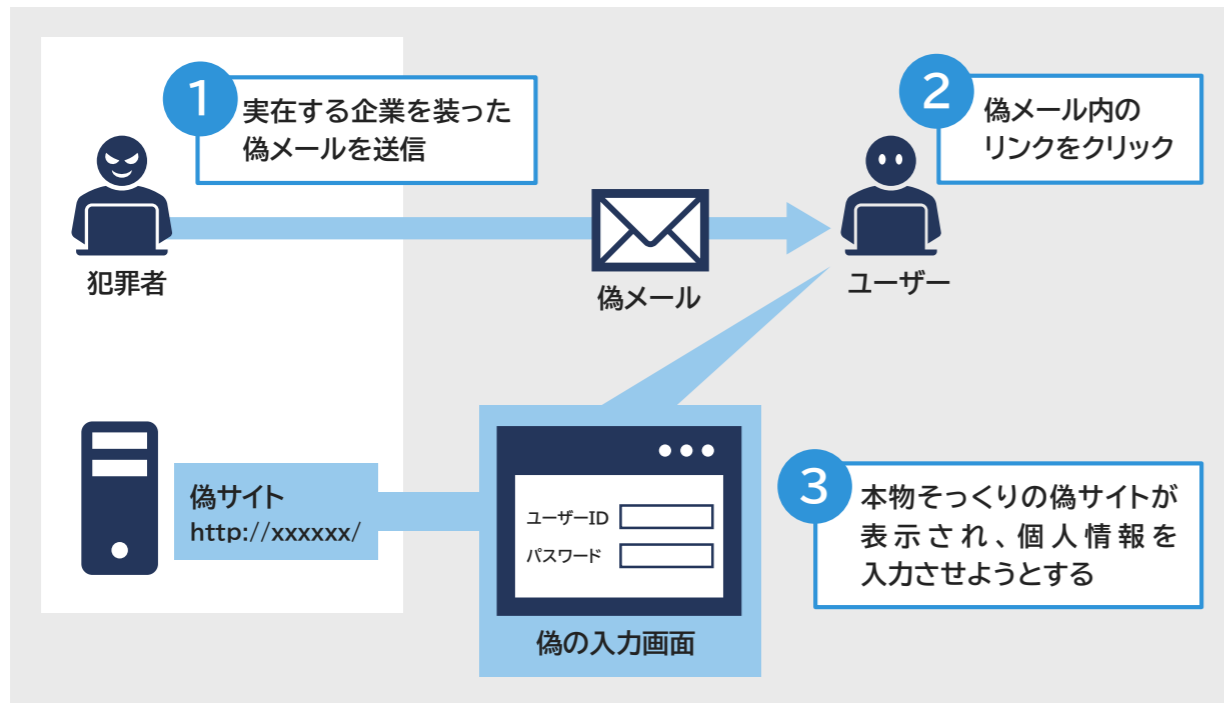


本物そっくりの偽サイトに誘導 フィッシング詐欺にご注意ください

フィッシング詐欺は、実在する銀行やクレジットカード会社などの金融機関、ショッピングサイトを装ったメールを送りつけ、これらのホームページとそっくりの偽サイトに誘導し、住所、氏名、銀行口座番号、クレジットカード番号などの重要な情報を入力させてだまし取る行為のことをいいます。

最近では、メールの送信者名を詐称し、もっともらしい文面や緊急を装う文面にするだけでなく、本物とほとんど区別がつかないような偽サイトを用意するなど、手口が巧妙になってきており、ひと目ではフィッシング詐欺であると判別できないケースが増えてきています。

さらに、最近ではパソコンだけでなく、スマートフォンでも同様にメールやSMSなどのメッセージ機能からフィッシングサイトに誘導される手口が増えてきています。



金融機関などの名前で作られたメールやSMSなどのメッセージの中で、通常と異なる手順を要求された場合には、内容を鵜呑みにせず、金融機関に直接確認しましょう。

ただし、メールに記載されている相手の情報は正しいものとは限らないため、電話をかける場合は必ず正規サイトや金融機関からの郵便物などで連絡先の電話番号を調べるようにしましょう。

安心してインターネットを使うために

サイバーセキュリティガイド



DXの推進と空間デザインで働き方改革のビジネス環境創りをお手伝いします

INEX 株式会社 アイネックス

パソコン専門店 COM

〇本社(管理本部)	秋田市牛島西1-4-5	Tel 018-887-5560
〇空間コーディネート事業部	秋田市牛島西1-4-5	Tel 018-832-1211
〇DX推進事業部	秋田市広面字鍋沼37	Tel 018-831-3131
〇DX推進事業部 能代営業所	能代市宇島小屋32-5 ハカマビル 1F	Tel 0185-55-3780
〇DX推進事業部 大仙営業所	大仙市大曲須和町2-2-20	Tel 0187-62-6630
〇店舗事業部(パソコン専門店COM)	秋田市広面字鍋沼37	Tel 018-837-9801



www.inecx.co.jp

脅威を知ろう

▶ インターネットにはどんな危険があるの？

安心して楽しむために

▶ 安全にインターネットを利用するための対策

インターネットの利用者すべてがセキュリティを意識して行動することが安全性を高めることにつながります。正しい知識と対策によって、安心して便利なインターネットを活用しましょう。

総務省「国民のためのサイバーセキュリティサイト」(https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/)をもとに作成

便利なインターネットを安全に

ホームページを見たり、メールをやり取りしたり、ショッピングサイトで買い物をしたりなど、インターネットを使った便利なサービスがある反面、インターネットを悪用した犯罪やいたずらなどもあります。


「車は便利だけど、事故が起きるかもしれないから車に乗らない」
「包丁を使うときれいに切ることができるけど、手を切ってしまうかもしれないから包丁は使わない」
という人はほとんどいらっしゃらないのではないのでしょうか。

「事故が起きないように安全運転を行う」「手を切らないように気を付けて包丁を使う」というように、インターネットの脅威と対策を知り、便利なインターネットを安全に利用しましょう。




インターネットにはどんな危険があるの？


金銭目的や恨み、不満を晴らす目的で、悪意のある第三者はウイルスを送りつけたり、不正アクセスを行ったり、重要な情報を盗んだりします。

 **ウイルス**


メールやホームページ閲覧などによってパソコンに侵入する特殊なプログラムで、パソコンに保存されている情報を盗んだり、システムを破壊したりする。
多くのウイルスは増殖するための仕組みを持つ。

 **不正アクセス**


本来アクセス権限を持たない者が、システム内部へ侵入する行為で、システムが停止したり、情報漏洩などの影響を及ぼす。
インターネットは世界中と繋がっており、不正アクセスは世界中のどこからでも行われる可能性がある。

 **詐欺等の犯罪**

インターネットを介した詐欺や犯罪行為などが増加している。
偽ホームページに誘導して個人情報を窃取するフィッシング詐欺、クリックしたことで架空請求をするワンクリック詐欺など多様な手口がある。

 ぜいじゃくせい
脆弱性


OSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となるセキュリティ上の欠陥のこと。
脆弱性は、不正アクセスに利用されたり、ウイルスに感染したりする危険性がある。

 **情報発信
トラブル**


自由に情報発信できる場所や機会が増えた反面、発信のしかたを誤るとトラブルを引き起こす原因にもなる。
情報発信のしかたを誤ると、重要な情報が漏洩したり、企業や組織のブランドやイメージを大きく低下させてしまうこともある。
また、自分のプライバシーを必要以上に公開してしまったり、他人のプライバシーを侵害してしまったりなどのトラブルが起こることも。

安全にインターネットを利用するための対策


インターネットのさまざまな脅威に晒され、大きな被害や影響を受けないためには、どのようなことをすればよいのでしょうか。

 **ウイルスに感染しないために**


1. ソフトウェアを更新して、脆弱性をなくす。
2. ウイルス対策ソフトを導入し、契約期間が切れないよう継続的に更新を行う。
3. 迷惑メールのリンクはクリックせず、添付ファイルも開かない。

 **不正アクセスに遭わないために**


1. 外部から自分の意図しない攻撃の通信を許可しないように、ファイアウォールを導入する。
2. IDやパスワードなどのアカウント情報をきちんと管理する。
3. 脆弱性への対策を行う（後述）

 **詐欺や犯罪に巻き込まれないために**

1. インターネットにおける詐欺や犯罪などの手口を知る。
2. インターネット上のやりとりで、少しでも不審な点を感じたら、情報の発信元や真意を確認する姿勢が重要。
3. 怪しい儲け話などの誘惑にのらないように心がける。

 **脆弱性を塞ぐために**

1. Windowsの場合：Windows Updateをきちんと行う。
2. 脆弱性が発見されてから修正プログラムが配布されるまでの間に、その脆弱性を利用して行われる攻撃（ゼロデイ攻撃）もあるため、十分な注意が必要。

 **情報発信の心得**

1. 自分・家族・友達を問わず、機密情報やプライバシー情報を掲示板やSNSなどに書き込まない・誹謗中傷しない。
2. 書き込む内容や情報を公開する範囲、その結果どのような影響が起こり得るか、常に意識して情報発信するよう心掛ける。
3. 司法機関によるプロバイダー開示請求によって発信者の情報は提供されるので、インターネットに匿名はないと考えた方がよい。