

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！

23 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)



69 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)



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 (レイトング) 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

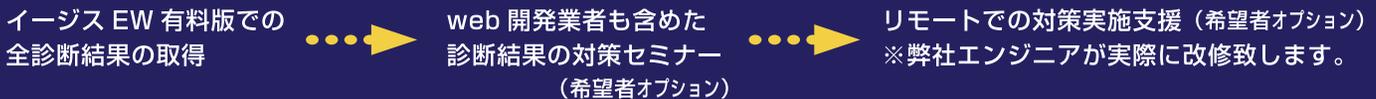
CVSS v3 基本値

- 赤 = 緊急
SE1 年目で乗っ取れるレベル!!
- オレンジ = 重要
SE2~3 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



広範囲に渡る脆弱性診断分野

イージスEWの診断結果は、各発生分野ごとに分類されているため、改修作業の効率を大幅に向上させることが可能です。

CVE
共通脆弱性識別子

Cloud
Cloudプラットフォーム診断

MAIL
送信ドメイン認証

BREACH
データ侵害

WEBCERT
Web認証関連

HEADER
HTTPヘッダー関連

PORT
ポートスキャン攻撃

野良端末検出機能
サブドメイン検出

脆弱性診断分野の詳細な技術情報はこちらのQRコードから



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!



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。技術的にはパッ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