

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。



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。
- とはいえ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、十分な作業効率を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。

Microsoft、「Windows 10」延命プログラム「ESU」をテスト開始、個人でもOK、無償オプションも
一般展開は7月から順次、8月中旬には広く利用できるようになる見込み
橋井 秀人 2025年6月25日 08:22

Stay secure with Windows 11, Copilot+ PCs and Windows 365 before support ends for Windows 10
By Yael Mink | Executive Vice President, Consumer Chief Marketing Officer

米Microsoftは6月24日(現地時間)、「Windows 10」の拡張セキュリティ更新プログラム(Extended Security Update: ESU)のテストをパイロットプログラム「Windows Insider Program」で開始した。「Windows 10」のサポートは米国時間2025年10月14日に終了するが、ESUを購入すればサポート終了後もセキュリティ更新プログラムを受け取ることができる。

昨年に発表された通り、「Windows 10」のESUは個人でも購入できる。ESUの提供が開始されると、通知トーストや「設定」アプリから登録ウィザードへアクセスできるようになるとのこと。

●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。

「メール購読解除ボタン」に注意、個人情報を盗む詐欺の恐れ

掲載日 2025/06/19 08:38 更新日 2025/06/20 16:59 著者: 後藤大地

eSecurity Planetは6月17日(現地時間)、「Think Before You Click: 'Unsubscribe' Buttons Could Be a Trap」において、覚えのないメールマガジンの購読を解除することで個人情報を流出する可能性があるとして、注意を喚起した。

フィッシングメールやスパムメールの最後に記載された購読解除リンクにアクセスすると、悪意のあるWebサイトに誘導される可能性があるという。

The screenshot shows the eSecurity Planet website with the article title 'Think Before You Click: 'Unsubscribe' Buttons Could Be a Trap, Experts Warn'. The article is dated June 17, 2025, and is written by Andrew Rodolakis. The article text discusses the risks of clicking on unsubscribe links in phishing or spam emails, which could lead to the disclosure of personal information. It mentions that while some unsubscribe mechanisms are secure, others are not, and that clicking on such links could be a trap. The article is categorized under 'Top Cybersecurity Companies'.