フィッシング対策協議会
Council of Anti-Phishing Japan

フィッシングレポート 2015

－　進む対策、利用者としてできること　－

平成 27 年 9 月

フィッシング対策協議会

ガイドライン策定ワーキンググループ

フィッシング対策協議会
Council of Anti-Phishing Japan

目次

1. フィッシングの動向

1.1. 国内の状況

2013 年に急増したフィッシング被害は、2014 年も増加し続け、さらに深刻化している。オンラインゲームを騙るフィッシング報告が増加しているのが 2014 年のフィッシングの特徴である。

また、警察庁の発表[1]によれば、インターネットバンキング利用者の口座情報を様々なウイルスやマルウエアを用いて盗み取り、利用者の口座から不正送金する手口がさらに悪質・巧妙化することで被害が拡大している。平成 25 年には 1,315 件、約 14 億 600 万円だった被害額が、平成 26 年には 1,876 件、約 29 億 1000 万円の被害が発生しており、件数で約 1.4 倍、被害額では約 2 倍に達した。

フィッシング対策協議会の統計でも、2014 年のフィッシング届出件数は 1 月に急増し、その後も高い水準が続いたが、夏ごろから減少傾向に転じた。ただし、2015 年 1 月には再び増加するなど、警戒すべき状況が続いている。これは、金融機関を対象としたフィッシングの届出が急増したためである(図 1-1)。ただし、件数的にはオンラインゲームのフィッシングが大半を占める状況に変わりはない。

フィッシング対策協議会に対するフィッシング情報の届出件数は 2014 年度で、対前年度若干減少し（2013 年度 15,171 件、2014 年度 14,085 件)、フィッシングサイトの件数は 1.6 倍に増加し(図 1-2)2013 年度 2,522 件、2014 年度 4,110 件、ブランド名を悪用された企業の延べ件数は 2013 年度 136 件、2014 年度 153 件であり、前年に比べ微増となった（図 1-3)。

近年の傾向として、フィッシングの対象となるブランド数は頭打ちの傾向にある、つまり犯罪者がターゲットとするブランドが固定化しつつある。

[1] 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

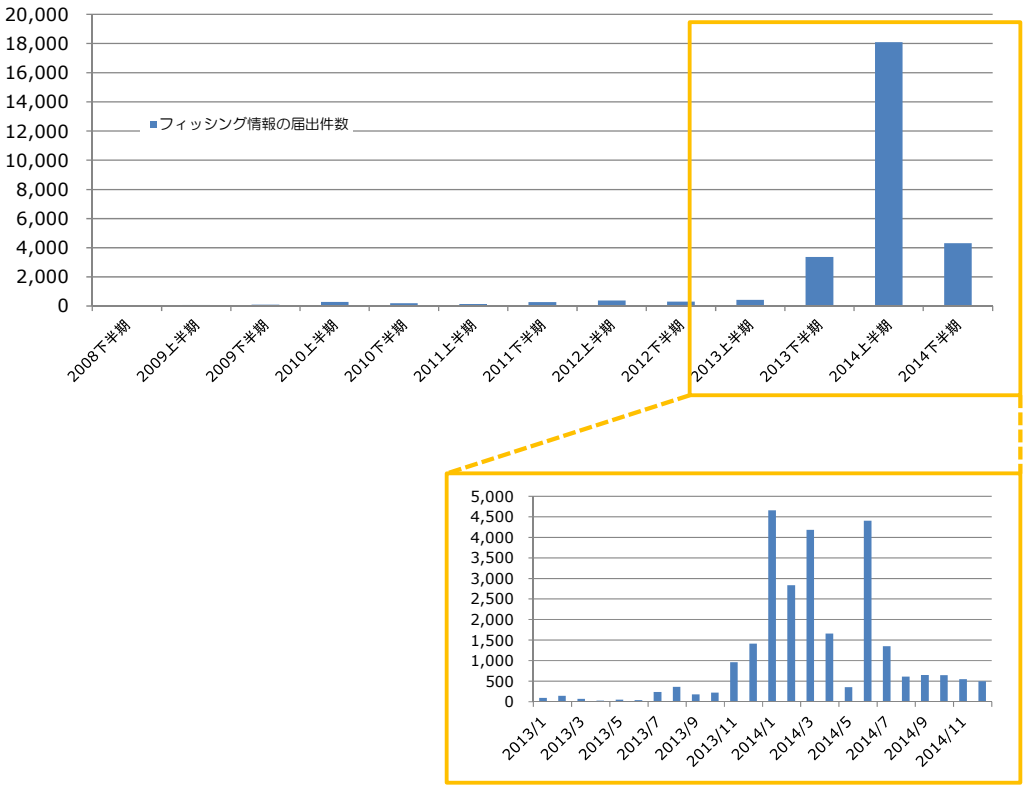


図 1-1　フィッシング情報の届出件数

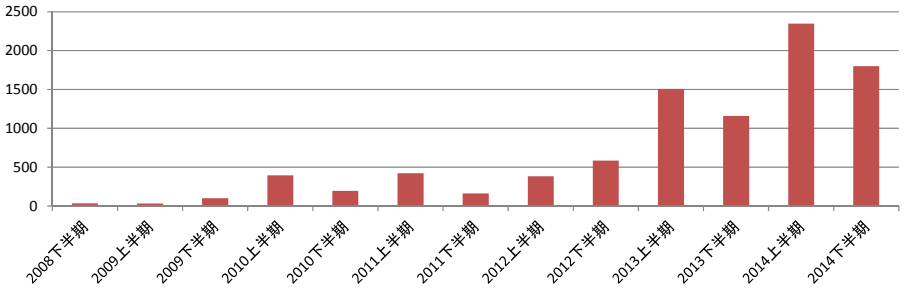


図 1-2　フィッシングサイトの件数

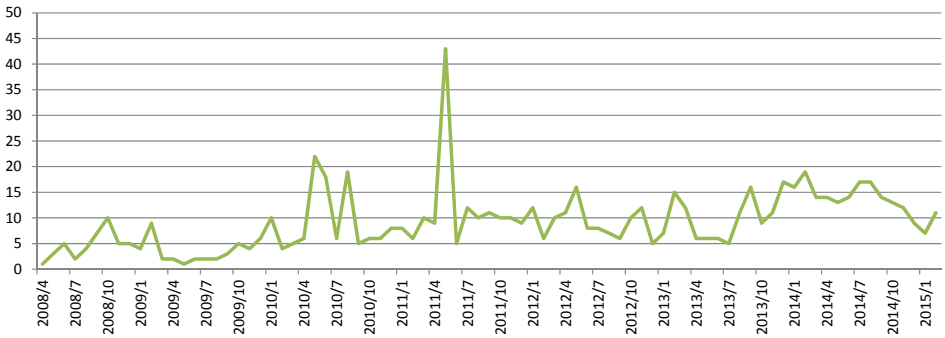


図 1-3　ブランド名を悪用された企業の件数

また、国家公安委員会・総務省・経済産業省の発表によれば、警察庁に報告のあった不正アクセス行為として、識別符号窃用型不正アクセス行為（ID 窃盗による不正アクセス行為）は昨年度に比べて減少した（図 1-4）。また、その手口を見ると、2014 年（平成 26 年）におけるフィッシングは 71 件であり、比率は約 21%となっている（図 1-5）。

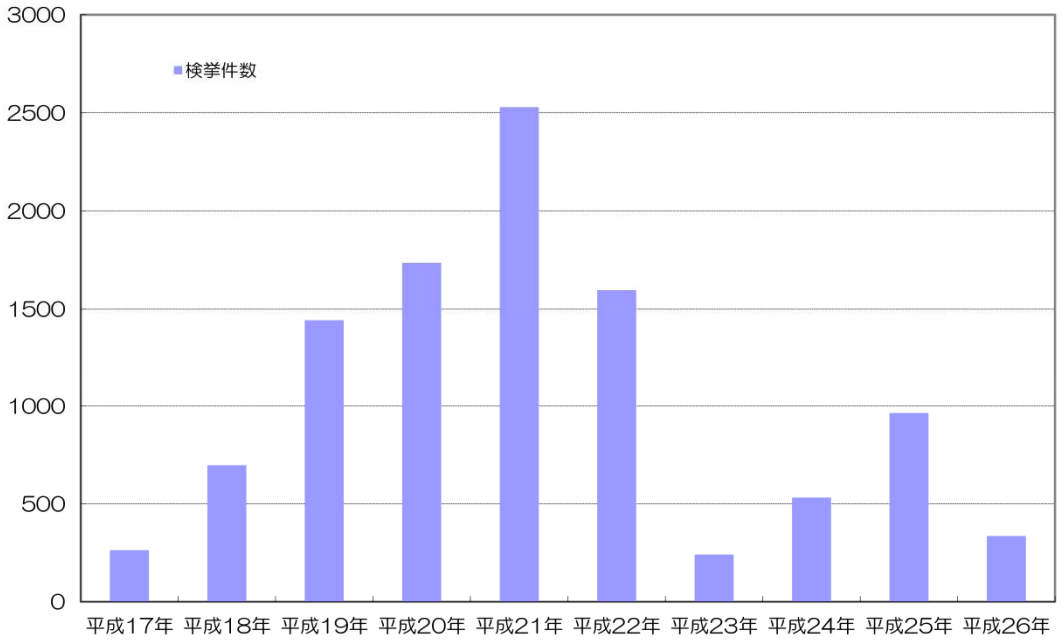


図 1-4　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数[2]

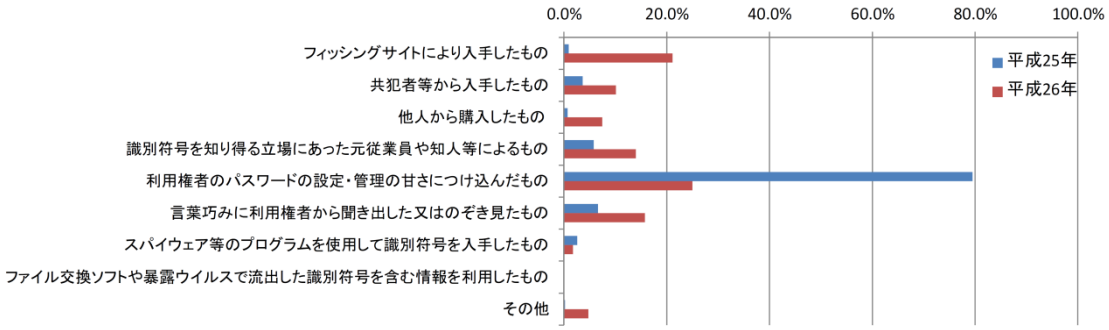


図 1-5　不正アクセス行為に係る犯行の手口の内訳（平成 25 年、平成 24 年）[3]

[2] 国家公安委員会・総務省・経済産業省,「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」,等、http://www.npa.go.jp/cyber/statics/h26/pdf041.pdf よりフィッシング対策協議会が作成
[3] 同上

近年特に問題となっているのは、狭義のフィッシングではなく、様々な手法を駆使して利用者情報を盗み取り、利用者の銀行口座から不正送金させるインターネットバンキングを狙った不正送金事件である。

警察庁の発表[4]によれば、平成 24 年には 64 件、約 4,800 万円だった被害額が、平成 25 年には 1,315 件、約 14 億 600 万円、平成 26 年には 1,876 件、約 29 億 1000 万円に達している。

1.2. 海外の状況

米国で設立されたフィッシング問題に関する国際組織 APWG（Anti-Phishing Working Group）の調査によれば、2014 年下期のフィッシング届出件数は、2014 年上期に引き続き過去最高水準となった（図 1-6）。引き続き注意が必要である。

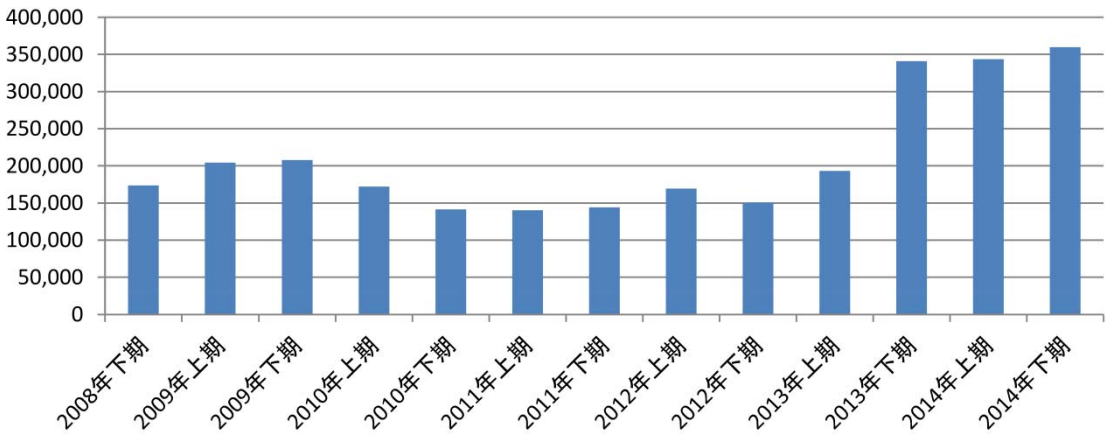


図 1-6　APWG へのフィッシングメール届出件数[5]

[4] http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf

[5] APWG (Anti-Phishing Working Group), "Phishing Activity Trends Report"、http://www.antiphishing.org/index.html、よりフィッシング対策協議会にて作成

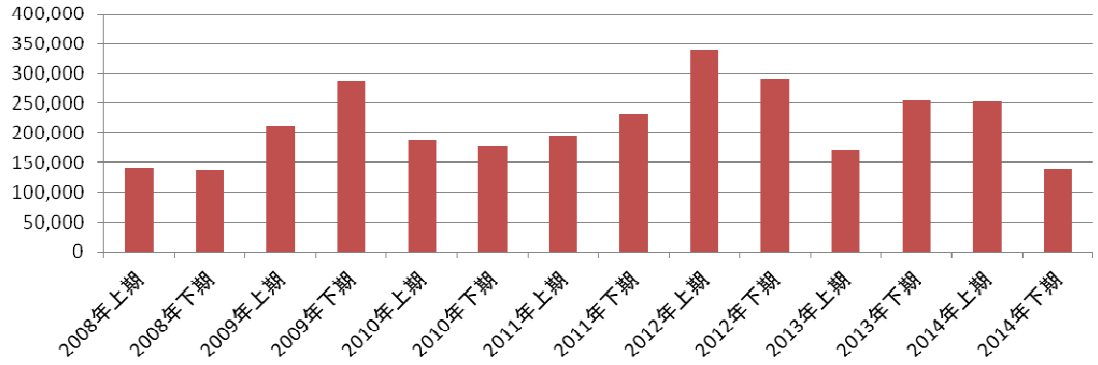


図 1-7　フィッシングサイトの件数（APWG）[6]

図 1-8　フィッシングによりブランド名を悪用された企業の件数（APWG）[7]

[6] APWG (Anti-Phishing Working Group), "Phishing Activity Trends Report"、http://www.antiphishing.org/index.html、よりフィッシング対策協議会にて作成
[7] APWG (Anti-Phishing Working Group), "Phishing Activity Trends Report"、http://www.antiphishing.org/index.html、よりフィッシング対策協議会にて作成

■コラム：「**STOP. THINK. CONNECT.**」（立ち止まる | 考える | 楽しむ）
ー「インターネット上で自分を守る」ということー

今日、世界中のほとんどの人々がインターネットに接続し、サイバー犯罪に巻き込まれる可能性がある。

日本は世界に先駆けて超高齢化社会を迎えようとしている中、すべての人が情報面で孤立しないようにすることが、この問題を解決するために重要である。「誰かが困っている時は助けを申し出るサイバー空間」の実現をビジョンに掲げ、国際キャンペーンパートナーの一員として、「STOP. THINK. CONNECT.」（立ち止まる | 考える | 楽しむ）日本版の活動がすでに始動している。

この「STOP. THINK. CONNECT.」（以下 STC）キャンペーンは、2010 年 2 月に世界的なネット犯罪対策コミュニティである米国 Anti Phishing Working Group 事務局長の Peter Cassidy 氏が、当時 National Cyber Security Alliance で勤務していた Aimee Larsen-Kirkpatrick 氏と「Optimizing Counter-eCrime Consumer Education Through Unified Online Safety Messaging」を共著で発表し、官民で共有できる統一されたメッセージ発信スキームの構築、メッセージの共鳴と維持、矛盾するメッセージの削減に対する呼びかけが端となっている。

同年 10 月には、米大統領告示[8]において、「民間やコミュニティに根ざした組織や政府機関のパートナーたちと共に、STOP. THINK. CONNECT.という国家レベルのサイバーセキュリティ意識向上キャンペーンを立ち上げるものとする。本イニシアティブを通じて、アメリカ人はサイバー空間のリスクについて学び、意識を高めることができるほか、国家のセキュリティ全体に貢献するための選択ができるようになる。」との宣言を受け、その活動は一気に知名度を高め、全世界へ拡がった。

現在は、アメリカに限らず、16 の国と地域からなる国際活動パートナー[9]がメンバーとして参加している。グローバル版 STC ウェブサイトでは、英語のみならず、スペイン語、フランス語、ポルトガル語、ロシア語など多言語による情報発信が行われている。

[8] http://www.whitehouse.gov/the-press-office/2010/10/01/presidential-proclamation-national-cybersecurity-awareness-month

[9] http://stopthinkconnect.jp/get-involved/international-program/

■日本国内にも拡がる活動

日本では、JPCERT コーディネーションセンター内に STC 普及啓発 WG 事務局を設置している。2014 年 12 月 3 日に、日本版 STC ウェブサイト (http://stopthinkconnect.jp/) の公開が行われた。2015 年 6 月 22 日には、Facebook ページ[10]の開設が行われ、その活動はソーシャルメディアにも拡がっている。2015 年 9 月現在、国内 17 団体がこのキャンペーンに賛同し、活動を推進している。

■STOP. THINK. CONNECT. とは？

歩行者が横断歩道を渡るときには、まず左右の安全確認である。インターネットを安心して利用するための習慣はこれと似ている。インターネットを安心して利用するための 3 つのステップを確認することを推奨している。

- STOP(立ち止まって理解する): インターネットは便利ですが、一般社会と同様、そこには危険もあります。どのような危険があるかを知り、解決策をどのように見つけるかについて、一旦、立ち止まって調べましょう。
- THINK(何が起こるか考える): 様々な警告の見極め方を知る必要があります。警告を確認したら、これから取ろうとする行動がコンピュータやあなた自身の安全を脅かさないか考えましょう。
- CONNECT(安心してインターネットを楽しむ): 危険を理解し、十分な対策をとれば、インターネットをより信頼できるようになるでしょう。

大事なのは、自分自身の身を守ることが、サイバー空間に参加するすべての人に恩恵をもたらし、インターネットをより安全な空間に保つ手助けとなるということである。

■活動成果とその利用

米国の一部企業においては、STC が発行するガイド[11]を使用し、従業員向けのセキュリティ啓発教育を実施するなどの利用事例がある。

また、2014 年 5 月からは『「TWO STEPS」推進・キャンペーン』[12]の実

[10] https://www.facebook.com/StopThinkConnectJapan
[11] http://www.stcguide.com/
[12] http://stopthinkconnect.jp/campaigns/details/?id=474

施など、新たな課題に対する情報配信も積極的に行われている。

日本版 STC での活動としては、活動内容を告知するパンフレット[13]やオリジナルステッカーなどのノベルティを作成し、各種セキュリティイベントでの配布を行っている。

また、日本版 STC サイトでは、第一段階としてグローバル版から抽出した情報を翻訳し配信している。

2015 年 6 月 22 日より、シチュエーション別に安全習慣の実践方法をまとめた『ヒントとアドバイス文書』[14]を配信している。

利用者へ啓発すべきサイバー空間における良識というのは万国共通である。しかし、啓発媒体となるポスターや教育資料の体裁などは国によって好みがかわってくるものである。このため、今後日本人に受け入れられやすいデザインに変更し、展開していくことを検討している。

日本が他国に先駆け突きつけられる課題に対し、答えを模索し、得た知見を全世界へ還元していく。このことも東アジア地域におけるイニシアティブを取っていく上で重要な活動の１つであるといえる。

■お問い合わせ

この啓発活動、および啓発メッセージの普及にご協力いただける企業様、団体様からのお問い合わせを受け付けている。是非、下記事務局へお問い合わせください。

STC 普及啓発 WG 事務局（一般社団法人 JPCERT コーディネーションセンター内）

〒101-0054 東京都千代田区神田錦町 3-17 廣瀬ビル 11 階

E-Mail: stc-sec@antiphishing.jp

主査: 丹京 真一氏(株式会社日立システムズ)

副主査: 林 憲明氏(トレンドマイクロ株式会社)

副主査: 駒場 一民氏(一般社団法人 JPCERT コーディネーションセンター)

[林 憲明　トレンドマイクロ株式会社]

[丹京 真一　株式会社日立システムズ]

[13] http://stopthinkconnect.jp/download/document/274/stc_brochure_low_resolution.pdf

[14] http://stopthinkconnect.jp/resources/

2. 手口の変化・影響の拡大

2.1. ID、パスワードの使いまわしによる被害

サイバー攻撃などで Web サイトから漏えいした ID やパスワードをもとに、他のサイトやサービスへログインを試み、パスワードを使いまわしているユーザの ID へ不正ログインを行い、インターネット上の資産を盗み取るなどの被害が発生している。

具体的には、ユーザのポイントや有償で購入したアイテムを盗むほか、オンラインサイトで勝手に物品を購入されるなどの被害がある。新たな手口としては、SNS サイトへログイン後、そのユーザに成りすまして連絡リストにある友人にプリペイドカードを購入させ、その利用権利を盗むなどの被害も多く確認された。

これらは、「パスワードリスト攻撃」もしくは「リスト型アカウントハッキング」と呼ばれており、2013 年ごろより国内でも確認されてきた被害であるが、特に 2014 年 6 月には大手サービス業者へ集中した被害が発生した。

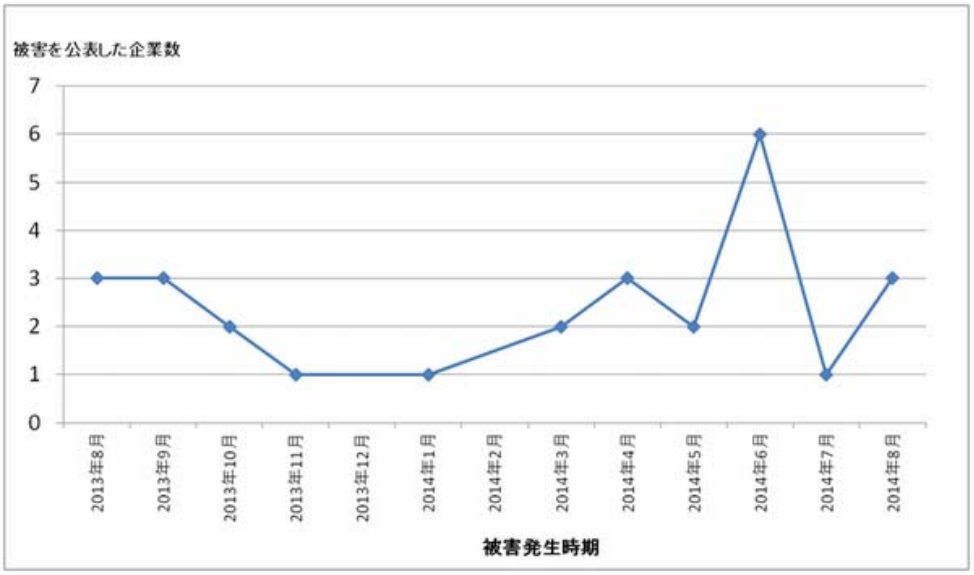


図 2-1 公表情報を元に JPCERT/CC が集計した被害企業の推移

2014 年 6 月に被害を公表した企業では、不正ログインの試行回数が数百万回にのぼり、不正にログインが行われた数は数千から数十万までと多くのユーザの資産が盗まれる、もしくは危険にさらされた。

以下に JPCERT/CC がまとめた、攻撃を受けたことを 2013 年 4 月以降に発

表した企業のうち、「試行件数」と「成立件数」の両方を公表した主なケースを紹介する。

表 2-1 不正ログインの成立率

被害企業	不正ログインの試行件数（A）	不正ログインの成立件数（B）	不正ログイン成立率※（B/A にて算出）
A 社	約 4,600,000	78,361	約 1.70%
B 社	2,293,543	38,280	1.67%
C 社	2,203,590	219,926	9.98%
D 社	約 4,300,000	263,596	約 6.13%
E 社	約 1,600,000	2,398	約 0.15%
F 社	3,420,000	15,092	0.44%
G 社	1,796,629	14,399	0.80%

これらの被害は、ユーザ ID とパスワードを使いまわしていることから発生しており、ID、パスワードの使い回しを行わないように注意喚起することが重要である。

[長谷部　一泰　アルプスシステムインテグレーション株式会社]

2.2. サポート切れソフトウエアの危険性

サポートが切れたソフトウエアは、脆弱性が発見されても対応がなされないため、利用し続けることは危険である。最近では、Windows XP (XP)のサポート切れは大きな問題となった。

昨年 4 月のセキュリティ更新でマイクロソフトは、Windows XP へのソフトウエアの修正の提供を終了し、XP のサポートが終了した。XP は古い Windows 16 ビットアプリケーションのサポートがセキュリティの機能の追加を難しくしていた。マイクロソフトは、Vista 以降に下記のようなセキュリティの機能を追加している。これらの機能は、マルウエアの感染を防ぐのに有効である。

Windows XP 以降に追加されたマルウエアに対する主なセキュリティ強化策

- DEP：XP SP2 より実装 -> EMET へ統合
  データ領域での実行命令を禁止し、バッファオーバーフローによる攻撃を無効化。
- ASLR：Vista より実装 -> EMET へ統合

プログラム実行時のアドレスをランダムに変更し、マルウエアが、特定のアドレスの情報の利用を困難に。

- UAC の導入：Vista より実装
  プログラムを基本は、低い権限レベルで実行させ、管理者権限での実行に確認を要求。
- ドライバ署名：Vista より実装
  64 ビットにおいては、ドライバの署名のチェックを厳密にし、無許可のドライバのインストールを困難に。
- Secure Boot/Trusted Boot：Windows 8 より実装
  OS の起動シーケンス中に不正なコードが挿入されることを無効化。

また、ブラウザである Internet Explorer(以下 IE と呼ぶ)についても IE7 以降に下記のようなセキュリティ機能を追加している。

IE のマルウエアに対するセキュリティ強化

- 保護モード：IE7 より
  ブラウザ動作時の権限を制限することで、悪意のあるコードが自動でインストールされることを防ぐ。
- SmartScreen フィルター：IE7より
  フィッシング攻撃、ソーシャルエンジニアリング、マルウエア、ポップアップに対する保護を行う。IE9 より不正プログラムのダウンロードサイトからの保護が追加。
- クロスサイトスクリプトフィルター：IE8 より
  フィッシング攻撃、ソーシャルエンジニアリング マルウエア、ボップアップに対する保護を行う。
- ドメイン強調表示：IE8 より
  アドレスバーで Web サイト ドメイン名を強調表示し、正しい URL か詐欺サイトかを一目でわかりやすくする。
- ActiveX フィルター：IE8 より
  セキュリティ上のリスクとなりうる ActiveX コントロールをサイト単位でブロックする。
- ダウンロードマネジャー：IE9 より
  全てのダウンロードを一元管理する機能。SmartScreen フィルターと共に動作し、悪意のあるダウンロードから保護する。
- MIME スニッフィングへの対応：IE9 より
  テキストの拡張子と MIME タイプが異なる場合に TXT の拡張子を優先。

- 拡張保護モード：IE10 より
  保護モード機能を拡張し、攻撃者によるソフトウエアのインストール、個人情報へのアクセス、企業イントラネット上の情報へのアクセス、およびシステム設定の変更を防ぐ。
- HTML5 Sandbox：IE10 より
  Iframe でホストされるコンテンツに対して、サンドボックスで実行し、外部のコンテンツの危険な実行を防ぐ。

したがって、ユーザはより最新の OS やアプリケーションを使うことによって、マルウエアへの感染のリスクを減らすことができる。

特に XP については、昨年のサポート終了後に提供された脆弱性については、修正が提供されておらず、攻撃の危険性が高まっている。昨年 11 月に修正が提供された Windows の OLE の二つの脆弱性(MS14-064/CVE-2014-6352, CVE-2014-6332)は、かなりの数の悪用が確認されており、注意が必要である。

CVE-2014-6352 は不正な PowerPoint ファイルを使っての標的型攻撃が、日本でも確認されている。

また、CVE-2014-6332 は、Web サイトに不正な VB スクリプトを仕込むことによって攻撃が可能な為、ブラウザでの Web 閲覧によって、攻撃を受ける可能性がある。さらに本脆弱性は、攻撃者が脆弱性を攻撃するサイトを容易に作成することができるツールキットに組み込まれたことが確認されており、実際、それ以後の脆弱性の悪用が増えていることが確認されている。

このように、XP については、昨年 11 月以降マルウエアへの感染のリスクの危険性がかなり上昇しており、インターネットを利用するには、適さない状態となっているので、利用の中止を推奨する。

[野々下 幸治　トレンドマイクロ株式会社]

2.3. クレジットカードのネット被害

クレジットカードはその利便性の高さから日常生活の様々な場所で使われている。同時に、犯罪者からのターゲットとなり、不正に利用される被害額は少なくない。業界発表によると平成 12 年最高の年間 309 億円もの被害があり、業界全体で対策を行い平成 24 年には 68 億円にまで減少させることができた。しかしながら平成 25 年からは増加し傾向に変わり一般社団法人日本クレジット協会の発表[15]によると平成 25 年には 78.6 億円 そして平成 26 年 1 月から 9

[15] 日本クレジット協会「クレジットカード不正使用被害の集計結果について」
http://www.j-credit.or.jp/information/statistics/download/inv_05_141226.pdf

月までの集計で 78.9 億円の被害が発生しており年間被害額は 100 億円を超える見通しである。その内訳は偽造カードによる被害が 12.8 億円、インターネット等カード番号が盗用される被害が 45.8 億円、盗難などその他が 20.3 億円とネット関連被害が全体の 60%を占めるまでに至っている。

ネット不正の手口は、フィッシングやマルウエアによりカード番号を詐取されてしまったり、クレジットマスターと言われるカード番号を作り出すものソフトウエアによるものがほとんどとなっており、業界全体で捜査当局と連携をはかったり消費者に向けて啓発活動を行っている。

利用者の方は、セキュリティソフトウエアの随時更新やカード利用明細書をよく確認することが望ましい。

[鈴木 哲治 株式会社ジャックス]

2.4. マルウエアを用いたフィッシング被害の拡大

2013 年の下半期から見られたインターネットバンキングを狙うマルウエアの拡大は、2014 年さらに勢いを増すことになった。その内容については前述(不正送金被害の拡大)の通りである。2014 年に改めて顕著になったのは、みなさんの預金が世界中の犯罪者から狙われているということだ。グローバルの傾向で見ても、一般に広く配布されるタイプのマルウエアではオンライン銀行から預金を盗むことを目的とした「バンキングトロジャン」と、ファイルを暗号化したりパソコンをロックしたりして人質にとり元に戻してほしければ身代金を払えという「ランサムウェア」の流行が見られた。どちらも金銭の窃取または詐取を目的とするものである。

日本におけるバンキングトロジャンを用いた不正活動は 2014 年、新たなフェーズを迎えた。2013 年に猛威をふるったのは Web インジェクションと呼ばれる手口で、感染 PC のブラウザでオンライン銀行を訪れた際、マルウエアが偽画面を表示させて認証情報を盗み取り、攻撃者がその情報でログインして不正送金を行うというものだった。そこから発展し、マルウエア VAWTRAK（別名 Neverquest、Snifula）による自動送金がついに観測されたのである。海外では 2012 年ごろに大規模な被害が見られた手口が日本に上陸したのだ。

その自動送金のシステムを攻撃者は「ATS(Auto Transfer System)」と自称する。感染 PC でオンライン銀行にアクセスした際にブラウザ上で発動する JavaScript プログラムが、正規ユーザのふりをして被害者のオンライン口座から攻撃者へ自動で送金するのである。この ATS には、必要になるたびにユーザに

入力させる偽画面を出すことでワンタイムパスワードなどの追加の認証を突破する機能や、一日当たりの送金可能金額が低い場合は自動で増額を行う機能、また残高が少ない場合は送金を取りやめる機能などが含まれていた。これらを実現するためにはそれぞれの Web 画面を解釈してユーザ操作を模した応答をする必要がある。このため JavaScript プログラムは銀行ごとに別々に用意され巧妙に作り込まれていた。

このような機能は一式をまとめたツールキットとしてアンダーグラウンド（闇市場）で取引されており、プログラム開発者とマルウエア配布・現金回収などの作戦行動を行う者が別々にいるとみられる。さらに、PC に潜み発動の機会を伺うマルウエア本体と、自動送金を行う ATS は別々のツールキットであるとみられ、Windows 向けプログラム開発が得意な者と JavaScript が得意な者とで開発を分業しているようにも見られた。

マルウエア本体側の機能で新たに明らかになった点もある。感染 PC から電子証明書を秘密鍵ごと盗む機能だ。感染時にその PC に保管されている証明書と秘密鍵をすべてエクスポートしてファイルに保存し、攻撃者の用意した C&C サーバに送るのである。またエクスポート不可設定の秘密鍵を持つ証明書はいったん削除され、再発行されたものをインポート時にコピーするという機能もあった。マルウエア ZeuS は以前からこれら機能を持っており、2014 年に大量感染があった VAWTRAK にもこれらの機能が確認された。クライアント証明書が秘密鍵とともに攻撃者に渡ることになり、SSL クライアント認証によって強化していた認証も破られた形だ。ただしこの攻撃が成功するためには秘密鍵がエクスポート可であるか、配布方法が PKCS12 方式である必要がある。この条件が成立しない場合は証明書と秘密鍵を盗むことはできず、また IC カードや USB トークンに格納された秘密鍵も持ち出すことはできない。

2013 年にみられたような単純な偽画面を用いる Web インジェクションには、トークン型などのワンタイムパスワードや SSL クライアント認証が有効だった。しかし、2014 年にみられたような ATS を用いた攻撃ではこれらは突破されてしまう。「本人が操作をしているか」という観点のこれらの認証は、ATS が持つ、バックグラウンドで不正送金の通信を行いながら必要になるたびに認証情報を入力させる偽画面を出す方法と、認証後のセッションを使用するという方法でそれぞれ突破されてしまったのだ。今後は本人認証を行ったうえで、本人が意図して実施した「取引内容」を認証するような取り組みが望まれる。パソコンからの取引申し込みをスマホで確認するといった別チャネルでの承認操作や、

ユーザ本人が口座番号や送金金額に対して電子的な署名を行いサーバ側で検証する「トランザクション署名」という技術が注目されている。

2014 年の暮れには、プロキシ自動構成(Proxy Auto-Config)の仕組みを悪用したマルウエア WERDLOD（別名 Peals）も日本で観測された。オンライン銀行のドメイン名にアクセスした場合には不正なプロキシサーバを経由するという設定が書かれた「proxy.pac」ファイルを使用する。これも数年前から継続的に海外で観測されている手口だ。

図 2-2：マルウエア WERDLOD が使用する難読化された proxy.pac の記述に関する一例[16]

この「proxy.pac」を用いる手口は MITM:Man-in-The-Middle 攻撃と呼ばれるものだ。通常であれば SSL/TLS 通信が成立せず、ブラウザの SSL 証明書検証エラーでユーザは異常に気付くことができる。しかしこのマルウエアは自分用の自己署名証明書を信頼済みルート証明書ストアに加えることで、そのブラウザのエラーを表示させないようにする機能を持っていた。MITM 攻撃を防ぐための手段であるはずの SSL/TLS が通じないという状況だが、幸いにも EVSSL の仕組みまではまだ突破されておらず、アドレスバーが緑にならないという点が最後のアラートとして残る。またこの手口ではプロキシサーバから不正に取得した認証情報で攻撃者が別途ログインし不正送金を行うことになるので、トークン型などのワンタイムパスワードが有効である。

このように、今後も海外で観測された手口が日本に上陸してくることが予想され、警戒が必要である。銀行を騙る偽のモバイルアプリの出現や、パスワード管理ソフトウエアのマスターパスワードを盗むような手口が挙げられるだろう。マルウエアを用いた手口に対抗していくには、ユーザが感染しないことはもちろんだが、事業者側で取引内容を保証できるような根本的な対策を行うことが望まれる。

[木村 仁美 トレンドマイクロ株式会社]

[16] トレンドマイクロセキュリティブログ「12 月 8 日から急増の請求書偽装スパム、主な狙いは国内銀行 15 行の認証情報か？」, 2014 年 12 月 10 日, http://blog.trendmicro.co.jp/archives/10558

■コラム：銀行を騙る偽のモバイルアプリ

フィッシング対策協議会では、2011 年 5 月に公開した「フィッシングレポート 2011」において、フィッシングアプリの登場について注意を促している。2015 年 3 月時点において、国内組織を狙った脅威はいまだ確認されていない。

しかしながら、それを予感させる出来事はすでに報告されている。そのひとつが、非公認アプリの問題である。2012 年 11 月には、「<省略>銀行口座開設」（省略部分には、実在する銀行名が記載）アプリが、Android 向け公式ストア Google Play 上に確認された。当該アプリの狙いは、広告収入であった。アプリ利用者が口座の開設を行った場合、アプリ作者に対価得られる仕組みがとられていた。

図　Google Play 上で確認された銀行口座開設アプリ（モザイク箇所には実在する銀行名が記載）

2014 年 1 月には、Apple iOS 向け公式ストア App Store 上に、大手 e コマースサイトの非公式アプリが相次いで確認され、運営元による注意が呼びかけられていた。確認された非公認アプリには、公式にはアプリの提供を行っていない企業によるものも含まれていた。これら非公認アプリケーションは、運営元企業が提供している公式のスマーフォンサイトに接続する仕組みがとられていた。アプリの振る舞いとして、不審な点はみられなかった。

いずれの非公認アプリの事例においても、利用者に対する直接的な被害は見られなかった。しかしながら、非権利者による組織のロゴが無断（不正）使用されていた。

サービス事業者側がこうした非公認アプリを放置した場合、自社の公認アプリによる営業機会を損失する可能性がある。また、もし、一般利用者が公認アプリと誤認して不正な非公認アプリを利用した場合、一般利用者の ID やパスワード情報の窃取が行われ、その情報を悪用して自社のサイトが不正ログインの被害に遭うことも考えられる。その結果、自社のサービスやブランドイメージが損なわれ、被害がサービス事業者側にも及ぶ可能性が考えられる。

利用者がアプリの認定状況を確認することは困難だが、サービス事業者の公式サイトからアプリを探す、レビューの数が多く、利用者の評価が高いアプリを選択する、開発元やアプリ名を検索して評判を調べた上で利用するといった心がけが重要といえる。ただし、不正アプリの開発元に雇われた第三者がレビューに良い評判を書き込むケースや、開発元を偽っているケースもあるため、慎重な判断が重要である。

[林 憲明 トレンドマイクロ株式会社]

3. 新しい対策の動向

ユーザ ID//パスワードの管理は、利用者の管理というのが、基本ではあるが、本質的には、オンラインサービスの利用の増加に伴うユーザ ID//パスワードの増加が問題である。そういう点で、オンランサービス事業者は、ユーザ ID//パスワードの発行については、利用者の管理責任とするのではなく、発行者としての責任も求められる必要があると思われる。

そうした中で、サービス提供事業者側でも対策が進んできている。

フィッシングの対象とされやすい金融機関やオンラインゲーム事業者では、ワンタイムパスワードの提供が増えてきている。ただし、現状では、オプションによる提供が多く、利用者が請求しなければ活用されない。

マルウエアによる不正送金の対策としても、一部の金融機関では、インターネットバンキング利用時の利用者のアクセスの挙動などから、サーバ側で利用者の PC のマルウエアへの感染を検知する仕組みを取り入れている。また、たとえ、感染していたとしても安全に取引が行えるように、銀行のサーバ側からブラウザの画面を転送し、安全な銀行のシステムを使ってインターネットバンキングを使える仮想ブラウザの仕組みを提供している金融機関も出てきた。また、振込先と振込金額を中間でマルウエアに改ざんされないように改ざん防止用のメッセージダイジェストによるトランザクション署名の導入を決めた金融機関も現れた。

そもそもユーザ ID//パスワードの問題は、サービス提供事業者が個別に ID//パスワードを発行することが問題ということで、ユーザ認証とサービスの提供を分ける ID 連携サービスも現れた。サービス提供事業者側は、このような ID 連携を使うことも考えるべきである。

また、セキュリティ対策ソフトウエアも最近の手口の変化に合わせて、マルウエアによるブラウザへのインジャクションを防ぐようなセキュアブラウザと呼ばれる機能など新しいセキュリティ機能を提供している。したがって、セキュリティ対策製品も最新のバージョンを利用することにより、感染のリスクを低くすることができる。

3.1. 中間者攻撃と対策

・トランザクション署名の活用

2014 年、フィッシング被害が拡大した要因にマルウエア感染による不正送金が上げられる。マルウエアによる不正送金は以下の 2 種類が発見されており、それぞれ異なる対策が必要である。

・偽画面を表示し認証情報を詐取するマルウエア
正規の入力ページにマルウエアが不正な入力欄を追加表示し、ID、パスワード、乱数表情報の全てを詐取するもので、攻撃者は詐取した情報から本人になりすましてログインし不正送金を行う。このマルウエアにはワンタイムパスワードやクライアント証明書などの認証の強化対策が有効である。

・送金情報をすり替えるマルウエア
この種のマルウエアでは中間者攻撃「Man In The Browser 攻撃」により、送金操作中に本人が気づかない形で送金情報を勝手にすり替えることで行われる。マルウエアは正当な利用者と正当なサイト間のリアルタイムなリレーを演じる。このとき、パスワードなど認証情報はそのまま使用し、振込先と金額をすり替える。このため、一度限り有効なパスワードを発行するワンタイムパスワード認証では、その有効期限が切れる前に署名が行われるため、対策にならない。また、クライアント証明書による対策が行われている場合も、すでに攻撃者の手により、秘密鍵が窃盗されている場合には対策にならない。

トランザクション署名方式は、この中間者攻撃（Man In The Browser 攻撃）に有効な対策であり、国内の銀行でも導入が始まった。

・トランザクション署名方式の概要
トランザクション署名ではテンキー付きハードウェアトークン（図 3-1）を使用し以下の流れで送金情報のすり替えを検知する。

図は、みずほ銀行より提供

図 3-1　テンキー付きハードウェアトークン

① ハードウェアトークンに振込先口座番号・振込金額等および署名生成の為のコードを入力し、メッセージダイジェストコード（署名）を生成する。このコードはハードウェアトークンを持っているユーザしか生成できない。
② インターネットバンキングの送金処理画面で振込先口座番号・振込金額に加え、トークンで生成したコードも入力しサーバに送信する。
③ インターネットバンキングサーバでは、ユーザに与えたハードウェアトークンと同じロジックで振込先口座番号・振込金額からコードを生成する。
④ ユーザが入力したコードと、サーバ側で生成したコードの一致を確認することで、振込先口座番号・振込金額がすり替えられていないことを確認できる。

トランザクション署名方式は送金情報をすり替えるマルウエアに有効な対策と言える。この方式の完全性を確保するためには、コード（署名）を生成するトークン自体をユーザ本人が保有していることに加え、生成ロジックが侵されていないことも必要となり、より安全なハードウェアトークンが推奨される。

3.2. ブラウザのアドオンソフトウエアの危険性

ブラウザのアドオンソフトウエアとはWebブラウザの設定を勝手に変更する「望ましくないソフトウエア」のことである。
ブラウザのアドオンソフトウエアはブラウザの機能を乗っ取ることで以下のような症状を引き起こす場合がある。

- Web ブラウザ起動時に、最初に表示される Web ページが勝手に変更される。
- 身に覚えのない Web サイトや広告のページが勝手に表示される(ポップアップする)。
- ツールバーを勝手にインストールされる。
- Web ブラウザの検索エンジンを勝手に変更される。
- Web ページの閲覧中に、有害な Web サイトへ勝手に誘導される
- マウスポインタが変わる
- インターネットに接続していない場合でも、ポップアップ広告が表示される
- 動作が遅くなる

これらの症状に加えて、ユーザの Web ページの閲覧履歴や、ブラウザ上で入力した ID/パスワードなどの秘密情報を盗み出す「スパイウェア」として活動するものがあり注意が必要である。

ブラウザのアドオンソフトウエアへの感染ルートは複数あり、フリーソフトウエアをインストールする際にオプションとして同時インストールさせるケースや、バナー経由で悪意のあるサイトへ誘導させるケース、迷惑メールなどから望ましくないソフトウエア配布サイトへ誘導させるケースなどがある。対策としては、パソコンを常にクリーンに保つ心がけが重要である。具体的には、セキュリティ対策ソフトウエア、ウェブブラウザー及び OS を最新に保つことが、オンライン上の脅威から守る上での最善の策である。また、多くのソフトウエアには、既知のリスクから自身を保護するために自動的に最新版に更新する機能がある。利用しているソフトウエアに自動更新オプションが実装されている場合には、こうした機能の利用を検討することが有効である。

[加藤 孝浩　トッパン・フォームズ株式会社]

[林 憲明　トレンドマイクロ株式会社]

3.3. POS への攻撃と対策

POS（Point Of Sales）は店舗で商品を販売するごとに商品の販売情報を記録し、集計結果を在庫管理やマーケティング材料として用いるシステムでクレジットカード情報も取り扱う。そして POS マルウエアは、POS システムから直接カード情報を奪うマルウエアの総称である。多くの場合、顧客のカードが読み取り機を通った瞬間に、磁気ストライプから読み取ったデータを攻撃者の元へ送る。つまり、サーバを攻撃して顧客情報のデータベースからデータを奪うのではなく、カードの読み取りと同時にデータを盗むのである。そのため企業側はデータが盗まれていることを認識しづらい。POS を狙ったマルウエアが注目を集めたのは、2013 年 12 月に米国有名小売店の決済ネットワークから 4000 万人分ものクレジットカード情報が漏洩した事件からである。このマルウエアは Windows ベースのオンライン型 POS 端末を狙いキーロギングやプロセスメモリスキャンの機能を有している。制御、指示を出す"コマンド＆コントロールサーバ（C&C サーバ）"への通信には「Tor（The Onion Router）」を活用するなどして通信を秘匿化している。POS マルウエアで盗まれたカードデータは犯罪サイトで取り引きされ、そこにはカード番号だけでなく、その所有者の氏名など、偽造カードを作るために必要な情報も含まれているという。日本国内でも POS マルウエアの存在が確認されているので、消費者にはこれまで以上にカードの明細をチェックすることを求められる。

[花村 実　EMC ジャパン株式会社]

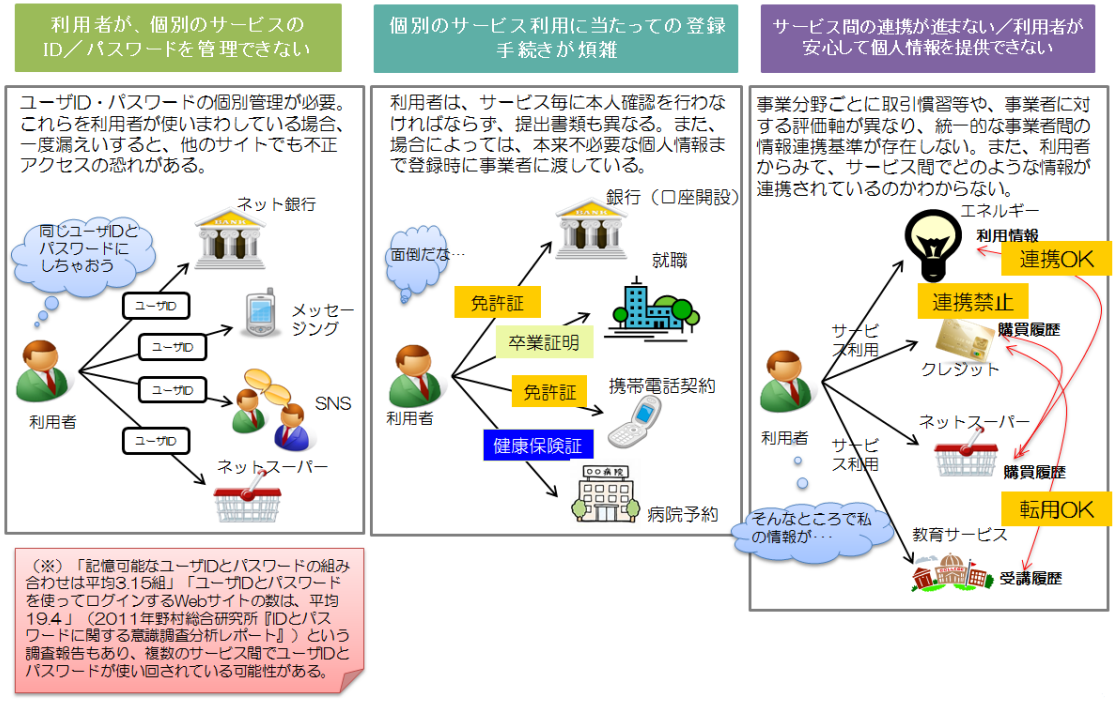
[水村 明博 EMC ジャパン株式会社]

3.4. 認証サービスの利用（ID 連携トラストフレームワーク）

インターネットサービスの普及に伴い、利用者は個別の事業者サービス毎に ID／パスワードを登録し、かつそれら情報を利用者自身が秘密に管理しなければならない。利用者は平均 20 個弱のユーザ ID／パスワードを使用していると言われ、人間の記憶の限界から、複数の異なるサービスに対して同一のユーザ ID／パスワードの組を使い回していることがよくある。この場合、情報セキュリティの脆弱な事業者からユーザ ID／パスワードが漏えいすると、それらが他のサイトでも不正アクセスに利用される恐れがある。

サービス事業者側にとっても、利用者の本人確認のためにユーザ ID／パスワードはもとより本人に係る属性を多数保持することとなり、それらパーソナルデータに対してやはり厳密なセキュリティ管理が求められる。

このように利用者および事業者の双方において利用者情報等の管理に係る努力が必要である（図 3-2）。



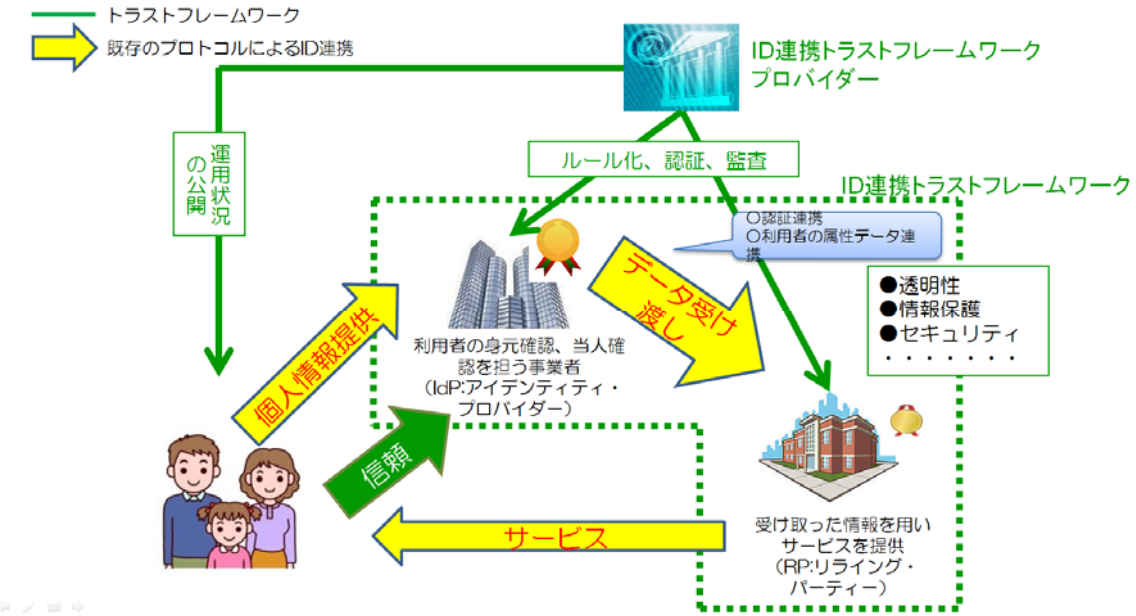
図は、（財）日本情報経済社会推進協会（JIPDEC）電子情報利活用研究部，"ID 連携トラストフレームワークとは（平成 26 年 10 月 21 日）"より転載

図 3-2　個人情報を取り扱うインターネットサービスを巡る課題

そこで信頼できる ID プロバイダー（以下、Idp）に認証に必要なユーザ ID／パスワードや各種属性情報を預け、各事業者は Idp と信頼関係をもつことによって利用者認証を Idp に任せその認証結果をもって利用者にサービスを提供するというスキームが考え出された。さらに事業者間で ID 連携を行なうことにより複数事業者間のサービスがワンストップで利用者に提供することが可能となる。すでに行なわれている OpenID などのフェデレーション認証がこれに該当するが、ただ既存の ID 連携は Idp の信頼性や事業者の信頼性の担保がなされていなかった。そのため利用者としては ID 連携することによって自身のパーソナルデータが他のサービス事業者に転々流通するのではないかという危惧があった。

そこで新たに ID 連携トラストフレームワークという枠組みが考案され、経済産業省主導でわが国に展開されようとしている。ID 連携トラストフレームワー

クとは、インターネット上（非対面の環境）で、利用者のデータ（利用者である個人に関する属性情報の集まり）やサービスの受け渡しを行う企業群が、「利用者がその相手を信用して情報利用を任せられる（信用；信頼）」状態であることを保証する枠組みのことである。これを実現するために、ID を発行する Idp は信頼できる第三者からお墨付きが与えられる。これによって利用者とサービス事業者は安心して単一のユーザ ID によって認証を行うことができる(図 3-3)。



図は、(財) 日本情報経済社会推進協会（JIPDEC）電子情報利活用研究部，"ID 連携トラストフレームワークとは（平成 26 年 10 月 21 日）"より転載

図 3-3　ID 連携トラストフレームワークの概念

このフレームワークの実現によって、以下のメリットが享受できる。

① 利用者視点：認証に必要な処理・手続きの手間を低減
② 事業者視点：認証に係る利用者の身元・当人確認の作業をフレームワークの認証に任せることにより、自社サービスの提供・事業開発に専念できる。
③ 社会的視点：上記①、②の実現による安全性、信頼性の向上と社会全体のコスト低減

[八津川 直伸　日本ユニシス株式会社]

4. パスワード管理

2-1 で紹介した通り、昨今、複数のインターネットサービスで同じパスワードを使い回していることが原因で生じてしまうユーザアカウントへの不正なログイン、いわゆるパスワードリスト攻撃による被害が継続的に発生している。

そのため利用者としては、複数のインターネットサービスを安全に使用するには、異なるパスワードをサービスごとに設定する必要がある。それら異なるパスワードを管理する手法はいくつがあるが、今回は専門家の意見をコラムとして以下の通り紹介する。

■コラム：位置記憶パスワードの提案

～ なぜ、文字列をパスワードとして覚えるのか？ ～

1. パスワード 覚えられますか？

パスワードとして、「**T{_3”}H=D+**」や「**u&![KiXjow**」を使って欲しいと言われたら、2 組のパスワードを各システムのユーザ ID とともに覚えられるだろうか？

多くの人は、「覚えられない」と回答するであろう。

しかし、これらの２つのパスワードは、図１に示すように、２行目の５列目から始まり、左下に順に、左端で、右下に折り返し、下端では右上にという規則で作成した。

この乱数表２つとそれぞれのユーザ ID を決め、図１で示したパターンを決めることで、パスワード文字列を覚える必要はない。 図１では、該当文字がわかるように色分けをしたが、パターンの規則を覚えられれば、それも必要ない。更に、パスワード長も 10 桁としたが、もっと長い文字列でも構わない。

User-ID: randoma　2015/4/1

	1	2	3	4	5	6	7	8	9	10
1	]	>	D	U	)	S	’	&	:	,
2	i	I	5	z	T	)	l	n	q	%
3	)	W	4	{	*	N	X	I	H	a
4	o	6	_	b	9	5	k	a	N	;
5	I	3	N	~	W	F	r	(	3	*
6	”	(	{	x	W	{	6	b	}	E
7	[	]	3	0	r	N	0	,	”	8
8	#	A	H	=	6	+	_	*	0	h
9	E	V	k	=	=	+	l	3	9	m
10	A	L	j	q	D	~	.	f	J	&

ID: randoma

User-ID: randomb　2015/4/1

	1	2	3	4	5	6	7	8	9	10
1	9	A	[	{	q	)	w	z	n	{
2	b	)	A	’	u	K	Q	%	5	4
3	u	0	%	&	3	Q	V	7	h	U
4	p	t	!	0	<	k	h	:	%	o
5	o	[	q	v	F	2	H	?	_	|
6	K	b	U	>	W	W	e	P	F	R
7	¥	i	`	0	a	+	W	[	7	k
8	7	Y	X	;	H	P	u	f	L	8
9	b	h	&	j	e	w	D	l	d	[
10	f	u	|	u	o	D	)	f	@	2

ID: randomb

図１　乱数表利用のパスワード例

ユーザ ID ごとに乱数表を割り振れば、同一パスワードになる可能性も低い。

例としたパスワード作成規則は、2 行目・５列目から始まり、斜め下に行く

ような規則で作成したが、規則は自分で決めれば良い。 更に、乱数表を他人に見せなければ、図１のようにパスワードをマークしても構わない。

2. 乱数表について

乱数表はマイクロソフト EXCEL で作成[17]した。現在は、以下の文字種の乱数表を作成でき、A4 用紙に乱数表を 6 組印刷する。

1. 英小文字と数字の組み合わせ
2. 英小文字と数字、記号の組み合わせ
3. 英文字（大・小文字）と数字の組み合わせ
4. 英文字（大・小文字）と数字、記号の組み合わせ

作成した EXCEL シートをダウンロードし、この EXCEL シートを開くと、画面上部に図 2 の内容が表示される。真ん中の枠内に、１～４の数字を入力し、乱数表に利用できる文字種類を決める。

１～４以外の数字を入力すると、枠下に「Enter(1-4)」と表示されるので、正しい値を再入力する。

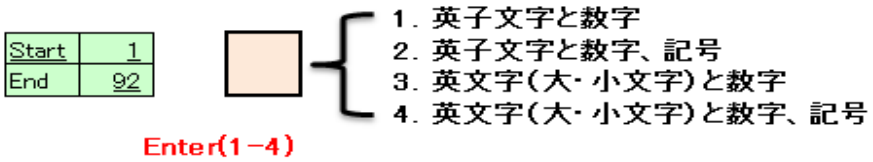


図 2 EXCEL シートの上部画面

正しい入力ができれば、印刷し、印刷した乱数表で、どの様なパターンを利用するかは、利用環境を考慮する。 自宅で他人に見られない環境であれば、図 1 に示したようにパターンを色づけしたものを利用しても構わない。

筆者は、職場の机上に A4 用紙を印刷したものを置いてある。簡単なショルダーハッキング実験を行ったが、ビデオで撮影されない限り、他人がパスワードを推測することは殆ど不可能であった。

安易なパスワードを利用しなくても、この方法で一般のユーザ ID／パスワード方式には最も有効な仕組みだと考えている。

3. 他の方式が利用できるのであれば・・・

ワンタイムパスワードや生体認証利用が遥かに安全だと指摘されることがある。それらを利用できるのであれば、この方式を使う必要はない。この位

[17] EXCEL で作成したワークシートは、以下に保存してある
日本語版： http://www2.gol.com/users/uchidak/research/RandomPassTable_JPN.xls
また、詳細な解説は、以下を参照のこと；
http://www2.gol.com/users/uchidak/research/RandomPassTable.pdf
なお、今後、利用文字種の組合せを増やすことを検討している。

置記憶パスワードの良さは、現在、インターネット等で利用されている多くのシステムの変更をせず、現在のユーザ ID／パスワードを利用できる。

ワンタイムパスワードや生体認証等では、サービス提供側も利用者も新たなシステムの導入が必要となるが、そのサービスが利用できるのであれば、それをお勧めする。

残念ながら、現在利用されているユーザ ID／パスワード方式のサービスが新しい認証システムを提供していなければ、この位置記憶パスワードを利用し、自分自身を守る必要がある。パスワードを使い回しても、「パスワードリスト攻撃」に遭わないかも知れない。ただ、利用者が「遭う、遭わない」を決められない。 この方法を利用するのも１つの方法であろう。

[内田 勝也 情報セキュリティ大学院大学 名誉教授]

■コラム：様々なパスワード管理について

■パスワード管理ソフトウエアの利用

最近では、オンラインでの銀行・株取引、ショッピング、ポータルサイト、SNS、ストレージサービスなど、一人で複数の Web サービスを利用することが多い。

しかし、複数の Web サービスのログイン ID とパスワード(ID//パスワード)を記憶することは容易ではく、かといって記憶し易いよう複数のサイトで同じ ID/パスワードを使い回すのは大変危険である。

一か所の ID/パスワードが何らかの理由で漏洩した場合、これを利用して他の Web サイトにも不正ログインされ、金銭的被害やプライバシー/機密情報の漏えい被害が拡大する可能性が高まる。

PCやスマートデバイスにインストールしたパスワード管理ソフトウエアを利用することで、各 Web サービスごとに個別に設定した ID/パスワードを安全な状態で記録できる。

各 Web サービスにログインする際は、専用ソフトウエアにより ID/パスワードが自動入力される。これにより、自身の記憶に頼ることなく、複数の ID/パスワードを安全に管理することができる。

■手書きメモの利用

複数のサイトで同じ ID/パスワードを使い回すよりは、Web サービスごとに個別に設定した ID/パスワードを手帳や紙にメモしておき、大切に管理する方が安全である。

その際、パスワードの一部を共通の文字列をとして自身で記憶し、残る部

分のみをメモに記録することでより安全性を高めることができる。
　万一メモを紛失した場合は、各サービスの提供するパスワードリマインダ機能や別途安全な場所に保管しておいたメモのコピーを用いてパスワードの変更を実施することで安全性を高めることができる。

■認証サービスの利用

以下の認証サービスが提供されている場合は、それらのサービスを利用することで安全性を高めることができる。

・ワンタイムパスワード
　トークンと呼ばれる１回限り有効なパスワードの生成器(特殊なハードウェアやスマートデバイス上のソフトウエア)を用いて、使い捨てのパスワードを利用してログインする方式。トークンは一定時間ごとに変化するため漏洩リスクが少ない。

・マトリクス認証
　事前に自ら指定した位置と順番通りに数字を入力することで本人であることを認証する方式。表示される数字がランダムなため、辿る位置と順番は同じでも送信される数字列は毎回異なり、漏洩リスクが少ない。
　特定の機器などを必要とせず、位置と順番の記憶のみで成り立つため、機器の紛失や故障によりログインできなくなる事態を防ぐことができる。

[早川 和実　NTT コミュニケーションズ株式会社]
[桐山 直樹　NTT コミュニケーションズ株式会社]

5. まとめ

2012 年後半から急激に増加したフィッシング被害は、2013 年に入っても減少するどころか増加を続け、2014 年上期にピークに達し、2014 年下期に入っても高水準の被害が続いている。特に金融機関における不正送金は 2014 年にはいっても大きな問題となっている。

2014 年に多発したネットバンク不正送金事件の多くは、マルウエアを利用したフィッシング事件である。このような手法は、過去数年来、フィッシングレポートで警戒を呼び掛けていたものであり、また 2014 年にはフィッシング対策協議会として不正送金被害防止のためのガイドラインを作成したが、残念ながら被害が続いている。2015 年においても被害の増加が予想される。

旧来型のフィッシングは手法としては少なくなってきているものの、ID 窃盗や不正送金手法の高度化・精緻化はますます進んできており、利用者・事業者ともに、常日頃からの情報収集や迅速な対応がより重要になってきている。

これらの現状に対しては、協議会は今後も動向に関する最新情報を収集し、新たな手法に対する技術的対策などを検討する必要がある。

（空白）

フィッシング対策協議会　ガイドライン策定ワーキンググループ
構成員名簿

（敬称略・順不同）

【主査】

内田 勝也	情報セキュリティ大学院大学名誉教授

【副主査】

野々下 幸治	トレンドマイクロ株式会社

【構成員】

水村 明博	EMC ジャパン株式会社
花村 実	EMC ジャパン株式会社
早川 和実	NTT コミュニケーションズ株式会社
桐山 直樹	NTT コミュニケーションズ株式会社
加藤 孝浩	トッパン・フォームズ株式会社
長谷部 一泰	アルプスシステムインテグレーション株式会社
八津川 直伸	日本ユニシス株式会社
山本 和輝	BB ソフトサービス株式会社
林 憲明	トレンドマイクロ株式会社
木村 仁美	トレンドマイクロ株式会社
鈴木 哲治	株式会社ジャックス
秋山 卓司	クロストラスト株式会社
丹京 真一	株式会社日立システムズ
上前 光宏	一般社団法人全国銀行協会

【オブザーバ】

経済産業省商務情報政策局情報セキュリティ政策室

【事務局】

一般社団法人 JPCERT コーディネーションセンター
株式会社三菱総合研究所