— AUS（アルテミス・ユーザ・サポート）便り 2019/12/23号 —
https://www.artemis-jp.com

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。

●マカフィー「2019年の10大セキュリティ事件ランキング」発表…1位は7payの不正利用、等

https://news.mynavi.jp/article/20191218-941627/
https://www.mcafee.com/enterprise/ja-jp/about/newsroom/press-releases/press-release.html?news_id=2019121701

このニュースをザックリ言うと･･･

- 12月17日(日本時間)、セキュリティベンダーのマカフィー社より、同社がIT担当者等1,552人に対し実施した「2019年のセキュリティ事件に関する意識調査」に基づく「10大セキュリティ事件ランキング」が発表されました。

- 最も認知度が高かったベスト3は「7payの不正利用発覚(認知度63.9%)」「クロネコメンバーズの不正ログイン(同36.4%)」「ファーウェイ製通信機器の安保上の理由による締め出し(同34.0%)」で、以下にも当AUS便りで取り上げたもの・取り上げられなかったもの含め、少なからず話題になった事件が取り上げられています。

AUS便りからの所感等

- 同社が昨年発表した2018年の10大セキュリティ事件ランキング(AUS便り 2018/12/17号参照)では、Coincheckからの流出事件が1位となったのをはじめ仮想通貨関連が3件ランクインしていましたが、今年は圏外となる等、セキュリティ業界における話題の移り変わりの激しさを物語っています。

- 一方で大規模な個人情報流出事件が3件、メールおよびSMSによるフィッシングが2件ランクインし、長年の間根強く問題となり続けている事柄も多く存在していることが窺い知れます。

- 年末年始には、大手セキュリティベンダーや関連団体等により、一年間に話題になったセキュリティ関連ニュースのまとめや、翌年における業界の動向予測等がリリースされますが、それぞれ異なる観点により独特の項目が挙げられることも多々ありますので、特にシステム管理者においては、セキュリティの脅威に関する情報収集を随時行うとともに、新しい脅威からの被害をも最小限に抑えられるようなシステム・ネットワークの見直しを随時検討して頂ければ幸いです。

McAfee

順位	セキュリティ事件（時期）	認知度(%)
1	セブン&アイ・ホールディングス傘下のセブン・ペイが運営するバーコード決済サービス「7pay」の一部アカウントへの不正アクセスを確認。経緯とともに同サービスの廃止を発表（7月～10月）	63.9
2	ヤマト運輸が提供するクロネコメンバーズのWebサービスにて外部からパスワードリスト攻撃による不正ログインが判明（7月）	36.4
3	通信機器でスパイ行為をしているとの指摘を受け、次世代通信規格5Gネットワーク建設で、中国の華為技術（ファーウェイ）の通信機器に対して、安保上の理由から締め出し強化（5月）	34.0
4	会員制交流サイト（ＳＮＳ）に投稿された顔写真の瞳に映った景色を手掛かりに、アイドル活動をしている女性の住所を特定し、わいせつな行為をしたとして男が逮捕、起訴（10月）	33.4
5	5億4000万件以上のFacebookユーザーの情報を含むデータセットが、Amazon Simple Storage Serviceのバケットからダウンロード可能な状態で公開されていたことが発覚（4月）	29.6
6	ゆうちょ銀行をかたり、「『ゆうちょ認証アプリ』による本人認証サービス開始」などの件名で、本文に記載したフィッシングURLからのログインを促す内容のフィッシングメールに対して注意喚起（6月）	28.4
7	トレンドマイクロの元従業員が顧客情報を盗み出し、第三者に売却したことで米国など海外の最大12万人分の情報が外部に流出（11月）	27.3
8	スマートフォンのSMS（ショートメッセージサービス）を使って個人情報を盗み取ろうとする「スミッシング」と呼ばれるサイバー攻撃が激化（4月）	25.6
9	「宅ふぁいる便」サーバへ不正アクセス、約480万件の個人情報が流出（1月～3月）	25.5
9	北朝鮮 金正恩氏と米 ドナルド・トランプ大統領による首脳会談中にも、北朝鮮のハッカー集団がアメリカや同盟国の企業に対するサイバー攻撃の手を緩めず（2月～3月）	25.5

●楽天グループ従業員の個人情報流出…偽役員からの電話で

https://www.nishinippon.co.jp/item/n/564720/
https://www.itmedia.co.jp/news/articles/1912/03/news132.html
https://bunshun.jp/articles/-/16703

このニュースをザックリ言うと･･･

- 12月3日(日本時間)、楽天グループの従業員情報を管理する社内システムに登録された個人情報が流出したと西日本新聞等で報じられました。

- 流出したのは社員の氏名・役職・メールアドレスおよび内線番号等で、複数の従業員がグループ会社役員を騙る人物からの英語による電話指示を受けてデータの抽出を行い、偽役員が指定した外部メールアドレスに送信したとされています。

- 11月中旬までに、流出した情報は特定できており、従業員の個人住所や家族名および銀行口座等の情報は含まれておらず、流出した社内アカウントへの不正ログインなども検知されていなかったとしています。

AUS便りからの所感

- 典型的なソーシャルエンジアリングの一種であり、特に楽天では社内公用語が英語であることから、偽役員からの英語での指示についても疑われなかったとされています。

- 一方で、いわゆるビジネスメール詐欺(BEC)や、10月以降に話題となったマルウェア「Emotet」の感染活動において、顧客等とやり取りされた本物のメールを基にした偽メールを用いる手口が使われており(AUS便り 2019/12/09号参照)、決して今回のニュースを対岸の火事などと油断することなく、社内外との安全なメールのやり取りに関して何らかの取り決めを設定すべきでしょう。


楽天、役員名乗る人物に情報漏えい　「指示が具体的で本人だと思った」

[谷井将人，ITmedia]

楽天の社員が、同社の役員を名乗る人物から個人情報を求める電話を受け、社員の氏名や役職、メールアドレスなどを流出させていたと、西日本新聞が12月3日に報じた。すでに警察に相談しており、社内では再発防止に向け注意喚起や教育を行っているという。

楽天のWebサイトより

●「Chrome 79」に流出したパスワード使用時の警告機能が搭載

https://www.itmedia.co.jp/news/articles/1912/11/news058.html

このニュースをザックリ言うと･･･

- 12月10日(現地時間)、Googleより、同社のWebブラウザー「Chrome」のバージョン79がリリースされました。

- 同社は、流出したユーザー名・パスワードの使用時に警告を出す拡張機能「Password Checkup」を2月に公開しており、今回これがChromeに統合されたとのことです。

- この他、アンチフィッシング機能「セーフブラウジング」について、フィッシングサイト情報をリアルタイムで参照する機能が追加される等、各種セキュリティ機能も強化されています。

AUS便りからの所感等

- Password CheckupはChromeにユーザーが記憶しているパスワードを自動的にチェックするもので、Googleでは利用者の1.5%に対し流出が確認されたパスワードの使用を警告したとする実績を発表しています(AUS便り 2019/8/26号参照)。

- またFirefoxも、流出したメールアドレス・パスワードを確認できるWebサイト「Have I Been Pwned」と提携する形で同様の機能を提供しています(https://www.itmedia.co.jp/news/articles/1906/05/news069.html)。

- パスワード設定に関する鉄則としては「推測されにくいパスワードにする」「複数のサイトで同じパスワードを使い回さない」等がある一方、今一つ重要なこととして「流出が発覚した場合は即座に変更する」ことが挙げられており、ブラウザーが提供する警告機能を活用することにより、変更すべき事態の発生に速やかに気付くことが期待できるでしょう。


「Chrome 79」の安定版公開　フィッシング対策や37件の脆弱性修正など

[佐藤由紀子，ITmedia]

Googleは12月10日（現地時間）、Webブラウザ安定版のアップデートとなる「Chrome 79」（バージョン79.0.3945.79）をWindows、Mac、Linux向けに公開した。数日かけてローリングアウトしていく。Android版は数週間かかる見込み。

パスワード保護、フィッシング対策、使わないタブの再読み込み停止機能、複数のアカウント同期ユーザー向けUI改善、多数の脆弱性修正などが行われた。

パスワード保護の強化

2月に拡張機能としてリリースし、10月にGoogleアカウントの機能として組み込んだ「Password Checkup」をChromeに統合した（ローリングアウト中）。

この機能は、オンラインで漏えいしたパスワードを使っているWebサイトをユーザーに通知し、パスワードを変更するよう促すというものだ。

この機能をChromeで有効にするには、Chromeブラウザに Google アカウントでログインし、［設定］→［自動設定］→［パスワード］に新たに追加される「Check password safety（パスワードの安全性をチェックする）」という項目を有効にする。

パスワードを変更するよう促す通知