

PCフォーラム

JA水郷つくばパソコン研究会会報

2024年4月号
https://dappe.com
mail:dappepc@gmail.com



担当部署：JA水郷つくば営農部
営農企画課
土浦市田中1-1-4
電話 029-823-7001



皆さんこんにちは。3月になっても雨が多く寒い日もあり思ったよりは暖かくなってきませんね。令和5年度ももうすぐ終わり新年度をむかえようとしています。

研究会のモットーであるお互いに教えあうことを実践し来年度も前進していきましょう。

さて、3月の定例会予定は以下の通りです。また前号でお知らせした総会にもぜひご出席をよろしくお願いいたします。

3月12日 監査、PCフォーラム発行など
19日 総会資料作成、スマホの知識など

26日 総会

午後7時30分より
パソコン教室前 食堂

※委任状ははがきを同封しましたので
総会前日までに到着するようにお願い
いたします。

特集1 PCのセルフチェックと最適化

Windows 10/11を長時間稼働していると、動作が不安定になることがあります。これは、アプリケーションなどが使用したメモリが終了時に完全に解放されずに、メモリの空き容量が少なくなってしまうのが原因になっていることが多いためです。

このようなメモリ内の不要になった領域などを解放すれば、Windows 10/11のメモリ空き容量が増え、結果、システムを安定させることができます。こうしたシステム最適化ツールとしては、Gen Digital(「ノートン 360」「Avast」などを販売するセキュリティソフトウェア企業)の

「CCleaner」が有名です。機能は制限されるが無料版も提供されているので、既に利用している人もいるかもしれませんがマルウェアが騒がれた時があったので敬遠される方もおるでしょう。

実は、同様のシステム最適化ツールがMicrosoftから「PC Manager」という名称で提供されています。「PC Manager」ページから直接ダウンロード可能です。
<https://pcmanager.microsoft.com/ja-jp>

PC Managerをインストールする

PC Managerは、Microsoft Storeで配布もされています。Microsoft Storeを起動し、検索ボックスに「PC Manager」と入力して検索すれば、「Microsoft PC Manager」が見つかります。「Microsoft PC Manager」のページを開き、提供元が「Microsoft Corporation」であることを確認してから、[インストール]ボタンをクリックすればインストールできます。(小)。





特集2 セキュリティについて

2 段階認証の必要性

今はたった1回のデータ侵害で、オンライン生活全体が大混乱に陥ってしまう時代です。問題はパスワードにあります。この保護手段は、貴重なリソースを守るには絶望的なまでもろいのです。

長く、複雑で、推測しにくいパスワードを作成すれば、何とかオンラインでの安全性を高められると信じ込み、誤った安全感を持たないようにしましょう。あまりに長く複雑で、例えば入力に5分かかるパスワードを作成しても、そのパスワードを使用するサービスで適切に保管されておらず、サーバーが侵害された場合には保護には何の役にも立ちません。そうした事態が頻繁に起きているのです。

強力なパスワードをランダムに生成して使い回しをしないという合理的なポリシーを定めていても、セキュリティという鎖で最も脆弱な部分は、やはり人間なのです。聡明な人であってもソーシャルエンジニアリングでだまされて認証情報をフィッシングサイトに入力することや、電話で教えてしまうことがあります。その解決策として最近採用が増えているのが**2要素認証**、すなわち**2FA**(多要素認証や**2段階認証**と呼ばれています)というものです。

サービスで2FAを有効にするとセキュリティ要件が変わり、少なくとも2種類の身元証明を提示して、保護されたサービスにアクセスしなければなりません。この2種類の認証形式は、以下の要素の少なくとも2つを任意に組み合わせたものとなっています。

*「自分が知っていること」。パスワードやPINなど。
*「自分の特徴」。指紋やその他の生体認証ID、FACEIDなど。

*「自分が所有しているもの」。確認コードの生成や受信が可能な信頼できるスマートフォン、ハードウェアベースのセキュリティデバイスなど。何者かがパスワードを盗

んで、未知のデバイスからサインインしようとする、2つ目のID証明の提供を(通常は数字コードの形式で)求められることとなります。そのサインイン要求を出したのがアカウントの認証情報を盗んだ者だった場合、そこから先に進むことはできません。その数字コードがなければ、サインインを続行できないからです。

現在導入されている2要素認証システムでは、多くの場合、最初の要素(パスワード)と最後の要素(スマートフォン)が使用されます。スマートフォンは広く普及しているため、最適なセキュリティデバイスとなっているからです。スマートフォンでは、サインイン時にパスワードと併せて使用する固有のコードを提供することで認証を支援することができます。

そのコードを取得する方法は2つあり、サービスからテキストメッセージとして送信させるか、スマートフォンにインストールされたアプリで生成する(一部のサービスでは、スマートフォン上でプッシュ通知を承認することもできる)というものです。

Microsoftのレポートでは、2FAがうまく機能し自動化された攻撃の99.9%をブロックしていると結論づけています。サービスプロバイダーが多要素認証をサポートしている場合は、それがSMSベースのワンタイムパスワードのような単純なものであっても使用した方がいいとMicrosoftは推奨しています。Googleによる別のレポートでも同様の結論が出ています。

これからは**2DA(2段階認証)**は**必ず設定することがおすす**めです。

(みやざき)



QRコードは4月からの年間予定です
ご確認ください。

今月のタイトルフォト Viola cornuta(Horned Pansy)