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 2016

－　世界に広がるフィッシング対策の輪　－

平成 28 年 5 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

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 年に件数ベースではピークを迎えたが、2015 年に入って件数は若干減少したが、被害額は微増するなど、引き続き金融機関をかたったフィッシングが高水準で続いている。

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 26 年には 1,876 件、約 29 億 1000 万円の被害だったものが、平成 27 年には 1,495 件、約 30 億 7300 万円の被害となっている。

フィッシング対策協議会の統計でも、2015 年のフィッシング届出件数は 1 月、4 月、5 月、12 月に急増している。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 1.1-1）。特徴としては、高水準の届出が継続するのではなく、急増したかと思えば急激に減少するなどの状況がみられる。

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 2015 年で、対前年で半減し（2014 年 22,411 件、2015 年 11,408 件）、フィッシングサイトの件数も 0.7 倍に減少し（図 1.1-2）2014 年 4,146 件、2015 年度 2,995 件、ブランド名を悪用された企業の延べ件数は 2014 年 172 件、2015 年 164 件であり、前年に比べ微減となった（図 1.1-3）。

[1] 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，https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf

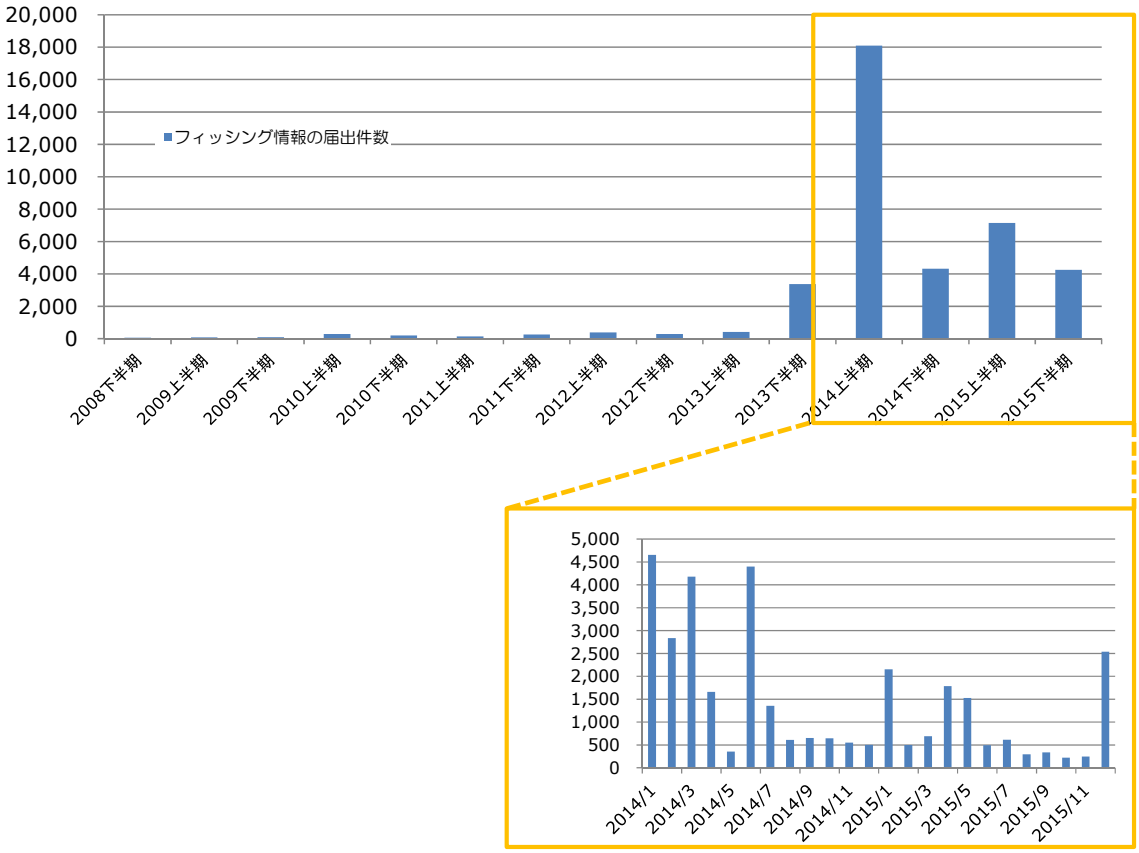


図 1.1-1　フィッシング情報の届出件数

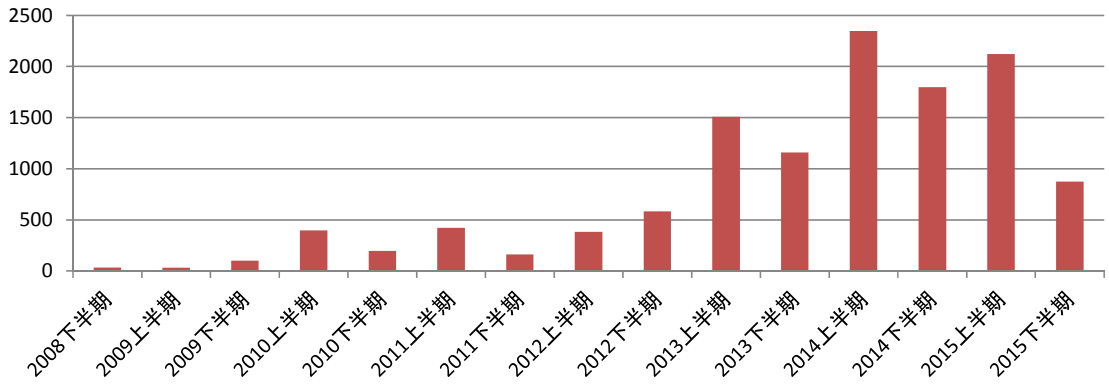


図 1.1-2　フィッシングサイトの件数

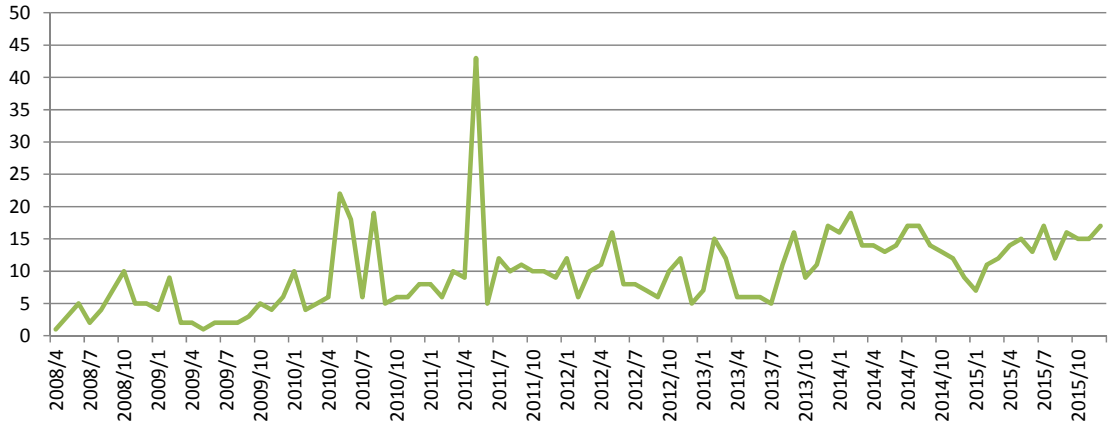


図 1.1-3　ブランド名を悪用された企業の件数

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）は昨年度と同水準で推移している（図 1.1-4）。また、その手口を見ると、2015 年（平成 27 年）における狭義のフィッシングは 24 件であり、比率は約 7%となっている（ 1.1-5）。

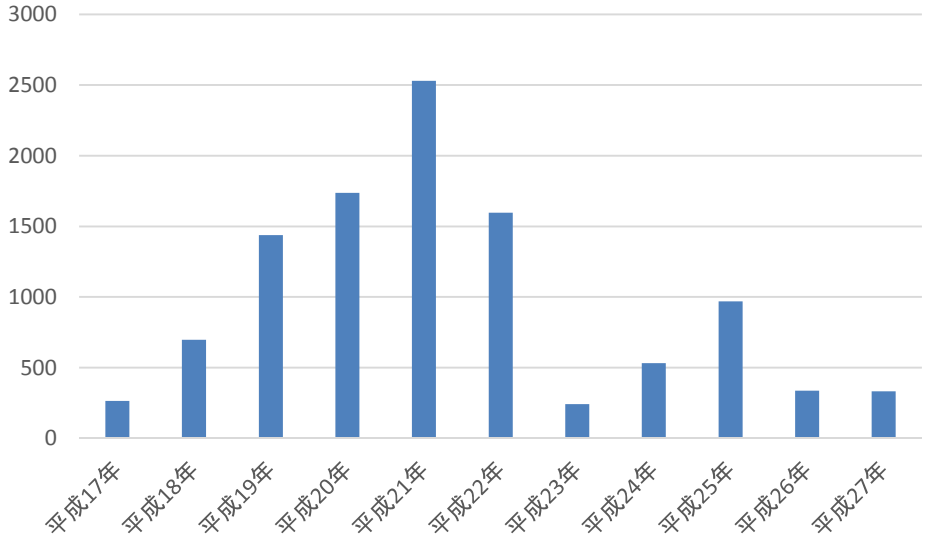
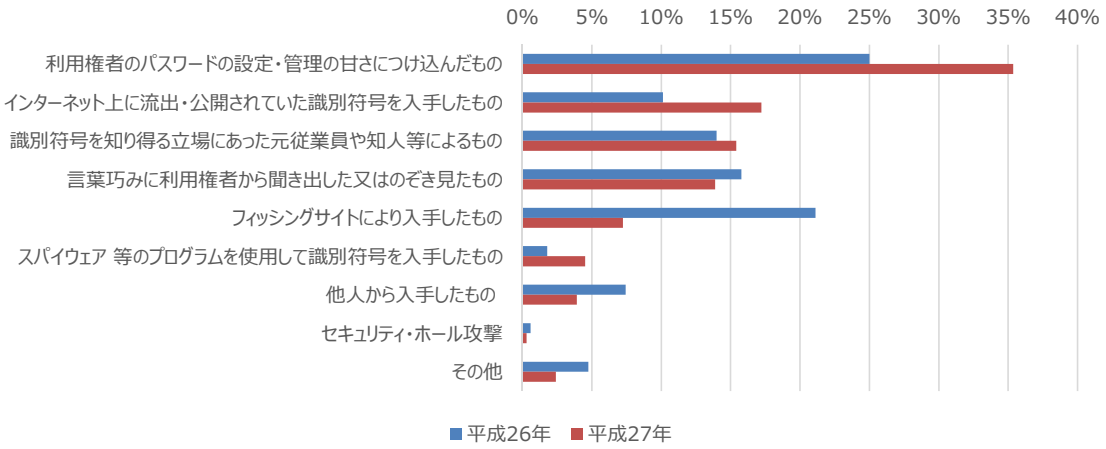


図 1.1-4　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数[2]

[2] 警察庁,「平成 27 年における不正アクセス行為の発生状況等の公表について」,等、https://www.npa.go.jp/cyber/pdf/H280324_access.pdf よりフィッシング対策協議会が作成



1.1-5　不正アクセス行為に係る犯行の手口の内訳（平成 27 年、平成 26 年）[3]

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、平成 27 年に前年より若干件数は減少し 1,495 件であったが、被害金額は増加し 30 億 7300 万円に達した。

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、2015 年上期のフィッシング届出件数は、2014 年から急増し過去最高水準となった（図 1.2-1)。引き続き注意が必要である。

[3] 同上
[4] https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf

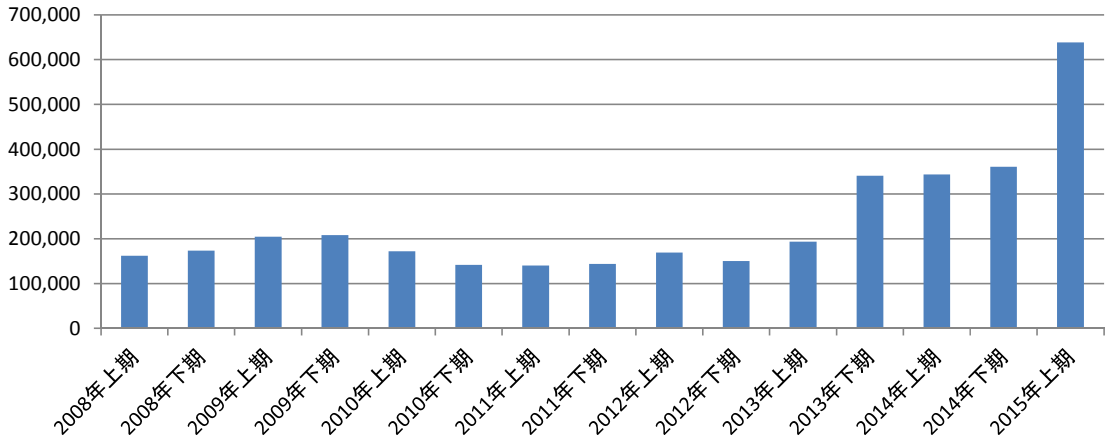


図 1.2-1　APWG へのフィッシングメール届出件数[5]

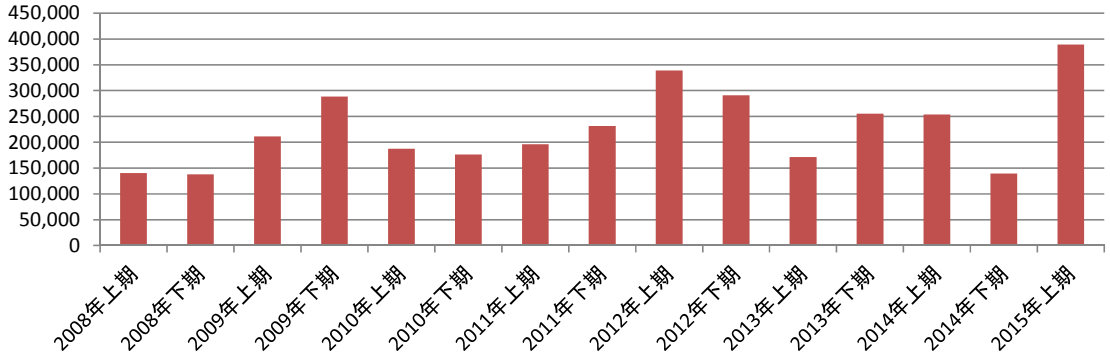


図 1.2-2　フィッシングサイトの件数（APWG）[6]

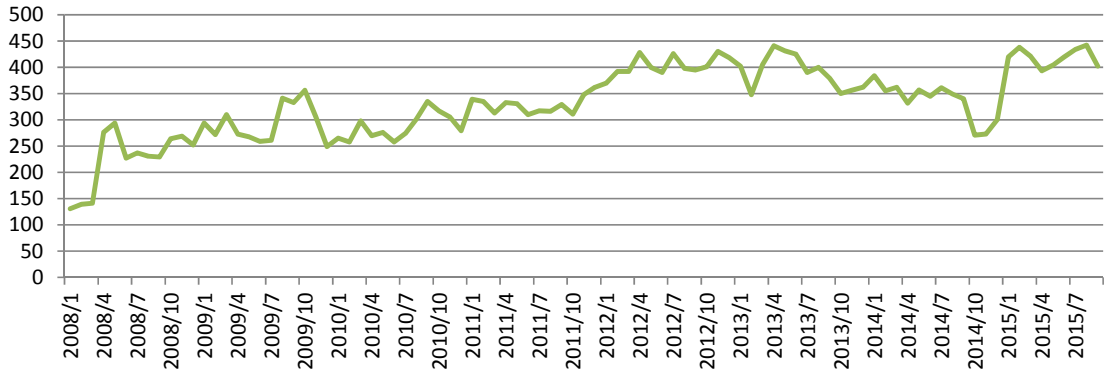


図 1.2-3　フィッシングによりブランド名を悪用された企業の件数（APWG）[7]

[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
[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

2. フィッシングこの一年

2.1. フィッシングの拡大

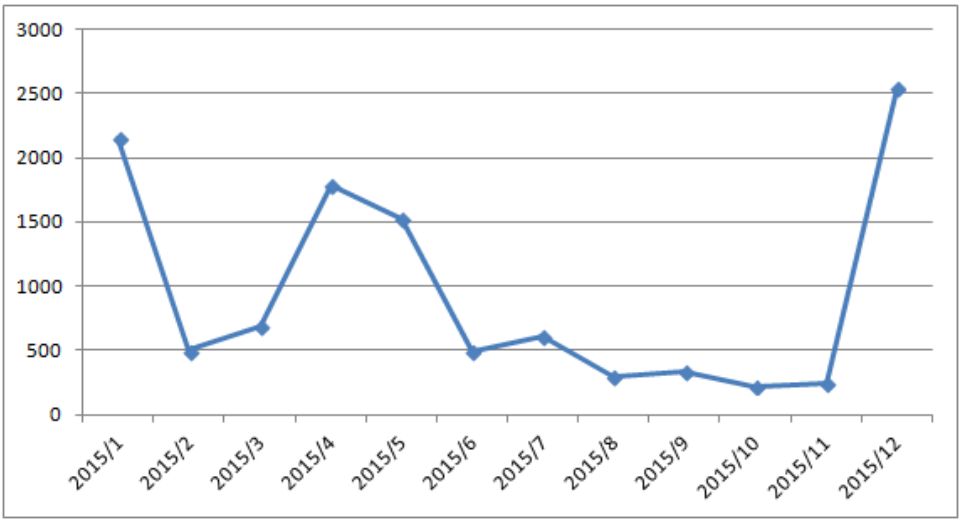


図 2.1-1 フィッシングの届出件数

2015 年フィッシング対策協議会へのフィッシングの届出件数の総数は 11,408 件でありフィッシングの届出件数を月別にしたグラフは上記の通りである。2015 年 1 月は 2,156 件で、オンラインゲームをかたるフィッシングの届出が多く寄せられた。4 月の届出件数は 1,787 件で金融機関をかたるフィッシングが増加した、また 12 月の届出件数は 2,540 件で、複数の金融機関をかたるフィッシングの届出が多く寄せられた。

2.2. 金融機関を狙った攻撃の激化

今までの日本は海外オンライン犯罪者にとって「言葉の壁」が参入障壁となっていたこともあり、いい意味で海外の惨状とは一線を画していた。しかしここ数年は利用者を狙う脅威環境が劇的に変化している。平成 26 年度のオンラインバンキング関連の不正送金被害が発生件数、被害額ともに過去最悪を記録し、平成 27 年度上半期も 754 件、約 15 億 4400 万円の被害が発生し勢いに陰りが見られない[8]。

[8] https://www.npa.go.jp/cyber/pdf/H270903_banking.pdf

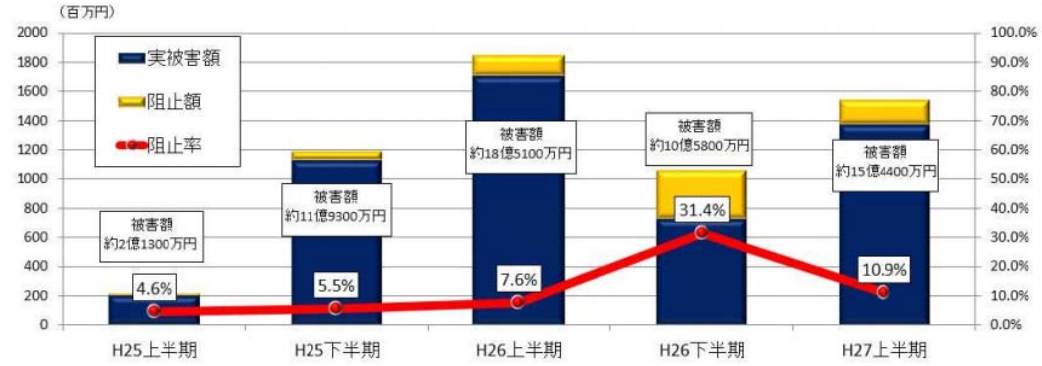


図 2.2-1　不正送金阻止状況[9]

外国人を含む犯罪集団は組織化され、指令役、不正送金先口座のブローカー(盗んだ預金を送金する口座を調達する役)、出し子(送金された口座から現金を引き出す役)、回収役(現金の受け取り、マネーロンダリング)などの役割で構成されている。最終的に犯罪集団中枢の"管理"部門で資金化しなければならないが、海外送金は好まれない。これは EU などと比べて、日本では海外送金に対するチェックが厳しく手数料が高いためと思われる。代わりに、 家電品、紙おむつや化粧品を爆買いして本国に送るケースがある。

図 2.2-2　金融機関を狙ったスマートフォン向けマルウエア「iBanking」の管理画面[10]

モバイル端末（iOS/Android）を対象とした不正な攻撃も増えている。モバイル機器をパソコン上でエミュレーションするなどしてから攻撃する例も一般化した。金融機関を狙ったスマートフォン向けマルウエア「iBanking」（画面）は管理画面が充実しており、金融機関から SMS メッセージで追加承認情報が送

[9] https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf
[10]出所：EMC ジャパン RSA 事業本部

られてきた際に、この SMS メッセージを犯罪者の管理サーバに転送するといった設定が簡単にできる。感染したスマートフォンは遠隔操作で通話内容を勝手に録音し秘密裏に犯罪者管理下のサーバにアップロードも可能だ。

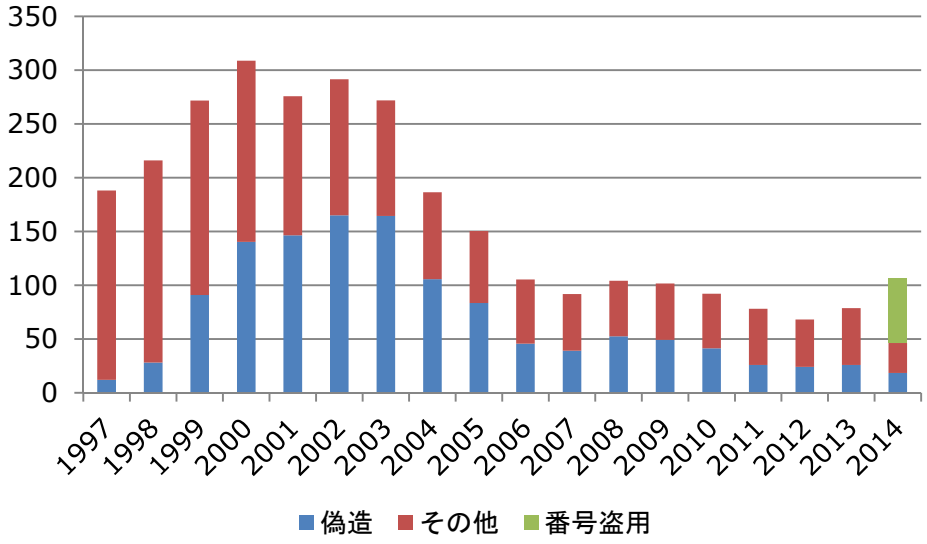


図 2.2-3　クレジットカード不正使用被害額[11]

クレジットカードの不正使用も増えている。日本クレジットカード協会によると従来の偽造、盗難による不正使用に代わって"番号盗用"の被害額が増えている。この"番号盗用"とは E コマース等のクレジットカード取引で物理的なカードではなくクレジットカード番号を盗まれて不正使用されていることを指す。2015 年に関しては年間でのデータがまとまっていないが、1 月～9 月で、全体被害額の 59.7%が"番号盗用"のよるものとなっている。

E コマースサイトでの犯罪行為は銀行の不正送金と比べて手間がかかり"割の良い"仕事ではなかった。ブラックマーケット等で盗まれたクレジット番号を用意して、高級家電品等の転売しやすいものを選び、空き家になっている住所を送付先に指定（あらかじめ空き家情報をしらべなければならない）して、アルバイトを空き家に待機させ宅配業者から受け取るといった複雑な段取りが必要だったからである。

残念なことに、海外では盗んだクレジット番号情報を簡単に現金化するツールが人気を博している。この「VOXIS」（画面）というツールは犯罪者が架空の E コマース事業者を名乗り、14 か所のクレジットカード決済代行サービス業者を登録し、盗んだカード情報を使い、あたかも EC ショッピングサイトで取引があったように装うことによって決済代行業者
（最終的には盗まれたカード所有者）から現金を窃取することが可能になる。

[11]出所：日本クレジットカード協会資料より作成
http://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf

多数のカード情報を VOXIS にロードし、スクリプトでショッピング取引を生成できるので、犯罪は何もしなくても自動的に現金がたまっていくという効率の良い犯罪が可能になるのである。

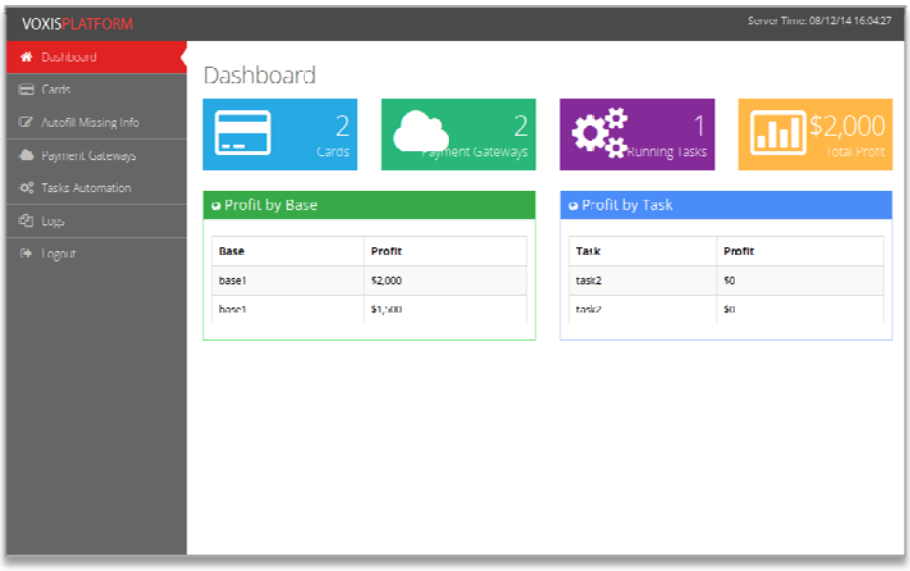


図 2.2-4　クレジットカード番号情報現金化ツール「VOXIS」のダッシュボード画面[12]

[花村 実　EMC ジャパン株式会社]

2.3. ソーシャルログインサービスの普及

「ソーシャルログイン」とは、SNS：ソーシャルネットワークサービスの既存のアカウント情報を利用して個人認証を行うことで、サードパーティの会員向けサービスの認証を実現するアイデンティティ（ID）連携機能である。

現在、ソーシャルログインを実装するスマートフォンのアプリや Web サイトのサービスが増えている。ここでは、利用者・運営者にもたらされるメリットと、セキュリティ上の懸念について述べる。

まず、利用者にもたらされるメリットについて検討する。

多くの利用者はサービス利用開始時に行う、エントリーフォームからの会員情報の入力を煩わしいと感じている。ソーシャルログインが実装されたサービスでは、ワンクリックで会員登録やログインが実現できる。また、利用頻度の低いサービスでは ID / パスワードの失念が起こりうる。ソーシャルログインが実装されていれば、ログイン時に要求される情報は普段利用している SNS の ID / パスワードに限られるため失念の可能性は低い。更に、PC に比べ画面表示や入力機能の劣るモバイル環境においては、ログインの手間を省くことのできる

[12]出所：EMC ジャパン RSA 事業本部

ソーシャルログインが利便性を高めている。事実、ソーシャルログイン利用者のうち 62.6%がモバイル、37.4%が PC という調査結果も発表[13]されている。

次に、運営者にもたらされるメリットについて検討する。

ソーシャルログインの実装により、利用者に対するユーザビリティを高めることができる。会員登録時における心理的障壁の引き下げや、サービスに対する離脱率の改善について期待することできる。また、サービスの継続利用を促すことができる。更に、登録されているソーシャルデータを取得することができ、取得情報を用いたターゲットマーケティングへの活用が期待できる。

表 2.3-1　ソーシャルログインによってもたらされるメリット

利用者	運営者
ワンクリックで会員登録やログイン可能	会員登録時の心理的ハードルの引き下げ、それに伴う離脱率の改善
ID / パスワードの失念に伴うサービス利用の断念 モバイル環境でのシームレスなログイン	サービスの継続利用
運営者からの属性にあわせた情報の提供	登録されているソーシャルデータの取得

このように利用者、運営者の両者にメリットが期待できるソーシャルログインではあるが、その機能を悪用したセキュリティ上の懸念がある。ここでは、そのうち二つを指摘する。

第一にあげられる懸念が、取得されたソーシャルデータの悪用である。ソーシャルログイン機能によって共有されるソーシャルデータには個人の特定につながる情報が含まれている。悪意をもって取得された個人情報が悪用され、詐欺など新たな犯罪被害に巻き込まれる可能性が懸念されている。

表 2.3-2　ソーシャルログインによって取得可能なソーシャルデータ

SNS	取得できるソーシャルデータの種類
Facebook	氏名、性別、血液型、誕生日、メールアドレス、住所（市区町村まで）、写真、 興味・関心、職歴、学歴、地域、友達リストほか

[13] feedforce「国内ソーシャルログイン利用率は Yahoo! JAPAN ID が 56.5%でシェア No.1！ソーシャルログイン利用者の６割がモバイルユーザーという結果に。」,
https://www.feedforce.jp/release/4979/

Google+	氏名、ニックネーム、メールアドレス、プロフィール写真、住所、言語ほか
LINE	ニックネーム、プロフィール写真、設定されたひとこと、内部的な識別子
Twitter	氏名、ニックネーム、メールアドレス、プロフィール写真、フォローリスト、フォロワーリストほか
Yahoo!	氏名、ふりがな、性別、生年、メールアドレス、郵便番号、都道府県、市区町村、電話番号、完全住所（番地以降の住所、マンション名など）

第二にあげられる懸念が、「拡散機能」を悪用したなりすまし投稿による犯罪の荷担である。

ソーシャルログインに利用されている SNS の機能によっては、連携により運営者による SNS への投稿を許可しているものもある。これを拡散機能と呼ぶ。拡散機能が有効な場合、悪意をもった運営者はこの機能を悪用し、利用者になりすまし有害な情報（悪意ある URL など）を投稿することができる。事実、そのような事例は多数報告[14]されている。このような場合、悪用された被害者本人だけでなく、その被害者と繋がっている友達へも有害情報が拡散され、ソーシャルログインによる連携を行った被害者に悪意がないにもかかわらず、犯罪に荷担する結果となり得る。

従って、ソーシャルログイン機能の利用を検討している運営者においては、必要以上の個人のソーシャルデータへのアクセスは避け、情報の取得を行う際には、利用者へ取得する情報と利用目的を明らかにし、利用者へ不安要素を与えることなく、適切なマーケティング活動を行う上で必要となる最低限の情報取得にとどめておくことが重要である。

また、利用者においては、ソーシャルログイン機能を利用する前に、連携するサービスの評判を確認すること、定期的に連携しているサービスの見直しを行うなどして予防措置を施すことが重要である。

[林 憲明　トレンドマイクロ株式会社]

[14] IPA 独立行政法人情報処理推進機構「2012 年 10 月の呼びかけ「 SNS におけるサービス連携に注意！ 」～　あなたの名前で勝手に使われてしまいます　～」,
http://www.ipa.go.jp/security/txt/2012/10outline.html

2.4. STC 普及啓発 WG 活動報告

2.4.1. 世界に拡がる「STOP. THINK. CONNECT.」キャンペーン

「STOP. THINK. CONNECT.」（以下、STC）キャンペーンは、インターネットを安全に使うための消費者向けセキュリティ普及啓発キャンペーンである。このキャンペーンはインターネットや Web サイトにアクセスする前に 「ちょっと立ち止まって、(例えば、その Web サイトにアクセスすることで) 何が起こるか考える」 意識を持つよう呼びかけている。

STC キャンペーンは、2010 年 10 月にアメリカ大統領告示 で、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として宣言されたことを皮切りに、日本をはじめ、パナマ、パラグアイ、ウルグアイ、カナダ、ドミニカ、ジャマイカ 、スペイン、スイスへその活動が拡がっている。各国の企業や非営利団体または政府機関は STOP. THINK. CONNECT. Messaging Convention Inc. との間で国際活動パートナープログラムの締結を行い、それぞれの国において、サイバーセキュリティ啓発キャンペーンとしての開発が行われている。

図 2.4-1　STC 国際活動パートナープログラム加盟国[15]

日本国内では、フィッシング対策協議会内に 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 Web サイト

[15] http://education.apwg.org/safety-messaging-convention/overview/global-partners

(http://stopthinkconnect.jp/) の公開が行われた。2015 年 6 月 22 日には、Facebook ページ[16]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。2016 年 2 月現在、国内 20 団体がこのキャンペーンに賛同し、活動を推進している。

2.4.2. スローガンとロゴ

アメリカ国内では、山火事防止のキャラクターとして長らく親しまれている「Smokey Bear」やシートベルト着用を訴える「Click it or Ticket」キャンペーンが広く知られている。これらのように、サイバー空間における安全意識に関するキャンペーンとして、「STOP. THINK. CONNECT.」を定着させていくことがこのキャンペーンに対する願いである。

図 2.4-2　STC スローガンとロゴ[17]

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 つのステップの確認を推奨している。

- 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。

[16] https://www.facebook.com/StopThinkConnectJapan
[17] http://education.apwg.org/safety-messaging-convention/overview/global-partners

これら活動の更なる推進を目指し、民間企業、政府機関及び非営利団体による連合体が組織され、2010 年 12 月にバージニア州にて、STOP. THINK. CONNECT. Messaging Convention, Inc.が法人化された。
なお、アメリカ合衆国内国歳入庁（IRS）は、STOP. THINK. CONNECT. Messaging Convention Inc.を、内国歳入法典第 501 条 C 項 3 号 501(c)(3)の規定に基づき、連邦法人所得税免税や寄付税制上の優遇措置などの対象となる免税(Exempted)非営利公益法人として認定を行っている。

2.4.3. 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 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。

サイバーセキュリティ意識向上キャンペーンにも力を注いでいる会員制量販店「コストコ・ホールセール」では、発行する会員誌『THE COSTCO CONNECTION（ザ・コストコ・コネクション）』を通じて「Staying safe online is your responsibility Stop. Think. Connect.」というテーマで、同社の名を騙ったフィッシング詐欺に関する被害実例を示しながら、National Cyber Security Alliance の Michael Kaiser 氏から 3 つのアドバイスをオンライン詐欺に対する心構えとして紹介している。

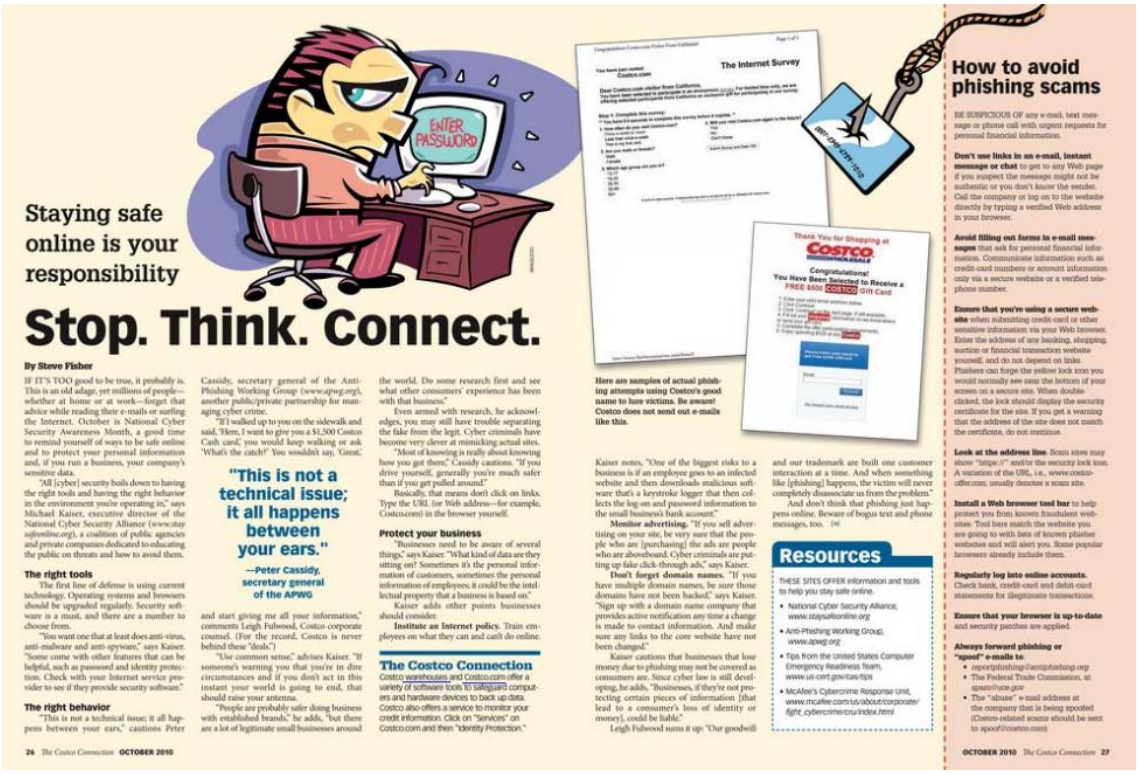


図 2.4-3 『THE COSTCO CONNECTION（ザ・コストコ・コネクション）』（抜粋）

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[18]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。

このほか、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』を。2015 年 10 月 14 日には、「サイバーセキュリティ国際キャンペーン」期間にあわせ、中学生向けのインターネットを安全に利用していただくためのルールやマナー、セキュリティなどを、インターネットの利用場面のイラストを用いた Q&A クイズ形式の学習資料『STOP. THINK. CONNECT. 立ち止まって、考えて、ネットを楽しむためのクイズ』を配信している。

2.4.4. 賛同組織による活動

日本国内においては、STC キャンペーンに賛同する組織による独自の活動も活発である。

BB ソフトサービス株式会社が運営するサイト「Online Security[19]」では、

[18] http://stopthinkconnect.jp/resources/
[19] http://www.onlinesecurity.jp/

フィッシング詐欺を題材にし、インターネット犯罪対策の啓発を目的とした漫画『THE WATCHERS』（瀬尾浩史 著）にて、STC キャンペーンを呼びかけている。

図 2.4-4　漫画『THE WATCHERS』（瀬尾浩史 著）（抜粋）

株式会社カスペルスキーがダウンロード提供、実費販売している冊子『セキュリティとモラルのハンドブック[20]』では、インターネットを安全に楽しむためとして、STC キャンペーンを呼びかけている。

千葉県警察本部サイバー犯罪対策課では、予てより、STC スローガンを使用し、サイバー空間における安全習慣についての呼びかけを行っている。2016 年 1 月 24 日に開催された「第 40 回 千葉マリンマラソン」では、約 1 万 8 千人のランナーに混じり、捜査員 20 人が STC タイアップ T シャツを着用し、更なる呼びかけを行った。その模様は産経新聞[21]、千葉日報[22]にて報じられている。

[20] http://kasperskylabs.jp/activity/csr/book.html
[21] http://www.sankei.com/region/news/160125/rgn1601250013-n1.html
[22] http://www.chibanippo.co.jp/news/national/300905

図 2.4-5　STOP. THINK. CONNECT. タイアップ T シャツ

2.4.5. 独立行政法人 情報処理推進機構 (IPA)との協力

独立行政法人 情報処理推進機構 (IPA)が継続的に実施している啓発活動とは、連携を目指し STC キャンペーンが検討されている。情報セキュリティ・ポータルサイト「ここから セキュリティ！[23]」では、サイバーセキュリティ国際キャンペーン関連コンテンツとして、STC Web サイトが紹介された。

また、IPA が主催する「ひろげよう情報モラル・セキュリティコンクール 2015[24]」では、「標語部門」/「ポスター部門」/「4 コマ漫画部門」の 3 つの部門において、優秀な作品に対し『優秀賞＜フィッシング対策協議会「STOP. THINK. CONNECT.」＞』と冠した表彰が実施された。

[23] http://www.ipa.go.jp/security/kokokara/
[24] http://www.ipa.go.jp/security/event/hyogo/2015/sakuhin.html

フィッシング対策協議会 STC 普及啓発ワーキンググループ (ワーキンググループ主査：丹京 真一、以下 「STC 普及啓発 WG」) は、IPA 主催の第 11 回 IPA 「ひろげよう情報モラル・セキュリティコンクール」 2015 を後援致しました。

情報セキュリティが叫ばれる中、小中高生の皆様にもセキュリティ意識を持っていただくために開催された IPA 主催の第 11 回 IPA 「ひろげよう情報モラル・セキュリティコンクール」 2015 を後援致しました。

以下の 3 つの部門において、優秀な作品に対してフィッシング対策協議会の賞を冠し、表彰することといたしました。

優秀賞の選考にあたり、STC 普及啓発 WG 主査の丹京 真一氏は、次のとおりコメントしています。
"我々は選考に際して、「STOP. THINK. CONNECT.」 キャンペーンの理念でもある 「立ち止まる 考える 楽しむ」 を意識し、ネットに潜む闇の部分に対して真摯に向き合い、安全な利用に向けての習慣を促している作品について、「標語」 / 「ポスター」 / 「4 コマ漫画」 の 3 部門毎に評価を行いました。最終的に 「フィッシング対策協議会 運営委員」 での承認を得て、今回の優秀賞を決定いたしました。"

STC 普及啓発 WG では、今後ともオンライン環境がすべてのインターネット利用者にとって安全になることを目指した活動に対してのさまざまな支援を継続して行っていきます。

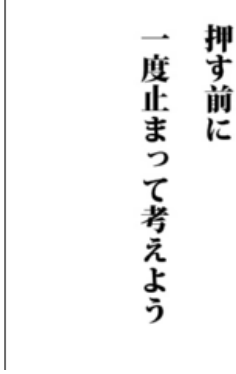
【標語部門】 優秀賞＜フィッシング対策協議会 「STOP. THINK. CONNECT.」＞ 桑木野　あずま さん 大阪府 大阪府立伯太高等学校 1 年	【ポスター部門】 優秀賞＜フィッシング対策協議会 「STOP. THINK. CONNECT.」＞ 但馬　涼子 さん 東京都 杉並区立天沼中学校 3 年	【4コマ漫画部門】 優秀賞＜フィッシング対策協議会 「STOP. THINK. CONNECT.」＞ 山川　潮莉 さん 岐阜県 岐阜県立岐阜総合学園高等学校 1 年
		

図 2.4-6　『優秀賞＜フィッシング対策協議会「STOP. THINK. CONNECT.」＞』受賞作品[25]

このほか、2016 年 2 月 1 日から 3 月 18 日までの「サイバーセキュリティ月間[26]」では、IPA、東京地下鉄株式会社 (東京メトロ)と協力し、「STOP. THINK. CONNECT.」 ポスターを、東京メトロにおける 160 の駅に掲出を行っている。

[25] https://www.antiphishing.jp/news/info/ipa_competition2015.html
[26] http://www.nisc.go.jp/security-site/month/index.html

図 2.4-7　青山一丁目駅における STC ポスター掲出風景

2.4.6. 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。詳細については、下記事務局まで。

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: 林 憲明氏(トレンドマイクロ株式会社)
副主査: 山本 和輝氏(BB ソフトサービス株式会社)
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　STC 普及啓発 WG]

3. 新しい攻撃手法・対策の動向

3.1. ショートメッセージを利用したフィッシング

フィッシング詐欺の多くは、まず、偽称したメールをユーザに送りつけ、あらかじめ用意した本物そっくりの偽サイトに誘導する。メールを使うことがフィッシングの典型的な手口であったが、2015 年にショートメッセージサービス（以下 SMS）を使ったフィッシングが発生した。（図 3.1-1）

図 3.1-1 SMS によるフィッシング例[27]

パスワードの変更を要求する SMS が海外から送信され、メッセージ内の URL から偽サイトに誘導される。誘導された偽サイトは ID と暗証番号、さらにワンタイムパスワードを入力させる画面になっておりメールを使ったフィッシングと同様である。

SMS は送信に費用が掛かることや端末認証のときに利用されるなど、メールと異なる面があるためフィッシングに使われないと思い込んでいる利用者も少なくない。SMS によるフィッシングはその思い込みに付け込んだ手法となる。また、フィッシングメールはスパムフィルタなどでブロックされる場合があるが、SMS はフィルタがかからず本人に届く場合が多い。利用者は偽メールに加え、偽の SMS にも注意が必要である。

[加藤 孝浩 トッパン・フォームズ株式会社]

[27]図はジャパンネット銀行より提供

3.2. オンラインバンキング詐欺における中間者攻撃における新しい方法

2014 年までは、日本の金融機関のインターネットバンキングの利用者を狙った不正ソフトウエアとしては、「ZBOT」,「VAWTRAK」[28]、「AIBATOOK」[29]が確認されていました。

いずれも利用者のインターネットバンキングの利用時に、ブラウザとインターネットバンキングのネットワークの間に、マルウエアが仲介し、ブラウザ上に偽のログインメッセージを表示して、認証情報を詐取したり、裏側で振込先を変更して預金を詐取したりします。いずれもシステム領域への変更を実行するため、感染の為には、高い権限を必要としている。Windows Vista 以降では、たとえ管理者権限で PC を利用していても、通常は低い権限で処理を行い、高い権限が必要になった時に、ユーザに確認メッセージを出し、承認を必要とする UAC が実装された。ただし、この UAC については、XP との互換性維持の為に UAC の回避機能が提供されており、マルウエアの感染では、この UAC の回避が一般的に使われている[30]。

2015 年に入りユーザが利用するブラウザとオンライン銀行のサイトとの間に新しい方法で介在する日本を標的としたマルウエアが見つかりました。
2014 年末から 2015 年初めに「TROJ_WERDLOD」の日本国内での感染が確認されました。「WERDLOD」は、感染時にユーザの PC の二つの設定を変更することで、認証情報の窃取を行い、感染後はマルウエアの起動や常駐を必要とせず、自身を削除してしまいます。一つ目の変更がブラウザの利用するプロキシーの設定を変更し、攻撃者が用意した不正なプロキシーを経由させます。二つ目は不正なルート証明書をインストールして、ブラウザが攻撃者の用意したプロキシーを経由した際に SSL サーバ証明書の検証エラーを出さないようにするものです。

非常に簡単な仕組みですが、設定の変更には特別な権限が必要ないことと、変更後は、変更を行ったマルウエアは、必要がないため削除できるので、攻撃側からするとセキュリティ対策製品に気が付かれるリスクを低くすることができます。

---

[28]http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=VAWTRAK+Plagues+Users+in+Japan
[29] http://blog.trendmicro.co.jp/archives/9236
[30]https://www.jpcert.or.jp/magazine/acreport-uac-bypass.html

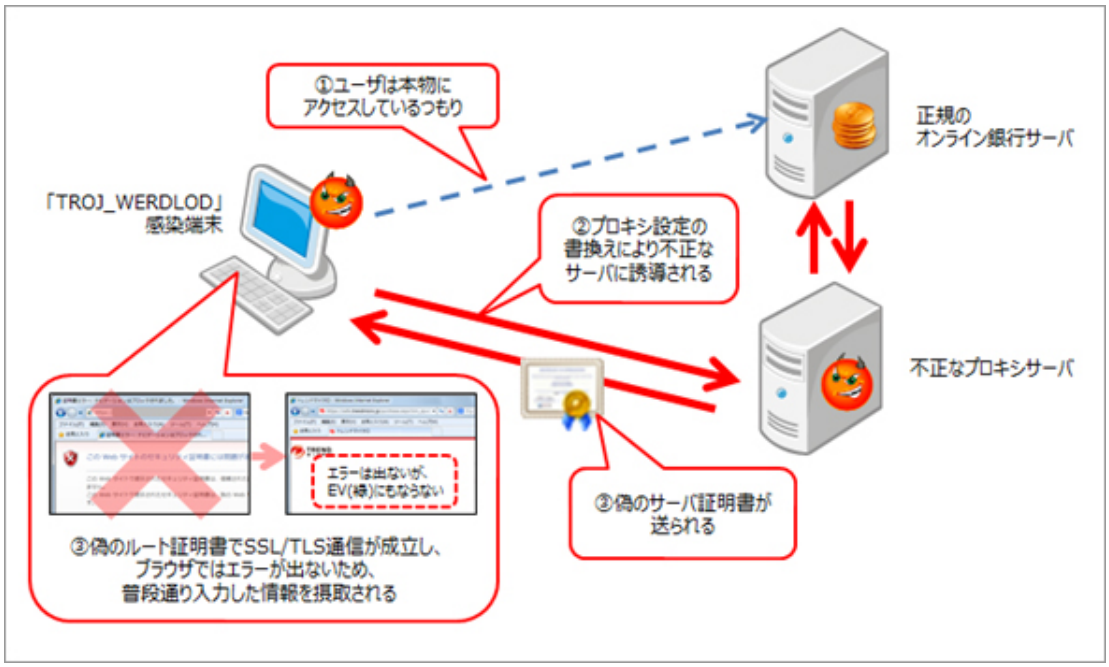


図 3.2-1　マルウエア TROJ_WERDLOD の動作

2015 年 10 月以降に請求書や注文確認メール、または FAX 受信通知などのメールを偽装したマルウエアスパムにより感染を広げる「SHIZ」が確認されました。「SHIZ」は PC 内でローカルプロキシーを実行し、WERDLOD と同様に認証情報を詐取します。

「VAWTRAK」のようにユーザのオンライン銀行利用の裏側で振込先口座番号や金額を変更する高度な手口もありますが、被害の多くは認証情報の詐取により、犯人が利用者になりすましてユーザの預金を搾取するのが主な手口となっています。

最後に、いろいろ新しい手口が出ていても、安全なオンライン銀行の利用方法を守るだけで被害は防ぐことができます。

もし、利用する金融機関がワンタイムパスワードカードなどを追加のセキュリティ強化オプションを提供している場合は、それらを利用することで認証情報の詐取による詐欺は防ぐことができます。また、パソコンのソフトウエアを常に最新にし、インターネットを利用するユーザは、一般ユーザ権限とするだけでマルウエアの感染リスクをかなり低くすることができます。

[野々下 幸治　トレンドマイクロ株式会社]

3.3. 金融庁監督指針／検査マニュアル、FISC ガイドライン改訂に伴う対応

近年、サイバー攻撃の増加や、その手口の複雑化・巧妙化が進んでおり、事業者において大規模な個人情報流出事件が発生するなど事態は深刻化している。しかしサイバー攻撃への対応については、事業者側の対応ノウハウや人的資源の制約がある中で、どのような具体的対策をとるべきか必ずしも判然としていない状況にあった。

我が国の重要インフラである金融システムにおいても同様な状況であり、サイバー攻撃によって利用者や決済システムに大きな被害が生じることが十分に想定される。

そこで金融システムの健全性確保の観点から、金融機関のサイバーセキュリティ強化を図るべく 2015 年 4 月から 6 月にかけて、金融庁の監督指針／金融検査マニュアル、ならびに金融情報システムセンター（FISC）の安全対策基準が改訂された。金融機関に対しては通常の事業者よりも高度なサイバー攻撃対応態勢の整備・運用が要求されているものと読み取ることができる。

以下にその概要を紹介する。

3.3.1. 監督指針／金融検査マニュアル

金融庁の監督指針／金融検査マニュアルにおけるサイバーセキュリティ強化の要諦は以下のとおりである。

① サイバーセキュリティについて、取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。

② サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。

> ・サイバー攻撃に対する監視体制
> ・サイバー攻撃を受けた際の報告及び広報体制
> ・組織内 CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制
> ・情報共有機関等を通じた情報収集・共有体制等

③ サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。

> ・入口対策（例えば、ファイアウォールの設置、抗ウイルスウイルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入等）
> ・内部対策（例えば、特権 ID・パスワードの適切な管理、不要な ID の削除、特定コマンドの実行監視等）
> ・出口対策（例えば、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断等）

④ サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を講じているか。

・攻撃元の IP アドレスの特定と遮断
・DDoS 攻撃に対して自動的にアクセスを分散させる機能
・システムの全部又は一部の一時的停止等

⑤ システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。

⑥ サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。

⑦ インターネット等の通信手段を利用した非対面の取引を行う場合には、以下のセキュリティの確保を講じているか。

・情報セキュリティに関する検討会の検討内容等を踏まえ、体制の構築時及び利用時の各段階におけるリスクを把握した上で、自らの顧客や業務の特性に応じた対策を講じているか。また、個別の対策を場当たり的に講じるのではなく、効果的な対策を複数組み合わせることによりセキュリティ全体の向上を目指すとともに、リスクの存在を十分に認識・評価した上で対策の要否・種類を決定し、迅速な対応が取られているか。
・インターネットバンキングに係る情報セキュリティ全般に関するプログラムを作成し、各種犯罪手口に対する有効性等を検証した上で、必要に応じて見直す態勢を整備しているか。また、プログラム等に沿って個人・法人等の顧客属性を勘案しつつ、全国銀行協会の申し合わせ等も踏まえ、取引のリスクに見合ったセキュリティ対策を講じているか。その際、犯罪手口の高度化・巧妙化等（「中間者攻撃」や「マン・イン・ザ・ブラウザ攻撃」など）を考慮しているか。
・Web ページのリンクに関し、利用者が取引相手を誤認するような構成になっていないか。また、フィッシング詐欺対策については、利用者がアクセスしているサイトが真正なサイトであることの証明を確認できるような措置を講じる等、業務に応じた適切な不正防止策を講じているか。

なお、認証方式や不正防止策として、全国銀行協会の申し合わせ（※）等には以下のセキュリティ対策事例が記載されている。

※セキュリティ対策向上・強化等に関する全国銀行協会の「申し合わせ」（平成 24 年 1 月、25 年 11 月、26 年 5 月、26 年 7 月等）における対策事例

・可変式パスワードや電子証明書などの、固定式の ID・パスワードのみに頼らない認証方式
・取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど、複数経路による取引認証
・ハードウェアトークン等でトランザクション署名を行うトランザクション認証
・取引時においてウイルス等の検知・駆除が行えるセキュリティ対策ソフトの利用者への提供
・利用者のパソコンのウイルス感染状況を金融機関側で検知し、警告を発するソフトの導入
・電子証明書を IC カード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式の採用
・不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備等

⑧ サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施しているか。また、必要に応じて、業界横断的な演習に参加しているか。
⑨ サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。

3.3.2. FISC の安全対策基準

金融機関等におけるサイバー攻撃対応態勢の整備に関することとして「FISC 安全対策基準」において基準項目【運 113】「サイバー攻撃対応態勢を整備すること」が新設された（表 3.3-1）。

表 3.3-1 【運 113】「サイバー攻撃対応態勢を整備すること」の内容

目的	内容
サイバー攻撃への対応に関する態勢の整備	サイバー攻撃に伴うシステムの停止や不正な資金移動に対する、「未然防止策・事前対策」、「検知策」、「対応策」を検討し、態勢を整備すること。
サイバー攻撃への対応に関する態勢整備にあたっての具体的な対策例の明示	態勢整備の後、上記の検討を具現化（表２）する。

なお、サイバー攻撃の手口は高度化かつ巧妙化しているため、サイバー攻撃対応態勢の整備にあたっては、手口の高度化や巧妙化にあわせて適時、見直すことが必要である。

基本的には表 3.3-2 に示す４つの対策が必要となる。

表 3.3-2　サイバー攻撃への４つの対策（【】で示す規程は本文を参照のこと）

	対策	具体的対策例
1	未然防止策・事前対策	(1) 外部の第三者によるセキュリティ評価を行うこと。不正侵入防止における評価については【技 43】を参照のこと。 (2) 業務委託先、業務提携先等のうち、重要な関係先のサイバー攻撃対応態勢の整備状況を確認すること。特に、外部委託先に対するサイバー攻撃対応態勢の整備状況確認については、監査の一環として行うことが有効であるため、【運 88】【運 90】【運 91】を参照のこと。 (3) インシデント発生時における部署間の連携や、外部との連絡窓口の機能を担い、経営陣への報告並びに経営陣からの指示を実施することができる組織を整備すること。例として CSIRT(Computer Security Incident Response Team)の設置等がある。【技 43】(参考 4) (4) 大規模な攻撃が行われた場合も含め、サイバー攻撃発生時の外部ベンダー等のフォレンジックなどに関するサービス提供能力を把握すること。 (5) 顧客が必要とする機能、並びに利用環境や IT リテラシー等のセキュリティレベルを踏まえて、利用可能な機能や限度額を設定すること。取引制限については【技 38】を参照のこと。 (6) インターネット取引を求める顧客に対し、不正プログラム対策ソフトの導入有無等、利用者が利用するパソコン環境の事前告知を求めること。
2	検知策	(1) インシデントレスポンス態勢を整備すること。その前提として、システム全体の監視を行うことが必要となるため、【運 60】を参照のこと。 (2) アクセス履歴を監査すること。アクセス履歴の監査については【技 37】の 2.を参照のこと。 (3) 不正アクセス監視の一環として、侵入検知システム等による自動監視等、ネットワークの監視を行うこと。詳細については、【技 45】を参照のこと。
3	対応策	(1) サイバー攻撃の発生直後はシステム障害と区別ができない可能性も想定されるため、システム障害時にサイバー攻撃の可能性を考慮すること。システム障害時の対応手順の整備については【運 63】、連絡手順については【運 62】を参照のこと。 (2) 利用者(顧客)への説明を行うこと。顧客への対応方針については、【運 105-1】を参照のこと。 (3) システムの全部または一部を、一時的に停止すること。不正アクセスの拡大防止については、【技 48】を参照のこと。 (4) 侵入経路及び手口、情報流出の痕跡及び範囲などを分析するフォレンジックを実施すること。ただし、サイバー攻撃の高度化及び複雑化に伴い、フォレンジックに必要なデータの取得対象、範囲及び期間並びに事象発生時の証拠保全方法は変化することから、実施にあたっては、専門的な知識や技術を持つ外部業者に委託することも有効である。
4	教育・訓練	(1) サイバー攻撃を想定した対応訓練を実施すること。 (2) サイバー攻撃対応の意識を高めるためにも、データやファイル交換を行う当事者同士が必要に応じて相互のサイバー攻撃対応態勢について確認すること。 (3) 教育・訓練の実施に際しては、コンピュータセンターと本部・営業店等との連携を行うこと。また、業界団体が訓練を開催する場合には参加すること。 (4) サイバー攻撃を受けるリスクや、受けた場合の対応手順は、関係する役職員、外部委託先に対して周知、啓発を行い、訓練を実施すること。関係する役職員に対しては【運 80】、外部委託先に対しては【運 89】をそれぞれ参照のこと。 (5) 顧客に対して、サイバー攻撃を受けるリスクや防止策を周知し、注意喚起を行うこと。注意喚起すべき内容については【運 105-1】を参照のこと。

以上、サイバー攻撃対応態勢の整備と具体的対策例を述べたが、サイバー攻撃の手口は絶えず変化、巧妙化することが予想されるので、今後、金融機関等の現場においては「FISC 安全対策基準」のどの対策で解釈運用すればよいのか判断に迷うケースが生じると考えられる。

そのため FISC では、状況に応じて安全対策基準の適切な解釈・運用のために有用な留意点及び参考情報を「FISC サイバーセキュリティ参考情報」として、FISC のホームページ等で公開しており、適時そちらも参照することが必要である。（https://www.fisc.or.jp/isolate/?id=822&c=topics&sid=241）

[八津川 直伸　日本ユニシス株式会社]

3.4. パスワードが抱えている問題点と複数要素認証

インターネット上では、さまざまな場面で利用者の本人確認が求められる。それは、オンライン銀行の口座にアクセスするとき、メール、健康情報、写真や動画、ソーシャルネットワーキングサイトなどである。このような場面において、最も多くのサービスで利用されているのが「ID」と「パスワード」の組による認証である。

3.4.1. 犯罪者がパスワードを探り出す手口

では、パスワード認証はあなたを確認する上で最良の方法なのか。表 3.4-1 が示すとおり、犯罪者はあらゆる手段を通じて利用者のパスワードを探りだそうとしている。

これらの中には利用者の注意だけでは防ぐことのできない手口もある。

表 3.4-1　犯罪者がパスワードを探り出す手口

No.	攻撃名	詳細
1	ソーシャルエンジニアリング	盗み見、盗み聞き、話術などの手段で探り出す攻撃方法。
2	ショルダーハック（shoulder hack）	パスワードなどの重要情報を入力している際に利用者に気づかれることなく近づき、入力する際のキー操作や画面を覗き見ることで探り出す攻撃方法。
3	類推攻撃（Guessing）	対象者の嗜好をソーシャルメディアなどの公開情報を使って調べ、パスワードを類推し、探り出す攻撃方法。 特にパスワード再設定の際の「秘密の質問」の答えとなるような情報（明らかな事実：[誕生日]/[母親の旧姓]/[ペットの

		名前]/[好きな果物]など）については、必ずしも秘密となっていない場合があることを知っておくべきである[31]。
4	パスワードリスト攻撃	利用者の多くが複数サイトで同一の ID とパスワードを使い回ししている状況に目を付け、事前に不正取得した他人の ID とパスワードのリストを連続自動入力プログラムを用いてログインを試行し、不正取得したものと同じ ID とパスワードの組を探り出す攻撃方法
5	フィッシングサイト	個人情報を所有している組織名を不正に名乗ったサイトを構築し、閲覧者に安心感を抱かせ、ID とパスワードの組を入力させる攻撃方法
6	ブルートフォース（Brute Force）攻撃	特定の ID に対してパスワードとなりうる英数記号の全ての組み合わせを順に試して、探り出す攻撃方法。 これに対し、パスワードを固定して ID の変更によって試行が行われる「リバースブルートフォース」と呼ばれる攻撃方法もある。
7	マルウエア（Malware）	犯罪者によって設計されたプログラムによって、探り出す攻撃方法。 入力したキー情報をすべて記録する「キーロガー」や、操作画面を記録する「スクリーンスクレーパー」、通信を盗聴する「スニファ」、特定のサイトへ訪れた場合に偽画面を表示させる「Webinject」、正規の Web サーバによって提供される Web ページに新しい HTML を注入し、ブラウザのメモリから直接情報を取得する「MITB: Man-in-the-Browser」など複数の機能が組み合わせた攻撃が確認されている。
8	レインボーテーブル（Rainbow Table）攻撃	あらかじめパスワードとなり得る文字列から事前にハッシュ値を算出。それを対応表（テーブル）とし、検索することで、探り出す攻撃方法。
9	辞書（Dictionary）攻撃	パスワードに、利用者にとって記憶しやすい文字列（一般的な単語、人名、地名、生年月日など）を辞書として用意し、これらをパスワードとして機械的に次々と当てはめ、探り出す攻撃方法。

このような状況を踏まえ、注目を集めているのが「複数要素認証（Multi Factor Authentication）」である。フィッシング対策協議会では、『フィッシング対策

[31] https://googleonlinesecurity.blogspot.jp/2015/05/new-research-some-tough-questions-for.html

ガイドライン[32]』において、複数要素認証の要求を推奨している。

3.4.2. 認証を行うための要素とは

認証をおこなうための「要素」とは、表 3.4-2 が示す 3 つに分けることができる。

表 3.4-2　犯罪者がパスワードを探り出す手口

分類	説明	メリット	デメリット	具体例
知識情報 SYK:Something You Know	本人のみが記憶している情報に基づいて認証	汎用性が高く実装コストが安価	忘却、漏えいの危険性が高い	パスワードや暗証番号
所持情報 SYH:Something You Have	本人のみが所持している物によって認証	実装や管理が容易	貸し借り、紛失、盗難の恐れがある	乱数表、 ハードウェアトークン、 携帯電話
生体情報 SYA:Something You Are	本人の生体データにより認証	なりすましが困難 忘却の恐れがない	実装コストが高価 体調変化により認識できない場合がある	指紋、静脈、虹彩、顔

ID とパスワードの組合せは、知識情報のみを使用した認証方法である。この状態は、自分のアカウントを守るためにたった一つの保護層に頼っている状態といえる。

3.4.3. 認証におけるトークン

認証におけるトークンとは、NIST SP 800-63-2[33]「Electronic Authentication Guideline」において、「認証要求者が所持し管理する何かであり、認証要求者の身元識別情報の認証に使用でることができる」と定義している。NIST SP 800-63-2 では、そのトークンを 9 種類に分類している。表 3 は、9 種類のトークンの種類と定義を示している。

[32] http://www.antiphishing.jp/report/guideline/antiphishing_guideline2015.html
[33] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

表 3.4-3　NIST ガイドラインにおけるトークンの種類と定義[34]

要素数	SYK	SYH	SYA	名称	概要及び利用方法
単要素	○			記憶された秘密トークン（Memorized Secret Token）	サービスサイトとの間で共有する秘密情報を使った認証。
	○			事前登録知識トークン（ Pre-registered Knowledge Token）	あらかじめサーバに登録した質問に対する回答による認証。
		○		ルックアップ秘密トークン（Look-up Secret Token）	サービスサイトとの間で共有される秘密情報を使った認証。
		○		帯域外トークン（Out of Band Token）	あらかじめ登録した携帯電話やスマートフォンなどに通知されるワンタイムパスワードによる認証
		○		単要素ワンタイムパスワードデバイス（Single-factor（SF） OTP Device）	トークンによって生成されるワンタイムパスワードによる認証。
		○		単要素暗号デバイス（SF Cryptographic Device）	暗号機能をもつハードウェアによる認証 TLS のクライアント認証（"certificate verify” メッセージ）
複数要素	□	○	□	複数要素ソフトウエア暗号トークン	利用するための第 2 の認証を必要とする情報による認証（暗号機能を使うための情報）。
	□	○	□	複数要素 ワンタイムパスワードデバイス（MF OTP Device）	利用するための第 2 の認証を必要とするトークンによって生成されるワンタイムパスワードによる認証。
	□	○	□	複数要素暗号デバイス（MF Cryptographic Device）	利用するための第 2 の認証を必要とする IC カードなどの暗号機能をもつハードウェアによる認証。

表内の○は必須の要素であり、□はいずれかの要素を用いることを示す。

[34] 独立行政法人情報処理推進機構『「オンライン本人認証方式の実態調査」報告書』, P7 より抜粋。
https://www.ipa.go.jp/files/000040778.pdf

3.4.4. 二要素認証とは

第二の要素を追加することで保護技術の層に厚みを持たせようとするのが、「二要素認証: Two-Factor Authentication」である。二要素認証では、二つの要素が揃っていなければ、認証を行うことができない。したがって、たとえ ID とパスワードが犯罪者に知られたとしても、もう一つの要素を取得されない限り、ログインすることができない。

ここで注意しなければいけないのが、同じ要素のみで構成される認証は厳密には、二要素認証として成立しない。例えば、パスワードに加えて、「秘密の質問の答え：事前登録知識」を認証要素として使用している場合、2 つの情報で認証を行っているが、いずれも知識情報に分類できる。このような認証方式は「多段認証・多段階認証」と呼ばれている。

フィッシング対策ガイドラインでは、サービス事業者におけるフィッシング詐欺対策の実施必要性として、複数要素認証に高い優先度を設定している。

- 正規サイトログイン時の認証には複数要素認証を利用すること（推奨事項）
- 資産の移動を実行する前に、複数要素認証を要求すること（実施すべき事項）

3.4.5. 「所持」と「生体」情報による「FIDO：Fast Identity Online」

利用者はパスワードでログインが必要なサイトを 1 人あたり 13.95 サイト利用していることが報告[35]されている。このような状況において、「SYK：知識情報」を利用者の記憶のみによって管理することは極めて困難である。従って、利用者は適切な方法で知識情報を管理することが求められる。しかしながら、利用者によるパスワードの使い回し[36]や、不適切な管理によって知識情報が漏えいする事件[37]が発生している。

こうした状況を受け、生体情報を使ったオープンなオンライン認証のプロトコル仕様を確立しようとする動きが注目されている。それが「FIDO(Fast IDentity Online) Alliance[38]」である。

FIDO Alliance では、公開鍵暗号方式に基づいて、「パスワード置き換え型（UAF：Universal Authentication Framework）」と「パスワード補完型（U2F：Universal Second Framework）」の 2 つの標準プロトコルを策定している。

---

[35] http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20130829075331.html
[36] https://www.jpcert.or.jp/pr/2014/pr140004.html
[37] 利用者が記憶の補助を目的に自らの意思でテキスト投稿・共有サービスにパスワード情報を記録。同サービスが初期設定で不特定多数によって閲覧可能な状態となっていたために、利用者の意図しない情報の漏えいが発生したという事件が報告されている。
[38] https://fidoalliance.org/

特に UAF 認証ではパスワードを含む知識情報を使用せず認証を行うものである。利用者はデバイスに「SYA：生体情報」を登録し、オンラインサービスにそのデバイス「SYH：所持情報」を登録すれば、デバイスの認証だけでログインが可能となる。

これにより、個人認証に用いる情報がインターネットを経由することがなくなり、流出の可能性が無くなることが期待されている。

■コラム：パスワード管理ソフトウエア

前述のとおり、知識情報のみに頼ったパスワード認証には様々な問題点を抱えていることは明らかである。しかしながら、UAF 認証など知識情報を使用しない認証の普及には時間を要する。したがって、パスワード認証が過渡期であるとの現状を考慮した現実的なアドバイスを推進していくことが重要である。

適切な知識情報の管理を支援する方法の一つとして「パスワード管理ソフトウエア」が注目されている。

図 3.4　パスワード管理ソフトウエア例：トレンドマイクロ パスワードマネージャー

パスワード管理ソフトウエアは、さまざまなサービスのパスワードを一元的に管理することができる。利用者は個々のパスワードを記憶する必要無く、マスターパスワードなどの入力によって各サービスを利用することができる。したがって、利用者へ複雑なパスワードの記憶による負担を強いることなく、適切なパスワードポリシーの遵守、実践が可能となる。

なお、「フィッシング対策ガイドライン」[39]では、ブラウザにおけるオートログイン機能ではなく、別途パスワード管理ソフトウエアを用意し、利用することが推奨されている。これは、ブラウザの脆弱性による ID/パスワードの窃盗リスクを考慮した推奨事項である。

以下の選考基準を参考に、利用者が必要と考える機能（例：自動ログイン、マルチデバイス対応やクラウドへのパスワード保管など）を見極めながら、パスワード管理ソフトウエアを選考することが望ましい。

金融機関では、パソコンのウイルス感染により、パソコン内のデータだけでなく、そのパソコンを利用したネットワーク上のサービスも乗っ取られることで、第三者に ID／パスワードを詐取されて不正送金される被害が発生している。金融機関のインターネットバンキングなどの ID／パスワードのパソコン、スマートフォン、Ｅメール、クラウドサーバー、ネットワーク上のサービス等への保管は特に注意が必要である。

表　パスワード管理ソフトウエアの選考基準

選考基準	理由
実績のあるソフトウエアを選ぶ	総合セキュリティ対策製品に付属している機能、セキュリティソフトウエアを継続してリリースしているなど、実績のある会社が提供しているソフトウエアを選ぶべき。 併せて、ソフトウエアは信頼できる公式サイトからの誘導に従って入手すべき。
安全性の高いパスワードの作成支援機能	パスワードの強度（長さ、複雑さ）の弱いパスワードをそのままにして一元管理または強度の弱いマスターパスワードで使用した場合、パスワード

[39] http://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf

	管理ソフトウエアはその効果を十分に発揮できない。
パスワード管理ソフトウエアによって保存される秘密情報の暗号化機能	万一パスワード管理ソフトウエアによって保存された秘密情報が漏えいしても暗号化されていればデータは意味のないものになり、実害を防ぐことが期待できる。

■コラム：文字入力に拠らない画像認証

利用者に安全性の高い文字列のパスワードを、長期的に記憶させることは困難である。

そこで、人間の画像認識能力の高さを利用し、画像を認証のパスワードとして用い、本人の知識情報を確認することによって認証を行う「画像認証」が注目されている。

画像認証は主に下記の方式に分類することができる。

表　画像認証方式[40]

方式名	詳細
Cognometric 方式	複数の画像から、本人のみが知る正しい画像を選択
Locimetric 方式	画像内の本人のみが知る特定箇所をマウス操作等により指定
Drawmetric 方式	本人が画像を描画し、事前に登録済みの描画パターンと照合

Microsoft 社では、Windows 8 以降、「ピクチャ パスワード」[41]と呼ぶ Locimetric 方式の画像認証機能を実装している。これは、利用者が選択する任意の画像とジェスチャを組み合わせることで、利用者に強いる記憶の負担を軽減することを狙った実装方法である。

また、Google 社では、Android 4.0（Ice Cream Sandwich）以降において画面ロックにおける認証方式として「パターン」[42]と呼ぶ Drawmetric 方式の画像認証機能を実装している。　このほか、Drawmetric 方式の利点を採用

[40] 電子政府ガイドライン作成検討会 セキュリティ分科会「電子政府ガイドライン作成検討会 セキュリティ分科会報告書」, https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf

[41] http://windows.microsoft.com/ja-jp/windows-8/personalize-pc-tutorial

[42] https://support.google.com/nexus/answer/2819522

したパスワード管理ソフトウエアもリリースされている。パスロジ社の「パスクリップ」[43]などがある。

これは、利用者があらかじめパターン（「位置」と「順序」からなる軌跡）を決定記憶し、ソフトウエアがサービス毎に異なる「マトリックス表（乱数表）」を示すことで、利用者があらかじめ決めたパターンに従って文字列を取り出せばサービス毎に異なる文字列の組をパスワードとして採用することができる仕組みである。利用者に求められるのは覚えやすいパターンの記憶のみとなるため、利用者に強いられる記憶の負担を軽減することが期待できる。

図 3.4　マトリックス表からあらかじめ決定したパターンに従って文字列を取り出す様子：パスロジ パスクリップ（PassClip）

パスワード認証が過渡期である現状においては、画像認証のような。利用者による知識情報管理の助けとなるような認証方式の検討が重要である。

[林 憲明　トレンドマイクロ株式会社]

[43] https://www.passclip.com/

3.5. ワンタイムパスワード

3.5.1. パスワード認証の危険性

利用者が、オンラインの銀行・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の Web サービスを利用する場合、ID とパスワードを入力しログインするケースが多いであろう。しかし、この ID とパスワードが悪意のある第三者に渡り、サービスを不正利用される危険性が昨今、ますます増加している。パスワードが悪意ある第三者に渡る、あるいは特定されるケースは、以下参考のとおり多岐にわたり常にリスクが存在する。中には利用者の注意では防ぐことができないケースもある。

＜参考：パスワードが悪意ある第三者に渡る、または特定されるケース＞

①パソコンがマルウエアに感染し、パスワードに何を入力したか直接読み取られる。

②パソコンと Web サーバ間の通信を傍受され、送信されたパスワードが読み取られる。

※ネットカフェや職場の LAN、自宅や公衆 Wi-Fi 無線などは通信データを読み取ることが可能な場合がある。例え暗号化されていても、パソコンや Web サーバが古く、暗号化方式が古い場合や、設定に不備がある、ソフトウエアを最新化せず不具合があるまま使用している場合などにおいては、容易に複合化されてしまう可能性がある。

③フィッシング詐欺に遭い、偽サイトにパスワードを入力してしまう。

④利用者の背後から、パスワードを入力している様子を盗み見られる。

⑤利用者の知人や同僚あるいは SNS で利用者の様々な情報を入手した第三者が、誕生日や好きなものなどからパスワードを推測し当ててしまう。

⑥利用者が知人や同僚に、何気ない会話の中でパスワードそのもの、あるいはパスワードを類推できるヒントを喋っている。

⑦パスワードが簡単あるいは一般的な単語等にしている場合、総当たりあるいは辞書攻撃と呼ばれる片っ端から試みる手法により、パスワードが特定されてしまう。

⑧利用している複数の Web サービスのうち１つが、悪意あるハッカーに侵入されサーバ内に保存していたパスワードを抜き取られた場合、利用者が同じ ID とパスワードを使いまわしていると他の Web サービスでも不正利用される。

3.5.2. ワンタイムパスワードとは

利用者がパソコンやスマートフォンなどから入力するパスワードが、サーバ側と利用者側の一定の取り決め（後述）に従って、１回ごとに変化する仕組みである。これによって、万一前述したケースにより、ある１回のパスワードが悪意ある第三者に渡ったり特定されても、正規利用者によって一度使われたパスワードの再利用はできず、また次のログイン時のパスワードは別のものに変わっているため不正ログインはできない。
ログインの際には、ID と従来の固定のパスワードに加えて、ワンタイムパスワード入力を求める場合や、ID とワンタイムパスワードのみで行う場合など、そのサービスにより異なる。

＜ワンタイムパスワード例＞

ある回のログインパスワード：	736183	←第三者がこれを知り得ても、
次のログインパスワード　：	263494	次のログインはできない。
次のログインパスワード　：	855168	

3.5.3. ワンタイムパスワードの種類

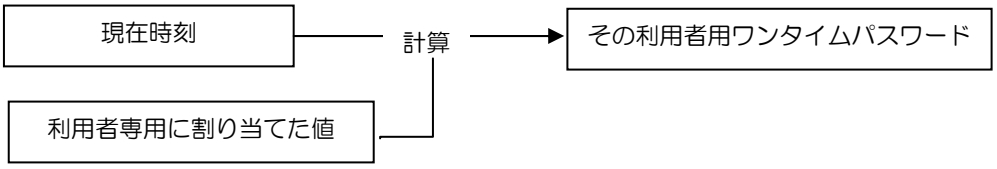
利用者側とサーバ側で次のパスワードを認識しあう必要があり、その方式は様々あるが主なものを以下に記載する。

① 現在時刻を元にする方式

現在時刻を元に、利用者側およびサーバ側でパスワードを相互に同一の特別な計算で求める。

利用者側では、携帯型の専用の装置やスマートフォンアプリが計算およびパスワードのディスプレイ表示を行う。

相互に時刻合わせが必要で、NTP などの時刻同期の仕組みが備わっている。

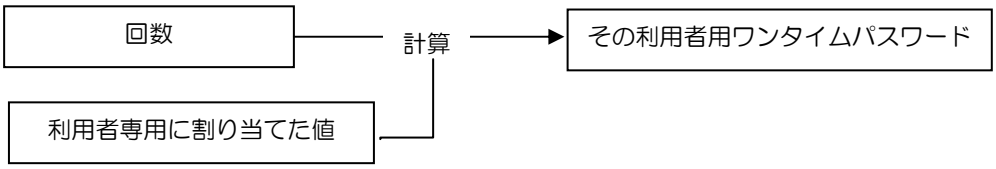


② パスワード生成の回数を元にする方式

次が何回目のパスワード生成かを利用者側とサーバ側でカウントして認識しており、相互に同一の特別な計算で求める。

利用者側では、携帯型の専用の装置やスマートフォンアプリが計算およびパ

スワードのディスプレイ表示を行う。
　相互に認識する回数がずれる可能性があり、別途同期する仕組みが備わっている。



③ メールや SMS で通知する方式
　ID と固定のパスワードを入力し認証成功した後、サーバ側で生成したワンタイムパスワードを、携帯やスマートフォンのメールアドレスや SMS 宛に送信し利用者に伝える。
　地下など携帯キャリアの電波が届かない、あるいは WiFi が無い環境などでは利用できない。

④ 乱数表を表示させる方式
　ログイン画面に乱数表を表示し、利用者はあらかじめ設定してある乱数表の位置と順番に従い、そこに表示されている数字を入力していく。
　該当の位置には、毎回異なる数字が表示されるため、入力するパスワードを毎回変えることができる。

3.5.4. ワンタイムパスワードの積極的利用

　利用者がワンタイムパスワードを利用する場合、悪意のある第三者が不正ログインをするためには、ID と固定パスワードの入手の他、ワンタイムパスワードを表示する機器やスマートフォン自体も入手する、あるいは、乱数表の位置情報も入手する必要があり、不正ログインは非常にしにくいものとすることができる。
　サービス事業者はワンタイムパスワードの導入および積極的な普及を推進し、利用者も自らを守る観点から積極的に利用することで、悪意ある第三者の不正ログイン成功率を低減させることができる。最終的に、不正ログインを試みる行為にかかるコストより、得られるメリットを下げることができれば、不正ログインを試みる行為そのものを減少させることができると考えられる。

3.5.5. ワンタイムパスワードの制限

例えば、フィッシングなどの偽サイトにワンタイムパスワードを入力してしまった場合、悪意ある第三者は、ワンタイムパスワードを使って不正ログインを試みることが可能である。金融機関では、利用者がID・パスワードを偽サイトに入力している裏で第三者がログインしてリアルタイムでワンタイムパスワードを入力させて詐取する新たな手口も発生している。しかし、現在時刻を元にした方式では入手したワンタイムパスワードを短時間のうちに利用する必要があるなど、従来の固定パスワードだけに比べて安全性が大幅に向上する。他の認証方式やセキュリティ方式と同様に注意すべき点もあるものの、それでも利用者は余りあるメリットを享受することができる。是非、積極的に利用することを推奨する。

[早川 和実　ＮＴＴコミュニケーションズ株式会社]

4. まとめ

2014 年にピークを迎えたフィッシング被害は、2015 年には件数こそ前年より微減したものの、被害額では 2014 年を超えるなど、引き続き極めて高い水準で推移した。

内容的には、金融機関をかたってフィッシングを仕掛け、ネットバンクの不正送金を目的としたものが目立つのも 2014 年の傾向と同様である。

金融機関としての対策も、ワンタイムパスワードの導入拡大などで進展は見られるものの、被害の完全な防止には至っていないのが実情である。また金融機関がワンタイムパスワードを導入しても全ての利用者が使用するには至っていない。またワンタイムパスワード導入も大手金融機関が中心であり、地方銀行等における導入は今後の課題であろう。

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
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