— AUS（アルテミス・ユーザ・サポート）便り 2017/08/28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。

●HISから最大11,975人分の個人情報流出

https://www.nikkei.com/article/DGXMZO20241860S7A820C1000000/
http://www.itmedia.co.jp/news/articles/1708/22/news093.html

このニュースをザックリ言うと･･･

- 8月22日（日本時間）、大手旅行業者のエイチ・アイ・エス（HIS）社より、同社が運営する国内バスツアーの予約サイトが不正アクセスを受け、個人情報が流出したと発表されました。

- 発表によれば、流出した個人情報は、3月18日16:03～7月27日17:30の間に予約を行った利用者11,975人分の氏名・メールアドレス・住所・電話番号等とされています（クレジットカード番号および金融機関口座情報は含まれていないとのことです）。

- 流出は17日に判明したもので、予約サイトのリニューアルによるデータ移行の際、誤って個人情報を含む予約データファイルをサイトの「公開領域」に残していたことが原因とされています。

AUS便りからの所感等

- 旅行業者からの個人情報流出事件としては、昨年JTBが大規模な被害を受けたもの（AUS便り2016/06/20号参照）が挙げられますが、今回は攻撃者の周到な準備やシステムの脆弱性といったものではなく、オペレーションミスを突かれたものようです。

- 先週のAUS便り（2017/08/21号）では、Webサイト上にデータベースのダンプファイルが残されているケースが多発しているとJPCERT/CCが8月8日にも警告を出していた件を取り上げていますが、状況的に似通ったものとなっているのがやはり気になるところです。

- 先週の繰り返しとなりますが、Webサイトのドキュメントルート以下のような外部からアクセスされる可能性のある場所に機密情報ファイルを置く構成にしないこと、また何らかの作業時にもそういったディレクトリに一時的にでもファイルを置くことはなるべく避けることが重要です。

日本経済新聞

HISで情報漏洩、バスツアー客の予約情報が流出

2017/8/23 6:00

共有 保存 印刷 その他

ITpro

エイチ・アイ・エス（HIS）は2017年8月22日、首都圏を出発地とする国内バスツアーの予約サイトで旅行を申し込んだ顧客の個人情報が外部からのアクセスにより流出したと発表した。流出した情報にクレジットカード番号や金融機関の口座情報は含まれていないという。

2017年3月18日16時3分～2017年7月27日17時30分になされた予約のうち、2017年8月1日～2017年12月31日に首都圏を出発する国内バスツアーを選んだ顧客の個人情報が流出した。予約代表者の氏名、性別、年齢、メールアドレス、住所、電話番号などが最大4566人分、同行者の情報は同7017人分が流出した。

流出は2017年8月17日に判明。同社はセキュリティーに関する情報収集を社外の専門家に依頼しており、外部のWebサイトにおいて予約サイトの情報流出を示唆する記述があったと報告を受けた。これを元に社内調査を実施したところ、外部から顧客の個人情報を含む圧縮ファイルをダウンロードした形跡が見つかった。

同社は予約サイトをリニューアルする作業に原因があったと見ている。旧サイトから顧客の予約データを移行する際、誤って公開領域に同データを残したという。同社は情報が流出した顧客に対して電子メールによる周知を実施済み。運営する他のオンライン予約サイトには影響がないという。

（日経コンピュータ 斉藤壮司）

ITmedia NEWS

速報 2017年08月22日 14時55分 公開

HIS、最大1万人超の個人情報流出　バスツアー予約サイトから

HISが、最大1万1975人分の個人情報が流出したと発表。首都圏出発のバスツアーの予約サイトをリニューアルする際、外部からアクセスできる場所に個人情報を誤って保存していた。

[ITmedia]

印刷／PDF 204 ツイート 78 いいね！ 78 シェア 13 B! Bookmark 21 Pocket G+ 通知

PR 「現代の魔法使い」落合陽一氏が語る「超AI時代の生存戦略」

エイチ・ア…
スを受け、最…
時に、旧サイ…
保存していた…

意図しないアクセスを受けたのは、首都圏を出発地とするバスツアーの予約サイト。2017年3月18日～7月27日に、8月1日～12月31日出発のツアーを申し込んだユーザーの個人情報が流出したという。

流出したとされるのは、ツアーを申し込んだ代表者（最大4566人分）の氏名や住所、性別、年齢、電話番号、メールアドレス、ツアー名、出発日。

さらに同行者（最大7017人分）の氏名、性別、年齢、電話番号、ツアー名、出発日、加えて緊急連絡先（最大392人分）の氏名、電話番号も漏えいしたという。クレジットカード番号、金融機関口座情報は一切含まれないとしている。

17日、同社が契約する外部セキュリティ専門家から報告を受け、社内調査を開始。第三者からのアクセスとファイルダウンロードの形跡を確認したという。同社の他の予約サイトは、被害を受けたサイトとは分離したシステムで運営しており、トラブルの影響はないとしている。

すでに観光庁、個人情報保護委員会、日本旅行業協会、プライバシーマーク制度を運用する日本情報経済社会推進協会（JIPDEC）、新宿警察署などに報告済みという。

対象のツアー代表者には22日にメールで連絡し、専用相談窓口（電話番号は0120-447-583）も設ける。再発防止のために、第三者機関によるセキュリティ診断や、内部チェック体制を強化するほか、スタッフへの啓蒙を行うとしている。

●7月のフィッシング報告件数は579件…Appleをかたるものと短縮URL悪用に注意

http://securityblog.jp/news/20170809.html
http://www.antiphishing.jp/report/monthly/201707.html

このニュースをザックリ言うと・・・

- 8月1日（日本時間）、フィッシング対策協議会より、7月に同協議会に寄せられたフィッシングの報告状況が発表されました。

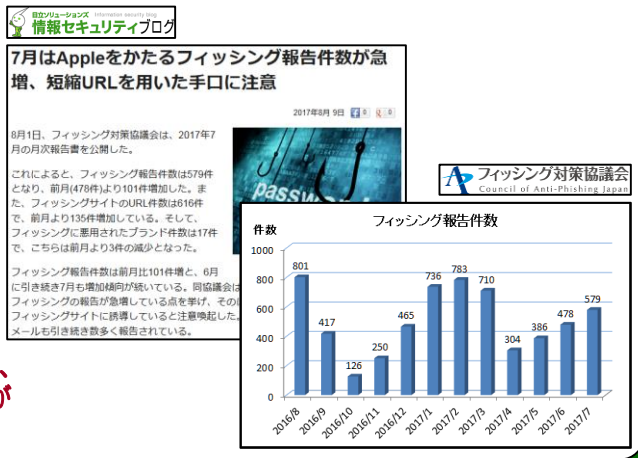
- 7月の報告件数は579件で、6月（478件）より101件の増加となっています。

- 4月以降月間の報告件数が80～100件ずつ増加していることについて、同協議会では理由の一つとして、Appleをかたるフィッシングの報告が増加していることを挙げており、またその殆どが短縮URLを利用してフィッシングサイトへ誘導していることを警告しています。

AUS便りからの所感等

- 長いURLをメール等で共有する際等に用いられる短縮URLですが、大抵は「不特定多数のユーザ」が「任意のURLを短縮できる」ことから、悪用の可能性は常にあるものと心得て、「信頼できる相手が短縮したURL」か「特定のサイトのURLのみ短縮できるサービス」でない限りは十分注意しましょう。

- 短縮URLからのフィッシングサイトへの誘導であっても可能な限り食い止められるよう、ブラウザやアンチウイルス、あるいはUTMのアンチフィッシング機能を有効にすることが肝要です。



●PlayStationのTwitter&Facebookアカウントがハッキングされる

http://jp.automaton.am/articles/newsjp/20170821-52790/

このニュースをザックリ言うと・・・

- 8月20日頃（現地時間）、PlayStation公式のTwitterおよびFacebookアカウントがハッカー集団によるとみられる乗っ取りを受け、不正な投稿などが行われる事態が発生しました。

- 乗っ取られたのはPlayStationのアメリカおよびブラジル版の公式Twitterアカウント、およびFacebookアカウントで、乗っ取りを行ったハッカー集団による「PlayStationネットワークのデータベースをリークさせた」という犯行宣言とみられる投稿がされていました。

- 現在SNSアカウントは全て復旧し、該当する投稿も削除されており、また漏洩したデータベースの内容が外部で確認された様子もまだない模様です。

AUS便りからの所感等

- 乗っ取りによる投稿で「OurMine」を名乗ったハッカー集団は、以前から有名人や作品の公式アカウントへのハッキングを仕掛けてきている一方、「ホワイトハットハッカー(善意のハッカー)」「セキュリティグループ」を自称しています。

- 今回の事件においても、SNSアカウントのみの乗っ取りであり、実際にデータベースの漏洩が発生した可能性は低いと見られています。

- SNSアカウントから不正な投稿が行われた場合、アカウントそのものが不正ログインされたケースと、連携していたアプリの中に悪意を持ったものがあり、それが投稿を行ったケースとが考えられますが、特に後者について、不正なアプリはユーザのPCやネットワークの外部で動くものもあり、アンチウイルスやUTMで防げるものではありませんので、ネット上の評判等をもとに必要最低限のアプリと連携するよう心がけるようにしましょう。