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。

## ●新聞社キャンペーン応募者の個人情報、委託会社への不正アクセスで削除、流出か…約143,000件分

https://www.itmedia.co.jp/news/articles/2106/25/news093.html
https://www.chunichi.co.jp/article/278807
https://www.tokyo-np.co.jp/article/112562

### このニュースをザックリ言うと･･･

- 6月24日(日本時間)、中日新聞社より、同社およびグループ各社(東京新聞・北陸中日新聞)がWeb上で開催したキャンペーン応募者の個人情報が、不正アクセスにより流出した可能性があると発表されました。

- 被害を受けた可能性があるのは、2009～2019年にグループ3社が開催した7種のWebキャンペーンへの応募者約143,000件分の個人情報(氏名・住所・性別・年代・新聞購読歴・電話番号およびメールアドレス。クレジットカード情報等は含まず)とされています。

- 同23日、キャンペーンサイトの運営を委託した外部企業から、サーバーへの不正アクセスにより保管されていた個人情報を削除されたとの報告を受け、削除されただけでなく、流出した可能性もあると判断したことから今回の発表となったとしており、当該企業含め契約関係にある企業に対するセキュリティ強化の指示などを行っているとのことです。

### AUS便りからの所感等

- キャンペーンページにおける個人情報取り扱いの表示によれば、当選の連絡・賞品等の発送といったキャンペーン関連のみならず、応募時に同意を得た上で、グループ各社のさらなるサービス・情報提供の用途でも利用されていた模様です。

- 個人情報の保護にあたり、当人からの開示や削除請求に確実に対応する体制を整えることも鑑み、流出のみならず不慮の削除が発生することもないよう留意する必要があるでしょう。

- また万が一の流出時のリスク等を軽減するため、個人情報の取得・保存に際しては、郵送等の目的で住所等を取得する必要がないのであれば初めから取得しないことと、キャンペーン以外の用途に同意されていない等といった場合に、当初の限定された用途での利用が終了次第適切に情報を削除するよう徹底することが重要です。

ITmedia NEWS

### 中日新聞、個人情報14万件漏えいか　委託先のサーバに不正アクセス

2021年06月25日 12時01分 公開　[ITmedia]

印刷　148　Share　B! 4

中日新聞社は6月24日、キャンペーンサイトの運営を委託していたランドマークス（東京都港区）のサーバが不正アクセスを受け、約14万3000件の個人情報が漏えいした可能性があると発表した。

中日新聞社

漏えいした可能性があるのは、同社が提供する中日新聞や東京新聞、北陸中日新聞の企画として、2009年から19年にかけて開催したWebキャンペーン7種に応募した人の氏名、住所、性別、年代、新聞の購読歴、電話番号、メールアドレス。漏えいしただけでなく、情報が削除された可能性もあるという。

## ●攻撃対象となり得る「野良サーバー」調査・発見サービス、マクニカネットワークスが開始

https://japan.zdnet.com/article/35172792/
https://www.macnica.net/pressrelease/mpressioncss_20210623.html/

### このニュースをザックリ言うと･･･

- 6月22日(日本時間)、マクニカネットワークス社より、同社が展開するセキュリティサービス「Mpression Cyber Security Service」の新メニュー「Attack Surface Managementサービス」を同23日より提供開始すると発表されました。

- クラウド上などで導入された、ユーザー企業のものと思われる外部公開アセットの存在について、攻撃者と同様の視点から調査・発見を行い、設定変更・パッチの適用あるいは撤去といった対処が必要なものについて適宜アドバイスを行うものとなっています。

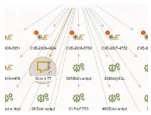
- 同社では、「従来主流だったWebやメールを悪用するかたちでの侵入は、各企業での多層防御や監視、またEDRやブラウザでのエンドポイント保護機能の充実により悪用することが難しくなってきたため、境界型多層防御を迂回できるAttack Surface（管理が不十分なサーバやネットワーク機器）が攻撃者の格好の侵入経路となっている」としています。

### AUS便りからの所感

- 個人情報や業務用のデータを社外ネットワークのデータベースサーバーに保存し、それが第三者からアクセス可能になっていることが発見された事例は、本田技研工業の事例(AUS便り 2019/8/5号参照)をはじめ度々報告されています。

- 社内ネットワーク上で稼動しながら管理下に置かれていない機器が何らかの経路で攻撃者に悪用され得るのと同様、開発・試験用に構築した環境についても、インターネット上に配置している限りは常時攻撃者が探し回っていると考え、今回取り上げたようなセキュリティサービスによる確認をもとに、アクセス制限等を確実に行うこと、場合によってはVPC等と呼ばれる仮想ネットワーク下に配置することも検討すべきでしょう。

ZDNet Japan



マクニカネット、サイバー攻撃に遭いやすいIT資産調査サービスを開始

國谷武史（編集部） 2021-06-23 14:41

シェア 22 ツイート B! 3 noteで書く Pocket 0

マクニカネットワークスは6月23日、サイバー攻撃に遭いやすい企業のIT資産を調査し、セキュリティ対策方法などを助言するサービス「Attack Surface Managementサービス」を開始すると発表した。利用料は都度見積もりになる。

新サービスでは、同社セキュリティ研究センターの専門家がドメイン情報などのOSINT（オープンソースインテリジェンス）を使って、インターネットに公開されているサーバーやネットワーク機器、システムのポートなどを調査、可視化する。これをもとに脆弱性の有無や危険性などを分析して顧客にレポートするとともに、アクセス制御や認証強化、パッチ適用、機材撤去などの対策方法をアドバイスする。

## ●WordPress用プラグイン「WordPress Popular Posts」にXSSの脆弱性…アップデート推奨

https://scan.netsecurity.ne.jp/article/2021/06/25/45869.html
https://jvn.jp/jp/JVN63066062/index.html

### このニュースをザックリ言うと･･･

- 6月23日(日本時間)、IPA・JPCERT/CCが運営する脆弱性情報サイト「JVN」より、WordPress用プラグイン「WordPress Popular Posts(以下WPP)」にクロスサイトスクリプティング(XSS)の脆弱性があるとして注意喚起が出されています。

- WPPはサイト上で人気のある記事をサイドバー等に表示するプラグインですが、JVNによれば「当該製品の管理者権限を持つユーザが、自身のブラウザ上で意図せずスクリプトを実行してしまう可能性」があるとしています。

- 脆弱性はWPPバージョン5.3.2以前に存在しており、修正バージョンである5.3.3へのアップデートが推奨されています。

### AUS便りからの所感

- WPPの開発者によれば、XSSの脆弱性を悪用するには攻撃者がWordPress上に「投稿者」以上の権限を持つユーザーとしてログイン可能であることなどが条件とされています。

- WordPressにおいては、本体はもちろん、数え切れないほどリリースされているサードパーティー製のプラグインについても脆弱性に注意する必要があり、インストール・有効化するプラグインはできる限り必要最小限とし、それら全てとWordPress本体について随時セキュリティ情報を確認しつつ、最新バージョンに保つよう留意することを強く推奨致します。

ScanNetSecurity by iid

WordPress 用プラグイン WordPress Popular Posts にクロスサイトスクリプティングの脆弱性

独立行政法人情報処理推進機構（IPA）および一般社団法人JPCERT コーディネーションセンター（JPCERT/CC）は6月23日、WordPress用プラグインWordPress Popular Postsにおけるクロスサイトスクリプティングの脆弱性について「Japan Vulnerability Notes（JVN）」で発表した。

シェア ツイート 送る

独立行政法人情報処理推進機構（IPA）および一般社団法人JPCERT コーディネーションセンター（JPCERT/CC）は6月23日、WordPress 用プラグイン WordPress Popular Posts におけるクロスサイトスクリプティングの脆弱性について「Japan Vulnerability Notes（JVN）」で発表した。株式会社セキュアスカイ・テクノロジーの岩間湧氏が報告を行っている。影響を受けるシステムは以下の通り。

WordPress Popular Posts 5.3.2 およびそれ以前

Hector Cabrera が提供する WordPress 用プラグイン WordPress Popular Posts には、クロスサイトスクリプティングの脆弱性が存在し、当該製品の管理者権限を持つユーザが自身のブラウザ上で意図せずスクリプトを実行してしまう可能性がある。