Jini ネットワークへのアクセス制御機能の導入

宮本　幹大　　Hoa TRAN Xuan　　吉永　努　　曽和　将容

電気通信大学　情報システム学研究科

1 はじめに

２１世紀に入り PC や情報家電などのホームネットワーク化、あるいは次世代ブロードバンド住宅、電子政府事業などに伴う取り組みが各方面で活発に行われている[1]。以上のような統合的なネットワーク環境を実現するものに、サンマイクロシステムズ社が開発した Java によるミドルウェア Jini[2][3]がある。

本研究では Jini を対象として、ホームネットワークをより安全で利便性の高いものとすることを目的とし、Jini にアクセス制御機能を導入する。

具体的にはホームネットワークや研究室などの小規模ネットワーク環境を想定したローカルネットワーク内および外出先からのリモートアクセスに対応するユーザ認証機能の追加とユーザ別に許可されたサービスの利用を可能にする。

2 Jini の解決すべき課題

Jini の解決すべき課題はサービス利用者とサービス提供者を仲介する Jini のルックアップサーバ（LUS）へのアクセスに制限がないということである。これにより LUS への無制限なサービス登録攻撃、あるいは LUS へ誰でも勝手にアクセスできてしまうことによるプライバシ流出の危険性など様々な問題の可能性[1]がある。特にネットワーク内の LUS を自動的に発見する Jini のプロトコル特性[4]によって発見できる LUS は裸同然と言える。

またファイヤーウォールの IP アドレス制限では IP アドレスが毎回変わる外出先などからのアクセスや IP アドレスのなりすましに対応できないので、IP アドレスに頼らないアクセス制限方法を考える必要がある。

以上によりサービス利用者からのアクセスを認証し、さらにそのユーザにサービスの利用権があるかどうかを特にチェックする必要がある。

"Introducing access control functions to a Jini network"
Mikihiro Miyamoto, Hoa TRAN Xuan, Tsutomu Yoshinaga, and Masahiro Sowa
The Graduate School of Information Systems, University of Electro-Communications

3 アクセス制御機能の導入

3.1 アクセス制御サーバ JACS の構築

２で挙げた問題解決方法としてアクセス制御サーバ JACS（Jini Access Control Server）を構築する。

JACS 構築に際して以下の設計方針で開発を行う。
・シンプルなシステム構築により、セキュリティホールの防止と、わかりやすさ・利便性を追求する
・セキュリティバランスの確保とそのレベルアップ
・Jini もともとのシステムやメリットを崩さない

従来の Jini アーキテクチャでは、サービス利用者が直接 LUS にアクセスするシステムだが、提案方式では、サービス利用者はまず JACS にアクセスする。JACS はアクセスを受けるとユーザ認証および、ユーザが要求するサービスが利用可能かどうかチェックする。その後サービス利用者に代わり LUS にアクセスする。この LUS を Private-LUS と呼ぶ。以下図１にそのシステム構成を示す。

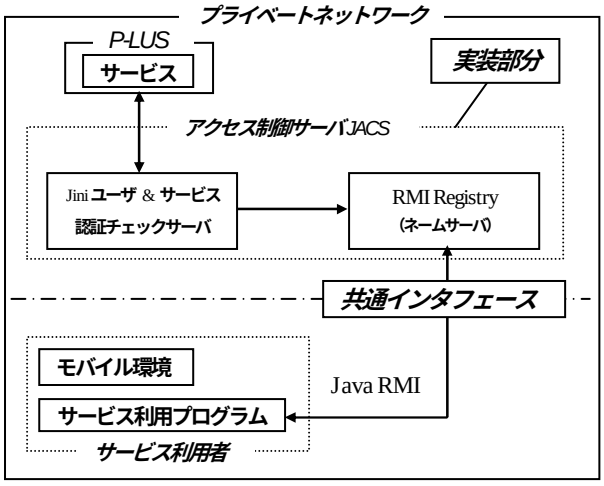

図１：JACS システム構成

3.2 画像情報一致型ユーザ認証システム ISS の導入

さらに本研究では画像情報一致型ユーザ認証システム ISS（Image-password based Secure-login System）を提案し Private-LUS にアクセスする JACS にこの機能を追加する。

ISS は、同じ画像ファイルを持つ情報機器同士であれば通信可能になるというシンプルなシステムである。この ISS を JACS に実装することによって、サービス利用者の画像ファイルを JACS でチェックすることが可能となり、画像ファイルで Jini ネットワークユーザかどうかの本人確認を行うことが可能になる。

4 処理の流れ

サービス利用者が JACS にアクセスし、要求するサービスの実行までの流れの概要を以下図２に示す。実験環境としては研究室内の PC やワークステーションを用いて Jini ネットワークを構築する。

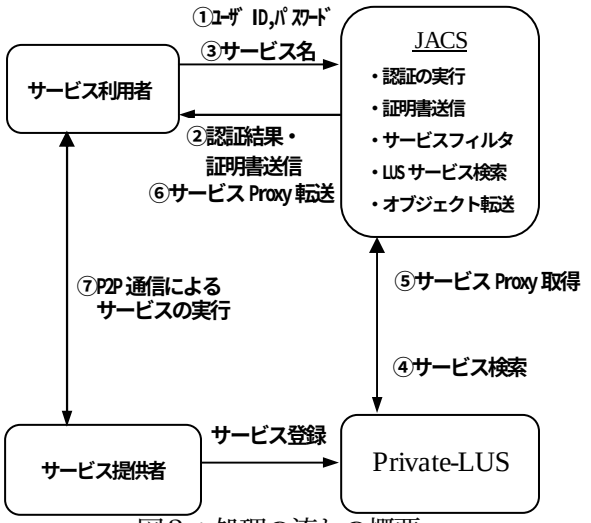

図２：処理の流れの概要

前提として JACS が起動し、あらかじめサービス利用者の要求するサービスが Private-LUS に登録されているものとする。JACS 起動時自動的にネームサーバ RMI Registry が立ち上がる。ユーザ別のサービス利用可能なリストは JACS で管理する。サービスの登録に関してはローカルネットワーク内では無制限に登録でき、ローカルネットワーク外からはルータで Private-LUS のポートを閉じることにより登録できない。ポートを閉じない場合でもサービス提供者が Private-LUS のホスト名または IP アドレスを知っていてなおかつ Java RMI の仕様により Private-LUS とサービス提供者両者が共通のインタフェースプログラムを持っていなければサービスの登録は不可能である[5]。

次にサービス利用までの各ステップを示す。

Step1: サービス利用者は JACS が RMI Registry に登録したアドレス（例: rmi://ホスト名 or IP アドレス/任意のプログラム名）でアクセスする。この時 Java RMI で通信する。

Step2: サービス利用者はユーザ ID とパスワードを JACS に渡す。パスワードについては、サービス利用者がキャラクタパスワード（JAAS 認証）もしくはイメージパスワード（ISS 認証）を選択できる。

Step3: 認証が成功した場合、JACS はサービス利用者に証明書を RMI で送り、サービス利用者はその証明書をメモリバッファ領域に格納する。その直後 JACS はサービス利用者の証明書を使って認証したサービス利用者かどうかチェックする。この証明書はサービス利用者のログアウト時、JACS が削除する。

Step4: サービス利用者は利用したいサービス名を JACS に送る。JACS ではサービス利用認証フィルタとして登録済のデータを元に、ユーザ ID 別の利用可能なサービスリストを参照する。認証フィルタを通過した場合、JACS はサービス利用者から要求のあったサービス名で Private-LUS にアクセスしサービスを検索する。目的のサービスが見つかった場合、Private-LUS からサービスプロキシを受け取り、これをサービス利用者にオブジェクトとして転送する。以上によりサービス利用者はそのサービスを提供した機器と P2P 通信を行うことができる。

以上、アクセス制御サーバ JACS により Jini ネットワークユーザ・機器別のアクセス制御が可能になる。

5 おわりに

本研究では Jini に JACS と ISS を導入し、ユーザ・機器別の安全でプライベートなアクセス制御を実現した。今後の課題としては通信路の暗号化や GUI によるユーザインタフェースの改善などが挙げられる。

参考文献

[1] 電子情報技術産業協会, ホームネットワーク化の進展に伴い生ずるセキュリティ(生活安全確保・個人情報等)の課題と対応に関する調査,(2001)

[2] Jini の仕様 v1.2 各ドキュメント
http://www.sun.com/software/jini/specs/japanese/

[3] Robert Flenner, “Jini and JavaSpaces Application Development”, Sams Publishing, (2001)

[4] Scott Oaks, Henry Wong, “Jini クイックリファレンス”, O'REILLY Japan,(2001)

[5] 中山　茂, “Java 分散オブジェクト入門”, 技報堂出版,(2000)