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。

●古いiPhone・iPadへのセキュリティアップデートがリリース

https://japan.zdnet.com/article/35192771/
https://support.apple.com/ja-jp/HT213428
https://www.jpcert.or.jp/newsflash/2022081801.html

このニュースをザックリ言うと･･･

- 8月31日(現地時間)、Appleより、iOS 12系のセキュリティアップデート12.5.6がリリースされました。
- iOS 12系は現行バージョンである15系にアップデートできないiPhone 5s・6・6 Plus、iPad Air・mini 2・mini 3およびiPod Touch(第6世代)が対象機種となっており、昨年9月以来約1年ぶりのリリースとなります。
- 8月18日リリースのiOS 15.6.1で修正されたWebKitコンポーネントの脆弱性(CVE-2022-32893)に12系でも対応するものとなっていますが、悪意のあるWebサイトの閲覧等により、機器を乗っ取られる恐れがあるとされ、アップデートが強く推奨されています。

AUS便りからの所感等

- iOS 15.6.1で修正された脆弱性は2件あり、macOSにおいてもこれらに対するセキュリティアップデートが出ています(ただしもう1件の脆弱性であるCVE-2022-32894はiOS 12の対象機種には影響しないとのことです)。
- WebKitはLinuxでも利用するツールがいくつかあり、CVE-2022-32893へのセキュリティアップデートがリリースされています。
- iOS 12系が最新となっている古い機種の他、秋にリリース予定のiOS 16でサポート対象外となるiPhone 6s・6s Plus・7・7 Plus・SE(第1世代)およびiPod Touch(第7世代)、同じくiPadOS 16で対象外になるiPad Air 2およびmini 4について、今後もセキュリティアップデートが提供されるかは未知数であり、これらを利用している場合は可能な限りiPhone 8・SE(第2世代)以降等に移行することも検討すべきでしょう。

ZDNet Japan

旧型「iPhone」「iPad」向けにセキュリティ更新、悪用されている脆弱性を修正

Liam Tung（Special to ZDNet.com）翻訳校正：編集部　2022-09-05 10:18

Appleは米国時間8月31日、「iPhone 5s」と「iPhone 6」「iPhone 6 Plus」「iPad Air」「iPad mini 2」「iPad mini 3」、そして「iPod touch」（第6世代）向けに「iOS 12.5.6」をリリースした。これは、「iOS 12」に存在する脆弱性に対処する重要なセキュリティアップデートだ。

iOS 12.5.6で対処されるのは、同社が8月中旬に「iOS 15.6.1」向けのアップデートで対処した2件の脆弱性のうちの1件であり、リモートコード実行（RCE）につながるものとなっている。

● 8月度フィッシング報告件数94,973件…前月度より減少も、今後も9万件台以上維持か

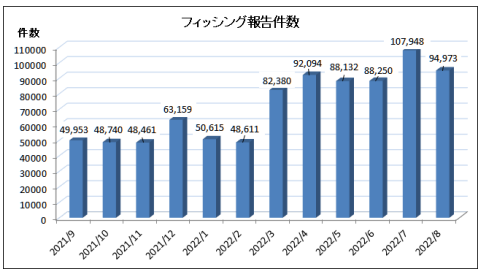
https://www.antiphishing.jp/report/monthly/202208.html

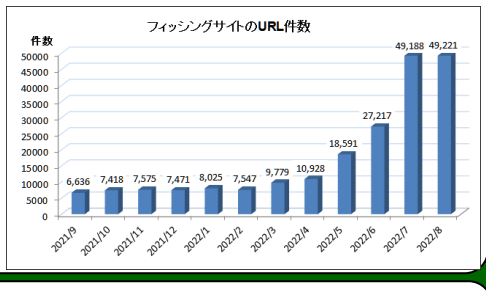
このニュースをザックリ言うと・・・

- 9月5日(日本時間)、フィッシング対策協議会より、8月に寄せられたフィッシング報告状況が発表されました。
- 8月度の報告件数は94,973件で、7月度(https://www.antiphishing.jp/report/monthly/202207.html)の107,948件から12,975件減少したものの、9万件台を維持しています。
- フィッシングサイトのURL件数は49,221件と、7月度(49,188件)から33件の微増ながら、過去最高を引き続き更新しています(ただしIPアドレスが同一のものが多いとされています)。
- フィッシングメールの発信元はCN(中国)の通信事業者が約91.9%、次いで日本国内からが約3.9%だったとのことです。

AUS便りからの所感

フィッシング対策協議会 Council of Anti-Phishing Japan





- 初めて10万件を突破した前月度から一転して9万件台に立ち戻ったものの、過去の傾向から、以後も9万件前後あるいはそれ以上の水準を維持し続ける可能性が高いとみられます。
- 同協議会が6月に緊急情報を出していた「クレジットカードの利用確認を装うフィッシング」が引き続き報告数全体の約32.4%を占めるほか、8月については国税庁を騙るフィッシング(AUS便り 2022/08/23号参照)についても多く報告を受けたとしています。
- 同協議会では、現時点で大量のフィッシングメールを受信している利用者に対し、正規メールにアイコンが表示される(BIMI)等フィッシング対策機能が強化されているメールサービスへの切り替えも呼び掛けており、例えばプライベートで利用している、ISPが提供するメールサービスが貧弱なものであるならば、大手Webメールサービスへの移行は有用でしょう。
- 一方、企業が提供するメールサーバーにおいてフィッシング対策機能が不十分な場合、個人で契約しているWebメールサービスにメールを転送し、これが第三者へ流出するリスクが発生する可能性があるため、単にこれを規制するのみならず、メールサーバーが十分な対策機能を実装するか、企業側でメールサービスを正式に契約することも視野に入れるべきです。

●サーバーの契約終了時に移行漏れ…14万件の個人情報が誤消去

https://www.itmedia.co.jp/news/articles/2209/05/news161.html
https://www.monogatari.co.jp/wp-content/uploads/2022/09/kojinjyohou.pdf

このニュースをザックリ言うと・・・

- 9月5日(日本時間)、飲食チェーン店「焼肉きんぐ」等の運営元の物語コーポレーション(以下・同社)より、同社顧客の個人情報を誤って消去したと発表されました。
- 発表によれば、誤消去された個人情報は、同社グループ各店の顧客のべ143,876件(氏名・住所・電話番号・生年月日・性別・メールアドレス)で、サービスや誕生日キャンペーン等の案内DM送付のために保持されていたとのことです。
- 個人情報を保存していたサーバーの契約が2022年6月に終了となったことで情報が消去されたとしており、外部への流出および不正利用は確認されていないとのことです。

AUS便りからの所感

ITmedia NEWS

- 対象となる個人情報を保存していたのは外部事業者のサーバー上で、6月の契約終了の際に別の外部事業者のサーバーへデータを移行していたものの、同社側での確認不足により、移行が行われなかったデータが消去されたことが8月5日に判明したとのことです。
- 自社が顧客の個人情報をどこに預けているかや、関連する契約等について確実に把握することはもちろん、個人情報に関連しない場面においても、サーバーや外部業者との契約やサービス自体の終了等で重要なデータが消失してしまうことは、少なくとも可用性・完全性の毀損に繋がり得るものと心得、くれぐれも契約の更新や、他のサービス・サーバーへのデータの移行漏れが発生しない体制を整えることが肝要です。

14万件の個人情報を誤削除、復旧できず　「焼肉きんぐ」運営元がサーバ移行でミス

2022年09月05日 19時14分 公開　[吉川大貴，ITmedia]

飲食チェーン「焼肉きんぐ」などを運営する物語コーポレーション（愛知県豊橋市）は9月5日、顧客の個人情報14万3876件を誤って削除し、復旧できない状態だと発表した。サーバ移行時の確認不足によりデータを移行し損ね、そのまま古いサーバの契約期間が終了したという。削除した情報の漏えいは確認していない。

誤って削除した情報は、焼肉きんぐに加え「お好み焼き本舗」「焼肉かるびとはらみ」など計6ブランドのチェーン店に来店したことがある顧客の氏名、住所、電話番号、生年月日、性別、メールアドレス。いずれも、誕生日の顧客にサービスやキャンペーンを告知する目的で保存していたという。