

2026 年 10 月 1 日

報道関係各位

GMO インターネット株式会社
GMO Flatt Security 株式会社

『ConoHa VPS byGMO』、AI エージェント開発環境に 悪意あるプログラム部品の侵入を防ぐ機能を無料で同梱 ～「Takumi byGMO」の「Guard」機能を標準提供、コマンド 1 行で有効化～

GMO インターネットグループの GMO インターネット株式会社（代表取締役 社長執行役員：伊藤 正 以下、GMO インターネット）が提供する『ConoHa VPS byGMO』（URL：<https://vps.conoha.jp/>）は、AI エージェント系スタートアップスクリプトの対象テンプレート 7 種に「Guard」機能^{（※1）} 専用スクリプトの無料同梱を、2026 年 9 月 25 日（金）より開始しました。これにより利用者は、AI エージェントの実行環境を構築した後、コマンド 1 行で悪性パッケージ対策を有効化できるようになります。



「Guard」機能は、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）が提供する「Takumi byGMO」（URL：<https://flatt.tech/takumi>）の機能です。パッケージレジストリ^{（※2）} から開発環境にプログラム部品が届く間に介在し、悪意あるプログラム部品（悪性パッケージ）のダウンロードを自動でブロックします。今回の同梱により、個人開発者や少人数チームでも、複雑な設定を行わずに対策を導入しやすくなります。

（※1）『Takumi byGMO』は、GMO Flatt Security が開発・提供しているサービスで、「Guard」機能はその中のソフトウェアサプライチェーン攻撃対策を担う機能です。

（※2）プログラムを組み立てるための部品（ソフトウェアパッケージ）を開発者が登録・公開し、他の開発者がダウンロードして利用できるようにする中央管理サービス。

【提供開始の背景】

生成 AI の活用拡大に伴い、ソフトウェア開発の現場では、AI が自律的にオープンソースのプログラム部品（ソフトウェアパッケージ）を取り込む開発スタイルが一般化しつつあります。一方で、パッケージレジストリに悪意ある部品を紛れ込ませ、開発環境や CI/CD 環境を侵害する「ソフトウェアサプライチェーン攻撃」への対策ニーズも高まっています。こうした状況を受け、悪性パッケージの侵入を防ぐ「Guard」機能の

利用は急速に拡大し、2026 年 8 月には 1 日あたり 5,000 万件を超えた日を観測しました^(※3)。激化する攻撃の中で、より多くの方に対策を行っていただくために、GMO インターネットは GMO Flatt Security と連携し、『ConoHa VPS byGMO』の AI エージェント系テンプレートに「Guard」機能の管理スクリプトを同梱することといたしました。これにより利用者は、AI エージェントの開発環境を構築した後、追加費用なしでサプライチェーン攻撃対策を導入しやすくなります。

(※3) GMO Flatt Security、「ソフトウェアサプライチェーン 脅威レポート 2026」を公開 ～半年で悪性パッケージ約 3 万 1,000 件を検出・Takumi Guard は 1 日 5,000 万件超のパッケージダウンロードを検査～ (<https://group.gmo/news/article/10179/>)

【「Guard」機能について】

「Guard」機能は、「ソフトウェアの部品を、受け取る前に検品してくれる仕組み」です。パッケージレジストリとエンジニアの開発環境の間に介在し、パッケージの取得リクエストを透過プロキシ経由に切り替えることで、ダウンロード時に悪性の有無をリアルタイムで検証します。悪性と判定されたパッケージは、開発者の端末や CI/CD 環境に到達する前に自動でブロックされます。当機能の中核にあるのは、GMO Flatt Security が独自に構築・運用するブロックリストです。このブロックリストは、npm に公開されている全パッケージを対象とした検査により、常に更新され続けています。加えて GMO Flatt Security のリサーチチームが検査精度を継続的に検証・改善しています。すでにインストールされたパッケージを事後的にスキャンする仕組みとは異なり、インストール時に介入するため、悪性パッケージの侵入そのものを未然に防ぎます。

「Guard」機能が対応するパッケージエコシステムは、npm/pip・uv/RubyGems/Go modules/Composer です^(※4)。

■同梱対象のテンプレート (計 7 種)^(※5)

AI コーディングエージェント系の「Claude Code」「Codex CLI」「OpenCode」「Antigravity CLI」と、AI タスク実行エージェント系の「OpenClaw」「NanoClaw」「Hermes Agent」の計 7 種のテンプレートに、「Guard」機能を設定するための専用スクリプトを同梱します。

■主な特長

1. サーバー構築後、コマンド 1 行でサプライチェーン攻撃対策を導入できる

AI エージェントの実行環境を自動構築するスタートアップスクリプトに専用スクリプトが同梱されるため、利用者は環境構築後に別途対策ツールを探して導入する必要がありません。VPS 上にインストール済みのパッケージマネージャーを自動検出し、検出されたものだけに設定を適用するため、作業時間の短縮や設定ミスの防止につながります。

2. 利用者が必要に応じて任意で有効化できる

スタートアップスクリプトの実行時点では「Guard」機能は有効化されません。利用者が必要に応じて専用スクリプトを実行した時点で有効化される設計です。

3. 専用スクリプトで状態確認から有効化・無効化まで管理できる

「Guard」機能は、独立した専用スクリプトとして提供し、状態確認、有効化、登録、認証、更新、無効化を行えます。主なコマンドは takumi-status、takumi-enable、takumi-register、takumi-login、takumi-renew、takumi-disable です^(※6)。

4. 用途に応じて 2 つの利用モードを選ぶ

①メール登録を行わず、悪性パッケージのブロックのみを行う匿名モード (takumi-enable) と、②メール認証でトークンを取得し、ダウンロードの追跡や侵害の通知を受けられるモード (takumi-register →

takumi-login) の2種類を用意しています。取得したトークンは、「Guard」機能が対応する全エコシステムで共通してご利用いただけます。

(※4) 2026年8月時点。

(※5) 同梱対象のテンプレートは2026年9月25日時点の予定であり、変更となる場合があります。

(※6) 常駐監視プロセスではなく、コマンド実行時点での設定適用です。そのため、後から新しいパッケージマネージャーを導入した場合は、再度スクリプトを実行する必要があります。

【ご利用方法】

1. 『ConoHa VPS byGMO』のコントロールパネルからサーバーを追加し、「スタートアップスクリプト」で対象のAIエージェント系テンプレートを選択します。
2. サーバー構築後、同梱された専用スクリプトを実行します。
3. 悪性パッケージのブロックのみを利用する場合は、takumi-enable を実行します。
4. ダウンロードの追跡や侵害の通知も利用する場合は、takumi-register でメール認証を行い、takumi-login でトークンを設定します。

【料金について】

『ConoHa VPS byGMO』のスタートアップスクリプト機能（サーバー追加時に設定したコマンドを自動実行できる機能）は無料でご利用いただけます。また、「Guard」機能による悪意あるプログラム部品のブロックも、個人・法人を問わず無料です。なお、テンプレートを稼働させる『ConoHa VPS byGMO』のサーバー利用料金は別途必要です。組織全体の端末への一括導入をご検討の場合は、「Takumi byGMO」の管理ツールによる一括セットアップ機能（有料）をご利用いただけます。

【GMO Flatt Security 株式会社 取締役副社長 Co-CTO 米内 貴志のコメント】

開発環境やプログラムの部品を狙う攻撃が増加した2026年において、ソフトウェアサプライチェーンの安全確保は、すべての開発者に共通する課題となりました。特にAIエージェント活用が進み、バيبコーディングが広く実践されるほど、知らず知らずに取り込まれたプログラム部品は増えてきます。これまでも「Takumi byGMO」は日々大量のプログラム部品を検査し、そこに潜む悪意をいち早く検出することで、多くの方の開発やAI利用を保護してまいりました。この度、AIエージェントの利活用も支える

『ConoHa VPS byGMO』と連携し、さらに多くのAI活用者・開発者に安全をお届けできることを、非常に喜ばしく思っております。今後もグループの力を掛け合わせ、「エンジニアの背中を預かる」ためのサービスを磨いてまいります。



【GMO インターネット株式会社 専務執行役員 児玉 公宏のコメント】

GMO インターネットグループは、「AI&ロボティクスで未来を創る No.1 企業グループ」を掲げ、AIの活用とAI産業に向けた新たなサービスの提供を進めています。『ConoHa VPS byGMO』でも、AIエージェントをいち早く試せる環境を提供してまいりましたが、その活用が広がるほど、個人開発者や少人数の開発チームにとって、専門的なセキュリティ対策を継続して行うことは大きな課題になります。私たちは、利便性とセキュリティはどちらかを選ぶものではなく、ともに高めていくべきものだと考えております。今回、AIとセキュリティの双方に高い専門性を持つGMO Flatt Securityの知見を取り入れることで、より多くの方が安心してAIを活用し、新しい価値



の創出に挑戦できる環境を提供してまいります。

【GMO Flatt Security 株式会社について】（URL : <https://flatt.tech>）

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」 <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」
<https://flatt.tech/takumi>
- ・AWS 等クラウドの継続的な診断ツール(CSPM)「Shisho Cloud byGMO」 <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」 <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。

【「ConoHa byGMO」について】（URL : <https://www.conoha.jp/>）

「ConoHa byGMO」は、国内ホスティングシェア No.1^(※7) を誇る GMO インターネットグループのホスティングサービスで、ブログや HP 作成に最適な国内最速^(※8) レンタルサーバー『ConoHa WING』をはじめ、よりサーバーを自由にカスタマイズ・構築することが可能な『ConoHa VPS byGMO』、ゲームテンプレートが無料で使えるゲームユーザー向けの『ConoHa for GAME』、ブラウザだけで本格的な AI 画像生成を楽しめる『ConoHa AI Canvas』など、お客様のご利用目的に応じて最適なサービスをお選びいただけます。初期費用無料で「簡単」、「使いやすく」を徹底的に追求したサービスとなっており、サーバーを初めてご利用いただく方から個人事業主、法人まで幅広くご利用いただいております。

(※7) 2026 年 8 月時点、domaintools.com にて調査、当社が定める国内主要レンタルサーバー各社においてホストされている、ドメイン件数に占める当社の割合。

(※8) 2026 年 5 月時点、自社調べ。国内シェア 90%以上を占めたトップ 10 サービスにおいて、各サービス最下位プランのサーバー処理速度を、負荷テストツール「Apache Bench」「h2load」で 5 回計測した平均値を比較。国内シェアは、Webhosting.info および DomainTools をもとに算出。

以上

【報道関係お問い合わせ先】

- GMO インターネット株式会社
広報担当 酒井
TEL : 03-5728-7900
お問い合わせ :
<https://internet.gmo/contact/press/>

- 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 川縁
TEL : 03-5456-2695
お問い合わせ :
<https://group.gmo/contact/press-inquiries/>

【サービスに関するお問い合わせ先】

- GMO インターネット株式会社
ConoHa 事業部 松井
お問い合わせ : info@conoha.jp

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

【GMO インターネット株式会社】（URL : <https://internet.gmo/>）

会 社 名	GMO インターネット株式会社 （東証プライム市場 証券コード：4784）
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 社長執行役員 伊藤 正
事 業 内 容	■インターネットインフラ事業 ドメイン登録・販売（レジストラ）事業 クラウド・レンタルサーバー（ホスティング）事業 インターネット接続（プロバイダー）事業 ■インターネット広告・メディア事業
資 本 金	106 億 9,160 万円

【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