YOORshop SAS
RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com
［会社情報追記欄］

レポート番号： YH-DEMO-2026-04
発行日： 2026年11月19日
● 復旧・堅牢化計画

インシデント対応＆セキュリティ再構築報告書 • 成果物 #4

インシデント分析および復旧・堅牢化

短時間の502エラー原因分析、不正アクセスのフォレンジック調査、およびマルウェア駆除・堅牢化計画。

対象クライアント
企業名： Horizons Médias & Édition SARL（架空）
対象ドメイン： portail-horizons.example（＋マルチサイト）
ホストサーバー： srv-demo-03.yoorhosting.com (Nginx/Apache)
アカウント： horizons_adm · horizons_wp

HTTP 502エラー原因解明	初期侵入経路	ホストサーバー横展開	復旧プロトコル
12 s・85 req	**FTP 1アカウント**	**感染拡大 0件**	**全10工程**
更新後のApache再起動による瞬断	chroot未設定の外部委託先ID	他cPanelアカウント・SSHは無傷	クリーン再構築と完全堅牢化

クライアントのご要望
「一時的な接続障害アラート（502エラー）に続き、マルチサイト環境での不正アクセスおよび大量迷惑メール送信の疑いが浮上したため、クライアントより以下の3点をご依頼いただきました：(1) 502瞬断の正確な技術的説明、(2) 侵入経路と影響範囲の完全なフォレンジック調査、(3) 安全なクリーン再構築と恒久的な堅牢化のための詳細技術プロトコルの策定。」

1 パート1 — 短時間通信断の解析（12秒間のHTTP 502エラー）

ログ時系列（NGINX / SYSTEMD / DNF）

```
[14:25:27 CEST] dnf : openssl, systemd, ea-apache24-config-runtime 自動更新
[14:27:43 CEST] systemd[1] : daemon-reload および再起動キュー登録
[14:27:48 CEST] systemd[1] : Stopping Apache web server...
[14:27:48] Nginx : upstream切断 (https://192.0.2.10:4430/...)
[14:27:58] Nginx : Apache停止中に 111 Connection refused
[14:28:00-01] Apache再起動完了 (OpenSSL/3.5.8) → 100 % HTTP 200 OK
```

事実確認： 当日発生した **85件の502エラー**はすべてこの12秒間に集中していました。ファイル破損、外部攻撃、ハード故障はありません。復旧後の応答確認：トップ（約180 ms）、商品（約210 ms）、管理画面（約150 ms）すべて `200 OK`。

管理画面の別事象（タイムアウト）と対策

アプリログ（`/home/horizons_adm/public_html/var/logs/`）より、`operateur@portail-horizons.example` がシステム情報を開いた際の別エラーを確認：

```
FatalError: Maximum execution time of 180 seconds exceeded
at .../classes/ConfigurationTest.php:246 (/img/ の再帰スキャン)
```

- OSパッケージ自動更新を深夜帯（02:00〜05:00）へスケジュール変更。
- 完全停止ではなく無停止リロード（`httpd -k graceful` / `systemctl reload`）を使用。
- 営業時間中の `ConfigurationTest.php` による `/img/` 再帰スキャンを回避。

2 パート2 — 不正アクセスのフォレンジック調査

初期侵入経路およびディレクトリ隔離の不備

ゼロデイ脆弱性は使われていません。08:26 UTCに `203.0.113.10` からcPanel（ポート2083）へのログインに失敗した後、15:17 UTCに外部委託先アカウント `agence-ext@portail-horizons.example` の正規認証情報を用いてFTP（ポート21）へ1回でログインに成功しました。**重大な設定不備：** このFTPアカウントが `public_html` に制限（*chroot*）されずcPanelルート `/home/horizons_adm` を指していたため、設定ファイルとMariaDB認証情報（`horizons_dbprod`）が読み取られました。

日時 (UTC)	IP (匿名化済)	発信元 / 中継	復元された攻撃アクション（同一FTP署名 + `CURL/8.7.1`）
15/09 08:26	`203.0.113.10`	VPS事業者 A	アカウント名を用いたcPanel（ポート2083）へのログイン試行（失敗）。
15/09 15:17	`203.0.113.10`	VPS事業者 A	初回FTPログイン成功（`agence-ext@...`）。`tools/.htaccess` 取得とテストファイル設置・削除。
16/09 02:21	`203.0.113.10`	VPS事業者 A	JSスキマー `themes/universal/assets/js/custome1.js`（64,210 bytes）設置および `payment.tpl` 改ざん。
22/09 12:29	`203.0.113.21`	プロキシ中継 B	`app/config/parameters.php`（DB認証情報・鍵）のFTP窃取およびバックドア `_ca_9f3a.php` 設置。
23/09 15:37–19:31	`203.0.113.22/23/24`	ローテーションProxy C/D/E	`clearcache.php` 設置、注文API（`/api/orders` 500件単位）からのデータ抽出、システム偵察（10 KB）。
23/09–08/10	`203.0.113.50`	VPSサーバー F	Webシェル `_npgop_*.php`、Base64化SQL実行、決済モジュールの偽コントローラー注入、その後 `npg_purge.json` で痕跡消去。

アプリおよびSQLデータベースの改ざん内容

- **MariaDB（`horizons_db2025`）：** `PS_WEBSERVICE` 有効化、`PS_MAIL_METHOD` 変更、外部モジュール再有効化、注文データ参照および監査ログの選択的削除。
- **JSスキマー：** 決済入力欄を傍受し、Base64化したデータを `sendBeacon` / `fetch` で外部回収サーバー（`collecte-tiers.example`）へ送信。
- **決済ゲートウェイ：** 偽コントローラー（`npginit.php`）と隠し状態ファイル（`var/.ppext/`）の注入。

SRV-DEMO-03 サーバー全体の隔離検証

検証対象	調査結果	状態
他cPanelアカウント（`tiers_a`, `tiers_b`）	不審なファイル・ログ・通信なし	無傷
SSH・OS権限（`/var/log/secure*`）	攻撃IPからのSSH試行ゼロ	無傷
Cronタスク（`/etc/cron*`）	正規の業務スクリプトのみ	健全
メモリ上の稼働プロセス	正規PHP-FPMとバックアップのみ	健全

3 パート3 — マルチサイト監査および完全駆除・堅牢化計画

クリーン再構築を必要とする監査所見（アカウント `HORIZONS_WP`）

- 重大 乗っ取られたメールボックスと不正PHPスクリプトから30日間で**410,000通超のスパム**を送信。
- 重大 7ドメイン中6サイト（`editions-alpha.example`, `atelier-beta.example`）で最大**83個のWebシェル**を検出。
- 重大 不正なWordPress管理者作成、パスワード窃取用隠し「must-use」プラグイン、不正SEOリダイレクト。
- 攻撃者が作成した**49個のメールボックス**と不明IPからのパネル/Webメール接続（全パスワード漏洩）。
- 既知の脆弱性を持つ旧版プラグイン（`WPForms 1.7.0`, `Elementor 2.4.7`, `Yoast SEO 5.7.1`）。
- 堅牢化未実施：ファイルエディタ有効、`XML-RPC` 開放、フォームのCAPTCHA未設定。

#	復旧ステップ	復旧プロトコルに含まれる技術アクション
1	**緊急封じ込め**	外部へのスパム送信を即時停止、攻撃者のアクセス遮断、侵害アカウント全体の証拠保全バックアップ取得。
2	**フォレンジック選別**	各ドメインの正規コンテンツと、攻撃者が設置した不正ファイル・フォルダ・ユーザー・DBレコードを分離。
3	**新規隔離アカウント作成**	クリーンなcPanelアカウントを新設、全パスワード（パネル・FTP・DB・メール・WP）刷新、SSH閉鎖、chroot制限付き単一FTP。
4	**クリーン再構築**	公式ソースからコア・テーマ・プラグインを再導入。不正管理者・注入リンク・不正設定をSQLから除去し、実行コードを除いたメディアを復元。
5	**プラグイン最新化**	旧版プラグインの更新または代替、動作検証、および不要プラグインの完全削除。
6	**フォーム保護強化**	ボット対策（TurnstileまたはhCaptcha）、ハニーポット、IP単位の速度制限、宛先固定、認証SMTP限定送信。
7	**メール整理と信頼回復**	承認済みメールボックスのみ維持、不正ボックス削除、送信上限設定、`SPF`・`DKIM`・`DMARC` の厳密設定。
8	**完全堅牢化（Hardening）**	ファイルエディタ無効化、`XML-RPC` 閉鎖、`uploads` 内のPHP実行禁止、管理者2要素認証（2FA）、WAFルール、自動セキュリティ更新。
9	**不正ドメインの廃止**	攻撃者専用サイトの安全な削除と、維持する全ドメインのDNS点検。
10	**30日間監視＆最終報告書**	ファイルと送信メールの継続監視、7日後の再点検、および削除・再構築・堅牢化内容を記載した完了報告書の提出。

追加推奨事項（パート2＆パート3）： Webサービスキー（`API_KEY_REVOQUEE_DEMO_01`）と旧FTPアカウントを即時失効させ、`custome1.js` と `clearcache.php` を削除し、公式版決済モジュールを再導入してください。また、9/16〜10/8の間に決済情報が傍受された可能性がある場合は、決済代行会社および所管機関へ速やかに通知してください。

技術検証・承認サイン：
CERT＆オペレーショナルセキュリティ部門 — YOORshop SAS

✓ プロトコル承認済