未来研究所
Future Research Inc.

令和７年９月１日　総務省より
「フィッシングメール対策の強化について（要請）」
（総基用第76号）

～　フィッシングメール対策・無料診断のご案内　～

TELESA
情報・通信をビジネスに活かし日本を発展させる企業が集う
一般社団法人 テレコムサービス協会

2025年11月20日
株式会社　未来研究所

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。

AEGIS EARLY WARNING SYSTEM

目次

- （株）未来研究所　会社案内
- フィッシングメール被害状況
- フィッシングメールとは？　対策とは？
- 総務省「フィッシングメール対策の強化に関する要請」について
- テレサ協での対策実施と、報告フローの説明
- フィッシングメール対策ツール、イージスEWご紹介
- 未来研究所からの報告書
- 今後のスケジュール
- 補足資料群

未来研究所　会社概要

未来研究所
Future Research Inc.

■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目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
- ●**所属団体　社団）テレコムサービス協会・北陸支部**
- ●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　事業概要

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

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）

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ー分野
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

米国　CTO
Dick Willson

ICT支援員

ギグワーカー/副業希望者

地域の提携SIer

弊社代表紹介

未来研究所
Future Research Inc.

小林　忍（こばやし　しのぶ）

㈱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、外資企業、起業、会社譲渡を経、現職】

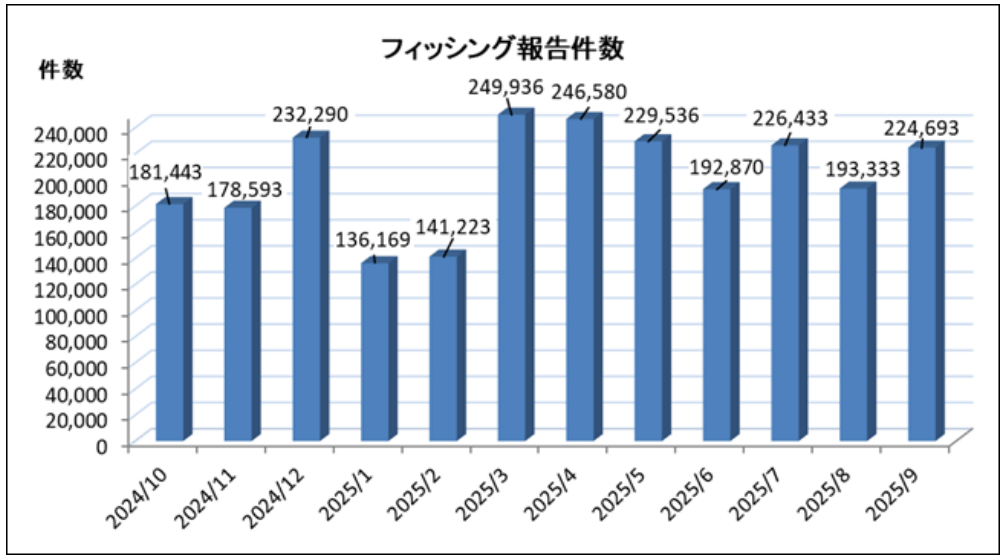
【代表的な事業化】
＊オセアニア政府群にて使用されている脆弱性診断・AEGIS-EWを、独占販売権にて日本市場に展開開始（2023/4～）
＊サイバーセキュリティ研修コース・設計・制作・講師実施。　大手・中堅企業でのCSIRT新設から運用迄のコンサルティング
＊サイバーセキュリティ分野でISACA　CSX（クラウド上でインシデント・シナリオ対応を実践学習できるeラーニング）を世界で初めて代理店契約を締結し日本で販売中
＊Extreme（L3 S/W）社の世界で4番目のOEMを締結し、アライドテレシスのS/W事業の基礎を構築
＊日本で初めてNetscapeを販売
等があり、主に海外商材・ソリュー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
＊㈱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む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 ー　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、人財派遣・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
＊大手電気メーカでのプログラマーを経、外資LSIメーカでの通信ボードの製造、アライドテレシス㈱でのNetScape日本販売を手掛ける

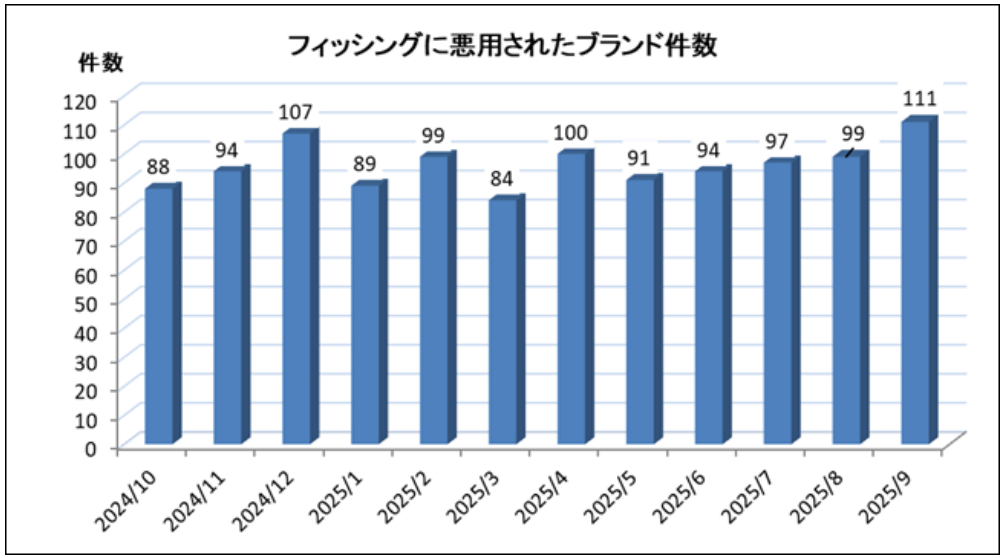
フィッシングメール被害状況

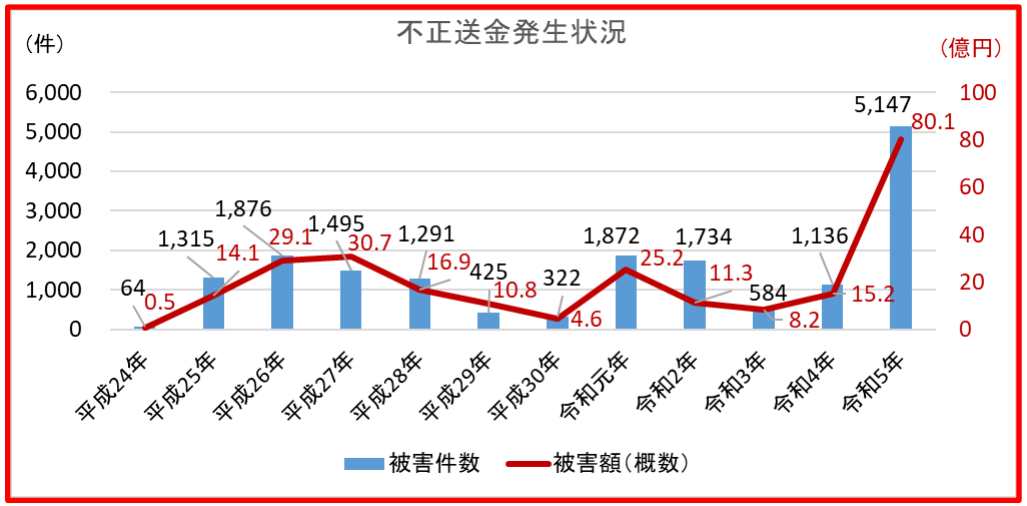
■フィッシングメール（なりすましメール）の被害



※2025年
約２４０万件/年

データリソース：
フィッシング対策協議会：
「報告窓口に寄せられた報告」





データリソース：金融庁

【フィッシングによるインターネット・バンキングの不正送金被害】
2023年　８０．１億円
2024年,2025年　急増中

※マスメディアによる報道（読売新聞）
フィッシングメール詐欺急増、総務省が業界に対策強化を要請…生成ＡＩで自然な日本語容易に：読売新聞

「なりすましメール（フィッシングメール）」とは？

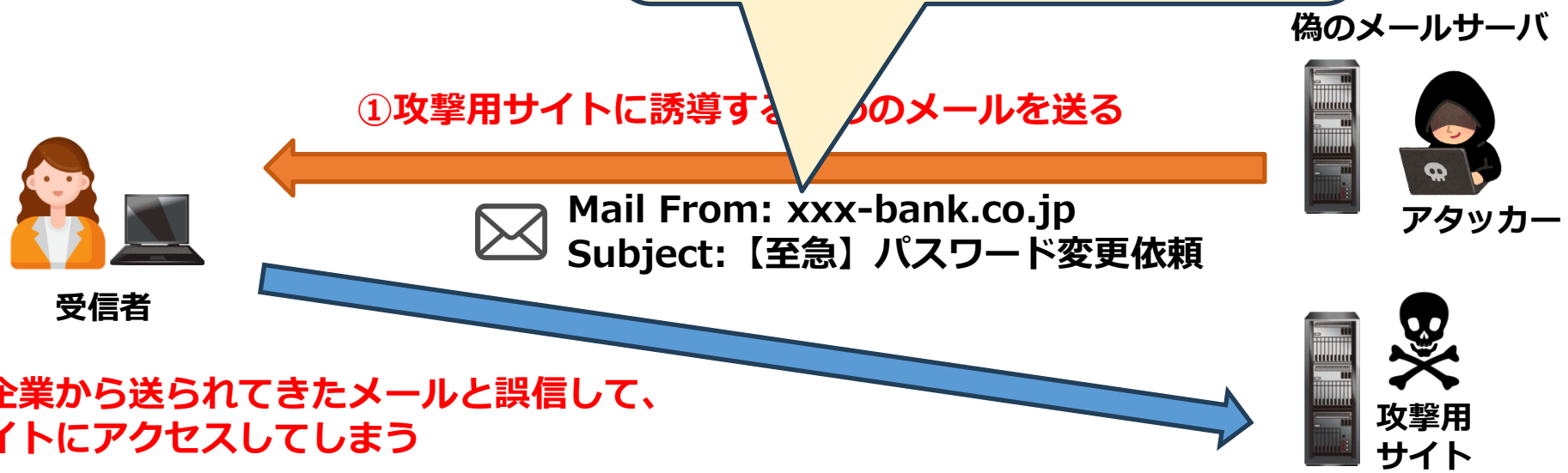
未来研究所
Future Research Inc.

■ 「なりすましメール」とは

「なりすましメール」とは、悪意ある攻撃者（アタッカー）が、実在している企業等を騙って送信するEメールを指します。

「なりすましメール」を誤信した受信者に、[redacted]させることによって攻撃用サイトへ誘導し、ユーザアカウントや個人情[redacted]

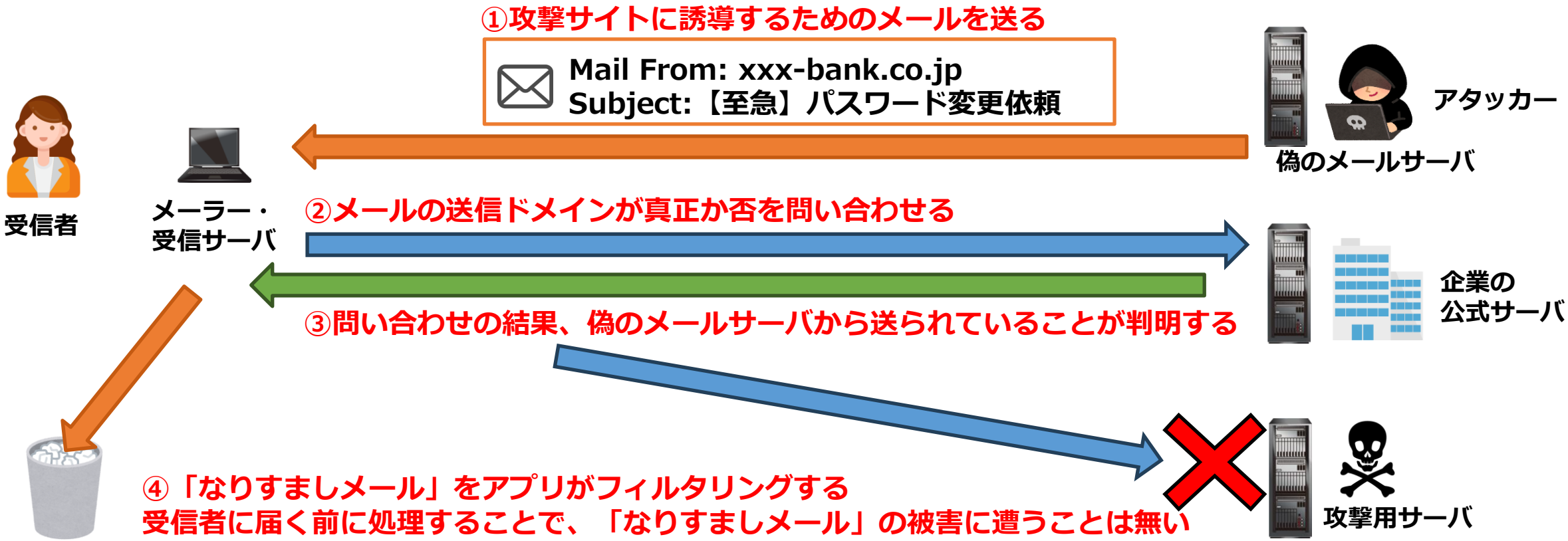
誰でも簡単に、送信メールアドレス（テキスト）を、変更することができる
MTA（Postfix / Sendmail / Eximなど）の設定（AIでの自動化も可能）



なりすましメール対策「送信ドメイン認証」

■ 「送信ドメイン認証」とは

「なりすましメール」は、「本当にそのメールが正規の送信元から送られてきたものかどうか」を確認できれば防ぐことができます。なりすましメールを防ぐための一連の仕組みが「送信ドメイン認証」です。
なりすましされている企業のサーバに対して、受信側が「IPアドレス認証」や「電子署名」を用いて、「真正なメール」かどうかを問い合わせ、「なりすましメール」を識別し、処理します。



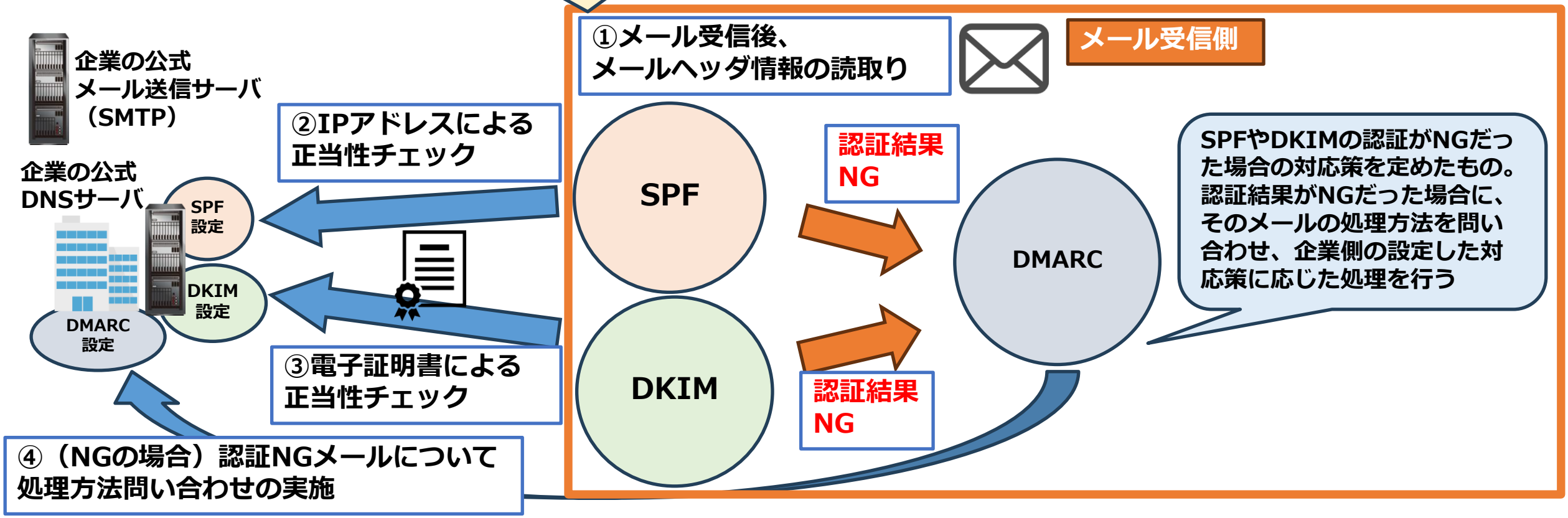
送信ドメイン認証の３技術　SPF・DKIM・DMARC

未来研究所
Future Research Inc.

■ 送信ドメイン認証の３技術

送信ドメイン
術によって構成されています。
これらは、企
へあらかじめ設定しておく必要があります。認証動作は、全て受信者
側のメール受
３技術の概要は以下の通りです。

必要なのは、簡単な設定変更のみ！
（DMARCがサポートされたメール
システムの使用が大前提）



総務省「フィッシングメール対策の強化に関する要請」

未来研究所 Future Research Inc.

■ 総務省：フィッシングメール対策の強化について（要請）

総務省からの告知案内
フィッシングメール（Mailなりすまし）対策についての調査予告（2025.9.1)

●対象団体

- 一般社団法人電気通信事業者協会
- 一般社団法人テレコムサービス協会
- 一般社団法人日本インターネットプロバイダー協会
- 一般社団法人日本ケーブルテレビ連盟

※『**要請**』の法的意味と、本要請の強制力について
要請とは、**行政手続法（平成５年法律第88号）第２条第６号に規定する行政指導**に該当するものです。
法的拘束はありませんが、行政活動の一環として公式に位置づけられており、従うことが社会的・実務的に強く期待されます。
本要請は、**総務省Webページのみならずマスメディアにより同日報道**されたことからも、**総務省の強い意向**が推測されます。
今後、**フィッシングメール対策の強化は、強制力を伴う方向へ進展する可能性があります**。

マスメディアによる報道（読売新聞）フィッシングメール詐欺急増、総務省が業界に対策強化を要請…生成ＡＩで自然な日本語容易に：読売新聞

要請内容と、取組むべきフィッシングメール対策（抜粋）

未来研究所 Future Research Inc.

■対象４団体への要請内容

令和７年９月から令和８年８月末までの間における各法人会員事業者の取組状況をフォローアップし、３か月ごとの期間の取組状況を、当該期間の末日から１月以内に総務省宛てに報告

■各団体の会員事業者が取組むべきフィッシングメール対策

（１）フィルタリングの判定技術の向上や迷惑メール判定におけるAIの活用等、メールのフィルタリングの精度の一層の向上を積極的に図ること。
また、迷惑メールのフィルタリング強度を適切に設定するなどして、高度化するフィッシングメールに対応可能なメールフィルタリングを目指すこと。

（２）なりすましメール対策として有効なDMARCの導入やDMARCポリシーの設定（隔離、拒否）を行うこと。送信側だけでなく受信側についても、適切なDMARCポリシーに基づく処理やレポート送信を設定すること。また、ドメインレピュテーション、BIMI、踏み台送信対策等の更なる対策の導入を積極的に検討していくこと。

（３）提供しているフィッシングメール対策サービスについて、様々な利用者層に向けた一層の周知・啓発を行うこと。

具体的に実施すべきフィッシングメール対策

未来研究所 Future Research Inc.

■各団体の会員事業者が実施すべき具体的なフィッシングメール対策

（１）フィルタリングの判定技術の向上や迷惑メール判定におけるAIの活用等、メールのフィルタリングの精度の一層の向上を積極的に図ること。

→**（対象：メールサービス・プロバイダー）**
メールサービスを提供している事業者は、自社フィルタリングの向上を図る必要あり
また、迷惑メールのフィルタリング強度を適切に設定するなどして、高度化するフィッシングメールに対応可能なメールフィルタリングを目指すこと。

→**（対象：全会員）フィルタリングや迷惑メール判定は、メーラー会社（MS Outlook、Gmail等）の提供済サービスを導入**
https://www.dekyo.or.jp/soudan/contents/auth/index.html

（２）なりすましメール対策として有効なDMARCの導入やDMARCポリシーの設定（隔離、拒否）を行うこと。送信側だけでなく受信側についても、適切なDMARCポリシーに基づく処理やレポート送信を設定すること。また、ドメインレピュテーション、BIMI、踏み台送信対策等の更なる対策の導入を積極的に検討していくこと。

→ **（対象：全会員）プラットフォーム脆弱性診断ツール（例：イージスＥＷ）により、DMARC等のメールなりすまし対策が実施されているかを診断し、不足している設定を導入する**
メールサービスを提供している事業者は、エンドユーザへなりすまし対策の診断を提供する

（３）提供しているフィッシングメール対策サービスについて、様々な利用者層に向けた一層の周知・啓発を行うこと。

→ **（対象：メールサービス・プロバイダー）自社で実施した（１）（２）の対策を周知するとともに、市販のフィッシングメール訓練ツールを利用した不正ファイルをクリックしない等の訓練の提供による啓発などを行う**

今回の、「無料フィッシングメール対策・診断サービス」

未来研究所
Future Research Inc.

■なりすまし対策が施されているか無料での診断を提供

未来研究所で保有している脆弱性診断ツールを利用して無料で診断いたします。

対　　象　　テレコムサービス協会　会員企業

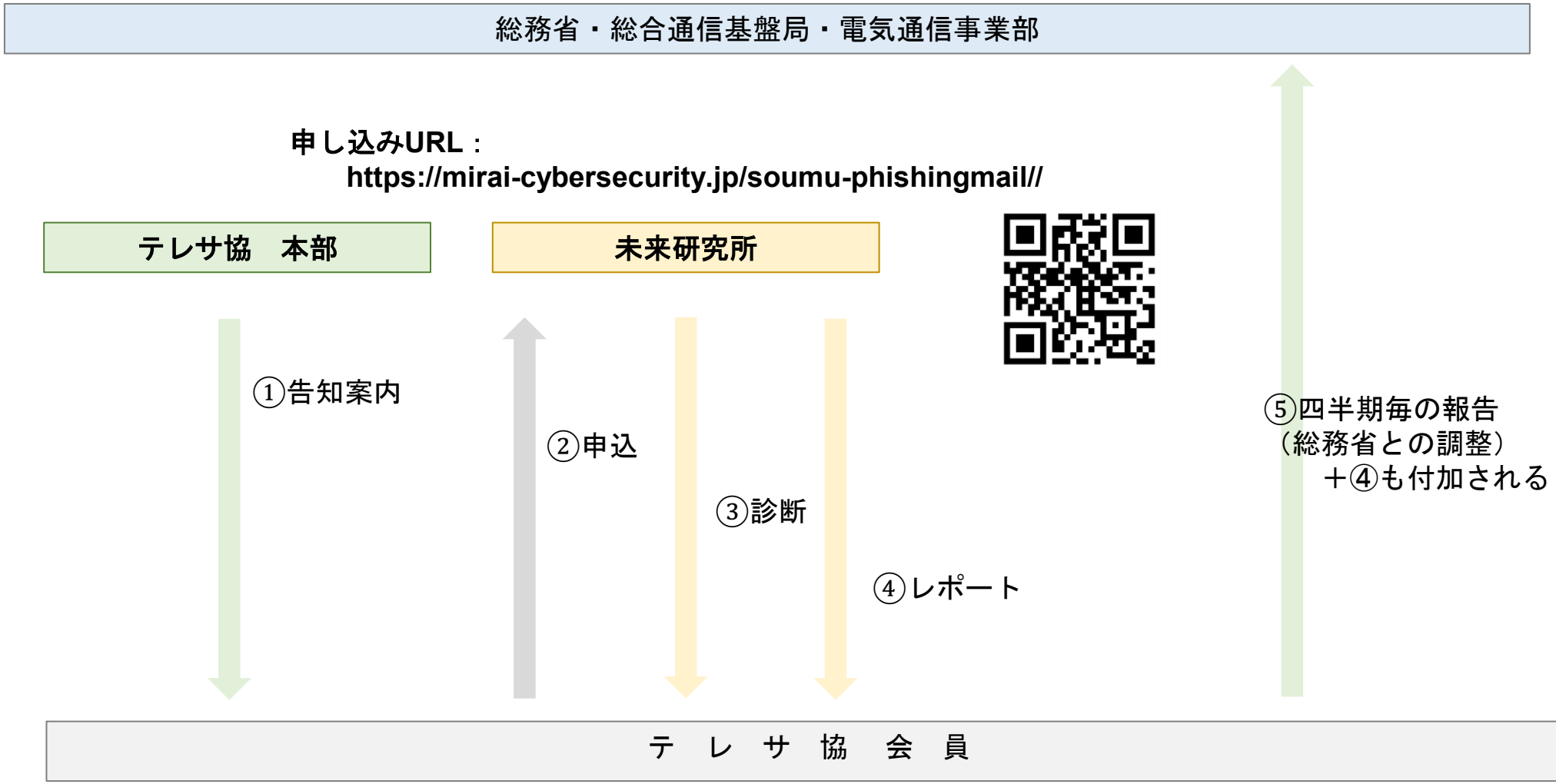
費　　用　　無料（初回のみ）

診断内容　　・「DMARC」の設定状況　（総務省からの報告要請のある メールなりすまし対策）
・「DKIM」・「SPF」の設定状況　（DMARCのための前提となる設定）
・その他、セキュリティ診断の一部（サブドメイン探索・データ侵害・HTTPヘッダ 等）

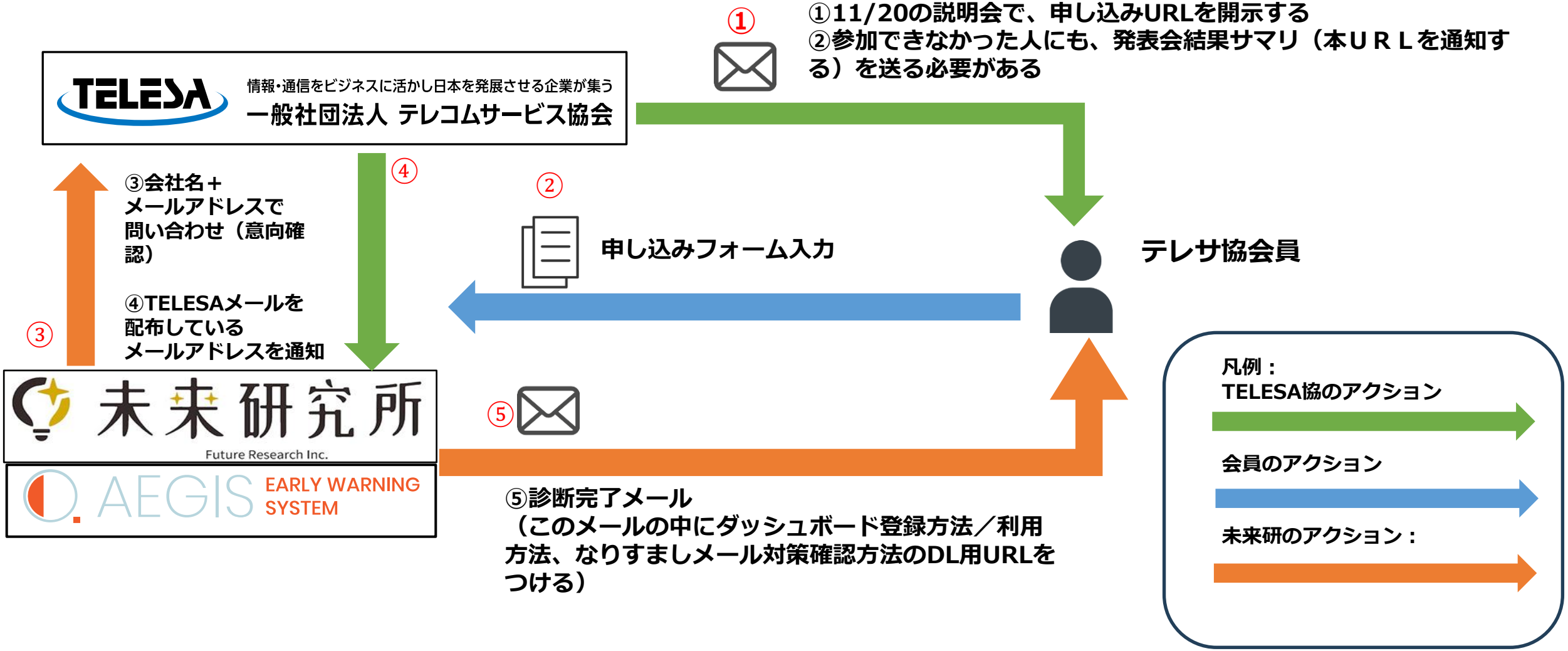
診断結果は、簡単なレポートを提出いたします。（別紙参照）

※診断結果によって、対策を希望する場合には別途応談で対応させて頂きます。

一般社団法人テレコムサービス協会での対応フロー



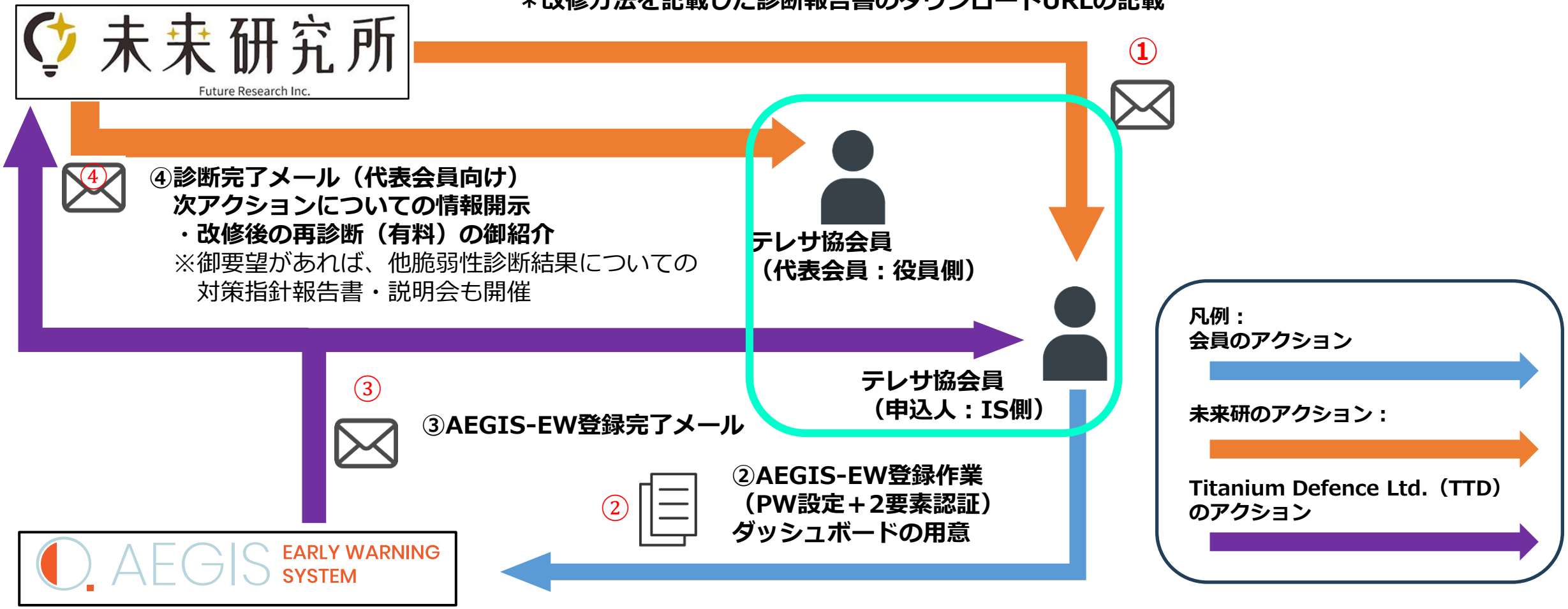
実際のフィッシングメール対策無料診断フロー



■診断後のフロー

■診断後のフロー

①診断完了メール（情報システムご担当者向け）
このメール中に、診断結果を確認し、改修するための資料をダウンロードURLを示します。
＊診断結果を確認するための、ダッシュボード登録方法／利用方法
＊改修方法を記載した診断報告書のダウンロードURLの記載



未来研究所からの提供サービス（予定）

- プラットホーム脆弱性診断ツール、イージスEWのASM診断の実施
  - 該当ドメイン（メールドメイン）での実施
  - 通常有料を1回の完全無料にて実施
- 総務省への報告フォームに準じた、「メールなりすまし対策診断結果報告書」をご提供
  - ワードファイルでお渡しします。以降、自社にてご活用してください。
  - 無料にて作成いたします
- 実際のDMARCメール改修作業について
  - 未来研究所にて、御希望があれば有料にて改修作業代行を致します
    - 有料（5万円税抜/１メールサーバ予定）、もしくは伴走サービス
- 2度目以降のイージスEW　ASM/脆弱性診断（定期がお勧め）価格について
  - テレサ協・会員様には、特別割引・10%OFFのご提供
- 総務省 総合通信基盤局への調査票制作代行サービス
  - ３万円税抜/回

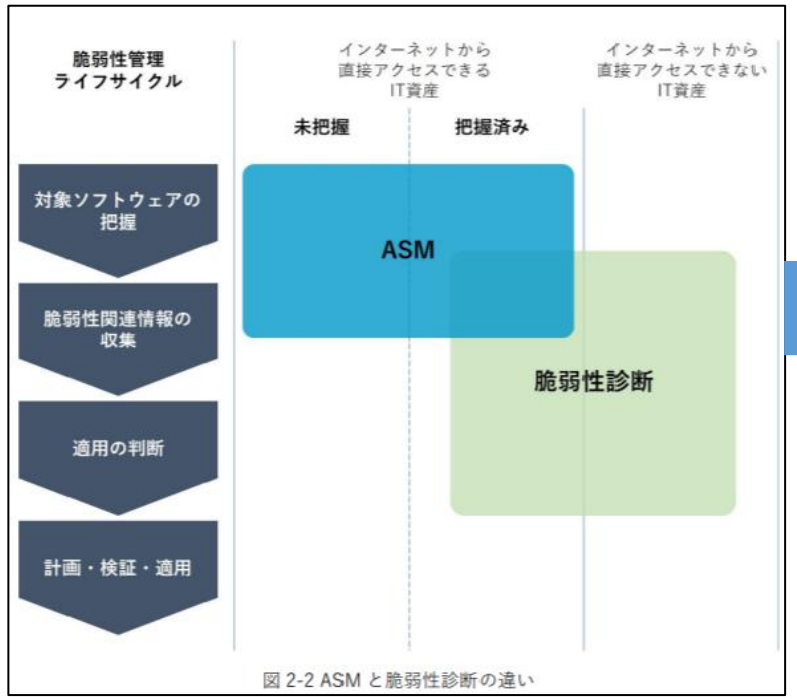
イージスEWとは？

024-0037-20

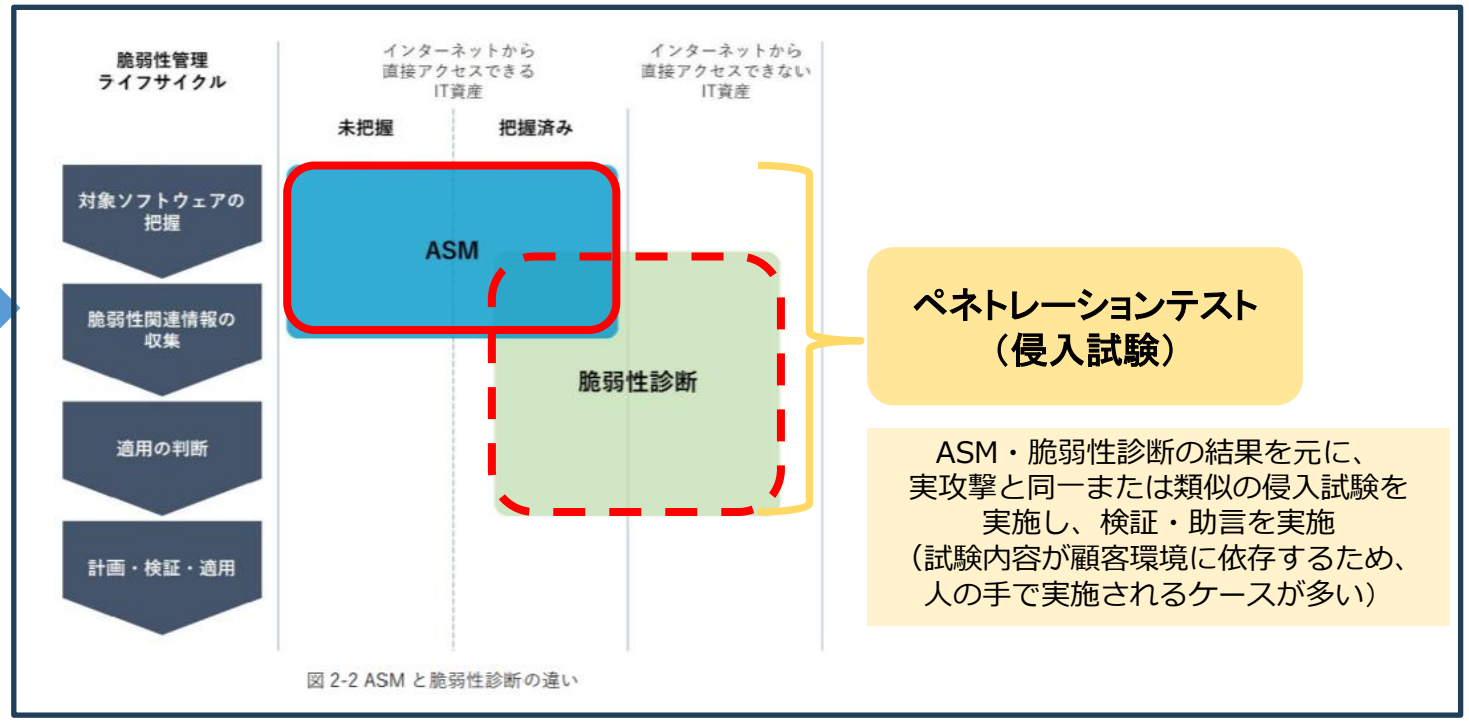
弊社のサイバーセキュリティ
脆弱性診断は、経済産業省策定の
情報セキュリティサービス基準適合
サービスに認定されております。

機器検証サービスの取得申請中

無料・フィッシングメール対策診断　＝　イージスEW ASM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）　：　完全無料で実施

■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）：　有料（会員特価）

・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）

プラットフォーム診断ツール『イージスEW』

※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』ダッシュボードの見方

■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)

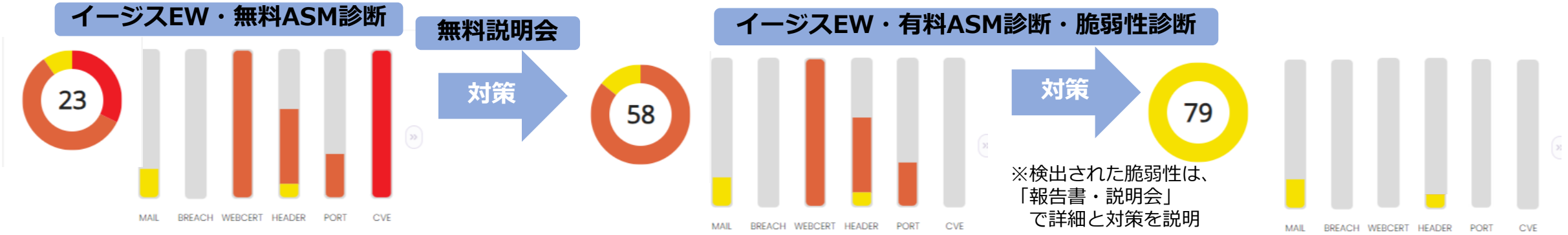
赤（緊急）・オレンジ（重要）色の脆弱性は1年目～３年目の新米SEでも乗っ取れます

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』　診断分野

未来研究所 Future Research Inc.

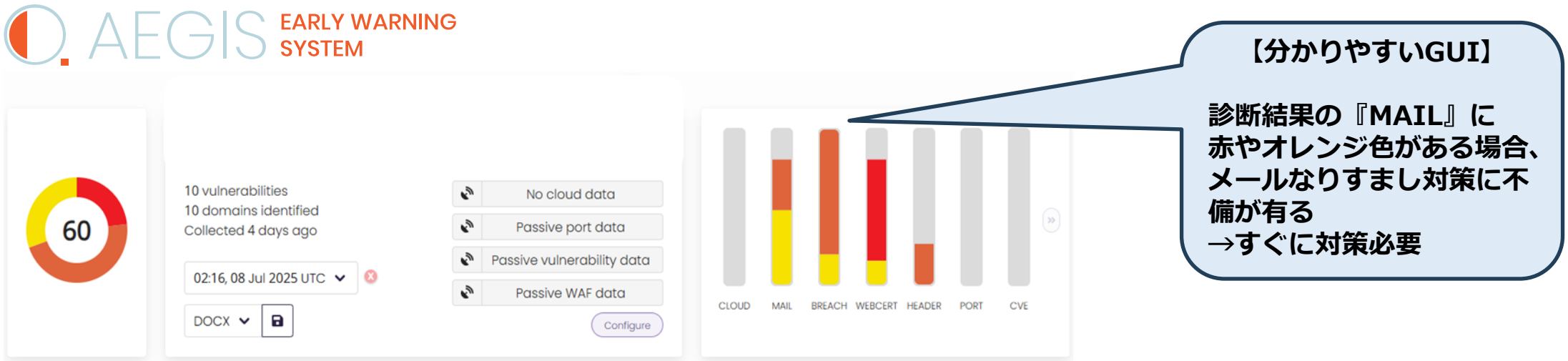
■8つの診断分野

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ものかどうか」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。 レコナイツール	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

イージスEW　DMARC・DKIM・SPFの診断例

■ イージスEW ASM診断は、本要請のフィッシングメール対策であるDMARCやDKIM・SPFの診断が可能です。赤やオレンジ色がある場合は対策必須です。



●イージスEW診断項目『MAIL』：送信ドメイン認証

送信ドメイン認証（DKIM・DMARC）とは、「受信したメールが正規の送信元から送られてきたものかどうか」を確認できる仕組みです。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DNSサーバに照会して「メールなりすまし」が行われているかどうかを判断します。イージスEWはそれらが設定されているか否かを診断します。

右図　イージスEWの報告書例：

■Mail 脆弱性（送信ドメイン認証）

Issues by category

All	Cloud	Mail	Breaches	Web certs	Headers	Ports	CVEs

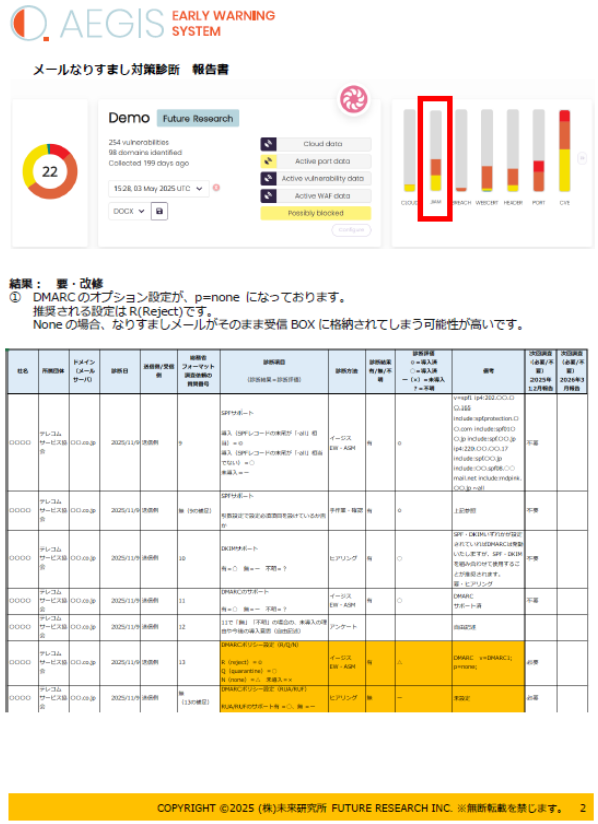
Priority	Issue	Count
High	Mail Configuration	1
	DMARC	
Medium	Mail Configuration	3

なりすましメール対策として修正箇所があります。DMARC の設定が欠落しているので、再確認をお願いします。
「SPF」の記述だけしか無く、対策としては片手落ちとなっています。
なお、具体的対策については別紙「Mail なりすまし対策」をご参照ください。

未来研究所　報告書例

未来研究所
Future Research Inc.

■未来研究所からの報告書例
・改修例も提示予定



社名	所属団体	ドメイン（メールサーバ）	診断日	送信側/受信側	総務省フォーマット調査依頼の質問番号	診断項目 （診断結果＝診断評価）	診断方法	診断結果 有/無/不明	診断評価 ◎＝導入済 ○＝導入済 －（×）＝未導入 ？＝不明	備考
○○○○	テレコムサービス協会	○○.co.jp	2025/11/9	送信側	9	SPFサポート 導入（SPFレコードの末尾が「-all」相当）＝◎ 導入（SPFレコードの末尾が「-all」相当でない）＝○ 未導入＝－	イージス EW・ASM	有	◎	v=spf1 ip4:202.○○.○○.165 include:spf.protection.○○.com include:spf01○○.jp include:spf.○○.jp ip4:220.○○.○○.17 include:spf.○○.jp include:○○.spf08.○○ mail.net include:mdpink.○○.jp ~all
○○○○	テレコムサービス協会	○○.co.jp	2025/11/9	送信側	無（9の補足）	SPFサポート 引数設定で設定必須項目を設けているか否か	手作業・確認	有	◎	上記参照
○○○○	テレコムサービス協会	○○.co.jp	2025/11/9	送信側	10	DKIMサポート 有＝○　無＝－　不明＝？	ヒアリング	有	○	SPF・DKIMいずれかが設定されていればDMARCは発動いたしますが、SPF・DKIMを組み合わせて使用することが推奨されます。 要・ヒアリング
○○○○	テレコムサービス協会	○○.co.jp	2025/11/9	送信側	11	DMARCのサポート 有＝○　無＝－　不明＝？	イージス EW・ASM	有	○	DMARC サポート済
○○○○	テレコムサービス協会	○○.co.jp	2025/11/9	送信側	12	11で「無」「不明」の場合の、未導入の理由や今後の導入意思（自由記述）	アンケート			自由記述
○○○○	テレコムサービス協会	○○.co.jp	2025/11/9	送信側	13	DMARCポリシー設定（R/Q/N） R（reject）＝◎ Q（quarantine）＝○ N（none）＝△　未導入＝×	イージス EW・ASM	有	△	DMARC　v=DMARC1; p=none;

イージスEW開発元　Titanium Defence社

■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。

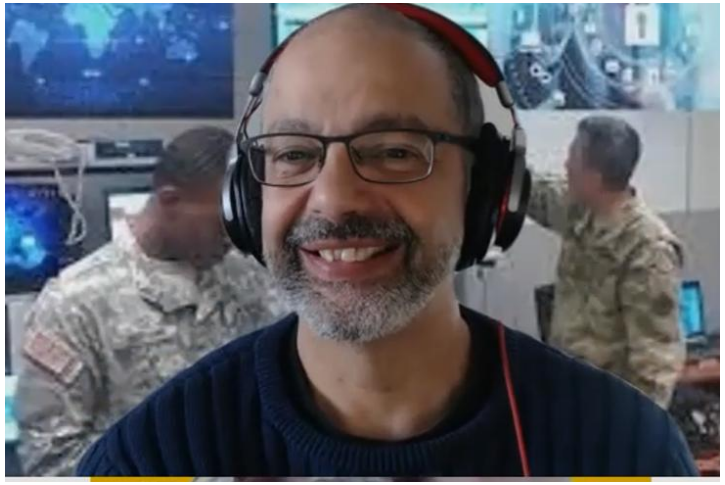
■オーストラリアがサイバーセキュリティ企業を誘致した理由

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/SB10922663126593136342045834496435786136 34
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



今後のスケジュール

スケジュール

11月5日　　テレサ協会員に一斉案内済み

11月20日（木曜日）　１３：３０－１４：３０
申し込み受付開始

12月下旬　　総務省に対する、第1回目のフィッシングメール対策・状況報告
/ アンケート調査（テレサ協・全会員対象）

【2026年】
2月　　第1回アンケートの結果報告・診断レポートの考察セミナー
（オンライン）
3月　　総務省に対する、第２回目のフィッシングメール対策・状況報告
/ アンケート調査（テレサ協・全会員対象）

Thanks

【補足】
脆弱性診断とは？　ASM（Attack Surface Management）とは？

イージスEW概要

サイバーセキュリティ脆弱性診断は、システムの健康診断

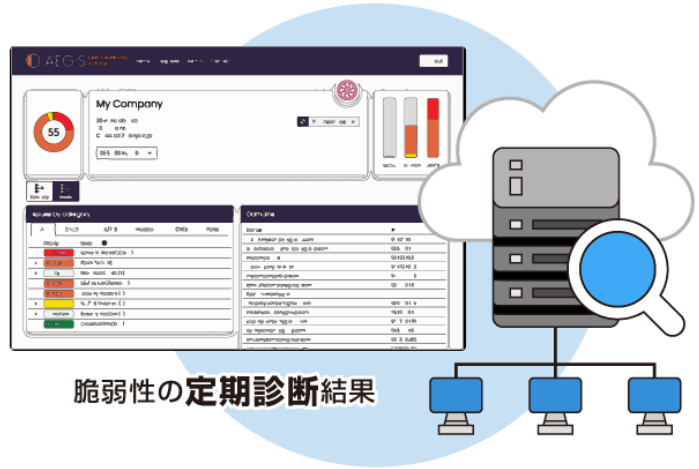
未来研究所
Future Research Inc.

■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、およびイントラ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

ハードニングの実施手順

■どのような順序で行うの？

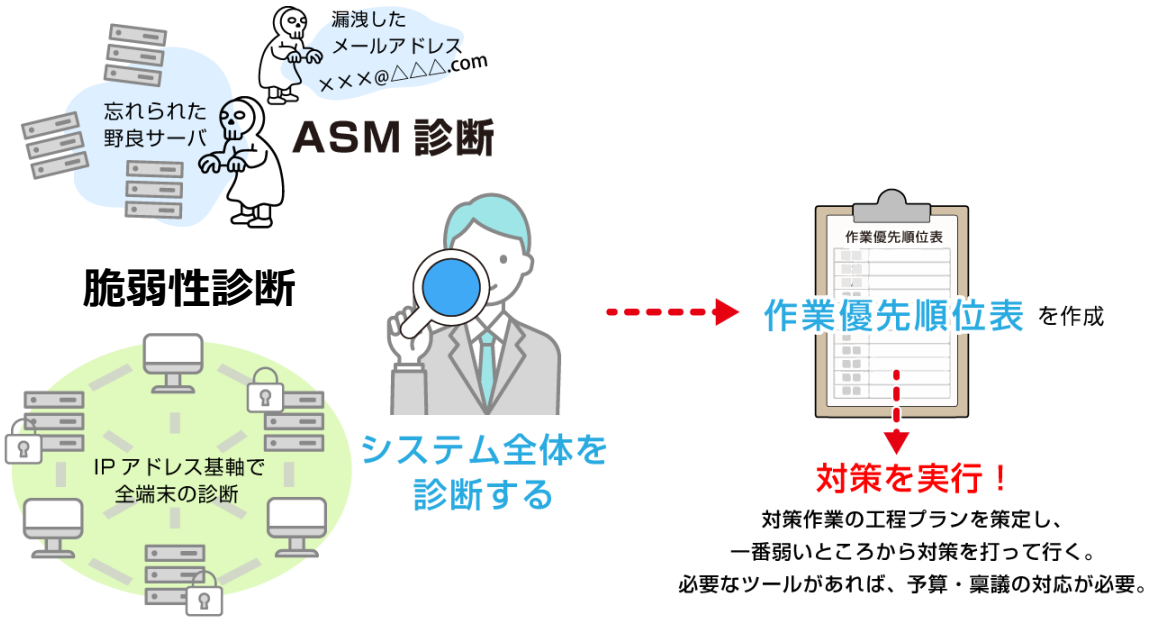
Step1　**システム全体を診断（ASM診断・脆弱性診断）**

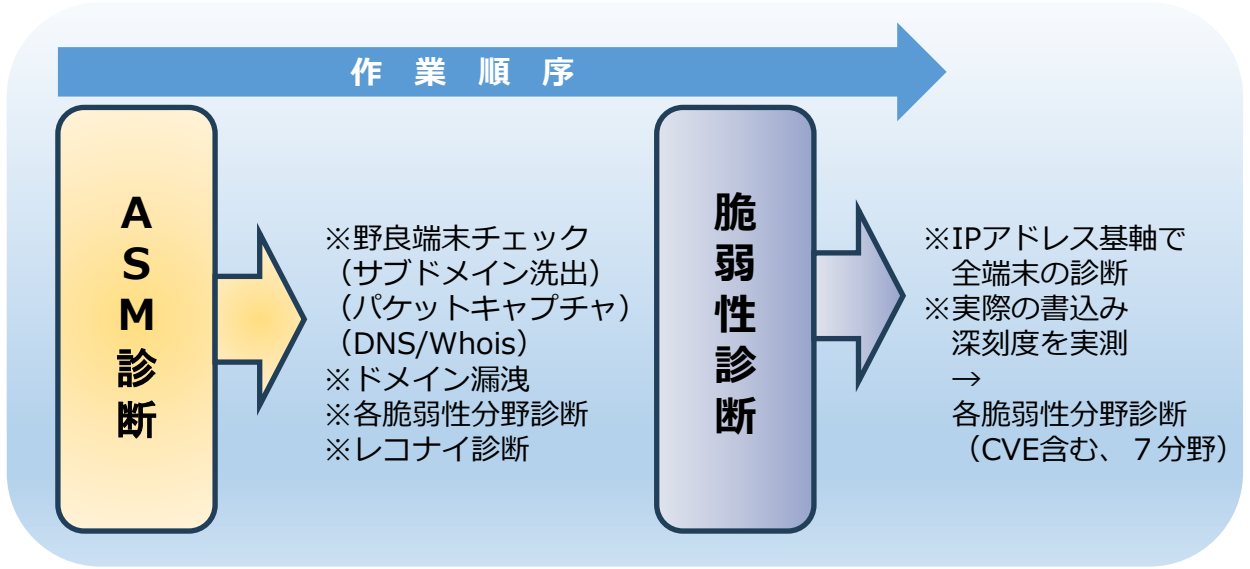
Step2　**作業優先順位表を作成（脆弱性の深刻度順）**

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とはなにか？

■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）導入ガイダンス」

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）導入ガイダンス～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

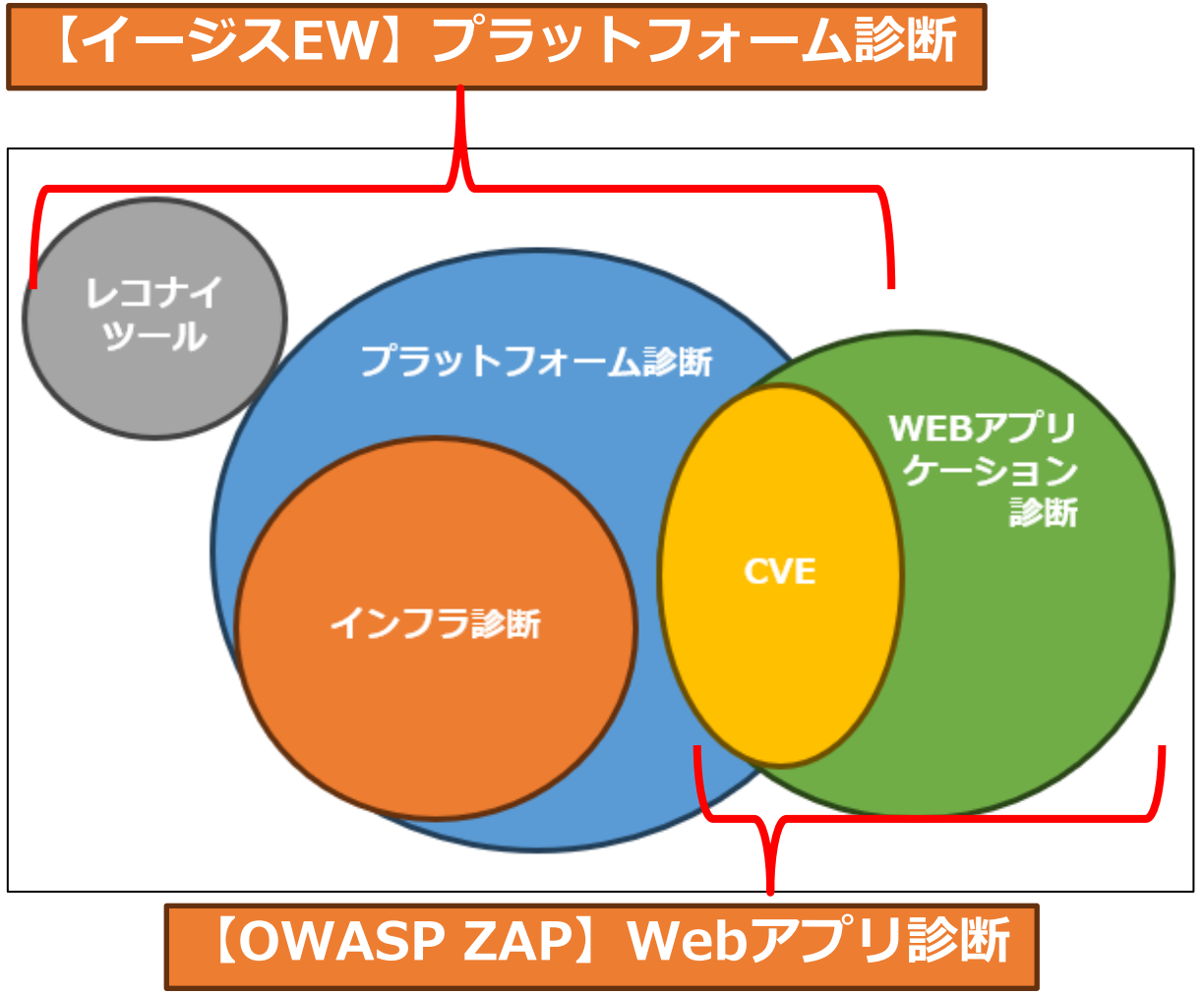
ASM診断で、ハッカーから狙われやすい脆弱性を早期に発見することが大切です

プラットフォーム診断とWebアプリ診断

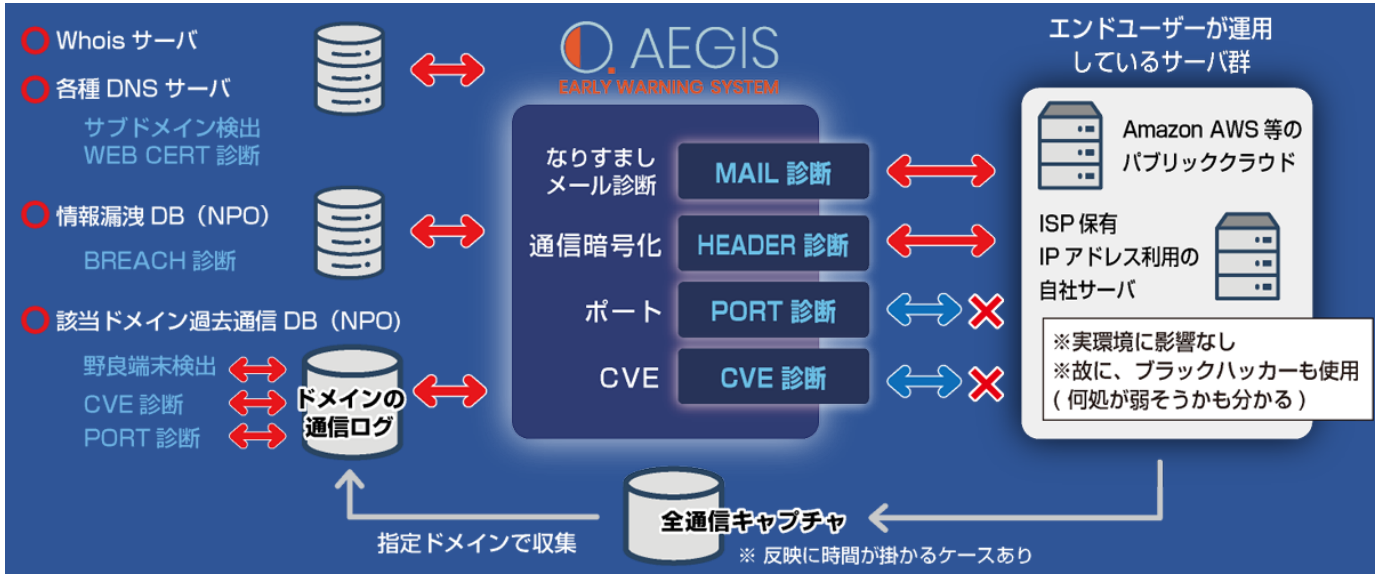
■プラットフォーム診断ツール『イージスEW』

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

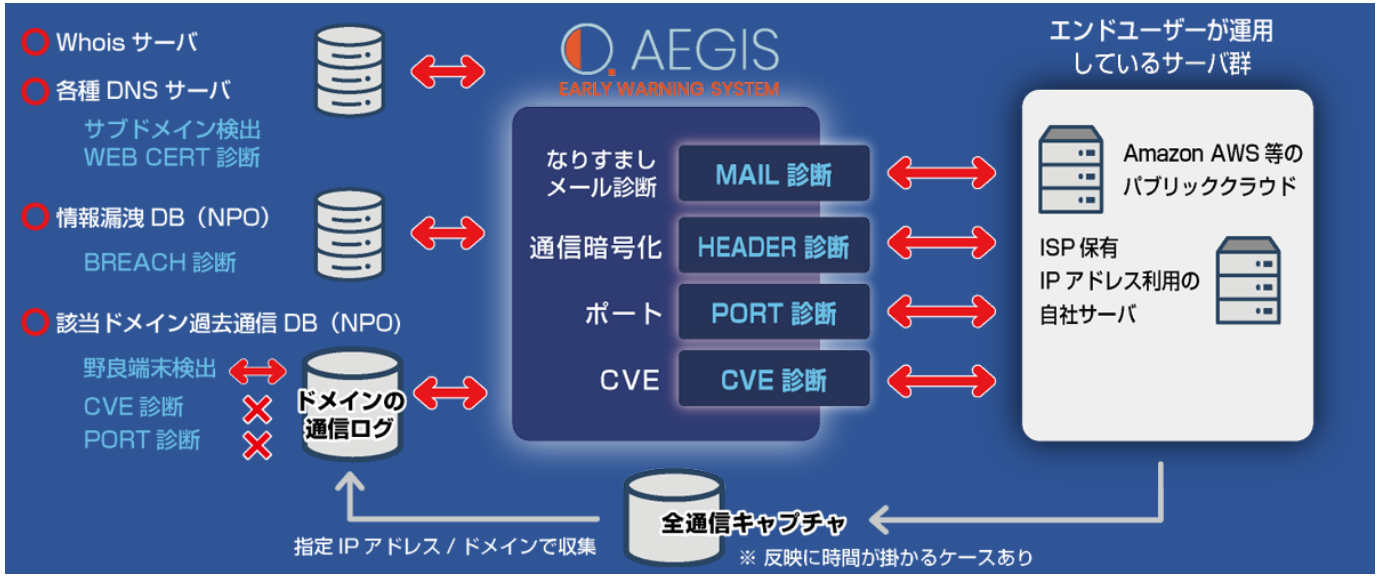
なお、Webアプリケーションにおける「コード診断」は、イージスEWでは実施しません
別ツールの「OWASP ZAP」で診断します。
例：「OWASP ZAP」にて調査する下記項目
・SQLインジェクション
・強制ブラウズ
・GETパラメータオーバーフローなど



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



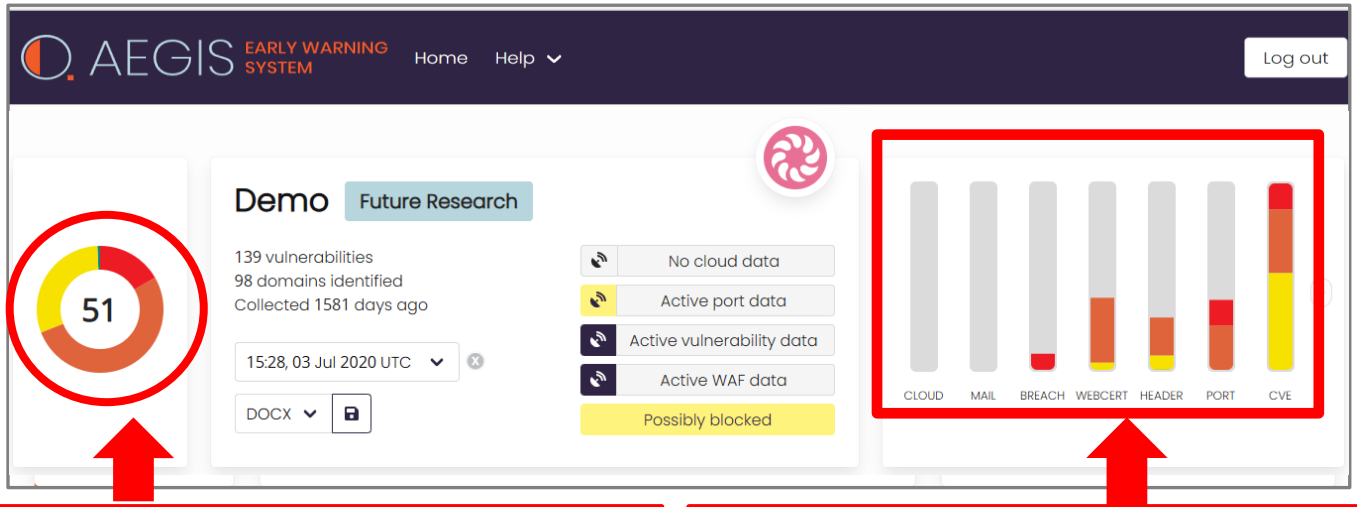
【脆弱性診断（アクティブスキャン）】
IPアドレスを基軸に、深い部分まで侵入を試み、パケットを書き込んだ結果をもとに診断します

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

見やすいGUI

■セキュリティの専門家でなくて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

『イージスEW』4つの特長

未来研究所
Future Research Inc.

ダッシュボードの見やすいGUI	強力なASMと脆弱性診断
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。	**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。
全てのプラットフォーム診断を一括管理	**リーズナブルな価格帯**
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。	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口ーコストで可能です。

リーズナブルな価格帯

未来研究所
Future Research Inc.

■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実施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

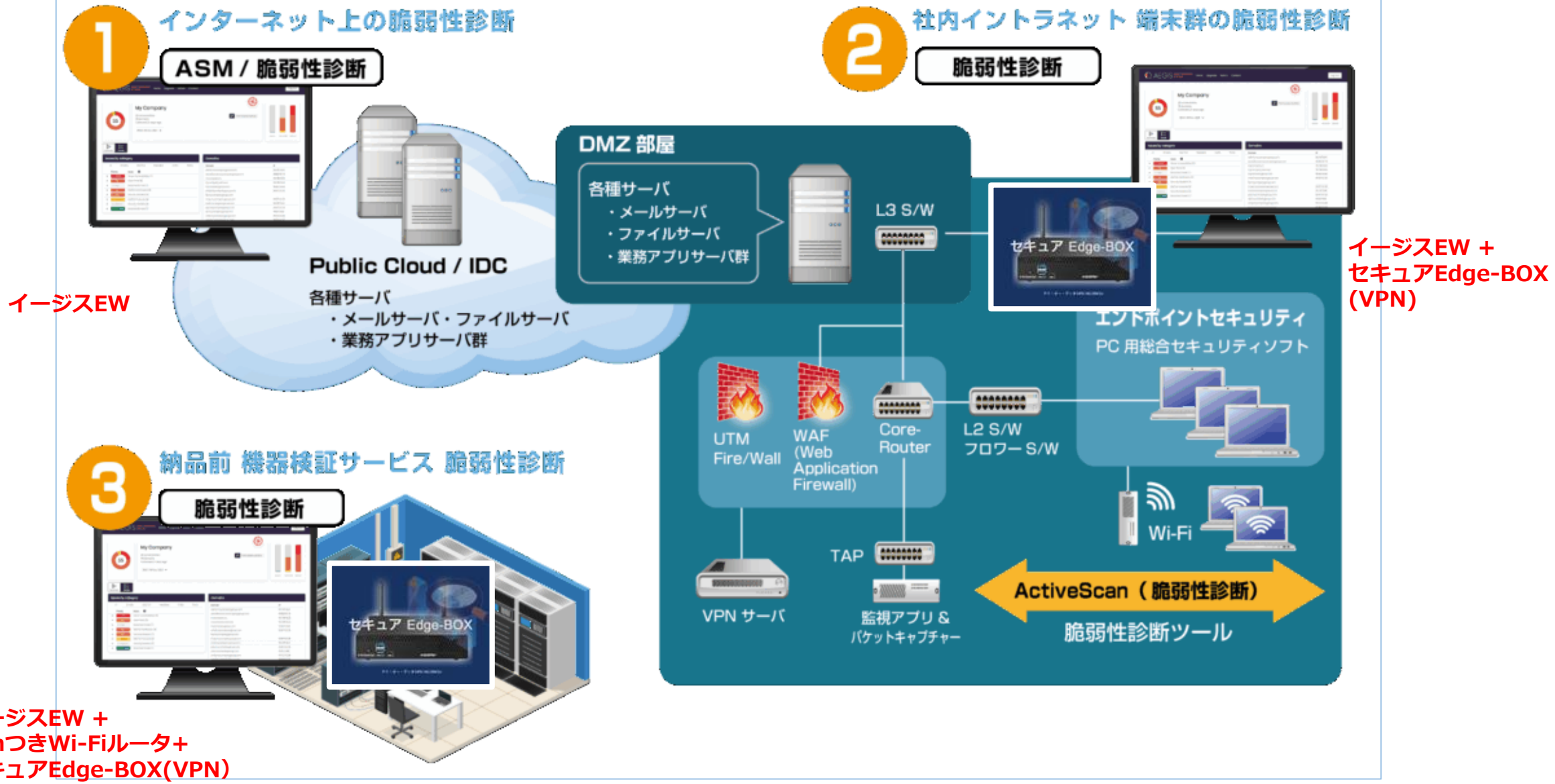
開発元のTitanium Defence社が政府系組織と連携しており政府資金の投入があることが理由です。
・イージスEW開発にあたりオーストラリア政府・ニュージランド政府の援助を受けている
・ヴィクトリア大学との産学連携である
・診断にイギリス政府系のＤＢを使用している

■日本でも多くの事例

既に500ドメインを超す実績数あり。大手携帯会社、数百の子会社を有する企業から、数十名のSaaSメーカ、Web受託会社さんでの再販等、多くの事例があります。
・数千を超すサブドメインを持つ大学群
・特定社会基盤事業者（コントロールセンターの定期診断、納品前システムの脆弱性診断・改修）
・公共施設でのＷｅｂ開発システムの検収・脆弱性診断

全てのプラットフォーム診断を一括管理

未来研究所
Future Research Inc.



イージスEWの導入フローとサービス

エンドユーザ/販売代理店・VAR の診断を一括管理

未来研究所 Future Research Inc.

■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

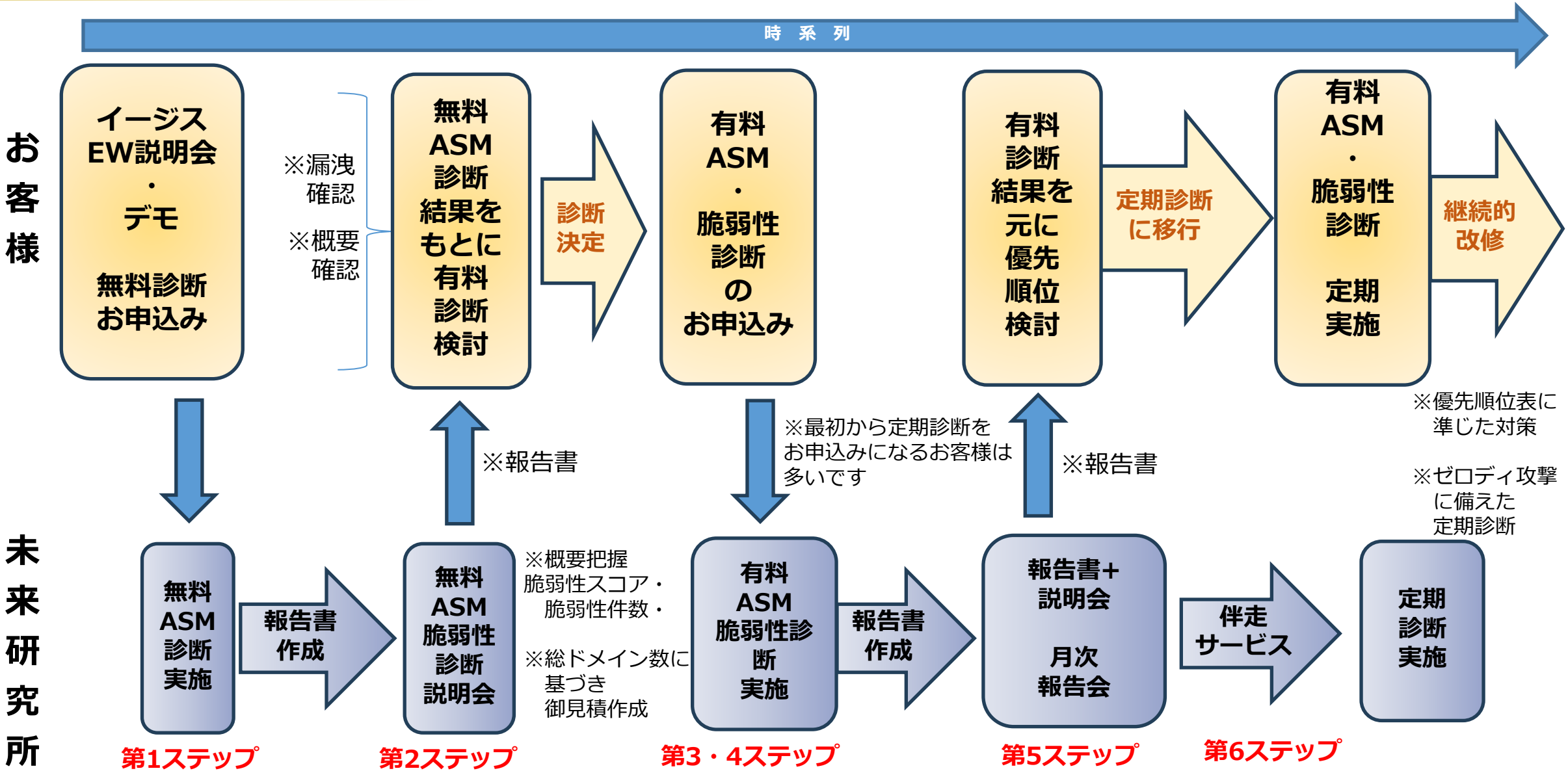
顧客の診断一括管理・
サポートが可能になります

顧客A

顧客B

顧客C

イージスEW　導入フロー



第2ステップ　無料ASM脆弱性診断　無料説明会

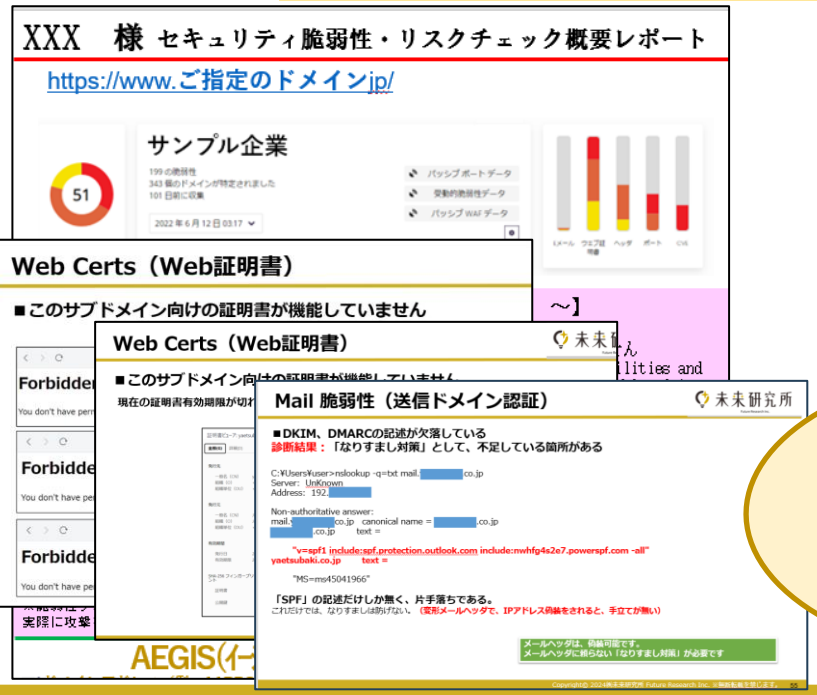
未来研究所 Future Research Inc.

■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お伝えします

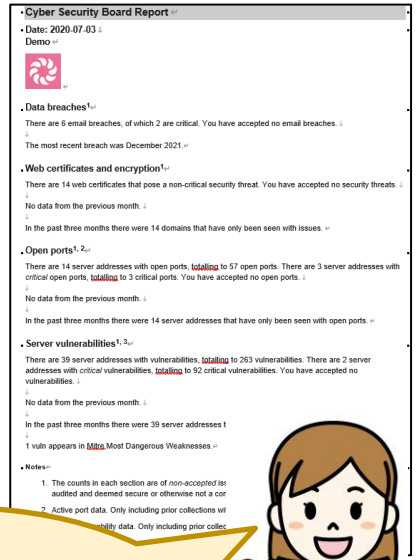
【弊社スタッフが作成する報告書】



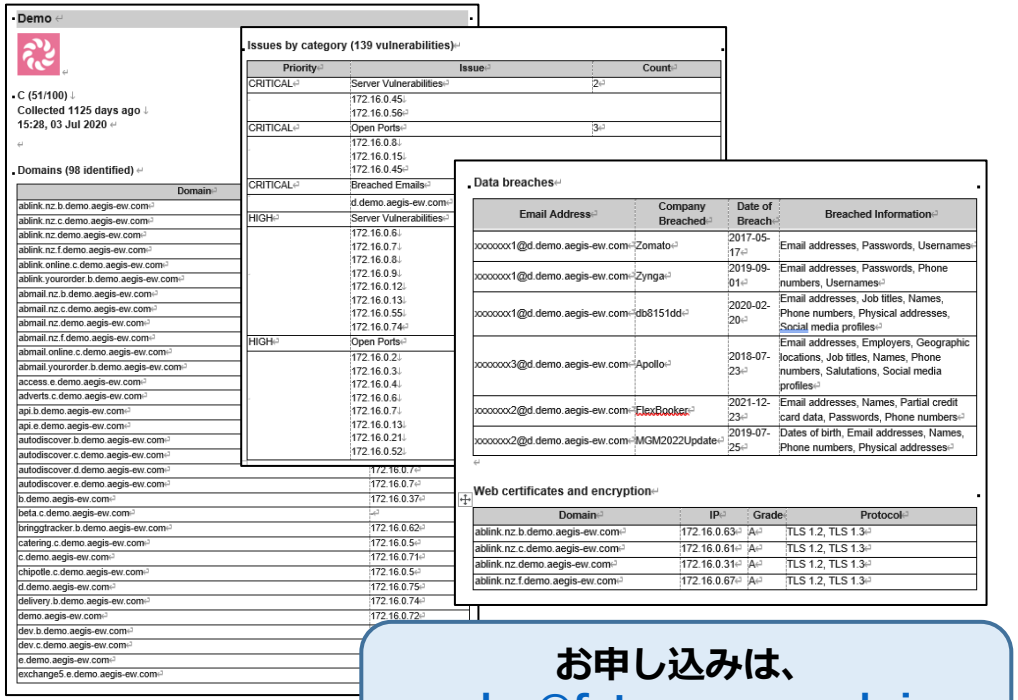
＋

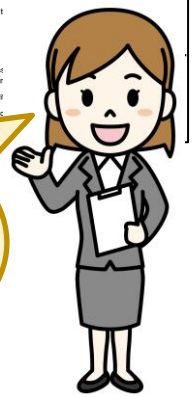
【イージスEWにより自動生成される評価レポート】

※概要



※詳細





ぜひこの機会に
ご検討ください。
おまちしております。

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

第3・４ステップ　有料ASM・有料脆弱性診断

未来研究所 Future Research Inc.

■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。

【報告書+説明会の報告書例】

■修正方法の例

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>
```


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>
```


弊社スタッフの
豊富な経験を
ご活用ください。

人財サービス：サイバー支援事業　～特定業種向け

未来研究所 Future Research Inc.

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ことが必要です。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。 ・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 ・特定社会基盤事業者の、社内イントラネットシステムに対する脆弱性診断と報告書の作成	35h（週・1日）～
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 / SaaS提供メーカ	「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）～

人財サービス：サイバー支援事業　～一般業種向け

未来研究所 Future Research Inc.

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。 ・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	35h（週・1日）～
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。 ・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 - お客様に最適なセキュリティツール（IDS/IPS、WAF、EDRなど）の選定支援 - 購入,設定,運用などのサポート	35h（週・1日）～
9		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
			技術	・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	