第1章

まずはサイバーセキュリティの基礎を固めよう

サイバー攻撃を受けないようにするため、まずは基礎的なセキュリティの固め方を理解しましょう。スマホやパソコンを最新の状態にすること、安全なパスワードの管理方法、もしものときのバックアップの必要性など、攻撃する側からのサイバー攻撃を防ぐためにはどうすればよいかを学びましょう。

1 最低限実施すべきサイバーセキュリティ対策を理解しよう

2 ①OSやソフトウェアは常に最新の状態にしておこう

2.1 パソコン本体とセキュリティの状態を最新に保とう

2.2 スマホやネットワーク機器も最新に保とう

3 ②パスワードは長く複雑にして、他と使い回さないようにしよう

3.1 パスワードってなに？

3.2 パスワードの安全性を高める

3.3 機器やサービス間でのパスワード使い回しは「絶対に」しない

3.4 秘密の質問は注意する

3.5 パスワードを適切に保管する

4 ③多要素認証を利用しよう

4.1 可能な限り多要素や生体認証を使う

4.2 パスワードはどうやって漏れるの？どう使われるの？

5 ④偽メールや偽サイトに騙されないように用心しよう

5.1 多様化する偽メールに注意しよう

5.2 信頼できるサイト以外からアプリをインストールすることは控えよう

コラム.1 災害時の情報収集

コラム.2 スマホによる災害時の情報収集

6 ⑤メールの添付ファイルや本文中のリンクに注意しよう

7 ⑥スマホやパソコンの画面ロックを利用しよう

7.1 スマホやパソコンには必ず画面ロックをかけよう

7.2 よくある情報の漏れ方と対策

8 ⑦大切な情報は失う前にバックアップ(複製)しよう

8.1 何をするにもバックアップを取ろう

8.2 ランサムウェアや天災にも対応できるバックアップ体制

9 ⑧外出先では紛失・盗難・覗き見に注意しよう

10 ⑨困ったときは1人で悩まず、まず相談しよう

コラム.3 攻撃されにくくするには、手間(コスト)がかかるようにする

コラム.4 利益が目的ではない攻撃に備えるには

コラム.5 セキュリティソフトを導入しても過信しないことが重要

コラム.6 セキュリティ要件適合評価及びラベリング制度(JC-STAR)

コラム.7 偽ショッピングサイトに注意しましょう

1 最低限実施すべきサイバーセキュリティ対策を理解しよう

攻撃者▶用語集P.182（悪意のハッカー▶用語集P.179）による攻撃を防ぐには、まずはパソコンやスマホの基本的なセキュリティを固め、また、トラブルが発生したときの対処手段を知ることが重要です。

現在、政府機関が掲げるサイバーセキュリティ対策の指針としては、NISC▶用語集P.177（内閣官房内閣サイバーセキュリティセンター▶用語集P.185）が「サイバーセキュリティ対策9か条」を公開しています。一般国民の誰もが最低限実施すべき対策をまとめており、本ハンドブックもこの9か条に則ってサイバーセキュリティ対策を解説していきます。

まず「**① OSやソフトウェアは常に最新の状態にしておこう**」はいわゆるアップデート▶用語集P.179のことです。IT機器にはセキュリティホール▶用語集P.184と呼ばれる弱点が日々見つかっています。一見、大丈夫そうに見えてもそれは「ただセキュリティホールが発見されていない」だけ。OS▶用語集P.177やソフトウェアメーカーが提供している修正用アップデートを常に適用し続け、攻撃の糸口となる穴を塞ぎます。

「**②パスワードは長く複雑にして、他と使い回さないようにしよう**」は、安全性の高いパスワード▶用語集P.186を設定する際の留意点、同じパスワードの使い回し▶用語集P.186の危険性、パスワードの適切な管理方法について解説します。

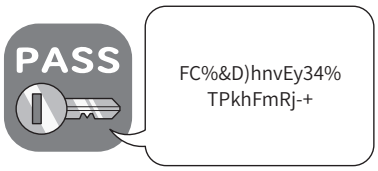
「**③多要素認証を利用しよう**」は、サービスへのログイン▶用語集P.189を安全に行うために、二要素以上を使って認証作業をする多要素認証▶用語集P.184について解説します。認証用アプリや生体認証▶用語集P.183を利用するとログインの安全性を高められます。

「**④偽メールや偽サイトに騙されないように用心しよう**」は、フィッシング詐欺メールが多様化しており攻撃が複雑になっていることや、信頼できるサイト以外からアプリ▶用語集P.179をインストール▶用語集P.180する危険性を解説します。

①OSやソフトウェアは常に最新の状態にしておこう

OSやソフトウェアを最新に状態にする理由は、最新の攻撃情報への対策が盛り込まれているからです。

②パスワードは長く複雑にして、他と使い回さないようにしよう



安全なパスワードの作成方法はもちろん多要素認証の重要性を説明します。

③多要素認証を利用しよう

認証用アプリや生体認証を利用したより安全性の高い多要素認証について説明します。

④偽メールや偽サイトに騙されないように用心しよう

多様化・複雑化するフィッシング詐欺メールや、信頼できるサイト以外からアプリをインストールする危険性について解説します。

「**⑤メールの添付ファイルや本文中のリンクに注意しよう**」は、「Emotet」のように、マルウェア▶用語集 P.188 添付メールで広がる感染、標的型メール▶用語集 P.187 やスパムメール▶用語集 P.183 の実例を挙げ、具体的リスクについて解説します。

「**⑥スマホや パソコン の画面ロックを利用しよう**」は、スマホやパソコン（PC）の情報を守るにはまず待ち受け画面をロック▶用語集 P.189 することが第一であることを解説します。また、生体認証を使用したロックの利点や、安易に他人へ端末を渡す危険性についても触れます。

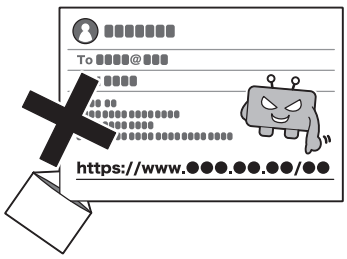
「**⑦大切な情報は失う前にバックアップ（複製）しよう**」は、普段からバックアップ▶用語集 P.186 をとっておくことがどれほど重要か解説します。正常な状態のファイルをバックアップして保管しておくことで、仮に攻撃を許して重要なファイルを失ってしまっても、バックアップから復元▶用語集 P.187 することにより、被害を軽減します。とくに昨今増加しているランサムウェア▶用語集 P.188 攻撃に対してもバックアップを準備しておくことは有効です。

「**⑧外出先では紛失・盗難・覗き見に注意しよう**」は、勤務先や外出先でスマホやパソコンを使う際、覗き見されるショルダーハッキング▶用語集 P.183 などのリスクなどについて解説します。また、飲食店などで離席時に端末を置いていく人を時折見かけますが非常に危険な行為です。公衆の場でスマホやパソコンを利用するときに注意すべきことについて把握しましょう。

「**⑨困ったときは１人で悩まず、まず相談しよう**」は、サイバー攻撃▶用語集 P.182 などインターネットの被害で自分だけでは対処できないときには、積極的に警察や IPA などの窓口へ相談する重要性を解説します。あらかじめ窓口を調べておくことで、困ったときにすぐに相談できるようになります。

*「サイバーセキュリティ９か条」https://security-portal.nisc.go.jp/guidance/cybersecurity9principles.html

⑤メールの添付ファイルや本文中のリンクに注意しよう

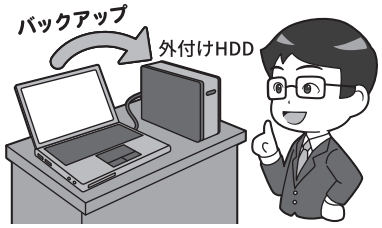


被害がなくならない「Emotet」、標的型メール、スパムメールの実例を紹介

⑥スマホやパソコンの画面ロックを利用しよう

スマホやパソコン（PC）の情報を守るにはまず待ち受け画面をロックすることが第一。そして生体認証が推奨

⑦大切な情報は失う前にバックアップ（複製）しよう

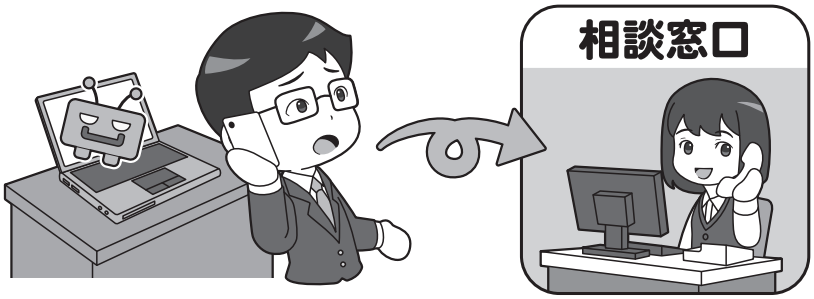


たとえ攻撃されても、適切にバックアップしておけば、すぐに復旧できます。

⑧外出先では紛失・盗難・覗き見に注意しよう

公衆の場における、ショルダーハッキングのリスク、スマホやパソコンの紛失・盗難など、利用時の注意すべきことを把握しましょう。

⑨困ったときは１人で悩まず、まず相談しよう



攻撃されたとき、どうしたらよいか分からないからとそのまま放置せず、相談窓口に相談しましょう。また、実質的な被害が出ている場合は、警察などの関係機関に報告した方がよい場合もあります。いざというとき慌てないように、あらかじめ連絡先を調べておきましょう。

2 ①OSやソフトウェアは常に最新の状態にしておこう

2.1 パソコン本体とセキュリティの状態を最新に保とう

悪意の攻撃からパソコンを守る第一歩は、セキュリティを最新に保ち、各種のアップデート（バージョンアップ▶用語集P.186）を行うことです。

最近の機種では、OS関連のアップデート処理は自動で行われるか、アップデートを行うよう通知が出るようになっています。しかし、緊急でアップデートを行った方がよいときもあります。セキュリティ関連ニュースサイトなどでアップデートを促す情報が流れていたら、自主的に更新処理をかけるようにしましょう。Office製品▶用語集P.177などOSのメーカーが作っている重要なソフト▶用語集P.184もここで同時にアップデートします。

次に、サイバー攻撃で狙われやすいソフトウェアの更新を重点的に行いましょう。Adobe社Acrobat ReaderやOracle社Javaまたはその実行環境、そしてGoogle Chromeをはじめとする各種のウェブブラウザ▶用語集P.180や、ブラウザ▶用語集P.188の機能を拡張するプラグインは攻撃のターゲットになりやすいのです。

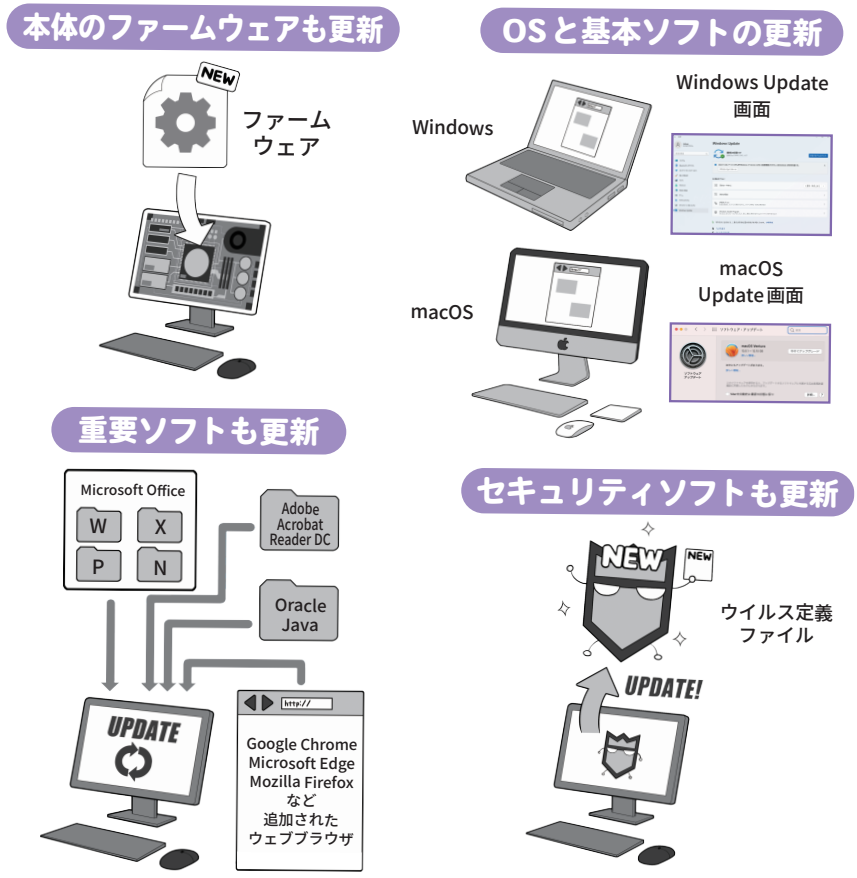
また、機器そのものの基本プログラムを更新するファームウェア▶用語集P.187アップデートにも気を配りましょう。こちらの更新通知は、自動で出る機器と出ない機器があるので、機器のアップデート情報は、どのようにすれば入手できるか、事前に確認して気を配ってください。（本章コラム5(P.51)参照）

セキュリティソフト▶用語集P.183をインストールしている場合は、最新のウイルス定義ファイル▶用語集P.180に自動更新されるよう設定しておきましょう。

なお、OSやソフトウェア、ファームウェアは、開発者がアップデートの期限を設定するものが多く、この期限を過ぎるとアップデートが提供されなくなります。

アップデートが提供されなくなったOSやソフトウェアは、セキュリティホールが見つかっても修正用アップデートが提供されず、攻撃に対して非常にぜい弱なので、使用しないようにしてください。

本体もOSもセキュリティソフトも重要ソフトもアップデート



OSやファームウェアなどは、ほとんどのパソコンで利用されており、社会でいえば鉄道や電気ガス水道のような社会インフラに相当します。

利用する側もアップデート（更新）が必要になれば速やかに適用して、攻撃者が攻撃できないようにしましょう。インストールしてあるが使っていないソフトは削除（アンインストール）してしまってもよいでしょう。

ボットネットも、そもそも攻撃して乗っ取れる機器がなければ成立しないように、攻撃できる穴を作らない1人1人の行動が、安全なインターネットを作り社会インフラを支えるのです。

2.2 スマホやネットワーク機器も最新に保とう

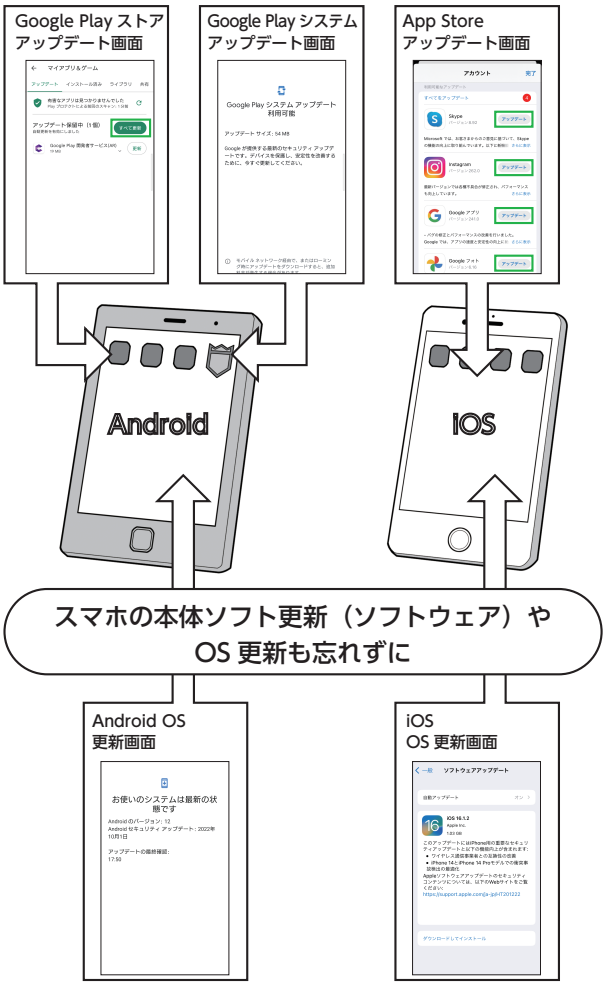
スマホも同様に各種のアップデートの適用が必須です。スマホの場合、比較的アップデートの通知がわかりやすくなっており、自動アップデート機能も充実しています。機器本体のファームウェアのアップデートでも、OSのアップデートでも、いつも使用している一般のアプリのアップデートでも、更新の通知が出たら、マメに適用するようにしましょう。

そのためには、本体のファームウェア(ソフトウェア更新やシステムアップデートと書かれることも)やOSの更新が、設定メニュー上のどこにあるのかと、更新の手順を確認しておきましょう。アプリの更新が自動になっているかも確認しましょう。すでに保守期間等がすぎて、ファームウェア等が更新できない場合には、以降の安全性が確保されないため、買い替え等も検討しましょう。

スマホアプリの自動更新は、設定によっては無線LAN ▶用語集 P.188 接続時のみ自動で行うことになっている場合もありますが、その設定でも更新時に権限▶用語集 P.181 変更で確認が必要な場合は自動更新されないこともあるので、気が付いたら未更新のアプリがたくさんたまったままになってしまっていることもあります。日に一度は意識してアップデート画面に行き、更新するように心がけましょう。

また、ネットワークにつながるルータ▶用語集 P.189 やIoT機器、スマート家電▶用語集 P.183、ネットワークカメラ▶用語集 P.186 などもぜい弱性▶用語集 P.183 を狙った攻撃の対象となるため、ファームウェアが自動更新されるよう設定しておきましょう。近時は国際情勢の影響もあり、更新されていないネットワーク機器を狙う攻撃が増加しました。ルータはここ数年で自動更新機能搭載のものが普及してきているので、可能であれば買い換えましょう。

アプリやセキュリティソフトの更新は自動更新にしつつ、まめにチェック



ネットにつながるIT機器(ルータやIoT機器)もファームウェア更新や管理者用初期IDとパスワードの変更をしておくこと

無線LANアクセスルータ　ネットワーク対応プリンタ　ネットワークカメラ

IoT機器のファームウェアの更新は、通常はウェブブラウザで本体にアクセスして行います。このときの管理者用IDとパスワードは、必ず購入時の初期のものから変更しておきましょう。同じ機種で共通だった場合など、不正アクセスされ乗っ取られてサイバー攻撃に使われます。

3 ②パスワードは長く複雑にして、他と使い回さないようにしよう

3.1 パスワードってなに？

私たちが、スマホやパソコンなどのIT機器や、各種のウェブ▶用語集 P.180サービスを使う上で、欠かせないのが「パスワード」です。

機器やウェブサービスを利用するときに、正当な利用者や持ち主である自分だけが利用でき、他人が利用できないようにするための鍵の役割を果たすものです。

パスワードは、いわば「家の鍵」や「金庫の鍵」。これを適切に守らなければ、家や車、金庫を勝手に開けられてしまうように、パソコンやスマホ、ウェブサービス上にある私たちの個人情報▶用語集 P.182やメール、銀行口座が攻撃者に不正にアクセスされ、情報が流出したり、お金を盗まれたりしてしまいます。

3.2 パスワードの安全性を高める

サイバー攻撃には、相手の機器をマルウェアに感染させて乗っ取る方法の他に、なんらかの手段でID▶用語集 P.177とパスワードを解明し、サービスや機器を乗っ取る方法もあります。

パスワードは利用しているウェブサービスなどから大量流出したものが使われる「リスト型攻撃▶用語集 P.189」、文字の組み合わせをすべて試す「総当たり攻撃▶用語集 P.184」、パスワードによく使われる文字列を利用する「辞書攻撃▶用語集 P.182」などにより探し当てる方法や、IoT機器のパスワードを購入時のまま利用していると乗っ取られることもあります。

総当たり攻撃を防ぐには、探り当てるまでに膨大な時間がかかるようにするのが一番の防御手段で、それには1桁の文字の種類と桁数による組み合わせを増やします。例えば数字だけなら1桁10通りしかありませんが、英字を入れると36通り、英大文字小文字を入れると62通り、これに33文字の記号を入れると95通りになります。これに桁を増やして、累乗で組み合わせを増やすわけです。総当たり攻撃は、理論上攻撃し続ければいつかは成功するのですが「時間がかかり事実上不可能な状態」にして防ぐのです。長いが覚えやすいパスワードにするか、短いが複雑なパスワードにするかは、好みの問題ともいえますが、最近では、桁数をできるだけ長くする方が安全であると言われています。さらにより安全にしたい場合には記号を入れることで安全性を高めるに、こしたことはありません。

ログイン用パスワードは、長くすることでより安全に

「数字＋英大文字＋英小文字」の8桁だと→約218兆通り
「数字＋英大文字＋英小文字」の12桁だと→約32垓通り

同じ文字種でも、パスワードを長く設定することで推認されにくくなります。

数字＋英大文字＋英小文字の組み合わせ数（例）

数字	英大文字	英小文字	合計	8桁（通り）	12桁（通り）	8桁と12桁の比較（倍）
10	26	—	36	2,821,109,907,456	4,738,381,338,321,616,896	1,679,616
10	26	26	62	218,340,105,584,896	3,226,266,762,397,899,821,056	14,776,336

3.3 機器やサービス間でのパスワード使い回しは「絶対に」しない

複雑なパスワードを使っても、それを複数のサービスや機器の間で使い回していれば意味がありません。1カ所から漏れればすべてのサービス等でログイン可能になってしまうからです。複雑なパスワードを1つ決めて、あとはおしりに数字や規則性のある文字を付けるのも、2つ以上漏れれば推測されます。それぞれに複雑なパスワードを設定し、使い回しをしないことが大切です。但し実際にすべての規則性のないパスワードを記憶することは、難しいため、本章3.5(P.33)に示すような形で適切なパスワード管理をすることが重要です。

同じパスワードを使い回さない。似たパスワード、単純な法則性のあるパスワードも×

	白うさ ネットワーク	おさるさん 銀行	三毛猫電気	
×使い回し	PASSPPOI	PASSPPOI	PASSPPOI	1個漏れたら一網打尽
×単純な法則性あり	USAGIPPOI	OSARUPPOI	NEKOPPOI	法則性がばれたらおしまい

3.4 秘密の質問は注意する

ウェブサービスの中には、パスワードを忘れてしまった場合や、あるいはいつもと違うログインがあった場合の本人確認のために「秘密の質問」▶用語集P.187と呼ばれる機能で対応しようとするものがあります。これはあらかじめ利用者が、自分しか知らない質問と答えを設定しておいて、合い言葉的にこれに答え、本人であることを証明するものです。

しかしこの秘密の質問は、自分で質問を作れるものもありますが、多くは「生まれた市は」、「ペットの犬の名前は」と回答が類推しやすいものが大半です。

SNS▶用語集P.178が普及した今、SNSの過去の投稿から簡単に見つけられることもあり、安全性が高いとはいえません。

秘密の質問に答えを設定する場合は推測できないものにし、忘れないようにパスワード管理アプリ▶用語集P.186などに保存しましょう。

3.5 パスワードを適切に保管する

使い回しをせず充分な複雑さと長さを持ったパスワードは、総当たり攻撃では突破されにくくなります。

しかし、適切に管理しておかず、別の方法で盗まれてしまってはひとたまりもありません。

例えばパソコンや壁に貼っていれば、誰かがそれを見て覚えてしまいますし、テキストファイルにまとめておけばマルウェアに感染したときに流出し、多くのアカウントが一気に乗っ取られるかもしれません。

パソコンでウェブブラウザにパスワードなどを覚えさせる「自動入力」機能も要注意です。あなたが席を離れた隙に、誰かがブラウザでウェブサービスを利用してしまうかもしれません。それにノートパソコンならば本体ごと盗まれることもあります。パスワードは基本的に利用する場所で保管してはいけないのです。

しかし、多くのサービスで複雑なパスワードをそれぞれ設定したら、とても覚えきることはできません。ではどうしたらよいでしょう。

具体的にはいくつかの方法が挙げられます。例えば、パスワードを管理する紙のノートに書いてパソコンとは別に保管する方法や、アプリのメモ帳や表計算ソフト等で管理するなどで管理する方法が挙げられます。またスマホのパスワード管理アプリを利用したり、ブラウザのパスワード管理機能を利用したりする方法なども挙げられます。なお、紙で管理する場合以外は、クラウド▶用語集 P.181でデータを保管する機能の利用は熟考し、過去に情報流出にまつわるトラブルのあったアプリやサービスは利用を避けるようにしましょう。それは他人の手元にIDやパスワードを保管することや、流出の危険が逆に増すことを意味するからです。

利用するところで保管するべきでないなら、スマホでパスワードを管理する場合リスクはありますが、こういったアプリは後述のPINコード▶用語集 P.177（第5章 1(P.99)参照）や生体認証＋暗号化▶用語集 P.179で情報がガードされます。盗まれても落としても、簡単に他人が使ったりすることはできません。

ただ、管理しているパスワードは、必ずバックアップするのを忘れないようにしましょう。

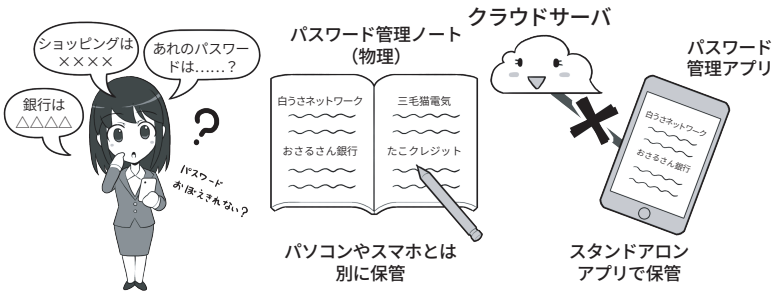
なお、紙で保存する場合には、紛失に備えて、予備を作成・保管しておき、その予備を参考にしながら早急にパスワードを変更することが必要です。また、パスワードを記録する際には、盗み見した者が記録されたパスワードを使用して、すぐに悪用できてしまう可能性を少しでも下げる工夫を施しておくと、より安全にパスワードを保管できます。

具体的には「実際には含まれない余分な文字を混ぜてノートに記録する」、「実際のパスワードは前後どちらかに2,3桁程度、暗記できる数の文字が追加されたものに設定して、すべての文字はノートに書き残さない」などがあります。

パスワードを使用する場所に置かない。パソコンの中も×

オフィスの中ならば外の人は見ないと判断するのは×。出入りの業者が見たり、外から双眼鏡で見たりすることもできるのです。内部の人間が勝手に使うリスクもあります。

パスワードは紙のノートに書いて保管するか、パスワード管理アプリで守る



クラウド保管＝ダメというわけではなく、それは利便性との兼ね合いです。アプリのバグや過去のトラブルは、アプリ名＋「トラブル」などで検索します。

4 ③多要素認証を利用しよう

4.1 可能な限り多要素や生体認証を使う

サービスへのログインを安全に行うために、二要素以上を使って認証作業をする多要素認証などの方法が提供されていれば必ず設定しましょう。

例えば、最近の機器では顔、虹彩▶用語集 P.182、指紋で本人確認をして機器のロック状態を解く、生体認証機能もあります。

生体認証は本人のみが使えて安全性が高く、肩越しの盗み見などよる暗証番号(PIN コード)の盗難には強い機能でもあります。ただ指紋認証などは寝ている間に勝手にロック解除されることがあり得るので過信は禁物です。

なお、生体認証はたいていは通常の PIN コードの替わりなので、スマホでは失敗すると通常の PIN コード入力に戻ります。誕生日などの個人情報を PIN コードにすると予想がされやすく、本体を盗まれてロック解除される可能性が上がるため使わないようにしましょう。

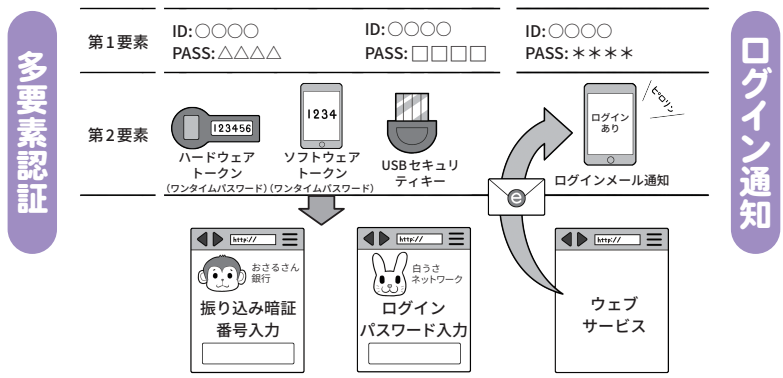
また通常のパスワードの他に、使い捨てにする別のパスワードを、ハードウェアトークン▶用語集 P.186 や生成アプリで作り、ログイン時に利用者に入力させます。なお、メールや SMS ▶用語集 P.178(ショートメッセージ。以降 SMS)を利用する方式もありますが、これらはその送信方法などによっては安全面で十分とは言えない場合があります。例えばウェブ上のサービスに対して、特定のスマホに対して SMS が送信される場合にはスマホを所持している人しかわからない情報なので、二要素認証として位置づけられますが、ウェブサービスに登録しているメールアドレスに送信される場合、安全性は低いと言えます。

その他、認証システムによっては、スマホなどへのプッシュ通知を多要素認証に組み入れることがあります。

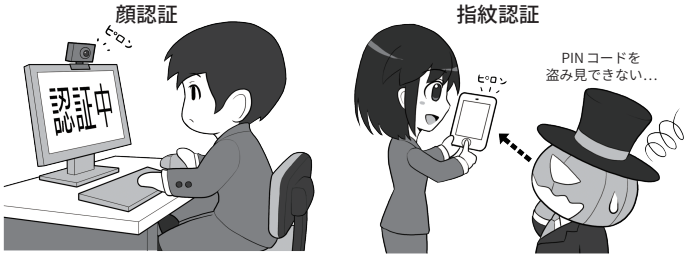
攻撃者がパスワードなどでの認証を成功させた場合にもプッシュ通知が送られるので見知らぬプッシュ通知には回答してはいけません。

その他にも、USB セキュリティキー▶用語集 P.178 などで利用者を確認する方法や、不正アクセス▶用語集 P.187 の兆候を知る手段として、サービスに不審なログインがあったときにメールで利用者に通知を送る機能も存在するので、あれば活用しましょう。

多要素認証やログイン通知でセキュリティを向上



生体認証を使う

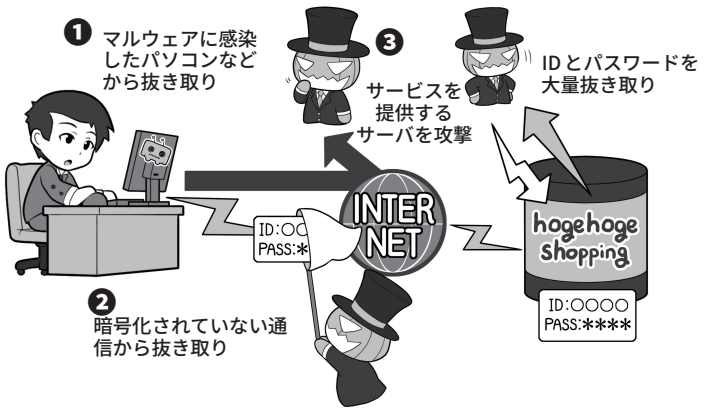


4.2 パスワードはどうやって漏れるの？どう使われるの？

さまざまなIDとパスワードの漏えいパターン

攻撃者にIDとパスワードが漏えいする事態は、機器がマルウェアに感染したり、自分が通信する過程で抜き取られたりする他に、利用しているサービス側からも流出するケースもあります。

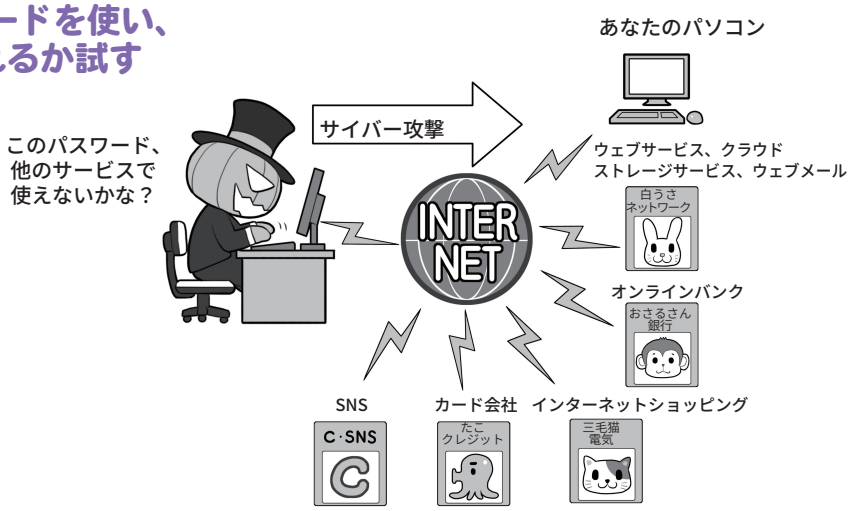
ニュースや通知でサービス側から流出が判明した場合は、速やかにパスワードを変更するなどの対応を取りましょう。



攻撃者は入手したIDとパスワードを使い、さまざまなサービスを乗っ取れるか試す

IDとパスワードをなんらかの手段で手に入れた攻撃者は、これをどこか別のサービスで使えないかさまざまな方法で試します。

こういった攻撃を成功させないために、パスワードの使い回しや、似たパスワード、パターンのあるパスワード、個人情報などから推測できるパスワードを利用するのはやめましょう。



私たちがパソコンやスマホ、あるいはSNSやウェブ上のサービスを利用するときに入力するIDやパスワード。サイバー攻撃でこれらの情報を盗まれると、かなり深刻な被害を起こしかねないものです。

では実際はどのように漏れてしまうのでしょう？

1つには、自分のパソコンなどがマルウェアに感染し、そのマルウェアがパスワードを盗み取って攻撃者に送信するケース。次に、ウェブサービスなどにログインするときに、私たちが利用する機器からウェブサービスまでの経路上のどこかで盗み取られてしまうケース。そして、ウェブサービス側でログインを認証するために控えとして持っているIDやパスワードが、攻撃者によって盗み取られ漏えいするケースなどがあります。

先ほど説明しましたが覚えておいてほしいのは、自分がマルウェアなどに感染していなくても、漏れてしまうケースがあるということです。

したがってIDやパスワードを普段入力していないから安心、とも言い切れません。

そしてIDとパスワードを盗み取った攻撃者は、それを使ってどこか別のウェブサービスなどが乗っ取れないか、さまざまな場所で試します。

あなたが複数のウェブサービスの間でIDとパスワードを使い回していたり、あるいは似た形のパスワードを使ったりしていると、これらのサービスのアカウントを一気に乗っ取られます。

乗っ取られると、あとはオンラインショッピングで勝手にものを買われてしまったり、現金は送れなくてもなんらかの送金システムが利用できる場合は、それを使ってお金を奪い取られたりされてしまうわけです。

もしパスワード流出が判明したら、まずはすぐにパスワードを変更しましょう。

5 ④偽メールや偽サイトに騙されないように用心しよう

5.1 多様化する偽メールに注意しよう

サイバー攻撃を行う際に、攻撃者は偽メール、偽サイトを使うことが多いです。

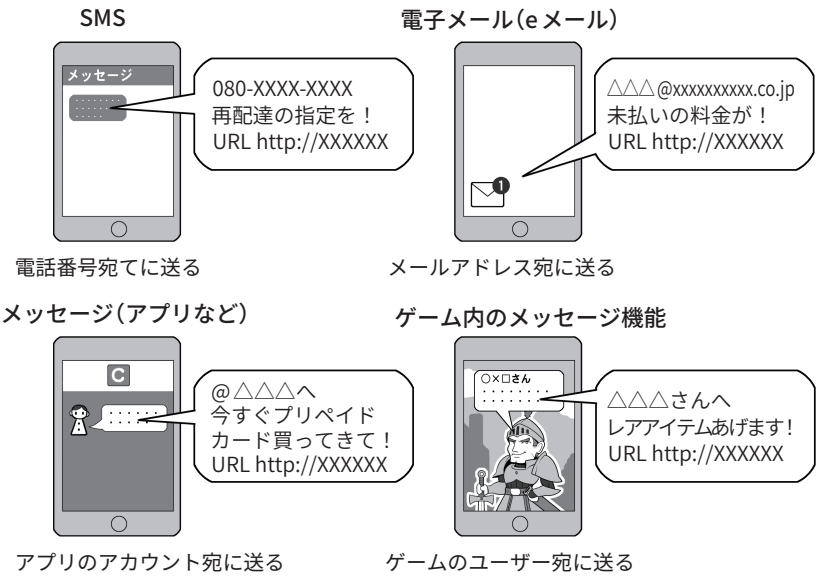
偽メールには、スマホ宛の偽SMSやSNSで使用可能なメッセージ機能なども含みます。メール・SMSからの誘導を受けて、アプリをダウンロードするのは原則としてやめましょう。

近年、フィッシング詐欺の攻撃で最も目を引いたのは、宅配業者の不在通知詐欺です。宅配業者を名乗って「配達に行ったが不在だった。下記のリンク▶用語集 P.189 から確認して欲しい」というようなSMSを送り付けて、利用者をリンク先の偽サイトに誘導し、そこでIDとパスワードなどを詐取するというものです。

実は、この業者は「SMSで不在通知を行なわない」のですが、それを知らない人たちはまんまと騙されてしまったわけです。関係機関で日々、「不審なメールに気を付けてください」というアナウンスをしているのですが、SMSとメールは違うものと思われてしまったのかもしれません。

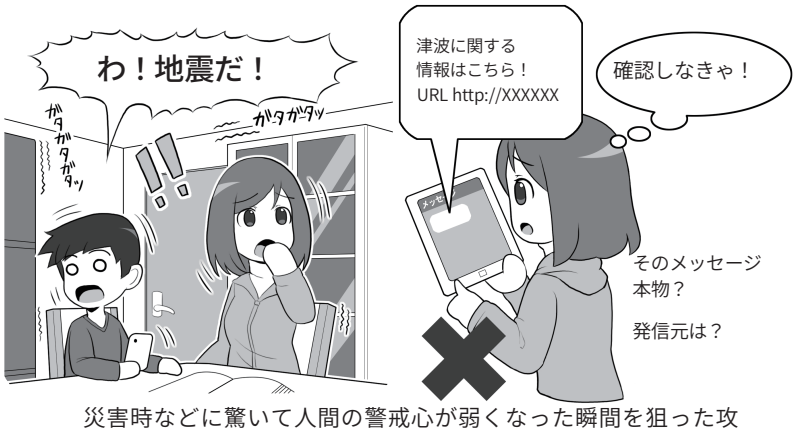
偽メールについても、国税庁を装ったりETCサービスを装ったりと、騙られる送信元にバリエーションが増えてきていますが、偽メールであることには間違いありません。また、すぐにアクセスしないとあなたの口座やアカウントが使えなくなる、一定の違約金が発生する等、不安を煽ることで一層、冷静な対応を妨げるものも多く存在します。そして誘導される偽サイトは短時間で消去される場合が多く、攻撃者が証拠をなるべく残さないようになっています。こういったメッセージを使った詐欺には、SMSやメールだけでなく、SNSのメッセージ機能、あるいはゲーム内のメッセージ機能を使った攻撃も実際に発生していますので、偽メールと同様に注意してください。

フィッシング詐欺はいろんな方法がある



「怪しいメール」といわれたら「メール」だけでなく似たような機能全般に気を付けましょう。

驚くと人間は警戒心を忘れる



災害時などに驚いて人間の警戒心が弱くなった瞬間を狙った攻撃もあります。注意しましょう。

フィッシング対策協議会 https://www.antiphishing.jp/
内閣サイバーセキュリティセンター X(旧 Twitter) @nisc_forecast

心当たりのないものは無視し、心当たりがあるものでも、そのメールやメッセージのURL▶用語集 P.178などにアクセスするのではなく、メールは通知と割り切って、そこに記載されているリンクは踏まないよう、心がけてください。

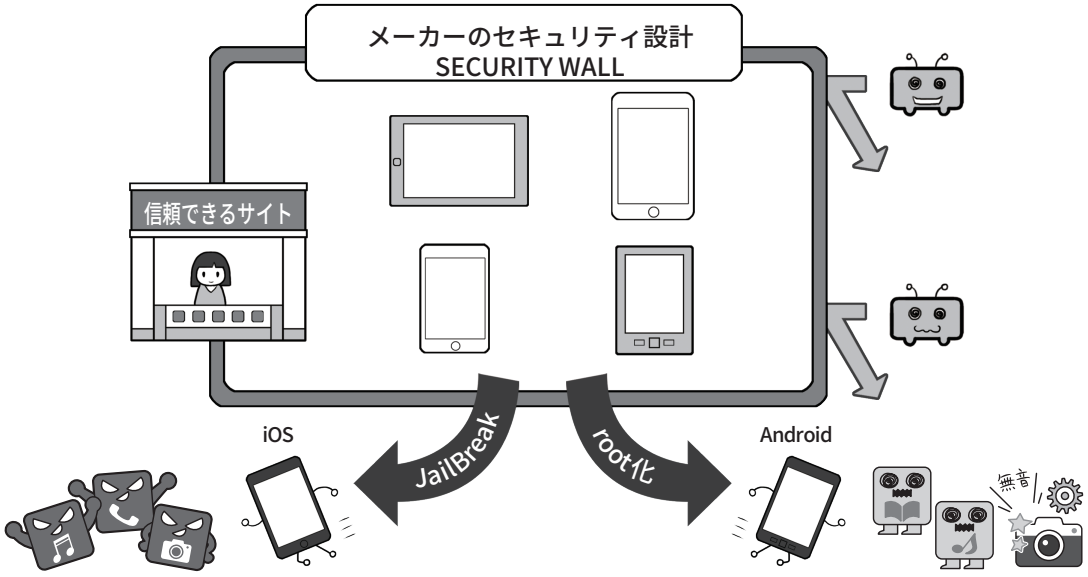
他にも、地震が発生したときに、気象庁を名乗って津波に関する迷惑メール▶用語集 P.189が送られた例もありました。いずれも私たちが「騙されないぞ」と身構えているのとは違う方向や、災害時などで正常な判断が行えない状況を狙っています。

こういった詐欺メールは年々手口が巧妙になっており、送信元アドレスやメッセージ中のリンクを確認しただけで、詐欺と見抜くことは極めて難しくなっています。基本は「見るだけで完結しない情報はすべて疑え」です。情報を確認する場合は、正規のウェブサイト▶用語集 P.180のURLを直接入力して見るか正規のアプリから行いましょう。検索結果上位に表示されるウェブサイト」であっても信頼性は必ずしも高くないこともありますので、注意が必要です。公式のアプリであると信じて偽サイトからダウンロードしたアプリにマルウェアが仕込まれていたという事例もありますので、注意が必要です。

また、日々巧妙になる手口を少しでも知るにはフィッシング対策協議会のウェブサイトや内閣サイバーセキュリティセンターのX(旧Twitter @nisc_forecast)をフォローするとよいでしょう。最新の事例をすぐに確認できます。

5.2 信頼できるサイト以外からアプリをインストールすることは控えよう

信頼できるサイト以外からのダウンロードやスマホの改造は控えましょう



スマホのセキュリティはメーカーが想定する利用方法を守っていることが前提条件です。信頼性が確保されていないアプリをインストールすることは危険が伴う可能性がありますし、「root化」や「JailBreak」といった改造は規約違反である場合もあります。いずれもセキュリティ上、ぜい弱になるので非常に危険で、やってはいけません。

スマホにインストールするアプリも同様に注意しなくてはいけません。

インストールしようとするアプリがどのような動作を行うものかをあらかじめ確認できればよいのですが、個人で、アプリの中身を分析し、不審な動作などがされないことを確認することは簡単なことではありません。そのような確認作業を自分ではなく信頼できる第三者がしてくれれば少し安心できます。

例えばスマホのOS事業者が運営するアプリストアから配信されるアプリに関しては、配信前にアプリストア運営者が審査しているので一定程度のリスクは軽減されます。

また、アプリストア間の競争を促進するための「スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律」が令和7年中に全面施行されますので、今後、様々なアプリストアが登場することが予想されます。ただし、同法の下でも、一定の要件を満たす場合は、スマホのOS事業者が、セキュリティ、プライバシー、青少年保護等のために必要な措置を引き続き採ることが

できます。

ユーザーには、アプリを利用する際の安全や安心を確保するためには一定のコストがかかることと、アプリの審査を行っている信頼できるアプリストアを使うという観点が不可欠です。スマホのOS事業者以外の事業者が運営するアプリストアについても、このような観点から信頼できるアプリストアを利用することも重要です。

このほか、アプリストア以外からアプリを入手する方法としては、おもにブラウザを介してアプリを直接ダウンロードする方法(以下、「サイドローディング」)があります。

サイドローディングについては、信頼できるサイトからのダウンロードと、セキュリティ設定の適切な管理が必要となります。一方で、信頼できるサイトのような偽サイトに誘導するフィッシングメール▶用語集 P.187などによる攻撃が行われる可能性がありますので、十分注意しましょう。

スマホの改造は規約違反になる場合もあり、セキュリティ上、ぜい弱になるので非常に危険です。スマホを標準にはない設定に変更できる改造を「root化」▶用語集 P.177「JailBreak」▶用語集 P.177と呼びますが、これらの行為はセキュリティレベルを下げることになります。

スマホには、個人に関する重要な情報がたくさん保存されているため、リスクの高いアプリをインストールし、重要な情報が漏えいしてしまうと、取り返しがつきません。例えばスマホの場合、攻撃者が用意したサイトに偽メールや偽SMSなどであなたを誘導して、不適切なアプリをインストールさせ、端末を乗っ取ったり、端末内の情報を盗んだりする可能性があります。

Android機器の場合、使用しているアプリで別のアプリをインストールする設定が最初からオフになっております。不明なアプリ▶用語集 P.188をインストールしないためにも、スマホのOS事業者以外の信頼できるアプリストアを利用したいとき以外には、この設定はオフのままにしておくようにしましょう。

また、Android機器でもiOSでも、アプリのインストール時や初回起動時に、同意を求められる「権限」には充分注意してください。権限とはインストールするアプリに対して、スマホのどの機能の利用を許可するか、という確認です。単なるカメラアプリなのに住所録にアクセスするものや、撮影する必要がないのにカメラにアクセスするもの、著しく多くの項目にアクセスしようとするものなどは要注意の例です。項目別に許可を却下するか、そうできない場合、そのアプリは導入しないようにしましょう。また、最初は無害に見えて、導入後のアップデートで権限の増加の許可を求めるものも、その変更項目に注意してください。

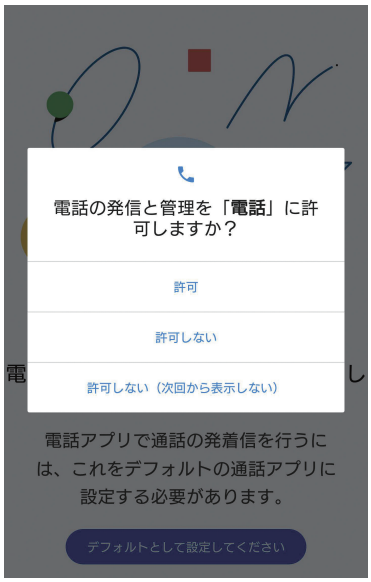
有用なアプリの開発者から、攻撃者が当該アプリを買い上げて、後からアプリをマルウェア化してしまう攻撃もあります。その他、アプリ間での機能連携やウェブサービス間で連携して、間接的に権限を奪取するものもあるので「連携」という言葉にも充分注意してください。

「不明のアプリ」という言葉に注意

• Android

項目や文言は、使用するAndroidのバージョンやスマホメーカーによって異なりますが、アプリのインストール時に「不明なアプリ」と表示されたり、最初からオフに設定されている「不明なアプリ」に関する項目を変更させようとするものは、セキュリティ上危険な可能性が高いものです。スマホのOS事業者以外の信頼できるアプリストアを利用したいとき以外にはオフの設定のままにしておくようにしましょう。アプリは、基本的にアプリストアからのみインストールするようにして、その他の場所からは避けましょう。

導入時や起動時の権限付与に注意



• Android、iOS（画面はAndroid）

アプリのインストール時や、起動時にさりげなく表示されるため、多くの人が無意識に「承認」や「同意」してしまっていますが、これは、「アプリがスマホのこれらの情報に自由にアクセスできる許可」を求めている画面です。

個別に却下することができない場合もあるので、その際は導入しないようにしましょう。そして、そもそも不必要な権限を求めるアプリは怪しいと警戒しましょう。

コラム.1 災害時の情報収集

近年は、さまざまな自然災害が発生し、その中でさまざまなデマが飛び交い、正確な情報収集の難しさを浮き彫りにしました。悪意のデマではないとしても、不正確な情報の拡散▶用語集P.180も多く見受けられました。このような場合、インターネットの特性上、同種の情報ばかり表示されるようになるので、それが信頼できると思いやすくなります。拡散する方々は善意で行っているのですが、情報源(ソース▶用語集P.184)がはっきりしないものの拡散は状況を混乱させます。物事の正確さ担保するためには、「現場」を知る責任がある方の「公式な情報発信」以外は、むやみに拡散するべきではありません。とくに、「誰かに聞いた」という伝聞は、たとえそれが「通信会社の人に聞いた」、「役所の人が言っていた」というものでも、公式発表ではないかぎり、「不正確」である可能性が高くなります。「伝聞情報」には気をつけて、「本当に拡散するべきか」よく考えてください。昨今は、耳目を引きやすいフェイク画像を簡単に生成できるウェブサービスもあり、SNSで流布している画像がフェイクである可能性もあります。公式もしくは信頼できるメディアからの情報でない限り留意しましょう。公開した情報が「悪質なデマ」と認定されると、公開した当人が何らかの罪に問われる可能性もあります。

また、災害時の救助要請をSNSで行う方法が、広く一般に認識されたことが確認されました。これも本人、もしくは直接依頼された家族などの代理人が行うことは大変有効な手段ともいえますが、上記と同様に伝聞の情報を拡散したり、あるいは本人が救助された後も救助要請が残されたままだったりすると、それが1人でも多く助けようとする方の妨げにもなります。それ以外にもSNSの情報を見て、直接関係がない人が善意で電話での救助要請を行うなどのケースがあったようです。

こういった情報は、本当に必要な情報収集への「雑音(ノイズ)」となる可能性があるので控えましょう。

また、最近はさまざまな災害時用のアプリが登場し、安否確認の方法も増えてきていますが、これらは連絡を取り合う人と、事前になにを使うか決めておかなければ意味を成しません。きちんと利用するサービスの確認をしておきましょう。

災害時の救助関係発信はわかりやすく確実に

公的機関の災害時の窓口は、あくまでも110番119番の電話ですが、SNSで救助関係の発信をするときは、住所やGPS情報を付けましょう。

コラム．2　スマホによる災害時の情報収集

災害時、街中なのにスマホが圏外になったら、それは通信用の基地局が被害にあって壊れている印です。そのまま電源をオンにしておくと、スマホはつながらない基地局に接続しようとして、普段以上に貴重な電池を消耗してしまいます。そういったときはスマホの電源を切る、スマホの中身を見る場合でもフライト（機内）モード▶用語集 P.188にして少しでも電池の消費を抑えましょう。

電波が回復しても、電話よりはデータ通信のメールやSNSを利用しましょう。災害時はそのほうがつながりやすく、また、電池の消費も少なくてすみます。いざというときに備えてモバイルバッテリーを、日常的に持ち歩くのもよいでしょう。

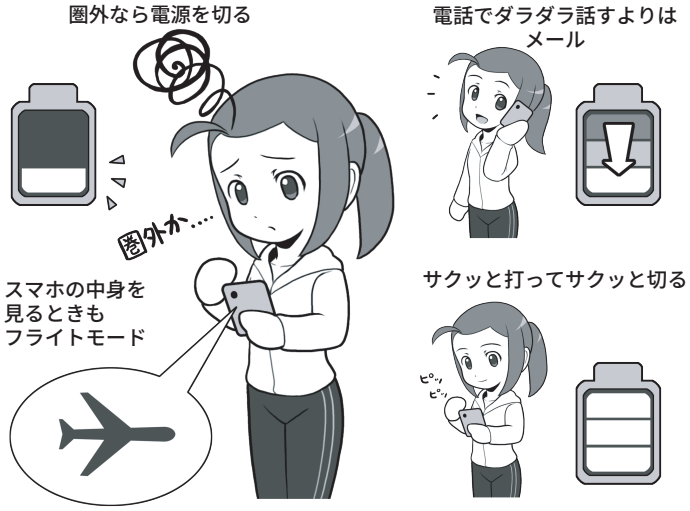
災害直後は情報が錯綜しますが、一定時間が経過すると救援物資や脱出ルートなどの情報がネットに掲載され、やがて整然とした情報発信が行われるようになります。効率的な情報収集のため、知り合いと連絡を取りながら必要な情報を収集しましょう。

また携帯電話網もスマホも使えなくなる場合、どういう手段で連絡を取り合うかも確認しておきましょう。

そのほか、災害時に利用可能になる、通信事業者が運用する伝言板システムを使い、対応に必要な情報を募る／安否確認を行うなども考えられます。

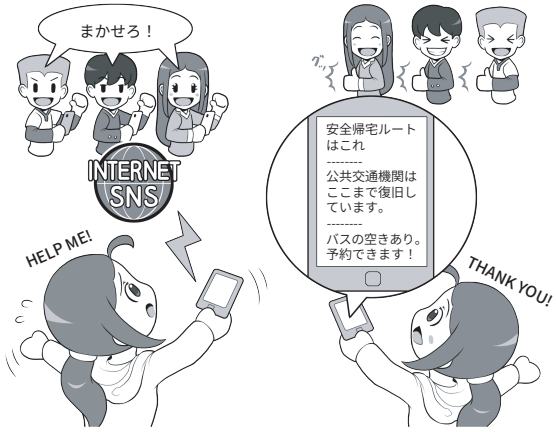
東日本大震災では旅行中に被災し、帰宅できなくなった方たちが、SNSを通じて友人に被災地から家に帰るためのルートの確認や車両手配、バスの予約などをしてもらった例もあります。なお、災害時の避難所などでは、自治体や電気通信事業者の取組により、無料で使えるWi-Fi「00000JAPAN（ファイブゼロジャパン）▶用語集 P.176」などが立ち上がることがありますが、このWi-Fiは接続しやすさを優先するため、暗号化されていないことを覚えておき、利用時はIDとパスワードの入力を避け、もし利用したい場合はVPN▶用語集 P.178など自前で通信を暗号化する知識を得ておきましょう。

電池をもたすテクニック



電波が圏外ならば電源を切るか、スマホの内容の閲覧時もフライトモードを利用します。電波が回復したら災害用の超省電力モードがあれば活用してもよいでしょう。電話で長く話すよりも、メールをさくっと打って電源を切ったほうが電池を消費しません。ACコンセントがあれば充電器にもなる一体型モバイルバッテリーを持ち歩くのも役立ちます。

情報収集に協力してもらう



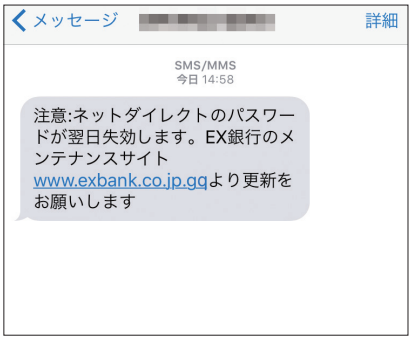
情報収集に長けた家族や友人・同僚に相談して、いざというときは情報収集や必要な交通手段の手配をお願いできるようにしておきましょう。自分1人では気づかない情報も外から見ていると気づく場合もあります。

6 ⑤メールの添付ファイルや本文中のリンクに注意しよう

標的型メールとスパムメールの例

標的型メールの例

スパムメールの例 SMSを使った例



本章5.1(P.36)で述べた「偽メール」と類似しますが、添付ファイルやリンクは、標的型攻撃でもよく使われますし、今でもときどき復活しては、猛威を振るう「Emotet」も、マルウェアを添付したメールを受信者が開き、添付ファイルを実行することで感染が成立します。

心当たりのない送信元からのメールに添付されているファイルやリンクは、信用できないものとして、原則、開かないようにするとともに、機器の設定などを堅牢に保ち、感染の隙を作らないようにしましょう。例えば、一般社団法人全国銀行協会や一般社団法人クレジットカード協会からは、フィッシング詐欺に遭わないようにするための注意が示されており、SMSやメールを受信した場合には、必ず公式のページから対応することを、推奨しています。

スパムメールでの攻撃は、引っかかる率が少なくとも、その攻撃の母数を大きく取ることで攻撃者にとっての利益回収のパフォーマンスを上げています。

例えば、「スパムメールの例」の画面は、実際にSMSに送り付けられた、銀行を名乗るフィッシングメール▶用語集 P.186を模したものです。

送信元とされる金融機関やカード会社の口座を持っていない人であれば、フィッシング(＝詐欺)メールだと気付くことができるかもしれませんが、現在もこういった攻撃に引っかかる人が相当数いるのが実態です。その先が詐欺サイトではなく、ゼロデイ攻撃▶用語集 P.184のマルウェアが埋め込まれたウェブサイトならば、開いただけで感染してしまうでしょう。

また、もっとやっかいなのが、攻撃者ではなく、善意でマルウェアを拡散▶用語集 P.180させてしまう人々です。友人から「このアプリ面白いよ！」と薦められたら、多くの人はあまり不審に思わないでしょう。

しかし、友人は知らなくても、実はこのアプリにマルウェアが仕込まれていたり、あるいは感染時点は無害でも、後に権限を拡大して個人情報を抜き取るかもしれません。

これが、他人の発信ならば警戒できますが、親しい友達や家族だった場合、警戒できるでしょうか？

対抗策としては、こういったお薦め系のものは1つの線引きを持って接するようにしましょう。メールの文面など、目の前に見ている情報で完結しないものは一律に警戒するのです。動画が面白いとかお金が儲かる方法があるとかだけでなく、リンクでジャンプするとか、添付ファイルを開かせるものは一律に避ける。

それは、現実世界で「ちょっと向こうまで付き合ってよ」とか「ちょっとこの車に乗ってよ」といって連れて行かれるのに等しいと思いましょう。

さらに、「リンクでジャンプしないけど検索エンジンで調べて見る分にはいいよね」、と思っても、攻撃者はそうやって検索エンジンからやってくる人向けに、二段構えでマルウェアを仕込んだウェブサイトを用意していることもある、と覚えておいてください。

7 ⑥スマホやパソコンの画面ロックを利用しよう

7.1 スマホやパソコンには必ず画面ロックをかけよう

スマホやパソコン(PC)の情報を守る第一歩は、待ち受け画面にロックをかけることです。

ロックには「PIN コード*」によるロック、パターンロック▶用語集 P.186、指紋や顔など生体情報を用いた認証によるロックなどがあります。ロック機能は「誰かにスマホを持ち去られるなど、手元からスマホが離れたとき」に情報を確実に守るためのしくみの1つです。

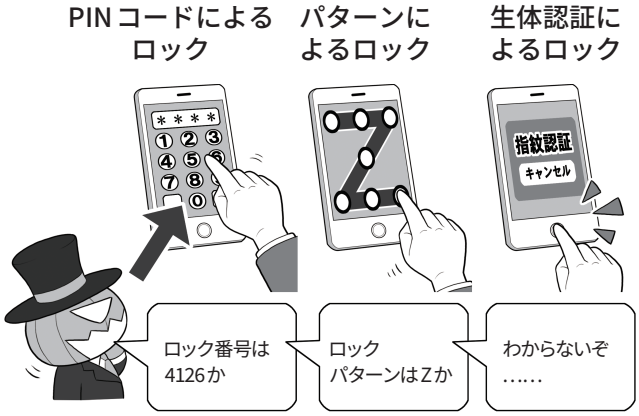
とくに生体認証は周りから覗かれPIN コードを盗まれる危険性の排除をしつつ、入力の面倒くささを省くので便利な機能です。

指紋認証や顔認証が代表的ですが、その他にも、スマートウォッチ▶用語集 P.183 など特定のウェアラブル機器を着けたり、GPS ▶用語集 P.176 に連動して自宅など特定の場所にいたりすることで自動的にロックを解除できるものもあります。

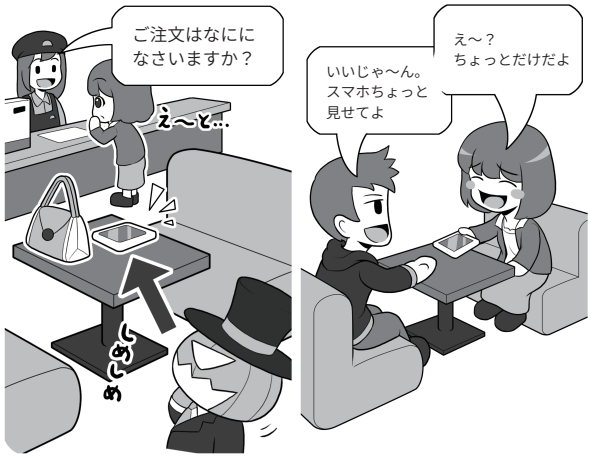
ただし、気を付けておきたいのは、セキュリティ向上のためのロック機能を設定しても、そのパソコンやスマホをロック解除したまま置いてその場所を離れたり、ロックを解除して他人に見せたり貸したりすれば、一瞬で情報を盗み、乗っ取ることが可能です。画面ロックは、情報を保護するための強力なツールですが、ロック解除するための認証方法がぜい弱だと意味がなくなります。ロックがかかっているから安心とそれだけに頼り切りにならず、ロックを解除するための機能や、スマホやパソコンの管理にも留意しましょう。

スマホやパソコンは自分のすべての情報が詰まった持ち歩く金庫だと思って、必ず肌身離さず自分のそばに置き、使わないときはこまめにロックをかけた状態にすることが重要です。

スマホやパソコンにはロックをかけよう



席において離れたり、人に貸したりしないようにしよう



スマホを席に置いたままでは、本体も情報も盗まれるおそれがあります（とくにロックを設定しなかったり、ロック解除したままの状態で放置）。

スマホを貸すと、プライバシーを覗かれたり、一瞬でスパイアプリのようなものをインストールされたりすることがあります。むやみに渡してはいけません。

* PIN コードに関しても、詳しくは第5章1(P.99)のパスワードに関する項目を参照

7.2 よくある情報の漏れ方と対策

SNS用のアプリなどでは、本体のPINコードなどとは別に、アプリ専用のPINコードが設定できるものもあります。盗難などの際、SNSの内容を見られたくなければ、このアプリPINコードも設定しましょう。情報の守りが二重になります。一部の機種では生体認証をアプリのロック解除に利用できるものもあるので、セキュリティを向上させても快適な利用の妨げにはなりません。

一方、攻撃する側から見ると、スマホのロックをなんらかの方法でパスできたとしても、また、別の関門が待ち構えることになります。手間をかけさせ侵入を諦めさせるというセオリーに沿っているわけです。

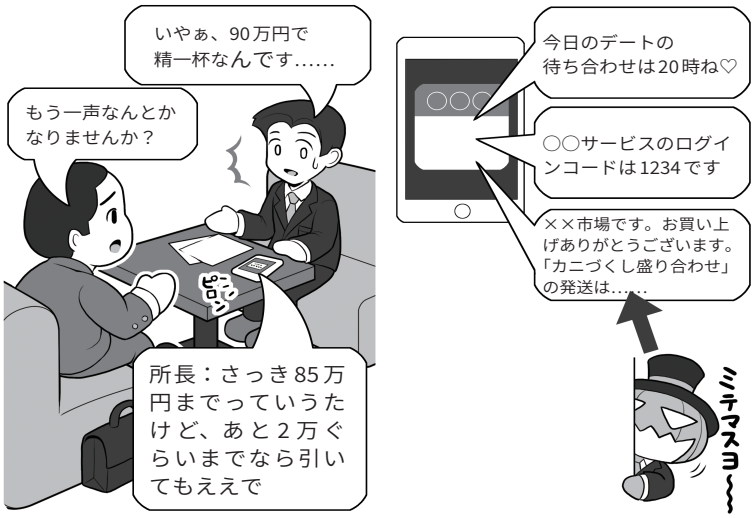
なお、アプリのPINコードを使う場合は、スマホロック解除のPINコードと異なるものを設定しましょう。PINコードの使い回しはセキュリティがないのと一緒になってしまいます。PINコードもそれぞれ異なってこそ意味があるのです。

スマホをロックしていても情報漏れが発生することもあります。

例えば自分だけで使っているときは便利なメールの通知機能▶用語集P.185。ロック画面▶用語集P.190にメールの内容を表示していると、誰かと会話中や商談中に、うっかり内部情報を見られてしまったり、あるいは差出人が分かるだけで、状況によっては知られると問題のある情報を提供してしまうことになりかねません。

また、同様にロック画面にメールの内容を表示していると、せっかくセキュリティ向上のために設定した多要素認証のパスワードメールも見られてしまうことがあり得ます。そうするとスマホやメールアドレスの正当な持ち主であることを確認する役割を果たせず、画面をのぞき見ただけの第三者によって認証が突破できてしまいます。

待ち受け画面に表示する通知はよく検討する



ロック画面だけでなく、普段使用している画面に通知ウインドウとして表示される場合でも、同じく情報を見られてしまう原因になります。スマホを使って説明しているときに、不適切なメールの内容が表示されることも……。情報漏えいには気を付けましょう。

アプリごとにPINコードをかけられる場合はかける

本体のロックを解除されても、SNSのアプリに別のPINコードがあれば、流出の危険性は低くなります。それでも、自分が席を離れるときにスマホを残してはいけません。なお、勝手に他人のスマホのロック解除をすることは、れっきとしたサイバー攻撃です。

8 ⑦大切な情報は失う前にバックアップ(複製)しよう

8.1 何をするにもバックアップを取ろう

各種のサイバー攻撃や、パソコン・スマホの故障などからいち早く復旧して事業を継続するには、システムやデータのバックアップが不可欠です。またランサムウェアの流行により、バックアップの重要性が格段に上がっています(第2章2 (P.59)参照)。バックアップを取ることで、ランサムウェア攻撃や、様々なシステムへの破壊や影響があった場合に、被害を最小限にとどめる有効な手段となります。

またバックアップは、いざというときに元に戻せることが必要です。定期的にバックアップファイルが使える状態にあることの確認はもちろん、バックアップから元のシステムに戻すための手順の整備や訓練なども行うことも重要です。

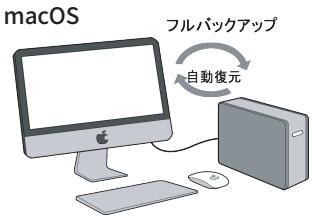
バックアップの方法はおもにパソコンやスマホのOSの種類により異なっています。

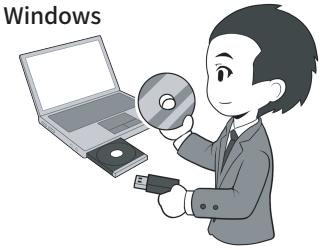
パソコンの場合、macOS搭載の機器のように、外付けの補助記憶装置▶用語集 P.188(ハードディスクやSSD▶用語集 P.178。以降記憶装置▶用語集 P.181)を接続するだけでバックアップが行え、復旧もシステムとデータすべてをほぼ全自動で行えるものもあります。

Windows搭載機器では、基本的にはデータをバックアップする考え方で、システムの復旧とデータの復元は、別に行うようになっています。

スマホの場合も機種ベンダーによる差もありますがほぼ同様です。

macOS機器、Windows機器のバックアップと復元

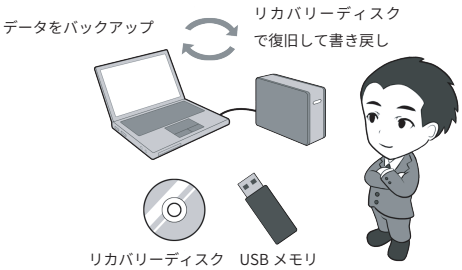




mac OS機器はまるごとバックアップ、まるごと復元の性格が強く、Windowsは基本的にはOSを復元後、別途データを書き戻すイメージと考えるとよいでしょう。

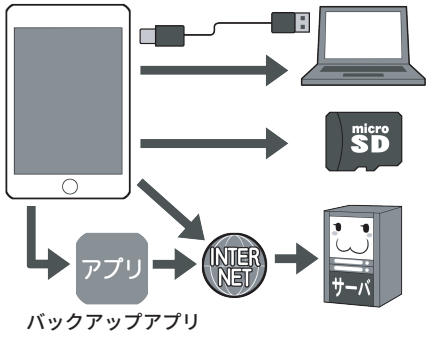
実際は他にも専用のソフトウェアを導入したり、細かい設定を変えることで、バックアップの方法を変える手段はあります。

ですから基本的なそれぞれのOSの立ち位置や性格と考えて下さい。善し悪しや優劣はありません。



スマホもバックアップは定期的に取ろう

バックアップの方法はいろいろ

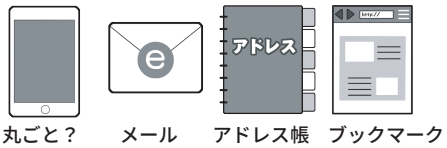


パソコンにつないで丸ごとバックアップ

内蔵できるmicroSDメモリカードにバックアップ

直接あるいはアプリ経由でクラウドサーバにバックアップ

なにがバックアップできるか確かめる



なにがバックアップできるのか確かめて、機種やバックアップ方法を選択します。また、取得したバックアップを用いてシステムがちゃんと復元できるか確認してください。

iOS搭載機器はパソコン上に専用の同期ソフトを導入して全体をバックアップします。機器を紛失した場合にも、新しい機器を接続すると自動で復元が行えます。

Androidに関しては標準ではパソコンに全体をバックアップする機能はないので、Windowsに似た、データのみをバックアップする形で行います。

8.2 ランサムウェアや天災にも対応できるバックアップ体制

ランサムウェアなどの、データを破壊することが多いマルウェアの対策にはバックアップが有効ですが、では実際にどう運用するのでしょう。

ランサムウェアはパソコンなどが感染すると、そのパソコンに繋がっている記憶装置すべてを暗号化してしまいます。仮にバックアップしていても、常時接続したままにしていると、その外付け記憶装置まで巻き添えで暗号化されることもあります。

そのため、バックアップ自体はマメにしておくべきですが、常時接続はしておかないという、かなり難しい運用が求められます。

また、最近は大雨などの異常気象や地震等の災害により、事務所にあったパソコンと外付け記憶装置が両方とも使用不能となり、復旧が困難になることもあります。これに対応する手段としては、バックアップの「3-2-1ルール」というものがあります。バックアップは本体を含め3個以上、2種類以上の媒体、そして1個は遠隔地に置くというものです。特に重要なファイルのバックアップは、使いやすい状態におくなどの選択も重要です。

遠隔地とは、現実的には「クラウドサーバ」▶用語集P.181などの利用を意味します。クラウドサーバは最近では手頃になりましたが、それでも本体の全データをバックアップできる容量は高価です。したがって、事業継続に必要な重要なデータを選別してバックアップすることになるでしょう。なお、会社に同時に災害に遭わなそうな支社などがある場合は、そこにバックアップをおいてもよいでしょう。

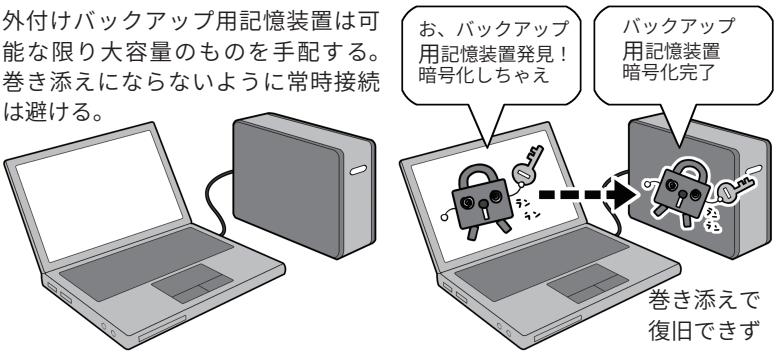
なお、ランサムウェアに対しては、変更不能な形でのバックアップが有効です。例えばDVDやBDなどのメディアで追記不能な形で記録したり、イミュータブル(変更不能)という機能に対応したクラウドサービスなども有効なので、利用にあたっては調べてみましょう。

ランサムウェア感染はビジネスにも影響

ランサムウェアはパソコン内のファイルを勝手に暗号化するため、感染すれば仕事上の極めて重要なファイルも人質に取られてしまいます。バックアップはまめにしておきましょう。

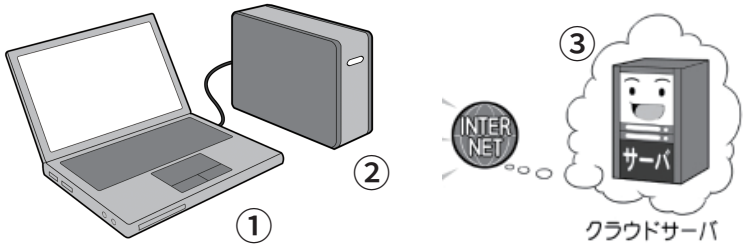
バックアップの体制を整える

外付けバックアップ用記憶装置は可能な限り大容量のものを手配する。巻き添えにならないように常時接続は避ける。



環境を整えたらバックアップを開始します。なにかソフトの導入や、環境を変更したらバックアップします。システムのアップデート後もバックアップします。ただし、バックアップ用記憶装置を常に接続しておくとランサムウェア感染で巻き添えになって、復旧に使うためのデータも失われてしまいます。

バックアップは3個以上、2種媒体以上、1個は遠い場所



本体＋バックアップ用記憶装置＋クラウドサーバで条件を満たします。クラウドサーバは多要素認証などで、攻撃者に乗っ取られないようにしましょう。

7.2 よくある情報の漏れ方と対策

SNS用のアプリなどでは、本体のPINコードなどとは別に、アプリ専用のPINコードが設定できるものもあります。盗難などの際、SNSの内容を見られたくなければ、このアプリPINコードも設定しましょう。情報の守りが二重になります。一部の機種では生体認証をアプリのロック解除に利用できるものもあるので、セキュリティを向上させても快適な利用の妨げにはなりません。

一方、攻撃する側から見ると、スマホのロックをなんらかの方法でパスできたとしても、また、別の関門が待ち構えることになります。手間をかけさせ侵入を諦めさせるというセオリーに沿っているわけです。

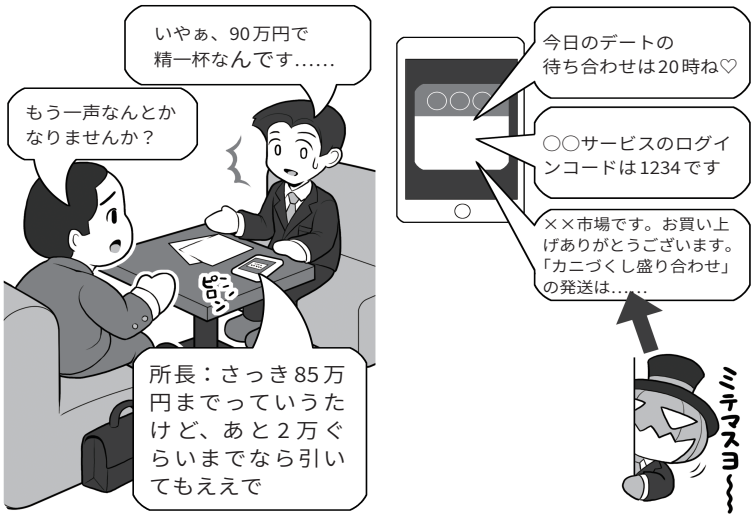
なお、アプリのPINコードを使う場合は、スマホロック解除のPINコードと異なるものを設定しましょう。PINコードの使い回しはセキュリティがないのと一緒になってしまいます。PINコードもそれぞれ異なってこそ意味があるのです。

スマホをロックしていても情報漏れが発生することもあります。

例えば自分だけで使っているときは便利なメールの通知機能▶用語集P.185。ロック画面▶用語集P.190にメールの内容を表示していると、誰かと会話中や商談中に、うっかり内部情報を見られてしまったり、あるいは差出人が分かるだけで、状況によっては知られると問題のある情報を提供してしまうことになりかねません。

また、同様にロック画面にメールの内容を表示していると、せっかくセキュリティ向上のために設定した多要素認証のパスワードメールも見られてしまうことがあり得ます。そうするとスマホやメールアドレスの正当な持ち主であることを確認する役割を果たせず、画面をのぞき見ただけの第三者によって認証が突破できてしまいます。

待ち受け画面に表示する通知はよく検討する



ロック画面だけでなく、普段使用している画面に通知ウインドウとして表示される場合でも、同じく情報を見られてしまう原因になります。スマホを使って説明しているときに、不適切なメールの内容が表示されることも……。情報漏えいには気を付けましょう。

アプリごとにPINコードをかけられる場合はかける

本体のロックを解除されても、SNSのアプリに別のPINコードがあれば、流出の危険性は低くなります。それでも、自分が席を離れるときにスマホを残してはいけません。なお、勝手に他人のスマホのロック解除をすることは、れっきとしたサイバー攻撃です。

8 ⑦大切な情報は失う前にバックアップ(複製)しよう

8.1 何をするにもバックアップを取ろう

各種のサイバー攻撃や、パソコン・スマホの故障などからいち早く復旧して事業を継続するには、システムやデータのバックアップが不可欠です。またランサムウェアの流行により、バックアップの重要性が格段に上がっています(第2章2 (P.59)参照)。バックアップを取ることで、ランサムウェア攻撃や、様々なシステムへの破壊や影響があった場合に、被害を最小限にとどめる有効な手段となります。

またバックアップは、いざというときに元に戻せることが必要です。定期的にバックアップファイルが使える状態にあることの確認はもちろん、バックアップから元のシステムに戻すための手順の整備や訓練なども行うことも重要です。

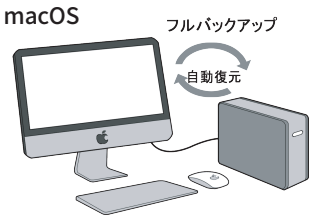
バックアップの方法はおもにパソコンやスマホのOSの種類により異なっています。

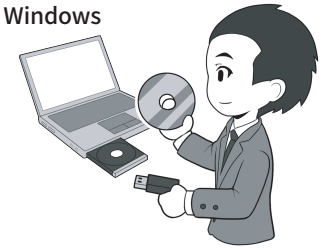
パソコンの場合、macOS搭載の機器のように、外付けの補助記憶装置▶用語集 P.188(ハードディスクやSSD▶用語集 P.178。以降記憶装置▶用語集 P.181)を接続するだけでバックアップが行え、復旧もシステムとデータすべてをほぼ全自動で行えるものもあります。

Windows搭載機器では、基本的にはデータをバックアップする考え方で、システムの復旧とデータの復元は、別に行うようになっています。

スマホの場合も機種ベンダーによる差もありますがほぼ同様です。

macOS機器、Windows機器のバックアップと復元

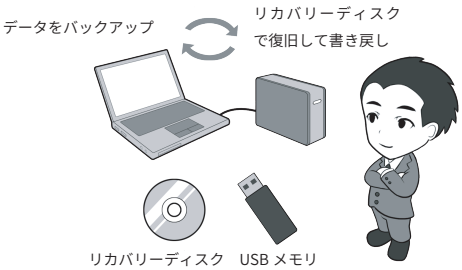




mac OS機器はまるごとバックアップ、まるごと復元の性格が強く、Windowsは基本的にはOSを復元後、別途データを書き戻すイメージと考えるとよいでしょう。

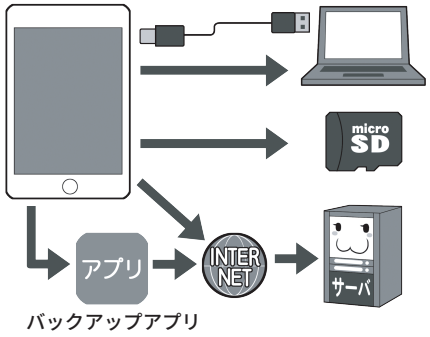
実際は他にも専用のソフトウェアを導入したり、細かい設定を変えることで、バックアップの方法を変える手段はあります。

ですから基本的なそれぞれのOSの立ち位置や性格と考えて下さい。善し悪しや優劣はありません。



スマホもバックアップは定期的に取ろう

バックアップの方法はいろいろ

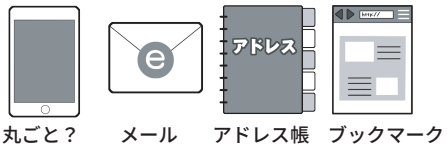


パソコンにつないで丸ごとバックアップ

内蔵できるmicroSDメモリカードにバックアップ

直接あるいはアプリ経由でクラウドサーバにバックアップ

なにがバックアップできるか確かめる



なにがバックアップできるのか確かめて、機種やバックアップ方法を選択します。また、取得したバックアップを用いてシステムがちゃんと復元できるか確認してください。

iOS搭載機器はパソコン上に専用の同期ソフトを導入して全体をバックアップします。機器を紛失した場合にも、新しい機器を接続すると自動で復元が行えます。

Androidに関しては標準ではパソコンに全体をバックアップする機能はないので、Windowsに似た、データのみをバックアップする形で行います。

8.2 ランサムウェアや天災にも対応できるバックアップ体制

ランサムウェアなどの、データを破壊することが多いマルウェアの対策にはバックアップが有効ですが、では実際にどう運用するのでしょう。

ランサムウェアはパソコンなどが感染すると、そのパソコンに繋がっている記憶装置すべてを暗号化してしまいます。仮にバックアップしていても、常時接続したままにしていると、その外付け記憶装置まで巻き添えで暗号化されることもあります。

そのため、バックアップ自体はマメにしておくべきですが、常時接続はしておかないという、かなり難しい運用が求められます。

また、最近は大雨などの異常気象や地震等の災害により、事務所にあったパソコンと外付け記憶装置が両方とも使用不能となり、復旧が困難になることもあります。これに対応する手段としては、バックアップの「3-2-1ルール」というものがあります。バックアップは本体を含め3個以上、2種類以上の媒体、そして1個は遠隔地に置くというものです。特に重要なファイルのバックアップは、使いやすい状態におくなどの選択も重要です。

遠隔地とは、現実的には「クラウドサーバ」▶用語集P.181などの利用を意味します。クラウドサーバは最近では手頃になりましたが、それでも本体の全データをバックアップできる容量は高価です。したがって、事業継続に必要な重要なデータを選別してバックアップすることになるでしょう。なお、会社に同時に災害に遭わなそうな支社などがある場合は、そこにバックアップをおいてもよいでしょう。

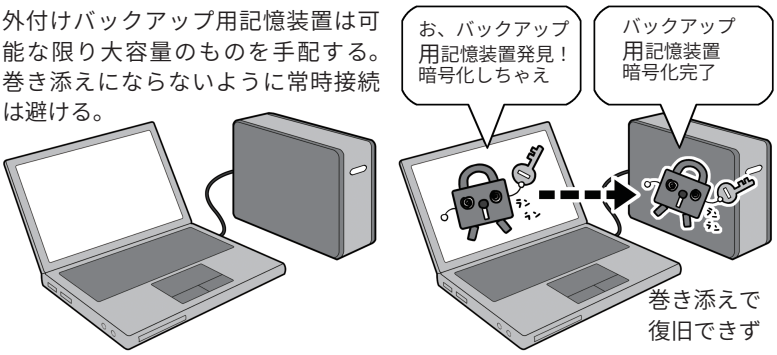
なお、ランサムウェアに対しては、変更不能な形でのバックアップが有効です。例えばDVDやBDなどのメディアで追記不能な形で記録したり、イミュータブル(変更不能)という機能に対応したクラウドサービスなども有効なので、利用にあたっては調べてみましょう。

ランサムウェア感染はビジネスにも影響

ランサムウェアはパソコン内のファイルを勝手に暗号化するため、感染すれば仕事上の極めて重要なファイルも人質に取られてしまいます。バックアップはまめにしておきましょう。

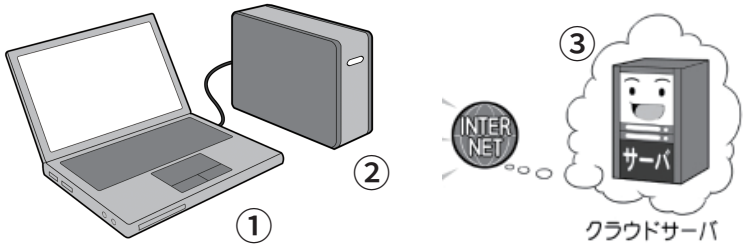
バックアップの体制を整える

外付けバックアップ用記憶装置は可能な限り大容量のものを手配する。巻き添えにならないように常時接続は避ける。



環境を整えたらバックアップを開始します。なにかソフトの導入や、環境を変更したらバックアップします。システムのアップデート後もバックアップします。ただし、バックアップ用記憶装置を常に接続しておくとランサムウェア感染で巻き添えになって、復旧に使うためのデータも失われてしまいます。

バックアップは3個以上、2種媒体以上、1個は遠い場所



本体＋バックアップ用記憶装置＋クラウドサーバで条件を満たします。クラウドサーバは多要素認証などで、攻撃者に乗っ取られないようにしましょう。

9 ⑧外出先では紛失・盗難・覗き見に注意しよう

勤務先や外出先でスマホやパソコンを使う際に、誰かにスマホやパソコンを覗き見られている、そう感じたことはありませんか？

友人知人と冗談の範囲で「何やってるの～？」と1回2回茶化すくらいならまだしもあまりに覗き見の頻度が高かったり、あるいは見知らぬ人に何も言わずにずっと横や後ろから覗き見られてたりしているようならば要注意です。

見られている内容が機密情報であったり、秘匿したい個人情報であったりする場合には、あなたの情報が漏れる心配があります。

「見られても大したことない情報しか自分のスマホやパソコンには保存してないよ」と心配しない人も多いかもしれませんが、覗き見している人はあなたの情報もさることながら、あなたがやりとりしている相手がターゲットかもしれません。

「ロックをかけてあるから大丈夫」と思っても、ロックを解除する方法がすでに相手の手に渡っている懸念もあります。例えば、相手に直接接触せず情報を入手する方法として、電車で座席に座っている人のスマホ操作を見てPINコードやパターンロック形状を盗む「ショルダーハッキング」、カフェなどのテーブルに放置されているスマホの画面に残る指の脂跡からパターンロックを見破る方法などがあります。本章7.1(P.42)でも説明しましたが、飲食店などで席の確保にスマホなどを置き去りにする行為を時折見かけますが、紛失・盗難・覗き見、いずれの被害に遭ってもおかしくない非常に危険な行為です。このような行為は、すぐにやめましょう。

外出時は自分のスマホやパソコンが他人から見られる可能性は高い

外出時は、使用しているスマホやパソコンを他人から覗き見されないよう注意が必要です。また、うっかり紛失して盗難されれば、大事な情報が盗まれるリスクは大きく高まるので、よく注意しましょう。

スマホ使用時によく狙われるソーシャルエンジニアリング

ショルダーハッキング

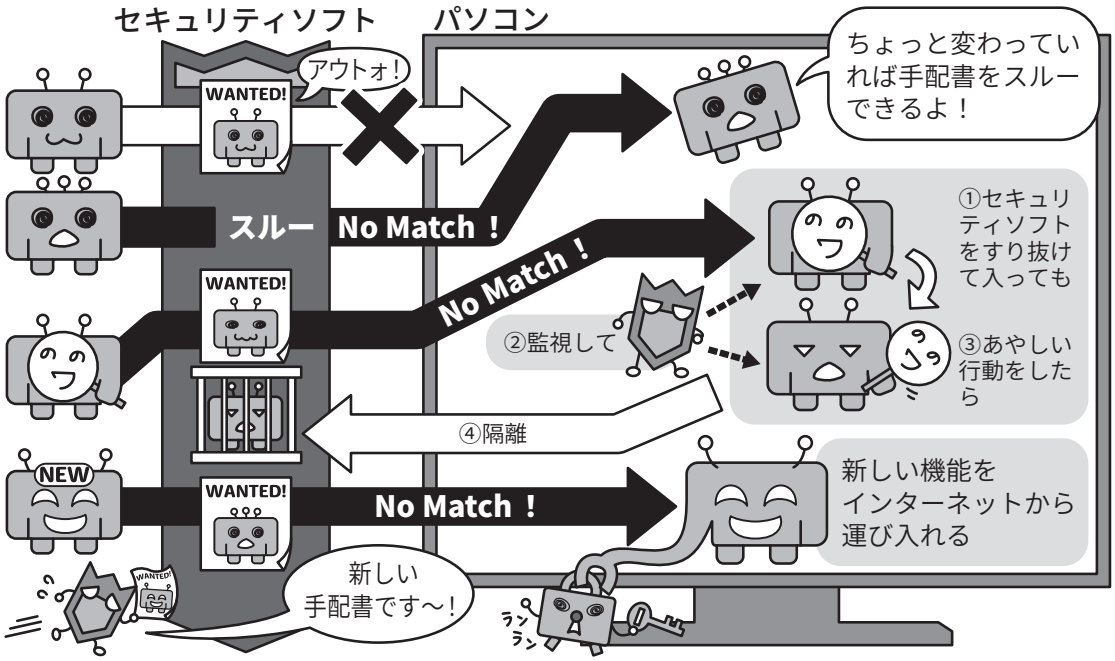
公共の場でロック解除をするときは、背後などから見られていないか気を付けましょう。

画面についた脂の跡を見る

スマホを席に残しておいたり、席取りのためにテーブルに置いて離れたりしてはいけません。

コラム.5 セキュリティソフトを導入しても過信しないことが重要

どんなセキュリティソフトでも、既知のマルウェア対策には有効だが、存在を知られていない新たな攻撃への対策は難しい



最近、一部のSNSやブログでは、「セキュリティソフトは不要」という論調の記事を見かけることがあります。本当に不要でしょうか？

個人利用の範囲では、OS標準で付属しているセキュリティソフトで事足りることも多く、企業利用でもOS標準のセキュリティソフトを用いることが増えています。

しかし、業務で使う場合、単純に攻撃をどれだけ防いでくれるか？という指標以外にも、複数のプラットフォームへの対応状況、企業内の端末管理用機能などもセキュリティソフト選びにおいては重要になってきます。

また市場流通するセキュリティソフトでは、パスワードマネージャーやネットバンキング保護など、OS標準のソフトには備わっていない機能も多く、ユーザーのさまざまな利用シーンに配慮している特長があります。

ただ、OS標準版、市場流通版、いずれにしろ使用する際、留意すべき点として共通しているのは、セキュリティソフトをパソコンやスマホにインストールした後は、アップデートし最新の状態を保つことです。なぜなら、セキュリティソフトがマルウェアを見つける方法に理由があります。

マルウェアを見つける方法は、事前に登録したマルウェアと同じ挙動をするプログラムを駆除する「手配書」方式、パソコン内に侵入された後も監視を続け不審な挙動があれば隔離や駆除を行う「ふるまい検知」、機能的に怪しい部分を検出する「ヒューリスティック分析」▶用語集P.187機能などが挙げられます。

これらは既知のマルウェア、既知の悪意あるふるまいを行うプログラムへの対策には有効ですが、検体▶用語集P.181が充分に収集されていないマルウェアや、まだ存在を知られていない全く新しいマルウェア、新たに考案された悪意あるふるまいの検知は難しいとされています。

セキュリティソフトを導入しているからといって過信はせず、「あやしいリンクはクリックしない」、「見覚えのないメールは開かない」と本ハンドブックでも解説する基本的なセキュリティ対策の徹底が重要です。

コラム.6 セキュリティ要件適合評価及びラベリング制度（JC-STAR）

サイバー攻撃の多様化・巧妙化が進む中、本文でも紹介した通り、IoT機器を狙った攻撃が増大し、これによる被害も大きくなっています。

従来、調達者・消費者にとって、IoT製品におけるセキュリティ対策が適切か否かの判断は難しい状況にありました。またサプライチェーン▶用語集 P.182・リスク管理の取組が広がる中、調達される製品が具備すべき、製品のセキュリティ機能や対策状況を確認することも難しいという現状があります。

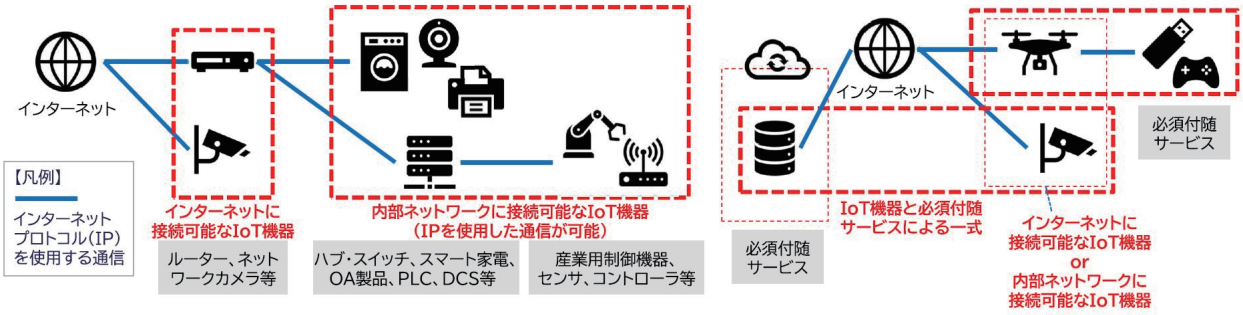
このような背景から、経済産業省から2024年8月に「IoT製品に対するセキュリティ適合性評価制度構築方針」が公表され、これに基づき、独立行政法人情報処理推進機構において2024年9月にIoT製品に対するセキュリティ適合性評価制度となる「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」を整備し、2025年3月から運用を開始することとなっています。

本制度では、これらの課題を解決するため、求められるセキュリティ水準に応じて、IoT製品共通の最低限の脅威に対応するための適合基準である★1（レベル1）とIoT製品類型ごとの特徴に応じた適合基準である★2（レベル2）、★3（レベル3）、★4（レベル4）を定め、適合が認められた製品には、二次元バーコード付きの適合ラベルを付与することで、製品詳細や適合評価、セキュリティ情報・問合せ先等の情報を調達者・消費者が簡単に取得できるようにしています。

また、スマートホームシステム、工場システム、ビルシステムなどの特定の分野や業界において類似の汎用的な構成で利用されるシステム（特定分野システム）で利用されるIoT製品に対するセキュリティ要件を定め、IoT製品に対するJC-STAR制度の活用を検討する際に参考となる情報を提供するため、経済産業省から2024年11月に「特定分野システムのIoT製品におけるJC-STAR制度活用ガイド（1.0版）」が公表されています。

セキュリティ要件適合評価及びラベリング制度

JC-STAR制度で適合ラベルが取得できる対象



JC-STAR制度のロゴ

適合ラベル（イメージ）

出所「IoT製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」（独立行政法人情報処理推進機構）

コラム.7 偽ショッピングサイトに注意しましょう

フィッシング攻撃では、偽の取引を行うために、本物のサイトと誤解されるようなサイトに誘導する場合もあります。このような偽ショッピングサイトについても特徴などを把握して、騙されないように注意しましょう。

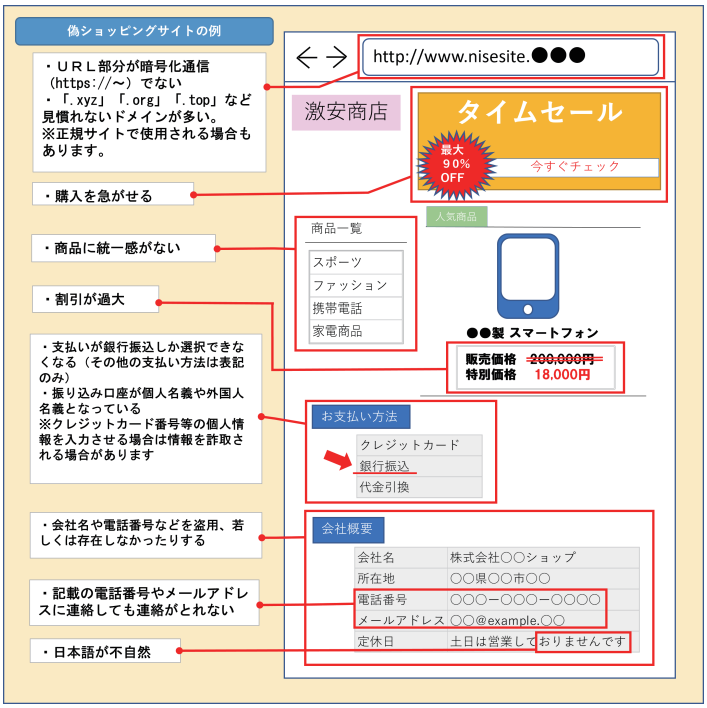
偽ショッピングサイトとは、正規のショッピングサイトを模倣する等により、利用者を騙して、取引に誘導するサイトです。その結果、利用者から購入代金を騙し取ったり、粗悪品を販売したりするなどが行われます。偽ショッピングサイトで商品を購入してしまった場合、商品が届かないことが多く、届いたとしても、偽物、全く別の物、空箱の場合もあります。

偽ショッピングサイトの特徴として、

- 価格が安い(商品価格が他のサイトと比べて極端に安価・割引率が高い)
- 支払い方法が銀行振込に限定されるものが多い(支払い方法としてクレジットカード決済が可能と記載があるものの、決済時に銀行振込のみ可能であると限定されることが多く、口座名義人は正規とは異なる法人、または法人と無関係の個人口座などが示される)。
- 不自然な日本語(文章の繋がりや単語などが不自然な日本語表現や、単なる誤記と考えにくい場合がある)
- URLのドメイン名(「.xyz」、「.top」等のTLD(トップレベルドメイン))を使用していることが多い。

などが挙げられます。

偽ショッピングサイトの特徴を知っておきましょう



偽ショッピングサイトの場合、いくつかの点で不審な点があります。一つでも気になったら、慎重に接しましょう。また不安な場合には、各種相談窓口で相談しましょう。

出所：「偽ショッピングサイト、詐欺サイトの手口」（警察庁）
(https://www.npa.go.jp/bureau/cyber/countermeasures/fake-shop.html)

偽ショッピングサイトには、フィッシング攻撃により、メールから誘導されるケースのほか、検索結果から誘導されるケース、広告から誘導されるケースなどがあります。

このうち、検索結果から誘導されるケースでは、検索結果の上位に偽ショッピングサイトへ誘導するサイトが表示される場合があります。偽ショッピングサイトの制作者がSEOポイズニングと呼ばれる攻撃手法を用いて検索結果でのサイトの表示順位を引き上げているためです。また広告から誘導されるケースでは、検索エンジンの検索結果には「広告」も表示され、この中に偽ショッピングサイトが表示されることもありますし、最近は、SNS上に表示された広告から偽ショッピングサイトへ誘導されるケースもあります。

このような偽ショッピングサイトの被害に遭わないようにするために、偽ショッピングサイトの特徴を踏まえたうえで、次の対応が重要です。

- 実在する会社であることを確認

する初めて利用するショッピングサイトでは、会社概要において、事業者の氏名（名称）、住所、電話番号が記載されているか確認しましょう。

・セキュリティ対策ソフトを利用する

市販のセキュリティ対策ソフトには、偽ショッピングサイトへのアクセスを防ぐ機能を持つものがあります。

- チェックサイトを活用する

「SAGICHECK」（https://sagicheck.jp/）や「Is it safe?」（https://global.sitesafety.trendmicro.com/）などのチェックサイトを活用することで、偽ショッピングサイトかどうかの判断に役立てることもできます。

偽ショッピングサイトの被害に遭った場合には、最寄りの警察又は消費生活センターに相談してください。また偽ショッピングサイト、またはこれと疑わしきサイトを見つけた場合には、悪質ECサイトホットラインへ連絡しましょう。

偽ショッピングサイト対策の参考になるサイト

参考となるサイト

一般社団法人日本サイバー犯罪対策センター（JC3）

「偽ショッピングサイトに注意」

（https://www.jc3.or.jp/threats/topics/article-462.html）

消費者庁

「インターネット通販トラブル」

（https://www.caa.go.jp/policies/policy/consumer_policy/caution/internet/trouble/internet.html）

警察庁

「偽ショッピングサイト・詐欺サイト対策」

（https://www.npa.go.jp/bureau/cyber/countermeasures/fake-shop.html）

一般社団法人セーファーインターネット協会

「悪質ECサイトホットライン　通報フォーム」

（https://www.saferinternet.or.jp/akushitsu_ec_form/）

9 ⑧外出先では紛失・盗難・覗き見に注意しよう

勤務先や外出先でスマホやパソコンを使う際に、誰かにスマホやパソコンを覗き見られている、そう感じたことはありませんか？

友人知人と冗談の範囲で「何やってるの～？」と1回2回茶化すくらいならまだしもあまりに覗き見の頻度が高かったり、あるいは見知らぬ人に何も言わずにずっと横や後ろから覗き見られてたりしているようならば要注意です。

見られている内容が機密情報であったり、秘匿したい個人情報であったりする場合には、あなたの情報が漏れる心配があります。

「見られても大したことない情報しか自分のスマホやパソコンには保存してないよ」と心配しない人も多いかもしれませんが、覗き見している人はあなたの情報もさることながら、あなたがやりとりしている相手がターゲットかもしれません。

「ロックをかけてあるから大丈夫」と思っても、ロックを解除する方法がすでに相手の手に渡っている懸念もあります。例えば、相手に直接接触せず情報を入手する方法として、電車で座席に座っている人のスマホ操作を見てPINコードやパターンロック形状を盗む「ショルダーハッキング」、カフェなどのテーブルに放置されているスマホの画面に残る指の脂跡からパターンロックを見破る方法などがあります。本章7.1(P.42)でも説明しましたが、飲食店などで席の確保にスマホなどを置き去りにする行為を時折見かけますが、紛失・盗難・覗き見、いずれの被害に遭ってもおかしくない非常に危険な行為です。このような行為は、すぐにやめましょう。

外出時は自分のスマホやパソコンが他人から見られる可能性は高い

外出時は、使用しているスマホやパソコンを他人から覗き見されないよう注意が必要です。また、うっかり紛失して盗難されれば、大事な情報が盗まれるリスクは大きく高まるので、よく注意しましょう。

スマホ使用時によく狙われるソーシャルエンジニアリング

ショルダーハッキング

公共の場でロック解除をするときは、背後などから見られていないか気を付けましょう。

画面についた脂の跡を見る

スマホを席に残しておいたり、席取りのためにテーブルに置いて離れたりしてはいけません。

10 ⑨困ったときは1人で悩まず、まず相談しよう

自ら、あるいは第三者からの連絡でサイバー攻撃に気付いた場合は、直ちに処置を取り、その後必要な各種窓口に相談しましょう。

あらかじめ対応者を決めてあるならば、その人を中心に対応するか、決めていない場合には、ITに詳しい社員などがいたらその人を中心に対処しましょう。

一番最初にするべきは電源を落とさないままインターネットから切断することです。これはマルウェアなどの拡散を防ぎつつ、後々警察に連絡をする場合の証拠保全になります。

次に、連絡するには状況を把握しなければならないので、なるべく分かる範囲で5W1Hのように分けて事象を記録しましょう。いつから始まったのか、どのようなことがあったのか、誰が作業していたのかなどです。

当然のことながらその間、攻撃が行われたと思われるパソコンなどの機器は使わず、その他の機器や紙のメモで記録します。

サイバー攻撃を受けたときに相談するサービスを契約している場合はそちらに相談し、無い場合は、IPAの相談窓口に相談しましょう。

ランサムウェアによりデータを暗号化されて脅迫されたり、情報を消されたり、何か機器を故障させられたり、あるいは情報を盗難されたりなど、明確に被害がある、もしくは被害に遭ったおそれがある場合は、各都道府県警のサイバー犯罪相談の窓口などに相談しましょう。

各種連絡窓口のウェブサイトなど

IPA「情報セキュリティ安心相談窓口（個人向け）」

https://www.ipa.go.jp/security/anshin/about.html
電話番号：03-5978-7509（受付時間：10時～12時　13時30分～17時
※土日祝祭日、年末年始除く）
メールアドレス：anshin@ipa.go.jp

IPA「サイバーセキュリティ相談窓口（企業組織向け）」

https://www.ipa.go.jp/security/support/soudan.html
メールアドレス：cs-support@ipa.go.jp

都道府県警察「サイバー犯罪等に関する相談窓口」

https://www.npa.go.jp/bureau/cyber/soudan.html

消費者庁「「消費者ホットライン」188」

https://www.caa.go.jp/policies/policy/local_cooperation/local_consumer_administration/damage/
電話番号：188

個人情報保護委員会「漏えい等の対応とお役立ち資料」

https://www.ppc.go.jp/personalinfo/legal/leakAction/

そして自社や団体で扱っている個人情報を盗まれたり消されたりしてしまった場合、個人情報保護委員会▶用語集P.182などへの速やかな報告、原因究明や再発防止策の策定などが求められます。ウェブサイトからフォーム入力による方法で報告できます。

* 詳しい報告先や対応方法は個人情報保護委員会ウェブサイトをご覧下さい。

コラム.3 攻撃されにくくするには、手間(コスト)がかかるようにする

サイバー攻撃を行う攻撃者は、軍事や産業スパイ▶用語集 P.183、名をあげること自体を目的に採算度外視でやる悪意のハッカーなどではない場合、なんらかの利益が目的の行動が多いということができるでしょう。

彼らにとってのサイバー攻撃はビジネスであり、ビジネスはコストパフォーマンス、つまりいかに手間をかけず大きな利益を生むかが重要です。

そういった攻撃者の視点から見ると、攻撃されにくい環境を作るにはどうしたらよいかが見えてきます。

例えば、現実世界では、泥棒は防犯がしっかりしていて警戒が厳重な家よりも、鍵をかけなかったり窓を開けっ放しで外出したりするような家の方に侵入します。その方が、彼らにとって安全、つまり手間(コスト)がかからないからです。

これは、ネットの世界でも同様です。侵入するまでに幾重にも難関があり、侵入を試みたら形跡を記録され(ログ▶用語集 P.189)、場合によってはしかるべき管理者に通知が行き、パスワードを破ろうとしても複雑で突破できない。システムも最新で、攻撃するにもセキュリティホールが見あたらない。セキュリティソフトも導入されている。さらに、ファイルを盗めても複雑な暗号化がされていれば、解読までに何百年もかかってしまい使えない。普通の攻撃者なら敬遠します。

横を見たら、セキュリティホールは放置、パスワードは非常に簡単だったり無しだったり、ファイルそのものも暗号化されておらず、パスワードを使っていても、たくさんのウェブサービスで全部同じものを使い回している。

これならば、どっちに行くのがビジネスとしてコストパフォーマンスがよいか明らかですよね。

こういった攻撃者の視点を持ち、侵入することがとても面倒くさく、攻撃したくなくなるような環境を構築するのが安全への近道です。

一方、単純な利益目的でない場合、すこし対策が変わってきます。

攻撃されにくくするには手間(コスト)がかかるようにする

コラム.4 利益が目的ではない攻撃に備えるには

金銭などの利益目的ではない攻撃の例としては、相手そのもの、つまり未成年者略取や、いかがわしい写真の入手などを目的とするものがあります。

現実の世界で、面と向かって「いかがわしい写真を撮らせてください」といったら、たいていの人は拒否して逃げ出すでしょう。それが、ネットの世界だと許容してしまう理由は、攻撃者がネットを利用して、警戒心をもたれないような人間になりすまし▶用語集P.185、相手をうまく騙してしまうからです。

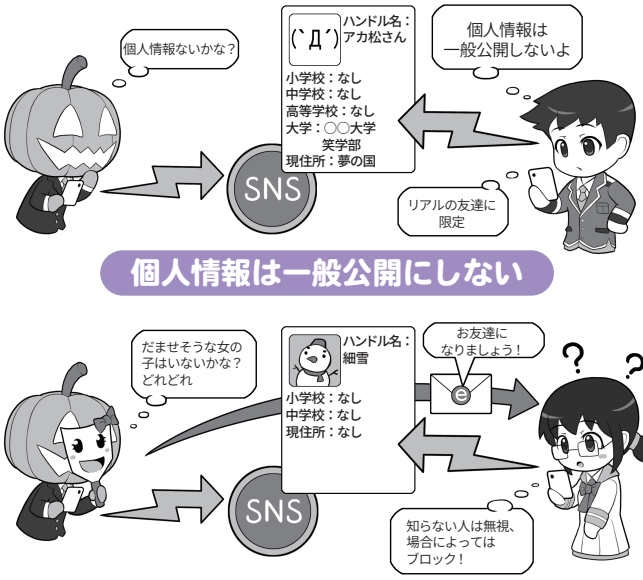
ですから、SNSや掲示板などのウェブサービスで知らない人物が近付いてきたら、注意して絶対に個人情報は教えないようにしましょう。現実の知り合いでもないのに会おうと誘われた場合は、基本的に会わないか、会う必要がある場合は必ず保護者同伴で行きましょう。

そして、少しでも変だなと思ったり、最初と話が違ったりした場合、それは人を騙す「心理的な」テクニックかもしれません。警戒し、その場から立ち去りましょう。

イントロダクション6(P.22)でも説明した「人を騙す心理的なテクニック(≒ソーシャルエンジニアリング▶用語集P.184)」は体系化されマニュアルのようになって存在するのです。

人を騙すこのようなテクニックは、なにも上記のような例だけでなく、私たちも日常生活のさまざまなシーンで直面しているのです。

金銭目的ではない攻撃にも備えよう



個人情報は一般公開にしない

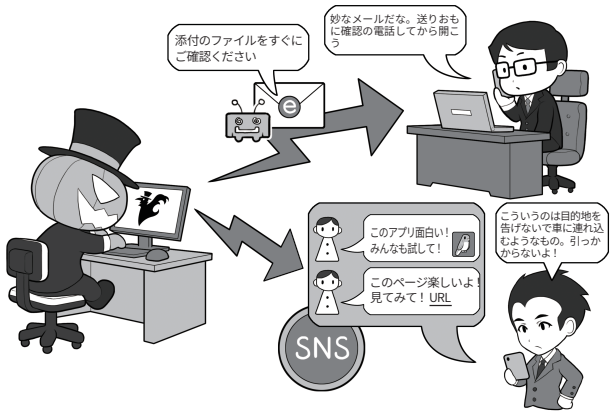
リアルで知り合いじゃない人とはネットで友達にならない！

未成年がSNSを利用する場合、写真や自分の個人情報を記載しないようにしましょう。また、投稿内容も原則的に一般に公開せず、SNSで友達になった人のみが見られる設定にしましょう。

SNSで、知らない人が友達になろうとリクエストを送ってきても、会ったことがない人はスルーするか基本的にお断り（ブロック）しましょう。

それは、現実の世界で自分の個人情報を書いた名札を付けて歩いたり、名前もわからない初めて会った人に、ついていったりするのと同じぐらい、たいへん危ないことなのです。

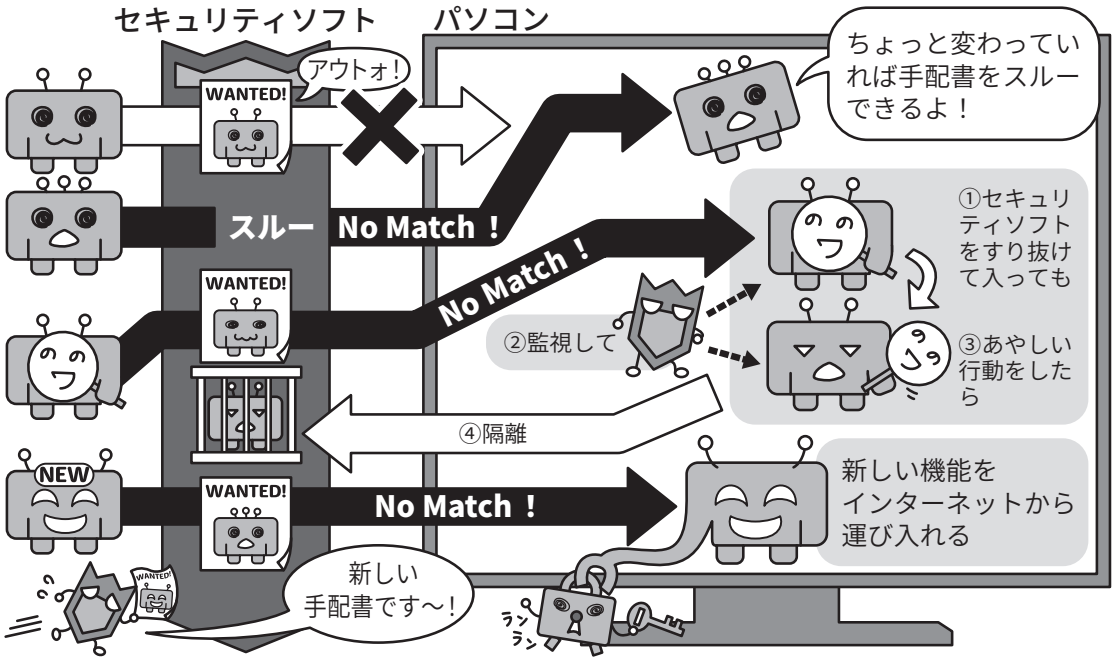
攻撃者に操られて、内側から鍵を開けてしまわないように、心がまえを持とう



不審なメールに気を付け、怪しいときは開かず送信者に確認する癖を付けましょう。ネットやSNSの引っかけは、セキュリティ関係のニュースをこまめに見ていると、次第に傾向がわかるようになります。訓練しましょう。

コラム.5 セキュリティソフトを導入しても過信しないことが重要

どんなセキュリティソフトでも、既知のマルウェア対策には有効だが、存在を知られていない新たな攻撃への対策は難しい



最近、一部のSNSやブログでは、「セキュリティソフトは不要」という論調の記事を見かけることがあります。本当に不要でしょうか？

個人利用の範囲では、OS標準で付属しているセキュリティソフトで事足りることも多く、企業利用でもOS標準のセキュリティソフトを用いることが増えています。

しかし、業務で使う場合、単純に攻撃をどれだけ防いでくれるか？という指標以外にも、複数のプラットフォームへの対応状況、企業内の端末管理用機能などもセキュリティソフト選びにおいては重要になってきます。

また市場流通するセキュリティソフトでは、パスワードマネージャーやネットバンキング保護など、OS標準のソフトには備わっていない機能も多く、ユーザーのさまざまな利用シーンに配慮している特長があります。

ただ、OS標準版、市場流通版、いずれにしろ使用する際、留意すべき点として共通しているのは、セキュリティソフトをパソコンやスマホにインストールした後は、アップデートし最新の状態を保つことです。なぜなら、セキュリティソフトがマルウェアを見つける方法に理由があります。

マルウェアを見つける方法は、事前に登録したマルウェアと同じ挙動をするプログラムを駆除する「手配書」方式、パソコン内に侵入された後も監視を続け不審な挙動があれば隔離や駆除を行う「ふるまい検知」、機能的に怪しい部分を検出する「ヒューリスティック分析」▶用語集P.187機能などが挙げられます。

これらは既知のマルウェア、既知の悪意あるふるまいを行うプログラムへの対策には有効ですが、検体▶用語集P.181が充分に収集されていないマルウェアや、まだ存在を知られていない全く新しいマルウェア、新たに考案された悪意あるふるまいの検知は難しいとされています。

セキュリティソフトを導入しているからといって過信はせず、「あやしいリンクはクリックしない」、「見覚えのないメールは開かない」と本ハンドブックでも解説する基本的なセキュリティ対策の徹底が重要です。

コラム.6 セキュリティ要件適合評価及びラベリング制度（JC-STAR）

サイバー攻撃の多様化・巧妙化が進む中、本文でも紹介した通り、IoT機器を狙った攻撃が増大し、これによる被害も大きくなっています。

従来、調達者・消費者にとって、IoT製品におけるセキュリティ対策が適切か否かの判断は難しい状況にありました。またサプライチェーン▶用語集 P.182・リスク管理の取組が広がる中、調達される製品が具備すべき、製品のセキュリティ機能や対策状況を確認することも難しいという現状があります。

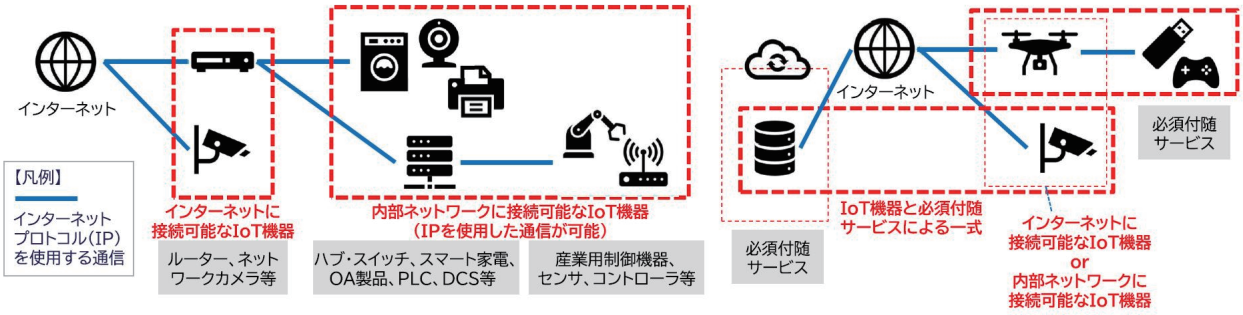
このような背景から、経済産業省から2024年8月に「IoT製品に対するセキュリティ適合性評価制度構築方針」が公表され、これに基づき、独立行政法人情報処理推進機構において2024年9月にIoT製品に対するセキュリティ適合性評価制度となる「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」を整備し、2025年3月から運用を開始することとなっています。

本制度では、これらの課題を解決するため、求められるセキュリティ水準に応じて、IoT製品共通の最低限の脅威に対応するための適合基準である★1（レベル1）とIoT製品類型ごとの特徴に応じた適合基準である★2（レベル2）、★3（レベル3）、★4（レベル4）を定め、適合が認められた製品には、二次元バーコード付きの適合ラベルを付与することで、製品詳細や適合評価、セキュリティ情報・問合せ先等の情報を調達者・消費者が簡単に取得できるようにしています。

また、スマートホームシステム、工場システム、ビルシステムなどの特定の分野や業界において類似の汎用的な構成で利用されるシステム（特定分野システム）で利用されるIoT製品に対するセキュリティ要件を定め、IoT製品に対するJC-STAR制度の活用を検討する際に参考となる情報を提供するため、経済産業省から2024年11月に「特定分野システムのIoT製品におけるJC-STAR制度活用ガイド（1.0版）」が公表されています。

セキュリティ要件適合評価及びラベリング制度

JC-STAR制度で適合ラベルが取得できる対象



JC-STAR制度のロゴ

適合ラベル（イメージ）

出所「IoT製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」（独立行政法人情報処理推進機構）

コラム.7 偽ショッピングサイトに注意しましょう

フィッシング攻撃では、偽の取引を行うために、本物のサイトと誤解されるようなサイトに誘導する場合もあります。このような偽ショッピングサイトについても特徴などを把握して、騙されないように注意しましょう。

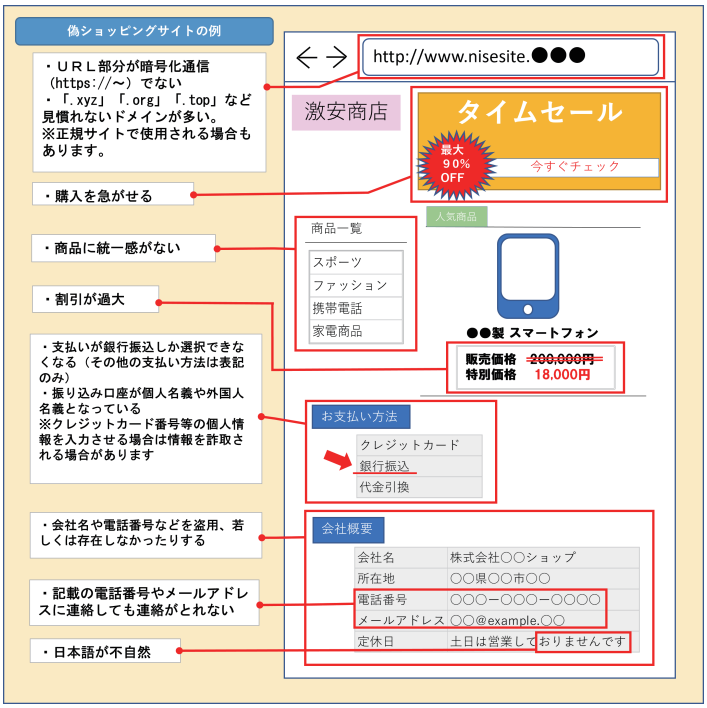
偽ショッピングサイトとは、正規のショッピングサイトを模倣する等により、利用者を騙して、取引に誘導するサイトです。その結果、利用者から購入代金を騙し取ったり、粗悪品を販売したりするなどが行われます。偽ショッピングサイトで商品を購入してしまった場合、商品が届かないことが多く、届いたとしても、偽物、全く別の物、空箱の場合もあります。

偽ショッピングサイトの特徴として、

- 価格が安い(商品価格が他のサイトと比べて極端に安価・割引率が高い)
- 支払い方法が銀行振込に限定されるものが多い(支払い方法としてクレジットカード決済が可能と記載があるものの、決済時に銀行振込のみ可能であると限定されることが多く、口座名義人は正規とは異なる法人、または法人と無関係の個人口座などが示される)。
- 不自然な日本語(文章の繋がりや単語などが不自然な日本語表現や、単なる誤記と考えにくい場合がある)
- URLのドメイン名(「.xyz」、「.top」等のTLD(トップレベルドメイン))を使用していることが多い。

などが挙げられます。

偽ショッピングサイトの特徴を知っておきましょう



偽ショッピングサイトの場合、いくつかの点で不審な点があります。一つでも気になったら、慎重に接しましょう。また不安な場合には、各種相談窓口で相談しましょう。

出所：「偽ショッピングサイト、詐欺サイトの手口」（警察庁）
(https://www.npa.go.jp/bureau/cyber/countermeasures/fake-shop.html)

偽ショッピングサイトには、フィッシング攻撃により、メールから誘導されるケースのほか、検索結果から誘導されるケース、広告から誘導されるケースなどがあります。

このうち、検索結果から誘導されるケースでは、検索結果の上位に偽ショッピングサイトへ誘導するサイトが表示される場合があります。偽ショッピングサイトの制作者がSEOポイズニングと呼ばれる攻撃手法を用いて検索結果でのサイトの表示順位を引き上げているためです。また広告から誘導されるケースでは、検索エンジンの検索結果には「広告」も表示され、この中に偽ショッピングサイトが表示されることもありますし、最近は、SNS上に表示された広告から偽ショッピングサイトへ誘導されるケースもあります。

このような偽ショッピングサイトの被害に遭わないようにするために、偽ショッピングサイトの特徴を踏まえたうえで、次の対応が重要です。

- 実在する会社であることを確認

する初めて利用するショッピングサイトでは、会社概要において、事業者の氏名（名称）、住所、電話番号が記載されているか確認しましょう。

・セキュリティ対策ソフトを利用する

市販のセキュリティ対策ソフトには、偽ショッピングサイトへのアクセスを防ぐ機能を持つものがあります。

- チェックサイトを活用する

「SAGICHECK」（https://sagicheck.jp/）や「Is it safe?」（https://global.sitesafety.trendmicro.com/）などのチェックサイトを活用することで、偽ショッピングサイトかどうかの判断に役立てることもできます。

偽ショッピングサイトの被害に遭った場合には、最寄りの警察又は消費生活センターに相談してください。また偽ショッピングサイト、またはこれと疑わしきサイトを見つけた場合には、悪質ECサイトホットラインへ連絡しましょう。

偽ショッピングサイト対策の参考になるサイト

参考となるサイト

一般社団法人日本サイバー犯罪対策センター（JC3）

「偽ショッピングサイトに注意」

（https://www.jc3.or.jp/threats/topics/article-462.html）

消費者庁

「インターネット通販トラブル」

（https://www.caa.go.jp/policies/policy/consumer_policy/caution/internet/trouble/internet.html）

警察庁

「偽ショッピングサイト・詐欺サイト対策」

（https://www.npa.go.jp/bureau/cyber/countermeasures/fake-shop.html）

一般社団法人セーファーインターネット協会

「悪質ECサイトホットライン　通報フォーム」

（https://www.saferinternet.or.jp/akushitsu_ec_form/）