

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。

## ●メルカリ装った詐欺メール出回る…本物そっくりのログイン画面で個人情報狙う

<https://www.itmedia.co.jp/news/articles/1904/04/news117.html>  
[https://www.antiphishing.jp/news/alert/mercari\\_20190403.html](https://www.antiphishing.jp/news/alert/mercari_20190403.html)



### このニュースをザックリ言うと…

- 4月3日（日本時間）、フィッシング対策協議会より、フリマアプリ「メルカリ」をかたるフィッシングメールが出回っているとして警告が出されています。

- メールは、

◆ 件名には「メルカリ事務局[MERCARI]重要なお知らせ」「メルカリ事務局サービス変更予定のお知らせ」

◆ 本文には「有効期限が過ぎる前に、ぜひアカウントをご更新ください」「アカウントを確認されない場合、以下の機能が制限されることとなります」等と記載され、

◆ 「ログインアカウント」(原文ママ)と書かれたリンクをクリックするとメルカリの偽のログイン画面および個人情報等の入力画面に誘導されます。

- 同協議会では、このようなフィッシングサイトでメールアドレス・パスワード・個人情報・クレジットカード情報などを絶対に入力しないよう呼びかけています。

### AUS便りからの所感等

- フィッシング対策協議会で示されている一例では、メールの文面において本物のサイトのURLや運営会社の住所を記載しており、フィッシングサイトの方に至っては、**メルカリの本物のログイン画面・新規登録時の各種情報入力画面をかなり巧みに模倣している**他、JCBのカードを使用する際の本人認証サービスの偽ページまで用意している模様で、フィッシングサイトのURLが「<https://www.mercari.com/>」ではなく「<http://●●●.xyz>」であることに気付かない限りはだまされてしまう可能性もあるでしょう。

- 特に不審なメールを受け取った場合には、同協議会のサイト等フィッシングメールに関する情報が集積されているページあるいはSNSにおいて報告がないか調査すること、また普段からブラウザやセキュリティソフトおよびUTMによるアンチフィッシング機能を有効化しておき、利用しているサービスには事前に登録しているブックマークからアクセスする等の習慣をつけ、フィッシングにだまされないよう行動するようにしましょう。

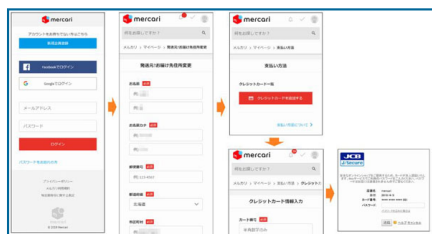


#### メルカリ装った詐欺メール出回る 本物そっくりのログイン画面で個人情報狙う

© 2019年04月04日 20時15分 公開 [ITmedia]

印刷 158 f 69 B! ?

フィッシング対策協議会は4月4日、フリマアプリのメルカリを装った詐欺メールが出回っているとして、消費者に注意を呼び掛けた。メール内のリンクをクリックすると、メルカリのログイン画面に酷似したWebサイトに遷移するが、遷移先は個人情報不正に入手するための偽サイトだという。



#### メルカリをかたるフィッシング (2019/04/03)

##### 概要

メルカリをかたるフィッシングメールの報告を受けています。

##### メールの件名

メルカリ事務局[MERCARI]重要なお知らせ  
メルカリ事務局サービス変更予定のお知らせ  
メルカリ事務局サービスが有効期限切れになります

##### 詳細内容

メルカリをかたるフィッシングの報告を受けています。

1. 2019/04/03 15:00 現在、フィッシングサイトは稼働中であり、JPCERT/CCにサイト開鎖のための調査を依頼中ですが、類似のフィッシングサイトが公開される可能性がありますので引き続きご注意ください。

2. このようなフィッシングサイトにてアカウント情報（メールアドレス・パスワード）、個人情報（お名前、郵便番号、住所、電話、生年月日など）、クレジットカード情報（カード番号、有効期限、セキュリティコード）、本人認証サービスのパスワード等を絶対に入力しないように注意してください。

3. 類似のフィッシングサイトやメールを発見した際には、フィッシング対策協議会 (info@antiphishing.jp) までご連絡ください。

## ●Facebookのユーザ情報、5億4,000万件がサードパーティーアプリ経由で流出

<https://www.itmedia.co.jp/enterprise/articles/1904/04/news061.html>



### このニュースをザックリ言うと…

- 4月3日(現地時間)、セキュリティベンダーの米UpGuard社より、Facebookアプリによって収集されたユーザのデータがAWS上に外部からアクセス可能な状態で保存されていたと発表されました。
- データはサードパーティー(外部企業)によるアプリ2種が収集していたものが確認されており、メキシコのCultura Colectiva社製アプリによるデータには、ユーザがFacebookに投稿したコメントや「いいね」などのリアクション、アカウント名、Facebook IDなど5億4,000万件以上の記録が含まれていたとされています。
- もう一つの「At the Pool」というアプリのデータにも、ユーザ22,000件余りのIDや各種情報、およびFacebookではなくアプリのものと思われるパスワードが平文で保存されていたとのことです。

### AUS便りからの所感等

- 今回はFacebook自体からの情報の流出でこそありませんが、全世界で20億人以上を超えるとされるユーザの1/4近くに相当するデータが含まれていたことは十分なインパクトを与えると考えられ、また悪意のある者がこれだけのまとまったデータを入手することにより、ユーザにspamを送信する等の行為を行うことも容易に想像できます。
- また、流出したパスワードを別のサービスで使い回していた場合、いわゆる「リスト型攻撃」によって芋づる式に不正ログインの被害を受ける可能性がありますので、各サービスに設定するパスワードは異なるものを設定するよう心掛けましょう。



ITmedia  
**179-プライズ**

Facebookのユーザー情報、5億4000万件がサードパーティーアプリ経由で流出

サードパーティーアプリに属するFacebookのユーザーに関する情報が、Amazon S3の公開バケットに保存され、一般ユーザーがファイルをダウンロードできる設定になっていた。

© 2019年04月04日 18時00分 公開 [記事変子, ITmedia]

人 102 | ツイート 102 | f 174 | B! 35

データ漏えい対策を手掛ける米セキュリティ企業UpGuardは4月3日、サードパーティーアプリに属するFacebookのユーザーに関する情報が、Amazon S3の公開バケットに保存されていたと伝えた。

UpGuardによると、メキシコのメディア企業Cultura Colectivaのデータには、ユーザがFacebookに投稿したコメントや「いいね」などのリアクション、アカウント名、Facebook IDなど5億4000万件以上の記録が含まれていた。

一方、「At the Pool」というFacebook連携アプリのバックアップ情報には、Facebook IDや友達、音楽、映画、写真、グループ、チェックインなどの情報が含まれる他、ユーザー2万2000人余りのパスワードが平文で保存されていた。

このパスワードはAt the Poolのものだったと思われるが、ユーザが同じパスワードを使い回していた場合は危険にさらされるとUpGuardは指摘する。At the Poolは2014年に廃業し、親会社のWebサイトにもつながらない。

## ●「Windows 10 Fall Creators Update」のサポート終了

<https://forest.watch.impress.co.jp/docs/news/1178952.html>



### このニュースをザックリ言うと…

- 4月10日(日本時間)、Windows 10の「Fall Creators Update」ことバージョン1709のサポートが一部のエディションを除いて終了しました。
- Windows 10の「Home」や「Pro」等のエディションについて、各バージョンにおけるサポート期間はリリースから18ヶ月間とされ、以後は毎月のセキュリティアップデート等が提供されなくなります。
- バージョン1709を使用しているユーザについては、最新バージョンである1809(October 2018 Update)へのアップデートを行うよう推奨される他、5月下旬には次期バージョン「May 2019 Update」の一般提供が開始される予定です。

### AUS便りからの所感等

- 企業向け上位エディション「Enterprise」および教育機関向けの「Education」は2020年4月がサポート終了となり、Enterpriseについてはさらにリリースから約10年間のサポートが受けられるオプションもあります。
- この他、Windows 10におけるバージョンアップやWindows Updateが予期せぬタイミングで実行されることに対する批判が相次いでいることから、May 2019 Updateおよびそれ以前のバージョンに対しアップデートのインストール等のタイミングを管理できる機能が追加される予定となっています。
- 2020年1月にサポート終了予定のWindows 7にも言えることですが、セキュリティアップデートを行わないままでいることにより、マルウェアに感染する等のリスクは徐々に増えていきますので、基本的な対策として各PCのOSのアップデートを確実に実行すること、これに加えてアンチウイルスやUTMによる多重防御を行うことが重要です。



Microsoft、「Windows 10 バージョン 1709」のサポートを終了

“Enterprise”“Education”の再エディションは来年4月14日まで利用可能

特記 秀人 2019年4月9日 12:30

米Microsoftは4月9日(現地時間)、「Windows 10 バージョン 1709」(Fall Creators Update)のサポートを終了する。セキュリティ更新プログラムの提供は、同日リリースされる月別アップデートが最後となる(日本時間では10日)。まだ利用中の場合は、後継バージョンへのアップデートが必要だ。

「Windows 10」の各機能アップデートは、リリースされてから18カ月サポートされるのが基本だ。「Windows 10 バージョン 1709」の場合、2017年10月17日のリリースから18カ月が経過した2019年4月9日をもって、サポート期間の満了を迎えることになる。