サーバーセキュリティ診断報告書

共用 Web／メールサーバー（Linux + Plesk）

診断日：2026 年 10 月 9 日

> **本書について：** 実際に行った診断の報告書から、ドメイン名・IP アドレス・ホスト名・ユーザー名、ソフトウェアの細かな版など、対象を特定できる情報を伏せたサンプルです。対象のサーバーは、この診断のあと新しいサーバーへ移行し、運用を終えています。伏せた箇所は「サイト A」「[管理者 IP]」のように表記しています。

1. 総合評価

今回の収集範囲では、侵害の痕跡は見つかりませんでした。ただし、攻撃を受ければ短時間で突破されうる弱点が重なっており、今週中の是正が必要です。このサーバーには数十のサイトが同居しているため、1 サイトの侵害がサーバー全体に波及するリスクがあります。

最優先の対処は次の 3 点です。

1. **root への総当たりを止める。** root のパスワードは 2017 年 7 月から変わっておらず、SSH でもパスワードでログインできます。9 月 25 日から Plesk 管理画面への root の総当たりが始まり、10 月 9 日までに 21,356 回失敗しています。今も 1 日約 180 回続いており、fail2ban では 1 件も遮断されていません。
2. **古い WordPress 7 サイトを止めるか更新する。** 2019 年の版の WordPress が 3 サイトあり、悪用実績のあるプラグイン（Duplicator・MW WP Form の古い版）も入っています。
3. **OS のセキュリティ更新を適用する。** 最終適用は 8 月 8 日です。未適用のセキュリティ修正が 97 件あり、OpenSSL、libxml2、PHP など Critical 評価のものを含みます。

OS の延長サポート（ELS）の契約、Imunify360、ModSecurity、fail2ban はすでに機能しており、更新とアクセス制限で短期間に大きく改善できる状態です。

2. 診断概要

項目	内容
対象	共用 Web／メールサーバー 1 台（仮想マシン、ホスト名・IP アドレスは非開示）
OS	CentOS 7（サポート終了。延長サポートの契約あり）
主な構成	Plesk、nginx + Apache、PHP（複数の版）、MariaDB、Postfix、Dovecot、BIND、ProFTPD
実施日時	2026 年 10 月（約 40 分）
手法	読み取り専用の収集スクリプトをサーバー上で実行し、出力を分析
範囲	OS・パッケージ、ネットワーク、ファイアウォール、サービス、SSH、アカウント、永続化の痕跡、ファイル改ざん（rpm -Va）、Web アプリ、ログ、カーネル設定

この診断の限界： 外部からのポートスキャンと Web アプリの動的検査（実際に攻撃を試す検査）は未実施です。ログはサーバー上に保存されている期間（多くは 4〜5 週間）しか見ていません。侵害の有無は「痕跡が見つからなかった」という意味で、侵害がなかったことの証明ではありません。

3. 侵害の痕跡の判定

追加確認の結果を含め、12 項目のうち 10 項目は異常なしです。root への総当たりは実際に続いている攻撃で、成功したログインがないかの確認が残っています。

確認項目	結果	判定
root パスワード照合失敗の急増	9/25 開始、9/26 に 1 日 5,853 件でピーク、10/9 までに計 21,356 件。記録元は Plesk の認証処理（sys_auth）で、管理画面への root の総当たり。現在も 1 日約 180 件、fail2ban の遮断は 0 件	攻撃継続中（成功の有無を要確認）
rpm -Va で内容が変化したシステムファイル	suexec、postdrop、mod_proxy.so、mod_proxy_fcgi.so の 4 件。suexec と postdrop は Plesk 版（埋め込み文字列で確認）。mod_proxy 系 2 件は Plesk の psa-mod_proxy パッケージによる置き換え	異常なし（rpm -V psa-mod_proxy で最終確認）
ログイン履歴	root の SSH ログインはすべて [管理者 IP] から。2019 年にサイト用ユーザーが [不明 IP] からシェルログイン	要確認（低）：接続元に心当たりがあるか
不審なプロセス	一時領域や隠しパスから動くプロセスなし	異常なし
削除済みファイルで動くプロセス	named、dnsmasq、python、Xorg の 6 件。パッケージ更新後に再起動していないだけ	異常なし（再起動が必要）
/etc/ld.so.preload	存在しない	異常なし
cron・systemd・rc.local	Plesk、Imunify、OS 由来の登録のみ	異常なし
/tmp・/var/tmp・/dev/shm	実行ファイル・PHP ファイルなし	異常なし
Web シェルの典型パターン	該当は Imunify のスキャナ（AI-Bolit）自身の 5 ファイルのみ	異常なし（誤検知）
30 日以内に変更された PHP	170 件。すべて WordPress 本体・言語ファイルで、4 日分の深夜の数分間に集中。WP Toolkit の自動更新の時刻と一致	異常なし
uploads 配下の PHP	4 件とも「Silence is golden」か 404 を返すだけのディレクトリ保護用	異常なし（中身を確認済み）
RPM 管理外の SUID/SGID	Plesk の postdrop のみ	異常なし

4. 指摘事項一覧

緊急 3 件、高 5 件、中 5 件の計 13 件です。重大度は「悪用のされやすさ × 被害の大きさ」で判定しています。

ID	重大度	指摘	対処の要点
C1	緊急	root でパスワードによる SSH ログインが可能。パスワードは 2017 年から未変更。fail2ban の SSH 監視は 22 番ポート向けで、実際の SSH ポート（非標準）は監視外	鍵認証のみにし、root パスワードを変更、fail2ban の監視ポートを修正
C2	緊急	古い WordPress 7 サイト。うち 3 サイトは 2019 年の版の WordPress + PHP 5.4 で、悪用実績のあるプラグインを含む	不要なサイトは停止、残すサイトは本体・プラグインを更新
C3	緊急	OS のセキュリティ更新が 8 月 8 日以降未適用（97 件）。カーネルも再起動待ち	更新を適用して再起動
H1	高	全サイトがサポート終了の PHP（5.4〜8.1）で稼働	サイトごとに PHP 8.2 以降へ移行
H2	高	Plesk が古い版のまま（7 月の更新で複数の脆弱性を修正）。管理画面 8443・8880 番を全世界に公開し、8880 番は平文 HTTP	Plesk を更新し、管理画面を接続元 IP で制限
H3	高	POP3・IMAP・FTP・poppassd（106 番）で平文のパスワード送信を許可。TLS 1.0/1.1 も有効	平文認証を禁止し、TLS 1.2 以上に限定
H4	高	SELinux 無効、送信方向の通信制限なし、auditd のルールなし。侵入後の封じ込めと検知が効かない	送信制限と監査ルールを追加
H5	高	サポート終了のミドルウェア：MariaDB 5.5 系、2019 年の版の Elasticsearch（認証なし、ローカルのみ待受、未使用）	不要なら停止、必要なら更新
M1	中	不要なサービスが稼働：デスクトップ環境、CUPS、Avahi、Bluetooth、libvirt、Docker（コンテナ 0 件）	停止して無効化
M2	中	ファイアウォールが不要なポートを許可：3306、5432、137〜139、445、TCP 49152〜65535	許可ルールを削除・絞り込み
M3	中	期限切れの SSL 証明書を使う vhost が 12 件	更新するか、使っていないドメインを削除
M4	中	ログが再起動で消える設定、外部へのログ転送なし、時刻同期なし、rkhunter が 2025 年 4 月で停止	ジャーナルを永続化し、chronyd を有効化
M5	中	SSH・アカウント設定の甘さ：古い暗号方式の許可、X11 転送、サイト用ユーザーへの bash 付与、最小パスワード長 5 文字	設定を強化

5. 緊急の指摘と対処

C1 root のパスワード SSH ログイン

SSH は非標準ポートで公開され、`PermitRootLogin yes`・`PasswordAuthentication yes` です。root パスワードの最終変更は 2017 年 7 月で、9 年間同じパスワードが総当たりの的になっています。さらに fail2ban の `ssh` jail は 22 番ポートを監視しており、実際の SSH ポートへの総当たりは遮断されません。

Plesk 管理画面にも root のパスワードでログインでき、9 月 25 日から総当たりを受けています。記録元は Plesk の認証処理（sys_auth）で、接続元 IP は secure ログに残りません。fail2ban でも遮断できていないため、管理画面（8443 番）を接続元 IP で制限し、8880 番を閉じることを手順 1 より先に実施してください。

対処手順（既存の SSH セッションを 1 本開いたまま作業してください）：

1. 手元 PC で鍵ペアを作り、`/root/.ssh/authorized_keys` に公開鍵を登録する。シェルを使うサイト用ユーザーにも鍵を用意する。
2. `/etc/ssh/sshd_config` を `PermitRootLogin prohibit-password`、`PasswordAuthentication no`、`X11Forwarding no` に変更し、`sshd -t && systemctl reload sshd` で反映する。
3. 新しいセッションで鍵ログインできることを確認してから、`passwd` で root パスワードを長いランダム値に変更する（Plesk に root でログインしている場合も新パスワードに変わります）。
4. fail2ban の `ssh` jail の監視ポートを実際の SSH ポートに変更し、`fail2ban-client reload` で反映する。

C2 古い WordPress サイト

最新の WordPress に自動更新されている 3 サイト（サイト F・G・H）は問題ありません。残る 7 サイトは次のとおりです。

サイト	WordPress	PHP	主な問題	推奨
サイト A（3 サブドメイン）	5.1 系	5.4	Duplicator の古い版（認証なしで任意のファイルを読まれる脆弱性 CVE-2020-11738。2020 年に大規模悪用）、投稿内で PHP を実行できる exec-php、2019 年以前のプラグイン多数	停止、または静的 HTML 化して保存
サイト B	6.5 系	7.1	2017 年ごろの版のまま更新されていないプラグインが複数	更新、使っていなければ停止
サイト C	6.1 系	7.4	本体は 9/24 に自動で修正適用済みと推定。問題は MW WP Form の古い版で、ファイル添付欄があるフォームでは、認証なしで任意のファイルを置かれる脆弱性（CVE-2023-6316、5.0.2 で修正）	プラグインと本体を更新
サイト D	5.8 系	7.1	9/24 に `template.php` が自動更新されており、CVE-2026-87902 の修正は適用済みと推定。ただし 5.8 系は 2021 年の版で、プラグインも古い	最新版へ更新
サイト E	6.9 系	5.6	CVE-2026-87902 の修正（6.9.9）より前。直近 30 日に自動更新された形跡もない	最新版へ更新

CVE-2026-87902 は、PEAR の `pearcmd.php` を足がかりに悪用されています。このサーバーには PEAR がインストールされているため、悪用の前提条件の 1 つを満たしています。更新後は、Plesk の WP Toolkit で全サイトの自動更新（本体・プラグイン）を有効にしてください。

C3 OS のセキュリティ更新

OS の延長サポート（ELS）の契約があり、更新は提供されていますが、8 月 8 日以降適用されていません。未適用の修正は 97 件で、OpenSSL、libxml2、expat、apr-util、pcre2、PHP 5.4 に Critical 評価の修正があります。カーネル、OpenSSH、Apache、BIND も更新待ちです。

1. 仮想マシンのスナップショットを取得する。
2. `yum update` を実行する。
3. 再起動し、`needs-restarting -r` で再起動待ちがないことを確認する。

再起動で、古いバイナリのまま動いている named・dnsmasq なども新しい版に切り替わります。

6. 高の指摘と対処

H1 サポート終了の PHP

すべてのサイトが、公式のセキュリティサポートが終了した PHP で動いています。

PHP	公式サポート終了
5.4（OS 標準）	2015 年 9 月
5.6	2018 年 12 月
7.1	2019 年 12 月
7.4	2022 年 11 月
8.0	2023 年 11 月
8.1	2025 年 12 月

OS 標準の PHP 5.4 だけは延長サポートの修正が入りますが、Plesk 版の PHP は更新されていません。CentOS 7 で新しい PHP をどこまで使えるかには制約があるため、根本対策は AlmaLinux など新しい OS のサーバーへの移行です。サーバーには Plesk Migrator が導入済みなので、サイト単位の移行が使えます。

H2 Plesk の更新と管理画面の公開

Plesk は古い版のままで、7 月に出た更新ではセキュリティ監査を受けた複数の脆弱性修正が入っています。管理画面は 8443 番（HTTPS）と 8880 番（平文 HTTP）で全世界に公開されています。

1. ファイアウォールで 8443 番を管理者の接続元 IP だけに許可し、8880 番は外部から閉じる。Plesk の「管理アクセスの制限」でも同じ制限ができます。
2. Plesk を最新版へ更新する。CentOS 7 と延長サポートの組み合わせでは、依存関係で更新が失敗する報告が Plesk フォーラムに出ているため、スナップショットを取ってから実施してください。

H3 平文のパスワード送信

Dovecot が `disable_plaintext_auth = no` のため、POP3（110）と IMAP（143）で暗号化なしのパスワードを受け付けます。FTP（21）と poppassd（106）も公開されています。nginx・Dovecot・Postfix は TLS 1.0/1.1 も許可しています。

1. Dovecot の独自設定ファイルで `disable_plaintext_auth = yes` を指定する。
2. FTP は SFTP への切り替えを案内したうえで 21 番を閉じるか、FTPS を必須にする。106 番はファイアウォールで閉じる。
3. Plesk の `sslmng` でメール・Web の TLS を 1.2 と 1.3 に限定する。

H4 侵入後の封じ込めと検知

SELinux は無効で、送信方向の通信（OUTPUT）はすべて許可、auditd にはルールが 1 つもありません。サイトが乗っ取られた場合、外部からのツール取得やリバースシェルを止める仕組みも、記録する仕組みもない状態です。

1. サイト用ユーザー（`psacln` グループ）の送信先を、HTTP/HTTPS・DNS・SMTP など必要なポートに限定する iptables ルールを追加する。
2. auditd に、`/etc/passwd`・`/etc/shadow`・sudoers・`sshd_config`・cron の変更監視と、サイト用ユーザーによるコマンド実行の記録を追加する。
3. SELinux の有効化は Plesk との相性確認が必要なため、新サーバーへの移行時に組み込む。

H5 サポート終了のミドルウェア

- **MariaDB 5.5 系：** 上流のサポートは 2020 年に終了しています。Plesk の手順で MariaDB 10 系へ更新してください。
- **Elasticsearch（2019 年の版）：** 待受はサーバー内部（localhost）のみで外部からは届きません。ただし認証がないため、どれか 1 サイトが乗っ取られると、そのサイト経由でデータを読み書きされます。インデックスは 0 件で使われていないため、`systemctl disable --now elasticsearch` で停止し、パッケージも削除してください。

7. 中の指摘と対処

M1 不要なサービス

Web サーバーなのに、デスクトップ環境（gdm・Xorg・GNOME）、印刷（CUPS）、Avahi、Bluetooth、ModemManager、wpa_supplicant、仮想化（libvirt・dnsmasq）、Docker（コンテナ 0 件）が動いています。Docker グループには Plesk の `psaadm` が入っており、これは root 権限と同等です。

`virsh list --all` で仮想マシンがないことを確認したうえで、不要なものを `systemctl disable --now` で止め、`systemctl set-default multi-user.target` で起動時のデスクトップを無効にします。Docker と libvirt を外せば、`net.ipv4.ip_forward` も 0 にできます。

M2 ファイアウォールの不要な許可

MySQL（3306）、PostgreSQL（5432）、SMB（137〜139、445）が許可されています。現在は待ち受けていないため実害はありませんが、将来サービスを起動した瞬間に外部へ公開されます。TCP 49152〜65535 の一括許可も、パッシブ FTP 用であれば ProFTPD の使用範囲に絞ってください。Plesk のファイアウォール画面から削除できます。

M3 期限切れの SSL 証明書

12 件の証明書（複数ドメインの共用証明書を含む）が、2018 年〜2026 年 7 月に期限切れになったまま使われています。DNS が別サーバーを向いて自動更新に失敗している可能性があります。使っているドメインは更新し、使っていないドメインは Plesk から削除してください。

M4 ログと時刻

- `/var/log/journal` がなく、systemd のログは再起動で消えます。ディレクトリを作成して永続化してください。
- ログの外部転送がないため、侵入者がログを消すと追跡できません。
- chronyd が無効で、時刻合わせは 1 日 1 回の ntpdate だけです。ログの時刻がずれると調査に支障が出るため、chronyd を有効にしてください。
- rkhunter の最終実行は 2025 年 4 月です。Imunify で代替できているなら削除して構いません。

M5 SSH・アカウント・カーネル設定

- SSH が 3DES・Blowfish・CBC 系の暗号や `diffie-hellman-group1-sha1` を許可しています。`Ciphers`・`MACs`・`KexAlgorithms` を現行の方式に限定し、`GSSAPIAuthentication no` にしてください。
- サイト用ユーザーの 1 つにシェル `/bin/bash` が付与されています。Plesk で chroot 付きシェルか「シェルなし」に変更してください。
- 最小パスワード長が 5 文字（`PASS_MIN_LEN 5`）です。12 文字以上を推奨します。
- `kernel.dmesg_restrict = 0`、`kernel.yama.ptrace_scope = 0`、`net.ipv4.conf.all.send_redirects = 1` です。それぞれ 1・1・0 にしてください。

8. 評価できる点

- **OS の延長サポート（ELS）の契約：** サポートが終了した CentOS 7 でも、カーネルや主要パッケージの修正を受け取れる状態です。適用さえすれば最新の修正が入ります。
- **多層の防御製品：** Imunify360（マルウェア検知・WordPress 保護）、ModSecurity（WAF）、fail2ban（14 jail）が稼働しています。
- **ファイアウォールの基本方針：** 受信は既定で遮断し、必要なポートだけを許可する構成です。
- **内部サービスの待受：** MariaDB、Elasticsearch、Grafana は localhost のみで待ち受けており、外部から直接は届きません。
- **一時領域の分離：** Web・PHP・DB の各サービスが専用の一時ディレクトリ（PrivateTmp）を使っています。
- **WordPress の自動更新：** 3 サイトは WP Toolkit で最新版まで自動更新されています。

9. 追加確認

「要確認」の項目に白黒をつけるため、読み取りのみのコマンドを 2 回に分けて実行していただきました。

1 回目（実施済み）

```
# 1. root パスワード失敗：日別の件数と、どのサービスが記録しているか
zgrep -h 'password check failed for user (root)' /var/log/secure* | awk '{print $1,$2}' |
sort | uniq -c
grep -h -B3 'password check failed for user (root)' /var/log/secure-20261004 | head -40

# 2. 内容が変化したシステムファイルの由来
ls -la --time-style=full-iso /usr/sbin/suexec /usr/sbin/postdrop \
    /usr/lib64/httpd/modules/mod_proxy.so /usr/lib64/httpd/modules/mod_proxy_fcgi.so
for f in /usr/sbin/suexec /usr/sbin/postdrop /usr/lib64/httpd/modules/mod_proxy*.so; do
  echo "== $f"; strings "$f" | grep -iE 'plesk|psa' | head -3
done

# 3. uploads 配下の小さな PHP ファイルの中身
cat /var/www/vhosts/<サイト>/httpdocs/…/wp-content/uploads/<プラグイン>/index.php  # ほか 3 件

# 4. Elasticsearch を使っているか（インデックスの一覧）
curl -s 'http://localhost:9200/_cat/indices?v'
```

結果、uploads 配下の PHP と suexec・postdrop は問題なしと確定し、Elasticsearch は未使用と分かりました。

2 回目（依頼中）

残りは、総当たりの接続元と、ログイン成功の有無です。

```
# A. Plesk 管理画面へのログイン試行の接続元 IP（上位 20）
grep -h 'login_up' /var/log/plesk/httpsd_access_log* | awk '{print $1}' | sort | uniq -c |
sort -rn | head -20

# B. mod_proxy 系が Plesk パッケージの正規ファイルか（何も出力されなければ一致）
rpm -V psa-mod_proxy
```

あわせて、Plesk の「ツールと設定」→「アクションログ」で、9 月 25 日以降に心当たりのない管理者ログインや設定変更がないかを確認していただきます。

10. 是正ロードマップ

今日と今週で緊急 3 件と、外部から突かれやすい高の指摘を片付け、OS 移行で根本解決する順番です。

今日

- ☐ 仮想マシンのスナップショットを取得（C3）
- ☐ SSH を鍵認証のみにし、root パスワードを変更（C1）
- ☐ fail2ban の ssh jail の監視ポートを修正（C1）
- ☐ 最優先：管理画面 8443 番を接続元 IP で制限し、8880・106 番を外部から閉じる（C1・H2・H3）

今週

- ☐ `yum update` を適用して再起動（C3）
- ☐ サイト A（3 サブドメイン）を停止または静的化（C2）

- ☐ 残る古い WordPress 4 サイトを更新し、WP Toolkit の自動更新を全サイトで有効化（C2）
- ☐ Dovecot の平文認証を禁止し、TLS を 1.2 以上に限定（H3）
- ☐ 追加確認のコマンドを実行し、要確認の項目を判定

今月

- ☐ Plesk を最新版へ更新（H2）
- ☐ 送信方向の通信制限と auditd ルールを追加（H4）
- ☐ Elasticsearch を停止・削除（H5）
- ☐ 不要なサービスとファイアウォールの許可を整理（M1・M2）
- ☐ 期限切れ証明書の更新・不要ドメインの削除（M3）
- ☐ ログの永続化、chronyd 有効化、SSH 暗号方式の整理（M4・M5）

中期（3 か月以内）

- ☐ AlmaLinux など新しい OS のサーバーを用意し、Plesk Migrator でサイトを移行（H1・H5）
- ☐ 新サーバーで PHP 8.3 以降、MariaDB 10 系以降、SELinux 有効で構築（H1・H4・H5）
- ☐ 移行後に同じ手順で再診断し、改善前後を比較

出典

- Plesk Obsidian 18.0.79 リリース告知（2026-07-03）：https://www.plesk.com/blog/2026/07/03/
- Plesk フォーラム（CentOS 7 のサポートに関するスレッド）：https://talk.plesk.com/threads/support-for-centos-7-soon.306306/
- The Hacker News（WordPress CVE-2026-87902 の悪用）：https://thehackernews.com/2026/09/attackers-exploit-wordpress-cve-2026.html