

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。

●全尼崎市民46万人の個人情報収めたUSBメモリー、一時紛失

<https://www.itmedia.co.jp/news/articles/2206/23/news142.html>
<https://www.kobe-np.co.jp/news/sougou/202206/0015410231.shtml>
<https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html>



このニュースをザックリ言うと…

- 6月23日(日本時間)、兵庫県尼崎市より、同市全市民分の個人情報等を記録したUSBメモリーが紛失したと発表されました。
- USBメモリーに保存されていたのは、同市民460,517人分の住民基本台帳の情報(統一コード、氏名、住所、生年月日、性別等)の他、住民税に係る税情報360,573件、2021年度・2022年度分の特例給付金の対象世帯情報のべ82,716世帯分および生活保護・児童手当受給世帯のべ86,026件分とのことでした。
- 同市から委託を受けていたBIPROGY社(以下B社)の協力会社の社員(後日協力会社からの再委託先の社員と発表あり)が業務のためデータをUSBメモリーに保存した後、それをかばんに入れたままB社社員らと飲食し、泥酔してかばんとともに紛失したとされています。
- USBメモリーのデータは暗号化されパスワードがかかっており、後かばんとともに発見されたことが同24日に発表されています。

AUS便りからの所感等

- B社が協力会社に依頼してデータを持ち出させた時点で市に必要な許可をとっておらず(データ処理に関する許可はとっていたものの、USBメモリーに保存することについての許可は得ていなかったともされています)、実際には協力会社のさらに再委託先が関与していたこと、USBメモリーの扱いについても、正副2本の両方を持ち歩いてきた・データをすぐに消去しなかった(強力なパスワードで暗号化されている限り直ちに問題とはならないでしょうが、パスワードのヒントとなり得るような情報が記者会見で明かされたともされています)等、多数の問題点が指摘される事案となっています。
- USBメモリーについて、紛失やそれ以前にUSBメモリーにデータを保存することが可能な設定であることのセキュリティリスク、あるいはマルウェアを拡散させる手段として攻撃者に悪用される場面も多いことは長年指摘されており、さらには業務上データの持ち出しにUSBメモリーを必要とするような周辺環境の事情(オンラインでデータの転送等ができない等)が逆説的にセキュリティリスクの増大を招いているといった指摘もなされ、(USB接続によるストレージ全般を含め)使用を停止する企業も出ているという状況です。
- ともあれ今回のような事案においてどのような問題があったかを挙げ、それぞれがあらゆる条件のもとで問題となり得るか、周辺の状況次第でカバーし得るものだったか、どういった策によって解決・回避し得るかの分析が行われることにより、企業・組織においてとられるべきセキュリティ対策が改めて意識されることを願いたいものです。



尼崎市、全市民46万人分の個人情報入りUSB紛失 委託先関係社員が飲食店でなくしたか

© 2022年06月23日 13時00分公開

[ITmedia]

兵庫県尼崎市は6月23日、臨時特別給付金の支給事務にあたった委託先「BIPROGY関西支社」(大阪市)の関係社員が、全市民46万人分の個人情報が入ったUSBメモリを紛失したとして謝罪した。USBメモリにはパスワードと暗号化をかけており、23日時点で情報の漏えいは確認されていないとしている。



●カード各社等を騙るフィッシング同時多発か…対策協議会が注意喚起

https://www.antiphishing.jp/news/alert/creditcard_20220624.html



このニュースをザックリ言うと…

- 6月24日(日本時間)、**フィッシング対策協議会**より、**多数のクレジットカード会社やキャッシュレス決済事業者を騙るフィッシングが確認**されたとして注意喚起が出されています。
- 挙げられているフィッシングメールは、**件名に「カード年会費のお支払い方法に問題があります」**や「**お支払い金額確定のご案内**」「**ご利用確認のお願い**」等と記載され、**利用確認のためのページを騙り、カード情報や個人情報を詐取る偽サイトへリンク**するものとなっています。
- 対象に挙げられているブランドは**JCB・Visa・Mastercard・イオンカード・三井住友カード**および**au PAY**となっており、**その他のブランドが無用されている可能性も示唆**されています。

AUS便りからの所感

- 提示されている**フィッシングサイトのURL**(ドメイン名部分は一部マスク)は、**パス部分がランダムな文字列**ながらも**一定のもの**となっており、**同一のサイバー犯罪組織による可能性**、また今後も別のブランドを騙るものが発生する**可能性は十分に考えられます**。
- **対策協議会や各セキュリティ団体などが随時挙げている対策**として、利用している各サービスの**公式サイトには事前に登録したブックマークからアクセス**すること、また不審なメールやSMSについては**Web上の報告や注意喚起がないか**、メールの**文面の一部等で検索して確認**することを常日頃心掛けるようにし、また**メーラー・Webブラウザあるいはアンチウイルス・UTMのアンチフィッシング機能**などを必ず有効にすることにより、フィッシングに引っかからないよう**幾重もの防衛策をとることが重要**です。



●Windows 8.1、2023/1/10にサポート終了…有償延長サポートはなし

https://japan.zdnet.com/article/35189433/
https://news.mynavi.jp/techplus/article/20220627-2379780/
https://support.microsoft.com/ja-jp/windows/3cfd4cde-f611-496a-8057-923fba401e93



このニュースをザックリ言うと…

- 6月25日(日本時間)、**Windows 8.1のサポート終了**となる**2023年1月10日まで200日**となり、一部ネットメディアで取り上げられています。
- マイクロソフト(以下MS)では**7月以降**、当該OSを使用する**PC上でサポート終了に関する通知を表示**するとしています。
- 一方で、Windows 7で提供している**有償サポート「拡張セキュリティ更新プログラム(ESU)」を8.1では提供しない**としており、後継である**Windows 10または11へのアップグレード**が推奨されています。

AUS便りからの所感



- 7からのインターフェース面での大きな変化等から8.1への移行は速やかに進まず、10リリースの時点でも7の方がシェアが多かったとされたことから、8.1については**有償サポートが公式に用意されなかったとみられます**。
- なお、**Windows 8**については**2016年にサポートが終了**しており、万が一8を使い続けている場合、**8.1へアップグレード(無償で可能)しない限りセキュリティアップデートは受け取れません**。
- 8と8.1をベースにした**Windows Server 2012**および**2012 R2**についても**2023年10月にサポート終了**となります(2012からR2への無償アップグレードはありません)ので、**こちらも併せてアップグレードを意識し計画**することが肝要です。



今もまだ「Windows 8.1」を使用しているというユーザーは、少ないだろう。しかし、使用しているユーザーは、Windows 8.1のサポートが2023年1月10日で終了することを覚えておく必要がある。

Microsoftは、Windows 8.1ユーザーに周知させるために、7月からサポート終了日についての通知を開始する。会社によると、通知が表示されたユーザーは、「Learn more (詳細について)」「Remind me later (後で通知)」「Remind me after the end-of-support date (サポート終了後に通知)」のいずれかを、2023年1月までクリックできる。会社はこれまで、旧バージョンのWindowsユーザーに、より新しいサポート対象となっているバージョンへのアップグレードを呼びかける際に、こうした通知を行ってきた(ちなみにこれまでは、ドメインに参加しているPCの場合は、アップグレードを促されていなかったようだ)。