未来研究所
Future Research Inc.

脆弱性診断からのシステムのハードニング作業紹介

AEGIS-EW（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

2024年8月
株式会社　未来研究所

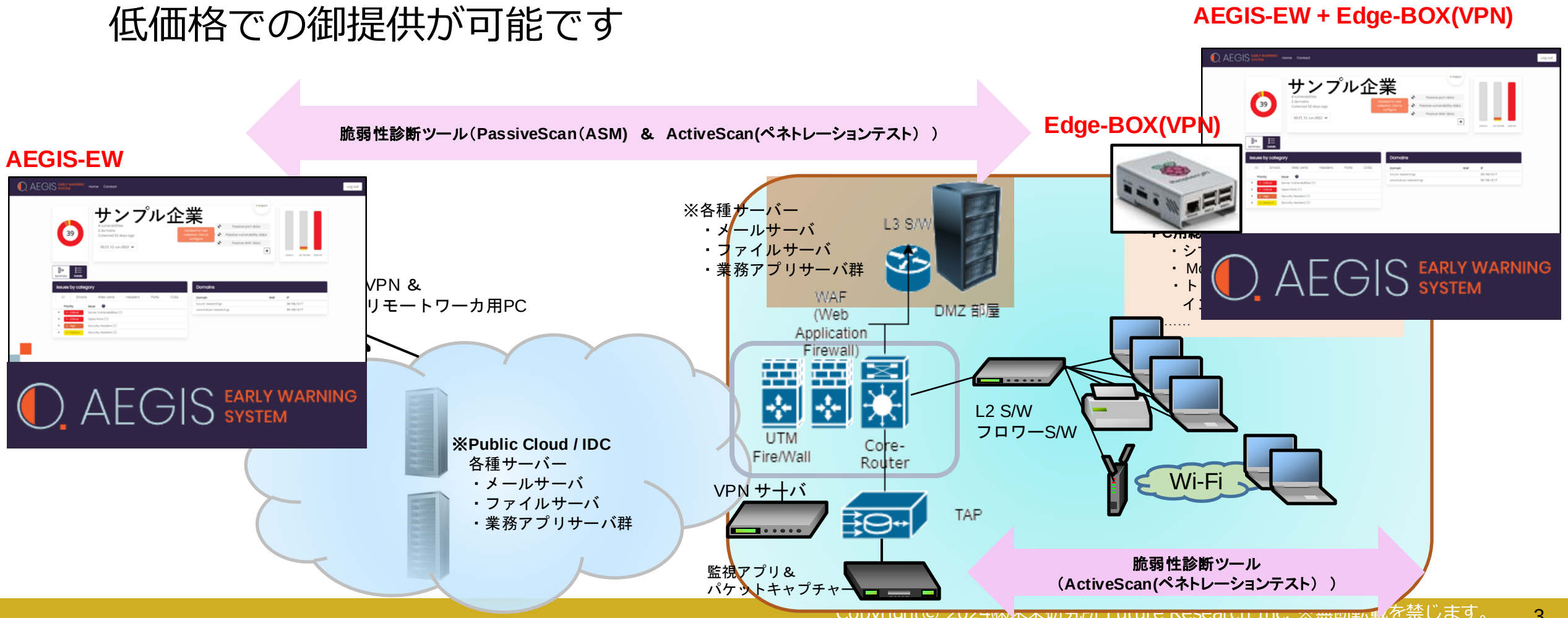
ASM・パッシブスキャン＋ペネトレの決定版
AEGIS-EW

AEGIS-EWの強み

ASMは必須、インターネット側もイントラ側も共通GUIで一括管理

未来研究所 Future Research Inc.

- インターネット上のASM＆ペネトレ、および社内イントラ・ペネトレを共通GUIダッシュボードで、定期管理が容易です
- AEGIS-EWは、オセアニア国群の資金で制作されました。低価格での御提供が可能です



脆弱性診断は、ASM＋ペネトレーションテスト

未来研究所
Future Research Inc.

- ペネトレーションテストだけでは、**砂上の城**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

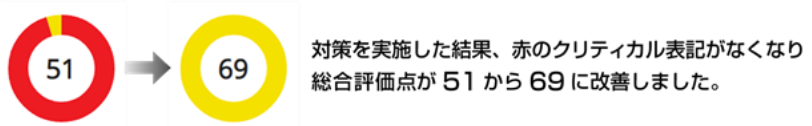
地面を強固（ASM を実施）にしたので
完全なハードニング基礎が完成して

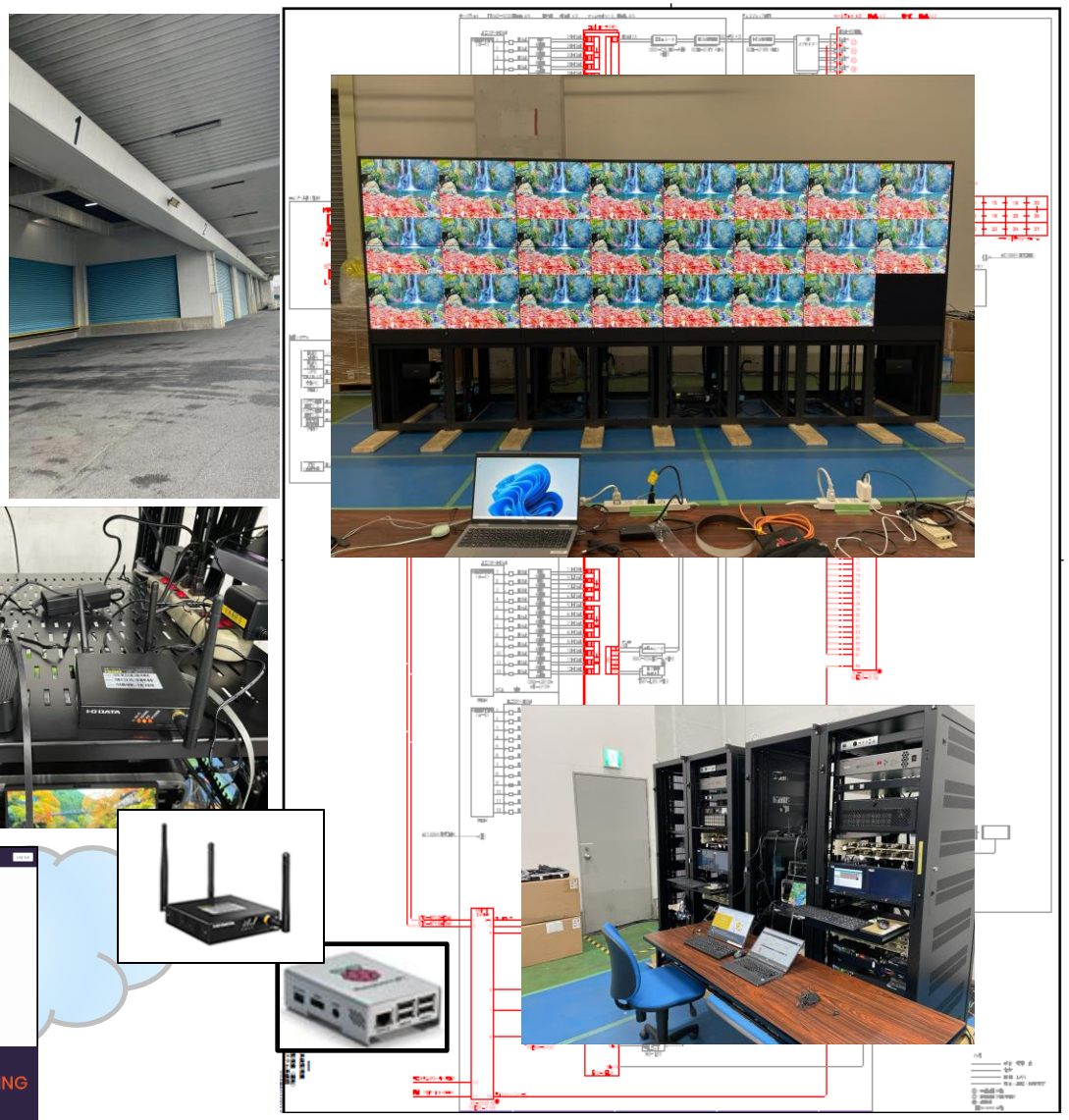
完全防備となった!!

AEGIS-EWを、NW構築の納入前品質評価で使用

未来研究所
Future Research Inc.

- 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、AEGIS-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



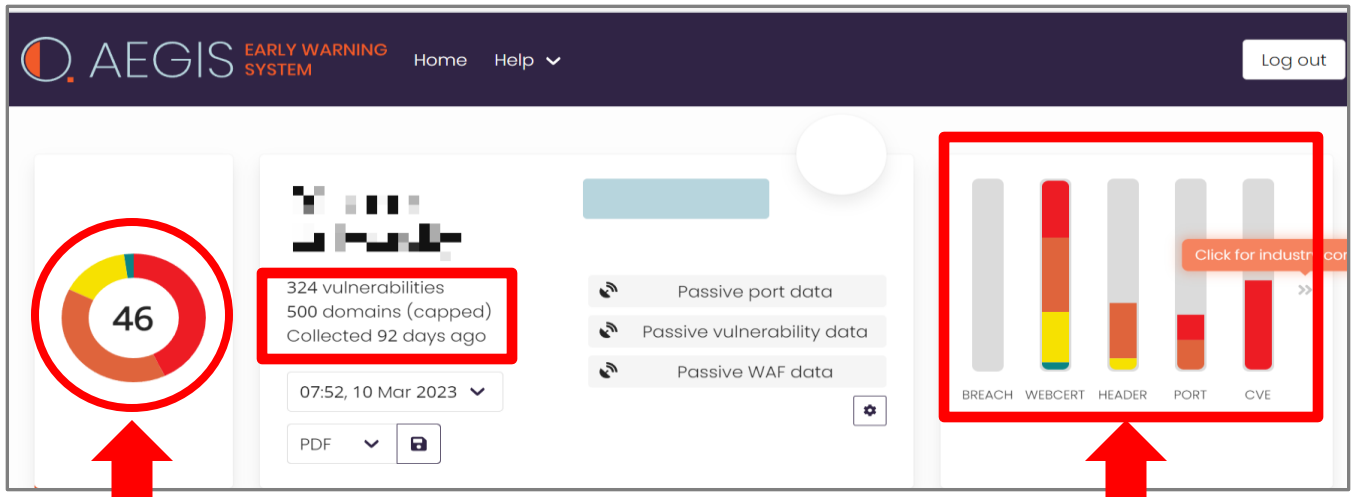


AEGIS-EW特徴：見やすいダッシュボード

未来研究所 Future Research Inc.

■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（レイティング）で示します。
なお、納品方法はについては**「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（レイティング）**（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。
色分けで理解できる！

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。

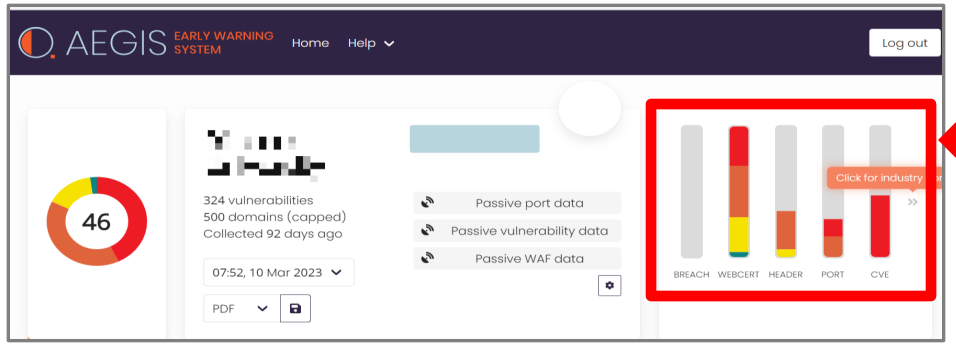
サイバーセキュリティ環境のレベル

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

AEGIS-EW特徴：脆弱性の診断分野（6分野）

未来研究所
Future Research Inc.



診断結果を、分かり易い６っの分野に識別します

分野識別	Mail	送信ドメイン認証	「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する。（SPF,DKIM,DMARCチェックもサポート）
	BREACH	データ侵害	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する
	WEBCERT	Web認証関連	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
	HEADER	HTTP関連ヘッダー関連	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、等をチェックする
	PORT	ポートスキャン攻撃	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締めておく対策が求められる
	CVE	共通脆弱性識別子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を利用している

AEGIS-EW特徴：販社/エンドユーザでの診断管理方法

- 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

- 販売店・VAR様
  - 顧客毎での管理・サポートが可能

AEGIS-EWのサイバー先進国での活用事例

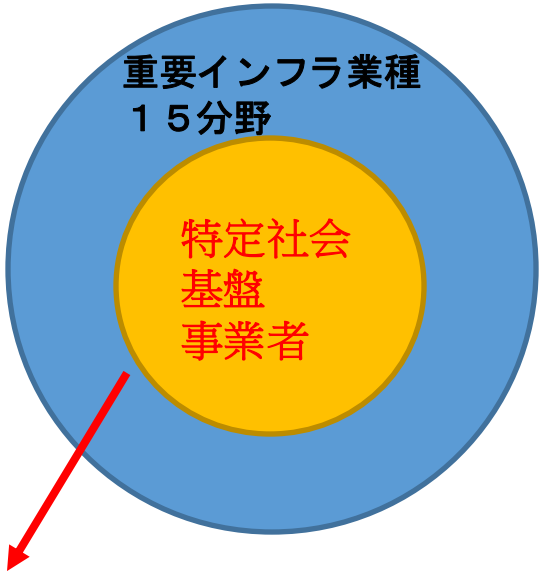
※政府系機関と業者の銀行口座維持のためには、脆弱性診断結果の提出が必須なのが
サイバーセキュリティ先進国です。下記の、米・英・オーストラリア3国を含め、
多くの国でAEGIS-EWが活用されています

- **NIST（米国立標準技術研究所）でのCSF、SP-800シリーズ適応報告書類として活用**
- NCSCNational 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？

脆弱性診断の実施が、法的にMUSTに成りました

- 経済安全保障推進法（令和４年法律第43号）
  - 公布2022/5/18，２年間の猶予期間が設定
  - 基幹インフラ役務の安定的な提供の確保に関する制度
    - 脆弱性診断が義務化
      - 法律での要件であり、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プロジェクト
    - 脆弱性診断の範囲
      - インターネット側・イントラ側等の定義は無く、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記載　**（AEGI-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分野に波及

重要インフラ業者へもNIST CSF/SP-800が適応

未来研究所 Future Research Inc.

- 内閣府指導により、政府調達資材に対し、米国基準・NIST SP800-171が適応条件となります（対象1000社から）
  - 特定社会基盤事業者はこの5月～義務化が開始
  - 重要インフラ事業者への適応も順次開始か？
- 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。

日本経済新聞

政府、サイバー対策で米基準義務付け　委託先1000社超に

23年度中に指針変更　アクセス制限や通信管理など

政府は2023年度中に業務委託先の企業に米政府基準のサイバーセキュリティー対策を義務付ける。サイバー攻撃から政府情報を守るため通信機器の管理やアクセス制限などを求める。シンクタンクや通信事業者など年間1千社以上が対象になる見通しだ。

政府のサイバーセキュリティ戦略本部が中央省庁や独立行政法人など政府に関係する機関の情報保全に関する統一基準を改める方向で調整する。外部の業務委託先に求めるサイバー攻撃対策を強化するのが柱になる。

米政府が採用するサイバー対策指針「NIST SP800-171」に沿った8項目の点検を課す。システムへのアクセス制限、アクセス権限を与える担当者の審査、リスクを定期評価する体制づくり、関係する通信の監視・管理・保護などが必要になる。

基準を満たさない企業とは業務委託契約をしない。契約後も定期的にサイバー対策状況の報告を要求する。

同指針は防衛省が取引する企業にはすでに適用している。行政のデジタル化を進めるにつれて保秘すべき情報が拡大するのを踏まえ、他省庁の業務委託先にも対象を広げる。

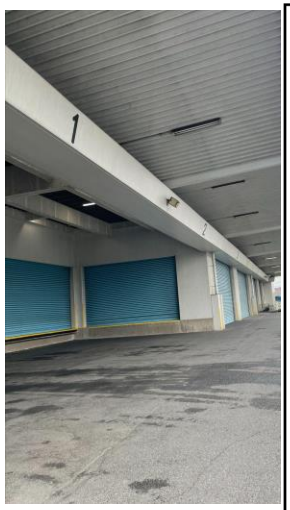
情報通信研究機構（NICT）の調査によると世界で発生したサイバー攻撃は15年から20年までの5年間で8.5倍に増えた。21～22年にかけては複数の省庁が利用する富士通のクラウドサービスが攻撃を受けた。

IoTサイバー対策認定

経産省 公共調達・補助金の要件に

AEGIS-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（ペネトレ）実施
  - 発注元からは、「納品前脆弱性診断テスト」が要件
  - 倉庫でのキッティング後の評価



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

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

（ご参考）SBOM切口での見識