コンピュータセキュリティ 11−13
（２０００．９．８）

マルチエージェントシステムにおける動的ドメイン生成とポリシー管理について

山崎重一郎*、荒木啓二郎**
*富士通研究所、**九州大学

概要

サーバーとクライアントの両方の機能を持つ末端システムがインターネットのプラットフォームとして注目され始めている。特にgnutellaのように固定的なサーバーを一切必要としないものを我々は「完全分散型システム」と呼んでいる。完全分散型システムは全ての末端システムがサービス提供者になれるために、デジタル著作物の不正コピーへの利用などが問題となっている。

本論文では、デジタル著作物の著作権管理などを可能とする完全分散型のマルチエージェントシステムのためのポリシー管理システムを提案する。我々が提案するポリシー管理システムの特徴は、参加者が動的に変化するドメインにおいて、デジタルコンテンツの複製権などのポリシーを集中管理システムを利用せずに安全に伝播させることが可能なことである。

On the Management of Dynamic Trust Domains and Those Policies for Decentralized Multi-Agent Systems

Shigeichiro Yamasaki *, Keijiro Araki**
*Fujitsu Laboratory, **Kyushu University

Abstract

A new type of end-user system that has both a server and client functionality like “Gnutella” become a popular platform of the Internet. We call such platform system "decentralized multi agent system." Every end user of the decentralized multi agent system can be a contents provider when he or she got the contents from another network site. This feature of the systems causes the problem of illegal copy of digital contents.

In this paper, we propose a policy management system for our decentralized multi agent system. The feature of our policy management system is that it is able to distribute policy declaration like a privilege of the copyright of digital contents safely without any central control system.

1. はじめに

Napster[1]や gnutella[2]などのようなサーバとクライアントの両者の機能を持つ自律的な末端システム同士のネットワークを利用するシステムがインターネット上で普及しはじめている。このような自律的なネットワークシステムのモデルは、以前からマルチエージェントシステムとして提案されてたが、これらのシステムの普及は、このモデルが実際に現実のインターネット上でスケーラブルに運用可能であり、しかも多くの利用者にとって魅力的なものであることを実証したと言ってよいであろう。

ただし、Napster と gnutella とではネットワークシステムのモデルとしては大きな違いがある。Napster には、末端システム間の接続の仲介を行うサーバーシステムが存在するが、gnutella はそのようなサーバーシステムを一切必要としない。我々は、gnutella のような末端システムのみで構成され、集中管理システムを一切持たないタイプのシステムを「完全分散型」と呼んでいる。一方で、Napster のように、情報の集約を仲介するサーバーシステムを利用するタイプのものを「仲介型」と呼んでいる。完全分散型のシステムは、多くの利点を持つ反面でデジタルコンテンツの不正な複製を追跡できないといった問題を抱えている。

本論文の目的は、一定のポリシーにそった健全な運用が可能な完全分散型のマルチエージェントシステムを提案することである。我々は、従来より提案していた広域分散環境における認証基盤モデルである「S3A モデル」[4]やこれに基づいたアクセス制御モデル[3]を元に、共通の認証や権限管理のエンジンを備えた完全分散型のマルチエージェントプラットフォームとして、一切の集中管理システムを必要とせずにデジタルコンテンツの複製権限などのポリシーを安全に管理できるシステムを構成する。

2. 完全分散型情報共有システムの概要

gnutella などの現在の完全分散型の情報共有システムは、末端のユーザー同士が相互に情報共有を行なうためのシステムである。全ての末端システムはそれぞれ自分のローカルファイルシステムに対する検索エンジンとサーバー機能およびクライアントの機能を備えている。各末端システムは、他のいくつかの末端システムに接続し、そのような末端システム群の相互接続からなるネットワークを作っている。ユーザーからのクエリーはこのネットワークを通じて接続されている他の末端システムに直接流され、該当する情報を持つノードに巡り合うまでリレーされてゆく。そしてクエリーを満たすものが発見されると、そのサイトの情報が検索の起点までリレーされて返される。実データのデーターの交換は検索された 2 者間で行われる。

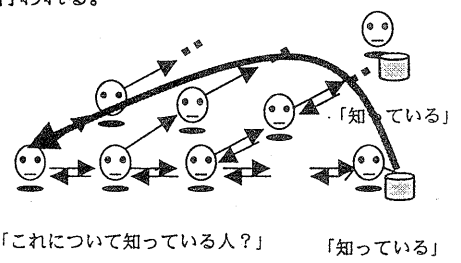

図 1 完全分散型情報共有システムの原理

3. 完全分散型システムの利点と問題点

3.1 情報提供の容易性

利点：末端システムのユーザーは、サーバーシステムへのデーターのアップロードなどの作業無しに即座にネットワークサービスを開始できる。提供したい情報が一旦ネットワークに流出すれば、起点のサイトはネットワーク接

続を終了してしまってもそれが始めたコンテンツ提供サービスは他の末端ユーザーによって継続され得る。この特徴は、サーバーの維持などのコストをかけずに簡単にインターネットを使った情報サービスの提供を行なう手段として利用できる。

問題点:末端ユーザーがそのサイトにあるデジタルコンテンツを他の末端ユーザーに直接提供でき、またネットワークへの接続を切断すると情報提供の痕跡は残らないため、もしそのやりとりが著作権侵害などの不正なものであったとしてもその検出や追跡は極めて困難になる。

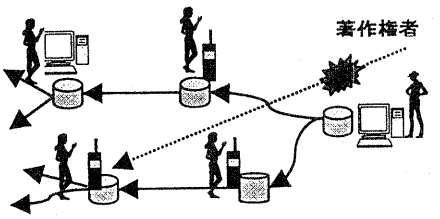

図 2.　違法コピーの連鎖

3.2 負荷分散、スケーラビリティ

利点:完全分散型システムではコンテンツの複製は容易であり、かつボトルネックとなるような集中管理システムを一切持たないため、負荷分散が容易である。また、この性質によって、強力なサーバーを利用することなく相互接続される端末システムの増加だけでサービスの規模を拡大して行くことができる。

問題点:同一内容の情報源が冗長に存在するために、網全体のトラフィックは増加する。また、各末端システムによる相互的な状態監視のためのトラフィックが爆発的に増加する可能性がある。

3.3 匿名性

利点:データーのやり取りをするノードは他者を介して紹介されるために、情報提供者の匿名化が可能であり、個人情報を保護したサービスが可能である。

問題点:匿名性が強いために、著作権侵害などの違法行為の発見や追跡や証明が困難である。

3.4 リアルタイム性

利点:WWW ではしばしばリンク先が存在しなくなっていたり内容が変わっていたりすることがあるが、このモデルではリアルタイムでコンテンツ実体を検索するために、常に最新の情報を得ることができる。

3.5　頑強性

利点:特定のサイトの破壊や運用の停止などが発生しても代替のサービス提供者が残っているかぎり同等のサービスを継続できる。

4. 提案するシステム

4.1 ポリシー証明書による分散的ポリシー管理

我々が提案するシステムの特徴は、著作権者が定義したデジタルコンテンツへの複製の条件などのポリシーを「ポリシー証明書」と呼ぶ電子署名付きのデーターとしてコンテンツとともに配信することである。ポリシー証明書には、人間に対する契約書としての意味とシステムに対するコンテンツや処理プログラムの実行権限の割当てに関するルールの集まりとしての意味を持つ。

我々は、あるポリシー証明書によって同一のポリシーが伝播している仮想的なネットワーク領域を「信用ドメイン」と呼んでいる。

我々が提案するシステムでは、新しい端末ユーザーが信用ドメインに参加するときに、まずポリシー証明書による合意契約とそれに基づく権限割当てを行なう。これによって、コンテンツの配信に先立ってそのコンテンツの扱い方についての共通のポリシーを確実に伝播させることができる。このポリシー伝播の方法は、一切の集中管理システムを持たないという完

全分散モデルの特性を維持する。

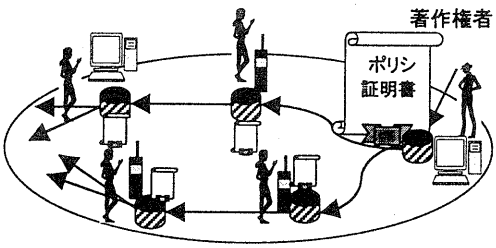

図 3. ポリシー証明書とコンテンツの伝播

4.2 感染型のサービス配信

gnutella などの情報共有システムは、コンテンツの共有だけしか行えないが、モバイルコードを扱うことができるマルチエージェントシステムでは、コンテンツだけでなく処理を行なうアプリケーションプログラムも交換し共有することができる。移動コードの安全性は、PKI に基づくオブジェクト署名とその検証系を利用することで実現できる。

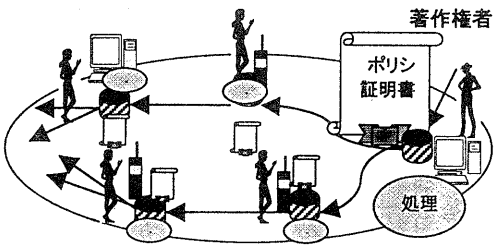

図 4.　感染型のサービス配信

音楽配信の例をとると、音楽データーの共有だけでなく、音楽データーの再生プログラムを同時に提供することも可能である。この機能を使うと料金を支払ったユーザーだけが良質の音楽を再生できるというようなサービスも可能になる。このときも、コンテンツのみの配信と同様に音楽の配信元は、自前で強力なサーバーを持つ必要はなく、委託契約を含んだポリシー証明書と音楽コンテンツとその処理システムのセットを他のサイトに複製してもらい、サービスそのものを複製させるだけでよい。このような処理を含んだサービスの複製を「感染」と呼ぶことにする。また、同様に店舗のページと受注システムに販売委託契約を含んだポリシー証明書を対にして配信することによって、自前ではサーバーを持たなくても、他のサイトに自分の店舗システムを「感染」させるとこによって電子店舗を維持することができる。

4.3 ポリシーサービスパッケージ (PSP)

感染型のサービスを配信するためには、コンテンツや処理プログラムとその利用ポリシーをパッケージ化したものを複製の単位にすると「感染」の方法が単純化される。我々はこのようなパッケージを PSP(Policy Service Package)と呼んでいる。PSP は次のような構造を持っている。

〈ポリシー証明書,(コンテンツ＋処理プログラム)〉

音楽配信の場合、PSP は典型的には次のようなものになる。

〈著作権契約,(音楽データー＋再生プログラム)〉

また、電子店舗ならば次のようになる。

〈委託販売契約,(店舗ページ＋受注システム)〉

5. 完全分散型認証モデル(S3A モデル)

我々は、PKI に基づく広域分散環境における認証基盤を実際のアプリケーションシステムに統合的に利用可能にするための枠組みとして「認証の S3A モデル」を提案している[4]。このモデルは、認証システムにおける、個体認証、属性認証、ポリシー定義の３つの側面について、それぞれ異る権威機能として分離し、広域分散環境において、情報へのアクセス権限や情報の信頼性などを管理可能にすることを目的にしている。S3A モデルでは 3 種類の権威機関は、それぞれ異る種類の証明書を発行する。

CA (Certification Authority) : 個体認証を行う権威機関である。公開鍵認証基盤に基づいた公開鍵証明書の発行を行なう。

AA (Attribute Authority) :個人の属性を認証する権威機関である。属性証明書を発行する。

個人の属性は複数存在し得る。

PAA (Policy Approving Authority): 実際のサービスやコンテンツの利用条件などを定義する機関である。ポリシー証明書を発行する。ポリシーとは、属性からそのサービスの領域における権限を表す「ロール」を割当てる規則である。

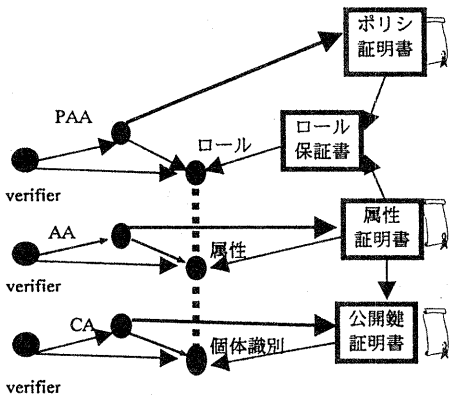

図 5.　3 つの権威機関による証明書

例えば、ある個人が、金融機関という AA によって、「A 社へ支払い済み」という属性を定義されており、あるサービスの PAA である A 社が、そのポリシーとして「A 社へ支払い済みという属性を持つ個体ならば、このサービスの会員というロールを与える」というルールを持っていた場合、実際にその個人が「A 社へ支払い済み」であるときに限り「会員」というロールが割当てられる。

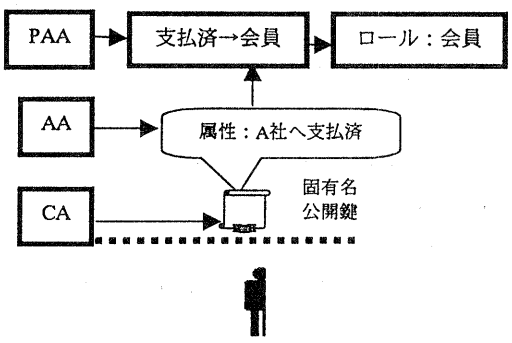

図 6.　ロール割当ての例

6. トラストエンジン

本論文で提案するシステムは、各端末システムがポリシー証明書や属性証明書を安全に解釈できることを前提にしている。我々は、この共通の解釈系を「トラストエンジン」と呼んでいる。トラストエンジンの機能は、ポリシー証明書と属性証明書を入力として、適切なロールを割当てることである。

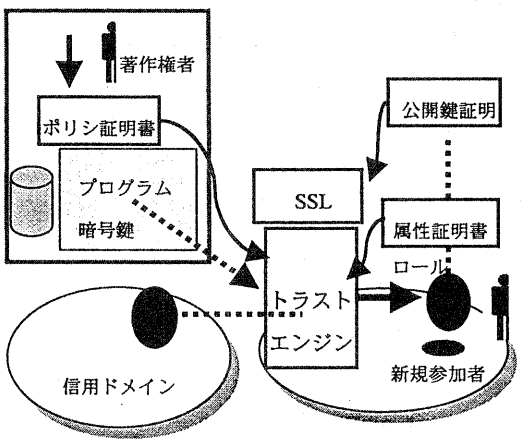

図 7.　トラストエンジンによるロール割当て

トラストエンジン自体の正統性は、公開鍵認証基盤に基づき、SSL による相互認証とオブジェクト署名の検証によって実現している。

7. 信用ドメインへのログイン

信用ドメインは、ポリシーが伝播する仮想的ネットワークの領域であるが、その参加者は動的に変化する。この仮想ネットワークは、岩尾によるマルチキャスト型通信に基づくエージェント間通信環境とその上での動的な並列計算モデルである「フィールドリアクターモデル[5]」に基づいて実現している。

完全分散型システムでは、ログインのための特定の信頼できるサイトを仮定できないので、新しく信用ドメインへ参加しようとするユーザーは、すでに参加済みの任意の参加者に対してログインの要求を行う。信用ドメインへのログインは、各ユーザーの属性情報とポリシーに

基づいて行われ、ログインの結果としてユーザーには、ロールが割り当てられる。

ログイン時にロール割り当て処理を行うトラストエンジンは、すでに信用ドメインに参加しているエージェント側ではなく、新規に参加しようとしている参加者の側で稼動しているものが使用されることに注意する。これは、属性情報がプライバシー情報であるためである。また、トラストエンジンが信頼できるということも前提になっている。新規参入者の側のトラストエンジンを使用することによって、個人の属性情報を一切ネットワークに流すことなく安全にログイン処理を行うことができる。

このようなログインの連鎖によって、集中管理システムなしにポリシーを安全に伝播させることができる。また、各エージェントは、任意にログアウト、もしくは消滅することができるが、そのような事態が発生しても信用ドメインに参加者が存在するかぎり信用ドメインは存在しつづける。

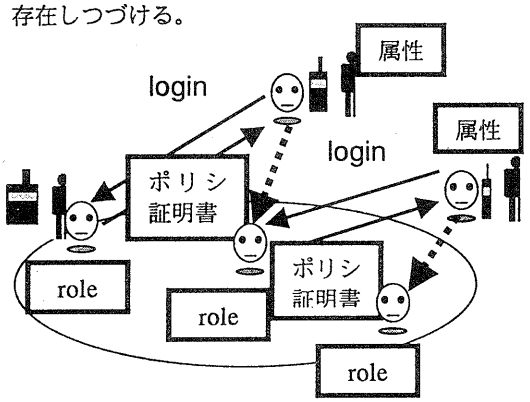

図 8.　信用ドメインへのログインの連鎖

8　まとめと今後の課題

デジタル著作物の著作権保護が可能な完全分散型のマルチエージェントプラットフォームを提案した。

本システムでは、コンテンツや処理プログラムとともにそのコンテンツの所有者が定義した利用ポリシーをポリシー証明書という電子署名付データとして伝播させることを特徴にしている。さらにこのプラットフォームの各末端システムが公開鍵認証基盤の元で相互に信頼できるトラストエンジンを備えていることを前提として、ポリシーに準拠した権限割り当てを行うことによって、集中管理システムを仮定するとなく著作権の保護を実現している。

このシステムをより安全にするためには、さらにコンテンツの暗号化や各エンジンでの処理のログの共有などの措置を組み合わせる方法が必要となるが、その鍵管理の方法などは今後の課題である。また、ポリシーには端末の性能や回線容量などの QoS 的な要素やトラフィックの制御の情報なども含まれることになろう。

謝辞

本研究のアイデアの多くは、富士通研究所ネットメディア研究センターの岩尾忠重氏との議論と氏による実装に負っている。ここに記して感謝する。

参考文献

[1]Napster: http://www.napster.com/

[2]gnutella: http://gnutella.wego.com/

[3]YAMASAKI Shigeichiro, ARAKI Keijiro: A Privacy Enhanced Access Control Model for Wide Area Distributed Information Systems, ICOIN-14 pp.6A2.1-6A2.5, 2000

[4]山崎重一郎、荒木啓二郎:信用情報と利用ポリシーの管理が可能な相互認証を実現する認証基盤の提案:情報処理学会論文誌　第 40 巻第 1 号平成 11 年 1 月 pp.296-309

[5]岩尾忠重,岡田誠,高田裕志:緩やかな分散オブジェクト連携モデル：Field-Reactor Model,情報処理学会第 57 会全国大会　3-535-536, 1998