

記者配布資料

2024年1月30日

大阪経済記者クラブ会員各位

大阪商工会議所・立命館大学共同研究

「中小企業等のホームページ脆弱性診断」調査結果

一定割合のホームページに改ざんや不正プログラム埋め込み等の危険性あり

〔お問合せ〕大阪商工会議所 経営情報センター(登坂、古川、野田、石田)

TEL:06-6944-6353

- 大阪商工会議所は、正しく安全なホームページの運用を促すことを目的に、立命館大学との共同研究調査として、中小企業等のホームページの脆弱性診断を実施した。日本国内で約8割のシェアを有する「WordPress」※1で作られたホームページを対象に調査を行った結果、**66%のURLに、改ざんや不正プログラム埋め込み等が行われる危険性（ユーザーリスト※2とログインページの双方が露出）**が見受けられた。
- この結果を受け、2月8日（木）に、「ホームページ作成ツール『WordPress』注意喚起セミナー」を開催する。同セミナーでは、診断結果から見た中小企業のセキュリティに関する実態を報告するとともに、ホームページ設定の確認方法や対策ポイントを解説する。

＜調査概要＞

- 背景：2023年9月に、鹿児島王将㈱のホームページが改ざんされ、実在する弁護士事務所の名で「破産手続きを開始した」などとする事実無根の表記がなされた。また、同年12月には、大阪商工会議所経営情報センターにも改ざんの相談が寄せられた。さらに、ホームページ作成ソフトの脆弱性を突かれ、不正に改ざんされたホームページから不正プログラム「Emotet」※3をダウンロードされるような、「被害者が加害者になってしまう」事例も確認されている。
- 調査目的：身近なITであるホームページに宿るリスクを見える化し、中小企業に警鐘を鳴らし、正しく安全なホームページの運用を促すこと。
- 調査期間：2023年10月3日（火）～11月10日（金）
- 調査対象：「WordPress」で作られたURLを所持する企業・団体111社
- 調査対象数：22都道府県の企業111社所有の192ホームページ
- 調査手法：①WordPressのバージョン、②ユーザーリストの露出、③ログイン画面の露出、④過去に脆弱性が公開されたプラグイン※4の利用有無の4つの観点で調査

※1…ホームページの作成と管理に利用される無料のソフトウェア。機能性と自由度が非常に高く、世界中で圧倒的なシェアを有するが、多くの利用者が存在するため、攻撃者の標的となりやすい側面もある。

※2…ユーザーリストとは、WordPressサイトの管理や編集などが可能なユーザーのリスト。ユーザーリストで表示されるIDと推測したパスワードを用いると、サイバー攻撃者であれば当該ホームページの編集ページに不正アクセスできてしまう。

※3…数年前から世界中で脅威をふるっている不正プログラム。ファイルを開くとウイルス感染し、メールボックスの情報を盗まれるだけでなく、その情報を元に他のユーザーへ感染メールが送信されてしまい、取引先や顧客を巻き込んでしまう可能性がある。

※4…プラグインとはWordPressに様々な追加機能を提供する仕組み。利用しているプラグインのバージョンが古い場合や、利用しているプラグインに危険度の高い脆弱性が存在する場合、脆弱性を悪用したページの改ざんや不正ファイルの設置、情報詐取などがサイバー攻撃者によって行われる可能性がある。

調査結果のポイント

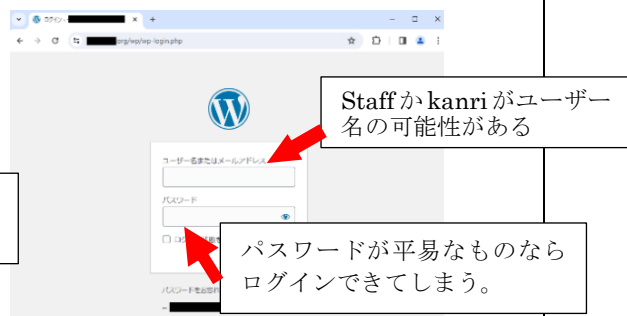
○ユーザーリスト（WordPress サイトの管理や編集などが可能なユーザーの情報）とログインページの双方が露呈している URL が 66%

サイトの「ユーザーリスト」と管理用の「ログインページ」の双方が露出している URL が 66% あった。ユーザーリストで表示されているユーザー名は、ログインする際の認証情報として用いられる。このユーザーリストに加えてログインページが露出していると、パスワードが平易なもの（例：Password 等）であれば、攻撃者は簡単に当該ホームページの編集ページに不正アクセス（ログイン）できてしまい、改ざんや不正プログラム埋め込み等が行われる危険性がある。

↓ ユーザーリスト公開の例



↓ ログインページ公開の例



○プラグイン（WordPress に様々な追加機能を提供する仕組み）に課題が存在する URL が 93%

WordPress に様々な追加機能を提供するプラグインのバージョンが古い場合や、危険度の高い脆弱性が存在する場合、脆弱性を悪用したページの改ざんや不正ファイルの設置、情報詐取等がサイバー攻撃者によって行われる可能性がある。

※本調査では過去に脆弱性が公開されたプラグインの利用有無のみを確認しており、プラグインのバージョンが最新であるかまでの確認は行っていない為、93%全ての URL が危険というわけではない。

<「ホームページ作成ツール『WordPress』注意喚起セミナー」開催概要>

○日 時： 2024 年 2 月 8 日（木）15：00～17：00

○場 所： ハイブリッド開催

【リアル受講】大阪商工会議所 6 階桜の間（大阪市中央区本町橋 2 番 8 号）

【オンライン受講】Zoom ウェビナー

○参加費： 無料

○プログラム：

（1）講演「脆弱性診断から判明した実態と対策ポイント」

立命館大学大学院 情報理工学研究科 博士後期課程 田中 啓介 氏

（2）大阪商工会議所 経営情報センター事業のご紹介

（3）大阪府「超簡易版 BCP『これだけは！』シート」のご紹介（全体概要版）

（4）ホームページ作成ツール「WordPress」に関する個別相談会（希望者のみ）

※当日ご取材頂けます。

以 上

<添付資料>

資料 1： ホームページ改ざん等の危険性等調査 調査結果概要

資料 2： 「ホームページ作成ツール『WordPress』注意喚起セミナー」案内状

大阪商工会議所・立命館大学「セキュリティ診断」
～大阪商工会議所がホームページ(WordPress)の点検を行います～
調査結果

1. 調査期間： 2023 年 10 月 3 日（火）～11 月 10 日（金）
2. 調査対象： 「WordPress」で作られた URL を所持する企業・団体
3. 調査方法： E メールにて調査協力依頼、web フォームで回答
4. 調査手法： ①WordPress のバージョン、②ユーザーリストの露出、③ログイン画面の露出、④過去に脆弱性が公開されたプラグインの利用有無 の 4 つの観点で調査
5. 調査対象概要：

- 調査対象数…111 社 192 のホームページ
- 調査対象都道府県…22（大阪府 62 社、千葉県・京都府各 6 社、東京都・兵庫県各 5 社、群馬県 4 社、和歌山県・愛媛県各 3 社、埼玉県・愛知県・広島県各 2 社、北海道・新潟県・茨城県・神奈川県・静岡県・長野県・岐阜県・滋賀県・岡山県・福岡県、宮崎県各 1 社）
- 調査対象企業の従業員数
- 調査対象企業の業種

項目	件数	割合
0人	0	0%
1～5人	19	17%
6～10人	8	8%
11～20人	13	12%
21～50人	16	14%
51～100人	12	10%
101～200人	7	6%
201～300人	3	3%
301人～	3	3%
不明	30	28%

項目	件数	割合
サービス業	46	44%
製造業・加工業	31	26%
サービス業（士業・コンサルタント等）	11	9%
卸売業	10	9%
建設業・工事業	4	3%
宿泊業・飲食業	2	2%
運輸業・通信業・不動産業	2	2%
サービス業（医療法人・医院・社会福祉法人等）	2	2%
その他	2	2%
小売業	1	1%
農林業・水産業・畜産業	0	0%
不明	0	0%

6. 調査結果：

- 結果概要

項目	問題あり		問題なし	
	件数	割合	件数	割合
①WordPressのバージョン	11	6%	181	94%
②ユーザーリストの露出	150	78%	42	22%
③ログイン画面の露出	147	77%	45	23%
④過去に脆弱性が公開されたプラグインの利用有無	179	93%	13	7%

（補足）①WordPress のバージョン：WordPress サイトの WordPress コアのバージョンが公開されており、かつ最新でないバージョンである場合、第三者が既知の脆弱性を悪用し、ページの改ざん等を行う可能性がある。

④過去に脆弱性が公開されたプラグインの利用有無：本調査では過去に脆弱性が公開されたプラグインの利用有無のみを確認しており、プラグインのバージョンが最新であるかまでの確認は行っていない為、93%全ての URL が危険というわけではない。

○ ユーザーリスト×ログイン画面の露出

項目	件数	割合
両方が露出	127	66%
上記以外	65	34%

ユーザーリスト（WordPress サイトの管理や編集などが可能なユーザーの情報）とログインページの双方が露呈している URL が 66%存在した。ユーザーリストに加えてログインページが露出していると、パスワードが平易なもの（例：Password 等）であれば、攻撃者は簡単に当該ホームページの編集ページに不正アクセス（ログイン）できてしまい、改ざんや不正プログラム埋め込み等が行われる危険性がある。

以 上

ホームページ作成ツール「WordPress」注意喚起セミナー ～ 脆弱性診断から判明した実態と対策ポイント ～

無料

ホームページを WordPress で構築、運営している企業は多いのではないのでしょうか？WordPress は素人でも簡単にホームページを構築、更新できるため、IT に長けた人材が不足している中小企業にとって便利なツールですが、利用者が多い為サイバー攻撃者のターゲットとなりやすく、故に脆弱性が多く存在します。基本的な対策を怠ると、ホームページの乗っ取りや改ざんといったサイバー攻撃の被害にあってしまう可能性もございます。

本セミナーでは、立命館大学と大阪商工会議所が共同で実施した、中小企業のホームページ改ざんの危険性を診断した結果から、リアルな実態をお伝えすると共に、設定の確認方法や対策ポイントをお知らせします。

また、サイバー攻撃など人為的犯罪行為に加えて、自然災害・感染症への備えも BCP という観点から重要です。カンタンに策定できる大阪府「超簡易版 BCP『これだけは！』シート」の概要も併せて紹介いたします。

日程等

2/8 (木) ハイブリッド開催

(1) リアル受講 (30 名)

大阪商工会議所 6階 桜の間 (大阪市中央区本町橋 2 番 8 号)

(2) オンライン受講 (Zoom ウェビナー 配信)

※本事業は大阪府補助金対象事業ですので (1) (2) とともに受講後アンケートのご提出をお願い申し上げます

内容

15:00～16:00

脆弱性診断から判明した実態と対策ポイント 講演&質疑応答

立命館大学 大学院 情報理工学研究科 博士後期課程 田中 啓介 氏

トレンドマイクロ株式会社 インシデントレスポンスチーム所属。2007 年に新卒社員としてトレンドマイクロに入社。製品のサポート業務を経て、2012 年より中央省庁担当のアカウントマネージャとしてセキュリティ監視、インシデントレスポンス、対策提言を実施。マネジメント業務を経て、2019 年よりインシデント対応支援サービスを主管。情報処理安全確保支援士、GCFA、GDAT、GOSI 立命館大学 情報理工学研究科 博士後期課程 上原研究室所属、滋賀県警察サイバーセキュリティ対策委員会アドバイザー

16:00～16:20

大阪商工会議所 経営情報センター事業のご紹介

大阪商工会議所 経営情報センター 担当

16:20～16:35

大阪府「超簡易版 BCP『これだけは！』シート」のご紹介 (全体概要版)

16:35～17:00

ホームページ作成ツール「WordPress」に関する個別相談会 (希望者のみ)

主催・お問合せ：大阪商工会議所 経営情報センター TEL：050-7105-6004

セミナー参加のお申し込みは下記 URL または QR コードから

<https://www.osaka.cci.or.jp/event/seminar/202312/D41231218017.html>

- 大規模災害や新型コロナウイルスの感染状況によっては中止や延期、もしくはオンライン開催のみへ変更変更させていただく場合がありますのでご承知おきください。
- 本講座にかかる映像、画像、テキスト、音声ならびに配布していない関連資料等の画面キャプチャ、撮影、録音、ダウンロード、複製、上映、公衆送信、頒布、譲渡、貸与、販売、翻案、転載、二次的利用等は、目的の如何を問わず、固く禁止します。
- ご記入情報は本大会が本事業の事務業務に利用するとともに各種連絡・情報提供 (Eメールの事業案内含む) に利用します。また講師・大阪府へ参加者名簿として提供します。これらについては受講者ご本人に同意いただいたものとして取り扱わせて頂きます。

