モバイルエージェントの正当性確認方式に関する一検討

吉田, 裕 / KANDA, Satoshi / YOSHIDA, Yutaka / 神田, 聡

(出版者 / Publisher)
法政大学計算科学研究センター
(雑誌名 / Journal or Publication Title)
Bulletin of Computational Science Research Center, Hosei University / 法政大学計算科学研究センター研究報告
(巻 / Volume)
13
(開始ページ / Start Page)
121
(終了ページ / End Page)
125
(発行年 / Year)
2000-03-31
(URL)
https://doi.org/10.15002/00024885

モバイルエージェントの正当性確認方式に関する一検討

神田　聡
法政大学大学院工学研究科

吉田　裕
法政大学工学部電子情報学科

モバイルエージェントを実現するにあたって、モバイルエージェントはエージェントシステム中のホストに到着する毎に自身の正当性を明らかにできることが望ましい。本稿では通信チャネルを監視する攻撃者からシステムを予防するために、ユーザの一定の手続きに基づくシステム利用期間を限定することと定期的にシステムキーを更新することとによりモバイルエージェントの正当性を証明する「IASA」を提案し、実装を試みたので報告する。

1．はじめに

近年のインターネットの爆発的流行とともに、エージェント技術がさかんに研究されている。エージェントはユーザの代理人としてネットワーク内で様々な仕事をこなし、ユーザの負荷の軽減を目指す。しかし、なりすましや改ざんなど、悪意の第三者の攻撃に対する対策として、複数のホスト（エージェントシステム）を行き来するモバイルエージェント（以下エージェント）は、各エージェントシステムに到着する毎に自身の正当性を明らかにすることが望ましい[1]。CORBA[2]などの代表的な分散ネットワークシステムのセキュリティポリシーは主にホスト内に留まっているオブジェクトを対象とするため、モバイルエージェントのような移動可能オブジェクトに対しては不充分である[3]。そこで本稿では通信チャネルを監視する攻撃者からシステムを予防するために、ユーザの一定の手続きに基づくシステム利用期間を限定することと定期的にシステムキーを更新することによりエージェントの正当性を証明する一手法 IASA を提案し、実装を試みた。

2. 正当性確認のための処理システム

2.1. 前提条件

今回実装したエージェントの正当性を確認するためのシステムは「IASA」（Identification and Active State Authentification）と名づけた。これはエージェントの移動可能な範囲（以下コミュニティ）に共通して不定期に更新される鍵（以下証明鍵）の利用とユーザの使用状態（以下アクティブ状態）の監視によって行われるＩＤ認証をもってエージェントの正当性を評価するためである。

IASA は、例え通信チャネルのいかなる場所で悪意の第３者が監視していたとしても、移動エージェントの成りすましや改ざんを不可能にすることで、通信線に流れるデータから読み取ることのできる情報からエージェントの発行主を保護することを目的としている。したがって IASA はシステムを構成する各サーバへのハッキングによるエージェントの改ざん、なりすましに対する防御策は考慮していない。

2.2. システム構成

IASA はエージェントシステムを利用するユーザの状態を監視するアクティブ状態監視サーバ（以下監視サーバ）、エージェントシステムを利用するユーザ全員のアカウントを管理するマスタサーバ、システム内の全ホストに対して証明鍵を配送するキーサーバの３要素により構成される[図 1]。

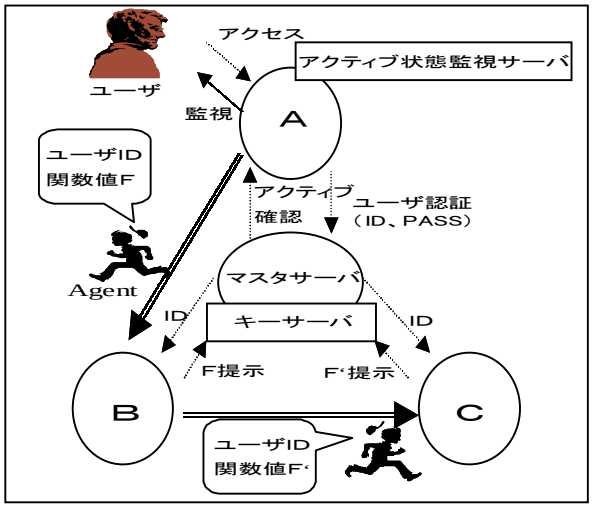

図１　IASA

2.3. アクティブ状態

一人のユーザＡがシステムを利用している状態をアクティブ状態という。アクティブ状態はユーザＡがシステム利用の終了を監視サーバに伝えるまで続く。IASA を用いてエージェントの正当性を証明するためにはユーザＡがシステム利用で使用できる計算機は同時に一台となる。

アクティブ状態の監視の実現方法を以下に示す[図 2]。ユーザ A、B に対するそれぞれの監視サーバは、エージェントシステムの利用を開始するときに、そのためのユーザ ID とパスワードを、エージェントシステムを利用するユーザのアカウントを管理するマスタサーバに送る。

マスタサーバは、エージェントシステムを利用するユーザのユーザ ID とパスワードが記載されたスタティックなリスト（アカウント）と、今現在エージェントシステムを利用しているユーザのみが登録されるダイナミックなリストを持つ。図２における U は、アクティブな全ユーザに対して使い捨ての一意なものである。マスタサーバはその後、監視サーバに U を送る。これは、後でエージェントに持たせるために利用される。

それぞれの監視サーバは、自分のホストでユーザがエージェントの利用を開始、終了した事を感知し、マスタサーバからの問い合わせに対して、ユーザがエージェントシステムを利用していればアクティブ、それ以外ではイナクティブを返す。マスタサーバはユーザが利用を開始したことを知るとその情報を登録し、必要に応じてエージェントが実行される外部ホストからの問い合わせに対して、監視サーバからの報告を元に応答する。ユーザに利用されているホストにはマスタサーバへの登録を義務付け、外部からエージェントを受け取ったホストはマスタサーバへの問い合わせを義務づける。

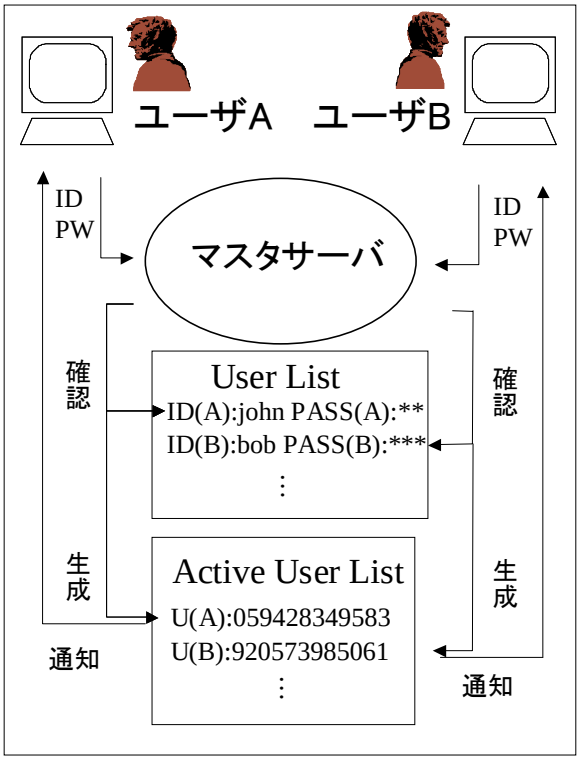

図２　アクティブ状態の監視方法

分（K'）である。差分を渡されたホストは、自身に保持している鍵 K をアップデートする。エージェントが他のホストへ移動する際には、この鍵は最終的に K と、マスタサーバから教えられた一意な U を利用して作られた F となりエージェントのヘッダに埋め込まれる。IASA では、各ホストにおいてエージェントの認証作業が終わったことを確かめて、認証にかかる時間、移動にかかる時間のマージン（約１秒）をとってから、鍵の送信を行う。各ホストは実行 OK をエージェントに伝えてから実際にはしばらくエージェントを待機させ、鍵のアップデートが可能であることをマスタサーバに伝える。これは、鍵の送信を行うたびに全てのホストに対して問い合わせが行われることを意味する[図３]。

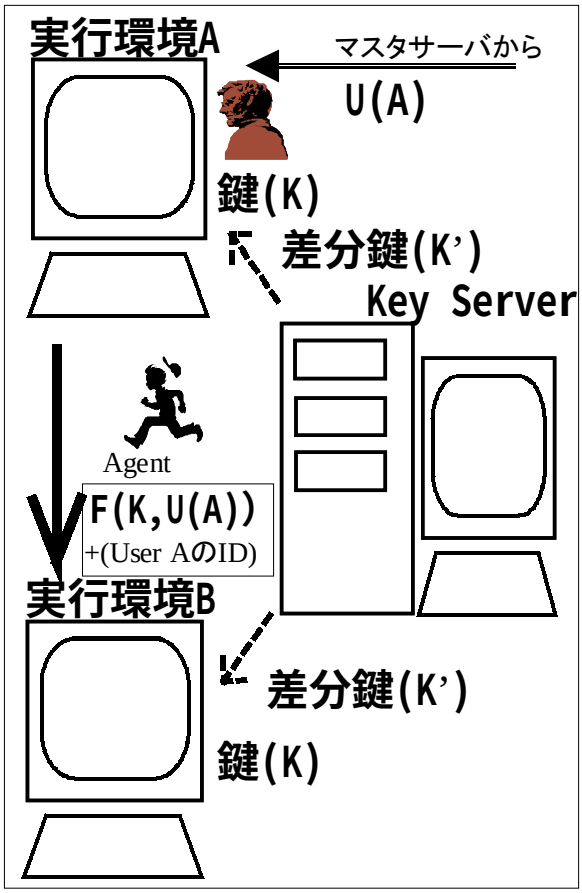

図３　証明鍵の配布

2.4. 証明鍵

証明鍵（以下、本文では「鍵」と表記）は、エージェント移動先の全ホストが認証作業の完了を通知した時点でキーサーバによって全ホストに対し配送される。キーサーバはマスタサーバに生成されたエージェント数を問い合わせることによって認証作業の完了を通知すべきホストの数を知る。配送される内容は３２ビットの鍵の差

3. IASA による正当性の確認

IASA の動作にはエージェントの移動、認証、実行という３つのフェーズが用意される。この３フェーズを１ターンと呼ぶ。各ホストはキーサーバに対し、認証フェーズが終了するごとにシグナルを通知し、キーサーバはマスタサーバから得られるエージェント数シグナルを受け取ると全サーバに対して一斉に鍵の変更通知を送るが、

この通知の内容はシステム全体が開始される時を除き鍵そのものではなく、その差分である。全ホストから更新完了の通知を受けると、キーサーバは次回の更新を準備する。

複数のエージェントが同時に実行されている環境では、各ホストによってフェーズの遷移時間が異なると考えられるため、ターンの終了する時間にはばらつきが生まれるはずである。前章 2.4 の方法によれば、それでも各ホストに同一の鍵を保持させるためには、一番時間がかかったホストのターン終了を全ホストが待つことになり、効率の悪化をもたらす。この問題の回避策として、作業内容が長時間にわたるエージェントに関しては、実行が終了しても新たな鍵がホストに到着するまでホスト内に待機させ、他のエージェントが実行に時間のかかるエージェントを待つことによる効率の悪化を軽減する試みを行っている。

アクティブ状態の監視と証明鍵を用いて最終的にエージェントの正当性を判断する手順を以下に示す[図 4]。ユーザ A のアクティブ状態監視サーバは、現在の鍵 K と、マスタサーバから送られたユーザ A に対する U、U(A)を用いて、さらにある関数を通した F(K,U(A))、またユーザがマスタサーバに入力したユーザ ID をエージェントに添付して送信する。図はそれらを持ったエージェントが実行環境 B に到着したところを示している。

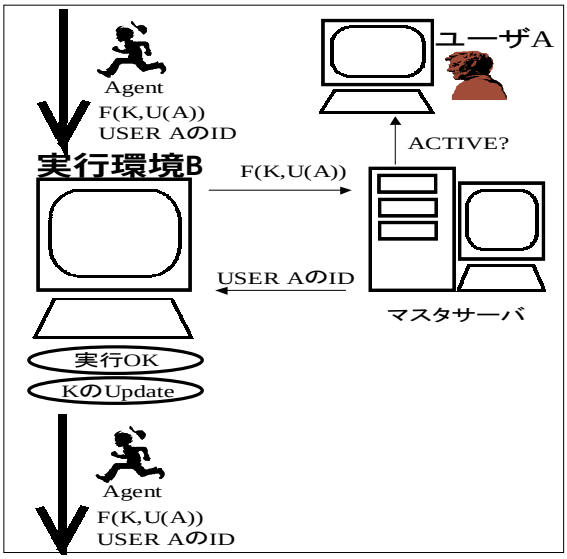

図４　認証のながれ

エージェントを受け取った実行環境 B は、マスタサーバにこの F を問い合わせ、マスタサーバはそれを用いて U(A)を取り出し、A がアクティブであるならば、U(A)から A のユーザ ID を返す。実行環境 B は、そのユーザ ID と、エージェントが持ってきたユーザ ID が一致していることを確認して、はじめてエージェントの実行を許可する。

4．実装

IASA はエージェントの作業内容をユーザがプログラム可能な移動エージェント実行環境「PARENT」のモジュールとして実装された。PARENT は UNIX 上で動作する C++で書かれたアプリケーションで、エージェントの移動、その上でのファイル操作などいくつかの動作をサポートしている。基本的に実装したシステムのモジュール群において IASA を構成するモジュールは論理的に独立しており、PARENT から IASA を構成する各モジュールを利用するようになっている[図 5]（一部例外あり）。図における各ホスト A～D のそれぞれに用意されている ARE はエージェント実行環境で、ユーザによってアクセスされたときはアクティブ状態監視サーバとしても機能する。キーサーバは鍵の配送時にマスタサーバとの通信を頻繁に行うと考えられるので、今回の実装ではマスタサーバ内の関数という形で処理されている。

それぞれのモジュール間のやり取りは、エージェントの移動を行うために開発したプロトコル MATP を TCP/IP 上で使用するが、IASA とは関係しないため説明は省略する。

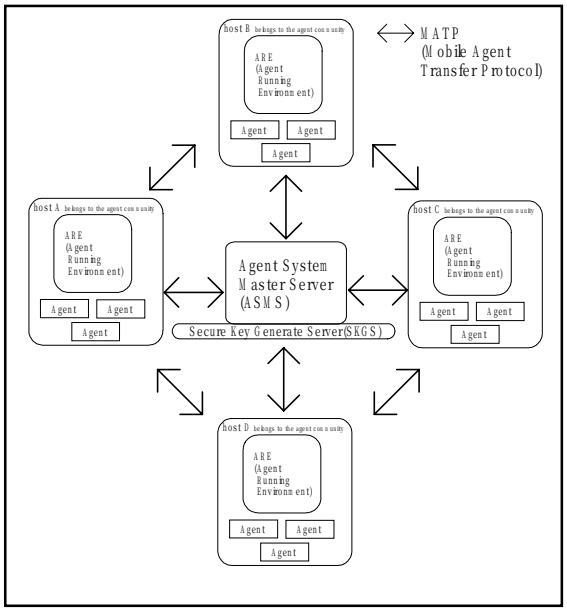

図５　実装システム（PARENT）

5. 検証

5.1 トラヒック量の増加

この方式の問題点の一つとして上げられるのは、全ホストにおいて同一の鍵を保持する同期作業のために、鍵の送信を行うたび全てのホストに対して問い合わせが行われることである。鍵を更新する間隔は、エージェントが移動先ホストにおいて作業をする時間に近ければ近いほどオーバーヘッドが減少すると考えられるが、ネットワークの負荷はそれだけ高くなり、結果としてシステム全体の作業効率は悪化すると予想されるが、現在の IASA においてその認証方法を変えずに効率を高めるのは難しい。

5.2 セキュリティの確保

攻撃者の立場から見ると IASA の動作する環境においてエージェントの成りすまし、改ざんを行なうためには、まず対象となるエージェントの発行主がアクティブ状態にあるかどうかを知る、つまり実際に発行主がシステムにログインしているかどうかを確かめる必要がある。何らかの方法でそれが確認できるとして、次に攻撃者はエージェントを動作させるために必要な証明鍵を偽造しなくてはならない。鍵を作成するためはマスタサーバがユーザに与えた使い捨ての数値 U、現在の証明鍵 K が必要である。だが通信線を移動するエージェントが持っているものは U と K を引数とした関数値 F であり、鍵の更新は差分で行なわれるため、証明鍵の偽造は困難であると思われる。

また、差分の履歴を得ていくことで鍵の逆算、予測等が行なわれることのないように、差分には純粋な乱数値を用いている。

攻撃者はユーザがアクティブ状態のときに F を偽造する必要があり、そのためには現在の鍵とUの双方を入手しなくてはならず、それは通信チャネルを監視するだけでは不可能である。IASA では鍵の生成とアクティブ状態の監視は別のシステムで管理し、鍵の配布に際しては鍵そのものを配布せず差分を配布することで通信網内におけるセキュリティを高めている。

6. むすび

モバイルエージェントの正当性を移動先において証明するための方式 IASA を提案した。ユーザのパスワード以外のものを用いて認証を行なう方法として、ユーザがエージェントシステムを利用しているか、していないかをアクティブ状態監視サーバに監視させ、マスタサーバに必要に応じて報告させること、移動するエージェントに渡す鍵を変化させつづけること、の２つを用いることでトータルのセキュリティの確保を目指した。

IASA は移動するエージェントの正当性を確保するために、アクティブ状態と証明鍵を利用し、成りすましや改ざんを防ぐ機構を備えているが、移動エージェントシステムにおいてより強力なセキュリティを確保するためには、データの暗号化や計算機自身のセキュリティの確保といった措置がまず求められ、IASA はあくまで二次的役割を担うべきであると考える。一般的にセキュリティの確保の問題に関しては人為的なものからアーキテクチャ関連まで多種多様であり、IASA に関してもその舞台を通信網に限定した補助的システムとしての利用が前提であり、有効であると思われる。

PREFERENCES

［１］ 岩井他, "Java Mobile Agent System-Architecture, Application,Security-",IP-22:MM New Technology Trial , 1998.

［２］ OMG, "Security Service Specification, CORBA services" , Common ObjectServices Specification Updated November 1997.

［３］ GMD FOKUS,International Business Machines Corporation,Suppoted by:Crystaliz,Inc.,General Magic,Inc.,"The Open Group:Joint Submission:Mobile Agent System Interoperability Facilities Specification", OMG TC Document orbos/97-10-05,November 10,1997.

キーワード.

エージェント、IASA、正当性の確認、アクティブ状態、システムキー、ユーザキー.

Summary.

A Study on Justification Scheme for Mobile Agent Systems

Satoshi Kanda*
* Department of Electrical Engineering, Hosei University†

Yutaka Yoshida**
** Department of Electronic Informatics, Hosei University†

It is desirable that a mobile agent should be justified after transferring to one of hosts consisting of an agent system and just before if has been executed on the host. Here,a trial scheme is proposed as a complementary means to other security schemes for access control and data transmission and so on.Its characteristics consist in both restriction of mobile agent execution to during the period,called user active state period,during which its associated user is keeping access to the system and full utilization of time-varying but unique system key distributed to all the related servers.

Keywords.
Mobile agent,IASA,Justification,Active state,System key,User key.

† 3-7-2,Kajino-cho,Koganei-shi,Tokyo 184,Japan