国民のための
サイバーセキュリティサイト

総務省

事前対策

（セキュリティ事故を未然に防ぐためには）

一般利用者向けの対策

インターネットを使ったサービスは、私たちの生活のあらゆる場面に浸透しており、私たちは日々、その利便性を享受しています。しかし同時に、インターネットにはさまざまな脅威も潜んでいます。

そこで個人個人が、インターネット上の脅威によりなんらかの被害に遭わない様にするために最低限意識してほしいことおよび、その他にも意識した方がよいことを紹介します。

目次

推測できる簡単なパスワードを利用しないようにしよう

パソコンにログインする等、インターネットのネットオークションやショッピングサイトを利用する際において、なりすましを防ぐための認証には、一般的にパスワードが利用されています。そのため、コンピュータやインターネットを利用する上では、どのようなパスワードを使用するかということが、とても重要なことであると言えます。

パスワードの適切な管理（安全なパスワードの作成、保管、更新）はパソコンやサーバを安全に利用するためには欠かせません。自分のパスワードの管理について再度確認をしてください。

パスワードの適切な管理には、以下の 3 つの要素があります。

■安全なパスワードの設定
安全なパスワードとは、他人に推測されにくく、ツールなどで割り出しにくいものを言います。

理想的には、最低でも 10 文字以上の文字数で構成されるある程度長いランダムな英数字の並びとし、パスワード内に数字や記号、アルファベット（大文字、小文字）が混ざっていることが好ましいですが、覚えなければならないパスワードの場合は、無関係な（文章にならない）複数の英単語をつなげたり、その間に数字列を挟んだりしたものであれば、推測されにくく、覚えやすいパスワードを作ることができます。
近年では、スマートフォンやＷｅｂブラウザの標準機能として、パスワード生成機能があるものもありますので、そういったものをうまく活用しましょう。

逆に、危険なパスワードとしては、以下のようなものがあります。このような危険なパスワードが使われていないかどうか、チェックをするようにしましょう。

(1) ID と同じ文字列
(2) 自分や家族の名前、電話番号、生年月日
　　yamada、tanaka、taro、hanako（名前）
　　09011112222（電話番号）
　　19960628、h020315（生年月日）
　　tokyo、kasumigaseki（住所）
　　3470、1297（車のナンバー）

(3) 辞書に載っているような一般的な英単語ひとつだけ

password、baseball、soccer、monkey、dragon

(4) 同じ文字の繰り返しやわかりやすい並びの文字列

aaaa、0000（同じ文字の組み合わせ）

abcd、123456、200、abc123（安易な数字や英文字の並び）

asdf、qwerty（キーボードの配列）

(5) 短すぎる文字列

gf、ps

この他、郵便番号、社員コード、他人に一度でも教えたことがあるパスワードなど、他人から類推しやすい情報やユーザ ID と同じものなどは避けましょう。

■パスワードの保管方法

せっかく安全なパスワードを設定しても、パスワードが他人に漏れてしまえば意味がありません。以下が、パスワードの保管に関して特に留意が必要です。

・パスワードは、同僚等の第三者に教えずに、秘密にすること
・パスワードを電子メールでやりとりしないこと
・パスワードのメモをディスプレイなど他人の目に触れる場所に貼ったりしないこと
・やむを得ずパスワードをメモなどで記載した場合は、鍵のかかる机や金庫など安全な方法で保管すること

なお、各サービスで異なる充分に安全なパスワードを覚えておくのは大変なので、パスワードを覚える必要のない、パスワード管理ツールを使うことも推奨されます。スマートフォンや Web ブラウザ標準機能、あるいは専用のアプリケーションのパスワード保存機能を活用しましょう。これらのツールやサービスは、マスターパスワード（覚えられる充分に安全なもの）や、利用デバイス（スマートフォンなど）のロック（生体認証など）で守る必要があります。

■パスワードを複数のサービスで使い回さない（定期的な変更は不要）

パスワードはできる限り、複数のサービスで使い回さないようにしましょう。サービスから流出したアカウント情報を使って、他のサービスへの不正ログインを試す攻撃の手口が知られています。もし重要情報を利用しているサービスで、他のサービスからの使い回しのパスワードを利用していた場合、他のサービスから何らかの原因でパスワードが漏洩してしまえば、第三者に重要情報にアクセスされてしまう可能性があります。

なお、利用するサービスによっては、パスワードを定期的に変更することを求められることもありますが、実際にパスワードを破られアカウントが乗っ取られる等のサービス側から流出した事実がない場合は、パスワードを変更する必要はありません。むしろ定期的な変更をすることで、パスワードの作り方がパターン化し簡単なものになることや、使い回しをするようになることの方が問題となります。定期的に変更するよりも、機器やサービスの間で使い回しのない、固有のパスワードを設定することが求められます。

これまでは、パスワードの定期的な変更が推奨されていましたが、2017 年に、米国国立標準技術研究所（NIST）からガイドラインとして、サービスを提供する側がパスワードの定期的な変更を要求すべきではない旨が示されたところです（※1）。また、日本においても、内閣サイバーセキュリティセンター（NISC）から、パスワードを定期変更する必要はなく、流出時に速やかに変更する旨が示されています（※2）。

（※1） NIST SP800-63B（電子的認証に関するガイドライン）
（※2） インターネットの安全・安心ハンドブック Ver 4.20 p.61
https://security-portal.nisc.go.jp/handbook/index.html

IPA 独立行政法人情報処理推進機構にてパスワードを安全に利用するための情報が公開されているため合わせて確認してください（※3）。

（※3）チョコっとプラスパスワード
https://www.ipa.go.jp/security/chocotto/

【コラム～多要素認証（2 要素認証）を活用しよう～】

より安全性を高めた認証の方式として、多要素認証や二段階認証があります。
多要素認証は、通常のユーザ名とパスワードに加え、追加のセキュリティ要素を使用してアカウントへのアクセスを確認する方法です。多要素認証の要素には
「知っているもの（知識要素）（例）パスワードなど」
「持っているもの（所持要素）（例）スマホなど」
「本人自身に関するもの（生体要素）（例）指紋、静脈、顔、虹彩など」
があり、これらのうち 2 つ以上の要素を組み合わせて認証します。これは、より高度なセキュリティを提供することができ、不正アクセスやハッキングなどの脅威からアカウントを保護するのに役立ちます。

身に覚えのないリンク（URL）を開かないようにしよう

近年フィッシング詐欺が増えており、その手口として Web サイトへ誘導するリンクを本文中に埋め込んだメールや SMS をユーザへ送付するものが多く報告されています。
マルウェアの感染もメール・SMS のリンク経由が多くなっています。
送信してきた相手が知人や仕事上の取引先だと警戒心が薄れてしまい、ついリンクをクリックしたり添付ファイルを開いたりしがちですが、そこが犯罪者の狙いです。さらに最近は手口が巧妙化し、金融機関や宅配業者からの緊急通知を詐称するものが多く注意が必要です。
取引先などに巧妙に偽装した「標的型攻撃」メールによる被害も急増しています。添付ファイルやリンク付きのメール等を受け取った場合は細心の注意を払いましょう。

メールや SMS で外部アクセスするリンクには十分に気を付ける必要があります。

■　**マルウェア（コンピュータウィルスやランサムウェア）に感染しないために**

メール本文中のリンクを安易にクリックしないことは重要ですが、添付されているファイルにも注意しましょう。マルウェアの実体はコンピュータプログラムですが、ファイルをよく確認せずに開いて（実行して）しまうとプログラムが起動しマルウェアに感染します。通常のマルウェアはセキュリティソフトで検知できる場合も多いですが、オフィスソフト（Word や Excel 等）に組み込まれたマクロ言語で書かれたマクロウイルスは、セキュリティソフトで検知できないケースが多く注意が必要です。
最近のオフィス製品は初期状態でマクロ機能がオフに設定されていますが、攻撃者は言葉巧みに「マクロの有効化」を促したり、無条件にマクロが実行できるフォルダへファイルを移動させたりしようとします。少しでも不審な点があればマクロ機能を有効にすべきではありません。

サポート切れソフトウェアを利用しないようにしよう

OS やアプリケーションを最新にしましょう

コンピュータはソフトウェア（プログラム）で制御され動作しています。ソフトウェアには、OS（基本ソフト）や Web ブラウザなどのアプリケーションの他、ネットワーク機器、家電製品などで動作しているファームウェアなどがあります。

これらのソフトウェアには、製造時の欠陥（バグ）や新たな攻撃手法に対する弱点（セキュリティホール）が発見されることがしばしばあり、脆弱性(ぜいじゃくせい）と呼ばれています。脆弱性を残したままでは、いくら他の対策を実施したとしても不正アクセスなどのサイバー攻撃を防ぎきれません。

この問題を解決するためには、ソフトウェアメーカーなどから提供される修正プログラムを速やかに適用して（アップデート）、ソフトウェアを最新の状態に保つように心がけなければなりません。

近年では、ネット接続されるスマート家電やカーナビゲーションなども増えてきました。これらもコンピュータが内蔵されてソフトウェアで動作している点で変わりはなく、脆弱性を放置したままにしておくと攻撃者に不正アクセスされるリスクが高まります。

パソコンやスマホでは、修正プログラムが提供された場合に、「ソフトウェアの更新が必要です」などの形でソフトウェアアップデートの通知が表示されることが多くなっています。通知が表示されたら、速やかに更新しましょう。また、自動更新機能がある場合は、この機能を有効に設定するのもよい方法です。

ネットワーク機器や家電、IoT 機器など、ソフトウェアアップデートの通知が無い機器では定期的にメーカーのホームページを確認するか、自動更新機能を有効にして確実にソフトウェアの更新ができるようにしておきましょう。

■ サポート期間が終了するソフトウェアに注意

■ ソフトウェアのサポート期間

ソフトウェアを安全に利用するためには開発元や機器メーカーから配布される更新プログラムを早急に適用することが重要ですが、更新プログラム配布等のサポートは一定期間で終了するものがあります。サポート期間が切れたソフトウェアは脆弱性が発見された場合も修正されないといったセキュリティ上の懸念があります。

サポート期間を見逃し易いものとして、ソフトウェアの中にはソフトウェア単体で動作するものだけでなく、他のシステムやアプリケーションに使用されているものがあります。その場合、気づかないうちにソフトウェアのサポート期間が切れ、セキュリティ上のリスクを抱えるといったことが発生します。こうしたソフトウェアのサポート期間はソフトウェアの提供元が予め公表しているものもあります。サポート終了時期を事前に把握しておき、計画的に更新を行いましょう。

■ Windows 10 のサポート期限 Office 2016

多くのユーザが利用している Microsoft 社の OS、Windows１０ですが、2025 年 10 月 14 日に製品サポートが終了となると発表されています。同社では、現在 Windows11 に移行することを強く推奨しています。

同様に Office 製品も Office 2016 の延長サポートが 2025 年 10 月 14 日で終了と発表されています。

セキュリティ対策ソフトを活用しよう

マルウェア（コンピュータウイルスなど電子機器に脅威となるようなプログラム）は、電子メールやホームページ、記憶媒体など、さまざまな経路からコンピュータに侵入して、情報漏洩（ろうえい）やデータ破壊などの被害をもたらします。侵入されると、自分のコンピュータが被害を受けるだけでなく、インターネットや記憶媒体を通じて他人のコンピュータに感染を広げ、加害に加担することにもなりかねません。
現在のほとんどのコンピュータには、OS やウェブブラウザの機能として、セキュリティ対策ソフトが標準装備されていますので、それを有効に活用して被害を防ぎましょう。
セキュリティ対策ソフトには、主に以下の機能があります。

- 電子メールやホームページ、CD-R、USB メモリなど外部からコンピュータが受け取るデータにマルウェアが含まれていないかをチェックし、マルウェアの侵入を防ぎます。
- ウェブブラウザで閲覧しようとするサイトが、偽サイトや攻撃サイトとしてすでに報告されているところであれば、アクセスをブロックします。
- ファイアウォール機能を有効にすると、不要な通信を遮断して、不正に操作される危険性を減らします。

もっとセキュリティ機能が必要と感じるなら、OS に標準装備されているものの他に、市販のセキュリティ対策ソフトの購入を検討してみるのもよいかもしれません。ただし、有償の対策ソフトは、有効期限が過ぎるとアップデートされなくなり、性能が低下していきますので、料金を支払い続けることが必要です。

OS によっては、市販の対策ソフトがインストールされると、OS 標準装備の対策ソフトが機能を停止するものがあります。その場合、市販の対策ソフトを期限切れのまま使い続けることは、かえって危険になります。特に、期間限定で無料にて試用できる「体験版」の対策ソフトを初めからインストールした状態で販売されているパソコンを使用している場合、体験版の有効期限が切れると危険な状態になります。料金を支払う予定がないのであれば、早めにアンインストールして、OS 標準装備の対策ソフトの機能が作動するよう、元に戻しておきましょう。

また、セキュリティ対策ソフトが機能していれば対策が万全ということではありません。対策ソフトのアップデートが間に合わず、マルウェアが対策をすり抜けてしまうことも少なくありません。対策ソフトは公衆衛生における「マスク着用」のようなものと考え、そもそも、知らない人からの電子メールやメッセージの添付ファイルを不用意に開かないように

したり、怪しいホームページはできるだけ閲覧しないようにしたりするなどの注意が必要です。

古い Wi-Fi 機器を利用しないようにしよう

無線 LAN は、ケーブルの代わりに無線を利用するという性質上、通信内容が傍受（盗聴）される危険性があります。そのため、無線 LAN を使ってユーザ ID やパスワードなどのログイン情報、クレジットカード番号のほか、プライバシー性の高い情報をやり取りする場合には、自分と相手先との間で通信が暗号化されていることを確認しましょう。

家庭内や職場のネットワークで複数のパソコンを利用する際には、家族や職場のパソコンとファイルのやり取りを円滑に行うために、ファイル共有機能を有効にしている人もいるかもしれません。しかし、公共の場で無線 LAN を利用するときに、このファイル共有機能が有効になっていると、他人からパソコンやスマートフォン内のファイルが読み取られたり、ウイルスなどの不正なファイルを送りこまれたりすることがあります。公共の場で無線 LAN を利用する際には、必ず他の端末等からアクセスがされないような設定にしましょう。

一方で、自宅内などに自分で無線 LAN のアクセスポイントを設置して利用する場合には、アクセスポイントで暗号化の設定を行ってください。現時点では、WPA2 方式または WPA3 方式による暗号化を推奨します。WPA3 の方が、より強固な暗号化方式を利用できます。旧来から WEP という暗号化方式もありましたが、WEP は短時間で解読される方法が発見され、安全な方式とは言えなくなっていますので、使用は推奨しません。

また、アクセスポイントに設定する管理パスワードや、認証・暗号化のための共有鍵（暗号化キーや PSK キー）は、単純なものや、無線 LAN のネットワーク識別子である SSID から類推できるものにしないよう、注意が必要です。一般的に SSID は公開されて使用されるため、SSID と似たパスワードを設定していると、第三者に類推されてしまう可能性があるからです。共有鍵が知られると、第三者がアクセスポイントに接続できたり、通信内容が容易に解読できたりします。安全なパスワードの設定に関しては、下記のリンクを参照してください。

さらに、最近では、自動ファームウェア更新や機種ごとに異なる ID/パスワードが最初から設定されている等のセキュリティ機能を強化した無線 LAN 機器が普及していますので、そのような機器を積極的に利用することをお勧めします。

PII（個人識別用情報）を不用意に公開しないようにしよう

PII（個人識別用情報：Personally Identifiable Information）とは、氏名、性別、生年月日のほか、住所、メールアドレス、電話番号などの連絡先情報や、顔写真、身分証番号など、個人を識別するために使用される又はされ得る情報のことです。この情報が第三者に知られた場合、迷惑メールを送りつけられたり、迷惑電話がかかってきたり、なりすましや不正ログインに使われたり、誹謗中傷あるいは脅迫、強盗、誘拐などの犯罪に利用される可能性もないとはいえません。

とはいえ、氏名や生年月日を表明してインターネット上で情報発信するのは個人の自由ともいえ、氏名や生年月日は必ず伏せるべきものというわけではありません。連絡先や顔写真を公開するのも個人の自由でしょう。

ただ、他人の公表されていない PII を、本人に断りなく公開してしまうと、その人に迷惑をかけることになるかもしれません。最近では X（旧 Twitter）、Facebook、Instagram など様々な SNS が普及しています。一部の SNS では、実名でのプロフィール登録が必要なサービスもあります。どのような情報を登録し、何がどの範囲まで公開されるのかをよく確認したうえで、適切な設定で利用するように注意しましょう。

特に、未成年者子どもの PII については要注意です。自分の情報が将来どのように使われることになるのか、自分で判断をすることが難しい年齢のうちは、保護者が判断してあげることも大切です。

また、氏名を明かさない場合でも、「cookie」を PII にして、ウェブサイトのアクセス履歴が自動的に収集されることがあります。収集されたアクセス履歴に基づいて個人に合わせた広告が表示されたりすることがありますが、そういった収集を望まない場合、拒否する（オプトアウトする）ことができるのが一般的です。
同様に、マイナンバーや基礎年金番号などの身分証番号を不用意に提示すると、履歴を取集するために流用される危険性があります。本来これらの番号は目的外に利用することが法律で禁止されており、目的外利用される危険性は少ないですが、不用意に提示しないようにしましょう。

なお、ここでいう「PII」（個人識別用情報）は、個人情報保護法の「個人情報」や「個人データ」のことではありません。個人情報や個人データについては、法律に従った取り扱いが求められます。

使わなくなった機器を放置しないようにしよう

パソコンやスマートフォンの情報機器、ハードディスク（SSD）、DVD や USB メモリなどの外部記録媒体は、個人に関する情報のほか、さまざまな情報が記録・保管されています。こうした機器を廃棄する際に、そのまま廃棄業者に依頼したり、不燃物として廃棄したりする場合、第三者にこれらの機器から情報を詐取される危険性もあります。

特に注意が必要なのは、保存されているデータを削除したり、ハードディスクをフォーマットしたりしただけで、パソコンを処分してしまう場合です。画面上でデータが消えているように見えても、実際にはハードディスク上にデータが残されたままになっていることがあり、特殊なソフトウェアを利用することで、削除されたはずのファイルを復元することが可能です。

情報漏洩（ろうえい）を防ぐためにも、こうした機器を廃棄する場合は、事前にデータを消去して廃棄しましょう。データの消去方法には以下の方法があります。

■スマートフォン
使用している機種によりますが、初期設定状態にする機能が付いている場合は、購入初期状態にしてから廃棄しましょう。スマートフォンは端末販売店で回収をしていることも多いため、そうした信頼できる事業者に廃棄を依頼するか、安全に廃棄できるリサイクル業者を選んで廃棄を依頼すると良いでしょう。

■ハードディスク（SSD）
専用のデータ消去ソフトなどを使うことで安全に消去が可能です。信頼できるリサイクル業者を選んで廃棄を依頼することもできます。
なお、SSD についてはその特性からハードディスク用のデータ消去ソフトでは完全に消去できない場合があるので、専用のソフトを使用するか物理的な破壊などを検討しましょう。

■DVD や USB メモリなどの外部記録メディア
他のパソコンで読み込めないように、傷を付ける、もしくは物理的に壊すなどして不燃物として廃棄しましょう。