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。

● IIJメールセキュリティサービスに不正アクセス、情報漏洩…Webメールプロダクトのゼロデイ脆弱性突かれる

https://internet.watch.impress.co.jp/docs/news/2006723.html
https://www.iij.ad.jp/news/pressrelease/2025/0415.html
https://www.iij.ad.jp/news/pressrelease/2025/0422-2.html
https://jvn.jp/jp/JVN22348866/

このニュースをザックリ言うと･･･

- 4月15日(日本時間)、IIJ社より、同社が運営する法人向けメールセキュリティサービス「IIJセキュアMXサービス」が不正アクセスを受け、顧客情報等が漏えいした可能性があると発表されました。

- 少なくとも2024年8月3日以降において不正アクセスが発生、システムに不正なプログラムが設置されていたことを確認しており、当該サービスの利用者(過去に利用していた利用者含む)最大6,493契約、メールアカウント4,072,650件の情報が漏えいした可能性があり、同22日の続報では、うち586契約およびメールアカウント311,288件について漏洩の事実が確認されたとしています。

- また続報では、不正アクセスについて、当該サービスで2025年2月まで使用していたサードパーティー製Webメールソフトウェア「Active! mail」において未発見・未修正だった(いわゆるゼロデイの)脆弱性「CVE-2025-42599」を悪用されたことが明らかになっています(同16日にはActive! mailの開発元よりセキュリティアップデートがリリースされています)。

- 同社では現在当該サービスを契約中で影響を受けた可能性があるユーザーに対し個別に案内を行っており、また過去利用していたユーザーに対しても連絡を呼び掛けています。

AUS便りからの所感等

- 発表では、被害を受けた情報として、当該サービスで作成されたメールアカウントの情報、送受信されたメールのヘッダー・本文、および当該サービスと連携して動作するように設定されていた他社クラウドサービスの認証情報にまで至っているとのことです。

- 想定される最悪のケースとして、当該サービスの契約者とやり取りした他社のメール等についても攻撃者に傍受されていた恐れもあり、また22日の続報において被害が確認されたとする一部の契約・メールアカウント以外についての問題の有無も不明ですが、今後もIIJ社から随時行われるであろう続報に着目すべきでしょう。

- また、不正アクセスの成立から発覚まで数ヶ月のスパンが発生した原因がゼロデイ脆弱性であったことに尽きるのか、今後そういった侵入経路に拘らず不正アクセスをより早期に発見できる防御策は現れるか、等についても議論が待たれるところです。

Impress Watch

IIJ、「セキュアMXメールサービス」で顧客情報漏えいの可能性、最大400万アカウント超

山田 貞幸　2025年4月15日 10:14

株式会社インターネットイニシアティブ（III）は4月15日、同社が提供する法人向けメールセキュリティサービス「IIJセキュアMXサービス」において、顧客情報の一部が漏えいした可能性があると発表した。

問題が確認されたのは4月10日のことで、同サービスの設備が、2024年8月3日以降に不正なアクセスを受け、不正なプログラムが実行されていた。これにより、同サービス上で送受信されたメールの情報や、認証情報が漏えいした可能性があるという。現在、不正なアクセス経路を特定して切り離しを行い、安全が確保されている。

原因および影響範囲については調査中としているが、最大で6493契約、メールアカウント407万2650件（同サービスの利用者全員）に影響がある可能性がある。

●「Nintendo Switch 2」便乗フィッシングを確認、任天堂が注意喚起

https://pc.watch.impress.co.jp/docs/news/2010049.html
https://x.com/nintendo_cs/status/1915410213089448244

このニュースをザックリ言うと・・・

- 4月24日(日本時間)、任天堂より、「Nintendo Switch 2」の抽選販売の結果を騙るフィッシングメールが確認されているとして注意喚起が出されています。

- 当日は4月4日～同16日の抽選応募者に対する抽選結果のメール発送が予定されていましたが、同社サポートのX(旧Twitter)アカウントより一連の注意喚起の投稿があり、19時20分(初報の投稿)以前に届いたメールや、予約や購入のURL、同社と異なる電話番号・FAX番号があるメールは、同社が送信したものではないとしています。

- 同日23時19分にメール送信を行った旨が上記アカウントから投稿されており、メールが届いていない応募者に対しては、ニンテンドーアカウントの「あなたへのお知らせ」で抽選結果を確認するよう呼び掛けています。

AUS便りからの所感

- 任天堂では同社を騙り「@accounts.nintendo.com」等の発信元アドレスでフィッシングメールが送信される事例について2024年10月にも注意喚起を出しています(AUS便り 2024/10/31号参照)。

- 今後第1回の抽選に外れた応募者についても任天堂による第2回抽選販売の対象となる他、量販店等での抽選販売も順次開始予定で、これらを騙るフィッシングも同様に発生することは明らかです。

- 同社がメール以外の手段での抽選結果確認を呼び掛けているように、ユーザー側のみならずWebサービスやアプリ等を提供する側からも、メール記載のリンクは安易に信用せず、別途ブックマークやスマホアプリから公式サイトにアクセスする(してもらう)方向へのシフトを、ユーザーをフィッシングから保護する意味でも期待したいものです。


Switch 2の抽選結果を装うフィッシングメール、任天堂が注意喚起

宇都宮 充　2025年4月25日 12:48

ポスト　リスト　シェア　はてブ　note　LinkedIn

任天堂サポート
@nintendo_cs · フォローする

[ご注意] マイニンテンドーストアの「Nintendo Switch 2」抽選販売の結果を装ったフィッシングメールを確認しております。本日お送りする抽選結果には、手続き期間の変更に伴い購入手続きのURLが記載されていません。予約や購入のURLがあるものは、当社が送信したものではありません。ご注意ください。

午後8:39 · 2025年4月24日

5万　返信　リンクをコピー

356件の返信を読む

新型ゲーム機「Nintendo Switch 2」の抽選販売に際し、抽選結果を装ったフィッシングメールが確認されているとして、任天堂が注意喚起している。

第1回の抽選結果のメールについては、少なくとも24日19時20分以前に届いたメールや、メール内に予約や購入のURLが記載されているものは、同社が送信したものではないとしている。なお、抽選結果の確認は「マイニンテンドー」内の「あなたへのお知らせ」の項目からも確認できる。

●ゴールデンウィークにおけるセキュリティ面の注意喚起、IPAから発表

https://www.ipa.go.jp/security/anshin/heads-up/alert20250421.html
https://www.ipa.go.jp/security/anshin/measures/vacation.html

このニュースをザックリ言うと・・・

- 4月21日(日本時間)、IPAより、「ゴールデンウイークにおける情報セキュリティに関する注意喚起」が発表されました。

- GW等長期休暇の時期、企業・組織によっては、「システム管理者が長期間不在になる」「友人や家族と旅行に出かける」等、いつもとは違う状況になり、ウイルス感染・不正アクセス等の被害発生時の対処が遅れる、あるいはSNSへの書き込み内容から思わぬ被害が発生する等の可能性があることを鑑み、「企業や組織の管理者」「企業や組織の利用者」「個人の利用者」それぞれを対象に、「休暇前」「休暇中」「休暇明け」に行うべき基本的な対策と心得が「長期休暇における情報セキュリティ対策」においてまとめられています。

- IPAでは、毎年のゴールデンウィークと夏季・冬季休暇の時期に注意喚起を行っていますが、企業や組織の利用者・管理者に対しては、2023年夏季休暇の注意喚起以降、インターネットに接続された機器・装置類の脆弱性を悪用する「ネットワーク貫通型攻撃」への警戒が毎回呼び掛けられています。

AUS便りからの所感

- ネットワーク貫通型攻撃については、情報の漏えいや改ざん、ランサムウェアへの感染に加え、不正な通信の中継点とされてしまう、いわゆるOperational Relay Box(ORB)化等の被害が予想されるとしており、機器類のファームウェア更新やサポート切れとなったものについての計画的なリプレースの他、こういった攻撃が特に管理者不在とみられる隙を突いて行われる可能性を鑑み、事前の監視体制、あるいは万一間に合わずとも事後のログ監査等の体制を確実に整備すべきでしょう。

- また「サポート詐欺」についても企業・組織での被害が継続して確認されているとのことで、IPAが提供している「偽セキュリティ警告(サポート詐欺)画面の閉じ方体験サイト」により、主な手口を把握しつつ慎重に行動できるよう備えることが推奨されます。

- GWまでに日にちがなく十分な対応が間に合わなかったとしても、GW明け以降に点検すべきことは多く存在しますし、以後も夏季休暇等に備えて対応しておくべき事柄も変わらず、また長期休暇に関係なく常時から注意すべき普遍的なものも「日常的に実施すべき情報セキュリティ対策(https://www.ipa.go.jp/security/anshin/measures/everyday.html)」として別途まとまっており、それぞれにおいて準備・点検を行うよう意識していくことが肝要です。


2025年度 ゴールデンウイークにおける情報セキュリティに関する注意喚起

公開日：2025年4月21日
独立行政法人情報処理推進機構
セキュリティセンター

多くの人がゴールデンウィークの長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、システム管理者が長期間不在になる等、いつもとは違う状況になりがちです。このような状況でセキュリティインシデントが発生した場合は、対応に遅れが生じたり、想定していなかった事象へと発展したりすることにより、思わぬ被害が発生し、長期休暇後の業務継続に影響が及ぶ可能性があります。

このような事態とならないよう、(1)個人の利用者、(2)企業や組織の利用者、(3)企業や組織の管理者、それぞれの対象者に対して取るべき対策をまとめています。また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

長期休暇における情報セキュリティ対策
日常における情報セキュリティ対策

注釈：上記リンク先において、対象者毎に参照すべき範囲は以下のとおりです。

1. 個人の利用者：個人向けの対策（3）
2. 企業や組織の利用者：個人及び企業・組織のシステム利用者向けの対策（2-2／3）
3. 企業や組織の管理者：個人、企業・組織のシステム利用者及び管理者向けの対策（2-1／2-2／3）