資料 2-4

分野・領域に係る強み分析の作業案

Ⅰ．現状の研究レベルでの強み分析

（別紙）専門調査会資料（検討の素材）に掲載されていた領域の整理例②（一部変更）のうち、対象領域（ピンク背景）ごとにご回答ください。その際、以下の事項にご留意ください。

- ✓ ご回答は、対象領域を構成する中分類・小分類の要素（水色背景）まで分解してお考えいただき、その上で対象領域を評価いただいても良いと思われます。
- ✓ 現状の研究レベルとは、カンファレンス等での論文発表などアカデミックな研究活動のレベルを対象としてください。
- ✓ 国際比較を行う対象地域は次のとおりです。その他の国で特筆すべき国が考えられる場合は、その国名を挙げた上で評価してください。なければ無回答で結構です。
  - ▪ 米国
  - ▪ 欧州
  - ▪ その他の国（カナダ、イスラエル、中国、シンガポール、韓国など）
- ✓ 各回答について、ご自身の把握状況も教えてください。

  ア．十分把握して回答している　　イ．ある程度把握して回答している
  ウ．あまり把握できていないかもしれないが知見を基に回答している
  エ．承知しておらず回答は控える（※この場合問いにはお答えいただかなくて結構です。）

各質問事項は以下のとおりです。

ⅰ．整理例②の領域について

Q1: 対象領域について、現状の研究レベルで国際比較を行う観点から、日本及び各地域の活動・成果状況を評価し、当てはまる番号をご回答ください。

①特に顕著な活動・成果が見えている ②顕著な活動・成果が見えている
③顕著な活動・成果が見えていない　④活動・成果がほとんど見えていない
⑤（国・地域によっては）承知しておらず回答は控える

Q2: 対象領域について、現状の研究レベルで国際比較を行う観点から、日本及び各地域の状況のトレンドを評価した場合、当てはまる番号をご回答ください。ここでのトレンドは直近２年程度の取り組み状況でお考えください。

①上昇傾向　②現状維持　③下降傾向
④（国・地域によっては）承知しておらず回答は控える

Q3: Q1 と Q2 に対し、各地域（欧州やその他の国の場合は国名）の状況として特筆すべきもの、及び、評価の際に参考にした根拠情報を、文章形式により箇条書きで挙げてください。

ⅱ．その他の領域について

Q4: ⅰの対象領域以外に取り上げるべき領域があれば、その名称と説明をご記載の上、Q5～Q7 にご回答ください。

Q5: Q4 の領域について、現状の研究レベルで国際比較を行う観点から、日本及び各地域の活動・成果状況を評価し、当てはまる番号をご回答ください。

①特に顕著な活動・成果が見えている ②顕著な活動・成果が見えている
③顕著な活動・成果が見えていない　④活動・成果がほとんど見えていない
⑤（国・地域によっては）承知しておらず回答は控える

Q6: Q4 の領域について、現状の研究レベルで国際比較を行う観点から、日本及び各地域の状況のトレンドを評価した場合、当てはまる番号をご回答ください。ここでのトレンドは直近２年程度の取り組み状況でお考えください。

①上昇傾向　　②現状維持　　③下降傾向
④（国・地域によっては）承知しておらず回答は控える

Q7: Q5 と Q6 に対し、各地域（欧州やその他の国の場合は国名）の状況として特筆すべきもの、及び、評価の際に参考にした根拠情報を、文章形式により箇条書きで挙げてください。

ｉ．整理例②の領域について

（1）通信系・アクセス系ネットワークセキュリティ

A1 と A2:

回答項目	日本	米国	欧州	その他（あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（2）認証

A1 と A2:

回答項目	日本	米国	欧州	その他（あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（3）Web セキュリティ

A1 と A2:

回答項目	日本	米国	欧州	その他 （あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（4）プログラム保護

A1 と A2:

回答項目	日本	米国	欧州	その他 （あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（5）実装セキュリティ

A1 と A2:

回答項目	日本	米国	欧州	その他 （あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（6）評価全般

A1 と A2:

回答項目	日本	米国	欧州	その他 （あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（7）データセキュリティ

A1 と A2:

回答項目	日本	米国	欧州	その他（あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（8）AI セキュリティ

A1 と A2:

回答項目	日本	米国	欧州	その他（あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（9）IoT セキュリティ

A1 と A2:

回答項目	日本	米国	欧州	その他 （あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（10）サプライチェーンセキュリティ

A1 と A2:

回答項目	日本	米国	欧州	その他 （あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（11）自動車セキュリティ

A1 と A2:

回答項目	日本	米国	欧州	その他 （あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（12）センサーセキュリティ

A1 と A2:

回答項目	日本	米国	欧州	その他 （あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（13）モバイルセキュリティ

A1 と A2:

回答項目	日本	米国	欧州	その他 （あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

（14）その他アプリケーションセキュリティまたはその他サービスセキュリティ

A1 と A2:

回答項目	日本	米国	欧州	その他 （あれば）
Q1 に対する回答				
Q2 に対する回答				
回答に対する把握状況				

（国名:　　）

A3:

ⅱ. その他の領域について（回答欄が足りなければ、適宜追加してください）

〇回答欄（1）

A4:

A5 と A6:

回答項目	日本	米国	欧州	その他（あれば）
Q5 に対する回答				
Q6 に対する回答				
回答に対する把握状況				

（国名:　　）

A7:

〇回答欄（2）

A4:

A5 と A6:

回答項目	日本	米国	欧州	その他（あれば）
Q5 に対する回答				
Q6 に対する回答				
回答に対する把握状況				

（国名:　　）

A7:

Ⅱ. ポテンシャルとしての強み分析

質問事項は以下のとおりです。

Q1: ポテンシャルとしての日本の強みには何が挙げられますか。日本の研究コミュニティの特性や日本の社会や産業等の特性を考慮して挙げて下さい。事務局としていくつかの案を以下に示しますので、意見や表現に相違があれば、修正してください。また、他にも挙げられると思われますので、挙げていただければと思います。(事務局でご回答を整理した後、全体を次の WG でご議論いただく予定です。)

案 1: センサー・自動車などの実空間技術とサイバーとの融合領域（Society 5.0）は日本として強みかつ力を入れるため、そのセキュリティを研究する、センサーセキュリティ、IoT セキュリティ、自動車セキュリティは、日本の強みとなるポテンシャルがある。

案 2: 攻撃のローカライゼーションが進展し、日本でしか観測できない攻撃があり、また、攻撃解析の粒度も高くなるところ、これまで日本で構築されてきた攻撃観測基盤を活用・発展させた攻撃観測をベースにした研究は、日本の更なる強みとなるポテンシャルがある。

案 3: 日本は暗号研究が国際的な強みを有しており、暗号の強みを生かした〇〇は、日本の強みとなるポテンシャルがある。

案 4: 品質や実運用に配慮する細やかさは日本の強みであり、それを生かした〇〇は、日本の強みとなるポテンシャルがある。

A1:

（別紙）分野・領域に係る強み分析の作業案

【専門調査会資料（検討の素材）に掲載されていた領域の整理例②を一部変更】

例②: 直近5年間のSCIS及びCSSのセッションから、領域の広さやフェーズを意識して整理

整理した58セッションを大項目、中項目、4つのフェーズ単位の小項目に割り当て、空白部を補足して作成した表が以下のとおり。今回、一部の中分類を統合するために、統合中分類の列を追加。

大分類（セキュリティ大項目）	統合中分類（統合セキュリティ中項目）	中分類（セキュリティ中項目）	小分類（フェーズ単位）			
			攻撃（不備）	検知（観測）	分析（解析）	対策
ネットワークセキュリティ（28項目）	通信系・アクセス系ネットワークセキュリティ（20項目）	通信系ネットワークセキュリティ（8項目）	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（12項目）	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
	認証（8項目）	認証（8項目）	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
コンピュータセキュリティ（19項目）	Webセキュリティ（8項目）	Webセキュリティ（8項目）	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
	プログラム保護（11項目）	プログラム保護（11項目）	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
実装セキュリティ（16項目）	実装セキュリティ（16項目）	暗号実装（4項目）	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（4項目）	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（4項目）	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（4項目）	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
評価全般（20項目）	評価全般（20項目）	セキュリティ評価（8項目）	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（12項目）	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
データセキュリティ（12項目）	データセキュリティ（12項目）	プライバシー保護（4項目）	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（4項目）	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（4項目）	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
アプリケーションセキュリティまたはサービスセキュリティ（13項目）	AIセキュリティ	AIセキュリティ	アプリケーションセキュリティは小分類（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13項目を対象とする。			
	IoTセキュリティ	IoTセキュリティ				
	サプライチェーンセキュリティ	サプライチェーンセキュリティ				
	自動車セキュリティ	自動車セキュリティ				
	センサーセキュリティ	センサーセキュリティ				
	モバイルセキュリティ	モバイルセキュリティ				
	その他アプリケーションセキュリティまたはその他サービスセキュリティ（7項目）	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				
計6大分類	計14統合中分類	計27中分類	計95小分類			

ピンク背景は対象領域

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

注1: 最先端の研究や海外での研究でSCISやCSSのセッション名にすぐには現れてこない領域がありうる。

注2: 学会には現れてこない、あるいは研究は行われていても論文として発表がなされない領域がありうる。