— AUS（アルテミス・ユーザ・サポート）便り 2017/03/06号 —
http://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。

●サイバー攻撃で個人情報流出1260万件　昨年、国内93組織

https://this.kiji.is/208894271421464579?c=395467418394624O1
http://www.chunichi.co.jp/article/front/list/CK2017022802000081.html

このニュースをザックリ言うと・・・

- 2月28日（日本時間）、共同通信より、2016年にサイバー攻撃を受けたことを公表した国内の企業や行政機関の93組織から流出、または流出した恐れがある個人情報などが少なくとも1260万件に上るという取材結果が発表されました。

- これは2015年の207万件から約6倍となり、最も多かったのはJTB（AUS便り 2016/06/20号参照）からの約679万件（※当初発表の約793万件から重複を除外）、次いでパイプドビッツ（同2016/06/27号参照）の98万件（※攻撃を受けた同社システムを使っていた複数のサイトからのもの）、J-WAVE（同2016/05/02号参照）からの64万件等となっています。

AUS便りからの所感等

- 2016年はJTBの事件だけで2015年における全体の件数の実に3.2倍となる個人情報流出が発生していましたことになります。

- その2015年には日本年金機構から125万件、また（サイバー攻撃というよりは内部関係者による犯行によるものですが）2014年にもベネッセから約3000万件が流出しています。

- ここ数年は毎年のように大規模な組織からの突出した流出事件が発生し、それが殊に語られることもありますが、それ以外にもあちこちで流出事件は発生しており、決して中小零細企業であっても対岸の火事と見なすべきではありません。

- それぞれの流出事件において、どういった攻撃によって発生したかなど、個人情報保護のための各種対策においてぜひとも参考としてほしいものです。

共同通信 47NEWS

個人情報流出1260万件

16年のサイバー被害集計

2017/2/27 19:33

サイバー攻撃被害を2016年に公表した国内の企業や行政機関の93組織から流出、または流出した恐れがある個人情報などが少なくとも1260万件に上ることが27日、共同通信の取材で分かった。JTBからの大量情報流出もあり、15年の207万件に比べて約6倍に急増した。

一部重複もあるが単純計算では人口の約10分の1の規模に当たり、情報流出がネット利用者の身近な脅威となっている実情が浮かんだ。クレジットカード情報が多く流出したことも判明。サイバー犯罪者が金銭目的でカード情報を狙っているとみられる。サイバー攻撃との関連が疑われるカード不正使用も増加している。

中日新聞 CHUNICHI Web

ツイート B! 0 シェア 22 G+1 0

2017年2月28日　朝刊

サイバー攻撃で個人情報流出1260万件　昨年、国内93組織

サイバー攻撃被害を二〇一六年に公表した国内の企業や行政機関の九十三組織から流出、または流出した恐れがある個人情報などが少なくとも千二百六十万件に上ることが、共同通信の取材で分かった。ＪＴＢからの大量情報流出もあり、一五年の二百七万件に比べて約六倍に急増した。

一部重複もあるが単純計算では人口の約十分の一の規模に当たり、情報流出がネット利用者の身近な脅威となっている実情が浮かんだ。クレジットカード情報が多く流出したことも判明。サイバー犯罪者が金銭目的でカード情報を狙っているとみられる。サイバー攻撃との関連が疑われるカード不正使用も増加し、深刻化している。

公式サイトや公表情報を基に取材し、各組織から詳しい状況を聞いた。内訳は、民間企業の関連が六十五、行政が十七、学校が十一。公表された事例のほとんどは個人情報関連だった。

件数が最多だったのはＪＴＢが昨年六月に発表した約六百七十九万件。ネット予約した客の氏名とパスポート番号などが流出した可能性がある。次いでＩＴ関連会社のパイプドビッツ（東京）が約九十八万件、ラジオ局Ｊ－ＷＡＶＥ（同）が約六十四万件などとなった。

資生堂は約四十二万件が流出。うち約六万六千件はカード情報を含んでいた。江崎グリコは約八万三千件で、約四万四千件にカード情報があった。ともにネット通販を一時中止した。カード裏面に書かれた「セキュリティーコード」まで漏れた例もあった。

日本クレジット協会によると、一六年一～九月のカードの不正使用被害額は前年同期比２５・２％増の百六億円。サイバー攻撃との関連が疑われる「番号盗用」の被害が急増した。

●「MyJCB」をかたるフィッシングメール出回る

http://internet.watch.impress.co.jp/docs/news/1045149.html

このニュースをザックリ言うと・・・

- 2月20日（日本時間）、フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会より、JCBカードのWebサービス「MyJCB」をかたるフィッシングメールが出回っているとして警告が出されています。

- フィッシングメールの件名は「【重要：必ずお読みください】 MyJCB ご登録確認 ●●●●」となっており、「MyJCBへの第三者によるアクセスを確認した」として、「http://www.myjcb●●●●.com/」というURLのフィッシングサイトへと誘導するものとなっています。

- 同協議会では、発表の時点でフィッシングサイトが稼働中として、サイト閉鎖のための調査をJPCERT/CCに依頼するとともに、今後類似したサイトが公開される恐れがあるとしており、こういったサイトでアカウント情報を絶対に入力しないよう、また同様のサイトやメールを見かけた場合は協議会へ連絡するよう呼び掛けています。

AUS便りからの所感等

- MyJCBの本物のサイトは「https://my.jcb.co.jp/」ですが、フィッシングサイトの方はHTTPSを用いていない等、見分けられるポイントはいくつか存在しています。

- 1月末に同協議会から警告が出された「OFFICEのプロダクトキーが不正コピーされています」という件名のフィッシングメール（AUS便り 2017/02/06号参照）も再び活発となっています。

- このようなフィッシングの話題では何度も申し上げていることですが、誤ってフィッシングサイトに誘導された場合にもアドレスバーを確認の上、慎重に行動するようにし、また、アンチウイルス・UTMあるいはブラウザのアンチフィッシング機能を必ず有効化し、普段利用するサービスへはブラウザのブックマークからアクセスするようにしましょう。

INTERNET Watch

カード情報を窃取、MyJCBをかたるフィッシングメール出回る、フィッシング対策協議会が注意喚起

岩崎 宰守　2017年2月20日 13:35

MyJCBをかたるフィッシングメールが出回っているとして、フィッシング対策協議会が20日、注意を呼び掛ける緊急情報を出した。誘導先となっている偽サイトは、同日12時現在も稼働中で、フィッシング対策協議会では、クレジットカード情報などを絶対に入力しないよう注意を呼び掛けている。

MyJCBをかたるフィッシングメールの件名は「【重要：必ずお読みください】MyJCB ご登録確認 xxxx」。第三者によるアクセスを確認したとして、登録IDを暫定的に変更したため、ウェブサイトへアクセスして任意のIDへの再変更を促すもの。

●研究室・サークルなどの“放置サイト”一掃に向け集中管理を

http://internet.watch.impress.co.jp/docs/news/1046522.html

このニュースをザックリ言うと・・・

- 2月27日（日本時間）、独立行政法人情報処理推進機構（IPA）より、大学等の学術組織に対し、所属する研究室やサークル等が独自に開設・運営するWebサイトの改ざん被害について注意喚起が出されました。

- 学術組織におけるこういった独自のWebサイトは、管理していた学生や教員の卒業・異動によって管理者が不在になる等により、役割が終了しても閉鎖されないことが多く、組織側でもセキュリティ対策の実施体制が不十分で、個々のサイトを確実に把握・管理できていない傾向にあることが改ざんを招いている主な原因としています。

- IPAでは、サイトにおけるソフトウェアの更新やセキュリティ更新を組織のシステム管理部門による集中管理とすること、公開しているページにセキュリティ上の問題が確認された場合には管理部門が公開停止等をできるよう周知しておくこと、アンケート実施により組織内のWebサイトの情報収集を行うこと、等を推奨しています。

AUS便りからの所感等

- サイトの改ざんは既に愉快犯のためだけの行為ではなく、例えばトップページなどではない「http://server/test.html」といった本来存在しないURL上に、密かにマルウェア等の不正なコンテンツをアップロードするケースも珍しくありませんし、こういった攻撃では、放置されたホストが格好のターゲットとなることでしょう。

- システム管理部門が組織内にある各種サーバ・クライアントの存在を把握しておくこと、そして放置されたホストがマルウェアの巣などにならないようセキュリティ対策を行い、時にはホスト自体の停止を行うことは、学術組織のみならず、中小を含む一般企業等においても重要なことです。

INTERNET Watch

研究室・サークルなどの“放置サイト”一掃に向け集中管理を、学術組織を狙ったサイト改ざん多発

磯谷 智仁　2017年2月27日 15:44

独立行政法人情報処理推進機構（IPA）は27日、研究室やサークルが独自に開設・運営するウェブサイトの改ざん被害を抑えるため、学術組織に対して注意喚起を行った。

研究室やサークルの独自ウェブサイトはその役割が終了した場合でも、閉鎖されないことがある。一方、組織側では個々のウェブサイトの把握・管理ができておらず、多くの学術組織において、セキュリティ対策が不十分なウェブサイトが相当数放置されたままになる。これがウェブサイト改ざんを招く主な原因となっている。

これは、学術組織ではウェブサイトの管理が学生や在籍期間が限定されている教員に委ねられることに関係してくる。卒業や異動などで担当者が不在になると、ウェブサイトの管理が継承されず、セキュリティ対策が厳かなウェブサイトが放置されることになる。

学術組織では、研究単位の情報だけでなく、企業との共同研究などの知的財産など貴重な情報を保有する。そのため、ウェブサイトの改ざんを契機に、情報漏えいが一度発生すると関係組織へのダメージが大きくなり、組織への評判に悪影響を及ぼす。