2026 年 3 月 3 日

報道関係各位

GMO Flatt Security 株式会社

「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～

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 3 月 3 日（火）より、セキュリティ AI エージェント「Takumi byGMO」において、ソフトウェアの開発時に悪意あるパッケージのインストールを自動でブロックする「Guard」機能と、ソフトウェアのビルド・テスト環境の実行状況を記録し、可視化する「Runner」機能の提供を開始いたします。

これにより、ソフトウェアサプライチェーンにおける開発環境や出荷されるソフトウェアへの攻撃から、開発組織を守ることが可能になります。いずれの機能も、エンジニアの作業手順を変えることなく、コマンド一つで導入いただけます。

【セキュリティ診断 AI エージェント「Takumi byGMO」とは】

「Takumi byGMO」は GMO Flatt Security が開発した、セキュリティ業務に特化した AI エージェントです。ブラックボックス診断（DAST／動的解析）・ホワイトボックス診断（SAST／静的解析）・脆弱性の自動修正機能により、2025 年 3 月のリリース以来ソフトウェア開発組織における堅牢な実装を継続的に支援してきました。

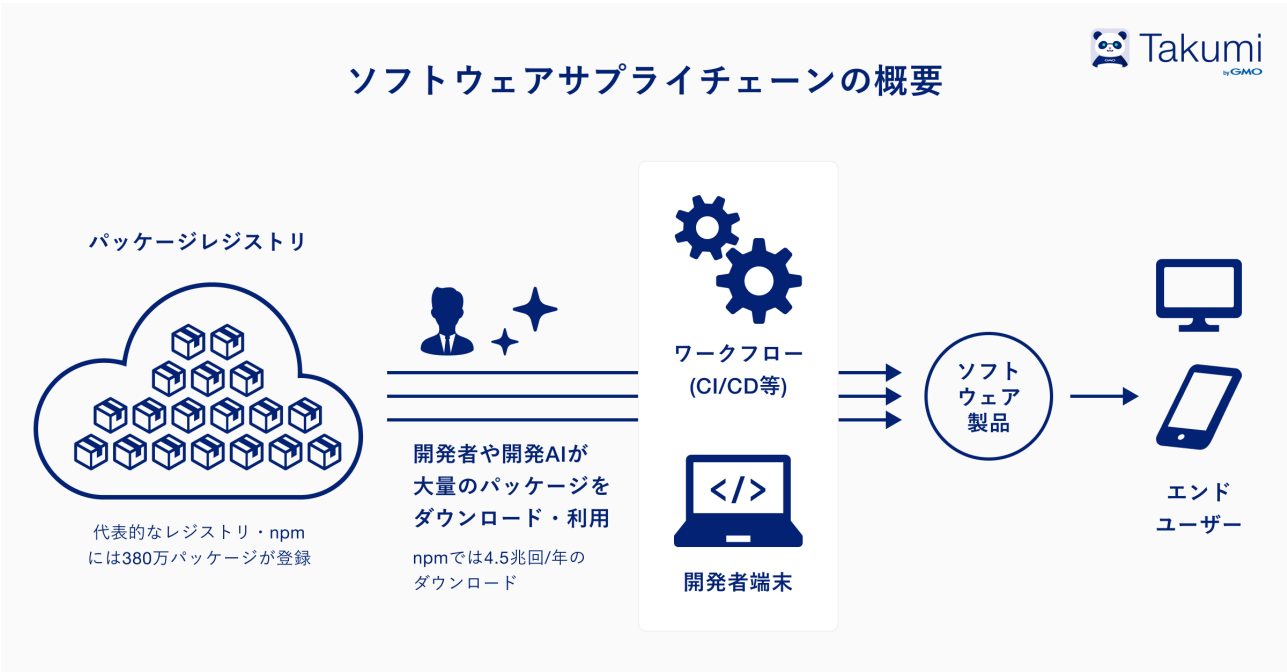
・「Takumi」Web サイト：https://flatt.tech/takumi

【機能の開発背景】

1.ソフトウェアエンジニアを狙うマルウェアの急増

現代のソフトウェアの大部分は、OSS のライブラリなど、世界に公開されている「パッケージ」と自社のソースコードを組み合わせて開発されています。外部パッケージの調達から、実行ファイルの作成（ビルド）、ユーザーに提供するまでの一連の流れを「ソフトウェアサプライチェーン」と呼びます。

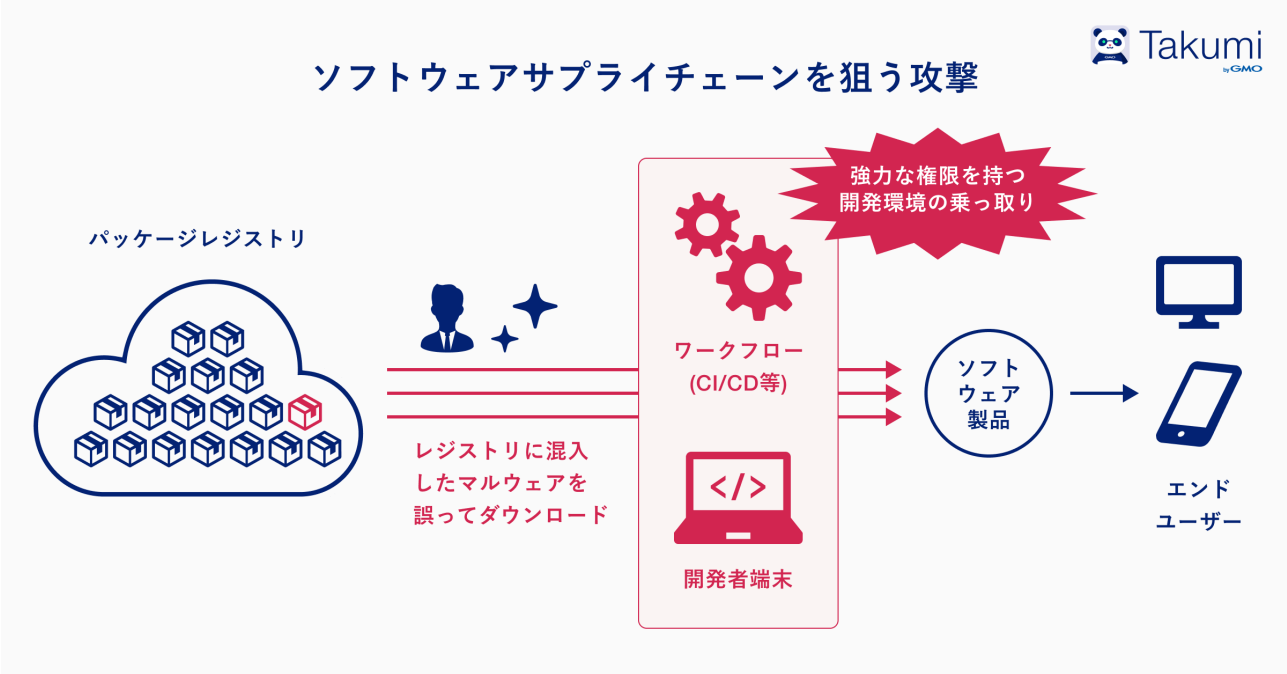
一つのソフトウェアが数百から数千のパッケージを要する場合もあり、JavaScript の世界最大級のパッケージレジストリ（※1）である npm には、約 380 万のパッケージが登録され、年間 4.5 兆回以上ダウンロードされているとの報告があります（※2）。



昨今、このソフトウェアサプライチェーンの構造を悪用した攻撃が注目を集めています。正規のパッケージに見せかけたマルウェアをレジストリに紛れ込ませ公開し、エンジニアがインストールした瞬間に悪意あるコードを自動実行させる攻撃手口です。npm にはパッケージのインストール時に任意のプログラムを自

動実行できる仕組みがあり、エンジニアがインストール操作を一度行うだけで、数百のパッケージが潜在的にプログラムを実行する可能性があります。その一つひとつの中身を人間が事前に確認することは現実的に不可能であり、気づかぬうちに開発者の端末や CI/CD ワークフローが侵害されるリスクが常に存在します。

ソフトウェアサプライチェーンマルウェアの件数は年々増加しています。米国のセキュリティ企業・Sonatype のレポートによると、2025 年 10 月～12 月の 3 ヶ月間で、オープンソース上で 39 万件以上の新たなマルウェアパッケージが特定され、同年 1 月～9 月の累計と比較して 476%増加しています（※3）。



(※1)レジストリ...パッケージを登録し、誰でも自由にダウンロードして使えるように公開しているデータベース

(※2) https://www.npmjs.com（2026 年 2 月時点の公開データ）、https://www.sonatype.com/press-releases/sonatypes-10th-annual-state-of-the-software-supply-chain-report（2024 年時点のパッケージリクエスト件数）

(※3)https://www.sonatype.com/blog/open-source-malware-index-q4-2025-automation-overwhelms-ecosystems（オープンソースマルウェアインデックス 2025 年第 4 四半期：自動化がエコシステムを圧倒）

2.ソフトウェアサプライチェーンのリスクを知らしめた「Shai-Hulud」

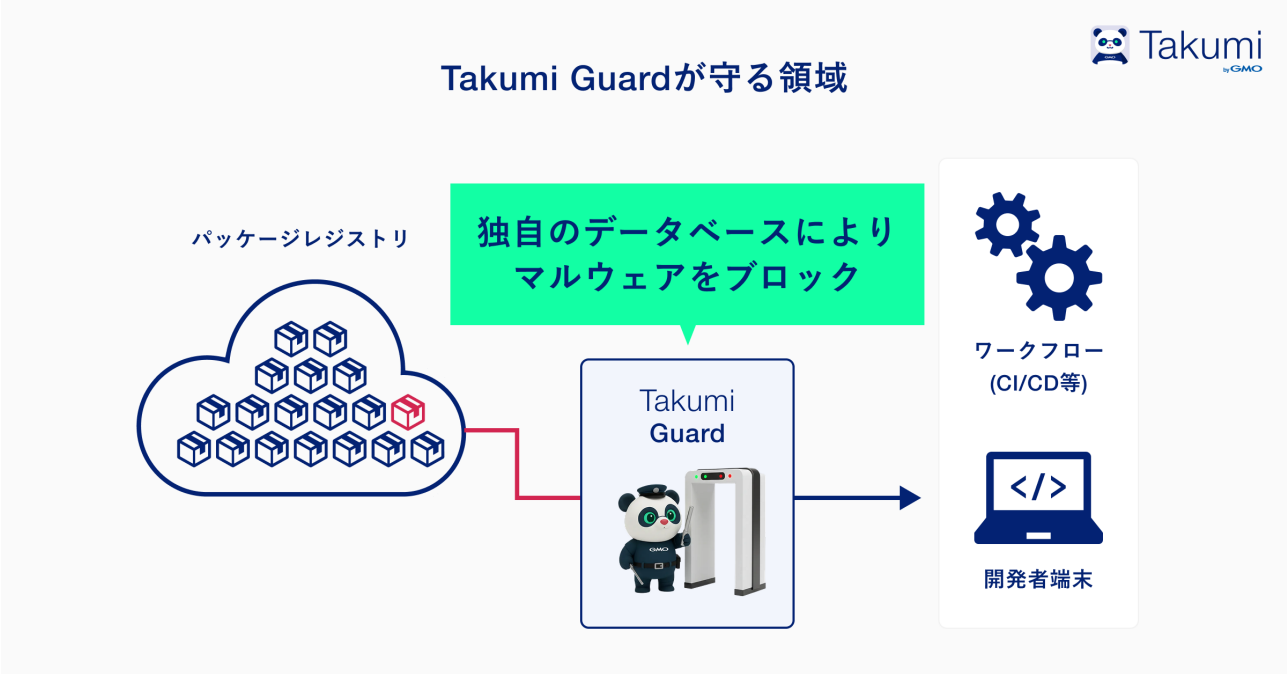
こうしたマルウェアが広く実害を及ぼしたのが、2025 年 9 月および 11 月に確認されたマルウェア「Shai-Hulud」です。「Shai-Hulud」は npm パッケージのダウンロードを通してエンジニアの端末や CI/CD 環境に感染すると、①クラウドサービスや開発プラットフォームの認証情報を窃取した後、②盗んだ情報の中に npm パッケージを公開する権限を持つ認証情報があった場合に、その情報を用いて正規のパッケージを改ざんし、悪意あるコードを埋め込んで公開します。最終的に、その汚染されたパッケージが別の端末等にダウンロードされることで、同様の手順で感染が連鎖的に拡大していきます。このように自己増殖する「ワーム」型の攻撃により、最終的に 796 以上の npm パッケージが侵害される被害が確認されました（※4）。「Shai-Hulud」は短期間でも攻撃手法が高度化しており、今後も巧妙な手口が生まれることが想定されます。

(※4) https://securitylabs.datadoghq.com/articles/shai-hulud-2.0-npm-worm/ （Shai-Hulud 2.0 npm worm：分析と知っておくべきこと）

3. AI によるソフトウェア開発の高速化がリスクを増幅

コーディングエージェントの普及は、ソフトウェアサプライチェーンマルウェアのリスクをさらに増大させています。AI はその行動に責任を負わない存在でありながら、能動的にパッケージをインストール・実行するため、本来最終的な責任を負うべき人間による検証プロセスに負荷が及びがちです。

こうした状況を踏まえ、GMO Flatt Security はエンジニアの検証負荷を抑えて開発の生産性を落とすことなく、ソフトウェアサプライチェーンの中でリスクを低減する「Guard」機能と「Runner」機能の開発に至りました。



【「Guard」機能：悪意あるパッケージをインストール前にブロック】

1.機能概要

「Takumi byGMO」の「Guard」機能は、npm レジストリとエンジニアの間に入り、パッケージのダウンロード時に悪性の有無を検証し、悪性パッケージが検出された場合は、ダウンロードをブロックします。導入はターミナルで特定のコマンドを一行実行することで完了します。既存のコードや作業手順への変更は不要です。

2.機能詳細

「Guard」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。

SBOM 管理ツールを始めとしたソフトウェアサプライチェーン領域の従来のツールの多くは、利用しているパッケージの中から既知の脆弱性情報をスキャンする仕組みがほとんどで、マルウェアの侵入そのものは防げませんでした。一方、「Guard」機能はパッケージがインストールされる瞬間に検知を行うため、悪意あるコードの実行そのものを水際で防ぎます。

3.料金について

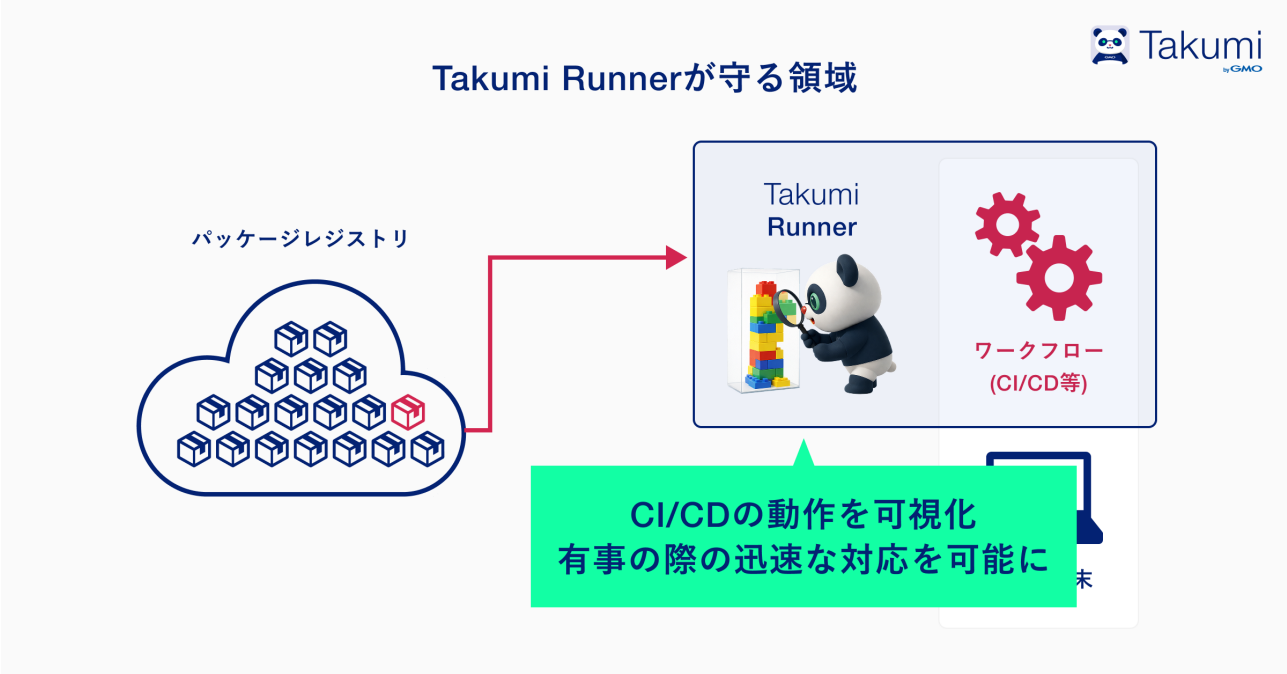
「Guard」機能のうち、悪性パッケージのインストールをブロックする機能は、個人・法人を問わず、無料でご利用いただけます。

・「Guard」機能 Web サイト：http://flatt.tech/takumi/features/guard

【「Runner」機能：CI/CD 環境の詳細ログ保全により、企業のインシデント対応を支援】

1.機能概要

「Takumi byGMO」の「Runner」機能は、CI/CD 環境(※5)として用いられるワークフローの動作を可視化する実行基盤です。ジョブごとに隔離された仮想環境を起動し、ビルドやテスト中のあらゆる挙動を詳細に記録します。導入は設定ファイルの一行を書き換えるだけで完了します。ソフトウェア開発プラットフォーム「GitHub」が提供する自動実行サービス「GitHub Actions」との完全な互換性を保っており、既存の自動化設定をそのまま利用できます。



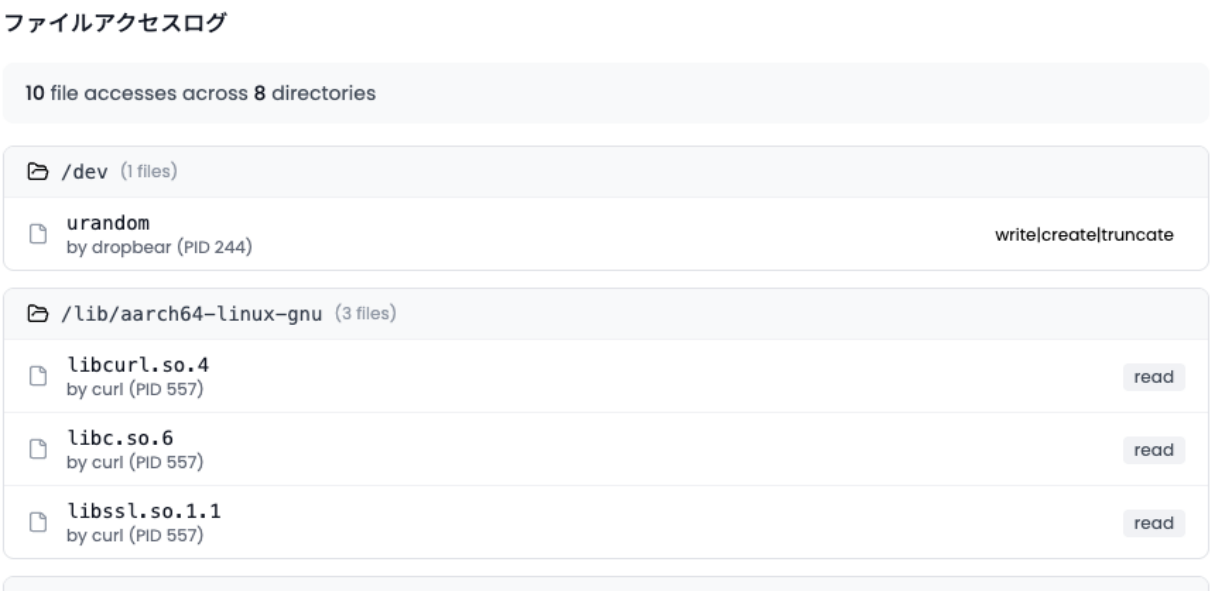
(※5)CI/CD 環境：ソフトウェアのビルドやテストを自動実行する環境

2.機能詳細

一般的に、企業に勤めるエンジニアの端末には EDR 等のセキュリティソフトウェアが導入されており、マルウェアの検知・対処に EDR が用いられています。一方で、ビルドやテストを自動実行する CI/CD 環境は多くの組織において管理の手が届いておらず、検知に足るログやテレメトリが取得されていない状態にあります。

しかし、CI/CD 環境は本番環境へのデプロイ権限を含む、極めて重要度の高い認証情報が集約される場所です。「Shai-Hulud」に代表されるソフトウェアサプライチェーン攻撃により環境が侵害された際、実行プロセスの挙動が取得されていなければ、被害範囲の特定や再発防止策の立案は極めて困難になります。

新機能の「Runner」は、プログラム実行、ファイルアクセス、外部通信を含む挙動を網羅的に記録し、有事の際の迅速な原因究明を可能にします。



3.料金について

「Runner」機能は法人でのご利用を想定しています。全ての「Takumi byGMO」ユーザーの皆様は追加料金やプラン変更は必要なく、一定の利用枠が付与されます。利用枠を超過した分については、「Runner」機能の実行時間に応じた従量課金となります。

・「Runner」機能 Web ページ：http://flatt.tech/takumi/features/runner

【今後の展望】

「Guard」機能においては、現在対応している npm に加え、PyPI（Python）、crates.io（Rust）等の主要なパッケージレジストリへの対応を順次進めてまいります。「Runner」機能についても、不審な通信先へのアクセスをブロックする機能の追加を予定しています。

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、AI 時代のソフトウェアサプライチェーンを守るインフラとして、ソフトウェアエンジニア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
・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

・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
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