～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による脆弱性診断

2024年12月20日
株式会社　未来研究所

会社概要

未来研究所
Future Research Inc.

- 我々が目指すビジョンとは？
  - 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のです
- 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
- 創業/URL　2021年１月、資本金1500万円　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
（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
（イージスEW・脆弱性診断ツール・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

ホームページの危険性、一目でまるわかり

未来研究所 Future Research Inc.

脆弱性診断ツール イージスEW（AEGIS-EW）

AEGIS EARLY WARNING SYSTEM

見やすい GUI

深刻度の割合が
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・オレンジが あると危険！

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

改修後の目標
総合評価（レイティング）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？

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
SE1年目で乗っ取れるレベル!!

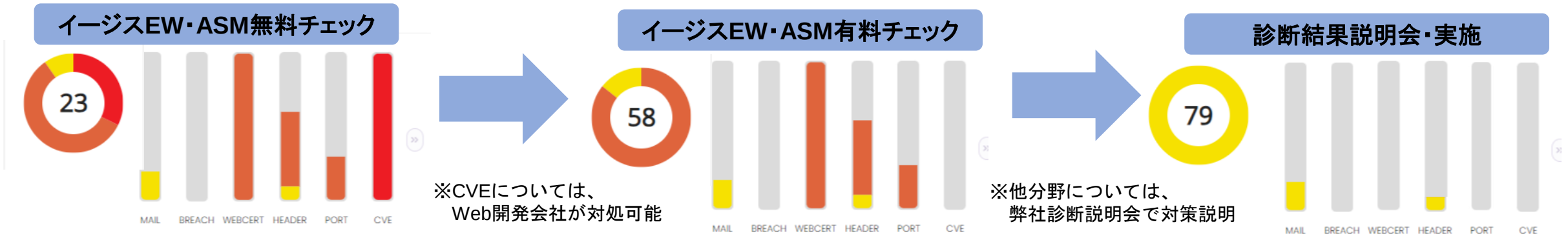
■オレンジ＝重要
SE2~3年目で乗っ取れるレベル!!

要改修です!!

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。

脆弱性（ぜいじゃくせい）診断の基準

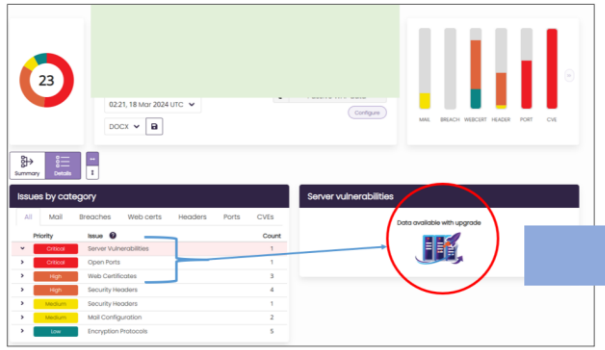
- イージスEWの安全基準は、100点満点
  - 診断結果が悪い場合は、発見された危険な個所を改善して60点以上を目指します
- グラフの色の見方（世界共通基準：CVSSv3.1)
  - 赤（緊急）・オレンジ（重要）色があると、大変危険です！
    1年目～３年目の新米SEでも乗っ取れます！
  - 赤・オレンジの危険性（脆弱性）を優先的に改修します
  - サイバー先進国（米国・イギリス・NATO主要国・オーストラリア等）では、赤・オレンジ色の危険性を放置している企業は、公共機関との取引口座を持てません
    - 日本においても、NIST SP800シリーズへの対応が義務化された、**特定社会基盤事業者**は対応必須



診断結果と対処

- **イージスEW・無料ASM診断**
  - 分野別に、「緊急」「重要」など深刻度ごとの危険性の件数がわかる
  - 無料診断では、危険性（脆弱性）の詳細までは判明しません
    - → 詳細は**イージスEWの「ASM有料診断」・「ペネトレーションテスト」**にて検出可能

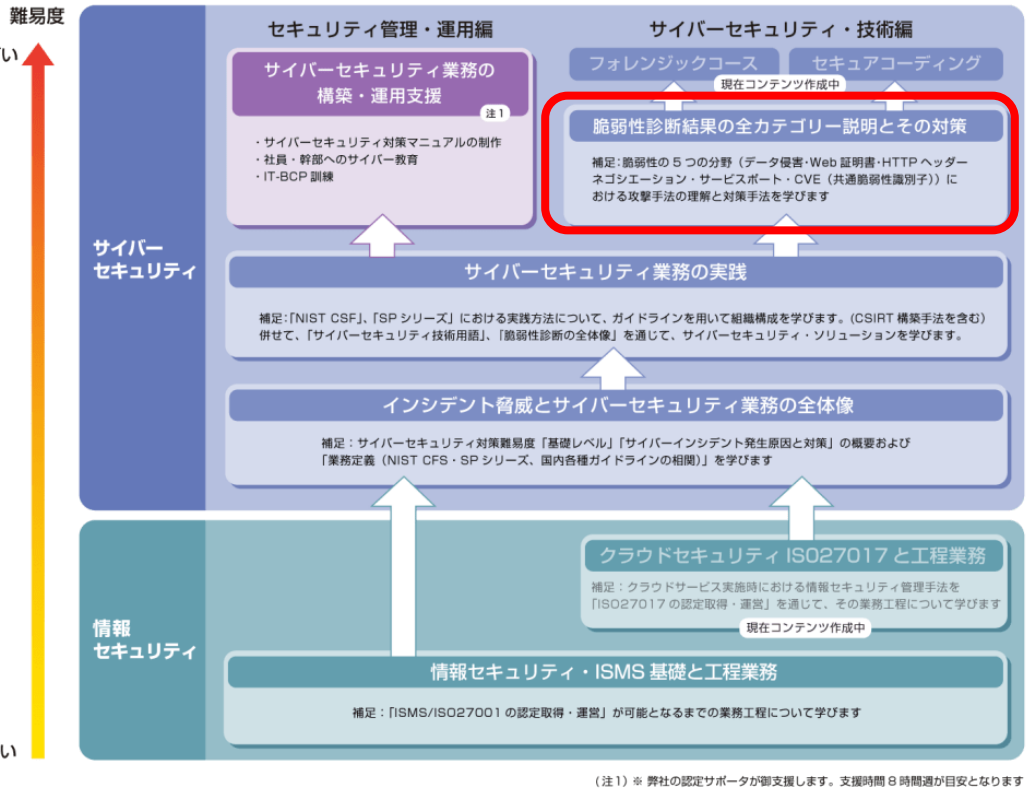
イージスEW･ASM無料チェック



イージスEW･ASM有料チェック

- **エンドユーザー様＆Web開発会社様向け説明会を実施**
  - CVEの多くの項目は、Web開発担当者さんが改修可能！
- **Web開発会社様が修正出来ない項目は、未来研究所が完全サポート**

※https://mirai-manabiya.jp/course001/



脆弱性（ぜいじゃくせい）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脆弱性診断

脆弱性（ぜいじゃくせい）診断は、システムの健康診断

- **人の場合：健康診断**
  システムの場合：脆弱性診断

人間の場合は、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緊急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　＝　脆弱性診断

ハードニングの実施手順

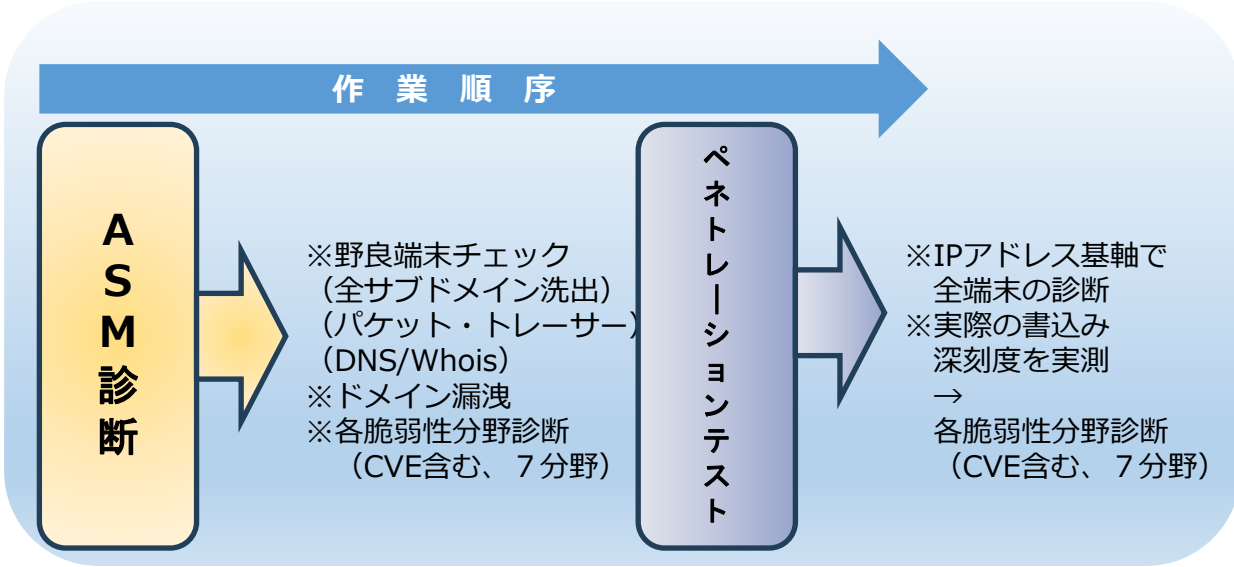
- 何から始めるの？

  Step1　**システム全体を脆弱性診断**して、作業優先順位表を作成

  Step2　**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

最初に必要なのが、
脆弱性診断と
作業優先順位の策定



ASM・ペネトレーションテスト・脆弱性診断

未来研究所 Future Research Inc.

■ASM(Attack Surface Management＝攻撃対象領域管理)

ASMとペネトレーションテストの違いは、次の通りです。
最も大きな違いは、ペネトレーションテストが「既知のサーバのみ」対象にしているのに対して、
ASMは「認知外（忘れられている）サーバ」も見つけ出して対象にします。

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う
出典；経済産業省ASM (Attack Surface Management）導入ガイダンス

①パッシブスキャン(Passive Scan)
パッシブスキャンでは、ドメイン情報から放置サーバ（野良サーバ）を検出して診断します。
②アクティブスキャン(Active Scan)
アクティブスキャンでは、調査対象診端末に対して、ハッカーと同様の攻撃手法を用いる診断方法（ペネトレーションテスト）を行って診断します。

広義の定義	脆弱性診断	脆弱性診断
狭義の定義（経済産業省の定義）	ASM	脆弱性診断（ペネトレーションテスト）
代表されるスキャン方法	パッシブスキャン (Passive Scan)	アクティブスキャン (Active Scan)
診断対象	インタネット上を検索し、発見した端末を対象とする	対象をあらかじめ指定（IPアドレス等）する
脆弱性の確定方法	通常アクセスの範囲で行うため、確度が低い可能性がある	攻撃を模したパケットを送信、その応答を診断するため確度が高い
対象への影響	パケットがセキュリティ監視装置（EDS/EDR）に検出されることは殆どない	セキュリティ監視装置（EDS/EDR）で検出される可能性は高い
イージスEWラインナップ	イージスASM診断	イージスペネトレ

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

脆弱性診断は、ASM＋ペネトレーションテスト

- ペネトレーションテストだけでは、**砂上の城**です
  - **ハッカーが最初に攻撃先を探すツールがASM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！

ペネトレーションテストを実施

建物は改築（ペネトレーションテスト）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！

ペネトレーションテストを実施
＋ ASM を実施

地面を強固（ASM を実施）にしたので
完全なハードニング基礎が完成して

完全防備となった!!

イージスEWの特徴

脆弱性診断ツール「イージスEW」とは？

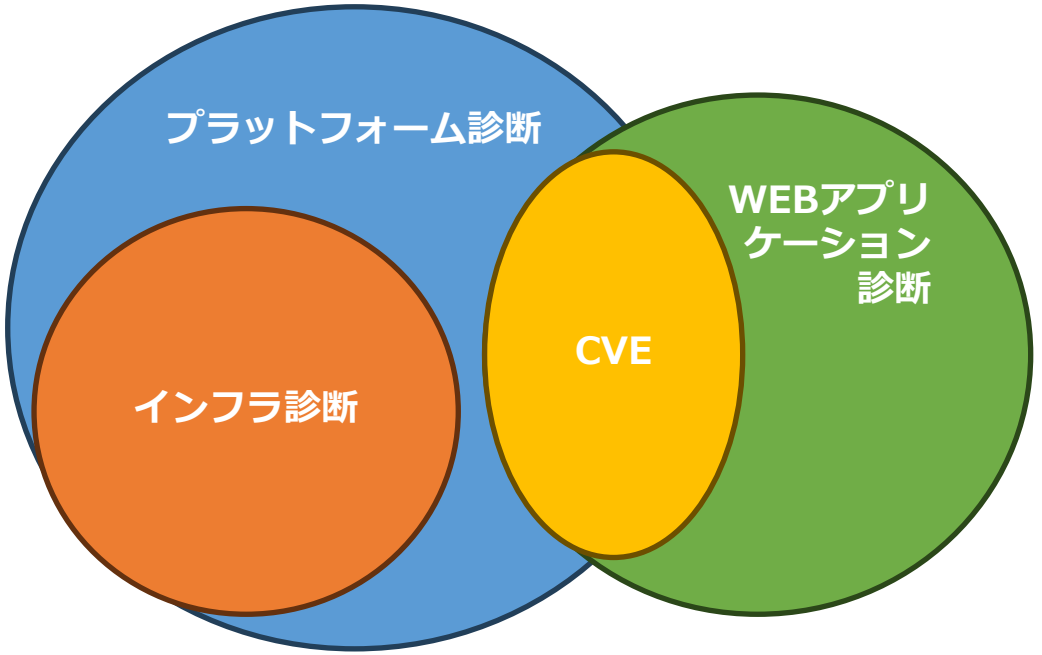
■イージスEWの立ち位置

イージスEW (AEGIS-EW)は、「プラットフォーム診断」と呼ばれる脆弱性診断ツールに該当する。
下記の脆弱性を調査する。

・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

なお、Webアプリケーションにおける「コード診断」は、実施しない。

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　4つの特徴

未来研究所
Future Research Inc.

見やすいGUI

診断結果の配色は、世界共通CVSS3.1を使用。サイバーの知識がなくても是非の判断が可能 です。サイバー先進国（米国、英国、NATOコア国家）では、システムに赤（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、米国NIST SP800シリーズと同様規約の適応が求められています。

Read More...

強力なASMとペネトレーションテスト

必要なのはメインドメインのみ。ASMにより、野良端末および漏洩したドメイン情報も検出いたします。

Read More...

全てのプラットホーム脆弱性診断を一括管理

インターネット・イントラネット・納品前システムの全てのプラットホーム脆弱性診断をイージスEWの共通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。

Read More...

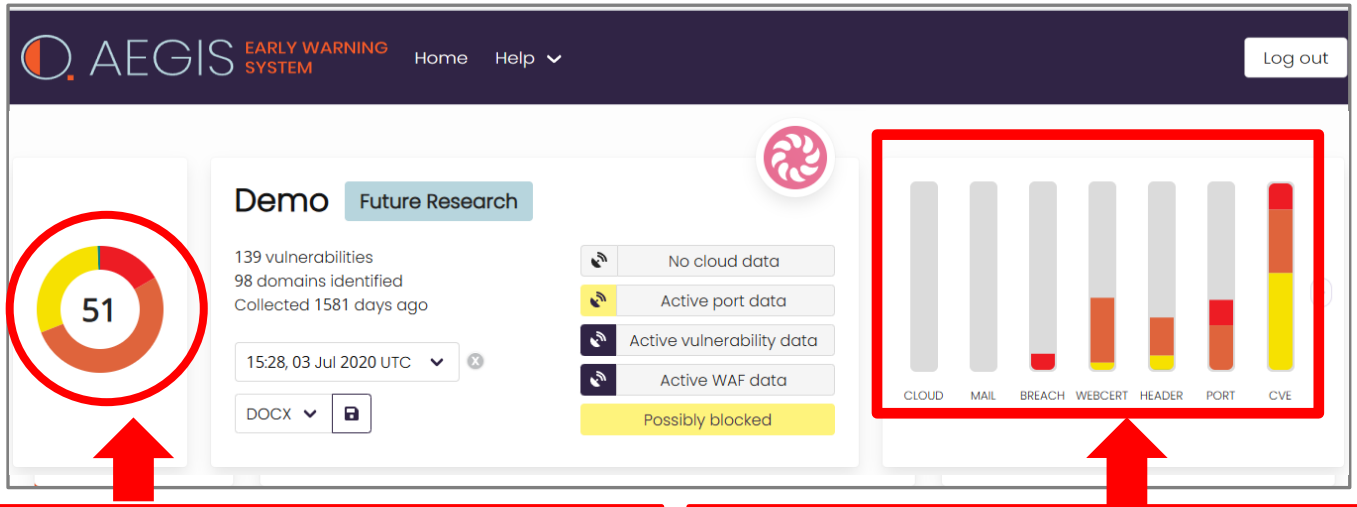
リーズナブルな価格帯

システムの「人間ドック」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、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、適切な定期診断の実施が困難になります。

Read More...

見やすいGUI

- **セキュリティの専門家でなくても判断できる**
- 全システムを共通のGUIで管理できる



総合評価（レイティング）（**51点/100満点**）
脆弱性危険度分類：
「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１（図内赤グラフ）の脆弱性」
が存在
色はCVSSv3.1の世界基準に準拠

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　診断分野

未来研究所
Future Research Inc.

■8つの分野別診断項目
脆弱性が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

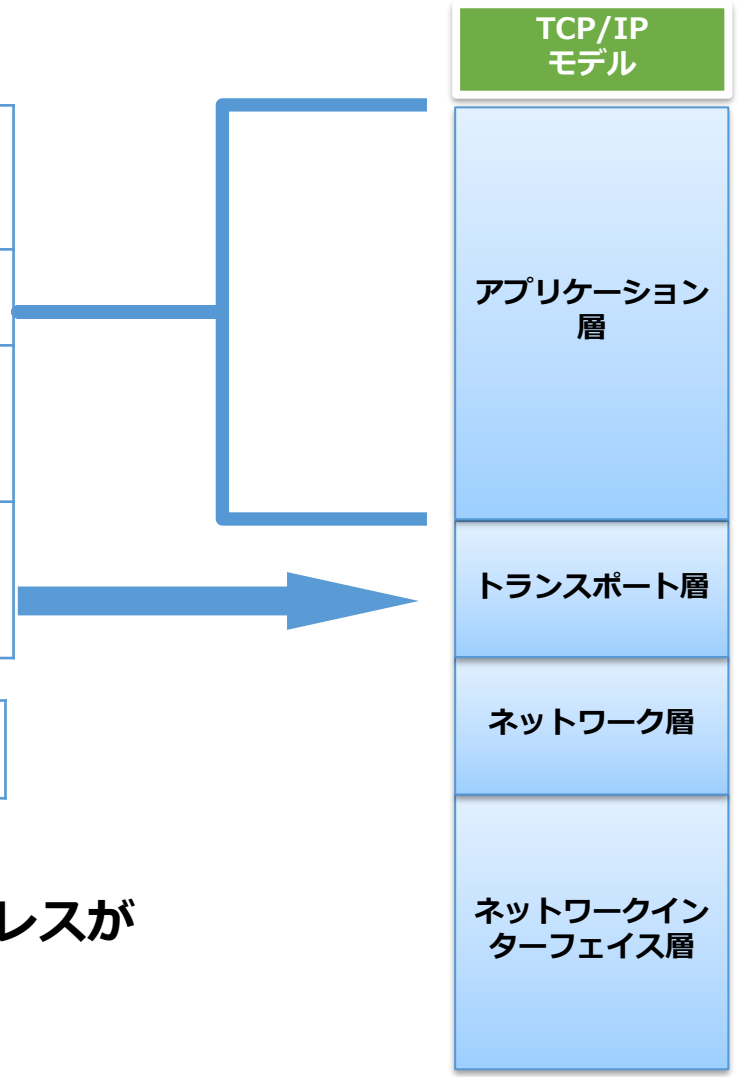
CVE 共通脆弱性識別子	CLOUD Cloudプラットフォーム診断	MAIL 送信ドメイン認証	BREACH データ侵害	WEBCERT Web 認証関連	HEADER HTTP ヘッダー関連	PORT ポートスキャン攻撃	SUBDOMAIN 野良端末検出
個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体のMITRE社が採番している識別子です。脆弱性検査ツールや脆弱性対策情報提供サービスの多くがCVEを利用しています。	Amazon AWS・Microsoft Azureにおけるセキュリティポリシーを診断します。VPC（Virtual Private Cloud）のデフォルト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。	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。

イージスEW　診断分野の階層

■通信レイヤ別の脆弱性

CVE	共通脆弱性識別子CVE (Common Vulnerabilities and Exposures)
WEBCERT	Web認証関連
HEADER	HTTPヘッダー関連
Cloud	AmazonAWS Azure のプラットフォーム診断

PORT	ポートスキャン攻撃



WANに
接しているサーバ・
端末

- 「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とペネトレーションテスト

※ASMは、ハッカーが最初に使用するツール使用することで何がわかるのか？

- **野良端末の存在が分かります（多くは、完全放置状態。モジュールが古く、乗っ取り可能な場合が多い）**
- **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

全てのプラットフォーム脆弱性診断を一括管理

未来研究所
Future Research Inc.

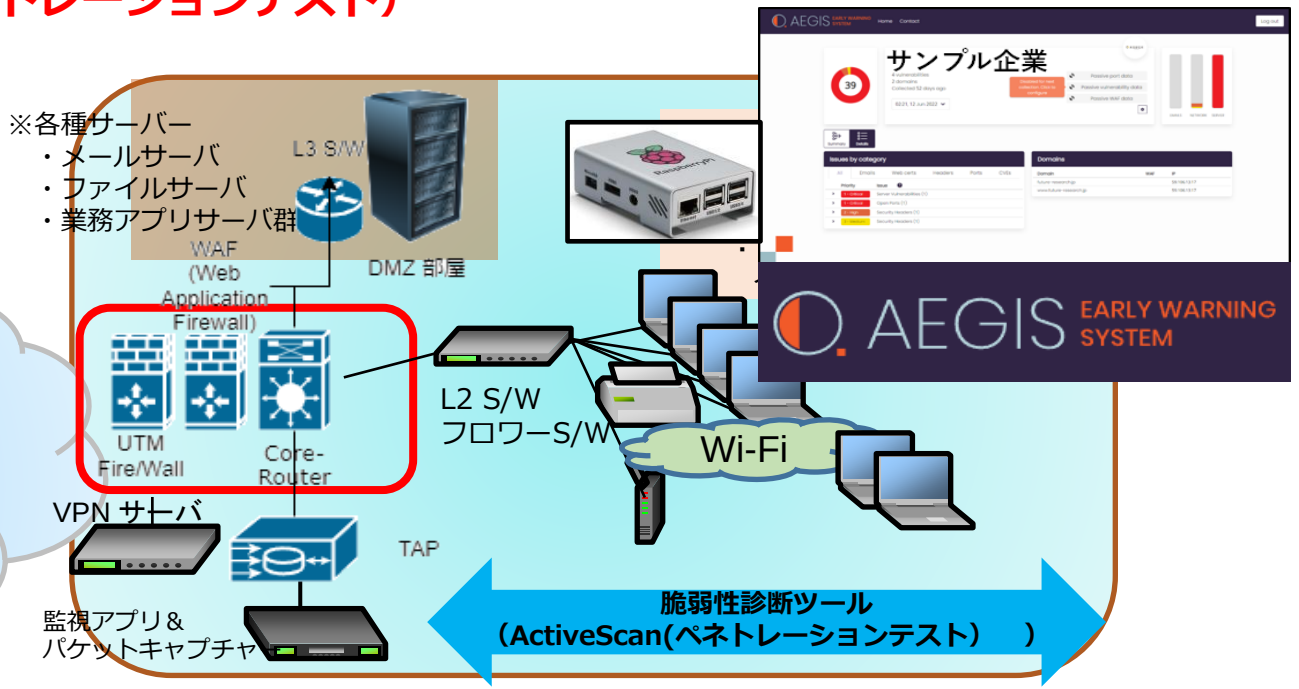
①インターネット上の脆弱性診断（ASM /ペネトレーションテスト）

イージスEW

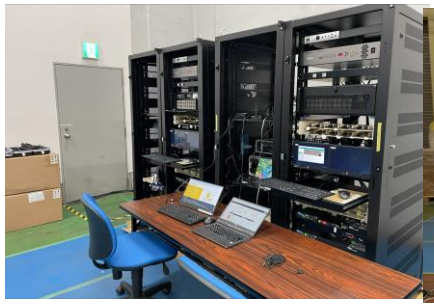
※Public Cloud / IDC
各種サーバー
・メールサーバ
・ファイルサーバ
・業務アプリサーバ群

②イントラネット（社内端末群）の脆弱性診断（ペネトレーションテスト）

イージスEW + Edge-BOX(VPN)



③納品前ネットワーク構築機材群の脆弱性診断（ペネトレーションテスト）



イージスEW + SimつきWi-Fiルータ+ Edge-BOX(VPN)

リーズナブルな価格帯

未来研究所
Future Research Inc.

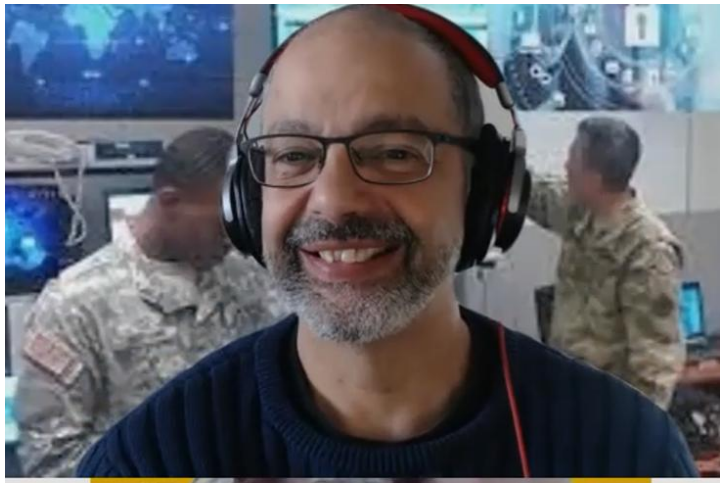
イージスEWは、チェック対象の端末総数が数千台以上になっても、脆弱性診断を定期的に実施できるリーズナブルな価格帯で提供しております
https://mirai-cybersecurity.jp/aegis-ew/aegis-ew-price/

■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（オセアニア）からの誘致プログラムを活用し、ニュージランドに会社移転をしたのがTTD社です。
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にて、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。
　イージスEWは、オーストラリア・ニュージランドの助成金も活用し、産学連携にて制作されたツールです。またパケットスニッファも英国との関係を活かし、英国のものを利用しています。そのため、低価格での御提供が実現されています。

・なぜオーストラリアは、サイバーセキュリティ事業者を誘致したのか？
　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への対応が義務付けされ、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、この事態を受けて世界中からサイバーセキュリティを強化する企業を誘致し、サイバーツールの製造・リリース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。

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

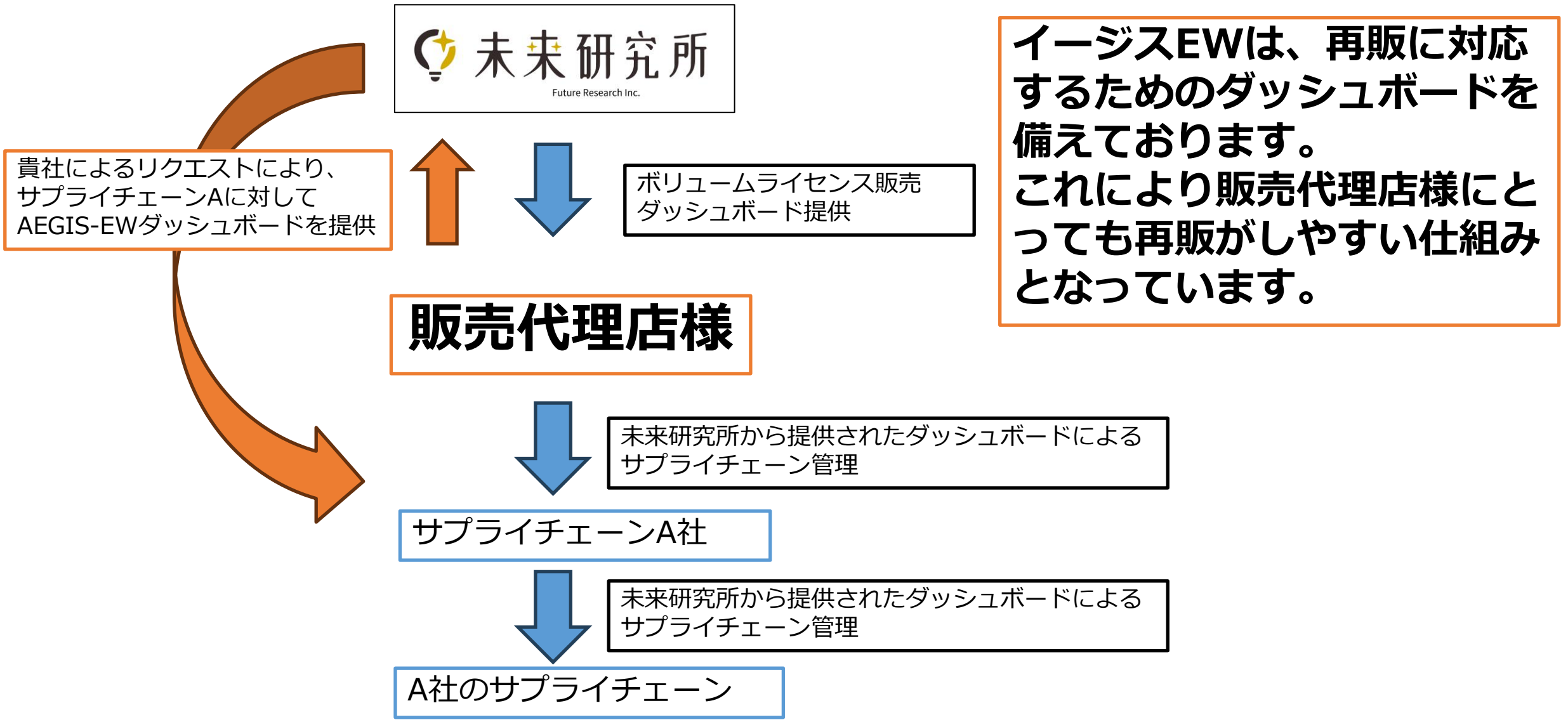


エンドユーザ/販売代理店・VAR　での診断管理

- エンドユーザ様
  - IS部/CSIRTによる、複数拠点の一括管理
    - アカウントは無料で作成

- 販売代理店・VAR様
  - 顧客毎での管理・サポートが可能

イージスEWボリューム販売概要

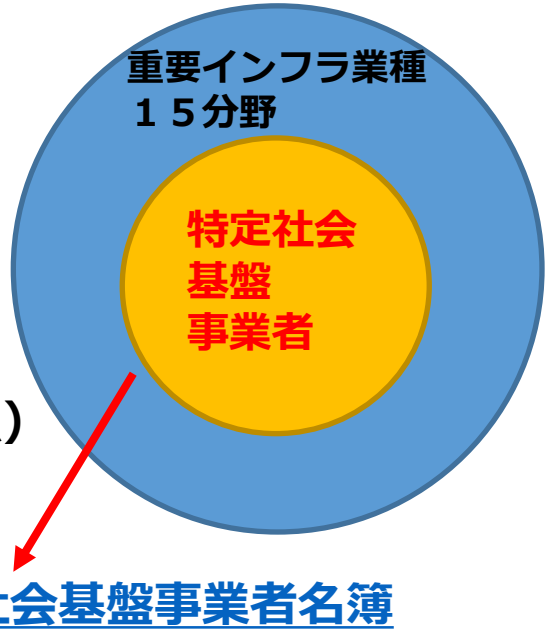


**イージスEWは、再販に対応するためのダッシュボードを備えております。
これにより販売代理店様にとっても再販がしやすい仕組みとなっています。**

脆弱性診断が必ず必要な案件は？

脆弱性診断の実施が、法律上必須に成りました

- 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、違反すると罰則が科せられる
    - 対象システム案件
      - 特定社会基盤事業者のシステム全般
    - 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、社内も含めたシステム全般が対象
      - 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要求される**（イージスEWの事例、御参照）**
    - 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、対象が重要インフラ業種15分野に拡大

イージスEWのサポート・サービス

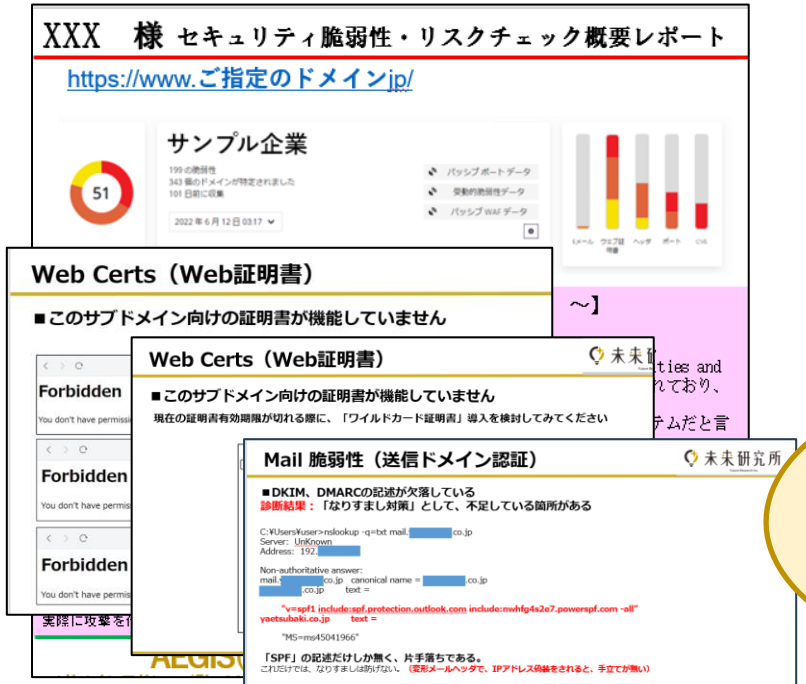
無料ASM脆弱性診断結果説明会

未来研究所
Future Research Inc.

■イージスEW無料ASM脆弱性診断　報告書を作成し説明会を実施いたします

イージスEWの無料ASM脆弱性診断結果の説明会を無料で実施いたします。
（個別の脆弱性の詳細を分析するためには、有料診断が必要です）

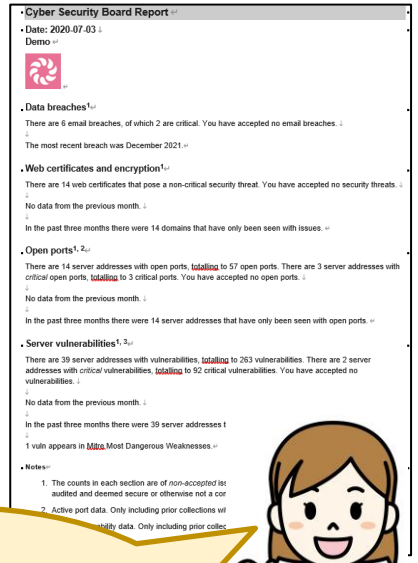
無料説明会
検出された脆弱性診断結果の
簡易的な対処方法をお伝えします



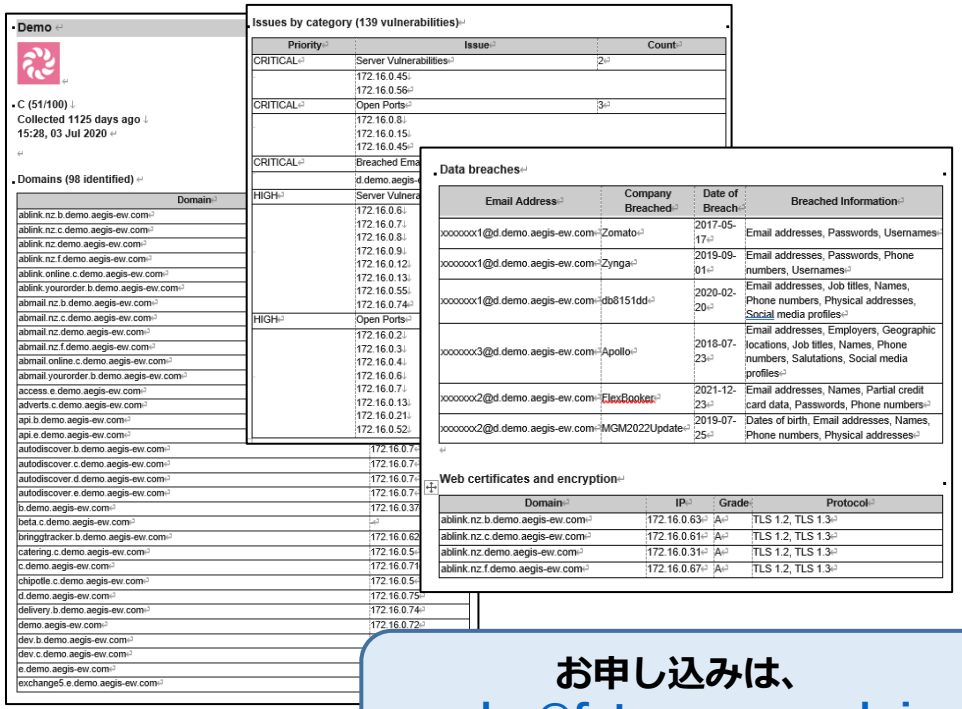
＋

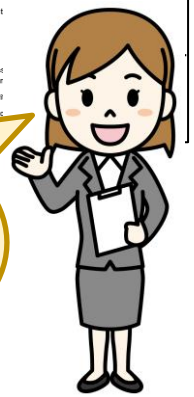
【イージスEWにより自動生成される評価レポート】

※サマリー版



※有料版：CVSS、CVE　等、過去の漏洩情報も記載





ぜひこの機会に
ご検討ください。
おまちしております。

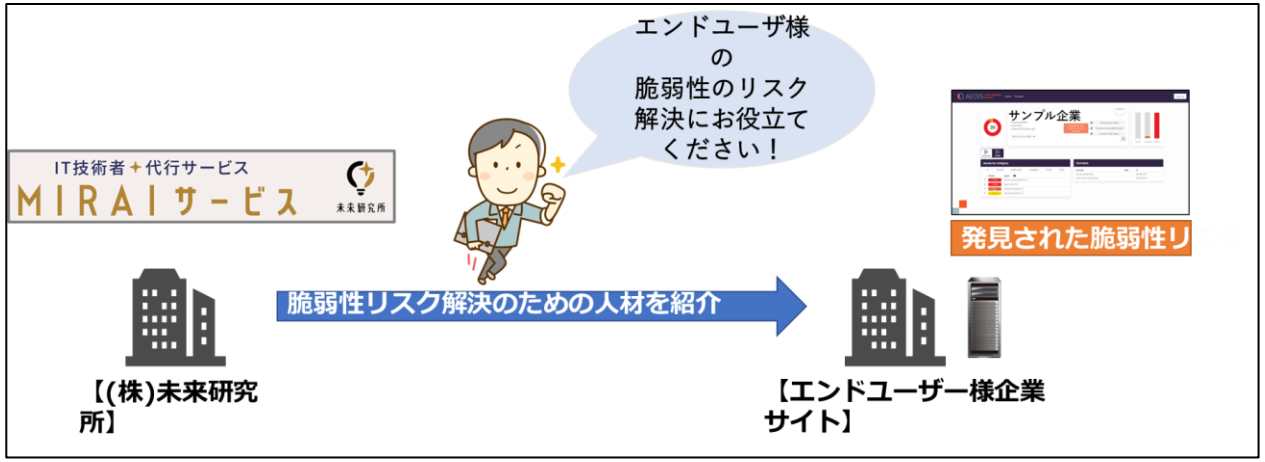
お申し込みは、
sales@future-research.jp
までお気軽にどうぞ！

脆弱性診断の付加サービス・ご案内

未来研究所
Future Research Inc.

■ イージスEW診断結果・有料セミナー

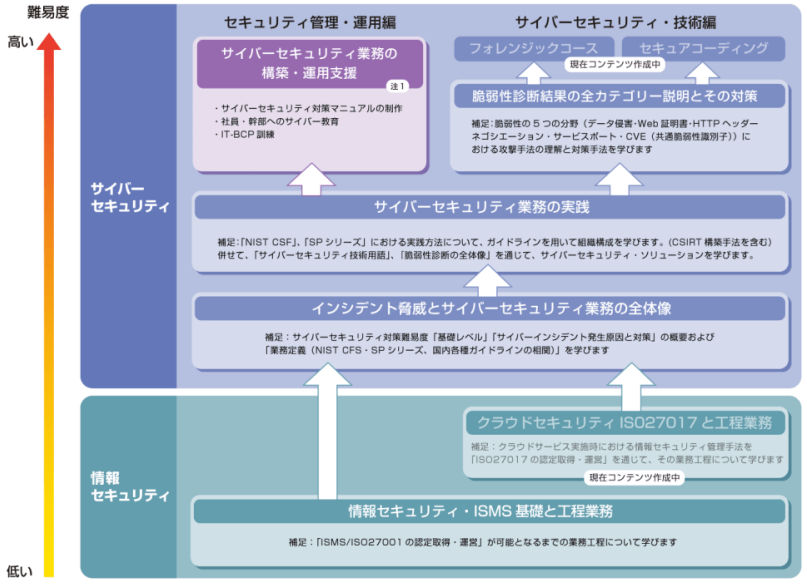
有料診断結果全般の説明と、各脆弱性分野の対策方法レクチャ、および実際の結果に基づいた対策セミナーを実施させていただきます。
　ご要望があれば、改修作業を対策エンジニアの支援も可能です。
脆弱性リスクを解決する人材をお探しの際は、是非ご相談ください。

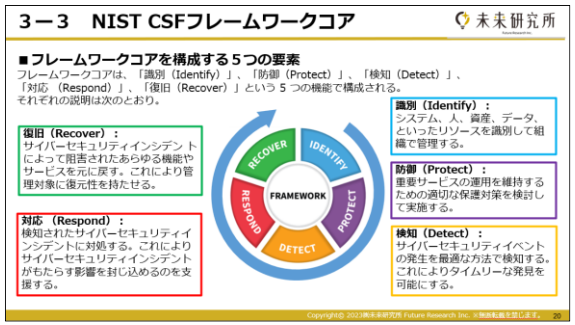


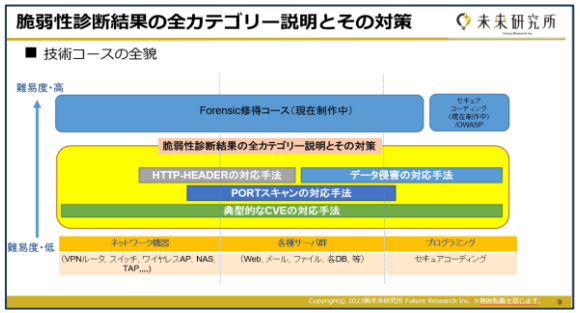
■ 未来の学舎・セキュリティ編の研修コース

　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





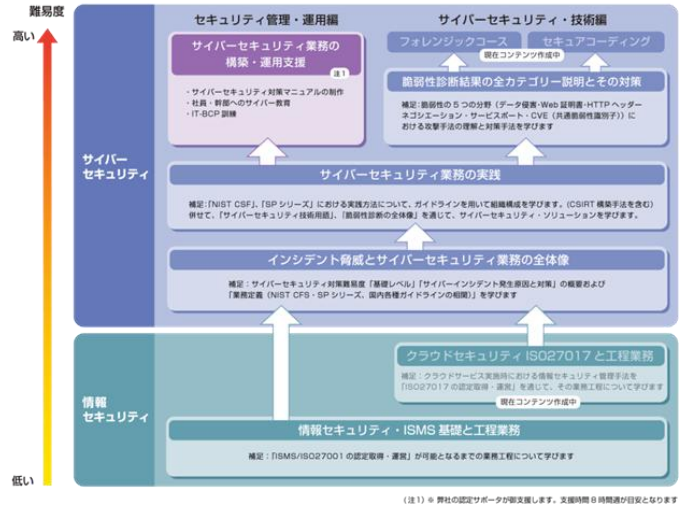


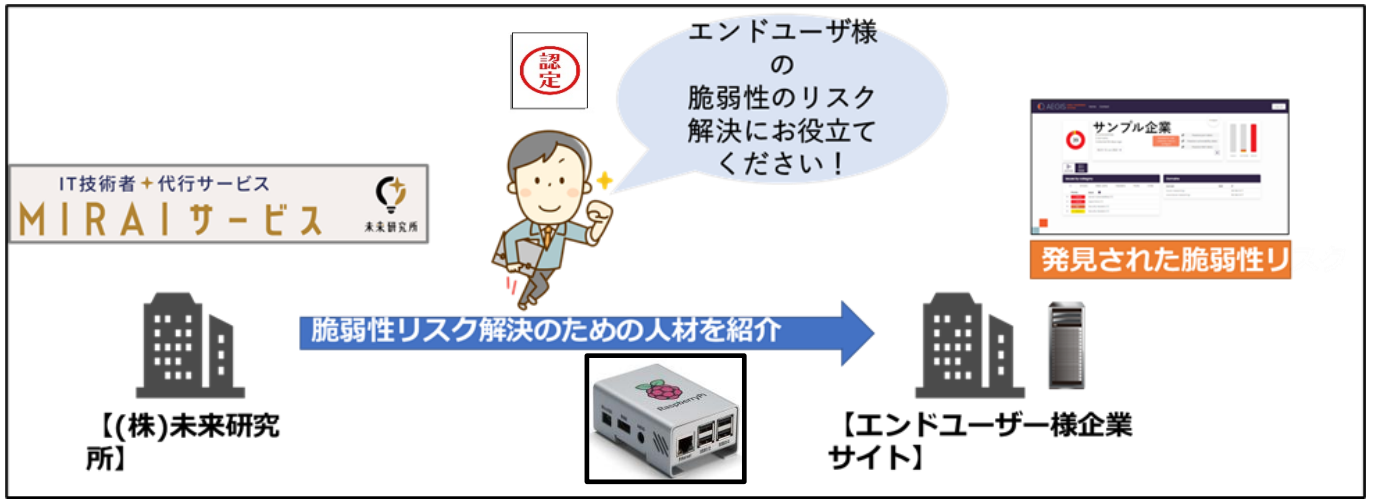
支援サービス

- 基本方針
  - 揺り籠から墓場まで、最後までご支援致します
- 脆弱性診断結果の改修サービス　**「伴走サービス」**
  - CVSS緊急・重要の改修支援を、週1日就業（35h/月）～から提供
  - 遠隔地の場合、Edge-BOX（VPN BOX）をお送りし、お客様と一緒に改修します
- 公共向け支援サービス
  - 病院機関
    - 「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
  - 学校系（＝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

MIRAIサービス

- 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





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）～

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	

Thanks