様式 1-4-2 (2020-1)

令和元年度研究開発成果概要書

採 択 番 号　：　19501
研究開発課題名　：　欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発
副　　題　：　ブロックチェーン・ビッグデータ・クラウド及び IoT を使用したハイパーコネクテッドスマートシティを実現するマルチレイヤセキュリティ技術
Acronym　：　M-Sec

（1）研究開発の目的

本研究開発では、ブロックチェーン・ビッグデータ・クラウド及び IoT を使用したハイパーコネクテッドスマートシティを実現するマルチレイヤセキュリティ技術（M-Sec)の研究開発を通じて人やモノ、サービス同士の通信においてエンド-エンドのセキュリティを多重的に保証していき、デバイス自体のセキュリティ向上、ネットワークのレジリエンスやアウェアネス向上まで総合的なセキュリティ対策を解決する。具体的には以下の５つの社会的および技術的目標をもってプロジェクトを推進する。

目標 1：デジタルとフィジカルが結合したスマートオブジェクトの価値を取引可能とする新たな分散（decentralized）IoT アーキテクチャを確立

- P2P、Publish/Subscribe、メッセージキューイングなどの多様な通信手法を介して、物理的、意味的、あるいは役割的な近接性に基づき、データに対する需要と供給をマッチング
- アーキテクチャで実現するハイパーコネクテッドスマートシティにおいて生じうる様々なリスクを同定（目標２でそれらのリスクへ対処）
- 多様な通信チャネル上でサービス同士の動的な結合や管理が可能な、シームレスな「ハイパーコネクティビティ」を実現する技術を確立
- フィジカルな人やモノとそれらに対応するデジタルなエンティティとを結合する仮想化レイヤを実現してデジタルを介したフィジカルへのアクセス技術を確立

目標 2：ブロックチェーンを用いてスマートシティとそのユースケースでの、人やモノ、サービス同士のシームレスで自律的かつセキュアなインタラクション技術を確立

- 物理的、意味的、あるいは役割的な近接性に基づき IoT デバイスをサービスチェーンに効果的に組み込む複合最適化技術を確立
- スマートシティでの個人あるいは企業のユースケースにおいてセキュリティ要求を主体とする非機能要求に基づくサービスチェーンの動的組換技術を確立

目標 3：インターネットに代表される大規模かつ低信頼・低信用プラットフォーム上で、新たなセキュリティ、トラスト、プライバシ保護技術を確立

- ブロックチェーンにおいて軽量パブリックレジャーと信用保証技術を実現してセキュアな IoT データ取引基盤を確立
- IoT デバイス中のセンサからエッジシステム、クラウドシステム、エンドユーザシステムに渡るエンド-エンドのセキュリティ保護技術を確立
- ソフトウエア工学のモデル検査技術等を用いてソフトウエアの自動検証と自己修復技術を構築し、ソフトウエアそのもののセキュリティ保証技術を確立
- ハイパーコネクテッドスマートシティにおけるマルチレイヤのセキュリティ・プライバシ分析フレームワークを確立

目標４：次世代の分散 IoT エコシステムのリファレンス実装とその可能性・持続性を検証
- スマートオブジェクト同士がデジタル情報財を取引でき、もって IoT 関連ステークホルダーが収益性の高いビジネスを展開可能な、革新的なマーケットプレイスを実現
- 上記のマーケットプレイスを社会実装し、データの需要側と供給側の横軸、データの生成側であるセンサとそこから受益するビジネス側の縦軸に広く跨る実社会ユースケースを通して実証
- マーケットプレイスへの新規参入を促進するために、破壊的ユースケースと創造的ビジネス企画とを広く公募し、プロジェクト期間中の起業を促進

目標５：プロジェクトの社会的インパクトの最大化
- 柔軟かつ再利用可能なビジネスモデルを構築するとともに個人情報やパーソナルデータの保護・利活用に関するベストプラクティスを蓄積
- 産業界との連携を通じて成果物の周知と社会実装を促進
- 学術界との連携を通じて本研究領域に関する新たな研究コミュニティを醸成するとともに次世代の人材を育成

（2）研究開発期間

平成 30 年度から令和３年度（36 ヶ月）

（3）実施機関

【日本】

- 東日本電信電話株式会社＜代表研究者＞
- 学校法人慶應義塾 慶應義塾大学 SFC 研究所
- 国立大学法人横浜国立大学
- 大学共同利用機関法人情報・システム研究機構
- 学校法人早稲田大学
- 株式会社エヌ・ティ・ティ・データ経営研究所

（4）研究開発予算（契約額）

総額 186 百万円（令和元年度　62 百万円）

※百万円未満切り上げ

（5）研究開発項目と担当

〈凡例〉
WP　：Work　Package

<u>WP1　プロジェクトおよびイノベーションマネジメント（東日本電信電話株式会社）</u>

Task1.1…プロジェクトの管理・運営（東日本電信電話株式会社）
Task1.2…モニタリングと品質管理（東日本電信電話株式会社）
Task1.3…戦略的イノベーションマネジメント及びデータマネジメント（東日本電信電話株式会社）

<u>WP2　ユースケースとパイロットスタディに関する市民参加、技術統合と評価（学校法人慶應義塾 慶應義塾大学 SFC 研究所）</u>

Task2.1…M-Sec ユースケースの検討（東日本電信電話株式会社）
Task2.2…M-Sec 実証実験の計画・実施、市民参加型の取り組み（東日本電信電話株式会社）

Task2.3…技術統合（学校法人慶應義塾 慶應義塾大学 SFC 研究所）

WP3　ハイパーコネクテッドスマートシティのための要求と設計（大学共同利用機関法人情報・システム研究機構　国立情報学研究所）

Task3.1…システムレベル及びユーザレベルの要求の分析（大学共同利用機関法人情報・システム研究機構　国立情報学研究所）

Task3.2…M-Sec アーキテクチャ（学校法人早稲田大学）

Task3.3…ハイパーコネクテッドスマートシティの要素技術（学校法人慶應義塾 慶應義塾大学 SFC 研究所）

WP4　マルチレイヤセキュリティ技術(学校法人早稲田大学)

Task4.1…IoT セキュリティ(国立大学法人横浜国立大学)

Task4.2…クラウドおよびデータレベルセキュリティ(国立大学法人横浜国立大学)

Task4.3…P2P レベルのセキュリティとブロックチェーン（大学共同利用機関法人情報・システム研究機構　国立情報学研究所)

Task4.4…アプリケーションレベルのセキュリティ(大学共同利用機関法人情報・システム研究機構　国立情報学研究所)

Task4.5…エンド-エンドセキュリティ(学校法人慶應義塾 慶應義塾大学 SFC 研究所)

WP5　GDPR（General Data Protection Regulation），普及、利活用、持続可能性（サステナビリティ）(株式会社エヌ・ティ・ティ・データ経営研究所)

Task5.1…普及展開・研究成果発表(東日本電信電話株式会社)

Task5.2…利活用及び知財(株式会社エヌ・ティ・ティ・データ経営研究所)

Task5.3…GDPR 遵守(株式会社エヌ・ティ・ティ・データ経営研究所)

Task5.4…コミュニティ形成、持続可能性関連活動(学校法人慶應義塾 慶應義塾大学 SFC 研究所)

（6）特許出願、外部発表等

		累計（件）	当該年度（件）
特許出願	国内出願	0	0
	外国出願	0	0
外部発表等	研究論文	7	6
	その他研究発表	41	23
	標準化提案	0	0
	プレスリリース・報道	1	0
	展示会	2	0
	受賞・表彰	0	0

（7）具体的な実施内容と成果

WP1　プロジェクトおよびイノベーションマネジメント（東日本電信電話株式会社）

Task1.1 プロジェクトの管理・運営（東日本電信電話株式会社）

- 日本側・欧州側の研究者の意志疎通及び研究の進捗状況共有の WEB 会議を主催しマンスリーにて実施した。また、年２回開催の F2F ミーティングにおいて日本開催に向けて主催者として各種調整を行った。

Task1.2…モニタリングと品質管理（東日本電信電話株式会社）

- 日本側の本研究進捗管理を実施する為の定例ミーティングを主催し各タスクの進捗、課題を共有し、進捗遅延や課題が有った場合は解決に向けた対策を講じる為の調整を実施した。

Task1.3…戦略的イノベーションマネジメント及びデータマネジメント（東日本電信電話株式会社）

- 社会課題の解決に向け、プロジェクトの成果がどのように利活用できるのか、社会的・経済的影響の評価を行った。

WP2　ユースケースとパイロットスタディに関する市民参加、技術統合と評価（学校法人慶應義塾 慶應義塾大学 SFC 研究所）

Task2.1…M-Sec ユースケースの検討（東日本電信電話株式会社）

- フィールドトライアル自治体である藤沢市とサンタンデール市それぞれの地域が抱える現状の課題・ニーズや保有するデータ・資産などの把握と分析を行った。その結果を整理し、それらを解決するためのユースケースの最新化をした。

Task2.2…M-Sec 実証実験の計画・実施、市民参加型の取り組み（東日本電信電話株式会社）

- Task２.１で策定したユースケースに基づいた実証実験の実現に向けて、地域及び住民の課題を分析・整理し、本研究開発におけるフィールドトライアルに参画すべきステークホルダーについて藤沢市と協議しながら参画を促し、フィールドトライアルを実施していくうえでの調整を行った。

Task2.3…技術統合（学校法人慶應義塾 慶應義塾大学 SFC 研究所）

- 各タスクで研究開発を行う要素技術を取りまとめ、全体として M-Sec アーキテクチャを構成した。令和 2 年度に実施予定の神奈川県藤沢市等での実証実験を念頭に置き、M-Sec アーキテクチャのプロトタイプとして構築している。

WP3　ハイパーコネクテッドスマートシティのための要求と設計（大学共同利用機関法人情報・システム研究機構　国立情報学研究所）

Task3.1…システムレベル及びユーザレベルの要求の分析（大学共同利用機関法人情報・システム研究機構　国立情報学研究所）

- M-Sec ユースケースとパイロットの WP2 でのさらなる分析・検討に沿って，初版で取りまとめた M-Sec フレームワークの機能要件とセキュリティ等の非機能要件の分析・検討をさらに進めた。

Task3.2…M-Sec アーキテクチャ（学校法人早稲田大学）

- Task3.1 で識別したシステムレベル・ユーザレベル要求から、初期の M-Sec アーキテクチャを構築した。また、構築した初期の M-Sec アーキテクチャの洗練化を行った。具体的には、ユースケースを実現するアーキテクチャに基づくアセット間相互作用を、ユースケース毎に分析し、初期アーキテクチャの妥当性と洗練化を行った。

Task3.3…ハイパーコネクテッドスマートシティの要素技術（学校法人慶應義塾 慶應義塾大学 SFC 研究所）

- ハイパーコネクテッドスマートシティにおける、特にセキュリティの観点でのリスク分析を行った。リスク分析を行うにあたっては欧州側研究機関とも連携し、ユースケースを具体的に念頭に置いた上でエッジ側、クラウド側、エンドツーエンドのデータ流通におけるリスクを、最終的な令和２年６月の成果提出に向けて、網羅的に整理・検討した。

WP4　マルチレイヤセキュリティ技術（学校法人早稲田大学）

Task4.1…IoT セキュリティ(国立大学法人横浜国立大学)

- ハイパーコネクテッド社会を構成する IoT デバイスのセキュリティ実現を目指し、IoT 機器向け IDS(Intrusion Detection System)の設計、プロトタイプ実装を行った。

Task4.2…クラウドおよびデータレベルセキュリティ(国立大学法人横浜国立大学)

- ハイパーコネクテッド社会を構成するクラウドおよびデータレベルのセキュリティ実現を目指し、軽量な暗号化技術を用いて、IoT デバイスとクラウドの間で行われる通信の安全性を確保する技術と、センサで観測された攻撃通信の集約・可視化を行う技術（Visualization Tool for Security）の設計、プロトタイプ実装を行った。

Task4.3…P2P レベルのセキュリティとブロックチェーン（大学共同利用機関法人情報・システム研究機構　国立情報学研究所)

- M-Sec プラットフォームの要件に沿って P2P レベルのセキュリティとブロックチェーンの技術的な課題の検討、分析を行い、“Blockchain Framework and Middleware Services”と“IoT Marketplace”デモの設計・実装を行った。

Task4.4…アプリケーションレベルのセキュリティ(大学共同利用機関法人情報・システム研究機構　国立情報学研究所)

- M-Sec プラットフォームの要件に沿ってアプリケーションレベルのセキュリティの技術的な課題の検討、分析を行い、“the Crypto Companion Database”と“Security Analysis Tool”デモの設計・実装を行った。

Task4.5…エンド-エンドセキュリティ(学校法人慶應義塾 慶應義塾大学 SFC 研究所)

- Publish/subscribe に基づくセンサデータ流通基盤を介したエンドツーエンドの通信において、データ流通基盤に対する機密性を確保するため、publisher が subscriber との暗号鍵を用いて、送信データを暗号化する技術を研究開発した。

WP5　GDPR（General Data Protection Regulation），普及、利活用、持続可能性（サステナビリティ）(株式会社エヌ・ティ・ティ・データ経営研究所)

Task5.1…普及展開・研究成果発表(東日本電信電話株式会社)

- 研究活動全体のスケジュール・計画を整理し、各プロセスにおいて適切なタイミングで対外発表を実施し、関係者や一般市民等に本研究活動内容を伝えるウェブサイトやフライヤーなどの広告物を作成した。標準化団体への M-Sec 紹介について欧州側と連携しながら適切な団体に対して効果的な提案活動を進める検討を行った。De dure 標準団体、Forum 標準団体など引き続き最も効果的なアプローチを検討して行く。特に IIC（Industrial Internet Consortium）の SecurityWG、TestbedWG に M-Sec の紹介をしたい要望を出した。

Task5.2…利活用及び知財(株式会社エヌ・ティ・ティ・データ経営研究所)

- 2018 年度のプロジェクトの活動を踏まえた M-Sec ソリューションの市場での活用方法および妥当性について検討した。競合機関及び製品の、市場分析についての草案作成を実施し、それらから当プロジェクト成果物の強みと弱みを検討した。また知的財産権（IPR）の効率的かつ効果的な取り扱いについても検討を実施した。

Task5.3…GDPR 遵守(株式会社エヌ・ティ・ティ・データ経営研究所)

- 2019 年度のプロジェクト活動の中で、GDPR ガイドラインに準拠したデータ取扱のための調査を必要に応じて実施した。それらの GDPR の定義・分析に基づき、日本での個人情報保護法との相関関係を導き日本企業へのガイドライン策定への課題や、blockchain に関わる GDPR 法規則の調査事項等を整理した。

Task5.4…コミュニティ形成、持続可能性関連活動(学校法人慶應義塾 慶應義塾大学 SFC 研究所)

- 日本国内のコミュニティ活動として、「地域 IoT と情報力研究コンソーシアム」の活動を継続推進した。第 3 回シンポジウム開催、健康情報コンソーシアムとの合同シンポジウム、勉強会を開催（勉強会 4 回、WG3 回）した。

（8）外国の実施機関

【欧州】

- Worldline Iberia SA (スペイン)＜代表研究者＞
- National Technical University of Atene（ギリシャ）
- CEA-LETI(フランス)
- F6S Network Limited（アイルランド）
- Tecnolog í as, Servicios Telem á ticos y Sistemas, S.A. (スペイン)
- Santander 市（スペイン）