分野	大分類	中分類	小分類	Silver	Gold	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	○	○	
			TCP	○	○	
			UDP	○	○	
			DNS	○	○	
			SSL/TLS	○	○	
			Web Socket	×	○	
			IPv6	×	○	
		名前解決	トップレベルドメイン(TLD)	○	○	
			ICANN	×	○	
			DNS /etc/hosts	○	○	
			レジストラ	×	○	
		文字コード		○	○	
		メール	SMTP	○	○	
	セキュリティ技術	暗号	共通鍵暗号	○	○	
			公開鍵暗号	○	○	
			暗号学的ハッシュ	○	○	
		PKI	認証局	○	○	
			証明書	○	○	
			認証	○	○	
		ネットワーク	ファイアウォール	○	○	
			IDS/IPS	×	○	
			WAF	○	○	
		認証	パスワード認証	○	○	
			２要素認証	○	○	
			シングルサインオン	○	○	
			CAPTCHA	○	○	
			ワンタイムトークン	○	○	
		情報セキュリティの三要素	機密性	○	○	
			完全性	○	○	
			可用性	○	○	
	WWW	URL/URI	スキーム名	○	○	
			ホスト名	○	○	
			ポート番号	○	○	
			クエリストリング	○	○	
			フラグメント	○	○	
		HTTP	リクエスト/レスポンス	○	○	
			メソッド	○	○	
			ステータスコード	○	○	
			HTTPヘッダ	○	○	
			Cookie	○	○	
			セッション管理	○	○	
			Webプロキシ	○	○	
			HTTPSのプロキシの方法、MITM	○	○	
			Referer	○	○	

			HTTP認証	○	○	BASIC認証、Digest認証、ネゴシエートなど
			リダイレクト	○	○	
			HTTPS	○	○	
		プロキシ	フォワードプロキシ	○	○	
			リバースプロキシ	○	○	
		ブラウザ	キャッシュ	○	○	
			オートコンプリート	○	○	
			ブラウザごとの挙動の差	×	○	
			レンダリング	○	○	
			ステータスバー・アドレスバー	○	○	
			Ajax/XHR	○	○	
			XSSフィルタ	○	○	
			Same Origin Policy	○	○	
			Content Sniffing	×	○	
			Content Security Policy	×	○	
			Cross-Origin Resource Sharing	×	○	
		エンコード	URLエンコード	○	○	
			Base64	○	○	
		言語	HTML	○	○	
			HTML5	×	○	
			JavaScript	○	○	
			CSS	○	○	
			SQL	○	○	
			DOM	○	○	
			XPATH	×	○	
			LDAP	×	○	
			OSコマンド	○	○	
			プログラミング言語	×	○	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	×	○	
			JSON	○	○	
			JSONP	×	○	
		その他	ロードバランサー	×	○	
			NAT/NAPT	×	○	
			robots.txt	○	○	
			ミドルウェア	○	○	
			フレームワーク	○	○	
			CGI	○	○	
			サーブレット	○	○	
	その他	HTTPDの製品名		○	○	
		DBの製品名		○	○	
		アプリケーションサーバの製品名		○	○	
		ライブラリの製品名		○	○	
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	○	○	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	○	○	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	×	○	CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')

			XPathインジェクション	×	○	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	×	○	CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')
			SSIインジェクション	×	○	CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page
			ORMインジェクション	×	○	CWE-943: Improper Neutralization of Special Elements in Data Query Logic
			NoSQLインジェクション	×	○	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 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)	○	○	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	×	○	フォーマットストリング攻撃 CWE-134: Uncontrolled Format String
			相対パストラバーサル	○	○	ディレクトリトラバーサル ?file=../../../etc/passwd CWE-23: Relative Path Traversal
			絶対パストラバーサル	○	○	?file=/etc/passwd CWE-36: Absolute Path Traversa
		オープンリダイレクト	オープンリダイレクト	○	○	オープンリダイレクター CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
		ファイルアップロードに係る脆弱性	サーバー側で実行されるファイルのアップロード	×	○	
			クライアント側で実行されるファイルのアップロード	×	○	
			許可されていないファイルのアップロード	×	○	
		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）	○	○	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	×	○	CWE-788: Access of Memory Location After End of Buffer
		レースコンディション		×	○	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
		クリックジャッキング		○	○	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	○	○	
			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 CWE-307: Improper Restriction of Excessive Authentication Attempts
			パスワードポリシーと実装の乖離	○	○	
			脆弱なパスワードポリシー	○	○	CWE-521: Weak Password Requirements
			復元可能なパスワード保存	○	○	CWE-257: Storing Passwords in a Recoverable Format
			パスワードリマインダの不備	○	○	
			推測可能なCAPTCHA	×	○	CWE-804: Guessable CAPTCHA
		認可制御の不備・欠落	権限の不正な昇格	○	○	
			パラメータ操作による不正な機能の利用	○	○	
		セッション管理の不備	セッションフィクセイション	○	○	セッションフィクセーション セッション固定攻撃 CWE-384: Session Fixation
			クロスサイトリクエストフォージェリ(CSRF)	○	○	CWE-352: Cross-Site Request Forgery (CSRF)
			CookieのHttpOnly属性未設定	○	○	

			推測可能なセッションＩＤ	○	○	（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	○	○	URLパラメータ CWE-598: Information Exposure Through Query Strings in GET Request
			ブラウザキャッシュからの情報漏洩	○	○	CWE-525: Information Exposure Through Browser Caching
			パスワードフィールドのマスク不備	○	○	CWE-549: Missing Password Field Masking
			エラーメッセージによる情報露出	○	○	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
			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Cookieへの平文保存	○	○	CWE-315: Cleartext Storage of Sensitive Information in a Cookie
			HTTPSの不適切な利用	○	○	
			不要な情報の存在	○	○	
		ビジネスロジックの問題		○	○	
	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	○	○	
			デフォルトエラー画面	○	○	
			バージョン番号表示	○	○	
			不要なHTTPメソッド	○	○	
		不要なファイルの存在確認	バックアップファイルの存在	○	○	
			サンプルファイルの存在	○	○	
			管理者ページの存在	○	○	
			デバッグオプションが有効	×	○	
		OS/フレームワーク/サーバソフトウェア/プログラミングライブラリの既知の脆		×	○	
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	○	○	
			診断対象の優先順位付け	×	○	
			診断対象の選定	×	○	
		見積もり方法	画面カウント制	×	○	
			アクションカウント制	×	○	
			リクエストカウント制	×	○	
			その他の見積もり方法について	×	○	
		顧客との事前打ち合わせ	実施内容説明	×	○	
			ヒアリング	×	○	
			環境・データ準備依頼	×	○	テストアカウント（権限、画面遷移に必要なアカウントが複数必要） 強制ログアウトロックアウト処理。物理デバイス、証明書の必要性。画面認証の有無等の確認と遷移先の確認 特定のパラメータ等の付加の確認
			作業環境の準備依頼	×	○	
			診断環境による差違	×	○	
			禁止事項	○	○	
			免責事項	×	○	
		実査準備	作業環境の準備	○	○	
			必要機材	○	○	
			診断ツールの準備	○	○	
			クライアントの準備	○	○	
			セキュリティツールの影響	○	○	
	診断実査	ログ取得		○	○	
		自動診断ツールを用いた診断		○	○	
		プロキシツールを用いた手動診断		○	○	
	診断実施後・アフターサポート	報告書作成		×	○	

		報告会		×	○	
		診断実施後のデータの取り扱い		×	○	
		再診断		○	○	
診断技術（自動診断ツール）	自動診断ツールの特徴	検出が得意な脆弱性		○	○	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		○	○	手動診断が必要な理由 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、権限越え、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		○	○	マクロ化＝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		○	○	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 シナリオが作れないもの。手順が決めにくいもの。乱数使ってたり再現性がない。 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
	ツール使用時の注意事項	診断中の注意	サーバに掛ける負荷	○	○	[関係]スレッド数、タイムアウトの設定。時々様子を見てあげないといけない。
	自動診断の準備	基本設定	ライセンス確認	○	○	ライセンスによって機能が異なる場合がある。
			シグネチャのアップデート	○	○	
			スレッド数の設定	○	○	設定が適切か必ず確認が必要
			タイムアウトの設定	○	○	設定可能であることを知っていること
			対象スコープの設定	○	○	診断対象となるドメインを設定等
			セッション識別子の確認	○	○	セッション識別子を判別し、設定することができる
			CSRFトークン	○	○	CSRFトークンを判別し、設定することができる
			ログ設定の確認	○	○	適切な設定を行うことができる。ログを取得する意味を理解している。ログが正しく書き込まれていることを確認でき
	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	○	○	適切なシナリオ作成を行うことができる。 ツールでは診断の実施が困難な画面の確認を行うことができる。 対象外ページの設定。不必要なパラメータ等の削除。必要なパラメータ情報の付加
			スキャン対象URL・画面の確認	○	○	診断対象とすべき画面が全て含まれているか。 診断で許容されていないURLが含まれていないか
			同時セッション、ログオン数の確認、最大接続数	○	○	
			診断項目・ポリシーの作成、選択	○	○	
		除外設定	パラメータ除外設定	○	○	診断対象から不要なパラメータを除外する設定を行うことができる
			ディレクトリ除外設定	○	○	診断対象から不要なディレクトリを除外する設定を行うことができる
	スキャン実行	正常動作の確認	稼動ログの適切な確認	○	○	
	診断結果の精査	診断結果の精査	誤検知の確認	○	○	
		診断対象画面の実施成否の確認		○	○	
	その他ツールの機能	補助機能	スパイダー	○	○	
			レポート機能	○	○	
診断技術（手動診断で使うツール）	手動診断補助ツールの機能	プロキシ		○	○	
		リバースプロキシ		○	○	
		リピーター		○	○	
		ファザー／イントルーダー		×	○	
		エンコーダ・デコーダ		○	○	
		diff／コンペア		×	○	
		CSRF PoC Generator		○	○	
		beautifier		×	○	
		ログ		○	○	
		ステートメント・ワンタイムトークンの設定		×	○	
		HTTPS復号		○	○	

		ブラウザのプロキシ切り替え		×	○	
		Webテストツール		×	○	
	手動診断の準備	基本設定	タイムアウトの設定	○	○	設定可能であることを知っていること
			対象スコープの設定	○	○	診断対象となるドメイン・ディレクトリ・パラメータを設定等
			認証機能の設定	○	○	アプリケーションに認証(BASIC認証等)やクライアント証明書が必要な場合、事前に設定しリクエスト時に自動付与するよう設定することができる
			ブラウザのプロキシ設定	○	○	ブラウザでプロキシを通す際の設定する方法を知っていること
			診断ツールのプロキシ設定	○	○	
		インターセプトの設定	リクエスト/レスポンスのインターセプト設定	○	○	
			特定条件下におけるインターセプト	○	○	リクエスト/レスポンスに特定の条件化(正規表現等)でヒットした場合にインターセプトする設定を(必要に応じて)行う
	診断を効率化するツール	netcat, stunnel, openssl		×	○	
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		○	○	
	報告書の種類	エグゼクティブ・サマリー		×	○	
		通常の報告書		×	○	
	報告書に記載する内容	導入部	診断対象について	×	○	
			本報告書について	×	○	
			診断の信頼性について	×	○	
			運営上存在する業務上のリスクについて	×	○	
			診断を行う際に同意した契約について	×	○	
			診断を行う際の制限事項について	×	○	
			環境について	×	○	
		診断実施概要	診断実施日時	○	○	
			診断対象のURL、IPアドレス、機器名、サービス名	○	○	
			診断時のネットワーク環境	○	○	
			診断実施者	○	○	
			診断ツール	○	○	
		総合評価	診断結果の総合評価	○	○	
			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	×	○	
			評価概要	×	○	
		個別の脆弱性	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	×	○	
法律	法律や犯罪	不正アクセス禁止法		○	○	
		威力業務妨害		○	○	
		不正指令電磁的記録に関する罪		○	○	
		個人情報保護法		○	○	

		電子計算機損壊等業務妨害罪		○	○	
		その他	損害賠償	×	○	
			著作権	×	○	
	診断時のルール・倫理	診断結果の扱い方	守秘義務	×	○	
			ゼロデイ情報の扱い方	×	○	
		脆弱性の届け出	IPAへの届け出制度	○	○	
			IPAへの届け出フロー	×	○	
			調整機関（JPCERT/CC)	×	○	
			ベンダーごとの報告・買取制度	×	○	
	セキュリティに関する基準	セキュリティに関する基準	ソフトウエア等脆弱性関連情報取り扱い基準	○	○	
			PCIDSS	×	○	
		各種ガイドライン	ウェブ健康診断	○	○	
			OWASP TOP 10	○	○	