

■セキュリティ関連タスクを担う分野の概観図

		経営層	戦略マネジメント層				実務者・技術者層				
				管理部門 (総務、法務、広報、調達、人事等)	セキュリティ統括室	経営企画部門 事業部門	設計・開発・テスト	運用・保守	研究開発		
ユーザ企業における組織の例		取締役会 執行役員会議	内部監査部門 (外部監査を含む)				デジタル部門／事業部門 (ベンダーへの外注を含む)				
セキュリティ関連タスクの例		・セキュリティ意識啓発 ・対策方針指示 ・ポリシー・予算・実施事項承認	・システム監査 ・セキュリティ監査	・BCP対応 ・官公庁等対応 ・法令等遵守対応 ・記者・広報対応 ・調達・契約・検収 ・施設管理・物理セキュリティ ・内部犯行対策	・リスクアセスメント ・ポリシー・ガイドライン策定・管理 ・セキュリティ教育 ・社内相談対応 ・インシデントハンドリング	・事業戦略立案 ・システム企画 ・要件定義・仕様書作成 ・プロジェクトマネジメント	・セキュアシステム要件定義 ・セキュアアーキテクチャ設計 ・セキュアソフトウェア方式設計 ・テスト計画	・基本・詳細設計 ・セキュアプログラミング ・テスト・品質保証 ・パッチ開発 ・脆弱性診断	・構成管理 ・運用設定 ・脆弱性対応 ・セキュリティツールの導入・運用 ・監視・検知・対応 ・インシデントレスポンス ・ペネトレテスト	・現場教育・管理 ・設備管理・保全 ・初動対応・原因究明・フォレンジック ・マルウェア解析 ・脅威・脆弱性情報の収集・分析・活用	・セキュリティ理論研究 ・セキュリティ技術開発
タスクに対応するセキュリティ関連分野	デジタル (IT/IoT/OT)	デジタル経営 (CIO/CDO)	システム監査			デジタルシステム ストラテジー	システム アーキテクチャ	デジタル プロダクト 開発	デジタル プロダクト マネジメント		
	セキュリティ	セキュリティ経営 (CISO)	セキュリティ監査		セキュリティ統括	※クラウド、アジャイル、DevSecOps等により境界は曖昧化の傾向 ※テック/IoT・組み込み/制御システム/OS/サーバ/NW/ソノト/Web等の 取扱う技術の種類や事業分野によりタスクやスキルは大きく異なる					
	その他	企業経営 (取締役)		経営リスク マネジメント	法務	事業ドメイン (戦略・企画・調達)	脆弱性診断・ ペネトレーションテスト		セキュリティ 監視・運用	セキュリティ 調査分析・研究開発	

※クラウド、アジャイル、DevSecOps等により境界は曖昧化の傾向  
※テック/IoT・組み込み/制御システム/OS/サーバ/NW/ソフト/Web等の  
取扱う技術の種類や事業分野によりタスクやスキルは大きく異なる

■分野とセキュリティ関連タスク等との対応

	区分	分野名	セキュリティ関連タスクの例	担当部署／機能の例（青字は社外ベンダー等）
経営層	デジタル	IT経営（CIO/CDO）	セキュリティ意識啓発、対策方針の指示、セキュリティポリシー・予算・対策実施事項の承認 等	経営者、経営層（CISOを含む）
	セキュリティ	セキュリティ経営（CISO）		
	その他	企業経営（取締役）		
戦略マネジメント層	デジタル	システム監査	システム監査、報告・助言 等	監査部門 ITベンダー・監査法人（システム監査サービス）
		デジタルシステムストラテジー	デジタル事業戦略立案、システム企画、要件定義・仕様書作成、プロジェクトマネジメント 等	経営企画部門、IT企画部門、IT・デジタル部門の企画機能 IT/セキュリティコンサルタント
	セキュリティ	セキュリティ監査	セキュリティ監査、報告・助言 等	監査部門 セキュリティベンダー・監査法人（セキュリティ監査サービス）
		セキュリティ統括	セキュリティ教育・普及啓発、セキュリティ関連の講義・講演、セキュリティリスクアセスメント、セキュリティポリシー・ガイドラインの策定・管理・周知、警察・官公庁等対応、社内相談対応、インシデントハンドリング 等	セキュリティ専門部門、CSIRT セキュリティ委員会 IT・デジタル部門のセキュリティ対策機能
	その他	経営リスクマネジメント	経営リスクマネジメント、BCP/危機管理対応、サイバーセキュリティ保険検討、記者・広報対応、施設管理・物理セキュリティ、内部犯行対策 等	総務部門（リスク管理部門を含む） 経営企画部署、総務部署等のリスクマネジメント機能
		法務	デジタル関連法令対応、コンプライアンス対応、契約管理 等	法務部門、総務部門の法務担当
		事業ドメイン（戦略・企画・調達）	事業特有のリスクの洗い出し、事業特性に応じたセキュリティ対応、サプライチェーン管理 等	事業部門の企画機能 事業戦略コンサルタント
実務者・技術者層	デジタル	デジタルシステムアーキテクチャ	セキュアシステム要件定義、セキュアシステムアーキテクチャ設計、セキュアソフトウェア方式設計、テスト計画 等	IT・デジタル部門の設計機能、IT子会社 IT/OTベンダー
		デジタルプロダクト開発	基本設計、詳細設計、セキュアプログラミング、テスト・品質保証、パッチ開発 等	IT・デジタル部門の開発・保守機能、IT子会社 IT/OTベンダー
		デジタルプロダクト運用	構成管理、運用設定、利用者管理、サポート・ヘルプデスク、脆弱性対策・対応、インシデントレスポンス 等	IT・デジタル部門の運用機能、IT子会社 IT/OT/セキュリティベンダー
	セキュリティ	脆弱性診断・ペネトレーションテスト	脆弱性診断、ペネトレーションテスト 等	IT・デジタル部門の運用機能、IT子会社 セキュリティベンダー（脆弱性診断サービス）
		セキュリティ監視・運用	セキュリティ製品・サービスの導入・運用、セキュリティ監視・検知・対応、インシデントレスポンス、連絡受付 等	IT・デジタル部門の運用機能、IT子会社 セキュリティベンダー（セキュリティ監視・運用サービス）
		セキュリティ調査分析・研究開発	サイバー攻撃捜査、原因究明・フォレンジック、マルウェア解析、脅威・脆弱性情報の収集・分析・活用、セキュリティ理論・技術の研究開発、セキュリティ市場動向調査 等	CSIRT/IT・デジタル部門のリサーチ機能、IT子会社 セキュリティベンダー（デジタルフォレンジックサービス）
	その他	事業ドメイン（生産現場・事業所管理）	現場教育・管理、設備管理・保全、QC活動、初動対応 等	運転、保全、計装、品質管理関連部署、PSIRT OT/セキュリティベンダー

■分野とセキュリティ関連知識・スキルとの対応

→ セキュリティ関連知識・スキルの内容は、情報処理安全確保支援士試験シラバス（[https://www.jitec.ipa.go.jp/1\\_13download/syllabus\\_sc\\_ver2\\_0.pdf](https://www.jitec.ipa.go.jp/1_13download/syllabus_sc_ver2_0.pdf)）を参照する

【注釈】

※1 「○」は主導できるレベル（情報処理安全確保支援士試験レベル）、「○」はコミュニケーションが取れるレベル（情報セキュリティマネジメント試験レベル）を想定。

※2 企業等によって、「○」、「○」の付し方の変更や、知識・スキル項目の追加・削除・詳細化が必要。

※3 分野に固有のタスクを実施するための知識・スキルについては含まれていない。

	分野	セキュリティ関連知識・スキル（大項目）		
		セキュリティマネジメント	システムセキュリティ	セキュリティオペレーション
戦略 マネ シ メン ト 層	経営リスクマネジメント	○		
	法務			
	システム監査			
	事業ドメイン（戦略・企画）			
	セキュリティ統括	◎	○	○
	セキュリティ監査			
	デジタルシステムストラテジー			
実務 者・ 技 術 者 層	デジタルシステムアーキテクチャ	○	◎	○
	デジタルプロダクト開発	○	◎	◎
	脆弱性診断・ペネトレーションテスト			
	セキュリティ監視・運用			
	セキュリティ調査分析・研究開発			
	デジタルプロダクト運用		○	○
	事業ドメイン（生産現場・店舗管理）			○

大項目	セキュリティマネジメント	システムセキュリティ	セキュリティオペレーション
大項目の概要	経営層の下で組織の特性に応じた適切なセキュリティ体制・ポリシーの構築・運用が行える	セキュアなシステムの企画・設計・開発が行える	セキュリティインシデントへの事前対策・事後対応が適切に行える
情報処理安全確保支援士試験シラバス大項目との対応	(1)情報セキュリティマネジメントの推進又は支援に関すること	(2)情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること	(3)情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること (4)情報セキュリティインシデント管理の推進又は支援に関すること

※情報処理安全確保支援士試験シラバス [https://www.jitec.ipa.go.jp/1\\_13download/syllabus\\_sc\\_ver2\\_0.pdf](https://www.jitec.ipa.go.jp/1_13download/syllabus_sc_ver2_0.pdf)

## ■ 旧版の専門分野との対応関係の目安

→ 旧版を活用している方に向け、旧版の専門分野との対応関係の目安を示すもの

分野			旧版の専門分野
経営層	セキュリティ	セキュリティ経営（CISO）	（対応する専門分野なし）
戦略マネジメント層	デジタル	システム監査	情報リスクストラテジ
		デジタルシステムストラテジー	情報セキュリティ監査
	セキュリティ	セキュリティ監査	CSIRTコマンド
		セキュリティ統括	CSIRTリエゾン
			CSIRTキュレーション
			情報セキュリティアドミニレーション
	その他	経営リスクマネジメント	情報リスクストラテジ
		法務	（対応する専門分野なし）
		事業ドメイン（戦略・企画・調達）	
実務者層・技術者層	デジタル	デジタルシステムアーキテクチャ	情報セキュリティデザイン
		デジタルプロダクト開発	セキュア開発管理
		デジタルプロダクトマネジメント	
	セキュリティ	脆弱性診断・ペネトレーションテスト	脆弱性診断
		セキュリティ監視・運用	情報セキュリティアドミニストレーション
		セキュリティ調査分析・研究開発	インシデントハンドリング
			情報セキュリティアナリシス
	その他	事業ドメイン（生産現場・店舗管理）	デジタルフォレンジクス
（対応する分野なし）			（対応する専門分野なし）
			情報セキュリティインベスティゲーション

領域	セキュリティ領域												
専門分野	情報リスクストラテジ	情報セキュリティデザイン	セキュリティ開発管理	脆弱性診断	アプリケーションセキュリティ	アプリケーションセキュリティ	C S I R T キュレーション	C S I R T リエゾン	C S I R T コマンド	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティゲーション	情報セキュリティ監査
レベル7													
レベル6													
レベル5													
レベル4													
レベル3													
レベル2													
レベル1													
登録せしめ 想定業務	経営 課題	設計・開発			運用・保守			緊急対応				監査	

専門分野	説明
情報リスクストラテジ	自組織または受託先における業務遂行の妨げとなる情報リスクを認識し、その影響を抑制するための、組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定等を推進する。自組織または受託先内の情報セキュリティ対策関連業務全体を俯瞰し、アウトソース等を含むリソース配分の判断・決定を行う。
情報セキュリティデザイン	「セキュリティバイデザイン」の観点から情報システムのセキュリティを担保するためのアーキテクチャやポリシーの設計を行うとともに、これを実現するために必要な組織、ルール、プロセス等の整備・構築を支援する。
セキュア開発管理	情報システムや製品に関するリスク対応の観点に基づき、機能安全を含む情報セキュリティの側面から、企画・開発・製造・保守などにわたる情報セキュリティライフサイクルを統括し、対策の実施に関する責任をもつ。
脆弱性診断	ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行い、診断結果の評価を行う。
情報セキュリティ アドミニストレーション	組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むとともに、対策の立案や実施（指示・統括）、その見直し等を通じて、自組織または受託先における情報セキュリティ対策の具体化や実施を統括する。また、利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する。
情報セキュリティアナリシス	情報セキュリティ対策の現状に関するアセスメントを実施し、あるべき姿とのギャップ分析をもとにリスクを評価した上で、自組織または受託先の事業計画に合わせて導入すべきソリューションを検討する。導入されたソリューションの有効性を確認し、改善計画に反映する。
CSIRTキュレーション	情報セキュリティインシデントへの対策検討を目的として、セキュリティイベント、脅威や脆弱性情報、攻撃者のプロファイル、国際情勢、メディア動向等に関する情報を収集し、自組織または受託先に適用すべきかの選定を行う。
CSIRTリエゾン	自組織外の関係機関、自組織内の法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、情報セキュリティインシデントに係る情報連携及び情報発信を行う。必要に応じてIT部門とCSIRTの間での調整の役割を担う。
CSIRTコマンド	自組織で起きている情報セキュリティインシデントの全体統制を行うとともに、事象に対する対応における優先順位を決定する。重大なインシデントに関してはCISOや経営層との情報連携を行う。また、CISOや経営者が意思決定する際の支援を行う。
インシデントハンドリング	自組織または受託先におけるセキュリティインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携する。情報セキュリティインシデントへの対応状況を管理し、CSIRTコマンドのタスクを担当する者へ報告する。
デジタルフォレンジクス	悪意をもつ者による情報システムやネットワークにを対象とした活動の証拠保全を行うとともに、消されたデータを復元したり、痕跡を追跡したりするための体系的な鑑識、精密検査、解析、報告を行う。
情報セキュリティ インベスティゲーション	情報セキュリティインシデントを対象として、外部からの犯罪、内部犯罪を捜査する。犯罪行為に関する動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に捜査対象の絞り込みを行う。
情報セキュリティ監査	情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、もって保証を与えあるいは助言を行う。

スキル項目 コード	スキル カテゴリ	スキル分類	スキル項目	ITSS+（セキュリティ）													ITスキル 準／CD
				情報リスクストラテジ	情報セキュリティデザイン	セキュリティ階層管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキエーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティグレーション	情報セキュリティ監査	
S110010010	メソドロジー	(戦略) 市場機会の評価と選定	ビジネス環境分析手法	○													
S110010020			ビジネス戦略と目標・評価	○													
S110010030			業界動向把握の手法	○													
S110010040			経営管理システム	○													
S110010050			経営戦略手法	○													
S110010060			最新技術動向把握の手法	○	○	○					○						
S110010070			市場調査手法														
S110020010	(戦略) マーケティング		ブランド・製品戦略手法														
S110020020			マーケットコミュニケーション戦略手法														
S110020030			マーケティングマネジメント手法														
S110020040			マーケティング分析手法														
S110030010	(戦略) 製品・サービス戦略		製品戦略手法														
S110030020			サービス戦略手法														
S110030030			ITSM戦略手法														
S110030040			データセンタ戦略手法														
S110040010	(戦略) 販売戦略		B2Bマーケティング戦略手法														
S110040020			販売実行戦略手法														
S110040030			販売チャネル戦略手法														
S110050010	(戦略) 製品・サービス開発戦略		顧客環境分析手法			○								○			
S110050020			製品開発戦略手法			○											
S110050030			技術開発計画		○	○											
S110050040			技術開発戦略の立案		○	○											
S110060010	(戦略) システム戦略立案手法		システム化戦略手法	○	○	○		○						○			
S110060020			システム活用促進・評価	○	○	○		○						○			
S110060030			ソリューションビジネス	○	○	○		○						○			
S110060040			業務プロセス	○	○	○		○						○			
S110060050			現行システムの調査・分析手法	○	○	○		○						○			
S110060060			事業戦略の把握・分析の手法	○	○	○		○						○			
S110060070			情報システム戦略	○	○	○		○						○			
S110060080			戦略分析手法														
S110070010	(戦略) コンサルティング手法		コンサルティング手法	○													
S110080010	(戦略) 業務動向把握手法		業務動向の把握手法	○	○			○			○			○			
S120010010	(企画) システム企画立案手法		システム化計画		○												
S120010020			システム企画立案手法	○	○	○		○						○			
S120010030			ソリューション提案手法	○		○		○									
S120010040			技術問題解決手法		○	○											
S120010050			調達計画・実施		○												
S120020010	(企画) セールス事務管理手法		セールス交渉手法														
S120020020			契約事務手法			○		○									
S120020030			経理事務手法														
S120030010	(企画) 要求分析手法		要求の抽出手法		○				○			○					
S120030020			要求の整理手法		○	○			○			○					
S120030030			要求の仕様化手法		○				○			○					
S120030040			要求の評価手法		○				○			○					
S120030050			要件定義		○				○			○					
S120040010	(企画) 非機能要件設計手法		プラットフォーム要件定義手法		○	○					○						
S120040020			システム基盤の非機能要件設計		○	○					○						
S130010010	(実装) アーキテクチャ設計手法		アーキテクチャ設計手法		○	○			○								
S130010020			アプリケーションアーキテクチャ設計手法		○	○											
S130010030			インダストリアルパッケージ設計・開発手法		○	○											
S130010040			インフラストラクチャアーキテクチャ設計手法		○	○			○			○					
S130010050			データアーキテクチャ設計手法		○	○											
S130020010	(実装) ソフトウェアエンジニアリング手法		セキュリティ実装手法	○	○	○											
S130020020			ソフトウェアデザイン手法		○	○											
S130020030			ソフトウェアのモデリング手法		○	○											
S130020040			ソフトウェア開発手法		○	○			○								
S130020050			ソフトウェア製作手法		○	○			○								
S130020060			ソフトウェア設計の表記手法		○	○											
S130020070			開発プロセス設定手法			○											
S130020080			開発環境設計手法			○											
S130020090			ソフトウェア設計手法		○	○											
S130020100			保守サービス提供手法														
S130050010	(実装) カスタマーサービス手法		ハードウェア導入手法														
S130050020			ソフトウェア導入・配備手法														
S130050030			予防保守手法														
S130060010	(実装) 業務パッケージ適用手法		業務パッケージ適用手法					○			○						
S130060020			業務パッケージ導入手法					○			○						
S130080010	(実装) データマイニング手法		データ分析手法														
S130080020			マイニングモデル手法														
S130080030			テキストマイニング手法														
S130090010	(実装) 見積り手法		見積の見積手法		○												
S130090020			コストの見積り手法														
S130100010	(実装) プロジェクトマネジメント手法		プロジェクトマネジメント			○				○							
S130100020			プロジェクト統合マネジメント			○				○							
S130100030			プロジェクトコストマネジメント			○				○							
S130100040			プロジェクトコミュニケーションマネジメント			○				○							

[illegible]



S210020070	テクノロジ		リアルタイムシステム設計			○			○									
S210020080			ソフトウェア開発のフォールトトレランス			○			○									
S210020090			ソフトウェア構築			○			○									
S210020100			ソフトウェア結合・ソフトウェア適格性確認テスト			○			○								○	
S210020110			受入れ支援			○			○									
S210020120			開発ツール			○	○										○	
S210020130			再利用のための構築			○											○	
S210020140			構築品質			○	○		○			○				○	○	
S210020150	テクノロジ		テストツール			○	○		○						○		○	
S210020160			セキュアプログラミング技法		○	○	○		○									
S210020170			セキュアプログラミング技法（データベース）		○	○	○		○									
S210030010		(システム)	ソフトウェアの利用技術				○											
S210030020			既存ソフトウェアの把握技法				○											
S210030030			ソフトウェアの進化や保守				○		○									
S210030040			業務パッケージ最新動向				○										○	
S210030050			インテリジェントシステム				○											
S210040010	(システム)	Webシステムの基礎技術	Webシステムとその技術				○											
S210040020			サーバ技術				○											
S210040030			インターネットアプリケーション基礎技術				○											
S210040040			アプリケーションサービス				○											
S210040050			アプリケーション実行方式				○											
S210050010		(システム)	Webシステムの構築技術				○											
S210050020			分散コンピューティング開発環境				○											
S210060010		(システム)	Webシステムの基礎技術				○											
S210070010	(システム)	データベースの基礎技術	データベース				○											
S210070020			リレーショナルモデル				○											
S210070030			データベース方式				○											
S210070040			データ操作				○											
S210070050			トランザクション処理				○											
S210070060			SQL				○											
S210070070			情報管理				○											
S210080010		(システム)	データベースの構築技術				○											
S210080020			データベース設計				○											
S210080030			データベースマネジメントシステム（DBMS）の選定・導入				○											
S210080040			データベースシステムの受け入れ				○											
S210080050			データベースマネジメントシステム（DBMS）への実装とテスト				○											
S210080060			データベース開発における重要技術				○											
S210090010		(システム)	データベースの利用技術				○											
S210090020			データのオペレーション管理技術				○											
S210090030			データベースシステム管理				○											
S210090040			データベース運用技術				○											
S210090050			データベース運用設計				○											
S210090060			データアクセスサービス設計技術				○											
S210090070			データクオリティ管理技術				○											
S210090080			データと情報の管理				○											
S210090090			データベース応用				○											
S210090100			データベース関連製品の利用技術				○											
S210090110			データベースの周辺技術				○											
S210090120			データベース診断技術とチューニング技術				○											
S210090130			データ移行				○											
S210090140			データ移行設計				○											
S210090150			データ統合サービス設計技術				○											
S210090160			マスタデータ管理技術				○											
S210090170			ドキュメントとコンテンツ管理技術				○											
S210090180			情報製品の設計技術				○											
S210090190			データ照会・加工・クレンジング技術				○											
S210090200			データマイニングツールの利用技術				○											
S210100010		(システム)	プラットフォームの基礎技術				○											
S210100020			ミドルウェア				○											
S210100030			プラットフォーム技術				○											
S210110010		(システム)	プラットフォームの構築技術				○											
S210110020			プラットフォーム実装技術				○											
S210110030			共通基盤としてのプラットフォーム設計構築				○											
S210120010		(システム)	プラットフォームの利用技術				○											
S210120020			システム診断技術と障害対策技術				○											
S210120030			プラットフォームシステム管理				○											
S210120040			製品知識（プラットフォーム）				○											
S210130010	(システム)	ハードウェアの基礎技術	ハードウェア				○											
S210130020			製品知識基礎															
S210140010	(システム)	ハードウェアの構築技術	ITアーキテクチャ（ハードウェア）				○											
S210140020			VLSIの設計および製造															
S210150010	(システム)	ハードウェアの利用技術	サーバ配置手法															
S210150020			ストレージ技術															
S210160010	(システム)	ネットワークの基礎技術	ネットワーク		○	○		○	○			○						
S210160020			ネットワークコンピューティング		○	○		○	○			○						
S210160030			ネットワークシステムの技術動向		○	○		○	○			○						
S210160040			ネットワーク標準		○	○		○	○			○						
S210160050			ネットワーク方式		○	○		○	○			○						
S210160060			通信プロトコル		○	○		○	○			○						
S210160070			データ通信と制御					○	○			○						
S210170010		(システム)	ネットワークの構築技術															
S210170020			ネットワーク設計															
S210170030			ネットワークシステムの実装技術															
S210170040			ネットワークシステムの導入と移行															
S210170050			ネットワークシステムの受け入れ															
S210170060			ネットワークシステムの運用・保守・管理															
S210180010	(システム)	ネットワークの利用技術	ネットワーク管理			○			○				○					

S210180020		ネットワーク応用			○				○										
S210180030		ネットワーク製品知識			○			○					○						
S210180040		業界固有のセキュリティ要件、事例	○	●	○			○	○				○					○	
S210180050		ネットワークシステムの評価			○			○	○				○						
S210180060		テレコミュニケーション			○														
S210190010	(システム) クラウドコンピューティングの構築技術	クラウドコンピューティング基礎		●	○			○	○				○						○
S210200010	(システム) クラウドコンピューティングの構築技術	クラウドデータベース技術		●	○														○
S210200020	(システム) クラウドコンピューティングの構築技術	クラウド構築技術		●	○														○
S210200030	(システム) クラウドコンピューティングの構築技術	クラウドアプリケーション実装技術		●	○														○
S210200040	(システム) クラウドコンピューティングの構築技術	仮想マシニングストのセキュリティ			○	○		○	○				○	○	●			○	○
S210210010	(システム) クラウドコンピューティングの構築技術	インタークラウド技術			○			○	○				○						○
S210210020	(システム) クラウドコンピューティングの構築技術	クラウドコンピューティング利用		●	○			○	○				○						○
S210210030	(システム) クラウドコンピューティングの構築技術	クラウドシステムの監視技術		●	○			○	○				○						○
S220010010	(開発) システムアーキテクティング技術	システム要件定義	○	●	●			○	○				○						○
S220010020	(開発) システムアーキテクティング技術	システムインテグレーションとアーキテクチャ		●	●			○	○				○						
S220010030	(開発) システムアーキテクティング技術	アプリケーション共通基盤要件定義手法		●	●				○				○						
S220010040	(開発) システムアーキテクティング技術	アプリケーション共通基盤設計手法		●	●														
S220010050	(開発) システムアーキテクティング技術	IT基盤構築プロセス		●	●				○				○						○
S220010060	(開発) システムアーキテクティング技術	システム間連携技術		●	●														
S220010070	(開発) システムアーキテクティング技術	システム方式設計		●	●														○
S220010080	(開発) システムアーキテクティング技術	システム結合・システム適合性確認テスト			○														
S220010090	(開発) システムアーキテクティング技術	導入			●														
S220010100	(開発) システムアーキテクティング技術	オブジェクト指向技術		○	●														
S220010110	(開発) システムアーキテクティング技術	ファイルシステム			●														
S220010120	(開発) システムアーキテクティング技術	フレームワーク要素技術			○														
S220010130	(開発) システムアーキテクティング技術	レガシーマイグレーション技術																	
S220020010	(開発) システム開発管理技術	開発プロセス・手法		○	●														
S220020020	(開発) システム開発管理技術	開発環境管理		○	●														
S220020030	(開発) システム開発管理技術	知的財産活用管理			○														
S220020040	(開発) システム開発管理技術	構成管理・変更管理			○														
S230010010	(保守・運用) ITサービスマネジメント業務管理技術	ITサービスマネジメントの業務フロー分析																	
S230010020	(保守・運用) ITサービスマネジメント業務管理技術	運用業務管理システムの運用管理																	
S230010030	(保守・運用) ITサービスマネジメント業務管理技術	運用業務管理システムの導入・設定																	
S230020010	(保守・運用) ITサービスオペレーション技術	サービスデリバリ																	○
S230020020	(保守・運用) ITサービスオペレーション技術	業務システムオペレーション																	○
S230020030	(保守・運用) ITサービスオペレーション技術	システム運用（オペレーション）																	○
S230020040	(保守・運用) ITサービスオペレーション技術	ジョブスケジュール																	○
S230020050	(保守・運用) ITサービスオペレーション技術	障害管理																	
S230020060	(保守・運用) ITサービスオペレーション技術	顧客デリバリ																	
S230020070	(保守・運用) ITサービスオペレーション技術	媒体管理																	
S230020080	(保守・運用) ITサービスオペレーション技術	システムの監視							○				○	○					○
S230020090	(保守・運用) ITサービスオペレーション技術	稼働状況管理							○				○						○
S230030010	(保守・運用) システム保守・運用・評価	移行設計			○								○						○
S230030020	(保守・運用) システム保守・運用・評価	移行			○								○						○
S230030030	(保守・運用) システム保守・運用・評価	プラットフォーム移行設計			○								○						○
S230030040	(保守・運用) システム保守・運用・評価	プラットフォーム移行			○								○						○
S230030050	(保守・運用) システム保守・運用・評価	アプリケーションシステムの受け入れ			○				○				○						○
S230030060	(保守・運用) システム保守・運用・評価	システム運用管理要件定義		○	○														
S230030070	(保守・運用) システム保守・運用・評価	システム運用管理設計		○	○														
S230030080	(保守・運用) システム保守・運用・評価	システム運用方式技法		○	○			○	○				○	○					○
S230030090	(保守・運用) システム保守・運用・評価	システムの投資評価技法		○	○														
S230030100	(保守・運用) システム保守・運用・評価	システム管理計画		○	○			○	○				○	○					○
S230030110	(保守・運用) システム保守・運用・評価	システム管理技術		○	○			○	○				○	○					○
S230030120	(保守・運用) システム保守・運用・評価	システム保守基準		○	○				○				○						○
S230030130	(保守・運用) システム保守・運用・評価	運行管理			○								○						○
S230030140	(保守・運用) システム保守・運用・評価	システム管理製品			○			○	○				○	○	○				○
S230030150	(保守・運用) システム保守・運用・評価	運用管理ソフト製品						○	○				○	○	○				○
S230030160	(保守・運用) システム保守・運用・評価	運用システムの構築											○						○
S230030170	(保守・運用) システム保守・運用・評価	運用システムの改善						○	○				○	○					○
S230030180	(保守・運用) システム保守・運用・評価	運用に関するシステム評価						○	○				○	○					○
S230030190	(保守・運用) システム保守・運用・評価	性能管理			○			○					○						○
S230030200	(保守・運用) システム保守・運用・評価	障害時運用方式	○	○	○			○					○	○	○			○	○
S230030210	(保守・運用) システム保守・運用・評価	災害対策	○	○	○			○					○	○	○			○	○
S230030220	(保守・運用) システム保守・運用・評価	構成管理			○								○						○
S230030230	(保守・運用) システム保守・運用・評価	保守技術			○				○				○	○					○
S230030240	(保守・運用) システム保守・運用・評価	メンテナンス			○				○				○	○					○
S230030250	(保守・運用) システム保守・運用・評価	保守・廃棄											○	○					○
S230040010	(保守・運用) 障害修理技術	障害状況把握・原因特定																	
S230040020	(保守・運用) 障害修理技術	障害コール受付																	
S230040030	(保守・運用) 障害修理技術	処置・修復作業の実践・動作検証																	
S230050010	(保守・運用) 施工実務技術	施工実務手法																	
S230050020	(保守・運用) 施工実務技術	工程・安全・環境管理																	
S230050030	(保守・運用) 施工実務技術	ファシリティ関連工事																	
S230060010	(保守・運用) ファシリティ設計技術	ファシリティマネジメント技術問題解決技法																	
S230060020	(保守・運用) ファシリティ設計技術	建築の基礎知識と建築用図面（CAD）基礎知識																	
S230060030	(保守・運用) ファシリティ設計技術	環境対策																	
S230060040	(保守・運用) ファシリティ設計技術	信頼性、可用性、保守性		○				○					○						
S230060050	(保守・運用) ファシリティ設計技術	耐震安全確保		○				○					○						
S230060060	(保守・運用) ファシリティ設計技術	物理ネットワーク（通信ネットワーク）の設計		○				○					○						
S230060070	(保守・運用) ファシリティ設計技術	防災防災設備設計		○				○					○						
S230060080	(保守・運用) ファシリティ設計技術	施工設計・計画																	
S230060090	(保守・運用) ファシリティ設計技術	コスト精算																	
S230060100	(保守・運用) ファシリティ設計技術	品質管理の知識		○				○					○						
S230070010	(保守・運用) サポートセンター基盤技術	インシデント管理システム	○	○	○			○			○	○	○	○				○	
S230070020	(保守・運用) サポートセンター基盤技術	コールトラッキングシステム																	
S230070030	(保守・運用) サポートセンター基盤技術	コンピュータテレフォニー																	
S240010010	非機能要件（可用性、性能、拡張性）	非機能要件の基礎		○	○			○					○					○	○

[illegible]



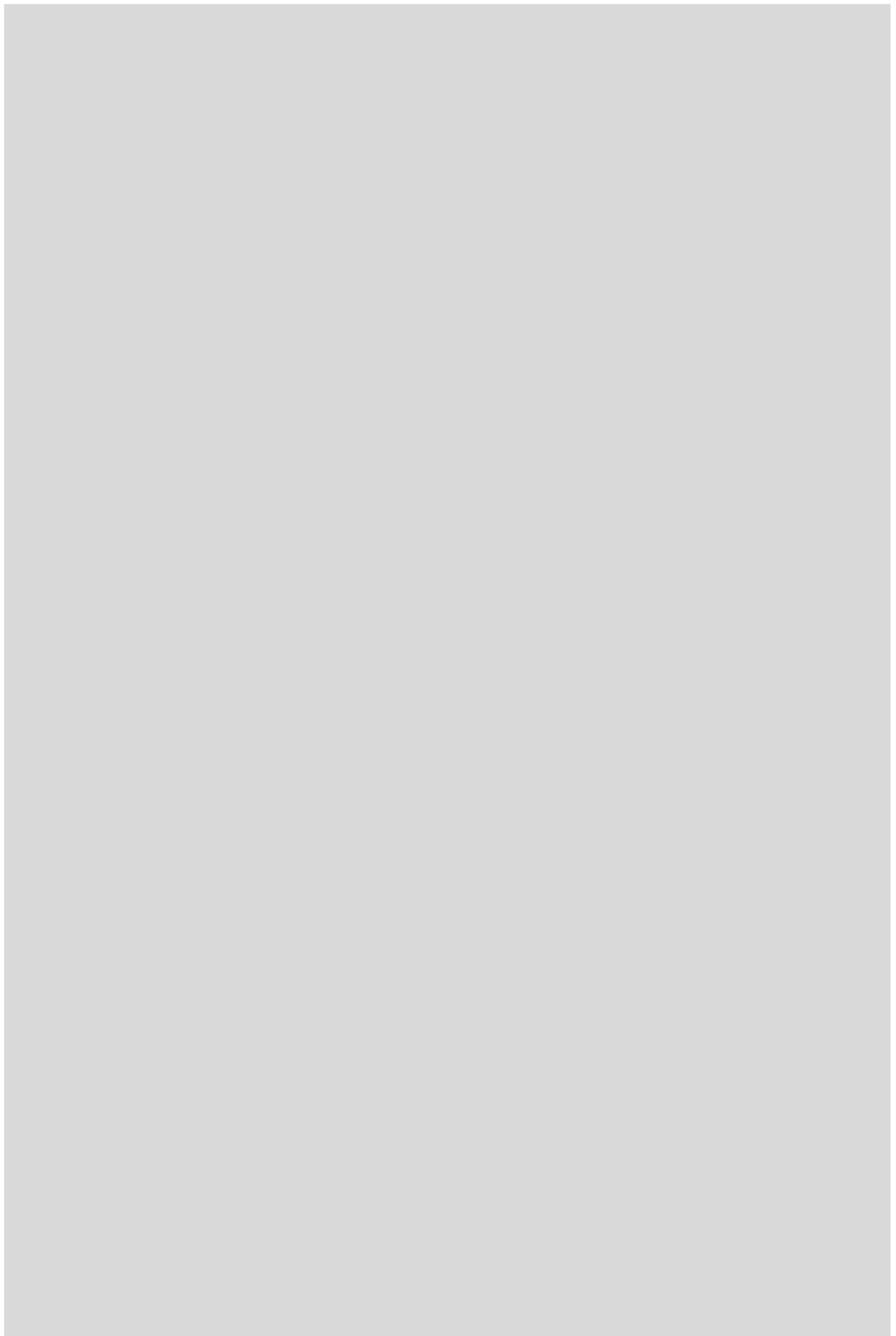


















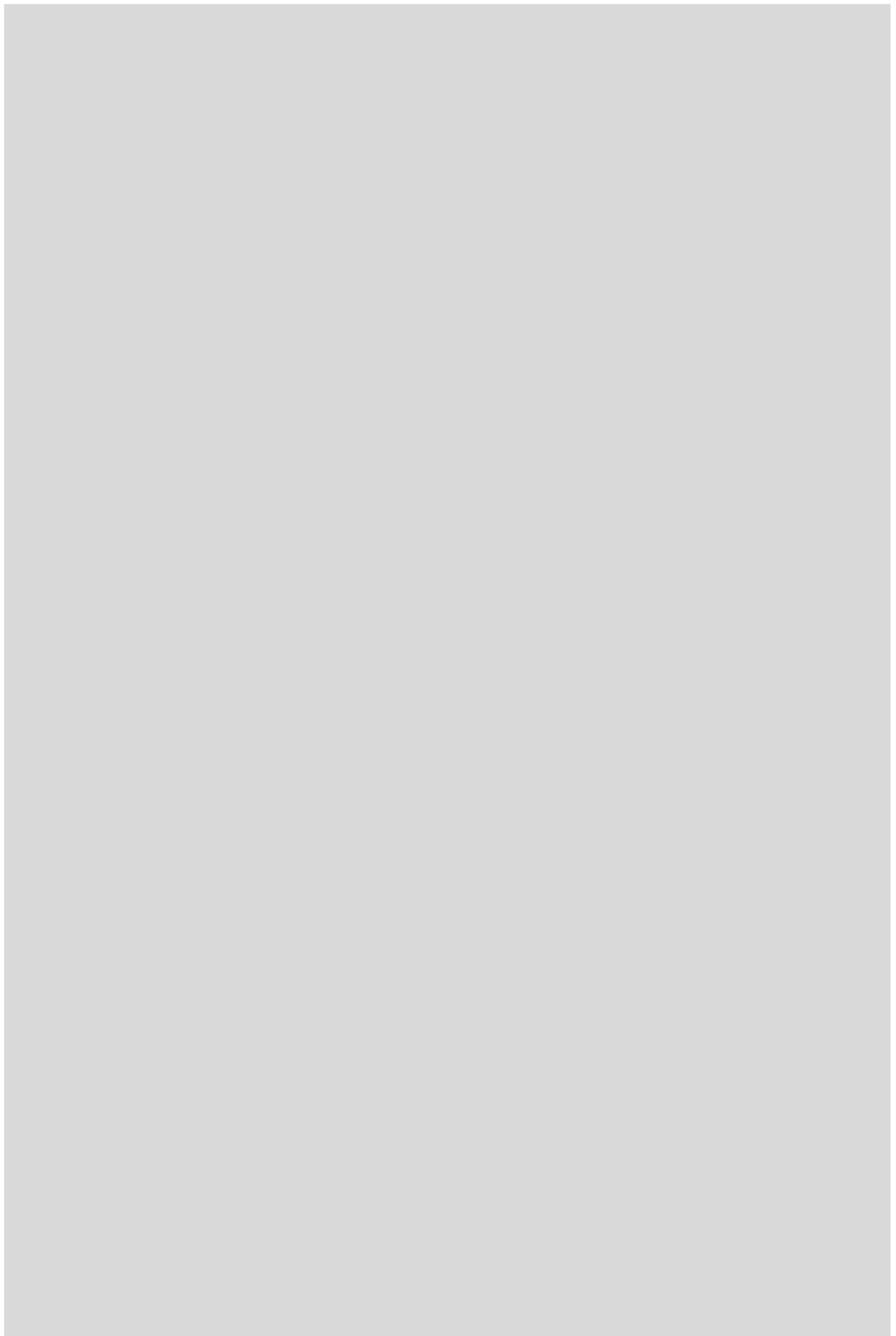


















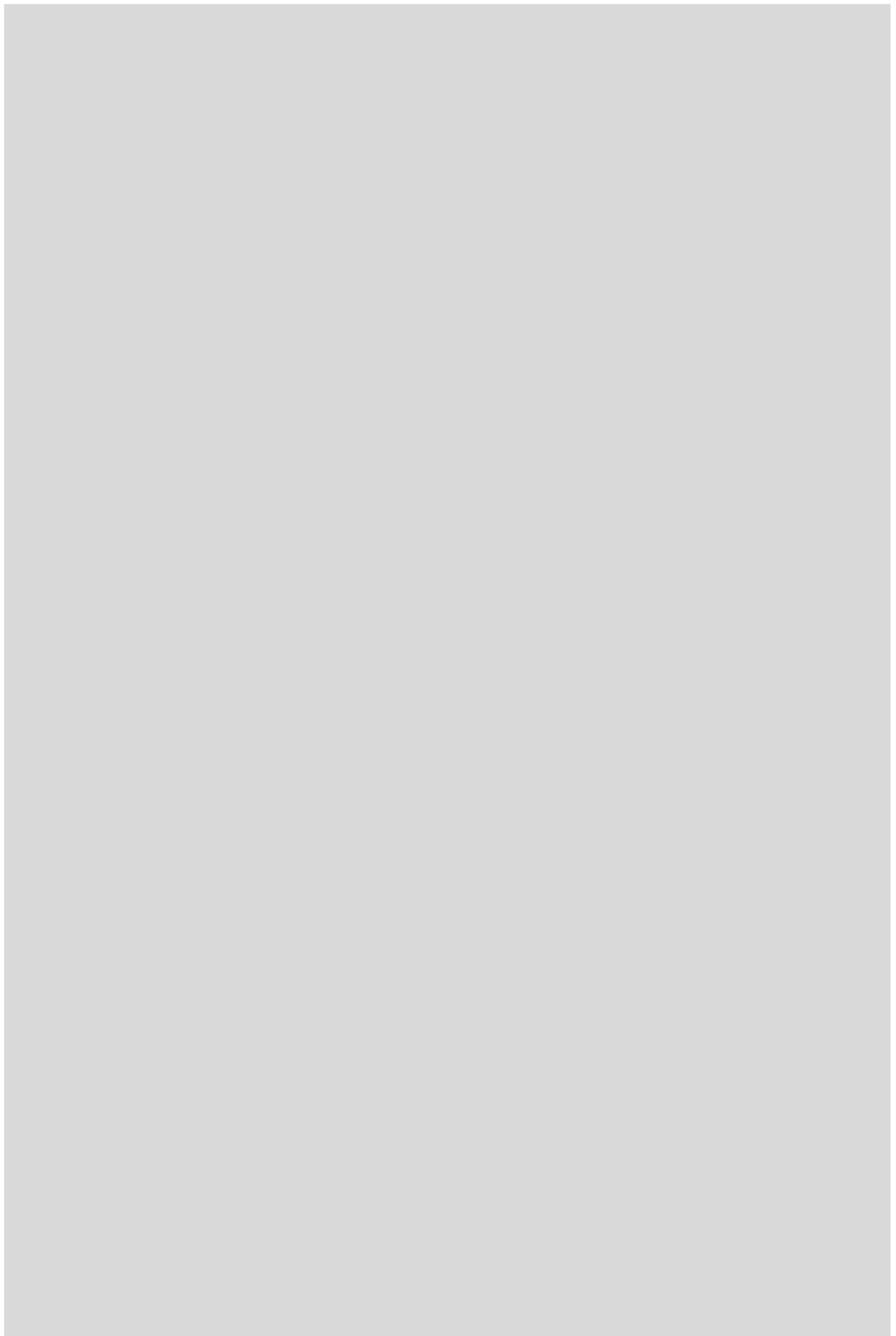


















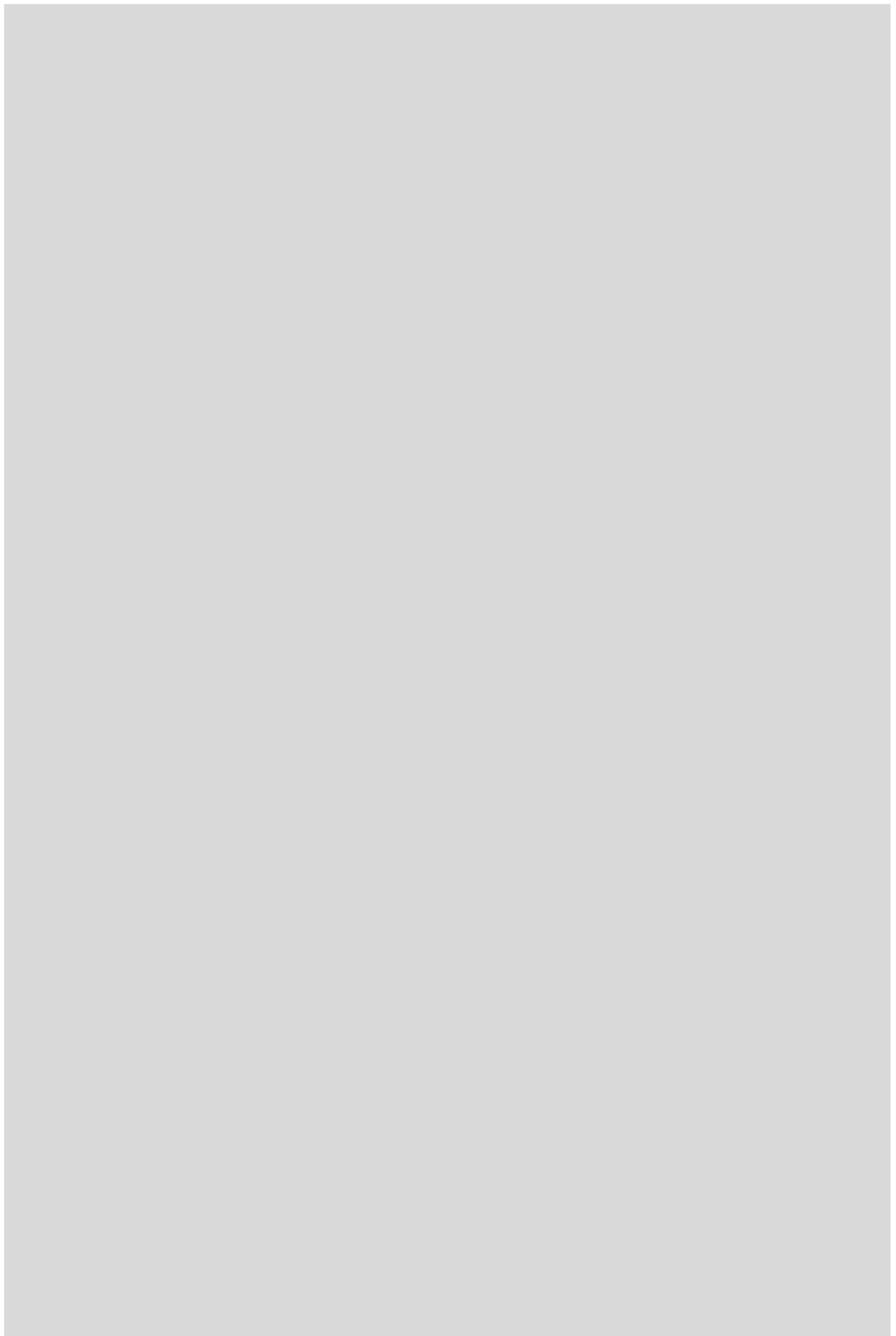


















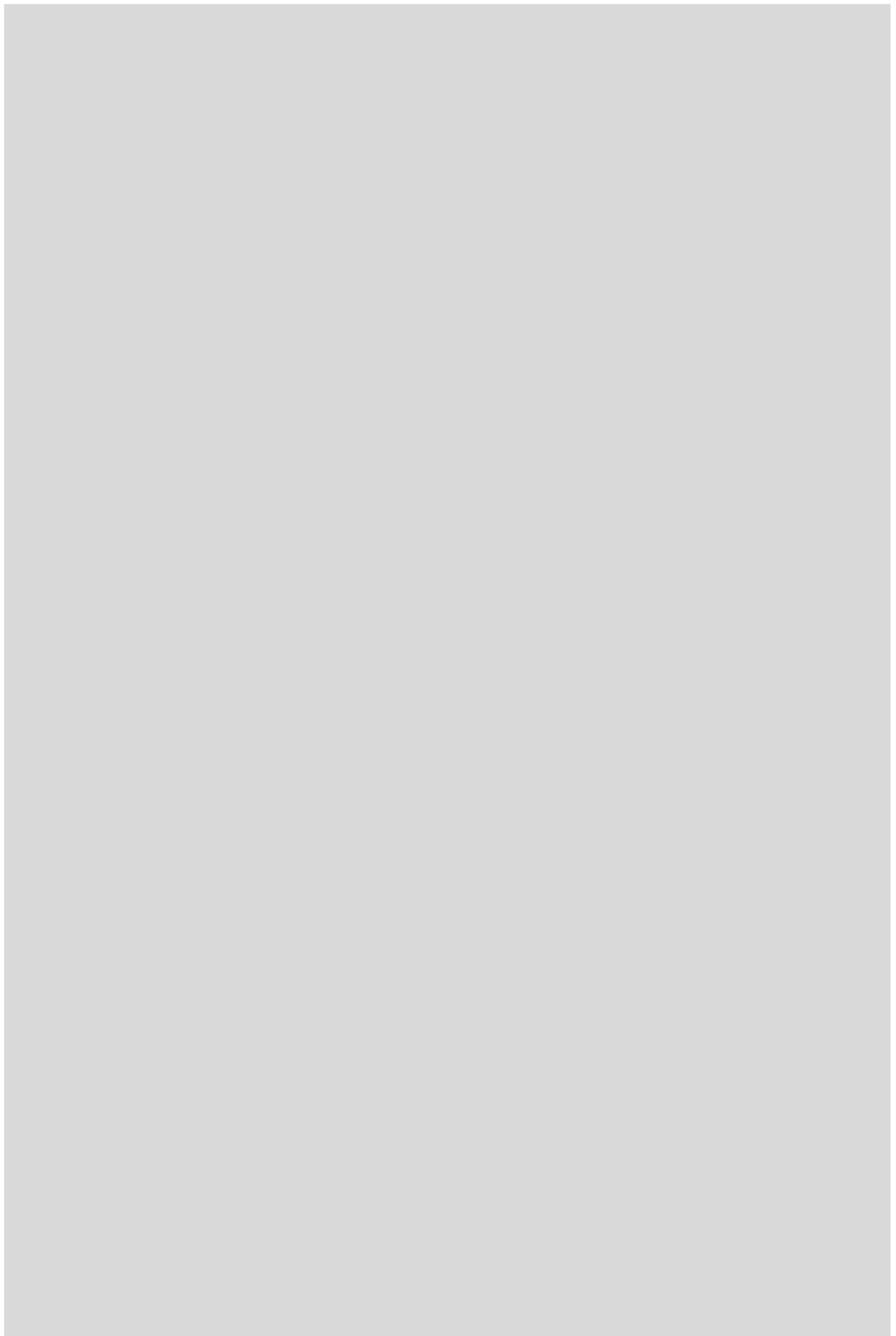


















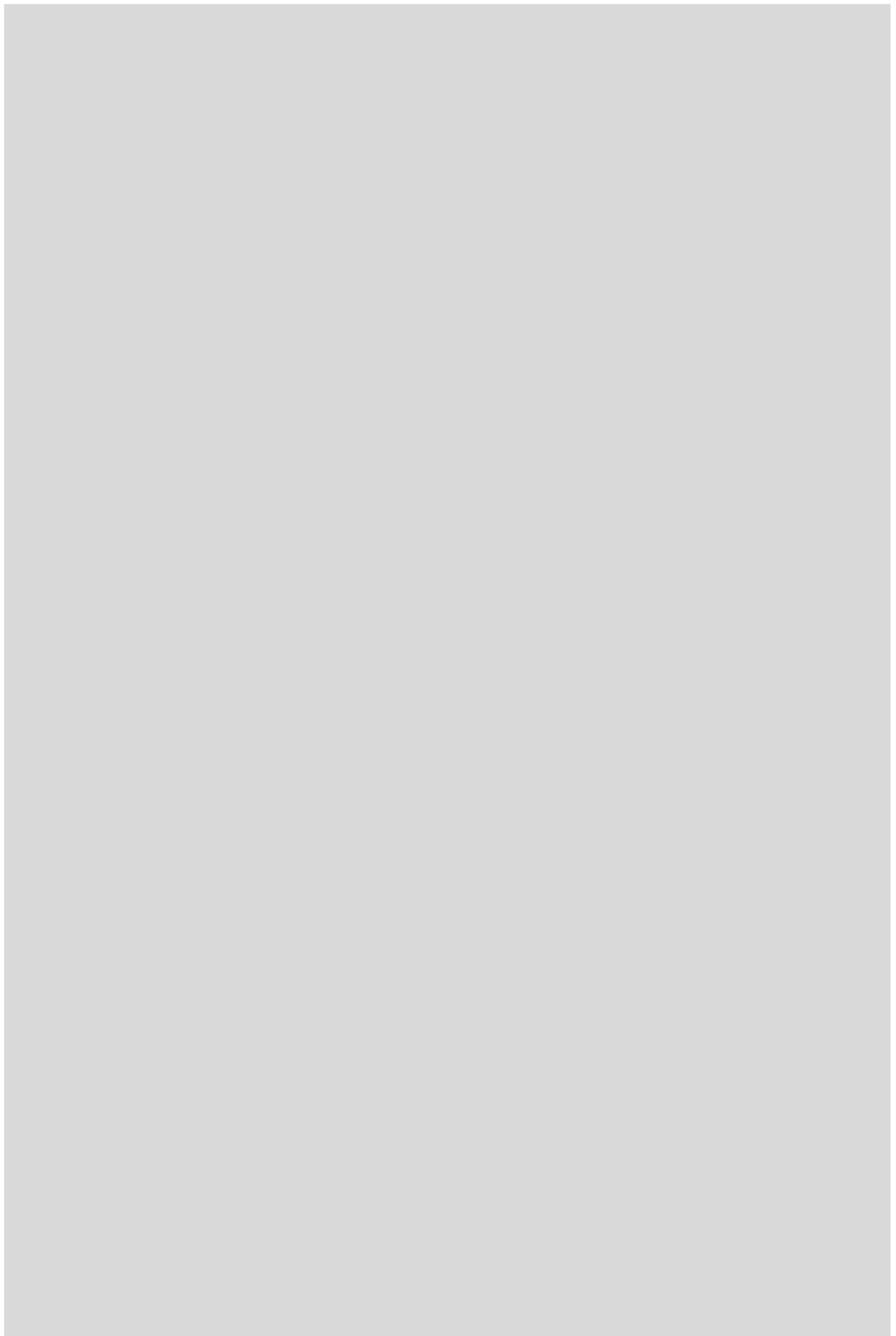


















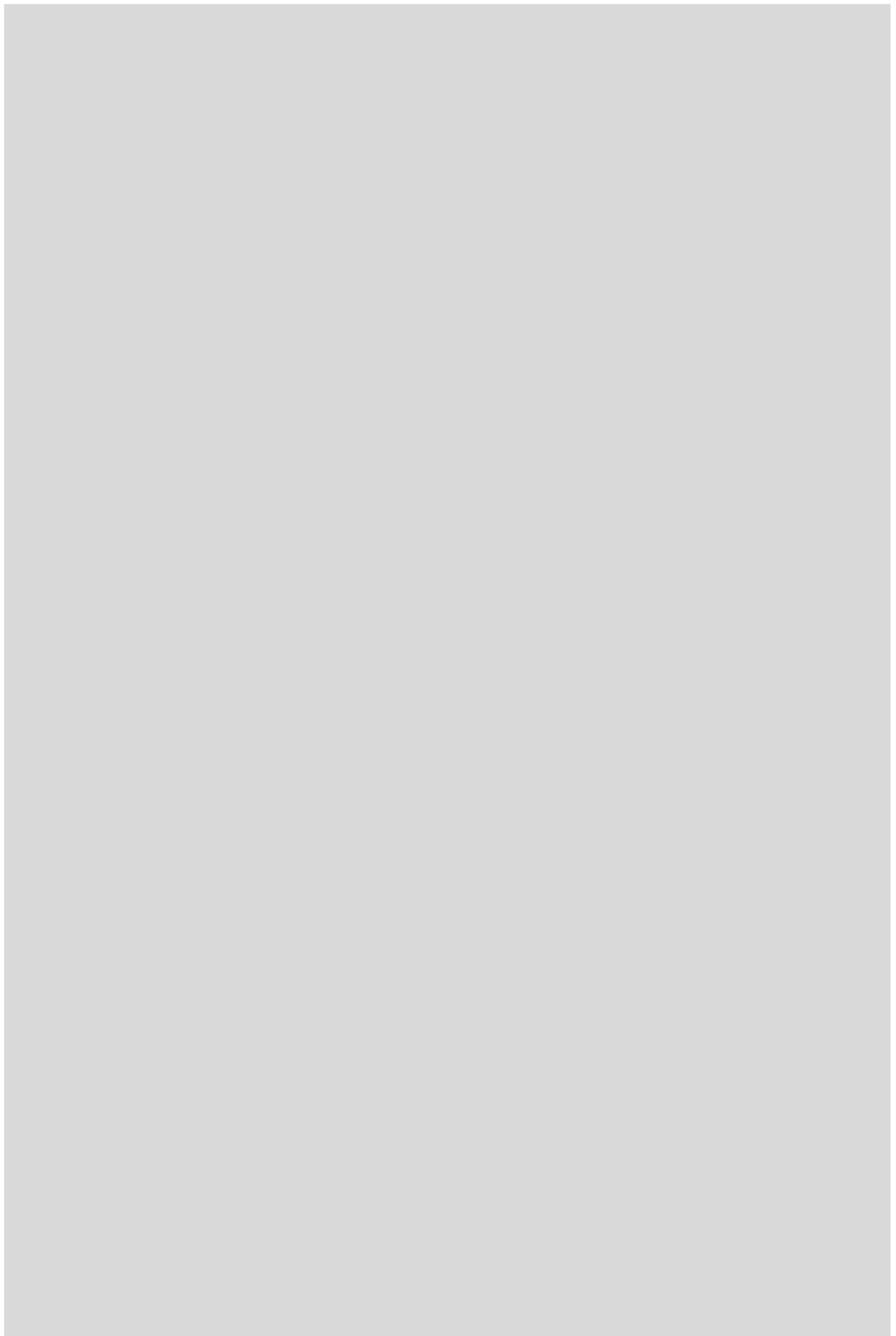




















タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）														ITスキル標準／ICD	ITスペシャリスト（セキュリティ）																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																									
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインバースティゲーション	情報セキュリティ監査																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																												
ST01	事業戦略策定	ST01.1	事業環境の分析	ST01.1.1	経営方針の確認																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																									

タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）													ITSS+標準 ／iCD	ITSS+標準 ／iCD （セキュリティ）
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティベンステイゲーション	情報セキュリティ監査		
DV01	システム要件定義・方式設計	DV01.1	システム化要件定義	DV01.1.4	非機能要件の定義		○	○											○	○
DV01	システム要件定義・方式設計	DV01.1	システム化要件定義	DV01.1.5	システム化要件の文書化とレビュー														○	○
DV01	システム要件定義・方式設計	DV01.2	システム化要件定義（Webサイト）	DV01.2.1	現状把握															
DV01	システム要件定義・方式設計	DV01.2	システム化要件定義（Webサイト）	DV01.2.2	対象Webサイトの要件定義															
DV01	システム要件定義・方式設計	DV01.2	システム化要件定義（Webサイト）	DV01.2.3	システム化要件の文書化とレビュー															
DV01	システム要件定義・方式設計	DV01.3	セキュリティ要件定義	DV01.3.1	現状把握		○				○								○	○
DV01	システム要件定義・方式設計	DV01.3	セキュリティ要件定義	DV01.3.2	セキュリティ要件の定義		○					○							○	○
DV01	システム要件定義・方式設計	DV01.3	セキュリティ要件定義	DV01.3.3	セキュリティ要件の評価		○				○			○					○	○
DV01	システム要件定義・方式設計	DV01.4	システム方式設計	DV01.4.1	システム方式の設計														○	○
DV01	システム要件定義・方式設計	DV01.4	システム方式設計	DV01.4.2	適用製品・技術の評価と選定		○	○											○	○
DV01	システム要件定義・方式設計	DV01.4	システム方式設計	DV01.4.3	システム方式設計の文書化とレビュー														○	○
DV01	システム要件定義・方式設計	DV01.5	システム方式設計（ソフトウェア製品）	DV01.5.1	システム方式の設計															
DV01	システム要件定義・方式設計	DV01.5	システム方式設計（ソフトウェア製品）	DV01.5.2	適用製品・技術の評価と選定															
DV01	システム要件定義・方式設計	DV01.5	システム方式設計（ソフトウェア製品）	DV01.5.3	システム方式設計の文書化とレビュー															
DV01	システム要件定義・方式設計	DV01.6	システム方式設計（組込みソフトウェア）	DV01.6.1	システム方式の設計															
DV01	システム要件定義・方式設計	DV01.6	システム方式設計（組込みソフトウェア）	DV01.6.2	適用製品・技術の評価と選定															
DV01	システム要件定義・方式設計	DV01.6	システム方式設計（組込みソフトウェア）	DV01.6.3	システム方式設計の文書化とレビュー															
DV01	システム要件定義・方式設計	DV01.7	システム方式設計（Webサイト）	DV01.7.1	システム方式の設計															
DV01	システム要件定義・方式設計	DV01.7	システム方式設計（Webサイト）	DV01.7.2	適用製品・技術の評価と選定															
DV01	システム要件定義・方式設計	DV01.7	システム方式設計（Webサイト）	DV01.7.3	システム方式設計の文書化とレビュー															
DV01	システム要件定義・方式設計	DV01.8	開発準備	DV01.8.1	開発手法の決定と開発プロセスの定義														○	○
DV01	システム要件定義・方式設計	DV01.8	開発準備	DV01.8.2	開発環境の準備														○	○
DV01	システム要件定義・方式設計	DV01.9	開発準備（アジャイル）	DV01.9.1	開発手法の決定と開発プロセスの定義															
DV01	システム要件定義・方式設計	DV01.9	開発準備（アジャイル）	DV01.9.2	開発環境の準備															
DV01	システム要件定義・方式設計	DV01.9	開発準備（アジャイル）	DV01.9.3	アジャイル開発の準備															
DV02	運用設計	DV02.1	システム運用設計	DV02.1.1	方針と基準の策定															
DV02	運用設計	DV02.1	システム運用設計	DV02.1.2	システム運用設計とレビュー			○											○	○
DV02	運用設計	DV02.2	ITサービス設計	DV02.2.1	運用・保守サービスの設計															
DV02	運用設計	DV02.3	Webサイト運用設計	DV02.3.1	Webサイトの運用設計															
DV03	移行設計	DV03.1	移行設計	DV03.1.1	移行の要件と方針の明確化														○	○
DV03	移行設計	DV03.1	移行設計	DV03.1.2	移行対象の明確化														○	○
DV03	移行設計	DV03.1	移行設計	DV03.1.3	移行テスト計画の作成														○	○
DV03	移行設計	DV03.1	移行設計	DV03.1.4	移行のスケジュールと体制の明確化														○	○
DV04	基盤システム構築	DV04.1	基盤システム設計（共通）	DV04.1.1	全体設計（基本設計）			○											○	○
DV04	基盤システム構築	DV04.2	基盤システム設計（プラットフォーム）	DV04.2.1	プラットフォーム設計														○	○
DV04	基盤システム構築	DV04.3	基盤システム設計（データベース）	DV04.3.1	物理データベース設計														○	○
DV04	基盤システム構築	DV04.3	基盤システム設計（データベース）	DV04.3.2	データベースの運用管理・保守の設計														○	○
DV04	基盤システム構築	DV04.4	基盤システム設計（ネットワーク）	DV04.4.1	ネットワークシステムの設計														○	○
DV04	基盤システム構築	DV04.4	基盤システム設計（ネットワーク）	DV04.4.2	ネットワークの運用管理・保守の設計														○	○
DV04	基盤システム構築	DV04.5	基盤システム設計（システム管理）	DV04.5.1	運用管理システムの設計														○	○
DV04	基盤システム構築	DV04.6	基盤システム設計（情報セキュリティ）	DV04.6.1	セキュリティの設計		○	○			○			○					○	○
DV04	基盤システム構築	DV04.7	基盤システム構築・テスト（プラットフォーム）	DV04.7.1	プラットフォームの構築														○	○
DV04	基盤システム構築	DV04.7	基盤システム構築・テスト（プラットフォーム）	DV04.7.2	テストの計画と実施														○	○
DV04	基盤システム構築	DV04.8	基盤システム構築・テスト（データベース）	DV04.8.1	データベースの構築														○	○
DV04	基盤システム構築	DV04.8	基盤システム構築・テスト（データベース）	DV04.8.2	テストの計画と実施														○	○
DV04	基盤システム構築	DV04.9	基盤システム構築・テスト（ネットワーク）	DV04.9.1	ネットワークの構築														○	○
DV04	基盤システム構築	DV04.9	基盤システム構築・テスト（ネットワーク）	DV04.9.2	テストの計画と実施														○	○
DV04	基盤システム構築	DV04.10	基盤システム構築・テスト（システム管理）	DV04.10.1	運用管理システムの構築														○	○
DV04	基盤システム構築	DV04.10	基盤システム構築・テスト（システム管理）	DV04.10.2	テストの計画と実施														○	○
DV04	基盤システム構築	DV04.11	基盤システム構築・テスト（情報セキュリティ）	DV04.11.1	セキュリティの実装			○			○								○	○
DV04	基盤システム構築	DV04.11	基盤システム構築・テスト（情報セキュリティ）	DV04.11.2	テスト計画と実施			○			○								○	○
DV05	アプリケーションシステム開発	DV05.1	ソフトウェア要件定義	DV05.1.1	機能要件と非機能要件の定義															
DV05	アプリケーションシステム開発	DV05.1	ソフトウェア要件定義	DV05.1.2	インタフェース要件の定義															
DV05	アプリケーションシステム開発	DV05.1	ソフトウェア要件定義	DV05.1.3	概念データモデルの作成															
DV05	アプリケーションシステム開発	DV05.1	ソフトウェア要件定義	DV05.1.4	ソフトウェア要件の評価															
DV05	アプリケーションシステム開発	DV05.1	ソフトウェア要件定義	DV05.1.5	パッケージ利用時のフィット&ギャップ分析															
DV05	アプリケーションシステム開発	DV05.2	ソフトウェア方式設計	DV05.2.1	ソフトウェアコンポーネントの方式設計															
DV05	アプリケーションシステム開発	DV05.2	ソフトウェア方式設計	DV05.2.2	インタフェースの方式設計															

タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）														ITSS+標準 ／iCD	ITSPベシャリスト（セキュリティ）
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査			
DV05	アプリケーションシステム開発	DV05.2	ソフトウェア方式設計	DV05.2.3	論理データベース設計（論理データモデルの作成）																
DV05	アプリケーションシステム開発	DV05.2	ソフトウェア方式設計	DV05.2.4	コード設計																
DV05	アプリケーションシステム開発	DV05.2	ソフトウェア方式設計	DV05.2.5	データサービスを活用した設計																
DV05	アプリケーションシステム開発	DV05.2	ソフトウェア方式設計	DV05.2.6	パッケージのカスタマイズ方針の決定																
DV05	アプリケーションシステム開発	DV05.3	開発環境構築	DV05.3.1	開発環境構築計画の立案																
DV05	アプリケーションシステム開発	DV05.3	開発環境構築	DV05.3.2	開発環境の構築と維持																
DV05	アプリケーションシステム開発	DV05.4	アプリケーション共通基盤設計・構築	DV05.4.1	アプリケーション共通基盤の設計															○	
DV05	アプリケーションシステム開発	DV05.4	アプリケーション共通基盤設計・構築	DV05.4.2	アプリケーション共通基盤の構築・テスト															○	
DV05	アプリケーションシステム開発	DV05.4	アプリケーション共通基盤設計・構築	DV05.4.3	アプリケーション構築の支援															○	
DV05	アプリケーションシステム開発	DV05.5	業務プロセス設計	DV05.5.1	業務プロセスの設計																
DV05	アプリケーションシステム開発	DV05.6	ソフトウェア詳細設計	DV05.6.1	ソフトウェアコンポーネント設計（機能分割・構造化）																
DV05	アプリケーションシステム開発	DV05.6	ソフトウェア詳細設計	DV05.6.2	入出力詳細設計																
DV05	アプリケーションシステム開発	DV05.6	ソフトウェア詳細設計	DV05.6.3	パッケージカスタマイズ・アドオン設計																
DV05	アプリケーションシステム開発	DV05.6	ソフトウェア詳細設計	DV05.6.4	データサービスの活用																
DV05	アプリケーションシステム開発	DV05.7	ソフトウェアコード作成・単体テスト	DV05.7.1	プログラム構造設計（モジュール分割・モジュール設計）																
DV05	アプリケーションシステム開発	DV05.7	ソフトウェアコード作成・単体テスト	DV05.7.2	単体テスト仕様作成																
DV05	アプリケーションシステム開発	DV05.7	ソフトウェアコード作成・単体テスト	DV05.7.3	プログラミング																
DV05	アプリケーションシステム開発	DV05.7	ソフトウェアコード作成・単体テスト	DV05.7.4	単体テストの実施と評価																
DV05	アプリケーションシステム開発	DV05.8	ソフトウェア結合テスト	DV05.8.1	結合テスト仕様作成																
DV05	アプリケーションシステム開発	DV05.8	ソフトウェア結合テスト	DV05.8.2	ソフトウェア結合																
DV05	アプリケーションシステム開発	DV05.8	ソフトウェア結合テスト	DV05.8.3	結合テストの実施と評価																
DV06	ソフトウェア製品開発	DV06.1	ソフトウェア要件定義	DV06.1.1	機能要件と非機能要件の定義																
DV06	ソフトウェア製品開発	DV06.1	ソフトウェア要件定義	DV06.1.2	インタフェース要件の定義																
DV06	ソフトウェア製品開発	DV06.1	ソフトウェア要件定義	DV06.1.3	概念データモデルの作成																
DV06	ソフトウェア製品開発	DV06.1	ソフトウェア要件定義	DV06.1.4	ソフトウェア要件の評価																
DV06	ソフトウェア製品開発	DV06.2	ソフトウェア方式設計	DV06.2.1	ソフトウェアコンポーネントの方式設計																
DV06	ソフトウェア製品開発	DV06.2	ソフトウェア方式設計	DV06.2.2	インタフェースの方式設計																
DV06	ソフトウェア製品開発	DV06.2	ソフトウェア方式設計	DV06.2.3	論理データベース設計（論理データモデルの作成）																
DV06	ソフトウェア製品開発	DV06.2	ソフトウェア方式設計	DV06.2.4	コード設計																
DV06	ソフトウェア製品開発	DV06.2	ソフトウェア方式設計	DV06.2.5	監視・通知・障害対策機能の設計																
DV06	ソフトウェア製品開発	DV06.3	開発環境構築	DV06.3.1	開発環境構築計画の立案																
DV06	ソフトウェア製品開発	DV06.3	開発環境構築	DV06.3.2	開発環境の構築と維持																
DV06	ソフトウェア製品開発	DV06.4	アプリケーション共通基盤設計・構築	DV06.4.1	アプリケーション共通基盤の設計																
DV06	ソフトウェア製品開発	DV06.4	アプリケーション共通基盤設計・構築	DV06.4.2	アプリケーション共通基盤の構築・テスト																
DV06	ソフトウェア製品開発	DV06.4	アプリケーション共通基盤設計・構築	DV06.4.3	アプリケーション構築の支援																
DV06	ソフトウェア製品開発	DV06.5	プロセス設計	DV06.5.1	プロセスの設計																
DV06	ソフトウェア製品開発	DV06.6	ソフトウェア詳細設計	DV06.6.1	ソフトウェアコンポーネント設計（機能分割・構造化）																
DV06	ソフトウェア製品開発	DV06.6	ソフトウェア詳細設計	DV06.6.2	入出力詳細設計																
DV06	ソフトウェア製品開発	DV06.7	ソフトウェアコード作成・単体テスト	DV06.7.1	プログラム構造設計（モジュール分割・モジュール設計）																
DV06	ソフトウェア製品開発	DV06.7	ソフトウェアコード作成・単体テスト	DV06.7.2	単体テスト仕様作成																
DV06	ソフトウェア製品開発	DV06.7	ソフトウェアコード作成・単体テスト	DV06.7.3	プログラミング																
DV06	ソフトウェア製品開発	DV06.7	ソフトウェアコード作成・単体テスト	DV06.7.4	単体テストの実施と評価																
DV06	ソフトウェア製品開発	DV06.8	ソフトウェア結合テスト	DV06.8.1	結合テスト仕様作成																
DV06	ソフトウェア製品開発	DV06.8	ソフトウェア結合テスト	DV06.8.2	ソフトウェア結合																
DV06	ソフトウェア製品開発	DV06.8	ソフトウェア結合テスト	DV06.8.3	結合テストの実施と評価																
DV06	ソフトウェア製品開発	DV06.9	システム適格性確認テスト	DV06.9.1	システム適格性確認テスト計画の作成																
DV06	ソフトウェア製品開発	DV06.9	システム適格性確認テスト	DV06.9.2	システム適格性確認テストの準備																
DV06	ソフトウェア製品開発	DV06.9	システム適格性確認テスト	DV06.9.3	システム適格性確認テストの実施と評価																
DV06	ソフトウェア製品開発	DV06.10	出荷	DV06.10.1	マニュアル作成とユーザ教育																
DV06	ソフトウェア製品開発	DV06.10	出荷	DV06.10.2	バージョン管理																
DV07	組込みソフトウェア開発	DV07.1	安全要件定義	DV07.1.1	対象プロダクトの仕様とシステム障害の検討																
DV07	組込みソフトウェア開発	DV07.1	安全要件定義	DV07.1.2	安全性実現のための要件の検討																
DV07	組込みソフトウェア開発	DV07.1	安全要件定義	DV07.1.3	安全要件仕様書の作成																
DV07	組込みソフトウェア開発	DV07.2	ソフトウェア要件定義	DV07.2.1	機能要件と非機能要件の定義																
DV07	組込みソフトウェア開発	DV07.2	ソフトウェア要件定義	DV07.2.2	インタフェース要件の定義																
DV07	組込みソフトウェア開発	DV07.2	ソフトウェア要件定義	DV07.2.3	ソフトウェア要件の評価																
DV07	組込みソフトウェア開発	DV07.3	ソフトウェア方式設計	DV07.3.1	ソフトウェアコンポーネントの方式設計																
DV07	組込みソフトウェア開発	DV07.3	ソフトウェア方式設計	DV07.3.2	インタフェースの方式設計																



タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）													ITスキル 標準／ICD
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査	
DV07	組み込みソフトウェア開発	DV07.4	開発環境構築	DV07.4.1	開発環境構築計画の立案														
DV07	組み込みソフトウェア開発	DV07.4	開発環境構築	DV07.4.2	開発環境の構築と維持														
DV07	組み込みソフトウェア開発	DV07.5	ソフトウェア詳細設計	DV07.5.1	ソフトウェアコンポーネント設計（機能分割・構造化）														
DV07	組み込みソフトウェア開発	DV07.5	ソフトウェア詳細設計	DV07.5.2	入出力詳細設計														
DV07	組み込みソフトウェア開発	DV07.6	ソフトウェアコード作成・単体テスト	DV07.6.1	プログラム構造設計（モジュール分割・モジュール設計）														
DV07	組み込みソフトウェア開発	DV07.6	ソフトウェアコード作成・単体テスト	DV07.6.2	単体テスト仕様作成														
DV07	組み込みソフトウェア開発	DV07.6	ソフトウェアコード作成・単体テスト	DV07.6.3	プログラミング														
DV07	組み込みソフトウェア開発	DV07.6	ソフトウェアコード作成・単体テスト	DV07.6.4	単体テストの実施と評価														
DV07	組み込みソフトウェア開発	DV07.7	ソフトウェア結合テスト	DV07.7.1	結合テスト仕様作成														
DV07	組み込みソフトウェア開発	DV07.7	ソフトウェア結合テスト	DV07.7.2	ソフトウェア結合														
DV07	組み込みソフトウェア開発	DV07.7	ソフトウェア結合テスト	DV07.7.3	結合テストの実施と評価														
DV07	組み込みソフトウェア開発	DV07.8	システム適格性確認テスト	DV07.8.1	システム適格性確認テスト計画の作成														
DV07	組み込みソフトウェア開発	DV07.8	システム適格性確認テスト	DV07.8.2	システム適格性確認テストの準備														
DV07	組み込みソフトウェア開発	DV07.8	システム適格性確認テスト	DV07.8.3	システム適格性確認テストの実施と評価														
DV07	組み込みソフトウェア開発	DV07.9	安全性テスト	DV07.9.1	安全性テストの準備						○								
DV07	組み込みソフトウェア開発	DV07.9	安全性テスト	DV07.9.2	安全性テストの実施と評価						○								
DV08	Webサイト開発	DV08.1	ソフトウェア要件定義	DV08.1.1	機能要件と非機能要件の定義														
DV08	Webサイト開発	DV08.1	ソフトウェア要件定義	DV08.1.2	Webコンテンツの要件定義														
DV08	Webサイト開発	DV08.1	ソフトウェア要件定義	DV08.1.3	Webサイトの要件定義														
DV08	Webサイト開発	DV08.1	ソフトウェア要件定義	DV08.1.4	プロトタイプ作成														
DV08	Webサイト開発	DV08.1	ソフトウェア要件定義	DV08.1.5	ソフトウェア要件の評価														
DV08	Webサイト開発	DV08.2	ソフトウェア方式設計	DV08.2.1	ソフトウェアコンポーネントの方式設計														
DV08	Webサイト開発	DV08.2	ソフトウェア方式設計	DV08.2.2	論理データベース設計（論理データモデルの作成）														
DV08	Webサイト開発	DV08.2	ソフトウェア方式設計	DV08.2.3	コード設計														
DV08	Webサイト開発	DV08.2	ソフトウェア方式設計	DV08.2.4	データサービスを活用した設計														
DV08	Webサイト開発	DV08.3	開発環境構築	DV08.3.1	開発環境構築計画の立案														
DV08	Webサイト開発	DV08.3	開発環境構築	DV08.3.2	開発環境の構築と維持														
DV08	Webサイト開発	DV08.4	ソフトウェア詳細設計	DV08.4.1	ソフトウェアコンポーネント設計（機能分割・構造化）														
DV08	Webサイト開発	DV08.4	ソフトウェア詳細設計	DV08.4.2	入出力詳細設計														
DV08	Webサイト開発	DV08.4	ソフトウェア詳細設計	DV08.4.3	データサービスの活用														
DV08	Webサイト開発	DV08.5	ソフトウェアコード作成・単体テスト	DV08.5.1	プログラム構造設計（モジュール分割・モジュール設計）														
DV08	Webサイト開発	DV08.5	ソフトウェアコード作成・単体テスト	DV08.5.2	単体テスト仕様作成														
DV08	Webサイト開発	DV08.5	ソフトウェアコード作成・単体テスト	DV08.5.3	プログラミング														
DV08	Webサイト開発	DV08.5	ソフトウェアコード作成・単体テスト	DV08.5.4	単体テストの実施と評価														
DV08	Webサイト開発	DV08.6	ソフトウェア結合テスト	DV08.6.1	結合テスト仕様作成														
DV08	Webサイト開発	DV08.6	ソフトウェア結合テスト	DV08.6.2	ソフトウェア結合														
DV08	Webサイト開発	DV08.6	ソフトウェア結合テスト	DV08.6.3	結合テストの実施と評価														
DV08	Webサイト開発	DV08.7	システム適格性確認テスト	DV08.7.1	システム適格性確認テスト計画の作成														
DV08	Webサイト開発	DV08.7	システム適格性確認テスト	DV08.7.2	システム適格性確認テストの準備														
DV08	Webサイト開発	DV08.7	システム適格性確認テスト	DV08.7.3	システム適格性確認テストの実施と評価														
DV09	システムテスト	DV09.1	システムテスト計画策定	DV09.1.1	システムテスト計画の作成														
DV09	システムテスト	DV09.1	システムテスト計画策定	DV09.1.2	システムテストの準備														
DV09	システムテスト	DV09.2	システムテスト実施	DV09.2.1	システム結合														
DV09	システムテスト	DV09.2	システムテスト実施	DV09.2.2	システムテストの実施と評価														
DV09	システムテスト	DV09.3	運用テスト	DV09.3.1	運用テストの準備														
DV09	システムテスト	DV09.3	運用テスト	DV09.3.2	運用テストの実施と評価														
DV10	セキュリティテスト	DV10.1	セキュリティテスト計画策定	DV10.1.1	セキュリティテスト計画の作成			○	○		○							○	
DV10	セキュリティテスト	DV10.1	セキュリティテスト計画策定	DV10.1.2	セキュリティテストの準備			○	○		○							○	
DV10	セキュリティテスト	DV10.2	セキュリティテスト実施	DV10.2.1	セキュリティテストの実施			○	○		○							○	
DV10	セキュリティテスト	DV10.2	セキュリティテスト実施	DV10.2.2	セキュリティテスト結果の対策実施			○			○		○						
DV11	移行・導入（システムリリース）	DV11.1	受入れテスト	DV11.1.1	受入れテスト計画の作成														
DV11	移行・導入（システムリリース）	DV11.1	受入れテスト	DV11.1.2	受入れテストの実施と評価														
DV11	移行・導入（システムリリース）	DV11.1	受入れテスト	DV11.1.3	受入れテストの支援						○								
DV11	移行・導入（システムリリース）	DV11.2	移行	DV11.2.1	移行の準備														
DV11	移行・導入（システムリリース）	DV11.2	移行	DV11.2.2	移行の実施														
DV11	移行・導入（システムリリース）	DV11.3	導入	DV11.3.1	教育準備と実施														
DV11	移行・導入（システムリリース）	DV11.3	導入	DV11.3.2	マニュアルの作成														
DV11	移行・導入（システムリリース）	DV11.3	導入	DV11.3.3	本稼働														

タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）													ITSS+標準／iCD	ITSS+標準（セキュリティ）
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティベンステイガーション	情報セキュリティ監査		
DV12	ソフトウェア保守	DV12.1	保守の方針と計画の策定	DV12.1.1	保守および更新・構成変更の方針策定															○
DV12	ソフトウェア保守	DV12.1	保守の方針と計画の策定	DV12.1.2	保守計画の策定															○
DV12	ソフトウェア保守	DV12.2	問題の調査と分析	DV12.2.1	問題の把握															○
DV12	ソフトウェア保守	DV12.2	問題の調査と分析	DV12.2.2	保守内容、影響範囲の調査と分析															○
DV13	ハードウェア・ソフトウェア製品導入	DV13.1	導入設計	DV13.1.1	ハードウェア導入設計															
DV13	ハードウェア・ソフトウェア製品導入	DV13.1	導入設計	DV13.1.2	ソフトウェア製品導入設計															
DV13	ハードウェア・ソフトウェア製品導入	DV13.2	ハードウェアの導入	DV13.2.1	ハードウェア導入作業の管理															
DV13	ハードウェア・ソフトウェア製品導入	DV13.2	ハードウェアの導入	DV13.2.2	ハードウェア導入作業（設置、据付）の実施															
DV13	ハードウェア・ソフトウェア製品導入	DV13.3	ソフトウェアの導入	DV13.3.1	ソフトウェア導入作業の管理															
DV13	ハードウェア・ソフトウェア製品導入	DV13.3	ソフトウェアの導入	DV13.3.2	ソフトウェア導入作業の実施															
DV14	ファシリティ設計・構築	DV14.1	ファシリティ設計	DV14.1.1	施工図の作成															
DV14	ファシリティ設計・構築	DV14.1	ファシリティ設計	DV14.1.2	施工計画書（要領書、計画書）の作成															
DV14	ファシリティ設計・構築	DV14.1	ファシリティ設計	DV14.1.3	試験・切替計画書の作成															
DV14	ファシリティ設計・構築	DV14.2	ファシリティ施工管理	DV14.2.1	施工準備															
DV14	ファシリティ設計・構築	DV14.2	ファシリティ施工管理	DV14.2.2	安全管理、作業管理、資材管理															
DV14	ファシリティ設計・構築	DV14.2	ファシリティ施工管理	DV14.2.3	施工後工程の管理															
DV14	ファシリティ設計・構築	DV14.3	ファシリティ施工実施	DV14.3.1	電気通信工事の実施															
DV14	ファシリティ設計・構築	DV14.3	ファシリティ施工実施	DV14.3.2	電気工事の実施															
DV14	ファシリティ設計・構築	DV14.3	ファシリティ施工実施	DV14.3.3	機器の設置															
DV14	ファシリティ設計・構築	DV14.3	ファシリティ施工実施	DV14.3.4	設備工事の実施															
DV14	ファシリティ設計・構築	DV14.3	ファシリティ施工実施	DV14.3.5	引き継ぎ															
DV15	プロジェクトマネジメント	DV15.1	プロジェクト立ち上げ	DV15.1.1	プロジェクト企画書の作成															
DV15	プロジェクトマネジメント	DV15.1	プロジェクト立ち上げ	DV15.1.2	プロジェクト企画書の申請と説明															
DV15	プロジェクトマネジメント	DV15.1	プロジェクト立ち上げ	DV15.1.3	プロジェクト企画書の完成															
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.1	スコープ計画の策定															
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.2	プロジェクト方針の決定															
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.3	スコープの定義															
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.4	スケジュール計画の策定															
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.5	資源計画の策定															
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.6	組織要員計画の策定															
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.7	調達計画の策定															
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.8	費用計画の策定															
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.9	品質保証計画の策定			○		○										
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.10	リスク管理計画の策定			○		○										
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.11	コミュニケーション計画の策定															
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	DV15.2.12	プロジェクト計画書の作成															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.1	プロジェクトの実行管理															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.2	プロジェクトの監視と追跡															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.3	問題管理															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.4	工程完了評価															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.5	プロジェクト状況の報告															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.6	進捗管理															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.7	資源管理															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.8	組織要員管理															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.9	調達管理															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.10	費用管理															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.11	品質管理			○		○										
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.12	リスク管理			○		○										
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.13	コミュニケーション管理															
DV15	プロジェクトマネジメント	DV15.3	プロジェクト追跡と実行管理	DV15.3.14	変更管理															
DV15	プロジェクトマネジメント	DV15.4	プロジェクト終結	DV15.4.1	プロジェクト終結の確認															
DV15	プロジェクトマネジメント	DV15.4	プロジェクト終結	DV15.4.2	プロジェクトの完了報告															
DV15	プロジェクトマネジメント	DV15.4	プロジェクト終結	DV15.4.3	プロジェクトの完了評価															
DV15	プロジェクトマネジメント	DV15.5	プロジェクト個別の品質マネジメント	DV15.5.1	レビューのマネジメント															
DV15	プロジェクトマネジメント	DV15.5	プロジェクト個別の品質マネジメント	DV15.5.2	テストのマネジメント															
DV15	プロジェクトマネジメント	DV15.5	プロジェクト個別の品質マネジメント	DV15.5.3	品質分析・評価のマネジメント															
US01	サービスデスク	US01.1	IT活用	US01.1.1	個別ITシステム活用促進															○
US01	サービスデスク	US01.1	IT活用	US01.1.2	個別評価とフィードバック															○

タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）													ITSS+標準／iCD	ITSS+標準（セキュリティ）
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査		
US01	サービスデスク	US01.1	IT利活用	US01.1.3	全体のIT活用能力底上げ															○
				US01.1.4	活用シナジーの促進															○
																				○
		US01.2	システム利用者対応	US01.2.1	業務運用															○
				US01.2.2	ユーザ教育と支援															○
				US01.2.3	インシデント管理															○
US01	サービスデスク	US01.3	顧客統括管理	US01.3.1	情報管理とコミュニケーション															
				US01.3.2	クレーム対応処理															
US02	IT運用コントロール	US02.1	IT運用管理	US02.1.1	ユーザ管理															○
				US02.1.2	オペレーション管理															○
		US02.2	情報セキュリティ管理	US02.2.1	情報セキュリティの運用					○			○	◎	○					○
				US02.2.2	情報セキュリティの評価と検証					○	◎									○
US03	システム運用管理	US03.1	障害管理	US03.1.1	障害対応															○
				US03.1.2	障害記録・再発防止															○
		US03.2	問題管理	US03.2.1	問題コントロールの開始															○
				US03.2.2	エラーコントロール															○
		US03.3	性能管理	US03.3.1	パフォーマンスとキャパシティの管理															○
		US03.4	変更管理	US03.4.1	変更要求の受付と記録															○
				US03.4.2	変更の実施															○
				US03.4.3	変更の評価						○									○
				US03.4.4	変更のレビューとクローズ															○
		US03.5	構成管理	US03.5.1	構成管理の計画策定と設計															○
				US03.5.2	構成管理の実施															○
		US03.6	資源管理	US03.6.1	ハードウェアの管理															○
				US03.6.2	ソフトウェアの管理															○
				US03.6.3	データの管理															○
				US03.6.4	ネットワーク資源の管理															○
		US03.7	リリース管理	US03.7.1	リリースの計画、準備と実施															○
				US03.7.2	妥当性確認とテスト						○									○
		US03.8	セキュリティ障害管理	US03.8.1	事故の検知							○		◎	◎					○
				US03.8.2	事故の初動処理							○		○	◎					○
				US03.8.3	事故の分析						○		◎	◎	◎	◎		○		○
				US03.8.4	事故からの復旧							○	○	◎	◎					○
				US03.8.5	再発防止策の実施						◎	○	○	○	◎					○
				US03.8.6	セキュリティの評価						◎				○					○
		US03.9	障害対応・保守支援	US03.9.1	問題発生時のコントロール（問題・障害管理）								◎							
				US03.9.2	障害発生時の対応（一次障害対応）															
				US03.9.3	重大障害発生時の対応（二次障害対応、復旧対応）															
				US03.9.4	障害の根治（製品の対応）															
		US03.10	予防保守	US03.10.1	ハードウェアの予防保守															
				US03.10.2	ソフトウェアの予防保守															
US04	Webサイト運用管理	US04.1	利用者向けサービス運用管理	US04.1.1	キャンペーン管理															
				US04.1.2	メール配信管理															
		US04.2	Webサービス運用管理	US04.2.1	Webコンテンツの運用管理															
				US04.2.2	Webコンテンツの制作と更新															
				US04.2.3	Webマーケティング施策の支援															
				US04.2.4	Webコンテンツ技術サポート															
US05	ファシリティ運用管理	US05.1	ファシリティ運用・保守	US05.1.1	保守計画の策定															
				US05.1.2	障害対応															
				US05.1.3	定期点検（予防保全、法定点検）の実施															
				US05.1.4	業務改善管理															
				US05.1.5	運用管理															
US06	サービスマネジメント	US06.1	サービス戦略管理	US06.1.1	ITサービス戦略管理															○
				US06.1.2	サービスポートフォリオ管理															○
				US06.1.3	課金管理															○
				US06.1.4	コスト管理															○
				US06.1.5	需要管理															○
				US06.1.6	事業関係管理															○

タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）													ITSS+標準 ／iCD	ITSS+標準 ／iCD （セキュリティ）
						情報リスクストラテジ	情報セキュリティデザイン	セキュリティ開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査		
US06	サービスマネジメント	US06.2	サービス設計と移行	US06.2.1	要員管理															○
				US06.2.2	サービスレベルの管理															○
				US06.2.3	サービス実施体制の管理															○
				US06.2.4	サービスカタログ管理															○
				US06.2.5	可用性管理															○
				US06.2.6	ITサービス継続管理															○
				US06.2.7	サプライヤ管理															○
				US06.2.8	ナレッジ管理															○
EV01	システム評価・改善	EV01.1	ITシステムの評価	EV01.1.1	ITシステム評価指標による検証															
				EV01.1.2	ITシステム評価報告の成案化															
				EV01.2	ITサービスの評価															
						EV01.2.1	評価目標の設定													
						EV01.2.2	ITサービス評価指標による検証													
						EV01.2.3	ITサービス評価報告の成案化													
						EV01.2.4	利用状況からの課題の発見と新たな価値の創出													
		EV01.3	Webサイトの評価	EV01.3.1	Webサイトの評価															
EV02	IT戦略評価・改善	EV02.1	IT戦略の評価	EV02.1.1	事業部門のIT化計画の評価															
				EV02.1.2	IT基盤計画の評価															
				EV02.1.3	全体計画の評価															
EV03	IT製品・サービス戦略評価・改善	EV03.1	IT製品・サービス戦略の評価	EV03.1.1	販売実績に基づく評価															
				EV03.1.2	調査・分析に基づく評価															
EV04	事業戦略評価支援・改善支援	EV04.1	事業戦略達成度の評価	EV04.1.1	モニタリング指標による検証															
				EV04.1.2	事業戦略評価報告の作成															
EV05	事業戦略評価・改善	EV05.1	事業戦略の評価	EV05.1.1	事業計画のモニタリング															
				EV05.1.2	事業戦略評価報告の作成															
EV06	資産管理・評価	EV06.1	資産管理規定の策定	EV06.1.1	資産管理方針と体制の策定															
				EV06.1.2	資産管理規定の作成と更新															
		EV06.2	資産管理プロセスの実施	EV06.2.1	資産管理規定に基づくプロセスの実施															
				EV06.2.2	情報機器の導入・更新計画の作成・実施・評価															
				EV06.2.3	廃棄計画の策定と実施															
MC01	ラインマネジメント	MC01.1	業務計画の策定	MC01.1.1	戦略と要求の確認															
				MC01.1.2	目標設定と周知															
				MC01.1.3	業務計画の具体化															
		MC01.2	業務計画の実行	MC01.2.1	業務の推進															
				MC01.2.2	業務計画遂行状況のモニタリング															
				MC01.2.3	業務計画の見直し															
		MC01.3	業務計画に基づく評価	MC01.3.1	自らが管理する組織の業務評価															
				MC01.3.2	個人の業務評価															
		MC01.4	リソース計画の策定	MC01.4.1	要員分析と計画の策定															
				MC01.4.2	スキル分析と計画の策定															
				MC01.4.3	情報分析と計画の策定															
				MC01.4.4	リスク分析と計画の策定															
		MC01.5	リソースの管理	MC01.5.1	メンバーとのコミュニケーション															
				MC01.5.2	メンバーの適正配置															
				MC01.5.3	メンバーの労務管理															
				MC01.5.4	諸規則・ルール の策定と遵守															
				MC01.5.5	組織の契約管理															
				MC01.5.6	リスク管理															
				MC01.5.7	問題対処															
				MC01.5.8	情報の管理と活用															
		MC01.6	メンバーの育成	MC01.6.1	育成計画の策定															
				MC01.6.2	育成計画の実行															
				MC01.6.3	育成計画に基づく評価															
MC02	事業継続マネジメント	MC02.1	事業継続計画の策定	MC02.1.1	事業継続計画策定の準備	○														
				MC02.1.2	対象事故・災害のリスク分析	○														
				MC02.1.3	事業継続計画の策定	○														
		MC02.2	事業継続計画の運用	MC02.2.1	関連部門への周知徹底															
				MC02.2.2	事業継続のためのリソースの確保	○														
		MC02.3	事業継続計画の見直し	MC02.3.1	事業継続計画の見直し	○														



タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）													ITスキル 標準／iCD
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査	
MC02	災害復旧マネジメント	MC02.4	災害復旧計画の策定	MC02.4.1	災害復旧計画の策定	○													
MC02	災害復旧マネジメント	MC02.4	災害復旧計画の策定	MC02.4.2	災害復旧計画の実現可能性の検証	○													
MC02	災害復旧マネジメント	MC02.4	災害復旧計画の策定	MC02.4.3	緊急時対応体制の確立	○													
MC02	災害復旧マネジメント	MC02.5	災害復旧計画の運用	MC02.5.1	関連部門への周知徹底														
MC02	災害復旧マネジメント	MC02.5	災害復旧計画の運用	MC02.5.2	災害発生時の予行・訓練の実施														
MC02	災害復旧マネジメント	MC02.6	災害復旧計画の見直し	MC02.6.1	災害復旧計画の見直し	○													
MC03	情報セキュリティマネジメント	MC03.1	情報セキュリティ戦略と方針の策定	MC03.1.1	基本戦略の策定	●				●	●								
MC03	情報セキュリティマネジメント	MC03.1	情報セキュリティ戦略と方針の策定	MC03.1.2	情報資産の評価	●		○		●	●								○
MC03	情報セキュリティマネジメント	MC03.1	情報セキュリティ戦略と方針の策定	MC03.1.3	脅威とリスクの識別	●		○	○	●	●			○					○
MC03	情報セキュリティマネジメント	MC03.1	情報セキュリティ戦略と方針の策定	MC03.1.4	リスクの評価	●		○		●	●			○					○
MC03	情報セキュリティマネジメント	MC03.1	情報セキュリティ戦略と方針の策定	MC03.1.5	セキュリティポリシーの策定	●		○		●	○								○
MC03	情報セキュリティマネジメント	MC03.2	情報セキュリティの運用	MC03.2.1	情報セキュリティガバナンス	○		○		●								○	○
MC03	情報セキュリティマネジメント	MC03.2	情報セキュリティの運用	MC03.2.2	情報セキュリティの周知と教育	○		○		●									○
MC03	情報セキュリティマネジメント	MC03.3	情報セキュリティの見直し	MC03.3.1	情報の収集と評価	○		○		●	○			●					○
MC03	情報セキュリティマネジメント	MC03.3	情報セキュリティの見直し	MC03.3.2	運用上の問題点整理と分析	○	●	○		●	○			○					○
MC03	情報セキュリティマネジメント	MC03.3	情報セキュリティの見直し	MC03.3.3	技術上の問題点整理と分析	○	●	○		●	○			●					○
MC03	情報セキュリティマネジメント	MC03.3	情報セキュリティの見直し	MC03.3.4	新たなリスクの整理と分析	○		○		●	●			●					○
MC03	情報セキュリティマネジメント	MC03.3	情報セキュリティの見直し	MC03.3.5	セキュリティポリシーの更新	○		○		●									○
MC04	品質マネジメント	MC04.1	品質管理のコントロール	MC04.1.1	品質マネジメントシステムの運用		●	○		●									
MC04	品質マネジメント	MC04.1	品質管理のコントロール	MC04.1.2	品質標準および品質管理実践基準の定義		●	○		○									
MC04	品質マネジメント	MC04.1	品質管理のコントロール	MC04.1.3	品質の測定、モニタリングおよび改善		●	○		○									
MC04	品質マネジメント	MC04.2	組織全体の品質マネジメント	MC04.2.1	検査のマネジメント		●	○											
MC05	契約管理	MC05.1	契約締結管理	MC05.1.1	委託／受託業務の内容と責任分担の明確化			○		●									
MC05	契約管理	MC05.1	契約締結管理	MC05.1.2	法的要件を満たした契約内容の作成			○		●									
MC05	契約管理	MC05.1	契約締結管理	MC05.1.3	契約の締結			○		●									
MC05	契約管理	MC05.1	契約締結管理	MC05.1.4	委託／受託契約ルール遵守			○		●									
MC05	契約管理	MC05.1	契約締結管理	MC05.1.5	供給／委託先の選択・交渉			○		●									
MC05	契約管理	MC05.2	契約変更管理	MC05.2.1	追加変更発生時の対応			○		●									
MC05	契約管理	MC05.2	契約変更管理	MC05.2.2	契約の変更要求の受付と影響分析			○		●									
MC05	契約管理	MC05.3	契約解除管理	MC05.2.3	契約変更の協議と締結			○		●									
MC06	コンプライアンス	MC06.1	管理方針と体制	MC06.1.1	法令および規範の管理体制確立	○													
MC06	コンプライアンス	MC06.1	管理方針と体制	MC06.1.2	遵守すべき法令および規範の識別	○													
MC06	コンプライアンス	MC06.1	管理方針と体制	MC06.1.3	情報倫理規定の策定	○													
MC06	コンプライアンス	MC06.1	管理方針と体制	MC06.1.4	個人情報の保護	○													
MC06	コンプライアンス	MC06.1	管理方針と体制	MC06.1.5	知的財産権の保護	○													
MC06	コンプライアンス	MC06.1	管理方針と体制	MC06.1.6	外部への情報提供	○						○							
MC06	コンプライアンス	MC06.2	実施と評価	MC06.2.1	教育と周知徹底	○													
MC06	コンプライアンス	MC06.2	実施と評価	MC06.2.2	遵守状況の評価と改善	○					●							●	
MC06	コンプライアンス	MC06.2	実施と評価	MC06.2.3	外部要件に対するコンプライアンスの保証	○													
MC07	人的資源管理	MC07.1	人材戦略の策定	MC07.1.1	人材育成施策・体制の維持														
MC07	人的資源管理	MC07.1	人材戦略の策定	MC07.1.2	人的資源の把握														
MC07	人的資源管理	MC07.2	人材戦略の運用	MC07.2.1	人材育成・教育の運営・実行														
MC07	人的資源管理	MC07.3	人材戦略の評価と分析	MC07.3.1	人材育成・教育の評価・分析														
MC07	人的資源管理	MC07.4	研修	MC07.4.1	研修の企画														
MC07	人的資源管理	MC07.4	研修	MC07.4.2	研修コンテンツの開発														
MC07	人的資源管理	MC07.4	研修	MC07.4.3	研修の実施														
MC07	人的資源管理	MC07.4	研修	MC07.4.4	研修の評価														
MC07	人的資源管理	MC07.5	ナレッジマネジメント	MC07.5.1	知的資産の管理方針策定と体制の確立														
MC07	人的資源管理	MC07.5	ナレッジマネジメント	MC07.5.2	ナレッジ管理システムの構築と運用														
MC07	人的資源管理	MC07.6	健康管理	MC07.6.1	健康管理を考慮した作業環境の提供														
MC07	人的資源管理	MC07.6	健康管理	MC07.6.2	健康診断とメンタルヘルスケア														
MC07	人的資源管理	MC07.7	人事・労務管理	MC07.7.1	要員の責任および権限の定義														
MC07	人的資源管理	MC07.7	人事・労務管理	MC07.7.2	要員の責任および権限の随時見直し														
MC07	人的資源管理	MC07.7	人事・労務管理	MC07.7.3	要員の責任および権限の周知徹底														
MC07	人的資源管理	MC07.7	人事・労務管理	MC07.7.4	要員の業績評価														
MC07	人的資源管理	MC07.7	人事・労務管理	MC07.7.5	適切な要員配置														
MC07	人的資源管理	MC07.7	人事・労務管理	MC07.7.6	適切な人材の確保														
MC07	人的資源管理	MC07.7	人事・労務管理	MC07.7.7	要員の交替時の留意														

タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）														ITスキル標準／ICD	ITスペシャリスト（セキュリティ）
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査			
MC08	内部統制状況のモニタリング	MC08.1	実行責任者によるモニタリングと評価	MC08.1.1	IT成果のモニタリング																
MC08	内部統制状況のモニタリング	MC08.1	実行責任者によるモニタリングと評価	MC08.1.2	成果改善策の明確化と実施																
MC08	内部統制状況のモニタリング	MC08.1	実行責任者によるモニタリングと評価	MC08.1.3	内部統制のモニタリングと評価																
MC08	内部統制状況のモニタリング	MC08.2	ガバナンスによる評価	MC08.2.1	ITガバナンスの提供																
MC09	システム監査	MC09.1	システム監査計画の策定	MC09.1.1	基本計画書の作成														○		
MC09	システム監査	MC09.1	システム監査計画の策定	MC09.1.2	個別計画書の作成														○		
MC09	システム監査	MC09.2	システム監査の実施	MC09.2.1	予備調査														○		
MC09	システム監査	MC09.2	システム監査の実施	MC09.2.2	監査手続書の作成														○		
MC09	システム監査	MC09.2	システム監査の実施	MC09.2.3	本調査														○		
MC09	システム監査	MC09.2	システム監査の実施	MC09.2.4	実施結果の記録（監査調査の作成）														○		
MC09	システム監査	MC09.2	システム監査の実施	MC09.2.5	監査報告書案の作成														○		
MC09	システム監査	MC09.3	システム監査結果の報告	MC09.3.1	監査報告の実施														○		
MC09	システム監査	MC09.3	システム監査結果の報告	MC09.3.2	フォローアップの実施														○		
MC09	システム監査	MC09.3	システム監査結果の報告	MC09.3.3	年次監査報告書の作成														○		
MC09	システム監査	MC09.4	システム監査対応	MC09.4.1	監査実施対応														○		
CM01	マーケティング・セールス	CM01.1	販売戦略の策定	CM01.1.1	ソリューションモデルの開発																
CM01	マーケティング・セールス	CM01.1	販売戦略の策定	CM01.1.2	製品・サービス導入事例の作成																
CM01	マーケティング・セールス	CM01.2	プロモーションの計画と実施	CM01.2.1	プロモーション戦略の策定																
CM01	マーケティング・セールス	CM01.2	プロモーションの計画と実施	CM01.2.2	プロモーション活動の実施と評価																
CM01	マーケティング・セールス	CM01.3	販売チャネル戦略の策定	CM01.3.1	流通チャネルの選択																
CM01	マーケティング・セールス	CM01.3	販売チャネル戦略の策定	CM01.3.2	流通チャネルを通じたセールス実行管理																
CM01	マーケティング・セールス	CM01.4	販売機会の創出	CM01.4.1	セグメンテーションとターゲットの選択																
CM01	マーケティング・セールス	CM01.4	販売機会の創出	CM01.4.2	顧客データベースやCRMを活用した販売																
CM01	マーケティング・セールス	CM01.5	アカウント戦略の策定	CM01.5.1	顧客分析																
CM01	マーケティング・セールス	CM01.5	アカウント戦略の策定	CM01.5.2	仮説の設定																
CM01	マーケティング・セールス	CM01.6	ソリューションの企画	CM01.6.1	顧客の状況把握と課題分析																
CM01	マーケティング・セールス	CM01.6	ソリューションの企画	CM01.6.2	顧客の課題とソリューションビジョンの共有																
CM01	マーケティング・セールス	CM01.6	ソリューションの企画	CM01.6.3	現行システムの把握と分析																
CM01	マーケティング・セールス	CM01.7	ソリューションの組立て	CM01.7.1	リスク計画の策定	○		○		○											
CM01	マーケティング・セールス	CM01.7	ソリューションの組立て	CM01.7.2	顧客のIT戦略の立案																
CM01	マーケティング・セールス	CM01.7	ソリューションの組立て	CM01.7.3	提案書の作成																
CM01	マーケティング・セールス	CM01.8	ソリューションの提案	CM01.8.1	革新的（最新）製品・サービス情報の提供																
CM01	マーケティング・セールス	CM01.8	ソリューションの提案	CM01.8.2	ソリューションの提案	○		○		○											
CM01	マーケティング・セールス	CM01.8	ソリューションの提案	CM01.8.3	最終提案内容の合意と契約締結																
CM01	マーケティング・セールス	CM01.9	顧客満足度管理	CM01.9.1	顧客満足度の調査と分析																
CM01	マーケティング・セールス	CM01.9	顧客満足度管理	CM01.9.2	中長期的な顧客支援																
CM02	再利用	CM02.1	再利用資産管理	CM02.1.1	再利用資産管理の準備		○														
CM02	再利用	CM02.1	再利用資産管理	CM02.1.2	再利用資産の保管と管理		○														
CM02	再利用	CM02.2	再利用施策管理	CM02.2.1	再利用施策の計画		○														
CM02	再利用	CM02.2	再利用施策管理	CM02.2.2	再利用施策の実施		○														
CM03	調達・委託	CM03.1	調達・委託先の選定	CM03.1.1	調達関連情報の収集																
CM03	調達・委託	CM03.1	調達・委託先の選定	CM03.1.2	調達・委託方法の検討																
CM03	調達・委託	CM03.1	調達・委託先の選定	CM03.1.3	提案評価基準の作成																
CM03	調達・委託	CM03.1	調達・委託先の選定	CM03.1.4	提案依頼書の作成と発行																
CM03	調達・委託	CM03.1	調達・委託先の選定	CM03.1.5	提案書の比較検討と委託先選定																
CM03	調達・委託	CM03.2	委託業務管理	CM03.2.1	セキュリティの調査			○		○									○		
CM03	調達・委託	CM03.2	委託業務管理	CM03.2.2	委託業務の開始・推進			○		○											
CM03	調達・委託	CM03.2	委託業務管理	CM03.2.3	進捗状況の把握と遅延、その他のリスク対策			○		○											
CM03	調達・委託	CM03.2	委託業務管理	CM03.2.4	成果物の検収			○		○											
CM03	調達・委託	CM03.2	委託業務管理	CM03.2.5	業務終了後のデータ、資料等の回収と廃棄確認			○		○											
CM03	調達・委託	CM03.2	委託業務管理	CM03.2.6	業務結果の分析と評価			○		○											
CM04	標準の策定・維持・管理	CM04.1	標準の策定	CM04.1.1	標準体系の策定																
CM04	標準の策定・維持・管理	CM04.1	標準の策定	CM04.1.2	ベースモデルの選定																
CM04	標準の策定・維持・管理	CM04.1	標準の策定	CM04.1.3	標準の作成																
CM04	標準の策定・維持・管理	CM04.2	標準の維持管理	CM04.2.1	実状調査		○	○													
CM04	標準の策定・維持・管理	CM04.2	標準の維持管理	CM04.2.2	標準の見直し		○	○													
CM05	新ビジネス・新技術の調査・分析と技	CM05.1	最新技術の研究・検証	CM05.1.1	調査対象の設定と情報収集	○								○							
CM05	新ビジネス・新技術の調査・分析と技	CM05.1	最新技術の研究・検証	CM05.1.2	最新技術の評価・検証	○								○							

タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）														ITスキル 標準／ICD
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティベンステイガーション	情報セキュリティ監査		
CM05	新ビジネス・新技術の調査・分析と検証	CM05.2	技術支援	CM05.2.1	技術伝承活動と技術支援															
CM06	データサイエンス	CM06.1	ビジネス目標の決定	CM06.1.1	ビジネス背景情報の収集															
CM06	データサイエンス	CM06.1	ビジネス目標の決定	CM06.1.2	ビジネス目標の決定															
CM06	データサイエンス	CM06.1	ビジネス目標の決定	CM06.1.3	ビジネス成功基準の設定															
CM06	データサイエンス	CM06.2	状況の評価	CM06.2.1	リソースの調査															
CM06	データサイエンス	CM06.2	状況の評価	CM06.2.2	要件、仮説、制約、リスクおよび用語の明確化															
CM06	データサイエンス	CM06.2	状況の評価	CM06.2.3	コストと利益の分析															
CM06	データサイエンス	CM06.3	目標の決定とプロジェクト計画の策定	CM06.3.1	プロジェクト目標の設定															
CM06	データサイエンス	CM06.3	目標の決定とプロジェクト計画の策定	CM06.3.2	プロジェクトの成功基準の設定															
CM06	データサイエンス	CM06.3	目標の決定とプロジェクト計画の策定	CM06.3.3	プロジェクト計画の策定															
CM06	データサイエンス	CM06.4	データの理解	CM06.4.1	初期データの収集															
CM06	データサイエンス	CM06.4	データの理解	CM06.4.2	データの説明															
CM06	データサイエンス	CM06.4	データの理解	CM06.4.3	データの探索															
CM06	データサイエンス	CM06.4	データの理解	CM06.4.4	データ品質の検証															
CM06	データサイエンス	CM06.5	データマイニングのためのデータの準備	CM06.5.1	データの選択															
CM06	データサイエンス	CM06.5	データマイニングのためのデータの準備	CM06.5.2	データのクリーニング															
CM06	データサイエンス	CM06.5	データマイニングのためのデータの準備	CM06.5.3	新規データの作成・統合・フォーマット															
CM06	データサイエンス	CM06.6	モデリング	CM06.6.1	モデリング手法の選択															
CM06	データサイエンス	CM06.6	モデリング	CM06.6.2	テスト設計															
CM06	データサイエンス	CM06.6	モデリング	CM06.6.3	モデルの構築															
CM06	データサイエンス	CM06.6	モデリング	CM06.6.4	モデルの評価															
CM06	データサイエンス	CM06.7	評価	CM06.7.1	結果の評価と次ステップの決定															
CM06	データサイエンス	CM06.7	評価	CM06.7.2	プロセスの見直し															
CM06	データサイエンス	CM06.8	結果とモデルの展開	CM06.8.1	展開のプランニング															
CM06	データサイエンス	CM06.8	結果とモデルの展開	CM06.8.2	監視と保守のプランニング															
CM06	データサイエンス	CM06.8	結果とモデルの展開	CM06.8.3	最終報告書の作成															
CM06	データサイエンス	CM06.8	結果とモデルの展開	CM06.8.4	最終プロジェクトレビューの実施															
CM06	データサイエンス	CM06.9	ビジネスでの活用と評価	CM06.9.1	ビジネスでの活用															
CM06	データサイエンス	CM06.9	ビジネスでの活用と評価	CM06.9.2	ビジネス成果の確認															
CM07	新たな価値創造による新規製品・サービス開発	CM07.1	疑似体験等を通した価値あるアイデアの発掘	CM07.1.1	実現を目指すアイデアの明確化															
CM07	新たな価値創造による新規製品・サービス開発	CM07.1	疑似体験等を通した価値あるアイデアの発掘	CM07.1.2	多様性に富んだチームビルディング															
CM07	新たな価値創造による新規製品・サービス開発	CM07.1	疑似体験等を通した価値あるアイデアの発掘	CM07.1.3	疑似体験等の実施															
CM07	新たな価値創造による新規製品・サービス開発	CM07.1	疑似体験等を通した価値あるアイデアの発掘	CM07.1.4	アイデアが持つ提供価値の確認															
CM07	新たな価値創造による新規製品・サービス開発	CM07.2	プロトタイピングを通した新規製品の検討	CM07.2.1	プロトタイピングによる提供価値の実証															
CM07	新たな価値創造による新規製品・サービス開発	CM07.2	プロトタイピングを通した新規製品の検討	CM07.2.2	新規製品・サービス化に向けた評価															
CM07	新たな価値創造による新規製品・サービス開発	CM07.3	新規製品・サービスの事業化計画立案	CM07.3.1	新規製品・サービスの事業化計画立案															
CM07	新たな価値創造による新規製品・サービス開発	CM07.4	ビジネス化の実証と新たな価値発見	CM07.4.1	新規製品・サービスの市場投入															
CM07	新たな価値創造による新規製品・サービス開発	CM07.4	ビジネス化の実証と新たな価値発見	CM07.4.2	ビジネス化の実証															
CM07	新たな価値創造による新規製品・サービス開発	CM07.4	ビジネス化の実証と新たな価値発見	CM07.4.3	新たな提供価値の発見															
SP01	営業業務	SP01.1	IT製品・サービス戦略評価・改善＞IT製品・サービス戦略の評価	SP01.1.1	調査・分析に基づく評価															
SP01	営業業務	SP01.2	マーケティング＞販売チャネル戦略の策定と実践	SP01.2.1	顧客分析															
SP01	営業業務	SP01.3	マーケティング＞アカウント戦略の実践	SP01.3.1	顧客状況の把握															
SP01	営業業務	SP01.3	マーケティング＞アカウント戦略の実践	SP01.3.2	顧客状況の資料化															
SP01	営業業務	SP01.3	マーケティング＞アカウント戦略の実践	SP01.3.3	仮説の設定															
SP01	営業業務	SP01.4	セールス活動＞プロモーションの計画と実施	SP01.4.1	メディアへのプロモーション															
SP01	営業業務	SP01.4	セールス活動＞プロモーションの計画と実施	SP01.4.2	フェア出展															

タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）													ITSS+標準／iCD	ITSS+標準 （セキュリティ）
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査		
SP01	営業業務	SP01.5	セールス活動＞販売機会の創出	SP01.5.1	セグメンテーションとターゲットの選択															
			セールス活動＞販売機会の創出	SP01.5.2	顧客との関係構築															
		SP01.6	セールス活動＞商談契機の前出	SP01.6.1	自社の顧客アピールとアポイント取得															
			セールス活動＞商談契機の前出	SP01.6.2	顧客に提供する話題づくり															
		SP01.7	セールス活動＞ソリューションの組立て	SP01.7.1	提案書の作成のための情報収集															
				SP01.7.2	提案書の作成															
				SP01.7.3	提案書の最終調整															
		SP01.8	セールス活動＞ソリューションの提案	SP01.8.1	事前ヒアリング															
				SP01.8.2	ネゴシエーション															
				SP01.8.3	提案（プレゼンテーション）															
				SP01.8.4	提案（デモンストレーションの準備）															
				SP01.8.5	提案（デモンストレーション）															
				SP01.8.6	提案後のフォロー															
		SP01.9	セールス活動＞SES（システム・エンジニアリング・サービス）	SP01.9.1	案件情報収集															
				SP01.9.2	提案準備															
				SP01.9.3	提案															
				SP01.9.4	合意															
		SP01.10	セールス活動＞営業事務	SP01.10.1	営業案件管理															
				SP01.10.2	営業成績管理															
				SP01.10.3	受注事前業務															
				SP01.10.4	受注管理業務															
		SP01.11	セールス活動＞顧客満足度管理	SP01.11.1	プロジェクト進捗管理・品質管理															
				SP01.11.2	要員・資材調達															
				SP01.11.3	中長期的な顧客支援															
				SP01.11.4	クレーム・障害時の対応															
				SP01.11.5	クレーム・障害時の対応（報告）															
		SP01.12	契約管理＞契約締結管理	SP01.12.1	口座開設															
				SP01.12.2	契約の締結															
				SP01.12.3	機密情報管理															
SP02	総務・人事・経理	SP02.1	経理＞日次経理業務	SP02.1.1	出金															
				SP02.1.2	支払い															
				SP02.1.3	現預金管理															
		SP02.2	経理＞月次決算業務	SP02.2.1	請求															
				SP02.2.2	会計処理															
				SP02.2.3	原価管理															
		SP02.3	経理＞経営数値管理	SP02.3.1	原価管理															
				SP02.3.2	計数分析															
				SP02.3.3	資金管理															
		SP02.4	財務＞債権・債務管理	SP02.4.1	債権・債務管理ルール策定															
				SP02.4.2	債権・債務管理ルール策定															
				SP02.4.3	債権・債務															
		SP02.5	財務＞決算業務	SP02.5.1	株主総会、取締役会対応															
				SP02.5.2	単体決算処理															
				SP02.5.3	連結決算処理															
				SP02.5.4	収益計上															
				SP02.5.5	資料棚卸															
		SP02.6	財務＞税務	SP02.6.1	タックスプランニング															
				SP02.6.2	税務申告															
				SP02.6.3	日常税務															
				SP02.6.4	税務調査対応															
		SP02.7	財務＞経営数値管理	SP02.7.1	事業計画立案支援															
				SP02.7.2	年度予算管理															
		SP02.8	ガバナンス（総務）＞対外ガバナンスの実行	SP02.8.1	法令順守対応															
				SP02.9.1	社内決裁対応															
		SP02.10	ガバナンス（総務）＞広報	SP02.10.1	広報の制作立案															
				SP02.10.2	広報物の制作															



タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）														ITSS+標準 ／ICD	ITスペシャリスト（セキュリティ）
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査			
SP02	総務・人事・経理	SP02.11	ガバナンス（総務）＞ファシリティマネジメント	SP02.11.1	職場環境の向上																
SP02	総務・人事・経理	SP02.12	ガバナンス（総務）＞庶務	SP02.12.1	地域貢献活動																
SP02	総務・人事・経理	SP02.12	ガバナンス（総務）＞庶務	SP02.12.2	社内交流																
SP02	総務・人事・経理	SP02.12	ガバナンス（総務）＞庶務	SP02.12.3	助成金管理																
SP02	総務・人事・経理	SP02.12	ガバナンス（総務）＞庶務	SP02.12.4	文書管理																
SP02	総務・人事・経理	SP02.12	ガバナンス（総務）＞庶務	SP02.12.5	秘書業務																
SP02	総務・人事・経理	SP02.12	ガバナンス（総務）＞庶務	SP02.12.6	証明書発行																
SP02	総務・人事・経理	SP02.13	ガバナンス（総務）＞危機管理	SP02.13.1	災害対応																
SP02	総務・人事・経理	SP02.13	ガバナンス（総務）＞危機管理	SP02.13.2	傷害・損害対応																
SP02	総務・人事・経理	SP02.13	ガバナンス（総務）＞危機管理	SP02.13.3	事故対応																
SP02	総務・人事・経理	SP02.13	ガバナンス（総務）＞危機管理	SP02.13.4	危機管理対応																
SP02	総務・人事・経理	SP02.14	ガバナンス（総務）＞安全管理	SP02.14.1	保険手続対応																
SP02	総務・人事・経理	SP02.15	ガバナンス（総務）＞情報資産管理	SP02.15.1	情報資産申請管理																
SP02	総務・人事・経理	SP02.15	ガバナンス（総務）＞情報資産管理	SP02.15.2	各種社内申請処理																
SP02	総務・人事・経理	SP02.16	ガバナンス（総務）＞情報セキュリティ事故対応	SP02.16.1	インシデント報告受付							◎	○		⊖						
SP02	総務・人事・経理	SP02.16	ガバナンス（総務）＞情報セキュリティ事故対応	SP02.16.2	対応状況確認							○	◎	○	○		○				
SP02	総務・人事・経理	SP02.16	ガバナンス（総務）＞情報セキュリティ事故対応	SP02.16.3	再発防止対策						◎		◎	○							
SP02	総務・人事・経理	SP02.16	ガバナンス（総務）＞情報セキュリティ事故対応	SP02.16.4	障害分析・改善						◎		◎	○							
SP02	総務・人事・経理	SP02.17	資産管理＞資産管理	SP02.17.1	棚卸資産管理																
SP02	総務・人事・経理	SP02.17	資産管理＞資産管理	SP02.17.2	固定資産管理																
SP02	総務・人事・経理	SP02.17	資産管理＞資産管理	SP02.17.3	リース資産管理																
SP02	総務・人事・経理	SP02.18	人事＞採用活動	SP02.18.1	学校への採用活動対応																
SP02	総務・人事・経理	SP02.18	人事＞採用活動	SP02.18.2	採用計画の策定と準備																
SP02	総務・人事・経理	SP02.18	人事＞採用活動	SP02.18.3	採用活動の実施																
SP02	総務・人事・経理	SP02.18	人事＞採用活動	SP02.18.4	雇用契約の実施																
SP02	総務・人事・経理	SP02.19	人事＞人材配置戦略	SP02.19.1	人員計画の策定																
SP02	総務・人事・経理	SP02.19	人事＞人材配置戦略	SP02.19.2	制度設計とリスクマネジメント																
SP02	総務・人事・経理	SP02.19	人事＞人材配置戦略	SP02.19.3	制度運用設計・管理																
SP02	総務・人事・経理	SP02.19	人事＞人材配置戦略	SP02.19.4	社内人事計画の実施																
SP02	総務・人事・経理	SP02.20	人事＞人材育成	SP02.20.1	教育・育成計画の策定																
SP02	総務・人事・経理	SP02.20	人事＞人材育成	SP02.20.2	内部教育と育成の実施																
SP02	総務・人事・経理	SP02.20	人事＞人材育成	SP02.20.3	外部研修の活用																
SP02	総務・人事・経理	SP02.20	人事＞人材育成	SP02.20.4	資格取得支援																
SP02	総務・人事・経理	SP02.21	人事＞労務管理	SP02.21.1	労働処遇運用																
SP02	総務・人事・経理	SP02.21	人事＞労務管理	SP02.21.2	給与管理対応																
SP02	総務・人事・経理	SP02.21	人事＞労務管理	SP02.21.3	労使関連対応																
SP02	総務・人事・経理	SP02.21	人事＞労務管理	SP02.21.4	安全衛生対応																
SP02	総務・人事・経理	SP02.22	リーガル（法務）＞法令順守	SP02.22.1	会計監査対応																
SP02	総務・人事・経理	SP02.23	リーガル（法務）＞法改正	SP02.23.1	法改正対応																
SP02	総務・人事・経理	SP02.24	リーガル（法務）＞契約書の作成と締結	SP02.24.1	相手先との契約内容の調整																
SP02	総務・人事・経理	SP02.24	リーガル（法務）＞契約書の作成と締結	SP02.24.2	契約書作成																
SP02	総務・人事・経理	SP02.24	リーガル（法務）＞契約書の作成と締結	SP02.24.3	契約締結																
SP02	総務・人事・経理	SP02.24	リーガル（法務）＞契約書の作成と締結	SP02.24.4	契約書の保管																
SP02	総務・人事・経理	SP02.25	リーガル（法務）＞ベンダーとのパートナー契約	SP02.25.1	ベンダーとのパートナー契約管理																
SP02	総務・人事・経理	SP02.26	外注管理＞外注発注の妥当性確認	SP02.26.1	外注申請のチェック																
SP02	総務・人事・経理	SP02.26	外注管理＞外注発注の妥当性確認	SP02.26.2	外注申請の決裁																
SP02	総務・人事・経理	SP02.27	外注管理＞外注先との契約交渉と契約書作成、締結	SP02.27.1	契約書作成																
SP02	総務・人事・経理	SP02.27	外注管理＞外注先との契約交渉と契約書作成、締結	SP02.27.2	契約締結																
SP02	総務・人事・経理	SP02.28	外注管理＞外注先からの納品受入管理	SP02.28.1	納品物検収																
SP02	総務・人事・経理	SP02.28	外注管理＞外注先からの納品受入管理	SP02.28.2	支払い処理																
SP02	総務・人事・経理	SP02.29	外注管理＞派遣要員の法的労務管理	SP02.29.1	協力会社派遣要員の法的労務管理																
SP02	総務・人事・経理	SP02.30	外注管理＞外注取引先の管理	SP02.30.1	取引先調査																
SP02	総務・人事・経理	SP02.30	外注管理＞外注取引先の管理	SP02.30.2	取引先評価																
SP02	総務・人事・経理	SP02.31	物品の購入管理＞購入・支払い管理	SP02.31.1	発注先選定																
SP02	総務・人事・経理	SP02.31	物品の購入管理＞購入・支払い管理	SP02.31.2	発注処理																
SP02	総務・人事・経理	SP02.31	物品の購入管理＞購入・支払い管理	SP02.31.3	検品、検収処理																
SP02	総務・人事・経理	SP02.31	物品の購入管理＞購入・支払い管理	SP02.31.4	支払い処理																
SP02	総務・人事・経理	SP02.32	物品の購入管理＞在庫管理	SP02.32.1	ソフトウェアライセンス管理																

タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）													ITスキル 標準／ICD
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査	
SP02	総務・人事・経理			SP02.32.2	物品管理														
SP02	総務・人事・経理	SP02.33	物品の購入管理＞廃棄処理	SP02.33.1	機器廃棄処理														
SP02	総務・人事・経理	SP02.34	物品の購入管理＞顧客所有物管理	SP02.34.1	入出庫管理														
SP02	総務・人事・経理	SP02.35	社内業務監査＞内部監査	SP02.35.1	監査計画													○	
SP02	総務・人事・経理	SP02.35	社内業務監査＞内部監査	SP02.35.2	監査実施													○	
SP02	総務・人事・経理	SP02.35	社内業務監査＞内部監査	SP02.35.3	監査結果分析と改善フォロー													○	
SP02	総務・人事・経理	SP02.36	社内業務監査＞外部審査	SP02.36.1	審査計画													○	
SP02	総務・人事・経理	SP02.36	社内業務監査＞外部審査	SP02.36.2	審査実施													○	
SP02	総務・人事・経理	SP02.36	社内業務監査＞外部審査	SP02.36.3	審査結果分析と改善フォロー													○	
SP02	総務・人事・経理	SP02.37	社内業務監査＞社内業務改善	SP02.37.1	社内業務改善活動の実施													○	
SP03	エデュケーション	SP03.1	研修の企画	SP03.1.1	前提条件、制約事項の把握														
SP03	エデュケーション	SP03.1	研修の企画	SP03.1.2	現状分析														
SP03	エデュケーション	SP03.1	研修の企画	SP03.1.3	研修の目的と目標の決定														
SP03	エデュケーション	SP03.1	研修の企画	SP03.1.4	内製、外製の決定														
SP03	エデュケーション	SP03.1	研修の企画	SP03.1.5	研修実施体制の決定														
SP03	エデュケーション	SP03.2	研修の設計	SP03.2.1	研修プランの策定														
SP03	エデュケーション	SP03.2	研修の設計	SP03.2.2	研修プランの評価と改善														
SP03	エデュケーション	SP03.2	研修の設計	SP03.2.3	科目の設計														
SP03	エデュケーション	SP03.2	研修の設計	SP03.2.4	研修環境の設計														
SP03	エデュケーション	SP03.3	研修教材の開発	SP03.3.1	研修教材の開発計画策定														
SP03	エデュケーション	SP03.3	研修教材の開発	SP03.3.2	研修教材の開発														
SP03	エデュケーション	SP03.3	研修教材の開発	SP03.3.3	研修教材の検証														
SP03	エデュケーション	SP03.4	研修の準備	SP03.4.1	研修講師の準備														
SP03	エデュケーション	SP03.4	研修の準備	SP03.4.2	運用担当者の準備														
SP03	エデュケーション	SP03.5	研修の実施	SP03.5.1	研修の開催（オープニング）														
SP03	エデュケーション	SP03.5	研修の実施	SP03.5.2	研修の展開（講義の実施）														
SP03	エデュケーション	SP03.5	研修の実施	SP03.5.3	研修の終結（クロージング）														
SP03	エデュケーション	SP03.5	研修の実施	SP03.5.4	研修受講者の評価														
SP03	エデュケーション	SP03.6	研修の評価と改善	SP03.6.1	研修の評価														
SP03	エデュケーション	SP03.6	研修の評価と改善	SP03.6.2	研修の改善														
追加タスク項目																			
DV01	システム要件定義・方式設計	DV01.4	システム方式設計	新規追加	セキュリティの観点からの設計	○	◎			○	○								
DV02	運用設計	新規追加	セキュリティ運用設計	新規追加	通常時におけるセキュリティ運用の設計	◎				◎			○		○				
				新規追加	インシデント発生時におけるセキュリティ運用の設計	◎				◎			◎		○				
DV10	セキュリティテスト	新規追加	第三者によるシステムセキュリティの確認	新規追加	第三者による確認に関する計画の作成			○											
				新規追加	第三者による確認の実施			○	◎										
				新規追加	第三者による確認結果の検討及び反映			○											
DV15	プロジェクトマネジメント	DV15.2	プロジェクト計画策定	新規追加	プロジェクトについてのセキュリティ管理計画の策定			○											
				新規追加	要員についてのセキュリティ管理計画の策定			○											
US01	サービスデスク	US01.1	IT利活用	新規追加	セキュリティ適合確認の実施	◎				◎	◎								
		US01.2	システム利用者対応	新規追加	セキュリティ適合確認の実施	◎				◎	◎								
		US01.3	顧客統括管理	新規追加	セキュリティ適合確認の実施	◎				◎	◎								
EV01	システム評価・改善	新規追加	セキュリティの評価	新規追加	セキュリティ計画に照らした評価	○				◎	◎								
				新規追加	評価結果を踏まえた改善の実施	○				◎	◎								
MC05	契約管理	MC05.1	契約締結管理	新規追加	セキュリティに関する契約内容の交渉・確認	◎				○									
新規追加	セキュリティ監査	新規追加	セキュリティ監査計画の策定	新規追加	基本計画書の作成	○				○								◎	
MC09	セキュリティ監査	MC09.1	セキュリティ監査計画の策定	新規追加	個別計画書の作成	○				○								◎	
MC09	セキュリティ監査	新規追加	セキュリティ監査の実施	新規追加	予備調査													◎	
MC09	セキュリティ監査	MC09.2	セキュリティ監査の実施	新規追加	監査手続書の作成													◎	
MC09	セキュリティ監査	MC09.2	セキュリティ監査の実施	新規追加	本調査													◎	
MC09	セキュリティ監査	MC09.2	セキュリティ監査の実施	新規追加	実施結果の記録（監査調査の作成）													◎	
MC09	セキュリティ監査	MC09.2	セキュリティ監査の実施	新規追加	監査報告書案の作成													◎	
MC09	セキュリティ監査	新規追加	セキュリティ監査結果の報告	新規追加	監査報告の実施													◎	
MC09	セキュリティ監査	MC09.3	セキュリティ監査結果の報告	新規追加	フォローアップの実施													◎	
MC09	セキュリティ監査	MC09.3	セキュリティ監査結果の報告	新規追加	年次監査報告書の作成													◎	
MC09	セキュリティ監査	新規追加	セキュリティ監査対応	新規追加	監査実施対応	○				○								◎	

タスク 大分類 コード	タスク大分類	タスク 中分類 コード	タスク中分類	タスク 小分類 コード	タスク小分類	ITSS+（セキュリティ領域）													ITスキル標準／ICD
						情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション		情報セキュリティ監査
CM01	マーケティング・セールス	CM01.7	ソリューションの組立て	新規追加	セキュリティ適合確認の実施	○					◎								
CM02	再利用	CM02.1	再利用資産管理	新規追加	セキュリティ適合確認の実施					◎	◎								
		CM02.2	再利用施策管理	新規追加	セキュリティ適合確認の実施					◎	◎								
CM04	標準の策定・維持・管理	CM04.1	標準の策定	新規追加	セキュリティの観点からの検討			○			○			○					
CM06	データサイエンス	CM06.2	状況の評価	新規追加	セキュリティとプライバシー保護の観点からの分析	○	○				◎								
CM07	新たな価値創造による新規製品・サービス開発	CM07.2	プロトタイピングを通した新規製品の検討	新規追加	セキュリティの観点からの評価	○	○				○								