



ドメイン診断【無料】  
ASM 脆弱性診断 お申し込みフォーム  
<https://future-research.jp/aegis-demo/>



イージス EW デモ【無料】  
各種お問い合わせフォーム  
<https://future-research.jp/contact/>



イージス EW ウェブサイト  
<https://mirai-cybersecurity.jp>



# AEGIS EARLY WARNING SYSTEM

総合サイバーセキュリティ脆弱性診断ツール イージス EW

ハッカーは、ホームページの  
ASM 脆弱性診断で、  
攻撃先を選定します!!

2025 年 5 月 1 日 発行

# イーゲスEW (AEGIS-EW)は、専門知識不要で運用できる総合サイバーセキュリティ脆弱性診断ツールです。

## ASM (Attack Surface Management) 対策にはパッシブスキャンが必須です。

イーゲス EW (AEGIS-EW) は、エンドユーザが所有するドメインに含まれるネットワーク機器（サーバ含む）に対し、ASM (Attack Surface Management) を実施するパッシブスキャンとペネトレーションテストを実施するアクティブスキャンをラインナップした脆弱性診断ツールです。エンドユーザは悪意ある攻撃が行われる前に、ネットワーク機器に含まれる脆弱性リスクを知ることができます。エンドユーザは、これらの総合的な脆弱性診断を「専門知識不要で運用できる」点が大きな特徴です。

現在お使いの「ドメイン名だけ」で、ドメインに紐づく情報（ホームページ、メールサーバ、公開済みサービス等）の総合的な脆弱性診断が可能です。なお、「公開済み IP アドレス」や「サブドメイン等」については、イーゲス EW が自動で検索を行います。

グラフや色分けによるグラフィカルで分かりやすい結果表示により、システム納入時の「ハードニング(脆弱性対策を施すこと)」実施済証明を作成する際に、大きな説得力をプラスすることができます。



- ・この図は、システム改修の対策を実施した結果。赤のクリティカル表記が解消され、総合評価点が51から69に改善した例です。
- ・グラフ内に、赤 (CVSS Critical)、オレンジ (CVSS High) があると、サイバー先進国 (米国、英国、オセアニア等) の公共系システムでは、システム受け入れの許可が下りません。

## ペネトレーションテスト (アクティブスキャン) だけでは不十分！パッシブスキャンも実施していますか？

一般的に脆弱性診断にはパッシブスキャン (ASM ツール) と、アクティブスキャン (ペネトレーションテスト) の2種類があります。パッシブスキャンを用いることにより、ゾンビ端末/ 野良IoT に起因する「野良IP・野良サブドメイン」を検知します。これにより、アクティブスキャン (ペネトレーションテスト) 実施時の診断漏れを防ぐことが可能です。

### パッシブスキャン (ASM ツール)



### アクティブスキャン (ペネトレーションテスト)



## 広範囲に渡る脆弱性診断分野

イーゲス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。

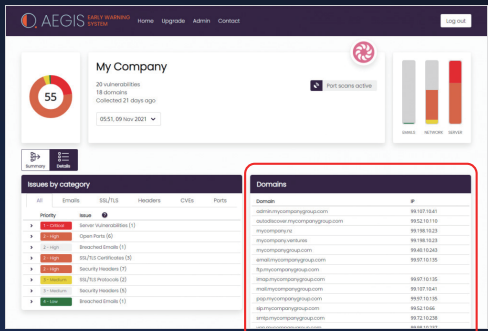
<b>CVE</b> 共通脆弱性識別子	<b>Cloud</b> (ペネトレーションテストのみ) Cloudプラットフォーム診断	<b>MAIL</b> 送信ドメイン認証	<b>BREACH</b> データ侵害(情報漏洩)
<b>WEBCERT</b> Web認証関連	<b>HEADER</b> HTTPヘッダー関連	<b>PORT</b> ポートスキャン攻撃	<b>野良端末検出機能</b> サブドメイン検出



# サブドメイン自動検出機能

Nessus にも、OpenVAS にも無いオリジナル機能！

メインドメインだけでなく、サブドメインも自動検出して脆弱性診断。  
イージス EW の最大の特徴です！  
英国が提供している NICT・NICTER 類似サービスを使用。



サブドメインも自動検出！

脆弱性診断対象として  
データベース化

POINT!  
必要な情報は、  
「メインドメイン名」  
だけで OK！

# グラフィカルで見やすい総合評価点

ドメイン環境の脆弱性リスクをグラフ化！  
診断結果の総合評価点を、(100点満点中 XX点) で表示します。

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

POINT!  
専門知識は不要。  
色分けで理解できる！



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？

この表は、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。

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

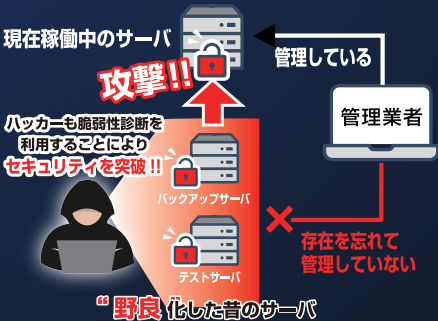
## CVSS v3 基本値

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

# 忘れられ、放置されたサーバを検知

パッシブスキャンにより「野良 IoT」の存在を検出します！

「野良 IoT」とは、忘れられ、放置されたネット上に存在する端末の総称です。  
過去に Amazon、PayPal などのメジャーなサービスもこの原因で被害に遭いました。



調査対象のドメイン名をベースに野良  
サブドメインと IP の組み合わせを調  
査します。対象項目は、HomePage  
の表記、メールサーバ、ファイルサー  
バ、SNS 系のサービスサーバ、  
DataBase サーバなどです。

POINT!  
イージス EW の  
無料診断ですぐに  
チェックが可能です！

# ペンテストにより、システムを深く検証

納品前のシステムのハードニング (堅固さ) を証明します！

アクティブスキャン (ペネトレーションテスト) を実施し、該当端末に脆弱性  
の攻撃パターンを掛けて、侵入を試みるアクションを実施します。

Cybersecurity Risk Rating (サイバーセキュリティ・リスク評価) は、  
マネージメント評価も含まれるケースが多いとされています。  
イージス EW は、技術的な要素に絞った診断機能となっています。

※弊社では、サイバーセキュリティ・マネージメント評価は IPA 等、多くの機関から各種  
ガイドラインが既にリリースされており、評価ツールも多数あるため、こちらを使用を推  
奨しております。

# 明瞭かつ低価格な導入コスト

調査対象のドメインに含まれる「メインドメイン」を  
「サブドメイン」の合計から価格が決定されます。

## イージス EW 販売価格



脆弱性診断 (有料版)、診断結果セミナーは  
全てオープン価格となります。  
ご質問、ご相談は弊社ホームページの  
問い合わせフォームからお願いいたします。

お問い合わせフォーム  
表示 QR コード



# イージスEW 導入～システム改修までのフロー

## ドメイン所有者

### ドメイン脆弱性を調査したい

自社HPなど重要なドメインで、無料ASM(脆弱性診断)を依頼。

### ASM 診断結果の検証

診断結果を受けて脆弱性の解消と、システム納入時の「ハードニング実施済証明」の提出に備えることが重要と判断。

### ASM【有料版】の実施を決定

深刻度レベル【赤】【オレンジ】の診断結果の仔細を知りたい。  
また、定期的にASMを実施したい。

### ASM・レコナイ診断結果の改修

自社での改修を実施。工数不足で対応ができない場合、弊社(未来研究所)の『**伴走サービス**』依頼を検討。

### 更に深く脆弱性を診断する

ペネトレーションテスト【有料版】定期的実施を決定

- ・各脆弱性の攻略パターンを用いて診断したい。
- ・各脆弱性の改修をイージスEWの改修方法を参考にハードニングを実施したい。
- ・工数不足で対応ができない場合『**伴走サービス**』にて改修（ハードニング）依頼を検討。

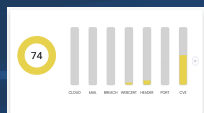
### 改修（ハードニング）実施を決定

自社工数では対応が難しいとの結論に至り、  
『**伴走サービス**』の依頼を決定。

### 改修作業・定期診断の状況確認



改修前



改修後

赤・オレンジの項目が無くなり、対策による成果が現れました！

特に深刻な脆弱性を示す「赤・オレンジ」の項目が消えることを達成目標とします。

定期診断によって新たな問題が発覚した場合は、速やかに対処できるよう、弊社とのヒアリング体制を整えておきます。

## 未来研究所 イージス EW 脆弱性診断

### ASM【無料版】を実施

総サブドメイン数の開示

総脆弱性件数の開示

CVSS・各分野の開示



### 診断結果

深刻度レベル

【赤】 SE1年目で乗っ取り可能！

【オレンジ】 SE2～3年目で乗っ取り可能！

無料版では、脆弱性の仔細の一部は表記されません。

### ASM【有料版】を実施

全脆弱性診断の仔細情報開示

弊社による主な診断結果の改修方法レポート

自動診断レポート生成

ダッシュボード使用アカウントを発行



ASMで検出できるCVSS緊急・重要な項目番号が分かれば、ハッカーも簡単に乗っ取ることができます！

### ペネトレーションテスト【有料版】を実施

テスト結果の詳細を開示

レポート内容の説明

## 未来研究所『伴走サービス』

### 改修（ハードニング）方法についてのヒアリング

お客様と一緒に、脆弱性の改修・改善を勧める『伴走サービス』についてのご説明、改修方針、手段等のヒアリングを実施。



### 『伴走サービス』工程プランを作成

ASM診断とペネトレーションテストから得られた結果から「作業優先順位表」を作成いたします。

### 改修（ハードニング）作業の実施

脆弱度が高いところから対策を打っていきます。

ASM脆弱性 改修作業

ペネトレ脆弱性 改修作業

### 脆弱性の定期診断（ASM・ペネトレーション）

イージスEWを使用した定期診断を実施します。



改修後の効果測定を、診断オーダー内容(毎日/毎週/毎月)に合わせて実施し、報告書を提出いたします。

お問い合わせはこちらへ



未来研究所

国内総販売代理店

Future Research Co., Ltd.

株式会社未来研究所

〒259-1126 神奈川県伊勢原市沼目 5-6-2

TEL : 0463-96-2196

E-mail : info@future-research.jp

URL : https://future-research.jp



024-0037-20



弊社のサイバーセキュリティ脆弱性診断は経済産業省策定の情報セキュリティサービス基準適合サービスに認定されております。