

商工会議所・商工会の会員様へ

# あなたのホームページ 脆弱性が狙われています。



ハッカーがあなたの財産を常に狙っています！

現在は高度な専門知識がなくてもハッカーになれてしまうのです。

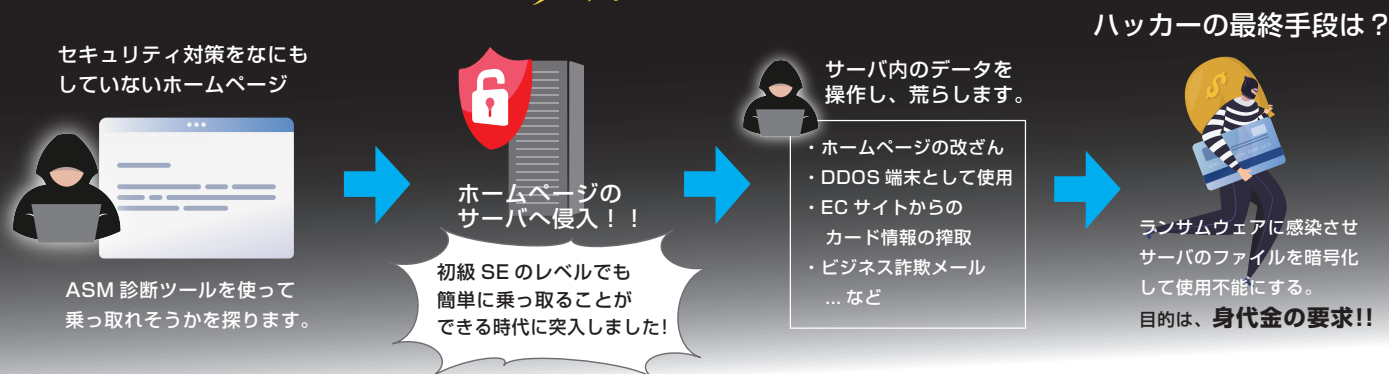
例えば乗っ取りの手法は AI チャットサービスなどで得られます。

では、その”見えない脅威”にどうやって対処したらよいのでしょうか。

まずは**無料**で

ホームページの **URL ドメイン脆弱性** を調べましょう！

## ハッカーの手口



世界標準の最新  
脆弱性診断ツール

## イージス EW (AEGIS-EW)

イージス EW は危険な個所を即座に発見し、診断結果を色（円グラフ）で視覚化します！



非常に深刻度が高いと判断された例  
(赤・オレンジ色は深刻脆弱性を示す)



サーバ（システム）を改善対策  
したことで脆弱性を軽減された！

脆弱性が発見された場合には、その深刻度に応じて対策を施す必要があります。

## 今すぐ無料診断を！

お申し込み方法は  
裏面をご覧ください

# 脆弱性診断ツール イージスEW (AEGIS-EW)

**AEGIS** EARLY WARNING SYSTEM

## 見やすい GUI

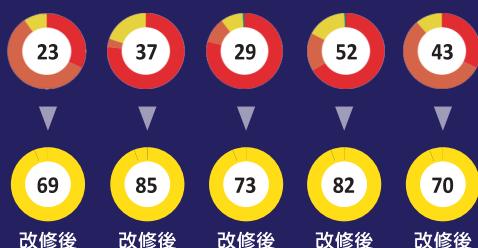
深刻度の割合が  
円グラフによって  
一目で認識できる



## 分析しやすい 分類分野

グラフは  
色で判断可能で、  
専門知識は不要です

イージス EW お客様の約 **95%**が  
赤・オレンジの脆弱性項目が発生していました



改修後の目標  
総合評価 (レーティング) は  
100 点満点制で  
**60 点以上**を  
達成しました！

世界標準 CVSSv3 の深刻度仕様・色の定義は？

深刻度	CVSS v3基本値
緊急 (Critical)	9.0~10.0
重要 (High)	7.0~8.9
警告 (Middle)	4.0~6.9
注意 (Low)	0.1~3.9
なし (None)	0

CVSS v3 基本値

**赤 = 緊急**  
**SE 1 年目**で乗っ取れるレベル !!

**オレンジ = 重要**  
**SE 2~3 年目**で乗っ取れるレベル !!

**要改修です!!**

米国 NIST、NCSC (英国)、NATO 先進国等の評価基準です。  
赤とオレンジの改修が義務づけられています。

## 無料版の脆弱性診断 (ASM) 実施後のメンテナンス作業手順

イージス EW 有料版での  
全診断結果の取得

web 開発業者も含めた  
診断結果の対策セミナー  
(希望者オプション)

リモートでの対策実施支援 (希望者オプション)  
※弊社エンジニアが実際に改修致します。

## 広範囲に渡る脆弱性診断分野

イージス EW の詳しい技術情報はこちら ▶ <https://mirai-cybersecurity.jp/>

### Cloud

#### クラウドサーバ診断

Amazon AWS 上のセキュリティポリシーを診断します。VPC (Virtual Private Cloud) のデフォルトセキュリティグループが不要な通信を制限しているかを確認します。その他、Amazon S3 におけるパブリックアクセスのブロック設定も調査します。また、セキュリティイベントに対するアラーム設定やルートアカウントへの MFA (Multi-Factor Authentication) の有効化について確認することも可能です。

### MAIL

#### 送信ドメイン認証

「受信したメールが正規の送信元から送られてきたものかどうか」を確認できる仕組み。メール送信が行われるサーバ (SMTP) に対して、「IP アドレス認証」や「電子署名」を用いて、「メールのなりすまし」が行われているかどうかを判断します。(SPF, DKIM, DMARC チェックもサポート)

### BREACH

#### データ侵害

攻撃者が、Web サービス等に攻撃を仕掛けて得た個人情報をダークウェブ等に拡散する行為のこと。特にメール情報の漏洩から発生が多く、メールアドレスを基にした診断を実施します。

### WEBCERT

#### Web 認証関連

WEB サーバ証明書に関する認証プロトコル全般の脆弱性チェックを診断します。例えば、TLS、SSL のバージョン情報、等。

### HEADER

#### HTTP ヘッダー関連

WEB アプリケーションとの HTTP プロトコルをセキュアにするための各種ヘッダーのサポート状況を確認します。これにより、サポート OS の正しいチェックモジュールが搭載されているか、攻撃防御を実施するための設定が成されているか、等をチェックします。

### PORT

#### ポートスキャン攻撃

ポートスキャンからの外部侵入に対する脆弱性の診断を行います。必要最低限のポートのみを使用し、不要なポートは常に締めおく対策が求められます。

### CVE

#### 共通脆弱性識別子

個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体の MITRE 社が採番している識別子です。脆弱性検査ツールや脆弱性対策情報提供サービスの多くが CVE を利用しています。

## ペネトレーションテストだけでは、“砂上の城”と同じです！ASMは必須です！



建物 (システム環境) は無防備。  
何も対策をしていないため  
ハッカー攻撃に遭う危険な状態！



建物は改築 (ペネトレーションテスト) を  
実施して立派な「お城」に変わったが  
砂の地面 (インターネット環境) が  
不安定なため、まだまだ危険な状態！



地面を強固 (ASM を実施) にしたので  
完全なハードニング基礎が完成して  
**これで完全防備となった!!**

### ASM (Attach Surface Management) とは？

インターネット上の野良端末 (忘れてたバックアップサーバ等) を検知したり、ネットに漏洩した情報をサーチします。また、各端末のプラットフォーム設定情報を取得し、脆弱性を診断します。技術的にはバシブスキャンと呼ばれます。

### ペネトレーションテストとは？

IP アドレスを有し実存する端末からのプラットフォーム設定情報を元に、データ書き込み等も実施することで、ASM よりより深い診断を実施します。技術的にはアクティブスキャンと呼ばれます。

## 脆弱性診断【無料】お申し込み先

<https://future-research.jp/aegis-demo/>

上記ページに必要事項を記入してお申し込みください

※ 尚、診断結果は“個人情報の取り扱い規約”に準じ機密扱いとなります。

**未来研究所** 販売元: (株) 未来研究所

Future Research Inc.



販売代理店はこちら