GMO CYBER SECURITY IERAE

攻撃者の視点で考える、CMSのリスク

作って終わりにしない CMSセキュリティ

— 放置されたCMSが招くリスクと、Web制作会社が明日からできること —

Web制作会社のための CREATORS UPDATE 2026 Summer

GMO CYBER SECURITY IERAE

セキュリティ診断、技術力に強み

脆弱性診断・侵入テスト

累計実績 **16000**件超え

北陸銀行 / KDDI / 森永乳業 / 横浜銀行 / freee / FUJIFILM RIPCORD / NEC / dwango / 北海道銀行 / TOPPAN / The Pokémon Company / CyberAgent / ALSOK / YKK AP / sansan

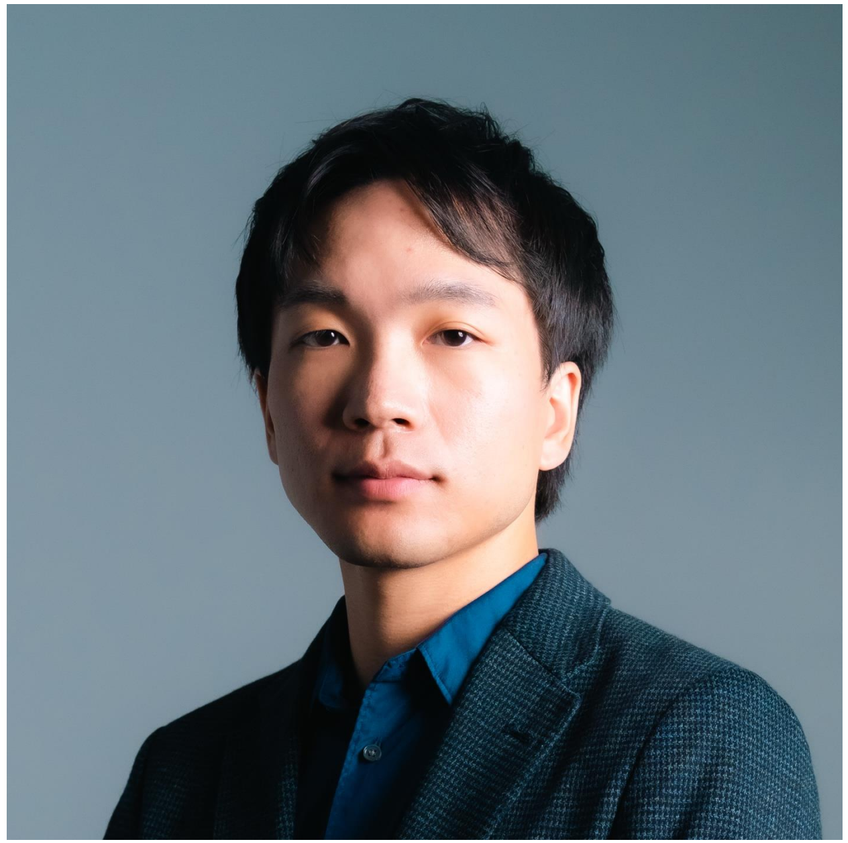
3年連続 世界No.1

世界最高峰のセキュリティコンテスト

2023年 DEF CON 31 Cloud Village CTF:世界1位
2024年 DEF CON 32 Cloud Village CTF:世界1位
2025年 DEF CON 33 Cloud Village CTF:世界1位

2025年	世界1位	DEF CON 33 Cloud Village CTF
2024年	世界1位	HITCON CYBER RANGE
2024年	世界1位	Hack the DRONE 2024決勝
2024年	国内1位	Automotive CTF 2024 グローバル決勝
2024年	国内1位	HTB Business CTF
2024年	国内1位	LINE CTF 2024
2023年	世界2位	DEF CON 31 CMD+CTRL Cyber Range CTF

登壇者紹介



意識しなくてもセキュリティ診断が
当たり前に行われる世界の実現を目指す

プロダクトサービス部 部長

市川 遼 Ryo Ichikawa

2019年	DEF CON CTF Finals 出場
2019年	CODE BLUE Briefings 登壇・U25最優秀発表
2019年	AIS3 (台湾) 講師
2019年	HITCON CTF Finals 3位
2019年	NDSS Workshop on Binary Analysis Research (BAR) 招待講演

2023年、セキュリティとプロダクト開発の知見を活かした新規事業開発の期待を受け、GMOサイバーセキュリティbyイエラエ株式会社に入社。

初めての方でも使いやすい国産ASM「GMOサイバー攻撃ネットde診断」のプロダクトオーナーとして製品開発や組織マネジメントを行う。

今日、伝えたい3つのこと

01

CMSは公開後に 古くなる

本体・テーマ・プラグイン・PHPは、数カ月で古くなっていく。

02

放置CMSは 攻撃者の入口に

狙われたからではなく、**見つかるから** 危ない。

03

棚卸し・更新・診断が 保守の価値になる

セキュリティは、継続提案と信頼につながる。

なぜ、Web制作会社に関係があるのか

制作会社は、CMSセキュリティの**かなり上流**に関わっている。日々の作業のほとんどに、セキュリティ上の判断が含まれている。

01 WordPressを導入する	02 テーマを選定する	03 プラグインを入れる
04 フォーム機能を追加する	05 検証環境を作る	06 本番サーバへ移行する
07 管理画面を引き渡す	08 納品後の修正を受ける	09 保守契約で更新する

診断データから見える現実

530万件

を超える診断を実施（2026年6月時点）

よく見つかる、リスクの高い問題

古いプラグインが残っている

既知の脆弱性があるWordPressプラグインの利用

サポート終了ソフトを使っている

古いWordPress・PHP・JavaScriptライブラリの放置

見えてはいけないものが見えている

設定ファイル・DB情報・バックアップが公開領域に

特殊な攻撃よりも、**「古いまま」「見えている」**問題の方が多い。

放置CMSは、こう攻撃される

01 **広くスキャンする**
ネット上で「入れそうなサイト」を探す

02 **中身を特定する**
CMS種別・バージョン・プラグイン・管理画面

03 **既知の脆弱性で侵入する**
公開済みの攻撃コード・自動化ツールで自動攻撃

04 **入口として使う**
管理者追加・改ざん・Webシェル設置・不正スクリプト

> “
>
> 狙われたから 危ない、ではない。 **見つかるから危ない。**

放置CMSから起こる被害

01

サイト改ざん

スパムページ・不正リンク・転送など、気づきにくい改ざんも。

02

フィッシング設置

正規ドメイン配下の偽ページは、本物らしく見えてしまう。

03

マルウェア配布

閲覧者を悪性サイトへ誘導。サイトが加害の起点に。

04

情報漏えい

氏名・メール・注文情報・DB接続情報・認証情報まで。

05

別サイトへ波及

同一サーバの他サイト・検証環境・バックアップへ。

06

信用低下

検索警告・順位下落・メール不達・顧客説明・保守責任。

制作会社が見落としがちなもの

＋ 検証・ステージング環境

認証が弱く、古いデータが残りやすい

＋ キャンペーンサイト・LP

終了後に放置。URLが生きていれば見える

＋ 旧サイト・旧サブドメイン

DNSやファイルが残れば攻撃対象に

＋ 管理ツールの公開

phpMyAdmin・管理画面・ファイルマネージャ

■ **公開領域に残りやすいもの**

stg.example.com old.example.com/renewal/ backup.zip ・

db.sql ・ dump.sql .env ・ wp-config.php.bak

忘れているサイトでも、**攻撃者からは見えている。**

攻撃のスケールが拡大

従来（AI活用前）

人手中心×試行回数に限りあり

攻撃試行回数	限定的
攻撃コスト	高い
成功確率	低い

AIを活用

現在（AI活用後）

攻撃自動化×高速学習

攻撃試行回数	大幅増加（自動化）
攻撃コスト	低い
成功確率	高い（高速で最適化/学習）

試行回数の増加によって、今まで見つからなかった侵入口が見つかるようになった🔥

自動化によりスキャン侵入試行が常時実行される

24時間365日、膨大な対象に自動で攻撃の試行が繰り返される

LLMによりペイロードや攻撃手法を高速生成・改善

自然言語での指示だけで多様な攻撃コードを生成し、結果を学習して次の攻撃に即反映

成功パターンが即座に横展開される

一度成功した攻撃手法が、コミュニティやツールを通じて瞬時に拡散

作って終わりにしないための対策

A 制作・納品時

不要なプラグインを入れない

使わないものは無効化ではなく削除

管理画面を保護する

多要素認証・ログイン制限・IP制限

バックアップを公開領域に置かない

検証環境にアクセス制限をかける

B 保守・運用時

定期的に更新する

検証環境で確認してから本番へ適用

使っていないサイトを閉じる

「リンクしていないから安全」は不十分

サブドメインを棚卸しする

外部から見える状態を診断する

ネットde診断 / ASM の考え方

明日から確認したい 5つのポイント

1

管理中のCMS一覧（台帳）はあるか

ドメイン・本番／検証／旧・CMS種別・バージョン・保守契約・最終更新日

2

本体・テーマ・プラグインは更新されているか

長期間未更新・配布停止・開発元不明・未使用のものに注意

3

使っていないサイト・検証環境が残っていないか

本番より旧環境・検証環境の方が危ないことがある

4

バックアップ・設定情報が公開されていないか

.env / wp-config.php / wp-config.php.bak / backup.zip / db.sql

5

外部から見える資産を、定期的に診断しているか

人が覚えている資産と、外から見えている資産は一致しない

GMO CYBER SECURITY IERAE

本日のまとめ

CMSは、作った後に古くなる。

放置されたCMSは、攻撃者の入口になる。

だからこそ、棚卸し・更新・診断を保守運用に。

作って終わりにしないことが、これからのWeb制作会社の**信頼**につながる。

ご清聴ありがとうございました。