L-005

IoT における制約，コンテキスト，及びリスクを意識した 適応的なアクセス制御方式の構想の提案

Proposal on Concept of Adaptive Access Control in IoT(Internet of Things) with being Aware of Constraints, Contexts, and Risks thereof

桑田 雅彦†
Masahiko Kuwata†

概要：IoT が急速に進展，普及するのに伴い社会のあらゆる面で IoT の影響力が増す中，IoT デバイスのセキュリティ対策は疎かになっており，サイバー空間のセキュリティ脅威に対して IoT のセキュリティ確保は重大な課題である．本論文は，IoT に求められるセキュリティのうちアクセス制御に焦点を当て，従来の ICT のアクセス制御を IoT に適用しようとしたときに，IoT の制約や新たな要件により生じる課題があることを指摘する．また，課題を解決するためのアプローチ案を提示し，関連する先行研究を紹介し残課題を挙げる．その残課題を解決するために，「IoT における制約，コンテキスト，及びリスクを意識した適応的なアクセス制御」を，Capability ベースの分散アクセス制御に組み合わせた，IoT におけるアクセス制御の管理及び実行のための方式の構想を提案する．最後に今後の研究の方向性と予定を示す．

Abstract: While IoT is evolving and spreading rapidly, and is increasing its influence on various aspects of our society, security measures on IoT devices are far from sufficient. So, it is very important to enhance IoT security against security threats of cyber space. This paper focuses on access control among security measures required to IoT, and points out the challenges to be tackled, which are caused by constraints and new requirements involving IoT, when the existing security measures in ICT are to be applied to IoT. Additionally, this paper presents the author's ideas about how to approach to those challenges, and introduces some prior researches and remaining tasks. To solve those tasks, this paper presents the author's proposal on concept of how to manage and execute access controls in IoT, which combine "adaptive access controls with being aware of constrains, contexts, and risks in IoT" with distributed capability-based access controls. Finally, future tasks of the author's research are shown.

キーワード：IoT, セキュリティ, アクセス制御, 分散, Capability ベース, コンテキスト意識, 適応的
Keywords: IoT, Security, Access Control, Distributed, Capability-based, Context-aware, Adaptive

1. はじめに

IoT が急速に進展，普及するのに伴い，社会のあらゆる面で IoT の影響力が増す中，IoT デバイスのセキュリティ対策は疎かになっており，サイバー空間のセキュリティ脅威に対して IoT のセキュリティ確保は重大な課題である．

本論文は，IoT に求められるセキュリティのうちアクセス制御に焦点を当て，従来の ICT のセキュリティ対策を IoT に適用しようとしたときに，IoT の制約や新たな要件により生じる課題があることを指摘する．また，課題を解決するためのアプローチ案を提示し，関連する先行研究を紹介し，残課題を挙げる．そして残課題を解決するために，「IoT における制約，コンテキスト，及びリスクを意識した適応的なアクセス制御」を，Capability ベースの分散アクセス制御に組み合わせた，IoT におけるアクセス制御の管理及び実行のための方式を提案する．最後に，今後の研究の方向性を示す．

構成は，まず前段として背景を説明するために， 2 章で「IoT に求められるセキュリティ」を紹介し，3 章で「IoT のセキュリティ実現に向けての課題」を指摘する．次に，4 章で「IoT におけるアクセス制御の課題に対するアプローチ案」を提示し，5 章で「IoT におけるアクセス制御に関する先行研究と残課題」を紹介する．そして，6 章で「IoT における制約，コンテキスト，及びリスクを意識した適応的なアクセス制御の構想提案」を説明する．最後に 7 章で「今後の研究の方向性」を示す．

†情報セキュリティ大学院大学,
Institute of Information Security

2. IoT に求められるセキュリティ

2.1 IoT におけるセーフティ，安定稼働，レジリエンス，プライバシの重要性

IoT に求められるセキュリティを考えるとき，物理的なモノの世界では，セキュリティにかかわる別の軸の重要な価値が存在し，それらの方がより優先される価値であることを意識する必要がある．それは，セーフティ，安定稼働，レジリエンス（耐性），プライバシである．

モノは，故障や誤作動により，人に物理的に危害を及ぼしうるため，セーフティ（安全性）が第一に重視される．

工場，自動車，装置，システム等を制御するデバイスの場合，通常の稼働状態が安定し継続することが期待されており，稼働が急に停止したり制御が不安定になったりすると，セーフティ（安全性）や品質確保の問題が生じる．そのため安定稼働やレジリエンス（耐性）が重視される．

監視カメラ，ウェアラブルデバイス，医療機器等，身の周りのモノの場合，個人のプライバシにかかわる情報を扱っており，従来の ICT において扱っていたプライバシ情報より機微な情報も多くなるため，プライバシ保護に対するこれまで以上の配慮が必要になる．

2.2 IoT におけるアクセス制御の重要性

IoT に求められるセキュリティ機能[1]は，IoT デバイスそれぞれで保護すべき対象，脅威，脆弱性，侵害されたときの影響度等が異なり，それに応じて適用すべきセキュリティ機能は異なるが，前述のとおり IoT におけるセーフティやプライバシが重視されることを考えると，IoT デバイスの制御やプライバシ情報へのアクセスを正しく実行させるためのアクセス制御の位置付けはとても重要なものになる．

2.3 想定ユースケースにおけるアクセス制御の場面及び脅威の具体例

本論文では想定するユースケースの一例として，モビリティ(具体例として自動車)の自動運転走行の場合を挙げて説明する．

情報処理推進機構(IPA)「自動車の情報セキュリティへの取組みガイド」[2]に示されているとおり，自動車の車載システムを構成する機能としては，以下に挙げるものがある．

機能	説明
A. 駆動系	「走る」に関する制御機能
B. シャーシ系	「止まる・曲がる」に関する制御機能
C. ボディ系	車体に関する制御機能
D. 安全快適機能	自動車を制御する機能との連携により，自動的に安全性や快適な運転を実現する機能
E. 診断・保守	故障診断・保守等の機能
F. ITS 機能	路側機や車車間通信により実現される機能
G. テレマティクス	通信機能による位置情報収集や遠隔サービス機能
H. インフォテイメント	搭乗者に対する娯楽や情報提供を行う機能

表 1 自動車の車載システムを構成する機能
（※文献[2] 表 2-2 「IPA カーの機能」をもとに作成）

そして，制御やプライバシ情報にかかわるこれらの機能と外界が，車載 LAN を介して繋がり様々な情報通信処理を行う．

ここで想定される不正アクセスの脅威としては，以下に挙げるようなものが考えられる．

- ■ 周囲の状況(移動体，道路，信号等)に関する情報収集に対する不正アクセスの脅威 [機能 F にかかわる]
  - ● 情報を不正に書き換え（挿入，消去を含む）
  - ● 情報の送受信を妨害(送信元/先の書き換え，経路への介在，DoS 攻撃等)
- ■ 自動運転走行(経路，方向，速度等)の制御に対する不正アクセスの脅威 [機能 A, B, C, D にかかわる]
  - ● 制御コマンドを不正に書き換え(挿入, 消去を含む)
  - ● 制御コマンドの送受信を妨害
- ■ 位置情報，搭載カメラ動画データ等に対する不正アクセスの脅威 [機能 G にかかわる]
  - ● データを不正に読み取り
  - ● データを不正に書き換え(挿入，消去を含む)
  - ● データの送受信を妨害
- ■ システムに対する不正アクセスの脅威 [機能 E, F にかかわる]
  - ● 実在しないモビリティの接続，及びデータの挿入

自動車の自動運転走行においては，これらの不正アクセスへの対策としてアクセス制御が必要であり重要になる．

3. IoT のセキュリティ実現に向けての課題

3.1 IoT と従来 ICT の違い(IoT にかかわる制約，新たな要件)

IoT の制約や新たな要件として，以下の点が存在する．

- ● リソース(CPU，メモリ，ディスク等)の制約
- ● 消費電力の制約
- ● コストの制約
- ● リアルタイム性の重要性
- ● データ処理方式の違い(ストリーム処理)
- ● 新たなネットワーク接続方式(M2M エリア NW)
- ● ネットワーク接続の非定常性，不安定性
- ● ノード数の規模大
- ● ダイナミック性(構成，接続，位置等の変化)の頻度大
- ● 利用／維持管理の長期化
- ● 設置場所(ICT 要員不在，目の行き届かない現場)
- ● 新たな主体(所有者，利用者，モノ)
- ● 新たな関係(モノーモノ，所有者ー利用者)
- ● セキュリティ関連の重視する価値
  (セーフティ，安定稼働，レジリエンス，プライバシ)
- ● 従来よりも重視される価値(自動，自律)

3.2 従来 ICT におけるセキュリティ対策(特にアクセス制御関連)の IoT 適用に当たっての課題

従来の ICT におけるセキュリティ対策を IoT に適用しようとすると，IoT の制約や新たな要件のために，課題が生じる．

例えば，IoT デバイスにはリソースの制約があるため，ICT の端末等に適用してきたセキュリティ対策製品は適用できないし，公開鍵暗号アルゴリズムは実用的ではない．

ICT におけるアクセス制御方式(RBAC: Role-Based Access Control, ABAC: Attribute-Based Access Control)は，TCP/IP ベースの通信プロトコル，利用者認証処理のためのプロトコル，認可処理のための利用者のロールや属性をやり取りするプロトコル，認可処理のための利用者のロールや属性とアクセス権限との対応付け，といった一連の処理によるオーバヘッドが大きく，軽量性やリアルタイム性を求められる IoT デバイスには向いていない（図 1）．

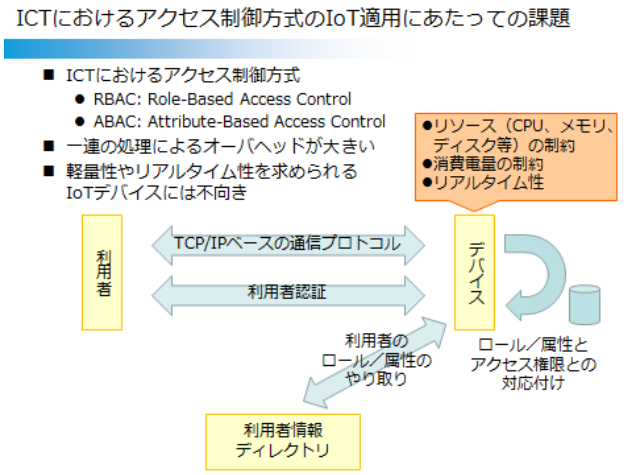

図 1 ICT におけるアクセス制御方式の IoT 適用に当たっての課題例①

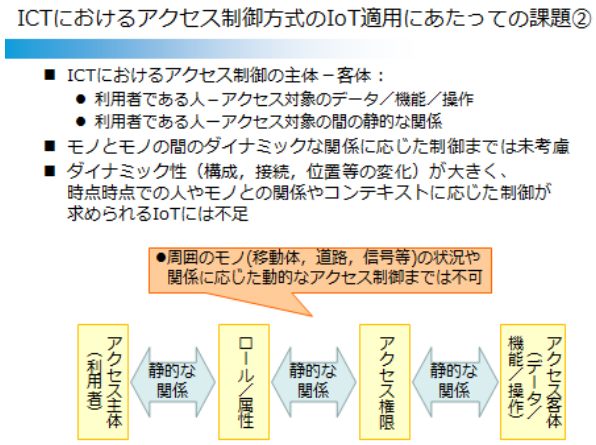

図 2 ICT におけるアクセス制御方式の IoT 適用に当たっての課題例②

IoT デバイスは，ネットワーク接続が定常的ではなく安定していないため，クラウド上で集中化されている認証サーバや利用者情報ディレクトリサーバへアクセスできることを前提にした認証・認可方式は向いていない．

クラウド上に集中化せずに，デバイス上に利用者の認証情報やロール／属性情報を格納し処理しようとすると，IoT デバイスのリソース制約に引っかかる．

ICT におけるアクセス制御の主体－客体は，利用者である人－アクセス対象のデータ／機能／操作であり，それらの間の関係は静的である．一方，IoT におけるアクセス制御の主体は，所有者，利用者，システム，モノといった従来にはない要素が増え，所有者－利用者の動的な関係や，モノとモノの動的な関係をアクセス制御のパラメータとして考慮に入れなければならなくなる．

IoT システムは，ダイナミック性（構成，接続，位置等の変化）が大きく，時点時点での人やモノとの関係やコンテキストに応じた制御が求められる場合がある．例えば，自動車の自動運転走行のユースケース例の場合，周囲の状況(移動体，道路，信号等)に応じて，自動運転走行(経路，方向，速度等)の制御の調整範囲を限定する必要がある．

また，サイバー攻撃による異常な制御を防ぐために，周辺の IoT デバイスの制御状態から逸脱しない範囲や，一つの IoT デバイス上における制御の連続性から逸脱しない範囲に，制御を限定する必要があるかもしれない．

しかし，従来の ICT におけるアクセス制御方式では，リスクベース認証等のコンテキストに応じた制御まで考慮されたものも一部あるが，モノとモノの間のダイナミックな関係に応じた制御までは考慮されていない(図 2).

他にも，たとえセキュリティが侵害されたとしても，セーフティ，安定稼働，レジリエンスの確保は優先して守らなければならない．

4. IoT におけるアクセス制御の課題に対するアプローチ案

本章では，前述の課題に対するアプローチ案を提示する．

まず，アクセス制御の管理と実行とでは，適するアプローチが異なると筆者は考える．

また，IoT システムは，新たな主体（所有者，利用者，モノ）や関係（モノ－モノ，所有者－利用者）が存在し，ダイナミック性（構成，接続，位置等の変化）が大きく，従来の ICT においては考慮されていない，時点時点での人やモノとの関係に応じた制御の仕組みが新たに必要である．

以下の 3 つの軸で筆者の考えを整理する．（図 3）

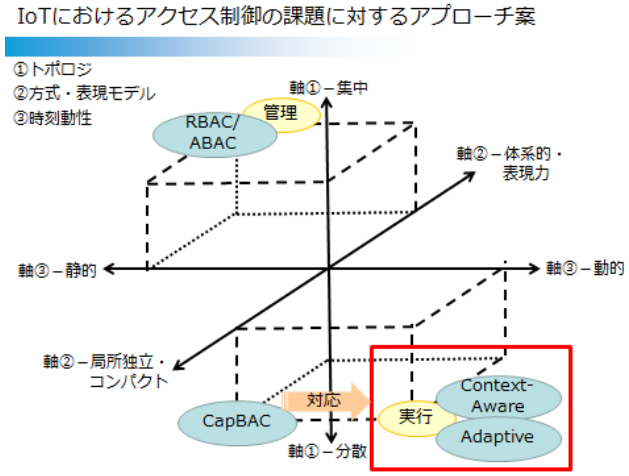

図 3 IoT におけるアクセス制御の課題に対するアプローチ案(3 軸で整理)

4.1 トポロジ：集中と分散

システム全体のアクセス制御の管理は，分散化すると全体としての整合の確保や全体状況を見通すことが難しくなり，管理コストも増えてしまうため，中央のクラウド上に集中化する方が良いと考える．

一方，アクセス制御の実行（ポリシ決定を含む）は，IoT デバイスの NW 接続の非定常性，不安定性という課題に対処するため，あるいは，IoT デバイスが求めるリアルタイム性という要件に対応するため，ローカルの IoT デバイス上に分散化する方が良いと考える．

ただし，IoT デバイスのリソース制約という課題があるため，IoT デバイス上に格納する認可ポリシ情報は，可能な限りコンパクトな表現にする必要がある．

4.2 方式・表現モデル：RBAC/ABAC と CapBAC

システム全体のアクセス制御の管理は，アクセス主体の属するカテゴリを含めて，全体を体系的に整理でき，管理しやすい表現力が求められるため，RBAC/ABAC のポリシ表現が適していると考える．

一方，アクセス制御の実行（ポリシ決定を含む）は，前述の課題として述べたとおり，RBAC, ABAC を用いると一連の処理によるオーバヘッドが大きく，リアルタイム性を求められるデバイスには RBAC, ABAC は向いていない．そのため，デバイス上で独立にアクセス権限の有無のみを判定することにより，オーバヘッドを最小化できる CapBAC (Capability-Based Access Control)が適していると考える．

ただし，アクセス主体に付与されているアクセス権限(capability)をコンパクトに表現できることが求められる．

4.3 時刻動性：関係及びリスクを含むコンテキストの意識，適応的(Adaptive)

IoT システムの特性である，時々刻々のダイナミック性（構成，接続，位置等の変化）に対応するためには，RBAC/ABAC のように，アクセス主体の属する静的なカテゴリに応じたアクセス制御に加えて，時点時点における人やモノとの関係や，リスクを含む，コンテキストを意識した適応的なアクセス制御を可能にする（Capability の範囲を制限するような）仕組みが新たに必要である．

4.4 想定するユースケース例でのアクセス制御対象の本アプローチ案における位置付け

2.3 節で挙げたユースケース例(自動車の自動運転走行)においてアクセス制御対象となる制御やプライバシにかかわる機能・情報に対するアクセス制御(実行)が，本アプローチにおいてどの位置付けに当たるかを整理する．

「A. 駆動系」，「B. シャーシ系」，「C. ボディ系」，「D. 安全快適機能」，「F. ITS 機能」，「G. テレマティクス」は，リアルタイム性やダイナミック性が求められるため，アクセス制御の実行を分散化し，CapBAC を用い，コンテキストを意識した適応的なアクセス制御が適している．

「E. 診断・保守」と「H. インフォテイメント」は，NW 接続の課題への対処やリアルタイム性という要件は求められないと考えられるため，従来の ICT 同様に，アクセス制御の実行は集中型で RBAC/ABAC を用いたアクセス制御でも問題はないと考えられる．

それぞれの位置付けを本アプローチ案の図上に示す(図 4).

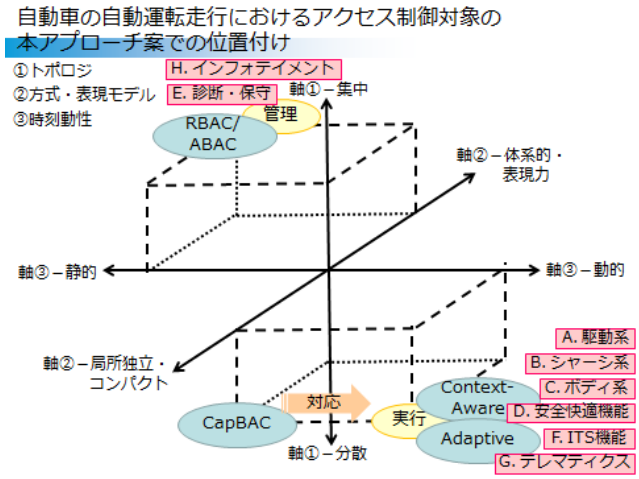

図 4 自動車の自動運転走行におけるアクセス制御対象の本アプローチ案での位置付け

5. IoT におけるアクセス制御に関する先行研究と残課題

5.1 Capability ベースの分散アクセス制御方式に関する先行研究

IoT におけるアクセス制御の課題への提案に関する最近の論文の中で，引用数の多いものとして， Hernández-Ramos, J. L.らの“Distributed Capability-based Access Control for the Internet of Things”(Nov, 2013)[3]がある．

本研究は，欧州 FP7 IoT@Work プロジェクトの中で検討されたものであり，capability ベースの分散アクセス制御方式を提案するものである．

Capability ベースのアプローチは，スケーラビリティを拡張するための，分散管理，権限委任のサポート，アクセスや認証の連鎖のトレーサビリティ，楕円曲線暗号に基づく標準的な証明書のサポートといった面で便益を提供する．

特に，エンド・ツー・エンドの認証，完全性，及び否認不可を確保するために，楕円曲線ディジタル署名アルゴリズム(ECDSA: Elliptic Curve Digital Signature Algorithm)を用いて署名された，CoAP(Constrained Application Protocol)リソース向けの capability トークンを提供している．

この分散ソリューションで，いかなる中間エンティティも介在しないシナリオの適用が可能になり，エンド・ツー・エンドのアクセス制御評価による分散シナリオが，Jennic/NXP JN5139 モジュール[1])ベースに評価されている．

実験で得られた結果は，提案したアプローチのフィージビリティを数値で実証するものであり，評価プロセス全体（スマートオブジェクトにおける署名評価を含む）を実行するのに平均で 480 ミリ秒を要したことが報告されている．

[1]) 16MHz 32-bit RISC CPU, 96kB RAM, 192kB ROM

5.1.1 本先行研究における今後の検討課題

本先行研究の論文の中で，以下に挙げる点は今後の検討課題として挙げられている．

- capability ベースのアクセス制御は，動的（ダイナミック）なコンテキストベースの条件管理モデルの定義が必要．
- capability の付与及び展開は，探索する必要のある新たな研究領域である．
- 失効管理と委任
- セキュリティの攻撃・脅威に対する抵抗力の理論的分析
- 仮名あるいは匿名の capability の利用のような技術によるプライバシ向上の追加のための検討

5.1.2 本先行研究に対する筆者の批評

本先行研究が提案する capability ベースの分散アクセス制御方式は，筆者のアプローチと合うものである．

ただ，アクセス制御の管理をどうするかは触れていない．

capability トークンの表現方法及びそれに基づく認可決定プロセスは，よりコンパクトにできる実現方式があるのではないかと考えている．具体的には，未だ検討中である．

署名アルゴリズムとして公開鍵暗号方式の楕円曲線ディジタル署名アルゴリズム(ECDSA)が用いられているが，格子暗号のようなより軽量なアルゴリズムを用いた方式が開発されるまでは，共通鍵暗号方式が実用的だと考えている．そのためには鍵管理の仕組みの向上が必要である．

本先行研究の今後の検討課題としても挙げられているが，コンテキストを意識した適応的なアクセス制御の仕組みを組み合わせる必要があると考えている．

5.2 Owner-to-Owner 認可問題，Owner-to-Any 認可問題に関する先行論文

IoT におけるアクセス制御の課題を指摘する最近の論文に，Heuer, J.らの“Toward the Web of Things: Applying Web Technologies to the Physical World”(May, 2015)[5]がある．

本論文は，Computer 誌(Volume: 48, Issue: 5)の Cover Feature “The Web: The Next 25 Years”として掲載されたものであり，ICT における現在の手法(SSL/TLS, Web Form Auth., Cookie)は，以下の“先進的な認可の問題”として述べる“owner-to-owner” あるいは “owner-to-*(any)” の認可問題をサポートしない，と述べている．

以下に，本論文が指摘する課題を紹介する．

5.2.1 先進的な認可の課題

“先進的な認可の問題”とは，以下の 2 つの問題である．

- Owner-to-Owner 認可：
  モノの所有者は他の用途で利用するのを自己認可する．
- Owner-to-*(any) 認可：
  モノの所有者はモノを他人が利用するのを認可する．

例えば，Owner-to-Owner 認可の問題は，利用者がオンライン印刷サービスを利用して，休暇中に撮った写真を印刷したいときに生じる．ここで，写真データはオンラインファイルサービスにより保存されている．この利用者が，オンラインファイルサービスの認証用の資格証明情報を，写真データにアクセスする印刷サービスへ渡すことが賢明ではないのは明らかだろう．

Owner-to-Owner 認可の問題を解決するために，OAuth 2.0 がユースケースの 3 者（リソースサーバ，リソース所有者，クライアント）に対応する新しい仕組みを取り込んだ．

ただ，センサや LED コントローラのような通信帯域，接続性，リソースアクセス等に制約のあるデバイス上での課題解決のためには，さらなる取り組みが必要である．

Owner-to-*(any) 認可の問題も同様に，UMA(User-Managed Access) は制約のあるデバイス上での課題解決のためには利用できないため，依然として残課題である．

5.2.2 認証に関する課題

アクセス要求者としてのモノの認証が必要である．

だが，モノを認証するためのインフラが存在しない．

- モノの ID 管理や，モノに付与される認証用の資格証明情報を保護するための仕組みが無い．
- PKI は，モノの証明書を提供するために必要な様々な要因によりスケールできそうにない．
- より軽量な手段，すなわち共通鍵暗号や，Datagram TLS を用いることになる．

5.2.3 認可に関する課題

モノは所有者である個人や法人の占有物であり，所有者はモノの公用は望まない．

よって，所有者が，モノと相互作用できる人やモノをコントロールできる仕組みが必要．

- Owner-to-*(any) 認可の問題
  - 所有者から利用者へのリソースアクセス管理権限の委譲を扱える必要がある．
  - 利用者がリソースにアクセスする現場に所有者がいることは前提にはできない．
  - 優先権のルールを確立する必要がある．
  - IETF で検討が進められている Delegated CoAP Authentication and Authorization Framework (DCAF) は，制約のある環境を想定しており，Datagram Transport Layer Security(DTLS)チャネルのための鍵となるアソシエーションを確立できるように設計されている．
  - DCAF を HTTP 向けの OAuth や UMA と組み合わせて利用できるのが理想的である．
- 所有権の管理
  - モノが生成された時点で所有者は未定である．
  - モノの所有権は頻繁に変わる．
  - モノの所有権を管理するための仕組みは Web セキュリティには未だ無い．
  - モノはデータと異なり再生産や再配置が容易ではない．

5.2.4 本先行研究に対する筆者の批評

筆者も前述したとおり，IoT におけるアクセス制御では，新たな主体（所有者，利用者，モノ）や新たな関係（モノーモノ，所有者－利用者）を扱える必要があり，Owner-to-Owner 認可や Owner-to-*(any)認可の問題や，所有権の管理の仕組みは，解決が必要な課題である．

その際に，Web の世界でこれらの問題を解決するために用いることのできる OAuth 2.0 や UMA といったプロトコルとの組合せを考慮に入れる必要があることを認識できた．

6. IoT における制約，コンテキスト，及びリスクを意識した適応的なアクセス制御の構想提案

6.1 想定するユースケースに適用可能なアクセス制御方式の構想

3 章で述べた IoT にかかわる制約や新たな要件から生じる課題，並びに 5 章で述べた先行研究の残課題を踏まえ，2.3 節で挙げたユースケース例(自動車の自動運転走行)における脅威への対策のために適用可能なアクセス制御方式の構想を提案する．

自動車の自動運転走行のようなオープンな環境では，情報を収集する相手(モノ)が不定であるという特性に対応できる必要がある．また，万一不正なアクセス主体が正当なアクセス主体になりすました場合であっても，自動車の制御や利用者のプライバシ情報にかかわる不正アクセスを許さないアクセス制御の実現が求められる．

このような要件を考えると，従来 ICT で用いられている単純な ID 管理と認証（who）だけでは，これに対応しきれない．また，その時点時点での他の条件(コンテキスト)を組み合わせてアクセス制御を決定する必要があると考えられる．（why,when,where,what,how の相関関係）

たとえば，以下に挙げるような，リスクを含むコンテキストを意識する必要があると考えられる．

- 収集する情報の送信元のモノが周囲に実在するか否か（物理的なコンテキストを検証）
- 収集する情報や制御コマンドの状態に連続性や妥当性があるか否か（状態のコンテキストを検証）
- 収集する情報や制御コマンドの関係に矛盾があるか否か（関係のコンテキストを検証）

IoT における課題を踏まえ適用可能なアクセス制御を実現するためには，上記のようなコンテキストを意識した適応的なアクセス制御を，Capability ベースの分散アクセス制御に組み合わせた，アクセス制御の管理及び実行のための方式が適していると考える．

7. 今後の研究の方向性

7.1 先行研究のさらなる調査

これまでの調査では，本研究の構想と同等の先行研究は見つかっていないが，調査は未だ不十分であると認識しており，IoT におけるアクセス制御の課題解決や，コンテキストを意識した適応的なアクセス制御方式を中心に，先行研究をさらに調査する必要がある．先行研究の成果から取り入れるべき内容が見つかれば取り入れていきたい．

7.2 IoT におけるコンテキストを意識した適応的アクセス制御方式の具体的な考案，及び実証評価

本論文で構想を提案した，IoT におけるコンテキストを意識した適応的なアクセス制御を，Capability ベースの分散アクセス制御に組み合わせた，アクセス制御の管理及び実行のための方式を具体的に考案していく．

また，最終的には，PoC(Proof of Concept)実装による定量的な実証評価を行いたいと考えている．定量指標としては，軽量化，高速化，脅威モデルへの対応能力（カバー率）などを考えている．

8. おわりに

本論文では，IoT に求められるセキュリティのうちアクセス制御に焦点を当て，従来の ICT のセキュリティ対策を IoT に適用しようとしたときに，IoT の制約や新たな要件により生じる課題があることを指摘した．また，課題を解決するためのアプローチ案を提示し，関連する先行研究を紹介し，残課題を挙げた．そして残課題を解決するために，「IoT における制約，コンテキスト，及びリスクを意識した適応的なアクセス制御」を，Capability ベースの分散アクセス制御に組み合わせた，IoT におけるアクセス制御の管理及び実行のための方式の構想を提案し，今後の研究の方向性を示した．

謝辞

本研究においてご指導・ご協力頂いた情報セキュリティ大学院大学 後藤厚宏教授ならびに後藤研究室の皆様に，謹んで感謝の意を表する．

参考文献

[1] Industrial Internet Consortium, “Industrial Internet Reference Architecture v1.7”, (2015). http://www.iiconsortium.org/IIRA-1-7-ajs.pdf
[2] 独立行政法人 情報処理推進機構(IPA), “自動車の情報セキュリティへの取組みガイド”, (2013). https://www.ipa.go.jp/security/fy24/reports/emb_car/documents/car_guide_24.pdf
[3] Hernández-Ramos, J. L. et al., “Distributed Capability-based Access Control for the Internet of Things”, Journal of Internet Services and Information Security (JISIS), Vol.3, No.3/4, pp.1-16 (2013).
[4] Skarmeta, A. F. et al., “A decentralized approach for security and privacy challenges in the internet of things”, *Internet of Things (WF-IoT), 2014 IEEE World Forum on* IEEE, pp.67-72. (2014).
[5] Heuer, J. et al., “Toward the Web of Things: Applying Web Technologies to the Physical World”, Computer, Vol.48, Issue.5, pp.34-42 (2015).