様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 ２４ 日現在

機関番号：８２６７０
研究種目：研究活動スタート支援
研究期間：2020～2021
課題番号：２０Ｋ２３３３６

研究課題名（和文）不正情報流に着目したIoTのセキュリティ向上と省電力化の研究

研究課題名（英文）Energy-efficient Information Flow Control for Secure IoT

研究代表者
中村　繁成（Nakamura, Shigenari）

地方独立行政法人東京都立産業技術研究センター・開発本部情報システム技術部通信技術グループ・研究員

研究者番号：４０８８０４９８

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：IoTでは、デバイス上のある情報資源からデータを取得する資格のないユーザが、他の情報資源を経由してそのデータを取得できてしまう「不正情報流」が生じる問題がある。本研究では、不正情報流を引き起こすアクセス要求をデバイス上で検出し、禁止することで、不正情報流を防止可能な方式を実装した。さらに、本方式におけるアクセス要求処理時間の短縮と通信量の削減に取り組み、省電力化を行った。評価では、本方式を実装して評価し、上記取り組みの実現を示した。

研究成果の学術的意義や社会的意義
IoTでは、センサデータを中心にシステム内で膨大かつ多種多様なデータが交換される。このようなシステムの安全性を保つためには、システム内を流れるデータについての情報流制御が重要となる。本研究では、従来のアクセス制御モデルでは対処しきれない不正情報流の防止と、その制御の省電力化を考えており、新規性と有用性がある。様々な場面、組織で利用されているIoTの安全化を促進し、産業発展に貢献する研究である。

研究成果の概要（英文）：The IoT (Internet of Things) is now one of the most significant infrastructure and has to be secure against malicious accesses. In the CBAC (Capability-Based Access Control) model adopted to the IoT, device owners issue subjects capability tokens, i.e. a set of access rights on objects in devices. Objects are data resource manipulated by subjects. Data are exchanged among subjects and objects through manipulating objects. Here, even if subjects attempt to manipulate objects in accordance with the capability tokens issued, the subjects can get data which the subjects are not authorized to get, i.e. illegal information flow occurs. In this research, we implemented a protocol to prevent illegal information flow from occurring. In addition, we improved the protocol to reduce the electric energy consumption of devices supporting the protocol. In the evaluation, the electric energy consumption in the improved protocol can be reduced compared with the conventional protocol.

研究分野：情報セキュリティ・情報ネットワーク

キーワード：情報流制御　不正情報流　遅延情報流　分散型IoT　資格ベースアクセス制御モデル　実装　資格書選択アルゴリズム　省電力化

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

近年、コンピュータのみならず様々なデバイスが相互接続された「もののインターネット(IoT: Internet of Things)」が、種々の分野で利用されている。IoT は大規模であることから、大量のデバイスを集中管理することが困難となるため、各デバイスが自律的に動作する分散型 IoT を考える必要がある。

アクセスリストを集中的に管理する従来の方式では、ユーザやアプリケーション等のサブジェクトによる不正アクセスの防止が、分散型 IoT の大規模性から困難である。このために本研究では、アクセスリスト方式に代わり、資格ベースアクセス制御(CBAC: Capability Based Access Control)モデルを考える。資格書は、各デバイスの管理者が、デバイス上のどのオブジェクト o にどのような操作 op を行えるかを示したアクセス権$<o, op>$の集合である。操作 op には、データの取得(GET)や保存(PUT)、オブジェクトの生成(POST)や削除(DELETE)がある。サブジェクトはオブジェクトにアクセスする際、当該オブジェクトを有するデバイスへ、資格書を添付したアクセス要求を送信する。デバイスは、アクセス要求が資格書によって許可されているか、資格書が有効かどうかの確認を行い、アクセス要求の許可/拒否を決定する。許可する場合には、アクセス要求に対する応答をサブジェクトに送信する。一方で拒否する場合には、アクセス要求が拒否されたことを示す応答をサブジェクトに送信する。

したがって CBAC モデルでは、資格書を付与されたサブジェクトのみがそのアクセスを許可されるため不正アクセスを防止できるが、不正情報流を防止できない問題がある。これは、あるオブジェクトからデータを取得する資格のないサブジェクトが、他のオブジェクトを経由して当該データを取得できてしまう問題であり、機密情報等の漏洩が生じる可能性がある。加えて、あるサブジェクトがデータを取得するために必要な資格書を有してはいるものの、当該資格書が有効となる時刻以前に生成されたデータについても取得できてしまう遅延情報流が生じる問題がある。

２．研究の目的

近年の情報システムは、コンピュータやセンサ等の多種多様な情報機器がネットワークにより相互接続され、IoT と呼ばれている。IoT における安全性を確保するために、CBAC モデルが提案されており、サブジェクトによる不正アクセスを防止可能である。しかし、サブジェクトとオブジェクト間で情報が流れることによって機密情報等が漏洩してしまう、不正情報流や遅延情報流を防止できない。したがって、本研究では、不正情報流や遅延情報流を防止可能な方式の実装と評価を目的としている。さらに、当該方式の改良による省電力化を行う。

このために、最初に、CBAC モデルに基づいて、不正情報流と遅延情報流を論理的に定義する。本定義に基づいて、不正情報流や遅延情報流を引き起こすアクセス要求をデバイス上で検出し、そのようなアクセス要求を禁止することで不正情報流や遅延情報流を防止可能な方式を設計する。当該方式を IoT デバイス上で実装し、性能評価を行う。得られた結果を踏まえて、当該方式の改良に取り組み、省電力化を行う。改良方式についても IoT デバイス上で実装し、性能評価を行う。さらに、シミュレーションによる性能評価も行う。

３．研究の方法

(1) 不正情報流を防止可能な方式の実装

最初に、CBAC モデルに基づいて、不正情報流を論理的に定義する。本定義に基づいて、不正情報流を引き起こすアクセス要求をデバイス上で検出し、そのようなアクセス要求を禁止することで不正情報流を防止可能な方式を設計する。このために、各サブジェクトによって発行されるアクセス要求、アクセス要求に付与される資格書、アクセス要求の認証処理等の設計を行う。当該方式を IoT デバイスとして広く用いられている Raspberry Pi 上で実装し、サブジェクトからのアクセス要求を処理させる。アクセス要求に添付されている資格書に基づいて、「アクセス要求は許可されているものか」、「資格書は有効か」、「不正情報流は生じていないか」といった確認により構成される認証処理に要する時間を実測し、その特徴を明らかにする。

(2) 不正情報流と遅延情報流を防止可能な方式の実装

(1)で実装する方式では不正情報流を防止可能だが、遅延情報流を防止できない課題がある。そこで CBAC モデルに基づいて、遅延情報流についても論理的に定義する。本定義に基づいて、遅延情報流を引き起こすアクセス要求についてもデバイス上で検出して禁止し、両情報流を防止可能な方式を設計する。このために、遅延情報流防止を考慮した、アクセス要求、資格書、アクセス要求の認証処理等を新たに設計する。当該方式を IoT デバイス上で実装し、サブジェクトからのアクセス要求を処理させる。デバイスがアクセス要求を受信してから応答を送信するまでのアクセス要求処理時間を実測し、その特徴を明らかにする。加えて、情報流制御を行わない方式、(1)で実装する不正情報流のみを防止可能な方式と比較評価を行う。

(3) アクセス要求処理時間短縮アルゴリズムの実装
(1)・(2)で明らかにする、実装方式におけるアクセス要求処理時間の特徴から、アクセス要求処理時間に大きく影響する要因を明らかにする。本要因を踏まえて、アクセス要求処理時間を短縮可能なアルゴリズムを設計する。本アルゴリズムを(1)・(2)で実装する方式に適用した新たな方式を IoT デバイス上で実装し、サブジェクトからのアクセス要求を処理させる。アクセス要求処理時間を実測し、情報流制御を行わない方式・(1)・(2)で実装する方式と比較評価を行う。

(4) 通信量削減アルゴリズムの実装
(1)・(2)・(3)での実装方式における動作内容から、情報流制御に伴う通信量に大きく影響する要因を明らかにする。本要因を踏まえて、通信量を削減可能なアルゴリズムを設計する。本アルゴリズムを(1)・(2)で実装する方式に適用した新たな方式を IoT デバイス上で実装し、サブジェクトからのアクセス要求を処理させる。通信量を実測し、情報流制御を行わない方式、(1)・(2)・(3)で実装する方式と比較評価を行う。

(5) デバイスの消費電力の観点での評価
(1)・(2)・(3)・(4)で考えてきた IoT デバイスにおける消費電力を実測し、不正情報流と遅延情報流の防止処理を伴う IoT デバイスの電力消費モデルを構築する。本モデルに基づいて、システム全体の消費電力を算出可能なシミュレータを開発する。(1)・(2)・(3)・(4)で実装する方式間で比較評価を行い、(3)・(4)での実装アルゴリズムにおける、省電力化への寄与を明らかにする。

４．研究成果
(1) 不正情報流を防止可能な方式の実装
最初に、CBAC モデルに基づいて不正情報流を論理的に定義した。本定義に基づいて、不正情報流を引き起こすアクセス要求をデバイス上で検出し、そのようなアクセス要求を禁止することで、不正情報流を防止する OI (Operation Interruption)方式を設計した。OI 方式を IoT デバイス上で実装し、サブジェクトからのアクセス要求を処理させ、認証処理に要する時間を実測した。認証に用いられる各資格書の正真性の確認に要する時間が、認証処理時間の大半を占めることを明らかにした。このため、認証処理に用いられる資格書数が増加するほど、認証処理時間が増加することが明らかとなった。

(2) 不正情報流と遅延情報流を防止可能な方式の実装
最初に、CBAC モデルに基づいて遅延情報流を論理的に定義した。本定義に基づいて、不正情報流を引き起こすアクセス要求のみならず、遅延情報流を引き起こすアクセス要求についてもデバイス上で検出し、そのようなアクセス要求を禁止することで、両情報流を防止する TBOI (Time-Based OI)方式を設計した。TBOI 方式を IoT デバイス上で実装し、サブジェクトからのアクセス要求を処理させ、アクセス要求処理時間を実測した。OI 方式と同程度の時間で、両情報流を防止できることを示した。なお、OI 方式と同様に、認証に用いられる各資格書の正真性の確認に要する時間が、認証処理時間の大半を占めることを明らかにした。このため、認証処理に用いられる資格書数が増加するほど、認証処理時間が増加することが明らかとなった。

(3) アクセス要求処理時間短縮アルゴリズムの実装
(1)・(2)より、OI・TBOI 方式では、認証処理に用いられる資格書数が増加するほど、認証処理時間が増加することが明らかとなった。これを踏まえて、認証処理に最低限必要な資格書をデバイス上で選択する MRCTSD (Minimum Required Capability Token Selection for Devices)アルゴリズムを提案した。MRCTSD アルゴリズムによって、正真性を確認する必要のある資格書数を削減でき、認証処理時間を短縮可能となる。評価では、OI・TBOI 方式に MRCTSD アルゴリズムを適用した OI-MRCTSD・TBOI-MRCTSD 方式を IoT デバイス上で実装し、サブジェクトからのアクセス要求を処理させ、アクセス要求処理時間を実測した。評価結果を図 1 に示している。ラベル CBAC は、CBAC モデルのみを実装し、情報流制御を行わない方式を意味している。ラベル et_A は資格書選択に要する時

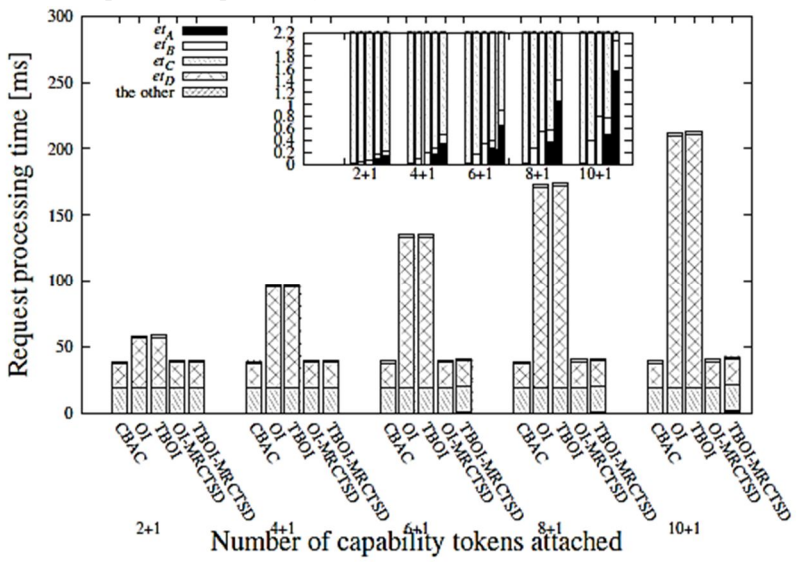

図 1　アクセス要求処理時間

間、et_Bは不正アクセス・不正情報流・遅延情報流の検出に要する時間、et_Cはサブジェクトの正真性の確認に要する時間、et_Dは各資格書の正真性の確認に要する時間を、それぞれ示している。認証処理時間は以上の 4 つの時間から構成される。ラベル the other は、アクセス要求処理時間の内、認証処理時間を除いた時間を示している。横軸は、アクセス要求に添付された資格書数である。値「n+1」は、n 個の資格書と、n 個の資格書を代替可能な 1 つの資格書が添付されていることを意味する。OI・TBOI 方式では n 個の資格書が用いられたが、OI-MRCTSD・TBOI-MRCTSD 方式では 1 つの資格書が選択されて用いられた。したがって、OI-MRCTSD・TBOI-MRCTSD 方式では、OI・TBOI 方式に比べて、アクセス要求処理時間を短縮できることを示した。

(4) 通信量削減アルゴリズムの実装

認証処理において、必要となることが予想される最低限の資格書を、サブジェクト上で選択する MRCTSS (MRCTS for Subjects)アルゴリズムを提案した。MRCTSS アルゴリズムによって、アクセス要求に添付される資格書数を削減でき、サブジェクトとデバイス間での通信量を削減可能となる。評価では、OI・TBOI 方式に MRCTSS アルゴリズムを適用した OI-MRCTSS・TBOI-MRCTSS 方式を IoT デバイス上で実装し、サブジェクトからのアクセス要求を処理させ、1 アクセス要求あたりの UDP データグラムの大きさを実測した。評価結果を図 2 に示している。ラベル OI(-MRCTSD)は、OI・OI-MRCTSD 方式を意味している。TBOI(-MRCTSD)についても同様である。横軸は、サブジェクトに付与された資格書数である。値「n+1」は、n 個の資格書と、n 個の資格書を代替可能な 1 つの資格書が付与されていることを意味する。OI(-MRCTSD)・TBOI(-MRCTSD)方式では n 個の資格書が選択されてアクセス要求に添付されたが、OI-MRCTSS・TBOI-MRCTSS 方式では 1 つの資格書が選択され、添付された。したがって、OI-MRCTSS・TBOI-MRCTSS 方式では、OI(-MRCTSD)・TBOI(-MRCTSD)方式に比べて、1 アクセス要求あたりの UDP データグラムの大きさを縮小でき、通信量を削減できることを示した。

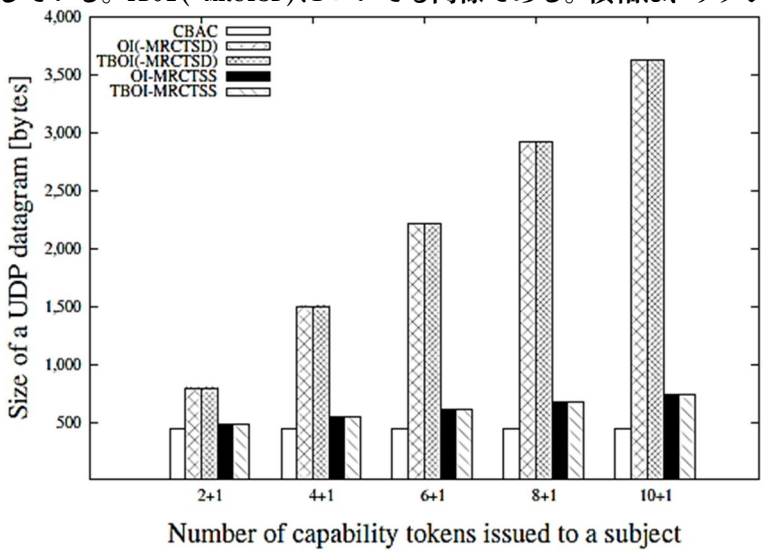

図 2　1 アクセス要求あたりの UDP データグラムの大きさ

(5) デバイスの消費電力の観点での評価

(1)・(2)・(3)・(4)で実装した各方式では、アクセス要求を受信した IoT デバイス上で認証処理を行う。当該処理は、IoT デバイスの計算資源を利用する計算プロセスとしてモデル化できる。そこで最初に、IoT デバイス上で計算プロセスを実行させたときの消費電力を実測した。測定結果を踏まえて、計算プロセス実行時における IoT デバイスの電力消費モデルを構築した。本モデルに基づいて、(1)・(2)・(3)・(4)で実装してきた各方式を動作させたときの、IoT デバイス全体の消費電力を算出可能なシミュレータを開発し、評価した。本評価では、サブジェクト数を 20、各サブジェクトに付与される資格書数を 5～10、デバイス数を 15、各デバイス上のオブジェクト数を 1～5 とし、評価結果を図 3 に示している。消費電力が最も少ない TBOI-MRCTSD 方式と、他の方式との消費電力の差を示している。(3)・(4)で実装したアルゴリズムにより、OI・TBOI 方式の省電力化を行えることを示した。

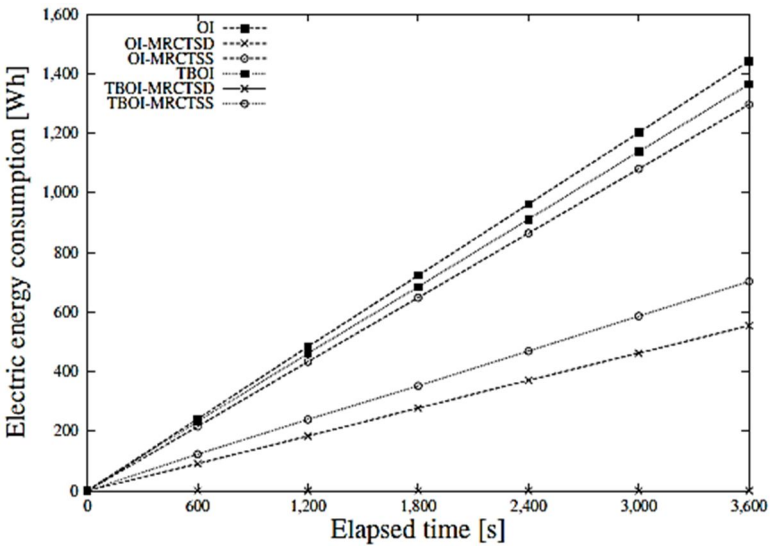

図 3　IoT デバイス全体の消費電力

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Nakamura Shigenari、Enokido Tomoya、Takizawa Makoto	４．巻 －
２．論文標題 Implementation and evaluation of the information flow control for the Internet of Things	５．発行年 2021年
３．雑誌名 Concurrency and Computation: Practice and Experience	６．最初と最後の頁 －
掲載論文のDOI（デジタルオブジェクト識別子） 10.1002/cpe.6311	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Nakamura Shigenari、Enokido Tomoya、Takizawa Makoto	４．巻 15
２．論文標題 Information Flow Control Based on Capability Token Validity for Secure IoT: Implementation and Evaluation	５．発行年 2021年
３．雑誌名 Internet of Things	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.iot.2021.100423	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Nakamura Shigenari、Enokido Tomoya、Takizawa Makoto	４．巻 19
２．論文標題 Capability Token Selection Algorithms to Implement Lightweight Protocols	５．発行年 2022年
３．雑誌名 Internet of Things	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.iot.2022.100542	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計6件（うち招待講演　0件／うち国際学会　6件）

１．発表者名 Nakamura Shigenari、Enokido Tomoya、Lidia Ogiela, Takizawa Makoto
２．発表標題 Implementation of a Device Adopting the OI (Operation Interruption) Protocol to Prevent Illegal Information Flow in the IoT
３．学会等名 The 9th International Conference on Emerging Internet, Data & Web Technologies (EIDWT-2021) (国際学会)
４．発表年 2021年

１．発表者名
Nakamura Shigenari、Enokido Tomoya、Takizawa Makoto

２．発表標題
Design and Implementation of the TBOI (Time-Based Operation Interruption) Protocol to Prevent Late Information Flow in the IoT

３．学会等名
The 35th International Conference on Advanced Information Networking and Applications (AINA-2021)（国際学会）

４．発表年
2021年

１．発表者名
Nakamura Shigenari、Enokido Tomoya、Takizawa Makoto

２．発表標題
A Capability Token Selection Algorithm for Lightweight Information Flow Control in the IoT

３．学会等名
The 24th International Conference on Network-Based Information Systems (NBiS-2021)（国際学会）

４．発表年
2021年

１．発表者名
Nakamura Shigenari、Enokido Tomoya、Takizawa Makoto

２．発表標題
Traffic Reduction for Information Flow Control in the IoT

３．学会等名
The 16th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2021)（国際学会）

４．発表年
2021年

１．発表者名
Nakamura Shigenari、Enokido Tomoya、Takizawa Makoto

２．発表標題
Energy Consumption Model of a Device Supporting Information Flow Control in the IoT

３．学会等名
The 10th International Conference on Emerging Internet, Data & Web Technologies (EIDWT-2022)（国際学会）

４．発表年
2022年

１．発表者名 Nakamura Shigenari、Enokido Tomoya、Takizawa Makoto
２．発表標題 Energy Consumption of the Information Flow Control in the IoT: Simulation Evaluation
３．学会等名 The 36th International Conference on Advanced Information Networking and Applications (AINA-2022)（国際学会）
４．発表年 2022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

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