サイトドック セキュリティ証跡レポート

対象サイト　demo.example.jp　　対象期間　2025-11-01 〜 2025-11-30　　発行日　2025-12-01

発行：日本情報基盤サービス株式会社 ／ JIISセキュリティラボ（兵庫県神戸市中央区御幸通8丁目1-6 神戸国際会館22F）

1 サマリ

60 / 100

要注意

診断スコア 60 点（前月比 -1）

新規 1 件　継続 12 件　解消 0 件

自動修復	エッジでの防御	改ざんチェック
0 回適用	323 件一致	0 件検知
検証済み 0 件	ポリシールールに一致したリクエスト	うち確認済み 0 件

2 今回の新規検出

情報　新規　X-Powered-By ヘッダで実装が分かる状態です

何が問題か　使用している実装を外から特定できます。

治し方　アプリ設定で X-Powered-By ヘッダの送出を無効にしてください。

該当　`https://demo.example.jp/`

3 自動修復の適用と検証

この期間に新たな適用はありません。

防御設定の強化履歴

影響を確かめながら、防御設定を段階的に強くしています。各段は観測データ（読み込みの制限に反した回数・アクセス実績・適用後の確認）が条件を満たしたときにだけ上げています。

この期間に防御設定の変更はありません。

オリジン保護：適用済み（最終確認 2026-07-14）　／　証明書の有効期限：2026-11-02

4 エッジでの防御実績



動作	どのように扱われたか	一致したリクエスト数
ブロック block	ルールに一致したリクエストをエッジで止め、オリジン（お客様のサーバ）へは渡していません。	254
自動判定チャレンジ managed_challenge	自動化されたアクセスかどうかを確かめる画面を挟みます。人による操作であれば、そのまま閲覧を続けられます。	47
記録のみ log	記録だけを行い、リクエストはそのまま通しています（新しいルールの影響を確かめる段階で使います）。	22
参考：総リクエスト		23980

件数は、Cloudflare のポリシールールに一致したリクエスト数です。一致したリクエストのすべてが攻撃とは限らず、また、ここに現れないアクセスが安全であることを示すものでもありません。

5 注意喚起：ポリシールールに一致しなかった攻撃と疑われるアクセス

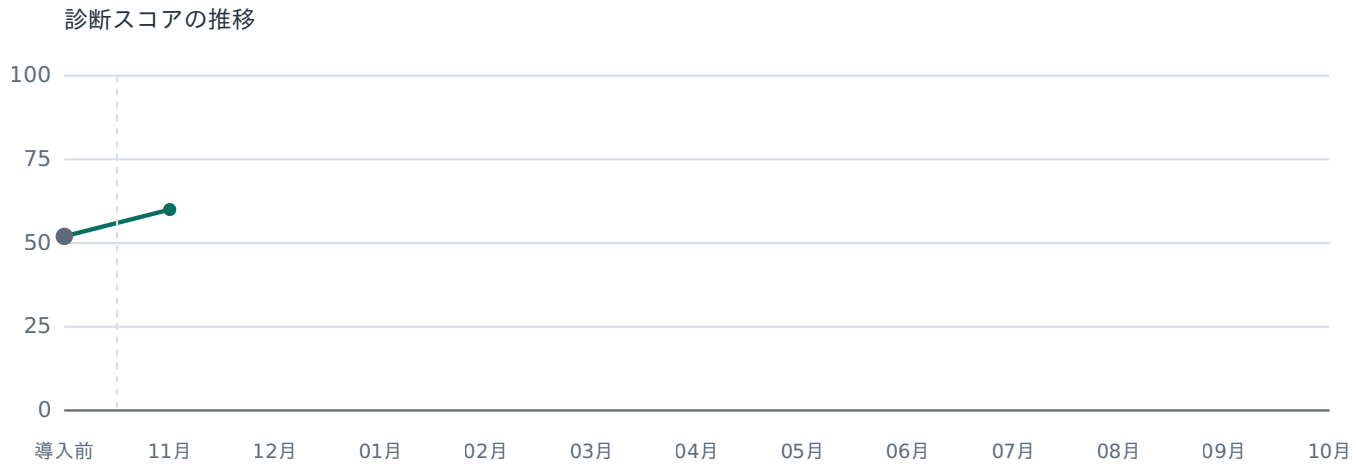
この期間、対処が必要と判断したアクセスはありません。

ポリシールールに一致しなかったアクセスのうち、攻撃の試行が疑われるものをお知らせします。被害の有無を示すものではありません。対応が必要と判断した場合は、対策案を起案したうえで、適用の可否を弊社担当者とご相談のうえ決定します。

6 改ざんチェックの状況

この期間、不正な変更は検知されませんでした。

7 診断スコアの推移



8 総評（残っている課題と次の対応）

残っている課題（新規・継続の指摘）と、次にとるべき対応の整理です。エッジ（通り道）で対処できる範囲と、根本改修が必要な範囲に分けて示します。

残っている課題：　中 5 件　低 6 件　情報 2 件（新規 1 件・継続 12 件）

エッジで対処できる範囲（投薬）　10 件

- 情報　X-Powered-By ヘッダで実装が分かる状態です
- 中　HSTS（常時HTTPS）が有効になっていません
- 中　X-Content-Type-Options が設定されていません
- 中　Content-Security-Policy が設定されていません
- 低　Cookie に Secure 属性が設定されていません
- ほか 5 件

ヘッダの調整や仮想パッチなど、エッジでの対処を適用中、または適用をご提案します。エッジでの対処は影響の緩和であり、根本原因を取り除くものではありません。

根本改修が必要（開発会社の領域＝手術）　3 件

- 中　古い TLS バージョンが有効になっています
- 中　HTTP から HTTPS への転送が設定されていません
- 低　問い合わせページにメールアドレスが平文で掲載されています

アプリケーションやサーバ内部の改修が必要な事項です。サイトを構築した開発会社さまでの根本改修をご検討ください。進め方は弊社担当者にもご相談いただけます。

9 参考情報（継続中の所見・バックナンバー）

危険度	タグ	内容	該当
中	継続	古い TLS バージョンが有効になっています	https://demo.example.jp/
中	継続	HTTP から HTTPS への転送が設定されていません	http://demo.example.jp/
中	継続	HSTS（常時HTTPS）が有効になっていません	https://demo.example.jp/
中	継続	X-Content-Type-Options が設定されていません	https://demo.example.jp/
中	継続	Content-Security-Policy が設定されていません	https://demo.example.jp/
低	継続	Cookie に Secure 属性が設定されていません	https://demo.example.jp/login
低	継続	X-Frame-Options が設定されていません	https://demo.example.jp/
低	継続	Referrer-Policy が設定されていません	https://demo.example.jp/
低	継続	Permissions-Policy が設定されていません	https://demo.example.jp/
低	継続	問い合わせページにメールアドレスが平文で掲載されています	https://demo.example.jp/contact
情報	継続	サーバのバージョン情報が応答ヘッダに出ています	https://demo.example.jp/
低	継続	ディレクトリの一覧が表示されるパスがあります	https://demo.example.jp/assets/

過去12ヶ月の記録

年月	スコア	等級	高	中	低
2024-12	38	危険	2	6	9
2025-01	37	危険	2	7	9
2025-02	41	危険	2	6	9
2025-03	43	危険	2	6	8
2025-04	42	危険	2	6	9
2025-05	46	危険	2	6	8
2025-06	48	危険	2	5	8
2025-07	50	要注意	2	5	7
2025-08	52	要注意	2	5	7
2025-09	55	要注意	1	5	7
2025-10	61	要注意	0	5	7
2025-11	60	要注意	0	5	8

10 付録：診断の範囲と留意事項

- 本レポートは、外部から確認できる範囲の診断結果と、エッジ（通り道）での適用状況をまとめたものです。
- 診断は、サービス停止を狙う検査を行わない範囲で実施しています。検査用の文字列を送る能動診断は、ご同意いただいたサイトに限り実施します。
- 記載のない事項について、問題が存在しないことを保証するものではありません。
- 自動修復はエッジでの緩和であり、サーバ内部やアプリケーションの改修が必要な事項は別途ご案内します。

証跡の検証用ハッシュ：3f9a000000000000000000000000000000000000000000000000000000000c21e（2025-11-30時点）