

TrendLabs 2013 年間 セキュリティラウンドアップ



金銭を狙う攻撃が世界規模で拡大

総括

2013 年 日本と海外における脅威動向

2013 年は、攻撃者が金銭的利益を得るための攻撃を国内外で激化させた年と言えるでしょう。

特にオンライン銀行詐欺ツールをはじめ、偽セキュリティソフト、ワンクリック詐欺、フィッシング詐欺など、「オンライン詐欺」に分類されるサイバー犯罪の被害が顕著です。中でもオンライン銀行詐欺ツールは、世界的に猛威を振るっており、2013 年間の検出件数は、99 万 8 千件に達しました。これは 2012 の年間検出件数 49 万 8 千件の約 2 倍です。日本国内でも検出件数は 2 万 5 千件を越え、過去最大規模の金銭被害に繋がっています。また、世界全体のオンライン銀行詐欺ツール検出数に占める国内の割合は、第 1 四半期の 3% から第 4 四半期には 19% になりました。これはアメリカに次いで二番目に当たり、日本が標的となる割合が大きく増加しています。

金銭を狙う攻撃としては、ランサムウェアも世界的に猛威をふるいました。特に第 3 四半期には、PC を動作不能にすることに加えて PC 内のファイルを暗号化する「CryptLocker」の影響もあり、世界全体の検出件数が 3 万台、国内でも過去最多の 10045 台に急増しています。世界的にみると、モバイルバンキングも金銭を狙う攻撃の対象になりつつあります。アプリの偽装によるアカウント情報窃取や、中間者攻撃 (MitM) による二経路認証の侵害が確認されています。

正規 Web サイト改ざんも 2013 年、猛威をふるいました。特に日本国内では、正規 Web サイト訪問者へ不正プログラムを感染させる目的の攻撃が全体の 8 割を占めています。これは、正規 Web サイト改ざんが、不正プログラムを使ったオンライン詐欺など他の脅威に連鎖する、影響の大きい攻撃であることを示しています。

また、1 年を通じて脆弱性の利用が国内外を問わず多数見られました。正規 Web サイト改ざん攻撃においては、改ざん時にサーバ側、特に管理用ミドルウェアの脆弱性が狙われています。同時に、サイト訪問者への不正プログラム感染時には、Java や Adobe 製品などクライアント PC 側アプリケーションの脆弱性が狙われています。

その他、国内ではアカウントリスト攻撃が不正アクセス被害全体の 54% を占め、不正アクセスの被害を急増させています。不正ログインの成功率が高いことから、1 件あたりの被害規模も拡大しており、最大で 25 万件以上の ID が侵害された事例も公表されています。一方で、世界的には、「アメリカ国家安全保障局 (NSA)」における国家レベルでの個人情報の監視活動の暴露という形で、個人のデジタル情報におけるプライバシーの問題が新たな懸案として、大きな話題となりました。

目次

日本セキュリティラウンドアップ

サイバー攻撃

止まらない「正規 Web サイト改ざん」と「アカウントリスト攻撃」の台頭 5

サイバー犯罪

過去最悪の「オンライン銀行詐欺ツール」被害を筆頭に「オンライン詐欺」が猛威 14

脆弱性とエクスプロイト

日本を標的とするゼロデイ攻撃頻発、古いバージョンを狙う攻撃傾向も 21

ソーシャル & クラウドの脅威

ソーシャルメディアとクラウドサービスの攻撃インフラ化を狙う攻撃者 24

モバイルの脅威

正規マーケットの審査を潜り抜ける不正アプリ 26

グローバルセキュリティラウンドアップ

サイバー犯罪とアンダーグラウンド活動

標的から直接金銭を奪う不正プログラムの被害台数と地域が増加 30

モバイルの脅威

PC からモバイルへの移行に合わせ、モバイルの脅威は数と巧妙さが増加 38

サイバー攻撃

大規模な報道は見られずとも、攻撃の勢いは衰えず 46

脆弱性とエクスプロイト

Java 脆弱性に代表されるサポートが終了した古いソフトウェアを狙う手口が問題に 51

ソーシャル & クラウドの脅威

「ソーシャルエンジニアリング」 + 「ソーシャルメディア」 = 「金銭目的の不正活動」 56

日本セキュリティラウンドアップ

2013 年 3 大脅威 「正規 Web サイト改ざん」、 「オンライン詐欺」、「アカウントリスト攻撃」

はじめに

「日本セキュリティラウンドアップ」は、2013 年の日本国内での脅威動向を事例ベースでまとめたレポートです。

2013 年の日本国内への攻撃では、「正規 Web サイト改ざん」、「不正プログラムによるオンライン詐欺」、「アカウントリスト攻撃」の 3 大脅威が中心となっていました。

ユーザの実害という面ではオンライン詐欺の中でもオンライン銀行詐欺ツールの検出数が過去最大の 2 万 5 千件を越え、大きな金銭被害を出しています。

また Web 改ざんについてはエンドユーザへ不正プログラムを感染させる目的の事例が全体の 8 割を占めており、オンライン詐欺など他の脅威に直接つながる攻撃であることが明らかになっています。

2013 年 3 月末から顕著になったアカウントリスト攻撃による不正ログインも、大きな被害をもたらしました。最大で 25 万件以上の ID が侵害された事例も公表されており、不正ログインを狙う攻撃としてこれまで確認されていたブルートフォース攻撃や辞書攻撃では考えられなかった大きな被害規模となっています。アカウントリスト攻撃は 2013 年不正アクセス被害全体の 54% を占めており、攻撃者がその効果の高さに注目し、攻撃を仕掛けているものと思われます。

また、1 年を通じて脆弱性の利用が攻撃の背景として見られました。Web 改ざん攻撃についてはサーバ側の脆弱性、特に管理用ミドルウェアが狙われています。オンライン銀行詐欺ツールなどの感染時にはクライアント側の脆弱性として Java や Adobe が多く狙われました。また、ゼロデイ攻撃が特に日本を狙う標的型サイバー攻撃で多く確認された傾向が大きく注目されます。8 月以降世界的に主要なゼロデイ攻撃は 4 回ありましたが、そのうちの 3 回は日本に対する標的型サイバー攻撃事例を発端に明らかになっています。これは攻撃者がゼロデイ攻撃の矛先を特に日本へ向けているということであり、日本が攻撃者にとって重要な攻撃目標となっていることを示すものと言えます。

サイバー攻撃

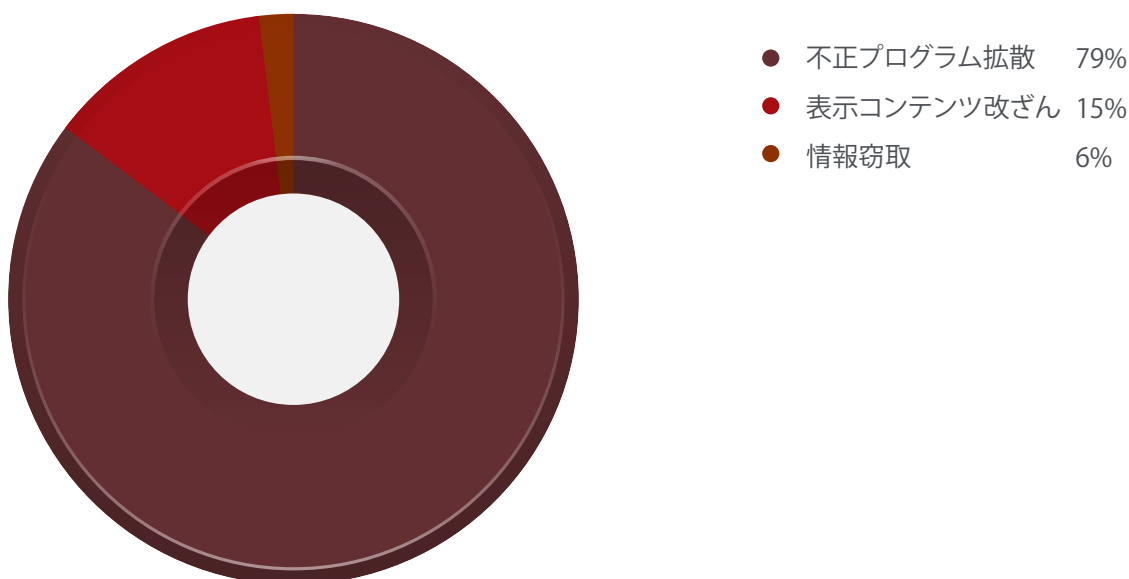
止まらない「正規 Web サイト改ざん」と「アカウントリスト攻撃」の台頭

止まらない「正規 Web サイト改ざん」：約 8 割はサイト訪問者への不正プログラム感染が目的

2013 年日本国内で最も大きな範囲に影響を与えた脅威は「正規 Web サイト改ざん (以下 Web 改ざん)」であったと言えるでしょう。トレンドマイクロでは 2013 年に何らかの形で公表された Web 改ざん被害を 71 件確認しました。IPA の報告¹でも、2013 年の Web 改ざん被害届は 75 件であり、過去に Web 改ざんが流行した 2010 年 (34 件) や前年の 2012 年 (38 件) と比べても 2 倍にのぼる数としています。また、JPCERT コーディネーションセンター (JPCERT/CC) の「インシデント報告対応レポート」²を元にした集計では、2013 年 1 年間に 7409 件の報告が寄せられており、2012 年の 1814 件と比べ約 4 倍となっています。

Web 改ざんの被害は単純に改ざんされたサイトに留まるものではありません。2013 年に被害が公表された 71 件の事例についてその攻撃内容を確認したところ、約 8 割がサイト訪問者への不正プログラム感染を最終目標とした攻撃でした。

2013 年に確認された Web 改ざん被害の攻撃内容内訳 (公表データを元にトレンドマイクロが独自に調査)



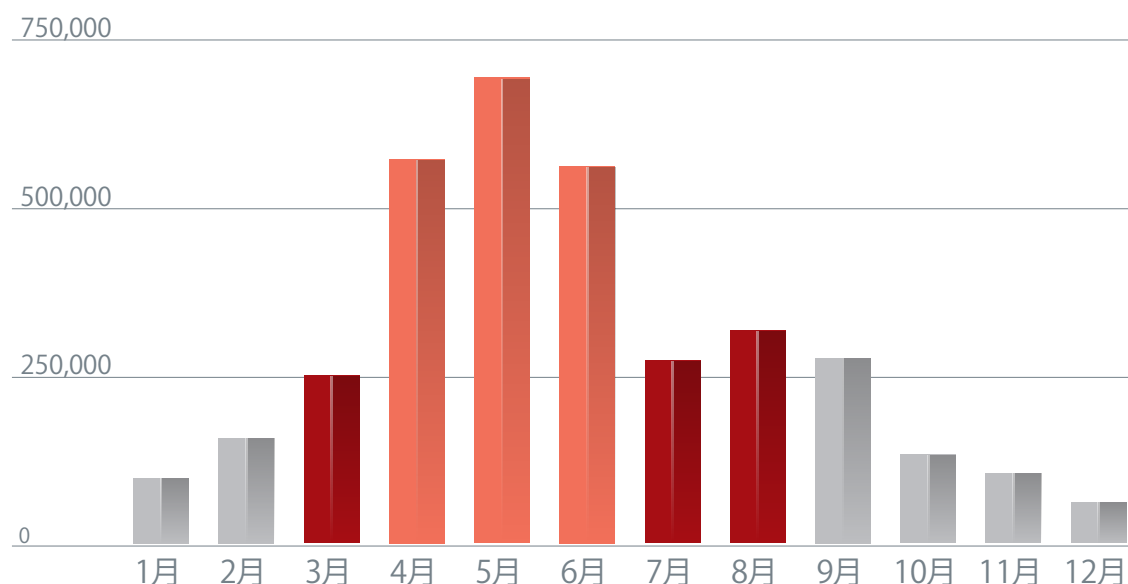
¹ <http://www.ipa.go.jp/security/txt/2014/01outline.html>

² <https://www.jpcert.or.jp/ir/report.html>

脅威連鎖の発端としての Web 改ざん

攻撃者は別の不正サイトへ誘導するためのスクリプトや iframe タグなどの仕組みを、改ざんサイトに埋め込みます。そして誘導先サイトでは主に PC ソフトの脆弱性を攻撃する細工が仕掛けられており、不正プログラムに感染させます。このような脆弱性攻撃を簡単に実現するための手段として、「エクスプロイトキット」と呼ばれる攻撃ツールの存在も確認されています。中でも、「Blackhole Exploit Kit (BHEK)」は 2013 年前半に最も多く利用された攻撃ツールであると考えられています。トレンドマイクロのクラウド型セキュリティ基盤「Trend Micro Smart Protection Network」(SPN) では、BHEK により自動生成される脆弱性攻撃 URL に対する国内ユーザのアクセス数の推移が確認できます。ピークとなった第 2 四半期の 3 か月間では 1 日平均 2 万件となる、187 万件以上の誘導がありました。7 月以降はアクセス数が減っていますが、これは対策側でも自動生成 URL の特徴を推定し、事前にクローリング調査を行うなどの対応が進んだことにより、攻撃者も自動生成 URL を使用しなくなっていったものと思われます。また、10 月以降はよりアクセス数が減少していますが、これは 10 月 9 日に BHEK 作者が逮捕³されたことが大きく関連しているものと推測されます。

BHEK が自動生成した脆弱性攻撃 URL への日本からのアクセス数推移 (SPN データによる)



このように Web 改ざんは、改ざんサイトから他の不正サイトへの誘導→脆弱性攻撃→不正プログラム感染、という脅威連鎖の発端となっており、インターネット利用者全員にとって関連する影響力の大きい脅威となっています。PC 利用者においては、「怪しいサイトにはアクセスしない」というこれまでの心掛けだけでなく、正規サイトを閲覧していても不正プログラム感染の被害に遭う危険性がある、ということを確認する必要があります。

³ <http://blog.trendmicro.co.jp/archives/8001>

新しい「情報窃取目的の Web 改ざん」も要注意

また、前述の Web 改ざん被害の内訳の中でまだ割合は 6% と少ないですが、情報窃取目的の Web 改ざんが新たに登場していることにもトレンドマイクロでは注目しています。これは主に正規 Web サイト上に不正モジュールを設置するという改ざん方法により情報を窃取することを目的とした攻撃です。窃取される情報としては、クレジットカードなどのオンライン決済情報とサイト訪問者に関する情報の 2 種が確認されています。特にクレジットカードなどのオンライン決済情報が窃取された事例⁴については、決済代行サービスへ取引を転送することで自身で決済情報を保持、保管しない Web サイトであっても、情報窃取の可能性があるという点で、これまでの Web サイトに関するセキュリティの常識を覆す攻撃方法と言えます。

Web サイト管理者は対策の再確認を

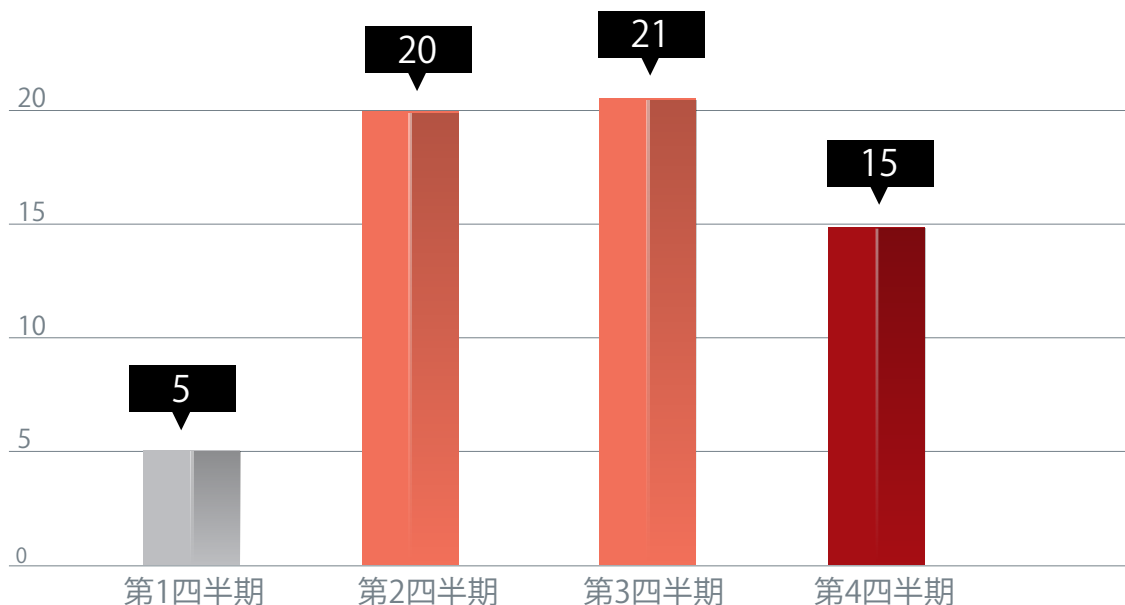
このような Web 改ざん被害については、当然、Web サイト側での対策がより重要になっています。前述のとおり、被害は自身の Web サイトに留まるものではなく、サイト訪問者にまで及びます。2013 年の日本における Web 改ざん攻撃事例では、管理アカウント情報の窃取とともにサーバ用ミドルウェアの脆弱性への攻撃が確認されています。特に脆弱性攻撃の面では、これまでのサーバ OS や Web アプリケーションに加えて、管理ツールやコンテンツ管理システム (CMS)、Web アプリフレームワークといったサーバ用ミドルウェアが狙われています。また、上述の情報窃取目的の攻撃のように Web コンテンツの改ざんは行わず、Web システム上のモジュールのみを改変することで、改ざん事実を隠ぺいする方法も確認されています。これは、脆弱性対策においても変更監視の対策においても、その対象範囲を広げる必要があることを意味しています。特に Web サイトのシステムに対する異変を早期に気づけるような監視の導入は今後必須となっていくでしょう。

「アカウントリスト攻撃」の台頭により、不正アクセス被害が急増

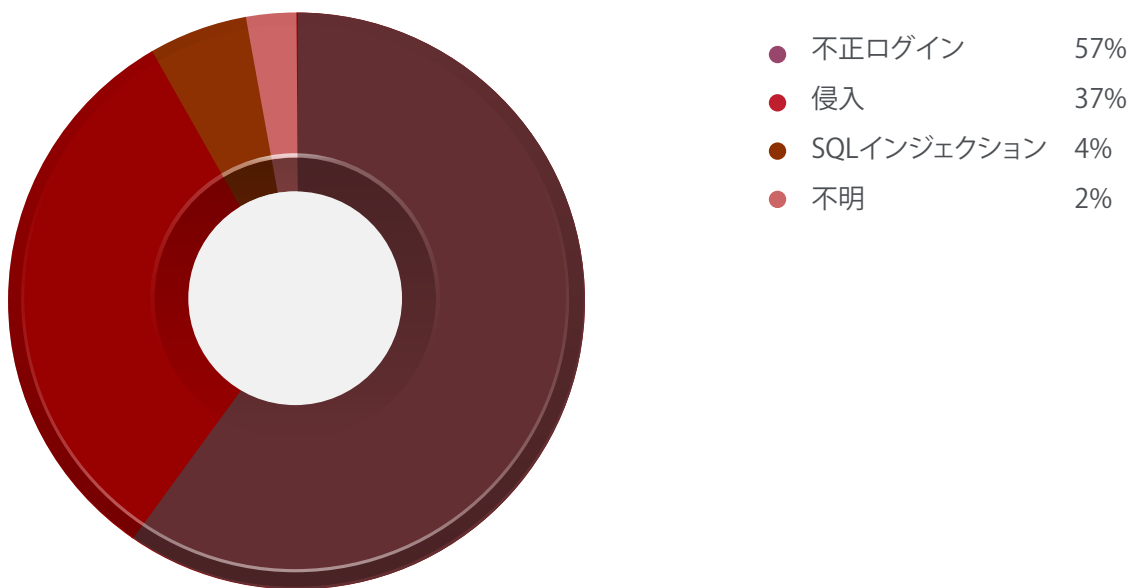
2013 年には「アカウントリスト攻撃」による不正ログインが、不正アクセス被害を急増させました。2013 年に公表された不正アクセス被害事例を見ると、不正ログインによる攻撃は、3 月下旬に初めて確認されています。その後の第 2 四半期から大幅な件数増加へとつながっており、実際、第 2 四半期以降の不正アクセス被害全体の 57% が不正ログインによるものでした。

⁴ <http://www.jins-jp.com/illegal-access/news.html>

2013 年各四半期ごとの不正アクセス被害件数推移 (公表データを元にトレンドマイクロが独自に集計)



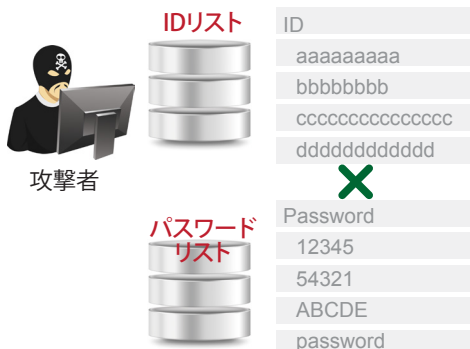
2013 年第 2 から第 4 四半期における不正アクセス被害内容の内訳 (公表データを元にトレンドマイクロが独自に集計)



アカウントリスト攻撃はあらかじめ用意されたIDとそのパスワードのリストを元に Web サイトやオンラインサービスに対して不正ログインを試行する攻撃であり、ユーザが複数サービスにおいて同一のパスワードを使いまわしている実態に付け込んだ手法です。

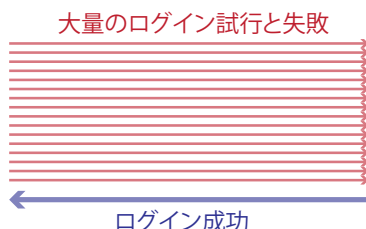
アカウントリスト攻撃概念図

ブルートフォースor辞書攻撃



1つのIDに対して、自らの用意したさまざまなパスワードをすべて試す

- ⇒ 試行回数が多く、ログイン失敗も多い
- ⇒ 非効率的な上、成功率も低い

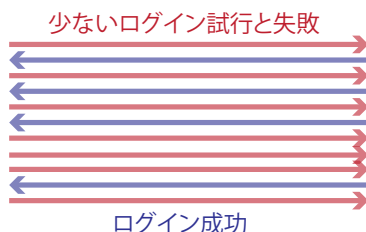


アカウントリスト攻撃



IDとパスワードがセットになったリストでログイン試行

- ⇒ 1IDあたりの試行回数は少ないが成功率は高い



その効果は非常に高く、1万件以上のアカウントに不正ログインが成功したとされている事例は33件中9件、うち10万件を超える非常に多くのアカウントが侵害されたとされる事例も2件ありました。

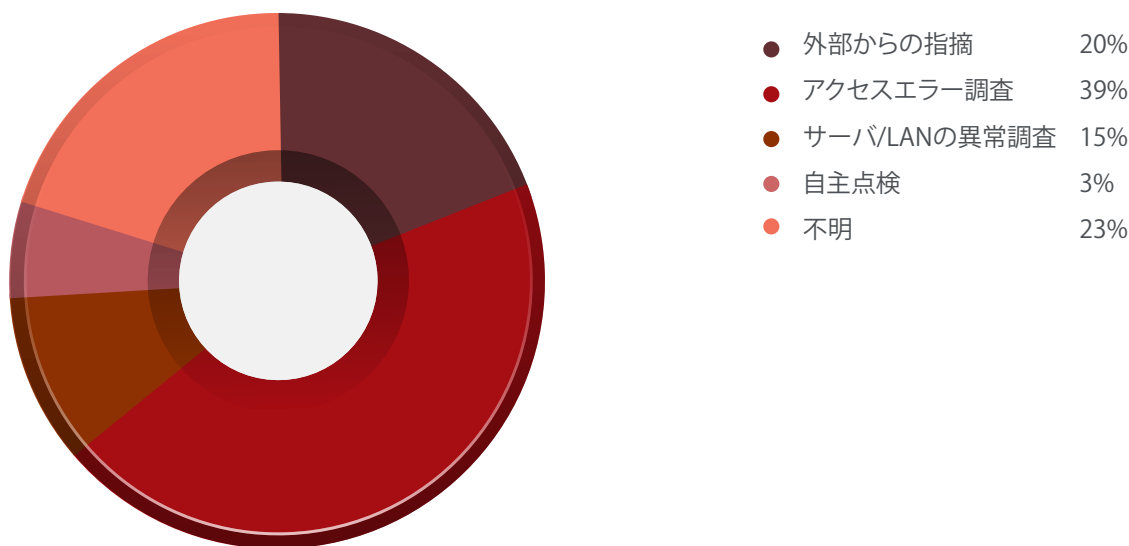
1万件以上のIDが侵害された不正アクセス事例（公表データを元にトレンドマイクロが独自に集計）

No.	不正ログイン被害ID数	被害企業業種
1	243,266	サービス業
2	150,165	小売業
3	83,961	情報通信業
4	39,590	情報通信業
5	35,252	情報通信業
6	28,452	サービス
7	28,000	人材総合サービス事業
8	23,926	サービス業
9	15,000	通信販売

このように大きな被害に繋がっているアカウントリスト攻撃ですが、決して新しい攻撃手法ではありません。オンラインゲーム業界では 2010 年後半から確認されていた手法です。攻撃者は常に成功しやすい攻撃方法を求めています。アカウントリスト攻撃の台頭は、限定した範囲に対して行われていた攻撃方法が、何らかのきっかけでより広い範囲への攻撃に利用されていく傾向をはっきり示した事例と言えます。

また、この 2013 年の不正アクセス被害の詳細からは、オンラインサービスの管理 / 運営者がどのような対策を施すべきであるかを教訓として学ぶことができます。被害が発覚した原因のうち、外部からの異常なアクセスに対する調査が 39%、内部のサーバやネットワークの異常に対する調査が 15% となっています。つまり、不正アクセス事例の 7 割以上で、何らかの異常がきっかけで調査を行った結果、結果的にサイバー攻撃の被害に遭っていたということが判明しています。このデータから、不正アクセスの発生に気付くためにはネットワーク内外の監視から異常をいち早く可視化する対応が必要ということがわかります。しかし、これは大きな異常がなければ気付けなかったということもでき、外部からの指摘で気づいた事例も 20% となっています。監視体制と同時に、平常時の継続した監視結果から定期的に異常の兆候を精査する体制や、迅速に異常の発生に対応できる体制を構築しておくことも重要です。

2013 年不正アクセス被害発見理由の内訳（公表データを元にトレンドマイクロが独自に集計）



Deep Web の悪用が顕在化：Tor ボット「Mevade」が日本でも被害

2012 年のなりすまし犯罪予告事件⁵以来、日本でも匿名ネットワーク「Tor」の存在が一般に知られるようになりました。トレンドマイクロでは、Tor ネットワークに代表される「Deep Web」のサイバー犯罪利用についてリサーチを進めており、特に闇市場での利用について詳細なレポート⁶も発表しています。

Deep Web とは、インターネット上にありながら通常の方法ではアクセスが困難なサイトの総称です。その Deep Web を悪用する不正プログラムが、2013 年 9 月に初めて確認されました⁷。「Mevade」と呼ばれるボットが一斉に Tor ネットワーク内に設置された C&C サーバとの通信を行ったことにより、Tor ネットワークへの通信が急増する事態になりました。この初の Tor ボットである「Mevade」については、日本でも大きな感染被害が確認されました。SPN で収集された情報を確認したところによると、9 月 9 日時点での「BKDR_MEVADE.C」の全世界での検出回数において、日本からの検出が 52% と最も多かったことが確認されています。⁸結果的に「Mevade」は第 3 四半期に日本リージョナルトレンドラボ（RTL）が最も多くの感染被害報告を受けた不正プログラムとなりました。また、9 月中にトレンドマイクロで確認した日本における「Mevade」とそのダウンロードの検出回数は 6723 件となり、その被害規模を証明しています。

現在すでに「Mevade」による当初の被害は沈静化しています。しかし、同様に Tor ネットワークを悪用する不正プログラムは今後も登場する懸念があります。今後の企業でのセキュリティ対策を考える上においては、自社ネットワークからの Tor 通信の発生を監視対象として考慮に入れるべきでしょう。

非 Windows、非 PC への攻撃傾向

2013 年にはこれまで中心的な攻撃対象となっていた Windows OS を使用する PC 以外への攻撃が、日本国内でも広がっていることが確認される事例がありました。非 Windows への攻撃としては RPM 系 Linux を狙うバックドア「SSHD ROOTKIT」（トレンドマイクロ検出名：「ELF_SSHDOOR.BJ」）の拡散が確認されました⁹。また、特にシェアの大きい Linux 上の Web サーバ「Apache」を狙う「Darkleech Apache Module」（トレンドマイクロ検出名：「ELF_CHAPRO」）は、2013 年を通じて大きな被害に繋がった Web 改ざん攻撃の先鞭となりました¹⁰。また非 PC への攻撃として、インターネット接続されている複合機や NAS、Web カメラ、などの悪用が警告され、実際に社内使用されているプリンタへの DoS 的な攻撃も確認されています¹¹。

このような非 Windows、非 PC への攻撃は今後来る「IOE（Internet Of Everything）」の時代に向け、新たな攻撃可能性を示すものと言えます。

⁵ <http://blog.trendmicro.co.jp/archives/6098>

⁶ <http://blog.trendmicro.co.jp/archives/7960>

⁷ <http://blog.trendmicro.co.jp/archives/7796>

⁸ <http://blog.trendmicro.co.jp/archives/7806>

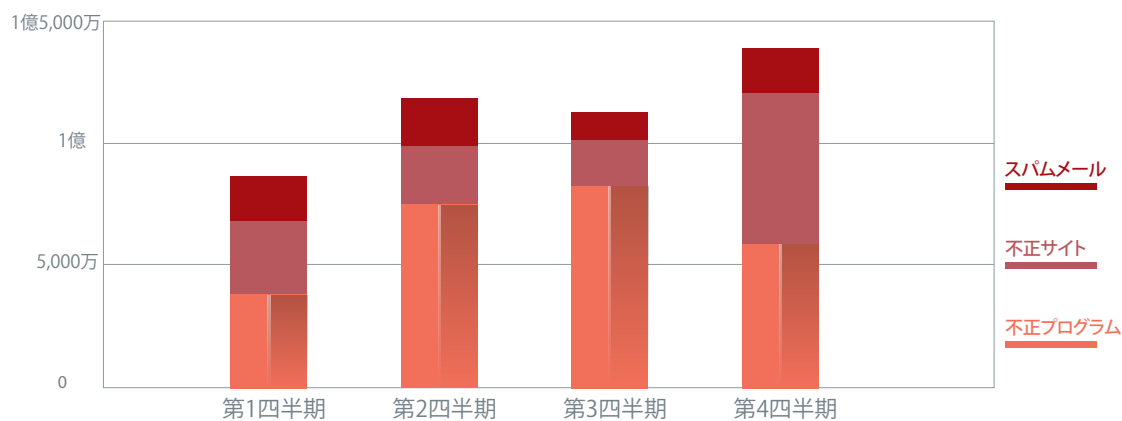
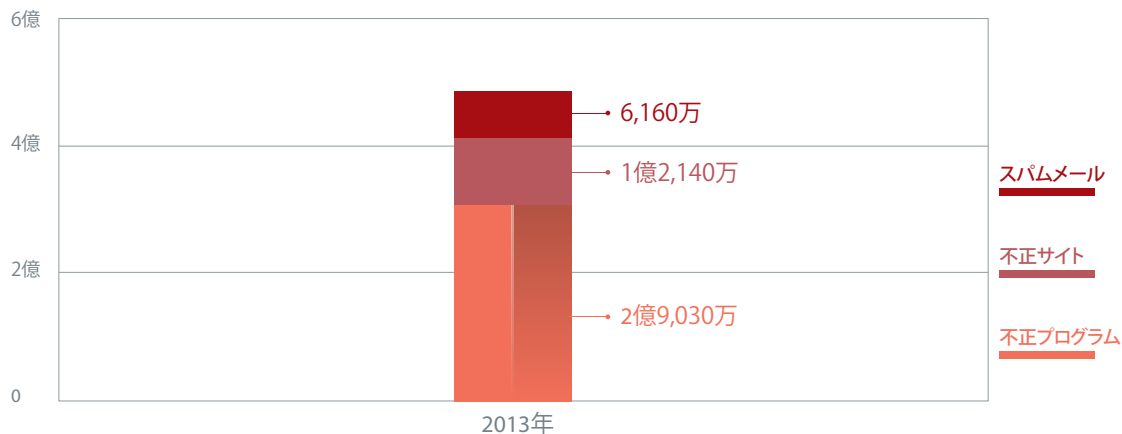
⁹ <http://blog.trendmicro.co.jp/archives/6759>

¹⁰ <http://blog.trendmicro.co.jp/archives/6888>

¹¹ <http://itpro.nikkeibp.co.jp/article/COLUMN/20131118/518594/>

トレンドマイクロのクラウド型セキュリティ基盤「Trend Micro Smart Protection Network (SPN)」による統計データ

2013 年 1 年間に日本国内で防御された脅威件数



2013 年の 1 年間にトレンドマイクロでは日本国内だけでおよそ 4 億 7300 万件の脅威をブロックしました。1 日平均ではおよそ 130 万件、また 1 秒あたり 15 件の脅威からユーザを防護したことになります。また、四半期毎の比較では、第 4 四半期が最大となり、脅威が拡大傾向にあることがわかります。

2013 年 日本国内で検出された不正プログラム Top3

不正プログラム	数
ADW_BHO	319,183
ADW_BPROTECT	167,032
ADW_OPENCANDY	141,835

不正プログラム	数
大企業	
WORM_DOWNAD.AD	54,908
ADW_OPENCANDY	41,296
ADW_BPROTECT	31,705
中小・中堅企業	
ADW_BPROTECT	15,054
WORM_DOWNAD.AD	11,807
ADW_OPENCANDY	11,547
個人ユーザ	
BKDR_BIFROSE.BMC	189,797
ADW_OPENCANDY	136,627
ADW_BHO	98,005

2013 年 1 年を通じて日本で検出報告の最も多かった不正プログラムは「ADW_BHO」でした。これまでもアドウェアの検出が多く確認されてきましたが、TOP3 すべてがアドウェアで占められたのは初めてです。この傾向は第 2 四半期から続いており、攻撃者がアドウェアによる広告表示を収入源の一つとみなし、攻撃に使用していることが推測されます。企業ユーザにおいては 2008 年に登場した「WORM_DOWNAD.AD」が 5 年を経てもトップの検出報告となっています。これは全世界的な傾向¹²であり、古い脆弱性がまだ企業内には残っていること、企業では USB メディアの管理徹底は難しいことを示していると言えます。

¹² <http://blog.trendmicro.co.jp/archives/8246>

サイバー犯罪

過去最悪の「オンライン銀行詐欺ツール」 被害を筆頭に「オンライン詐欺」が猛威

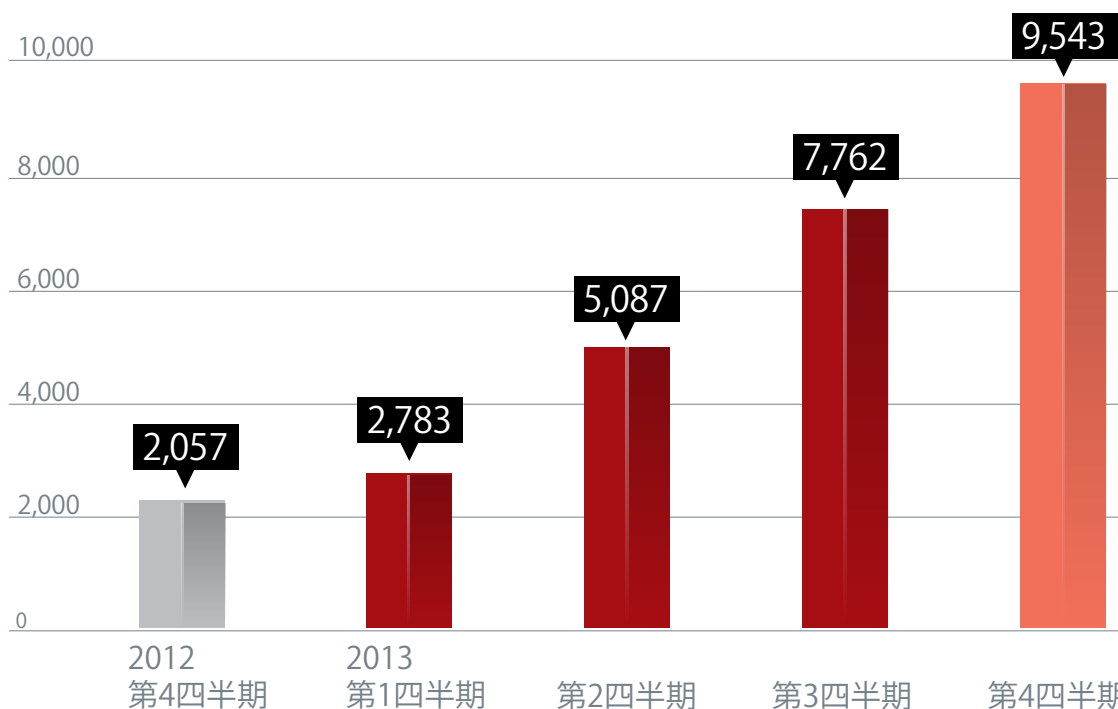
本格上陸した「オンライン銀行詐欺ツール」が過去最悪の被害

2013 年日本の PC 利用者に最も大きな被害をもたらした脅威は、不正プログラムを利用した「オンライン詐欺」と言えるでしょう。中でも「オンライン銀行詐欺ツール」が脅威の中心となりました。2012 年 10 月末に日本の銀行を狙うオンライン銀行詐欺ツールの攻撃が確認¹³されて以来、被害は拡大の一途を辿っています。特に「Web インジェクション」もしくは「Man in the Middle (MitM)」、「Man in the Browser (MitB)」などと呼ばれる攻撃手法が日本の銀行向けにカスタマイズされ本格上陸したことが急激な被害の増加の背景であると考えられます。Web インジェクションとは、特定の銀行サイトの表示に合わせて認証情報の入力を促す偽画面を表示する攻撃手法です。正規 Web サイト表示の上に偽画面が表示されるため、利用者が騙されやすい攻撃手法となっています。

トレンドマイクロのクラウド型セキュリティ基盤「Trend Micro Smart Protection Network」(SPN) による集計でも、日本で特に被害の多いオンライン銀行詐欺ツール「ZBOT」の検出数は 2013 年を通じて増加し続け、2013 年第 4 四半期では前年同期比 4.6 倍の 9543 台となり過去最悪の被害となりました。年間を通じてみても、2012 年の 7375 件に対し、2013 年は 25,175 件と前年比 3.4 倍の増加となっています。

¹³ <http://blog.trendmicro.co.jp/archives/6187>

代表的なオンライン銀行詐欺ツール ZBOT ファミリーの日本における検出台数推移 (トレンドマイクロ SPN による)



2012 年から増加を続け、2013 年第 4 四半期には前年同期比 4.6 倍に

また、警察庁の発表でも、オンライン銀行に関する 2013 年の不正送金被害金額は 14 億 600 万円とされています¹⁴。これは過去最多だった 2011 年の被害 3 億円と比べても約 4.7 倍となり、実際の金銭的被害という面からも過去最悪となっています。

このような被害拡大の背景には、海外のサイバー犯罪組織の活動があります。日本を標的とした活動を示す例として、これまで海外で確認されていた「Web インジェクション」という攻撃手法が国内に入ってきたことに加え、第 2 四半期以降には窃取した銀行口座情報を元に現金を引き出すいわゆる「出し子」が海外の組織から指示を受けていた事例¹⁵が、第 3 四半期以降には「マネーミュール」と呼ばれる不正送金の実行役を「求人」する日本語スパムメール事例¹⁶が確認されています。警察庁の発表によれば、日本国内のインターネット利用者がこのようなスパムメールをきっかけに犯罪行為と知らずに海外への不正送金に加担してしまった事例が 2013 年 11 月時点で 149 人も確認されています¹⁷。これは、日本を狙うサイバー犯罪組織の動きが現実であることの裏付けと言えます。

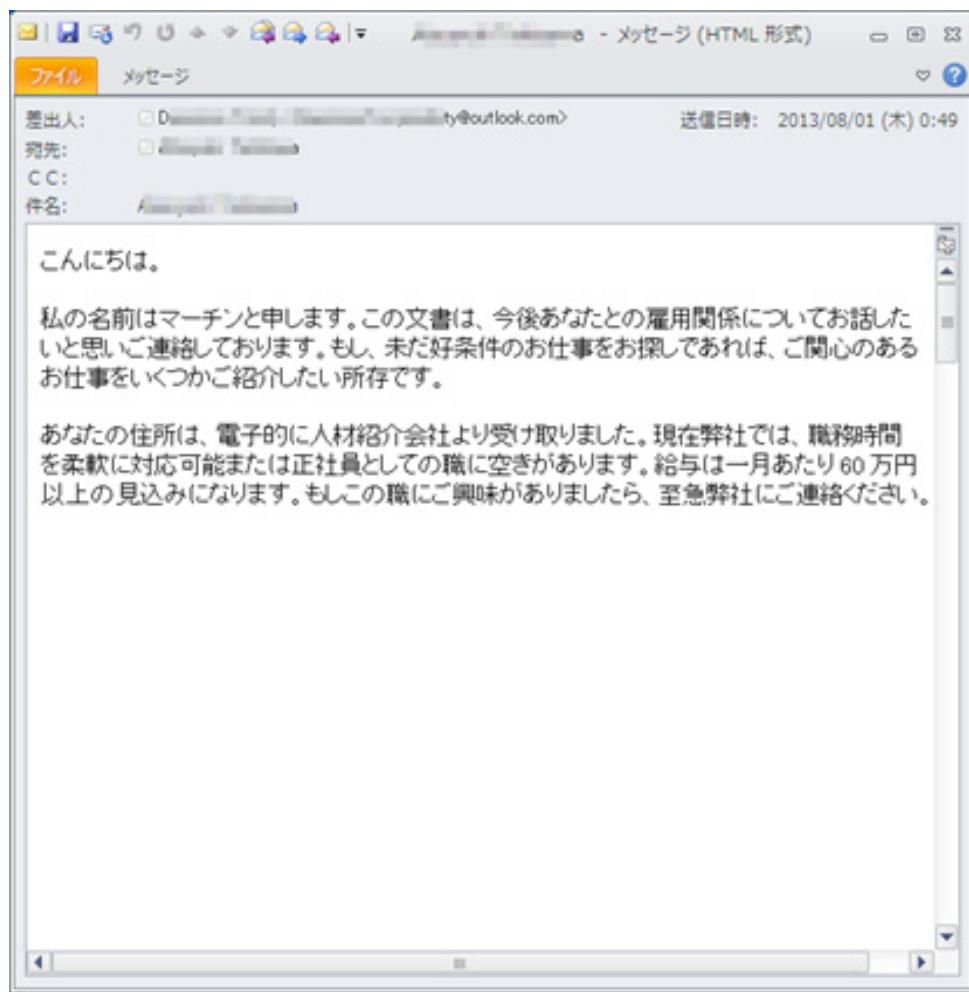
¹⁴ http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf

¹⁵ <http://www.47news.jp/CN/201307/CN2013070901002106.html>

¹⁶ <http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku430.htm>

¹⁷ <http://sp.mainichi.jp/m/news.html?cid=20131213k0000e040183000c>

マネーミュール求人を目的とした日本語スパムメール例



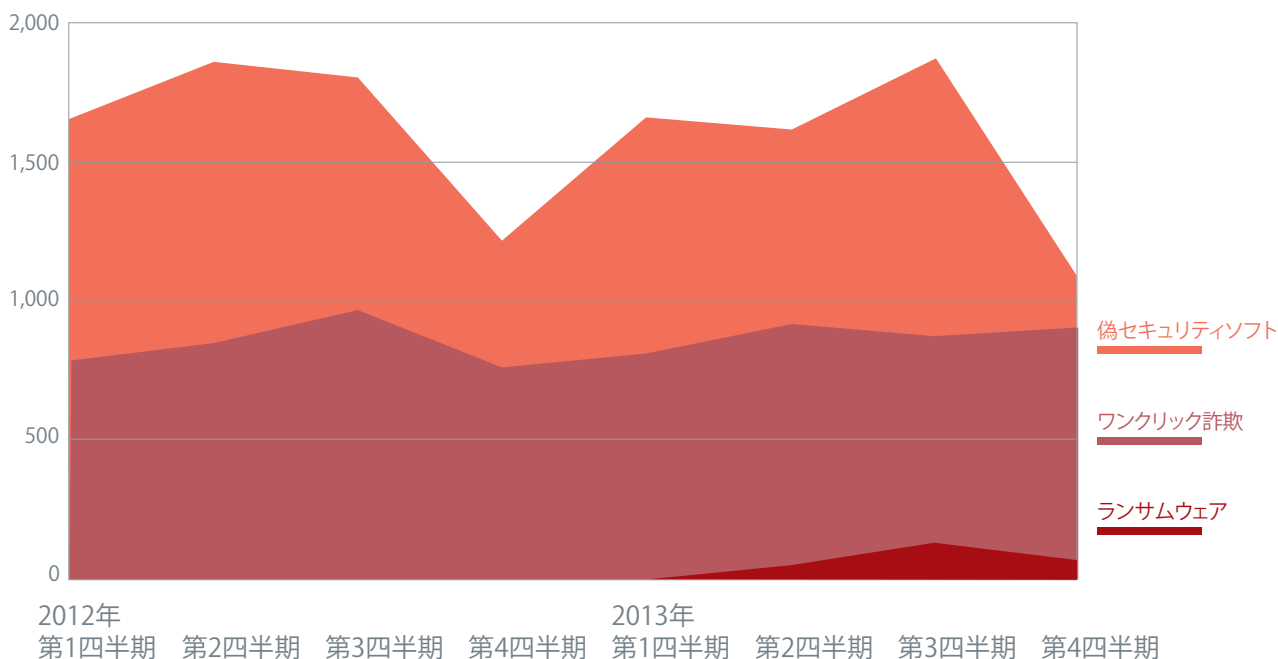
また、世界的に見ても日本の感染被害の割合が急増しています。全世界のオンライン詐欺ツール検出台数で日本が占める割合は、2013年第1四半期には3%でしたが、第4四半期には19%と全体の2割近くに達しました。これは米国の22%に次ぐ第2位であり、世界的に日本がオンライン銀行詐欺ツールの標的となっていることを示していると言えます。

実社会において「振り込め詐欺」の被害が止まないように、サイバー空間におけるオンライン銀行利用者を狙った詐欺ツールの攻撃も拡大が予想されます。被害に遭わないためにも、また、自身が犯罪に加担するような行為に巻き込まれないためにも、その手口をよく理解することが重要です。例えば、いつもと違う情報入力画面が表示される、など、不審なWeb表示や電子メールに遭遇した場合には、必ず金融機関への確認を行ってください。

既存の「ワンクリックウェア」、「偽セキュリティソフト」被害に加え 「ランサムウェア」も日本へ流入開始

不正プログラムによる「オンライン詐欺」脅威として以前から確認されている「ワンクリックウェア」、「偽セキュリティソフト」の被害も継続しています。日本トレンドマイクロサポートセンターへの問い合わせ統計では2012年、2013年と3000件前後の感染報告数が継続していることがわかります。

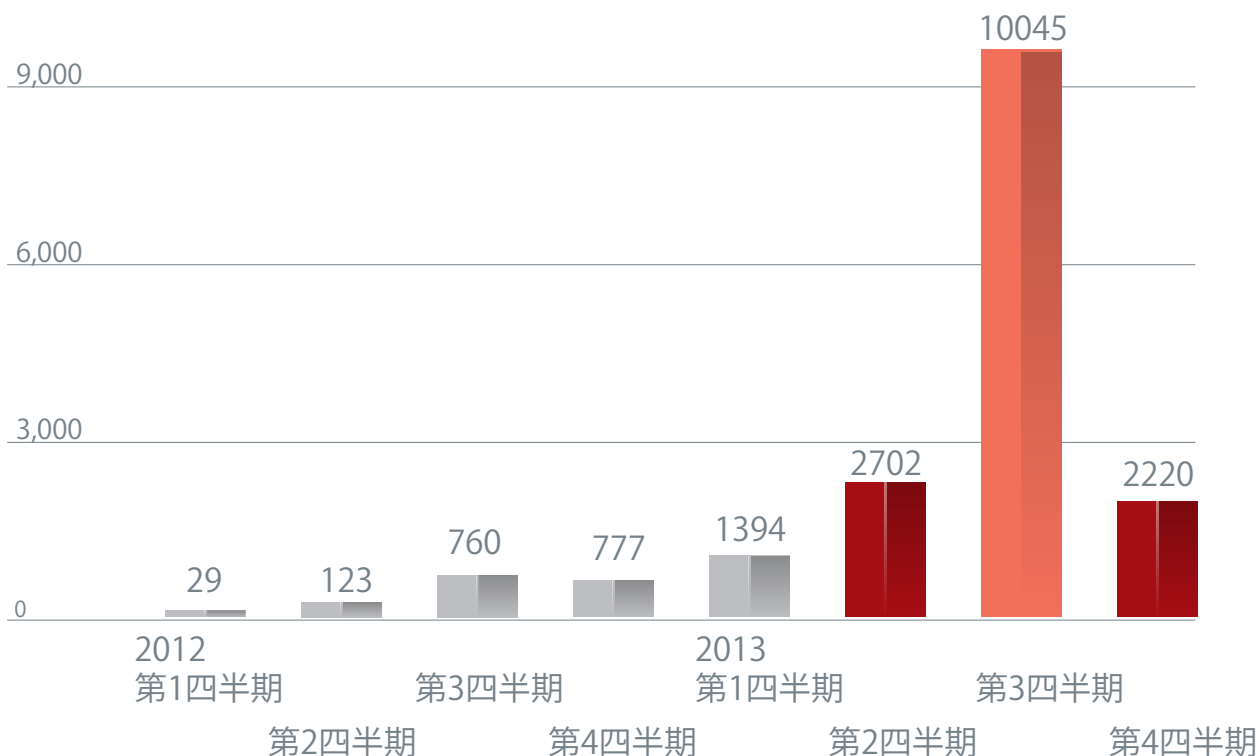
トレンドマイクロコンシューマサポートセンターに入った偽セキュリティソフト、ワンクリックウェア、ランサムウェア関連の感染報告数



2012年から2013年の比較では、偽セキュリティソフト：2990件から2834件、ワンクリックウェア：3460件から3243件

これに加え、2012年にはは感染報告が無かったランサムウェアについても5月以降に日本国内での感染報告が入っていることが確認されています。トレンドマイクロSPNによる日本でのランサムウェア検出台数でも、2013年第3四半期には過去最多の10045台の検出が確認されています。

日本でのランサムウェア検出件数推移 (トレンドマイクロ SPN による)



減少したように見える 2013 年第 4 四半期でも前年同期比では 3 倍以上の検出数

この検出件数データからもランサムウェア被害が日本へ流入していることは明らかですが、まだ日本語表示に対応したものは確認されていません。現時点では特に日本ユーザを狙ったものではないものと考えられる状況ですが、今後は日本語化され、実際の金銭被害に繋がっていくことが懸念されます。

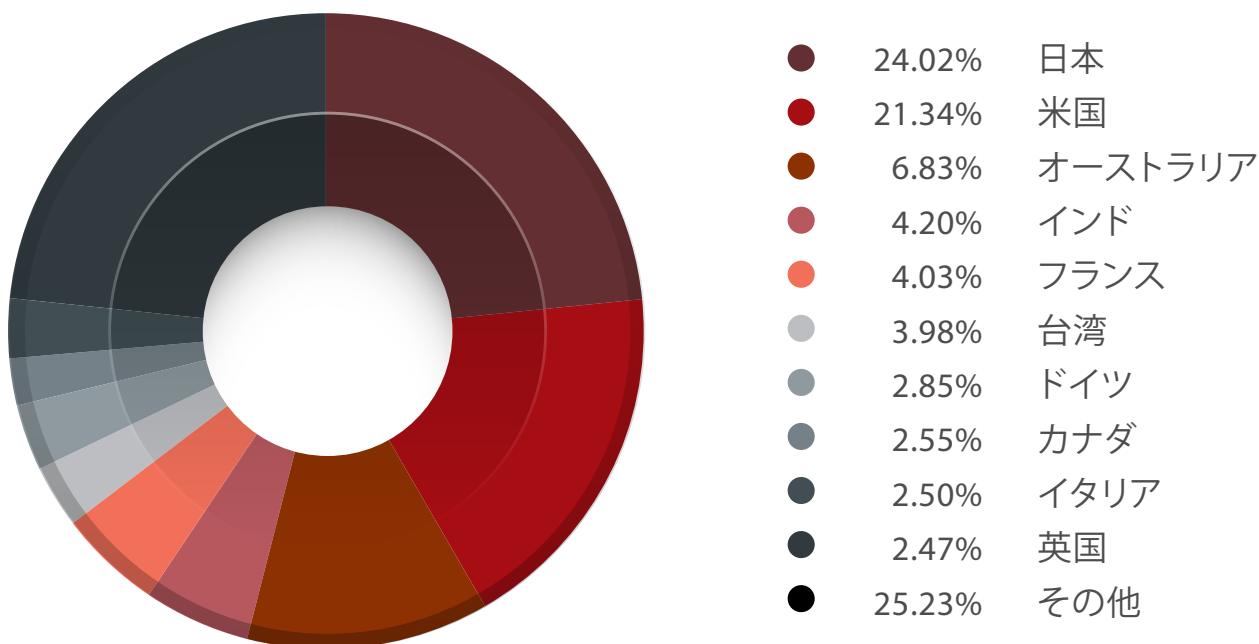
被害に遭わないためには、不正プログラムによるオンライン詐欺全体の動向に注意し最新の攻撃事例を理解することによって「騙されないための知識」を持つことが必要でしょう。

日米を中心にビットコイン発掘不正プログラムの被害を確認

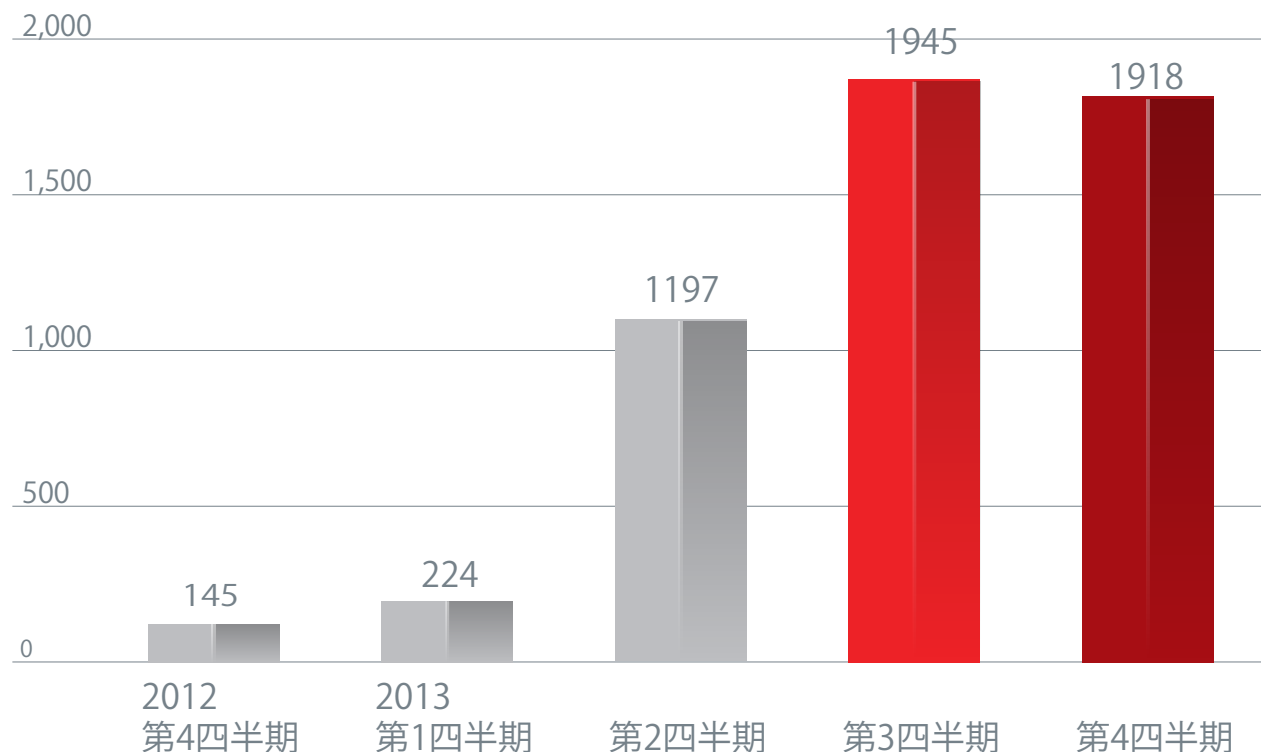
「ビットコイン」は 2009 年ころから運用が開始されている仮想通貨です。中央銀行にあたる存在を持たず取引の匿名性が高いことなどから、ハッカーやアンダーグラウンド市場が好んで使用する仮想通貨としても知られていました。一般的には、対 \$ の取引価格が一時 1200\$ を越える最高値をつけるなどのニュースによって、この 2013 年から特に注目が集まっています。

このビットコインについて、攻撃者はビットコインを入手するための「発掘（マイニング）」という仕組みを狙っていることがわかっています。侵入した感染端末でビットコインの「発掘」を行う「ビットコイン発掘不正プログラム」の存在は 2010 年ころから確認されています。このビットコイン発掘不正プログラムの被害が、世界でも特に日本とアメリカで発生していることが 2013 年第 4 四半期に確認されました。トレンドマイクロ SPN の統計データによれば、2013 年 9～11 月の期間におけるビットコイン発掘不正プログラムの検出数は全世界で 1 万 2 千台以上と確認されています。この検出数の国別割合では、日本が 24.02%、アメリカが 21.34%と、この 2 か国のみで全体の 45%以上を占めており、世界的に見て日本からの被害が大きいことが確認されました。

2013 年 9～11 月における全世界でのビットコイン発掘不正プログラムの国別検出数割合（トレンドマイクロ SPN による）



日本におけるビットコイン発掘不正プログラムの検出回数推移（トレンドマイクロ SPN による）



また、日本におけるビットコイン発掘不正プログラム検出回数推移からは、2013 年第 2 四半期から検出回数が急増していることもわかりました。2013 年 1 年間の検出回数では 5284 台となり、前年比 4.1 倍の増加となっています。この急増の背景としては、ビットコイン取引価格の高騰にによって攻撃者のビットコインに対する関心が高まったことが推測されます。

ビットコイン発掘不正プログラムは感染ユーザから直接ビットコインを窃取するものではありません。感染 PC 上でビットコイン発掘を行うためのマシンリソースの盗用がユーザの被害と言えます。裏を返せば、ビットコイン利用の有無に限らずすべてのユーザが攻撃対象になる可能性があるということです。また、日本での被害が多い理由については、ビットコインの発掘には大きなマシンリソースが必要となるため、比較的高スペックの PC が使用されている可能性の高い国が狙われているのではないかと推測されます。感染割合の上位 10 か国は、ほぼすべて先進国とされる国であることも、その裏付けと言えるでしょう。

ただし、利益を得るためのビットコインの発掘に関しては、専用ハードウェアの開発なども行われているのが現状であり、既にユーザ環境への感染によるリソース盗用程度では十分な利益は得られないものと、トレンドマイクロでは見ています。今後、ビットコインを狙った攻撃はオンライン銀行詐欺ツールのように利用者のビットコイン口座（ウォレット）の情報窃取や不正操作を狙ったものへと移行していくものと予想されます。

脆弱性とエクスプロイト

日本を標的とするゼロデイ攻撃頻発、古いバージョンを狙う攻撃傾向も

ゼロデイ攻撃頻発：日本への標的型サイバー攻撃を 8 月以降だけで 4 件確認

2013 年は世界的に見てもゼロデイ攻撃が頻発しましたが、8 月以降、特に日本を狙った標的型サイバー攻撃にてゼロデイ脆弱性が利用されたことが明らかになっています。2 月に発覚した「一太郎」へのゼロデイ攻撃を皮切りに、日本を標的としたゼロデイ攻撃としては 6 件が確認されましたが、そのうち 4 件は 8 月以降に集中しました。

具体例として、9 月には日本国内サイトの改ざんによる水飲み場攻撃において、Internet Explorer のゼロデイ脆弱性¹⁸を利用する攻撃は 8 月中に発生していたことが、発覚しました。これ以降、11 月には Microsoft Office と Windows XP のゼロデイ脆弱性^{19,20}の利用も確認されました。その他、11 月には 1 年で 3 回目となった「一太郎」へのゼロデイ攻撃²¹が 9 月中に発生していたことも発覚しています。

このように日本への標的型サイバー攻撃での利用を発端として多くのゼロデイ脆弱性が確認されたことは特筆すべき傾向です。標的型サイバー攻撃の攻撃者にとって、日本が重要なターゲットのひとつとなっていることがうかがえます。また、これらの日本を標的としたゼロデイ脆弱性の事例では、すべてのにおいて攻撃の確認から修正プログラムの公開まで 1 か月以上が経過しています。サポート終了のため未修正のままの Java6 への攻撃を除いた 11 件の平均でも、修正プログラムが利用できないいわゆる「ゼロデイ期間」は 1 か月となっています。ゼロデイ攻撃については、基本的に事前の対策方法がありません。攻撃の到来をいち早く気付ける監視体制と、脆弱性攻撃の確認から修正プログラム公開までのゼロデイ期間における脆弱性防御の代替策導入が重要となっていくでしょう。

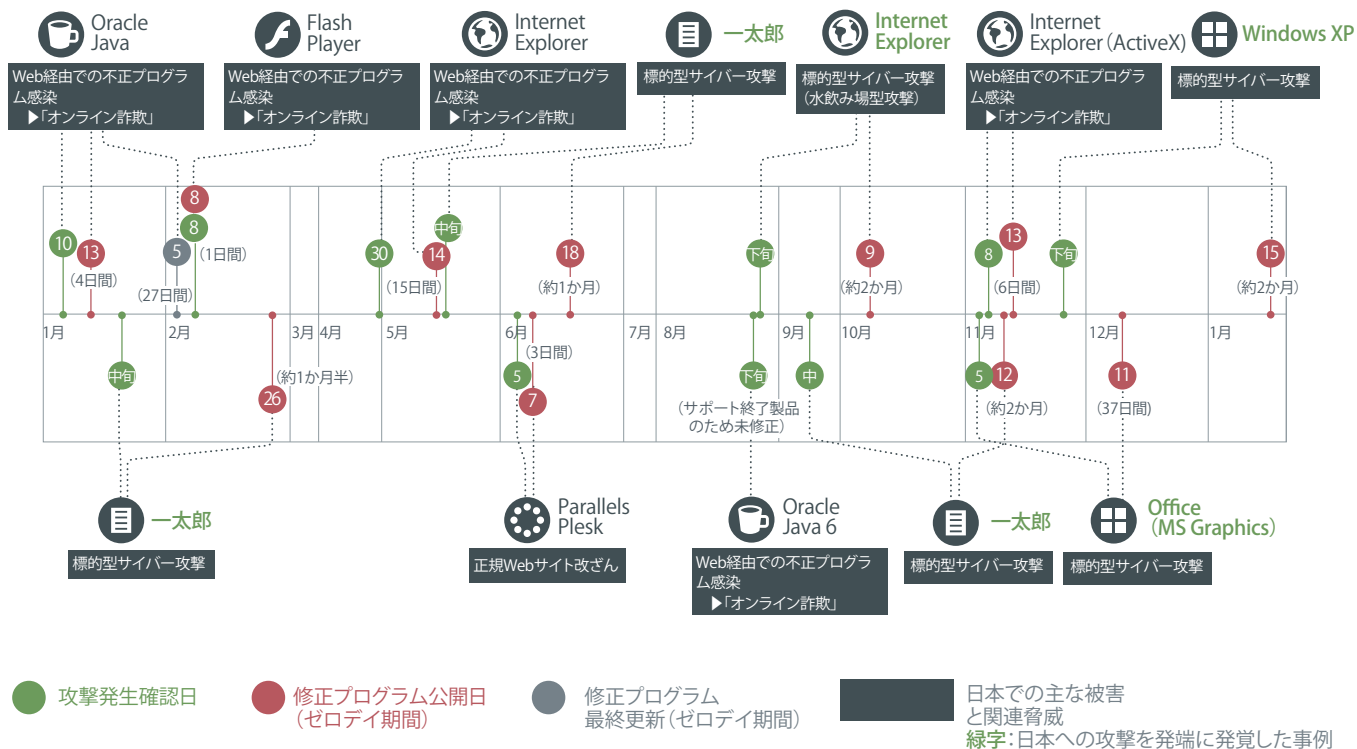
¹⁸ <https://technet.microsoft.com/ja-jp/security/bulletin/ms13-080>

¹⁹ <https://technet.microsoft.com/ja-jp/security/bulletin/ms13-096>

²⁰ <https://technet.microsoft.com/ja-jp/security/bulletin/ms14-002>

²¹ <http://www.justsystems.com/jp/info/js13003.html>

2013 年に確認された主なゼロデイ攻撃リスト (トレンドマイクロ調べ)



古いバージョンのソフトウェアに対する新たな脆弱性攻撃

2013 年には、古いバージョンのソフトウェアに対する攻撃も顕著になってきました。攻撃者は過去に確認されすでに修正プログラムが公開されている脆弱性であっても、攻撃を続けます。2013 年にはそれに加え、過去のバージョンのみに影響する脆弱性やその攻撃方法 (エクスプロイト) が新たに確認され攻撃される例も明らかになっています。

代表例として Java バージョン 6 (Java 6) への攻撃があります。近年の Web 改ざん攻撃においては、サイト訪問者へ不正プログラムを感染させるための攻撃手段として、Adobe 製品と並び Java の脆弱性への攻撃が継続して確認されています。Java の最新バージョンは既に Java 7 へ移行しており、Java 6 のサポートは 2 月で終了し、実際に 6 月以降に確認された脆弱性に関してはアップデートが行われていません。この状況下において、8 月にも新たに Java 6 に影響する脆弱性へのエクスプロイトが確認され、攻撃が発生しました²²。この攻撃が確認された 8 月の時点で最新の Java 7 の使用率は全体の 19% のみとされており²³、多くのユーザが脆弱性の影響する古いバージョンを使用していました。その他、Internet Explorer や Parallels Presk などの古いバージョンのみを対象とした脆弱性攻撃も確認²⁴されています。

22 <http://blog.trendmicro.co.jp/archives/7773>

23 <http://community.websense.com/blogs/securitylabs/archive/2013/09/05/new-java-and-flash-research-shows-a-dangerous-update-gap.aspx>

24 <http://blog.trendmicro.co.jp/archives/7385>

サポートが終了しアップデートが行われなくなったソフトウェアは、ゼロデイの状況がずっと継続されているのと同様です。また、古いソフトウェアほどそもそも脆弱性攻撃に弱い構造となっている可能性が高いことも注意点です。例えば、マイクロソフトでは最新の Internet Explorer 10 では SEHOP (Structured Exception Handling Overwrite Protection)、ASLR(Address Space Layout Randomization)、ヒープの強化など、Internet Explorer 8 に含まれていない脆弱性対策が当初から盛り込まれているとしています。

攻撃者にとって、古いバージョンの利用者がいる限り、価値のある攻撃対象となり続けます。2014 年 4 月には、まだ多くの利用者が残っている Windows XP および Office2003 のサポート終了が控えており、攻撃者が積極的に攻撃を行ってくるであろうことが予測されます。

Web 改ざんからの脅威連鎖の背景に脆弱性

攻撃者は正規 Web サイト改ざんを中心とする脅威連鎖においても脆弱性を利用しています。Web 改ざん時には特にサーバ上のミドルウェアの脆弱性が狙われていることが 2013 年を通じて確認されました。特に日本では CMS(コンテンツ管理システム)の「WordPress」と「Joomla!」、また Web アプリフレームワークである「Apache Struts」への攻撃が顕著でした。

また、改ざんサイトからの誘導先となる不正サイトでは、サイト訪問者が使用するクライアント PC に存在する脆弱性を攻撃することで、不正プログラムを感染させます。クライアント側の脆弱性では Java、Adobe Reader、Adobe Acrobat などのような、インターネット上で広く使用されている技術への攻撃が顕著です。この背景には、「Blackhole Exploit Kit (BHEK)」のようなエクスプロイトキット (脆弱性攻撃ツール) を使用することにより、攻撃者が容易に脆弱性への攻撃環境を構築できる実態があります。

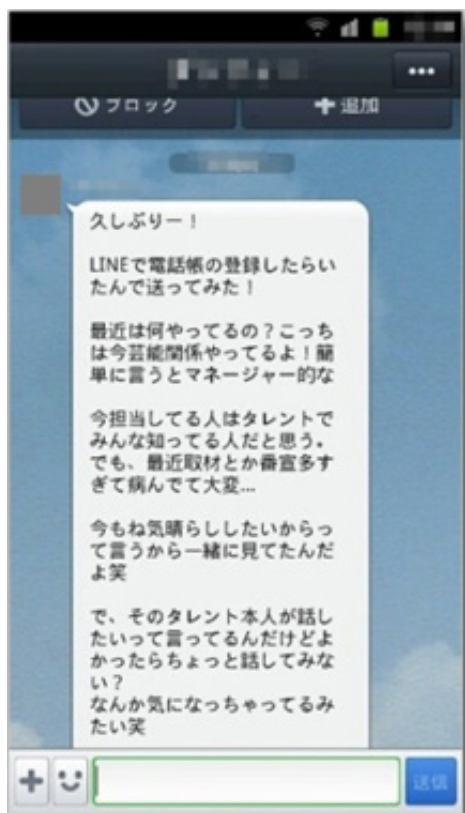
ソーシャル & クラウドの脅威

ソーシャルメディアとクラウドサービスの攻撃インフラ化を狙う攻撃者

ソーシャルメディア上での脅威への誘導と不正プログラムによるクラウドサービス利用

ソーシャルメディアやクラウドサービスを、「新しい攻撃インフラ」として利用しようとする攻撃者の活動が、2013年を通じて確認されています。ソーシャルメディアの具体的な攻撃事例としてトレンドマイクロでは、「LINE」のメッセージからサクラサイトへ誘導する事例²⁵、Facebookのメッセージでユーザ情報の入力を促す不審サイトへ誘導する事例²⁶などを確認しています。

2013年に確認されたLINEやFacebookでの誘導メッセージ例



²⁵ <http://blog.trendmicro.co.jp/archives/6730>

²⁶ <http://blog.trendmicro.co.jp/archives/7300>



これらの攻撃は、特に「アカウントの乗っ取り」と「脅威への誘導」を狙ったものと推測されます。最終的な攻撃者の狙いはソーシャルメディアのユーザをオンライン詐欺など何らかの「脅威」へ誘導することです。この誘導を成功させるためには、攻撃者はアカウントの乗っ取りによる成りすましを狙っています。特にアカウント乗っ取りの対象として「Twitter」と「Facebook」のアカウントに対する情報窃取攻撃が確認されています。攻撃方法としては、2種を確認しています。1つはオンライン銀行詐欺ツール同様の不正プログラムによるWebインジェクションです。TwitterやFacebookのWebサイト上に偽画面を表示し、認証を詐取します。もう1つはより古典的なフィッシング詐欺です²⁷。メールやSNS上のダイレクトメッセージ、ツイートなどに含まれているURLをクリックすると偽のログイン画面が表示されます。この手口の巧妙なところは、アクセス先をTwitterやFacebook内のコンテンツと偽装することで、ログイン画面の表示を不審に思わせないところです。また、「Facebook」ではユーザに誤解を与えることにより友達申請を認めさせる、より間接的な攻撃手法も確認されています。

²⁷ <http://blog.trendmicro.co.jp/archives/7085>

例えば、現在すでに Facebook 上の友達となっている人物と同じ名前、もしくは一文字変えた名前のアカウントから友達申請が来ます。利用者は友達が何らかの事情でアカウントを失効してしまい入りなおしたなどと勘違いし、安易に友達申請を認めてしまう場合があるようです。各種ソーシャルメディアの利用時にはこのような攻撃手法が存在することを十分に認識し、乗っ取り被害、誘導被害に遭わないよう注意を払うべきでしょう。

また、攻撃者によるクラウドサービスの利用についてはよりシンプルです。2013 年トレンドマイクロでは、オンラインストレージ、クラウド型サーバサービス、ブログサービスなどの正規サービスが不正プログラムの C&C サーバやデータ送信先といったまさに脅威インフラとして利用された具体例^{28 29 30}を確認しています。このような正規サービスの利用は遠隔操作や外部への情報送信といった不正プログラム活動の隠蔽の目的があるものと考えられます。

クラウドサービスとソーシャルメディア使用上のミスが企業の情報漏洩を招く

2013 年にはクラウドサービスやソーシャルメディアが、ちょっとした設定や使用方法のミスにより、重大な情報漏洩リスクを招いた事例が複数確認されています。特に大きな問題となったのは、7 月～9 月に多く確認された「Google グループ」の事例です³¹。Google グループのデフォルト設定では、共有した情報がインターネットに公開されます。これに気付かず結果的に機密情報が公開状態になっていた組織は、官公庁を初めとして通販サイト、学校、医療機関や新聞社など、多岐にわたっていました。また、Facebook、Twitter などでも使用者が想定していた以上の情報や公開範囲が設定されていたことによる情報漏洩事例が確認³²されています。このような情報漏洩の防止には利用者のリテラシ向上が重要です。

28 <http://blog.trendmicro.co.jp/archives/6956>

29 <http://blog.trendmicro.co.jp/archives/7062>

30 <http://blog.trendmicro.co.jp/archives/7150>

31 <http://www.yomidr.yomiuri.co.jp/page.jsp?id=81134>

32 <http://www.yomiuri.co.jp/kyoiku/syuukatsu/snews/20131002-OYT8T00592.htm>

モバイルの脅威

正規マーケットの審査を潜り抜ける不正アプリ

正規マーケット上での不正アプリ頒布が 2013 年を通じて問題に

2013 年には Android OS 向け正規マーケットである「Google Play」上に審査を潜り抜けて掲載される不正アプリが 1 年を通じて確認されました。特に 3 月に確認された「ワンクリックウェア」アプリ³³の手法は、その後も継続的に確認されています。この手法では、不正アプリが実際に行う活動を詐欺サイトへの誘導のみと限定し、Web サイトへのアクセス以外の活動は行いません。このため、アプリ単体の動作のみから判定した場合には不正であるか特定が困難なことを狙っているものと推測されます。不正アプリ対策の上でも、このような機能を限定した不正アプリの解析では、アプリ単体の動作の分析と同時に、誘導先サイトの調査を行った上で判定する取り組みも必要となります。

また、ワンクリックウェアアプリ事例以外にも、Android 向けアプリとして人気が高い「Adobe Flash Player」を偽装する不正アプリ（トレンドマイクロでは「ANDROIDOS_REVMOB.A」³⁴として検出）が国内外合わせて 5 万件以上ダウンロードされていた事例³⁵など、Google Play 上での不正アプリ頒布は止まらない状況が続いています。攻撃者の視点に立てば、より効果の高い Google Play での頒布を狙うことは当然であり、今後もこの傾向が続く可能性は高いと言えます。

ユーザを騙す攻撃方法はモバイルでも定着

使用者であるユーザを騙す攻撃手法、いわゆる「ソーシャルエンジニアリング」は、プラットフォームを問わず有効な攻撃手法です。モバイル向けの脅威においても不正サイトや不正アプリなどでユーザを騙す手口として、「偽装マーケット」、「贋作アプリ」、「リパックアプリ」といった手法があります。「偽装マーケット」は正規マーケットに偽装した不正サイトによってユーザを騙す攻撃であり、2013 年上半期に継続して確認されました。確認された攻撃では、「Google Play」や Apple の「App Store」のデザインを偽装した不正サイトを表示して利用者にアプリがインストールされたものと誤解させる方法で、最終的にサクラサイトやワンクリック詐欺サイトへ誘導する手口がとられていました³⁶。また、不正アプリの頒布方法として、不正アプリを有名アプリの名称を偽装して配布する「贋作アプリ」、有名アプリのモジュールに不正アプリを挿入する「リパックアプリ」は既に定着した攻撃方法と言えます³⁷。特に、2013 年にはリパックを簡単な操作で行える「バインダー」と呼ばれる不正ツールの存在も確認されました。

³³ <http://blog.trendmicro.co.jp/archives/6984>

³⁴ http://about-threats.trendmicro.com/malware.aspx?language=jp&name=ANDROIDOS_REVMOB.A

³⁵ <http://blog.trendmicro.co.jp/archives/7825>

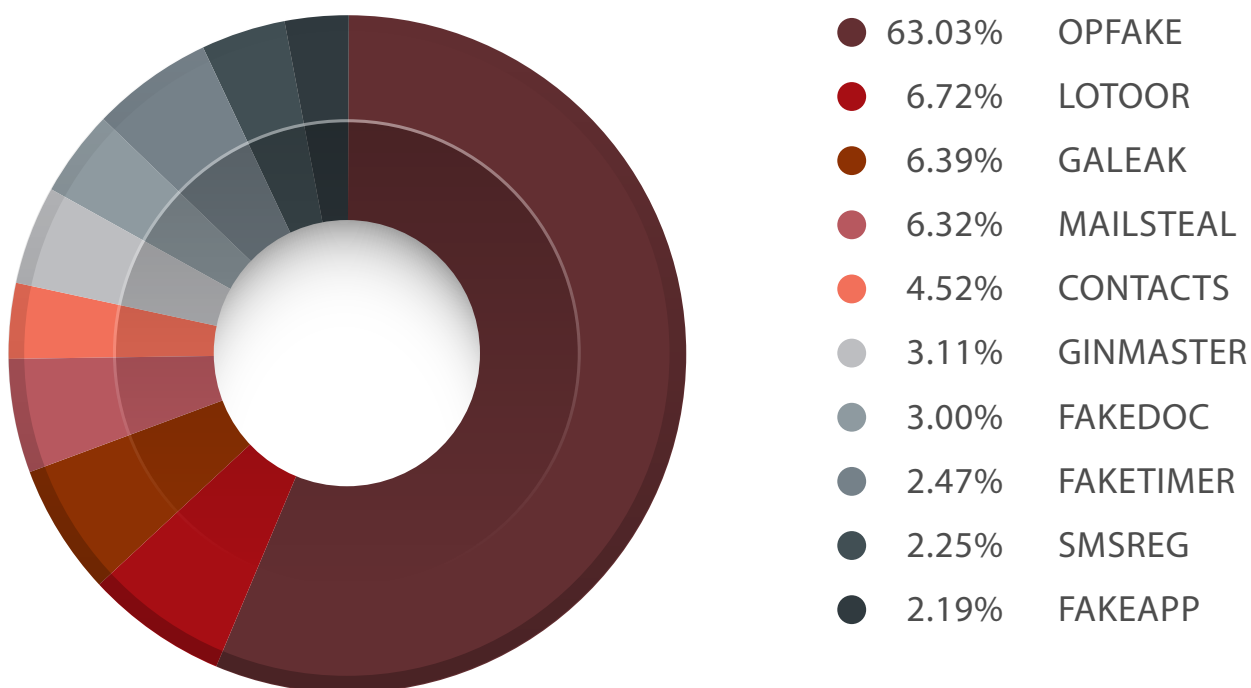
³⁶ <http://blog.trendmicro.co.jp/archives/6730>

³⁷ <http://blog.trendmicro.co.jp/archives/7479>

2013 年、日本で検出された Android 向け不正アプリ TOP10

トレンドマイクロのクラウド型セキュリティ基盤「Trend Micro Smart Protection Network」(SPN) ではモバイルアプリの評価システムである「MAR (Mobile App Reputation)」により、モバイル向け脅威の分析と対策の提供をしています。MAR で分析した不正アプリのうち、2013 年を通じて日本で最も多く検出されたものは OPFAKE でした。これは有名アプリに偽装した不正アプリの総称であり、上述の有名アプリへの偽装によりユーザーを騙す攻撃方法が、実際に多く出回っていることを示しています。また、2 位となっている LOTOOR は、Android OS のルート化を行うハッキングツールです。攻撃者はルート権限を奪うことにより、自由に端末内の情報にアクセスできる上、侵入した不正アプリの検出、削除を困難にさせることができます。第 3 四半期に日本で攻撃者が逮捕されその被害実態が明らかになった CONTACTS ファミリーは、通年では 4.52% の検出を占めていました。これらの不正アプリのもたらす被害として、情報の窃取と不正な広告表示が主要となっています。前出の CONTACTS ファミリー攻撃者の事例からは、窃取された情報がフィッシング詐欺、サクラサイトなどのオンライン詐欺サイトへ誘導するスパムメール送信に利用される実態が明らかになっています。

2013 年日本から検出された不正アプリファミリー割合 (トレンドマイクロ SPN の検出上位 10 種による)



2013 年に確認された iPhone など iOS 端末での脅威危険性動向

2013 年には iPhone に代表される iOS 端末でも、脅威について考えさせるいくつかの事例が確認されました。中でも不審な Web コンテンツと様々なメッセージによる誘導という攻撃手口の危険性が再認識されましたが、特に iOS ユーザを狙ったと考えられる攻撃として、iOS 向けアプリマーケットである App Store のデザインを偽装したサクラサイトが確認されています³⁸。また、iOS 利用者であれば所持している Apple ID を狙ったフィッシングサイトが 2013 年 5 月以降に急増しました^{39 40}。このようなオンライン詐欺への誘導は一般的なスパムメールの他に、Facebook や Twitter のようなソーシャルメディアのメッセージが使われます。ソーシャルメディアによる脅威への誘導が特に顕在化した事例として、ブラウザクラッシャーの事例⁴¹ や iOS をブルー画面にする動画ファイルの事例⁴² がありました。これらの事例では Twitter 上で不審な Web サイトへ誘導するツイートが多く確認されました。

Twitter 上で確認された iPhone ユーザを誘導しようとするツイートの例



利用者の多い iOS 端末は攻撃者にとって魅力的な攻撃対象です。フィッシング詐欺、ワンクリック詐欺、サクラサイトなど、Web によってユーザを騙すタイプのオンライン詐欺はプラットフォームを問わない脅威であり、各種メッセージから Web に誘導する攻撃は既に注意が必要です。また iOS では不正アプリの脅威はほとんどないと考えられますが、カテゴリとは異なる不審な Web に誘導するアプリや、ロゴや商標などを権利者に許可なく使用するアプリなど、AppStore 上に不審なアプリが公開される事例も複数確認されています^{43 44}。これらは大きな脅威ではありませんが、連絡先など端末内の情報にアクセスを求めようとするアプリについては、開発元、情報の利用内容をよく確認してから許諾する注意は必要となってくるでしょう。

³⁸ <http://blog.trendmicro.co.jp/archives/6730>

³⁹ <http://blog.trendmicro.co.jp/archives/7171>

⁴⁰ <http://blog.trendmicro.co.jp/archives/7930>

⁴¹ <http://blog.trendmicro.co.jp/archives/6916>

⁴² <http://blog.trendmicro.co.jp/archives/8114>

⁴³ <http://blog.trendmicro.co.jp/archives/7710>

⁴⁴ <http://www.security-next.com/045762>

グローバルセキュリティラウンドアップ

金銭目的で狙われるデジタル情報

オンライン銀行詐欺ツールやランサムウェアの猛威

はじめに

2013年は、金銭を狙った犯罪がデジタルの世界でもリアリティを帯びてきた年だったといえます。クレジットカード番号や、銀行口座情報、その他の個人情報をわずかな時間で窃取できるサイバー犯罪者は、その巧みな手法を金銭の強奪へ駆使し始め、デジタル情報が“新たな通貨”と見なされています。このような中で、サイバー犯罪者がもたらした被害は、まさしく予想を上回るものでした。

また、2013年は、従来の脅威の“さらなる巧妙化”が確認された年でもありました。オンライン銀行詐欺ツールの検出数は、年間を通して増加を続け、これまで狙われたことのなかった国で感染事例が確認されました。2013年10月には、ランサムウェアの感染に数多くのユーザが悩まされ、より大きな被害をもたらす新種のランサムウェア「CryptoLocker」も登場しました。その他の巧妙な攻撃の事例と共にこうした例はいずれも、トレンドマイクロが以前から予測していた傾向とも一致しています。すなわち、サイバー犯罪者は、新たなツールを開発する代わりに既存のツールを改良して不正活動を行うという傾向です。¹

モバイル関連の脅威に関しては、不正アプリや高リスクアプリの数が2013年の9月時点で早くも累計100万個を突破しました。²そして現時点では累計でほぼ140万個に達しており、2013年の1年間だけで100万個に及んでいます。

持続的標的型攻撃に関する報道は2013年、若干減少しましたが、そうした中でも、持続的標的型攻撃の作戦活動（キャンペーン）は、依然世界中で発生しており、その標的も、ブラジルやフランス、ドイツを含むさまざまな国に及びました。

脆弱性関連では、オラクルのJava™ 6のサポート終了が問題を深刻化させ、ソフトウェアの更新を怠ったり、サポートされていないソフトウェアを使い続けたりするリスクを改めて再認識させたといえます。³

いわゆる「個人情報を狙う攻撃」の脅威は、従来から発生してきたとはいえ、2013年は、その脅威への関心が社会全体に広がった年だといえます。個人情報へ大きな関心が向けられる中、国家の監視体制に関するエドワード・スノーデンの暴露に端を発した議論は、その状況をさらにエスカレートさせました。今日の“デジタル化時代”において特に2013年は、「どのようにして個人情報を守るべきか」という問いを突き詰められた年だったといえます。そしてその解は、「個人情報の公開を最小限にとどめる、あるいは最適なセキュリティ製品を利用すること」のいずれかに集約されるでしょう。

註：本稿に掲載されるデータ等の数値は、特に明記されていない場合、トレンドマイクロのクラウド型セキュリティ基盤「Trend Micro Smart Protection Network」が出典となります。

¹ <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/sp-trend-micro-predictions-for-2013-and-beyond.pdf>

² <http://about-threats.trendmicro.com/us/mobile/monthly-mobile-review/2013-10-malicious-and-high-risk-android-apps-hit-1-million>

³ <http://www.trendmicro.co.jp/cloud-content/jp/pdfs/security-intelligence/threat-report/pdf-2013q3-20131107.pdf>

サイバー犯罪とアンダーグラウンド活動

標的から直接金銭を奪う不正プログラムの被害 台数と地域が増加

金銭目的の不正プログラム検出台数が急増

2013 年は、世界中のユーザにとって試練の年でした。巧妙化した脅威は、デジタル化の進んだユーザの生活に深刻なリスクをもたらしたからです。オンライン銀行の取引やその他のオンラインの金融取引において、ユーザの個人情報や口座自体が大きなリスクにさらされました。

オンライン銀行詐欺ツールは、その検出台数が急増したことで大きな注目を集めました。オンライン銀行詐欺ツールの検出台数は、2013 年の年末にほぼ 100 万に到達しました。米国と日本が 2013 年第 4 四半期に最も感染被害を受けた上位二カ国となり、ブラジルや台湾がその後が続きました。また、オンライン銀行詐欺ツールの感染総数増大の要因として、特にブラジルと日本で 2013 年この脅威が拡大したことがあげられます。

ブラジルでは、.CPL ファイル(不正なコントロールパネル)を用いた攻撃手法の増加が確認されました。このファイルは、スパムメールの添付ファイルである .RTF ファイルに組み込まれていました。⁴ この傾向は、2013 年 9 月から登場し始め、添付ファイルに .RAR や .ZIP ファイルを用いるような従来の典型的なオンライン銀行詐欺ツールとは異なる手法といえます。

また、2013 年第 3 四半期および第 4 四半期には、不正プログラム「ZBOT」の日本での検出台数増加も確認しました。これは、こうしたサイバー犯罪活動が日本で急増したことや、今までオンライン銀行詐欺ツールの主要な標的ではなかった日本のユーザが新たに狙われ始めたことを意味するといえます。

これらの不正プログラムの巧妙化や、オンライン銀行詐欺ツール検出台数の増大は、標的となったユーザに対して金銭的損失という深刻な被害をもたらしました。^{5 6 7 8}

⁴ <http://blog.trendmicro.co.jp/archives/8348>

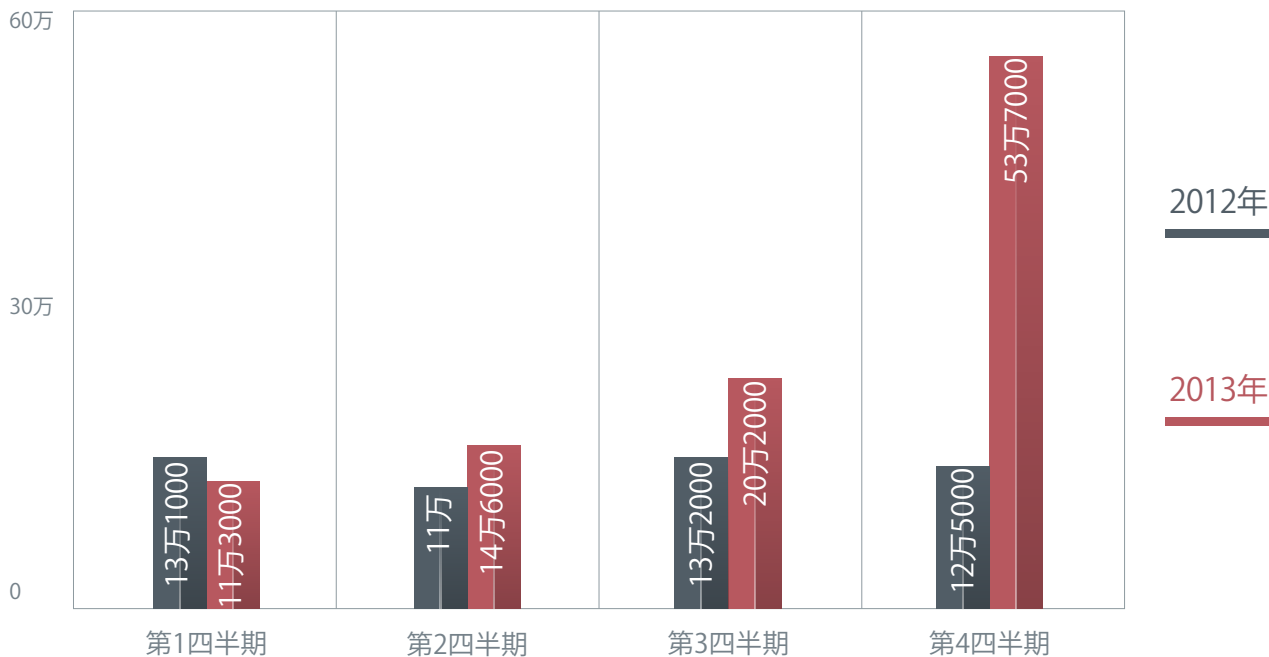
⁵ <http://krebsonsecurity.com/2013/08/1-5-million-cyberheist-ruins-escrow-firm/>

⁶ <http://krebsonsecurity.com/2013/05/hc-fuel-distributor-hit-by-800000-cyberheist/>

⁷ <http://krebsonsecurity.com/2013/04/wash-hospital-hit-by-1-03-million-cyberheist/>

⁸ <http://news.idg.no/cw/art.cfm?id=F0176E45-E7DE-BA82-31C5C4AE4C5B7FB7>

2012年・2013年のオンライン銀行詐欺ツールの検出回数



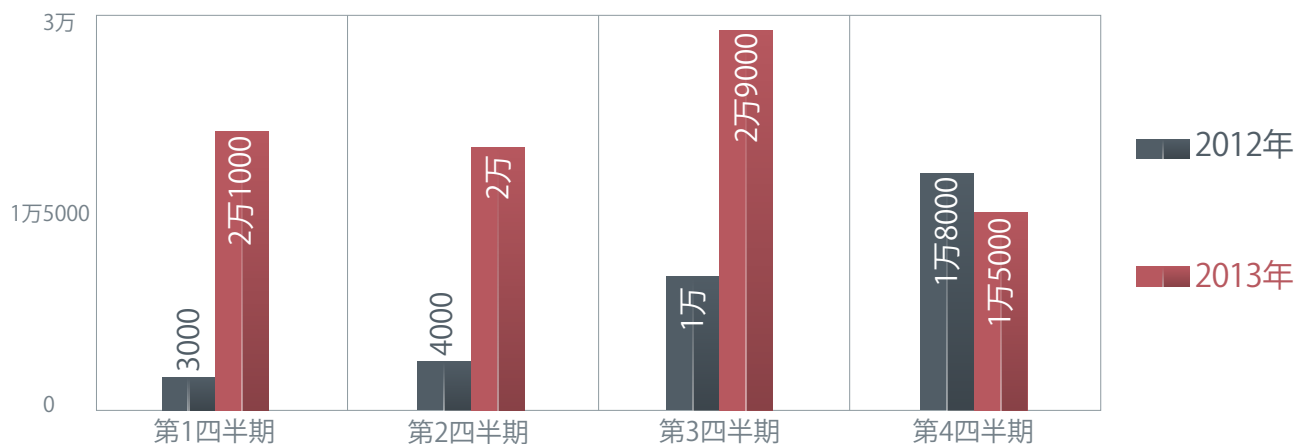
2013年のオンライン銀行詐欺ツールの感染総数は、2012年の約50万から倍増しています。これは、2013年第4四半期に日本で検出回数が急増したことが要因といえます。同様の急増は、サイバー犯罪者がフィッシングメールを駆使してオンライン銀行詐欺ツールの拡大を図った、休暇シーズンのブラジルにおいても確認されました。

このような巧妙化の例としてあげられるのが、身代金要求型ランサムウェアの改良版として2013年10月に登場した「CryptoLocker」であり、新たなツールを開発する代わりに従来のツールを改良するというサイバー犯罪者の手法を示す好例といえます。⁹ 「TROJ_UPATRE」の亜種が添付されたスパムメールも確認され、こうしたスパムメールの送信活動も「CryptoLocker」の感染増加に加担していました。¹⁰ 「CryptoLocker」は、感染したコンピュータへのユーザのアクセスをブロックするだけでなく、ブロックを解除するために必要な復号ツールを300米ドルもしくは（仮想通貨の）クリプト通貨などの“身代金”で購入するよう、ユーザへ強要します。

⁹ <http://blog.trendmicro.co.jp/archives/7984>

¹⁰ <http://blog.trendmicro.co.jp/archives/8017>

2012 年・2013 年ランサムウェア検出件数



2013 年のランサムウェア感染総数は、2012 年の 2 倍以上となっています。特に 2013 年の第 3 四半期は、10 月に発生した「CryptoLocker」の影響もあり、検出件数が（ほぼ 3 万に）急増しています。

サイバー犯罪者は、特に隠ぺい活動に関してあらゆる手段を駆使します。¹¹ 隠ぺい手段の 1 つとして、トレンドマイクロでは 2013 年 10 月、Deep Web という匿名かつ追跡を不可能にする Web サイトに関する調査結果を報告しました。¹² この調査では、Deep Web 内に存在する闇市場に注目し、Deep Web 内のネットワーク上でサイバー犯罪者がどのようにツールや手口を共有・交換しているかを分析しています。

このような状況ではありましたが、セキュリティ業界は 2013 年、ただ手をこまねいていたわけではありません。通称 Paunch と呼ばれる「Blackhole Exploit Kit」作成者が 2013 年 10 月に逮捕されたことは、トレンドマイクロのクラウド型セキュリティ基盤「Trend Micro Smart Protection Network」のデータも示すとおり、11 月におけるスパムメール総数の顕著な減少に貢献したといえます。¹³ この減少傾向は、Blackhole Exploit Kit の消滅に起因していたといえます。¹⁴ しかしながら、12 月になって、サイバー犯罪者が金融業界やソフトウェア業界の企業や組織を狙い始めたことから、スパムメールの総数は再び増加し始めました。

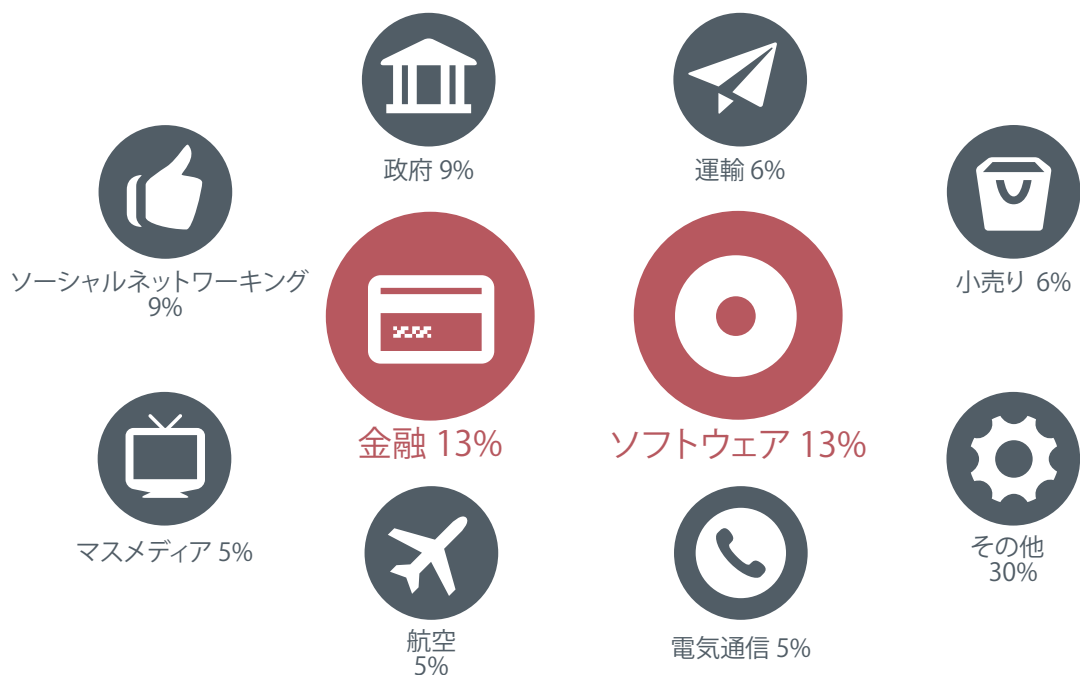
¹¹ <http://blog.trendmicro.co.jp/archives/8128>

¹² <http://blog.trendmicro.co.jp/archives/7960>

¹³ <http://blog.trendmicro.co.jp/archives/8001>

¹⁴ <http://blog.trendmicro.co.jp/archives/8386>

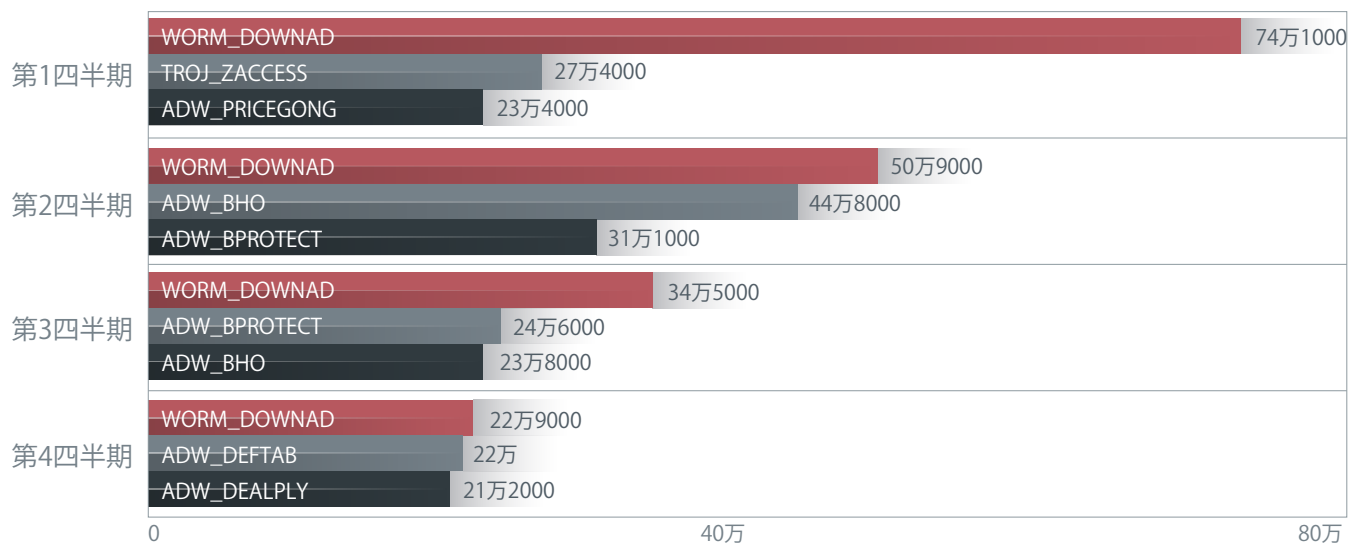
2013 年に「Blackhole Exploit Kit」によるスパムメールがなりすました主要業界



「Blackhole Exploit Kit」に関連したスパムメール送信活動を追跡したところ、サイバー犯罪者は、他のどの業界の企業よりも、特に銀行やソフトウェア企業になりすます傾向が多いことを確認しています。

悪名高いワーム「DOWNAD」の検出数が 2013 年を通じてゆっくりとその勢いを失いつつあることは、より多くのユーザ（個人ユーザも企業も）が Windows® の新しいバージョンに移行している状況を踏まえると、驚くべきことではないでしょう。実際、2013 年全体でも、「Trend Micro Smart Protection Network」のデータによると、「DOWNAD」の検出数が 2013 年第 1 四半期の 74 万 1000 から同年 12 月には 22 万 9000 へ減少しています。ただし、こうした減少にも関わらず、「DOWNAD」は、2013 年も大企業および中小・中堅企業の双方において、最も検出数の多い不正プログラムとなりました。「DOWNAD」に対しては、セキュリティパッチ「MS08-067」の適用による脆弱性対策を行うことで、感染を阻止できます。また、「Trend Micro Deep Security」による保護も、このワームのネットワーク拡散を防ぎます。

2013 年不正プログラムトップ3



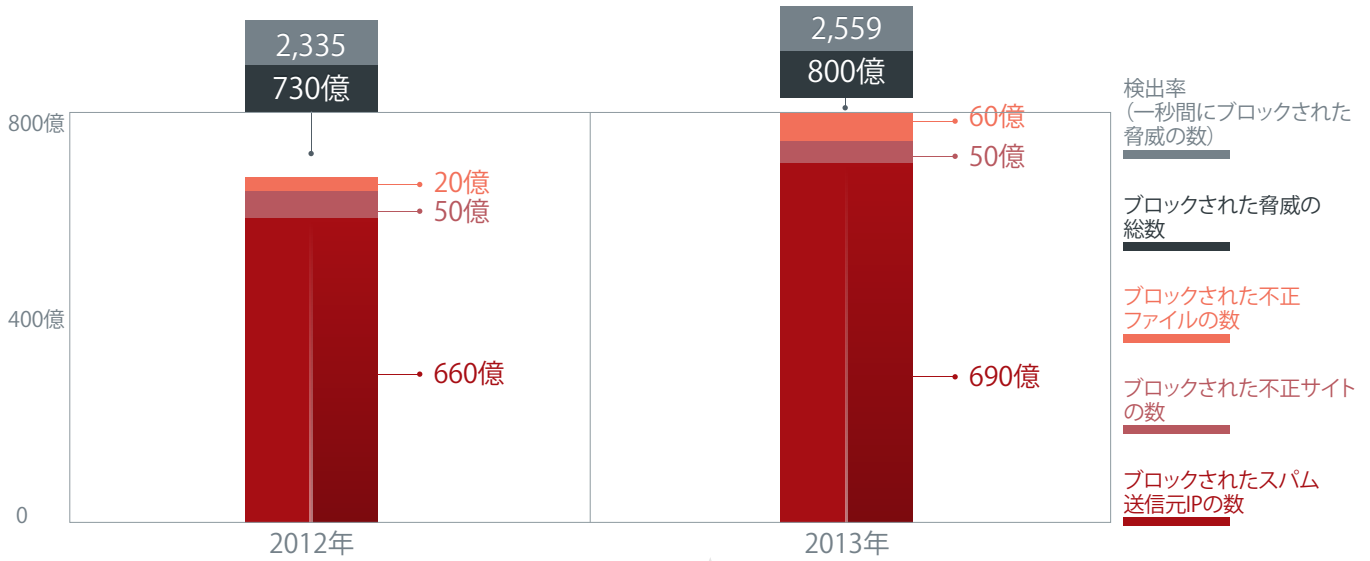
「DOWNAD」は、2013 年第 1 四半期の 74 万 1000 から大幅に減少したものの、2013 年第 4 四半期の時点でもトップ 1 の順位を保持しています。

不正プログラムトップ3：セグメント別

第1四半期		第2四半期		第3四半期		第4四半期	
大企業							
WORM_DOWNAD	36万 4000	WORM_DOWNAD	36万	WORM_DOWNAD	8万 6000	WORM_DOWNAD	18万 4000
PE_SALITY	8万 1000	ADW_BPROTECT	5万 3000	ADW_BPROTECT	3万 3000	ADW_DEALPLY	4万 4000
PE_VIRUX	3万 4000	ADW_BHO	2万 8000	ADW_TOOLBAR	2万 1000	ADW_DEFTAB	4万 3000
中堅・中小企業							
WORM_DOWNAD	8万 1000	WORM_DOWNAD	5万 9000	WORM_DOWNAD	1万 7000	WORM_DOWNAD	4万 2000
PE_SALITY	1万 7000	ADW_BPROTECT	9000	ADW_TOOLBAR	9000	ADW_DEFTAB	2万 3000
TROJ_ZACCESS	1万 4000	ADW_BHO	8000	ADW_BPROTECT	8000	HKTL_PASSVIEW	1万 7000
個人ユーザ							
TROJ_ZACCESS	16万 3000	ADW_BHO	37万	ADW_BHO	15万 8000	ADW_DEFTAB	8万 9000
CRCK_KEYGEN	16万 2000	ADW_BPROTECT	21万 6000	ADW_BPROTECT	13万 8000	ADW_OPENCANDY	6万
ADW_PRICEGONG	15万 7000	BKDR_BIFROSE	20万 8000	TROJ_FAKEAV	8万 7000	ADW_BHO	5万 4000













2013年の第4四半期も多くの企業が「DOWNAD」の被害に見舞われました。個人ユーザは、ほとんどがアドウェアによる被害でした。一般に個人ユーザの方が企業よりも頻繁にソフトウェアの更新を行えること、企業側は予算や統制上の問題などから更新頻度が下がる可能性があることから、この結果は予想内といえます。

2012年・2013年：「Trend Micro Smart Protection Network」の検出率
 「Trend Micro Smart Protection Network」によりブロックされた数量（出典：SPN ポータル）



ブロックされた脅威の総数は、2012年から2013年にかけて約70億増加しています。検出率も増加し、2013年は、一秒間に約2500の脅威をブロックしています。

2013年：Deep Web とロシアのアンダーグラウンドにおける闇市場の商品価格一覧

	欧米のクレジットカード	10~150米ドル	2~120米ドル		PayPalのアカウント	1000米ドルアカウント作成で126米ドル	2~15米ドル
	偽造ID	1,352~1,555米ドル			偽造パスポート	3,380~5,400米ドル	
	偽の米国市民権の関連文書	10,000米ドル			偽の米国運転免許証	200米ドル	
	偽造英国パスポート	4,000米ドル			偽造ユーロ紙幣	2,500 ユーロ紙幣で676米ドル 3,000 ユーロ紙幣で1,352米ドル 6,000 ユーロ紙幣で2,570米ドル	
	偽造米国紙幣	2,500 米ドル紙幣で600米ドル 5,000 米ドル紙幣で2,000米ドル			偽造紙幣	紙幣価格の半額	
	ハッキングのサービス	270~676米ドル 16~500米ドル			Webサイトの開発	時給126米ドル	

Deep Web内での標準価格 ロシアのアンダーグラウンド市場での価格

サイバー犯罪のアンダーグラウンドにおける商品価格は、どの闇市場で売られているかによって異なります。ユーロや米ドルなどの偽造紙幣はかなりの高額で販売されており、いわゆる偽造文書は、貴重な商品として取り引きされていたようです。サイバー犯罪者は、窃取された情報を販売するだけでなく、Web サイト開発のようなサービスも提供している点は注目すべき点の一つです。

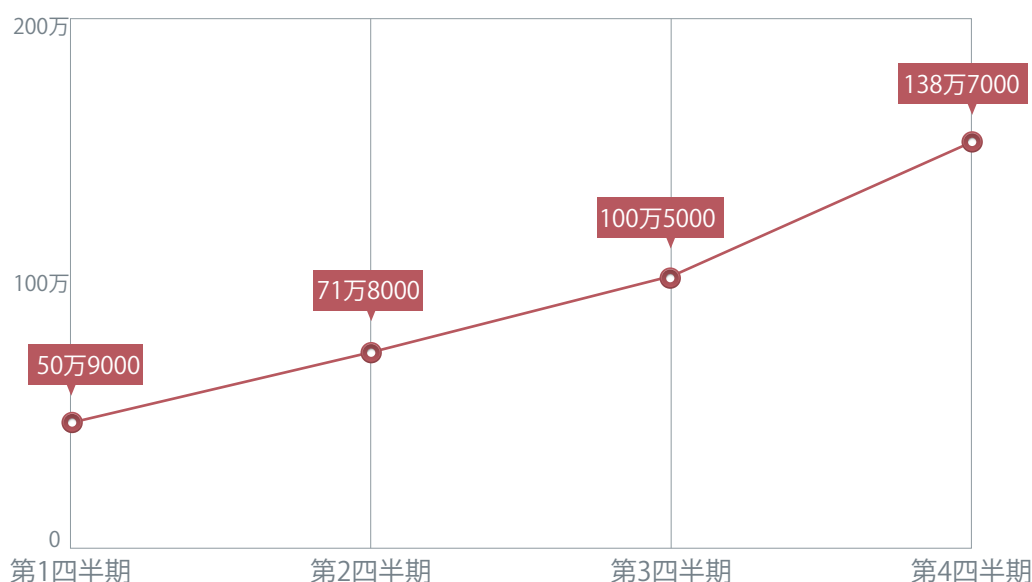
モバイルの脅威

PC からモバイルへの移行に合わせ、モバイルの脅威は数と巧妙さが増加

脅威の数と範囲の拡大

Android™は、市場で最も大きな勢力を占めるモバイル OS であり、その状況は現在も続いています。Gartner も、2014 年には Android ユーザの数は 10 億人を記録するだろうと予測しています。¹⁵ こうした勢いに伴い、2013 年には不正アプリや高リスクアプリの数も増大し、その数は年末にはほぼ 140 万に到達しました。サイバー犯罪者は、今後も大きな勢力を占めるモバイル OS を狙ってくることから、2014 年末には、不正アプリや高リスクアプリの数は、300 万に達するとトレンドマイクロでも予測しています。¹⁶

2013 年：不正アプリ・高リスクアプリの増加



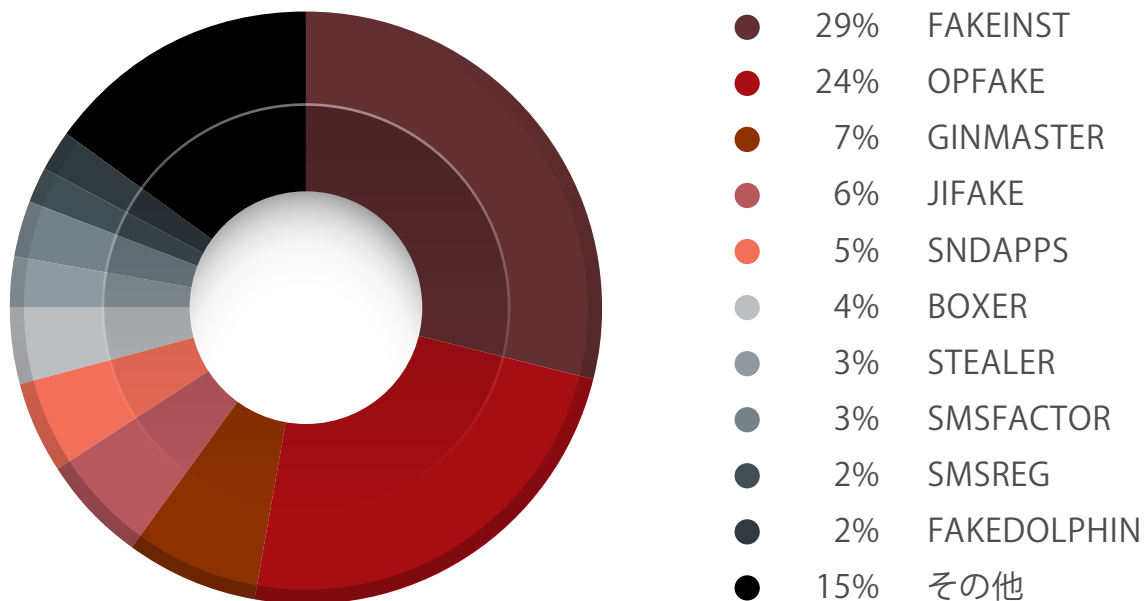
不正アプリおよび高リスクアプリの数は、2012 年から 2013 年にかけて 2 倍以上の増加を示しています。サードパーティのアプリストアおよび正規のアプリストアの双方において、不正アプリの検出数が増加しています。

註：「高リスクアプリ」もしくは「迷惑行為を行う可能性のあるアプリ」とは、無用な広告を表示させたり、不必要なショートカットを作成したり、ユーザに知らせずに端末情報を収集したりして、ユーザへ迷惑をもたらすアプリのことを指します。執拗な迷惑広告を表示するアプリもここに含まれます。

¹⁵ <http://www.gartner.com/newsroom/id/2645115>

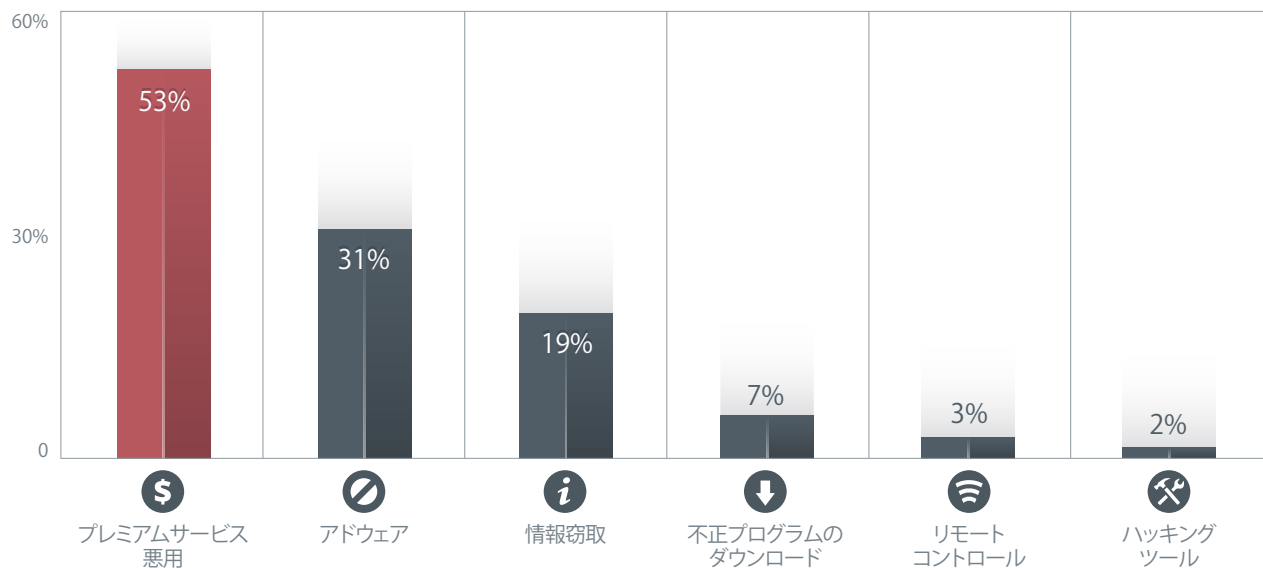
¹⁶ <http://blog.trendmicro.co.jp/archives/8289>

2013 年新たに確認された不正・高リスクアプリ



Android 端末向け不正プログラムとして 2013 年に新たに確認されたもののほとんどが、例年どおり、人気アプリをトロイの木馬化した不正プログラムとなっています。

Android 端末向け不正プログラムを脅威タイプ別に分類



プレミアムサービス悪用およびアドウェアが、2013 年も最も多く確認された Android 端末向け脅威でした。プレミアムサービス悪用は、ユーザを高額利用料のサービスに登録させるものです。アドウェアは、広告を執拗に表示させ、場合によってはユーザが気づかぬうちに個人情報を窃取することもあります。

註：Android 端末向け不正プログラムの 1 つのファミリーが複数の脅威タイプを実行する場合があります。

2013 年第 3 四半期、不正アプリや高リスクアプリの大半 (80%) は不正なドメイン上に存在していました。また、その一部 (27%) がサードパーティのアプリストアと共に正規のアプリストアにも姿を表し始めたことが確認されました。例えば、不正アプリのいくつかは、Google Play からダウンロード可能であり、ダウンロードすると、この不正アプリによりユーザは詐欺サイトへ誘導されます。¹⁷ BlackBerry の場合、トレンドマイクロとのパートナーシップが効を奏し、再パッケージされた Android アプリの 2% が事前に「不正アプリ」もしくは「高リスクアプリ」として検出され、正規アプリストアの BlackBerry World で販売される前にブロックされました。Apple の App StoreSM で、これらの不正アプリの侵入は確認されていませんが、セキュリティ専門家たちは、既にこの正規アプリストアに関しても、ベンダ側の承認プロセスをすり抜けて侵入する手法の概念実証 (PoC、Proof of Concept) を提示しています。この手法は、2011 年にも発生したとおり、ベンダ側の承認プロセスの際に攻撃者側の不正活動を巧みに隠ぺいして審査をすり抜けることを可能にします。^{18 19} これらの事例は、サイバー犯罪者が自分たちの不正アプリを改変し続け、正規アプリストアへの侵入を図ろうとしている状況を如実に示しているといえます。

¹⁷ <http://blog.trendmicro.com/trendlabs-security-intelligence/1730-malicious-apps-still-available-on-popular-android-app-providers/>

¹⁸ <http://blog.trendmicro.co.jp/archives/7243>

¹⁹ <http://blog.trendmicro.co.jp/archives/7846>

アプリ承認のプロセス



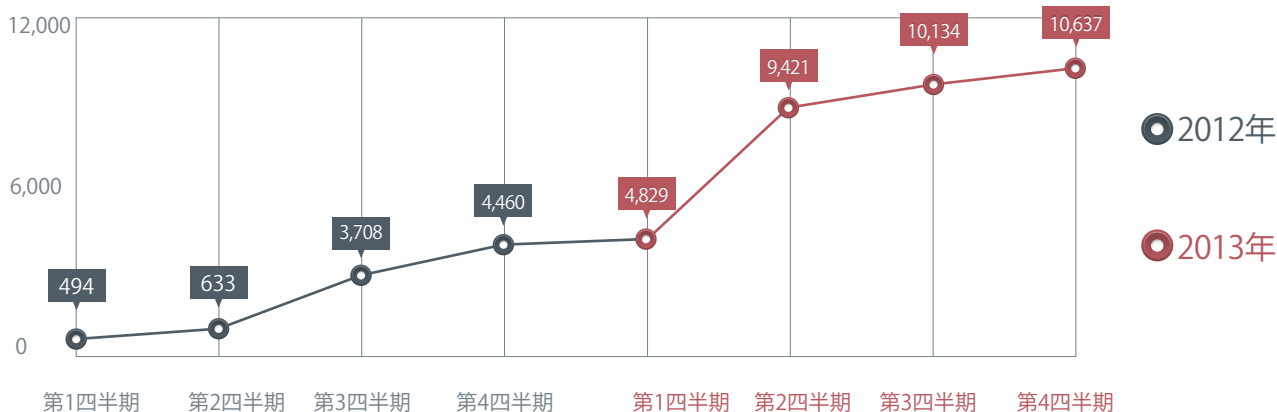
上図は、アプリ開発者が自作のアプリを Google Play および App Store の双方に提出する際のプロセスを示したものです。Android アプリの場合、APK が有効化されてアプリが公開される前に、承認済み APK や、市場状況、その他の詳細をアップロードする必要があります。他方、App Store の場合、開発者は、Apple 側の細かい審査プロセスを経る必要があります。このプロセスは、ユーザ情報を保護し、なおかつアプリが開発者の知らないところで勝手に改良・配布されるのを防ぐ、1つのセキュリティモデルを示しているといえます。

不正アプリや高リスクアプリの他、フィッシングサイトなどの Web からの脅威も PC からモバイル端末へのシフトが確認されました。²⁰ 2013 年におけるモバイル端末向けのフィッシングサイトの総数は、まだ PC と比べられるほどの数ではないものの、2012 年から 2013 年にかけて 38% の増加を示しています。PC における従来型のフィッシングサイトとは異なり、モバイル端末向けのフィッシングサイトは、スマートフォンやその他の各種モバイル端末を使用してインターネットを利用するユーザから情報窃取することを目的に作成されています。²¹

²⁰ <http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/>

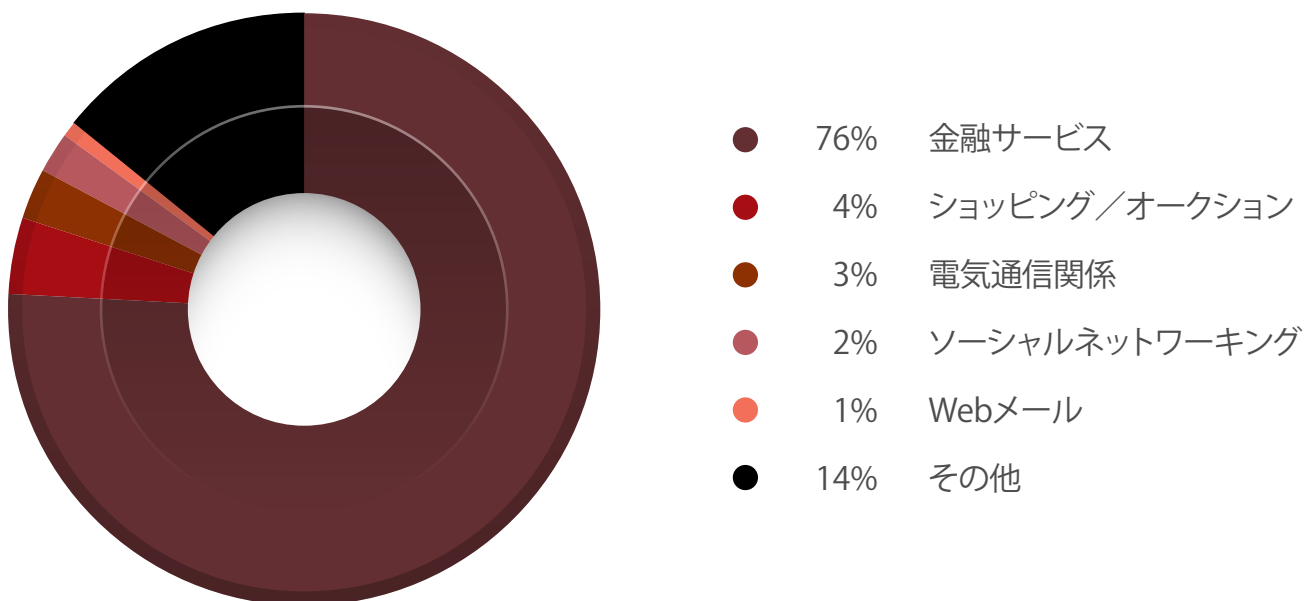
²¹ <http://about-threats.trendmicro.com/us/mobilehub/mobilereview/rpt-monthly-mobile-review-201302-mobile-phishing-a-problem-on-the-horizon.pdf>

モバイル端末向けのフィッシングサイトの数



増加の割合に変化ははあったものの、フィッシングサイトの累積数としては、2012年から2013年から一貫して増え続けています。特に2013年の第2四半期に大きな増加を示しましたが、これは、PayPalのなりすましサイトの増加に起因しています。

2013年：モバイル向けフィッシングのなりすましサイトの種別



2013年、モバイル端末においても、金融関連を装うサイトが最も多くフィッシング詐欺に悪用され、第2四半期、特にその傾向が顕著でした。フィッシング詐欺という点では、PayPalが最も多く悪用された企業でした。

スパムメール送信活動も、2013年9月に確認された「WhatsApp」関連の詐欺が示すとおり²²、モバイルの脅威を拡散する経路として悪用されました。このことから、モバイルの脅威も、単に数が増えているだけでなく、感染の経路などにおいて、手口の巧妙化が進んでいることが分かります。サイバー犯罪者や攻撃者は、ユーザが使用するオペレーティングシステム（OS）に応じて、スパムメールやそこから感染をもたらす不正プログラムの種類を巧みに使い分けています。

WhatsApp 関連詐欺の感染フロー



銀行関連の脅威でもモバイル端末が標的となり、二要素認証をすり抜ける手口等が確認され大きく注目されました。²³ 特に「Perkele」というクライムウェアのツールキットは、モバイル関連のアプリ向けに設計されており、「中間者攻撃（MitM、Man-in-the-Middle）」で利用されました。ツールキット「Perkele」で作成された不正プログラム「PERKEL」は、モバイル端末によるオンライン銀行の認証メッセージを傍受します。²⁴ さらに2013年の第2四半期、不正プログラム「FAKEBANK」は、正規のオンライン銀行アプリになりすまし、モバイル端末によるオンライン銀行ユーザの口座情報や、通話ログ、テキストメッセージ等を窃取しました。²⁵

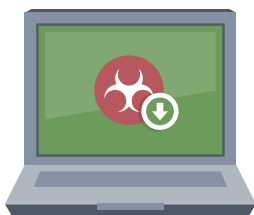
²² <http://www.nngroup.com/articles/mobile-site-vs-full-site/>

²³ <http://www.theguardian.com/technology/appsblog/2013/aug/19/ios-malware-apple-iphone-ipad-jekyll>

²⁴ <http://about-threats.trendmicro.com/us/mobile/monthly-mobile-review/2013-08-mobile-banking-threats>

²⁵ http://about-threats.trendmicro.com/us/malware/ANDROIDOS_FAKEBANK.A

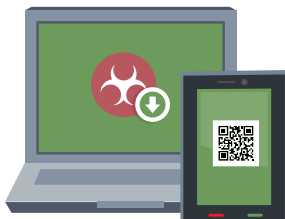
中間者攻撃の手法



1 不正プログラムがユーザのPCに感染



2 ユーザが、監視されたオンライン銀行サイトを閲覧



3 PC上の不正プログラムがユーザにQRコードをスキャンするよう促す。スキャンされると、QRコードをコードは他の不正プログラムをダウンロードする。



4 PC上の不正プログラムが、オンライン銀行取引を開始。認証コードを含むSMSがモバイル端末に送信される。



5 モバイル端末上の不正プログラムが、ワンタイムコードの入ったSMSを傍受し、攻撃者のサーバでコードを受信



6 PC上の不正プログラムもコードを受信し、オンライン銀行の取引が完了

中間者攻撃により、攻撃者は、ユーザのオンライン銀行情報にアクセスできるようになります。特にモバイル端末向けの中間者攻撃の場合、攻撃者は、ユーザがスマートフォンでオンライン銀行サイトと行うすべてのやりとりを窃取することが可能になります。

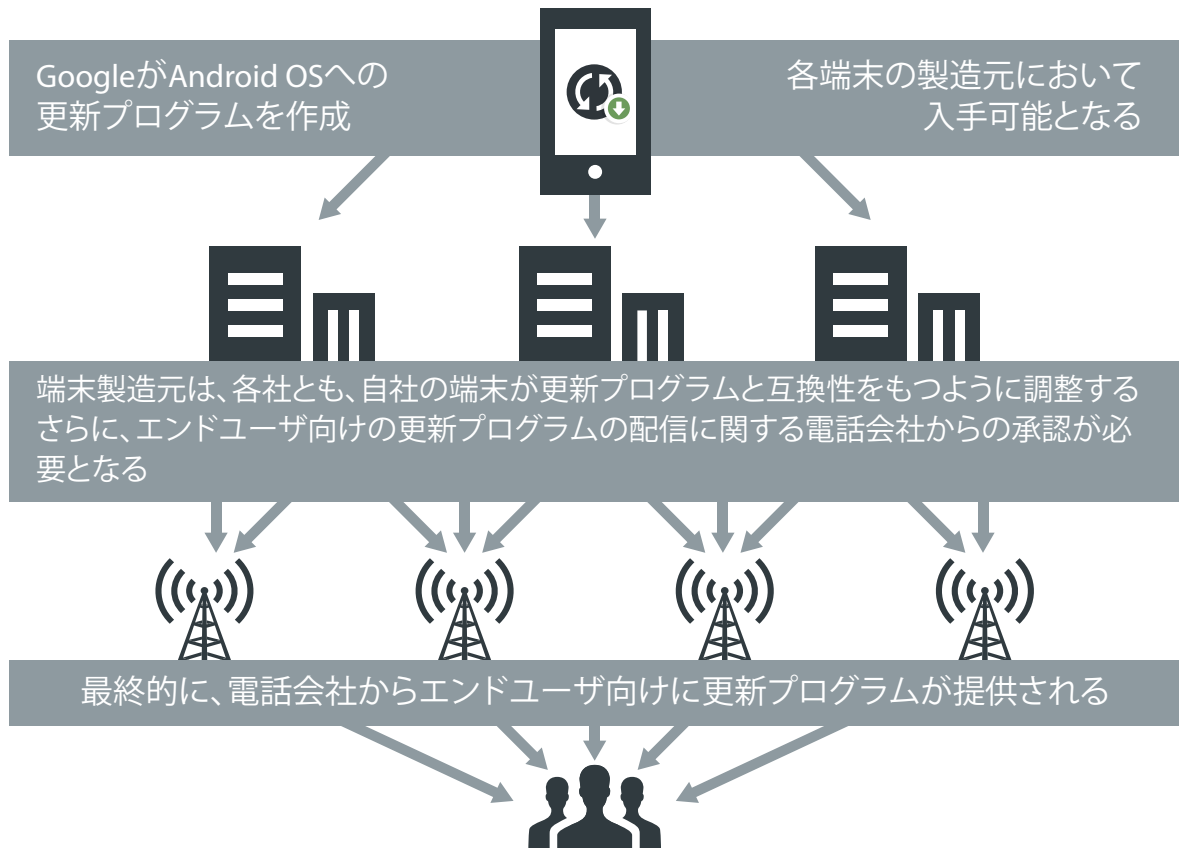
2013年、モバイル関連の脆弱性も大きな話題となりました。²⁶ SIMカードやモバイルOS上のセキュリティ関連の不具合も明らかにされ、特に2013年7月に確認されたAndroid端末関連の「マスターキー」とよばれる脆弱性は、端末内にインストールされたアプリをユーザが知らない間に不正なアプリに変更することさえ可能にしました。²⁷ 不正プログラム「OBAD」も、Android端末上の深刻な脆弱性を悪用しました。²⁸ そうした中、大半のユーザは、Android端末関連の脆弱性の修正パッチを受け取るまでに複数の段階を経る必要があるため、脆弱性へのパッチ適用が懸案となっています。全てのOSにおいて安全は担保されていません。iOS 6にもセキュリティ上の不具合が確認され、このOSが稼働するiPhone® やiPad® への外部からの完全なアクセスが可能になることも明らかにされました。

²⁶ <http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=Emerging+Vulnerabilities%3A+Glitches+Go+Mobile>

²⁷ <http://blog.trendmicro.co.jp/archives/7526>

²⁸ <http://blog.trendmicro.co.jp/archives/7410>

Android OS における脆弱性の更新プロセス



このような Android OS の複雑な更新プロセスが、さまざまな脅威に対して Android 端末が脆弱である理由の 1 つといえます。

サイバー攻撃

大規模な報道は見られずとも、攻撃の勢いは衰えず

標的型サイバー攻撃の傾向

2013 年も攻撃者は、攻撃手法に磨きをかけ続け、特に政府関連の情報を狙うことに注力していました。攻撃は世界のさまざまな地域に及び、従来の脆弱性と共に新たに確認された脆弱性も攻撃の手法に悪用されました。例えば、脆弱性「CVE-2012-0158」は、特別に細工された文書ファイル（拡張子：.DOC や .RTF）で悪用され、Microsoft™ Office®2003、2007、2010 のバージョンを使用していた世界中のユーザが被害を受けました。この脆弱性には、既に修正パッチが公開されていましたが、未適用のユーザの存在で被害が大きくなりました。²⁹ 新たな脆弱性としては、Internet Explorer® の未修正のゼロデイ脆弱性が 2013 年 5 月、米国労働省のサイトを狙った「水飲み場（Watering Hole）」攻撃に利用されました。³⁰ トレンドマイクロの調査でも、改ざんされたサイトを閲覧したユーザは、何度かリダイレクトされた後、「BKDR_POISON」に感染するサイトへ誘導されることが分かっています。³¹

これらの攻撃によるデータ損失の甚大さを考慮した場合、組織の内部を守るセキュリティ対策がこれまで以上に重要となってきていると言えます。

²⁹ <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158>

³⁰ <http://blog.trendmicro.com/trendlabs-security-intelligence/may-2013-patch-tuesday-includes-critical-ie-8-zero-day-issue/>

³¹ http://about-threats.trendmicro.com/Search.aspx?language=jp&p=BKDR_POISON

2013 年に標的となった業界



2013 年に発生した持続的標的型攻撃では、政府関連機関が最も多くの被害に見舞われました。

註：上図は、2013 年にトレンドマイクロでモニタリングした持続的標的型攻撃に基づいて作成したものです。

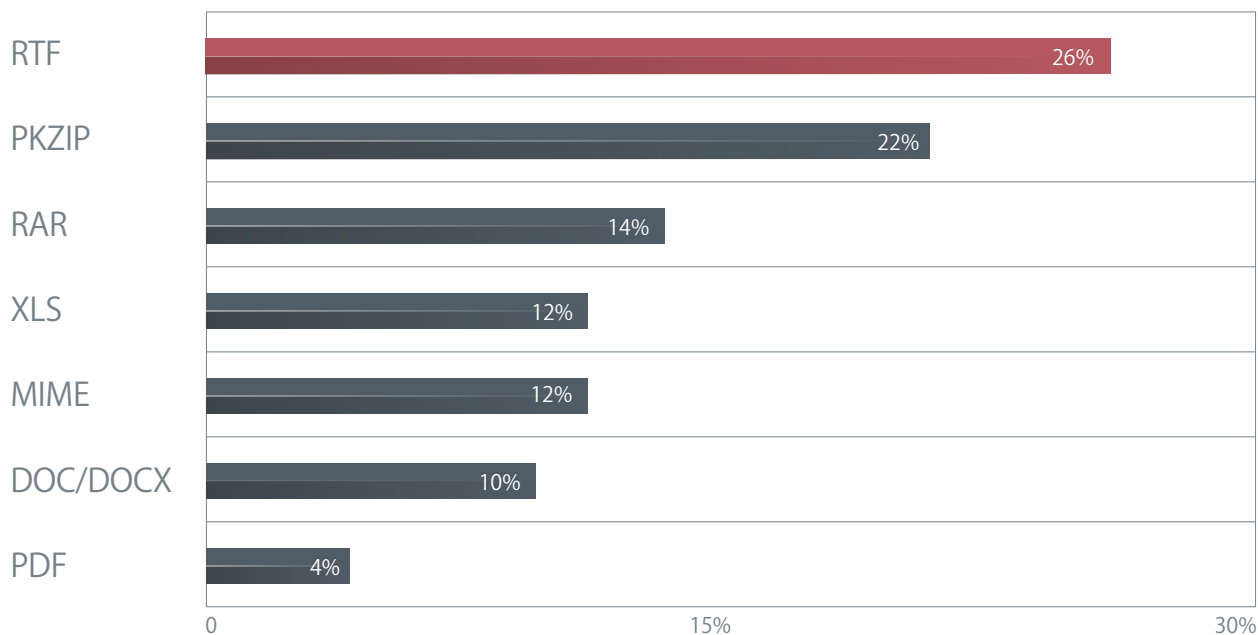
2013 年に標的となった国や地域



2013 年、持続的標的型攻撃は、特定の国や地域に限らず発生したようです。ただし、アジア地域では特に日本と台湾が集中して標的となりました。

註：上図は、2013 年にトレンドマイクロでモニタリングした持続的標的型攻撃に基づいて作成したものです。

2013 年の持続的標的型攻撃においてスパイフィッシングメールに使用された添付ファイルの形式



.RTF ファイルが最も多く利用された形式であり、その次に .PKZIP 形式が続きます。これは、.RTF ファイルが複数のプラットフォームでの文書交換が可能であることと、.PKZIP ファイルの場合は、ほとんどのセキュリティソフトウェアが、圧縮されたファイルのスキャンを行わないことに起因しているといえます。

註：上図は、2013 年にトレンドマイクロでモニタリングした持続的標的型攻撃に基づいて作成したものです。

2013 年は、持続的標的型攻撃のさまざまな作戦活動（キャンペーン）が、それぞれに特化した手法を駆使していたことが確認された年でもありました。キャンペーン「Safe」の場合、Microsoft Office の脆弱性「CVE-2012-0158」を利用したスパイフィッシングメールを用いており³²、攻撃者は、わずか2台のコマンド&コントロール (C&C) サーバに接続する 100 カ国に及ぶ 1 万 2000 もの固有 IP アドレスを使用していました。キャンペーン「EvilGrab」は、主にアジア太平洋地域の組織を標的にしており、攻撃者が標的を限定していることを如実に示した事例といえます。このキャンペーンでは、各種のカスタマイズが施され、「Tencent QQ」のデータを狙っていたことも確認されました。³³ 調査では、「EvilGrab」のキャンペーン活動の 89%は、政府系組織を標的にしていたことも判明しました。³⁴

³² <http://blog.trendmicro.com/trendlabs-security-intelligence/hiding-in-plain-sight-a-new-apt-campaign/>

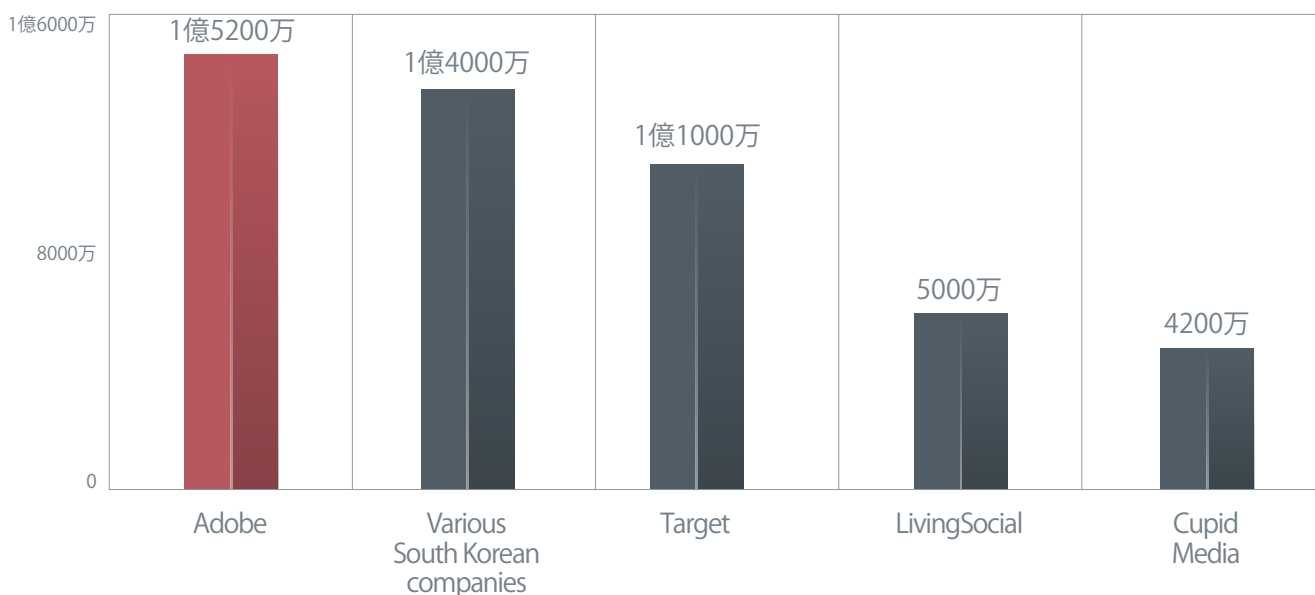
³³ <http://blog.trendmicro.co.jp/archives/7886>

³⁴ <http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/2q-report-on-targeted-attack-campaigns.pdf>

増加する情報漏えいの事例

大手企業が標的にされていた事実が発覚する中、大規模な情報漏えい事例も2013年に多く発生しました。例えば、「Evernote」は、2013年3月に情報漏えいの被害に見舞われ、5000万にも及ぶユーザのパスワードをリセットする必要に迫られました。³⁵ 2013年5月に発生した「LivingSocial」の情報漏えい事例も、ほぼ同数の被害規模となりました。³⁶ さらに「Identity Theft Resource Center (ITRC)」の報告では、医療業界も全体で267件にも及ぶ情報漏えい被害に見舞われており、これは400万人分以上の診療記録の消失に相当にします。³⁷

2013年に発生した大規模情報漏えい事例



このように多様な企業が大規模な情報漏えい被害を受けたことは、どのような企業も規模を問わず、こうしたサイバー攻撃を受ける可能性があることを示しているといえます。

現実世界に甚大な被害を及ぼすサイバー攻撃

2013年3月初旬、「MBR Wiper」攻撃が韓国へ仕掛けられ、複数の主要銀行やメディア企業が業務不能に陥りました。これにより、多くの韓国人は、ATMから現金を引き出せなくなり、ニュース番組のスタッフも報道を行うことができなくなりました。³⁸ さらにもう一つ、破壊的な攻撃が2013年6月25日、韓国へ仕掛けられ、同国のセキュリティ警告がレベル1から3へ引き上げられました。この攻撃では、複数の政府関連機関やニュースサイトも被害を受けました。³⁹ これらの事例は、サイバー攻撃がどれだけ破壊的な被害を現実世界にもたらすことができるかを示したといえるでしょう。

³⁵ <http://www.nbcnews.com/technology/evernote-resets-50-million-passwords-after-hackers-access-user-data-1C8659106>

³⁶ <http://www.bna.com/livingsocial-reveals-cyberattack-n17179873787/>

³⁷ <http://www.idtheftcenter.org/images/breach/2013/BreachStatsReportSummary2013.pdf>

³⁸ <http://blog.trendmicro.co.jp/archives/7436>

³⁹ <http://blog.trendmicro.co.jp/archives/6923>

脆弱性と 익스プロイト

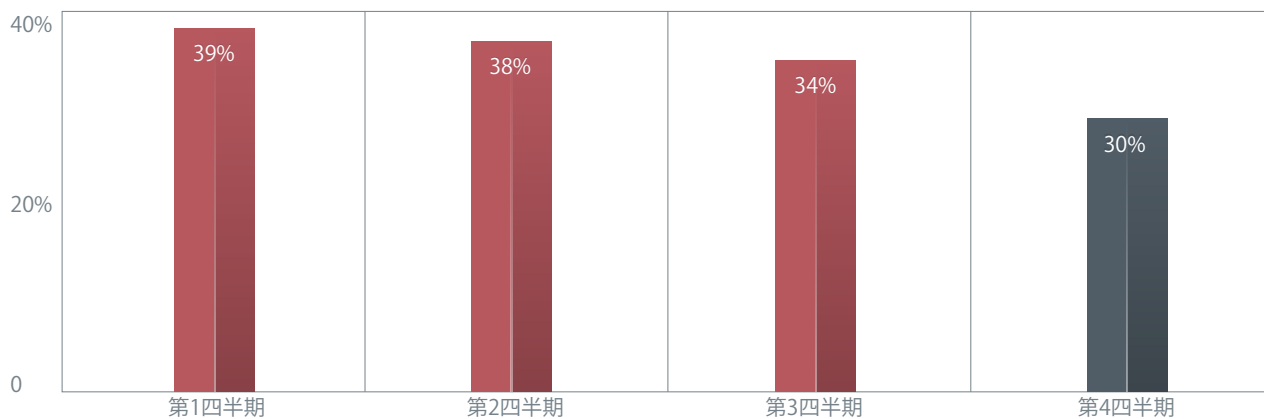
Java 脆弱性に代表されるサポートが終了した古いソフトウェアを狙う手口が問題に

「脆弱性の修正不可」問題

修正パッチを適用していなかったり、サポート終了したソフトウェアを使い続ける PC は依然存在することから、2013 年も攻撃者は、新たな脆弱性を探す必要はありませんでした。この傾向は、攻撃者が特にサポートの終了した Java 6 を継続して狙っていた事実から確認できました。76% の企業や組織が Oracle によるサポート終了後も、Java 6 を使用しており、実際、2013 年に発生した Web からの攻撃全体の実に 91% が Java の脆弱性に関連することからも疑問の余地はありません。⁴⁰

攻撃者は、Java 以外にも同じような「利用しやすい脆弱性」を狙っていました。その好例がオペレーティングシステム (OS) の Windows XP です。2012 年 7 月から 2013 年 7 月の間に Windows XP に関連する Microsoft セキュリティ情報が 45 件もリリースされたことから明らかといえます。⁴¹ 世界中の PC の実に 30% が現在もこの OS を使用している中、2014 年 4 月にサポートは終了するため、Windows XP を使用している PC は一層この種の攻撃に対して脆弱となります。⁴² この事実は、銀行業務へも深刻な問題をもたらすことにもなります。米国の現金自動預入支払機 (ATM) の 95% 以上が現在も Windows XP を使用しているからです。⁴³

2013 年 Windows XP 使用者の推移



Microsoft のオペレーティングシステム (OS) の中で Windows XP の占める割合は、2013 年、徐々に減少しました。2014 年 4 月のサポート終了が主な理由といえます。サポートが終了することで、ユーザは各種の脅威、特に未修正の脆弱性に対して注意が必要となり、OS をアップグレードするか、少なくともセキュリティソフトによる対応を求められることとなります。(出典：NetMarketshare.com)

⁴⁰ https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

⁴¹ <http://www.pcworld.com/article/2046839/zero-day-forever-move-away-from-windows-xp-now.html>

⁴² <http://www.pcmag.com/article2/0,2817,2429423,00.asp>

⁴³ <http://www.foxnews.com/tech/2014/01/17/atms-running-windows-xp-and-wildly-out-date/>

TrendLabs 2013 年間 セキュリティラウンドアップ

2013 年 2 月、「Adobe® Flash®」や「Adobe Reader®」が、不正な .SWF ファイルや不正な .PDF ファイルが添付されたスパムメール送信による攻撃を受けました。^{44 45}

「Ruby on Rails™」などのサーバ側の脆弱性も 2013 年 5 月に発生し、これにより攻撃者は、感染させたサーバを不正な「Internet Relay Chat (IRC) ボット」に変更することが可能になりました。⁴⁶ 2013 年 6 月に確認された「Plesk」のゼロデイ脆弱性利用の場合、攻撃者は、Web サーバのコントロールを取得することが可能になりました。また、2013 年 10 月に発生した Web アプリケーション開発プラットフォーム「ColdFusion」のソースコード窃取では、サイバー犯罪者は、すでにセキュリティが確保された IT オペレーションへの権限さえ取得することが可能になりました。これらの事例は、Web サーバのセキュリティを保持し、各 PC のパッチ処理を行うことが、とりわけ企業の IT 環境でいかに重要であるかを知らしめたといえます。⁴⁷

2013 年、脆弱性を利用するエクスプロイト攻撃では、Windows もかなりの割合を占めました。例えば、2013 年 11 月、脆弱性「CVE-2013-5065」を利用した攻撃では、攻撃者は、感染した PC を権限昇格により、完全な制御下におくことが可能となりました。この脆弱性は、不正な PDF ファイルを介したエクスプロイトでも利用され、持続的標的型攻撃のキャンペーンの一部として、感染した PC にバックドア型不正プログラムをもたらす事例が発生しました。⁴⁸ なお、この脆弱性には、すでに修正パッチが提供されています。

2013 年は、過去に悪用された脆弱性が、現在も有効であることが示された年でもありました。過去の脆弱性が存在するソフトウェアに対して、ユーザ側の何らかの理由により、適切なパッチ適用やアップグレードが実施されていなかったためです。これにより、攻撃者は、容易に攻撃を成功させました。ユーザ側の対応が変わらないかぎり、2014 年も同じ状況が続くこととなります。

⁴⁴ <http://blog.trendmicro.co.jp/archives/6674>

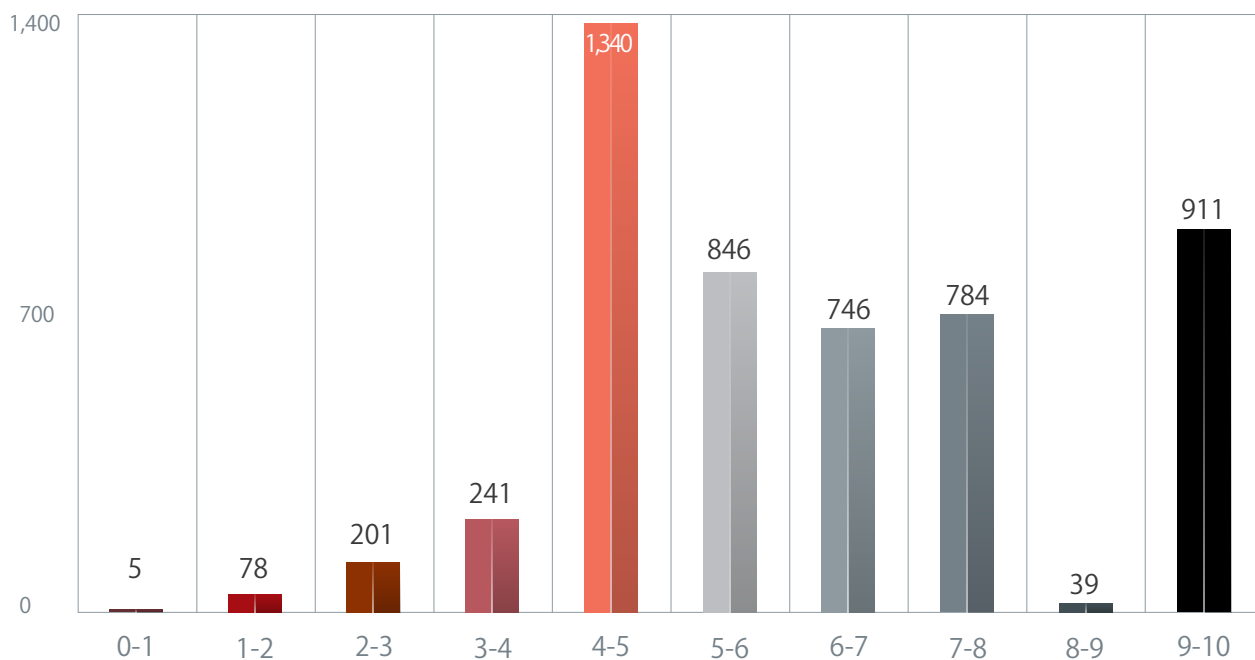
⁴⁵ <http://blog.trendmicro.co.jp/archives/6711>

⁴⁶ <http://blog.trendmicro.co.jp/archives/7329>

⁴⁷ <http://blog.trendmicro.co.jp/archives/7385>

⁴⁸ <http://blog.trendmicro.co.jp/archives/8238>

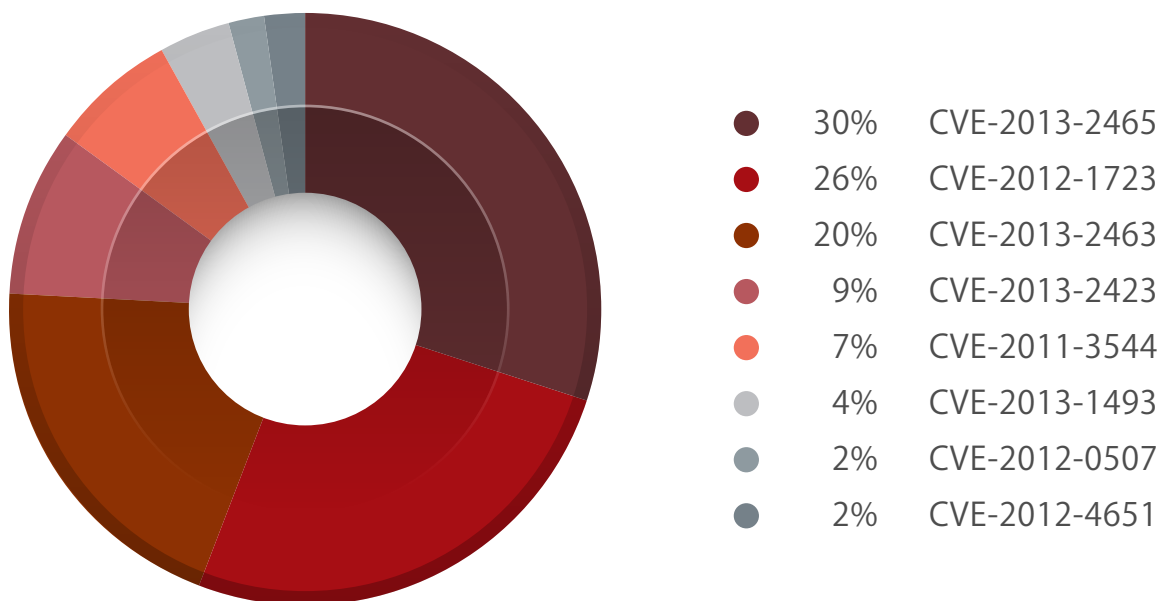
2013 年に発生した脆弱性の CVE 深刻度別の分布



「CVEdetails.com」によると、2013 年に確認された脆弱性の 62% が深刻度「中 (4.0-6.9)」、約 30% が深刻度「高 (7.0-10.0)」でした。この割合は、2012 年から大きく変わっていません。ユーザ側では、ソフトウェアの更新および最新バージョンへのアップグレードを怠らず、万一、修正パッチがリリースされていない脆弱性に関しては信頼のおけるセキュリティソフトを使用する等、細心の注意が必要です。

出典：CVEdetails.com

最も多く利用されたブラウザ関連の Java の脆弱性



上図は、トレンドマイクロの「Browser Exploit Prevention System」のデータに基づき、Java 6 および Java 7 において 2013 年に最も多く利用されたブラウザ関連の脆弱性を示したものです。このデータによると、サイバー犯罪者は、古い脆弱性も、新規の脆弱性同様に利用しようとしていたことが分かります。

註：この数値は、1ヶ月継続した脆弱性攻撃で 2013 年にトレンドマイクロでモニタリングした Java 関連の脆弱性の範囲から割り出しています。

ソーシャル&クラウドの脅威

ソーシャルメディアや、個人向けクラウドサービス、オンライン口座の利用等、ユーザ生活のデジタル化が進む中、国家レベルの個人情報の監視体制の発覚は、デジタル情報に対するリスクへの気づきに

「ソーシャルエンジニアリング」 + 「ソーシャルメディア」 = 「金銭目的の不正活動」

サイバー犯罪において、従来からの“常とう手段”である金銭目的の手口は、個人情報の安全という点でも大きな懸案となっています。2013年、「アメリカ国家安全保障局（National Security Agency、NSA）による膨大な量の個人情報収集に関する報道と合わせ、個人情報に対するこれまで知られていなかった「収集法」や「利用法」も、新たな懸案として浮かび上がってきました。⁴⁹ 他方、ソーシャルメディアを悪用するサイバー犯罪者は、2013年も、粛々と活動を進めていました。

サイバー犯罪者がユーザに不正なリンクをクリックさせたり、不正プログラムをダウンロードさせたり、あるいは誤って個人情報を漏えいさせる上では、ここ数年、ソーシャルエンジニアリングが最も有効な手段となっています。2013年は、「PlayStation 4[®]」や「Xbox[®] One」など待望のゲーム機発売、ハロウィンのお祝い、台風30号「ハイアン」による深刻な被害といったトピックをソーシャルエンジニアリングへ悪用した事例が確認されました。

ソーシャルエンジニアリングで多用されたトピック



例年どおり、サイバー犯罪は、できるだけ多くのユーザを狙うため、話題になった社会問題や、出来事、映画、ガジェット、自然災害などをソーシャルエンジニアリングの材料にしました。

⁴⁹ <http://www.zdnet.com/obama-unveils-nsa-reforms-keep-calm-and-carry-on-spying-7000025303/>

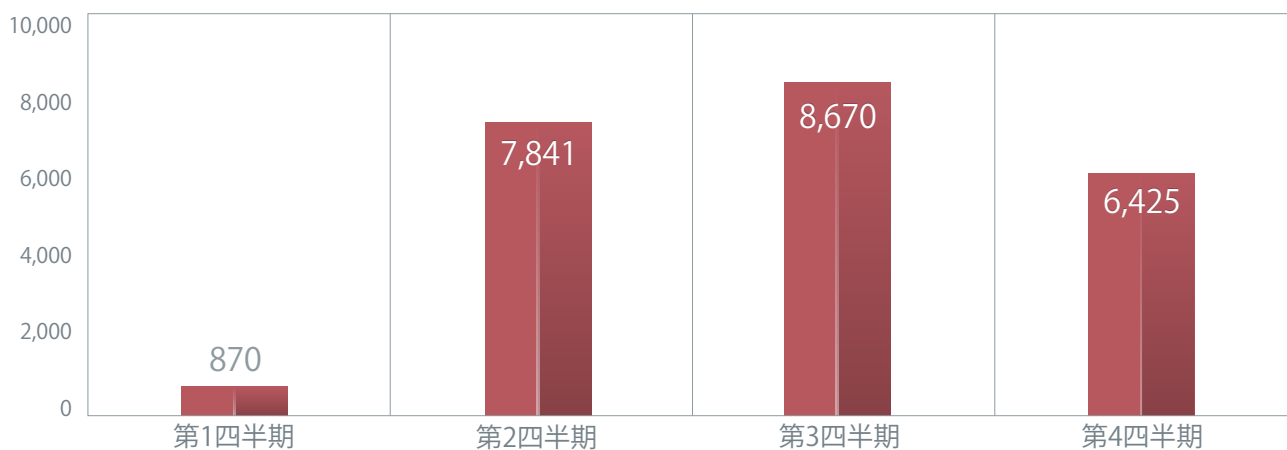
TrendLabs 2013 年間 セキュリティラウンドアップ

2013 年も引き続き、さまざまな人気のソーシャルメディアが標的にされました。Facebook 関連の詐欺事例も増加を続け、Facebook のメッセージアプリもターゲットとなりました。^{50 51 52 53} Twitter では、2013 年 4 月初旬の大規模なアカウントハッキング事例後、早くも同年 10 月には、さまざまなハッキングツールが不正な Twitter アカウントを介して提供されていたことも確認されました。^{54 55}

Pinterest の場合、「Blackhole Exploit Kit」によるスパムメール送信活動において名称が借用されていた以外、大きな攻撃に見舞われることはありませんでした。一方、Tumblr を介した詐欺目的の偽ビデオストリーミングサイトの拡散も確認されました。^{56 57} 2013 年のソーシャルメディア関連で最も注目された脅威は、Instagram を狙った攻撃です。同サイトの偽アカウントや「無料フォロワー獲得」詐欺は、2013 年を通して増加し続けました。^{58 59}

こうしたソーシャルメディアの喧騒の中でも、最も儲かる手口は、依然フィッシング詐欺であり、Apple ID を窃取されたユーザの事例からも明らかのように⁶⁰、フィッシング詐欺は、犯罪者にとっての格好の金儲けの手段となっています。

2013 年：Apple 関連のフィッシングページの増加傾向



2013 年、Apple ID を狙ったフィッシング攻撃の増加を確認。そのいくつかは、Apple ID だけでなく、支払い用の住所やその他の個人情報や金融関連情報も狙っていました。

⁵⁰ <http://blog.trendmicro.co.jp/archives/7938>

⁵¹ <http://blog.trendmicro.co.jp/archives/7037>

⁵² <http://blog.trendmicro.co.jp/archives/7000>

⁵³ <http://blog.trendmicro.co.jp/archives/7192>

⁵⁴ <http://blog.trendmicro.co.jp/archives/7978>

⁵⁵ <http://blog.trendmicro.com/trendlabs-security-intelligence/another-day-another-twitter-hack/>

⁵⁶ <http://blog.trendmicro.co.jp/archives/7516>

⁵⁷ <http://blog.trendmicro.co.jp/archives/7182>

⁵⁸ <http://blog.trendmicro.co.jp/archives/7442>

⁵⁹ <http://blog.trendmicro.co.jp/archives/7270>

⁶⁰ <http://blog.trendmicro.co.jp/archives/7930>

Web サイト上に多くの個人情報を公開することは、サイバー犯罪者に対して金銭目的で悪用できるエサを提供しているようなものだという点をユーザは理解する必要があります。サイバー犯罪のアンダーグラウンドでは、こうした情報は、当たり前の商品として出回っており、ビジネスモデル化⁶¹されています。氏名や住所、クレジットカード番号にとどまらず、さまざまな重要情報を集めたコレクションは、「Fullz」などと呼ばれ、何も知らないユーザから窃取された情報は、現在もアンダーグラウンドフォーラム等で売り捌かれています。

ユーザを取り巻くデジタル情報への脅威は、とりわけ国家による一般市民の情報収集活動が発覚したことで大きな不信感が広がり、「今日のデジタル化時代に、プライバシーは存在しないのか?」という疑問を抱かずにはいられない状況を招いています。

⁶¹ <http://blog.trendmicro.co.jp/archives/6856>

別表

2013 年オンライン銀行詐欺ツール四半期ごとの検出数：国別トップ 10

第 1 四半期	
国名	割合
米国	33%
ブラジル	10%
オーストラリア	5%
台湾	5%
カナダ	4%
日本	3%
インド	3%
フランス	3%
フィリピン	3%
ドイツ	2%
その他	29%

第 2 四半期	
国名	割合
米国	28%
ブラジル	22%
オーストラリア	5%
フランス	5%
日本	4%
台湾	4%
ベトナム	3%
インド	2%
ドイツ	2%
カナダ	2%
その他	23%

第3 四半期	
国名	割合
米国	23%
ブラジル	16%
日本	12%
インド	6%
オーストラリア	3%
フランス	3%
ドイツ	2%
ベトナム	2%
台湾	2%
メキシコ	2%
その他	29%

第4 四半期	
国名	割合
米国	22%
日本	19%
ブラジル	12%
台湾	6%
フランス	5%
ドイツ	3%
インド	3%
カナダ	2%
オーストラリア	2%
イタリア	2%
その他	24%

2013 年第3 四半期と第4 四半期、日本では「ZBOT」の検出数が増大。これは、日本でのサイバー犯罪活発化や、過去数年は狙われていなかった日本が新たにオンライン銀行詐欺ツールの標的となってきたことを示しています。

2013 年ボットネットの C&C サーバの数が最も多い国：トップ 10

第1 四半期	
国名	割合
米国	36%
オーストラリア	11%
韓国	6%
中国	6%
ドイツ	3%
イギリス	3%
ブラジル	2%
イタリア	2%
台湾	2%
チリ	2%
その他	27%

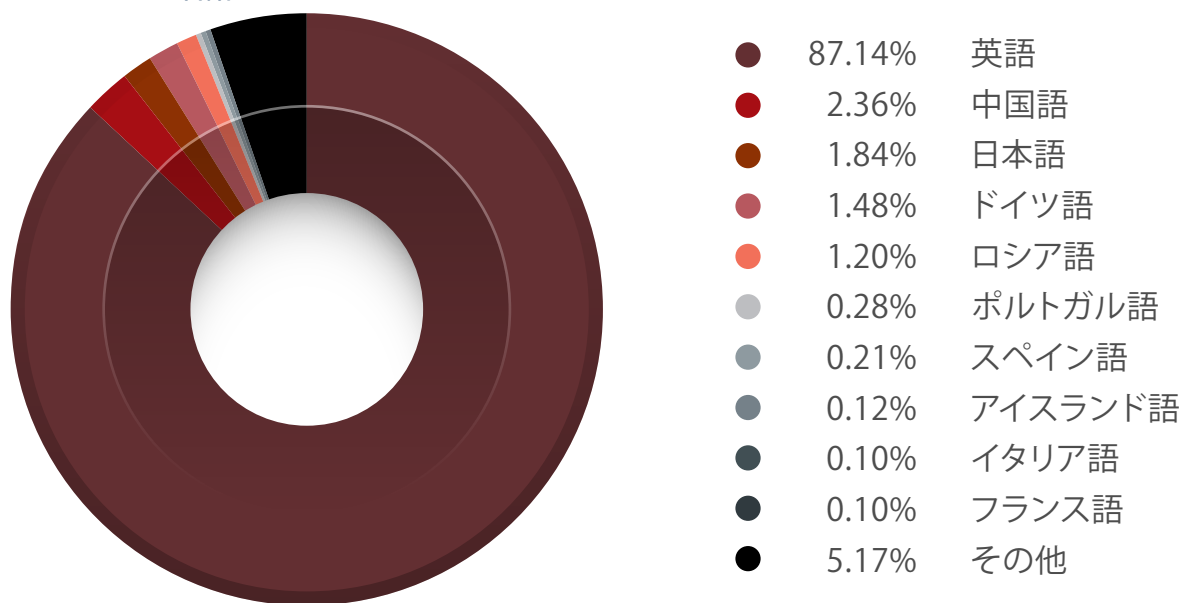
第2 四半期	
国名	割合
米国	24%
オーストラリア	5%
韓国	3%
中国	3%
ドイツ	3%
台湾	2%
フランス	2%
イギリス	2%
ブラジル	1%
カナダ	1%
その他	54%

第3 四半期	
国名	割合
米国	14%
ウクライナ	7%
ロシア	3%
ドイツ	3%
中国	2%
台湾	2%
オーストラリア	2%
韓国	2%
イギリス	2%
オランダ	1%
その他	62%

第4 四半期	
国名	割合
イギリス	17%
米国	15%
ウクライナ	4%
ドイツ	3%
オランダ	3%
ロシア	3%
中国	2%
オーストラリア	1%
韓国	1%
インド	1%
その他	50%

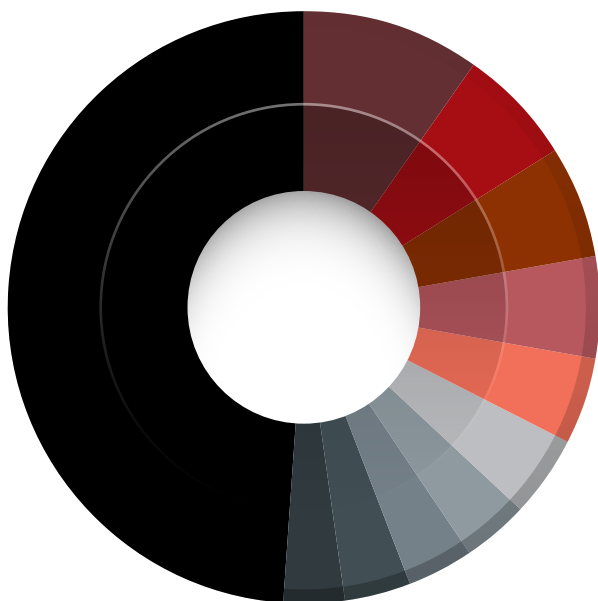
2013 年の大半において銀行関連の被害は常に米国がトップですが、オンライン銀行詐欺ツールの感染被害は世界規模で拡大していることが分かります。2013 年第3 四半期、感染先のターゲットは、上位常連のアメリカからヨーロッパ地域へ移行しています。

スパムメールの言語：トップ10



世界規模で最もよく使用されることから、英語がスパムメール送信者が最も好む言語となっています。

スパムメールを送信する国：トップ 10



- 10% 米国
- 6% スペイン
- 6% インド
- 5% アルゼンチン
- 5% イタリア
- 4% 台湾
- 4% コロンビア
- 4% 中国
- 4% ペルー
- 3% メキシコ
- 49% その他

スパム使用言語とも一致し、米国が最も多くのスパムメールを送信した国としてトップに位置しています。アルゼンチン、コロンビア、メキシコ、ペルーなど南アメリカの国々、さらにスペインもトップ 10 入りしています。

2013 年不正 URL ホスト国：トップ 10

国名	割合
米国	24%
オランダ	4%
ドイツ	3%
中国	3%
日本	3%
韓国	2%
フランス	2%
ロシア	2%
イギリス	1%
カナダ	1%
その他	55%

トレンドマイクロがアクセスをブロックした不正 URL の多くが米国に存在していました。

2013 年不正な Web サイトへ最も多くアクセスした国：トップ 10

国名	割合
米国	29%
日本	15%
中国	7%
インド	5%
台湾	5%
韓国	4%
ロシア	3%
オーストラリア	3%
ドイツ	3%
イタリア	2%
その他	24%

不正な URL へアクセスの大半のユーザが米国のものとなりました。

2013 年不正な Android アプリの数が最も多い国：トップ 10



● ベラルーシ	10%
● ブルガリア	5%
● ベトナム	5%
● アルゼンチン	5%
● ロシア	4%
● ウクライナ	4%
● カナダ	2%
● インド	2%
● フランス	2%
● イタリア	2%

不正な Android アプリの数が最も多い国としては、ベラルーシがトップでした。これは、この国でのスマートフォンの急速な普及も要因の 1 つと考えられます。⁶²

註：ランキングは、スキャンしたすべてのアプリに対して「不正」と評価されたアプリのパーセンテージを国別に比較して割り出しています。また、このランキング対象は、アプリへのスキャンが少なくとも 1 万回以上確認された国に限定しています。

2013 年アプリ使用によるプライバシー侵害のリスクが最も高い国：トップ 10



● ウガンダ	17%
● サウジアラビア	17%
● ブルガリア	11%
● インド	9%
● アルゼンチン	8%
● ウクライナ	8%
● カナダ	6%
● インドネシア	6%
● イタリア	6%
● シンガポール	6%

ウガンダが「アプリ使用によるプライバシー侵害のリスクが最も高い国」としてトップであり、この国は 2013 年を通して上位に位置していました。

註：ランキングは、スキャンしたすべてのアプリに対して「不正」と評価されたアプリのパーセンテージを国別に比較して割り出しています。また、このランキング対象は、アプリへのスキャンが少なくとも 1 万回以上確認された国に限定しています。

⁶² <http://www.telecompaper.com/news/mts-belarus-smartphone-penetration-jumps-to-25--991402>

TREND MICRO™

本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。

トレンドマイクロ株式会社が書面により事前に承諾している場合を除き、形態および手段を問わず本書またはその一部を複製することは禁じられています。本書の作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容は予告なしに変更される場合があります。

本書に記載されている各社の社名、製品名、およびサービス名は、各社の商標または登録商標です。

〒151-0053

東京都渋谷区代々木 2-1-1 新宿マインズタワー
大代表 TEL : 03-5334-3600 FAX : 03-5334-4008

<http://www.trendmicro.co.jp>

TRENDLABSSM

フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 ヶ所の各国拠点と連携してソリューションを提供しています。

数カ月におよぶ厳しいトレーニングを経て最終合格率約 1% の難関を突破した、選びぬかれた 1,000 名以上の専門スタッフが、脅威の解析やソリューションへの反映など、24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

世界中から収集した脅威情報を、各種レピュテーションデータベースや不正プログラム、迷惑メールなどの各種パターンファイルなど、グローバル共通のソリューションに随時反映しています。

サポートセンターの役割も兼ねる研究所として、お客様に満足いただけるサポート体制を整備し、より多くの脅威に迅速に対応しています。

Trend Micro Incorporated, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. For more information, visit www.trendmicro.com.

©2014 Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



Securing Your Journey
to the Cloud