

フィッシング対策には最新版ガイドラインをご活用ください



利用者向けフィッシング詐欺対策

ガイドライン

※最新版ガイドラインをご活用ください

2013年6月

フィッシング対策には最新版ガイドラインをご活用ください



目次

1. フィッシングとは ～あなたのパスワードが狙われている～	1
1.1. 類似手法 ～フィッシングだけではありません～	3
1.1.1 ウイルスによるパスワードの取得	3
2. フィッシング対策3つの心得	5
3. 今すぐできるフィッシング対策	6
3.1. 怪しいメールに注意しましょう	6
3.1.1 銀行やショッピングサイト等のサービス内容を確認しましょう	6
3.1.2 電子署名の確認	7
3.1.3 自動検知機能の活用	7
3.2. 正しいURL にアクセスする	8
3.2.1 正しいURL を確認し、ブックマークに登録する	8
3.2.2 電子メール中のリンクはクリックしない	8
3.2.1 錠前マークの確認	9
3.3. パソコンを安全に保ちましょう	10
3.3.1 最新のセキュリティパッチの適用とウイルス対策	10
3.3.2 パスワードのしっかりとした管理	10
3.4. 正しいアプリをつかう	10
3.5. 間違って重要情報を入力してしまったら	11
4. フィッシング対策協議会と本ガイドラインの位置づけ	13
5. 付録：フィッシング事例	14

フィッシング対策には最新版ガイドラインをご活用ください



1. フィッシングとは ～あなたのパスワードが狙われている～

フィッシング (Phishing) とは、「魚を釣る (Fishing)」フィッシングのことではなく、人をだまして情報を盗み、最終的に金銭的な利益を得ようとする不正行為のことを意味します。フィッシングにより、例えば、あなたのインターネットバンクやショッピングサイトの登録情報 (ID、パスワード) が盗まれ、勝手にお金が引き出されたり、物品を購入されたりする恐れがあります。

魚釣り (Fishing) と紛らわしいので、「フィッシング詐欺¹」と呼ばれることもあります。その定義は様々ですが、我々フィッシング対策協議会では次のように定義しています。

フィッシング (Phishing) とは、金融機関 (銀行やクレジットカード会社) などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為です。(フィッシング対策協議会 HP より)

魚釣りにたとえると、魚を集めるための撒き餌として電子メール (フィッシングメールと呼びます) を大量に送りつけ、魚を釣るための釣り針として正規ウェブサイトの模倣サイト (フィッシングサイト) を設置し、魚、つまりインターネットユーザがかかるのを待つという一連の行為となります。

2012 年のフィッシングは、インターネットバンキングの利用者を標的とするものが多発し、都市銀行、ゆうちょ銀行などの大手金融機関を中心に 7 行が標的となりました。特に 6-7 月期には総額 2950 万円もの不正引き出しが発生するなど、実被害に発展するケースが多くみられました。

●偽メール・偽銀行サイトを用いる手口

2012 年前半は、金融機関を装う偽メールを使い偽銀行サイトへ誘導後、送金に必要な暗証番号、第二暗証の乱数表の全てを入力させるといった手口が多く見られました。

●ウイルスを用いた新たな手口

偽メール、偽銀行サイトを用いる手口が警戒されるようになってきた 10 月には、ウイルスを用いた新たなフィッシング手口が発生しました。

これは、インターネットバンキング利用者の PC をウイルスに感染させ、利用者が

¹2012 年 3 月に不正アクセス禁止法が改正され、2012 年 5 月に改正法が施行されたことにより、フィッシング詐欺行為が処罰対象となりました。

フィッシング対策には最新版ガイドラインをご活用ください

感染 PC から正規の銀行サイトへアクセスした際にウイルスを稼働させ、偽の暗証番号入力画面を表示するといった手の込んだものです。正規サイトのログイン操作を行う際に、偽の入力画面がポップアップ表示されるため、ほとんどの利用者は疑うこともなく、偽の入力画面に暗証番号を入力してしまいます。

このように、犯罪者は利用者が気づきにくい手口や、思いもよらない新しい手口を次々と編み出してくるため、セキュリティソフトの機能やこれまでの知識だけでは、被害を防ぐことが困難になっています。

被害に会わないようにするためには、

- ・ OS やアプリケーションの脆弱性に関する修正プログラムを迅速に適用する。
- ・ セキュリティソフトのプログラムアップデート、定義ファイルを最新のものにしておく。
- ・ 最新のフィッシング手口に関する情報に関心を持ち、予備知識を得ておく。
- ・ 金融機関が行わない事（ネット上で第二暗証を全て入力させるなど）を把握しておく。

などの行動を取り、つねに関心と警戒意識を維持することが大切です。

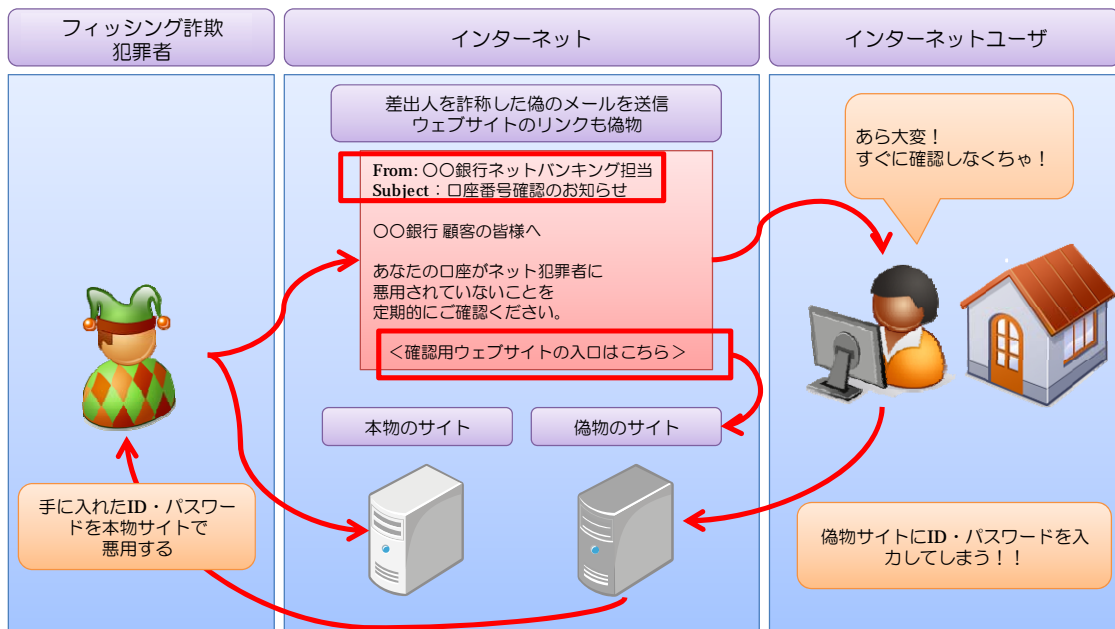


図1 典型的な「フィッシング詐欺」行為

※スマートフォンを対象とするフィッシングも確認されています。本ガイドラインは主

フィッシング対策には最新版ガイドラインをご活用ください



に PC の利用者を想定した対策を示していますが、スマートフォンユーザーもフィッシング詐欺の対象となり得ることを覚えていてください。

1.1. 類似手法 ～フィッシングではありません～

何らかの手法を使って個人情報をだまし取る行為については、フィッシング詐欺だけではなく、次のような手法が知られています。本ガイドラインで対象とするフィッシング詐欺だけでなく、このようなだましの手法にも十分な注意が必要です。

1.1.1 ウイルス²によるパスワードの取得

閲覧したインターネットユーザのコンピュータに情報を窃取する機能をもったウイルスをダウンロードさせるよう、有名企業の正規サイトを改ざんする事例が急増しています。このようなタイプの典型的なウイルスには、コンピュータのユーザがキーボードから打ち込んだ文字列を記録し、所定のサーバに送信する機能をもつものがあります。

近年ではゆうちょ銀行のゆうちょダイレクトをはじめとした、いくつかの金融機関のインターネットバンキングサービスを利用しているユーザに対して、第二認証情報の入力を求めるウイルスの存在が確認されています。このウイルスはユーザが正規のインターネットバンキングにログインした後に、ブラウザ上に第二認証情報の入力を促す不正なポップアップメッセージ（図 2）を表示し、あたかも正規サイトが入力を促しているようにユーザに見せかけ、第二認証情報などの詐取を試みます。

² ここでのウイルスとは、いわゆるコンピュータウイルスや、不正プログラム（マルウェア）、スパイウェアなどの総称として用いています。

フィッシング対策には最新版ガイドラインをご活用ください

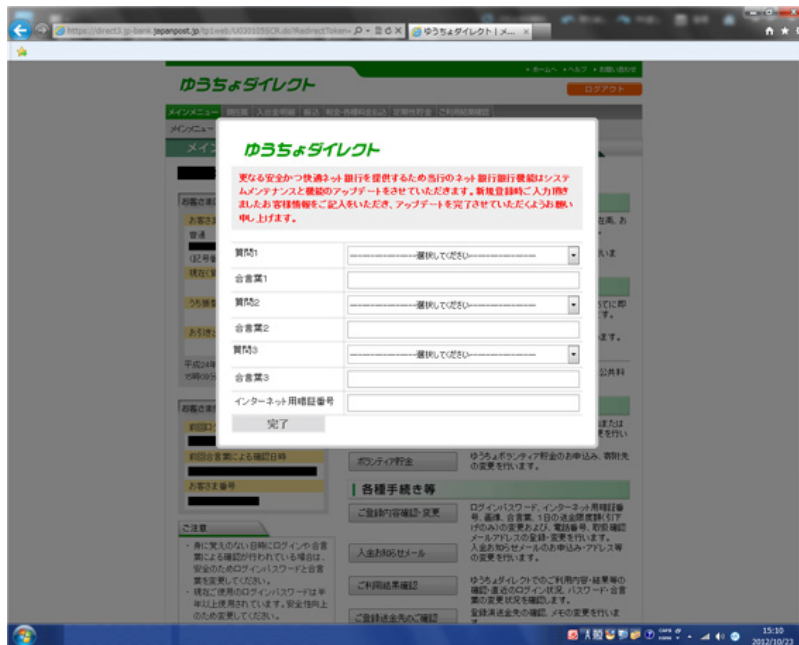


図2 不正なポップアップ画面イメージ（ゆうちょダイレクト）³

このようなウイルスはメールに添付されたり、ウェブサイト経由で感染を広げたりするだけでなく、無料ソフトウェアに混入され、ソフトウェアをインストールする際に、同時にインストールされてしまう場合も多いといわれています（有料ソフトウェアも汚染されていた事例が報告されています）。

³ゆうちょ銀行 Web サイト：【重要】不正にポップアップ画面を表示させてゆうちょダイレクトの情報を盗み取ろうとする犯罪にご注意ください
http://www.jp-bank.japanpost.jp/direct/pc/drnews/2012/drnews_id000041.html より

フィッシング対策には最新版ガイドラインをご活用ください



2. フィッシング対策3つの心得

フィッシング詐欺の被害は世界中で発生しており、年間の被害額は数千億円ともいわれられており、日本でも多数の被害が出ています。ここでは、フィッシング詐欺にあわないための3つの心得を示します。

心得1. 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。

心得2. 何が起こるか考える

フィッシング詐欺にひっかからないためには、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。

一般にフィッシング詐欺は、クレジット会社やネットショッピングサイトであるかのように、差出人を偽装、文面を工夫した電子メール等を被害者に送るつづけるところから始まります（餌を撒く）。この段階で疑いを持ち、信憑性を確認できれば被害を受けずにすませることができます。もし、電子メールを疑わずに、リンクをクリックしてしまった場合でも、重要な情報（ユーザID、パスワード、クレジットカード番号、金融口座番号、個人情報等）を入力後、送信ボタンを押す（釣り針にひっかかる）前に、「もしかして怪しい？」と感ずることができれば、ただちにブラウザを閉じて、被害を避けることができます。

心得3. 安心して楽しむ

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。

上記の心得を忘れずに、インターネットを楽しんでください。

フィッシング対策には最新版ガイドラインをご活用ください

3. 今すぐできるフィッシング対策

以降では、あやしいメールの見分け方、正しい URL にアクセスする、パソコンを安全に保つための方法、スマートフォンの正しいアプリのインストール方法、ひょっとして重要情報を盗まれたかもしれないと感じたときの事後対策に分けて、フィッシング対策を解説します。

3.1. 怪しいメールに注意しましょう

3.1.1 銀行やショッピングサイト等のサービス内容を確認しましょう

メールの差出人情報などは簡単に詐称ができ、差出人情報などを頼りにメールの真偽を見抜くことは不可能です。銀行やショッピングサイト等からどのようなタイミングで、どのようなメールが届くかを事前に理解し、それに当てはまらないものは全て怪しいと考えることが大切です。

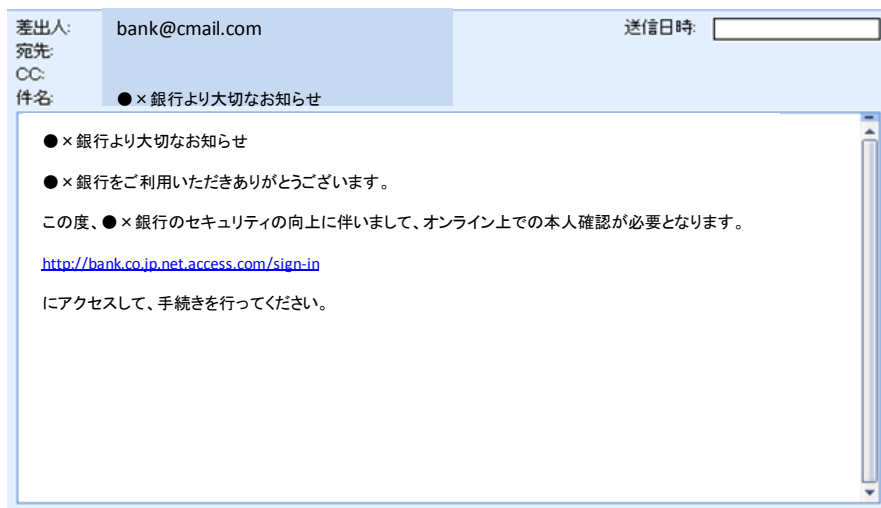


図 3 怪しいメールの例

たとえば、国内のある銀行ではウェブサイト上で、第二認証カードの番号全ての入力をもとめることはないとしています。また別の事業者ではメールにてパスワードの変更を依頼することはないとしています。このように各社のサービス内容を事前に確認しておくことで、本来あり得ない問い合わせを見抜くことが可能です。

フィッシング対策には最新版ガイドラインをご活用ください



3.1.2 電子署名の確認

銀行によっては電子メールに電子署名を付与してメールを送っています。その理由は電子署名を付けることにより、電子メールの送信元の確認と改ざんされていないことを確認することが出来るためです。多くの銀行は電子署名に S/MIME⁴という規格を採用しており、S/MIME を使用した電子署名付き電子メールは、メール本文と電子証明書に電子署名が付加され、添付ファイルとしてユーザに送信されます。ユーザは電子署名を確認することで、正規の事業者から送られているものや改ざんされていないことを確認することが可能ですので、必ず電子署名を確認するようにしましょう。

※S/MIME の確認にはメールソフトが対応している必要があります。

3.1.3 自動検知機能の活用

最近では、フィッシングメール、フィッシングサイトは人をだますために工夫をこらしているため、見破ることは難しくなっています。本ガイドラインでは、フィッシングメールであるかどうかの識別のため、迷惑メール同様、過去のフィッシングメール、フィッシングサイト情報から、一定の推測を自動的に行うツールを導入することを推奨します。ただし、ツールによる検知には限界がありますから、頼り切るのではなく、引き続き、自分自身で「怪しさ」に注意することを忘れないでください。

一般に利用されているウェブブラウザの多くにはフィッシングサイト検知機能が備わっています。ご利用のブラウザの設定を確認し、これらの機能が有効になっていることを確認してください。

また、似たような機能として、ユーザがアクセスしようとする URL をあらかじめ用意した URL のブラックリストと比較し、フィッシングサイトへのアクセスを遮断する機能を主要ブラウザ、各ウイルス対策ベンダ、インターネットサービス事業者などが提供しています。

このフィッシングアクセス遮断機能は、フィッシングサイトが停止するまでの期間のユーザ保護として有効だと考えられます。ユーザが被害に遭うリスクを低減させることを目的として、当協議会でも 2010 年 2 月 1 日よりヤフー株式会社の「Yahoo!ツールバー」を皮切りに、主要なフィルタリングソフトやウイルス対策ソフトなどにフィッシングサイト URL を提供しています。

※フィッシング対策協議会からフィッシングサイト情報を提供している事業者については

⁴ S/MIME は PKI を利用した電子証明書を用いる手法で、電子メールの暗号化や電子署名を行うことができます。

フィッシング対策には最新版ガイドラインをご活用ください



協議会の HP (<https://www.antiphishing.jp/enterprise/url.html>) をご覧ください。

3.2. 正しい URL にアクセスする

3.2.1 正しい URL を確認し、ブックマークに登録する

オンラインサービス初回利用時にはその URL を利用者カード/請求書などで確認し、直接入力してください。初回利用時にブラウザのブックマークに登録などすることで、以後入力を省くことが可能です。特にフィッシング詐欺被害が金銭面に及ぶ可能性の高い、クレジットカード会社、銀行、ショッピングサイト等について、ブックマークを活用するようにしてください。

3.2.2 電子メール中のリンクはクリックしない

やむを得ず、案内メールの本文中の URL リンクを利用する場合には、左クリック等による直接のアクセスではなく、図 4 に示すよう、URL リンクを右クリックし、ハイパーリンクをコピーして、ウェブブラウザのアドレスバーにペースト、文字列としてフィッシング詐欺で無いことを確認してからアクセスするように心がけてください。

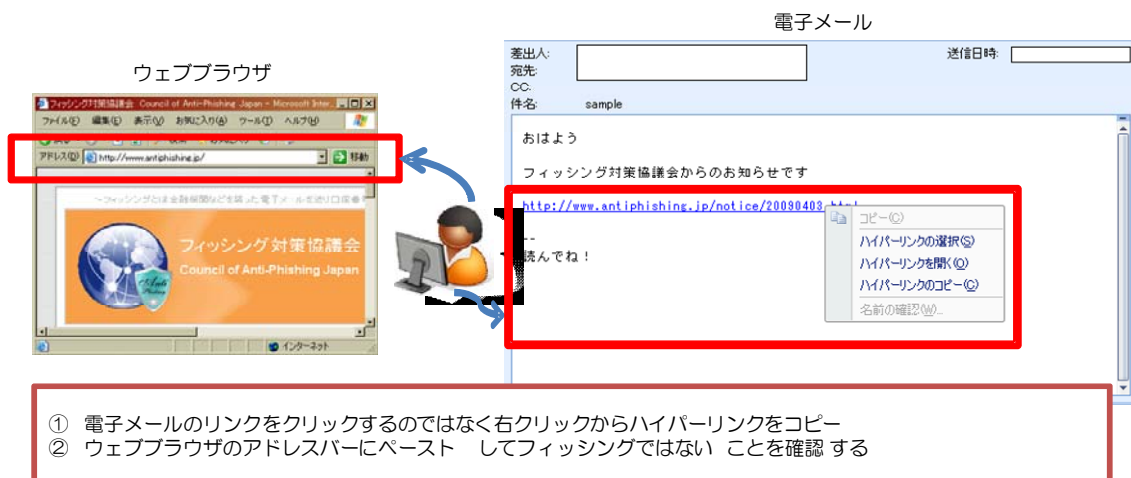


図 4 電子メール中の URL リンクにアクセスする場合の注意事項

なお、電子メールだけでなく、電子掲示板、ブログ、マイクロブログ（短い文章を書き込む形態のブログ）及び SNS⁵ サイト等でユーザが書き込んだ URL リンクについても、同様の配慮が必要です。

⁵ Social Network Service

フィッシング対策には最新版ガイドラインをご活用ください

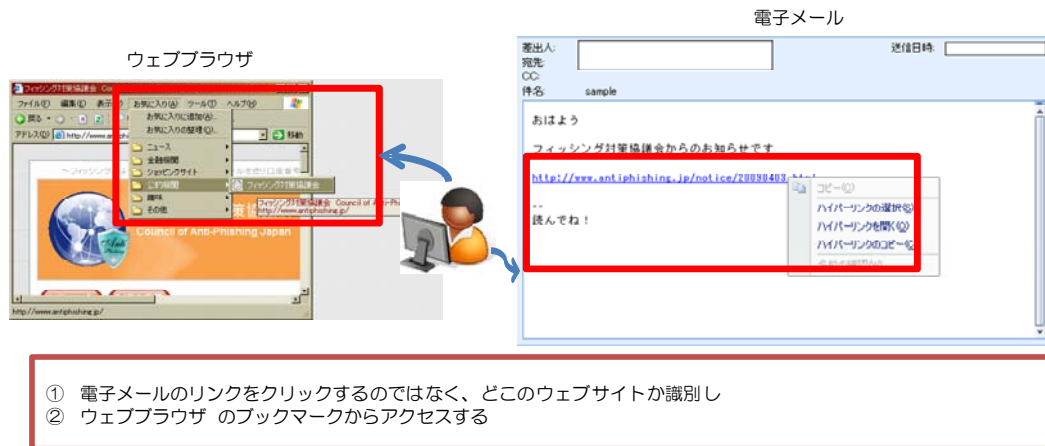


図 5 ウェブブラウザのブックマークの活用

3.2.1 錠前マークの確認

3.2.1 の補足となりますが、ウェブサイトへアクセスした際に、ブラウザ上で錠前のマークが表示されていれば、その通信は適切に暗号化されています。特にパスワードなどの入力の前には①正しい URL にアクセスしているか？ ②錠前マークが表示されているかの2点を確認してください。両者が確認された場合にのみ、入力をおこなってください。

なお、EV-SSL サーバ電子証明書が使われている場合には、電子証明書自体を確認しなくても、サイトの運営者がウェブブラウザのアドレスバー付近に表示されるため⁶、確認が確実かつ容易になるよう工夫されています。



図 6 EV-SSL サーバ電子証明書が使用されているサイトの例

⁶ https://www.verisign.co.jp/ssl/products/ev_ssl/browsers.html にて各ブラウザでの表示方式が一覧できる

フィッシング対策には最新版ガイドラインをご活用ください



3.3. パソコンを安全に保ちましょう

3.3.1 最新のセキュリティパッチの適用とウイルス対策

Windows などの OS やウェブブラウザ、アプリケーションソフトは、自動更新などにより最新の状態に保つことが重要です。さらに、ウイルス対策はフィッシング対策にもつながるとても大切なものです。ウイルス対策ソフトなどをインストールしましょう。ただし、ウイルス対策ソフトの過信は禁物です。発行元不明のソフトウェアはインストールしないなど、その他のセキュリティ対策を合わせて行いましょう。

ウイルス等が PC の設定を書き代えてしまったり、スパイウェアがコンピュータの情報を盗んだりしてしまうと、以降で説明する対策は意味がなくなってしまいます。

3.3.2 パスワードのしっかりとした管理

不正アクセス行為、ウイルス感染等の原因でウェブサイトからユーザのパスワードが漏えいする事件が現実には発生しています。ユーザ側の努力だけでは ID・パスワードが漏れてしまうリスクをゼロにすることはできないことから、一つのサイトからの漏えい被害が他のサイトのアカウントに影響を及ぼさないよう、利用するウェブサイト毎に ID・パスワードを別々にしておくべきです。例えば同じパスワードを SNS とインターネットバンキングで使いまわしていると、SNS からパスワードが漏れた場合、インターネットバンキングのアカウントも危険にさらされることになります。

上記の対策に加え、フィッシング詐欺に騙されてしまい、ID・パスワードを盗まれてしまった場合に備え、サイトにどのような情報を登録しているのか（特にクレジットカード情報など重要な情報について）、サイト登録時及び情報更新時に記録しておくといでしょう。フィッシング詐欺犯罪者は、奪ったパスワードでログインした後、正規ユーザを締め出すため、パスワードを変更してしまいます。こうなると、登録しておいた情報にアクセスできなくなるため、被害の大きさを測ることができなくなります。

3.4. 正しいアプリをつかう

スマートフォンを対象にしたフィッシングでは SNS やメールのなりすましだけではなく、インターネットバンキングアプリなどを装って不正なアプリをインストールさせ、そのアプリに入力した ID やパスワードが盗られるケースがあるため、スマートフォンではフィッシングサイトやメールだけではなくアプリにも気をつける必要があります。

この不正なアプリの多くは偽アプリケーションストアで配布されていることが確認されています。アプリをインストールする場合は正規のアプリケーションストア (iOS デバイ

フィッシング対策には最新版ガイドラインをご活用ください

スの場合は AppStore、Android の場合は GooglePlay や携帯キャリアが提供しているアプリケーションストア) からインストールするようにしましょう。

※正規のアプリケーションストアは事業者によって不正アプリかのチェックがされていますが、そのチェックをすり抜けてしまうアプリの中にはあります。セキュリティベンダから不正なアプリケーションのブラックリストを使ったアプリフィルタが提供されていますので、これらのサービスをつかうことでより安全に安心してアプリを使うことも可能です。

3.5. 間違っ重要情報を入力してしまったら

フィッシング詐欺被害を受けたことに気が付くタイミングとして考えられる状況は、正規サイトに重要情報を入力した際に不審な挙動が観られた（期待した手続き画面に進まなかった等）、正規サイトに ID/パスワードを入力したがエラーとなってログインできなかった（フィッシング詐欺犯罪者にパスワードを変更されていた）、クレジットカードの利用明細あるいは金融機関の通帳等に覚えのない取引が記載されていた（口座番号、暗唱番号等が詐取されていた）、オンラインゲームのキャラクターステータスが記憶に無い状況になっている（フィッシング詐欺犯罪者がアイテムを売買してしまった）等のケースが考えられます。

このような不審な現象が起きた場合には、被害を最小限に抑え、二次被害を防止するために、すみやかに関係機関等に報告・相談を行ってください。

詐取された情報に応じて関連する金融機関やクレジットカード会社、ショッピングサイト、プロバイダへ連絡を取り、当該アカウントの利用停止等の対応を依頼します。

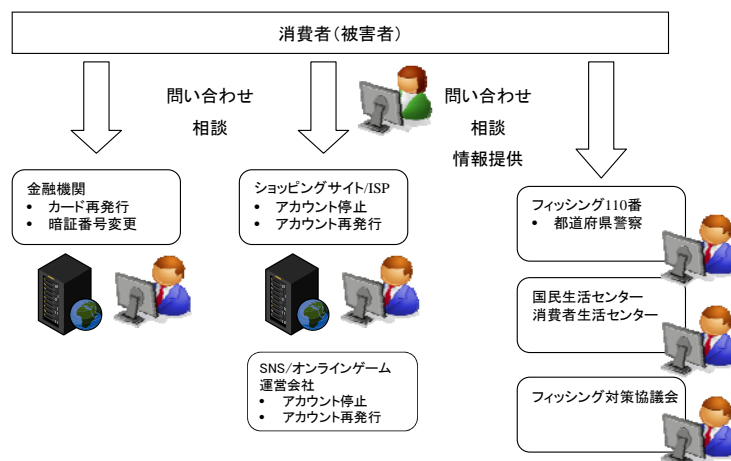


図7 フィッシング被害に遭ってしまった時の問い合わせ、相談、情報提供

フィッシング対策には最新版ガイドラインをご活用ください



(1) サービス事業者（連絡）

情報を詐取された疑いを持ったサービスを提供している事業者に、フィッシング詐欺被害の疑いがあることを伝え、指示によっては暗証番号の変更やカードの再発行、ショッピングサイトやプロバイダの ID 及びパスワードの変更を行います。

(2) 警察への連絡（相談）

金銭的な被害等、実質的な被害が確認された場合には、被害者の居住する地区の都道府県警察サイバー犯罪相談窓口（フィッシング 110 番）へ連絡して下さい。

フィッシング 110 番	http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm
--------------	---

(3) 国民生活センターまたは各地の消費生活センター（相談）

国民生活センターまたは各地の消費生活センターは消費生活全般に関する苦情や問合せなど、利用者からの相談を専門の相談員が受け付け、公正な立場で対応しています。

国民生活センター	http://www.kokusen.go.jp/
全国の消費生活センター	http://www.kokusen.go.jp/map/index.html

(4) 法テラス（相談）

法テラス（日本司法支援センター）は国によって設立された法的トラブル解決のための総合案内を行っています。フィッシング被害に関して、法的トラブルに巻き込まれた場合には、法テラスへ相談してください。

法テラス	http://www.houterasu.or.jp/
------	---

(5) フィッシング対策協議会（情報提供）

同様の被害拡大を防ぐため、フィッシング対策協議会へ情報提供してください。協議会では提供された情報を、事例調査や利用者への注意喚起のフィッシング対策協議会ホームページ掲載に活用するとともに、対策機関との連携に活用しています。

フィッシング対策協議会	https://www.antiphishing.jp/
電子メールアドレス	info@antiphishing.jp

フィッシング対策には最新版ガイドラインをご活用ください



4. フィッシング対策協議会と本ガイドラインの位置づけ

フィッシング対策協議会は平成 17 年 4 月に設置されました。フィッシング詐欺において騙られるサービス事業者を中心とした集まりとして、事例情報、技術情報の収集及び共有を中心に活動してまいりました。

当協議会では、利用者向け啓発教材として「STOP！フィッシング詐欺」を作成、提供してまいりましたが、近年においては、インターネットを利用したサービスも増え続けており、そういったサービスを利用する利用者がフィッシング詐欺の被害に合うという報道も後をたちません。その被害は金融機関やクレジットカード会社、SNS、オンラインゲーム、Web メールサービスなど多岐にわたります。平成 24 年に入っても、その傾向が引き続き見られることから、利用者側での対策を呼び掛けることが、フィッシング詐欺被害の拡大抑制に必要なとの認識に至り、「利用者向けのフィッシング詐欺対策」として、本ガイドラインを策定いたしました。

フィッシング詐欺被害のリスクを低減するため、「被害にあわないための 5 カ条⁷」に加え、本ガイドラインで提示する対策を実践してください。

なお、本ガイドライン中で、いくつかのセキュリティ対策ソフトウェア等を例示しておりますが、それらソフトウェアのインストール及び利用上の問題等については、ソフトウェアの開発・販売・配布元事業者にお問い合わせくださるようお願いいたします。

⁷ https://www.antiphishing.jp/stop_phishing/gokajou.html

フィッシング対策には最新版ガイドラインをご活用ください



5. 付録：フィッシング事例

現在、日本で確認されている主要なフィッシング事例を紹介します。

2009 年以降、日本人を狙ったと思われるフィッシング詐欺が増加しています。以前は英語で書かれたフィッシングサイトがほとんどでしたが、日本人を狙ったフィッシングの場合、サイトは日本語で書かれており、サイトへ誘導するメールの文面も日本語で書かれているものがほとんどです。また、以前は銀行のインターネットバンキングを狙ったフィッシングサイトがほとんどでしたが、最近ですと、SNS やオンラインゲーム、Web メールアカウントを詐取するフィッシングを確認しています。

フィッシング対策には最新版ガイドラインをご活用ください

(ア) クレジットカードをかたるフィッシング

2009 年後半より大手クレジットカード会社をかたるフィッシングサイトを確認しています。フィッシングサイトの多数は英語表記のフィッシングサイトですが、図は日本語表記の MasterCard をかたるフィッシング事例です。MasterCard のフィッシングの多くの場合、メールは英語表記ですが、フィッシングサイトは日本語表記になっています。

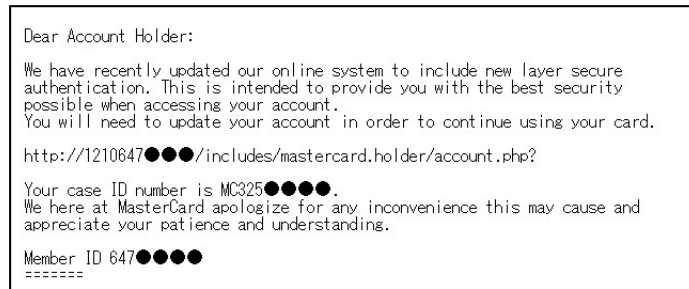
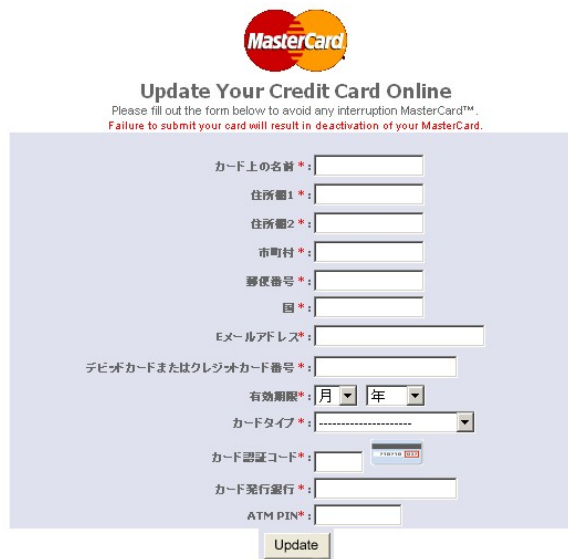



図 8 Mastercard をかたるフィッシングメール





Update Your Credit Card Online

Please fill out the form below to avoid any interruption MasterCard™.
Failure to submit your card will result in deactivation of your MasterCard.

カード上の名前*:

住所欄1*:

住所欄2*:

市町村*:

郵便番号*:

国*:

Eメールアドレス*:

デビオカードまたはクレジットカード番号*:

有効期限*: 月 年

カードタイプ*:

カード認証コード*:

カード発行銀行*:

ATM PIN*:

図 9 Mastercard をかたるフィッシングサイト

フィッシング対策には最新版ガイドラインをご活用ください



(イ) 銀行をかたるフィッシング

2012年より国内の銀行をかたり、乱数表や第二暗証番号などの第二認証情報を詐取するフィッシングが増加しています。銀行から乱数表や第二暗証番号などの全ての入力を求めることはありませんので、第二暗証情報の「全て」の情報を入力する画面が表示された場合には、絶対に情報を入力しないようにしてください。

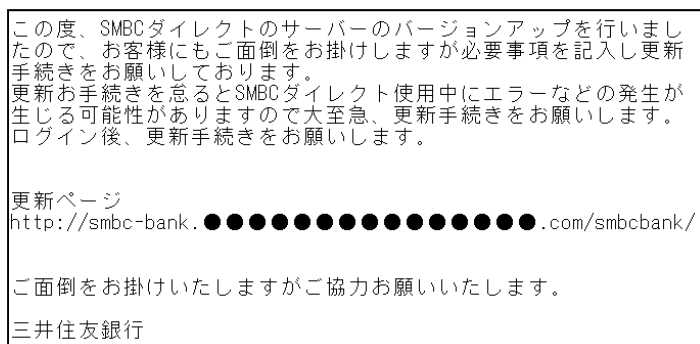


図10 三井住友銀行をかたるフィッシングメール



図11 三井住友銀行をかたるフィッシングサイト

フィッシング対策には最新版ガイドラインをご活用ください



(ウ) オンラインゲームをかたるフィッシング

オンラインゲームをかたるフィッシングの目的は様々な理由が考えられる。詐取したアカウント情報を売買するケースもあるが、多くの場合、アカウントが所持しているレアアイテムの詐取を目的にしています。

◆既に報道されておりますが、オンラインサービスを提供している他社において 数千万件規模でID、パスワードやクレジット情報などの会員情報が不正アクセスの影響により 流失したとの情報を確認いたしました。
◆本人確認のための認証メールを送信いたします。メールを受信して、記載されているURLをクリックしてください。 :

```
<http://megatenonline.com.●●●●●●●●.in/>http://www.megatenonline.com/beginner/index2.html
```

図 12 真女神転生 IMAGINE をかたるフィッシングメール

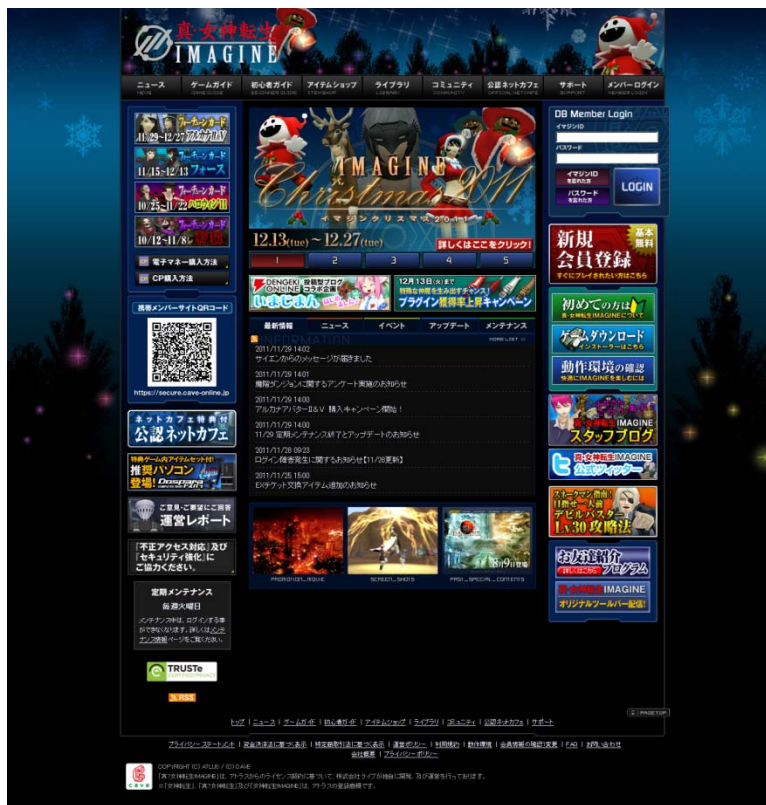


図 13 真女神転生 IMAGINE をかたるフィッシングサイト

フィッシング対策には最新版ガイドラインをご活用ください

(エ) SNS をかたるフィッシング

SNS は比較的閉じたコミュニティであるため、詐取されたアカウントを悪用された場合、会員同士が既に友達であることの信頼を逆手にとり、ソーシャルエンジニアリングなどの手法を用いて、個人情報の窃取や悪意あるサイトへの誘導に使用される可能性が高いです。



図 14 アメーバ (Ameba) をかたるフィッシングサイト

フィッシング対策には最新版ガイドラインをご活用ください

(オ) プロバイダをかたるフィッシング

複数のプロバイダのメールアドレスを詐取するフィッシングサイトを確認しています。アカウント情報を詐取されると、なりすましメールを送られてたり、SPAMメールの送信元として、使用される可能性があります。



図 15 OCNをかたるフィッシングサイト