分野	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
基礎知識(技術)	標準的なプロトコルと技術	プロトコル	IP	○	○	IPアドレスの形式を理解している(S/G) IPv6アドレスの形式を理解している(G) ブロードキャストアドレスを理解している(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、NAT/NAPT、IPマスカレード、static NAT、dynamic NAT	
			TCP	○	○	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	○	○	ブラウザにURL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、ブロードキャスト	
			SSL/TLS	○	○	SSLの役割(機密性・完全性)を理解している(S/G) TCP接続上で任意のデータを送受信できる(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、サーバ認証、クライアント認証、デジタル証明書	
			HTTP	○	○	SSL/TLS上で任意のデータを送受信できる(G) HTTPの基本的な役割、機能を理解している(S/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、パイプライン	
			HTTPS	○	○	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	×	○	WebSocketの基本的な役割、機能を理解している(G) WebSocket上で任意のデータを送受信できる(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	
			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)	○	○	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	○	○	名前解決の仕組みを理解している(S/G) 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(S/G) Whoisで提供される情報を理解している(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、再帰問い合わせ、DNSSEC	
			ドメイン管理の仕組み	×	○	ドメイン管理の仕組みを理解している(G)	レジストラ・レジストリ	
		文字コード		○	○	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) 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)	UTF-8、Shift_JIS、EUC-JP、ISO-2022-JP、ASCII	
		メール	SMTP/POP/IMAP	○	○	SMTPの基本的な役割、機能を理解している(S/G) メールの送受信に必要なMUAの設定ができる(S/G) 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)	MTA、MUA、MAIL FROM、RCPT TO、SMTP/POP/IMAP、メールヘッダ	
	セキュリティ技術	暗号	共通鍵暗号	○	○	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、RC4、RSA、DSA、MD5、SHA-1、SHA-2、CRYPTREC、bcrypt	
			公開鍵暗号	○	○	公開鍵暗号の性質を理解している(S/G)		
			暗号学的ハッシュ	○	○	暗号学的ハッシュの性質を理解している(S/G) 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) ハッシュ値が算出できる(S/G)		
		PKI	認証局	○	○	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を理解している(S/G)	公開鍵、秘密鍵、署名、証明書、認証局、PGP、Web of Trust、CSR、自己署名証明書、CRL、PKCS#12	
			証明書	○	○			
			認証	○	○	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ブ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)		
		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) IDS/IPSの基本的な仕組みを理解している(S/G) WAF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ペクション	
			IDS/IPS	○	○		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	○	○		WAF、NGFW	
		認証	フォーム(ベース)認証	○	○	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	○	○	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 Base64、チャレンジレスポンス、NTLM認証	
			クライアント認証(SSL)	○	○		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	
			二要素認証(多要素認証)・二段階認証	○	○		二要素認証(多要素認証)、二段階認証、個人識別、本人認証	
			シングルサインオン	○	○		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	
			ハードウェアトークン・ソフトウェアトークン	○	○		ハードウェアトークン、ソフトウェアトークン、OTP	
			認証要素	○	○		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カード)、FIDO	
		その他のセキュリティ技術	CAPTCHA	○	○	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	
			CSRF対策トークン	○	○		CSRF対策トークン	
			ワンタイムトークン	○	○		ワンタイムトークン	
			リスクベース認証	×	○		リスクベース認証、追加認証	
		情報セキュリティの三要素	機密性	○	○	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	
			完全性	○	○		完全性、改竄防止、改竄検出	
			可用性	○	○		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	○	○	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	
			ホスト名	○	○	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	
			ポート番号	○	○	URLエンコードが必要な文字と方法を理解している(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	○	○	HTTP URLの各部分の意味を理解している(S/G)	クエリストリング、URLパラメタ、GET、URL Rewriting、URLエンコード	
			フラグメント	○	○	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)	フラグメント識別子、リンク	
		HTTP	リクエスト/レスポンス	○	○	各種HTTPメソッドの役割を理解している(S/G) 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)	リクエスト/レスポンス レスポンス分割、HTTPメッセージ、メッセージヘッダ、メッセージボディ、エンティティボディ、メディアタイプ	
			メソッド	○	○	HTTPメッセージのフォーマットを理解している(S/G) プロキシサーバを経由する場合のHTTPリクエスト・レスポンスの形式を理解している(S/G)	GET、POST、HEAD、OPTIONS、TRACE PUT、DELETE、CONNECT	
			ステータスコード	○	○		100、200、206、302、304、401、403、404、405、500	
			HTTPヘッダ	○	○	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) 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)	User-Agent、Referer、Connection、Keep-Alive、Range、Authorization、Host、Cookie Content-Type、Content-Length、Server、Via、Cache-Control、Set-Cookie、Location、Content-Disposition	

分野	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
			セキュリティ関連のHTTPヘッダ	×	○	3rdパーティーCookieについて理解している(S/G) 代表的なHTTP認証の区別ができる(S/G) バーチャルホストの挙動について理解している(S/G)	x-frame-options、x-content-type-options、x-xss-protection、Content Security Policy、Strict-Transport-Security、Cross-Origin Resource Sharing、Access-Control-Allow-Origin	
			Cookie	○	○	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	○	○	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	○	○	任意のHTTPリクエストを送信できる(S/G) 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)	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、X-Forwarded-For	
			Referer	○	○		Refererヘッダ、リファラ、デリファラ	
			HTTP認証	○	○		Basic認証、Digest認証	
			リダイレクト	○	○		Location、Refresh	
		プロキシ	フォワードプロキシ	○	○	フォワードプロキシの仕組みを理解している(S/G)	キャッシュ、負荷分散、WAF	
			リバースプロキシ	○	○	リバースプロキシの仕組みを理解している(S/G)		
		ブラウザ	ブラウザ基本機能	○	○	ブラウザの基本的な動作を理解している(S/G) ブ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)	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、オートコンプリート、自動フィルイン	
			拡張機能・開発者ツール	○	○	各種ブ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	○	○	各種ブ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	○	○	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	○	○	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	×	○	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	×	○	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	×	○	Content Security Policyについて、機能・仕組みを理解している(G) 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) 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(G)	プリフライト、Originヘッダ、Access-Control-Allow-Origin	
		エンコード	パーセントエンコーディング	○	○	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・デコードを行える(S/G)	文字コード、URLエンコード	
			Base64	○	○	Base64エンコードの仕組みを理解し、エンコード・デコードを行える(S/G)	Basic認証	
		言語	HTML	○	○	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) 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)	HTMLタグ、実体参照、数値文字参照	
			HTML5	×	○	HTML5の基本的な役割、機能を理解している(G) 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)	WebStorage、Web Workers、svg、canvas、websocket、サンドボックス	
			JavaScript	○	○	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) Unicode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)	ECMAScript、JScript、Unicodeエスケープシーケンス、イベントハンドラ	
			CSS	○	○	CSS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)	セレクタ、Expression	
			SQL	○	○	SQLの基本的な役割、機能を理解している(S/G) 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)	サブクエリ、副問い合わせ、プレースホルダ(静的/動的)、ストアドプロシージャ	
			XPath	×	○	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	
			プログラミング言語	×	○	基本的な構文を理解している(G) 脆弱性検証用のウェブアプリケーションを書ける(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
		データ形式	XML	○	○	基本的な構文を理解している(S/G)	XSLT、DTD	
			JSON	○	○	基本的な構文を理解している(S/G)	JSONP	
		その他	ロードバランス	×	○	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	
			LDAP	×	○	仕組みを理解している(G) LDIFの基本的な構文を理解している(G)	Active Directory、LDIF (LDAP Interchange Format)	
			Web API	×	○	概要を理解している(G)	REST、SOAP、XML-RPC	
			Special files	×	○	ファイルの役割、機能を理解している(G)	robots.txt、crossdomain.xml、.htaccess 、clientaccesspolicy.xml	
			CGI	○	○	仕組みを理解している(S/G)	環境変数	
			DOM	○	○	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サーバの製品名		○	○	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		○	○	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		○	○	代表的な アプリケーションサーバの製品名、種類，代表的な特徴を理解している(S/G)		
		プラグインの製品名		○	○	代表的な ブラウザのプラグインの製品名、種類，代表的な特徴を理解している(S/G)		
		ライブラリ/フレームワークの製品名		○	○	代表的なライブラリ/フレームワークの製品名、種類、代表的な特徴を理解している(S/G)	MVC	
		検証環境構築		×	○	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	
基礎知識(脆弱性)	Webアプリケーションの脆弱性	インジェクション	SQLインジェクション	○	○	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) 典型的なパターンの場合の脆弱性を発見できる (S/G)	Blind SQL Injection、Second Order Injection、UNION Injection Prepared Statement、プレースホルダ(静的/動的)、information schema	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
			コマンドインジェクション	○	○	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) 脆弱性を利用し被害の実証確認ができる(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 CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')
			LDAPインジェクション	×	○	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 Injection')
			XPathインジェクション	×	○		Blind XPath Injection	CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection')
			XMLインジェクション	×	○			CWE-91: XML Injection (aka Blind XPath Injection)
			evalインジェクション	×	○		eval	CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')
			SSIインジェクション	×	○		SSI	CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page
			ORMインジェクション	×	○		Object-relational mapping	CWE-943: Improper Neutralization of Special Elements in Data Query Logic

分野	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
			NoSQLインジェクション	×	○		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	○	○		HTTPヘ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 Splitting')
			クロスサイトスクリプティング(XSS)	○	○		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	×	○		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		○	○		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=../../../etc/passwd CWE-36: Absolute Path Traversa ?file=/etc/passwd
		XML外部エンティティ参照 (XXE)		○	○		DTD	CWE-611: Improper Restriction of XML External Entity Reference ('XXE')
		オープンリダイレクト		○	○		**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')
		安全でないデシリアライゼーション		○	○		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性	サーバ側で実行されるファイルのアップロード	×	○		実行ファイル、ファイル名文字種制限	
			クライアント側で実行されるファイルのアップロード	×	○		**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	×	○		**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)	○	○		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	バッファーオーバーフロー	×	○		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
		レースコンディション		×	○		**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		○	○		**透過レイヤ、**X-FRAME-OPTIONS	CWE-693: Clickjacking/Clickjack/UI Redress/UI Redressing
		認証	認証回避	○	○			CWE-592: Authentication Bypass Issues
			ログアウト機能の不備や未実装	○	○		HTTP認証、セッション破棄、アクセストークン	
			過度な認証試行に対する対策不備・欠落	○	○		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	○	○		パスワード強度	CWE-521: Weak Password Requirements
			復元可能なパスワード保存	○	○		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、パスワードリマインダ	CWE-257: Storing Passwords in a Recoverable Format
			パスワードリセットの不備	○	○		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	×	○		CAPTCHA	CWE-804: Guessable CAPTCHA
		認可制御の不備・欠落	権限の不正な昇格	○	○			
			強制ブラウズ	○	○		アクセス制御	CWE-425: Direct Request ('Forced Browsing')
			パラメータ操作による不正な機能の利用	○	○		なりすまし、デバッグオプション	
		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)	○	○		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)	○	○		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	○	○		XSS	
			推測可能なセッションID	○	○		**暗号論的擬似乱数生成器**、セッションハイジャック	(長さ・乱数の強度) CWE-334: Small Space of Random Values
		情報漏洩	クエリストリング情報の漏洩	○	○		Referer、URLリライティング	URLパラメータ CWE-598: Information Exposure Through Query Strings in GET Request
			キャッシュからの情報漏洩	○	○		HTTPリダイレクション、cache-controlヘッダ、pragmaヘッダ、expiresヘッダ、last-modified	CWE-524: Information Exposure Through Caching
			パスワードフィールドのマスク不備	○	○		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	○	○		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
			機微情報の表示	○	○			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
			HTTPS利用時の**secure**属性がない**機微**Cookie	○	○			CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
			機微情報の平文保存	○	○			CWE-312: Cleartext Storage of Sensitive Information
			HTTPSの不適切な利用	○	○		**独自**CA、SSL、TLS、HSTS	
			不要な情報の存在	○	○			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
		ビジネスロジックの問題		×	○			設計上の問題
	Webアプリケーションの動作環境への診断項目	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	○	○		Indexes、アクセス権	CWE-548: Information Exposure Through Directory Listing
			バージョン番号表示	○	○		ServerSignature、ServerTokens、server_tokens	
			不要なHTTPメソッド	○	○		TRACE、PUT、DELETE	
		不要な機能・ファイル・ディレクトリの存在		○	○		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	
		OS/フレームワーク/サーバソフトウェア/プログラ		×	○		CVE	
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	○	○	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)	**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)	
			診断対象の優先順位付け	×	○	**優先順位付けの基準とその必要性を理解している(G)**		
			診断対象の選定	×	○	**診断対象の選定ができる(G)**		
		見積もり方法	画面カウント制	×	○	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	
			アクションカウント制	×	○		アクション数	
			リクエストカウント制	×	○		リクエスト数	
			その他の見積もり方法について	×	○		**サイト数、ドメイン数、機能数**(検索機能○円、ログイン機能○円など)	
		顧客との事前打ち合わせ	実施内容説明	×	○	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

分野	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	×	○	**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 **・アプリケーション**(サービス)の概要について **・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) ・システム、ネットワーク構成 **・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) **・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) **・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有無) ・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) **・診断対象範囲**(ドメイン、機能、権限など) ・テスト環境、ステージング環境の有無
			環境・データ準備依頼	×	○	**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ＩＰから疎通可能な状態にしてもらう **・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 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 ・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 ・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 ・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 **・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	×	○	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 **・診断端末に割り振るIP**アドレスなどの情報の入手 **・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	×	○	**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がある
			禁止事項	○	○	**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 診断データやログについては定められた範囲内でしか取り扱わない 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 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
			免責事項	×	○	**免責事項の確認とその必要性を理解している(G)**	サービス利用規約	
		診断準備	作業環境の準備	○	○	**診断環境に応じて、必要な機材を準備できる(S/G)**		
			必要機材	○	○	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、ライセンス更新ができる(S/G)		**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	○	○	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(S/G)		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	○	○			**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	○	○	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を理解している(S/G) WindowsとLinuxで、IPアドレス・ルーティングやデフォルトゲートウェイ等を指定できる(S/G)		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
	診断	ログ取得		○	○	**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)**		
		自動診断ツールを用いた診断		○	○	**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診断		○	○	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(S/G)		
	診断実施後・アフターサポート	報告会		×	○	**報告書を用いて、内容を説明できる(G)**		
		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
		問い合わせ対応		×	○	**診断実施後の問い合わせ対応ができる(G)**		
		再診断		○	○	**再診断の業務フローを理解している (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。
診断技術(診断ツール)	自動診断ツールの特徴	診断方法		○	○	**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脆弱性の検出を行う。
		検出が得意な脆弱性		○	○	**検出が得意な代表的な脆弱性を理解している(S/G)**		**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脆弱性、**HTML**や**Cookie**などのセキュリティ設定不備、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脆弱性など
		検出が難しい脆弱性		○	○	**検出が難しい代表的な脆弱性を理解している(S/G)**		セッション管理の不備、認可制御の不備・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、CSRFなど
		ツールによる診断が適している処理・機能		○	○	**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)**		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
		ツールによる診断が適していないまたは実施不可能な処理・機能		○	○	**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	処理が複数ページに渡る持続型の検出。入力値の影響が次画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がランダムに変わるなどの再現性のないもの。一度しか実行できない処理。脆弱性の発動に複数のパラメーターを利用するもの。**メール受信**、CAPTCHA、二要素認証などの人間の判断や操作が必要になるもの。
	自動診断ツールの選定	機能の検証		×	○	当該ツ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)**		
	自動診断ツールの準備	基本設定	ライセンス確認	○	○	**ライセンスが有効であることを確認できる(S/G)** ライ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)		
			シグネチャのアップデート	○	○	**シグネチャ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チャ**(診断パターン、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)	シグネチャ、ペイロード	
			スレッド数の設定	○	○	**スレッド数の設定ができる(S/G)** **同時に送信するスレッド数**(リクエスト数)を適切に設定し、対象サーバに与える負荷を調整できる(G)		

分野	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
			タイムアウトの設定	○	○	**タイムアウト値の設定ができる(S/G)** 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け取る時間を調整できる (G)		
			対象スコープの設定	○	○	**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う対象スコープを設定できる(S/G)**		
			セッション識別子の確認	○	○	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(S/G)		
			クレデンシャルの設定	○	○	**クレデンシャルを設定できる(S/G)**		
			CSRFトークン	○	○	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	○	○	**クライアントSSL証明書が必要な場合、クライアントSSL証明書を設定できる(S/G)**	PKCS#12、インポートパスワード、CN	
			ログ設定の確認	○	○	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を適切に行える(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	○	○	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) シナリオのレビューができる(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	
			スキャン対象URL・画面の確認	○	○	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いことを確認できる(S/G)	URL、ドメイン、パス、正規表現	
			同時セッション、ログオン数の確認、最大接続数	○	○	**同時セッション数の制限を設定できる(S/G)** 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理解している(G)	セッション数、同時ログイン	
			診断項目・ポリシーの作成、選択	○	○	**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)** **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	○	○	**パラメータの除外設定ができる(S/G)** **診断不要なパラメーターを判断できる(G)**	Cookie、パラメータ(POST、GET)、hiddenフィールド、URL、ドメイン、パス、正規表現	
			ディレクトリ・ページ除外設定	○	○	**ディレクトリやページの除外設定ができる(S/G)** **診断不要なディレクトリやページを判断できる(G)**	URL、ドメイン、パス、正規表現	
	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	○	○	**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、対処を行える(G)		
	自動診断ツールの診断結果の精査	診断結果の精査	誤検知の確認	○	○	**誤検知の確認方法を知っている(S/G)** **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		○	○	**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他機能	補助機能	スパイダー	○	○	**スパイダーの動作について理解している(S/G)** **スパイダーの利点と問題点を理解している(G)**	HTML、セッション、トークン、CAPTCHA、ワンタイムURL、Cookie、パラメータ(POST、GET)、URL、ドメイン、パス、正規表現	
			レポート機能	○	○	**レポート機能を使用して、レポートを作成できる(S/G)**		
	手動診断補助ツールの機能	プロキシ		○	○	**プロキシツールの挙動について理解している(S/G)** **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) HTTPS復号(と同等の機能)を利用できる(S/G)	MITM、SSL、SSL証明書	
		リピーター／再送機能		○	○	**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／イントルーダー／シグネチャ送信機能		○	○	**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)** **ファザーの利点と問題点を理解している(G)**		
		エンコーダ・デコーダ		○	○	**エンコーダ・デコーダの挙動について理解している(S/G)** **エンコーダ・デコーダ(と同等の機能)を利用できる(S/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	
		diff／コンペア		×	○	diffの挙動について理解している(G) **diff(と同等の機能)を利用できる(G)**		
		ステートメント・ワンタイムトークンの設定		×	○	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(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	基本設定	タイムアウトの設定	○	○	**タイムアウト値の設定ができる(S/G)** 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け取る時間を調整できる(G)		
			対象スコープの設定	○	○	**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う対象スコープを設定できる(S/G)**		
			ブラウザのプロキシ設定	○	○	**ブラウザのプロキシ設定ができる(S/G)**	HTTPプロキシ、HTTPSプロキシ	
			SSL証明書の設定	○	○	**クライアントSSL証明書が必要な場合、クライアントSSL証明書を設定できる(S/G)**	PKCS#12、インポートパスワード、CN	
			診断ツールのプロキシ設定	○	○	**診断ツールのプロキシ設定ができる(S/G)**	**上位プロキシ、プロキシ認証**、SOCKSプロキシ、トンネリング	
レポーティング・リスク算出	リスク算出方法	**共通脆弱性評価システム CVSS**		○	○	CVSSの目的や概要について知っている(S/G)	CVSS v2、CVSS v3、基本評価基準、現状評価基準、環境評価基準、スコープ、コンポーネント	
	報告書の種類			×	○	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)		**報告相手(**経営層・発注者・技術者**)**、立場の違い
	報告書に記載する内容	導入部		×	○	**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)**		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
		総合評価		×	○	**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)**		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
		個別の脆弱性		○	○	**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(S/G)** **リスク評価基準に則ってリスク評価ができる(S/G)**		**脆弱性名称、リスク評価、検出場所、ペイロードのHTTP**リクエストメッセージの内容、脆弱性があると判断した理由、画面キャプチャ、脆弱性の解説 **脆弱性の対策、セキュリティの問題を一意に識別する識別子(**CWE、CVEなど**)**、ビジネスへの影響や脅威

分野	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
関係法令・ガイドライン	法律や犯罪	不正アクセス禁止法		○	○	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る(S/G)		
		威力業務妨害		○	○	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る(S/G)		
		不正指令電磁的記録に関する罪		○	○	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いる(S/G)		いわゆるコンピュータ・ウイルスに関する罪
		個人情報保護法		○	○	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る(S/G)		
		電子計算機損壊等業務妨害罪		○	○	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いる(S/G)		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
	診断時のルール・倫理	診断結果の扱い方	守秘義務	×	○	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	×	○	ゼロデイ情報の適切な扱い方を知っている(S/G) ゼロデイ情報を伝える範囲を決定できる(G)		
		脆弱性の届け出	脆弱性関連情報の届け出制度	○	○	概要を理解している(S/G)	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基準	
	セキュリティに関する基準	セキュリティに関する基準	PCIDSS	×	○	概要を理解している(G)	ASV、認定スキャン、ペネトレーションテスト、PAN	
		各種ガイドライン	ウェブ健康診断	○	○	概要を理解している(S/G)		
			OWASP TOP 10	○	○	概要を理解している(S/G)		
			OWASP Webシステム／Webアプリケーションセキュリティ要件書	×	○	概要を理解している(G)		
			OWASP Testing Guide	×	○	概要を理解している(G)		
			安全なウェブサイトの作り方	○	○	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