PRESS RELEASE

2025 年 3 月 3 日

報道関係各位

GMO Flatt Security 株式会社

独自調査の Web 脆弱性検出数ランキング「GMO Flatt Security Top 10」2025 年版を発表

～検出数最多の「認可制御不備」をはじめとして、アプリケーションのビジネスロジックに関わるものが半分以上～

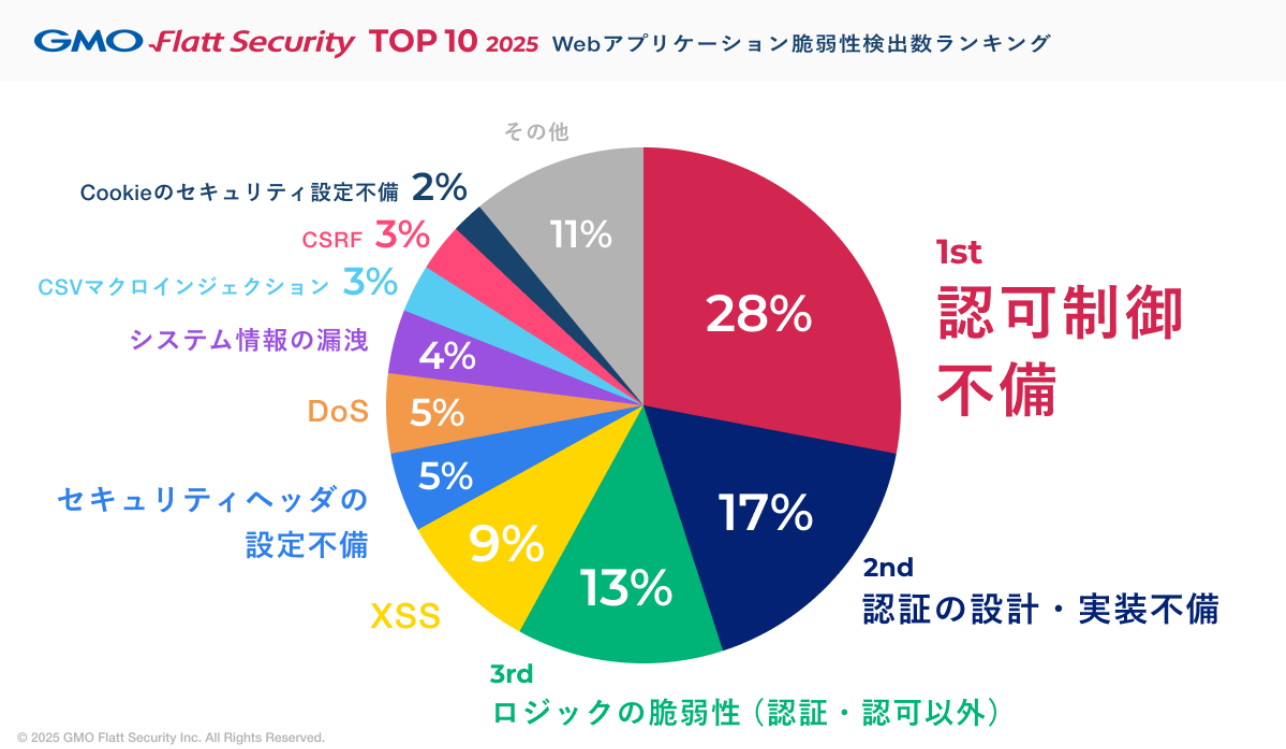
GMO インターネットグループでプロダクト開発組織に向けたサイバーセキュリティ関連事業を展開する GMO Flatt Security 株式会社（代表取締役社長：井手 康貴　以下、GMO Flatt Security）は、Web アプリケーションに存在する脆弱性に関する独自調査の最新版「GMO Flatt Security Top 10 2025」を 2025 年 3 月 3 日に公開しました。

検出数最多の「認可制御不備」をはじめとして、アプリケーションごとに固有の仕様を踏まえる必要がある「ロジックの脆弱性」が半数以上を占める結果となり、一般的な脆弱性対策に留まらない高度な対策の必要性を示す結果となりました。

【調査背景】

Web アプリケーションをはじめとするソフトウェアの脆弱性対策はますますその重要性を増しています。ソフトウェア企業 GitLab は、自社の製品に脆弱性を報告したセキュリティ研究者に対して報奨金を支払う制度（バグ・バウンティ）において、2024 年の 1 年間で 275 個の脆弱性報告を有効と認定し、100 万ドル以上の報奨金を支払ったとするレポートを公開しました。これは世の中のソフトウェアにいかに多数の脆弱性が存在しているかを示唆しています。

こうした脆弱性のうち、現在のトレンドとしてどのようなものが多いか調査したレポートとしては OWASP Top 10 が有名であり、世界中のセキュリティ従事者に参照されています。一方で、このようなグローバルな調査レポートが日本のソフトウェア産業やその中の特定のセグメントの実態にそのまま合致するとは限りません。そこで、日本における Web サービスの内製開発企業を主な顧客層とする GMO Flatt Security が独自調査を実施することで、当該セグメントで日本のソフトウェア産業を支える皆様にセキュリティ上の懸念を適切にお伝えし、最終的にサービスユーザーの皆様の安全に資することを目指します。



【調査概要】

以下の条件のもと脆弱性データを集計し、脆弱性の検出数でランキングを作成。上位 10 個を「GMO Flatt Security Top 10 2025」として公開しています。

- 対象の発見された脆弱性：弊社サービス「脆弱性診断」において Web アプリケーション・Web API を対象に発見された 1000 個以上の脆弱性を分類
- 対象期間：2023 年 1 月 1 日～2024 年 12 月 31 日
- 脆弱性のリスク評価において「informational」と評価されたものは除外

【調査結果】

- 1 位：認可制御不備 **28%**
- 2 位：認証の設計・実装不備 **17%**
- 3 位：ロジックの脆弱性（認証・認可以外） **13%**
- 4 位：XSS（クロスサイト・スクリプティング） **9%**
- 5 位：セキュリティヘッダの設定不備 **5%**
- 6 位：DoS **5%**

- 7 位：システム情報の漏洩 **4%**
- 8 位：CSV マクロインジェクション **3%**
- 9 位：CSRF（クロスサイト・リクエストフォージェリ） **3%**
- 10 位：Cookie のセキュリティ設定不備 **2%**

※各脆弱性が検出数に占める割合の数値は小数第一位を四捨五入しています。

■各脆弱性の解説や技術的な分析は GMO Flatt Security の技術ブログで公開しています。
https://blog.flatt.tech/entry/flatt_top10_2025

【調査結果の分析】

GMO Flatt Security は、1 位の「認可制御不備」、2 位の「認証の設計・実装不備」、3 位の「ロジックの脆弱性（認証・認可以外）」をまとめて「ロジックの脆弱性」と呼称しています。これは各アプリケーションに期待される挙動、すなわちビジネスロジックに反しているかいないかを考慮しないとリスク判断ができないタイプの脆弱性であるということを意味します。

調査結果として、こうした「ロジックの脆弱性」だけで 58%の割合を占めており、中でも 1 位として 28%を占める「認可制御不備」は OWASP Top 10 の最新 2021 年版でも 1 位のリスクと評価されています。セグメントを問わず、現代の脆弱性対策における最重要課題であると考えられます。

一般的にこうした「ロジックの脆弱性」を検出するには、アプリケーションのセキュリティに精通したセキュリティエンジニアが対象のビジネスロジックを理解しながら脆弱性診断を行うような、高コストな対策が必要です。それだけに多くの企業で対策が進んでいないと考えられます。

【望ましい対策】

Web サービスを提供する企業としては「認可制御不備」のような脆弱性が発生しないよう、アプリケーションの適切な設計・実装の重要性について開発組織全体で共通認識を持つことが重要だと考えられます。

一方、セキュリティベンダー側は例えば AI による自動化を通してサービスの提供費用を圧縮するなど、より多くの企業が高度な脆弱性対策にアクセスできるような仕組みづくりが求められます。GMO Flatt Security もこのような課題を解決できるよう鋭意サービス開発を進めてまいります。

【OWASP Japan 代表 / GMO Flatt Security 社外取締役 上野 宣のコメント】

私が取締役を務める GMO Flatt Security への評価になるので手前味噌ですが、まずは認可制御不備をきちんと検出してることが素晴らしく、技術力の高さを示していると思いました。元々は OWASP が開発した「ZAP」などが自動脆弱性診断ツールとしては有名ですが、こうしたツールでは認可制御不備やロジックの脆弱性は検出できません。ツールも進化してきましたが、依然これらの脆弱性は「最後の砦」のように残っ

ている現状が今回の調査で示されたと言えます。まずは大きなリリースの前の手動脆弱性診断での対策を推奨しつつ、ツールのさらなる進化にも期待したいです。

【GMO Flatt Security 株式会社について】

GMO Flatt Security は「エンジニアの背中を預かる」をミッションに、業界を問わず DX 推進・ソフトウェア開発のセキュリティを支援してきた、日本発のセキュリティプロフェッショナル企業です。セキュリティ製品の自社開発や様々な企業へのセキュリティ支援、徹底したユーザーヒアリングを通じて得た知見を元に、一つひとつの顧客組織に寄り添った伴走型のセキュリティサービスを提供しています。

■「エンジニアの背中を預かる」ための、エンジニア向けサービス群

・Web&クラウドまるごと脆弱性診断ツール「Shisho Cloud byGMO」
URL： https://shisho.dev/ja
・セキュリティエンジニアによる手動脆弱性調査・分析サービス「脆弱性診断」
URL：https://flatt.tech/assessment
・クラウド型セキュアコーディング学習プラットフォーム「KENRO byGMO」
URL： https://flatt.tech/kenro

以上

【報道関係お問い合わせ先】

●GMO Flatt Security 株式会社　広報
E-mail：pr@flatt.tech

●GMO インターネットグループ株式会社
グループ広報部　PR チーム　田部井
TEL：03-5456-2695
お問い合わせ：https://www.gmo.jp/contact/press-inquiries/

【GMO Flatt Security 株式会社】（URL：https://flatt.tech）

会社名	GMO Flatt Security 株式会社
所在地	東京都渋谷区桜丘町 26 番 1 号 セルリアンタワー
代表者	代表取締役社長　井手 康貴
事業内容	■サイバーセキュリティ関連サービス
資本金	4 億 3,042 万円（資本準備金含む）

【GMO インターネットグループ株式会社】（URL：https://www.gmo.jp/）

会社名	GMO インターネットグループ株式会社　（東証プライム市場　証券コード：9449）
所在地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代表者	代表取締役グループ代表　熊谷 正寿
事業内容	持株会社（グループ経営機能） ■グループの事業 インターネットインフラ事業 インターネットセキュリティ事業 インターネット広告・メディア事業 インターネット金融事業 暗号資産事業
資本金	50 億円