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

2019 年度版

2019 年 5 月

フィッシング対策協議会

https://www.antiphishing.jp/

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～ 2
2. フィッシング対策３つの心得 4
3. 今すぐできるフィッシング対策 5
3.1. 怪しいメールに注意しましょう 5
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 5
3.1.2 電子署名の確認 6
3.2. 正しい URL にアクセスする 6
3.2.1 正しい URL を確認し、ブックマークに登録する 6
3.2.2 電子メール中のリンクはクリックしない 6
3.2.3 本来の Web サイトであるかどうかを確認する 7
3.2.4 モバイル端末向けの注意事項 9
3.3. パソコンやモバイル端末を安全に保ちましょう 10
3.3.1 ソフトウエアを最新の状態にする 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 12
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 14
5. 付録：フィッシング事例 15
5. 付録 2：パスワードの考え方 （「フィッシングレポート 2015」より） 21

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、本ガイドラインでは次のように定義しています。

> フィッシング（Phishing）とは、実在する組織を騙って、ユーザネーム、パスワード、アカウント ID、ATM の暗証番号、クレジットカード番号といった個人情報を詐取すること。

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。

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。

[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。

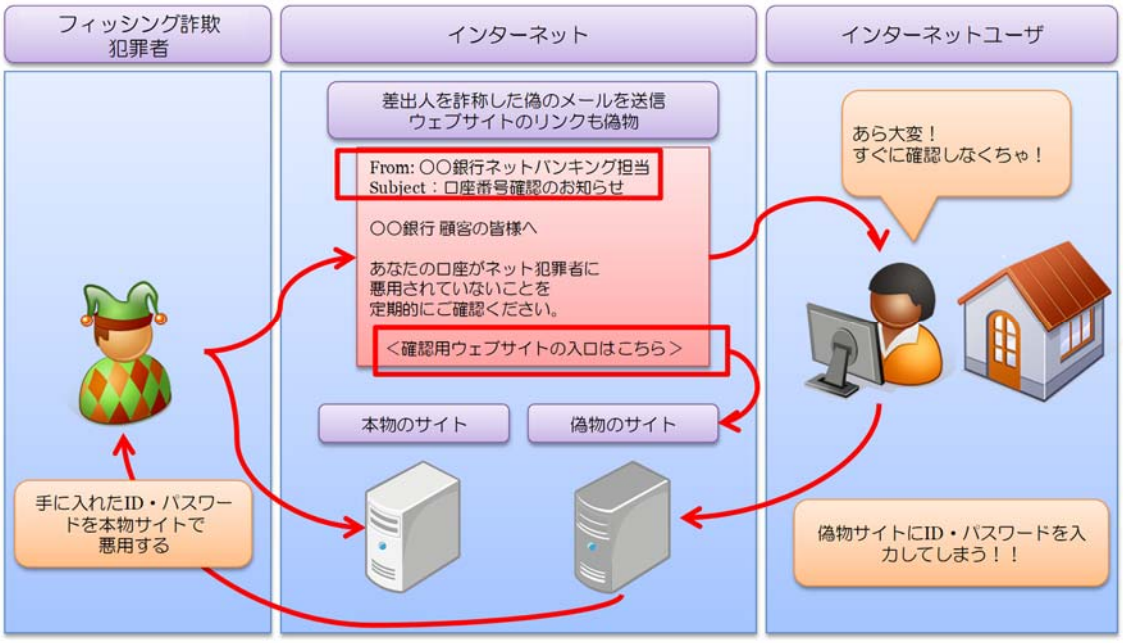


図 1　典型的な「フィッシング詐欺」行為

※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。

- 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。

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

[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。

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
https://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（https://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/>

――CopyrighkTc¥¥ivVoWe55116327¥MiPZZUBNmBLFkQvaCopyright 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。

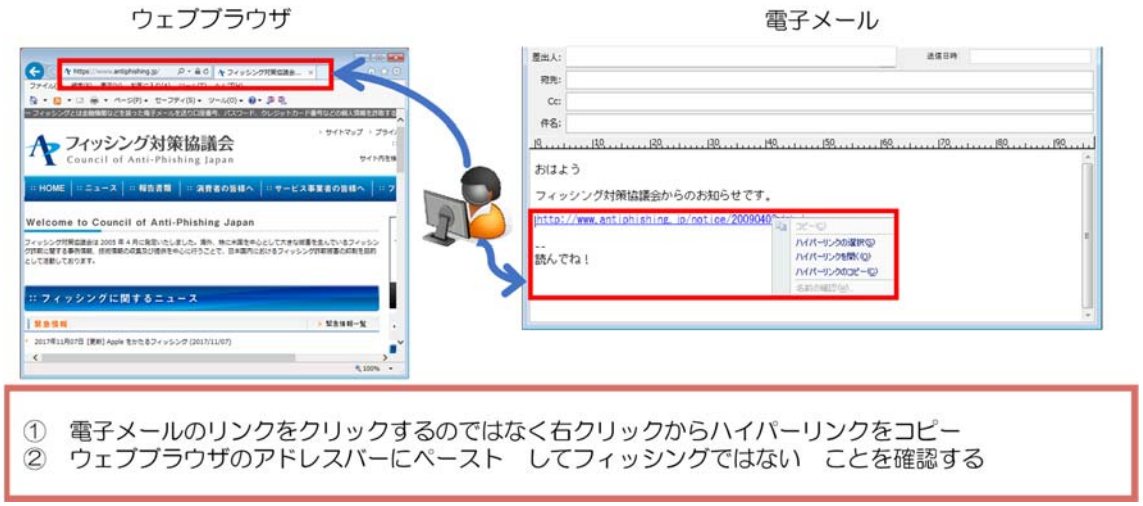


図 4　電子メール中の URL リンクにアクセスする場合の注意事項

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。

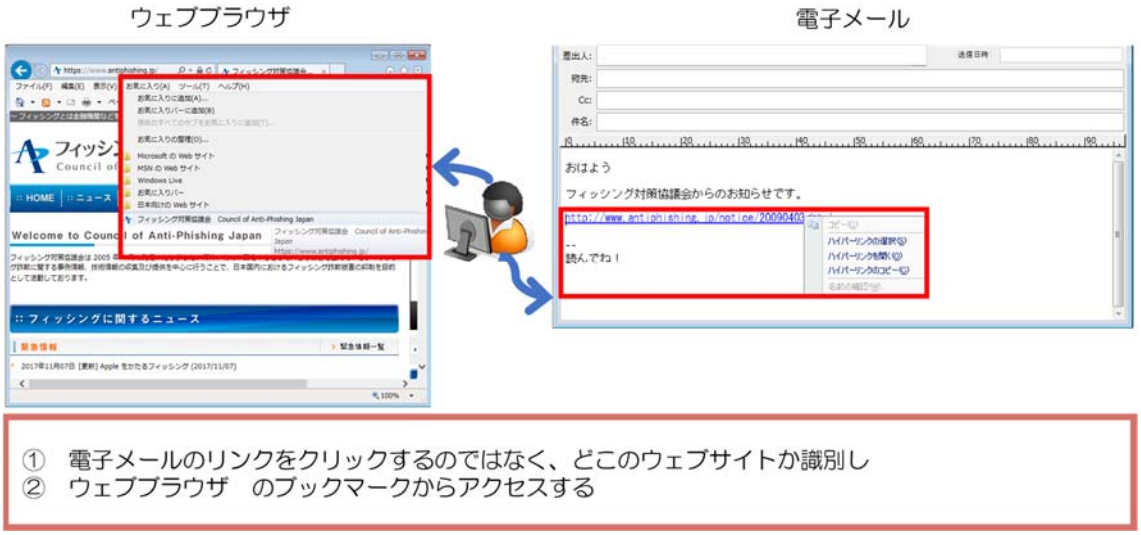


図 5　Web ブラウザのブックマークの活用

3.2.3　本来の Web サイトであるかどうかを確認する

パソコンやスマートフォンで Web サイトにアクセスしているとき、その Web サイトが本来アクセスしようとしている Web サイトなのか、それとも見た目がそっくりに作られてい

るだけの偽の Web サイトなのかを見分ける事が重要です。

最近はパソコンやスマートフォンの Web サイトに関する表示の方法が様々になっていて、下記のどれか一つを確認すれば、間違いないとは言いにくくなっています。必ず複数の方法を使って確認しましょう

本来の Web サイトであるかどうかを確認する方法：

〇ドメイン名が正しいかどうかを確認する

Web サイトの上部に表示されている URL のドメイン名を確認します。ドメイン名は「https://（ドメイン名）/」もしくは「(鍵マーク) (ドメイン名)」のように表示されます。ドメイン名が分かっている場合には、一致しているかどうかを確認します。ドメイン名の末尾が .jp や .com などのように、予め自分自身が知っているもので終わっているかどうかを確認する方法もあります。

〇鍵マークが表示されているかどうかを確認する

通信が暗号化される HTTPS でアクセスしている場合には、鍵マークが表示されます。最近、鍵マークが表示されるフィッシングサイトが増えています。鍵マークだけで安心せず、同時に他の方法を確認しましょう。

〇EV 証明書の表示（アドレスバーが緑色になるなど）や組織名を確認する

HTTPS でアクセスしており、更に Web サイトのサーバ証明書が EV（エクステンデド・バリデーション）証明書である場合には、URL の背景が色付きで表示されることがあります。その色は多くの Web ブラウザでは緑色ですが、緑色になるかどうかは使っている Web ブラウザやスマートフォン（の Web ブラウザ）によって異なります。

また EV 証明書の場合、URL の隣や URL が表示されるところに Web サイトを運営している会社などの組織の名称が表示されます。その名称が、アクセスしようとしていた Web サイトの会社などの組織名と一緒になっている事を確認します。色や組織名の表示方法は、使っているブラウザやスマートフォンによって異なります。通常、どのように表示されるのかを確認しておきましょう。

Web サイトが正しいかどうかの確認ができないときには、利用を止めます。特に、銀行、オンラインショッピング、オンラインの電子申請の Web サイトにアクセスするときには注意が必要です。

どうしても利用したい時や、初めてアクセスする Web サイトであって、偽サイトかどうかが分かりにくい場合には、URL がフィッシングサイトのものでないかどうかを調べる事が考えられます。その方法として、そのサービスを提供している事業者によって提供された Web 以外の情報、例えば新聞や広告を使って正しい URL を知る事が考えられます。厳密さが問われる場合にはサポート窓口に電話で確認する方法もあります。またフィッシング対策協議会では、ある URL がフィッシングサイトのものであるかどうかに関する問い合わせを受け付けています。この他には、初めて利用する URL であれば、その URL をいくつかの検索サイトで検索して、偽サイトであるという発言があるかどうかを調べる方法も考えられます。

3.2.4　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、サイトが正しいかどうかを判別する事に利用できる URL がすべて表示されないことがあります。その場合、お使いのモバイル端末を操作して、URL が正しいかどうか、また通常、URL（特にトップレベルドメイン）がどのように表示されるようになっているかを確認します(図 6)。

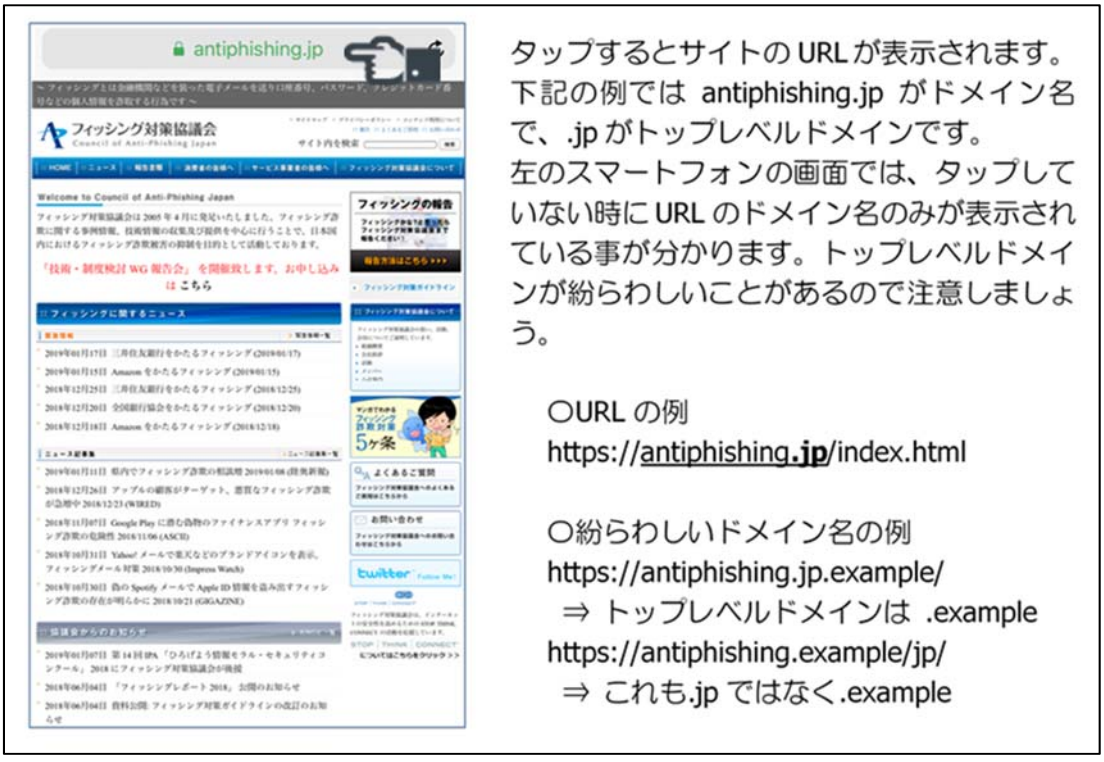


図 6　表示の確認

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。（5.付録 2 参照）

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

[6] 出典：Microsoft

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。

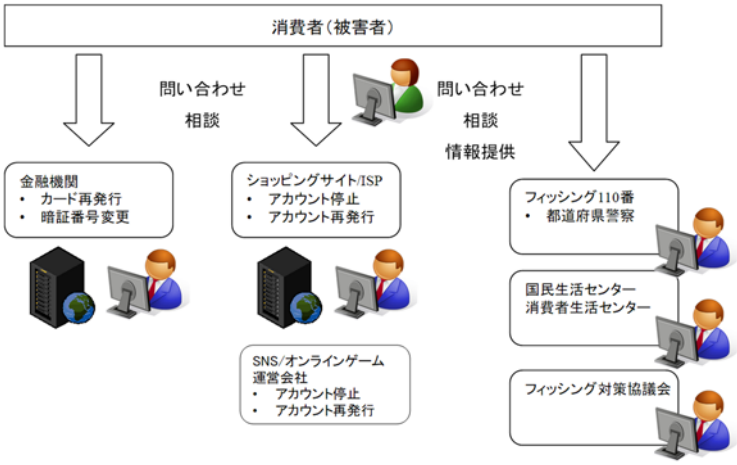


図 8 フィッシング被害に遭ってしまった時の問い合わせ、相談、情報提供

（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	https://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	https://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。

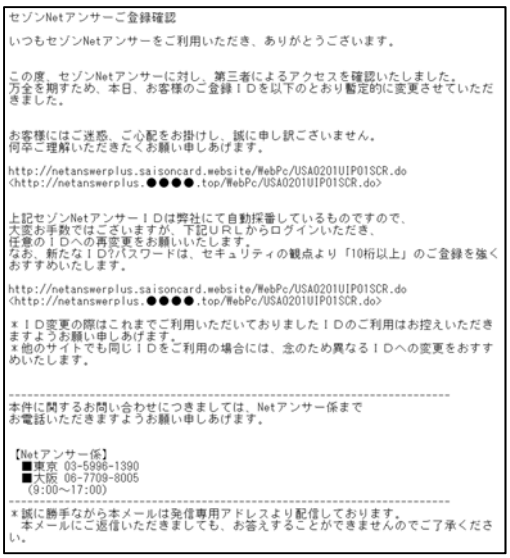
[7] https://www.antiphishing.jp/phishing-5articles.html

5. 付録：フィッシング事例

確認されている主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、最近では、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も確認されています。

(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。図はセゾンカードをかたるフィッシング事例です。このセゾンカード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騙ったサイトに誘導します。


セゾンNetアンサーご登録確認

いつもセゾンNetアンサーをご利用いただき、ありがとうございます。

この度、セゾンNetアンサーに対し、第三者によるアクセスを確認いたしました。
万全を期すため、本日、お客様のご登録ＩＤを以下のとおり暫定的に変更させていただきました。

お客様にはご迷惑、ご心配をお掛けし、誠に申し訳ございません。
何卒ご理解いただきたくお願い申しあげます。

http://netanswerplus.saisoncard.website/WebPc/USA0201UIP01SCR.do
<http://netanswerplus.●●●●.top/WebPc/USA0201UIP01SCR.do>

上記セゾンNetアンサーＩＤは弊社にて自動採番しているものですので、
大変お手数ではございますが、下記ＵＲＬからログインいただき、
任意のＩＤへの再変更をお願いいたします。
なお、新たなＩＤ?パスワードは、セキュリティの観点より「10桁以上」のご登録を強くおすすめいたします。

http://netanswerplus.saisoncard.website/WebPc/USA0201UIP01SCR.do
<http://netanswerplus.●●●●.top/WebPc/USA0201UIP01SCR.do>

＊ＩＤ変更の際はこれまでご利用いただいておりましたＩＤのご利用はお控えいただきますようお願い申しあげます。
＊他のサイトでも同じＩＤをご利用の場合には、念のため異なるＩＤへの変更をおすすめいたします。

本件に関するお問い合わせにつきましては、Netアンサー係まで
お電話いただきますようお願い申しあげます。

【Netアンサー係】
■東京 03-5996-1390
■大阪 06-7709-8005
(9:00～17:00)

＊誠に勝手ながら本メールは発信専用アドレスより配信しております。
本メールにご返信いただきましても、お答えすることができませんのでご了承ください。

図 9　セゾンカードをかたるフィッシングメール

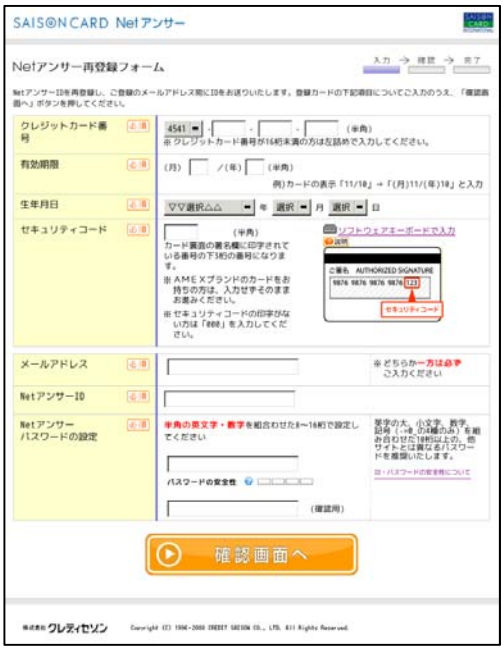


図 10　セゾンカードをかたるフィッシングサイト

(イ)　　銀行をかたるフィッシング

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見つかっています。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。

＊＊＊＊＊＊＊＊＊＊ランダムで長大な文字列＊＊＊＊＊＊＊＊＊＊＊＊＊＊

****
りそな銀行Ｅメール配信サービス
****

＊＊＊＊＊＊＊＊＊＊ランダムで長大な文字列＊＊＊＊＊＊＊＊＊＊＊＊＊＊

2016年「りそな銀行」のシステムセキュリティのアップグレードのため、貴様のアカウントの利用中止を避けるために、検証する必要があります。

以下のページより登録を続けてください。

＊＊＊＊＊＊＊＊＊＊ランダムで長大な文字列＊＊＊＊＊＊＊＊＊＊＊＊＊＊

https://mp.resona-gr.co.jp/mypage/MPMBO10XO10M.mp?BK=0010
<http://www.●●●●.com/img/index.htm>

＊＊＊＊＊＊＊＊＊＊ランダムな長大な文字列＊＊＊＊＊＊＊＊＊＊＊＊＊＊

――Copyright (c) Resona Holdings, Inc. All Rights Reserved――

図 11　りそな銀行をかたるフィッシングメール

図 12　りそな銀行をかたるフィッシングサイト

(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ものが考えられます。詐取したアカウント情報を売買するケースもありますが、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。

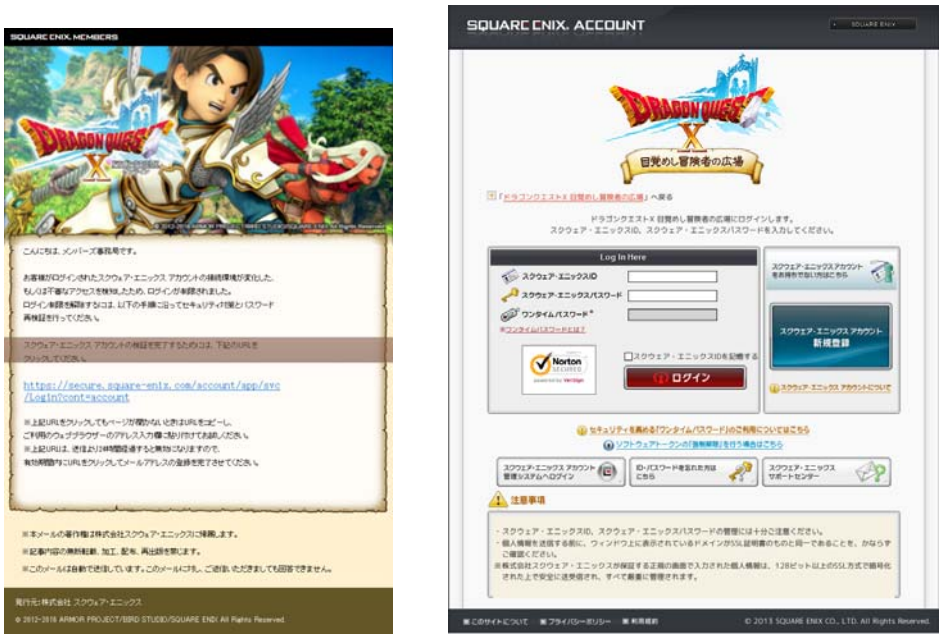


図 13　スクウェア・エニックス（ドラゴンクエスト X）をかたるフィッシング
左：フィッシングメール　右：フィッシングサイト

(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。

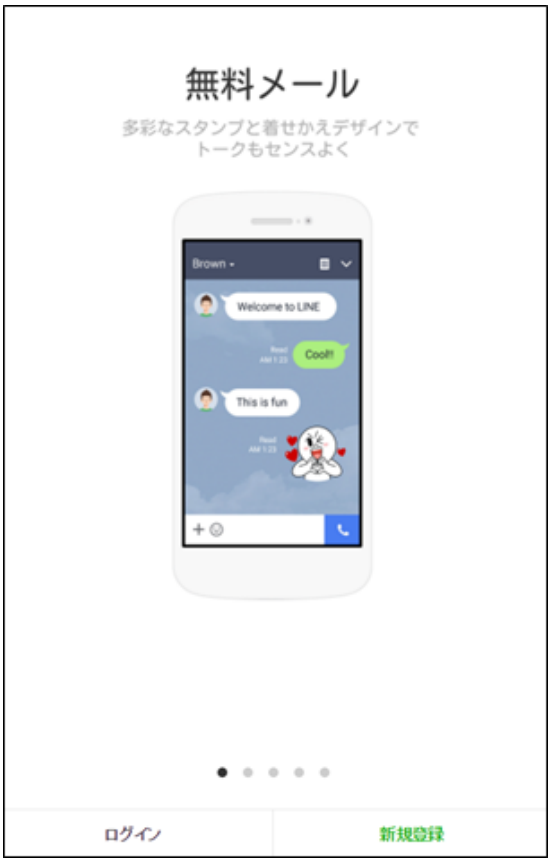


図 14　LINE をかたるフィッシングサイト

(オ)　　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。

図 15　　Amazon をかたるフィッシングサイト

5. 付録 2：パスワードの考え方

（「フィッシングレポート 2015」より）

複数のインターネットサービスで同じパスワードを使い回していることが原因で生じてしまうユーザアカウントへの不正なログイン、いわゆるパスワードリスト攻撃による被害が継続的に発生しています。

そのため利用者としては、複数のインターネットサービスを安全に使用するに、異なるパスワードをサービスごとに設定する必要があります。それら異なるパスワードを管理する手法はいくつがありますが、フィッシングレポート 2015 で紹介された事例を以下に記載します。

■コラム：位置記憶パスワードの提案

～ なぜ、文字列をパスワードとして覚えるのか？ ～

1．パスワード 覚えられますか？

パスワードとして、「T{_3”}H=D+」や「u&![KiXjow」を使って欲しいと言われたら、2 組のパスワードをそれぞれのシステムのユーザ ID とともに覚えられるだろうか？

多くの人は、「覚えられない」と回答するであろう。

しかし、これらの２つのパスワードは、表１に示すように、２行目の５列目から始まり、左下に順に、左端では、右下に折り返し、下端では右上にという規則で作成した。

この乱数表２つとそれぞれのユーザ ID を決めてあれば、図１で示したようなパターンを決めることができれば、パスワード文字列を覚える必要もない。 なお、図１は、該当文字がわかるように色分けをしたが、パターンの規則を覚えられれば、それも必要ない。更に、パスワードの長さも、10 桁としたが、もっと長い文字列も覚えられる。

User-ID: randoma　2015/4/1

	1	2	3	4	5	6	7	8	9	10
1	]	>	D	U	)	S	’	&	:	,
2	i	I	5	z	T	)	l	n	q	%
3	)	W	4	{	*	N	X	I	H	a
4	o	6	_	b	9	5	k	a	N	;
5	I	3	N	~	W	F	r	(	3	*
6	”	(	{	x	W	{	6	b	}	E
7	[	]	3	0	r	N	0	,	”	8
8	#	A	H	=	6	+	_	*	0	h
9	E	V	k	=	=	+	l	3	9	m
10	A	L	j	q	D	~	.	f	J	&

ID: randoma

User-ID: randomb　2015/4/1

	1	2	3	4	5	6	7	8	9	10
1	9	A	[	{	q	)	w	z	n	{
2	b	)	A	’	u	K	Q	%	5	4
3	u	0	%	&	3	Q	V	7	h	U
4	p	t	!	0	<	k	h	:	%	o
5	o	[	q	v	F	2	H	?	_	|
6	K	b	U	>	W	W	e	P	F	R
7	¥	i	`	0	a	+	W	[	7	k
8	7	Y	X	;	H	P	u	f	L	8
9	b	h	&	j	e	w	D	l	d	[
10	f	u	|	u	o	D	)	f	@	2

ID: randomb

図１　乱数表利用のパスワード例

ユーザ ID ごとに乱数表を作成し、ユーザ ID 毎に割り振れば、同一パスワードになる可能性も低い。

例としたパスワード作成規則は、2 行目・５列目から始まり、斜め下に行く規則で作成したが、どの様な規則でも構わない。 更に、乱数表を他人に見せなければ、図１のようにパスワードをマークしても構わない。

2．乱数表について

乱数表はマイクロソフト EXCEL で作成[8]した。現在は、以下の文字種の乱数表を作成でき、A4 用紙に乱数表を 6 組印刷する。

1． 英小文字と数字の組み合わせ
2． 英小文字と数字、記号の組み合わせ
3． 英文字（大・小文字）と数字の組み合わせ
4． 英文字（大・小文字）と数字、記号の組み合わせ

作成した EXCEL シートをダウンロードし、この EXCEL シートを開くと、画面上部に図 2 の内容が表示される。真ん中の枠内に、１～４の数字を入力し、乱数表に利用できる文字種類を決める。

１～４以外の数字を入力すると、枠下に「Enter(1-4)」と表示されるので、正しい値を再入力する。

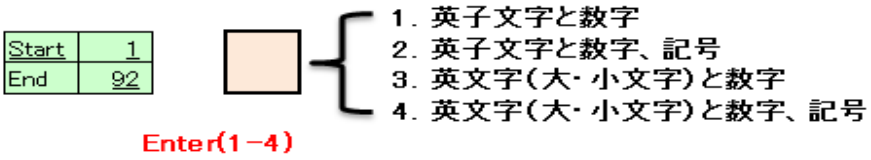


図２ EXCEL シートの上部画面

正しい入力ができれば、印刷できる。

印刷した乱数表で、どの様なパターンを利用するかは、利用環境を考慮することが大切である。 自宅で他人に見られない環境であれば、図 1 に示したようにパターンを色づけしたものを利用しても構わない。

筆者は、職場の机上に A4 用紙を印刷したものを置いてあるが、パスワードとして何を使っているかは、ビデオで撮影されない限り、他人が推測することは殆ど不可能だと考えている。

安易なパスワードを利用しなくても、この方法で一般のユーザ ID／パスワード方式には最も有効な仕組みだと考えている。

3．他の方式が利用できるのであれば・・・

ワンタイムパスワードや生体認証利用が遥かに安全だと指摘されることがある。それ

[8] EXCE で作成したワークシートは、以下に保存してある
日本語版： http://www2.gol.com/users/uchidak/research/RandomPassTable_JPN.xls
また、詳細な解説は、以下を参照のこと；
http://www2.gol.com/users/uchidak/research/RandomPassTable.pdf
なお、今後、利用文字種の組合せを増やすことを検討している。

に反対し、この方式が優れていると考えていない。ただ、この位置記憶パスワードの良さは、現在、インターネット等で利用されている多くのシステムの変更が必要ない。現在のユーザ ID／パスワード方式をそのまま利用できる。

ワンタイムパスワードや生体認証等を利用では、大部分の認証システムは、サービス提供側も利用者も新たなシステムの導入を必要とする。その仕組みを提供するサービスが利用できるのであれば、それをお勧めする。

残念ながら、現在利用されているユーザ ID／パスワード方式のサービスが新しい認証システムを提供してくれなければ、この位置記憶パスワードを利用して、自分自身を守る必要がある。パスワードを使い回しても、「パスワードリスト攻撃」に遭わないかも知れない。ただ、利用者は「遭う、遭わない」を決められない。 そうであれば、この方法を利用するのも１つの方法であろう。

[内田 勝也 情報セキュリティ大学院大学 名誉教授]

■コラム：様々なパスワード管理について

■パスワード管理ソフトの利用

最近では、オンラインでの銀行・株取引、ショッピング、ポータルサイト、SNS、ストレージサービスなど、一人で複数の Web サービスを利用することが多い。

しかし、複数の Web サービスのログイン ID とパスワード(ID//パスワード)を記憶することは容易ではく、かといって記憶し易いよう複数のサイトで同じ ID//パスワードを使い回すのは大変危険である。

一か所の ID//パスワードが何らかの理由で漏洩した場合、これを利用して他の Web サイトにも不正ログインされ、金銭的被害やプライバシー/機密情報の漏えい被害が拡大する可能性が高まる。

PC やスマートデバイスにインストールしたパスワード管理ソフトを利用することで、各 Web サービスごとに個別に設定した ID//パスワードを安全な状態で記録できる。

各 Web サービスにログインする際は、専用ソフトにより ID//パスワードを自動入力される。これにより、自身の記憶に頼ることなく、複数の ID//パスワードを安全に管理することができる。

■手書きメモの利用

複数のサイトで同じ ID//パスワードを使い回すよりは、Web サービスごとに個別に設定した ID//パスワードを手帳や紙にメモしておき、大切に管理する方が安全である。

その際、パスワードの一部を共通の文字列をとして自身で記憶し、残る部分のみをメモ

に記録することでより安全性を高めることができる。
　万一メモを紛失した場合は、各サービスの提供するパスワードリマインダ機能や別途安全な場所に保管しておいたメモのコピーを用いてパスワードの変更を実施することで安全性を高めることができる。

■認証サービスの利用
以下の認証サービスが提供されている場合は、それらのサービスを利用することで安全性を高めることができる。

・ワンタイムパスワード
　トークンと呼ばれる 1 回限り有効なパスワードの生成器(特殊なハードウェアやスマートデバイス上のソフトウェア)を用いて、使い捨てのパスワードを利用してログインする方式。トークンは一定時間ごとに変化するため漏洩リスクが少ない。

・マトリクス認証
　事前に自ら指定した位置と順番通りに数字を入力することで本人であることを認証する方式。表示される数字がランダムなため、辿る位置と順番は同じでも送信される数字列は毎回異なり、漏洩リスクが少ない。
　特定の機器などを必要とせず、位置と順番の記憶のみで成り立つため、機器の紛失や故障によりログインできなくなる事態を防ぐことができる。

[早川 和実　NTT コミュニケーションズ株式会社]
[桐山 直樹　NTT コミュニケーションズ株式会社]