MARS（Mutual Authentication RSS）
ー相互認証を基盤とした未来型 RSS 配信ソフトウェアの開発ー

１．背景及び目的

コンピュータやセンサの小型・省電力化などに伴い、我々が生活する環境には様々な情報機器群が存在するようになった。ユビキタス・コンピューティングやセンサ・ネットワークの普及に伴い現実世界の多種多様な情報リソースを、各個人ユーザが利用・提供する時代が来ることが想定される。一方で、Web の世界では Web2.0 と呼ばれる新たな Web 形態が進化してきた。Web2.0 では特に、各所で公開されている Web サービスをユーザ自らが参加し自由に組み合わせ、新しいサービスを創生するマッシュアップが促進されている。

以上のような背景から、今後の Web 形態ではセンサ・ネットワークの普及により各個人が現実世界の情報を管理し、それらのリソースをマッシュアップすることで、今までに無かった新たな有益なサービスを創生する時代が来ると想定される。しかしながら、これからの時代(未来)を想定すると以下の点を考慮する必要がある。

1. リソースやユーザへの認可
   これまで Web サービスは、広く公に公開されてきたがセンサ情報のように個人に関わる機密性の高い情報は、「誰にどの情報を公開するかを制限する」認可を考慮する必要がある。
2. 相互認証と通信暗号化
   情報を提供する側と利用する側が互いに信頼し合う相互認証に基づいて、情報が配信されなくてはならない。また、悪意のあるユーザを想定し通信暗号化も考慮する必要がある。
3. 利便性の高い利用形態
   組織間をまたいだ広域ネットワーク上でのリソースの提供・利用を想定し、一度の認証で様々なリソースへアクセス可能な SSO(Single Sign-On)の機構を考慮する必要がある。
4. マッシュアップを促進する統一的なデータ形式
   センサ・リソースはセンスするその対象によって多くのデータフォーマットが存在する。センサ・リソースを利用したアプリケーション開発者がデータフォーマットの差異を気にすることなく開発するための、統一的なデータフォーマットを考慮する必要がある。

以上より、本プロジェクトでは、認証基盤(認可や認証、暗号化、SSO)にグリッド・コンピューティングを利用し、センサ・リソースの統一的なデータフォーマットに RSS を利用した情報配信ソフトウェアを開発することを目的とする。グリッドの相互認証基盤を利用することで、複数組織間にまたがるデータ配信や個々人のプライベートにまで至るデータをセキュアかつ透過的に扱うことが可能となる。また、センサ・リソースの表現に既存の RSS を利用することで、データを統一的かつ容易に利用することができ、既存の RSS アプリケーションの利用だけでなく、今までに無かった有益な新たなセンサ・サービスの開発が期待される。

２．開発内容

開発ソフトウェア　MARS の利用形態を図 1 に示す。MARS の利用形態では、各ユーザやホストは第３者認証局(CA:Certificate Authority)から署名を受けることでグリッド環境への参加となる。その後、クライアントからリソース・サーバ(リ

ソースを保持するサーバ)への通知予約(Subscribe)を行う。その際にユーザの証明書をもとに認証や認可が行われる。そして、センサ管理者が提供するセンサ・リソースに更新があると、通知先のクライアントへリソースの通知(Notify)が Push 型で行われる。クライアント～リソース・サーバ間は両者の証明書に基づく公開鍵証明書による相互認証や公開鍵暗号化が行われ、また Web サービスの通信プロトコルである SOAP(Simple Object Access Protocol)により通信が行われる。そして最後に、クライアント側でセンサ・リソースを RSS に変換することで、アプリケーション開発者は RSS という統一的かつ標準的なフォーマットを想定したアプリケーション開発が可能となる。

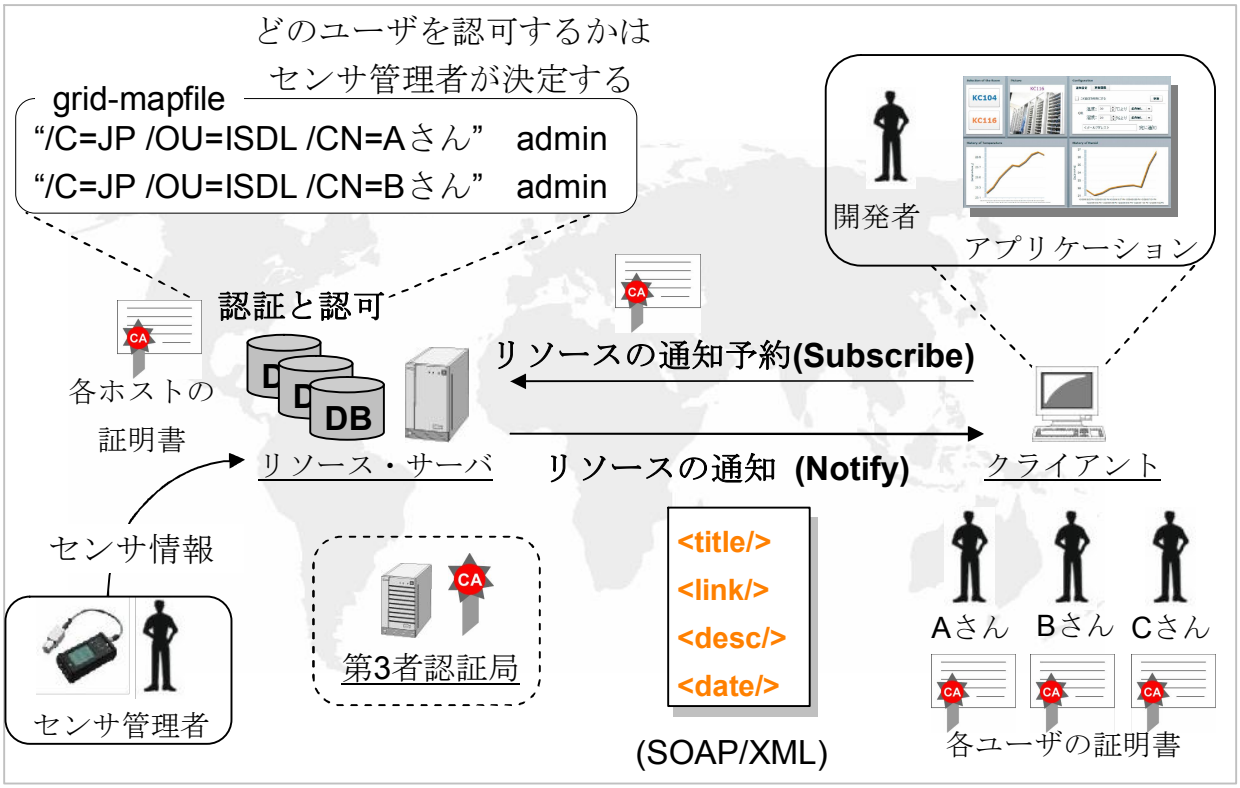

図 1. MARS の利用形態

2．1．グリッド上の Web サービス間での Push 型配信

MARS ではセンサ・リソースの提供・利用を、グリッド上の Web サービスとして行う。データ配信のモデルを図２に示すとおり Notification-Subscription にすることで、リソースの更新をリアルタイムに通知することが可能となる。そして、１つのリソース(リソースを提供するサービス)には複数のユーザが利用することを想定するため、利用ユーザ固有のリソースを Factory サービスにより実現する。そして、サービス間の相互認証と通信暗号化および認可をグリッド技術で実現する。

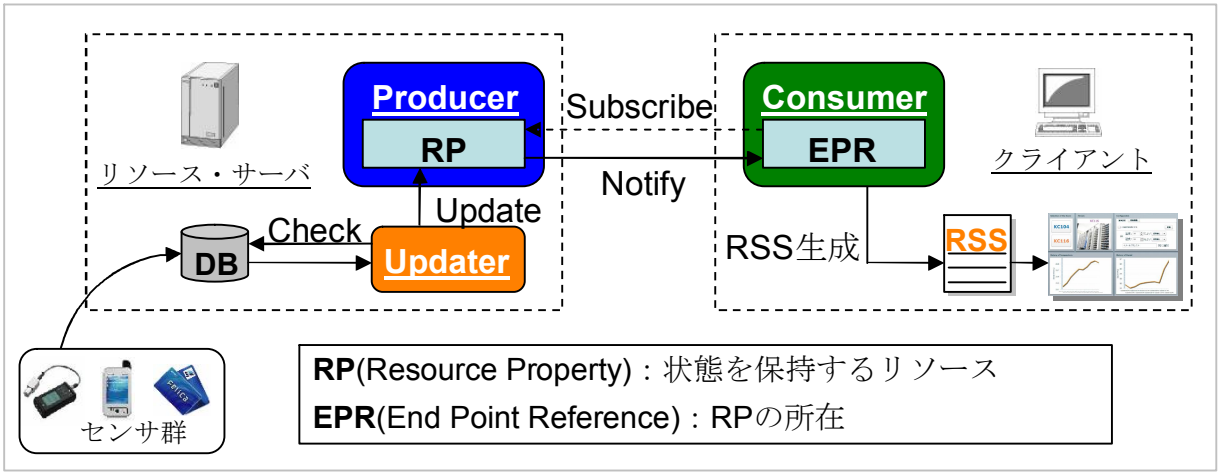

図２． Notification-Subscription による Push 型配信の構成

２．２　センサ管理者とアプリケーション開発者の支援

通常、グリッド上で Web サービスを公開する際には非常に複雑な作業が必要となる。MARS ではセンサ管理者およびアプリケーション開発者がグリッドの知識を有していないことを想定しているため、複雑な諸作業を簡易化するため、センサ管理者とアプリケーション開発者を支援する各種ライブラリとビルド用の設定ファイルを提供する。Jakarta プロジェクトで提供される Ant ツールを利用し、build.xml と build.properties を提供することで、センサ管理者とアプリケーション開発者の任意のサービスを実行することが可能となる。

２．３　MARS を利用したアプリケーション例

MARS を利用したアプリケーション例として２つのシナリオに沿ったアプリケーションを開発した。MARS は通常のグリッドのように大規模なものではなく、個人レベルでの利用を想定しているが、グリッドの認証技術を利用することで、より有益なサービスの開発が期待できる。

２．３．１　シナリオ１ ～ 多忙な先生をタイミング良く捕まえる ～

（背景）

- 先生は大変多忙であり、いつ部屋にいるかが不明である。
- ミーティングをしたい学生としては、先生を“タイミング良く”捕まえたい
- 先生としては、“誰それかまわず”居場所を公開したいわけではない（例えば、研究を頑張っている学生には積極的に居場所を公開したい）。

（設計および実装）

- 利用するセンサ：RFID Tag（先生が保持）、RFID Reader（先生が部屋にいることを検知）
- 外部アプリケーション：Plagger（Consumer サービスから生成される RSS を取得し、GMail 経由で学生の携帯電話へ通知）
- 配信形態：Push 型配信
- 認可：グリッド用認可ファイル：Gridmapfile

アプリケーション実行例を図３に示す。図３の YYY は RFID Tag を保持しており部屋には RFID Reader が設置してある。部屋に入ると RFID Reader で Tag を読み取り、リソース・サーバへデ

ータを格納する。その後、Updater サービス→Producer サービス→Consumer サービスまでを Push 型でデータの配信を行い、Consumer サービスの RSS 生成時に外部アプリケーションとして Plagger を実行し、XXX の携帯電話へ通知する。YYY はあらかじめ、Gridmapfile にて XXX の認可を行うことで、通知する人を制限することが可能となる。

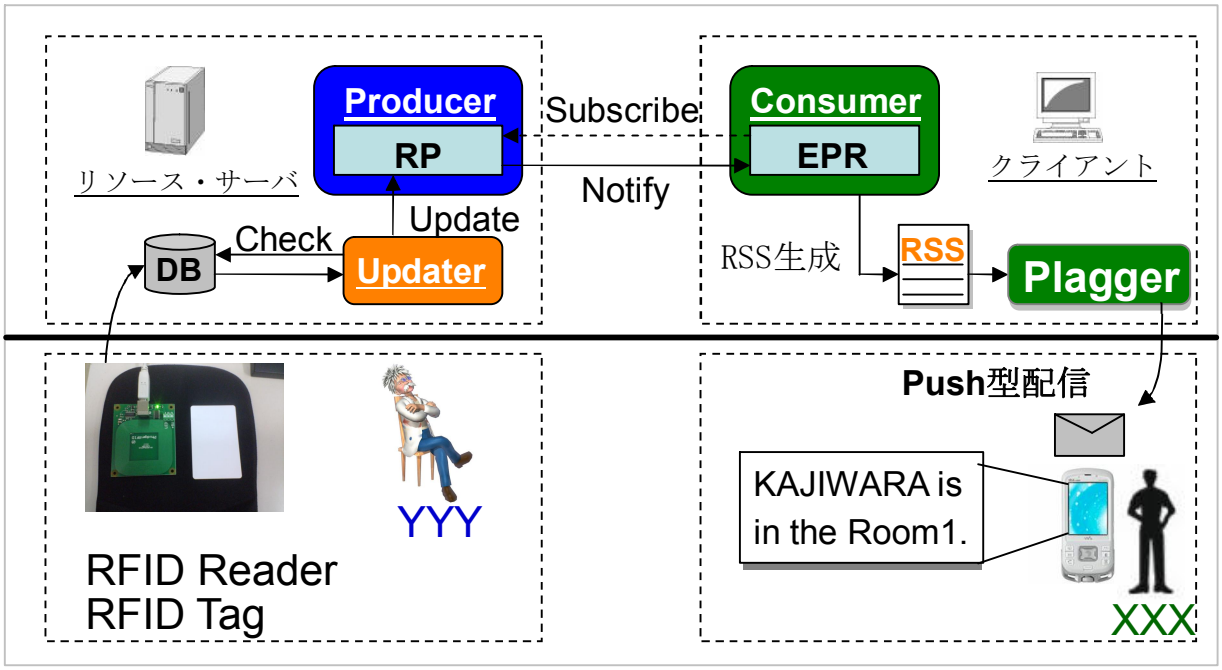

図３．アプリケーション実行例（シナリオ 1）

２．３．２　シナリオ２ ～ それとなく飲みに誘ってもらえる ～

（背景）

－ 出張先の仲間（比較的目上の方）に飲みに誘ってもらいたい。
－ 一緒に飲みたい人もいれば、そうでない人もいる。
－ 自分から飲みに誘うのには抵抗がある（ちょっとした責任感）。
－ 自分の居場所に“それとなく”気づいた相思相愛な人に飲みに誘ってもらいたい。

（設計および実装）

－ 利用するセンサ：GPS（端末は「au W42S Sony Ericson」、アプリケーションは「au EZ ナビウォーク」を利用）
－ 外部アプリケーション：既存の RSS リーダを利用
－ 配信形態：Pull 型配信
－認可：グリッド用認可ファイル：Gridmapfile

アプリケーション実行例を図４に示す。図４の YYY は GPS 情報をリソース・サーバへ格納する。その後は図３同様 MARS にて RSS 生成までを自動で行うが、本アプリケーションは Push 型ではなく、あえて Pull 型配信を行う。これは、背景にもあったように自身から積極的に誘うという行為には多少なりとも責任感が伴うためであり、YYY と相思相愛な関係にあるユーザからの誘いを期待するためである。また、MARS では RSS を利用するため、既存の汎用の RSS リーダが利用可能となっている。YYY はあらかじめ、Gridmapfile にて XXX の認可を行うことで、誘ってもらう人を限定することが可能となる。

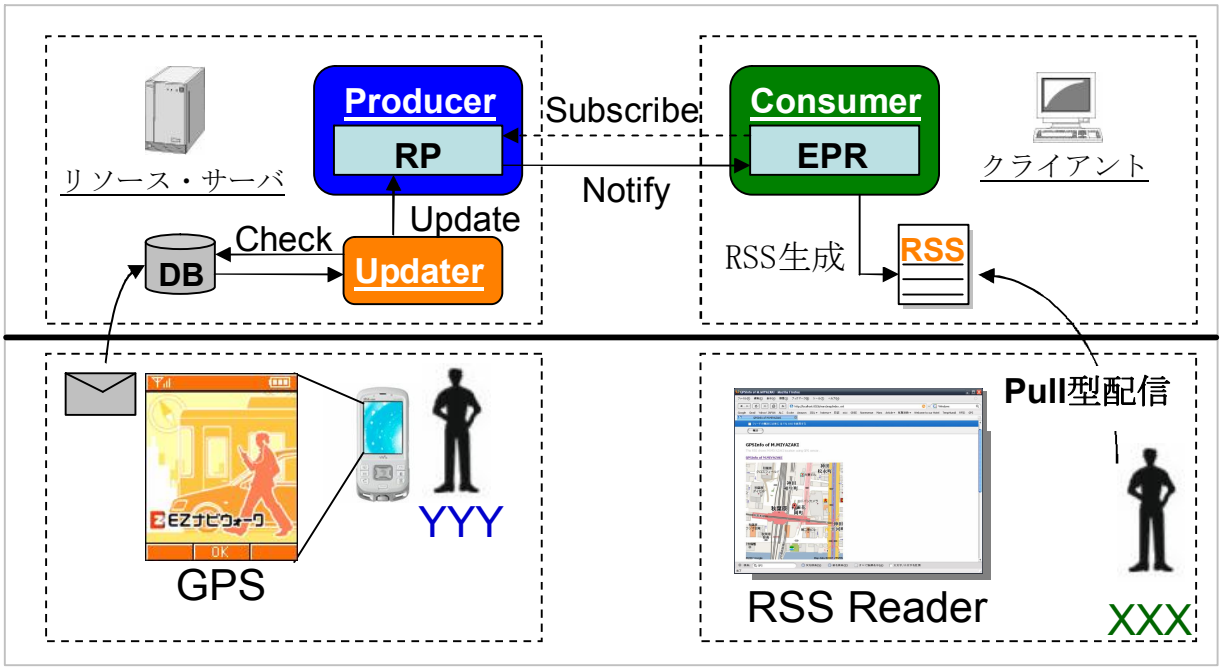

図４．アプリケーション実行例（シナリオ 2）

３．期待される効果

本プロジェクトを通して、MARS を用いた 2 つのアプリケーションを開発したが、今後の展望としては、ホームセキュリティ分野への応用を考えている。MARS の特徴はグリッドの強力な認証基盤を利用し、既存の Web 環境に容易に適用可能という点である。そのため、より強力な認証基盤や高い機密性の保持、組織間をまたぐ利用形態が必要となる、ホームセキュリティ分野に着目している。

４．普及（または活用）の見通し

本プロジェクトで開発を行った MARS は、グリッド・コンピューティングに由来する。グリッド・コンピューティングは、これまで主に科学技術計算分野で利用されてきた。しかしながら、本提案では、グリッド・コンピューティングの本質が「仮想化を実現する認証基盤」と位置づけることで、従来の Web 環境にもグリッド・コンピューティングが普及することを想定している。そのため、今後 MARS の普及は、グリッド・コンピューティングが、ビジネス分野やコンシューマ分野においても普及することが、重要だと考える。

５．開発者名（所属）

＋梶原広輝（同志社大学大学院 工学研究 知識工学専攻）

（参考）開発者 URL

http://mikilab.doshisha.ac.jp