

Home P2P Networkにおける 複数ユーザのアクセスコントロール

鈴木 尚宏[†] , 萩野 達也^{††}

[†] 慶應義塾大学大学院 政策・メディア研究科

E-mail: nao@tom.sfc.keio.ac.jp

^{††} 慶應義塾大学 環境情報学部

E-mail: hagino@tom.sfc.keio.ac.jp

概要

本論文では人間関係の情報を利用してホームネットワークのアクセスコントロールを実現するシステムを提案する。ホームネットワークのような小規模ネットワークにおけるアクセスコントロールは、「情報技術の知識を持っていない人も管理者となる」、「基本的にネットワークの利用は顔見知りに限られる」といった特徴を持っている。前者の特徴よりアクセスコントロールの設定を行う際、あまりに複雑な手順を必要としてはならない。また後者の特徴より、人間関係をアクセスコントロールに利用することができると考えられる。人間関係をアクセスコントロールに利用することにより、機器ごとに煩雑なアクセスコントロールの設定を行う負担を軽減する。

Access Control for Multiuser in Home P2P Network

Naohiro SUZUKI[†] Tatsuya HAGINO^{††}

[†] Graduate School of Media and Governance, Keio University

E-mail: nao@tom.sfc.keio.ac.jp

^{††} Faculty of Environmental Information, Keio University

E-mail: hagino@tom.sfc.keio.ac.jp

Abstract

In this paper, we propose an access control system for home network using human relationships. Access control of small-sized network like home network has aspects as below: a) average person who does not have technology literacy could be an administrator; b) acquaintances use only. Due to former reason, configuration of access control should be user-friendly. Latter reason suggests using human relationships for access control. Applying human relationships to access control, our system reduces complicated configuration of access controls.

1 背景

デジタル情報技術とネットワーク技術の発展により、デジタルホームネットワーク環境が整ってきている。この結果、パソコンや携帯電話を使用し、ネットワークを経由して、家庭内等の機器のサービスを利用する形態が生まれてきている。

本論文においてはホームネットワークは家庭内のネットワークだけでなく、大学の研究室のネットワーク等の小規模なネットワークを含む。現在、

家庭内や研究室内の機器はドアなどで隔たれた地理的にセキュリティが確保された場所でしか利用できないようにすることで、セキュリティを確保していた。ネットワークを経由することで、地理的に離れた場所から家庭内や研究室内の機器を利用できるようになった。これにより、家庭内や研究室内の機器に対して、地理的なセキュリティ以外で、セキュリティを確保する必要が生じてきた。さらに、ホームネットワークの機器に対してはあまり情報技術に詳しくないユーザが使用するこ

とを考慮する必要がある．単純な設定で十分なレベルのセキュリティを確保でき、また複雑な設定を行えば、より細かいレベルのセキュリティを確保できるのが理想的であると考えられる．

ホームネットワークの特徴として、お互い顔を知っているもの同士のみがユーザとなるネットワークであると考えられる．つまり顔見知りでない人に利用されることがホームネットワークの不正利用であるといえる．また顔見知りの中でも、ある機器を利用してよいユーザと利用してほしくないユーザに分けることが必要になると考えられる．

そこで、本論文では単純な設定で十分なレベルのセキュリティを確保し、ユーザごとにアクセスコントロールを設定できる手法として人間関係のデータを利用し、ホームネットワークのアクセスコントロールを行うシステムを提案する．

第2節では本論文におけるホームネットワークについて述べる．第3節では関連研究を交えつつ、ホームネットワークにおけるアクセスコントロールについて記述する．第4節ではこれらを踏まえ、本論文で提案するアクセスコントロールのモデルについて述べる．第5節ではそのモデルに従ったアクセスコントロールシステムを提案する．第6節では提案したアクセスコントロールシステムについてまとめる．

2 ホームネットワーク

本節では、ホームネットワークについて述べる．まずホームネットワークの特徴について記述し、次にホームネットワークの形態について記述する．最後に我々が想定するホームネットワークについて述べる．

2.1 特徴

本項では、ホームネットワークの特徴について述べる．4つのホームネットワークの特徴を挙げ、それぞれについて簡単に説明する．

機器の参加・離脱・状態変化が頻繁に発生

ホームネットワークでは、様々な種類の機器が存在する．そして、それらの機器は必ず長期間存在するのではなく、機器が取り外されたり、機器の電源を切ることが多く、機器の状態変化や参加・離脱が激しく起こる．そのため、ホームネットワークのエンドノードである機器を固定化することが難しく、また機器の状態を管理するための負荷が

高いネットワークであるといえる．

複数の管理者が存在

ホームネットワークでは、家族や同居者・友人などのユーザが存在し、そして、それぞれのユーザが自分用の機器を管理している．また自分用の機器のみではなく、共用の機器も存在する．これにより、ホームネットワークは1人の管理者が全てを管理してよいネットワークではなく、複数の管理者が協調して、複数の機器を管理する必要のあるネットワークであるといえる．例えば、父親が娘に使用させたくないデバイスが存在することも考えられるし、またはその逆の娘が父親に使用させたくないデバイスが存在することも考えられる．この時、ホームネットワーク全体の管理者としてしか管理者が設定できない場合、このような要求に答えることができない．

情報技術に詳しくないユーザが管理者として存在

ホームネットワークが普及した社会では全てのユーザが管理者となりうるため、情報技術に詳しくないユーザが管理者となることが考えられる．そのため、情報技術に詳しくないユーザでもアクセスコントロールの管理を行えるシステムが必要になる．

基本的に顔見知りを利用するネットワーク

ホームネットワークが利用される形態として家庭内や大学の研究室が考えられ、これらの場所ではお互い顔を知っているユーザが機器を利用している．そのため、顔を知らない(知り合いでない)ユーザがホームネットワークに接続されている機器を利用できないようにすることで、ホームネットワークにおける最も単純なアクセスコントロールが実現できると考えられる．

2.2 形態

本項ではホームネットワークの形態について述べる．ホームネットワークの形態として、中央管理型のホームネットワークとP2P型のホームネットワークの2種類が存在する．それぞれの概要について述べ、利点・欠点についても記述する．

中央管理型ホームネットワーク

中央管理型のホームネットワーク (Fig. 1) とは、一言で言えば全ての機器の管理を行っているサーバが存在するホームネットワークである．中央管理型ホームネットワークの利点として、1つのサー

バ内で全ての機器を管理するため、管理が容易になる点があげられる。しかし、中央管理型ホームネットワークの欠点として、管理をしているサーバがダウンしてしまった場合、全ての機器のサービスが利用できなくなること、またホームネットワークの機器は日々進化し続けるため、管理用のサーバに対応していない新しい機器がリリースされた場合、それを使用することができなくなるなどの管理用のサーバの制約が大きくなってしまいう点があげられる。



Fig. 1 中央管理型ホームネットワーク概要図

P2P 型のホームネットワーク

P2P 型のホームネットワーク (Fig. 2) とは、機器が Peer-to-Peer で繋がっているホームネットワークである [1]。P2P 型のホームネットワークを本論文では、Home P2P Network と呼ぶ。Home P2P Network の利点として、全てのデバイスを同列に扱うことができる点が上げられる。この利点により、1 つのデバイスが故障等により使用できなくなっても、他のデバイスに大きな影響を与えることなく、他のデバイスで提供されるサービスは使用できる。これに対し、中央管理型のホームネットワークでは管理サーバが故障などで使用できなくなってしまう場合、ホームネットワークの全てのサービスが利用できなくなってしまう。Home P2P Network の欠点として、各機器が集中管理されているのではなく、全ての機器が対等なノードとして、存在し、特別なノードが存在しないため、機器の集中管理を行うことができず、機器を管理することが困難となる点があげられる。

この欠点を解消するため、我々が想定している Home P2P Network では、各機器にエージェン

トである ASMA (Autonomous State Management Agent) を配置し、以下の情報を XML 形式で記述されたテキストで管理している [3][6]。

- デバイス
デバイスの情報、例えばプリンタの解像度、ディスプレイのサイズ等のスペック情報を管理する。また、管理者ユーザの情報を持つデバイスの位置も管理する。
- サービス
デバイスで提供されるサービスの情報、例えば必要な入力データ形式や出力データ形式等を管理する。また、サービスを使用するために必要な信頼度も管理する。

このような情報を ASMA が相互にやり取りすることで、Home P2P Network の管理を行う。



Fig. 2 Home P2P Network 概要図

2.3 想定するホームネットワーク

ホームネットワークではデバイスの電源 ON・OFF 等の状態の変化が起こりやすく、全てを中央管理サーバで管理を行うと中央管理サーバに負荷が集中してしまう。また中央管理サーバが故障や設定ミス等で正常に動作しなくなった場合、その影響によりホームネットワークの全てのサービスが使用できなくなることが考えられる。このため、中央管理サーバに設定変更をするのは心理的負担が増大すると考えられる。Home P2P Network では個々の機器に対して様々な設定を行うので、設

定ミスをしてそのミスをした機器の問題のみとなる。以上の理由により、中央管理型のホームネットワークは不相当であると考え、本論文では Home P2P Network を選択する。

3 関連研究

本節ではホームネットワークのアクセスコントロールに関する関連研究について述べる。Kim は [4] の手法でホームネットワークにおけるアクセスコントロールを実現している。この手法は中央管理型のホームネットワークにおいて、管理サーバがユーザー一覧を管理していて、そのユーザーそれぞれに対し、父・母といった役割を割り当てる。その役割にそれぞれのデバイスを許可することでホームネットワークにおけるアクセスコントロールを可能にする。しかし、この方法ではデバイスごとに許可・不許可を決定しなくてはならないため、デバイスが増減しやすいホームネットワークでは役割とデバイスの対応表を管理するのに手間がかかってしまう。

Dimitris は [5] の手法でアクセスコントロールを実現している。この手法は個々のデバイスにセキュリティポリシーを適用することで、ホームネットワークのアクセスコントロールを実現する。ユーザーが自分のプロフィールを持ち、その情報をホームネットワークに参加しているデバイスに送信し、デバイスが保持しているポリシーと比較して、設定されたセキュリティポリシーを満たす場合にデバイスが使用可能となり、アクセスコントロールを実現している。デバイスごとにポリシーを適用するため、デバイスが P2P 形式で接続される Home P2P Network と相性が良いと考えられている。しかしこの手法ではデバイスのアクセス管理を行う際に、デバイスごとにユーザを管理する必要が生じるため、セキュリティを確保するための手間が大きくなってしまう。

4 提案するシステム

本節では、提案するアクセスコントロールシステムについて述べる。

4.1 モデル

本項では、本論文で提案するアクセスコントロールモデルについて述べる。提案するアクセスコントロールモデルの基本として、人間関係の情報を利用する。人間関係の情報からホームネットワー

クを利用するユーザの情報を引き出し、認証を行う。人間関係の情報を利用することにより、ホームネットワークの「基本的に顔見知りしか利用しない」という特徴を活かすことができ、デバイス 1 つ 1 つに使用するユーザのアクセスコントロールリストを記述する必要がなくなる。また友人が家に訪問してきたときホームネットワーク内に存在する機器を使用させてあげるために、逐一アクセスコントロールの設定をする必要がほとんどなくなる。

4.2 人間関係

本項では、提案するシステムで利用する人間関係のデータについて述べる。人間関係を表すデータとしては、FOAF を利用する [2]。FOAF とは、Friend-Of-A-Friend の略で、友達の友達の友達... という連鎖をメタデータとしての表現する RDF である。FOAF を利用して、ネットワーク上の興味深い属性や関係を、ASMA を用いて分析することにより、新しいサービスを提供することができるのではないかと期待されている。

次に我々が想定する Home P2P Network においてアクセスコントロールを実現するための FOAF の拡張について、説明する。Home P2P Network 内で FOAF を利用するために、FOAF の拡張を行う。拡張として、FOAF に追加する語彙は以下の通りである。また追加する語彙の名前空間は asma とする。

- trustlevel
trustlevel は人のホームネットワークにおける信頼度を数字で表すタグとして使用する。信頼度は 0 を基準として、表 1 のように信頼度を定義する。
- relation
relation は知り合いとの関係を表す語彙として使用する。例えば、家族関係・友人関係等を記述する。以下の語彙を使用して記述する。
 - name: 関係の名称を記述する。
 - whose: どのユーザにとっての関係であるかを記述する。

上記 2 つの語彙を拡張した FOAF の例を Fig.3 に示す。

信頼度	数値
完全に信用する	3
ほとんど信用する	2
少しだけ信用する	1
基準値	0
少し信用しない	-1
ほとんど信用しない	-2
まったく信用しない	-3

Table 1 信頼レベル

```

<rdf:RDF ...>
  <foaf:Person rdf:ID="me">
    <foaf:name>My Name</foaf:name>
    <foaf:mbox_sha1sum>
      My Mail Address Hash
    </foaf:mbox_sha1sum>
    <foaf:knows>
      <foaf:Person>
        <foaf:name>Name</foaf:name>
        <foaf:mbox_sha1sum>
          Mail Address Hash
        </foaf:mbox_sha1sum>
        <asma:trustlevel>
          3
        </asma:trustlevel>
        <asma:relation>
          <asma:name>family</asma:name>
          <asma:whose
            rdf:resource="#me" />
          </asma:relation>
        </foaf:Person>
      </foaf:knows>
    </foaf:Person>
  </rdf:RDF>

```

Fig. 3 拡張 FOAF ・例

4.3 FOAF 拡張の仕組み

他人からその人を表す拡張した FOAF 情報を送信してもらう。そして、その FOAF 情報と自分の持っている FOAF 情報をマージすることにより、FOAF 情報の拡張を進めていく (Fig. 4)。このように FOAF 情報の交換を繰り返していくことにより、ユーザが持っている FOAF 情報に知り合いの FOAF 情報を追加していく。



Fig. 4 FOAF 交換図

4.4 アクセスコントロール手順

本項では、拡張した FOAF データを利用して行うアクセスコントロール手順について述べる。

アクセスコントロールは以下の手順で実現する。

1. FOAF 情報を利用したいデバイスに送信

まず FOAF 情報を管理している端末、例えば携帯電話などから自分の FOAF 情報を利用したいデバイスに送信する。

2. デバイスの ASMA が FOAF 情報を受信

デバイスの ASMA が送られてきた FOAF 情報を受信して、利用しようとしているユーザを把握する。このデバイスが管理者の FOAF 情報を管理しているデバイスであった場合、この時点で管理者として認証される。

3. 管理者の FOAF 情報を管理しているデバイスに管理者の FOAF 情報を要求

利用しようとしているユーザの把握後、ASMA は管理者ユーザの FOAF を管理しているデバイスに管理者の FOAF 情報を要求命令を送信する。この時点で管理者の FOAF 情報を管理しているデバイスが Home P2P Network 上に存在しなかった場合、ユーザはデバイスを利用

用することができない。これはたとえ、顔を知っている人であっても、管理者が把握していないときにデバイスの利用を不可能にするためである。

4. 知人の信頼レベルとサービスの信頼レベルの比較

管理者の FOAF 情報に利用しようとしているユーザの情報が存在した場合、そのユーザが管理者の知り合いであると判断する。そして、利用しようとしているサービスの情報から必要な信頼度と関係の条件を取得し、管理者の FOAF 情報のユーザ部分と比較する。条件が成立した場合、サービスが利用可能となる。

このアクセスコントロール手法により、管理者が顔を知らない人のホームネットワークのサービスを使用不可能にすることができる。また管理者の FOAF 情報を持つデバイスがホームネットワークに参加していない場合は顔見知りの人でもホームネットワークのサービスを使用不可能にすることができる。その結果、Home P2P Network のアクセスコントロールが可能になり、Home P2P Network で提供されているサービスが不正に利用されるリスクを軽減することができる。

4.5 具体例

本項では提案したアクセスコントロール手法を用いて、具体的にアクセスコントロールを行う手順について記述する。ユーザ認証におけるシナリオは「ユーザ A の家にユーザ B がデジカメを持ってやってきた。そのデジカメの写真をユーザ A の持つ液晶ディスプレイに写したい」とする。またユーザ A とユーザ B は知り合いとする。知り合いとはつまり既に FOAF 情報の交換が済んでいて、お互いの FOAF 情報を保持していることをさす。そして、液晶ディスプレイに表示するサービスを利用するために必要な信頼度は 1 で、ユーザ A におけるユーザ B の信頼度は 2 である。

以下のステップを辿り、ユーザ認証を行うことでシナリオを実現する。

1. ユーザ B が管理しているデジカメのデータをユーザ A が管理している液晶ディスプレイに送信するため、デジカメとユーザ B の FOAF

情報を管理している携帯電話をディスプレイと同じ Home P2P Network に参加させる。同じ Home P2P Network に接続されると、Fig.5 の形態となる。

2. ユーザ B の FOAF 情報を管理している携帯電話などのデバイスからデジカメに向けてユーザ B の FOAF 情報を送信する。
3. デジカメはユーザ B の FOAF データを受け取り、データの送信先から管理者ユーザの FOAF 情報を管理しているデバイスから送信されたことが判明したので、管理者としてサービスの利用許可を出す。
4. デジカメはそのままユーザ B の FOAF 情報を液晶ディスプレイに向けて送信する。
5. 液晶ディスプレイはユーザ B の FOAF データを受け取り、管理者ユーザ A の FOAF データを探し、発見した場合、そのデバイスからユーザ A の FOAF 情報を受信する。
6. ユーザ A の FOAF データを受け取り、分析した結果ユーザ B が知り合いであると判明する。また液晶ディスプレイを使用するための trustlevel を超えていたため、液晶ディスプレイが使用可能となる

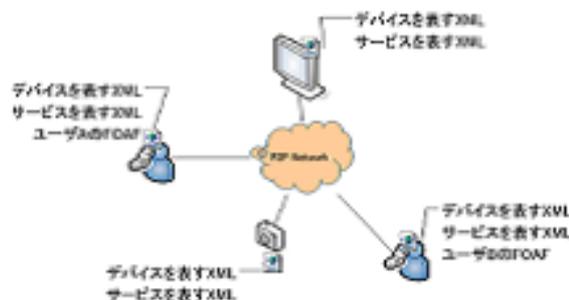


Fig. 5 Home P2P Network 例

5 おわりに

本論文では、Home P2P Network における人間関係を利用した認証機構を提案した。人間関係を表現するデータとして、FOAF を拡張したものを利用する。これにより、複雑な設定をしなくても基本的なアクセスコントロールシステムの実現を

可能とした。また他人が記述した FOAF 情報を交換することで、アクセスコントロールの元とするユーザデータ等を全て管理者が記述する必要がなくなり、管理者の負担を軽減することができる。そしてデバイスごとに異なる管理者を設定できるため、複数の管理者が共存してホームネットワークを管理することが可能となる。

今後の課題として、送られてきた FOAF データの正当性保証を行っていないため、なりすましを防ぐことはできない点があげられる。この問題を解決するために、FOAF データの正当性を保証する PGP 等の仕組みの導入を検討している。また、FOAF に単純な信頼度を表す語彙と関係を表す語彙の拡張のみ行ったため、単純な認証を行うことしかできない。現在、基本的な認証機構は用意することができたが、ホームネットワークを利用するには、もう少し複雑なアクセスコントロールが求められる場合も考えられる。単純なアクセスコントロールシステムを継承しつつ、複雑なアクセスコントロールを適用できるようにするための FOAF の拡張方法について検討し、評価する。

参考文献

- [1] Kitagawa Kazuhiro, Saito Nobuo, Shimizu Noritada and Kato Fumihiro: “A Framework for Descriptions and Reasoning for Adaptive Composite Service Structure and Behavior”, The International Workshop on Cyberspace Technologies and Societies 2005, Feb. 2005
- [2] The Friend of a Friend (FOAF) project, <http://www.foaf-project.org/>
- [3] 鈴木 尚宏, 清水 智公, 加藤 文彦, 北川 和彦: “AV 機器状態通知エージェントの設計と実装”, 情報処理学会 第 67 回全国大会, Mar. 2005
- [4] Do-Woo Kim, Geon Woo Kim, Jun-Ho Lee, and Jong-Wook Han: “Role-based Access Control Model in Home Network Environments”, 2005 WORLD ENFORMATIKA SOCIETY p97-99, 2005
- [5] Dimitris M. Kyriazanos, George I. Stassinopoulos: “Ubiquitous Access Control and Policy Management in Personal Networks”, International Workshop on Ubiquitous Access Control, 2006
- [6] Shimizu Noritada, Kitagawa Kazuhiro, Wan Haoyi, Ishikawa Norihiro and Hjelm Johan: “A Device and Service Description Framework for