いますぐ自分でできるセキュリティ対策
～備えの第一歩～

株式会社　TAKA（タカ）

博士（工学）福永隆文

情報処理安全確保支援士（登録ｾｷｭﾘﾃｨｽﾍﾟｼｬﾘｽﾄ）

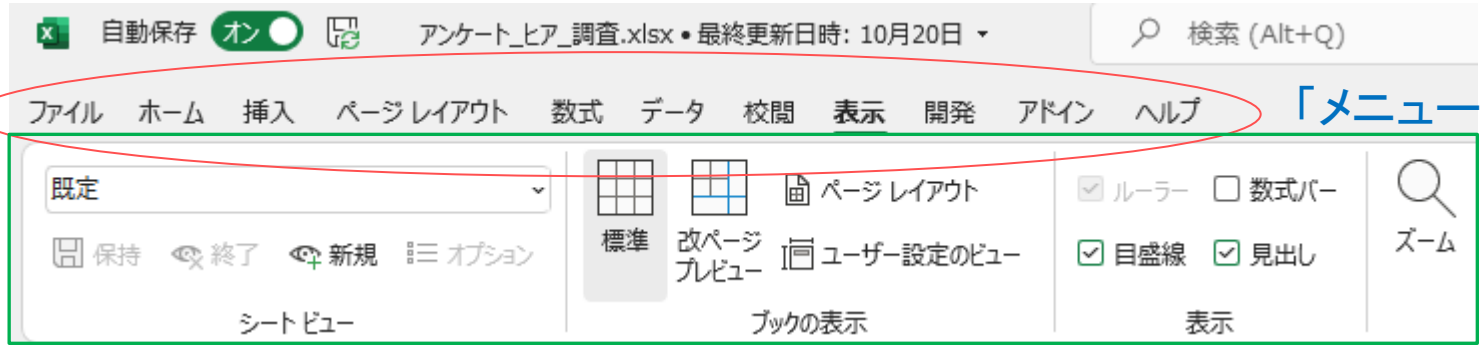
TEL 096-287-1151 携帯 090-5736-1111

fukunaga@ict-taka.jp

目次

はじめに

1. アプリの操作欄の呼び方



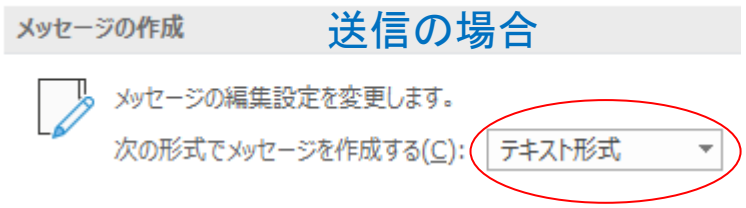
「メニュー」と呼びます

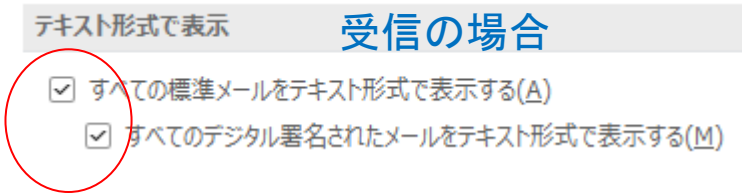
「リボン」と呼びます

2. 「スタートボタン」は画面一番下のタスクバーと呼ばれる部分の  のことです。
3. 操作説明の見方
   - 「ファイル」「オプション」「メール」「メッセージの作成」欄と書いてあれば、メニューの「ファイル」をクリックし、新たに表示された「オプション」をクリックし、新たに表示された「メール」をクリックして表示される「メッセージの作成」欄を見る、という流れになります。
4. 会社提供のパソコンに本書で紹介する設定を行う場合は事前に管理者にその旨を伝えてください。会社の事情でセキュリティ強化が行えない場合もあります。

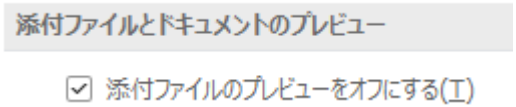
メール編（Outlook編）

1. テキスト形式でメールを送信、受信する。（HTML形式は悪用の危険があるため）
   - 送信は「ファイル」「オプション」「メール」「メッセージの作成」欄で「テキスト形式」を選択
   - 受信は「ファイル」「オプション」「トラストセンター」「トラストセンターの設定」「電子メールのセキュリティ」「テキスト形式で表示」欄の2か所にチェックを入れる

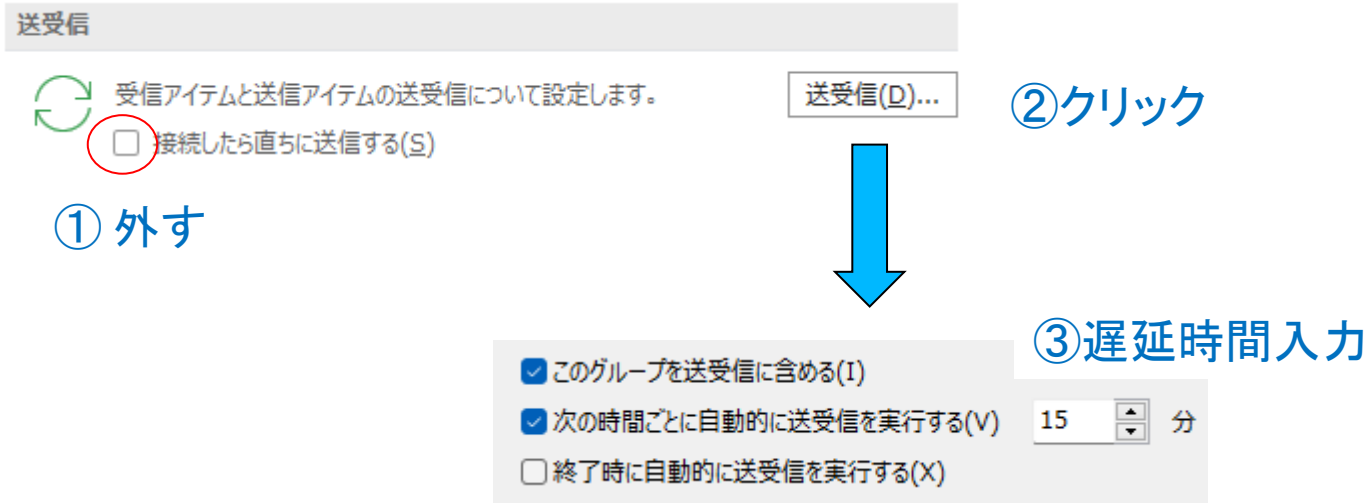




2. 添付ファイルのプレビュー機能をオフにする。（プレビューするだけで感染するウイルス事例有）
   - 「ファイル」「オプション」「トラストセンター」「トラストセンターの設定」「添付ファイルの取り扱い」「添付ファイルのプレビューをオフにする」にチェックを入れる



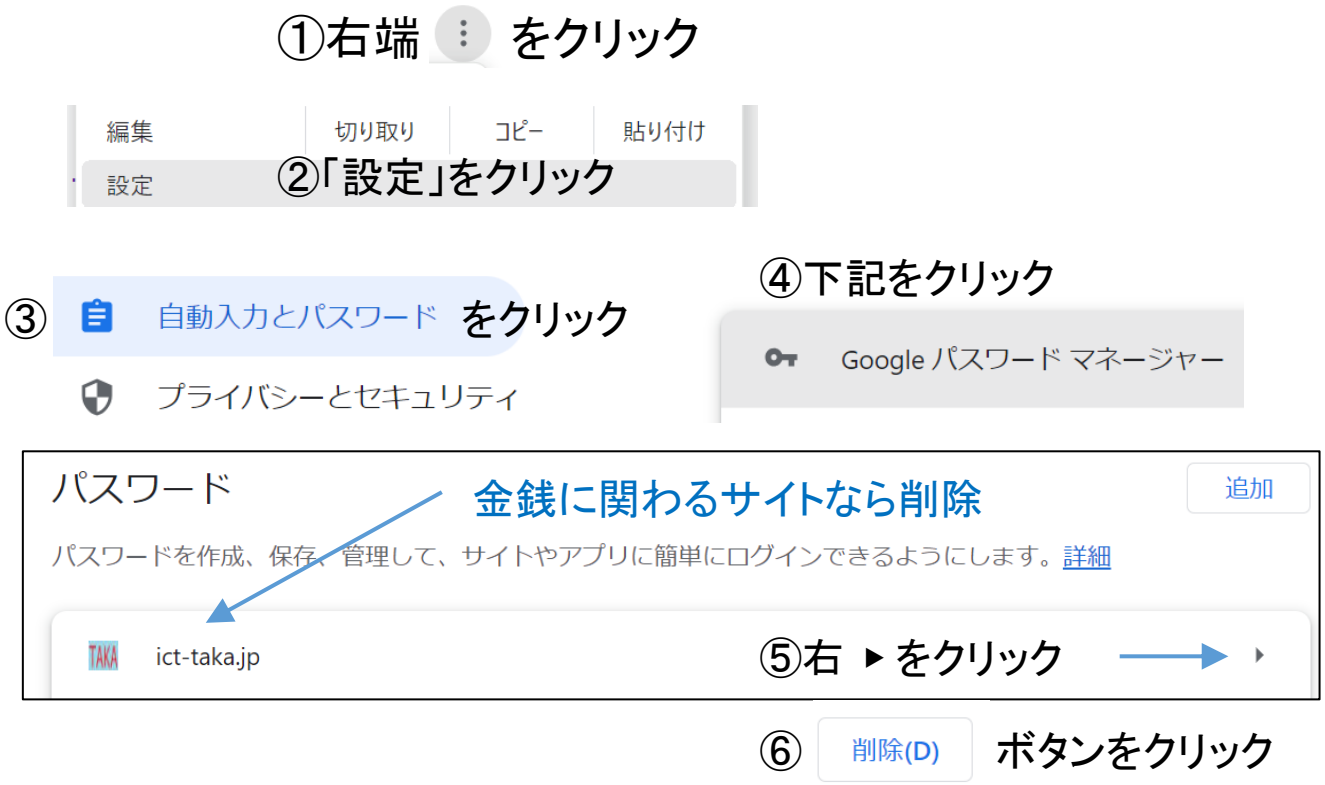
3. メール送信遅延時間を設ける。（誤送信、添付ファイルの間違いを緩和）
   - 「ファイル」「オプション」「詳細設定」「送受信」欄で「接続したら直ちに送信する」のチェックを外し、「送受信」ボタンで遅延時間を設定（15分など）します（図参照）
   - 直ちに送信したいときはリボン（上部の操作ボタン群）の「すべてのフォルダーを送受信」ボタンを押すことで直ちに送信できます



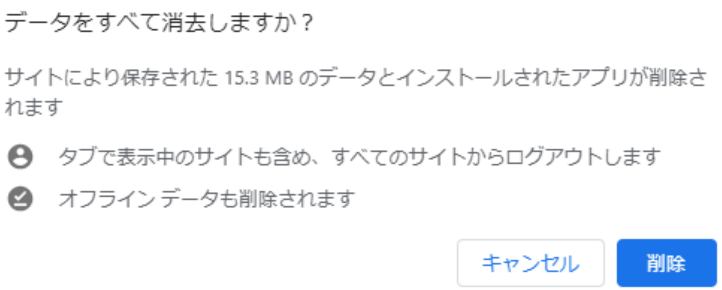
ブラウザ編

Chromeを例にご説明します

1. 金銭に関わるサイトではパスワードを記憶させない。（ブラウザに保存されたパスワードはツールで窃取されてしまうため）
   - 下記手順でパスワード保存の有無を確認し、金銭に関わるサイトは削除する



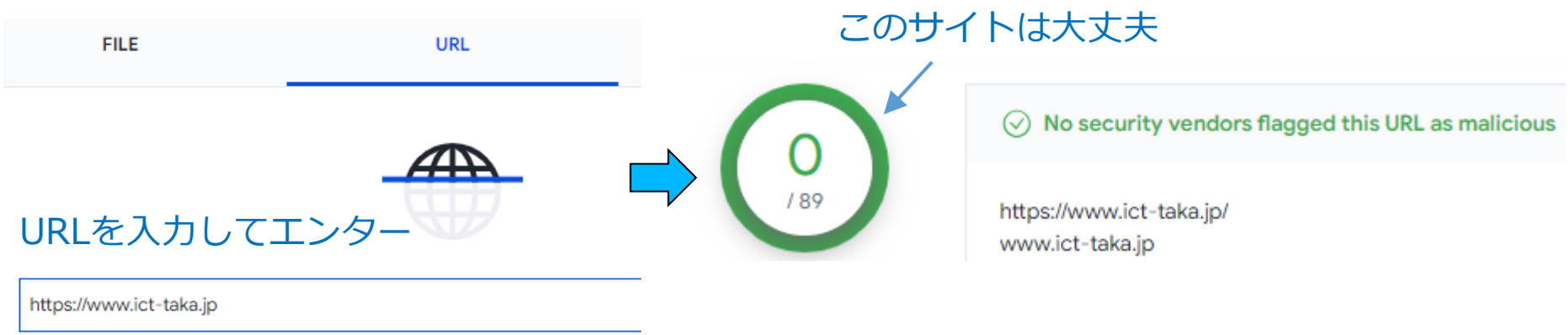
2. 定期的にすべてのCookieを削除する。定期的とは「月ごとに」など。
   - Cookieは再ログイン時にID、パスワードの入力を省略したり、ネットショップで買い物をするときなどに必要な情報を記憶しますが、便利な反面盗まれると危険です。
   - 「設定」「プライバシーとセキュリティ」「Cookieと他のサイトデータ」「すべてのサイトデータと権限を表示」「データをすべて消去」で下記画面が表示されるので「削除」ボタンを押します。
     ※Chromeバージョンによって操作が異なります



削除直後は再度ログイン情報の入力など不便が生じますが必要なことです。

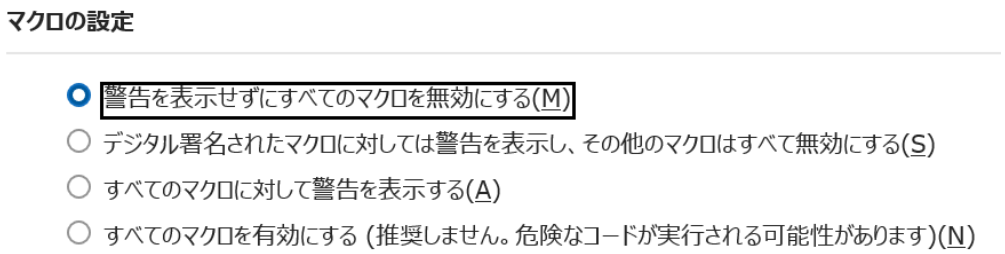
3. 検索結果ページのリンクが安全かのマークをつけてくれるソフトの活用またはURLの安全性を確認できるツールの活用
   - McAfee ウエブアドバイザーのように各リンクの右に安全マークを付けてくれると安心してクリックできます。（ブラウザのアドオンソフトなのでESETなどと共存できます）

   - 上記のソフトを導入しなくても無料でリンク（URL）をチェックしてくれるサイトがあります（下図）。アクセス先：https://www.virustotal.com/gui/home/url



マイクロソフトOffice製品　共通設定編

1. EXCEL, WORD, PowerPoint, OutlookでVBAおよびマクロを利用していなければマクロを完全に無効にする。（悪意のあるプログラム実行を防ぐため）
   - 「ファイル」「オプション」「トラストセンター」「トラストセンターの設定」「マクロの設定」で「警告を表示せずにすべてのマクロを無効にする」に節句を入れる。
   - VBAおよびマクロを利用しているかどうかは管理者にお尋ねください。



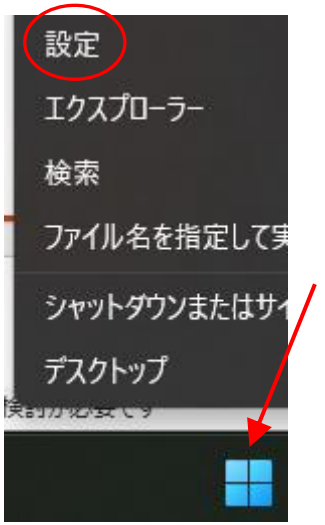
2. 各Office製品が自動更新で最新にアップデートされているかを確認します。
   - 「ファイル」「アカウント」の右欄に「更新プログラムは自動的にダウンロードされインストールされます」が表示されていれば問題なし（左図）
   - 上記が表示されていなければ（右図）、「更新オプション」ボタンをクリックし、「更新を有効にする」をクリックします。この操作は1つのOffice製品で設定すれば他の製品に波及します。

Windows設定編

Windows11を例として説明しています

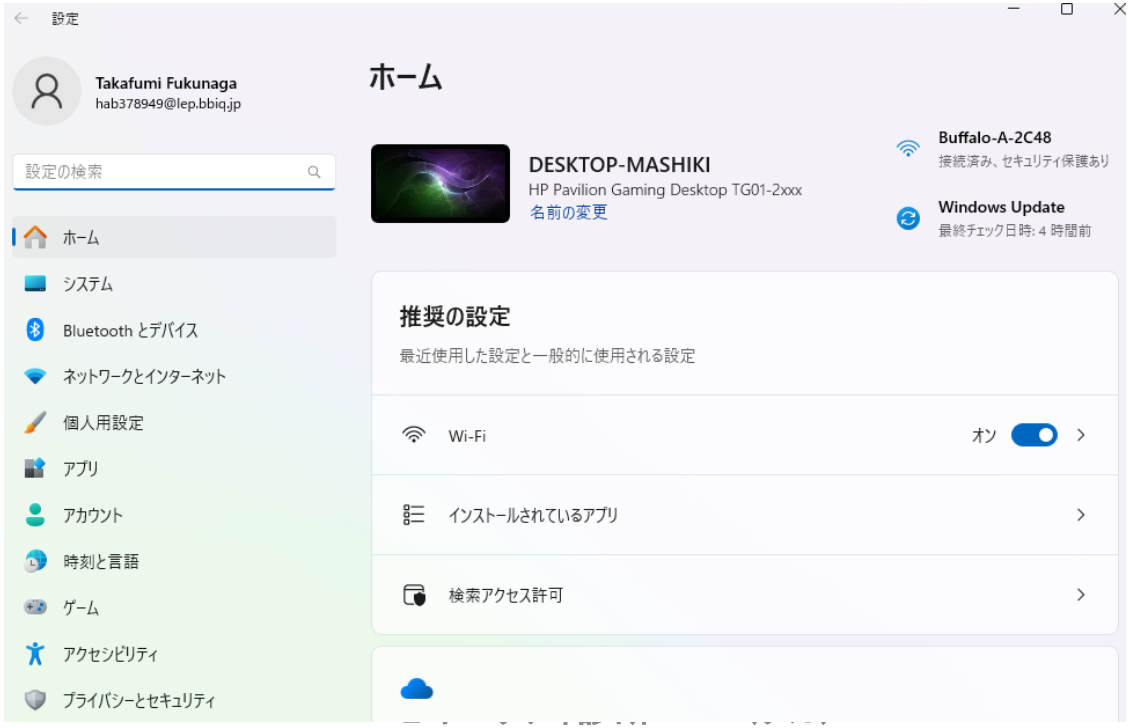
はじめに

1. 「設定」画面の表示
   - Windowsの設定画面がスタートボタンをクリックしても表示されない場合は、スタートボタン上にマウスポインタを合わせ「右クリック」で表示されます。または、検索欄に「設定」と入れても表示されます。

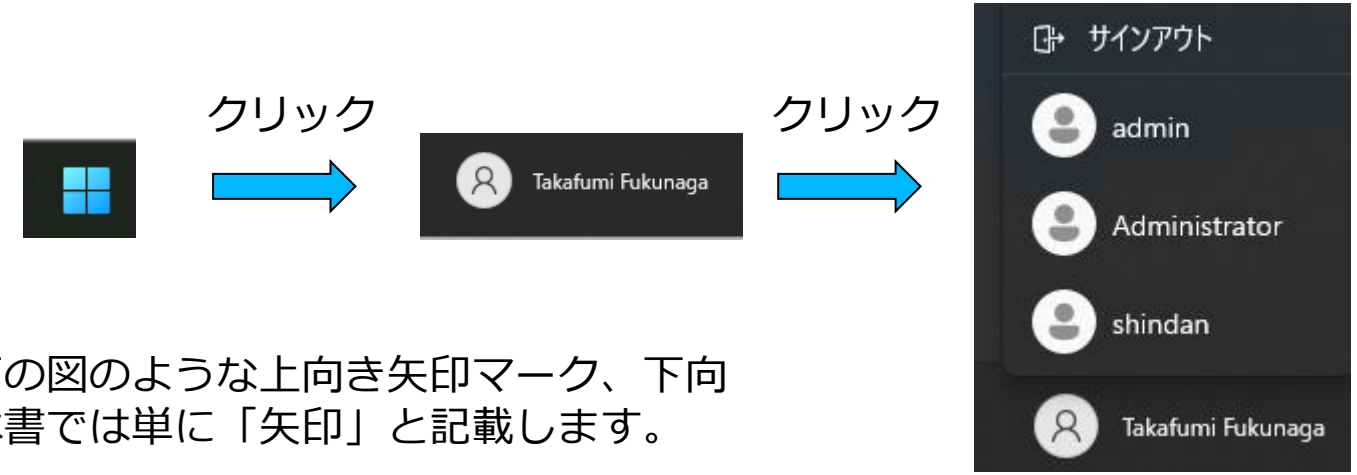


スタートボタンで右クリック

「設定」画面



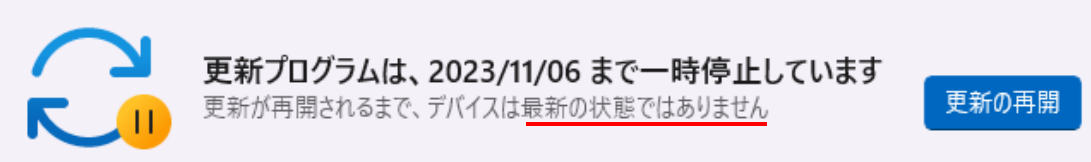
2. （ユーザの切り替え方法）現在ログインしているユーザから他のユーザに切り替える操作は以下となります。
   ① スタートボタンをクリックし、表示されるウインドウの一番下の現在のユーザ名をクリックする。
   ② 他のユーザが表示されるので切り替えたいユーザをクリックし、パスワードを入力しログインする。
   ③ 元のユーザに戻るときは再びスタートボタン、現在のユーザ、をクリックし、今度はサインアウトをクリックする。



3. （用語）下の図のような上向き矢印マーク、下向き矢印は本書では単に「矢印」と記載します。

1. Windows Updateは正常に行われているかを確認する。「設定」画面で「Windows Update」をクリックする。
   - 下記のように「最新の状態」の表示があればOK

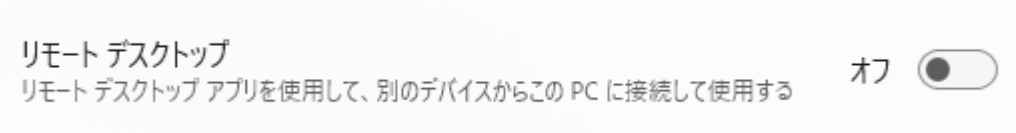
   - 下記例のように最新の状態ではない旨の表示がある場合は「更新の再開」ボタンをクリックする。



   - 下記例のように「ダウンロードとインストール」ボタンが表示されていればクリックする。再起動も必要で時間が数十分かかります。

2. パスワードは英大文字、小文字、数字、できれば記号を含めて複雑にする。（Windows以外も同様です）
   - Windows起動状態の時CTRL+ALT+DELETE（３つのキーを同時に押す）でパスワードの変更ができます。
3. ネットワークの種類を「パブリック」にする。外部、特にインターネットからの不正アクセスを防止できます。
   - 「設定」画面で「ネットワークとインターネット」をクリック下記図のように「プライベートネットワーク」となっていたら「プロパティ」をクリックし、「パブリックネットワーク」を選択する。

4. 攻撃に悪用されることが多いリモートデスクトップ機能をオフにする。
   - 「設定」画面で「システム」「リモートデスクトップ」「リモートデスクトップ」欄で機能をオフにする。



5. 不要なアカウントは削除する（退職者など）。
   - 「設定」画面で「アカウント」「他のユーザ」「他のユーザ」欄で不要なアカウントがあれば削除する。
   - 削除は不要なアカウントの右端の下矢印をクリックし「削除」ボタンをクリックする。

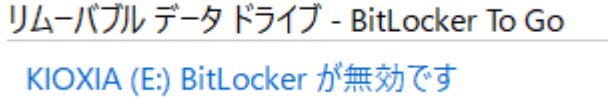
USBメモリなど持出機器の暗号化編（無くしても危険を緩和）

Windows Pro付属のBitLockerを活用してUSBメモリ内データを
暗号化できます（Windows Homeにはこの機能はありません）

USBメモリを例に説明しますが、外付けHDDでも同じです

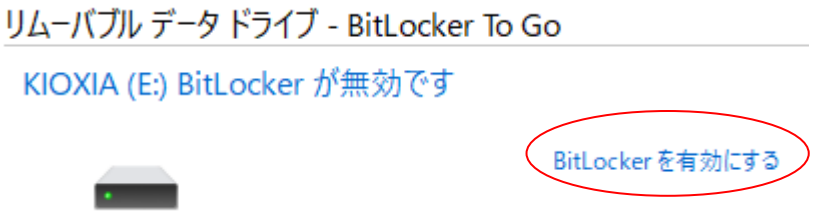
1. USBメモリを挿入します。
2. 画面下の検索欄に「bitlocker」と入力し、右上に表示される「BitLockerの管理」を起動します。

3. 右下に

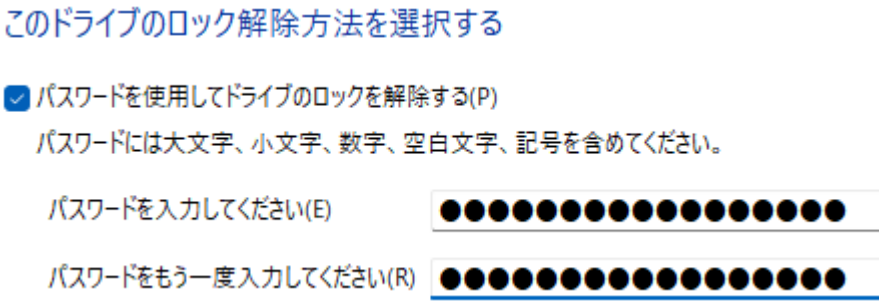


と表示されます。

右の矢印をクリックすると「BitLockerを有効にする」が出てきますのでクリックします。

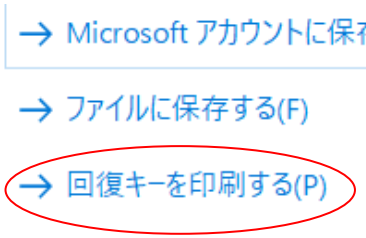


4. 「パスワードを使用してドライブのロックを解除する」をチェックし、パスワードを入力します。



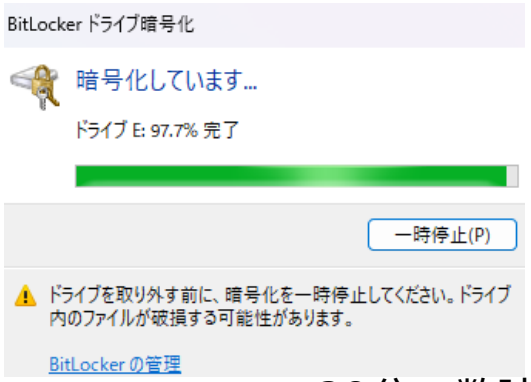
（パスワードのルール）
英大文字、小文字、数字、記号を混在

5. パスワードを忘れたときのために回復キーの保存方法が表示されます。「回復キーを印刷する」をクリックします（状況に応じ他でもOK）。



6. 「次へ」ボタンをクリック。「使用する領域のみ暗号化する」が選択されているのでそのまま「次へ」、「互換モード」が選択されているのでそのまま「次に」クリック。「暗号化の開始」ボタンをクリック。「暗号化しています」が表示されます。容量に応じた時間がかかります（下図）。これでパスワードを知らない人はUSBメモリにアクセスできません。ロックがかかった状態となります。

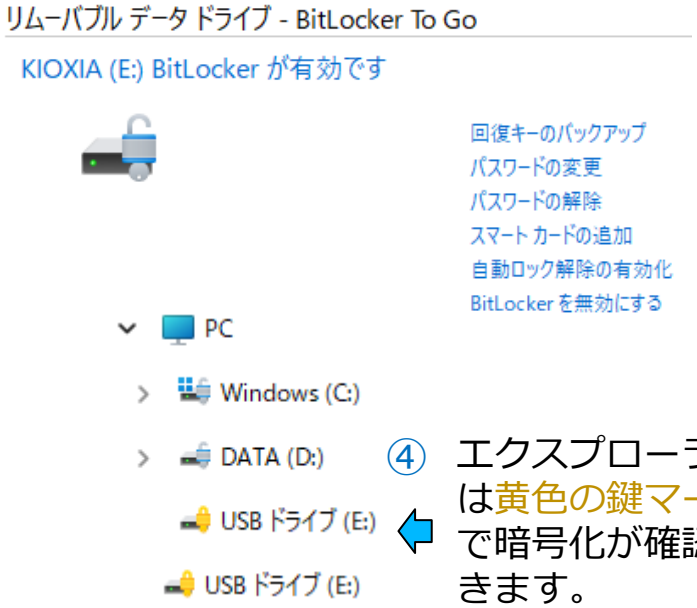
①



20分～数時間かかります

②

③ 暗号化されると表示が変わります



④ エクスプローラでは黄色の鍵マークで暗号化が確認できます。

7. 暗号化されたUSBメモリをパソコンに挿入すると右下に「ロックを解除する」の通知が表示されます（図1）。クリックすると暗号化の時に指定したパスワードの入力が求められます（図2）。通知が消えている場合はエクスプローラーでUSBメモリをクリックするとパスワード入力画面が現れます。パスワードを入力して「ロック解除」ボタンをクリックすると暗号化によるロックが解除されデータの参照ができるようになります。エクスプローラで確認するとロックが解除されたUSBメモリは灰色の鍵マークが付いています（図3）。

図1

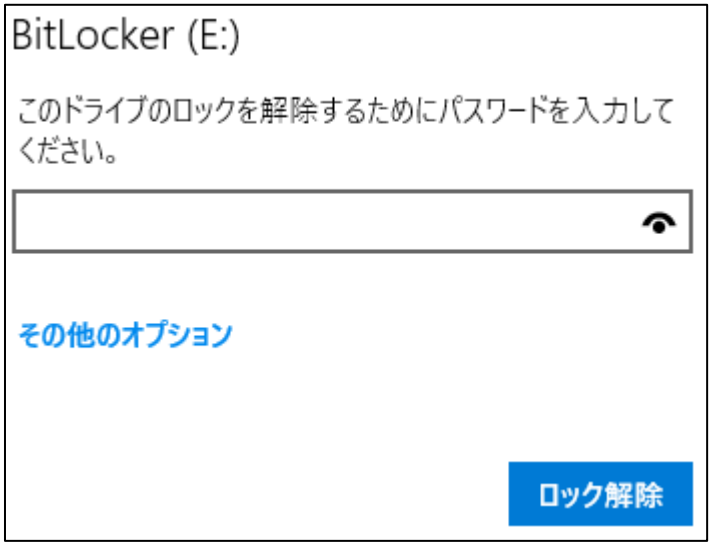


図2

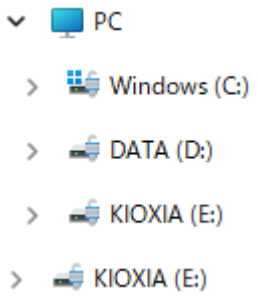


図3

ウイルス対策ソフトの活用強化編

ESET Internet Securityを例にご説明します

Windowsにもセキュリティ対策ソフトDefenderが含まれていますが、二重防御が叫ばれる現在、PCの対策ソフトに関しても同様に二重防御が必要です。メーカーが異なる対策ソフトを導入することで防御力はさらに向上します。一方のソフトを通過したウイルスがもう一方のソフトで駆除されることはよくあります。
価格も安くなってきています（例：ESET Internet Security 5台分 3年 1万円以下など）。

1．定期的に自動ウイルス検査を実行する。

- 現在は新種ウイルスの拡散が速いのでリアルタイムで駆除できない場合がありますが、後日の自動ウイルス検査で駆除できる場合があります。
- ESETアイコンは画面一番下のタスクバーと呼ばれる部分の右端の矢印をクリックすると出てきますのでクリックし起動します（図１）。「ツール」「スケジューラ」「タスクの追加」でタスク名に「定期フルスキャン」、タスクの種類を「オンデマンドコンピュータの検査」にします（図２）。「次へ」ボタンで「実行するスケジュールタスク」を「毎週」にします（図３）。「次へ」で実行する時間と曜日を入れます（図４）。「次へ」を押し、次画面はそのままでいいので、さらに「次へ」をクリックします。検査場所としてPCの左ボックスをチェックします（図５）。「OK」ボタン、「終了」ボタンで完成です。右上「×」で終了してください。

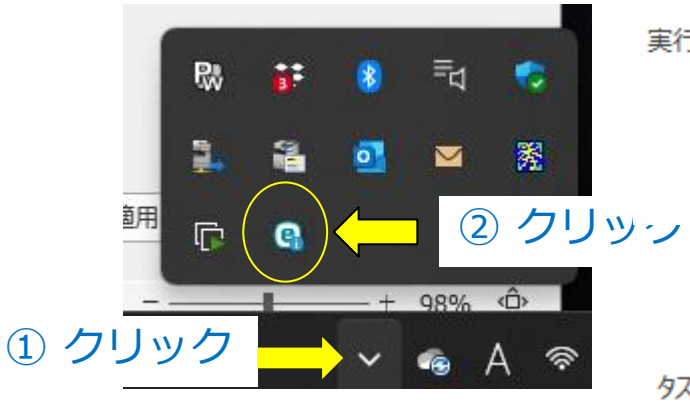


図１ ESET起動

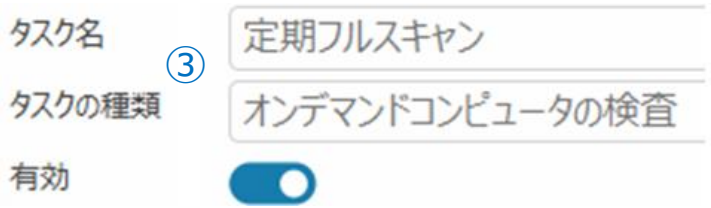


図２

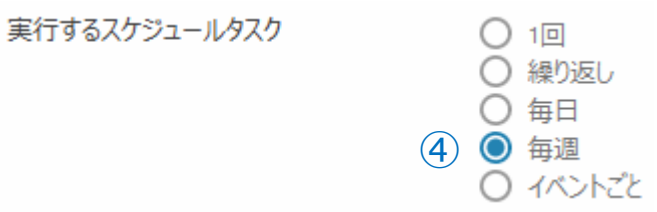


図３

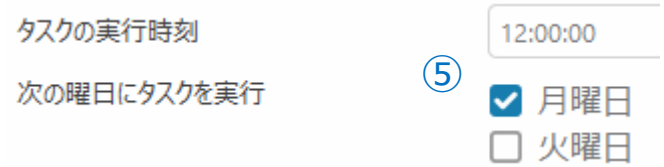


図４

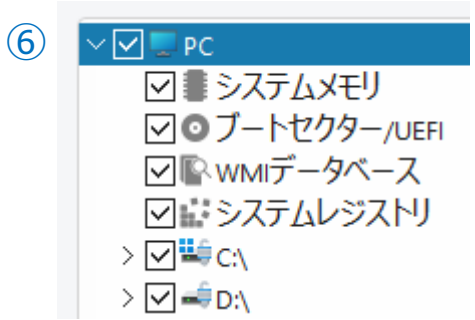


図５

※土、日曜の分のメールなどが届くので月曜日を推奨

2. USBメモリ、外付けハードディスクを挿入した時点で自動ウイルス検査する。
   - ESETの起動は前述①②同様です。「設定」（右下の）「詳細設定」「マルウェア検査」で「リムーバブルメディア」の左にある[+]をクリックします。「リムーバブルメディアの挿入時に行うアクション」が表示されますので右のプルダウンメニューから「自動デバイスの検査」を選択します（図１）。「OK」ボタンで完了です。
   - USBメモリなどを接続すると自動でウイルススキャンが実施され右下に検査結果が通知されます（図２）。

図１

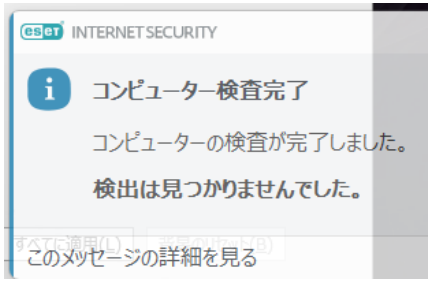


図２

ちょっと進んで
日常使うユーザから「管理者権限」を削除する

ここだけは管理者にお願いしてください

「自分でできる」からは外れますが、マイクロソフトが毎年繰り返し「攻撃の７５%がこれにより回避可能」と警告しておりますのでご紹介します。管理者権限をもつユーザでログイン中にウイルスに感染するとウイルスも管理者権限で動きます。つまり、何でもできます。

Microsoft Report 2023 の一部

事情でアップデートができない環境でも効果がある

管理者権限の削除

Enforce least privilege, such as by removing local admin rights: This proactive approach can provide highly effective protection, even in the absence of patching. Removing local admin rights, and controlling execution, has historically mitigated 75% of Microsoft's critical vulnerabilities, as we have demonstrated in

最も効果的な防御策

重大な攻撃できる欠陥を75%軽減できる

まず、日常ログインに使っているユーザが「管理者権限」を持っているかを確認します。持っていなければ問題ありません。これ以降の処理は不要です。

「設定」画面で「アカウント」「ユーザーの情報」をクリックし、上部に表示されるログインユーザー名に「管理者」の表示があれば「管理者権限」を持ち、なければ「管理者権限」を持ちません。

ユーザーTAKAFUMI FUKUNAGAは「管理者権限」を持つ

ユーザーSHINDANは「管理者権限」を持たない

日常ログインするユーザが管理者権限を持つ場合、管理者権限を外す

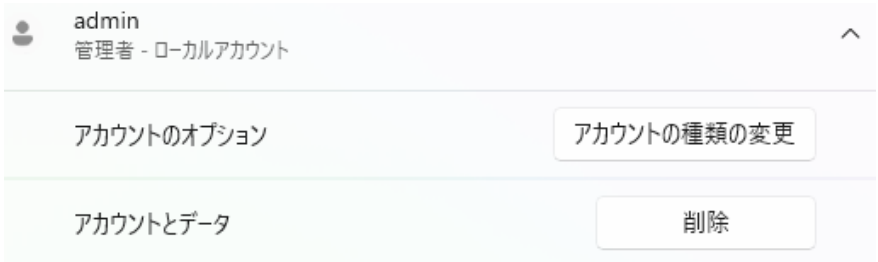
1. 日常使うユーザとは別に「管理者権限」をもつユーザを作成します。
（すでに存在していたら必要ありません。）

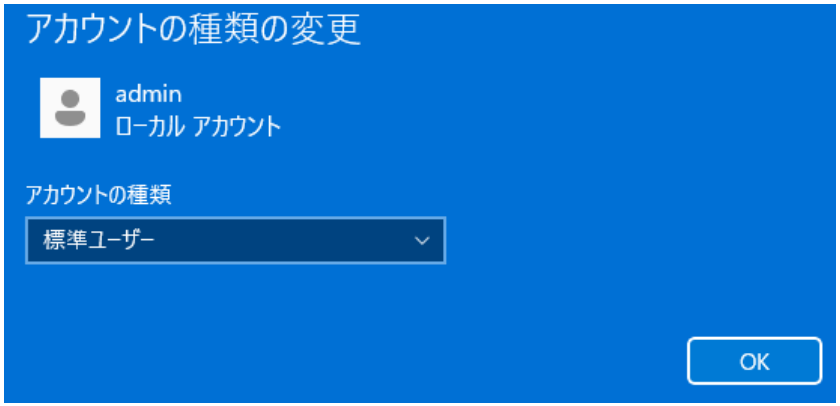
① 「設定」画面で「アカウント」「他のユーザ」「その他のユーザを追加する」欄の「アカウントの追加」ボタンをクリックし指示に従いユーザを追加する。この時点では追加したユーザは「管理者権限」を持たない。

② 「他のユーザ」欄に追加したユーザが表示されるので右の矢印をクリックしてアカウントのオプションを表示する。下図はkanri2023を追加した例。

③ 「アカウントの種類の変更」をクリックし、「管理者」を選択し「OK」ボタンをクリックする。これで追加したユーザは「管理者権限」を持つ。

2. 日常ログインするユーザから「管理者権限」を外す。
   ① 「管理者権限」を持つユーザでログインしなおす(Windows編「はじめに」参照)
   ② 「設定」画面で「アカウント」「他のユーザ」で通常使うユーザ欄の右にある矢印をクリックし、表示された「アカウントの種類の変更」ボタンをクリックする。
   ③ アカウントの種類を「標準ユーザー」に変更し「OK」ボタンをクリックする。これで「管理者権限」を持たない標準ユーザ―となる。
   ④ サインアウト（ログアウト）し、通常使うユーザでログインしなおす。





お疲れさまでした

ご意見いただければ幸いです。