セキュリティ監査レポート

株式会社****

ターゲット: www.****.co.jp

開始日: 2025-02-26 **終了日:** 2025-03-12

総評

1 診断評価:

危険 （重大なセキュリティ問題が検出された）

2 コメント

非常に古いバージョンの Apache (2.2.15) と OpenSSH (5.3) が稼働しており、多数の深刻な脆弱性が存在します。
これらは悪用される可能性が非常に高く、緊急のアップデートが必要です。
SSLv3 が有効になっていることも重大な問題であり、POODLE 攻撃に対して脆弱です。
また、Slowloris 攻撃にも脆弱であり、サービス停止を引き起こされる可能性があります。
oa-system (OpenSSH 5.3 が8022ポートで稼働している) の詳細が不明なため、SSH の設定の確認と適切なアクセス制限が必要です。SSH が不要であれば、サービスを停止するべきです。
WordPress も古いバージョンであるため、アップデートが必要です。
HTTP アクセスが可能であり、HTTPS へのリダイレクトが適切に設定されていない可能性もあります。
全体的にセキュリティリスクが非常に高く、早急な対応が必要です。

3 各診断結果一覧

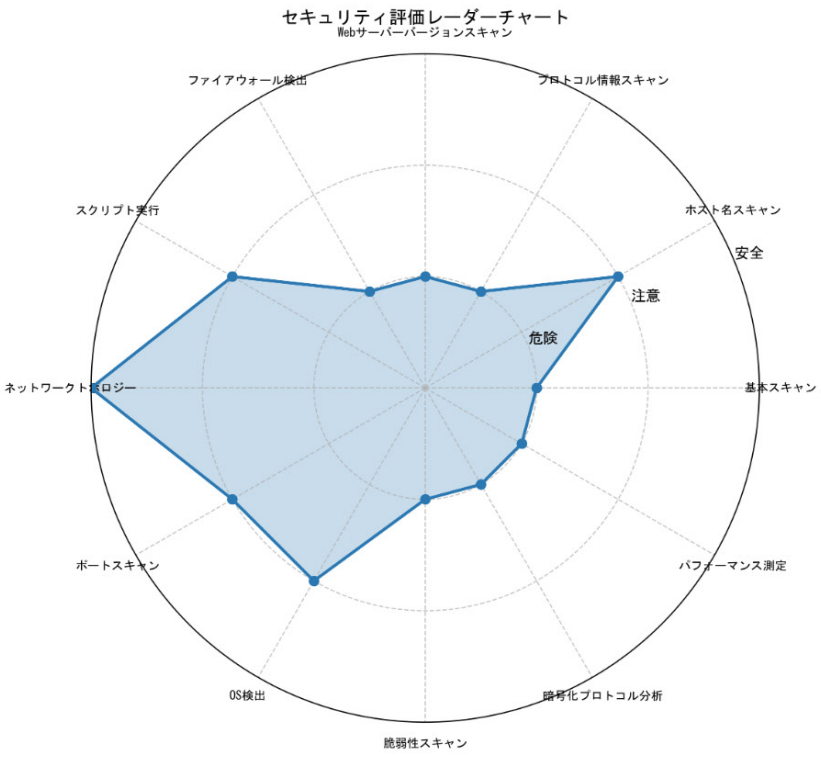
診断方法	診断評価
基本スキャン	△
ホスト名スキャン	△
プロトコル情報スキャン	×
Webサーバーバージョンスキャン	×
ファイアウォール検出	×
スクリプト実行	△
ネットワークトポロジー	○
ポートスキャン	△
OS検出	△
脆弱性スキャン	×
暗号化プロトコル分析	×
パフォーマンス測定	×

4 推奨する対応案

診断方法	対応策	優先度
Apache、OpenSSH	最新バージョンへアップデート	高
SSLv3	無効化	高
Slowloris 攻撃	WAF の導入、接続タイムアウトの短縮、同時接続数の制限	高
oa-system (OpenSSH 5.3)	SSH 設定の確認、アクセス制限の実施、不要であればサービスの停止	高
WordPress	最新バージョンへアップデート	中
HTTPS	HTTP アクセスを HTTPS へリダイレクトするよう設定	中
ディレクトリリスティング	無効化	中
OS	最新バージョンまたは LTS バージョンへアップデート	中
安全でない暗号化方式	RC4、3DES、IDEA、MD5 を無効化し、安全な暗号スイートのみ利用	高

```

## 5 レーダーチャート


```

基本スキャン - AI診断結果

1 診断評価:

要改善 （軽微から中程度のセキュリティ問題が検出された）

オープンなポート80、443に加え、8022番ポートでoa-systemが稼働していることが確認されました。HTTP/HTTPSは標準的なWebサービスのポートですが、oa-systemの公開は潜在的なセキュリティリスクとなります。oa-systemの種類やバージョンが不明なため、脆弱性の存在を確認する必要があります。また、不必要なポートの公開は攻撃対象領域を広げるため、適切なアクセス制限が必要です。

2 検出されたサービスとポートの概要

ポート番号	サービス名	状態
80	http	open
443	https	open
8022	oa-system	open

3 セキュリティ上の懸念点

OAシステムの公開：リスクレベル：中

8022番ポートでOAシステムが稼働しており、外部に公開されています。OAシステムは機密情報を扱うことが多く、脆弱性を突かれた場合、情報漏洩やシステム乗っ取りなどの深刻な被害につながる可能性があります。特に、製品名とバージョンが不明なため、既知の脆弱性の有無を確認することができません。

不必要なポートの公開：リスクレベル：低

必要のないポートが外部に公開されている場合、攻撃対象領域を広げ、セキュリティリスクを高めます。今回のスキャンでは、HTTP/HTTPS以外のサービスが公開されているため、本当に必要なポートのみを公開する必要があります。

4 推奨される対策

OAシステムのアクセス制限：優先度：中

OAシステムへのアクセスを特定のIPアドレス範囲に制限するか、VPN接続を必須とすることで、外部からの不正アクセスを防ぐことができます。また、OAシステムの製品とバージョンを特定し、セキュリティパッチを適用することで既知の脆弱性を解消してください。もし不要であれば、OAシステムをインターネットから隔離することを検討してください。

不要なポートの閉鎖：優先度：高

ファイアウォール設定を見直し、使用していないポートを閉鎖してください。これにより、攻撃対象領域を縮小し、セキュリティリスクを軽減できます。特に、8022番ポートはOAシステム以外で使用されていない場合、速やかに閉鎖する必要があります。

5 追加の注意事項

今回のスキャンはポートスキャンのみであり、アプリケーションレベルの脆弱性やシステム内部の設定に関する情報は取得できていません。より詳細なセキュリティ評価を実施するためには、脆弱性診断やペネトレーションテストなどを検討する必要があります。また、OAシステムの具体的な製品情報が不明なため、ベンダーに問い合わせてセキュリティ対策に関する情報を収集することも重要です。

ホスト名スキャン - AI診断結果

1 診断評価:

要改善 (caution)

ホスト名が公開されているため、サービスの種類や利用状況に関する情報が外部に漏洩する可能性があります。これは、攻撃者が標的を絞りやすくする情報となり、セキュリティリスクを高める可能性があります。深刻な脆弱性は検出されていませんが、情報漏洩のリスクを低減するために、更なる対策が必要です。

2 検出されたホスト名の概要

IPアドレス	ホスト名	状態
**********	****.sakura.ne.jp	up

3 セキュリティ上の懸念点

ホスト名による情報漏洩：リスクレベル：中

ホスト名"ik1-332-26489.vs.sakura.ne.jp"から、さくらインターネットの仮想サーバーであることが推測できます。この情報は、攻撃者にとってサービスの種類やシステム構成を推測する手がかりとなり、攻撃対象を絞り込むのに利用される可能性があります。例えば、さくらインターネットの特定サービスに既知の脆弱性が存在する場合、攻撃者はこのホスト名を手がかりに攻撃を試みるかもしれません。

4 推奨される対策

逆引きDNSレコードの変更/削除：優先度：中

ホスト名からサービス情報が漏洩するのを防ぐため、逆引きDNSレコードを必要最低限の情報に変更、もしくは削除することを推奨します。もし特定のサービスを提供するためにホスト名が必要な場合は、サービス名や機能が推測しにくい汎用的な名前に変更してください。例：server01.example.com

ファイアウォール設定の確認：優先度：高

公開が必要なサービスポートのみを許可し、不要なポートはファイアウォールで遮断してください。これにより、外部からの不正アクセスを最小限に抑えることができます。特に、使用していないサービスのポートは閉じることが重要です。

脆弱性スキャンの実施：優先度：中

定期的に脆弱性スキャンを実施し、システムのセキュリティ状態を把握することで、潜在的な脆弱性を早期に発見し、

脆弱性スキャンの実施：優先度：中
定期的に脆弱性スキャンを実施し、システムのセキュリティ状態を把握することで、潜在的な脆弱性を早期に発見し、対策を講じることができます。Nessus、OpenVAS、QualysGuardなどのツールを利用できます。

5 追加の注意事項

今回のスキャンはホスト名と状態のみを対象としており、システム全体のセキュリティ状態を網羅的に評価するものではありません。より詳細なセキュリティ評価を行うためには、ポートスキャン、脆弱性診断、侵入テストなどを実施する必要があります。また、検出されたホスト名に対する適切なアクセス制御の設定も重要です。この結果を元に、必要に応じて更なる調査と対策を実施してください。

プロトコル情報スキャン - AI診断結果

1 診断評価:

危険 （重大なセキュリティリスクあり）

Apache httpd 2.2.15 および OpenSSH 5.3 は非常に古いバージョンであり、既知の脆弱性が多数存在します。これらの脆弱性は悪用される可能性が高く、システムへの不正アクセスやデータ漏洩につながる重大なリスクがあります。

2 検出されたプロトコル情報の概要

ポート番号	プロトコル	サービス名	バージョン
80	tcp	http	Apache httpd 2.2.15
443	tcp	http	Apache httpd 2.2.15
8022	tcp	ssh	OpenSSH 5.3

3 セキュリティ上の懸念点

古いApache httpdの使用：リスクレベル：高
Apache httpd 2.2.15はサポートが終了しており、多くの既知の脆弱性が修正されていません。これにより、システムが攻撃に対して脆弱になります。

古いOpenSSHの使用：リスクレベル：高
OpenSSH 5.3も同様にサポートが終了しており、既知の脆弱性が存在します。SSHはシステムへのリモートアクセスを提供するため、脆弱なバージョンを使用すると、攻撃者がシステムを制御できる可能性があります。

4 推奨される対策