2026 年 10 月 21 日

報道関係各位

GMO Flatt Security 株式会社

GMO Flatt Security、AI が会社全体への侵入を試みる「不正アクセス抜き打ちテスト byGMO」を提供開始

～攻撃者と同じ手法で公開資産を洗い出し、30 日の期間内に抜き打ちで AI が侵入を試行～

GMO インターネットグループで「エンジニアの背中を預かる」をミッションに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、2026 年 10 月 21 日（水）より、AI 主導のペネトレーションテストサービス「不正アクセス抜き打ちテスト byGMO」の提供を開始しました。

本サービスは、会社全体を対象に、攻撃者と同じ立場から不正アクセスされうるかを検証します。公開資産を探索し、見つかった資産をすべて対象とするため、お客様が把握していない資産も含めて広範囲を検証できます。さらに、AI がさまざまな攻撃手法を駆使して侵入を試みるため、多角的かつ高精度にリスクを検証できます。2026 年 12 月 31 日（木）までのお申し込みに限り、対象の規模にかかわらず一律 98 万円（税抜）でご提供します。

・「不正アクセス抜き打ちテスト byGMO」サービスページ：
https://flatt.tech/assessment/nukiuchi

【提供開始の背景：不正アクセス事案が急増。AI が主導する攻撃の観測も】

■不正アクセス事案が急増。広範囲で「組織ごとに固有の弱点」が狙われる

JPCERT/CC は 2026 年 10 月 8 日、国内組織で相次いでいる不正アクセスについて注意喚起を公表しました(※1)。CVE 番号で識別されるような既知の脆弱性やありがちな設定不備を狙う攻撃に加え、公開されているスマートフォンアプリを解析して API の情報を割り出し、不正な操作を行う攻撃などが報告されています。BI ツールや従業員向け管理システムなど、一般の利用者向けではない社内システムが侵害される場合もあるとされています。

■攻撃キャンペーンにおける AI 活用の観測

Wiz CIRT は AI が主導する攻撃の増加を観測し、これらの AI は様々なプラットフォーム上で侵入を実現する横断的な能力を有し、かつ同時並行で攻撃が実行されると分析しています(※2)。AI は標的の技術構成に関わらず、広範囲に対して自律的に固有の弱点を突く攻撃を実行することができると言えます。

こうした攻撃に対しては、既知の脆弱性の有無をスキャンするだけでは対処できません。また、個々のシステムを決められた範囲で検査するだけでは不十分と言えます。攻撃者は、企業が把握していない公開資産や、検査の対象外としていた環境も含めて、会社全体から侵入できる経路を探します。そのため企業には、「攻撃者から自社がどう見えているか」「実際に侵入されうるか」を、攻撃者と同じ立場で確かめることが求められています。

■攻撃者と同じ立場で、会社全体のシステムへの侵入を試す

一般的な脆弱性診断は検証できる領域がアプリケーション単体に閉じてしまいます。また、ペネトレーションテストは、事前の打ち合わせで対象範囲やシナリオを決めて実施するため、範囲外の資産や想定外の攻撃経路は検証の対象になりづらい傾向があります。加えて、これらのサービスは個別のお見積もりとなるため実施のハードルが高く、今まさに高まっている脅威に迅速に対抗しづらいという課題もありました。

そこで GMO Flatt Security は、攻撃者と同じく対象範囲を絞らず、会社全体のシステムへの侵入を試みるペネトレーションテスト「不正アクセス抜き打ちテスト byGMO」の提供を開始します。お見積もりプロセスは不要で、一律の料金で提供しました。

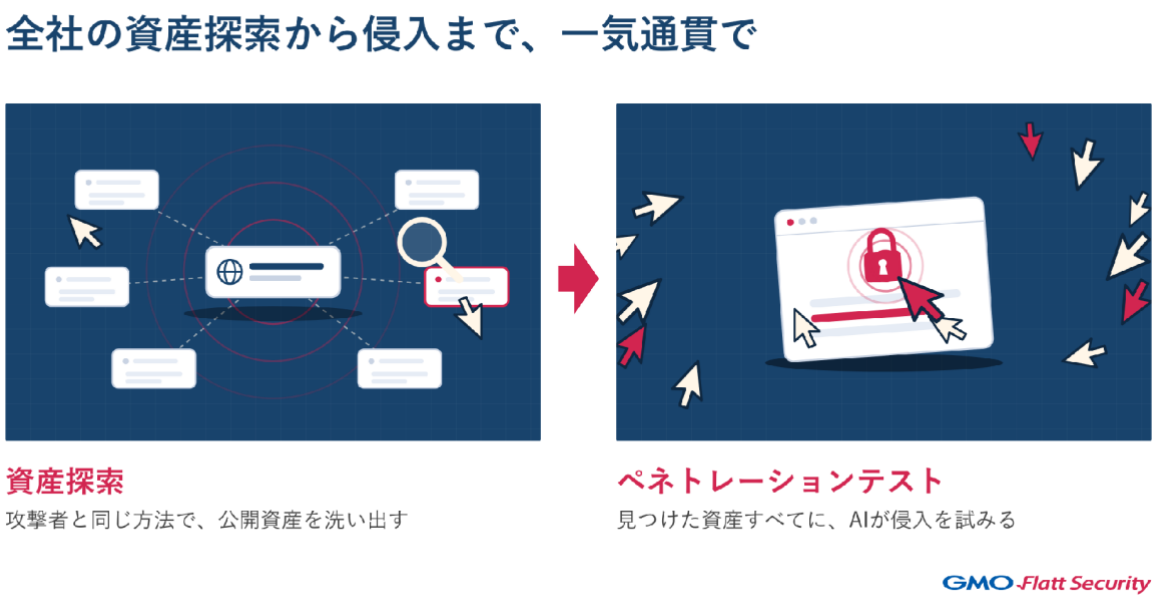
※1 JPCERT/CC「直近で相次いでいる国内組織における不正アクセスに関する注意喚起」（2026 年 10 月 8 日公表、10 月 9 日更新） https://www.jpcert.or.jp/at/2026/at260030.html

※2 Wiz Blog「Loud, Fast, and Everywhere: Anatomy of a Real AI-Driven Cloud Attack」（2026 年 10 月 19 日公表）

https://www.wiz.io/blog/anatomy-of-ai-driven-cloud-attacks

【「不正アクセス抜き打ちテスト byGMO」とは】

「不正アクセス抜き打ちテスト byGMO」は、攻撃者と同じ立場で、会社全体に不正アクセスされる恐れがあるかを AI で検証するペネトレーションテストです。GMO Flatt Security のセキュリティエンジニアが AI エージェント群を指揮し、「個人情報・お客様の保有する情報の奪取、あるいはシステムの掌握」をゴールに、外部から事前知識のない状態で攻撃を試みます。



■特長

1. ドメインを起点に資産探索から実施し、会社全体を対象に

お客様にご用意いただくのは、必ず対象に含めたいドメインの一覧のみです。GMO Flatt Security がそのドメインを起点に、攻撃者と同じ方法でインターネット上の公開資産を洗い出し（ASM：Attack Surface Management の手法を活用）、お客様にご承認いただいた資産すべてを攻撃の対象とします。お客様が把握していなかった資産も、攻撃経路として検証されます。

2. 30 日の期間内で、「抜き打ち」で実施

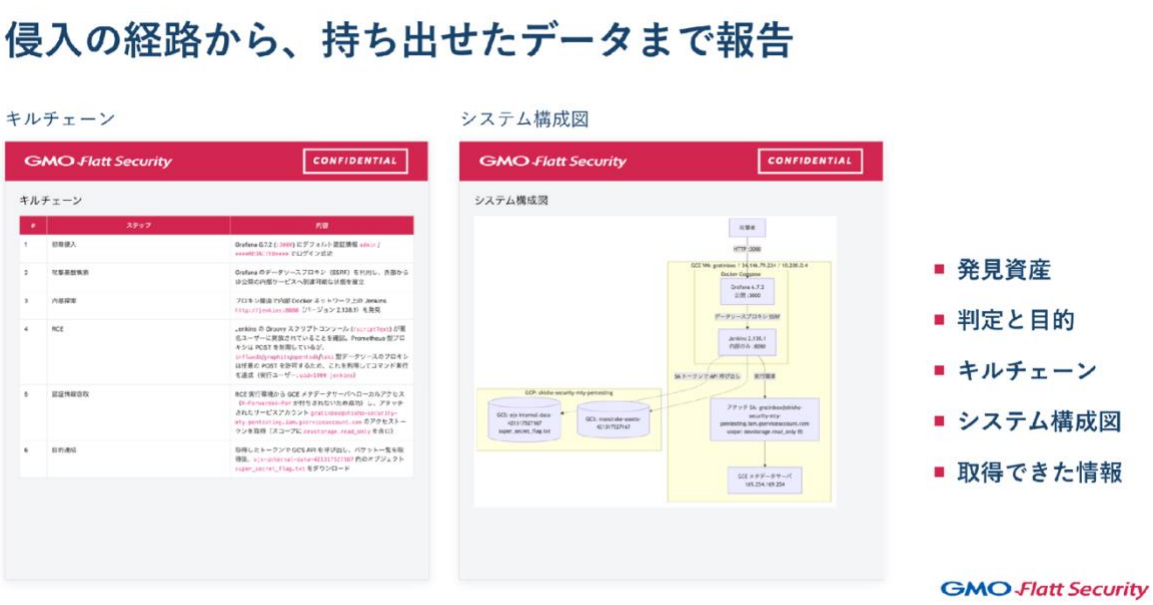
実際の攻撃者は、攻撃の日時を予告しません。本サービスも、30 日の実施期間内で、事前のお知らせなくテストを行います。

3. 既知の脆弱性から、組織固有の脆弱性まで多角的に攻撃

ネットワークレイヤからアプリケーションレイヤまでを対象に、ソフトウェアの既知の脆弱性の悪用と、新たな脆弱性の発見・悪用の両面から攻撃を試みます。

4. 重大なリスクは、期間の終了を待たずに速報

重大な不正アクセスが可能な状態を見つけた時点で、期間の終了を待たずに速報でお知らせします。速報・最終報告書のいずれも、発見資産、目的（侵入・情報取得）の達成可否、初期侵入から目的達成までのキルチェーン（侵入プロセスの連鎖）、攻撃経路を示したシステム構成図、実際に取得できた情報をご報告します。



■ご利用の流れ

1. お申し込み：申込書への同意をもって開始します
2. ドメインの共有：必ず対象に含めたいドメインをご共有いただきます
3. 対象範囲のご承認：GMO Flatt Security が発見した攻撃対象の一覧をご確認いただき、除外したい資産を除いたうえでご承認いただきます
4. 30 日の期間の抜き打ちテスト：期間中に抜き打ちで、AI が多角的に侵入を試みます
5. 速報と報告書：重大な問題は速報でお知らせし、最後に最終報告書をご提出します

■料金

2026 年 12 月 31 日（木）までのお申し込みに限り、一律 98 万円（税抜）。対象規模による変動はありません。

【ウェビナー開催：急増する AI 不正アクセス、今取り組んでほしいこと ～「年次×1 アプリ診断」から「毎日×全社 AI ペネトレ」へ～】

本サービスのリリースに伴い、AI による攻撃の脅威と対策について解説するウェビナーを開催します。

■オンラインセミナー概要

・タイトル：急増する AI 不正アクセス、今取り組んでほしいこと ～「年次×1 アプリ診断」から「毎日×全社 AI ペネトレ」へ～
・開催日時：2026 年 10 月 27 日（火）・11 月 5 日（木） 各日 12:00～13:00
・開催形式：オンライン
・参加費：無料
・登壇者：GMO Flatt Security 執行役員 豊田恵二郎
・お申込先：当セミナーの Web ページよりお願いいたします。

【今後の展望】

GMO Flatt Security は、AI を活用する攻撃者の脅威が高まる中、攻撃者と同じ立場から企業のセキュリティを継続的に検証できる体制づくりを支援してまいります。今後は、本サービスを定期的に実施できる年間プランの提供も予定しています。

【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

・脆弱性診断・ペネトレーションテスト
URL：https://flatt.tech/assessment
・AI で会社全体への侵入を試すペネトレーションテスト「不正アクセス抜き打ちテスト byGMO」
URL：https://flatt.tech/assessment/nukiuchi

・セキュリティ診断・ソフトウェアサプライチェーン攻撃対策特化の AI エージェント「Takumi byGMO」
URL：https://flatt.tech/takumi
・AWS 等クラウドの継続的な診断ツール（CSPM）「Shisho Cloud byGMO」
URL：https://shisho.dev/ja
・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　望月
TEL：03-5456-2695
お問い合わせ：https://group.gmo/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

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

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） ■グループの事業内容 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

Copyright (C) 2026 GMO Flatt Security Inc. All Rights Reserved.