

FX自動売買VPS 侵害前提チェック 10項目

これは自己点検用のチェックリストです。診断の代替ではありません。

設定変更・削除・スキャン負荷をかける前に、バックアップと変更管理を確認してください。

外部からの攻撃テストは、書面許可のある専門家だけが行えます。

1. RDP / SSH がインターネットに露出していないか

なぜ: 露出したRDPは、パスワード総当たり・既知脆弱性・ランサムウェアの入口になる。

安全な確認:

- VPS事業者の管理画面で、ファイアウォール/セキュリティグループを確認
- 自宅IP・VPN・踏み台のみ許可されているか
- 可能なら外部からポートスキャン（許可された範囲のみ）

NGなら: VPN/踏み台経由に限定。不要なら停止。MFAを有効化。

2. 管理者アカウントは最小限か。MFAは有効か

なぜ: 管理者が1つでも奪われると、MT5・EA・取引口座に到達される。

安全な確認:

- ローカル管理者の一覧
- 共有アカウント、退職者アカウント、既定ユーザー
- RDP/管理画面のMFA

NGなら: 個別アカウント化、最小権限、MFA、既定アカウント無効化。

3. OS・MT4/MT5は最新か

なぜ: 古いOS・MT5・EAは、既知の脆弱性や互換性問題を抱える。

安全な確認:

- Windows Update / ビルド番号
- MT4/MT5のビルド
- EA・ライブラリの更新日

NGなら: 変更管理に沿って更新。取引時間外に再起動計画。

4. MT4/MT5に取引口座のパスワードを保存していないか

なぜ: VPSが侵害されると、保存パスワードから取引口座にログインされる。

安全な確認:

- MT5のログイン画面の「パスワードを保存」
- ブラウザの保存パスワード
- EA/ツールの設定ファイル

NGなら: 保存を解除。VPS外の端末でパスワード変更。MFA・出金制限。

5. EA・ライブラリの配布元は明確か

なぜ: 出所不明のEA/ライブラリは、バックドアや認証情報窃取を含むことがある。

安全な確認:

- 配布元、購入履歴、署名、ハッシュ
- 更新日、最終更新者
- 不要なDLL/EX5

NGなら: 配布元に確認。ハッシュを記録。不要なら削除。再発行。

6. スタートアップ・タスク・サービスに不審なものがないか

なぜ: マルウェアは再起動後も動き続けるために永続化する。

安全な確認:

- スタートアップ（ユーザー/全ユーザー）
- タスクスケジューラ
- サービス
- レジストリのRunキー

NGなら: 配布元・ハッシュ・署名を確認。安易に削除せず、証拠を保全。

7. 不審なプロセス・通信・ログインがないか

なぜ: 侵害されても、取引が正常に見えることがある。通信・ログイン履歴が手かかり。

安全な確認:

- 見慣れないプロセス
- 外部への不審な通信
- RDP/管理画面のログイン履歴
- 失敗ログインの急増

NGなら: ネットワークを切り離さず、証拠を保全。専門家に相談。

8. バックアップはオフラインか。復旧手順はあるか

なぜ: ランサムウェアは、同じネットワーク上のバックアップも暗号化する。

安全な確認:

- バックアップの保存先
- 世代、暗号化、リストアテスト
- 復旧にかかる時間
- 取引口座の再設定手順

NGなら: オフライン/別アカウントのバックアップ。リストア演習。

9. 取引口座のMFA・出金制限・ログ確認はできているか

なぜ: VPS侵害の最終目的は、取引口座の不正操作・出金。

安全な確認:

- 取引口座のMFA
- 出金先ホワイトリスト、出金制限
- ログイン通知
- 最終ログイン・取引履歴

NGなら: MFA、出金制限、通知、パスワード変更。FX会社に連絡。

10. インシデント時の連絡体制・公表手順はあるか

なぜ: 初動の遅れが、被害・信用・法的リスクを拡大する。

安全な確認:

- 緊急連絡先（経営、技術、法務、広報）
- 取引口座の停止手順
- 顧客への説明文
- 警察・監督官庁への相談先

NGなら: 1ページの連絡網と初動チェックリストを作る。

次の一步

- 1つでもNGがあれば、変更管理とバックアップを確認してから修正。
- 侵害が疑われる場合は、自分で削除・再起動せず、証拠を保全して専門家へ。

- 非破壊の診断は、書面許可・NDA・RoE・実施体制（資格・保険）の確認が前提。

Habilis Security

<https://habilis.io/security>

sakai@habilis.io