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

2023 年度版

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「情報」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、あなたのクレジットカード情報やインターネットバンク、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。その定義はさまざまですが、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、実在する組織をかたって、ユーザーネーム、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ー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付きにくい手口や、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。

被害に遭わないようにするためには、

- OS やアプリケーションのアップデートを迅速に適用する。
- セキュリティソフトのアップデートを迅速に適用し、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。
- サービス提供事業者が行わないこと（SMS での通知、ネット上で第二暗証をすべて入力させるなど）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。

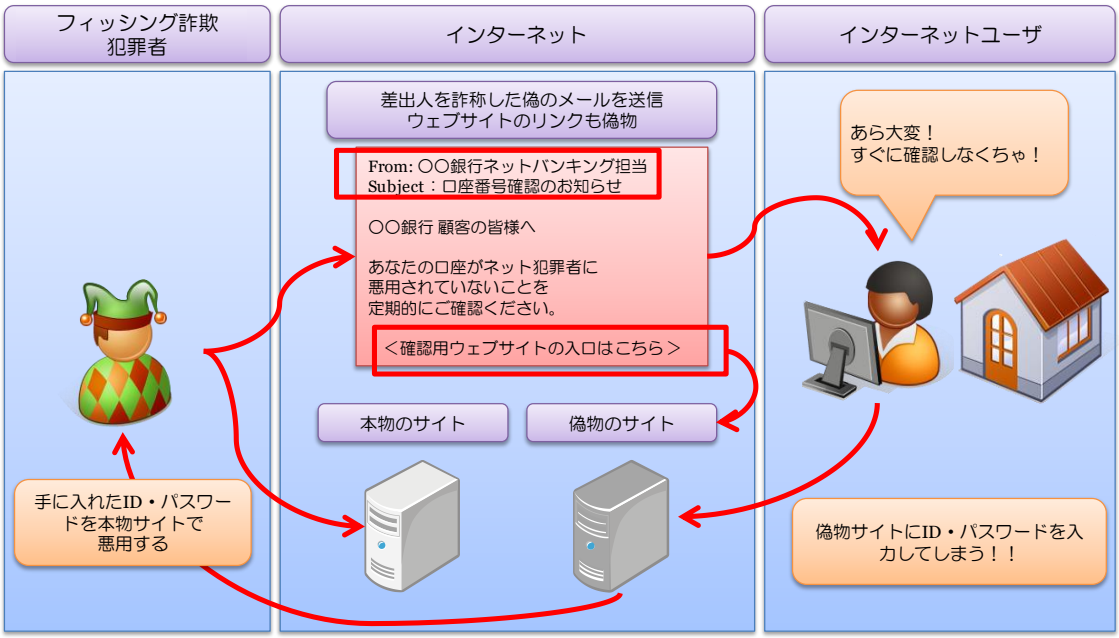


図 1　典型的な「フィッシング」行為

1.1.　類似手法　～フィッシングだけではありません～

年々スマートフォン利用者は増えており、2021 年時点では[2]、国内インターネット利用者の 9 割近くがスマートフォンを利用しています。以前は PC をマルウェアに感染させ犯罪者が使用するネットワーク（ボットネット）の支配下に置き、遠隔操作でフィッシングメールなど不正メールの配信を行わせたりしていましたが、近年はスマートフォンに不正アプリ（マルウェア）をインストールさせ、同様にフィッシングや不正アプリのインストールへ誘導する SMS を配信させています。本ガイドラインで対象とするフィッシングだけでなく、このようなだましの手法にも十分な注意が必要です。

- 不正アプリ[3]によるスマートフォンの遠隔操作

2018 年頃からスマートフォンを狙い、宅配便の不在通知やモバイルキャリア、国税庁などをかたる SMS 文面で誘導する手口がフィッシング対策協議会へ報告され続けています。このタイプは同一のリンクから iPhone など Apple 端末はモバイルキャリアや銀行、Apple

[2] 総務省：第 2 部　情報通信分野の現状と課題
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nd238110.html
[3] ここでのマルウェアとは、いわゆるコンピューターウイルスや、不正プログラム、不正アプリ、スパイウェアなどの総称として用いています。

などをかたるフィッシングサイトへ誘導されますが、Android 端末はブラウザー、セキュリティ対策アプリのアップデートや事業者のスマホアプリなどを装って不正アプリのインストールへ誘導されます。

図 2　フィッシングサイトまたは不正アプリのインストールへ誘導される例[4]

[4]フィッシング対策協議会：ソフトバンクをかたるフィッシング（2022/12/01）
https://www.antiphishing.jp/news/alert/softbank_20221201.html より

- 不正アプリをインストールしてしまうと、情報を窃盗されたり、遠隔操作で自分のスマートフォンから不正な SMS を配信させられるため、問い合わせや苦情の電話が殺到したり、SMS 配信料金で高額な請求がくることで、初めて異変に気が付くケースが多いようです。アプリをインストールする際には「3.6. 正しいアプリを使う」も参考に、正規のアプリストアからのみインストールするよう心がけてください。

2. フィッシング対策３つの心得

フィッシング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、フィッシングに遭わないための 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

さまざま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ー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り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（ユーザー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、フィッシングに遭わないために日ごろから心がけること、クレジットカード番号などの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. フィッシングメール対策をする

3.1.1 迷惑メールフィルターを使う

フィッシングメールは迷惑メールの一種であり、迷惑メールフィルターでその多くが検知、分別、削除できます。ほとんどのメールサービスでは迷惑メールフィルターが利用できますが、標準では設定が無効となっていることが多いため、設定を確認し、有効にしましょう。メールアプリやセキュリティ対策ツールの迷惑メールフィルター機能も併用すると効果的です。

3.1.2 メールアドレスを新しく作る

フィッシングメールや迷惑メールは、一度届きはじめると、止まることはありません。大量にそのようなメールが届いている場合は、そのメールアドレスが広くインターネット上に漏えいしてしまっていることを意味します。漏えいした情報は完全に消すことはできません。同時にパスワードも漏えいしている可能性もあるため、安全のためメールアドレスを新しく作り、利用中のオンラインサービスに登録し直しましょう。

3.1.3 不正メール対策が充実したメールサービスを使う

メールサービスによって、不正メール対策機能に差があります。メールサービスを選ぶ際には、フィッシング対策に有効な以下の要件に対応しているか、確認すると良いでしょう。

- メールの認証（送信ドメイン認証）に対応している
- 認証された正規メールにアイコンやマークが付く（メールサービス標準のメールアプリや Web メールで確認）
- すり抜けた不正メールを報告するための、メールサービスの窓口がある

3.2. Web フィルターを活用する

パソコンやスマートフォンに入っている標準の Web ブラウザーは Web フィルター機能があります。フィッシングサイトや危険なサイトを閲覧しようとすると、警告画面を表示してブロックしてくれます。ブラウザーによって警告が表示されるまでの時間に差があるため、早く警告が出るブラウザーを使ったり、セキュリティ対策ツールのフィルターも併用すると良いでしょう。

3.3. 正しい URL や正規のアプリケーションを用いてアクセスする

3.3.1 ブックマークや正規のアプリケーションを活用する

オンラインサービス初回利用時にはそのドメイン名を利用者カード／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ー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。事業者が提供している正規のスマホアプリを利用することも有効です。スマホアプリをダウンロードする際は正規の提供元（Google Play や App Store）から入手してください。偽のバナー広告や検索結果からフィッシングサイトに誘導される事例もあり、特によく利用するオンラインサービスについては、ブックマークや正規のスマホアプリを活用するようにしてください。また、定期的にブックマークが正しいものかを確認し、更新するようにしてください。

3.3.2 正規メール以外のメール中のリンクからはアクセスしない

正規メールであると認証されていないメール中のリンクはアクセスすると危ないサイトに行く可能性があるため、安易にアクセスしないでください。もしアクセスする必要がある場合は、ブラウザーに登録したブックマークや正規アプリからアクセスして、状況を確認してください。

なお、電子メールだけでなく、電子掲示板、ブログおよび SNS サイトなどで表示される広告やユーザーが書き込んだ URL リンクについても、同様に注意が必要です。

マウスカーソルをリンクに重ねたり、スマートフォンの場合はリンクを長押しするとリンクの内容が表示されるので、文字列としてフィッシング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。なお Apple 端末の場合は、リンク長押しでプレビュー

を表示するとサイトへアクセスしてしまうため、あらかじめ安全なサイトでリンクを長押しして、プレビューを非表示にすることもできます。

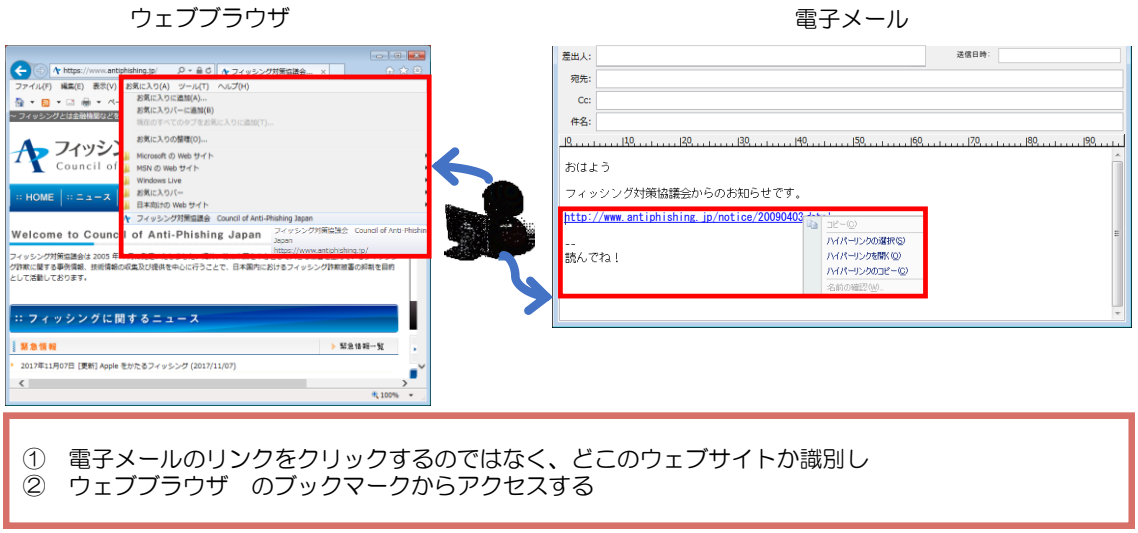


図 3 Web ブラウザーのブックマークの活用

3.3.3 Web サイトに不審な点がないかを確認する

フィッシングサイトはそのサービスの正規の Web サイトをコピーして作られることが多く、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ことは非常に困難です。

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さまざまになっているので、まず、ご自身が使っているブラウザーやスマートフォンでドメイン名や鍵マークが、普段、どのように表示されるのかを確認しておきましょう。その後、次の方法を使って確認しましょう。

Web サイトに不審な点がないかを確認する方法：

<u>○ドメイン名が正しいか、不審なサイトではないかを確認する</u>

正規のドメイン名が分かっている場合には、ブラウザーの上部または下部に表示されている Web サイトの URL のドメイン名が一致しているかどうかを確認します。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。

ドメイン名が分からない場合は、表示されたドメイン名をネットで調べて、フィッシングや詐欺の情報がないか、確認しましょう。

〇Web サイトを運営している組織の表示を確認する

ー組織の名称が表示されている場合ー

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ている場合には、その名称が、アクセスしようとしている Web サイトの会社名と一緒になっていることを確認します。

〇鍵マークをクリックして証明書の内容を確認する

鍵マークが表示されているにもかかわらず、フィッシングサイトであるケースが増えています。鍵マークには、Web サイトとの通信が暗号化されているという意味と、Web サイトを運営している組織が実在しているといった全く異なる意味がありますが、いずれも同じように表示されています。鍵マークだけで安心せず、より詳しく、もしくは他の方法と組み合わせて確認しましょう。

確認のポイント：

- 発行先／証明書の発行先

  Web サイトを運営している法人などの組織の名称になっているかどうかを確認します。特に、銀行、オンラインショッピング、電子申請の Web サイトでは、その Web サイトを運営している会社の名称になっていることを確認します。

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ことが考えられます。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 を知ることが考えられます。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。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。

3.3.4 モバイル端末向けの注意事項

スマートフォンなど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ことに利用できる 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 4）。

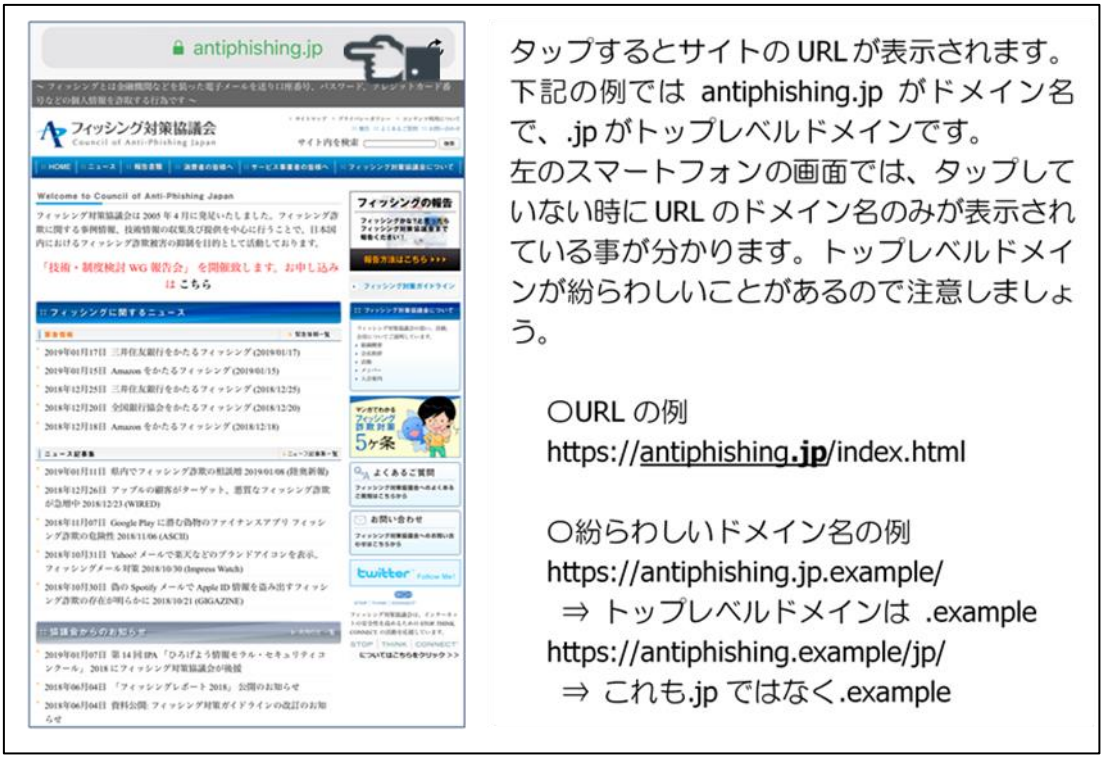


図 4　表示の確認

3.4. なりすましメールに注意しましょう

3.4.1 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すべ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。

図 5　怪しいメールの例[5]

[5] フィッシング対策協議会: ゆうちょ銀行をかたるフィッシング (2022/11/08)
https://www.antiphishing.jp/news/alert/japanpostbank_20221108.html

図 6　怪しい SMS の例[6]

例えば、国税庁（国税局、税務署を含む）、各配達業者では SMS による案内は送信していない、と注意喚起しています。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すべての入力を求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。

3.4.2 正規メールに付くアイコンやマークの確認

「送信ドメイン認証」という技術を使い、認証された正規メールにブランドアイコンやマークを表示するメールサービスが増えています。アイコンが表示されるためには厳しいセキュリティ要件を満たす必要があるため、2022 年現在ではセキュリティ意識の高い一部の大手サービスしかアイコンやマークが表示されませんが、そのようなサービスは安心して利用することができるとも言えます。

---

[6] ソフトバンクをかたるフィッシング（2022/12/01）
https://www.antiphishing.jp/news/alert/softbank_20221201.html
au および KDDI をかたるフィッシング（2021/11/26）
https://www.antiphishing.jp/news/alert/au_kddi_20211126.html
国税庁をかたるフィッシング（2022/08/15）
https://www.antiphishing.jp/news/alert/nta_20220815.html
宅配便の不在通知を装うフィッシング（2020/12/18）
https://www.antiphishing.jp/news/alert/fuzaiSMS_20201218.html
NTT ドコモをかたるフィッシング（2022/02/10）
https://www.antiphishing.jp/news/alert/nttdocomo_20220210.html

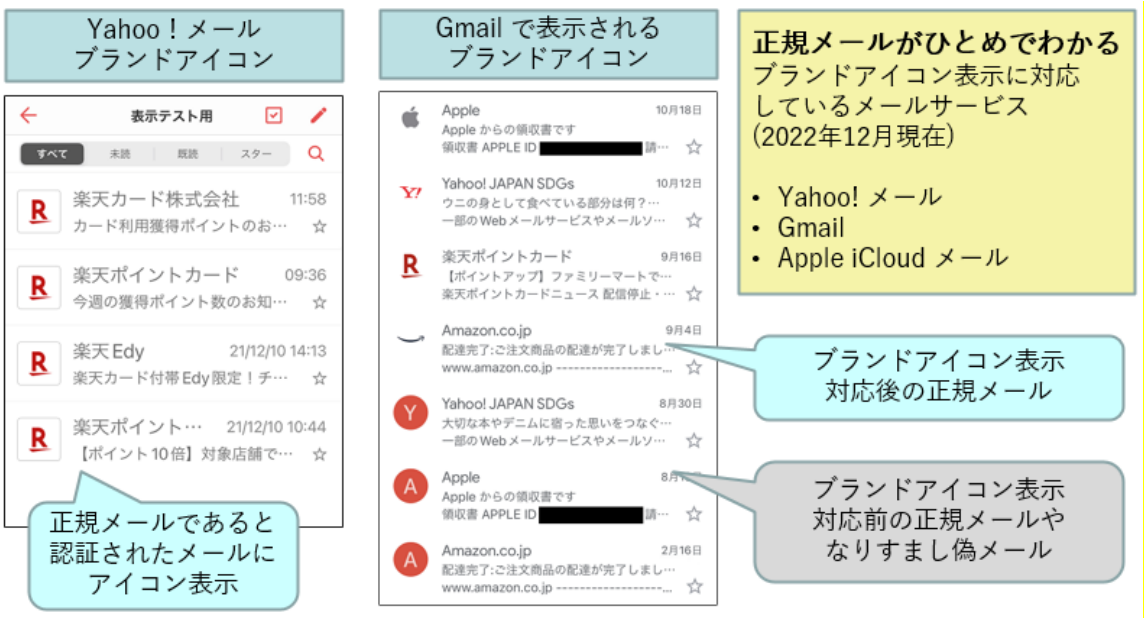


図 7　各社のアイコンやマークの例

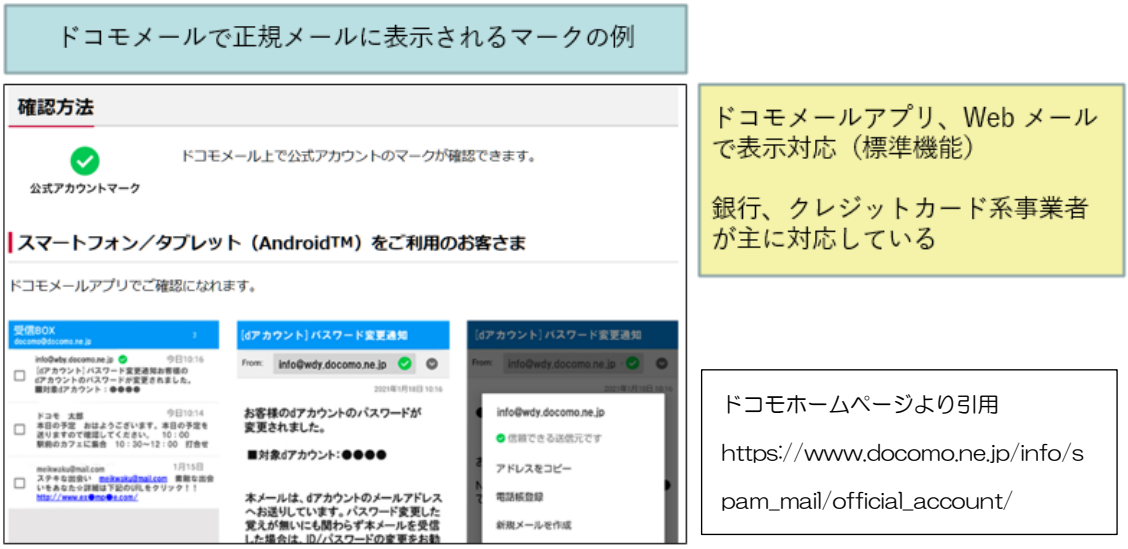


図 8　各社のアイコンやマークの例[7]

[7] ドコモホームページより引用
https://www.docomo.ne.jp/info/spam_mail/official_account/

3.4.3 送信ドメイン認証に対応したメールサービスの使用

メール差出人に実在するサービスのメールアドレス（ドメイン）を使用した「なりすまし」フィッシングメールは、送信ドメイン認証技術 DMARC によりプロバイダーが受信した段階で、排除や迷惑メールボックスへの振り分けが可能となっています（実在するサービス側で DMARC のポリシーを reject または quarantine に設定した場合）。また、正規メールにアイコンが表示されるなどのフィッシング対策機能（BIMI）が強化されています。大量のフィッシングメールを受信している利用者は、これらの送信ドメイン認証技術に対応したメールサービスに新たにメールアドレスを作成し、オンラインサービスへ登録しているメールアドレスを切り替えていくことを検討してください。

3.4.4 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できるためです。多くの銀行は電子署名に S/MIME[8]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ーに送信されます。ユーザー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。

3.4.5 SMS（Short Message Service）の発信者番号表示の確認

SMS を使ったフィッシングが急増しています。SMS の配信には以下図 9 の 3 種類があり、国際網経由の SMS についてはフィッシングの可能性を疑い、慎重に行動することが大切です。SMS が届いた際には発信者番号表示の電話番号が海外の電話番号やアルファベットになっていないことを確認しましょう。また、近年は不審な SMS のリンクから不正アプリをインストールしてしまい、乗っ取られた一般利用者のスマートフォンからのスミッシング[9]配信が非常に多いので、発信者番号が携帯電話番号の場合は、正規の発信者であるか、事業者のホームページを確認しましょう。事業者名が判らない場合は、リンクにアクセスし

[8] 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。
[9] SMS を利用して、個人情報を抜き取るフィッシングサイトへと誘導するフィッシングのこと。

ないようにしましょう。

	国内直接接続の SMS 配信	国際網を経由した SMS 配信	携帯電話端末からの SMS 配信
発信者番号表示	日本電話番号 （例：03-0000-0000） 携帯キャリアごとの特別番号 （例：50000）	海外の電話番号 （例：+1 000-000-0000） アルファベット （例：FOOBAR）	携帯電話番号 （例：090-0000-0000）

※国内直接接続の SMS 配信においても双方向サービスでは、利用審査を経た携帯電話番号を用いる場合がある。

図 9　SMS 配信経路の種類と怪しい SMS の例

また、SMS の次世代版である RCS（Rich Communication Service）に準拠したサービス「＋メッセージ」では企業が携帯キャリア 3 社それぞれの審査を受け、認証を得たことを示す「認証済みマーク」が表示される仕組みがあります。「+メッセージ」で企業からのメッセージを受信した場合は「認証済みマーク」を確認しましょう。

図 10　認証済みマークのイメージの例[10]

3.5. パソコンやモバイル端末を安全に保ちましょう
～パソコンやスマートフォンを安心して使うために

パソコンやスマートフォンを使っているとき、気付かないうちにフィッシングにあってしまうかも知れない、そのような不安を持つことは実は大切なことです。ただ、不安をそのままにしていては意味がありません。本節では、パソコンやスマートフォンの利用にあたって、日頃から気を付けておくことでフィッシング対策につながる事柄についてまとめます。

[10] 出典：NTT ドコモ
https://www.nttdocomo.co.jp/info/news_release/2019/04/23_00.html より

3.5.1 ソフトウェアを最新の状態にする

パソコンやスマートフォンのようなモバイル端末にセキュリティ上の脆弱性があると、利用者が気付くことなくマルウェ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やモバイル端末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 8.1 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。

3.5.2 パスワードのしっかりとした管理

不正アクセス行為、マルウェア感染などの原因で Web サイトからユーザー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。ユーザー側の努力だけでは 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 サイトごとに 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。

「1234」「1111」といった安易なパスワード、個人情報から類推されやすいパスワードを設定しないということも重要です。特に安易なパスワードは未だ多くの方が設定されている傾向にあり、パスワードが奪われずとも数回のログイン試行により突破されてしまう可能性があります。

上記の対策に加え、フィッシングに騙されてしまい、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、正規ユーザーを締め出すため、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。

3.5.3 サービス事業者が提供するセキュリティ機能を積極的に利用する

サービス事業者は利用者の安全を目的にさまざまなセキュリティ機能を提供しています。

オプションとして手続きが必要な機能もありますが、積極的にセキュリティ機能を利用するようにしましょう。サービス事業者が提供するセキュリティ機能例としては、以下のものがあります。

- ワンタイムパスワード
- アプリ生体認証
- メール認証、ＳＭＳ認証
- 利用状況メール通知
- ソフトウェアキーボード
- ウイルス対策ソフト
- フィッシングサイト検知ソフト

SMS 認証やワンタイムパスワード認証などの複数要素認証を利用することが、攻撃者による不正ログインと「収益化」を阻止するために有効です。
ID とパスワード認証だけではフィッシング対策として十分とは言えないため、各 Web サービスで提供されているセキュリティ機能は積極的に利用するようにしましょう。2022 年 9 月に、経済産業省は EC サイトでのクレジットカードの不正利用防止に向け、カード所有者本人であることを複数手段で認証する国際的なシステム規格（認証規格「EMV-3D セキュア」）の導入義務化の検討を発表しています。（2022 年 9 月、経済産業省発表より）

3.6. 正しいアプリを使う

不正アプリは正規のアプリケーションストア以外から配布されていることが多く、ダウンロード時やインストール時に警告が出ます。アプリをインストールする場合は正規のアプリストア（iOS デバイスの場合は App Store 、 Android の場合は Google Play など）からインストールし、警告が出た場合は絶対にインストールしないようにしましょう。

※正規のアプリ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ーから不正なアプリのブラックリストを使ったアプリフィルターが提供されていますので、これらのサービスを使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、ソフトウェアを実行・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。信用できるアプリをインストールする場合に限って「実行」「はい」などを選択するようにしてください。

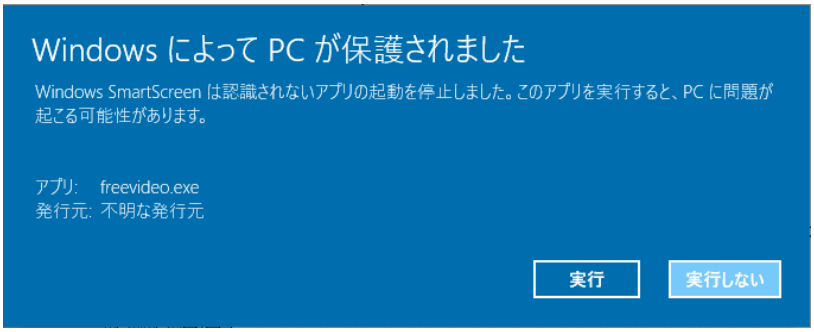


図 11　ソフトウェアのインストール時に表示されるダイアログの例[11]

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「3.3」で示したような URL の確認と鍵マークの確認ができ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。

3.7.　履歴を確認する

普段からクレジットカードやキャッシュレス決済の利用明細を確認しましょう。また、アカウントのログイン履歴などを確認することも、不正利用の痕跡を見つけるためには有効です。

3.8.　間違って重要情報を入力してしまったら

自分がフィッシングサイトにアクセスしていることに気付かないまま、ID、パスワード、

[11] 出典：Microsoft

さらにクレジットカード番号など重要な情報を入力してしまっている可能性もあります。

フィッシング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、暗証番号などが不正利用された）、スマホのキャリア決済やキャッシュレス決済で身に覚えのない利用履歴があった（携帯電話番号、モバイル契約管理アカウント情報が詐取されていた）、要求した覚えのない認証コードを受信した（認証情報が不正利用された）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、プロバイダーへ連絡を取り、当該アカウントの利用停止などの対応を依頼します。

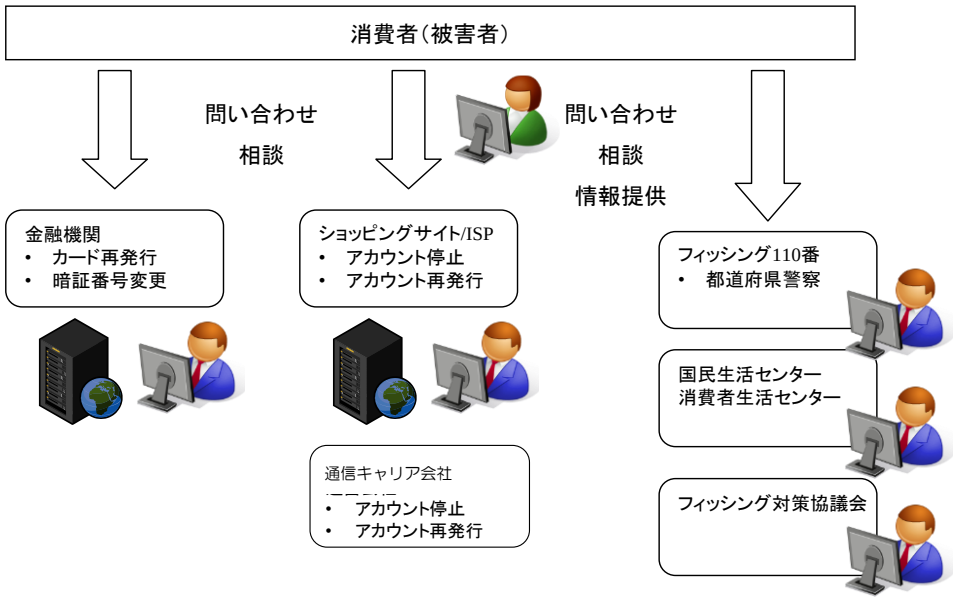


図 12　フィッシング被害に遭ってしまった時の問い合わせ、相談、情報提供

（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ーの 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	https://www.kokusen.go.jp/
全国の消費生活センター	https://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
Web フォーム	https://www.antiphishing.jp/registration.html

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、フィッシングをはじめとするオンライン犯罪の増加を予見し、関係者が情報交換を行い、また被害状況に応じた対策を推進するという目的で発足いたしました。

その後、日本国内において多様なインターネットサービスをかたった日本語のフィッシングメールやフィッシングサイトが多く確認され、金銭的な損害を被ってしまうインターネット利用者が増加しました。2012 年、このような状況に鑑みて、インターネット利用者向けの対策を示した本ガイドラインを策定し、以後、フィッシングを取り巻く状況の変化にあわせて毎年改定しております。

協議会では、本ガイドライン以外に、インターネット利用者に向けた対策コンテンツを公開しております。本ガイドラインとあわせて対策を実践してください。

緊急情報 協議会に報告されたフィッシングメールやフィッシングサイトの実例を公開	https://www.antiphishing.jp/news/alert/
マンガでわかる フィッシング詐欺対策 5 ヶ条 インターネット利用者がとるべき 5 つの対策をマンガで紹介	https://www.antiphishing.jp/phishing-5articles.html

5. 付録

5.1. 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。2020 年以降、フィッシングが激増しています。近年はさまざまなサービスをかたり、最終的にはクレジットカード情報を盗むことを目的としたフィッシングがとても多くみられます。2021 年後半からキャッシュレス決済の不正利用目的のフィッシングが増えはじめたり、2022 年は省庁からの納税に関する通知を装ったフィッシングが急増しました。

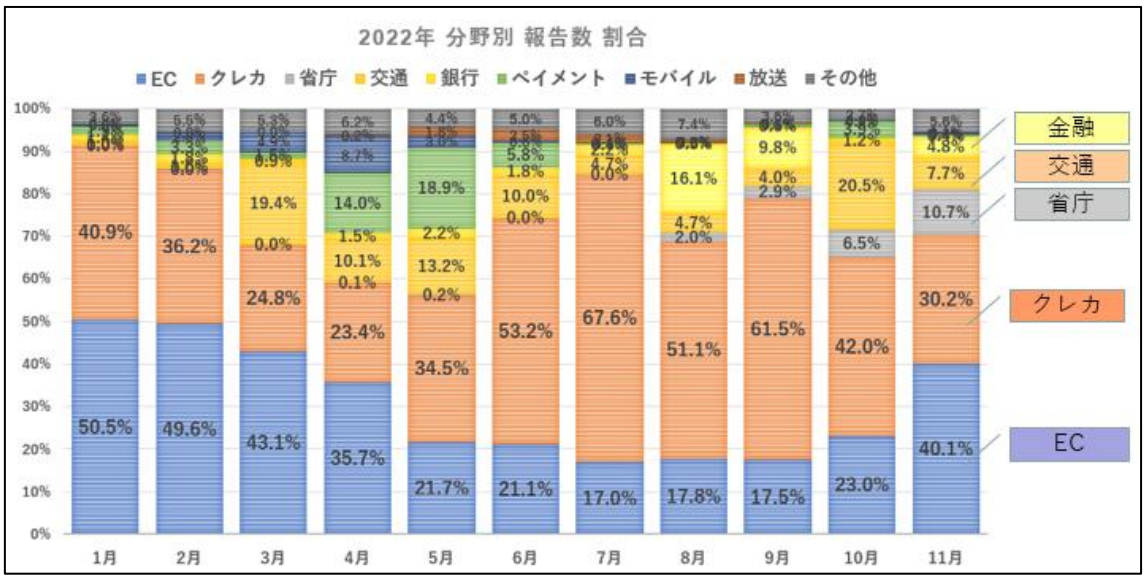


図 13　2022 年分野別報告数の割合（フィッシング対策協議会）

(ア)　　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 14　　Amazon 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すべ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「すべて」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/MPMB010X010M.mp?BK=0010
<http://www.●●●●.com/img/index.htm>

＊＊＊＊＊＊＊＊＊＊ランダムな長大な文字列＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

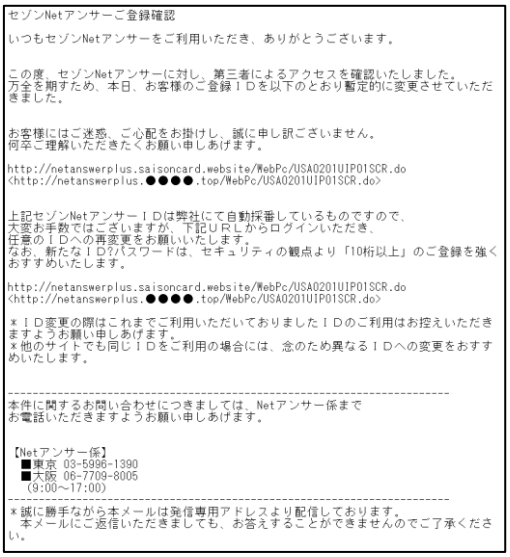
――Copyright (c) Resona Holdings, Inc. All Rights Reserved――

図 15　りそな銀行をかたるフィッシングメール

図 16　りそな銀行をかたるフィッシングサイト

(ウ)　　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などのサービスページをかた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>

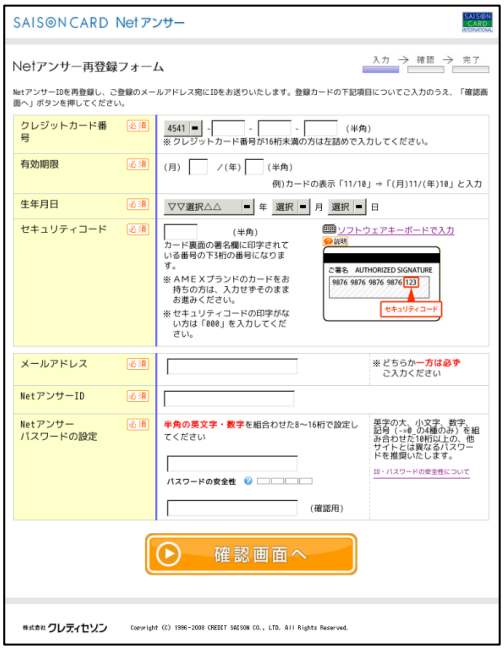
＊ＩＤ変更の際はこれまでご利用いただいておりましたＩＤのご利用はお控えいただきますようお願い申しあげます。
＊他のサイトでも同じＩＤをご利用の場合には、念のため異なるＩＤへの変更をおすすめいたします。

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 17　セゾンカードをかたるフィッシングメール



SAISON CARD Netアンサー

Netアンサー再登録フォーム

入力 → 確認 → 完了

Netアンサーを再登録し、ご登録のメールアドレス宛にIDをお送りいたします。登録カードの下記項目についてご入力のうえ、「確認画面へ」ボタンを押してください。

クレジットカード番号 必須
4541 - - - （半角）
※クレジットカード番号が16桁未満の方は左詰めで入力してください。

有効期限 必須
（月） /（年） （半角）
例）カードの表示「11/10」→「(月)11/(年)10」と入力

生年月日 必須
▽▽選択△△ 年 選択 月 選択 日

セキュリティコード 必須
（半角）
カード裏面の署名欄に印字されている番号の下3桁の番号になります。
※ＡＭＥＸブランドのカードをお持ちの方は、入力せずそのままお進みください。
※セキュリティコードの印字がない方は「000」を入力してください。
ソフトウェアキーボードで入力
説明
ご署名 AUTHORIZED SIGNATURE
9876 9876 9876 9876 123
セキュリティコード

メールアドレス 必須
※どちらか一方は必ずご入力ください

Netアンサー ID 必須

Netアンサー パスワードの設定 必須
半角の英文字・数字を組合わせた8～16桁で設定してください
パスワードの安全性
（確認用）
英字の大、小文字、数字、記号（-+@_の4種のみ）を組み合わせた10桁以上の、他サイトとは異なるパスワードを推奨いたします。
ID・パスワードの安全性について

確認画面へ

株式会社クレディセゾン Copyright (C) 1996-2008 CREDIT SAISON CO., LTD. All Rights Reserved.

図 18　セゾンカードをかたるフィッシングサイト

(エ)　　生命保険会社をかたったフィッシング

2021 年 11 月以降、複数の生命保険会社をかたったフィッシングの報告を受けています。これは、登録された個人情報の再確認を求めるフィッシングメールから契約者専用サイトを装ったフィッシングサイトに誘導し、契約者専用ページの ID とパスワード、さらに保険証券番号の入力を求めてくるものです。このフィッシングは、保険の契約者貸付制度（解約返戻金の一定範囲内で必要資金を用立てする制度）を悪用した可能性があり、詐取した ID を使って振込先を偽装口座に変更し、貸付金を不正に受け取る詐欺となっています。　利用者（契約者）の対策としては、保険会社の Web サイトのドメインが正規のものかを確認するようにし、契約者ページには保険会社の Web サイトまたはスマートフォンアプリを経由してアクセスし、ログインするようにしてください。

図 19　明治安田生命をかたるフィッシングサイト