

令和 3 年 5 月 24 日現在

機関番号：14401

研究種目：基盤研究(C)（一般）

研究期間：2017～2020

課題番号：17K00123

研究課題名（和文）セキュアで透過的なIoTエージェントプラットフォームの研究

研究課題名（英文）Research on Secure and Transparent IoT Agent Platform

研究代表者

中川 郁夫（NAKAGAWA, IKUO）

大阪大学・サイバーメディアセンター・招へい准教授

研究者番号：70647437

交付決定額（研究期間全体）：（直接経費） 3,500,000円

研究成果の概要（和文）：セキュアで透過的なIoTエージェントプラットフォームの研究を行った。本研究はクラウド上にエージェントプラットフォームを設置し、IoTデバイスのデジタルツインを構成するIoTエージェントを配置、IoTデバイスが持つべきデバイス機能と、通信・セキュリティなどのIoT機能を分離する。同アーキテクチャは、運用・ポリシーの異なる機能を完全に分離し、通信やセキュリティをサービスネットワーク上で運用・管理できることを特徴とする。そのため、従来、IoTの知見やノウハウの蓄積をしてこなかったデバイスベンダーであっても、容易にIoTサービスの展開が可能になる。

研究成果の学術的意義や社会的意義

IoT (Internet of Things) が注目を集め、さまざまなデバイスがネットにつながり、新たなIoTサービスが登場しているが、同時に、IoTデバイスのセキュリティが深刻な問題を引き起こしている。本研究では、IoTデバイスにデバイス本来の機能とIoT機能を混在させることがセキュリティ上の課題を引き起こしていると考えられる。そのため、デバイス本来の機能と、通信やセキュリティなどのIoT機能を分離することで課題解決を目指す。本研究で提案するアーキテクチャはクラウド上にIoTエージェントを構成し、デバイスが本来の機能に専念できる仕組みを提供する。

研究成果の概要（英文）：We proposed IoT Agent Platform with Secure and Transparent mechanism. In our architecture, IoT agent platform on a cloud service has IoT agents which consists digital twins for various IoT devices.

One of our goal is to divide device features and IoT (communication and security) features. The architecture separates two operational domains that is physical devices with physical features and IoT domain with communication and security features. Device vendors with poor knowledge or experiences for IoT would be able to deploy new IoT services with IoT agent platform which would be operated by cloud service provider.

研究分野：IoT

キーワード：IoT エージェント 秘匿分散統計解析手法 透過的クラウド

1. 研究開始当初の背景

IoT (Internet of Things) 時代には膨大な数のセンサーやデバイスがネットに接続され、その数は指数的に増加を続けている。これらのセンサーからは、例えば、位置情報、温湿度、音、個人の購買行動や行動履歴を含むあらゆる情報が収集され、気象、交通、防犯、医療・ヘルスケア、工業、農業はもちろん、ビジネスの現場においても実用的な活用が始まっていた。

一方、IoT デバイスのセキュリティ確保は極めて重要な課題であると認識されていた。例えば、研究開始当時には KrebsOnSecurity への DDoS アタックの事例[*] (2016/9) では、世界中に存在する膨大な数の IoT デバイスが不正に制御され、特定のシステムに対して 620GB ものトラフィックを「送りつけた」ことが報告されていた。

IoT デバイスに関しては、セキュリティに関する次のような本質的な課題が指摘されていた。

- ✓ 家電や車、工作機器などのライフタイムが IoT システムに比較して圧倒的に長い
- ✓ デバイスのサポートや保守は、セキュリティインシデントの緊急度を想定していない
- ✓ 所有者・利用者が IoT の仕組みやセキュリティ対策の必要性を理解・意識していない

上記の課題は、従来の物理デバイスに無理やり IoT 機能を持たせたために生じたギャップであり、根本的な解決策は物理デバイスと IoT 機能、特にセキュリティ機能を分離することが解決策の一つであると考えられた。

2. 研究の目的

本研究ではクラウド上のエージェントモデルにより、上記課題への解決策を実現する方法を提案した。本研究が目指すモデルは、デバイスが持つ IoT 機能とセキュリティ機能を分離し、前者をクラウド上のエージェントで仲介・代替、後者をクラウド上のエージェントで実装、更新、管理、運用する。このことは、各デバイスが外部と直接通信する必要性を排除し、次のようなメリットをもたらすことを目指した。

- ✓ デバイスのライフサイクルにあわせて、クラウド上でセキュリティ機能を管理・更新できる
- ✓ 緊急度・重要度に応じてクラウド上でインシデントに対応できる
- ✓ デバイスの所有者・利用者ではなく事業者がセキュリティ上の責任を担うことができる

本モデルでは、デバイスが本来持つ物理的機能と、IoT 機能の実現に必要な通信・データ処理機能に分離する。物理的機能はデバイス本来の機能だが、IoT 機能は付加的な機能であり、同機能をクラウド上のエージェントに対応付けて (Digital Twin) クラウド上で実装することが可能である。

この際、IoT セキュリティに関わる機能は IoT 機能の一部であり、クラウド上のエージェントにその機能を実装する。クラウド上のエージェントはクラウド事業者がサービスとして運用することを想定しており、監視・運用やセキュリティインシデント対応などはインターネットサービスとして求められる品質が期待できる。また、その一方で、物理デバイスが必要とする通信はエージェントとの限られた通信に限定することが可能であり、物理デバイスのセキュリティを向上させることができる。

また、本研究では、クラウド上でエージェントがデータを扱う際に課題になりえる、次の 2 つの機能についても研究を行った。

- ✓ 課題-1: エージェントを仲介することによるデータ漏洩リスク増
- ✓ 課題-2: エージェント機能の実装に関わるシステム開発コスト増

上記、課題-1については秘匿分散技術を応用した。中川、下條は科研費プロジェクト「インターネットクラウド環境を用いたセンサーデータの分散解析手法の研究」において IoT デバイスが扱うデータのプライバシー情報の漏洩リスク低減のための技術開発を行った。同成果の秘匿分散技術をクラウド上のエージェントに応用し、エージェントが扱うデータの漏洩リスクを低減する。

また、中川は IoT デバイスがクラウド上の計算機リソースを透過的に利用するためのフレームワークの研究を進めている。同透過的クラウドモデルは、上記システム開発コストを圧倒的に軽減する。

3. 研究の方法

4 カ年（コロナの影響で研究機関を延長したため）にわたる研究をステップに分けて記述する。

<初年度 [2017] IoT のエージェントモデルに関する研究>

本研究の中核となる IoT エージェントモデルのアーキテクチャ設計及び基本機能のプロトタイプ実装、及びその有効性の検証を行った。

- ✓ デバイスの機能モデル/コミュニケーションモデルの整理とセキュリティ機能の分離
- ✓ エージェントプラットフォームの設計とプロトタイプ実装
- ✓ プロトタイプの機能検証とエージェントモデルの有効性の検証

<2 年目 [2018] エージェントプラットフォームの高機能化>

上記、IoT エージェントモデルを拡張し、同モデルに以下の機能を実装した。

- ✓ エージェントが扱うデータの秘匿分散化
- ✓ 透過的な機能呼び出しのフレームワーク化

<3 年目以降 [2019, 2020] エージェントプラットフォームの実用化研究>

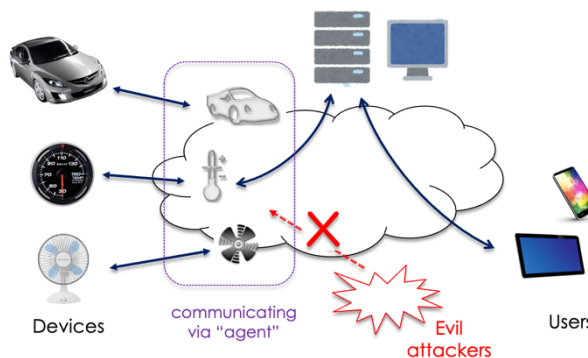
エージェントプラットフォームの産業応用の可能性の検討を行った。検討にあたっては、中川が参加する Tクラウド研究会（代表：東京大学 江崎教授）での検討・ディスカッションや、同会員との研究・検討会を通して実現性及び課題と対応策について検討した。

4. 研究成果

<初年度 [2017] IoT のエージェントモデルに関する研究>

IoT エージェントモデルの基本アーキテクチャを設計した。右に、簡単な概念図を示す。IoT エージェントはクラウド上に配置される。各物理デバイスはひとつの IoT エージェントが対応付けられる（複雑なデバイスには機能や要素が入れ子構造になる）。

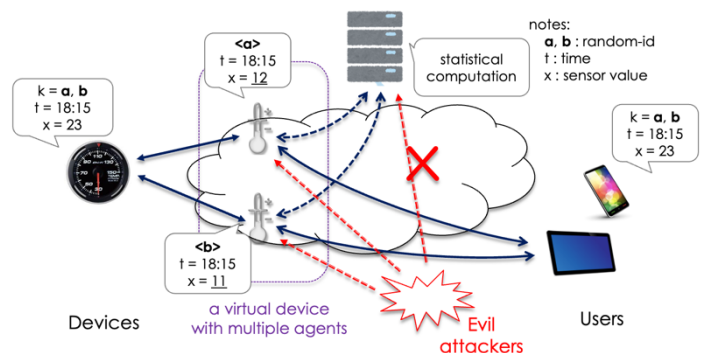
IoT エージェントは、IoT に必要な通信やデータ処理の機能を有し、外部のすべての通信はエージェントを介して行う。結果的に、デバイスはインターネットとの直接通信を行うことなく、すべてのセキュリティ機能は IoT エージェントが担うことになる。なお、本研究では、IoT エージェントはクラウドサービスの一環として（例えば“Agent as a Service” などの形で）提供されることを想定しており、IoT 機能と関連するセキュリティに関する監視・運用責任をクラウド事業者が担うことを想定した。



本研究では、同コンセプトに基づいて、クラウド上での IoT エージェントの配置や実装方法、機能などについて検討しプロトタイプ実装を行った。また、IoT エージェントのプロトタイプを用いて、デバイスが有するべき IoT 機能をクラウド上で実装できること、および、デバイスと外部ネットワークの通信を遮断することが可能であることなど、基本コンセプトの有効性を確認した。

<2 年目 [2018] エージェントプラットフォームの高機能化>

エージェントが扱うデータの秘匿分散化では、本エージェントモデルに、中川、下條らが研究してきた秘匿分散統計解析手法を応用した。具体的には、IoT エージェントを複数の異なるクラウド上で実装し、各 IoT エージェントにランダムシェアによって秘匿分散されたデータを保存することで、クラウド上でのデータ漏えいリスクを低減し、かつ、所有者だけが必要に応じてデータを参照することを可能にした。



また、透過的な機能呼び出しのフレームワーク化にあたっては、中川が研究を進める透過的クラウドの技術を応用し、IoT エージェントをクラウド上の透過的オブジェクトとして扱うことによって、通信やデータベースを意識しない簡単な IoT 機能の開発を可能とした。なお、透過的クラウドの技術はスケールアウト型のデータ処理基盤を基本としており、クラウド上でスケラブルかつ信頼性の高いエージェント処理基盤になりえる。

<3 年目以降 [2019, 2020] エージェントプラットフォームの実用化研究>

実用化研究では、いくつかの具体的なビジネスシーンを想定し、本研究が提案する IoT エージェントプラットフォームモデルの実用化・産業応用可能性について検討した。以下では、T クラウド研究会での検討・ディスカッションや企業ヒアリングなどを通して検討したビジネスシーンから抜粋して述べる。

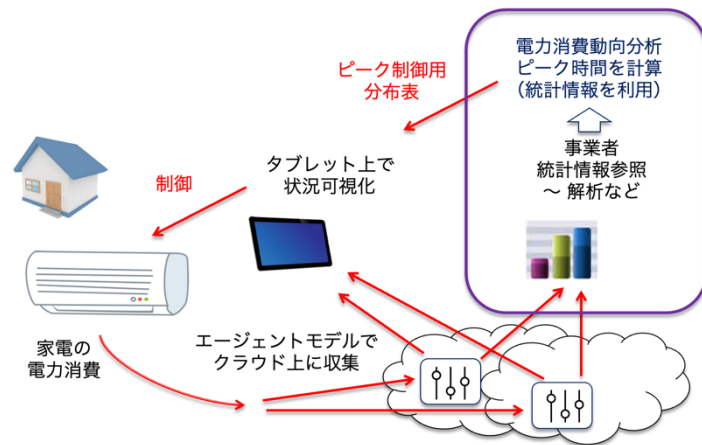
[スマートホームへの応用]

家電がネットにつながることによって、動的に家電の稼働状況や電力使用量などを把握する、スマートホームへの応用を検討した。

本モデルでは、家電の IoT 機能をクラウド上のエージェントが代替することで、家電を外部ネットワークから分離する。

また、本研究では、Nest Labs が提供した、街全体のエネルギー使用量に応じて家電を動的に制御する仕組みへの適応も検討した。

同サービスでは、事業者が統計情報を取得して街全体の電力消費のピーク制御を行うことを特徴とするが、本モデルの秘匿分散モデルの応用により、エージェント上にデータを秘匿分散したままで街全体のエネルギー制御が可能になるなど、技術的相性の良さが確認できた。



[ヘルスケアデバイスへの応用]

ヘルスケアデバイスに対して、クラウド上の IoT エージェントを配置して IoT 機能を代替するモデルを検討した。ヘルスケア情報は個人に関わる機微な情報を持ちえることから、秘匿分散モデルの応用を前提とした。ひとつのヘルスケアデバイスに対して、複数の IoT エージェントが、それぞれ異なるクラウド上に分散配置され、データを秘匿分散して保持する。データは所有者のみが必要なときに参照することが可能であり、クラウド上からのデータ漏えいリスクを低減できることを確認した。

多数のヘルスケアデバイス利用者のデータから統計データなどを取得し、利用者全体での健康情報を統計処理する場合など、秘匿分散統計解析手法の強みを活かして、事業者側が個々のヘルスケアデバイスの個別データを必要とせずに、正確に統計処理ができることを確認した。

一方で、ヘルスケアデバイスから収集されるデータから(例えば、歩数計データから取得されるデータから、歩数のランキングを集計する場合など)事業者が明示的な数値を必要とする場合には、データを解読するためのキーをデバイスの所有者と事業者が共有する必要があり、提供されるサービスによっては、セキュリティ上の対応に工夫が必要になることなども明らかになった。

[実用化に向けたその他の課題]

IoT エージェントプラットフォームの実用化に向けては、クラウド上でのサービスモデルが鍵を握る。技術的には、本研究で提案するアーキテクチャ及び実装を用いることで、デバイス上の IoT 機能をクラウド上のエージェントに代替させることが可能であることは確認できた。なお、本研究では、実用にあたって、責任分界点の定義、信頼性指標の定義、エージェントの状態の可視化・監視、などサービス上のさまざまな定義や実装が必要であることも検討し、今後の、実用化検討のための整理を行った。

5. 主な発表論文等

〔雑誌論文〕 計2件（うち査読付論文 2件/うち国際共著 1件/うちオープンアクセス 2件）

1. 著者名 Ikuo Nakagawa, Shinji Shimojo	4. 巻 2
2. 論文標題 Secure IoT Agent Platform with m-Cloud Distributed Statistical Computation Mechanism	5. 発行年 2018年
3. 雑誌名 2018 IEEE 42nd Annual Computer Software and Applications Conference	6. 最初と最後の頁 528-533
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/COMPSAC.2018.10289	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1. 著者名 Ikuo Nakagawa, Shinji Shimojo	4. 巻 2
2. 論文標題 IoT Agent Platform Mechanism with Transparent Cloud Computing Framework for Improving IoT Security	5. 発行年 2017年
3. 雑誌名 Proc. of COMPSAC 2017	6. 最初と最後の頁 685-689
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/COMPSAC.2017.156	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 -

〔学会発表〕 計6件（うち招待講演 1件/うち国際学会 1件）

1. 発表者名 Ikuo Nakagawa
2. 発表標題 The Connected-Economy in the Digital Age - Technologies & Business Strategies
3. 学会等名 2019-11-1A（招待講演）（国際学会）
4. 発表年 2019年

1. 発表者名 中川郁夫
2. 発表標題 Secure IoT Agent Platform のビジネス応用に関する考察
3. 学会等名 ITRC RICC
4. 発表年 2019年

1. 発表者名 中川郁夫, 下條真司
2. 発表標題 IoTエージェントモデルを応用したセキュアで透過的な情報流通基盤の設計と実装
3. 学会等名 広域センサーネットワークとオーバーレイネットワークに関するワークショップ
4. 発表年 2020年

1. 発表者名 中川郁夫, 下條真司
2. 発表標題 Secure IoT Agent Platform の産業応用に関する考察
3. 学会等名 センサーネットワークとオーバーレイ研究会
4. 発表年 2018年

1. 発表者名 中川郁夫, 下條真司
2. 発表標題 IoTセキュリティの向上を目指す IoT Agent Platformの提案
3. 学会等名 広域センサーネットワークとオーバーレイネットワークに関するワークショップ
4. 発表年 2017年

1. 発表者名 中川郁夫, 下條真司
2. 発表標題 Secure IoT Agent Platform における秘匿分散解析手法の応用
3. 学会等名 ITRC RICC Worksho@
4. 発表年 2017年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

-

6. 研究組織

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
研究 分担 者	下條 真司 (Shimojo Shinji) (00187478)	大阪大学・サイバーメディアセンター・教授 (14401)	

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関
---------	---------