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。

●チケット販売サイトで他ユーザーの個人情報が表示・変更可能状態に… 負荷対策の設定ミス

https://www.itmedia.co.jp/news/articles/2506/25/news084.html
https://relief-ticket.jp/magazines/guide/info-0624

このニュースをザックリ言うと・・・

- 6月24日(日本時間)、チケット販売大手のぴあ社より、同社運営のSTARTO ENTERTAINMENT(旧ジャニーズ事務所)公式リセールサービス「RELIEF Ticket」において、ユーザー情報が第三者から閲覧・変更可能な事象が発生していたと発表されました。

- 事象が発生していた情報は、同サイトへのログイン履歴があるユーザーの氏名・住所・電話番号・生年月日・メールアドレス・クレジットカード情報(番号下3桁・有効期限・名義)・銀行口座情報とのことです。

- 同23日18時15分～22時0分頃にかけて、ログインユーザー向けページが、他のユーザーがログイン済みの状態で表示されていたとしています。

AUS便りからの所感等

- Webサイトの負荷対策のためにWebページのキャッシュ設定強化を行った際、誤ってログイン情報のCookieもキャッシュに保存する設定としていたのが原因とのことです。

- 2017年にはメルカリでも、CDN切り替え時のキャッシュ設定不備による同様の事例が発生しており、同社から原因となった不備について技術的な詳細が報告されています(https://engineering.mercari.com/blog/entry/2017-06-22-204500/)。

- Webにおけるキャッシュ設定不備の問題は、クライアント側が組織内からプロキシー経由でアクセスする場合に、同じ組織の別のユーザーのPCに情報が露呈する形で発現する可能性もあり、いずれにしろ過去の事例、セキュリティ面での注意事項の解説記事、またCDNサービスからの注意喚起等に従った設定を心掛けることが重要です。

ITmedia NEWS

旧ジャニーズ系チケット公式リセール「RELIEF Ticket」で情報漏えい　他ユーザーの口座情報など一時編集可能に　Cookie誤設定で

2025年06月25日 14時12分 公開　[ITmedia]

ぴあは6月24日、公式リセールサービス「RELIEF Ticket」で、利用者の個人情報が一時的に他のユーザーから閲覧・編集できる状態になっていたと発表し、謝罪した。原因は外部からの攻撃や不正アクセスではなく、キャッシュの設定の誤りだったとしている。

問題が起きたのは、23日午後6時15分から午後10時頃にかけて。アクセス集中による負荷軽減のため、Webページのキャッシュ（一時保存）設定を強化した際、ログイン状態を識別するCookie情報まで誤って保存してしまっていた。この影響で、RELIEF Ticketにログインした利用者が、ログイン履歴のある別のユーザーのマイページにアクセスしてしまう事態が発生。個人情報が閲覧、または編集可能になっていたという。

対象となった個人情報は以下の通り。

- 住所・電話番号：閲覧、変更が可能
- 氏名・生年月日・メールアドレス：閲覧が可能
- クレジットカード番号（下3桁）・有効期限・名義：閲覧、登録、削除が可能
- 銀行口座情報（金融機関名・支店名・口座種別・番号・名義）：閲覧、編集が可能

● Windows 10のサポートを延長するオプション、個人向けは条件付きで無料提供も

https://forest.watch.impress.co.jp/docs/news/2025455.html
https://learn.microsoft.com/en-us/windows/whats-new/extended-security-updates
https://blogs.windows.com/windowsexperience/2025/06/24/stay-secure-with-windows-11-copilot-pcs-and-windows-365-before-support-ends-for-windows-10/
https://pc.watch.impress.co.jp/docs/news/1636047.html

このニュースをザックリ言うと・・・

- 6月25日(日本時間)、Windows 10のセキュリティパッチを本来のサポート終了期限となる2025年10月以降も受け取ることが可能となるオプション「Extended Security Update(ESU)」の開発者向けテストの開始が発表されました。

- 7月より個人ユーザーを含めた一般向け提供が開始され、8月中旬には広く利用できるようになる見込みとされています。

- 今回個人ユーザーについては、「Windows バックアップで設定をクラウドに同期する」か「Microsoft Rewardsのポイント1,000と引き換え」の条件付きで、無料で利用可能になることが発表されています。

AUS便りからの所感

- Windows 10のESUについては2023年の時点で提供が発表され、本来は企業向け(最大3年間提供)に年間61ドルから、個人向けにも30ドルからで提供される有償オプションとなります(企業向けについては年毎に価格が上昇することが示唆されています)。

- かつてWindows 7においても企業向けのみでESUが提供されていましたが、10においても11への移行が(ハードウェア条件等の理由により)想定より進んでいなかったことから、個人向けへの提供、かつ条件付き無償提供といった施策がとられたとみられます。

- とは言え11に移行できないようなスペックのPCを延長した後の期限まで使い続けることは、様々なリスクの潜在の他、十分な作業効率が得られない可能性もあり、十分な量のメモリ(今日では基本16GBとすべきです)とSSDを搭載した新しいPCへ早期に乗り換えるよう計画することを強く推奨致します。

●メルマガ解約ボタンからフィッシングサイトへ誘導する手口に注意喚起

https://news.mynavi.jp/techplus/article/20250619-3357199/
https://www.esecurityplanet.com/news/unsubscribe-buttons-could-be-a-trap/

このニュースをザックリ言うと・・・

- 6月17日(現地時間)、セキュリティニュースサイト「eSecurity Planet」において、メールマガジンの購読解除手続きを騙り悪意のあるWebページへ誘導する手口への注意喚起が出されています。

- フィッシングメール・スパムメールの最後に「購読解除ページへのリンク」が記載されており、これをクリックすると個人情報を詐取するようなWebページに繋がる可能性があるとしています。

- またリンクのクリックにより、「メールの送信先のアドレスが実在することを特定される」「誘導先のWebページでマルウェアに感染する」恐れもあるとしています。

AUS便りからの所感

- GMail等では大量メール発信業者に対しList-Unsubscribe: ヘッダーを用いたメール購読解除機構の対応を義務付けており、ブラウザーによってWebサイトを開く必要がないことから、記事ではこの機構をより安全なものとして紹介しています(ただし「メールの送信先のアドレスが実在することを特定される」という面でのリスクは同様にあると思われます)。

- ともあれ、悪意を以てフィッシングメール・スパムメールを送信する相手に対し、送信を停止してもらおうとするアクションが確実に受け入れられるとは限らないため、そのような手口が存在するという情報収集を随時行いながら、アンチウイルス・UTM等の不正なメールについて受信を防止したり警告を出したりする機構を確実に有効化し、不審なリンクに安易に触らないよう慎重に行動することが重要です。