別紙2 機能定義とNICE・NIST

セキュリティ機能一覧 & 機能分化プロセス			部門	主な機能概要	セキュリティ機能定義	機能を実現する役割	役割を担う作業要件	スキルセット
情報システム	システム構築	システム構築	IT企画	IT戦略	中期計画	コンプライアンス及び力バナンスの観点からのセキュリティ対策整合性の担保	情報収集・情報比較検討 企画立案・計画立案	
					年次計画	セキュリティ対策に係る実施計画	情報収集・情報比較検討 企画立案・計画立案	
					事業戦略 IT企画	各事業に対するIT導入・構築運用改善計画	情報収集・情報比較検討 企画立案・計画立案	
						ライセンス等を踏まえた、リプレース計画	情報収集・情報比較検討 企画立案・計画立案	
				システム企画	機能構想	ユーザビリティからの機能改善	情報収集・情報比較検討 要件定義	
						システムセキュリティからの機能改善	情報収集・情報比較検討 要件定義	
					コスト管理	セキュリティサービス・ツール導入に関するコスト管理	情報収集・情報比較検討	
				事業継続	IT-BCP	ICT環境における事業継続計画の策定	情報収集・情報比較検討 企画立案・計画立案	
				セキュリティ予防対策	ディザスタリカバリ	災害対策に関する改善計画	情報収集・情報比較検討 企画立案・計画立案	
						災害対策に関する稼働計画	情報収集・情報比較検討 要件定義・訓練	
					情報セキュリティ（ISMS）	情報セキュリティ改善計画	情報収集・情報比較検討 企画立案・計画立案	
						情報セキュリティ改善格闘	情報収集・情報比較検討 要件定義・訓練	
			調達	調達	調達	取引先選定	情報収集・情報比較検討	
						製品・サービス調達	情報収集・情報比較検討	
		インフラ構築	基幹システム構築	構築・実装	機能改善	パッチマネジメント計画	情報収集・情報比較検討 企画立案・計画立案	
						製品選定	情報収集・情報比較検討 企画立案・計画立案	
						セキュリティ対策におけるシステム的機能の継続的改善活動	情報収集・情報比較検討 計画立案・運用管理	
					導入・開発計画	セキュア設計（構築段階）	基本設計・詳細設計 導入計画・開発計画	
						セキュア設計（運用段階）	基本設計・詳細設計 導入計画・運用改善	
						多層防御に関する取り組み	基本設計・詳細設計 導入計画・運用改善	
			インフラ構築		製品品質管理	製品・サービス評価	情報収集・情報比較検討	
					セキュリティ対応プロジェクト	システム構築及び運用のセキュリティ対策に関するプロジェクトマネジメント	基本設計・詳細設計 導入計画・運用改善	
	システム運用	基幹システム運用	基幹システム運用	アプリケーション管理	アプリケーション バージョン管理	業務システムに関するバージョン管理	詳細設計 導入計画・運用改善	
			運用テスト	運用テスト	運用テスト パッチ管理	パッチマネジメントの実施 パッチ適用時のテスト実施	詳細設計 導入計画・運用改善	
		インフラ運用	インフラ運用	データベース管理	DB機器 ver管理	DB機器等に関するバージョン管理 クラウドサービス等のセキュリティ対策	詳細設計 導入計画・運用改善	
					DB機器 構成管理	データマネジメントに必要なDB管理（データ特性に合わせたDB構成	詳細設計 導入計画・運用改善	
					DBデータ セキュリティ	DB設定及び格納されるデータに対するセキュリティ対策	詳細設計 導入計画・運用改善	
				ネットワーク管理	通信環境管理 Firewall / WAF	ファイアウォール設定	詳細設計 導入計画・運用改善	
						WAF設定	詳細設計 導入計画・運用改善	
					通信監視 IDS / IPS	通信監視	詳細設計 導入計画・運用改善	
						通信遮断管理	詳細設計 導入計画・運用改善	
		権限管理	権限管理	権限管理	ID管理 アクセス権管理	ActiveDirectry管理 シングルサインオン管理	詳細設計 導入計画・運用改善	
						システム、フォルダ等アクセス権管理	詳細設計 導入計画・運用改善	
		システム監査	システム監査	システム監査	セキュリティ監査	情報セキュリティ監査、物理的セキュリティ監査	内部監査・改善計画	
					システム監査	システム監査	内部監査・改善計画	
			セキュリティ	セキュリティ事後対応	SOC	セキュリティオペレーション業務	詳細設計 導入計画・運用改善	
					CSIRT	コマンダー	企画立案・運用改善	
						インシデントハンドリング	運用改善・情報収集	
						脅威情報収集、対策情報収集	情報収集・情報分析	
						フォレンジックス	情報収集・情報分析	
						トレーニング	情報収集・情報比較検討 企画立案・計画立案	
		ユーザーサポート	ユーザーサポート	ユーザーサポート	ユーザーサポート	インシデント発生時の対応窓口	情報収集・運用改善	
				ヘルプデスク	ヘルプデスク	インシデント発生時の問合せ窓口	情報収集・運用改善	

NICE / サイバーセキュリティ教育イニシアティブ

セキュリティ（概念の）提供			運用・保守			守備・防衛			捜査			運用・情報収集			分析			監督と開発		
1	1	情報保証コンプライアンス										5	3	サイバーオペレーション計画						
1	1	情報保証コンプライアンス										5	3	サイバーオペレーション計画						
1	4	システム要件計画										5	1	情報収集オペレーション	6	3	ターゲット	7	1	教育と訓練
												5	3	サイバーオペレーション計画				7	2	情報システムセキュリティオペレーション
1	6	技術研究開発										5	1	情報収集オペレーション				7	3	法的助言と弁護
1	5	システムセキュリティアーキテクチャ																		
																		7	5	戦略的なポリシー策定
			2	2	データアドミニストレーション															
			2	3	ナレッジマネジメント															
1	1	情報保証コンプライアンス										5	1	情報収集オペレーション				7	1	教育と訓練
																		7	2	情報システムセキュリティオペレーション
																		7	3	法的助言と弁護
1	3	システム開発										5	3	サイバーオペレーション計画						
1	5	システムセキュリティアーキテクチャ																		
1	3	システム開発										5	3	サイバーオペレーション計画						
1	4	システム要件計画																		
1	5	システムセキュリティアーキテクチャ																		
			2	6	システムセキュリティ分析															
												5	2	サイバーオペレーション	6	1	全情報源の諜報活動	7	2	情報システムセキュリティオペレーション
1	2	ソフトウェア保証とエンジニアリング																7	2	情報システムセキュリティオペレーション
1	7	試験と評価	2	6	システムセキュリティ分析	3	4	脆弱性アセスメントと管理										7	2	情報システムセキュリティオペレーション
1	2	ソフトウェア保証とエンジニアリング	2	2	データアドミニストレーション													7	2	情報システムセキュリティオペレーション
			2	3	ナレッジマネジメント															
1	5	システムセキュリティアーキテクチャ																7	2	情報システムセキュリティオペレーション
			2	4	ネットワークサービス	3	1	コンピューター ネットワーク防御分析										7	2	情報システムセキュリティオペレーション
			2	5	システムアドミニストレーション	3	2	コンピューターネットワーク防御インフラ支援												
1	7	試験と評価	2	4	ネットワークサービス	3	1	コンピューター ネットワーク防御分析				5	1	情報収集オペレーション				7	2	情報システムセキュリティオペレーション
			2	5	システムアドミニストレーション	3	2	コンピューターネットワーク防御インフラ支援												
			2	3	ナレッジマネジメント															
1	5	システムセキュリティアーキテクチャ							4	2	接査							7	3	法的助言と弁護
									4	2	接査							7	3	法的助言と弁護
1	7	試験と評価	2	4	ネットワークサービス	3	1	コンピューター ネットワーク防御分析				5	1	情報収集オペレーション				7	2	情報システムセキュリティオペレーション
			2	5	システムアドミニストレーション	3	2	コンピューターネットワーク防御インフラ支援												
1	6	技術研究開発	2	3	ナレッジマネジメント	3	3	インシデントレスポンス				5	1	情報収集オペレーション	6	1	全情報源の諜報活動	7	1	教育と訓練
			2	6	システムセキュリティ分析	3	4	脆弱性アセスメントと管理	4	2	接査	5	2	サイバーオペレーション	6	2	エクスプロイト分析	7	2	情報システムセキュリティオペレーション
									4	2	接査				6	3	ターゲット			
									4	1	デジタルフォレンジック				6	4	脅威分析			
			2	1	カスタマーサポート&技術サポート													7	1	教育と訓練
			2	1	カスタマーサポート&技術サポート															

NIST / サイバーセキュリティフレームワーク

ID	特定	PR	防御	DE	検知	RS	対応	RC	復旧
BE	ビジネス環境								
BE	ビジネス環境					RP	対応計画の作成		
GV	ガバナンス	IP	情報を保護するためのプロセス及び手順			RP	対応計画の作成	RP	復旧計画の作成
RM	リスク管理戦略								
		IP	情報を保護するためのプロセス及び手順			CO	伝達	CO	伝達
BE	ビジネス環境					RP	対応計画の作成	RP	復旧計画の作成
AM	資産管理	IP	情報を保護するためのプロセス及び手順			RP	対応計画の作成	RP	復旧計画の作成
RM	リスク管理戦略								
AM	資産管理	IP	情報を保護するためのプロセス及び手順			RP	対応計画の作成	RP	復旧計画の作成
RM	リスク管理戦略	AT	意識向上およびトレーニング						
		PT	保護技術			CO	伝達	CO	伝達
						IM	改善	IM	改善
		PT	保護技術						
RM	リスク管理戦略	IP	情報を保護するためのプロセス及び手順	AE	異常とイベント	IM	改善	IM	改善
		PT	保護技術			IM	改善	IM	改善
		AT	意識向上およびトレーニング	AE	異常とイベント	IM	改善	IM	改善
		PT	保護技術			IM	改善	IM	改善
		MA	保守			IM	改善	IM	改善
		PT	保護技術			IM	改善	IM	改善
AM	資産管理	PT	保護技術	CM	セキュリティの継続的なモニタリング	IM	改善	CO	伝達
		MA	保守			CO	伝達	IM	改善
		PT	保護技術	AE	異常とイベント	IM	改善	CO	伝達
		MA	保守	CM	セキュリティの継続的なモニタリング	CO	伝達	IM	改善
AM	資産管理	AC	アクセス制御						
		DS	データセキュリティ						
		IP	情報を保護するためのプロセス及び手順					IM	改善
		IP	情報を保護するためのプロセス及び手順						
		MA	保守	CM	セキュリティの継続的なモニタリング	CO	伝達	CO	伝達
				AE	異常とイベント	AN	分析	IM	改善
				DP	検知プロセス				
RM	リスク管理戦略	MA	保守	AE	異常とイベント	RP	対応計画の作成	RP	復旧計画の作成
RA	リスクマネジメント	AT	意識向上およびトレーニング	CM	セキュリティの継続的なモニタリング	CO	伝達	CO	伝達
				DP	検知プロセス	AN	分析	IM	改善
						MI	提言		
						IM	改善		
		AT	意識向上およびトレーニング	AE	異常とイベント				
				CM	セキュリティの継続的なモニタリング				