— AUS（アルテミス・ユーザ・サポート）便り 2022/11/29号 —
https://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●Windows 8.1のサポート終了まで2ヶ月切る…MSが注意喚起

https://forest.watch.impress.co.jp/docs/news/1455403.html
https://learn.microsoft.com/en-us/windows/release-health/windows-message-center#2949
https://support.microsoft.com/ja-jp/windows/3cfd4cde-f611-496a-8057-923fba401e93
https://support.microsoft.com/ja-jp/office/34e28be4-1e4f-4928-b210-3f45d8215595

このニュースをザックリ言うと･･･

- 11月10日(現地時間)、マイクロソフト(以下MS)より、Windows 8.1のサポート終了となる2023年1月10日まで2ヶ月となったことによる注意喚起が出されています。

- 8.1では、7で提供されている有償サポートの提供予定はなく、サポート終了後も8.1を使い続けることにより、企業・組織がセキュリティリスクにさらされたり、コンプライアンス義務を満たす能力に影響を与えたりする可能性が高いとしています。

- またMicrosoft 365(Officeのサブスクリプション版)についても、8.1向けのセキュリティパッチ提供が同時に終了予定となっています。

- MSでは、8.1以前が動作するデバイスについて、デバイスでサポートされる最新のOSに更新すること、またそのデバイスが最新バージョンであるWindows 11に対応していない場合は、11に対応するより新しいデバイスに置き換えることを推奨しています。

AUS便りからの所感等

- 買い切り版のOfficeについては、Office 2013が2023年4月、2016が2025年10月にサポート終了予定となっています(2019・2021は8.1に対応していません)が、OS自体のサポート終了にともない、引き続き使用することはやはり危険とされています。

- またMicrosoft Storeにおいても、サポート終了後は新たなアプリの購入・インストールができなくなるとのことです。

- 万が一8.1が動作するPCが社内に残っており、10以降にアップグレードできない場合は、最低でもその他アップデートできるソフトウェアを全て最新のものにし、UTM等を利用して他のPCから隔離されたネットワークに配置するべきでしょう。

- Windows 10についても2025年10月にサポート終了となるため、それまでに10未対応のデバイスを置き換える計画を確実に立てるようにしてください。

Impress Watch

「Windows 8.1」のサポート終了まで2カ月を切る ～ Microsoftが注意喚起

OSだけでなく、「Microsoft 365」アプリのパッチも終了

樽井 秀人　2022年11月14日 09:00

Message	Date
Reminder: Windows 8.1 support ends on January 10, 2023 As a reminder, Windows 8.1 will reach the end of support on January 10, 2023, at which point technical assistance and software updates will no longer be provided. If you have devices running Windows 8.1, we recommend upgrading them to a more current, in-service, and supported Windows release. If a device does not meet the technical requirements to run a more current release of Windows, we recommend that you replace the device with one that supports Windows 11. Microsoft will not be offering an Extended Security Update (ESU) program for Windows 8.1. Continuing to use Windows 8.1 after January 10, 2023, might increase an organization's exposure to security risks or impact its ability to meet compliance obligations.	2022-11-10 14:30 PT

「Windows 8.1」のサポート終了を

2013年11月13日（米国時間、以下同）にリリースされた「Windows 8.1」は、2023年1月10日に延長サポートの終了を迎える。米Microsoftは11月10日、公式ドキュメントサイトに告知ページを設置して注意を喚起している。

Windows 8.1には5年間のメインストリームサポートと、5年間の延長サポートの計10年間のサポート期間が設定されている。現在は基本的にセキュリティパッチのみの提供が行われている延長サポートフェイズにあるが、2023年1月10日以降はそれも満了し、セキュリティパッチが提供されなくなる。Windows 7などで有償提供されていた「拡張セキュリティ更新プログラム」（ESU）も用意されていない。

●ワコムECサイトが不正アクセス…個人情報147,545件、クレカ情報1,938件流出か

https://news.mynavi.jp/article/20221122-2519741/
https://www.wacom.com/ja-jp/about-wacom/news-and-events/2022/1484

このニュースをザックリ言うと･･･

- 11月21日(日本時間)、ワコム社より、同社運営の「ワコムストア」が不正アクセスを受け、個人情報およびクレジットカード情報が流出した可能性があると発表されました。

- 発表によれば、2022年2月19日～4月19日に同サイトで決済に使用されたクレジットカード情報最大1,938件(名義・番号・有効期限・セキュリティコード・メールアドレス)について、ペイメントアプリケーションの改ざんにより不正に外部に送信された可能性があるとしています。

- また、過去に同サイトを利用したユーザー最大147,545名の個人情報(氏名・住所・電話番号・メールアドレス等)についても、2021年2月22日～2022年4月19日にかけての不正アクセスにより流出していた可能性があることが判明しています。

AUS便りからの所感

- 同サイトではクレジットカード情報を保持しない仕様でしたが、改ざんにより、決済時に入力された(セキュリティコードを含む)カード情報が外部に送信される状態となっており、近年のECサイトからのクレジットカード情報漏洩における主要な手口がとられた形です。

- 独自にECサイトを立ち上げる際は、Webアプリケーションやサーバーの脆弱性について確実に修正・対策を行い、利用しているフレームワーク等についても随時最新のバージョンに保つこと、加えて攻撃の形跡・兆候を検知・遮断するためのIDS・IPSおよびWAFの設置により、攻撃者による侵入や改ざんの余地をなくすよう努めることが重要です。

- 入力フォーム支援サービスを提供する外部企業が不正アクセスを受けたことにより、サービスを採用する複数のECサイトが被害を受けたケースもあり(AUS便り2022/11/01号参照)、指定された送信先以外に情報が送信されるのを防ぐ仕組みとして、既に主要なブラウザーに実装されているContent Security Policy(CSP)の活用が進むか、あるいは更なる新たな仕組みが実装されるのか等も注目されるところです。


ワコム、直営サイトへの不正アクセスで最大14万7,545名の個人情報が漏洩か

掲載日 2022/11/22 11:39

ワコムは11月21日、直営通販サイト「ワコムストア」において、第三者による不正アクセスを受けたことを発表した。最大1,938件のクレジットカード情報、14万7,545名の個人情報が漏洩したおそれがある。

今回の不正アクセスにより、2022年2月19日～2022年4月19日午前中の期間に「ワコムストア」で製品等を購入したユーザーのクレジットカード情報が漏洩し、その件数は最大1,938件となるとしている。

漏洩した可能性のある情報は、クレジットカード名義人名、クレジットカード番号、クレジットカード有効期限、セキュリティコード、Eメールアドレス。一部のユーザーのクレジットカード情報が不正利用されたおそれがあると判明している。

● SMTP認証からの不正アクセス、スパムメール送信の踏み台に

https://scan.netsecurity.ne.jp/article/2022/11/28/48552.html

このニュースをザックリ言うと･･･

- 11月25日(日本時間)、創価大学より、同大学のメールサーバーが不正アクセスを受け、スパムメール送信の踏み台にされたことが発表されました。

- 発表によれば、10月31日夕方～11月1日未明に同大学教員のメールアカウント1件に対しSMTP認証の不正ログインがあり、スパムメール795件の送信が試行、うち11件が相手に受信されたとのことです。

- 11月1日に当該教員から「大量の迷惑メールを受信している」と相談があり調査したところ、セキュリティシステムによるエラーメールだったことから発覚したとしています。

AUS便りからの所感

- メール送信(SMTP)・受信(POP3・IMAP4)時の従来の認証においては「ID・パスワードのみでログイン試行が可能」という問題があることから、OAuth 2.0等による多要素認証の採用が進んでおり、GoogleやMicrosoftが提供するようなメールサービスでも、特にメーラーによる接続時には多要素認証を必須とするようになっています。

- 組織で独自にメールサーバーを立てているケースで、多要素認証の導入が容易ではない場合は、メールサーバーの設定等で不審なログイン試行を検知・遮断する仕組みを有効にするよう検討すべきでしょう。

- また今回の事案では795件中784件のメールが外部へ送信されず遮断されており、受信のみならず外部への送信においても不審な内容のメールを遮断するよう、メールサーバー自体もしくはその前面にUTMの設置等ソリューションの導入を推奨致します。


インシデント・事故／インシデント・情報漏えい

2022.11.28 Mon 8:05

創価大学の教員のメールアカウントが迷惑メール送信の踏み台に、SMTP認証を悪用した攻撃と推測

創価大学は11月25日、不正アクセスによる迷惑メールの送信について発表した。

シェア　ツイート　送る

創価大学は11月25日、不正アクセスによる迷惑メールの送信について発表した。

これは10月31日午後4時1分に、同学教員1名のメールアカウント1件に不正アクセスがあり、同アカウントが踏み台となり不特定多数の迷惑メールを送信したというもの。当該教員から11月1日に、大量の迷惑メールを受信しているとの一報があり調査をしたところ、同教員のメールアカウントが不正ログインされ大量の迷惑メールを発信したことが判明した。

トップページ

全 3 枚

拡大写真