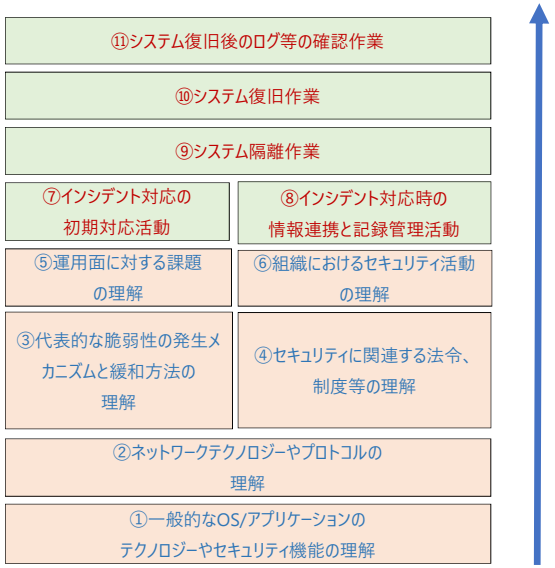
2023/7/29 Ver.2.0

## ●インシデントハンドラー

| | | | 定義 |
|---|---|---|---|
| ジョブディスクリプション | | | **インシデント発生から調査完了までの技術的な知見をベースにした上位層への報告、専門職への指示を含む各種マネジメント**<br>・対応状況の把握とプライオリティの決定<br>・上位層、セキュリティ責任者、事業責任者、必要者への報告・共有<br>・専門家（外部ベンダ含む）への作業依頼<br>・経過報告、最終報告など必要資料の作成、とりまとめ（含む広報対応支援）<br>・初動対応、復旧措置、暫定対応、再発防止策の立案、とりまとめ（原則として、実装完了までは追跡しない） |
| エントリー | 業務遂行能力 | 管理 | 上位者のサポートにより、以下を部分的に実施できる：<br>**⑧インシデント対応時の情報連携と記録管理活動**<br>- インシデントハンドリングに伴う守秘義務、業務委託時のNDA等を理解遂行する<br>- インシデント報告を受け付け、知るべき部署などに連携する<br>- 一連の対応について記録を残す |
| | | 技術 | 上位者のサポートにより、以下を部分的に実施できる：<br>**⑦インシデント対応の初期対応活動**<br>- PCやサーバ、通信機器などのシステムからのログ収集作業<br>- ログなどの簡易調査（文字列調査、パケット調査 等）<br>- セキュリティパッチ適用やパッチの確認作業<br>**⑨システム隔離作業**（VLAN切り替え、LAN切り離し、サービス停止 等）<br>**⑩システム復旧作業**（VLAN切り替え、LAN接続、サービス再開 等）<br>**⑪システム復旧後のログ等の確認作業**<br>- 期間を定めた検知機構のシグネチャ検証やログ等の確認作業<br>**⑫検知機構に対するシグネチャ登録作業** |
| | 知識 | 管理 | **④セキュリティに関連する法令、制度等の理解**<br>- 不正アクセス禁止法、個人情報保護保護法 等<br>- ISO/IEC 27001、PCIDSS 等<br>- 外部組織との情報連携や脆弱性情報等の取扱い(TLP)<br>**⑥組織におけるセキュリティ活動の理解**<br>- 組織内におけるポリシーなどの理解<br>- 組織内における重要システム、資産等の把握<br>- 組織内におけるシステム構成や課題等の理解 |
| | | 技術 | **①一般的なOS/アプリケーションのテクノロジーやセキュリティ機能の理解**<br>- OSの基本的な設定項目<br>- GUIやシェルの基本的な操作<br>**②ネットワークテクノロジーやプロトコルの理解**<br>- ネットワークセキュリティの基本的な仕組み<br>- セキュリティ管理や検知・防御システムの理解<br>**③代表的な脆弱性の発生メカニズムと緩和方法の理解**<br>- 各脆弱性の発生要因と対策<br>- 脅威動向の把握や脆弱性情報の取り扱い方法<br>**⑤運用面に対する課題の理解**<br>- バックアップや一般的なパッチ適用、アップデートサイクル<br>- 相互に連携したシステムの理解 |

### アプローチ

（習得の順番を表しています。下から順番に習得するのが推奨です。）



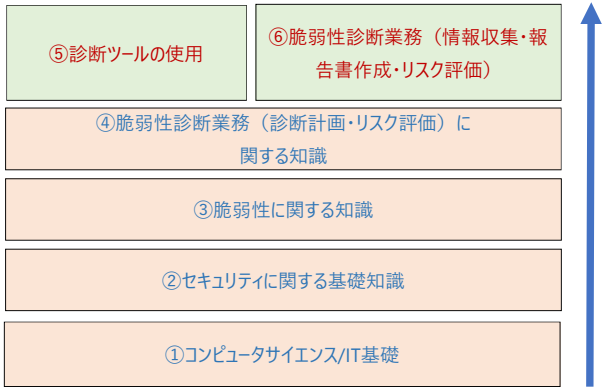
# ●Web/NW脆弱性診断士

2023/7/29 Ver.2.0

| | | | 定義 |
|---|---|---|---|
| ジョブディスクリプション | | | **ITシステムの脆弱性診断を実施**<br>・Webアプリケーションやプラットフォームの脆弱性やセキュリティ機能の調査<br>・脆弱性診断の報告書の作成と説明、対策の提言 |
| エントリー | 業務遂行能力 | 管理 | 上位のサポートにより以下を部分的に実施できる：<br>**⑥脆弱性診断業務（情報収集・報告書作成・リスク評価）**<br>-脆弱性に関する公開情報(NVD、JVNなど)を収集できる<br>-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<br>-リスク評価基準に則ってリスク評価ができる |
| | | 技術 | 上位のサポートにより以下を部分的に実施できる：<br>**⑤診断ツールの使用**<br>-診断環境に応じて、必要な環境を準備できる<br>-対象の診断に必要なネットワーク設定を行うことができる<br>-代表的な診断ツールの設定を行うことができる<br>-代表的な診断ツールやコマンドを利用して、典型的なパターンの場合の脆弱性を発見できる<br>-必要なログ、画面キャプチャ、パケットなどを取得できる<br>-正常に診断していることをログなどより確認できる<br>-自動診断ツールの診断結果の精査を行える<br>-時間当たりのセッション数や通信量を設定し診断が行える |
| | 知識 | 管理 | **④脆弱性診断業務（診断計画・リスク評価）に関する知識**<br>-診断の業務フローを理解している<br>-診断対象の画面、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<br>-クラウド環境など診断対象のプラットフォームに応じた注意事項や診断許可を得る方法を理解している<br>-診断中に対象環境に与える可能性がある影響を理解している<br>-禁止事項の確認とその必要性を理解している<br>-診断をする際における守秘義務について知っている<br>-ゼロデイ情報の適切な扱い方を理解している<br>-脆弱性診断業務に関連する法律の基礎的な知識や、典型的な事例を理解している<br>-脆弱性関連情報の届け出制度の概要を理解している<br>-代表的なリスク算出方法を理解している<br>-脆弱性診断業務に関連するセキュリティ基準やガイドラインの概要を理解している |
| | | 技術 | **①コンピュータサイエンス/IT基礎**<br>-標準的なプロトコルと技術の用途や特徴、悪用された場合の影響を理解している<br>-ネットワークセキュリティ技術の基本的な仕組みを理解している<br>-OSの基本的な設定項目を理解している<br>-シェルの基本的な操作方法を理解している<br>-スクリプト言語について、基本的な構文を理解している<br>-プログラミング言語について、基本的な構文を理解している<br>**②セキュリティに関する基礎知識**<br>-暗号、PKI、認証要素の特徴や不備による影響を理解している<br>**③脆弱性に関する知識**<br>-代表的な脆弱性を理解している<br>-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<br>-典型的な対策方法を知っている<br>-典型的な被害を知っている<br>-代表的な攻撃手法とシナリオを理解している<br>-代表的な防止方法を理解している<br>-パッチマネジメントの重要性を理解している |

## アプローチ

（習得の順番を表しています。下から順番に習得するのが推奨です。）



2023/7/29 Ver.2.0

## ●情報システムペンテスター

| | | | 定義 |
|---|---|---|---|
| ジョブディスクリプション | | | **ITシステムのセキュリティ検証を実施**<br>・対象の情報システムにおける脅威シナリオの作成<br>・発見した脆弱性を使用した脅威の実現可否確認<br>・脅威の実現可否に基づくセキュリティ耐性の評価<br>・セキュリティ耐性評価を基にした対策の提言 |
| エントリー | 業務遂行能力 | 管理 | 上位のサポートにより以下を部分的に実施できる：<br>**④報告書案の作成**<br>-報告書作成能力（エグゼクティブサマリー、検証結果の詳細報告）<br>**⑤顧客との調整**<br>-ペネトレーション実施における顧客との調整（ゴールの共有、報告内容の取扱い、対策記載レベルの合意など） |
| | | 技術 | 上位のサポートにより以下を部分的に実施できる：<br>**③ペネトレーションテストの実施**<br>-下記のような様々な攻撃手法※を用いたペネトレーションテストの実施<br>（策定された脅威シナリオに基づいた脅威の顕在化）<br>- Reconnaissance（偵察）：作戦を計画するために使用できる情報の収集<br>- Resource Development（資源開発）：作戦を支援するために使用できるリソースの確立<br>- Initial Access（初期アクセス）：ネットワークへの侵入<br>- Execution（実行）：悪意のあるコードの実行<br>- Persistence（永続性）：確立したアクセスやリソースの維持<br>- Privilege Escalation（特権の昇格）：より高いレベルの権限の取得<br>- Defense Evasion（防衛回避）：検出からの回避<br>- Credential Access（ID情報へのアクセス）:アカウント名とパスワードの窃取<br>- Discovery（発見）：環境の掌握<br>- Lateral Movement（横方向の動き）：ターゲット内部での移動<br>- Collection（コレクション）：関連するデータの収集<br>- Command and Control（コマンドと制御）：C&Cサーバーとの通信による制御<br>- Exfiltration（抽出）：データの窃取<br>- Impact（影響）：システムとデータの操作、中断、または破壊<br>※攻撃手法参照元：MITRE ATT&CK エンタープライズ向け戦術<br>**④報告書案の作成**<br>-検証結果の上位層への報告、報告書案の作成 |
| | 知識 | 管理 | |
| | | 技術 | **①最新の攻撃の手口に関する知識**<br>-サイバー攻撃の戦略・戦術・手順に関する知識（例：MITRE ATT&CK エンタープライズ向け戦術）<br>-検証対象の関連サービスに対して想定される脅威に関する知識<br>**②ハードニング技術に関する知識**<br>-機器やアプリケーションのハードニング技術に関する知識 |

### アプローチ

（習得の順番を表しています。下から順番に習得するのが推奨です。）

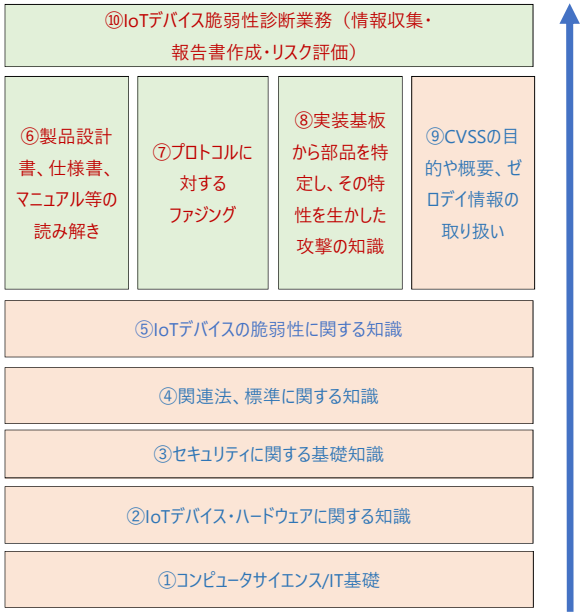
2023/7/29 Ver.2.0

# ●IoTデバイス脆弱性診断士

| | | | 定義 |
|---|---|---|---|
| ジョブディスクリプション | | | **IoTデバイスの脆弱性診断を実施**<br>・IoT機器のファームウェアやハードウェアの脆弱性やセキュリティ機能の調査<br>・脆弱性診断の報告書の作成と説明、対策の提言 |
| エントリー | 業務遂行能力 | 管理 | 上位のサポートにより以下を部分的に実施できる：<br>**⑩IoTデバイス脆弱性診断業務（情報収集・報告書作成・リスク評価）**<br>-脆弱性に関する公開情報(NVD、JVNなど)を収集できる<br>-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<br>-リスク評価基準に則ってリスク評価ができる |
| | | 技術 | 上位のサポートにより以下を部分的に実施できる：<br>**⑥製品設計書、仕様書、マニュアル等の読み解き**<br>-製品設計書・仕様書から製品の構成要素や実装を読み解く<br>-マニュアルから製品の持つ機能要素を推測する<br>-製品の設計書、仕様書、フローチャート、データシートを読み解く<br>**⑦プロトコルに対するファジング**<br>-製品に実装されたプロトコルを把握し、対象となるプロトコルに対するファジングや脆弱性調査(通信内容解析、ポートスキャン、中間者攻撃など)を実施できる<br>**⑧実装基板から主要部品を特定し、その特性を悪用して攻撃を行うスキル**<br>-対象となる製品の実装基板上に実装されている主要なIC等の部品を特定し、部品の機能や特性を悪用した攻撃(デバッグ機能の悪用など)の検討および実施できる |
| | 知識 | 管理 | **④関連法、標準に関する知識**<br>-法律または罪状に関する基礎的な知識や、典型的な事例の知識<br>-診断をする際の守秘義務を理解している<br>**⑨CVSSの目的や概要の知識、ゼロデイ情報の取り扱い**<br>-ゼロデイ情報の適切な扱い方を理解している<br>-脆弱性関連情報の届け出制度を理解している<br>-脆弱性診断業務に関連するセキュリティに関する基準の概要を理解している |
| | | 技術 | **①コンピュータサイエンス/IT基礎**<br>-コンピュータの基本構成、動作原理、コンピュータサイエンスに関する基礎的な知識<br>-ソフトウェア開発、言語、特性などソフトウェアエンジニアリングに関する基礎的な知識<br>-ネットワーク構成、プロトコル、機能、特性などネットワークに関する基礎的な知識<br>-OSやディストリビューションなどOSに関する基礎的な知識<br>**②IoTデバイス・ハードウェアに関する知識**<br>-基本的な電子部品・回路設計に関する知識<br>-デバイスデータシートの読み方の知識<br>-CPU、メモリ、SoCに関する知識<br>-デバッグ機能に関する知識<br>**③セキュリティに関する基礎知識**<br>-セキュリティにおける基本的概念<br>-サイバー攻撃における共通的な手法、主要な手法に関する知識<br>-データ保護に関する知識<br>**⑤IoTデバイスの脆弱性に関する知識** |

## アプローチ

（習得の順番を表しています。下から順番に習得するのが推奨です。）



## ●IoTシステムペンテスター

| | | | 定義 |
|---|---|---|---|
| ジョブディスクリプション | | | **IoT機器を含むシステムのセキュリティ検証を実施**<br>・IoT機器を含むシステムにおける脅威シナリオの作成<br>・発見した脆弱性を使用した脅威の実現可否確認<br>・脅威の実現可否に基づくセキュリティ耐性の評価<br>・セキュリティ耐性評価を基にした対策の提言 |
| エントリー | 業務遂行能力 | 管理 | 未定義 |
| | | 技術 | |
| | 知識 | 管理 | |
| | | 技術 | |

### アプローチ

（習得の順番を表しています。下から順番に習得するのが推奨です。）

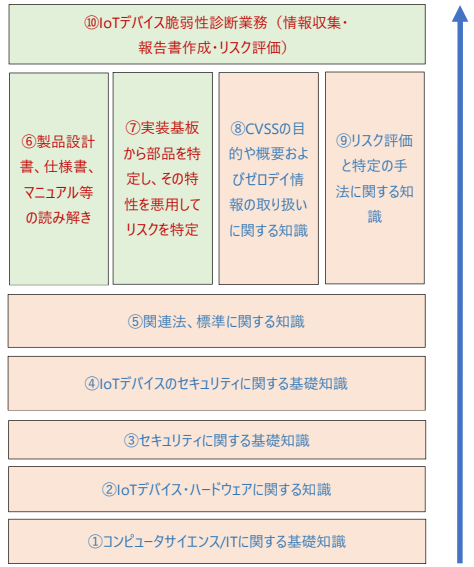
## ●IoT脅威分析士

2023/7/29 Ver.2.0

| | | | 定義 |
|---|---|---|---|
| ジョブディスクリプション | | | **IoTデバイスを含むIoTシステムの脅威分析し、想定脅威に対する脆弱性の報告や対策の提言**<br>・IoTデバイスおよび構成するIoTシステムに対して脅威を想定しリスクを特定<br>・設計・開発段階において考慮すべきリスクの優先度とその対策を提言<br>・判明したリスクを報告・提案 |
| エントリー | 業務遂行能力 | 管理 | 上位のサポートにより以下を部分的に実施できる：<br>**⑩IoTデバイス脅威分析業務（情報収集・報告書作成・リスク評価）**<br>-脆弱性に関する公開情報(NVD、JVNなど)を収集できる<br>-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<br>-リスク評価基準に則ってリスク評価ができる |
| | | 技術 | 上位のサポートにより以下を部分的に実施できる：<br>**⑥製品設計書、仕様書、マニュアル等の読み解き**<br>-製品設計書・仕様書から製品の構成要素や実装を読み解く<br>-マニュアルから製品の持つ機能要素を推測する<br>-製品の設計書、仕様書、フローチャート、データシートを読み解く<br><br>**⑦実装基板から主要部品を特定し、その特性を悪用してリスクを特定**<br>-対象となる製品の実装基板上に実装されている主要なICなどの部品を特定し、部品の機能や特性を悪用した攻撃リスク(FWの更新による悪用方法など)の指摘および対策の提案ができる |
| | 知識 | 管理 | **⑤関連法、標準に関する知識**<br>-法律または罪状に関する基礎的な知識や、典型的な事例の知識<br>-診断をする際の守秘義務を理解している<br>-必要な情報の正しい取得方法を理解している<br><br>**⑧CVSSの目的や概要の知識およびゼロデイ情報の取り扱いに関する知識**<br>-ゼロデイ情報の適切な扱い方を理解している<br>-脆弱性関連情報の届け出制度を理解している<br>-脆弱性診断業務に関連するセキュリティに関する基準の概要を理解している<br><br>**⑨リスク評価と特定の手法に関する知識**<br>-リスク評価の手法に対する目的や概要の知識(CVSS, DREADなど)<br>-リスク特定の手法に対する目的な概要の知識(STRIDE/CCDS-STRIDE, EVITA, Attack Treeなど) |
| | | 技術 | **①コンピュータサイエンス/ITに関する基礎知識**<br>-コンピュータの基本構成、動作原理、コンピュータサイエンスに関する基礎的な知識<br>-ソフトウェア開発、言語、特性などソフトウェアエンジニアリングに関する基礎的な知識<br>-ネットワーク構成、プロトコル、機能、特性などネットワークに関する基礎的な知識<br>-OSやディストリビューションなどOSに関する基礎的な知識<br>-通信における認証方式に関する知識<br><br>**②IoTデバイス・ハードウェアに関する知識**<br>-基本的な電子部品・回路設計に関する知識<br>-デバイスデータシートの読み方の知識<br>-CPU、メモリ、SoCに関する知識<br>-デバッグ機能に関する知識<br><br>**③セキュリティに関する基礎知識**<br>-セキュリティにおける基本的概念<br>-サイバー攻撃における共通的な手法、主要な手法に関する知識<br>-データ保護に関する知識<br><br>**④IoTデバイスのセキュリティに関する基礎知識**<br>-基盤の保護方法に関する知識<br>-ファームウェアの更新方法に関する知識<br>-セキュアブートに関する知識　-通信プロトコルに関する知識(CAN, MOSTなど)<br>-IoTデバイスに用いられるOSの知識 |

### アプローチ

（習得の順番を表しています。下から順番に習得するのが推奨です。）



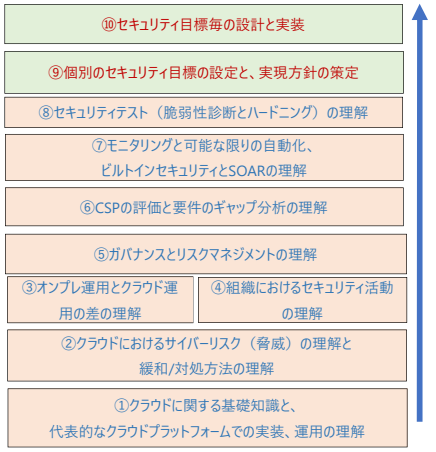
2023/7/29 Ver.2.0

## ●クラウドセキュリティプロフェッショナル

| | | | 定義 |
|---|---|---|---|
| ジョブディスクリプション | | | **クラウドを安全に利活用・運用するためのセキュリティ対策や設計、セキュリティ評価を実施**<br>・データセキュリティ　クラウドにおける安全なデータライフサイクル、データ分散、アクセス制御、データセキュリティ技術の理解と方針策定<br>・アプリケーション開発　クラウド環境におけるセキュリティ対応方針の策定<br>・インフラセキュリティ　クラウド環境のネットワーク、ストレージ、仮想化機能、認証・アクセス管理機能に関するセキュリティ対応方針の策定と、管理方法の策定<br>・インシデント対応　クラウド環境でインシデントが発生した場合を想定した場合の対応方法　　の理解、BCDRの計画立案<br>・オペレーション　クラウドのセキュリティコントロール機能の設計・実装、運用管理策の方針策定・実装、モニタリング・ロギング機能の設計・実装、セキュリティ評価・診断・Penテストの手順の理解 |
| エントリー | 業務遂行能力 | 管理 | 上位のサポートにより以下を部分的に実施できる：<br>**⑩セキュリティ目標毎の設計と実装**<br>- クラウドにおけるセキュリティ目標を立てることができる<br>- 設計通りに実装することができる |
| | | 技術 | 上位のサポートにより以下を部分的に実施できる：<br>**⑨個別のセキュリティ目標の設定と、実現方針の策定**<br>- クラウドにおけるセキュリティ目標を立てることができる<br>- 設計通りに実装することができる |
| | 知識 | 管理 | **④組織におけるセキュリティ活動の理解**<br>- 組織内におけるポリシーなどの理解<br>- 組織内における重要システム、資産等の把握<br>- 組織内におけるシステム構成や課題等の理解<br><br>**⑤ガバナンスとリスクマネジメントの理解**<br>- クラウドにおけるGRCの理解と実装<br>- クラウドにおけるリスクマネジメントのフレームワークとプロセスの理解<br>- クラウドコンプライアンスの理解<br>- クラウドコンピューティングに影響を与える法律についての理解 |
| | | 技術 | **①クラウドに関する基礎知識と、代表的なクラウドプラットフォームでの実装、運用の理解**<br>- クラウドプラットフォームとインフラストラクチャの理解<br><br>**②クラウドにおけるサイバーリスク（脅威）の理解と緩和/対処方法の理解**<br>- クラウドにおけるデータセキュリティ戦略や技術の理解<br>- クラウドデータストレージのリスク、攻撃、問題点の理解<br><br>**③オンプレ運用とクラウド運用の差の理解**<br>- クラウドアプリケーションのセキュリティについての理解<br>- クラウドにおけるデータセキュリティについての理解<br>- クラウドデータセンターの物理的/論理的運用における要素（標準と手法）の理解<br>- クラウド基盤を構築するためのセキュリティ運用の理解<br>- クラウドインフラのセキュリティ運用の監視<br>- クラウドインシデントレスポンスの理解<br><br>**⑥CSPの評価と要件のギャップ分析の理解**<br>- セキュリティの評価制度についての理解<br>- 期待される成果とのギャップ分析についての理解<br><br>**⑦モニタリングと可能な限りの自動化、ビルトインセキュリティとSOARの理解**<br>- SOARによるインシデントレスポンスの高速化についての理解<br><br>**⑧セキュリティテスト（脆弱性診断とハードニング）の理解**<br>- セキュリティテストの範囲の理解<br>- クラウドにおける一般的なセキュリティテストの理解 |

### アプローチ

（習得の順番を表しています。下から順番に習得するのが推奨です。）



2023/7/29 Ver.2.0

## ●サービス企画におけるリスク分析士

| | | | 定義 |
|---|---|---|---|
| ジョブディスクリプション | | | **サービスや業務の企画・設計段階で、想定されうるセキュリティ面でのリスクや脅威を評価・検証**<br><br>・さまざまなリスク分析手法を用い、システムや業務の観点からサービスや業務に潜む想定されうる脅威やリスクを調査<br>・想定されうる脅威やリスクを調査・評価した結果の報告書の作成と説明、対策の提言 |
| エントリー | 業務遂行能力 | 管理 | 上位者のサポートにより、以下を部分的に実施できる：<br>**⑨リスク分析対象となるサービスや業務のビジネスモデル上想定される脅威に関する情報収集** |
| | | 技術 | 上位者のサポートにより、以下を部分的に実施できる：<br>**⑩分析対象のモデル化とリスク分析** |
| | 知識 | 管理 | 上位者のサポートにより、以下を部分的に実施できる：<br>**⑥リスク分析対象のサービスや業務に関する理解**<br>ビジネスモデル、連携するサービスなど<br>**⑦分析の目的や手順の理解**<br>**⑧リスク分析に係る守秘義務や法的要件に関する知識** |
| | | 技術 | 上位者のサポートにより、以下を部分的に実施できる：<br>**①ITセキュリティに関する基礎知識**<br>特に認証、認可<br>**②リスク、脅威、脆弱性に関する基礎知識**<br>用語や代表的な定量化手法などに対する理解<br>**③代表的な攻撃手法とシナリオの理解**<br>④サービスや業務に対して行なわれた攻撃<br>⑤脆弱性を作りこむことになった原因のパターン化<br>**④典型的なパターンと対策方法の理解**<br>- サービスリスクによって発生する可能性がある問題の理解<br>**⑤代表的なリスク分析手法に関する知識** |

### アプローチ

（習得の順番を表しています。下から順番に習得するのが推奨です。）