※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

利用者向けフィッシング詐欺対策ガイドライン

2018 年度版

2018 年 3 月

フィッシング対策協議会

https://www.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

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

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 Web 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。

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。

被害にあ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こと（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。

[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。

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。

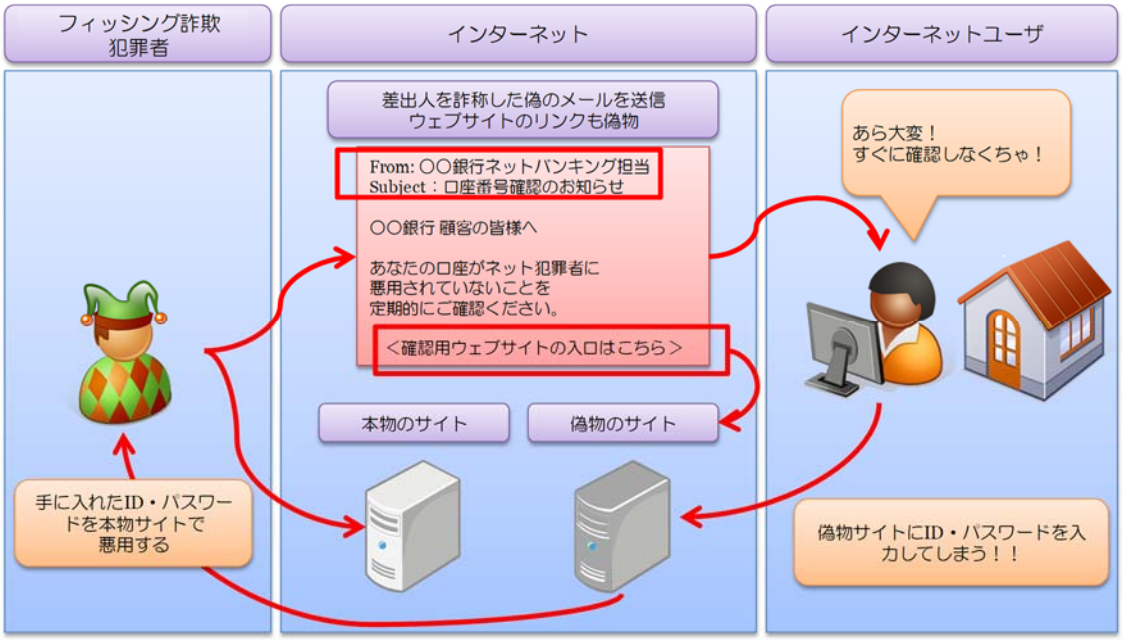


図 1 典型的な「フィッシング詐欺」行為

※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[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。

[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（マルウエア）、スパイウエアなどの総称として用いています。

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（ワンタイムパスワード等）を入力させる偽画面（図 2）を自動で表示し、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 2 偽画面の例（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、Web サイト経由で感染を広げたりするだけでなく、無料ソフトウエアに混入され、ソフトウエ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（有料ソフトウエ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：ゆうちょダイレクトを狙った犯罪にご注意ください
http://www.jp-bank.japanpost.jp/crime/crm_direct.html
より

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（STOP. THINK. CONNECT.）を示します。STOP. THINK. CONNECT.は、全世界共通のサイバーセキュリティキャンペーン（http://stopthinkconnect.jp/）です。

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、これからと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など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、ウイルスに感染させられたり、偽の入力フォームに個人情報を入力させられるなどにより重要な情報（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、個人情報など）を盗まれる可能性があります。リンクをクリックする前に、「もしかして怪しい？」と感じることができれば、被害を避けることができます。

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。

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、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など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など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。電子メールだけでなく、SNS（Social Networking Service）や SMS（Short Message Service）による連絡においても同様です。


こんにちは！
最近、利用者の個人情報が一部のネットショップサーバーに不正取得され、利用者の個人情報漏洩事件が起こりました。
お客様のアカウントの安全性を保つために、「じぶん銀行システム」がアップグレードされましたが、お客様はアカウントが凍結されないように直ちにご登録のうえご確認ください。

以下のページより登録を続けてください。

https://bk02.jibunbank.co.jp/ibretail/RetailLogin.html?2014091300
<http://www.●●●●.com/images/i/>

――CopyrighkTcV¥ivVoWe55116327VMiPZZUBNmBLFkQvaCopyright Jibun Bank Corporation. All rights reserved.

図 3　怪しいメールの例[4]

例えば、国内のある銀行では Web 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。

[4] https://www.antiphishing.jp/news/alert/jibunbank_20160119.html

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、怪しいメールが届いた際には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。

3.2. 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などについて、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

電子メール中のリンクはクリックすると危ないサイトに行く可能性があるため、安易にクリックしないでください。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、左クリックなど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、Web 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。

[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。

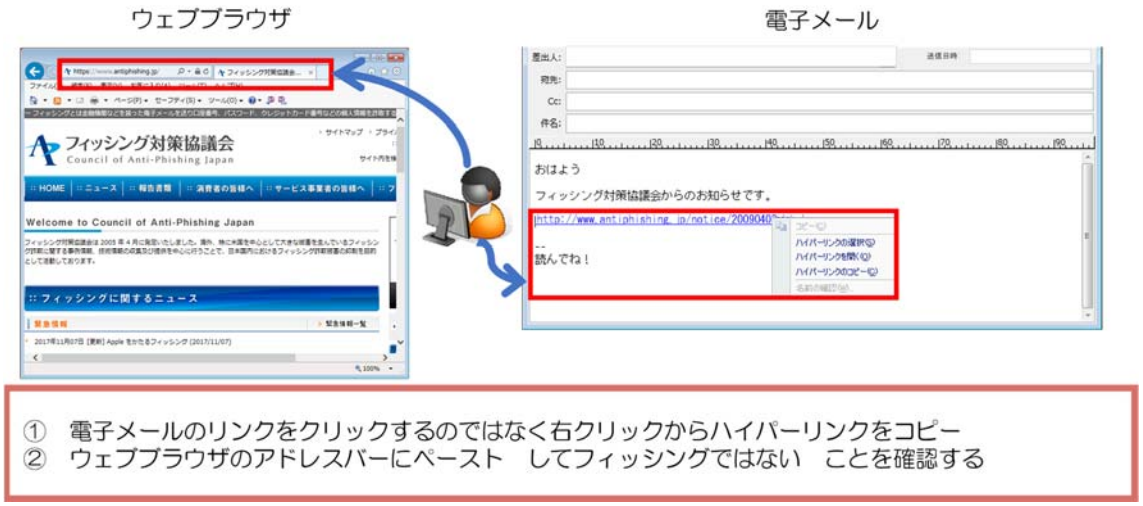


図 4　電子メール中の URL リンクにアクセスする場合の注意事項

なお、電子メールだけでなく、電子掲示板、ブログおよび SNS サイトなど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。

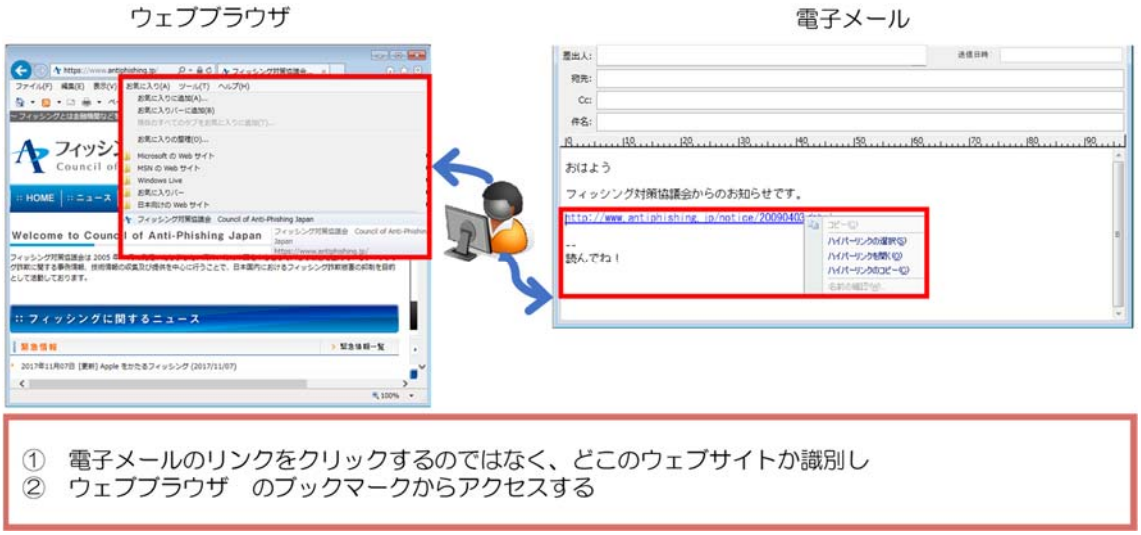


図 5　Web ブラウザのブックマークの活用

3.2.1　錠前マークの確認

3.2.1 の補足となりますが、Web 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、入力を行ってください。

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 Web ブラウザのアドレスバー付近に表示されるため、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

3.2.2 モバイル端末向けの注意事項

スマートフォン等のモバイル端末の場合、ブラウザ上で URL が一部しか表示されないなど、URL の確認が難しい場合がある。初回にアクセスする際は、トップレベルドメイン（.jp や.com 等）が正しいか等の手段を併用することで確認するようにしてください。

3.3. パソコンやモバイル端末を安全に保ちましょう

3.3.1 ソフトウエアを最新の状態にする

パソコンにセキュリティ上の脆弱性があると、利用者が気づくことなくマルウエアへの感染や脆弱性を利用した攻撃を受けることになります。最新の OS やアプリケーションには自動的に最新のセキュリティパッチを適用する機能が備えられていることが多いので、できるだけその機能を有効にし、最新のセキュリティパッチが確実に適用された状態でパソ

コンを利用することが重要です。

また、セキュリティのサポートがされなくなった古いパソコンの基本ソフト（OS）（例：Windows XP など）の使用はやめて、新しい基本ソフト（OS）を使いましょう。

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、ウイルス感染などの原因で Web 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 Web 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。パスワード管理についての考え方は、フィッシング対策協議会の「フィッシングレポート 2015」で詳しく紹介しています。

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）、サイト登録時およ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. 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 デバイスの場合は App Store、Android の場合は Google Play 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も中にはあります。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。

Windows の場合、ソフトウエアを実行・インストールしようとする際に「発行元を確認できませんでした」「PC が保護されました」などという以下のようなダイアログが表示される場合があります。信用できるアプリケーションをインストールする場合に限って「実行」「はい」等を選択するようにしてください。

図 7 ソフトウエアのインストール時に表示されるダイアログの例[6]

正規アプリをかたった不正なアプリだけではなく、非公認アプリによる ID やパスワードが窃取される事件が発生しています。非公認アプリとはサービス事業者が提供するアプリよりも便利な機能を提供するなどにより、広く使われている場合もありますが、悪意のある第三者が作成した非公認アプリの中には、ID やパスワードを含む個人情報を盗むものがあることに注意してください。

また、スマートフォンのアプリには「3.2.正しい URL にアクセスする」で示したような URL の確認と錠前マークの確認が出来ないものが多くあります。したがって、PC の場合よりも、信頼できるアプリやサービスの選択がより重要となります。

3.5. 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みられた（期待した手続き画面に進まなかったなど）、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などに覚えのない取引が記載されていた（口座番号、暗唱番号などが詐取されていた）、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）などのケースが考え

[6] 出典：Microsoft

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などに報告・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などの対応を依頼します。

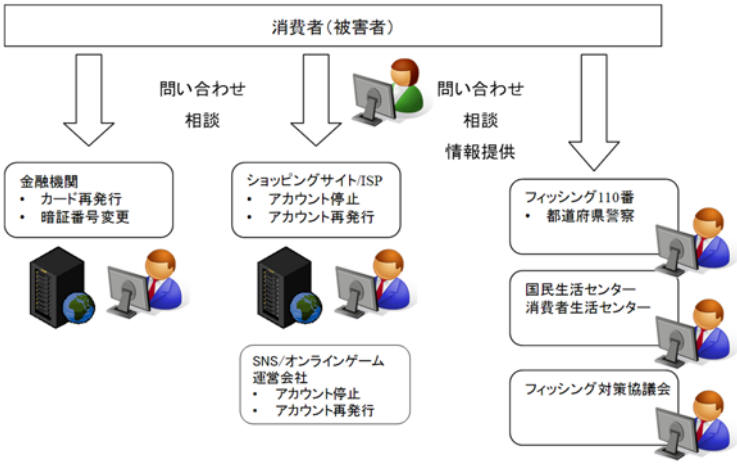


図 8 フィッシング被害に遭ってしまった時の問い合わせ、相談、情報提供

（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 およびパスワードの変更を行います。

（2） 警察への連絡（相談）

金銭的な被害など、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）へ連絡してください。

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い合わせなど、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

また、フィッシングではなく、なりすまし EC サイト（偽サイト）で被害を受けた場合には、「なりすまし EC サイト対策協議会」（https://www.saferinternet.or.jp/narisumashi/）に相談しましょう。

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 2005 年 4 月に設置されました。フィッシング詐欺においてかた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、技術情報の収集およ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遭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。2012 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、「マンガでわかる フィッシング詐欺対策 5 ヶ条[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エアなどを例示しておりますが、それらソフトウエアのインストールおよび利用上の問題などについては、ソフトウエアの開発・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/phishing-5articles.html

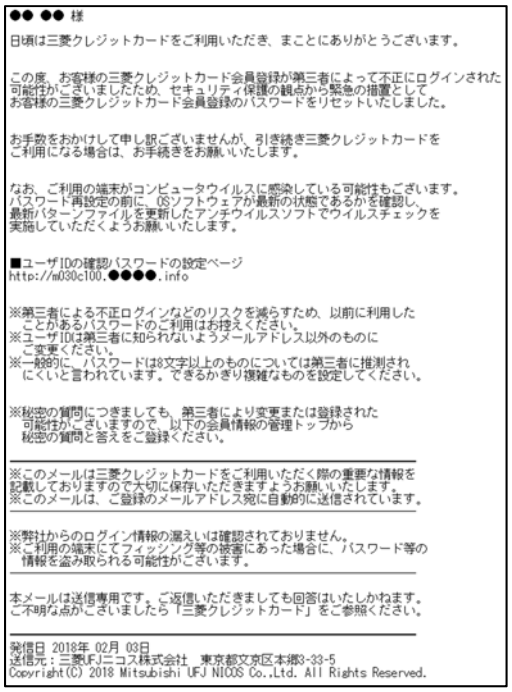
5. 付録：フィッシング事例

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。

日本人を狙ったと思われるフィッシング詐欺が激増しています。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。

(ア)　　クレジットカードをかたるフィッシング

　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。図は三菱 UFJ ニコスをかたるフィッシング事例です。この三菱 UFJ ニコスのフィッシングの多くの場合、カード会員向けの利用明細確認等のサービスページをかたったサイトに誘導します。



●● ●● 様

日頃は三菱クレジットカードをご利用いただき、まことにありがとうございます。

この度、お客様の三菱クレジットカード会員登録が第三者によって不正にログインされた可能性がございましたため、セキュリティ保護の観点から緊急の措置として
お客様の三菱クレジットカード会員登録のパスワードをリセットいたしました。

お手数をおかけして申し訳ございませんが、引き続き三菱クレジットカードをご利用になる場合は、お手続きをお願いいたします。

なお、ご利用の端末がコンピュータウイルスに感染している可能性もございます。
パスワード再設定の前に、(1)ソフトウェアが最新の状態であるかを確認し、
最新パターンファイルを更新したアンチウイルスソフトでウイルスチェックを
実施していただくようお願いいたします。

■ユーザIDの確認パスワードの設定ページ
http://m030c100.●●●●.info

※第三者による不正ログインなどのリスクを減らすため、以前に利用したことがあるパスワードのご利用はお控えください。
※ユーザIDは第三者に知られないようメールアドレス以外のものにご変更ください。
※一般的に、パスワードは8文字以上のものについては第三者に推測されにくいと言われています。できるかぎり複雑なものを設定してください。

※秘密の質問につきましても、第三者により変更または登録された可能性がございますので、以下の会員情報の管理トップから秘密の質問と答えをご登録ください。

※このメールは三菱クレジットカードをご利用いただく際の重要な情報を記載しておりますので大切に保存いただきますようお願いいたします。
※このメールは、ご登録のメールアドレス宛に自動的に送信されています。

※弊社からのログイン情報の漏えいは確認されておりません。
※ご利用の端末にてフィッシング等の被害にあった場合に、パスワード等の情報を盗み取られる可能性がございます。

本メールは送信専用です。ご返信いただきましても回答はいたしかねます。
ご不明な点がございましたら「三菱クレジットカード」をご参照ください。

発信日 2018年 02月 03日
送信元：三菱UFJニコス株式会社　東京都文京区本郷3-33-5
Copyright(C) 2018 Mitsubishi UFJ NICOS Co.,Ltd. All Rights Reserved.

図 9　三菱 UFJ ニコスをかたるフィッシングメール

図 10　三菱 UFJ ニコスをかたるフィッシングサイト

(イ)　　仮想通貨取引所をかたるフィッシング

国内の仮想通貨取引所をかたり、ログイン ID やパスワードなどを不正に詐取するフィッシングが見つかっています。国内の取引所ではログイン ID とパスワードだけでは別の口座に送金することはできませんが、国外の取引所ではメールアドレスとパスワードだけでアカウントが作成でき、送金可能な取引所もありますので、絶対に情報を入力しないようにしてください。


こんにちは！

「bitFlyer」のシステムが安全性の更新がされたため、お客様はアカウントが凍結?休眠されないように、直ちにアカウントをご認証ください。

以下のページより登録を続けてください。

https://bitflyer.jp/login/ <http://bitflyer.jp.login.●●●●.xyz/login/>

――Copyright (c) Copyright 2017 bitFlyer, Inc. All Rights Reserved――

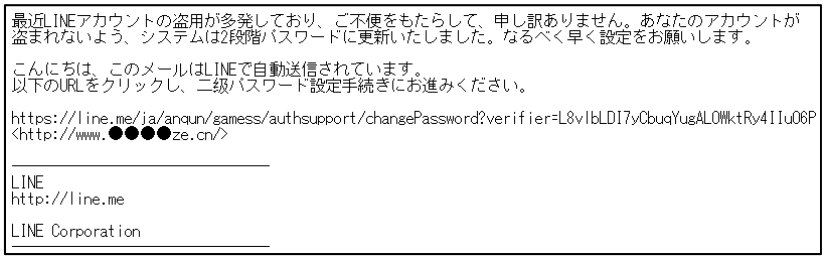
図 11 bitFlyer をかたるフィッシングメール

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

図 12 bitFlyer をかたるフィッシングサイト

(ウ)　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、会員同士がすで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。また、友人をかたり、プリペイドカードを購入させるなどの金銭的被害が発生しています。


最近LINEアカウントの盗用が多発しており、ご不便をもたらして、申し訳ありません。あなたのアカウントが盗まれないよう、システムは2段階パスワードに更新いたしました。なるべく早く設定をお願いします。

こんにちは、このメールはLINEで自動送信されています。
以下のURLをクリックし、二級パスワード設定手続きにお進みください。

https://line.me/ja/anqun/gamess/authsupport/changePassword?verifier=L8vlbLDI7yCbuqYugALOMktRy4IIuO6P
<http://www.●●●●ze.cn/>

LINE
http://line.me

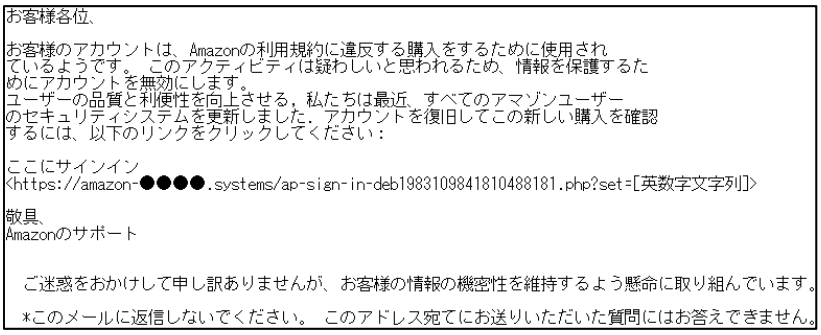
LINE Corporation

図 13 LINE をかたるフィッシングメール

図 14 LINE をかたるフィッシングサイト

(エ)　ショッピングサイトをかたるフィッシング

ショッピングサイトをかたるフィッシングサイトにて、アカウント情報およびクレジットカード情報などを詐取するフィッシングサイトを確認しています。情報を詐取されると、クレジットカードが不正に使用され、金銭的な被害が発生する可能性があります。


お客様各位、

お客様のアカウントは、Amazonの利用規約に違反する購入をするために使用されているようです。 このアクティビティは疑わしいと思われるため、情報を保護するためにアカウントを無効にします。
ユーザーの品質と利便性を向上させる，私たちは最近、すべてのアマゾンユーザーのセキュリティシステムを更新しました．アカウントを復旧してこの新しい購入を確認するには、以下のリンクをクリックしてください：

ここにサインイン
<https://amazon-●●●●.systems/ap-sign-in-deb1983109841810488181.php?set=[英数字文字列]>

敬具、
Amazonのサポート

ご迷惑をおかけして申し訳ありませんが、お客様の情報の機密性を維持するよう懸命に取り組んでいます。

*このメールに返信しないでください。 このアドレス宛てにお送りいただいた質問にはお答えできません。

図 15 Amazon をかたるフィッシングメール

図 16　Amazon をかたるフィッシングサイト