

GMO事案相当 攻撃鎖シミュレーション

これは実GMO・実VPS・実MT5・実ブローカーへの攻撃ではありません。

GMOインターネットグループの公開情報に基づき、報告された攻撃鎖をローカルの模擬環境で再現した防御検証です。

実在の取引口座・資金・認証情報・マルウェアは使用していません。

1. 目的

GMO「お名前.com デスクトップクラウド」の事案で報告された、

- ・ サーバーへの不正プログラム設置
- ・ 取引口座ログイン情報の取得可能性
- ・ 取引口座の不正操作報告
- ・ 全プランのサーバー停止

という流れを、**安全なローカルラボ**で再現し、以下を確認する。

1. 攻撃鎖のどこで止められたか
2. どのログ・証拠が残るか
3. 検知・封じ込め・再発防止のどこが弱い
4. 実VPS/MT5で何を確認すべきか

2. 公開情報の整理

日付	公表内容
2026-10-20	一部利用者のサーバー環境に第三者の不正プログラム設置を確認
2026-10-21	4:00から全プランを順次停止。個人情報漏えい・悪用は未確認と説明
2026-10-22（第2報）	影響可能性 26,739サーバー。取引口座ログイン情報等の取得可能性、取引口座の不正操作報告。カード決済情報は保持していない
続報待ち	初期侵入経路、不正プログラムの挙動、設置時期、原因、補償、再開時期

未確認情報: X等の「数十万～数百万円の損失」投稿はユーザー側の報告であり、GMOが被害額を確認したものではない。本レポートでは事実として扱わない。

3. ラボ構成

要素	模擬内容
VPS管理パネル	127.0.0.1:18082。露出した管理画面、既定認証、更新ファイルのアップロード・実行
模擬MT5設定	架空の取引口座・パスワード・APIトークンをJSONに保存
模擬ブローカーAPI	127.0.0.1:18083。トークン認証、注文記録、トークン失効
不正プログラム	署名なし更新として実行される、ローカルのみで動く無害なNodeスクリプト
永続化	実OSのスタートアップではなく、ラボ内の startup/ マーカー
外部通信	なし。すべてループバック

初期侵入経路について: GMOの初期侵入経路は公式未公表。本ラボでは「露出した管理プレーン＋既定/弱い認証」を**代表例**として使用した。これはGMOの実際の経路を断定するものではない。

4. 実行結果

ID	判定	重大度	テスト	観測
GMO-01	PASS	High	管理プレーンの露出	管理ポートに到達
GMO-02	PASS	Critical	既定/弱い管理者認証	admin/admin でログイン、MFAなし
GMO-03	PASS	High	署名検証なしの更新実行	アップロード→実行→PID取得
GMO-04	PASS	High	不正プログラム設置・模擬永続化	startup/agent.cmd と heartbeat
GMO-05	PASS	High	MT5設定から認証情報取得	架空の口座・トークンを取得
GMO-06	PASS	Critical	窃取情報で模擬不正注文	架空ブローカーにSELL 0.10
GMO-07	PASS	Medium	検知・アラート欠如	ログイン・実行・注文でアラートなし
GMO-08	PASS	High	封じ込め	プロセス停止、永続化削除、旧トークン401

集計: 8/8 PASS、Critical 2 / High 5 / Medium 1。

GMO公表事実との対応

GMOの公表・報告	ラボでの模擬	実VPS/MT5での確認
不正プログラム設置	GMO-03/04（更新実行・設置・模擬永続化）	更新経路、署名、スタートアップ/タスク/サービス、ハッシュ
取引口座ログイン情報の取得可能性	GMO-05（MT5設定から取得）	保存パスワード、config、APIトークン、ブラウザ保存

GMOの公表・報告	ラボでの模擬	実VPS/MT5での確認
取引口座の不正操作報告	GMO-06（模擬不正注文）	ブローカーのログイン履歴、注文履歴、出金制限、MFA
全プランのサーバー停止	GMO-08（封じ込め）	証拠保全、隔離、セッション切断、復旧手順
初期侵入経路は未公表	GMO-01/02（露出管理 + 既定認証を代表例）	RDP/SSH/VPN/管理パネル、既定認証、MFA、patch

5. 攻撃鎖

```

[1] 露出した管理プレーンを発見
[2] 既定/弱い管理者認証でログイン (MFAなし)
[3] 署名検証なしの「更新」として不正プログラムをアップロード
[4] 管理パネルから実行
[5] ラボ内のスタートアップ・タスクで複製実行
[6] MT5設定から取引口座情報・APIトークンを取得
[7] 模擬ブローカーAPIへ不正注文
[8] 検知・アラートなし
[9] 封じ込め: プロセス停止、マーカー削除、トークン失効
  
```

6. 何が問題か

6.1 入口

- 管理プレーンが外部から到達できる
- 既定/弱い認証、MFAなし
- ログイン失敗の制限・通知がない想定
- 管理画面の操作ログが運用に接続されていない

6.2 実行・永続化

- 更新ファイルの署名・ハッシュ・配布元を検証していない
- 管理パネルから任意のNodeスクリプトを実行できる
- スタートアップ・タスク・サービスの監視がない
- EDR/AVの検知・隔離が運用に接続されていない

6.3 取引口座

- MT5設定に取引口座のパスワード/トークンを保存
- APIトークンが長期間有効
- 注文の送信元・デバイス・地理・時刻の異常検知がない
- 出金制限・MFA・セッション失効が弱い

6.4 検知・対応

- 管理ログイン、実行、注文のいずれもアラートなし
- 不正プログラムの設置に気づくのが遅い
- 侵害後のパスワード変更・セッション切断・ブローカー連絡の手順が未整備

7. 実VPS/MT5で確認すべきこと

以下は読み取り中心のチェック。変更・削除はバックアップと変更管理の後に行う。

入口

- ☐ RDP/SSH/管理ポートがインターネットに露出していない
- ☐ VPN/踏み台/IP制限がある
- ☐ 管理者は最小限、MFAがある
- ☐ 既定アカウント・共有アカウントが無効
- ☐ OS/MT4/MT5/EAが最新
- ☐ 管理パネルのログイン履歴・失敗回数を確認
- ☐ 不審なログイン（時刻・地理・デバイス）がない

不正プログラム・永続化

- ☐ 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Runキー
- ☐ 最近作成/更新されたEXE/DLL/PS1/JS
- ☐ ハッシュ・署名・配布元
- ☐ EDR/AVの検知履歴
- ☐ 不審なプロセス・通信

取引口座

- ☐ MT5にパスワードを保存していない
- ☐ `config / accounts.dat` 等の保存状態を確認（値は表示しない）

- ☐ APIトークンの有効期限・権限
- ☐ ブローカーのログイン履歴
- ☐ 注文履歴（心当たりのない注文）
- ☐ 出金先・出金制限・MFA
- ☐ セッションの失効
- ☐ パスワード変更はVPS外の端末から実施
- ☐ 他サービスと同じパスワードを使っていない

検知・対応

- ☐ 管理ログイン、実行、注文のアラート
- ☐ ファイル整合性監視
- ☐ ネットワーク外向き通信の制限
- ☐ ログ保全（Security/System/Application/PowerShell/TaskScheduler）
- ☐ インシデント連絡網
- ☐ 証拠保全と復旧手順
- ☐ ブローカー・警察・監督官庁への連絡

8. 封じ込めの結果

ラボでは以下を実施し、PASSした。

- 不正プロセスの停止（PID指定）
- 模擬永続化マーカーの削除
- 旧APIトークンの失効（旧トークンで401）
- 新規の不正注文が増えないこと
- 証拠のハッシュ記録

実環境では、削除より先に証拠保全を行う。

停止・隔離の判断は顧客の決裁者と合意し、ブローカーへの連絡、パスワード変更、セッション切断を並行する。

9. 限界

- 実GMOの初期侵入経路・マルウェア挙動は未公表。本ラボは代表例。
- 実Windows Server / 実MT5 / 実ブローカーではない。
- 実マルウェア、実C2、実データ持ち出しは行っていない。
- 独立した第三者再現は未実施。
- 実環境の診断は、書面許可・NDA・RoE・有資格者・保険が前提。

10. 商品への反映

このシミュレーションを、VPS・FX自動売買 緊急診断（29.8万円）の**攻撃鎖検証**に使用する。

- 入口: 露出、認証、MFA、更新経路
- 実行: 署名・ハッシュ・配布元
- 永続化: スタートアップ・タスク・サービス
- 取引口座: 保存認証情報、APIトークン、注文履歴
- 検知: ログ、EDR、アラート
- 対応: 証拠保全、封じ込め、再発防止

「攻撃して終わり」ではなく、同じ攻撃鎖を止められる状態まで確認する。

Habilis / 坂井 大騎

sakai@habilis.io

<https://habilis.io/security>

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