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。

●文科省の閉鎖済みサイトのドメインがオークションに

https://tech.nikkeibp.co.jp/atcl/nxt/news/18/04366/
https://www.jiji.com/jc/article?k=2019030700899&g=soc

このニュースをザックリ言うと･･･

- 3月7日（日本時間）、時事通信より、文部科学省が2012年度～2016年度に実施した「大学間連携共同教育推進事業」に関するサイトのドメインについて、ドメイン業者のオークションに出品されていたと報じられました。

- 出品されていたドメインは同事業の支援先大学等を紹介するポータルサイトのもので、事業終了後もサイトが残っていましたが、今年1月にドメインが失効していたとのことです。

- 今後事業とは関係ないWebサイトや文科省をかたる偽サイト等が立ち上がる可能性が考えられ、文科省では参加していた大学等にリンクの削除を依頼しているとのことです。

- なお、当該ドメインは同14日には第三者とみられる者に落札された模様です。

AUS便りからの所感等

- 今回のような経緯でイベント等のための独自ドメインが失効し第三者に取得されたケースとしては、2015年に内閣府が開催したシンポジウムのサイトについて（AUS便り 2018/05/14号参照）等が挙げられます。

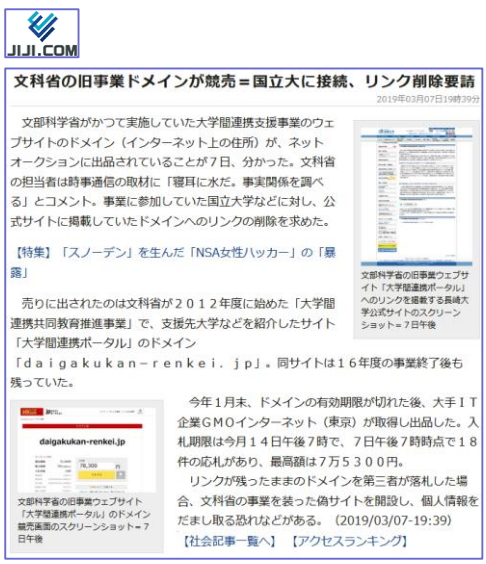
- 政府の各府省情報化統括責任者（CIO）連絡会議では「Webサイトドメイン管理ガイドライン」を定め、政府機関が公開するドメイン一覧も作成しています（https://cio.go.jp/node/2323）が、今回のケースはガイドラインの対象外となっていた模様です。

- このような問題は政府機関・自治体系のサイトに限ったものではなく、大手シネコンが名称変更の際に放棄した古いドメインが失効後に第三者に取得され、シネコン側が古いドメインへのアクセスを行わないよう呼び掛けたこともあります。

- 企業のブランド等のために独自ドメインを取得することは後々今回のようなケースが発生するリスクをはらんでいることに注意し、可能な限り企業ドメインのサブドメイン等を用いる、サイトの閉鎖時にはサイト上での告知や関係各所への通知を十分に行う、閉鎖後も数年以上はドメインを維持する、等を検討すべきでしょう。


日経 XTECH

2019/03/08 19:30
ニュース
文科省の「大学間連携支援事業」サイトの旧ドメインが競売に、大学などにリンク削除を要請
大豆生田 崇志＝日経 xTECH／日経コンピュータ、齊藤 貴之＝日経 xTECH／日経NETWORK
日経 XTECH
この記事を評価する
この記事は ○仕事に役立った 0 ○人に勧めたい 0 ○難しい 0 ○易しい 0
文部科学省が実施していた大学間連携支援事業の旧Webサイトのドメインが GMOインターネットのオークションに出品されていることが2019年3月8日までに分かった。文科省は「参加していた大学などにドメインへのリンクを削除してもらっている」と話す。
ドメイン名
daigakukan-renkei.jp
78,300 円
入札する


JIJI.COM

文科省の旧事業ドメインが競売＝国立大に接続、リンク削除要請
2019年03月07日19時39分
文部科学省がかつて実施していた大学間連携支援事業のウェブサイトのドメイン（インターネット上の住所）が、ネットオークションに出品されていることが7日、分かった。文科省の担当者は時事通信の取材に「寝耳に水だ。事実関係を調べる」とコメント。事業に参加していた国立大学などに対し、公式サイトに掲載していたドメインへのリンクの削除を求めた。
【特集】「スノーデン」を生んだ「NSA女性ハッカー」の「暴露」
売りに出されたのは文科省が２０１２年度に始めた「大学間連携共同教育推進事業」で、支援先大学などを紹介したサイト「大学間連携ポータル」のドメイン「ｄａｉｇａｋｕｋａｎ－ｒｅｎｋｅｉ．ｊｐ」。同サイトは１６年度の事業終了後も残っていた。
今年1月末、ドメインの有効期限が切れた後、大手ＩＴ企業ＧＭＯインターネット（東京）が取得し出品した。入札期限は今月１４日午後７時で、７日午後７時時点で１８件の応札があり、最高額は７万５３００円。
リンクが残ったままのドメインを第三者が落札した場合、文科省の事業を装った偽サイトを開設し、個人情報をだまし取る恐れなどがある。（2019/03/07-19:39）
【社会記事一覧へ】【アクセスランキング】

●iCloudをかたるフィッシングメール…JC3が警告

https://www.itmedia.co.jp/news/articles/1903/08/news089.html

このニュースをザックリ言うと・・・

- 3月7日（日本時間）および9日、日本サイバー犯罪対策センター（JC3）より、Appleをかたり偽のiCloudサイトへ誘導す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。

- メールは、件名が「警告！！パスワードの入力は数回間違いました。」、本文には「お客様はウェブサイトでAppleにログインした時にパスワードの入力は数回間違いました」「最近iCloudへサインインを行ったことがなく、他者が違法にお客様のアカウントを使用していると考えられる場合は、確認を完了するにはここをクリック」等と記載されているとのことです。

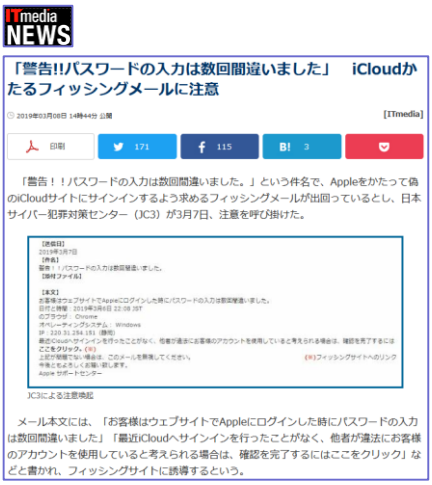
- JC3では、このようなメールのリンクをクリックしないよう呼び掛けています。

AUS便りからの所感等

- JC3からは、以後もamazonをかたるフィッシングメールや「電子メールとデバイスをクラックした」という脅迫メール等について警告が出ています。

- これまでJC3が注意喚起を出したメールの一覧がサイト（https://www.jc3.or.jp/topics/vm_index.html）に上がっていますので、不審な日本語のメールはこのページで件名を検索することが有用でしょう。

- これ以外にもフィッシングやマルウェアメールからの防御を徹底するため、PCのアンチウイルスソフトやブラウザのセキュリティ機能は必ず有効にし、加えてUTMの設置等、各種防衛策を複数実施することが重要です。


ITmedia NEWS

「警告!!パスワードの入力は数回間違いました」 iCloudかたるフィッシングメールに注意

2019年03月08日 14時44分 公開 [ITmedia]

印刷 171 115 B! 3

「警告！！パスワードの入力は数回間違いました。」という件名で、Appleをかたって偽のiCloudサイトにサインインするよう求めるフィッシングメールが出回っているとし、日本サイバー犯罪対策センター（JC3）が3月7日、注意を呼び掛けた。

JC3による注意喚起

メール本文には、「お客様はウェブサイトでAppleにログインした時にパスワードの入力は数回間違いました」「最近iCloudへサインインを行ったことがなく、他者が違法にお客様のアカウントを使用していると考えられる場合は、確認を完了するにはここをクリック」などと書かれ、フィッシングサイトに誘導するという。

●メールマーケティング会社、個人情報20億件以上流出か

https://news.mynavi.jp/article/20190315-788144/

このニュースをザックリ言うと・・・

- 3月11日（現地時間）、セキュリティベンダーのESET社より、メールマーケティング会社Verifications.ioのサーバにおいて20億件を超えるデータが外部からアクセス可能な状態になっていたと発表されました。

- 同社が収集したメールアドレス・氏名・ソーシャルメディア（Facebook・Instagram・LinkedIn）のアカウント・電話番号・生年月日・郵便番号・クレジットスコア情報・住宅ローンの金額・企業の名前や収益等が対象となっています。

- 2月にこのデータを発見したセキュリティ研究者によれば、当初は1つのデータベースにおいて約8億8,000万件を確認、その後新たに3つのデータベースを発見し、最終的に20億7,000万件のデータを見つけたとのことです。

AUS便りからの所感等

- データにアクセス可能になっていた原因は、データベースソフトウェア「MongoDB」が使用するサービスポートにパスワード等のアクセス制限がかかっていなかったこととされています。

- 内部のデータベースを含め、不特定多数への公開を意図していないサービスへのリモートからのアクセスを遮断・制限するため、サーバ自身もしくはルータ・UTMのファイアウォール機能を設定した上で可能な限りパスワードをかけること、また、不正アクセスの有無やアクセス元の分析を確実かつ迅速に行うためにあらゆるアクセスについてログを取得することが重要となるでしょう。


マイナビニュース

2019/03/15 10:10:31

メールマーケティング会社から20億件のデータが漏洩

後藤大地

関連キーワード：情報漏えい

ESETは3月11日(米国時間)、「Over 2 billion records exposed by email marketing firm」において、Verifications.ioというメールマーケティング会社から20億件を超えるデータがインターネット経由で誰でもアクセスできる状態で置かれていたと伝えた。

メールアドレス、氏名、ソーシャルメディアアカウント、電話番号、生年月日、郵便番号、クレジットスコア情報、住宅ローンの金額、企業の名前や収益などがアクセス可能な状況にあったようだ。

データは保護されていないMongoDBサーバ上でデプロイされており、Diachenko氏が発見した時点で、8億8000万件を超えるデータにアクセスできる状態になっていたという。調査の結果、アクセス可能だったデータベースは1つではなく4つだったことがわかり、結果的に20億7000万件のデータがアクセス可能な状態になっていたとされている。

MongoDBのデータベースがインターネット経由でアクセス可能な状態になっていたためにデータが漏洩したケースはこれまでいくつも報告されている。データベースの設定にはくれぐれも気を付けたいものだ。