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　馬場 達也　山岡 正輝　松田 栄之
㈱NTT データ 技術開発本部
e-mail: {kusakat, babatt, yamaokam, 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, 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指定できる物理的位置情報を提供するものである. インターネットにおけるネームサービスは DNS (Domain Name System)[1][2]であり, ホスト名から IP アドレスを検索 (名前解決)するために利用される. 情報家電向けプロトコルのひとつである Jini [3]において, ネームサービスは LUS (Lookup Service) と呼ばれ, サービス名からサービス内容である遠隔手続き呼び出しの Java RMI スタブと接続先 URL を提供する. これらのネームサービスは, どのユーザからであっても, サービス検索や IP アドレス検索の問い合わせに対して無制限に回答する仕組みになっている. 特に, 家電がインターネットから接続できる環境では, 誰にでも自宅の家電が提供するサービス内容や IP アドレスを知ることができることを意味している. このことは, 不正アクセスに利用されることとなり, セキュリティ上問題と考えられる.

そこで, 本稿では, ネームサービスへの問い合わせ元に対して認証を行い, 認証結果によってサービスへのアクセス制御を実施することを提案する. さらにネームサービス間における認証情報を共有することによるユーザ利便性の向上と, 異なるネームサービスでそれぞれアクセス制御を行うことによる, ネームサービス全体のセキュリティ向上を図ることを提案する.

2. ネームサービスのセキュリティ対策

インターネット上で, Jini による情報家電ネットワークの利用を想定する. ユーザは情報家電の提供サービスを利用するとき, まず LUS を使って Jini サービスの位置情報 (URL)の検索を行う. 得られた URL から, 次に DNS を使ってサービスの IP アドレスを検索する. 最後に, 以上の URL と IP アドレスをもって, ユーザはサービスへアクセスできる. (図 1)

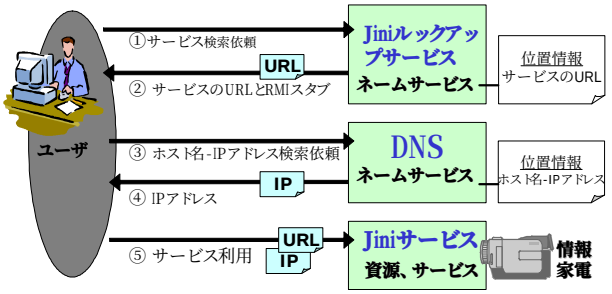

図 1 情報家電へのアクセス手順

情報家電は, グローバルなアドレスによる外部アクセスや, プラグ&プレイによる動的なアドレス割当てと動的サービス登録が求められる. 一方で, 家電所有者が家電の位置情報を隠蔽したり, 利用者によってアクセスを制限したりすることがセキュリティ上望まれる. その対応策として, DNS の代表的実装である BIND では, 問い合わせ元の IP アドレスを識別し, ゾーン情報単位でアクセス制御を実現している. しかし, この方法では, 問い合わせ元アドレスが動的に割当てされている場合や, アドレスのなりすましに対抗できない. 追加の対策として, ユーザ名や問い合わせ元 IP アドレスに対し, DNS のゾーン情報中のリソースレコード単位でアクセス制御する提案[4]を行ったが, ネームサービス全体に適用できるものではなく, DNS 以外のネームサービスは考慮されていない. LUS では, 問い合わせ元に対する回答可否の制限は行わず, アクセス先の資源自身においてアクセス制御がなされることを前提にしているのみであり, LUS がアクセス制御に関わることはない.

そこで, それぞれのネームサービスで問い合わせ元ユーザを認証し, 認証結果によって DNS のリソースレコードや Jini サービスのアクセス制御を行う方式を提案し, ネームサービス全体のセキュリティ向上を図る. しかし, ネームサービスごとに認証やアクセス制御を実施することはセキュリティを向上させる半面, 一つのサービスに対して何度も認証作業が必要になるなど, ユーザに冗長な作業を要求することになる. そこで, 同一ユーザが, 認証を必要とする複数のネームサービスに検索を依頼したとき, 一度の認証で検索が実行できるように, シングルサインオンによるネームサービス間の連携方

A study of access control on name services for information appliances
Takayoshi KUSAKA, Tatsuya BABA, Masaki YAMAOKA, and Shigeyuki MATSUDA,
Research and Development Headquarters, NTT DATA CORPORATION

式を，併せて提案する．

3. ネームサービスの認証とアクセス制御方式の提案

ユーザ名を用いてDNSとLUSで問い合わせ元を認証する．さらに，両ネームサービス間の認証情報をシングルサインオンで連携する．次に，認証結果に基づいて，DNSのリソースレコードやLUSのリモートオブジェクト(Jini サービス)単位に，アクセス制御を可能にする．以上の方式を提案し，実装を行った．

3.1. シングルサインオンにより連携された認証方式

DNSとLUSに，ユーザ名による認証機能を実装した．両ネームサービスにそれぞれ認証機能を持たせると，1回のサービス要求につき，2回のネームサービスによる認証が必要になる．2 回の認証作業は，ユーザにとって冗長であるので，認証情報を共有するシングルサインオンを適用し，ユーザの認証作業が1回で済むようにした．シングルサインオンの仕組みには，代表的なKerberos認証方式[5]を使用した．

ユーザ認証方式（図 2）は，ユーザからの問い合わせにユーザ名とパスワードを与えるようにし，DNS やLUS とは分離された KDC（Key Distribution Center, Kerberos 認証サーバ）によって認証を行うものである．認証に成功すれば，各ネームサービスは問い合わせに対して回答を行い，さらに，KDCより証明証が発行され，ユーザは証明証をユーザ名とパスワードの代わりに使うことができる．

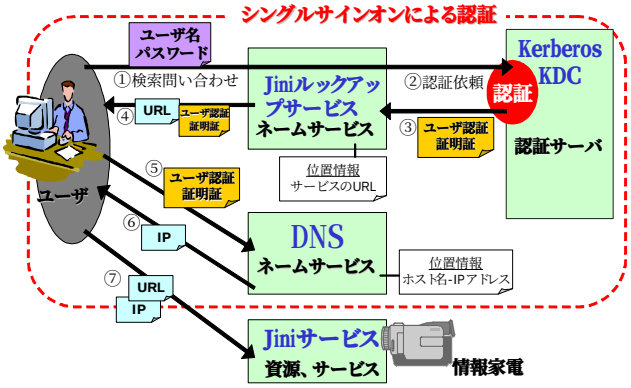

図 2 認証処理概要

DNSとLUSに，ユーザ名による認証機能を持たせることで，情報家電の所有者は，特定の利用者に対してのみ，その位置情報を知らせるように対処できる．さらに，認証をシングルサインオン化することで，認証作業（ユーザ名とパスワードの入力作業）を省力化し，ユーザの利便性向上が図られる．

3.2. サービス利用許可証によるアクセス制御方式

認証の結果，特定ユーザのみにアクセスを許可するアクセス制御方式（図 3）を実装した．アクセス制御機能はKDCに持たせ，ネームサービスは，KDCへ認証を依頼すると同時に，ユーザが要求しているサービスを通知する．KDC は，認証に成功すると，アクセス制御リストを参照することにより該当ユーザが要求しているサービスの許可の可否を判断し，許可であればサービス利用の許可証を発行する．ネームサービスは，許可証を受け取ることで，ユーザへ位置情報を通知するとともに，許可証も中継して送信する．

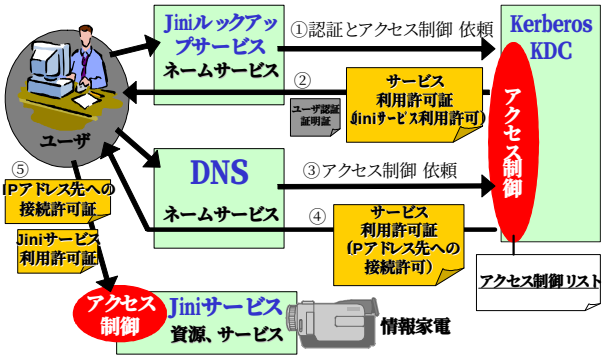

図 3 アクセス制御処理概要

ネームサービスを介したKDCによる認証とアクセス制御の結果，サービスの位置情報と許可証を得ることができたユーザは，位置情報を使ってサービスへアクセスするとき，許可証も提示する．サービスは，許可証が正しいものかを判定することのみで，ユーザの認証と自身へのアクセス制御に代替することができる．

以上により，ネームサービスが管理するサービス名（資源名）の位置情報通知可否に関するアクセス制御と，サービス自身によるアクセス制御が実現される．従来のサービス自身によるアクセス制御に加え，異なるネームサービスでアクセス制御を行うことにより，システム全体の統一したセキュリティ向上が実現される．

4. まとめ

ネームサービスへの問い合わせ元を，ユーザ単位で認証し，認証情報をネームサービス間で共有させる方式，および，認証結果に基づいて，ネームサービスが管理する資源やサービスの位置情報の通知可否を判断するネームサービスでのアクセス制御方式を提案し，実装した．今後は，情報家電のプラグ＆プレイ機能を想定し，アクセス制御情報のプラグ&プレイ対応を検討する予定である．

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] RFC1034,Domain names concepts and facilities, 1987.
[2] RFC1035,Domain names implementation and specification. 1987.
[3] Java Information Network Infrastructure, http://www. jini. org/
[4] DNSにおけるアクセス制御の一検討, 山岡正輝 他, 第64回情報処理学会全国大会
[5] RFC1510, "Kerberos Network Authentication Service(V5)",1993.