

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実装

日下 貴義 馬場 達也 山岡 正輝 松田 栄之

(株)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、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前で管理し、それらへアクセスするための物理的位置情報を提供するもの(名前解決)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、名前解決の際、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のアクセス制御を実施することを提案した[1]。さらに、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]と、情報家電向けプロトコルのひとつ Jini[3]におけるネームサービスであるLUS(Lookup Service)に、アクセス制御機能と、シングルサインオンによってアクセス制御を連携する実装を行った[4]。また、アクセス制御機能を情報家電で求められるプラグ&プレイ機能に対応させ、運用性の向上に関する検討を行った[5]。本稿では、検討結果からの実装と、評価結果について述べる。

2. プラグ&プレイ対応アクセス制御の実装

複数のネームサービスの名前解決におけるアクセス制御連携機能の実装[4]を拡張し、サービスのアクセス制御情報のプラグ&プレイ機能[5]を実装した。実装の概要を図1に示す。この実装により、プラグ&プレイ対応アクセス制御機能として以下の動作が確認された。

情報家電サービスを、ネットワークへ新規にプラグ&プレイで提供するとき、同時にネームサービス内で、情報家電サービスに対応するアクセス制御情報も、自動的に登録や削除される機能の動作。特に、サービス消滅検知においては、リース間隔(サービスの登録を維持する時間)が短く設定できることにより実現し、機敏な削除となるよう工夫した。

アクセス制御機能上(本実装では、Kerberos シス

テムを活用)において、複数のネームサービスにまたがってプラグ&プレイによって登録される同一サービスのアクセス制御情報を自動的に統合する機能の動作。

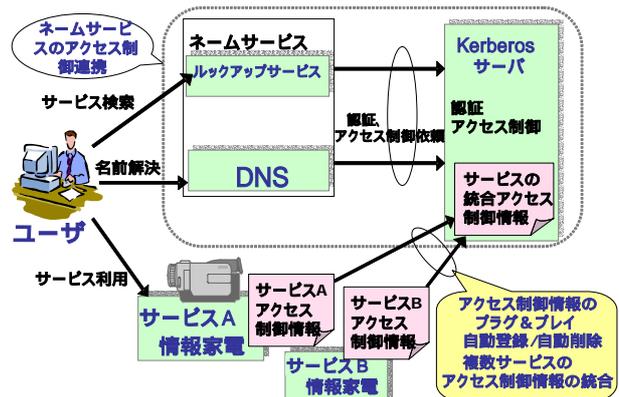


図1 実装の概要

以上、サービスの出現と消滅にあわせ、ネームサービスのアクセス制御情報の自動登録と自動削除、ネームサービス間で共有するアクセス制御情報の自動統合ができることから、アクセス制御においてもプラグ&プレイの利便性を損ねることがないことを確認した。

3. 運用性への影響の評価

本研究において、ネームサービスが管理する情報には、情報家電などのサービス名と位置情報の対応という従来の管理情報以外に、アクセス制御用の情報としてユーザ名と許可サービスの対応が追加されている。これらアクセス制御用の情報分だけ、従来のプラグ&プレイに比べ、サービス登録、削除、実行の処理に追加動作が発生する。これまで、ネームサービスに対し、アクセス制御対応によるセキュリティの向上と、プラグ&プレイ対応による利便性の向上を図ってきたが、追加動作によってシステムに負荷を与えては、運用性が維持できているとはいえない。そこで、プラグ&プレイ対応アクセス制御が、運用性に対して与える影響について、サービスの管理規模に注目し評価を行った。

3.1. 評価の内容と結果

サービスの登録、削除、実行それぞれの動作において、従来の動作と異なる点を明らかにし、動作完了までの時間を測定した。評価環境は図1にならって構成し、各構成機器のスペックは表1のとおりである。

表 1 評価環境で使用した機器

| | | |
|--------------------------|--|---|
| 構成機器名 (すべて PC で構成) | Kerberos サーバ, DNS, LUS, Web AP サーバ (ユー ザ側機器) | ユーザ 端末 (ユーザ側機器), 情報家電 (PC により仮想的 に構成) |
| OS | Red Hat Linux 9 (Kernel 2.4.20) | Windows 2000 |
| CPU | Intel Pentium 4 (2.53GHz) | |
| Memory | 1GB | |

(1) サービスの登録と削除

ネームサービスにおけるサービスの登録と削除に関して、アクセス制御に対応したプラグ & プレイと、従来のプラグ & プレイとで異なる点を、以下に示す。

サービス登録の場合

サービスの持つアクセス制御情報は、起動されると同時にネームサービスへ送信されることによって統合アクセス制御リストに自動追加登録される。さらに、複数ネームサービスで管理される同一サービスのアクセス制御情報であれば、ネームサービス間の管理情報の包含関係を反映して階層的にマージされ、統合アクセス制御リストを作成する。

サービス削除の場合

ネームサービスによってサービス停止を検知させ、同時に統合アクセス制御情報を検索し、該当するサービスのアクセス制御情報を抽出して削除する。

同時に登録または削除されるサービスの数を 10 とし、プラグ & プレイによるサービス登録速度とサービス削除時間を測定した。測定結果を表 2 に示す。

表 2 サービス登録・削除速度

| 測定環境 | アクセス制御なし | アクセス制御あり |
|---------|----------|----------|
| 登録時間(秒) | 3.00 | 31.0 |
| 削除時間(秒) | 287 | 17.0 |

それぞれ 10 回測定時の平均値、有効数字三桁とする

(2) サービスの実行

サービスの実行において、ネームサービスにおけるアクセス制御対応の有無による相違点は、サービスを実行するときに Kerberos を使ったユーザ認証とアクセス制御が実施されるかどうかである。

PC により作成した擬似的な情報家電サービスの実行時間を測定した。測定結果を表 3 に示す。

表 3 サービス実行速度

| 測定環境 | アクセス制御なし | アクセス制御あり |
|---------|----------|----------|
| 実行時間(秒) | 0.213 | 1.69 |

それぞれ 10 回測定時の平均値、有効数字三桁とする

3.2. 考察

サービスの登録・削除速度の測定結果により、アクセス制御情報のプラグ & プレイ対応がある場合は、ない場合に比べて、削除時間では実装の工夫により改善が見られたものの、登録時間は 10 倍程度の劣化が見られる。これは主に、Kerberos サーバへアクセス制御用の情報を登録する際に時間がかかっているためであ

る。同時にサービス登録されることが頻繁に繰り返されるような利用環境であれば、プラグ & プレイのための登録時間は著しく増大し、本システムが運用できる管理規模は低いといえる。しかし、本システムが対象としている、家庭内における情報家電の利用程度であれば、数十の家電が一斉に電源のオン・オフを繰り返すような状況は想定しにくい。多数のサービスが同時登録を頻繁に実施しない家庭内程度の利用環境であれば、運用できる規模は管理可能な範囲と考えられる。

また、サービスの実行速度の測定結果により、アクセス制御がない場合に比べてアクセス制御がある場合は、実行速度にしてほぼ 8 倍程度の劣化が見られる。相対的には大きく劣化しているが、劣化しても 2 秒以下の実行時間であることから、家庭内で提供するサービスの実行時間としては、ユーザにとって著しいレスポンスの低下とは考えにくい。ただし、同時にサービスの実行を要求したときは、急速にレスポンス時間が増大すると予想される。しかし、家庭内利用であれば、同時要求が数十に及びことは考えにくく、また、同時要求の排他制御により早い実行順番が獲得できない場合でも、ミッションクリティカルなものを優先し、それ以外は再アクセスを促すといった運用による対処が可能である。

以上から、情報家電などの家庭内利用に管理規模を限定すれば、プラグ & プレイ対応のアクセス制御がある場合でも、運用性は維持できると考えられる。

4. まとめ

プラグ & プレイ対応のアクセス制御として、ネームサービス間で関連するアクセス制御情報を統合して管理し、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実装を行った。さらに、運用性としてサービスの管理規模に注目し、本システムで想定するような家庭内における情報家電利用に対しては十分であるとの仮説を立てた。

今後は、情報家電サービスが複数存在する環境での運用を検証するとともに、独立したネームサービスが存在しない Peer to Peer ネットワークにおけるプラグ & プレイ対応アクセス制御について検討したい。

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] 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
 [2] RFC1035, Domain names implementation and specification, RFC1034, Domain names concepts and facilities, 1987.
 [3] Java Information Network Infrastructure, <http://www.jini.org/>
 [4] 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
 [5] 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, 日下貴義 他, 第 2 回情報科学技術フォーラム