

【保護司用】 情報セキュリティ対策 チェックリスト用語集 (令和8年8月14日)



フリーソフトについて

フリーソフトとは以下のようなものを指します。※ソフトウェアを省略して「ソフト」と言います。

- ・金額の支払いなしで使用できるソフト。
- ・インターネット上などから自由にダウンロードできるソフト。

フリーソフトは以下の特徴があります。

- ・フリーソフトは「無料」ですが「安全」とは限りません。
- ・ダウンロードすることでパソコンやスマートフォンがウイルスに感染するリスクがあります。

このため以下のように対応する必要があります。

- ・安易にインターネット上で「ダウンロード」をしない。
- ・やむなくダウンロードする際はMicrosoftやAdobeなどの、真に信用できる公式サイトからしかダウンロードしない。
- ・ダウンロードする際も信用できそうなサイトなのか、会社名を検索して調査を行う。
- ・もしダウンロードしたことで、「今すぐ電話が必要」、「ウイルスに感染した」、「パソコンのが勝手に動く」などの警告や挙動があった場合は、すぐに保護観察所に相談してください。

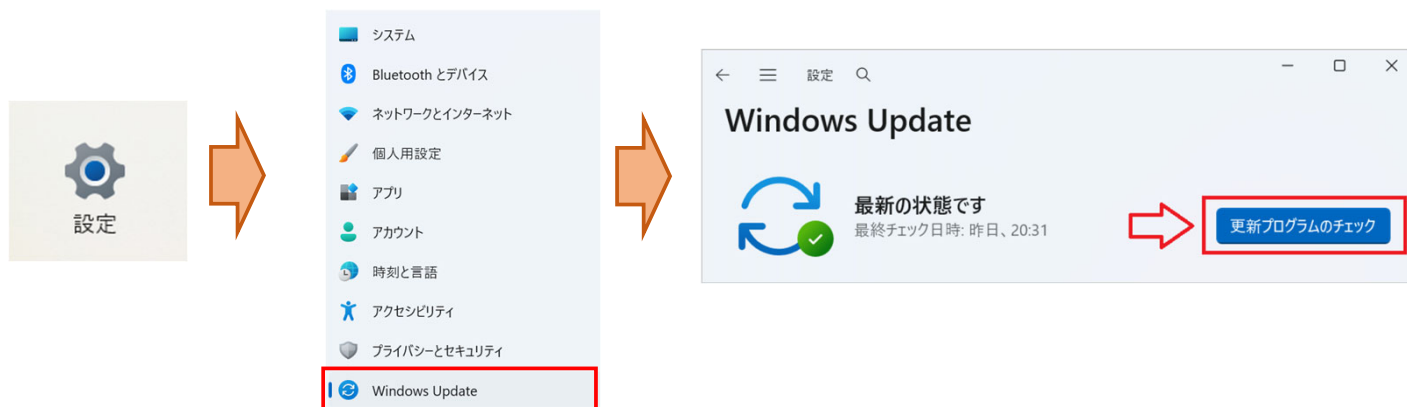
不正プログラム対策ソフトウェアについて

不正プログラム対策ソフトウェアとは以下のようなものを指します。

- ・コンピュータウイルスをブロックするためのソフトウェアです。
- ・このソフトウェアがあることでパソコンのウイルス感染を防ぐことができます。
- ・代表的なソフトウェアは「Windows Update」です。

- ・コンピュータウイルスは日々更新されています。このことから、最新のウイルスに対応するため、不正プログラム対策ソフトウェアを日々更新する必要があります。

【Windows Updateの更新例】



OSについて

OSとは以下のようなものを指します。

- ・パソコンやスマートフォンを動かす土台です。
- ・パソコンだとWindows、スマートフォンだとiPhoneのiOS、AndroidのAndroidOSが有名です。

OSは以下の特質があります。

- ・パソコンやスマートフォンを動かす土台となりますので、**最新の状態**にしておかないとコンピュータウイルスに感染しやすくなります。
- ・ウイルス感染を防ぐために各企業がサポートを行っています。Windows10など古いOSはサポートが終了していることから使用を控えていただく必要があります。自身の**OSがサポートされているか検索**して調査してください。

【パソコンのOSの表示例】



Wi-Fiについて

Wi-Fiとは以下のようなものを指します。

- ・ケーブルを使わずにインターネットに接続できる仕組みです。
- ・ルーターから電波（無線）でインターネットに接続できるようになります。

Wi-Fiは以下の特質があります。

- ・**フリーWi-Fi**（無料で公共の場でアクセスできるWi-Fi）だと、Wi-Fi経由で不正アクセスされる場合があります。
- ・フリーWi-Fiは公共の場でアクセスする前提です。公共の場でパソコンやスマートフォンを使用する場合、情報の**盗み見防止**や**端末の紛失、盗難を防止**しておく必要があります。

このため以下のように対応する必要があります。

- ・**フリーWi-Fiは極力使用しない。**
- ・どうしてもフリーWi-Fiを使用したい場合は**どのような方式を使ったWi-Fiなのか確認が必要**です。安全なWi-FiはWPA3 又はWPA2という方式を使ったWi-Fiです。
- ・公共の場でパソコンやスマートフォンを使用し、保護司活動をすることは避ける。やむを得ず行う場合でも、情報の盗み見を防止するため、覗き見防止フィルムを貼る。端末の紛失、盗難を防止するため、席を離れる場合でも端末は常に持ち歩くなどの対策を行う。

パスワードについて

情報システムへのログインに使われるパスワードは、本人しか知らない秘密情報であり、細心の注意を払って管理しなければなりません。

パスワードが漏えいすると、第三者が情報システムに不正アクセスして、深刻な被害につながる可能性があります。

- ・ **個人情報の漏えい**（自分自身の情報にとどまりません！）
- ・ **アカウントの乗っ取り**
- ・ 金融サービスの不正利用による**金銭被害** など



【パスワード設定における注意点】

- ・ 自分や家族の名前、生年月日などは使わない
- ・ 簡単な英単語だけにしない（password、など）
- ・ 単純な文字の繰り返しはだめ（abcde、12345など）
- ・ 他のパスワードを使いまわさない

【パスワードの保管における注意点】

- ・ 安全な場所に管理する
- ・ 他人に絶対に教えない
- ・ メモをパソコン画面などに貼らない
- ・ メールでパスワードをやりとりしない

USBメモリについて

USBメモリは、データの書き込み・消去ができて、小型・軽量で持ち運んで、パソコンなどの機器で利用できる便利なものです。その反面、次のような危険性があるため、対策が必要です。

- ・ **紛失や盗難**が起こりやすい
 - ・ USBメモリを介して、ウィルス感染が広がることもある
- ⇒これらは、ただちに**情報漏えいやパソコンなどのウィルス感染**につながります。



利用する場合は、必ず対策をとりましょう

- ・ よほどの必要がなければ、保護司活動では**できるだけUSBメモリを使わない**（**保護観察経過報告書などのデータを保存することは、元々禁止されています**）
- ・ USBメモリに記録するファイルには、必ずパスワードを付す（暗号化機能があるUSBメモリを使うとより安全です）
- ・ 使う前に、ウィルススキャンをする（Windows11に搭載のMicrosoft Defenderを使う、などの方法）
- ・ 持ち運びにおいては、常に自分の管理下に置くようにして、カバンに入れたまま離れる、どこかに置き忘れるといったことがないように、細心の注意をする。

【Windows11 を使ったウィルスチェック手順】



プライバシーとセキュリティ → Windowsセキュリティ → ウィルスと脅威の防止



スキャンのオプション

カスタムスキャン

「今すぐスキャン」でUSBメモリ選択