6E−2

# 有効距離を考慮した認証チケットシステムの構築

中西 健一[1] 松宮 健太[2] 石井 かおり[2] 楠本 晶彦[2] 徳田 英幸[1,2]

[1] 慶應義塾大学 環境情報学部 [2] 慶應義塾大学大学院 政策・メディア研究科

## 1 はじめに

近年，家電機器の高機能化に加え，ネットワーク接続可能な家電機器の増加により，家電機器の利用形態に変化が生じている．その一例として，ネットワーク接続性を有する家電機器の登場によりネットワークを介して多数のデバイスやユーザが家電機器を操作できるようになった．このような家電機器の利用形態を考慮し，家電機器の操作権限を管理することが必要となってきている．外部ユーザの家電操作権限を制限することにより，不正使用の防止を行える．また，幼い子供にはガスストーブの作動権限を許可しないなどの安全管理も可能となる．

家電操作権限を管理するためには家電機器の操作を試みているユーザを特定する必要がある．そのために、異なる家電操作デバイスを利用するたびにユーザ認証を行う必要がある．しかしこれはユーザにとって非常に煩雑である．

本研究では家電操作デバイスの変更のたびにユーザ認証を要求することなく家電操作権限を管理できる機構を提案する．本研究ではユーザと家電操作デバイスの空間情報を用いることにより家電操作権限の管理を行う．

## 2 概要

本稿で提案する機構 AccConBA(Access Control Based on Area) では，家電機器の操作を行っているユーザを特定しない．ユーザと家電操作デバイスの空間情報を取得することにより，家電操作権限の管理を行う．家電操作デバイスの空間情報を保証するためにチケットを用いる．

### 2.1 家電操作権限に関する方針

本機構では家電機器の操作を行っているユーザを特定しない．この方針は同一空間にいあわせることによるユーザの相互信用に基づく．そのため，本研究では一定空間内に複数のユーザが存在する場合，家電操作権限は各認証済みユーザの和集合とする．つまりその空間にいるユーザ全員に対して同等の家電操作権限を与える．これにより，家電操作権限が縮小するユーザは存在しないが，家電操作権限が拡大するユーザが存在する．図1に家電操作権限の和の例を示す．幼い子供は家に一人で留守番をしている時にはガスストーブを作動させる権限を有さないが，親が一緒にいる時にはガスストーブ作動権限が与えられる．

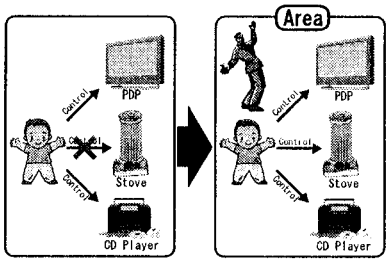


図 1: 家電操作権限の和

### 2.2 利用する空間情報

本研究では，ユーザの空間情報と家電操作デバイスの空間情報を取得し，利用する．以下にそれぞれの説明を述べる．

**ユーザの空間情報**

ユーザの空間情報とはあるユーザが該当空間内に存在するか否かの情報を指す．本研究では空間内のどの場所にいるかなどの細かい粒度の空間情報は考慮しない．本研究では，ユーザ認証によってこの情報を取得する．具体的には，ある空間内で認証を行ったユーザは該当空間内に存在するユーザとしてシステムによって認識され，その情報が一定期間保持される．よって，認証済ユーザは有効期間中に再認証を行う必要はない．

ユーザの空間情報は該当空間内のユーザ全員に適用する家電操作権限の和を作成する際に用いられる．

**家電操作デバイスの空間情報**

家電操作デバイスが該当空間に存在するか否かの情報である．この情報もユーザの空間情報と同様，空間内のどの場所にあるデバイスかなどの細かい粒度の空間情報は考慮しない．

本機構では，家電操作デバイスが該当空間内に存在するか否かによってその後に行う処理を変更する．以下にそれぞれの場合の説明を述べる．

- 該当空間内の場合上で述べた家電操作権限の和に基づく家電操作を行う．
- 該当空間外の場合別途ユーザ認証を要求し，そのユーザの家電操作権限に基づく管理を行う．

## 3 システムの設計

空間情報を取得，利用及び保証する為に設計した本機構について述べる．

### 3.1 用語の定義

以下に本稿で使用する用語の定義を行う．

- 登録済ユーザ: 該当空間内で登録されているユーザ
- ゲストユーザ: 登録済ユーザ以外のユーザ
- アクティブユーザ: 現在該当空間内で認証済のユーザ
- ユーザクライアント: 家電機器操作デバイス

---

A System for Access Control Based on User and User client's Area

Kenichi Nakanishi[1] Kenta Matsumiya[2] Kaori Ishii[2] Akihiko Kusumoto[2] Hideyuki Tokuda[1,2]

[1]Faculty of Environmental Information, Keio University

[2]Graduate School of Media and Governance, Keio University

e-mail: ken@ht.sfc.keio.ac.jp

### 3.2 システム構成

本システムは，ユーザクライアント，エリアサーバ，家電機器で構成される．
図2にシステム構成図を示す．

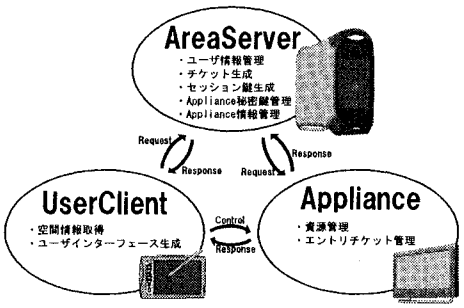


図 2: システム構成図

以下に各構成要素について説明する．

#### 3.2.1 エリアサーバ

ユーザクライアントが家電機器と適切な通信を行える為の処理を行う．ユーザ情報・家電機器情報の管理や，ユーザクライアントと家電機器間の通信に必要なチケットの生成を行う．

**チケット生成モジュール**

ユーザクライアントから家電機器との通信要求を受け取り，通信要求相手の家電機器に適したチケットを生成する．チケットの構成要素を以下に述べる．

- セッション鍵 ユーザクライアントと家電機器間の暗号化通信に使用する鍵
- アクティブユーザリスト アクティブユーザのユーザ ID の集合
- 空間 ID ユーザクライアントの空間 ID
- 時間情報 チケット生成時間・有効期間

このチケットを操作対象となっている家電機器の秘密鍵で暗号化し，ユーザクライアントに渡す．

**セッション鍵生成モジュール**

ユーザクライアントと家電機器間の通信で使用する鍵を生成する．この鍵は有効期限を持ち，その有効期限を過ぎた後は利用不可となる．このモジュールはチケット生成モジュールの要求を受けて動作する．

**家電機器秘密鍵管理モジュール**

該当空間内の各家電機器が保有する秘密鍵を管理する．家電機器の秘密鍵はチケット生成モジュールがチケットを暗号化する為に必要である．

**ユーザ情報管理モジュール**

登録ユーザ，アクティブユーザの情報を管理する．また，ユーザ認証機構を有する．

#### 3.2.2 ユーザクライアント

家電操作デバイスであり，PDA，携帯電話，PC などを想定している．

**ユーザインタフェース生成モジュール**

ユーザが情報を入力する必要がある際に，ユーザインタフェースを生成する．エリアサーバ，家電機器から受け取った情報を解析し，適したユーザインタフェースを生成．

**空間情報取得モジュール**

自身の空間情報を取得する．本機構ではユーザクライアントの空間情報によって提供する家電操作権限が異なるため，ユーザクライアントが自身の空間情報を取得する必要がある．

#### 3.2.3 家電機器

計算機資源とネットワーク接続性を持った家電機器を想定している．

**資源管理モジュール**

家電操作権限による資源管理を行う．必要に応じて家電機能のロックを行う．

**エントリチケット管理モジュール**

本研究において，ユーザクライアントはチケットを家電機器に渡すことで家電機器の信用を得たのち，セッション鍵による通信を行う．しかし，ある家電機器との通信要求を持つユーザクライアントは複数になり得る．本モジュールはどのユーザクアイアントがどのチケットを登録したのかを管理する．

### 3.3 動作概要

家電機器操作時における本システムの動作概要を示す．

1. ユーザは操作対象家電機器を選択する．
2. ユーザクライアントは操作対象家電機器との通信を希望するメッセージと自身の空間情報をエリアサーバに渡す．
3. エリアサーバはチケットとセッション鍵をユーザクライアントに渡す．
4. ユーザクライアントはチケットに自身の空間情報を加えて家電機器に渡す．
5. 家電機器は受け取った情報を複合化し有効性を判断する．有効な場合はチャレンジ（乱数）をユーザクライアントへ渡す．
6. ユーザは実行したい機能を選択する．
7. ユーザクライアントは機能の実行要求と乱数をセッション鍵で暗号化したものを家電機器へ渡す．
8. 家電機器は乱数の有効性を確認し，有効なら機能を実行する．

## 4 関連研究

家電機器に対するセキュリティ・家電操作権限を考慮した研究に X.509 based secure device control[1] が挙げられる．この研究では X.509 証明書を用いてユーザと家電機器制御サーバ間の相互認証を行うが，家電操作デバイスの変更のたびに再認証が必要である．本研究では一定空間外からの遠隔操作時には同様に認証を行うが，該当空間内の場合は一度認証を行った後は異なる家電操作デバイスを使う際に再認証の必要は無い．

## 5 まとめと今後の課題

本稿では，ユーザと家電操作デバイスの位置情報を用いて家電操作権限の管理を実現する機構 AccConBA について述べた．現在，本モデルを J2SE[3]，JCE[4] で実装中であり，今後は測定，評価を行う予定である．

## 参考文献

[1] 冨岡 和陽, 文 武, 溝口 文雄：X.509 証明書を用いた安全な情報機器のコントロール，情報処理学会第 59 回全国大会予稿，(1999.9)
[2] Sun Microsystems, Inc: Java 2 Platform, Standard Edition.
[3] Sun Microsystems, Inc: Java Cryptography Extention.