(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4313171号
(P4313171)

(45)発行日　平成21年8月12日(2009.8.12)　(24)登録日　平成21年5月22日(2009.5.22)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330D
E05B 49/00	(2006.01)	G06F	15/00	330G
G08B 25/04	(2006.01)	E05B	49/00	F
		G08B	25/04	F

請求項の数 7　(全 29 頁)

(21)出願番号　特願2003-410397(P2003-410397)
(22)出願日　平成15年12月9日(2003.12.9)
(65)公開番号　特開2005-173805(P2005-173805A)
(43)公開日　平成17年6月30日(2005.6.30)
審査請求日　平成17年7月19日(2005.7.19)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(72)発明者　西木　健哉
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所　システム開発研究所内
(72)発明者　坂田　匡通
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所　システム開発研究所内

審査官　赤穂　州一郎

最終頁に続く

(54)【発明の名称】認証制御装置および認証制御方法

(57)【特許請求の範囲】

【請求項１】

複数の機器から構成される管理対象システムの管理単位である複数のサブセグメントを各々管理し、前記管理対象システムのユーザの認証方法を決定し、該決定した認証方法による認証結果が認証成立である場合に、当該ユーザを、自身の管理するサブセグメントの管理対象システムを構成する各機器の存在するエリアに入出可能とし、自身の管理するサブセグメントの管理対象システムを構成する各機器の機能を使用可能とする認証制御装置であって、

前記認証制御装置は、認証要求が入力されると、当該認証要求に含まれる認証方法を示す情報に従い、当該認証要求に含まれる認証情報を用いて認証する認証装置と接続されており、

前記ユーザの記憶媒体には、当該ユーザの属性と、当該ユーザの前記管理対象システムの利用頻度と、当該ユーザが入出するエリアを示す情報と当該ユーザが前記機器の機能を用いて接続する通信網を示す情報とを有するアクセス場所と、を有する属性情報が記憶されており、

ネットワークを介して、自身の管理するサブセグメントの管理対象システムを構成する前記機器の各々から、該機器の存在するエリアと、該機器の種別と、該機器を使用するユーザの属性とを示す機器情報を収集する機器情報収集手段と、

前記記憶媒体より前記属性情報を取得する属性情報取得手段と、

前記機器情報収集手段により収集された前記各機器情報を用いて前記管理対象システム

の安全レベルを決定する安全レベル決定手段と、
前記属性情報取得手段により取得された前記ユーザの属性情報を用いて前記ユーザの信頼レベルを決定する信頼レベル決定手段と、
前記安全レベル決定手段で決定された前記各機器の安全レベルおよび前記信頼レベル決定手段で決定された前記ユーザの信頼レベルを用いて前記ユーザの認証方法を決定する認証方法決定手段と、
前記決定した認証方法により前記ユーザを認証するために必要な認証情報を取得し、前記決定した認証方法を示す情報と前記取得した認証情報とを含む認証要求を前記認証装置に出力し、当該認証装置から出力された認証結果が認証成立である場合、前記ユーザを、自身の管理するサブセグメントの管理対象システムを構成する各機器の存在するエリアに入出可能とし、自身の管理するサブセグメントの管理対象システムを構成する各機器の機能を使用可能とする認証制御手段と、を有すること
を特徴とする認証制御装置。
【請求項２】
請求項１に記載の認証制御装置であって、
前記記憶媒体には、前記ユーザの認証に利用する認証情報が記憶されており、
前記認証制御手段は、
前記認証方法決定手段で決定された認証方法による認証に必要な認証情報を前記記憶媒体および/または前記ユーザより取得し、
前記認証装置から出力された認証結果が認証成立である場合、前記認証方法決定手段で決定された認証方法に応じた認証レベルと、電子署名とを有する認証チケットを生成して、前記記憶媒体にさらに記憶させ、
認証チケットを含む要求が入力されると、当該認証チケットに含まれる電子署名により、当該認証チケットが正当なものであるか否か判定し、この判定の結果、当該認証チケットが正当なものである場合、自身の管理するサブセグメントの管理対象システムを構成する各機器の存在するエリアに入出可能とし、自身の管理するサブセグメントの管理対象システムを構成する各機器の機能を使用可能とすること
を特徴とする認証制御装置。
【請求項３】
請求項２に記載の認証制御装置であって、
前記属性情報取得手段は、前記記憶媒体に前記認証チケットが記憶されている場合、当該認証チケットを前記ユーザの属性情報と共に取得し、
前記認証方法決定手段は、前記属性情報取得手段により前記認証チケットが取得されている場合、前記安全レベル決定手段で決定された前記各機器の安全レベルおよび前記信頼レベル決定手段で決定された前記ユーザの信頼レベルを用いて前記ユーザの認証レベルを決定し、決定した認証レベルが前記認証チケットで指定されている前記認証レベルよりも高い場合に、前記ユーザを再認証するための前記ユーザの認証方法を決定すること
を特徴とする認証制御装置。
【請求項４】
請求項３に記載の認証制御装置であって、
前記ユーザの端末は、自身と接続された前記機器のいずれかに、前記記憶媒体に記憶されているアクセスチケットを含むアクセス要求を出力し、
前記機器の各々は、前記端末から、アクセスチケットを含むアクセス要求が入力されると、当該アクセスチケットに含まれる電子署名により、当該アクセスチケットが正当なものであるか否か判定し、当該アクセスチケットが正当なものであると判定した場合、当該アクセスチケットに含まれるアクセス権限に従い、前記端末による自身の機能の使用を可能とし、
前記認証方法決定手段は、前記安全レベル決定手段で決定された前記各機器の安全レベルおよび前記信頼レベル決定手段で決定された前記ユーザの信頼レベルを用いて決定された前記ユーザの認証レベルが、前記属性情報取得手段により取得された前記認証チケット

で指定されている前記認証レベル以下である場合に、前記認証制御手段にアクセスチケットの生成を指示し、
前記認証制御手段は、
前記判定の結果、認証チケットが正当なものである場合、前記ユーザのアクセス権限と、電子署名とを有するアクセスチケットを生成して、前記記憶媒体にさらに記憶させること
を特徴とする認証制御装置。
【請求項５】
請求項４に記載の認証制御装置であって、
前記機器の各々は、前記判定により、アクセスチケットが正当なものであると判定された場合、前記端末と自身との通信を、当該アクセスチケットに対応付けて設定されたセキュリティポリシに従い行うものであり、
前記認証制御手段は、
アクセスチケットを生成して前記記憶媒体に記憶させた場合に、前記ユーザから、前記管理対象システムを構成する各機器と前記端末との通信に適用するセキュリティポリシをさらに受付け、
前記受付けたセキュリティポリシを、前記生成したアクセスチケットに対応付けて、自装置の管理するサブセグメントの前記管理対象システムを構成する各機器にさらに設定すること
を特徴とする認証制御装置。
【請求項６】
複数の機器から構成される管理対象システムの管理単位である複数のサブセグメントを各々管理し、前記管理対象システムのユーザの認証方法を決定し、該決定した認証方法による認証結果が認証成立である場合に、当該ユーザを、自身の管理するサブセグメントの管理対象システムを構成する各機器の存在するエリアに入出可能とし、自身の管理するサブセグメントの管理対象システムを構成する各機器の機能を使用可能とする、コンピュータで読取り可能なプログラムであって、
前記コンピュータは、認証要求が入力されると、当該認証要求に含まれる認証方法を示す情報に従い、当該認証要求に含まれる認証情報を用いて認証する認証装置と接続されており、
前記ユーザの記憶媒体には、当該ユーザの属性と、当該ユーザの前記管理対象システムの利用頻度と、当該ユーザが入出するエリアを示す情報と当該ユーザが前記機器の機能を用いて接続する通信網を示す情報とを有するアクセス場所と、を有する属性情報が記憶されており、
前記コンピュータに、
ネットワークを介して、自身の管理するサブセグメントの管理対象システムを構成する前記機器の各々から、該機器の存在するエリアと、該機器の種別と、該機器を使用するユーザの属性とを示す機器情報を収集する機器情報収集手段と、
前記記憶媒体より前記属性情報を取得する属性情報取得手段と、
前記機器情報収集手段により収集された前記各器情情報を用いて前記管理対象システムの安全レベルを決定する安全レベル決定手段と、
前記属性情報取得手段により取得された前記ユーザの属性情報を用いて前記ユーザの信頼レベルを決定する信頼レベル決定手段と、
前記安全レベル決定手段で決定された前記各機器の安全レベルおよび前記信頼レベル決定手段で決定された前記ユーザの信頼レベルを用いて前記ユーザの認証方法を決定する認証方法決定手段と、
前記決定した認証方法により前記ユーザを認証するために必要な認証情報を取得し、前記決定した認証方法を示す情報と前記取得した認証情報とを含む認証要求を前記認証装置に出力し、当該認証装置から出力された認証結果が認証成立である場合、前記ユーザを、自身の管理するサブセグメントの管理対象システムを構成する各機器の存在するエリアに

入出可能とし、自身の管理するサブセグメントの管理対象システムを構成する各機器の機能を使用可能とする認証制御手段と、として機能させること
を特徴とするコンピュータで読取り可能なプログラム。
【請求項７】
複数の機器から構成される管理対象システムの管理単位である複数のサブセグメントを各々管理し、前記管理対象システムのユーザの認証方法を決定し、該決定した認証方法による認証結果が認証成立である場合に、当該ユーザを、自身の管理するサブセグメントの管理対象システムを構成する各機器の存在するエリアに入出可能とし、自身の管理するサブセグメントの管理対象システムを構成する各機器の機能を使用可能とする情報処理装置による認証制御方法あって、
前記情報処理装置は、認証要求が入力されると、当該認証要求に含まれる認証方法を示す情報に従い、当該認証要求に含まれる認証情報を用いて認証する認証装置と接続されており、
前記ユーザの記憶媒体には、当該ユーザの属性と、当該ユーザの前記管理対象システムの利用頻度と、当該ユーザが入出するエリアを示す情報と当該ユーザが前記機器の機能を用いて接続する通信網を示す情報とを有するアクセス場所と、を有する属性情報が記憶されており、
前記情報処理装置は、
ネットワークを介して、自身の管理するサブセグメントの管理対象システムを構成する前記機器の各々から、該機器の存在するエリアと、該機器の種別と、該機器を使用するユーザの属性とを示す機器情報を収集する機器情報収集ステップと、
前記記憶媒体より前記属性情報を取得する属性情報取得ステップと、
収集した前記各機器情報を用いて前記管理対象システムの安全レベルを決定する安全レベル決定ステップと、
取得した前記ユーザの属性情報を用いて前記ユーザの信頼レベルを決定する信頼レベル決定ステップと、
決定された前記各機器の安全レベルおよび前記ユーザの信頼レベルを用いて前記ユーザの認証方法を決定する認証方法ステップと、
前記決定した認証方法により前記ユーザを認証するために必要な認証情報を取得し、前記決定した認証方法を示す情報と前記取得した認証情報とを含む認証要求を前記認証装置に出力し、当該認証装置から出力された認証結果が認証成立である場合、前記ユーザを、自身の管理するサブセグメントの管理対象システムを構成する各機器の存在するエリアに入出可能とし、自身の管理するサブセグメントの管理対象システムを構成する各機器の機能を使用可能とする認証制御ステップと、を行なうこと
を特徴とする認証制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、システムのユーザの認証方法を決定する技術、および、システムを構成する各機器へのアクセスを制御する技術に関する。
【背景技術】
【０００２】
特許文献１には、複数種類の身体的特徴における認証結果をテーブルに記憶しておき、予め設定された認証のセキュリティレベルの情報と、前記テーブルの情報とを用いて、各身体的特徴の信頼性を表す評価関数を計算することにより、前記複数種類の身体的特徴の中から認証に最も適する身体的特徴を選定する技術が開示されている。該技術では、選定した身体的特徴について、ユーザから入手した情報と前記テーブルに記憶されている情報とを照合することで、認証成立の有無を判定している。
【０００３】
【特許文献１】特開２００１-５２１８１号公報

【発明の開示】
【発明が解決しようとする課題】
【０００４】
ところで、システムのユーザの認証に要求されるレベルは、当該ユーザの属性および当該システムの構成に依存することが多い。特許文献１に記載の技術は、これらの点を何ら考慮していない。
【０００５】
本発明は上記事情に鑑みてなされたものであり、本発明の目的は、ユーザ属性およびシステム構成に適したレベルの認証方法を決定することにある。
【課題を解決するための手段】
【０００６】
上記課題を解決するために、本発明の認証制御装置は、管理対象システムを構成する各機器の情報に応じた当該システムの安全レベル、および、ユーザの属性情報に応じた当該ユーザの信頼レベルに基づいて、管理対象システムを利用するために当該ユーザに適用する認証方法を決定する。
【０００７】
例えば本発明の認証制御装置は、複数の機器から構成される管理対象システムの管理単位である複数のサブセグメントを各々管理し、前記管理対象システムのユーザの認証方法を決定し、該決定した認証方法による認証結果が認証成立である場合に、当該ユーザを、自身の管理するサブセグメントの管理対象システムを構成する各機器の存在するエリアに入出可能とし、自身の管理するサブセグメントの管理対象システムを構成する各機器の機能を使用可能とする認証制御装置であって、前記認証制御装置は、認証要求が入力されると、当該認証要求に含まれる認証方法を示す情報に従い、当該認証要求に含まれる認証情報を用いて認証する認証装置と接続されており、前記ユーザの記憶媒体には、当該ユーザの属性と、当該ユーザの前記管理対象システムの利用頻度と、当該ユーザが入出するエリアを示す情報と当該ユーザが前記機器の機能を用いて接続する通信網を示す情報とを有するアクセス場所と、を有する属性情報が記憶されており、ネットワークを介して、自身の管理するサブセグメントの管理対象システムを構成する前記機器の各々から、該機器の存在するエリアと、該機器の種別と、該機器を使用するユーザの属性とを示す機器情報を収集する機器情報収集手段と、前記記憶媒体より前記属性情報を取得する属性情報取得手段と、前記機器情報収集手段により収集された前記各機器情報を用いて前記管理対象システムの安全レベルを決定する安全レベル決定手段と、前記属性情報取得手段により取得された前記ユーザの属性情報を用いて前記ユーザの信頼レベルを決定する信頼レベル決定手段と、前記安全レベル決定手段で決定された前記各機器の安全レベルおよび前記信頼レベル決定手段で決定された前記ユーザの信頼レベルを用いて前記ユーザの認証方法を決定する認証方法決定手段と、前記決定した認証方法により前記ユーザを認証するために必要な認証情報を取得し、前記決定した認証方法を示す情報と前記取得した認証情報とを含む認証要求を前記認証装置に出力し、当該認証装置から出力された認証結果が認証成立である場合、前記ユーザを、自身の管理するサブセグメントの管理対象システムを構成する各機器の存在するエリアに入出可能とし、自身の管理するサブセグメントの管理対象システムを構成する各機器の機能を使用可能とする認証制御手段と、を有する。
【発明の効果】
【０００８】
本発明によれば、ユーザの属性情報に応じた当該ユーザの信頼レベルおよび管理対象システムの構成に応じた当該システムの安全レベルに基づいて、ユーザの認証方法を決定する。したがって、ユーザ属性およびシステム構成に適したレベルの認証方法を決定することができる。

【発明を実施するための最良の形態】
【０００９】

以下に、本発明の実施の形態を説明する。

【００１０】

図１は本発明の一実施形態が適用されたビル内ネットワークシステムの概略図である。図示するように、本実施形態のビル内ネットワークシステムは、ビルのフロア毎に構築されたネットワークのサブセグメント１０を有する。本実施形態では、フロア１Ｆにサブセグメント10_1が構築され、フロア２Ｆにサブセグメント10_2が構築され、そして、フロア３Ｆにサブセグメント10_3が構築されている。各サブセグメント10_1～10_3は、スイッチングハブ（ＳＷＨＵＢ）20_1～20_3により相互接続されている。また、ビル内ネットワークシステムは、ルータ３０およびＷＡＮ４０を介して、ユーザ認証を行なう認証装置５０と接続されている。

【００１１】

サブセグメント１０は、ネットワーク接続された認証制御装置６０および管理対象システム７０を有する。本実施形態では、サブセグメント10_1が認証制御装置60_1および管理対象システム70_1を有し、サブセグメント10_2が認証制御装置60_2および管理対象システム70_2を有し、そして、サブセグメント10_3が認証制御装置60_3および管理対象システム70_3を有している。

【００１２】

認証制御装置６０は、直接あるいはユーザ端末８０を介してユーザ所有のハードウエアトークン（ＨＴ）９０と通信を行ない、認証装置５０と連携してユーザ認証を行なう。そして、認証が成立した場合にのみ、例えば自認制御装置６０が属するサブセグメント１０が構築されたフロアの入口に設置されたゲート、ドアを開くなどして、該フロアへの入場を許可する。また、認証が成立したユーザのユーザ端末８０による該サブセグメント１０に属する管理対象システム７０を構成する各機器へのアクセス制御を行う。ここで、管理対象システム７０を構成する機器としては、無線アクセスポイント（ＡＰ）７０１等のネットワーク機器、プリンタ７０２、スキャナ７０３、ファイルサーバ７０４等のネットワーク端末（情報機器）がある。

【００１３】

図２は、認証制御装置６０の概略図である。図示するように、認証制御装置６０は、ネットワークＩＦ部６０１と、無線通信部６０２と、指示受付部６０３と、開閉制御部６０４と、サブセグメント情報収集部６０５と、ユーザ情報収集部６０６と、安全レベル決定部６０７と、信頼レベル決定部６０８と、認証制御部６０９と、安全レベル評価値管理ＴＬ記憶部６１０と、サブセグメント情報管理ＴＬ記憶部６１１と、信頼レベル評価値管理ＴＬ記憶部６１２と、認証レベル管理ＴＬ記憶部６１３と、チケット管理ＴＬ記憶部６１４と、認証メソッド管理ＴＬ記憶部６１５と、を有する。

【００１４】

ネットワークＩＦ部６０１は、ビル内ネットワークシステムを構成する各装置（ネットワーク機器、情報機器）およびＷＡＮ４０と通信を行なうためのものであり、ネットワークケーブルを介してＳＷＨＵＢ２０に接続されている。

【００１５】

無線通信部６０２は、赤外線通信などの近距離無線通信によりユーザ端末８０およびＨＴ９０と通信を行なう。

【００１６】

指示受付部６０３は、ユーザに対する情報の表示および情報の入力受付を行なう。指示受付部６０３は、例えばタッチパネルなどの入出力装置であってもよい。あるいは、ネットワークＩＦ部６０１を介して接続された受付端末であってもよい。

【００１７】

開閉制御部６０４は、例えば自認証制御装置６０のサブセグメント１０が構築されたフロアの入口に設けられたドア、ゲートの開閉を制御する。なお、開閉制御部６０４を設ける代わりに、ネットワークＩＦ部６０１を介して自認証制御装置６０に接続された開閉制御装置を別途用意し、この開閉制御装置によりドア、ゲートの開閉を制御するようにして

もよい。自認証制御装置６０のサブセグメント１０が構築されたフロアの入口にドア、ゲートの開閉制御が不要の場合やドア、ゲートが設けられていない場合は、当然のことながら、開閉制御部６０４は不要である。

【００１８】

サブセグメント情報収集部６０５は、ネットワークＩＦ部６０１を介して、自認証制御装置６０のサブセグメント１０に属する管理対象システム７０を構成する各機器から属性情報を収集し、サブセグメント情報管理ＴＬ記憶部６１１に登録する。また、認証制御部６０９よりの指示に従いサブセグメント情報管理ＴＬ記憶部６１１に、自認証制御装置６０のサブセグメント１０を利用するユーザの属性情報を追加したり、削除したりする。さらに、サブセグメント情報収集部６０５は、サブセグメント情報管理ＴＬ記憶部６１１に登録されている情報を読み出して、安全レベル決定部６０７に送信する。

【００１９】

図３は、サブセグメント情報管理ＴＬ記憶部６１１の登録内容例を示す図である。図示するように、ビル内ネットワークシステム内で対象物を識別するための識別情報を登録するためのフィールド６１１１と、対象物の属性情報を登録するためのフィールド６１１２と、を備えてレコード６１１０が形成される。

【００２０】

ここで、サブセグメント情報管理ＴＬ記憶部６１１には、対象物をサブセグメントのエリアとするレコード６１１０ａ、対象物を管理対象システム７０の構成機器とするレコード６１１０ｂ、および、対象物をサブセグメント１０を利用するユーザとするレコード６１１０ｃの、３種類のレコード６１１０が登録される。レコード６１１０ａは、認証制御装置６０のオペレータによって予め登録されているレコードである。レコード６１１０ｂは、サブセグメント情報収集部６０５が管理対象システム７０の各構成機器から収集した属性情報に基づいて登録・削除するレコードである。そして、レコード６１１０ｃは、サブセグメント情報収集部６０５が認証制御部６０９の指示に従って登録・削除するレコードである。

【００２１】

レコード６１１０ａのフィールド６１１１には、例えば認証制御装置６０のオペレータが選んだユニークな番号が識別情報として登録される。レコード６１１０ｂのフィールド６１１１には、管理対象システム７０の構成機器のアドレス（例えばＩＰアドレス）が登録される。そして、レコード６１１０ｃのフィールド６１１１には、後述する認証チケットの仮想ＩＤが登録される。

【００２２】

フィールド６１１２に登録される属性情報は、サブセグメントの安全性への影響因子となる情報（環境情報）である。対象物の大まかな種別（種別（大））を示す情報と、該大まかな種別における詳細な種別（種別（小））を示す情報とを有する。レコード６１１０ａでは、種別（大）を示す情報として「エリア」が登録され、種別（小）を示す情報として「受付け」、「実験室」、「応接室」、「会議室」といったエリアの種別（属性）が登録される。レコード６１１０ｂでは、種別（大）を示す情報として「機器」が登録され、種別（小）を示す情報として「無線ＡＰ」、「ファイルサーバ」、「プリンタ」、「スキャナ」、「ＰＣ」といった機器の種別（属性）が登録される。そして、レコード６１１０ｃでは、種別（大）を示す情報として「ユーザ」が登録され、種別（小）を示す情報として「部長」、「課長」、「一般社員」、「部外者」、「顧客」といったユーザの地位・所属（属性）が登録される。

【００２３】

ユーザ情報収集部６０６は、認証制御部６０９よりの指示に従い、無線通信部６０２を介してユーザ端末８０あるいはＨＴ９０から、ユーザの信頼性への影響因子となる当該ユーザの属性情報（環境情報）を収集する。そして、収集したユーザの属性情報を信頼レベル決定部６０８に送信する。ユーザの属性情報としては、ユーザの識別情報であるユーザＩＤ、ユーザの地位（一般社員、係長、課長、部長、派遣社員、社外者など）、ユーザの

所属（所属部署など）、ビル内ネットワークシステムの利用頻度（毎日、週４～６日、週１～３日、週１日未満）、および、アクセス場所（入口、社内、公衆網（携帯網）、公衆網（無線ＬＡＮ）など）がある。

【００２４】

安全レベル決定部６０７は、安全レベル評価値管理ＴＬ記憶部６１０に登録されている情報と、サブセグメント情報収集部６０５を介してサブセグメント情報管理ＴＬ記憶部６１１から読み出した情報とを用いて、自認証制御装置６０のサブセグメント１０の安全レベルを決定する。そして、決定した安全レベルを認証制御部６０９に送信する。

【００２５】

図４は、安全レベル評価値管理ＴＬ記憶部６１０の登録内容例であり、図４（Ａ）は種別（大）の情報として「エリア」が登録されているサブセグメント情報管理ＴＬ記憶部６１１のレコード６１１０ａの評価値を決定するのに使用するテーブル６１０１ａ、図４（Ｂ）は種別（大）の情報として「機器」が登録されているサブセグメント情報管理ＴＬ記憶部６１１のレコード６１１０ｂの評価値を決定するのに使用するテーブル６１０１ｂ、そして、図４（Ｃ）は種別（大）の情報として「ユーザ」が登録されているサブセグメント情報管理ＴＬ記憶部６１１のレコード６１１０ｃの評価値を決定するのに使用するテーブル６１０１ｃである。各テーブル６１０１ａ～６１０１ｃには、種別（小）の情報６１０２毎に、該情報の評価値６１０３が登録されている。

【００２６】

安全レベル決定部６０７は、図４（Ａ）に示すテーブル６１０１ａを用いて、サブセグメント情報管理ＴＬ記憶部６１１から読み出したレコード６１１０ａの種別（小）の情報に対応する評価値を特定する。同様に、図４（Ｂ）に示すテーブル６１０１ｂを用いて、サブセグメント情報管理ＴＬ記憶部６１１から読み出した各レコード６１１０ｂの種別（小）の情報に対応する評価値を特定する。また、図４（Ｃ）に示すテーブル６１０１ｃを用いて、サブセグメント情報管理ＴＬ記憶部６１１から読み出した各レコード６１１０ｃの種別（小）の情報に対応する評価値を特定する。そして、以上のようにして求めたサブセグメント情報管理ＴＬ記憶部６１１の各レコード６１１０の評価値の総和を安全レベルに決定する。決定した安全レベルは、認証制御部６０９に送信される。なお、安全レベルは、値が大きいものほど、管理対象システム７０により高い安全性が要求されることを示している。

【００２７】

信頼レベル決定部６０８は、信頼レベル評価値管理ＴＬ記憶部６１２に登録されている情報と、ユーザ情報収集部６０６から受信したユーザの属性情報とを用いて、当該ユーザの信頼レベルを決定する。そして、決定した信頼レベルを認証制御部６０９に送信する。

【００２８】

図５は、信頼レベル評価値管理ＴＬ記憶部６１２の登録内容例であり、図５（Ａ）はユーザの属性（地位、所属）に対する評価値を決定するのに使用するテーブル６１２１ａ、図５（Ｂ）はユーザのビル内ネットワークシステムの利用頻度に対する評価値を決定するのに使用するテーブル６１２１ｂ、そして、図５（Ｃ）は自認証制御装置６０が属するサブセグメント１０へのユーザのアクセス場所に対する評価値を決定するのに使用する６１２１ｃである。各テーブル６１２１ａ～６１２１ｃには、それぞれ、ユーザ属性（地位・所属）、利用実績、アクセス場所６１２２毎に、評価値６１２３が登録されている。

【００２９】

信頼レベル決定部６０８は、図５（Ａ）に示すテーブル６１２１ａを用いて、ユーザ情報収集部６０６から受信したユーザ属性に対応する評価値を特定する。同様に、図５（Ｂ）に示すテーブル６１２１ｂを用いて、ユーザ情報収集部６０６から受信した利用頻度に対応する評価値を特定する。また、図５（Ｃ）に示すテーブル６１２１ｃを用いて、ユーザ情報収集部６０６から受信したアクセス場所に対応する評価値を特定する。そして、以上のようにして求めたユーザの各属性情報の評価値の総和を信頼レベルに決定する。決定した信頼レベルは、認証制御部６０９に送信される。なお、信頼レベルは、値が高いもの

ほど、ユーザの信頼性が高いことを示している。

【００３０】

認証制御部６０９は、認証されたユーザであることを証明する認証チケットの発行処理、および、管理対象システム７０の構成機器に対するアクセス権限を有することを証明するアクセスチケットの発行処理を行う。認証チケットの発行処理およびアクセスチケットの発行処理については後述する。

【００３１】

認証レベル管理ＴＬ記憶部６１３には、図６に示すように、信頼レベル６１３１および安全レベル６１３２の組合せ毎に、ユーザ認証の認証レベルが登録されている。認証レベルは、高いものほどより厳重なセキュリティチェックが必要なことを意味している。

【００３２】

認証メソッド管理記憶部６１５には、図７に示すように、認証レベル６１５１毎に、ユーザ認証の認証メソッド（認証方法）が登録されている。図７に示す例では、認証レベルが「低」の場合はパスワード認証が採用され、認証レベルが「中」の場合はパスワード認証および電子署名認証が採用され、そして、認証レベルが「高」の場合は生体認証および電子署名認証が採用されるようにしている。

【００３３】

チケット管理ＴＬ記憶部６１４には、認証制御部６０９が発行した認証チケットおよびアクセスチケットが登録される。

【００３４】

図８は、認証チケットの一例を説明するための図である。この例では、認証チケットをＸＭＬ形式の電子データとしている。図示するように、認証チケットは、仮想ＩＤ６１４１と、発行元の認証制御装置６０の識別情報（例えばＩＰアドレス）６１４２と、認証チケットの有効期限６１４３と、認証レベル６１４４と、ユーザ属性６１４５と、電子署名６１４６と、を有する。仮想ＩＤ６１４１は、認証チケットを識別するためのユニークな情報である。サブセグメント情報管理ＴＬ記憶部６１１に追加される当該認証チケットのユーザのレコード６１１０ｃのフィールド６１１１に、識別情報として登録される。ユニーク性を保証するために、仮想ＩＤ６１４１は、例えば発行元の認証制御装置６０の識別情報と、当該認証制御装置６０での認証チケットの生成回数に応じたシリアル番号とを繋げることで生成するようにしてもよい。認証チケットの有効期限６１４３は、例えば本日から所定期間経過後の日としてもよい。ユーザ属性６１４５には、ユーザ情報収集部６０６が収集したユーザの属性情報（ユーザＩＤ、地位、所属）が用いられる。そして、電子署名６１４５は、例えば仮想ＩＤ６１４１、発行元の認証制御装置６０の識別情報６１４２、認証チケットの有効期限６１４３、認証レベル６１４４およびユーザ属性６１４５のメッセージダイジェストに対して、発行元の認証制御装置６０の署名鍵を用いて生成するようにしてもよい。

【００３５】

図９は、アクセスチケットの一例を説明するための図である。この例も、図８に示す認証チケットと同様に、アクセスチケットをＸＭＬ形式の電子データとしている。図示するように、アクセスチケットは、仮想ＩＤ６１６１と、発行元の認証制御装置６０の識別情報（例えばＩＰアドレス）６１６２と、アクセスチケットの有効期限６１６３と、アクセス対象機器の識別情報６１６４と、ユーザ属性６１６５と、電子署名６１６６と、を有する。仮想ＩＤ６１６１は、アクセスチケットを識別するためのユニークな情報である。ユニーク性を保証するために、仮想ＩＤ６１６１は、例えば発行元の認証制御装置６０の識別情報と、当該認証制御装置６０でのアクセスチケットの生成回数に応じたシリアル番号とを繋げることで生成するようにしてもよい。アクセスチケットの有効期限６１６３は、例えば本日から所定期間経過後の日としてもよい。アクセス対象機器の識別情報６１６４には、アクセス対象機器のアドレス（例えばＩＰアドレス）が用いられる。ユーザ属性６１６５には、認証チケットに登録されているユーザ属性６１６５が用いられる。そして、電子署名６１６６は、例えば仮想ＩＤ６１６１、発行元の認証制御装置６０の識別情報６

１６２、認証チケットの有効期限６１６３、対象機器の識別情報６１６４およびユーザ属性６１６５のメッセージダイジェストに対して、発行元の認証制御装置６０の署名鍵を用いて生成するようにしてもよい。

【００３６】

以上のような構成を有する認証制御装置６０は、例えば図１０に示すような、ＣＰＵ９０１と、メモリ９０２と、ＨＤＤ等の外部記憶装置９０３と、ＣＤ-ＲＯＭやＤＶＤ-ＲＯＭ等の可搬性を有する記憶媒体９０４から情報を読み出す読取装置９０５と、キーボードやマウスなどの入力装置９０６と、ディスプレイなどの出力装置９０７と、ネットワークを介して相手装置と通信を行なうための通信装置９０８と、ユーザ端末８０やＨＴ９０と無線通信を行なうための無線通信装置９０９と、ドアやゲートの開閉機構に対して制御信号を出力するためのＩ/Ｏ装置９１０と、を備えたコンピュータシステムにおいて、ＣＰＵ９０１がメモリ９０２上にロードされた所定のプログラムを実行することで実現できる。この所定のプログラムは、読取装置９０５を介して記憶媒体９０４から、あるいは、通信装置９０８を介してネットワークから、外部記憶装置９０３にダウンロードされ、それから、メモリ９０２上にロードされてＣＰＵ９０１により実行されるようにしてもよい。また、読取装置９０５を介して記憶媒体９０４から、あるいは、通信装置９０８を介してネットワークから、メモリ９０２上に直接ロードされ、ＣＰＵ９０１により実行されるようにしてもよい。なお、この場合において、記憶部６１０～６１５には、メモリ９０２や外部記憶装置９０３や記憶媒体９０４が利用される。

【００３７】

図１１は認証制御装置６０の認証チケットの発行処理を説明するための図である。

【００３８】

認証制御部６０９は、指示受付部６０３を介してユーザから認証要求を受け取ると（ステップＳ１１０１）、サブセグメント情報収集部６０５に、自認証制御装置６０と同じサブセグメント１０に属する管理対象システム７０の構成変更有無の検出を依頼する。これを受けて、サブセグメント情報収集部６０５は、ネットワークＩＦ部６０１を介して、例えば自認証制御装置６０と同じサブセグメント１０のサブネットワークを有するＩＰアドレスに対して順番にＰＩＮＧ（Packet InterNet Groper）を送信し、その応答を確認することにより、自認証制御装置６０と同じサブセグメント１０に属する管理対象システム７０の各構成機器のＩＰアドレスを検出する。そして、検出した各構成機器のＩＰアドレスと、サブセグメント情報管理ＴＬ記憶部６１１に登録されている各構成機器のレコード６１１０ｂのフィールド６１１１に登録されている識別情報（ＩＰアドレス）とを比較して、管理対象システム７０の構成変更の有無を検出する（ステップＳ１１０２）。

【００３９】

ステップＳ１１０２で変更なしが検出された場合、つまり、検出した各構成機器のＩＰアドレスとサブセグメント情報管理ＴＬ記憶部６１１に登録されている各構成機器の識別情報とが一致する場合（ステップＳ１１０３でＮＯ）は、ステップＳ１１０８に移行する。一方、ステップＳ１１０２で変更ありが検出された場合（ステップＳ１１０３でＹＥＳ）、サブセグメント情報収集部６０５は、管理対象システム７０に構成機器が追加されたか、それとも、削除されたかをさらに調べる（ステップＳ１１０４）。

【００４０】

ステップＳ１１０４で構成機器が削除されたと判断された場合、つまり、検出した各構成機器のＩＰアドレスには存在しないＩＰアドレスが、構成機器の識別情報としてサブセグメント情報管理ＴＬ記憶部６１１に登録されている場合、サブセグメント情報収集部６０５は、当該識別情報がフィールド６１１１に登録されているレコード６１１０ｂをサブセグメント情報管理ＴＬ記憶部６１１から削除する（ステップＳ１１０７）。それから、ステップＳ１１０８に移行する。一方、ステップＳ１１０４で構成機器が追加されたと判断された場合、つまり、検出した各構成機器のＩＰアドレスの中に、サブセグメント情報管理ＴＬ記憶部６１１に構成機器の識別情報として登録されていないＩＰアドレスが存在する場合、サブセグメント情報収集部６０５は、例えばＳＮＭＰ（Simple Network Manag

ement Protocol）を用いて、当該ＩＰアドレスを持つ機器から属性情報（上述の種別（大）および種別（小）の情報を含む）を取得する（ステップＳ１１０５）。そして、セグメント情報管理ＴＬ記憶部６１１に機器のレコード６１１０ｂを追加し、当該レコード６１１０ｂのフィールド６１１１に当該ＩＰアドレスを、フィールド６１１２に収集した属性情報を登録する（ステップＳ１１０６）。それから、ステップＳ１１０８に移行する。

【００４１】

次に、ステップＳ１１０８において、サブセグメント情報収集部６０５は、サブセグメント情報管理ＴＬ記憶部６１１に登録されている全てのレコード６１１０を読み出して、安全レベル検定部６０７に送信し、安全レベルの決定を依頼する。これを受けて、安全レベル決定部６１０は、サブセグメント情報収集部６０５から受け取ったサブセグメント情報管理ＴＬ記憶部６１１の各レコード６１１０と、安全レベル評価値管理ＴＬ記憶部６１０とを用いて、安全レベルを決定する。そして、決定した安全レベルを認証制御部６０９に送信する。

【００４２】

次に、認証制御部６０９は、ユーザ情報収集部６０６にユーザの属性情報の収集を依頼する。これを受けて、ユーザ情報収集部６０６は、無線通信部６０２を介してＨＴ９０と通信し、ＨＴ９０からユーザの属性情報（ユーザＩＤ、地位、所属、利用頻度など）を入手する。あるいは、無線通信部６０２を介してユーザ端末８０と通信し、ユーザ端末８０経由でＨＴ９０からユーザの属性情報を入手する（ステップＳ１１０９）。この際、ＨＴ９０に認証チケットが登録されているならば、当該認証チケットもユーザの属性情報と共にＨＴ９０から入手する。

【００４３】

次に、ユーザ情報収集部６０６は、ＨＴ９０から入手したユーザの属性情報を信頼レベル検定部６０８に送信し、信頼レベルの決定を依頼する。この際、ＨＴ９０から認証チケットを入手しているならば、当該認証チケットも併せて信頼レベル決定部６０８に送信する。これを受けて、信頼レベル決定部６０８は、ユーザ情報収集部６０６から受け取ったユーザの属性情報と、信頼レベル評価値管理ＴＬ記憶部６１２とを用いて、信頼レベルを決定する（ステップＳ１１１０）。そして、決定した信頼レベルを認証制御部６０９に送信する。この際、ユーザ情報収集部６０６から認証チケットを受け取っているならば、当該認証チケットも併せて認証制御部６０９に送信する。なお、本実施形態では、信頼レベルを決定するのに用いるアクセス場所の情報として（図５（Ｃ）参照）、フロア１Ｆに設置された認証制御装置60_1では「入口」、フロア２Ｆ以上に設置された認証制御装置60_2、60_3では「社内」となるように、予め信頼レベル決定部６０８に設定している。

【００４４】

次に、認証制御部６０９は、安全レベル決定部６０７および信頼レベル決定部６０８から安全レベルおよび信頼レベルを受け取ると、受け取った安全レベルおよび信頼レベルの組合せに対応するユーザ認証の認証レベルを認証レベル管理ＴＬ記憶部６１３（図６参照）から検索し、検索した認証レベルをユーザ認証に利用する認証レベルに決定する（ステップＳ１１１０ａ）。

【００４５】

次に、認証制御部６０９は、信頼レベル決定部９０８から認証チケット（ＨＴ９０に登録されている認証チケット）を受け取っていない場合（ステップＳ１１１１でＮＯ）、ステップＳ１１１３に移行する。受け取っている場合（ステップＳ１１１１でＹＥＳ）は、当該認証チケットに記述されている認証レベル６１４４（図８参照）と、ステップＳ１１１０ａで決定した認証レベルとを比較し、後者が前者よりも高いか否かを調べる（ステップＳ１１１２）。決定した認証チケットの認証レベルがＨＴ９０に登録されている認証レベルより高い場合（ステップＳ１１１２でＹＥＳ）は、ユーザの再認証が必要であるとして、ステップＳ１１１３に移行する。一方、決定した認証チケットの認証レベルがＨＴ９０に登録されている認証レベルより高い場合（ステップＳ１１１２でＹＥＳ）は、ユーザの再認証が必要でないとして、ステップＳ１１１８に移行する。

【００４６】
ステップＳ１１１３では、ステップＳ１１１０ａで決定した認証レベルに対応する認証メソッドを認証メソッド管理ＴＬ記憶部６１５から検索し、検索した認証メソッドをユーザ認証に用いる認証メソッドに決定する。そして、決定した認証メソッドによる認証に必要な認証情報をユーザより収集する（ステップＳ１１１３）。具体的には、認証メソッドが「パスワード認証」の場合、例えばパスワードの入力を促すメッセージを表示し、指示受付部６０３を介してユーザよりパスワードの入力を受付けることにより、認証情報を収集する。また、認証メソッドが「パスワード認証+電子署名認証」の場合、上述のようにしてユーザよりパスワードの入力を受付けると共に、無線通信部６０２を介してＨＴ９０に署名対象データ（例えば乱数）を送信し、当該署名対象データに対する電子署名を受け取ることにより、認証情報を収集する。また、認証メソッドが「生体認証+電子署名認証」の場合、上述のようにして送信データに対する電子署名を受付けると共に、例えば生体情報を採取する旨のメッセージを表示して、図示していない生体情報採取装置（例えば指紋採取装置や虹彩採取装置）を用いて生体情報を採取することにより、認証情報を収集する。
【００４７】
次に、認証制御部６０９は、ステップＳ１１０９で収集したユーザの属性情報に含まれているユーザＩＤ、認証メソッドの指定および収集した認証情報を含む認証依頼を生成し、ネットワークＩＦ部６０１を介して認証装置５０に送信する。これを受けて、認証装置５０は、指定された認証メソッドを用いて認証情報の認証を行なう。そして、その認証結果を認証依頼元の認証制御装置６０に送信する（ステップＳ１１１４）。ここで、認証装置５０と連携するためのインターフェースとしては、例えばディレクトリの標準プロトコルであるＬＤＡＰ（Lightweight Directory Access Protocol）やリモードユーザ認証の標準プロトコルであるＲａｄｉｕｓ（Remote Authentication Dial-In User Service）を利用できる。認証装置５０の詳細は後述する。
【００４８】
次に、認証制御部６０９は、認証装置５０から受け取った認証結果が認証不成立を示している場合（ステップＳ１１１５でＮＯ）、例えば図示していない表示装置にエラーメッセージを表示するなどのエラー処理を行い（ステップＳ１１１７）、その後、このフローを終了する。一方、認証装置５０から受け取った認証結果が認証成立を示している場合（ステップＳ１１１５でＹＥＳ）、認証チケット（図８参照）を生成し、これをチケット管理ＴＬ記憶部６１４に記憶する。また、無線通信部６０２を介してＨＴ９０に格納する。あるいは、無線通信部６０２を介して、ユーザ端末８０経由でＨＴ９０に格納する（ステップＳ１１１６）。それから、ステップＳ１１１８に移行する。
【００４９】
さて、ステップＳ１１１８において、認証制御部６０９は、ステップＳ１１１２で再認証の必要なしと判断された認証チケット、あるいは、ステップＳ１１１６で新たに発行した認証チケットの仮想ＩＤおよびユーザ属性を、サブセグメント情報収集部６０５に通知して、サブセグメント情報管理ＴＬ記憶部６１１へのレコード追加を依頼する。これを受けて、サブセグメント情報収集部６０５は、サブセグメント情報管理ＴＬ記憶部６１１にユーザのレコード６１１０ｃを追加し、当該レコード６１１０ｃのフィールド６１１１に、認証制御部６０９から通知された仮想ＩＤを登録し、フィールド６１１２に認証制御部６０９から通知されたユーザ属性を登録する。
【００５０】
次に、認証制御部６０９は、ステップＳ１１１２で再認証の必要なしと判断された認証チケット、あるいは、ステップＳ１１１６で新たに発行した認証チケットの仮想ＩＤを指定を伴うレコード削除要求を生成し、ネットワークＩＦ部６０１を介して、他の認証制御装置６０に送信する（ステップＳ１１１９）。これを受けて、他の認証制御装置６０のサブセグメント収集部６０５は、レコード削除要求で指定された仮想ＩＤが識別情報としてフィールド６１１１に登録されているユーザのレコード６１１０ｃをサブセグメント情報

管理ＴＬ記憶部６１１から検索し、検索したレコード６１１０ｃを削除する。

【００５１】

それから、認証制御部６０９は、開閉制御部６０４に、自認証制御装置６０のサブセグメント１０が構築されたフロアにユーザが入場できるように、ドア、ゲートを開閉させる（ステップＳ１１２０）。その後、このフローを終了する。

【００５２】

図１２は認証制御装置６０のアクセスチケットの発行処理を説明するための図である。

【００５３】

認証制御部６０９は、ネットワークＩＦ部６０１を介して、自認証制御装置６０のサブセグメント１０に属する管理対象システム７０の構成機器より当該機器へのアクセス要求が転送されてくると（ステップＳ１２０１）、当該アクセス要求に添付されている認証チケットの正当性を検証する（ステップＳ１２０２）。具体的には、現在日が認証チケットの有効期限６１４３を経過しておらず、且つ、認証チケットの電子署名６１４６の署名検証が成立した場合に、認証チケットが正当であると判断する。なお、認証制御装置６０は、認証制御装置６０各々の署名検証鍵を有しており、認証チケットの発行元６１４２の認証制御装置６０に対応付けられた署名検証鍵を用いて認証チケットの電子署名６１４６の署名を検証するものとする。

【００５４】

さて、認証制御部６０９は、認証チケットの正当性が確認されなかった場合（ステップＳ１２０３でＮＯ）、その旨のメッセージをネットワークＩＦ部６０１を介して、アクセス要求の転送元の構成機器に送信するなどのエラー処理を行い（ステップＳ１２０８）、このフローを終了する。

【００５５】

一方、認証制御部６０９は、認証チケットの正当性が確認された場合（ステップＳ１２０３でＹＥＳ）は、アクセスチケット（図９参照）を生成し、これをチケット管理ＴＬ記憶部６１４に記憶する。また、ネットワークＩＦ部６０１を介してアクセス要求の転送元の構成機器に送信する（ステップＳ１２０４）。

【００５６】

次に、認証制御部６０９は、安全レベル決定部６０７に安全レベルの決定を依頼する。これを受けて、安全レベル決定部６０７は、サブセグメント情報収集部６０５を介して、サブセグメント情報管理ＴＬ記憶部６１１に登録されている全てのレコード６１１０を読み出す。そして、読み出した各レコード６１１０と、安全レベル評価値管理ＴＬ記憶部６１０とを用いて、安全レベルを決定し、決定した安全レベルを認証制御部６０９に送信する。認証制御部６０９は、この安全レベルを、ネットワークＩＦ部６０１を介してアクセス要求の転送元の構成機器に送信する（ステップＳ１２０５）。

【００５７】

次に、認証制御装置６０９は、アクセス要求の転送元の構成機器を介して当該構成機器に設定するセキュリティポリシを受信すると（ステップＳ１２０６）、このセキュリティポリシにステップＳ１２０３で発行したアクセスチケットの仮想ＩＤを付与して、アクセス要求の転送元の構成機器に返送する（ステップＳ１２０７）。それから、このフローを終了する。これを受けて、アクセス要求の転送元の構成機器は、アクセスチケットを伴うアクセス要求に対して、このアクセスチケットの仮想ＩＤ６１６１に対応付けられたセキュリティポリシを適用する。その後、このフローを終了する。

【００５８】

図１に戻って説明を続ける。認証装置５０は、認証制御装置６０から受信した認証依頼に従いユーザ認証を行なって、その結果を認証制御装置６０に通知する。

【００５９】

図１３は、認証装置５０の概略図である。図示するように、ネットワークＩＦ部５０１と、認証処理部５０２と、ビル内ネットワークシステムのユーザ毎に認証情報が登録された認証情報ＤＢ（データベース）５０３と、を有する。ネットワークＩＦ部５０１は、Ｗ

ＡＮ４０を介してビル内ネットワークシステムの各認証制御装置６０と通信を行なう。認証処理部５０２は、ネットワークＩＦ部５０１を介して認証制御装置６０より受信した認証依頼で指定されている認証メソッドにより、認証情報ＤＢ５０３を用いて認証依頼対象の認証情報を認証する。そして、認証結果を認証依頼元の認証制御装置６０へ送信する。

【００６０】

図１４は、認証情報ＤＢ５０３の登録内容例を示す図である。ユーザのユーザＩＤが登録されたフィールド５０３１と、当該ユーザの認証情報が登録されたフィールド５０３２とを備えて１つのレコードが形成される。フィールド５０３２は、当該ユーザのパスワードが登録されたサブフィールド５０３２１と、当該ユーザの署名検証鍵（当該ユーザのＨＴ９０に登録されている署名鍵と対の鍵）が登録されたサブフィールド５０３２２と、当該ユーザの生体情報（指紋、虹彩など）が登録されたサブフィールド５０３２３と、を有する。

【００６１】

以上のような構成を有する認証装置５０は、例えば図１０に示す構成から無線通信装置９０９およびＩ/Ｏ装置９１０を省略した一般的な構成を有するコンピュータシステムにおいて、ＣＰＵ９０１がメモリ９０２上にロードされた所定のプログラムを実行することで実現できる。この所定のプログラムは、読取装置９０５を介して記憶媒体９０４から、あるいは、通信装置９０８を介してネットワークから、外部記憶装置９０３にダウンロードされ、それから、メモリ９０２上にロードされてＣＰＵ９０１により実行されるようにしてもよい。また、読取装置９０５を介して記憶媒体９０４から、あるいは、通信装置９０８を介してネットワークから、メモリ９０２上に直接ロードされ、ＣＰＵ９０１により実行されるようにしてもよい。なお、この場合において、認証情報ＤＢ５０３には、メモリ９０２や外部記憶装置９０３や記憶媒体９０４が利用される。

【００６２】

図１５は、認証装置５０の認証処理を説明するための図である。

【００６３】

認証処理部５０２は、ネットワークＩＦ部５０１を介して、認証制御装置６０より認証依頼を受け取ると（ステップＳ１５０１）、当該認証依頼に含まれているユーザＩＤがフィールド５０３１に登録されているレコードを認証情報ＤＢ５０３から抽出する（ステップＳ１５０２）。それから、認証処理部５０２は、当該認証依頼で指定されている認証メソッドを特定する（ステップＳ１５０３）。本実施形態では、上述したように、パスワード認証、生体情報認証および電子署名認証のうちの少なくとも１つの組合せが認証メソッドで指定されるものとしている。

【００６４】

次に、認証処理部５０２は、指定された認証メソッドがパスワード認証を含んでいるか否かを調べる（ステップＳ１５０４）。含んでいない場合は、ステップＳ１５０６に移行する。含んでいる場合は、認証依頼に含まれるパスワードとステップＳ１５０２で抽出したレコードのサブフィールド５０３２１に登録されているパスワードとが一致するか否かを調べる（ステップＳ１５０５）。そして、一致する場合は、ステップＳ１５０６に移行する。一致しない場合は、認証不成立と判断し、その旨を示す認証結果を、認証依頼元の認証制御装置６０に送信する（ステップＳ１５１２）。

【００６５】

次に、ステップＳ１５０６において、認証処理部５０２は、指定された認証メソッドが生体情報認証を含んでいるか否かを調べる。含んでいない場合は、ステップＳ１５０８に移行する。含んでいる場合は、認証依頼に含まれる生体情報とステップＳ１５０２で抽出したレコードのサブフィールド５０３２３に登録されている生体情報とが一致するか否かを調べる（ステップＳ１５０７）。そして、一致する場合は、ステップＳ１５０８に移行する。一致しない場合は、認証不成立と判断し、その旨を示す認証結果を、認証依頼元の認証制御装置６０に送信する（ステップＳ１５１２）。

【００６６】

次に、ステップＳ１５０８において、認証処理部５０２は、指定された認証メソッドが電子署名認証を含んでいるか否かを調べる。含んでいない場合は、ステップＳ１５１１に移行する。含んでいる場合は、認証依頼に含まれている電子署名をステップＳ１５０２で抽出したレコードのサブフィールド５０３２２に登録されている署名検証鍵で復号し、その復号結果が認証依頼に含まれている署名対象データと一致するか否かを調べる（ステップＳ１５０９）。そして、一致する場合は、ステップＳ１５１１に移行する。一致しない場合は、認証不成立と判断し、その旨を示す認証結果を、認証依頼元の認証制御装置６０に送信する（ステップＳ１５１２）。

【００６７】

次に、ステップＳ１５１１において、認証処理部５０２は、認証成立と判断し、その旨を示す認証結果を、認証依頼元の認証制御装置６０に送信する。

【００６８】

図１に戻って説明を続ける。ＨＴ９０は、ユーザの属性情報（ユーザＩＤ、地位、所属、利用頻度）、認証情報（パスワード）、認証チケット、アクセスチケットなどの各種情報の格納、および、電子署名の生成を行なう。

【００６９】

図１６はＨＴ９０の概略図である。図示するように、無線通信ＩＦ部９０１と、署名生成部９０２と、記憶部９０３と、主制御部９０４とを有する。無線通信部９０１は、赤外線通信などの近距離無線通信によりユーザ端末８０および認証制御装置６０と通信を行なう。記憶部９０３には、ユーザの属性情報（ユーザＩＤ、地位、所属、利用頻度）、認証情報（パスワード）および署名鍵が予め登録されている。但し、ユーザの属性情報のうちの利用頻度は更新される情報である。また、記憶部９０３には、認証チケットおよびアクセスチケットが登録される。署名生成部９０２は、記憶部９０３に記憶されている署名鍵を用いて、無線通信部９０１を介してユーザ端末８０より受信したデータに対する電子署名を生成する。そして、主制御部９０４は、各部９０１～９０３を統括制御する。ＨＴ９０には、ＣＰＵ、耐タンパ構造を持つメモリ、および、赤外線通信などの近距離無線通信を行なうためのＩ/Ｏ装置を備えた通常のハードウエアトークンにおいて、ＣＰＵがメモリに格納された所定のプログラムを実行することで実現できる。この場合、記憶部９０３にはメモリが利用される。

【００７０】

図１７は、ＨＴ９０の動作を説明するための図である。ＨＴ９０は、ユーザ端末８０あるいは認証制御装置６０に近づくと、赤外線通信などの近距離無線通信により通信相手装置との間に通信路を確立する。そして、通信路が確立されると、このフローが開始される。なお、通信相手装置との通信路は、相互認証などによりセキュリティが確保されたものとするとよい。

【００７１】

まず、主制御部９０４は、無線通信部９０１を介して通信相手装置より属性情報送信要求を受信すると（ステップＳ１７０１）、記憶部９０３に認証チケットが格納済みであるか否かを調べる（ステップＳ１７０２）。格納済みである場合、ユーザの属性情報および認証チケットを記憶部９０３から読み出して、通信相手装置へ送信する（ステップＳ１７０３）。一方、認証チケットが格納済みでないならば、ユーザの属性情報を記憶部９０３から読み出して、通信相手装置へ送信する（ステップＳ１７０４）。

【００７２】

また、主制御部９０４は、無線通信部９０１を介して通信相手装置より署名要求を受信すると（ステップＳ１７０５）、当該署名要求に含まれている署名対象データ（例えば乱数）を署名生成部９０２に渡す。これを受けて署名生成部９０２は、記憶部９０３に記憶されている署名鍵を用いて署名対象データに対する電子署名を生成する。主制御部９０４は、この電子署名を通信相手装置へ送信する（ステップＳ１７０６）。

【００７３】

また、主制御部９０４は、無線通信部９０１を介して通信相手装置より認証チケットあ

るいはアクセスチケットを受信すると（ステップＳ１７０７）、これを記憶部９０３に格納する（ステップＳ１７０８）。

【００７４】

また、主制御部９０４は、無線通信部９０１を介して通信相手装置より認証チケットあるいはアクセス対象機器の識別情報６１６４が指定されたアクセスチケットの送信要求を受信すると（ステップＳ１７０９）、記憶部９０３に該当するチケットが格納済みであるか否かを調べる（ステップＳ１７１０）。格納済みである場合、該当するチケットを記憶部９０３から読み出して、通信相手装置へ送信する（ステップＳ１７１１）。その後、記憶部９０３に記憶されているユーザの属性情報の利用頻度を更新する（ステップＳ１７１２）。一方、格納済みでないならばエラーメッセージを通信相手装置へ送信する（ステップＳ１７１３）。

【００７５】

図１に戻って説明を続ける。ユーザ端末８０は、各種情報のＨＴ９０への書込みおよび読出しを制御する。また、ＨＴ９０に対して電子署名の生成を依頼する。

【００７６】

図１８はユーザ端末８０の概略図である。図示するように、無線通信部８０１と、無線ＬＡＮＩＦ部８０２と、入力部８０３と、表示部８０４と、記憶部８０５と、主制御部８０６とを有する。無線通信部８０１は、赤外線通信などの近距離無線通信によりＨＴ９０および認証制御装置６０と通信を行なう。無線ＬＡＮＩＦ部８０２は、無線ＡＰ７０１と通信を行なうためのインターフェースである。入力部８０３はユーザより指示や情報の入力を受付ける。表示部８０４は情報を表示する。記憶部８０５は必要に応じて各種情報を記憶する。そして、主制御部８０６は、各部８０１～８０３を統括制御する。ユーザ端末８０には、ＣＰＵ、メモリ、操作ボタンやタッチパネルなどの入力装置、液晶パネルなどの表示装置、赤外線通信などの近距離無線通信を行なうためのＩ/Ｏ装置、および、無線ＬＡＮ通信装置を備えたＰＤＡ（Personal Digital Assistant）などの情報端末において、ＣＰＵがメモリに格納された所定のプログラムを実行することで実現できる。この場合において、記憶部８０３にはメモリが利用される。

【００７７】

図１９は、ユーザ端末８０の動作を説明するための図である。ユーザ端末８０は、ＨＴ９０に近づくと、赤外線通信などの近距離無線通信によりＨＴ９０との間に通信路を確立する。また、無線ＡＰ７０１の管轄エリアに属する場合、この無線ＡＰ７０１との間に通信路を確立する。そして、両通信路が確立されると、このフローが開始される。なお、ＨＴ９０および無線ＡＰ７０１各々との通信路は、相互認証などによりセキュリティが確保されたものとするとよい。

【００７８】

まず、主制御部８０６は、入力装置８０３を介してユーザより、ユーザが位置するフロアに構築されたサブセグメント１０に属する管理対象システム７０の構成機器に対するアクセス指示を受け取ると（ステップＳ１９０１）、無線通信部８０１を介してＨＴ９０にアクセスチケット送信要求を送信する（ステップＳ１９０２）。そして、ＨＴ９０からアクセスチケットを受信したならば（ステップＳ１９０３でＹＥＳ）、ステップＳ１９１２に移行する。一方、ＨＴ９０からアクセスチケットが格納されていないことを示すエラーメッセージを受信したならば（ステップＳ１９０３でＮＯ）、無線通信部８０１を介してＨＴ９０に認証チケット送信要求を送信する（ステップＳ１９０４）。それから、ステップＳ１９０５に移行する。

【００７９】

ステップＳ１９０５において、主制御部８０６は、ＨＴ９０から認証チケットが格納されていないことを示すエラーメッセージを受信したならば、表示部８０４にエラーメッセージを表示させるなどして、ユーザ認証されていないことをユーザに知らせ（ステップＳ１９１５）、その後、このフローを終了する。一方、ＨＴ９０から認証チケットを受信したならば、この認証チケットを伴うアクセスチケット発行要求を、無線ＬＡＮＩＦ部８０

２を介してアクセス対象の構成機器に送信する（ステップＳ１９０６）。そして、アクセス対象の構成機器からアクセスチケットを受信したならば（ステップＳ１９０７でＹＥＳ）、ステップＳ１９０８に移行する。一方、アクセス対象の構成機器からエラーメッセージを受信した場合（ステップＳ１９０７でＮＯ）、表示部８０４にエラーメッセージを表示させるなどして、認証チケットが正当でないこと（例えば期限切れ）をユーザに知らせ（ステップＳ１９１５）、その後、このフローを終了する。

【００８０】

ステップＳ１９０８において、主制御部８０６は、無線通信部８０１を介してＨＴ９０に受信したアクセスチケットを送信し、このアクセスチケットをＨＴ９０の記憶部９０３に記憶させる（Ｓ１９０８）。次に、主制御部８０６は、無線ＬＡＮＩＦ部８０２を介してアクセス対象の構成機器から、ユーザが位置するフロアに構築されたサブセグメント１０の安全レベルおよびアクセス対象の構成機器に設定可能なセキュリティポリシの項目の情報を受信する（ステップＳ１９０９）。そして、これらの情報を含むセキュリティポリシの設定受付画面を表示部８０４に表示して、ユーザよりセキュリティポリシの設定を受付ける（ステップＳ１９１０）。

【００８１】

図２０はユーザ端末８０の表示部８０４に表示されるセキュリティポリシ設定受付画面の一例を示している。図示するように、セキュリティポリシ設定受付画面は、ユーザが位置するフロアに構築されたサブセグメント１０の安全レベルを表示する表示欄８０４１と、アクセス対象の構成機器に設定可能なセキュリティポリシの項目各々について、設定の有無を受付けるための指示入力欄８０４２と、設定ボタン８０４３と、を有する。ユーザは入力部８０３を介してカーソル８０４５を操作し、指示入力欄８０４２各々に設定の有無を入力することができる。なお、ユーザ端末８０に、サブセグメント１０の安全レベルを表示するインジケータを表示部８０４とは別に設けてもよい。

【００８２】

さて、図２０に示すようなセキュリティポリシ設定受付画面において、ユーザにより入力部８０３を介してカーソル８０４５が操作され、設定ボタン８０４３が選択されたならば、主制御部８０６は、指示入力欄８０４２各々に入力されている設定の有無を各セキュリティポリシ項目の設定情報とし、無線ＬＡＮＩＦ部８０２を介して、アクセス対象の構成機器に送信する。そして、アクセス対象の構成機器よりセキュリティポリシ情報の設定完了が通知されるのを待つ（ステップＳ１９１１）。それから、ステップＳ１９１２に移行する。

【００８３】

ステップＳ１９１２において、主制御部８０６は、無線ＬＡＮＩＦ部８０２を介してアクセス対象の構成機器にアクセスチケットを送信する。そして、アクセス対象の構成機器よりアクセス許可を受信したならば（ステップＳ１９１３でＹＥＳ）、アクセス対象の構成機器へのアクセスを開始する（ステップＳ１９１４）。一方、アクセス対象の構成機器よりエラーメッセージを受信したならば（ステップＳ１９１３でＮＯ）、表示部８０４にエラーメッセージを表示させるなどして、アクセスチケットが正当でないこと（例えば期限切れ）をユーザに知らせ（ステップＳ１９１５）、その後、このフローを終了する。

【００８４】

図１に戻って説明を続ける。管理対象システム７０の各構成機器は、当該管理対象システム７０と同じサブセグメント１０に属する認証制御装置６０との間で行われる、自構成機器にアクセスするためのアクセスチケット発行の仲介処理を行う。また、アクセスチケットを用いてユーザ端末８０からのアクセスを制御する。

【００８５】

図２１は管理対象システム７０の構成機器の概略図である。ここでは無線ＡＰ７０１の概略構成を例示している。図示するように、無線ＡＰ７０１は、ネットワークＩＦ部７０１１と、無線ＬＡＮＩＦ部７０１２と、アクセス制御部７０１３と、装置本来の機能を実現する部分である装置本体７０１４とを有する。プリンタ７０２やスキャナ７０３やファ

イルサーバ７０４の場合は、無線ＬＡＮＩＦ部７０１２は不要である。ネットワークＩＦ部６０１は、ビル内ネットワークシステムを構成する各装置（認証制御装置６０、ネットワーク機器、情報機器）と通信を行なうためのものであり、ネットワークケーブルを介してＳＷＨＵＢ２０に接続されている。無線ＬＡＮＩＦ部７０１２は、無線ＬＡＮ端末（ユーザ端末８０を含む）と無線通信を行なうためのものである。そして、アクセス制御部７０１３はアクセスチケット発行の仲介処理およびユーザ端末８０からのアクセス制限処理を行う。なお、アクセス制御部７０１３は、ＡＳＩＣ（Application Specific Integrated Circuit）などの集積ロジックＩＣによりハード的に実行されるものでもよいし、あるいは、ＤＳＰ（Digital Signal Processor）などの計算機によりソフトウエア的に実行されるものでもよい。

【００８６】

図２２は、管理対象システム７０を構成する各機器のアクセス制御部７０１３の動作を説明するための図であり、図２２（Ａ）はアクセス制限処理の動作フローを、そして、図２２（Ｂ）はアクセスチケット発行処理の動作フローを示している。

【００８７】

まず、図２２（Ａ）を用いてアクセス制限処理を説明する。このフローは、アクセス制御部７０１３がネットワークＩＦ部７０１１あるいは無線ＬＡＮＩＦ部７０１２を介してユーザ端末８０よりアクセス要求を受け取ると開始される。

【００８８】

アクセス制御部７０１３は、受信したアクセス要求に付加されているアクセスチケットの正当性を調べる（ステップＳ２２０１）。具体的には、現在日がアクセスチケットの有効期限６１６３を経過しておらず、且つ、アクセスチケットの電子署名６１６６の署名検証が成立した場合に、アクセスチケットが正当であると判断する。なお、アクセス制御部７０１３は、認証制御装置６０各々の署名検証鍵を有しており、アクセスチケットの発行元６１６２の認証制御装置６０に対応付けられた署名検証鍵を用いてアクセスチケットの電子署名６１６６の署名を検証するものとする。

【００８９】

次に、アクセス制御部７０１３は、アクセスチケットの正当性が確認できたならば（ステップＳ２２０２でＹＥＳ）、アクセス許可メッセージをアクセス要求送信元のユーザ端末８０に送信する（ステップＳ２２０３）。そして、当該ユーザ端末８０の装置本体７０１４に対するアクセスを許可する（ステップＳ２２０４）。この際、正当性を確認したアクセスチケットの仮想ＩＤ６１６１に対応付けられて設定されているセキュリティポリシがあるならば、当該ユーザ端末からのアクセス要求に当該設定されているセキュリティポリシを適用する。

【００９０】

一方、アクセス制御部７０１３は、アクセスチケットの正当性を確認できなかった場合（ステップＳ２２０２でＮＯ）、エラーメッセージをアクセス要求送信元のユーザ端末８０に送信する（ステップＳ２２０５）。そして、当該ユーザ端末８０の装置本体７０１４に対するアクセスを拒否する（ステップＳ２２０６）。

【００９１】

次に、図２２（Ｂ）を用いてアクセスチケット発行の仲介処理を説明する。このフローは、アクセス制御部７０１３がネットワークＩＦ部７０１１あるいは無線ＬＡＮＩＦ部７０１２を介してユーザ端末８０よりアクセスチケット発行要求を受け取ると開始される。

【００９２】

アクセス制御部７０１３は、受信したアクセスチケット発行要求を当該要求に付加されている認証チケットと共に、自構成機器と同じサブセグメント１０に属する認証制御装置６０に転送する（ステップＳ２２５１）。

【００９３】

次に、アクセス制御部７０１３は、認証制御装置６０からアクセスチケット発行要求の応答としてアクセスチケットを受信すると、これをユーザ端末８０に転送する（ステップ

Ｓ２２５２）。
【００９４】
次に、アクセス制御部７０１３は、認証制御装置６０から自構成機器と同じサブセグメント１０の安全レベルおよび自構成機器に設定可能なセキュリティポリシの項目の情報を受信すると、これをユーザ端末８０に転送する（ステップＳ２２５３）。
【００９５】
次に、アクセス制御部７０１３は、自構成機器に設定するセキュリティポリシの情報を含んだセキュリティポリシ設定要求をユーザ端末８０から受信すると、これを認証制御装置６０に転送する（ステップＳ２２５４）。そして、認証制御装置６０からアクセスチケットの仮想ＩＤ６１６１および設定すべきセキュリティポリシの情報を含むセキュリティポリシ設定指示を受信すると、これを自構成機器に設定すると共に、セキュリティポリシの設定が完了した旨の通知をユーザ端末８０に送信する。その後、当該アクセスチケットを伴うアクセス要求に、当該セキュリティポリシを適用する（ステップＳ２２５５）。
【００９６】
次に、認証チケットの発行に際して、ＨＴ９０、認証制御装置６０および認証装置５０間で行なわれるやり取りを説明する。
【００９７】
図２３は、認証チケットの発行に際して、ＨＴ９０、認証制御装置６０および認証装置５０間で行なわれる情報の流れを示す図である。
【００９８】
認証制御装置６０はユーザより認証要求を受付けると（Ｔ２３０１）、図１１に示すフローを開始する。そして、ユーザの信頼レベルを決定するためにユーザ属性情報送信要求をＨＴ９０に送信する（Ｔ２３０２）。
【００９９】
ＨＴ９０は、認証制御装置６０よりユーザ属性情報送信要求を受信すると、図１７に示すフローにより認証チケットが格納済みか否かを調べる。ここでは、認証チケットが格納済みでないとする。この場合、ＨＴ９０は、ユーザ属性情報を認証制御装置６０に送信する（Ｔ２３０３）。
【０１００】
認証制御装置６０は、ＨＴ９０から認証チケットを受信しなかった場合、ユーザ属性情報を用いて決定した信頼レベルおよびサブセグメント１０の安全レベルに基づいて認証レベルを決定し、決定した認証レベルに対応する認証メソッドを特定する。ここでは、「パスワード認証+電子署名認証」が特定されたものとする。この場合、認証制御装置６０は、パスワード要求をユーザに要求し、ユーザよりパスワードの入力を受付ける（Ｔ２３０４）。また、署名対象データを生成し、これをＨＴ９０に送信して電子署名を要求する（Ｔ２３０６）。
【０１０１】
ＨＴ９０は、認証制御装置６０より電子署名要求を受信すると、当該電子署名要求に付加されている署名対象データの電子署名を生成して、認証制御装置６０に送信する（Ｔ２３０７）。
【０１０２】
さて、認証制御装置６０は、特定した認証メソッドに必要な認証情報（パスワード、電子署名および署名対象データ）が揃ったならば、これらの情報と、ユーザ属性情報に含まれているユーザＩＤと、認証メソッドの指定とを含む認証依頼を生成して、認証装置５０に送信する（Ｔ２３０８）。
【０１０３】
認証装置５０は、認証制御装置６０より認証依頼を受信すると、図１５に示すフローにより認証処理を行う。そして、認証結果を認証制御装置５０に送信する（Ｔ２３０９）。ここでは、認証成立の認証結果が認証制御装置５０に送信されたものとする。
【０１０４】

認証制御装置６０は、認証装置５０より認証成立を示す認証結果を受信すると、認証チケットを生成し、ＨＴ９０に送信する（Ｔ２３１０）。

【０１０５】

次に、アクセスチケットの発行に際して、ＨＴ９０、ユーザ端末８０、構成機器７０１～７０３（７０ｘとする）および認証制御装置６０間で行なわれるやり取りを説明する。

【０１０６】

図２４は、アクセスチケットの発行に際して、ＨＴ９０、ユーザ端末８０、構成機器７０ｘおよび認証制御装置６０間で行なわれる情報の流れを示す図である。

【０１０７】

ユーザ端末８０はユーザより構成機器７０ｘへのアクセス指示を受付けると（Ｔ２４０１）、図１９に示すフローを開始する。そして、ＨＴ９０に構成機器７０ｘの識別情報の指定を含むアクセスチケット送信要求を送信する（Ｔ２４０２）。

【０１０８】

ＨＴ９０は、ユーザ端末８０からアクセスチケット送信要求を受信すると、図１７に示すフローにより構成機器７０ｘに対するアクセスチケットが格納済みか否かを調べる。ここでは、アクセスチケットが格納済みでないとする。この場合、ＨＴ９０は、エラーメッセージをユーザ端末８０に送信する（Ｔ２４０３）。

【０１０９】

ユーザ端末８０は、ＨＴ９０からエラーメッセージを受信したならば、さらに、認証チケット送信要求をＨＴ９０に送信する（Ｔ２４０４）。これを受けて、ＨＴ９０は、認証チケットをユーザ端末８０に送信する（Ｔ２４０５）。

【０１１０】

さて、ユーザ端末８０は、ＨＴ９０から認証チケットを受信したならば、この認証チケットを含むアクセスチケット発行要求を、アクセス対象である構成機器７０ｘへ送信する（Ｔ２４０６）。そして、構成機器７０ｘは、図２２（Ｂ）のフローにより、ユーザ端末８０より受信したアクセスチケット発行要求を、自構成機器と同じサブセグメント１０に属する認証制御装置６０に転送する（Ｔ２４０７）。

【０１１１】

認証制御装置６０は、構成機器７０ｘよりアクセスチケット発行要求を受信すると、図１２のフローを開始する。そして、アクセスチケット発行要求に含まれている認証チケットの正当性を確認した後、アクセスチケット発行要求の転送元である構成機器７０ｘに対するアクセスチケットを生成し、該構成機器７０ｘへ送信する（Ｔ２４０８）。このアクセスチケットは、構成機器７０ｘ、ユーザ端末８０を転送され、最終的にＨＴ９０に格納される（Ｔ２４０９、Ｔ２４１０）。

【０１１２】

次に、認証制御装置６０は、サブセグメント１０の安全レベルおよびアクセスチケット発行要求の転送元である構成機器７０ｘに設定可能なセキュリティポリシの情報を、構成機器７０ｘに送信する（Ｔ２４１１）。構成機器７０ｘは、これらの情報をユーザ端末８０に送信する（Ｔ２４１２）。

【０１１３】

ユーザ端末８０は、構成機器７０ｘを介して、サブセグメント１０の安全レベルおよび当該構成機器７０ｘに設定可能なセキュリティポリシの情報を受信すると、図２０に示すようなセキュリティポリシ設定画面を表示し、ユーザよりセキュリティポリシの設定を受付ける。受付けたセキュリティポリシは、構成機器７０ｘを介して認証制御装置６０に転送される（Ｔ２４１３、Ｔ２４１４）。

【０１１４】

次に、認証制御装置６０は構成機器７０ｘよりセキュリティポリシを受信すると、このセキュリティポリシをアクセスチケットの仮想ＩＤに対応付けて、構成機器７０ｘに設定する（Ｔ２４１５）。

【０１１５】

さて、ユーザ端末８０は、ＨＴ９０に構成機器７０ｘの識別情報の指定を含むアクセスチケット送信要求を送信する（Ｔ２４１６）。そして、ＨＴ９０から構成機器７０ｘに対するアクセスチケットを受信すると（Ｔ２４１７）、これを構成機器７０ｘに送信して、構成機器７０ｘに対するアクセスを要求する（Ｔ２４１８）。これにより、構成機器７０ｘは、図２２（Ａ）のフローによりアクセスを制御する。

【０１１６】

以上、本発明の一実施形態を説明した。

【０１１７】

本実施形態によれば、認証制御装置６０は、ＨＴ９０に格納されたユーザの属性情報に応じた当該ユーザの信頼レベルおよび当該ユーザが利用しようとしているサブセグメント１０の安全レベルに基づいて認証レベルが決定され、当該認証レベルに対応する認証メソッドが当該ユーザのユーザ認証に適用される。したがって、ユーザの認証メソッドの決定、サブセグメントの状況（コンテキスト）に対応させることができる。

【０１１８】

また、本実施形態によれば、ユーザが第１のサブセグメント１０から第２のサブセグメント１０に移動する場合、第１のサブセグメント１０を利用するために当該第１のサブセグメント１０に属する認証制御装置６０が発行した当該ユーザの認証チケットの認証レベルが、第２のサブセグメント１０に属する認証制御装置６０が決定した当該第２のサブセグメントを利用するための認証に要求される認証レベルよりも高い場合、認証装置５０に対して認証依頼を再度行なわない。したがって、複数のサブセグメント１０（サービス）の利用を認証装置５０での１度の認証で利用する、いわゆるシングルサインオンを実現することができる。

【０１１９】

また、本実施形態によれば、認証制御装置６０は、ユーザ端末８０から提示された認証チケットに基づいて、管理対象システム７０の構成機器に対するアクセスを許可するためのアクセスチケットを発行する。そして、ユーザ端末８０はこのアクセスチケットを用いて管理対象システム７０の構成機器にアクセスする。したがって、個々の構成機器を利用するために、認証装置５０に対して認証依頼をその都度行わないで済む。したがって、複数の構成機器（サービス）の利用を認証装置５０での１度の認証で利用する、いわゆるシングルサインオンを実現することができる。

【０１２０】

なお、本発明は上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【０１２１】

例えば、上記の実施形態では、フロア単位でサブセグメント１０が構築されている場合を例にとり説明した。そして、認証制御装置６０に、当該認証制御装置６０が属するサブセグメント１０が構築されているフロアへの入場を制限するドア・ゲートの開閉制御部を６０４を設けた場合を例にとり説明した。しかし、本発明はこれに限定されない。サブセグメント１０は、フロアやルームといった物理的条件を単位として構築するようにしてもよいし、電子会議室といった仮想空間を単位として構築するようにしてもよい。

【０１２２】

図２５は、本発明を電子会議室システムに適用した場合の一例を示している。この例では、電子会議室毎にサブセグメント１０が構築されており、各サブセグメント１０は、認証制御装置６０と、管理対象システムの構成機器に相当する会議室サーバ７０４とを有する。ユーザが所望の電子会議室のサブセグメント１０を利用する場合、当該サブセグメント１０に属する認証制御装置６０は、図１１に示すフロー（但しステップＳ１１２０の開閉制御は不要）を実行する。そして、ユーザが当該サブセグメント１０の会議室サーバ７０４にアクセスする場合、当該サブセグメント１０に属する認証制御装置６０は、図１２に示すフローを実行する。

【０１２３】

図２５に示す例においても、認証制御装置６０は、ＨＴ９０に格納されたユーザの属性情報に応じた当該ユーザの信頼レベルおよび当該ユーザが利用しようとしているサブセグメント１０（電子会議室）の安全レベルに基づいて認証レベルが決定され、当該認証レベルに対応する認証メソッドが当該ユーザのユーザ認証に適用される。また、ユーザが第１のサブセグメント１０（電子会議室Ａ）から第２のサブセグメント１０（電子会議質Ｂ）に移動する場合、第１のサブセグメント１０を利用するために当該第１のサブセグメント１０に属する認証制御装置６０が発行した当該ユーザの認証チケットの認証レベルが、第２のサブセグメント１０に属する認証制御装置６０が決定した当該第２のサブセグメントを利用するための認証に要求される認証レベルよりも高い場合、認証装置５０に対して認証依頼を再度行なわない。したがって、複数のサブセグメント１０（電子会議室）の利用を認証装置５０での１度の認証で利用する、いわゆるシングルサインオンを実現することができる。

【０１２４】

また、上記の実施形態では、ユーザ属性情報や認証チケットやアクセスチケットなどの各種情報の格納および電子署名の生成を、ＨＴ９０で行わせる場合を例にとり説明したが、情報の格納および電子署名の生成は、ユーザ端末８０で行わせるようにしても構わない。さらに、いずれかの認証制御装置６０に認証装置６０としての機能を持たせるようにしても構わない。

【図面の簡単な説明】

【０１２５】

【図１】図１は本発明の一実施形態が適用されたビル内ネットワークシステムの概略図である。

【図２】図２は認証制御装置６０の概略図である。

【図３】図３はサブセグメント情報管理ＴＬ記憶部６１１の登録内容例を示す図である。

【図４】図４は安全レベル評価値管理ＴＬ記憶部６１０の登録内容例を示す図である。

【図５】図５は信頼レベル評価値管理ＴＬ記憶部６１２の登録内容例を示す図である。

【図６】図６は認証レベル管理ＴＬ記憶部６１３の登録内容例を示す図である。

【図７】図７は認証メソッド管理記憶部６１５の登録内容例を示す図である。

【図８】図８は認証チケットの一例を説明するための図である。

【図９】図９はアクセスチケットの一例を説明するための図である。

【図１０】図１０は認証制御装置６０のハードウエア構成例を示す図である。

【図１１】図１１は認証制御装置６０の認証チケットの発行処理を説明するための図である。

【図１２】図１２は認証制御装置６０のアクセスチケットの発行処理を説明するための図である。

【図１３】図１３は認証装置５０の概略図である。

【図１４】図１４は認証情報ＤＢ５０３の登録内容例を示す図である。

【図１５】図１５は認証装置５０の認証処理を説明するための図である。

【図１６】図１６はＨＴ９０の概略図である。

【図１７】図１７はＨＴ９０の動作を説明するための図である。

【図１８】図１８はユーザ端末８０の概略図である。

【図１９】図１９はユーザ端末８０の動作を説明するための図である。

【図２０】図２０はユーザ端末８０の表示部８０４に表示されるセキュリティポリシ設定受付画面の一例を示す図である。

【図２１】図２１は管理対象システム７０の構成機器の概略図である。

【図２２】図２２は管理対象システム７０を構成する各機器のアクセス制御部７０１３の動作を説明するための図である。

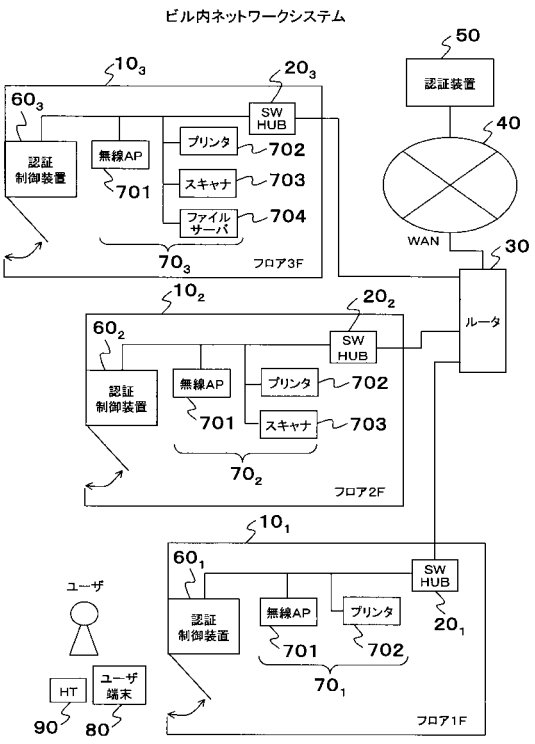
【図２３】図２３は認証チケットの発行に際して、ＨＴ９０、認証制御装置６０および認証装置５０間で行なわれる情報の流れを示す図である。

【図２４】図２４はアクセスチケットの発行に際して、ＨＴ９０、ユーザ端末８０、構成

機器７０ｘおよび認証制御装置６０間で行なわれる情報の流れを示す図である。
【図２５】図２５は本発明の電子会議室システムへの適用例を示す図である。
【符号の説明】
【０１２６】
１０：サブセグメント、２０：ＳＷＨＵＢ、３０：ルータ、４０：ＷＡＮ、５０：認証装置、６０：認証制御装置、７０：管理対象システム、８０：ユーザ端末、９０：ＨＴ、７０１：無線ＡＰ、７０２：プリンタ、７０３：スキャナ、７０４：ファイルサーバ

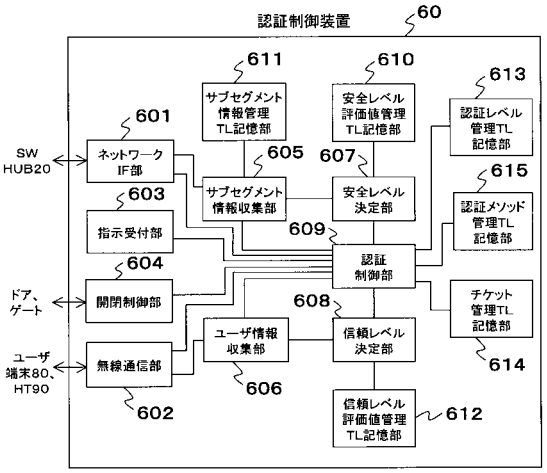
【図１】

図1



【図２】

図2



【図３】

図3

サブセグメント情報管理TL記憶部611

識別情報 (6111)	属性情報 (6112)	
****	種別(大):エリア、種別(小):実験室	6110a
****	種別(大):機器、種別(小):無線AP	
****	種別(大):機器、種別(小):プリンタ	6110b
****	種別(大):機器、種別(小):スキャナ	
****	種別(大):機器、種別(小):PC	
****	種別(大):ユーザ、種別(小):部長	6110c
****	種別(大):ユーザ、種別(小):社外者	

6110

【図４】

図4

安全レベル評価値管理TL記憶部610

(A) 6101a 種別(大):エリア

種別(小)	評価値
受付け	5
応接室	10
会議室	15
事務室	15
実験室	20

6102 6103

(B) 6101b 種別(大):機器

種別(小)	評価値
無線AP	5
PC	10
プリンタ	15
スキャナ	15
サーバ	20

(C) 6101c 種別(大):ユーザ

種別(小)	評価値
社外者	5
一般社員	5
係長	10
課長	15
部長以上	20

【図５】

図5

信頼レベル評価値管理TL記憶部612

(A) 6121a

ユーザ属性	評価値
部署社員	20
部外社員	15
部署派遣社員	10
部外派遣社員	10
社外者	5

6122 6123

(B) 6121b

利用頻度	評価値
毎日	20
週4～6日	15
週1～3日	10
週1日未満	5

(C) 6121c

アクセス場所	評価値
入口	20
社内	15
公衆網(携帯網)	10
公衆網(無線LAN)	5

【図６】

図6

認証レベル管理TL記憶部613

6131 6132

安全レベル＼信頼レベル	8未満	8～12	12以上
8未満	認証レベル中	認証レベル低	認証レベル低
8～12	認証レベル高	認証レベル中	認証レベル低
12以上	認証レベル高	認証レベル高	認証レベル中

【図７】

図7

認証メソッド管理TL記憶部615

認証レベル (6151)	認証メソッド (6152)
低	パスワード認証
中	パスワード認証+電子署名認証
高	生体認証+電子証明書認証

【図８】

図8

認証チケット

6141	仮想ID	*********
6142	発行元	www.***.com
6143	有効期限	2003-07-15T10:00:00
6144	認証レベル	中
6145	ユーザ属性	ユーザID:** 地位:部長 所属:**部署
6146	電子署名	********

【図９】

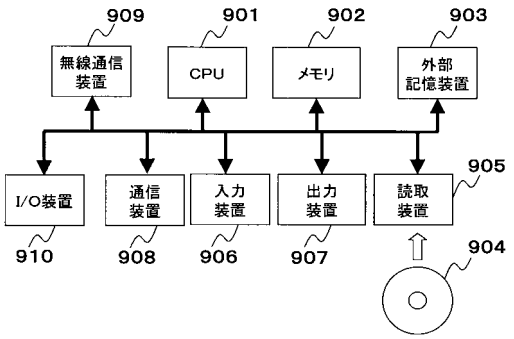
図9

アクセスチケット

6161	仮想ID	*********
6162	発行元	www.***.com
6163	有効期限	2003-07-15T10:00:00
6164	対象機器	printer.***.***
6165	ユーザ属性	ユーザID:** 地位:社外者 所属:-
6166	電子署名	********

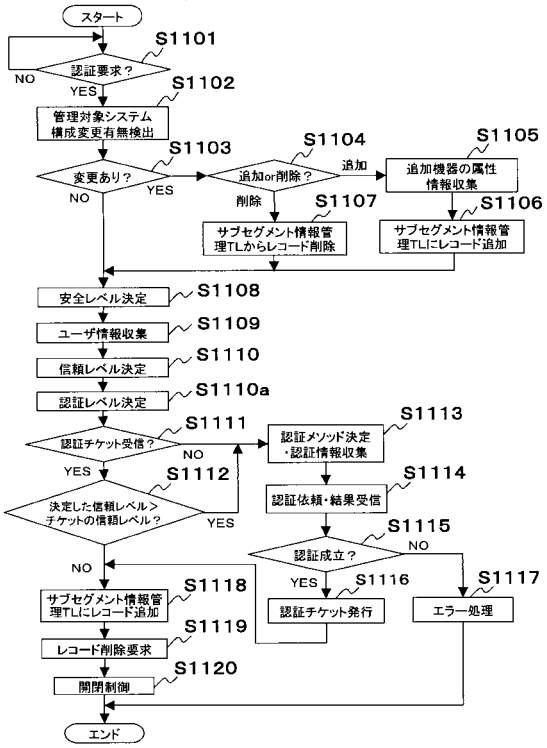
【図１０】

図10



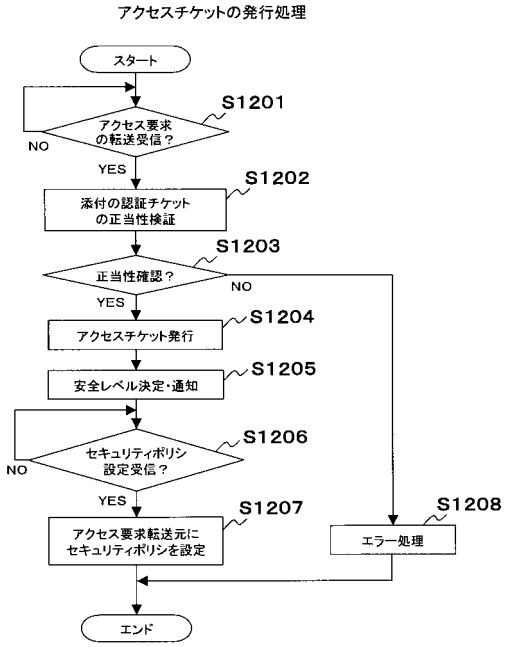
【図１１】

図11



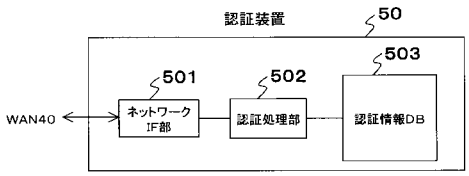
【図１２】

図12



【図１３】

図13



【図１４】

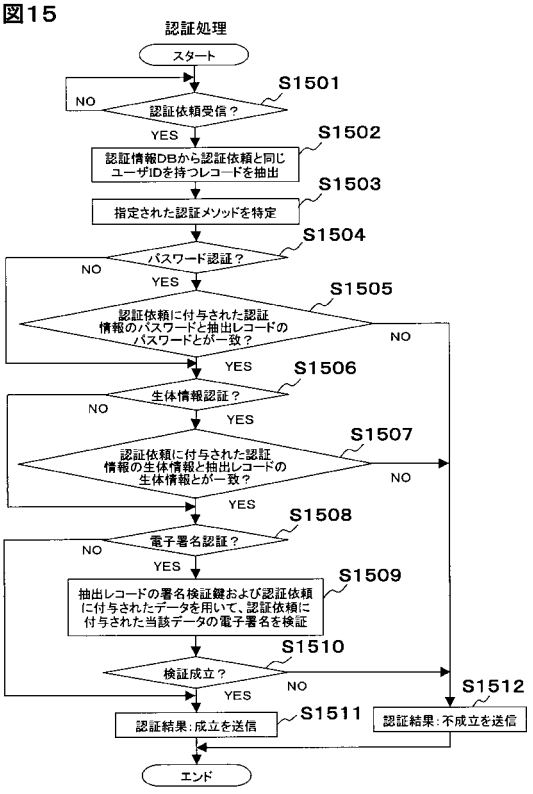
図14

認証情報DB503

5031	50321	50322	5032	50323
ユーザID	認証情報			
	パスワード	署名検証鍵	生体情報（指紋、虹彩など）	
****	****	****	****	
****	****	****	****	
：	：	：	：	

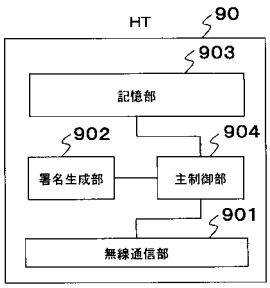
【図１５】

図15



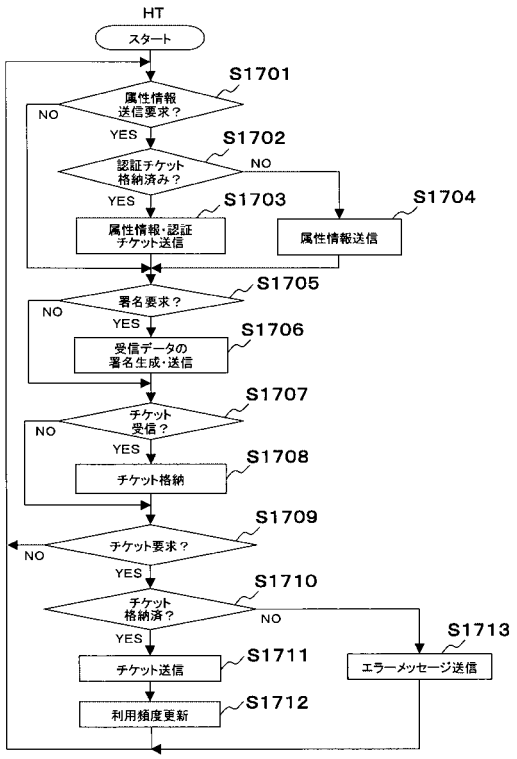
【図１６】

図16



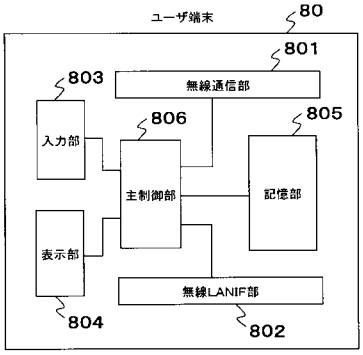
【図１７】

図17



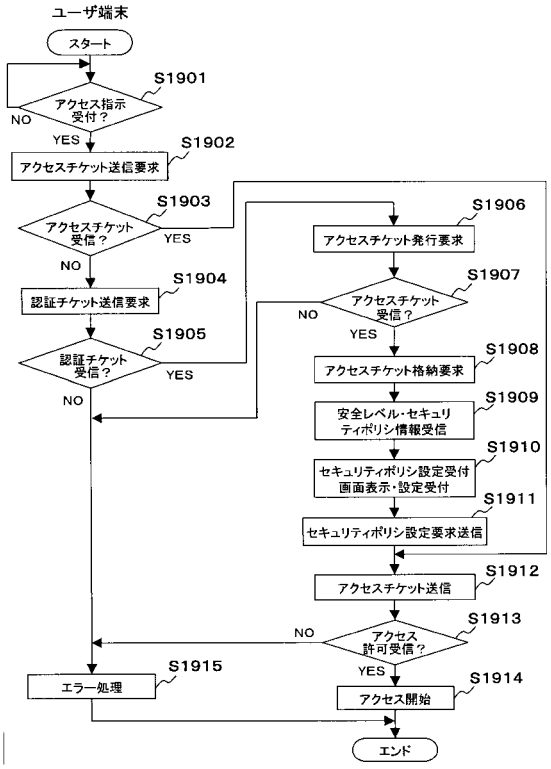
【図１８】

図18



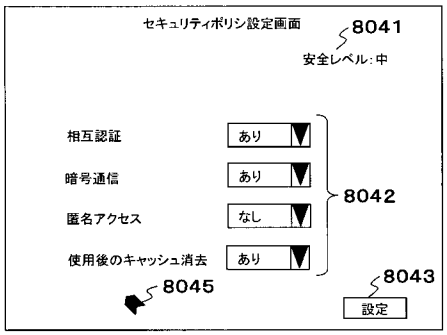
【図１９】

図19



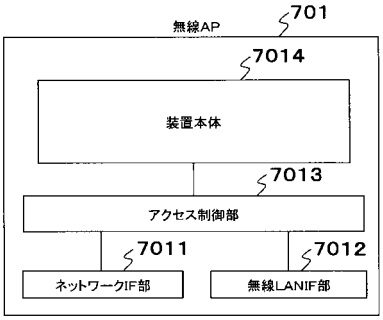
【図２０】

図20



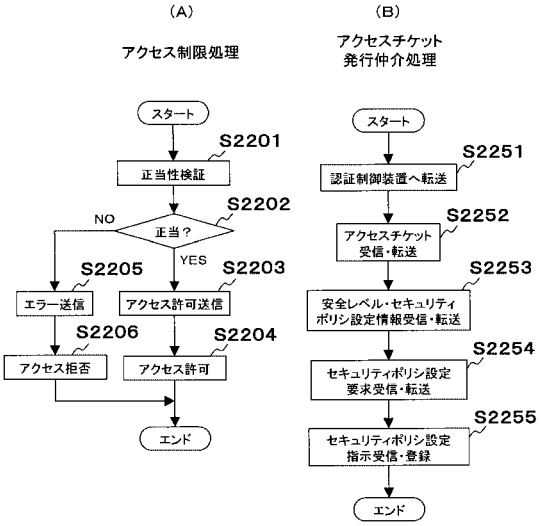
【図２１】

図21



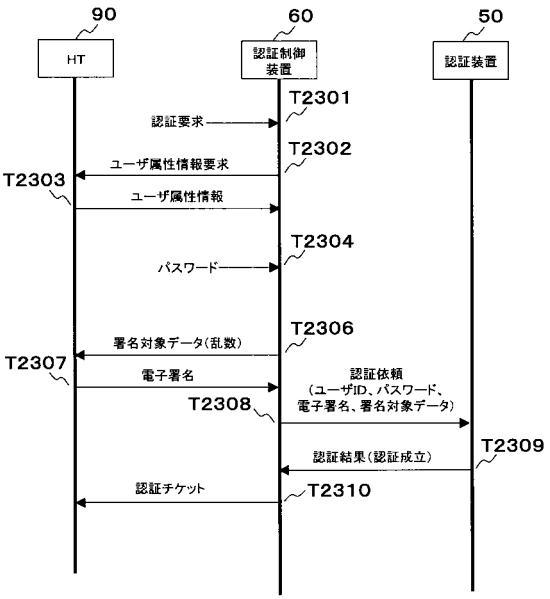
【図２２】

図22



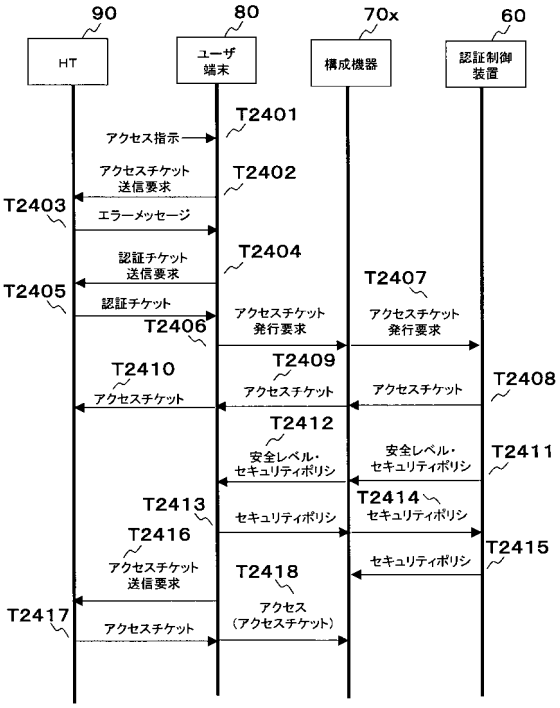
【図２３】

図23



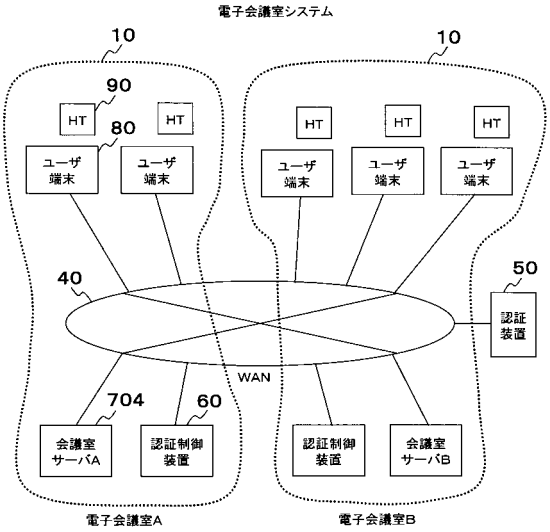
【図２４】

図24



【図２５】

図25


電子会議室システム
10
10
90
HT
HT
80
ユーザ端末
ユーザ端末
HT
HT
HT
ユーザ端末
ユーザ端末
ユーザ端末
40
50
認証装置
WAN
704
60
会議室サーバA
認証制御装置
認証制御装置
会議室サーバB
電子会議室A
電子会議室B

フロントページの続き

(56)参考文献 特開２００３－１９６５６６（ＪＰ，Ａ）
特表２００２－５１８７２０（ＪＰ，Ａ）
特開平１１－０２５０５１（ＪＰ，Ａ）
特開２０００－１０５７４７（ＪＰ，Ａ）
特開２０００－０１０９３０（ＪＰ，Ａ）
特開２００１－２８２７４７（ＪＰ，Ａ）
特開２００２－３１８７８８（ＪＰ，Ａ）
特開平１０－２６９１８４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２０
Ｅ０５Ｂ ４９／００
Ｇ０８Ｂ ２５／０４