

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)
- 多様な通信チャン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え技術を確立

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、プライバシー保護技術を確立

- 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
- ソフトウェア工学のモデル検査技術等を用いてソフトウェアの自動検証と自己修復技術を構築し、ソフトウェ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・プライバシー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 (39 カ月間)

(3) 実施機関

- ・ 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 2 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

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)

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)

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)

Task2.2…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)

Task2.4…システム全体の妥当性確認と評価 (学校法人早稲田大学)

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 (システムナビリティ) (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	12	5
	その他研究発表	56	14
	標準化提案・採択	0	0
	プレスリリース・報道	1	0
	展示会	4	2
	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・欧州側研究者の意志疎通及び研究の進捗状況の共有のため WEB 会議を主催し隔週にて実施した。また、年 2 回開催の F2F ミーティングにおいてはコロナ禍での渡航がかなわなかったためオンライン実施に変更し各種調整を行った。
- 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、進捗遅延や課題があ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）

Task2.2...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）

- ユースケースの検討をもとに藤沢市やステークホルダーと協議しながらコロナ禍での、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い、M-Sec プラットフォームを活用した実証シナリオを実施、検証をした。
- WP3 では、Keio SOXFire と ICCS の MarketPlace との Integration を進め、環境センサデータを MarketPlace 上で閲覧できることをレビュー会議でデモを実施した。
- WP4 では、ハイパーコネクテッド参加型センシングのスマホアプリである、SmileCityReport を用いた初めての実証実験を藤沢市の Jazz Meeting イベントで実施した。特に、プライバシー保護のための画像処理技術“GANonymizer”の有効性も具体的な実証現場で確認できた。

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。特にUC3ではYNUのセキュリティ技術、ICCSのMarketPlaceとの連携により、M-Secプロジェクトとしての全体アーキテクチャ実現に貢献した。UC4では、藤沢市の実証を元にSantanderへの展開のために、SmileCityReportのiPhone版、Android版それぞれのグローバル版を開発した。

Task2.4...システム全体の妥当性確認と評価（学校法人早稲田大学）

- 最終年度に実施するパイロットシステムの妥当性確認・評価に向けて、実証シナリオの洗練化に対応して各パイロットで評価するKPIの再検討、洗練化を行った。

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 プラットフォーム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、他の WP の Task と連携してさらに進め、システムレベル及びユーザレベルの要求の最終版の取りまとめを完了した。

Task3.2...M-Sec アーキテクチャ（学校法人早稲田大学）

- 前年度に構築した成果を洗練化し、M-Sec アーキテクチャを定義した。

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の結果を TST, YNU と連携して報告書 Deliverables 3.5 としてまとめた。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、特にユースケースを具体的に念頭に置いた視点からエッジ側、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

クを網羅的に検討した。

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)

- IoT 機器向け IDS の実装改善・実験を行った。藤沢市での Pilot-1 では、攻撃通信の90%以上をブロックするという Use-Case3 の目標 (D2.3.2) を達成した。更に攻撃通信の完全ブロックを目指し、ステルスセキュリティ機能を介しての安全なリモートアクセスを追加してセキュリティを強化する手法を開発した。この機能は、ポートを非表示に保ち、正しいシークレットロックシーケンスを受信した時にのみポートが開くもので、Pilot-2 で適用評価する。

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)

- 軽量の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・可視化を行う技術の実装改善・実験を行った。Pilot-1 では、Visualization Tool for Security の攻撃通信の集約・可視化を行う機能の有効性が確認できた。Pilot-2 では、ユーザ位置情報機能を用いて、IoT デバイスの正確な位置を表示する機能改善版を適用評価する。

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基づいて、“Blockchain Framework and Middleware Services” の設計・実装を完了し、ブロックチェーンの構築と P2P レベルのセキュリティを実現した。

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基づいて、“IoT Marketplace”, “Modal System Transition Analyzer” 及び “Security Analysis Tool” の設計・実装を完了し、アプリケーションのセキュリティを実現した。

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、悪意のあるユーザ等によるアタックからデータを保護するために、publisher および subscriber それぞれのアカウント機構と、データの暗号化機構を YNU と連携することによる実現性を検討した。

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・場所・関係者に対して発表を行うとともに、関係者や一般市民等に本研究活動内容を伝えるフライヤーなどの広告物を作成した。また、標準化に向け IoT やセキュリティ、クラウド、ビッグデータ等に関する標準化団体と情報交換を行い、M-Sec の研究成果に関して標準化団体へ紹介や提案等を実施した。

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)

- 2019 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。特に、競合サービスである中小企業規模の IoT プラットフォームとの比較を行い、差別化の発見を意識して、サービス価値向上を検討した。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整理した。

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

- 2020 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いのための調査とモニタリングをクロスボーダーユースケースを中心に必要に応じて実施した。それら 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、具体的ユースケース事例毎の対処事項と、対応方策を検討した。

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)

- プロジェクトメンバーとステークホルダーが情報交換できるオンラインプラットフォームの企画、ワークショップやハッカソンなどといったイベントの企画については、M-Sec プロジェクトとして開催した各 Webinar にプレゼンターとして参加した。他コミュニティへの参加としては、慶応大学が推進している神奈川県エリアでのスマートシティコンソーシアムである「地域 IoT と情報力研究コンソーシアム」において M-Sec の活動を紹介し、具体的なソリューションの水平展開や実証における連携などの可能性について検討した。具体的な活動としては、コロナ対策として藤沢市の飲食店における換気度を検証するための CO2 センサーの設置などをこのコンソーシアムメンバーとの連携により進めた。

(8) 今後の研究開発計画

これまでの実証実験で得られたデータの分析を行い、各実証実験にマッピングされた日欧の技術要素間の連携が円滑に機能して利用されているかを検証するとともにクロスボーダー実証を実施し、成果や効果、汎用性について評価を行う。また、実証協力自治体である藤沢市及び関連する機関からのフィードバック等により得られた教訓を踏まえ、課題の解決につながるようなプラットフォームやアプリケーション等をさらに洗練、進化させ、実用化を目指した取り組みを行う。

(9) 外国の実施機関

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