基本的なセキュリティ対策

基本的なセキュリティ対策を実施し、安全にインターネットを利用してください。

① OSやソフトウェアの適切な更新

○ぜい弱性対策

ぜい弱性（セキュリティホール）とは、OS[*1] やソフトウェア、ネットワーク機器等において、プログラムの不具合や設計上のミスが原因となって発生したセキュリティ上の欠陥を言います。

ぜい弱性が放置された状態でコンピュータやネットワーク機器等を利用していると、不正アクセス、ウイルス感染、ウェブサイトの改ざん、情報漏えい等の被害に遭うおそれがあります。

したがって、OS やソフトウェア、ネットワーク機器等のぜい弱性情報を収集し、メーカーが提供する修正プログラム（パッチ）を速やかに適用（OS やソフトウェア等を更新）して、OS やソフトウェア、ネットワーク機器等を最新の状態に保ってください。

一度、ぜい弱性を塞いでも、新たなぜい弱性が発見される可能性があるので、継続的に対策を講じてください。

ぜい弱性情報については、ソフトウェア等を開発したメーカーのウェブサイトのほか、次のウェブサイトでも確認できますので、参考にしてください。

JVN iPedia 脆弱性対策情報データベース（外部サイト）
（https://jvndb.jvn.jp）

○ゼロデイ攻撃

ゼロデイ攻撃とは、メーカーが修正プログラムを配布するまでの間（ゼロデイ）に、OS やソフトウェア、ネットワーク機器等のぜい弱性を利用して行われる攻撃を言います。

修正プログラムが配布されていないため、根本的な対策を講じることは困難ですが、ウイルス対策ソフト等の導入、ネットワークやパソコン等の挙動監視等によって、被害の未然防止・拡大防止を図ることが大切です。

---

*1　OS：パソコンやスマートフォンなどの基本的な機能を管理するソフトウェア。
（例：Windows、iOS、Android など）

② IDとパスワードの適切な管理

ID とパスワードが窃取されてしまうと、不正アクセスされ、サーバやネットワーク機器等を乗っ取られたり、サービスを悪用されたりします。そのような被害に遭わないために ID やパスワードは、適切に管理してください。

○初期パスワードの変更

初期パスワード（デフォルトパスワード）は、初期のテストやインストール、設定等に使用するため、ソフトウェアやインターネットサービス、ネットワーク機器等にあらかじめ設定されているパスワードです。

多くの場合、初期パスワードは製品やサービスごとに共通で、取扱説明書等に記載されているため、初期パスワードを変更せずにソフトウェアやサービス、ネットワーク機器等を使用していると、攻撃者にそれらを乗っ取られる危険があります。

初期パスワードは必ず変更してください。

○安全なパスワードの設定

単語や生年月日等を含めたパスワードは、攻撃者に簡単に推測されてしまいますので、次の例を参考に、安全なパスワードを設定してください。

- **パスワードの文字列は 10 文字以上にする。**
- **推測されやすい単語や数字、生年月日、キーボードの配列順等の文字の並びや ID は含めない。**
- **大小英字・数字・記号を全て使う。**
- **複数の ID でパスワードを使い回さない。**

○「コアパスワード」の活用

(1) コアパスワードの作成

趣味や興味のあることなどから決めたフレーズを基に、覚えやすく、強度の強いパスワードを作成します。これを全てのパスワードで共通して使用するコアパスワードとします。

例)「テレビが好き」というフレーズをコアパスワードにする方法
(1)　ローマ字へ変更　「terebigasuki」
(2)　一部を大文字に　「terebiGAsuki」　※ ga を GA に変換
(3)　記号・数字を追加　「terebiGAsuki!!06」※記号「!!」数字「06」を追加
(4)　強度の高いコアパスワード「terebiGAsuki!!06」が完成

(2) コアパスワードの活用

サービス名の略称、頭文字等から、サービス毎に短い文字列を決めます。

これをサービス毎の識別子として、コアパスワードの前又は後に追加します。

（作成例）

サービス名	サービス毎の識別子	コアパスワード
abcクラウド	abc	terebiGAsuki!!06
いろは銀行	irh	terebiGAsuki!!06

完成したパスワード
abc terebiGAsuki!!06
irh terebiGAsuki!!06

コアパスワードが共通でも、異なる識別子を追加すれば、サービス毎に異なるパスワードが作成可能となり、パスワードの使い回しが回避できます。

○パスワードやIDの適切な管理方法

パスワードや ID は、次の例を参考に適切に管理してください。

- パスワードは他人に教えない。
- ID、パスワードは、紙にメモして、人目に触れない場所で保管する。
- ID、パスワードは、不用意にインターネット上で入力・記録しない。
- ネットカフェ等、不特定多数が使用するパソコンでは、ID、パスワード等を入力しない。
- 利用頻度の低いサービスや不要なサービスの ID は削除する。

○ワンタイムパスワード等の二段階認証機能の活用

通常のパスワードに加え、インターネットサービスが提供する生体認証（指紋、顔等）やワンタイムパスワード（ログイン時に一定時間だけ有効なパスワード）を利用する二要素認証機能を活用することで強いセキュリティとなります。また、二要素認証以上の多要素認証を活用することで、安全性はより高まります。

○ログイン履歴機能、ログインアラート機能の活用

ログインの履歴を確認することで、心当たりのない不正なアクセスに早期に気がつくことができます。また、通常と異なる時間帯やアクセス元からログインされた際にメールが送信されるアラート機能を活用することも有効です。

○IDとパスワードが流出してしまったら

ログインできる場合は、ログインしてすぐにパスワードを変更するとともに、アクセス履歴を確認してください。不審なアクセス履歴を発見した場合は、被害の状況をサービスの提供者やシステム管理者に連絡してください。

ログインできない場合は、サービスの提供者やシステム管理者に連絡して、ID の停止、被害状況の確認等を依頼してください。

クレジットカードや銀行口座情報等を登録していた場合は、クレジットカード会社や銀

行に使用停止を依頼してください。

※　他人の ID・パスワードを不正利用しログインすることは、不正アクセス禁止法違反に該当するおそれがあります。

○事業者の方へ

従業員やサービスの利用者等が設定するパスワードは、使用しなければならない文字数や種類を可能な限り増やすなど、簡単に推測されるパスワードを設定できないようにするとともに、ワンタイムパスワード等の二要素認証や二経路認証を積極的に採用し、認証を強化してください。

また、利用者に対して、パスワードの適正な設定について周知してください。

なお、退職や異動、サービスの退会等の理由により、従業員やサービスの利用者等が ID、パスワード等を利用する立場でなくなった場合には、割り当てていた ID の削除・停止やパスワードの変更を速やかに行ってください。

③ ウイルス対策ソフト等の導入等

○ウイルス対策ソフト等の導入

コンピュータ・ウイルス（不正プログラム）に感染してしまうと、情報が窃取されたり、バッグドアと呼ばれる不正な侵入口を設置されたりするため、必ずウイルス対策ソフト等を導入してください。

ウイルス対策ソフトがパソコンにインストールされている場合には、通常、パソコンのタスクバーにウイルス対策ソフトが動作していることを示すアイコンが表示されます。また、プログラムの一覧で、ウイルス対策ソフトがインストールされているかどうかを確認する方法もあります。

○パターンファイルの更新

パソコンにウイルス対策ソフト等がインストールされていても、パターンファイルが古いままでは、ウイルスに感染してしまう危険があります。新しいウイルスに対応するため、常にウイルス対策ソフト等のパターンファイルを最新のものに更新してください。

○定期的なウイルススキャンの実行

ウイルス対策を万全にするため、ウイルス対策ソフト等を導入して、パターンファイルを更新するだけでなく、定期的にウイルススキャンを実行してください。

○　参考リンク

- **総務省**

「国民のためのサイバーセキュリティサイト」（外部サイト）
（https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html）

- **独立行政法人情報処理推進機構**
  「安心相談窓口だより」（外部サイト）
  （https://www.ipa.go.jp/security/anshin/mgdayori20160803.html）