	大分類	中分類	小分類	Silver	Gold		用語例(修得すべき用語、キーワード)	備考
技術)	標準的なプロトコルと	プロトコル	IP	0	o I	IPアドレスの形式を理解している(S/G)	IPアドレス、グローバルIPアドレス、プライベートIPアドレス、サブネットマス	
	技術					IPv6アドレスの形式を理解している(G)	ク、ルーティング、デフォルトゲートウェイ、ネットワークアドレス、	
						プロードキャストアドレスを理解している(S/G)	NAT/NAPT、IPマスカレード、static NAT、dynamic NAT	
			TCP	0	0	サブネットマスクの計算ができる(S/G) ローカルアドレスとグローバルアドレスの区別がつく(S/G)	コネクション指向、制御フラグ、3wayhandshake、ポート、確認応答、順序制 御 再送制御 ユニキャスト	
			UDP	_			御、井达制御、ユニキャスト トランザクション指向、ポート、リアルタイム性、マルチキャスト、ブロードキャ	
			ODP	0		アプリットCORLを入れてから画面が表示されるまでの一連の流れを理解している(S/G)	トランリクション指向、ホート、リアルライム性、マルデギャスト、フロートギャースト	
			SSL/TLS	0		SSLの役割(機密性・完全性)を理解している(S/G)	認証、暗号化、改竄検出、OpenSSL、鍵共有、証明書、ネゴシエーション、サー	
				1	-	TCP接続上で任意のデータを送受信できる(G)	バ認証、クライアント認証、デジタル証明書	
			HTTP	0	0	SSL/TLS上で任意のデータを送受信できる(G)	クライアント、サーバ、リクエスト、レスポンス、ステートレス、持続的接続、パ	
						HTTPの基本的な役割、機能を理解している(S/G)	イプライン	
			HTTPS	0		HTTP上で任意のデータを送受信できる(S/G)	SSL、TLS、公開鍵、証明書	
			HTTP/2	×		HTTPS の基本的な動作を理解している(S/G)	サーバプッシュ、HPACK	
			WebSocket	×		HTTP/2の基本的な役割、機能を理解している(G)	ws:、wss: 、双方向通信	
			IPv6	×	0	WebSocketの基本的な役割、機能を理解している(G)	IPv6アドレス、サブネットマスク、近隣探索、ユニキャストアドレス、エニーキャ	
					- "	WebSocket上で任意のデータを送受信できる(G)	ストアドレス、マルチキャストアドレス、グローバルユニキャストアドレス、リン クローカルユニキャストアドレス、ユニークローカルユニキャストアドレス	
		名前解決	トップレベルドメイン(TLD)	^		hostsファイルなどの書き換えができる(S/G)	トップレベルドメイン(TLD)、gTLD、ccTLD、sTLD	
		41 門用代	ICANN	×		OSの名前解決の仕組みを理解している(S/G)	ICANN, APNIC, JPNIC, JPRS	
			静的な名前解決(hostsファイル)	0		ドメインの階層構造(ホスト名・サブドメイン)を理解している(S/G)	hostsファイル、名前解決、別名定義	
			DNS	0		名前解決の仕組みを理解している(S/G)	正引き、逆引き、レコード、権威サーバ、キャッシュサーバ、ゾーン転送、再帰間	
						コマンドを用いて、任意のDNSレコードの正引き・逆引きができる	い合わせ、DNSSEC	
						(S/G)		
			ドメイン管理の仕組み	_		Whoisで提供される情報を理解している(S/G)	レジストラ・レジストリ	
			トグイン日注の江地か	^	0	ドメイン管理の仕組みを理解している(G)	VVAF7. VVAF9	
		ducto . 14	l .			Andre Mal law declaration and a self-animal account	LITTE O DI W. HO. FILO ID. IDO COCO ID. ACCUI	
		文字コード		0	0	一般的に使われる文字エンコーディングを理解している(S/G)	UTF-8、Shift_JIS、EUC-JP、ISO-2022-JP、ASCII	
		l				ブラウザや診断ツールのエンコーディングの設定が適切にできる (S/G)		
		1				(3/3)		
		メール	SMTP/POP/IMAP	0	0 1	SMTPの基本的な役割、機能を理解している(S/G)	MTA、MUA、MAIL FROM、RCPT TO、SMTP/POP/IMAP、メールヘッダ	
		l' '*	Siiii // Ol /livini	~	, I,	メールの送受信に必要なMUAの設定ができる(S/G)	min, mon, marriton, not i to, omit it of himmi, 7-70-199	
		1				SMTPコマンドを用いて任意のメールメッセージを送信できる(G)		
		1			[
	セキュリティ技術	暗号	共通鍵暗号	0		共通鍵暗号の性質を理解している(S/G)	共通鍵暗号、公開鍵暗号、ソルト、ストレッチング、3DES、AES、Camellia、	
			公開鍵暗号	0		公開鍵暗号の性質を理解している(S/G)	RC4、RSA、DSA、MD5、SHA-1、SHA-2、CRYPTREC、bcrypt	
			暗号学的ハッシュ	0	o 1	暗号学的ハッシュの性質を理解している(S/G)		
					11	代表的な暗号・ハッシュアルゴリズムの名称を知っている(S/G)		
						ソルト、ストレッチングの効果を理解している(S/G)		
					l l	ハッシュ値が算出できる(S/G)		
		PKI	認証局	0	0	秘密鍵生成・署名要求・証明書生成など、電子証明書発行までの手順	公開鍵、秘密鍵、署名、証明書、認証局、PGP、Web of Trust、CSR、自己署名証	
			証明書	0	0	を理解している(S/G)	明書、CRL、PKCS#12	
			12 iiE	0	0	自己署名証明書(サーバ・クライアント)を作成できる(S/G) 自己署名証明書使用時のプラウザの警告内容を理解できる(S/G) 証明書をブラウザに追加できる(S/G)		
					i i			
		ネットワーク	ファイアウォール	^		ファイアウォールの基本的な仕組みを理解している(S/G)	ファイアウォール、パーソナルファイアウォール、パケットフィルタ型、サーキッ	
		4717	271724 7	Ŭ	Ŭ .	IDS/IPSの基本的な仕組みを理解している(S/G)	トレベルゲートウェイ型、アプリケーションゲートウェイ型、ステートフルインス	
					1 1	WAFの基本的な仕組みを理解している(S/G)	ペクション	
			IDS/IPS	0	0	THE SECTION OF SCHOOL	IDS/IPS、フォルスポジティブ、フォルスネガティブ、シグネチャ、UTM	
			WAF	0	0		WAF, NGFW	
		認証	フォーム(ベース)認証	0		各認証の基本的な仕組みを理解している(S/G)	フォーム(ベース)認証、ユーザID、パスワード、ログイン、ログアウト	
			HTTP認証	0	0 2	各認証のメリット・デメリットを説明できる(G)	Basic/Digest認証、ダイジェスト(ハッシュ)、MD5、改竄防止、盗聴防止、nonce	
		1					Base64、チャレンジレスポンス、NTLM認証	
		l	クライアント認証(SSL)	0	0		クライアント認証(SSL)、秘密鍵、公開鍵、証明書、署名、ダイジェスト	
		1	二 要素認証(多要素認証)・二段	0	0		二要素認証(多要素認証)、二段階認証、個人識別、本人認証	
		1	階認証				O. H. O. H. O. I. D. Andrewskin D. A. A. A. W.	
		l	シングルサインオン	0	0		OAuth、SAML、OpenID、認証基盤、代理認証、リバースプロキシ型、エージェント型、OpenAM	
		1	ハードウェアトークン・ソフト	^	_		ト型、OpenAM ハードウェアトークン、ソフトウェアトークン、OTP	
		l	ウェアトークン	~	~		・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
		1	ジェアトークン 認証要素	0	0		知識ベース認証(秘密の質問・あいことば)、所有物認証・生体認証、生体情報(指	
		1	HC/HIL-3C 7T	~	Ĭ		和職ペース略能(秘密の員同・めいことは)、別有物総能・生体総能、生体情報(指 紋、静脈、顔)、知識情報(パスワード、OTP)、所持情報(ハードウェアトークン、IC	
		l					カード). FIDO	
		その他のセキュリ	CAPTCHA	0	0 :	各技術の基本的な仕組みを理解している(S/G)	CAPTCHA、チャレンジレスポンス型テスト、自動入力防止	
		ティ技術	CSRF対策トークン	0	0		CSRF対策トークン	
		l	ワンタイムトークン	0	0		ワンタイムトークン	
			リスクベース認証	×	0		リスクベース認証、追加認証	
		情報セキュリティ	機密性	0	0	機密性・完全性・可用性を理解している(S/G)	機密性、アクセス制御、ユーザ認証、漏洩	
		の三要素	完全性	0	0		完全性、改竄防止、改竄検出	
	144 1 00 No. 144 / 114	LIDI WIDI	可用性	0	0	LIDI KIDI KANAN ANDARA MARIAN	可用性、冗長化、稼働率、負荷分散、ロードバランサ、DoS	
	Web関連技術	URL/URI	スキーム名	0		URL/URIのフォーマットを理解している(S/G)	スキーム名、http、(https)、ftp、file、mailto、javascript、data	
		l	ホスト名	0		代表的なスキームと意味を理解している(S/G)	ホスト名、ドメイン、FQDN	
		l	ポート番号 クエリストリング	0		URLエンコードが必要な文字と方法を理解している(S/G) HTTP URLの各部分の意味を理解している(S/G)	ポート番号、well-knownポート、登録済みポート番号、80/tcp、443/tcp クエリストリング、URLパラメタ、GET、URL Rewriting、URLエンコード	
		1	クエリストリング フラグメント	0		HTTP URLの各部分の意味を理解している(S/G) base URLや絶対URLと相対パスの違いと挙動を理解している(S/G)	クエリストリング、URLバラメタ、GET、URL Rewriting、URLエンコード フラグメント勝則子 リンク	
		HTTP	フフクメント リクエスト/レスポンス	0	0	base URLや絶対URLと相対バスの遅いと挙動を理解している(S/G) 各種HTTPメソッドの役割を理解している(S/G)	ファクメント識別子、リンク リクエスト/レスポンス	
		niie	ッッエ ヘ F/ レヘホンス	J	٥ .	各種HTTPメソッドの役割を埋解している(S/G) GETとPOSTの違いを理解している(S/G)	リクエスト/レスポンス レスポンス分割、HTTPメッセージ、メッセージへッダ、メッセージボディ、エン	
		l				GETとPOSTの違いを理解している(S/G) HTTPがステートレスである性質を理解している(S/G)	レスホンス分割、HTIPメッセーン、メッセーンへッタ、メッセーンホティ、エン ティティボディ、メディアタイプ	
		l	メソッド	_		HTTPがステートレスである性質を埋解している(S/G) HTTPメッセージのフォーマットを理解している(S/G)	GET、POST、HEAD、OPTIONS、TRACE	
		l	/ / ツト	V			PUT. DELETE, CONNECT	
		I	ステータスコード	^	0	式を理解している(S/G)	100, 200, 206, 302, 304, 401, 403, 404, 405, 500	
							,,,,,,,,,	
			HTTP~~#	0		代表的なHTTPへッダフィールドの意味を理解している(S/G)	User-Agent, Referer, Connection, Keep-Alive, Range, Authorization, Host	
			HTTP~ッダ	0	0 1	代表的なHTTPヘッダフィールドの意味を理解している(S/G) 代表的なHTTPステータスコードの意味を理解している(S/G)	User-Agent、Referer、Connection、Keep-Alive、Range、Authorization、Host、 Cookie	
			НТТР~уУ	0	0	代表的なHTTPへッダフィールドの意味を理解している(S/G) 代表的なHTTPステータスコードの意味を理解している(S/G) HTTPのセッション管理機構の挙動について理解している(S/G) Cookieの各属性について挙動を理解している(S/G)		

分野	大分額	中分類	小分額	Silve	r Gold	スキル	用語例(修得すべき用語、キーワード)	備考
5525	737788	1 22 38	セキュリティ関連のHTTPへッ	×	0	3rdパーティーCookieについて理解している(S/G)	x-frame-options, x-content-type-options, x-xss-protection, Content Security	NO. 7
			y		_	代表的なHTTP認証の区別ができる(S/G)	Policy, Strict-Transport-Security, Cross-Origin Resource Sharing, Access-	
						バーチャルホストの挙動について理解している(S/G)	Control-Allow-Origin	
			Cookie	0	0	Refererの挙動について理解している(S/G)	domain, path, secure, httponly, expires	
			セッション管理	0	0	リダイレクトの挙動について理解している(S/G)	セッションタイムアウト、セッションID	
			Webプロキシ	0	0	任意のHTTPリクエストを送信できる(S/G)	HTTP、HTTPS、代理アクセス、キャッシング、フィルタリング、プロキシ認証、	
				4		セキュリティ関連のHTTPヘッダフィールドの意味を理解している(G)		
			Referer HTTP認証	0	0		Referer~yダ、リファラ、デリファラ	
			HIIP認証 リダイレクト	0	0		Basic認証、Digest認証 Location、Refresh	
		プロキシ	フォワードプロキシ	0	0	フォワードプロキシの仕組みを理解している(S/G)	たっという。 キャッシュ、負荷分散、WAF	
		プロヤン	リバースプロキシ	0	0	リバースプロキシの仕組みを理解している(S/G)	イヤツンユ、貝何方似、WAF	
		ブラウザ	ブラウザ基本機能	0	0	プラウザの基本的な動作を理解している(S/G)	レンダリング、キャッシュ、ステータスバー、アドレスバー、自動補完、オートコ	
			> > > > as-1-1wild		_	プラウザの各種インタフェースの役割を理解している(S/G)	ンプリート、自動フィルイン	
			拡張機能・開発者ツール	0	0	各種プラウザをインストールし利用できる(S/G)	デバッグ、DOM操作、F12	
			Ajax/XHR	0	0	各種プラウザの固有の挙動について理解している(G)	XMLHttpRequest、Same Origin Policy(同一生成元ポリシー)、非同期通信	
			XSSフィルタ	0	0	Ajax/XHRについて理解している(S/G)	XSS Auditor、XSS Filter、反射型XSS、x-xss-protection	
			Same Origin Policy	0	0	XSSフィルタについて、機能・仕組みを理解している(S/G)	Same Origin Policy(同一生成元ポリシー)	
			Content Sniffing	×	0	Same Origin Policyについて、機能・仕組みを理解している(S/G)	メディアタイプ、Content-Type、X-Content-Type-Options	
			Content Security Policy	×	0	Content sniffingについて、機能・仕組みを理解している(G)	Content-Security-Policy、インラインスクリプト	
			Cross-Origin Resource Sharing	×	0	Content Security Policyについて、機能・仕組みを理解している(G)	プリフライト、Originヘッダ、Access-Control-Allow-Origin	
						Cross-Origin Resource Sharingについて、機能・仕組みを理解して		
						いる(G)		
						プロキシサーバの設定が行える(S/G)		
		l				ブラウザの各機能について、ブラウザごとの挙動の際を理解している		
		エンコード	パーセントエンコーディング	_	_	(G) パーセントエンコーディングの仕組みを理解し、エンコード・デコー	文字コード LIPLエンコード	
	1		Base64	0	0	アーセントエンコーティングのL組みを理解し、エンコート・テコードを行える(S/G)	文字コード、ORLエンコード Basic認証	
	1	1		1	1	Base64エンコードの仕組みを理解し、エンコード・デコードを行え		
		l				る(S/G)		
	1	1	1	1	1	w()		
1	1	言語	HTML	0	0	HTMLの基本的な役割、機能を理解している(S/G)	HTMLタグ、実体参照、数値文字参照	
1	1	L-1 PD		ľ	Ŭ	HTMLの基本的な役割、機能を理解している(S/G) HTMLの構文を理解している(S/G)	TIME// XPPM MEATPM	
						HTMLの代表的なタグを理解している(S/G)		
						HTMLでエスケープする必要性と方法を理解している(S/G)		
						脆弱性検証用のHTMLを書ける(G)		
						HTML 実体参照の仕組みを理解し、エンコード・デコードができる		
						(S/G)		
						数値参照(16 進)の仕組みを理解し、エンコード・デコードができる		
						(S/G)		
			HTML5	×	0	HTML5の基本的な役割、機能を理解している(G)	WebStorage、Web Workers、svg、canvas、websocket、サンドボックス	
						HTML5で追加された代表的なタグ・機能を理解している(G)		
						脆弱性検証用のHTMLを書ける(G)		
			Tarra Carda A	-	-	1	FOMAC-St. 10-St. University of St. Aver. Astrology 15	
			JavaScript	0	0	JavaScriptの基本的な役割、機能を理解している(S/G) 基本的な構文を理解している(S/G)	ECMAScript、JScript、Unicodeエスケープシーケンス、イベントハンドラ	
						Micodeエスケープシーケンスの必要性と方法を理解している(S/G)		
						脆弱性検証用のJavaScriptを書ける(G)		
			CSS	0	0	CSSの基本的な役割、機能を理解している(S/G)	セレクタ、Expression	
			000	~	Ŭ	基本的な構文を理解している(S/G)	C V / / C Expression	
			SQL	0	0	SQLの基本的な役割、機能を理解している(S/G)	サブクエリ、副間い合わせ、プレースホルダ(静的/動的)、ストアドプロシージャ	
						基本的な構文やコメント・複文を理解している(S/G)		
						INFORMATION_SCHEMAについて理解している(G)		
						SQL特殊文字のエスケープの必要性と方法を理解している(S/G)		
						DBMSごとに固有の挙動があることを知っている(G)		
						脆弱性検証用のSQLを書ける(G)		
1	1	1	XPath	×	0	XPathの基本的な役割、機能を理解している(G) 基本的な構文を理解し	ロケーションパス	
	1	1	プログラミング言語	×	0	基本的な構文を理解している(G)		主にWebアプリケーションを記述するために用いるもの
	1		LVA.II	4—	4-	脆弱性検証用のウェブアプリケーションを書ける(G)	VOLT. PTD	
	1	データ形式	XML	0	0	基本的な構文を理解している(S/G)	XSLT, DTD	
	1	7. m/h	JSON	0	0	基本的な構文を理解している(S/G)	JSONP	
	1	その他	ロードバランス I DAP	×	0	仕組みを理解している(G)	ラウンドロビン方式、静的分散方式、動的分散方式 Active Directory LDIF (LDAP Interchange Format)	
		l	LDAF	1*	0	仕組みを理解している(G)	Active Directory, EDIF (EDAP Interchange Format)	
		l	Web API	×	0	概要を理解している(G)	REST, SOAP, XML-RPC	
		l	Special files	×	0	ファイルの役割、機能を理解している(G)	robots.txt, crossdomain.xml, .htaccess, clientaccesspolicy.xml	
		l	CGI	0	0	仕組みを理解している(S/G)	TODOIS.DX:、CIOSSOOMAIII.XIII、:Maccess 、Cilentaccesspolicy.XIIII 環境変数	
		l	DOM	0	0	DOMの役割、機能を理解している(S/G)	ツリー構造、ノード	
	その他	Webサーバの製品		0	0	代表的なWebサーバの製品名を知っている(S/G)	Apache, nginx, IIS	
	-	DBの製品名		0	0	代表的な DBの製品名、種類、代表的な特徴を理解している(S/G)	RDBMS, NoSQL	
		アプリケーション	サーバの製品名	0	0	代表的な アプリケーションサーバの製品名、種類、代表的な特徴を		
				<u> </u>		理解している(S/G)		
		プラグインの製品:	名	0	0	代表的な ブラウザのブラグインの製品名、種類、代表的な特徴を理		
					1	解している(S/G)		
		ライブラリ/フレー	ムワークの製品名	0	0		MVC	
		L				を理解している(S/G)		
	NAT 1 87 -211 1	検証環境構築	Inou do structura	×	0	上記のような代表的な製品の検証環境を作れる(G)	仮想環境、Vagrant、Docker、コンテナ	005001
	Webアプリケーション の胎弱件	インジェクション	SQLインジェクション	0	0	典型的なパターンの場合の脆弱性を発見する方法を知っている (S/G)	Blind SQL Injection, Second Order Injection, UNION Injection	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL
基礎知識(脆弱性)		1		+	+-	典型的なパターンの場合の脆弱性を発見できる (S/G)	Prepared Statement、プレースホルダ(静的/動的)、information schema	Injection')
基礎知識(脆弱性)	ONEWITE	1	コマンドインジェクション	0	0	典型的な対策方法を知っている (S/G) 典型的な被害を知っている (S/G)	OSコマンドインジェクション	OSコマンドインジェクション
基礎知識(脆弱性)	O DESCRITE		1	1	1	典型的な被害を知っている (S/G) 脆弱性を利用し被害の実証確認ができる(G)		CWE-77: Improper Neutralization of Special Elements used in a Command ('Command
基礎知識(脆弱性)	o nearte							Injection')
基礎知識(脱弱性)	ooneans:		I DAD インジェクション	~	^	肥羽性を利用し飲香の夫能傳統ができる(G) 監視性が発生する質用を理解している(C)		CWE-90: Improper Neutralization of Special Florents used in an LDAR Quart (II DAR)
基礎知識(脱弱性)	O JUL SUITE		LDAPインジェクション	×	0	肥物性を利用し飲香の天証準部ができる(G) 脆弱性が発生する原因を理解している(G)		CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP
基礎知識(能弱性)	олициять:			×	0	脱羽性が発生する原因を理解している (G)	Blind YPath Injection	Injection')
基礎知識(能弱性)	Oneson		XPathインジェクション	×	0	那部社を利用し飲含の天血(蝶&のかできる)(G) 脆弱性が発生する原因を理解している (G)	Blind XPath Injection	Injection') CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection')
基礎知識(能弱性)	Onewitz		XPathインジェクション XMLインジェクション	×	0	飛翔はど利用し板市が大正体能ができる(G) 脱羽性が発生する原因を理解している (G)		Injection') CWE-943: Improper Neutralization of Data within XPath Expressions ("XPath Injection") CWE-91: XML Injection (aka Blind XPath Injection)
基礎知識(能弱性)	Улент:		XPathインジェクション XMLインジェクション evalインジェクション	× × ×	0 0	現明社を利用し板音の失点機能がいてきる(b) 整钢性が発生する原因を理解している (G)	eval	Injection') CWE-943: Improper Neutralization of Data within XPath Expressions (XPath Injection') CWE-91: XML Injection (aka Blind XPath Injection) CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code (Eval Injection)
基礎知識(能弱性)	Олент		XPathインジェクション XMLインジェクション	× × × × × ×	0 0 0	飛頭性を利用し板音の失点機能ができる(C) 搬到性が発生する原因を理解している(G)		Injection') CWE-943: Improper Neutralization of Data within XPath Expressions ("XPath Injection") CWE-91: XML Injection (aka Blind XPath Injection)

分野	大分額	中分類	小分類	Silver	Gold	スキル	用語例(修得すべき用語、キーワード)	備老
~~	7 177 701	. 27 88	NoSQLインジェクション	×	0		NoSQL、キー・バリュー型、ソート済みカラム指向型、ドキュメント指向型	CWE-943: Improper Neutralization of Special Elements in Data Query Logic
			CRLFインジェクション	٥	٥		HTTPへッダインジェクション、メールヘッダインジェクション、HTTPレスポンス 分割(HTTPレスポンススプリッティング)	CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Spiltting')
			クロスサイトスクリプティング (XSS)	0	0		Reflected XSS、Stored XSS、DOM Based XSS、Server XSS、Client XSS、expression、XST	https://www.owasp.org/index.php/Types_of_Cross-Site_Scripting DOM based XSS
								Server XSS Client XSS CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
			フォーマットストリングバグ	×	0		フォーマット文字列、フォーマット関数	フォーマットストリング攻撃 CWE-134: Uncontrolled Format String
		パストラバーサル		0	0		ディレクトリトラバーサル、パス区切り文字、カレントディレクトリ、相対パス、 絶対パス	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') CWE-23: Relative Path Traversal ?file=./fil-file/passwd
		XMI 外部エンティ	ティ参照 (YYE)	_	0	-	OTTO	CWE-36: Absolute Path Traversa ?file=/etc/passwd CWE-611: Improper Restriction of XML External Entity Reference ('XXE')
		オープンリダイレ		0	0		オープンリダイレクタ、Location:レスポンスヘッダ、リダイレクト先ドメイン チェック	CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
		安全でないデシリ		0	0		オブジェクトインジェクション、シリアライゼーション、デシリアライゼーション	CWE-502: Deserialization of Untrusted Data
		ファイルアップ ロードに係る脆弱	サーバ側で実行されるファイル のアップロード	×	0		実行ファイル、ファイル名文字種制限	
		性	の アップロート クライアント側で実行される ファイルのアップロード	×	0		マジックバイト、Content-Type	
			許可されていないファイルの アップロード	×	٥		ファイルフォーマット(拡張子)制限、ファイル容量制限、アップロード先ディレクトリ制限	
		インクルードにま つわる脆弱性	リモートファイルインクルー ジョン(RFI)	0	0		RFI無効設定、include系関数	CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program (PHP Remote File Inclusion')
		サービス不能攻撃 (DoS)につながり うる問題		×	٥		メモリ領域、スタック、ヒープ、リターンアドレス	CWE-788: Access of Memory Location After End of Buffer
		レースコンディシ	コン	×	0		共有リソースの排他制御、競合状態、デッドロック	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
		クリックジャッキ:	ング Landanana	0	0		透過レイヤ、X-FRAME-OPTIONS	CWE-693: Clickjacking/Clickjack/UI Redress/UI Redressing
		認証	認証回避 ログアウト機能の不備や未実装	0	0	1	HTTP認証。セッション破棄。アクセストークン	CWE-592: Authentication Bypass Issues
			過度な認証試行に対する対策不 備・欠落	0	0		アカウントロック、ロックアウト、ブルートフォース攻撃、辞書攻撃、パスワード リスト攻撃	アカウントロック CWE-307: Improper Restriction of Excessive Authentication Attempts
			脆弱なパスワードポリシー 復元可能なパスワード保存	0	0		パスワード強度 ハッシュと暗号化、ソルト、ストレッチング、レインボーテーブル、パスワードリ	CWE-521: Weak Password Requirements CWE-257: Storing Passwords in a Recoverable Format
			パスワードリセットの不備	0	0		マインダ 秘密の質問、登録済メールアドレス、パスワードリセット設定拒否	,
			推測可能なCAPTCHA	×	0]	CAPTCHA	CWE-804: Guessable CAPTCHA
		認可制御の不備・ 欠落	権限の不正な昇格 強制プラウズ	0	0	1	アクセス制御	CWE-425: Direct Request ('Forced Browsing')
		Am.	パラメータ操作による不正な機 能の利用	0	0		なりすまし、デバッグオプション	OWL-423. Direct neguest (Loced browsing)
		セッション管理の 不備	セッションフィクセイション (セッション固定攻撃)	0	0		セッション管理、ログイン前セッション、セッションアダプション、セッションハ イジャック	CWE-384: Session Fixation
			クロスサイトリクエストフォー ジェリ(CSRF)	0	0		CSRF対策トークン、再認証、Referer	CWE-352: Cross-Site Request Forgery (CSRF)
			CookieのHttpOnly属性未設定	0	0		XSS	CEE In and March on Marches
		情報漏洩	推測可能なセッションID	0	0		暗号論的擬似乱数生成器、セッションハイジャック Referer、URLリライティング	(長さ・乱数の強度) CWE-334: Small Space of Random Values IU駅 パラメータ
		1月 宋 6 年 7 年 7 年 7 年 7 年 7 年 7 年 7 年 7 年 7 年	クエリストリング情報の漏洩 キャッシュからの情報漏洩	٥	٥		HTTPリダイレクション、cache-controlヘッダ、pragmaヘッダ、expiresヘッダ、	URL 77 X = 9 CWE-598: Information Exposure Through Query Strings in GET Request CWE-524: Information Exposure Through Caching
				٥	0		last-modified	, , ,
			パスワードフィールドのマスク 不備	0	٥		パスワードフィールド	CWE-549: Missing Password Field Masking
			エラーメッセージによる情報露出	٥	٥		カスタムエラーメッセージ、エラーメッセージの抑制	CWE-209: Information Exposure Through an Error Message
			機徽情報の表示 HTTPS利用時のsecure属性がな	0	0			確認画面でクレジットカード番号などのマスクを行っていない CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
			い機像Cookie 機微情報の平文保存	0	0			CWE-312: Cleartext Storage of Sensitive Information
			HTTPSの不適切な利用 不要な情報の存在	0	0	1	独自CA、SSL、TLS、HSTS	攻撃のヒントになるような情報がコメントなどに記載されている
	MI-L 22 211 7 - 3	ビジネスロジック(×	0]	ladama S habarda	設計上の問題 CMF 540 kf
	Webアプリケーション の動作環境への診断項	サーバソフトウェ アの設定の不備	ディレクトリリスティング バージョン番号表示	0	0	1	Indexes、アクセス権 ServerSignature、ServerTokens、server tokens	CWE-548: Information Exposure Through Directory Listing
	E		不要なHTTPメソッド	ō	o]	TRACE, PUT, DELETE	
1		不要な機能・ファ- OS/フレームワー?	イル・ディレクトリの存在 カ/サーバソフトウェア/プログラ	°	0	-	バックアップファイル、サンプルファイル、公開不要な管理機能	
基礎知識(診断業 務)	診断前・準備	診断対象の確認	テストケースの作成	0	0	画面、リクエスト、アクション、パラメータを洗い出す方法を理解している(S/G)	CVE 画面遷移図、リクエスト、アクション、パラメータ、サイトマップ、I/F仕様書(API の場合)	
170)			診断対象の優先順位付け	×	0	優先順位付けの基準とその必要性を理解している(G)	×/	
1		merchen as 1 51	診断対象の選定	×	0	診断対象の選定ができる(G)		
1		見積もり方法	画面カウント制 アクションカウント制	×	0	サービスを提供するうえで、見積を作るための基準、算出方法を理解 している(G)	画面数 アクション数	
			リクエストカウント制	×	0	S (. S(S)	リクエスト数	
			その他の見積もり方法について	×	0		サイト数、ドメイン数、機能数(検索機能の円、ログイン機能の円など)	
		顧客との事前打ち 合わせ	実施内容説明	×	0	診断を実施するにあたり、事前に説明すべき事項とその必要性を理解 している(G)		診断概要、診断項目、サービス提供の流れ、サービス提供の範囲(作業内容、提出物、提供期間など)、診断時の注意事項について
•		•		•	•	•		

	大分類	中分類	小分類	Silver	Gold	スキル	用語例(修得すべき用語、キーワード)	備考
			ヒアリング	×	0	事前に確認すべき事項とその必要性を理解している(G)		以下のような項目のヒアリングが診断事前に必要と思われる
]			1	1				・アプリケーション(サービス)の概要について
			1	1				・診断対象サイトの利用用途について(PC向け、モバイル向け、スマートフォンアプリと連携など)
			1	1				と) ・システム、ネットワーク構成
			1					・診断の実施形態について(リモート実施可能か、オンサイト実施か)
]			1	1				・診断対象のプラットフォームについて(オンプレミス、ホスティング環境、クラウド利用など)
]			1	1				・診断対象環境情報について(OS、利用言語、フレームワーク、DBMS、パッケージ製品の利用
			1	l				有無)
			1					・アプリケーションに存在する権限について ・アプリケーションの認証方式(フォーム認証、Basic認証、クライアント認証など)
			1					・診断対象範囲(ドメイン、機能、権限など)
			感· → → → → → → → → → → → → → → → → → → →	Ų.		参照が色です前に灌飾さい幅//ナッキ車でに ヘノ、マ畑Φ1 マ・マバ		・テフト環接 フテージング環接の女無
			環境・データ準備依頼	*	0	診断対象で事前に準備をお願いすべき事項について理解している(G)		診断対象のシステム担当者と以下のような項目について事前調整が必要と思われる ・アクセス元 I P から疎通可能な状態にしてもらう
			1	l				アクセスに必要な情報を取得(テスト用アカウント情報、ダミークレジットカードデータ、物理
			1	1				デバイス、クライアント証明書、指定UA、専用の横入り画面の利用、特定のパラメータ等を付
			1	1				加する必要など)
								・アカウントによって権限や遷移可能な画面が分れていたりする場合には複数のテストアカウントの取得調整が必要
			1	l				アクセスするために、が必要な場合などもある
								・非監視対応依頼をしてもらう(IDS・IPS・WAF)
								・プラットフォーム管理元への脆弱性診断実施の事前許可をいただく
I			1	1				・テスト環境やステージング環境があればそちらでの実施について推奨する・診断事前のデータバックアップのお願い
			1	1				・診断事前のテータバックアップのお願い・診断時までに、正常遷移可能な診断用のダミーデータの投入をお願いする
			1	1				・仕様書、画面遷移図などのドキュメントの提供をお願いする
			1	1				WebAPIなどを診断するためには、正常処理される送信パラメータ、応答結果などが記載され
								ている仕様書の入手が必要
			作業環境の準備依頼	×	0	オンサイト環境で事前に準備をお願いすべき事項について理解してい		診断対象のシステム担当者と以下のような項目について事前調整が必要と思われる
						る(G)		・診断端末に割り振るIPアドレスなどの情報の入手
I			1	1				・診断対象ネットワークへの接続方法(LANポートの確保・ネットワークケーブル、VPNなど) ・電源の確保
								作業場所の情報について(ロケーション、入館申請方法、立ち合い担当者の情報など)
			診断環境による差違	×	0	診断環境による差異を理解している(G)	本番環境、テスト(ステージング)環境	テスト環境を利用して診断を実施する場合には、本番環境のものと同一のコンテンツである必要 *****
			禁止事項	٥	0	禁止事項の確認とその必要性を理解している(S/G)		診断対象範囲以外の箇所には診断実施をしない 取り決められた時間帯以外には診断実施をしない
			1					診断データやログについては定めされた範囲内でしか取り扱わない
			1					診断結果を許可なく第三者に伝えたり、公開したりしない
			Ì	1				その他、顧客から指示があった禁止事項について厳守する
			A strategy			At the above as related 1, 27 as 30 mellat. A resident	11 12 15 THE HIGH	
		診断準備	免責事項 作業環境の準備	×	0	免責事項の確認とその必要性を理解している(G) 診断環境に応じて、必要な機材を準備できる(S/G)	サービス利用規約	
			必要機材	0	0	診断に必要なツールのインストール、及び、バージョンアップ、ライ		診断PC、ネットワークケーブル、スイッチングハブ、電源タップ、セキュリティワイヤー
			診断ツールの準備	0	0	センス更新ができる(S/G) 顧客の要件に合わせた適切なバージョンのクライアントを準備できる		自動診断ツール、手動診断ツール、ローカルプロキシ、ライセンス取得・更新、ブラウザプラグ イン
			クライアントの準備	0	0	(S/G)		取り決められたルールにのっとり準備(セキュリティパッチの適用、HDDの暗号化など)
			セキュリティツールの影響	0	0	アンチウイルスソフトなどのセキュリティツールによって生じる影響		利用するアンチウイルスソフトについての仕様理解、影響を避けるための事前設定など
			1			を理解している(S/G)		
			l			Windows とLinuxで、IPアドレス・ルーティングやデフォルトゲート		
	診断	ログ取得 自動診断ツールを	田いた砂転	0	0	診断時のログ保存方法とその必要性を理解している(S/G)		
		目動診断ツールを プロキシツールを		0	0	自動診断ツールを用いた診断の業務フローを理解している (S/G) プロキシツールを用いた手動による診断の業務フローを理解している		
				Ĺ		(S/G)		
	診断実施後・アフター	報告会		×	0	報告書を用いて、内容を説明できる(G)		
	サポート	診断実施後のデー	タの取り扱い			診断実施後のデータの保存理由とその必要性を理解している(S/G)		提出するデータ内容、保存場所、保存期間、診断実施後のサポート対応範囲・対応期間
	1	問い合わせ対応		0	J			
		正於斯		×	0	診断実施後の問い合わせ対応ができる(G) 亜診断の業務フローを理解している (S/G)		提権! た胎弱性が修正されていることを確認すること
診断技術(診断	自動診断ツールの特徴	再診断		o × o	000	診断実施後の問い合わせ対応ができる(G) 再診断の業務フローを理解している (S/G) 一般的な自動診断ツールの診断方法について理解している(S/G)		指摘した脆弱性が修正されていることを確認すること。 一般的な自動診断ツールでは、ツールによる自動巡回機能または診断者の手動作業によりWebサ
診断技術(診断 ツール)	自動診断ツールの特徴	再診断		o × o	0 0	再診断の業務フローを理解している (S/G)		
	自動診断ツールの特徴	再診断		o *	0 0 0	再診断の業務フローを理解している (S/G) 一般的な自動診断ツールの診断方法について理解している(S/G)		一般的な自動診断ツールでは、ツールによる自動巡回機能または診断者の手動作業によりWebサイトをクロールし、発見したパラメーターに対して、検出バターンを挿入し、腕勁性を発見する。
	自動診断ツールの特徴	再診断		o × o	0 0	再診断の業務フローを理解している (S/G) 一般的な自動診断ツールの診断方法について理解している(S/G)		一般的な自動診断ツールでは、ツールによる自動巡回機能または診断者の事動作業によりWebサイトをクロールし、発見したパラメーターに対して、検出パターンを挿入し、脆弱性を発見する。 検出ロジックとしては、正常時のレスボンスと、検出パターン挿入時のレスボンスを比較する。
		再診断 診断方法	M:	o × o	0000	再診断の業務フローを理解している (S/G) 一般的な自動診断ツールの診断方法について理解している (S/G) 一般的な自動診断ツールの検出ロジックについて理解している (S/G)		一般的な自動診断ツールでは、ツールによる自動※回機能または診断者の手動作業によりWebサイトをクロールし、発見したパラメーターに対して、検出バターンを挿入し、能別性を発見する。 核出ロジックとしては、正常時のレスポンスと、検出パターン挿入時のレスポンスを比較する。 または、レスポンスに含まれる特定の文字列を検出するなどして能別性の検出を行う。
		再診断	性	o × o	0 0 0	再診断の業務フローを理解している (S/G) 一般的な自動診断ツールの診断方法について理解している(S/G)		一般的な自動診断ツールでは、ツールによる自動返回機能または診断者の手動作業によりWebサイトをクロールし、発見したパラメーターに対して、検出パターンを挿入し、能調性を発見する。 検出ロジックとしては、正常時のレスポンスと、検出パターン挿入時のレスポンスを比較する。 または、レスポンスに含まれる特定の文字列を検出するなどして施研性の検出を行う。 SQLインジェクションやXSSなどの値をインジェクションさせるタイプの能測性、HTMLや Coolieなどのセキュリティ波定不備。ディレクトリやファイルの発見、ブレームワークサーバ
		再診断 診断方法 検出が得意な脆弱		o x o o	0 0	再診断の実務プローを理解している (S/G) 一般的な自動診断ツールの診所方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G)		一般的な自動診断ツールでは、ツールによる自動巡回機能または診断者の事動作業によりWebサイトをクロールし、発見したパラメーターに対して、検出パターンを挿入し、能制性を発見する。 ・機田ロジックとしては、正常時のレスポンスと、検出パターン挿入時のレスポンスと比較する。 または、レスポンスに含まれる特定の文字列を検出するなどして能動性の検出みを比較する。 または、レスポンスに含まれる特定の文字列を検出するなどして能動性の検出みを比較する。 SOLインジェクションやXSSなどの値をインジェクションさせるタイプの能弱性、HTMLや Cookleなどのセキュリティ設定不順、ディレクトリやファイルの発見、フレームワーク/サーバ ソフトウェアの既知の能明性など
		再診断 診断方法		o x o o	0 0	再診断の業務フローを理解している (S/G) 一般的な自動診断ツールの診断方法について理解している (S/G) 一般的な自動診断ツールの検出ロジックについて理解している (S/G)		一般的な自動診断ツールでは、ツールによる自動部回機能または診断者の手動作業によりWebサイトをクロールし、発見したパラメーターに対して、検出パターンを挿入し、能場性を発見する。 検出ロジックとしては、正常時のレスポンスと、検出パターン・挿入時のレスポンスを比較する。 または、レスポンスに含まれる特定の文字列を検討するなどして観察性の検出を行う。 SQLインジュクションや水SSなどの値をインジュクションさせるタイプの影響性、HTMLや Cookieなどのセキュリティ(表写不順、ディレクト)やウァイルの発見、フレースリーケーソフトウ・フの既知の機能性など セッション管理の不順、影可制御の不備・欠落、意図しない仕様外の挙動、ビジネスロジック上
		再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱		o x o o o o o o o o o o o o o o o o o o	0 0	再診断の実務プローを理解している(S/G) 一般的な自動診断ツールの診所方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 検出が難しい代表的な脆弱性を理解している(S/G)		一般的な自動診断ツールでは、ツールによる自動巡回機能または診断者の事動作業によりWebサイトをクロールし、発見したパラメーターに対して、検出パターンを挿入し、能明性を発見する。 ・機田ロジックとしては、正常時のレスポンスと、検出パターン挿入時のレスポンスと比較する。 または、レスポンスに含まれる特定の文字列を検出するなどして能明性の検出みを比較する。 または、レスポンスに含まれる特定の文字列を検出するなどして能明性の検出みを比較する。 SOLインジェクションやXSSなどの値をインジェクションさせるタイプの能弱性、HTMLや Cookleなどのセキュリティ設定不順、ディレクトリやファイルの発見、フレームワーク/サーバ ソフトウェアの既知の能明性など
		再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断	性が適している処理・機能	o x o o o o o o o o o o o o o o o o o o	0 0 0	再診断の実務プローを理解している (S/G) 一般的な自動診断ツールの診所方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 検出が釋しい代表的な脆弱性を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G)		一般的な自動診断ツールでは、ツールによる自動返回機能または診断者の手動作業によりWebサイトをクロールし、発見したパラメークーに対して、検出パターンを挿入し、能弱性を発見する。 検出ロジックとしては、正常時のレスポンスと、検出パターン挿入人時のレスポンスを比較する。または、レスポンスに含まれる特定の文字列を検出するなどして随野性の検出を行う。 SOLインジェクション学外SSなどの値をインジェクションさせるタイプの聴労性、HTMLや Cookieなどのキュリティ状態を発生のジェクションさせるタイプの聴労性、HTMLや Cookieなどのキュリティ状態を発生のイルクトリやファイルの発見、フレームワーク/サーバソフトウェアの医知の聴労性など セッション管理の不偏、影可制御の不備・欠落、意図しない仕様外の挙動、ビジネスロジック上の問題、CSRでなど 検索処理やアンケートなど複数回同じ処理を行える機能、マクロ化による診断手順の自動化
		再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断 ツールによる診断	性	0 x 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0	再診断の実務プローを理解している(S/G) 一般的な自動診断ツールの診所方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 検出が難しい代表的な脆弱性を理解している(S/G)	CAPTCHA、二架希認証(多架素認証)・二段階認証	一般的な自動診断ツールでは、ツールによる自動部回機能または診断者の手動作業によりWebサイトをクロールし、発見したパラメーターに対して、検出パターンを挿入し、能弱性を発見する。 ・ 機田ロジックをしては、正常時のレンボンスと、検出パターンを挿入し、能弱性を発見する。 または、レスポンスに含まれる特定の文字列を検出するなどして施弱性の検出を行う。 SQLインジュクションマ水SSなどの値をインジュクションさせるタイプの施弱性、HTMLで Coolieなどのセキュリティ会形で編。ディレクトリやファイルの発見、プレームワークけーバ ソフトウェアの更知の施弱性など セッション管理の不備。認可制御の不備・大落、意図しない仕様外の挙動、ビジネスロジック上の閲覧、CSRFなど 検索処理やアンケートなど複数回同し処理を行える機能、マクロ化による診断手順の自動化 処理が複数ページに渡る骨線型の検出、入力値の影響が次画面ではなく他の画面にでるもの。手
		再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断	性が適している処理・機能	o x o o o o o o o o o o o o o o o o o o	0 0 0	再診断の実務プローを理解している (S/G) 一般的な自動診断ツールの診所方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 検出が釋しい代表的な脆弱性を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G)	CAPTCHA、二要素認証(多要素認証)・二段階認証	- 板的な自動診断ツールでは、ツールによる自動返回機能または診断者の手動作業によりWebサイトをクロールし、発見したパラメーターに対して、検出パターンを挿入し、能弱性を発見する。 検出ロジックとしては、正常時のレスポンスと、検出パターン挿入内時のレスポンスを比較する。または、レスポンスに含まれる特定の文字列を検出するなどして施弱性の検担を行う。 SQLインジェクション学なSSなどの値をインジェクションさせるタイプの聴動性、HTMLや Cookieなどのセキュリティ賞を不備。ディレクトリやファイルの発見、プレームワークリサーバ ソフトウェアの既知の態態性など セッション管理のを開発など セッション管理の不備、認可制御の不備・ケス席、意図しない仕様外の挙動、ビジネスロジック上 の問題、CSRFなど 検索処理やアンケートなど複数回回に処理を行える機能、マクロ化による診断手順の自動化 処理が複数ページに渡る持続型の検出。入力値の影響が次端面ではなく総の画面にでるもの。手順を決めるとが困難でシナリオを作ることができないもの、ゲームなどレスポンスポランダム
		再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断 ツールによる診断	性が適している処理・機能	o x o o o o o o o o o o o o o o o o o o	0 0 0	再診断の実務プローを理解している (S/G) 一般的な自動診断ツールの診所方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 検出が釋しい代表的な脆弱性を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G)	CAPTCHA、二要素認証(多要素認証) - 二段階認証	一般的な自動診断ツールでは、ツールによる自動窓回機能または診断者の手動作業によりWebサイトをクロールし、発見したバラメーターに対して、検出パターンを挿入し、能弱性を発見する。 を出ロジックとしては、正常時のレスボンスと、核出パターンを挿入し、能弱性を発見する。 または、レスボンスに含まれる特定の文字列を検出するなどして範弱性の検出を行う。 SQLインジェクションでXSSなどの能をインジェクションでも6クイブの総対性、HTMLや Cooksなどのセキュリティ表定不順、ディレクトリケラアイルの発見、フレームワークリサーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケラアイルの発見、フレームワークリケーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケースでは、全球発型やアンケートなど複数回回じ処理を行える機能、マクロ化による診断手順の自動化 処理が複数ベージに渡る背接型の検出。入力値の影響が次面面ではなく他の画面にでるもの。手順を決めることが困難でナナリオを作ることができないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなりの可能がある。
		再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断 ツールによる診断 な処理・機能	性が適している処理・機能	o	0 0 0	再診断の実務プローを理解している(S/G) 一般的な自動診断ツールの診所方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得度な代表的な脆弱性を理解している(S/G) 検出が難しい代表的な脆弱性を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G)	CAPTCHA、二要素認証(多要素認証) - 二段階認証	- 板的な自動診断ツールでは、ツールによる自動返回機能または診断者の手動作業によりWebサイトをクロールし、発見したパラメーターに対して、検出パターンを挿入し、能弱性を発見する。 検出ロジックとしては、正常時のレスポンスと、検出パターン挿入内時のレスポンスを比較する。または、レスポンスに含まれる特定の文字列を検出するなどして施弱性の検担を行う。 SQLインジェクション学なSSなどの値をインジェクションさせるタイプの聴動性、HTMLや Cookieなどのセキュリティ賞を不備。ディレクトリやファイルの発見、プレームワークリサーバ ソフトウェアの既知の態態性など セッション管理のを開発など セッション管理の不備、認可制御の不備・ケス席、意図しない仕様外の挙動、ビジネスロジック上 の問題、CSRFなど 検索処理やアンケートなど複数回回に処理を行える機能、マクロ化による診断手順の自動化 処理が複数ページに渡る持続型の検出。入力値の影響が次端面ではなく総の画面にでるもの。手順を決めるとが困難でシナリオを作ることができないもの、ゲームなどレスポンスポランダム
		再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断 ツールによる診断	性が適している処理・機能	o x o o o o o o o o o o o o o o o o o o	0 0 0 0 0 0 0 0	再診断変務プローを理解している(C)(G) 一般的な自動診断ツールの診断方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 検出が構しい代表的な脆弱性を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G)	CAPTCHA、二要素認証(多要素認証)・二段階認証	一般的な自動診断ツールでは、ツールによる自動窓回機能または診断者の手動作業によりWebサイトをクロールし、発見したバラメーターに対して、検出パターンを挿入し、能弱性を発見する。 を出ロジックとしては、正常時のレスボンスと、核出パターンを挿入し、能弱性を発見する。 または、レスボンスに含まれる特定の文字列を検出するなどして範弱性の検出を行う。 SQLインジェクションでXSSなどの能をインジェクションでも6クイブの総対性、HTMLや Cooksなどのセキュリティ表定不順、ディレクトリケラアイルの発見、フレームワークリサーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケラアイルの発見、フレームワークリケーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケースでは、全球発型やアンケートなど複数回回じ処理を行える機能、マクロ化による診断手順の自動化 処理が複数ベージに渡る背接型の検出。入力値の影響が次面面ではなく他の画面にでるもの。手順を決めることが困難でナナリオを作ることができないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなりの可能がある。
	自動診断ツールの遷定	再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断 ツールによる診断 な処理・機能	性が適している処理・機能	0	0 0 0 0 0 0 0 0 0 0	再診断の実務プローを理解している(S/G) 一般的な自動診断ツールの診所方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得度な代表的な脆弱性を理解している(S/G) 検出が難しい代表的な脆弱性を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G)	CAPTCHA、二要素認証(多要素認証)・二段階認証	一般的な自動診断ツールでは、ツールによる自動窓回機能または診断者の手動作業によりWebサイトをクロールし、発見したバラメーターに対して、検出パターンを挿入し、能弱性を発見する。 を出ロジックとしては、正常時のレスボンスと、核出パターンを挿入し、能弱性を発見する。 または、レスボンスに含まれる特定の文字列を検出するなどして範弱性の検出を行う。 SQLインジェクションでXSSなどの能をインジェクションでも6クイブの総対性、HTMLや Cooksなどのセキュリティ表定不順、ディレクトリケラアイルの発見、フレームワークリサーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケラアイルの発見、フレームワークリケーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケースでは、全球発型やアンケートなど複数回回じ処理を行える機能、マクロ化による診断手順の自動化 処理が複数ベージに渡る背接型の検出。入力値の影響が次面面ではなく他の画面にでるもの。手順を決めることが困難でナナリオを作ることができないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなりの可能がある。
	自動診断ツールの適定	再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断 ツールによる診断 な処理・機能	性 が適している処理・機能 が適していないまたは実施不可能	0		再診断の実務プローを理解している(S/G) 一般的な自動診断ツールの診断方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 検出が構しい代表的な脆弱性を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G) フールが検出可能な脆弱性、診断方法、検出方法、利点や欠点、リスクなどを理解してツールを選定できる(G/G) ライセンスは、で、機能が異なるととを理解している	CAPTCHA、二要素認証(多要素認証) - 二段階認証	一般的な自動診断ツールでは、ツールによる自動窓回機能または診断者の手動作業によりWebサイトをクロールし、発見したバラメーターに対して、検出パターンを挿入し、能弱性を発見する。 を出ロジックとしては、正常時のレスボンスと、核出パターンを挿入し、能弱性を発見する。 または、レスボンスに含まれる特定の文字列を検出するなどして範弱性の検出を行う。 SQLインジェクションでXSSなどの能をインジェクションでも6クイブの総対性、HTMLや Cooksなどのセキュリティ表定不順、ディレクトリケラアイルの発見、フレームワークリサーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケラアイルの発見、フレームワークリケーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケースでは、全球発型やアンケートなど複数回回じ処理を行える機能、マクロ化による診断手順の自動化 処理が複数ベージに渡る背接型の検出。入力値の影響が次面面ではなく他の画面にでるもの。手順を決めることが困難でナナリオを作ることができないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなりの可能がある。
	自動診断ツールの適定	再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断 ツールによる診断 な処理・機能	性 が適している処理・機能 が適していないまたは実施不可能 ライセンス確認	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		再診断の業務プローを理解している(S/G) 一般的な自動診断ツールの診断方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 一ルによる診断が適している処理・機能を理解している(S/G) フールによる診断が適している処理・機能を理解している(S/G) ブールによる診断が適している処理・機能を理解している(S/G) ブールによる診断が適していない処理・機能を理解している(S/G) フールによる診断が適していない処理・機能を理解している(S/G) フールンなどを理解してジールを選定できる(G) フィセンスが成功であることを理解している(S/G) フィセンスによって機能が異なる場合があることを理解している (S/G)		一般的な自動診断ツールでは、ツールによる自動窓回機能または診断者の手動作業によりWebサイトをクロールし、発見したバラメーターに対して、検出パターンを挿入し、能弱性を発見する。 を出ロジックとしては、正常時のレスボンスと、核出パターンを挿入し、能弱性を発見する。 または、レスボンスに含まれる特定の文字列を検出するなどして範弱性の検出を行う。 SQLインジェクションでXSSなどの能をインジェクションでも6クイブの総対性、HTMLや Cooksなどのセキュリティ表定不順、ディレクトリケラアイルの発見、フレームワークリサーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケラアイルの発見、フレームワークリケーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケースでは、全球発型やアンケートなど複数回回じ処理を行える機能、マクロ化による診断手順の自動化 処理が複数ベージに渡る背接型の検出。入力値の影響が次面面ではなく他の画面にでるもの。手順を決めることが困難でナナリオを作ることができないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなりの可能がある。
	自動診断ツールの適定	再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断 ツールによる診断 な処理・機能	性 が適している処理・機能 が適していないまたは実施不可能	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		再診断の実務プローを理解している(G/G) 一般的な自動診断ツールの診断方法について理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 検出が構造しい代表的な脆弱性を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G) フールによる診断が適していない処理・機能を理解している(S/G) フールンなが有効であることを確認できる(G/G) フイセンスに、つて機能が異なる場合があることを理解している(S/G) メグタチャのアップデートができること(S/G)	CAPTCHA、二要素認証(多要素認証)・二段階認証 シグネチャ、ペイロード	一般的な自動診断ツールでは、ツールによる自動窓回機能または診断者の手動作業によりWebサイトをクロールし、発見したバラメーターに対して、検出パターンを挿入し、能弱性を発見する。 を出ロジックとしては、正常時のレスボンスと、核出パターンを挿入し、能弱性を発見する。 または、レスボンスに含まれる特定の文字列を検出するなどして範弱性の検出を行う。 SQLインジェクションでXSSなどの能をインジェクションでも6クイブの総対性、HTMLや Cooksなどのセキュリティ表定不順、ディレクトリケラアイルの発見、フレームワークリサーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケラアイルの発見、フレームワークリケーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケースでは、全球発型やアンケートなど複数回回じ処理を行える機能、マクロ化による診断手順の自動化 処理が複数ベージに渡る背接型の検出。入力値の影響が次面面ではなく他の画面にでるもの。手順を決めることが困難でナナリオを作ることができないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなりの可能がある。
	自動診断ツールの適定	再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断 ツールによる診断 な処理・機能	性 が適している処理・機能 が適していないまたは実施不可能 ライセンス確認	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		所診断を養務プローを理解している(S/G) 一般的な自動診断ツールの診所を注こいて理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G) フールによる診断が適していない処理・機能を理解している(S/G) フールによる診断が適していない処理・機能を理解している(S/G) シールが検別であることを確認できる(S/G) フィセンスによって機能が異なる場合があることを理解している(S/G) シグネテャのアップデートができること(S/G) 自動診断シールが使用するシグネテャ(診所パターン、ペイロード)のアップデートができること(S/G)		一般的な自動診断ツールでは、ツールによる自動窓回機能または診断者の手動作業によりWebサイトをクロールし、発見したバラメーターに対して、検出パターンを挿入し、能弱性を発見する。 を出ロジックとしては、正常時のレスボンスと、核出パターンを挿入し、能弱性を発見する。 または、レスボンスに含まれる特定の文字列を検出するなどして範弱性の検出を行う。 SQLインジェクションでXSSなどの能をインジェクションでも6クイブの総対性、HTMLや Cooksなどのセキュリティ表定不順、ディレクトリケラアイルの発見、フレームワークリサーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケラアイルの発見、フレームワークリケーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケースでは、全球発型やアンケートなど複数回回じ処理を行える機能、マクロ化による診断手順の自動化 処理が複数ベージに渡る背接型の検出。入力値の影響が次面面ではなく他の画面にでるもの。手順を決めることが困難でナナリオを作ることができないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなりの可能がある。
	自動診断ツールの適定	再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断 ツールによる診断 な処理・機能	性 が適している処理・機能 が適していないまたは実施不可能 ライセンス確認 シグネチャのアップデート	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		再診断の業務プローを理解している(C)(円) 一般的な自動診断ツールの終出ロジックについて理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 検出が構進しい代表的な脆弱性を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G) フールによる診断が適していない処理・機能を理解している(S/G) フールによる診断が適していない処理・機能を理解している(S/G) フィセンスが前効であることを確定できる(S/G) ライセンスが高効であることを認定(S/G) ライヤンスが高かであることを理解している (S/G) シグネティのアップデートができること(S/G) 自動診断ツールが使用するシグネティ(診断パクーン、ペイロード)の アップデートで、最新の診断手法に対応する必要性について理解して いる(S/G) シグネティのアップデートで、最新の診断手法に対応する必要性について理解して いる(S/G) シグネア・(S/G) シグネア・(S/G) シグネア・(S/G) シグネア・(S/G) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		一般的な自動診断ツールでは、ツールによる自動窓回機能または診断者の手動作業によりWebサイトをクロールし、発見したバラメーターに対して、検出パターンを挿入し、能弱性を発見する。 を出ロジックとしては、正常時のレスボンスと、核出パターンを挿入し、能弱性を発見する。 または、レスボンスに含まれる特定の文字列を検出するなどして範弱性の検出を行う。 SQLインジェクションでXSSなどの能をインジェクションでも6クイブの総対性、HTMLや Cooksなどのセキュリティ表定不順、ディレクトリケラアイルの発見、フレームワークリサーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケラアイルの発見、フレームワークリケーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケースでは、全球発型やアンケートなど複数回回じ処理を行える機能、マクロ化による診断手順の自動化 処理が複数ベージに渡る背接型の検出。入力値の影響が次面面ではなく他の画面にでるもの。手順を決めることが困難でナナリオを作ることができないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなりの可能がある。
	自動診断ツールの適定	再診断 診断方法 検出が得意な脆弱 検出が難しい脆弱 ツールによる診断 ツールによる診断 な処理・機能	性 が適している処理・機能 が適していないまたは実施不可能 ライセンス確認	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		所診断を養務プローを理解している(S/G) 一般的な自動診断ツールの診所を注こいて理解している(S/G) 一般的な自動診断ツールの検出ロジックについて理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) 検出が得意な代表的な脆弱性を理解している(S/G) ツールによる診断が適している処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G) ツールによる診断が適していない処理・機能を理解している(S/G) フールによる診断が適していない処理・機能を理解している(S/G) フールによる診断が適していない処理・機能を理解している(S/G) シールが検別であることを確認できる(S/G) フィセンスによって機能が異なる場合があることを理解している(S/G) シグネテャのアップデートができること(S/G) 自動診断シールが使用するシグネテャ(診所パターン、ペイロード)のアップデートができること(S/G)		一般的な自動診断ツールでは、ツールによる自動窓回機能または診断者の手動作業によりWebサイトをクロールし、発見したバラメーターに対して、検出パターンを挿入し、能弱性を発見する。 を出ロジックとしては、正常時のレスボンスと、核出パターンを挿入し、能弱性を発見する。 または、レスボンスに含まれる特定の文字列を検出するなどして範弱性の検出を行う。 SQLインジェクションでXSSなどの能をインジェクションでも6クイブの総対性、HTMLや Cooksなどのセキュリティ表定不順、ディレクトリケラアイルの発見、フレームワークリサーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケラアイルの発見、フレームワークリケーバソフトウェアの原知の態勢性など セッション管理の不順、認可制度の不順、ディレクトリケースでは、全球発型やアンケートなど複数回回じ処理を行える機能、マクロ化による診断手順の自動化 処理が複数ベージに渡る背接型の検出。入力値の影響が次面面ではなく他の画面にでるもの。手順を決めることが困難でナナリオを作ることができないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ゲームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなどの再現性のないもの、一度しか来できないもの。ケームなどレスボンスがランダムに変わるなりの可能がある。

分野	大分額	中分類	小分額	Silver G	old スキル	用語例(修得すべき用語、キーワード)	備老
20-21	2 C 24 28t	1 2/38	タイムアウトの設定	o o	タイムアウト値の設定ができる(S/G)		nu · y
					タイムアウト値を適切に設定し、対象サーバからのレスポンスを受	tt i	
			対象スコープの設定	0 0	取る時間を調整できる (G) 対象スコープの設定ができる(S/G)		
					診断対象ドメインもしくは診断対象URL以外に診断を実施しないよ	5	
			セッション識別子の確認	0 0	対象スコープを設定できる(S/G) 認証状態を継続するためのセッション識別子を判別し、設定できる		
			C 2 2 2 88/01 1 4248/80		(S/G)		
			クレデンシャルの設定	ļ. ļ.	クレデンシャルを設定できる(S/G)		
			CSRFトークン	0 0	CSRF対策として使用されているCSRFトークンを判別し設定できる	,	
					(S/G)		
			SSL証明書の設定	0 0	クライアントSSL証明書が必要な場合、クライアントSSL証明書を 定できる(S/G)	段 PKCS#12、インボートバスワード、CN	
			ログ設定の確認	0 0	自動診断ツールが実施した診断を記録するために必要なログの設定	·	
					適切に行える(S/G) ログを取得する意味を理解している(S/G)		
					ログが正しく書き込まれていることを確認できる(S/G)		
	自動診断の実施の準 備、設定	シナリオ作成	シナリオ(ジョブ・マクロ、ワー クフロー)の作成	0 0	テストケースからシナリオを作成できる(S/G) 対象サイトにアクセスし必要なシナリオを作成できる(S/G)	画面遷移図、セッション、トークン、CAPTCHA、ワンタイムURL、Cookie、パラメータ(POST、GET)、アカウントロック	
	侧、政化		y y u — just Fix		対象サイトにナクセスしむ安なシナリオをTF成できる(S/G) シナリオのレビューができる(G)	x-9(POSI, GEI), 7 X 9 2 F L 9 9	
			スキャン対象URL・画面の確認	0 0	作成したシナリオに診断対象とすべき画面がすべて含まれているか	確 URL、ドメイン、パス、正規表現	
					認できる(S/G) 作成したシナリオに診断対象外の画面に対する診断が含まれていな		
					ことを確認できる(S/G)		
			同時セッション、ログオン数の 2007年 日本は45年	0 0	同時セッション数の制限を設定できる(S/G)	セッション数、同時ログイン	
			確認、最大接続数		同時セッション数、ログオン数、最大接続数の制限の効果について 解している(G)	Paris	
			診断項目・ポリシーの作成、選	0 0	既に存在する診断項目・ポリシーから指示通り選択できる(S/G)		
			坎		診断内容に応じて診断項目・ポリシーを新規に作成できる(G) 環境に応じて診断項目・ポリシーを新規に作成できる(G)		
		除外設定	パラメータ除外設定	0 0	パラメータの除外設定ができる(S/G)	Cookie、パラメータ(POST、GET)、hiddenフィールド、URL、ドメイン、パス、	
			ディレクトリ・ページ除外設定		診断不要なパラメーターを判断できる(G) ディレクトリやページの除外設定ができる(S/G)	正規表現 URL、ドメイン、パス、正規表現	
				Ľ	診断不要なディレクトリやページを判断できる(G)		
	自動診断ツールのス キャン実行	正常動作の確認	稼動ログの適切な確認	0 0	正常に診断していることをログから確認できる(S/G) 正常に診断できていない場合、正常に動いていない原因を究明し、	N	
	ヤヤン夫们				近常に診断できていない場合、正常に動いていない原因を先列し、 処を行える(G)	N)	
	自動診断ツールの診断	診断結果の精査	誤検知の確認	0 0	誤検知の確認方法を知っている(S/G)		
	結果の精査				診断結果の確認ができ、誤検知の理由を説明できる(G) 自動診断ツールがよく起こしやすい誤検知を理解している(G)		
		診断対象画面の実	施成否の確認	0 0	診断結果から、実施が出来ているかどうかを判断できる(S/G)		
					想定したシナリオ通りスキャンができているか確認できる(S/G) 診断対象外に対するスキャンをしていないか確認できる(S/G)		
	自動診断ツールのその	補助機能	スパイダー	0 0	スパイダーの動作について理解している(S/G)	HTML、セッション、トークン、CAPTCHA、ワンタイムURL、Cookie、パラメー	
	他機能		レポート機能	0 0	スパイダーの利点と問題点を理解している(G) レポート機能を使用して、レポートを作成できる(S/G)	タ(POST、GET)、URL、ドメイン、パス、正規表現	
	手動診断補助ツールの	プロキシ	F 41 119686	0 0	プロキシツールの挙動について理解している(S/G)	MITM、SSL、SSL証明書	
	機能				プロキシツール(と同等の機能)を利用できる(S/G) インターセプトの設定(フィルタなど)が利用できる(S/G)		
					HTTPS復号の機能について理解している(S/G)		
1							
	The No. of American Administration of the Control o				HTTPS復号(と同等の機能)を利用できる(S/G)		
		リピーター/再送	幾能	0 0	HTIPS復考(と同等の機能)を利用できる(S/G) リピーターの挙動について理解している(S/G) リピーター(と同等の機能)を利用できる(S/G)		
			機能 ルーダー/シグネチャ送信機能	0 0	リピーターの挙動について理解している(S/G) リピーター(と同等の機能)を利用できる(S/G) ファザーの動作について理解している(S/G)		
				0 0	リビーターの挙動について理解している(S/G) リビーター(と同等の機能)を利用できる(S/G) ファザーの動作について理解している(S/G) ファザー(と同等の機能)を利用できる(G)		
			ルーダー/シグネチャ送信機能	0 0	リピーターの楽動について理解している(SIG) リピーター(と同等の機能)を利用できる(SIG) ファザーの動作についで理解している(SIG) ファザー(と同等の機能)を利用できる(G) ファザーの利点と問題」を理解している(G) エンコーダ・デコーダの楽動について理解している(SIG)	Base64、HTMLエンコード・デコード、URLエンコード・デコード、文字コード	
		ファザー/イント エンコーダ・デコ	ルーダー/シグネチャ送信機能	0 0	リピーターの姿動について理解している(SIG) リピーターの姿動について理解している(SIG) ファザーの動作について理解している(SIG) ファザーの利息と問題点を理解している(GIG) エンコーダ・デコーダンの事動について理解している(SIG) エンコーダ・デコーダンの事動について理解している(SIG) エンコーダ・デコーダンの事動について理解している(SIG)	Base64、HTMLエンコード・デコード、URLエンコード・デコード、文字コード	
		ファザー/イント エンコーダ・デコ diff/コンペア	ルーダー/シグネチャ送信機能 ーダ	0 0 0 x 0	リピーターの楽動について理解している(SIG) フェザーの楽動について理解している(SIG) ファザーの動作について理解している(SIG) ファザーの利点と問題点を理解している(SIG) エンニグ・デニーダンの事動について理解している(SIG) エンニグ・デニーダンの事動について理解している(SIG) エンニーグ・デニーダンの事動について理解している(SIG) は対している(SIG) d群の挙動について理解している(GIG) d群と国等の機能と利用できる(G)	Base64、HTMLエンコード・デコード、URLエンコード・デコード、文字コード	
		ファザー/イント エンコーダ・デコ diff/コンペア	ルーダー/シグネチャ送信機能	0 0 0 x 0 x	リピーターの姿動について理解している(SIG) リピーターの姿動について理解している(SIG) ファザーの動作について理解している(SIG) ファザーの動作について理解している(SIG) ファザーと同等の機能)を利用できる(G) ファザーと同等の機能)を削っている(G) エンコーダ・デコーダンの季動について理解している(SIG) は近いでは、デニーダンのでの機能)を利用できる(SIG) は近いでの機能)を利用できる(G) のがに同等の機能)を利用できる(G) のがに同等の機能)を利用できる(G)	Base64、HTMLエンコード・デコード、URLエンコード・デコード、文字コード	
		ファザー/イント エンコーダ・デコ diff/コンペア	ルーダー/シグネチャ送信機能 ーダ	0 0 0 0 x 0 x	リピーターの楽動について理解している(SIG) フェザーの楽動について理解している(SIG) ファザーの動作について理解している(SIG) ファザーの利点と問題点を理解している(SIG) エンニグ・デニーダンの事動について理解している(SIG) エンニグ・デニーダンの事動について理解している(SIG) エンニーグ・デニーダンの事動について理解している(SIG) は対している(SIG) d群の挙動について理解している(GIG) d群と国等の機能と利用できる(G)		
		ファザー/イント エンコーダ・デコ diff/コンベア ステートメント・	ルーダー/シグネチャ送信機能 ーダ ワンタイムトークンの設定	0 0 0 0 0 x 0 x	リピーターの季動について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの自分に同学の地能と利用できる(G) ファザーの利点と問題点を理解している(G) エンエーダ・デューダの季動について理解している(G) ボンコーダ・デューダンの季動について理解している(G) はアコーダーの動力の場合である(G) はアードメント・ワンダイムトークンの設定について理解している (G) ステートメント・ワンダイムトークンの設定(と同等の機能)を利用できる(G) ステートメント・ワンダイムトークンの設定(と同等の機能)を利用できる(G)		
	手動診断補助ツールの 準備	ファザー/イント エンコーダ・デコ diff/コンベア ステートメント・	ルーダー/シグネチャ送信機能 ーダ	0 0 0 0 x 0 0 x 0 0	リピーターの姿勢について理解している(SIG) リピーターの姿勢について理解している(SIG) ファザーの動作について理解している(SIG) ファザーの動作について理解している(SIG) ファザー(と同等の後聴)を利用できる(G) エンコーダ・デューダの姿勢について理解している(SIG) エンコーダ・デューダの姿勢について理解している(SIG) エンコーダ・デューダを呼い後能)を利用できる(SIG) dff(と同等の機能)を利用できる(G) ステートメント・ワンダイムトークンの設定について理解している (G) ステートメント・ワンダイムトークンの設定(と同等の機能)を利用できる(G) ステートメント・ワンダイムトークンの設定(と同等の機能)を利用できる(G)		
	手動診断補助ツールの	ファザー/イント エンコーダ・デコ diff/コンベア ステートメント・	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定	0 0 0 0 x 0 0 x	リピーターの姿動について理解している(SIG) リピーターの姿動について理解している(SIG) ファザーの動作について選解している(SIG) ファザーの利息と問題点を理解している(SIG) ファザーの利息と問題点を理解している(SIG) エンコーダ・デヨーダと同等の機能と利用できる(SIG) エンコーダ・デヨーダンの事態について理解している(SIG) エンコーダ・デヨーダンの事態について理解している(SIG) インコーダー・デヨーダンの表記について理解している(GIG) オテートメント・ワンタイムトークンの設定について理解している (GI) ステートメント・ワンタイムトークンの設定(と同等の機能)を利用できる(GI) タイムアウト値の設定ができる(SIG) タイムアウト値の設定ができる(SIG) タイムアウト値を適切に設定し、対象サーバからのレスポンスを受 表も時間を顕微できる(SIG)		
	手動診断補助ツールの	ファザー/イント エンコーダ・デコ diff/コンベア ステートメント・	ルーダー/シグネチャ送信機能 ーダ ワンタイムトークンの設定	0 0 0 0 0 X 0 0 0 0 0 0 0 0 0 0 0 0 0 0	リピーターの季動について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの相点と問題点を理解している(G) ファザーの相点と問題点を理解している(G) エンコーダ・デコーダの総合がについて理解している(G) エンコーダ・デコーダーを対象について理解している(G) ロボレコーダーを対象的では、では、では、では、「G) ロボレコーダーを対象ができる(G) ステートメント・ワンダイムトークンの設定について理解している (G) ステートメント・ワンダイムトークンの設定(と同等の機能)を利用できる(G) スケートメント・ワンダイムトークンの設定(と同等の機能)を利用する(G) スケートメント・ウンダイムトークンの設定(と同等の機能)を利用する(G) スケートメント・ウンダイムトークンの設定(と同等の機能)を利用する(G) タイムアウト能の設定ができる(SIG) タイムアウト能の設定ができる(SIG)	7	
	手動診断補助ツールの	ファザー/イント エンコーダ・デコ diff/コンベア ステートメント・	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定	0 0 0 0 0 X 0 0 0 0 0 0 0 0 0 0 0 0 0 0	リピーターの季動について開発している(SIG) ファザーの動物について開発している(SIG) ファザーの動物について開発している(SIG) ファザーの動物について開発している(SIG) ファザーの側点と問題点を開業している(G) ファザーの側点と問題点を開業している(G) エンコーダ・デコーダン原動について更難している(G) エンコーダ・デコーダと間等の機能を利用できる(SIG) d研の季節について理解している(G) ステートメント・ワンダイムトークンの設定について理解している (G) ステートメント・ワンダイムトークンの設定について理解している (G) ステートメント・ワンダイムトークンの設定について理解している (G) ステートメント・ワンダイムトークンの設定について理解している (G) ステートメント・ワンダイムトークンの設定について理解している (B) カイムアウト能の設定ができる(SIG) タイムアウト能の設定ができる(SIG) 第64日では、対象サーバからのレスポンスを受取ら時間を調整できる(G) 対象オコープの設定ができる(SIG)	*	
	手動診断補助ツールの	ファザー/イント エンコーダ・デコ diff/コンベア ステートメント・	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	リピーターの姿態について理解している(SIG) リピーターの姿態について理解している(SIG) ファザーの動作について理解している(SIG) ファザーの動作について理解している(SIG) ファザーの利息と問題点を理解している(SIG) エンコーダ・デューダンの事態について理解している(SIG) エンコーダ・デューダンの事態について理解している(SIG) ボンコーダ・デューダンの事態について理解している(SIG) ボンコーダ・デューダンの事態について理解している(GIG) d群に対策を総計を利用できる(GIG) ステートメント・ワンタイムトークンの設定について理解している (GIG) ステートメント・ワンタイムトークンの設定と同等の機能)を利用できる(GIG) オイムアウト値の設定ができる(SIG) オイムアウト値を適切に設定し、対象サーバからのレスボンスを受取ら時間を実施でしてのでは、対象サーバからのレスボンスを受取ら時間を表すくとしてしまい。	7	
	手動診断補助ツールの	ファザー/イント エンコーダ・デコ diff/コンベア ステートメント・	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定	000000000000	リピーターの姿勢について関係している[SIG] フェザーの影射について関係している[SIG] ファザーの動料について関係している[SIG] ファザーの動料について関係している[SIG] ファザーの利点と問題点を理解している[GIG] ファザーの利点と問題点を理解している[GI] エンニグ・アニーダンの事態について理解している[GI] エンニグ・アニーダンの事態について理解している[GI] オンニーグ・アニーダンの事態について理解している[GI] オント・ワンタイムトークンの設定について理解している (GI) ステートメント・ワンタイムトークンの設定について理解している (GI) ステートメント・ワンタイムトークンの設定について理解している (GI) ステートメント・ワンタイムトークンの設定について理解している (GI) ステートメント・ワンタイムトークンの設定にクロック機能)を利用する ある[GI] タイムアウト能の設定ができる[SIG] タイムアウト能の設定ができる[SIG] オ金スコープの設定ができる[SIG] オ金スコープの設定ができる[SIG] オ金スコープの設定ができる[SIG] オ金スコープの設定ができる[SIG]	* HTTPプロキシ、HTTPSプロキシ	
	手動診断補助ツールの	ファザー/イント エンコーダ・デコ diff/コンベア ステートメント・	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定 ブラウザのプロキン設定 SSL証明書の設定	000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000<l< td=""><td>リピーターの季動について理解している(SIG) ファザーの動動について理解している(SIG) ファザーの動計について理解している(SIG) ファザーの動計について理解している(SIG) ファザーの関本と間壁点を理解している(SIG) ファザーの利本と間壁点を理解している(SIG) エンヨーダ・デヨーダの準備している(SIG) エンヨーダ・デヨーダルでは、アロッドのでは、「はいいでは、「はいいでは、「いっては、「はいいでは、「いっては、「はいいでは、「いっては、「はいいでは、「いっと、「いっ」」 ボファートメント・ワンタイムトータンの設定(と同等の機能)を利用できる(SIG) スクートメント・ワンタイムトータンの設定(と同等の機能)を利用できる(SIG) オイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) オイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カインアウト値を適切に設定し、対象サーバからのレスボンスを受扱をおいてする設定できる(SIG)</td><td>† † † † † † † † † † † † † † † † † † †</td><td></td></l<>	リピーターの季動について理解している(SIG) ファザーの動動について理解している(SIG) ファザーの動計について理解している(SIG) ファザーの動計について理解している(SIG) ファザーの関本と間壁点を理解している(SIG) ファザーの利本と間壁点を理解している(SIG) エンヨーダ・デヨーダの準備している(SIG) エンヨーダ・デヨーダルでは、アロッドのでは、「はいいでは、「はいいでは、「いっては、「はいいでは、「いっては、「はいいでは、「いっては、「はいいでは、「いっと、「いっ」」 ボファートメント・ワンタイムトータンの設定(と同等の機能)を利用できる(SIG) スクートメント・ワンタイムトータンの設定(と同等の機能)を利用できる(SIG) オイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) オイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カインアウト値を適切に設定し、対象サーバからのレスボンスを受扱をおいてする設定できる(SIG)	† † † † † † † † † † † † † † † † † † †	
	手動診断補助ツールの	ファザー/イント エンコーダ・デコ diff/コンペア ステートメント・ 基本設定	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定 ブラウザのプロキン設定 SSL証明書の設定 診断ツールのプロキン設定	 O O	リピーターの季動について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの利息と問題点を理解している(SIG) エンニーダ・デニーダの準備している(SIG) エンニーダ・デニーダン準備している(SIG) エンニーダ・デニーダと同学の機能と利用できる(SIG) オア・ドメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定について理解している(SIG) ステートスト・ロンタイムトークンの設定に同等の機能)を利用できる(SIG) オイムアウト報を造切に設定し、対象サーバからのレスポンスを受扱の時間を調整できる(SIG) オイムアウト報を造切に設定し、対象サーバからのレスポンスを受扱の時間を調整できる(SIG) フィイアントを記述できる(SIG) フラヴザのプロオン設定ができる(SIG) クライアントSSL証明書が必要な場合、クライアントSSL証明書を定できる(SIG)	† † † † † † † † † † † † † † † † † † †	
レポーティング・	手動診断補助ツールの	ファザー/イント エンコーダ・デコ diff/コンベア ステートメント・	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定 ブラウザのプロキン設定 SSL証明書の設定 診断ツールのプロキン設定	OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO<l< td=""><td>リピーターの季動について理解している(SIG) ファザーの動動について理解している(SIG) ファザーの動計について理解している(SIG) ファザーの動計について理解している(SIG) ファザーの関本と間壁点を理解している(SIG) ファザーの利本と間壁点を理解している(SIG) エンヨーダ・デヨーダの準備している(SIG) エンヨーダ・デヨーダルでは、アロッドのでは、「はいいでは、「はいいでは、「いっては、「はいいでは、「いっては、「はいいでは、「いっては、「はいいでは、「いっと、「いっ」」 ボファートメント・ワンタイムトータンの設定(と同等の機能)を利用できる(SIG) スクートメント・ワンタイムトータンの設定(と同等の機能)を利用できる(SIG) オイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) オイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カインアウト値を適切に設定し、対象サーバからのレスボンスを受扱をおいてする設定できる(SIG)</td><td></td><td></td></l<>	リピーターの季動について理解している(SIG) ファザーの動動について理解している(SIG) ファザーの動計について理解している(SIG) ファザーの動計について理解している(SIG) ファザーの関本と間壁点を理解している(SIG) ファザーの利本と間壁点を理解している(SIG) エンヨーダ・デヨーダの準備している(SIG) エンヨーダ・デヨーダルでは、アロッドのでは、「はいいでは、「はいいでは、「いっては、「はいいでは、「いっては、「はいいでは、「いっては、「はいいでは、「いっと、「いっ」」 ボファートメント・ワンタイムトータンの設定(と同等の機能)を利用できる(SIG) スクートメント・ワンタイムトータンの設定(と同等の機能)を利用できる(SIG) オイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) オイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カイムアウト値を適切に設定し、対象サーバからのレスボンスを受扱の時間を調整できる(SIG) カインアウト値を適切に設定し、対象サーバからのレスボンスを受扱をおいてする設定できる(SIG)		
レポーティング・ リスク 算出	手動診断補助ツールの	ファザー/イント エンコーダ・デコ diff/コンペア ステートメント・ 基本設定	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定 ブラウザのプロキン設定 SSL証明書の設定 診断ツールのプロキン設定	 O O	リピーターの季動について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの利息と問題点を理解している(SIG) エンニーダ・デニーダの準備している(SIG) エンニーダ・デニーダン準備している(SIG) エンニーダ・デニーダと同学の機能と利用できる(SIG) オア・ドメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定について理解している(SIG) ステートスト・ロンタイムトークンの設定に同等の機能)を利用できる(SIG) オイムアウト報を造切に設定し、対象サーバからのレスポンスを受扱の時間を調整できる(SIG) オイムアウト報を造切に設定し、対象サーバからのレスポンスを受扱の時間を調整できる(SIG) フィイアントを記述できる(SIG) フラヴザのプロオン設定ができる(SIG) クライアントSSL証明書が必要な場合、クライアントSSL証明書を定できる(SIG)		報告相手(経常層・発注者・技術者)、立場の違い
	手動診断補助ツールの 準備 リスク算出方法 報告書の種類	ファザー/イント エンコーダ・デコ diff/コンペア ステートメント・ 基本設定 共通脆弱性評価シ	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定 ブラウザのプロキン設定 SSL証明書の設定 診断ツールのプロキン設定		リピーターの季動について理解している(SIG) リピーターの季動について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの利息と問題点を理解している(SIG) エンニーダ・デニーダの準備している(SIG) エンニーダ・デニーダと間等の機能)を利用できる(SIG) ボアートメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定に同等の機能)を利用できる(GI) ステートメント・ロンタイムトークンの設定に同等の機能)を利用できる(GI) ステートメント・ロンタイムトークンの設定に同等の機能)を利用できる(GI) フィムアクト報を適切に設定し、対象サーバからのレスボンスを受扱の向間を調整できる(SIG) タイムアクト報を適切に設定し、対象サーバからのレスボンスを受扱の向間を調整できる(SIG) フクラザのプロオン設定ができる(SIG) フラウザのプロオン設定ができる(SIG) 参野ツールのプロキン設定ができる(SIG) 参野ツールのプロキン設定ができる(SIG) 都告訴に記載すべき内容について知っている(SIG) 報告書に記載すべき内容について知っていて、報告書を作成できる(GIG)		
	予動診断補助ツールの 準備 リスク算出方法	ファザー/イント エンコーダ・デコ diff/コンペア ステートメント・ 基本設定 共通脆弱性評価シ	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定 ブラウザのプロキン設定 SSL証明書の設定 診断ツールのプロキン設定	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	リピーターの季動について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの動物について理解している(SIG) ファザーの自身に関係を連続している(SIG) ファザーの自身に関係を連続している(SIG) エンニッグ・デニッグの季動について理解している(SIG) エンニッグ・デニッグと間等の機能を利用できる(SIG) の研を関係がついて理解している(G) ステートメント・ワンタイムトークンの設定について理解している (G) ステートメント・ワンタイムトークンの設定について理解している (G) ステートメント・ワンタイムトークンの設定について理解している (G) ステートメント・ワンタイムトークンの設定について解έしを利用 きる(G) タイムアウト値の設定ができる(SIG) タイムアウト値の設定ができる(SIG) カイアウト値を適切に変化、対象サーバからのレスポンスを受 取ら時間を調整できる(G) オ象スコープを設定する(SIG) 参断がまドメインもしくは診断対象に以外に診断を実施しないよ 対象スコープを設定する(SIG) カタイアントSSL証明書が必要な場合、クライアントSSL証明書が 定できる(SIG) のアイアントSSL証明書が必要な場合、クライアントSSL証明書を 定できる(SIG)		報告相手(経営層・発注者・技術者)、立場の違い 診断対象、本報告書、診断の信頼性、運営上存在する業務上のリスク、診断を行う際に同意した 契約、診断を行う際の制限単項、環境
	手動診断補助ツールの 準備 リスク算出方法 報告書の種類	ファザー/イント エンコーダ・デコ diff/コンペア ステートメント・ 基本設定 共通脆弱性評価シ	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定 ブラウザのプロキン設定 SSL証明書の設定 診断ツールのプロキン設定	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	リピーターの季動について理解している(SIG) リピーターの季動について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの利息と問題点を理解している(SIG) エンニーダ・デニーダの準備している(SIG) エンニーダ・デニーダと間等の機能)を利用できる(SIG) ボアートメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定について理解している(SIG) ステートメント・ワンタイムトークンの設定に同等の機能)を利用できる(GI) ステートメント・ロンタイムトークンの設定に同等の機能)を利用できる(GI) ステートメント・ロンタイムトークンの設定に同等の機能)を利用できる(GI) フィムアクト報を適切に設定し、対象サーバからのレスボンスを受扱の向間を調整できる(SIG) タイムアクト報を適切に設定し、対象サーバからのレスボンスを受扱の向間を調整できる(SIG) フクラザのプロオン設定ができる(SIG) フラウザのプロオン設定ができる(SIG) 参野ツールのプロキン設定ができる(SIG) 参野ツールのプロキン設定ができる(SIG) 都告訴に記載すべき内容について知っている(SIG) 報告書に記載すべき内容について知っていて、報告書を作成できる(GIG)		診断対象、本報告書、診断の信頼性、運営上存在する業務上のリスク、診断を行う際に同意した 契約、診断を行う際の制限事項、環境 診断結果の総合評価、評価襲要、診断結果に対する診断員のコメント、緊急性の高い脆弱性につ
	手動診断補助ツールの 準備 リスク算出方法 報告書の種類	ファザー/イント エンローダ・デコ dff/コンペア ステートメント・ 基本設定 共通腕弱性評価シ 導入部 総合評価	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定 ブラウザのプロキン設定 SSL証明書の設定 診断ツールのプロキン設定	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	リピーターの季動について理解している(SIG) リピーターの季動について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの可利なト間型点を理解している(SIG) エンニーダ・デニーダーの製造について理解している(SIG) エンニーダ・デニーダーを対している(G) ばの半端について理解している(G) ばの半端について理解している(G) ばの半端について理解している(G) ステートメント・ワンタイムトータンの設定(と同等の機能)を利用できる(G) ステートメント・ワンタイムトータンの設定(と同等の機能)を利用できる(SIG) タイムアウト幅の設定ができる(SIG) タイムアウト幅の設定ができる(SIG) タイムアウト幅の設定ができる(SIG) タイムアウト幅の設定ができる(SIG) タイムアウト電の変定ができる(SIG) タイプアントSSL証明書が必要な場合、クライアントSSL証明書が必要な場合、クライアントSSL証明書が必要な場合、クライアントSSL証明書ができる(SIG) クライアントSSL証明書が必要な場合、クライアントSSL証明書ができる(SIG) 都第ツールのプロキン設定ができる(SIG) でSSの目的や概要について知っていて、報告書を作成できる(G) 報告書に記載すべき内容について知っていて、報告書を作成できる(G) 報告書に記載すべき内容について知っていて、記述できる(G)		参解対象、本報告書、参照の信頼性、運営上存在する業務上のリスク、参照を行う際に同意した 契約、参斯を行う際の制限事項、環境 参斯結果の総合評価、評価機要、参斯結果に対する参斯員のコメント、緊急性の高い脆弱性につ いてのコメント、流行りの攻撃についてのコメント
	手動診断補助ツールの 準備 リスク算出方法 報告書の種類	ファザー/イント エンコーダ・デコ dff/コンペア ステートメント・ 基本設定 共通腕弱性評価シ 導入部	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定 ブラウザのプロキン設定 SSL証明書の設定 診断ツールのプロキン設定	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	リピーターの季動について理解している(SIG) リピーターの季動について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの動料について理解している(SIG) ファザーの可利なト間型点を理解している(SIG) エンニーダ・デニーダーの場合に対して対象している(SIG) エンニーダ・デニーダーを対している(SIG) エンニーダ・デニーダーを対して関係している(SIG) ボンニーダ・デニーダーを対している(GIG) オアートメント・ワンタイムトークンの設定しいで理解している(GIG) ステートメント・ワンタイムトークンの設定と同等の機能)を利用できる(GIG) ステートメント・ワンタイムトークンの設定と同等の機能)を利用できる(GIG) ステートメント・ワンタイムトークンの設定と同等の機能)を利用できる(GIG) カイムアウト幅の設定ができる(SIG) タイムアウト幅の設定ができる(SIG) タイムアウトをの設定ができる(SIG) タイスアーを設定できる(SIG) アラヴのプロキン設定ができる(SIG) フラヴのプロキン設定ができる(SIG) アラヴのプロキン設定ができる(SIG) アラヴのプロキン設定ができる(SIG) オール・アを設定できる(SIG) アラヴのプロキン設定ができる(SIG) アラヴのプロキン設定ができる(SIG)		参解対象、本報告書、診断の信頼性、運営上存在する業務上のリスク、診断を行う際に同意した 契約、診断を行う際の制限事項、環境 診断結果の総合評価、評価販要、診断結果に対する診断員のコメント、緊急性の高い脆弱性につ いてのコメント、流行りの必要についてのコメント 騰強性名称、リスク評価、検出場所、ベイロードのHTPリクエストメッセージの内容、脆弱性 があると判断と理由、両部キャプチャ、能対性の解説
	手動診断補助ツールの 準備 リスク算出方法 報告書の種類	ファザー/イント エンローダ・デコ dff/コンペア ステートメント・ 基本設定 共通腕弱性評価シ 導入部 総合評価	ルーダー/シグネテャ送信機能 ーダ ワンタイムトークンの設定 タイムアウトの設定 対象スコープの設定 ブラウザのプロキン設定 SSL証明書の設定 診断ツールのプロキン設定	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	リピーターの季動について関係している(SIG) ファザーの動物について関係している(SIG) ファザーの動物について関係している(SIG) ファザーの動物について関係している(SIG) ファザーの関点と関係となっている(SIG) ファザーの関点と関係となっている(SIG) ファザーの関点と関係といて関係している(G) エンコーダ・デコーダの勝念を対解している(G) エンコーダ・デコーダントの場合と利用できる(SIG) dffの季節について更新している(G) ステートメント・ワンダイムトークンの設定について理解している(G) ステートメント・ワンダイムトークンの設定について理解している(G) ステートメント・ワンダイムトークンの設定について理解している(G) ステートメント・リンダイムトークンの設定について理解している(AF) 多る(G) タイムアウト値の設定ができる(SIG) タイムアウト値の設定ができる(SIG) タイムアウト値を適切に設定し、対象サーバからのレスポンスを受取ら時間を調整できる(SIG) オタスコープを設定できる(SIG) プラウザのプロネン設定ができる(SIG) プラサのプロネン設定ができる(SIG) グライアントSSL証明書が必要な場合、クライアントSSL証明書を定さきる(SIG) のように記載すべき内容について知っていて、報告書を作成できる(G) 報告書に記載すべき内容について知っていて、記述できる(G) 報告書に記載すべき内容について知っていて、記述できる(G)		参斯対象、本報告書、診断の信頼性、運営上存在する業務上のリスク、診断を行う際に同意した 契約、診断を行う際の制理事項、環境 診断結果の総合評価、評価概要、診断結果に対する診断員のコメント、緊急性の高い能弱性につ いてのコメント、流行りの攻撃についてのコメント 販費性名称、リスク評価、株田樹所、ベイロードOHTTPリクエストメッセージの内容、脆弱性

								T
分野				Silver	Gold			備考
関係法令・ガイド	法律や犯罪	不正アクセス禁止	法		0	法律または罪状に関する基礎的な知識や、典型的な事例を理解できて		
ライン		威力業務妨害				いる(S/G)		
				0	0	法律または罪状に関する基礎的な知識や、典型的な事例を理解できて		
			300 0 300 D3 30 D3			いる(S/G)		
		不正指令電磁的記憶	縁に関する罪	0	0	法律または罪状に関する基礎的な知識や、典型的な事例を理解できて		いわゆるコンピュータ・ウイルスに関する罪
						いる(S/G)		
		個人情報保護法		0	0	法律または罪状に関する基礎的な知識や、典型的な事例を理解できて		
		INTO CITA TRADICIONA			~	いる(S/G)		
		電子計算機損壞等	業務标案罪	^	^	法律または罪状に関する基礎的な知識や、典型的な事例を理解できて		コンピュータを不正に操作して他人のコンピュータ業務を妨害する
		电丁川 界域與似乎來仍 奶 音非			~	いる(S/G)		TO CI / ETILICIENTO CIENTO CI / RINGWENTEN
	診断時のルール・倫理	終版年日の扱い士	ch fi 羊 数	-		診断をする際における守秘義務について知っている(G)		
			ゼロデイ情報の扱い方	Û	0	ゼロデイ情報の適切な扱い方を知っている(S/G)		
			ヒロノイ旧和の扱いの	^	Ů.	ゼロデイ情報を伝える範囲を決定できる(G)		
		M755M W ES 15 111	脆弱性関連情報の届け出制度	 	_		コンピュータウイルスに関する届け出、不正アクセスに関する届け出、脆弱性関連	
		肥明生の油り口	胞羽生関連情報の舶り四制度	0	0	概要を理解している(S/G)		
							情報に関する届け出、IPA、JPCERT/CC、ソフトウェア等脆弱性関連情報取り扱い	
				1			基準	
	セキュリティに関する		PCIDSS	×	0	概要を理解している(G)	ASV、認定スキャン、ベネトレーションテスト、PAN	
		する基準						
		各種ガイドライン		0		概要を理解している(S/G)		
			OWASP TOP 10	0		概要を理解している(S/G)		
			OWASP Webシステム/Webア	×	0	概要を理解している(G)		
			プリケーションセキュリティ要					
			件書					
			OWASP Testing Guide	×	0	概要を理解している(G)		
			安全なウェブサイトの作り方	0	0	概要を理解している(S/G)		

^{※ (}G): Goldに必要なスキル、(S/G): どちらにも必要なスキル