



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 ASM・脆弱性診断ツール イージス EW

2025 年 8 月 発行

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!!

イージス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 ASM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。

イージス 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、パッシブスキャンを実施する ASM (Attack Surface Management) とアクティブスキャンを実施する脆弱性診断をラインナップしたプラットフォーム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、イージス 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、システム納入時に提出しなくてはならない脆弱性の改修証明書を作成する際に、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。赤のクリティカル脆弱性が解消され、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、オセアニア主要国、等）の公共系システムでは、システム受け入れが許可されません。

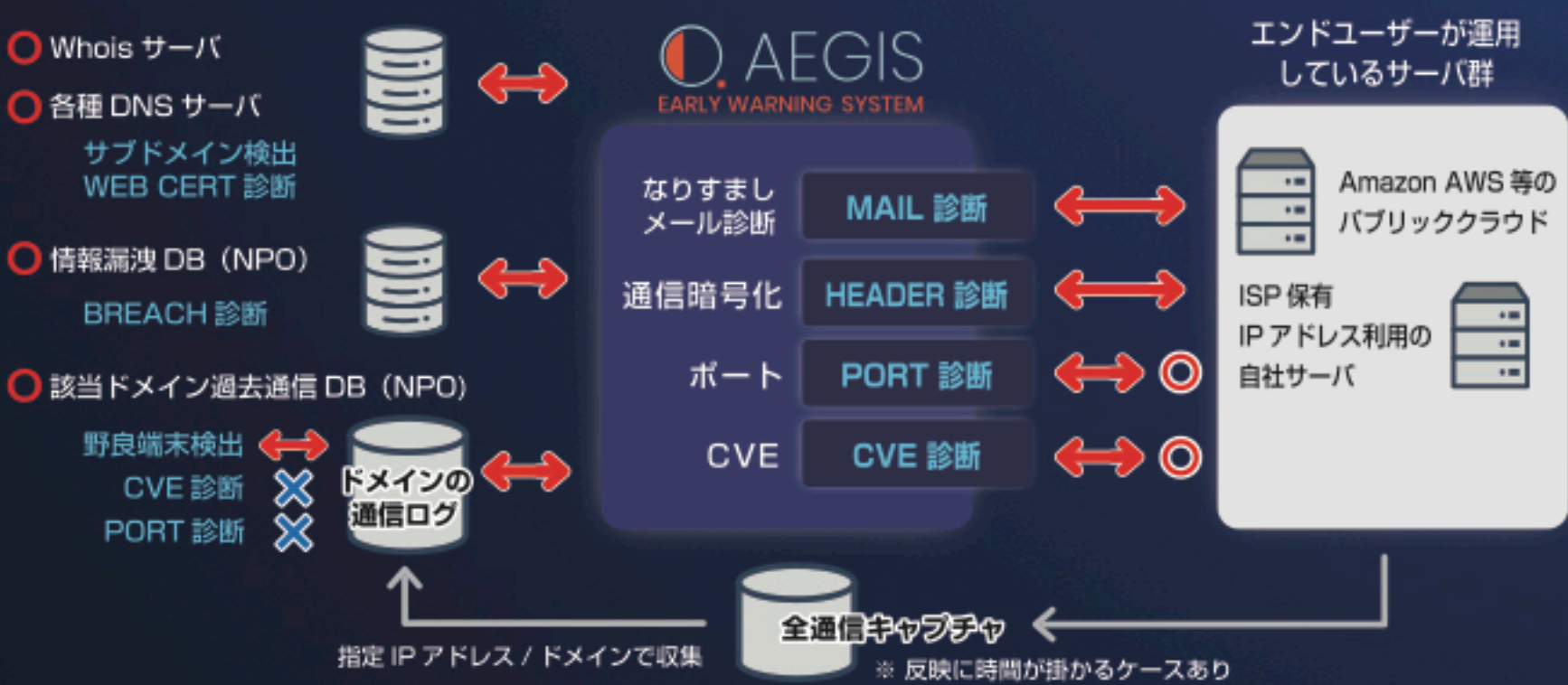
脆弱性診断 (アクティブスキャン) だけでは不十分！ASM (パッシブスキャン) 診断も実施していますか？

一般的に脆弱性診断にはパッシブスキャン (ASM) と、アクティブスキャン (脆弱性診断) 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)



アクティブスキャン (脆弱性診断)



広範囲に渡る脆弱性診断分野

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

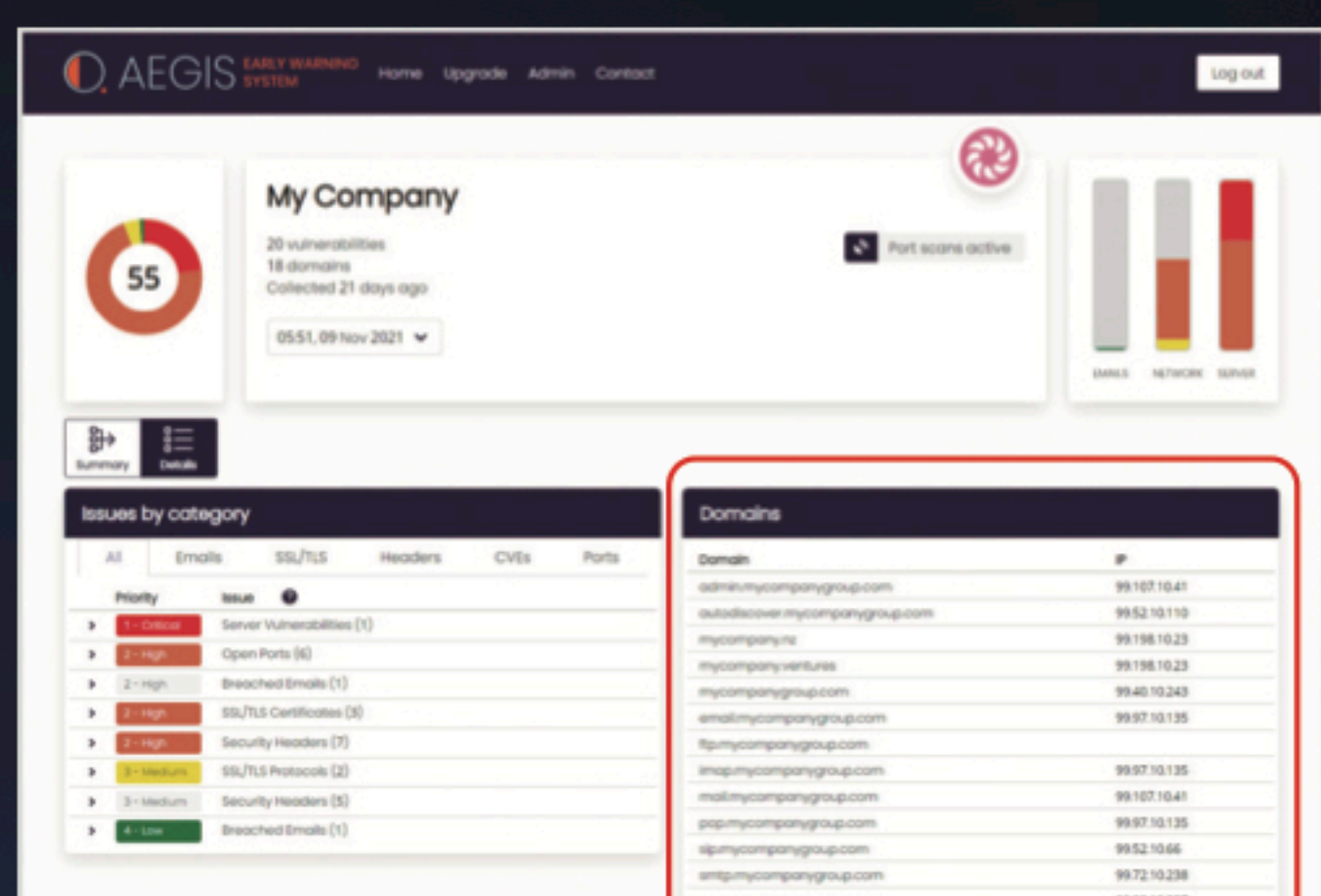
CVE 共通脆弱性識別子	Cloud (脆弱性診断のみ) Cloudプラットフォーム診断	MAIL 送信ドメイン認証	BREACH データ侵害(情報漏洩)
WEBCERT Web認証関連	HEADER HTTPヘッダー関連	PORT ポートスキャン攻撃	野良端末検出機能 サブドメイン検出



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！
英国が開発運用しているサービス（日本の NICTER と類似）。



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！

忘れられ、放置されたサーバを検知

ASM 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。



診断対象のドメイン名を基に、DNS サーバや Whois 情報に加え、過去の通信ログも活用して情報を収集します。

これにより、管理されず放置されている可能性のあるサブドメインや IP アドレスを検出します。

調査対象には、各種サーバ（ホームページ、メール、ファイル、データベース等）だけでなく、該当ドメインを利用する IoT 機器など、プラットフォームに関わるすべての端末が含まれます。

POINT!

イージス EW の
無料診断ですぐに
チェックが可能です！

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！



赤・オレンジの脆弱性を改修後
総合評価(レーティング)は
100点満点中

60点以上を達成しました！

世界基準の CVSSv3.1 の深刻度仕様・色の定義は？

CVSS は、米国 NIST、NCSC（英国）、NATO 主要国等の評価基準です。
サイバー先進国や特定社会基盤事業者には赤とオレンジの改修が義務づけられています。

深刻度	CVSSv3.1 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

CVSSv3.1 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!!

診断・ハードニングの全工程

ASM ▶ 脆弱性診断 ▶ ペネトレーションテスト

ASM スキャン技術：パッシブスキャン

レコナイ（偵察）ツールも用い、野良端末・情報漏洩・メールなりすまし等は
実サーバで診断し、他（CVE、PORT）は、過去データベースを基に診断します。
このため実システム群への影響はないので、何時でも診断が可能です。

脆弱性診断 スキャン技術：アクティブスキャン

実際のシステムに対しパケット書き込みを行い CVE・PORT の診断を実施します。
診断の確度が上がりますが、システムへの負荷も大きくなるため診断タイミングは
該当システムの稼働に影響しない、夜・土日等での診断実施をお勧めします。

ペネトレーションテスト 人手によるアクティブスキャン

ASM および脆弱性診断の結果を基に、より深い侵入試験を実施します。

明瞭かつ低価格な導入コスト

イージス EW 販売価格



QR コードはこちら

脆弱性診断（有料版）、診断結果セミナー等は
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
お問い合わせフォームからお願いいたします。
<https://future-research.jp/contact/>

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など診断を検討しているドメインで、無料ASMを依頼。

ASM 診断結果の検証

診断結果を受けて、脆弱性の改修と、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】の診断結果の詳細を知りたい。
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

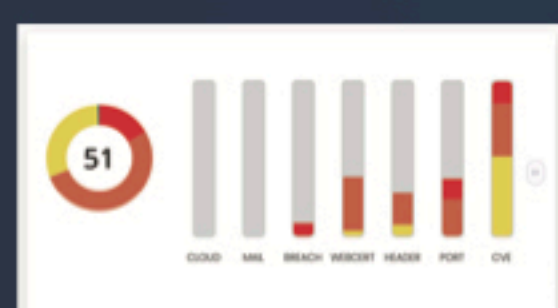
脆弱性診断【有料版】 定期的実施を決定

- ・各脆弱性の攻略パターンを用いて診断したい。
- ・各脆弱性をイージスEWの改修方法を参考に改修を実施したい。
- ・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。

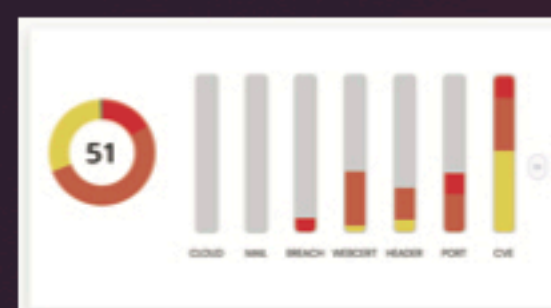
未来研究所 イージスEW 脆弱性診断

ASM【無料版】を実施

総サブドメイン数の検出

総脆弱性件数の検出

分野別 CVSS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、脆弱性の詳細は表示されません。

ASM【有料版】を実施

診断レポート自動生成

ダッシュボード使用アカウントを発行

診断結果の詳細表示

弊社による診断結果と主な脆弱性の改修方法レポート



ASMで検出できるCVSS緊急・重要な脆弱性が存在すると
ハッカーも簡単に乗っ取ることができます!

脆弱性診断【有料版】を実施

診断結果の詳細を表示

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・改善を進める『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診断と脆弱性診断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

深刻度が高いところから対策を実施していきます。

ASM診断結果の改修作業

脆弱性診断結果の改修作業

ASM 定期診断・脆弱性定期診断

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.

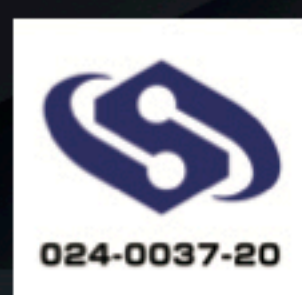
株式会社未来研究所

〒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



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。