M-025

情報家電のネームサービスにおけるプラグ＆プレイ対応アクセス制御の検討

A Study of access control for plug & play in name services for information appliances

日下 貴義† 馬場 達也† 松田 栄之†
Takayoshi Kusaka Tatsuya Baba Shigeyuki Matsuda
e-mail: { kusakat, babatt, matsudasg }@nttdata.co.jp

1. はじめに

近年，適用範囲が拡大され続けているインターネット技術は，家電の基盤技術にも応用され，情報家電としての利用形態が模索されている．

インターネット上で，情報家電などのサービスに接続するとき，一般に，ネームサービスの利用を伴う．ネームサービスとは，ネットワーク上の資源やサービスを名前で管理し，それらへのアクセス手段を決定できる物理的位置情報を提供するものである．

これまでに著者らは，ネームサービスのセキュリティ向上対策として，ネームサービスへの問い合わせ元ユーザに対して，認証を行い，認証結果によって問い合わせ元へのアクセス制御を実施することを提案し，実装を行った[1]．実装では，インターネットにおけるネームサービスである DNS（Domain Name System）[2][3]に，ホスト名から IP アドレスを検索（名前解決）するための認証とアクセス制御の仕組みを実現した．また，情報家電向けプロトコルのひとつである Jini[4]のネームサービスの LUS（Lookup Service）にも同様に，サービス名から URL を含んだ JavaRMI スタブを検索するための認証とアクセス制御の仕組みを実現した．ネームサービスの認証とアクセス制御の実装には，Kerberos[5]システムを利用し，シングルサインオンを実現した．これにより，ネームサービスにおける認証とアクセス制御が連携できることを確認した．

2. ネームサービスにおけるアクセス制御情報の運用上の問題点

ネームサービスにおけるアクセス制御では，アクセス制御情報を，Kerberos KDC（Key Distribution Center/認証とアクセス制御用のサーバ）で一元管理し，複数ネームサービス間の認証やアクセス制御の連携を可能とした．しかし，これらのアクセス制御情報は，サービス提供者やシステム管理者によるメンテナンスが通常である．アクセス制御情報のメンテナンスは作業コストがかかるうえ，情報更新には人為的な誤りが起きやすいなど，運用上問題があると考えられる．また，サービス提供者やシステム管理者によるメンテナンスは，適用分野として想定している情報家電プロトコルの特徴であるプラグ＆プレイの利便性も損なっているといえる．

そこで，本研究では，情報家電におけるサービスのプラグ＆プレイを想定し，ネームサービスが認証やアクセス制御に使用するアクセス制御情報を，プラグ＆プレイで自動登録する方法を提案する．

3. アクセス制御情報のプラグ＆プレイ

参考文献[1]で構築したネームサービスのアクセス制御連携モデル（以後，「アクセス制御連携モデル」と呼ぶ）において，Kerberos が参照するアクセス制御情報は，サービスごとにユーザによるアクセス許可の可否を記述したものとしている．例えば，「サービス A に対して，ユーザ B のアクセスを許可する」といった記述である．実装では，許可するユーザのみを記すポジティブリスト形式をとっている．

プラグ＆プレイ機能を利用して，サービスが動的に追加されたり削除されたりすると，それに対応したアクセス制御情報も動的に追加されたり削除されたりする必要がある．そこで，サービスがプラグ＆プレイ機能によってネームサービスに登録されるのと同時に，サービスが所持するアクセス制御情報を自動登録させるための仕組みや，サービスが消滅すると，該当するアクセス制御情報も自動的に削除される仕組みを提案する．これを，プラグ＆プレイ対応アクセス制御と呼ぶ．

アクセス制御連携モデルを参考にし，プラグ＆プレイ対応アクセス制御を以下で説明する．

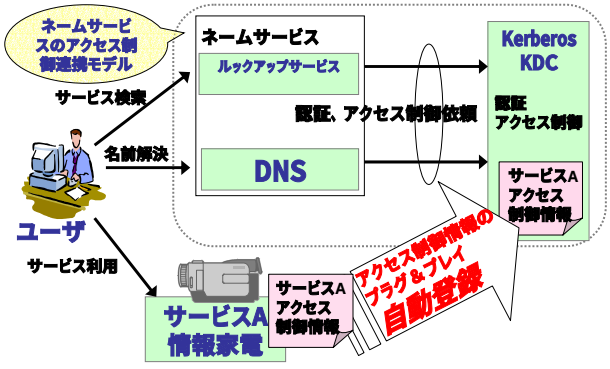

図 1 アクセス制御情報登録のプラグ＆プレイ

†（株）NTT データ 技術開発本部
Research and Development Headquarters
NTT DATA CORPORATION

あるサービスに対してアクセス制御する必要があれば，そのサービスはアクセス制御情報を持つことになる．プラグ＆プレイに対応したこれらサービスが起動したとき，ネームサービスへ自サービスの登録（サービスの所在や属性等の登録）を行うと同様に，Kerberos KDC へアクセス制御情報を登録させるようにする．アクセス制御情報の書式は，OASIS[6]で検討されている XACML（eXtensible Access Control Markup Language）形式を参考に，汎用的なものとした．XACML で記述されたアクセス制御情報は，アクセス制御対象となるサービスから Kerberos KDC へ送信され，登録される．（**図** 1参照）

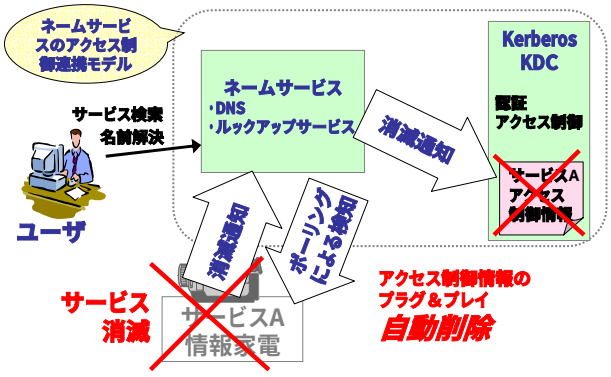

図 2 アクセス制御情報削除のプラグ＆プレイ

また，サービスが消滅した場合，ネームサービスからそのサービスの登録情報が削除される．このとき，Kerberos KDC は，該当するサービスを管理するネームサービスから消滅通知を受信するか，ネームサービスが行っているサービスへのポーリングのタイムアウトによる消滅通知を受信することによって，サービスの消滅を検知し，対応したアクセス制御情報を削除する．これにより，以後 Kerberos KDC が，消滅したサービスに対するアクセス制御を実施することはない．（**図** 2参照）

4. 階層的なネームサービスへの対応

アクセス制御連携モデルでは、DNS や LUS など複数のネームサービスは，それぞれで管理している共通のサービスのアクセス制御を行うために，アクセス制御の連携を行っている．このとき，ネームサービスそれぞれのアクセス制御情報は，単独のネームサービスのためだけでなく，一方のネームサービスでアクセス許可になれば，他方のネームサービスでもアクセス許可にならなければならないものもある．例えば，LUS 管理の Jini サービスのアクセス許可が得られるのであれば，Jini サービス URL 中のホストにもアクセスする許可（DNS の名前解決許可）がなくてはならない．このように，関連するアクセス制御であれば，個々のネームサービスごとにアクセス制御情報を管理するより，統合したほうがネームサービス間のアクセス制御情報に矛盾が生じることを防ぐことができる．統合は，プラグ＆プレイでアクセス制御情報が集約される Kerberos KDC において実施される．

先の例のように，DNS と LUS ではアクセス制御が階層的であり，LUS でアクセスが許可される Jini サービスのあるホストは，DNS でもアクセスが許可されねばならない．そこで，アクセス制御情報の記述を入れ子状にし，LUS のアクセス制御情報を，DNS のアクセス制御情報で包含する記述で統合することとした．（**図** 3参照）

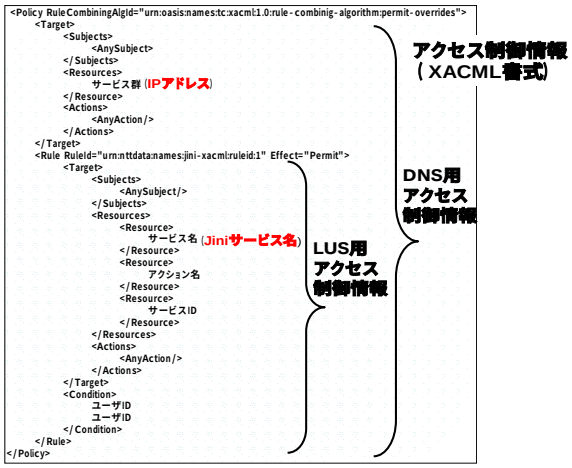

図 3 複数ネームサーバ用の統合アクセス制御情報

これにより，包含されたアクセス制御情報（LUS 用）の条件マッチングで許可となった場合に，その上位で包含するアクセス制御情報（DNS）でも許可になる記述となり，関連するネームサービス間で統合されたアクセス制御リストが表記されたこととなる．さらに，統合の動作を考える場合，この表記であれば，アクセス制御情報が別々に Kerberos KDC へ送信されても，それぞれの関連を検出し，自動的に統合させることができる．

5. まとめ

プラグ＆プレイ対応のアクセス制御として，ネームサービスへのサービス登録や削除と同時に，ネームサービスのアクセス制御情報も自動的に登録と削除をする方式の提案を行った．さらに，ネームサービス間で関連するアクセス制御情報は，自動的に統合させて管理できる表記方法の提案を行った．今後は，提案したプラグ＆プレイ対応アクセス制御を実装し，運用性について検証する予定である．

謝辞

本研究は，通信･放送機構(TAO)の委託研究テーマである「次世代 DNS に関する研究開発」の一環として行われているものです．

[参考文献]

[1] 情報家電向けネームサービスにおけるアクセス制御の一検討，日下貴義 他，第 65 回情報処理学会全国大会
[2] RFC1034,Domain names concepts and facilities, 1987.
[3] RFC1035,Domain names implementation and specification. 1987.
[4] Java Information Network Infrastructure, http://www. jini. org/
[5] RFC1510, ”Kerberos Network Authentication Service(V5)”,1993.
[6] Organization for the Advancement of Structured Information Standards, http://www.oasis-open.org/home/index.php