# サイトドック　Webサイト セキュリティ診断レポート

| | | | |
|---|---|---|---|
| 診断対象 | https://www.example-sample.jp | | |
| システム名 | サンプル株式会社 コーポレートサイト | 診断日 | 2026/06/03 |
| IPアドレス | 203.0.113.10 | 確認状況 | ✓ 所有者確認済み |

60
/ 100点

## 外から見える弱点が見つかりました

公開情報の範囲だけでも改善すべき点が見つかりました。早めの対応をおすすめします。

緊急 1 件　要改善 4 件　情報 1 件

検出6件のうち、3件は申込後すぐ自動で治せます。1件は攻撃を自動でブロックしながら、根本対応を専門家がご案内します。

サイトドックの自動修復（月額）＝セキュリティヘッダ注入・Cookie属性付与・常時HTTPS・攻撃ブロック（仮想パッチ）・改ざん検知をエッジで自動適用。料金は sitedock.jp/service をご覧ください。

## 対応すべき順に並べています（上から着手してください）

### 緊急対応（1件）

緊急　**WordPressに既知の脆弱性**　攻撃を自動で防げます　WordPress既知脆弱性（CVE-2022-21661）

何が問題か　WordPress本体・プラグイン・テーマに、公表済みの脆弱性を含むバージョンが使われています。攻撃コードが出回っている場合、乗っ取りや改ざんを試される恐れがあります。

治し方　該当する本体・プラグイン・テーマを、脆弱性が修正された最新版へ更新します。未使用のプラグイン/テーマは削除し、自動更新の有効化も検討してください。

自分で根本改修する（上記の治し方・無料）のほか、仮想パッチで攻撃を今すぐ自動ブロックできます（根本改修は専門家がご案内します）。

作業目安：更新作業（影響確認含む）　要：WordPress管理　整理番号：WP_20260603000000-001

検出内容：WordPress本体 5.8.1：格納型クロスサイトスクリプティング（XSS）の脆弱性があります。投稿スラッグ経由で任意のスクリプトを埋め込まれる恐れがあります。

### 要改善（4件）

要改善　**SSHの暗号設定が古い**　専門家の対応が必要　SSH脆弱な暗号方式（CVE-2008-5161）

何が問題か　SSHサーバが、現在は安全でないとされる鍵交換方式・暗号方式（CBCモード、1024ビット以下のDiffie-Hellman、旧式のKEXアルゴリズム等）を許可しています。通信の盗聴・改ざんや、解読の足がかりにされる恐れがあります。

治し方　SSHサーバ設定で、弱い暗号方式・鍵交換方式・MACを無効化し、現行の強い方式のみに限定します。設定変更後は既存クライアントの接続可否を確認してください。

```
例）/etc/ssh/sshd_config: KexAlgorithms / Ciphers / MACs を強い方式に限定して再起動
```

この項目はエッジでは治せません。改善の伴走支援（お見積もり）または上記の手順をご利用ください。

※ エッジ（Cloudflare）では技術的に対処できない項目です。エッジ収容によりオリジンIPの露出自体を抑える副次効果があります

作業目安:30分〜1時間　要:サーバ設定　整理番号：NV_20260603000000-001

検出内容:SSH Server CBC Mode Ciphers Enabled

要改善 **通信が保護に切り替わらない** 自動で治せます　HSTS未設定

何が問題か　初回アクセスや手入力時にHTTPへ誘導され、盗聴・改ざんされた通信に乗せられる余地が残ります。

治し方　HTTPSレスポンスに Strict-Transport-Security ヘッダを追加します。まず短いmax-ageで動作確認し、問題なければ延長します。

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
```

自分で治す（上記の治し方・無料）のほか、サイトドックの自動修復（申込後すぐ反映・月額）でもそのまま治せます。

作業目安:15分　要:サーバ設定　整理番号：NI_20260603000000-001

検出内容:SSLを使用していますが、Strict-Transport-Security HTTPヘッダーが定義されていません。HSTSの設定を有効化することを推奨致します。(/)

要改善 **ファイル種別の誤認を突かれる** 自動で治せます　X-Content-Type-Options未設定

何が問題か　ブラウザがファイル種別を推測してしまい、本来無害なファイルがスクリプトとして実行されるなどの誤動作を突かれる恐れがあります。

治し方　全レスポンスに nosniff を付与し、種別の推測を止めます。

```
add_header X-Content-Type-Options "nosniff" always;
```

自分で治す（上記の治し方・無料）のほか、サイトドックの自動修復（申込後すぐ反映・月額）でもそのまま治せます。

作業目安:10分　要:サーバ設定　整理番号：NI_20260603000000-002

検出内容:X-Content-Type-Optionsヘッダーが設定されていません。「nosniff」が設定されていることを確認してください。(/)

要改善 **使用ソフトのバージョンが見えている** 自動で治せます　ソフトウェア露出

何が問題か　サーバ種別やバージョンが外から読め、古い場合は既知の弱点を狙い撃ちされやすくなります。

治し方　Serverヘッダ等からバージョン表記を抑制し、ミドルウェアを最新に保ちます。

```
server_tokens off;   # nginx の場合
```

自分で治す（上記の治し方・無料）のほか、サイトドックの自動修復（申込後すぐ反映・月額）でもそのまま治せます。

作業目安:15分　要:サーバ設定　整理番号：ZA_20260603000000-001

検出内容:Serverヘッダにソフトウェアのバージョンが表示されています（nginx/1.18.0）。

## 参考情報（1件）

情報　公開ポート 2件　専門家の対応が必要　　公開ポート

何が問題か　外部から到達できるポートです。必要なものに絞れているか確認が必要です。

治し方　不要なポートはファイアウォール/セキュリティグループで閉じます。

この項目はエッジでは治せません。改善の伴走支援（お見積もり）または上記の手順をご利用ください。

※ エッジ（Cloudflare）では技術的に対処できない項目です。エッジ収容によりオリジンIPの露出自体を抑える副次効果があります

作業目安：確認のみ　要：ネットワーク管理　整理番号：PS_20260603000000-001

検出内容：ssh (22/tcp)、smtp (25/tcp)

### 小さなほころびを、そのままにしないために

「割れ窓理論」— 小さなほころびを放置すると、全体の管理が行き届かなくなる、という考え方があります。今回の 5件 は、同じ体制で運用されている他のサイトや社内システムにも、似た見直しポイントがあるかもしれない、という手がかりです。この機会に、範囲を広げた点検をご検討ください。

この診断で確認できたのは公開サイトのうち外から見える範囲です。サブドメイン・社内ネットワーク・ 認証基盤（AD/Entra ID）・退職者アカウント・EOL機器などは、外部からの自動診断では確認できません。これらを含めた組織全体の状態は、専門家によるアセスメントで把握できます。

検出項目の自動修復（月額）、気になる項目の改善への伴走支援、見えていない範囲を含めた全体診断について、無料でお見積もり・ご相談を承ります。下記の連絡先、またはサイトドックの相談フォームよりお気軽にお問い合わせください。

※ 検査の性質上、結果には過検知・誤検知が含まれる場合があります。対応の前に内容のご確認をおすすめします。
※ 修正後に再診断しても結果が変わらない場合は、対象サイトの CDN・WAF・リバースプロキシ等のキャッシュをクリアのうえ再診断してください（古い応答がキャッシュ配信され最新状態が反映されないことがあります）。
本レポートは所有者確認済みの範囲で実施しています。
JIISセキュリティラボ ／ 自治体情報セキュリティクラウド運用・支援実績多数
運営：日本情報基盤サービス株式会社（兵庫県神戸市中央区御幸通8丁目1-6 神戸国際会館22F）　www.jiis.co.jp