

これはサンプルレポートです(架空のデータ)。実際の診断結果ではありません。



Mii Secure Scan by Miichisoft

外部セキュリティ診断レポート

<https://sample-shop.example.jp>

診断種別	Advanced（メール認証・詳細診断(非侵入)）
診断実施日	2026-10-27
レポートID	SAMPLE0001
エンジン版	0.22.0 / DB
作成	Mii Secure Scan by Miichisoft

機密区分: 社外秘(取引先共有可)

総合評価

C

72 / 100

指摘 5 件（脆弱性 2 ・ 設定 5） **KEV該当 1件**

■ 重大 0 ■ 高 2 ■ 中 3 ■ 低 0

本レポートは診断時点のスナップショットであり、脆弱性が存在しないことを保証するものではありません。

エグゼクティブサマリー

総合評価

C

72 / 100

いくつかの改善点が見つかりました。計画的な対応をおすすめします。検出した脆弱性のうち **1件** は、悪用が実証されている(CISA KEV)ものに該当する可能性があります。該当可否の確認と優先的な対応のご検討をおすすめします。

確認済みの設定事項 **5 件**
脆弱性(CVE・推定) **2 件 (うちKEV該当 1件)**
検出技術スタック nginx、wordpress



優先して確認・対応したい項目

- **高** nginx 1.20.1 に既知の脆弱性(推定・要確認)
- **高** 重要なセキュリティヘッダ(Content-Security-Policy)が未設定です
- **中** Cookie に Secure / HttpOnly 属性が付与されていません

※ 深刻度は 重大 / 高 / 中 / 低 の4段階。確度は「確定(外部から確認)」と「推定(要確認)」を区別しています。

診断範囲と手法

診断対象	https://sample-shop.example.jp
診断の種類	Advanced — ドメイン所有確認のうえで詳細を開示する非侵襲的(パッシブ)な診断です。
参照データ	NVD(CVE/CVSS)・CISA KEV(悪用実績)・EPSS(悪用確率)・JVN(国内脆弱性情報)・OSV(サプライチェーン)・endoflife.date(EOL)
確度の定義	確定: 外部から直接確認できた設定事項。 推定(要確認): バナー/バージョン表示などからの推定で、誤検知・バックポートの可能性を含みます。
深刻度の基準	CVSS・KEV該当・外部からの到達性を踏まえ 重大/高/中/低 に区分。

Standardは外部から取得できる情報のみで判定するため、バージョン推定を含み、誤検知・見落としが生じ得ます。Advancedでは推定を検証して確定し、依存関係(SBOM)まで確認します。

指摘事項一覧

ID	深刻度	確度	指摘	CVSS	KEV
CVE-2021-23017	■ 高	推定(要確認)	nginx 1.20.1 に既知の脆弱性(推定・要確認)	—	有
MII-RULE-header-csp	■ 高	外部から確認	重要なセキュリティヘッダ(Content-Security-Policy)が未設定です	—	—
MII-RULE-cookie-attr	■ 中	外部から確認	Cookie に Secure / HttpOnly 属性が付与されていません	—	—
MII-RULE-tls-weak	■ 中	外部から確認	TLS 設定に古い暗号スイートが含まれています	—	—
CVE-2023-XXXXX	■ 中	推定(要確認)	WordPress 6.1 系に既知の脆弱性(推定・要確認)	—	—

指摘事項の詳細

CVE-2021-23017

■ 高

推定(要確認)

nginx 1.20.1 に既知の脆弱性(推定・要確認)

影響を受ける可能性のある資産

nginx

CISA KEV(悪用実績)

該当あり(既知の悪用あり・本サイトの被害有無は要確認)

推奨対応

nginx を修正済みバージョン（1.20.1 以降）へ更新してください。※ Server バナーからの推定のため、ディストリのバックポート修正により実際には対策済みの可能性があります(要確認)。

参考情報

- ・ nvd.nist.gov ↗
- ・ mailman.nginx.org ↗

※ 本指摘はバナー/バージョン表示など外部から取得できる情報に基づく推定です。バックポート修正や設定により実際には影響しない場合があります。Advanced(ドメイン認証)で確定できます。

MII-RULE-header-csp

■ 高

外部から確認

重要なセキュリティヘッダ(Content-Security-Policy)が未設定です

推奨対応

Content-Security-Policy ヘッダを設定し、スクリプトの読み込み元を信頼できるドメインに制限してください。

参考情報

- ・ owasp.org ↗

MII-RULE-cookie-attr

■ 中

外部から確認

Cookie に Secure / HttpOnly 属性が付与されていません

推奨対応

Cookie に Secure 属性と HttpOnly 属性を付与してください。SameSite 属性の設定も推奨します。

参考情報

- ・ owasp.org ↗

MII-RULE-tls-weak

■ 中

外部から確認

TLS 設定に古い暗号スイートが含まれています

推奨対応

TLS 1.0 / 1.1 および脆弱な暗号スイートを無効化し、TLS 1.2 以降のみを有効にしてください。

参考情報

- ・ ssl-config.mozilla.org ↗

CVE-2023-XXXXX

■ 中

推定(要確認)

WordPress 6.1 系に既知の脆弱性(推定・要確認)

影響を受ける可能性のある資産 wordpress

CISA KEV(悪用実績) 該当なし

推奨対応

WordPress を最新版へ更新してください。※ バージョン表示からの推定です。実際の該当可否は Advanced 診断で確定できます(要確認)。

参考情報

- ・ nvd.nist.gov ↗
- ・ wordpress.org ↗

※ 本指摘はバナー/バージョン表示など外部から取得できる情報に基づく推定です。バックポート修正や設定により実際には影響しない場合があります。Advanced(ドメイン認証)で確定できます。

資産・攻撃対象領域

検出技術スタック nginx、wordpress

外部から確認できた良好な設定

- ・ 特記事項なし

Advanced(ドメイン認証)では、サブドメイン・ポート・依存ライブラリ(SBOM)を含む攻撃対象領域を確認できます。

対応ロードマップ

今すぐ対応を検討 (1件)

深刻度	確度	指摘
■ 高	推定(要確認)	nginx 1.20.1 に既知の脆弱性(推定・要確認)

30日以内を目安に対応 (1件)

深刻度	確度	指摘
■ 高	外部から確認	重要なセキュリティヘッダ(Content-Security-Policy)が未設定です

計画的に対応 (3件)

深刻度	確度	指摘
■ 中	外部から確認	Cookie に Secure / HttpOnly 属性が付与されていません
■ 中	外部から確認	TLS 設定に古い暗号スイートが含まれています
■ 中	推定(要確認)	WordPress 6.1 系に既知の脆弱性(推定・要確認)

対応後は再診断で改善状況をご確認いただけます。

より詳細な診断について

本レポートはStandard(パッシブ・公開情報のみ)診断の結果です。対象ドメインのメール認証による深い診断(Advanced・無料)で、

推定の該当可否を確定し、依存関係(SBOM)まで確認できます。攻撃シナリオの検証から修正・システム移行の実施までは、**受託診断 (Professional)**にて承ります。

付録

A. 用語集

CVE	共通脆弱性識別子。個別の脆弱性に付与される番号。
CVSS	脆弱性の深刻度を0～10で表す指標。
KEV	CISAが公開する「悪用が確認された脆弱性」カタログ。
EPSS	今後30日以内に悪用される確率の推定値。
SBOM	ソフトウェア部品表。依存ライブラリの一覧。
推定 / 確定	推定=外部情報からの判定(要確認)。確定=検証済み。

B. 診断の制約事項

- ・ パッシブ診断は公開情報の読み取りに基づくため、誤検知・見落としが生じ得ます。
- ・ WAF/CDN の影響で実際の構成と異なる場合があります。
- ・ 内部・認証後の診断、ソーシャルエンジニアリングは含みません。
- ・ バージョンはパナー/ファイル名からの推定を含み、バックポート修正を判別できない場合があります。

Mii Secure Scan by Miichisoft ・ レポートID SAMPLE0001 ・ お問い合わせは当社サイトのお問い合わせフォームよりお願いいたします。