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

COPYRIGHT© 2025㈱未来研究所 FUTURE RESEARCH INC. ※無断転載を禁じます。2025/04/01

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	…р.	2
1 – 2	深刻度の説明	…р.	2
1 – 3	総合得点の算出の仕方	…р.	3

2章 イージス EW 操作説明

2 – 1	ログインの仕方	…р.	4
2 – 2	ダッシュボードの概要	…р.	6
2 – 3	ドメイン別ダッシュボードの見方	…р.	7
2 – 4	ドメイン別/IP 別脆弱性詳細情報の見方	…р.	8
2 – 5	検出済みドメイン別/IP 別脆弱性詳細情報の見方	…р.	9
2 6	新規ドメインの迫加(add ID (damain to company)	n	1 0

2-6 新規ドメインの追加(add IP / domain to company) … p. 10

3章 イージス EW 脆弱性分野別操作方法

3 – 1	Subdomain Discovery(サブドメイン調査)	…р.	11
3 – 2	Mail (送信ドメイン認証)	…р.	12
3 – 3	BREACH(データ侵害:情報漏洩)	…р.	13
3 – 4	Web Certs(Web 証明書)	…р.	15
3 – 5	Headers(HTTP ヘッダーネゴシエーション)	…р.	20
3 – 6	PORTs(サービスポート)	…р.	23
3 – 7	CVE(共通脆弱性識別子) [;]	…р.	25
(ペネト	∽レーションテスト時の CVE 詳細確認方法)	…р.	26
3 – 8	CLOUD	…р.	27
	Amazon AWS セキュリティ診断設定方法	…р.	28
	Microsoft Azure セキュリティ診断設定方法	…р.	34

4章 イージス EW 運用方法

4 – 1	過去履歴の参照	…p. 38
4 – 2	レポートの出力	…p. 38
4 – 3	修正後の消し込み操作	…p. 39
4 – 4	修正時の点数回復について	…p. 39

補記 略語集

…p. 41

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 $(\forall \forall Z \pi b)$
- 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[®]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[®]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

■AEGIS-EW(イ 「AEGIS-EW」では、 Response and Secur 図の赤枠の部分が該当の	ージス K国CEF ity Tea 表記でる	、・EW) 深刻度レ RT/CC等の機関が設立 ms)が提案した「CVS ある。	ベル したフ S評価	につ オーラ システ	いて ムであるFIRST(For ム」に基づいて深刻度	技術説明 操作説明 um of Incident レベルが表示される。	
Demo Future Research 139 submobilities		Acts	Ciex	or industry comparis	深刻度	CVSS v3基本值	
51 Collected 1058 days ago		Active rulner of thy data		>>	緊急(Critical)	9.0~10.0	
1528, 03 Jul 2020 V POF V B		Possibly blocked	EADER PORT	CVE	重要 (High)	7.0~8.9	
Services by category	ック	Domains			警告 (Middle)	4.0~6.9	
All Breaches Web certs 🕢 Headers 💿 Ports	🖯 CVEs 😝	Domain	VAF IP	0	注意		
Priority Issue	Count	ablinknzb.demo.aegis-ew.com	172.16.0.6	0		0.1~3.9	
Critical Server Vulnerabilities	2	abink.nz.c.aemo.aegis-ew.com abink.nz.demo.aegis-ew.com	172.16.0.6	0	(LOW)		
Open Ports	3	ablink.nzf.demo.aegis-ew.com	172.16.0.6	0	かし		
Processing Freedback	2	ablink.online.c.demo.aegis-ew.com	172.16.0.6	0	~~~~	0	
Prostriko bitolis							

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

■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	Future Research Inc. Participation 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 </th
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 CVSS値が計算される基の要素数値(CVE Information Grade 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	気されてます。)が用いられます 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。

		Log in
	Login	
	G Sign in with Google	
	Sign in with email	
	Create new Alloti account	
335 e .		
		_

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。

Login				
	check@future-	research.jp]
			0	
		Cancel	Next	2
Create ne	ew AEGIS account			

■多要素認証入力画面

 「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)

AEGIS SYSTEM Home	Contact Product site	Log in
	Login Please enroll for multi-factor authentication. Phone/SMS Authenticator Skip Create new AEGS account	

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。

AEGIS SYSTEM Home Contact Product site	og in
Login	
Please enter your phone number.	
+00 111 222 3333 Back Send code 2	
Create new AEGIS occount	
885 	

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。

O. AEGIS 🕯		Log out
2	Future ResearchDemo139 vulnerabilities98 domains identifiedCollected 1626 days ago	4

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。



■ AE	E GIS-EW(イージス GIS-EW」Dash Board名	・EW) DashBoard機能説明(2) 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		
	Summary Details	2	
	Issues by category		
	All Cloud	Mail Breaches Web certs 🕢 Headers 🔘 Parts 😝	CVES 🖶 (3)
(4)	Priority	issue 🔮	Count
\odot	CHILD	Den for Formation	
	> Critical	Open Ports Breachard Emplis	3
	> Hith	Server Vulnerobilities	-
	3 High	Open Ports	11
	> High	Encryption Protocols	9
	High	Web Certificates	14
	> High	Security Headers	27
	Medium	Server Vulnerabilities	28
	Medium	Breached Emails	1
	> Medium	Encryption Protocols	5
	Medium	Web Certificates	1
	Medium	Security Headers	20
	> Low	Web Certificates	1
	> Lów	Security Headers	6

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(「↔」「1」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「ţ」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、紫色にて八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」)

Domains			
IP V			0
172.16.0.1			•
172.16.0.2	help.b.demo.aegis-ew.com help.c.demo.aegis-ew.com help.demo.aegis-ew.com	Linux Kernel (O/S)	0
172.16.0.3	photos.demo.aegis-ew.com www.photos.demo.aegis-ew.com	Linux Kernel (O/S)	0
172.16.0.4	social.demo.aegis-ew.com www.social.demo.aegis-ew.com	Linux Kernel (O/S)	0
172.16.0.5	catering.c.demo.aegis-ew.com chipotle.c.demo.aegis-ew.com flavourmenu.c.demo.aegis-ew.com survivor.c.demo.aegis-ew.com	Microsoft Windows (O/S)	θ
172.16.0.6	guest.e.demo.aegis-ew.com	Linux Kernel (O/S)	0

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。

AEGIS EARLY Syste	Y WARNING EM Home Help V	Log out
51	Add company to dashboard Add domain/IP to company Minage users Demo Ft Contact us 139 vulnerabilities Info 98 domains identifiea Collected 1625 days ago 1528, 03 Jul 2020 UTC V Contigue Contact V Contact V Con	Click for industry com

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。

Add domain/IP to company
Company
Select company 🗸 🗸
Domain/IP(s)
www.yourcompany.com or 1.2.3.4 (press enter)
have read and agree to the terms of service
2 Cancel Send Email

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
Oomain Discoverv機能					
ois, DNSサーバ群の調査に基づき、	公開ドメインに対し	て「閉じぶ	忌れたIPアト	ドレス等を含	むサフドメー
寝IP・ゾンビ端末と呼ばれる)」 か	「あるか否かを調査を	た行う。これ	こは、「野良	ミIP」 から正	規ネットワ-
入を許し、各種サイバー攻撃を防ぐ	効果がある。				
Domains					
Domain	WAF	IP (
access.		61.196.			
admin.platcast.i			-		
aeoncinema-test.platcasti			_		
ag.		- 6			
ag-scap.		- 6	New domain		
agw.idm.c		153.127.			
api.dev27.test.cld.i					
↑					
		644×=-	++++>		

「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。

Location Rec MX	ord Contents saytech-co- jp0i.mail.protection.outlook.com	Valid	Failed Tests	0	
MX	saytech-co- jp0i.mail.protection.outlook.com	-			
NS				0	②SPF/DKIM対応状況が表示される。
	ns1-07.azure-dns.com	-		0	📕 図はSPFの保護範囲となるメールサーバの
NS	ns2-07.azure-dns.net	-		¢	ドメインが表示されている
NS	ns3-07.azure-dns.org	-		0	
NS	ns4-07.azure-dns.info	-		0	
2 SPF	v=spf1 +ip4:150.249.197.20 include:spf.protection.outlook.com include:smp.ne.jp include:spf.secure.ne.jp include:_spf.activegate-ss.jp - all	Yes		¢	

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。

Issues by cate	gory					
All (1 Breache	S	Web certs	Headers	Ports	CVEs
Priority	Iss	ue 🕐				Count
> High	Br	eached Emails				10
> Medium	Br	eached Emails				4
Data breaches						
Email Address	Compar Breache	Date of Breach	Breached Information			
address_1@ sample-domain.jp	Peatix	2019-01- 20	Email addresses, Names	s, Passwords		
address_2@	Adobe	2013-10-	Email addresses, Passwo	ord hints, Passwords, Usernam	Ies	

②「Data breaches」の各項目を確認します。

μ	Issues by categ	lory		Web code	Hender	0-1-	01/5-	
	All	Breaches	•	Web certs	Headers	Ports	CVES	
	High	Bread	hed Emails				Count 10	-
	> Medium	Bread	hed Emails				4	-
	address 1@	Breached	Breach 2019-01-	Email addresses. Names	: Passwords			
1	address_1@ sample-domain.jp	Peatix	2019-01- 20	Email addresses, Names	, Passwords			
	address_2@ sample-domain.jp	Adobe	2013-10- 04	Email addresses, Passwo	ord hints, Passwords, Usernan	nes		
								_

🗘 未来研究所

■BREACH 項目一覧

Email Adress 調査対象ドメイン

②Company Breached

③Date of Breach

④Breached Information

BF	REA	CH 項目一覧	技術説明
	Data b	preaches	
1	Email Ado	dress 2 Company 3 Breached	hate of (4) Breached Information reach
	addres sample	e-domain.jp Peatix 2	019-01- Email addresses, Names, Passwords 0
	addres sample	ss_2@ Adobe 2 e-domain.jp 0	013-10- Email addresses, Password hints, Passwords, Usernames 4
ł	野号	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	on 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/)

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



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。



■「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。

Issues by cate	gory					
All	Breaches	Web certs 🚯	Headers 🛞	Ports 🔂	CVEs 🔂	
1 Priority	Issue	0			Count	
Í	autodisc autodisc autodisc autodisc dev.c.de mail.b.de mail.b.de rbl-rdsg(rds.e.der	over.b.demo.aegis-ew.com over.d.demo.aegis-ew.com over.d.demo.aegis-ew.com no.aegis-ew.com mo.aegis-ew.com 11.e.demo.aegis-ew.com 11.e.demo.aegis-ew.com				

■「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

■ 「AEG	SIS-EWJ	サーバ証明書脆弱性調査結果画面 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	技術説明 操作説明
	All B Priority High	eaches Web certs Headers Ports CVES CVES COUNT State Count Incryption Protocols Audodiscover d.elman.org/in-ew.com audodiscover d.elman.org/in-ew.com audodiscover d.elman.org/in-ew.com audodiscover d.elman.org/in-ew.com robita.demo.org/in-ew.com robita.demo.org/in-ew.com robita.demo.org/in-ew.com robita.demo.org/in-ew.com	
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。

Web certificates and encryption					
Domain	P	Grade	Protocol	0	
ablink.nz.b.demo.aegis-ew.com	172.16.0.63	Α	TLS 1.2, TLS 1.3		
ablink.nz.c.demo.aegis-ew.com	172.16.0.61	A	TLS 1.2, TLS 1.3		
ablink.nz.demo.aegis-ew.com	172.16.0.31	Α	TLS 1.2, TLS 1.3		
ablink.nz.f.demo.aegis-ew.com	172.16.0.67	A	TLS 1.2, TLS 1.3		
ablinkonline.c.demo.aegis-ew.com	172.16.0.69	Α	TLS 1.2, TLS 1.3		
 ablinkyourorder.b.demo.aegis-ew.com 	172.16.0.0	Α	TLS 1.2, TLS 1.3		
access.e.demo.aegis-ew.com	172.16.0.0	Α	TLS 1.2, TLS 1.3		
aplb.demo.aegis-ew.com	172.16.0.0	A	TLS 1.2, TLS 1.3		
autodiscover.b.demo.aegis-ew.com	172.16.0.7	м	SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2		
Index cop C. Supports decided RC4 cipher suite index cop C. Supports decided RC4 cipher suite index cop C. Supports decided RC4 cipher suite index cop C. Vulnerable in Support Utabular index cop C. Vulnerable in Swetzz attack index cop D. Supports decided protocol: 15:10 prodex cop B. Supports decided protocol: 15:11 prodex cop B. Supports decided protocol: 15:11	2			-	

- ■「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



■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



■イージス EW における、サーバ証明書グレードの評価方法

■サーバ証明書グレードについて	技術説明	操作説明
「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、各たある場合、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、元のグレードに「+」を付与する場合がある。	コテゴリて D特徴を評 「 A+ 」0	ご0点が F価する Dように
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 「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 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 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 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。	の不一致 こいない場 重要ではか を付与する)」や 洽、悪 なくな 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

■サ 「AEC (参照	ー バ証明書グレードにつ GIS-EW」における、サーバ証明 売: https://www.ssllabs.c	Dいて 月書グレード評価ポイント説明はつぎのとおり 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

■サーバ証	■サーバ証明書グレードについて 「AFOTO FINL (こかける、)」、「「TITITITITIC」」、 (「TITITITITIC」」、 (「TITITITIC」」、 (「TITITITIC」」、 (「TITITIC」」、 (「TITITIC」、 (「TITIC」、 (TITIC」、 (「TITIC」、 (TITIC」、 (「TITIC」、 (TITIC」、 (TITIC」、 (TITIC」、 (TITIC」、 (TITIC」、 (TITIC」、 (TI								
AEGIS-EW	(_d	らける、サーハ証明書ク	/レートス」)	クリンク区分は以下のとおり					
	番믄	スコア区分	グレード	備老					
	1			כי נוזע					
		score >= 80	A						
	2	score >= 65	В						
	3	score >= 50	С						
	4	score >= 35	D						
	5	score >= 20	E						
	6	score < 20	F						
	7	なし	М	証明書名の不一致(証明書と実ドメイン名が違う)					
	8	なし	Т	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



■「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。



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

Issues by cate	egory						
All	Cloud	Mail	Breaches	Web certs 🚹	Headers 🛞	Ports 🔂	CVEs 🚯
Priority		Issue					Count
Critical		Open Ports					3
> High		Open Ports					11
Open ports							
IP	Domain 🔘	(2)	Open Ports				0
> 172.16.0.2	help.b.demo.aegi	is-ew.com	TCP: 80, 443, 2052, 20	53, 2082, 2083, 2086, 2087, 2095	, 2096, 8080, 8443, 8880		0
> 172.16.0.3	photos.demo.aeg	gis-ew.com	TCP: 80, 443, 2052, 20	53, 2082, 2083, 2086, 2087, 2095	, 2096, 8080, 8443, 8880		θ
> 172.16.0.4	social.demo.aegi	s-ew.com	TCP: 80, 443, 2052, 20	53, 2082, 2083, 2086, 2087, 2095	, 2096, 8080, 8443, 8880		0
) (1) 172.16.0.5	catering.c.demo.d	aegis-ew.com	TCP: 80, 443 TCP (low confidence): 164 hidden			0
> 172.16.0.6	guest.e.demo.aeç	gis-ew.com	TCP: 53, 80, 443, 853 UDP: 53				θ
> 172.16.0.7	autodiscover.b.de	emo.aegis-ew.com	TCP: 443, 993				

■狙われやすいポート一覧

■狙われ	■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	ТСР	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)					
		10105	1.						

■外部公開禁止ポート一覧

■外部公園	開禁止ポ	ートー覧		技術説明操作説
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	ТСР	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 (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 (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 たいしょう ちょうしょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひ	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 (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 (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	тср	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。

■ AI AEGI	EGIS- S-EW(a as by cat	- EWにおけるCV こおけるCVE番号を確 egory	'E確認方 認した以降	法(1 の分析方) 法について	∃技術説明 操作説明
All	Mail	Breaches Web certs 🚯	Headers 🛞	Ports 🚯	CVEs 🚯	
P	riority	Issue			Count	「 項日から、「CVES」を選択
>	Critical	Server Vulnerabilities			2	
>	High	Server Vulnerabilities			8	
>	Medium	Server Vulnerabilities			29	
]

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



■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」(<u>https://jvndb.jvn.jp/</u>) にて検索・分析が可能です。

the second state in the second state is a second state in the second state is a second state i

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。

AEGIS SYSTEM Home Admin Help ~		Log out
	Demo 139 vulnerabilities 98 domains identified Collected 1417 days ago	

②次に、「Configure」をクリックしてください。

AEGIS EARLY WARNING	Home Admin Help 🗸			Log out
51	Demo 139 vulnerabilities 98 domains identified Callected 1417 days ago 1528, 03 Jul 2020 UTC Y DOCX Y	No cloud data Active part data Active vulnerability data Active WAF data Active WAF data Possibly Monhaet Configure		WERCERT HEADER PORT CVE
Summary Details				
Issues by category				
All Clou	ud Mail Breaches	Web certs 🚯	Headers 💿 Por	CVES
		No issues found		
Cloud findings	y test by resource	unt		
	No c	lata available. Requires linked accoun	t	

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。

👌 🚭 https://signin.aws. amazon.com /signin?redirect_uri=https%3A%2F%2Fc	onsole.aws.amazon.com%2Fcloudformation%2Fhome%3FhashArgs%3D%2523%252Fstacks%25
aws	
Sign in	
Root user Account owner that performs tasks requiring unrestricted access. Learn more	Welcome to a new world of work with
O IAM user User within an account that performs daily tasks.	Amazon Q
Root user email address	Your generative AI-powered assistant designed for work
username@example.com	that can be tailored to your businesss
Next	
By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.	Learn more >
New to AWS?	
Create a new AWS account	
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserve	d. English 🔻

⑤AWS CloudFormation の設定を行ってください。

loud	Formation > Stacks > Create stack
Qu	ick create stack
Те	emplate
Те	emplate URL
htt	tps://s3-ap-southeast-2.amazonaws.com/aegis-for-clients/ClientRole-CloudFormation.yaml
Sta	ack description
Cre	eates an IAM role in this account with the read-only permissions needed to scan for security issues. Sets the trust policy so AEGIS can assume this role. You do not need to enter or change any values. Click the check-box to
Pr	rovide a stark name
Sta	ack name
A	AEGISEnableCloudAssess-1234-5678-Prod
Sta	ack name can include letters (A-2 and a-2), numbers (0-9), and slashes (-).
	a som affast

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。

Stack name can include letters (A-Z and a-z),	umbers (b-9), and dashes (-).
Parameters	
Parameters are defined in your template and	allow you to input custom values when you create or update a stack.
ClientCompany DO NOT CHANGE. Used by AEGIS to identify	and assume the IAM role.
1234-5678	
LoginUser The user who made the request.	
esample@demo.com	
SystemName DO NOT CHANGE. Used by AEGIS to identify	and assume the IAM role.
Prod	
Permissions - optional	
Specify an existing AWS Identity and Access N	fanagement (JAM) service role that CloudFormation can assume.
IAM role - optional Choose the IAM role for CloudFormation to u	se for all operations performed on the stack.
IAM role name 🔻	Sample-role-name Remove
apabilities	

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。

Stacks Stack details	🖻 Stacks (5)	Dalete Update Stack actions V Create stack	•
Drifts	Q. Filter by stack name	Stack info Events Resources Outputs Parameters Template Change sets Git sync - new	0 × ×
StackSets Exports	Filter status Active View nested	Events (11) Detect root cause	,
Application Composer New	< 1 >	Q. Search events	0
laC generator	Stacks	Timestamp 🔻 Logical ID Status Detailed status Status reason	
Registry		2024-05-18 11:45:24 AEGISEnableCloudAssess UTC+1200 -2-3-Prod © CREATE_COMPLETE -	
Public extensions Activated extensions	0 2024-05-18 11:45:10 UTC+1200 CREATE COMPLETE	2024-05-18 11:45:23 CreateExtraReadonlyPoli UTC+1200 cy OCREATE_COMPLETE	© X X A A A A A A A A A A A A A A A A A
Publisher	AEGISEnableCloudAssess-2-3- Prod	2024-05-18 11:45:12 LinkCloudAccountsTrigg UTC+1200 er @CREATE_COMPLETE -	
Spotlight	2024-05-18 11:44:42 UTC+1200	2024-05-18 11:45:11 LinkCloudAccountsTrigg © CREATE_IN_PROGRES Resource creation UTC+1200 er 5 Initiated	
eedback		2024-05-18 11:45:07 CreateExtraReadonlyPolil © CREATE_IN_PROGRES Resource creation II UTC+1200 cy 5 Initiated	
	O 2024-05-09 11:37:55 UTC+1200	2024-05-18 11:45:06 LinkCloudAccountsTrigg © CREATE_IN_PROGRES UTC+1200 er S	
	CREATE_COMPLETE	2024-05-18 11:45:05 CreateExtraReadonlyPoli O CREATE_IN_PROGRES UTC+1200 cy S	
	O 2024-05-05 13:58:10 UTC+1200	2024-05-18 11:45:04 AEGISEnableCloudAssess OCREATE_COMPLETE - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -	
	© CREATE_COMPLETE	2024-05-18 11:44:46 AEGISEnableCloudAssess @ CREATE_IN_PROGRES Resource creation UTC+1200 Role 5 Initiated	
	O 2024-05-05 13:57:43 UTC+1200	2024-05-18 11:44:45 AEGISEnableCloudAssess @ CREATE_IN_PROGRES UTC+1200 Role S	
	Ø CREATE_COMPLETE	2024-05-18 11:44:42 AEGISEnableCloudAssess ③ CREATE_IN_PROGRES User Initiated UTC+1200 -2-3-Prod 5 User Initiated	

high 17 🚯

■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。

ams Ensure only hardware MFA is enabled for the root account
 critical 1
 Risk: The root account is the most privileged user in an AWS account. MFA adds an extra layer of protection on top of a user name and password. With MFA enabled when a user signs in to an AWS website they will be prompted for their user name and password as well as for an authentication code from their AWS MFA device. For Level 2 it is recommended that the root account be protected with only a hardware MFA.
 Recommendation: Using IAM console navigate to Dashboard and expand Activate MFA on your root account. See documentation.

us-east-1 <root_account>

【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。

		~
Risk: AWS CloudTr of the API call; the	rail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller; the tim e source IP address of the API caller; the request parameters; and the response elements returned by the AWS service.	e
Recommendatio	n: Ensure Logging is set to ON on all regions (even if they are not being used at the moment. See documentation.	
ap-northeast-1	010	
ap-northeast-2	010	
ap-northeast-3	010	
ap-south-1	010	
ap-southeast-1	010	
ap-southeast-2	010	
ca-central-1	010	
eu-central-1	010	
eu-north-1	010	
eu-west-1	010	
eu-west-2	010	
eu-west-3	010	
sa-east-1	010	
us-east-1	010	
us-east-2	010	
us-west-1	010	
us-west-2	010	

【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。

`	aws/010	ec2	Ensure the default security group of every VPC restricts all traffic	high	17	0
	Risk: Even having instance.	a perimeter firew	vall, having security groups open allows any user or malware with vpc access to scan for well known and sensitive ports and g	ain access	to	
	Recommendation narrow the definition of the second	n: Apply Zero Trus tion for the minin	st approach. Implement a process to scan and remediate unrestricted or overly permissive security groups. Recommended b num ports required. See documentation.	est practice	es is to	
	ap-northeast-1	sg-				
	ap-northeast-2	sg-				
	ap-northeast-3	sg-				
	ap-south-1	sg-				
	ap-southeast-1	sg-				
	ap-southeast-2	sg-				
	ca-central-1	sg-				
	eu-central-1	sg-				
	eu-north-1	sg-				
	eu-west-1	sg-				
	eu-west-2	sg-				
	eu-west-3	sg-				
	sa-east-1	sg-				
	us-east-1	sg-				
	us-east-2	sg-				
	us-west-1	sg-				
	us-west-2	sq-				

high

0

【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。

aws/01C s3 Check S3 Account Level Public Access Block

 Risk Public access policies may be applied to sensitive data buckets.

 Recommendation: You can enable Public Access Block at the account level to prevent the exposure of your data stored in S3. See documentation.

 us-east-1

【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。

~	aws/010	cloudwatch	Ensure a log metric filter and alarm exist for AWS Config configuration changes	medium 1	0
Ri	sk: Monitoring unauth	orized API calls will	help reveal application errors and may reduce time to detect malicious activity.		
Re	commendation: It is i	recommended the	at a metric filter and alarm be established for unauthorized requests. See documentation.		

■ 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。

AEGIS SYST	.Y WARNING Home Help ↓ TEM			Log out
26	287 vulnerabilities 2 domains identified Collected 21 days ago 05:49, 18 Feb 2025 UTC V DOCX V	 Cloud data Active port data Active vulnerability data Active WAF data Possibly blocked 	CLOUD MAL BREACH WEBCERT HEADER	Click for industry comparison

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

		_
	Configure active modules	
	Active modules interact with your systems in an intrusive manner. They can only be run with authorized consent. Although designed to be safe it's possible they can cause adverse effects.	
abili	Cloud scans	
iers iers	Vulnerability scans WAF scans	
	Are these the active modules you want running in the next collection onwards?	
	Cancel Yes, save	

「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。

IVIICIOSOIT		
Sign in		
Email or phone		>0
Can't access your acco	ount?	
	Back	Next
	Back	Next

「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。

35

Microsoft
要求されているアクセス許可
AegisCloudAssess 禾確認
このアプリは危険である可能性があります。このアプリが信 頼できる場合のみ続行してください。詳細情報
このアプリで必要なアクセス許可:
◇ 自分として Azure Service Management にアクセスする (プレ ビュー)
\checkmark Sign you in and read your profile
✓ Maintain access to data you have given it access to
□ 組織の代理として同意する
これらのアクセス許可を受け入れることは、サービス利用規約とプライバシー に関する声明で指定されているとおりにこのアブルゲークを使用することを許 可することを意味します。 確認を行うための利用規約へのリンクが発行元 によって提供されていません。 これらのアクセス許可は https://myapps.microsoft.com で変更できます。詳細の表示
このアプリは疑わしいと思われますか? こちらでご報告ください
キャンセル 承諾

COPYRIGHT© 2025㈱未来研究所 FUTURE RESEARCH INC. ※無断転載を禁じます。

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。

要組織	求されているアクセス許可 ^{のレビュー}	
	AegisCloudAssess 未確認	
この よっ	アプリケーションは、Microsoft またはお客様の組織に て公開されたものではありません。	
この	アプリで必要なアクセス許可:	
\sim	Read directory data	
\checkmark	Read your organization's policies	
\sim	Read all users' authentication methods	
\sim	Sign in and read user profile	
同意 スでき 他の	すると、このアプリは組織内のすべてのユーザーの指定のリソースにアクセ きるようになります。これらのアクセス許可の確認を求めるメッセージは、 ユーザーには表示されません。	
これら に関う 可す によう http:	5のアクセス許可を受け入れることは、サービス利用規約とプライバシー する声明で指定されているとおりにこのアプリがデータを使用することを許 ることを意味します。 確認を行うための利用規約へのリンクが発行元 って提供されていません。 これらのアクセス許可は s://myapps.microsoft.com で変更できます。詳細の表示	
このア	アプリは疑わしいと思われますか? こちらでご報告ください	
	キャンセル 承諾	

⑤ 画面遷移により、リンク完了と表示されます。

С linkaegis.azurewebsites.net/api/handle_admin_consent < > Account linked successfully: Tenant: f86502cd-c43a-4407-Subscriptions linked: ['5af89681-3bt7-474t-9079-]

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 <u>enquiries@aegis-ew.com</u>.

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

ⁱCVE(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。