２０２０年　３月　２３日

2019 年度若手研究者共同研究プロジェクト実施報告書

法政大学総長　殿

以下のとおり研究実施報告書を提出します。

基本情報	研究課題名：大規模分散システムにおける不正情報流防止方式の研究
	研究代表者　氏名：　中村　繁成
	（在籍者）研究科・専攻・学年：理工学研究科・システム理工学専攻・博士後期課程３年 （修了者）所属・職種：
	指導教員（所属・職・氏名）：　滝沢　誠 （※在籍者のみ記入）
	共同研究者（所属・職・氏名）： （※指導教員と同人の場合は記入不要）
	その他　研究分担者：
	研究期間：　２０１８年度　～　２０１９年度（※研究修了年度を記載）
年間の研究実施概要	※研究計画の進捗状況を中心に今年度の研究実施状況を記載してください。 近年、情報システムのモデルとして IoT が種々の分野で広く利用されてきている。IoT は、コンピュータに加えてセンサ等の情報通信機能を有したデバイスが相互接続された大規模なものとなっていることから、これらのデバイスを集中管理することは困難となっている。このため、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。分散型 IoT は種々のデバイスによって構成される。各デバイスはデータをどのように扱うかという観点から、次の 3 種に大別される。1)周辺環境のデータを取得するセンサ、2)センサデータの内容に基づいて動作するアクチュエータ、3)センサとアクチュエータの両方の機能を持つハイブリッドデバイス(自動車やロボット等)である。 分散型 IoT では、ユーザや応用等のサブジェクトによる不正アクセスを防止するために、従来からのアクセスリスト方式では、アクセスリストを集中的に管理することが困難である。このために本研究では、CBAC(資格(capability)ベースアクセス制御)モデルを考える。これは、各デバイスの管理者が、デバイスに対してどのような操作を行えるかの権限を示した資格書をサブジェクトに発行し、資格書を付与されたサブジェクトのみがその資格書に示された操作を行うことを許可されるものである。ここで次のようなケースを考える。サブジェクト *sb*1 はセンサ *s* からのデータ取得(get)とハイブリッドデバイス *h* にデータ保存(put)を行える権限、サブジェクト *sb*2 はハイブリッドデバイス *h* からデータの get を行える権限を付与されている。最初に、*sb*1 が *s* からデータを get する。次に、*sb*1 が *s* から get したデータに基づいて *h* を動作させるために、データを *h* に put し、*h* がそのデータを保持する。ここで、*s* のデータが *h* に流れることになる。最後に、*sb*2 が *h* からデータを get する。このとき、*sb*2 は *s* からデータを get する権限を付与されていないにもかかわらず、*h* に流れてきた *s* のデータを get できてしまう。分散型 IoT では、このような不正情報流が生じる問題がある。CBAC モデルでは、各サブジェクトによるデバイスへの不正アクセスを防止できるが、不正

年間の研究実施概要

情報流は防止できず、機密情報等の漏洩が生じる可能性があり、不正情報流の防止は重要な研究課題となっている。

本年度では最初に、CBAC モデルに基づいて不正情報流を論理的に明らかにしている。このために、各サブジェクト sb と各デバイス d に、流れてきたデータの生成元デバイスの集合($sb.D$ 及び $d.D$)を保持させる。さらに、sb がデータを get する権限を付与されているデバイスの集合 $IN(sb)$ を考える。sb が d への get を試みたとき「$d.D \subseteq IN(sb)$」が成立するならば、不正情報流が生じると定義する。d は sb の資格書を用いて不正情報流を検出し、sb の get 操作を禁止することで、不正情報流を防止できる OI(Operation Interruption)方式を以下の論文で新たに考案している。

- S. Nakamura, T. Enokido, M. Takizawa: Capability-Based Information Flow Control Model in the IoT , *Proc. of the 13th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (*IMIS-2019*), 口頭, Sydney, Australia, pp.63-71, July 2019.

以下の論文では、禁止される get 操作数の観点で OI 方式をシミュレーションにより評価している。システム内のサブジェクト数が増加しても、全 get 操作数に対する不正 get 操作数の割合は一定に保たれることを示し、OI 方式の有用性を明らかにしている。

- S. Nakamura, T. Enokido, M. Takizawa: Evaluation of an OI (Operation Interruption) Protocol to Prevent Illegal Information Flow in the IoT, *Proc. of the 22nd International Conference on Network-Based Information Systems* (*NBiS-2019*), 口頭, Oita, Japan, pp.15-26, Sept. 2019.

以下の論文では、システム内のサブジェクト数、デバイス数、発行される操作数等がより多い状況で、OI 方式を評価している。大規模なシステム内においても、OI 方式が有用であることを示している。

- S. Nakamura, T. Enokido, M. Takizawa: Information Flow Control Based on the CapBAC (Capability-Based Access Control) Model in the IoT, *International Journal of Mobile Computing and Multimedia Communications* (*IJMCMC*), Vol.10, No.4, pp.13-25, 2019.

CBAC モデルにおいて各サブジェクトに付与されるアクセス権には、有効期間が存在する。OI 方式では、システム全体で不正情報流を防止可能だが、あるサブジェクトが時刻 t にあるデータを get することを許可されていないにもかかわらず、時刻 t に生成された当該データを取得できてしまう問題を防止できない。当該データは時刻 t の後にサブジェクトによる get によって、当該サブジェクトへと流れてくる。このとき、サブジェクトには、現在有効なアクセス権の有効期間内に生成されたデータであれば get を許可されたが、それ以前の時刻 t に生成されたデータが流れてきたことになる。つまり、サブジェクトからすれば、get することを期待した期間に対して、データが遅れて流れてきたということになる。したがって、本研究では、このような遅延情報流(late information flow)を新たに定義している。不正情報流に加え、遅延情報流を起こす操作を禁止することで、双方を防止可能な TBOI(Time-Based Operation Interruption)方式を以下の論文で新たに考案している。

- S. Nakamura, T. Enokido, M. Takizawa: A TBOI (Time-Based Operation Interruption) Protocol to Prevent Late Information Flow in the IoT, *Proc. of the 14th International Conference on Broad-Band Wireless Computing, Communication and Applications* (*BWCCA-2019*), 口頭, Antwerp, Belgium, pp.13-25, Nov. 2019.

以下の論文では、禁止される get 操作数の観点で TBOI 方式をシミュレーションにより評価している。TBOI 方式では不正情報流に加えて遅延情報流についても防止しているため、OI 方式よりも多くの get 操作が禁止されることを示している。

- S. Nakamura, T. Enokido, M. Takizawa: Evaluation of a TBOI (Time-Based Operation Interruption) Protocol to Prevent Late Information Flow in the IoT, *Prof. of the 8th International Conference on Emerging Internet, Data & Web Technologies* (*EIDWT-2020*), 口頭, Kitakyushu, Japan, pp.12-23, Feb. 2020.

以上の内容を論文としてまとめ、国際会議 IMIS(Sydney, Australia)、NBiS(大分)、BWCCA(Antwerp, Belgium)等で 4 件の筆頭著者論文の発表を行った。また、筆頭著者の国際学術論文誌論文が 3 件採録されている。

研究業績

成果発表（学会・論文・研究会等）

学会・論文・研究会等の別	タイトル	発行または発表年月
Service Oriented Computing and Applications (SOCA)	Protocol to Efficiently Prevent Illegal Flow of Objects in P2P Type of Publish/Subscribe (PS) Systems	2019年9月 筆頭，査読有
International Journal of Communication Networks and Distributed Systems (IJCNDS)	A Topic-Based Synchronisation Protocol in Peer-to-Peer Publish/Subscribe Systems	2019年10月 筆頭，査読有
International Journal of Mobile Computing and Multimedia Communications (IJMCMC)	Information Flow Control Based on the CapBAC (Capability-Based Access Control) Model in the IoT	2019年12月 筆頭，査読有
Proc. of the 13th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp.63-71	Capability-Based Information Flow Control Model in the IoT	2019年7月 筆頭，査読有，口頭
Proc. of the 8th International Conference on Emerging Internet, Data & Web Technologies, pp.12-23	Evaluation of a TBOI (Time-Based Operation Interruption) Protocol to Prevent Late Information Flow in the IoT	2020年2月 筆頭，査読有，口頭