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。

●地方スーパーのECサイト利用者個人情報・予約情報6,337件が不正アクセスで流出

https://www.itmedia.co.jp/news/articles/2109/17/news153.html
https://ryubostore.jp/news_detail.html?code=65
https://www.grinc.co.jp/information202109.pdf
http://www.mrk09.co.jp/%e9%87%8d%e8%a6%81%e3%81%aa%e3%81%8a%e7%9f%a5%e3%82%89%e3%81%9b/

このニュースをザックリ言うと･･･

- 9月17日(日本時間)、沖縄県のスーパーマーケット運営会社であるリウボウストア社より、同社オンラインショップへの不正アクセスにより、個人情報の流出が発生したと発表されました。

- 被害を受けたのは、オンラインショップ会員の個人情報(氏名・性別・会社名・郵便番号・住所・電話番号・メールアドレス等)1,201件および商品予約情報5,136件の、計6,337件とされています(クレジットカード情報の流出は確認されていないとのことです)。

- オンラインショップを管理する東芝テック社から再委託を受けたジーアール社(京都市)の会社のサーバーで、3月から4月にかけて不正アクセスが発生していたことが、9月の調査で発覚したとのことです。

AUS便りからの所感等

- 近年頻発する決済フォームの改ざんによるものではなかったとみられる一方、不正アクセスを受けたサーバーは複数社にECサイト関連サービスを提供する共用システムのサーバーだったとされ、同じシステムを利用していた山口県のスーパーマーケット運営会社である丸久社からも同様の情報流出が発表されており、今後も不正アクセスの詳細や、同じサービスを利用する他のスーパーマーケット等にも被害が発生していたかについて、追加発表があるとみられます。

- 似通ったケースとしては、今年5月にも、プロジェクト情報管理ツールが不正アクセスを受け、複数の企業にまたがる情報流出が発生したことが発表されています(AUS便り 2021/06/01号参照)。

- ジーアール社では、これまでにも毎月のシステムチェックや、二ヶ月に一度のプログラム改修およびセキュリティの強化対策を実施しており、今後は追加対策として15分おきの攻撃プログラム監視等を行うと報告しているとのことですが、万が一未発表・未修正の脆弱性を悪用されてサーバーへの侵入等が発生したとしても、そこから外部への情報流出を阻止するような「出口対策」を可能とするよう、堅牢なネットワーク構成をUTM等を用いて行うことが、今後重要となるでしょう。

ITmedia NEWS

沖縄のスーパーで個人情報など計6000件以上が流出した可能性　商品の予約情報も

2021年09月17日 19時19分 公開　[松浦立樹，ITmedia]

印刷　134　Share　B!　8

沖縄県でスーパーマーケットを展開するリウボウストア（那覇市）は9月17日、ECサイトを管理するサーバに不正アクセスを受け、個人情報など6337件が流出した可能性があると発表した。ECサイトの会員データに加え、店頭で販売していた商品の予約情報も流出した可能性があるという。

ECサイト会員の氏名や性別、会社名、郵便番号、住所、電話番号、メールアドレスなど計1201件が3月25日に、うなぎやワインといった商品の予約情報5136件が4月8日に漏えいした可能性がある。9月17日時点ではクレジットカード情報の漏えいや、個人情報などの悪用は確認していないという。

●小学校でいじめ原因の自殺…貸与タブレットでパスワード共有、なりすまし横行か

https://www.tokyo-np.co.jp/article/130621
https://www.tokyo-np.co.jp/article/130896
https://president.jp/articles/-/49923

このニュースをザックリ言うと・・・

- 9月13日(日本時間)、町田市立小学校に通っていた当時小学6年生の児童が2020年11月にいじめが原因で自殺していたことについて、遺族が記者会見を行ったことが新聞・テレビ等で報じられました。

- 会見において、同小学校で各児童に貸与されていたタブレット(一部メディアによれば、Chromebookとされています)のチャット機能で、自殺した児童を中傷する書き込みがあったとされていますが、このタブレットについて、パスワードが「123456789」に統一されていたことと、IDが児童の所属学級と出席番号の組合せとなっていたことが指摘されています。

- 遺族から児童の同級生への聞き取りにより、「自分が書いていないのに勝手に書き込まれた」「書いていた内容を消された」といった被害が発生していたことも明らかになっており、他の児童のIDを推測することによる「なりすまし」が発生していたとみられています。

AUS便りからの所感

- 他のユーザーのIDが推測しやすいこと自体が直ちに直接的な問題となるわけではありませんが、加えて共通のパスワードが設定されていたことから、「不正ログイン」が容易に行える状態にあったことになります。

- 例えば各端末に管理者がログイン可能とする設定にしたかったにしても、管理者と所有者当人以外がなりすましでログイン可能になってしまうのでは本末転倒であり、ユーザーに対し「パスワードを安易に人に教えたりしない」等といったセキュリティ教育を確実に行う意味でも、全てのユーザー毎に異なる、かつ推測されにくいパスワードを設定することが、管理側において最低限要求される事項といえます。

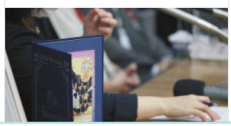
東京新聞

いじめ温床のタブレット端末、パスワードは「123456789」　町田の小６自殺

2021年9月15日 06時00分

東京都町田市立小学校の６年生女児＝当時（１２）＝が２０２０年１１月、「いじめを受けていた」とメモを残し自殺したことをめぐり、萩生田光一文部科学相は１４日、「ＧＩＧＡスクール構想」の先進事例として児童に配られたタブレット端末がいじめに使われたことを明らかにした。「極めて残念な事実。重く受け止め事実関係を確認する」として問題点を解明し全国の教育現場に伝える方針を示した。（小松田健一、服部展和、奥野斐）

【関連記事】東京・町田の小6女児が自殺、同級生からのいじめ示すメモ　遺族「学校のタブレット温床に」



女児の両親は学校側に、端末のチャット履歴について開示を求めていたが「履歴は見当たらない」と回答しており、いじめとタブレット端末の関連が、文科省の都教委、町田市教委への聞き取りで初めて明らかになった。

両親によると、児童同士がタブレット端末の画面上で女児の名前を挙げ「うざい」「お願いだから死んで」などと会話。女児もこれを見ていたという。

●Acrobat Reader等Adobe製品に脆弱性…セキュリティアップデートの適用を

https://news.mynavi.jp/article/20210917-1974074/
https://www.jpcert.or.jp/at/2021/at210040.html
https://www.ipa.go.jp/security/ciadr/vul/20210915-adobereader.html

このニュースをザックリ言うと・・・

- 9月15日(日本時間)、Adobe社より、Acrobat ReaderやAcrobat等同社製品の脆弱性を修正するセキュリティアップデートがリリースされています。

- 細工されたPDFファイルをAcrobat Readerで開く等により、脆弱性が悪用され、PC上で任意のコードが実行される恐れがあるとされています。

- 同日にはJPCERT/CCおよびIPAからも脆弱性に関する注意喚起が出され、関連する製品のアップデートが呼び掛けられています。

AUS便りからの所感

- Adobe社製品のセキュリティアップデートは、他にもPhotoshopやInDesign等についてもリリースされています(https://forest.watch.impress.co.jp/docs/news/1351353.html)。

- Acrobat Reader DC(およびAcrobat DC)2021.007.20091等が最新バージョンとなっており、通常は自動更新が有効となっていますが、念の為手元で利用している製品のバージョンを確認し、最新でない場合は「ヘルプ」→「アップデートの有無をチェック」の実行を行うことを強く推奨致します。

- また、アップデートを即座に行っている・いないに拘らず、もしくは完了に間に合わない状態でマルウェア等の攻撃を受ける可能性を考慮し、アンチウイルス(デフォルトで含まれるMicrosoft Defender含む)やUTMによる防御を確実に行い、無防備な状態を作らないよう十分に注意しましょう。

TECHR Powered by マイナビニュース

Adobe AcrobatとReaderに攻撃リスクの高い脆弱性、アップデートを

2021/09/17 09:31　　著者：後藤大地

JPCERTコーディネーションセンター（Japan Computer Emergency Response Team Coordination Center：JPCERT/CC）は9月15日、「Adobe AcrobatおよびReaderの脆弱性（APSB21-55）に関する注意喚起」において、Adobe AcrobatおよびAdobe Acrobat Readerに脆弱性が存在すると伝えた。

対象の脆弱性を悪用されると、ユーザーが細工されたコンテンツを開くことで任意のコードが実行される危険性があるとされている。