— AUS（アルテミス・ユーザ・サポート）便り 2020/06/08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。

●仮想通貨取引所がサイバー攻撃被害…原因はドメイン名管理サービスへの不正アクセス

https://www.itmedia.co.jp/news/articles/2006/03/news060.html
https://corporate.coincheck.com/2020/06/02/97.html
https://corporate.coincheck.com/2020/06/04/98.html
https://www.onamae.com/news/domain/20200603_1/

このニュースをザックリ言うと･･･

- 6月2日(日本時間)、仮想通貨取引所「Coincheck」運営のコインチェック社より、サイバー攻撃によって同社宛メールの一部が攻撃者に取得されていたと発表されました。

- 5月31日～6月1日の間に送信されたユーザー約200人の問合せメールについて、メールおよび記載されていた名前・住所・生年月日・電話番号・IDセルフィー(顔と本人確認を撮影した画像)が流出したとされています。

- 同社ドメイン名を管理するドメイン名登録サービス「お名前.com」が不正アクセスを受け、ドメイン名情報が一時改ざんされたことが原因とされ、同社が預かっている資産には影響していないとのことです。

- 6月4日には同業となる「bitbank」からも、同じくお名前.comへの不正アクセスによる被害を受けていたことが発表されています(https://blog.bitbank.cc/20200604/)。

AUS便りからの所感等

- お名前.comの管理機能におけるWebアプリケーション側の不具合(現在は修正済み)を突いて攻撃が行われたことにより、NSレコード(DNSサーバーのアドレス)が改変され、攻撃者が用意した偽のドメイン情報を返すDNSサーバー、さらには偽のメールサーバーにメールを送るよう誘導される事象が発生していた模様です。

- ドメイン名とそれを管理するDNSにおける障害や改ざんの発生は、他にも偽のWebサーバーへの誘導やSSL証明書の不正取得等につながることにより、サービス全体の機密性・可用性・完全性に影響する恐れがあり、2019年1月にもDNS設定の改ざんによってドメイン名のハイジャックを行おうとする攻撃に対し、米国政府機関やjpドメインを管理するJPRSから注意喚起が出されています(AUS便り 2019/2/4号参照)。

- 今回のようなドメイン管理サービス側の脆弱性以外のケースでも、管理アカウントに不正ログインされないよう強力なパスワードを設定することや、第三者による不正な移管申請等が行われないようレジストリロックの設定を行うこと、あるいは万が一の改ざん発生を速やかに把握できるような監視体制の用意等、様々な攻撃の手口を認識し、管理者側で自衛するための方策を可能な限りとっておくことが肝要です。

Coincheck

ドメイン取るなら 公式登録サービス お名前.com .com .jp .co.jp https://www.onamae.com by GMO

当社利用のドメイン登録サービスにおける不正アクセスについて（第一報）

2020.6.2

このたび、コインチェック株式会社（本社：東京都渋谷区、代表取締役：蓮尾 聡）が利用しているドメイン登録サービス「お名前.com（GMOインターネット株式会社）」内の当社アカウントにおいて、不正アクセスが確認されました。本事象により、不正アクセスを行なった第三者（以下、第三者）が2020年5月31日～6月1日の期間に当社のお客様からお問い合わせを頂いた一部のメールを不正に取得できる状態になっていたことが判明いたしました。

このような事態が発生し、お客様にご迷惑をおかけしましたことをお詫び申し上げます。現時点で判明している情報は以下の通りです。

なお、本件に関しまして、ドメイン登録サービス運営元にも調査を依頼しており、今後新たな情報が判明した場合は、速やかにご案内いたします。

2020.06.03 【お知らせ】

お名前.com Naviで発生した事象につきまして

平素はお名前.comをご利用いただきまして、まことにありがとうございます。
この度、お客様のドメインやサーバーの管理ツール「お名前.com Navi」において、以下の事象の発生が確認されました。

1. 事象の概要と原因
お名前.comをご利用のお客様の管理画面が不正にアクセスされ、ご登録いただいている情報が書き換えられるという事案が発生しました。
これについて調査を行ったところ、悪意のある第三者が、当該お客様のIDと、「お名前.com Navi」における通信を改ざんできる不具合(※)を利用して、お客様のお名前.com会員情報(メールアドレス)を書き換えたことが判明しました。
なお、調査により、他のお客様については影響がないことを確認しております。
また、本事象の対象のお客様とは連絡が取れ、正しい情報に修正済みとなります。
※個人情報が閲覧できる、あるいは通常のブラウザ上の操作で悪用できる不具合ではありません。

●雇用助成金オンライン申請、システムの不具合で休止

https://www3.nhk.or.jp/news/html/20200606/k10012460571000.html
https://netshop.impress.co.jp/node/7695

このニュースをザックリ言うと･･･

- 5月20日(日本時間)、厚生労働省が同日に受付を開始した「雇用調整助成金」のオンライン申請システムに不具合が確認され、一時受付を休止する事態となりました。

- 6月2日の同省の発表では、申請するための画面にアクセスした際に、他の申請者の名前・メールアドレス・電話番号等が表示されるケースが発生したとの問合せがあったとされ、申請を行った事業者のうち1,118事業者においてこの問題が発生していたとのことです。

- 同省ではシステムの改修を行い、6月5日正午より受付を再開しましたが、再び同様の問題が発生し、受付を停止しています。

AUS便りからの所感

- 前述の1,118事業者に割り当てられたIDについて、全く同時刻に申請した事業者同士で重複が発生していたのが原因としており、登録時間の秒単位でIDを生成していた可能性が指摘されています。

- 3月には、成人向けコンテンツサービス「ソフトオンデマンド」において他のユーザーの個人情報が表示される問題が発生していますが、こちらは使用しているCDNにおけるキャッシュ設定のミスにより、個々のユーザーの情報がキャッシュされ、他のユーザーに表示されたことが原因とされています(https://scan.netsecurity.ne.jp/article/2020/03/31/43887.html)。

- 各種サービスの開発・構築にあたっては、個人情報流出の様々な事例を参考とし、ユーザーアカウント情報を収納するデータベース上でIDの衝突を防ぐよう設定する等、必要な対策を把握し、確実に実行することに注意を払いましょう。

NHK

雇用調整助成金 オンライン申請トラブルで個人情報流出か

2020年6月6日 7時31分　新型コロナウイルス

システムトラブルで運用を中止していた「雇用調整助成金」のオンライン申請を、5日再開直後に再びトラブルで中止した問題で、厚生労働省は個人情報が流出した可能性があることを明らかにしました。

雇用を維持するための「雇用調整助成金」について、厚生労働省は新型コロナウイルスの影響で休業を余儀なくされる企業が増えたことを踏まえて制度を拡充するとともに、手続きを簡素化するため、先月20日からオンライン申請の受け付けを始めました。

ところが初日からシステムトラブルが発生し、運用をいったん中止してシステムを改修したうえで2週間たった5日、正午からオンラインによる受け付けを再開していました。

しかし5日午後2時半ごろ、申請した企業から「他社の情報が見られる」という連絡があり、再開から3時間もたたずに再び受け付けを中止する事態となりました。

●経団連の関連団体、約500件の個人情報流出か…Webサイトに不正アクセス

https://www.itmedia.co.jp/news/articles/2005/29/news111.html
https://xtech.nikkei.com/atcl/nxt/news/18/07995/
https://www.keidanren-jigyoservice.or.jp/200528.pdf

このニュースをザックリ言うと･･･

- 5月28日(日本時間)、日本経済団体連合会(経団連)の関連法人である経団連事業サービスより、同法人が運営するWebサイトが不正アクセスを受け、個人情報が流出した可能性があると発表されました。

- 被害を受けたのは、1月21日～5月3日にセミナー・書籍等の申込を行った者約500件の会社・団体名、氏名、所属・役職、住所、電話番号およびメールアドレスとされています。

- 5月21日に、Webサイトの管理委託業者により、サイト内に不正なプログラムが発見されたことで不正アクセスが発覚、同27日に当該サイトを停止し、臨時サイトへの切り替えで対応しているとのことです。

AUS便りからの所感

- 発表によれば、申込フォームへの入力内容を攻撃者が指定したサーバー上のファイルに保存するようプログラムが改ざんされ、攻撃者が当該ファイルに外部からアクセスした形跡も確認されたとのことです。

- 今回クレジットカード情報が流出したという発表はなかったものの、数多く報告されるクレジットカード情報奪取の手口としてフォームの改ざんは非常によく使われています。

- 早期の攻撃や改ざんの発見ひいては情報流出の阻止のため、アクセスログの(自動的な)分析、サーバー上のファイル改ざんの検知、WAFによる不正なリクエストの遮断、あるいは(今回の手口では有効ではありませんが)サーバー側から外部への不審な通信の検知・遮断等が有用となるでしょう。

ITmedia NEWS

経団連の関連団体、約500件の個人情報流出か　Webサイトに不正アクセス

2020年05月29日 15時14分 公開　[ITmedia]

印刷　見る　Share　B! 18

日本経済団体連合会（経団連）の関連法人、経団連事業サービスは5月28日、運営するWebサイトが不正アクセスを受け、約500件の個人情報が流出した可能性があると発表した。流出の疑いがあるのは、2020年1月21日～5月3日にセミナーや書籍などを申し込んだ人の勤務先、役職、電話番号、氏名、住所、メールアドレスなど。

一般社団法人 経団連事業サービス

当法人ホームページへの不正アクセスによる情報漏洩可能性について(2020年5月28日)

Zoom オンライン開催
2020年 7月28日(火)・29日(水)
概要・お申込はこちら

第119回 経団連 労働法フォーラム

第1日テーマ・報告者
(報告1)「職場のハラスメント防止に向けた法的留意点と企業の対応」
渡邉 徹 弁護士(弁護士法人淀屋橋・山上合同)

第2日テーマ・報告者
(報告11)「労働契約の解消に関する労務管理上の留意点」
梅木 佳則 弁護士(安西法律事務所)