

～あなたのホームページ、狙われています！～

ホームページの危険性、調査します イージスEW『サイバーセキュリティ脆弱性診断』

2025年7月30日
株式会社 未来研究所



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。

■我々のビジョン

未来研究所は、あなたの「困りごと」を解決し、あなたがその先の未来へ進むためのサポーターでありたい

- 会社名 株式会社 未来研究所
- 所在地 神奈川県伊勢原市沼田5丁目 6 - 2
- 概要 設立2021年 1 月 資本金2500万円 TEL0463-96-2196 www.future-research.jp
- 代表 CEO：小林忍 CTO: Dick Willson
- 主要事業 ITサービス・人財育成・R&D
- 我々のミッション

IT技術者が不足するSME・中堅企業様への
IS（情報システム）代行サービスにて、
少しでも日本のITデバインド問題の改善に貢献する

**Managed Service Provider(MSP)として、
IT分野の『OMOTENASHI・おもてなし』を世界に！**



未来研究所： Managed Service Provider (MSP)
IT分野のおもてなしを世界に！

SOHO ← SME（中小企業） — 中堅企業 → 大企業

【MIRAIサービス】
情報システム代行サービス
(セキュアEdge-BOX・サブスク・
の販売)

サイバーセキュリティ分野
サイバー業務の支援サービス
(プラットフォーム脆弱性診断ツール・
イージスEWの販売)

MIRAIサービス（IT分野の支援サービス）

(MIRAIサポータの支援業務)

サポーターへの教育・認定

人財募集

ICT支援員

ギグワーカー/副業希望者

地域の提携SIer

サポート・サービスのシステム構築
(BOX制作、VPN、DCサービス等)

米国 CTO
Dick Willson



小林 忍 (こばやし しのぶ)

(株)未来研究所 代表取締役 兼 サイバーセキュリティ・コンサルタント

取締役社長 アライドテレシスアカデミー (株) (2016年1月～2019年12月)

非特定営利活動法人 医療福祉クラウド協会 監事、等

講師 早稲田大学NEO、神奈川大学 : リカレント教育コース IT分野でのDX新規事業・起業、サイバーセキュリティ「その時どうする?」、リモートワーク環境での脅威、日本版BSC (ビジネス・スコア・カード) での自走する会社の作り方、etc.

【三重県出身 愛媛大学卒業後、大手電機メーカー、外資企業、起業、会社譲渡を経、現職】

【代表的な事業化】

- * オセアニア政府群にて使用されている脆弱性診断・AEGIS-EWを、独占販売権にて日本市場に展開開始 (2023/4～)
 - * サイバーセキュリティ研修コース・設計・制作・講師実施。 大手・中堅企業でのCSIRT新設から運用迄のコンサルティング
 - * サイバーセキュリティ分野でISACA CSX (クラウド上でインシデント・シナリオ対応を実践学習できるeラーニング) を世界で初めて代理店契約を締結し日本で販売中
 - * Extreme (L3 S/W) 社の世界で4番目のOEMを締結し、アライドテレシスのS/W事業の基礎を構築
 - * 日本で初めてNetscapeを販売
- 等があり、主に海外商材・ソリューションの日本事業展開において多くの実績を有します

【現職】

IT分野と教育の融合事業を主軸とし、サイバーセキュリティ分野でのCSIRTメンバーに向けた教育事業、およびコンサルティングを実施。
各種、団体および警察庁・大学等にてサイバーセキュリティ人材育成のセミナーを実施

【履歴概要】

愛媛大学 工学部卒

* (株)未来研究所 代表取締役社長 某上場会社でのセキュリティコンサルタント (ISMS,CSMS)、脆弱性診断からの事業支援の事業化

2023年7月～ 脆弱性診断ツール・イージスEWを独占にて日本市場に展開。現在、特定社会基盤事業者に向けた脆弱性診断を実施中

2021年1月～ 大手製造業、通信会社、派遣会社等に対し、インシデント発生から、社内でのサイバーセキュリティ業務の立ち上げ・運用迄を、支援中

* 2016 - 2019/12月 アライドテレシスアカデミー (株) 代表取締役 (サイバーセキュリティ教育事業の企画・実施) ISACA CSXの再販商材等、研修ソリューションを、レベル1～5までを構築。 経済産業省、第四次産業革命スキル習得講座の認定も取得。Level1～2コースは、JMOOCでも採用され第2位 2019年の実績。 警察庁、サイバー系団体にて、サイバーインシデント現状等、セミナー講師を多数実施。 NISC様での種々採用を機に、アライドテレシス (株) への合併が決定 (2020年1月)

・アライドテレシスアカデミーにて、サイバーセキュリティ研修マップ、および研修ソリューションをゼロから構築し、実施運営を実施

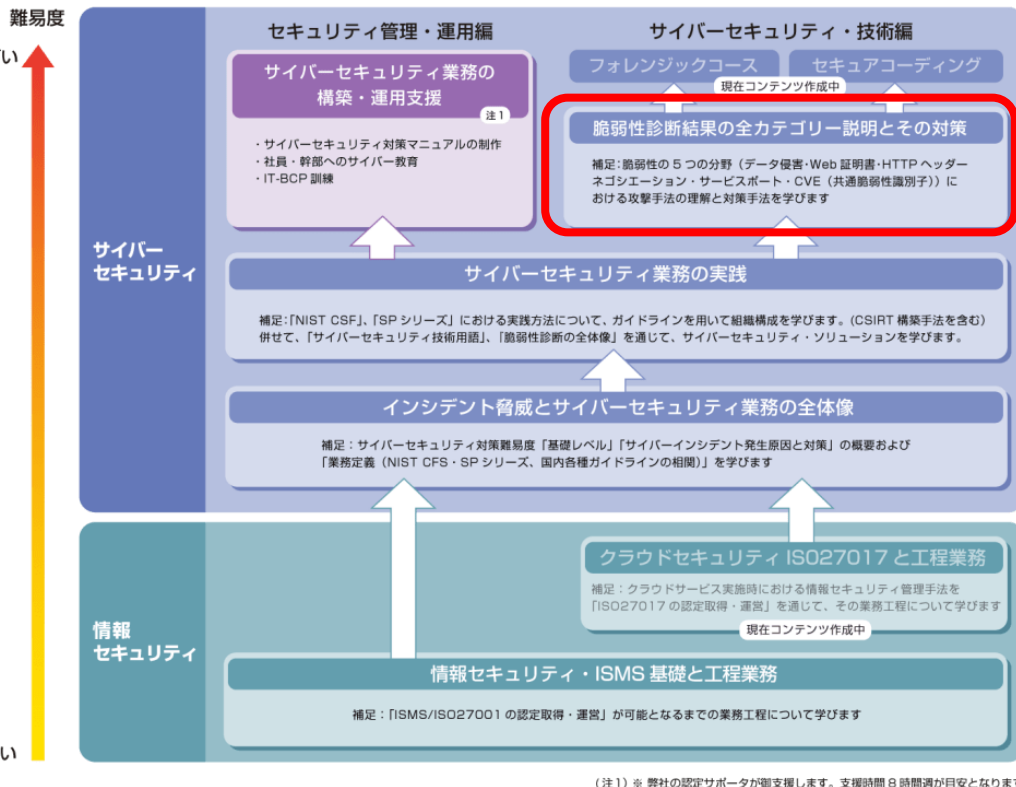
* 2006-2016 スリーイーグルス (株) 代表取締役 (ITソリューション構築、教育事業、人材派遣・紹介事業)、日本初のサイバー演習CYDER (総務省) にてJAIST協業にて、サイバーセキュリティ人材育成のためのITSSを参考にしたレベル定義と、各レベルでのスキル項目の洗い出し研修を構築。→後の経団連・人材定義レファレンスの基となる。 2016年にアライドテレシスグループに事業転売 (M&A)

* 2000-2016 NACSE JPN (株) 代表取締役 (アライドテレシス100%子会社のIT教育会社)、ベンダーニュートラルなネットワーク資格の日本市場・中国市場への展開

* スリーコムジャパン (株) シニアディレクター・コア事業部、NC (=SE)、ダイレクトタッチ営業本部

* 大手電機メーカーでのプログラマーを経、外資LSIメーカーでの通信ボードの製造、アライドテレシス (株) でのNetScape日本販売を手掛ける

※<https://mirai-manabiya.jp/course001/>



サイバーセキュリティ脆弱性診断とは？

サイバー攻撃を防御するためのシステムを再構築する（総称：ハードニング）
ハードニングの前段階で行うのが、サイバーセキュリティ脆弱性診断

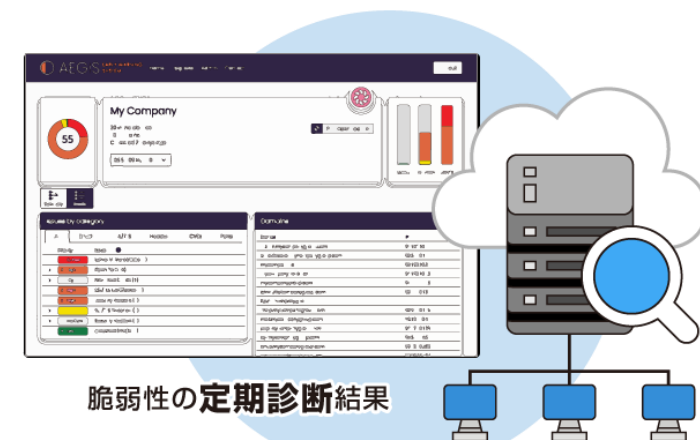
■ システムの健康診断

人間が病気を見つける場合、いきなり細胞診をしたり治療を始めたりしません。まず、健康診断を受け、病気を見つけます

システムも同じです。
インターネット上の資産、およびインターネットの端末に対して診断を行い、検出された脆弱性の深刻度に応じて対策を行います



人の健康診断



システムの健康診断
||

サイバーセキュリティの脆弱性診断

システムの健康診断 = サイバーセキュリティ脆弱性診断

■ どのような順序で行うの？

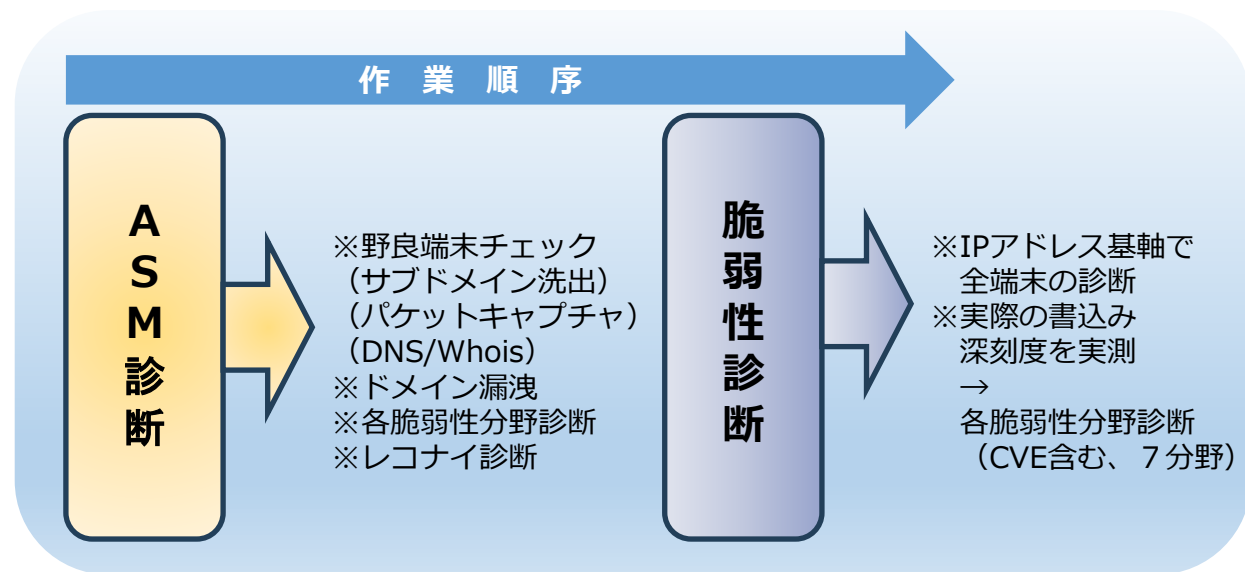
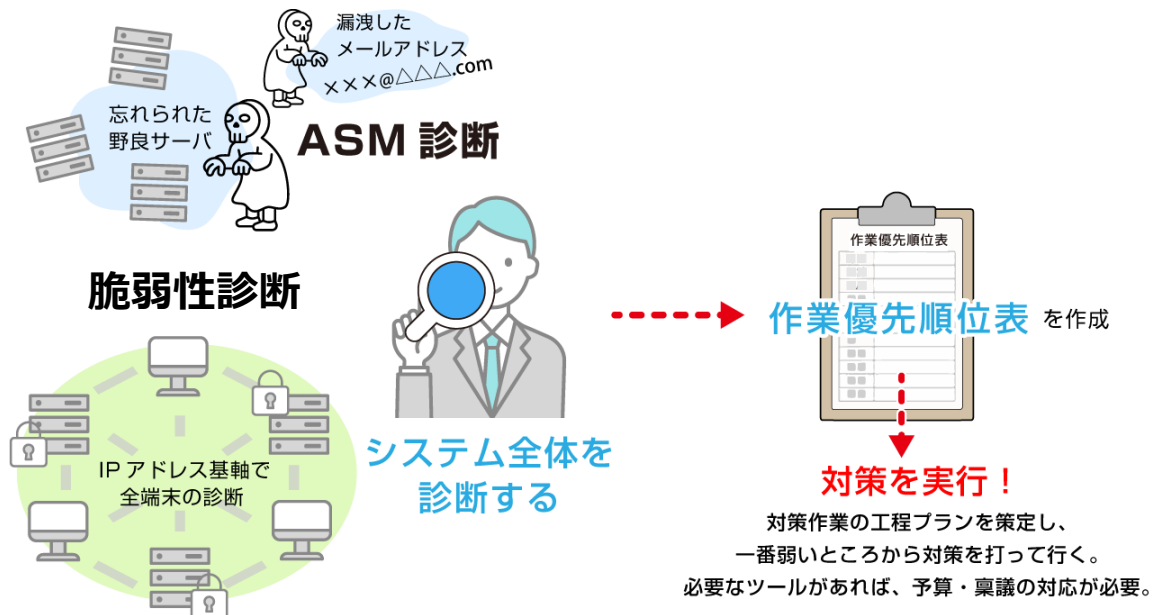
Step1 システム全体を診断（ASM診断・脆弱性診断）

Step2 作業優先順位表を作成（脆弱性の深刻度順）

Step3 一番危険なところから対策を行う

- 対策にツールが必要な場合は、予算・稟議が必要
- ハードニング作業の工程プランを策定
- 対策の実施

- 1、ASM診断
- 2、脆弱性診断
- 3、作業優先順位の策定
- 4、対策の実施



■ASMとは？

組織の外部（インターネット）からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスをいいます。

出典：経済産業省「[ASM \(Attack Surface Management\) 導入ガイドンス](#)」

ASMでは、標準の通信方法でのみ調査をしています。このため、調査できる内容に限界があります。

①ASM…パッシブスキャン(Passive Scan)

パッシブスキャンは、ドメイン情報から放置サーバ（野良サーバ）も検出して、ハンドシェイクパケットと外部脆弱性DBのみで診断します。

②脆弱性診断…アクティブスキャン(Active Scan)

アクティブスキャンは、調査対象端末に対して、ハッカーが実際にアクセスする手法に近いパケット書込みを行って診断します。

**ASM（パッシブスキャン）は、あくまで資産洗い出しのために使います。
特に、ポート脆弱性とCVEはリアルタイムのサーバ情報を見ていません。
正確な診断をするためには、脆弱性診断（アクティブスキャン）が必要です。**

参考：経済産業省

「[ASM \(Attack Surface Management\) 導入ガイドンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～](#)」

<https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf>

セキュリティ診断は、ASMが必須です

■脆弱性診断・ペネトレーションテストだけでは、砂上の城

ハッカーが最初に攻撃先を探すツールがASMです

ASM診断で、ハッカーから狙われやすい脆弱性を早期に発見することが大切です

何も対策をしていない状態



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！

脆弱性診断を実施



建物は改築（脆弱性診断）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！

脆弱性診断を実施
+ ASM 診断を実施



地面を強固に（ASM 診断を実施）改良し
完全なハードニング基礎が完成して
完全防備となった!!

世界定義の脆弱性診断は、ASM診断と脆弱性診断です。

■プラットフォーム診断ツール『イージスEW』

イージスEW (AEGIS-EW)は、「プラットフォーム診断」を実施するSaaSです。

下記の脆弱性を調査します

- ・ OSI参照モデルのトランスポート層（通信ポート）
- ・ Mailなりすまし対策実施状況
- ・ サーバ証明書の安全性
- ・ HTTPヘッダの安全性
- ・ 公表済みCVEに該当する脆弱性の有無の可能性

加えて「レコナイツール（偵察=Reconnaissance）」機能を持ち、ダークウェブに漏洩した情報を検出します

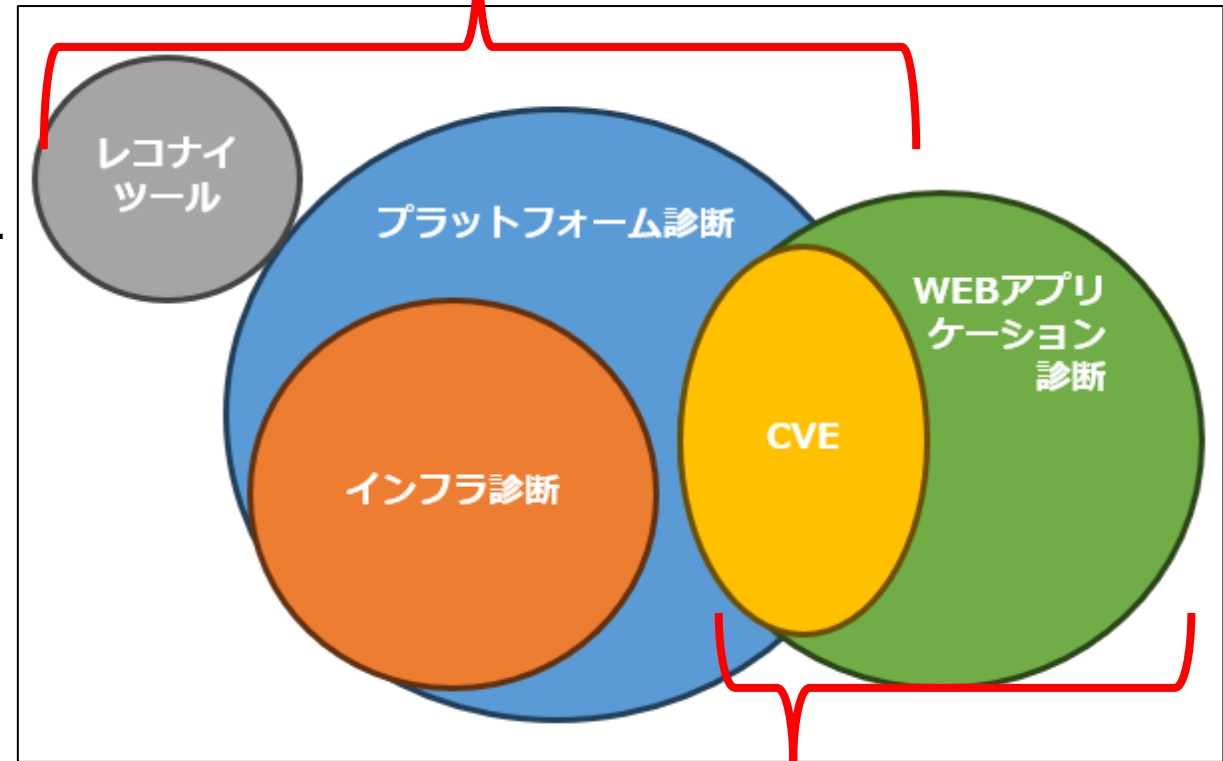
- ・ Breach（データ侵害） ・ サブドメイン

なお、Webアプリケーションにおける「コード診断」は、イージスEWでは実施しません
別ツールの「OWASP ZAP」で診断します。

例：「OWASP ZAP」にて調査する下記項目

- ・ SQLインジェクション
- ・ 強制ブラウズ
- ・ GETパラメータオーバーフローなど

【イージスEW】プラットフォーム診断



【OWASP ZAP】Webアプリ診断

■ 経済産業省の定義

経済産業省の定義では、ASMと脆弱性診断を異なる概念として定義しています。
NessusやOpenVASを用いた脆弱性診断は、パケットの書き込み等を行います。

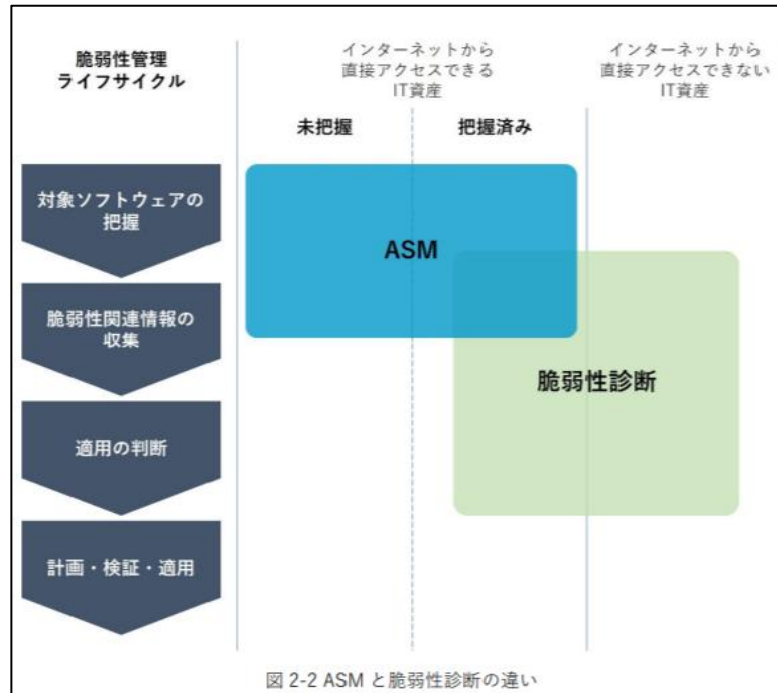
広義の定義	脆弱性診断	
経済産業省の定義	ASM	脆弱性診断
スキャン方法	パッシブスキャン (Passive Scan)	アクティブスキャン (Active Scan)
情報収集方法	WhoisサーバとDNSサーバから情報を取得	あらかじめ指定した IPアドレスを対象とする
脆弱性の確定方法	通常アクセス+脆弱性DB参照 の範囲で行う。精度が低い	攻撃を模したパケットを送信し、 応答で診断するため確度が高い
対象への影響	セキュリティ監視装置（EDS/EDR）に検出される可能性は殆どない	セキュリティ監視装置で アラームを検出することがある 多くの帯域を使用する

経済産業省の定義する「ペネトレーションテスト」は、
NIST-CSF800に基づき各種シナリオを作成し、
エンジニアにより人力で侵入して不具合を検出する試験です。

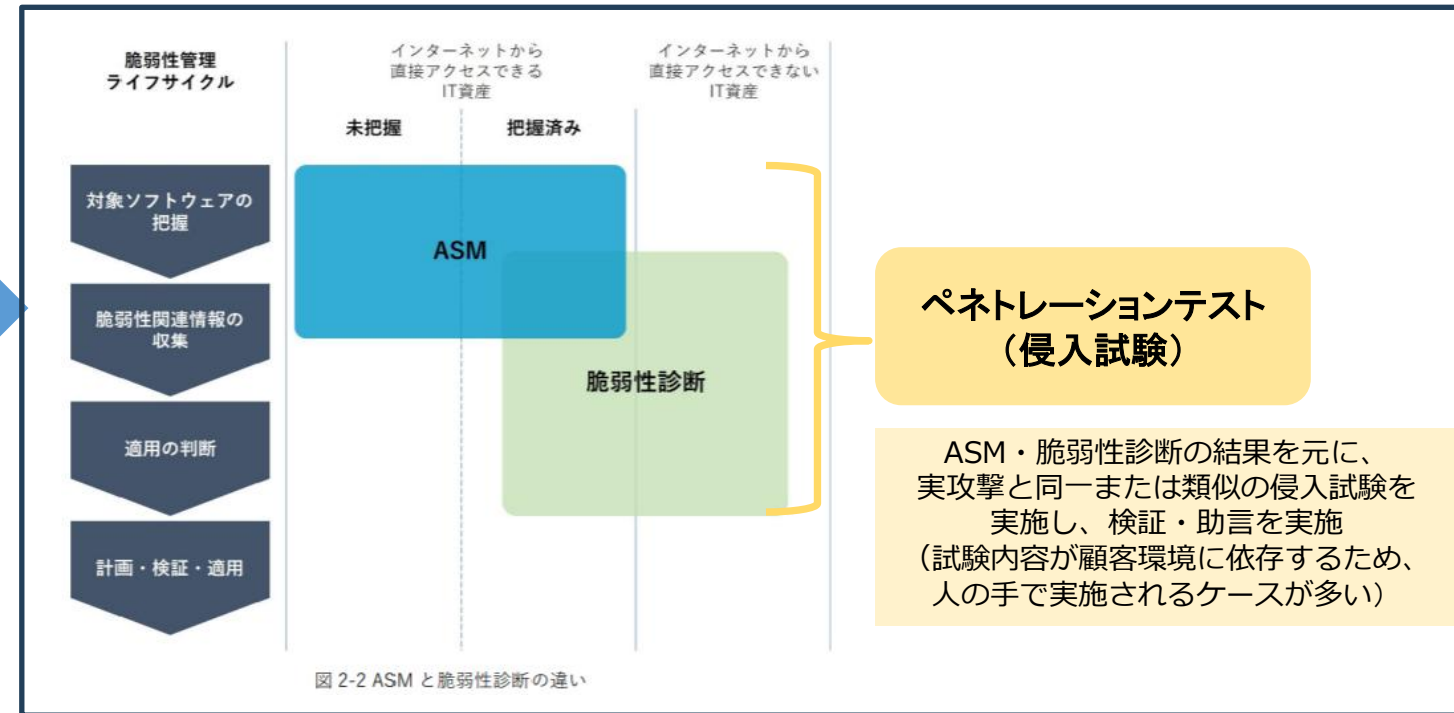
■イージスEWの定義

ASMと脆弱性診断の違いは、以下の通りです。
最も大きな違いは、脆弱性診断が「既知のサーバ」のみを対象にしているのに対して、ASMはレコナイ診断も含み、「認知外（忘れられている）サーバ」も見つけ出して対象にすることです。

経済産業省の定義	ASM診断	脆弱性診断
イージスEWの診断内容	ASM+レコナイ診断	脆弱性診断
スキャン方法	パッシブスキャン (Passive Scan)	アクティブスキャン (Active Scan)
情報収集方法	WhoisサーバとDNSサーバから情報を取得 イージスEW独自契約のデータベースをもとに インターネット上を検索し、発見した端末を対象とする ダークウェブに漏洩した情報も収集する（レコナイ）	あらかじめ指定した IPアドレスを対象とする
脆弱性の確定方法	通常アクセス+脆弱性DB参照 の範囲で行う。精度が低い	攻撃を模したパケットを送信し、 応答で診断するため確度が高い
対象への影響	セキュリティ監視装置（EDS/EDR）に検出される可能性は殆どない	セキュリティ監視装置で アラームを検出することがある 多くの帯域を使用する
イージスEWラインナップ	イージスASM診断	イージス脆弱性診断



※経済産業省「ASM導入ガイダンス」より



未来研究所は、経済産業省の定義するASM・脆弱性診断・ペネトレーションテストを提供いたします

■ ASM (Attack surface Management)

『イージスEW』 (パッシブスキャン)

■ 脆弱性診断

・ プラットホーム脆弱性診断

『イージスEW』 (アクティブスキャン)

・ Webアプリケーション脆弱性診断

『OWASP ZAP+報告会』

■ ペネトレーションテスト (侵入試験)

個別対応 (伴走サービスでのご対応)

プラットフォーム脆弱性診断ツール 『イージスEW』

脆弱性診断ツール イージスEW (AEGIS-EW)

AEGIS EARLY WARNING SYSTEM

見やすい GUI

深程度の割合が
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

※専門知識不要！※

赤色

オレンジ色

の脆弱性は危険！

脆弱性を放置すると、
ハッカーに乗っ取られ、
多大な金銭的被害を受け、
社会的信用に傷が
つきます！

- ・ イージスEWは、プラットフォーム診断SaaSアプリです。
- ・ ツールをインストールすることなく、ASM診断および脆弱性診断が可能です。
- ・ ブラウザで診断結果をご覧いただけます。

赤色やオレンジ色の脆弱性（ぜいじゃくせい）が検出されたホームページは
1年目～3年目の初心者SEでも簡単に乗っ取ることができてしまいます。
イージスEWで診断し、赤色やオレンジ色の脆弱性を修正しましょう。

■イージスEWの診断は、100点満点のスコアと色別グラフで結果表示

イージスEW脆弱性診断の平均点は55点前後です。

スコアが悪い場合は、発見された脆弱性を改善して60点以上を目指すのが目標です。

■グラフの色の見方（国際共通基準：CVSSv3.1）

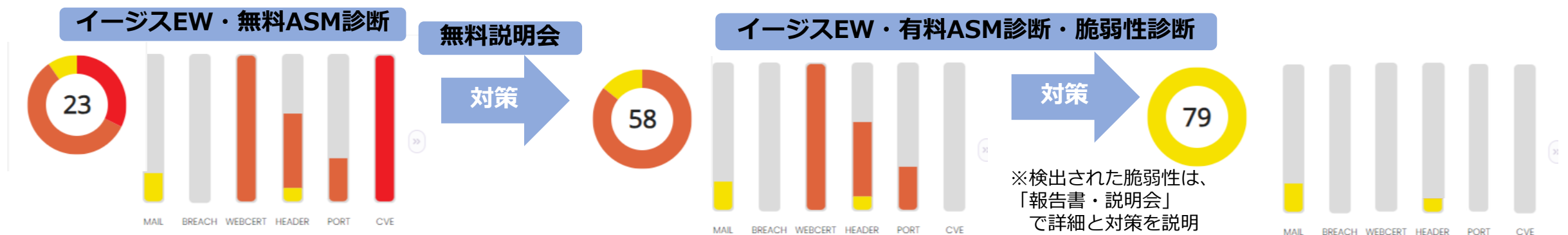
赤（緊急）・オレンジ（重要）色の脆弱性は1年目～3年目の新米SEでも乗っ取れます

赤・オレンジの脆弱性を優先的に改修することが大切です

サイバー先進国（米国・イギリス・NATO主要国・オーストラリア等）では、赤・オレンジ色の脆弱性を放置している企業は、公共機関との取引口座を持てません

日本においても、NIST SP800シリーズへの対応が義務化された、**特定社会基盤事業者**は対応必須

赤やオレンジ色の脆弱性は、必ず対策しましょう！



『イージスEW』 4つの特長

ダッシュボードの見やすいGUI

診断結果の配色は、世界共通の基準CVSS3.1を使用。サイバーセキュリティの知識が無くても深刻度の判断が可能です。サイバー先進国（米国・英国・NATO主要国）では、システムに赤色（緊急）またはオレンジ（重要）の脆弱性が存在すると、公共機関との取引ができません。日本でも、特定社会基盤事業者等には、米国NIST 800シリーズと同等の対応が義務付けられています。イージスEWは、特定社会基盤事業者へ納品する機器の脆弱性診断にもご活用いただけます。

全てのプラットフォーム診断を一括管理

インターネット・イントラネット・納品前機器検証の全てのプラットフォーム脆弱性診断を**イージスEWのGUIで一括管理できる**ため運用保守の管理費用を削減することが可能です。診断結果を一括管理するダッシュボードも、有料診断をご実施いただくことで無料利用可能ですので、他社製品の様に管理ツールを多数インストールすることなく、ブラウザのみで脆弱性管理を完遂できます。

強力なASMと脆弱性診断

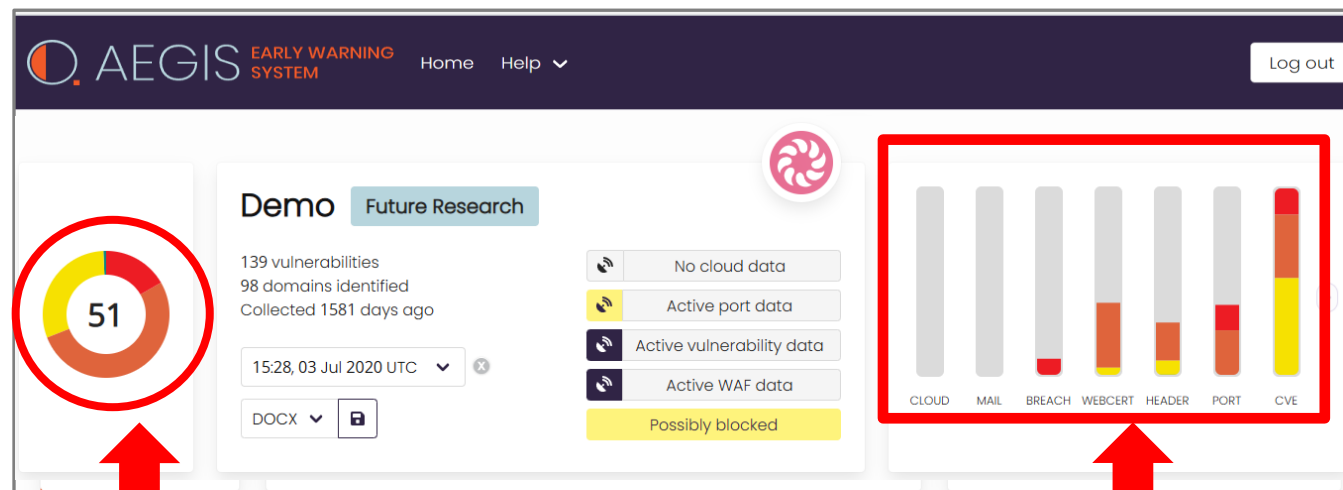
診断に必要なのはメインドメインのみ。ハッカーが攻撃対象を絞り込むために用いるレコナイツール機能を含んだASM診断により、野良端末及び漏洩したドメイン情報も検出いたします。脆弱性診断は、ASM診断で判明したIPアドレスを基軸に対象にパケット書込みを行うなど深く診断します。

リーズナブルな価格帯

システムの「健康診断」である脆弱性診断は、定期的な実施が必須です。ユーザネットワークの拡大に伴い、サイバー攻撃の対象端末も増加しています。そのため、**脆弱性診断のコストが高額になると、適切な回数の定期診断の実施が困難になります。**イージスEWは1,000を超えるドメイン数の診断も他社製品より圧倒的安価に実施可能であり、増え続けるドメイン管理への対応も一口コストで可能です。

■セキュリティの専門家でなくとも深刻度が判断できます

共通のGUIを用いたダッシュボードで、全てのプラットフォーム診断を管理できます



総合評価（レイティング）（**51点/100満点**）
脆弱性深刻度分類：
「非常に重要度の高い脆弱性リスク」あり

本来、あってはならないはずの
「深刻度緊急（グラフ赤色）の脆弱性」
が存在することが判明

色は国際基準であるCVSSv3.1に準拠

深刻度	CVSS v3.1 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

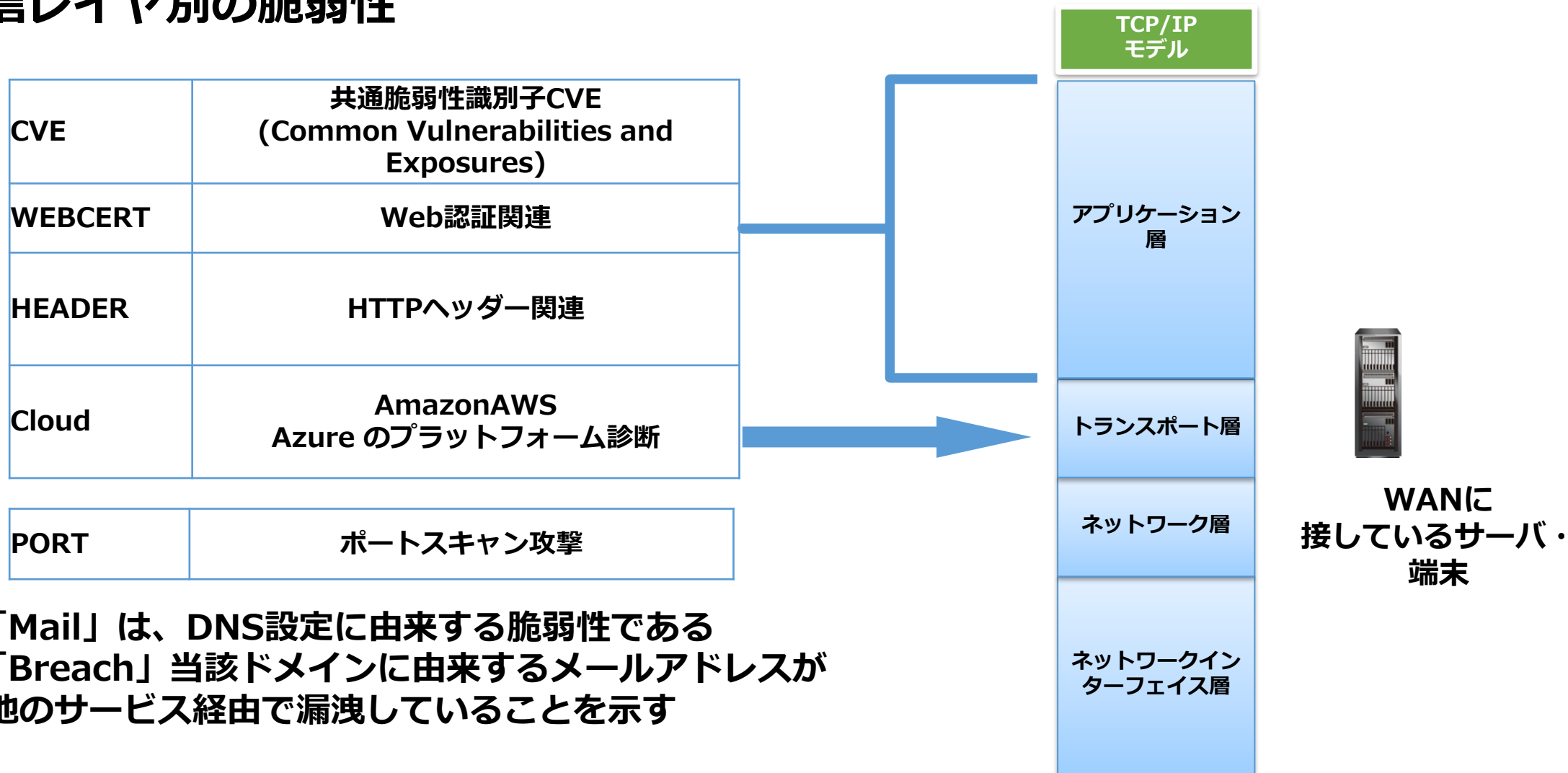
赤：SE1年目で乗っ取れます
オレンジ：SE2－3年目で乗っ取れます

■ 8つの診断分野

8つの分野別に表示されるため、各分野ごとに分析・対策が可能です

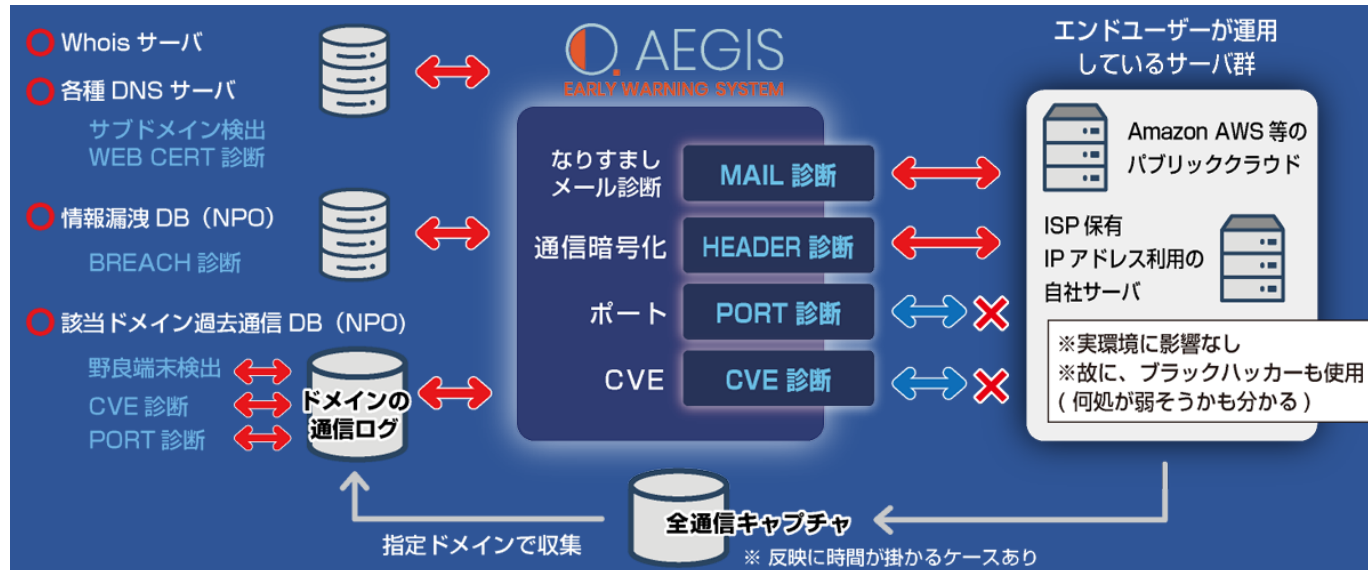
CVE 共通脆弱性識別子	CLOUD Cloudプラットフォーム診断	MAIL 送信ドメイン認証	BREACH データ侵害 (情報漏洩)	WEBCERT Web 認証関連	HEADER HTTP ヘッダー 関連	PORT ポートスキャン 攻撃	SUBDOMAIN 野良端末検出
個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体のMITRE社が採番している識別子です。脆弱性検査ツールや脆弱性対策情報提供サービスの多くがCVEを利用しています。	Amazon AWS・Microsoft Azureにおけるセキュリティポリシーを診断します。VPC (Virtual Private Cloud) 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。また、重要な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に対するハードウェアMFA (Multi-Factor Authentication) の有効化について確認することも可能です。	「受信したメールが正規の送信元から送られてきたかどうか」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)	攻撃者が、Webサービス等に攻撃を仕掛けて得た個人情報やデータ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軸にした診断を実施します。	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。	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診断します。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。	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閉めておく対策が求められます。	サブドメインの管理は、セキュリティにおいて非常に重要な要素です。管理されていない野良端末（特に開発環境やテスト環境）が存在する場合、攻撃者にその隙間を突かれるリスクが高まります。野良端末検出機能は、これらの放置されたサーバを自動的に探し出して、リスト化します。
			レコナイ ツール				レコナイ ツール

■ 通信レイヤ別の脆弱性



- ・「Mail」は、DNS設定に由来する脆弱性である
- ・「Breach」当該ドメインに由来するメールアドレスが他のサービス経由で漏洩していることを示す

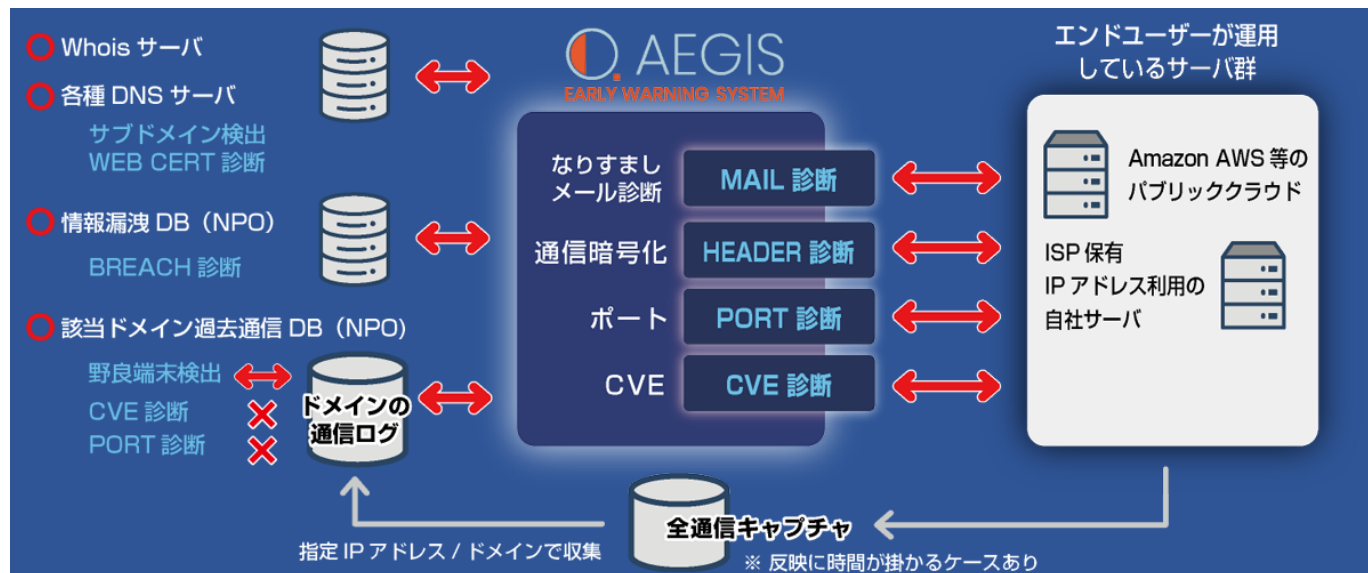
強力なASMと脆弱性診断



【ASM (パッシブスキャン)】
ハッカーが攻撃対象サイトの偵察に使用します

- ・ 野良端末の存在が分かります
(多くは**完全放置**。モジュールが古く乗っ取り可能)
- ・ 機器のファームバージョンが分かります
(バナー表示がONの場合)
→ **VPNルータの簡単乗っ取り**
- ・ 外部サービス経由で漏洩したドメイン由来の個人情報も分かります
→ **例：社員のメールアドレスがPW付きで漏洩している**

※CVE・Portについては、確度が低くなります



【脆弱性診断 (アクティブスキャン)】
IPアドレスを基軸に、深い部分まで侵入を試み、パケットを書き込んだ結果をもとに診断します

イージスEWは、OpenVAS (Github/Freeware) の診断項目を網羅したGreenBorn社のAPIを使用し、14万にも渡る項目の診断を実施します

■イージスEW ASM診断のレコナイツール機能（レコネサンス＝偵察）

イージスEWのASM診断（パッシブスキャン）には、レコナイツール機能が盛り込まれています。（BREACH・SUBDOMAIN）

「レコナイ」とは、「レコナイサンス」または「レコネサンス」という単語の略で、軍事・サイバー用語で「偵察」の意味があります。 **（Reconnaissance＝偵察）**

レコナイサンス (偵察) ツールは、ハッカーが攻撃対象を絞り込むために用います。ハッカーはレコナイツールを用いて、世界中のインターネット上から、脆弱性が多く侵入しやすいようなシステムをまず見つけ出します。

イージスEWは、ハッカーと同等のツールを使用し、攻撃対象領域（Attack Surface）や漏洩した情報を見つけ出します。

※ASM（パッシブ）の診断結果のうち
Port・CVEは、確度が低くなります。

全てのプラットフォーム診断を一括管理

1 インターネット上の脆弱性診断

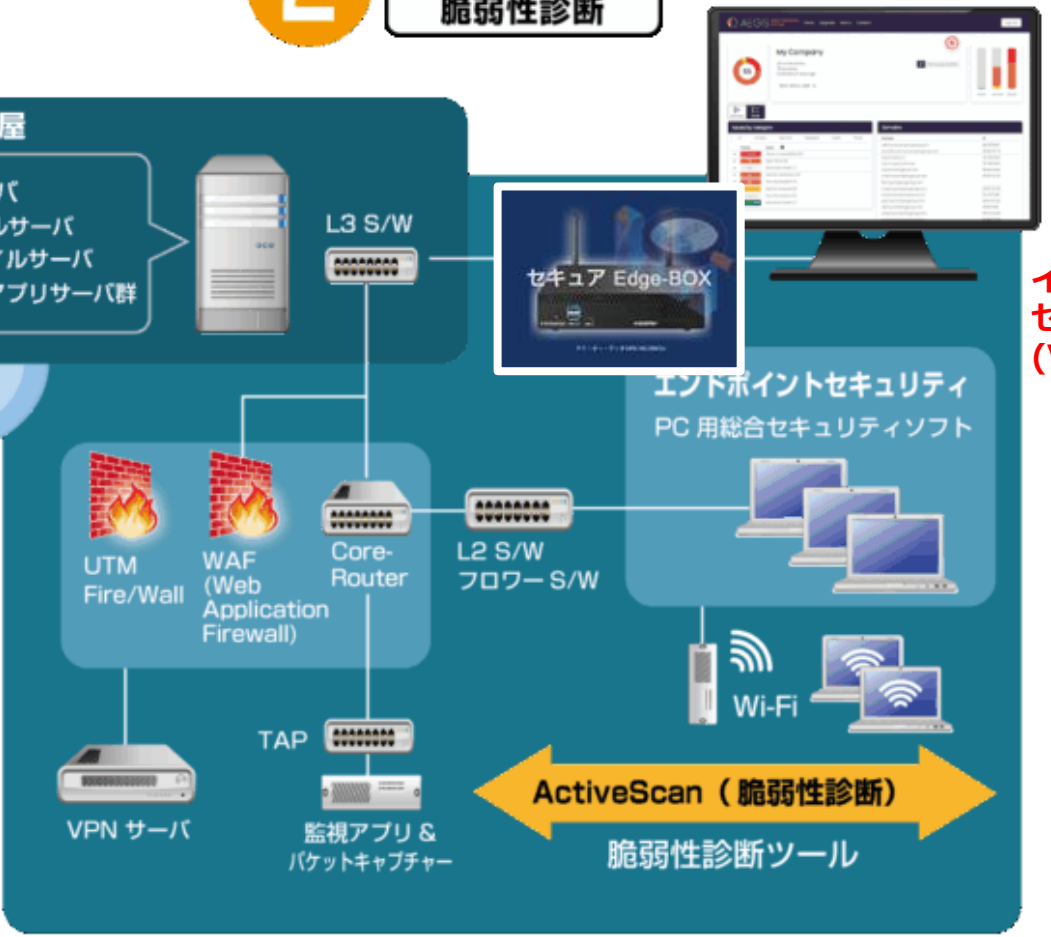
ASM / 脆弱性診断



イージスEW

2 社内イントラネット 端末群の脆弱性診断

脆弱性診断



イージスEW +
セキュアEdge-BOX
(VPN)

3 納品前 機器検証サービス 脆弱性診断

脆弱性診断



イージスEW +
SimつきWi-Fiルータ+
セキュアEdge-BOX(VPN)

■エンドユーザ様…複数拠点・診断の一括管理

有料診断をお申込みいただくことで、
複数診断結果を一括管理可能なダッシュボードを
ブラウザで無料でご利用いただけます



個別ドメイン診断結果



■販売代理店・VAR様

顧客の診断一括管理・
サポートが可能になります



顧客A

顧客B

顧客C



■小規模システムから大規模システムまでリーズナブルに診断可能

イージスEWは、チェック対象の端末総数が数千台以上になっても、ASM・脆弱性診断を定期的に行うことができるリーズナブルな価格帯で提供しております。

また、少ないドメイン数であっても、ツールなどの初期投資が不要で、リーズナブルな価格帯となっております。

ASM・脆弱性診断とも、1ショットから年間契約の定期診断まで、実施可能です。

価格は完全オープン価格となっておりますが、

お問い合わせいただければ、価格開示とともに各種御見積を作成いたします。

(正確な御見積を作成するには、無料ASM診断によるドメイン数の算出が必要です)

■リーズナブルな価格帯の理由

開発元のTitanium Defence社が政府系組織と連携しており政府資金の投入があることが理由です。

- ・イージスEW開発にあたりオーストラリア政府・ニュージーランド政府の援助を受けている
- ・ヴィクトリア大学との産学連携である
- ・診断にイギリス政府系のDBを使用している

■イージスEW開発元 Titanium Defence Ltd. (TTD)

[TTD \(Titanium Defence Ltd.\)](#) の前身は、英国サイバーセキュリティ機関（GCHQ UK Intelligence・Security and Cyber Agency、MI6等）での就業経験者が集まったサイバー・コンサルファームでした。2017年のオーストラリアからの誘致プログラムを活用し、彼らの出身国であったニュージーランドに会社移転をして設立されたのがTTD社です。イージスEWは、オーストラリア・ニュージーランドの助成金を活用し、ヴィクトリア大学との産学連携にて制作されたツールです。また、イージスEWのスキャンに用いるDBやパケットスニッファ（パケットキャプチャ）も英国との関係を活かし、英国政府のものを特価で利用しています。そのため、低価格での提供が実現されています。

■オーストラリアがサイバーセキュリティ企業を誘致した理由

2017年、オーストラリア軍のサプライチェーンに属する従業員約50名の企業から、ロッキード・マーチン社製の最新鋭ステルス戦闘機「F-35」に関する30GBのデータ、およびボーイング社製哨戒機「P-8」の情報が流出するインシデントが発生しました。この事件をきっかけに、米国ではNIST SP800-171への対応が義務化され、世界的にサプライチェーンの強化が求められるようになりました。オーストラリア政府は、この事態を受けてサイバーセキュリティを強化するため世界中から企業を誘致し、サイバーツールの製造・開発を行う企業への支援を実施しました。その厳しいプログラム選考を通過したのが、TTD社の「イージスEW」です。

TTD社CEO兼CTOであるAnthony Grasso氏は、その高いサイバーセキュリティの知見をもとに、ニュージーランド国営ラジオ局（ラジオNZ）でのサイバーセキュリティプログラムも担当しています。

オーストラリア企業の情報流出事件に関する記事：

BB News：

<https://www.afpbb.com/articles/-/3146446>

ウォール・ストリート・ジャーナル：

<https://jp.wsj.com/articles/SB10922266312659313634204583449643578613634>

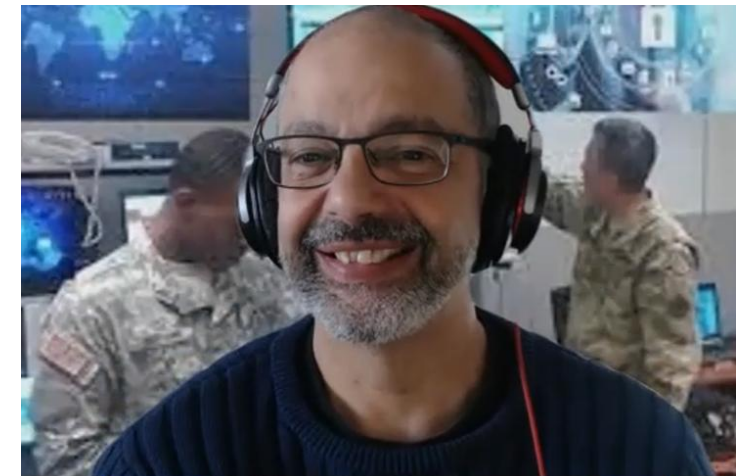
日経新聞：

https://www.nikkei.com/article/DGXLASGM19H7Z_Z10C15A1FF8000/

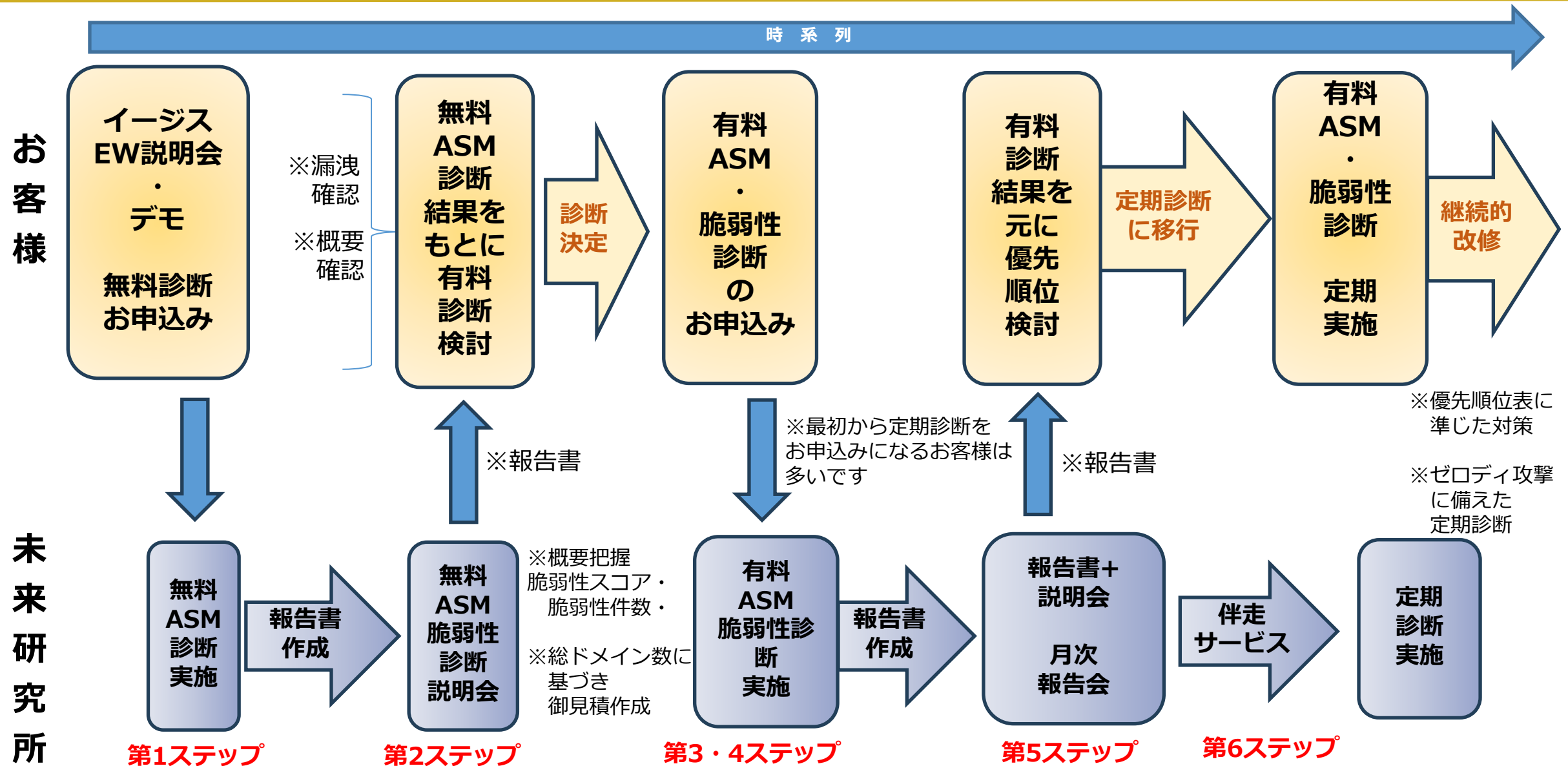
Anthony Grasso氏の国営ラジオNZプログラム例：

[Technology: Is 'it's inevitable' good enough after a hack?](#)

[LPM breach could have revealed thousands of people's data](#)



イージスEWの導入フローとサービス



第1ステップ 無料ASM診断

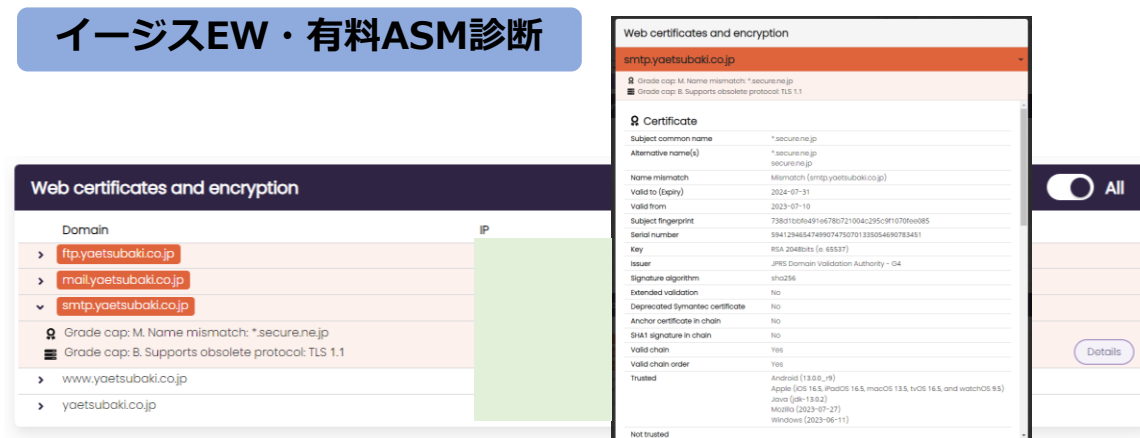
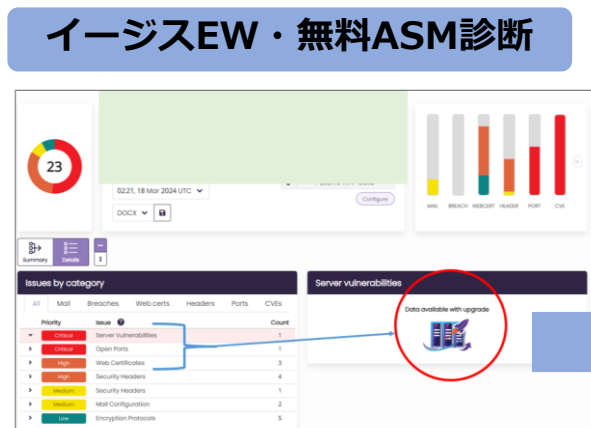
■ イージスEW・無料ASM診断

分野別に、「緊急」「重要」など深刻度ごとの脆弱性の件数などの概要が判明します

しかし、無料診断では、脆弱性の詳細は判明しません

→ 詳細は**イージスEW「ASM診断」・「脆弱性診断」**

※「ASM診断」は、「脆弱性診断」に比べて精度が落ちます



無料ASM診断実施後、エンドユーザ様&Web開発会社様へ、無料説明会を実施いたします
Web開発会社様が修正出来ない事項は、未来研究所が完全サポートし脆弱性改修いたします

第2ステップ 無料ASM脆弱性診断 無料説明会

■ イージスEW無料ASM脆弱性診断の報告書を作成し、説明会を実施いたします

ただし、無料ASM脆弱性診断は、簡易的な診断であり、診断内容の詳細や正確性に限界があります
脆弱性の詳細を分析し、詳しい対策を知るためには、有料診断が必要です

無料説明会

無料ASM脆弱性診断の報告書を提出し
対処方法を簡易的に伝えします

【弊社スタッフが作成する報告書】

XXX 様 セキュリティ脆弱性・リスクチェック概要レポート

<https://www.ご指定のドメイン.jp/>

サンプル企業

199 の脆弱性
343 個のドメインが特定されました
101 日前に収集

2022年6月12日 03:17

バックポートデータ
自動的脆弱性データ
バックポートデータ

Web Certs (Web証明書)

■このサブドメイン向けの証明書が機能していません

Web Certs (Web証明書)

■このサブドメイン向けの証明書が機能していません

現在の証明書有効期限が切れ

Mail 脆弱性 (送信ドメイン認証)

■DKIM, DMARCの記述が欠落している
診断結果: 「なりすまし対策」として、不足している箇所がある

C:\Users\Fuser>nslookup -q=txt mail. co.jp
Server: unknown
Address: 192

Non-authoritative answer:
mail. co.jp canonical name = co.jp
text =
"v=spf1 include:spf.protection.outlook.com include:mwhg4s27.powerspf.com -all
youtubelink.co.jp text =
"MS=ms45041966"

「SPF」の記述が無く、片手落ちである。
こいつでは、なりすまし対策がない。(悪意メールヘッダーで、IPアドレスを盗ると、手立てが限られる)

メールヘッダーは、信頼可能です。
メールヘッダーに「なりすまし対策」が必要です

AEGIS(イ)

【イージスEWにより自動生成される評価レポート】

※概要

Cyber Security Board Report

• Date: 2020-07-03
Demo

• Data breaches^{1,2}
There are 6 email breaches, of which 2 are critical. You have accepted no email breaches.
The most recent breach was December 2021.

• Web certificates and encryption^{1,2}
There are 14 web certificates that pose a non-critical security threat. You have accepted no security threats.
No data from the previous month.
In the past three months there were 14 domains that have only been seen with issues.

• Open ports^{1,2}
There are 14 server addresses with open ports, totaling to 57 open ports. There are 3 server addresses with critical open ports, totaling to 3 critical ports. You have accepted no open ports.
No data from the previous month.
In the past three months there were 14 server addresses that have only been seen with open ports.

• Server vulnerabilities^{1,2}
There are 39 server addresses with vulnerabilities, totaling to 263 vulnerabilities. There are 2 server addresses with critical vulnerabilities, totaling to 2 critical vulnerabilities. You have accepted no vulnerabilities.
No data from the previous month.
In the past three months there were 39 server addresses with vulnerabilities.
1 vuln appears in **Info** Most Dangerous Weaknesses.

• Notes¹
1. The counts in each section are of non-accepted as audited and deemed secure or otherwise not a concern.
2. Active port data. Only including prior collections via

※詳細

• Demo

• C (51/100)
Collected 1125 days ago
15:28, 03 Jul 2020

• Domains (98 identified)

Domain	IP	Grade	Protocol
ablink.nz.b.demo.aegis-ew.com	172.16.0.63	A	TLS 1.2, TLS 1.3
ablink.nz.c.demo.aegis-ew.com	172.16.0.61	A	TLS 1.2, TLS 1.3
ablink.nz.d.demo.aegis-ew.com	172.16.0.31	A	TLS 1.2, TLS 1.3
ablink.nz.f.demo.aegis-ew.com	172.16.0.67	A	TLS 1.2, TLS 1.3

Issues by category (139 vulnerabilities)

Priority	Issue	Count
CRITICAL	Server Vulnerabilities	2
CRITICAL	Open Ports	3
CRITICAL	Breached Emails	1
HIGH	Server Vulnerabilities	1
HIGH	Open Ports	1

Data breaches

Email Address	Company Breached	Date of Breach	Breached Information
xxxxxxxx1@demo.aegis-ew.com	Zomato	2017-05-17	Email addresses, Passwords, Usernames
xxxxxxxx1@demo.aegis-ew.com	Zynga	2019-09-01	Email addresses, Passwords, Phone numbers, Usernames
xxxxxxxx1@demo.aegis-ew.com	db151dd	2020-02-20	Email addresses, Job titles, Names, Phone numbers, Physical addresses, Social media profiles
xxxxxxxx3@demo.aegis-ew.com	Apollo	2018-07-23	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles
xxxxxxxx2@demo.aegis-ew.com	FlexBooks	2021-12-23	Email addresses, Names, Partial credit card data, Passwords, Phone numbers
xxxxxxxx2@demo.aegis-ew.com	MGM2022Update	2019-07-25	Dates of birth, Email addresses, Names, Phone numbers, Physical addresses

Web certificates and encryption

Domain	IP	Grade	Protocol
ablink.nz.b.demo.aegis-ew.com	172.16.0.63	A	TLS 1.2, TLS 1.3
ablink.nz.c.demo.aegis-ew.com	172.16.0.61	A	TLS 1.2, TLS 1.3
ablink.nz.d.demo.aegis-ew.com	172.16.0.31	A	TLS 1.2, TLS 1.3
ablink.nz.f.demo.aegis-ew.com	172.16.0.67	A	TLS 1.2, TLS 1.3

ぜひこの機会に
ご検討ください。
お待ちしております。

お申し込みは、
sales@future-research.jp
までお気軽にどうぞ！

■ 有料ASM・有料脆弱性診断の実施

有料ASM診断

脆弱性の発生しているドメインや、脆弱性の具体的内容が判明します。
但し、表面的な診断のため正確性には劣ります。

有料脆弱性診断

実際のパケット書込み等を実施してCVE脆弱性を正確に診断し、
詳細や改修方法まで判明します。

■ 有料ASM・有料脆弱性診断のサービス内容

脆弱性診断＋診断結果管理機能（1年間ダッシュボードを利用可能）

イージスEWで実施した脆弱性診断の自動生成レポートは出力されますが、
弊社スタッフ作成の報告書と説明会は、有料診断には付随いたしません
貴社ご担当者様が、イージスEWを利用して診断結果を分析される場合、
インターネット上の膨大な情報から情報収集する必要があります。

脆弱性詳細・対策方法の把握と、今後の工程の指標として、
脆弱性の改修を確実にご進行し、セキュアな環境を構築されるため、

**新規ドメインの有料診断をお申込みいただく際は、
初回診断時「報告書＋説明会」または、「月次報告会」
をバンドルでお申込みいただいております。**

■ 修正方法の例

【報告書＋説明会の報告書例】

以下は、Apache における「IP アドレス直接ブラウジング禁止」設定例です。

■ 「IP アドレス直接指定によるブラウジングの禁止」設定手順

Apache の設定ファイルを編集します。

通常、設定ファイルは以下のいずれかです：

```
/etc/httpd/conf/httpd.conf (CentOS, RHEL など)  
/etc/apache2/apache2.conf または /etc/apache2/sites-available/000-default.conf  
(Debian, Ubuntu など)  
仮想ホストで IP アドレスへのアクセスを制御  
デフォルトの仮想ホストに次の設定を追加します。
```

```
-----  
<VirtualHost *:80>  
    ServerName _default_  
    <Location />  
        Order deny,allow  
        Deny from all  
    </Location>  
    ErrorDocument 403 "Direct IP address browsing is not allowed."  
</VirtualHost>  
-----
```

設定の説明

ServerName _default_: IP アドレスに対するリクエストをキャッチするための仮想ホスト。
<Location /> ブロックで、すべてのアクセスを拒否します。
ErrorDocument 403 を指定して、拒否時に返すエラーメッセージをカスタマイズ。

なお、HTTPS(ポート 443)でも同様に設定する必要があります：

```
-----  
<VirtualHost *:443>  
    ServerName _default_  
    <Location />  
        Order deny,allow  
        Deny from all  
    </Location>  
    ErrorDocument 403 "Direct IP address browsing is not allowed."  
    SSLEngine on  
    SSLCertificateFile /path/to/your/certificate.crt  
    SSLCertificateKeyFile /path/to/your/private.key  
</VirtualHost>  
-----
```

COPYRIGHT ©2025 (株)未来研究所 FUTURE RESEARCH INC. ※

弊社スタッフの
豊富な経験を
ご活用ください。



第5ステップ「報告書+説明会」「月次報告会」

- 有料ASM・脆弱性診断の実施により、脆弱性の詳細が判明します
ただし、有料診断に弊社報告書は付帯しないため、新規ドメインの少なくとも初回診断時は、報告書をバンドルで付帯しております。

■ 「報告書+説明会」

弊社スタッフが、検出された脆弱性を分析して報告書（2時間程度で説明可能な分量）を作成し、2時間程度の説明会で脆弱性詳細や修正方法のご説明を差し上げます。

- ・ サーバ環境の調査
- ・ 脆弱性重要度に応じた具体的な修正方針はここに含みます

■ 「月次報告会」

ASM・脆弱性診断の年間契約の診断に対して、毎月の月報作成と毎月の報告会を実施いたします。

【報告書+説明会の報告書例】

です。

■ 「IP アドレス直接指定によるブラウジングの禁止」設定手順
Apache の設定ファイルを編集します。
通常、設定ファイルは以下のいずれかです：

```
/etc/httpd/conf/httpd.conf (CentOS, RHEL など)  
/etc/apache2/apache2.conf または /etc/apache2/sites-available/000-default.conf (Debian, Ubuntu など)  
仮想ホストで IP アドレスへのアクセスを制御  
デフォルトの仮想ホストに次の設定を追加します。
```

```
-----  
<VirtualHost *:80>  
    ServerName _default_  
    <Location />  
        Order deny,allow  
        Deny from all  
    </Location>  
    ErrorDocument 403 "Direct IP address browsing is not allowed."  
</VirtualHost>  
-----
```

設定の説明
ServerName _default_：IP アドレスに対するリクエストをキャッチするための仮想ホスト。
<Location /> ブロックで、すべてのアクセスを拒否します。
ErrorDocument 403 を指定して、拒否時に返すエラーメッセージをカスタマイズ。

なお、HTTPS(ポート 443)でも同様に設定する必要があります：

```
-----  
<VirtualHost *:443>  
    ServerName _default_  
    <Location />  
        Order deny,allow  
        Deny from all  
    </Location>  
    ErrorDocument 403 "Direct IP address browsing is not allowed."  
    SSLEngine on  
    SSLCertificateFile /path/to/your/certificate.crt  
    SSLCertificateKeyFile /path/to/your/private.key  
</VirtualHost>  
-----
```

COPYRIGHT ©2025 (株)未来研究所 FUTURE RESEARCH INC. ※

弊社スタッフの
豊富な経験を
ご活用ください。



■「伴走サービス」…イージスEWで検出された脆弱性の改修サービス

基本方針「揺り籠から墓場まで、最後までご支援致します」

CVSS3.1深刻度緊急（赤）・重要（オレンジ）の脆弱性改修支援を、
週1日就業（35h/月）～からチケット制で提供

遠隔地の場合、セキュアEdge-BOX（VPN BOX）をお送りし、お客様と一緒に改修します

■その他特定業種支援サービス

医療機関

- ・「[医療情報システムの安全管理に関するガイドラインV6](#)」の御支援

教育機関・中小企業

- ・[地方公共団体における情報セキュリティポリシーに関するガイドライン（2023年（令和5年）3月版総務省）](#)の御支援
- ・[サイバーセキュリティ経営ガイドラインV3](#)の御支援

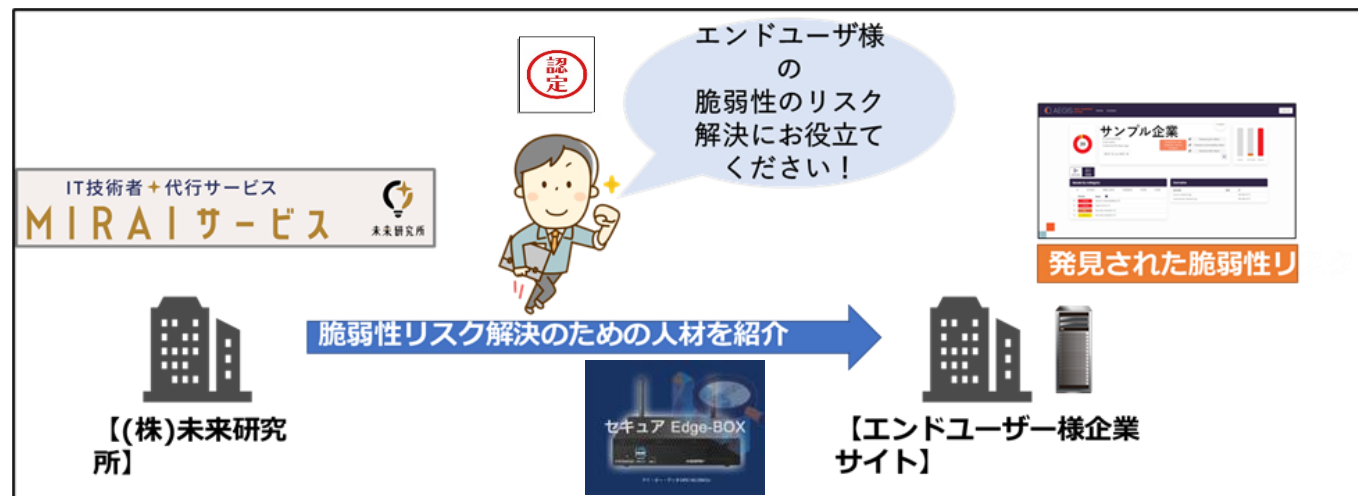
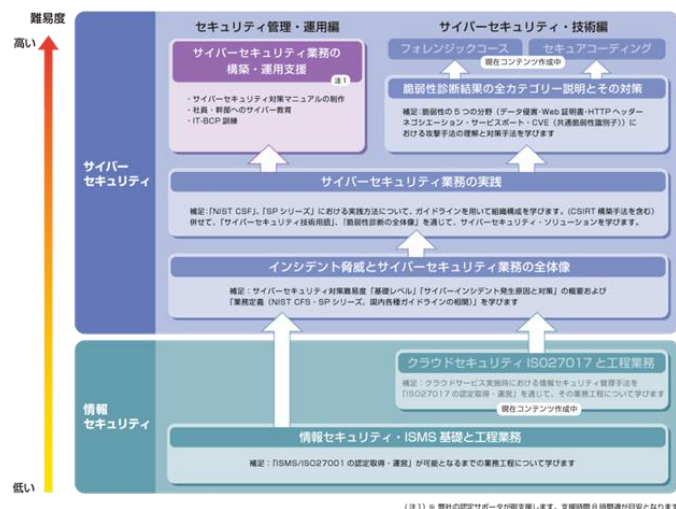
■重要インフラ安全審査の技術分野の支援サービス

[機器のサイバーセキュリティ確保のためのセキュリティ検証](#)の御支援

Thanks

その他各種サービス・補足資料

- 脆弱性診断結果の改修サービス「伴走サービス」以外にも、IT技術者が不足して「一人IS」「IS不在」を余儀なくされているSME・中堅企業様への、IS（情報システム）代行サービスを行います
- 専門知識と技術を持った弊社スタッフがサポートします
- ICT支援員・ギグワーカー/副業希望者・地域の提携SIerと協力します
- 協力希望者には弊社の研修コースを受講してもらい試験に合格した方を「サポーター」として認定し、品質を保証します

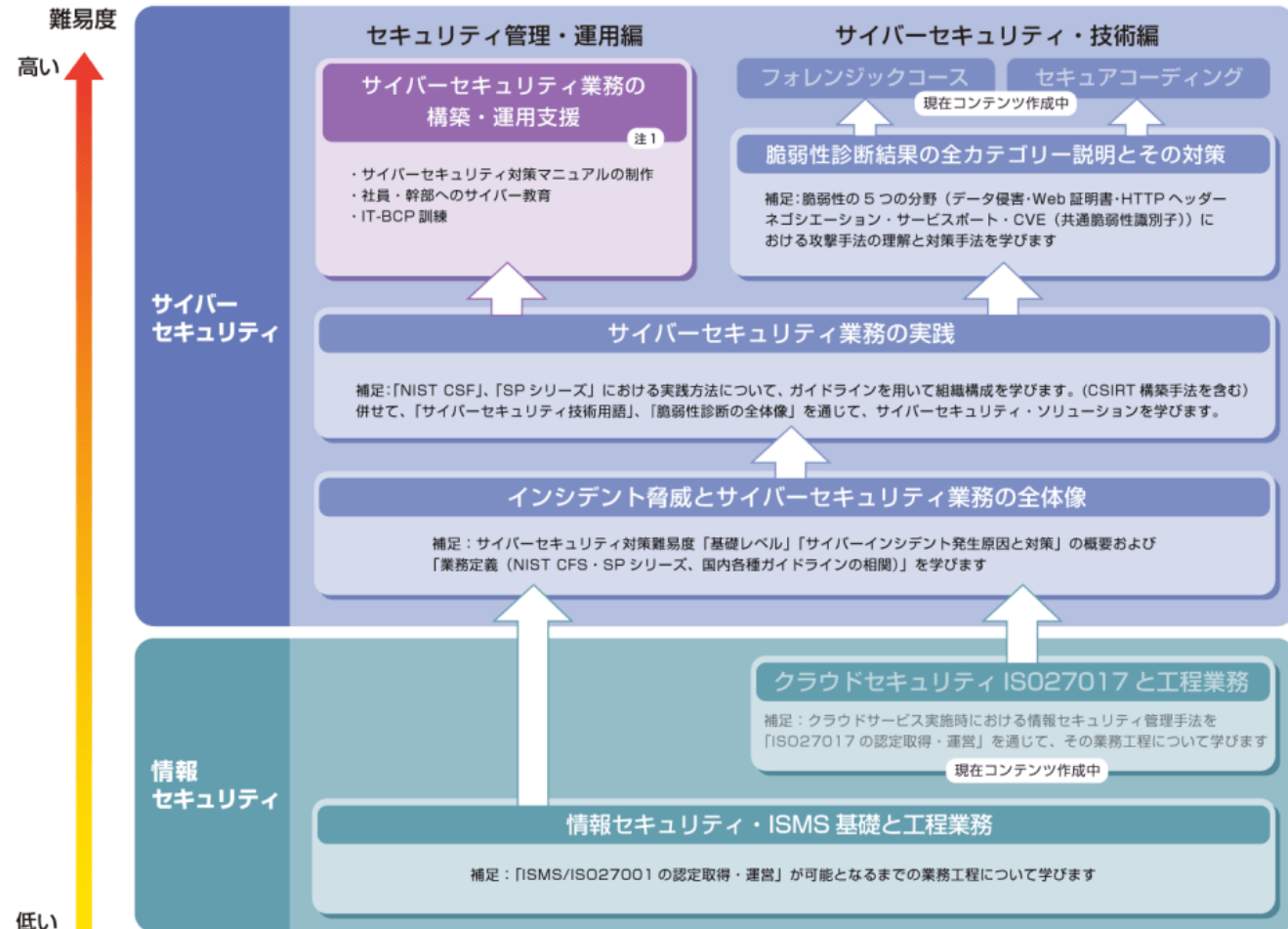
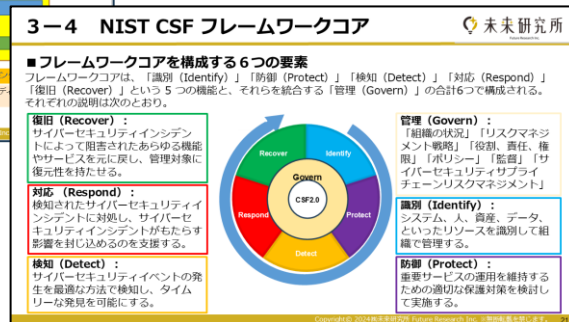
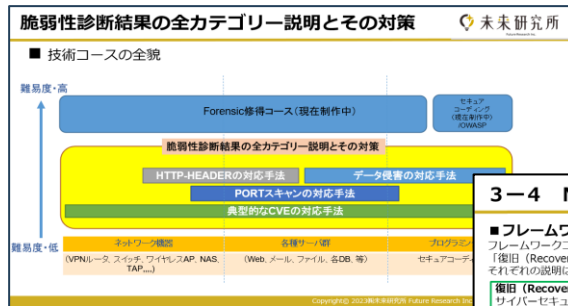


■ 未来の学舎・セキュリティ編の研修コース

対象者：

- ①セキュリティ業務を実行しなくてはならないが、何処から始めて良いかが分からない方
- ②公共組織でIT分野の受発注を担当するが、サイバーセキュリティ商材全般、およびポイントが良くわからない方
- ③脆弱性診断結果に基づいて改修対策を実施する必要があるシステム担当者

上記の御要望に応え、業務目的に応じ難易度別に研修をマッピングしました



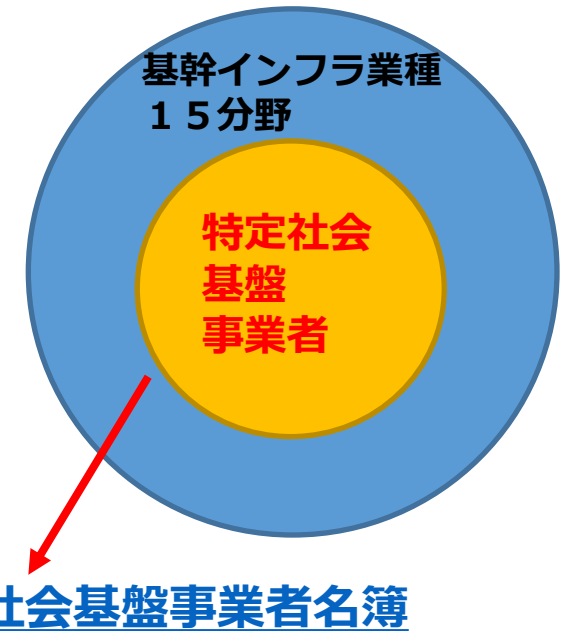
(注1) ※ 弊社の認定サポートが御支援します。支援時間 8 時間週が目安となります

■ 経済安全保障推進法（令和4年法律第43号）

2022年5月18日公布

基幹インフラ役務の安定的な提供の確保に関する制度 2024年5月より運用

- 脆弱性診断の義務化
法律で定められ、届出違反すると罰則が科せられる
- 対象システム
特定社会基盤事業者の特定重要設備
- 脆弱性診断の範囲
インターネット側・イントラ側等の限定は無く、
指定された事業に関する特定重要設備が対象
某電力会社のRFPにて、NW構築の納品前品質証明書として
脆弱性診断報告書の提出がSIに要求される（**イージスEW事例**）
- SBOMの提出
SIが構築するWEBサーバには、SBOM提出が必要
(弊社支援サービスで対応可能)



今後は、規制対象が基幹インフラ業種15分野の事業者に拡大の方向

サイバー支援事業 ～特定業種向け～

セキュリティ業務支援（特定分野・業種向け）

支援番号	支援対象事業者	支援名	支援属性	支援概要	支援時間/月
1	医療施設 (重要インフラ分野)	「医療情報システムの安全管理に関するガイドラインV6」に準じた説明とレポート作成	管理・運営・技術	医療法の規則が改定され、2023年4月1日からは「医療情報システムの安全管理に関するガイドライン」への準拠が義務付けられます。このガイドラインでは、医療機関全体が経営管理、企画管理、システム運用に関する幅広いサポートを行う必要があります。当社の支援サービスでは、プロジェクトマネージャー（PM）またはプロジェクトマネジメントオフィス（PMO）として、この評価や報告書の作成、運用のサポートを行います。	35h（週・1日）～
2	特定社会基盤事業者/ 特定社会基盤事業者からの受託 SI	構築システムの脆弱性診断・評価 レポートの作成	技術	経済安全保障推進法（令和4年法律第43号）により、令和6年5月から特定社会基盤事業者は、自社のシステムに対する脆弱性診断を行う義務が課せられます。当サポートでは、この法律で指定されたシステム脆弱性診断を行い、お客様の要望に応じて以下のサービスを提供します。	35h（週・1日）～
				・特定社会基盤事業者へのシステム納品前の、システム脆弱性診断と報告書の作成	
				・特定社会基盤事業者の、インターネット上のドメインに対するシステム脆弱性診断と報告書の作成	
3		Web構築システムのSBOM制作	技術	特定社会基盤事業者が個人情報を扱うシステムに独自のWebサーバーを構築する場合、SBOM（Software Bill of Materials）の提出が求められる場合があります。当支援では、該当するWebシステムに対するSBOM作成サービスを提供します。	35h（週・1日）～
4	重要インフラ業種/事業者 (含む特定社会基盤事業者)	NIST SP800-171を用いたサイバーセキュリティ業務のチェックと対策	管理・運営	NIST SP800-171は、ISMSの内容を基にしたサイバーセキュリティ業務を定義した規定です。当支援では、お客様の環境に合わせてSP800-171をカスタマイズし、実施してまいります。さらに、この業務を効率的に進めるために、複数のツール（CIS Controls、各種ガイドラインなど）も併用して実施いたします。 特に、NISCや経済産業省からの要望が注目されており、最近では特定社会基盤事業者が経済安全保障推進法への対応としてこれを活用し始め、重要インフラ事業者にも影響が広がりつつあります。	35h（週・1日）～
5	重要インフラ業種/事業者 (含む特定社会基盤事業者) / インフラ機器製造メーカー / SaaS提供メーカー	「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」に準じた説明とレポート作成	技術	「2. 構築システムの脆弱性診断・評価レポートの作成」は、ネットワーク構築系およびCVE（Common Vulnerabilities and Exposures）が中心となる広範な脆弱性診断を対象としています。本手引きでは、対象ネットワークに接続される全機器の脆弱性診断手法についても言及されています。 当支援では、この手引きに基づいた脆弱性診断・評価レポートの作成に関するサポートを提供します。必要に応じて、各メーカーとの交渉も担当させていただきます。	35h（週・1日）～

サイバー支援事業 ～一般業種向け～

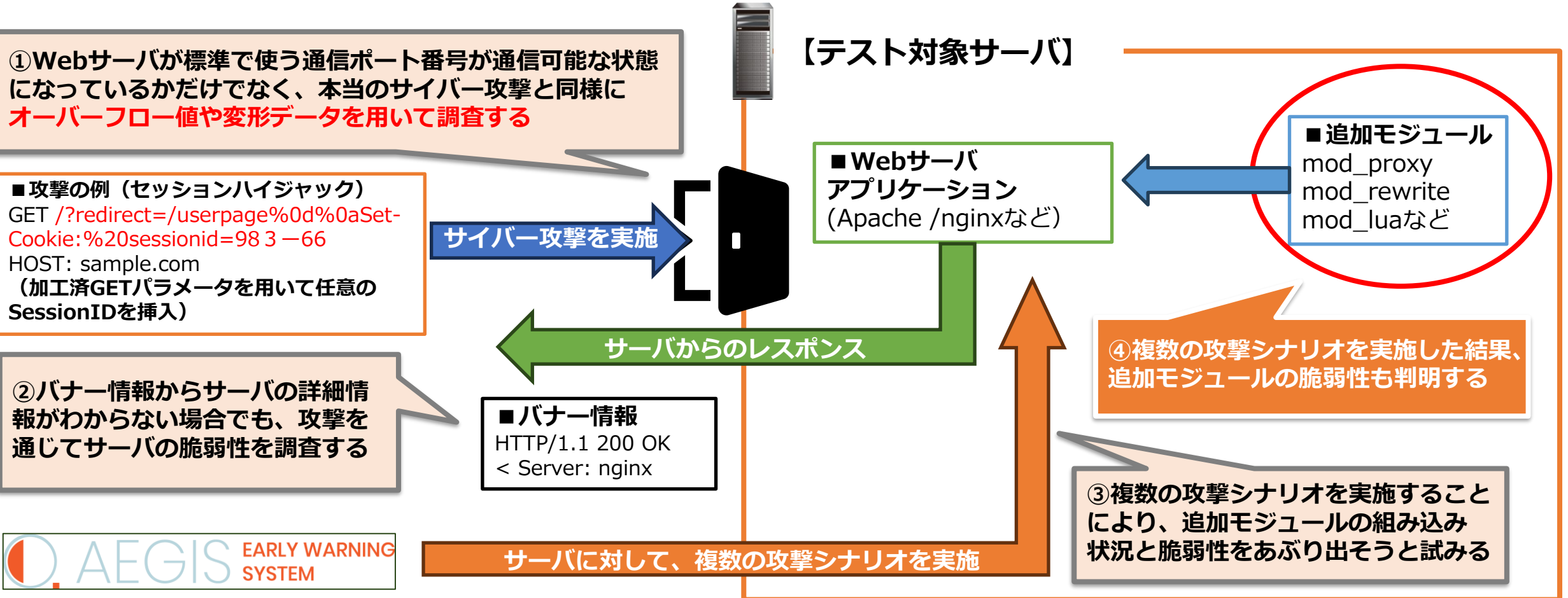
セキュリティ業務支援（一般向け）

支援番号	支援対象事業者	支援名	支援属性	支援概要	支援時間/月
6	一般企業・団体 【含む、公共施設（県庁・市町村、病院、学校、等々）】	サイバーセキュリティ業務支援	管理・運営	新規・既存のサイバーセキュリティ業務の立ち上げや改善、運用に関する支援サービスを提供いたします。	35h（週・1日）～
				・サイバー対策チームの設立支援や社内の稟議書の作成	
				・サイバーセキュリティ関連部門の業務定義書の作成	
				・CSIRT（Computer Security Incident Response Team）を含む関連部門の運用支援	
				・関連部門や社内向けのサイバーセキュリティ訓練の実施 など	
7		サイバーセキュリティ経営ガイドラインV3でのチェックと対処	管理・運営	本ガイドラインのチェックシートなどを活用し、関連部署間の連携が正常に機能し、サイバー攻撃に対応できているかを診断し、その結果に基づいて改善や運用の支援を行います。	35h（週・1日）～
8		サイバー攻撃からのシステム防御	技術	サイバー攻撃に備え、システム全体のセキュリティ対策を強化し、防御力を高めます。	35h（週・1日）～
				・インターネット側とイントラ側の脆弱性診断（ASM・ペネトレーションテスト）の実施	
				・各工程での対策業務の実施	
				・診断結果からの防御対策の優先タスクリストの作成	
				・各工程での対策業務	
		インシデント発生時の対処	管理・運営	マルウェアに感染し、ランサムウェアの攻撃を受け金銭要求を受けているなど、緊急を要する対策支援	要相談
9				・神奈川、東京、さいたま、千葉などへの現地訪問による対処作業	
				・遠隔地の場合、弊社よりリモート・トリアージキット（SIM付Wi-Fiルータ+Edge-BOX）を郵送し、お客様先に設置いただく事で、データ分析・対処作業を行います	

■脆弱性診断では、具体的に何を見ているのか？(1)

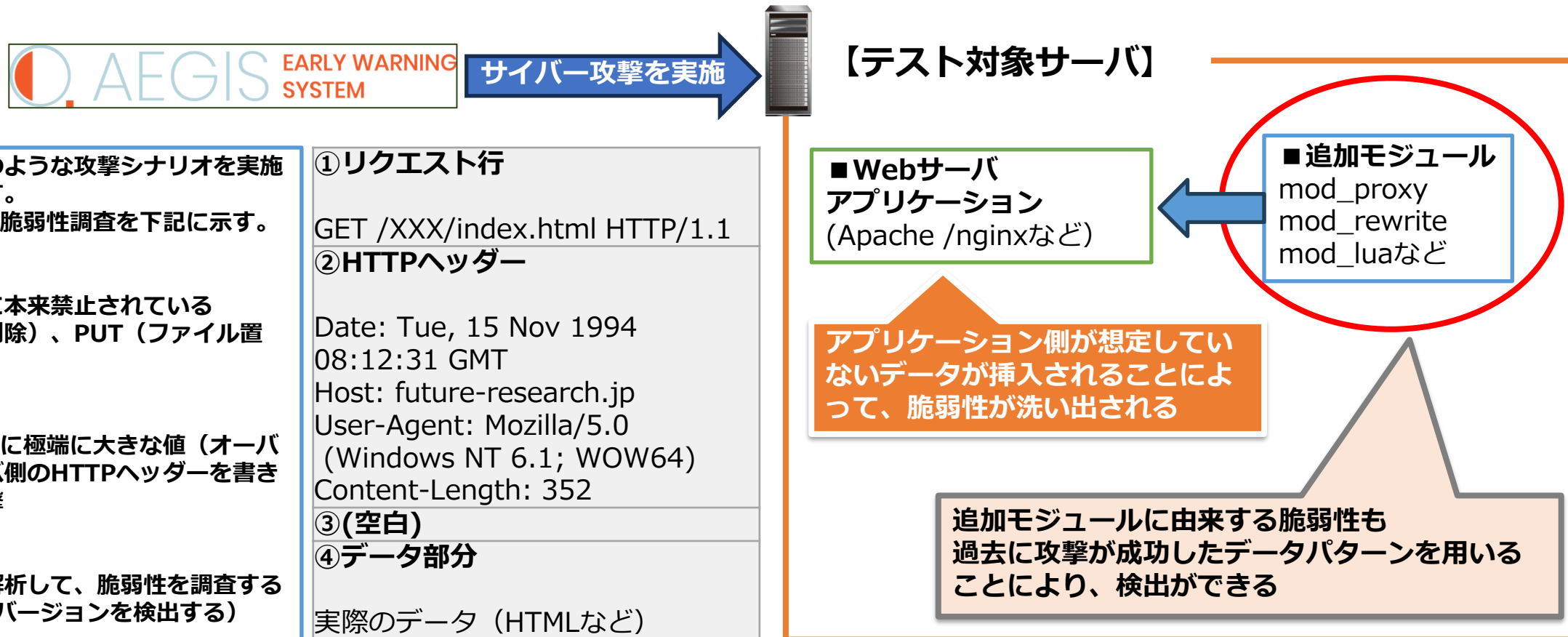
脆弱性診断は、実際のサイバー攻撃を安全な範囲で行います。

このため、ASMより深い範囲で脆弱性診断を行います。



■脆弱性診断では、具体的に何を見ているのか？(2)

脆弱性診断では、「データ部分とヘッダ部の両方を用いて攻撃シナリオを実施」します。
これにより、ASMでは検出することができない脆弱性を調査可能です。



■ASMと脆弱性診断の比較

なぜ、脆弱性診断を行う必要があるのか？
理由は、「ASMだけではわからないことがある」ためです。
【ASMと脆弱性診断の違い】

項目	ASM (Attack Surface Management)	脆弱性診断
診断の目的	<ul style="list-style-type: none">・ 外部攻撃に対する表面的な脆弱性を可視化し、早期に対応可能な問題をリスト化する・ リスク評価の補助	<ul style="list-style-type: none">・ 内部・外部攻撃を含めた本番環境での攻撃リスクを詳細に調査し、実際に悪用されるシナリオを想定
対象とするシステム	本番、ステージングいずれでも実施可能（影響が極めて少ない）	ステージング環境で実施。ステージングが無ければ本番で実施
診断の深度	「浅い」 <ul style="list-style-type: none">・ そのポートが空いているか・ バナー読み取りは正常通信の範囲のみ ※正確な結果は表示されない。	「深い」 <ul style="list-style-type: none">・ 侵入攻撃を実際に仕掛けている・ エラー時の戻り値や攻撃成功時の挙動から脆弱性を調査する
読み取れる情報の範囲	「狭い」 <ul style="list-style-type: none">・ バージョン情報からわかる脆弱性のみ・ オプションモジュールについては、バナーでわかる場合だけ・ モジュールのバージョン検出ができる場合のみ、CVEを列挙	「広い」 <ul style="list-style-type: none">・ パスワードの強度がわかる（FTP／SSH）・ オプションのモジュールに由来する脆弱性もわかる・ 挙動からバージョンを推測・ モジュールバージョンが検出できない場合でも、ハッキングアルゴリズムを実施してCVEを洗い出す・ 本当に脆弱性を検出できた場合のみCVEを表示
実施のリスク	<ul style="list-style-type: none">・ 軽微：通常、システムのパフォーマンスにほとんど影響を与えない・ 本番環境でも安全に実施可能	<ul style="list-style-type: none">・ 中～高：本番環境での負荷や、一部サービスの停止リスクを伴う可能性・ 攻撃シミュレーションが原因でシステムの動作が不安定になる場合がある・ 事前のバックアップが必要である
コスト・時間	<ul style="list-style-type: none">・ 低：自動化ツールでの定期実施が可能・ 短時間で完了	<ul style="list-style-type: none">・ 高：専門スキルを持つテスターによる評価が必要・ 時間がかかるケースが多い

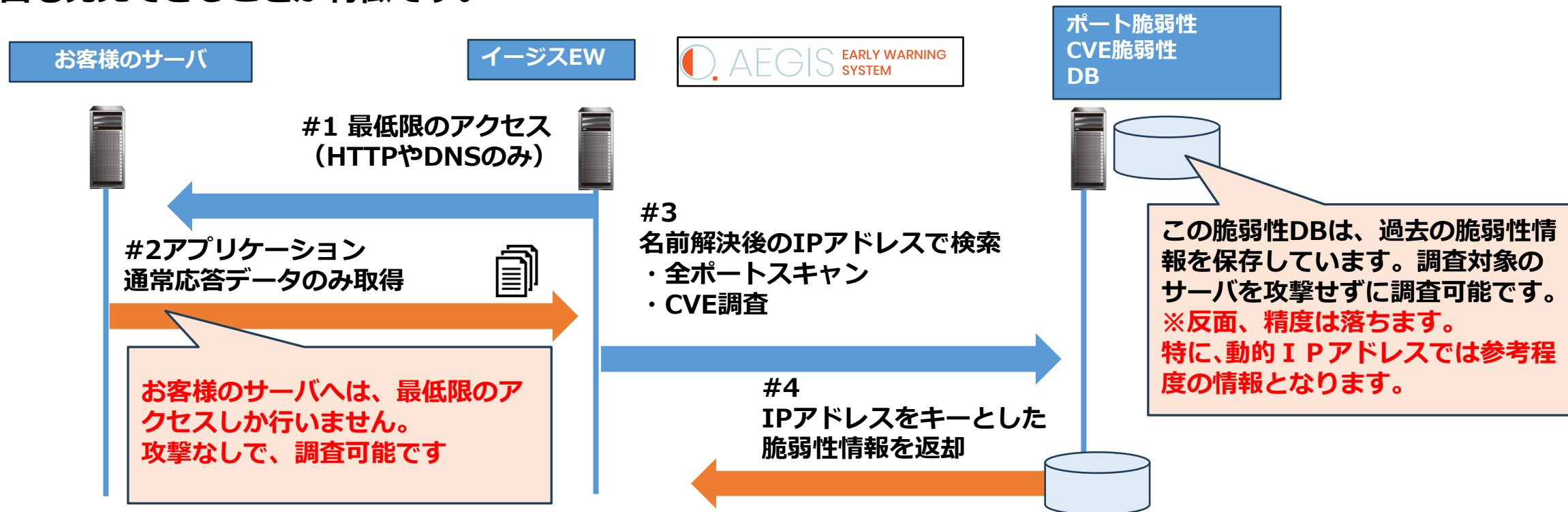
パッシブスキャンとは？（ASM注意すべき事項）

■パッシブスキャンの特徴

パッシブスキャンとは、ネットワーク上を流れるトラフィックを監視・分析することで、デバイスやサービス、資産（アセット）を自動的に検出する手法です。

アクティブスキャン（対象に直接通信を送る手法）と異なり、パッシブスキャンは非侵入型でネットワークやシステムに負荷をかけず、主にセンサーやログ解析によって資産情報や脆弱性を把握します。

このため、野良IPやゾンビ端末、忘れられたサブドメインなど、アクティブスキャンでは見落としがちな攻撃面も発見できることが特徴です。



■ イージスEW・ASM（パッシブスキャン）『3.2.4 注意すべき事項（ASM導入ガイドンス）』

- イージスEWは、ASM導入ガイドンスが言う、検索エンジン型とオンアクセス型が、診断分野により異なります

①検索エンジン型： PORT分野・CVE分野

②オンアクセス型： MAIL分野・BREACH（漏洩）分野・WEB CERT分野・HEADER分野・野良端末検出

■ ASM（パッシブスキャン）が検索エンジンを使う理由

- オンデマンド診断は負荷が大きい

サーバが稼働中にポートや CVE の検査パケットを大量に送ると、CPU や帯域を奪い、利用中のユーザに影響を与える恐れがあります

- アクセスが負荷が多くなるPORT診断・CVE診断では、外部DBを参照

負荷をかけないパッシブ方式では、定期的にトラフィックをキャプチャしている外部データベース（多くは IP アドレスまでの L3 情報）を利用します

- 動的 IP 環境では情報がずれる場合がある

パブリッククラウド上で動作するアプリで IP アドレスが変わる仕様では、外部DBに未だPORT分野・CVE分野の最新情報が反映されてない場合があります。このケースでは 能動的な脆弱性診断（Active Scan）を強く推奨します

■ イージスEWによる脆弱性診断（ActiveScan）

- PORT分野・CVE分野も含めすべてオンアクセス方式の該当端末群へのリアルタイムアクセスで行います。そのため、診断日時の事前調整と、イージスEWが通過できる固定IPアドレスの許可設定が必要になる場合があります
- サブドメインが多数ある場合は、対象をグループ分けし、段階的に脆弱性診断を実施することも可能です