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。

●「リスト型攻撃」で不正ログイン…ECサイトから97,533件の個人情報流出か

https://www.itmedia.co.jp/news/articles/2411/27/news182.html
https://www.oisixradaichi.co.jp/news/posts/20241126/

このニュースをザックリ言うと･･･

- 11月26日(日本時間)、オイシックス・ラ・大地社より、同社が運営する食品宅配ECサイト「Oisix.com」が不正アクセスを受け、個人情報が不正に閲覧された可能性があると発表されました。

- 被害を受けたのは、同サイトユーザのうち約97,533件の個人情報(氏名・住所・電話番号・メールアドレス・届け先情報・予約・購入履歴)とされており、クレジットカード情報は含まれていないとのことです。

- 同24・25日に、いわゆる「リスト型攻撃」によって不正ログインを受けたとされ、対象ユーザーについてはパスワードのリセットを行い、再設定を案内したとしています。

AUS便りからの所感等

- 発表では当該サイトでの不正ログイン攻撃対策としてWAFを導入していながら不正ログインを防げなかったとし、さらなる対策の強化を行うとしています。

- 発表においてユーザーに対し定期的なパスワードの変更も呼び掛けていますが、逆にパスワードの安全性を下げる可能性もあることからセキュリティ専門家の間では「悪手」とされ、リスト型攻撃を回避するため、ユーザー側においては各サービスで共有していない独自のパスワードを設定することが最も重要であり、またアカウントが不正ログインを受けた場合の他、万が一パスワードを他で共有していた場合には、それら全てのサービスで速やかにパスワードの変更を行う必要があります。

- 一方で、このようなセオリーが定着して何年も経っている現在に至っても、今回のように リスト型攻撃で一つのサイトから大量の不正ログインが発生する事態は度々発生しており、特に大規模なサービス提供側において、不審なログイン試行を遮断する各種機構の導入のみならず、多要素認証やパスキーといった強力な認証機構についても導入と利用の推奨さらには義務化が進むのかが注目されるところです。

ITmedia NEWS

「Oisix.com」に不正ログイン10万件　WAF導入も、パスワードリスト攻撃防げず

2024年11月27日 15時44分 公開　[ITmedia]

オイシックス・ラ・大地は11月26日、食品宅配ECサービス「Oisix.com」がパスワードリスト型攻撃による不正ログインを受け、9万7533件の個人情報が閲覧された可能性があると発表した。同社は不正ログイン攻撃対策としてWAF（Web Application Firewall）を導入していたが、防げなかったという。

クレジットカード番号は決済代行会社が保持しているため流出の可能性はない。

【重要】当社WEBサイトへの「なりすましログイン」への対応に関して

日頃は、弊社のサービスをご利用いただきまして、誠にありがとうございます。
弊社が運営する「Oisix.com」におきまして、第三者が外部から不正に取得したIDとパスワードを使用し、お客さまになりすましてログインする事象（以下、「なりすましログイン」）が発生いたしました。
なりすましログイン時に第三者がお客さまの氏名、住所、電話番号、メールアドレス、お届け先等の情報が閲覧される可能性がございますため、対象のお客さまには、11月25日（月）に弊社にてパスワードのリセットを実施いたしました。
なお、クレジットカード番号につきましては決済代行会社にて保持しておりますため、第三者に閲覧されている可能性はございません。
お客さまをはじめ、関係者の皆様に多大なるご心配とご迷惑をおかけすることとなり、深くお詫び申し上げます。

● Windows 11ハードウェア要件緩和の噂を否定か…MS「TPM 2.0は必須」

https://forest.watch.impress.co.jp/docs/news/1644814.html
https://techcommunity.microsoft.com/blog/windows-itpro-blog/tpm-2-0/4339066
https://forest.watch.impress.co.jp/docs/news/1645150.html

このニュースをザックリ言うと・・・

- 12月4日(現地時間)、Microsoft(以下・MS)より、Windows 11インストールのためのハードウェア要件に関する記事が「Windows IT Pro Blog」で発表されました。

- 従来からハードウェア要件の一つとしていた「TPM(Trusted Platform Module) 2.0」への対応について、各種セキュリティの問題に対処し、Windows 11の安全性と将来性を確保するために必要な要素とし、今後も要件から外す予定はないとしています。

- 11月28日に「要件を満たさない古いPCについても11のインストールが許可される」という真偽不明の情報が海外のブログに投稿されており、これを否定する意味も含めての発表ともみなされています。

AUS便りからの所感

- インプレス「窓の杜」においても日本マイクロソフト社に問合せており、同様に「Microsoftから変更の発表をした事実はなく、Windows 11のシステム要件に変更はありません」と回答されたとのことです。

- TPM 2.0非対応のPCにWindows 11をインストールする非公式な方法はネット上で見つかるものの、MSではこれを行った場合「PCはサポートされなくなり、更新プログラムを受け取る資格がなくなる」としているとのことです。

- またそのようなPCは、CPU・メモリ・ストレージ等の要因により、10でも快適な動作が期待できず、2025年10月の10サポート終了時には5年以上は稼働しているとみられることから、より新しいPCへのリプレースを行う機会と考えるべきでしょう。

Windows 11に「TPM 2.0」は必須 ～ハードウェア要件緩和の風説にMicrosoftが釘をさす

「TPM 2.0」は単なる推奨事項ではない

樽井 秀人　2024年12月4日 12:35

米Microsoftは12月4日（現地時間）、公式ブログ「Windows IT Pro Blog」で、『TPM 2.0 – a necessity for a secure and future-proof Windows 11』と題する記事を公表した。最近、Microsoftが「TPM 2.0」をはじめとするWindows 11のハードウェア要件を緩和し、これまでインストールできなかったデバイスにもインストールを許可する方針だという風説が流布しているが、それに反応した記事のようだ。

「TPM」（Trusted Platform Module）は、ハードウェアレベルのセキュリティサービスを提供する専用のチップまたはファームウェアのこと。暗号化キー、証明書、パスワード、機密データを安全に保存し、不正アクセスから保護する役割や、乱数の生成、データの暗号化と復号化、デジタル署名の確認などの暗号化操作を担当する。

●三菱UFJ銀行、貸金庫資産窃盗事件に便乗した詐欺メールに注意喚起

https://www.itmedia.co.jp/news/articles/2411/25/news185.html
https://www.bk.mufg.jp/emeg/10_1490.html
https://www.itmedia.co.jp/news/articles/2411/22/news174.html

このニュースをザックリ言うと・・・

- 11月25日(日本時間)、三菱UFJ銀行より、同行の貸金庫取引を騙る詐欺メールが報告されたとして注意喚起が出されています。

- 詐欺メールは、同22日に発表された、当時の同行行員による貸金庫資産窃盗事件に便乗するものとされ、暗証番号等を詐取する偽ページに誘導し、個人情報を奪取しようとする内容とされています。

- 同行では、現時点ではメールにて貸金庫取引に関する連絡は行わないとし、不審なページで暗証番号等を入力しないよう呼び掛けています。

AUS便りからの所感

- 同行で発生した窃盗事件は十数億円の被害が出る等してニュースでも大きく報じられ、金融業界全体に対する貸金庫業務への信頼性についても議論となっているようです。

- 国内外でニュースとなるような大きな事件・イベントには必ず便乗しての詐欺・フィッシング・マルウェア感染を目論む攻撃が発生するものであり、本物の企業・運営団体やセキュリティ関連団体からの注意喚起、実際にメールやSMSが送信される場合のポリシーを確認し、決して無闇にリンクをクリックしないこと、また実際に利用しているサービスのWebサイトには予め登録したブックマークやスマホアプリからアクセスする等、慎重に行動するよう心掛けることが重要です。

三菱UFJ、貸金庫取引を装うメールに注意喚起　元行員による顧客資産の窃取を受けてか

2024年11月25日 18時33分 公開　[ITmedia]

三菱UFJ銀行の不祥事に便乗した詐欺メールを確認したとして、同行は11月25日までに注意を呼び掛けた。貸金庫取引に関する情報をかたったメールで、同行と関係のない虚偽のWebページにアクセスさせ、暗証番号などの個人情報を盗み取ろうとするという。