(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-18772
(P2006-18772A)
(43)公開日　平成18年1月19日(2006.1.19)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	510F	5B017
G06F 21/20	(2006.01)	G06F	12/14	540A	5B045
G06F 15/16	(2006.01)	G06F	15/00	330A	5B085
		G06F	15/16	620W	

審査請求 未請求　請求項の数 9　ＯＬ　（全 16 頁）

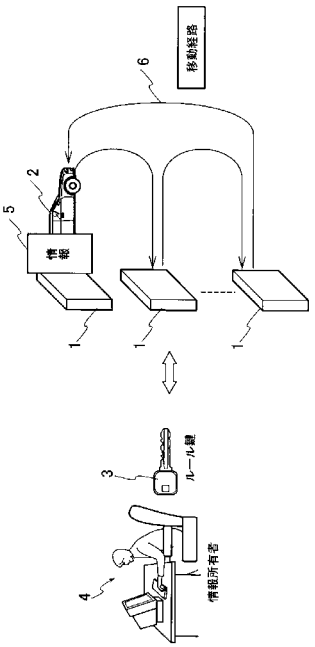
(21)出願番号　特願2004-198493 (P2004-198493)
(22)出願日　平成16年7月5日 (2004.7.5)

(71)出願人　399041158
西日本電信電話株式会社
大阪府大阪市中央区馬場町３番１５号
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100095500
弁理士　伊藤　正和
(74)代理人　100101247
弁理士　高橋　俊一
(74)代理人　100098327
弁理士　高松　俊雄
(72)発明者　太田　崇博
大阪府大阪市中央区馬場町３番１５号　西日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】エージェント制御システムおよび方法

(57)【要約】　（修正有）
【課題】　情報への攻撃に対して情報の位置の秘匿を可能とし、情報を分割して保管することもでき、分割情報に関連した他の分割情報の探索も困難にすることが可能なエージェント制御システムを提供する。
【解決手段】　ネットワーク上に互いに通信可能に配置された複数の防御サーバ１と、情報５を所持して防御サーバ１間を移動するエージェント２と、エージェント２が所持し前記移動を決定するためのルール関数と、ルール関数の初期値と係数とを含むルール鍵３と、ルール鍵３に基づきエージェント２の管理を行うためのエージェント管理装置と、を備える。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ネットワーク上に保管された情報所有者の情報を不正アクセスによる盗難から防御するためのエージェント制御システムであって、
前記ネットワーク上に互いに通信可能に配置された複数の防御サーバと、
前記情報を所持して前記防御サーバ間を移動するエージェントと、
前記エージェントが所持し前記移動を決定するためのルール関数と、
前記ルール関数の初期値と係数とを含むルール鍵と、
前記ルール鍵に基づき前記エージェントの管理を行うためのエージェント管理装置と、
を備えることを特徴とするエージェント制御システム。
【請求項２】
前記ルール関数は、
一方向関数であることを特徴とする請求項１に記載のエージェント制御システム。
【請求項３】
前記情報は、
分割され複数の前記エージェントにより所持されることを特徴とする請求項１または２のいずれかに記載のエージェント制御システム。
【請求項４】
前記エージェント管理装置は、
前記エージェントが現在において位置する前記防御サーバを前記ルール関数と前記ルール鍵とに基づいた演算により求めることを特徴とする請求項１～３のいずれかに記載のエージェント制御システム。
【請求項５】
前記エージェント管理装置は、
前記演算により求めた前記防御サーバに前記エージェントが位置していない場合に、この防御サーバへ前記エージェントが移動する前もしくは後に移動する予定の他の防御サーバを前記演算により求め、もって前記エージェントが現在において位置する防御サーバを検索し求めることを特徴とする請求項４に記載のエージェント制御システム。
【請求項６】
前記防御サーバは、
前記エージェントと前記情報所有者とを照会して認証を行うことを特徴とする請求項１～５のいずれかに記載のエージェント制御システム。
【請求項７】
前記ルール鍵は、
前記エージェントの移動開始時刻および移動毎の移動タイミング時間とを含むことを特徴とする請求項１～６のいずれかに記載のエージェント制御システム。
【請求項８】
前記エージェントは、
前記エージェント管理装置からの帰還命令に基づいて前記エージェント管理装置に帰還するとともに自身が所持する前記情報を前記情報所有者に提示することを特徴とする請求項１～７のいずれかに記載のエージェント制御システム。
【請求項９】
ネットワーク上に保管された情報所有者の情報を不正アクセスによる盗難から防御するためのエージェント制御方法であって、
前記ネットワーク上に互いに通信可能に配置された複数の防御サーバにより互いに前記通信を行うステップと、
前記情報を所持して前記防御サーバ間を移動するエージェントにより前記情報を移動させるステップと、
前記エージェントが所持し前記移動を決定するためのルール関数により前記移動を決定するステップと、

前記ルール関数の初期値と係数とを含むルール鍵により前記初期値と前記係数とを取得するステップと、
前記ルール鍵に基づき前記エージェントの管理を行うためのエージェント管理装置により前記エージェントの管理を行うステップと、を有し、
もって前記エージェントの前記防御サーバ間における移動を制御することを特徴とするエージェント制御方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワーク上に保管された情報の秘密管理に関する。
【背景技術】
【０００２】
従来のネットワーク上における情報の秘密管理としては、対象となる情報を認証サーバによる認証の有無を確認することによって秘密保護したり、あるいは対象となる情報を暗号化して秘密管理を行っている。
【０００３】
こうした従来技術のうちの一つの秘密保護の方法としては、暗号化された情報を更に暗号化して保護を行う。この暗号化された情報を解読するには、複数のグループから構成された解読機能を適用するためのアクセス公式を正しく解く必要がある。このように情報の暗号化や解読機能の分散化、アクセス公式の要求などをもって情報の秘密保護を提供している（特許文献１参照）。
【０００４】
また、別の秘密保護の方法としては、分配者の無い環境で秘密鍵を算出せずに、ｎ個の機関のうち、任意ｔ個の機関による分散復号や署名を実現できる（ｔ、ｎ）型の秘密分散システムを構築している。こうした構成の秘密分散システムによって情報の秘密保護を提供している（特許文献２参照）。
【０００５】
また、別の秘密保護の方法としては、分散保管サーバに冗長化データとシェア鍵を組にして保管する手段を備え、鍵の紛失や、データの流出や、ディスククラッシュによるデータの破壊に対して、暗号鍵の管理を容易にした分散保管データシステムが知られている（特許文献３）。
【特許文献１】特表２００２－５３８７０２号公報
【特許文献２】特開２００１－０３４１６４号公報
【特許文献３】特開２００３－３４８０６５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、従来技術による秘密管理システムや秘密管理方法では、秘密情報の保管先が固定されており、そのため不正アクセス者が保管先を見つけ出して、この単一箇所に時間をかけて攻撃することが可能であった。
【０００７】
また、秘密情報が単一箇所にまとまって保管されているので、その情報の意味や素性を知ることが可能であり、秘密情報をまとめて得ることが可能であった。
【０００８】
このような課題に鑑み、本発明は、情報の保管場所をエージェントにより随時変更することができ、情報への攻撃に対して情報の位置の秘匿を可能とし、また、情報への攻撃が可能な時間を情報の位置での滞在時間内として規制することができ、さらに、複数の防御拠点サーバへ攻撃せざるを得ないので攻撃を難しくすることができ、
また、情報を分割して保管することができるので、一つの分割情報のみから意味や素性

が判明することを阻止でき、分割情報に関連した他の分割情報の探索も困難にすることが可能なエージェント制御システムを提供することを目的とする。

【課題を解決するための手段】

【０００９】

請求項１に記載の本発明は、ネットワーク上に保管された情報所有者の情報を不正アクセスによる盗難から防御するためのエージェント制御システムであって、前記ネットワーク上に互いに通信可能に配置された複数の防御サーバと、前記情報を所持して前記防御サーバ間を移動するエージェントと、前記エージェントが所持し前記移動を決定するためのルール関数と、前記ルール関数の初期値と係数とを含むルール鍵と、前記ルール鍵に基づき前記エージェントの管理を行うためのエージェント管理装置と、を備えることを主旨とする。

【００１０】

このような請求項１においては、ネットワーク上に保管された情報所有者の情報を不正アクセスによる盗難から防御するためのエージェント制御システムを構成するために、前記ネットワーク上に互いに通信可能に配置された複数の防御サーバと、前記情報を所持して前記防御サーバ間を移動するエージェントと、前記エージェントが所持し前記移動を決定するためのルール関数と、前記ルール関数の初期値と係数とを含むルール鍵と、前記ルール鍵に基づき前記エージェントの管理を行うためのエージェント管理装置と、を備えている。

【００１１】

また、請求項２に記載の本発明は、請求項１において、前記ルール関数は、一方向関数であることを主旨とする。

【００１２】

このような請求項２においては、ルール関数に一方向関数を用いている。

【００１３】

また、請求項３に記載の本発明は、請求項１または２のいずれかにおいて、前記情報は、分割され複数の前記エージェントにより所持されることを主旨とする。

【００１４】

このような請求項３においては、情報を分割して複数のエージェントにより所持されている。

【００１５】

また、請求項４に記載の本発明は、請求項１～３のいずれかにおいて、前記エージェント管理装置は、前記エージェントが現在において位置する前記防御サーバを前記ルール関数と前記ルール鍵とに基づいた演算により求める。

【００１６】

このような請求項４においては、エージェントが現在において位置する前記防御サーバを前記ルール関数と前記ルール鍵とに基づいた演算により求めている。

【００１７】

また、請求項５に記載の本発明は、請求項４において、前記エージェント管理装置は、前記演算により求めた前記防御サーバに前記エージェントが位置していない場合に、この防御サーバへ前記エージェントが移動する前もしくは後に移動する予定の他の防御サーバを前記演算により求め、もって前記エージェントが現在において位置する防御サーバを検索し求めることを主旨とする。

【００１８】

このような請求項５に記載の本発明は、演算により求めた防御サーバにエージェントが位置していない場合に、この防御サーバへエージェントが移動する前もしくは後に移動する予定の他の防御サーバを演算により求めることにより、エージェントが現在において位置する防御サーバを検索し特定している。

【００１９】

また、請求項６に記載の本発明は、請求項１～５のいずれかにおいて、前記防御サーバ

は、前記エージェントと前記情報所有者とを照会して認証を行うことを主旨とする。

【００２０】

このような請求項６においては、防御サーバでエージェントと情報所有者とを照会して認証を行っている。

【００２１】

また、請求項７に記載の本発明は、請求項１～６のいずれかにおいて、前記ルール鍵は、前記エージェントの移動開始時刻および移動毎の移動タイミング時間とを含むことを主旨とする。

【００２２】

このような請求項７においては、ルール鍵がエージェントの移動開始時刻および移動毎の移動タイミング時間とを含んでいる。

【００２３】

また、請求項８に記載の本発明は、請求項１～７のいずれかにおいて、前記エージェントは、前記エージェント管理装置からの帰還命令に基づいて前記エージェント管理装置に帰還するとともに自身が所持する前記情報を前記情報所有者に提示することを主旨とする。

【００２４】

このような請求項８においては、エージェントがエージェント管理装置からの帰還命令に基づいてエージェント管理装置に帰還するとともに、自身が所持する情報を情報所有者に提示する。

【００２５】

また、請求項９に記載の本発明は、ネットワーク上に保管された情報所有者の情報を不正アクセスによる盗難から防御するためのエージェント制御方法であって、前記ネットワーク上に互いに通信可能に配置された複数の防御サーバにより互いに前記通信を行うステップと、前記情報を所持して前記防御サーバ間を移動するエージェントにより前記情報を移動させるステップと、前記エージェントが所持し前記移動を決定するためのルール関数により前記移動を決定するステップと、前記ルール関数の初期値と係数とを含むルール鍵により前記初期値と前記係数とを取得するステップと、前記ルール鍵に基づき前記エージェントの管理を行うためのエージェント管理装置により前記エージェントの管理を行うステップと、を有し、もって前記エージェントの前記防御サーバ間における移動を制御することを主旨とする。

【００２６】

このような請求項９においては、ネットワーク上に保管された情報所有者の情報を不正アクセスによる盗難から防御するためのエージェント制御方法を実現するために、前記ネットワーク上に互いに通信可能に配置された複数の防御サーバにより互いに前記通信を行うステップと、前記情報を所持して前記防御サーバ間を移動するエージェントにより前記情報を移動させるステップと、前記エージェントが所持し前記移動を決定するためのルール関数により前記移動を決定するステップと、前記ルール関数の初期値と係数とを含むルール鍵により前記初期値と前記係数とを取得するステップと、前記ルール鍵に基づき前記エージェントの管理を行うためのエージェント管理装置により前記エージェントの管理を行うステップと、を有し、もって前記エージェントの前記防御サーバ間における移動を制御している。

【発明の効果】

【００２７】

本発明によれば、情報の保管場所をエージェントにより随時変更することができ、情報への攻撃に対して情報の位置の秘匿を可能とし、また、情報への攻撃が可能な時間を情報の位置での滞在時間内として規制することができ、さらに、複数の防御拠点サーバへ攻撃せざるを得ないので攻撃を難しくすることができ、

また、情報を分割して保管することができるので、一つの分割情報のみから意味や素性が判明することを阻止でき、分割情報に関連した他の分割情報の探索も困難にすることが

可能なエージェント制御システムを提供することができる。
【発明を実施するための最良の形態】
【００２８】
＜第１の実施の形態＞
図１に示すのは、本発明のエージェント制御システムの第１の実施の形態に係る、構成の概要を説明するための説明図である。この図１に示す構成には、図示しないネットワーク上に配置されたサーバから構成される複数の防御サーバ１と、防御サーバ１により保護された情報５と、情報５を伴って移動するエージェント２と、エージェント２が防御サーバ１の間を移動する所定の経路を示す移動経路６と、エージェント２の移動経路６を解読するためのルール鍵３と、情報５を所有する情報所有者（情報端末）４と、が示されている。
【００２９】
この図１に参照される本発明の第１の実施の形態においては、エージェント２に情報５を持たせ、図示しないネットワークに接続された不正アクセス防御箇所（防御サーバ＝サーバ）である複数の防御サーバ１の間において、所定の経路である移動経路６に従って移動させることにより、情報５に対する攻撃や窃盗を目的とした不正アクセスを阻止している。
【００３０】
情報５を保管場所である防御サーバ１間において所定の経路で移動させるために、情報所有者４と情報５を移動させるエージェント２との間で移動経路６に係る移動ルールを定めている。この移動ルールを、情報５に不正にアクセスしようとする不正アクセス者に対して容易に見破ることができない移動ルールを適用することにより、エージェント２の過去の移動経路と予定する移動経路とを不正アクセス者が推定することを困難にしている。
【００３１】
この移動ルールを構成するための手法として、図２中に示した（イ）、（ロ）、（ハ）に参照されるように、僅かな初期値の違いや係数の違いで出力結果が異なり、一方向関数である関数の出力結果を離散化することによりエージェントの経路順序を示す数列の作成方法がある。
【００３２】
この作成方法により、一方向性を持ち、関数の係数特定が難しく、将来の値の予測も困難な移動ルールにより移動経路６を構成することが可能になる。この関数には数学的に従来から保障されているものを用いることを考える。
【００３３】
図２の(イ)に参照されるように、ここで用いる一方向性の関数は既知のハッシュ関数、ＭＤ５、カオス関数、などであり、（イ）においてはカオス関数（ロジスティック関数）「Ｘｎ＋１＝ＣＸｎ（１－Ｘｎ）」をルール関数に適用している。このルール関数に対して、その係数「Ｃ」および初期値「ｘ１」をルール鍵３とし、これを情報所有者４とエージェント間で移動の始めに取り交わすこととする。ルール鍵３をルール関数に適用し、移動経路が演算により作成され、例えば（ロ）に示すような一方向の数列「４．１→８．４→９．６→５．３→１０．１・・・・・・７．６→３．１」が作成される。このような数列に対して（ハ）に示すように、（ロ）に示した数値を四捨五入して離散化が実行され「４→８→９→５→１０・・・・・・７→３」といった一方向の数列へ処理され、この数列をもって予測不能な移動先ノードＩＤとして作成している。
【００３４】
このルール鍵３により情報所有者４は、任意にエージェント２の現在位置を把握することができ、一方、不正アクセス者にとってはルール鍵３を所持しないのでエージェント２の現在位置を把握することは困難である。
【００３５】
また、不正アクセス者は、あるエージェントの移動経路の一部を入手できたとしても関数の一方向性から、エージェントの過去の移動経路の全て、およびエージェントの出所の

特定が困難であり、また、経路は離散化した値であるため将来の移動経路の推定が困難である。

【００３６】

図３に示すのは、本発明のエージェント制御システムの第１の実施の形態に係る、エージェント制御の概要を説明するための説明図である。この図３に示す構成には、エージェント管理装置１１と、情報所有者４と、情報所有者Ｂ１６と、情報所有者Ｘ１７と、ルール鍵３と、ネットワーク１５と、複数の防御サーバ１と、情報５と、情報Ａ７と、情報Ｘ８と、情報Ｂ９と、ルール関数１０と、エージェント２と、移動経路６と、が示されている。

【００３７】

次に、個々の構成の動作を説明する。まず、防御サーバ１はネットワーク１５上に複数が配置されており、他の同構成の防御サーバとの間でネットワーク１５を介した通信を可能としている。防御サーバ１と他の防御サーバとの間でエージェント２が移動しており、エージェント２と情報所有者の認証が防御サーバ１にて行われる。さらに防御サーバ１に他の防御サーバから移動してきたエージェント２に対して、活性化が行われる。

【００３８】

次に、エージェント２は、情報所有者４の情報５を所持し、さらにルール鍵３により決定されるルール関数１０を所持している。また、情報所有者４の指示に基づいて情報５を情報所有者４に対して提示する。また、ルール関数１０に従い移動経路を演算により求めて自身が次に移動する先の防御サーバを決定し、エージェント２自身が現在滞在している防御サーバに対して、決定した次の移動先の防御サーバへの移動依頼を行う。

【００３９】

次に、エージェント管理装置１１は、エージェント２の作成を行い、作成したエージェント２と情報所有者４との間に介在して通信を可能にしている。また、ルール鍵３に基づいたルール関数１０により演算を実行し、エージェント２の現在の位置を把握するための位置情報を取得する。また、このエージェント管理装置１１は情報所有者４が唯一に管理している。

【００４０】

ルール関数１０は、既に図２を参照して説明したように、僅かな初期値の違いや係数の違いで出力結果が異なり、一方向関数が適用されている。また、ルール鍵３についても図２に参照されるように、ルール関数１０に適用する初期値と係数により構成されている。

【００４１】

以上は情報所有者４と情報５の一対一の関係について説明したが、図３に参照されるように情報Ａ７と情報５の２つの情報をエージェント管理装置１１で管理することもできる。この場合に管理される情報は、例えば図示しない元の情報を情報Ａ７と情報５の２つに分割してそれぞれ複数のエージェント２に所持させる方法である。もちろん図示しない元の情報を情報Ａ７と情報５の２分割にすることに限定せずに、３分割や４分割といった任意の分割数に分けてもよい。

【００４２】

なお、ネットワーク１５に情報所有者４以外の情報所有者Ｂ１６や更に多くの情報所有者（例えばＸ人）が接続している場合においても、情報所有者４、情報所有者Ｂ１６、更に多くの情報所有者Ｘ１７のそれぞれの情報を同時に独立して管理することができる。例えば、情報所有者Ｂ１６の所有する情報Ｂ９と、情報所有者Ｘ１７の所有する情報Ｘ８とを、互いに干渉することなくそれぞれ独立に管理することができる。

【００４３】

次に、本発明の第１の実施の形態のエージェント制御システムにおける、「エージェントの作成」、「エージェントの移動」、「エージェントの検索」、「エージェントの帰還」の４種類の制御について、図４、図５、図６をそれぞれ参照して説明する。

【００４４】

まず、図４に示すのは、本発明のエージェント制御システムの第１の実施の形態に係る

、エージェント管理装置と防御サーバとエージェントの構成を説明するための説明図である。この図４に示す構成には、エージェント管理装置１１と、防御サーバ１と、エージェント２とが示されている。また、エージェント管理装置１１は、エージェント位置計算機能２１と、エージェント作成機能２２と、エージェント送受信機能２３と、防御サーバリスト２４とを有している。

【００４５】

また、防御サーバ１は、エージェントアクセス認証機能２７と、エージェント送受信機能２８と、エージェント活性化機能２９とを有している。さらに、エージェント２は、移動先決定機能３０と、情報保管機能３１と、エージェント内部データ３２とを有している。

【００４６】

また、図５に示すのは、本発明のエージェント制御システムの第１の実施の形態に係る、エージェント内部データが有するルール関数データとルール鍵データの構成を説明するための説明図である。

【００４７】

また、図６に示すのは、本発明のエージェント制御システムの第１の実施の形態に係る、構成装置相互の動作を説明するためのシーケンス図であり、情報所有者４と、エージェント管理装置１１と、エージェント２と、防御サーバ１と、防御サーバＮ２０とが示されている。

【００４８】

以上の図４～図６を参照して、まず、本発明の第１の実施の形態によるエージェントの作成について説明する。

【００４９】

最初に、図６中のステップＳ１において、エージェント２の作成が行われる。このエージェント２の作成は、エージェント管理装置１１において実行され、この際に情報所有者４に指示に基づいた複数個のエージェント２を作成することも可能である。

【００５０】

このエージェント２の作成は、図４に参照されるように、エージェント管理装置１１におけるエージェント作成機能２２により実行される。また、このエージェント２の作成に伴って、エージェント２に保管するエージェント内部データ３２も同時に作成され、さらに、作成したエージェント２をエージェント送受信機能２３へ送出する。

【００５１】

なお、エージェント内部データ３２には図５に参照されるようにルール関数データ３３とルール鍵データ３４とを含んでいる。このうちルール関数データ３３には、本発明のエージェント制御システムにおいて適用されるルール関数の様式が所持されている。なお、ここで示すルール関数データ３３は、本発明の第１の実施の形態を説明するための一例であって、カオス関数の一種であるロジスティック関数の様式を示している。

【００５２】

またルール鍵データ３４には、本発明のエージェント制御システムにおいて適用されるルール関数の初期値および係数が所持されている。さらに、エージェント２の移動開始時刻と移動毎の移動タイミング時刻をも有し構成されている。

【００５３】

次に、ステップＳ２において、ステップＳ１にて作成したエージェント２に必要な情報を入力する。このエージェント２への情報５の入力は、情報所有者４が実行し、この際に入力する情報５を任意の複数個に分割して、それぞればらばらに複数個のエージェントへ入力することも可能である。なお、ここで入力する情報５は、図４に参照されるエージェント内部データ３２に対応している。

【００５４】

次に、ステップＳ３において、図１および図３に参照されるルール鍵３の入力が行われる。ここで入力されるルール鍵３は情報所有者４により決定され、エージェント２へ渡さ

れる。

【００５５】

次に、ステップＳ４において、移動タイミングの入力が情報所有者４によって行われる。ここで入力されるのは、エージェント２が移動するタイミングを指示するためのものであり、例えば何時間おきに移動するかといった情報である。

【００５６】

なお、移動タイミングの入力に代えてルール関数１０を適用して移動タイミングを演算して求め、この演算結果を移動タイミングとして適用することもできる。この場合においても図２に示したように、ルール関数１０とルール鍵３との組み合わせで、移動経路の代わりに移動タイミングとして用いる数列を求め、この数列を四捨五入により離散化して移動タイミングとして用いることができる。

【００５７】

次に、ステップＳ５において、エージェント２が任意に選択された防御サーバ１へ移動される。この移動はエージェント管理装置１１によって実行され、防御拠点サーバとなる防御サーバ１へエージェント２が移動する。

【００５８】

こうしたステップＳ２～ステップＳ５におけるエージェント２の移動は、図４に参照されるエージェント送受信機能２３によって実行される。エージェント作成機能２２から送出されたエージェント２を受けてコード化し、防御サーバ１へ通信を介して送出する。また、防御サーバ１から帰還してくるエージェント２を受信し、エージェント内部データ３２の保管情報を取り出す。

【００５９】

以上説明したステップＳ１～ステップＳ５により「エージェントの作成」が実行される。

【００６０】

次に、図４～図８を参照して、本発明の第１の実施の形態による「エージェントの移動」について説明する。

【００６１】

図６のステップＳ６において、防御拠点サーバである防御サーバ１に移動したエージェント２が起動（活性化）される。この活性化は、図４に参照されるエージェント活性化機能２９によって実行され、エージェント送受信機能２８から送出されるコード化されたエージェント２のコードに基づいて活性化される。

【００６２】

次に、ステップＳ７において、エージェント２が起動したことに伴い、防御サーバ１からエージェント２が移動する先が決定される。エージェント２は、図７に参照されるフロー図に従って決定された新たな防御サーバへ移動する。

【００６３】

この図７に参照されるフロー図にはステップＳ２０～ステップＳ２８までの処理ステップが示されており、このうちステップＳ２０～ステップＳ２２までの処理ステップにおいてエージェント２に情報所有者４から情報５が付与され、さらにルール鍵３も付与される。ここまでの処理ステップを経た後に、エージェント２の移動先の決定がステップＳ２３から開始される。

【００６４】

ステップＳ２３において、活性化された状態のエージェント２に対し、次のステップＳ２４において次に移動する先の防御サーバが決定される。この決定はルール鍵３により決められるルール関数１０（図３参照）に従って移動経路を演算し、次にエージェント２が移動する先の防御サーバが決定される。ここでは、ルール関数１０の演算による出力結果を四捨五入で整数に離散化し、この離散化した値が次の防御拠点サーバのＩＤもしくは登録番号を直接に指定するものとしている。

【００６５】

なお、エージェント２には、図４に参照されるように、その内部に移動先決定機能３０と情報保管機能３１とを備えている。

【００６６】

このうち、移動先決定機能３０は、受信したエージェント２のエージェント内部データ３２に基づき、このエージェント内部データ３２が有するルール鍵データとルール関数データとを取得する。この取得を実行した後にエージェント２の次の移動先を決定して、エージェント送受信機能２８に移動先を送出する。

【００６７】

また、情報保管機能３１は、エージェントアクセス認証機能２７からの認証要求を受けてエージェント内部データ３２が有する認証データを取得して返信する。また、エージェント作成機能２２において新規にエージェント２が作成される際に、このエージェント２についてのエージェント内部データを同時に作成する。なお、ここで作成されるエージェント内部データは、図４に参照されるエージェント内部データ３２と同様のデータを有して構成されている。

【００６８】

また、エージェント２の移動先として決定される防御サーバ１は、その内部に図４に参照されるようにエージェントアクセス認証機能２７とエージェント送受信機能２８とを備えている。

【００６９】

このうち、エージェントアクセス認証機能２７は、その認証機能を実行するためにエージェント管理装置１１からの通信を受信してエージェント２が備える情報保管機能３１にアクセスする。このアクセスにより情報保管機能３１は、エージェント内部データ３２が有する認証データを適用してエージェント管理装置１１からのアクセスを認証し、その結果をエージェント管理装置１１へ返信する。この返信において、認証が不可であった場合は該当するエージェント２がこの防御サーバ１には存在していないとしてエージェント管理装置１１に認識される。

【００７０】

また、エージェント送受信機能２８は、エージェント管理装置１１からの通信を受信し、この通信に含まれるエージェント２のエージェントコードを取得してエージェント活性化機能２９へ送る。また、エージェント２が有する移動先決定機能３０からエージェント２の次の移動先の防御サーバを指示されると、この指示に従いエージェント２をコード化してエージェント管理装置１のエージェント送受信機能２３を介し、次の移動先の防御サーバへコード化されたエージェント２を送出する。

【００７１】

ここで、図８に示すフロー図を参照して、ステップＳ２４におけるルール関数１０の使用について説明する。まず、ルール関数１０は既に説明したステップＳ３において、情報所有者４がルール鍵３をエージェント２へ入力することに伴って、ステップＳ３０にてルール関数１０の作成が開始される。

【００７２】

次に、ステップＳ３１にて、入力されたルール鍵３により決められる係数でルール関数１０を作成する。次に、ステップＳ３２にて、エージェント２の移動が最初の移動なのか否かが判断され、最初の移動である（Ｙ）場合はステップＳ３３に進み、ルール関数１０にルール鍵３により決められる初期値Ｘ１を入力する。

【００７３】

また、ステップＳ３２における判断でエージェント２の移動が最初の移動でないと判断（Ｎ）されると、ステップＳ３４に進む。ステップＳ３４では、エージェント２が所持しているルール関数の出力結果X_{new}をX_{old}としてルール関数に入力する。

【００７４】

次に、ステップＳ３３もしくはステップＳ３４を経た処理は、ステップＳ３５へ進む。ステップＳ３５では、ルール関数１０の出力結果X_{new}をエージェント２にて所持する

。

【００７５】

次に、ステップＳ３６では、ルール関数１０の出力結果を四捨五入して離散化し、その結果を基に次の移動先を決定する。ステップＳ３６を終了すると、再びステップＳ３２へ戻り、同様の処理が繰り返される。このように、ルール関数１０の演算による出力結果はエージェント２で所持され、次の移動先でのルール関数の入力として用いられることとなる。

【００７６】

再び図７を参照し、ステップＳ２５において情報所有者４からの情報５の提示の指示があるか否かが判断される。ここで、指示があれば（Ｙ）ステップＳ２７において情報所有者４からの指示に従い情報５の提示が実行された後に、ステップＳ２８にて一連の動作が終了する。

【００７７】

一方、ステップＳ２５にて情報所有者４からの情報提示の指示が確認されない（Ｎ）場合は、ステップＳ２６へ処理が進む。このステップＳ２６においては、現在滞在する防御サーバに対して、次の移動先の防御サーバへ移動するための移動依頼を発する。この後にステップＳ２３へ戻り、同様の処理が繰り返される。

【００７８】

再び図６を参照し、ステップＳ８において、エージェント２の移動依頼を防御サーバ２へ要求し、防御サーバ２は、ステップＳ４で入力された移動タイミングに従ってステップＳ７で決定された移動先の新たな防御サーバＮ２０へエージェント２を移動させる。

【００７９】

以上説明したステップＳ６～ステップＳ８により「エージェントの移動」が実行される。

【００８０】

次に、本発明の第１の実施の形態による「エージェントの検索」について説明する。

【００８１】

図６のステップＳ９において、エージェント２の検索が実行される。情報所有者４は、エージェント２の現在位置を把握しておくためや、あるいはエージェント２が所持している情報を提示してもらうために検索を実行する。この検索はエージェント管理装置１１にて行われ、情報所有者４がエージェント管理装置１１へルール鍵３と移動タイミングを入力することで検索が実行される。

【００８２】

次に、ステップＳ１０において、エージェント２の現在位置を求める演算がエージェント管理装置１１において実行される。エージェント管理装置１１では、エージェント２が最初に防御拠点サーバ（防御サーバ１）に送り出された時刻と現在時刻、移動タイミングからエージェント２の移動回数を計算して、この移動回数とルール鍵３が示すルール関数１０とによりエージェント２の現在位置を演算して求める。

【００８３】

次に、ステップＳ１１において、エージェント２の現在位置の確認が実行される。エージェント管理装置１１は、ステップＳ１０で演算され求められたエージェント２の現在位置に従い、この現在位置に該当する防御拠点サーバと通信し、エージェント２が実際に存在しているか否かを確認する。この確認においては、エージェント２の移動回数とルール関数１０が予め分かっているので、ほぼ演算した結果に従った位置にエージェント２が存在していることが確認される。また、仮に、演算により求められたエージェント２の移動回数と、実際の移動回数との間で誤差が生じたとしても、演算結果の回数の前後の値の回数で存在すると思われる位置にてエージェント２の存在の有無を確認すればよい。

【００８４】

このようなステップＳ１１の処理は、図４に参照されるエージェント位置計算機能２１によって実行される。防御サーバリスト２４の中からルール鍵データとルール関数データ

を抽出し、これらに基づいてエージェント２が現在滞在している防御サーバを演算により特定する。次に、防御サーバリスト２４の中から特定した防御サーバに向けてエージェント２の位置確認のための通信を実行する。この通信において、防御サーバリスト２４に含まれる認証鍵を認証データとして同時に送信する。

【００８５】

以上説明したステップＳ９～ステップＳ１２により「エージェントの検索」が実行される。

【００８６】

次に、本発明の第１の実施の形態による「エージェントの帰還」について説明する。

【００８７】

図６のステップＳ１２において、エージェント管理装置１１は、ステップＳ１１で位置確認したエージェント２の現在位置を情報所有者４に提示する。

【００８８】

次に、ステップＳ１３において、情報所有者４がエージェント２の移動を中止させるか、あるいはエージェント２が所持する情報の内容を確認するために、エージェント２をエージェント管理装置１１へ戻るように帰還命令を発する。この帰還命令は情報所有者４がエージェント管理装置１１に直接に指示する。

【００８９】

次に、ステップＳ１４において、エージェント管理装置１１は情報所有者４から指示された帰還命令に従い、エージェント２の現在位置を既に説明したステップＳ１０における演算により求め、エージェント２が現在位置する防御サーバを特定し、その防御サーバに滞在するエージェント２に帰還命令を発行する。

【００９０】

次に、ステップＳ１５において、帰還命令を受けたエージェント２はエージェント管理装置１１へ帰還し、自身が所持している情報５を情報所有者４に提示し、その後にエージェント２は消滅する。

【００９１】

以上説明したステップＳ１２～ステップＳ１５により「エージェントの移動」が実行される。

【００９２】

＜第２の実施の形態＞

図９に示すのは、本発明のエージェント制御システムの第２の実施の形態に係る、ルール関数データとルール鍵データの構成を説明するための説明図である。この図９に示す構成は、すでに本発明の第１の実施の形態における図６のステップ３に適用するルール関数データ４０とルール鍵データ４１である。ルール関数データ４０は図５に示したルール関数データ３３と同じ構成であり、一方、ルール鍵データ４１はルール鍵データ３４の構成に加えて最大移動回数を表すデータが増えている。

【００９３】

図６におけるステップ３において、エージェント２の移動回数が最大移動回数に一致したら、その一致に基づいて情報所有者４へ情報５を提示する。第１の実施の形態においては、エージェント２が所持している情報５は、情報所有者４がエージェント２の現在位置を取得し、帰還命令を発することにより提示されている。これに対して本発明の第２の実施の形態においては、必ずしも情報所有者４の帰還命令によることはなく、他の判断としてルール鍵データ４１が有する最大移動回数とエージェント２の移動回数が一致した時点で、情報５が提示される。

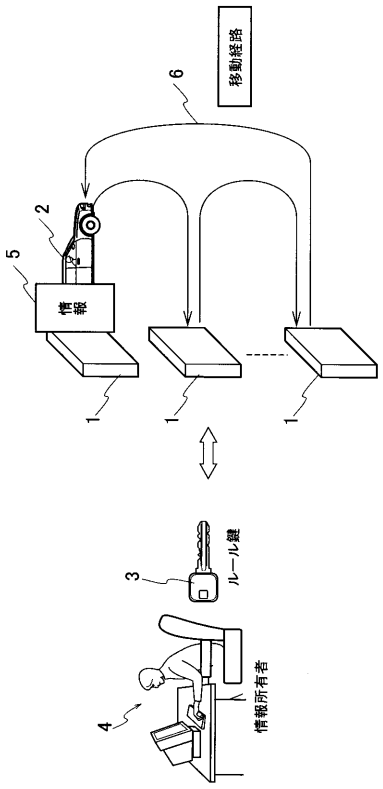
【００９４】

図１０に参照されるフロー図に従ってエージェント２は決定された新たな防御サーバへ移動する。この図１０に参照されるフロー図にはステップＳ４０～ステップＳ４８までの処理ステップが示されており、既に図７に示したフロー図のステップＳ２０～ステップＳ２８にそれぞれ対応している。

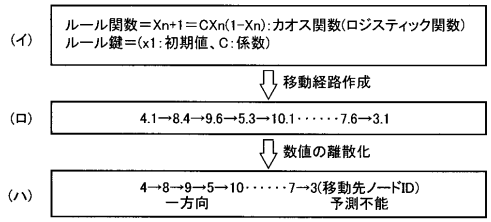
【００９５】
まず、ステップＳ４０～ステップＳ４２までの処理ステップにおいて、図７を参照して説明した処理と同様に、エージェント２に情報所有者４から情報が付与され、さらにルール鍵３も付与される。ここまでの処理ステップを経た後に、エージェント２の移動先の決定がステップＳ４３から開始される。
【００９６】
次に、ステップＳ４３において、活性化された状態のエージェント２に対してステップＳ４４において、次に移動する先の防御サーバが決定される。ここで実行される防御サーバの決定方法は、図７に参照されるステップＳ２４と同様の処理により実行される。
【００９７】
次に、ステップＳ４５において、図７に参照されるステップＳ２５の処理と同様に、情報所有者４からの情報５の提示の指示があるか否かが判断される。さらに本発明の第２の実施の形態においては、このステップＳ４５において、今までの移動回数が予め設定された最大移動回数と一致したか否かの判断も行われる。ここで適用する最大移動回数は、図９に示したルール鍵データ４１が有する最大移動回数のデータである。
【００９８】
このステップＳ４５で、情報提示の指示か、もしくは最大移動回数との一致が確認されると（Ｙ）ステップＳ４７において情報所有者４からの指示に従い情報５の提示が実行された後に、ステップＳ４８にて一連の動作が終了する。
【００９９】
一方、ステップＳ４５にて情報所有者４からの情報提示の指示か、もしくは最大移動回数との一致が確認されない（Ｎ）場合は、ステップＳ４６へ処理が進む。このステップＳ４６においては、現在滞在する防御サーバに対して、次の移動先の防御サーバへ移動するための移動依頼を発する。この後にステップＳ４３へ戻り、同様の処理が繰り返される。
【図面の簡単な説明】
【０１００】
【図１】本発明のエージェント制御システムの第１の実施の形態に係る、構成の概要を説明するための説明図である。
【図２】本発明のエージェント制御システムの第１の実施の形態に係る、一方向関数および関数の出力結果の離散化とエージェントの経路順序を示す数列の作成方法を説明するための説明図である。
【図３】本発明のエージェント制御システムの第１の実施の形態に係る、エージェント制御の概要を説明するための説明図である。
【図４】本発明のエージェント制御システムの第１の実施の形態に係る、エージェント管理装置と防御サーバとエージェントの構成を説明するための説明図である。
【図５】本発明のエージェント制御システムの第１の実施の形態に係る、エージェント内部データが有するルール関数データとルール鍵データの構成を説明するための説明図である。
【図６】本発明のエージェント制御システムの第１の実施の形態に係る、構成装置相互の動作を説明するためのシーケンス図である。
【図７】本発明のエージェント制御システムの第１の実施の形態に係る、エージェントの防御サーバへの移動を説明するためのフロー図である。
【図８】本発明のエージェント制御システムの第１の実施の形態に係る、ルール関数の使用について説明するためのフロー図である。
【図９】本発明のエージェント制御システムの第２の実施の形態に係る、ルール関数データとルール鍵データの構成を説明するための説明図である。
【図１０】本発明のエージェント制御システムの第２の実施の形態に係る、エージェントの防御サーバへの移動を説明するためのフロー図である。
【符号の説明】
【０１０１】

1　防御サーバ
2　エージェント
3　ルール鍵
4　情報所有者
5　情報
6　移動経路
１１　エージェント管理装置
１５　ネットワーク
２１　エージェント位置計算機能
２２　エージェント作成機能
２３　エージェント送受信機能
２４　防御サーバリスト
２７　エージェントアクセス認証機能
２８　エージェント送受信機能
２９　エージェント活性化機能
３０　移動先決定機能
３１　情報保管機能
３２　エージェント内部データ
３３　ルール関数データ
３４　ルール鍵データ

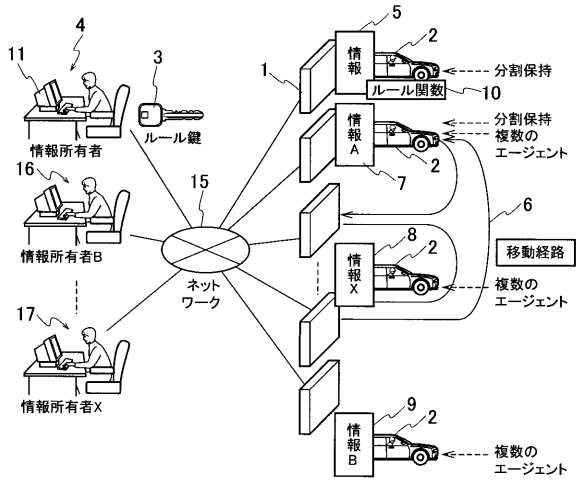
【図１】



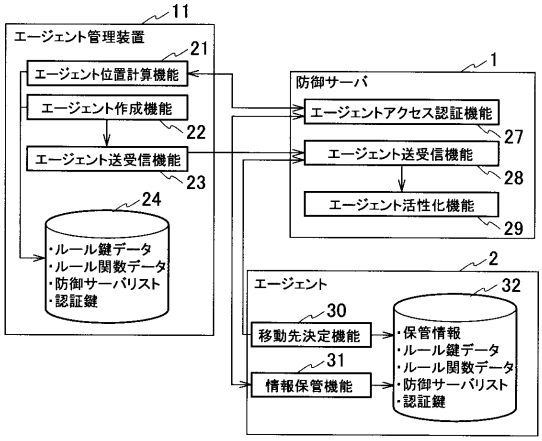
【図２】



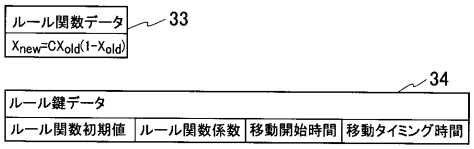
【図３】



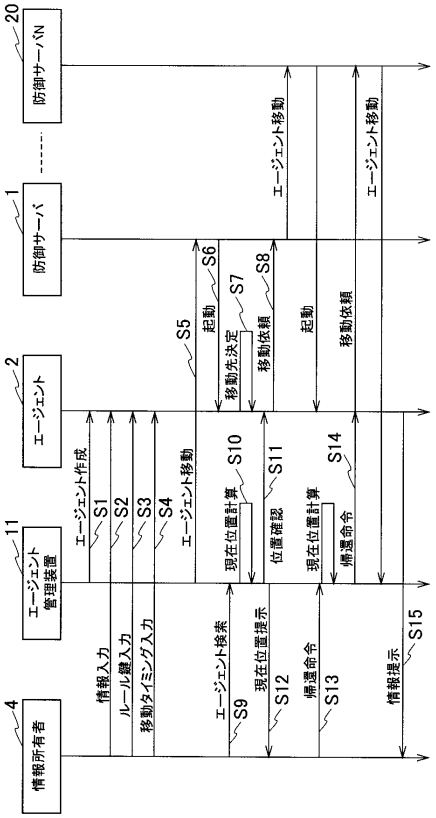
【図４】



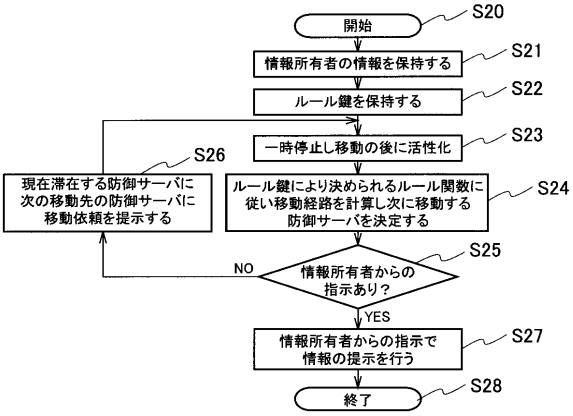
【図５】



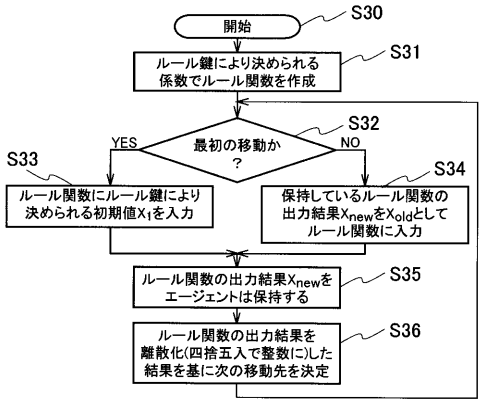
【図６】



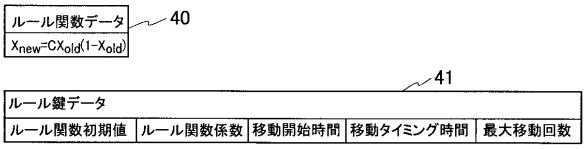
【図７】



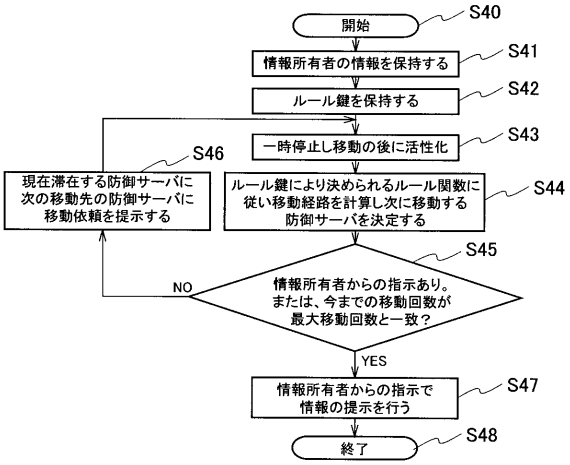
【図８】



【図９】



【図１０】



フロントページの続き

Ｆターム(参考) 5B017 AA03 BA07 BA10 BB07 CA15 CA16
5B045 BB48 GG01 JJ35
5B085 AE00