資料2-2

分野・領域に係る検討の素材
～日本の強み（弱み）をどう分析・整理するか～

令和2年8月

内閣サイバーセキュリティセンター（NISC）
基本戦略第1グループ

日本の強みやポテンシャルの高い領域はどれか

1. 今の研究レベルで日本の強み（弱み）を分析・整理するために、どのような方法が考えられるか。

（例）

ア. カンファレンスやジャーナルにおける日本の発表件数や受賞歴で評価する方法

→ カンファレンス例・ジャーナル例（参考1）、論文賞（Paper Award）例（参考2）

イ. セキュリティ分野の研究コミュニティが主観的に評価する方法

→ JST/CRDS 研究開発の俯瞰報告書 システム・情報科学技術分野（2017年）（参考3）

→ どのような作業に落とし込むか。

2. ポテンシャルとしての日本の強み（弱み）を分析・整理するために、どのような方法が考えられ、何が挙げられるか。

（例）

ア. 日本の研究コミュニティの特性を考慮して評価する方法

イ. 日本の社会や産業等の特性を考慮して評価する方法

→ 資料2-1の2. 日本の強み（ポテンシャル）参照。これ以外にもありうると思われる。
いずれにしても、本WGで知恵を持ち寄る必要。

（参考1）

カンファレンス例・ジャーナル例

カンファレンス例

ランク	カンファレンス名
Tier1	Network and Distributed System Security Symposium（NDSS）
	IEEE Symposium on Security and Privacy（IEEE S&P）
	USENIX Security Symposium（USENIX Security）
	ACM Conference on Computer and Communications Security（ACM CCS）
Tier2	IEEE European Symposium on Security and Privacy（Euro S&P）
	ACM ASIA Conference on Computer and Communications Security（ASIACCS）
	International Symposium on Research in Attacks, Intrusions and Defenses（RAID）
	Annual Computer Security Applications Conference（ACSAC）

ジャーナル例

学会名	論文誌名
電子情報通信学会	電子情報通信学会論文誌英文論文誌A／和文論文誌A
	電子情報通信学会論文誌英文論文誌D／和文論文誌D
情報処理学会	情報処理学会論文誌

（参考2）

論文賞（Paper Award）例

論文賞（Paper Award）例

種別		論文賞（Paper Award）名
カンファレンス		各カンファレンスにおけるPaper Award等
ジャーナル	電子情報通信学会	論文賞
		末松安晴賞
	情報処理学会	論文賞
		業績賞
		情報処理技術研究開発賞
		マイクロソフト情報学研究賞

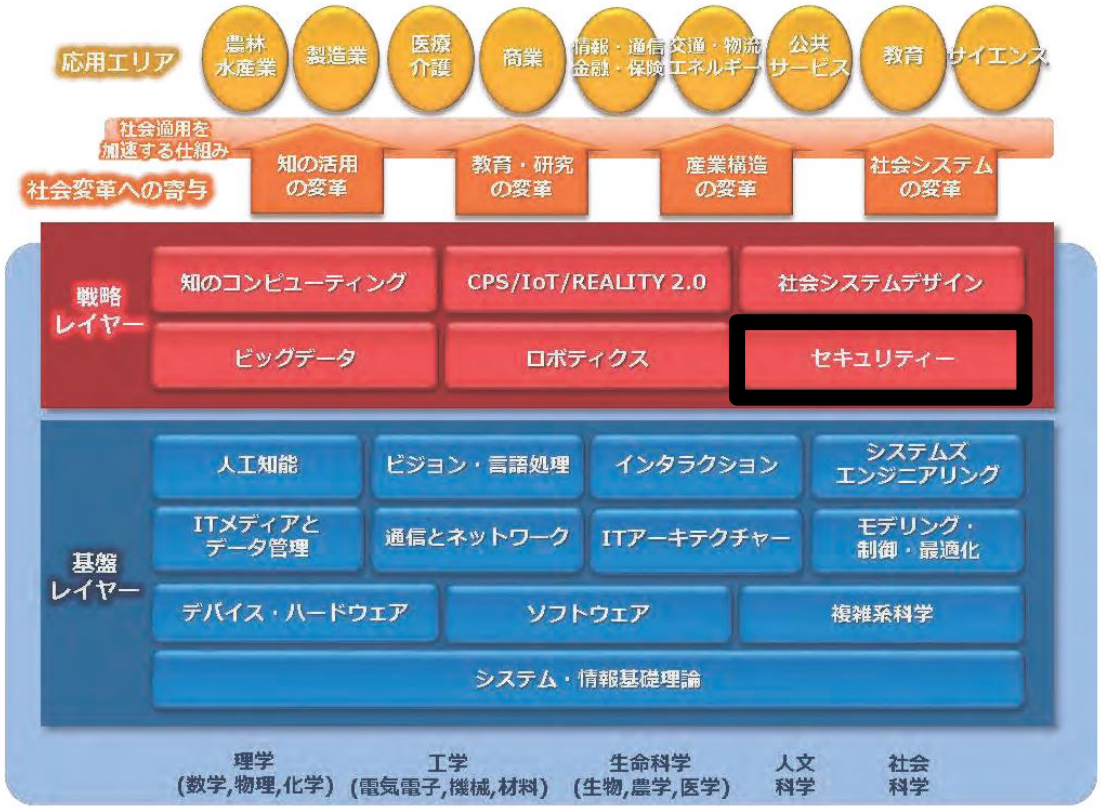
日本の論文賞（Paper Award）受賞例と対象分野領域

名称	論文情報	対象分野領域
NDSS2020 Distinguished Paper Award	Melting Pot of Origins: Compromising the Intermediary Web Services that Rehost Websites Takuya Watanabe, Eitaro Shioji, Mitsuaki Akiyama (NTT), Tatsuya Mori (Waseda University, NICT, and RIKEN AIP)	例②整理での記載: Web攻撃対策
NDSS2019 Distinguished Paper Award	Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai Orcun Cetin, Carlos Ganan, Lisette Altena (Delft University of Technology), Takahiro Kasama, Daisuke Inoue (National Institute of Information and Communications Technology), Kazuki Tamiya, Ying Tie, Katsunari Yoshioka (Yokohama National University), Michel van Eeten (Delft University of Technology)	例②整理での記載: IoTセキュリティ

（参考3）

JST/CRDS 研究開発の俯瞰報告書 システム・情報科学技術分野（2017年）より

システム・情報科学技術分野の構造



戦略レイヤーの研究開発領域

知のコンピューティング
- 知の集積・増幅・探索
- 予測、発見の促進
- 知のアクチュエーション
- 知のプラットフォーム
- ELSIと社会適用
- 人文・社会科学に学ぶ
- 生命科学に学ぶ
- 情報科学に学ぶ

CPS/IoT/REALITY 2.0
- REALITY 2.0による社会デザイン
- ソフトウエアデファインドソサエティーのサービスプラットフォーム
- モノ、ヒト、コトのスマートなサービス化技術
- CPS/IoT/REALITY2.0 アーキテクチャー
- モノ・ヒト・コトのインターフェース

社会システムデザイン
- 社会計測
- 分析・評価モデル
- サービスプラットフォーム（CPS/IoT/REALITY2.0）
- 社会インフラオペレーション
- 社会システムアーキテクチャー
- 制度設計
- サービスサイエンス
- 社会システム基礎理論（基盤レイヤー）

ビッグデータ
- ビッグデータ処理基盤技術
- 機械学習技術
- 画像・映像解析技術
- 自然言語処理技術
- ビッグデータ活用促進技術
- ビッグデータによる価値創造
- ビッグデータに関わる制度設計
- 新計算原理

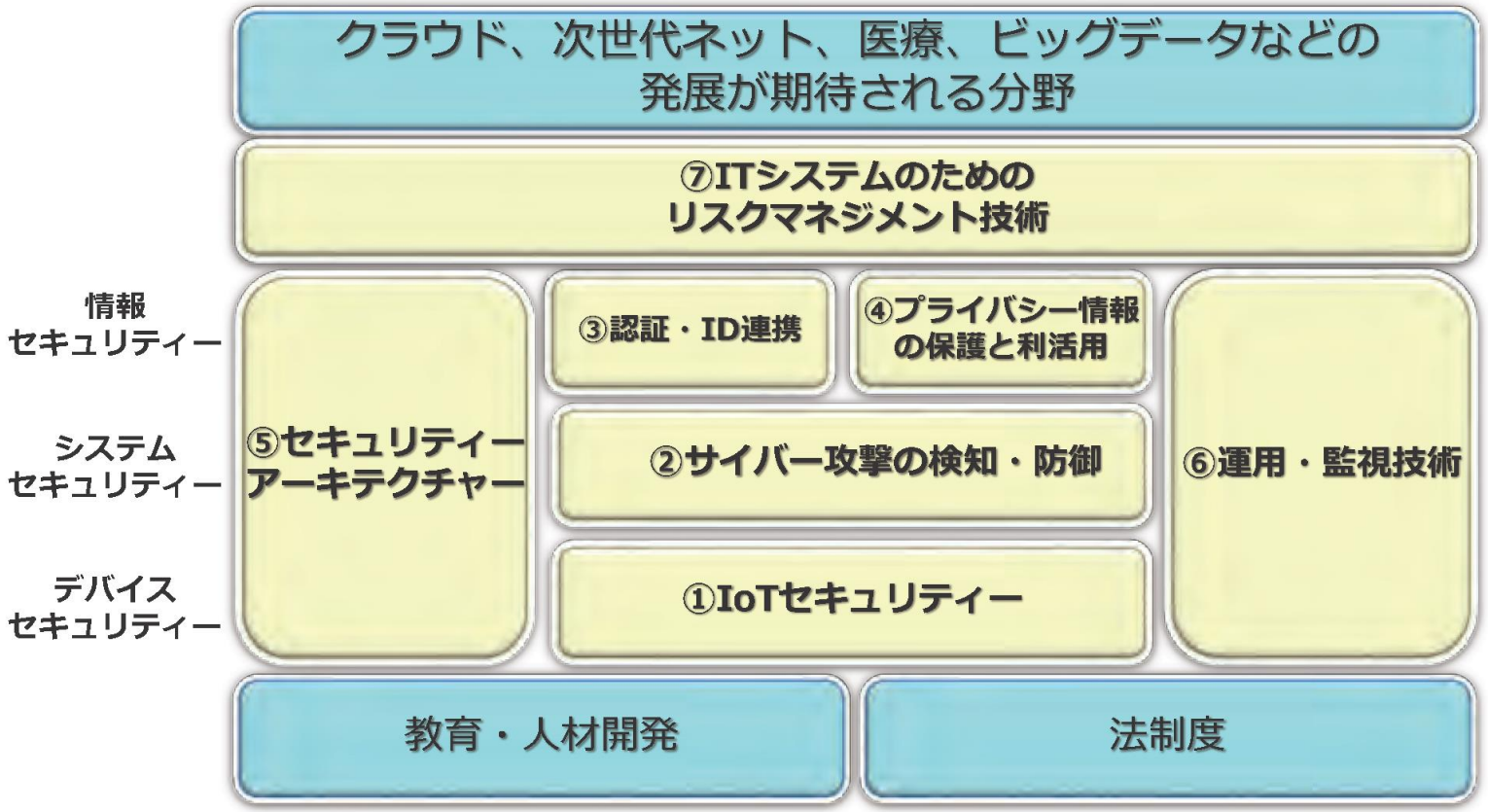
ロボティクス
- ロボティクスと社会
- モビリティ・フィールドロボット
- 空中ロボット
- 生活支援・福祉ロボット
- 医療ロボット
- 産業用・研究開発用ロボット
- システム化技術
- ソフトロボティクス
- 認知発達ロボティクス

セキュリティー
- IoTセキュリティー
- サイバー攻撃の検知・防御
- 認証・ID連携
- プライバシー情報の保護と利活用
- セキュリティーアーキテクチャ
- 運用・監視技術
- ITシステムのためのリスクマネージメント技術

（出典）JST/CRDS 研究開発の俯瞰報告書 システム・情報科学技術分野（2017年）

JST/CRDS 研究開発の俯瞰報告書 システム･情報科学技術分野（2017年）より

セキュリティー区分俯瞰図



（出典）JST/CRDS 研究開発の俯瞰報告書 システム･情報科学技術分野（2017年）

強みの分析例

作成協力者一覧

※五十音順、敬称略、所属・役職は本報告書作成時点

■セキュリティー

佐々木　良一	東京電機大学　未来科学部　情報メディア学科　教授【総括責任者】
大久保　隆夫	情報セキュリティ大学院大学　情報セキュリティ研究科　教授
菊池　浩明	明治大学　総合数理学部　先端メディアサイエンス学科　教授
工藤　誠也	情報処理推進機構　技術本部　セキュリティーセンター　情報セキュリティ技術ラボラトリー　研究員
佐久間　淳	筑波大学大学院　システム情報工学研究科　教授
下道　高志	東京電機大学　未来科学部　情報メディア学科　セキュリティー研究室　研究員
高倉　弘喜	国立情報学研究所　アーキテクチャ科学研究系　教授 / サイバーセキュリティー研究開発センター　センター長
高橋　健志	情報通信研究機構　サイバーセキュリティ研究所　サイバーセキュリティ研究室　主任研究員
辻　宏郷	情報処理推進機構　技術本部　セキュリティセンター　情報セキュリティ技術ラボラトリー　研究員

研究開発の俯瞰報告書作成メンバー

（2017年3月時点）

木村　康則	上席フェロー	
岩野　和生	上席フェロー	（～ 2016 年 12 月）
鈴木　慶二	フェロー	
高島　洋典	フェロー	
土井　直樹	フェロー	（～ 2016 年 3 月）
富川　弓子	フェロー	（～ 2016 年 3 月）
坂内　悟	フェロー	
福島　俊一	フェロー	
藤井新一郎	フェロー	
的場　正憲	フェロー	
茂木　強	フェロー	
山田　直史	フェロー	
合原　一幸	特任フェロー	
井上　友二	特任フェロー	
喜連川　優	特任フェロー	
國吉　康夫	特任フェロー	
竹内　健	特任フェロー	
徳田　英幸	特任フェロー	
森川　博之	特任フェロー	
山口　高平	特任フェロー	

強みの分析例

①IoTセキュリティー

- キーワード

  IoT、IoE、IIoT、脆弱性対策、脅威分析、制御システム、重要インフラ、攻撃観測技術、軽量暗号、高機能暗号、ハードウエアセキュリティー

- 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	↗	軽量暗号、認証技術ならびにビッグデータ、AI と連携した検知技術の研究を進めている。
	応用研究・開発	○	↗	総務省、経済産業省による IoT 推進コンソーシアムを設立し、ガイドラインを策定、公開している。
米国	基礎研究	◎	↗	製品寿命の長い IoT デバイスに対応する暗号技術やゲートウェイ、アプリケーションのフレームワークを研究するプロジェクトを発足している。
	応用研究・開発	◎	↗	CSA（Cloud Security Alliance）、OTA（Online Trust Alliance）、OWASP（The Open Web Application Security Project）がガイドラインを公開している。IoT 関連ベンダーも並行して、IoT 向けのセキュリティーソリューションを公表している。制御システムに関しては、米国政府によるセキュリティーガイドラインが公開されている。
欧州	基礎研究	○	→	IoT デバイスの研究開発に力をいれている。
	応用研究・開発	◎	↗	ENISA（The European Union Agency for Network and Information Security）によるスマートホームに対するセキュリティーの勧告文書を公開し、GSMA はサービスプロバイダー、製造業、ネットワークオペレーターなどに向けたガイドラインを公開している。また、ドイツ主導によるインダストリー 4.0 プラットフォームは実現戦略におけるセキュリティーの要求事項を公開している。
中国	基礎研究	△	→	IoT のセキュリティーに関する具体的な研究は公開されていない。
	応用研究・開発	○	→	ウイルス検知や防御技術の開発や自動車のハッキング実験を行っているが、IoT/ 制御システムに特化した製品は見当たらない。
韓国	基礎研究	△	→	IoT のセキュリティー関する具体的な研究は公開されていない。
	応用研究・開発	△	→	IoT のセキュリティー要件をまとめる動きはみえるが、国家もしくは標準化団体主導によるガイドライン策定の動きはない。また、具体的は製品も見当たらない。

（注１） フェーズ
基礎研究フェーズ：大学・国研などでの基礎研究のレベル
応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル
（注２） 現状　※わが国の現状を基準にした評価ではなく、CRDS の調査・見解による評価である。
◎　特に顕著な活動・成果が見えている、　○　顕著な活動・成果が見えている
△　顕著な活動・成果が見えていない、　×　活動・成果がほとんど見えていない
（注３） トレンド
↗：上昇傾向、　→：現状維持、　↘：下降傾向

（出典）JST/CRDS 研究開発の俯瞰報告書 システム･情報科学技術分野（2017年）

強みの分析例

②サイバー攻撃の検知・防御

- キーワード

  サイバーセキュリティー、サイバー攻撃、標的型攻撃、ドライブ・バイ・ダウンロード攻撃、DDoS攻撃、マルウエア、サイバー攻撃可視化、サイバー攻撃情報共有、脆弱性対策、モバイルセキュリティー、IoTセキュリティー

- 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	↗	・国内シンポジウム等でのサイバーセキュリティーやマルウエア解析に関する発表件数は大学、企業とも増加傾向。一方、著名な国際会議での発表件数については、暗号系分野においては以前から Crypto, Eurocrypt, Asiacrypt などにおいて一定の存在感を維持。サイバーセキュリティー分野では従来は存在感に乏しかったものの、近年、RAID 2013/2015/2016 や ACM CCS 2015 に採録されるなど、国際的な成果も伸びつつある。 ・日欧連携が積極的に行われている。例えば、総務省戦略的国際連携型研究開発推進事業と FP7 との日欧 ICT 協調課題である「サイバー脅威に対する回復性強化のためのサイバーセキュリティ」（NECOMA プロジェクト）は終了したものの、本コミュニティを中心に、日欧の研究機関が集結して国際共同研究を行っている。
	応用研究・開発	○	→	・総務省が主導する「国際連携によるサイバー攻撃予知・即応プロジェクト」（PRACTICE, 2015 年度末まで）や、「官民連携による国民のマルウエア対策支援プロジェクト」（ACTIVE）、「実践的サイバー防御演習」（CYDER）の中で、実践的な応用研究が進められている。 ・情報通信研究機構は日本最大規模のサイバー攻撃観測・分析・対策システム NICTER を中心とした研究開発を推進しており、特にそのリアルタイム分析・可視化技術は世界をリードしている。
米国	基礎研究	◎	→	・米国の大学・公的研究機関による基礎研究レベルは非常に高く、著名な国際会議でのプレゼンスも高い。 ・NSF、DoD、DHS 等からの豊富な研究資金に基づく大小のプロジェクトが継続的に実施されている。
	応用研究・開発	◎	→	・大学での研究が実用を目指した応用研究であるものが多く、ミシガン大学発祥の Arbor Networks や、カリフォルニア大学サンタバーバラ校発祥の Lastline 社等、起業につながっている例も多い。 ・情報共有のフォーマットを規格化する動きが活発化しており、特に STIX や TAXII と呼ばれる脅威情報の交換のための規格は DHS から OASIS（Organization for the Advancement of Structured Information Standards, 構造化情報標準促進協会）へ移管して検討が進められている。
欧州	基礎研究	○	→	・ウィーン工科大学（オーストリア）や Eurecom Institute（フランス）等、マルウエア解析技術やサイバー攻撃観測技術等で高い研究成果実績有。 ・一方で、優秀な研究者が米国等の研究機関に移籍する事例も多く、研究人材の確保は容易ではないようにうかがえる。
	応用研究・開発	○	↗	・FP7 の後継の Horizon 2020 で、セキュリティーは七つの社会的課題の一つにあげられており、応用研究はさらに進むものと思われる。 ・EC は 14 カ国 28 組織（ISP、CERT、Law Enforcement、IT プロバイダー、学術ネットワーク、学術機関、重要インフラ事業者）で構成される ACDC（Advanced Cyber Defense Center）を設立。応用研究から実運用まで情報共有が進んでいる。
中国	基礎研究	△	↗	・中国国内トップクラスの大学の学生が米国等に留学し、研究成果を上げているが、中国国内の大学における研究成果が著名な国際会議に採録されるまでには至っていない。
	応用研究・開発	△	↗	・これまで国際的に注目される大規模研究プロジェクトは公表されているレベルでは見られない。 ・サイバーセキュリティー分野における国際標準化活動に徐々に注力。例えば IETF では Alibaba や Huawei のエンジニア、もしくは雇用した欧米のコンサルタントなどが chair の役職を務めたり、規格を提案してくるようになってきている。同様の傾向は ITU-T やその他の標準化団体でも見られる。
韓国	基礎研究	○	↗	・KAIST や POSTECH 等トップクラスの大学の研究成果が ACM CCS や NDSS 等の著名な国際会議に採録される等、基礎研究の国際的な評価は上がりつつある。
	応用研究・開発	○	→	・国家的なセキュリティーインシデントを多数経験しており、政府主導のセキュリティー対策を実践。 ・KISA、ETRI、KISTI といった公的機関が、サイバーセキュリティー技術の研究開発や、モニタリング、インシデント対応を行っており、特に政府機関に導入されているセキュリティー機器は 100% 国産と言われている。

（出典）JST/CRDS 研究開発の俯瞰報告書 システム・情報科学技術分野（2017年）

強みの分析例

③認証・ID連携

- キーワード

  アイデンティティー、認証連携、フェデレーション、強固な認証、生体認証、プライバシー、マイナンバー、機械学習、AI、グラフ、ブロックチェーン

- 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	→	・認証分野：生体認証では顔認証等の研究のように、世界に先んじて進んでいる分野がある。また国内外への論文投稿も活発であり研究が進んでいるとみられる。 ・機械学習、グラフ技術の技術を認証技術へ適用する研究は少ない。ブロックチェーンは幾つかの例が散見される[13]。 ・ID 連携分野：日本独自の基礎研究は進んでいない。
	応用研究・開発	△	↑	・認証分野：顔認証の実証実験等、認証精度向上・問題点克服のための研究・開発・実証が進んでいる。IPA では生体認証の導入・運用についてのガイドラインを公開している[15]。 ・機械学習、グラフ技術等の技術を認証技術へ適用する基礎研究が進んでいないため応用研究に結びつかない。ブロックチェーンは基礎研究から応用研究・開発のフェーズでの十分な実証を行われず実用試行のケースもある[14]。 ・ID 連携分野：学術認証ネットワーク（学認）による ID およびサービス連携のための応用研究・開発が進んでおり、国際学会での発表も多く行っている。学認が開発した uApprove.jp は本人同意による属性提供を実装している。 ・認証と ID 連携の広範囲の適用として期待されるものに、将来医療等を含み、広範囲の用途が考えられているマイナンバーとそれを支えるシステムがあり、さまざまな実証が行われている[16]。
米国	基礎研究	◎	↑	・認証分野：国防関連を含め生体認証の研究が進んでいる。 ・ID 連携分野：ネット企業を中心に民間での研究が進んでいてる。 ・機械学習、グラフ技術、ブロックチェーン等の技術を認証技術へ適用する多くの研究が行われている。[11]
	応用研究・開発	◎	↑	・認証分野：官民の重要施設や安全保障対策を優先として、応用研究・開発を行っている。 ・機械学習、グラフ技術、ブロックチェーン等の技術を認証技術へ適用し、応用も進みいくつかは実用化の域に達している。米国特許取得の例もある[12]。 ・ID 連携分野：ネット企業を中心に民間での応用研究が進んでいて、積極的に技術標準化のイニシアチブをとる。IETF や W3C のようなインターネット中心の規格に大きな影響力を行使している。
欧州	基礎研究	△	→	・認証分野：欧州の通信会社を中心とした研究が以前は多かったが、最近は特筆すべき顕著な研究成果が見受けられない。 ・機械学習、グラフ技術、ブロックチェーン等の技術を認証技術へ適用する研究は少ない。 ・ID 連携分野：EU のプライバシー保護の動きと併せ、プライバシーと併せた関連研究が散見される。
	応用研究・開発	○	→	・認証分野：EU の eID や EU 諸国の電子政府を中心としたシステムのための認証技術に関する応用研究・開発が進んでいる[17]。 ・機械学習、グラフ技術、ブロックチェーン等の技術を認証技術へ適用する基礎研究が進んでいないため応用研究に結びつかないと思われる。 ・ID 連携分野：EU の TAS3 プロジェクトでは 2011 年までに大規模な ID 連携実証実験を行った[18]。
中国・韓国	基礎研究	△	→	・特筆すべき顕著な研究成果が見受けられない（公開されていない）。
	応用研究・開発	△	→	・特筆すべき顕著な研究成果が見受けられない（公開されていない）。

（出典）JST/CRDS 研究開発の俯瞰報告書 システム・情報科学技術分野（2017年）

強みの分析例

④プライバシー情報の保護と利活用

- キーワード

  匿名化、仮名化、k-匿名性、l-多様性、マルチパーティー計算、Secure Function Evaluation、加法準同型性暗号、水平分割、垂直分割、プライバシー保護データマイニング、プライベートマッチング、差分プライバシー

- 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	↑	・暗号理論に関する基礎研究は、企業、大学、国立研究所ともに高いレベルにある。国際的にも競争力があり、優れた成果を挙げている。 ・プライバシー保護技術・システムセキュリティーについての基礎研究は、トップ国際会議等での発表は数が多くなく、国際的に競争力があるとは言えない。
	応用研究・開発	○	→	・ゲノムのプライバシー保護プロジェクト等、応用を意識したプロジェクトが増えてきている。NTT や三菱等は実装を発表している。
米国	基礎研究	◎	↑	・多くの学術論文が発表されている。いずれの研究領域においても、差分プライバシー、完全準同型暗号など多くの理論的アイデアはほとんど米国の大学・企業の研究者から提案されている。
	応用研究・開発	◎	↑	・MIT の CryptDB や SFE の実装等、高い技術力で提案された概念の実装が先行している。 ・高速秘密計算の開発環境 ObliVM, JustGarble などの秘匿回路開発フレームワークが発表されている。
欧州	基礎研究	○	→	・論文レベルではコンスタントに発表が続いている。差分プライバシーや暗号理論の研究も強い。
	応用研究・開発	○	→	・EU のプロジェクトなどで、ユビキタスネットワーク等の多くの分野を統合する動きが見られる。EU データ保護指令などの法整備も先行している。
中国	基礎研究	○	→	・秘匿回路評価の提案者を排出するなど学者を生み出しているが、活躍の場は米国などが主である。
	応用研究・開発	○	↑	・データ工学分野を中心に、複数名のデータプライバシー研究者が活動している。
韓国	基礎研究	○	→	・各種の暗号アルゴリズムの基礎的な研究を行い、国際標準に提案活動を行っている。
	応用研究・開発	△	→	・特に目立った活動は見られない。

（出典）JST/CRDS 研究開発の俯瞰報告書 システム・情報科学技術分野（2017年）

強みの分析例

⑤セキュリティーアーキテクチャー

- キーワード

  セキュリティー・バイ・デザイン、セキュリティー要求工学、脅威分析、リスク評価、形式手法、機能安全、セーフティ、IoT、組み込み

- 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	要求工学分野において、ゴール指向を中心に研究がされてきた。
	応用研究・開発	△	↗	また十分ではないが、IoT など具体的な応用分野を中心に活発化しつつある[13]。
米国	基礎研究	◎	→	CMU（Carnegie Mellon University）、FAU（Florida Atlantic University）を中心にあらゆる領域において先行している。
	応用研究・開発	◎	→	ツールやサービス提供、業界ごとの規格やガイドラインなどの開発が活発である。
欧州	基礎研究	◎	→	各種要求工学手法の応用や、プライバシーを含めた研究が各国で活発である。
	応用研究・開発	◎	↗	近年では Industrie 4.0[14] での CPS へのセキュリティーの組み込みも進む。
中国	基礎研究	○	→	要求工学をセキュリティーに応用する研究など、いくつかの事例が見られる。
	応用研究・開発	○	↗	IoT、ビッグデータなど特定の分野における応用研究が見られる。
韓国	基礎研究	×	→	国際会議等で顕著な研究成果が見られない。
	応用研究・開発	×	→	上に同じ。

（出典）JST/CRDS 研究開発の俯瞰報告書 システム・情報科学技術分野（2017年）

強みの分析例

⑥運用・監視技術

- キーワード

  サイバーセキュリティー、サイバー攻撃対策、標的型サイバー攻撃、レジリエントネットワーク、セキュリティー情報イベント管理（Security Information Event Management）

- 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	→	監視運用に携わる研究者が極めて少ないが、大学情報センター系の教員などを中心に基礎研究は行われている。ただし、自校の通信であっても実データを研究に利用できる大学は少ないのが現状である。
	応用研究・開発	△	→	製品化では実データによる検証および機能強化が必須であるが、実データの入手が極めて困難であることもあり、外国製品との差を埋めることに苦労している。このため、アンチウイルスソフトなどを除けば、監視運用の製品化まで至った例はごく少数に止まっている。
米国	基礎研究	○	↗	DoD（DARPA）、DHS、NSF などにより潤沢な研究資金が幅広く投資されており、かつ、研究に必要な実データの入手も一定条件のもとで可能となっている。
	応用研究・開発	○	↗	大学で生まれたアイデアを元に起業化する流れがうまく循環している。ただし、すべての起業化が成功しているわけではなく、実際にはごくわずかである。 また、実データを活用した製品の性能検証や高機能化が有効に働いている。極端な事例として、実際に Botnet を乗っ取って運用してみた実事例を論文で発表するなど、わが国を含めた諸国では違法性が問われる活動まで容認されている。
欧州	基礎研究	○	↗	サイバーセキュリティー全般として基礎研究は活発であり、国際会議での発表も数多くなされている。
	応用研究・開発	△	→	欧州も個人情報保護や通信の秘密の制限が厳しくかけられているため、実用化段階の検証が行いにくいのが現状である。5 年ほど前であるが、フランス Eurecom の研究者が大挙して渡米し、米国のセキュリティー企業や大学に転職するという事態も発生している。
中国	基礎研究	－	－	監視運用に関する情報はほとんど公開されていないため評価が難しい。
	応用研究・開発	－	－	Golden Firewall（金盾）と言われる通信監視が極めて効果的に機能していることから、かなりのレベルの技術開発が行われていることは推定できるが、監視運用に関する情報はほとんど公開されていない。
韓国	基礎研究	○	↗	北朝鮮が関与したとされるサイバー攻撃を受け重要情報が流出するなどの被害が年に数回の頻度で発生しているため、監視運用に必要な基礎技術の開発は比較的活発である。
	応用研究・開発	△	→	基礎技術の製品化は、政府機関等での採用必須化などもあり、アンチウイルスソフトや IDS など一定の分野で進んでいる。ただし、米国やイスラエル製品と競合する分野では、厳しい競争にさらされ、製品化が難しいのが現状である。
イスラエル	基礎研究	○	↗	サイバーセキュリティーに直結しないものであっても、国防に関連する可能性がある基礎理論分野については、大学や研究機関において活発に研究されている。
	応用研究・開発	△	→	国家による支援制度もあり、数多くのベンチャー企業が立ち上がっている。また、大学等の研究機関との連携も国家が後押しする体制が整っている。ただし、製品化に関するノウハウが十分にないこともあり、他国企業と共同で製品化する事例も多い。また、米国製品と競合することが多いのも実情である。

（出典）JST/CRDS 研究開発の俯瞰報告書 システム・情報科学技術分野（2017年）

強みの分析例

⑦ITシステムのためのリスクマネジメント

- キーワード
  リスクアセスメント、リスクコミュニケーション、リスクマネジメント

- 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	↗	IT システムに関するリスクコミュニケーションなどの研究が大学などで積極的に進められているが層は薄い。
	応用研究・開発	○	↗	IPA 等でセキュリティー経済学やリスク心理学的アプローチが進み始めているが層は薄い。
米国	基礎研究	◎	↗	リスクアセスメントに関する大学における研究は多い。また、理論的研究に関するアプローチが開始されている。
	応用研究・開発	◎	↗	NIST を中心に、リスクマネジメントに関する基準やガイドを策定して公開している。国の組織の安全性評価に積極的に適用している。
欧州	基礎研究	○	→	ディフェンスグラフを用いる対策案選定法などのリスクアセスメント技術が大学などで積極的に進められている。
	応用研究・開発	◎	→	セキュリティー経済学については、ENISIA で 2011 年より、WG が作成され研究がおこなわれてきたが、最近は目立った新しい動きは見られない。
中国	基礎研究	○	↗	大学などにおいてリスクアセスメントに関する研究は行われているようであり、論文などは増えつつある。
	応用研究・開発	△	→	目立った動きが見えない。
韓国	基礎研究	○	→	大学などにおいてリスクアセスメントに関する研究は行われている。
	応用研究・開発	○	→	政府機関などにおいてリスクアセスメントが実施されている。

（出典）JST/CRDS 研究開発の俯瞰報告書 システム・情報科学技術分野（2017年）