サイトドック　Webサイト セキュリティ健診レポート

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	健診日	2026/06/03
IPアドレス	203.0.113.10	確認状況	✓ 所有者確認済み

6
/ 100点

至急の対応が必要な弱点があります

外から見える範囲で、優先的に対応すべき重大な弱点が見つかりました。

緊急 3 件　要改善 7 件　情報 1 件

検出11件のうち、6件は申込後すぐ自動で直せます。2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/autofix 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（3件）

緊急　**サーバを乗っ取られうる重大な欠陥**　攻撃を自動で防げます　OSコマンドインジェクション

何が問題か　入力値がサーバ上でOSコマンドの一部として実行され得る状態です。攻撃者に任意のコマンドを実行されると、データの窃取・改ざん・暗号化（ランサムウェア）や、他サーバ攻撃の踏み台化など、事実上のサーバ乗っ取りに直結する最も危険な脆弱性です。

直し方　外部コマンドの呼び出しを避け、言語標準のAPIで処理します。やむを得ず実行する場合はシェルを介さず引数を配列で渡し（shell=False）、入力値は許可リストで厳格に検証します。

```
× os.system('ping '+host)   →   ○ subprocess.run(['ping','-c','1',host])
```

自分で根本改修する（上記の直し方・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：要改修・最優先（半日〜）　要：アプリ改修　整理番号：ZA_20260603000000-001

検出内容：Remote OS Command Injection

緊急　**ログイン情報が盗まれうる**　自動で直せます　Cookie HttpOnly未設定

何が問題か　ページに混入したスクリプト(XSS等)からセッションCookieを読み取られ、利用者になりすましてログイン操作をされる恐れがあります。

直し方　ログインに関わるCookieに HttpOnly と Secure を付与します。可能なら SameSite も設定してください。

```
Set-Cookie: session=...; HttpOnly; Secure; SameSite=Lax
```

自分で直す（上記の直し方・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）でもそのまま直せます。

作業目安:1〜2時間　要:アプリ改修　整理番号：ZA_20260603000000-002

検出内容:cookieにHttpOnly属性が設定されていません。

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。

直し方　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（上記の直し方・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（7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。

直し方　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直せません。改善代行（お見積もり）または上記の手順をご利用ください。

※ 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　自動で直せます

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。

直し方　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;
```

自分で直す（上記の直し方・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）でもそのまま直せます。

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 **画面を乗っ取られる恐れ** 自動で直せます X-Frame-Options未設定

何が問題か　貴社の画面を透明な枠で覆い被せ、利用者に気づかせず操作させるクリックジャッキング攻撃を受ける余地があります。

直し方　X-Frame-Options か、より新しい CSP frame-ancestors で他サイトからの埋め込みを禁止します。

```
add_header Content-Security-Policy "frame-ancestors 'self'" always;
```

自分で直す(上記の直し方・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)でもそのまま直せます。

作業目安:15分　要:サーバ設定　整理番号：NI_20260603000000-002

検出内容:X-Frame-Optionsヘッダが存在しません。クリックジャック対策のため、このヘッダを設定することを検討してください。(/)

要改善 **ファイル種別の誤認を突かれる** 自動で直せます 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。

直し方　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;
```

自分で直す(上記の直し方・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)でもそのまま直せます。

作業目安:10分　要:サーバ設定　整理番号：NI_20260603000000-003

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 **不正スクリプトの実行を抑止できない** 自動で直せます CSP未設定

何が問題か　読み込み元の制限が無いため、混入した不正スクリプトの実行や情報送信を防ぐ最後の砦が機能しません。

直し方　Content-Security-Policy を段階的に導入します。まず Report-Only で影響を観測し、Googleアナリティクス・タグマネージャ・利用中のCDN等、必要な外部参照先を許可リストに加えてから、強制(Content-Security-Policy)へ切り替えます。全てを自サイト('self')に限定する必要はなく、使っている正規の外部サービスは明示的に許可して構いません。

```
Content-Security-Policy: default-src 'self'; script-src 'self' https://www.googletagmanager.com;
connect-src 'self' https://*.google-analytics.com
```

自分で直す(上記の直し方・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)でもそのまま直せます。

作業目安:数時間～(サイト構成に依存)　要:サーバ設定・動作確認　整理番号：ZA_20260603000000-003

検出内容:Content-Security-Policy ヘッダーが設定されていません。

要改善 **使用ソフトのバージョンが見えている** 自動で直せます 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。

直し方　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
```

自分で直す（上記の直し方・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）でもそのまま直せます。

作業目安:15分　要:サーバ設定　整理番号：ZA_20260603000000-004

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）。

要改善　ユーザ名が列挙される　専門家の対応が必要　WordPressユーザ列挙

何が問題か　ログインユーザ名が外部から列挙できます。ユーザ名が分かると、総当たり（ブルートフォース）ログイン攻撃の足がかりになります。

直し方　author アーカイブ/REST API/ログインエラー差異からのユーザ名露出を抑制し、ログイン試行回数制限・多要素認証・強固なパスワードを導入します。

この項目はエッジでは直せません。改善代行（お見積もり）または上記の手順をご利用ください。

作業目安:設定・プラグイン導入（1〜2時間）　要:WordPress管理　整理番号：WP_20260603000000-002

検出内容:ユーザ:ユーザ名が外部から列挙できます（admin）。総当たり攻撃の足がかりになります。

参考情報（1件）

情報　公開ポート 4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。

直し方　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直せません。改善代行（お見積もり）または上記の手順をご利用ください。

※ 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:https (443/tcp)、http (80/tcp)、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 10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。

この健診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代行、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