— AUS（アルテミス・ユーザ・サポート）便り 2025/10/16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。

●Microsoft月例のセキュリティアップデート…Windows10他サポート終了

https://forest.watch.impress.co.jp/docs/news/2054928.html
https://msrc.microsoft.com/blog/2025/10/202510-security-update/
https://www.microsoft.com/ja-jp/windows/end-of-support

このニュースをザックリ言うと･･･

- 10月15日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。

Windowsの最新バージョンはWindows 10 22H2 KB5066791(ビルド 19045.6456)、11 23H2 KB5066793(ビルド 22631.6060)および11 24H2・25H2 KB5066835(ビルド 26100.6899・26200.6899)等となります。

- 修正された脆弱点のうち、Windows・Office・Microsoft 365 Copilot・Windows Server Update Service(WSUS)等計17件について、危険度が4段階中最高の「Critical」と評価されています。

- かねてからの告知の通り、Windows 10については無償サポートが終了となり、Windows 10で引き続きセキュリティアップデートを取得するには基本的に有償となる拡張セキュリティ更新プログラム(ESU)の入手が必要となります(Office 2016・2019等については完全にサポート終了となります)。

AUS便りからの所感等

- ESUは企業向けについては最長3年(2028年10月まで)提供、個人向けについては1年(2026年10月まで、条件付きで無料入手も)提供とされていますが、個人向けについて2年目以降の提供があるとは明言されておらず、安易に提供に期待しないこと、企業向けも2年目・3年目で値段が上昇し決して見過ごせないコストとなり得ることを鑑み、今回やむを得ず導入したとしても、もう1年において確実にWindows 11へ移行する計画を立てることが強く求められます。

- また買い切り版のOffice 2016・2019についてはESUのようなものは提供されず、Office 2021についても2026年10月がサポート期限(Office 2024は2029年10月まで)となっているため、例えばプレインストールされていたOfficeをサポート切れ以降も気付かずに使い続けることがないよう注意し、最新バージョンへのアップグレードも行われるサブスクリプション版Microsoft 365の導入検討もセキュリティの観点で有用でしょう。

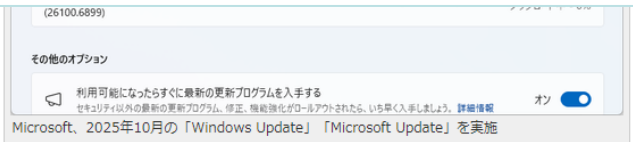
- 今回修正された脆弱点においても、既に悪用が確認されているもの3点、攻撃手法が公知となっているもの3点(うち1点は危険度Critical)が含まれ、脆弱点への根本的対策としての早急なアップデートの適用はもちろん、さらには次回11月12日のセキュリティアップデートリリースあるいはその前後で、脆弱性が修正されないWindows 10等を狙った攻撃が展開されることは確実であり、アンチウイルス・UTMによる防御についても怠りなく実施することが肝要です。

Impress Watch

ゼロデイ多数、比較的大規模 ～Microsoft、2025年10月の「Windows Update」を実施

「Windows 10」「Office 2016」「Office 2019」などサポート終了製品多し、注意

樽井 秀人　2025年10月15日 07:05



Microsoft、2025年10月の「Windows Update」「Microsoft Update」を実施

米Microsoftは10月14日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで177件（サードパーティーのものを含めると195件）の脆弱性が新たに対処されている。

●多要素認証を突破するリアルタイムフィッシング、楽天証券が注意喚起

https://www.itmedia.co.jp/news/articles/2510/14/news108.html
https://www.rakuten-sec.co.jp/web/info/info20251010-01.html

このニュースをザックリ言うと・・・

- 10月10日、楽天証券より、同証券をターゲットとするいわゆる「リアルタイムフィッシング」詐欺が確認されたとして注意喚起が出されています。

- 注意喚起で挙げられている手口の一例では、ID・パスワードの入力後、絵文字によるログイン追加認証についても偽画面を表示しており、これもリアルタイムフィッシングによって突破される恐れがあるとしています。

- 上記の例ではさらにユーザーの取引暗証番号や個人情報も詐取していますが、同証券の正規サイトにおいては、ログイン直後にこれらの入力を求めることはないとしています。

AUS便りからの所感

- リアルタイムフィッシングの事例は、既に他のネット証券等を狙い、ワンタイムパスワード(OTP)等が奪取される事例が報告されており(AUS便り 2025/08/04号参照)、楽天証券のログイン追加認証もリアルタイムフィッシングによる情報の奪取に対してはワンタイムパスワード等と同様に弱いとする指摘が散見されていました。

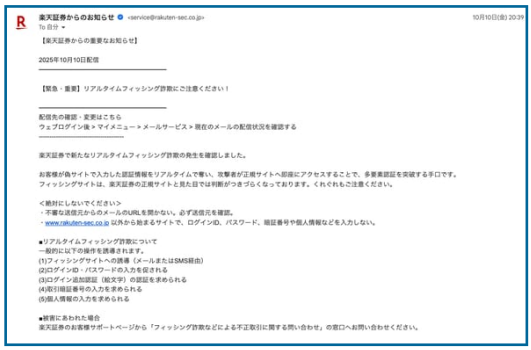
- 楽天証券では10月26日にパスキー認証の導入を予定、また他のネット証券各社でも今年に入って複数の多要素認証が導入されるケースもある等しており、利用しているサービスでの認証における流動的な状況を十分に確認し、手元で利用する認証手段についても適宜追随することが重要です。

ITmedia NEWS

楽天証券、多要素認証を突破する「リアルタイムフィッシング詐欺」を確認　ユーザーに注意喚起

2025年10月14日 19時09分 公開　[ITmedia]

楽天証券は10月10日、新たなリアルタイムフィッシング詐欺の発生を確認したとして、利用者に注意喚起した。ユーザーが入力した認証情報をリアルタイムで窃取し、正規サイトへ即座に不正アクセスすることで、多要素認証を突破する手口だった。



楽天証券からのお知らせ <service@rakuten-sec.co.jp> 10月10日(金) 20:39
To 自分

【楽天証券からの重要なお知らせ】

2025年10月10日配信

【緊急・重要】リアルタイムフィッシング詐欺にご注意ください！

配信先の確認・変更はこちら
ウェブログイン後＞マイメニュー＞メールサービス＞現在のメールの配信状況を確認する

楽天証券で新たなリアルタイムフィッシング詐欺の発生を確認しました。

お客様が偽サイトで入力した認証情報をリアルタイムで奪い、攻撃者が正規サイトへ即座にアクセスすることで、多要素認証を突破する手口です。
フィッシングサイトは、楽天証券の正規サイトと見た目では判別がつきづらくなっております。くれぐれもご注意ください。

＜絶対にしないでください＞
・不審な送信元からのメールのURLを開かない。必ず送信元を確認。
・www.rakuten-sec.co.jp 以外から始まるサイトで、ログインID、パスワード、暗証番号や個人情報などを入力しない。

■リアルタイムフィッシング詐欺について
一般的には下の操作を誘導されます。
(1)フィッシングサイトへの誘導（メールまたはSMS経由）
(2)ログインID・パスワードの入力を促される
(3)ログイン追加認証（絵文字）の認証を求められる
(4)取引暗証番号の入力を求められる
(5)個人情報の入力を求められる

■被害にあわれた場合
楽天証券のお客様サポートページから「フィッシング詐欺などによる不正取引に関する問い合わせ」の窓口へお問い合わせください。

楽天証券が利用者に送ったメール（出典：楽天証券、以下同）

今回のケースは、楽天証券を装ったメールやSMSでユーザーを偽サイトへ誘導し、ログインIDやパスワードを入力させ、そこで窃取した情報を用いて攻撃者がリアルタイムで楽天証券の正規サイトにログイン。要求された追加認証（絵文字）の情報も窃取し、偽サイトに表示してユーザーに入力させる。攻撃者はその情報を用いて正規サイトにログインしたという。

●「NHK ONE」アカウント登録メールエラーがGMail等に届かないトラブル

https://www.itmedia.co.jp/mobile/articles/2510/01/news059.html
https://www.itmedia.co.jp/news/articles/2510/02/news085.html
https://www.nhk.or.jp/nhkone/release/assets/pdf/251001_001.pdf
https://www.nhk.or.jp/nhkone/release/assets/pdf/251002_001.pdf

このニュースをザックリ言うと・・・

- 10月1日(日本時間)、NHKより、この日開始したサービス「NHK ONE」において、アカウント登録時の認証コードメールが届かない不具合の発生が発表されました。

- GMail(@gmail.com)の他、ドコモメール(@docomo.ne.jp)・auメール(@ezweb.ne.jp)等でメールが受信されないトラブルが確認された模様です。

- NHKでは「認証コードメールに新しいドメインを使用し、かつ短時間に大量送信したこと」を不具合の原因とし、送信量の調整を行った結果、同2日正午頃までに不具合は解消されたとしています。

AUS便りからの所感

- GMail宛に大量のメールを送信する相手に対する「メール送信者のガイドライン」等に抵触したものとされていますが、既存のドメイン名(@nhk.or.jp, @nhk.jp等)ではなく新規のドメイン名(@mail.nhk)を用いるにあたり、事前のドメインウォームアップ(徐々にメールの送信量を増やす等)を行わず、10月1日のサービス開始時において大量のメール送信が発生したことからトラブルに至ったとされます。

- 今回のケースではSPF・DKIM・DMARCといった設定の問題はありませんでしたが、例えば2024年1月には、神奈川県公立高校へのネット出願システムにおいてDNS設定上の問題による受信トラブルが発生しており、メール送信が絡むサービス構築にあたっては、迷惑メールと誤認識されることのないよう、メールサーバー・DNSサーバーの構築・設定に留まらず、どのドメイン名を使うかといった段階からの運用計画の策定が求められるでしょう。

ITmedia NEWS

「NHK ONE」登録不具合が解消　原因は「新規ドメインからの大量送信」

2025年10月02日 14時33分 公開　[岡田有花，ITmedia]

NHKが10月1日にスタートした新ネットサービス「NHK ONE」で、アカウント登録に必要な認証コードがGmailなど一部のメールアドレスに届かない不具合について、2日正午までに問題が解消した。

NHKによると原因は、「NHKからの認証コードメールに新しいドメインを使用し、かつ短時間に大量送信したこと」。対策として「NHKのシステム側で送信数を調整するなど様々な対応」を行った結果、不具合が解消したという。