

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4547597号
(P4547597)

(45) 発行日 平成22年9月22日(2010.9.22)

(24) 登録日 平成22年7月16日(2010.7.16)

(51) Int.Cl.		F I			
G06F 21/20	(2006.01)	G06F 15/00	330C		
G06F 13/00	(2006.01)	G06F 13/00	650B		
H04L 9/32	(2006.01)	H04L 9/00	675A		

請求項の数 12 (全 35 頁)

(21) 出願番号	特願2003-281479 (P2003-281479)	(73) 特許権者	000002185
(22) 出願日	平成15年7月29日(2003.7.29)		ソニー株式会社
(65) 公開番号	特開2005-50129 (P2005-50129A)		東京都港区港南1丁目7番1号
(43) 公開日	平成17年2月24日(2005.2.24)	(74) 代理人	100082131
審査請求日	平成18年6月1日(2006.6.1)		弁理士 稲本 義雄
		(72) 発明者	小澤 武史
			東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(72) 発明者	青木 幸彦
			東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(72) 発明者	河野 真一
			東京都品川区北品川6丁目7番35号 ソニー株式会社内

最終頁に続く

(54) 【発明の名称】 情報処理システム、情報処理装置および方法、記録媒体、並びにプログラム

(57) 【特許請求の範囲】

【請求項1】

ネットワークを介して相互に接続される第1の情報処理装置と第2の情報処理装置とを備える情報処理システムにおいて、

前記第1の情報処理装置は、

インスタントメッセージングシステムを介した、前記第2の情報処理装置の前記ネットワークのアドレスと、前記第2の情報処理装置により生成された鍵とを含むメッセージの受信を制御する第1の受信制御手段と、

前記インスタントメッセージングシステムにおいて用いられる前記第1の情報処理装置を特定する特定情報、および前記鍵を、前記ネットワークを介して前記第2の情報処理装置に送信させ、前記第2の情報処理装置に所定の処理の実行を要求する送信制御手段とを備え、

前記第2の情報処理装置は、

前記第1の情報処理装置からの前記所定の処理の実行の要求を受け付けるか否かを示す受付判定情報、前記インスタントメッセージングシステムを介して取得した前記特定情報、および前記鍵を対応付けて記録する記録手段と、

前記ネットワークを介して、前記第1の情報処理装置から送信されてきた、前記特定情報および前記鍵の受信を制御する第2の受信制御手段と、

前記記録手段に記録されている前記受付判定情報、前記特定情報、および前記鍵と、前記第1の情報処理装置から受信した前記特定情報および前記鍵とに基づいて、前記第1

10

20

の情報処理装置が、前記インスタントメッセージングシステムに登録され、かつ前記所定の処理の実行の要求を受け付ける相手であるか否かを判定する判定手段と、

前記判定手段による判定結果に応じて、前記所定の処理を実行する実行手段とを備えることを特徴とする情報処理システム。

【請求項 2】

インスタントメッセージングシステムにネットワークを介して接続される情報処理装置において、

他の情報処理装置からの所定の処理の実行の要求を受け付けるか否かを示す受付判定情報、前記インスタントメッセージングシステムを介して取得した、前記インスタントメッセージングシステムにおいて用いられる前記他の情報処理装置を特定する特定情報、および前記情報処理装置により生成され、前記インスタントメッセージングシステムを介して前記他の情報処理装置に送信された鍵を対応付けて記録する記録手段と、

前記ネットワークを介して前記他の情報処理装置から送信されてきた、前記特定情報および前記鍵を含む、前記所定の処理の実行の要求の受信を制御する受信制御手段と、

前記記録手段に記録されている前記受付判定情報、前記特定情報、および前記鍵と、前記他の情報処理装置から受信した前記特定情報および前記鍵とに基づいて、前記他の情報処理装置が、前記インスタントメッセージングシステムに登録され、かつ前記所定の処理の実行の要求を受け付ける相手であるか否かを判定する判定手段と、

前記判定手段による判定結果に応じて、前記所定の処理を実行する実行手段とを備えることを特徴とする情報処理装置。

【請求項 3】

前記受信制御手段は、前記インスタントメッセージングシステムを介した、前記他の情報処理装置からの認証を要求する第 1 のメッセージの受信をさらに制御し、

前記判定手段は、前記第 1 のメッセージに含まれている前記特定情報が、前記記録手段に記録されているか否かを判定するとともに、前記記録手段に前記特定情報と対応付けて記録されている前記受付判定情報を基に、前記他の情報処理装置からの前記所定の処理の実行の要求を受け付けるか否かをさらに判定し、

前記第 1 のメッセージに含まれている前記特定情報が前記記録手段に記録され、かつ、前記他の情報処理装置からの前記所定の処理の実行の要求を受け付けると判定された場合、前記鍵を生成する鍵生成手段と、

前記インスタントメッセージングシステムを介した、自己のアドレスおよび前記鍵を含む第 2 のメッセージの前記他の情報処理装置への送信を制御する送信制御手段と

をさらに備えることを特徴とする請求項 2 に記載の情報処理装置。

【請求項 4】

受信制御手段は、少なくともいずれか一方が暗号化されている前記特定情報および前記鍵を含む、前記所定の処理の実行の要求の受信を制御し、

暗号化されている前記特定情報または前記鍵を復号する復号手段をさらに備えることを特徴とする請求項 2 に記載の情報処理装置。

【請求項 5】

インスタントメッセージングシステムにネットワークを介して接続される情報処理装置の情報処理方法において、

他の情報処理装置からの所定の処理の実行の要求を受け付けるか否かを示す受付判定情報、前記インスタントメッセージングシステムを介して取得した、前記インスタントメッセージングシステムにおいて用いられる前記他の情報処理装置を特定する特定情報、および前記情報処理装置により生成され、前記インスタントメッセージングシステムを介して前記他の情報処理装置に送信された鍵を対応付けて記録手段に記録させる記録制御ステップと、

前記ネットワークを介して前記他の情報処理装置から送信されてきた、前記特定情報および前記鍵を含む、前記所定の処理の実行の要求の受信を制御する受信制御ステップと、

前記記録手段に記録されている前記受付判定情報、前記特定情報、および前記鍵と、前

10

20

30

40

50

記他の情報処理装置から受信した前記特定情報および前記鍵とに基づいて、前記他の情報処理装置が、前記インスタントメッセージングシステムに登録され、かつ前記所定の処理の実行の要求を受け付ける相手であるか否かを判定する判定ステップと、

前記判定ステップの処理による判定結果に応じて、前記所定の処理を実行する実行ステップと

を含むことを特徴とする情報処理方法。

【請求項 6】

インスタントメッセージングシステムにネットワークを介して接続される情報処理装置に、

他の情報処理装置からの所定の処理の実行の要求を受け付けるか否かを示す受付判定情報、前記インスタントメッセージングシステムを介して取得した、前記インスタントメッセージングシステムにおいて用いられる前記他の情報処理装置を特定する特定情報、および前記情報処理装置により生成され、前記インスタントメッセージングシステムを介して前記他の情報処理装置に送信された鍵を対応付けて記録手段に記録させる記録制御ステップと、

前記ネットワークを介して前記他の情報処理装置から送信されてきた、前記特定情報および前記鍵を含む、前記所定の処理の実行の要求の受信を制御する受信制御ステップと、

前記記録手段に記録されている前記受付判定情報、前記特定情報、および前記鍵と、前記他の情報処理装置から受信した前記特定情報および前記鍵とに基づいて、前記他の情報処理装置が、前記インスタントメッセージングシステムに登録され、かつ前記所定の処理の実行の要求を受け付ける相手であるか否かを判定する判定ステップと、

前記判定ステップの処理による判定結果に応じて、前記所定の処理を実行する実行ステップと

を含む処理を実行させることを特徴とするプログラムが記録されている記録媒体。

【請求項 7】

インスタントメッセージングシステムにネットワークを介して接続される情報処理装置に、

他の情報処理装置からの所定の処理の実行の要求を受け付けるか否かを示す受付判定情報、前記インスタントメッセージングシステムを介して取得した、前記インスタントメッセージングシステムにおいて用いられる前記他の情報処理装置を特定する特定情報、および前記情報処理装置により生成され、前記インスタントメッセージングシステムを介して前記他の情報処理装置に送信された鍵を対応付けて記録手段に記録させる記録制御ステップと、

前記ネットワークを介して前記他の情報処理装置から送信されてきた、前記特定情報および前記鍵を含む、前記所定の処理の実行の要求の受信を制御する受信制御ステップと、

前記記録手段に記録されている前記受付判定情報、前記特定情報、および前記鍵と、前記他の情報処理装置から受信した前記特定情報および前記鍵とに基づいて、前記他の情報処理装置が、前記インスタントメッセージングシステムに登録され、かつ前記所定の処理の実行の要求を受け付ける相手であるか否かを判定する判定ステップと、

前記判定ステップの処理による判定結果に応じて、前記所定の処理を実行する実行ステップと

を含む処理を実行させることを特徴とするプログラム。

【請求項 8】

インスタントメッセージングシステムにネットワークを介して接続される情報処理装置において、

前記インスタントメッセージングシステムを介した、他の情報処理装置の前記ネットワークのアドレスと、前記他の情報処理装置により生成された鍵とを含む第 1 のメッセージの受信を制御する受信制御手段と、

前記アドレスに基づいて、前記インスタントメッセージングシステムにおいて用いられる前記情報処理装置を特定する特定情報、および前記鍵を、前記ネットワークを介して前

10

20

30

40

50

記他の情報処理装置に送信させ、前記他の情報処理装置に所定の処理の実行を要求する送信制御手段と

を備えることを特徴とする情報処理装置。

【請求項 9】

前記送信制御手段は、前記インスタントメッセージングシステムを介した、前記他の情報処理装置宛での、前記第 1 のメッセージの送信および認証を要求する第 2 のメッセージの送信をさらに制御する

ことを特徴とする請求項 8 に記載の情報処理装置。

【請求項 10】

インスタントメッセージングシステムにネットワークを介して接続される情報処理装置の情報処理方法において、

前記インスタントメッセージングシステムを介した、他の情報処理装置の前記ネットワークのアドレスと、前記他の情報処理装置により生成された鍵とを含むメッセージの受信を制御する受信制御ステップと、

前記アドレスに基づいて、前記インスタントメッセージングシステムにおいて用いられる前記情報処理装置を特定する特定情報、および前記鍵を、前記ネットワークを介して前記他の情報処理装置に送信させ、前記他の情報処理装置に所定の処理の実行を要求する送信制御ステップと

を含むことを特徴とする情報処理方法。

【請求項 11】

インスタントメッセージングシステムにネットワークを介して接続される情報処理装置に、

前記インスタントメッセージングシステムを介した、他の情報処理装置の前記ネットワークのアドレスと、前記他の情報処理装置により生成された鍵とを含むメッセージの受信を制御する受信制御ステップと、

前記アドレスに基づいて、前記インスタントメッセージングシステムにおいて用いられる前記情報処理装置を特定する特定情報、および前記鍵を、前記ネットワークを介して前記他の情報処理装置に送信させ、前記他の情報処理装置に所定の処理の実行を要求する送信制御ステップと

を含む処理を実行させることを特徴とするプログラムが記録されている記録媒体。

【請求項 12】

インスタントメッセージングシステムにネットワークを介して接続される情報処理装置に、

前記インスタントメッセージングシステムを介した、他の情報処理装置の前記ネットワークのアドレスと、前記他の情報処理装置により生成された鍵とを含むメッセージの受信を制御する受信制御ステップと、

前記アドレスに基づいて、前記インスタントメッセージングシステムにおいて用いられる前記情報処理装置を特定する特定情報、および前記鍵を、前記ネットワークを介して前記他の情報処理装置に送信させ、前記他の情報処理装置に所定の処理の実行を要求する送信制御ステップと

を含む処理を実行させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理システム、情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、簡単かつ確実に、ネットワークを介して、特定のユーザに対してのみサービスを提供するか、または特定のユーザのみがサービスの提供を受けることができるようにした情報処理システム、情報処理装置および方法、記録媒体、並びにプログラムに関する。

【背景技術】

10

20

30

40

50

【 0 0 0 2 】

ネットワークを介した機能提供サービスが広く利用されている。

【 0 0 0 3 】

FTP (File Transfer Protocol) サーバやHTTP (Hyper Text Transfer Protocol) サーバのような機器にユーザごとにアクセス権を設定しようとした場合、機器の管理者(所有者)は、アクセスを許可するユーザのために、機器上にユーザのアカウントを作成し、パスワードを設定し、ユーザの権限を設定する。さらに、機器の管理者は、作成したアカウントおよびパスワードをユーザに伝える。

【 0 0 0 4 】

インターネットを介して機器を利用するユーザは、管理者から伝えられたアカウントおよびパスワードを覚えておき、機器を利用するとき、その機器のアカウントおよびパスワードを正しく入力する。

10

【 0 0 0 5 】

また、インターネット上のクライアントサービスサーバのサービス利用に先立ち、ユーザが携帯情報端末の固有識別情報を含むユーザ個人情報をクライアントサービスサーバに予め登録し、その後、ユーザが端末を用いてクライアントサービスサーバを経由してコンテンツサーバを利用するシステムが知られている(例えば、特許文献1参照)。このシステムでは、端末は、その暗号化された固有識別情報をクライアントサービスサーバに送信し、クライアントサービスサーバは、暗号化された固有識別情報を復号し、この固有識別情報に基づきユーザの認証を行い、課金代行サービスサーバにおける当該ユーザのユーザ登録の有無を確認し、いずれもOKの場合に、コンテンツサーバによる携帯情報端末のユーザに対するサービスの提供を許可する。

20

【 0 0 0 6 】

【特許文献1】特開2002-64483号公報

【発明の開示】

【発明が解決しようとする課題】

【 0 0 0 7 】

このようなシステムの場合、複数の機器を利用するには、ユーザは、機器ごとのアカウントおよびパスワードを覚えていなければならないという問題があった。

【 0 0 0 8 】

30

そこで、相手との接続のために、例えば、Jabber(商標)のような中央サーバを介するインスタントメッセージングサービスを利用することができる。この場合、相手との全てのやりとりを中央サーバを経由して行うようなアプリケーションプログラムでは、認証のための操作は特に必要とされない。

【 0 0 0 9 】

しかしながら、中央サーバを介したメッセージングを相手とのアドレス交換にのみ利用して、実際のデータ転送や操作を、直接P2P(Peer to Peer)で行うアプリケーションプログラムにおいては、インスタントメッセージングサービス上でアドレスを交換した相手と、直接P2Pで接続してきた相手と同じ相手であるかどうかを確認することができないという問題があった。

40

【課題を解決するための手段】

【 0 0 1 0 】

本発明の情報処理システムは、第1の情報処理装置が、インスタントメッセージングシステムを介した、第2の情報処理装置のネットワークのアドレスと、第2の情報処理装置により生成された鍵とを含むメッセージの受信を制御する第1の受信制御手段と、インスタントメッセージングシステムにおいて用いられる第1の情報処理装置を特定する特定情報、および鍵を、ネットワークを介して第2の情報処理装置に送信させ、第2の情報処理装置に所定の処理の実行を要求する送信制御手段とを備え、第2の情報処理装置が、第1の情報処理装置からの所定の処理の実行の要求を受け付けるか否かを示す受付判定情報、インスタントメッセージングシステムを介して取得した特定情報、および鍵を対応付けて

50

記録する記録手段と、ネットワークを介して、第1の情報処理装置から送信されてきた、特定情報および鍵の受信を制御する第2の受信制御手段と、記録手段に記録されている受付判定情報、特定情報、および鍵と、第1の情報処理装置から受信した特定情報および鍵とに基づいて、第1の情報処理装置が、インスタントメッセージングシステムに登録され、かつ所定の処理の実行の要求を受け付ける相手であるか否かを判定する判定手段と、判定手段による判定結果に応じて、所定の処理を実行する実行手段とを備えることを特徴とする。

【0011】

本発明の第1の情報処理装置は、他の情報処理装置からの所定の処理の実行の要求を受け付けるか否かを示す受付判定情報、インスタントメッセージングシステムを介して取得した、インスタントメッセージングシステムにおいて用いられる他の情報処理装置を特定する特定情報、および情報処理装置により生成され、インスタントメッセージングシステムを介して他の情報処理装置に送信された鍵を対応付けて記録する記録手段と、ネットワークを介して他の情報処理装置から送信されてきた、特定情報および鍵を含む、所定の処理の実行の要求の受信を制御する受信制御手段と、記録手段に記録されている受付判定情報、特定情報、および鍵と、他の情報処理装置から受信した特定情報および鍵とに基づいて、他の情報処理装置が、インスタントメッセージングシステムに登録され、かつ所定の処理の実行の要求を受け付ける相手であるか否かを判定する判定手段と、判定手段による判定結果に応じて、所定の処理を実行する実行手段とを備えることを特徴とする。

【0015】

受信制御手段は、インスタントメッセージングシステムを介した、他の情報処理装置からの認証を要求する第1のメッセージの受信をさらに制御し、判定手段は、第1のメッセージに含まれている特定情報が、記録手段に記録されているか否かを判定するとともに、記録手段に特定情報と対応付けて記録されている受付判定情報を基に、他の情報処理装置からの所定の処理の実行の要求を受け付けるか否かをさらに判定し、第1のメッセージに含まれている特定情報が記録手段に記録され、かつ、他の情報処理装置からの所定の処理の実行の要求を受け付けると判定された場合、鍵を生成する鍵生成手段と、インスタントメッセージングシステムを介した、自己のアドレスおよび鍵を含む第2のメッセージの他の情報処理装置への送信を制御する送信制御手段とをさらに設けることができる。

【0019】

受信制御手段は、少なくともいずれか一方が暗号化されている特定情報および鍵を含む、所定の処理の実行の要求の受信を制御するようにし、暗号化されている特定情報または鍵を復号する復号手段をさらに設けることができる。

【0021】

本発明の第1の情報処理方法、第1の記録媒体のプログラム、または第1のプログラムは、他の情報処理装置からの所定の処理の実行の要求を受け付けるか否かを示す受付判定情報、インスタントメッセージングシステムを介して取得した、インスタントメッセージングシステムにおいて用いられる他の情報処理装置を特定する特定情報、および情報処理装置により生成され、インスタントメッセージングシステムを介して他の情報処理装置に送信された鍵を対応付けて記録手段に記録させる記録制御ステップと、ネットワークを介して他の情報処理装置から送信されてきた、特定情報および鍵を含む、所定の処理の実行の要求の受信を制御する受信制御ステップと、記録手段に記録されている受付判定情報、特定情報、および鍵と、他の情報処理装置から受信した特定情報および鍵とに基づいて、他の情報処理装置が、インスタントメッセージングシステムに登録され、かつ所定の処理の実行の要求を受け付ける相手であるか否かを判定する判定ステップと、判定ステップの処理による判定結果に応じて、所定の処理を実行する実行ステップとを含むことを特徴とする。

【0024】

本発明の第2の情報処理装置は、インスタントメッセージングシステムを介した、他の情報処理装置のネットワークのアドレスと、他の情報処理装置により生成された鍵とを含

10

20

30

40

50

む第1のメッセージの受信を制御する受信制御手段と、アドレスに基づいて、インスタントメッセージングシステムにおいて用いられる情報処理装置を特定する特定情報、および鍵を、ネットワークを介して他の情報処理装置に送信させ、他の情報処理装置に所定の処理の実行を要求する送信制御手段とことを特徴とする。

【0026】

送信制御手段は、インスタントメッセージングシステムを介した、他の情報処理装置宛ての、第1のメッセージの送信および認証を要求する第2のメッセージの送信をさらに制御するようにすることができる。

【0027】

本発明の第2の情報処理方法、第2の記録媒体のプログラム、または第2のプログラムは、インスタントメッセージングシステムを介した、他の情報処理装置のネットワークのアドレスと、他の情報処理装置により生成された鍵とを含むメッセージの受信を制御する受信制御ステップと、アドレスに基づいて、インスタントメッセージングシステムにおいて用いられる情報処理装置を特定する特定情報、および鍵を、ネットワークを介して他の情報処理装置に送信させ、他の情報処理装置に所定の処理の実行を要求する送信制御ステップとを含むことを特徴とする。

10

【0030】

ネットワークとは、少なくとも2つの装置が接続され、ある装置から、他の装置に対して、情報の伝達をできるようにした仕組みをいう。ネットワークを介して通信する装置は、独立した装置どうしであっても良いし、1つの装置を構成している内部ブロックどうし

20

であっても良い。

【0031】

また、通信とは、無線通信および有線通信は勿論、無線通信と有線通信とが混在した通信、即ち、ある区間では無線通信が行われ、他の区間では有線通信が行われるようなものであっても良い。さらに、ある装置から他の装置への通信が有線通信で行われ、他の装置からある装置への通信が無線通信で行われるようなものであっても良い。

【0032】

情報処理装置は、独立した装置であっても良いし、情報処理を行うブロックであっても良い。

【0033】

本発明の情報処理システムにおいては、インスタントメッセージングシステムを介した、第2の情報処理装置のネットワークのアドレスおよび鍵を含むメッセージが受信され、ネットワークを介した、アドレスを基にした、第2の情報処理装置宛ての、インスタントメッセージングシステムの第1の情報処理装置を特定する特定情報および鍵が送信される。そして、ネットワークを介して、第1の情報処理装置から送信されてきた、特定情報および鍵が受信され、特定情報および鍵を基に、第1の情報処理装置が正規の相手であるか否かが判定される。

30

【0034】

本発明の第1の情報処理装置および方法、第1の記録媒体、並びに第1のプログラムにおいては、ネットワークを介して、他の情報処理装置から送信されてきた、インスタントメッセージングシステムの他の情報処理装置を特定する特定情報および鍵が受信され、特定情報および鍵を基に、他の情報処理装置が正規の相手であるか否かが判定される。

40

【0035】

本発明の第2の情報処理装置および方法、第2の記録媒体、並びに第2のプログラムにおいては、インスタントメッセージングシステムを介した、他の情報処理装置のアドレスおよび鍵を含むメッセージが受信され、ネットワークを介した、アドレスを基にした、他の情報処理装置宛ての、インスタントメッセージングシステムのユーザを特定する特定情報および鍵が送信される。

【発明の効果】

【0036】

50

アカウントまたはパスワードなどの入力を要求する必要がなく、かつ、相手が正規の相手であるか否かを、簡単かつ確実に判定することができ、もって、特定の相手に対してのみサービスを提供したり、特定の相手のみがサービスを利用できるようになる。

【発明を実施するための最良の形態】

【0054】

図1は、本発明に係るサービス提供システム11の一実施の形態の構成を示すブロック図である。ユーザ1に所有されるハードディスクレコーダ付きテレビジョン受像装置2は、インターネット3に接続され、インターネット3を介して、ユーザ4に所有されるパーソナルコンピュータ5と接続する。インターネット3は、無線または有線（光ファイバを含む）によるネットワークの一例であり、ローカルエリアネットワーク、または専用回線などを含む。

10

【0055】

ハードディスクレコーダ付きテレビジョン受像装置2は、インスタントメッセージングシステムにより、パーソナルコンピュータ5とメッセージを交換する。

【0056】

インスタントメッセージングシステムは、インスタントメッセージングサービスサーバとしてのサーバ6により構成される。このシステムには、インターネット3を介して、ハードディスクレコーダ付きテレビジョン受像装置2、パーソナルコンピュータ5などのクライアントが所定のタイミングで接続される。インスタントメッセージング機能を提供するプロトコルとしては、Jabber Protocol（商標）が挙げられる。サーバ6は、インスタントメッセージングシステムへのユーザの登録、クライアントのログイン、他のクライアントの状態を示す情報の提供、またはメッセージの転送などのサービスをクライアントに提供する。すなわち、サーバ6は、いわゆる、メッセージングサービス機能を有する。

20

【0057】

インスタントメッセージングシステムのサービスの提供を受ける場合、ユーザ1は、ハードディスクレコーダ付きテレビジョン受像装置2を操作して、インスタントメッセージングシステムにおいて、ユーザ1を特定するインスタントメッセージングIDの取得とパスワードの登録を、サーバ6に要求する。インスタントメッセージングIDを取得し、パスワードが登録された場合、ユーザ1は、インスタントメッセージングIDおよびパスワードをサーバ6に提示することにより、サーバ6に対して、本人であることを証明して、インスタントメッセージングシステムにログインする（そのサービスの提供を受ける）ことができる。

30

【0058】

同様に、ユーザ4は、インスタントメッセージングシステムのサービスの提供を受ける場合、パーソナルコンピュータ5を操作して、インスタントメッセージングシステムにおいて、ユーザ4を特定するインスタントメッセージングIDの取得とパスワードの登録を、サーバ6に要求する。インスタントメッセージングIDを取得し、パスワードが登録された場合、ユーザ4は、インスタントメッセージングIDおよびパスワードをサーバ6に提示することにより、サーバ6に対して、本人であることを証明して、インスタントメッセージングシステムにログインすることができる。

40

【0059】

このように、インスタントメッセージングシステムにログインする場合、ユーザ1またはユーザ4は、インスタントメッセージングIDおよびパスワードによって、認証される。

【0060】

インスタントメッセージングシステムにおいて、サーバ6と、クライアントであるハードディスクレコーダ付きテレビジョン受像装置2とは、SSL（Secure Sockets Layer）などにより、暗号化されたメッセージを交換することにより、セキュアにメッセージを交換する。同様に、サーバ6と、クライアントであるパーソナルコンピュータ5とは、SSLなどにより、暗号化されたメッセージを交換することにより、セキュアにメッセージを交換する。

50

【 0 0 6 1 】

また、ハードディスクレコーダ付きテレビジョン受像装置 2 からパーソナルコンピュータ 5 にメッセージを直接送る場合も、メッセージが暗号化されて、インターネット 3 を介して送られる。逆に、パーソナルコンピュータ 5 からハードディスクレコーダ付きテレビジョン受像装置 2 にメッセージを直接送る場合も、暗号化されたメッセージが、インターネット 3 を介して送られる。

【 0 0 6 2 】

すなわち、ハードディスクレコーダ付きテレビジョン受像装置 2 およびパーソナルコンピュータ 5 は、インターネット 3 およびサーバ 6 を介して、セキュアにメッセージを交換することができる。従って、第三者は、インターネット 3 を伝送されるメッセージを取得しても、復号ができないので、その内容を知ることは出来ない。

10

【 0 0 6 3 】

ユーザ 1 またはユーザ 4 が、インスタントメッセージング ID およびパスワードをサーバ 6 に提示してログインすることは、より具体的には、ユーザ 1 またはユーザ 4 によって操作されるハードディスクレコーダ付きテレビジョン受像装置 2 またはパーソナルコンピュータ 5 が、インスタントメッセージング ID およびパスワードをサーバ 6 に送信することである。

【 0 0 6 4 】

ユーザ 1 またはユーザ 4 は、ハードディスクレコーダ付きテレビジョン受像装置 2 またはパーソナルコンピュータ 5 を介して、インスタントメッセージング ID およびパスワードをサーバ 6 に送信して、インスタントメッセージングシステムにログインし、サーバ 6 に、メッセージを交換する相手のインスタントメッセージング ID からなるリストを作成させることができる。例えば、Jabber において、メッセージを交換する相手のインスタントメッセージング ID からなるリストは、Roster と称される。以下、メッセージを交換する相手のインスタントメッセージング ID からなるリストを、ユーザ登録リストと称する。

20

【 0 0 6 5 】

各ユーザは、自分自身のユーザ登録リストに、このインスタントメッセージングシステムに参加しているユーザのうちの、任意のものを指定して登録させることができる。例えば、ユーザ 1 は自分自身のユーザ登録リストに、ユーザ 4 を登録させることができる。サーバ 6 は、ユーザ 1 からそのユーザ登録リストにユーザ 4 を加えることが指示されたとき、そのユーザ登録リストに、ユーザ 4 のインスタントメッセージング ID を登録する。同様に、ユーザ 4 が自分自身のユーザ登録リストにユーザ 1 の登録を指示すると、サーバ 6 は、ユーザ 4 のユーザ登録リストに、ユーザ 1 のインスタントメッセージング ID を登録する。

30

【 0 0 6 6 】

サーバ 6 に Jabber を利用した場合、サーバ 6 はユーザ登録リストに登録された相手とのメッセージのみを中継する。従って、各ユーザは、自分自身が許可した特定のユーザとだけ安全に通信することができる。

【 0 0 6 7 】

必要に応じて自分自身のユーザ登録リストから他のユーザの登録の抹消を指示することができ、この指示を受けたとき、サーバ 6 は、そのユーザのユーザ登録リストから指定されたユーザのインスタントメッセージング ID を削除する。

40

【 0 0 6 8 】

ハードディスクレコーダ付きテレビジョン受像装置 2 は、サーバ 6 から通知されたユーザ 4 のインターネット 3 上のアドレスによって、パーソナルコンピュータ 5 にアクセスし、パーソナルコンピュータ 5 は、サーバ 6 から通知されたユーザ 1 のインターネット 3 上のアドレスによって、ハードディスクレコーダ付きテレビジョン受像装置 2 にアクセスする。これにより、両者は、以後、直接 (P2P (Peer to Peer) で)、メッセージをやりとりすることができる。

【 0 0 6 9 】

50

インスタントメッセージングIDおよびパスワードによって本人であることが証明できれば、各ユーザは、サーバ6に作成させた、ユーザ登録リストにアクセスすることができる（リストに記述されているインスタントメッセージングIDを利用することができる）。例えば、ユーザ4は、パーソナルコンピュータ5を操作することにより、自己のインスタントメッセージングIDおよびパスワードによって、インスタントメッセージングシステムにログインし、パーソナルコンピュータ5にユーザ登録リストにアクセスさせることができる。また、例えば、ユーザ4は、自分が所有するPDA7を操作することにより、自己のインスタントメッセージングIDおよびパスワードによって、パーソナルコンピュータ5を介してインスタントメッセージングシステムにログインし、PDA7に、サーバ6に作成させたユーザ登録リストにアクセスさせることができる。

10

【0070】

本発明のサービス提供システムにおいては、セキュアなインスタントメッセージングシステムを利用して、インターネット3に接続されている機器に認証に必要な情報を交換させ、機能を他の機器に提供する場合に、セキュアなインスタントメッセージングシステムによって交換された情報を基に、相手を認証する。

【0071】

以下、ハードディスクレコーダ付きテレビジョン受像装置2によるサービスを、パーソナルコンピュータ5に提供する場合を例に説明する。

【0072】

ハードディスクレコーダ付きテレビジョン受像装置2は、インターネット3を介して、サーバ6から、自分自身のユーザ登録リストを取得する。このユーザ登録リストには、ユーザ4が登録されていれば、そのインスタントメッセージングIDが記録されている。そして、ハードディスクレコーダ付きテレビジョン受像装置2は、ユーザ1からの指示に基づいて、ユーザ4のインスタントメッセージングIDに関係付けてアクセス権限を設定する。アクセス権限は、相手からの要求を受け付けるか否かを示す情報である。

20

【0073】

インターネット3を介して、パーソナルコンピュータ5から認証リクエストとしての、セキュアなインスタントメッセージングシステムのメッセージが送信されてきたとき、ハードディスクレコーダ付きテレビジョン受像装置2は、メッセージを受信し、メッセージに含まれているインスタントメッセージングIDに対応するインスタントメッセージングIDがアクセス権設定リストに記録されているか否かを判定する。メッセージに含まれているインスタントメッセージングIDに対応するインスタントメッセージングIDがアクセス権設定リストに記録されていると判定された場合、ハードディスクレコーダ付きテレビジョン受像装置2は、さらに、そのインスタントメッセージングIDで特定される相手がアクセス権限を有するユーザとして登録されているか否かを判定する。

30

【0074】

相手がアクセス権限を有すると判定された場合、ハードディスクレコーダ付きテレビジョン受像装置2は、パーソナルコンピュータ5の所有者であるユーザ4に対する鍵を生成（発行）するとともに、生成した鍵をユーザ4のインスタントメッセージングIDに対応させて鍵リストに記録する。ここで、鍵は、その都度生成される所定のビット数の乱数とすることができる。鍵は、例えば、64ビット乃至256ビットで表される乱数とすることができる。

40

【0075】

そして、ハードディスクレコーダ付きテレビジョン受像装置2は、パーソナルコンピュータ5からの認証リクエストに対するレスポンスとしての、セキュアなインスタントメッセージングシステムのメッセージを、インターネット3を介して、パーソナルコンピュータ5に送信する。パーソナルコンピュータ5に送信されるメッセージには、ハードディスクレコーダ付きテレビジョン受像装置2のアドレス（例えば、URL（Uniform Resource Locator）方式で記述されているアドレス）およびユーザ4のために生成した鍵が含まれている。

50

【 0 0 7 6 】

パーソナルコンピュータ 5 は、ハードディスクレコーダ付きテレビジョン受像装置 2 からのメッセージを受信することにより、ハードディスクレコーダ付きテレビジョン受像装置 2 のアドレスおよびユーザ 4 に対する鍵を取得する。

【 0 0 7 7 】

パーソナルコンピュータ 5 が、ハードディスクレコーダ付きテレビジョン受像装置 2 に対して、例えば、番組の予約録画や既に記録されている番組の映像データの提供などの処理（サービス）を要求する場合、パーソナルコンピュータ 5 は、ハードディスクレコーダ付きテレビジョン受像装置 2 に、ユーザ 4 のインスタントメッセージング ID および受信した鍵と共に、所望の処理の要求を含む操作リクエストを、インターネット 3 を介して送信する。この操作リクエストの送信は、インスタントメッセージングシステムを介さないで行われる。すなわち、操作リクエストは、パーソナルコンピュータ 5 からインターネット 3 を介して、ハードディスクレコーダ付きテレビジョン受像装置 2 に直接送信される。

【 0 0 7 8 】

ハードディスクレコーダ付きテレビジョン受像装置 2 は、パーソナルコンピュータ 5 から送信されてきた操作リクエスト、インスタントメッセージング ID、および鍵を受信し、インスタントメッセージング ID および鍵を基に、操作リクエストを送信してきた相手が正規の相手（自分自身が鍵を送った相手）であるか否かを判定する。

【 0 0 7 9 】

この場合、ハードディスクレコーダ付きテレビジョン受像装置 2 は、受信されたインスタントメッセージング ID に対応するインスタントメッセージング ID がアクセス権設定リストに記録されており、かつ、受信された鍵に対応する鍵（例えば、同じ鍵）が鍵リストに記録されている場合、操作リクエストを送信してきた相手である、パーソナルコンピュータ 5 が正規の相手であると判定する。

【 0 0 8 0 】

パーソナルコンピュータ 5 が正規の相手であると判定された場合、ハードディスクレコーダ付きテレビジョン受像装置 2 は、相手がアクセス権限を有するか否かを判定する。相手がアクセス権限を有する場合、ハードディスクレコーダ付きテレビジョン受像装置 2 は、操作リクエストを受け付けて、それに対応する処理を実行する。

【 0 0 8 1 】

このようにすることで、ハードディスクレコーダ付きテレビジョン受像装置 2 は、パーソナルコンピュータ 5 に対して、アカウントまたはパスワードなどの入力を要求する必要がなく、かつ、パーソナルコンピュータ 5 が正規の相手であるか否かを、簡単かつ確実に判定することができるようになる。

【 0 0 8 2 】

パーソナルコンピュータ 5 は、例えば、図 2 で示されるように構成される。CPU (Central Processing Unit) 2 1 は、ROM (Read Only Memory) 2 2、または記録部 2 8 に記録されているプログラムに従って各種の処理を実行する。RAM (Random Access Memory) 2 3 には、CPU 2 1 が実行するプログラムやデータなどが適宜記憶される。これらの CPU 2 1、ROM 2 2、および RAM 2 3 は、バス 2 4 により相互に接続されている。

【 0 0 8 3 】

CPU 2 1 にはまた、バス 2 4 を介して入出力インタフェース 2 5 が接続されている。入出力インタフェース 2 5 には、キーボード、マウス、マイクロホンなどよりなる入力部 2 6、ディスプレイ、スピーカなどよりなる出力部 2 7 が接続されている。CPU 2 1 は、入力部 2 6 から入力される指令に対応して各種の処理を実行する。そして、CPU 2 1 は、処理の結果得られた画像や音声等を出力部 2 7 に出力する。また、CPU 2 1 は、後述するプログラムを実行し、通信部 2 9 に、各種のデータ（インスタントメッセージング ID およびパスワードなど）を送信させるか、または、インターネット 3 を介して送信されてきたデータ（アドレスおよび鍵など）を受信させる。CPU 2 1 は、通信部 2 9 を介して受信したデータを取得する。

【 0 0 8 4 】

入出力インタフェース 2 5 に接続されている記録部 2 8 は、例えばハードディスクなどで構成され、CPU 2 1 が実行するプログラムや各種のデータを記録する。通信部 2 9 は、インターネット 3、その他のネットワークを介して、サーバ 6 またはハードディスクレコーダ付きテレビジョン受像装置 2 などの外部の装置と通信する。

【 0 0 8 5 】

また、通信部 2 9 を介してプログラムを取得し、記録部 2 8 に記録してもよい。

【 0 0 8 6 】

入出力インタフェース 2 5 には、必要に応じてドライブ 3 0 が接続される。ドライブ 3 0 は、磁気ディスク 5 1、光ディスク 5 2、光磁気ディスク 5 3、或いは半導体メモリ 5 4 などが装着されたとき、それらを駆動し、そこに記録されているプログラムやデータなどを取得する。取得されたプログラムやデータは、必要に応じて記録部 2 8 に転送され、記録される。

10

【 0 0 8 7 】

図 3 は、ハードディスクレコーダ付きテレビジョン受像装置 2 の構成例を示すブロック図である。ハードディスクレコーダ付きテレビジョン受像装置 2 は、パーソナルコンピュータ 5 と同様の構成にチューナおよび表示部を追加した構成とすることができる。

【 0 0 8 8 】

すなわち、CPU 7 1 は、ROM 7 2、または記録部 7 8 に記録されているプログラムに従って各種の処理を実行する。RAM 7 3 には、CPU 7 1 が実行するプログラムやデータなどが適宜記憶される。これらの CPU 7 1、ROM 7 2、および RAM 7 3 は、バス 7 4 により相互に接続されている。

20

【 0 0 8 9 】

CPU 7 1 にはまた、バス 7 4 を介して入出力インタフェース 7 5 が接続されている。入出力インタフェース 7 5 には、各種のスイッチまたはリモートコントローラの指令を受信する受信部などよりなる入力部 7 6、LED (Light Emitting Diode) または液晶表示装置などよりなる出力部 7 7 が接続されている。CPU 7 1 は、入力部 7 6 から入力される指令に対応して各種の処理を実行する。CPU 7 1 は、後述するプログラムを実行し、通信部 7 9 に、各種のデータ (アドレスおよび鍵など) を送信させるか、または、インターネット 3 を介して送信されてきたデータ (ユーザ登録リストなど) を受信させる。CPU 7 1 は、通信部 7 9 を介して受信したデータを取得する。

30

【 0 0 9 0 】

入出力インタフェース 7 5 に接続されている記録部 7 8 は、例えばハードディスクなどで構成され、CPU 7 1 が実行するプログラム、または番組の映像データなどの各種のデータを記録する。通信部 7 9 は、インターネット 3、その他のネットワークを介して、サーバ 6 またはパーソナルコンピュータ 5 などの外部の装置と通信する。

【 0 0 9 1 】

また、通信部 7 9 を介してプログラムを取得し、記録部 7 8 に記録してもよい。

【 0 0 9 2 】

チューナ 8 0 は、放送局からの放送を受信し、受信した放送の映像信号などを復調し、表示部 8 1 に供給すると共に、映像データを入出力インタフェース 7 5 を介して、記録部 7 8 に記録させる。表示部 8 1 は、プラズマ表示装置または液晶表示装置およびスピーカなどからなり、チューナ 8 0 から供給された映像信号を基に、画像を表示し、音声を出力する。また、表示部 8 1 は、記録部 7 8 に記録されている映像データを基に、画像を表示し、音声を出力する。

40

【 0 0 9 3 】

なお、通信部 7 9 は、記録部 7 8 に記録されている映像データを、インターネット 3、その他のネットワークを介して、パーソナルコンピュータ 5 などの外部の装置に送信することができる。

【 0 0 9 4 】

50

入出力インタフェース75には、必要に応じてドライブ82が接続される。ドライブ82は、磁気ディスク91、光ディスク92、光磁気ディスク93、或いは半導体メモリ94などが装着されたとき、それらを駆動し、そこに記録されているプログラムやデータなどを取得する。取得されたプログラムやデータは、必要に応じて記録部78に転送され、記録される。

【0095】

図4は、ハードディスクレコーダ付きテレビジョン受像装置2が有するプログラムを示す図である。ハードディスクレコーダ付きテレビジョン受像装置2は、サービス提供プログラム101およびインスタントメッセージプログラム102を有する。

【0096】

サービス提供プログラム101は、インターネット3を介して、パーソナルコンピュータ5など外部の機器からの要求に応じて、外部の機器にサービスを提供するプログラムである。サービスの提供とは、機能の提供を意味する。サービスは、例えば、予約録画、既に記録されている映像データの提供、またはスケジュール情報の公開などである。

【0097】

インスタントメッセージプログラム102は、インスタントメッセージングシステムのクライアントプログラムであり、インターネット3を介して、サーバ6に、ログインを要求するか、他のクライアントの状態を示す情報を要求するか、またはパーソナルコンピュータ5などの他のクライアント宛のメッセージを送信する。また、インスタントメッセージプログラム102は、インターネット3を介して、サーバ6から送信されてきた、

【0098】

さらに、インスタントメッセージプログラム102は、サーバ6から、ユーザ4のインスタントメッセージングIDを含むユーザ登録リストを取得する。

【0099】

インスタントメッセージプログラム102は、サービス提供プログラム101の要求に応じて、パーソナルコンピュータ5などの他のクライアント宛のメッセージを送信するか、または受信したメッセージをサービス提供プログラム101に供給する。また、インスタントメッセージプログラム102は、サーバ6から取得したユーザ登録リストをサービス提供プログラム101に供給する。

【0100】

サービス提供プログラム101は、アクセス権設定プログラム121、認証プログラム122、操作要求受付プログラム123、アクセス権設定リスト124、鍵リスト125、および受信制御プログラム126を含む。

【0101】

アクセス権設定プログラム121は、インスタントメッセージプログラム102に、ユーザ登録リストの取得を要求し、サーバ6から、インスタントメッセージプログラム102によって取得されたユーザ登録リストを基に、アクセス権設定リスト124を生成する。

【0102】

認証プログラム122は、インスタントメッセージプログラム102が、パーソナルコンピュータ5から送信されてきた認証リクエストとしてのメッセージを受信したとき、アクセス権設定リスト124を基に、ユーザ4からの要求に対してサービスを提供するかどうかを判定し、ユーザ4からの要求に対してサービスを提供すると判定した場合、ユーザ4に対する鍵を生成し、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスおよび生成した鍵を含む、認証レスポンスとしてのメッセージを、インスタントメッセージプログラム102に送信させる。また、生成された鍵は、鍵リスト125に格納される。

【0103】

操作要求受付プログラム123は、外部の機器へのサービスの提供の処理を実行するプ

10

20

30

40

50

プログラムである。例えば、受信制御プログラム 1 2 6 により、パーソナルコンピュータ 5 から送信された、ユーザ 4 のインスタントメッセージングIDおよび鍵が付加された操作リクエストが受信された場合、操作要求受付プログラム 1 2 3 は、インスタントメッセージングIDおよび鍵を基に、パーソナルコンピュータ 5 が正規の相手（鍵を送信した相手）であるか否かを判定し、パーソナルコンピュータ 5 が正規の相手であると判定された場合、パーソナルコンピュータ 5 からの操作リクエストに応じた処理を実行する。

【 0 1 0 4 】

また、例えば、操作要求受付プログラム 1 2 3 は、パーソナルコンピュータ 5 が正規の相手であると判定された場合、さらに、アクセス権リスト 1 2 5 に基づいて、パーソナルコンピュータ 5 からの要求を受け付けるか否かを判定し、パーソナルコンピュータ 5 からの要求を受け付けると判定された場合、パーソナルコンピュータ 5 からの操作リクエストに応じた処理を実行する。

【 0 1 0 5 】

受信制御プログラム 1 2 6 は、パーソナルコンピュータ 5 から送信された、ユーザ 4 のインスタントメッセージングIDおよび鍵が付加された操作リクエストを受信し、受信したユーザ 4 のインスタントメッセージングIDおよび鍵が付加された操作リクエストを操作要求受付プログラム 1 2 3 に供給する。

【 0 1 0 6 】

図 5 は、パーソナルコンピュータ 5 が有するプログラムを示す図である。パーソナルコンピュータ 5 は、サービス要求プログラム 1 5 1 およびインスタントメッセージングプログラム 1 5 2 を有する。

【 0 1 0 7 】

サービス要求プログラム 1 5 1 は、インターネット 3 を介して、ハードディスクレコーダ付きテレビジョン受像装置 2 など外部の機器に、サービスの提供を要求するプログラムである。

【 0 1 0 8 】

インスタントメッセージングプログラム 1 5 2 は、インスタントメッセージングシステムのクライアントプログラムであり、インターネット 3 を介して、サーバ 6 に、ログインを要求するか、他のクライアントの状態を示す情報を要求するか、またはハードディスクレコーダ付きテレビジョン受像装置 2 等の他のクライアント宛のメッセージを送信する。また、インスタントメッセージングプログラム 1 5 2 は、インターネット 3 を介して、サーバ 6 から送信されてきた、ハードディスクレコーダ付きテレビジョン受像装置 2 などの他のクライアントからのメッセージを受信する。

【 0 1 0 9 】

インスタントメッセージングプログラム 1 5 2 は、サービス要求プログラム 1 5 1 の要求に応じて、ハードディスクレコーダ付きテレビジョン受像装置 2 等の他のクライアント宛のメッセージを送信するか、または受信したメッセージをサービス要求プログラム 1 5 1 に供給する。

【 0 1 1 0 】

また、インスタントメッセージングプログラム 1 5 2 は、ユーザ 4 のインスタントメッセージングIDをサーバ 6 から取得し、記録している。

【 0 1 1 1 】

サービス要求プログラム 1 5 1 は、認証プログラム 1 7 1、操作要求プログラム 1 7 2、およびアドレス/鍵リスト 1 7 3 を含む。

【 0 1 1 2 】

認証プログラム 1 7 1 は、インスタントメッセージングプログラム 1 5 2 に、ハードディスクレコーダ付きテレビジョン受像装置 2 等の他のクライアント宛の、認証リクエストとしてのメッセージを送信させる。ハードディスクレコーダ付きテレビジョン受像装置 2 において、認証された場合、すなわち、ユーザ 4 からの要求に対してサービスを提供すると判定された場合、ハードディスクレコーダ付きテレビジョン受像装置 2 から、ハードデ

10

20

30

40

50

ィスクレコーダ付きテレビジョン受像装置 2 のアドレスとユーザ 4 に対する鍵とが含まれた認証レスポンスとしてのメッセージが送信されてくるので、認証プログラム 171 は、インスタントメッセージプログラム 152 に、認証レスポンスとしてのメッセージを受信させ、ハードディスクレコーダ付きテレビジョン受像装置 2 のアドレスおよびユーザ 4 に対する鍵を取得する。

【0113】

認証プログラム 171 は、ハードディスクレコーダ付きテレビジョン受像装置 2 のアドレスおよびユーザ 4 に対する鍵を、相互に関係づけて、アドレス/鍵リスト 173 に格納する。これにより、アドレス/鍵リスト 173 には、サービスを受けることができる機器のアドレスと、これに対する鍵が格納されることになる。

10

【0114】

操作要求プログラム 172 は、サービスを提供する機器にサービスを要求するプログラムである。例えば、ハードディスクレコーダ付きテレビジョン受像装置 2 にサービスを要求する場合、操作要求プログラム 172 は、アドレス/鍵リスト 173 から、ハードディスクレコーダ付きテレビジョン受像装置 2 のアドレス、およびユーザ 4 に対する鍵を読み出す。そして、操作要求プログラム 172 は、ハードディスクレコーダ付きテレビジョン受像装置 2 のアドレスを基に、インターネット 3 を介して、ユーザ 4 のインスタントメッセージングIDおよび鍵を付加した操作リクエストをハードディスクレコーダ付きテレビジョン受像装置 2 に送信する。

【0115】

なお、操作リクエストは、インスタントメッセージングシステムとしてのサーバ 6 を介さずに、直接送信される。

20

【0116】

操作リクエストに付加されたインスタントメッセージングIDおよび鍵が正当なものであれば、ハードディスクレコーダ付きテレビジョン受像装置 2 は、操作要求プログラム 172 からの要求に応じて、パーソナルコンピュータ 5 にサービスを提供する。

【0117】

図 6 は、サービス提供プログラム 101 およびインスタントメッセージングプログラム 102 を実行するハードディスクレコーダ付きテレビジョン受像装置 2 のアクセス権の設定の処理を説明するフローチャートである。

30

【0118】

なお、この処理が行われる前に、ユーザ 1 はインスタントメッセージングシステムの会員となり、パスワードとインスタントメッセージングIDの割り当てを受けておく。そして、ユーザ 1 はそのパスワードとインスタントメッセージングIDを利用して、ハードディスクレコーダ付きテレビジョン受像装置 2 からインターネット 3 を介して、サーバ 6 にアクセスし、インスタントメッセージングシステムを介して通信したい相手を、ユーザ登録リストに登録しておく。

【0119】

各ユーザがサーバ 6 にアクセスしたとき、そのパスワードとインスタントメッセージングIDを利用して、そのユーザが会員であるか否かの認証処理が行われ、認証が得られない場合、そのユーザはアクセスが拒絶され、認証が得られたユーザのみがアクセスが許容され、その後の処理が実行可能となる。

40

【0120】

最初の認証が得られた後、ステップ S 11 において、サービス提供プログラム 101 のアクセス権設定プログラム 121 は、インスタントメッセージングプログラム 102 に、サーバ 6 から、ユーザ 1 のユーザ登録リストを取得させる。ユーザ登録リストは、サービス提供プログラム 101 のアクセス権設定プログラム 121 に供給される。

【0121】

図 7 は、このようにして取得されたユーザ登録リストの例を示す図である。図 7 で示されるように、ユーザ登録リストには、ハードディスクレコーダ付きテレビジョン受像装置

50

2のユーザ1が、メッセージを交換する相手のインスタントメッセージングIDが含まれている。前述したように、例えば、ユーザ1から、ユーザ4などの他のユーザの登録を指示されると、サーバ6は、指示された他のユーザのインスタントメッセージングIDをユーザ登録リストに格納する。ユーザ1が、インスタントメッセージングシステムにログインした後、ユーザ1からユーザ登録リストが要求されると、サーバ6は、その要求に従って、ユーザ1のユーザ登録リストをユーザ1（ハードディスクレコーダ付きテレビジョン受像装置2）に提供する。

【0122】

図7で示されるユーザ登録リストの例には、ユーザBのインスタントメッセージングID、ユーザXのインスタントメッセージングID、ユーザYのインスタントメッセージングID、およびユーザZのインスタントメッセージングIDが含まれている。例えば、図7におけるユーザBはユーザ4に対応し、そのインスタントメッセージングIDは、ユーザ4のインスタントメッセージングIDである。

10

【0123】

ステップS12において、アクセス権設定プログラム121は、既に記録されているアクセス権設定リスト124を読み出して、アクセス権設定リスト124に未登録のインスタントメッセージングIDが、ユーザ登録リストに含まれているか否か（アクセス権設定リスト124に記録されていないインスタントメッセージングIDが、ユーザ登録リストに含まれているか否か）を判定する。ステップS12において、アクセス権設定リスト124に未登録のインスタントメッセージングIDが、ユーザ登録リストに含まれていると判定された場合、ステップS13に進み、アクセス権設定プログラム121は、未登録のインスタントメッセージングIDを、アクセス権設定リスト124に追加して（アクセス権設定リスト124に記録して）、ステップS14に進む。

20

【0124】

なお、アクセス権設定リスト124がまだ記録されていない場合、すなわち、初めてアクセス権の設定の処理を実行する場合、ステップS13において、アクセス権設定プログラム121は、アクセス権設定リスト124を生成し、ユーザ登録リストに含まれている全てのインスタントメッセージングIDをアクセス権設定リスト124に格納する。

【0125】

ステップS14において、アクセス権設定プログラム121は、新たに追加したインスタントメッセージングIDに対応するアクセス権限に「権限なし」をデフォルトとして設定して、処理は終了する。より詳細には、ステップS14において、アクセス権設定プログラム121は、ステップS13の処理でアクセス権設定リスト124に記録されたインスタントメッセージングIDに関するアクセス権限として「権限なし」をアクセス権設定リスト124に記録する。

30

【0126】

なお、ステップS14において、アクセス権設定プログラム121は、ユーザ1にアクセス権限の入力を促し、ユーザ1の操作に対応した入力部76からの信号を基に、アクセス権限に「権限なし」および「権限あり」のいずれか一方を記録するようにしてもよい。

【0127】

図8は、このようにしてアクセス権限が付加されたアクセス権設定リスト124の例を示す図である。アクセス権設定リスト124には、インスタントメッセージングIDと、インスタントメッセージングIDに関するアクセス権限が記述されている。受付判定情報の一例であるアクセス権限は、例えば、「権限あり」または「権限なし」とすることができる。「権限あり」は、インスタントメッセージングIDで特定される相手からの要求を受け付けることを示し、「権限なし」は、インスタントメッセージングIDで特定される相手からの要求を受け付けないことを示す。

40

【0128】

図8で示される例においては、ユーザBのインスタントメッセージングIDに関して「権限あり」のアクセス権限が記録され、ユーザXのインスタントメッセージングIDに関係

50

して「権限なし」のアクセス権限が記録され、ユーザYのインスタントメッセージングIDに関して「権限あり」のアクセス権限が記録され、ユーザZのインスタントメッセージングIDに関して「権限なし」のアクセス権限が記録されている。

【0129】

例えば、ステップS13の処理で、アクセス権設定リスト124に、ユーザZのインスタントメッセージングIDが記録された場合、ステップS14において、アクセス権設定リスト124に、ユーザZのインスタントメッセージングIDに係るアクセス権限として「権限なし」が、記録される。

【0130】

このように、新たにインスタントメッセージングIDが取得された場合、取得されたインスタントメッセージングIDに対して、デフォルトで、アクセス権限として「権限なし」が設定される。

10

【0131】

ステップS12において、アクセス権設定リスト124に未登録のインスタントメッセージングIDが、ユーザ登録リストに含まれていないと判定された場合、新たなインスタントメッセージングIDを登録する必要はないので、ステップS13およびステップS14の処理はスキップされ、処理は終了する。

【0132】

ユーザ1による操作に対応するか、またはリモートコントローラからの指令に対応する入力部76からの信号に基づいて、アクセス権設定プログラム121は、アクセス権設定リスト124を編集して、所望のインスタントメッセージングIDに係るアクセス権限を「権限あり」に設定したり、逆に、アクセス権限を「権限なし」に設定したりすることができる。

20

【0133】

次に、図9乃至図11のフローチャートを参照して、サービス提供プログラム101およびインスタントメッセージングプログラム102を実行するハードディスクレコーダ付きテレビジョン受像装置2、サーバ6、並びにサービス要求プログラム151およびインスタントメッセージングプログラム152を実行するパーソナルコンピュータ5によりログインしたとき最初に実行される認証の処理を説明する。

【0134】

30

ユーザ4からのアクセスの指令があったとき、ステップS1001において、インスタントメッセージングプログラム152は、サービス要求プログラム151の認証プログラム171からの要求に基づいて、通信部29に、インターネット3を介して、サーバ6にインスタントメッセージングIDおよびパスワードを送信させる。なお、インスタントメッセージングIDおよびパスワードは、例えば、ユーザ1による入力部26への操作により、パーソナルコンピュータ5に入力される。

【0135】

ステップS2001において、サーバ6は、パーソナルコンピュータ5から送信されてきた、インスタントメッセージングIDおよびパスワードを受信する。インスタントメッセージングIDおよびパスワードが対応して登録されているものである場合、パーソナルコンピュータ5のユーザが正規のユーザなので、ステップS2002において、サーバ6は、パーソナルコンピュータ5のユーザのログインの処理を実行すると共に、インターネット3を介して、ユーザ4のユーザ登録リストに登録されている他のユーザの装置（例えば、ハードディスクレコーダ付きテレビジョン受像装置2）のインスタントメッセージングシステムへの参加の状態（例えば、インスタントメッセージングシステムにログインしている、ログインしていない、あるいは、ログインしているが、離席しているといったような状態）を示す情報をパーソナルコンピュータ5に送信する。

40

【0136】

また、ステップS2003において、サーバ6は、パーソナルコンピュータ5のユーザ4のユーザ登録リストに登録されているユーザのうち、そのユーザのユーザ登録リストに

50

ユーザ4を登録しているユーザであって、いまログインしているユーザを検索し、その検索したユーザの装置（例えば、ユーザ1のハードディスクレコーダ付きテレビジョン受像装置2）に、ユーザ4がログインしてきたことを通知する。

【0137】

ステップS3001において、ハードディスクレコーダ付きテレビジョン受像装置2のインスタントメッセージプログラム102は、この通知を受信する。そして、そのことが、受信制御プログラム126により、表示部81に表示される。

【0138】

インスタントメッセージIDおよびパスワードが対応付けて登録されていない場合、パーソナルコンピュータ5のユーザは正規のユーザではないので、パーソナルコンピュータ5のユーザのログインの処理およびステップS2002以降の処理は実行されず、処理は終了する。

【0139】

ステップS1002において、インスタントメッセージプログラム152は、サーバ6から送信されてきた、ハードディスクレコーダ付きテレビジョン受像装置2を含む他の機器のインスタントメッセージシステムへの参加の状態を示す情報を受信する。他の機器のインスタントメッセージシステムへの参加の状態を示す情報は、サービス要求プログラム151の認証プログラム171に供給される。

【0140】

パーソナルコンピュータ5が、ピアツーピアでハードディスクレコーダ付きテレビジョン受像装置2にメッセージを送信するために、ステップS1003において、インスタントメッセージプログラム152は、インターネット3を介して、サーバ6にハードディスクレコーダ付きテレビジョン受像装置2のインターネット3上のアドレスを要求する。すなわち、インスタントメッセージプログラム152は、通信部29に、インターネット3を介して、サーバ6宛てに、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスの要求を送信させる。ステップS2004において、サーバ6は、パーソナルコンピュータ5から送信されてきた、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスの要求を受信する。

【0141】

ステップS2005において、サーバ6は、インターネット3を介して、パーソナルコンピュータ5にハードディスクレコーダ付きテレビジョン受像装置2のアドレスを送信する。このアドレスは、ハードディスクレコーダ付きテレビジョン受像装置2がログインしてきたときサーバ6により検知されている。ステップS1004において、インスタントメッセージプログラム152は、通信部29に、サーバ6から送信されてきた、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスを受信させ、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスを取得する。

【0142】

パーソナルコンピュータ5は、ステップS1004の処理でハードディスクレコーダ付きテレビジョン受像装置2のアドレスを取得することにより、インターネット3を介して、ピアツーピアで、ハードディスクレコーダ付きテレビジョン受像装置2にメッセージを送信することができるようになる。

【0143】

一方、ハードディスクレコーダ付きテレビジョン受像装置2が、ピアツーピアでパーソナルコンピュータ5にメッセージを送信するために、ステップS3002において、インスタントメッセージプログラム102は、通信部79に、インターネット3を介して、サーバ6宛てに、パーソナルコンピュータ5のアドレスの要求を送信させる。ステップS2006において、サーバ6は、ハードディスクレコーダ付きテレビジョン受像装置2から送信されてきた、パーソナルコンピュータ5のアドレスの要求を受信する。

【0144】

ステップS2007において、サーバ6は、インターネット3を介して、ハードディス

10

20

30

40

50

クレコーダ付きテレビジョン受像装置 2 にパーソナルコンピュータ 5 のアドレスを送信する。ステップ S 3 0 0 3 において、インスタントメッセンジャプログラム 1 0 2 は、通信部 7 9 に、サーバ 6 から送信されてきた、パーソナルコンピュータ 5 のアドレスを受信させる。

【 0 1 4 5 】

ハードディスクレコーダ付きテレビジョン受像装置 2 は、ステップ S 3 0 0 3 の処理でパーソナルコンピュータ 5 のアドレスを取得することにより、インターネット 3 を介して、ピアツーピアで、パーソナルコンピュータ 5 にメッセージを送信することができるようになる。

【 0 1 4 6 】

ステップ S 1 0 0 5 において、サービス要求プログラム 1 5 1 の認証プログラム 1 7 1 は、インスタントメッセンジャプログラム 1 5 2 に、インターネット 3 を介して、相手の機器であるハードディスクレコーダ付きテレビジョン受像装置 2 に、ハードディスクレコーダ付きテレビジョン受像装置 2 のアドレスを要求するメッセージを認証リクエストとして送信させる。すなわち、インスタントメッセンジャプログラム 1 5 2 は、ステップ S 1 0 0 4 の処理で取得したアドレスを基に、通信部 2 9 に、インターネット 3 を介してピアツーピアで（サーバ 6 を介さずに）、認証リクエストとしての、ハードディスクレコーダ付きテレビジョン受像装置 2 宛のメッセージを、パーソナルコンピュータ 5 のインスタントメッセージング ID を含めて送信させる。インスタントメッセンジャプログラム 1 5 2 が送信するメッセージは、SSL などの方式により、暗号化されている。

【 0 1 4 7 】

ステップ S 3 0 0 4 において、インスタントメッセンジャプログラム 1 0 2 は、通信部 7 9 に、パーソナルコンピュータ 5 から送信されてきた、認証リクエストとしての、ハードディスクレコーダ付きテレビジョン受像装置 2 のアドレスを要求するメッセージを受信させる。受信したメッセージは、サービス提供プログラム 1 0 1 の認証プログラム 1 2 2 に供給される。受信されたメッセージには、パーソナルコンピュータ 5 のインスタントメッセージング ID が付されている。

【 0 1 4 8 】

ステップ S 3 0 0 5 において、認証プログラム 1 2 2 は、アクセス権設定リスト 1 2 4 に登録されているユーザからの認証リクエストであるか否か、すなわち、認証リクエストに付されているインスタントメッセージング ID と同じインスタントメッセージング ID がアクセス権設定リスト 1 2 4 に記録されているか否かを判定し、アクセス権設定リスト 1 2 4 に記録されている、すなわち、アクセス権設定リスト 1 2 4 に登録された正規のユーザからの認証リクエストであると判定された場合、ステップ S 3 0 0 6 に進む。

【 0 1 4 9 】

ステップ S 3 0 0 6 において、認証プログラム 1 2 2 は、認証リクエストを送信したユーザのアクセス権が、「権限あり」に設定されているか否か、すなわち、認証リクエストに付されているインスタントメッセージング ID と同じインスタントメッセージング ID に関係付けられた、相手からの要求を受け付けることを示す「権限あり」であるアクセス権限がアクセス権設定リスト 1 2 4 に記録されているか否かを判定する。換言すれば、ステップ S 3 0 0 6 においては、受付判定情報の一例であるアクセス権限を基に、相手からの要求を受け付けるか否かが判定される。

【 0 1 5 0 】

ステップ S 3 0 0 6 において、認証リクエストを送信してきたユーザのアクセス権が、「権限あり」に設定されている、すなわち、「権限あり」であるアクセス権限がアクセス権設定リスト 1 2 4 に記録されていると判定された場合、相手からの要求を受け付けると判定されたので、ステップ S 3 0 0 7 に進み、認証プログラム 1 2 2 は、認証リクエストを送信してきたユーザ 4 のための鍵を生成する。鍵は、例えば、その都度生成、変更される、6 4 ビット乃至 2 5 6 ビットの乱数とされる。

【 0 1 5 1 】

10

20

30

40

50

次に、ステップS3008において、認証プログラム122は、鍵リスト125に、認証リクエストを送信してきたユーザ4のインスタントメッセージングIDに対応させて（関係付けて）、ステップS3007の処理で生成した鍵を記録する。

【0152】

図12は、鍵リスト125の例を示す図である。図12で示される鍵リスト125において、ユーザBのインスタントメッセージングIDに関係付けてユーザBであるユーザ4のための鍵Bが記録され、ユーザXのインスタントメッセージングIDに関係付けてユーザXのための鍵Xが記録されている。

【0153】

例えば、ユーザ4であるユーザBからの認証リクエストを受信した場合、ユーザ4であるユーザBのための鍵Bが生成されるので、鍵リスト125において、ユーザBのインスタントメッセージングIDに関係付けて鍵Bが記録されることになる。

10

【0154】

次に、ステップS3009において、認証プログラム122は、インスタントメッセージングプログラム102に、認証レスポンスとしてのメッセージをパーソナルコンピュータ5に返信させる。すなわち、認証プログラム122がインスタントメッセージングプログラム102に、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスおよびステップS3007で生成した鍵を供給するので、インスタントメッセージングプログラム102は、パーソナルコンピュータ5宛ての、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスおよび認証リクエストを送信してきた相手のための鍵を含む、認証レスポンスとしてのメッセージを生成して、通信部79に、生成したメッセージを送信させる。認証レスポンスとしてのメッセージは、SSLなどの方式により、暗号化されている。

20

【0155】

ステップS1006において、インスタントメッセージングプログラム152は、ハードディスクレコーダ付きテレビジョン受像装置2から送信されてきた、認証レスポンスとしての、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスおよびユーザ4のための鍵を含むメッセージを通信部29に受信させて、処理は終了する。受信されたメッセージは、サービス要求プログラム151の認証プログラム171に供給される。認証プログラム171は、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスおよび鍵をアドレス/鍵リスト173に記録する。アドレスと鍵は暗号化されているので、認証プログラム171により復号されて記録される。

30

【0156】

インターネット3で伝送中に、メッセージが第三者に取得されても、メッセージは暗号化されているので、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスおよび鍵が第三者に知られることはない。

【0157】

一方、ステップS3005において、認証リクエストに付されているインスタントメッセージングIDと同じインスタントメッセージングIDがアクセス権設定リスト124に記録されていない、すなわち、アクセス権設定リスト124に登録されたユーザからの認証リクエストでないかと判定された場合、メッセージを交換していない相手からの認証リクエストなので（正規の相手ではないので）、認証の要求を受け付けすることはできないから、ステップS3010に進み、認証プログラム122は、エラー処理を実行して、処理は終了する。

40

【0158】

ステップS3006において、認証リクエストを送信したユーザのアクセス権が、「権限なし」に設定されていると判定された場合、すなわち、メッセージを交換する相手であっても、その相手からの要求を受け付けると判定された場合、メッセージを交換する相手であっても、その要求を受け付けると設定している相手からの要求なので、ステップS3010に進み、認証プログラム122は、エラー処理を実行して、処理は終了する。

50

【 0 1 5 9 】

例えば、ステップ S 3 0 1 0 において、認証プログラム 1 2 2 は、認証を受け付けられないことを示すメッセージをパーソナルコンピュータ 5 に送信する。認証を受け付けられないことを示すメッセージには、アドレスまたは鍵が付加されていない。

【 0 1 6 0 】

このように、登録されていないユーザからのリクエストである場合、または相手からの要求を受け付けない旨がアクセス権限に設定されている場合、相手は、アドレスおよび鍵を取得することができない。その結果、後述のサービス提供の処理において、サービスを要求することができない。

【 0 1 6 1 】

言い換えれば、登録されている正規のユーザからのリクエストであり、かつ、相手からの要求を受け付ける旨がアクセス権限に設定されている場合にのみ、認証を要求した相手は、サービスを要求するために必要なアドレスおよび鍵を取得することができる。従って、ハードディスクレコーダ付きテレビジョン受像装置 2 のアドレスおよび鍵が正規のユーザ以外の者に取得されることによる、正規のユーザ以外の者の成りすましを防止することができる。

【 0 1 6 2 】

なお、パーソナルコンピュータ 5 がハードディスクレコーダ付きテレビジョン受像装置 2 に送信するメッセージ、またはハードディスクレコーダ付きテレビジョン受像装置 2 がパーソナルコンピュータ 5 に送信するメッセージは、サーバ 6 を介して、伝送するようにしてもよい。但し、P2Pで伝送するようにした方が、サーバ 6 の負荷を軽くすることができる。

【 0 1 6 3 】

以上のようにして、アドレスと鍵を取得したパーソナルコンピュータ 5 は、ハードディスクレコーダ付きテレビジョン受像装置 2 を利用するとき、図 1 3 のフローチャートに示される処理を実行する。

【 0 1 6 4 】

ステップ S 1 0 2 1 において、サービス要求プログラム 1 5 1 の操作要求プログラム 1 7 2 は、アドレス / 鍵リスト 1 7 3 から、ハードディスクレコーダ付きテレビジョン受像装置 2 から受信して記録されている、ハードディスクレコーダ付きテレビジョン受像装置 2 のアドレスおよび鍵を読み出す。また、操作要求プログラム 1 7 2 は、インスタントメッセージングプログラム 1 5 2 から、ユーザ 4 のインスタントメッセージング ID を取得する。そして、操作要求プログラム 1 7 2 は、ユーザ 4 のインスタントメッセージング ID および読み出された鍵を付加した操作リクエストを生成し、やはり読み出されたハードディスクレコーダ付きテレビジョン受像装置 2 のアドレス宛てに、通信部 2 9 から、インターネット 3 を介して送信させる。

【 0 1 6 5 】

ステップ S 3 0 2 1 において、サービス提供プログラム 1 0 1 の受信制御プログラム 1 2 6 は、通信部 7 9 に、パーソナルコンピュータ 5 から送信されてきた、ユーザ 4 のインスタントメッセージング ID およびユーザ 1 が付与した鍵が付加された操作リクエストを受信させる。この操作リクエストは、操作要求受付プログラム 1 2 3 に供給される。

【 0 1 6 6 】

ステップ S 3 0 2 2 において、操作要求受付プログラム 1 2 3 は、アクセス権設定リスト 1 2 4 に登録されたユーザからのリクエストであるか否か、すなわち、受信された操作リクエストに付加されているインスタントメッセージング ID と同じインスタントメッセージング ID がアクセス権設定リスト 1 2 4 に記録されているか否かを判定し、アクセス権設定リスト 1 2 4 に登録されたユーザからのリクエストであると判定された場合、すなわち、インスタントメッセージング ID がアクセス権設定リスト 1 2 4 に記録されている場合、ステップ S 3 0 2 3 に進む。

【 0 1 6 7 】

ステップS3023において、操作要求受付プログラム123は、鍵リスト125に、このユーザに対する鍵が記録されているか否かを判定する。より具体的には、操作要求受付プログラム123は、受信された操作リクエストに付加されているインスタントメッセージIDと同じインスタントメッセージIDに関係する鍵が鍵リスト125に記録されているか否かを判定することにより、このユーザに対する鍵が記録されているか否かを判定する。

【0168】

ステップS3023において、このユーザに対する鍵が記録されていると判定された場合、ステップS3024に進み、操作要求受付プログラム123は、操作リクエストに付加されている鍵と、鍵リスト125に記録されている鍵が一致するか否かを判定する。より具体的には、操作要求受付プログラム123は、操作リクエストに付加されている鍵と、操作リクエストに付加されているインスタントメッセージIDと同じインスタントメッセージIDに関係付けられて鍵リスト125に記録されている鍵とが一致するか否かを判定する。

10

【0169】

ステップS3024において、操作リクエストに付加されている鍵と、鍵リスト125に記録されている鍵が一致すると判定された場合、ステップS3025に進み、操作要求受付プログラム123は、このユーザに権限が与えられているか否か、すなわち、アクセス権設定リスト124において、操作リクエストに付加されているインスタントメッセージIDと同じインスタントメッセージIDに関して、「権限あり」のアクセス権限が記録されているか否かを判定する。

20

【0170】

ステップS3025において、このユーザに権限が与えられていると判定された場合、すなわち、アクセス権設定リスト124において、操作リクエストに付加されているインスタントメッセージIDと同じインスタントメッセージIDに関して、「権限あり」のアクセス権限が記録されていると判定された場合、ステップS3026に進み、操作要求受付プログラム123は、パーソナルコンピュータ5のユーザ4が正規のユーザであり、パーソナルコンピュータ5からの要求を受け付ける旨が設定されているので、パーソナルコンピュータ5からの操作リクエストを受け付けて、要求された処理、例えば、予約録画の処理または記録されている映像データの送信などの処理を実行して、サービス提供の処理は終了する。

30

【0171】

ステップS3022において、アクセス権設定リスト124に登録されたユーザからのリクエストでないと判定された場合、すなわち、インスタントメッセージIDがアクセス権設定リスト124に記録されていない場合、パーソナルコンピュータ5のユーザ4は正規のユーザではないので、ステップS3027に進み、操作要求受付プログラム123は、エラー処理を実行して処理は終了する。ステップS3027におけるエラー処理は、具体的には、例えば、パーソナルコンピュータ5に、操作リクエストを受け付けられない旨を示すメッセージを送信する処理である。

【0172】

また、同様に、ステップS3023において、このユーザに対する鍵が記録されていないと判定された場合、並びに、ステップS3024において、操作リクエストに付加されている鍵と、鍵リスト125に記録されている鍵が一致しないと判定された場合、パーソナルコンピュータ5のユーザ4は正規のユーザではないので、ステップS3027に進み、操作要求受付プログラム123は、エラー処理を実行して処理は終了する。

40

【0173】

さらに、ステップS3025において、このユーザに権限が与えられていないと判定された場合、パーソナルコンピュータ5からの要求は受け付けられないので、ステップS3027に進み、操作要求受付プログラム123は、エラー処理を実行して処理は終了する。

50

【0174】

なお、ステップS3025の処理を省略して、ステップS3024において、操作リクエストに付加されている鍵と、鍵リスト125に記録されている鍵が一致すると判定された場合、操作要求受付プログラム123は、操作リクエストを受け付けて、要求された処理を実行するようにしてもよい。

【0175】

すなわち、この場合、ステップS3022乃至ステップS3024の処理において、パーソナルコンピュータ5のユーザ4が正規のユーザであるか否かが判定され、パーソナルコンピュータ5のユーザ4が正規のユーザであると判定された場合、パーソナルコンピュータ5からの操作リクエストが受け付けられて、パーソナルコンピュータ5にサービスが提供される。

10

【0176】

ただし、図13に示されるように、パーソナルコンピュータ5のユーザ4が正規のユーザである場合、ステップS3025の処理において、さらに、インスタントメッセージングIDに関して記録されている受付判定情報であるアクセス権限を基に、パーソナルコンピュータ5のユーザ4からの要求を受け付けられるか否かを判定するようにした方が、ユーザ登録リストに登録されているユーザの中で、さらに細かく使用の可否を設定することができるようになる。

【0177】

また、このようにすることで、例えば、一旦、ユーザ4からの要求を受け付けると設定し、認証の処理を行った後でも、鍵が不正に利用された場合に、ユーザ1は、ユーザ4からの要求を拒否することができるように、権限を変更することができる。

20

【0178】

以上のように、サービスを提供するユーザが、インスタントメッセージングシステムのインスタントメッセージングIDを、他のユーザがそのサービスを利用する場合のユーザアカウントとしてそのまま利用することで、機器毎にユーザアカウントを作成する必要がなくなる。

【0179】

インスタントメッセージングシステムからユーザ登録リストを取得し、ユーザ登録リストからインスタントメッセージングIDを取得するので、サービスを提供する機器のユーザは、相手のインスタントメッセージングIDをいちいち入力する必要がない。

30

【0180】

また、ユーザは、相手のインスタントメッセージングIDを直接知る必要もないので、受信したIDを記録はしても表示はさせないようにすることもできる。これにより、IDの不正な利用を防止することができる。

【0181】

さらに例えば、アクセス権限などの受付判定情報を設定することにより、相手のユーザ毎に、サービスの利用の可否や利用可能の操作の範囲などを提供側で決定することができる。

【0182】

成りすましや改竄のできないインスタントメッセージングシステム経由で認証リクエストを送送するので、パスワードなどを入力することなくユーザ認証することができる。

40

【0183】

利用権限のあるユーザからの認証リクエストに対して、ランダムに生成した鍵をセキュアなインスタントメッセージングシステム経由で返信するので、鍵が第三者に盗まれる危険性がほとんど無くなり、サービス提供の処理において、インスタントメッセージングシステム経由でサービスを要求する必要がなく、サービスの提供側は、鍵が付加されたアクセスであれば、相手が認証済みのユーザであることを確認できる。

【0184】

サービスを要求する側においては、受けるサービス毎に、アカウントおよびパスワード

50

を覚えておく必要がなく、また、サービスを要求するときに、いちいちアカウントおよびパスワードを入力する必要がない。その結果、サービスを要求する側は、迅速に、サービスを要求することができるようになる。

【0185】

なお、セキュアな環境がそれ程必要ないのであれば、暗号化は省略することができる。それでも、その点に基づく安全性が若干損なわれるだけで、その他の効果は同様に奏することができる。

【0186】

また、上述した処理により、パーソナルコンピュータ5に限らず、ユーザ4は、PDA7を操作して、ハードディスクレコーダ付きテレビジョン受像装置2に機能の提供を要求することができる。

10

【0187】

さらに、パーソナルコンピュータ5がサービス提供プログラムを実行し、ハードディスクレコーダ付きテレビジョン受像装置2がサービス要求プログラムを実行するようになれば、パーソナルコンピュータ5が、ハードディスクレコーダ付きテレビジョン受像装置2に機能を提供することができる。この場合、パーソナルコンピュータ5およびハードディスクレコーダ付きテレビジョン受像装置2は、相互に、機能を提供しあうことができる。

【0188】

このように、パーソナルコンピュータ5からの操作リクエストに対応して処理を実行するようにした場合には、ハードディスクレコーダ付きテレビジョン受像装置2は、パーソナルコンピュータ5にサービスを提供することができるようになる。

20

【0189】

また、ネットワークを介して、相手から送信されてきた、インスタントメッセージングシステムのユーザを特定する特定情報としてのインスタントメッセージングIDおよび鍵の受信を制御し、特定情報および鍵を基に、相手が正規の相手であるか否かを判定するようにした場合には、パーソナルコンピュータ5において、アカウントまたはパスワードなどの入力を要求する必要がなく、かつ、ハードディスクレコーダ付きテレビジョン受像装置2において、相手が正規の相手であるか否かを判定することができるようになる。

【0190】

なお、アクセス権限は、「権限あり」または「権限なし」に限らず、権限の種類をより多くすることができる。例えば、アクセス権限は、「一部使用可」、「全部使用可」、または「使用不可」などとしてもよい。また、例えば、アクセス権限を、「映像データの読み出しのみ」、「新規の映像データの記録」、「映像データの書き換え」などとすることができる。例えば、アクセス権限が「映像データの読み出しのみ」である場合、映像データの記録または書き換への要求は受け付けられず、映像データの読み出しの要求は受け付けられる。また、例えば、アクセス権限が「新規の映像データの記録」である場合、映像データの読み出しの要求、新規の映像データの記録の要求、および映像データの書き換への要求が受け付けられる。

30

【0191】

さらに、アクセス権限は、全ユーザを一括して設定するようになすことができる。例えば、ユーザ1の指令に対応する入力部76からの信号に基づいて、アクセス権設定プログラム121は、アクセス権設定リスト124の全ユーザに対するアクセス権限を、全て「権限あり」に設定したり、逆に、全て「権限なし」に設定したりすることができる。

40

【0192】

また、アクセス権リスト124は、図14および図15で示されるように、ユーザのインスタントメッセージングIDに関係させて、グループ名を記録することができる。また、アクセス権限は、グループ毎に設定することができる。図14で示される例において、ユーザBのインスタントメッセージングID、ユーザXのインスタントメッセージングID、およびユーザZのインスタントメッセージングIDは、グループ であるグループ名に関係付けられ、ユーザYのインスタントメッセージングIDは、グループ であるグループ名に関

50

係付けられている。

【0193】

図15で示される例において、グループであるグループ名に関係付けられるアクセス権限として「権限あり」が設定され、グループであるグループ名に関係付けられるアクセス権限として「権限なし」が設定されている。

【0194】

この場合、ステップS3006において、ユーザ4であるユーザBからの認証リクエストであるとき、認証プログラム122は、アクセス権リスト124において、ユーザBのインスタントメッセージングIDに関係付けられているグループ名であるグループを読み出し、さらに、グループであるグループ名に関係付けられるアクセス権限である「権限あり」を読み出して、読み出したアクセス権限を基に、相手からの要求を受け付けるか否かを判定し、相手からの要求を受け付けると判定する。一方、ユーザYからの認証リクエストであるとき、認証プログラム122は、アクセス権リスト124において、ユーザYのインスタントメッセージングIDに関係付けられているグループ名であるグループを読み出し、さらに、グループであるグループ名に関係付けられるアクセス権限である「権限なし」を読み出して、読み出したアクセス権限を基に、相手からの要求を受け付けるか否かを判定し、相手からの要求を受け付けると判定する。

10

【0195】

多数のユーザのアクセス権限をより少ない操作で設定することができるようになる。

【0196】

また、受付判定情報の一例であるアクセス権限は、図16で示されるように、サービス毎に設定するようにしてもよい。例えば、ハードディスクレコーダ付きテレビジョン受像装置2が、記録のサービス（例えば、予約録画）と再生のサービス（例えば、記録されている映像データの提供）とを提供する場合、アクセス権設定リスト124には、ユーザのインスタントメッセージングIDに関係付けて、提供するサービスおよびアクセス権限が記録されるようにしてもよい。

20

【0197】

例えば、ユーザBのインスタントメッセージングIDに関係付けて、記録であるサービスおよび「権限あり」であるアクセス権限が記録されているので、ユーザBから、記録の処理が要求された場合、ハードディスクレコーダ付きテレビジョン受像装置2は、記録のサービスを提供する。また、ユーザYのインスタントメッセージングIDに関係付けて、再生であるサービスおよび「権限あり」であるアクセス権限が記録されているので、ユーザYから、再生の処理が要求された場合、ハードディスクレコーダ付きテレビジョン受像装置2は、再生のサービスを提供する。

30

【0198】

例えば、ユーザBから、再生の処理が要求された場合、ユーザBのインスタントメッセージングIDに関係付けて、再生であるサービスおよび「権限あり」であるアクセス権限が記録されていないので、ハードディスクレコーダ付きテレビジョン受像装置2は、再生のサービスを提供しない。また、ユーザYから、記録の処理が要求された場合、ユーザYのインスタントメッセージングIDに関係付けて、記録であるサービスおよび「権限あり」であるアクセス権限が記録されていないので、ハードディスクレコーダ付きテレビジョン受像装置2は、記録のサービスを提供しない。

40

【0199】

なお、サービス毎に、アクセス権設定リスト124を設けるようにしてもよい。例えば、再生であるサービスに対して1つのアクセス権設定リスト124を設け、記録であるサービスに対して他の1つのアクセス権設定リスト124を設けるようにしてもよい。

【0200】

さらにまた、相手の機器毎に鍵を生成するようにしてもよい。例えば、ユーザ4がパーソナルコンピュータ5以外の機器であるPDA7から、ハードディスクレコーダ付きテレビジョン受像装置2にサービスを要求できるように、パーソナルコンピュータ5およびPDA

50

7のそれぞれに、異なる鍵を生成し、割り当てるようにしてもよい。

【0201】

また、鍵には、有効期限を設けるようにしてもよい。これにより提供するサービスの管理が容易となる。

【0202】

図17は、有効期限が設けられた機器毎の鍵を記録する鍵リスト125の例を示す図である。この場合、例えば、ステップS1005の処理において、パーソナルコンピュータ5は、ハードディスクレコーダ付きテレビジョン受像装置2宛てに、自分自身の機器IDであるzzzを付した、認証リクエストとしてのメッセージを送信する。ステップS3008において、ハードディスクレコーダ付きテレビジョン受像装置2は、インスタントメッセージングIDに関係付けて、zzzである機器IDおよび鍵B1を記録する。また、PDA7が自分自身の機器IDであるyyyを付した、認証リクエストとしてのメッセージを送信してきた場合、ハードディスクレコーダ付きテレビジョン受像装置2は、インスタントメッセージングIDに関係付けて、yyyである機器IDおよび鍵B2を記録する。

10

【0203】

サービス提供の処理においては、ステップS1021で、パーソナルコンピュータ5は、zzzである機器ID、インスタントメッセージングID、鍵B1を付加した操作リクエストをハードディスクレコーダ付きテレビジョン受像装置2に送信する。ハードディスクレコーダ付きテレビジョン受像装置2は、zzzである機器IDである機器IDが鍵リスト125に記録されているか否かをさらに判定し、zzzである機器IDである機器IDが鍵リスト125に記録されていると判定された場合、操作リクエストを受け付けて処理を実行し、zzzである機器IDである機器IDが鍵リスト125に記録されていないと判定された場合、操作リクエストを受け付けない。

20

【0204】

なお、機器IDに代えて、機器名を使用するようにしてもよい。

【0205】

また、ステップS3023において、ハードディスクレコーダ付きテレビジョン受像装置2は、機器IDに対する鍵が記録されているか否かを判定するようにしてもよい。

【0206】

鍵リスト125の鍵に対して有効期限が設定されている場合、ハードディスクレコーダ付きテレビジョン受像装置2は、図示せぬリアルタイムクロックから日付および時刻を取得して、鍵リスト125から、有効期限を過ぎた鍵（および鍵に関係するインスタントメッセージングIDなどのデータ）を削除する（消去する）。有効期限を適切に設定することで、インターネット3を介して送信されるインスタントメッセージングIDおよび鍵を取得した者からの不正な操作リクエストの受付を防止することができる。

30

【0207】

鍵リスト125の鍵に対する有効期限までの期間をより短くする（例えば、30分）ことで、鍵をいわゆるセッションキーとすることができる。鍵をセッションキーとすれば、セッションキーである鍵を他人に取得されても、成りすましによる、サービスの不正な利用を許す可能性を低くすることができるので、サービス提供の処理において、鍵を平文のまま送信することができる。

40

【0208】

認証の処理の後、1つのサービスを提供したとき、鍵が消去されるようにしてもよい。

【0209】

さらに、図9乃至図11を参照して説明した認証の処理において、ハードディスクレコーダ付きテレビジョン受像装置2は、サーバ6から送信された認証リクエストを受信する場合、同時に、サーバ6から、メッセージの送信を特定するセッションIDを取得し、アクセス権設定リスト124に、インスタントメッセージングIDに関係付けてセッションIDを記録するようにしてもよい。この場合、セッションIDは、認証レスポンスに付されて相手に送信される。

50

【0210】

そして、サービス提供の処理において、セッションIDを付した操作リクエストを要求し、操作リクエストに付されたセッションIDと、アクセス権設定リスト124に記録されているセッションIDとが一致する場合にのみ、サービスを提供するようにすることができる。

【0211】

パーソナルコンピュータ5が、暗号化した操作リクエストをハードディスクレコーダ付きテレビジョン受像装置2に送信するようにしてもよい。図18は、操作リクエストを暗号化する場合のサービス提供の処理を説明するフローチャートである。

【0212】

ステップS1041において、サービス要求プログラム151の操作要求プログラム172は、アドレス/鍵リスト173から、ハードディスクレコーダ付きテレビジョン受像装置2から受信して記録されている、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスおよび鍵を読み出す。また、操作要求プログラム172は、インスタントメッセージプログラム152から、ユーザ4のインスタントメッセージIDを取得する。そして、操作要求プログラム172は、ユーザ4のインスタントメッセージIDおよび鍵を付加した操作リクエストを生成する。

【0213】

ステップS1042において、操作要求プログラム172は、生成された操作リクエストを鍵で暗号化する。この場合、暗号化方法は、DES(Data Encryption Standard)またはIDEA(International Data Encryption Algorithm)などの共通鍵暗号方式とすることができる。

【0214】

ステップS1043において、操作要求プログラム172は、通信部29に、インターネット3を介して、暗号化された操作リクエストを、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスに宛てて送信させる。

【0215】

ステップS3041において、サービス提供プログラム101の受信制御プログラム126は、通信部79に、パーソナルコンピュータ5から送信されてきた、暗号化されている操作リクエストを受信させる。暗号化されている操作リクエストは、操作要求受付プログラム123に供給される。

【0216】

ステップS3042において、操作要求受付プログラム123は、鍵リスト125に記録されている鍵で、ユーザ4のインスタントメッセージIDおよび鍵が付加された操作リクエストを復号する。

【0217】

ステップS3043乃至ステップS3048の処理のそれぞれは、図13のステップS3022乃至ステップS3027の処理のそれぞれと同様なので、その説明は省略する。

【0218】

このように、操作リクエストを暗号化することで、インターネット3を介して、送信される操作リクエストが第三者に取得され、その第三者にインスタントメッセージIDおよび鍵が不正に利用されることを防止することができる。

【0219】

なお、インスタントメッセージIDおよび鍵を暗号化したり、インスタントメッセージIDおよび鍵のいずれか一方を暗号化したりしてもよい。

【0220】

さらに、ハードディスクレコーダ付きテレビジョン受像装置2とパーソナルコンピュータ5とで共有している鍵を使用して、ダイジェストを発行して交換するなど、認証を行うようにしてもよい。

【0221】

10

20

30

40

50

例えば、操作要求プログラム172および受信制御プログラム126には、共通のハッシュ関数が予め格納される。操作要求プログラム172は、インスタントメッセージングIDおよび鍵を送信する前に、乱数を生成し、乱数にハッシュ関数を適用することによりハッシュ値(ダイジェスト)を求めて、乱数およびハッシュ値をハードディスクレコーダ付きテレビジョン受像装置2に送信する。受信制御プログラム126は、パーソナルコンピュータ5から送信されてきた乱数およびハッシュ値を受信し、受信した乱数にハッシュ関数を適用してハッシュ値を求めて、受信したハッシュ値と求めたハッシュ値とが一致するか否かを判定する。受信制御プログラム126は、受信したハッシュ値と求めたハッシュ値とが一致すると判定された場合、パーソナルコンピュータ5を認証する。

【0222】

認証の方式は、ダイジェストを使用する方法に限らない。

【0223】

図19は、チャレンジアドレスポンス方式の認証を行う場合のサービス提供の処理を説明するフローチャートである。ステップS1061において、サービス要求プログラム151の操作要求プログラム172は、ハードディスクレコーダ付きテレビジョン受像装置2に認証を要求する。この場合、インスタントメッセージングIDがパーソナルコンピュータ5からハードディスクレコーダ付きテレビジョン受像装置2に送信される。

【0224】

パーソナルコンピュータ5から認証が要求されると、ステップS3061において、サービス提供プログラム101の受信制御プログラム126は、チャレンジアドレスポンス方式の認証処理を実行する。そして、ステップS1062において、操作要求プログラム172は、チャレンジアドレスポンス方式の認証処理を実行する。

【0225】

より具体的には、受信制御プログラム126は、パーソナルコンピュータ5から送信されてきたインスタントメッセージングIDに関係付けられて記録されている鍵を鍵リスト125から読み出す。受信制御プログラム126は、乱数を生成し、生成した乱数をチャレンジコードとして、パーソナルコンピュータ5に送信する。

【0226】

操作要求プログラム172は、ハードディスクレコーダ付きテレビジョン受像装置2から、チャレンジコードが送信されてくると、チャレンジコードを受信して、受信したチャレンジコードをアドレス/鍵リスト173に記録されている鍵で暗号化して、レスポンスを生成する。操作要求プログラム172は、生成したレスポンスをハードディスクレコーダ付きテレビジョン受像装置2に送信する。

【0227】

受信制御プログラム126は、パーソナルコンピュータ5からレスポンスが送信されてくると、レスポンスを受信し、受信したレスポンスと、生成した乱数を鍵で暗号化した値とを比較し、受信したレスポンスと生成した乱数を鍵で暗号化した値とが一致した場合、パーソナルコンピュータ5を適正な相手として認証する。受信制御プログラム126は、受信したレスポンスと生成した乱数を鍵で暗号化した値とが一致しない場合、パーソナルコンピュータ5を適正な相手として認証しない(不適正な相手であると認証する)。

【0228】

ステップS1063において、操作要求プログラム172は、通信部29に、インターネット3を介して、ユーザ4のインスタントメッセージングIDおよび鍵を付加した操作リクエストを、ハードディスクレコーダ付きテレビジョン受像装置2のアドレスに宛てて送信させる。

【0229】

パーソナルコンピュータ5が認証された場合、ステップS3062において、受信制御プログラム126は、通信部79に、パーソナルコンピュータ5から送信されてきた、ユーザ4のインスタントメッセージングIDおよび鍵が付加された操作リクエストを受信させ、ステップS3063に進む。

10

20

30

40

50

【 0 2 3 0 】

パーソナルコンピュータ 5 が認証されない場合、ステップ S 3 0 6 2 において、受信制御プログラム 1 2 6 は、受信した操作リクエストを破棄し、以下の処理はスキップされ、操作リクエストに対する処理は実行されない。

【 0 2 3 1 】

ステップ S 3 0 6 3 乃至ステップ S 3 0 6 8 の処理のそれぞれは、図 1 3 のステップ S 3 0 2 2 乃至ステップ S 3 0 2 7 の処理のそれぞれと同様なので、その説明は省略する。

【 0 2 3 2 】

このように、ハードディスクレコーダ付きテレビジョン受像装置 2 は、認証された相手からの操作リクエストのみを受け付けるようにすることができる。なお、レスポンスをセッションキーとして、セッションキーで操作リクエストを暗号化するようにしてもよい。

10

【 0 2 3 3 】

このようにすることで、成りすましをより強力に排除することができるようになる。

【 0 2 3 4 】

ネットワークを介して、相手から送信されてきた、インスタントメッセージングシステムのユーザを特定する特定情報を基に、相手が正規の相手であるか否かを判定するようにした場合、成りすましを防止することができる。

【 0 2 3 5 】

また、ネットワークを介して、相手から送信されてきた、インスタントメッセージングシステムのユーザを特定する特定情報および鍵の受信を制御し、特定情報および鍵を基に、相手が正規の相手であるか否かを判定するようにした場合には、アカウントまたはパスワードなどの入力を要求する必要がなく、かつ、相手が正規の相手であるか否かを、簡単かつ確実に判定することができ、もって、特定の相手に対してのみサービスを提供したり、特定の相手のみがサービスを利用できるようになる。

20

【 0 2 3 6 】

上述した一連の処理は、ハードウェアにより実行させることもできるし、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

30

【 0 2 3 7 】

この記録媒体は、図 2 または図 3 に示されるように、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク 5 1 若しくは磁気ディスク 9 1 (フレキシブルディスクを含む)、光ディスク 5 2 若しくは光ディスク 9 2 (CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む)、光磁気ディスク 5 3 若しくは光磁気ディスク 9 3 (MD(Mini-Disc)(商標)を含む)、または半導体メモリ 5 4 若しくは半導体メモリ 9 4 などよりなるパッケージメディアにより構成されるだけでなく、コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM 2 2 またはROM 7 2 や、記録部 2 8 または記録部 7 8 に含まれるハードディスクなどで構成される。

40

【 0 2 3 8 】

なお、上述した一連の処理を実行させるプログラムは、必要に応じてルータ、モデムなどのインタフェースを介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を介してコンピュータにインストールされるようにしてもよい。

【 0 2 3 9 】

また、本明細書において、記録媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

50

【 0 2 4 0 】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【 図面の簡単な説明 】

【 0 2 4 1 】

【 図 1 】 本発明に係るサービス提供システムの一実施の形態の構成を示すブロック図である。

【 図 2 】 図 1 のパーソナルコンピュータの構成例を示すブロック図である。

【 図 3 】 図 1 のハードディスクレコーダ付きテレビジョン受像装置の構成例を示すブロック図である。

【 図 4 】 図 1 のハードディスクレコーダ付きテレビジョン受像装置が有するプログラムを示す図である。

【 図 5 】 図 1 のパーソナルコンピュータが有するプログラムを示す図である。

【 図 6 】 アクセス権の設定の処理を説明するフローチャートである。

【 図 7 】 ユーザ登録リストの例を示す図である。

【 図 8 】 アクセス権設定リストの例を示す図である。

【 図 9 】 認証の処理を説明するフローチャートである。

【 図 1 0 】 認証の処理を説明するフローチャートである。

【 図 1 1 】 認証の処理を説明するフローチャートである。

【 図 1 2 】 鍵リストの例を示す図である。

【 図 1 3 】 サービス提供の処理を説明するフローチャートである。

【 図 1 4 】 アクセス権設定リストの他の例を示す図である。

【 図 1 5 】 アクセス権設定リストの他の例を示す図である。

【 図 1 6 】 アクセス権設定リストの他の例を示す図である。

【 図 1 7 】 鍵リストの他の例を示す図である。

【 図 1 8 】 サービス提供の他の処理を説明するフローチャートである。

【 図 1 9 】 サービス提供の他の処理を説明するフローチャートである。

【 符号の説明 】

【 0 2 4 2 】

2 ハードディスクレコーダ付きテレビジョン受像装置, 3 インターネット, 5
 パーソナルコンピュータ, 6 サーバ, 7 PDA, 21 CPU, 22 RO
 M, 23 RAM, 28 記録部, 29 通信部, 51 磁気ディスク, 52
 光ディスク, 53 光磁気ディスク, 54 半導体メモリ, 71 CPU, 7
 2 ROM, 73 RAM, 78 記録部, 79 通信部, 91 磁気ディスク
 , 92 光ディスク, 93 光磁気ディスク, 94 半導体メモリ, 101 サ
 ービス提供プログラム, 102 インスタントメッセージプログラム, 121 ア
 クセス権設定プログラム, 122 認証プログラム, 123 操作要求受付プログラ
 ム, 124 アクセス権設定リスト, 125 鍵リスト, 126 受信制御プログラ
 ム, 151 サービス要求プログラム, 152 インスタントメッセージプログラ
 ム, 171 認証プログラム, 172 操作要求プログラム, 173 アドレス
 / 鍵リスト

10

20

30

40

【 図 1 】

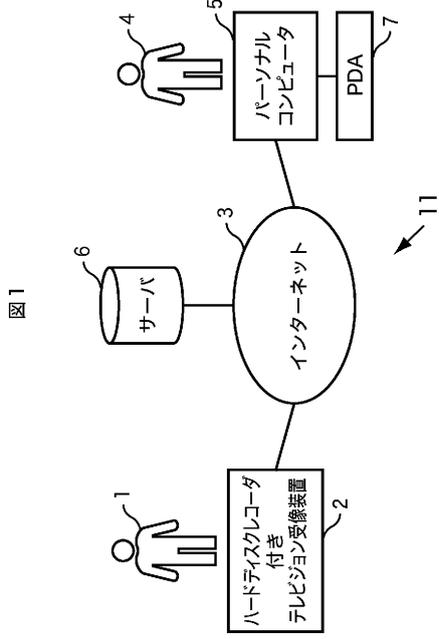


図 1

【 図 2 】

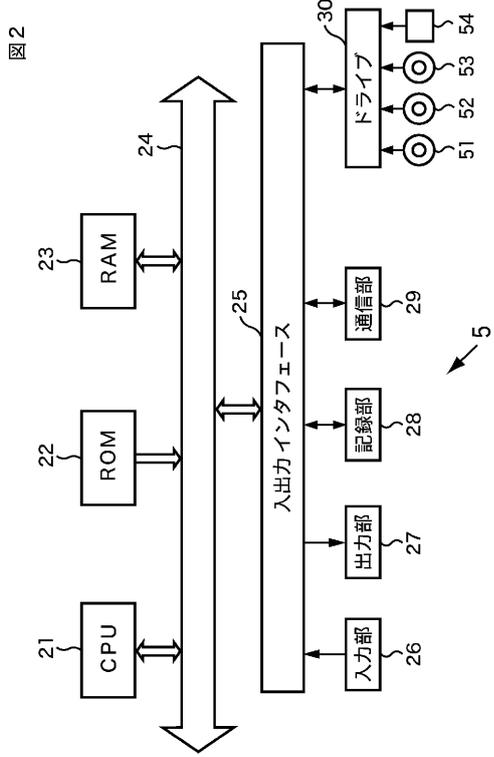


図 2

【 図 3 】

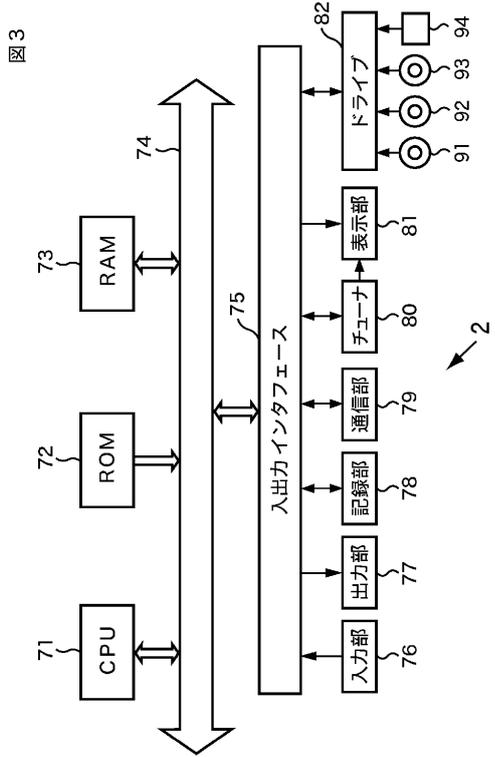


図 3

【 図 4 】

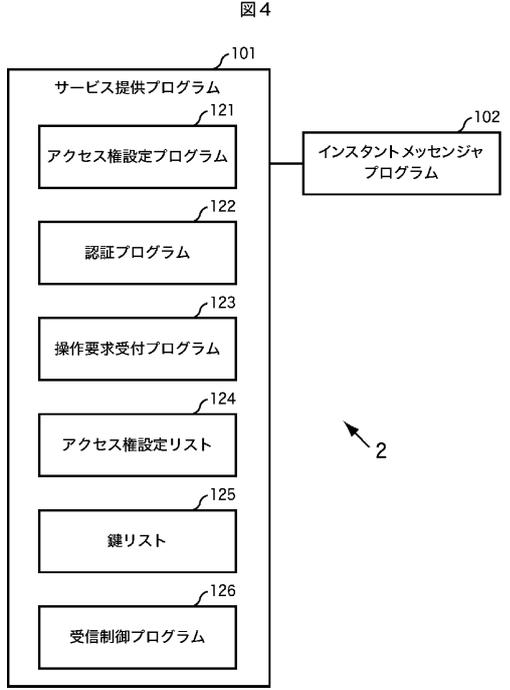
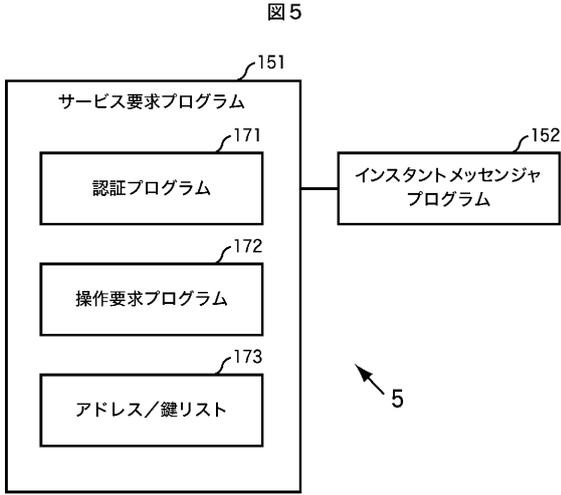


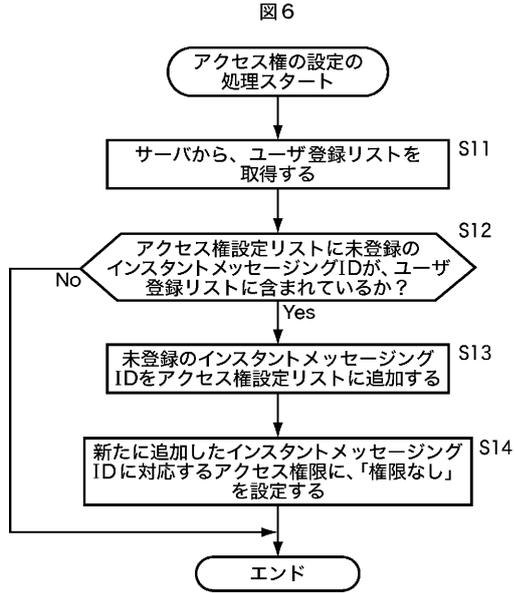
図 4

2

【 図 5 】



【 図 6 】



【 図 7 】

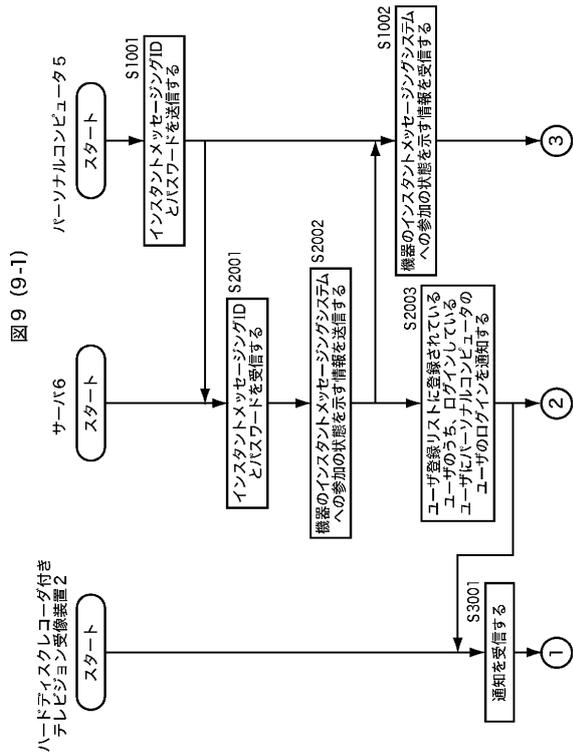


【 図 8 】

図8

ユーザのリスト	アクセス権限
ユーザBのインスタントメッセージングID	権限あり
ユーザXのインスタントメッセージングID	権限なし
ユーザYのインスタントメッセージングID	権限あり
ユーザZのインスタントメッセージングID	権限なし

【 図 9 】



【図14】

図14

ユーザのリスト	グループ名
ユーザBのインスタントメッセージングID	グループα
ユーザXのインスタントメッセージングID	グループα
ユーザYのインスタントメッセージングID	グループβ
ユーザZのインスタントメッセージングID	グループα
⋮	⋮

124

【図15】

図15

グループ名	アクセス権限
グループα	権限あり
グループβ	権限なし
⋮	⋮

124

【図16】

図16

ユーザのリスト	サービス	アクセス権限
ユーザBのインスタントメッセージングID	記録	権限あり
ユーザXのインスタントメッセージングID	記録	権限なし
ユーザYのインスタントメッセージングID	再生	権限あり
ユーザZのインスタントメッセージングID	再生	権限なし
⋮	⋮	⋮

124

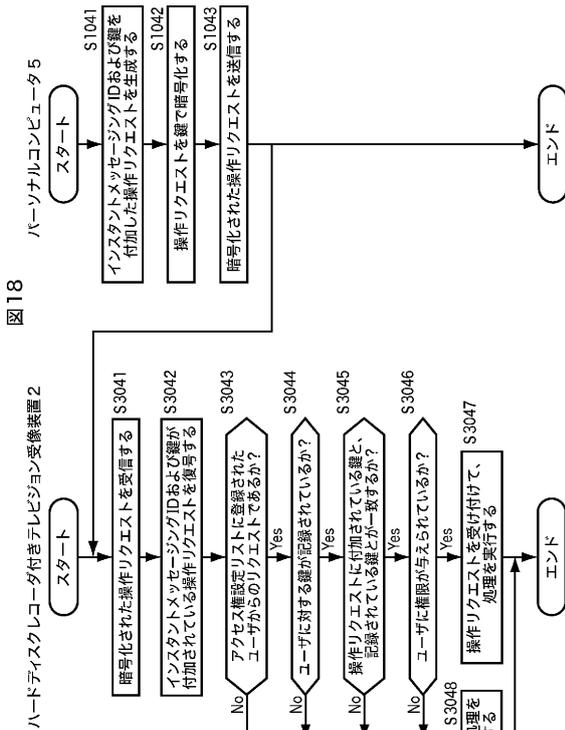
【図17】

図17

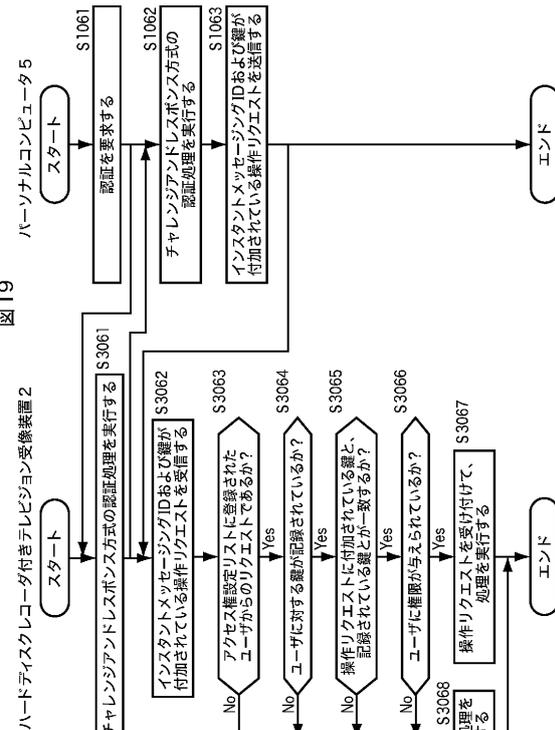
鍵を発行したユーザのリスト	機器ID	鍵情報	有効期限
ユーザBのインスタントメッセージングID	zzz	鍵B 1	aaaa
ユーザBのインスタントメッセージングID	yyy	鍵B 2	bbbb
ユーザXのインスタントメッセージングID	xxx	鍵X	cccc
⋮	⋮	⋮	⋮

125

【図18】



【図19】



フロントページの続き

審査官 鳥居 稔

(56)参考文献 国際公開第02/009437(WO, A1)

特表2004-505363(JP, A)

特開2001-211200(JP, A)

特開2003-046657(JP, A)

特表2005-505054(JP, A)

特表2003-528543(JP, A)

特表2005-507119(JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/00-20

G06F 13/00

H04L 9/00-32