イージス EW ダッシュボード

操作マニュアル

FR-USM-2025-04-001-v1.1

イージス EW ダッシュボード操作マニュアル

目次

1章　イージス EW 概要

1－1　イージス EW の機能

イージス EW は、調査対象ドメインに含まれるサーバに対して、以下の８項目の脆弱性調査を行います。

1．　Subdomain Discovery（サブドメイン調査）
2．　Mail （送信ドメイン認証）
3．　BREACH（データ侵害）
4．　Web Certs（Web 証明書）
5．　Headers（HTTP ヘッダーネゴシエーション）
6．　PORTs（サービスポート）
7．　CVE（共通脆弱性識別子）
8．　Cloud（AWS/Azure テスト）※

※　Cloud（Cloud Security Posture Management(CSPM)による AWS/Azure テスト）はペネトレーションテスト時のみ調査を行います。

1－2　深刻度の説明

イージス EW は CVSS[ii] 評価システムに基づいて、深刻度レベルが色分けで表示されます。（2024 年時点でのイージス EW 評価は CVSS3.1[iii] に準じています）

①当該ドメインの脆弱性件数

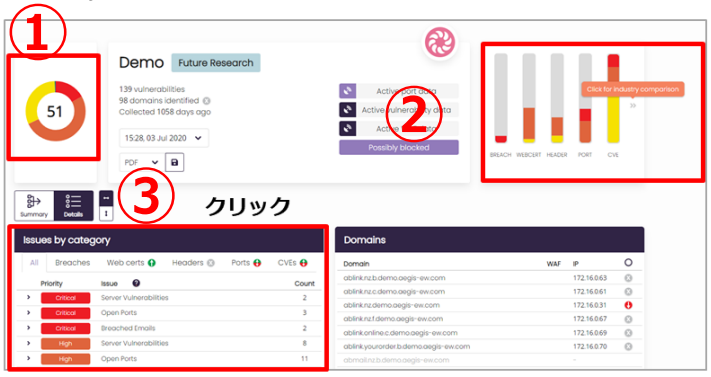
②分野別の脆弱性件数

③分野別・項目別・深刻度別の脆弱性件数

技術説明 | 操作説明

■AEGIS-EW(イージス・EW) 深刻度レベルについて

「AEGIS-EW」では、米国CERT/CC等の機関が設立したフォーラムであるFIRST（Forum of Incident Response and Security Teams)が提案した「CVSS評価システム」に基づいて深刻度レベルが表示される。図の赤枠の部分が該当の表記である。



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

１－３　総合得点の算出の仕方

100 点を満点とし、各分野の重要度に応じて配点しています。総合得点は検出された脆弱性に応じた減点法により計算されます。
また、「緊急を要する脆弱性（赤色）」が複数存在する場合、その分野のスコアは「0 点」となります。
脆弱性件数が多い場合はマイナス点が積算されるため、改修を実施しても点数が「0 点」のまま加点されない場合があります。ただし、脆弱性件数が多い場合でも、分野別の配点を超えた減点をされることはありません。

分野別の配点

CVE：３５点

PORT:１５点

BREACH：２５点

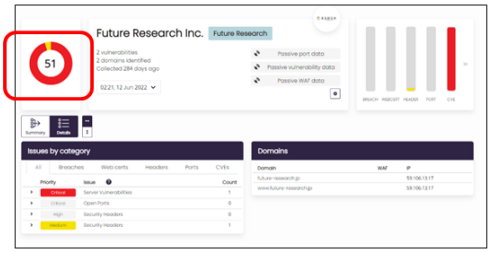
HEADER：１０点

WEBCERT：１５点

技術説明 | 操作説明

■AEGIS-EW(イージス・EW)総合得点について

総合評価の見方
100点からの減点法により表記
構成される分野と分配された点数
CVE:　　cve_composite.cost: 35
PORT :　port_composite.cost: 15
BREACH :　email_breaches.cost: 25
HEADER:　header.cost: 10
WEBCRT :　ssl.cost: 15



各脆弱性項目で定義されている深刻度（CVSS値）に基づき、配点されてます。
CVSS値が計算される基の要素数値（CVE Information Grade)が用いられます
深刻度が高い項目が多数あると、上記３５点は、０点のままとなります

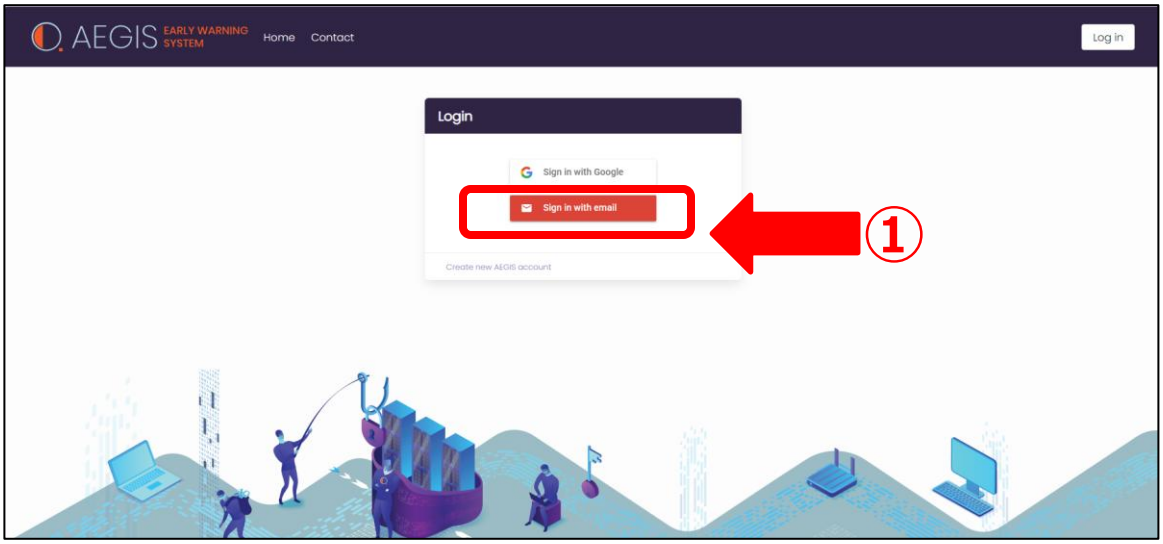
※なお、ペネトレーションテスト実施時に Cloud を含める場合は、上記の採点配分とは異なります。

2章　イージス EW 操作説明

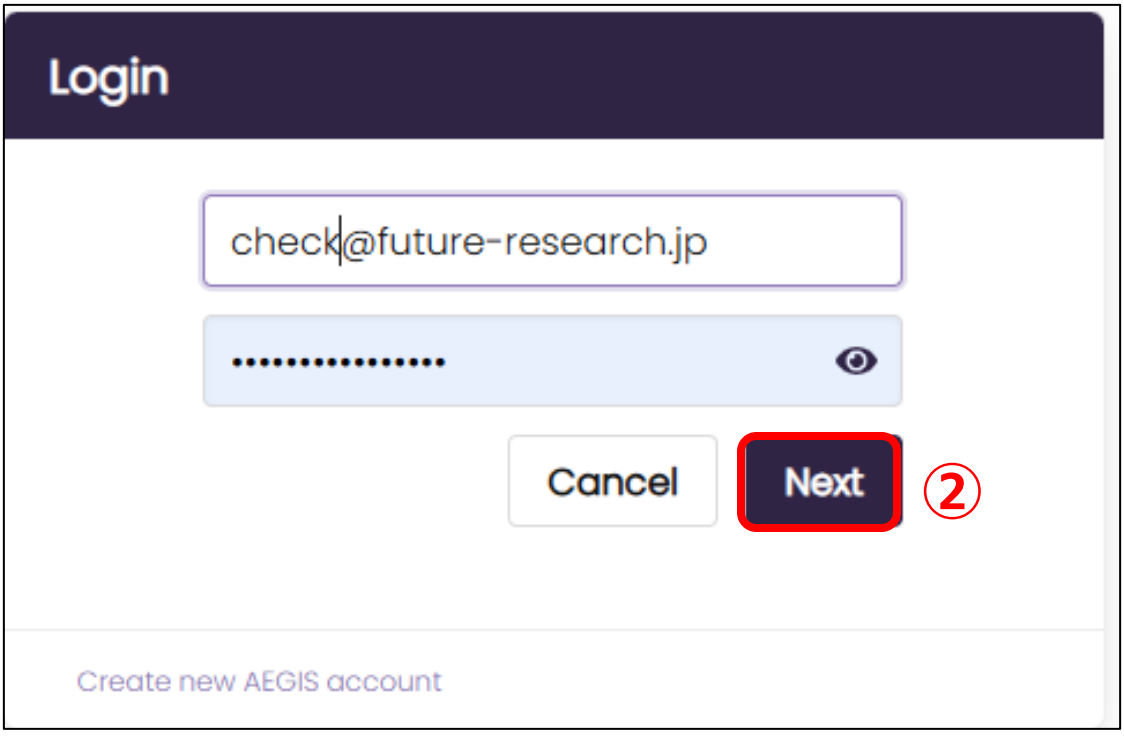
2－1　ログインの仕方

ログイン URL（https://aegis-ew.com/login/）

① 「Sign in with email」を押します。

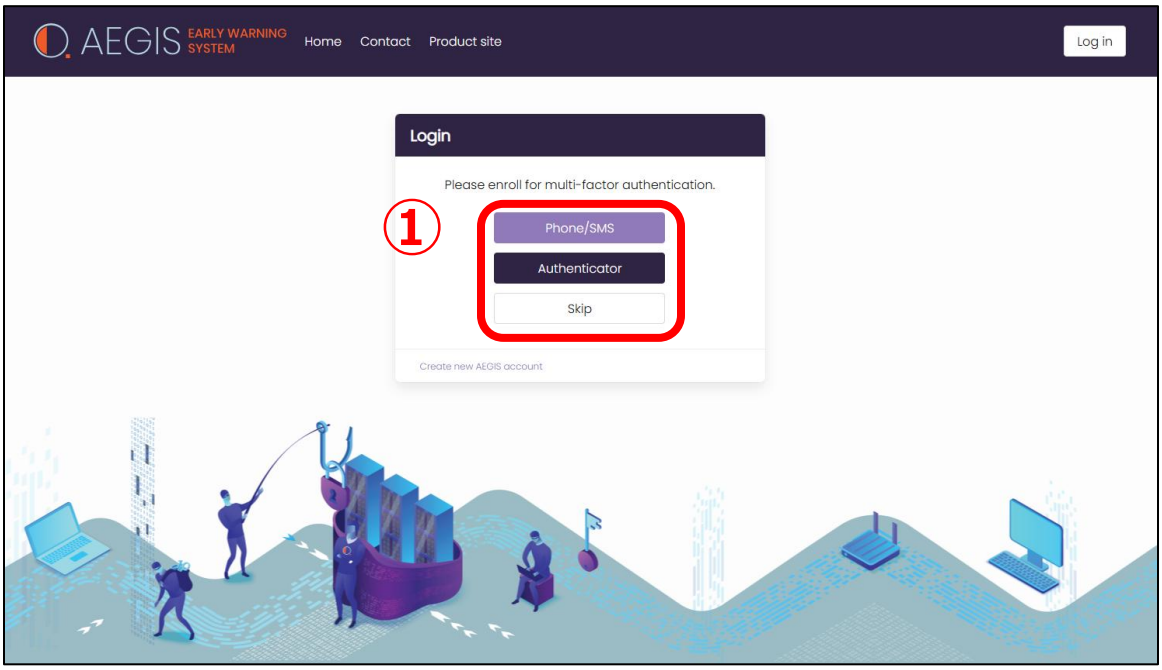


② メールアドレス・パスワードを入力し、「Next」ボタンを押します。

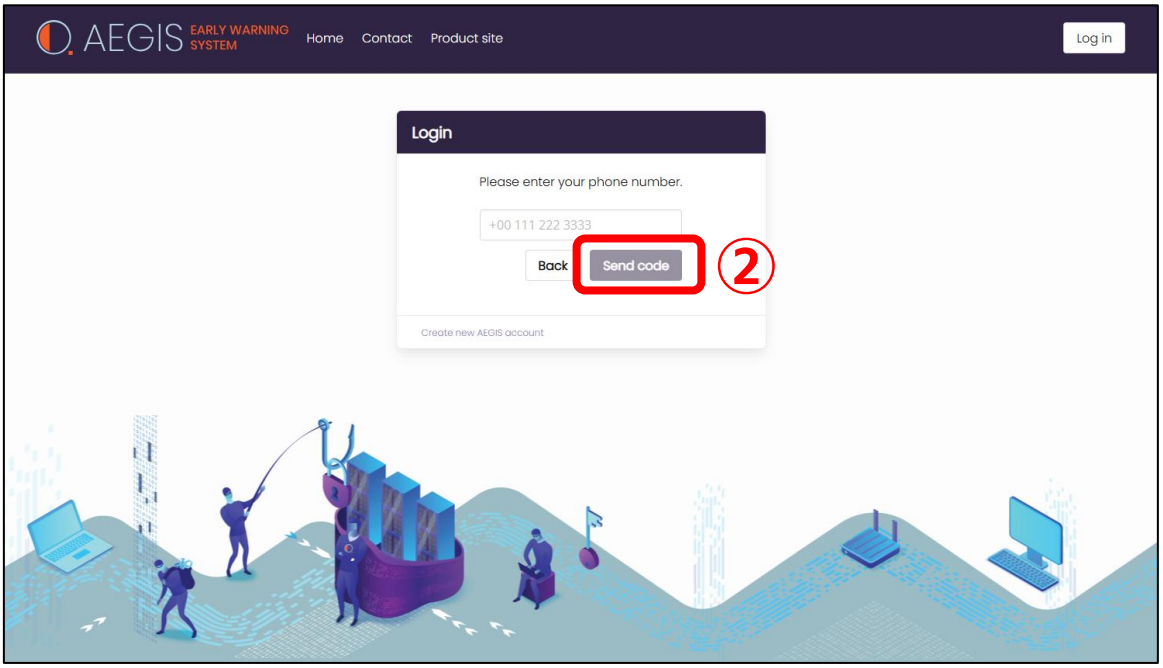


■多要素認証入力画面

① 「Phone/SMS」または「Authenticator」を押します。　（多要素認証を省略する場合は「Skip」を押します）



② 「Phone/SMS」認証の場合は、携帯電話番号を入力し「Send code」を押します。



③ 「Authenticator」認証の場合は、表示される QR コードを二要素認証用アプリで読み込みます。

2－2　ダッシュボードの概要

ログインが完了すると、ドメイン別のダッシュボードが表示されます。
イージス EW　ダッシュボード（ドメイン別）の機能は以下のとおりです。

①ドメイン別の脆弱性診断結果サマリ

ドメイン別にアイコンが表示されます。
このアイコンをクリックすることにより、各ドメイン別の脆弱性診断結果が表示されます。また、このサマリでは次の項目がサマリとして表示されます。

- 発見された脆弱性の数
- 発見されたドメイン数
- 最初の脆弱性診断日から経過した日数
- スコアリング（100 点満点中のスコア）

②表示切り替えボタン

ドメインごとにアルファベット順に表示するか、グループごとに表示するかを選択できます。

③Help ボタン

自動検出されなかったサブドメインの手動追加を依頼するボタンです。

④ログアウトボタン

このボタンをクリックして、ログアウトをします。

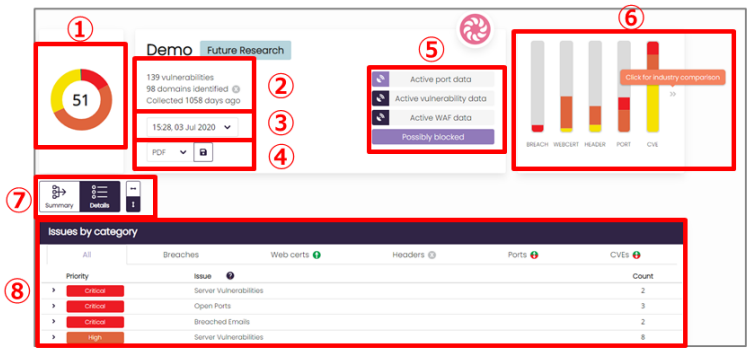
2－3　ドメイン別ダッシュボードの見方

ドメイン別のダッシュボードにおける各機能は次のとおりです。

技術説明 | 操作説明

■AEGIS-EW(イージス・EW) DashBoard機能説明(1)

「AEGIS-EW」Dash Boardの見方は次のとおり。



番号	機能名
1	脆弱性総合スコア
2	調査結果サマリ
3	調査履歴
4	レポート出力ボタン
5	スキャン方法
6	脆弱性区分
7	サマリー／詳細切り替え
8	脆弱性一覧

技術説明 | 操作説明

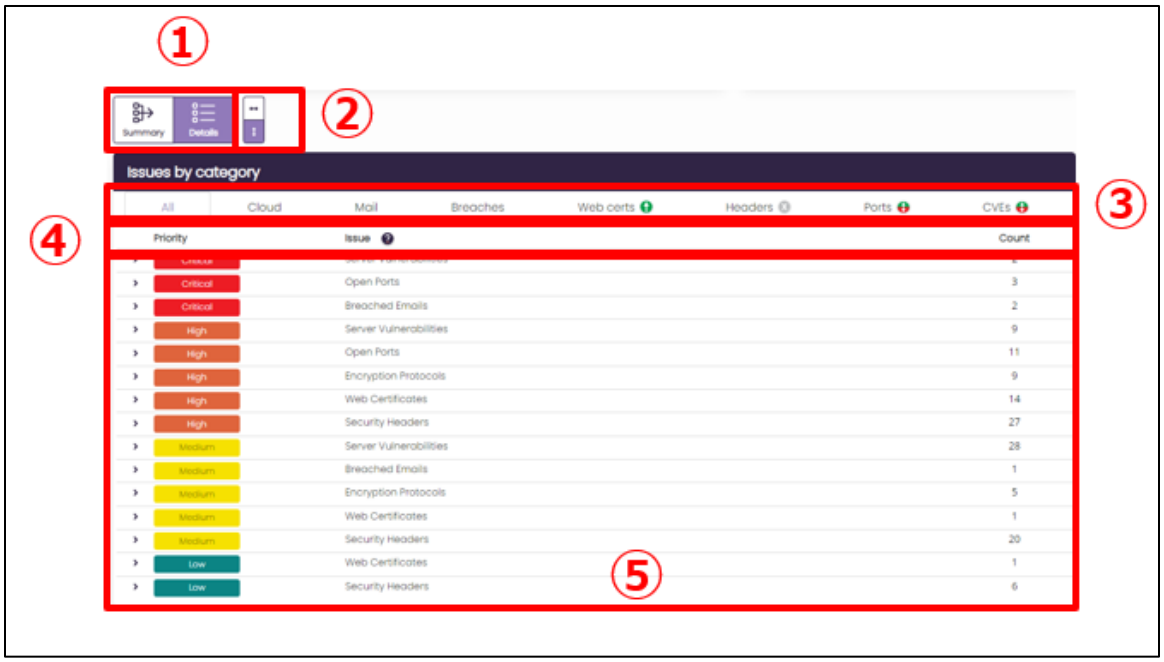
■AEGIS-EW(イージス・EW) DashBoard機能説明(２)

「AEGIS-EW」Dash Board各機能の説明は次のとおり。

番号	機能名	
1	脆弱性総合スコア	脆弱性調査を行った結果の総合得点。なお１００点満点中何点で表示される
2	調査結果サマリ	発見された脆弱性の数、調査対象サブドメイン数、調査日からの経過日数
3	調査履歴	過去に行った脆弱性調査について表示、詳細は「過去診断結果の参照」記載
4	レポート出力ボタン	レポート出力を行うことができる。詳細は「レポート出力機能」記載
5	スキャン方法	現在表示されている項目で使われたスキャン方法を表示。
6	脆弱性区分	各脆弱性区分に応じた脆弱性レベル別の分布図
7	サマリー／詳細切り替え	簡易表示・詳細表示の切り替え
8	脆弱性一覧	脆弱性調査結果の具体的な内容。詳細は、各脆弱性説明ページ内に記載

2－4　ドメイン別／IP 別脆弱性詳細情報の見方

ドメイン別／IP 別各画面では、調査対象ドメインに対して発見された脆弱性を表示します。各機能の説明は、次のとおりです。



①サマリ／詳細切り替えボタン

紫色にてハイライトされている側が現在選択されている表示形態となります。
（図では、「Details」側が選択されている）
「Summary」側では、脆弱性の分布状態を視覚的に表示します。
「Detail」側では、脆弱性がどの IP アドレスに起きているのかを表示します。

②表示位置変更ボタン（「↔」「↕」ボタン）

「ドメイン一覧」の表示位置を「脆弱性一覧」の右「↔」または下「↕」に切り替えることができます。

③脆弱性一覧別メニューバー

脆弱性一覧の分野を切り替えることができます。

④脆弱性分野別の詳細項目

項目名をクリックすることで、昇順降順を切り替えることができます。

⑤脆弱性詳細内容

分野ごと、深刻度ごとに、脆弱性の具体的内容と検出された個数が表示されます。

2－5　検出済みドメイン別／IP 別詳細情報の見方

検出済みドメイン・IP 別詳細情報欄では、WAF[iv]の有無や OS 情報を表示します。
なお、紫色にてハイライトされている部分が選択済みの項目となります。

■「Domains」が選択されている場合

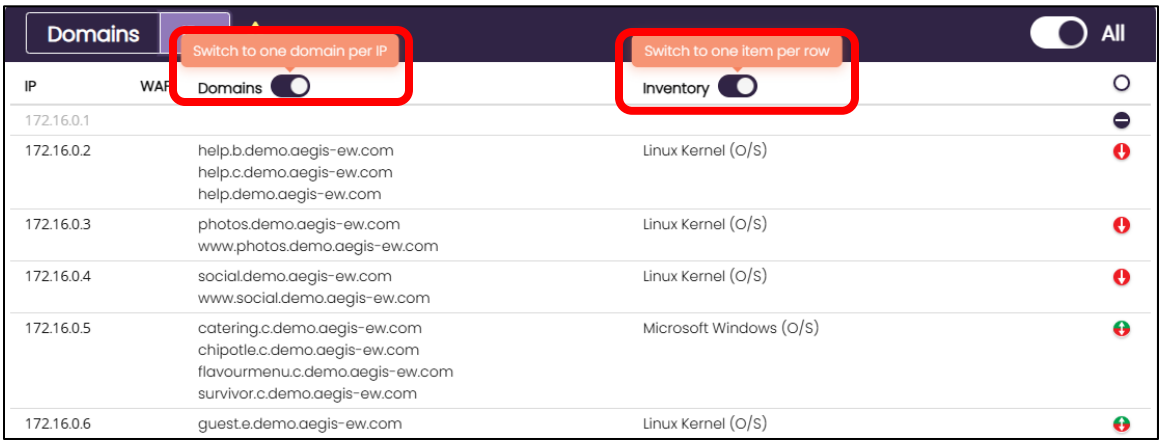
ドメイン・WAF・Address Records・（Inventory　ペネトレーションテストのみ）、スコアリング変動（赤：低下、緑：上昇）の順番で表示されます。

■「IPs」が選択されている場合

IP・WAF・ドメイン・（Inventory　ペネトレーションテストのみ）、スコアリング変動（赤：低下、緑：上昇）の順番で表示されます。この際に、表示結果上部の項目をクリックすることで、昇順降順にソートすることができます。

また、「IPs」が選択されている場合に、Domains・Inventory 欄に表示されているスイッチをクリックして切り替えることで、一行 1 件表示と複数行全権表示を切り替えることができます。

・表示の例（「IPs」が選択済みの場合」）

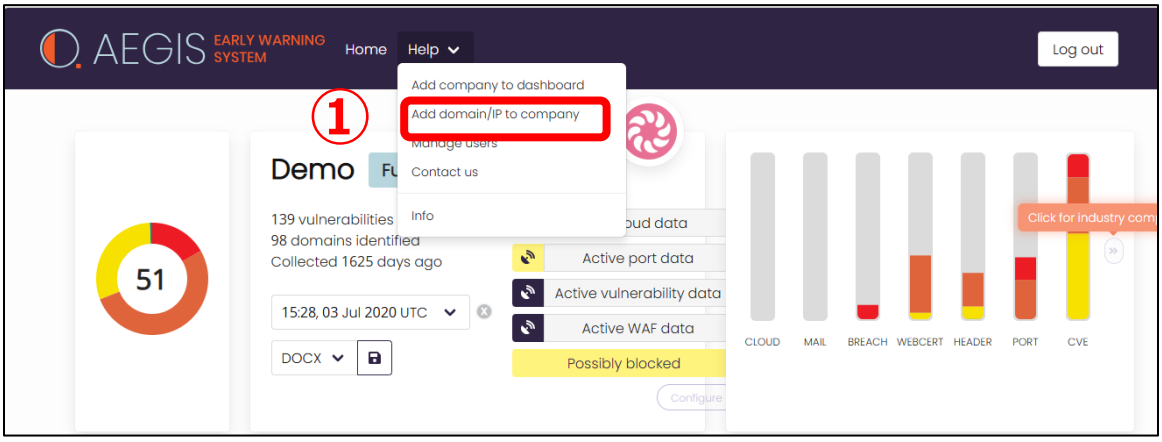


2－6　新規ドメインの追加（add ip /domain to company）

前提として、イージス EW はベストエフォート型サービスであり、次回テストから、追加したサブドメインの診断が行われます。登録された新規 IP アドレス・ドメインは、次回テスト時に「New IP」で追加されます。

■新規サブドメイン／IP の追加方法

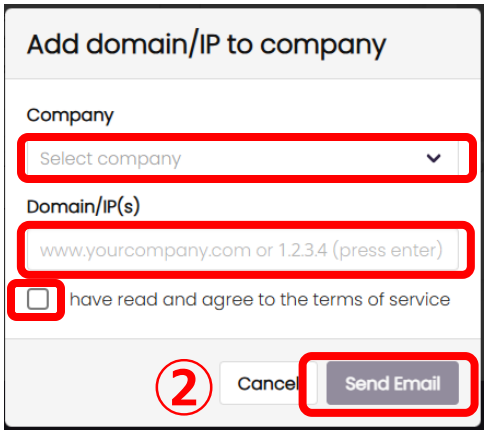
①ダッシュボード上部の「Help」をクリックし「Add domain/IP to company」をクリックします。



②ポップアップで表示されるフォームに Company・追加する Domain を入力し、

「I have read and agree to the terms of service」にチェックを入れ、

「Send Emal」ボタンを押してください。



3章　イージス EW 脆弱性分野別操作方法

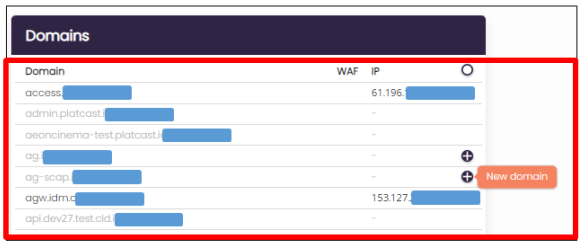
3－1　Subdomain Discovery 機能

「ドメイン一覧」には、以下のように、サブドメインと IP アドレスの組み合わせが表示されます。

技術説明 | 操作説明

■Domain Discovery機能

Whois, DNSサーバ群の調査に基づき、公開ドメインに対して「閉じ忘れたIPアドレス等を含むサブドメイン（野良IP・ゾンビ端末と呼ばれる）」があるか否かを調査を行う。これは、「野良IP」から正規ネットワークへの侵入を許し、各種サイバー攻撃を防ぐ効果がある。



サブとメインとIPアドレスの組み合わせが表示される

「Domains」ボタンを押すと、左側から「ドメイン・WAF・Adress Records・Inventory」の順に表示されます。

「IPs」ボタンを押すと、左側から「IP・WAF・Domains・Inventory」の順に表示されます。

3 – 2　Mail （送信ドメイン認証）

①　「Issues by category（脆弱性一覧）」から「Mail」をクリックします。

②　SPF／DKIM 対応状況が表示されます。

③DMARC の対応状況が表示されます。

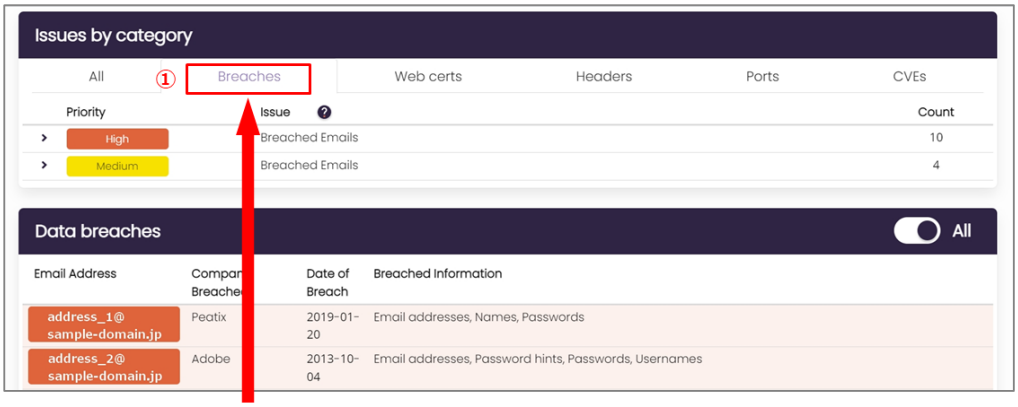
3 – 3　BREACH（データ侵害：情報漏洩）

■イージス EW 上での BREACH 確認方法

①「Issue by category」の項目から「BREACH」をクリックして選択します。

■「AEGIS-EW」上でのBREACH確認方法(1)

技術説明 操作説明

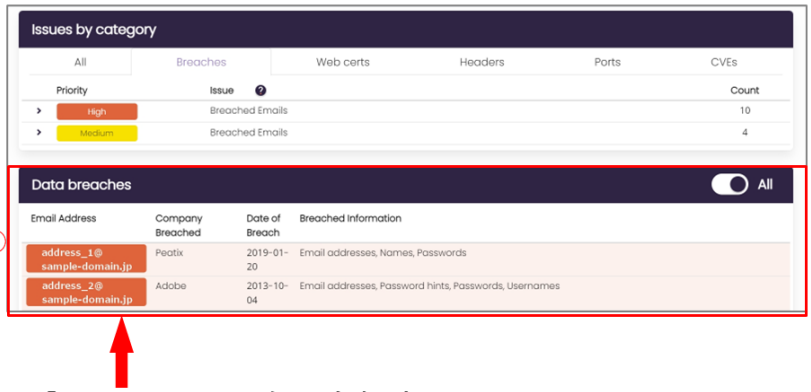


①「BREACH」をクリック

②「Data breaches」の各項目を確認します。

■「AEGIS-EW」上でのBREACH確認方法(2)

技術説明 操作説明



②「Data breaches」の各項目を確認する

■BREACH 項目一覧

①Email Adress　調査対象ドメイン

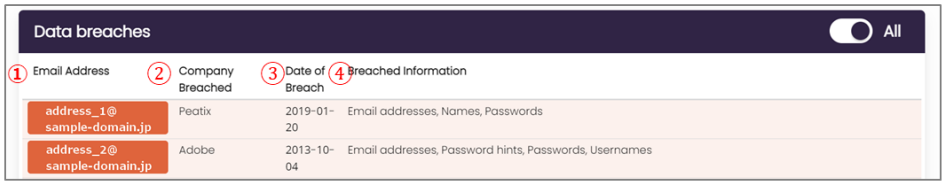
②Company Breached

③Date of Breach

④Breached Information

■BREACH　項目一覧

技術説明 | 操作説明



番号	項目名	説明
1	Email Address	調査対象ドメイン内で、データ侵害が確認されたメールアドレス
2	Company Breached	データ侵害の原因となった流出元サービス名
3	Date of Breach	データ侵害が確認された日付
4	Breached Information	データ侵害が発生した際に該当サービスで流出した情報区分

■BREACH 裏付けの確認方法（https://haveibeenpwned.com/）

①メールアドレスを入力する

②「Pwnwd?」ボタンをクリック

③対象メールアドレスを確認

■BREACH　裏付けの確認方法

技術説明 | 操作説明

BREACHの対象になっているメールアドレスについては、裏付け確認をすることができる。
今回、一例として「Have I Been Pwned?(https://haveibeenpwned.com/)」の場合を示す。

3－4　Web Certs（Web 証明書）

■脆弱性のあるサーバ証明書の種類

①期限切れの証明書：期限が切れている証明書は信頼性が失われたものと見なします。

②自己署名証明書：自己署名証明書は、信頼できる認証局（CA）によって署名されていないため脆弱性があります。

③署名アルゴリズムの脆弱性：DSA などの古い署名アルゴリズムは、攻撃者が秘密鍵を解読することができます。RSA2048 および 4096bit の RSA、または EdDSA を推奨します。

④暗号アルゴリズムセットの脆弱性：SSL/TLS プロトコルに使用される暗号アルゴリズムセットの脆弱性がある場合、攻撃者は暗号化通信を解読し、機密情報を取得することができます。

■「Web Certs（Web 証明書）」脆弱性調査結果画面の見方

「Issue by category」の項目から「Web Certs」をクリックして選択します。

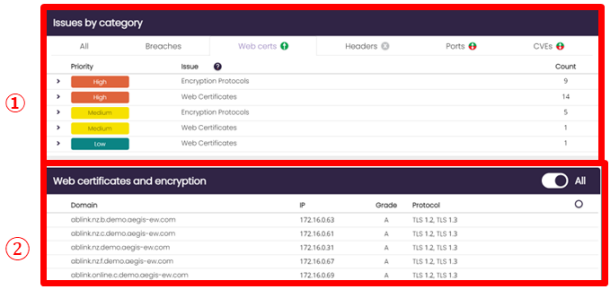
①「Issue by category」：ドメインごとの脆弱性深刻度の区分と分布について表示します。

②「Web Certificates and Encryption」：サーバ証明書に対する調査結果と対応する暗号化プロトコルについて表示します。

技術説明 | 操作説明

■Web Cert脆弱性結果画面について

「AEGIS-EW」における、サーバ証明書脆弱性調査結果画面の見方は次のとおり



番号	項目名	説明
1	Issue by category	ドメインごとの脆弱性深刻度の区分と分布について表示
2	Web Certificates and Encryption	サーバ証明書に対する調査結果と対応する暗号化プロトコルについて表示

■「Issue by category」詳細表示操作について

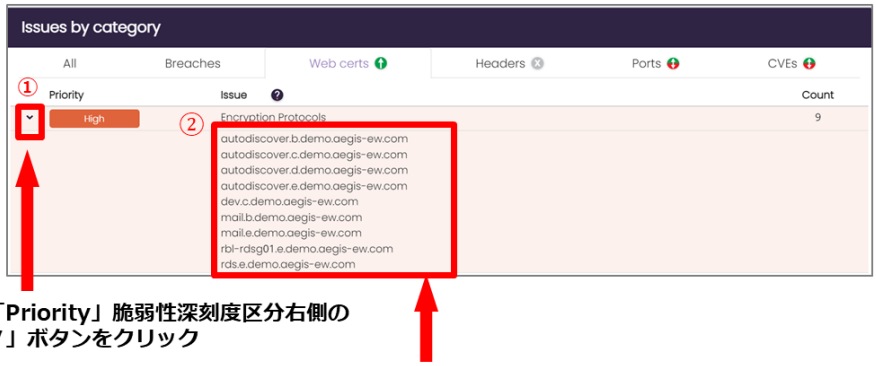
「Priority（脆弱性深刻度区分）」左側の「＞」ボタンをクリックします。

脆弱性を含む証明書が使用されているドメインの詳細を確認します。

技術説明 操作説明

■Web Cert脆弱性調査結果画面　詳細表示操作について

「Issue by category」サーバ証明書脆弱性調査結果画面にて詳細表示方法は次のとおり



①「Priority」脆弱性深刻度区分右側の「V」ボタンをクリック

②脆弱性を含む証明書が使用されているドメインの詳細を確認

■「Issue by category」表示結果画面の各項目について

①Priority　脆弱性深刻度区分

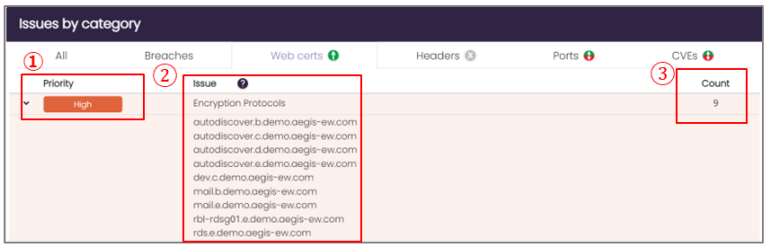
②Issue　脆弱性種別

③Count　該当ドメインに含まれる脆弱性の数

技術説明 操作説明

■「AEGIS-EW」サーバ証明書脆弱性調査結果画面

「Issue by category」サーバ証明書脆弱性調査結果画面の各機能は次のとおり



番号	項目名	説明
1	Priority	脆弱性深刻度の区分「Critical」「High」「Middle」「Low」
2	Issue	脆弱性種類(例では、Encryption Protocol」)および該当ドメイン一覧
3	Count	該当ドメインに含まれる脆弱性の数

■「Web Certificates and Encryption」詳細表示操作について

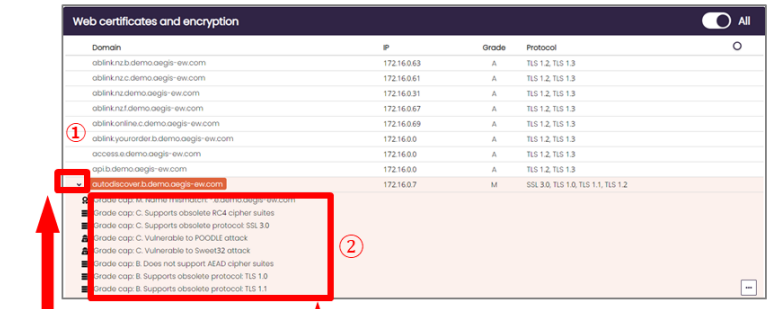
「Domain（ドメイン）」左側の「＞」ボタンをクリック

脆弱性を含む証明書の詳細を確認します。

技術説明 操作説明

■Web Cert脆弱性調査結果画面　詳細表示操作について

「Web Certificates and encryption」サーバ証明書脆弱性調査結果画面にて詳細表示方法は次のとおり



①「Domain」区分右側の「V」ボタンをクリック

②脆弱性を含む証明書の詳細を確認 脆弱性の理由が記載されている

■「Web Certificates and Encryption」表示結果画面の各項目について

①Domain　調査対象のドメイン一覧と証明書の評価結果

②IP　該当ドメインの名前解決後 IP アドレス

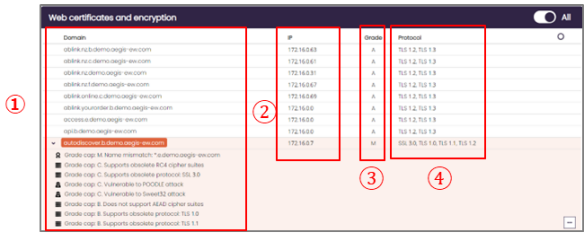
③Grade　証明書を評価した結果のグレード他

④Protocol　証明書が対応している暗号化アルゴリズム

技術説明 操作説明

■「AEGIS-EW」サーバ証明書脆弱性調査結果画面

「Web Certificates and Encryption」サーバ証明書脆弱性調査結果画面の各機能は次のとおり



番号	項目名	説明
1	Domain	調査対象のドメイン一覧と証明書の評価結果
2	IP	該当ドメインの名前解決後IPアドレス
3	Grade	証明書を評価した結果のグレード値。詳細は後述
4	Protocol	証明書が対応している暗号化アルゴリズム

■サーバ証明書脆弱性調査結果画面の見方

①ドメインネーム照合結果

②暗号化プロトコル評価結果

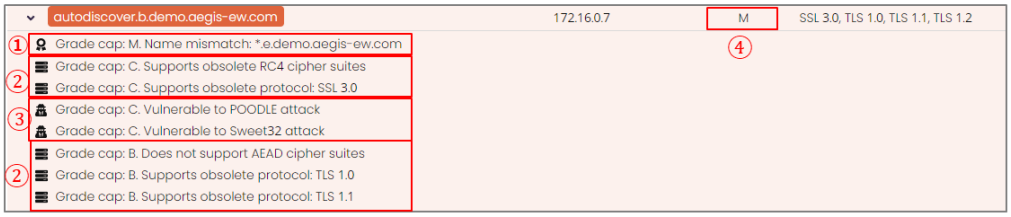
③証明書に含まれる脆弱性結果

④サーバグレード表示

技術説明 操作説明

■Web Cert脆弱性結果画面について

「AEGIS-EW」における、サーバ証明書脆弱性調査結果画面の見方は次のとおり



番号	項目名	説明
1	ドメインネーム照合結果	サーバー証明書内に記載されているドメイン名と実ドメイン名との比較結果
2	暗号化プロトコル評価結果	サーバ証明書が対応している暗号化プロトコルについての評価結果
3	証明書に含まれる脆弱性結果	サーバ証明書に含まれる脆弱性を利用して攻撃者が攻撃する場合の攻撃名
4	サーバーグレード表示	サーバ証明書に含まれる脆弱性のうち最も深刻なもののグレード記号を表示

■イージス EW における、サーバ証明書グレードの評価方法

技術説明 操作説明

■サーバ証明書グレードについて

「AEGIS-EW」における、サーバ証明書グレードの評価方法は次のとおり（参照元：https://www.ssllabs.com/ ）

まず、下記の4つのカテゴリについて評価する。

①証明書の有効性

②サポートされている証明書署名プロトコル

③鍵交換の対応状況

④対応している暗号アルゴリズム

各カテゴリごとにスコアをつけ、合計スコア（0～100の範囲で表示）で算出。（ただし、各カテゴリで0点がある場合、合計スコアも0点）これに加えて、数値スコアだけでは表現できないサーバー構成の特徴を評価するため、グレード（A-、B、C、D、E、またはF）を付与する。優れた構成が評価される場合、「 A+ 」のように元のグレードに「+」を付与する場合がある。

特定の状況下では、通常のA～Fグレードを使用しない。この場合は、「Mグレード（証明書名の不一致）」や「Tグレード（サイト証明書が信頼されていない）」という表記を用いる。証明書が信頼されていない場合、悪意ある攻撃者が接続セキュリティを破壊できる可能性があるため、実際のセキュリティ等級は重要ではなくなります。このように、サーバ証明書の格付けは複数の要素を総合的に評価して適切なグレードを付与する。これによりサーバのセキュリティ状況を把握できるようになる。

■イージス EW における、サーバ証明書グレード評価ポイント

技術説明 | 操作説明

■サーバ証明書グレードについて

「AEGIS-EW」における、サーバ証明書グレード評価ポイント説明はつぎのとおり
（参照元： https://www.ssllabs.com/ ）

番号	項目名	説明
1	証明書自体の有効性	①サーバ証明書内に記載されているドメイン名と実ドメイン名との比較結果 ②サーバ証明書内に記載されている有効期限の確認 ③サーバ証明書内に記載されている認証局署名の確認 ④自己署名サーバ証明書であるかの確認
2	証明書プロトコルのサポート状況	サーバ証明書が対応している暗号化プロトコルについての評価結果
3	鍵交換対応状況	サーバ証明書が対応している鍵交換アルゴリズムについての確認
4	暗号アルゴリズム対応状況	サーバ証明書が対応している暗号化アルゴリズムについての確認

■イージス EW における、サーバ証明書グレードスコアリング区分

技術説明 | 操作説明

■サーバ証明書グレードについて

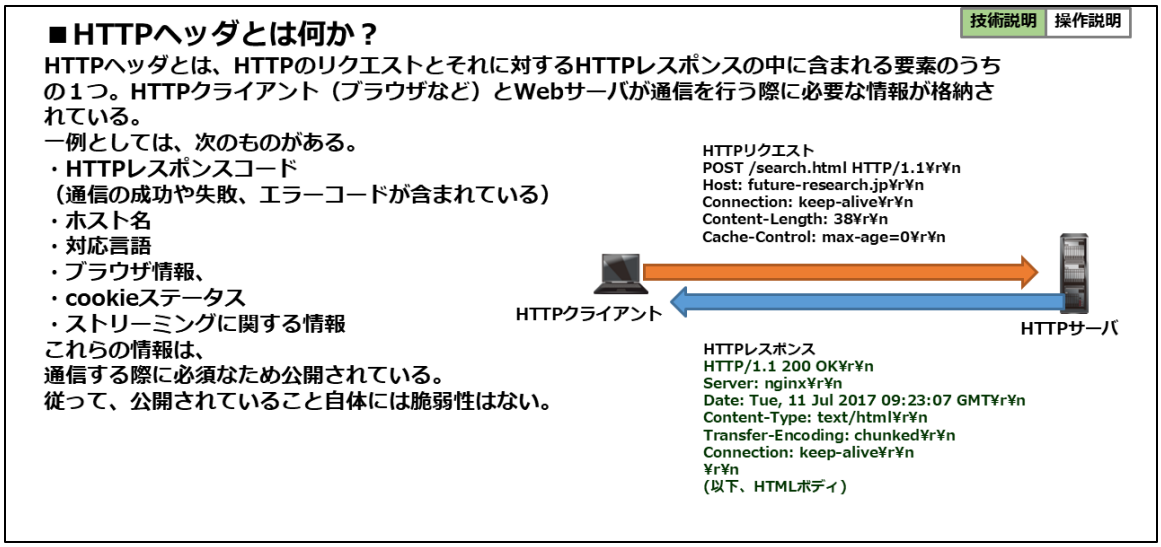
「AEGIS-EW」における、サーバ証明書グレードスコアリング区分は以下のとおり

番号	スコア区分	グレード	備考
1	score >= 80	A	
2	score >= 65	B	
3	score >= 50	C	
4	score >= 35	D	
5	score >= 20	E	
6	score < 20	F	
7	なし	M	証明書名の不一致（証明書と実ドメイン名が違う）
8	なし	T	証明書が信頼されていない（自己署名証明書）

3－5　HTTP ヘッダ

■HTTP ヘッダとは

HTTP ヘッダとは、HTTP のリクエストとそれに対する HTTP レスポンスの中に含まれる要素のうちの１つです。HTTP クライアント（ブラウザなど）と Web サーバが通信を行う際に必要な情報が格納されています。



また、HTTP ヘッダには、セキュリティヘッダー（CSP: Content-Security-Policy, HSTS: HTTP Strict Transport Security など）と呼ばれる Web サーバとクライアント（Web ブラウザ）間の通信を安全に行うための情報が含まれています。
これらが不足している場合には、XSS（クロスサイトスクリプティング）や MITM(Man-In-The-Middle:中間者盗聴攻撃)を受けやすくなります。

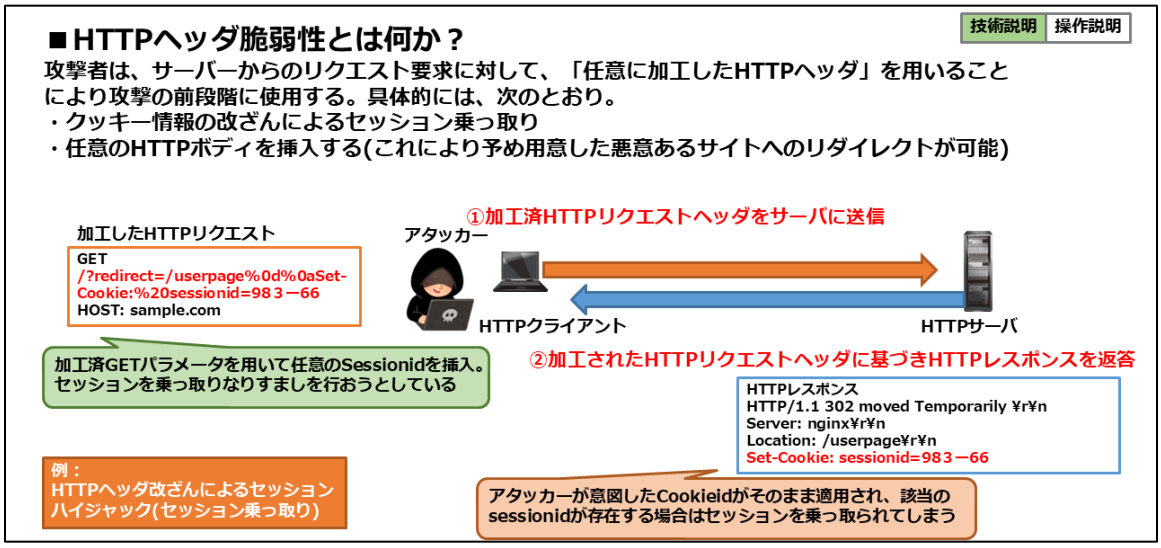
■HTTP ヘッダ脆弱性とは

イージス EW では、Web サーバとブラウザ間の通信において、欠落している HTTP セキュリティヘッダの有無を確認します。不足している HTTP セキュリティヘッダが存在する場合には、各サブドメインごとに一覧を表示します。

■ペネトレーションテストにおける HTTP ヘッダー脆弱性調査

また、イージス EW ペネトレーションテストでは、HTTP セキュリティヘッダの不足を検出するだけでなく、HTTP ヘッダにおけるエスケープ処理の不足を突いた攻撃をシュミレーションして脆弱性を発見します。

攻撃シナリオの例：
攻撃者は、サーバからのリクエスト要求に対して、「任意に加工した HTTP ヘッダ」を用いることにより攻撃の前段階に使用します。



■イージス EW での Headers 脆弱性画面の見方

「Issue by category」の項目から「Headers」をクリックして選択します。

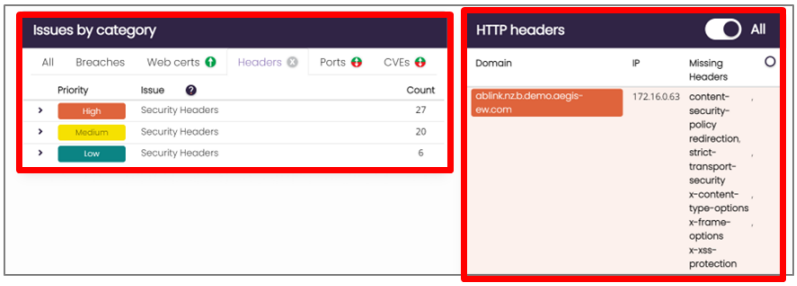
①Priority　脆弱性深刻度の区分

②Http headers　脆弱性調査を行った結果の HTTP ヘッダ情報

技術説明 | 操作説明

■AEGIS-EW上でのHeaders脆弱性画面の見方

Headers脆弱性画面の見方は次のとおり



番号	項目名	説明
1	Priority	脆弱性深刻度の区分「Critical」「High」「Middle」「Low」および、各脆弱性深刻度の数
2	Http headers	脆弱性調査を行った結果のHTTPヘッダ情報

■「Issue by category」欄では、各脆弱性深刻度の左側「＞」をクリックすることによって、各脆弱性深刻度に含まれるサブドメインを確認することが可能です。
脆弱性区分ごとに含まれるサブドメインが表示されます。

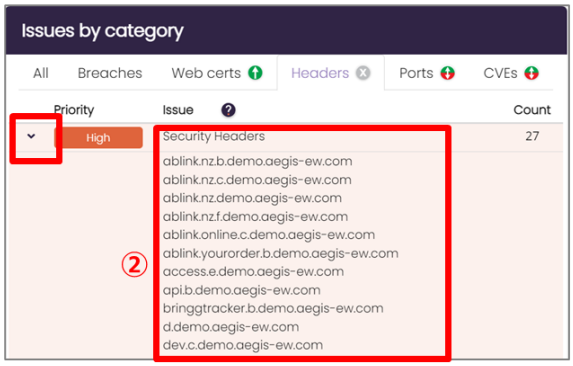
技術説明 | 操作説明

■AEGIS-EW上でのHeaders脆弱性画面の見方

「Issue by category」欄では、各脆弱性レベルの右側「V」をクリックすることによって、角度脆弱性レベルに含まれるサブドメインを確認することが可能

①脆弱性レベル表示左側「V」をクリック

②画脆弱性区分ごとに含まれるサブドメインが表示される



3－6　PORTs（サービスポート）

■ポートとポートスキャン

ネットワーク上でサービスを提供するソフトウェアには、「ポート」と呼ばれる通信に用いられる窓口を介して行われます。ポートは番号で管理されており、サービスを提供するソフトウェアごとに固有の番号が割り当てられます。（デフォルト設定時）

攻撃者は、脆弱性のあるサーバを見つけるためにポートスキャンという手法を用います。

ポートスキャンとは、実際にデータを送ってサービス稼働状況を外部から調査することです。

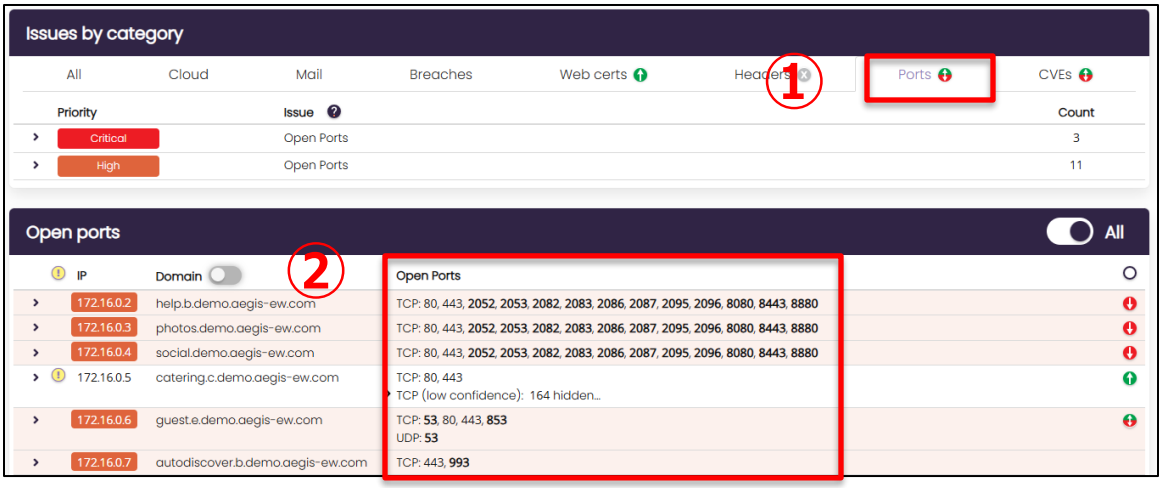
サービスを提供するソフトウェアごとに固有のポート番号があり、稼働中のサービスを特定することができます。

なお、ポートスキャン自体は、既に公開されているサービスポートに対して、正常な通信データを送っているため違法行為ではありません。

■「PORTs（サービスポート）」脆弱性調査結果画面の見方

①「Issue by category」の項目から「PORTs」をクリックして選択します。

②「Open ports」に各 IP のオープンポートが表示されます



■狙われやすいポート一覧

技術説明 操作説明

■狙われやすいポート一覧

ポート番号	プロトコル	サービス名	狙われやすさ	用途および備考
22	TCP	SSH	特大	rootログインの禁止。証明書を使用した接続の強制。サーバ側で運用ポート番号の変更を推奨
25	TCP	SMTP	中	SMTPs(port 465)の利用を推奨
53	UDP	DNS	大	名前解決用。不必要なDDNSサービスは停止すること
80	TCP	HTTP	中	HTTPS(port 1－3)の利用を推奨
110	TCP	POP3	中	POP3s(port 995)の利用を推奨
123	UDP	NTP	中	時刻同期用
143	TCP	IMAP4	中	IMAP4s(port 993)の利用を推奨
1－3	TCP	HTTPS	中	通常のWeb閲覧やWebサービス用
465	TCP	SMTPs	中	メール送信用(SMTP over SSL)
587	TCP	Submission	中	SMTPs(port 465)の利用を推奨
993	TCP	IMAP4s	中	IMAP形式のメール閲覧用(IMAP4 over SSL)
995	TCP	POP3s	中	メール受信用(POP3 over SSL)

■外部公開禁止ポート一覧

技術説明 操作説明

■外部公開禁止ポート一覧

ポート番号	プロトコル	サービス名	危険度	備考
20	TCP,UDP	FTP-data	特大	FTPサービスを閉じて、SFTPへの移行を推奨
21	TCP,UDP	FTP	特大	FTPサービスを閉じて、SFTPへの移行を推奨
23	TCP	Telnet	特大	Telnetサービスを閉じて、SSHへの移行を推奨
67	TCP,UDP	BOOTP	中	公開サービスとせず、IPSecと併用してローカルサービスとして稼働を推奨
70	TCP,UDP	Gopher	中	
79	TCP,UDP	Finger	大	Fingerサービスを閉じて、他のグループウェア等への切り替えを推奨
111	TCP,UDP	SunRPC	中	
137-139	TCP,UDP	NetBIOS	大	公開サービスとせず、IPSecと併用してローカルサービスとして稼働を推奨
512	TCP,UDP	Rexec(TCP),biff(UDP)	大	Rexecサービスを閉じて、SSHへの移行を推奨
513	TCP,UDP	rlogin(TCP),Who(UDP)	大	公開サービスとせず、IPSecと併用してローカルサービスとして稼働を推奨
520	UDP	Router	中	
1080	TCP	SOCKS	中	
2049	TCP,UDP	NFS	大	公開サービスとせず、IPSecと併用してローカルサービスとして稼働を推奨
4000	TCP,UDP	Terabase	中	
6000～6063	TCP,UDP	X Window System	中	公開サービスとせず、IPSecと併用してローカルサービスとして稼働を推奨
7070	TCP,UDP	ARCP	中	
8080	TCP	HTTP Alternative Services	中	
26000	TCP,UDP	Quake	中	
27910	TCP,UDP	Quake2	中	

3－7　CVE（共通脆弱性識別子）

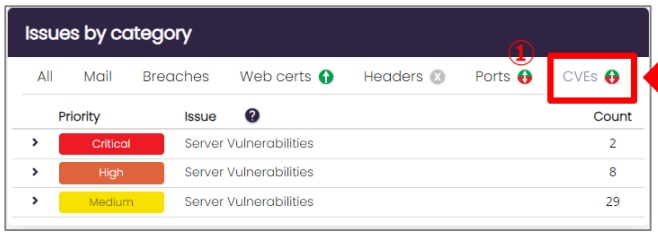
■イージス EW における CVE 番号の分析方法

「Issue by category」の項目から「CVEs」をクリックして選択します。

技術説明 | 操作説明

■AEGIS-EWにおけるCVE確認方法（１）

AEGIS-EWにおけるCVE番号を確認した以降の分析方法については次のとおり



①「Issue by category」の項目から、「CVEs」を選択

②画面右側に「Server vulnerabilities」が表示されます。

技術説明 | 操作説明

■AEGIS-EWにおけるCVE確認方法（２）

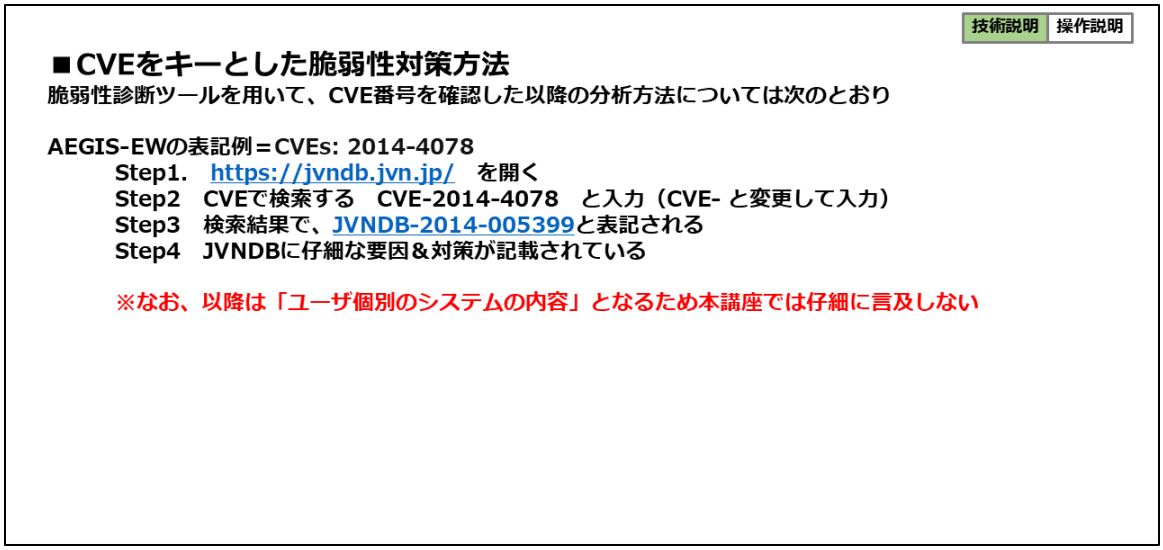
AEGIS-EWにおけるCVE番号を確認した以降の分析方法については次のとおり

①画面右側に「Server vulnerabilities」が表示される。
なお、それぞれの項目の意味は次のとおり

番号	項目名	説明
1	IP	各ドメインに紐付いたIPアドレス
2	Domain	IPアドレスからDNS逆引きしたドメイン名
3	Vulnerabilities Found	脆弱性の一覧。 なお、ここでは二つのテストを行っている ①脆弱性検出エンジンである「OpenVas」が定義した NVT（Network Vulnerability Tests）で不合格とされた項目 「NVTs-A****」で表示される。 ②CVEに基づくテスト 「CVEs-YYYY-****」で表示される

■検出されたＣＶＥの分析方法

JVN iPedia「脆弱性対策情報データベース」（https://jvndb.jvn.jp/）にて検索・分析が可能です。



※なお、ペネトレーションテストを実施することにより CVE が確定するため、イージス EW ペネトレーションテスト実施後、ダッシュボード上の CVE 番号にマウスカーソルを乗せると詳細が表示されます。

3－8　CLOUD

■CSPM（Cloud Security Posture Management）

CSPM（Cloud Security Posture Management）は、クラウド環境におけるセキュリティポスチャー（セキュリティの状態）を管理、監視、改善するためのプロセスを指します。これにより、クラウドインフラの設定や運用の中で発生するリスクや脆弱性を発見し、迅速に対処することができます。

CSPM は、AWS や Azure、Google Cloud などのクラウドサービスにおける設定ミスや脆弱性を自動的に検出し、それらのリスクを最小化するために必要なアクションを提案します。これにより、企業はクラウドサービスの管理が複雑になりがちな中で、セキュリティのベストプラクティスに沿った運用を確保することができます。

■CLOUD 診断

イージス EW の CLOUD 診断は、イージス EW ペネトレーションテスト時のみ実施可能です。2024 年 4 月時点では Amazon AWS、 Microsoft Azure、の診断が可能で、Google Cloud も実装予定です。

CLOUD 診断は、クラウド環境のセキュリティ状態を包括的に評価・診断するためのセキュリティアセスメントツールです。特に以下のような目的で使用されます。

・セキュリティ評価

・アカウントの設定が「セキュリティのベストプラクティス」に従っているかを確認

・潜在的なセキュリティリスクの発見

・セキュリティ設定の不備を検出

・組織のセキュリティポリシーへの準拠状況を確認

・業界標準（CIS、HIPAA、GDPR など）への準拠状況を評価

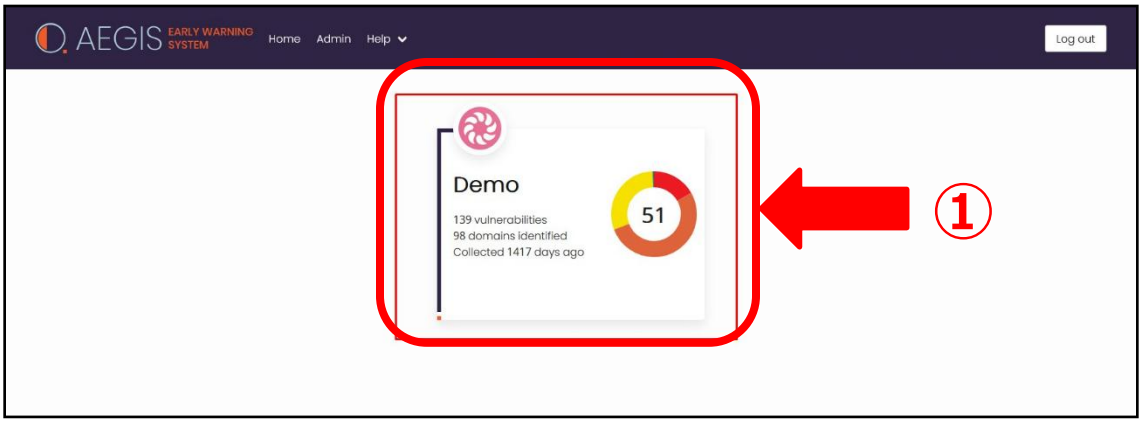
・監査のためのエビデンス収集

なお、これらの調査は、AWS の場合、予め Amazon によって明示的に許可された範囲のみ診断を行うように設計されています。

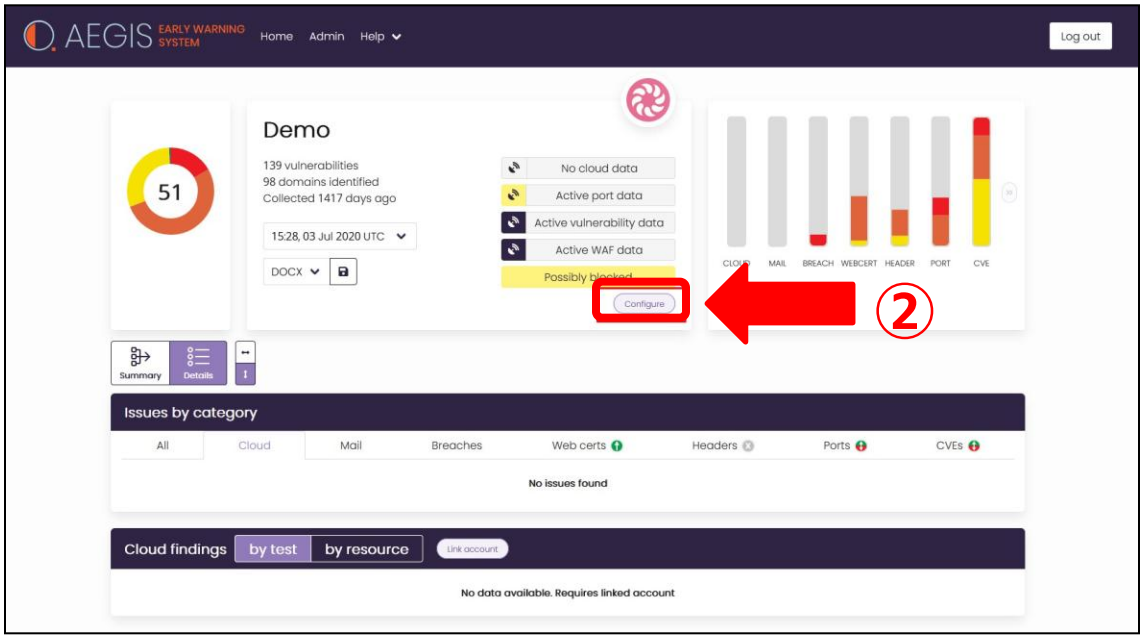
詳しくは、下記 URL をご参照ください。

https://aws.amazon.com/jp/security/penetration-testing/

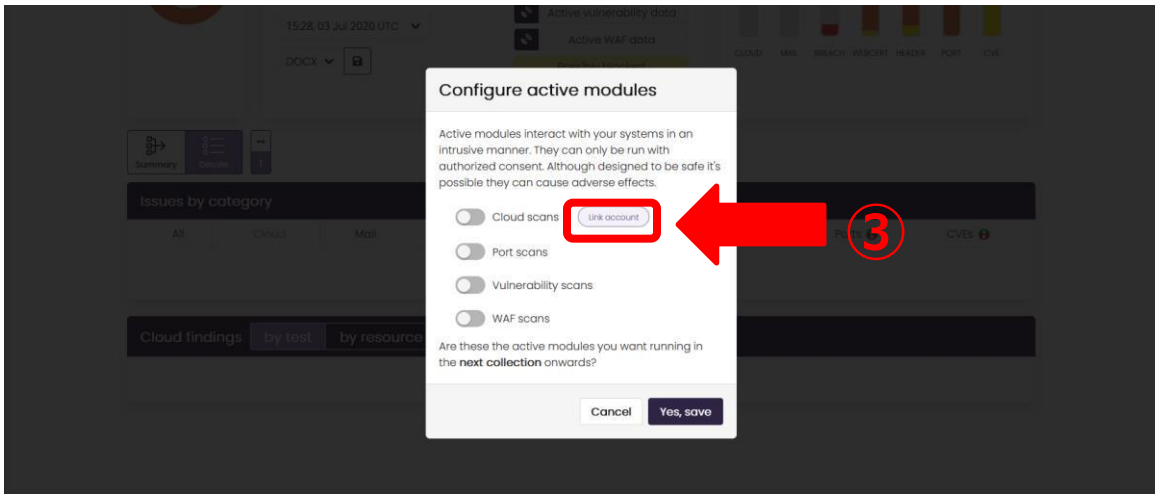
■Amazon AWS セキュリティ診断設定方法
①ダッシュボードにログイン後、診断するドメインサマリを選択してください。



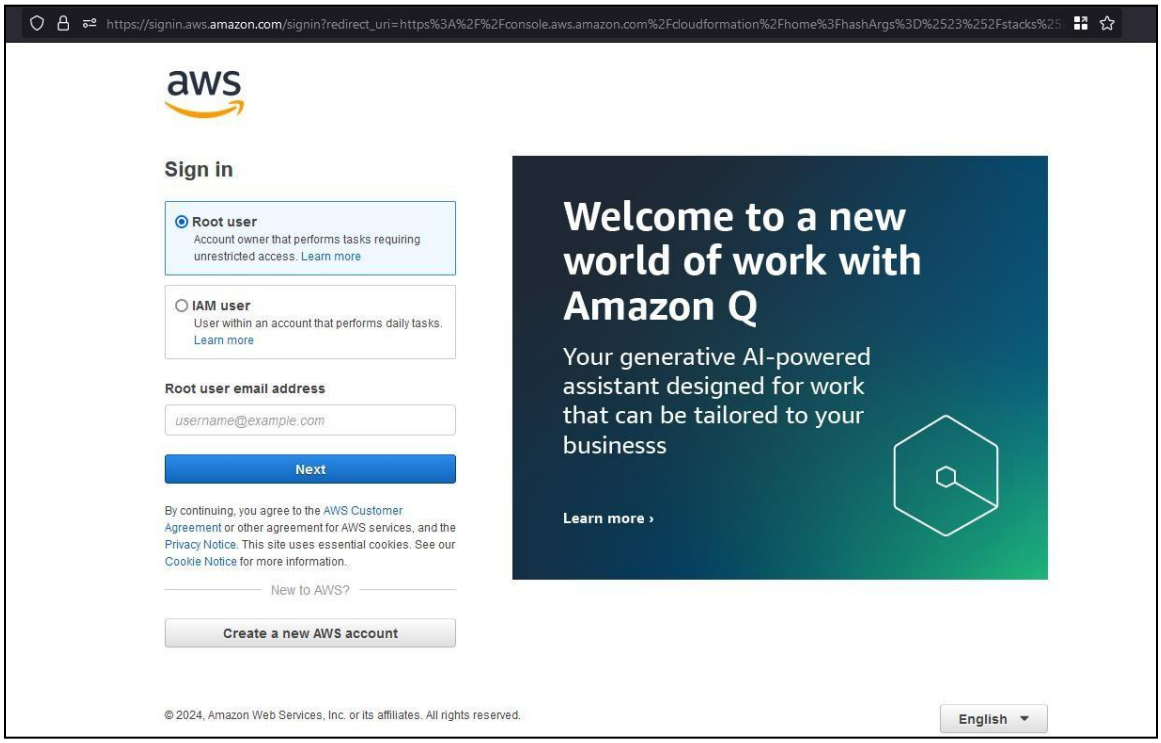
②次に、「Configure」をクリックしてください。



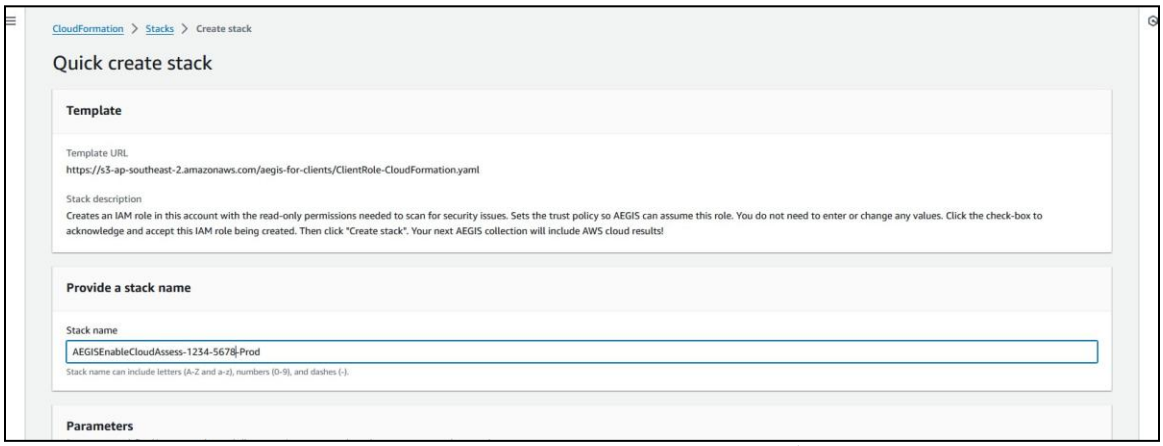
③「Link　Account」ボタンをクリックしてください。



④AWS インフラストラクチャにサインインするための AWS ログインページに移動し、Amazon AWS のアカウントにログインを行ってください。
ログインすると、AWS CloudFormation を実行するよう促されます。
なお、このアカウントには、AWS CloudFormation の実行、スタックの作成、Role の作成、Read-Only Policies の作成が許可されている必要があります。



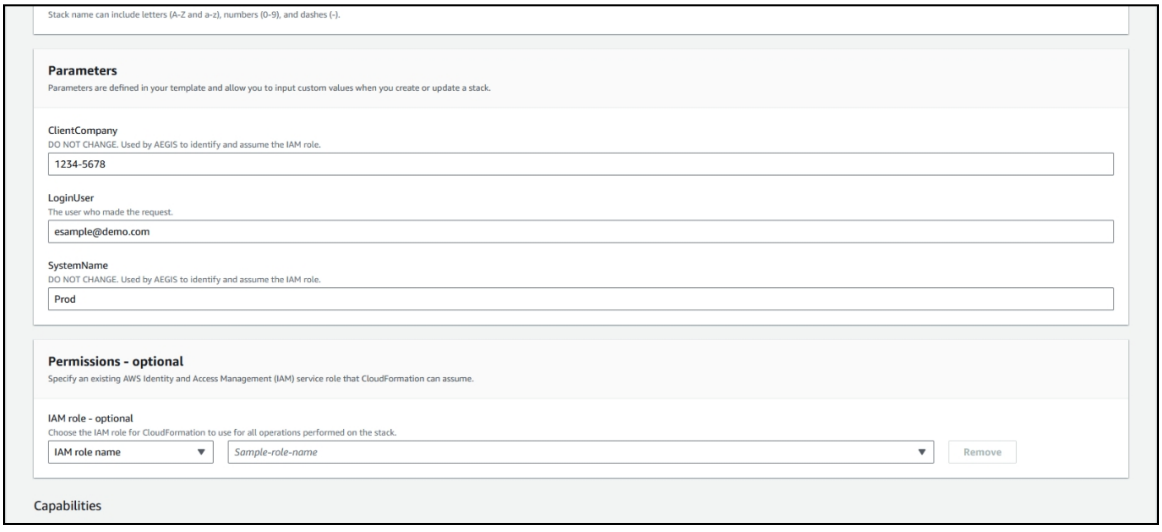
⑤AWS CloudFormation の設定を行ってください。



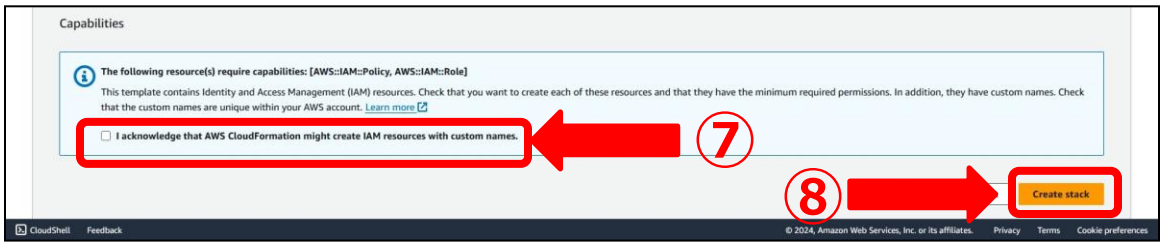
CloudFormation は、読み取り専用権限を持つ AWS Role が割り当てられた自己完結型の Stack をセットアップします。この Role はイージス EW によってのみアクセス可能です。これにより、イージス EW 側にログイン情報を保存することなく、AWS インフラストラクチャをスキャンすることができます。なお、この画面にて CloudFormation で実行される操作の説明を確認や、作成されるスタックの名前を変更できます。

注意：
ここでは、パラメータやパーミッションを変更しないでください。これらを変更すると、リンク処理が失敗します。

⑥画面下までスクロールしてください。



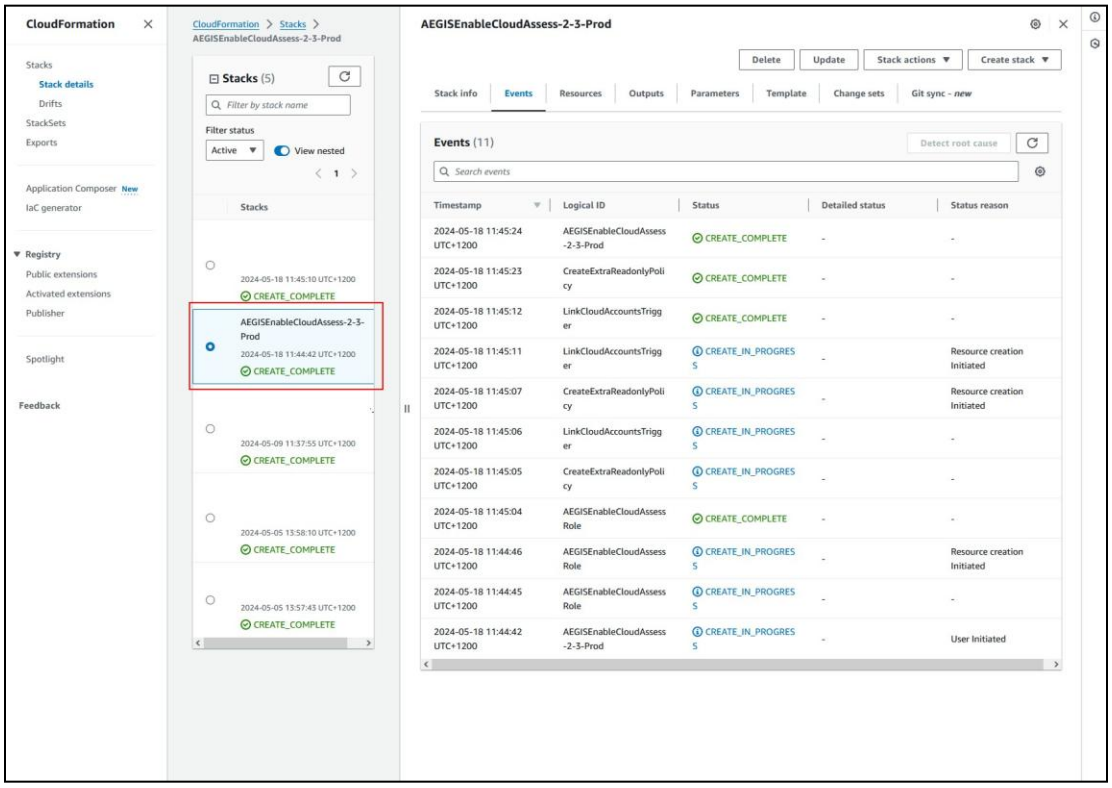
⑦プロンプトを読み、'I acknowledge that AWS CloudFormation may create IAM resources with custom names'と書かれたチェックボックスをクリックしてください。
⑧次に「Create Stack」をクリックしてください。



⑨AWS アカウントの CloudFormation セクションに移動します。CloudFormation が自己完結型の Stack を作成していることを確認してください。Stack が完了すると、緑色のチェックマークと「作成完了」が表示されます。

作成した Stack のリンクが通知されます。また、このタブを閉じて、イージス EW ダッシュボードに戻ることができます。

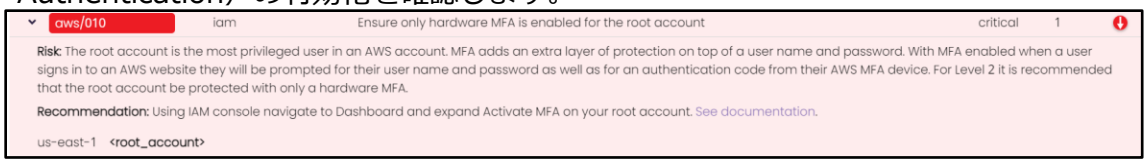
以上のリンク作業を行うことにより、イージス EW がお客様の AWS セキュリティポリシーをスキャンできるようになります。



■Amazon AWS セキュリティ診断機能

AWS では以下の診断を実施します。

【ルートアカウントの設定】
IAM におけるルートアカウントに対するハードウェア MFA（Multi-Factor Authentication）の有効化を確認します。



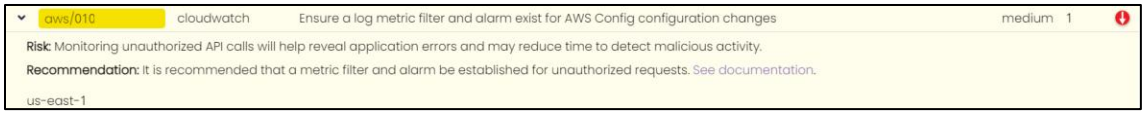
【CloudTrail の有効化】
全リージョンにおける CloudTrail の適切な設定を診断します。

【VPC のセキュリティグループ設定】

VPC（Virtual Private Cloud）における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チェックし、VPC フローのログ記録や複数リージョンでの設定も確認します。

【S3 の公開アクセスブロック】
Amazon S3 におけるパブリックアクセスのブロック設定を確認します。

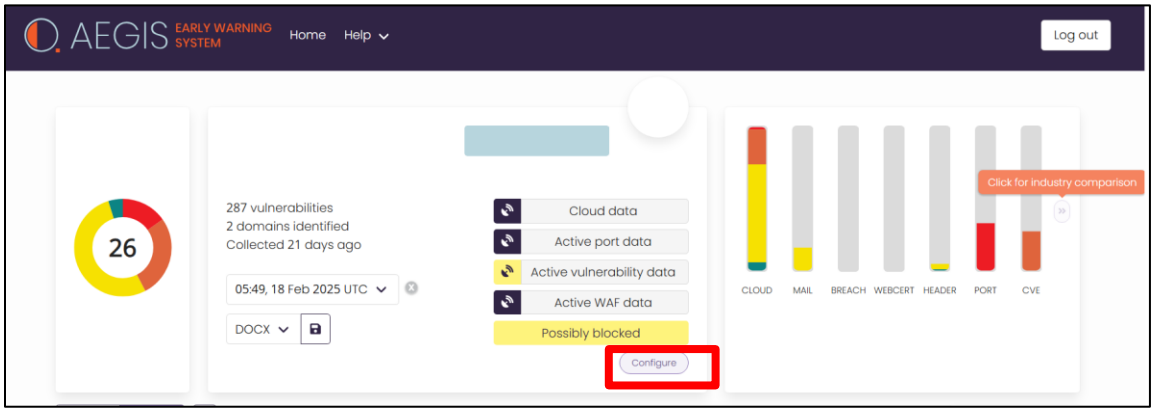
【CloudWatch イベントアラーム設定】
重要なセキュリティイベントに対するアラーム設定（IAM:Identity and Access Management）ポリシー変更、ルートアカウントの使用、API の不正利用など）を自動的にチェックします。



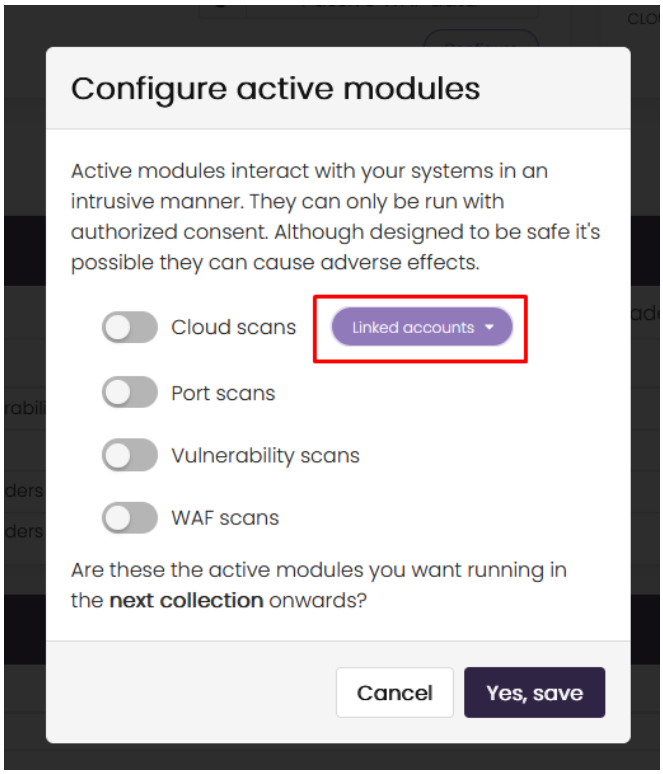
■Microsoft Azure セキュリティ診断設定方法

① ダッシュボードにログイン後、Azure アカウントを登録するドメインサマリをクリックします。

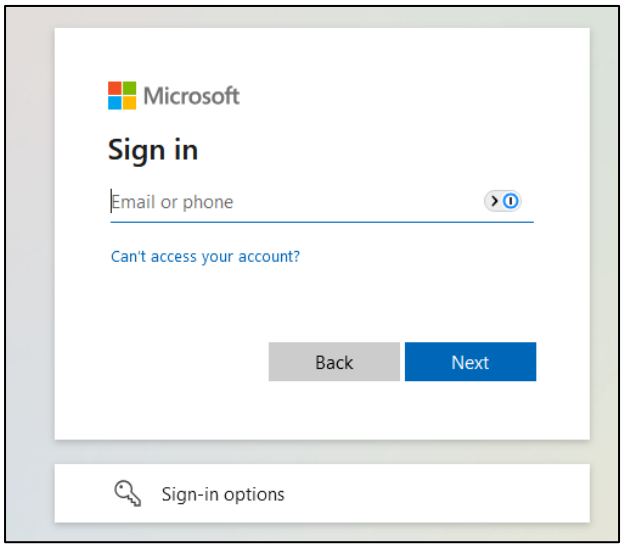
② ダッシュボードが表示されたら「Configure」をクリックします。



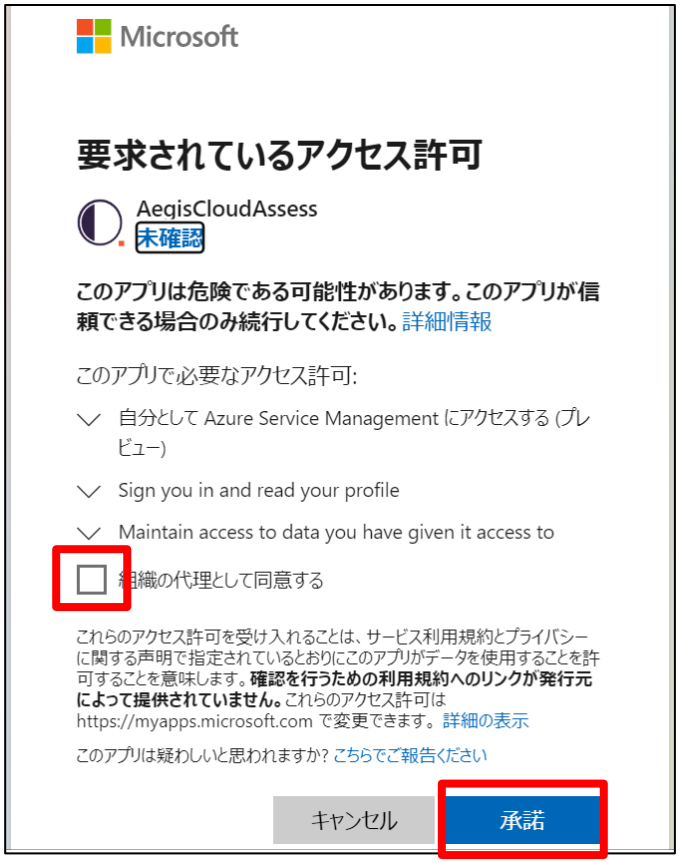
③ Config 画面が表示されます。「Linked Accout」をクリックします。



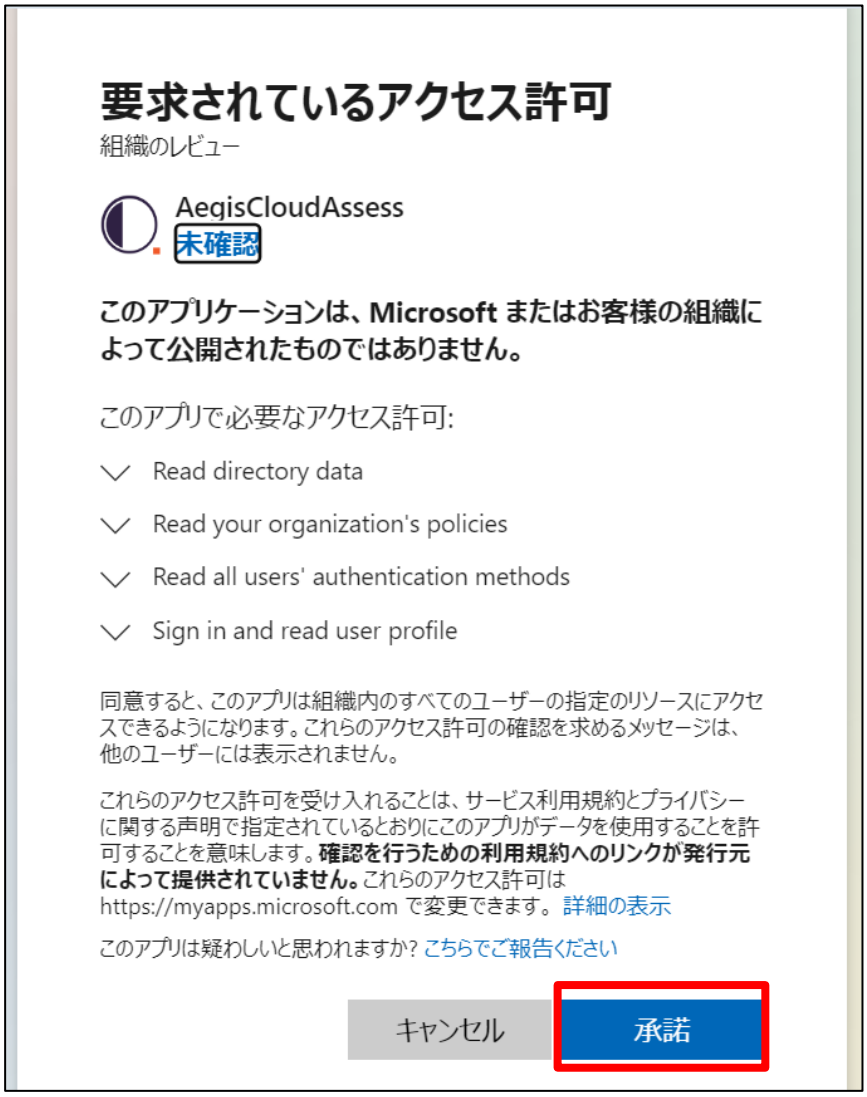
「Linked Accout」をクリックすると、Azure のログインページに移動します。
移動後に、Azure インフラストラクチャにサインインします。



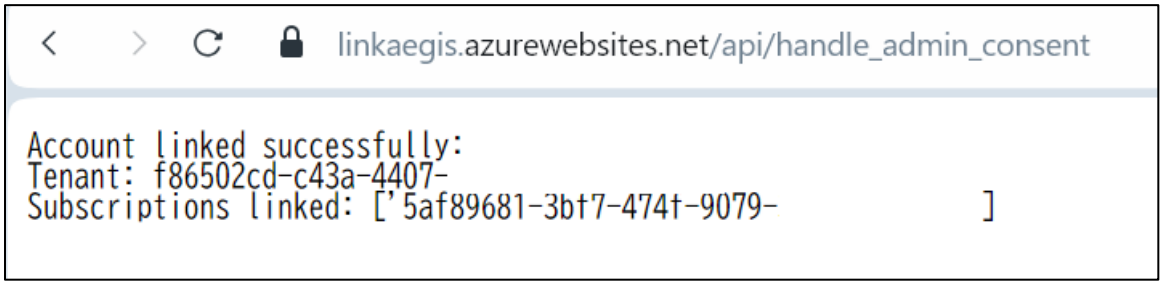
「組織の代理として同意する」にチェックを付けます。その後、「承諾」をクリックします。このアカウントは、外部ユーザーにアクセス権を付与し、サブスクリプションのスコープで読み取り専用権限を割り当てる権限が必要です。このリンクプロセスにより、AEGIS - Early Warning System がクラウドインフラストラクチャをスキャンできるようになります。



④ このリンクによって読み取り可能になる項目の一覧が表示されます。「承諾」をクリックします。



⑤ 画面遷移により、リンク完了と表示されます。



⑥ イージス EW に登録したメールアカウントに、Info@omnisciencesolutions.com より、Azure アカウントとのリンク完了メールが届きます。
これによってリンクが完了します。

Hi
Your cloud subscription is linked, and a new scan has been run.

Please wait up to 24 hours for your results.

Please do not reply to this email. To get in touch, email us at enquiries@aegis-ew.com.

Kind regards,
The AEGIS Early Warning System Team,

Omniscience Solutions.

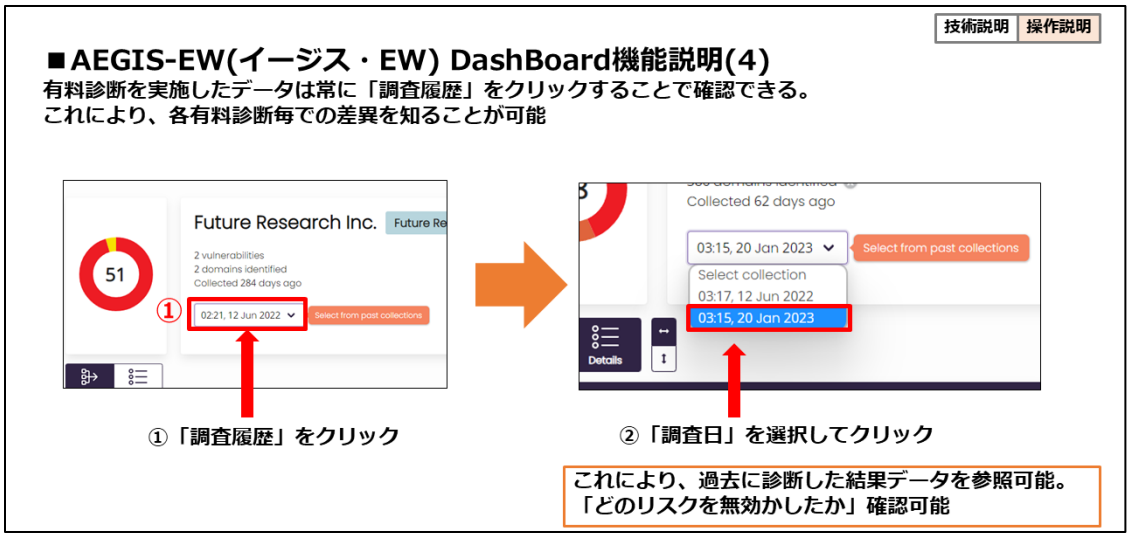
4章　イージス EW 運用方法

4－1　過去履歴の参照

①「調査履歴」をクリックしてください。

②参照したい調査日を選択してクリックしてください。

③ダッシュボードが、選択した調査日の結果で表示され、過去結果を参照できます。



4－2　レポートの出力

①「レポート出力」のプルダウンメニューから、ファイル形式を選択してください

②「ダウンロード」ボタンをクリックしてください。ブラウザ指定のダウンロードフォルダに、「Data」「Board Report」２種のファイルが保存されます。

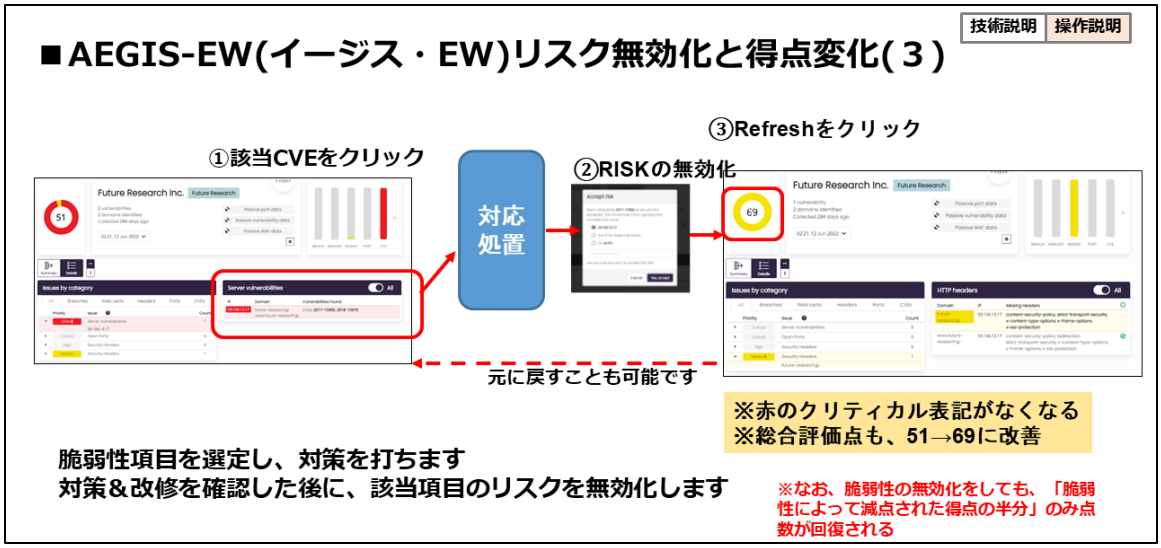
４－３　修正後の消し込み操作（Accept the risk ボタン操作）

①脆弱性の修正を行った後、該当 IP・ドメイン・CVE・ポートをクリックしてください

②「Accept risk」ポップアップが表示されます。

③「Yes,accept」ボタンを押してください。該当するリスクが無効化されます。

Refresh をクリックすると総合スコアに反映されます



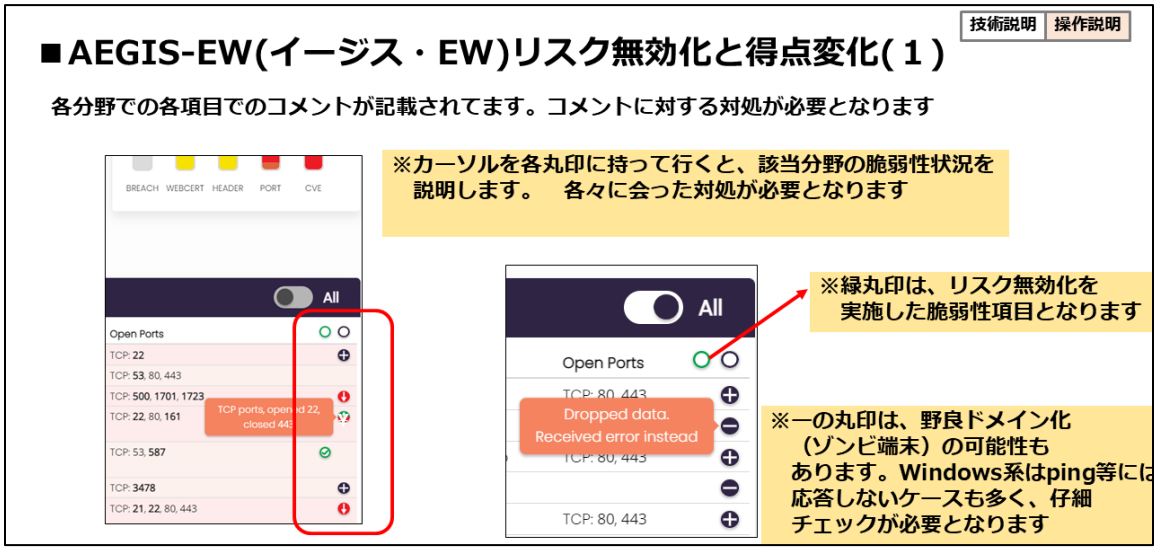
４－４　修正時の点数回復について

修正した脆弱性の消し込み作業を行うと、スコアが回復し総合点が上昇します。ただし、スコアの回復は該当する脆弱性が無かった場合の半分に制限されています。減点されたスコアが全回復するためには再度の脆弱性診断の実施が必要です。消し込みを取り消し、スコアを消し込み前に戻すことも可能です。

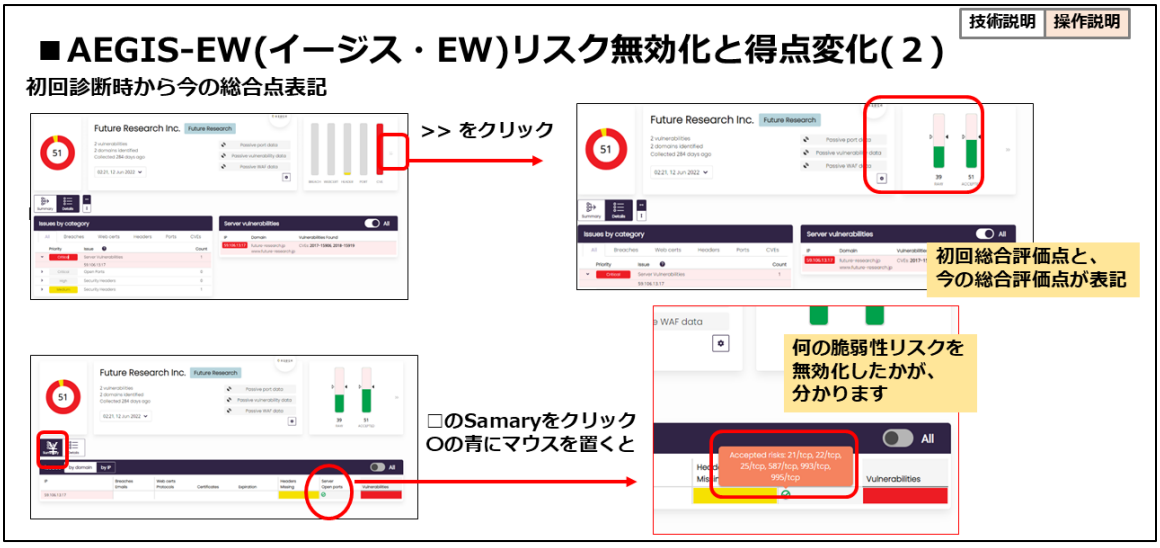
■脆弱性改修・対策と、評価点の変更

脆弱性一覧　右側の欄に各分野での各項目のコメントが記載されます。

「サマリ/詳細切り替え」をクリックしてサマリを表示し、緑色の「✓」マークにマウスカーソルを合わせると、消し込みして無効化した脆弱性リスクがポップアップ表示されます。



「脆弱性区分」棒グラフ右側の「>> 」をクリックすると、初回総合評価点と現在の総合評価点が表記されるグラフに切り替わります。「＞＞」をもう一度クリックすると「脆弱性区分」棒グラフに切り替わります。



補記　略語集

[i] CVE（共通脆弱性識別子）

一つ一つの脆弱性を識別するための共通の識別子

[ii] CVSS: Common Vulnerability Scoring System

IPA CVSS 説明文：https://www.ipa.go.jp/security/vuln/scap/cvssv3.html

[iii] Common Vulnerability Scoring System Version 3.1

FIRST CVSS V3.1 説明：https://www.first.org/cvss/v3-1/

[iv] WAF

WAF（Web Application Firewall）は、ウェブアプリケーションへの攻撃を防ぐために、データ暗号化等も用いHTTP/HTTPS通信を監視・制御するセキュリティ対策手法の一つです。