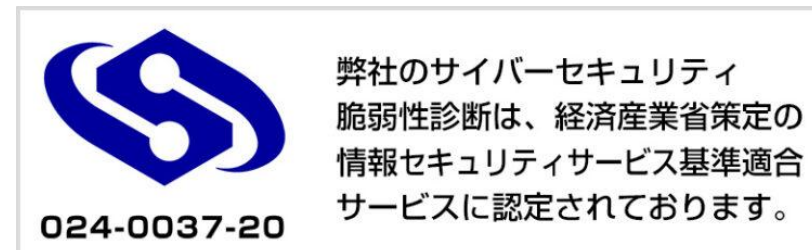


脆弱性診断からのシステムのハードニング作業紹介
プラットフォーム診断ツール
イージス EW御紹介
&
サイバーセキュリティ事業の御支援ソリューション

2025年7月30日
株式会社 未来研究所

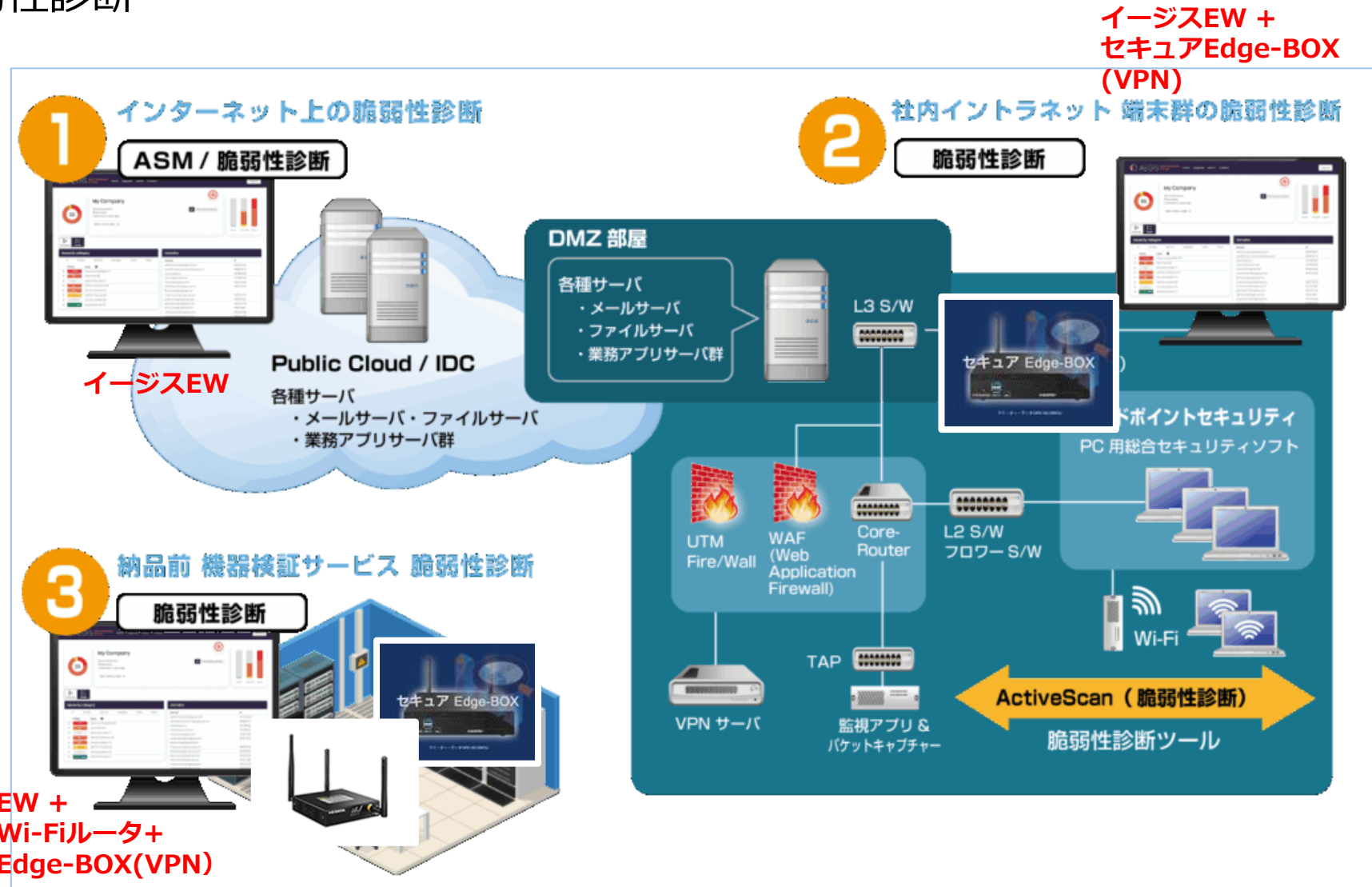
ASM・レコナイ+脆弱性診断の決定版
イージスEW



イージスEWの強み

インターネット上：ASM&脆弱性診断
社内イントラ：脆弱性診断
共通GUIのダッシュボードで
一括管理できます

イージスEWは、
オセアニア主要国の資金で
制作されたため、
低価格での御提供が可能です



■ 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！

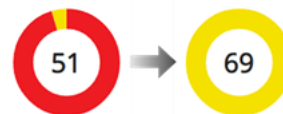
脆弱性診断を実施
+ ASM 診断を実施



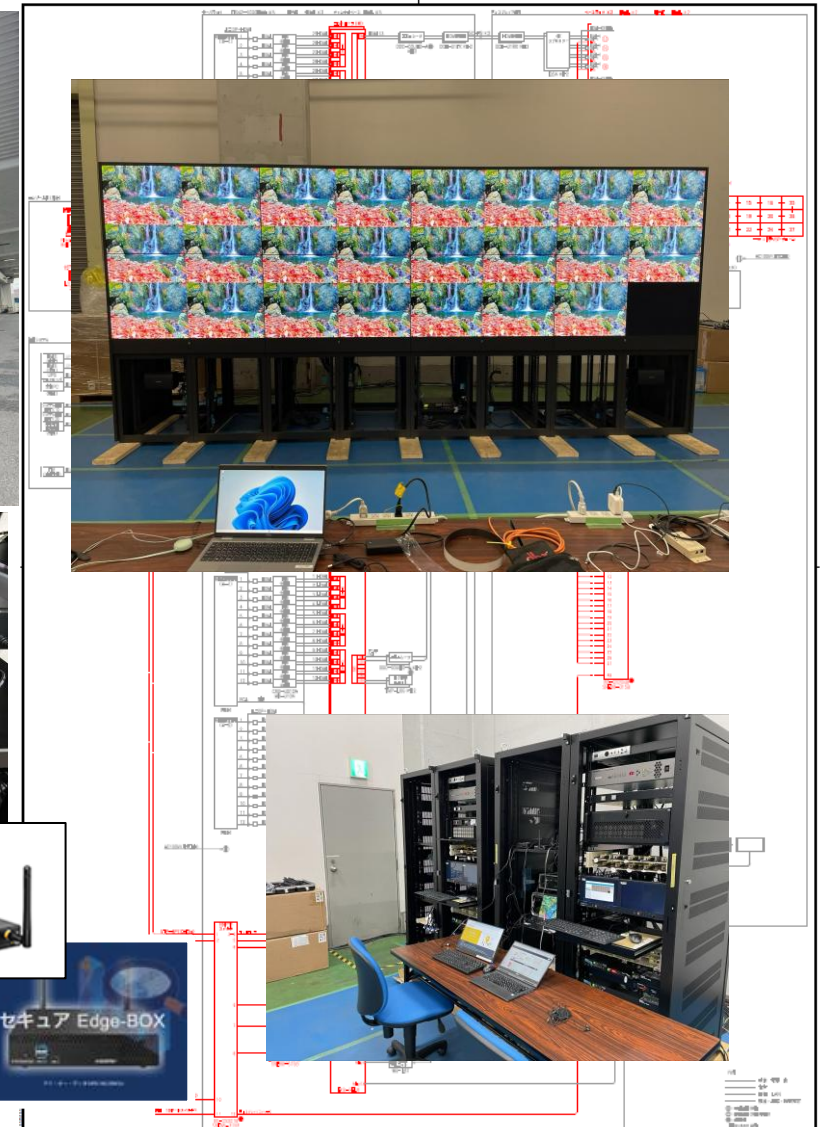
地面を強固に（ASM 診断を実施）改良し
完全なハードニング基礎が完成して
完全防備となった!!

世界定義の脆弱性診断は、ASM診断と脆弱性診断です。

- NW構築案件での品質管理には、脆弱性診断が必須です
NW構築の納品前品質証明として、イージスEWをご活用ください
納品後、および運用保守時の監視ルールとしても、御提案ください



対策を実施した結果、赤のクリティカル表記がなくなり
総合評価点が 51 から 69 に改善しました。

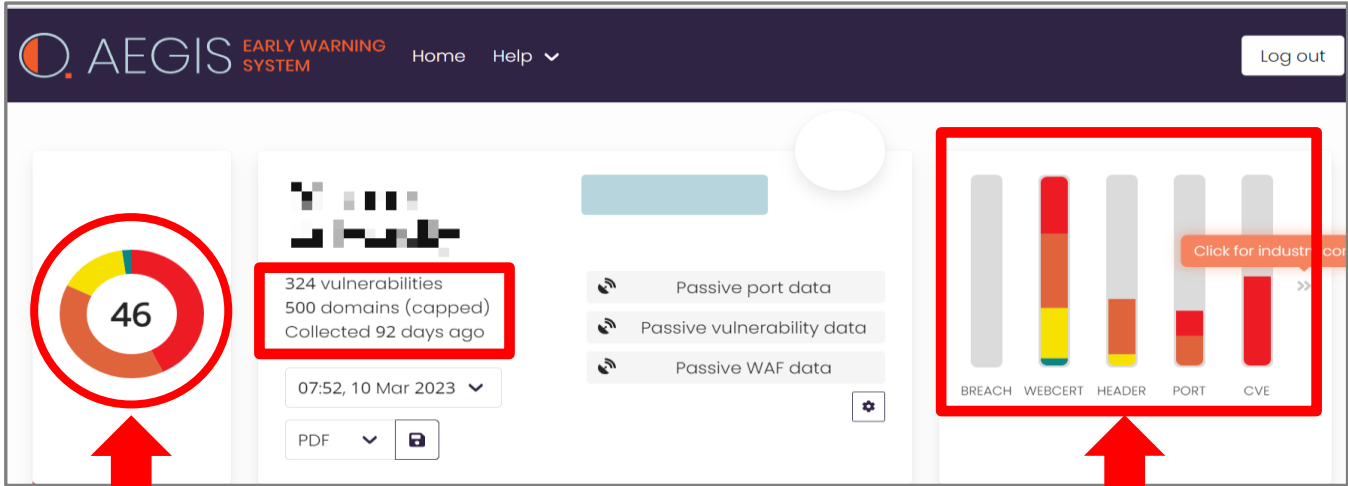


AEGIS-EW特徴：見やすいダッシュボード

■ AIGES-EW(イージス EW)におけるダッシュボード

「AIGES-EW(イージス EW)」では該当ドメインの診断結果を、総合評価点(レーティング)で示します。

なお、納品方法については「**ダッシュボードでの診断結果表示**」となります。(ダッシュボード内にレポート出力機能もあります)。



総合評価 (レーティング) **(46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、あつてはならないはずの
「深刻度 1 (図内赤グラフ) の脆弱性」
がサブドメイン内に存在

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

視覚的なサーバ安全度スコアリング

ドメインの脆弱性リスクをグラフ化！
サーバ安全度スコアリングを
(100点満点中 XX 点) で表示します。

POINT!
専門知識は不要。
色分けて理解できる！

AEGIS-EW は、サーバ脆弱性診断に詳しくないエンドユーザー様でも見やすく、わかり易いものとなっています。
スコアリング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。

サイバーセキュリティ環境のレベル

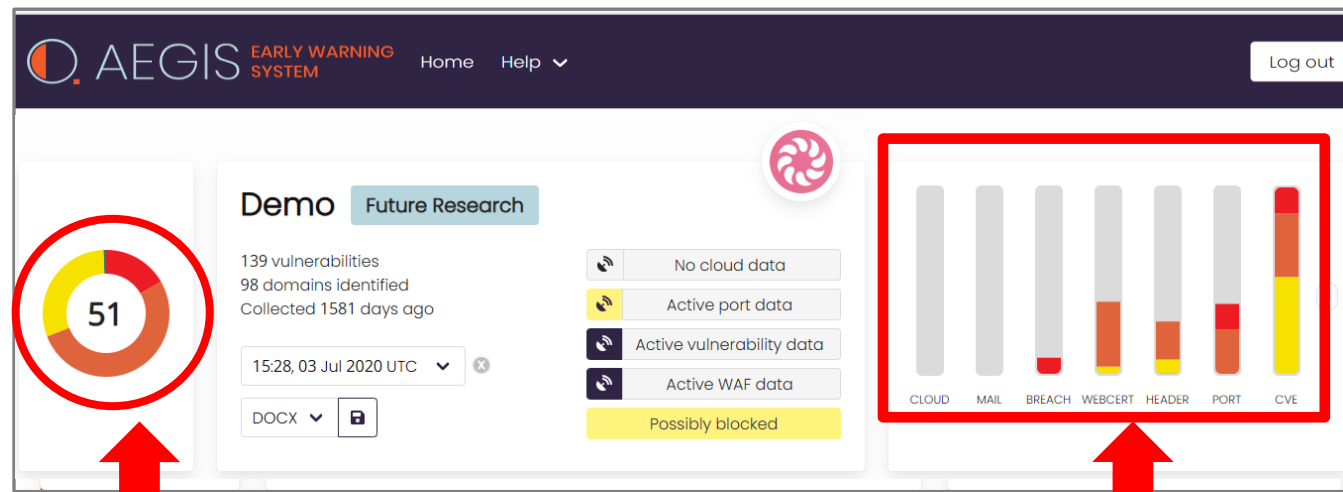
総合点が円グラフによって
分かりやすく示されます。



- 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

■イージス EWのダッシュボード

イージス EWでは該当ドメインの診断結果を、総合評価点（レーティング）とグラフで示します。



総合評価（レーティング）（**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

診断結果が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 (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

■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



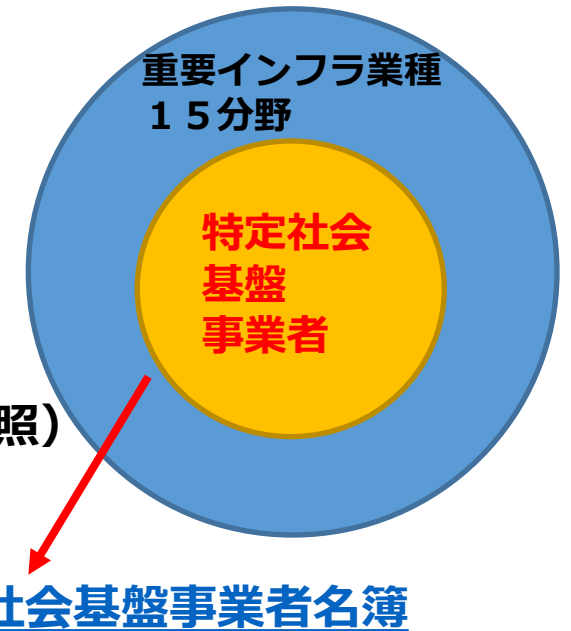


※政府系機関と業者の銀行口座維持のために、脆弱性診断結果の提出が必須なのがサイバーセキュリティ先進国です。下記の、米・英・オーストラリア3国を含め、多くの国でAEGIS-EWが活用されています

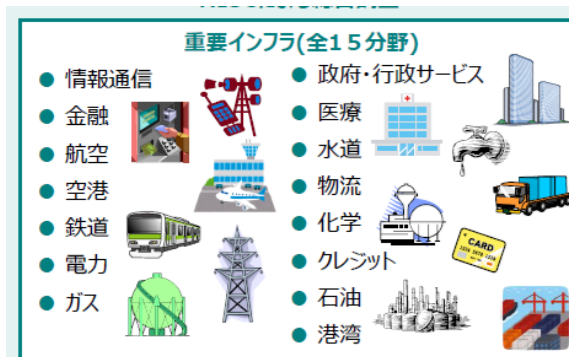
- ・ **NIST（米国立標準技術研究所）でのCSF、SP-800シリーズ適合報告書類として活用**
- ・ NCSC National Cyber Security Center（英国・国家サイバーセキュリティ・センター）
- ・ ASD（Australian Signals Directorate: オーストラリア・参謀本部国防信号局）

脆弱性診断が必ず必要な案件は？

- 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、対象会社が**重要インフラ業種15分野に拡大**

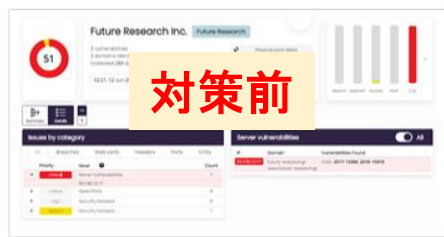
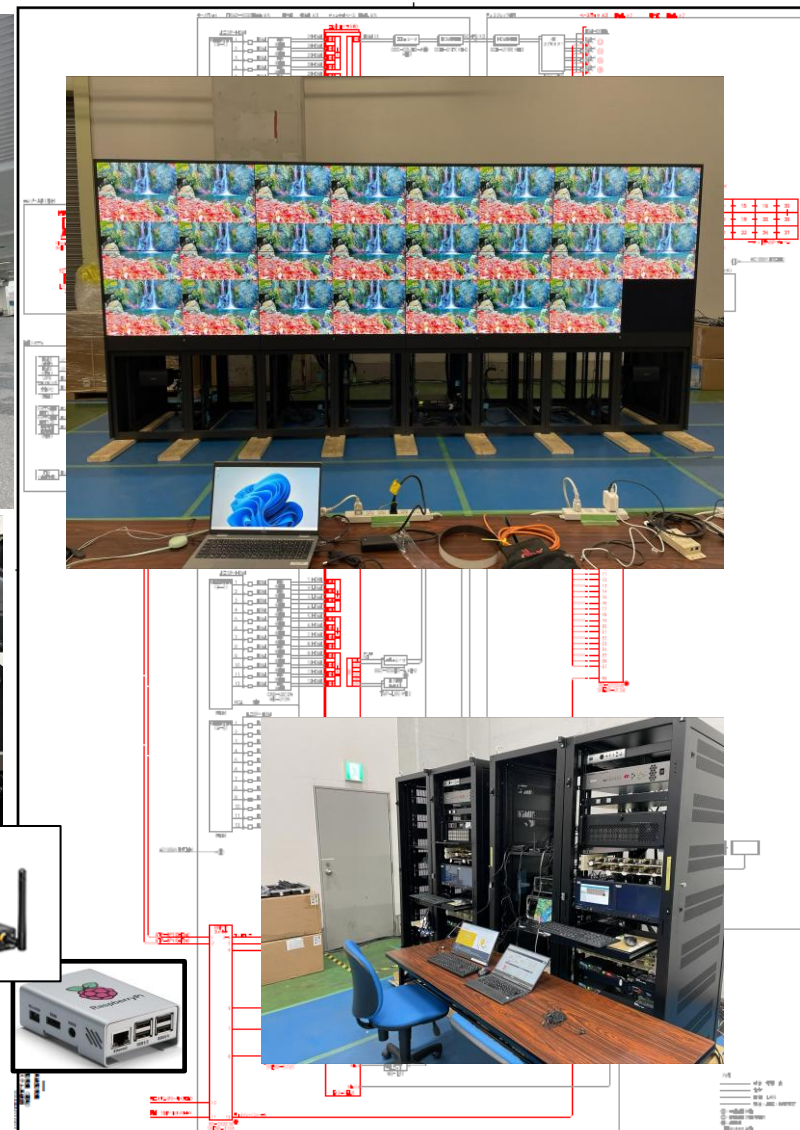


- 内閣府指導により、政府調達資材に対し、米国基準・NIST SP800-171の適用が義務付けられます（対象1000社超）
 - 特定社会基盤事業者は2024年5月より義務化が開始
 - 重要インフラ事業者への適用も順次開始か？
- 経済産業省が、IoT機器に対し、サイバーセキュリティ対策の認証を始めます
 - サイバー被害の約 40% は IoT デバイスから発生しています。

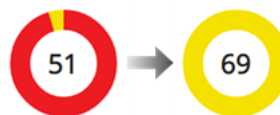
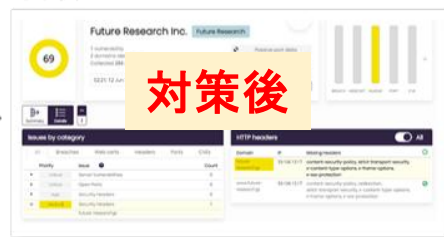


イージスEW：重要インフラでの納入前診断

- 某電力会社ネットワーク施設工事前の、評価システムでの脆弱性診断実施
 - 発注元からは「納品前脆弱性診断テスト」が要件
 - 倉庫でのキitting後の評価



対策実施



対策を実施した結果、赤のクリティカル表記がなくなり
総合評価点が 51 から 69 に改善しました。



未来研究所でのサイバーセキュリティ支援 サービス

※弊社では、サイバーセキュリティ業務全般での御支援を開始させていただいております。
何なりとお声がけの方、宜しくお願い申し上げます

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。	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/ 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）～

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	- 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	要相談
				- 購入,設定,運用などのサポート	
9				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	
			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

