資料 3-2

現状の強み分析のための研究領域の整理について

作業対象の研究領域	整理案	備考（左の作業対象との関係など）
① 通信系・アクセス系ネットワークセキュリティ ② 認証 ③ Web セキュリティ ④ プログラム保護 ⑤ 実装セキュリティ ⑥ 評価全般 ⑦ データセキュリティ ⑧ AI セキュリティ ⑨ IoT セキュリティ ⑩ サプライチェーンセキュリティ ⑪ 自動車セキュリティ ⑫ センサーセキュリティ ⑬ モバイルセキュリティ ⑭ その他アプリケーションまたはサービスセキュリティ	○基礎的要素 ・保護対象 (1) ネットワークセキュリティ研究 (2) コンピュータセキュリティ（プログラム保護）研究 (3) コンピュータセキュリティ（Web セキュリティ）研究 (4) アイデンティティ管理・認証研究 (5) データセキュリティ及びプライバシー保護研究 (6) 人的要素セキュリティ研究 ・手法 (7) 実装セキュリティ（ハードウェアセキュリティ・暗号実装含む）研究 (8) セキュリティ評価・リスク評価研究	①、対象変更なし、名称簡潔化 ④、対象変更なし、名称明確化 ③、対象変更なし、名称明確化 ②、対象変更なし、名称明確化 ⑦、対象変更なし、名称明確化 （もとよりプライバシー保護含む） 新設　主要国際カンファレンスでセッション設定、WG 作業で提案 ⑤、対象変更なし、内容が分かるよう名称明確化 ⑥、対象変更なし、内容がわかるよう名称明確化
	○対象分野 (9) AI セキュリティ研究 (10) IoT セキュリティ研究 (11) 自動運転セキュリティ研究 (12) サプライチェーンセキュリティ研究 (13) センサーセキュリティ研究 (14) モバイルセキュリティ研究	 ⑧ ⑨ ⑪、対象変更なし、名称明確化 ⑩ ⑫ ⑬

※今般の分析は、実践的なサイバーセキュリティの研究分野を対象とし、我が国における暗号と情報セキュリティやコンピュータセキュリティに係る研究集会で発表される研究分野のうち、純理論系の暗号研究分野を除いたものを対象としている。なお、暗号研究分野は、国際的に著名な研究集会（トップカンファレンス）においても、我が国は一定の高い存在感を示している。

また、研究領域は、研究開発戦略専門調査会第 14 回会合での事務局説明資料に基づき、我が国の研究集会において過去 5 年に設けられたセッションであって、実践的なサイバーセキュリティの研究分野のものを一定の領域のまとまり毎に網羅的に整理したものを分析作業上の土台とした。なお、分析資源や詳細化に限りがあるため、「対象分野」における研究領域のうち、一部対象にできなかったものがあるが、アカデミックな研究の広がりを考慮しつつ Society 5.0 関連のものは出来る限り分析対象とした。

以上

現状の強み分析のための研究領域の整理について

我が国の研究集会において過去5年に設けられたセッションであって、実践的なサイバーセキュリティの研究分野のものを一定の領域のまとまり毎に網羅的に整理

・過去5年間の電子情報通信学会「暗号と情報セキュリティシンポジウム（SCIS）」及び情報処理学会「コンピュータセキュリティシンポジウム（CSS）」の158セッションから、他セッション名で表せるものを除き58セッションに整理。ただし、我が国が一定の高い存在感を示している純理論系の暗号研究分野を除いたものが対象。
・上記58セッションを中分類、4つのフェーズ単位の小分類に割り当て、空白部を補足して以下の表を作成。
・さらに、各研究領域を基礎的要素となる保護対象や手法及び対象分野に再整理・名称明確化を行った表が以下のとおり。

	現状の強み分析のための研究領域の整理	中分類	小分類（フェーズ単位）			
			攻撃	検知（観測）	分析（解析）	対策
基礎的要素保護対象	●ネットワークセキュリティ研究	通信系ネットワークセキュリティ	ネットワーク攻撃	●ネットワーク攻撃検知	●ネットワーク攻撃分析	●ネットワーク攻撃対策
			不正通信	●不正通信検知	不正通信分析	不正通信対策
		アクセス系ネットワークセキュリティ	不正アクセス	●不正アクセス検知	不正アクセス分析	不正アクセス対策
			DoS攻撃	DoS攻撃検知	DoS攻撃分析	●DoS攻撃対策
			悪性ドメイン構築	悪性ドメイン検知	悪性ドメイン分析	●悪性ドメイン対策
	コンピュータセキュリティ（プログラム保護）研究	プログラム保護	マルウェア	●マルウェア検知	●マルウェア分析	●マルウェア対策
			不正機能埋込	不正機能埋込検知	●動的解析 ●表層解析 ●プログラム解析 静的解析	●難読化
	コンピュータセキュリティ（Web セキュリティ）研究	●Webセキュリティ	Web攻撃	Web攻撃検知	●Web攻撃分析	Web攻撃対策
			悪性サイト構築	悪性サイト検知	悪性サイト分析	●悪性サイト対策
	アイデンティティ管理・認証研究	●認証	なりすまし攻撃	なりすまし攻撃検知	なりすまし攻撃分析	●ID管理 ●個人認証 ●ユーザ認証 ●人工物メトリクス ●PKI
	データセキュリティ及びプライバシー保護研究	●プライバシー保護	プライバシー情報漏洩	プライバシー情報漏洩検知	プライバシー情報漏洩分析	●加工技術
		●個人情報保護	個人情報漏洩	個人情報漏洩検知	個人情報漏洩分析	個人情報漏洩対策
		●コンテンツ保護	コンテンツ不正流通	コンテンツ不正流通検知	コンテンツ不正流通分析	●情報ハイディング
	人的要素セキュリティ研究	人的要素セキュリティ（ユーザブルセキュリティ）	本研究は小分類（フェーズ単位）まで細かく分けられていないと思われるため、中分類までの項目を対象とする。			
手法	実装セキュリティ（ハードウェアセキュリティ・暗号実装含む）研究	●暗号実装	●暗号実装攻撃	暗号実装攻撃検知	暗号実装攻撃分析	暗号実装攻撃対策
		●ハードウェアセキュリティ	ハードウェア実装攻撃	ハードウェア実装攻撃検知	ハードウェア実装攻撃分析	ハードウェア実装攻撃対策
		●OSセキュリティ	OS実装攻撃	OS実装攻撃検知	OS実装攻撃分析	OS実装攻撃対策
		●ソフトウェアセキュリティ	ソフトウェア実装攻撃	ソフトウェア実装攻撃検知	ソフトウェア実装攻撃分析	ソフトウェア実装攻撃対策
	セキュリティ評価・リスク評価研究	●セキュリティ評価	セキュリティ実装不備 セキュリティ設計不備 セキュリティ対策不備	●セキュリティ調査	●セキュリティ分析	●セキュリティ実装 ●セキュリティ設計 セキュリティ対策
		●リスク評価	脆弱性 リスク 脅威	脆弱性検知 リスク検知 脅威検知	●脆弱性分析 ●リスク分析 ●脅威分析	●脆弱性対策 ●リスク管理 脅威対策
対象分野	AIセキュリティ研究	●AIセキュリティ				
	IoTセキュリティ研究	●IoTセキュリティ				
	自動運転セキュリティ研究	●自動運転セキュリティ				
	サプライチェーンセキュリティ研究	●サプライチェーンセキュリティ				
	センサーセキュリティ研究	●センサーセキュリティ				
	モバイルセキュリティ研究	●モバイルセキュリティ				
		●FinTechセキュリティ				
		●オンラインバンキングセキュリティ				
		●クラウドセキュリティ				
		●計測セキュリティ				
		●産業制御システムセキュリティ				
		●無線セキュリティ				
		●メールセキュリティ				

攻撃者の視点に立って未知の脅威を発見する方法の研究（攻撃研究）

検知（観測）に基づく研究

これらの研究は小分類（フェーズ単位）まで細かく分けられていないと思われるため、中分類までの項目を対象とする。

ピンク背景は現状の強み分析を行った対象領域
水色背景は上記対象領域を構成する中分類・小分類の要素
●は上記のとおり過去5年間で設けられた58セッション
赤字は研究開発戦略専門調査会第14回会合での事務局説明資料（資料3の整理例②）からの修正箇所

注1: 人的要素セキュリティ研究は近年の主要国際カンファレンスでセッションが設定されており、WG作業で提案され追加された。
注2: 分析資源や詳細化に限りがあるため、「対象分野」における研究領域のうち、一部対象にできなかったものがあるが、アカデミックな研究の広がりを考慮しつつSociety 5.0関連のものは出来る限り分析対象とした。