2026 年 5 月 26 日

報道関係各位

GMO Flatt Security 株式会社

GMO Flatt Security、「ソフトウェアサプライチェーン診断」および「ソフトウェアサプライチェーン攻撃演習」を提供開始

～依存パッケージ侵害から CI/CD・権限設計、ソースコード漏洩時のリスクまで横断評価。開発チーム向けインシデント対応の机上演習も同時提供～

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 5 月 26 日（火）より開発組織向けにソフトウェアサプライチェーン攻撃対策を支援する「ソフトウェアサプライチェーン診断」および「ソフトウェアサプライチェーン攻撃演習」の提供を開始いたします。

「ソフトウェアサプライチェーン診断」とは、依存パッケージの管理から CI/CD 環境の構成・権限設計までを対象に、侵害時の被害範囲と対応優先度を可視化する診断サービスです。攻撃が成立した場合に、認証情報・機密情報・個人情報の漏えいの被害がどこまで拡大するかシミュレーションすることが可能です。また、「ソフトウェアサプライチェーン攻撃演習」は「axios」など実際に発生した侵害事例をもとに、開発チーム自らがインシデント対応と判断を実践する机上演習サービスです。

両者を組み合わせることで、ソフトウェアサプライチェーン上のリスクの可視化からインシデント発生時に開発チームが自ら動ける体制の構築まで、開発パイプライン全体の堅牢化を一貫して支援いたします。

【提供開始の背景：相次ぐソフトウェアサプライチェーン攻撃】

■ソースコードリポジトリ・CI/CD 環境の侵害による、認証情報と個人情報の流出リスク

2026 年初頭から多発しているソフトウェアサプライチェーン攻撃は、ソースコードリポジトリや CI/CD

環境にまで被害が及ぶケースが多く、認証情報・個人情報の流出リスクが深刻化しています。

3 月には週間 1 億ダウンロード超の主要パッケージ「axios」が侵害され、悪意のあるパッケージが依存関係に追加されました [(*1)]。また、4 月にはパスワード管理ツール「Bitwarden」の公式パッケージが侵害され、開発者の認証情報を窃取するマルウェアが配布される事案が確認されています [(*2)]。

こうした攻撃では、開発者端末の侵害だけでなく、ソースコードや CI/CD 環境に含まれる「認証情報・機密情報・個人情報」の漏えいのリスクが深刻です。これらには API キー・アクセストークン等の認証情報が集約されている上、場合によっては個人情報を含む実データの一部が残されているケースもあり、漏えいした認証情報を起点に連携サービスへの二次被害にまで発展しかねません。

攻撃の最大の特徴は、正規のレジストリから正規のコマンド（npm install 等）によりパッケージをインストールするだけで感染が成立する点にあります。開発者が業務で行うごく当たり前の作業が、組織全体を揺るがす重大なリスクに直結しているといえます。

■高度化する脅威に備え、ツールとプロフェッショナルの両面でソフトウェアサプライチェーンを堅牢化

こうした脅威に対し、GMO Flatt Security は 2026 年 3 月より、「Takumi byGMO」の「Guard」機能による悪性パッケージの自動ブロックや、「Runner」機能による CI/CD 実行トレースの可視化など、ソフトウェアサプライチェーン防御のための機能を提供してまいりました。 [(*3)]

今回提供を開始する「ソフトウェアサプライチェーン診断」および「ソフトウェアサプライチェーン攻撃演習」は 、セキュリティのプロフェッショナルが CI/CD 環境の構造的なリスク評価と開発チームの対応力強化を支援するサービスです。ソフトウェア開発者が直面するセキュリティ課題に対し、ソフトウェアサプライチェーン防御支援をさらに強化してまいります。

（*1）https://blog.flatt.tech/entry/axios_compromise（axios ソフトウェアサプライチェーン攻撃の概要と対応指針）

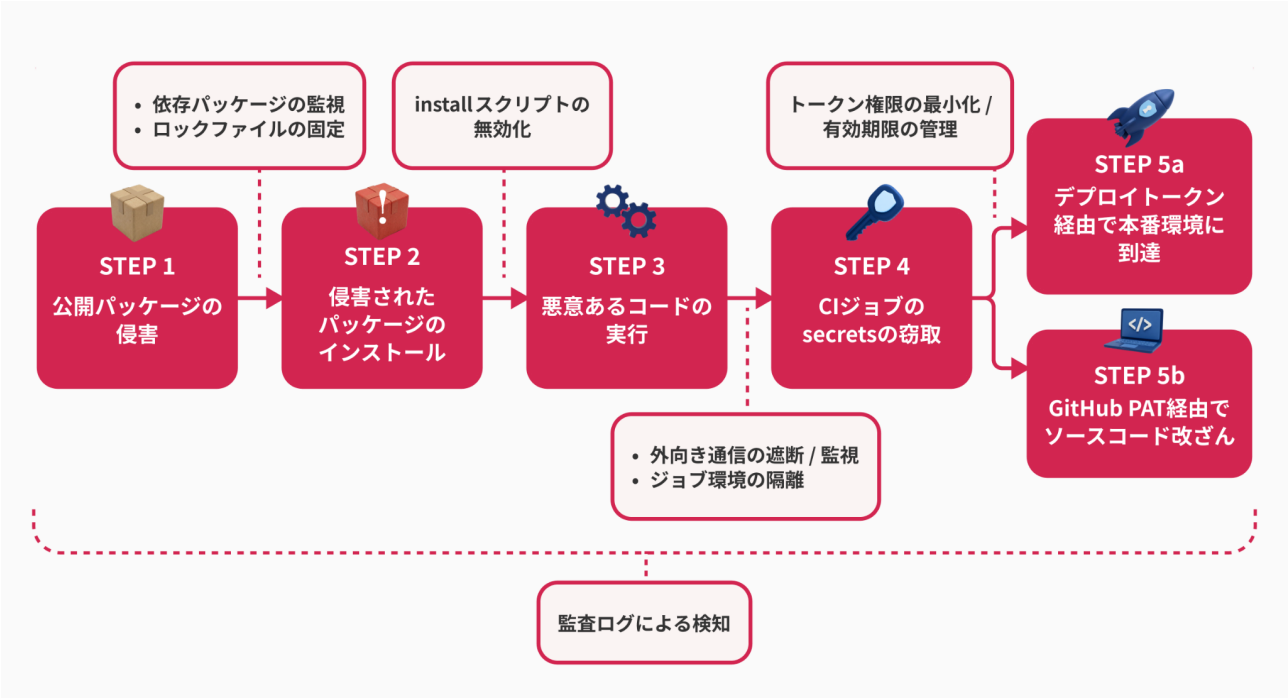
（*2）https://blog.flatt.tech/entry/bitwarden_compromise（Bitwarden ソフトウェアサプライチェーン攻撃の概要と対応指針）

（*3）https://prtimes.jp/main/html/rd/p/000000067.000027502.html（「Takumi byGMO」、ソフトウェアサプライチェーン攻撃対策領域へ進出 コード一行の設定で、開発環境のマルウェア感染防止・有事対応支援を実現 ）

【「ソフトウェアサプライチェーン診断」とは】

■診断概要

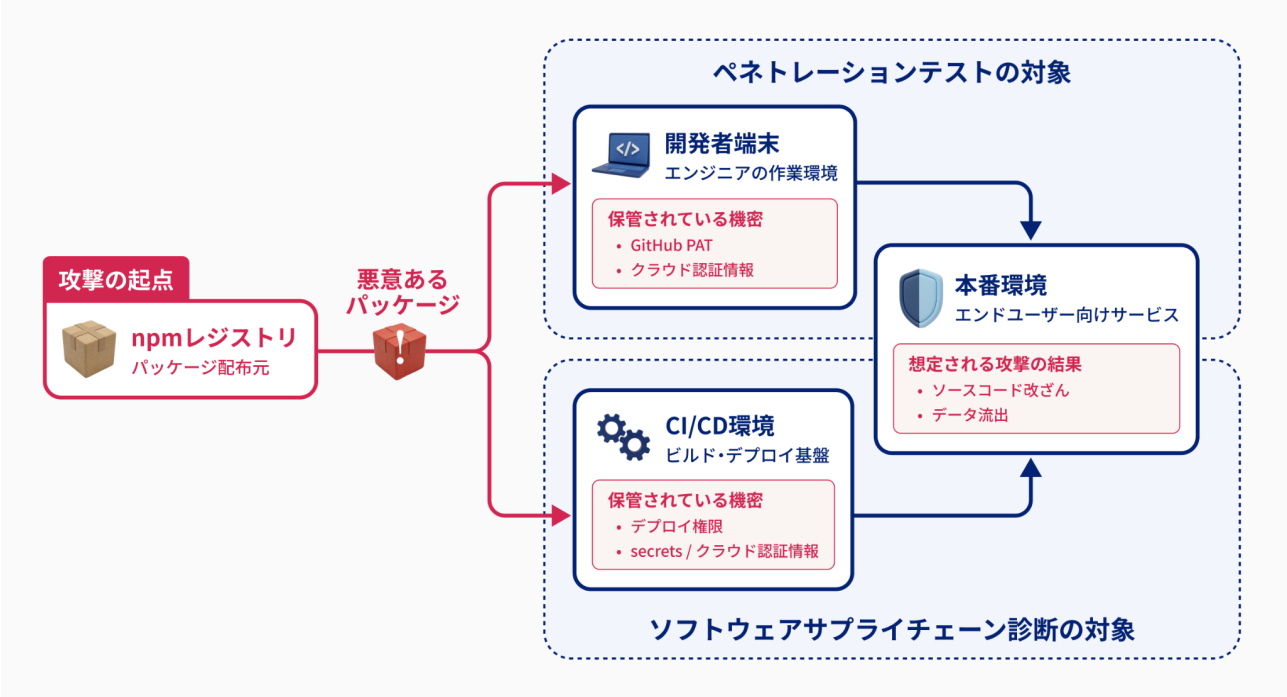
本診断は、対象組織の依存関係に含まれるパッケージやソースコードリポジトリが侵害された場合に、「自社の環境ではどの段階で攻撃が止まるか」を評価します。一般的なチェックリスト型の評価とは異なり、対象組織の環境で実際に成立しうる攻撃経路をシミュレーションし、防御の各段階で何が機能し何が機能しないかを明らかにします。リポジトリ内に残された機微情報や依存パッケージの管理状況、CI/CD の環境の隔離・通信制御、トークン権限の分離度、インシデント時の追跡可能性までを横断して対象とし、被害シナリオに基づく優先順位付きのアクションリストを導出します。



■既存の開発者端末のペネトレーションテストと診断は補完関係にある

ソフトウェアサプライチェーン攻撃において多くの企業が懸念するのは、開発者端末の侵害です。悪意あるパッケージの実行により端末が侵害されると、そこに保存された GitHub や各種クラウド環境の認証情報を足がかりに、ソースコードの改ざんや本番環境への侵入にまで到達する可能性があるためです。

GMO Flatt Security では、既に提供中のペネトレーションテスト[(*4)]において、悪意あるパッケージによる端末侵害を起点に、実際にどの認証情報・システムに到達できるかを実証的に評価しています。一方、ソフトウェアサプライチェーン診断は端末侵害の検証だけではカバーしきれない、CI/CD 環境の構成や権限設計に起因するリスクが対象です。ペネトレーションテストが開発者端末の侵害を実証的に検証するのに対し、本診断は CI/CD 環境の設定・権限設計を構造的に評価します。両者を組み合わせることで、開発者端末と CI/CD 環境の双方からソフトウェアサプライチェーンのリスクを評価することが可能です。



(*4) https://flatt.tech/assessment/penetration_test

・ソフトウェアサプライチェーン診断 Web サイト：http://flatt.tech/assessment/ssc

【「ソフトウェアサプライチェーン攻撃演習」とは】

■演習概要

本演習は、「axios」や「Bitwarden CLI」等の実際の侵害事例に基づき、開発チームが主体となってインシデント対応を体験する机上演習（TTX）です。（1）事前ブリーフィング（2）演習本体（3）振り返りの 3 フェーズで構成されます。「ソフトウェアサプライチェーン診断」の結果を踏まえて実施することで、自社環境の実態に基づいたシナリオでの演習が可能になります。

■ソフトウェアサプライチェーン攻撃演習の特長：開発チーム向け

最大の特徴は、開発チームが中心となってインシデント対応を実施する場合を想定している点です。

ソフトウェアサプライチェーン攻撃によるインシデントは、「自社の開発環境が影響を受けているか」の判定から対応が始まります。その際、パッケージの利用状況や CI の実行履歴・CI/CD 設定といった、その企業の開発現場の理解が欠かせません。セキュリティチームだけでは完結できない領域で、開発チームが中心となって調査・判断する体験を提供します。

・ソフトウェアサプライチェーン攻撃演習 Web サイト：http://flatt.tech/assessment/ssc/exercise

【今後の展望】

今後も、ソフトウェアサプライチェーン攻撃は多様化・高度化すると予想されます。その中で、GMO Flatt Security はコーポレートミッション「エンジニアの背中を預かる」のもと、「Takumi byGMO」の「Guard」・「Runner」機能をはじめ、ソフトウェア開発者の皆様が安心して開発に専念できる環境の実現に取り組んでまいります。

【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

・セキュリティエンジニアによる「脆弱性診断・ペネトレーションテスト」
URL：https://flatt.tech/assessment
・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

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.techpr@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
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://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