PRESS RELEASE

2025 年 3 月 5 日

報道関係各位

GMO Flatt Security 株式会社

GMO Flatt Security、国産脆弱性診断ツール「Shisho Cloud byGMO」内で AI を活用した認可制御診断機能を提供開始

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、2025 年 3 月 5 日より国産脆弱性診断ツール「Shisho Cloud byGMO」（読み：シショウ クラウド バイジーエムオー URL：https://shisho.dev/ja ）内で Web アプリケーションの認可制御診断機能を提供いたします。

これにより、情報漏洩などの重大なインシデントの原因となりやすい脆弱性「認可制御不備」を自動で検知することができるようになり、従来はセキュリティエンジニアによる手動脆弱性診断等の高コストなサービスを利用しなければ進まなかった脆弱性への対策が、継続的かつ低コストで実施可能となります。

■「Shisho Cloud byGMO」認可制御診断イメージ動画

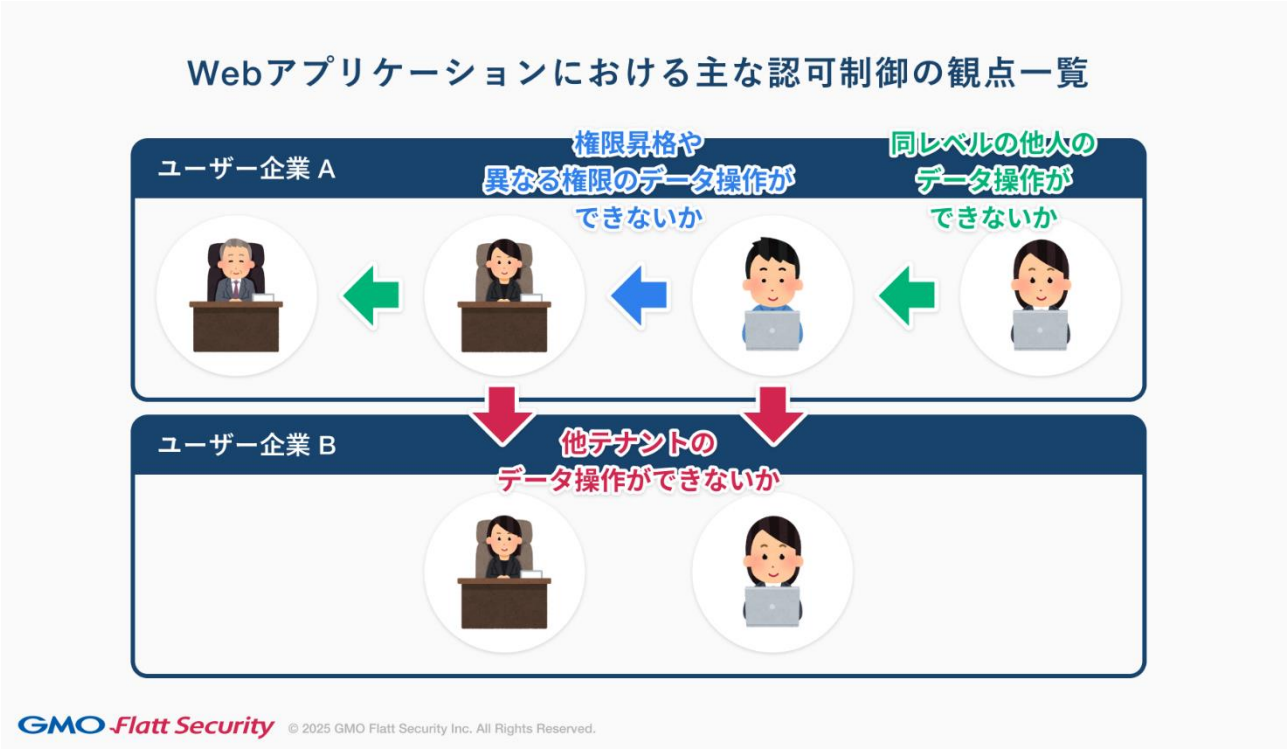
https://youtu.be/8UfUo1yj0AU

【認可制御診断機能　提供の背景】

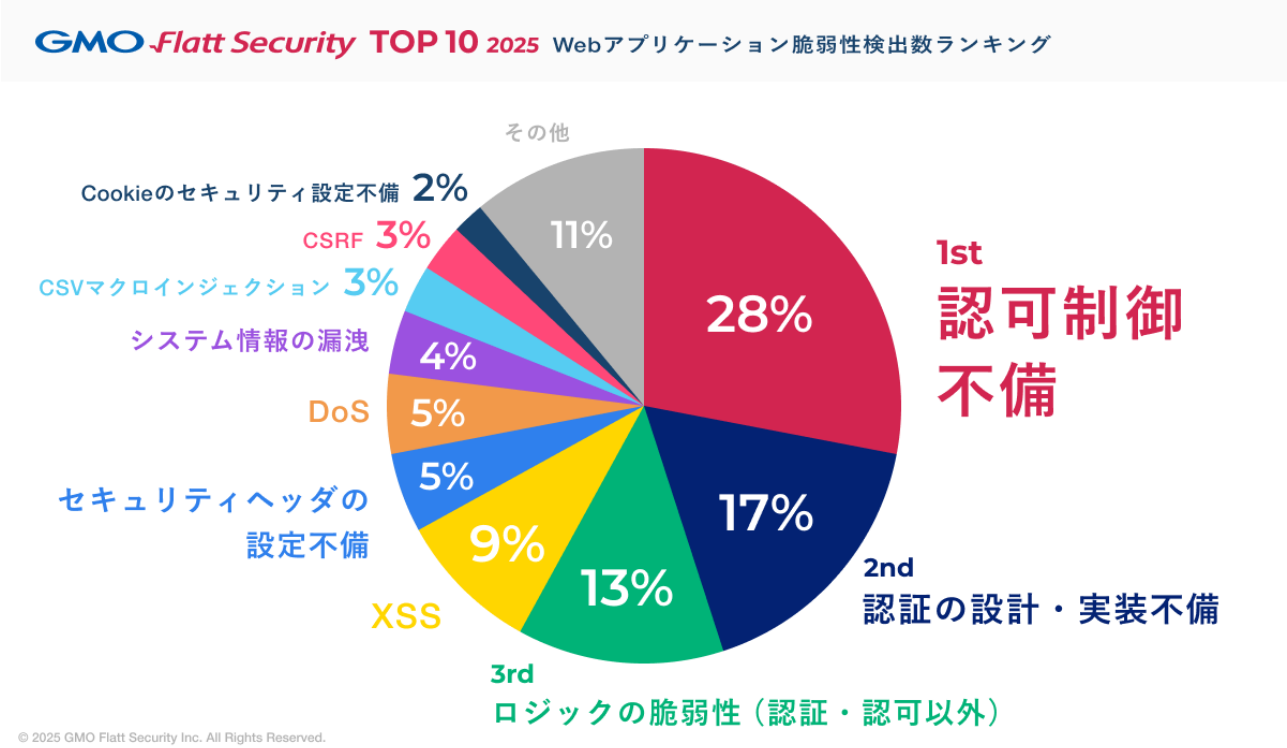
■「認可制御不備」とは

認可制御とは、Web アプリケーションのユーザーに対して、付与されたアクセス権限通りの操作のみを許し、それ以外の操作を禁止する制御のことです。そのような制御があるべき箇所に実装されていなかったり、制御を迂回して本来禁止された操作を実行できたりしてしまう脆弱性を「認可制御不備」と呼びます。

脆弱性が存在すると、一般ユーザーでありながら全ユーザーの個人情報が閲覧できてしまうなど、情報漏洩をはじめとする様々なリスクに直結します。



■「認可制御不備」は現代の Web アプリケーションにおける最大のリスク



「認可制御不備」は、現代の Web アプリケーションにおける最大のリスクと言うことができます。実際に、世界中のセキュリティ従事者に参照されるグローバルな調査リポート「OWASP Top 10[※1]」の最新 2021 年版において第 1 位のリスクとされています。一つ前のバージョンである 2017 年版では第 5 位だったところから大幅に順位を上げています。

加えて、「認可制御不備」は弊社独自の調査リポート「GMO Flatt Security Top 10[※2]」2025 年版でも 1 位の脆弱性となっています。単純な検出数が 1 位であることに加えて、母集団を脆弱性深刻度「高」「重大」のみに絞り込んでも全体の 25%を占める検出数 1 位の脆弱性となっています。

※1 OWASP Top 10：https://owasp.org/Top10/ja/

※2 GMO Flatt Security Top 10 2025 年版：https://blog.flatt.tech/entry/flatt_top10_2025

■「認可制御不備」の対策が進まない理由

上記のリポートの示す通り、「認可制御不備」は多くの企業で対策が進んでおらず、リスクとして残存していると考えられます。

「認可制御不備」を検出するには、セキュリティエンジニアがアプリケーションの仕様を理解した上で脆弱性診断を実施する等の対策が必要です。しかし、こうした対策は専門家の稼働を必要とするため高コストになりがちであり、アジャイル開発の頻繁なアップデートに応じた頻度で実施することは多くの場合難しいものになります。

「認可制御不備」の対策のこのような特性が、多くの企業で脆弱性が残存している理由になっていると考えられます。弊社も脆弱性診断サービスの提供の中で多くの「認可制御不備」を検出してきましたが、全てのお客様に同様の価値提供ができていない点を課題と認識していました。

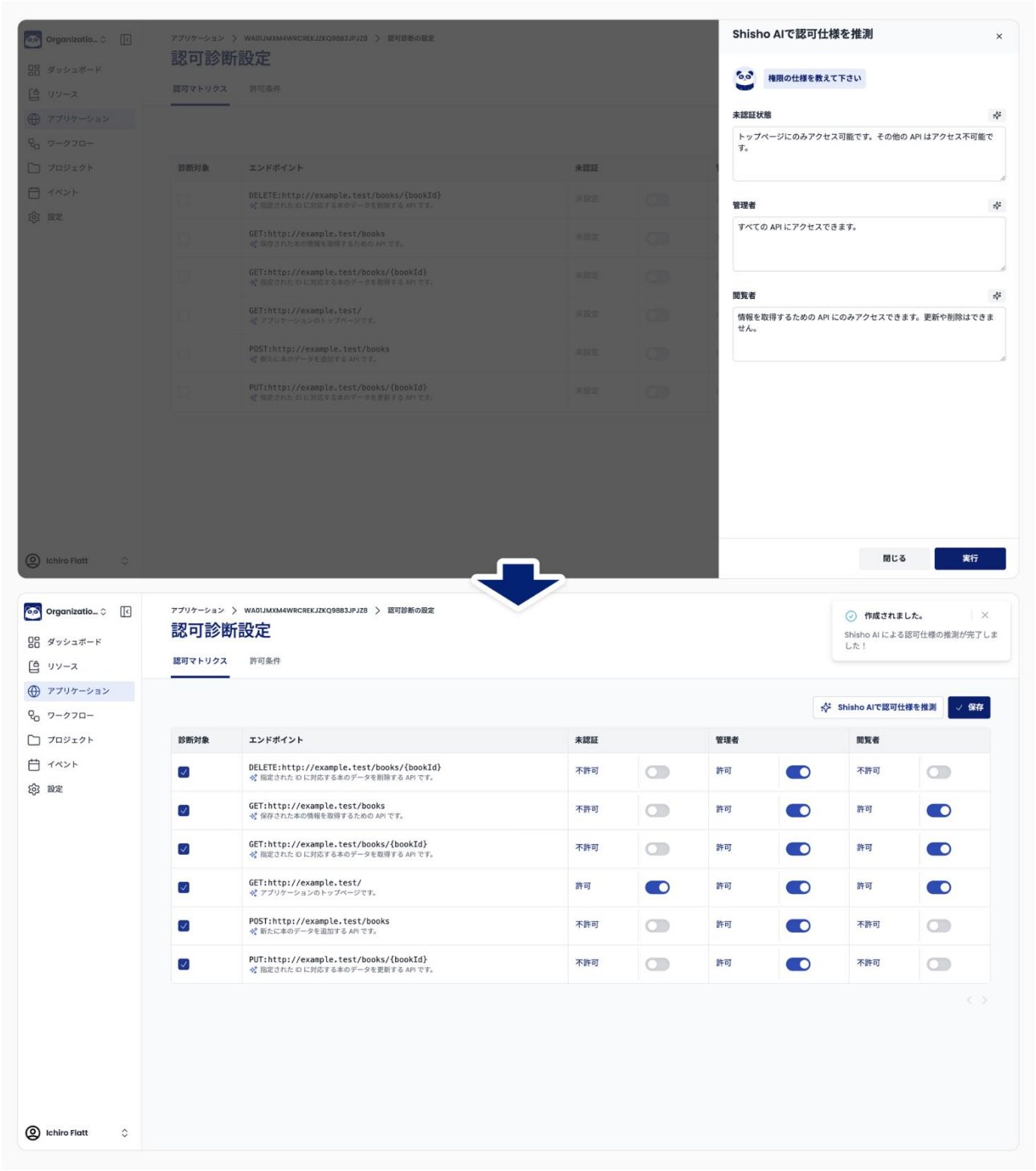
【「Shisho Cloud byGMO」の認可制御診断機能の概要】

前述の通り、「認可制御不備」の検出にはセキュリティエンジニアによるアプリケーションの仕様理解が必要でした。今回、AI を活用しこのような人間しかできなかった部分を推論させることにより「Shisho Cloud byGMO」において認可制御診断機能を提供可能となりました。人間を介さず自動化されたプロセスとして認可制御診断を提供することにより、これまでより安価にかつ継続的に「認可制御不備」の対策を実施可能になります。なお、本機能は Starter プラン以上の全てのお客様に利用いただけます。

【「Shisho Cloud byGMO」の認可制御診断機能の特徴】

1. AI が権限マトリクスを自動で推測・提案

AI がアプリケーションの仕様を把握し、権限ごとに可能な操作を一覧化した権限マトリクスを自動で作成します。権限ごとに実際にアプリケーションにリクエストを送信し、挙動が権限マトリクスに沿っているかどうかを自動で診断します。なお、提案された権限マトリクスが不正確な場合でも人の手で修正することができます。



2. 開発サイクルに合わせた頻度で継続的に診断

自動脆弱性診断ツールである「Shisho Cloud byGMO」であれば開発サイクルに合わせた継続的な脆弱性診断が可能です。アジャイル開発で随時追加・変更されていく機能にも、正しく認可制御を実装できているかを、機能リリースの度に洗い出すことができます。

3. 低コストにアプリ全体を診断

AI を活用し認可制御診断のフロー全体を自動化したことにより、手動脆弱性診断と比べ費用を大幅に削減できます。例えば、年に一度の手動脆弱性診断で約 500 万円の費用が必要であるのに対し、「Shisho Cloud byGMO」であれば年間 150 万円（税抜き／Starter プラン）で継続的に自動診断が可能です。これ

まで予算の都合で「認可制御不備」を診断できなかった、あるいは診断対象を絞らざるを得なかったお客様にも提供しやすくなりました。

【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

※ 記載されている会社名及び製品名は、各社の商標または登録商標です。

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