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 2017

－　普及が進むユーザ認証の新しい潮流　－

2017 年 6 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

国内金融機関を対象としたフィッシングは 2015 年に引き続き 2016 年も高水準に移行したが、春頃から急速に減少した。一方でこれまで目立った攻撃のなかった LINE などの SNS を対象とした攻撃が増えたのが 2016 年の特徴であった。

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に係る不正送金は前年度に較べて件数、被害額ともに減少傾向にあるが、引き続き高水準であるだけでなく、電子決済サービスを使用して電子マネーを購入する手口などが増加するなど、手法も高度化してきている。

フィッシング対策協議会の統計でも、2016 年のフィッシング届出件数は 2 月にピークとなったが、その後急速に減少し、4 月頃から比較的低位な水準で移行した。この減少の要因は、金融機関を対象としたフィッシングの届出が急減したためである（図 1-1）。

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、対前年比で若干減少した（2015 年 11,408 件→2016 年 10,759 件）一方で、フィッシングサイトの件数は 1.3 倍に増加し（図 1-2）、ブランド名を悪用された企業の延べ件数は大きく増加（2015 年 164 件→2016 年 261 件）した（図 1-3）。

2016 年の傾向として、フィッシングの対象となるブランド数が増加に転じたことがあげられる。これは新しい攻撃対象として SNS などへの攻撃が増加したことを反映しているものである。

[1] 警察庁, 平成 28 年中におけるサイバー空間をめぐる脅威の情勢等について, https://www.npa.go.jp/kanbou/cybersecurity/H28cyber_jousei.pdf

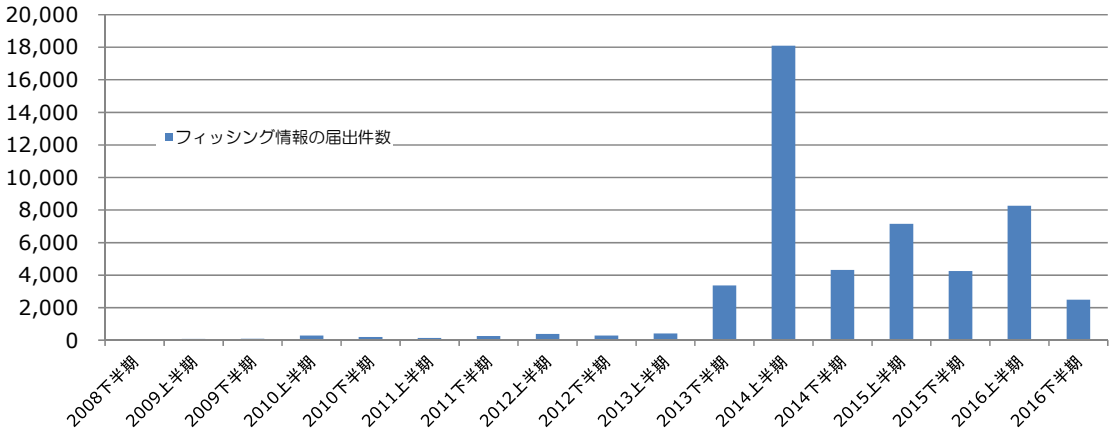


図 1-1　フィッシング情報の届出件数

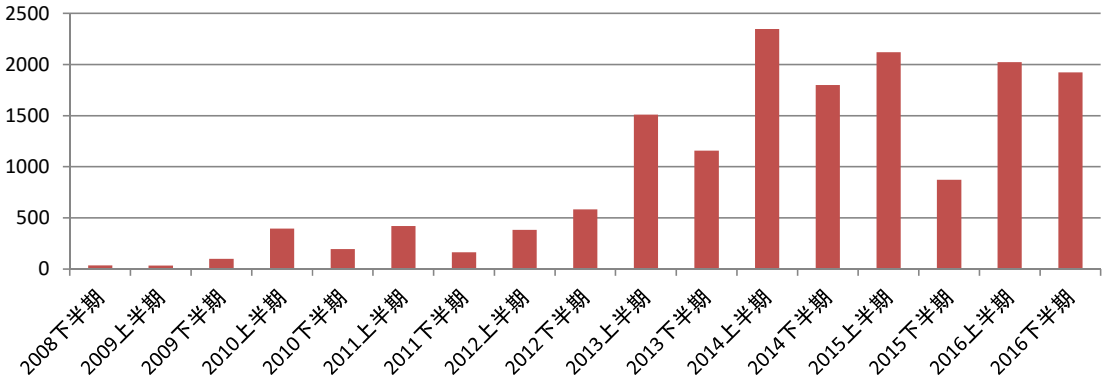


図 1-2　フィッシングサイトの件数

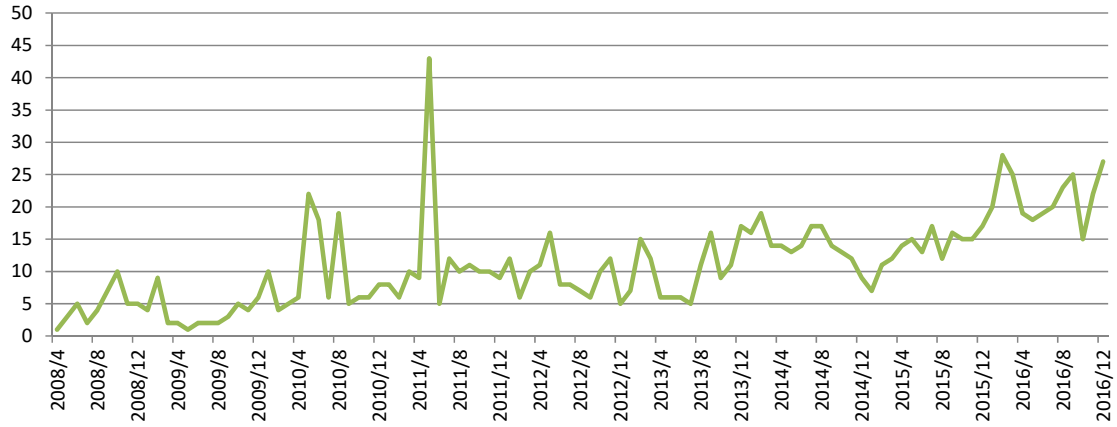


図 1-3　ブランド名を悪用された企業の件数

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）は昨年度に比べてやや増加した（図 1-4）。また、そ

の手口を見ると、2016 年におけるフィッシングは 3 件であり、比率は約 1%となっている（図 1-5）。前年はそれぞれ 24 件 7%、前々年は 71 件 21%であったことを考えると、フィッシングの検挙件数および検挙に占める比率は大幅に低下してきている。

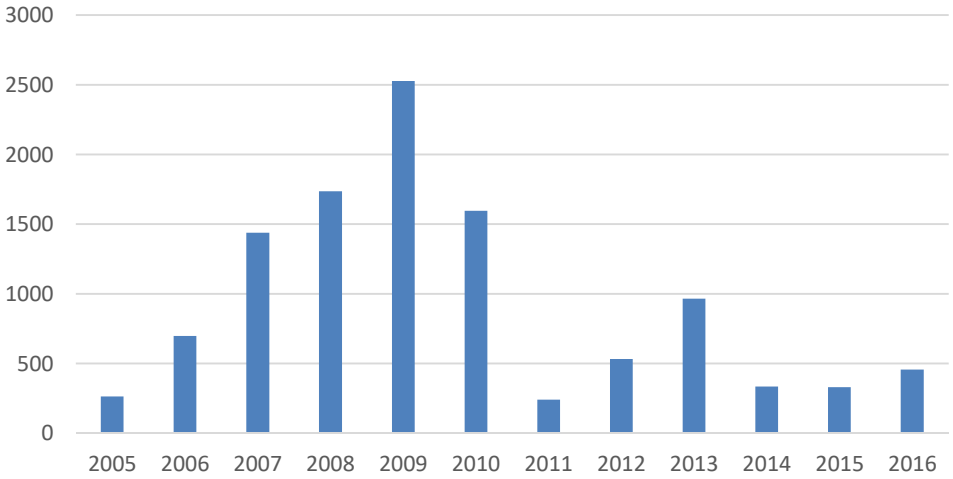


図 1-4　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数[2]

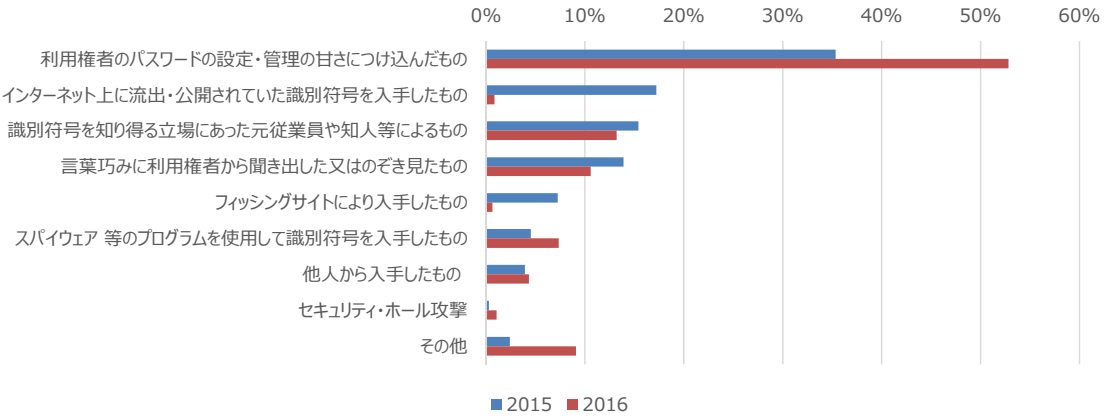


図 1-5　不正アクセス行為に係る犯行の手口の内訳（2015 年、2016 年）[3]

ここ数年、特に問題となっているのは、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、インターネットバンキングの不正送金の被害額は 2014 年には 1,876 件、約 29 億円、2015 年には 1,495 件、約 31 億万円、

---

[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」,http://www.meti.go.jp/press/2016/03/20170323002/20170323002-1.pdf よりフィッシング対策協議会が作成

[3] 同上

[4] https://www.npa.go.jp/kanbou/cybersecurity/H28cyber_jousei.pdf

2016 年は若干減少し 1,291 件、約 16 億 8,700 万円となっている。この減少については金融機関の対策が進んできたことが理由として考えられるが、引き続き高水準である。

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、2016 年上期のフィッシング届出件数は、2015 年に引き続き過去最高水準となった（図 1-6）。2016 年下期には届出件数は減少したが、フィッシングサイトの件数はそれほど大きな減少は観察されていない。引き続き注意が必要である。

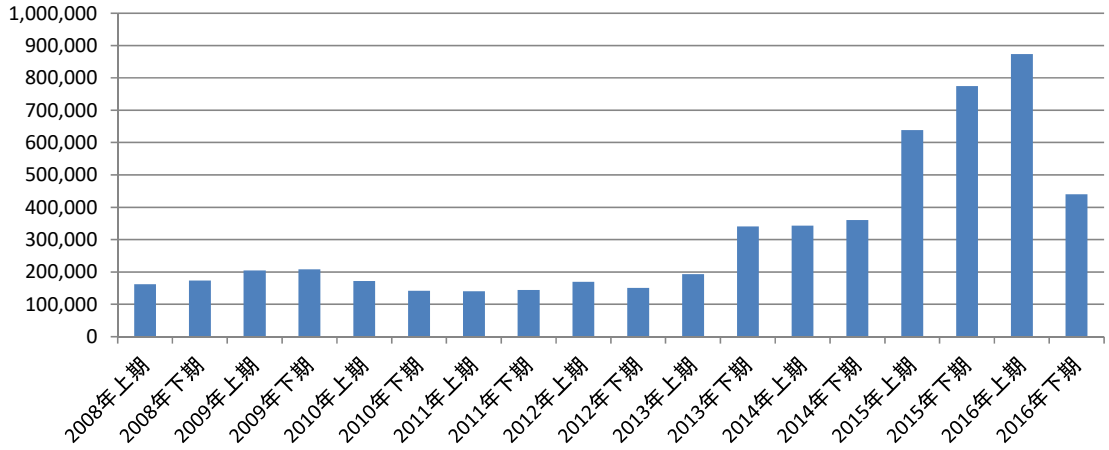
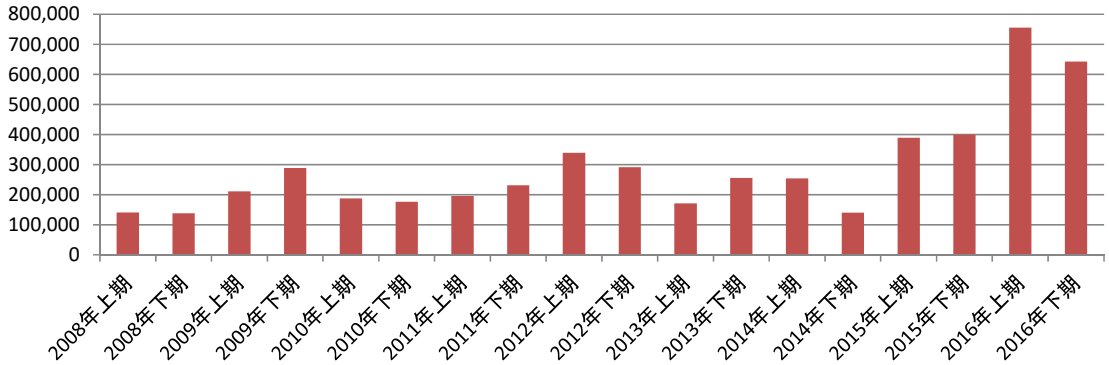


図 1-6　APWG へのフィッシングメール届出件数[5]



[5] APWG （Anti-Phishing Working Group), "Phishing Activity Trends Report"、http://www.antiphishing.org/resources/apwg-reports/、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]

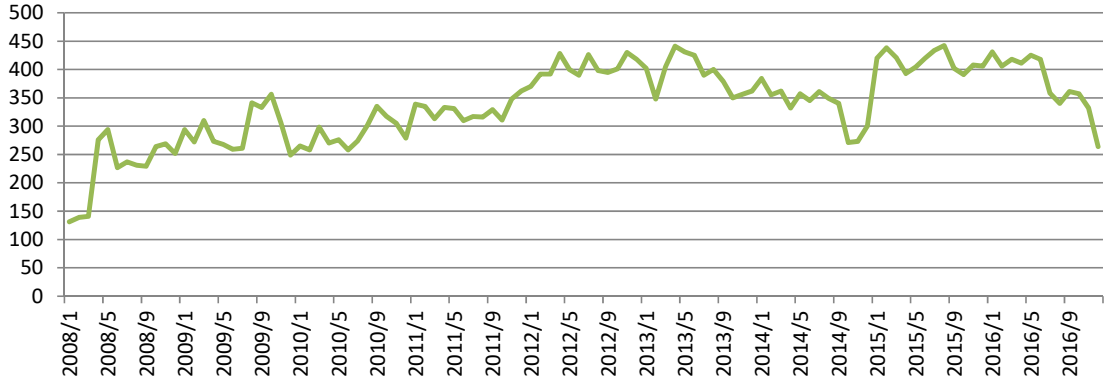


図 1-8　フィッシングによりブランド名を悪用された企業の件数（APWG）[7]

[株式会社三菱総合研究所]

[6] APWG (Anti-Phishing Working Group), "Phishing Activity Trends Report"、http://www.antiphishing.org/resources/apwg-reports/、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/resources/apwg-reports/、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. スピアフィッシング

「ビジネスメール詐欺（BEC：Business E-mail Compromise）」とは、「スピアフィッシング」の一種である。役員や取引先などを装ったメールを送りつけ、犯罪者の管理下にある口座へと誘導し、多額の送金などを指示するオンライン詐欺である。経営幹部という大きな標的に絞って大金を狙う様から、捕鯨にたとえられ、「ホエーリング（Whaling、捕鯨）」とも呼ばれている。

米連邦捜査局（FBI）の発表[8]によると、2013 年 10 月から 2016 年 6 月における BEC による被害総額は約 31 億米ドル（約 3245 億円。2016 年 6 月 17 日のレートで換算）に達している。

また、日本国内でも同様の被害が深刻化している。法人間における海外送金の資金をだまし取ろうとする手口が数多く確認されており、日本経済新聞の報道[9]によれば、全国で少なくとも約 60 社が被害を受け、1 社あたり数百万円から数億円がだましとられている。

2016 年 11 月には、大阪府警天王寺署が取引先のサウジアラビアの商社を装い、貿易会社に商品の見積書を送るよう英文のメールを送信し、不正に見積書の入手を行ったとして、東京都内の貿易会社に勤める男性社員を「不正競争防止法違反（営業秘密の不正取得）」容疑で検挙している。[10]

■報告されている事例

ビジネスメール詐欺では企業の経理担当者を狙い撃ちにするケースが多く報告されている。なりすましメールでは、「最高経営責任者（CEO）」または「最高財務責任者（CFO）」などの役職になりすましたケースが数多く報告[11]されている。

---

[8] BUSINESS E-MAIL COMPROMISE: THE 3.1 BILLION DOLLAR SCAM, 2016/07/14, https://www.ic3.gov/media/2016/160614.aspx

[9] 「企業狙う振り込め詐欺 上司・取引先装い送金指示 被害約 60 社に 警視庁が捜査」日本経済新聞, 2016/07/13

[10] 「「ビジネスメール詐欺」国内外で続発、注意！…狙いは企業情報・マネー 大阪府警が初摘発」産経新聞, 2017/01/31

[11] 『2016 年上半期セキュリティラウンドアップ』トレンドマイクロ株式会社, http://www.trendmicro.co.jp/jp/security-intelligence/sr/sr-2016h1/index.html

ときには組織の存続を脅かすほどの詐欺手口だが、報告されている手口のほとんどは古典的な「ソーシャルエンジニアリング」攻撃によるものである。具体的な手口として次の事例が報告されている。

1. 海外の取引先や海外の関係法人になりすまし、送金指示やメールに添付した請求書に従って海外送金を指示
2. 幹部の名前をかたり、経理担当者に送金を指示
3. 実際の取引メールが盗取され、文面の改ざんを行い本来とは異なる口座へ送金を指示

■BEC に対する対策

これまでと同様のフィッシング詐欺対策が必要になる。それに加えて、正当な処理を標準化し、通常とは異なる対応（例外）を求められた場合にどのような対応をすべきなのかあらかじめ決めておくことが有効である。

- 承認プロセスの標準化
- 承認プロセスの電子化（STP：Straight Through Processing）人手を介すことなく決済処理を行う
- 二経路確認(電子メールとは異なる手段､電話や FAX での事実確認を行う)
- 二重確認

[林　憲明　トレンドマイクロ株式会社]

2.2. クレジットカード情報を狙うフィッシングの増加

フィッシングの目的のひとつに、金銭の詐取がある。2013 年頃から急増し 2016 年前半も活発に行われていたネットバンキングをかたるフィッシングでは、利用者の銀行口座から第三者の口座に勝手に預金が送金される被害が発生している。2016 年 11 月から高頻度で続いている LINE をかたるフィッシングでは、使用中の LINE が乗っ取られ、友だち登録していた人たちに勝手にメッセージが送られる被害が発生している。送られるメッセージは、利用者になりすましてプリペイドカードの購入を依頼するもので、購入したカードの番号を送らせ、電子マネーをだましとろうとする。そしてもうひとつ、色々なブランドになりすましたクレジットカード情報を狙うフィッシングが年間を通じて繰り返し行われ、カードを勝手に使われる被害が発生している。

クレジットカード情報を狙うフィッシングは、早くからカード会社をかたるものが国内で行われており、2010 年から 12 年にかけては、国際ブランドをかたる日本語のフィッシングが多発した。翌 2013 年にカード会社の会員サイトへの登録変更を促すフィッシングが登場し、このタイプが現在に至るまで断続的に繰り返されている。2016 年もまた、複数の会員サイトの会員を標的に、この手口のフィッシングが続いた。

オンラインショッピングをはじめとする、クレジットカードの利用度が高いサービスも狙われることが多い。ネットオークションのアカウント更新を口実にクレジットカード情報を詐取するフィッシングが、2008 年から 2010 年にかけて激化したことは、まだ記憶に新しい。国内の複数の犯行グループが摘発され沈静化したが、それぞれ数百万から数千万の被害を出していたという。

クレジットカード情報を狙うフィッシングでは、このような登録情報の更新や再登録、アカウントのロックを解除するためなどの口実で偽サイトに誘導し、クレジットカード情報などを入力させようとする。2016 年 2 月から毎月頻繁に行われるようになった Amazon をかたるフィッシングもこのタイプで、メールのほかに電話番号あてにメッセージを送る SMS もよく使われた。メールを使った誘導は、2017 年に入ってからも頻繁に続いている。

図 2-1　Amazon のフィッシングサイト[12]

[12] フィッシング対策協議会, Amazon をかたるフィッシング　(2016/11/08), https://www.antiphishing.jp/news/alert/amazon_20161108.html

2016 年 11 月から 2017 年 1 月にかけ、小規模な複数のショッピングサイトの会員あてに、金券配布や特価販売に見せかけたメールを送り、誘導先の偽サイトでクレジットカード情報を入力させようとするフィッシングが相次ぎ行われた。大半のショップが不正アクセスによる会員情報の流出を確認、またはその可能性があると発表しており、小規模店の会員がピンポイントで狙われていることや、誘導先のログインページに各自のログイン ID（会員 ID やメールアドレス）が入力済になるよう細工されていたことなどを照らし合わせると、流出情報を悪用したスピアフィッシングの可能性が高い。

パソコンやスマートフォンのシステムと連携するサービスでも、クレジットカードの利用が進み、これを狙ったフィッシングも増えている。Mac や iPhone を販売する Apple をかたるフィッシングは、日本語を含む多国語に対応した偽サイト構築キットが 2014 年に登場したが、当初日本人を狙う攻撃は見られなかった。翌年になると、アカウント情報を確認するよう促す怪しい日本語のメールが舞い込むようになり、2016 年は同種のフィッシングメールが年間を通じて繰り返し不特定多数あてに送られた。

図 2-2　Apple のフィッシングサイト[13]

[13] フィッシング対策協議会, Apple をかたるフィッシング　(2016/12/01), https://www.antiphishing.jp/news/alert/apple_20161201.html

2016 年 7 月には、Android 端末の利用者を狙う、Google をかたるフィッシングも登場した。誘導にはもっぱら SMS が使われ、公式アプリストア「GooglePlay」の支払方法を登録するよう促すメッセージと、端末からウイルスを確認したので削除するよう促すメッセージが不特定多数あてに送られた。前者はストレートにカード情報などを入力させるフィッシングだが、後者はアンチウイルスソフトの特価販売を口実にカード決済かコンビニ決済を選択させ、必要事項を入力させる。コンビニ払いを悪用し、直接現金を手に入れようとする手口は珍しい。

クレジットカード情報を狙う Apple や Google をかたるフィッシングは、2017 年に入ってからも繰り返されており、2017 年 1 月には、Microsoft をかたるフィッシングも登場している。オフィスソフトのプロダクトキーが違法コピーされた可能性があるので認証するよう促すメールを送り、誘導先の偽サイトで個人情報やクレジットカード情報を入力させようとする。

総務省の「通信利用動向調査」によると、インターネットで購入する際の決済方法は「クレジットカード払い」が約７割と最も多い。特にここ数年の利用者増加は著しく、これを狙うフィッシングは、今後ますます増加するかもしれない。

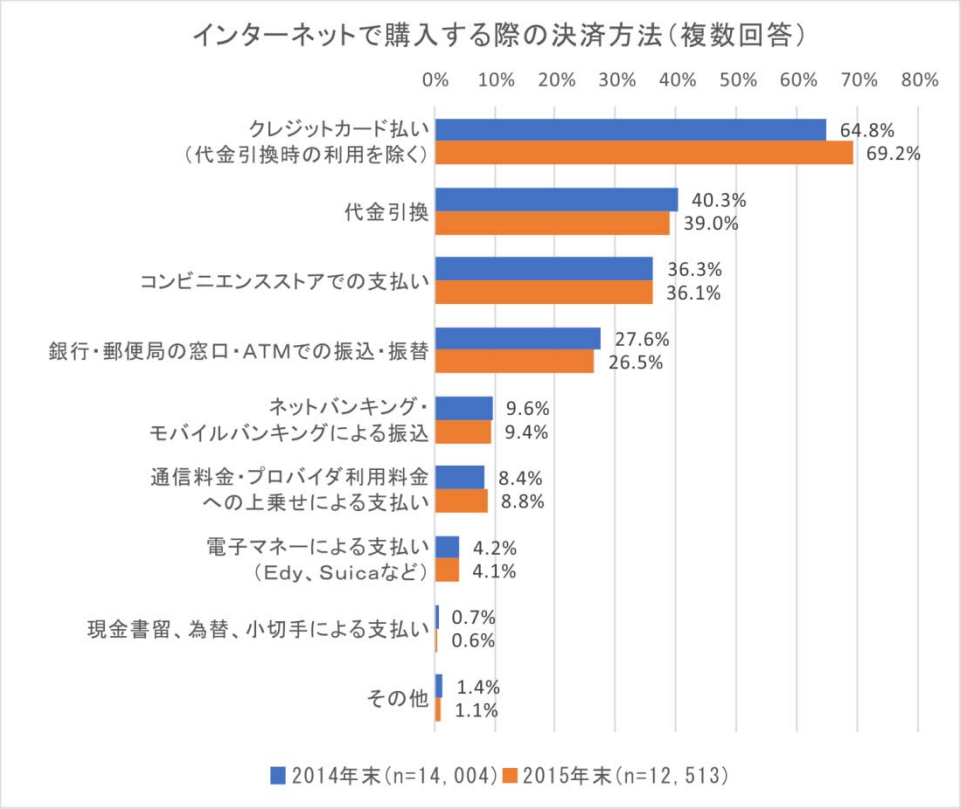


図 2-3　インターネットで購入する際の決済方法[14]

[鈴木　直美　ワークス]

2.3. 国内の大学を狙ったフィッシング動向

ここ数年、日本国内の大学において、フィッシングが発生していることを協議会では確認している。また、海外においては金銭的な被害が発生しているという事例も紹介する。まず初めに日本国内におけるフィッシング事例として、複数の国公立大学や私立大学をかたり、生徒や従業員を狙ったものと思われるフィッシングメールが発見されており、各校からフィッシングに対する注意喚起が行われている。

[14] 総務省「通信利用動向調査」平成 26 年報告書,
http://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html

図 2-4　名古屋大学ホームページ　フィッシングメールの注意喚起[15]

図 2-5　関西学院大学ホームページ　フィッシングメールの注意喚起[16]

[15] 名古屋大学，名古屋大学を装ったフィッシングメールについて(2016/4/26)，
http://www.icts.nagoya-u.ac.jp/ja/information/security/2016-04-26-fishingmail.html
[16] 関西学院大学，フィッシングサイトへのアクセスによる個人情報漏えいについて(2016/10/7)
http://www.kwansei.ac.jp/notice/2016/notice_20161007_013525.html

フィッシングの手法については、いくつか共通点がある。

1. 大学の管理者をかたり、フィッシングメールを多数のユーザへ送信する。
2. 各校が実際に使用しているサービスなどをかたりフィッシングサイトに誘導する。
3. フィッシングメールの内容はメールサーバの容量オーバーなどをかたるものが多く、誘導したフィッシングサイトにて ID とパスワードを詐取する。

ただし、日本国内の大学において金銭的な被害が出たという報告は確認できていない。なお海外の大学においては、金銭詐取を目的としたフィッシングが発生している。2016 年 9 月に米国のミシシッピ大学では、銀行口座やクレジットカード番号、Apple ID とパスワードを不正に詐取しようとするフィッシングメールが学内のメールアドレスに送信されたことに関して注意喚起を行っており[17]、報道によるとルイジアナ州ニューオーリンズのトゥレーン大学では、2016 年 10 月に大学職員がフィッシングの被害にあい、攻撃者は詐取した ID とパスワードを使用し、大学職員の給与振込先を変更、結果として 200 万円の被害がでたと発表されている[18]。

大学においては、研究などにおける最先端技術情報や、貴重な情報資産が保管されているので、フィッシングや標的型攻撃といったサイバー攻撃の対象となる。その結果サイバー攻撃により、貴重な情報が外部に流出するといった被害が発生するため、学生および教職員に対する啓発活動を日々行っていただく必要がある。

[JPCERT コーディネーションセンター]

[17] http://thedmonline.com/phishing-scams-rise-nationally-campus/
[18] http://www.nola.com/crime/index.ssf/2016/10/tulane_employees_hit_by_phishi.html

3. 新しい攻撃手法・対策の動向

3.1. ユーザ認証のシステムに関する新しい動向

3.1.1. はじめに

パスワード認証に代表されるユーザ認証の仕組みは、インターネットを使ったオンラインのサービスにおいてその設計や運用が見直されつつある。インターネットが使われるようになると、他社を含む複数のサービスが同じ端末で使われることが日常的に起こる。するとユーザの端末やネットワーク機器、それらで動作しているプログラム、そして登録手順や登録後のユーザ認証方式に至るまで、さまざまな要素が絡んでくる。ハードウエアやソフトウエアの種類を限定しやすいシステムに比べると、認証システムへの攻撃をやりやすい一面もある。オープンな仕様のプログラムが使われていることに加えて、国際的に攻撃手法を研究している技術者は数多くいる。

このような状況変化の中では、自社や、国内に閉じた技術やノウハウでシステムを設計すると大きな二つの落とし穴に陥る恐れがある。一つは国際的に普及しているプラットフォーム（ハードウエアやソフトウエアなど）への追従が後手になってしまいかねないことである。例えばスマートフォンへの対応が遅れていると、ユーザ環境を最大限に活かしたサービスを提供することが難しい上に、脆弱性を持ちやすい古いプラットフォームを使わざるを得ない事にもなる。もう一つは暗号やハッシュのアルゴリズムやセキュアな通信のためのプロトコルにおいて、国際的には既知の脆弱性を持つ可能性がある。

そこで、国際的に専門家の目にさらされる形で検討されているような仕様や方式にいち早く目を向けることをお勧めしたい。それによってさまざまな攻撃に対して堅牢なシステムを構築しやすくなるというだけでなく、認証システムがどういった概念や要素で成り立っていて、攻撃対象となりうる要素には何があるのか、といった共通理解の基盤になりうるという意味もある。この事は国内における検討と情報交換の上でも、とても重要である。

本節では米国国立標準技術研究所（NIST）が策定しているガイドライン SP 800-63 を紹介したい。

3.1.2. SP 800-63 とは

NIST の情報技術研究所（ITL）では、米国政府のコンピューターシステムに

おけるセキュリティのための技術開発やガイドラインの策定が行われている。活動成果をまとめる位置づけであるスペシャル・パブリケーション（SP）と呼ばれるレポートの一つである SP 800-63[19]では、電子認証に関するガイドラインがまとめられている。

SP 800-63 は、インターネットなどのリモートの認証をテーマとしたもので、初版は 2004 年に出され、2016 年に大きな改訂作業が行われている。改訂作業にあたって GitHub を使ってオープンな場でコメントの募集が行われているという、オープンな策定プロセスとなっている。また専門的な内容でありながらその一部は日本でも話題となった。日本では OpenID ファウンデーション・ジャパンの有志によって日本語版が作られつつある[20]。2017 年 1 月 30 日から 3 月 31 日までがパブリックコメントを受け付ける期間となっている。そのため内容は今後変わっていく可能性がある。

3.1.3. SP 800-63 の読み方

SP 800-63 は元来米国政府の情報システムを念頭にして書かれたものである。つまり米国政府の情報システムの調達に関わらなければ要件とは無関係であると言える。しかし認証システムについて網羅的に書かれており、日本におけるシステム構築・維持・改善にあたって参考とするに有益な文書である。以降、SP 800-63 の内容を紹介していく。

SP 800-63 は、全体概要をまとめた SP 800-63-3、ユーザの本人性の確認や登録についてまとめた SP 800-63A、登録されたユーザを認証する段階についてまとめた SP 800-63B、ユーザ認証のシステム間連携、認証連携についてまとめた SP 800-63C に分かれている。各々が認証システムに関する概念に基づいて書かれているため、はじめにその概念を押さえておきたい。また用語も多用されており、固有の概念であり和訳が一般的になっていない言葉も含まれている。

表 3-1　各文書の内容

SP 800-63-3	認証の全体概要・認証の考え方・保証レベルの選び方
SP 800-63A	ユーザの本人性確認や登録時の要件について

[19] Draft NIST SP 800-63-3, https://pages.nist.gov/800-63-3/
[20] OpenID ファウンデーション・ジャパンの有志による日本語訳, NIST SP 800-63-3 Digital Authentication Guideline, https://openid-foundation-japan.github.io/800-63-3/

SP 800-63B	リモートのユーザを認証する段階の考え方と管理方法
SP 800-63C	フェデレーションと認証結果の伝搬

ここで SP 800-63 の中で一貫して使われている概念を紹介したい。簡潔に表現するならばユーザの状態である。認証システムへ登録される前の人はアプリカント（Applicant）と呼ばれている。身分証明書などを使って本人性の確認がなされ、登録手続きに成功するとその人はサブスクライバー（Subscriber）と呼ばれる。サブスクライバーはパスワードなどの認証に使われる情報ないし IC カードなどの認証に使われるものである、オーセンティケーター（Authenticator）を所持し、場合によっては複数を使って（多要素認証）ユーザ認証手続きに入る。全体的な概念は SP 800-63-3 Figure4-1 に図示されているが、この流れについては SP 800-63-3 の 4 章で書かれている手順の記述がわかりやすい。

これらの用語は、SP 800-63-3 3 章、SP 800-63A 3 章、SP 800-63B 3 章、SP 800-63C 3 章で定義されている。IC カードなどの認証に使われるものを発行する「クレデンシャル・サービス・プロバイダー（CSP）」やオンラインなどでユーザ認証を行った後にアプリケーション上の処理を行う「リライングパーティー（RP）」といった用語は SP 800 の中で多用されている。他にも用語が多いため、改めて SP 800-63 における定義を確認することをお勧めしたい。

3.1.4. 保証レベル

SP 800-63 では、保証レベル（Assurance Level）と呼ばれる概念も導入されている。これはユーザの本人性確認の程度やオンラインなどでユーザ認証を行う際の方策の度合いを示している。本人性確認の程度の方はアイデンティティ保証レベル（IAL）と呼ばれる。

IAL1 は身分証明書などを必須とせず、基本的に申告に基づいたものと見なされるレベルである。IAL2 は現実社会に存在することが、リモートまたは対面で確認されることを必須としている。そして IAL3 は対面での確認を必須とされる。これらの定義については SP 800-63A の 2.2 節が分かりやすい。国内でも、オンラインでアカウントを作ることのできるサービスがあったり、窓口で身分証明書を提示してはじめて登録できるサービスがあったりする。国内のサービスが必ずしもレベル 1 から 3 に当てはまるかどうかはわからないため検証を要するが、一種の指標として捉えることはできる。

ユーザ認証を行う際の方策の度合いの方は、オーセンティケーター保証レベル（AAL）と呼ばれる。パスワードのような記憶に頼る情報を使うのか、ワンタイムパスワード（OTP）を使うのか、もしくは認証機能のついた IC カードを使うのか、といった技術的な違いに加えて、これらを複数使うことで不正への対策を強化する「多要素認証」もレベルの違いとして現れる。AAL について詳しく述べられている SP 800-63B 4 章には、レベルごとの要件だけでなくノウハウともとれる情報も載せられている。例えば、一度認証に通ったユーザに対してパスワードを再度要求するタイミングはどのように設計すればいいのか、といった点である。

なお IAL と AAL を別々に設定できるのには意味がある。ユーザの登録を多くの書類に基づいて行う必要のあるサービスでも、オンラインの認証は簡単でいい場合が考えられる。つまり異なる保証レベルを組み合わせてサービスを構成することができる。自社のシステムを照らし合わせて予めレベルを想定した上で、各章の部分を読んでいくと分かりやすい。

すでにあるサービスについて、保証レベルはどのように選んでいけばいいのだろうか。その方法は SP 800-63-3 の 5 章が詳しい。Figure 5-1 - Selecting AAL と Figure 5-2 - Selecting IAL には、「個人情報を扱うか yes/no」といった選択肢や経済的な損失が想定されるかどうかといった指標が示されている。

3.1.5. 各文書の目次

本節では、各文書の目次を簡単に紹介する。下記は筆者の私訳であり、OpenID ファウンデーションジャパン有志による日本語訳とも若干違う部分があるが、原文で使われている用語に、広く普及している和訳がない点を踏まえて、ご容赦いただきたい。

SP 800-63-3 認証の全体概要・認証の考え方・保証レベルの選び方

1. 本書の目的
2. はじめに
3. 用語と略語
4. 認証のモデル
5. 保証レベルに関する新しいアプローチ
6. 参照

SP 800-63A ユーザの本人性確認や登録時の要件について
1. 本書の目的
2. はじめに
3. 用語と略語
4. アイデンティティ・保証レベルにおける要件
5. アイデンティティの特定・検査と検証
6. 先行する確認処理の作用について
7. 脅威とセキュリティに関する考察
8. プライバシーに関する考察
9. ユーザビリティに関する考察
10. 参照

SP 800-63B リモートのユーザを認証する段階の考え方と管理方法
1. 本書の目的
2. はじめに
3. 用語と略語
4. オーセンティケーター（Authenticator）・保証レベル
5. オーセンティケーターとベリファイアー（Verifier）の要件
6. オーセンティケーターのライフサイクルの要件
7. セッション管理
8. 脅威とセキュリティに関する考察
9. プライバシーに関する考察
10. ユーザビリティに関する参考資料
11. 参照
付録 A. 記憶シークレットの強度

SP 800-63C 認証連携と認証結果の伝搬
1. 本書の目的
2. はじめに
3. 用語と略語
4. フェデレーション
5. アサーションの強度
6. アサーションの表現形式
7. アサーション・保証レベル
8. セキュリティ

9. プライバシー要件と考察
10. ユーザビリティ
11. アサーションの例
12. 参照

3.1.6. 位置づけについて

SP 800-63 は、本節の最初に述べたとおり、あくまで参考情報に留まると言える。しかしユーザ認証における不正行為を未然に防止し、トラブルを避けることができるのは、網羅的に検討し設計された仕組みであり運用である。構成要素の位置付けや各業務の元来の意図に関する理解があれば、国内の詳細な議論に左右されることなく対処しやすいと考えられる。本節がその一助になれば幸いである。

[木村　泰司　一般社団法人 日本ネットワークインフォメーションセンター]

3.2. ID フェデレーション

ID を必要とするサービスが増えていく中で、サイト利用者は、ID、パスワードの使い回しを行い、一方で、その ID、パスワードを管理するサイト側は安全管理の義務を怠っている。このような状況により、安全管理を怠っている脆弱なサイトから ID、パスワードが漏れることにより、きちんとした管理を行っている利用者にとって重要なサイトが大きな被害を受ける事件が増えている。

3.2.1. 利用者および事業者の ID、パスワードの管理実態

2015 年のディーディーエス PR 事務局のパスワードに関する実態調査[21] の結果によれば、サイトなどに関するログインする際の ID、パスワードの一人あたりが管理している数は、平均 6 個以上となっている。そのため、多くの人が異なるサイトで、同じ ID やパスワードを使いまわす傾向が、約 80%もの人に見受けられる。

一方で、総務省が 2015 年 7 月 30 日に公開した「Web サービスに関する ID・パスワードの管理・運用実態調査結果[22]」によれば、事業者の約半数は、パスワードのハッシュ化を実施しておらず、さらに 14%はパスワードの保管時の暗号化さえ実施していない。正しく、ハッシュ・暗号化を実施している 43%のサイトにおいても、ソルトおよびストレッチを実施しているサイトは、19%しか存

[21] https://prtimes.jp/main/html/rd/p/000000006.000010113.html
[22] http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000099.html

在しない。一部のサイトでは、それほど重要な情報をユーザから預かっていないとして、管理を怠っている可能性もあるが、サイト利用者の ID の管理の傾向を考えると ID、パスワードの重要性は、そのサイトの内容とは関係なく個人情報として重要な管理が求められるものである。

3.2.2. ID フェデレーション（ID 連携）とは

ID フェデレーションとは、ユーザの ID 情報（認証結果および属性情報）をサイト間で交換するサービスのことである。これまで各サイト管理者が個別に発行・管理していた ID 情報を利用者の許諾を得て事業者間で連携させる仕組みである。ID 情報を外部に提供するサービスをアイデンティティプロバイダ（IdP）、IdP から ID 情報を受け取る側のサービスをリライングパーティ（RP）と呼ぶ。RP は、ID とパスワードによるユーザの認証は、IdP にゆだねることができるので、ID とパスワードを自サイトに保持する必要がない。よって認証情報の安全管理や問い合わせにかけるコストを削減することができ、ユーザは、そのサイトの認証情報を記憶する必要がなくなる。サイト運営者および利用者双方にとってメリットのあるサービスとなっており、多くのサイトで利用が進んでいる。

近年、Google、Yahoo、Microsoft など総合ネットサービスおよび Facebook、twitter、Linkedin などソーシャルネットワークサービス、楽天、Amazon などのオンラインショッピングサイト、KDDI の au ID、Docomo の d アカウントなどの携帯事業者など多くのネットサービス企業が ID 連携を提供している。さらにスマートフォンなどによる多要素認証を提供して、さらに安全な認証情報の管理を提供している事業者も増えている。

3.2.3. まとめ

サイト運営事業者は、ID をサイト利用者に発行する際、ID の発行の必要性をよく考え、発行が必要であるのであれば、その管理を安全にする義務があることを認識し、容易な ID の発行は慎むべきである。利用者への容易な ID の発行を避け、できるだけ ID 連携を使うことが推奨される。その際、ユーザの選択の為、複数の ID 連携提供事業者を選択できるようにするのが望ましい。また、利用者は、容易に ID を作成するのではなく、ID 連携が利用できるのであれば、そちらを選択するのが望ましい。

ID 連携の普及により、利用者が管理する ID が少しでも少なくなり、また、IdP は多要素認証など安全な認証情報のサービスを提供し、フィッシングの被害

が減ることを期待したい。

[野々下　幸治　トレンドマイクロ株式会社]

3.3. 他業界における参考となる取り組み

3.3.1. ゲーム業界における不正アプリへの取り組み

ゲーム業界においては、不正アプリによるサービス利用の被害が大きな問題となっている。不正アプリはチートツールと呼ばれ、これらチートツールを利用しゲームの利用レベルを簡単にアップさせたり、有料アイテムを不正に得ることをチート行為という。

「日本オンラインゲーム協会」によると、チート行為は 2004 年ごろ存在が確認され、2006 年ごろからはチートツールを販売する事業者も現れたという。

不正利用者は、チートツールにより有料アイテムを支払いせずに入手したり、実際にはクリアしていないゲームステージをクリアしたことにするなどの不正を行うが、これらの行為により、ゲームサービス事業者は、課金アイテムによる収入の被害を受け、通常利用者と不正利用者との格差が生まれることでゲームバランスが崩れ、ゲームの価値が下がるなどの被害が出ている。

これらの不正行為は、もちろん犯罪でありチート行為を行った者、チートツールを作成、販売した者は、私電磁的記録不正作出・同供用、電子計算機損壊等業務妨害、著作権法違反（公衆送信）、組織犯罪処罰法違反（組織的偽計業務妨害）などで逮捕されている。

2016 年は、多数の逮捕者がでているが、これらは氷山の一角であると考えられ、被害は甚大であるとゲーム業界は見ている。

その背景にはスマートフォンの普及があり、それとともにゲーム業界は拡大している一方、チート行為による損害の影響も大きくなり、多くのゲーム事業者で対策の必要性を認めている。

チートツールによる不正は、データ改ざん、課金回避、通信のパケットの変更などで行われるが、これらへの対策として、アプリプログラムの不正な解析や改ざんを防止するクラッキング対策ソフトウエアが開発されている。ゲーム事業者は、独自による防止策のほか、このような対策ツールを利用しチート行為対策を行っている。また、iPhone にてチートツールを利用するためには、iOS を改造した脱獄端末（ジェイルブレイク端末）である必要がある。これらからの不正を防ぐために脱獄端末での利用を制限し対策とした例もある。

もう一つの対策として、利用者への呼びかけも行われている。チート行為が犯罪であることを認知していない利用者への呼びかけをゲームアプリ上で目立つように表示するなどしている。

2016 年には、スマートフォンでの歩きながらの利用が、大きな社会問題として取り上げられるほど注目されたゲームサービスがリリースされた。このサービスを利用するためのアプリについては、チートツールも数多く存在しているが、通常のチート行為と違い、ID やパスワード、クレジット番号をフィッシングする目的で作成された不正偽アプリも多く確認されている。

チートツールとは目的が違う不正アプリではあるが、ゲーム業界としては、偽アプリへの対策も必要な状況である。

このようなアプリの解析や改造を行い、インターネット上のサービスを不正利用する犯罪や、偽アプリによる個人情報のフィッシングは、ゲーム業界に限ったことではない。IoT 時代の到来により多くのデバイスがインターネットに繋がることで、多くの業界で対策を実施する必要がでてくると思われる。

[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]

3.3.2. 事業者サイトも常時 SSL 化のながれに

Web サイトの信用度を高める手法として、全世界的に SSL 化がすすんでいるが、日本は他国に比べ進んでいない。2014 年 8 月、「Google Web マスター向け公式ブログ」において常時 SSL 化しているサイトの評価を優遇することを正式発表[23]した。常時 SSL 化をすることにより、検索順位が大きく上がることはないが、HTTP サイトより HTTPS サイトのほうが優遇される。

表 3-2　Google による常時 SSL 化にむけた推奨

1	必要な証明書タイプを決定:シングル、マルチ ドメイン、ワイルド カード
2	2048 bit の証明書を使用します
3	同じ安全なドメイン上にあるリソースには相対 URL を使用します
4	他のすべてのドメインにはプロトコル相対 URL を使用します
5	robots.txt を使用して HTTPS サイトへのクロールをブロックしないでください
6	可能な限り検索エンジンがページをインデックス登録できるようにします。Noindex メタタグの使用は避けます。

※その他詳細は Google サポートページを参照[24]

[23] https://webmaster-ja.googleblog.com/2014/08/https-as-ranking-signal.html
[24] https://support.google.com/webmasters/answer/6073543

続いて、2016 年 8 月に「Google SecurityBlog[25]」において Google Chrome を利用しているユーザに対し常時 SSL を施していないサイトに関しては、アドレスバーに「Not Secure」と表示されるアルゴリズムを適応することを計画していると発表、その一環として 2017 年 1 月に発表されたブラウザ「Chrome56（バージョン 56.0.2924.76）」の日本語版ではパスワードやクレジットカード番号を収集するページが HTTPS で保護されていない場合、「保護されていません」と表示される仕様となった。GoogleChrome のブラウザーシェアは高く、事業者側では対策が急がれる。

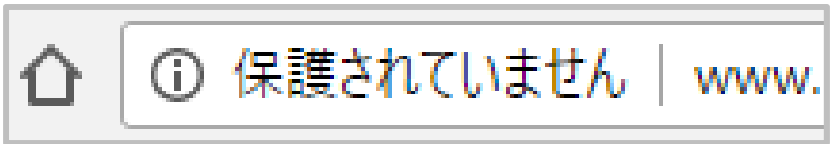


図 3-1　Google Chrome 表示画面

Google の仕様変更や、フィッシング被害が世界的に広がってきていることもあり、対策は世界中で進んでいるが、国別にみる主要企業サイトの対応状況を見ると米国・ヨーロッパを中心に常時 SSL 化は進んでいるが、日本の主要企業サイトでは 2016 年 5 月時点で 2%しか対応していない。

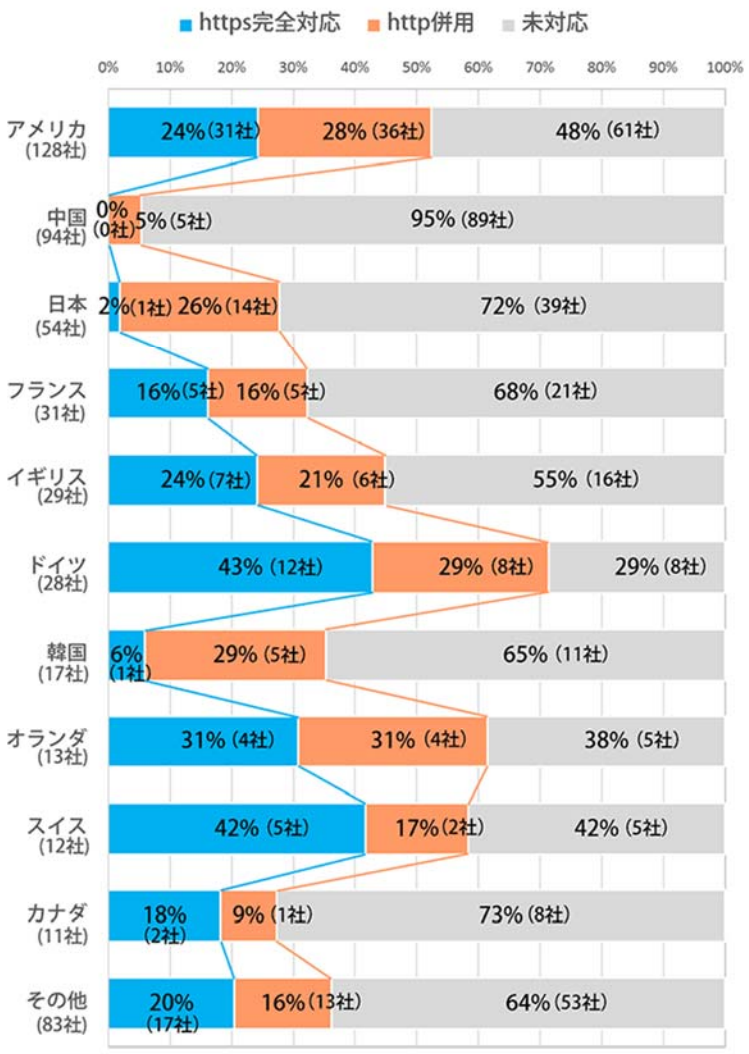


図 3-2 世界主要企業サイトの国別　常時 SSL 対応状況（対象企業が 10 社以上ある国）[25]

今後 Google の常時 SSL 対応サイトへの優遇は進んでいくことも想定され、「Web サイト運営会社名」「認証局」が記載される EV SSL 証明書を導入するなど、ユーザに対してのフィッシングサイトへの注意喚起も含め対応していく必要がある。

[池田　良介　BB ソフトサービス株式会社]

[25] 世界主要企業サイト/国内主要企業サイト，常時 SSL 対応調査 2016 年 5 月版，http://at21.jp/web/topic/topic24.html

3.4. ソーシャルエンジニアリング

ソーシャルエンジニアリングの定義は明確に定まっていないが、以下のように考えている。

人間の心理的な弱さを利用したり、他人になりすましたりして、必要な情報を盗み見したり、盗取するもので、いくつかの方法を組み合わせたり、複数の人から情報収集を行うこともある。

ここでは、そのいくつかの事例を紹介する。

3.4.1. スマートフォンにおけるショルダーハッキングの危険性

最近、多くの人がスマートフォンを利用するようになり、インターネットショッピングなどをはじめ、パスワード入力を求められるアプリケーションを利用することがある。

通常、パソコンを利用したパスワード入力では、入力した文字は、画面上に「*」が表示され、入力文字が表示されることはない。

しかしながら、スマートフォンの場合、図 3-3 に示すように入力された文字が画面に表示され、その後「●」に変わる。図 3-3 は、最初の文字は既に「●」で表示されているが、２番目の入力文字は「a」が表示されている。

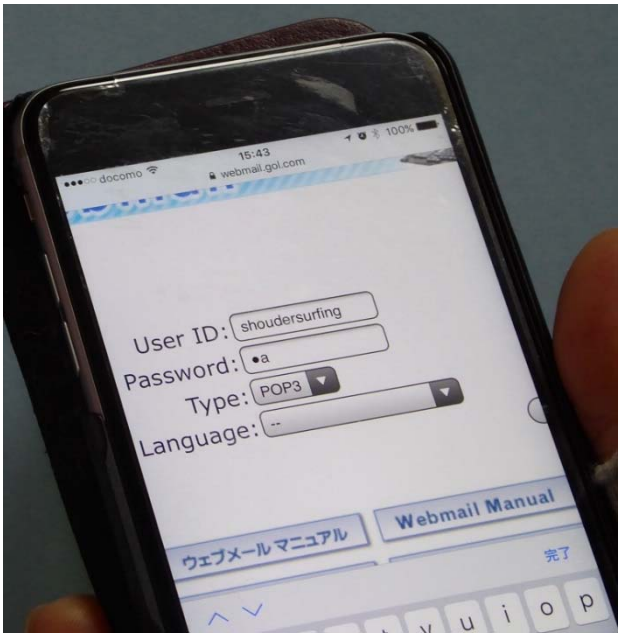


図 3-3　パスワード入力画面

最近のコンパクトカメラでも高倍率の望遠機能を持ち、4K 動画を撮影できる。図 3-3 は、4K 相当の静止画で、十分画面の文字を識別できる。

パソコンでも、スマートフォンでも、ショルダーハッキングを行えば、入力した文字をキーボードから判断できると言われているが、30 名程度の社会人中心の研究会で、ショルダーハッキングの実験を行い、文字認識ができるかを確認したが、識別できる参加者はいなかった。

スマートフォンのパスワード入力をデジタルカメラの動画を利用すれば、ユーザ ID とパスワードを盗撮できる。多少、離れていても、高倍率のズーム機能があり、盗撮されていることも分からない可能性がある。

現在のスマートフォンの機能は、当初のパソコンより遙かに高機能化しており、多くのアプリケーションを利用できる。このため、パスワードの重要性が高くなってきている。時代の変化はリスクの変化でもあることを理解して、現在の方法はリスクが高いことをスマートフォンメーカーや通信会社が気づき今後対応することを期待する。

3.4.2. タブレット利用による ID 窃盗～佐賀県学校教育ネットワーク事件から～

2016 年 6 月に公表された「佐賀県学校教育ネットワーク事件[26]」は、無職の少年と高等学校の生徒による情報漏えい事件である。
軽量のノートパソコンやタブレットの利用が一般的になってきたが、この事件はこれらの機器を利用して「ID 窃盗[27]」が行われた。

無職の少年および生徒は学習用 PC の「管理者権限」を持つ教員のユーザ ID とパスワードを盗取するため、生徒が使っているパソコンを利用して、ユーザ ID とパスワードを盗取するための画面を作成し、教員にそのパソコンを操作させ、管理者権限のユーザ ID とパスワードを盗取した。
高等学校教育現場での「ID 窃盗」だが、タブレット利用のパソコン内で完結する仕組みであった。ただこういったことは、特に学校現場に限らず、どの様な組織でも発生する可能性がある。

例えば、ある社員が自分のパソコンが動かなくなったと言って、同僚などに操作させ、同僚のユーザ ID とパスワードを盗取できれば、同僚になりすますことができる。最近のパソコンやタブレットの利用で、ユーザ ID とパスワードだけで認証を行う場合は、十分な注意が必要であろう。このようなことを防ぐた

[26]佐賀県, 学校教育ネットワークに係る不正アクセス被害がありました(2016/6/27), http://www.pref.saga.lg.jp/kyouiku/kiji00348361/index.html
[27]佐賀県学校教育ネットワークセキュリティ対策検討委員会から提言がなされました(2016/10/27), http://www.pref.saga.lg.jp/kyouiku/kiji00351508/index.html

めには、同僚は自分のユーザ ID とパスワードを利用せず、本人のユーザ ID とパスワードを利用する、あるいは、システム担当などに連絡をして対応する必要がある。

パソコンやタブレットの利用では、生体認証を利用しているとの反論もあるが、生体認証利用を利用して認証を拒否された場合には、どの様な対応をしているのだろうか、ピン番号を入力していないだろうかなど、適切な対応を考えることが大切になるであろう。

3.4.3. 生体認証の拒否リスクを考える

最近は、多くの生体認証が実用化され、多方面で利用されているが、それらを採用する場合には、生体認証システムの課題を考えておく必要がある。

(a) 登録未対応率

生体認証が人間の持つ指、手、顔などを利用するため、生体認証システムがそれらを受け入れてくれない人がいる。これを「登録未対応率（FTER： Failure To Enroll）」と呼んでいる。

指紋では、数百人に一人の割合で発生し、指静脈認証でも 10,000 人に数人と言われている。

一般的な組織の場合、導入時に誰も未対応にならなくても、新規の利用者があれば、その利用者が登録未対応になる可能性がある。

(b) 本人拒否率

生体認証システムに自分の生体を登録できても、実際に利用する場合に、システムが拒否することがある。繰り返し行うことにより、認証されることがあるが、認証できなかった場合、システムでは代替手段を設けざるを得ない。

(c) 攻撃者の思考

登録未対応の利用者に対して、システム管理者は何を考える傾向があるか。パソコンであれば、ユーザ ID とパスワードの入力を求める、あるいは、スマートフォンであれば、ピン番号を入力する方法が考えられる。

攻撃者は、生体認証システムとユーザ ID／パスワードかピン番号のいずれかの攻撃を考えるであろう。指紋認証であれば、偽造指紋を作ることが簡単かも知れない。

偽造の難しい生体認証システムであれば、パスワード／ピン番号を考える可能性がある。１つの生体認証システムでは、本人拒否が発生した場合、パスワ

ード／ピン番号を入力させる仕組みであれば、本人拒否を意識的に行えば、パスワード／ピン番号入力になる。

(d)　攻撃されないために

生体認証システムの導入の場合、複数の生体認証システムを導入しているケースもある。これにより、１つの生体認証システムで、登録未対応や本人拒否が発生しても、他の生体認証システムを利用することにより、脆弱性を小さくする工夫もある。

１つの生体認証システムでは、登録未対応や本人拒否が発生すれば、パスワード／ピン番号を入力することになり、生体認証の導入がセキュリティ対策としては意味のないものになる。

生体認証とユーザ ID などとの根本的な相違は、「アナログ的認証」と「デジタル認証」の違いだと説明することがある。厳密には、生体認証もデジタル方式であるが、選択する位置が異なると、本人拒否になることがあるという点で「アナログ的認証」と考えている。ユーザ ID などは、ゼロ・イチで判断するので、「正しい」か「エラー」かが明確である。この点の相違を考慮する必要がある。

生体認証も利用の仕方で、非常に便利であるが、使い方を誤らないで欲しいと考えている。

世の中に、完全なものなどないのだから・・・

[内田　勝也　情報セキュリティ大学院大学]

■コラム：ドメイン名のトラブルに巻き込まれないために

2016 年、ドメイン名をめぐるトラブルとして、地方公共団体をかたった偽の観光サイトが確認され話題となった。

悪用されたドメイン名は、元々当該地方公共団体が登録し、観光サイトに使用していたが、LG.JP ドメイン名に移行するのに伴って廃止したものであった。

期限切れのドメイン名を再登録して別の用途に転用する事例はこれまでにもあったが、この事例では本物をかたった偽サイトが作られたことが特徴的であった。偽サイトはオンラインカジノサイトへの誘導に悪用されており、地方公共団体が公式サイトで注意を呼び掛ける事態となった。

登録者が自主的に廃止する以外にも、ドメイン名は登録の更新を行わない

場合、一定期間を置いた後に廃止され、別の希望者が登録できる状態になる。更新手続きを忘れていた場合など、意図せず期限切れとなることもあるため注意しておきたい。

意図せず廃止となったドメイン名を元の登録者が運良く再登録できることもあるが、これまでに Web サイトなどで利用されていたドメイン名は、SEO の観点でメリットがある場合もあるため、廃止のタイミングを狙って第三者が再登録する「ドロップキャッチ」が行われることもある。

そのため、地方公共団体に限らず、一度利用を開始したドメイン名は安易に変更・廃止しないということが大切である。やむを得ず変更・廃止することを考える際にも、その影響を考え、しばらく登録を維持しておくのが望ましい。

なお、ドメイン名の種類によってはその登録・使用に関して生じた紛争を、裁判よりも費用を抑え、なおかつ短い時間で処理するための規則として、ドメイン名紛争処理方針（Domain Name Dispute Resolution Policy：DRP）が用意されている場合がある。「.com」や「.net」などの gTLD（generic TLD）では UDRP（Uniform Domain Name Dispute Resolution Policy）が、JP ドメイン名では JP-DRP が制定されている。

DRP によって、不正な行為に対しては、そのドメイン名の取り消しや移転を要求でき、紛争処理機関による裁定というルール化された形の中で解決できるようになっている。しかし、DRP でドメイン名に関するあらゆるトラブルを解決できるわけではないため、やはりドメイン名の登録者や登録検討者がトラブルに巻き込まれないように注意することが重要である。

[宇井　隆晴　株式会社日本レジストリサービス]

■コラム：犯罪者目線でのフィッシングスキームとテクニック内容

2016 年はフィッシングサイトの検知数がグローバルで増加した。APWG（Anti Phishing Working Group）の統計情報[28]によれば、2016 年は APWG が 2004 年に観測を始めて以来、最も高い数値である 1,220,523 サイトを記録した。これは前年比で 65%増である。2004 年が月平均で 1,609 サイトが検知されていたことを考えると、2016 年は実に約 58 倍のフィッシングサ

[28] Phishing Activity Trends Report 4th Quarter 2016, http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

イトが世の中に立っていることになる。
　ここまでフィッシングサイトが増えた理由は複数あるが、大きく二つがあげられるだろう。一つは、被害者が後を絶たないこと、そしてもう一つはフィッシングサイトが大量生産できるようになったことと考えられる。

　前者は、被害者が思わずクリックしてしまうようなスキームが世界的に確立しており、例えば税還付が行われるというパターンや、ディスカウントが受けられるというパターン、あるいは男性諸君が注意すべき色仕掛けのパターンなど、人の心につけ込んだ手口が山ほどある。税還付の例で言えば、さまざまな国の国税当局（あるいはそれに相当する機関)を装った偽の還付金通知を送りつけるものである。フィッシングサイトのリンクをクリックすると、国税当局とそっくりのサイトに、その国すべての銀行の一覧が表示され、訪問者は自身が口座を保有する銀行を選んで、還付を受け取るための個人情報を入力する仕組みになっている。被害者が持っている口座の情報が一度に手に入れられるよう工夫された手口は、フィッシング犯から好まれる傾向にある。

　後者では、ターゲット被害者ごとに専用のフィッシングページを"自動で"生成するタイプのフィッシングキットの存在が確認されている。つまり、同一犯罪者から、あなたとわたしに送られるフィッシングサイト URI は異なるのである。そのリンクをクリックして、ターゲットにより必要な情報が入力されたら、個人情報が即座に犯罪者の元に送られ、ほぼ同時に証拠隠滅のため個人情報の入っていたフォルダは削除されるのである。また、このフィッシングサイトページ自体も数分後には証拠隠滅のため削除される。

　この動作は、セキュリティ担当者に、フィッシングサイトが閉鎖されたと誤認させる可能性が高く、実際にはフィッシングサイトはターゲットごとに異なって乱立して、個人情報が次々と盗まれても、気がつきにくいという犯罪者にとってのメリットがある。アンダーグラウンドの世界では、「ランダム・フォルダ・ジェネレータ」を使ったスキームと呼ばれており、このスキームに対処するためには、フィッシングページごとの削除ではなく、おおもとのフィッシングサイトとランダム生成のためのリソースを含むベースディレクトリを検知した上で閉鎖する必要があるという非常にやっかいなものである。

　また、犯罪者に対して、盗んだ情報の有効性が確認できるサイトの存在が

わかっている。例えば、クレジットカードの有効性や銀行口座の有効性を調べられるサイトが存在する。どちらも FaaS （Fraud As A Service） と呼ばれるサービスで提供がされており、最近発見されたサービスサイトでは、複数の盗んだリストの有効性をまとめてチェックできる機能が付いており、犯罪者にもよく使われているという。昨今のオンラインバンキングや決裁のためのログインは、複数の認証や CAPTCHA などを介した複雑なものもあるが、これらのサービスサイトにはそれらを認識するモジュールが開発されており、ことごとく破られているようである。

　このような犯罪者目線でのサービスが充実することにより、高いフィッシング詐欺の技術を持たなくとも犯罪を実行できることが、昨今のフィッシングサイトの急増に繋がっていることが容易に想像できる。

[水村　明博　EMC ジャパン株式会社]

4. まとめ

年々増加していたインターネットバンキングの被害額は、金融庁の調査によると、2016 年 7 ～ 9 月、約 1 億 7 千万円で前年同期と比べ 8 割減少し、被害件数も 113 件で同 7 割減となった。これは金融機関におけるワンタイムパスワード導入など、フィッシング対策が定着し始めたことが背景にある。

地道ではあるものの対策をすれば効果が得られることを実感した１年であったとも言えるであろう。

一方で、年末には金融機関以外の Amazon、マイクロソフト、LINE、Apple などをかたるフィッシングが続けざまに発生し、アカウント情報 （E メールアドレス・パスワード）に加え、クレジットカード情報も詐取する攻撃が続いており、

これら対策の導入を着実に根付かせていくことと、対策の利用者を拡大する取り組みが必要である。

また、正規証明書を使ったフィッシングメールやサイト、高度化するマルウエアなど手口の巧妙化も進んでいる。

各事業者は、これら基本的な対策の着実な促進と、常日頃の情報収集による最新動向の把握とその対策の自社展開の検討を両輪として取り組むことが重要になってきている。利用者の各対策の積極的な利用も重要である。

本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ことで利用者・事業者を支援していくことがますます必要である。

[加藤　孝浩　トッパン・フォームズ株式会社]

[早川　和実　NTT コミュニケーションズ株式会社]

（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
早川 和実	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
山本 和輝	BB ソフトサービス株式会社
池田 良介	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
宇井 隆晴	株式会社日本レジストリサービス
木村 泰司	一般社団法人日本ネットワークインフォメーションセンター
鈴木 直美	ワークス
武藤 蔵	一般社団法人全国銀行協会
貞広 憲一	株式会社みずほ銀行
中山 広樹	株式会社三井住友銀行
川名 健太	株式会社三井住友銀行
鈴木 智之	株式会社三菱東京ＵＦＪ銀行
瀬古 敏智	株式会社三菱東京ＵＦＪ銀行

【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