、SetupDiGetDeviceRegistryProperty関数によりデバイス名を取得し、仮想環境に特有の文字列がないか確認する
- GetCursorPos関数でマウスポインタの座標を繰り返し計測し、前回の座標との差が特定の値になるまで動作を開始しない
- CPUID命令の実行時間を計測する
- CreateFile関数で自分自身を排他モードで開き、デバッガなどほかのプロセスが自身を開いていないか確認する
- EnumFonts関数のコールバックを利用したコード実行
- プロセス一覧やウィンドウ一覧から解析ツールが動作していないか確認する
- 複数のメモリ領域、複数のプロセスにわたる複雑なジャンプやコードインジェクション
- 大量のダミーコード
- シェルコードやペイロードの暗号化
- ドメイン生成アルゴリズム（DGA）を用いて通信先C&Cドメインを動的に生成する
- 後述のステルス性を与える各機能

ステルス性

バンキングマルウェアは、攻撃を秘密裏かつ継続的に行ったり、解析を妨害したりするため、さまざまな方法で自身のプロセスやその他の痕跡を隠蔽しながら動作します。
以下に、その代表例を示します。

- explorer.exeやsvchost.exeに自身のコードをインジェクションし、実行プロセスを偽装する
- 正規のプロセスをサスペンド状態で起動した後、そのプロセスメモリに自身のコードを書き込み、動作を再開することで正規のプロセスに偽装する（Process Hollowing）
- 上記プロセス偽装を多重に行う
- 感染の永続化を自身のプロセス終了時に行う
- 自身の実行ファイルを削除する
- ルートキットを用いて自身のファイルやプロセスを隠蔽する

感染、攻撃の永続性

バンキングマルウェアは、攻撃を継続的に行うため、コンピューターを再起動しても攻撃を継続できるよう、感染を永続化させます。
以下に、その代表例を示します。

- レジストリのRunキーに自身（のコピー）を登録し、次回起動時に再度実行されるようにする
- セキュリティソフトウェアの動作を妨害する
- 自身のオンラインアップデートを行う

対策

バンキングマルウェアに感染した場合、感染が発生してからそれを検知・対応するまでの短時間に不正送金被害が発生するおそれがあり、感染の予防（感染リスクの軽減）が重要になります[38]。それに加えて、バンキングマルウェアに感染してしまった場合でも迅速に対応できるように複数の対策を講じておく必要があります[39]。
例えば、バンキングマルウェアに対して以下のような対策を講じることができます。

- 利用しているWebサービスのアカウントの棚卸と利用権限の整理を行う
- インターネットバンキング等を利用する端末と担当者を限定する
- 担当者やその他のメンバーに対してリテラシー教育やインシデント対応訓練を行う
- 金融機関の提供するセキュリティ対策（ワンタイムパスワードなど）を実施する
- システムやアプリケーションのアップデートを適用する、あるいは脆弱性緩和ツールを用いて、脆弱性を軽減する
- マクロ機能やスクリプトの実行を制限し、ダウンローダーの実行を防止する[40]
- マルウェア対策製品を導入し、マルウェアを迅速に検知・駆除する
- ネットワーク監視を行い、不審な通信先への通信を迅速に検知・遮断する
- インシデント発生時の封じ込め手順、復旧手順を策定し、訓練を行う
- 利用しているWebサービスでの不正送金被害の対応窓口や補償条件、補償内容を確認する

など

ESET製品では、下記の機能によって脆弱性やマルウェア感染のリスクを軽減することが可能です。

- リアルタイムファイルシステム保護
  - ファイルシステムのイベントを監視し、マルウェアの実行を防ぎます
- エクスプロイトブロック/ネットワーク攻撃保護
  - アプリケーションやネットワークプロトコルの脆弱性をついた攻撃を防ぎます
- ボットネット保護
  - C&Cサーバーへの接続を遮断します
- Webアクセス保護/フィッシング対策機能
  - 認証情報やクレジットカード情報を窃取しようとするサイトへの接続を遮断します
- インターネットバンキング保護
  - Webブラウザーを、セキュアブラウザーとして起動します。セキュアブラウザーでは、アドオンが無効になり、キー入力内容が保護され、認証情報の漏えいを防ぎます

[38] バンキングマルウェアはばらまき型メールによって拡散されることが多いため、ばらまき型メール全般への対策を実施することで、バンキングマルウェアへの感染リスクを軽減することが期待できます。
[39] 米国国立標準技術研究所（NIST）が策定したサイバーセキュリティフレームワーク（https://www.ipa.go.jp/security/publications/nist/index.html）などを用いることができます。
[40] マルウェア情報局：2018年上半期マルウェアレポート https://eset-info.canon-its.jp/malware_info/trend/detail/180824.html

おわりに

バンキングマルウェアについては、金融機関や利用者側での対策が進んでいるため、既存手法に依存する攻撃は減少していくと考えられます。

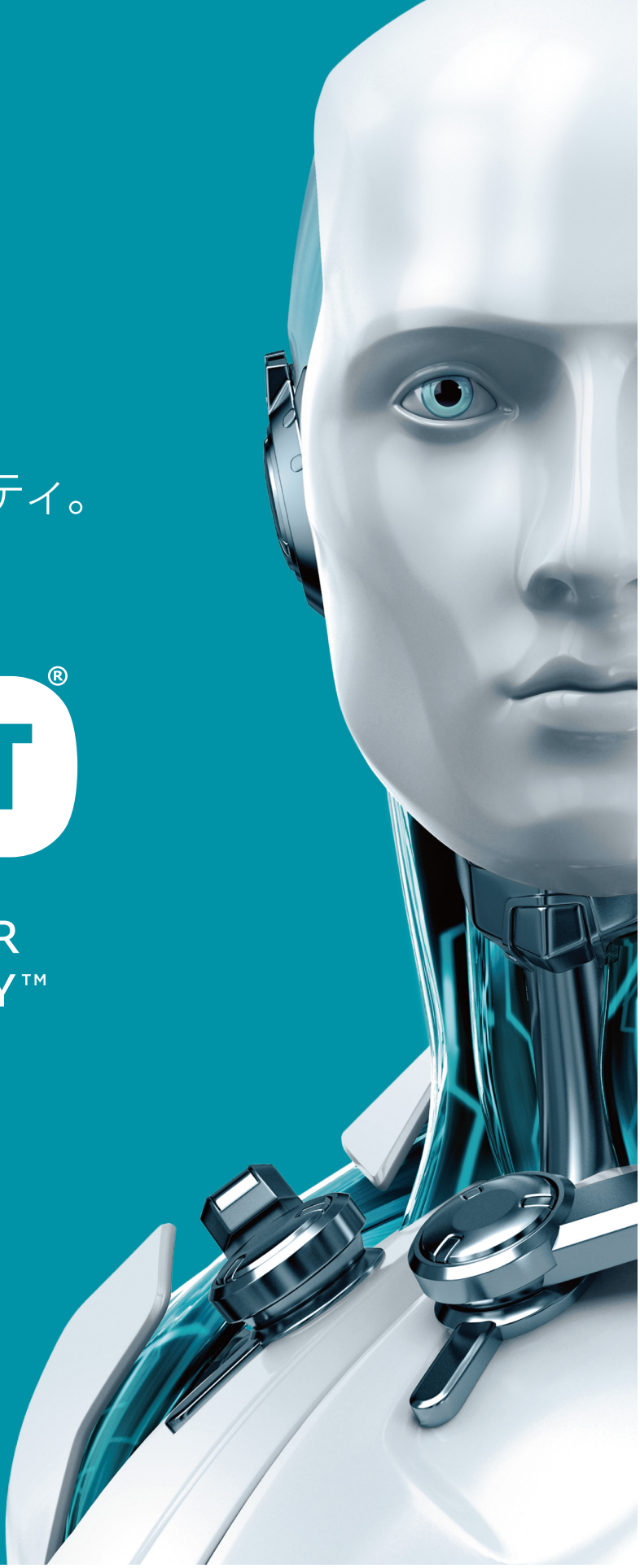
しかしながら、現在も新たな攻撃手法が観測されており、バンキングマルウェアに感染させようとする攻撃は続くとみられます。また、新たな攻撃手法やターゲットが開発されると、新たな大規模攻撃が発生する可能性があります。

常に最新の脅威情報をキャッチアップし、都度対策を講じていくことが重要です。

強くて軽い。
妥協なきセキュリティ。

ESET®

ENJOY SAFER TECHNOLOGY™



Canon キヤノンマーケティングジャパン株式会社

〒140-8526 東京都品川区東品川2-4-11 TEL. 03-6701-3475

MWJ1812CITS-PDF