参考資料1-2

分野・領域に係る強み分析・整理の作業結果（第1次的まとめ）

令和2年9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

実践的なサイバーセキュリティの研究分野　アカデミックな研究レベルの国際比較　（第1次的まとめ）

（1）通信系・アクセス系ネットワークセキュリティ

中分類:	小分類:			
通信系ネットワークセキュリティ	ネットワーク攻撃	同検知	同分析	同対策
	不正通信	同検知	同分析	同対策
アクセス系ネットワークセキュリティ	不正アクセス	同検知	同分析	同対策
	DoS攻撃	同検知	同分析	同対策
	悪性ドメイン構築	同検知	同分析	同対策

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	↗	早稲田大、NTT、横浜国立大、NICTなどが主要国際カンファレンスに採録され、プレゼンスが向上し、今後も期待できる分野のひとつである（IoTセキュリティ・Webセキュリティと重複する部分あり）。NICTにおけるNICTERやNOTICEなど、NTTにおける悪性ドメインに係る研究等、実践的かつ独自の研究が継続的に進められている。
米国	◎	→	伝統的に強く、世界をリードし、主要国際カンファレンスにおいても圧倒的に多数の発表を占めている。産業界でも強い。NSFやDARPA等から豊富な研究資金が供給され実データや大規模疑似データを用いて実用面でも理論面でも先進的な研究が継続的に実施されている。
欧州	◎	→	主要国際カンファレンスでは米国の◎には及ばないものの、研究拠点数や発表数を考慮すると中国や日本よりも強い。伝統的に強く、主要国際カンファレンスでも産業界でも強い。
その他（中国）	○	↗	主要国際カンファレンスでは、中国（清華大など）からの存在感が増している。量的に日本より若干リードしている印象。米国との共同研究だけでなく、単独の発表も増えてきている。

【研究領域の特徴】
ネットワークセキュリティ（侵入検知・攻撃検知）分野としては、1995年頃から存在するサイバーセキュリティの本流とも言える研究分野である。主要国際カンファレンスにおいて、ネットワークセキュリティは、必ずセッションが存在するが、2000～2005年頃のような盛り上がりはなく、2020年ではIoT/Webセキュリティ/Phishingといった周辺分野へ拡大している。DNS等通信基盤となっているが、DDoS対策などのように実課題がいまだに根強く残っているため、今後も継続する研究テーマであると考えられる。

（2）認証

中分類:	小分類:			
認証	なりすまし攻撃	同検知	同分析	ID管理、個人認証（生体認証含む）、ユーザ認証、人工物メトリクス、PKI

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	→	Tier2国際カンファレンス（AsiaCCS）には、暗号・認証系の発表がコンスタントにある。生体認証では、国際的にもNEC、日立、富士通等の産業技術が強く、主要国際カンファレンス（IJCB）でも一定の存在感。特に、NECはNISTコンペで精度での世界一位を取り続けている。
米国	◎	→	大学、企業いずれも非常に活発で、世界をリードし続けている。2020年の主要国際カンファレンス（IEEE S&P、ACM CCS、USENIX Security、NDSSの4大会議）では認証関連論文12件のうち4件が米国で、国別トップである。生体認証でも同様に国別トップである。GoogleやMicrosoftはOpenID ConnectやFIDOなどID連携、認証の標準仕様策定でも主導的に活動している。
欧州	○	→	大学等からの研究発表が活発。2020年の主要国際カンファレンス（4大会議）では認証関連論文12件のうち4件が欧州。生体認証では、仏IDEMIAなど産業技術で大きなシェアを持つ企業があり、研究発表も活発。
その他（中国）	○	↗	2020年の主要国際カンファレンス（4大会議）では認証関連論文12件のうち2件が中国で、国別2位である。顔認証でSensetimeなどベンチャー企業が国際コンペで高い成績を出し、IJCBでも存在感を高めている。

【研究領域の特徴】
ID管理では、Microsoftなど米国企業を中心に分散ID /自己主権IDの研究が活発。

評価の基準
【現状】◎：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
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

・実践的なサイバーセキュリティの研究分野とは、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。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。
・現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。

アカデミックな研究レベルの国際比較

（第1次的まとめ）

（3）Webセキュリティ

中分類:	小分類:			
Webセキュリティ	Web攻撃	同検知	同分析	同対策
	悪性サイト構築	同検知	同分析	同対策

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	↗	NTTを中心に主要国際カンファレンスで発表されるようになってきており、その一つのNDSSやTier3国際カンファレンス（DIMVA）で2020年にBest Paperをそれぞれ獲得（NTT・早稲田大、NTT・横浜国立大）。特に攻撃研究で良い成果が出ているように思われる。Webからの脅威を観測するセンサーをユーザに配布して観測を行うWarpDriveプロジェクトが実施されており、その成果がTier2国際カンファレンス（RAID）でも採択。
米国	◎	→	欧米大学が特に強い分野であり、Webセキュリティに関するデータの収集などの知見は、日本より欧米の方が多く持っているように思われる。（本領域において、検索エンジンとWebブラウザはデータの観測点であり、主要なものは米国企業が中心に開発されたものであるため。）
欧州	◎	→	欧米大学が特に強い分野であり、Webセキュリティに関するデータの収集などの知見は、日本より欧米の方が多く持っているように思われる。欧州ではEU一般データ保護規則の施行に伴い、Web上でのプライバシー情報に関する研究（Webトラッキング、Cookieの取り扱い、プライバシーポリシーの記述等）が促進されている。

【研究領域の特徴】

Webセキュリティでは、NDSSをはじめ、主要国際カンファレンスでは根強く人気が高いテーマである。米国を中心に近年ではcensorship（国家による検閲）やweb browser finger printingに関するプライバシー観点からの研究が盛ん。

（4）プログラム保護

中分類:	小分類:			
プログラム保護	マルウェア	同検知	同分析	同対策
	不正機能埋込	同検知	動的解析、表層解析、プログラム解析、静的解析	難読化

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	↗	マルウェア分析や対策などでは、NTTを中心にTier2国際カンファレンス（ACSAC、RAID等）への採録など存在感を増しつつある。特に、2019年はACSACでの採録が2件あった。継続的に提供されているMWSデータセットの存在もあり、特に国内研究会では多くの研究がなされている。
米国	◎	→	Fuzzingなどマルウェア分析技術は米欧が特に強く、サイバーセキュリティ研究の花形的研究であったため、存在感が高かった。学術研究から産業技術まで広くカバーかつ主導している。また、Lastlineのような大学発のベンチャーもあり、研究から産業へ昇華するスキームも整っていると言える。
欧州	○	→	マルウェア分析技術は米欧が特に強く、サイバーセキュリティ研究の花形的研究であったため、存在感が高かった。欧州・米国の有力大学の複数の研究室からなるiSecLabが2005年に発足して以来、現在も継続してマルウェア対策研究の主要な研究はiSecLabから出版され続けており、またLastlineもiSecLabを運営する研究者によって誕生した。

【研究領域の特徴】

マルウェア分析そのものの研究領域自体が下火にある印象であり、プログラム保護という考え方からCPUセキュリティ設計にシフトしているように思われる。

評価の基準

【現状】◎：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
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

- 実践的なサイバーセキュリティの研究分野とは、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。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。
- 現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。

アカデミックな研究レベルの国際比較

（第1次的まとめ）

（5）実装セキュリティ

中分類:	小分類:			
暗号実装	暗号実装攻撃	同検知	同分析	同対策
ハードウェアセキュリティ	ハードウェア実装攻撃	同検知	同分析	同対策
OSセキュリティ	OS実装攻撃	同検知	同分析	同対策
ソフトウェアセキュリティ	ソフトウェア実装攻撃	同検知	同分析	同対策

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	→	主要国際カンファレンス（USENIX Security、IEEE S&P、ACM CCS）などにも採録されており、一定の存在感がある。暗号に関連した実装セキュリティ分野でも主要国際カンファレンス（CHES）でBest Paper Awardを受賞するなど日本が国際的に一定の強みを発揮している。国内でも電子情報通信学会にハードウェアセキュリティ研究会が発足するなど活発化の傾向がみられる。
米国	○	↗	近年は米国でも関心が急速に高まっており、論文投稿数・採択数とも増加傾向が見られる。特に、ハードウェアトロイについては盛んに研究されている。また、実装セキュリティに関連したベンチャー企業も一定数存在する。
欧州	◎	→	本分野は欧州が研究者規模の面で牽引してきた。特に、SpectreやMeltdownに端を発したCPUの脆弱性については、欧州の研究者を中心に盛んに研究され、世界的に追従されている。また、暗号に関連した実装セキュリティについても、ECRYPT II等のEUプロジェクトの成果が質・量ともに特筆される。
その他（中国）	○	↗	近年は中国でも関心が急速に高まっており、論文投稿数・採択数とも増加傾向が見られる。特に、CPUの脆弱性については、主要国際カンファレンスでの発表が一定数あると認識している。

【研究領域の特徴】

OSセキュリティは下火であり、NECや三菱電機等の貢献によりサイドチャネル攻撃は2000年前後に日本でかなり進んだと思われる。現在、実装セキュリティ（ハードウェアセキュリティ）分野は世界的に拡大しており各地域で活発化している。この傾向はスコープに加える国際カンファレンス、主要国際カンファレンスでの関連論文数、参加者などがすべて増加していることから見てとれる。

（6）評価全般

中分類:	小分類:			
セキュリティ評価	セキュリティ実装不備	セキュリティ調査	セキュリティ分析	セキュリティ実装
	セキュリティ設計不備			セキュリティ設計
	セキュリティ対策不備			セキュリティ対策
リスク評価	脆弱性	同検知	同分析	同対策
	リスク	同検知	同分析	同管理
	脅威	同検知	同分析	同対策

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	↗	日本も評価に関わる攻撃研究の存在感が出てきている。特に、AIスピーカーへの攻撃やWebサービスへの攻撃などが主要国際カンファレンス（USENIX Security、NDSS）で発表されている。
米国	○	→	米欧が強く、特に大規模なセキュリティの調査や評価などは米欧の方が研究として実施されている印象がある。主要国際カンファレンス（IEEE S&P）では、米欧からコンシューマ向けIoT機器を販売する際のセキュリティ対策表記がどうあるべきかについて研究発表が2件なされ、攻撃技術に関するTier3国際カンファレンス（WOOT）も米欧の発表がほとんどである。
欧州	○	→	米欧が強く、特に大規模なセキュリティの調査や評価などは米欧の方が研究として実施されている印象がある。主要国際カンファレンス（IEEE S&P）では、米欧からコンシューマ向けIoT機器を販売する際のセキュリティ対策表記がどうあるべきかについて研究発表が2件なされ、攻撃技術に関するTier3国際カンファレンス（WOOT）も米欧の発表がほとんどである。欧州はセキュリティ評価に関する標準化活動を主導的に実施し始めている。

【研究領域の特徴】

網羅的なセキュリティ評価よりも、特定の新たな攻撃や現状調査を行い、それを結果的にセキュリティ向上につなげるというシナリオの研究が多い。日本では、実システムや製品に対する評価は控えられる傾向にあったが（ただし、生体認証に対する人工指による攻撃など先駆的な研究もある）、最近では適切な研究倫理考察、対応に基づき、実施されることが増えてきている。

評価の基準

【現状】◎：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
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

- 実践的なサイバーセキュリティの研究分野とは、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。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。
- 現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。

アカデミックな研究レベルの国際比較

（7）データセキュリティ

中分類:	小分類:	
プライバシー保護	プライバシー情報漏洩	同検知　同分析　加工技術
個人情報保護	個人情報漏洩	同検知　同分析　同対策
コンテンツ保護	コンテンツ不正流通	同検知　同分析　情報ハイディング

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	◎	↗	主要国際カンファレンス（USENIX Security、ACM CCS、IEEE S&P、CRYPTO）やTier2国際カンファレンス（ESORICS、PETS）にも採録されており、2016年にACM CCSでBest Paperを獲得（NEC）。また日本からPETSのプログラム委員も出しており存在感がある。国内でも、匿名加工競技PWS Cupでの取組やSCIS・CSSの発表件数の増加など、顕著な活動が行われている。プライバシー保護ではNTTとNECが牽引し、関連技術である秘密計算は商用までこぎつけた。
米国	◎	↗	主要国際カンファレンス（USENIX Securityなど）では、米国からの発表が大半を占めており、欧州がそれに続く。
欧州	◎	↗	主要国際カンファレンス（USENIX Securityなど）では、米国からの発表が大半を占めており、欧州がそれに続く。

【研究領域の特徴】

プライバシー保護関連の秘密計算、秘密分散技術などの理論・実装論文がここ数年で世界的にも増加している。また、種々の実システムからの個人情報漏洩対策などがホットトピックとして議論されている。2000年代前半の著作権保護・管理技術の研究はDVDのコピーガードがハッキングされたことにより下火となったと思われる。

（8）AIセキュリティ

中分類:	小分類:
AIセキュリティ	なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	↗	ここ数年AIセキュリティに関連する分野に参入する研究者が上昇傾向にある。機械学習系の主要国際カンファレンス（AAAI、KDD、IJCAI等）では筑波大・理研をはじめとして、国内からの研究が定期的に採録されている。本分野におけるセキュリティ系の国際カンファレンスにおける国内研究者のプレゼンスは低い。九州大の自動運転などが見られ、今後も拡大すると想像される。
米国	◎	↗	2013年頃より、GoogleやAppleに所属する研究者を中心に新しい概念が次々提案されてきた。大学、企業いずれも非常に活発で、企業はMicrosoftなどが発表。採録論文数の著者の約半数が米国であり、他国が主発表では米国は共著、米国が主発表では単独が多い。機械学習系の国際カンファレンスのみならず、セキュリティ系カンファレンスでもプレゼンスが高い。
欧州	○	↗	採録論文数の著者の約4分の1は欧州である。特にブラウンシュヴァイク工科大、ザールランド大をはじめ独国のプレゼンスが高い。実装関連の研究発表は欧州を中心に増加傾向にある。

【研究領域の特徴】

本分野は現在最もホットな研究分野の1つであり、どこの国も力を入れている競争が激しい分野である。主要国際カンファレンスでも複数のセッションが設けられることが多く、関連ワークショップ（AISecなど）も開催されている。セキュリティコミュニティのみならず、機械学習研究コミュニティがadversarial exampleなどに関する研究を精力的に実施している。

評価の基準

【現状】◎：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
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

- 実践的なサイバーセキュリティの研究分野とは、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。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。
- 現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。

アカデミックな研究レベルの国際比較

（9）IoTセキュリティ

中分類: IoTセキュリティ　小分類: なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	→	主要国際カンファレンス（NDSS）に共著で、Tier3国際カンファレンス（WOOT）に主著でそれぞれ採録されており、前者はDistinguished Paper Awardを受賞し、後者は高い被引用率を誇っている。国内の観測網（NICTのNICTER、JPCERT/CCのTSUBAMEなど）により、脆弱性発見等のIoTデバイスの分析も盛んに行われている。関連技術である暗号理論や実装セキュリティは日本が強みのある分野であり、利用が期待される軽量暗号とその実装等の分野では活動成果が見えている。さきがけや基盤研究において学術界での研究基盤もより整いつつある。
米国	○	↗	IoTサイバー攻撃が顕著になり、その攻撃実態の観測、IoTマルウェア解析や対策の研究が行われるようになった。攻撃の原因となる脆弱性の検知、脆弱性の原因となるソフトウェア開発における課題など、基盤となる技術に関する研究も進んでいる。
欧州	○	↗	研究の動向は米国に似るが、IoT機器のセキュリティ要件やガイドラインは各国が独立して策定しているものもあり、特定国でニーズが高い技術が出てくる可能性がある。英国・ブリストルやスペイン・サンタンデールなどスマートシティの実証実験が進んでいる。

【研究領域の特徴】

Mirai等の影響もあって、この数年注目度が高い領域であり、主要国際カンファレンスにおいてはセッションが必ず存在している。一方で、いろいろなテーマが出尽くした感もある。ただし、IoTと呼ばれるデバイスは日進月歩であり、今後出てくるデバイス（自動運転車、HEMS、医療なども含む）の新しい課題が出てくる可能性が常にある。

（10）サプライチェーンセキュリティ

中分類: サプライチェーンセキュリティ　小分類: なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	→	アカデミアでは、サプライチェーンセキュリティを主題とした研究発表は、ほとんどされていない。一方で、サプライチェーンセキュリティ確保のために活用できる要素技術（ハードウェアトロイ対策等）の研究は行われている。日本での取組は、経済産業省のサイバーセキュリティフレームワークとSIPでの研究推進がある。
米国	○	↗	主要国際カンファレンスでも、サプライチェーン全体を対象としたセキュリティはあまり盛んではないと思われる。一方、関連する要素技術（Fuzzing等）の研究は、特に米国・欧州で盛んと思われる。2019年のセキュリティカンファレンス（CODE BULE）において、ソフトウェアに係るサプライチェーンの講演が行われた。DARPAの研究プログラムにもサプライチェーンセキュリティが採択されている。ガイドライン策定（強制化）とブロックチェーン連携などの研究促進を実施している。本分野の関連研究として、MicrosoftのThe Enemy Within: Modern Supply Chain Attacksの例がある。
欧州	△	→	主要国際カンファレンスでも、サプライチェーン全体を対象としたセキュリティはあまり盛んではないと思われる。一方、関連する要素技術（Fuzzing等）の研究は、特に米国・欧州で盛んと思われる。欧州は認証フレームワークの策定（法制化）を実施している。

【研究領域の特徴】

多様なサプライヤーから部品等を調達して、製品を製造することが一般的になり、サプライチェーンのセキュリティの重要性が高まっている。脅威としては、サプライヤーを対象としたサイバー攻撃により、情報の窃取、製造物への不正なソフトウェアの混入、生産活動停止・妨害などの脅威があり、サプライチェーンのセキュリティは、非常に重要になっている。また、ソフトウェア部品表であるSBoMを調達の要件とする場合が増加傾向にある。

評価の基準

【現状】◎：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
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

- 実践的なサイバーセキュリティの研究分野とは、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。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。
- 現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。

アカデミックな研究レベルの国際比較

（11）自動車セキュリティ

中分類: 自動車セキュリティ　小分類: なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	→	横浜国立大などが車載制御ネットワークに関する攻撃手法を報告。セキュリティカンファレンス（Black Hat Europe）では、横浜国立大・トヨタが共同発表。産業系の標準関係の会議（Escar）では、日本の存在感あり。日本の自動運転プラットフォームAutowareは国際的な評価も高い。ISO/SAE21434で自動車のサイバーセキュリティの法制化に係るUN規則をどのように実現するかを規定する規格を策定中であるが、その標準化を独国と推進。
米国	○	→	ミシガン大、テキサス大などが車載LANのセキュリティ強化技術（IDS、Firewall）をSAE Technical Paperなどに積極的に投稿。ニューヨーク大、サウスウェスト研究所及びミシガン大交通研究所の共同リサーチプロジェクトがソフトウェアアップデート技術の標準フレームワーク等を発表。SAE主催で自動車ハッキングコンテストを実施し積極的に自動車へのセキュリティ攻撃技術を議論する取組が進んでいる。
欧州	○	→	Fraunhofer SIT等の欧州研究所及び大学機関がEVITAなどの自動車セキュリティ研究開発プロジェクトに参加。CANメッセージ認証方式、車載LANのセキュリティ強化技術（IDS、Firewall）、ハードウェアセキュリティモジュール、車車間及び路車間通信におけるセキュリティ要件定義などの技術分野の研究発表。独国、仏国、英国を中心にISO/SAE21434標準化を推進。

【研究領域の特徴】

自動車セキュリティの研究は一定数存在するが、数は少ない。主要国際カンファレンスでセッションを組まれることもない。現状の自動車での研究はやり尽くされた感もあり、各社がフレームワーク提案に参入してきた数年前に比べると、だいぶ落ち着いてきた印象である。ただし、今後、自動運転のプラットフォームの普及が進むと、セキュリティ課題が顕著になる可能性がある。AIセキュリティやIoTセキュリティの側面を含むため、分野横断的領域であり、注目株である。

（12）センサーセキュリティ

中分類: センサーセキュリティ　小分類: なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	↗	主要国際カンファレンス（USENIX Security、ACM CCS、IEEE S&P）で散発的に活動成果が見られるが、絶対数が少なく、国際的に目立っているとは言えない。ただし、この2年で採録された実績があるため、上昇傾向とした。また、センサーへの各種攻撃によるセキュリティ評価などが国内外で成果が出てきている。ハードウェアセキュリティ研究会などの活動も影響していると思われる。
米国	○	→	センサーの読取やセンサーへの注入に関するセキュリティの研究はミシガン大やワシントン大が強く、国際カンファレンスでも多数の論文がある。特に、ミシガン大では過去5年間だけでもセンサーセキュリティ関連で、主要国際カンファレンス（IEEE S&Pが4件、ACM CCSが2件）を含む多数の発表がなされており、同研究領域を牽引している。
欧州	△	→	主要国際カンファレンスでの発表件数やインパクトでは顕著な活動・成果はあまり見えていない。一部、レーダに係るセキュリティでは、主要国際カンファレンス（USENIX Security）やセキュリティカンファレンス（Black Hat）で活動成果が見られる。また、音声認識のセキュリティでベンチマークコンテスト開催等の活動が見られる。

【研究領域の特徴】

メッシュネットワークの鍵管理やルーティングなどの基礎研究がある一方、センサー用ネットワークのためのSIMカードがバルク販売されるようになるなど実用面で材料が揃いつつある。また、自動車応用等も含め、各種センサーを含むシステムが増加傾向にあることから、センサーそのものもしくはセンサーネットワーク・システムに対する攻撃及び防御の研究は今後急速に伸びる可能性がある。実システムへの攻撃は、現状では米国が圧倒的に存在感があり、日本を除くアジアでは中国や韓国の顕著な成果が散見される。

評価の基準

【現状】◎：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
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

- 実践的なサイバーセキュリティの研究分野とは、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。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。
- 現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。

アカデミックな研究レベルの国際比較

（13）モバイルセキュリティ

中分類: モバイルセキュリティ　小分類: なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	→	スマートフォンのハードウェアやソフトウェアを対象にした研究は増えておらず、ファームウェアやカーネル等の研究はほとんどない。端末外部の観測データからモバイル端末を保護する研究やプライバシー保護研究が目立つ成果。早稲田大・NTTを中心に、主要国際カンファレンスやTier2国際カンファレンス（AsiaCCS、SOUPS）に採録も日本の存在感は出せていない。NICT委託研究WarpDriveでAndroidが対象の実証実験が開始。
米国	○	↗	Android OSやAndroid malwareに関して米国を中心に研究が盛ん。2020年の主要国際カンファレンス（IEEE S&P、USENIX Security、NDSS）では本領域の論文数が11件であり、ファームウェア、カーネルなどスマートフォン内部のソフトウェア研究が増えていると思われる。
欧州	△	↗	2020年の主要国際カンファレンス（上記3つ）では本領域の論文数が6件であり、アプリを対象とした識別方法やセキュリティ機能の利用状況などの研究が多い。
その他（中国）	◎	↗	本領域は伝統的に中国の大学（復旦大、上海交通大等）から質が高い研究で主要国際カンファレンスに多数の論文が採録。2020年の主要国際カンファレンス（上記3つ）では本領域の論文数が5件であり、攻撃方法や脆弱性関連の研究が多いと思われる。

【研究領域の特徴】

Androidアプリの研究が主流だった分野であり、ここ10年で爆発的に進展して、サイバー系だけでなくソフトウェア工学系の主要国際カンファレンスでも論文が多数発表。研究のデータセット収集が比較的容易だったため、多くの研究者が本分野に参画。今でも、一定数の論文が主要国際カンファレンスで発表され続けており、手堅い分野。最近では、OSやファームウェア分析やエッジ環境下でのセキュリティに研究がシフトしてきている印象。また、新しいハードウェア機能が出てきているため、今後も重要な研究領域であると思われる。iOSを対象とした研究もAndroidに比べ少ないが行われている。

（14）人的要素セキュリティ

中分類: 人的要素セキュリティ（ユーザブルセキュリティ）　小分類: なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	↗	主要国際カンファレンス（ACM CCS）やTier2国際カンファレンス（SOUPS、ACSAC）などに採録されている。また、サイバー系ではないが、ヒューマンコンピュータインタラクション分野の主要国際カンファレンス（CHI）でも発表されている。
米国	◎	→	カーネギーメロン大CyLab Usable Privacy and Security Laboratory（CMU CUPS）のCranor教授がユーザブルセキュリティの第一人者。Cranor教授がTier2国際カンファレンス（SOUPS）を2005年に始め、それ以来、米国を中心にユーザブルセキュリティに関して研究が盛んに行われている。CMU CUPSのOB/OGが米国の各種大学で研究室を持ち、多くの有力研究グループが生まれている。
欧州	◎	↗	独国の複数の研究チーム（Mathew Smith、Sascha Fahl/Yasemi Acar）を中心に、ソフトウェアの脆弱性と開発者に着目した研究成果が主要国際カンファレンスやヒューマンコンピュータインタラクション分野の主要国際カンファレンス（CHI）で多数発表されている。特に、Sascha FahlとYasemi Acarはユーザブルセキュリティ分野の賞（John Karat Usable Privacy and Security Student Research Award）を受賞している。

【研究領域の特徴】

近年盛り上がっている分野であり、主要国際カンファレンス（USENIX Security）では、2020年に複数のセッションが設けられ、本分野の論文3件がDistinguished Paper Awardを受賞した。エンドユーザを対象にした研究だけでなく、なぜ脆弱性を生んでしまうのかといった開発者の行動原理の解明などに着目した研究も出てきている。

評価の基準

【現状】◎：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
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

- 実践的なサイバーセキュリティの研究分野とは、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。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。
- 現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。