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	TCP/IP	IP	○	○	IPアドレスの形式を理解している(S/G)		
			TCP	○	○	IPv6アドレスの形式を理解している(G)		
			UDP	○	○	ブロードキャストアドレスを理解している(S/G)		
			ICMP	○	○	サブネットマスクの計算ができる(S/G)		
			ARP	○	○	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)		
			Ethernet	○	○	SSL/TLSの役割（機密性・完全性）を理解している(S/G)		
			Wi-Fi	○	○	TCP接続上で任意のデータを送受信できる(G)		
			IPSEC	×	○	SSL/TLS上で任意のデータを送受信できる(G)		
			SSL/TLS	○	○	NAT/NAPTの仕組みを理解している(S/G)		
			NAT/NAPT	○	○	IPSECの役割を理解している(G)		
			IPv6	×	○			
		名前解決	トップレベルドメイン(TLD)	○	○	OSの名前解決の仕組みを理解している(S/G)	FQDN	
			ICANN	×	○	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)		
			レジストラ	×	○	名前解決の仕組みを理解している(S/G) Whoisで提供される情報を理解している(S/G) ドメイン管理の仕組みを理解している(G)		
		個別サービス	ftp	○	○	用途や役割、悪用された場合の影響を理解している(S/G) クライアントソフトでサービスを利用できる(S/G) 利用するポート番号を知っている(S/G) 代表的な製品名を知っている(S/G) 特別なクライアントソフト無しに、netcat等で簡単な通信ができる(S/G) コマンドライン操作でサービスを利用できる(S/G)	PASV	
			ssh	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) クライアントソフトでサービスを利用できる(S/G) 利用するポート番号を知っている(S/G) 代表的な製品名を知っている(S/G) SSHの認証方式を理解している(S/G) コマンドライン操作でサービスを利用できる(S/G)		
			telnet	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) クライアントソフトでサービスを利用できる(S/G) 利用するポート番号を知っている(S/G) コマンドライン操作でサービスを利用できる(S/G)		
			smtp/smtps	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) クライアントソフトでサービスを利用できる(S/G) 利用するポート番号を知っている(S/G) 代表的な製品名を知っている(S/G) 特別なクライアントソフト無しに、netcat等で簡単な通信ができる(S/G) SMTPの認証方式を理解している(S/G) コマンドライン操作でサービスを利用できる(S/G)		
			dns	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) 利用するポート番号を知っている(S/G) 代表的な製品名を知っている(S/G) コマンドライン操作でサービスを利用できる(S/G)	A,PTR,NS,MX,キャッシュサーバ、権威サーバ、ゾーン転送, dig,nslookup	
			finger	×	○	用途や特徴、悪用された場合の影響を理解している(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)		

			http/https	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) 利用するポート番号を知っている(S/G) 代表的な製品名を知っている(S/G) 特別なクライアントソフト無しに、netcat等で簡単な通信ができる(S/G) HTTPの認証方式を理解している(S/G) Webアプリケーションの仕組みを知っている(S/G) HTTPプロキシの用途や特徴を理解している(S/G) コマンドライン操作でサービスを利用できる(S/G)	basic認証、digest認証、NTLM認証、フォワードプロキシ、リバースプロキシ	
			pop3/pop3s	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) クライアントソフトでサービスを利用できる(S/G) 利用するポート番号を知っている(S/G) 代表的な製品名を知っている(S/G) 特別なクライアントソフト無しに、netcat等で簡単な通信ができる(S/G) POP3の認証方式を理解している(S/G) コマンドライン操作でサービスを利用できる(S/G)		
			sunrpc	×	○	用途や特徴を理解している(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)		
			ident	×	○	用途や特徴、悪用された場合の影響を理解している(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)		
			MSRPC	×	○	用途や特徴、悪用された場合の影響を理解している(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)		
			SMB/CIFS	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) クライアントソフトでサービスを利用できる(S/G) 利用するポート番号を知っている(S/G) コマンドライン操作でサービスを利用できる(S/G)	匿名接続（Null Session）、rpcclient, NET USE、smbclient	
			imap/imaps	○	○	用途や特徴と、悪用された場合の影響を理解している(S/G) クライアントソフトでサービスを利用できる(S/G) 利用するポート番号を知っている(S/G) 代表的な製品名を知っている(S/G) 特別なクライアントソフト無しに、netcat等で簡単な通信ができる(S/G) IMAPの認証方式を理解している(S/G) コマンドライン操作でサービスを利用できる(S/G)		
			ldap/ldaps	×	○	用途や特徴、悪用された場合の影響を理解している(G) 利用するポート番号を知っている(G) 代表的な製品名を知っている(G) コマンドライン操作でサービスを利用できる(G)	Active Directory,LDIF	
			r系サービス	×	○	用途や特徴、悪用された場合の影響を理解している(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)	exec/login/shell	
			mssql	×	○	用途や特徴を理解している(G) クライアントソフトでサービスを利用できる(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)		
			oracle tns	×	○	用途や特徴、悪用された場合の影響を理解している(G) クライアントソフトでサービスを利用できる(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)		

		NFS	×	○	用途や特徴、悪用された場合の影響を理解している(G) クライアントソフトでサービスを利用できる(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)		
		mysql	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) クライアントソフトでサービスを利用できる(S/G) 利用するポート番号を知っている(S/G) コマンドライン操作でサービスを利用できる(S/G)		
		RDP	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) クライアントソフトでサービスを利用できる(S/G) 利用するポート番号を知っている(S/G)		
		postgresql	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) クライアントソフトでサービスを利用できる(S/G) 利用するポート番号を知っている(S/G) コマンドライン操作でサービスを利用できる(S/G)		
		VNC	×	○	用途や特徴、悪用された場合の影響を理解している(G) クライアントソフトでサービスを利用できる(G) 利用するポート番号を知っている(G) 代表的な製品名を知っている(G)		
		X11	×	○	用途や特徴、悪用された場合の影響を理解している(G) クライアントソフトでサービスを利用できる(G) 利用するポート番号を知っている(G)		
		echo	×	○	用途や特徴、悪用された場合の影響を理解している(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)		
		discard	×	○	用途や特徴、悪用された場合の影響を理解している(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)		
		chargen	×	○	用途や特徴、悪用された場合の影響を理解している(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)		
		tftp	×	○	用途や特徴、悪用された場合の影響を理解している(G) クライアントソフトでサービスを利用できる(G) 利用するポート番号を知っている(G) コマンドライン操作でサービスを利用できる(G)		
		ntp	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) 利用するポート番号を知っている(S/G) コマンドライン操作でサービスを利用できる(S/G)		
		snmp/snmptrap	○	○	用途や特徴、悪用された場合の影響を理解している(S/G) 利用するポート番号を知っている(S/G) コマンドライン操作でサービスを利用できる(S/G)		
		isakmp,IKE	×	○	用途や特徴、悪用された場合の影響を理解している(G) クライアントソフトでサービスを利用できる(G) 利用するポート番号を知っている(G)		
		syslog	×	○	用途や特徴、悪用された場合の影響を理解している(G) 利用するポート番号を知っている(G)		
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)	salt	
		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)		
	PKI	認証局	○	○	PKIの仕組みを理解している(S/G)	有効期限、CN、チェーン	
		証明書	○	○	不備による影響を理解している(S/G)		
		認証	○	○			
	ネットワーク	ファイアウォール	○	○	基本的な仕組みを理解している(S/G)		

			IDS/IPS	○	○	代表的な製品名を知っている(S/G)		
			ロードバランサ	○	○	診断への影響を理解している(G)		
			プロキシサーバ	○	○			
			ルータ・L3スイッチ	○	○			
			スイッチ・リピータ	○	○			
			UTM	○	○			
			SSL アクセラレータ	○	○			
			WAF	○	○			
		認証要素	知識認証	○	○	各認証要素の特徴について理解している(S/G)	パスワード・秘密の質問・合い言葉など	
			所有物認証	○	○		電子証明書・端末固有ID・IPアドレスなど	
			生体認証	○	○			
		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	
	その他	OS	Windows	○	○	基本的な設定項目を理解している(S/G) 代表的な製品名を知っている(S/G)	ユーザ管理、パッチ適用状況、ファイル共有、ネットワーク設定、パーソナルファイアウォール、ログ、ファイルシステム、Active Directory	
			UNIX	○	○		Linux, Solaris、ユーザ管理、パッチ適用状況、ファイル共有、ネットワーク設定、パーソナルファイアウォール、ログ、ファイルシステム	
			主要アプライアンス	×	○	基本的な操作方法を理解している(G) 代表的な製品名を知っている(G)	IOS/ScreenOS	
		言語	OSコマンド	○	○	シェルの基本的な操作方法を理解している(S/G)		
			スクリプト言語	×	○	基本的な構文を理解している(G) 脆弱性検証用のツール等を書ける(G)	bash、sed、awk、expect python,perl,ruby,powershell	
	セキュリティの問題の発生要因	アプリケーションの欠		×	○	各脆弱性の発生要因を区別できる(G)		
		設定の不備		×	○			
		運用の不備		×	○			
基礎知識（脆弱性）	データ操作	数値処理の問題		○	○	代表的な攻撃手法とシナリオを理解している (S/G)		Numeric Errors - (CWE-189)
		不適切な入力確認		○	○	技術的影響とビジネスへの影響を理解している (S/G)		Improper Input Validation - (CWE-20)
		情報漏えい		○	○	典型的なパターンにおける脆弱性の有無の確認方法を理解している (S/G)		Information Exposure - (CWE-200)
		バッファエラー		○	○	代表的な防止方法を理解している (S/G)		Improper Restriction of Operations within the Bounds of a Memory Buffer - (CWE-119)
		パストラバーサル		○	○			Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - (CWE-22)
		リンク解釈の問題		○	○			Improper Link Resolution Before File Access ('Link Following') - (CWE-59)
		書式文字列の問題		○	○			Uncontrolled Format String - (CWE-134)
		OSコマンドインジェクション		○	○			Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - (CWE-78)
		XSS		○	○			Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - (CWE-79)
		SQLインジェクション		○	○			Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - (CWE-89)
		コードインジェクション		○	○			Improper Control of Generation of Code ('Code Injection') - (CWE-94)

	セキュリティ機能	証明書・パスワード管理		○	○			Credentials Management - (CWE-255)
		認可・権限・アクセス制御		○	○			Permissions, Privileges, and Access Controls - (CWE-264)
		暗号の問題		○	○			Cryptographic Issues - (CWE-310)
		不適切な認証		○	○			Improper Authentication - (CWE-287)
		CSRF		○	○			Cross-Site Request Forgery (CSRF) - (CWE-352)
	タイミングと状態	競合状態		○	○			Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') - (CWE-362)
	貧弱なコード	リソース管理の問題		○	○			Resource Management Errors - (CWE-399)
	環境設定			○	○			Configuration - (CWE-16)
	動作環境			○	○			Environment - (CWE-2)
	その他のセキュリティの問題	推測可能なパスワード		○	○			
		運用の不備		○	○			
基礎知識（診断業務）	診断前・準備	診断対象の確認	診断対象の優先順位付け	×	○	システム構成を理解している(G)		
			診断対象の選定	×	○	顧客へ対象システムの用途や重要性を確認し、優先的に診断すべき対象をアドバイス、選定できる(G)		
		顧客との事前打ち合わせ	実施内容説明	×	○	診断実施内容（利用ツール、診断項目、診断時間、注意事項等）を説明できる(G)		
			ヒアリング	×	○	以下のヒアリングができる(G) ・ホスティング・クラウド利用有無 ・動的IPアドレスの有無 ・FW等でのアクセス制限の有無 ・診断対象へのアクセス方法 ・オンサイト診断関連（診断元IPアドレス等） ・診断時の注意事項の有無		Whoisで対象のIPアドレスの所有者など確認、診断元IPアドレスの確認など
			作業環境の準備依頼	×	○	以下の準備依頼ができる(G) ・ホスティングやクラウドサービス（AWS等）利用時の診断許可申請依頼 ・FW等で診断対象へアクセス制限している場合、アクセス許可設定依頼（アクセス制限なしで診断したい場合） ・オンサイト診断関連（診断元IPアドレス、サブネットマスク、デフォルトゲートウェイ、電源、スイッチ接続口、作業場所・環境、入館手続き等）		
			診断環境による差異	×	○	診断環境による差異を理解している(G) FWやIPS、WAF、LB等による診断結果への影響を説明できる(G)		
			禁止事項	×	○	診断対象に対する禁止事項を確認できる(G)		
			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	
		見積もり方法	IPアドレス数	×	○	見積もりの変動要素を把握している(G)		
			VirtualHost数	×	○	それぞれの項目による作業工数、セキュリティスキャナのライセンス費用を算出できる(G)		
			セグメント数	×	○			
			オンサイト・リモート	×	○			
			ポートスキャン範囲	×	○			
			その他の見積もり方法について	×	○			
		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)		
			診断ツールの準備	○	○			
			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の指定ができる(S/G) WindowsとLinuxで、DHCPの設定ができる(S/G)		
	環境設定、基本ポリシー作成	診断環境の確認	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(S/G) セキュリティスキャナ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)		
		セキュリティスキャナの設定	基本となる診断ポリシーの作成	×	○	利用するセキュリティスキャナにおいてあらかじめ取り決められた診断ポリシーファイル及び、設定項目を用いて診断を実施できる(S/G)		
			DoSの有無	○	○			
			認証・クレデンシャルの設定	○	○	利用するセキュリティスキャナにおいて、デフォルトで利用するポリシーファイルを単独にて作成できる(G)		
			スレッド数／同時接続数の設定	○	○			
			タイムアウトの設定	○	○	診断対象に負荷などを与えないように考慮した診断ポリシーや設定内容を判断し適切な設定ができる(G)		
			ログ出力設定の確認	○	○	診断ツール側で適切なログを出力する設定となっているか確認できる(S/G)		
	実施の準備、設定	診断プロジェクト作成	診断対象IPアドレスの設定	○	○	セキュリティスキャナに顧客と取り決めたIPアドレスを診断対象として設定できる(S/G)		
			診断対象への疎通状況確認	○	○	診断対象への疎通状況を確認できる(S/G)		
			利用する診断ポリシーの選択	○	○	適切な診断ポリシーを選択できる(S/G)		
	セキュリティスキャナの実行	正常動作の確認	診断状況の確認	○	○	正常に診断していることをログなどより確認できる(S/G) 診断終了までの残り時間の状況や正常にパケットが送信されているか確認できる(S/G)		
		異常動作の対処	状況の確認、対処	×	○	正常に診断できていない場合、原因を究明し、対処を行える(G)		
		検出結果の出力	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)		
	手動診断作業	検出結果の精査作業		○	○	セキュリティスキャナで検出された脆弱性について、ターミナルエミュレータやブラウザ等を利用して証拠ログを取得できる(S/G) 報告書を作成するにあたって必要なログ、画面キャプチャ、パケットなどを取得できる(S/G) セキュリティスキャナの検出結果や取得情報を利用して、脆弱性の誤検知や検出もれがないか確認ができる(S/G) 利用するセキュリティスキャナの特性を理解している(S/G)		
		追加での診断作業	脆弱なアカウントの調査	○	○	製品のデフォルトアカウント/パスワードや推測しやすいアカウント/パスワードが利用されていないか確認ができる(S/G) 取得した診断情報をアカウントの調査に反映できる(G)	デフォルトアカウント、デフォルトパスワード	
			バナー情報／バージョン情報	○	○	サービスに応じた接続方法、コマンドの実行により、稼働しているソフトウェアのバナー情報やバージョン情報を取得ができる(S/G)		
			プロトコルごとの代表的な設定不備の確認	○	○	稼働サービスにおいてセキュリティ上望ましくない機能の有無を確認できる(S/G)	ゾーン転送、オープンリゾルバ、オープンリレー、EXPN、VRFY、anonymousFTP、Lame Delegation	
		診断ツール、コマンド		○	○	代表的なセキュリティスキャナ、コマンドを利用できる(S/G)	nmap、Wireshark、sslscan、hydra、netcat、openssl、telnet、ping、traceroute、nping、hping3、tcpdump、snmpwalk、nslookup、dig、rpcinfo、ftp、ssh、nikto、whois、ldapsearch、wpscan	
	診断時の注意事項	サーバ、ネットワークにおける負荷		○	○	時間当たりのTCPセッション数や通信量を設定し診断が行える(S/G) 最適な時間当たりのTCPセッション数や通信量を考慮し診断が行える(G)		
		挙動の変化		○	○	診断中にサーバやネットワークの状況に変化が起きる可能性があることを知っている(S/G) 診断中に挙動が変化した場合に対応ができる(S/G)		挙動が変化する例：メンテナンス、サービス停止、エフェメラルポート、ロードバランス、セキュリティ機器による影響、NATテーブルの限界
		アカウントロック		○	○	アカウントロックの影響を理解している(S/G) ロック状態になった際に解除のための対応ができる(S/G)		
	診断実施後･アフターサポート	報告会		×	○	報告書の内容を理解している(G) 質疑応答に対応ができる(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)		
		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)		

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
		診断実施概要		○	○	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）		診断実施日時、診断対象のホスト名、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、診断体制、連絡先、診断ツール
		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）		システム全体の評価、評価概要
		ホスト情報		○	○	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）		IPアドレス、プロトコル、ポート番号、ホスト名、OS、バナー情報
		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、危険度、検出場所のIPアドレス・プロトコル・ポート番号・サービス名、脆弱性があると判断した理由、証跡、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）
関係法令	法律や犯罪	不正アクセス行為の禁止等に関する法律		○	○	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)		いわゆる不正アクセス禁止法
		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
		個人情報の保護に関する法律		○	○	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)		いわゆる個人情報保護法
		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)	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、コンピュータウイルスに関する届け出、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	PCI DSS	×	○	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	
			システム監査基準	○	○	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