経済産業省
ASM
Attack Surface Management
導入ガイダンス対応

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

AEGIS-EW（イージス 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。

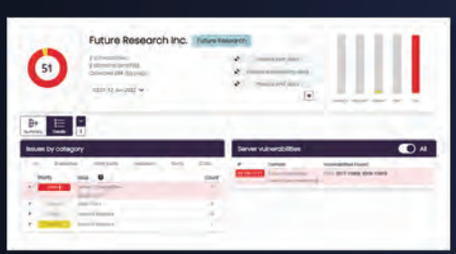
ASM（Attack Surface Management）対策にはパッシブスキャンが必須です。

AEGIS-EW（イージス 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、「AIGES-EW(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。

対策前



対策実施

対策後

・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

BREACH
データ侵害

利用中の他社クラウドサービスで「アカウント乗っ取り」が発生した結果、社内重要情報に攻撃者がアクセス可能となります。メールアドレスをキーとした流出が多いため、「AIGES-EW（イージス EW）」は、これを基軸にした診断を実施します。

WEBCERT
Web 認証関連

Web サーバ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、Web サーバ証明書（有効性等）チェック、暗号化プロトコル（Version 含む）のチェック等がこれに該当します。

HEADER
HTTP ヘッダー関連

Web クライアントと Web サーバ間でやり取りされる「HTTP ヘッダネゴシエーション」に含まれる脆弱性について診断します。CSP(Content Security Policy)、HSTS(HTTP Strict-Transport-Security)、XFO (X-Frame-Options) 等の HTTP ヘッダセキュリティオプション群に対してのサポート状況も診断します。

PORT
ポートスキャン攻撃

調査対象のサーバで展開されているサービスポートに対して、ポートスキャンを実施して脆弱性を診断します。パッシブスキャンでは、調査対象のサーバに対して「通常アクセス」を試み、通信結果からサービスに含まれる脆弱性を診断します。Acvite Scan では、ブラックハッカーが用いる攻撃を試み、サービスに含まれる脆弱性を診断します。

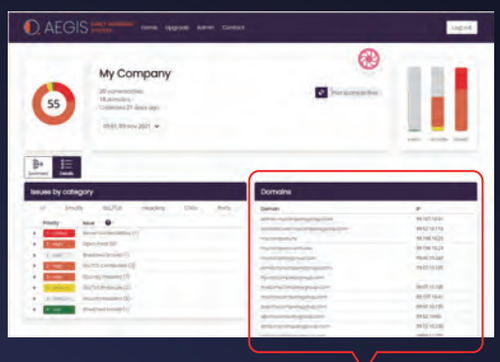
CVE
Common Vulnerabilities and Exposures

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。

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。
AEGIS-EW（イージス EW）の最大の特徴です！



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。

AEGIS-EW（イージス EW）は、サーバ脆弱性診断に詳しくないエンドユーザでも見やすく、わかり易いものとなっています。
総合評価点は一般的な脆弱性診断に用いられるリソース群だけでなく、開発元である Titanium Defence Ltd. チームが保有する 30 年以上のサイバーセキュリティ・コンサルティングで得たチェック項目によって評価されます。

総合評価点のグラフ表記例

総合点が円グラフによって
分かりやすく示されます。

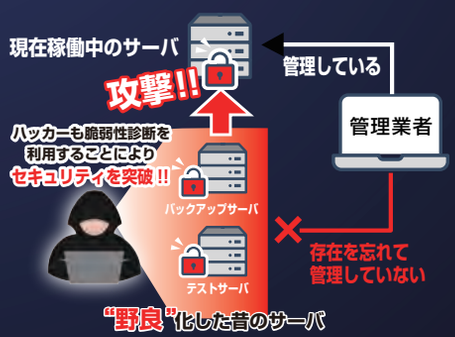
100 ～ 80 = 最小限のリスクで非常に安全度が高い
79 ～ 60 = 比較的安全度が高い … 部分的に「脆弱性リスク」あり
59 ～ 40 = 脆弱性リスクがある … 「重要度の高い脆弱性リスク」あり
39 ～ 20 = 安全度が低い … 「非常に重要度の高い脆弱性リスク」あり
19 ～ 0 = 深刻な状態にある … 「極端に危険な脆弱性リスク」あり

POINT!
専門知識は不要。色分けで理解できる！

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!
AEGIS-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。
AEGIES-EW（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。

診断名	プロフェッショナル	エキスパート
診断内容	パッシブスキャン脆弱性チェック	アクティブスキャン脆弱性チェック
スキャン方法	パッシブスキャン	アクティブスキャン
ドメイン数・価格（サブドメインを含む）	1～9 ¥93,500（85,000） 100～199 ¥130,240（118,400） 1000～2000 ¥176,000（160,000）	1～9 ¥165,000（150,000） 100～199 ¥275,000（250,000） 1000～2000 ¥357,500（325,000）
診断結果有料セミナー	AEGIS-EW をご購入いただいたお客様に向けた、診断結果の有料説明セミナー（約 2 時間）です。	¥165,000（150,000）

（ ）は税抜価格

上記価格は、推奨販売価格表から一部抜粋したものです。
各プランの詳細価格、セミナー診断結果セミナーの詳細はお問い合わせください。

AEGIS EARLY WARNING SYSTEM

あなたの組織のデジタル資産を守るために！
AEGIS-EW を体験いただくことができます。

ドメイン診断【無料】

御社で最も重要とされているドメイン名を一つお知らせください。
例）https://example.co.jp

無料キャンペーンの診断結果（サブドメインを含むドメイン数）を元にして、AEGIS-EW 有料版の正式なお見積もりを作成することができます。

※ なお、診断結果は「個人情報取り扱い規約」に基づき外部への開示等は一切おこないません。

個別デモ【無料】

AEGIS-EW 個別デモンストレーション【無料】を Web 会議ツール（zoom/Teams）にて承っております。

デモ内容は、ドメイン診断結果の実例をもとに、主に UI の簡単な説明・深刻度グラフの見方などを説明いたします。

AEGIS-EW の使いやすさや豊富な機能について知ることができます。この機会に是非お気軽にお申し込みください！

詳細・お申し込みはこちらから　https://future-research.jp/

AEGIS-EW 開発元　Titanium Defence Ltd. 社　について

AEGIS-EW は世界で既に採用実績のある「総合サイバーセキュリティ脆弱性診断ツール」です。システム提供会社である「Titanium Defence Ltd. 社（本社New Zealand Upper Hutt, CEO&CTO Anthony Grasso）」に所属する AEGIS-EW 開発・運用コアメンバーの多くは、米国政府機関、英国国家機関、オセアニア政府機関などにおいて脆弱性診断を実施した経験を持つプロフェッショナル集団により構成されています。

TITANIUM DEFENCE
Ultimate Cyber Security Protection

AEGIS EARLY WARNING SYSTEM

https://www.titanium-defence.com

お問い合わせはこちらへ

国内販売総代理店
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/

未来研究所
Future Research Co., Ltd.

2023 年 7 月 21日 発行