情報セキュリティ研究開発戦略に関する技術課題見直しの概要

参考資料3

分類	重要テーマ名	技術課題（旧）	技術課題（見直し案）	見直しのポイント
情報通信システム全体のニュー・ディペンダビリティの確保				
①	実世界とコンピュータ内のモデル世界が融合した次世代ネットワークにおける情報セキュリティ基盤技術		仮想化ネットワークによるセキュリティ基盤の確立【新規】	・次世代ネットワークを実現する上で、仮想化技術が重要な位置づけにあるため、推進項目として独立化
		(a)センサーネットワークの情報セキュリティ基盤技術の研究開発	センサーネットワークの情報セキュリティ基盤の確立	
		(b)アドホックネットワークにおける利便性と安全性のバランスを考慮した情報セキュリティ基盤技術等の研究開発	アドホックネットワークの情報セキュリティ基盤の確立	
		(c)スマートフォンの情報セキュリティ基盤の開発	スマートフォンの情報セキュリティ基盤の開発	
②	システムのセキュリティ設定を上位から下位まで自動保証する技術	(a)情報セキュリティ・ポリシーやコンフィグレーションを管理するフレームワーク開発	システム構成の変化に対応したセキュリティポリシーの管理フレームワークの構築	・システム全体のコンフィグレーションの整合性をとるフレームワークと、自動検証技術を整理 ・脆弱性対策情報の流通とオートメーション化の国際動向を考慮し課題を独立化
		(b)形式手法等の技術を活用した自動検証技術の研究開発	システム全体のセキュリティポリシーを自動検証する機構の開発	
			脆弱性データベースと連携し、ソフトウェアの脆弱性の更新を効率化する仕様の開発【新規】	
③	障害に対する自動回復可能なコンピュータネットワーク構築技術	(a)ダイバーシティ・ネットワーク・アーキテクチャの研究開発	ネットワーク仮想化と計測技術の基盤確立	・次世代ネットワーク技術として、ネットワーク自体をプログラム可能とする技術動向を考慮して独立化
		(b)自己治癒型ネットワークの構築技術	多重化・冗長化ネットワークを活用した自動回復機能の実現	
			プログラマブルネットワークの基盤構築【新規】	
④	生体情報をコンピュータで管理するためのID管理と生体情報を統合するシステム設計構築技術	(a)OpenID をベースとしたミドルウェア・アーキテクチャの開発	ID統合のための共通仕様の開発	・OpenID等特定の技術に依存した記述を見直し
		(b)SAML等を活用してバイオメトリック・デバイスとのインタフェースやプロトコルを開発	生体情報とID管理の統合化のための共通仕様の開発	
		(c)バイオメトリクス認証技術の適合性評価を行う国際的なフレームワークの構築	バイオメトリクス認証技術の適合性評価を行う国際的なフレームワークの構築	
攻撃者の行動分析に基づくゼロデイ・ディフェンス				
⑤	攻撃者の行動分析等による予防基盤技術	(a)情報漏えいを起こす内部攻撃者やネットワークを介した外部攻撃者の行動観測によるプロファイリング	攻撃者の行動と攻撃手法の研究	・攻撃者の行動観測と攻撃に対するリスク低減に整理、明確化
		(b)攻撃者の行動モデル分析により、攻撃の公算や影響を予測し、対策の最適化を行う技術の研究開発	攻撃者のインセンティブと脅威の低減に関する研究	
⑥	大規模ネットワークにおける広域観測技術とマルウェアの挙動分析技術の統合	(a)広大なアドレス空間を効率的に観測する技術の研究開発	広域攻撃観測技術（マクロ的分析技術）	マクロ、ミクロのアプローチと、それらの組み合わせ技術に整理
		(b)マルウェアの自動検知技術及び自動対処技術（トラフィックの制御など）	マルウェア収集挙動分析技術（ミクロ的分析技術）	
			広域攻撃観測とマルウェア収集挙動分析を用いた統合解析技術【新規】	

分類	重要テーマ名	技術課題（旧）	技術課題（見直し案）	見直しのポイント
個人情報等の柔軟管理の実現				
⑦	個人情報等の利活用を促進する自己情報の統制技術	(a)利用者ごとにプライバシー保護レベルやポリシーを柔軟に設定するシステムの開発	プライバシー保護に関する多様な要求レベルを柔軟に管理する手法の確立	・プライバシー保護に関する多様な要求対応と、プライバシーデータの安全な計算、クラウドに整理、統合
		(b)プライバシーを保護したまま有用なデータを計算するための秘密計算	プライバシーを保護したまま有用情報を抽出する技術の開発【統合】	
		(c)プライバシー保護データマイニング等の基礎的研究		
		(d)クラウドに係わる情報セキュリティ課題の研究開発	クラウド環境におけるプライバシー保護技術の確立	
⑧	フォレンジック等を支援するためのデータ管理・追跡技術	(a)リアルタイムの証拠データの保全・調査技術	リアルタイム証拠データ保全・分析技術	・表現の見直し
		(b)ネットワーク・フォレンジック（大容量データの収集・解析を効率的に行うための研究）	ネットワーク・フォレンジックの実用化	
		(c)証拠データの信頼性評価などの研究	証拠データ全体の信頼性向上・評価技術	
⑨	ITリスクに関する理論から実務までの体系化	(a)リスク対リスクを回避するための手段の研究	ITリスクの体系化	・体系化と対策技術、合意形成手法に分離、明確化
		(b)複数の関係者間で合意を得るためのコミュニケーション手段の研究	動的および複合リスクの評価・対策モデ	
		(c)対策の最適な組み合わせを求めるシステムを開発する	合意形成のためのリスクコミュニケーション手法	
研究開発の促進基盤の確立とセキュリティ理論の体系化				
⑩	情報セキュリティ研究の基盤体系化	(a)サイバーセキュリティ研究の科学的な評価フレームワークの確立	サイバーセキュリティ研究における科学的アプローチの導入	・主旨を踏まえて、広く研究を支援する基盤を意味するように表現を見直し
		(b)実証研究のためのデータ基盤の整備	技術評価のための実証データベース等の整備	
⑪	セキュリティ部品が正しく実装されていることを保証する製品評価認証技術	(a)セキュリティ製品のセキュリティレベルを評価するための基準設計	ソフトウェア/ハードウエアのセキュリティ品質を客観的に評価する手法の確立	・セキュリティ品質の評価と、組み合わせ技術に分離、整理
		(b)セキュリティ製品の組み合わせ方の正当性を評価する手法の開発	セキュリティ部品を正しく組み上げる方法の開発	
		(c)評価プロセスの標準化	※上記2つのテーマに統合化	
⑫	情報理論的安全性を備えた暗号技術	(a)情報理論的に安全な暗号技術の研究	情報理論的に安全な暗号技術の研究	・量子暗号と情報理論的に安全であることの関係の記述を見直し
		(b)リソースやリアルタイム性の制約を考慮した方式の研究開発	リソースやリアルタイム性の制約を考慮した方式の研究開発	