経済産業省委託事業

平成 24 年度情報セキュリティ対策推進事業

(情報セキュリティ人材の育成指標等の策定事業)

事業報告書

～ 第３編 ～

情報セキュリティ関連タスク一覧

平成 25 年 3 月

みずほ情報総研株式会社

～ 第３編 ～ 目次

情報セキュリティ関連タスク一覧

～ 事業報告書の構成 ～

＜第１編＞　本編
＜第２編＞　３スキル標準見直し案
＜第３編＞　情報セキュリティ関連タスク一覧
＜第４編＞　情報セキュリティに関する認定・資格調査結果
＜第５編＞　情報セキュリティ人材のモデルキャリア（冊子）

第1章　情報セキュリティ関連タスク一覧

情報セキュリティに関するタスクとスキル項目の一覧

凡例：
- 情報セキュリティ分野のタスクで、CCSFで定義されているもの
- 情報セキュリティに近い分野（事業継続、コンプライアンス、システム監査）のタスクで、CCSFで定義されているもの
- CCSFで定義されていないが、人材像定義のために必要なタスク

大分類	中分類	小分類	スキルコード	スキル項目	根拠	見直しの内容
事業戦略>情報セキュリティ戦略	情報セキュリティ戦略の策定	最新技術動向の調査・分析	(仮)S-1.4-1-1-01	システムのセキュリティやリスクに関する技術動向調査を行い、その情報をIT戦略立案に活用することができる	UISS作業委員会	中分類の追加
事業戦略>情報セキュリティ戦略	情報セキュリティ戦略の策定	情報セキュリティ戦略実行体制の確立	(仮)S-1.4-1-2-01	情報セキュリティ戦略を実施するに当たって、その実行体制を確立することができる	UISS作業委員会	中分類の追加
事業戦略>情報セキュリティ戦略	情報セキュリティ戦略の策定	EAの推進（EAプロセスの統括）	(仮)S-1.4-1-3-01	経営戦略に準じた組織全体の改善サイクルとなるよう各EA（BA,DA,AA,TA）開発組織を統轄することができる	UISS作業委員会	中分類の追加
事業戦略>情報セキュリティ戦略	情報セキュリティ戦略の策定	委託先管理	(仮)S-1.4-1-4-01	セキュリティ業務全体をみたときに、その業務の一部を委託をすべきなのかを判断、決定する	UISS作業委員会	中分類の追加
IT戦略実行マネジメント	IT戦略実現上のリスクへの対応	リスクの管理	S-3-3-1-01	部門戦略におけるプログラムに影響を与える変化を分析・評価できる		
IT戦略実行マネジメント	IT戦略実現上のリスクへの対応	対策策定	S-3-3-2-01	部門戦略におけるプログラム全般のリスクに対して、対応策・防止策を立案することができる		
IT戦略実行マネジメント	IT戦略実現上のリスクへの対応	調整等対応策の実施	S-3-3-3-01	複数のプロジェクト間、保守運用間で、優先順位や各種リソース（人、時間、予算など）配分などの調整をすることができる		
標準の維持・管理と品質管理	品質保証	品質管理基準の設定	S-4-3-1-01	品質保証フレームワークの策定ができる		
標準の維持・管理と品質管理	品質保証	品質統制プロセスの運営	S-4-3-2-01	標準、品質保証フレームワーク（品質管理基準）への準拠性の評価と例外の妥当性を判断することができる		
標準の維持・管理と品質管理	品質保証	品質統制プロセスの運営	S-4-3-2-02	品質統制プロセスを推進する組織体制を構築・維持することができる		
標準の維持・管理と品質管理	品質保証	品質統制プロセスの運営	S-4-3-2-03	品質統制プロセスを担保するための公的基準を含む評価基準、測定方法を定め、遵守するための啓蒙活動、教育を推進することができる		
標準の維持・管理と品質管理	品質保証	評価のフィードバック	S-4-3-3-01	品質統制プロセス結果を分析し、準拠状況と原因を集計し、非準拠の要因を特定することができる		
標準の維持・管理と品質管理	標準の維持管理	標準化した妥当性確認（テスト）の実施管理	S-4-4-5-01	標準化された品質管理基準に準じて、テストに関する規定（テスト基準、判定基準）を設定・改訂することができる		
標準の維持・管理と品質管理	標準の維持管理	標準化したレビュープロセスの実施管理	S-4-4-6-01	標準化された品質管理基準に準じて、各プロセス・タスクのレビューに関する規定（対象、体制、判定基準など）を設定・改訂することができる		
標準の維持・管理と品質管理	標準の維持管理	標準化した改善プロセスの実施管理	S-4-4-7-01	標準化された各プロセスの手順、文書様式、その他の規定について、業務の安全性、効率性を促す改善を推進する体制の確保と啓蒙活動を推進することができる		
営業・調達活動>(IT事業）セールス活動	ソリューション提案／戦略立案	リスク計画	S-5.2-6-2-02	リスク発生に伴うすべての事項を文書化することできる		
営業・調達活動>(IT事業）セールス活動	ソリューション提案／提案	（ソリューション提案）	S-5.2-7-3-05	顧客のセキュリティ基準、監査基準をヒアリングすることができ、基準に適合するよう可能な限り調整したうえで提案ができる		
営業・調達活動>開発パートナーの選定	委託先の選定	セキュリティの調査	(仮)S-5.3-1-7-01	委託開始時と更新時においてセキュリティが担保されていることを調査する	UISS作業委員会	小分類の追加
プロジェクトマネジメント	プロジェクト計画策定	リスク管理計画	S-7-2-10-04	リスクがプロジェクトに与える影響度を計り、対応の優先順位を決定し、対応策を講ずることができる		
プロジェクトマネジメント	プロジェクト計画策定	品質保証計画	S-7-2-9-01	品質保証計画の必要性と目的を理解しており、説明することができる		
プロジェクトマネジメント	プロジェクト計画策定	品質保証計画	S-7-2-9-02	プロジェクトに求められる品質特性を理解し、品質品質方針、達成目標（品質基準）を設定することができる		
プロジェクトマネジメント	プロジェクト計画策定	品質保証計画	S-7-2-9-03	品質保証のための組織構造、責任、プロセス、リソース等を明確にし、品質保証計画をの説明をすることができる		
プロジェクトマネジメント	プロジェクト計画策定	品質保証計画	S-7-2-9-04	定められている品質標準を満たすための方策・手段を策定することができる		
プロジェクトマネジメント	プロジェクト計画策定	品質保証計画	S-7-2-9-05	品質リスクを文書化することができる		
プロジェクトマネジメント	プロジェクト追跡と実行管理	品質管理	S-7-3-11-01	定められた手順に沿って品質管理を実施することができる		
プロジェクトマネジメント	プロジェクト追跡と実行管理	品質管理	S-7-3-11-02	品質未達が識別された場合、対応策を講じることができる		

大分類	中分類	小分類	スキルコード	スキル項目	根拠	見直しの内容
プロジェクトマネジメント	プロジェクト追跡と実行管理	品質管理	S-7-3-11-03	プロジェクト全体の品質に大きな影響が予測される場合、品質保証計画を変更し、承認を受けて実施することができる		
プロジェクトマネジメント	プロジェクト追跡と実行管理	品質管理	S-7-3-11-04	品質保証計画の変更に伴う改善状況を確認することができる		
ITシステム企画>ITシステム企画策定	システム計画の立案	サービスレベルと品質に対する基本方針の明確化	S-8.1-2-10-01	サービスレベルと品質に対する基本方針を明確にすることができる		
ITシステム企画>ITシステム企画策定	システム化計画の具体化	システム要件の定義	S-8.1-3-2-08	リモート運用に対する制限など、セキュリティ要件を検討できる		
システム開発・構築>基盤システム	システム化計画の具体化	情報セキュリティアーキテクチャの設計	(仮)S-8.1-3-5-01	アプリケーション、システム及びネットワークの実装のためのセキュリティアーキテクチャを設計することができる	NICEタスク定義をもとに追加	小分類の追加
ITシステム企画>ITシステム企画策定	システム化計画の具体化	セキュリティ設計仕様書へのセキュリティポリシー等の反映	(仮)S-8.1-3-6-01	セキュリティポリシーやコンプライアンス、情報保証上の必要性をセキュリティ要件に反映させることができる	NICEタスク定義をもとに追加	小分類の追加
ITシステム企画>ITシステム企画策定	システム化計画の具体化	情報技術の変化に応じたセキュリティ要件の見直し	(仮)S-8.1-3-7-01	情報技術の変化に応じて、セキュリティ要件を変更、もしくは変更が不要なことを確認することができる	NICEタスク定義をもとに追加	小分類の追加
ITシステム企画>ITシステム企画策定	システム化計画の具体化	設計段階におけるセキュリティ要件の定義	(仮)S-8.1-3-8-01	実装すべきセキュリティの要件（障害発生時の復旧時間の許容時間、データ復旧範囲など、障害対応に関する要件を含む）、レベル感、考慮点等を明確にすることができる。	UISS作業委員会（文言変更）	小分類の追加
システム開発・構築>基盤システム	システム化計画の具体化	セキュリティ設計仕様書の作成	(仮)S-8.1-3-9-01	セキュリティ要件をもとに、ソフトウェア及びシステムが備えるべきセキュリティ機能に関するセキュリティ設計仕様書を文書化することができる	NICEタスク定義をもとに追加	小分類の追加
システム要件定義	システム化要件の定義	要求事項の分析・調査	S-9-1-3-03	システム化で利用する予定の技術、製品について調査し、機能、制約、リスクを把握することができる		
システム要件定義	システムアーキテクチャ設計	適用製品の評価・選定	S-9-2-5-02	利用する技術・製品の選定し、その事由と実装リスク、前提条件を明らかにすることができる		
システム開発・構築>アプリケーションシステム	アプリケーション開発	ソフトウェアコード作成	S-10.1-7-2-05	SQLインジェクション等、作成するプログラムのセキュリティホールへの対策を理解して、セキュアなプログラミングができる		
システム開発・構築>基盤システム	システム設計（セキュリティ）	認証と権限のコントロール	S-10.2-3-1-01	セキュリティポリシーに則して、情報資産別にアクセス方法を設計することができる		
システム開発・構築>基盤システム	システム設計（セキュリティ）	物理セキュリティのコントロール	S-10.2-3-2-01	セキュリティポリシーに則して、情報資産の機密性、完全性、可用性等の要件別にプロパティ設計をすることができる		
システム開発・構築>基盤システム	システム設計（セキュリティ）	論理セキュリティのコントロール	S-10.2-3-3-01	セキュリティポリシーに則して、情報資産の機密性、完全性、可用性等の要件別に、ネットワークセキュリティ設計をすることができる		
システム開発・構築>基盤システム	システム設計（セキュリティ）	ネットワーク基盤上データの信頼性確保	S-10.2-3-4-01	ネットワーク上のデータの改ざんや攻撃、コンピュータウイルス等の脅威を抑止するための安全策を設計することができる		
システム開発・構築>基盤システム	システム設計（セキュリティ）	ネットワーク基盤を経由しない攻撃等に対するデータの信頼性確保	(仮)S-10.2-3-7-01	ネットワーク以外の攻撃等について、脅威を抑止するための安全策を設計することができる	NICEタスク定義をもとに追加	小分類の追加
システム開発・構築>基盤システム	システム設計（セキュリティ）	データの機密保持	S-10.2-3-5-01	個人単位によるデータへのアクセス制限、データへのアクセスを記録、データの暗号化などの設計ができる		
システム開発・構築>基盤システム	システム設計（セキュリティ）	セキュリティ運用手続きの作成	S-10.2-3-6-01	バックアップ、緊急事態対策要件に基づき、セキュリティ監視の範囲、セキュリティ監視結果の情報の保管方法を決定することができる		
システム開発・構築>基盤システム	システム設計（セキュリティ）	情報セキュリティアーキテクチャと対策との整合性確保	(仮)S-10.2-3-8-01	実施するセキュリティ対策について、セキュリティアーキテクチャとの整合を図ることができる	NICEタスク定義をもとに追加	小分類の追加
システム開発・構築>基盤システム	システム設計（セキュリティ）	新技術等への対応状況の分析	(仮)S-10.2-3-9-01	新たな技術や技術改良についてのセキュリティプログラムの実装を識別する	NICEタスク定義をもとに追加	小分類の追加
システム開発・構築>基盤システム	システム設計（セキュリティ）	形式手法を用いたソフトウェアシステムの設計、開発、ならびに修正	(仮)S-10.2-3-10-01	特に高度なセキュリティが求められる箇所について、形式手法等を用いて脆弱性が生じにくいソフトウェアの設計・開発を行うことができる	NICEタスク定義をもとに追加	小分類の追加
システム開発・構築>基盤システム	システム設計（セキュリティ）	脆弱性に対する対策方針の決定	(仮)S-10.2-3-11-01	システムに存在する脆弱性について、その対策と緩和のための取り組みの方針を決定することができる（アプリケーションの可用性維持からパッチを適用しない場合の対策等を含む）	NICEタスク定義をもとに追加	小分類の追加
システム開発・構築>基盤システム	システム設計（セキュリティ）	セキュリティ、回復力、及び信頼性に関する対策の提言	(仮)S-10.2-3-12-01	情報保証において、レビュー結果をもとにセキュリティ、回復力、及び信頼性に関する対策を提言することができる	NICEタスク定義をもとに追加	小分類の追加

大分類	中分類	小分類	スキルコード	スキル項目	根拠	見直しの内容
システム開発・構築>基盤システム	システム設計（セキュリティ）	セキュリティ体制、能力及び脆弱性に関する評価結果の文書化	(仮)S-10.2-3-13-01	情報保証において、アプリケーション、システムまたはネットワークについてのセキュリティ評価を実施した結果を文書化することができる	NICEタスク定義をもとに追加	小分類の追加
システム開発・構築>基盤システム	システム設計（セキュリティ）	運用計画へのセキュリティ対策の反映	(仮)S-10.2-3-14-01	対象とするシステムの運用計画に、必要なセキュリティレベルを確保するために実施すべき情報セキュリティ対策を反映させることができる	NICEタスク定義をもとに追加	小分類の追加
システム開発・構築>基盤システム	システム設計(ネットワーク)	ネットワークシステムの設計	S-10.2-5-1-05	信頼性対策を費用対効果、実現の可能性を評価の上でネットワークアーキテクチャ、セキュリティ対策、シナリオを作成することができる		
システム開発・構築>基盤システム	構築・テスト（セキュリティ）	セキュリティ製品の選定および導入	S-10.2-9-1-01	企業の情報システムやネットワークの構成要素を識別し、それぞれの構成要素に対してセキュリティ製品を選択し導入することができる		
システム開発・構築>基盤システム	構築・テスト（セキュリティ）	セキュリティシステムの開発	S-10.2-9-2-01	セキュリティシステムの設計要件を実装する適当なセキュリティ製品が存在しない場合、必要に応じて独自にソフトウェア開発ををおこなうことが		
システム開発・構築>基盤システム	構築・テスト（セキュリティ）	セキュリティ要件の実装	(仮)S-10.2-9-4-01	セキュリティ設計仕様書に則ったセキュリティ対策を実装することができる	UISS作業委員会	小分類の追加
システム開発・構築>基盤システム	構築・テスト（セキュリティ）	セキュリティ評価の実施	(仮)S-10.2-9-5-01	ISO/IEC 15408の定める手順により、ソフトウェア及びシステムについてのセキュリティ評価を行うことができる	NICEタスク定義をもとに追加	小分類の追加
システム開発・構築>基盤システム	構築・テスト（セキュリティ）	セキュリティ、回復力、信頼性の要件に関するシステムの適合性の評価	(仮)S-10.2-9-6-01	情報保証において、セキュリティ、回復力、信頼性の要件に関してシステムの適合性を測定、評価することができる	NICEタスク定義をもとに追加	小分類の追加
システム開発・構築>基盤システム	構築・テスト（セキュリティ）	対策の修正に関する取組みの実施状況の確認	(仮)S-10.2-9-7-01	情報保証において、不適切に実装されたアプリケーションやシステム、ネットワークについて修正のための取り組みを実施させ、その実施状況を確認できる	NICEタスク定義をもとに追加	小分類の追加
システム開発・構築>基盤システム	構築・テスト（セキュリティ）	セキュリティ実装の確認	S-10.2-9-3-01	導入製品の環境設定または開発機能のセキュリティテスト（要件万像、脆弱性確認）をおこなうことができる		
システム開発・構築>ソフトウェア製品	ソフトウェア開発	ソフトウェアコード作成	S-10.3-5-2-05	SQLインジェクション等、作成するプログラムのセキュリティホールへの対策を理解して、セキュアなプログラミングができる		
システム運用	セキュリティ障害管理	事故の検知	S-12-5-1-01	正常なシステム動作がどのようなものか把握できる		
システム運用	セキュリティ障害管理	事故の検知	S-12-5-1-02	ログファイルを定期的にチェックすることができる		
システム運用	セキュリティ障害管理	事故の検知	S-12-5-1-03	システムの整合性を定期的にチェックすることができる		
システム運用	セキュリティ障害管理	事故の検知	S-12-5-1-04	自動ツールを駆使し、不正侵入を検知することができる		
システム運用	セキュリティ障害管理	事故の初動処理	S-12-5-2-01	事故の初動処理に対する手続きを文書化することができる		
システム運用	セキュリティ障害管理	事故の初動処理	S-12-5-2-02	情報システム責任者や関連部署への連絡を手続どおりに行うことができる		
システム運用	セキュリティ障害管理	事故の初動処理	S-12-5-2-03	処置の優先順位づけを行うことができる		
システム運用	セキュリティ障害管理	事故の初動処理	S-12-5-2-04	優先順位によって、被害拡大を回避する処置を行うことができる		
システム運用	セキュリティ障害管理	事故の初動処理	S-12-5-2-05	初動処理の記録を文書化し、報告を行うことができる		
システム運用	セキュリティ障害管理	事故の分析	S-12-5-3-01	事故の分析体制を整備することができる		
システム運用	セキュリティ障害管理	事故の分析	S-12-5-3-02	被害の範囲を識別することができる		
システム運用	セキュリティ障害管理	事故の分析	S-12-5-3-03	セキュリティホール情報やセキュリティ勧告およびパッチ情報の最新情報を得て、分析を行なうことができる		
システム運用	セキュリティ障害管理	事故の分析	S-12-5-3-04	事故の原因を特定することができる		
システム運用	セキュリティ障害管理	事故からの復旧	S-12-5-4-01	事故から復旧が迅速にでき、必要に応じてシステムの再編成を行うことができる		
システム運用	セキュリティ障害管理	事故からの復旧	S-12-5-4-02	復旧について、詳しい記録を文書化することができる		
システム運用	セキュリティ障害管理	事故からの復旧	S-12-5-4-03	情報システム管理者および利用者に復旧を通知することができる		
システム運用	セキュリティ障害管理	事故からの復旧	S-12-5-4-04	復旧後、セキュリティの見直しを行うことができる		
システム運用	セキュリティ障害管理	再発防止策の実施	S-12-5-5-01	同じような事故に対しての再発防止策を決定し、実施し、必要に応じてシステムの再構築を行うことができる		
システム運用	セキュリティ障害管理	再発防止策の実施	S-12-5-5-02	再発防止策の決定後、セキュリティの見直しを行うことができる		
システム運用	セキュリティ障害管理	セキュリティの評価	S-12-5-6-01	侵入検査を行い、セキュリティポリシーの遵守状況を評価することができる		
システム運用	セキュリティ障害管理	セキュリティの評価	S-12-5-6-02	侵入検査を継続的に実施することができる		
システム運用	セキュリティ障害管理	セキュリティの評価	S-12-5-6-03	侵入検査で不備のある場合は、速やかに対策を行うことができる		
システム運用	セキュリティ障害管理	セキュリティの評価	S-12-5-6-04	セキュリティの評価情報をセキュリティの見直しで利用することができる		

大分類	中分類	小分類	スキルコード	スキル項目	根拠	見直しの内容
システム運用	セキュリティ管理	セキュリティ侵害の監視と状況分析	S-12-8-1-01	ログファイルを定期的にチェックし、セキュリティ事故を検知することができる		
システム運用	セキュリティ管理	セキュリティ侵害の監視と状況分析	S-12-8-1-02	システムの整合性を定期的にチェックし、セキュリティ事故を検知することができる		
システム運用	セキュリティ管理	セキュリティ強度の確認	S-12-8-2-01	同じような事故に対しての再発防止策を決定して実施し、必要に応じてシステムの再構築を行うことができる		
システム運用	セキュリティ管理	セキュリティ強度の確認	S-12-8-2-02	セキュリティホール情報やセキュリティ勧告およびパッチの最新情報を得ることができる		
システム運用	セキュリティ管理	セキュリティ強度の確認	S-12-8-2-03	最新のセキュリティ技術情報を収集し、社内システムへの適用可否を評価することができる		
システム運用	セキュリティ管理	セキュリティ監査対応	S-12-8-3-01	設計したセキュリティの安全性・有効性を検証できる		
システム運用	セキュリティ管理	セキュリティ対策の実施	S-12-8-4-01	既存セキュリティを調査し、耐監査性・機密性・可用性・完全性等の視点から問題点を抽出できる		
システム運用	セキュリティ管理	セキュリティ障害管理	S-12-8-5-01	セキュリティ対策計画を企画・立案・分析・改善できる		
システム運用	セキュリティ管理	セキュリティ障害管理	S-12-8-5-02	外部からのアタックやウィルス進入の防止策を立案できる		
システム運用	セキュリティ管理	手続とガイドラインのポリシーへの準拠状況の監視	(仮)S-12-8-6-01	手続やガイドラインがセキュリティポリシーに確実に適合しているかどうか、ポリシーに基づく標準と実装戦略を監視することができる	NICEタスク定義をもとに追加	小分類の追加
システム運用	セキュリティ管理	実行中のサービスからの要求の予測に基づくセキュリティ上の前提条件についての評価	(仮)S-12-8-7-01	実行中のサービスからの要求を予測し、必要に応じてセキュリティ上の前提条件に関する評価を行うことができる	NICEタスク定義をもとに追加	小分類の追加
システム運用	セキュリティ管理	業務機能に関する識別と優先度の設定	(仮)S-12-8-8-01	組織内の関係者との連携のもとで、重要な業務機能を識別し、優先度を設定することができる	NICEタスク定義をもとに追加	小分類の追加
システム運用	セキュリティ管理	リスクのレベルに関する継続的な検査	(仮)S-12-8-9-01	情報保証において、ソフトウェアアプリケーション、ネットワークまたはシステムのリスクのレベルが許容範囲内であるかどうかを、観測結果をもとに継続的に検査することが出来る	NICEタスク定義をもとに追加	小分類の追加
システム運用	セキュリティ管理	上位者または本部組織への報告	(仮)S-12-8-10-01	上位者または本部組織に対して、技術文書、インシデントレポート、検査結果、他の観測情報を提供することができる	NICEタスク定義をもとに追加	小分類の追加
システム運用	セキュリティ管理	他組織との情報交換	(仮)S-12-8-11-01	インシデント対応とコンピュータネットワーク防御に関して、外部組織と情報交換を行うことができる	NICEタスク定義をもとに追加	小分類の追加
システム運用	セキュリティ管理	適用基準に則ったセキュリティパッチ適用	(仮)S-12-8-12-01	パッチ適用基準に基づくパッチマネジメントができる	UISS作業委員会	小分類の追加
システム運用	セキュリティ管理	アウトソース管理	(仮)S-12-8-13-01	セキュリティ基準に基づき、アウトソース選定時及び継続時におけるセキュリティ実施状況の有効性を検証できる	UISS作業委員会	小分類の追加
システム運用	セキュリティ管理	第三者機関電子証明書の申請、期限管理、更新	(仮)S-12-8-14-01	第三者機関が発行する電子証明書を申請して入手し、その有効期限を管理し、期限切れになる前に更新手続きを行うことができる	UISS作業委員会	小分類の追加
システム運用	セキュリティ管理	自社電子証明書の企画、設計	(仮)S-12-8-15-01	自社で発行する電子証明書について、その発行業務を企画し、発行手続きを定めることができる。	UISS作業委員会	小分類の追加
システム運用	セキュリティ管理	自社電子証明書の発行、期限管理、更新	(仮)S-12-8-16-01	自社で発行する電子証明書について、その発行を管理し、それぞれの電子証明書の有効期限を管理し、期限切れになる前に更新手続きが必要なことを通知することができる	UISS作業委員会	小分類の追加
システム運用	セキュリティ管理	利用者管理	(仮)S-12-8-17-01	従業員が発信する電子メールの内容確認、閲覧するサイトの管理、機器の持ち出し・持ち込み管理等を行うことができる	UISS作業委員会	小分類の追加
システム運用	セキュリティ管理	情報システムの保証と認定の維持に必要な対策の実施	(仮)S-12-8-18-01	情報保証において、情報システムに関する保証と認定を維持するために必要な対策を講じて、これらの保証と認定を維持することができる	NICEタスク定義をもとに追加	小分類の追加
コンプライアンス	管理方針と体制	法令及び規範の管理体制確立	S-13-1-1-01	組織体内において、法令及び規範の所管部署を定めることができる		
コンプライアンス	管理方針と体制	法令及び規範の管理体制確立	S-13-1-1-02	該当部門の職務分掌として、法令及び規範の所管を明確に位置づけることができる		
コンプライアンス	管理方針と体制	法令及び規範の管理体制確立	S-13-1-1-03	法令及び規範の遵守状況を確認することができる		
コンプライアンス	管理方針と体制	管理責任者の選定	S-13-1-2-01	法令及び規範の所管部署において、管理責任者を定め、責任の所在を明確にすることができる		
コンプライアンス	管理方針と体制	遵守すべき法令及び規範の識別	S-13-1-3-01	必要な関係法令や規範を識別し特定することができる		
コンプライアンス	管理方針と体制	遵守すべき法令及び規範の識別	S-13-1-3-02	特定した関係法令及び規範については、定期的に見直しをすることができる		

大分類	中分類	小分類	スキルコード	スキル項目	根拠	見直しの内容
コンプライアンス	管理方針と体制	情報倫理規定の策定	S-13-1-4-01	業務遂行上必要となる関係法令や規範に基づき、組織体が遵守すべきルールを情報倫理規定として定めることができる		
コンプライアンス	管理方針と体制	情報倫理規定の策定	S-13-1-4-02	情報倫理規定を周知徹底するための教育体制を確立し、必要な関係者に教育することができる		
コンプライアンス	管理方針と体制	情報倫理規定の策定	S-13-1-4-03	情報倫理規定を定期的に見直すことができる		
コンプライアンス	管理方針と体制	個人情報保護	S-13-1-5-01	個人情報保護の観点から個人情報取り扱い方針を定めることができる		
コンプライアンス	管理方針と体制	知的財産権保護	S-13-1-6-01	知的財産権保護の観点から知的財産取り扱い方針を定めることができる		
コンプライアンス	管理方針と体制	外部データ提供管理方針	S-13-1-7-01	各種権利保護とデータ取り扱いの観点から、外部へのデータ提供に関する方針を定めることができる		
コンプライアンス	管理方針と体制	外部データ提供管理方針	S-13-1-7-02	定めた方針を実行するため、業務遂行に必要な手順書、マニュアルを定め、組織体内外の関係者に周知徹底することができる		
コンプライアンス	実施・評価	教育・周知徹底	S-13-2-1-01	特定した関係法令や規範について、組織体内外の必要な関係者に周知徹底するために必要な教育体制を確立することができる		
コンプライアンス	実施・評価	教育・周知徹底	S-13-2-1-02	関係法令及び規範についての教育実施責任者を定め、必要な教育を実施し、関係者に周知徹底することができる		
コンプライアンス	実施・評価	遵守状況の評価と改善	S-13-2-2-01	法令及び規範及び情報倫理規定の遵守状況を定期的に点検・評価することができる		
コンプライアンス	実施・評価	遵守状況の評価と改善	S-13-2-2-02	遵守状況の点検・評価によって、明らかになった指摘事項・改善事項に対して、改善計画を策定し、改善のための必要な方策を講ずることができる		
コンプライアンス	実施・評価	遵守状況の評価と改善	S-13-2-2-03	改善計画は、マネジメントレビューを実施し、組織体の長に承認させることができる		
情報セキュリティマネジメント	セキュリティ方針の策定	情報資産の評価	S-14-1-1-01	企業の情報資産（システム、データ、人材、ドキュメント）を識別することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	情報資産の評価	S-14-1-1-02	機密性、完全性、可用性の3つの側面から経営における重要度、致命度を評価し、整理することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	情報資産の評価	S-14-1-1-03	整理、評価された情報資産について、経営層、情報セキュリティ関係担当役員、企画関係者に説明でき、承認を受けることができる		
情報セキュリティマネジメント	セキュリティ方針の策定	脅威の認識	S-14-1-2-01	正確な調査情報を取得することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	脅威の認識	S-14-1-2-02	適切な方法論を用いて情報源および要求を把握することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	脅威の認識	S-14-1-2-03	現状の脅威に関する情報を網羅的に収集することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	脅威の認識	S-14-1-2-04	収集された情報について、情報の改ざん、情報の漏洩、資源の浪費、資源の不正利用、人による過ちなどの分類項目で整理することができ		
情報セキュリティマネジメント	セキュリティ方針の策定	リスクの識別	S-14-1-3-01	情報資産について、現状のリスクが識別することができる（システム廃棄を含む）		
情報セキュリティマネジメント	セキュリティ方針の策定	リスクの識別	S-14-1-3-02	リスクの発生しうる場所および発生時期を整理することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	リスクの識別	S-14-1-3-03	リスクの原因について、物理的な要因、技術的な要因、人的な要因に整理をすることができる		
情報セキュリティマネジメント	セキュリティ方針の策定	対策の整理と調査	S-14-1-4-01	識別されたリスクに対して、対策を決定することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	対策の整理と調査	S-14-1-4-02	対策が現状どの程度実施されているかどうか調査でき、整理することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	リスクの評価	S-14-1-5-01	整理されたリスクの発生確率を明確にすることができる		
情報セキュリティマネジメント	セキュリティ方針の策定	リスクの評価	S-14-1-5-02	リスクが発生したときの損害額を算定することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	リスクの評価	S-14-1-5-03	各リスクに対して、リスク軽減の対策とコストを算定することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	リスクの評価	S-14-1-5-04	各リスクに対する、リスク発生時の損害額と対策コストのバランスを考慮することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	リスクの評価	S-14-1-5-05	残存リスクを評価することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	リスクの評価	S-14-1-5-06	リスク対策について、ランク付けすることができる		
情報セキュリティマネジメント	セキュリティ方針の策定	セキュリティ方針・体制の策定	S-14-1-6-01	セキュリティ対策への取り組みを経営方針に反映させることができる		
情報セキュリティマネジメント	セキュリティ方針の策定	セキュリティ方針・体制の策定	S-14-1-6-02	個々の技術に依存せずに方針策定することができる		

大分類	中分類	小分類	スキルコード	スキル項目	根拠	見直しの内容
情報セキュリティマネジメント	セキュリティ方針の策定	セキュリティ方針・体制の策定	S-14-1-6-03	セキュリティ対策の目的、適用範囲、達成レベル、対策基準の方針、情報セキュリティの責任者、経営者／従業員の遵守事項、組織または実施体制、運用、罰則、公開、見直しについて記述することができる		
情報セキュリティマネジメント	セキュリティ方針の策定	セキュリティ方針・体制の策定	S-14-1-6-04	経営層、情報セキュリティ関係担当役員、企画関係者に説明し、承認を受けることができる		
（追加すべきタスク）	セキュリティ方針の策定	ポリシー案の承認	(仮)S-14-1-7-01	ポリシー案およびその調整に関するレビューと承認を行うことができる	NICEタスク定義をもとに追加	小分類の追加
（追加すべきタスク）	セキュリティ方針の策定	代替案の分析	(仮)S-14-1-8-01	組織のセキュリティ目標を実現するための情報セキュリティ戦略の代替案を分析することができる	NICEタスク定義をもとに追加	小分類の追加
情報セキュリティマネジメント	セキュリティ基準の策定	企業活動のセキュリティ規定の作成	S-14-2-1-01	企業セキュリティ方針の策定で整理された対策を基準に網羅することができる		
情報セキュリティマネジメント	セキュリティ基準の策定	企業活動のセキュリティ規定の作成	S-14-2-1-02	経営層、情報セキュリティ関係担当役員、企画関係者に説明し、承認を受けることができる		
情報セキュリティマネジメント	セキュリティ基準の策定	情報システムのセキュリティ規定の作成	S-14-2-2-01	ITセキュリティ方針の策定で整理された対策を基準に網羅することができる		
情報セキュリティマネジメント	セキュリティ基準の策定	情報システムのセキュリティ規定の作成	S-14-2-2-02	経営層、情報セキュリティ関係担当役員、企画関係者に説明し、承認を受けることができる		
情報セキュリティマネジメント	セキュリティ基準の策定	物理的保護レベルの定義	S-14-2-3-01	ビジネス戦略、事業継続計画に沿った、各物理的サイトの物理的保護レベルを定義できる		
情報セキュリティマネジメント	セキュリティ基準の策定	セキュリティ計画の立案	(仮)S-14-2-4-01	情報セキュリティをベースにしたセキュリティ計画を、立案することができる	UISS作業委員会	小分類の追加
情報セキュリティマネジメント	セキュリティ基準の策定	ソリューション提案	(仮)S-14-2-5-01	セキュリティ計画の立案、およびセキュリティ計画を実行するに当たって発生する問題のソリューションを提案することができる	UISS作業委員会	小分類の追加
情報セキュリティマネジメント	セキュリティ基準の策定	パッチマネジメント基準の策定	(仮)S-14-2-6-01	セキュリティホール情報やセキュリティ勧告およびパッチ情報の最新情報の分析をもとに、パッチ適用基準を策定できる	UISS作業委員会	小分類の追加
情報セキュリティマネジメント	セキュリティ基準の策定	ソーシャルメディア使用に関するポリシー・ガイドラインの策定	(仮)S-14-2-7-01	社員のソーシャルメディア使用に関するルールを策定できる	UISS作業委員会	小分類の追加
情報セキュリティマネジメント	セキュリティ基準の策定	アウトソース先の選定・管理のためのセキュリティ基準の策定	(仮)S-14-2-8-01	アウトソース先のセキュリティ基準を策定できる	UISS作業委員会	小分類の追加
情報セキュリティマネジメント	セキュリティ基準の策定	電子証明書利用手続きの策定	(仮)S-14-2-9-01	電子データの信頼性を確保するために、第三者機関が発行する電子証明書と自社が発行する電子証明書をそれぞれ利用する手続きを策定することができる	UISS作業委員会	小分類の追加
情報セキュリティマネジメント	セキュリティ基準の策定	情報ネットワークのセキュリティ対策のためのガイダンス文書の作成管理	(仮)S-14-2-10-01	情報ネットワークのセキュリティ対策のためのガイダンス文書の発行管理を行うことができる	NICEタスク定義をもとに追加	小分類の追加
情報セキュリティマネジメント	情報セキュリティガバナンス	リスクガバナンスプロセスへの関与	(仮)S-14-4-1-01	セキュリティリスク、緩和策、及び他の技術リスクを扱うリスクガバナンスのプロセスに関与する	NICEタスク定義をもとに追加	中分類の追加
情報セキュリティマネジメント	情報セキュリティガバナンス	情報セキュリティ対策に関する関係者との連携	(仮)S-14-4-2-01	組織の目標の達成に向けて組織管理者と連携できる	NICEタスク定義をもとに追加	中分類の追加
情報セキュリティマネジメント	情報セキュリティガバナンス	情報セキュリティ予算、要員、契約の主導	(仮)S-14-4-3-01	情報セキュリティ予算、要員、契約について主導・監督する	NICEタスク定義をもとに追加	中分類の追加
情報セキュリティマネジメント	情報セキュリティガバナンス	セキュリティ管理に必要なリソースの確保	(仮)S-14-4-4-01	セキュアな運用と情報保全の維持に必要なリソースを確保することができる	NICEタスク定義をもとに追加	中分類の追加
情報セキュリティマネジメント	情報セキュリティガバナンス	認定ないし保証されたセキュリティ対策の実施状況に関する最新の文書の入手と利用	(仮)S-14-4-5-01	認定ないし保証されたセキュリティ対策の実施状況に関する最新の文書を入手し、利用することができる	NICEタスク定義をもとに追加	中分類の追加
情報セキュリティマネジメント	情報セキュリティガバナンス	情報セキュリティに関する関係者との情報交換	(仮)S-14-4-6-01	組織内のざまざまな関係者と情報セキュリティ対策の在り方について意見交換することができる	NICEタスク定義をもとに追加	中分類の追加
情報セキュリティマネジメント	情報セキュリティガバナンス	識別された脆弱性への対策	(仮)S-14-4-7-01	リスクアセスメント、監査、検査を通じて識別された脆弱性に対して、適切な対策を講じることができる	NICEタスク定義をもとに追加	中分類の追加
情報セキュリティマネジメント	情報セキュリティガバナンス	緊急時の判断権限の発揮	(仮)S-14-4-8-01	予め緊急時の対応について権限を委任され、必要な対処を行う	NISC調査をもとに追加	中分類の追加
情報セキュリティマネジメント	情報セキュリティガバナンス	セキュリティリスクに対する組織的対応	(仮)S-14-4-9-01	セキュリティリスクの分析結果を、組織設計、職務分掌、業務プロセス定義等に反映させる	ITSS作業委員会での委員指摘	中分類の追加

大分類	中分類	小分類	スキルコード	スキル項目	根拠	見直しの内容
情報セキュリティマネジメント	情報セキュリティガバナンス	現場部門における戦略に対応したプロセスの実行	(仮)S-14-4-10-01	現場部門において、企画部門の戦略立案に対応したプロセスを実施させることができる	ITSS作業委員会での委員指摘	中分類の追加
情報セキュリティマネジメント	調達におけるセキュリティ要件の反映	調達要件におけるセキュリティ関連事項の策定	(仮)S-14-4-11-01	必要なセキュリティレベルを確保するために満足すべきセキュリティ対策に関する要件を、システム及びサービスの調達要件に反映させることができる(→UISS)	NICEタスク定義をもとに追加	中分類の追加
情報セキュリティマネジメント	検査の実施	ネットワーク環境に適した検査の実施	(仮)S-14-4-12-01	組織で実施する検査、テスト、レビューを、ネットワーク環境に適した形で確実に実施させることができる	NICEタスク定義をもとに追加	中分類の追加
情報セキュリティマネジメント	セキュリティの見直し	技術情報の収集と評価	S-14-3-1-01	セキュリティホール情報やセキュリティ勧告およびパッチ情報の最新情報を得ることができる		
情報セキュリティマネジメント	セキュリティの見直し	技術情報の収集と評価	S-14-3-1-02	最新のセキュリティ技術情報を収集し、社内システムに適用できるかどうか評価することができる		
情報セキュリティマネジメント	セキュリティの見直し	運用上の問題点整理と分析	S-14-3-2-01	利用者にアンケートやヒアリングを行い、ポリシー実施上の問題点を収集、整理することができる		
情報セキュリティマネジメント	セキュリティの見直し	運用上の問題点整理と分析	S-14-3-2-02	違反者の多い基準を収集、整理することができる		
情報セキュリティマネジメント	セキュリティの見直し	運用上の問題点整理と分析	S-14-3-2-03	整理された問題点について、セキュリティポリシー変更に対する分析を行い、ポリシーの見直しを行うことができる		
情報セキュリティマネジメント	セキュリティの見直し	運用上の問題点整理と分析	S-14-3-2-04	事故の再発防止策の実施によって、セキュリティポリシーの受ける影響を分析し、ポリシーの見直しを行うことができる		
情報セキュリティマネジメント	セキュリティの見直し	技術上の問題点整理と分析	S-14-3-3-01	新技術の開発により影響を受けるセキュリティポリシーの箇所を識別し、整理することができる		
情報セキュリティマネジメント	セキュリティの見直し	技術上の問題点整理と分析	S-14-3-3-02	セキュリティ分析の評価結果から、影響を受けるセキュリティポリシーの箇所を識別し、整理することができる		
情報セキュリティマネジメント	セキュリティの見直し	技術上の問題点整理と分析	S-14-3-3-03	整理された問題点について、セキュリティポリシー変更に対する分析ができ、ポリシーの見直しを行うことができる		
情報セキュリティマネジメント	セキュリティの見直し	リスク対策が適切に行われていることのレビュー	(仮)S-14-3-6-01	情報保証において、リスクのレベルが各ソフトウェアアプリケーション、システム及びネットワークにおいて許容範囲内であることを確認するためのレビューを行うことができる	NICEタスク定義をもとに追加	小分類の追加
情報セキュリティマネジメント	セキュリティの見直し	非遵守事項のインパクト分析	(仮)S-14-3-7-01	非遵守事項が情報セキュリティにどのような影響を及ぼすかを導き出せる	NICEタスク定義をもとに追加	小分類の追加
情報セキュリティマネジメント	セキュリティの見直し	監査指摘事項への対応	(仮)S-14-3-8-01	適切な緩和策を確実に実施するための監査指摘事項と勧告の追跡を行うことができる	NICEタスク定義をもとに追加	小分類の追加
情報セキュリティマネジメント	セキュリティの見直し	改善状況の検証	(仮)S-14-3-9-01	セキュリティ対策に関する改善策が確実に実施されていることを確認する	NICEタスク定義をもとに追加	小分類の追加
情報セキュリティマネジメント	セキュリティの見直し	新たなリスクの整理と分析	S-14-3-4-01	新たなリスクを収集でき、整理することができる		
情報セキュリティマネジメント	セキュリティの見直し	新たなリスクの整理と分析	S-14-3-4-02	新たなリスクにより影響を受けるセキュリティポリシーの箇所を識別でき、整理することができる		
情報セキュリティマネジメント	セキュリティの見直し	新たなリスクの整理と分析	S-14-3-4-03	整理された問題点について、セキュリティポリシー変更に対する分析ができ、ポリシーの見直しを行うことができる		
情報セキュリティマネジメント	セキュリティの見直し	セキュリティポリシーの更新	S-14-3-5-01	セキュリティポリシー更新の体制を整備することができる		
情報セキュリティマネジメント	セキュリティの見直し	セキュリティポリシーの更新	S-14-3-5-02	分析結果からポリシー変更部分について、再度リスク分析を行い、ポリシーを更新することができる		
情報セキュリティマネジメント	セキュリティの見直し	セキュリティポリシーの更新	S-14-3-5-03	セキュリティポリシーの更新について、経営層、情報セキュリティ関係担当役員、企画関係者の承認を得ることができる		
情報セキュリティマネジメント	セキュリティの見直し	セキュリティポリシーの更新	S-14-3-5-04	継続的にセキュリティポリシーの見直しを行うことができる		
事業継続計画	事業継続計画策定	対象事故・災害のリスク分析(業務継続計画と事業ニーズの把握)	S-16-1-4-01	想定した被災発生時に求められる業務継続性、事業ニーズを明らかにし、関係者の合意を得ることができる		
事業継続計画	事業継続計画策定	事業継続計画の策定(事業継続計画策定と承認)	S-16-1-6-03	事業継続の方針と事業継続計画の整合性を取ることができる		
事業継続計画	事業継続計画策定	情報セキュリティに関するガイダンスの提供	(仮)S-16-1-10-01	事業継続計画の作成のための情報セキュリティに関するガイダンスを提供することができる	NICEタスク定義をもとに追加	小分類の追加
事業継続計画	IT災害継続・復旧計画の作成	資産評価結果に基づく災害時対応計画の策定	(仮)S-16-2-8-01	情報資産の評価結果を踏まえた災害時対応計画が策定できる	UISS作業委員会	小分類の追加
事業継続計画	IT災害継続・復旧計画の作成	緊急時対応体制	S-16-2-6-02	作業の優先順位を判断することができる		

大分類	中分類	小分類	スキルコード	スキル項目	根拠	見直しの内容
事業継続計画	IT災害継続・復旧計画の作成	事業継続のためのリソースの獲得	(仮)S-16-2-9-01	事業継続のための財政措置を含む必要なリソースを確保することができる	NICEタスク定義をもとに追加	小分類の追加
人的資源管理(人材育成)	情報セキュリティ	利用者教育	S-18-6-1-01	情報利用者の教育を実施できる		
人的資源管理(人材育成)	情報セキュリティ	セキュリティ技術者教育	S-18-6-2-01	セキュリティ技術者の教育を実施できる		
人的資源管理(人材育成)	情報セキュリティ	セキュリティインシデントに関する教育	(仮)S-18-6-3-01	セキュリティインシデントがもたらす社会的影響を従業員に理解させることができる	ITSS作業委員会での委員指摘	小分類の追加
システム監査	システム監査の計画	基本計画の作成、実施環境の確保	S-19-1-1-01	経営目標の実現に向けて、システム監査の視点からIS戦略及びISについて効果的かつ効率的な点検・評価を行うための中長期計画書(システム監査技術者の育成含む)を作成することができる		
システム監査	システム監査の計画	基本計画の作成、実施環境の確保	S-19-1-1-02	中長期計画について、経営層に申請し、承認を受けることができる		
システム監査	システム監査の計画	基本計画の作成、実施環境の確保	S-19-1-1-03	中長期計画書を受けて、年度単位に基本計画書を作成することができる		
システム監査	システム監査の計画	基本計画の作成、実施環境の確保	S-19-1-1-04	当年度の監査目的、監査対象、重点監査テーマ、実施体制、実施スケジュールなどを盛り込むことができる		
システム監査	システム監査の計画	個別計画書の作成	S-19-1-2-01	基本計画書を受けて、個々のシステム監査ごとに監査目標を設定し、監査実施、監査報告、フォローアップまでの全プロセスまで作成することができる		
システム監査	システム監査の計画	個別計画書の作成	S-19-1-2-02	個々のシステム監査自体の有用性の確保とともに、監査の実現性や監査業務の効率性についても考慮することができる		
システム監査	システム監査の計画	外部監査計画の作成	(仮)S-19-1-3-01	J-SOX監査等、外部監査に関する実施計画・改善計画が策定できる	UISS作業委員会	小分類の追加
システム監査	システム監査の実施	実施準備	S-19-2-1-01	予備調査の実施に先立って、個別計画書の内容を再確認することができる		
システム監査	システム監査の実施	実施準備	S-19-2-1-02	被監査部門に対して、個別計画書の内容を通知に協力を要請することができる		
システム監査	システム監査の実施	予備調査	S-19-2-2-01	監査対象システムおよび監査対象業務の概要、コントロールの状況などを把握するために必要な情報を収集することができる		
システム監査	システム監査の実施	予備調査	S-19-2-2-02	文書・資料などの関連資料の収集、関係者へのインタビュー、現地調査などで情報収集をすることができる		
システム監査	システム監査の実施	予備調査	S-19-2-2-03	チェックリストを被監査部門に送付・回収し、必要な情報を収集することができる		
システム監査	システム監査の実施	予備調査	S-19-2-2-04	収集した情報から監査対象システム、業務およびコントロールの実態を把握することができる		
システム監査	システム監査の実施	予備調査	S-19-2-2-05	現実の状態とあるべき状態の間の問題点を認識することができる		
システム監査	システム監査の実施	予備調査	S-19-2-2-06	現状把握に際して、個別監査計画書の監査目的に対して組織体が目標すべきレベルを事前に明確にすることができる		
システム監査	システム監査の実施	予備調査	S-19-2-2-07	個別計画書作成時に予測できなかった問題点の存在の可能性を意識することができる		
システム監査	システム監査の実施	監査手続書の作成	S-19-2-3-01	本調査で実施する具体的な監査手続を検討し、監査手続書を作成することができる		
システム監査	システム監査の実施	監査手続書の作成	S-19-2-3-02	監査手続書は、次回以降の監査の参考として利用できるように作成することができる		
システム監査	システム監査の実施	本調査	S-19-2-4-01	現地に赴き、自らの目で確認、評価をすることができる		
システム監査	システム監査の実施	本調査	S-19-2-4-02	現地調査では、監査意見の裏づけとなる証拠資料を入手することができる		
システム監査	システム監査の実施	本調査	S-19-2-4-03	適切な対象者、日程、質問事項などを事前に準備し、的確なインタビューを実施することができる		
システム監査	システム監査の実施	本調査	S-19-2-4-04	監査手続書に基づいてでドキュメントを入手し、レビューすることができる		
システム監査	システム監査の実施	本調査	S-19-2-4-05	監査目標やシステム環境に合わせて、適切な監査技法やツールを利用することができる		
システム監査	システム監査の実施	実施結果の記録(監査調書の作成)	S-19-2-5-01	本調査にて入手した監査証跡に基づき、監査調書を作成することができる		
システム監査	システム監査の実施	実施結果の記録(監査調書の作成)	S-19-2-5-02	監査調書は被監査部門の確認を取りつけることができる		
システム監査	システム監査の実施	実施結果の記録(監査調書の作成)	S-19-2-5-03	監査調書の中に、監査担当者の判断なども記載することができる		

大分類	中分類	小分類	スキルコード	スキル項目	根拠	見直しの内容
システム監査	システム監査の実施	監査意見の明確化	S-19-2-6-01	監査調書に基づいて、総合評価、指摘事項、改善勧告の原案をまとめることができる		
システム監査	システム監査の実施	監査意見の明確化	S-19-2-6-02	総合評価として、監査目的に適合するようにまとめることができる		
システム監査	システム監査の実施	監査意見の明確化	S-19-2-6-03	事実を裏付ける監査証拠がそろっているか、事実誤認がないかなどを確かめ、指摘事項の適正性確保に努めることができる		
システム監査	システム監査の実施	監査意見の明確化	S-19-2-6-04	改善勧告の実現可能性について、改善実施部門の意見を加味してまとめることができる		
システム監査	システム監査の実施	評価・結論の総合検討	S-19-2-7-01	全社的な観点から評価・結論をまとめることができる		
システム監査	システム監査の実施	評価・結論の総合検討	S-19-2-7-02	監査担当としての見解の整合性を加味して原案をまとめることができる		
システム監査	システム監査の実施	監査報告書案	S-19-2-8-01	監査結果を定められた形式で取りまとめ、試案である旨を示すことができる		
システム監査	システム監査の実施	監査報告書案	S-19-2-8-02	報告書を被監査部門へ提示し誤認確認を行うことができる		
システム監査	システム監査の実施	外部監査計画の実施対応	(仮)S-19-2-9-01	J-SOX等、外部監査に対応できる	UISS作業委員会	小分類の追加
システム監査	システム監査の報告	指摘事項の記載	S-19-3-1-01	システム監査の実施結果は、監査報告書にまとめてトップマネジメントに報告することができる		
システム監査	システム監査の報告	指摘事項の記載	S-19-3-1-02	システム監査の結果判明した問題点を指摘事項として記載することができる		
システム監査	システム監査の報告	指摘事項の記載	S-19-3-1-03	指摘事項として、発見事項の内容、それを問題とするに至った根拠、問題を生じさせている原因、それが及ぼしている影響、他の指摘事項との関連性について記載することができる		
システム監査	システム監査の報告	指摘事項の記載	S-19-3-1-04	複数の指摘事項について、総合的に判断して優先順位をつけることができる		
システム監査	システム監査の報告	改善勧告の記載	S-19-3-2-01	指摘事項を改善するために必要な事項を改善勧告として記載することができる		
システム監査	システム監査の報告	改善勧告の記載	S-19-3-2-02	改善内容は可能な限り具体的、詳細なものとするよう努め、改善実施部門との意見交換を行い、改善策の実現可能性について確認するこ		
システム監査	システム監査の報告	改善勧告の記載	S-19-3-2-03	改善勧告は、技術レベルの問題だけではなく、経営の視点やビジネスプロセスの視点も盛り込むことができる		
システム監査	システム監査の報告	補足事項の記載	S-19-3-3-01	トップマネジメントに監査結果を十分理解してもらうために必要な補足資料やシステムの現状判断または改善のために必要な情報を盛り込む		
システム監査	システム監査の報告	補足事項の記載	S-19-3-3-02	速やかに監査報告書を作成し、トップマネジメントに提出することができる		
システム監査	システム監査の報告	監査報告書の提出	S-19-3-4-01	緊急を要する場合には、まず口頭で報告し、後で報告書を提出するといった柔軟な対応ができる		
システム監査	システム監査の報告	監査報告書の提出	S-19-3-4-02	関係者を一堂に会して監査報告会を開催することができる		
システム監査	システム監査の報告	監査報告会の開催	S-19-3-5-01	監査報告会では、改善作業のスケジュールや担当者を決定し、関係者の同意を取ることができる		
システム監査	システム監査の報告	フォローアップの実施	S-19-3-6-01	監査報告後にフォローアップを実施することができる		
システム監査	システム監査の報告	フォローアップの実施	S-19-3-6-02	監査報告会の開催や改善作業の実行計画所および改善報告書などによる実施状況の把握、次回以降のシステム監査での確認などの方法を取ることができる		
システム監査	システム監査の報告	年次監査報告書の作成	S-19-3-7-01	基本計画書に対応して、当該年度に実施した結果を年次監査報告書として作成することができる		
システム監査	システム監査の報告	年次監査報告書の作成	S-19-3-7-02	次年度の基本計画に反映させるべき課題などの事項を記述することができる		
システム監査	システム監査業務の管理	進捗管理	S-19-4-1-01	基本計画書、個別計画書、監査手続書で計画された事項が円滑かつ確実に遂行されるように管理することができる		
システム監査	システム監査業務の管理	品質管理	S-19-4-2-01	システム監査の品質を高めるために、監査手続書および監査調書の内容をレビューすることができる		
システム監査	システム監査業務の管理	監査業務の改善	S-19-4-3-01	システム監査業務の作業実績値などを集計し、計画値との対比を行い、その原因を分析することができる		
システム監査	システム監査業務の管理	監査業務の改善	S-19-4-3-02	個別計画書および監査手続書の改善点などから、システム監査業務の改善を図ることができる		

大分類	中分類	小分類	スキルコード	スキル項目	根拠	見直しの内容
システム監査	システム監査業務の管理	監査体制の整備	S-19-4-4-01	人材ポートフォリオやキャリアパスを考えた、中長期的な視点でシステム監査技術者を計画的に育成することができる		
（未定）	コンピュータ・フォレンジック	証拠証跡の特定	(仮)S-20-1-1-01	インシデント等の証拠・証跡となる情報を特定できる	ISEPA職種定義をもとに追加	中分類の追加
（未定）	コンピュータ・フォレンジック	証拠証跡の分析	(仮)S-20-1-2-01	証拠・証跡として利用可能な情報を分析し、証拠性が担保可能かどうかを判断できる	ISEPA職種定義をもとに追加	中分類の追加
（未定）	コンピュータ・フォレンジック	証拠保全	(仮)S-20-1-3-01	証拠・証跡となる情報を改変されないように保全できる	ISEPA職種定義をもとに追加	中分類の追加
（未定）	コンピュータ・フォレンジック	証拠開示手続き	(仮)S-20-1-4-01	外部に保存されている情報について、フォレンジックス遂行の目的で情報の開示手続きを行うことができる	ISEPA職種定義をもとに追加	中分類の追加
（未定）	（未定）	セキュリティ当事者のメンタルケア	(仮)S-99-1-1-01	セキュリティ障害の当事者（被害者やセキュリティ障害の発端となってしまった人）のメンタルケアに当たることができる	UISS作業委員会	（保留）

第2章　情報セキュリティに関するタスク個票

整理番号		1	
タスクコード		(仮)T-1.4-1-1	
タスク	大分類	事業戦略>情報セキュリティ戦略	
	中分類	情報セキュリティ戦略の策定	
	小分類	最新技術動向の調査・分析	
スキル項目		スキルコード	スキル項目定義
		(仮)S-1.4-1-1-01	システムのセキュリティやリスクに関する技術動向調査を行い、その情報を IT 戦略立案に活用することができる
関連するタスク		(仮)T-8.1-3-7（情報技術の変化に応じたセキュリティ要件の見直し）：情報技術の変化に応じて、セキュリティ要件を変更、もしくは変更が不要なことを確認 T-14-1-2（脅威の認識）：正確な調査情報の取得、脅威に関する情報の網羅的収集 T-14-1-2（対策の整理と調査）：対策の実施状況の調査・整理 T-14-3-1（技術情報の収集と評価）：セキュリティホール情報、セキュリティ勧告、パッチ情報の最新情報の収集	
作成根拠		UISS 作業委員会	
見直しの内容		中分類の追加	

整理番号		2	
タスクコード		(仮)T-1.4-1-2	
タスク	**大分類**	事業戦略>情報セキュリティ戦略	
	中分類	情報セキュリティ戦略の策定	
	小分類	情報セキュリティ戦略実行体制の確立	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-1.4-1-2-01	情報セキュリティ戦略を実施するに当たって、その実行体制を確立することができる
関連するタスク		T-14-1-6（セキュリティ方針・体制の策定）：情報セキュリティの責任者、組織または実施体制を定め、経営層の承認を得る (仮)T-14-4-3（情報セキュリティ予算、要員、契約の主導）：情報セキュリティ予算、要員、契約についての主導・監督	
作成根拠		UISS 作業委員会	
見直しの内容		中分類の追加	

整理番号		3	
タスクコード		(仮)T-1.4-1-3	
タスク	大分類	事業戦略>情報セキュリティ戦略	
	中分類	情報セキュリティ戦略の策定	
	小分類	EA の推進（EA プロセスの統括）	
スキル項目		スキルコード	スキル項目定義
		(仮)S-1.4-1-3-01	経営戦略に準じた組織全体の改善サイクルとなるよう各 EA（BA,DA,AA,TA）開発組織を統轄することができる
関連するタスク		(仮)T-8.1-3-5（情報セキュリティアーキテクチャの設計）：アプリケーション、システム及びネットワークの実装のためのセキュリティアーキテクチャの設計	
作成根拠		UISS 作業委員会	
見直しの内容		中分類の追加	

整理番号		4	
タスクコード		(仮)T-1.4-1-4	
タスク	大分類	事業戦略>情報セキュリティ戦略	
	中分類	情報セキュリティ戦略の策定	
	小分類	委託先管理	
スキル項目		スキルコード	スキル項目定義
		(仮)S-1.4-1-4-01	セキュリティ業務全体をみたときに、その業務の一部を委託をすべきなのかを判断、決定する
関連するタスク		(仮)T-5.3-1-7（セキュリティの調査）：委託先候補でセキュリティが担保されていることの確認	
作成根拠		UISS 作業委員会	
見直しの内容		中分類の追加	

整理番号		5	
タスクコード		(仮)T-5.3-1-7	
タスク	**大分類**	営業・調達活動>開発パートナーの選定	
	中分類	委託先の選定	
	小分類	セキュリティの調査	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-5.3-1-7-01	委託開始時と更新時においてセキュリティが担保されていることを調査する
関連するタスク		(仮)T-1.4-1-4（委託先管理）：外部委託すべきかどうかの判断・決定 (仮)T-12-8-13（アウトソース管理）：セキュリティ基準に基づき、アウトソース選定時及び継続時におけるセキュリティ実施状況の有効性を検証	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		6	
タスクコード		(仮)T-8.1-3-5	
タスク	大分類	IT システム企画>IT システム企画策定	
	中分類	システム化計画の具体化	
	小分類	情報セキュリティアーキテクチャの設計	
スキル項目		スキルコード	スキル項目定義
		(仮)S-8.1-3-5-01	アプリケーション、システム及びネットワークの実装のためのセキュリティアーキテクチャを設計することができる
関連するタスク		(仮)T-1.4-1-3（EA の推進（EA プロセスの統括））：経営戦略に準じた組織全体の改善サイクルとなるよう各 EA（BA,DA,AA,TA）開発組織を統轄 (仮)T-10.2-3-8（情報セキュリティアーキテクチャと対策との整合性確保）：実施するセキュリティ対策について、セキュリティアーキテクチャとの整合を図る	
作成根拠		NICE タスク定義（Task ID=502 ほか）をもとに追加	
見直しの内容		小分類の追加	

整理番号		7	
タスクコード		(仮)T-8.1-3-6	
タスク	大分類	IT システム企画>IT システム企画策定	
	中分類	システム化計画の具体化	
	小分類	セキュリティ設計仕様書へのセキュリティポリシー等の反映	
スキル項目		スキルコード	スキル項目定義
		(仮)S-8.1-3-6-01	セキュリティポリシーやコンプライアンス、情報保証上の必要性をセキュリティ要件に反映させることができる
関連するタスク		(仮)T-8.1-3-9（セキュリティ設計仕様書の作成）：セキュリティ要件をもとに、ソフトウェア及びシステムが備えるべきセキュリティ機能に関するセキュリティ設計仕様書を文書化 (仮)T-12-8-6（手続とガイドラインのポリシーへの準拠状況の監視）：手続やガイドラインがセキュリティポリシーに確実に適合しているかどうか、ポリシーに基づく標準と実装戦略を監視する T-14-1-6（セキュリティ方針・体制の策定）：セキュリティ対策の目的、適用範囲、達成レベル、対策基準の方針等を記述	
作成根拠		NICE タスク定義（Task ID=548 ほか）をもとに追加	
見直しの内容		小分類の追加	

整理番号		8	
タスクコード		(仮)T-8.1-3-7	
タスク	大分類	IT システム企画>IT システム企画策定	
	中分類	システム化計画の具体化	
	小分類	情報技術の変化に応じたセキュリティ要件の見直し	
スキル項目		スキルコード	スキル項目定義
		(仮)S-8.1-3-7-01	情報技術の変化に応じて、セキュリティ要件を変更、もしくは変更が不要なことを確認することができる
関連するタスク		(仮)T-1.4-1-1（最新技術動向の調査・分析）：システムのセキュリティやリスクに関する技術動向調査の結果を IT 戦略立案に活用 (仮)T-10.2-3-9（新技術等への対応状況の分析）：新たな技術や技術改良についてのセキュリティプログラムの実装を識別 (仮)T-12-8-7（実行中のサービスからの要求の予測に基づくセキュリティ上の前提条件についての評価）：実行中のサービスからの要求を予測し、必要に応じてセキュリティ上の前提条件に関する評価を行う T-14-1-2（脅威の認識）：正確な調査情報の取得、脅威に関する情報の網羅的収集 T-14-1-2（対策の整理と調査）：対策の実施状況の調査・整理 T-14-3-1（技術情報の収集と評価）：セキュリティホール情報、セキュリティ勧告、パッチ情報の最新情報の収集	
作成根拠		NICE タスク定義（Task ID=676）をもとに追加	
見直しの内容		小分類の追加	

整理番号		9	
タスクコード		(仮)T-8.1-3-8	
タスク	大分類	IT システム企画>IT システム企画策定	
	中分類	システム化計画の具体化	
	小分類	設計段階におけるセキュリティ要件の定義	
スキル項目		スキルコード	スキル項目定義
		(仮)S-8.1-3-8-01	実装すべきセキュリティの要件（障害発生時の復旧時間の許容時間、データ復旧範囲など、障害対応に関する要件を含む）、レベル感、考慮点等を明確にすることができる。
関連するタスク		(仮)T-8.1-3-6（セキュリティ設計仕様書へのセキュリティポリシー等の反映）：セキュリティポリシーやコンプライアンス、情報保証上の必要性をセキュリティ要件に反映	
作成根拠		UISS 作業委員会(文言変更)	
見直しの内容		小分類の追加	

整理番号		10	
タスクコード		(仮)T-8.1-3-9	
タスク	大分類	IT システム企画>IT システム企画策定	
	中分類	システム化計画の具体化	
	小分類	セキュリティ設計仕様書の作成	
スキル項目		スキルコード	スキル項目定義
		(仮)S-8.1-3-9-01	セキュリティ要件をもとに、ソフトウェア及びシステムが備えるべきセキュリティ機能に関するセキュリティ設計仕様書を文書化することができる
関連するタスク		(仮)T-8.1-3-6（セキュリティ設計仕様書へのセキュリティポリシー等の反映）：セキュリティポリシーやコンプライアンス、情報保証上の必要性をセキュリティ要件に反映	
作成根拠		NICE タスク定義（Task ID＝432）をもとに追加	
見直しの内容		小分類の追加	

整理番号		11	
タスクコード		(仮)T-10.2-3-10	
タスク	大分類	システム開発・構築>基盤システム	
	中分類	システム設計（セキュリティ）	
	小分類	形式手法を用いたソフトウェアシステムの設計、開発、ならびに修正	
スキル項目		スキルコード	スキル項目定義
		(仮)S-10.2-3-10-01	特に高度なセキュリティが求められる箇所について、形式手法等を用いて脆弱性が生じにくいソフトウェアの設計・開発を行うことができる
関連するタスク			
作成根拠		NICE タスク定義（Task ID＝506）をもとに追加	
見直しの内容		小分類の追加	

整理番号		12	
タスクコード		(仮)T-10.2-3-11	
タスク	大分類	システム開発・構築>基盤システム	
	中分類	システム設計（セキュリティ）	
	小分類	脆弱性に対する対策方針の決定	
スキル項目		スキルコード	スキル項目定義
		(仮)S-10.2-3-11-01	システムに存在する脆弱性について、その対策と緩和のための取り組みの方針を決定することができる（アプリケーションの可用性維持からパッチを適用しない場合の対策等を含む）
関連するタスク		(仮)T-12-8-9（リスクのレベルに関する継続的な検査）：情報保証において、ソフトウェアアプリケーション、ネットワークまたはシステムのリスクのレベルが許容範囲内であるかどうかを、観測結果をもとに継続的に検査 (仮)T-10.2-9-7（対策の修正に関する取組みの実施状況の確認）：情報保証において、不適切に実装されたアプリケーションやシステム、ネットワークについて修正のための取り組みを実施させ、その実施状況を確認 T-14-2-3（物理的保護レベルの定義）：ビジネス戦略、事業継続計画に沿った、各物理的サイトの物理的保護レベルを定義	
作成根拠		NICE タスク定義（Task ID＝971, 972）をもとに追加	
見直しの内容		小分類の追加	

整理番号		13	
タスクコード		(仮)T-10.2-3-12	
タスク	**大分類**	システム開発・構築>基盤システム	
	中分類	システム設計（セキュリティ）	
	小分類	セキュリティ、回復力、及び信頼性に関する対策の提言	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-10.2-3-12-01	情報保証において、レビュー結果をもとにセキュリティ、回復力、及び信頼性に関する対策を提言することができる
関連するタスク		T-10.2-9-3（セキュリティ実装の確認）：導入製品の環境設定または開発機能のセキュリティテスト（要件万像、脆弱性確認）の実施 (仮)T-10.2-3-13（セキュリティ体制、能力及び脆弱性に関する評価結果の文書化）：情報保証において、アプリケーション、システムまたはネットワークについてのセキュリティ評価を実施した結果を文書化	
作成根拠		NICE タスク定義（Task ID＝937）をもとに追加	
見直しの内容		小分類の追加	

整理番号		14	
タスクコード		(仮)T-10.2-3-13	
タスク	大分類	システム開発・構築>基盤システム	
	中分類	システム設計（セキュリティ）	
	小分類	セキュリティ体制、能力及び脆弱性に関する評価結果の文書化	
スキル項目		スキルコード	スキル項目定義
		(仮)S-10.2-3-13-01	情報保証において、アプリケーション、システムまたはネットワークについてのセキュリティ評価を実施した結果を文書化することができる
関連するタスク		(仮)T-10.2-3-12（セキュリティ、回復力、及び信頼性に関する対策の提言）：情報保証において、レビュー結果をもとにセキュリティ、回復力、及び信頼性に関する対策を提言	
作成根拠		NICE タスク定義（Task ID＝798）をもとに追加	
見直しの内容		小分類の追加	

整理番号		15	
タスクコード		(仮)T-10.2-3-14	
タスク	大分類	システム開発・構築>基盤システム	
	中分類	システム設計（セキュリティ）	
	小分類	運用計画へのセキュリティ対策の反映	
スキル項目		スキルコード	スキル項目定義
		(仮)S-10.2-3-14-01	対象とするシステムの運用計画に、必要なセキュリティレベルを確保するために実施すべき情報セキュリティ対策を反映させることができる
関連するタスク		(仮)T-10.2-3-11（脆弱性に対する対策方針の決定）：システムに存在する脆弱性について、その対策と緩和のための取り組みの方針を決定	
作成根拠		NICE タスク定義（「Collect and Operate」の定義）をもとに追加	
見直しの内容		小分類の追加	

<table>
<tr><td colspan="2">整理番号</td><td colspan="2">16</td></tr>
<tr><td colspan="2">タスクコード</td><td colspan="2">(仮)T-10.2-3-7</td></tr>
<tr><td rowspan="3">タスク</td><td>大分類</td><td colspan="2">システム開発・構築>基盤システム</td></tr>
<tr><td>中分類</td><td colspan="2">システム設計（セキュリティ）</td></tr>
<tr><td>小分類</td><td colspan="2">ネットワーク基盤を経由しない攻撃等に対するデータの信頼性確保</td></tr>
<tr><td colspan="2" rowspan="3">スキル項目</td><td>スキルコード</td><td>スキル項目定義</td></tr>
<tr><td>(仮)S-10.2-3-7-01</td><td>ネットワーク以外の攻撃等について、脅威を抑止するための安全策を設計することができる</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">関連するタスク</td><td colspan="2">T-10.2-3-4（ネットワーク基盤上データの信頼性確保）：ネットワーク上のデータの改ざんや攻撃、コンピュータウイルス等の脅威を抑止するための安全策を設計</td></tr>
<tr><td colspan="2">作成根拠</td><td colspan="2">NICE タスク定義（「Analyze」の定義）をもとに追加</td></tr>
<tr><td colspan="2">見直しの内容</td><td colspan="2">小分類の追加</td></tr>
</table>

整理番号		17	
タスクコード		(仮)T-10.2-3-8	
タスク	大分類	システム開発・構築>基盤システム	
	中分類	システム設計（セキュリティ）	
	小分類	情報セキュリティアーキテクチャと対策との整合性確保	
スキル項目		スキルコード	スキル項目定義
		(仮)S-10.2-3-8-01	実施するセキュリティ対策について、セキュリティアーキテクチャとの整合を図ることができる
関連するタスク		(仮)T-8.1-3-5（情報セキュリティアーキテクチャの設計）：アプリケーション、システム及びネットワークの実装のためのセキュリティアーキテクチャを設計	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

<table>
<tr><td colspan="2">整理番号</td><td colspan="2">18</td></tr>
<tr><td colspan="2">タスクコード</td><td colspan="2">(仮)T-10.2-3-9</td></tr>
<tr><td rowspan="3">タスク</td><td>大分類</td><td colspan="2">システム開発・構築>基盤システム</td></tr>
<tr><td>中分類</td><td colspan="2">システム設計（セキュリティ）</td></tr>
<tr><td>小分類</td><td colspan="2">新技術等への対応状況の分析</td></tr>
<tr><td colspan="2" rowspan="3">スキル項目</td><td>スキルコード</td><td>スキル項目定義</td></tr>
<tr><td>(仮)S-10.2-3-9-01</td><td>新たな技術や技術改良についてのセキュリティプログラムの実装を識別する</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">関連するタスク</td><td colspan="2">(仮)T-8.1-3-7（情報技術の変化に応じたセキュリティ要件の見直し）：情報技術の変化に応じて、セキュリティ要件を変更、もしくは変更が不要なことを確認</td></tr>
<tr><td colspan="2">作成根拠</td><td colspan="2">NICE タスク定義をもとに追加</td></tr>
<tr><td colspan="2">見直しの内容</td><td colspan="2">小分類の追加</td></tr>
</table>

整理番号		19	
タスクコード		(仮)T-10.2-9-4	
タスク	大分類	システム開発・構築>基盤システム	
	中分類	構築・テスト（セキュリティ）	
	小分類	セキュリティ要件の実装	
スキル項目		スキルコード	スキル項目定義
		(仮)S-10.2-9-4-01	セキュリティ設計仕様書に則ったセキュリティ対策を実装することができる
関連するタスク		T-10.2-9-2（セキュリティシステムの開発）：セキュリティシステムの設計要件を実装する適当なセキュリティ製品が存在しない場合、必要に応じて独自にソフトウェア開発ををおこなう	
作成根拠		UISS 作業委員会(文言変更)	
見直しの内容		小分類の追加	

整理番号		20	
タスクコード		(仮)T-10.2-9-5	
タスク	大分類	システム開発・構築>基盤システム	
	中分類	構築・テスト（セキュリティ）	
	小分類	セキュリティ評価の実施	
スキル項目		スキルコード	スキル項目定義
		(仮)S-10.2-9-5-01	ISO/IEC 15408 の定める手順により、ソフトウェア及びシステムについてのセキュリティ評価を行うことができる
関連するタスク		T-10.2-9-3（セキュリティ実装の確認）：導入製品の環境設定または開発機能のセキュリティテスト（要件万像、脆弱性確認）をおこなう	
作成根拠		NICE タスク定義（Task ID＝826）をもとに追加	
見直しの内容		小分類の追加	

<table>
<tr><td colspan="2">整理番号</td><td colspan="2">21</td></tr>
<tr><td colspan="2">タスクコード</td><td colspan="2">(仮)T-10.2-9-6</td></tr>
<tr><td rowspan="3">タスク</td><td>大分類</td><td colspan="2">システム開発・構築>基盤システム</td></tr>
<tr><td>中分類</td><td colspan="2">構築・テスト（セキュリティ）</td></tr>
<tr><td>小分類</td><td colspan="2">セキュリティ、回復力、信頼性の要件に関するシステムの適合性の評価</td></tr>
<tr><td colspan="2" rowspan="3">スキル項目</td><td>スキルコード</td><td>スキル項目定義</td></tr>
<tr><td>(仮)S-10.2-9-6-01</td><td>情報保証において、セキュリティ、回復力、信頼性の要件に関してシステムの適合性を測定、評価することができる</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">関連するタスク</td><td colspan="2">(仮)T-10.2-3-12（セキュリティ、回復力、及び信頼性に関する対策の提言）：情報保証において、レビュー結果をもとにセキュリティ、回復力、及び信頼性に関する対策を提言</td></tr>
<tr><td colspan="2">作成根拠</td><td colspan="2">NICE タスク定義（Task ID＝710, 772）をもとに追加</td></tr>
<tr><td colspan="2">見直しの内容</td><td colspan="2">小分類の追加</td></tr>
</table>

整理番号		22	
タスクコード		(仮)T-10.2-9-7	
タスク	大分類	システム開発・構築>基盤システム	
	中分類	構築・テスト（セキュリティ）	
	小分類	対策の修正に関する取組みの実施状況の確認	
スキル項目		スキルコード	スキル項目定義
		(仮)S-10.2-9-7-01	情報保証において、不適切に実装されたアプリケーションやシステム、ネットワークについて修正のための取り組みを実施させ、その実施状況を確認できる
関連するタスク		(仮)T-10.2-3-11（脆弱性に対する対策方針の決定）：システムに存在する脆弱性について、その対策と緩和のための取り組みの方針を決定	
作成根拠		NICE タスク定義（Task ID＝878）をもとに追加	
見直しの内容		小分類の追加	

整理番号		23	
タスクコード		(仮)T-12-8-10	
タスク	**大分類**	システム運用	
	中分類	セキュリティ管理	
	小分類	上位者または本部組織への報告	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-12-8-10-01	上位者または本部組織に対して、技術文書、インシデントレポート、検査結果、他の観測情報を提供することができる
関連するタスク		T-12-5-2（事故の初動処理）：初動処理の記録を文書化し、報告を行うことができる	
作成根拠		NICE タスク定義（Task ID＝818）をもとに追加	
見直しの内容		小分類の追加	

整理番号		24	
タスクコード		(仮)T-12-8-11	
タスク	大分類	システム運用	
	中分類	セキュリティ管理	
	小分類	他組織との情報交換	
スキル項目		スキルコード	スキル項目定義
		(仮)S-12-8-11-01	インシデント対応とコンピュータネットワーク防御に関して、外部組織と情報交換を行うことができる
関連するタスク		(仮)T-14-4-6（情報セキュリティに関する関係者との情報交換）：組織内のざまざまな関係者と情報セキュリティ対策の在り方について意見交換する	
作成根拠		NICE タスク定義（Task ID＝674）をもとに追加	
見直しの内容		小分類の追加	

整理番号		25	
タスクコード		(仮)T-12-8-12	
タスク	**大分類**	システム運用	
	中分類	セキュリティ管理	
	小分類	適用基準に則ったセキュリティパッチ適用	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-12-8-12-01	パッチ適用基準に基づくパッチマネジメントができる
関連するタスク		(仮)T-14-2-6（パッチマネジメント基準の策定）：セキュリティホール情報やセキュリティ勧告およびパッチ情報の最新情報の分析をもとに、パッチ適用基準を策定できる	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		26	
タスクコード		(仮)T-12-8-13	
タスク	**大分類**	システム運用	
	中分類	セキュリティ管理	
	小分類	アウトソース管理	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-12-8-13-01	セキュリティ基準に基づき、アウトソース選定時及び継続時におけるセキュリティ実施状況の有効性を検証できる
関連するタスク		(仮)T-5.3-1-7（セキュリティの調査）：委託開始時と更新時においてセキュリティが担保されていることを調査 (仮)T-14-2-8（アウトソース先の選定・管理のためのセキュリティ基準の策定）：アウトソース先のセキュリティ基準を策定	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		27	
タスクコード		(仮)T-12-8-14	
タスク	大分類	システム運用	
	中分類	セキュリティ管理	
	小分類	第三者機関電子証明書の申請、期限管理、更新	
スキル項目		スキルコード	スキル項目定義
		(仮)S-12-8-14-01	第三者機関が発行する電子証明書を申請して入手し、その有効期限を管理し、期限切れになる前に更新手続きを行うことができる
関連するタスク		(仮)T-14-2-9（電子証明書利用手続きの策定）：電子データの信頼性を確保するために、第三者機関が発行する電子証明書と自社が発行する電子証明書をそれぞれ利用する手続きを策定	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		28	
タスクコード		(仮)T-12-8-15	
タスク	大分類	システム運用	
	中分類	セキュリティ管理	
	小分類	自社電子証明書の企画、設計	
スキル項目		スキルコード	スキル項目定義
		(仮)S-12-8-15-01	自社で発行する電子証明書について、その発行業務を企画し、発行手続きを定めることができる。
関連するタスク		(仮)T-14-2-9（電子証明書利用手続きの策定）：電子データの信頼性を確保するために、第三者機関が発行する電子証明書と自社が発行する電子証明書をそれぞれ利用する手続きを策定	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		29	
タスクコード		(仮)T-12-8-16	
タスク	**大分類**	システム運用	
	中分類	セキュリティ管理	
	小分類	自社電子証明書の発行、期限管理、更新	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-12-8-16-01	自社で発行する電子証明書について、その発行を管理し、それぞれの電子証明書の有効期限を管理し、期限切れになる前に更新手続きが必要なことを通知することができる
関連するタスク		(仮)T-14-2-9（電子証明書利用手続きの策定）：電子データの信頼性を確保するために、第三者機関が発行する電子証明書と自社が発行する電子証明書をそれぞれ利用する手続きを策定	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		30	
タスクコード		(仮)T-12-8-17	
タスク	大分類	システム運用	
	中分類	セキュリティ管理	
	小分類	利用者管理	
スキル項目		スキルコード	スキル項目定義
		(仮)S-12-8-17-01	従業員が発信する電子メールの内容確認、閲覧するサイトの管理、機器の持ち出し・持ち込み管理等を行うことができる
関連するタスク		(仮)T-14-2-7（ソーシャルメディア使用に関するポリシー・ガイドラインの策定）：社員のソーシャルメディア使用に関するルールを策定できる T-18-6-1（利用者教育）：情報利用者の教育を実施できる	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		31	
タスクコード		(仮)T-12-8-18	
タスク	**大分類**	システム運用	
	中分類	セキュリティ管理	
	小分類	情報システムの保証と認定の維持に必要な対策の実施	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-12-8-18-01	情報保証において、情報システムに関する保証と認定を維持するために必要な対策を講じて、これらの保証と認定を維持することができる
関連するタスク		(仮)T-14-4-5（認定ないし保証されたセキュリティ対策の実施状況に関する最新の文書の入手と利用）：認定ないし保証されたセキュリティ対策の実施状況に関する最新の文書を入手し、利用する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

整理番号		32	
タスクコード		(仮)T-12-8-6	
タスク	**大分類**	システム運用	
	中分類	セキュリティ管理	
	小分類	手続とガイドラインのポリシーへの準拠状況の監視	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-12-8-6-01	手続やガイドラインがセキュリティポリシーに確実に適合しているかどうか、ポリシーに基づく標準と実装戦略を監視することができる
関連するタスク		(仮)T-8.1-3-6（セキュリティ設計仕様書へのセキュリティポリシー等の反映）：セキュリティポリシーやコンプライアンス、情報保証上の必要性をセキュリティ要件に反映させることができる	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

整理番号		33	
タスクコード		(仮)T-12-8-7	
タスク	**大分類**	システム運用	
	中分類	セキュリティ管理	
	小分類	実行中のサービスからの要求の予測に基づくセキュリティ上の前提条件についての評価	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-12-8-7-01	実行中のサービスからの要求を予測し、必要に応じてセキュリティ上の前提条件に関する評価を行うことができる
関連するタスク		T-9-2-5（適用製品の評価・選定）：利用する技術・製品の選定し、その事由と実装リスク、前提条件を明らかにすることができる (仮)T-8.1-3-7（情報技術の変化に応じたセキュリティ要件の見直し）：情報技術の変化に応じて、セキュリティ要件を変更、もしくは変更が不要なことを確認	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

<table>
<tr><td colspan="2">整理番号</td><td colspan="2">34</td></tr>
<tr><td colspan="2">タスクコード</td><td colspan="2">(仮)T-12-8-8</td></tr>
<tr><td rowspan="3">タスク</td><td>大分類</td><td colspan="2">システム運用</td></tr>
<tr><td>中分類</td><td colspan="2">セキュリティ管理</td></tr>
<tr><td>小分類</td><td colspan="2">業務機能に関する識別と優先度の設定</td></tr>
<tr><td colspan="2" rowspan="3">スキル項目</td><td>スキルコード</td><td>スキル項目定義</td></tr>
<tr><td>(仮)S-12-8-8-01</td><td>組織内の関係者との連携のもとで、重要な業務機能を識別し、優先度を設定することができる</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">関連するタスク</td><td colspan="2">T-12-5-2（事故の初動処理）：処置の優先順位づけを行う</td></tr>
<tr><td colspan="2">作成根拠</td><td colspan="2">NICE タスク定義をもとに追加</td></tr>
<tr><td colspan="2">見直しの内容</td><td colspan="2">小分類の追加</td></tr>
</table>

整理番号		35	
タスクコード		(仮)T-12-8-9	
タスク	**大分類**	システム運用	
	中分類	セキュリティ管理	
	小分類	リスクのレベルに関する継続的な検査	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-12-8-9-01	情報保証において、ソフトウェアアプリケーション、ネットワークまたはシステムのリスクのレベルが許容範囲内であるかどうかを、観測結果をもとに継続的に検査することが出来る
関連するタスク		(仮)T-14-3-6（リスク対策が適切に行われていることのレビュー）：情報保証において、リスクのレベルが各ソフトウェアアプリケーション、システム及びネットワークにおいて許容範囲内であることを確認するためのレビューを行う	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

<table>
<tr><td colspan="2">整理番号</td><td colspan="2">36</td></tr>
<tr><td colspan="2">タスクコード</td><td colspan="2">(仮)T-14-1-7</td></tr>
<tr><td rowspan="3">タスク</td><td>大分類</td><td colspan="2">（追加すべきタスク）</td></tr>
<tr><td>中分類</td><td colspan="2">セキュリティ方針の策定</td></tr>
<tr><td>小分類</td><td colspan="2">ポリシー案の承認</td></tr>
<tr><td colspan="2" rowspan="3">スキル項目</td><td>スキルコード</td><td>スキル項目定義</td></tr>
<tr><td>(仮)S-14-1-7-01</td><td>ポリシー案およびその調整に関するレビューと承認を行うことができる（承認側タスク）</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">関連するタスク</td><td colspan="2">T-14-1-6（セキュリティ方針・体制の策定）：経営層、情報セキュリティ関係担当役員、企画関係者に説明し、承認を受ける（申請側タスク）</td></tr>
<tr><td colspan="2">作成根拠</td><td colspan="2">NICE タスク定義をもとに追加</td></tr>
<tr><td colspan="2">見直しの内容</td><td colspan="2">小分類の追加</td></tr>
</table>

整理番号		37	
タスクコード		(仮)T-14-1-8	
タスク	大分類	（追加すべきタスク）	
	中分類	セキュリティ方針の策定	
	小分類	代替案の分析	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-1-8-01	組織のセキュリティ目標を実現するための情報セキュリティ戦略の代替案を分析することができる
関連するタスク			
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

<table>
<tr><td colspan="2">整理番号</td><td colspan="2">38</td></tr>
<tr><td colspan="2">タスクコード</td><td colspan="2">(仮)T-14-2-10</td></tr>
<tr><td rowspan="3">タスク</td><td>大分類</td><td colspan="2">情報セキュリティマネジメント</td></tr>
<tr><td>中分類</td><td colspan="2">セキュリティ基準の策定</td></tr>
<tr><td>小分類</td><td colspan="2">情報ネットワークのセキュリティ対策のためのガイダンス文書の作成管理</td></tr>
<tr><td colspan="2" rowspan="3">スキル項目</td><td>スキルコード</td><td>スキル項目定義</td></tr>
<tr><td>(仮)S-14-2-10-01</td><td>情報ネットワークのセキュリティ対策のためのガイダンス文書の発行管理を行うことができる</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">関連するタスク</td><td colspan="2">T-12-5-2（事故の初動処理）：事故の初動処理に対する手続きを文書化する
(仮)T-16-1-10（情報セキュリティに関するガイダンスの提供）：事業継続計画の作成のための情報セキュリティに関するガイダンスを提供する</td></tr>
<tr><td colspan="2">作成根拠</td><td colspan="2">NICE タスク定義をもとに追加</td></tr>
<tr><td colspan="2">見直しの内容</td><td colspan="2">小分類の追加</td></tr>
</table>

整理番号		39	
タスクコード		(仮)T-14-2-4	
タスク	大分類	情報セキュリティマネジメント	
	中分類	セキュリティ基準の策定	
	小分類	セキュリティ計画の立案	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-2-4-01	情報セキュリティをベースにしたセキュリティ計画を、立案することができる
関連するタスク		T-14-1-6（セキュリティ方針・体制の策定）：セキュリティ対策への取り組みを経営方針に反映させる	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		40	
タスクコード		(仮)T-14-2-5	
タスク	大分類	情報セキュリティマネジメント	
	中分類	セキュリティ基準の策定	
	小分類	ソリューション提案	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-2-5-01	セキュリティ計画の立案、およびセキュリティ計画を実行するに当たって発生する問題のソリューションを提案することができる
関連するタスク		T-14-1-6（セキュリティ方針・体制の策定）：セキュリティ対策の目的、適用範囲、達成レベル、対策基準の方針、情報セキュリティの責任者、経営者／従業員の遵守事項、組織または実施体制、運用、罰則、公開、見直しについて記述する	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		41	
タスクコード		(仮)T-14-2-6	
タスク	大分類	情報セキュリティマネジメント	
	中分類	セキュリティ基準の策定	
	小分類	パッチマネジメント基準の策定	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-2-6-01	セキュリティホール情報やセキュリティ勧告およびパッチ情報の最新情報の分析をもとに、パッチ適用基準を策定できる
関連するタスク		(仮)T-12-8-12（適用基準に則ったセキュリティパッチ適用）: パッチ適用基準に基づくパッチマネジメント	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		42	
タスクコード		(仮)T-14-2-7	
タスク	**大分類**	情報セキュリティマネジメント	
	中分類	セキュリティ基準の策定	
	小分類	ソーシャルメディア使用に関するポリシー・ガイドラインの策定	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-14-2-7-01	社員のソーシャルメディア使用に関するルールを策定できる
関連するタスク		(仮)T-12-8-17（利用者管理）：従業員が発信する電子メールの内容確認、閲覧するサイトの管理、機器の持ち出し・持ち込み管理等を行う T-18-6-1（利用者教育）：情報利用者の教育を実施	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		43	
タスクコード		(仮)T-14-2-8	
タスク	**大分類**	情報セキュリティマネジメント	
	中分類	セキュリティ基準の策定	
	小分類	アウトソース先の選定・管理のためのセキュリティ基準の策定	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-14-2-8-01	アウトソース先のセキュリティ基準を策定できる
関連するタスク		(仮)T-12-8-13（アウトソース管理）：セキュリティ基準に基づき、アウトソース選定時及び継続時におけるセキュリティ実施状況の有効性を検証	
作成根拠		UISS 作業委員会（小分類名変更）	
見直しの内容		小分類の追加	

<table>
<tr><td colspan="2">整理番号</td><td colspan="2">44</td></tr>
<tr><td colspan="2">タスクコード</td><td colspan="2">(仮)T-14-2-9</td></tr>
<tr><td rowspan="3">タスク</td><td>大分類</td><td colspan="2">情報セキュリティマネジメント</td></tr>
<tr><td>中分類</td><td colspan="2">セキュリティ基準の策定</td></tr>
<tr><td>小分類</td><td colspan="2">電子証明書利用手続きの策定</td></tr>
<tr><td colspan="2" rowspan="3">スキル項目</td><td>スキルコード</td><td>スキル項目定義</td></tr>
<tr><td>(仮)S-14-2-9-01</td><td>電子データの信頼性を確保するために、第三者機関が発行する電子証明書と自社が発行する電子証明書をそれぞれ利用する手続きを策定することができる</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">関連するタスク</td><td colspan="2">(仮)T-12-8-14（第三者機関電子証明書の申請、期限管理、更新）：第三者機関が発行する電子証明書を申請して入手し、その有効期限を管理し、期限切れになる前に更新手続きを行う
(仮)T-12-8-15（自社電子証明書の企画、設計）：自社で発行する電子証明書について、その発行業務を企画し、発行手続きを定める
(仮)T-12-8-16（自社電子証明書の発行、期限管理、更新）：自社で発行する電子証明書について、その発行を管理し、それぞれの電子証明書の有効期限を管理し、期限切れになる前に更新手続きが必要なことを通知する</td></tr>
<tr><td colspan="2">作成根拠</td><td colspan="2">UISS 作業委員会</td></tr>
<tr><td colspan="2">見直しの内容</td><td colspan="2">小分類の追加</td></tr>
</table>

整理番号		45	
タスクコード		(仮)T-14-3-6	
タスク	大分類	情報セキュリティマネジメント	
	中分類	セキュリティの見直し	
	小分類	リスク対策が適切に行われていることのレビュー	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-3-6-01	情報保証において、リスクのレベルが各ソフトウェアアプリケーション、システム及びネットワークにおいて許容範囲内であることを確認するためのレビューを行うことができる
関連するタスク		(仮)T-12-8-9（リスクのレベルに関する継続的な検査）: 情報保証において、ソフトウェアアプリケーション、ネットワークまたはシステムのリスクのレベルが許容範囲内であるかどうかを、観測結果をもとに継続的に検査	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

整理番号		46	
タスクコード		(仮)T-14-3-7	
タスク	大分類	情報セキュリティマネジメント	
	中分類	セキュリティの見直し	
	小分類	非遵守事項のインパクト分析	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-3-7-01	非遵守事項が情報セキュリティにどのような影響を及ぼすかを導き出せる
関連するタスク		T-14-1-4（対策の整理と調査）：対策が現状どの程度実施されているかどうか調査、整理する T-14-3-2（運用上の問題点整理と分析）：違反者の多い基準を収集、整理する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

整理番号		47	
タスクコード		(仮)T-14-3-8	
タスク	大分類	情報セキュリティマネジメント	
	中分類	セキュリティの見直し	
	小分類	監査指摘事項への対応	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-3-8-01	適切な緩和策を確実に実施するための監査指摘事項と勧告の追跡を行うことができる
関連するタスク		T-14-3-2（運用上の問題点整理と分析）：整理された問題点について、セキュリティポリシー変更に対する分析を行い、ポリシーの見直しを行う T-14-3-3（技術上の問題点整理と分析）：整理された問題点について、セキュリティポリシー変更に対する分析を行い、ポリシーの見直しを行う	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

整理番号		48	
タスクコード		(仮)T-14-3-9	
タスク	大分類	情報セキュリティマネジメント	
	中分類	セキュリティの見直し	
	小分類	改善状況の検証	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-3-9-01	セキュリティ対策に関する改善策が確実に実施されていることを確認する
関連するタスク		T-14-3-5（セキュリティポリシーの更新）：分析結果からポリシー変更部分について、再度リスク分析を行い、ポリシーを更新する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

整理番号		49	
タスクコード		(仮)T-14-4-1	
タスク	大分類	情報セキュリティマネジメント	
	中分類	情報セキュリティガバナンス	
	小分類	リスクガバナンスプロセスへの関与	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-1-01	セキュリティリスク、緩和策、及び他の技術リスクを扱うリスクガバナンスのプロセスに関与する
関連するタスク		(仮)T-1.4-1-3（EA の推進（EA プロセスの統括)）: 経営戦略に準じた組織全体の改善サイクルとなるよう各 EA（BA,DA,AA,TA）開発組織を統轄する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		中分類の追加	

整理番号		50	
タスクコード		(仮)T-14-4-10	
タスク	大分類	情報セキュリティマネジメント	
	中分類	情報セキュリティガバナンス	
	小分類	現場部門における戦略に対応したプロセスの実行	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-10-01	現場部門において、企画部門の戦略立案に対応したプロセスを実施させることができる
関連するタスク		T-14-2-1（企業活動のセキュリティ規定の作成）：企業セキュリティ方針の策定で整理された対策を基準に網羅する	
作成根拠		ITSS 作業委員会での委員指摘	
見直しの内容		中分類の追加	

整理番号		51	
タスクコード		(仮)T-14-4-11	
タスク	大分類	情報セキュリティマネジメント	
	中分類	調達におけるセキュリティ要件の反映	
	小分類	調達要件におけるセキュリティ関連事項の策定	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-11-01	必要なセキュリティレベルを確保するために満足すべきセキュリティ対策に関する要件を、システム及びサービスの調達要件に反映させることができる
関連するタスク		T-10.2-9-1（セキュリティ製品の選定および導入）：企業の情報システムやネットワークの構成要素を識別し、それぞれの構成要素に対してセキュリティ製品を選択し導入する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		中分類の追加	

整理番号		52	
タスクコード		(仮)T-14-4-12	
タスク	大分類	情報セキュリティマネジメント	
	中分類	検査の実施	
	小分類	ネットワーク環境に適した検査の実施	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-12-01	組織で実施する検査、テスト、レビューを、ネットワーク環境に適した形で確実に実施させることができる
関連するタスク		T-10.2-5-1（ネットワークシステムの設計）：信頼性対策を費用対効果、実現の可能性を評価の上でネットワークアーキテクチャ、セキュリティ対策、シナリオを作成する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		中分類の追加	

整理番号		53	
タスクコード		(仮)T-14-4-2	
タスク	大分類	情報セキュリティマネジメント	
	中分類	情報セキュリティガバナンス	
	小分類	情報セキュリティ対策に関する関係者との連携	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-2-01	組織の目標の達成に向けて組織管理者と連携できる
関連するタスク		(仮)T-12-8-8（業務機能に関する識別と優先度の設定）：組織内の関係者との連携のもとで、重要な業務機能を識別し、優先度を設定する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		中分類の追加	

整理番号		54	
タスクコード		(仮)T-14-4-3	
タスク	大分類	情報セキュリティマネジメント	
	中分類	情報セキュリティガバナンス	
	小分類	情報セキュリティ予算、要員、契約の主導	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-3-01	情報セキュリティ予算、要員、契約について主導・監督する
関連するタスク		(仮)T-14-4-4（セキュリティ管理に必要なリソースの確保）：セキュアな運用と情報保全の維持に必要なリソースを確保する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		中分類の追加	

整理番号		55	
タスクコード		(仮)T-14-4-4	
タスク	大分類	情報セキュリティマネジメント	
	中分類	情報セキュリティガバナンス	
	小分類	セキュリティ管理に必要なリソースの確保	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-4-01	セキュアな運用と情報保全の維持に必要なリソースを確保することができる
関連するタスク		(仮)T-14-4-3（情報セキュリティ予算、要員、契約の主導）：情報セキュリティ予算、要員、契約について主導・監督する (仮)T-16-2-9（事業継続のためのリソースの獲得）：事業継続のための財政措置を含む必要なリソースを確保する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		中分類の追加	

整理番号		56	
タスクコード		(仮)T-14-4-5	
タスク	大分類	情報セキュリティマネジメント	
	中分類	情報セキュリティガバナンス	
	小分類	認定ないし保証されたセキュリティ対策の実施状況に関する最新の文書の入手と利用	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-5-01	認定ないし保証されたセキュリティ対策の実施状況に関する最新の文書を入手し、利用することができる
関連するタスク		(仮)T-12-8-18（情報システムの保証と認定の維持に必要な対策の実施）: 情報保証において、情報システムに関する保証と認定を維持するために必要な対策を講じて、これらの保証と認定を維持する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		中分類の追加	

整理番号		57	
タスクコード		(仮)T-14-4-6	
タスク	大分類	情報セキュリティマネジメント	
	中分類	情報セキュリティガバナンス	
	小分類	情報セキュリティに関する関係者との情報交換	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-6-01	組織内のざまざまな関係者と情報セキュリティ対策の在り方について意見交換することができる
関連するタスク		(仮)T-12-8-11（他組織との情報交換）：インシデント対応とコンピュータネットワーク防御に関して、外部組織と情報交換を行う	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		中分類の追加	

整理番号		58	
タスクコード		(仮)T-14-4-7	
タスク	大分類	情報セキュリティマネジメント	
	中分類	情報セキュリティガバナンス	
	小分類	識別された脆弱性への対策	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-7-01	リスクアセスメント、監査、検査を通じて識別された脆弱性に対して、適切な対策を講じることができる
関連するタスク		(仮)T-10.2-3-11（脆弱性に対する対策方針の決定）：システムに存在する脆弱性について、その対策と緩和のための取り組みの方針を決定する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		中分類の追加	

整理番号		59	
タスクコード		(仮)T-14-4-8	
タスク	大分類	情報セキュリティマネジメント	
	中分類	情報セキュリティガバナンス	
	小分類	緊急時の判断権限の発揮	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-8-01	予め緊急時の対応について権限を委任され、必要な対処を行う
関連するタスク		T-12-5-2（事故の検知）：事故の初動処理に対する手続きを文書化する	
作成根拠		NISC 調査をもとに追加	
見直しの内容		中分類の追加	

整理番号		60	
タスクコード		(仮)T-14-4-9	
タスク	大分類	情報セキュリティマネジメント	
	中分類	情報セキュリティガバナンス	
	小分類	セキュリティリスクに対する組織的対応	
スキル項目		スキルコード	スキル項目定義
		(仮)S-14-4-9-01	セキュリティリスクの分析結果を、組織設計、職務分掌、業務プロセス定義等に反映させる
関連するタスク		T-14-1-6（セキュリティ方針・体制の策定）：セキュリティ対策の目的、適用範囲、達成レベル、対策基準の方針、情報セキュリティの責任者、経営者／従業員の遵守事項、組織または実施体制、運用、罰則、公開、見直しについて記述する	
作成根拠		ITSS 作業委員会での委員指摘	
見直しの内容		中分類の追加	

整理番号		61	
タスクコード		(仮)T-16-1-10	
タスク	大分類	事業継続計画	
	中分類	事業継続計画策定	
	小分類	情報セキュリティに関するガイダンスの提供	
スキル項目		スキルコード	スキル項目定義
		(仮)S-16-1-10-01	事業継続計画の作成のための情報セキュリティに関するガイダンスを提供することができる
関連するタスク		(仮)T-14-2-10（情報ネットワークのセキュリティ対策のためのガイダンス文書の作成管理）：情報ネットワークのセキュリティ対策のためのガイダンス文書の発行管理を行う	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

整理番号		62	
タスクコード		(仮)T-16-2-8	
タスク	大分類	事業継続計画	
	中分類	IT 災害継続・復旧計画の作成	
	小分類	資産評価結果に基づく災害時対応計画の策定	
スキル項目		スキルコード	スキル項目定義
		(仮)S-16-2-8-01	情報資産の評価結果を踏まえた災害時対応計画が策定できる
関連するタスク		(仮)T-8.1-3-8（設計段階におけるセキュリティ要件の定義：実装すべきセキュリティの要件（障害発生時の復旧時間の許容時間、データ復旧範囲など、障害対応に関する要件を含む)、レベル感、考慮点等を明確にすることができる。	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		63	
タスクコード		(仮)T-16-2-9	
タスク	大分類	事業継続計画	
	中分類	IT 災害継続・復旧計画の作成	
	小分類	事業継続のためのリソースの獲得	
スキル項目		スキルコード	スキル項目定義
		(仮)S-16-2-9-01	事業継続のための財政措置を含む必要なリソースを確保することができる
関連するタスク		(仮)T-14-4-4（セキュリティ管理に必要なリソースの確保）：セキュアな運用と情報保全の維持に必要なリソースを確保する	
作成根拠		NICE タスク定義をもとに追加	
見直しの内容		小分類の追加	

整理番号		64	
タスクコード		(仮)T-18-6-3	
タスク	大分類	人的資源管理（人材育成）	
	中分類	情報セキュリティ	
	小分類	セキュリティインシデントに関する教育	
スキル項目		スキルコード	スキル項目定義
		(仮)S-18-6-3-01	セキュリティインシデントがもたらす社会的影響を従業員に理解させることができる
関連するタスク		T-18-6-1（利用者教育）：セキュリティ技術者の教育を実施できる	
作成根拠		ITSS 作業委員会での委員指摘	
見直しの内容		小分類の追加	

整理番号		65	
タスクコード		(仮)T-19-1-3	
タスク	大分類	システム監査	
	中分類	システム監査の計画	
	小分類	外部監査計画の作成	
スキル項目		スキルコード	スキル項目定義
		(仮)S-19-1-3-01	J-SOX 監査等、外部監査に関する実施計画・改善計画が策定できる
関連するタスク		(仮)T-19-2-9（外部監査計画の実施対応）：J-SOX 等、外部監査に対応	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		66	
タスクコード		(仮)T-19-2-9	
タスク	大分類	システム監査	
	中分類	システム監査の実施	
	小分類	外部監査計画の実施対応	
スキル項目		スキルコード	スキル項目定義
		(仮)S-19-2-9-01	J-SOX 等、外部監査に対応できる
関連するタスク		(仮)T-19-1-3（外部監査計画の作成）: J-SOX 監査等、外部監査に関する実施計画・改善計画を策定	
作成根拠		UISS 作業委員会	
見直しの内容		小分類の追加	

整理番号		67	
タスクコード		(仮)T-20-1-1	
タスク	**大分類**	（未定）	
	中分類	コンピュータ・フォレンジック	
	小分類	証拠証跡の特定	
スキル項目		**スキルコード**	**スキル項目定義**
		(仮)S-20-1-1-01	インシデント等の証拠・証跡となる情報を特定できる
関連するタスク		(仮)T-20-1-2（証拠証跡の分析）：インシデント等の証拠・証跡となる情報を特定	
作成根拠		ISEPA 職種定義をもとに追加	
見直しの内容		中分類の追加	

整理番号		68	
タスクコード		(仮)T-20-1-2	
タスク	大分類	（未定）	
	中分類	コンピュータ・フォレンジック	
	小分類	証拠証跡の分析	
スキル項目		スキルコード	スキル項目定義
		(仮)S-20-1-2-01	証拠・証跡として利用可能な情報を分析し、証拠性が担保可能かどうかを判断できる
関連するタスク		(仮)T-19-1-3（証拠証跡の特定）：インシデント等の証拠・証跡となる情報を特定	
作成根拠		ISEPA 職種定義をもとに追加	
見直しの内容		中分類の追加	

<table>
<tr><td colspan="2">整理番号</td><td colspan="2">69</td></tr>
<tr><td colspan="2">タスクコード</td><td colspan="2">(仮)T-20-1-3</td></tr>
<tr><td rowspan="3">タスク</td><td>大分類</td><td colspan="2">（未定）</td></tr>
<tr><td>中分類</td><td colspan="2">コンピュータ・フォレンジック</td></tr>
<tr><td>小分類</td><td colspan="2">証拠保全</td></tr>
<tr><td colspan="2" rowspan="3">スキル項目</td><td>スキルコード</td><td>スキル項目定義</td></tr>
<tr><td>(仮)S-20-1-3-01</td><td>証拠・証跡となる情報を改変されないように保全できる</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">関連するタスク</td><td colspan="2">(仮)T-20-1-4（証拠開示手続き）：外部に保存されている情報について、フォレンジックス遂行の目的で情報の開示手続きを行う</td></tr>
<tr><td colspan="2">作成根拠</td><td colspan="2">ISEPA 職種定義をもとに追加</td></tr>
<tr><td colspan="2">見直しの内容</td><td colspan="2">中分類の追加</td></tr>
</table>

整理番号		70	
タスクコード		(仮)T-20-1-4	
タスク	大分類	（未定）	
	中分類	コンピュータ・フォレンジック	
	小分類	証拠開示手続き	
スキル項目		スキルコード	スキル項目定義
		(仮)S-20-1-4-01	外部に保存されている情報について、フォレンジックス遂行の目的で情報の開示手続きを行うことができる
関連するタスク		(仮)T-20-1-3（証拠保全）：証拠・証跡となる情報を改変されないように保全	
作成根拠		ISEPA 職種定義をもとに追加	
見直しの内容		中分類の追加	

整理番号		71	
タスクコード		(仮)T-99-1-1	
タスク	大分類	（未定）	
	中分類	（未定）	
	小分類	セキュリティ当事者のメンタルケア	
スキル項目		スキルコード	スキル項目定義
		(仮)S-99-1-1-01	セキュリティ障害の当事者（被害者やセキュリティ障害の発端となってしまった人）のメンタルケアに当たることができる
関連するタスク		(仮)T-12-8-17（利用者管理）：従業員が発信する電子メールの内容確認、閲覧するサイトの管理、機器の持ち出し・持ち込み管理等を行う	
作成根拠		UISS 作業委員会	
見直しの内容		（保留）	

第３章　情報セキュリティに関するタスクとスキル標準見直し案との対応関係

情報セキュリティに関するタスクとスキル標準見直し案との対応

CCSFタスクと追加項目
（水色の項目は追加されたタスク）

表中「1」はコアタスク　（人材像が責任を持つ主たる担当領域のタスク）
「2」は非コアタスク　（人材像が関わる必要のある従たる担当領域のタスク）

	大分類	情報セキュリティに関するタスク（中分類or小分類）	具体的タスク（★は情報保証に必要なタスク）	タスクについての補足説明	ITSS マーケティング（参考）	ITSS セールス（タスクの追加）	ITSS コンサルタント インダストリ（タスクの追加）	ITSS コンサルタント ビジネスファンクション（タスクの追加）	ITSS コンサルタント 情報リスクマネジメント【追加】	ITSS ITアーキテクト アプリケーションアーキテクチャ（タスクの追加）	ITSS ITアーキテクト インテグレーションアーキテクチャ（タスクの追加）	ITSS ITアーキテクト インフラストラクチャアーキテクチャ（タスクの追加）	ITSS ITアーキテクト セキュリティアーキテクチャ【追加】	ITSS プロジェクトマネジメント（参考）	ITSS ITS セキュリティ（タスクの追加）	ITSS アプリケーションスペシャリスト（タスクの追加）	ITSS ソフトウェアディベロップメント（タスクの追加）	ITSS カスタマサービス（参考）	ITSS ITSM 運用管理（タスクの追加）	ITSS ITSM システム管理（タスクの追加）	ITSS ITSM オペレーション（タスクの追加）	UISS セキュリティ分野以外の既存の人材像 ビジネスストラテジスト（既存）	UISS ISストラテジスト（参考）	UISS プログラムマネージャ（参考）	UISS プロジェクトマネージャ（参考）	UISS ISアナリスト（参考）	UISS アプリケーションデザイナー（参考）	UISS システムデザイナー（参考）	UISS ISオペレーション（参考）	UISS ISアドミニストレータ（参考）	UISS ISアーキテクト（参考）	UISS ISスタッフ（事業継続計画）（参考）	UISS ISスタッフ（コンプライアンス）（参考）	UISS セキュリティアドミニストレータ 情報セキュリティアドミニストレータ【役割として明確化】	UISS セキュリティアドミニストレータ ISセキュリティアドミニストレータ【役割として明確化】	UISS セキュリティアドミニストレータ インシデントハンドラ【役割として明確化】	UISS ISオーディタ ISオーディタ（既存）	ETSS プロジェクトマネージャ（参考）	ETSS ドメインスペシャリスト（タスクの追加）	ETSS システムアーキテクト（タスクの追加）	ETSS ソフトウェアエンジニア（タスクの追加）	ETSS ブリッジSE（参考）	ETSS 開発環境エンジニア（タスクの追加）	ETSS 開発プロセス改善スペシャリスト（参考）	ETSS QAスペシャリスト（参考）	ETSS セキュリティマネージャ【追加】組込みセキュリティ
1.1	事業戦略>事業戦略策定					1	1	1														1	2																							
1.2	事業戦略>IT事業戦略策定						1	1																																						
1.3	事業戦略>事業戦略評価						1	1														1	2																							
1.4	事業戦略>情報セキュリティ戦略	情報セキュリティ戦略の策定	最新技術動向の調査・分析				1	1	1																									1												
			情報セキュリティ戦略実行体制の確立				1	1	1																									1												
			EAの推進（EAプロセスの統括）				1	1	1																									1												
			委託先管理				1	1	1																									1												
2	IT戦略						1	1	1													2	1	2																						
3	IT戦略実行マネジメント	IT戦略実現上のリスクへの対応	リスクの管理																				2	1										2												
			対策策定																				2	1										2												
			調整等対応策の実施																				2	1										2												
4	標準の維持・管理と品質管理	品質保証	品質管理基準の設定							1	1	1	1															2			1				2										2	1	2
			品質統制プロセスの運営							1	1	1	1															2			1				2										2	1	2
			評価のフィードバック							1	1	1	1															2			1				2										2	1	2
		標準の維持管理	標準化した妥当性確認（テスト）の実施管理							1	1	1	1																						1										1	1	1
			標準化したレビュープロセスの実施管理							1	1	1	1																						1										1	1	1
			標準化した改善プロセスの実施管理							1	1	1	1																						1										1	1	1
5	営業・調達活動	ソリューション提案／戦略立案	リスク計画			1			2																										1												2
			戦略立案	顧客のセキュリティ基準、監査基準に適合した提案の実施		1			2																										1												2
		委託先の選定	セキュリティの調査			1										2			2	2															1												2
6	契約管理	―																														1			1												2
7	プロジェクトマネジメント	プロジェクト計画策定	品質保証計画											1											1	2									2			1		2		1		2		1
			リスク管理計画											1											1	2									2			1		2		1		2		1
		プロジェクト追跡と実行管理	品質管理											1											1	2									2			1				1		2		1
			リスク管理											1											1	2									2			1				1		2		1
8	ITシステム企画	システム計画の立案	サービスレベルと品質に関する基本方針の明確化							1	1	1	1																						1					2						2
		システム化計画の具体化	システム要件の定義							1	1	1	1																						1					2						2
			情報セキュリティアーキテクチャの設計							1	1	1	1																		1									2						2
			設計段階におけるセキュリティ要件の定義							1	1	1	1																		1									2						2
			セキュリティ設計仕様書の作成							1	1	1	1																		1									2						2
			セキュリティ設計仕様書へのセキュリティポリシー等の反映							1	1	1	1																		1									2						2
			情報技術の変化に応じたセキュリティ要件の見直し							1	1	1	1																		1									2						2
9	システム要件定義	システム化要件の定義	要求事項の分析・調査							1	1	1	1		2	2									2	2	2	1	2	2									1	1		1		1		2
		システムアーキテクチャ設計	適用製品の評価・選定							1	1	1	1		2	2									2	2	2	1	2	2									1	1		1		1		2
10.1	システム開発・構築>アプリケーションシステム	アプリケーション開発	ソフトウェアコード作成	セキュリティホール対策を踏まえたセキュアプログラミングの実施						2						1									2	2	1	2	2	2																
10.2	システム開発・構築>基盤システム	システム設計（セキュリティ）	認証と権限のコントロール								2	2			1	2												1													1		1			1
			物理セキュリティのコントロール								2	2			1	2												1													1		1			1
			論理セキュリティのコントロール								2	2			1	2												1													1		1			1
			ネットワーク基盤上データの信頼性確保								2	2			1	2												1													1		1			1
			ネットワーク基盤を経由しない攻撃等に対するデータの信頼性確保								2	2			1	2												1													1		1			1
			データの機密保持								2	2			1	2												1													1		1			1
			セキュリティ運用手続きの作成								2	2			1	2												1													1		1			1
			情報セキュリティアーキテクチャと対策との整合性確保								2	2			1	2												1													1		1			1
			新技術等への対応状況の分析								2	2			1	2												1													1		1			1
			形式手法を用いたソフトウェアシステムの設計、開発、ならびに修正								2	2			1	2												1													1		1			1
			脆弱性に対する対策方針の決定								2	2			1	2												1													1		1			1
			セキュリティ、回復力、及び信頼性に関する対策の提言★								2	2			2	2												1													2		2			2
			セキュリティ体制、能力及び脆弱性に関する評価結果の文書化★								2	2			2	2												1													2		2			2
			運用計画へのセキュリティ対策の反映								2	2			1	2												1													1		1			1
		システム設計（ネットワーク）	ネットワークシステムの設計								2	2			2	2									2	2	2	1	2	2												1		1			
			セキュリティ製品の選定および導入								2	2			1	2									2	2	2	1	2	2												1		1			1
			セキュリティシステムの開発								2	2			1	2												1													1		1			1
			セキュリティ要件実装												1	2												1													1		1			1
		構築・テスト（セキュリティ）	セキュリティ評価の実施												1	2												1													1		1			1

CCSFタスクと追加項目
（水色の項目は追加されたタスク）

表中「1」はコアタスク （人材像が責任を持つ主たる担当領域のタスク）
「2」は非コアタスク （人材像が関わる必要のある従たる担当領域のタスク）

	大分類	情報セキュリティに関するタスク（中分類or小分類）	具体的タスク（★は情報保証に必要なタスク）	タスクについての補足説明	ITSS マーケティング（参考）	ITSS セールス（タスクの追加）	ITSS コンサルタント インダストリ（タスクの追加）	ITSS コンサルタント ビジネスファンクション（タスクの追加）	ITSS コンサルタント 情報リスクマネジメント【追加】	ITSS ITアーキテクト アプリケーションアーキテクチャ（タスクの追加）	ITSS ITアーキテクト インテグレーションアーキテクチャ（タスクの追加）	ITSS ITアーキテクト インフラストラクチャアーキテクチャ（タスクの追加）	ITSS ITアーキテクト セキュリティアーキテクチャ【追加】	ITSS プロジェクトマネジメント（参考）	ITSS ITS セキュリティ（タスクの追加）	ITSS アプリケーションスペシャリスト（タスクの追加）	ITSS ソフトウェアデベロップメント（タスクの追加）	ITSS カスタマサービス（参考）	ITSS ITSM 運用管理（タスクの追加）	ITSS ITSM システム管理（タスクの追加）	ITSS ITSM オペレーション（タスクの追加）	UISS セキュリティ分野以外の既存の人材像 ビジネスストラテジスト（既存）	UISS ISストラテジスト（参考）	UISS プログラムマネージャ（参考）	UISS プロジェクトマネージャ（参考）	UISS ISアナリスト（参考）	UISS アプリケーションデザイナー（参考）	UISS システムデザイナー（参考）	UISS ISオペレーション（参考）	UISS ISアドミニストレータ（参考）	UISS ISアーキテクト（参考）	UISS ISスタッフ（事業継続計画）（参考）	UISS ISスタッフ（コンプライアンス）（参考）	UISS セキュリティアドミニストレータ 情報セキュリティアドミニストレータ【役割として明確化】	UISS セキュリティアドミニストレータ ISセキュリティアドミニストレータ【役割として明確化】	UISS セキュリティアドミニストレータ インシデントハンドラ【役割として明確化】	UISS ISオーディタ ISオーディタ（既存）	ETSS プロジェクトマネージャ（参考）	ETSS ドメインスペシャリスト（タスクの追加）	ETSS システムアーキテクト（タスクの追加）	ETSS ソフトウェアエンジニア（タスクの追加）	ETSS ブリッジSE（参考）	ETSS 開発環境エンジニア（タスクの追加）	ETSS 開発プロセス改善スペシャリスト（参考）	ETSS QAスペシャリスト（参考）	ETSS セキュリティマネージャ【追加】組込みセキュリティ
		構築・テスト（セキュリティ）	セキュリティ、回復力、信頼性の要件に関するシステムの適合性の評価★												2	2												1													2		2			2
			対策の実施に関する取組みの実施状況の確認★												2	2												1													2		2			2
			セキュリティ実装の確認												1	2												1													1		1			1
10.3	システム開発・構築>ソフトウェア製品	ソフトウェア開発	ソフトウェアコード作成	セキュリティホール対策を踏まえたセキュアプログラミングの実施													1																								1		1			2
10.4	システム開発・構築>システム受入・導入	－													1	1									2	2	1	1	2	2											1		1			
11	システム保守	－													1	1		1									1	1	2	2																
12	システム運用	セキュリティ障害管理	事故の検知												2	2			1	1	1						2	2	1																	
			事故の初動処理												2	2			1	1	1						2	2	2								1										
			事故の分析												2	2			1	1	1						2	2	2								1										
			事故からの復旧												2	2			1	1	1						2	2	2								1										
			再発防止策の実施												2	2			1	1	1						2	2	2								1										
			セキュリティの評価												2	2			1	1	1						2	2	2								1										
		セキュリティ管理	セキュリティ侵害の監視と状況分析												2	2			1	1	1						2	2	2								1										
			セキュリティ強度の確認												2	2			1	1	1						2	2	1							2											
			セキュリティ監査対応												2	2			1	1	1						2	2	1							2											
			セキュリティ対策の実施												2	2			1	1	1						2	2	1							2											
			セキュリティ障害管理												2	2			1	1	1								1							2											
			手続とガイドラインのポリシーへの準拠状況の監視												2	2			1	1	1								1							2											
			実行中のサービスからの要求の予測に基づくセキュリティ上の前提条件についての評価												2	2			1	1	1								1							2											
			業務機能に関する識別と優先度の設定												2	2			1	1	1								1							2											
			リスクのレベルに関する継続的な検査★												2	2			2	2	2								1							2											
			上位者または本部組織への報告												2	2			1	1	1								1							2											
			他組織との情報交換												2	2			1	1	2								1							2											
			適用基準に則ったセキュリティパッチ適用												2	2			1	1	1								1							2											
			アウトソース管理												2	2			1	1	1								1							2											
			第三者機関電子証明書の申請、期限管理、更新												2	2			1	1	1								1							2											
			自社電子証明書の発行、期限管理、更新												2	2			1	1	1								1							2											
			利用者管理												2	2			1	1	1								1							2											
			情報システムの保証と認定の維持に必要な対策の実施★												2	2			2	2	2								1							2											
13	コンプライアンス	管理方針と体制	法令及び規範の管理体制確立						2																								1													
			管理責任者の選定						2																								1													
			遵守すべき法令及び規範の識別						2																								1													
			情報倫理規定の策定						2																								1													
			個人情報保護						2																								1													
			知的財産権保護						2																								1													
			外部データ提供管理方針						2																								1													
		実施・評価	教育・周知徹底						2																								1													
			遵守状況の評価と改善						2																								1													
		セキュリティ方針の策定	情報資産の評価						2						2																				1											2
			脅威の認識						2						2																				1											2
			リスクの識別						2						2																				1											2
			対策の整理と調査						2						2																				1											2
			リスクの評価						2						2																				1											2
			セキュリティ方針・体制の策定						2																										1											2
			ポリシー案の承認						2																										1											2
			代替案の分析						2																										1											2
			企業活動のセキュリティ規定の作成						2																										1											2
			情報システムのセキュリティ規定の作成						2																										1											2
			物理的保護レベルの定義						2																										1											2
		セキュリティ基準の策定	セキュリティ計画の立案						2																										1											2
			ソリューション提案						2																										1											2
			パッチマネジメント基準の策定						2																										1											2
			ソーシャルメディア使用に関するポリシー・ガイドラインの策定						2																										1											2
			アウトソース先の選定・管理のためのセキュリティ基準の策定						2																										1											2
			電子証明書利用手続きの策定						2																										1											2

CCSFタスクと追加項目
（水色の項目は追加されたタスク）

表中「1」はコアタスク（人材像が責任を持つ主たる担当領域のタスク）
「2」は非コアタスク（人材像が関わる必要のある従たる担当領域のタスク）

					ITSS																	UISS																ETSS								
							コンサルタント			IT アーキテクト					ITS				ITSM			セキュリティ分野以外の既存の人材像												セキュリティアドミニストレータ			ISオーディタ									
					マーケティング	セールス	インダストリ	ビジネスファンクション	情報リスクマネジメント	アプリケーションアーキテクチャ	インテグレーションアーキテクチャ	インフラストラクチャアーキテクチャ	セキュリティアーキテクチャ	プロジェクトマネジメント	セキュリティ	アプリケーションスペシャリスト	ソフトウェアディベロップメント	カスタマサービス	運用管理	システム管理	オペレーション	ビジネスストラテジスト	ISストラテジスト	プログラムマネージャ	プロジェクトマネージャ	ISアナリスト	アプリケーションデザイナー	システムデザイナー	ISオペレーション	ISアドミニストレータ	ISアーキテクト	ISスタッフ(事業継続計画)	ISスタッフ(コンプライアンス)	情報セキュリティアドミニストレータ	ISセキュリティアドミニストレータ	インシデントハンドラ	ISオーディタ	プロジェクトマネージャ	ドメインスペシャリスト	システムアーキテクト	ソフトウェアエンジニア	ブリッジSE	開発環境エンジニア	開発プロセス改善スペシャリスト	QAスペシャリスト	セキュリティマネージャ
	大分類	情報セキュリティに関するタスク（中分類or小分類）	具体的タスク（★は情報保証に必要なタスク）	タスクについての補足説明	（参考）	（タスクの追加）	（タスクの追加）	（タスクの追加）	【追加】	（タスクの追加）	（タスクの追加）	（タスクの追加）	【追加】	（参考）	（タスクの追加）	（タスクの追加）	（タスクの追加）	（参考）	（タスクの追加）	（タスクの追加）	（タスクの追加）	（既存）	（参考）	（参考）	（参考）	（参考）	（参考）	（参考）	（参考）	（参考）	（参考）	（参考）	（参考）	【役割として明確化】	【役割として明確化】	【役割として明確化】	（既存）	（参考）	（タスクの追加）	（タスクの追加）	（タスクの追加）	（参考）	（タスクの追加）	（参考）	（参考）	【追加】組込みセキュリティ
14	情報セキュリティマネジメント		情報ネットワークのセキュリティ対策のためのガイダンス文書の作成管理						2																										1											2
		情報セキュリティガバナンス	リスクガバナンスプロセスへの関与						2																										1											2
			情報セキュリティ対策に関する関係者との連携						2																										1											2
			情報セキュリティ予算、要員、契約の主導						2																										1											2
			セキュリティ管理に必要なリソースの確保						2																										1											2
			認定ないし保証されたセキュリティ対策の実施状況に関する最新の文書の入手と利用						2																										1											2
			情報セキュリティに関する関係者との情報交換						2																										1											2
			識別された脆弱性への対策						2						2																				1											2
			緊急時の判断権限の発揮						2																										1											2
			セキュリティリスクに対する組織的対応						2																										1											2
			現場部門における戦略に対応したプロセスの実行						2																										1											2
		調達におけるセキュリティ要件の反映	調達要件におけるセキュリティ関連事項の策定													2			2	2															1											2
		検査の実施	ネットワーク環境に適した検査の実施												2																				1											2
		セキュリティの見直し	技術情報の収集と評価												2																				1											2
			運用上の問題点整理と分析																2	2															1											2
			技術上の問題点整理と分析												2																				1											2
			リスク対策が適切に行われていることのレビュー★						2																										1											2
			非遵守事項のインパクト分析						2																										1											2
			監査指摘事項への対応						2																										1											2
			改善状況の検証						2																										1											2
			新たなリスクの整理と分析						2						2																				1											2
			セキュリティポリシーの更新						2																										1											2
15	新ビジネス・新技術に関する研究・検証と支援	－								1	1	1	1			1	1																						1							
16	事業継続計画	事業継続計画策定	対象事故・災害のリスク分析(業務継続計画と事業ニーズの把握)						2																							1														
			事業継続計画の策定(事業継続計画策定と承認)						2																							1														
			情報セキュリティに関するガイダンスの提供						2																							1														
		IT災害継続・復旧計画の作成	資産評価結果に基づく災害時対応計画の策定						2																							1														
			緊急時対応体制						2																							1														
			事業継続のためのリソースの獲得						2																							1														
17	資産管理	－																																												
18	人的資源管理（人材育成）	情報セキュリティ	利用者向けの教育の実施												2																				2											
			セキュリティ技術者向けの教育の実施												2																				2											2
			セキュリティインシデントに関する教育												2																				2											
19	システム監査	システム監査の計画	基本計画の作成、実施環境の確保																																		1									
			個別計画書の作成																																		1									
			外部監査計画の作成																																		1									
		システム監査の実施	実施準備																																		1									
			予備調査																																		1									
			予備調査																																		1									
			監査手続書の作成																																		1									
			本調査																																		1									
			実施結果の記録（監査調書の作成）																																		1									
			監査意見の明確化																																		1									
			評価・結論の総合検討																																		1									
			監査報告書案																																		1									
			外部監査の実施対応																																		1									
		システム監査の報告	指摘事項の記載																																		1									
			改善勧告の記載																																		1									
			補足事項の記載																																		1									
			監査報告書の提出																																		1									
			監査報告会の開催																																		1									
			フォローアップの実施																																		1									
			年次監査報告書の作成																																		1									
		システム監査業務の管理	進捗管理																																		1									
			品質管理																																		1									
			監査業務の改善																																		1									
			監査体制の整備																																		1									
		証拠証跡の特定	インシデント等の証拠・証跡となる情報の特定												1																				2				2							
		証拠証跡の分析	分析に基づく証拠性の判断												1																				2				2							

CCSFタスクと追加項目 （水色の項目は追加されたタスク） 表中「1」はコアタスク （人材像が責任を持つ主たる担当領域のタスク） 「2」は非コアタスク （人材像が関わる必要のある従たる担当領域のタスク）				ITSS																						UISS																												ETSS										
				マーケティング	セールス	コンサルタント			ITアーキテクト				プロジェクトマネジメント	ITS				ITSM			セキュリティ分野以外の既存の人材像																					セキュリティアドミニストレータ		ISオーディタ																						
						インダストリ	ビジネスファンクション	情報リスクマネジメント	アプリケーションアーキテクチャ	インテグレーションアーキテクチャ	インフラストラクチャアーキテクチャ	セキュリティアーキテクチャ		セキュリティ	アプリケーションスペシャリスト	ソフトウェアディベロップメント	カスタマサービス	運用管理	システム管理	オペレーション	ビジネスストラテジスト	ISストラテジスト	プログラムマネージャ	プロジェクトマネージャ	ISアナリスト	アプリケーションデザイナー	システムデザイナー	ISオペレーション	ISアドミニストレータ	ISアーキテクト	ISスタッフ(事業継続計画)	ISスタッフ(コンプライアンス)	情報セキュリティアドミニストレータ	ISセキュリティアドミニストレータ	インシデントハンドラ	ISオーディタ	プロジェクトマネージャ	ドメインスペシャリスト	システムアーキテクト	ソフトウェアエンジニア	ブリッジSE	開発環境エンジニア	開発プロセス改善スペシャリスト	QAスペシャリスト	セキュリティマネージャ
	大分類	情報セキュリティに関するタスク（中分類or小分類）	具体的タスク （★は情報保証に必要なタスク）	タスクについての補足説明	（参考）	（タスクの追加）	（タスクの追加）	（タスクの追加）	【追加】	（タスクの追加）	（タスクの追加）	（タスクの追加）	【追加】	（参考）	（タスクの追加）	（タスクの追加）	（参考）	（タスクの追加）	（タスクの追加）	（タスクの追加）	（既存）	（参考）	（参考）	（参考）	（参考）	（参考）	（参考）	（参考）	（参考）	（参考）	（参考）	【役割として明確化】	【役割として明確化】	【役割として明確化】	（既存）	（参考）	（タスクの追加）	（タスクの追加）	（タスクの追加）	（参考）	（タスクの追加）	（参考）	（参考）	【追加】組込みセキュリティ
20	コンピュータ・フォレンジック	証拠保全	情報についての改変からの保全												1																							2				2												
		証拠開示手続き	外部に保存されている情報について、フォレンジックス遂行の目的で情報の開示手続きを行うことができる												1																							2				2												
ー	（現状では分類未定）		セキュリティ当事者のメンタルケア																																																				