

診断商品シート

2026年10月24日 / Habilis 坂井 大騎 / sakai@habilis.io

LP: <https://habilis.io/security>

サンプル報告書: <https://habilis.io/security/sample-report.pdf>

1. 誰のためか

- FX自動売買用のVPS（Windows / MT4 / MT5）を運用している
- EA・シグナル配信・取引用ツールを顧客に配っている
- GMOお名前.comの事案（2026年10月公表）を受け、取引口座・VPSの侵害前提の確認をしたい
- 取引先・顧客・経営層に「何を確認したか」を説明する必要がある

2. 商品

A. VPS・FX自動売買 緊急診断

298,000円（税別） / 5営業日 / 1 VPS

見るもの:

- RDP / SSH / 管理ポートの外部露出、Firewall、IP制限、VPN
- 管理パネル、更新ファイルの署名・ハッシュ・配布元、実行経路
- OS・MT4/MT5・EA・ライブラリの更新状況
- 管理者アカウント、MFA、最小権限
- MT4/MT5の保存パスワード、取引口座情報
- ブローカーのログイン履歴、注文履歴、APIトークン、出金制限
- スタートアップ、タスク、サービス、レジストリの永続化
- 不審ファイル、プロセス、通信、ログイン、イベントログ
- バックアップ、復旧手順、秘密情報の再発行

成果物:

- 経営者向け1ページサマリー
- 技術所見（再現手順・証拠・CVSS・影響）
- 修正チェックリスト（優先度・担当・期限）
- 60分デブリーフ

- 30日以内の再確認1回

B. 外部攻撃面 抜き打ち診断

580,000円（税別・導入価格） / 30日 / 1ドメイン・最大20資産

- 資産探索: ドメイン、サブドメイン、証明書、クラウド、管理画面、API
- 侵害検証: 認証回避、アクセス制御、インジェクション、SSRF、権限昇格、横展開（非破壊）※提供開始は下記「受注開始条件」を満たしてから
- 漏洩調査: 公開情報からのパスワード/APIキー候補（ログイン検証はしない）
- 速報: 重大な問題は発見次第共有
- 最終報告: 資産一覧、キルチェーン、構成図、到達情報、修正チェックリスト

「抜き打ち」の意味

予告なしで行うのは外部監視・資産探索まで。本番への侵入検証は、事前合意した範囲・時間・停止条件のみ。データ持ち出し、マルウェア、DoS、第三者へのテストは行わない。

受注開始条件（現時点では未達）

次の4点が揃うまで、攻撃的な検証を含む受注は開始しません。①提携パートナー契約、②賠償責任保険（E&O/サイバー）の付保、③契約雛形の弁護士レビュー、④30日間の監視・速報・証拠管理フロー。現時点では、相談・見積り・非破壊の確認までです。

追加

- 追加VPS 1台: +100,000円
- 追加ドメイン: +200,000円
- 追加20資産: +100,000円
- 追加Webアプリ/API: +150,000円
- 土日・夜間: +30%
- 再テスト（30日以降）: 80,000円

3. 品質

- 意図的に脆弱なデモラボで **9ケース** を検証
- **8所見**（High 5 / Medium 2 / Low 1）を再現
- **同一環境・同スクリプトの連続2回で同一結果**（環境非依存の再現性は未検証）
- 外部の実システムへの攻撃 **0**
- DoS・データ持ち出し・マルウェア・WebShell **0**
- 重大所見は対照リクエストと比較し、**実施者による自己レビュー済み**。独立レビューは未実施（パートナー契約後）
- 本ドライランの実行・証拠整理・報告ドラフトはAIエージェントが支援し、内容は人が確認

- GMO事案の公開情報に基づく攻撃鎖（管理プレーン→不正プログラム→取引口座情報→不正注文）もラボで模擬済み

サンプル報告書は、実際のデモラボ結果に基づいています。実在の顧客環境ではありません。

<https://habilis.io/security/sample-report.pdf>

GMO事案相当の再現レポート:

<https://habilis.io/security/gmo-emulation-report.pdf>

4. 進め方

1. 相談（チャット可・ビデオ必須ではない）
2. 対象・目的・制約のヒアリング
3. スコープ・見積り
4. NDA・許可書・RoE
5. キックオフ（緊急連絡・停止条件・バックアップ）
6. テスト（非破壊）
7. 報告・デブリーフ
8. 最終報告後30日以内の再確認

5. 実施体制

- Habilis（代表）：営業、PM、スコープ、進行、経営層向け報告、再確認
- 実施責任者: 現時点で、OSCP / GPEN / CREST / PNPT 等のハンズオン系資格、および CISSP・情報処理安全確保支援士等の保有はありません。**資格保有を前提としたご依頼はお受けしません**
- 提携パートナー: **未締結（準備中）**。締結後に、実際のテスト・証拠取得・技術レビューの分担を提案書に明記します
- 保険: **未加入**（賠償責任保険・E&O/サイバー）。加入した場合は、補償範囲を着工前に書面で提示します
- 法務: **契約雛形は未確定**。弁護士レビュー後に確定します

現状と提供範囲: 資格・保険・法務レビュー・パートナー契約はいずれも未取得／未締結です。そのため、**攻撃的な侵入検証は提供していません**。現在ご提供できるのは、**非破壊の確認**（公開情報の整理、設定・セキュリティヘッダ・TLS・公開資産の確認、書面で許可された範囲の読み取り中心の点検）と、その報告です。加えて、再確認1回・NDA・再委託不可・賠償上限の明示を条件にしています。LP・相談・見積り・サンプル提示は可能です。

6. やらないこと

- 許可のないテスト
- 本番停止を伴う操作
- DoS / 負荷テスト

- データの破壊・改ざん・持ち出し
- マルウェア、WebShell、ランサムウェア
- ソーシャルエンジニアリング（別SOWなし）
- 第三者システム、クラウド基盤、取引所、決済代行
- 修正作業（別途見積り）
- 「必ず侵入できる」「必ず安全」の保証

7. よくある質問

脆弱性が見つからなかったら？

それも結果です。テスト範囲・方法・証拠・確認できた防御を報告します。「侵入できなければ返金」は約束しません。

攻撃がすぐ防がれたら？

既存の防御が機能した証拠です。返金対象ではありません。必要なら、認証済み・別入口・API・権限昇格まで範囲を広げて再確認します。

同種サービスより安いのはなぜ？

1ドメイン・最大20資産に限定し、AI支援で偵察・整理・報告を効率化しているためです。品質を下げた安売りではありません。導入価格です。

個人事業主で信用できる？

資格・保険・法務はいずれも未取得であることを、先に明示します。その上で、①範囲を限定する（非破壊・読み取り中心）、②同じ確認を1回やり直して再現性を示す、③NDAを結ぶ、④再委託しない、⑤賠償上限を契約で明示する、という条件でお受けしています。まずは小さいスコープから始め、成果物で判断いただきます。

パスワードを渡す必要は？

原則として不要です。必要な場合も、一時的な限定権限・専用アカウント・終了後削除を契約に明記します。

本番を止めない？

非破壊を前提に、事前合意した範囲・時間・停止条件で実施します。バックアップと復旧手順を確認します。

30日間で何をする？

外部監視・資産探索・速報・合意済み範囲の検証・最終報告です。常時攻撃するわけではありません。

8. 相談

- LP: <https://habilis.io/security#contact-form>
- メール: sakai@habilis.io

- 件名例: 「VPS緊急診断の相談」「外部攻撃面診断の相談」
- 30分のビデオ通話は必須ではありません。チャット・メールで進められます。

Habilis / 坂井 大騎

sakai@habilis.io

<https://habilis.io/>

Habilis / 坂井 大騎 / sakai@habilis.io / <https://habilis.io/security>