

# コンテキストウェア・アクセス制御技術ACA<sup>2</sup> A Context-Aware Access Control Mechanism: ACA<sup>2</sup>

横山重俊(Shigetoshi Yokoyama) 山田 茂樹(Shigeki Yamada)

## 何がわかる?

ユーザの場所や行動のような、ユーザの身の回りの情報(ユーザコンテキスト)を活用することによって、「いま」「ここで」欲しい情報を安全に提供できるようになります。  
We aim at providing secure information-providing services, utilizing user context information such as user's location and actions.

## どんな研究?

ユーザにサービスを提供中に、ユーザコンテキストの変化をセンサ経由でサービス提供者に通知し、サービスを継続できる条件が満たされなくなるとサービス提供を中断する機構(アクセス制御機構)を研究しています。  
This research focuses on an access control mechanism that enables on-going services to be discontinued in the service where any user context change is informed to the service provider and the conditions to continue the service has not been satisfied anymore.

## どのようなことに役立か

例えば、携帯電話のユーザが飛行場の待合室に居る間は通信ができますが、飛行機に搭乗すると自動的に通信できなくするようにしたり、コンサート会場で上演中は携帯電話を使えなくするようなことも可能になります。  
For example, the proposed technology could be used to switch off the mobile phone while its user is inside the airplane or during playing in a concert hall because both situations do not allow mobile communications.

## 研究状況

### 研究の動機 Motivation of the Research

**電車内 In the Train**  
電話接続ポリシー Call permission policy  
- 車内は通話禁止 Policy Prohibited inside the train  
- 車内は通話禁止 Policy Prohibited inside the train

**劇場内 In the Theater**  
電話接続ポリシー Call permission policy  
- 上演中は通話禁止 Policy Prohibited inside the theater during staging  
- 上演中は通話禁止 Policy Prohibited inside the theater during staging

**自動車で In the Car**  
電話接続ポリシー Call permission policy  
- 運転中は通話禁止 Policy Prohibited during driving  
- 運転中は通話禁止 Policy Prohibited during driving

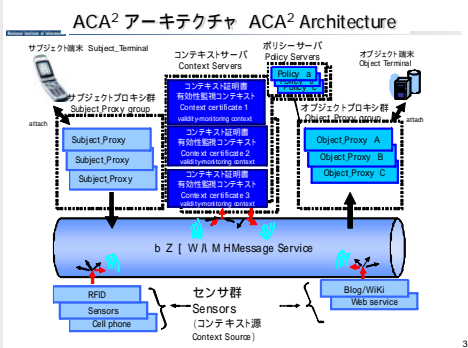
**結論**  
電話接続はコンテキストに基づいて制御されるべき  
Call connection and disconnection should be controlled, based on the contexts.  
? コンテキストウェア・アクセス制御方式ACA<sup>2</sup>  
Context-Aware Access Control for Ubiquitous Services: ACA<sup>2</sup>

### ACA<sup>2</sup> 接続モデル ACA<sup>2</sup> Connection Model

(similar to Public-Phone Connection Model)

**公共電話モデル Public-Phone Connection Model**  
- 受話器を上げる Pick up a phone receiver  
- オペレーターに料金を聞く Ask operator for charge  
- お金を入れる Insert Coins  
- ダイヤルする Dial  
- 通話 Talk  
- お金がなくなれば通話終了 Call terminates if money runs out

**ACA<sup>2</sup> 接続モデル ACA<sup>2</sup> connection Model**  
- サブジェクトをサブジェクトプロキシにアタッチ Attach Subject to Subject Proxy  
- オブジェクトプロキシにポリシーを聞く Ask Object proxy for policy  
- コンテキスト収集源証明書を渡す Transfer Context-Collection-Source Certificate  
- コンテキスト証明書を渡す、オブジェクトにアクセスを要求する Transfer Context Certificate and request access to Object  
- オブジェクトにアクセス Access to Object  
- コンテキストが変化してアクセス権が無くなる場合 Access is cut off when context changes and access right is not authenticated anymore.



### ACA<sup>2</sup> アクセス制御手順 ACA<sup>2</sup> Access Control Procedure (1/4)

◆ サブジェクトからサービス要求があると、サブジェクトプロキシが動的に割り付けられ、サブジェクト端末にアタッチされる  
◆ When a service is requested by Subject, Subject Proxy is dynamically allocated and attached to Subject Terminal to connect to ACA<sup>2</sup> architecture.

Subject Terminal  
Pre-registered ID Area  
Subject Proxy group  
Subject Proxy a  
Subject Proxy B  
Subject Proxy ?  
Message Service  
RFID  
Sensors  
Cell phone  
Blog/Wiki Web service

Attach  
httpセッションなどにより、Subject ProxyグループにあるSubject Proxy BにSubject TerminalをAttachする  
ACA<sup>2</sup> system attaches Subject Proxy B in Subject Terminal through an http session or other means

### ACA<sup>2</sup> アクセス制御手順 ACA<sup>2</sup> Access Control Procedure (2/4)

◆ サブジェクトはコンテキスト情報証明書をサブジェクトプロキシに送る  
◆ Subject sends Context-Collection-Source Certificate to Subject Proxy  
◆ コンテキスト情報証明書を、コンテキスト収集源情報(コンテキストID、収集源ID、収集先URL)に符号化されたSubject ID, Subject\_Terminal\_IDに関するコンテキストサーバ固有のコンテキスト証明書をSubject Proxyが生成して送る  
◆ The Context-Collection-Source Certificate is the document such as context source ID, encrypted subject ID, subject terminal, signed by Context Server.

コンテキスト収集源証明書を渡す Put  
Send context-collection-source certificate? (OK)  
Context-collection-source  
Message Service  
RFID  
Sensors  
Cell phone  
Blog/Wiki Web service

### ACA<sup>2</sup> アクセス制御手順 ACA<sup>2</sup> Access Control Procedure (3/4)

◆ サブジェクトプロキシがセンサから必要なコンテキストを収集。Subject Proxy collects necessary contexts from Sensors.  
◆ サブジェクトプロキシがコンテキストとコンテキスト証明書に基いて、オブジェクトプロキシに接続し、Subject Proxy groups the collected contexts into Context-Certificate, signs it, and sends it to Object Proxy. This enables Subject Proxy to access Object Proxy.  
◆ サブジェクトプロキシはコンテキスト証明書とContext-Certificate Validity Monitoring Contextをコンテキストサーバに登録し、コンテキストが変更されると通知を受け取る。  
◆ Subject Proxy registers Context-Certificate Validity Monitoring Context with Context Server to monitor the context changes.

2次元 QRコードを提示し、アクセスを許可する  
Call Engineer Y2 at 09:00  
YYYYYY  
YYYYYY  
OK

Subject Proxyがコンテキスト証明書とContext-Certificate Validity Monitoring Contextをコンテキストサーバに登録し、コンテキストが変更されると通知を受け取る。  
Subject Proxy registers Context-Certificate Validity Monitoring Context with Context Server to monitor the context changes.

### ACA<sup>2</sup> アクセス制御手順 ACA<sup>2</sup> Access Control Procedure (4/4)

◆ コンテキスト監視機能を持つコンテキストウェアがSubject Proxy またはObject ProxyがSubscribeする。これによってコンテキストが変化して、条件が満たされなくなると、Subject Proxy またはObject Proxyにサービスの停止が指示される。  
◆ Subject Proxy or Object Proxy subscribes to Context-Certificate Validity Monitoring Context in the Context Server that will receive the context change from sensors. This enables Context Server to notify Subject Proxy or Object Proxy of service cutoff.

Context Server  
Subject Proxy  
Object Proxy  
Message Service  
RFID  
Sensors  
Cell phone  
Blog/Wiki Web service

### 追従性に関する性能評価 Performance Simulation Models

◆ 性能指標: コンテキスト変化からサービス停止までの応答時間  
◆ Performance Metric: Context Response Time from Context Change to Service Suspension  
◆ コンテキスト変化のラフな発生するセンサ間でドメインの割り振りがあることを想定  
◆ We assume Context Change Traffic Generated from Sensors is unbalanced among sensors.

System Model 1: Centralized Traffic Distribution  
System Model 2: Static Traffic Distribution  
System Model 3 (ACA<sup>2</sup>): Dynamic Traffic Distribution

