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 2018

2018 年 3 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. 国内外の状況

2017 年のフィッシングの特徴は、金融機関、特に銀行に対する攻撃が減少する傾向にある一方、クレジットカードを狙った攻撃が急増した点にある。クレジットカード不正使用被害において、フィッシングなどによる番号盗用による被害額は前年の二倍近い金額に達した[1]。また SNS に対する攻撃も高水準で移行している。

警察庁の発表[2、3]によると、各金融機関によるモニタリングの強化やワンタイムパスワードの導入等の対策が進み、2017 年ではインターネットバンキングの不正送金による個人口座の被害額が大幅に減少し、発生件数および被害額がピーク時と比較して大幅に減少した。一方で、仮想通貨における個人口座の不正アクセスにより、不正に別口座への送金がおこなわれるなど、新たな手口が発生している。

フィッシング対策協議会の統計では、2017 年のフィッシング届け出件数が 8 月から急激に増加した。その後 10 月にやや減少するものの、11 月に再び増加に転じピークに達するなど、上半期は比較的高位な水準で推移した。この増加の要因は、大手インターネット関連製品メーカを語るフィッシングの届け出が急増したためである（図 1.1-1）。

[1]一般社団法人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および数値の訂正について
https://www.j-credit.or.jp/download/171228news_c.pdf

[2] 警察庁、 平成 29 年上半期におけるサイバー空間をめぐる脅威の情勢等について、
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_kami_cyber_jousei.pdf

[3] 警察庁、平成 29 年中におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf

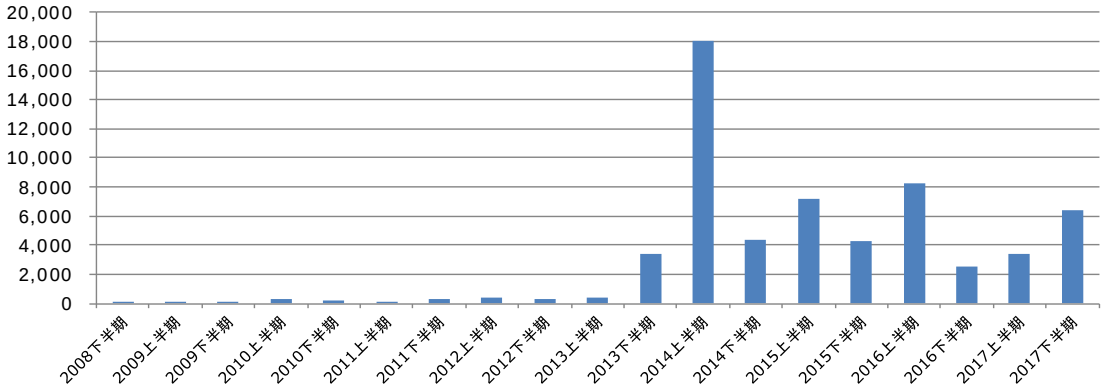

図 1.1-1　フィッシング情報の届け出件数

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け出件数は、対前年比でやや減少し、（2016 年 10,759 件→2017 年 9,812 件）ブランド名を悪用された企業の延べ件数も若干減少（2016 年 261 件→2017 年 248 件）した（図 1.1-3）。一方で、フィッシングサイトの URL 件数（重複無し）は 1.7 倍と例年と比べて大きく増加しているのが目立っている（図 1.1-2）。

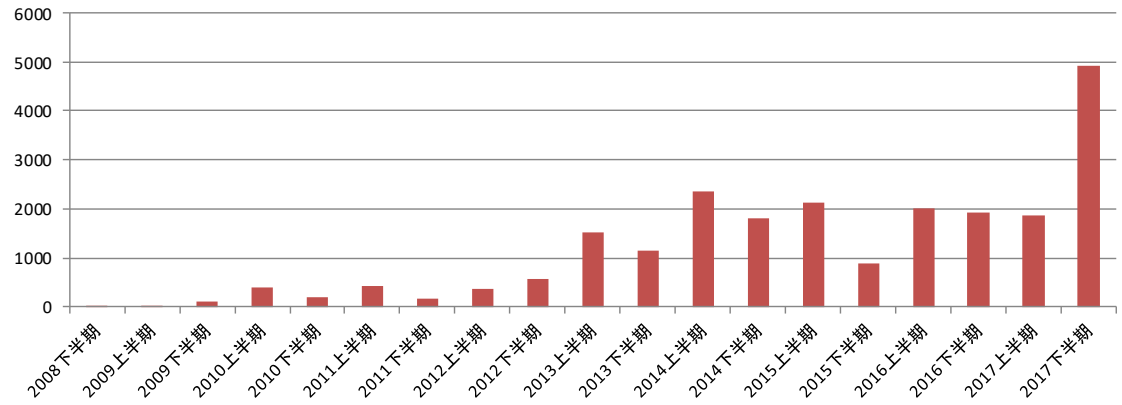

図 1.1-2　フィッシングサイトの URL 件数（重複無し）

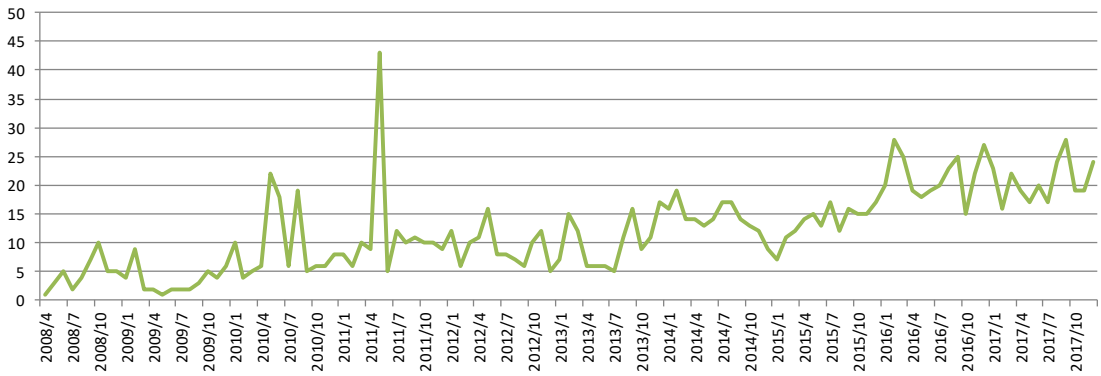

図 1.1-3　ブランド名を悪用された企業の件数

また、国家公安委員会・総務省・経済産業省の発表によれば、2017 年に警察庁に報告のあった不正アクセス行為のうち、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 2016 年に比べてやや増加した（図 1.1-4）。手口を見ると、2017 年におけるフィッシングは 2 件であり、前年と同様に比率は全体の 1%に満たない（図 1.1-5）。

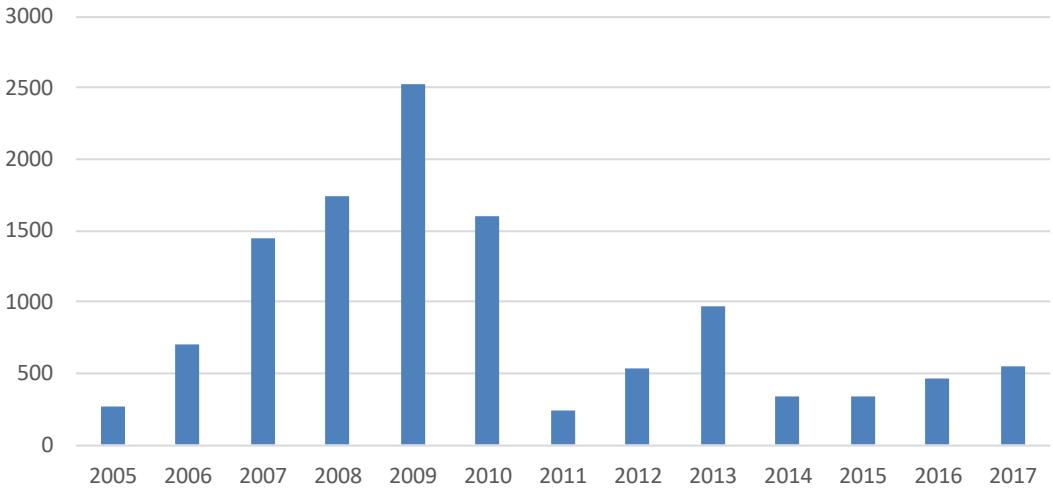

図 1.1-4　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数[4]

[4] 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/2017/03/20180322004/20180322004-1.pdf よりフィッシング対策協議会が作成

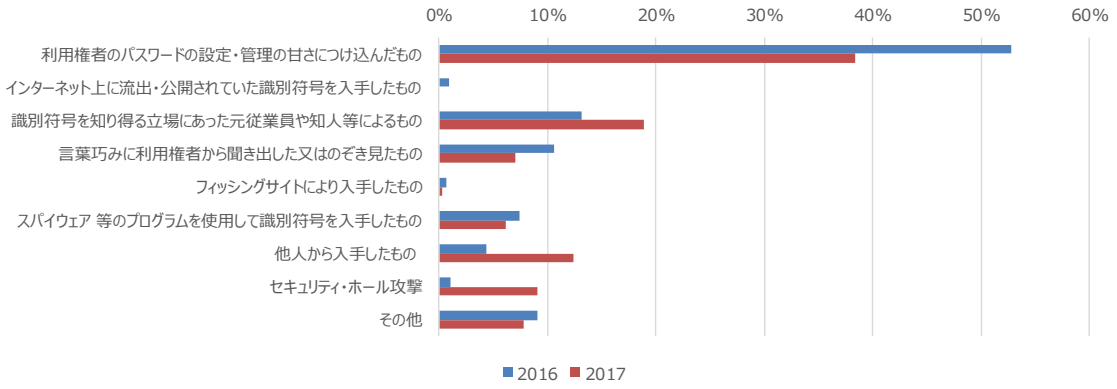

図 1.1-5　不正アクセス行為に係る犯行の手口の内訳（2016 年、2017 年）[5]

ここ数年、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が話題となっているが、警察庁の発表[6]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、2016 年は 1,291 件、約 16 億 8,700 万円と毎年減少傾向にあり、2017 年には 425 件、約 10 億 8,100 万円と大幅に減少している。一方で、電子決済サービスを悪用した不正送金やワンタイムパスワードを聞きだす手口による不正送金等の新たな手口も発生している。

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、2017 年上期のフィッシング届け出件数は、2016 年下期からやや増加した（図 1.2-1）。一方、フィッシングサイトの件数は、2016 年下期から引き続き減少傾向にある。

[5] 同上
[6] 警察庁、平成 29 年中におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf

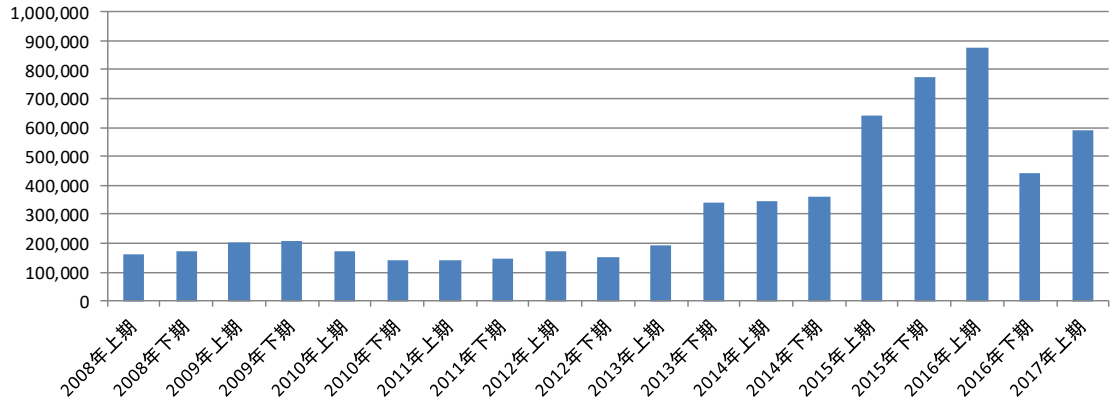

図 1.2-1　APWG へのフィッシングメール届け出件数[7]

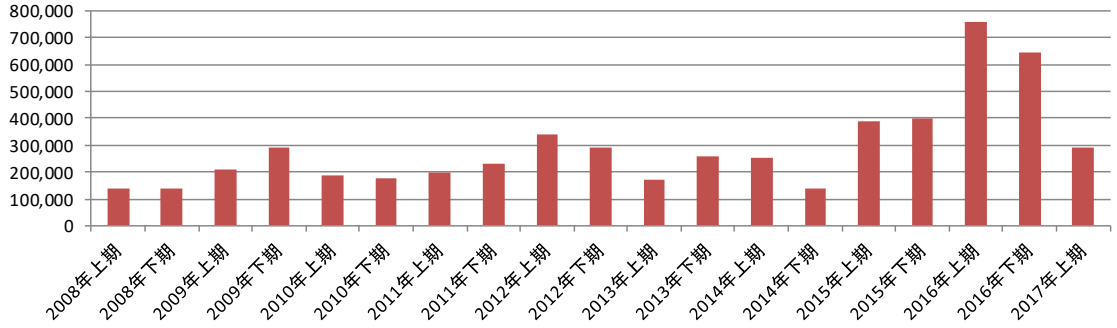

図 1.2-2　フィッシングサイトの件数（APWG）[7]

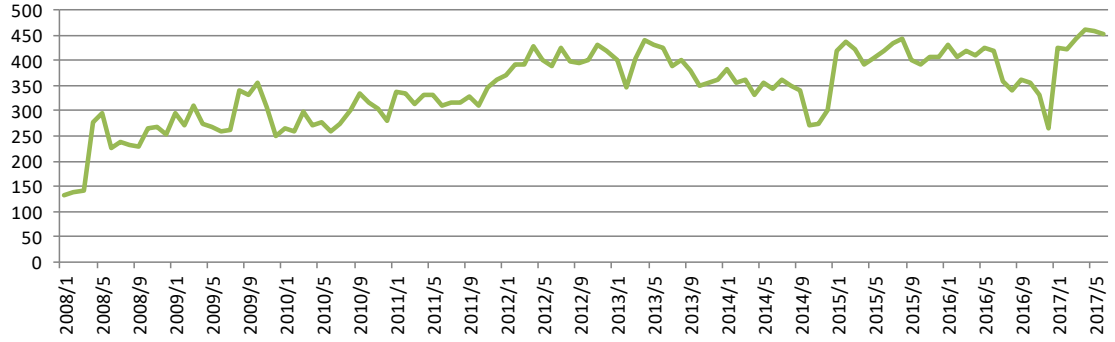

図 1.2-3　フィッシングによりブランド名を悪用された企業 月次件数推移（APWG）[7]

[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. フィッシング報告状況からみた、この 1 年の動向

2017 年のフィッシング報告件数は 2017 年 8 月から増加したが、報告されるフィッシングのほとんどがクレジットカード情報を詐取することを目的としていた。また 2017 年から HTTPS に対応したフィッシングサイトが増えており、全体の 15%以上が自ドメイン用の SSL サーバ証明書を使用していた。特に証明書発行時の審査基準が低い SSL サーバ証明書（DV）を使用する場合が多く、フィッシング対策協議会の証明書普及促進 WG で行った SSL サーバ証明書に関するアンケート調査[8]では、利用者における SSL サーバ証明書に違いに関する意識が薄いという結果となり、今後 SSL サーバ証明書の違いに関する普及啓発が必要であると思われる。

クレジットカード情報の詐取を目的としたフィッシングのうち、報告が非常に多かったあるブランドをかたるフィッシングの特徴としては、フィッシングメールに記載されている URL から最終的なフィッシングサイトまで、短縮 URL などいくつかのサイトをリダイレクト（転送）で経由するものが多く[9]、被害が発生したサイトを後日調査のため確認すると、途中でリダイレクト先を正規サイトに変更されていたり、一度アクセスした IP アドレスからは再度アクセスできなくなるフィッシングサイトも存在した。

またクレジットカード情報以外を狙ったフィッシングとしては、SNS のブランドをかたるフィッシングの報告が多く寄せられており、フィッシングにより詐取したアカウントを不正に利用して、最終的には友達に成りすまし詐欺行為を行うことが目的と考えられる。

金融関連ブランドにおいては、インターネットバンキング関連は多要素認証やワンタイムパスワードなどの対策が進み、フィッシングの報告がほとんど無くなったが、仮想通貨関連サービスのアカウント情報の詐取を目的としたフィッシングの報告が見られるようになってきた。

このように詐欺行為は環境の変化に応じて年々変化し、それに関連して日々新しいフィッシングも行われているため、今後も引き続き寄せられる報告に注視していく必要がある。

---

[8] SSL サーバー証明書に関する事業者ならびに利用者向けアンケート調査結果について (2017/09/12)
https://www.antiphishing.jp/news/info/ssl_servercertified_questionnaire.html
[9] 一例として、Apple をかたるフィッシング (2017/08/30)
https://www.antiphishing.jp/news/alert/apple_20170830.html

2.2. SMS を使用したフィッシングの増加（未納料金をかたった架空請求詐欺の手口について）

従来、フィッシングは、電子メールによる個人情報の詐取が中心であったが、携帯電話番号に短文メッセージを配信する SMS（ショート・メッセージ・サービス）による被害が増加している。

SMS によるフィッシングが増加したのは、スマートフォンの普及に伴い、電子メール（特に、携帯電話で利用するキャリアメール）の利用率、開封率が落ちている一方で、国内キャリア間の相互接続による SMS の利便性の向上、LINE などのスマートフォン・アプリでの本人認証の際の SMS の利用などによって、日本における SMS に関する認知が向上し、SMS の利用率、開封率が高まったことが背景として考えられる。このような背景によって、SMS によるフィッシングは今後も増加する可能性があるため、基本的な手口、特徴や留意点を理解しておくことは詐欺被害を予防する上で有効と思われる。

フィッシングからは少し離れるが、昨今、実在する企業を装って、架空請求をする SMS を送り、未納料金の名目で金銭を支払わせようとする架空請求詐欺が急増し、架空請求に遭う被害が急増している。

愛知県県民生活課によると、大手通販会社をかたる事業者からの SMS やメールによる架空請求の相談が急増しており、2017 年 4 月から 10 月までの7か月で、前年度1年間（38 件）の 30 倍以上（1,431 件）の相談が寄せられているとのことで、県民に対して注意を呼びかけている[10]。

事態を重く見た消費者庁からは、消費者安全法に基づき、消費者被害の発生または拡大の防止に資する情報を公表し、消費者に注意を呼びかける目的で、「SMS を用いて未納料金の名目で金銭を支払わせようとする架空請求に関する注意喚起」が公表されている[11、12]。

【架空請求詐欺の手口】

典型的な手口は、下記の流れとなる。

1） 有名企業をかたる事業者が、「有料動画閲覧の未納料金を滞納しております。本日中にご連絡なき場合には法的手続きに移ります。 03-xxxx-x

[10]◆消費者注意情報◆大手通販会社をかたる架空請求に注意しましょう！ 2017 年 11 月 10 日
http://www.pref.aichi.jp/soshiki/kenminseikatsu/1017.html

[11] SMSを用いて有料動画の未納料金の名目で金銭を支払わせようとする 「アマゾンジャパン合同会社等をかたる架空請求」に関する注意喚起 2017 年 11 月 14 日
http://www.caa.go.jp/policies/policy/consumer_policy/information/pdf/consumer_policy_information_171114_0001.pdf

[12] SMSを用いて未納料金の名目で金銭を支払わせようとする「ヤフー株式会社をか たる架空請求」に関する注意喚起 2017 年 12 月 22 日
http://www.caa.go.jp/caution/phone/pdf/caution_phone_171222_0001.pdf

xxx　有名なサービス提供企業名」などと記載した架空請求 SMS を、不特定多数の携帯電話番号に宛てて送信する。

２） SMS を読んで不安を覚えた受信者が、SMS に記載されている電話番号に電話をすると、電話を受けた事業者は、様々な偽りの説明をおこない、不安を煽り、その日のうちに未納料金を支払うように説得する。時には、一旦支払えば、後で返金されると説得することもある。

３） 支払い方法として、大手通販サイトのギフトカードをコンビニエンスストアなどで購入して、ギフトカードの番号を事業者に連絡するように指示する。

４） 説得により不安が増した受信者は、事業者の指示に従い、大手通販サイトのギフトカードを購入して、ギフトカード番号を連絡し、騙し取られてしまう。

【SMS による架空請求詐欺の特徴と留意点】

SMS は、自分の携帯電話番号宛にメッセージが送信されてくるため、すでに自分の携帯電話番号を知っている相手からのメッセージだと思いこみやすい。したがって、メッセージに対する反応率は高い傾向にある。

一方、詐欺行為を行う者にとっては、SMS の発信者が自身であると特定されないことが、非常に重要である。

SMS の配信経路は、国内 SMS 配信と海外網経由の国際 SMS の２経路がある。このうち、国際 SMS に関しては、配信依頼者の本人確認や利用用途の申告が不要で、オンライン申し込みによって SMS 配信ができる海外 SMS 配信事業者が存在するため、この配信経路を悪用することで、詐欺行為を行う事業者は自身を特定されるリスクを回避しつつ、SMS 配信を行うことが可能となる。

日本で確認されているフィッシング SMS は、海外から日本に送信される国際 SMS が多くみられる状況である。なお、国際 SMS の判別方法としては、SMS の送信元が「海外の電話番号（国番号＋電話番号）」、もしくは「アルファベット表記」となっていることから判別が可能である。

その中でも、特に注意が必要なのは、送信元がアルファベット表記の SMS の場合である。下記の事例は、送信元が「有名企業名（アルファベット表記）」となっており、有名企業から送信された SMS であると誤認させる意図で海外から配信された架空請求詐欺 SMS である。

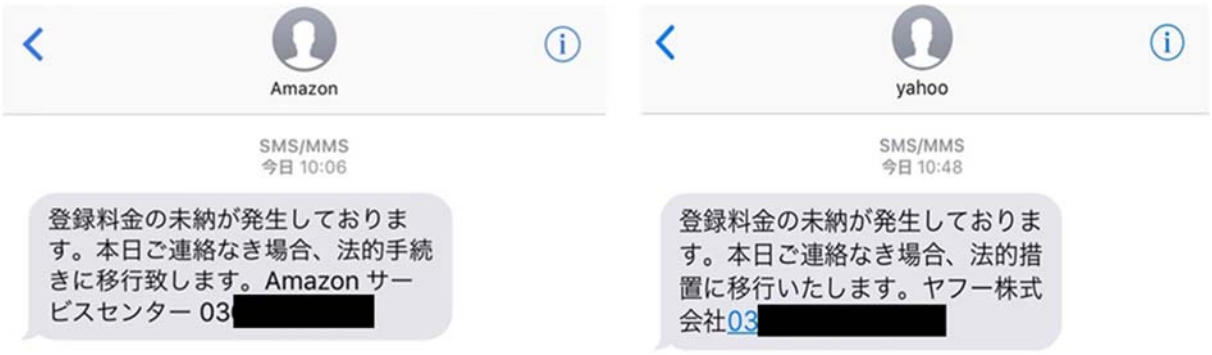

図 2.2-1　送信元がアルファベット表記の SMS の例

海外から配信される国際 SMS では、送信元を誰でも任意の「アルファベット」として SMS を送信することが可能である。つまり、送信元名が契約者と一致しているか確認されることなく SMS を送信することができるため、有名な企業からの SMS をかたることが容易である。一般消費者は、その様な認識がないため、送信元が「アルファベット」表記の企業名である場合、あたかもドメインの様に第三者機関に登録されているかのように感じ、かたられた企業そのものから送信された SMS であると信じてしまう。

以上のことより、送信元情報が、「海外の電話番号（国番号＋電話番号）」、もしくは「アルファベット表記」である SMS を受信した場合には、本文の内容いかんに関わらず、特に慎重な対応が必要と思われる。

【伊藤彰浩　株式会社アクリート】

2.3. フィッシングなどによるクレジット情報詐取

インターネットの普及とともにネットショッピングの取り扱いは急激な伸びを見せており、ネットショッピングの支払い手段として利便性が高く数々の特典を有するクレジットカードが広く用いられている。一方でクレジットカード番号さえ入手すれば他人になりすまして各種商品・サービスを購入することができてしまうことから被害も多発している。

一般社団法人日本クレジット協会の発表によると、2017 年のクレジットカード不正使用被害額は 236.4 億円で、前年 2016 年の被害額（142.0 億円）を上回っている。このうちクレジットカード番号が非対面取引（インターネット取引等）で不正使用されたケースは 176.7 億円にのぼる。

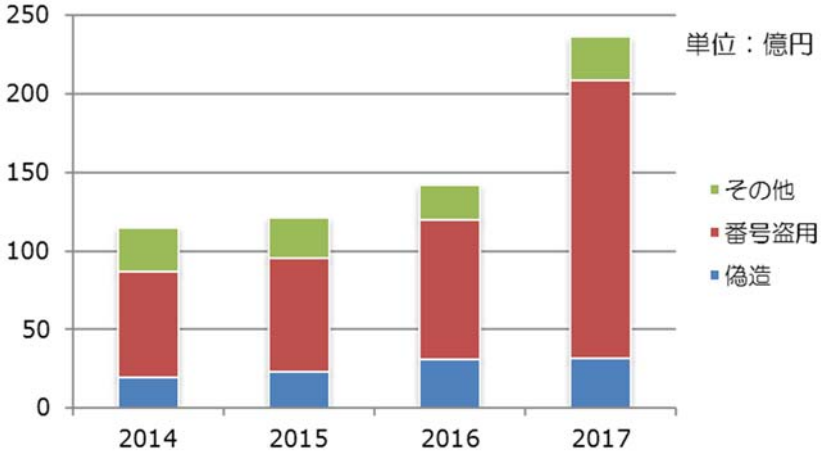

図 2.3-1　クレジットカード不正使用被害額の発生状況[13]

表 2.3-1　クレジットカード不正使用被害額とその内訳 [13]

	2014 年	2015 年	2016 年	2017 年
偽造*1	19.5	23.1	30.6	31.7
番号盗用*2	67.3	72.2	88.9	176.7
その他*3	27.7	25.6	22.5	28.0

（単位：億円）

*1：日本のクレジットカード会社が発行したカードの偽造による被害

*2：情報漏えい等によりカード番号が不正利用された被害

*3：紛失・盗難等による被害

[13] 一般社団法人日本クレジット協会資料「クレジットカード不正使用被害の集計結果について」（https://www.j-credit.or.jp/download/news20180330b.pdf）より作成

カード番号が他人に使用される原因にはフィッシングメールを開封して偽サイトに誘導されカード番号を入力、あるいはマルウエアに感染しカード番号が外部に漏れる、利用加盟店からの情報漏えいにより大量のカード情報が窃取される等のケースが考えられる。クレジットカード会社では 24 時間 365 日クレジットカードの利用状況をモニタリングしながら必要に応じて利用内容の確認し、また明らかな不正利用と判断された場合はカード利用を停止するなど、クレジットカード番号が詐取され不正利用されたとしても被害が最小限になるように努力している。

あわせて一般消費者(クレジットカード利用者)がクレジットカード被害にあわないように注意するとともに EC 加盟店にも割賦販売法の改正に伴い様々な対応が求められる。

具体的には、クレジットカード情報の漏えい防止の為、カード情報の非保持化、カード情報を取り扱う事業者は国際規格（PCIDSS）準拠することなどである。詳細については契約するクレジットカード会社に問い合わせ願いたい。

3. 新しい攻撃手法・対策の動向

3.1. DV 証明書の悪用、ブラウザ側の DV 証明書に対する警告

Web 通信における「通信の暗号化と改ざん防止」、および「サイト存在性の証明（なりすまし防止）」のために利用される SSL 証明書には、認証レベルにより「ドメイン認証型（DV : Domain Validation）証明書」、「企業認証型（OV : Organization Validation）証明書」、および「EV (Extended Validation 証明書」の 3 種類がある。

OV 証明書では登記事項証明書や第三者データベースを用いた事業者の実在性が認証され、EV 証明書では更に厳格な実在性確認が行われるのに比較し、DV 証明書はドメイン使用権の有無のみの認証となり、事業者の実在性は審査対象外となるのが最大の違いである。

各 SSL 証明書の認証レベルを考慮すると、OV 証明書や EV 証明書が外部向け Web サイトにおける暗号化通信となりすまし防止の両方の目的に利用しうるものであるのに対し、DV 証明書はどちらかというとイントラネットなどで暗号化通信の実現に目的を絞って利用するのが望ましいと言えよう。

一方で DV 証明書は安価（あるいは無料）かつ容易に入手が可能であり、さらに DV 証明書を使用することでブラウザ上に安全な通信を意味する鍵マークが表示されるため、悪意のある不正行為者がフィッシングサイトを立てる際に DV 証明書を用いてユーザに安心なサイトのように誤解させるために悪用されるケースが数多く見受けられる。

ブラウザ上で SSL 証明書の詳細情報を確認することは技術的には可能だが、一般ユーザに対して Web サイトにアクセスするたびにそのような操作を強いることは現実的とは言えない。各 Web サイトで使用されている SSL 証明書の種類により、ブラウザ上でその違いを明示的に表現するといった提案もされており、一定の効果は期待できるが、事業者においてもユーザ名とパスワードの入力を求めるサイトにおいては OV 証明書や EV 証明書を利用するといった配慮が必要とされている。

【小池浩之　EMC ジャパン株式会社 RSA】

3.2. Web ブラウザにおける表示や証明書の有効性に関わる動向

Web のサービスを利用する環境は、従来のパソコンで動作する Web ブラウザから、スマートフォンで動作するものに至るまで多様化している[14]。HTTPS のセキュリティを担うサーバ証明書の仕組みは基本的に多くのサーバ/ユーザ環境で共通しているが、そこで使われる認証局や Web ブラウザなどの位置づけは変化しつつある。本節では Web ブラウザにおける表示や証明書の有効性に関わる最近の動向について紹介する。

■ Symantec のサーバ証明書の移行

2017 年 8 月、Symantec はサーバ証明書に関わる事業を DigiCert に売却することを発表した[15]。

これは Google による証明書発行の適切さに関する指摘を受けた後、最終的に至ったもので、今後、Symantec のルート証明書は Google Chrome において段階的に無効化されてゆくことが計画されている[16][17]。この計画によると、2016 年 6 月より前に発行された Symantec のサーバ証明書は、2018 年 4 月に安定版が公開される予定の Chrome66 では有効ではなくなることになる（Chrome66 のベータ版は 2018 年 3 月に公開予定）。

これに対して Symantec のサーバ証明書に関わる PKI の事業を買収した DigiCert では新しい CA がすでに構築されており、DigiCert の子会社で日本法人であるデジサート・ジャパンは、サーバ証明書の発行を受けている国内ユーザにサーバ証明書の申請手続きを案内している[18]。Symantec のサーバ証明書を購入していた場合、自社のサーバ証明書を更新する必要があるのかどうか、今一度確認が必要である。

■ Chrome におけるグリーンバーの表示

---

[14]総務省｜平成 29 年版 情報通信白書｜数字で見たスマホの爆発的普及（5 年間の量的拡大）
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc111110.html

[15] ［続報］Symantec Website Security からの重要なお知らせ
https://knowledge.symantec.com/jp/support/code-signing-support/index?vproductcat=V_C_C&vdomain=VERISIGN.JP&page=content&id=ALERT2420&actp=LIST&viewlocale=ja_JP&locale=ja_JP&redirected=true

[16] Chrome's Plan to Distrust Symantec Certificates, September 11, 2017
https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

[17] Google Developers Japan: Chrome が Symantec の証明書に対する信頼を破棄する予定について, 2017 年 9 月 28 日木曜日
https://developers-jp.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

[18] 【続報】【重要】マネージド CA 対応に伴う SSL サーバ証明書製品ならびに申請システム等における仕様変更などのご案内, デジサート・ジャパン合同会社, 2017 年 11 月 17 日
https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=ALERT2446

Web サーバにおいて正常に EV 証明書が利用できるように設定されているにも関わらず、Web ブラウザなどでグリーンバーの表示がされないことがある。これは Chrome 上での不具合のほかに、Web ブラウザによる Web ページのチェックに起因するものである。Google では Chrome におけるこの仕様について 2015 年に公表している[19]。

特に注意が必要なのは HTTPS でアクセスされている Web ページ中に HTTP のコンテンツが混在している「Mixed Contents」と呼ばれる状態で、ユーザが複数のサーバからコンテンツを取得して閲覧するような形で構成されている Web ページにおいては確認が必要である。「Mixed Contents」の詳細については Google Developers のページ[20]が詳しい。

Google Chrome は Internet Explorer や Firefox と共に一定のシェアがある Web ブラウザであり、特に自社の運営する Web サイトについては、その表示を確認しておきたい。

■ トラストアンカーをめぐる関係性の変化

トラストアンカーとは、証明書の有効性の確認のために使われる認証局証明書である。Web のいわゆるパブリック認証局に関わる事業を行う企業がトラストアンカーとなる認証局を運営している。

従来、認証局は WebTrust for CA やそのガイドラインなどをクリアするような一定の運用が行われ、その業務に関する監査を受け、認定を取ることで Web ブラウザや OS のいわゆる「信頼されたルート証明機関」に入っていた。

しかし、2011 年頃、認定を受けていた認証局において不正証明書発行事件が発生したため、現在は不正な証明書を発見するための CT（Certificate Transparency）ログのような新たな技術的な仕組みが導入されたほかに、Web ブラウザの開発元における独自の審査が行われるようになった。各国の行政サービスに使われるような認証局であっても Web ブラウザに組み込まれるまでの審査が長びくことがあり、認証局にとって、この審査が課題となっている。証明書をユーザに有効であると表示することに関して、実質的に Web ブラウザの影響力が高まりつつある。

前述の CT ログは、各認証局によって発行された証明書を衆人環視できるようにする仕組みと言える。多くの CT ログは一般に公開されており、CT ログを使

[19] Google Online Security Blog: Simplifying the Page Security Icon in Chrome view-source:https://security.googleblog.com/2015/10/simplifying-page-security-icon-in-chrome.html

[20] 混合コンテンツの防止 | Web Fundamentals, Google Developers https://developers.google.com/web/fundamentals/security/prevent-mixed-content/fixing-mixed-content?hl=ja

って、どの認証局がどのような種類の証明書を発行しているかといった情報を閲覧できるサイトも作られている[21]。分析のみならず、どの認証局に証明書の発行を受けるのかを判断するためにも使われていると考えられる。

■フィッシング対策としてのチェック事項

ユーザがアクセスしているサイトが正規のサイトなのか偽のサイトなのかを判別できるようにしておくことはフィッシング対策として重要な位置づけにある。この判別を容易にするためには、平常時には「セキュア」な状態を見せておいて、異常があればその状態とは異なるということを周知徹底しておくことになる。

- HTTPS

  HTTPS の設定について、簡単にチェックできるサイトがある。Qualys の提供する SSL Server Test[22]は自社のサーバの設定をチェックするために利用できる。チェックの結果には、ユーザ環境で正常にアクセスできるかどうかについても表示されるが、前述の Chrome におけるグリーンバーの表示のように実際にコンテンツにアクセスしてみないとわからないこともある。SSL Server Test と合わせて、主要なユーザ環境で実際にアクセスしてみて、正常に表示されるかどうかを確認する事が必要である。

  主要なユーザ環境が何なのかは Web サーバのログを分析する事で調べることができる。使われている TLS のバージョンや TLS のアルゴリズムは Web ブラウザにおけるグリーンバーの表示にも関わるため、こちらも確認しておきたい。

- サーバ証明書

  フィッシング詐欺の発生を低減されるという観点では、ユーザが認知しやすい社名の EV 証明書を利用し、その旨をユーザに案内しておくことが重要であると考えられる。スマートフォンの中には URL ではなく EV 証明書を通じて確認された社名が表示されるものがある。ドメイン名などの技術に詳しくないユーザでもアクセス先を判別できるようになってきていると言える。

■対策にあたって

本節では Web ブラウザにおける表示や証明書の有効性に関わる動向をまと

---

[21] Censys：https://censys.io/

[22] SSL Server Test (Powered by Qualys SSL Labs)
https://www.ssllabs.com/ssltest/

めた。Web サーバを自社で構築して運用しておらず、サーバ証明書を扱うシステムが外注先によって設計開発される場合には、発注側による要件として含める際などにご利用いただきたい。

　ユーザに対して警告表示を無視するような案内をすることは、不正なサイトと正規のサイトとの区別がつかないような事態を招きかねない。今後も最新動向を踏まえた構成や設定にすることによって、技術的な知識がないユーザでもリスクを避けられるようになることを願いたい。

3.3. DKIM に関して

送信ドメイン認証には SPF（Sender Policy Framework）と DKIM（DomainKeys Identified Mail）などがあり、ドメイン名の部分で認証を行い、フィッシングメールを防ぐ技術である。フィッシングメールは正規のメールサーバを経由せずにドメイン名（メールアドレスの@より右側部分）を偽って送信される場合がある。送信ドメイン認証技術はメールが正規なメールサーバから送信されたものであることを判別する機能となる。

3.3.1. 国内での普及率

総務省が行っている電気通信事業者における全電子メール数の送信ドメイン認証結果調査によると、2017 年 12 月時点での SPF の普及率は 94.74%と高い普及率を保っており、DKIM の普及率は順調に増加し 50%を超えている。

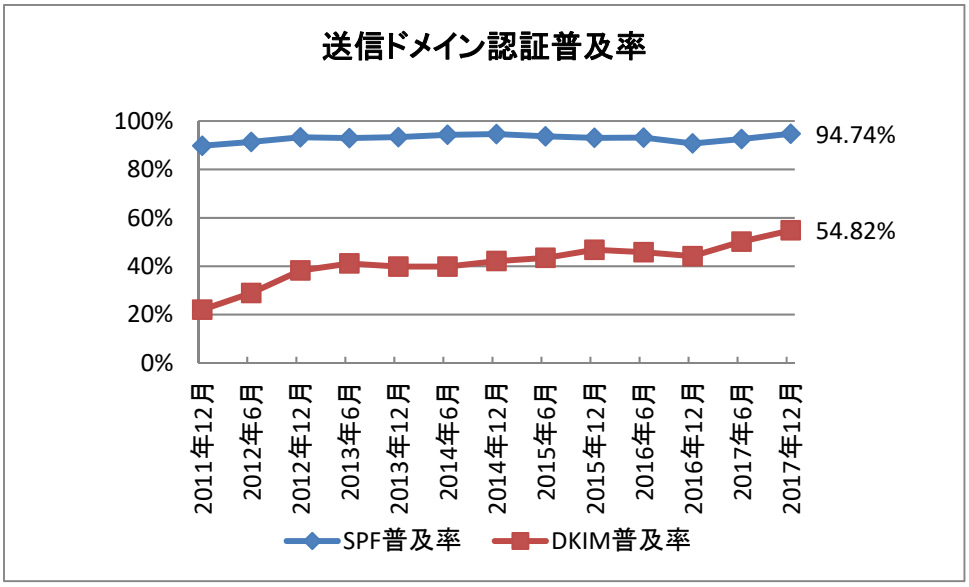

図 3.3-1 送信ドメイン認証普及率（総務省 送信ドメイン認証結果の集計(DKIM)[23]より）

3.3.2. DMARC の動向

DMARC （ Domain-based Message Authentication, Reporting & Conformance）とは SPF や DKIM の認証結果を元にメールヘッダ上の送信者情報（From:ヘッダ）のドメインとの関係性を比較し DMARC として認証を行

[23] 総務省 迷惑メール対策「送信ドメイン認証結果の集計（DKIM）」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei

い、あらかじめ決めたポリシーにより送信者側がメールの挙動を管理する仕組みである。認証が失敗したメールの状況を見ながら徐々に失敗したメールをフィッシングメールとして利用者に届けないようにしていく運用なども可能になる。

■ DMARC レコードのポリシー
①None：そのまま受信させる（そのまま受信者に届ける）
②Quarantine：隔離させる（認証に失敗した旨を付して隔離する（迷惑メールとして扱う）
③Reject：受信を拒否する（受信サーバから削除する（受信者は存在を認識しない）

■ DMARC の設定
メールの送信側は、すでに SPF や DKIM を導入している場合は、DMARC レコードを追加設定することで導入することができる。

■ DMARC 導入に関する法的な留意点
総務省は迷惑メール対策技術に関して、法的な整理を行い迷惑メール対策技術の導入を促進している。2017 年 7 月 6 日に「DMARC 導入に関する法的な留意点」が公開され、DMARC の特徴であるポリシーに基づいた受信サーバ側のメール処理について、フィルタリングサービスが利用者の有効な同意に基づいて提供される場合、送信ドメイン認証行為は、正当業務行為に該当し、このことは DMARC 実施のために行われる送信ドメイン認証行為においても同様であるとまとめられた。また、同意について以下の 5 つの条件を満たすことが必要としている。

■ DMARC 導入にあたっての利用者同意に関する 5 つの条件
①利用者が、随時、任意に設定変更できること。
②同意の有無に関わらず、その他の提供条件が同一であること。
③同意の対象・範囲が明確にされていること。
④送信ドメイン認証の結果に係るレポートを送付する場合、レポートの内容に電子メールの本文および件名が含まれていないこと。
⑤DMARC の内容について、事前に以下を含めた十分な説明を行うこと。
- ポリシーにより受信拒否を行う場合は、「受信拒否を行う旨」「受信拒否された場合、利用者はその内容を確認できない旨」を説明する。
- 送信側管理者の求めに応じてレポートを行う場合は、「レポートに記載す

る事項」、「送信側の指定した宛先に送付される旨」を説明する。

今後、DMARC が受信サーバ側および送信側の双方で導入が進むことにより、正規ドメインをなりすましたフィッシングメールを利用者に届けない運用の拡大が期待できる。2017 年の後半に楽天カードや楽天銀行、アマゾンのフィッシングメールが多くみられたが、両社はすでに DMARC を導入済みであることから、DMARC を実装しているプロバイダーの利用者においては、本フィッシングメールが届かない、または迷惑メールフォルダに隔離されることが期待できる。

【加藤孝浩　トッパン・フォームズ株式会社】

3.4. 利用者に信頼してもらうための方策

3.4.1. BANK TLD などでの事例

インターネットバンキングの利用者をフィッシングなどの詐欺から保護する為に、顧客へのウイルス対策ソフトの配布やサーバ側でのユーザ端末の感染状況の監視など、不正ソフトウエア対策についてはほとんどの金融機関が提供している。さらにフィッシングによる不正送金の被害を防ぐために、ワンタイムパスワードトークンの配布、さらにトランザクション署名の導入と、詐欺被害からインターネットバンキング利用者を守るための技術的な対策もほとんどの金融機関が提供済みとなっている。

それにより、全銀協や金融庁のインターネット銀行の不正振り込み被害の統計データによれば、被害件数はかなり減少している。

しかし、どんなに技術的な対策を実施しても、ワンタイムパスワードを電話で聞かれて教えてしまうなど、ユーザが騙されるソーシャルな部分での対策は困難である。

被害を防ぐ技術的な対策は一巡し、今後は、インターネットバンキングのサイトや銀行からの通知メールを利用者が信頼できるようにし、なるべく騙されにくくする対策が求められる。

そうした点で、金融機関向けの特別な gTLD(Top Level Domain)である fTLD の一つの.BANK は、そのドメイン名に利用者が信頼をおけるように、以下のようなセキュリティ対策をそのドメインの取得に求めている。

- DNSSEC の実装 ： 今後の信頼を基礎としたセキュリティ技術の実装の為の基本として要求
- 強い暗号(TLS 1.1 以上)の使用：Web は常時 HTTPS を要求
- Email 認証(DMARC)の実装：メールの送受信においても暗号通信が必要
- DNS リソースレコードの強化：権威ネームサーバのホスト名が.BANK ドメインゾーンにあることなど

ちなみに.BANK では EV 証明書を求めていない。これは、.BANK を取得するための要件が、EV 証明書の取得要件より厳しいため、.BANK を取得できていれば、ドメイン名で EV 証明書以上の信頼を置けるためであると思われる。

また、英国の NCSC では、Active Cyber Defence という DMARC を含む以下のような活動を 1 年行ってきたレポート[24]を公開しており、DMARC は、政府

[24] National Cyber Security Center: Active Cyber Defence – one year on https://www.ncsc.gov.uk/information/active-cyber-defence-one-year

組織のドメインを騙ってのフィッシングメールを防ぐのにかなりの効果を発揮したとされている。

- 不正なサイト、送信元の閉鎖
- DMARC の導入
- 政府の Web サイトの安全性の自動検査
- 政府用の DNS サービスの提供による不正サイトへの接続ブロック

さらに、米国政府の DHS(米国国土安全保障省)は、昨年 10 月にすべての政府機関に対し DMARC の導入を 3 か月以内に実施するよう指示し、約 50%の機関で DMARC の導入が行われたという。これも、米国証券取引所をなりすましての金融機関への標的型メールがきっかけとなっている。

これまでは、セキュリティ対策はどちらかと言えば、悪いものを判別して防御する技術が主流であった。これからは DMARC や DNSSEC などのように詐称を防ぐ技術を使い、Internet 利用者が正しいものを見分けられる技術が必要となってくる。まずは、政府機関や銀行など人々に高い信頼を得ていて、詐称される危険性の高い組織からの積極的に導入をお願いしたい。

3.4.2. その他の取り組み

インターネットでのサービス提供が多種多様となり利用が広がるなか、フィッシング詐欺による被害や情報漏えい事件による被害も多く発生し、その被害が身近となっている。インターネットサービスの利用者は、常にフィッシング詐欺などに遭う危険を認知し、注意しながらサービスを利用することが要求されている。このような状況で、できる限り被害に遭わないような対策がされているサービスを利用したいと思うのは必然なことである。

利用者の安心につながる対策がとられている事を利用者へ知らせることが、利用者にとっても、サービス提供者にとっても価値のあることといえる。

また、SNS 利用者による発言がサービス提供者の存続をも左右するソーシャルネットワーク時代において、サービス提供者は、被害防止、事故、事件による被害（インシデント）対応について透明性を持って公開していくことが重要となっている。公開すると攻撃者に狙われるという理由でセキュリティに関することを隠す傾向は依然としてあるが、自社が行っているセキュリティ対策・体制などを公開することの利点を認め、実施している企業、組織も増えている。

公開すべき内容は大きく 2 つあり、被害防止観点の対応についてと、インシデントが発生した後の対応についてとに分類できる。

被害防止での事例としては、自サービスを巧妙に真似たフィッシングサイトを探し出し、利用者へ注意喚起するとともに、削除の対応をとるなど利用者を被害から守る活動を行い、その活動について公表し利用者からの信頼を得ている例がある。

被害発生後の対応だけでなく、事前での対応も含む例では、コンピュータセキュリティインシデント対応チーム（CSIRT）を構築し、インシデント、被害への対応、日ごろのセキュリティ対策の実施を企業全体として取り組むことを実施、その状況を公開することで利用者からの信頼を得ている例がある。日本コンピュータセキュリティインシデント対応チーム協議会（NCA）による「CSIRT スタータキット」においても、その目的はいろいろとあるが、サービス対象や社外へ CSIRT の存在をアピールすることが必要である、と言っている。

以上のように利用者に信頼してもらうための方策として、セキュリティ対策、体制について透明性を持って公開する取り組みが重要であり、その実施が多く見られるようになった。

【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】

3.5. フィッシングの類似手法

最近、偽の通販サイトで会員登録を装って個人情報やクレジットカード番号を詐取する手口が増えている。偽の通販サイトは、EC サイト構築ツールを使用しており、サイトの構成や機能、日本語表記も普通の通販サイトと遜色ないものが多くなっている。

新規の利用の場合、商品の配送先として必要な全ての個人情報、ID のメールアドレスとパスワードの入力フォームが表示される。また決済情報を詐取する場合は次に決済のためのクレジットカード番号やセキュリティコード（３桁もしくは 4 桁の数字）を入力するフォームが表示されるものもある。

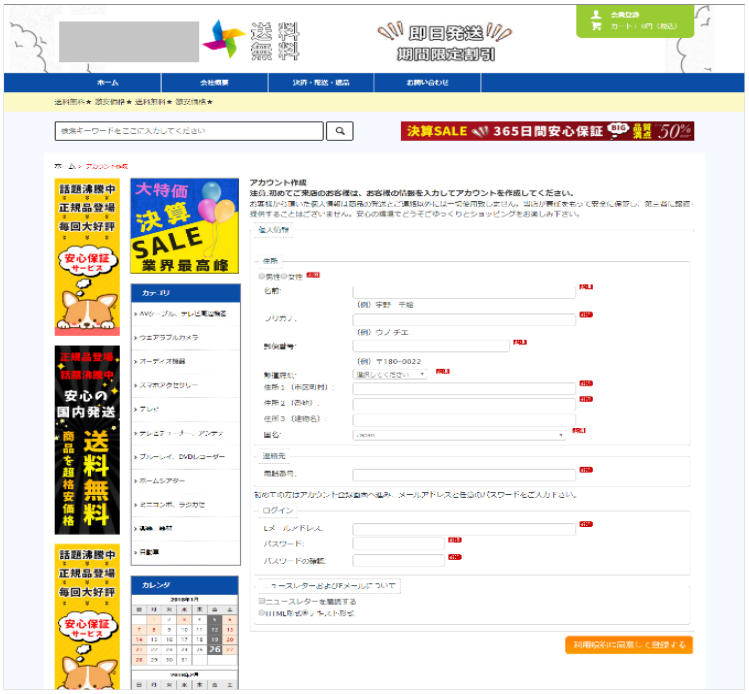

図 3.5-1 ある偽通販サイトの入力フォームの例

入力情報を送信すると、注文完了となるが、当然商品が送られてくることはなく、しばらくするとサイトは消滅してしまう。

問題は、詐取された情報がどのように使われるかである。仮に被害者が他の通販サイトでも同じ ID、パスワードを使用していた場合、成りすましログインをされ、商品を勝手に購入、詐取されてしまう可能性がある。また、クレジットカード情報を使って勝手に買い物をされる恐れもある。

有名な会社名、ブランド名をかたったフィッシングサイトとは異なるものの、認証情報や決済情報を詐取する手口のバリエーションが増えていることが伺える。

【山本和輝　BB ソフトサービス】

4. まとめ

ワンタイムパスワードなどの対策の普及促進により、インターネットバンキングにおける被害は、特に個人利用者を中心に昨年の傾向から引き続き減少を示している[25]。年々増加していた被害額を、業界をあげての努力により、傾向を反転させることに成功したとも言えるであろう。

また、攻撃側にも損益分岐点は必ず存在する。これをすれば被害は防げるという絶対的な対策は無くとも、二重三重に対策を積み重ね、攻撃側のコストパフォーマンスを下げ、攻撃を敬遠させることが重要となる。一方で、防衛側はこれら対策を一過性の短期的実施に留めることなく、中長期に渡って継続して対抗することで効果をあげられるよう、コストを下げ、日常の当たり前のルーチンにまで対策を定着させたい。そのためには、認知・検知からはじまる一連の対応を滞ることなく短時間で完了するための自動化とフロー化を推進することも重要となる。

一方で、従来から続く大手サービス事業者をかたるフィッシングなども依然として発生しているとともに、フィッシング対策協議会に寄せられるフィッシング報告件数が高水準で推移し、フィッシングサイト件数も昨年比 1.7 倍と大幅増加している。さらに最近では、仮想通貨という新しい分野での攻撃も発生しており、各事業者や利用者は、これら動向を注視のうえ、まだ被害が大きくない業界も含めて、日常からできる対策は社内教育やお客様啓発含め、地道にかつしっかりと進めていきたい。

メール送信をサービスの一部として扱う事業者は、フィッシングを含む多くのサイバー攻撃の起点となる標的型メールや無差別のフィッシングメールなどに高い効果が期待できる DMARC の導入については是非検討したい。

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対策の展開や啓発などを推進し、利用者・事業者を今後とも一層支援していくこととしたい。

【早川和実　NTT コミュニケーションズ株式会社】

---

[25] インターネット・バンキングによる預金等の不正払戻し件数・金額について
https://www.zenginkyo.or.jp/topic/correspondence/

（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)

【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】

伊藤 彰浩	株式会社アクリート
大岩 伸行	株式会社アクリート
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
渡辺 アラン	Vade Secure 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
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
山本 和輝	BB ソフトサービス株式会社
小池 浩之	EMC ジャパン株式会社
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
武藤 蔵	一般社団法人全国銀行協会
貞広 憲一	株式会社みずほフィナンシャルグループ
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
中山 広樹	株式会社三井住友銀行
鈴木 哲治	株式会社ジャックス
黒田 和宏	NTT コムオンライン･マーケティング･ソリューション株式会社
福地 雅之	NTT コムオンライン･マーケティング･ソリューション株式会社

【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