

インターネットの

# 安全・安心 ハンドブック



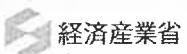
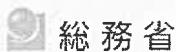
内閣サイバーセキュリティセンター  
National center of Incident readiness and  
Strategy for Cybersecurity

一般利用者向け 抜粋版



サイバーセキュリティ普及啓発

協力



Ver 5.00



# はじめに

みなさん、はじめてまして。私たち内閣サイバーセキュリティセンター(NISC)です。日本の政府機関で、国のサイバーセキュリティ政策を担当しています。突然ですが、世界中のコミュニケーションの手段と聞いたら、みなさんは何を思い浮かべるでしょうか？手紙、会話、写真、プレゼント、などいろいろなものを連想されるかもしれません。

その中でも、形は見えないけれど現代においては「インターネット」という技術が主役の1つだろう、と何となく意識されている方も多いのではないでしょうか。

インターネットによりコミュニケーションのスタイルは大きく変わりました。インターネットが普及していない昔は、どんな場所にも設置されていた公衆電話で連絡を取ることは普通でしたが、インターネットが身近になると小型化された携帯電話、いわゆるガラケーが普及しまし

た。当時のインターネットの通信速度では、ガラケーを使って短い文章、すなわちメッセージを送る形のコミュニケーションが主流でした。

そして現代、インターネットの通信速度も安定し、大半の国民がパソコンだけでなく、スマホを所有しています。スマホは単なる電話機ではなく、「持ち歩ける小さなパソコン」と呼べるほど多機能なもので、基本的に常にインターネットに接続しています。多くの人がスマホやパソコンからチャットしたり、SNSで写真を送りあったり、映像付きのインターネット電話を使ったりして、家族や友人とのコミュニケーションを楽しんでいます。コミュニケーションの用途以外にも、調べたいがあればブラウザでウェブサイトを検索したり、オンラインストアで買い物をしたりして、インターネットにつながったサービスに多くの人が慣れ親しんでいます。またクラウドと

呼ばれるインターネット上のサーバから業務上必要なデータの保存・共有をしたり、コロナ禍で普及したテレビ会議アプリでリモート会議をしたりと、仕事で多用している人もいるでしょう。さらには社会保障や税関係など、スマホやパソコンがあればできる行政機関への申請・申告も増えています。

もはや現代において、スマホやパソコンからインターネットにつながり、民間企業・公的機関問わず、無料・有料含めて、さまざまなサービスを利用することは、家庭や職場、学校と生活のあらゆる場面で求められています。多様なサービスにつながり多くのコミュニティが形づくられ、インターネット上には1つの社会領域といえる「サイバー空間」が形成されています。

そのような便利で欠かすことのできないサイバー空間は、地域や老若



男女問わず、全国民が参画する基礎的なインフラであると呼べ、私たちが社会経済活動を営む上で重要な公共性の高い場として位置付けられるものです。

しかし、このサイバー空間、便利さもあれば、問題もあります。

世界中のひとと距離を超えてつながるため、中には、自らの利益や自己顯示のために平気で他人の情報や財産を奪おうと悪事を働く者ともつながってしまいます。そのような悪事を働く者は、ありとあらゆる手段を用いて、スマホやパソコン、ルータなどのIT機器に対して、「マルウェア」という不正なプログラムを送りつけようとしています。インターネットにつながるということは、常にそのようなサイバー攻撃のリスクにさらされているのです。

また、SNSなどで自分の発言を広く読んでもらい自由に他の人と交流できることは、インターネットにつ

ながることで享受できるメリットの1つですが、接する人が常に自分と友好的な意見であるとは限りません。感情的になり、誹謗中傷といえるような発言が飛び交うことも珍しくありません。しかし、SNSでの発言から、精神的に追い詰められ、自らを傷付ける行為を選んでしまう人や事例も残念ながら生じています。面と向かって言えないような他人を傷付ける発言は、インターネット上でも決して発信してはいけないです。

サイバー空間が、人々のくらしと密接につながり基礎的なインフラとなりつつある中、国民全員が、誰一人取り残されずその恩恵を享受していくためには、国民一人ひとりが能動的にサイバー空間における攻撃や脅威の存在を知り、サイバーセキュリティに関する素養・基本的な知識を身に付けていくことが必須です。スマホやパソコンを使ってインターネットにつながるときは、みんなが

常にサイバーセキュリティ対策を心掛けるべきなのです。

そのため本書では、サイバー攻撃の手口やリスク、そして被害とはどんなものがあるのかをイメージしやすくなるように、身近な具体例を取り上げながら解説しています。そして、被害を受けないようにするにはどんな対策をすればよいのか？また被害を受けてしまった場合はどんな対処をすればよいのか？についても、具体的な手順や頼れる相談窓口を紹介しています。

ほかにも、

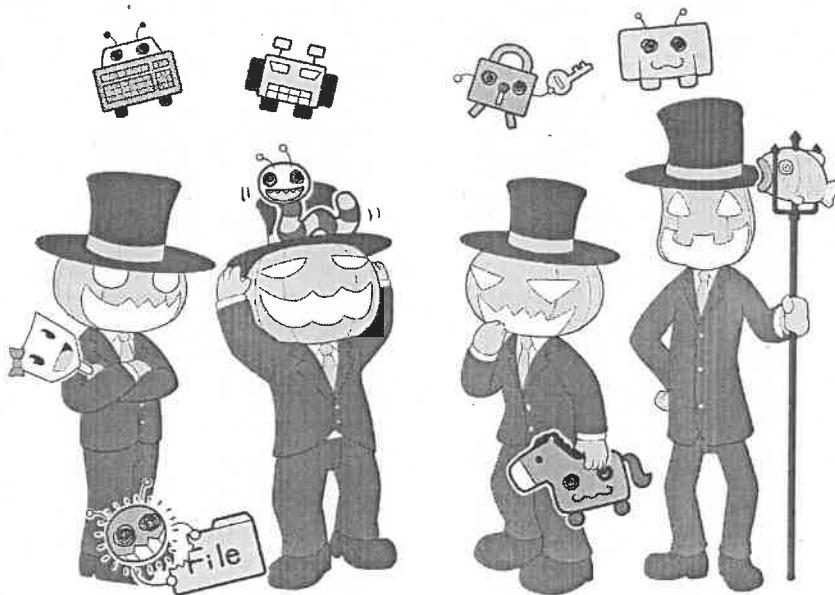
- ・サイバー攻撃を防ぐための基本となるパスワードの適切な管理
- ・こどもやシニアが安全にインターネット上のサービスを利用するための方法
- ・SNSなどで多くの人と交流する際に気を付けたいマナーや法律
- ・スマホやパソコンを不安なく利用するための設定

このイラストはインターネット上の悪意の人たちである攻撃者と、彼らが使う武器である「コンピュータウイルス（正確にはマルウェア）」をキャラクターにしたもの。

サイバー空間（インターネット）を悪意を持って利用し、自らの利益のためには他人の情報や財産を容赦なく奪い、ときにサイバー攻撃を通じて自己顯示欲を満たすといった、さまざまな悪事を働きます。

また、彼らが普通の人の仮面を被り、あるいは普通の人々が彼らの仮面を被ることもあります。

解説のイラストではそのあたりをきちんと描き分けていきますので、じっくり見てくださいね。



- ・災害や海外など普段とは違う環境でインターネットにつながるときの事前の対策
  - ・インターネットにおける通信の安全性を支える暗号化の基本
  - ・中小組織のセキュリティ部門担当者に役立つ情報
- など、サイバーセキュリティ対策に必要な内容を幅広く取り上げ、いずれも読む前には専門知識を必要とし

ない形でやさしく説明しています。本書を読んで、安全・安心なサイバースペース空間と一緒に作っていきましょう。

また、NISCでは、本書だけにとどまらず、「みんなで使おうサイバーセキュリティ・ポータルサイト」を運営して、サイバーセキュリティの普及啓発や人材育成に取り組んでいます。

ポータルサイトでは、こども、シニア、企業の一般社員・経営者など対象者別に適したセキュリティ施策の紹介や、セキュリティ施策におけるセミナーやイベントの実施状況などを公開しています。本書やポータルサイトをご覧いただき、国民一人ひとりのサイバーセキュリティ対策の意識を高められれば幸いです。



## 「みんなで使おうサイバーセキュリティ・ポータルサイト」

<https://security-portal.nisc.go.jp/>

### ※ご注意

本書では、初心者の方にサイバーセキュリティ関連の問題を理解してもらうために、実際のケースと比較してわかりやすく簡略化したり、内容を理解しやすいように関連する事項の一部を省略したりして記述している場合があります。ご了承ください。

このハンドブックを読んで、よりサイバーセキュリティに関する理解を深めていきたいと思う方は、ぜひステップアップして、さまざまな専門誌や最新の記事にチャレンジしていただけると幸いです。

なお、登場する人物、および、団体は架空のものであり、実在するいかなる人物・団体とも関係はありません。

# 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(悪意のハッカー)による攻撃を防ぐには、まずはパソコンやスマートホン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、政府系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(内閣官房内閣サイバーセキュリティセンター)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「①OS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のことです。IT機器にはセキュリティホール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を設定する際の留意点、同じパスワードの使い回しの危険性、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について解説し

### 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多要素認証を利用するよう



認証用アプリや生体認証を利用して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、公式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。

ます。認証用アプリや生体認証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、公

式サイト以外からアプリをインストールする危険性を解説します。

「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、近時また猛威を振るう「Emotet」のように、マルウェア添付メールで広がる感染、標的型メールやスパムメールの実例を挙げ、具体的なリスクについて解説します。

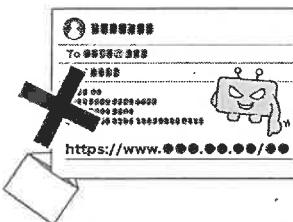
「⑥スマホやPCの画面ロックを利用しよう」は、スマホやパソコン(PC)の情報を守るにはまず待ち受け画面をロックすることが第一であることを解説します。また、生体認証を使用したロックの利点や、安易に他人へ端末を渡す危険性についてもふれます。

「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をとっておくことがどれほど重要なか解説します。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、サイバー攻撃などインターネットの被害で自分で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

## 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PC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



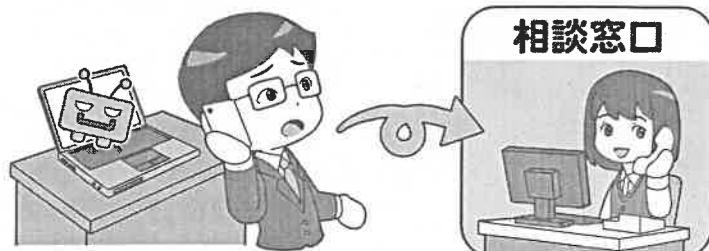
たとえ攻撃されても、適切にバックアップしておけば、すぐに復旧できます。

## 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ぬ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。

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対策9か条」<https://www.nisc.go.jp/pdf/council/cs/jinzai/dai17/17shiryou0101.pdf>

# ①OSやソフトウェアは常に最新の状態にしておこう

## ①.1 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)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るなら、自主的に更新処理をかけるようにしましょう。Office製品などOSのメーカーが作っている重要なソフトもここで同時にアップデートします。

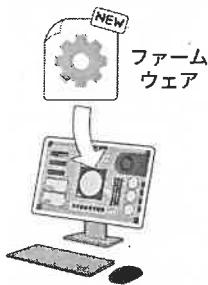
次に、サイバー攻撃で狙われやすいソフトウェアの更新を重点的に行いましょう。Adobe社 Acrobat Reader や Oracle 社 Java、そして Google Chrome をはじめとする各種のウェブブラウザは攻撃のターゲットになりやすいのです。

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、自分の機器用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。

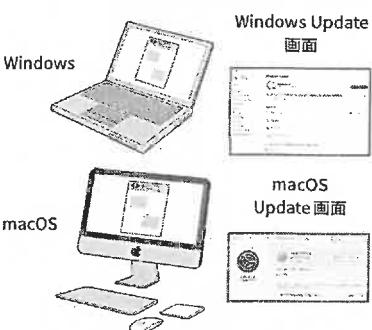
セキュリティソフトをインストールしている場合は、最新のウイルス定義ファイルに自動更新されるよう設定しておきましょう。

### 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

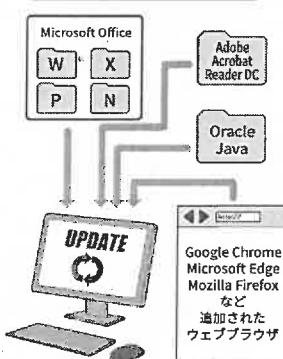
#### 本体のファームウェアも更新



#### OSと重要ソフトの更新



#### 重要ソフトも更新



#### セキュリティソフトも更新



OSやファームウェアなどは、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、そのためほとんどのパソコンで利用されています。

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重要ソフトは削除(アンインストール)してしまってもよいでしょう。

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。

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しているものが多く、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脆弱なので、使用しないようにしてください。

## ①.2 スマホやネットワーク機器も最新に保とう

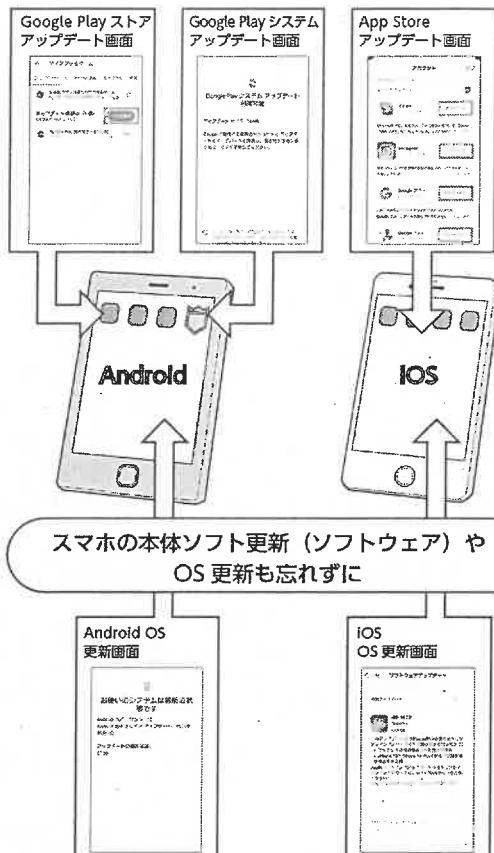
スマホも同様に各種のアップデートの適用が必須です。スマホの場合、比較的アップデートの通知がわかりやすくなっています。自動アップデート機能も充実しています。機器本体のファームウェアのアップデートでも、OSのアップデートでも、いつも使用している一般的なアプリのアップデートでも、更新の通知が出たら、マメに適用するようにしましょう。そのためには、本体のファームウェア(ソフトウェア更新やシステムアップデートと書かれることもある)やOSの更新が、設定メニュー上のどこにあるのかと、更新の手順を確認しておきましょう。アプリの更新が自動になっているかも確認しましょう。

スマホアプリの自動更新は、設定によっては無線LAN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変更で確認が必要な場合は自動更新されないこともありますので、気が付いたら未更新のアプリがたくさんたまつ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、更新作業を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やIoT機器、スマート家電なども脆弱性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。2022年以降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。

## 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

### ②.1 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」、文字の組み合わせをすべて試す「総当たり攻撃」、パスワードによく使われる文字列を利用する「辞書攻撃」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な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、

#### ログイン用パスワードは英大文字小文字+数字+記号で10桁以上

「ログインに使うパスワードは、英大文字小文字+数字+記号で10桁以上」の理由

「数字のみ」の10乗だと→100億通り

(英大文字小文字+数字+記号(88個として))の10乗だと→約2785京97兆6009億通り

数字だけで10桁と、英大文字小文字+数字+記号で10桁では雲泥の差がある。  
そしてこれほど多量な組み合わせは、機械入力でも事実上突破不可能。

#### 英大文字小文字+数字+記号混じりの組み合わせ数

アルファベット(大)+アルファベット(小)+数字+記号(例)

$$26 + 26 + 10 + 26 = 88$$

数字	英大文字	英小文字	記号	合計	5	6	7	8	9	10	
10			10	數	100,000	1,000,000	10,000,000	100,000,000	1,000,000,000	10,000,000,000	
10	26		36	數英	6,405,156	2,175,422,165	75,391,164,796	251,193,757,456	1,153,955,659,451	3,656,152,440,323,76	
10	26	26	62	數英大+小	915,172,837	35,893,725,584	1,271,616,606,708	41,840,154,544,875	11,273,385,342,762,551	32,259,265,834,340,224	
10	26	26	26	98	數英大小記	5,271,129,158	444,944,585,764	16,961,505,689,792	130,952,242,25,259	216,470,391,325,582,341	77,560,975,636,940,128

これに26文字の記号を入れると約88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、ログイン用パスワードであれば入力ごとに遅延がかかるので、英大文字小文字+数字+記号混じりで10桁以上を安全圏として推奨します。しかし、より組み合わせ数を増やし安全性を高めるにこしたことはありません。

### ②.2 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ログイン可能になってしまします。複雑なパスワードを1つ決めて、あとはお尻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

同じパスワードを使い回さない。似たパスワード、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	たこ クレジット	
×使い回し	PASSPPOI	PASSPPOI	PASSPPOI	PASSPPOI	1個漏れたら一網打尽
×お尻だけ違う	PASSPPO1	PASSPPO2	PASSPPO3	PASSPPO4	推測しやすい
×法則性あり	USAGIPPOI	OSARUPPOI	NEKOPPOI	TACOPPOI	法則性がばれたらおしまい

ドを設定し、使い回しをしないこと

が大切です。

## ②.3 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しますし、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。

1つは、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。もう1つはスマホのパスワード管理アプリを利用する方法です。なお、後者の場合、クラウド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。

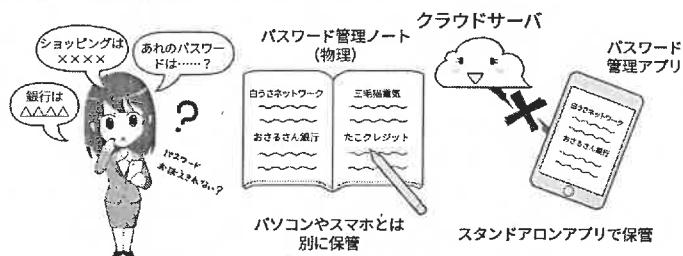
利用するところで保管するべきでないなら、スマホでパスワードを管理する場合リスクはありますが、こ

### 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。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。

### ウェブブラウザの自動入力にパスワードを覚えさせない



パスワードなどの自動入力は便利ですが、仕事場などであなたがパソコンをロックしないまま席を離ると、他人が各種サービスにログインし放題になります。

ういいったアプリは後述のPINコードや指紋認証+暗号化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。落としたスマホが戻るとは限りませんから。

## ③多要素認証を利用しよう

### ③.1 可能な限り多要素や生体認証を使い、秘密の質問にはまじめに答えない

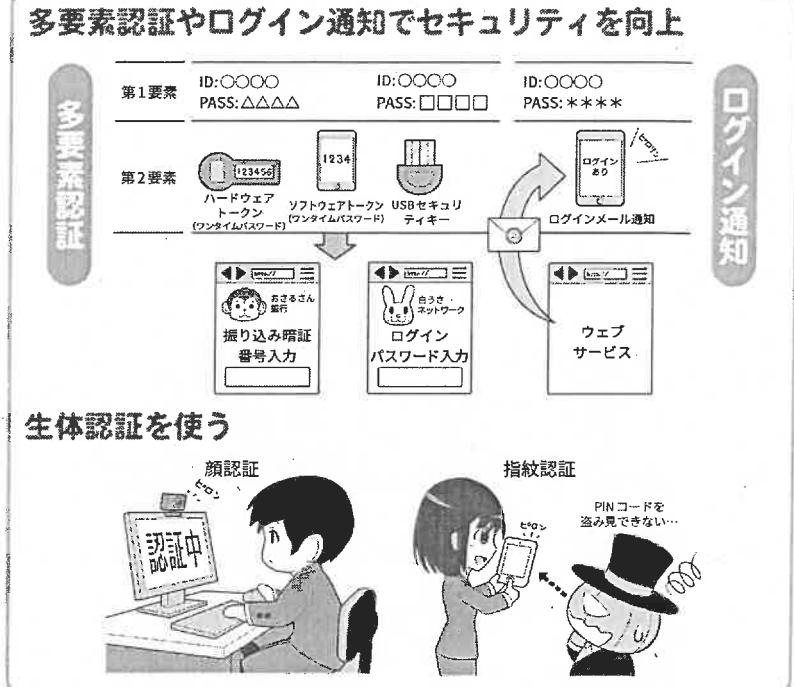
サービスへのログインを安全に行うために、二要素以上を使って認証作業をする多要素認証などの方法が提供されていれば必ず設定しましょう。これらの方では通常のパスワードの他に、使い捨てにする別のパスワードを、ハードウェアトークンや生成アプリで作り、ログイン時に利用者に入力させます。メールやSMS・ショートメッセージを利用する方式もありますが、これらは安全面で非推奨です。

その他にも、USBセキュリティキーなどで利用者を確認する方法や、不正アクセス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。

また、最近の機器では顔、虹彩、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って安全性が高く、肩越しの盗み見などによる暗証番号(PINコード)の盗難には強い機能であります。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、スマート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。

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できます。攻撃者がパスワードなど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。

その他の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」と呼ばれる機能で対応しようと/or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。

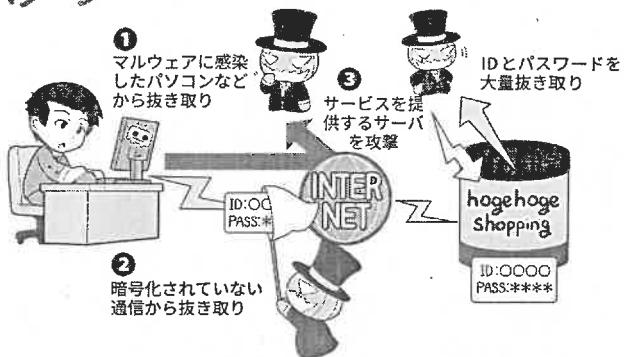
SNSが普及した今、ネット上で簡単に見つけられることもあり、安全性が高いとはいえない。秘密の質問に答えを設定する場合は推測できないものにし、忘れないようにパスワード管理アプリなどに保存しましょう。

## ③.2 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

攻撃者は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。

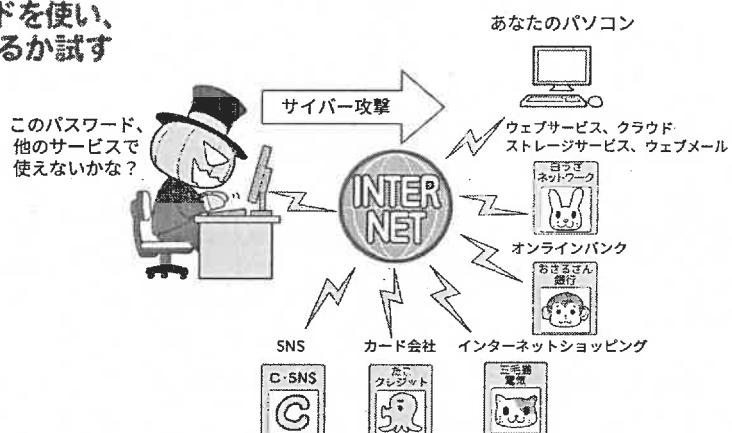
ニュースや通知でサービス側から流出が判明した場合は、速やかにパスワードを変更するなどの対応を取りましょう。



### 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か？

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いても、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、とも言いたりません。

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かいか、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、現金は送れなくと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。

## ④ 偽メールや偽サイトに騙されないように用心しよう

### ④.1 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。これは、攻撃者からしたら攻撃のためのコストを低く抑えられるためです。

偽メールには、スマートフォンの偽SMSやSNSで使用可能なメッセージ機能なども含みます。

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。下記のリンクから確認して欲しい」というようなSMS(ショートメッセージ)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だま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、国税庁を装つたりETCサービスを装つたりと、騙さ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

#### フィッシング詐欺はいろんな方法がある

SMS(ショートメッセージ)



電話番号宛てに送る

電子メール(eメール)



メールアドレス宛に送る

メッセージ(アプリなど)



アプリのアカウント宛に送る

ゲーム内のメッセージ機能



ゲームのユーザー宛に送る

「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 Twitter @nisc\_forecast

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。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

セージのURLなどにアクセスするのではなく、後述するような対処を行ってください。

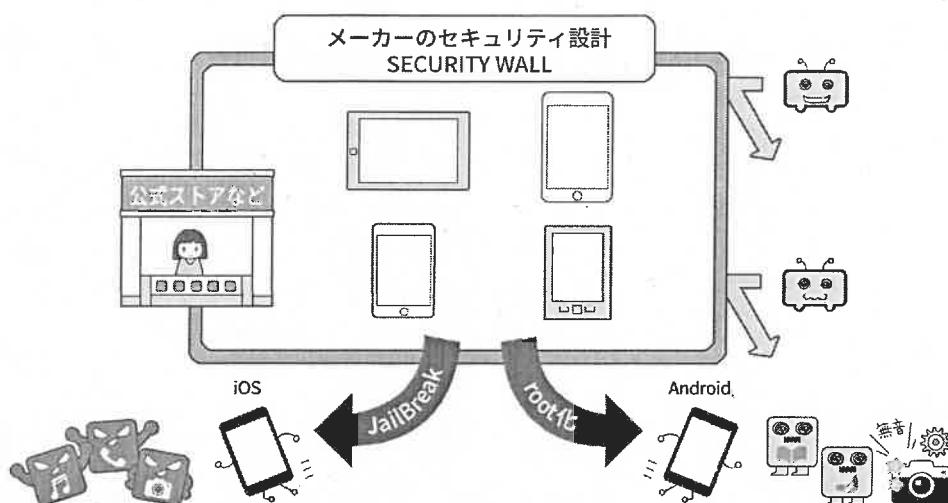
他にも、地震が発生したときに、気象庁を名乗って津波に関する迷惑メールが送られた例もありました。いずれも私たちが「だまされないぞ」と身構えているのとは違う方向や、災害時で正常な判断が行えない状況を狙っています。

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。

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(<https://www.antiphishing.jp/>)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。

## ④.2 公式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

### サイドローディング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。非公式なアプリをインストールする「サイドローディング」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、脆弱になるので非常に危険で、やってはいけません。

前項で紹介した偽メール、偽サイトの手法は多様化していて注意が必要ですが、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る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。

公式ストアで配信されるアプリに関しては、公式ストアでの配信前に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。

公式のアプリストア以外のサイトからアプリをダウンロードすることを「サイドローディング」、さらに非公式なアプリのインストール以外にもスマホを標準にはない設定に変更できる改造を「root化」「JailBreak」と呼びますが、これらはセキュリティレベルを下げるためやってはいけません。

サイドローディングは、アプリをさまざまなサイトからインストールできることで企業間の競争が促進される可能性があるかもしれません。しかし、アプリの審査を行うためには、費用や時間・労力が必要です。で、何もチェックを行わず自由に公開を許すようなサイトよりは、運営費用がかかるのは当然で、そのようなコストが価格に反映される点も考慮する必要があります。また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、脆弱になるので非常に危険です。

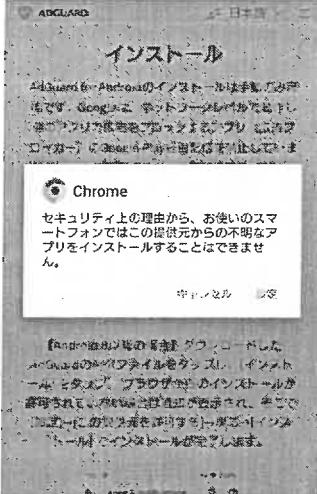
スマホには、個人に関する重要な情報がたくさん存在していますから、リスクの高いアプリをインストールし、重要な情報が漏えいしてしまうと、取り戻しがつきません。アプリを利用する際には、安全を確保するために一定の費用が必要なことと、アプリの審査を行っている信頼できるストアを使うという観点が不可欠です。

例えばスマホの場合、iOS機器は公式のストア以外からはアプリを導入できない仕組みになっていますが、Android機器の場合は公式ストアやベンダー・メーカーのストア以外からもアプリをインストール可能です。それを利用し攻撃者がメールやSMSなどであなたを誘導して、公式ストアでない場所から不明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、不明なアプリをインストールしないためにもこの設定はオフのままにしておくようにしましょう。

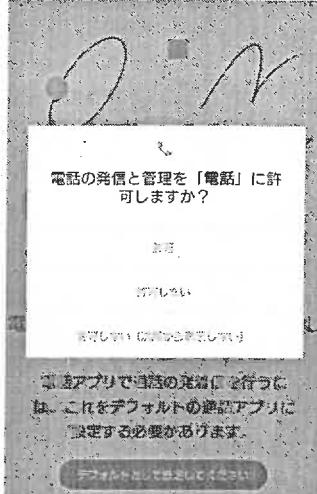
また、Android機器でもiOSでも、

「不明なアプリ」と  
いう言葉に注意



This screenshot shows a warning message from the AdGuard app asking if the user wants to install it from an unknown source. It includes a note that such installations are not recommended for security reasons.

導入時や起動時の  
権限付与に注意



This screenshot shows a permission request for a call-related app. It asks for permission to manage calls and makes a note that this is required for the app to function correctly.

• **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せようとするものは、すべてセキュリティ上危険なものと判断するようにし、最初から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、基本的に公式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。

• **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、そもそも必要な権限を求めるアプリは怪しいと警戒しましょう。

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。

その他、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。

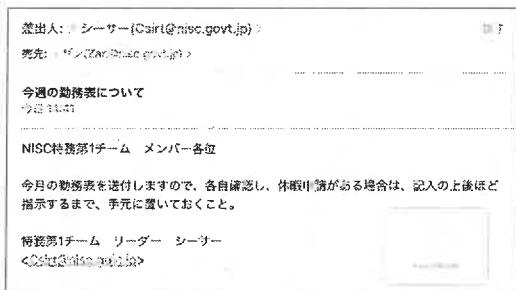
このような場合は、ニュースサイトでそのような事案が紹介されることが多いので、情報収集時に気にかけておくとよいでしょう。

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。

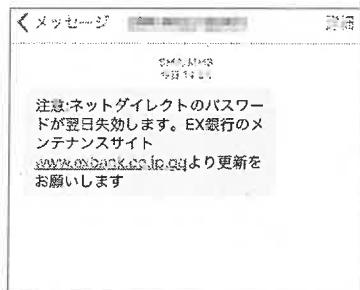
## ⑤メールの添付ファイルや本文中のリンクに注意しよう

### 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(ショートメッセージ)を使った例



前節で述べた「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、基本信用ならないものとして、むやみやたらに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。

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、「フィッシングメールの例」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を模したものです。

送信元とされる金融機関の口座を

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、現在もこういった攻撃に引っかかる人が一定の割合でいます。その先が詐欺サイトではなく、ゼロデイ攻撃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、実はこのアプリがマルウェア入りだったり、あるいは拡散する間は無害でも、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、警戒するでしょうか？

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。

## ⑥スマホやPCの画面ロックを利用しよう

### ⑥.1 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、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にしくみの1つです。

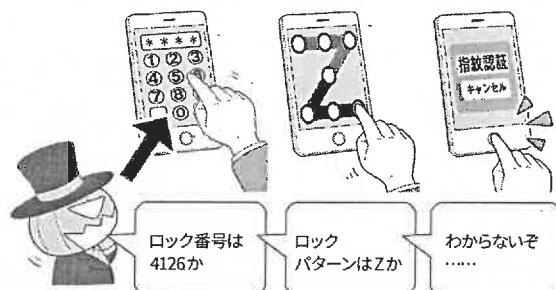
とくに生体認証は周りから覗かれ PINコードを盗まれる危険性の排除をしつつ、入力の面倒しさを省くので便利な機能です。

指紋認証や顔認証が代表的ですが、その他にも、スマートウォッチなど特定のウェアラブル機器を着けたり、GPS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脆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

#### スマホやパソコンにはロックをかけよう

PINコードによるロック      パターンによるロック      生体認証によるロック



#### 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、プライバシーを窺かれたり、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。

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。

## ⑥.2 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いなれば、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、スマートフォンのロックをなんらかの方法でパスできたとしても、また、別の閂門が待ち構えているわけで、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、スマートフォンロック解除のPINコードと異なるものを設定します。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つてこそ意味があるのです。

スマートフォンをロックしていても情報漏洩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。ロック画面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漏洩してしまったり、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問題のある情報を提供してしまうことになります。

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漏洩してしまうことがあります。そ

### 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、同じく情報を漏洩してしまう原因になります。スマートフォン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……。情報漏洩には気をつけましょう。

### 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ートフォンを残してはいけません。なお、勝手に他人のスマートフォン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。

うするとスマートフォン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、画面を除き見ただ

けの第三者によって認証が突破できてしまいます。

# ⑦大切な情報は失う前に バックアップ(複製)しよう

## ⑦.1 何をするにもバックアップを取ろう

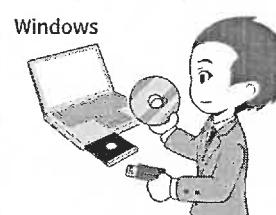
各種のサイバー攻撃や、パソコン・スマホの故障などからいち早く復旧して事業を継続するには、システムやデータのバックアップが不可欠です。とくに近年は感染するとファイルを暗号化して身代金を要求するランサムウェアの流行により、バックアップの重要性が格段に上がってきます。バックアップの方法は主にパソコンやスマホのOSの種類により異なっています。パソコンの場合には、macOS搭載の機器のように、外付けの補助記憶装置(ハードディスクやSSD。以降記憶装置)を接続するだけでバックアップが行え、復旧もシステムとデータすべてをほぼ全自動で行えるものもあります。これに対してWindows搭載機器では、基本的にはデー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。

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。この機能は機器を紛失した場合にも、新しい機器を接続すると全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。なお、バックアップを取得するだけではなく、できれば取得した

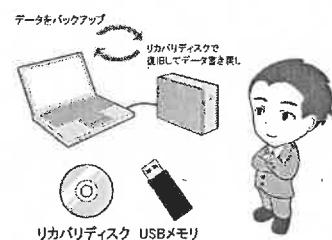
### macOS機器、Windows機器のバックアップと復元



mac OS機器はあ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。

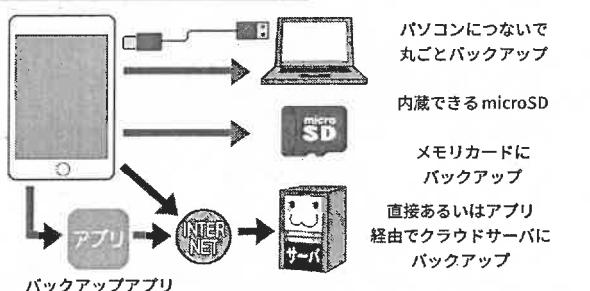
実際は他にも専用のソフトウェアを導入したり、細かい設定を変えることで、バックアップの方法を変える手段はあります。

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ーに  
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。

バックアップを用いてちゃんとシステムの復元を行えるか確認してください。

## ⑦.2 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か。

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、かなり難しい運用が求められます。

また、最近は大雨による水害で、事務所にあったパソコンと外付け記憶装置が両方とも水没して復旧が困難になるという話もありました。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。

遠隔地とは、現実的には「クラウドサーバ」などの利用を意味します。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。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、最近のクラウドでのバックアップはランサムウェアの巻き添えになりにくい規格のものもあるので、利用にあたっては調べてみましょう。

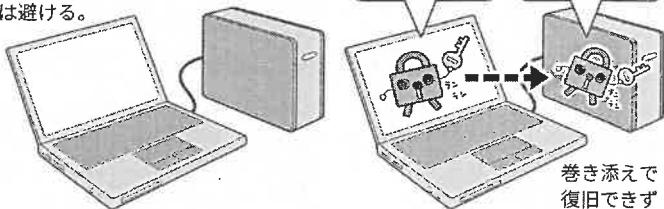
### ランサムウェア感染はビジネスにも影響



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。

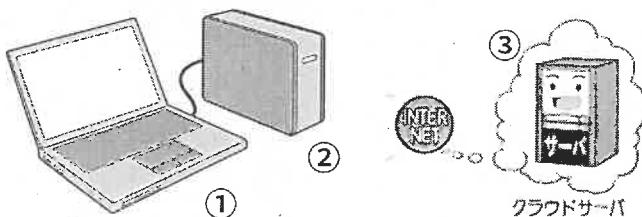
### バックアップの体制を整える

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。

## 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いないよ」と心配しない人も多いかもしれません。しかし、覗き見している人はあなたの情報もさらることながら、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、相手に直接接觸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。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

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に注意が必要です。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。

行為です。ついやってしまう、という人はすぐにやめてください。

## ⑨困ったときは1人で悩まず、 まず相談しよう

自らサイバー攻撃に気付いたり、あるいは第三者からの連絡で気付いた場合は、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「情報セキュリティ安心相談窓口」のウェブサイトを検索して、類似の例がないか調べてから、電話やメールで相談しましょう。

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

### 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」

<https://www.ipa.go.jp/security/anshin/>  
電話番号：03-5978-7509(平日 10:00-12:00, 13:30-17:00)  
メールアドレス：anshin@ipa.go.jp

#### J-CRAT/ 標的型サイバー攻撃特別相談窓口

<https://www.ipa.go.jp/security/tokubetsu/index.html>  
メールアドレス：tokusou@ipa.co.jp

#### 東京中小企業サイバーセキュリティ支援ネットワーク (Tcyss)「中小企業サイバーセキュリティ相談窓口」

<https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/tcyss.html>  
電話番号：03-5320-4773(平日 9:00-12:00, 13:00-17:00)

#### 経済産業省「サイバー犯罪等に関する相談窓口」

<https://www.npa.go.jp/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/](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/>

窓口などに相談しましょう。

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、「望ましい対応」として、原因究明や再発防止策の策定、そして「努力義務」として個人情報保

護委員会などへの速やかな報告が求められます。

従来はファックスや郵送での報告ですが、令和元年3月からは、ウェブサイトからフォーム入力による方法で報告できるようになりました\*。

\* 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。