(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-114869
(P2010-114869A)
(43)公開日　平成22年5月20日(2010.5.20)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601A	5B285
G06F 21/20	(2006.01)	G06F	15/00	330A	5J104
H04L 9/32	(2006.01)	G06F	15/00	330D	
		H04L	9/00	601E	
		H04L	9/00	673D	

審査請求 有　請求項の数 19　OL　（全 21 頁）

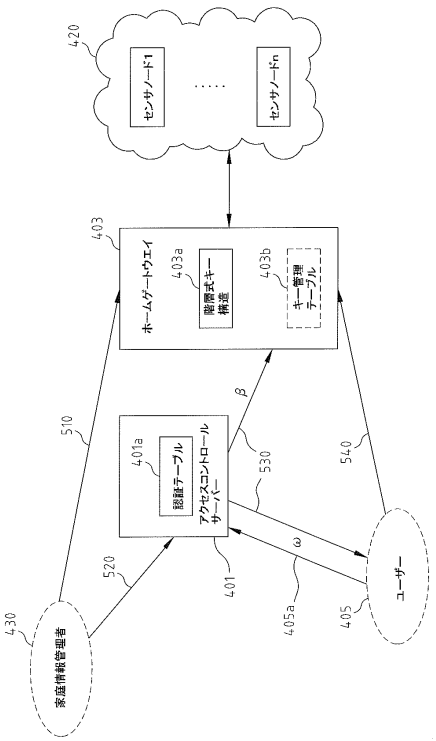
(21)出願番号　特願2008-320546 (P2008-320546)
(22)出願日　平成20年12月17日 (2008.12.17)
(31)優先権主張番号　097143211
(32)優先日　平成20年11月7日 (2008.11.7)
(33)優先権主張国　台湾 (TW)

(71)出願人　390023582
財団法人工業技術研究院
INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE
台湾新竹縣竹東鎮中興路四段１９５號
１９５ Chung Hsing Rd., Sec. 4, Chutung, Hsin-Chu, Taiwan R. O. C
(74)代理人　100082304
弁理士　竹本　松司
(74)代理人　100088351
弁理士　杉山　秀雄
(74)代理人　100093425
弁理士　湯田　浩一

最終頁に続く

(54)【発明の名称】階層式キーに基づくアクセスコントロールシステムと方法

(57)【要約】
【課題】階層式キーに基づくアクセスコントロールシステムと方法の提供。
【解決手段】このシステムはアクセスコントロールサーバーＡＣＳ、ホームゲートウエイ、ホームネットワークに配置された複数のセンサ装置を包含する。該ＡＣＳはユーザーのアクセス権限と認証コードを設定し、ユーザーパスワードの関係データとユーザーのアクセス権限の情報を保存する。該ホームゲートウエイは階層式キー構造に基づき構築された権限レベルと権限キーを記録する。ユーザーがＡＣＳにログインしてアクセス要求する時、該ユーザーと該ホームゲートウエイ間のワンタイム通信キーが、該ＡＣＳより発行されたチケットとトークンの交換により構築される。これによりユーザーは該センサ装置の情報にアクセス許可される。
【選択図】図４



【特許請求の範囲】
【請求項１】
階層式キーに基づくアクセスコントロールシステムにおいて、
ユーザーのアクセスコントロール権限と授権検証コードを設定し、並びにユーザーのパスワード関係データとアクセス権限の情報を保存するアクセスコントロールサーバーと、
階層式キー構造により構築されたアクセス権限と権限キーを記録したホームゲートウエイと、
センシングネットワークに配置された複数のセンサノードと、
を包含し、ユーザーが該アクセスコントロールサーバーにログオンしてアクセス要求する時、該ユーザーと該ホームゲートウエイの商法が該アクセスコントロールサーバーの発行したチケットとトークンを交換することにより、ワンタイムの通信キーを生成し、該ユーザーの該複数のセンサノードの情報へのアクセスを許可することを特徴とする、階層式キーに基づくアクセスコントロールシステム。
【請求項２】
請求項１記載の階層式キーに基づくアクセスコントロールシステムにおいて、該ホームゲートウエイはキー管理テーブルを有し、該キー管理テーブルに該階層式キー構造により生成されたアクセス権限、該複数のセンサノードの識別コードとそれに対応するアクセス権限、及び最高権限のキーを記録することを特徴とする、階層式キーに基づくアクセスコントロールシステム。
【請求項３】
請求項１記載の階層式キーに基づくアクセスコントロールシステムにおいて、該アクセスコントロールサーバー中に第１認証テーブルが設けられ、該第１認証テーブルに既に登録されたユーザーＩＤ、ユーザーパスワードに関係する認証コード、及びユーザー権限の関係認証値が記録されることを特徴とする、階層式キーに基づくアクセスコントロールシステム。
【請求項４】
請求項１記載の階層式キーに基づくアクセスコントロールシステムにおいて、該ホームゲートウエイ中に第２認証テーブルが設けられ、該第２認証テーブルに既に登録されたユーザーＩＤ、及びユーザー権限が記録されることを特徴とする、階層式キーに基づくアクセスコントロールシステム。
【請求項５】
請求項１記載の階層式キーに基づくアクセスコントロールシステムにおいて、該ホームゲートウエイは、
権限キー及びセンサキーを生成し、該権限キーはアクセスコントロール設定に用いられ、該センサキーは該ホームゲートウエイとセンサノードの間の情報伝達暗号化に用いられる、階層式キーモジュールと、
ユーザーのチケットでのログイン検証を請け負うチケット検証及びメッセージ処理センターと、
を包含することを特徴とする、階層式キーに基づくアクセスコントロールシステム。
【請求項６】
請求項１記載の階層式キーに基づくアクセスコントロールシステムにおいて、該アクセスコントロールサーバーは、
ユーザーのアクセス権限を設定し並びに該アクセス権限の検証コードを保存する検証コード授権代理モジュールと、
ユーザーと該ホームゲートウエイのセッションキーを協調並びに生成し、合法ユーザーが該ホームゲートウエイのアクセス授権を要求する時、該チケットとトークンの交換と対比により、該ホームゲートウエイに該ユーザーの合法性を知らせる、ユーザー検証授権モジュールとチケットトークン交換センターと、
を包含したことを特徴とする、階層式キーに基づくアクセスコントロールシステム。
【請求項７】

請求項１記載の階層式キーに基づくアクセスコントロールシステムにおいて、該階層式キー構造中、低レベルの権限キーはそれより高いレベルの権限キーより生成されることを特徴とする、階層式キーに基づくアクセスコントロールシステム。

【請求項８】

請求項１記載の階層式キーに基づくアクセスコントロールシステムにおいて、該複数のセンサノードの各センサノードの検証キーは該センサノードの所属レベルの権限キーと該センサノードの識別コードにより生成されることを特徴とする、階層式キーに基づくアクセスコントロールシステム。

【請求項９】

階層式キーに基づくアクセスコントロール方法において、

ホームゲートウエイ中に階層式キー構造を構築するステップ、

アクセスコントロールサーバー中にユーザーアクセスコントロール権限と授権検証コードを構築するステップ、

ユーザーがアクセスコントロールサーバーにログオンしてアクセス要求する時、該アクセスコントロールサーバーがユーザーに対応する授権検証コードによりチケットとトークンを発行するステップ、

該ユーザーと該ホームゲートウエイの双方が、該チケットとトークンの交換を通して、ワンタイムの通信キーを生成し、該ユーザーにホームネットワークに配置された複数のセンサノードの情報へのアクセスを許可するステップ、

を包含することを特徴とする、階層式キーに基づくアクセスコントロール方法。

【請求項１０】

請求項９記載の階層式キーに基づくアクセスコントロール方法において、該階層式キー構造の構築ステップは、

最高レベルの権限キーが存在するか否かを検査するステップ、

最高レベルの権限キーが存在する時、全てのセンサノードの検証キーが全て構築完成しているかを確認するステップ、

最高レベルの権限キーが不存在の時、この最高レベルの最高レベルの権限キーを生成し、並びに全てのセンサノードの検証キーが既に生成完成したかを確認するステップ、

全てのセンサノードの検証キーが生成完成した時、キーの生成を終了するステップ、

全てのセンサノードの検証キーが生成完成していない時、次の検証キー未生成のセンサノードの識別コード及びその所属レベルを入力し、並びに該センサノードの検証キーを計算し並びに該センサノードに割り当て、その後、全てのセンサノードの検証キーが既に生成完成したかを確認するステップに戻るステップ、

を包含したことを特徴とする、階層式キーに基づくアクセスコントロール方法。

【請求項１１】

請求項１０記載の階層式キーに基づくアクセスコントロール方法において、該階層式キー構造中、低レベルの権限キーはそれより高いレベルの権限キーより生成されることを特徴とする、階層式キーに基づくアクセスコントロール方法。

【請求項１２】

請求項１０記載の階層式キーに基づくアクセスコントロール方法において、該複数のセンサノードの各センサノードの検証キーは該センサノードの所属レベルの権限キーと該センサノードの識別コードにより生成されることを特徴とする、階層式キーに基づくアクセスコントロール方法。

【請求項１３】

請求項１１記載の階層式キーに基づくアクセスコントロール方法において、該権限キー生成は非可逆関数方式の計算によることを特徴とする、階層式キーに基づくアクセスコントロール方法。

【請求項１４】

請求項１２記載の階層式キーに基づくアクセスコントロール方法において、該検証キー生成は非可逆関数方式の計算によることを特徴とする、階層式キーに基づくアクセスコン

トロール方法。
【請求項１５】
請求項９記載の階層式キーに基づくアクセスコントロール方法において、該アクセスコントロールサーバー中のユーザーアクセス権限は、
ユーザーに提供された単一のＩＤ、パスワード及びユーザー権限を該アクセスコントロールサーバーに提供するステップ、
該アクセスコントロールサーバーが該ＩＤ及びパスワードにより該ユーザーの単一性を確認するステップ、
該ユーザーの単一性を確認した後、該アクセスコントロールサーバーが該ＩＤ及び該ユーザー権限を該ホームゲートウエイに伝送するステップ、
該ホームゲートウエイが権限認証コードを該アクセスコントロールサーバーに伝送するステップ、
該アクセスコントロールサーバーが該権限検証コードを秘蔵して授権ユーザーが該ホームゲートウエイにアクセスするのに用いるステップ、
以上のステップにより構築されることを特徴とする、階層式キーに基づくアクセスコントロール方法。
【請求項１６】
請求項９記載の階層式キーに基づくアクセスコントロール方法において、該ワンタイムの通信キーの生成は、
該チケットとトークンを通し、該アクセスコントロールサーバーがチケットトークンマッチングを該ホームゲートウエイに伝送するステップ、
該ホームゲートウエイが非可逆関数を通してセッションキーを生成するステップ、
該ユーザーも該チケットと選定した乱数を通して、該セッションキーを生成するステップ、
該ユーザーが該ホームゲートウエイの命令メッセージを伝送し、該セッションキーを暗号化したキーとなし、該ホームゲートウエイも該キーを利用して応答メッセージを暗号化して該ユーザーに伝送するステップ、
以上のステップを包含することを特徴とする、階層式キーに基づくアクセスコントロール方法。
【請求項１７】
ユーザーが遠方よりアクセスする際の認証授権に用いられる認証キー交換方法において、
ユーザーがその単一のＩＤ、及び秘蔵の乱数をアクセスコントロールサーバーに提供するステップ、
これにより、該アクセスコントロールサーバーが対応する権限認証値を探し出し、並びに該秘蔵の乱数及び別の乱数を通して、該ユーザーのチケットマッチング（ω，μ）とトークンを生成し、該チケートとトークンを対応するホームゲートウエイに伝送するステップ、
該ホームゲートウエイの確認成功を受けて、該アクセスコントロールサーバーが該チケットマッチングを該ユーザーに伝送するステップ、
該秘蔵の乱数、μ、該トークン及び非可逆演算を通して、該ユーザーが該アクセスコントロールサーバーの身分が正確であると確認した後、チケットωを受け取るステップ、
以上のステップを包含したことを特徴とする、認証キー交換方法。
【請求項１８】
請求項１７記載の認証キー交換方法において、該対応する権限認証値は該ユーザーの単一のＩＤにより、該アクセスコントロールサーバー中の認証テーブルを検索して探し出されることを特徴とする、認証キー交換方法。
【請求項１９】
請求項１７記載の認証キー交換方法において、該チケットマッチングのω値は該対応する権限認証値と該別の乱数を通して計算され、該対応する権限認証値は該ユーザーの単一

のＩＤとアクセス権限の非可逆演算を通して得られることを特徴とする、認証キー交換方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は一種の階層式キー（Ｈｉｅｒａｒｃｈｉｃａｌ　Ｋｅｙ）に基づくアクセスコントロール（Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）システムと方法、及びその認証キー交換の方法に関する。

【背景技術】

【０００２】

近年、無線センシングネットワークの発展は、軍事用途、環境監視等の大規模な配置から、徐々に家庭に導入されている。センシングネットワークを更に容易に家庭に融合させるため、ホームゲートウエイ（Ｈｏｍｅ　Ｇａｔｅｗａｙ）がセンシングネットワーク（Ｓｅｎｓｉｎｇ　Ｎｅｔｗｏｒｋ）情報の収集と対応値変化の制御を負担し、更に便利に、更に活発に利用されて家庭で不可欠なツールとなることが期待されている。ホームゲートウエイはホームメッセンジャー（Ｈｏｍｅ　Ｍｅｓｓｅｎｇｅｒ）としての役割を果たす。

【０００３】

多くの家庭では家中にセンシングネットワーク装置を配置し、ホームゲートウエイで情報を収集している。使用者が習慣的にホームゲートウエイを観て家庭のセンシング情報を得る時、一つのハイコントロールポイントに位置し、多くの家庭に既に配置されているセンシングネットワーク上に、アクセスコントロールサービスを如何に提供するかは、ユーザーが家にいなくとも家庭のセンシング状況を知ることができるようにする将来的に可能なサービスである。

【０００４】

ある家庭に関して、大量に配置されているセンサは、その属性分類上、権限レベルの違いが必然的に発生する。例えば、家中監視用モニタの安全レベルは一般の温度と湿度センサより高い。家庭管理員から各家族メンバーを見ると、メンバーがアクセスできるセンサ情報はそれぞれ同じでない。ゆえに簡単なアクセスコントロール権限区分方式が必要とされる。

【０００５】

アクセスコントロール構築は二つの基本要素を有し、すなわち、相互認証（Ｍｕｔｕａｌ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）、及びアクセス授権（Ａｃｃｅｓｓ　Ａｕｔｈｏｒｉｚａｔｉｏｎ）である。認証はすなわち身分の表面であり、どのような通信であり、その基礎は身分の表面にある。ただしサーバーがユーザーの身分を知ることはユーザーが自由に通行できることを意味するわけではなく、ユーザーはアクセス対象の認可を受けなければ、目標のアクセスを実行できない。

【０００６】

よく見られる安全なアクセスコントロール方法は、通信経路中の各セグメントを接続し、認証と授権メカニズムを構築することである。暗号学上、キーの構築により一つの実体を代表し、即ち、身分を代表する。図１は周知の一種のアクセスコントロール方法の実施例の表示図であり、ユーザーが遠方よりセンシングネットワーク中のあるノードのデータにアクセスする場合を説明する。

【０００７】

まず、ステップ１１０に示されるように、ユーザー１０１はユーザーＩＤとパスワードを使用してサービスプロバイダが提供するアクセスコントロールサーバー（Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ｓｅｒｖｅｒ：ＡＣＳ）１０３に対してホームゲートウエイ１０５とのアクセスを要求する。このとき、ＡＣＳ１０３は既に構築されているアクセスコントロールリスト（Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ｌｉｓｔ：ＡＣＬ）を検査する。その後、ステップ１２０に示されるように、ユーザー１０１のアクセスの合法性を検査し、合法で

あると確認すれば、ＡＣＳ１０３とホームゲートウエイ１０５がユーザー１０１の今回のセッションキー（Ｓｅｓｓｉｏｎ　Ｋｅｙ）に協商し、これはステップ１３０のとおりである。

【０００８】

セッションキー生成の目的は、２点あり、第１はＡＣＳ１０３がユーザー１０１のホームゲートウエイ１０５に対するアクセスの合法性を確認したことを表示すること、第２は毎回セッションキーは異なり、既存の登録秘密情報を通信ネットワークに不公開に保持するのに有効であり、毎回の通信に一定の安全品質を提供できることである。

【０００９】

セッションキーを協商した後、ステップ１４０のように、ユーザー１０１はこのセッションキーを用いてホームゲートウエイ１０５に対して、あるホームセンシングネットワーク１０７上のあるノード（Ｎｏｄｅ）ｉとのアクセスを要求する。このとき、ホームゲートウエイ１０５は先ず、ユーザー１０１がノードｉへのアクセス権限を有しているかを検査し、これはステップ１５０のとおりである。ステップ１５０の結果がイエスであれば（即ち、ユーザー１０１がノードｉへのアクセス権限を有していれば）、ホームゲートウエイ１０５がノードｉに諮問し、安全通信を実行し並びにノードｉより応答情報を得て、これはステップ１７０のとおりである。ホームゲートウエイ１０５は更に該セッションキーを使用して暗号化情報をユーザー１０１に送り、これはステップ１８０のとおりである。

【００１０】

こうして、ユーザーによる遠方からの安全なホームノードへのアクセスが達成される。このアクセスコントロール方法において、各ホームゲートウエイ上に、そのホームセンシングネットワーク上の全てのノードの安全通信キーが記録される。一人のユーザーに対しては、各ホームゲートウエイに対応するアクセスＩＤとパスワードを記録して、一致しないユーザーはアクセスできないようにする必要があり、記憶上、非常に不便である。大量のユーザーが権限の指定を必要とするとき、ホームゲートウエイは管理上、非常に大きな負担となり得る。並びにアクセスコントロールサーバーは効率的な協調セッションキー方式を実行することができなければ、全体サービスがアクセスコントロールサーバー中においてネックを形成し得る。

【００１１】

特許文献１にはＡＡＡメカニズムにおける遠方データアクセスコントロール方法及びシステムが記載されている。図２の実施例に示されるように、このアクセスコントロール方法の動作フロー中、モバイルユーザーは単純に現地ネットワークのＡＡＡサーバーに向けて認証請求（ステップ２１）し、両者はそれぞれに計算により同じセッションキーを生成（ステップ２２）する。ＡＡＡサーバーはセッションキーを、モバイルユーザーのＩＤと共に現地ネットワークのアプリケーションサーバーに送った後（ステップ２３）、更にこのアプリケーションサーバーがこのＩＤを受け取って対応するセッションキーで、モバイルユーザーとの間にチャネルを構築する（ステップ２５）。

【００１２】

特許文献２には単一サインオン（Ｓｉｎｇｌｅ　Ｓｉｇｎ－Ｏｎ）認証を具えたワンタイムパスワード（Ｏｎｅ－Ｔｉｍｅ　Ｐａｓｓｗｏｒｄｓ）の認証メカニズムが記載されている。図３の実施例構造に示されるように、この認証メカニズムは認証プロキシサーバー（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｘｙ　Ｓｅｒｖｅｒ）３２０、ユーザー装置３００を包含する。ユーザー装置３００はネットワークを通して認証プロキシサーバー３２０に接続される。ネットワークを通して、認証プロキシサーバー３２０は第三者認証サーバー（Ｔｈｉｒｄ　Ｐａｒｔｙ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｓｅｒｖｅｒ）３４０とコミュニケートできるほか、キー発送センター（Ｋｅｙ　Ｄｉｓｔｒｉｂｕｔｉｏｎ　Ｃｅｎｔｅｒ）３５０とコミュニケートできる。キー発送センター３５０は別の認証サーバー３５２とチケット授与サーバー（Ｔｉｃｋｅｔ　Ｇｒａｎｔｉｎｇ　Ｓｅｒｖｅｒ）３５４を有し、ユーザーのパスワードと要求を更新し、授与チケット（Ｇｒａｎｔｉｎｇ　Ｔｉｃｋｅｔ）とサービスチケット（Ｓｅｒｖｉｃｅ　Ｔｉｃｋｅｔ）を受け取る。

この認証メカニズムのチケット授与サーバーはサービスプロバイダの負担を重くし得る。
【００１３】
【特許文献１】台湾特許第Ｉ２５８９６４号
【特許文献２】国特許公開第２００７／０００６２９１号
【発明の開示】
【発明が解決しようとする課題】
【００１４】
本発明は、一種の階層式キーに基づくアクセスコントロールシステムと方法及びその認証キー交換方法を提供することを目的とする。
【課題を解決するための手段】
【００１５】
ある実施例において、本発明は一種の階層式キーに基づくアクセスコントロールシステムを提供する。このアクセスコントロールシステムは、アクセスコントロールサーバー、ホームゲートウエイ、及びホームゲートウエイに配置された複数のセンサノード（Ｓｅｎｓｏｒ　Ｎｏｄｅ）を包含する。このアクセスコントロールサーバーにはユーザーアクセスコントロール権限と授権認証コードが設定され、並びにユーザーパスワード関係データとアクセス権限の情報が保存される。このホームゲートウエイには階層式キー構造により構築されたアクセス権限と権限キーが記録される。ユーザーがこのアクセスコントロールサーバーにログインしてアクセス要求するとき、このユーザーとこのホームゲートウエイの双方はこのアクセスコントロールサーバーが発行したチケットとトークンを交換し、ワンタイムの通信キーを生成し、このユーザーにこの複数のセンサノードの情報に対するアクセスを許可する。
【００１６】
別の実施例において、本発明は一種の階層式キーに基づくアクセスコントロール方法を提供する。このアクセスコントロール方法は、ホームゲートウエイ中に一種の階層式キー構造を構築する。アクセスコントロールサーバー中にユーザーアクセスコントロール権限と認証コードを構築する。ユーザーがこのアクセスコントロールサーバーにログインしてアクセス要求する時、このアクセスコントロールサーバーはこのユーザーに対応する認証コードによりチケットとトークンを発行し、このユーザーとこのホームゲートウエイの双方がこのチケットとトークンの交換を通して、ワンタイム通信キーを生成し、このユーザーにホームネットワーク下の複数のセンサノードの情報へのアクセスを許可する。
【００１７】
また別の実施例において、本発明はユーザーの遠方からのアクセスの認証授権に用いる認証キーの交換方法を提供する。この認証キー交換方法は、ユーザーが唯一のＩＤ、及び隠された乱数ｍをアクセスコントロールサーバーに与え、これにより、アクセスコントロールサーバーが対応する権限認証値を探し出し、並びに乱数ｍと別の乱数ｙを通して、ユーザーのチケットマッチング（ω，μ）とトークンβを生成し、このトークンβを対応するホームゲートウエイに伝送し、このホームゲートウエイの確認成功を受けて、このアクセスコントロールサーバーはこのチケットマッチングをユーザーに伝送し、ｍ、μ、β及び非可逆演算を通し、ユーザーはこのアクセスコントロールサーバーの身分が正確であると確認した後、トークンωを受け取る。
【発明の効果】
【００１８】
総合すると、ここに記載の実施例は一種の階層式キーに基づくアクセスコントロールメカニズムとその認証キー交換方法を提供している。このアクセスコントロールメカニズムはホームゲートウエイが階層式キー構造を通してセンシングネットワーク下の多くのセンサノードに異なる安全レベルを採用させられ、並びに弾性的にホームセンシングネットワークキーを分類管理できるようにする。この階層式キー構造に基づき、アクセスコントロールサーバーは直接ホームキーを保存する必要がなくなり、ホームゲートウエイは簡単にアクセスコントロールサーバー上でユーザー権限を設定でき、有効にアクセスコントロー

ルサーバーの保存データの漏洩を有効に防止する。ユーザーにとっては、独特のＩＤパスワードを使用して一台のホームゲートウエイを通して遠方のセンサノードの情報にアクセスできる。同様に、ユーザーも一組のＩＤパスワードを使用して複数のホームゲートウエイを通行でき、こうしてアクセスコントロールサーバーのセッションキー協調時の演算量を軽減できる。

【００１９】

ここに記載の実施例中、全体のユーザーとアクセスコントロールサーバーの間は認証キー交換協定構造を基礎としてユーザーの遠方でのアクセスを実現し、システム施行上の負担を軽減できる。

【発明を実施するための最良の形態】

【００２０】

本発明の実施例中、一種の階層式キーに基づくアクセスコントロールメカニズム、及びその認証キー交換方法が提供される。このアクセスコントロールメカニズムの応用例、例えば、家庭情報管理者がホームゲートウエイを持ち帰った後、このアクセスコントロールメカニズムがアクセスコントロールサーバー、このホームゲートウエイ及びホームセンシングネットワーク設備を直列に接続し、この家庭情報管理者は簡単にこのアクセスコントロールサーバーを通して、ユーザーアクセスコントロール対策を講じることができ、並びにユーザーはこれにより簡単にアクセスコントロールサーバーの幇助を通し、許可されたセンサ情報にアクセスできる。

【００２１】

このホームゲートウエイを持ち帰った後、この家庭情報管理者はサービスプロバイダのアクセスコントロールサーバーに、このホームゲートウエイにこの管理者のＩＤとパスワード、及びこのホームゲートウエイの基本接続情報と安全通信キーを登録し、基礎安全信任起点を構築する。少なくとも、このホームゲートウエイを識別する識別情報、例えばホームゲートウエイのシリアルナンバーとＩＰアドレスを包含する情報を登録し、アクセスコントロールサーバーにこのホームゲートウエイの基本情報を了解させる。さらに必要に応じてアクセスコントロールサーバーとホームゲートウエイの管理者が安全通信を行う時に必要な情報、例えば家庭情報管理者のＩＤ、パスワード及びキーを包含するか否かを決定する。

【００２２】

図４は階層式キーに基づくアクセスコントロールシステムの一つの実施例構造図である。図４中、このアクセスコントロールシステムは、アクセスコントロールサーバー４０１、ホームゲートウエイ４０３、及びセンシングネットワーク４２０下に配置された複数のセンサノード１～ｎを包含する。図５はこのアクセスコントロールシステムの動作フローの凡例表示図であり、本発明のある実施例と一致する。

【００２３】

図１から図４のアクセスコントロールシステムの実施例構造及び図５の動作フローに示されるように、家庭情報管理者４３０がアクセスコントロールサーバー４０１に対してホームゲートウエイ４０３関係情報を登録した後、家庭情報管理者４３０はこのホームゲートウエイ４０３をアクセスコントロール基礎構築点となし、ホームゲートウエイ４０３中に階層式キー構造４０３ａを構築し、これはステップ５１０のとおりである。これにより、センシングネットワーク４２０がキー管理（Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ）と権限分類（Ｒｉｇｈｔ　Ｃｌａｓｓｉｆｉｃａｔｉｏｎ）を行うのに便利となる。

【００２４】

その後、構築した階層式キー構造４０３ａにより、家庭情報管理者４３０がアクセスコントロールサーバー４０１中にユーザーアクセスコントロール権限と授権認証コードを設定し、これはステップ５２０のとおりである。並びに、ユーザーパスワード関係情報及びアクセス権限の情報をアクセスコントロールサーバー４０１中に保存する。

【００２５】

ユーザー４０５がアクセスコントロールサーバー４０１にログオンしアクセス要求４０

５ａを行う時、アクセスコントロールサーバー４０１はユーザー４０５の対応する授権認証コードにより、チケットωとトークンβを生成し、これはステップ５３０のとおりである。

【００２６】

ユーザー４０５とホームゲートウエイ４０３の双方はこのチケットとトークンの交換により、ワンタイム通信キーを生成し、これはステップ５４０のとおりである。こうして、ユーザー４０５にセンサノード１～ｎの情報へのアクセスを許可する。

【００２７】

以上を受けて、ホームゲートウエイ４０３中にキー管理テーブル４０３ｂを具え、それに階層式キー構造４０３ａが構築したアクセス権限、該複数のセンサノードの識別コードとそれに対応するアクセス権限、及び最高権限のキーを記録する。アクセスコントロールサーバー４０１とホームゲートウエイ４０３は各自が認証テーブルを具備し、それぞれ認証テーブル４０１ａと認証テーブル４０３ｃとされ、そのうち、アクセスコントロールサーバー４０１中のて認証テーブル４０１ａは既に登録されたユーザーＩＤ（ＵＩＤ）、ユーザーパスワードと関係認証コード（Ｖｅｒｉｆｉｅｒ）、及びユーザー権限の関係認証値を記録する。ホームゲートウエイ４０３中の認証テーブル４０３ｃは一種の権限キーテーブルであり、既に登録されたユーザーＩＤ、及びユーザー権限の関係情報（例えば暗号化されたユーザー権限）を記録する。

【００２８】

図６は更に詳細にアクセスコントロールサーバー４０１とホームゲートウエイ４０３の内部装置及びそのアクセスコントロールサービスを説明する図であり、並びに本発明のある実施例と一致する。図６を参照されたい。ホームゲートウエイ４０３は階層式キーモジュール６０３、及びチケット検証及びメッセージ処理センター（Ｔｉｃｋｅｔ Ｖｅｒｉｆｉｃａｔｉｏｎ Ａｎｄ Ｍｅｓｓａｇｅ Ｐｒｏｃｅｓｓｉｎｇ Ｃｅｎｔｅｒ）６１３を包含する。階層式キーモジュール６０３は権限キー６０３ａ及びセンサ検証キー６０３ｂを構築し、権限キー６０３ａはアクセスコントロール設定に用いられ、センサ検証キー６０３ｂはホームゲートウエイ４０３とセンサノードの間の情報伝送暗号化に用いられる。チケット検証及びメッセージ処理センター６１３はユーザーのチケットによるログオンの検証を担う。

【００２９】

アクセスコントロールサーバー４０１は検証コード授権代理モジュール６０１、及びユーザー検証授権モジュール（Ｕｓｅｒ Ｖｅｒｉｆｉｃａｔｉｏｎ／Ａｕｔｈｏｒｉｚａｔｉｏｎ Ｍｏｄｕｌｅ）とチケットトークン交換センター（Ｔｉｃｋｅｔ／Ｔｏｋｅｎ Ｅｘｃｈａｎｇｅ Ｃｅｎｔｅｒ）６１１を包含する。検証コード授権代理モジュール６０１は家庭情報管理者がユーザーのアクセス権限を設定できるようにし、並びにこのアクセス権限の検証コードを保存し、ユーザー検証授権モジュールとチケットトークン交換センター６１１は協調し並びにユーザーとホームゲートウエイのセッションキーを生成し、合法的ユーザーがホームゲートウエイのアクセス授権を要求する時、チケットとトークンの対比を通して、ホームゲートウエイにこのユーザーの合法性を了解させる。

【００３０】

ゆえに、ここに記載の階層式キーに基づくアクセスコントロールメカニズムに関わる役割において、家庭情報管理者４３０は構造全体のアクセスコントロール方式を負担し、それは階層式キー構築、対内的にはセンシングネットワークのセンサノードキーを指定し、対外的にアクセスコントロール権限を設定する。ユーザー４０５は任意の遠端装置を通してセンシングネットワーク４２０上のセンサノードのデータにアクセスできる。アクセスコントロールサーバー４０１はログオンしたユーザーに対して身分認証を行う必要がある。このサーバー中にはユーザーパスワードと関係するデータ及びアクセス権限の情報が保存されている。このサーバーはセッションキーを生成してユーザーとホームゲートウエイ４０３の間の供給キーとなす。ホームゲートウエイ４０３はセンシングネットワーク４２０上のセンサノード１～ｎのデータを集めて、更にデータをスクリーン上に表示する。ホ

ームゲートウエイ４０３はセンシングネットワーク４２０上のノードに対して初期化及び認証の作業を行う必要がある。センサノードは周辺環境の各種変化因子、例えば温度、湿度、リアルタイム画像等を検出し、並びにデータをその他のセンシングネットワークうえのノードを通してホームゲートウエイ４０３に伝送する。

【００３１】

センシングネットワーク４２０上のセンサノードは周辺環境の各種変化因子に基づき数組のセンサノードに分類され、例えば三種類のセンサノードにわけられ、それぞれ周辺環境の温度、湿度、リアルタイム画像とされる。これにより、ユーザーは一組の三つのＩＤパスワードを保有し、それを身分認証に用いる。

【００３２】

以下に階層式キー構造の構築と図５の動作フローについて更なる説明を行う。図７は階層式キー構造構築のモデルであり、並びに本発明に記載の実施例と一致する。図７のモデル中、センシングネットワークには６個のセンサノードがあり、三種類のセンサノードに分類され、例えば、それぞれ周辺環境の映像監視用のセンサノードCAM_1とCAM_2、一酸化炭素と二酸化炭素のセンサノードCO_1とCO_2、及び温度検出のセンサノードTM_1とTEM_2である。各センサノードは唯一の識別コード（Ｎｏｄｅ　Ｉｄｅｎｔｉｆｉｅｒ）ＮＩＤを有し、この六個のセンサノードの識別コードはそれぞれ、NID_1からNID_6と記録される。この階層式キー構造には三種類のレベルがあり、それぞれレベル０、レベル１及びレベル２と記録される。各レベルはいずれも各自の権限キーを有し、この三種類のレベルの権限キーK_{LV}はそれぞれK_0、K_1、K_2と記録される。

【００３３】

センサノードCAM_1とCAM_2の所属するレベルはレベル０とされ、センサノードCO_1とCO_2の所属するレベルはレベル１、センサノードTM_1とTEM_2の所属するレベルはレベル２とされる。各センサノードはいずれも各自の検証キー（Ｖｅｒｉｆｉｃａｔｉｏｎ　Ｋｅｙ）ＮＫを有し、この６個のセンサノードの検証キーはそれぞれNK_1からNK_6とされる。

【００３４】

本発明の階層式キー構造の構築方式は比較的低いレベル（例えばレベル１）の権限キーが比較的高いレベル（例えばレベル０）の権限キーにより生成され、並びに各センサノードの検証キーは該センサノードの所属レベルの権限キーと該センサノードのＮＩＤにより生成される。図８は階層式キー構造構築の凡例フローであり、並びに本発明に記載の実施例と一致する。

【００３５】

図８の凡例フローを参照すると、まず、ステップ８１０に示されるように、最高レベルの権限キーが存在するか否かを検査する。最高レベルの権限キーが存在する時、ステップ８２０に示されるように、全てのセンサノードの検証キーが全て構築完成しているかを確認する。最高レベルの権限キーが不存在の時、ステップ８３０のように、この最高レベルの最高レベルの権限キーを生成し、その後、ステップ８２０に進む。

【００３６】

全てのセンサノードの検証キーが構築完成した時、ステップ８４０のように、キーの構築を終了する。ステップ８２０で最高レベルの権限キーが存在しなければ、ステップ８５０のように、次の検証キー未構築のセンサノードの識別コード及び所属レベル、システム記録（ＮＩＤ、所属レベル）を入力し、並びにこのセンサノードの検証キーを計算し、及び検証キーをこのセンサノードに割り当て、その後、ステップ８２０に進む。

【００３７】

図９は図７の凡例モデルであり、ホームゲートウエイ４０３中のキー管理テーブルの記録内容の一つの凡例であり、並びに本発明に記載の実施例に一致する。図９から分かるように、キー管理テーブルの内容はただこの階層式キー構造の最高レベルの権限キーの値１０１００１００１０１０、及び全てのノードの点ＮＩＤを記録する。この記録内容で各センサノードの検証キーＮＫを推算する。各センサノードの検証キーは家庭情報管理者４３

０がノード初期化時に算出し、並びにホームゲートウエイ４０３とセンサノードの間の情報伝送に用いる暗号化キーとする。権限キー或いは検証キー構築の関係は非可逆関数、例えばハッシュ関数（Ｈａｓｈ　Ｆｕｎｃｔｉｏｎ）の方式で計算される。

【００３８】

図９のキー管理テーブルの記録内容を例とし、以下にどのように各レベルの権限キーと各センサノードの検証キーを生成するかを説明する。図９中、レベル０（最高レベル）の権限キーK_0の内容は１０１００１００１０１０とされる。レベル０のモニタ画像検出のノードCAM_1とCAM_2は、その検証キーNK_1＝Ｈａｓｈ（NID_1，０）；NK_2＝Ｈａｓｈ（NID_1，０）である。レベル１の権限キーK_1＝Ｈａｓｈ（K_0）であり、その一酸化炭素或いは二酸化炭素検出のセンサノードCO_1とCO_2の検証キーNK_3＝Ｈａｓｈ（NID_3，１）；　NK_4＝Ｈａｓｈ（NID_4，１）である。レベル２の権限キーK_2＝Ｈａｓｈ（K_1）であり、その温度検出のノードTM_1とTEM_2の検証キーNK_5＝Ｈａｓｈ（NID_5，２）；NK_6＝Ｈａｓｈ（NID_6，２）である。ゆえにホームゲートウエイ４０３中のキー管理テーブルの内容はただ最高レベルの権限キーと各センサノードのＩＤを保存するだけでよい。センサノードの検証キー情報及び全てのレベルの権限キー情報をホームゲートウエイ中に保存する必要がないため、空間を節約し、安全度を高めることができる。

【００３９】

並びにユーザーにとっては、唯一独特のＩＤとパスワードを使用して一台のホームゲートウエイを通してセンシングネットワークに配置されたの複数のセンサノードの情報にアクセスできる。これから類推できるように、ユーザーは一組のＩＤパスワードを使用して複数のホームゲートウエイを通ることができ、アクセスコントロールサーバー４０１のセッションキー協調時の演算量を軽減することができる。

【００４０】

家庭階層式キーの設定を終え、並びにセンサノード配置を終えた後、続いて、これを基礎として、アクセスコントロールサーバーに対してユーザーＩＤパスワード及びアクセス権限をどのように構築するか、について以下に説明する。図１０は一つの凡例フローチャートであり、如何にユーザーのアクセス権限を構築するかを説明し、並びに本発明のある実施例に一致する。

【００４１】

図１０に示されるように、まず、ユーザーの唯一のＩＤ（すなわちＵＩＤ）、パスワード及びユーザー権限をアクセスコントロールサーバー４０１に提供し、これはステップ１０１０に示されるとおりである。アクセスコントロールサーバー４０１はこのＵＩＤとパスワードによりユーザーの単一性を確認し、これはステップ１０２０のとおりである。ユーザーの単一性を確認した後、アクセスコントロールサーバー４０１はＵＩＤ及びユーザー権限をホームゲートウエイ４０３に伝送し、これはステップ１０３０のとおりである。これにより、ホームゲートウエイ４０３は権限検証コードをアクセスコントロールサーバー４０１に伝送し、これはステップ１０４０のとおりである。アクセスコントロールサーバーはこの権限検証コードを保存し、授権ユーザーをホームゲートウエイ４０３にアクセスさせるのに用い、これはステップ１０５０のとおりである。

【００４２】

ステップ１０４０において、ホームゲートウエイ４０３は非可逆関数を利用してこの権限検証コードを計算し、並びにこのＵＩＤとこの権限検証コードのマッチングを認証テーブル４０３ｃに保存する。ステップ１０５０において、アクセスコントロールサーバーは一種の非可逆関数を利用してこの権限検証コードを暗号化し、並びにこの暗号化した認証コードを認証テーブル４０３ｃ中に記録する。

【００４３】

図１１は一つの凡例であり、ユーザーのアクセス権限をどのように構築するかを説明し、並びに本発明のある実施例と一致する。図１１に示されるように、ユーザー４０５は登録時に取得した家庭情報管理者４３０のＩＤとパスワードを通してアクセスコントロール

サーバー４０１にログオンし、アクセスコントロールサーバー４０１にこのホームゲートウエイ４０３がユーザー登録を必要としていることを知らせる。その後、家庭情報管理者はユーザーＡの唯一のＩＤであるＵＩＤ$_A$、パスワードＰＷ$_A$、及び構築したいユーザー権限Ｈをアクセスコントロールサーバー４０１に入力する。アクセスコントロールサーバー４０１は入力情報を受け取った後、このＵＩＤとパスワードによりユーザーの単一性を確認する。もしユーザー４０５が既に存在していれば、アクセスコントロールサーバー４０１は現在ユーザー登録を行っているホームゲートウエイ４０３をユーザー４０５のＩＤ下に増加する。

【００４４】

ユーザーの単一性を確認した後、アクセスコントロールサーバー４０１はこのＵＩＤ及びこのユーザー権限をホームゲートウエイ４０３に伝送する。ホームゲートウエイ４０３はこれによりその内部の認証テーブル４０３ｃを更新し、並びにこのユーザー権限に対応する権限キー関係の認証値をアクセスコントロールサーバー４０１に伝送する。この認証値はこのＵＩＤ$_A$及びこのユーザー権限に対応する権限キーＫ$_H$を通して単方向演算され、例えばハッシュ関数Ｈ$_1$により得られる。アクセスコントロールサーバー４０１はこの認証値を得た後、関係情報を認証テーブル４０３ｃに保存し、この関係情報は例えば、ユーザーＩＤ、秘蔵のパスワード、ホームゲートウエイのシリアルナンバー、及びこの認証値に対応する秘蔵の認証コードを包含する。この関係情報はアクセスコントロールサーバー４０１がユーザーがホームゲートウエイに対してデータアクセスを行う時、ユーザー権限に対する認証を行うのに使用される。

【００４５】

ユーザー権限構築の後、ユーザーに関しては、ただその唯一のＩＤとパスワードを記憶しておけば、遠方からのアクセス時の認証に用いることができる。アクセスコントロールサーバー４０１はただユーザーのＩＤパスワードと検証コードをマッチングさせて保存しておくだけでよく、強制的にアクセスコントロールテーブルを構築する必要はない。

【００４６】

上述のユーザー権限構築完成後、ユーザーが遠方よりアクセスコントロールサーバー４０１にログオンしてアクセス要求する時、前述したように、アクセスコントロールサーバー４０１はこのユーザーに対応する検証コードにより、アクセス授権チケットを発行し、並びにトークンでホームゲートウエイ４０３にユーザーのアクセス要求を通知し、ユーザーとホームゲートウエイ４０３双方にこのチケットとトークンによりこの度のセッションキーを計算させて、ワンタイムの通信データ認証暗号化に用いる。言い換えると、ユーザーが遠方よりアクセスコントロールサーバー４０１にログオンしてアクセス要求する時、このユーザーの遠方からのアクセスはツーステップに分けられ、第１ステップではユーザーがアクセスコントロールサーバー４０１に向けて認証授権を要求し、第２ステップではユーザーとホームゲートウエイ４０３が通信キーを生成する。以下にこのツーステップについて説明を行う。

【００４７】

第１ステップにおいては、全体のユーザーとアクセスコントロールサーバーの間は認証キー交換協定構造を基礎としてこのユーザーの認証授権が実現される。図１２はユーザーがアクセスコントロールサーバーに向けて認証授権を要求する時の、この認証キー交換方法の一つの凡例フローチャートであり、本発明に記載の実施例と一致する。

【００４８】

図１２に示されるように、まず、このユーザーがその唯一のＩＤ（すなわちＵＩＤ）、及び秘蔵の乱数ｍをアクセスコントロールサーバー４０１に提供し、ステップ１２１０のとおりである。これにより、アクセスコントロールサーバー４０１は対応する権限認証値を探し出し、並びにｍともう一つの乱数ｙを通し、ユーザーのチケットマッチング（ω，μ）とトークンβを計算し、トークンβをホームゲートウエイ４０３に伝送し、これはステップ１２２０のとおりである。ホームゲートウエイ４０３の確認成功を受け、アクセスコントロールサーバー４０１はチケットマッチング（ω，μ）をこのユーザーに伝送し、

これはステップ１２３０のとおりである。ｍ、μ、β及び非可逆演算を通して、ユーザーはアクセスコントロールサーバー４０１の身分が正確であることを確認した後、チケットωを受け取り、これはステップ１２４０のとおりである。

【００４９】

図１３は上述のフローに基づき、ユーザーとアクセスコントロールサーバーの間でどのように数学モデルの構築を通して認証授権を達成するかを説明し、並びに本発明の実施例と一致する。図１３に示されるように、ユーザーＡがUID_A、パスワードPW_Aでアクセスコントロールサーバー４０１にログオンした後、符号１３１０のように、前述のステップ１２１０の秘蔵の乱数ｍは以下のモデルにより構築される。すなわち、一つのZ_q^*のサブグループＧ中よりランダムに一つのｘ値を取り、ｍをg^xとなし、そのうち、Z_q^*はモデルｐ下で、全てがｐと互いに素であり集合を形成し、ｇは一つのＧ中の生成元である。

【００５０】

前述のステップ１２２０の権限認証値はアクセスコントロールサーバー４０１中の認証テーブル４０３ａを通して探し出せる。認証テーブル４０１ａより探し出した対応する認証値はサブグループＧ中よりランダムに取り出した別の乱数ｙと数学モデルを構築し、チケットマッチングのω値とμ値を計算でき、アクセスコントロールサーバー４０１も数学モデル$\beta = m^y$を通してトークンβを得ることができ、これらの数学モデルの凡例は符号１３２０のように示される。

【００５１】

アクセスコントロールサーバー４０１がチケットマッチング（ω，μ）をユーザーに送った後、ユーザーＡはｘ値及びパスワードを利用してｓ値を計算し並びに$\alpha = \mu^s$となす。続いて、$v_1 = H_2$（ｍ，α）をアクセスコントロールサーバー４０１に伝送し、これは符号１３４０ａのとおりである。アクセスコントロールサーバー４０１はv_1が$v'_1 = H_2$（ｍ，β）と同じであるか対比し、これは符号１３４０ｂのとおりである。もし$v_1 = v'_1$であれば、すなわち、アクセスコントロールサーバー４０１がユーザーＡの身分を認証したことを示す。アクセスコントロールサーバー４０１は続いて$v_2 = H_2$（μ，β）を計算し並びにこの値をユーザーＡに伝送し、これは符号１３４１ａのとおりである。ユーザーＡは$v'_2 = H_2$（μ，α）を計算し並びに$v_2 = v'_2$であるか否か対比し、これは符号１３４１ｂのとおりである。もし、$v_2 = v'_2$であれば、すなわち、アクセスコントロールサーバー４０１がユーザーＡの身分を認証したことを示す。これにより、ユーザーＡとアクセスコントロールサーバー４０１の双方向認証を完成し、同時にユーザーＡはアクセスコントロールサーバー４０１にチケットωを提供する。

【００５２】

言い換えると、ユーザーとアクセスコントロールサーバーの間は認証キー交換（Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ）協定構造を基礎として、このユーザーの遠方アクセスを実現する。

【００５３】

ユーザーＡとアクセスコントロールサーバー４０１の双方向認証を完成し、ユーザーＡはアクセスコントロールサーバー４０１にチケットωを提供した後、ユーザー遠方アクセスは第２ステップに進入し、すなわちユーザーとホームゲートウエイ４０３が通信キーを生成するステップである。図１４はユーザーとホームゲートウエイ４０３が通信キーを生成する凡例のフローの表示図であり、並びに本発明の実施例と一致する。

【００５４】

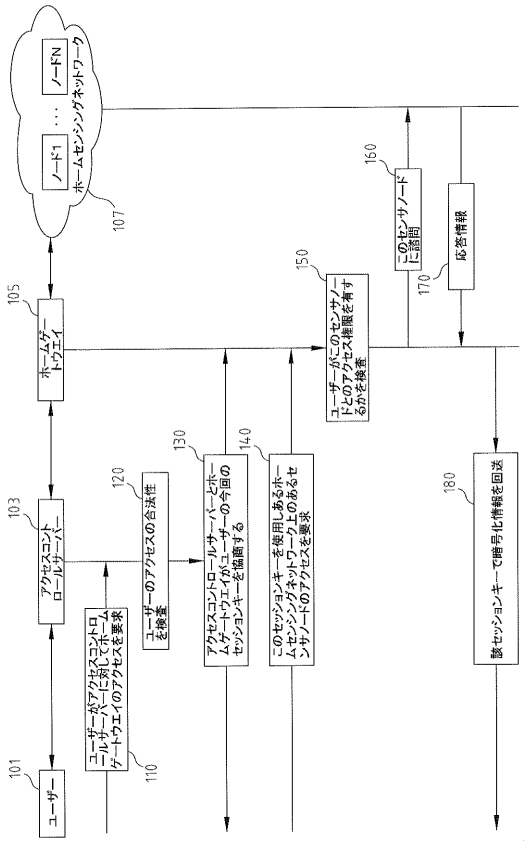
図１４に示されるように、まず、アクセスコントロールサーバー４０１がトークンマッチング（UID_A，β）をホームゲートウエイ４０３に伝送し、これは符号１４１０のとおりである。ホームゲートウエイ４０３はセッションキーＳＫ＝$\beta^{H1(UIDA,KH)}$を計算し、これは符号１４２０ａのとおりである。ユーザーＡは、アクセスコントロールサーバー４０１を通して与えられたチケットωと選定した乱数ｘを通してセッションキーＳＫ＝ω^xを計算し、これは符号１４２０ｂのとおりである。この計算により、ユーザーＡとホー

ムゲートウエイ４０３の間に構築されるセッションキーＳＫは同じである。
【００５５】
その後、符号１４３０ａのように、ユーザーＡがホームゲートウエイ４０３に伝送した命令情報はこのセッションキーＳＫを暗号化キーとし、E_{sk}（ｃｏｍｍａｎｄ）でこの暗号化された命令情報を表示する。同様に符号１４３０ｂに示されるように、ホームゲートウエイ４０３もこのキーを利用して応答情報を暗号化してユーザーに伝送し、E_{sk}（ａｎｓｗｅｒ）でこの暗号化された応答情報を表示する。こうしてユーザーとホームゲートウエイの間の安全チャネルが構築される。
【００５６】
特筆すべきことは、ここに記載のアクセスコントロールサーバーが生成するトークンとチケットは暗号化せずに伝送することも可能である、ということである。すなわち、攻撃者がこのチケットωを有していても、正確なセッションキーを計算できず、これにより、ここに記載の実施例もシステム施行上の負担を軽減できる。
【図面の簡単な説明】
【００５７】
【図１】周知のアクセスコントロール方法の実施例図である。
【図２】周知の遠方でのデータカクセスコントロール方法の実施例図である。
【図３】周知の単一サインオン（Ｓｉｎｇｌｅ　Ｓｉｇｎ－Ｏｎ）認証を具えたワンタイムパスワード（Ｏｎｅ－Ｔｉｍｅ　Ｐａｓｓｗｏｒｄｓ）の認証メカニズムの実施例図である。
【図４】本発明の階層式キーを基礎とするアクセスコントロールシステムの実施例構造図である。
【図５】本発明のアクセスコントロールシステムの動作フローの実施例図である。
【図６】本発明のアクセスコントロールサーバーとホームゲートウエイの内部装置とそのアクセスコントロールサービスの実施例図である。
【図７】本発明の階層式キー構造により構築されるモデル実施例図である。
【図８】本発明の階層式キー構造により構築されるフロー実施例図である。
【図９】図７のモデル実施例による、ホームゲートウエイ中のキー管理テーブルの記録内容の実施例図である。
【図１０】本発明のユーザーのアクセス権限構築の実施例図である。
【図１１】本発明のユーザーの権限構築の実施例図である。
【図１２】本発明のユーザーがアクセスコントロールサーバーに対して認証授権を要求する時の、認証キー交換方法のフロー実施例図である。
【図１３】図１２のフローに基づき、ユーザーとアクセスコントロールサーバーの間の数学モデルの構築を通しての認証授権の実施表示図である。
【図１４】本発明のユーザーとホームゲートウエイの通信キー構築のフロー実施例図である。
【符号の説明】
【００５８】
１０１　ユーザー　　１０３　アクセスコントロールサーバー
１０５　ホームゲートウエイ　　１０７　ホームセンシングネットワーク
１１０　ユーザーがアクセスコントロールサーバーに対してホームゲートウエイのアクセスを要求
１２０　ユーザーのアクセスの合法性を検査
１３０　アクセスコントロールサーバーとホームゲートウエイがユーザーの今回のセッションキーを協商する
１４０　このセッションキーを使用しあるホームセンシングネットワーク上のあるセンサノードのアクセスを要求
１５０　ユーザーがこのセンサノードとのアクセス権限を有するかを検査
１６０　このセンサノードに諮問　　１７０　応答情報

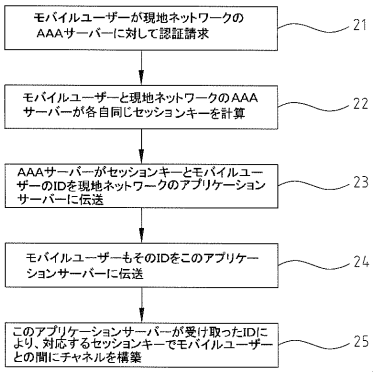
１８０　該セッションキーで暗号化情報を回送
２１　モバイルユーザーが現地ネットワークのＡＡＡサーバーに対して認証請求
２２　モバイルユーザーと現地ネットワークのＡＡＡサーバーが各自同じセッションキーを計算
２３　ＡＡＡサーバーがセッションキーとモバイルユーザーのＩＤを現地ネットワークのアプリケーションサーバーに伝送
２４　モバイルユーザーもそのＩＤをこのアプリケーションサーバーに伝送
２５　このアプリケーションサーバーが受け取ったＩＤにより、対応するセッションキーでモバイルユーザーとの間にチャネルを構築
３００　ユーザー装置　　３２０　認証サーバー
３３０　ネットワーク　　３４０　第３者認証サーバー
３５０　キー発送センター　　３５２　もう一つの認証サーバー
３５４　チケット授与サーバー
４０１　アクセスコントロールサーバー　　４０３　ホームゲートウエイ
４０３ａ　階層式キー構造　　４０５　ユーザー
４２０　センシングネットワーク　　４３０　家庭情報管理者
４０１ａ、４０３ｃ　認証テーブル　　４０３ｂ　キー管理テーブル
４０５ａ　アクセス要求　　ω　チケット
β　トークン
５１０　ホームゲートウエイ中に階層式キー構造構築
５２０　アクセスコントロールサーバー中にユーザーアクセスコントロール権限と授権検証コードを設定
５３０　ユーザーがアクセスコントロールサーバーにログオンして授権要求する時、アクセスコントロールサーバーがユーザーに対応する授権検証コードによりチケットとトークンを発行する
５４０　ユーザーとホームゲートウエイの双方がこのチケットとトークンの交換によりワンタイムの通信キーを生成
６０１　検証コード授権代理モジュール　　６０３　階層式キーモジュール
６０３ａ　権限キー　　６０３ｂ　センサ検証キー
６１３　チケット検証及びメッセージ処理センター
６１１　ユーザー検証授権モジュールとチケットトークン交換センター
NID_1 から NID_6 センサノードの識別コード
K_0、K_1、K_2　レベルの権限キー
CAM_1、CAM_2 周辺環境検出の映像モニタのセンサノード
CO_1、CO_2 一酸化炭素或いは二酸化炭素検出のセンサノード
TEM_1、TEM_2 温度検出のセンサノード
NK_1、NK_2 センサノードの検証キー
８１０　最高レベルの権限キーが存在するかを検査
８２０　全てのセンサノードの検証キーが既に構築完成したかを確認
８３０　この最高レベルの権限キーを生成
８４０　キーの構築終了
８５０　次の検証キー未構築のセンサノードの識別コード及びその所属レベル、システム記録（ＮＩＤ、所属レベル）を入力し、並びにこのセンサノードの検証キーを計算し、検証キーをこのセンサノードに割り当てる
１０１０　ユーザーに与えられた唯一のＩＤ、パスワード及びユーザー権限をアクセスコントロールサーバーに提供する
１０２０　アクセスコントロールサーバーがこのＩＤとパスワードによりユーザーの単一性を確認する
１０３０　ユーザー単一性確認の後、アクセスコントロールサーバーがこのＩＤ及びこのユーザー権限をホームゲートウエイに伝送する

１０４０　これにより、ホームゲートウエイが権限検証コードをアクセスコントロールサーバーに伝送する
１０５０　アクセスコントロールサーバーがこの権限検証コードを秘蔵し、授権使用者のホームゲートウエイへのアクセスに用いる
１２１０　ユーザーがその唯一のＩＤ、及び秘蔵の乱数ｍをアクセスコントロールサーバーに提供する
１２２０　これによりアクセスコントロールサーバーが対応する権限認証値を探し出し、並びにｍともう一つの乱数ｙを通し、ユーザーのチケットマッチング（ω，μ）とトークンβを計算し、トークンβをホームゲートウエイに伝送する
１２３０　ホームゲートウエイの確認成功を受けて、アクセスコントロールサーバーがチケットマッチング（ω，μ）をこのユーザーに伝送する
１２４０　ｍ、μ、β及び非可逆演算を通し、ユーザーがアクセスコントロールサーバーの身分が正確であることを確認した後、チケットωを受け取る
１３１０　ＩＤ、パスワードでログオン
１３２０　数学モデル
１３４０ａ　$v_1 = H_2$（ｍ，α）を伝送
１３４０ｂ　v_1 が $v'_1 = H_2$（ｍ，β）と同じであるか対比
１３４１ａ　$v_2 = H_2$（μ，β）を伝送
１３４１ｂ　$v'_2 = H_2$（μ，α）を計算し並びに $v_2 = v'_2$ であるか否か対比
１４１０　トークンマッチング（ＵＩＤ，β）を伝送
１４２０ａ　セッションキーＳＫ＝$\beta^{H1(UIDA,KH)}$ を計算
１４２０ｂ　セッションキーＳＫ＝w^x を計算
E_{sk}（ｃｏｍｍａｎｄ）　暗号化された命令情報
E_{sk}（ａｎｓｗｅｒ）　暗号化された応答情報
１４３０ａ　ユーザーが暗号化された命令情報を伝送
１４３０ｂ　ホームゲートウエイが暗号化された応答情報を伝送

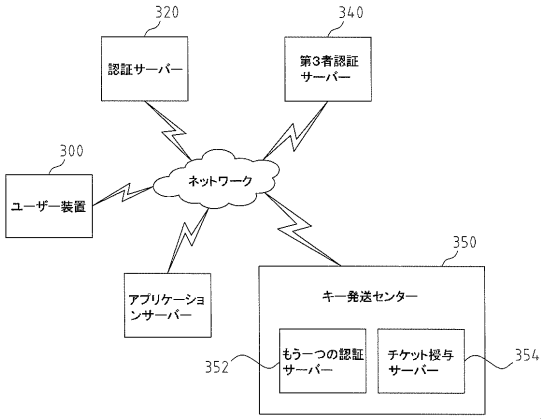
【図１】


ノードN
ノード1
ホームセンシングネットワーク
107
160
このセンサノードに照会
170
応答情報
150
ユーザーがこのセンサノードとのアクセス権限を有するかを検査
105
ホームゲートウエイ
130
140
120
180
103
アクセスコントロールサーバー
アクセスコントロールサーバーとホームゲートウエイがユーザーの今回のセッションキーを協商する
このセッションキーを使用しあるホームセンシングネットワーク上のあるセンサノードのアクセスを要求
ユーザーのアクセスの合法性を検査
暗号化情報を回送
ユーザーがアクセスコントロールサーバーに対しホームゲートウエイのアクセスを要求
110
101
ユーザー

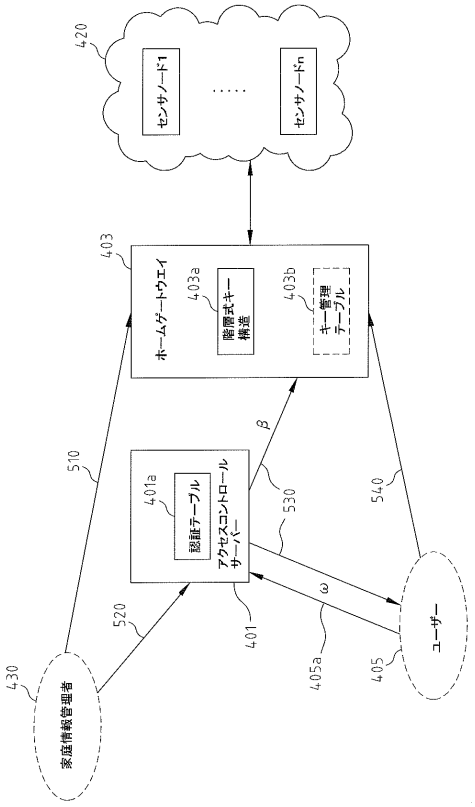
【図２】


モバイルユーザーが現地ネットワークのAAAサーバーに対して認証請求
21
モバイルユーザーと現地ネットワークのAAAサーバーが各自同じセッションキーを計算
22
AAAサーバーがセッションキーとモバイルユーザーのIDを現地ネットワークのアプリケーションサーバーに伝送
23
モバイルユーザーもそのIDをこのアプリケーションサーバーに伝送
24
このアプリケーションサーバーが受け取ったIDにより、対応するセッションキーでモバイルユーザーとの間にチャネルを構築
25

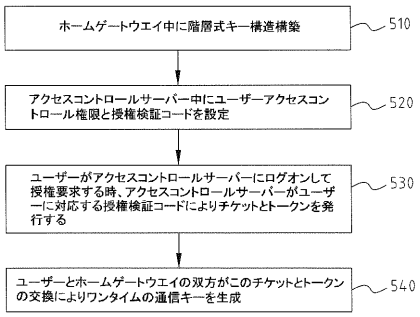
【図３】


320
認証サーバー
340
第3者認証サーバー
300
ネットワーク
ユーザー装置
350
アプリケーションサーバー
キー発送センター
352
もう一つの認証サーバー
チケット授与サーバー
354

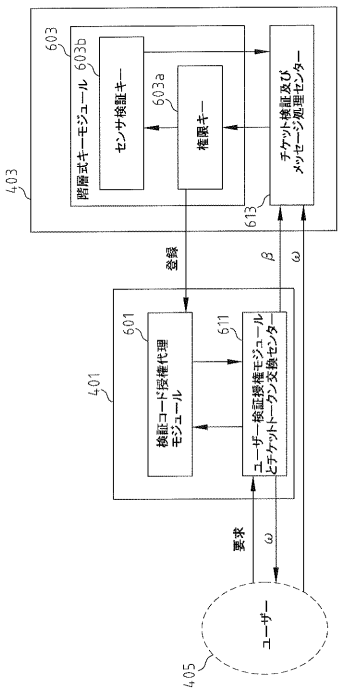
【図４】


420
センサノード1
センサノードn
403
ホームゲートウエイ
403a
階層式キー構造
403b
キー管理テーブル
β
510
401a
認証テーブル
アクセスコントロールサーバー
530
540
ω
520
401
405a
405
ユーザー
430
家庭情報管理者

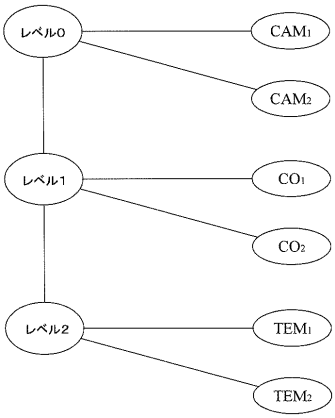
【図５】


ホームゲートウエイ中に階層式キー構造構築
510
アクセスコントロールサーバー中にユーザーアクセスコントロール権限と授権検証コードを設定
520
ユーザーがアクセスコントロールサーバーにログオンして授権要求する時、アクセスコントロールサーバーがユーザーに対応する授権検証コードによりチケットとトークンを発行する
530
ユーザーとホームゲートウエイの双方がこのチケットとトークンの交換によりワンタイムの通信キーを生成
540

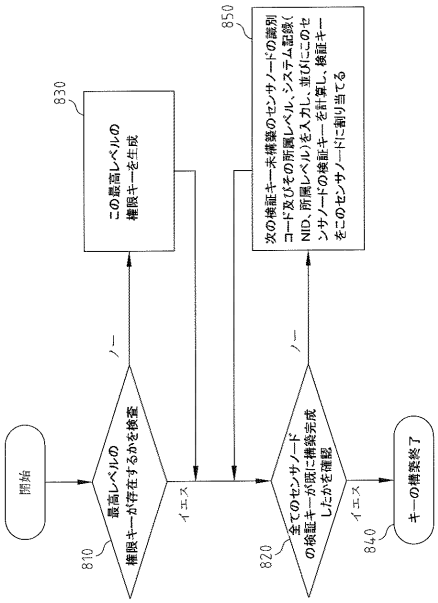
【図６】



【図７】



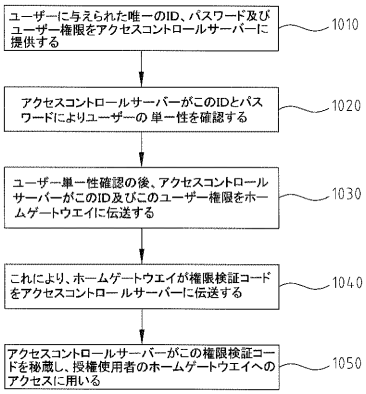
【図８】



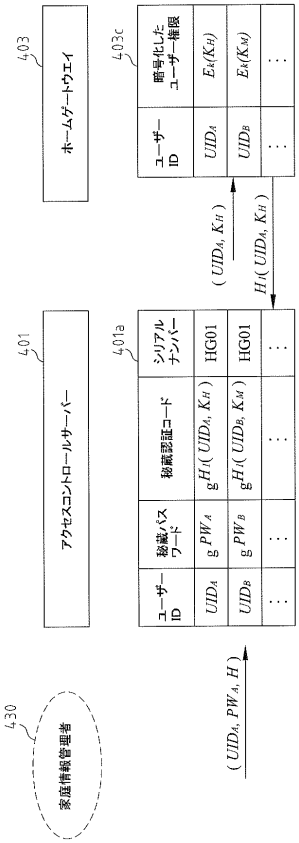
【図９】

K_0	101001001010
CAM_1	(NID_1, 0)
CAM_2	(NID_2, 0)
CO_1	(NID_3, 1)
CO_2	(NID_4, 1)
TEM_1	(NID_5, 2)
TEM_2	(NID_5, 2)

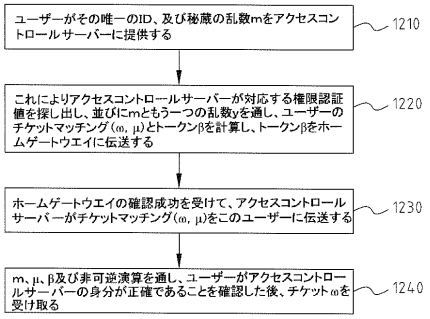
【図１０】



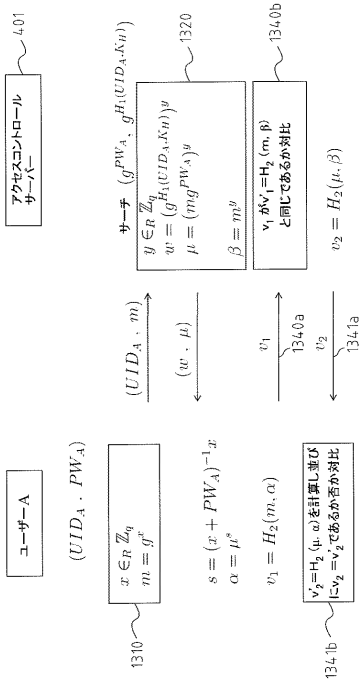
【図１１】



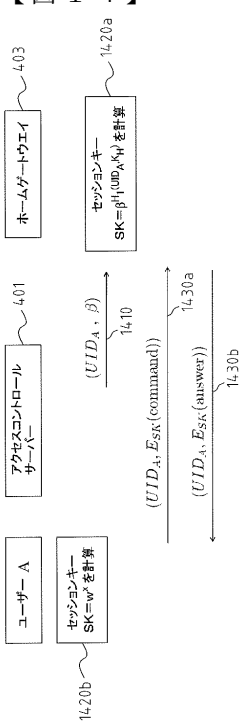
【図１２】



【図１３】



【図１４】


ホームゲートウエイ
403
セッションキー
SK=β^H1(UID_A,Ky)を計算
1420a
アクセスコントロール
サーバー
401
ユーザー A
セッションキー
SK=w^r を計算
1420b
(UID_A , β)
1410
(UID_A, E_SK(command))
1430a
(UID_A, E_SK(answer))
1430b

フロントページの続き

(74)代理人 100102495
弁理士 魚住 高博
(74)代理人 100112302
弁理士 手島 直彦
(74)代理人 100152124
弁理士 白石 光男
(72)発明者 黄 義雄
台湾台南縣麻豆鎮南勢里１２鄰１５之３號
(72)発明者 郭 倫嘉
台湾台中市西屯區惠來里３９鄰政和路５０巷９號
(72)発明者 曾 文貴
台湾新竹市東區高峰里１９鄰高翠路１７３巷５弄４１號
(72)発明者 林 煥宗
台湾台中縣沙鹿鎮中棲路東明巷５８－５號
(72)発明者 蔡 家宏
台湾台北市辛亥路六段２１巷２０號４樓

Ｆターム(参考) 5B285 AA01 BA01 CA02 CA06 CA41 CB02 CB47 CB62 CB72 CB76
CB84
5J104 AA07 AA16 EA01 EA03 EA04 EA15 EA16 EA17 EA18 JA03
KA01 KA04 KA21 MA01 MA05 NA02 NA05 NA27 NA37 NA38
PA07