※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

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

消費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

2012 年 12 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

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

目次

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

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、あなたのオンライン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。

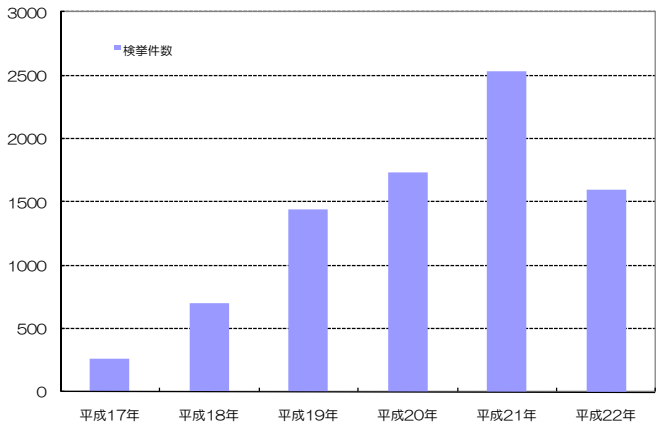

図 1　ID 窃盗型不正アクセス行為の検挙件数[2]

[1]2012 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。
[2]「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/20110303004/20110303004.pdf　より三菱総合研究所作成

国家公安委員会・総務省・経済産業省の発表によれば、フィッシングを含む ID を窃盗する手法を用いた不正アクセスの件数は数年前から急増しています（図 1）。このような不正アクセスの中でも、特にフィッシングを用いたものが急増しています。

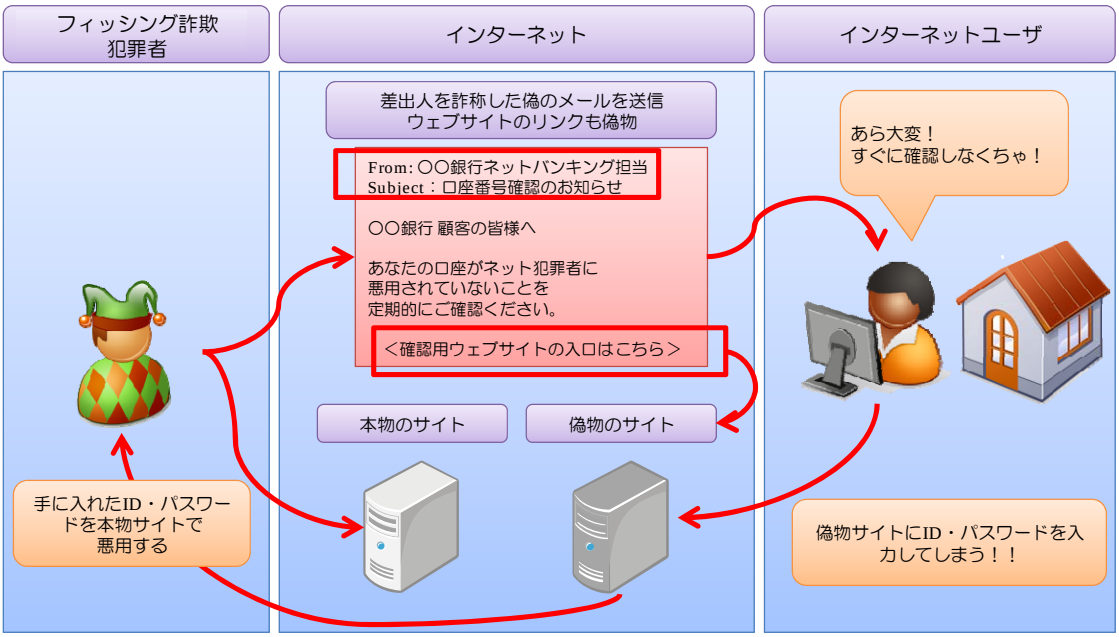

図 2 典型的な「フィッシング詐欺」行為

※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 ～フィッシングだけではありません～

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[3]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

[3] 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。

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 3）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。

図 3 不正なポップアップ画面イメージ（ゆうちょダイレクト）[4]

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）。

1.1.2 電話によるフィッシング： ビッシング（Vishing）

ビッシングとは、適当に電話をかけて応答した相手に「〇〇銀行の△△ですが、お客様の口座取引の調査をしております。」などと、音声により相手をだまして個人情報を引き出

[4]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

そうとする行為です。音声は英語で「Voice」、つまり音声によるフィッシング詐欺ということで「Voice + Phishing = Vishing」と名付けられたとされています。

現実のビッシング事例では、人間のオペレータが応答するのではなく、機械応答システムを用いることで、低コストに大量の不正行為を実行しているとのことです。

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？」と感じることができれば、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。

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、パソコンを安全に保つための方法、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贋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。

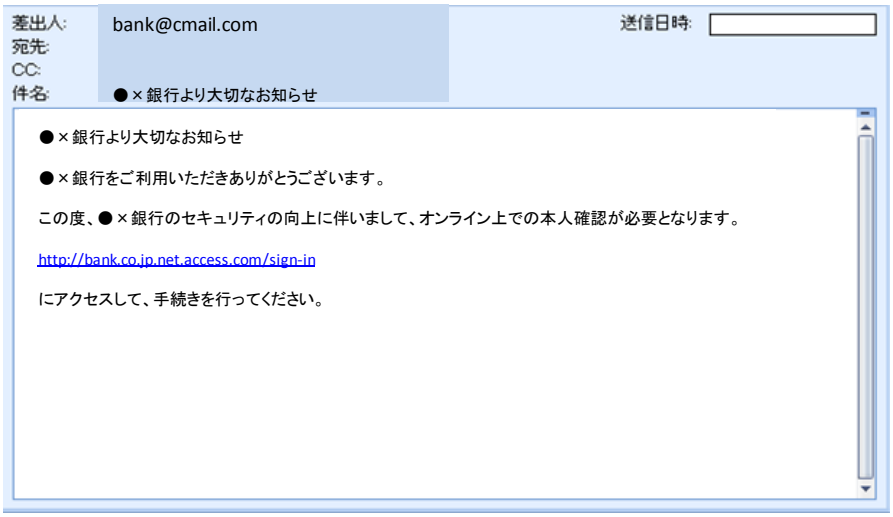

図 4　怪しいメールの例

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。

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/MIME[5]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

[5] 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。

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 3 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。

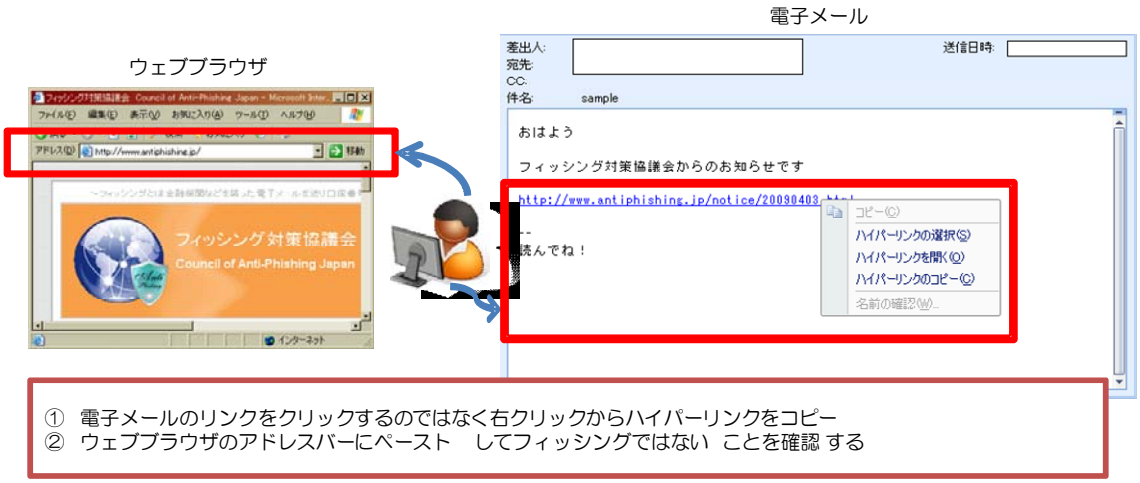

図 5 電子メール中の URL リンクにアクセスする場合の注意事項

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 SNS[6]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。

[6] Social Network Service

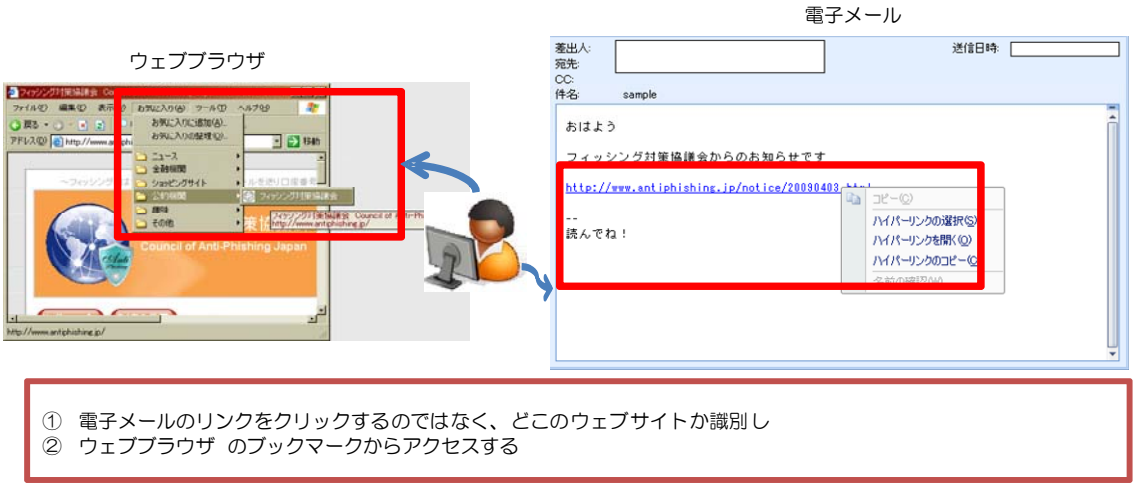

図 6　ウェブブラウザのブックマークの活用

3.2.1　鍵マークの確認

3.2.1 の補足となりますが、ウェブサイトにアクセスした際に、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鍵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[7]、確認が確実かつ容易になるよう工夫されています。

[7] 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

図 7 EV-SSL サーバ電子証明書が使用されているサイトの例

3.3. パソコンを安全に保ちましょう

3.3.1 ウイルス対策

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。また、ウイルス対策ソフトはもちろん、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ってください。

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 とオンライン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、オンライン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よいでしょう。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. 間違って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。

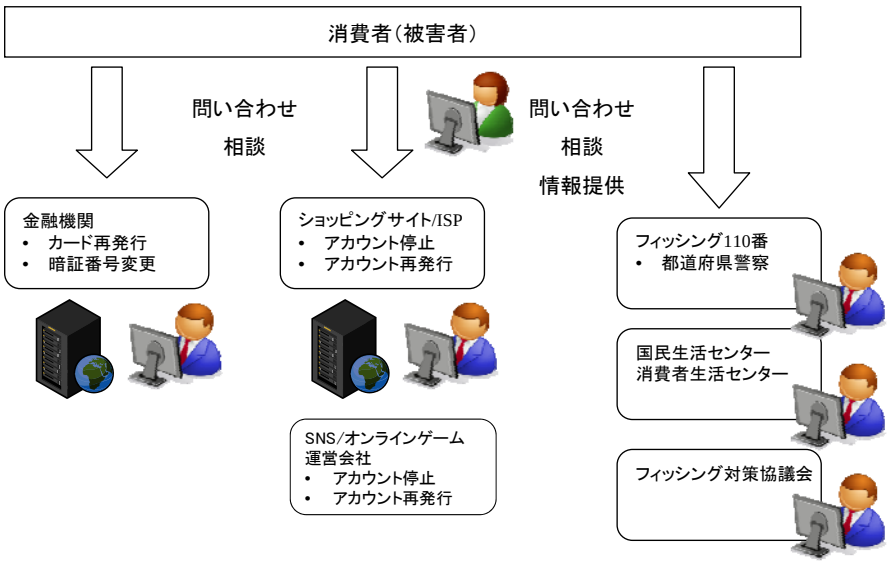

図 8 フィッシング被害に遭ってしまった時の問い合わせ、相談、情報提供

（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、消費者からの相談を専門の相談員が受付け、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、事例調査や消費者への注意喚起のフィ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	http://www.antiphishing.jp/
電子メールアドレス	info@antiphishing.jp

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。

従来から、消費者向け啓発教材として「STOP！フィッシング詐欺[8]」を作成、提供してまいりましたが、平成 19 年から平成 20 年にかけて、日本におけるフィッシング詐欺被害について増加傾向が見られるようになり、平成 21 年に入っても、その傾向が引き続き見られることから、サービス事業者側のフィッシング詐欺対策だけでなく、消費者側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との認識に至り、平成 20 年策定のサービス事業者を主な対象とした「フィッシング対策ガイドライン」に続き、消費者を主な対象としたフィッシング対策ガイドラインとして、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[9]」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。

[8] http://www.antiphishing.jp/stop_phishing/
[9] http://www.antiphishing.jp/stop_phishing/gokajou.html