2003－DSM－29 (9)
2003／4／25

信頼の輪モデルに基づいた システム利用権限の委譲による個人認証手法

正岡 元, 菊池 豊

高知工科大学大学院 工学研究科 基盤工学専攻 情報システム工学コース

概要

信頼の輪は、個人と個人との信頼関係が複数存在する際に、それらの合成によって構築される個人認証モデルである。本研究では、この信頼の輪をもとにしてシステムにおける利用権限をユーザに委譲することにより、個人認証を行う手法を提案する。

システムにおけるユーザの権限は、そのシステムの管理者が委譲するのが一般的である。NIS などの管理システムを導入した場合でも、NIS 管理者の権限によって、ユーザへの権限委譲が行われる。これらの管理手法では、管理コストが管理者に集中してしまう。

本提案では、従来の管理手法に信頼の輪モデルを導入することで、既に権限を持っているユーザの信頼に基づいて、一部あるいは全部の権限をユーザに与える手法を実現する。この場合管理者がユーザに直接権限を委譲する必要は無く、これにより従来管理者に集中していた管理コストを分散でき、管理者の負担を軽減することが可能となる。

A Person Authentication Method using Authority Delegation Based on the Web of Trust Model

MASAOKA Hajime, KIKUCHI Yutaka

Information Systems Engineering Course, Department of Engineering,
Graduate School of Engineering, Kochi University of Technology

Abstract

The web of trust is a model that composed of trust relations among users. This research proposes a person authentication method using authority delegation based on the web of trust.

It is usual that system administrator gives system using authority to users. therefore the administration cost is concentrated on the administrator.

This proposal introduces the web of trust model to the conventional administration method. The method is based on trust of the user who already has authority. And the method gives a user a part of the system using authority.

1　はじめに

信頼の輪は、個人と個人との信頼関係が複数存在する際に、それらの合成によって構築される個人認証のモデルである。本研究では、この信頼の輪モデルを基にしてシステムにおける利用権限をユーザに委譲することによって個人認証を行う手法を提案する。

従来のユーザ管理手法では、システムの利用権限はそのシステムの管理者がユーザに対して委譲することが一般的である。そのため、管理コストが管理者に集中してしまう。この管理コストは、ユーザの数やシステムの数にあわせて増加する。さらに従来の手法では、個々のユーザに対して与える権限の制限を、細かく行うことは困難であった。

本研究では、従来の管理手法に信頼の輪モデルを導入することで、既にシステムの利用権限を持っているユーザの信頼に基づいて、一部、あるいは全部の権限をあらたなユーザに与える手法を実現する。この場合管理者はユーザに直接権限を委譲する必要は無い。そのため、管理コストを分散させることが可能であり、管理者の負担を軽減することが可能となる。

2　信頼の構造

本研究における認証手法は信頼関係をベースにしている。本節では、この信頼の構造について述べる。まず一対一の信頼関係が構築されることを述べ、さらに複数の信頼関係が結合して拡張されることを示す。

2.1　信頼の定義

ノードが他のノードを信頼する関係を想定する。ここでノードとはシステムやユーザを含め、認証やシステムの利用の主体となるものの総称として使用する。ここで言う信頼とは、システムの利用権限を相手に与えてもよいと信頼の主体の責任において認める行為である。

信頼されたノードは、そのシステムにおいて、ある程度の利用権限を得ることができる。得られる権限の度合いは、信頼する主体が元々持っている権限と、信頼度によって決定される。この定義によれば、システムにおける一般的なユーザ登録は、システム管理者が一般ユーザを信頼する行為と捉えることが可能である。

2.2　信頼関係の構築

信頼する側は、信頼されるノードがシステムに被害を与えた場合に責任を負う可能性があり、不用意に信頼することが自分にとって不利益である事を知っている。そのため、ノードが信頼するに値するかどうかを判断した上で信頼する。また信頼される側は、自分が不利益を被らないためにも、自分を信頼している管理者を裏切らないように行動することになる。

しかしシステムにおけるコミュニティが大きくなると、管理者は直接知らない人物に対して権限を与えなければならない場合が出てくる。その場合、このような信頼関係によるユーザアカウントの発行は難しくなる。この問題を解決するために、信頼の判断を他人に委ねると言う方法を考える。この方法について次節以降に述べる。

2.3　信頼の結合

ノード同士は信頼関係を作ることができる。複数の信頼関係が結合することにより、より複雑な構造を持つようになる。この構造には網構造と木構造とがあり、それぞれ第 2.4 節と第 2.5 節にて詳細に述べる。これらの信頼の構造によって、直接知らないノードを間接的に信頼することができる。

2.4　信頼の網構造

第 2.3 節に述べた信頼関係の構造である網構造と木構造について、特徴を述べる。

まず、網構造を図 1 に示す。図中の矢印は根元の人物が先の人物を信頼している状態を示す。網構造では、信頼関係は一方向と双方向とがある。A と B との信頼関係は双方向であり、B と D とは一方向である。この、網構造を持つ信頼の集まりを、信頼の輪 (Web of Trust) と呼ぶ。信頼の網構

造の代表例として OpenPGP[2][1] (以下 PGP と表記) における鍵リングがあげられる。

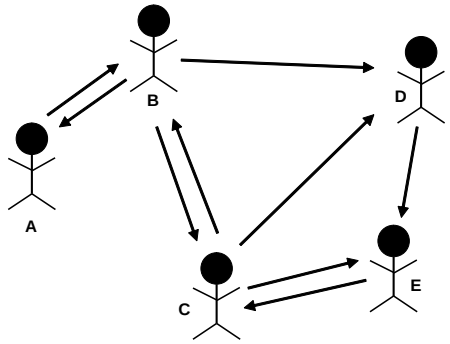

図 1: 信頼の網構造

網構造には、第 3 者機関を必要とせずに信頼関係を結合できる利点がある。しかし、個人同士の信頼関係によってしか任意の人物を評価できないという欠点もある。

2.5 信頼の木構造

木構造では、頂点から末端への一方向に信頼関係が構築される。木構造は PKI[1][3] のモデルとして利用されている。PKI においてノードは認証機関 (CA) であり、頂点の CA を特に Root CA と呼ぶ。この状態を図 2 に示す。

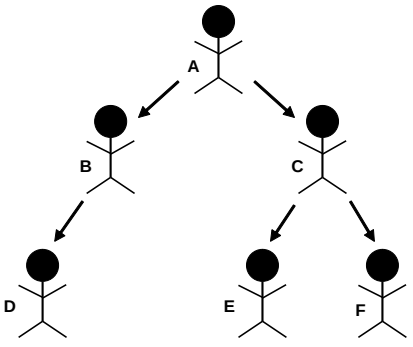

図 2: 信頼の木構造

木構造では、Root CA が認証の規準を持つため、統一的な判断ができる。しかし、Root CA を用意する必要があることや、Root CA を信頼できない場合は全体を信頼できない、という欠点がある。

さらに、Root CA は木構造全体に責任を負うため、Root CA の運用コストが高くなる、という欠点がある。

2.5.1 P2P モデル

信頼の木構造の特殊な形態として、ピア・ツー・ピア (P2P) モデルがある。複数の CA は互いに信頼しあい、対等の関係を築く。3 つの CA が P2P モデルによって連携している様子を図 3 に示す。

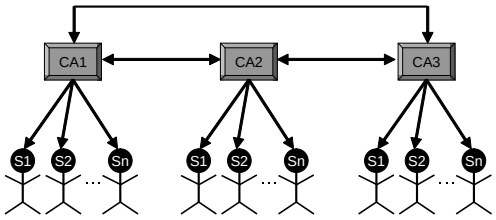

図 3: P2P モデルによる CA の連携

3 つの CA は互いに対等であるため、どの CA も自らの下位のノードに対する責任のみを負えばよく、運用コストが小さくなる。しかし、N 個の CA が存在する場合、必要な信頼関係の数は $\frac{N^2-N}{2}$ になり、現実的ではない。

2.5.2 ブリッジモデル

信頼の木構造の、もう 1 つの特殊な形態として、ブリッジ・モデルがある。ブリッジ・モデルでは、図 4 に示すように CA と CA との間にブリッジ CA を儲ける。各 CA はブリッジ CA と信頼関係を結ぶ。これにより、P2P モデル同様に全ての CA は対等の関係となる。この場合、必要な信頼関係の数は N 個の CA に対して N でよく、十分運用することが可能である。

2.6 既存のモデルの評価

第 2.4 節と第 2.5 節とで述べたように、信頼を結合した構造は大きく 2 つの形態があり、木構造

[1] http://www.openpgp.org/

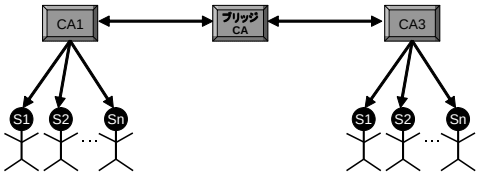

図 4: ブリッジ・モデルによる CA の連携

には 3 つのモデルがある。

ここで、本章で説明してきたいくつかのモデルについて整理し、比較を行う。まず、比較する点を以下に示す。

基準 1 第 3 者機関の必要性

基準 2 root CA の必要性

基準 3 木構造のスケーラビリティの高さ

基準 4 双方向の信頼関係の存在

基準 5 運用コスト

これらの基準を元に、各構造を比較した結果を表 1 に示す。

表中の「−」は、その項目に該当しないことを示す。基準 3 では、スケーラビリティが高い形態を「○」、低い形態を「×」とした。また、基準 5 では、必要な費用がより少なくてすむ形態を○、多く必要な形態を「×」、その中間を「△」とした。

第 3.3 節で述べる提案手法では、相手を信頼することで自分の持つ権限を他人に委譲できる。互いに相手の持たない権限を委譲しあえるためには、互いに相手を信頼しあえるモデルが必要である。双方向の信頼関係を構築できるのは、基準 4 より網構造のみである。また、基準 5 よりコスト面でも網構造は優れており、本提案では、網構造を手法のモデルとして採用した。

3 認証手法

本節では、認証に対して求められる事柄をまとめ、既存の認証手法の問題点をあげ、その改善手法を提案する。また、その手法を実現する実装について述べる。

3.1 認証に求めるもの

ユーザが利用するソフトウェアや、システムが与えることのできる権限は各システムで異なる可能性がある。そのため、新たなユーザを登録する際に管理者が注意すべき点がいくつかある。まずユーザの求める利用権限を調べ、ユーザに与える権限を決定する。この際不要な権限を与えないように注意する。次に決定した権限を、利用する全てのシステムにおいて、ユーザに適用する。

しかし既存の認証手法では、これらを実現することは困難であるか、大きな管理コストを必要とする。

3.2 既存の認証手法の問題点

既存の認証手法において、第 3.1 節で述べた点を実現する際に問題となる点を示す。

UNIX のユーザ認証では、システムの利用を許すか許さないかという両極的な制御しかできない。そのため、不必要な権限を与えずに利用を許可することは難しい。プログラムの実行権限を操作することで、ある程度の制限は可能である。しかし、各ユーザに対して異なる権限を適用しようとすると管理コストが増大してしまう。これらの問題点によって、各ユーザに適切な権限のみを与える事は困難である。

3.3 改善手法の提案

第 3.2 節で述べたように、既存の認証手法では要求を満たせない。本節ではこれを改善する手法を提案する。

ここに、システムを利用できるユーザ A(以降、A と表記) とできないユーザ B(以降、B と表記) を仮定する。A が B を信頼している時、A の持つ権限の一部を B に与えることにする。すると、信頼する側の持つ権限に基づいて権限が与えられるため、新たなユーザはシステムを利用する際に必要な権限を自動的に得られる。そのために、第 2.4 節で述べた信頼の輪モデルを利用する。これによって、A が B を信頼しているという情報が存在するとき、システムは間接的に B を信頼することができる。そして、A の持つ権限の一部を B に適

構造の形態	基準 1	基準 2	基準 3	基準 4	基準 5
網構造（信頼の輪モデル）	不要	不要	−	可	○
木構造（階層モデル）	必要	必要	○	不可	×
木構造（P2P・モデル）	必要	不要	×	不可	△
木構造（ブリッジ・モデル）	必要	不要	○	不可	△

表 1: 信頼の構造の評価

用する。

このモデルにおいて考えられる問題点は、間接的な信頼関係によって権限を与えることがセキュリティ上の危険を招く可能性があるということである。これは、管理者がユーザの信頼関係を監視することである程度防ぐことが可能である。しかしそれは管理コストの増加を招くため、当初の目的を果たすとは言い難い。とは言えそのユーザに権限を与える必要があるとすれば、必要最低限の権限のみを与えることのできる本手法は、不必要な権限も与えてしまう従来の手法に比較して安全であると言える。

3.4 sudo

今回は、権限の一部を与える方法として sudo[2] を用いる。sudo は多くの UNIX または UNIX 互換 OS で動作するアプリケーションであり、一般ユーザに対して super user の権限を適切に与えるツールとして利用されている。そのため、特定の OS に依存してしまうことも無く、多様なシステムが存在する環境に導入することも可能である。設定が非常に柔軟であり、簡単な設定で十分に適切な権限を与えることが可能である。

3.5 提案の実装

第 3.4 節で述べた sudo を利用して、提案した機能を実装する。この実装の現時点での機能は、ユーザの信頼関係を調べ、適切な権限が適用された sudo の設定ファイルを出力する。これは多くの UNIX で動作する perl 言語で記述するため、特定の OS に対する依存性を減らすことができる。信頼関係は公開鍵暗号における電子署名によって記述され、署名を検証することで信頼関係を確認できる。提案した手法が動作するメカニズムを図 5 に示す。

システムを利用する際に適切な権限を与えようとすれば、ログインする際に信頼関係を確認し、その都度 sudo の設定ファイルを再生成することが望ましい。しかし、システムを利用する手段は、以下のように様々なものがある。

- コンソールからのログイン
- ssh などのリモートログイン
- POP や SMTP のユーザ認証

これらはそれぞれ違う手段で認証を行っている。そのため、これらの認証手法全てに対して、ログイン時に設定ファイルを再生成する仕組みを付加する必要がある。また、全ての状況で sudo の利用が可能なわけではない。

システムを利用する際に適切な権限を与えるためには、sudo の設定ファイルの出力はログイン時に行われることが望ましい。しかし、ユーザ認証はコンソールからのログイン、リモートログイン、メール受信など様々な場面で行われる。これらはそれぞれ違う手段で認証を行っており、全てに対して変更を加える必要がある。

そのため、今回はこれらの認証手法に対する変更は加えず、sudo の設定ファイルを生成する部分のみを実装する。これは、提案した手法を実現するのに最低限必要な部分であるとともに、この部分だけでも提案を評価することが可能であるためである。

図中の番号に従って、以下のように動作する。

1. ユーザ A がユーザ B を信頼する
2. 提案された手法により、信頼関係が sudo の設定ファイルに反映される

[2] http://www.courtesan.com/sudo/

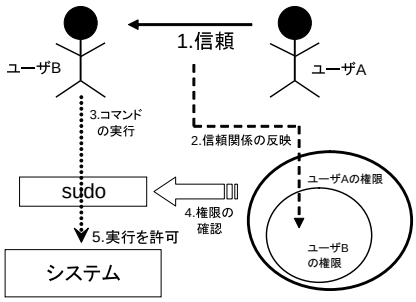

図 5: 動作メカニズム

3. ユーザがコマンドを実行しようと試みる
4. sudo が設定ファイルを読み、権限を確認する
5. 与えられた権限に基づき、コマンドは実行される

4 考察

第 3.5 節に述べた実装は、基本的な仕様が正しく動作することを確認した。

今回の実装では sudo を用いている。しかし、それ以外にもユーザの権限を制御する仕組みはいくつか存在する。それらについて考察する。

4.1 PAM

一部の UNIX には PAM と呼ばれる機構がある。PAM は、認証を必要とする複数のプログラムに対して、統一的な認証を実現する。PAM を利用すれば、1 つのプログラムに本手法を実装するのみで、システムにログインする複数のプログラムに適用することが可能である。そのため、PAM が利用できるシステムにおいては、PAM を利用して実装することで多様な状況に対応することが可能となる。

4.2 UFS2

FreeBSD 5.0-RELEASE には UFS2 という File System の実装がある。UFS2 には ACL という機能があり、通常の UFS に比べて細かい権限の制御が可能となっている。

UFS では、ユーザをファイルの所有者、同一グループ、その他の 3 つに分け、それぞれに対して、読み、書き、実行の許可ができるに過ぎない。そのため、あるファイルの実行権限をユーザごとに決めることはできない。このような設定が、ACL を用いると可能となる。

sudo を使用する理由の一つが、UFS のこのような欠点にあるため、UFS2 の ACL を用いることでも手法を実現できる可能性がある。

5 まとめ

本研究では、個人間の信頼関係に基づいて構築された信頼の輪の概念を用いることにより、適切なシステムの利用権限を与える手法を示した。信頼の輪は、個人と個人との信頼関係が複数存在する時、それらを合成することによって構築される個人認証のモデルである。このモデルによって、直接知らない相手を、間接的に信頼することができる。

この手法を用いることで、従来管理者に集中していていたユーザ管理のコストを分散することが可能となる。さらに従来の手法では困難であった、ユーザに与える権限を細かく制御することも可能となる。

本手法は、本来不要である権限を割り当ててしまう従来の手法に比べ安全にユーザ管理を行うことができる。

参考文献

[1] ITU-T Recommendation X.509 (03/00): Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate, March 2000. X.509.

[2] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer. OpenPGP Message Format, November 1998. RFC2440.

[3] R. Housley, W. Polk, W. Ford, and D.Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002. RFC 3280.