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。

●報道機関向けページでアクセス制限かけ忘れ…約1,000人分の個人情報、第三者が閲覧可能状態に

https://newsdig.tbs.co.jp/articles/-/545600?display=1
https://www.fnn.jp/articles/-/543356

このニュースをザックリ言うと･･･

- 6月15日(日本時間)、熊本県より、のべ955人分の個人情報を含んだ資料を掲載するWebページが誤って第三者に公開された状態にあったと発表されました。
- Webページは県から報道機関へ資料を提供するためのもので、資料には叙勲・褒章受賞者888人の住所、および取材の問合せ先67人分の名前・電話番号が掲載されていたとのことです。
- 当該Webページは2020年2月から提供され、この時点ではID・パスワードによるアクセス制限がかかっていましたが、同12月から2023年6月3日にかけて外部から閲覧可能な状態にあったとしています。
- 発表の時点でシステムは再構築されているとのことで、現在は対策されている模様です。

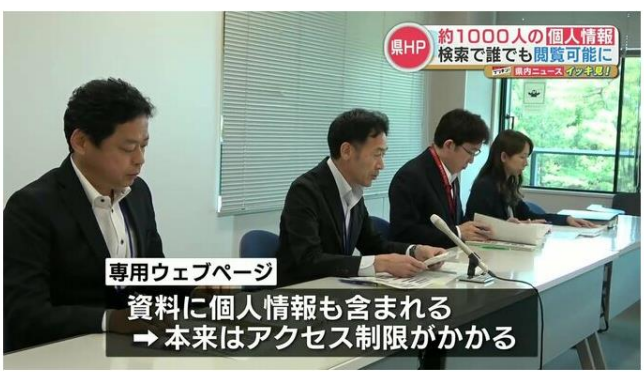
AUS便りからの所感等

- Webページが公開状態となったのは2020年12月に管理委託業者が変わった後とされ、サーチエンジンにも掲載される状態にあったようです。
- このような変更が発生したことについて、県では「ホームページの仕様で県のイメージと委託業者のイメージにズレがあったこと」等が原因としていますが、当初のアクセス制限が外されていたことが委託業者側の意図したものか、設定ミスによるものかは、明らかではありません。
- 推測されにくいURLによる隠しページを用意する発想はよくとられますが、例えばWordPressにおいてこの手法をとり、公開状態を「非公開(WordPress管理者・編集者のみ表示)」や「パスワード保護」にしなかった場合、そのページへのパーマリンクの一部のみ入力されたとしても補完・リダイレクトされ、ページの内容が閲覧可能となってしまう場合があるため、最低でもパスワード保護を行う等、適切なアクセス制限を設定することが肝要です。

TBS NEWS DIG Powered by JNN

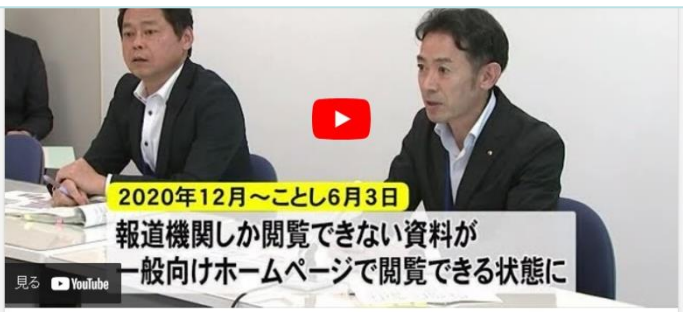
熊本県の報道専用ページで個人情報流出　1000人近くの住所や電話番号など

資料には個人情報も含まれることから、本来はアクセス制限がかかっていますが、県によりますと2020年12月から今月までの約2年半、一部の資料はインターネット上で検索すると誰でも閲覧できる状態だったということです。



資料には叙勲や褒章の受賞者888人の住所のほか、取材の問い合わせ先として67人分の名前や電話番号が載っていました。

FNNプライムオンライン



熊本県のホームページで報道資料が一般にも閲覧できる状態に　955人分個人情報が漏えい

テレビ熊本　2023年6月15日 木曜 午後6:45

熊本県は、報道機関に対して2020年2月から県のホームページでIDとパスワードが必要な専用ページで報道向けの資料を提供しています。

県によりますと、ホームページの管理委託業者が代わった2020年12月から今月3日までの約2年半にわたり、本来、報道機関しか閲覧できない資料が一般向けのホームページで閲覧できる状態になっていたということです。

資料の中には、個人の住所が番地まで載っているものなどもあり、県は955人分の個人情報が漏えいしたとしています。

●北海道電力・沖縄電力を騙るフィッシング、対策協議会が注意喚起

https://www.antiphishing.jp/news/alert/hokuden_20230613.html
https://www.antiphishing.jp/news/alert/okiden_20230613.html

このニュースをザックリ言うと･･･

- 6月13日(日本時間)、フィッシング対策協議会より、北海道電力(北電)と沖縄電力(沖電)を騙るフィッシングについて注意喚起が出されています。

- フィッシングの一例として、件名が「北海道電力利用料金のご請求です【重要なお知らせ】」等で、北電の「Ｗｅｂ料金お知らせサービス」や沖電の「電気ご使用実績照会サービス」を騙り、アカウントや個人情報の入力およびVプリカによる料金支払いを要求する偽サイトへ誘導するものが挙げられています。

- 同協議会では、このようなフィッシングサイトにて、ID・パスワード・メールアドレス・電話番号・名前・Vプリカ発行コード番号・額面等を絶対に入力しないよう呼び掛けています。

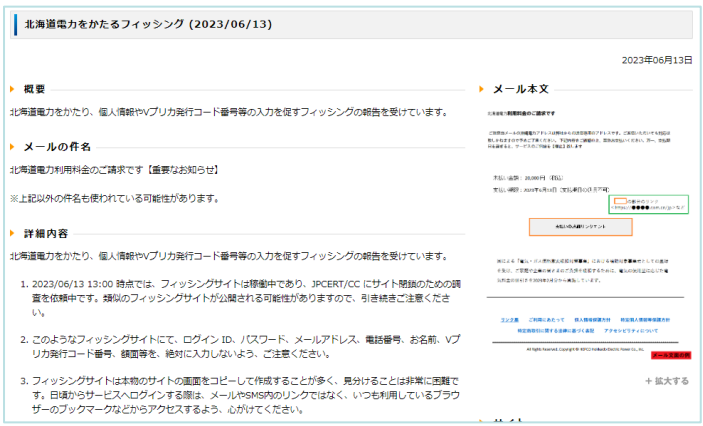
AUS便りからの所感

- 同協議会による電力会社を騙るフィッシングへの注意喚起は昨年までごく少数でしたが、今年に入り3月に東京電力と関西電力を騙るものについて挙げられています。

- 3月のフィッシングを含めフィッシングメールのリンクに「支払いの詳細リンクエント」と書かれている点が共通しており、全て同じサイバー犯罪グループによるものとみられます。

- 電力各社もフィッシングメールに対する注意喚起を出していますので、利用しているサービスの本物のサイトをあらかじめブックマークしてそこからアクセスするようにし、発信されている情報を随時確認しつつ、フィッシングメールに対し慎重に行動すること、また可能な限りメーラーやブラウザー・アンチウイルスソフトのアンチフィッシング機能等を有効にすることを心掛けましょう。

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


北海道電力をかたるフィッシング (2023/06/13)

2023年06月13日

概要

北海道電力をかたり、個人情報やVプリカ発行コード番号等の入力を促すフィッシングの報告を受けています。

メールの件名

北海道電力利用料金のご請求です【重要なお知らせ】

※上記以外の件名も使われている可能性があります。

詳細内容

北海道電力をかたり、個人情報やVプリカ発行コード番号等の入力を促すフィッシングの報告を受けています。

1. 2023/06/13 13:00 時点では、フィッシングサイトは稼働中であり、JPCERT/CC にサイト閉鎖のための調査を依頼中です。類似のフィッシングサイトが公開される可能性がありますので、引き続きご注意ください。
2. このようなフィッシングサイトにて、ログイン ID、パスワード、メールアドレス、電話番号、お名前、Vプリカ発行コード番号、額面等を、絶対に入力しないよう、ご注意ください。
3. フィッシングサイトは本物のサイトの画面をコピーして作成することが多く、見分けることは非常に困難です。日頃からサービスへログインする際は、メールやSMS内のリンクではなく、いつも利用しているブラウザーのブックマークなどからアクセスするよう、心がけてください。

メール本文

＋拡大する

●米政府機関へのサイバー攻撃相次ぐ…露攻撃者集団がソフト脆弱性悪用か

https://www.tokyo-np.co.jp/article/256965
https://www.cnn.co.jp/usa/35205305.html
https://www.trendmicro.com/ja_jp/research/23/f/insight-on-vulnerabilities-in-moveit-transfer.html

このニュースをザックリ言うと･･･

- 6月15日(現地時間)、米セキュリティ機関のCISAより、複数のアメリカ政府機関が相次いでサイバー攻撃を受けていると発表されました。

- 「MOVEit」というファイル転送ソフトウェアの脆弱性を悪用され、侵入の被害を受けたとしている一方、情報流出等の重大な影響はなかったとも報じられています。

- MOVEitの脆弱性を突く攻撃が世界中で確認されており、ロシアの攻撃者集団「CLOP」の関与が疑われているとのことです。

AUS便りからの所感

- MOVEitはProgress Software社が開発提供し、米政府機関等で広く使われているとされていますが、5月末以降、3件の脆弱性が報告され、3度アップデートがリリースされています。

- 特にSQLインジェクションの脆弱性(CVE-2023-34362)については、セキュリティアップデートのリリース前から悪用されていたゼロデイ脆弱性とみられています。

- 一般的な話とはなりますが、クライアントPC～サーバーにインストールされているあらゆるソフトウェア、さらには各種ネットワーク機器のファームウェアに至るまで、直接的・間接的に脆弱性が悪用される可能性を抑制するため、全てを常に最新に保つようにし、加えてアンチウイルスやUTM等による防御も確実に行うことが重要です。

東京新聞 TOKYO Web

複数の米政府機関にサイバー攻撃　ソフトの脆弱性突かれる

2023年6月16日 07時22分 （共同通信）

【ワシントン共同】米国土安全保障省サイバー・インフラ安全局（ＣＩＳＡ）高官は１５日、複数の連邦政府機関がサイバー攻撃を受けたと明らかにした。ロシアに拠点があるとされるサイバー犯罪集団「クロップ」がファイル転送ソフトの脆弱性を突いたとみている。情報流出など「重大な影響」はなかったとしている。

CNN.co.jp

世界的なサイバー攻撃発生、米政府機関も被害　CNN EXCLUSIVE

2023.06.16 Fri posted at 07:45 JST

（CNN）米国土安全保障省傘下のサイバー・インフラ安全局（CISA）は15日、広く使用されているソフトウェアの脆弱（ぜいじゃく）性につけこんだ世界的なサイバー攻撃で、「複数」の政府機関が被害に遭ったと発表した。

CISA高官のエリック・ゴールドスタイン氏は声明で、問題のアプリケーションは「MOVEit」だと言及。複数の政府機関で侵入が確認されたことを明らかにし、「被害の程度を把握し、タイムリーな修復を行うために緊急に取り組んでいる」と述べた。