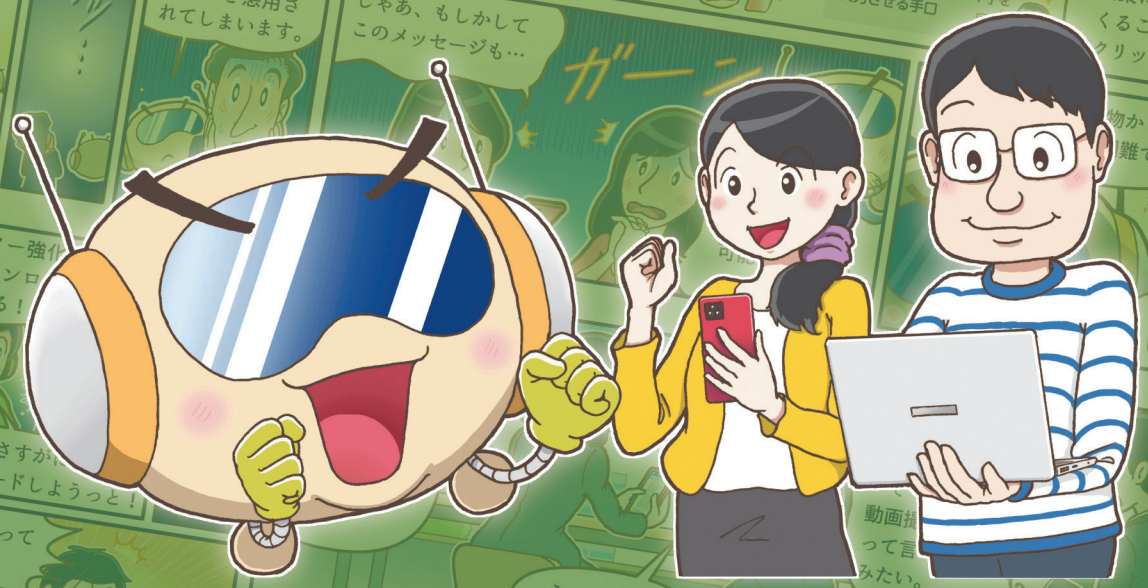
# マンガでわかる
# サイバーセキュリティ

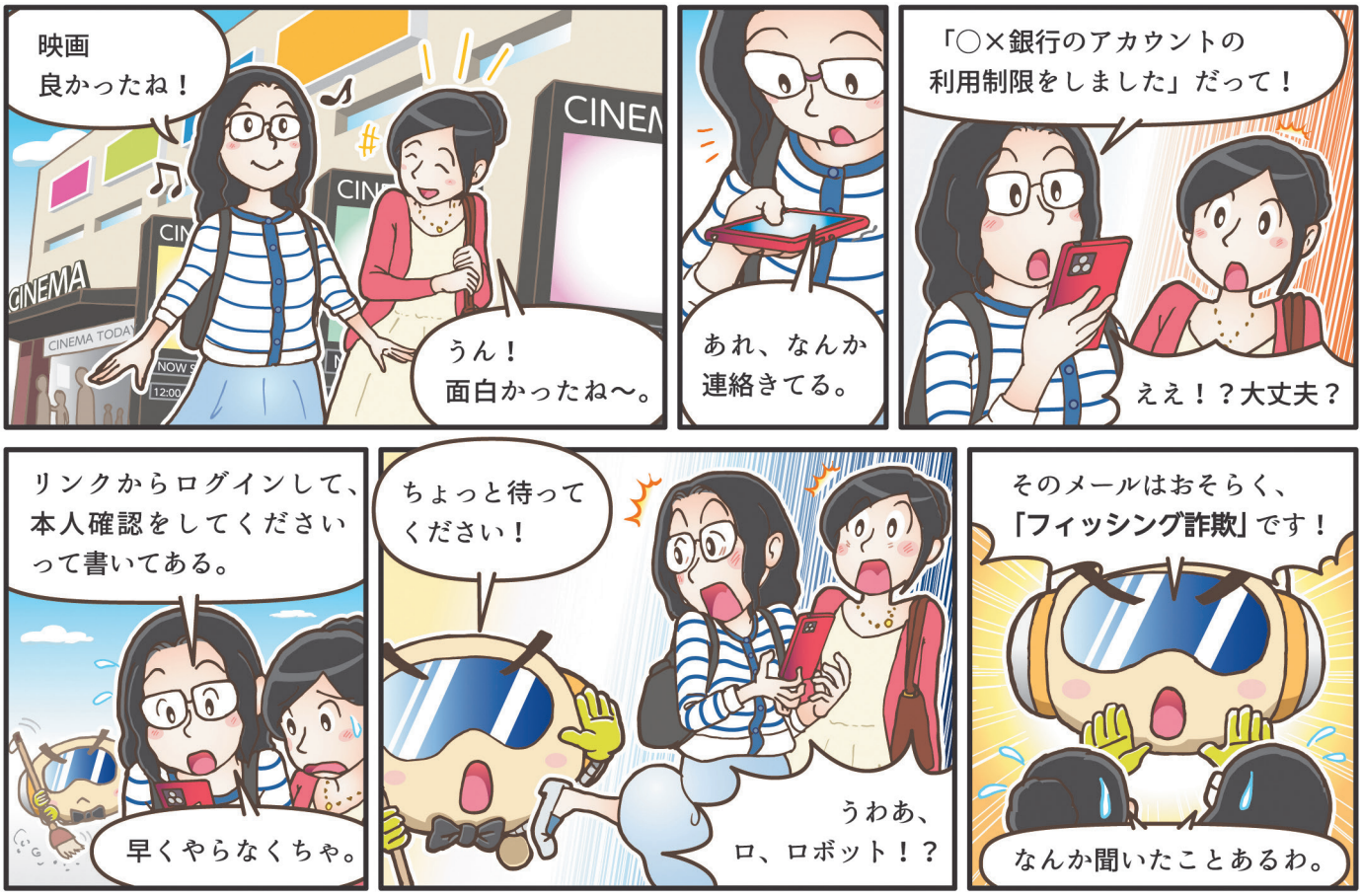
## 個人編



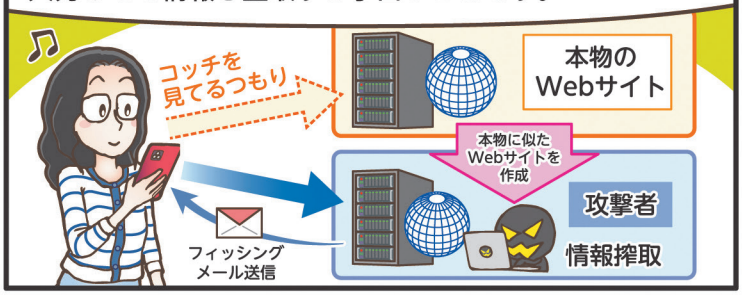
目次

# マンガでわかる サイバーセキュリティ

## フィッシング詐欺に気を付けよう




「フィッシング」とは、実在する銀行やクレジットカード会社等を装った電子メールやSMSを送付して、その企業のWebサイトに似せた偽物のサイトに、アカウント情報（ユーザID、口座番号、パスワード、暗証番号等）を入力させて情報を盗取する手口のことです。



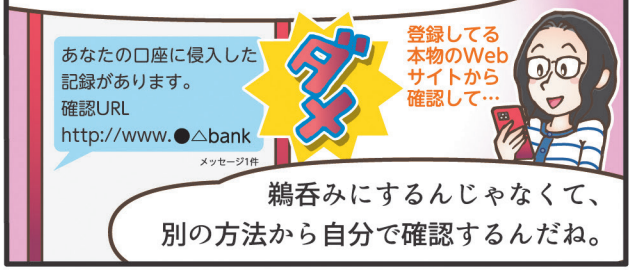

攻撃者は情報を盗んだ後、本人になりすまして本物のWebサイトで取引を行い、銀行であれば不正に送金を実行したりします。


また電子メールやSMSの他にも、SNSやオンラインゲーム等を利用したフィッシング詐欺も横行しているので注意が必要です。

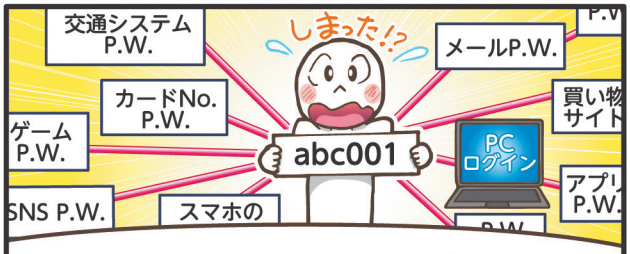
まず、
**IDや**
**パスワード、**
**ワンタイム**
**パスワード等の**
**入力を促す**
**メールやSMS**
**には注意**
しましょう。


**銀行やクレジットカード会社等が、メールやSMSで情報を求めることはありませんので、**このような誘導には気を付けてください。

本文に記載されたURLにはアクセスしないことも重要です。正しいWebページのURLを予めブックマークしておき、そこからアクセスして情報を確認するのも方法の一つです。




鵜呑みにするんじゃなくて、別の方法から自分で確認するんだね。



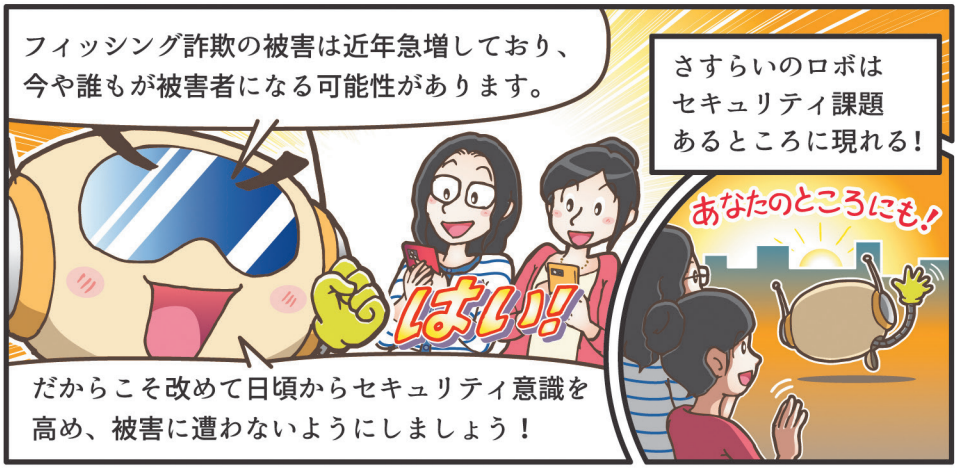

万が一情報を盗取された場合の被害を拡大させないために、**IDやパスワードの使い回しはやめましょう。**また、企業が推奨する多要素認証や生体認証等の認証方法がある場合は利用するのもおススメです。

他にも、**端末のOSやアプリ・ソフトウェアを最新の状態にアップデート**することや携帯電話会社等の**セキュリティ設定（迷惑メッセージブロック機能等）を活用**するといった基本的な対策も忘れないでください。


改めて聞くと当たり前みたいな意識とか対策が大事なんだ。

よく聞くような話だもんね。

フィッシング詐欺の被害は近年急増しており、今や誰もが被害者になる可能性があります。




だからこそ改めて日頃からセキュリティ意識を高め、被害に遭わないようにしましょう！

**他の事例**

- **銀行を騙る電子メールや SMS 等を受け取り、フィッシングサイト（偽の銀行サイト）へ誘導された結果、インターネットバンキングの ID やパスワード、ワンタイムパスワード等の情報を窃取され、預金の不正送金を行われた**
- **クレジットカード会社を名乗る送信元から「プライバシーポリシーを変更したため、アカウント情報を確認してください」というメールを受け取り、本文中の URL からアカウント情報とカード情報を入力した結果、身に覚えのないカード利用請求をされた**

**ここがポイント**

- **ID やパスワード、ワンタイムパスワード等の入力を促すメールや SMS 等には注意する**
  **※銀行やクレジットカード会社等が、メールや SMS で上記のような情報を求めることはない**
- **メールや SMS 等の本文に記載された URL にはアクセスせず、予めブックマークした公式サイトから情報を確認する**
- **複数のサービスで ID やパスワードの使い回しをしない**
- **企業が推奨する多要素認証や、FIDO・パスキー・生体認証等の認証方式がある場合は利用する**
- **端末の OS やアプリ・ソフトウェアを最新の状態にアップデートする、携帯電話会社等のセキュリティ設定（迷惑メッセージブロック機能等）を活用する**


**＜参考文献＞**
**●フィッシングとは：フィッシング対策協議会**
**https://www.antiphishing.jp/consumer/abt_phishing.html**
**●フィッシング対策：警察庁**
**https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html**
**●金融犯罪の手口（フィッシング詐欺）：一般社団法人全国銀行協会**
**https://www.zenginkyo.or.jp/hanzai/15300/**

# マンガでわかる サイバーセキュリティ

## SIMスワップ詐欺の手法を知ろう



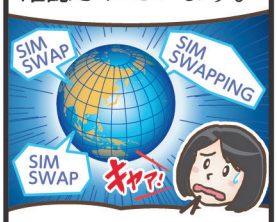




SIMスワップ詐欺とは、攻撃者がフィッシング等で盗んだ個人情報を使って本人を装い、通信キャリアからSIMカードを不正に入手して電話番号を乗っ取る手法です。


SIM スワップが成立すると、SMS や自動音声応答システム（IVR）による認証を突破できるため、それらを利用する他のサービスにも被害が及ぶ可能性があります。

海外では近年この手法による被害が増加しており、既に日本でも被害が確認されています。




電話番号を乗っ取られるなんて怖いね…

まず攻撃者は、標的（被害者）の電話番号・利用している通信キャリア会社・通信キャリアのアカウントID・メールアドレス等の個人情報を様々な方法で収集します。


被害者の個人情報を手に入れた攻撃者は、本人になりすましてSIMカードの再発行やMNP※（Mobile Number Portability）等の手続を行います。


偽造した本人確認書類を持って、実際に店頭へ行って手続をする場合もあります。

被害者の電話番号を制御可能となった（電話番号の乗っ取りに成功した）攻撃者は、その番号宛の電話やテキストメッセージを受け取ることができます。

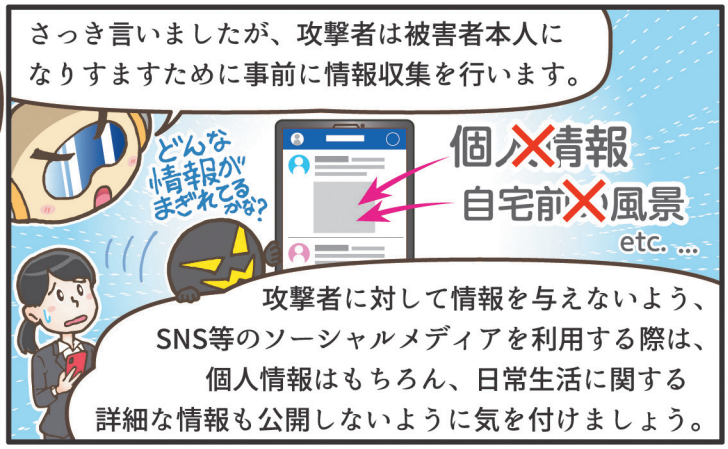

ここまでくると自分のスマホだけ通信が切れちゃうのね。

もし被害者が利用するサービスにSMSやIVRによる認証があった場合は、この手法で突破されてしまいます。


登録している電話番号のSMSに送られたワンタイムパスワードを確認する方法も確かにあるよね。

※使用中の電話番号を変更せずに他の通信キャリア会社へ乗り換えられる制度

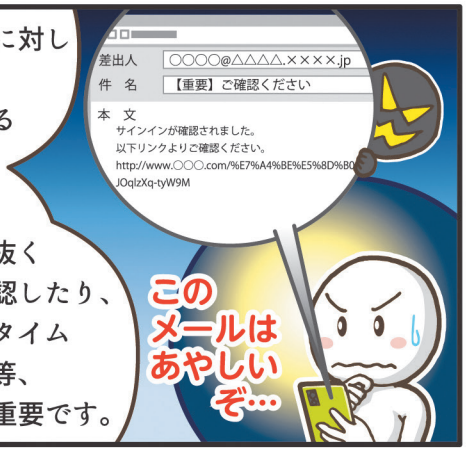

現時点で「こうすれば絶対に大丈夫」という方法はありません。


攻撃者に対して情報を与えないよう、SNS等のソーシャルメディアを利用する際は、個人情報はもちろん、日常生活に関する詳細な情報も公開しないように気を付けましょう。

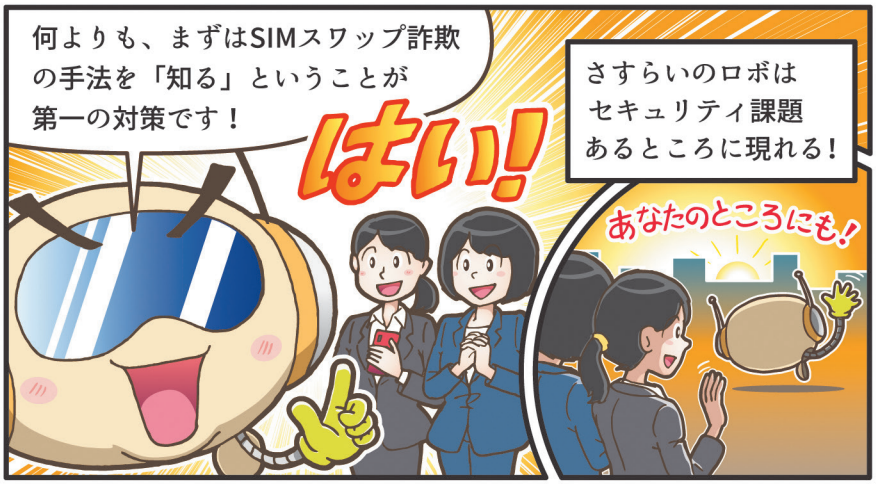
また、攻撃者は被害者に対しメールや電話を使って直接情報を盗もうとする場合もあります。

メールやSMSによるフィッシング詐欺を見抜くポイントや注意点を確認したり、電話で個人情報やワンタイムパスワードを伝えない等、普段からの意識付けも重要です。




サービス利用時の本人確認についても、SMS認証を入れているからといって油断せず、追加認証の方法が他にある場合は、生体認証や認証アプリ、ハードウェアトークン等を利用するのも有効です。


突然スマホの通信が切れた時には、周りの状態を確認して通信障害も疑いつつ、このような詐欺に遭っている可能性まで考えることができると、その後の素早い対応へ繋げられます。


**他の事例**

- ●電話番号が奪われた結果、銀行口座から多額の送金も行われた上に、携帯自体も解約されてしまった
- ●SIM スワップによって影響力のある人物のアカウントが乗っ取られた後、SNS 上で差別的なコメントや投稿を発信されてしまった
- ●2021 年に FBI へ報告された SIM スワップ詐欺の被害額は、6,800 万ドル超と大幅に増加（2018 ～ 2020 年の被害額合計は 1,200 万ドル）

**ここがポイント**

- ●SNS 等のソーシャルメディアには、個人情報を含む内容を投稿しない
- ●電話で個人情報やワンタイムパスワードを伝えない、メールや SMS で受信した不審なリンクや添付ファイルを開かない（フィッシング詐欺に注意する）
- ●利用サービスに SMS や IVR 以外の追加認証方法がある場合は、生体認証や認証アプリ、ハードウェアトークン等を導入する
- ●通信キャリアのアカウントに用いる認証情報は他サービスとの使い回しを避ける
- ●モバイル通信の利用が出来なくなった時や、身に覚えのない通知（ログイン、デバイス有効化、振込等）を受け取った時は、通信キャリア、銀行、クレジットカード等の不正利用についても確認する

＜参考文献＞
●Beware of the Sim Swapping Fraud!：The European Union Agency for Cybersecurity（ENISA）
https://www.enisa.europa.eu/news/enisa-news/beware-of-the-sim-swapping-fraud
●PII（個人識別用情報）を不用意に公開しないようにしよう：国民のためのサイバーセキュリティサイト（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/end_user/general/07/

# マンガでわかる サイバーセキュリティ

## サポート詐欺に気をつけよう

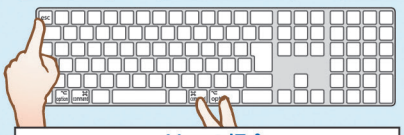
もし、ブラウザや警告画面の「×（とじる）」を押しても表示が消えない場合はこちらの方法も試してみてください。

Ctrl ＋ Alt ＋ Delete

**Windowsの場合**

「Crtl」＋「Alt」＋「Delete」を同時に押して「タスクマネージャ」を起動、利用しているブラウザを右クリックで「タスクの終了」を選択

option ＋ command ＋ esc

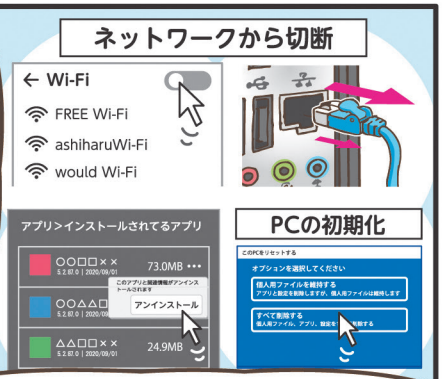


**Macの場合**

「option」＋「command」＋「esc」を同時に押して「強制終了」ウインドウを起動、利用しているアプリを選択し強制終了

それでもダメな場合は、電源ボタンを長押しして PC自体を強制終了するのも方法の一つです。

アプリやソフトウェア等をインストールしてしまった場合、PCをネットワークから切断してウイルスチェックを行い、インストールしたものをアンインストールしてください。




可能であればPCの初期化を行い、各種パスワードを変更するとより安全です。

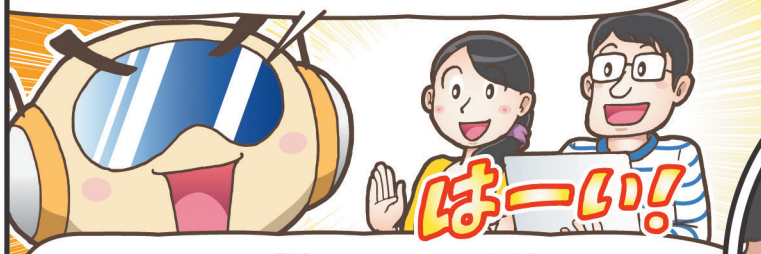
不安なときは、信頼できる正規のサポート窓口への問い合わせや警察等へ相談しましょう。


その際、偽のセキュリティ警告画面やダウンロードしたソフトウェアが分かる資料を保存しておくと、相談時に有用です。

こんな詐欺の手口があるのね。

何も知らなかったら、ただ慌てて電話しちゃってたよ。

まずはこのようなサポート詐欺の手口を知ることが何よりも重要です！そして、万が一自分が被害に遭った時には、落ち着いて正しい対処を取れるように備えましょう。




さすらいのロボはセキュリティ課題あるところに現れる！


そして、ウイルス感染へのリスクを低減させるためのセキュリティソフトの導入やOS・ソフトウェアの更新等の基本的なセキュリティ対策もお忘れなく！

**他の事例**

- ●偽の警告画面にある連絡先へ電話した結果、ウイルス除去の名目でサポート代金をネットバンキングから送金させられた
- ●偽の警告画面の連絡先へ電話をかけたところ、遠隔操作ソフトをダウンロードしてしまい、インターネットバンキングによるサポート代金の送金時に遠隔操作され、金額に桁を付け足されて送金してしまった
- ●サポート詐欺に遭い、修理費用として電子マネーを要求されたので、購入後に番号を伝えたが「間違っている」と言われ、何度も購入して被害が拡大した

**ここがポイント**

- ●インターネット閲覧中にセキュリティ警告画面が出てきた場合は慌てず、画面上の連絡先には絶対に連絡しない
- ●閲覧していたブラウザやアプリを終了する（できない場合はブラウザやアプリ、端末自体の強制終了を利用する）
- ●アプリやソフトウェア等をインストール・ダウンロードしてしまった場合、ネットワークから切断しウイルスチェックを実施の上でアンインストール・削除を行う（可能なら PC の初期化やパスワード変更も実施する）
- ●スクリーンショット等を利用し、偽のセキュリティ警告画面やダウンロードしたソフトウェアの情報を保存する
- ●不安なときは信頼できる正規のサポート窓口や警察等へ相談する


＜参考文献＞
●サポート詐欺対策：警察庁
https://www.npa.go.jp/bureau/cyber/countermeasures/support-fraud.html
●PC やスマホに警告画面が出ても慌てないで！『サポート詐欺』にご注意：政府広報オンライン
https://www.gov-online.go.jp/prg/prg27221.html
●サポート詐欺の手口について（動画解説）：日本サイバー犯罪対策センター（JC3）
https://www.jc3.or.jp/threats/examples/article-356.html

# マンガでわかる サイバーセキュリティ

## 巧妙な詐欺の手口に注意しよう


**他の事例**

- 「カードのチェックが通りませんので、別のカードはありませんか？」等と言って複数枚のクレジットカード情報を得ようとするケース
- 給付金関連の手続きの為に銀行口座の情報が必要と言われ、教えてしまった

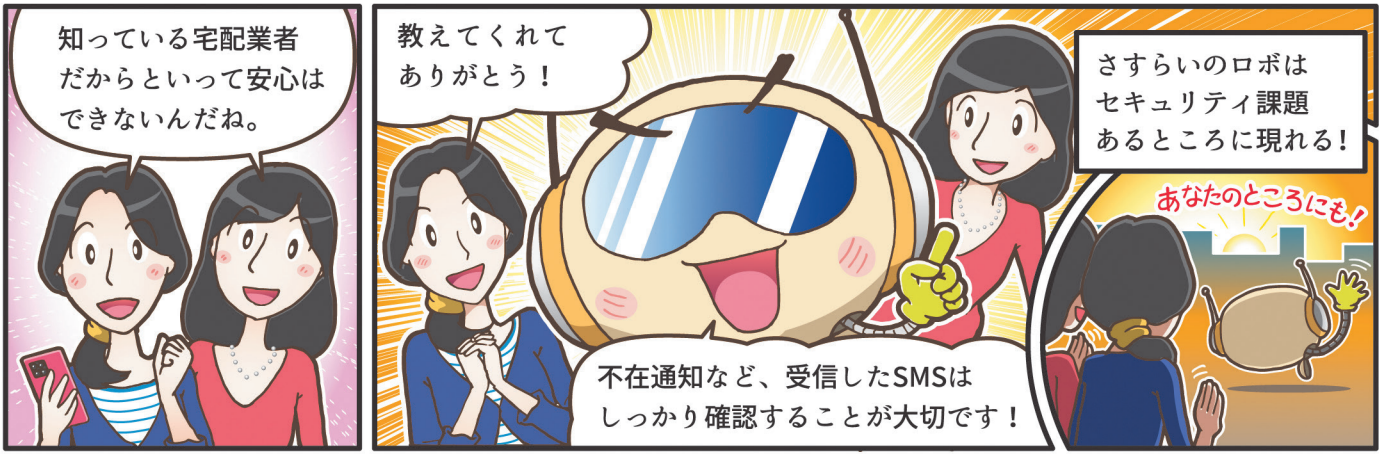
**ここがポイント**

- クレジットカード情報や、確認コードを聞いてくる電話は詐欺の可能性が高い
- 少しでも不安や不信に感じたら情報は伝えず、一度電話を切って公式サイト記載の番号からコールバックする
- 詐欺師は一度のやり取りですべての情報を聞き出すとは限らない。様々な関係者に成りすまし、複数回・複数人で情報を聞き出す可能性がある
- 電話番号の表示は偽装することができるので注意する
- お店しか知りえない情報であっても、店のシステムから漏洩している可能性があることに注意する

# マンガでわかる サイバーセキュリティ

## 不審なSMSに注意しよう（不在通知編）






**他の事例**

- クレジットカード会社を装った SMS に記載された電話番号に返電し、個人情報を伝えてしまった
- 携帯会社を装った SMS に記載された URL から、ID・パスワードや暗証番号を入力してしまった
- インストールされた不審アプリが、電話帳や連絡先を盗み、そのスマホから SMS を送り続けるケースもある

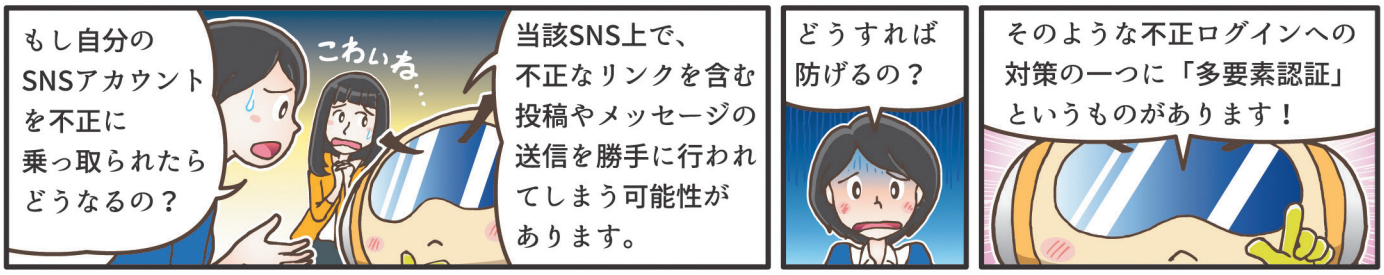
**ここがポイント**

- SMS の URL を安易にクリックしない
- パスワードや認証コード等を安易に入力しない
- 身に覚えのない連絡先であれば、公式サイト等をインターネットで調べる
- パソコンだけではなく、スマホにもセキュリティソフトをインストールする
  偽物のセキュリティソフトもあるので注意（公式サイトからダウンロードする）

＜参考文献＞
●宅配便業者をかたる偽ショートメッセージに引き続き注意！：独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/anshin/attention/2020/mgdayori20200220.html

# マンガでわかる サイバーセキュリティ

## SNSアカウントの乗っ取りに気をつけよう




多要素認証とは、「記憶」「所持」「生体」の情報から複数の要素を用いた認証方式のことです。

| 要素 | 例 |
|---|---|
| 記憶情報 Something You Know | ●パスコード ●PINコード ●秘密の質問 |
| 所持情報 Something You Have | ●携帯電話 ●ハードウェアトークン ●ICカード |
| 生体情報 Something You Are | ●指紋 ●静脈 ●声紋 |

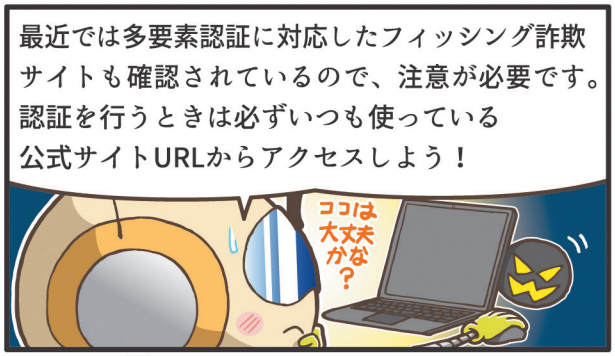
① ID、パスワードによる認証

ID maru@batsu.com　PW ●●●●●●●　1項目目 記憶情報の利用

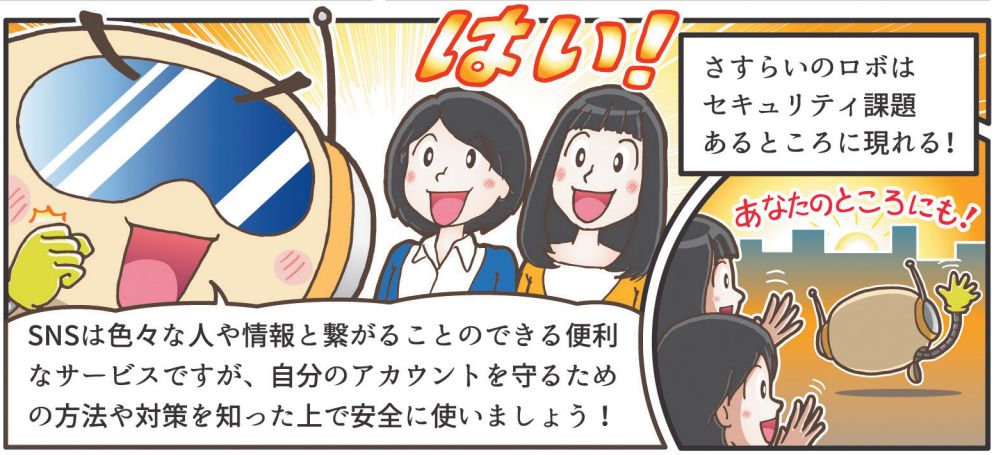
② 指紋による認証

2項目目 生体情報の利用

例えば、IDとパスワード（記憶情報）による認証に加え、顔認証や指紋認証（生体情報）によって初めてログインが完了するといったものです。






**他の事例**

- ●知り合いになりすました人物と気づかずチャットでやり取りを行い、個人情報（電話番号、メールアドレス等）を盗取されてしまった
- ●宅配業者や EC 業者を騙ったメールを受信し、メッセージ内の不正なリンクへと誘導されてしまった
- ●リンクを見た目で判断できないよう、短縮 URL（Web サイトの URL を短く変換したもの）を利用するケース

**ここがポイント**

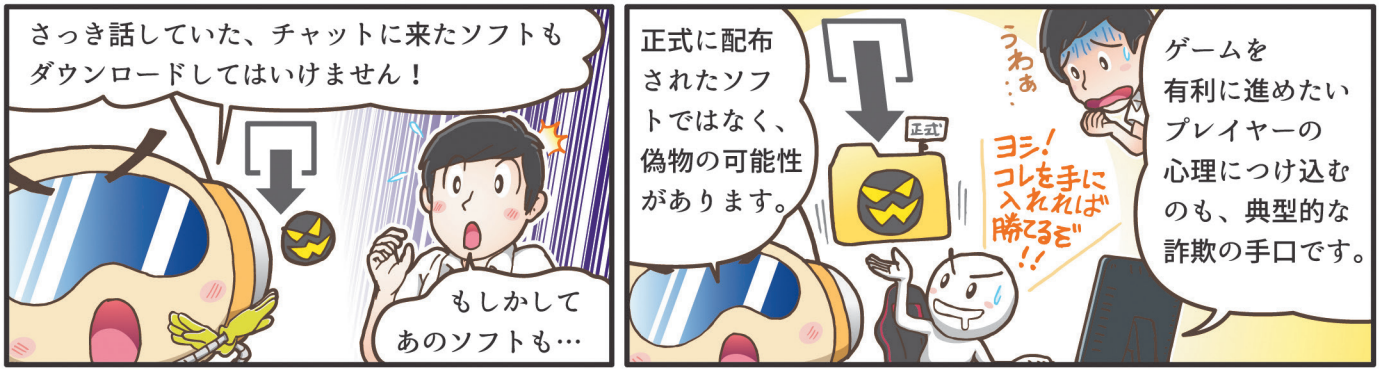
- ●SNS のログイン認証には、多要素認証を利用する
  - 例１）X（旧 Twitter）：パスワード＋ 認証アプリ、確認コード（SMS）、セキュリティキー
  - 例２）Apple：パスワード＋ 確認コード（SMS）/ 自動音声案内 等
  - 例３）Google：パスワード＋ 認証アプリ、確認コード（SMS）/ 自動音声案内、セキュリティキー 等
- ※ご利用の際は各社の公式 HP 等で最新の情報をご確認ください

＜参考文献＞
●不正ログイン対策特集ページ：独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/anshin/account_security.html
●不正アクセス対策：警察庁
https://www.npa.go.jp/bureau/cyber/countermeasures/unauthorized-access.html
●公式アカウントが乗っ取られた：国民のためのサイバーセキュリティサイト（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/case/business/07/

# マンガでわかる サイバーセキュリティ

## オンラインゲームを利用するときのリスクを知ろう





**他の事例**

- **発売前のゲームを無償で入手できるという偽サイトからファイルをダウンロードし、入手する条件としてアンケートの回答を促された結果、入力した個人情報を窃取された**
- **ゲーム内で個人間の取引を行い、お金と引き換えにアイテムを貰う約束だったが、先払いしたお金だけ持ち逃げされた（ゲームによっては利用規約でゲーム内での通貨やアイテムの取引を禁止している場合があるので確認する）**

**ここがポイント**

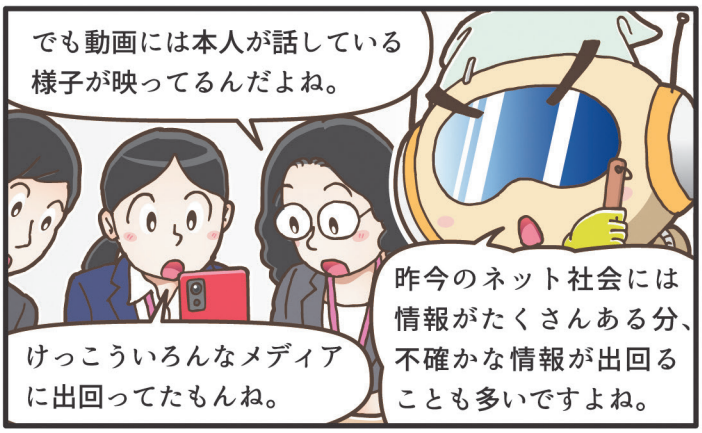
- **PC やスマートフォンにゲームをダウンロードするときは、運営元の公式サイトや公式アプリストアから行う**
- **ダウンロードする前に、レビュー・開発者や開発元・注意喚起等の情報取集を行う**
- **見知らぬ人とのコミュニケーションは慎重に行い、チャット内の URL リンクやファイルを開かない**
- **システムやアプリは最新の状態を保ち、セキュリティ対策ソフト（アプリ）を導入する等の基本的な対策も実施する**
- **家族でパソコンを共有する場合、情報漏洩を防ぐため、個々で作成したユーザ権限のアカウントを利用する**


**＜参考文献＞**

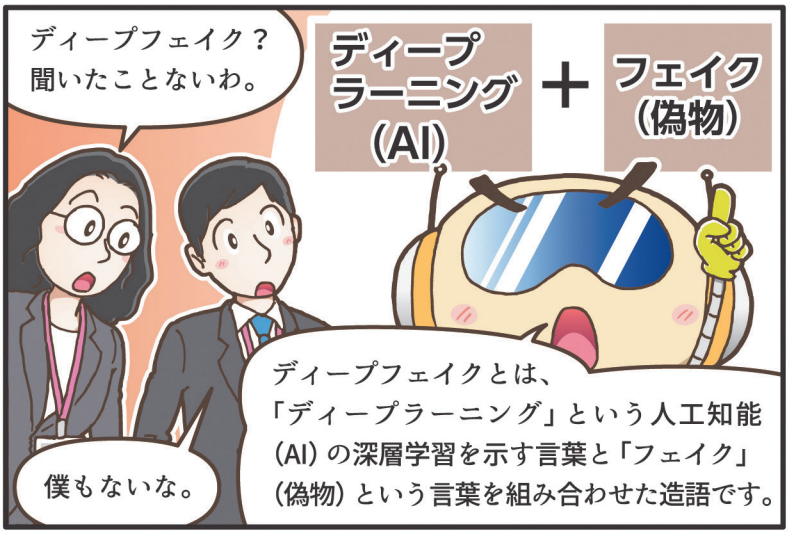
**●スマートフォンを利用している方へ：警視庁**
**https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/security/cyber414.html**
**●オンラインゲーム利用時の注意点：滋賀県警察**
**https://www.pref.shiga.lg.jp/police/seikatu/304409/304411/311552.html**

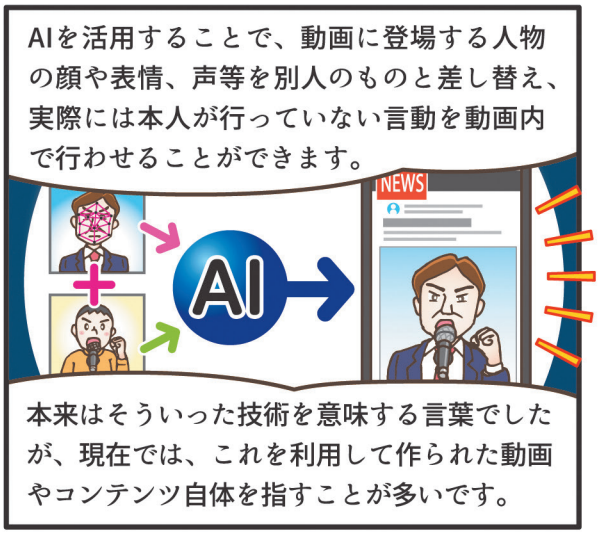
# マンガでわかる サイバーセキュリティ

## 情報の正しさを自分で確認しよう

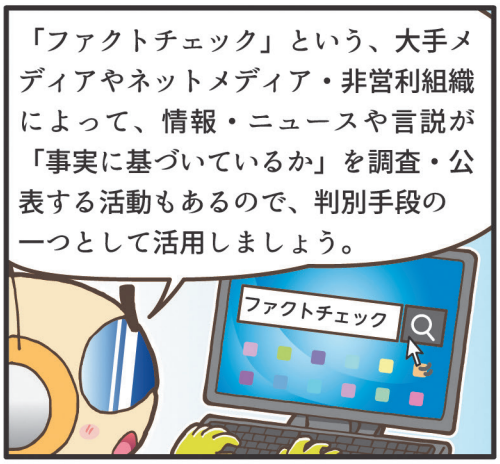












**他の事例**

- **子会社の CEO が親会社の CEO を偽ったディープフェイクボイス攻撃に遭い、偽物と気づかずに 22 万ユーロを送金してしまった**
- **画像生成 AI を用いて、偽の水害画像を意図的に作成し、インターネット上でデマが拡散された**
- **首長選挙において、世論操作等を目的としたフェイクニュースがソーシャルメディアへ投稿される**
- **地震発生直後に「動物園のライオンが脱走した」というフェイクニュースが画像と共に拡散し、投稿した男性が逮捕された**

**ここがポイント**

- **目にした情報は不確かかもしれないという意識を持って鵜呑みにせず、正確性を自分で判断する**

**(確認方法の例)**
- **他の Web サイトや新聞、本など、他の情報源との比較を行う**
- **情報の発信元(人・Web サイト)や一次情報(オリジナル情報の発信時期や情報源)を確かめる**
- **大手メディアやネットメディア・非営利組織によるファクトチェックサイトを利用する**

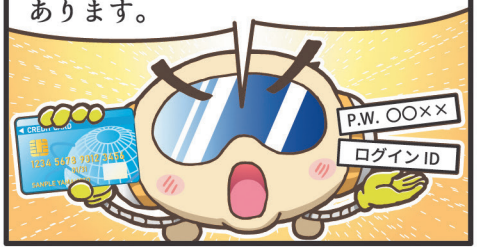

**＜参考文献＞**

**●(特集ページ)インターネット上に流通する真偽の不確かな情報 / 安心・安全なインターネット利用ガイド：総務省**
**https://www.soumu.go.jp/use_the_internet_wisely/special/fakenews/**
**●FactCheck Navi：認定 NPO 法人ファクトチェック・イニシアティブ(FIJ)**
**https://navi.fij.info/**
**●Bellingcat(ベリングキャット)：イギリスに本拠を置く、非営利の調査報道機関及びその Web サイト**
**https://www.bellingcat.com/**

# マンガでわかる サイバーセキュリティ

## 偽情報に注意しよう

加えて、**偽サイトに入力したクレジットカード番号や個人情報を窃取**された結果、他の犯罪に利用されてリスクが拡大する可能性もあります。




タイムセールみたいに制限時間があると判断が鈍るな…


攻撃者は我々を**心理的に惑わせる手口**を用いるので、**冷静に情報を確認する**ことが重要です！

確認といっても見分け方はあるの？

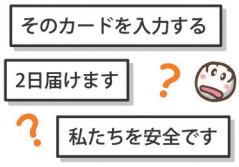

その情報を他の方法で検索して、二次情報を探すことで真偽を確かめることも可能です。

また、このような点は偽サイトの特徴となることがあるので、特に注意しましょう。


販売価格が極端に値引きされていたり、大幅な割引率が適用されている


サイトのURL表記が正式な英語表記と少し異なる等、違和感がある


サイト内のリンクが適切に機能しない




記載されている文章や表現が不自然


決済手段が限定されている（クレジットカードのみ、銀行振込のみ、代金引換のみ等）

こういう特徴もあるのか。参考にするよ！

他にも、実店舗の有無を確認することもリスクを減らすための方法の一つです。

写真やロゴが本物のように見えても、簡単に信用してはいけません。もし詐欺に引っ掛かってお金を盗まれてしまったら勉強料ではすみませんよ！

これからは目先の情報に惑わされないように気を付けます！

さすらいのロボはセキュリティ課題あるところに現れる！


**他の事例**

- **通販サイトにてクレジットカードで決済を行ったが商品が届かず、そのクレジットカードを不正利用された**
- **ショッピングサイトで買い物したところ粗悪品が届き、記載された連絡先に電話やメールをしたが繋がらない**
- **SMS のメッセージに記載された URL をクリックすると出会い系サービスの入会契約成立と表示され、入会金の支払いを要求された**

**ここがポイント**

- **インターネットに出てきたポップアップが不審な場合は、その内容を検索し二次情報を取得してその真偽を確かめる**
- **以下のような偽サイトの特徴に注意する**
  - **販売価格が極端に値引きされていたり、大幅な割引率が適用されている**
  - **サイトの URL 表記が正式な英語表記と少し異なる等、違和感がある**
  - **サイト内のリンクが適切に機能しない、日本語の字体や文章表現が不自然**
  - **決済手段が限定されている（クレジットカードのみ、銀行振込のみ、代金引換のみ等）**


**＜参考文献＞**

**●その通販サイト本物ですか！？“偽サイト”に警戒を！！－最近の“偽サイト”の見分け方を知って、危険を回避しましょう！－：独立行政法人国民生活センター**
**https://www.kokusen.go.jp/news/data/n-20230130_1.html**
**●偽ショッピングサイト・詐欺サイト対策：警察庁**
**https://www.npa.go.jp/bureau/cyber/countermeasures/fake-shop.html**
**●フリマアプリの商品が届かない：国民のためのサイバーセキュリティサイト（総務省）**
**https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/case/end_user/04/**


Memo