

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4207465号
(P4207465)

(45) 発行日 平成21年1月14日(2009.1.14)

(24) 登録日 平成20年10月31日(2008.10.31)

(51) Int.Cl.		F I			
H O 4 L	9/08	(2006.01)	H O 4 L	9/00	6 O 1 E
H O 4 L	9/32	(2006.01)	H O 4 L	9/00	6 7 5 B
			H O 4 L	9/00	6 7 5 D

請求項の数 11 (全 119 頁)

(21) 出願番号	特願2002-167480 (P2002-167480)	(73) 特許権者	000002185
(22) 出願日	平成14年6月7日(2002.6.7)		ソニー株式会社
(65) 公開番号	特開2004-15527 (P2004-15527A)		東京都港区港南1丁目7番1号
(43) 公開日	平成16年1月15日(2004.1.15)	(74) 代理人	100093241
審査請求日	平成17年6月6日(2005.6.6)		弁理士 宮田 正昭
		(74) 代理人	100101801
			弁理士 山田 英治
		(74) 代理人	100086531
			弁理士 澤田 俊夫
		(72) 発明者	川口 貴義
			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	島田 昇
			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】 データ処理権限管理システム、情報処理装置、および方法、並びにコンピュータ・プログラム

(57) 【特許請求の範囲】

【請求項1】

サービスプロバイダの提供するサービスを実行するユーザデバイスにおけるデータ処理権限を管理するデータ処理権限管理システムであり、

サービスプロバイダ機器は、

暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス (A d) 情報とを格納データとして有し、署名をユーザデバイスのセキュリティチップの秘密鍵、または実行属性証明書中の格納鍵で行うことを許容した実行属性証明書をサービス受領デバイスであるユーザデバイスに対して提供し、

ユーザデバイスは、

前記実行属性証明書に格納されたアドレス (A d) 情報に従って、該ユーザデバイスのメモリから取得した登録鍵を適用して、該実行属性証明書に格納された暗号化実行命令の復号を行ない、復号結果に基づくデータ処理を実行する構成としたことを特徴とするデータ処理権限管理システム。

【請求項2】

データ処理を実行する情報処理装置であり、

暗号化データの復号処理に適用する登録鍵を格納するメモリ部と、

暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵の情報処理装置内のメモリにおける格納領域を示すアドレス

(A d) 情報とを格納データとして有し、発行者署名のなされた実行属性証明書であり、署名をユーザデバイスのセキュリティチップの秘密鍵、または実行属性証明書中の格納鍵で行うことを許容した実行属性証明書を入力し、署名検証処理を実行するとともに、署名検証の成立を条件として、前記アドレス (A d) 情報に従って、前記メモリ部から取得した登録鍵を適用して前記暗号化実行命令を復号する暗号処理部と、

前記暗号処理部において復号された実行命令を実行するデータ処理部と、
を有することを特徴とする情報処理装置。

【請求項 3】

前記データ処理部は、

前記登録鍵格納領域を指定したアドレス (A d) に対応するメモリ領域に、前記登録鍵と異なるデータ構成を持つリセット鍵データを書き込むことにより登録鍵の破棄処理を実行する構成であることを特徴とする請求項 2 に記載の情報処理装置。

10

【請求項 4】

前記実行属性証明書に格納された暗号化実行命令には、

実行命令の適用可能回数識別値が格納され、

前記データ処理部は、

実行命令の実行に応じて前記適用可能回数識別値を更新して、情報処理装置内のセキュリティチップの秘密鍵による署名を実行して更新された適用可能回数識別値を含む新たな実行属性証明書の生成を行なう構成であることを特徴とする請求項 2 に記載の情報処理装置。

20

【請求項 5】

前記実行属性証明書に格納された暗号化実行命令には、

実行命令の適用可能回数識別値が格納され、

前記データ処理部は、

実行命令の実行に応じて前記適用可能回数識別値を更新して、更新された適用可能回数識別値が 0 となった場合に、前記登録鍵格納領域を指定したアドレス (A d) に対応するメモリ領域に、前記登録鍵と異なるデータ構成を持つリセット鍵データを書き込むことにより登録鍵の破棄処理を実行する構成であ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 6】

前記実行属性証明書に格納された暗号化実行命令は、

前記情報処理装置のセキュリティチップの秘密鍵での署名が許容され、さらに他デバイスへの譲渡処理の許容された譲渡用実行属性証明書の生成処理命令を含み、

前記データ処理部は、

前記譲渡用実行属性証明書の生成処理命令に従い、

情報処理装置内のセキュリティチップの秘密鍵による署名を付与した新たな譲渡用実行属性証明書の生成処理を実行し、生成した譲渡用実行属性証明書の他デバイスへの提供処理を実行する構成であることを特徴とする請求項 2 に記載の情報処理装置。

30

【請求項 7】

前記実行属性証明書に格納された暗号化実行命令には、

他デバイスの属性を証明する証明書として、該他デバイスに対して発行する属性証明書であり、前記暗号化実行命令に含まれる署名生成用鍵によって署名のなされる審査代行属性証明書の発行処理命令、および該審査代行属性証明書の生成に必要とする署名生成用鍵を含み、

40

前記データ処理部は、

前記審査代行属性証明書の発行処理命令に従い、

前記他デバイスの属性確認の審査を属性証明書の真の発行者に代わって実行し、属性が確認された場合に、前記署名生成用鍵を適用して署名を実行した審査代行属性証明書の生成処理を実行して前記他デバイスに提供する構成であることを特徴とする請求項 2 に記載の情報処理装置。

50

【請求項 8】

前記実行属性証明書に格納された暗号化実行命令には、

自デバイスの属性を証明する証明書として、前記暗号化実行命令に含まれる署名生成用鍵によって署名のなされる代理署名属性証明書の発行処理命令、および該代理署名属性証明書の生成に必要とする署名生成用鍵を含み、

前記データ処理部は、

前記代理署名属性証明書の発行処理命令に従い、

該代理署名属性証明書の検証を実行する検証デバイスから受領した検証用乱数 (R a) を格納データとして含み、属性証明書の真の発行者の鍵の代わりに前記署名生成用鍵を適用した署名を有する代理署名属性証明書の生成処理を実行する構成であることを特徴とする請求項 2 に記載の情報処理装置。

10

【請求項 9】

サービスプロバイダの提供するサービスを実行するユーザデバイスにおけるデータ処理権限を管理するデータ処理権限管理方法であり、

サービスプロバイダ機器における実行ステップとして、

暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス (A d) 情報とを格納データとして有し、署名をユーザデバイスのセキュリティチップの秘密鍵、または実行属性証明書中の格納鍵で行うことを許容した実行属性証明書をサービス受領デバイスであるユーザデバイスに対して提供するステップを有し、

20

ユーザデバイスにおける実行ステップとして、

前記実行属性証明書に格納されたアドレス (A d) 情報に従って、該ユーザデバイスのメモリから登録鍵を取得するステップと、

取得した登録鍵を適用して、該実行属性証明書に格納された暗号化実行命令の復号を実行するステップと、

復号結果に基づくデータ処理を実行するステップと、

を有することを特徴とするデータ処理権限管理方法。

【請求項 10】

データ処理を実行する情報処理装置における情報処理方法であり、

暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵の情報処理装置内のメモリにおける格納領域を示すアドレス (A d) 情報とを格納データとして有し発行者署名のなされた実行属性証明書であり、署名をユーザデバイスのセキュリティチップの秘密鍵、または実行属性証明書中の格納鍵で行うことを許容した実行属性証明書を入力するステップと、

30

署名検証処理を実行するとともに、署名検証の成立を条件として、前記アドレス (A d) 情報に従って、前記メモリから登録鍵を取得するステップと、

取得した登録鍵を適用して前記暗号化実行命令を復号するステップと、

復号された実行命令を実行するデータ処理ステップと、

を有することを特徴とする情報処理方法。

【請求項 11】

40

データ処理を実行する情報処理装置における情報処理を実行せしめるコンピュータ・プログラムであって、

暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵の情報処理装置内のメモリにおける格納領域を示すアドレス (A d) 情報とを格納データとして有し発行者署名のなされた実行属性証明書であり、署名をユーザデバイスのセキュリティチップの秘密鍵、または実行属性証明書中の格納鍵で行うことを許容した実行属性証明書を入力するステップと、

署名検証処理を実行するとともに、署名検証の成立を条件として、前記アドレス (A d) 情報に従って、前記メモリから登録鍵を取得するステップと、

取得した登録鍵を適用して前記暗号化実行命令を復号するステップと、

50

復号された実行命令を実行するデータ処理ステップと、
を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、データ処理権限管理システム、情報処理装置、および方法、並びにコンピュータ・プログラムに関する。例えばコンテンツ利用、あるいはサービス利用処理等において確認が要求されるユーザ等のサービス受領権限の管理を行い、正当なサービス受領権限を有するユーザに対してのみサービスが実行可能となる構成として、サービスの利用を厳格に制限することを可能としたデータ処理権限管理システム、情報処理装置、および方法、並びにコンピュータ・プログラムに関する。

10

【0002】

【従来の技術】

昨今、インターネット等の通信網、あるいは、DVD、CD、ICカード等の流通可能な記憶媒体を介した音楽データ、画像データ、ゲームプログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）の配信、あるいは端末間のデータ送受信処理を伴う決済等、端末間の通信処理を伴ったサービス提供処理が盛んに実行されている。例えばPC、携帯通信端末、ポータブルデバイス、あるいはICカード等の様々なユーザデバイスを有するユーザが、自宅、外出先等においてユーザデバイスをサービスプロバイダのサービス提供デバイスと接続し、デバイス間で情報の交換、あるいはコンテンツ、サービスの受領を行なうことが日常的になりつつある。

20

【0003】

具体的なサービス利用例としては、例えば、PC、携帯端末等を用いて、コンテンツ配信サービスプロバイダにアクセスし、音楽、動画、ゲームプログラム等の様々なコンテンツをダウンロードしたり、あるいは、個人情報、銀行口座情報、利用可能金額情報等を格納したICチップ内蔵のメモリカード等を用いて、ショッピングに利用したり、振替処理を行ったり、あるいは、駅の改札、バス等において切符の代替手段として用いるなど、様々な利用がなされつつある。

【0004】

このように通信網あるいは媒体を介したコンテンツあるいはサービス等の流通が盛んになる一方、コンテンツ、あるいはサービスの不正利用、すなわち正当な権限を有しないユーザによるサービス利用の問題が発生しており、正当な利用権限を有するユーザにのみ確実にコンテンツあるいはサービス等の提供を行ない、サービスの不正利用を排除するシステムの構築が望まれている。

30

【0005】

例えば、音楽データ、画像データ、ゲームプログラム等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されており、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにセキュリティを考慮したシステムが採用されている。

40

【0006】

サービスを受領する機器あるいはユーザの利用制限を実現する1つの手法が、暗号化処理である。例えばコンテンツあるいはサービス情報を機器またはユーザに提供する際に、暗号化して提供し、正規の機器またはユーザのみに利用可能な復号鍵を配布し、コンテンツあるいはサービス利用を可能とする形態がある。暗号化データは、復号鍵を用いた復号化処理によって復号データ（平文）に戻すことができる。

【0007】

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通の

50

ものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にDES（データ暗号標準：Data encryption standard）がある。

【0008】

また、暗号化するとき使用する暗号化鍵による処理と、復号するとき使用する復号化鍵の処理とを異なる鍵で行なう方式がいわゆる公開鍵暗号方式と呼ばれる方式である。公開鍵暗号方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が生成した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号化処理が可能となる。秘密鍵は、公開鍵を生成した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号方式の代表的なものには、楕円曲線暗号、あるいはRSA（Rivest-Shamir-Adleman）暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

【0009】

上記のようなコンテンツあるいはサービスの利用管理構成において、正当なユーザであるか否かの判定は、例えばコンテンツあるいはサービスの提供者であるサービスプロバイダとPC、携帯端末、ICカード等のユーザデバイス間において、コンテンツ、サービス情報等の暗号化データ、あるいは復号鍵の提供前の認証処理によって行なう方法が知られている。一般的な認証処理においては、相手の確認を行なうとともに、その通信でのみ有効なセッションキーを生成して、認証が成立した場合に、生成したセッションキーを用いてコンテンツ、あるいは復号鍵等のデータを暗号化して通信を行なう。

【0010】

【発明が解決しようとする課題】

ユーザ権限を確認するシステムとしては、上述のように、サービスを提供するサービスプロバイダとユーザ間で1対1の認証処理を実行し、ユーザ権限の確認を実行する手法があるが、コンテンツ提供サービス、その他の情報利用サービス、決済サービス等、ユーザ端末で実行可能なサービスが多様化するにつれ、個々のユーザ、あるいはユーザ端末のサービス利用権限の有無を効率的に確実にかつセキュアに実行するシステムの構築が望まれている。

【0011】

本発明は、上記問題点に鑑みてなされたものであり、様々なサービスをPC、通信端末装置、携帯端末、ICカード等のユーザデバイスを介してサービスプロバイダの提供するデバイス等から受領する際、ユーザのサービス利用権限を効率的に確実にかつセキュアに確認して、正当なサービス受領権限を有するユーザに対してのみサービスが実行可能となる構成として、サービスの利用を厳格に制限することを可能としたデータ処理権限管理システム、情報処理装置、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

【0012】

【課題を解決するための手段】

本発明の第1の側面は、

サービスプロバイダの提供するサービスを実行するユーザデバイスにおけるデータ処理権限を管理するデータ処理権限管理システムであり、

サービスプロバイダ機器は、

暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス（Ad）情報とを格納データとして有し、署名をユーザデバイスのセキュリティチップの秘密鍵、または実行属性証明書中の格納鍵で行うことを許容した実行属性証明書をサービス受領デバイスであるユーザデバイスに対して提供し、

ユーザデバイスは、

前記実行属性証明書に格納されたアドレス（Ａｄ）情報に従って、該ユーザデバイスのメモリから取得した登録鍵を適用して、該実行属性証明書に格納された暗号化実行命令の復号を行ない、復号結果に基づくデータ処理を実行する構成としたことを特徴とするデータ処理権限管理システムにある。

【００２４】

さらに、本発明の第２の側面は、

データ処理を実行する情報処理装置であり、

暗号化データの復号処理に適用する登録鍵を格納するメモリ部と、

暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵の情報処理装置内のメモリにおける格納領域を示すアドレス（Ａｄ）情報とを格納データとして有し、発行者署名のなされた実行属性証明書であり、署名をユーザデバイスのセキュリティチップの秘密鍵、または実行属性証明書中の格納鍵で行うことを許容した実行属性証明書を入力し、署名検証処理を実行するとともに、署名検証の成立を条件として、前記アドレス（Ａｄ）情報に従って、前記メモリ部から取得した登録鍵を適用して前記暗号化実行命令を復号する暗号処理部と、

前記暗号処理部において復号された実行命令を実行するデータ処理部と、

を有することを特徴とする情報処理装置にある。

【００２５】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記登録鍵格納領域を指定したアドレス（Ａｄ）に対応するメモリ領域に、前記登録鍵と異なるデータ構成を持つリセット鍵データを書き込むことにより登録鍵の破棄処理を実行する構成であることを特徴とする。

【００２６】

さらに、本発明の情報処理装置の一実施態様において、前記実行属性証明書に格納された暗号化実行命令には、実行命令の適用可能回数識別値が格納され、前記データ処理部は、実行命令の実行に応じて前記適用可能回数識別値を更新して、情報処理装置内のセキュリティチップの秘密鍵による署名を実行して更新された適用可能回数識別値を含む新たな実行属性証明書の生成を行なう構成であることを特徴とする。

【００２７】

さらに、本発明の情報処理装置の一実施態様において、前記実行属性証明書に格納された暗号化実行命令には、実行命令の適用可能回数識別値が格納され、前記データ処理部は、実行命令の実行に応じて前記適用可能回数識別値を更新して、更新された適用可能回数識別値が０となった場合に、前記登録鍵格納領域を指定したアドレス（Ａｄ）に対応するメモリ領域に、前記登録鍵と異なるデータ構成を持つリセット鍵データを書き込むことにより登録鍵の破棄処理を実行する構成であることを特徴とする。

【００２８】

さらに、本発明の情報処理装置の一実施態様において、前記実行属性証明書に格納された暗号化実行命令は、前記情報処理装置のセキュリティチップの秘密鍵での署名が許容され、さらに他デバイスへの譲渡処理の許容された譲渡用実行属性証明書の生成処理命令を含み、前記データ処理部は、前記譲渡用実行属性証明書の生成処理命令に従い、情報処理装置内のセキュリティチップの秘密鍵による署名を付与した新たな譲渡用実行属性証明書の生成処理を実行し、生成した譲渡用実行属性証明書の他デバイスへの提供処理を実行する構成であることを特徴とする。

【００２９】

さらに、本発明の情報処理装置の一実施態様において、前記実行属性証明書に格納された暗号化実行命令には、他デバイスの属性を証明する証明書として、該他デバイスに対して発行する属性証明書であり、前記暗号化実行命令に含まれる署名生成用鍵によって署名のなされる審査代行属性証明書の発行処理命令、および該審査代行属性証明書の生成に必要とする署名生成用鍵を含み、前記データ処理部は、前記審査代行属性証明書の発行処理命令に従い、前記他デバイスの属性確認の審査を属性証明書の真の発行者に代わって実行

10

20

30

40

50

し、属性が確認された場合に、前記署名生成用鍵を適用して署名を実行した審査代行属性証明書の生成処理を実行して前記他デバイスに提供する構成であることを特徴とする。

【 0 0 3 0 】

さらに、本発明の情報処理装置の一実施態様において、前記実行属性証明書に格納された暗号化実行命令には、自デバイスの属性を証明する証明書として、前記暗号化実行命令に含まれる署名生成用鍵によって署名のなされる代理署名属性証明書の発行処理命令、および該代理署名属性証明書の生成に必要とする署名生成用鍵を含み、前記データ処理部は、前記代理署名属性証明書の発行処理命令に従い、該代理署名属性証明書の検証を実行する検証デバイスから受領した検証用乱数 (R a) を格納データとして含み、属性証明書の真の発行者の鍵の代わりに前記署名生成用鍵を適用した署名を有する代理署名属性証明書の生成処理を実行する構成であることを特徴とする。

10

【 0 0 3 1 】

さらに、本発明の第 3 の側面は、

サービスプロバイダの提供するサービスを実行するユーザデバイスにおけるデータ処理権限を管理するデータ処理権限管理方法であり、

サービスプロバイダ機器における実行ステップとして、

暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス (A d) 情報とを格納データとして有し、署名をユーザデバイスのセキュリティチップの秘密鍵、または実行属性証明書中の格納鍵で行うことを許容した実行属性証明書をサービス受領デバイスであるユーザデバイスに対して提供するステップを有し、

20

ユーザデバイスにおける実行ステップとして、

前記実行属性証明書に格納されたアドレス (A d) 情報に従って、該ユーザデバイスのメモリから登録鍵を取得するステップと、

取得した登録鍵を適用して、該実行属性証明書に格納された暗号化実行命令の復号を実行するステップと、

復号結果に基づくデータ処理を実行するステップと、

を有することを特徴とするデータ処理権限管理方法にある。

【 0 0 4 3 】

さらに、本発明の第 4 の側面は、

データ処理を実行する情報処理装置における情報処理方法であり、

暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵の情報処理装置内のメモリにおける格納領域を示すアドレス (A d) 情報とを格納データとして有し発行者署名のなされた実行属性証明書であり、署名をユーザデバイスのセキュリティチップの秘密鍵、または実行属性証明書中の格納鍵で行うことを許容した実行属性証明書を入力するステップと、

30

署名検証処理を実行するとともに、署名検証の成立を条件として、前記アドレス (A d) 情報に従って、前記メモリから登録鍵を取得するステップと、

取得した登録鍵を適用して前記暗号化実行命令を復号するステップと、

復号された実行命令を実行するデータ処理ステップと、

を有することを特徴とする情報処理方法にある。

40

【 0 0 5 0 】

さらに、本発明の第 5 の側面は、

データ処理を実行する情報処理装置における情報処理を実行せしめるコンピュータ・プログラムであって、

暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵の情報処理装置内のメモリにおける格納領域を示すアドレス (A d) 情報とを格納データとして有し発行者署名のなされた実行属性証明書であり、署名をユーザデバイスのセキュリティチップの秘密鍵、または実行属性証明書中の格納鍵で行うことを許容した実行属性証明書を入力するステップと、

50

署名検証処理を実行するとともに、署名検証の成立を条件として、前記アドレス（Ａｄ）情報に従って、前記メモリから登録鍵を取得するステップと、
取得した登録鍵を適用して前記暗号化実行命令を復号するステップと、
復号された実行命令を実行するデータ処理ステップと、
を有することを特徴とするコンピュータ・プログラムにある。

【００５１】

【作用】

本発明の構成によれば、暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、暗号化実行命令の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス（Ａｄ）情報とを格納データとして有する実行属性証明書をサービス受領デバイスであるユーザデバイスに対して提供し、ユーザデバイスにおいて、実行属性証明書に格納されたアドレス（Ａｄ）情報に従って、ユーザデバイスのメモリから取得した登録鍵を適用して、実行属性証明書に格納された暗号化実行命令の復号を行ない、復号結果に基づくデータ処理を実行する構成としたので、登録鍵を実行属性証明書に格納したアドレスに従って取得可能なユーザデバイスにおいてのみ実行属性証明書に格納した実行命令を実行することが可能となり、サービス利用権限を有するユーザに対して厳格に限定したサービスの提供が可能となる。

10

【００５２】

さらに、本発明の構成によれば、サービス提供実行属性証明書に適用する登録鍵の格納を登録鍵生成実行属性証明書に従って実行する構成としたので、不正な登録鍵の格納が防止され、不正なサービス受領を確実に防止できる。

20

【００５３】

さらに、本発明の構成によれば、リセット鍵の書き込みによる登録鍵の破棄処理を実行する構成としたので、不正な登録鍵の保持を防止することが可能となる。

【００５４】

さらに、本発明の構成によれば、実行命令内に適用可能回数識別値を格納し、実行命令の実行に応じて適用可能回数識別値を更新して、更新された適用可能回数識別値を含む新たな実行属性証明書の生成を行なう構成としたので、利用回数制限のあるサービスの受領を確実な回数制限の下に実行可能となる。

【００５５】

さらに、本発明の構成によれば、譲渡用実行属性証明書の生成処理命令、審査代行属性証明書の発行処理命令、代理署名属性証明書の発行処理命令等の各種の実行命令を実行属性証明書に格納することにより、様々な属性証明書の利用形態が実現される。

30

【００５６】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

40

【００５７】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００５８】

【発明の実施の形態】

以下、本発明について図面を参照して詳細に説明する。なお、以下、下記に示す項目順に説明する。

（１）権限管理システム構成概要

50

- (2) ユーザデバイス構成
- (3) グループ属性証明書発行、利用処理
- (3 - 1) グループ属性証明書発行前準備処理
- (3 - 2) グループ属性証明書発行処理
- (3 - 3) グループ属性証明書利用処理
- (4) ユーザデバイス間におけるグループ属性証明書の発行、利用処理
- (5) グループ属性証明書の具体的利用例
- (5 - 1) コンテンツ配信サービス
- (5 - 2) リモートコントロールサービス
- (5 - 3) リモートメンテナンスサービス
- (5 - 4) パーソナルコミュニケーションサービス
- (6) 実行属性証明書 (実行 A C)
- (6 - 1) 実行属性証明書概要
- (6 - 2) 実行属性証明書発行処理
- (6 - 3) 実行属性証明書適用処理
- (6 - 4) 登録鍵リセット処理
- (6 - 5) 実行属性証明書リセット (破棄) 処理
- (7) 実行属性証明書の具体的利用処理
- (7 - 1) 回数制限付きサービス提供実行属性証明書
- (7 - 2) 譲渡機能付きサービス提供実行属性証明書
- (7 - 3) 代理発行実行属性証明書
- (8) 各エンティティの構成

10

【 0 0 5 9 】

[(1) 権限管理システム概要]

本発明の権限管理システムは、図 1 に示すように、公開鍵証明書 (P K C : P u b l i c Key certificate) 1 2 1 に基づく公開鍵基盤 (P K I : P u b l i c Key infrastructure) 1 0 1、属性証明書 (A C : A t t r i b u t e certificate) 1 2 2 に基づく権限管理基盤 (P M I : P r i v i l e g e management Infrastructure) 1 0 2 を基本インフラとし、これらのインフラの下で、耐タンパ性のセキュリティチップ (あるいはセキュリティモジュール) を持つユーザデバイス 1 1 1、1 1 3 およびサービスプロバイダ側のサービスプロバイダデバイス 1 1 2 間、あるいはユーザデバイス 1 1 1、1 1 3 相互間において権限確認処理を実行するとともに、権限確認に基づくサービス提供処理を実行する構成を持つ。

30

【 0 0 6 0 】

ユーザデバイス 1 1 1、1 1 3 は、例えば、サービスプロバイダ 1 1 2 から音楽、画像、プログラム等の各種コンテンツ提供サービス、その他の情報利用サービス、決済サービス等の各種サービスの提供を受領するユーザの端末であり、具体的には、P C、ゲーム端末、D V D、C D 等の再生装置、携帯通信端末、P D A、メモリカード等である。

【 0 0 6 1 】

また、ユーザデバイス 1 1 1、1 1 3 は、ユーザデバイス相互間における通信処理が実行可能な端末であり、各ユーザデバイスに対するアクセス可否等の処理を権限確認に基づいて実行する。ユーザデバイスは、耐タンパ構成のセキュリティチップを搭載している。ユーザデバイスの詳細については後述する。

40

【 0 0 6 2 】

サービスプロバイダ 1 1 2 は、セキュリティチップを持つユーザデバイス 1 1 1、1 1 3 に対してコンテンツ提供、決済処理等の各種サービス提供を行なうサービスプロバイダである。図 1 には、ユーザデバイスを 2 つとサービスプロバイダを 1 つのみ示してあるが、公開鍵基盤 (P K I) 1 0 1、権限管理基盤 (P M I) 1 0 2 のインフラの下には、多数のユーザデバイスおよびサービスプロバイダが存在し、それぞれが権限確認に基づくサー

50

ビス提供を実行する。なお、サービスは、サービスプロバイダがユーザデバイスに対して提供するのみならず、ユーザデバイス間においても相互にサービスの提供が行なわれる。

【 0 0 6 3 】

(公開鍵証明書 : P K C)

次に、公開鍵基盤について説明する。公開鍵基盤 (P K I : P u b l i c K e y i n f r a s t r u c t u r e) 1 0 1 は、公開鍵証明書 (P K C : P u b l i c K e y c e r t i f i c a t e) を適用して通信エンティティ間の認証処理、あるいは転送データの暗号処理等を実行可能とした基盤 (インフラ) である。(公開鍵証明書 (P K C)) について図 2 , 図 3、図 4 を用いて説明する。公開鍵証明書は、認証局 (C A : C e r t i f i c a t i o n A u t h o r i t y) が発行する証明書であり、ユーザ、各エンティティが自己の I D、公開鍵等を認証局に提出することにより、認証局側が認証局の I D や有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

10

【 0 0 6 4 】

なお、認証局 (C A) の事務代理機関として、登録局 (R A : R e g i s t r a t i o n A u t h o r i t y) を設け、登録局 (R A) において、公開鍵証明書 (P K C) の発行申請受理、申請者の審査、管理を行なう構成が一般的となっている。

【 0 0 6 5 】

公開鍵証明書のフォーマット例を図 2 ~ 図 4 に示す。これは、公開鍵証明書フォーマット I T U - T X . 5 0 9 に準拠した例である。

【 0 0 6 6 】

20

バージョン (version) は、証明書フォーマットのバージョンを示す。

シリアルナンバ (Serial Number) は、公開鍵証明書の認証局 (C A) によって設定される公開鍵証明書のシリアルナンバである。

シグネチャ (Signature) は、証明書の署名アルゴリズムである。なお、署名アルゴリズムとしては、楕円曲線暗号および R S A があり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、R S A が適用されている場合には鍵長が記録される。

発行者 (issuer) は、公開鍵証明書の発行者、すなわち公開鍵証明書発行局 (I A) の名称が識別可能な形式 (D i s t i n g u i s h e d N a m e) で記録されるフィールドである。

有効期限 (validity) は、証明書の有効期限である開始日時、終了日時が記録される。

サブジェクト公開鍵情報 (subject Public Key Info) は、証明書所有者の公開鍵情報として鍵のアルゴリズム、鍵が格納される。

30

【 0 0 6 7 】

証明局鍵識別子 (authority Key Identifier - key Identifier、authority Cert Issuer、authority Cert Serial Number) は、署名検証に用いる証明書発行者の鍵を識別する情報であり、鍵識別子、機関証明書発行者の名称、機関証明書シリアル番号を格納する。

サブジェクト鍵識別子 (subject key Identifier) は、複数の鍵を公開鍵証明書において証明する場合に各鍵を識別するための識別子を格納する。

鍵使用目的 (key usage) は、鍵の使用目的を指定するフィールドであり、(0) デジタル署名用、(1) 否認防止用、(2) 鍵の暗号化用、(3) メッセージの暗号化用、(4) 共通鍵配送用、(5) 認証の署名確認用、(6) 失効リストの署名確認用の各使用目的が設定される。

40

秘密鍵有効期限 (private Key Usage Period) は、証明書に格納した公開鍵に対応する秘密鍵の有効期限を記録する。

認証局ポリシー (certificate Policies) は、公開鍵証明書発行者の証明書発行ポリシーを記録する。例えば I S O / I E C 9 3 8 4 - 1 に準拠したポリシー I D、認証基準である。

ポリシー・マッピング (policy Mapping) は、認証パス中のポリシー関係の制限に関する情報を格納するフィールドであり、認証局 (C A) 証明書にのみ必要となる。

サブジェクト別名 (subject Alt Name) は、証明書所有者の別名を記録するフィールドである。

50

発行者別名 (issuer Alt Name) は、証明書発行者の別名を記録するフィールドである。
サブジェクト・ディレクトリ・アトリビュート (subject Directory Attribute) は、証明書所有者のために必要とされるディレクトリの属性を記録するフィールドである。
基本制約 (basic Constraint) は、証明対象の公開鍵が認証局 (C A) の署名用か、証明書所有者のものかを区別するためのフィールドである。

許容サブツリー制約名 (name Constraints permitted Subtrees) は、発行者が発行する証明書の名前の制限情報を格納するフィールドである。

制約ポリシー (policy Constraints) は、認証パス中のポリシーの関係の制限情報を格納するフィールドである。

C R L 参照ポイント (Certificate Revocation List Distribution Points) は、証明書所有者が証明書を利用する際に、証明書が失効していないか、どうかを確認するための失効リストの参照ポイントを記述するフィールドである。

署名アルゴリズム (Signature Algorithm) は、証明書の署名付けに用いるアルゴリズムを格納するフィールドである。

署名は、公開鍵証明書発行者の署名フィールドである。電子署名は、証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して発行者の秘密鍵を用いて生成したデータである。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果がある。

【 0 0 6 8 】

認証局は、図 2 ～ 図 4 に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための失効リスト (Revocation List) の作成、管理、配布 (これをリボケーション : Revocation と呼ぶ) を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【 0 0 6 9 】

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

【 0 0 7 0 】

(属性証明書 : A C)

権限管理基盤 (P M I : P r i v i l e g e m a n a g e m e n t I n f r a s t r u c t u r e) 1 0 2 は、属性証明書 (A C : A t t r i b u t e c e r t i f i c a t e) 1 2 2 を適用した権限確認処理を実行可能とする基盤 (インフラ) である。属性証明書の 1 形態としてのグループ属性証明書 (グループ A C) について図 5 乃至図 7 を参照して説明する。属性証明書の機能は、サービス利用権限の確認機能であり、属性証明書には、例えばサービスプロバイダの提供するコンテンツ、あるいはサービスの利用権といった権利関連情報や権限に関する所有者の属性情報が記述される。

【 0 0 7 1 】

属性証明書は、基本的には属性認証局 (A A : A t t r i b u t e A u t h o r i t y) が発行する証明書であり、証明書発行対象の属性情報を格納し、属性認証局側が I D や有効期限等の情報を付加し、さらに属性認証局の秘密鍵による署名を付加して作成される証明書である。ただし、以下において説明するグループ属性証明書、実行属性証明書は、必ずしも属性認証局 (A A : A t t r i b u t e A u t h o r i t y) が発行機関として限定されるものではなく、サービスプロバイダ、ユーザデバイスにおける発行処理が可能である。

【 0 0 7 2 】

なお、属性認証局 (A A) の事務代理機関として、属性証明書登録局 (A R A : A t t r i b u t e R e g i s t r a t i o n A u t h o r i t y) を設け、属性証明書登録局 (A R A) において、属性証明書 (A C) の発行申請受理、申請者の審査、管理を行なう構成により、処理負荷の分散が可能である。

【 0 0 7 3 】

10

20

30

40

50

本発明の構成において適用されるグループ属性証明書（グループ A C）は、複数の対象、例えば複数のユーザ、あるいは複数のユーザ機器を 1 つの同一属性集合としたグループとして設定し、設定したグループを単位として、グループの構成機器または構成ユーザに対して発行される属性証明書である。グループ属性証明書は、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加された証明書である。

【 0 0 7 4 】

例えば複数人が所属している会社、組織、学校といった属性、あるいは家族といったグループに属する各ユーザまたはユーザ機器に対して発行される。あるいは、1 つのサービスプロバイダの提供するサービスを受領する複数のユーザ単位といったグループのメンバ（ユーザ、ユーザ機器）に対して発行される。グループについては、様々な設定が可能であり、具体例については、後述する。

10

【 0 0 7 5 】

なお、後段で説明する実行属性証明書は、暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス（A d）情報とを格納データとして有する。実行属性証明書の詳細については、後段で詳細に説明する。

【 0 0 7 6 】

属性証明書の基本フォーマットはITU-T X.509で規定されており、IETF PKIX WGでProfileを策定している。公開鍵証明書とは異なり所有者の公開鍵を含まない。しかし属性認証局（Attribute Certificate Authority）の署名がついているため、改竄されていないかどうかの判定はこの署名を検証することで行える、という点は公開鍵証明書と同様である。

20

【 0 0 7 7 】

なお、本発明において適用するグループ属性証明書、あるいは実行属性証明書は、属性証明書の基本フォーマットに準拠したものとして構成可能である。ただし、ITU-T X.509で規定されたフォーマットに従うことが必須ではなく、独自フォーマットとした属性証明書構成としてもよい。

【 0 0 7 8 】

本発明の構成においては、属性証明書（A C）の発行管理を行なう属性認証局（A A : Attribute Certificate Authority）、および属性証明書登録局（A R A）の機能を、サービスプロバイダ、あるいはユーザデバイスが兼務することが可能である。すなわち、サービスプロバイダあるいはユーザデバイス自身が、属性認証局（A A）、属性証明書登録局（A R A）の各機能を果たす構成が可能である。

30

【 0 0 7 9 】

属性証明書は基本的に公開鍵証明書と関連づけて利用する。すなわち属性証明書所有者の本人性自体は公開鍵証明書で確認し、その上で所有者にいかなる権限が与えられているかを属性証明書によって確認する。例えばサービスプロバイダがユーザ、あるいはユーザ機器に対するサービスを提供する際、サービスを受領する権利を有するか否かを属性証明書を検証して確認する。属性証明書の検証にあたっては、当該証明書の署名検証を行った後、その属性証明書に関連づけられている公開鍵証明書の検証も行う。

40

【 0 0 8 0 】

なお、その際、原則的には証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施することが好ましい。複数の認証局（C A）が存在し、階層構成をなす認証局構成では、下位の認証局自身の公開鍵証明書は、その公開鍵証明書を発行する上位認証局によって署名されている。すなわち、下層の認証局（C A - L o w）に対して上位の認証局（C A - H i g h）が公開鍵証明書を発行するという連鎖的な公開鍵証明書発行構成をとる。公開鍵証明書の連鎖検証とは、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位（ル - ト C A）までの公開鍵証明書の署名検証を行なうことを意味する。

【 0 0 8 1 】

50

属性証明書の有効期間を短期間とすることにより、失効処理を行わないことも可能である。この場合、証明書の失効手続きや失効情報の参照手順等を省くことができ、システムが簡易となる長所がある。ただし証明書の不正利用に対しては失効以外の何らかの対策が必要となるため、十分に注意しなければならない。

【 0 0 8 2 】

図 5 を参照してグループ属性証明書の構成について説明する。

証明書のバージョン番号は、証明書フォーマットのバージョンを示す。

A C 保持者の公開鍵証明書情報、これは属性証明書 (A C) の発行者に対応する公開鍵証明書 (P K C) に関する情報であり、P K C 発行者名、P K C シリアル番号、P K C 発行者固有識別子等の情報であり、対応公開鍵証明書を関連づけるリンクデータとしての機能を持つ。

10

属性証明書の発行者の名前は、属性証明書の発行者、すなわち属性認証局 (A A) の名称が識別可能な形式 (Distinguished Name) で記録されるフィールドである。

署名アルゴリズム識別子は、属性証明書の署名アルゴリズム識別子を記録するフィールドである。

証明書の有効期限は、証明書の有効期限である開始日時、終了日時が記録される。

属性情報フィールドには、グループ属性証明書のグループを識別するグループ識別情報としてグループ I D が格納される。グループ I D は、このグループ属性証明書を利用した権限確認を行なうサービスプロバイダの有するサービスプロバイダ (S P) 管理グループ情報データベース (図 5 右下欄参照) のエントリと対応する識別子 (I D) である。

20

【 0 0 8 3 】

サービスプロバイダの有するサービスプロバイダ (S P) 管理グループ情報データベースは、図 5 右下欄に示すように、例えば、グループ属性証明書の発行者 (A R A) と、グループ識別子としてのグループ識別情報 (グループ I D) 、および「 A 者の社員」、「 B さんの家族」といったグループ情報を対応付けたテーブルである。サービスプロバイダは、グループ証明書に基づく権限確認処理において、証明書格納データとしてのグループ識別情報 (グループ I D) に基づいてテーブルから対応エントリを抽出し、グループ情報を含むグループ属性証明書情報を取得する。

【 0 0 8 4 】

なお、属性情報フィールドには、グループ識別情報 (グループ I D) 以外にも、様々な情報が格納可能であり、例えば、コンテンツ利用期限等のコンテンツ利用制限情報、サービス利用制限情報等の権限に関する詳細情報、さらにはサービスプロバイダ識別子 (I D) 、サービスプロバイダ・ネーム等の各種情報を格納することが可能である。また、詳細は、後述するが、暗号化コンテンツの復号に適用するコンテンツ鍵を取得するために必要となる情報を格納するフィールドとしての適用も可能である。

30

【 0 0 8 5 】

サービスプロバイダは、グループ属性証明書をユーザデバイスに対して送付し、ユーザデバイスは属性証明書の検証の後、自己のセキュリティチップ内のメモリに格納する。

【 0 0 8 6 】

属性証明書には、さらに、署名アルゴリズムが記録され、属性証明書発行者、例えば属性認証局 (A A) によって署名が施される。発行者がサービスプロバイダ、あるいはユーザデバイスである場合は、各発行者の署名がなされる。電子署名は、属性証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して属性証明書発行者の秘密鍵を用いて生成したデータである。

40

【 0 0 8 7 】

図 6 にグループ属性証明書 (グループ A C) の発行者、所有者、検証者、属性情報の構成例を示す。例えば同一の会社、あるいは 1 つの家族に属するユーザの所有する複数のユーザ機器グループの各々に対してグループ属性証明書が発行される場合、発行されたグループ属性証明書は、ユーザの所有する機器内のセキュリティチップ (S C : Security Chip 、あるいは U S C : User Security Chip) に格納される。ユーザデバイスの詳細について

50

は後述する。

【 0 0 8 8 】

ユーザデバイスに対して発行されたグループ属性証明書に基づいて権限確認を実行する検証者は、サービス提供エンティティ、例えばサービスプロバイダの機器内のセキュリティモジュール（ＳＭ：Security Module）、あるいはユーザデバイスのセキュリティチップ（ＳＣ：Security Chip）である。なお、ユーザデバイスのセキュリティチップ、サービスプロバイダの機器内のセキュリティモジュールは、外部からのデータ読み出しの制限された耐タンパ構成を持つことが好ましい。

【 0 0 8 9 】

グループ属性証明書には、例えば同一の会社、あるいは１つの家族等を識別可能な識別情報としてのグループ識別情報（グループＩＤ）を属性情報として有することとなる。

10

【 0 0 9 0 】

図７にグループ属性証明書の発行ポリシーテーブルの構成例を示す。グループ属性証明書の発行ポリシーテーブルは、グループ属性証明書を発行するエンティティ、例えば属性認証局（ＡＡ：Attribute Certificate Authority）、属性認証局（ＡＡ）の事務代行を行なう属性証明書登録局（ＡＲＡ：Attribute Registration Authority）、あるいはサービスプロバイダ、ユーザデバイスにおいて管理されるテーブルであり、発行したグループ属性証明書のグループ識別情報（グループＩＤ）、グループ情報、発行基準等の発行ポリシーとを対応付けたテーブルである。例えば、グループ属性証明書の新規発行、追加発行、更新処理等の際し、グループ属性証明書の発行ポリシーテーブルに基づいて、審査が実行され、ポリシーを満足する場合に限り、発行、更新等の手続きがなされる。

20

【 0 0 9 1 】

図８に権限管理システムに参加する各エンティティの信頼関係構成を説明するトラストモデルを示す。

【 0 0 9 2 】

システムホルダ（ＳＨ：System Holder）１３０は、本発明の権限管理システム全体の統括的管理を行なう主体、すなわちシステム運用主体であり、システムに参加する各エンティティのセキュリティチップ（ＳＣ）、セキュリティモジュール（ＳＭ）の正当性を保証するとともに、公開鍵証明書（ＰＫＣ）の発行責任を持つ。システムホルダ（ＳＨ）１３０は、最上位認証局としてのルートＣＡ（Root CA）１３１、階層構成の複数の認証局（ＣＡ）１３２、および公開鍵証明書発行事務局としての登録局（ＲＡ）１３３を有する。

30

【 0 0 9 3 】

システムホルダ（ＳＨ：System Holder）１３０は、属性認証局（ＡＡ）１４０、属性証明書登録局（ＡＲＡ）１５０、サービスプロバイダ１６０、およびユーザデバイス１７０としてのユーザ識別デバイス（ＵＩＤ：User Identification Device）１７１、エンドエンティティ（ＥＥ：End Entity）１７２の各エンティティに対応する公開鍵証明書（ＰＫＣ）を発行し、各エンティティは、必要とするエンティティの公開鍵証明書をそれぞれの機器内の耐タンパ構成を持つセキュリティチップ（ＳＣ）またはセキュリティモジュール（ＳＭ）、もしくは、場合によっては外部の記憶装置に公開鍵証明書（ＰＫＣ）を格納する。

40

【 0 0 9 4 】

また、グループ属性証明書（グループＡＣ）は、サービスプロバイダ１６０、およびユーザデバイス１７０としてのユーザ識別デバイス（ＵＩＤ：User Identification Device）１７１、エンドエンティティ（ＥＥ：End Entity）１７２の各エンティティ等からの属性証明書発行要求を、例えば属性証明書登録局（ＡＲＡ）１５０において受領し、先に図７を参照して説明したポリシーテーブル１５１のポリシー（発行条件等）に従って属性証明書発行審査を行ない、発行可と判定された場合に属性認証局（ＡＡ）１４０に対して、属性証明書登録局（ＡＲＡ）１５０から発行依頼を転送する。

【 0 0 9 5 】

50

属性認証局(AA)140は、グループ属性証明書発行依頼に基づいて、グループ識別情報(グループID)を属性情報として格納し、属性認証局(AA)140の秘密鍵による署名を付加したグループ属性証明書(図5参照)を発行要求者に対して発行する。

【0096】

なお、前述したように、これら属性認証局(AA)140、および属性証明書登録局(ARA)150は、サービスプロバイダ、あるいはユーザデバイスがその機能を実行する構成とすることも可能である。

【0097】

〔(2)ユーザデバイス構成〕

次にサービスを利用する情報処理装置としてのユーザデバイスの構成について説明する。ユーザデバイスは、その機能に基づいて、2つのカテゴリに分類される。一方はサービスを実際に利用する機器としてのエンドエンティティ(EE)であり、サービスプロバイダの提供するサービス情報を受領するインタフェースを持つ例えばPC、ホームサーバ、PDA等の携帯端末、ICカード等、各種データ処理装置である。これらの機器は、耐タンパ構成を持つセキュリティチップ(SC)またはモジュール(SM)を有し、機器対応の公開鍵証明書、機器対応のグループ属性証明書が必要に応じて格納される。

【0098】

もう一方は、個人認証処理に適用するデバイスとしてのユーザ識別デバイス(UID)である。ユーザ識別デバイス(UID)もエンドエンティティと同様の機器によって構成されるが、サービスプロバイダの提供するサービス情報を直接受領するためのインタフェースを必ずしも有することのない機器である。サービスプロバイダ機器との通信は、エンドエンティティ(EE)を介して実行する。ユーザ識別デバイス(UID)は、ユーザの認証に適用される機器である。これらの機器は、耐タンパ構成を持つセキュリティチップ(SC)またはセキュリティモジュール(SM)を有し、ユーザ対応の公開鍵証明書、機器対応のグループ属性証明書が必要に応じて格納される。

【0099】

なお、エンドエンティティ(EE)とユーザ識別デバイス(UID)は個別の機器としてそれぞれ構成することも可能であるが、1つの機器内に両機能を備えた構成とすることも可能である。

【0100】

個別の構成具体例としては、例えばICカード等の機器をユーザ識別デバイス(UID)として構成し、エンドエンティティ(EE)をPCとした構成がある。この構成では、ICカードをPCにデータ転送可能な状態にセットし、まずICカードとサービスプロバイダ間との通信をPCを介して実行して公開鍵証明書、グループ属性証明書を適用したユーザ認証、ユーザ権限確認処理を実行し、さらにこれらの処理の後にエンドエンティティとしてのPCとサービスプロバイダ間での認証、権限確認を行なう等の処理が実行可能となる。これらの権限確認処理の詳細については、後述する。

【0101】

ユーザデバイスとしてのエンドエンティティ(EE)とユーザ識別デバイス(UID)に構成されるセキュリティチップの構成例について、図9を参照して説明する。なお、エンドエンティティ(EE)は、データ処理手段としてのCPU、通信機能を備えた例えばPC、ゲーム端末、携帯端末、PDA、ICカード(メモリカード)、DVD、CD等の再生装置、記録再生装置等によって構成され、耐タンパ構造を持つセキュリティチップ(SC)が実装される。

【0102】

図9に示すように、エンドエンティティ(EE)またはユーザ識別デバイス(UID)により構成されるユーザデバイス200には、セキュリティチップ210が、ユーザデバイス側制御部221に対して、相互にデータ転送可能な構成として内蔵される。

【0103】

セキュリティチップ210は、プログラム実行機能、演算処理機能を持つCPU(Centra

10

20

30

40

50

I Processing Unit) 201を有し、データ通信のインタフェース機能を持つ通信インタフェース202、CPU201によって実行される各種プログラム、例えば暗号処理プログラムなどを記憶するROM(Read Only Memory)203、実行プログラムのロード領域、また、各プログラム処理におけるワーク領域として機能するRAM(Random Access Memory)204、外部機器との認証処理、電子署名の生成、検証処理、格納データの暗号化、復号化処理等の暗号処理を実行する暗号処理部205、サービスプロバイダ毎の情報、各種鍵データを含むデバイスの固有情報を格納した例えばEEPROM(Electrically Erasable Programmable ROM)によって構成されるメモリ部206を有する。

【0104】

ユーザデバイス200は、暗号化コンテンツあるいはサービス情報等を格納する領域としてのEEPROM、ハードディスク等によって構成される外部メモリ部222を有する。外部メモリ部222は、公開鍵証明書、グループ属性証明書の格納領域としても利用可能である。

10

【0105】

セキュリティチップを搭載したユーザデバイスが、外部エンティティ、例えばサービスプロバイダと接続し、データ転送処理を実行する場合には、ネットワークインタフェース232を介したサービスプロバイダとの接続を実行する。ただし、前述したようにサービスプロバイダとの接続を実行するインタフェースを有するのは、エンドエンティティ(EE)であり、ユーザ識別デバイス(UID)は、必ずしもネットワークインタフェース232を持つとは限らないので、ユーザ識別デバイス(UID)の接続機器インタフェース231を介してエンドエンティティ(EE)の接続機器インタフェース231に接続し、エンドエンティティのネットワークインタフェース232を介した通信を実行する。

20

【0106】

すなわち、ユーザ識別デバイス(UID)は、エンドエンティティを介してサービスプロバイダの機器との通信を実行する。

【0107】

エンドエンティティ(EE)、ユーザ識別デバイス(UID)等のユーザデバイスのセキュリティチップ210とサービスプロバイダ間でデータ転送を実行する場合には、必要に応じて、セキュリティチップ210と、外部エンティティ間の相互認証が行われ、また転送データの暗号化が行なわれる。これらの処理の詳細については、後段で詳述する。

30

【0108】

ユーザデバイスのセキュリティチップの格納データ例を図10に示す。これらの多くは、不揮発性メモリの一形態であるフラッシュメモリ等のEEPROM(Electrically Erasable Programmable ROM)によって構成されるメモリ部206に格納されるが、公開鍵証明書、グループ属性証明書、あるいは後述する実行属性証明書は、セキュリティチップ内のメモリに格納しても、外部メモリに格納してもよい。

【0109】

各データについて説明する。

公開鍵証明書(PKC)：公開鍵証明書は、第三者に対して正当な公開鍵であることを示す証明書で、証明書には配布したい公開鍵を含み、信頼のおける認証局により電子署名がなされている。ユーザデバイスには、前述した階層構成の最上位認証局(ルートCA)の公開鍵証明書、ユーザデバイスに対するサービスを提供するサービスプロバイダの公開鍵証明書等、ユーザデバイスとのデータ通信を実行する際の認証、暗号化、復号処理等に適用する公開鍵を取得するために必要となる公開鍵証明書が格納される。

40

【0110】

グループ属性証明書(AC)：公開鍵証明書が証明書利用者(所有者)の“本人性”を示すのに対し、グループ属性証明書は証明書利用者のグループを識別しグループの構成メンバーに付与された利用権限を確認するものである。利用者はグループ属性証明書を提示することにより、グループ属性証明書に記載された権利・権限情報に基づいて、サービス利用が行えるようになる。なお、グループ属性証明書は所定の発行手続きに基づいて発行され

50

グループ属性証明書を受領した各エンティティは、機器内の耐タンパ構成を持つセキュリティチップ（SC）またはセキュリティモジュール（SM）、もしくは、場合によっては外部の記憶装置に格納する。発行、格納処理の詳細は後述する。

【0111】

実行属性証明書：暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス（Ad）情報とを格納データとして有する属性証明書であり、アドレス情報に基づいてユーザデバイス内メモリから取得する登録鍵を適用して暗号化実行命令を復号して実行命令を取得し、実行命令を実行することで各種サービスが実行される。これらの処理の詳細は後述する。

10

【0112】

鍵データ：鍵データとしては、セキュリティチップに対して設定される公開鍵、秘密鍵のペア、上述した実行属性証明書に格納された暗号化実行命令を復号する際に適用する登録鍵、登録鍵の破棄（リセット）処理に適用するリセット鍵、さらに、乱数生成用鍵、相互認証用鍵等が格納される。なお、登録鍵の格納領域は、あらかじめ決められたアドレスによって決定されるメモリ領域に格納される。登録鍵、リセット鍵については、後段で詳細に説明する。

【0113】

識別情報：識別情報としては、セキュリティチップ自身の識別子としてのセキュリティチップIDが格納される。さらに継続的なサービス提供を受けるサービスプロバイダ（SP）の識別子としてのサービスプロバイダID、ユーザデバイスを利用するユーザに付与されたユーザID、サービスプロバイダの提供するサービスに対応するアプリケーションを識別するアプリケーションID等が格納可能である。

20

【0114】

その他：ユーザデバイスには、さらに、乱数生成用のシード情報、すなわち認証処理、暗号処理等の際に適用する乱数をANSI X9.17に従って生成するための情報や、様々な利用制限が付加されたサービスに関する利用情報、例えば、コンテンツ利用回数制限が付加されたコンテンツを利用した際に更新されるコンテンツ利用回数情報、あるいは決済情報等の情報、あるいは、各情報に基づいて算出されるハッシュ値が格納される。

【0115】

なお、図10に示すデータ構成例は、一例であり、この他にも必要に応じて、ユーザデバイスの受領するサービスに関連する各種の情報が格納可能である。

30

【0116】

なお、例えばサービス提供側のサービスプロバイダ側の有するセキュリティチップ、あるいはセキュリティモジュールも図9に示すユーザデバイスにおけるセキュリティチップ構成と同様の構成によって実現可能であり、以下に説明するグループ属性証明書の検証処理、生成処理、あるいは実行属性証明書の検証処理、生成処理の各実行手段として機能する。例えば、データ送受信部であるネットワークインタフェースを介して受信したグループ属性証明書あるいは実行属性証明書の検証処理の実行、あるいは、グループ属性証明書あるいは実行属性証明書の生成処理の実行手段として、図9に示すセキュリティチップと

40

【0117】

〔（3）グループ属性証明書発行、利用処理〕

次に、同一の学校、会社等の組織、あるいは1つの家族等、様々な集合に属するユーザ、あるいは、同一メーカーの機器、同一サービスプロバイダのサービスを受領するユーザ、機器等、複数のユーザまたは機器をグループとして設定し、グループに属するユーザまたは機器の各々に対して発行するグループ属性証明書の発行処理、および利用処理について説明する。

【0118】

グループ属性証明書は、サービスを受けようとするユーザまたは機器（ユーザデバイス）

50

が特定のグループに属することを確認可能な証明書であり、サービス受領時等に、サービス提供エンティティ、例えばサービスプロバイダに提示する。サービスプロバイダは、提示されたグループ属性証明書の検証処理を実行して、ユーザまたはユーザデバイスが特定のグループに属することが確認されたことを条件としてサービスを提供する。

【0119】

グループ属性証明書は、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名を有する証明書である。

【0120】

図11にグループ属性証明書の発行申請、発行処理、利用処理の流れの概略を説明する図を示す。グループ属性証明書に基づいたグループ所属証明の確認を条件としたサービス提供を行なうサービスプロバイダ314の提供するサービスを受領しようとするユーザデバイス311、すなわちセキュリティチップを有するエンドエンティティ(EE)またはユーザ識別デバイス(UID)は、まず、グループ属性証明書の発行エンティティに発行要求を行なう。例えば、属性証明書登録局(ARA: Attribute Registration Authority)312にグループ属性証明書の発行申請を行なう。

【0121】

属性証明書登録局(ARA)312は、発行申請に基づいて、発行ポリシーテーブル313を参照し、ポリシーを満足する場合には、属性認証局(AA: Attribute Certificate Authority)に対して属性証明書の発行を依頼し、属性認証局(AA)の発行したグループ属性証明書316をユーザデバイス311に送信する。

【0122】

グループ属性証明書316には、グループ識別子としてのグループIDが、属性情報フィールドに格納される(図5参照)。ユーザデバイス311は、サービスプロバイダ314の提供するサービス、例えばコンテンツ配信、決済処理等の何らかのサービスを受領する際に、グループ属性証明書316をサービスプロバイダ314に提示する。サービスプロバイダ314は、グループ属性証明書の検証処理、グループ情報データベース315の参照により、サービス提供を要求してきたユーザデバイス311がサービスを受領する権限を有するか否かを判定して、権限ありと判断した場合には、ユーザデバイス311に対するサービス提供を実行する。

【0123】

以下、グループ属性証明書発行、利用処理について、

(3-1) グループ属性証明書発行前準備処理

(3-2) グループ属性証明書発行処理

(3-3) グループ属性証明書利用処理

以上、3項目について、順次説明する。

【0124】

(3-1) グループ属性証明書発行前準備処理

まず、グループ属性証明書発行前準備処理について説明する。先に説明したように、グループ属性証明書は、基本的に属性認証局(AA)が発行し、属性証明書登録局(ARA)が属性証明書発行要求エンティティからの発行要求を受理し、ポリシー審査等を実行して、発行可と判定した後、属性認証局(AA)に属性証明書発行要求を転送し、属性認証局(AA)の発行した属性証明書を属性証明書登録局(ARA)を介して、発行要求エンティティに対して送付する処理構成が通常のスタイルである。ただし、以下、説明するように、サービスプロバイダ(SP)、ユーザデバイスにおいて、それぞれのポリシーの下に発行することも可能である。

【0125】

本発明のグループ属性証明書は、識別可能なグループ、例えば家族、学校、会社、あるいは特定のメーカーの機器等、何らかのグループを特定した上で、そのグループ構成メンバー(機器またはユーザ)に対して発行するものであり、一方、サービスを提供するサービス

10

20

30

40

50

プロバイダは、サービスを要求してきたユーザまたは機器が、特定のグループに属するかどうかをグループ属性証明書に基づいて判定する。従って、グループ属性証明書の発行処理実行エンティティと、グループ属性証明書に基づく権限確認（検証処理）を実行しサービスを提供するエンティティは、グループ属性証明書に対応して定義されるグループについて共通の認識を持つことが必要な場合、グループ属性証明書に対応して定義されるグループに関する情報、すなわちグループ情報を、グループ属性証明書発行エンティティと、サービス提供エンティティとが共有化する処理がグループ属性証明書発行前準備処理として必要となる。

【0126】

以下、グループ属性証明書発行エンティティを属性認証局（AA）または属性証明書登録局（ARA）とし、サービス提供エンティティをサービスプロバイダ（SP）とした場合のグループ情報共有化処理について、図12を参照して説明する。

【0127】

なお、以下に説明する例では、属性認証局（AA）と属性証明書登録局（ARA）は信頼関係にあり、属性証明書登録局（ARA）がグループ属性証明書の発行審査を行ない、属性証明書登録局（ARA）の審査結果に基づいて、属性認証局（AA）がグループ属性証明書の発行処理を行なう構成を例として説明する。従って、グループ情報の共有エンティティは、サービスプロバイダ（SP）と属性証明書登録局（ARA）の2つのエンティティとなる。

【0128】

図12に示す処理シーケンス図に従ってサービスプロバイダ（SP）と属性証明書登録局（ARA）のグループ情報共有処理について説明する。

【0129】

まずステップS101において、サービスプロバイダ（SP）とグループ属性証明書の発行審査を実行する属性証明書登録局（ARA）との間で相互認証処理が実行される。なお、グループ属性証明書の発行審査を行なう属性証明書登録局（ARA）を、以下、グループ属性証明書登録局（ARA）とする。

【0130】

サービスプロバイダ（SP）とグループ属性証明書登録局（ARA）との間で実行される相互認証は、データ送受信を実行する2つのエンティティ間で相互に相手が正しいデータ通信者であるか否かの確認のために実行される処理である。認証成立を条件として必要なデータ転送を行なう。また、相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として、その後は、セッション鍵に基づく暗号化処理を施したデータ転送を行なう構成が好ましい。相互認証方式としては、公開鍵暗号方式、共通鍵暗号方式等、各方式の適用が可能である。

【0131】

ここでは、公開鍵暗号方式の1つの認証処理方式であるハンドシェイクプロトコル（TLS1.0）について図13のシーケンス図を参照して説明する。

【0132】

図13において、エンティティA（クライアント）、エンティティB（サーバ）が、通信を実行する2エンティティであり、ここではサービスプロバイダ（SP）またはグループ属性証明書登録局（ARA）に対応する。まず、（1）エンティティBが暗号化仕様を決定するためのネゴシエーション開始要求をハローリクエストとしてエンティティAに送信する。（2）エンティティAはハローリクエストを受信すると、利用する暗号化アルゴリズム、セッションID、プロトコルバージョンの候補をクライアントハローとして、エンティティB側に送信する。

【0133】

（3）エンティティB側は、利用を決定した暗号化アルゴリズム、セッションID、プロトコルバージョンをサーバーハローとしてエンティティAに送信する。（4）エンティティBは、自己の所有するルートCAまでの公開鍵証明書（X.509v3）一式をエンテ

10

20

30

40

50

ィテイ A に送信（サーバ・サーティフィケート）する。なお、証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施しない場合には、必ずしもルート C A までの公開鍵証明書（X . 5 0 9 v 3）一式を送付する必要はない。（5）エンティティ B は、R S A 公開鍵または D i f f i e & H e l l m a n 公開鍵情報をエンティティ A に送信（サーバ・キー・エクスチェンジ）する。これは証明書が利用できない場合に一時的に適用する公開鍵情報である。

【 0 1 3 4 】

（6）次にエンティティ B 側は、エンティティ A に対してサーティフィケート・リクエストとして、エンティティ A の有する証明書を要求し、（7）エンティティ B によるネゴシエーション処理の終了を知らせる（サーバハロー終了）。

10

【 0 1 3 5 】

（8）サーバハロー終了を受信したエンティティ A は、自己の所有するルート C A までの公開鍵証明書（X . 5 0 9 v 3）一式をエンティティ B に送信（クライアント・サーティフィケート）する。なお、公開鍵証明書の連鎖検証を行なわない場合は公開鍵証明書の一式送付は必須ではない。（9）エンティティ A は、48 バイト乱数をエンティティ B の公開鍵で暗号化してエンティティ B に送信する。エンティティ B、エンティティ A は、この値をもとに送受信データ検証処理のためのメッセージ認証コード：M A C（Message Authentication Code）生成用のデータ等を含むマスターシークレットを生成する。

【 0 1 3 6 】

（10）エンティティ A は、クライアント証明書の正しさを確認するため、ここまでのメッセージのダイジェストをクライアントの秘密鍵で暗号化してエンティティ B に送信（クライアントサーティフィケート確認）し、（11）先に決定した暗号化アルゴリズム、鍵利用の開始を通知（チェンジ・サイファー・スペック）し、（12）認証の終了を通知する。一方、（13）エンティティ B 側からエンティティ A に対しても、先に決定した暗号化アルゴリズム、鍵利用の開始を通知（チェンジ・サイファー・スペック）し、（14）認証の終了を通知する。

20

【 0 1 3 7 】

上記処理において決定された暗号化アルゴリズムに従ってエンティティ A とエンティティ B 間のデータ転送が実行されることになる。

【 0 1 3 8 】

データ改竄の検証は、上述の認証処理でエンティティ A とエンティティ B 間の合意のもとに生成されたマスターシークレットから算出されるメッセージ認証コード：M A C（Message Authentication Code）を各エンティティの送信データに付加することでメッセージの改竄検証を行なう。

30

【 0 1 3 9 】

図 1 4 にメッセージ認証コード：M A C（Message Authentication Code）の生成構成を示す。データ送信側は、送信データに対して、認証処理において生成したマスターシークレットに基づいて生成される M A C シークレットを付加し、これらの全体データからハッシュ値を計算し、さらに M A C シークレット、パディング、ハッシュ値に基づいてハッシュ算出を行なってメッセージ認証コード（M A C）を生成する。この生成した M A C を送信データに付加して、受信側で受信データに基づいて生成した M A C と受信 M A C との一致が認められればデータ改竄なしと判定し、一致が認められない場合には、データの改竄があったものと判定する。

40

【 0 1 4 0 】

図 1 2 に示すステップ S 1 0 1 において、サービスプロバイダ（S P）とグループ属性証明書の発行審査を実行する属性証明書登録局（A R A）との間で、例えば上述したシーケンスに従った相互認証処理が実行され、双方が正しい通信相手であることの確認がなされると、ステップ S 1 0 2 において、サービスプロバイダ（S P）と、属性証明書登録局（A R A）との間で、グループ情報の共有処理を実行する。

【 0 1 4 1 】

50

グループ情報の共有とは、具体的には、グループ属性証明書の発行エンティティ（例えば属性証明書登録局（ＡＲＡ））の管理する発行ポリシーテーブルと、グループ属性証明書の検証および検証に基づくサービス提供エンティティ（例えばサービスプロバイダ（ＳＰ））の有するグループ情報データベースとが整合した情報を保有する状態に設定する処理として行われる。

【０１４２】

先に説明したように、グループ属性証明書の発行エンティティ（例えば属性証明書登録局（ＡＲＡ））は、発行ポリシーテーブルを有し、グループ属性証明書の検証および検証に基づくサービス提供エンティティ（例えばサービスプロバイダ（ＳＰ））は、グループ情報データベースを有する。図１５に各情報構成例を示す。

10

【０１４３】

（Ａ）発行ポリシーテーブルは、属性証明書登録局（ＡＲＡ）が保持管理し、グループ属性証明書の発行処理等において参照する。一方、（Ｂ）グループ情報データベース（ＤＢ）は、サービスプロバイダ（ＳＰ）が保持管理し、サービス提供時のグループ属性証明書検証時に参照する。

【０１４４】

属性証明書登録局（ＡＲＡ）が保持管理する（Ａ）発行ポリシーテーブルと、サービスプロバイダ（ＳＰ）が保持管理する（Ｂ）グループ情報データベース（ＤＢ）は、整合性を有することが必要となる。図１５の例では、（Ａ）発行ポリシーテーブルのエントリ３４１は、（Ｂ）グループ情報データベース（ＤＢ）のエントリ３５１と整合しており、（Ａ）発行ポリシーテーブルのエントリ３４２は、（Ｂ）グループ情報データベース（ＤＢ）のエントリ３５２と整合している。このように、属性証明書登録局（ＡＲＡ）が保持管理する（Ａ）発行ポリシーテーブルと、サービスプロバイダ（ＳＰ）が保持管理する（Ｂ）グループ情報データベース（ＤＢ）との整合性保持処理が図１２のシーケンス図におけるステップＳ１０２のグループ情報共有処理である。

20

【０１４５】

なお、グループ情報共有処理の態様としては、以下の２例がある。

ポリシー受諾型：グループ属性証明書の検証および検証に基づくサービス提供エンティティ（例えばサービスプロバイダ（ＳＰ））は、種々のグループ属性証明書の発行エンティティ（例えば属性証明書登録局（ＡＲＡ））の発行ポリシーを検討し、自身のサービスに適合するグループＡＲＡを選択し、その選択したグループＡＲＡが管理するグループ情報をサービスプロバイダ（ＳＰ）が取得する。

30

【０１４６】

発行委託型：独自の属性証明書発行ポリシーを持たずに、単にグループ属性証明書の発行を請け負う形態のグループ属性証明書の発行エンティティ（例えばグループ属性証明書登録局（ＡＲＡ））に対して、グループ属性証明書の検証および検証に基づくサービス提供エンティティ（例えばサービスプロバイダ（ＳＰ））が設定した発行ポリシーをグループ属性証明書登録局（ＡＲＡ）に提示して、グループ属性証明書登録局（ＡＲＡ）が提示されたポリシーに従って、グループ属性証明書の発行処理を行なう。

【０１４７】

40

具体的なグループ情報共有処理の形態としては、グループ属性証明書に関するグループＩＤ、発行者、グループ情報、発行ポリシー等の情報をグループ属性証明書の発行エンティティ（例えばグループ属性証明書登録局（ＡＲＡ））が設定し、グループ属性証明書の検証および検証に基づくサービス提供エンティティ（例えばサービスプロバイダ（ＳＰ））に提示して、双方のエンティティが合意する態様、または、これらの情報をサービスプロバイダが設定し、グループＡＲＡに提示して、双方のエンティティが合意する態様、あるいは、それぞれの情報を双方で分担して設定し、総合した情報に関して合意に至る態様、あるいはサービスプロバイダがグループ属性証明書登録局（ＡＲＡ）を一方的に信頼した態様等が可能である。

【０１４８】

50

なお、発行委託型の場合には、新規なサービスプロバイダ（ＳＰ）が、グループ属性証明書を利用した新たなサービスを開始する場合には、属性証明書登録局（ＡＲＡ）がサービスプロバイダ（ＳＰ）自体の登録審査を行ない、その後に、上述のグループ情報共有処理を実行することになる。

【０１４９】

ステップＳ１０２のグループ情報共有処理が終了すると、サービスプロバイダ（ＳＰ）は、ステップＳ１０３において、自己の管理するグループ情報データベースについて、合意した情報に基づくデータ更新処理を実行する。図１５に示すように、グループ情報データベースには、発行者、グループ識別情報（グループＩＤ）、グループ情報の各データが格納され、これらの情報に関するデータ登録、更新を実行する。一方、属性証明書登録局（ＡＲＡ）は、ステップＳ１０４において、自己の管理する発行ポリシーテーブルについて、合意した情報に基づくデータ更新処理を実行する。図１５に示すように、発行ポリシーテーブルには、グループＩＤ、グループ情報、発行ポリシーの各データが格納され、これらの情報に関するデータ登録、更新を実行する。

【０１５０】

なお、上述した処理は、サービスプロバイダ（ＳＰ）と、属性証明書登録局（ＡＲＡ）とが、独立したエンティティとして構成されている場合に必要となる処理であり、サービスプロバイダ（ＳＰ）が、属性証明書登録局（ＡＲＡ）を兼ねている場合は、サービスプロバイダ（ＳＰ）自身が、グループ情報データベースおよび発行ポリシーテーブルの両者を保持管理することになり、上述したサービスプロバイダ（ＳＰ）と、属性証明書登録局（ＡＲＡ）間でのグループ情報共有処理は省略可能となる。

【０１５１】

また、上述した例は、グループ属性証明書の発行エンティティをグループ属性証明書登録局（ＡＲＡ）とし、グループ属性証明書の検証および検証に基づくサービス提供エンティティをサービスプロバイダ（ＳＰ）とした例を説明したが、それぞれのエンティティの組み合わせに応じて、上述の処理が実行されることになる。

【０１５２】

（３－２）グループ属性証明書発行処理

次に、グループ属性証明書発行処理について説明する。グループ属性証明書発行処理は、基本的には、属性認証局（ＡＡ）が実行することが原則である。ただし、サービスプロバイダ、ユーザデバイスにおいても独自の発行ポリシーに基づいて発行することが可能である。以下では、属性認証局（ＡＡ）によるグループ属性証明書の発行処理シーケンスについて説明する。

【０１５３】

属性証明書登録局（ＡＲＡ）が属性証明書発行要求エンティティからの発行要求を受理し、ポリシー審査等を実行して、発行可と判定した後、属性認証局（ＡＡ）に属性証明書発行要求を転送し、属性認証局（ＡＡ）の発行した属性証明書を属性証明書登録局（ＡＲＡ）を介して、発行要求エンティティに対して送付する処理構成が通常の属性証明書発行シーケンスである。

【０１５４】

図１６を参照して、ユーザデバイスであるエンドエンティティ（ＥＥ）のセキュリティチップ（ＳＣ）がグループ属性証明書の発行要求主体である場合の処理について説明する。

なお、図１６において、

ＵＩＤ：ユーザ識別デバイス（ユーザデバイス）制御部、
ＵＳＣ：ＵＩＤ内に構成されるユーザセキュリティチップ、
ＥＥ：エンドエンティティ（ユーザデバイス）制御部、
ＳＣ：ＥＥ内に構成されるセキュリティチップ、
グループＡＲＡ：グループ属性証明書登録局制御部、
グループＡＡ：グループ属性認証局制御部、
である。

【0155】

まず、ステップS111において、ユーザがエンドエンティティ（EE）の入力インタフェースを介して、グループ属性証明書（Gp・AC）の発行要求コマンドを入力する。この際、ユーザはグループ属性証明書発行に必要な属性値を入力する。属性値は、グループID、あるいはグループに属することを証明する情報等である。

【0156】

エンドエンティティ（EE）がユーザからのグループ属性証明書（Gp・AC）の発行要求の入力を受領すると、ステップS112において、エンドエンティティ（EE）は、グループAAAに対する接続要求を行ない、一方、ステップS113において、エンドエンティティ（EE）内のセキュリティチップ（SC）に対して、相互認証開始要求を出力する。

10

【0157】

ステップS114において、セキュリティチップと、グループAAA間の相互認証が実行される。これは例えば先に図13を参照して説明した公開鍵方式の相互認証処理として実行される。ステップS115では、セキュリティチップからエンドエンティティに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップS116において、エンドエンティティ（EE）は、グループAAAに対してグループ属性証明書（Gp・AC）発行要求を送信する。このグループ属性証明書（Gp・AC）発行要求には、エンドエンティティ情報、属性値（例えばグループID、グループ情報）が含まれる。

20

【0158】

エンドエンティティ（EE）からグループ属性証明書（Gp・AC）発行要求を受信したグループAAAは、ステップS117において、発行ポリシーテーブルを参照して、ポリシーに準拠したグループ属性証明書の発行が可能か否かを判定し、可であれば、ステップS118に進み、不可であれば、発行不可メッセージをエンドエンティティに通知する。

【0159】

ステップS118では、グループAAAが属性値（グループID）を伴うグループ属性証明書（Gp・AC）発行要求をグループAAに送信し、ステップS119において、グループAAが、グループIDを属性情報として格納し、電子署名を施したグループ属性証明書（図5参照）を生成し、グループAAAに送信する。

30

【0160】

ステップS120において、グループAAAが、発行されたグループ属性証明書（Gp・AC）をエンドエンティティ（EE）に送信する。エンドエンティティ（EE）は、受信したグループ属性証明書（Gp・AC）をメモリに格納する。この際、グループ属性証明書（Gp・AC）の電子署名の検証を実行して、改竄の無いことを確認した後、メモリに格納する。

【0161】

グループ属性証明書の生成時にグループAAが実行する電子署名の生成、および、グループ属性証明書の格納時にエンドエンティティが実行する電子署名の検証処理について、図17、図18を参照して説明する。

40

【0162】

署名は、データ改竄の検証を可能とするために付加されるものであり、前述のMAC値を用いることも可能であり、公開鍵暗号方式を用いた電子署名を適用することも可能である。

【0163】

まず、公開鍵暗号方式を用いた電子署名の生成方法について、図17を用いて説明する。図17に示す処理は、EC-DSEA（（Elliptic Curve Digital Signature Algorithm）、IEEE P1363/D3）を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号（Elliptic Curve Cryptosystem（以下、ECCと呼ぶ））を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外に

50

も、同様の公開鍵暗号方式における、例えばRSA暗号（（Rivest、Shamir、Adleman）など（ANSI X9.31））を用いることも可能である。

【0164】

図17の各ステップについて説明する。ステップS1において、 p を標数、 a 、 b を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ， $4a^3 + 27b^2 \neq 0 \pmod{p}$ ）、 G を楕円曲線上のベースポイント、 r を G の位数、 K_s を秘密鍵（ $0 < K_s < r$ ）とする。ステップS2において、メッセージ M のハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。

【0165】

ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD4、MD5、SHA-1などが用いられる場合もあるし、DES-CBCが用いられる場合もある。この場合は、最終出力値となるMAC（チェック値：ICVに相当する）がハッシュ値となる。

【0166】

続けて、ステップS3で、乱数 u （ $0 < u < r$ ）を生成し、ステップS4でベースポイントを u 倍した座標 $V(X_v, Y_v)$ を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

【0167】

【数1】

$P=(X_a, Y_a), Q=(X_b, Y_b), R=(X_c, Y_c)=P+Q$ とすると、

$P \neq Q$ の時（加算）、

$$X_c = \frac{Y_b - Y_a}{X_b - X_a}^2 - X_a - X_b$$

$$Y_c = \frac{Y_b - Y_a}{X_b - X_a} (X_a - X_c) - Y_a \\ = (Y_b - Y_a) / (X_b - X_a)$$

$P=Q$ の時（2倍算）、

$$X_c = \frac{3X_a^2 + a}{2Y_a} - 2X_a$$

$$Y_c = \frac{3(X_a - X_c)(X_a + X_c) + a}{2Y_a} - Y_a \\ = (3(X_a)^2 + a) / (2Y_a)$$

【0168】

これらを用いて点 G の u 倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。 G 、 $2 \times G$ 、 $4 \times G \cdots$ を計算し、 u を2進数展開して1が立っているところに対応する $2^i \times G$ （ G を i 回2倍算した値（ i は u のLSBから数えた時のビット位置））を加算する。

【0169】

ステップS5で、 $c = X_v \bmod r$ を計算し、ステップS6でこの値が0になるかどうか判定し、0でなければステップS7で $d = [(f + cK_s) / u] \bmod r$ を計算し、ステップS8で d が0であるかどうか判定し、 d が0でなければ、ステップS9で c および d を電子署名データとして出力する。仮に、 r を160ビット長の長さであると仮定すると、電子署名データは320ビット長となる。

【0170】

ステップS6において、 c が0であった場合、ステップS3に戻って新たな乱数を生成し直す。同様に、ステップS8で d が0であった場合も、ステップS3に戻って乱数を生成し直す。

【0171】

次に、公開鍵暗号方式を用いた電子署名の検証方法を、図18を用いて説明する。ステップS11で、 M をメッセージ、 p を標数、 a 、 b を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ， $4a^3 + 27b^2 \neq 0 \pmod{p}$ ）、 G を楕円曲線上のベースポイント、 r を G

10

20

30

40

50

の位数、 G および $Ks \times G$ を公開鍵 ($0 < Ks < r$) とする。ステップ S 1 2 で電子署名データ c および d が $0 < c < r$ 、 $0 < d < r$ を満たすか検証する。これを満たしていた場合、ステップ S 1 3 で、メッセージ M のハッシュ値を計算し、 $f = Hash(M)$ とする。次に、ステップ S 1 4 で $h = 1/d \bmod r$ を計算し、ステップ S 1 5 で $h_1 = f h \bmod r$ 、 $h_2 = c h$

$\bmod r$ を計算する。

【0172】

ステップ S 1 6 において、既に計算した h_1 および h_2 を用い、点 $P = (X_p, Y_p) = h_1 \times G + h_2 \cdot Ks \times G$ を計算する。電子署名検証者は、ベースポイント G および $Ks \times G$ を知っているのので、図 1 7 のステップ S 4 と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップ S 1 7 で点 P が無限遠点かどうか判定し、無限遠点でなければステップ S 1 8 に進む (実際には、無限遠点の判定はステップ S 1 6 でできてしまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、 $P + Q$ が無限遠点であることが判明している)。ステップ S 1 8 で $X_p \bmod r$ を計算し、電子署名データ c と比較する。最後に、この値が一致していた場合、ステップ S 1 9 に進み、電子署名が正しいと判定する。

【0173】

電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【0174】

ステップ S 1 2 において、電子署名データ c または d が、 $0 < c < r$ 、 $0 < d < r$ を満たさなかった場合、ステップ S 2 0 に進む。また、ステップ S 1 7 において、点 P が無限遠点であった場合もステップ S 2 0 に進む。さらにまた、ステップ S 1 8 において、 $X_p \bmod r$ の値が、電子署名データ c と一致していなかった場合にもステップ S 2 0 に進む。

【0175】

ステップ S 2 0 において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。上述したように、署名付けやハッシュをとるだけでは改竄は可能であるが、検出により実質的に改竄できないことと同様の効果がある。

【0176】

次に、図 1 9 を参照して、ユーザ識別デバイス (UID) 内のユーザセキュリティチップ (USC) 対応のグループ属性証明書を発行する手順について説明する。先に説明したように、UID は、エンドエンティティ (EE) を介して外部と通信が可能な構成であるので、属性証明書の取得処理もエンドエンティティ (EE) を介して実行される。

【0177】

ステップ S 1 3 1 ~ S 1 3 5 の処理は、図 1 6 を参照して説明したステップ S 1 1 1 ~ S 1 1 5 の処理と同様の処理であり、説明を省略する。

【0178】

ステップ S 1 3 4 におけるエンドエンティティ内のセキュリティチップ (SC) とグループ ARA 間の相互認証が成立すると、ステップ S 1 3 7 において、ユーザ識別デバイス (UID) 内のユーザセキュリティチップ (USC) と、エンドエンティティ内のセキュリティチップ (SC) との間における相互認証処理が実行される。この認証処理は、エンドエンティティ (EE) と、ユーザ識別デバイス (UID) との接続機器インタフェース 2 3 1 (図 9 参照) を介して実行される。この認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部 (図 9 参照) を中心とした処理として先に図 1 3 を参照して説明した公開鍵方式に基づく認証処理として実行可能である。ステップ S 1 3 8 において、認証の成立情報を含む認証完了通知がエンドエンティティ (EE) に通知され、認証成立を条件として次ステップに進む。

【0179】

ステップS 1 3 9では、エンドエンティティ(E E)からユーザセキュリティチップ(U S C)相互認証開始要求が出力され、ステップS 1 4 0において、U S Cと、グループA R A間の相互認証処理が実行される。ステップS 1 4 1において、認証の成立情報を含む認証完了通知がU S Cからエンドエンティティ(E E)に通知され、認証成立を条件として、エンドエンティティ(E E)は、ステップS 1 4 2において、グループA R Aに対してグループ属性証明書(G p . A C)発行要求を送信する。このグループ属性証明書(G p . A C)発行要求には、エンドエンティティ情報、属性値(例えばグループID、グループ情報)が含まれる。

【0180】

エンドエンティティ(E E)からグループ属性証明書(G p . A C)発行要求を受信したグループA R Aは、ステップS 1 4 3において、発行ポリシーテーブルを参照して、ポリシーに準拠したグループ属性証明書の発行が可能か否かを判定し、可であれば、ステップS 1 4 4に進み、不可であれば、発行不可メッセージをエンドエンティティに通知する。

【0181】

ステップS 1 4 4では、グループA R Aが属性値(グループID)を伴うグループ属性証明書(G p . A C)発行要求をグループA Aに送信し、ステップS 1 4 5において、グループA Aが、グループIDを属性情報として格納し、電子署名を施したグループ属性証明書(図5参照)を生成し、グループA R Aに送信する。

【0182】

ステップS 1 4 6において、グループA R Aが、発行されたグループ属性証明書(G p . A C)をエンドエンティティ(E E)を介してU I Dに送信する。U I Dは、受信したグループ属性証明書(G p . A C)をメモリに格納する。この際、グループ属性証明書(G p . A C)の電子署名の検証を実行して、改竄の無いことを確認した後、メモリに格納する。

【0183】

上述したように、ダイレクトにグループA R Aとの通信機能を持たないユーザ識別デバイス(U I D)がユーザセキュリティチップ(U S C)に対応するグループ属性証明書を取得するためには、エンドエンティティ(E E)を介する処理が必要となる。その際、ユーザセキュリティチップ(U S C)とグループA R Aとの間で相互に認証を行なうためには、たとえば、

- (1) E EのS CとグループA R Aとの相互認証、
- (2) E EのS CとU I DのU S Cとの相互認証、
- (3) U I DのU S CとグループA R Aとの相互認証、

のすべてが成立することが条件となる。あるいは、簡便な方式として、U I DがE Eに接続されることで、E Eは基本的にこれを受け入れる(認証したものとする)という処理構成としてもよく、この場合は、上記(2)の相互認証の省略が可能となる。さらに、上記3種の相互認証の様々な組み合わせによる認証構成が可能である。

【0184】

(3-3) グループ属性証明書利用処理

ユーザデバイス内のセキュリティチップ(S C)、あるいはユーザセキュリティチップ(U S C)に格納したグループ属性証明書を利用した処理について説明する。なお、ここでは、具体的なサービス形態については言及せず、サービス提供開始に至るまでのグループ属性証明書に基づくサービス利用権限確認処理について説明する。具体的なサービス形態については、後段の別項目において説明する。

【0185】

図20以下を参照して、ユーザデバイスとしてのエンドエンティティ(E E)内のセキュリティチップ(S C)に対して発行されたグループ属性証明書を利用したサービス利用権限確認を含むサービス開始までの処理について説明する。なお、図20において、
U I D: ユーザ識別デバイス(ユーザデバイス)制御部、
U S C: U I D内に構成されるユーザセキュリティチップ、

10

20

30

40

50

ＥＥ：エンドエンティティ（ユーザデバイス）制御部、
ＳＣ：ＥＥ内に構成されるセキュリティチップ、
ＳＰ：サービスプロバイダ制御部、
ＳＭ：ＳＰ内のセキュリティモジュール、
である。

【０１８６】

なお、ユーザデバイス（ＥＥ）のセキュリティチップ（ＳＣ）、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）、およびサービスプロバイダ（ＳＰ）のセキュリティモジュールは、例えば先に説明した図９のセキュリティチップと同様の構成を持つ。

10

【０１８７】

まず、ステップＳ１５１において、ユーザがエンドエンティティ（ＥＥ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）の利用要求コマンドを入力する。この際、ユーザは利用するグループ属性証明書に設定されたグループＩＤを指定する。ただし、特定のサービスを指定することにより唯一のグループＩＤが決定可能である場合は、サービスの指定のみとしてもよい。

【０１８８】

エンドエンティティ（ＥＥ）がユーザからのグループ属性証明書（Ｇｐ．ＡＣ）の利用要求入力を受領すると、ステップＳ１５２において、エンドエンティティ（ＥＥ）は、サービスプロバイダ（ＳＰ）に対する接続要求を行ない、一方、ステップＳ１５３において、

20

エンドエンティティ（ＥＥ）内のセキュリティチップ（ＳＣ）に対して、相互認証開始要求を出力する。

【０１８９】

ステップＳ１５４において、セキュリティチップと、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証が実行される。これは、セキュリティチップと、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）内に構成される、例えば図９に示す暗号処理部２０５を中心とした処理として、例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。

【０１９０】

ステップＳ１５５では、セキュリティチップからエンドエンティティに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ１５６において、エンドエンティティ（ＥＥ）は、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）に対して自己のメモリに格納したグループ属性証明書（Ｇｐ．ＡＣ）を送信する。なお、グループ属性証明書（Ｇｐ．ＡＣ）の送信は、サービスプロバイダ（ＳＰ）からの送信要求に応答する形で実行する構成としてもよい。また、エンドエンティティ（ＥＥ）は、グループ属性証明書（Ｇｐ．ＡＣ）の送信に併せて、グループ属性証明書（Ｇｐ．ＡＣ）の利用要求を行なう場合もある。このグループ属性証明書（Ｇｐ．ＡＣ）には、グループ識別情報（グループＩＤ）が属性値として格納されている。

30

【０１９１】

サービスプロバイダは、例えば図９に示すユーザデバイスと同様の構成を持つネットワークインタフェースを受信部として、エンドエンティティ（ＥＥ）からグループ属性証明書（Ｇｐ．ＡＣ）を受信し、セキュリティモジュール（ＳＭ）に転送する。セキュリティモジュール（ＳＭ）は、ステップＳ１５７において、グループ属性証明書検証処理を実行する。セキュリティモジュールは、先に説明したように、図９に示すユーザデバイスのセキュリティチップと同様の構成を持ち、セキュリティモジュールが、グループ属性証明書検証処理部として機能することになる。

40

【０１９２】

グループ属性証明書の検証処理の詳細について、図２１乃至図２３を参照して説明する。まず、属性証明書（ＡＣ）と公開鍵証明書（ＰＫＣ）との関連確認処理について、図２１

50

を参照して説明する。図 2 1 のフローは、属性証明書 (A C) の検証を実行する際に行なわれる属性証明書 (A C) に関連する公開鍵証明書 (P K C) の確認処理である。

【 0 1 9 3 】

確認対象の属性証明書 (A C) がセット (S 2 1) されると、属性証明書の A C 保持者の公開鍵証明書情報 (ホルダー) フィールドを抽出 (S 2 2) し、抽出した公開鍵証明書情報 (ホルダー) フィールド内に格納された公開鍵証明書の発行者情報 (P K C 発行者)、公開鍵証明書シリアル番号 (P K C シリアル) を確認 (S 2 3) し、公開鍵証明書の発行者情報 (P K C 発行者)、公開鍵証明書シリアル番号 (P K C シリアル) に基づいて公開鍵証明書 (P K C) を検索 (S 2 4) して、属性証明書 (A C) に関連付けられた公開鍵証明書 (P K C) を取得 (S 2 5) する。

10

【 0 1 9 4 】

図 2 1 に示すように、属性証明書 (A C) と公開鍵証明書 (P K C) とは、属性証明書に格納された公開鍵証明書情報 (ホルダー) フィールド内の公開鍵証明書発行者情報 (P K C 発行者)、および公開鍵証明書シリアル番号 (P K C シリアル) により関連付けがなされている。

【 0 1 9 5 】

次に、図 2 2 を参照して属性証明書 (A C) の検証処理について説明する。まず、検証対象となる属性証明書 (A C) をセット (S 5 1) し、属性証明書 (A C) 格納情報に基づいて、属性証明書 (A C) の所有者および署名者を特定 (S 5 2) する。さらに、属性証明書 (A C) の所有者の公開鍵証明書を直接あるいはリポジトリなどから取得 (S 5 3)

20

【 0 1 9 6 】

図 2 3 を参照して公開鍵証明書 (P K C) の検証処理について説明する。図 2 3 に示す公開鍵証明書 (P K C) の検証は、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位 (ル - ト C A) までの公開鍵証明書の署名検証を行なう連鎖検証処理フローである。まず、検証対象となる公開鍵証明書 (P K C) をセット (S 3 1) し、公開鍵証明書 (P K C) 格納情報に基づいて、公開鍵証明書 (P K C) 署名者を特定 (S 3 2) する。さらに、検証対象となる証明書連鎖の最上位の公開鍵証明書であるかを判定 (S 3 3) し、最上位でない場合は、最上位公開鍵証明書を直接あるいはリポジトリなどから取得 (S 3 4) する。最上位公開鍵証明書が取得されセット (S 3 5) されると、署名検証に必要な検証鍵 (公開鍵) を取得 (S 3 6) し、検証対象の署名が自己署名であるか否かを判定し (S 3 7)、自己署名でない場合は、下位 P K C をセット (S 3 9) して、上位の公開鍵証明書から取得した検証鍵 (公開鍵) に基づいて署名検証を実行 (S 4 0) する。なお、ステップ S 3 7 における自己署名判定において、自己署名の場合は自己の公開鍵を検証鍵とした検証を実行 (S 3 8) し、ステップ S 4 1 に進む。

30

【 0 1 9 7 】

署名検証に成功した場合 (S 4 1 : Y e s) は、目的とする P K C の検証が完了したか否かを判定 (S 4 2) し、完了している場合は、 P K C 検証を終了する。完了していない場合は、ステップ S 3 6 に戻り、署名検証に必要な検証鍵 (公開鍵) の取得、下位の公開鍵証明書の署名検証を繰り返し実行する。なお、署名検証に失敗した場合 (S 4 1 : N o) は、ステップ S 4 3 に進み、エラー処理、例えばその後の手続きを停止する等の処理を実行する。

40

【 0 1 9 8 】

図 2 2 に戻り、属性証明書検証処理の説明を続ける。図 2 3 で説明した公開鍵証明書の検証に失敗した場合 (S 5 5 で N o) は、ステップ S 5 6 に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合 (S 5 5 で Y e s) は、属性証明書 (A C) の署名者に対応する公開鍵証明書を直接あるいはリポジトリなどから取得 (S 5 7) して、属性証明書 (A C) の署名者に対応する公開鍵証明書の検証処理を実行 (S 5 8) する。

50

【 0 1 9 9 】

属性証明書（ＡＣ）の署名者に対応する公開鍵証明書の検証に失敗した場合（Ｓ５９でＮｏ）は、ステップＳ６０に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（Ｓ５９でＹｅｓ）は、属性証明書（ＡＣ）の署名者に対応する公開鍵証明書から公開鍵を取り出し（Ｓ６１）て、取り出した公開鍵を用いて属性証明書（ＡＣ）の署名検証処理を実行（Ｓ６２）する。署名検証に失敗した場合（Ｓ６３でＮｏ）は、ステップＳ６４に進み、エラー処理を行なう。例えばその後の処理を中止する。署名検証に成功した場合（Ｓ６３でＹｅｓ）は、属性証明書検証を終了し、その後の処理、すなわちサービス提供のために実行すべきその他の条件確認処理に移行する。

【 0 2 0 0 】

図２０のシーケンス図に戻って説明を続ける。ステップＳ１５７のグループ属性証明書（Ｇｐ．ＡＣ）の検証が上述した処理によって実行されると、セキュリティモジュール（ＳＭ）は、検証結果をサービスプロバイダ（ＳＰ）に出力し、検証不成功の場合は、エラー処理として、サービス提供を実行せず処理を中止する。この場合、グループＡＣの検証が不成立であった旨をエンドエンティティに通知する処理を実行してもよい。

【 0 2 0 1 】

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ１６１に進む。ステップＳ１６１以下の処理を図２４を参照して説明する。ステップＳ１６１では、グループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、サービスプロバイダの保有するグループ情報データベースに基づいて実行する。

【 0 2 0 2 】

グループ属性証明書（Ｇｐ．ＡＣ）の審査処理について、図２５を参照して説明する。ステップＳ１６１－１において、サービスプロバイダ（ＳＰ）は、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）から発行者情報を取得する。さらに、ステップＳ１６１－２において、属性フィールドから属性値、すなわちグループ識別情報（グループＩＤ）を取得する。

【 0 2 0 3 】

ステップＳ１６１－３において、グループ属性証明書（Ｇｐ．ＡＣ）から取得したＡＣ発行者、およびグループＩＤに基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、ステップＳ１６１－４において、グループ情報データベースからグループ情報を取得する。

【 0 2 0 4 】

図２４のシーケンス図に戻り説明を続ける。グループ属性証明書（Ｇｐ．ＡＣ）に対応するグループ情報が登録されていない場合、あるいはユーザがグループ情報に示された条件を満足していない場合は、審査不成功（Ｓ１６２：Ｎｏ）となり、ステップＳ１６３のエラー処理を実行する。例えばグループＡＣの審査不成立であり、サービス実行ができない旨のメッセージをエンドエンティティ（ＥＥ）に通知する。また、サービス提供に際して複数のグループ属性証明書の検証・審査が必要な場合は、この条件をサービス情報データベースで管理する。

【 0 2 0 5 】

なお、サービス情報データベースは、サービスを提供するにあたり、どのグループＡＣが必要であるかという情報を格納しているデータベースである。ただし、前述したグループ情報データベースとサービス情報データベースを各々個別に保有することは必須ではなく、グループ情報データベースとサービス情報データベースとを融合あるいはリンクさせたデータベース構成を持つことが可能である。すなわち、サービス提供にどのグループＡＣが必要であるかというデータを、前述のグループ情報データベース、あるいはグループ情報データベースのリンク情報から取得する構成も可能である。以下の説明において、グループ情報データベースは、サービス情報データベースとしての機能も併せ持つものとして説明する。

10

20

30

40

50

【0206】

図24のシーケンス図に戻り説明を続ける。審査成功(S162: Yes)の場合は、サービス実行のための他の条件の必要性の有無を判定する。この条件は、サービスプロバイダが任意に設定可能な条件である。さらに、ステップS165において、サービス提供のために他のグループ属性証明書が必要であるか否かを判定する。

【0207】

これは、図26に示すように、サービスを提供条件として、ユーザあるいはユーザ機器が異なる複数のグループに属することが条件とされる場合を想定したものである。例えば、図26(a)に示すように、2つの異なるグループに属することの証明により、サービスを提供するという設定ができる。

10

【0208】

具体的には、例えばユーザの居住地が特定の地域に属することを証明するグループ属性証明書A(グループA)と、ユーザ機器が特定メーカーの機器であることを示すグループ属性証明書B(グループB)との2つのグループ属性証明書の提示、検証によりサービスを提供するといった設定である。

【0209】

さらに、図26(b)に示すように、3つ以上の異なるグループに属することの証明により、サービスを提供するという設定もできる。具体的には、例えばユーザの居住地が特定の地域に属することを証明するグループ属性証明書A(グループA)と、ユーザ機器が特定メーカーの機器であることを示すグループ属性証明書B(グループB)と、さらに、ユーザの年齢が所定の範囲に属することを示すグループ属性証明書C(グループC)の3つのグループ属性証明書の提示、検証によりサービスを提供するといった設定である。

20

【0210】

このように、ユーザあるいはユーザ機器に対して発行された異なる2以上のグループ属性証明書を適用して、ユーザあるいはユーザ機器が複数の異なるグループに属していることの検証を条件としたサービス提供を行なう場合、サービスプロバイダ(SP)は、ステップS166において、エンドエンティティ(E E)に対して他のグループ属性証明書(G p . A C)の提示を要求する。他のグループ属性証明書の提示を求められたエンドエンティティ(E E)は、ステップS167において、求めに応じたグループ属性証明書をサービスプロバイダ(SP)のセキュリティモジュール(S M)に送信する。セキュリティモジュール(S M)はエンドエンティティ(E E)から受信した新たなグループ属性証明書について、図20に示すステップS157以下の処理、すなわち、グループ属性証明書の検証処理、審査処理等を実行する。

30

【0211】

サービス提供に必要なグループ属性証明書の検証、審査に成功したことを条件として、ステップS168においてサービス提供が実行される。このサービスは、サービスプロバイダの提供するコンテンツ配信、決済処理、ユーザデバイスとしての機器(例えば家電機器)のリモートコントロール、リモートメンテナンス処理、コミュニケーションサービス等、様々である。これらサービスの具体例については、後段で説明する。

【0212】

40

次に、図27、図28を参照して、ユーザデバイスとしてのユーザ識別デバイス(U I D)内のユーザセキュリティチップ(U S C)に対応して発行されたグループ属性証明書に基づくサービス提供までの処理について説明する。ユーザ識別デバイス(U I D)は個人識別デバイスとして機能する機器である。グループ属性証明書は、エンドエンティティおよびユーザ識別デバイス各々に対して個別に発行可能である。基本的には、ユーザ識別デバイスに発行されるグループ属性証明書は、ユーザ自体がある特定のグループのメンバーであるか否かの確認を可能とする証明書として発行される。U I Dは、エンドエンティティ(E E)を介して外部と通信が可能な構成であるので、属性証明書の利用処理もエンドエンティティ(E E)を介して実行される。

【0213】

50

図 27 において、ステップ S 171 ~ S 175 は、図 20 に示すステップ S 151 ~ S 155 と同様の処理、すなわち、エンドエンティティ (E E) 内のセキュリティチップ (S C) とサービスプロバイダ (S P) のセキュリティモジュール (S M) 間の相互認証を中心とした処理である。

【0214】

ステップ S 174 に示すエンドエンティティ内のセキュリティチップ (S C) とサービスプロバイダ (S P) のセキュリティモジュール (S M) 間の相互認証が成立すると、ステップ S 177 において、ユーザ識別デバイス (U I D) 内のユーザセキュリティチップ (U S C) と、エンドエンティティ内のセキュリティチップ (S C) との間における相互認証処理が実行される。この認証処理は、エンドエンティティ (E E) と、ユーザ識別デバイス (U I D) との接続機器インタフェース 231 (図 9 参照) を介して実行される。この認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部 (図 9 参照) を中心とした処理として先に図 13 を参照して説明した公開鍵方式に基づく認証処理として実行可能である。ステップ S 178 において、認証の成立情報を含む認証完了通知がエンドエンティティ (E E) に通知され、認証成立を条件として次ステップに進む。

10

【0215】

ステップ S 179 では、エンドエンティティ (E E) からユーザセキュリティチップ (U S C) に相互認証開始要求が出力され、ステップ S 180 において、U S C と、サービスプロバイダ (S P) のセキュリティモジュール (S M) 間の相互認証処理が実行される。ステップ S 181 において、認証の成立情報を含む認証完了通知が U S C からエンドエンティティ (E E) に通知され、認証成立を条件として、ユーザ識別デバイス (U I D) は、ステップ S 182 において、サービスプロバイダ (S P) のセキュリティモジュール (S M) に対してグループ属性証明書 (G p . A C) を提示する。このグループ属性証明書 (G p . A C) は、ユーザ識別デバイス (U I D) のユーザセキュリティチップ (U S C) に対応して発行されたグループ属性証明書 (G p . A C) である。

20

【0216】

ユーザセキュリティチップ (U S C) からグループ属性証明書 (G p . A C) を受信したサービスプロバイダ (S P) のセキュリティモジュール (S M) は、ステップ S 183 において、受信したグループ属性証明書の検証処理を実行する。この検証処理は、図 21 ~ 図 23 を参照して説明したと同様の処理である。以下、ステップ S 184 ~ ステップ S 198 (図 28) の処理は、図 20 および図 24 を用いて説明したエンドエンティティのセキュリティチップ (S C) 対応のグループ属性証明書に対する処理と基本的に同様であるので説明を省略する。ただし、図 28 に示すステップ S 197 では、新たなグループ属性証明書の送信は、ユーザ識別デバイス (U I D) が実行することになる。

30

【0217】

上述したように、ダイレクトにサービスプロバイダ (S P) との通信機能を持たないユーザ識別デバイス (U I D) がユーザセキュリティチップ (U S C) に対応するグループ属性証明書の利用を行なうためには、エンドエンティティ (E E) を介する処理が必要となる。その際、ユーザセキュリティチップ (U S C) とサービスプロバイダ (S P) との間で相互に認証を行なうためには、たとえば、

40

(1) E E の S C とサービスプロバイダ (S P) との相互認証、

(2) E E の S C と U I D の U S C との相互認証、

(3) U I D の U S C とサービスプロバイダ (S P) との相互認証、

のすべてが成立することが条件となる。あるいは、簡便な方式として、U I D が E E に接続されることで、E E は基本的にこれを受け入れる (認証したものとする) という処理構成としてもよく、この場合は、上記 (2) の相互認証の省略が可能となる。さらに、上記 3 種の相互認証の様々な組み合わせによる認証構成が可能である。

【0218】

なお、図 20 および図 24 では、エンドエンティティ (E E) のセキュリティチップ (S C) 対応のグループ属性証明書を利用した処理を説明し、図 27、図 28 では、ユーザ識

50

別デバイス（U I D）のユーザセキュリティチップ（U S C）に対応して発行されたグループ属性証明書を利用した処理を説明したが、エンドエンティティ（E E）のセキュリティチップ（S C）対応のグループ属性証明書と、ユーザ識別デバイス（U I D）のユーザセキュリティチップ（U S C）に対応して発行されたグループ属性証明書との双方の複数の属性証明書の検証および審査に基づいてサービスを提供する構成、例えば先に図 2 6 を参照して説明したような構成も可能である。この場合は、図 2 7、図 2 8 に示す処理と、図 2 0、図 2 4 に示す処理とを組み合わせた処理を実行することになる。

【 0 2 1 9 】

例えば、サービスプロバイダは、ユーザデバイスとしてのエンドエンティティ（機器）をグループのメンバとしたグループ定義に基づく第 1 のグループ属性証明書から取得される第 1 のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行うとともに、ユーザ識別デバイスから送付されるユーザをグループのメンバとしたグループ定義に基づく第 2 のグループ属性証明書から取得される第 2 のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行い、全てのグループ識別情報がサービス許容対象であることの判定を条件としてサービス提供可の判定処理を実行する構成が可能である。

【 0 2 2 0 】

〔（４）ユーザデバイス間におけるグループ属性証明書の発行、利用処理〕上述した説明において、グループ属性証明書は、主としてサービスプロバイダがユーザデバイスに対して提供するサービスの利用権限を確認するための証明書として適用するものとして説明した。グループ属性証明書の発行主体は、基本的には、グループ属性認証局（グループ A A）であるが、サービスプロバイダ（S P）がグループ属性認証局（グループ A A）およびグループ A R A の機能を実行し、サービスプロバイダ（S P）が独自のポリシーの下にグループ属性証明書を発行する形態も可能である。さらにユーザデバイス自身がグループ属性認証局（グループ A A）およびグループ A R A の機能を実行し、ユーザデバイスが独自のポリシーの下にグループ属性証明書を発行する形態も可能である。以下、ユーザデバイスがグループ属性証明書を発行し、ユーザデバイスに対するアクセス制限をグループ属性証明書を利用して実行する構成について説明する。

【 0 2 2 1 】

具体的な利用形態としては、例えば通信機能を有する通信処理装置としてのユーザデバイス（エンドエンティティ）が特定のメンバーからのアクセスのみを許可したい場合、特定メンバーをグループとして設定したグループ属性証明書を発行して、アクセスを要求してきた他のユーザデバイスから、その発行済みのグループ属性証明書の提示を求めて、提示されたグループ属性証明書の検証を実行して、アクセスを許可するアクセス権管理形態がある。

【 0 2 2 2 】

このサービス提供形態、すなわちアクセス許可サービスの提供形態は、サービスプロバイダ（S P）がグループ属性証明書を発行する構成も可能であるが、ユーザデバイスにおいて、例えば特定の友人、家族、同一の会社、学校等のメンバー等をグループとして設定し、設定したグループに対応するグループ識別情報として格納してグループ属性証明書を生成して発行することにより、個人ベースでのアクセス管理が可能となる。

【 0 2 2 3 】

まず、図 2 9 を参照して、ユーザデバイス間においてグループ属性証明書を発行し、格納する処理について説明する。

【 0 2 2 4 】

図 2 9 において、ユーザデバイスである通信処理装置としてのエンドエンティティ（E E）のセキュリティチップ（S C）がグループ属性証明書の発行要求主体である場合の処理について説明する。なお、図 2 9 において、

U I D：アクセス要求元ユーザ識別デバイス（ユーザデバイス）制御部、

U S C：アクセス要求元 U I D 内に構成されるユーザセキュリティチップ、

アクセス元 E E：アクセス要求元エンドエンティティ（ユーザデバイス）制御部、

ＳＣ１：アクセス要求元ＥＥ内に構成されるセキュリティチップ、
アクセス先ＥＥ：アクセス要求先エンドエンティティ（ユーザデバイス）制御部、
ＳＣ２：アクセス要求先ＥＥ内に構成されるセキュリティチップ、
である。

【０２２５】

ここでは、アクセス元ＥＥ、アクセス先ＥＥはそれぞれ異なるユーザの通信処理装置である。また、セキュリティチップ（ＳＣ１、ＳＣ２）、ユーザセキュリティチップ（ＵＳＣ）は先に説明した図９のセキュリティチップと同様の構成を持ち、セキュリティチップにおいてグループ属性証明書の検証によるアクセス権限判定処理等が実行される。

【０２２６】

すなわち、アクセス要求元デバイスからアクセス要求先に送付されたグループ属性証明書をネットワークインタフェース等の受信部で受信したアクセス要求先デバイスは、受信したグループ属性証明書をアクセス権限判定処理部としてのセキュリティチップに渡し、セキュリティチップ内で受信したグループ属性証明書に基づいて、アクセス権限判定処理が実行される。

【０２２７】

なお、図２９以下の処理シーケンス図では、アクセス権限を有することを証明するグループ属性証明書の発行処理段階からの処理手続きについて説明する。すなわち、まず、通信処理装置のセキュリティチップがグループ属性証明書生成処理を実行し、アクセス権限を有することを証明するグループ属性証明書の発行処理を行なう。その後、発行されたグループ属性証明書を通信処理装置間で送受信してアクセス権限確認を行なう処理シーケンスである。従って、通信処理装置のセキュリティチップは、グループ属性証明書の生成手段、および検証手段として機能する。

【０２２８】

図２９のシーケンス図に従って処理手順を説明する。まず、ステップＳ２０１において、アクセス要求元のユーザがエンドエンティティ（アクセス元ＥＥ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）の新規発行要求コマンドを入力する。

【０２２９】

エンドエンティティ（アクセス元ＥＥ）がユーザからのグループ属性証明書（Ｇｐ．ＡＣ）の発行要求の入力を受領すると、ステップＳ２０２において、エンドエンティティ（アクセス元ＥＥ）は、アクセス要求先のエンドエンティティ（アクセス先ＥＥ）に対する接続要求を行ない、一方、ステップＳ２０３において、アクセス元エンドエンティティ（アクセス元ＥＥ）内のセキュリティチップ（ＳＣ）に対して、相互認証開始要求を出力する。

【０２３０】

ステップＳ２０４において、アクセス要求元のユーザデバイスのセキュリティチップ（ＳＣ１）と、アクセス要求先のエンドエンティティ（アクセス先ＥＥ）に対応するセキュリティチップ（ＳＣ２）間の相互認証が実行される。これは例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ２０５では、アクセス要求元のセキュリティチップ（ＳＣ１）とユーザセキュリティチップ（ＵＳＣ）間の相互認証が実行され、ステップＳ２０６では、アクセス要求元のユーザセキュリティチップ（ＵＳＣ）と、アクセス要求先のエンドエンティティ（アクセス先ＥＥ）に対応するセキュリティチップ（ＳＣ２）間の相互認証が実行される。ステップＳ２０７では、アクセス要求元のユーザセキュリティチップ（ＵＳＣ）からエンドエンティティ（ＥＥ）に対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。

【０２３１】

なお、ステップＳ２０５～Ｓ２０７の処理は、アクセス要求元のユーザセキュリティチップ（ＵＳＣ）に対応するグループ属性証明書を発行する場合に必要な処理であり、アクセス要求元のセキュリティチップ（ＳＣ１）に対応するグループ属性証明書を発行する場合には省略可能である。

10

20

30

40

50

【 0 2 3 2 】

上記各相互認証のいずれかが不成立の場合は、処理の続行は中止される。すべての相互認証が成立すると、ステップ S 2 0 8 において、アクセス要求元のエンドエンティティ (E E) は、アクセス要求先のセキュリティチップ (S C 2) に対して、すでに保有済みのグループ属性証明書 (G p . A C) を提示して、新たなグループ属性証明書 (G p . A C) の発行要求を行なう。

【 0 2 3 3 】

ここでの処理は、アクセス要求元がすでに保有するグループ属性証明書 (G p . A C) を検証して新たな異なる定義のグループ属性証明書 (G p . A C) を発行する処理例である。すなわち新規発行のグループ属性証明書 (G p . A C) の発行ポリシーとして、既存のグループ属性証明書 (G p . A C) による属性の確認が含まれることになる。例えばユーザ本人であることの確認や、あるいは特定のメーカーの機器であることの確認を既存のグループ属性証明書 (G p . A C) に基づいて実行して、これらの確認がなされたことを条件として新規のグループ属性証明書 (G p . A C) の発行処理を行なうものである。

【 0 2 3 4 】

既存のグループ属性証明書 (G p . A C) の例としては、例えばユーザ識別デバイス (U I D) のユーザセキュリティチップ (U S C) との相互認証を行なってユーザに対応して発行されるクレジットカード会社発行のグループ属性証明書がある。また、通信処理装置としての通信端末や、 P C 等エンドエンティティ (E E) のセキュリティチップ (S C) との相互認証の結果としてエンドエンティティ (E E) に格納されるメーカーの発行するメーカー製の端末であることを証明するグループ属性証明書等がある。

【 0 2 3 5 】

アクセス要求先デバイスのセキュリティチップ (S C 2) は、アクセス要求元デバイスのエンドエンティティ (E E) から受領した既発行のグループ属性証明書を検証する。この検証処理は、先に図 2 1 ~ 図 2 3 を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。

【 0 2 3 6 】

アクセス要求先セキュリティチップ (S C 2) は、検証結果をアクセス要求元エンドエンティティ (E E) に出力し、検証不成功の場合は、エラー処理として、その後の処理を実行せず処理を中止する。この場合、エラー通知をアクセス要求元エンドエンティティ (E E) に送信する処理を行なってもよい。

【 0 2 3 7 】

グループ属性証明書 (G p . A C) の検証が成功し、グループ属性証明書 (G p . A C) の正当性が確認されるとステップ S 2 1 1 に進む。ステップ S 2 1 1 では、グループ属性証明書 (G p . A C) の審査を実行する。審査は、アクセス要求元エンドエンティティ (E E) の保有するグループ情報データベースに基づいて実行する。この審査処理は、先に図 2 5 を参照して説明した処理と同様の処理である。すなわち、検証済みのグループ属性証明書 (G p . A C) から発行者情報、グループ識別情報 (グループ I D) を取得し、取得した A C 発行者、およびグループ I D に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

【 0 2 3 8 】

グループ属性証明書 (G p . A C) に対応するグループ情報が登録されていない場合、あるいはグループ情報の条件を満たさない場合は、審査不成功となり、エラーとして処理を中止する。一方、審査成功の場合はステップ S 2 1 2 において、要求に従って、新たなグループ属性証明書の生成要求をセキュリティチップ (S C 2) に出力し、セキュリティチップ (S C 2) は、ステップ S 2 1 3 において、要求に従って、グループ属性証明書を生成して、ステップ S 2 1 4 において、アクセス先エンドエンティティ (E E) からアクセス要求元ユーザデバイスのユーザ識別デバイス (U I D) に対して新たなグループ属性証明書 (G p . A C) を発行する。

【 0 2 3 9 】

この新規発行グループ属性証明書は、例えば、アクセス要求先ユーザデバイスが会社 B のセキュアな情報を格納した P C 等の通信端末装置である場合、属性として、
「会社 B から U I D に発行された “ 会社 B の社員 ” という属性」
「会社 B から U I D に発行された “ C プロジェクトのメンバ ” という属性」
等の属性に対応するものとなる。

【 0 2 4 0 】

会社 B のセキュアな情報を格納した P C 等の通信端末装置であるアクセス要求先ユーザデバイスは、不特定のユーザデバイスからのアクセス要求時に、グループ属性証明書の提示を要求して、提示されたグループ属性証明書の検証、審査を実行してアクセスの可否を決定することが可能となる。

10

【 0 2 4 1 】

次に、図 3 0 を参照してアクセス許可情報を属性として持つグループ属性証明書の発行処理シーケンスについて説明する。図 3 0 において、ステップ S 2 2 1 ~ S 2 3 5 は、図 2 9 におけるステップ S 2 0 1 ~ S 2 1 5 に対応し、その処理も同様である。

【 0 2 4 2 】

図 3 0 では、ステップ S 2 2 8 において、アクセス要求元エンドエンティティ（アクセス元 E E ）がアクセス要求先ユーザデバイスのセキュリティチップ（ S C 2 ）に対して提示するグループ属性証明書が、「会社 B から U I D に発行された “ 会社 B の社員 ” という属性」を持つ証明書であり、アクセス要求先ユーザデバイスのセキュリティチップ（ S C 2 ）は、この属性証明書の検証、審査を実行して、新たなグループ属性証明書、すなわち、属性として、この機器（アクセス要求先ユーザデバイス）に対するアクセス可とした属性情報を持つ証明書を発行する構成である。

20

【 0 2 4 3 】

なお、この機器（アクセス要求先ユーザデバイス）に対するアクセス可としたグループ情報としての属性情報を持つ証明書を発行する条件として、「会社 B から U I D に発行された “ 会社 B の社員 ” という属性」を持つグループ属性証明書以外に、他のグループ属性証明書による証明が必要な場合は、ステップ S 2 2 8 ~ S 2 3 1 の処理を必要なグループ属性証明書の数に対応する回数繰り返し実行する。

【 0 2 4 4 】

図 3 1 を参照して、アクセス許可情報をグループ情報として持つグループ属性証明書と、他のグループ属性証明書との対応例について説明する。（ a ）は、アクセス許可情報をグループ情報として持つグループ属性証明書は、グループ に対応し、例えばこのグループ に対応するグループ属性証明書の発行条件は、グループ のメンバーであることが条件となる。例えばグループ のメンバーであることは、「会社 B から U I D に発行された “ 会社 B の社員 ” という属性」を証明するグループ属性証明書によって証明可能であり、グループ に対応するグループ属性証明書は、グループ のメンバーであることを証明するグループ属性証明書が提示され、その検証、審査が成功したことを条件として発行されることになる。

30

【 0 2 4 5 】

図 3 1 （ b ）は、アクセス許可情報をグループ情報として持つグループ属性証明書は、グループ に対応し、例えばこのグループ に対応するグループ属性証明書の発行条件は、グループ のメンバーであり、グループ のメンバーであり、グループ のメンバーであることすべての条件を満足することが条件となる。

40

【 0 2 4 6 】

具体的には、例えばユーザの居住地が特定の地域に属することを証明するグループ属性証明書（グループ ）と、ユーザ機器が特定メーカーの機器であることを示すグループ属性証明書（グループ ）と、さらに、ユーザの年齢が所定の範囲に属することを示すグループ属性証明書（グループ ）の 3 つのグループ属性証明書の提示、検証によりグループ に対応するアクセス許可情報をグループ情報として持つグループ属性証明書を発行

50

するといった設定である。

【 0 2 4 7 】

なお、アクセス要求元デバイスを構成する個人識別デバイスとしてのユーザ識別デバイスに対してグループ属性証明書を発行することにより、通信処理装置としてのエンドエンティティ（ E E ）を変更した場合であっても、個人識別デバイスとしてのユーザ識別デバイスに対して発行したグループ属性証明書に基づく審査においてアクセスを許可することが可能となり、通信処理装置（エンドエンティティ（ E E ））の変更によってアクセスが拒否されてしまうといったことを防止できる。

【 0 2 4 8 】

次に、図 3 2 を参照して、アクセス要求先ユーザデバイスが、自ら属性証明書の発行処理を実行せずに属性証明書の発行処理を他のユーザデバイスに依頼して実行する処理シーケンスについて説明する。図 3 2 において、

U I D : アクセス要求元ユーザ識別デバイス（ユーザデバイス）制御部、

U S C : アクセス要求元 U I D 内に構成されるユーザセキュリティチップ、

アクセス元 E E : アクセス要求元エンドエンティティ（ユーザデバイス）制御部、

S C 1 : アクセス要求元 E E 内に構成されるセキュリティチップ、

アクセス先 E E : アクセス要求先エンドエンティティ（ユーザデバイス）制御部、

S C 2 : アクセス要求先 E E 内に構成されるセキュリティチップ、

他 E E : 第 3 のユーザデバイス（手続き代行ユーザデバイス）

S C 3 : 他 E E のセキュリティチップ、

である。

【 0 2 4 9 】

図 3 2 において、ステップ S 2 4 1 ~ S 2 4 8 は、図 2 9 におけるステップ S 2 0 1 ~ S 2 0 8 に対応し、その処理も同様であり、説明を省略する。ステップ S 2 4 8 において、アクセス要求先ユーザデバイスのエンドエンティティ（アクセス先 E E ）は、アクセス要求元エンドエンティティ（アクセス元 E E ）から提示されたグループ属性証明書を手続き代行ユーザデバイスのセキュリティチップ（ S C 3 ）に転送し、セキュリティチップ（ S C 3 ）が転送されたグループ属性証明書の検証（ S 2 5 0 ）を実行し、手続き代行ユーザデバイスのエンドエンティティ（他 E E ）が検証結果通知（ S 2 5 1 ）に基づいて、さらに審査（ S 2 5 2 ）を実行する。

【 0 2 5 0 】

さらに、検証、審査に成功したことを条件として、グループ属性証明書の生成要求をセキュリティチップ（ S C 3 ）に出力（ S 2 5 3 ）し、セキュリティチップ（ S C 3 ）は、ステップ S 2 5 4 において、要求に従って、グループ属性証明書を生成して、ステップ S 2 5 5 において、手続き代行エンドエンティティ（他 E E ）からアクセス要求元ユーザデバイスのユーザ識別デバイス（ U I D ）に対して新たなグループ属性証明書（ G p . A C ）を発行し、ステップ S 2 5 7 においてアクセス要求元ユーザデバイスのユーザ識別デバイス（ U I D ）が受領したグループ属性証明書を格納する。

【 0 2 5 1 】

図 3 2 に示す処理シーケンスは、アクセス要求先ユーザデバイスが属性証明書の検証、審査、および発行機能を持たない場合に第 3 のデバイスにこれらの処理を委託して実行可能とした構成である。なお、手続き代行ユーザデバイスは、サービスプロバイダ（ S P ）等によって構成してもよい。

【 0 2 5 2 】

次に、アクセス許可情報をグループ情報として定義したグループ属性証明書を利用したアクセス可否判定処理を伴うサービス利用シーケンスについて、図 3 3 を参照して説明する。

【 0 2 5 3 】

まず、ステップ S 2 6 1 において、アクセス要求元のユーザがエンドエンティティ（アクセス元 E E ）の入力インタフェースを介して、グループ属性証明書（ G p . A C ）の利用

10

20

30

40

50

処理としてのアクセス要求コマンドを入力する。

【0254】

エンドエンティティ（アクセス元 E E）がユーザからの要求を受領すると、ステップ S 2 6 2 において、エンドエンティティ（アクセス元 E E）は、アクセス要求先のエンドエンティティ（アクセス先 E E）に対する接続要求を行ない、一方、ステップ S 2 6 3 において、アクセス元エンドエンティティ（アクセス元 E E）内のセキュリティチップ（S C 1）に対して、相互認証開始要求を出力する。

【0255】

ステップ S 2 6 4 において、アクセス要求元のユーザデバイスのセキュリティチップ（S C 1）と、アクセス要求先のエンドエンティティ（アクセス先 E E）に対応するセキュリティチップ（S C 2）間の相互認証が実行される。これは例えば先に図 1 3 を参照して説明した公開鍵方式の相互認証処理として実行される。ステップ S 2 6 5 では、アクセス要求元のセキュリティチップ（S C 1）とユーザセキュリティチップ（U S C）間の相互認証が実行され、ステップ S 2 6 6 では、アクセス要求元のユーザセキュリティチップ（U S C）と、アクセス要求先のエンドエンティティ（アクセス先 E E）に対応するセキュリティチップ（S C 2）間の相互認証が実行される。ステップ S 2 6 7 では、アクセス要求元のユーザセキュリティチップ（U S C）からエンドエンティティ（E E）に対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。

【0256】

なお、ステップ S 2 6 5 ~ S 2 6 7 の処理は、アクセス要求元のユーザセキュリティチップ（U S C）に対応するグループ属性証明書を利用した処理の場合に必要な処理であり、アクセス要求元のセキュリティチップ（S C 1）に対応するグループ属性証明書を利用した処理の場合には省略可能である。

【0257】

上記各相互認証のいずれかが不成立の場合は、処理の続行は中止される。すべての相互認証が成立すると、ステップ S 2 6 8 において、アクセス要求元のエンドエンティティ（E E）は、アクセス要求先のセキュリティチップ（S C 2）に対して、グループ属性証明書（G p . A C）を提示して、アクセス許可を要求する。

【0258】

アクセス要求先のセキュリティチップ（S C 2）は、アクセス要求元のエンドエンティティ（E E）から受領したグループ属性証明書を検証（S 2 6 9）する。この検証処理は、先に図 2 1 ~ 図 2 3 を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。

【0259】

アクセス要求先セキュリティチップ（S C 2）は、検証結果をアクセス要求先エンドエンティティ（E E）に出力（S 2 7 0）し、検証不成功の場合は、エラー処理として、その後の処理を実行せず処理を中止する。この場合、エラー通知をアクセス要求元エンドエンティティ（E E）に送信する処理を行なってもよい。

【0260】

グループ属性証明書（G p . A C）の検証が成功し、グループ属性証明書（G p . A C）の正当性が確認されるとステップ S 2 7 1 に進む。ステップ S 2 7 1 では、グループ属性証明書（G p . A C）の審査を実行する。審査は、アクセス要求先エンドエンティティ（E E）の保有するグループ情報データベースに基づいて実行する。この審査処理は、先に図 2 5 を参照して説明した処理と同様の処理である。すなわち、検証済みのグループ属性証明書（G p . A C）から発行者情報、グループ I D を取得し、取得した A C 発行者、およびグループ I D に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。グループ情報には、例えば「この機器にアクセス可」、あるいは「データ読み出しのみ可」等の情報が含まれ、これらの情報に従ってサービスが提供される。

10

20

30

40

50

【 0 2 6 1 】

グループ属性証明書（ G p . A C ）に対応するグループ情報が登録されていない場合、あるいはグループ情報の条件を満足しない場合は、審査不成功となり、エラーとして処理を中止する。一方、審査成功の場合はステップ S 2 7 2 において、サービス提供、すなわち、グループ情報として登録されたサービス、例えば機器に対するアクセスを許可する。

【 0 2 6 2 】

〔（ 5 ）グループ属性証明書の具体的利用例〕

次に、グループ属性証明書の具体的利用例について説明する。以下、利用形態を、

（ 5 - 1 ）コンテンツ配信サービス

（ 5 - 2 ）リモートコントロールサービス

（ 5 - 3 ）リモートメンテナンスサービス

（ 5 - 4 ）パーソナルコミュニケーションサービス

以上の各利用形態について各々説明する。

【 0 2 6 3 】

上記の各サービスにおいて利用されるグループ属性証明書の例を図 3 4 に示す。図 3 4 には、グループ属性証明書の発行者、発行タイミング、所有者、検証者、属性を対応付けて示してある。発行者は、前述したように、グループ属性証明書の発行処理のみを実行するグループ A R A の他、サービスプロバイダ、ユーザデバイス等、様々な発行主体が可能であり、サービスプロバイダとしては、例えばクレジットカードを発行する「カード会社 A」、所定の組織、例えば「会社 B」、「役所」、さらにユーザ個人としての「甲さん」、さらに P C、通信端末、ゲーム機等のエンドエンティティ（ E E ）を製造する「 E E メーカー C」等がある。

【 0 2 6 4 】

グループ属性証明書の発行タイミングは、任意のタイミング、 P C、通信端末、ゲーム機等のエンドエンティティ（ E E ）の購入時、製造時、購入後等、証明書に基づいて提供するサービスに応じて、様々な設定が可能である。

【 0 2 6 5 】

グループ属性証明書の所有者は、所定のグループのメンバとしてのユーザ、あるいはユーザ機器であり、ユーザ、例えば「甲さん」を所有者として発行されるグループ属性証明書は、甲さんのユーザ識別デバイス（ U I D ）のユーザセキュリティチップ（ U S C ）を対象としてユーザセキュリティチップ（ U S C ）の認証に基づいて発行され、例えばある家族の各メンバに提供されるグループ属性証明書は、家族各々のユーザ識別デバイス（ U I D ）のユーザセキュリティチップ（ U S C ）を対象としてユーザセキュリティチップ（ U S C ）の認証に基づいて発行され、また、 P C、通信端末、ゲーム機等のユーザ機器、すなわちエンドエンティティ（ E E ）を対象として提供されるグループ属性証明書は、エンドエンティティ（ E E ）のセキュリティチップ（ S C ）を対象としてユーザセキュリティチップ（ U S C ）の認証に基づいて発行される。

【 0 2 6 6 】

これらのグループ属性証明書の検証処理の実行者は、グループ属性証明書によって証明される属性に基づいてサービスを提供するサービスプロバイダ（ S P ）のセキュリティモジュール（ S M ）、あるいは図には示されていないが、ユーザデバイスのセキュリティチップ（ S C , U S C ）である。

【 0 2 6 7 】

各グループ属性証明書の証明する所有者属性は、例えば「カード会社 A 会員」、「会社 B の社員」、「甲さんの家族」、「登録されたユーザ」、「登録されたユーザデバイス」、「属性証明書発行者の所有機器（ E E ）」、「甲さんの所有機器（ E E ）」等であり、グループ属性証明書の検証、審査により、グループ属性証明書の提示ユーザまたは提示機器について、上記の各属性が証明されることになる。サービスプロバイダ等の属性証明書検証者は、証明された所有者属性に基づいて所定のサービスを提供する。

【 0 2 6 8 】

(5 - 1) コンテンツ配信サービス

まず、グループ属性証明書を利用したコンテンツ配信サービスについて説明する。コンテンツ配信におけるコンテンツの利用権限について、グループ属性証明書を適用して確認する態様としては、様々な態様がある。

【 0 2 6 9 】

まず、一例として、クレジットカード会社の発行するクレジットカード会員であることを証明する第 1 のグループ属性証明書 A に基づいて、コンテンツの利用許可情報をグループ情報として含むコンテンツ配信サービス主体であるコンテンツ配信サービスプロバイダの発行する第 2 のグループ属性証明書 B の発行を行ない、この第 2 のグループ属性証明書 B を適用してコンテンツ利用権限の確認を実行してコンテンツ配信サービスを実行する処理例について説明する。

10

【 0 2 7 0 】

図 3 5 を参照して、ユーザデバイスが、クレジットカード会員であることを証明する第 1 のグループ属性証明書 A に基づいて、コンテンツの利用許可情報をグループ情報として含む第 2 のグループ属性証明書 B を発行する処理について説明する。

【 0 2 7 1 】

図 3 5 の例においては、ユーザ識別デバイス (U I D) のユーザセキュリティチップ (U S C) を対象として発行したクレジットカード会員であることを証明する第 1 のグループ属性証明書 A をグループ属性証明書登録局 (G p . A R A) に提示して、グループ属性認証局 (G p . A A) からコンテンツ配信サービスプロバイダが発行主体である第 2 のグループ属性証明書 B の発行処理例である。ここでは、コンテンツ配信サービスプロバイダは、グループ属性証明書登録局 (G p . A R A) と、グループ属性証明書発行ポリシーについて合意しているものとする。

20

【 0 2 7 2 】

図 3 5 において、

U I D : ユーザ識別デバイス (ユーザデバイス) 制御部、
U S C : U I D 内に構成されるユーザセキュリティチップ、
E E : エンドエンティティ (ユーザデバイス) 制御部、
S C : E E 内に構成されるセキュリティチップ、
グループ A R A : グループ属性証明書登録局制御部、
グループ A A : グループ属性認証局制御部、
である。

30

【 0 2 7 3 】

まず、ステップ S 3 0 1 において、ユーザがエンドエンティティ (E E) の入力インタフェースを介して、グループ属性証明書 (G p . A C) の発行要求コマンドを入力する。この際、ユーザはグループ属性証明書発行に必要な属性値を入力する。属性値は、グループ I D 、あるいはグループに属することを証明する情報等である。

【 0 2 7 4 】

エンドエンティティ (E E) がユーザからのグループ属性証明書 (G p . A C) の発行要求の入力を受領すると、ステップ S 3 0 2 において、ユーザセキュリティチップ (U S C) と、グループ A R A 間の相互認証が実行される。なお、ここでは省略して示してあるが、ダイレクトにグループ A R A との通信機能を持たないユーザ識別デバイス (U I D) の場合は、

40

- (1) E E の S C とグループ A R A との相互認証、
- (2) E E の S C と U I D の U S C との相互認証、
- (3) U I D の U S C とグループ A R A との相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、U I D が E E に接続されることで、E E は基本的にこれを受け入れる (認証したものとする) という処理構成としてもよく、この場合は、上記 (2) の相互認証の省略が可能となる。さらに、上記 3 種の相互認証の様々な組み合わせによる認証構成が可能である。

50

【 0 2 7 5 】

認証処理は、各デバイスのセキュリティチップの暗号処理部（図 9 参照）における暗号処理を主とした処理によって実行され、例えば先に図 1 3 を参照して説明した公開鍵方式の相互認証処理として実行される。ステップ S 3 0 3 では、ユーザセキュリティチップ（U S C）からエンドエンティティに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップ S 3 0 4 において、エンドエンティティ（E E）は、グループ A R A に対してグループ属性証明書（G p . A C）発行要求を送信する。このグループ属性証明書（G p . A C）発行要求には、エンドエンティティ情報、属性値（例えばグループ I D、グループ情報）が含まれ、さらに、コンテンツ配信サービスプロバイダが発行主体である第 2 のグループ属性証明書 B の発行条件として提示すべき、クレジットカード会員であることを証明する第 1 のグループ属性証明書 A が含まれる。

10

【 0 2 7 6 】

エンドエンティティ（E E）からグループ属性証明書（G p . A C）発行要求を受信したグループ A R A は、クレジットカード会員であることを証明する第 1 のグループ属性証明書 A の検証の後、ステップ S 3 0 5 において、発行ポリシーテーブルを参照して、ポリシーに準拠したグループ属性証明書の発行が可能か否かを判定し、可であれば、ステップ S 3 0 6 に進み、不可であれば、発行不可メッセージをエンドエンティティに通知する。

【 0 2 7 7 】

ステップ S 3 0 6 では、グループ A R A が属性値（グループ I D）を伴うグループ属性証明書（G p . A C）発行要求をグループ A A に送信し、ステップ S 3 0 7 において、グループ A A が、グループ I D を属性情報として格納し、電子署名を施したグループ属性証明書、すなわち、コンテンツの利用許可情報をグループ情報として含む第 2 のグループ属性証明書 B を生成し、グループ A R A に送信する。

20

【 0 2 7 8 】

ステップ S 3 0 8 において、グループ A R A が、発行されたグループ属性証明書 B（G p . A C）をユーザ識別デバイス（U I D）に送信する。ユーザ識別デバイス（U I D）は、受信したグループ属性証明書（G p . A C）をメモリに格納する。この際、グループ属性証明書（G p . A C）の電子署名の検証を実行して、改竄の無いことを確認した後、メモリに格納する。

30

【 0 2 7 9 】

次に、図 3 6 を参照して、上述の処理によって発行されたグループ属性証明書 B、すなわちコンテンツの利用許可情報をグループ情報として含む第 2 のグループ属性証明書 B をサービスプロバイダに提示して、コンテンツ利用権限のあることの確認を行なって、サービス提供、すなわちコンテンツ配信サービスを受領する処理について説明する。図 3 6 において、

U I D：ユーザ識別デバイス（ユーザデバイス）制御部、
 U S C：U I D 内に構成されるユーザセキュリティチップ、
 E E：エンドエンティティ（ユーザデバイス）制御部、
 S C：E E 内に構成されるセキュリティチップ、
 S P：サービスプロバイダ制御部、
 S M：S P 内のセキュリティモジュール、
 である。

40

【 0 2 8 0 】

セキュリティチップ（S C）、ユーザセキュリティチップ（U S C）、セキュリティモジュール（S M）は先に説明した図 9 のセキュリティチップと同様の構成を持ち、セキュリティチップにおいてグループ属性証明書の検証による権限判定処理等が実行される。すなわち、サービス要求元デバイスからサービス要求先に送付されたグループ属性証明書をネットワークインタフェース等の受信部で受信したサービスプロバイダは、受信したグループ属性証明書を権限判定処理部としてのセキュリティモジュール（チップ）に渡し、セキ

50

セキュリティモジュール（チップ）内で受信したグループ属性証明書に基づいて、権限判定処理が実行される。

【0281】

まず、ステップS311において、ユーザがエンドエンティティ（EE）の入力インタフェースを介して、グループ属性証明書（Gp・AC）の利用要求コマンドを入力する。この際、ユーザは利用するグループ属性証明書に設定されたグループIDを指定する。ただし、特定のサービスを指定することにより唯一のグループIDが決定可能である場合は、サービスの指定のみとしてもよい。

【0282】

エンドエンティティ（EE）がユーザからのグループ属性証明書（Gp・AC）の利用要求入力を受領すると、ステップS312において、ユーザセキュリティチップ（USC）と、サービスプロバイダのセキュリティモジュール（SM）間の相互認証が実行される。なお、ここでは省略して示してあるが、ダイレクトにSPとの通信を実行できないユーザ識別デバイス（UID）の場合は、

- （1）EEのSCとSP-SMとの相互認証、
- （2）EEのSCとUIDのUSCとの相互認証、
- （3）UIDのUSCとSP-SMとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、UIDがEEに接続されることで、EEは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（2）の相互認証の省略が可能となる。さらに、上記3種の相互認証の様々な組み合わせによる認証構成が可能である。

【0283】

認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部を中心として先に図13を参照して説明した公開鍵方式の相互認証処理として実行される。ステップS313では、セキュリティチップからエンドエンティティに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップS314において、ユーザセキュリティチップ（USC）は、サービスプロバイダ（SP）のセキュリティモジュール（SM）に対して自己のメモリに格納したグループ属性証明書（Gp・AC）を送信する。このグループ属性証明書（Gp・AC）は、先に図35を参照して説明した処理により取得したコンテンツの利用許可情報をグループ情報として含む第2のグループ属性証明書Bである。

【0284】

ユーザセキュリティチップ（USC）からグループ属性証明書（Gp・AC）を受信したセキュリティモジュール（SM）は、ステップS315において、グループ属性証明書検証処理を実行する。グループ属性証明書の検証処理については、先に図21乃至図23を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（PKC）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

【0285】

グループ属性証明書（Gp・AC）の検証処理後、セキュリティモジュール（SM）は、検証結果をサービスプロバイダ（SP）に出力し、検証不成立の場合は、エラー処理として、サービス提供を実行せず処理を中止する。この場合、グループACの検証が不成立であった旨をエンドエンティティ通知する処理を実行してもよい。

【0286】

グループ属性証明書（Gp・AC）の検証が成功し、グループ属性証明書（Gp・AC）の正当性が確認されるとステップS317に進む。ステップS317では、先に図25を参照して説明したグループ属性証明書（Gp・AC）の審査を実行する。審査は、サービスプロバイダの保有するグループ情報データベースに基づいて実行する。すなわち、サービスプロバイダ（SP）は、検証済みのグループ属性証明書（Gp・AC）から発行者情報、グループIDを取得し、取得情報に基づいて、グループ情報データベースを検索し、

登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

【0287】

この場合のグループ情報は、コンテンツの利用許可情報をグループ情報、例えばコンテンツとしてのゲームXを3ヶ月利用可能とする情報等である。サービスプロバイダ（SP）は、ステップS318において、サービス提供処理、すなわち、グループ情報に従って、3ヶ月の利用期間を設定したゲームプログラムをユーザデバイスのエンドエンティティ（EE）に対して配信する。

【0288】

上述したコンテンツ配信サービス処理は、1つのグループ属性証明書によってコンテンツ利用権の確認を行なう例であったが、次に、異なるグループ属性を証明する複数の異なる属性証明書を適用してユーザあるいはユーザ機器のコンテンツ利用権を確認してサービスを提供する処理例について説明する。

【0289】

図37に本処理例で適用する複数のグループ属性証明書を示す。グループ属性証明書（Gp・AC）AC01は、A大学によって発行され、A大学の学生であることを証明する学生証であり、C君のユーザ識別デバイス（UID）のユーザセキュリティチップ（USC）との認証に基づいて発行されたグループ属性証明書（Gp・AC）である。グループ属性証明書（Gp・AC）AC02は、A大学によって発行され、美術講座の受講権利を有することを証明する美術講座受講証であり、C君のユーザ識別デバイス（UID）のユーザセキュリティチップ（USC）との認証に基づいて発行されたグループ属性証明書（Gp・AC）である。

【0290】

グループ属性証明書（Gp・AC）AC03は、A大学によって発行され、A大学の管理する機器であることを証明する管理機器証明書であり、エンドエンティティ（EE）としてのテレビDのセキュリティチップ（SC）との認証に基づいて発行されたグループ属性証明書（Gp・AC）である。グループ属性証明書（Gp・AC）AC04は、文部科学省によって発行され、教育使用目的の機器であることを証明する教育用機器証明書であり、エンドエンティティ（EE）としてのテレビDのセキュリティチップ（SC）との認証に基づいて発行されたグループ属性証明書（Gp・AC）である。

【0291】

これらAC01～AC04の4種類の異なるグループ属性証明書を適用したコンテンツ利用権限確認および、サービス提供処理について図38を参照して説明する。

【0292】

図38は、ユーザデバイス側処理を左に、サービスプロバイダ側処理を右側に示している。なお、ユーザデバイスは、エンドエンティティ（EE）、EE内に構成されるセキュリティチップ（SC）、ユーザ識別デバイス（UID）、UID内に構成されるユーザセキュリティチップ（USC）を含む。

【0293】

ステップS321、S331において、ユーザデバイスと、サービスプロバイダ間の相互認証処理が実行される。なお、相互認証は、提示するグループ属性証明書の発行対象機に応じて実行し、EEのSCとSP-SMとの相互認証、あるいは、UIDのUSCとSP-SMとの相互認証のいずれか、あるいはその双方が実行される。

【0294】

本例の場合は、図37に示す4つのグループ属性証明书中AC01、AC02は、C君のユーザ識別デバイス（UID）のユーザセキュリティチップ（USC）を対象として発行されたものであり、AC03、AC04は、エンドエンティティ（EE）としてのテレビDに構成されるセキュリティチップ（SC）に対して発行されているものである。処理としては、C君のユーザ識別デバイス（UID）をエンドエンティティ（EE）としてのテレビDに接続機器インタフェース231（図9参照）を介して接続し、エンドエンテ

10

20

30

40

50

ィテイ（E E）としてのテレビDのネットワークインタフェース232（図9参照）を介してサービスプロバイダ（S P）のセキュリティモジュール（S M）と接続し、E EのS CとS P - S Mとの相互認証、および、U I DのU S CとS P - S Mとの相互認証の双方を実行する。

【0295】

認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部を中心とした処理として例えば先に図13を参照して説明した公開鍵方式の相互認証処理として実行される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップS322において、ユーザデバイスは、サービスプロバイダ（S P）のセキュリティモジュール（S M）に対して自己のメモリに格納した複数のグループ属性証明書（G p . A C）A C 01～A C 04を送信する。このグループ属性証明書（G p . A C）A C 01～A C 04は、図37に示す4種類のグループ属性証明書である。

10

【0296】

なお、サービス提供にあたり、必要となるグループ属性証明書の組み合わせデータは、サービスプロバイダ側からユーザ側に通知する構成としてもよい。サービスプロバイダは、例えば図39に示すサービス提供条件として設定されるグループ属性証明書の組み合わせテーブルデータを保有する。図39に示す例では、例えばサービスとしてコンテンツBの視聴のためには、A大学発行の学生証としてのグループ属性証明書、文部科学省発行の教育用機器証明書としてのグループ属性証明書等が必要であることを示すデータが格納され、このテーブルを適用して、必要となるグループ属性証明書の提示をユーザデバイスに対して通知する。

20

【0297】

ステップS332において、ユーザデバイスから本例におけるサービス提供に必要な4種類のグループ属性証明書（G p . A C）A C 01～A C 04を受信したセキュリティモジュール（S M）は、ステップS333において、複数のグループ属性証明書から、順次1つのグループ属性証明書を選択し、検証処理を実行する。グループ属性証明書の検証処理については、先に図21乃至図23を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（P K C）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

【0298】

グループ属性証明書（G p . A C）の検証処理後、検証不成立（S334：N o）の場合は、エラー処理（S339）として、サービス提供を実行せず処理を中止する。この場合、グループA Cの検証が不成立であった旨をエンドエンティティ通知する処理を実行してもよい。

30

【0299】

グループ属性証明書（G p . A C）の検証が成立（S334：Y e s）し、グループ属性証明書（G p . A C）の正当性が確認されるとステップS335に進む。ステップS335では、先に図25を参照して説明したグループ属性証明書（G p . A C）の審査を実行する。審査は、サービスプロバイダの保有するグループ情報データベースに基づいて実行する。すなわち、サービスプロバイダ（S P）は、検証済みのグループ属性証明書（G p . A C）から発行者情報、グループI Dを取得し、取得情報に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。この場合のグループ情報は、コンテンツの配信許可情報を含む情報である。

40

【0300】

グループ属性証明書の審査が不成立（S336：N o）の場合、例えば、グループ情報の取得に失敗した場合は、エラー処理（S339）として、サービス提供を実行せず処理を中止する。この場合、グループA Cの検証が不成立であった旨をエンドエンティティ通知する処理を実行してもよい。

【0301】

50

グループ属性証明書の審査が成立 (S 3 3 6 : Y e s) した場合、ステップ S 3 3 7 に進み、提示されたグループ属性証明書の全ての検証、審査が終了したか否かを判定し、未終了分がある場合は、ステップ S 3 3 3 以下の検証、審査処理を未終了分のグループ属性証明書について実行する。

【 0 3 0 2 】

ステップ S 3 3 7 において、提示されたグループ属性証明書の全ての検証、審査が終了したと判定した場合は、ステップ S 3 3 8 において、サービス提供を実行し、ユーザデバイスにおいてステップ S 3 4 0 のサービス受領を実行する。具体的には、エンドエンティティとしてのテレビ D (図 3 7 参照) において、ユーザ C 君が配信コンテンツの視聴を可能となる。

10

【 0 3 0 3 】

上述した複数のグループ属性証明書を適用した利用権限確認処理を模式図で示すと、図 4 0 のように示される。すなわち、4 種類の異なる属性を定義したグループ属性証明書の定義領域が、図 4 0 に示すグループ A C 0 1 ~ A C 0 4 によって示されるとき、上述したコンテンツの利用権限が認められるためには、(a) に示すように、ユーザのグループ属性としての学生証 (グループ属性証明書 (A C 0 1)) と美術講座受講証 (A C 0 2) の両グループに属していること、および利用機器のグループ属性として、(b) に示すように、機器のグループ属性として、管理機器証明書と、教育機器証明書を保有する機器であることの両条件を満足することが必要となる。

20

【 0 3 0 4 】

(a) に示すユーザのグループ属性としての学生証 (グループ属性証明書 (A C 0 1)) と美術講座受講証 (A C 0 2) の両グループに属していることの証明は、ユーザ識別デバイス (U I D) のユーザセキュリティチップ (U S C) 対応のグループ属性証明書の検証、審査によって確認され、(b) に示す機器のグループ属性としての管理機器証明書と、教育機器証明書を保有する機器であることの証明はエンドエンティティ (E E) のセキュリティチップ (S C) 対応のグループ属性証明書の検証、審査によって確認される。

【 0 3 0 5 】

なお、図 3 9 を参照して説明したフローにおいては、4 つのグループ属性証明書の検証、審査が成功したことを条件としてサービスを提供する処理としたが、4 つのグループ属性証明書の検証、審査が成功したことを条件としてサービスを実行するのではなく、サービス提供を認める新たなグループ属性証明書を発行する処理を行ない、ユーザが新たにこの 1 つの新規発行のグループ属性証明書を提示し、その検証を実行することによりサービスの提供を受けることが可能となる。

30

【 0 3 0 6 】

ただし、この場合、この新規発行されたグループ属性証明書は、ユーザグループおよび機器グループの両グループを定義するものとなり、グループ定義に合致するユーザ識別デバイス (U I D) をグループ定義に合致する機器 (E E) に設定し、U I D のセキュリティチップ (U S C) とサービスプロバイダ (S P) のセキュリティモジュール (S M) との相互認証により、U I D のセキュリティチップ (U S C) 認証が成立し、さらに、エンドエンティティ (E E) のセキュリティチップ (S C) とサービスプロバイダ (S P) のセキュリティモジュール (S M) との相互認証によりセキュリティチップ (S C) の認証が成立し、さらに、上述の新規発行グループ属性証明書の検証、審査が成立することがサービス利用条件となる。

40

【 0 3 0 7 】

(5 - 2) リモートコントロールサービス
次に、グループ属性証明書に基づく、データ処理システム構成の一例として権限確認を実行してエンドエンティティ (E E) としての機器のリモートコントロールを実行するサービス利用例について説明する。

【 0 3 0 8 】

ここでは、医療機器をエンドエンティティ (E E) として、自宅等に設置した医療機器と

50

、サービスプロバイダとしての病院側の医療機器（ＳＰ）との間で通信を実行して、病院側の医療機器（ＳＰ）から送信する命令に基づいて、自宅設置の医療機器（ＥＥ）によりユーザの医療診断、検査等を実行し、検査データ等の取得情報を自宅設置の医療機器（ＥＥ）から病院側の医療機器（ＳＰ）に送信する医療処理例について説明する。

【０３０９】

上述の医療処理を実行するデータ処理システムにおける各処理の実行の際、それぞれグループ属性証明書の検証、審査に基づいて処理の実行可否を確認する処理が行なわれ、実行可否確認の後、医療処理手続きに係る様々なデータ処理が実行される。適用するグループ属性証明書の例を図４１に示す。

【０３１０】

グループ属性証明書ＡＣ０１は、発行者が、サービスプロバイダ（ＳＰ）としての病院側医療機器であり、所有者、すなわちグループ属性証明書ＡＣ０１の発行時に発行者である病院側医療機器（ＳＰ）と認証処理を行なうことによりグループ属性証明書の発行対象となった所有者は、自宅側医療機器（ＥＥ）によって医療サービスを受けるユーザ甲さんのユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）である。あるいは自宅側医療機器（ＥＥ）のセキュリティチップ（ＳＣ）であってもよい。

【０３１１】

このグループ属性証明書ＡＣ０１は、医療プログラムの実行可否を判定する確認処理の際に適用され、所有者であるユーザデバイスのＵＳＣあるいはＳＣから病院側医療機器（ＳＰ）に送付されて、病院側医療機器（ＳＰ）において、グループ属性証明書ＡＣ０１の検証、審査の後、サービス、すなわち医療診断プログラムの実行が許可される。

【０３１２】

グループ属性証明書ＡＣ０２は、発行者が、自宅側医療機器（ＥＥ）であり、所有者、すなわちグループ属性証明書ＡＣ０２の発行時に発行者である自宅側医療機器（ＥＥ）と認証処理を行なうことによりグループ属性証明書の発行対象となった所有者は、サービスプロバイダ（ＳＰ）としての病院側医療機器のセキュリティモジュール（ＳＭ）である。

【０３１３】

このグループ属性証明書ＡＣ０２は、医療プログラムの実行によって診断対象者（甲さん）から取得し、診断データ、例えば血圧値、脈拍、採血データ等の診断データを、自宅側医療機器（ＥＥ）から病院側医療機器（ＳＰ）に対して送信する処理の実行可否判定処理に適用される。

【０３１４】

このグループ属性証明書ＡＣ０２は、病院側医療機器（ＳＰ）から自宅側医療機器（ＥＥ）に送付されて、自宅側医療機器（ＥＥ）において、グループ属性証明書ＡＣ０２の検証、審査の後、サービス、すなわち医療診断結果データの送付処理が実行される。

【０３１５】

なお、グループ属性証明書ＡＣ０１、ＡＣ０２の発行処理は、病院側医療機器（ＳＰ）あるいは自宅側医療機器（ＥＥ）、あるいはユーザ識別デバイス（ＵＩＤ）自体が、グループ属性認証局（グループＡＡ）およびグループ属性証明書登録局（グループＡＲＡ）の機能を実行して、みずから発行することが可能であるが、グループ属性認証局（グループＡＡ）およびグループ属性証明書登録局（グループＡＲＡ）に依頼して発行処理を行なう構成も可能である。ただし、この場合には発行者のポリシーに従った処理が実行されることが条件である。

【０３１６】

例えばグループ属性証明書ＡＣ０１の発行処理は、発行者である病院側医療機器（ＳＰ）あるいは、発行代理を行なうグループ属性証明書登録局（グループＡＲＡ）が、医療診断対象者としての甲さんから、甲さんであることを証明する既発行のグループ属性証明書、例えばクレジットカード会社の発行したグループ属性証明書を提示させ、その提出されたグループ属性証明書の検証を実行した後、新たなグループ属性証明書ＡＣ０１の発行処理を行なう方法をとることが好ましい。このような既発行のグループ属性証明書の検証を条

10

20

30

40

50

件として、新たなグループ属性証明書を発行する処理シーケンスは、先に図 29、図 30、図 32 等を参照して説明した処理シーケンスと同様となる。

【0317】

また、グループ属性証明書 AC02 の発行処理においても、同様に、発行者である自宅側医療機器 (EE) あるいは、発行代理を行なうグループ属性証明書登録局 (グループ ARA) が、病院側医療機器 (SP) から、病院側医療機器 (SP) であることを証明する既発行のグループ属性証明書、例えばメーカーあるいは公の管理組織が発行したグループ属性証明書を提示させて、その提出されたグループ属性証明書の検証を実行した後、グループ属性証明書 AC02 の発行処理を行なう方法をとることが好ましい。

【0318】

医療処理を行なうリモートコントロールのシステムにおいて、各機器に格納される属性証明書は、図 42 に示す通りとなる。サービスプロバイダとしての病院側医療機器 (SP) 401 と、エンドエンティティとしての自宅側医療機器 (EE) 411 は通信ネットワークにより相互にデータ転送可能であり、自宅側医療機器 (EE) 411 と、ユーザ識別デバイス (UID) 421 は、双方の接続機器インタフェース 231 (図 9 参照) を介して相互にデータ転送が可能である。

【0319】

それぞれの機器には、耐タンパ構成を持つ (ユーザ) セキュリティチップ 412, 423 またはセキュリティモジュール 403 が備えられ、データ通信処理の際の相互認証処理、あるいは転送データの暗号化、復号処理等を実行する。またグループ属性証明書の検証処理も (ユーザ) セキュリティチップ 412, 423 またはセキュリティモジュールにおいて実行される。

【0320】

ユーザ識別デバイス 421 には、先に図 41 を参照して説明したグループ属性証明書 AC01, 422 が格納される。グループ属性証明書 AC01, 422 は、発行者が、サービスプロバイダとしての病院側医療機器 (SP) 401 であり、医療プログラムの実行可否を判定する確認処理の際に適用され、所有者であるユーザデバイスの USC421 から病院側医療機器 (SP) 401 に送付されて、病院側医療機器 (SP) 401 のセキュリティモジュール (SM) 403 において、グループ属性証明書 AC01 の検証、審査の後、サービス、すなわち医療診断プログラムが実行される。

【0321】

また、サービスプロバイダとしての病院側医療機器 (SP) 401 には、グループ属性証明書 AC02, 402 が格納される。グループ属性証明書 AC02, 402 は、発行者が、自宅側医療機器 (EE) 411 であり、所有者が病院側医療機器 (SP) 401 であり、病院側医療機器 (SP) から自宅側医療機器 (EE) に送付され、診断対象者 (甲さん) から取得した診断データを、自宅側医療機器 (EE) 411 から病院側医療機器 (SP) 401 に対する送信処理の前に、自宅側医療機器 (EE) 411 のセキュリティチップ (SC) 412 においてグループ属性証明書 AC02, 402 の検証、審査が実行され、検証、審査成立を条件として診断結果データの送信が実行される。

【0322】

図 43 を参照して、ユーザ識別デバイス 421 に格納されたグループ属性証明書 AC01, 422 を適用して医療診断プログラムの実行サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する。図 43 において、

UID: ユーザ識別デバイス (ユーザデバイス) 制御部、
USC: UID 内に構成されるユーザセキュリティチップ、
EE: 自宅側医療機器 (EE) 制御部、
SC: EE 内に構成されるセキュリティチップ、
SP: 病院側医療機器 (SP) 制御部、
SM: SP 内のセキュリティモジュール、
である。

10

20

30

40

50

【0323】

セキュリティチップ（SC）、ユーザセキュリティチップ（USC）、セキュリティモジュール（SM）は先に説明した図9のセキュリティチップと同様の構成を持ち、セキュリティモジュールまたはチップにおいてグループ属性証明書の検証による権限判定処理等が実行される。すなわち、サービス、ここではデータ処理要求元デバイスからデータ処理要求先に送付されたグループ属性証明書をネットワークインタフェース等の受信部で受信したサービスプロバイダまたはユーザデバイスは、受信したグループ属性証明書を権限判定処理部としてのセキュリティモジュール（チップ）に渡し、セキュリティモジュール（チップ）内で受信したグループ属性証明書に基づいて、権限判定処理が実行し、権限ありの判定に基づいて、様々なデータ処理を実行する。

10

【0324】

まず、ステップS321において、ユーザがエンドエンティティとしての自宅側医療機器（EE）の入力インタフェースを介して、グループ属性証明書（Gp.AC）=AC01の利用要求コマンドを入力する。このグループ属性証明書（Gp.AC）は、図41、図42に示すAC01である。この処理の際、ユーザは利用するグループ属性証明書AC01に設定されたグループIDを指定する。ただし、特定のサービスを指定することにより唯一のグループIDが決定可能である場合は、サービスの指定のみとしてもよい。

【0325】

自宅側医療機器（EE）がユーザからのグループ属性証明書（Gp.AC）AC01の利用要求入力を受領すると、ステップS322において、ユーザセキュリティチップ（USC）と、サービスプロバイダとしての病院側医療機器（SP）のセキュリティモジュール（SM）間の相互認証が実行される。なお、ここでは省略して示してあるが、ダイレクトにSPとの通信を実行できないユーザ識別デバイス（UID）の場合は、

20

（1）EEのSCとSP-SMとの相互認証、

（2）EEのSCとUIDのUSCとの相互認証、

（3）UIDのUSCとSP-SMとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、UIDがEEに接続されることで、EEは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（2）の相互認証の省略が可能となる。さらに、上記3種の相互認証の様々な組み合わせによる認証構成が可能である。

30

【0326】

認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部（図9参照）を中心とした処理として例えば先に図13を参照して説明した公開鍵方式の相互認証処理として実行される。ステップS323では、ユーザセキュリティチップからエンドエンティティに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップS324において、ユーザセキュリティチップ（USC）は、サービスプロバイダ（SP）のセキュリティモジュール（SM）に対して自己のメモリに格納したグループ属性証明書（Gp.AC）AC01を送信する。このグループ属性証明書（Gp.AC）は、先に図41、図42を参照して説明したように、医療プログラムのサービス受領資格権限を判定する処理に適用するグループ属性証明書AC01である。

40

【0327】

ユーザセキュリティチップ（USC）からグループ属性証明書（Gp.AC）AC01を受信した病院側医療機器（SP）のセキュリティモジュール（SM）は、ステップS325において、グループ属性証明書検証処理を実行する。グループ属性証明書の検証処理については、先に図21乃至図23を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（PKC）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

【0328】

グループ属性証明書（Gp.AC）の検証処理後、セキュリティモジュール（SM）は、

50

検証結果を病院側医療機器（ＳＰ）に出力し、検証不成立の場合は、エラー処理として、サービス提供を実行せず処理を中止する。この場合、グループＡＣの検証が不成立であった旨をエンドエンティティ通知する処理を実行してもよい。

【０３２９】

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ３２７に進む。ステップＳ３２７では、先に図２５を参照して説明したグループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、サービスプロバイダとしての病院側医療機器（ＳＰ）の保有するグループ情報データベースに基づいて実行する。すなわち、病院側医療機器（ＳＰ）は、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１から発行者情報、グループＩＤを取得し、取得情報に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

10

【０３３０】

この場合のグループ情報は、医療診断プログラムの実行許可情報を含むものである。サービスプロバイダとしての病院側医療機器（ＳＰ）は、ステップＳ３２８において、サービス提供処理、すなわち、グループ情報に従って、医療診断プログラムの実行を行なう。すなわち、リモートコントロールによる医療診断処理、すなわち各種診断プログラムの実行コマンドを自宅側医療機器（ＥＥ）に送信して自宅側医療機器（ＥＥ）を介してユーザの診断を実行する。

【０３３１】

20

次に、図４４を参照して、病院側医療機器（ＳＰ）４０１に格納されたグループ属性証明書ＡＣ０２，４０２を適用して医療診断プログラムの実行結果としての診断データ引き取り処理サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する。

【０３３２】

まず、ステップＳ３３１において、病院側のシステムを操作するユーザが病院側医療機器（ＳＰ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）＝ＡＣ０２の利用要求コマンドを入力する。このグループ属性証明書（Ｇｐ．ＡＣ）は、図４１、図４２に示すＡＣ０２である。この処理の際、病院側のシステムを操作するユーザは利用するグループ属性証明書ＡＣ０２に設定されたグループＩＤを指定する。ただし、特定のサービスを指定することにより唯一のグループＩＤが決定可能である場合は、サービスの指定のみとしてもよい。

30

【０３３３】

病院側医療機器（ＳＰ）がグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０２の利用要求入力を受領すると、ステップＳ３３２において、ユーザセキュリティチップ（ＵＳＣ）と、サービスプロバイダとしての病院側医療機器（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証が実行される。なお、ここでは省略して示してあるが、ダイレクトにＳＰとの通信を実行できないユーザ識別デバイス（ＵＩＤ）の場合は、

（１）ＥＥのＳＣとＳＰ－ＳＭとの相互認証、

（２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、

（３）ＵＩＤのＵＳＣとＳＰ－ＳＭとの相互認証、

40

のすべてを実行することになる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

【０３３４】

認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部（図９参照）を中心とした処理として例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ３３３では、セキュリティモジュール（ＳＭ）から病院側医療機器（ＳＰ）に対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が

50

出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップS 3 3 4において、病院側医療機器（S P）のセキュリティモジュール（S M）は、自宅側医療機器側のユーザセキュリティチップ（U S C）に対して自己のメモリに格納したグループ属性証明書（G p . A C）A C 0 2を送信する。このグループ属性証明書（G p . A C）は、先に図4 1、図4 2を参照して説明したように、診断結果データの引き取り処理権限を判定する処理に適用するグループ属性証明書A C 0 2である。

【0 3 3 5】

病院側医療機器（S P）のセキュリティモジュール（S M）からグループ属性証明書（G p . A C）A C 0 2を受信したユーザセキュリティチップ（U S C）は、ステップS 3 3 5において、グループ属性証明書検証処理を実行する。グループ属性証明書の検証処理については、先に図2 1乃至図2 3を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（P K C）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

【0 3 3 6】

グループ属性証明書（G p . A C）の検証処理後、ユーザセキュリティチップ（U S C）は、検証結果を自宅側医療機器（E E）に出力（S 3 3 6）し、検証不成立の場合は、エラー処理として、診断結果の送信サービスを実行せず処理を中止する。この場合、グループA Cの検証が不成立であった旨を病院側医療機器（S P）に通知する処理を実行してもよい。

【0 3 3 7】

グループ属性証明書（G p . A C）の検証が成功し、グループ属性証明書（G p . A C）の正当性が確認されるとステップS 3 3 7に進む。ステップS 3 3 7では、先に図2 5を参照して説明したグループ属性証明書（G p . A C）の審査を実行する。審査は、自宅側医療機器（E E）の保有するグループ情報データベースに基づいて実行する。すなわち、自宅側医療機器（E E）は、検証済みのグループ属性証明書（G p . A C）A C 0 2から発行者情報、グループIDを取得し、取得情報に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

【0 3 3 8】

この場合のグループ情報は、医療診断プログラムの診断結果送信許可情報を含むものである。自宅側医療機器（E E）は、ステップS 3 3 8において、サービス提供処理、すなわち、グループ情報に従って、医療診断プログラムの診断結果送信処理を実行する。すなわち、医療診断処理結果を自宅側医療機器（E E）から病院側医療機器（S P）に送信する処理を実行する。

【0 3 3 9】

（5 - 3）リモートメンテナンスサービス

次に、グループ属性証明書に基づいて権限確認を実行してデータ処理の実行を行なうデータ処理システムの構成例として、エンドエンティティ（E E）としての機器、例えば家電製品のリモートメンテナンスを実行するサービス利用例について説明する。

【0 3 4 0】

ここでは、通信機能を有するA V機器、エアコン、冷蔵庫等の様々な家電機器をエンドエンティティ（E E）として、自宅等に設置したこれらの家電機器と、サービスプロバイダとしての家電機器メーカー側のサービス提供機器（S P）との間で通信を実行して、メーカー側のサービス提供機器（S P）から送信する命令に基づいて、自宅設置の家電機器（E E）の修理、メンテナンス、アップグレード、その他コントロール処理を実行する例について説明する。

【0 3 4 1】

上述の各処理の実行の際、それぞれグループ属性証明書の検証、審査に基づいて処理の実行可否を確認する処理が行なわれ、実行可否確認の後、各処理が実行される。適用するグループ属性証明書の例を図4 5に示す。グループ属性証明書は、大きく2つのカテゴリに

分類される。１つはサービス属性証明書（ＡＣ）であり、他方はコントロール属性証明書（ＡＣ）である。

【０３４２】

サービス属性証明書（ＡＣ）は、発行者が、サービスプロバイダ（ＳＰ）としての家電機器メーカー側機器であり、所有者、すなわちサービス属性証明書（ＡＣ）の発行時に発行者である家電機器メーカー側機器（ＳＰ）と認証処理を行なうことにより属性証明書の発行対象となった所有者は、自宅等に設置した家電機器（ＥＥ）を利用するユーザのユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）、あるいは家電機器（ＥＥ）のセキュリティチップ（ＳＣ）である。

【０３４３】

このサービス属性証明書は、家電機器を購入したユーザとメーカー側との間で、家電機器購入時にサブスクリバ契約を交わすことで、その後の家電機器（ＥＥ）の修理、メンテナンス、アップグレード、その他コントロール処理に関するサービスを受領する権限を認めた家電機器購入者グループ、あるいは家電機器グループに対して発行されるものである。従って、サービス属性証明書は、家電機器購入者グループ、あるいは家電機器グループを対象として発行されるグループ属性証明書である。

【０３４４】

家電機器購入者グループを対象として発行する場合は、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）と家電機器メーカー（ＳＰ）のセキュリティモジュール間の相互認証の成立を条件とした発行処理がなされ、家電機器グループを対象として発行する場合は、家電機器（ＥＥ）のセキュリティチップ（ＳＣ）と家電機器メーカー（ＳＰ）のセキュリティモジュール間の相互認証の成立を条件とした発行処理がなされる。

【０３４５】

このサービス属性証明書は、家電機器（ＥＥ）の修理、メンテナンス、アップグレード、その他コントロールサービスの要求の際に、家電機器（ＥＥ）あるいはユーザ識別デバイス（ＵＩＤ）からメーカー側機器（ＳＰ）に送付されて、メーカー側機器（ＳＰ）において、サービス属性証明書の検証、審査の後、サービスの提供に移行することになる。

【０３４６】

コントロール属性証明書は、発行者が、修理、メンテナンス、アップグレード、その他コントロールサービスを受領する家電機器（ＥＥ）であり、所有者、すなわちコントロール属性証明書の発行時に発行者である家電機器（ＥＥ）と認証処理を行なうことによりグループ属性証明書の発行対象となった所有者は、サービスプロバイダ（ＳＰ）としてのメーカー側機器のセキュリティモジュール（ＳＭ）である。

【０３４７】

このコントロール属性証明書は、家電機器を購入したユーザとメーカー側との間で、家電機器購入以後に、サービス属性証明書の保有を条件として発行される証明書であり、例えば同一メーカーの複数の家電機器を有するユーザが、各々の家電機器に対するメンテナンスサービス実行範囲を権限情報とした証明書として、各家電機器に対応して、サービス提供者であるメーカー側機器に対して発行する。あるいは、１つの家電機器に対して、異なるコントロール権限情報を各々記録した証明書として発行することも可能である。例えば、家電機器のコントロール情報として、ソフトウェアのアップグレード処理依頼のために、アップグレード処理のみを受領サービスとして許容することを示す属性証明書、あるいは、定期点検のための点検処理のみを許容することを示す属性証明書等である。

【０３４８】

コントロール属性証明書は、例えば１ユーザの所有する複数の家電機器グループ、あるいは１つの家電機器を対象として複数発行可能なグループ属性証明書である。１ユーザの所有する複数の家電機器グループを対象として発行する場合は、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）と家電機器メーカー（ＳＰ）のセキュリティモジュール間の相互認証の成立を条件とした発行処理がなされ、１つの特定の家電機器を対象として発行する場合は、上述のＵＩＤのＵＳＣ、あるいは特定の家電機器（ＥＥ）の

10

20

30

40

50

セキュリティチップ（ＳＣ）と家電機器メーカー（ＳＰ）のセキュリティモジュール間の相互認証の成立を条件とした発行処理がなされる。

【０３４９】

このコントロール属性証明書は、ユーザ側（ＥＥまたはＵＩＤ）から発行されてサービスを提供するメーカー側機器に格納され、家電機器（ＥＥ）の修理、メンテナンス、アップグレード、その他コントロールサービスの実行時にメーカー側機器から、ユーザ側（ＥＥまたはＵＩＤ）に送信されて、ユーザ側（ＥＥまたはＵＩＤ）において、コントロール属性証明書の検証、審査の後、サービスの提供に移行することになる。

【０３５０】

なお、サービス属性証明書、コントロール属性証明書の発行処理は、メーカー側機器（ＳＰ）あるいは家電機器（ＥＥ）、あるいはユーザ識別デバイス（ＵＩＤ）自体が、グループ属性認証局（グループＡＡ）およびグループ属性証明書登録局（グループＡＲＡ）の機能を実行して、みずから発行することが可能であるが、グループ属性認証局（グループＡＡ）およびグループ属性証明書登録局（グループＡＲＡ）に依頼して発行処理を行なう構成も可能である。ただし、この場合には発行者のポリシーに従った処理が実行されることが条件である。

【０３５１】

例えばサービス属性証明書の発行処理は、発行者であるメーカー側機器（ＳＰ）あるいは、発行代理を行なうグループ属性証明書登録局（グループＡＲＡ）が、サービス提供を受けようとするユーザから、ユーザ自身を証明する既発行のグループ属性証明書、例えばクレジットカード会社の発行したグループ属性証明書を提示させ、その提出されたグループ属性証明書の検証を実行した後、新たなグループ属性証明書として、サービス属性証明書を発行したり、あるいは家電機器に対して、製造時にメーカーが格納したメーカー製の製品グループに属することを証明するグループ属性証明書を提示させ、その提出されたグループ属性証明書の検証を実行した後、新たなグループ属性証明書として、サービス属性証明書を発行するといった発行処理を行なうことが好ましい。このような既発行のグループ属性証明書の検証を条件として、新たなグループ属性証明書を発行する処理シーケンスは、先に図２９、図３０、図３２等を参照して説明した処理シーケンスと同様となる。

【０３５２】

また、コントロール属性証明書の発行処理においても、同様に、発行者である家電機器（ＥＥ）あるいは、発行代理を行なうグループ属性証明書登録局（グループＡＲＡ）が、メーカー側機器（ＳＰ）から、メーカー側の真正な機器であることを証明する既発行のグループ属性証明書、例えば、前述したようにメーカーの発行したグループ属性証明書としてのサービス属性証明書を提示させて、その提出証明書の検証を実行した後、新たなグループ属性証明書としてのコントロール属性証明書の発行処理を行なう方法をとることが好ましい。

【０３５３】

メンテナンスサービスを行なうシステムにおいて、各機器に格納される属性証明書は、図４６に示す通りとなる。サービスプロバイダとしてのメーカー側機器（ＳＰ）４５１と、エンドエンティティとしてのユーザー側家電機器（ＥＥ）４６１は通信ネットワークにより相互にデータ転送可能であり、ユーザー側家電機器（ＥＥ）４６１と、ユーザ識別デバイス（ＵＩＤ）４７１は、双方の接続機器インタフェース２３１（図９参照）を介して相互にデータ転送が可能である。

【０３５４】

それぞれの機器には、耐タンパ構成を持つ（ユーザ）セキュリティチップ４６３，４７２またはセキュリティモジュール４５３が備えられ、データ通信処理の際の相互認証処理、あるいは転送データの暗号化、復号処理等を実行する。またグループ属性証明書の検証処理も（ユーザ）セキュリティチップ４６３，４７２またはセキュリティモジュール４５３において実行される。

【０３５５】

10

20

30

40

50

ユーザ側家電機器（ＥＥ）４６１には、先に図４５を参照して説明したサービス属性証明書４６２が格納される。サービス属性証明書４６２は、発行者が、サービスプロバイダとしてのメーカー側機器（ＳＰ）４５１であり、家電メンテナンス、修理等の実行可否を判定する確認処理の際に適用され、所有者であるユーザ側家電機器（ＥＥ）４６１のＳＣ４６３からメーカー側機器（ＳＰ）４５１に送付される。メーカー側機器（ＳＰ）４５１のセキュリティモジュール（ＳＭ）４５３において検証、審査の後、サービス、すなわちコントロール属性証明書送信、およびコントロール属性証明書によって許可された権限範囲でのメンテナンス等の処理が実行される。

【０３５６】

サービスプロバイダとしてのメーカー側機器（ＳＰ）４５１には、コントロール属性証明書４５２が格納される。コントロール属性証明書４５２は、発行者が、ユーザ側家電機器（ＥＥ）４６１であり、所有者がメーカー側機器（ＳＰ）４５１であり、メーカー側機器（ＳＰ）からユーザ側家電機器（ＥＥ）４６１に送付され、メンテナンス等のサービス実行の前に、ユーザ側家電機器（ＥＥ）４６１のセキュリティチップ（ＳＣ）４６３においてコントロール属性証明書の検証、審査が実行され、検証、審査成立を条件としてメンテナンス、修理、あるいはアップグレード等の処理が、コントロール属性証明書によって確認された権限範囲内で実行される。

【０３５７】

サービス実行時におけるサービス属性証明書およびコントロール属性証明書の利用形態について、図４７を参照して説明する。まず、メンテナンス、修理、点検、アップグレード等のサービスを受領したい家電機器（ＥＥ）あるいは家電機器に接続したユーザ識別デバイス（ＵＩＤ）側から、サービス属性証明書（ＡＣ）４８４をメーカー側機器（ＳＰ）４８２に提示する。メーカー側機器（ＳＰ）４８２は、セキュリティモジュール（ＳＭ）におけるサービス属性証明書の検証の後、サービス属性証明書に対応するグループＩＤに基づいて、グループ情報データベース４８３を検索して、グループ情報としてのコントロールＡＣあるいはコントロールＡＣの識別データを抽出して、サービスＡＣに対応するコントロールＡＣを取得する。

【０３５８】

メーカー側機器（ＳＰ）４８２は、取得したコントロール属性証明書（ＡＣ）４８５を家電機器（ＥＥ）あるいは家電機器に接続したユーザ識別デバイス（ＵＩＤ）に送信し、家電機器（ＥＥ）あるいは家電機器に接続したユーザ識別デバイス（ＵＩＤ）におけるセキュリティチップで検証の後、コントロール属性証明書（ＡＣ）で許容されたコントロール情報に従って家電機器（ＥＥ）に対してメンテナンス等のサービスが実行される。

【０３５９】

なお、メンテナンス、修理、アップグレード等の実行プログラムは、予め家電機器内のメモリに格納したものを利用してもよく、あるいは、必要に応じて、メーカー側機器から家電機器に対して送信して実行する構成としてもよい。なお、実行プログラムの送信の際には、認証処理、送信データの暗号化処理を実行することが好ましい。

【０３６０】

次に、図４８以下を参照して、ユーザデバイスとしての家電機器（ＥＥ）に格納されたサービス属性証明書、サービスプロバイダに格納されたコントロール属性証明書を適用して家電機器のメンテナンス等のサービスに関する利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する。図４８において、

ＥＥ：ユーザ側家電機器（ＥＥ）制御部、
 ＳＣ：ＥＥ内に構成されるセキュリティチップ、
 ＳＰ：メーカー側機器（ＳＰ）制御部、
 ＳＭ：ＳＰ内のセキュリティモジュール、
 である。

【０３６１】

セキュリティチップ（ＳＣ）、ユーザセキュリティチップ（ＵＳＣ）、セキュリティモジ

10

20

30

40

50

ユーモジュール（SM）は先に説明した図9のセキュリティチップと同様の構成を持ち、セキュリティモジュールまたはチップにおいてグループ属性証明書の検証による権限判定処理等が実行される。すなわち、サービス、ここではメンテナンス処理等のデータ処理要求元デバイスからデータ処理要求先に送付されたグループ属性証明書をネットワークインタフェース等の受信部で受信したサービスプロバイダまたはユーザデバイスは、受信したグループ属性証明書を権限判定処理部としてのセキュリティモジュール（チップ）に渡し、セキュリティモジュール（チップ）内で受信したグループ属性証明書に基づいて、権限判定処理が実行し、権限ありの判定に基づいて、様々なデータ処理を実行する。

【0362】

まず、ステップS341において、ユーザがエンドエンティティとしてのユーザ側家電機器（EE）の入力インタフェースを介して、グループ属性証明書（Gp.AC）であるサービス属性証明書（AC）の利用要求コマンドを入力する。この処理の際、ユーザは利用するサービス属性証明書（AC）に設定されたグループIDを指定する。ただし、特定のサービスを指定することにより唯一のグループIDが決定可能である場合は、サービスの指定のみとしてもよい。

【0363】

ユーザ側家電機器（EE）がユーザからのサービス属性証明書（AC）の利用要求入力を受領すると、ステップS342において、セキュリティチップ（SC）と、サービスプロバイダとしてのメーカー側機器（SP）のセキュリティモジュール（SM）間の相互認証が実行される。なお、ここでは、家電機器（EE）のセキュリティチップ（SC）を発行対象としたサービス属性証明書の利用例を示してあるが、ユーザ識別デバイス（UID）のユーザセキュリティチップ（SC）を発行対象としたサービス属性証明書を利用した処理も同様に可能である。ただし、ダイレクトにSPとの通信を実行できないユーザ識別デバイス（UID）の場合は、

- （1）EEのSCとSP-SMとの相互認証、
- （2）EEのSCとUIDのUSCとの相互認証、
- （3）UIDのUSCとSP-SMとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、UIDがEEに接続されることで、EEは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（2）の相互認証の省略が可能となる。さらに、上記3種の相互認証の様々な組み合わせによる認証構成が可能である。

【0364】

認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部（図9参照）を中心とした処理として例えば先に図13を参照して説明した公開鍵方式の相互認証処理として実行される。ステップS343では、セキュリティチップからエンドエンティティに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップS344において、セキュリティチップ（SC）は、メーカー側機器であるサービスプロバイダ（SP）のセキュリティモジュール（SM）に対して自己のメモリに格納したサービス属性証明書を送信する。

【0365】

ユーザ側家電機器のセキュリティチップ（SC）からサービス属性証明書を受信したメーカー側機器（SP）のセキュリティモジュール（SM）は、ステップS345において、サービス属性証明書の検証処理を実行する。サービス属性証明書の検証処理については、先に図21乃至図23を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（PKC）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

【0366】

サービス属性証明書の検証処理後、セキュリティモジュール（SM）は、検証結果をメーカー側機器（SP）に出力し、検証不成立の場合は、エラー処理として、サービス提供を

10

20

30

40

50

実行せず処理を中止する。この場合、サービス属性証明書の検証が不成立であった旨をエンドエンティティ通知する処理を実行してもよい。

【0367】

サービス属性証明書の検証が成功し、サービス属性証明書の正当性が確認されるとステップS347に進む。ステップS347では、サービス属性証明書の審査を実行する。審査は、サービスプロバイダとしてのメーカー側機器（SP）の保有するグループ情報データベースに基づいて実行する。

【0368】

サービス属性証明書の審査処理について、図49を参照して説明する。ステップS351において、サービスプロバイダ（SP）は、検証済みのサービス属性証明書から属性値としてのグループIDを取得する。ステップS352において、サービス属性証明書から取得したグループIDに基づいて、グループ情報データベースを検索（S352）し、登録されたエントリーから、コントロール属性証明書情報、例えばコントロール属性証明書の識別子（ID）を取得（S353）する。

10

【0369】

図49に示すように、サービスプロバイダの保有するグループ情報データベース（DB）には、発行者、サービスACのグループID、およびグループ情報としての対応コントロール属性証明書情報、例えばIDが対応付けられて格納され、サービスプロバイダ（SP）は、ユーザ側家電機器から受領し、検証の成立したサービス属性証明書（AC）から取得したグループIDに基づいて、グループ情報データベース（DB）を検索してグループ情報として、サービスACに対応するコントロール属性証明書（AC）の特定情報を取得する。

20

【0370】

次に、サービスプロバイダとしてのメーカー側機器（SP）は、ステップS348（図48）において、グループ情報データベース（DB）から取得したコントロール属性証明書（AC）のIDに基づいて、コントロール属性証明書（AC）を取得する。

【0371】

次に、サービス属性証明書を受領したサービスプロバイダが、コントロール属性証明書に基づくサービス、例えば家電機器に対するメンテナンス、点検、修理、アップグレード、あるいはコントロール等の処理を実行するシーケンスについて、図50以下を参照して説明する。

30

【0372】

図50のステップS370において、メーカー側機器を操作するオペレータがメーカー側機器（SP）の入力インタフェースを介して、コントロール属性証明書を適用したメンテナンス処理実行コマンドを入力する。この処理の際、オペレータは利用するコントロール属性証明書に設定されたグループIDを指定する。

【0373】

メーカー側機器（SP）がコントロール属性証明書を適用したメンテナンス処理実行要求入力を受領すると、ステップS371において、家電機器（EE）のセキュリティチップ（SC）と、サービスプロバイダとしてのメーカー側機器（SP）のセキュリティモジュール（SM）間の相互認証が実行される。なお、先に図48を参照して説明したサービス属性証明書の検証処理シーケンスと同一セッションで図50に示すコントロール属性証明書に基づくサービス提供シーケンスが実行される場合は、この相互認証処理は不要となる。

40

【0374】

認証処理が実行された場合は、ステップS372で、セキュリティモジュール（SM）からメーカー側機器（SP）に対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップS373において、メーカー側機器（SP）のセキュリティモジュール（SM）は、ユーザ側家電機器側のセキュリティチップ（SC）に対して、受信した

50

サービス属性証明書に基づいて抽出したコントロール属性証明書を送信する。このコントロール属性証明書は、先に説明したように、家電機器に対するコントロール範囲処理権限を確認する処理に適用するグループ属性証明書である。

【0375】

メーカー側機器（SP）のセキュリティモジュール（SM）からコントロール属性証明書を受信したセキュリティチップ（SC）は、ステップS374において、コントロール属性証明書検証処理を実行する。コントロール属性証明書の検証処理は、先に図21乃至図23を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（PKC）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

【0376】

コントロール属性証明書の検証処理後、セキュリティチップ（SC）は、検証結果をユーザ側家電機器（EE）に出力（S375）し、検証不成立の場合（S376：NG）は、エラー処理（S377）として、メンテナンス等の処理の実行を中止する。この場合、コントロール属性証明書の検証が不成立であった旨をメーカー側機器（SP）に通知する処理を実行してもよい。

【0377】

コントロール属性証明書の検証が成功（S376：OK）し、コントロール属性証明書の正当性が確認されるとステップS378に進む。ステップS378では、家電機器（EE）がメンテナンス実行プログラムの検索を行なう。このメンテナンス実行プログラムは、あらかじめ家電機器（EE）にコントロール属性証明書ID、あるいはグループIDに対応付けられてメモリに格納されているか、あるいは処理実行時にメーカー側機器（SP）から送信されるプログラムであり、必要に応じて暗号化されている。このシーケンス図においては、メンテナンス実行プログラムは、あらかじめ家電機器（EE）にコントロール属性証明書ID、あるいはグループIDに対応付けられて格納されている場合の例である。

【0378】

ステップS379では、家電機器（EE）が抽出した暗号化メンテナンスプログラムをセキュリティチップ（SC）に転送し、ステップS380において、セキュリティチップ（SC）側において復号処理を実行する。復号処理は、例えばサービスプロバイダ（SP）側から提供された鍵、あるいは各ユーザデバイスに固有の鍵等に基づいて実行される。プログラムの暗号化処理態様としては、公開鍵方式、共通鍵方式等、各種の処理方式が採用可能である。なお、鍵を格納した属性証明書を利用して鍵をセキュリティチップに提供する構成としてもよい。

【0379】

ステップS381において、セキュリティチップ（SC）から復号されたメンテナンスプログラムが家電機器としてのエンドエンティティ（EE）に出力され、ステップS382において、メンテナンスプログラムが実行され、プログラム実行完了の後、ステップS383において、実行結果がサービスプロバイダ（SP）に送信される。

【0380】

図51は、図50と同様、サービス属性証明書を受領したサービスプロバイダが、コントロール属性証明書に基づくサービス、例えば家電機器に対するメンテナンス、点検、修理、アップグレード、あるいはコントロール等の処理を実行するシーケンスであり、メンテナンス実行プログラムをメーカー側機器（SP）からユーザ側家電機器（EE）に対して送信する処理とした例である。ステップS384～S392は、図50のステップS370～S377に対応する。

【0381】

コントロールACの検証OKの後のステップS393において、ユーザ側家電機器（EE）からメーカー側機器（SP）に対してメンテナンスプログラムの送信要求が出力され、ステップS394において、サービスプロバイダとしてのメーカー側機器がメンテナンスプログラムの検索を実行し、ステップS395において検索したプログラムをユーザ側家

10

20

30

40

50

電機器（ＥＥ）に対して送信する処理部分が、図５０の処理シーケンスと異なっている。

【０３８２】

なお、送信プログラムは、必要に応じて暗号化される。例えばセッション鍵、サービスプロバイダ（ＳＰ）側から提供された鍵、あるいは各ユーザデバイスに固有の鍵等に基づいて復号可能な態様で暗号化がなされて送信される。プログラムの暗号化処理態様としては、公開鍵方式、共通鍵方式等、各種の処理方式が採用可能である。なお、鍵を格納した属性証明書を利用して鍵をセキュリティチップに提供する構成としてもよい。

【０３８３】

図５２の処理シーケンスは、図５０、図５１と同様、サービス属性証明書を受領したサービスプロバイダが、コントロール属性証明書に基づくサービス、例えば家電機器に対するメンテナンス、点検、修理、アップグレード、あるいはコントロール等の処理を実行するシーケンスであるが、メンテナンス実行プログラムをメーカー側機器（ＳＰ）から、逐次コマンドを家電機器（ＥＥ）に送信し、コマンド実行に基づく応答を家電機器（ＥＥ）から受信しながらレスポンス対応の処理を実行する構成としたものである。

10

【０３８４】

ステップＳ４１０～Ｓ４２０は、図５１のステップＳ３８４～Ｓ３９４に対応する。サービスプロバイダ（ＳＰ）は、ステップＳ４２１でメンテナンスプログラムに従ったコマンドを必要に応じて暗号化して家電機器（ＥＥ）に送信し、家電機器（ＥＥ）はステップＳ４２２において、暗号化コマンドをセキュリティチップに渡し、セキュリティチップ（ＳＣ）における復号（Ｓ４２３）、セキュリティチップ（ＳＣ）から復号コマンドの引き渡し（Ｓ４２４）の後、家電機器（ＥＥ）においてコマンドを実行（Ｓ４２５）し、実行結果をコマンド実行レスポンスとして家電機器（ＥＥ）からサービスプロバイダ（ＳＰ）に送信し、レスポンスを受信したサービスプロバイダ（ＳＰ）がレスポンスに基づく次実行コマンドを家電機器（ＥＥ）に送信する構成としている。

20

【０３８５】

メンテナンスプログラムに従ったコマンドの実行がすべて終了すると、ステップＳ４２７において、メンテナンスプログラム実行処理を終了する。

【０３８６】

上述したメンテナンス処理形態は、ユーザ側の家電機器からサービス属性証明書を、メーカー側機器に提示し、一方、メーカー側機器がコントロール属性証明書を家電機器に提示して、相互に各属性証明書の検証、審査を実行して、サービスの受領あるいは提供範囲の権限確認を行なう形態である。

30

【０３８７】

サービス属性証明書、コントロール属性証明書の利用形態は上述した処理形態に限らず、例えば図５３に示すように、両属性証明書をユーザ側機器４９１に格納して、サービス提供要求時にサービス属性証明書４９３、コントロール属性証明書４９４をメーカー側（ＳＰ）４９２に提示し、メーカー側（ＳＰ）４９２において、サービス属性証明書４９３、コントロール属性証明書４９４の検証、審査を実行するとともに、両者の対応関係を確認の後、コントロール属性証明書４９４によって示される権限の範囲でのメンテナンス処理をユーザ側機器４９１に対して実行する形態としてもよい。

40

【０３８８】

また、家電機器において一定時間毎にメンテナンス自動実行を行なうプログラムを格納し、プログラムされた時間間隔でサービス属性証明書を伴うメンテナンス要求をメーカー側に送信し、メーカー側が要求受信に基づいて、コントロール属性証明書の送信およびメンテナンス処理を実行する形態としてもよい。

【０３８９】

（５－４）パーソナルコミュニケーションサービス

次に、グループ属性証明書に基づいて権限確認を実行してエンドエンティティ（ＥＥ）としてのＰＣ、ＰＤＡ、その他の通信端末を利用したコミュニケーションサービス利用例について説明する。

50

【 0 3 9 0 】

ここでは、P C、P D A、その他の通信端末をエンドエンティティ（E E）として、自宅等に設置した通信端末が、チャットルームを提供するサービスプロバイダのサーバに接続して、チャットルームを介した通信端末間のコミュニケーション、およびエンドエンティティ（E E）間の直接通信において、グループ属性証明書を利用したアクセス制限処理を実行してコミュニケーションサービスを行なう例を説明する。コミュニケーションサービスにおいて適用するグループ属性証明書の例を図 5 4 に示す。

【 0 3 9 1 】

グループ属性証明書 A C 0 1 は、発行者が、サービスプロバイダ（S P）としてのチャット運営者であり、所有者、すなわちグループ属性証明書 A C 0 1 の発行時に発行者であるチャット運営サービスプロバイダ（S P）と認証処理を行なうことによりグループ属性証明書 A C 0 1 の発行対象となった所有者は、ユーザ甲さんの通信端末としてのエンドエンティティ（E E）のセキュリティチップ（S C）、あるいはユーザ甲さんのユーザ識別デバイス（U I D）のユーザセキュリティチップ（U S C）である。

10

【 0 3 9 2 】

このグループ属性証明書 A C 0 1 は、チャット運営サービスプロバイダ（S P）の提供するチャットルームを構成するサーバに対するアクセス権を有することを証明する属性証明書であり、チャットルームに対して参加する権限を有するユーザーグループあるいはユーザ機器グループに対して発行される。

【 0 3 9 3 】

グループ属性証明書 A C 0 2 は、発行者が、乙さんのユーザデバイス、（E EまたはU I D）であり、所有者、すなわちグループ属性証明書 A C 0 2 の発行時に発行者である乙さんのユーザデバイスのセキュリティチップ（S CまたはU S C）と認証処理を行なうことによりグループ属性証明書 A C 0 2 の発行対象となった所有者は、甲さんのユーザデバイスのセキュリティチップ（S CまたはU S C）である。

20

【 0 3 9 4 】

このグループ属性証明書 A C 0 2 は、乙さんのユーザデバイスの管理サーバーへのアクセス権を有することを証明する属性証明書であり、乙さんのユーザデバイスの管理サーバーにアクセスする権限を有するユーザーグループあるいはユーザ機器グループに対して発行される。

30

【 0 3 9 5 】

なお、グループ属性証明書 A C 0 1、A C 0 2 の発行処理は、サービスプロバイダ（S P）あるいは乙さんユーザデバイスとしてのエンドエンティティ（E E）あるいはユーザ識別デバイス（U I D）自体が、グループ属性認証局（グループ A A）およびグループ属性証明書登録局（グループ A R A）の機能を実行して、みずから発行することが可能であるが、グループ属性認証局（グループ A A）およびグループ属性証明書登録局（グループ A R A）に依頼して発行処理を行なう構成も可能である。ただし、この場合には発行者のポリシーに従った処理が実行されることが条件である。

【 0 3 9 6 】

例えばグループ属性証明書 A C 0 1、A C 0 2 の発行処理は、発行者であるサービスプロバイダ（S P）、乙さんのユーザデバイス（E E、U I D）、あるいは、発行代理を行なうグループ属性証明書登録局（グループ A R A）が、発行要求者としての甲さんから、甲さんであることを証明する既発行のグループ属性証明書、例えばクレジットカード会社の発行したグループ属性証明書を提示させ、その提出されたグループ属性証明書の検証を実行した後、新たなグループ属性証明書 A C 0 1、A C 0 2 の発行処理を行なう方法をとることが好ましい。このような既発行のグループ属性証明書の検証を条件として、新たなグループ属性証明書を発行する処理シーケンスは、先に図 2 9、図 3 0、図 3 2 等を参照して説明した処理シーケンスと同様となる。

40

【 0 3 9 7 】

図 5 4 に示すグループ属性証明書の発行、格納形態は、図 5 5 に示す通りとなる。チャッ

50

トルーム提供サービスプロバイダ (S P) 5 0 1 と、エンドエンティティとしての甲さん通信端末 (E E) 5 1 1、乙さん通信端末 (E E) 5 3 1 は通信ネットワークにより相互にデータ転送可能であり、通信端末 (E E) 5 1 1 とユーザ識別デバイス (U I D) 5 2 1、通信端末 (E E) 5 3 1 とユーザ識別デバイス (U I D) 5 3 3 は、双方の接続機器インタフェース 2 3 1 (図 9 参照) を介して相互にデータ転送が可能である。

【 0 3 9 8 】

それぞれの機器には、耐タンパ構成を持つ (ユーザ) セキュリティチップ 5 1 2 , 5 2 2 , 5 3 2 , 5 3 4 またはセキュリティモジュール 5 0 2 が備えられ、データ通信処理の際の相互認証処理、あるいは転送データの暗号化、復号処理等を実行する。またグループ属性証明書の検証処理もこれらセキュリティチップ、セキュリティモジュールにおいて実行される。

10

【 0 3 9 9 】

甲さんのユーザ識別デバイス 5 2 1 には、先に図 5 4 を参照して説明したグループ属性証明書 A C 0 1 , 5 2 3 が格納される。グループ属性証明書 A C 0 1 , 5 2 3 は、発行者が、チャットルーム提供サービスプロバイダ (S P) 5 0 1 であり、チャットルーム参加権限確認処理に適用され、所有者である甲さんユーザデバイスの U S C 5 2 1 からチャットルーム提供サービスプロバイダ (S P) 5 0 1 に送付されて、チャットルーム提供サービスプロバイダ (S P) 5 0 1 のセキュリティモジュール (S M) 5 0 2 において、グループ属性証明書 A C 0 1 の検証、審査の後、サービス、すなわちチャットルーム参加が認められる。

20

【 0 4 0 0 】

また、甲さんのユーザ識別デバイス 5 2 1 には、先に図 5 4 を参照して説明したグループ属性証明書 A C 0 2 , 5 2 4 も格納される。グループ属性証明書 A C 0 2 , 5 2 4 は、発行者が、乙さんユーザデバイス (E E 5 3 1 または U I D 5 3 3) であり、乙さんのユーザデバイスの管理サーバーに対するアクセス権限確認処理に適用され、所有者である甲さんユーザデバイスの U S C 5 2 1 から乙さんユーザデバイス (E E 5 3 1 または U I D 5 3 3) に送付されて、乙さんユーザデバイス (E E 5 3 1 または U I D 5 3 3) のセキュリティチップ (S C 5 3 2 または U S C 5 3 4) において、グループ属性証明書 A C 0 2 の検証、審査の後、サービス、すなわち乙さんデバイスの管理サーバーに対するアクセスが認められる。

30

【 0 4 0 1 】

図 5 6 を参照して、甲さんのユーザ識別デバイス 4 2 1 に格納されたグループ属性証明書 A C 0 1 , 5 2 3 を適用してチャットルーム参加サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する。図 5 6 において、

U I D : 甲さんユーザ識別デバイス (ユーザデバイス) 制御部、

U S C : U I D 内に構成されるユーザセキュリティチップ、

E E : 甲さん通信端末 (E E) 制御部、

S C : E E 内に構成されるセキュリティチップ、

S P : チャットルーム提供サービスプロバイダ (S P) 制御部、

S M : S P 内のセキュリティモジュール、

40

である。

【 0 4 0 2 】

まず、ステップ S 4 5 1 において、ユーザ (甲さん) がエンドエンティティとしての甲さん通信端末 (E E) の入力インタフェースを介して、グループ属性証明書 (G p . A C) = A C 0 1 の利用要求コマンドを入力する。このグループ属性証明書 (G p . A C) は、図 5 4、図 5 5 に示す A C 0 1 である。この処理の際、ユーザは利用するグループ属性証明書 A C 0 1 に設定されたグループ I D を指定する。ただし、特定のサービスを指定することにより唯一のグループ I D が決定可能である場合は、サービスの指定のみとしてもよい。

【 0 4 0 3 】

50

甲さん通信端末（ＥＥ）がユーザからのグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１の利用要求入力を受領すると、ステップＳ４５２において、ユーザセキュリティチップ（ＵＳＣ）と、サービスプロバイダとしてのチャットルーム提供サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証が実行される。なお、ここでは省略して示してあるが、ダイレクトにＳＰとの通信を実行できないユーザ識別デバイス（ＵＩＤ）の場合は、

- （１）ＥＥのＳＣとＳＰ－ＳＭとの相互認証、
- （２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、
- （３）ＵＩＤのＵＳＣとＳＰ－ＳＭとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

【０４０４】

認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部（図９参照）を中心とした処理として例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ４５３では、ユーザセキュリティチップからエンドエンティティに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ４５４において、ユーザセキュリティチップ（ＵＳＣ）は、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）に対して自己のメモリに格納したグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１を送信する。このグループ属性証明書（Ｇｐ．ＡＣ）は、先に図５４、図５５を参照して説明したように、チャットルームへの参加資格権限を判定する処理に適用するグループ属性証明書ＡＣ０１である。

【０４０５】

ユーザセキュリティチップ（ＵＳＣ）からグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１を受信したチャットルーム提供サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）は、ステップＳ４５５において、グループ属性証明書検証処理を実行する。グループ属性証明書の検証処理については、先に図２１乃至図２３を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

【０４０６】

グループ属性証明書（Ｇｐ．ＡＣ）の検証処理後、セキュリティモジュール（ＳＭ）は、検証結果をチャットルーム提供サービスプロバイダ（ＳＰ）に出力し、検証不成立の場合は、エラー処理として、サービス提供を実行せず処理を中止する。この場合、グループＡＣの検証が不成立であった旨をエンドエンティティに通知する処理を実行してもよい。

【０４０７】

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ４５７に進む。ステップＳ４５７では、先に図２５を参照して説明したグループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、サービスプロバイダとしてのチャットルーム提供サービスプロバイダ（ＳＰ）の保有するグループ情報データベースに基づいて実行する。すなわち、チャットルーム提供サービスプロバイダ（ＳＰ）は、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１から発行者情報、グループＩＤを取得し、取得情報に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

【０４０８】

この場合のグループ情報は、チャットルームへの参加許可情報を含むものである。サービスプロバイダとしてのチャットルーム提供サービスプロバイダ（ＳＰ）は、ステップＳ４５８において、サービス提供処理、すなわち、グループ情報に従って、チャットルームへ

10

20

30

40

50

の参加許可を行なう。すなわち、チャットルームを提供するサーバーへのアクセスを許可する処理を行なう。

【0409】

次に、図57を参照して、甲さんのユーザ識別デバイス421に格納されたグループ属性証明書AC02, 524を適用して乙さんのユーザデバイスへのアクセス権限確認処理を行ない、甲さんおよび乙さんとのコミュニケーションを開始する処理シーケンスについて説明する。図57において、

UID：甲さんユーザ識別デバイス（ユーザデバイス）制御部、

USC：UID内に構成されるユーザセキュリティチップ、

EE1：甲さん通信端末（EE）制御部、

SC1：EE1内に構成されるセキュリティチップ、

EE2：乙さん通信端末（EE）制御部、

SC2：EE2内に構成されるセキュリティチップ、

である。

【0410】

まず、ステップS461において、ユーザ（甲さん）がエンドエンティティとしての甲さん通信端末（EE1）の入力インタフェースを介して、グループ属性証明書（Gp・AC）＝AC02の利用要求コマンドを入力する。このグループ属性証明書（Gp・AC）は、図54、図55に示すAC02である。この処理の際、ユーザは利用するグループ属性証明書AC02に設定されたグループIDを指定する。

【0411】

甲さん通信端末（EE1）がユーザからのグループ属性証明書（Gp・AC）AC02の利用要求入力を受領すると、ステップS462において、ユーザセキュリティチップ（USC）と、乙さんユーザデバイスのセキュリティチップ（SC2）間の相互認証が実行される。なお、ここでは、グループ属性証明書（Gp・AC）AC02は、乙さん通信端末（EE）のセキュリティチップ（SC2）が発行主体であった例を説明する。発行主体が乙さんのユーザ識別デバイス（UID）である場合は、乙さんのユーザ識別デバイス（UID）のユーザセキュリティチップ（USC）との認証を行なうことになる。

【0412】

認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部（図9参照）を中心とした処理として例えば先に図13を参照して説明した公開鍵方式の相互認証処理として実行される。ステップS463では、甲さんのユーザセキュリティチップ（USC）からエンドエンティティ（EE1）に対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップS464において、ユーザセキュリティチップ（USC）は、乙さん通信端末（EE）のセキュリティチップ（SC2）に対して自己のメモリに格納したグループ属性証明書（Gp・AC）AC02を送信する。このグループ属性証明書（Gp・AC）は、先に図54、図55を参照して説明したように、乙さんのユーザデバイスのサーバーへのアクセス権限を判定する処理に適用するグループ属性証明書AC02である。

【0413】

ユーザセキュリティチップ（USC）からグループ属性証明書（Gp・AC）AC02を受信した乙さん通信端末（EE）のセキュリティチップ（SC2）は、ステップS465において、グループ属性証明書検証処理を実行する。グループ属性証明書の検証処理については、先に図21乃至図23を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（PKC）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

【0414】

グループ属性証明書（Gp・AC）の検証処理後、乙さん通信端末（EE）のセキュリティチップ（SC2）は、検証結果を乙さん通信端末（EE）に出力し、検証不成立の場合

10

20

30

40

50

は、エラー処理として、サービス提供を実行せず処理を中止する。この場合、グループ A C の検証が不成立であった旨を甲さん側に通知する処理を実行してもよい。

【 0 4 1 5 】

グループ属性証明書 (G p . A C) の検証が成功し、グループ属性証明書 (G p . A C) の正当性が確認されるとステップ S 4 6 7 に進む。ステップ S 4 6 7 では、先に図 2 5 を参照して説明したグループ属性証明書 (G p . A C) の審査を実行する。審査は、乙さん通信端末 (E E) の保有するグループ情報データベースに基づいて実行する。すなわち、乙さん通信端末 (E E) は、検証済みのグループ属性証明書 (G p . A C) A C 0 2 から発行者情報、グループ I D を取得し、取得情報に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

10

【 0 4 1 6 】

この場合のグループ情報は、乙さんユーザデバイスのサーバーへのアクセス権限情報を含むものである。乙さん通信端末 (E E) は、ステップ S 4 6 8 において、サービス提供処理、すなわち、グループ情報に従って、乙さんユーザデバイスのサーバーへのアクセス許可を行なう。

【 0 4 1 7 】

[(6) 実行属性証明書 (実行 A C)]

次に、属性証明書を利用した権限確認に基づくサービス提供処理態様において、属性証明書に基づいてサービス受領権限を判定するのみならず、サービスの実行自体を属性証明書によって制限することを可能とした実行属性証明書 (実行 A C) について説明する。

20

【 0 4 1 8 】

(6 - 1) 実行属性証明書概要

上述したグループ属性証明書、あるいは従来から知られる一般的な属性証明書は、所有者の属性としての権限情報等、属性証明書の格納データが改竄されていないことを署名検証により検証することができる。以下、説明する実行属性証明書 (実行 A C) は、検証により、証明書が改竄されていないことの確認を実行するのみならず、さらに、証明書所有者が実行属性証明書に格納した暗号化データ (プログラム) を復号して、暗号化データ (プログラム) の復号に基づいてサービスを受領する構成を持つ。

【 0 4 1 9 】

実行属性証明書に格納した暗号化データ (プログラム) を復号するために適用する鍵 (登録鍵) は、実行属性証明書発行者と、実行属性証明書の所有者としてのサービス受領者に対応するユーザデバイスのセキュリティチップ (S C) のみが知り得る秘密の共通鍵である。従って、特定のユーザデバイスにおいてのみ実行属性証明書に基づくサービス実行が可能となる。

30

【 0 4 2 0 】

なお、以下の説明においては、ユーザデバイスであるエンドエンティティ (E E) のセキュリティチップ (S C) が実行属性証明書の処理を行なうものとして説明するが、以下に説明するセキュリティチップ (S C) での処理は、前述したグループ属性証明書における処理と同様、ユーザ識別デバイス (U I D) のユーザセキュリティチップ (U S C) においても同様に実行可能な処理である。

40

【 0 4 2 1 】

実行属性証明書は、図 5 8 (a) に示すように、提供サービスの実行に必要なプログラム等の実行命令を登録鍵で暗号化したデータと、登録鍵を格納したセキュリティチップのメモリ、例えば図 5 8 (c) に示すセキュリティチップの E E P R O M 2 0 6 内に形成される共通鍵メモリ領域 2 0 7 における登録鍵格納領域を示すアドレスデータとしてのメモリ領域ブロックアドレスを有する。その他、各種の属性証明書データ (図 5 参照) を有し、発行者署名を付したものである。データの改竄検証は、署名検証により実行可能である。署名生成、検証処理は、先に図 1 7、図 1 8 を参照して説明した処理に従って実行可能である。

50

【 0 4 2 2 】

なお、実行属性証明書は、属性証明書の基本フォーマット、例えばITU-T X.509に準拠したものとして構成可能である。ただし、ITU-T X.509で規定されたフォーマットに従うことが必須ではなく、独自フォーマットとした実行属性証明書を構成してもよい。

【 0 4 2 3 】

セキュリティチップ（SC）の共通鍵メモリ領域207には、図58（b）に示すように、ユーザデバイスとしてのエンドエンティティ（EE）の有する複数の実行属性証明書に対応する複数の登録鍵が所定のブロックアドレスに対して格納される。

【 0 4 2 4 】

共通鍵メモリ領域207は、例えば64ビットなどある固定されたサイズのブロックから構成される不揮発性メモリのメモリ領域である。登録鍵の格納処理、およびリセット処理は、所定の手続きに従って実行される。この処理については後述する。リセット命令を除き、登録鍵格納メモリ領域へのアクセスは、アクセスするブロックに格納された登録鍵で暗号化された命令を用いることによってのみ実行可能となる。また、秘密鍵についても、秘密鍵を読み出せない仕組みに加え、入力したデータを秘密鍵で暗号化または復号化した結果を直接読み出すことは出来ないような、仕組みを持っているものとする。ここで、直接読み出すことが出来ないというのは、例えば、ハッシュをかけた後、秘密鍵で暗号化することや、公開鍵で暗号化した命令を、秘密鍵で復号して実行することはできることを意味する。以下、実行属性証明書の所有者であるセキュリティチップあるいはモジュールは、この仕組みを持つものとする。

【 0 4 2 5 】

実行属性証明書の利用手続き概要を図59に示すフローに従って説明する。図59は、例えば実行属性証明書の発行者としてのサービスプロバイダ（SP）と、実行属性証明書によるサービス受領者としてのユーザデバイスにおける処理の該略を示すフローである。ステップS501において、サービスプロバイダ（SP）とユーザデバイス間で相互認証が実行され、ステップS502において、例えば前述したグループ属性証明書に基づくサービス利用権限の審査が実行される。ここでの処理は、前述したグループ属性証明書における認証処理、検証処理と同様であり、認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部（図9参照）を中心とした処理として例えば先に図13を参照して説明した公開鍵方式の相互認証処理として実行される。検証処理は、先に図21乃至図23を参照して説明した、属性証明書の署名検証、関連の公開鍵証明書（PKC）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

【 0 4 2 6 】

次にステップS503の処理として、実行属性証明書（実行AC）に基づくサービス提供処理が行なわれる。実行属性証明書（実行AC）に基づくサービス提供処理は、ステップS504に示す実行属性証明書（実行AC）の発行処理、ステップS505に示す実行属性証明書（実行AC）の適用処理、ステップS506に示す実行属性証明書（実行AC）の破棄処理のいずれかの態様で実行されることになる。以下、これらの処理の詳細について、図を参照して説明する。

【 0 4 2 7 】

（ 6 - 2 ） 実行属性証明書発行処理

まず、実行属性証明書発行処理について説明する。図60に実行属性証明書の発行シーケンス図を示す。図60において、

EE：ユーザデバイスのエンドエンティティ（EE）制御部、

SC：EE内に構成されるセキュリティチップ、

実行ACテーブル：実行ACの管理テーブル格納メモリおよびメモリ制御部

SP：実行ACの発行処理を実行するサービスプロバイダ機器（SP）制御部、

SM：SP内のセキュリティモジュール、

である。

【 0 4 2 8 】

まず、ステップS511において、ユーザがユーザデバイスとしてのエンドエンティティ（EE）の入力インタフェースを介して、実行属性証明書（実行AC）発行要求コマンドを入力する。エンドエンティティ（EE）がユーザからの実行属性証明書の発行要求を受領すると、ステップS512において、セキュリティチップ（SC）と、サービスプロバイダ（SP）のセキュリティモジュール（SM）間の相互認証、および実行属性証明書（実行AC）発行条件として適用される発行済みのグループ属性証明書の検証、審査処理が行なわれる。

【0429】

認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部（図9参照）を中心とした処理として例えば先に図13を参照して説明した公開鍵方式の相互認証処理として実行される。検証処理は、先に図21乃至図23を参照して説明した、属性証明書の署名検証、関連の公開鍵証明書（PKC）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

10

【0430】

なお、ここでは、エンドエンティティ（EE）のセキュリティチップ（SC）を発行対象とした実行属性証明書の発行処理例を示してあるが、ユーザ識別デバイス（UID）のユーザセキュリティチップ（USC）を発行対象とした実行属性証明書発行処理の場合は、

（1）EEのSCとSP-SMとの相互認証、

（2）EEのSCとUIDのUSCとの相互認証、

（3）UIDのUSCとSP-SMとの相互認証、

20

のすべてを実行することになる。あるいは、簡便な方式として、UIDがEEに接続されることで、EEは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（2）の相互認証の省略が可能となる。さらに、上記3種の相互認証の様々な組み合わせによる認証構成が可能である。

【0431】

ステップS512の認証、グループ属性証明書の検証、審査がすべて成立すると、サービスプロバイダ（SP）は、ユーザデバイスのエンドエンティティ（EE）に対して、登録鍵生成実行AC生成情報要求処理を行なう。これは、具体的には、実行属性証明書の実行命令（図58参照）の暗号化、復号化処理に適用する登録鍵の格納領域として使用するメモリのメモリ領域空きアドレスを要求する処理である。

30

【0432】

エンドエンティティ（EE）は、登録鍵生成実行AC生成情報要求を受信すると、ステップS514において、登録鍵の格納領域として使用するメモリのメモリ領域空きアドレス検索を実行ACテーブル制御部に対して出力し、実行ACテーブル（制御部）がこの要求に応じて、実行ACテーブルを参照して、新規登録用の登録鍵を格納すべきメモリ領域空きアドレスをエンドエンティティに通知する。実行ACテーブルは、例えば図62に示すように、サービスプロバイダの識別データとしてのSP情報、サービスプロバイダの提供するサービス情報、例えば暗号化コンテンツ情報、サービスプロバイダの提供するサービス情報利用のために必要となるプログラムを実行命令として格納した実行ACとを対応付けたテーブルである。実行ACテーブルは、エンドエンティティ（EE）またはセキュリティチップ（SC）内のメモリに格納される。

40

【0433】

実行ACテーブル（制御部）は、すでに格納済みの実行ACに対応する登録鍵のメモリ領域ブロックアドレスを参照して、自己のセキュリティチップにおける空きアドレスを検出して、新規登録用の登録鍵を格納すべきメモリ領域空きアドレスをエンドエンティティに通知する。実行ACテーブル制御部は、実行ACテーブルを格納したメモリのアクセス制御、データ抽出を実行し、エンドエンティティ（EE）またはセキュリティチップ（SC）のメモリアccess制御処理を実行するCPU等により構成される制御部である。

【0434】

エンドエンティティ（EE）は、ステップS516において、空きアドレスをサービスプ

50

ロバイダ (S P) に送信する。新規登録鍵のメモリ領域ブロックアドレスを受信したサービスプロバイダ (S P) は、ステップ S 5 1 7 において、登録鍵生成実行 A C の生成要求をセキュリティモジュール (S M) に出力し、ステップ S 5 1 8 において、セキュリティモジュール (S M) は、登録鍵生成実行 A C の生成処理を行なう。サービスプロバイダ (S P) からセキュリティモジュール (S M) に対して出力される登録鍵生成実行 A C の生成要求には、セキュリティチップ公開鍵 (K p S C) を格納したセキュリティチップ公開鍵証明書、登録鍵のリセット時に適用するリセット鍵 (K r e s e t)、登録鍵生成命令 (G e n K e r)、メモリ領域ブロックアドレス (A d) が含まれる。

【 0 4 3 5 】

図 6 3 を参照して、セキュリティモジュール (S M) における登録鍵生成実行 A C の生成処理の詳細を説明する。

【 0 4 3 6 】

セキュリティモジュール (S M) 6 0 1 は、先に図 9 を参照して説明したセキュリティチップ構成と同様の構成であり、図 6 3 は、その構成中の暗号処理部、メモリ部を抽出して示すものである。暗号処理部としては、公開鍵暗号エンジン 6 0 2、共通鍵暗号エンジン 6 0 3 を有する。セキュリティモジュール (S M) 6 0 1 は、先に、図 9 を参照して説明したように、C P U、R A M、R O M 等の構成を持ち、その他のデータ処理、データ入出力処理が可能である。

【 0 4 3 7 】

公開鍵暗号エンジン 6 0 2 は、楕円曲線暗号、あるいは R S A (R i v e s t - S h a m i r - A d l e m a n) 暗号処理等の公開鍵方式の暗号処理を実行し、データの暗号化、復号化、署名生成、検証処理等を行なう。共通鍵暗号エンジン 6 0 3 は、例えば D E S、トリプル D E S 等の共通鍵暗号方式の暗号処理を実行し、データの暗号化、復号化等を行なう。なお、セキュリティモジュール (S M) 6 0 1 は、さらにハッシュ生成処理、乱数発生処理機能を持つ。

【 0 4 3 8 】

セキュリティモジュール (S M) は、上述したように登録鍵生成実行 A C 生成要求に伴い、セキュリティチップ公開鍵 (K p S C) を格納したセキュリティチップ公開鍵証明書、登録鍵のリセット時に適用するリセット鍵 (K r e s e t)、登録鍵生成命令 (G e n K e r)、メモリ領域ブロックアドレス (A d) を入力する。

【 0 4 3 9 】

ステップ S 5 4 1 の乱数発生処理において、発生した乱数に基づくセッション鍵 (K c s) と登録鍵生成命令 (G e n K e r) がステップ S 5 4 2 において、セキュリティチップ公開鍵 (K p S C) を用いて暗号化され、暗号化データ (E p (G e n K c r || K c s ; K p S C)) が生成される。なお、a || b は a、b の連結データを示し、E p (a ; b) は、鍵 b を適用した a の公開鍵暗号方式に基づく暗号化メッセージを示す。

【 0 4 4 0 】

次に、ステップ S 5 4 3 において、実行命令付加処理が行なわれる。D p c [a] は、公開鍵暗号方式に基づく秘密鍵による復号に基づいてデータ a 内のコマンドを実行する実行命令を示す。さらに、ステップ S 5 4 4 において、リセット鍵 (K r e s e t) に基づく共通鍵方式の暗号化処理が実行され、暗号化データ (E c (D p c [E p (G e n K c r || K c s ; K p S C)] ; K r e s e t)) が生成される。なお、E c (a ; b) は、鍵 b を適用した a の共通鍵暗号方式に基づく暗号化メッセージを示す。

【 0 4 4 1 】

さらに、ステップ S 5 4 5 において、上記暗号化データ (E c (D p c [E p (G e n K c r || K c s ; K p S C)] ; K r e s e t)) と、新規登録鍵の格納領域を示すメモリ領域ブロックアドレス (A d) との連結データに対して、セキュリティモジュール (S M) の秘密鍵 (K s S M) を適用した署名処理が実行される。これらの処理の結果、登録鍵生成実行 A C 6 1 1 が生成される。

【 0 4 4 2 】

登録鍵生成実行 A C 6 1 1 は、

10

20

30

40

50

新規登録鍵の格納領域を示すメモリ領域ブロックアドレス (Ad)、暗号化データ (Ec (Dpc [Ep (GenKcr || Kcs ; KpSC)] ; Kreset))、および、署名データ、Ep (H (Ad || Ec (Dpc [Ep (GenKcr || Kcs ; KpSC)] ; Kreset ; KsSM))を含む構成となる。なお、H(a)は、aのハッシュ値を示す。

【0443】

図60のシーケンス図に戻り、説明を続ける。ステップS518においてセキュリティモジュール(SM)における登録鍵生成実行AC生成処理が終了すると、セキュリティモジュール(SM)からサービスプロバイダ(SP)に登録鍵生成実行ACが送付され、ステップS519において、サービスプロバイダ(SP)から、ユーザデバイスのエンドエンティティ(EE)に登録鍵生成実行ACが送付される。

10

【0444】

ステップS520において、ユーザデバイスのエンドエンティティ(EE)は、実行ACテーブル(図62参照)の更新要求を実行ACテーブル(制御部)に送信し、実行ACテーブル(制御部)は、ステップS521において実行ACテーブル更新を行なう。実行ACテーブル(図62参照)の更新要求には、新規登録鍵を適用して利用可能なコンテンツ情報、サービスプロバイダ情報、メモリ領域ブロックアドレスが含まれ、実行ACテーブルに対する新規エントリデータとして、これらの情報を登録する。

20

【0445】

さらに、ユーザデバイスのエンドエンティティ(EE)は、ステップS522において、セキュリティチップ(SC)に対して、登録鍵生成要求を出力する。この要求は、登録鍵生成実行ACをセキュリティチップ(SC)に対して送付する処理として行われる。

【0446】

セキュリティチップ(SC)は、ステップS523において登録鍵生成処理を実行する。セキュリティチップで実行される登録鍵生成実行ACに基づく登録鍵生成処理について、図64を参照して説明する。

【0447】

セキュリティチップ(SC)605は、先に図9を参照して説明したセキュリティチップ構成と同様の構成である。ただし、図58において説明したように、共通鍵メモリ領域を有する。図64は、その構成中の暗号処理部、メモリ部を抽出して示すものである。暗号処理部としては、公開鍵暗号エンジン606、共通鍵暗号エンジン607を有し、メモリ部として共通鍵メモリ領域608を有する。セキュリティチップ(SC)605は、先に、図9を参照して説明したように、CPU、RAM、ROM等の構成を持ち、その他のデータ処理、例えば暗号処理部において復号された実行命令に基づくデータ処理、データ入出力処理等も実行可能である。例えば共通鍵メモリ608に対するデータの書き込み、読み取り、外部からのデータ入力、外部へのデータ出力、各素子間のデータ転送等のデータ処理はCPUの制御を中心として実行される。

30

【0448】

公開鍵暗号エンジン606は、楕円曲線暗号、あるいはRSA(Rivest-Shamir-Adleman)暗号処理等の公開鍵方式の暗号処理を実行し、データの暗号化、復号化、署名生成、検証処理等を行なう。共通鍵暗号エンジン607は、例えばDES、トリプルDES等の共通鍵暗号方式の暗号処理を実行し、データの暗号化、復号化等を行なう。共通鍵メモリ領域608は、登録鍵を格納するメモリであり、例えば64ビットなどある固定されたサイズのブロックから構成される不揮発性メモリからなるメモリである。なお、セキュリティチップ(SC)605は、さらにハッシュ生成処理、乱数発生処理機能を持つ。

40

【0449】

セキュリティチップ(SC)は、上述したようにエンドエンティティからの登録鍵生成要求に伴い、登録鍵生成実行AC611を入力する。

【0450】

50

ステップS551において、リセット鍵(Kreset)を適用した共通鍵方式の復号処理によって、登録鍵生成実行AC611の実行命令データ(Dpc[Ep(GenKcr||Kcs;KpSC)])が取り出され、さらに、ステップS552において、復号した実行命令に対応するデータ処理として、セキュリティチップの秘密鍵(KsSC)を適用した公開鍵方式の復号処理によって、登録鍵生成命令(GenKer)と、セッション鍵(Kcs)との連結データが取り出される。

【0451】

次のステップS553も、復号実行命令に対応するデータ処理であり、登録鍵生成命令(GenKer)の実行処理ステップである。ステップS554において乱数に基づく登録鍵(Kcr)を生成し、ステップS555において、登録鍵(Kcr)を登録鍵の格納領域アドレスであるメモリ領域ブロックアドレス(Ad)に従って、共通鍵メモリ領域608に書き込む。

【0452】

さらに、ステップS556において、登録鍵(Kcr)とメモリ領域ブロックアドレス(Ad)との連結データをセッション鍵(Kcs)で暗号化して、登録鍵生成結果612として、エンドエンティティ(EE)に出力する。

【0453】

登録鍵生成結果612のエンドエンティティ(EE)への出力ステップは図61におけるステップS524に相当する。

【0454】

登録鍵(Kcr)とメモリ領域ブロックアドレス(Ad)との連結データをセッション鍵(Kcs)で暗号化した登録鍵生成結果は、ユーザデバイスのエンドエンティティ(EE)から、サービスプロバイダ(SP)に送信される。

【0455】

サービスプロバイダ(SP)は、登録鍵生成結果を受信すると、ステップS526において、登録鍵生成結果をセキュリティモジュール(SM)に送付することにより、サービス提供実行ACの生成要求を行なう。セキュリティモジュール(SM)は、ステップS527において、サービス提供実行ACの生成処理を実行する。

【0456】

セキュリティモジュール(SM)によるサービス提供実行ACの生成処理を図65を参照して説明する。

【0457】

まず、ステップS561において、セッション鍵(Kcs)を適用して、登録鍵生成結果の復号処理を実行し、登録鍵(Kcr)とメモリ領域ブロックアドレス(Ad)との連結データ(Ad||Kcr)を取得する。さらに、ステップS562において、サービス提供実行ACに格納する実行命令(DecEData||Kcd)613を登録鍵(Kcr)を適用して暗号化する。なお、実行命令は、サービス提供実行ACに応じて設定される実行プログラム等の実行命令である。ここでは、データ復号鍵(Kcd)と、暗号化データの復号命令(DecEData)との連結データによって構成された実行命令を例として示している。

【0458】

さらに、ステップS563において、実行命令(DecEData||Kcd)613を登録鍵(Kcr)で暗号化したデータ(Ec(DecEData||Kcd);Kcr)と、登録鍵(Kcr)を格納するユーザデバイスにおけるセキュリティチップのメモリ領域ブロックアドレス(Ad)とのデータに対して、セキュリティモジュールの秘密鍵(KsSM)によって署名(図17参照)が生成され、サービス提供実行AC614が生成される。ここでは、サービス提供実行AC614は、暗号化データの復号処理をサービスとして実行する実行属性証明書である。

【0459】

この実行属性証明書に格納される実行命令を復号するためには、登録鍵(Kcr)の適用

10

20

30

40

50

が必須となり、登録鍵の情報を有するのは、ここでは、このサービス提供実行 A C の生成プロセスに参加しているユーザデバイスのセキュリティチップ (S C) およびサービスプロバイダのセキュリティモジュール (S M) のみとなる。

【 0 4 6 0 】

図 6 1 に戻りシーケンス図の説明を続ける。ステップ S 5 2 7 において、セキュリティモジュール (S M) がサービス提供実行 A C を生成すると、サービス提供実行 A C はステップ S 5 2 8 において、サービスプロバイダ (S P) からユーザデバイスのエンドエンティティ (E E) に送付され、さらに、ステップ S 5 2 9 において、実行 A C テーブル制御部に送付されて、ステップ S 5 3 0 において、実行 A C テーブル (図 6 2 参照) 内に格納される。

10

【 0 4 6 1 】

上述のプロセスにより、図 5 8 (a) に示すように、登録鍵を格納したユーザデバイスのセキュリティチップのメモリ領域ブロックアドレスと、その登録鍵で暗号化された実行命令と、さらに発行者署名、以上の各データを有する実行属性証明書 (実行 A C) がユーザデバイスに格納されることになる。なお、これらのデータ以外にも、先に図 5 を参照して説明したグループ属性証明書の各フィールドのデータを格納することは任意である。ただし、署名は、改竄チェック対象となるデータ全体に対して実行することが必要となる。

【 0 4 6 2 】

(6 - 3) 実行属性証明書適用処理

次に、上述の手続きにおいて発行された実行属性証明書の適用処理について説明する。図 6 6 は、サービス提供実行 A C のユーザデバイス側における適用シーケンスをまとめた図である。すでに、前述の処理によって、ユーザデバイスの実行 A C テーブルにサービス提供実行 A C が格納済みである。

20

【 0 4 6 3 】

ステップ S 5 7 1 において、ユーザがエンドエンティティ (E E) のユーザインタフェースを介してサービス提供実行 A C の適用処理要求を入力する。この処理要求には、実行 A C の識別子、またはサービスプロバイダ (S P) 情報、サービス内容を特定するデータ、例えば利用コンテンツ、利用プログラムの指定データが含まれる。エンドエンティティ (E E) は、ステップ S 5 7 2 において、ユーザ指定のサービス提供実行 A C の検索要求を実行 A C テーブルに出力する。検索キーは、例えばコンテンツ情報やサービスプロバイダ (S P) 情報等である。

30

【 0 4 6 4 】

ステップ S 5 7 3 において、実行 A C テーブルは、エンドエンティティからの入力キーに基づいて、対応するサービス提供実行 A C を検索し、ステップ S 5 7 4 において、テーブルから抽出したサービス提供実行 A C をエンドエンティティ (E E) に出力する。

【 0 4 6 5 】

ステップ S 5 7 5 において、エンドエンティティ (E E) は、受領 A C をセキュリティチップ (S C) に出力し、サービス提供実行 A C の適用処理要求を行なう。セキュリティチップは、ステップ S 5 7 6 において、受領 A C の提供処理、すなわち、実行属性証明書 (実行 A C) に従ったサービス提供を行なう。

40

【 0 4 6 6 】

セキュリティチップ (S C) におけるステップ S 5 7 6 のサービス提供処理の詳細を図 6 7 を参照して説明する。セキュリティチップ 6 0 5 は、サービス提供実行 A C 6 1 4 を入力する。

【 0 4 6 7 】

サービス提供実行 A C 6 1 4 は、実行命令 (D e c E D a t a || K c d) を登録鍵 (K c r) で暗号化したデータ (E c (D e c E D a t a || K c d) ; K c r) と、登録鍵 (K c r) を格納するユーザデバイスにおけるセキュリティチップのメモリ領域ブロックアドレス (A d) と、各データに対して、セキュリティモジュールの秘密鍵 (K s S M) によって署名したデータを含む。

50

【0468】

セキュリティチップ605は、ステップS581において、サービス提供実行AC内のメモリ領域ブロックアドレス(Ad)に従って、共通鍵メモリ領域608から登録鍵(Kcr)を取得し、取得した登録鍵(Kcr)によって、サービス提供実行AC内の暗号化データ(Ec(DecEData||Kcd);Kcr)の復号処理を実行し、データ復号鍵(Kcd)と、暗号化データの復号命令(DecEData)を取得する。

【0469】

ステップS582において、復号した実行命令に基づくデータ処理が実行される。すなわち、データ復号鍵(Kcd)を適用して、外部から入力される復号対象の暗号化データ(Ec(データ;Kcd))615の復号処理を実行し、復号されたデータ616を出力する。復号対象の暗号化データ(Ec(データ;Kcd))615は、例えば画像、音楽、プログラム等のコンテンツを、鍵(Kcd)により暗号化したデータであり、サービス提供実行AC内の格納実行命令を登録鍵(Kcr)によって復号することによって取得可能なデータ復号鍵(Kcd)によって復号可能となる。

10

【0470】

図66のシーケンス図に戻り説明を続ける。ステップS576のサービス提供の後、セキュリティチップ(SC)は、ステップS577において、登録鍵破棄処理を行なう。この登録鍵破棄処理は、サービス提供実行ACに応じて実行する場合と実行不要となる場合とがある。サービス提供実行ACに基づくサービス提供処理を一度限りとして設定した実行ACである場合は、この破棄処理をサービス提供処理に続いて実行する。

20

【0471】

ステップS577のSC(セキュリティチップ)登録鍵破棄処理について、図68を参照して説明する。登録鍵のリセット処理は、共通鍵メモリ領域608の登録鍵の格納領域にリセット鍵(Kreset)を上書きすることによって行われる。破棄対象となる登録鍵(Kcr)のメモリ領域ブロックアドレス(Ad)とリセット鍵(Kreset)とからなるリセット処理命令617が例えばエンドエンティティ(EE)から入力されると、ステップS583において、リセット処理命令617に格納されたメモリ領域ブロックアドレス(Ad)に対応するメモリ領域に、リセット鍵(Kreset)の書き込み処理が実行され、登録鍵の削除が完了する。

【0472】

図66のシーケンス図に戻り説明を続ける。ステップS577において、登録鍵の破棄が完了すると、ステップS578において登録鍵破棄通知がエンドエンティティ(EE)に出力され、エンドエンティティ(EE)は、ステップS579において、実行ACテーブルに対してサービス提供実行ACの削除要求を出力し、実行ACテーブル(制御部)は、実行ACテーブルから対応する実行ACを削除する。

30

【0473】

(6-4)登録鍵リセット処理

なお、登録鍵の破棄処理は、サービス提供実行ACの提供処理に続いて実行されとは限らず、任意タイミングのリセット要求に基づいて登録鍵の破棄処理としてのリセット処理を実行することが可能である。このリセット要求に基づく処理について、図69を参照して説明する。

40

【0474】

ステップS601において、ユーザがエンドエンティティ(EE)のユーザインタフェースを介してユーザデバイスに格納されているサービス提供実行ACに対応する登録鍵のリセット要求を入力する。エンドエンティティ(EE)は、ステップS602において、実行ACテーブルに検索要求を出力する。リセット要求の態様は2通ある。第1の態様は、ユーザが実行ACテーブルのあるメモリ領域ブロックアドレスに書き込んだサービス内容を忘れた場合、メモリ領域ブロックアドレスをキーとして実行ACテーブルを検索し、出力されたSP情報・コンテンツ情報に対応する登録鍵をユーザが不要であると判断するとリセット実行要求を行う態様である。この処理要求には、例えば実行ACの識別子、また

50

はサービス内容を特定するデータ、例えばコンテンツ、プログラム、あるいはサービスプロバイダ（ＳＰ）情報データが含まれる。第２の態様は、ユーザがＳＰ情報・コンテンツ情報を既知の場合、これらをキーとして実行ＡＣテーブルを検索し、出力されたメモリ領域ブロックアドレスをリセット実行要求と共にＳＣへ送信する態様である。なお、登録鍵のメモリ領域ブロックアドレスは、コンテンツ、あるいはサービスプロバイダに対応するデータとしてエンドエンティティにおいて、任意に格納することが可能である。

【０４７５】

ステップＳ６０３において、実行ＡＣテーブルは、エンドエンティティからの入力キーに基づいて、対応するサービス提供実行ＡＣを検索し、サービス提供実行ＡＣに対応するサービスプロバイダ、利用可能コンテンツを検索し、ステップＳ６０４において、エンドエンティティ（ＥＥ）に出力する。

10

【０４７６】

エンドエンティティ（ＥＥ）では、サービスプロバイダ、利用可能コンテンツ情報を表示し、ユーザが不要であると判定すると、ステップＳ６０６において、セキュリティチップに対してリセット実行要求を出力する。

【０４７７】

登録鍵のリセット処理は、共通鍵メモリ領域の登録鍵の格納領域にリセット鍵（Ｋｒｅｓｅｔ）を上書きすることによって行われ、破棄対象となる登録鍵（Ｋｃｒ）のメモリ領域ブロックアドレス（Ａｄ）とリセット鍵（Ｋｒｅｓｅｔ）とからなるリセット処理命令をエンドエンティティ（ＥＥ）から入力し、ステップＳ６０７において、先に図６８を参照して説明した通りの、メモリ領域ブロックアドレス（Ａｄ）に対応するメモリ領域に、リセット鍵（Ｋｒｅｓｅｔ）の書き込み処理が実行され、登録鍵がリセットされる。ステップＳ６０７において、登録鍵のリセットが完了すると、ステップＳ６０８においてリセット完了通知がエンドエンティティ（ＥＥ）に出力される。

20

【０４７８】

（６－５）実行属性証明書リセット（破棄）処理

次に、ユーザデバイスに格納された実行属性証明書を破棄し、破棄が間違いなく実行されたことをサービスプロバイダに通知する実行属性証明書リセット（破棄）処理について説明する。

【０４７９】

30

図７０、図７１の処理シーケンス図に従って説明する。図７０、図７１において、

ＥＥ：ユーザデバイスのエンドエンティティ（ＥＥ）制御部、

ＳＣ：ＥＥ内に構成されるセキュリティチップ、

実行ＡＣテーブル：実行ＡＣの管理テーブル格納メモリおよびメモリ制御部

ＳＰ：実行ＡＣの発行処理を実行するサービスプロバイダ機器（ＳＰ）制御部、

ＳＭ：ＳＰ内のセキュリティモジュール、

である。

【０４８０】

まず、ステップＳ６１１において、ユーザがエンドエンティティ（ＥＥ）の入力インタフェースを介して、実行属性証明書（実行ＡＣ）破棄申請要求コマンドを入力する。この要求に基づき、実行属性証明書破棄申請がサービスプロバイダに送信される。申請には、例えば実行属性証明書（実行ＡＣ）ＩＤ、あるいはコンテンツ、サービス指定データ等、破棄対象とする実行属性証明書（実行ＡＣ）を特定可能なデータが含まれる。

40

【０４８１】

サービスプロバイダ機器制御部（ＳＰ）が実行属性証明書破棄申請を受領すると、ステップＳ６１２において、セキュリティチップ（ＳＣ）と、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証、および、必要に応じて実行属性証明書（実行ＡＣ）破棄処理条件として適用されるサービスプロバイダに発行済みのグループ属性証明書の検証、審査処理が行なわれる。実行属性証明書破棄処理をひとつのサービスと見立てた場合、エンドエンティティがサービスプロバイダの役割をになうことになる。

50

【 0 4 8 2 】

認証処理は、セキュリティチップ、セキュリティモジュールの暗号処理部（図 9 参照）を中心とした処理として例えば先に図 1 3 を参照して説明した公開鍵方式の相互認証処理として実行される。検証処理は、先に図 2 1 乃至図 2 3 を参照して説明した、属性証明書の署名検証、関連の公開鍵証明書（P K C）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

【 0 4 8 3 】

なお、ここでは、エンドエンティティ（E E）のセキュリティチップ（S C）を発行対象とした実行属性証明書の破棄処理例を示してあるが、ユーザ識別デバイス（U I D）のユーザセキュリティチップ（U S C）を発行対象とした実行属性証明書の破棄処理の場合は

10

- （ 1 ） E E の S C と S P - S M との相互認証、
- （ 2 ） E E の S C と U I D の U S C との相互認証、
- （ 3 ） U I D の U S C と S P - S M との相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、U I D が E E に接続されることで、E E は基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（ 2 ）の相互認証の省略が可能となる。さらに、上記 3 種の相互認証の様々な組み合わせによる認証構成が可能である。

【 0 4 8 4 】

ステップ S 6 1 2 の認証、グループ属性証明書の検証、審査がすべて成立すると、ユーザデバイスのエンドエンティティ（E E）は、ステップ S 6 1 3 において、破棄対象の実行 A C の検索要求を実行 A C テーブルに出力する。検索キーは、例えばコンテンツ情報やサービスプロバイダ（S P）情報等である。

20

【 0 4 8 5 】

ステップ S 6 1 4 において、実行 A C テーブルは、エンドエンティティからの入力キーに基づいて、対応するサービス提供実行 A C を検索し、ステップ S 6 1 5 において、テーブルから抽出したサービス提供実行 A C をエンドエンティティ（E E）に出力する。さらに、実行 A C テーブル（制御部）は、ステップ S 6 1 6 において、破棄対象実行 A C のエントリを実行 A C テーブルから削除する。

【 0 4 8 6 】

ステップ S 6 1 7 において、エンドエンティティ（E E）は、セキュリティチップに対してリセット実行要求を出力する。ステップ S 6 1 8 において、登録鍵のリセット処理として、共通鍵メモリ領域の登録鍵の格納領域にリセット鍵（K r e s e t）を上書きする処理（図 6 8 参照）が実行され、リセット完了通知がエンドエンティティ（E E）に出力される。

30

【 0 4 8 7 】

さらに、エンドエンティティ（E E）は、図 7 1 に示すステップ S 6 2 1 において、リセット完了通知をサービスプロバイダ（S P）に送信する。このリセット完了通知は、破棄対象実行 A C を伴う。破棄対象実行 A C を受領したサービスプロバイダ（S P）は、ステップ S 6 2 2 において、リセット確認実行 A C の生成要求をセキュリティモジュール（S M）に出力する。この要求は破棄対象実行 A C を伴って実行される。

40

【 0 4 8 8 】

ステップ S 6 2 3 において、セキュリティモジュール（S M）は、破棄対象の実行 A C から、対応する登録鍵を格納したメモリ領域ブロックアドレス情報を抽出し、ステップ S 6 2 4 においてリセット確認実行 A C の生成処理を実行する。リセット確認実行 A C は、破棄対象の実行 A C の対応登録鍵を格納したメモリ領域ブロックアドレス情報（A d）と、リセット確認実行 A C によって、ユーザデバイスのセキュリティチップ（S C）において実行すべき命令としての実行命令と、発行者、すなわちセキュリティモジュール（S M）の署名とを含むデータ構成（図 7 2、リセット確認実行 A C 6 2 1 参照）である。

【 0 4 8 9 】

50

生成されたりセット確認実行ACは、ステップS625においてサービスプロバイダ(SP)からエンドエンティティ(EE)に送信され、さらに、ステップS626において、セキュリティチップ(SC)に転送される。

【0490】

セキュリティチップ(SC)では、ステップS627において、リセット確認実行ACに基づくリセット確認結果生成処理を実行する。ステップS627のリセット確認結果生成処理の詳細について図72を参照して説明する。

【0491】

図72に示すように、セキュリティチップ605は、ステップS641において、リセット確認実行ACの実行命令を、リセット確認実行AC621に格納されたアドレスに基づいて共通鍵メモリ領域608から取り出したリセット鍵(Kreset)を適用して復号し、セキュリティチップの公開鍵(KpSC)で暗号化されたデータ(Ep(ConfReset||Kcs;KpSC))の復号命令データ(Dpc[Ep(ConfReset||Kcs;KpSC)])を取得し、ステップS642において、セキュリティチップの秘密鍵(KsSC)を適用して復号し、リセット確認結果作成コマンド(ConfReset)、セッション鍵(Kcs)、を取得し、ステップS643のリセット確認結果作成処理を実行する。

【0492】

ステップS643のリセット確認結果作成処理では、まず、ステップS644において、リセット確認実行AC621に格納されたアドレスに基づいて共通鍵メモリ領域608からリセット鍵(Kreset)が読み出され、さらに、ステップS645において、メモリ領域ブロックアドレス情報(Ad)と、リセット鍵(Kreset)の連結データをセッション鍵(Kcs)で暗号化し、暗号化データ(Ec(Ad||Kreset;Kcs))からなるリセット確認結果622をエンドエンティティ(EE)に出力する。

【0493】

エンドエンティティ(EE)は、図71のステップS628においてリセット確認結果をサービスプロバイダ(SP)に送信し、サービスプロバイダ(SP)は、ステップS629においてリセット確認結果をセキュリティモジュール(SM)に送信し、セキュリティモジュール(SM)はサービスプロバイダ(SP)にリセット確認結果通知を送信して処理が終了する。

【0494】

上述した処理によって、発行済みの実行ACの破棄処理が、サービスプロバイダの確認の下に確実に実行されることになる。

【0495】

なお、登録鍵の破棄処理については、実行ACに基づいて行なうことが可能である。図73を参照して実行ACに基づく登録鍵の破棄処理について説明する。登録鍵実行ACは、例えば対応するサービス提供実行ACを発行したサービスプロバイダ(SP)によって発行され、ユーザデバイスのエンドエンティティ(EE)を介してセキュリティチップ(SC)に入力される。

【0496】

登録鍵破棄実行AC623は、図73に示すように、破棄対象となる登録鍵を格納した共通鍵メモリ領域のメモリ領域ブロックアドレス情報(Ad)、登録鍵で暗号化した登録鍵破棄コマンド(RevK)、発行者署名を持つ実行ACである。

【0497】

ステップS651において、登録鍵破棄実行AC623のメモリ領域ブロックアドレス情報(Ad)に基づいて、共通鍵メモリ領域608から取得した登録鍵(Kcr)に基づいて、登録鍵破棄実行AC623の実行命令を復号して、破棄コマンド(RevK)を取得して、ステップS652においてコマンドに基づく破棄処理を実行する。ステップS653では、登録鍵破棄実行AC623のメモリ領域ブロックアドレス情報(Ad)に基づいて、対応メモリ領域にリセット鍵(Kreset)が上書きされ、登録鍵が破棄(リセッ

10

20

30

40

50

ト)される。

【0498】

(7) 実行属性証明書の具体的利用処理

次に、上述した実行属性証明書(実行AC)を適用した具体的な利用処理について説明する。利用処理例として、以下の項目について各々説明する。

(7-1) 回数制限付きサービス提供実行属性証明書

(7-2) 譲渡機能付きサービス提供実行属性証明書

(7-3) 代理発行実行属性証明書

以下、上記項目毎に説明する。

【0499】

(7-1) 回数制限付きサービス提供実行属性証明書

まず、回数制限付きサービス提供実行属性証明書の適用処理について説明する。図74、図75に、回数制限付きサービス提供実行属性証明書をユーザデバイスにおいて適用してサービス、すなわち、回数制限付き暗号化データ、例えば画像、音楽、プログラム等のコンテンツを復号して利用する処理シーケンスを示す。各ステップに従って処理シーケンスについて説明する。

【0500】

ユーザデバイスには、すでに回数制限付きサービス提供実行属性証明書がメモリ、例えば前述した実行ACテーブルに格納されており、その残利用回数はn回であるものとする。回数制限付きサービス提供実行属性証明書の実行命令中に実行命令の適用可能回数識別値としての残利用回数データ(例えばn回)が記録される。記録例については後述する。

【0501】

ステップS701において、ユーザがエンドエンティティ(EE)のユーザインタフェースを介してサービス提供実行AC、この例では、暗号化データ復号実行ACの適用処理要求を入力する。この処理要求には、実行ACの識別子、またはサービスプロバイダ(SP)情報、サービス内容を特定するデータ、例えば利用コンテンツ指定データが含まれる。エンドエンティティ(EE)は、ステップS702において、ユーザ指定のサービス提供実行AC(暗号化データ復号実行AC)の検索要求を実行ACテーブルに出力する。検索キーは、例えばコンテンツ情報やサービスプロバイダ(SP)情報等である。

【0502】

ステップS703において、実行ACテーブルは、エンドエンティティからの入力キーに基づいて、対応する暗号化データ復号実行ACを検索し、ステップS704において、テーブルから抽出した暗号化データ復号実行ACをエンドエンティティ(EE)に出力する。この暗号化データ復号実行ACには、残利用回数 = n回の情報が記録されている。

【0503】

ステップS704において、エンドエンティティ(EE)は、受領ACをセキュリティチップ(SC)に出力し、サービス提供実行AC(暗号化データ復号実行AC)の適用処理要求を行なう。この適用処理は以下に行なう。まず、ステップS705において、暗号化データ復号実行ACの実行命令を登録鍵で復号して、復号鍵のセット処理を実行し、復号鍵セット完了通知をエンドエンティティ(EE)に出力(S706)し、EEにおいて、例えば外部メモリから復号対象の暗号化データを取得(S707)し、SCに対して復号要求を行ない(S708)、SCにおいてデータ復号処理を実行(S709)し、復号データをSCからEEに送信する(S710)データ復号処理を行ない、さらに、ステップS711において、暗号化データ復号実行AC中の実行命令中の残利用回数データをnからn-1に更新する。

【0504】

さらに、更新後の残利用回数の判定(S712)の後、残利用回数 1の場合は、図75(a)に示すシーケンスに従い、登録鍵の再生成、保存(S721)、暗号化データ復号実行ACの再生成(S722)、EEへの送信、EEからの暗号化データ復号実行AC保存要求(S723)に応じて、実行ACテーブルへの保存(S724)が実行される。

10

20

30

40

50

【0505】

一方、残利用回数 = 0 の場合は、図 75 (b) に示すシーケンスに従い、SC において、登録鍵の破棄処理 (S725) が実行され、EE に対する登録鍵破棄通知 (S726) の後、EE からの暗号化データ復号実行 AC 削除要求 (S727) に応じて、実行 AC テーブルの暗号化データ復号実行 AC 削除 (S728) が実行される。

【0506】

ステップ S705 以下のセキュリティチップ (SC) における処理を図 76 および図 77 を参照して説明する。図 76 は、更新後の残利用回数 1 の場合の処理であり、図 77 は、更新後の残利用回数 = 0 の場合の処理である。

【0507】

まず、図 76 を参照して、更新後の残利用回数 1 の場合のセキュリティチップ (SC) における処理について説明する。

【0508】

回数制限付きサービス提供実行属性証明書 701 は、実行命令 (Ec (DecEData || Kcd || NumTr (n) ; Kcr1)) と、実行命令を復号する登録鍵を格納した共通鍵メモリ領域におけるブロックアドレス (Ad) と、発行者署名を有する。実行命令には、暗号化データ復号コマンド (DecEData)、データ復号鍵 (Kcd)、残利用回数 (n) に応じた回数処理実行コマンド (NumTr (n)) が含まれ、登録鍵 (Kcr1) によってこれらのデータが暗号化された実行命令 (Ec (DecEData || Kcd || NumTr (n) ; Kcr1)) である。

【0509】

まず、セキュリティチップ (SC) は、ステップ S731 において、実行 AC 中のブロックアドレス (Ad) に基づいて共通鍵メモリ領域から取り出した登録鍵 (Kcr1) を適用して実行 AC 701 の実行命令を復号し、データ (DecEData || Kcd || NumTr (n)) を取り出して、さらに、ステップ S732 において、データ復号鍵 (Kcd) を適用して、外部から入力される暗号化コンテンツ等の暗号化データ 702 (Ec (Data ; Kcd)) の復号を実行して、復号コンテンツ (データ) 703 をエンドエンティティに出力する。

【0510】

さらに、ステップ S733 において、回数処理実行コマンド (NumTr (n)) に基づく処理を実行する。この処理は、残回数を更新した新たな回数制限付きサービス提供実行属性証明書 704 を生成することを目的とする処理である。

【0511】

乱数発生処理 (S734) により、新たな登録鍵 Kcr2 を生成し、これを元の回数制限付きサービス提供実行属性証明書 701 に書き込まれていたブロックアドレスに対応する共通鍵メモリ領域 608 に書き込む。これにより、先に書き込まれていた登録鍵 (Kcr1) が新たな登録鍵 (Kcr2) に置き換えられることになる。

【0512】

ステップ S736 において、回数処理実行コマンド (NumTr (n)) に基づいて抽出される残利用回数 = n をコンテンツの復号処理に伴い (-1) する更新を実行する。すなわち、実行命令中のデータ (DecEData || Kcd || NumTr (n)) を (DecEData || Kcd || NumTr (n - 1)) に書き替え、ステップ S737 において、新規生成登録鍵 (Kcr2) を適用した暗号化処理を実行する。この暗号化データは、新たな回数制限付きサービス提供実行属性証明書 704 中の実行命令 (Ec (DecEData || Kcd || NumTr (n - 1) ; Kcr2)) に相当する。

【0513】

ステップ S738 では、ブロックアドレス (Ad) と、ステップ S737 において生成した更新した残回数データを持つ実行命令に基づく電子署名をセキュリティチップの秘密鍵 (KsSC) によって実行し、新たな更新した回数制限付きサービス提供実行属性証明書 704 を生成する。この場合の署名は、セキュリティチップにおいてなされることになる

10

20

30

40

50

。

【0514】

この新たな回数制限付きサービス提供実行属性証明書704が、図75のステップS722においてセキュリティチップ(SC)からエンドエンティティ(EE)に出力後、ステップS724で実行ACテーブルに保存される。

【0515】

一方、図74の処理ステップS712の残利用回数審査において、残利用回数=0と判定された場合のセキュリティチップ(SC)における処理を図77を参照して説明する。

【0516】

回数制限付きサービス提供実行属性証明書705は、実行命令(Ec(DecEda||Kcd||NumTr(1);Kcr1))と、実行命令を復号する登録鍵を格納した共通鍵メモリ領域におけるブロックアドレス(Ad)と、発行者署名を有する。

10

【0517】

まず、セキュリティチップ(SC)は、ステップS741において、実行AC中のブロックアドレス(Ad)に基づいて共通鍵メモリ領域から取り出した登録鍵(Kcr1)を適用して実行AC705の実行命令を復号し、データ(DecEda||Kcd||NumTr(n))を取り出して、さらに、ステップS742において、データ復号鍵(Kcd)を適用して、外部から入力される暗号化コンテンツ等の暗号化データ706Ec(Data;Kcd)の復号を実行して、復号コンテンツ(データ)707をエンドエンティティに出力する。

20

【0518】

さらに、ステップS743において、回数処理実行コマンド(NumTr(1))に基づく処理を実行する。この処理は、さらなる実行ACを利用したサービス利用、すなわち暗号化データの復号を停止するため、登録鍵の破棄を実行する処理として行われる。すなわち、ステップS744において登録鍵(Kcr1)の破棄を実行する。登録鍵の破棄は、回数制限付きサービス提供実行属性証明書705に記録された登録鍵を格納した共通鍵メモリ領域中のブロックアドレス(Ad)の対応領域にリセット鍵を上書きする処理として実行される。

【0519】

この処理により、回数制限付きサービス提供実行属性証明書705の格納された実行命令を復号する登録鍵(Kcr1)が破棄され、実行命令を復号することが不可能になり、実行ACを適用したサービス利用が停止される。この処理の後、図75に示すステップS727, S728が実行されて、実行ACテーブルから対応する実行ACが削除される。

30

【0520】

(7-2)譲渡機能付きサービス提供実行属性証明書

次に、譲渡機能付きサービス提供実行属性証明書の適用処理について説明する。図78に、譲渡機能付きサービス提供実行属性証明書の適用処理、すなわち、ユーザデバイス間で譲渡機能付きサービス提供実行属性証明書に基づく処理を実行して、新たな譲渡機能付きサービス提供実行属性証明書、あるいはサービス提供実行ACを生成して他のユーザデバイス(譲渡先)に送付するとともに、自デバイス(譲渡元)の登録鍵を破棄する処理を行なうことで、他のユーザデバイスにおいて暗号化データ(例えば暗号化コンテンツ)を利用することを可能とした処理シーケンスを示す。

40

【0521】

図78において、

EE1: 譲渡元ユーザデバイスのエンドエンティティ(EE)制御部、

SC1: 譲渡元EE内に構成されるセキュリティチップ、

実行ACテーブル1: 譲渡元エンドエンティティ(EE)実行ACテーブル制御部、

EE2: 譲渡先ユーザデバイスのエンドエンティティ(EE)制御部、

SC2: 譲渡先EE内に構成されるセキュリティチップ、

実行ACテーブル2: 譲渡先エンドエンティティ(EE)実行ACテーブル制御部、

50

である。

【0522】

まず、ステップS752において、譲渡先のユーザがエンドエンティティ（EE2）の入力インタフェースを介して、譲渡機能付きサービス提供実行属性証明書に基づく譲渡処理、すなわち暗号化データの利用を譲渡先ユーザデバイスで実行可能とするための譲渡要求を入力する。譲渡要求には、譲渡機能付きサービス提供実行属性証明書のID、および所有者情報、あるいは利用コンテンツ（暗号化データ）、あるいはサービスプロバイダ情報等、適用する譲渡機能付きサービス提供実行属性証明書を特定するための情報が含まれる。

【0523】

エンドエンティティ（EE2）がユーザからの譲渡要求の入力を受領すると、エンドエンティティ（EE2）は、ステップS752において、譲渡機能付きサービス提供実行属性証明書を所有する譲渡元ユーザデバイスのエンドエンティティ（EE1）に対する接続要求を行ない、各ユーザデバイスのセキュリティチップ（SC1）、（SC2）間において相互認証を実行する。これは例えば先に図13を参照して説明した公開鍵方式の相互認証処理として実行される。

【0524】

相互認証が成立すると、ステップS753において、譲渡元のユーザデバイスのエンドエンティティ（EE1）は、指定された譲渡機能付きサービス提供実行属性証明書の検索要求を実行ACテーブル1に出力する。検索キーは、例えばコンテンツ情報やサービスプロバイダ（SP）情報等である。

【0525】

ステップS754において、実行ACテーブル1は、エンドエンティティ（EE1）からの入力キーに基づいて、対応する譲渡機能付きサービス提供実行属性証明書を検索し、テーブルから抽出した実行ACをエンドエンティティ（EE）に出力する。

【0526】

ステップS755において、エンドエンティティ（EE）は、受領ACをセキュリティチップ（SC）に出力し、譲渡機能付きサービス提供実行属性証明書の適用処理要求を行なう。セキュリティチップは、ステップS756において、受領ACの処理、すなわち、実行属性証明書（譲渡機能付きサービス提供実行属性証明書）に格納されたアドレス（Ad）によって指定された領域から取得される登録鍵に基づく実行命令の復号（S756）を行なう。

【0527】

さらに、ステップS757において、エンドエンティティ（EE1）から譲渡処理要求がセキュリティチップ（SC）に出力し、エンドエンティティ（EE1）はステップS758において、譲渡処理のために必要とするグループ属性証明書の提示を譲渡先のユーザデバイス（EE2）に対して要求する。このグループ属性証明書は、例えば、譲渡機能付きサービス提供実行属性証明書を生成発行したサービスプロバイダ（SP）によって管理された譲渡可能ユーザデバイスあるいはユーザのグループであることを証明するグループ属性証明書等である。

【0528】

譲渡先ユーザデバイスのエンドエンティティ（EE2）は、ステップS759において、指定のグループ属性証明書（Gp.AC）を譲渡元ユーザデバイスのエンドエンティティ（EE1）に送信し、エンドエンティティ（EE1）は、受領ACをセキュリティチップ（SC1）に転送し、セキュリティチップ（SC1）が、グループ属性証明書を検証する（S761）。この検証処理は、先に図21～図23を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。

【0529】

検証不成立の場合は、エラー処理として、その後の処理を実行せず処理を中止する。この場合、エラー通知を譲渡先エンドエンティティ（EE2）に送信する処理を行なってもよ

10

20

30

40

50

い。

【0530】

グループ属性証明書（Gp・AC）の検証が成功し、グループ属性証明書（Gp・AC）の正当性が確認されるとステップS762に進む。ステップS762では、譲渡先ユーザデバイスにおいて暗号化データの利用を可能とするための実行属性証明書の生成、送信が行なわれることになる。これらの処理は、先に図60、図61を参照して説明した登録鍵生成実行ACの生成、検証、サービス提供実行ACの生成送信に対応する処理であり、図60、図61におけるサービスプロバイダ（SP）の処理を譲渡元ユーザデバイスが実行するものである。

【0531】

ステップS762において、新たなサービス提供実行AC、この例では、サービス提供実行属性証明書が生成されて、譲渡先ユーザデバイスに送付される。さらに、ステップS763において、譲渡元ユーザデバイスが保有していた譲渡機能付きサービス提供実行属性証明書の実行命令を復号するために適用する登録鍵の削除が実行される。この処理は、前述したリセット鍵の上書きによって行なわれるものである。なおここでは、譲渡の機能について述べたが、登録鍵の削除を行わない実行属性証明書をを用いれば、譲渡ではなく複製の機能を持たせることが出来る。

【0532】

譲渡元ユーザデバイスのセキュリティチップ（SC1）で実行するステップS756の譲渡機能付きサービス提供実行属性証明書の復号処理以下の処理の詳細について、図79、図80を参照して説明する。

【0533】

譲渡機能付きサービス提供実行属性証明書（AC）711には、実行命令、実行命令を復号するための登録鍵を格納した共通鍵メモリ領域608のブロックアドレス（Ad1）、発行者署名の各データを有する。実行命令（Ec（Sel||Jdg（SDB）||GenAC（GenKcr）||GenAC（Ex）||RevK||DecEData||Kcd；Kcr1））には、処理選択コマンド（Sel）、検証審査コマンド（Jdg（SDB））、登録鍵生成実行AC作成コマンド（GenAC（GenKcr））、実行AC作成コマンド（GenAC（Ex））、登録鍵破棄コマンド（RevK）、暗号化データ復号コマンド（DecEData）、データ復号鍵（Kcd）が含まれ、これらを登録鍵（Kcr1）で暗号化したデータ構成である。

【0534】

なお、検証審査コマンド（Jdg（SDB））は、サービス情報データベース（SDB）に基づく実行ACの検証審査処理コマンドである。なお、サービス情報データベース（SDB）は、サービス提供に必要なAC情報、および先に説明したグループ情報データベース（図15参照）と同様のデータ構成を持ち、発行者、グループID、グループ情報の各データを有する。

【0535】

譲渡機能付きサービス提供実行属性証明書（AC）711を入力して、譲渡先に新たな譲渡機能付きサービス提供実行属性証明書を発行する処理を実行する譲渡元セキュリティチップ（SC）は、まず、譲渡機能付きサービス提供実行属性証明書（AC）711のアドレス（Ad1）に基づいて共通鍵メモリ領域608から登録鍵を取得し、譲渡機能付きサービス提供実行属性証明書（AC）711内の実行命令を復号する。次に、譲渡実行トリガ712をエンドエンティティから入力すると、ステップS772以下の譲渡実行処理を行なう。

【0536】

ここで、譲渡実行トリガ712は、譲渡機能付きサービス提供実行属性証明書（AC）711に基づく、譲渡処理を実行することのエンドエンティティからの要求処理を示す。譲渡機能付きサービス提供実行属性証明書（AC）711は、譲渡処理のみならず、暗号化データの復号処理の際にも適用される実行ACであり、そのいずれの処理を実行するかを

10

20

30

40

50

エンドエンティティからの要求（トリガ）によって選択する。譲渡機能付きサービス提供実行属性証明書（AC）711の実行命令（Ec（Sel||Jdg（SDB）||GenAC（GenKcr）||GenAC（Ex）||RevK||DecEData||Kcd；Kcr1））から選択処理によって、譲渡実行処理に対応する実行命令（Jdg（SDB）||GenAC（GenKcr）||GenAC（Ex）||RevK）が取得され、ステップS772以下の処理を実行命令に従って実行する。

【0537】

ステップS772では、検証審査コマンド（Jdg（SDB））に従って、譲渡先から取得したグループ属性証明書（Gp．AC）713の検証、審査を行なう。この検証処理は、先に図21～図23を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。検証不成立の場合は、エラー処理として、その後の処理を実行せず処理を中止する。グループ属性証明書（Gp．AC）の検証が成功し、グループ属性証明書（Gp．AC）の正当性が確認されるとステップS773に進む。

10

【0538】

ステップS773以下では、譲渡先ユーザデバイスにおいて暗号化データの利用を可能とするための実行属性証明書の生成、送信が行なわれることになる。これらの処理は、先に図60、図61、図63～図65を参照して説明した登録鍵生成実行ACの生成、検証、サービス提供実行ACの生成送信に対応する処理であり、図60、図61におけるサービスプロバイダ（SP）の処理を譲渡元ユーザデバイスが実行するものである。

20

【0539】

これらの処理に必要なリセット鍵（Kreset）、譲渡先の共通鍵メモリの登録鍵格納領域のブロックアドレス（Ad2）、譲渡先のセキュリティチップの公開鍵（KpSC2）等のデータ714は、譲渡先のユーザデバイス等から取得する。これらの必要データに基づいて、まず、ステップS773において、実行命令中の登録鍵生成実行AC作成コマンド（GenAC（GenKcr））に従って、登録鍵生成実行AC715の生成処理がなされる。この処理は、先に図63を参照して説明した登録鍵生成実行ACの生成処理と同様である。

【0540】

次に、譲渡元ユーザデバイスのセキュリティチップから、登録鍵生成実行ACを受信した譲渡先ユーザデバイスのセキュリティチップは、実行命令中の実行AC作成コマンド（GenAC（Ex））に従い、先に図64を参照して説明した処理に従って、登録鍵生成実行結果（図80，721）を生成して譲渡元ユーザデバイスのセキュリティチップに送信する。

30

【0541】

譲渡先ユーザデバイスのセキュリティチップから、登録鍵生成実行結果（図80，721）を受信した譲渡元ユーザデバイスのセキュリティチップは、図80に従った処理を行なって、新たな譲渡機能付きサービス提供実行属性証明書（AC）722を生成して譲渡先ユーザデバイスに送信するとともに、自己の共通鍵メモリ領域中の登録鍵を破棄する処理を実行する。

40

【0542】

図80のステップS781において、セッション鍵（Kcs）を適用して、登録鍵生成結果の復号処理を実行し、登録鍵（Kcr2）とメモリ領域ブロックアドレス（Ad2）を取得する。さらに、ステップS782において、新たな譲渡機能付きサービス提供実行属性証明書（AC）722に格納する実行命令（Ec（Sel||Jdg（SDB）||GenAC（GenKcr）||GenAC（Ex）||RevK||DecEData||Kcd；Kcr2））を、譲渡先ユーザデバイスの登録鍵（Kcr2）を適用して暗号化する。なお、実行命令は、サービス提供実行ACとしての新たな譲渡機能付きサービス提供実行属性証明書（AC）722に設定される実行プログラム等の実行命令である。

【0543】

50

さらに、ステップ S 7 8 3 において、実行命令を登録鍵 (K c r 2) で暗号化したデータと、登録鍵 (K c r 2) を格納する譲渡先ユーザデバイスにおけるセキュリティチップのメモリ領域ブロックアドレス (A d 2) とのデータに対して、譲渡元のセキュリティチップ (S C 1) の秘密鍵 (K s S C 1) によって署名 (図 1 7 参照) が生成され、新たな譲渡機能付きサービス提供実行属性証明書 (A C) 7 2 2 が生成されて、譲渡先ユーザデバイスに送信される。

【 0 5 4 4 】

さらに、ステップ S 7 8 4 では、元の譲渡機能付きサービス提供実行属性証明書 (A C) 7 1 1 に格納されたアドレス (A d 1)、すなわち、譲渡元のユーザデバイスの共通鍵メモリ領域の登録鍵格納アドレスに対するリセット鍵の書き込みが実行されて、登録鍵の破棄処理が実行される。

【 0 5 4 5 】

なお、上記説明では、譲渡元から譲渡先に対して新たな譲渡機能付きサービス提供実行属性証明書 (A C) 7 2 2 を生成して送付する構成例を示したが、新たな譲渡機能付きサービス提供実行属性証明書 (A C) 7 2 2 ではなく、通常の、すなわち譲渡機能を持たないサービス提供実行属性証明書 (A C) を生成して送付する構成としてもよい。

【 0 5 4 6 】

譲渡機能付きサービス提供実行属性証明書 (A C) は、先に説明したように、譲渡処理のみならず、暗号化データの復号処理の際にも適用される実行 A C である。そのいずれの処理を実行するかをエンドエンティティからの要求 (トリガ) によって選択する。トリガが暗号化データの復号処理の要求である場合のセキュリティチップにおける処理を図 8 1 を参照して説明する。

【 0 5 4 7 】

譲渡機能付きサービス提供実行属性証明書 (A C) 7 3 1 には、実行命令、実行命令を復号するための登録鍵を格納した共通鍵メモリ領域 6 0 8 のブロックアドレス (A d 1)、発行者署名の各データを有する。

【 0 5 4 8 】

譲渡機能付きサービス提供実行属性証明書 (A C) 7 3 1 を入力したセキュリティチップ (S C) は、まず、譲渡機能付きサービス提供実行属性証明書 (A C) 7 3 1 のアドレス (A d 1) に基づいて共通鍵メモリ領域 6 0 8 から登録鍵を取得し、譲渡機能付きサービス提供実行属性証明書 (A C) 7 3 1 内の実行命令を復号する。次に、暗号化データ復号トリガ 7 3 2 をエンドエンティティから入力すると、ステップ S 7 8 6 において、トリガに基づく選択処理、すなわち、データ復号実行の選択を行ない、ステップ S 7 8 7 において、復号処理を実行する。

【 0 5 4 9 】

すなわち、譲渡機能付きサービス提供実行属性証明書 (A C) 7 3 1 の実行命令 (E c (S e l || J d g (S D B) || G e n A C (G e n K c r) || G e n A C (E x) || R e v K || D e c E D a t a || K c d ; K c r 1)) から選択処理によって、データ復号処理に対応する実行命令 (D e c E D a t a || K c d) が取得され、ステップ S 7 8 7 において、データ復号鍵 (K c d) を適用して、外部から入力される復号対象の暗号化データ (E c (D a t a ; K c d)) 7 3 3 の復号処理を実行し、復号されたデータ 7 3 4 を出力する。復号対象の暗号化データ (E c (D a t a ; K c d)) 7 3 3 は、例えば画像、音楽、プログラム等のコンテンツを、鍵 (K c d) により暗号化したデータであり、譲渡機能付きサービス提供実行属性証明書 (A C) 7 3 1 内の格納実行命令を登録鍵 (K c r 1) によって復号することによって取得可能なデータ復号鍵 (K c d) によって復号可能となる。

【 0 5 5 0 】

譲渡機能と回数制限を組み合わせた適用例も考えられる。例えば、譲渡される実行 A C は、譲渡を行う実行 A C の回数情報が一つ減ったものとなるように設定すれば、移動回数を制限できる。また、複製機能と回数制限を組み合わせた適用例も考えられる。例えば、複

10

20

30

40

50

製を行うたびに実行属性証明書の回数情報が一つ減ったものとなるように設定すれば、複製回数を制限できる。ここで、複製というのは、複製機能を持たないサービス提供実行属性証明書に対して行う。さらに、一旦複製したサービス提供実行属性証明書を破棄する代わりに、回数情報を一つ増える機能を持たせれば、チェックイン・チェックアウト機能が実現できる。

【0551】

チェックイン・チェックアウトについて簡単に説明する。サービス利用権限を他の機器に転送することをチェックアウトといい、さらにチェックアウトした機器から元の機器に転送することをチェックインという。サービス利用権限がチェックアウトした機器から元の機器以外に転送することの出来ない時、チェックイン・チェックアウト機能を持つという。

10

【0552】

(7-3) 代理発行実行属性証明書

次に代理発行実行属性証明書について説明する。(6-3) 実行属性証明書適用処理では、コンテンツを暗号化したデータの復号サービスについて述べたが、サービスプロバイダしか知らない暗号鍵を実行属性証明書に書き込み、その暗号鍵を使って署名付けした証明書を発行するサービスも実行属性証明書をを用いて行うことが出来る。このサービス提供実行属性証明書が代理発行実行属性証明書である。

【0553】

この暗号鍵として、共通鍵を用いる方法と秘密鍵を用いる方法がある。以下では、秘密鍵を用いる場合について述べる。代理発行実行属性証明書をを用いて発行する証明書を検証するには、検証者は、上記秘密鍵に対応した公開鍵を知る必要がある。そのため、代理発行実行属性証明書発行者は、上記公開鍵の証明書を発行し、代理発行実行属性証明書をを用いて発行する証明書所有者は、検証者に、上記公開鍵証明書を提示する。この公開鍵証明書を代理署名鍵証明書と呼ぶ。この代理発行実行属性証明書として、以下の項目について各々説明する。

20

(7-3-1) 審査代行実行属性証明書

(7-3-2) 代理署名実行属性証明書

以下、上記項目ごとに説明する。

【0554】

30

(7-3-1) 審査代行実行属性証明書

まず、審査代行実行属性証明書について説明する。属性証明書登録局が、直接情報をやり取りするのが難しいエンドエンティティに属性証明書を発行する際、発行ポリシーを規定した状態で、予め属性証明書登録局が直接情報をやり取りすることの出来る別のエンドエンティティに、発行の審査を代行させることを可能とさせるのが、審査代行実行属性証明書である。

【0555】

図82を参照して審査代行実行属性証明書の概要を説明する。図82(a)は、通常の属性証明書の発行形態を示し、属性証明書(AC)の利用者である属性保持者から例えば属性認証局(AA)、属性証明書登録局(ARA)あるいはサービスプロバイダ(SP)等の発行者に対して属性証明書、ここではグループ属性証明書(Gp.AC)の発行要求(S801)を行なう。例えばこの場合、AC利用者の属性を証明するデータの提出が必要となる。前述した実施例では、例えばクレジットカード会社がすでにAC利用者に対して発行済みのグループ属性証明書の提示をする例を説明した。

40

【0556】

発行者は、AC利用者の属性等のユーザ確認としての審査を実行(S802)して、審査成立と判定すると、AC利用者の属性を証明する属性証明書(ここではGp.AC)801を利用者に発行(S803)する。

【0557】

(b)に示す例は、以下において詳細に説明する審査代行実行属性証明書を適用したグル

50

ープ属性証明書 (G p . A C) 発行シーケンスである。

【 0 5 5 8 】

まず、 A C 利用者に対してグループ属性証明書を代理発行する審査代行者が、本来の発行者、例えば属性認証局 (A A)、属性証明書登録局 (A R A) あるいはサービスプロバイダ (S P) に対して、審査代行実行属性証明書の発行要求 (S 8 1 1) を行ない、真の発行者である属性認証局 (A A)、属性証明書登録局 (A R A) あるいはサービスプロバイダ (S P) 等が、審査代行者の審査 (S 8 1 2) を行なう。これは、従来と同様、審査代行者の属性等を証明するデータ、あるいは既発行の属性証明書の提示等に基づいて実行する。審査成立後、発行者は、代理署名鍵証明書 8 0 4 と、審査代行実行属性証明書 8 0 3 を審査代行者に付与 (S 8 1 3) する。

10

【 0 5 5 9 】

代理署名鍵証明書 8 0 4 は、代理署名生成、検証の際に用いる公開鍵 (K p a) と、発行者署名データを有する。また、審査代行実行属性証明書 8 0 3 は、前述の実行証明書と同様、審査代行者のユーザデバイスの共通鍵メモリの登録鍵 (K c r) の格納領域を示すブロックアドレス (A d)、登録鍵 (K c r) で暗号化された実行命令 (E c (代行審査命令 || 属性情報 || K s a ; K c r))、発行者署名からなる。

【 0 5 6 0 】

実行命令に含まれる秘密鍵 (K s a) は、代理署名生成、検証の際に用いる秘密鍵であり、前述の公開鍵 (K p a) に対応する秘密鍵である。

【 0 5 6 1 】

ステップ S 8 1 1 ~ S 8 1 3 は、代行委託フェーズであり、この代行委託フェーズの完了の後、代行実行フェーズが開始される。 A C 利用者 (属性保持者) から、属性証明書 (G p . A C) の発行要求が審査代行者になされる (S 8 1 4)。ここでは、審査代行者の発行するグループ属性証明書を審査代行グループ属性証明書と呼ぶ。

20

【 0 5 6 2 】

審査代行グループ属性証明書の発行要求を受領した審査代行者は、利用者の審査 (S 8 1 5) を行なう。ここでの審査は、審査代行者と A C 利用者との信頼関係に基づいて実行することも可能であり、審査代行者の属性等を証明するデータ、あるいは既発行の属性証明書の提示等を必ずしも必要としない。例えば審査代行者をある家族の 1 人とし、利用者をその家族とする設定であれば、審査代行者が家族であることを認定すれば、審査成立とする等、審査代行者と A C 利用者との信頼関係に基づいて任意の審査を行なうことが可能である。

30

【 0 5 6 3 】

審査成立の後、審査代行者は、審査代行グループ属性証明書 8 0 2 を生成する。審査代行グループ属性証明書 8 0 2 は、 A C 利用者 (属性保持者) のセキュリティチップに対して発行された公開鍵証明書 (P K C) シリアル番号、属性情報等、先に図 5 を参照して説明した各情報を持つ。さらに、先に、審査代行者が発行者から受領した審査代行実行属性証明書 8 0 2 の実行命令中に格納された秘密鍵 (K s a) を適用した署名が付加される。

【 0 5 6 4 】

審査代行者は、生成した審査代行グループ属性証明書 8 0 2 と、代理署名鍵証明書 8 0 4 を併せて A C 利用者に送付 (S 8 1 6) する。 A C 利用者は、審査代行グループ属性証明書 8 0 2 を、例えばサービスプロバイダ (S P) に提示して属性を証明してサービスを受領する。

40

【 0 5 6 5 】

サービス提供も含めた各エンティティ間でのデータの流れを図 8 3 を参照して説明する。まず、代行委託フェーズにおいて、発行者 8 1 1 から審査代行実行 A C 8 2 2、代理署名鍵証明書 8 2 1 が審査代行者 8 1 2 に送付される。次に、代行実行フェーズにおいて、審査代行グループ属性証明書 8 2 3 と、代理署名鍵証明書 8 2 1 が A C 利用者 (属性所有者) 8 1 3 に送付される。さらに、サービスプロバイダ (S P) 等の検証者 8 1 4 に対して、審査代行グループ属性証明書 8 2 3 と、代理署名鍵証明書 8 2 1 が A C 利用者 (属性所

50

有者) 8 1 3 から送付され、検証者 8 1 4 が、審査代行グループ属性証明書 8 2 3 と、代理署名鍵証明書 8 2 1 に基づく A C 利用者の属性検証を実行し、検証成立を条件としてサービスを提供する。

【 0 5 6 6 】

サービスプロバイダ (S P) 等の検証者 8 1 4 は、代理署名鍵証明書 8 2 1 の署名検証の後、代理署名鍵証明書 8 2 1 に格納された代理署名検証用の公開鍵 (K p a) を取り出して、取り出した公開鍵 (K p a) を適用して、審査代行グループ属性証明書 8 2 3 の署名検証を実行することができる。

【 0 5 6 7 】

次に、発行者から審査代行実行 A C 8 2 2、代理署名鍵証明書 8 2 1 を受領した審査代行者が A C 利用者の要求に基づいて、審査代行グループ属性証明書 8 2 3 を生成、発行する処理について、図 8 4 を参照して説明する。図 8 4 において、

E E 1 : 属性証明書利用ユーザデバイスのエンドエンティティ (E E) 制御部、

S C 1 : E E 1 内に構成されるセキュリティチップ、

E E 2 : 審査代行者ユーザデバイスのエンドエンティティ (E E) 制御部、

S C 2 : E E 2 内に構成されるセキュリティチップ、

実行 A C テーブル : E E 2 の実行 A C テーブル制御部、

である。

【 0 5 6 8 】

なお、審査代行者は、ユーザデバイスに限らず、例えばサービスプロバイダ (S P) が実行する構成も可能である。ここでは一例としてユーザデバイスが審査代行者として機能する例を説明する。

【 0 5 6 9 】

まず、ステップ S 8 2 1 において、A C 利用者 (属性所有者) としてのユーザがエンドエンティティ (E E 1) の入力インタフェースを介して、審査代行グループ属性証明書 (G p . A C) の発行要求を入力する。要求には、審査代行者の指定データ、および利用予定のコンテンツあるいはサービスプロバイダ情報等、審査代行グループ属性証明書 (G p . A C) の生成に必要な情報を含む。

【 0 5 7 0 】

エンドエンティティ (E E 1) がユーザからの審査代行グループ属性証明書 (G p . A C) の発行要求を受領すると、エンドエンティティ (E E 1) は、ステップ S 8 2 2 において、審査代行者のユーザデバイスのエンドエンティティ (E E 2) に対する接続要求を行ない、各ユーザデバイスのセキュリティチップ (S C 1)、(S C 2) 間において相互認証を実行する。これは例えば先に図 1 3 を参照して説明した公開鍵方式の相互認証処理として実行される。

【 0 5 7 1 】

相互認証が成立すると、ステップ S 8 2 3 において、審査代行者ユーザデバイスのエンドエンティティ (E E 2) は、審査代行実行 A C の検索要求を実行 A C テーブルに出力する。検索キーは、例えばコンテンツ情報やサービスプロバイダ (S P) 情報等である。

【 0 5 7 2 】

ステップ S 8 2 4 において、実行 A C テーブルは、エンドエンティティ (E E 2) からの入力キーに基づいて、対応する審査代行実行 A C を検索し、テーブルから抽出した実行 A C とその A C に付帯して発行者から発行された代理署名鍵証明書 (図 8 2 , 8 0 4 参照) をエンドエンティティ (E E 2) に出力する。

【 0 5 7 3 】

ステップ S 8 2 5 において、エンドエンティティ (E E 2) は、受領 A C をセキュリティチップ (S C 2) に出力し、実行属性証明書の適用処理要求を行なう。セキュリティチップ (S C 2) は、ステップ S 8 2 6 において、受領 A C の処理、すなわち、実行属性証明書 (審査代行実行 A C) に格納されたアドレス (A d) によって指定された領域から取得される登録鍵に基づく実行命令の復号を行なう。

10

20

30

40

50

【 0 5 7 4 】

さらに、ステップ S 8 2 7 において、A C 利用者の審査のためのグループ属性証明書が A C 利用者のエンドエンティティ (E E 1) から審査代行者のエンドエンティティ (E E 2) に入力され、審査代行者のセキュリティチップ (S C 2) において検証処理が実行される。

【 0 5 7 5 】

前述したように、審査代行者は、A C 利用者の審査を審査代行者と A C 利用者との信頼関係に基づいて実行可能であり、審査代行者の属性等を証明するデータ、あるいは既発行の属性証明書の提示等を必ずしも必要としないが、ここでは、既発行のグループ属性証明書の提示、検証を条件として審査代行グループ属性証明書を発行する例を示している。

10

【 0 5 7 6 】

セキュリティチップ (S C 2) によるグループ属性証明書の検証は、先に図 2 1 ~ 図 2 3 を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。検証不成功の場合は、エラー処理として、その後の処理を実行せず処理を中止する。この場合、エラー通知を A C 利用者エンドエンティティ (E E 1) に送信する処理を行なってもよい。

【 0 5 7 7 】

グループ属性証明書 (G p . A C) の検証が成功し、グループ属性証明書 (G p . A C) の正当性が確認されるとステップ S 8 3 0 において、審査代行グループ属性証明書の生成に必要とする追加情報 (A d d i n f o) をエンドエンティティ (E E 2) からセキュリティチップ (S C 2) に入力し、セキュリティチップ (S C 2) は審査代行グループ属性証明書を生成し、エンドエンティティ (E E 2) に送付の後、エンドエンティティ (E E 2) から A C 利用者のエンドエンティティ (E E 1) に送付 (S 8 3 2) される。この送付処理に際しては、生成した審査代行グループ属性証明書に代理署名鍵証明書を付加して送付する。

20

【 0 5 7 8 】

審査代行者のセキュリティチップ (S C 2) で実行する処理、すなわち審査代行実行属性証明書を入力して審査代行グループ属性証明書を生成する処理の詳細を図 8 5 を参照して説明する。審査代行実行属性証明書 (A C) 8 5 1 には、実行命令、実行命令を復号するための登録鍵 (K c r) を格納した審査代行セキュリティチップ (S C) 8 6 1 の共通鍵メモリ領域 8 6 4 のブロックアドレス (A d)、発行者署名の各データを有する。実行命令 (E c (J d g (S D B) || G e n A C (G p) || a t t || K s a ; K c r)) には、検証審査コマンド (J d g (S D B))、グループ属性証明書作成コマンド (G e n A C (G p))、属性情報 (a t t)、代理署名用秘密鍵 (K s a) が含まれ、これらを登録鍵 (K c r) で暗号化したデータ構成である。

30

【 0 5 7 9 】

審査代行実行属性証明書 (A C) 8 5 1 を入力すると、まず、審査代行実行属性証明書 (A C) 8 5 1 のアドレス (A d) に基づいて共通鍵メモリ領域 8 6 4 から登録鍵を取得し、審査代行実行属性証明書 (A C) 8 5 1 内の実行命令を復号する。次に、ステップ S 8 4 2 において、検証審査コマンド (J d g (S D B)) に基づいて、A C 利用者からエンドエンティティを介して入力するグループ属性証明書の検証を実行する。この検証処理は、先に図 2 1 ~ 図 2 3 を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。検証不成功の場合は、エラー処理として、その後の処理を実行せず処理を中止する。グループ属性証明書 (G p . A C) の検証が成功し、グループ属性証明書 (G p . A C) の正当性が確認されるとステップ S 8 4 3 に進む。

40

【 0 5 8 0 】

ステップ S 8 4 3 では、審査代行実行 A C 8 5 1 内の実行命令中のグループ属性証明書作成コマンド (G e n A C (G p)) に基づいて、審査代行グループ属性証明書の生成、送信が行なわれることになる。これらの処理は、先に図 6 0、図 6 1、図 6 3 ~ 図 6 5 を参

50

照して説明した登録鍵生成実行ACの生成、検証、サービス提供実行ACの生成送信に対応する処理であり、図63～図65におけるサービスプロバイダ(SP)のセキュリティモジュールにおける処理と同様である。なお、例えば審査代行属性証明書であることを示す追加情報(addinfo)853を審査代行属性証明書に付加して、通常の属性証明書と異なることを示すものとするのが好ましい。

【0581】

ステップS844では、審査代行実行属性証明書(AC)851の実行命令中から取得した代理署名用の秘密鍵(Ksa)を適用して、追加情報(addinfo)および属性情報(att)に対する署名を行ない、審査代行グループ属性証明書854を生成し、エンドエンティティ(EE2)を介してAC利用者(属性所有者)に送信する。なお、AC利用者には、生成した審査代行グループ属性証明書に代理署名鍵証明書を付加して送付する。

10

【0582】

AC利用者は、上述の処理によって発行された審査代行グループ属性証明書と、代理署名鍵証明書を、サービスプロバイダ等の検証者に提示して、属性検証を条件としたサービスを受領することになる。サービスプロバイダ等の検証者は、代理署名鍵証明書から取得可能な鍵を適用して審査代行グループ属性証明書の署名検証が可能となる。

【0583】

上述した審査代行グループ属性証明書の適用例としては、例えばアカウント数を制限した審査代行グループ属性証明書の発行例がある。サービスプロバイダ(SP)がAさんの家族全員にサービスを提供する時に、Aさんの家族であるかどうかA家の家族であることを証明するグループ属性証明書(Gp.AC)を用いて審査するとする。

20

【0584】

このとき、A家の家族であることを証明するグループ属性証明書(Gp.AC)として、役所など住民の基本情報を持った第三者機関が発行した属性証明書(AC)を用いることができれば、信頼性の高い属性審査が可能となるが、このような属性証明書が利用可能な状態にあるとは限らない。一方、Aさん自身にA家の家族であることを証明するグループ属性証明書(Gp.AC)を発行させることはAさんの意思に応じて可能となる。しかし、属性証明書の真の発行主体である属性認証局(AA)としてAさん等の個人を信頼できると判定することは難しい。

30

【0585】

そこで、上述した審査代行実行ACを適用した審査代行グループ属性証明書を発行する。この場合、Aさんの家族の代表者としてのAさんが審査代行者として、審査代行実行ACを適用した審査代行グループ属性証明書の発行を行なう。この時の審査代行グループ属性証明書の発行審査は、審査代行者(Aさん)とAC利用者(Aさんの家族)との信頼関係に基づいて実行することが可能であり、審査代行者の属性等を証明するデータ、あるいは既発行の属性証明書の提示等を必ずしも必要としない。審査代行者が家族であることを認定すれば、審査成立とする等、審査代行者とAC利用者との信頼関係に基づいて審査代行グループ属性証明書を発行することが可能である。

【0586】

40

ただし、Aさんは、本当は家族でない友人のBさんにもAさんの家族であることを属性として示す審査代行グループ属性証明書を発行してしまうかもしれない。このような可能性を抑えるため、審査代行グループ属性証明書の発行枚数に制限、例えば上限=5とした設定をするなど、発行処理における制限を付帯することで、極端な不正利用の発生を防止することが可能である。

【0587】

上述の審査代行グループ属性証明書の発行処理態様は、Aさんの所有機器をグループとして設定したグループ属性証明書においても同様に処理可能であり、審査代行実行ACを適用した審査代行グループ属性証明書としてAさんが審査代行者として審査代行実行ACに基づいて審査代行グループ属性証明書をAさんの所有機器各々に発行することが可能とな

50

る。

【 0 5 8 8 】

さらに、審査代行グループ属性証明書を適用した処理例として、選挙における投票に適用する例がある。審査代行グループ属性証明書を利用することで、有権者が、投票する候補者以外、選挙管理委員にすら誰に投票したかわからないようにして選挙を行うことができる。

【 0 5 8 9 】

この処理例では、

審査代行者：有権者

ＡＣ利用者（属性所持者）：候補者

10

とする。この選挙システムは、投票時に有権者は選挙管理委員と通信する代わりに候補者と通信すればよいというモデルであり、現実の選挙とは異なる。まず、サービスプロバイダ（ＳＰ）は、有権者に審査代行実行ＡＣを発行する。有権者は、投票予定の候補者から、ユニークな識別値、すなわち他の投票とかぶらない識別値を教えてもらい、その数と投票予定の候補者のＰＫＣシリアルＮｏ．を属性として持つ審査代行グループ属性証明書（Ｇｐ．ＡＣ）を審査代行実行ＡＣに基づいて、発行して候補者に送付する。審査代行実行ＡＣは、この審査代行グループ属性証明書（Ｇｐ．ＡＣ）の生成後、自動的に破棄される。

【 0 5 9 0 】

各候補者に対して発行された審査代行グループ属性証明書（Ｇｐ．ＡＣ）数に基づいて、得票数がカウントされ、当落を決定する。同じ識別値の書かれた審査代行グループ属性証明書は、コピーしたとみなされ一票にしかない。

20

【 0 5 9 1 】

（ 7 - 3 - 2 ）代理署名実行属性証明書

次に、代理署名実行属性証明書について説明する。代理署名実行ＡＣはＡＣ利用者（属性保持者）自身が、自らサービスに適用するためのグループ属性証明書（代理署名グループ属性証明書）を発行することを可能とした実行属性証明書である。

【 0 5 9 2 】

図 8 6 を参照して代理署名実行属性証明書の概要を説明する。図 8 6 （ a ）は、通常の属性証明書の発行、適用処理形態を示す。属性証明書（ＡＣ）の利用者である属性保持者から例えば属性認証局（ＡＡ）、属性証明書登録局（ＡＲＡ）あるいはサービスプロバイダ（ＳＰ）等の発行者に対して属性証明書、ここではグループ属性証明書（Ｇｐ．ＡＣ）の発行要求（Ｓ 9 0 1）を行なう。例えばこの場合、ＡＣ利用者の属性を証明するデータの提出が必要となる。前述した実施例では、例えばクレジットカード会社がすでにＡＣ利用者に対して発行済みのグループ属性証明書の提示をする例を説明した。

30

【 0 5 9 3 】

発行者は、ＡＣ利用者の属性等のユーザ確認としての審査を実行（Ｓ 9 0 2）して、審査成立と判定すると、ＡＣ利用者の属性を証明する属性証明書（ここではＧｐ．ＡＣ） 9 2 1 を利用者に発行（Ｓ 9 0 3）する。

【 0 5 9 4 】

ＡＣ利用者（属性保持者）は、発行されたグループ属性証明書（Ｇｐ．ＡＣ）をサービスプロバイダ（ＳＰ）等の検証者に提示してサービスの適用を受けることが可能であり、検証者からのグループ属性証明書（Ｇｐ．ＡＣ）提示要求（Ｓ 9 0 4）に応じて、ＡＣ利用者（属性保持者）が提示（Ｓ 9 0 5）を行ない、検証者がグループ属性証明書（Ｇｐ．ＡＣ）の検証（Ｓ 9 0 6）を実行する。

40

【 0 5 9 5 】

（ b ）に示す例は、以下において詳細に説明する代理署名実行属性証明書を適用したグループ属性証明書（Ｇｐ．ＡＣ）発行、適用処理シーケンスである。

【 0 5 9 6 】

まず、ＡＣ利用者（属性保持者）は、例えば属性認証局（ＡＡ）、属性証明書登録局（Ａ

50

R A)あるいはサービスプロバイダ(S P)等の発行者に対して代理署名実行属性証明書(A C)の発行要求(S 9 1 1)を行なう。発行者は、A C利用者の属性を証明するデータ、例えば発行済みのグループ属性証明書等に基づいて審査(S 9 1 2)を実行し、審査成立と判定すると、代理署名実行属性証明書9 2 3を発行する。発行者は、この際、代理署名鍵証明書9 2 4も併せてA C利用者(属性保持者)に提供する。

【0 5 9 7】

代理署名鍵証明書9 2 4は、代理署名生成、検証の際に用いる公開鍵(K p a)と、発行者署名データを有する。また、代理署名実行属性証明書9 2 3は、前述の実行証明書と同様、審査代行者のユーザデバイスの共通鍵メモリの登録鍵(K c r)の格納領域を示すブロックアドレス(A d)、登録鍵(K c r)で暗号化された実行命令(E c(代理署名命令||属性情報||K s a; K c r))、発行者署名からなる。

10

【0 5 9 8】

実行命令に含まれる秘密鍵(K s a)は、代理署名生成、検証の際に用いる秘密鍵であり、前述の公開鍵(K p a)に対応する秘密鍵である。

【0 5 9 9】

ステップS 9 1 1 ~ S 9 1 3は、発行フェーズであり、この発行フェーズの完了の後、検証フェーズが開始される。ステップS 9 1 4において、サービスプロバイダ(S P)等の検証者は、A C利用者(属性保持者)に対して代理署名グループ属性証明書(G p . A C)の提示要求を実行する。この提示要求に際して、サービスプロバイダ(S P)等の検証者は、代理署名グループ属性証明書(G p . A C)の検証用乱数(R a)をA C利用者(属性保持者)に対して送信する。

20

【0 6 0 0】

A C利用者(属性保持者)は、ステップS 9 1 5において、サービスプロバイダ(S P)等の検証者からの代理署名グループ属性証明書(G p . A C)の提示要求に応じて、先に発行者から受領した代理署名実行属性証明書を適用して代理署名グループ属性証明書(G p . A C)9 2 2を生成する。この生成処理の詳細については後述する。代理署名グループ属性証明書(G p . A C)9 2 2は、A C利用者(属性保持者)の公開鍵証明書(P K C)のシリアル番号、属性情報等の情報に、検証者から受信した検証用乱数(R a)を含み、先に、発行者から受領した代理署名実行属性証明書9 2 3の実行命令中に格納された秘密鍵(K s a)を適用した署名が付加される。

30

【0 6 0 1】

A C利用者(属性保持者)は、生成した代理署名グループ属性証明書9 2 2と、代理署名鍵証明書9 2 4を併せて検証者に送付(S 9 1 6)する。検証者は、代理署名鍵証明書9 2 4の署名検証の後、代理署名鍵証明書9 2 4に格納された代理署名検証用の公開鍵(K p a)を取り出して、取り出した公開鍵(K p a)を適用して、代理署名グループ属性証明書9 2 2の署名検証を実行する。さらに、代理署名グループ属性証明書中に格納された乱数と自己が先に生成した乱数の一致を検証することにより、今回の検証で、検証者の要求に対して提示された代理署名グループ属性証明書であることを確認できる。

【0 6 0 2】

サービス提供も含めた各エンティティ間でのデータの流れを図8 7を参照して説明する。まず、発行フェーズにおいて、発行者9 3 1からA C利用者(属性保持者)9 3 2に対して代理署名鍵証明書9 4 1、および代理署名実行属性証明書9 4 2がA C利用者(属性保持者)9 3 2に送付される。次に、A C利用者(属性保持者)9 3 2からサービスプロバイダ(S P)等の検証者9 3 3にサービス要求がなされると、検証者9 3 3は、A C利用者(属性保持者)9 3 2に対して代理署名グループ属性証明書(G p . A C)の提示要求を実行する。この提示要求に際して、検証者9 3 3は、代理署名グループ属性証明書(G p . A C)の検証用乱数(R a)をA C利用者(属性保持者)9 3 2に対して送信する。

40

【0 6 0 3】

A C利用者(属性保持者)9 3 2は、検証者9 3 3からの代理署名グループ属性証明書(G p . A C)の提示要求に応じて、先に発行者から受領した代理署名実行属性証明書を適

50

用して代理署名グループ属性証明書 (Gp . AC) 9 4 3 を生成する。代理署名グループ属性証明書 (Gp . AC) 9 4 3 は、AC 利用者 (属性保持者) 9 3 2 の公開鍵証明書 (PKC) のシリアル番号、属性情報等の情報に、検証者から受信した検証用乱数 (Ra) を含み、先に、発行者から受領した代理署名実行属性証明書 9 4 2 の実行命令中に格納された秘密鍵 (Ksa) を適用した署名が付加される。

【0604】

次に、AC 利用者 (属性所有者) 9 3 2 は、代理署名グループ属性証明書 9 4 3 と、代理署名鍵証明書 9 4 1 を検証者に送付し、検証者が、代理署名グループ属性証明書 9 4 3 と、代理署名鍵証明書 9 4 1 に基づく AC 利用者の属性検証を実行し、検証成立を条件としてサービスを提供する。

10

【0605】

サービスプロバイダ (SP) 等の検証者 9 3 3 は、代理署名鍵証明書 9 4 1 の署名検証の後、代理署名鍵証明書 9 4 1 に格納された代理署名検証用の公開鍵 (Kpa) を取り出して、取り出した公開鍵 (Kpa) を適用して代理署名グループ属性証明書 9 4 3 の署名検証を実行し、また代理署名グループ属性証明書 9 4 3 の格納乱数の照合により検証を行なう。

【0606】

次に、発行者の発行した代理署名実行属性証明書と代理署名鍵証明書とを有する AC 利用者が、サービスプロバイダ (SP) 等の検証者からの代理署名グループ属性証明書の提示要求に際して実行する処理の詳細を図 8 8 を参照して説明する。図 8 8 において、

20

SP : 属性証明書の検証を実行するサービスプロバイダ制御部、

SM : SP のセキュリティモジュール

EE : 属性証明書利用ユーザデバイスのエンドエンティティ (EE) 制御部、

SC : EE 内に構成されるセキュリティチップ、

実行 AC テーブル : EE の実行 AC テーブル制御部、
である。

【0607】

図 8 8 の処理は、サービスプロバイダ (SP) のセキュリティモジュール (SM) と、ユーザデバイスのセキュリティチップ (SC) 間で相互認証が成立した後の処理を示している。

30

【0608】

相互認証成立の後、サービスプロバイダ (SP) は、セキュリティモジュール (SM) に対して、属性証明書検証時に適用する乱数の生成要求 (S951) を行なう、ステップ S952 において、セキュリティモジュール (SM) は、要求に応じて乱数を生成しサービスプロバイダ (SP) に出力する。

【0609】

ステップ S953 において、サービスプロバイダ (SP) は、エンドエンティティ (EE) に対して代理署名グループ属性証明書の提示要求を実行する。この際、サービスプロバイダ (SP) は、エンドエンティティ (EE) に対して代理署名グループ属性証明書 (Gp . AC) の検証用乱数 (Ra) を併せて送信する。

40

【0610】

ステップ S954 において、エンドエンティティ (EE) は、代理署名グループ属性証明書 (Gp . AC) の生成に適用する代理署名実行属性証明書の検索を実行 AC テーブルに対して行ない、実行 AC テーブルは、ステップ S955 において、代理署名実行属性証明書およびそれに対応する代理署名鍵証明書をエンドエンティティ (EE) に対して出力する。

【0611】

ステップ S956 において、エンドエンティティ (EE) は、代理署名実行属性証明書の適用処理、すなわち、代理署名グループ属性証明書の生成処理をセキュリティチップ (SC) に要求し、ステップ S958 において、セキュリティチップ (SC) は、代理署名グ

50

ループ属性証明書の生成処理を実行する。この代理署名グループ属性証明書の生成処理の詳細は、先に図 8 5 を参照して説明した審査代行実行属性証明書に基づく審査代行グループ属性証明書の処理と同様である。ただし、代理署名グループ属性証明書には、検証者から受信した乱数 (R a) が格納される。

【 0 6 1 2 】

ステップ S 9 5 8 において、セキュリティチップ (S C) は、生成した代理署名グループ属性証明書をエンドエンティティ (E E) に送付する。エンドエンティティ (E E) は、ステップ S 9 5 9 において、代理署名グループ属性証明書、および、先に発行者から受領済みの代理署名鍵証明書をサービスプロバイダ側のセキュリティモジュール (S M) に送信する。

10

【 0 6 1 3 】

サービスプロバイダ側のセキュリティモジュール (S M) が、代理署名グループ属性証明書と、代理署名鍵証明書を受信すると、代理署名鍵証明書に格納された代理署名検証用の公開鍵 (K p a) を取り出して、取り出した公開鍵 (K p a) を適用して代理署名グループ属性証明書の署名検証を実行し、また代理署名グループ属性証明書の格納乱数の照合処理に基づく検証を行ない、検証結果をサービスプロバイダ (S P) に通知する。サービスプロバイダ (S P) は応答結果に応じて、検証成立の場合はサービス提供を実行し、検証不成立の場合はサービス提供の停止処理を行なうことになる。

【 0 6 1 4 】

代理署名実行属性証明書の適用例として、通常の属性証明書がある。すなわち、通常の属性証明書の代わりに、代理署名実行属性証明書を用いれば、実行属性証明書の破棄処理機能を用いることが出来るので、検証のたびに破棄リストを参照するなどの、失効処理による煩雑さ、信頼性の低下を解決することが出来る。

20

【 0 6 1 5 】

さらなる適用例としては、属性証明回数を制限した代理署名属性証明書がある。すなわち、アクセス許可など、暗号化データの復号以外のサービスに対しても、サービス提供を認めるグループ属性証明書として、回数制限の機能を持った代理署名実行属性証明書を用いれば、サーバ等外部に回数情報を持たせるなどの処理の煩雑さ、処理効率の低下なく、制限されたサービス提供を行うことが出来る。

【 0 6 1 6 】

30

[(8) 各エンティティの構成]

次に、上述した処理、すなわち属性証明書の生成、検証、送受信等を実行するユーザデバイスとしてのセキュリティチップ (S C) を備えたエンドエンティティ (E E)、あるいはセキュリティチップ (S C) を備えたユーザ識別デバイス (U I D)、あるいはサービスプロバイダ (S P) 等、各エンティティの情報処理装置としての構成例について図を参照しながら、説明する。

【 0 6 1 7 】

ユーザデバイス、サービスプロバイダ等、各エンティティの情報処理装置は、各種のデータ処理、および制御を実行する C P U を有し、かつ他エンティティと通信可能な通信手段を備えた例えば、サーバ、 P C 、 P D A 、携帯通信端末装置等の各種の情報処理装置によって構成可能である。

40

【 0 6 1 8 】

図 8 9 に情報処理装置構成例を示す。なお、図 8 9 に示す構成例は 1 つの例であり、各エンティティは、ここに示すすべての機能を必ずしも備えることが要求されるものではない。図 8 9 に示す C P U (Central processing Unit) 9 5 1 は、各種アプリケーションプログラムや、 O S (Operating System) を実行するプロセッサである。 R O M (Read-Only-Memory) 9 5 2 は、 C P U 9 5 1 が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。 R A M (Random Access Memory) 9 5 3 は、 C P U 9 5 1 の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

50

【 0 6 1 9 】

HDD 954 はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。セキュリティチップ 962 は、前述したように耐タンパ構造を持つ構成であり、暗号処理に必要な鍵データ等を格納し、権限確認処理としての属性証明書の検証、あるいは生成処理等を実行する暗号処理部、データ処理部、メモリを有する。

【 0 6 2 0 】

バス 960 は P C I (Peripheral Component Interface) バス等により構成され、各モジュール、入出力インタフェース 961 を介した各入出力装置とのデータ転送を可能にしている。

10

【 0 6 2 1 】

入力部 955 は、例えばキーボード、ポインティングデバイス等によって構成され、C P U 951 に各種のコマンド、データを入力するためにユーザにより操作される。出力部 956 は、例えば C R T、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。

【 0 6 2 2 】

通信部 957 はデバイスの接続したエンティティ、例えばサービスプロバイダ等との通信処理を実行するネットワークインタフェース、接続機器インタフェース等からなり、C P U 951 の制御の下に、各記憶部から供給されたデータ、あるいは C P U 951 によって処理されたデータ、暗号化されたデータ等を送信したり、他エンティティからのデータを受信する処理を実行する。

20

【 0 6 2 3 】

ドライブ 958 は、フレキシブルディスク、C D - R O M (Compact Disc Read Only Memory)、M O (Magneto optical) ディスク、D V D (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体 959 の記録再生を実行するドライブであり、各リムーバブル記録媒体 959 からのプログラムまたはデータ再生、リムーバブル記録媒体 959 に対するプログラムまたはデータ格納を実行する。

【 0 6 2 4 】

各記憶媒体に記録されたプログラムまたはデータを読み出して C P U 951 において実行または処理を行なう場合は、読み出したプログラム、データはインタフェース 961、バス 960 を介して例えば接続されている R A M 953 に供給される。

30

【 0 6 2 5 】

前述の説明内に含まれるユーザデバイス、サービスプロバイダ等における処理を実行するためのプログラムは例えば R O M 952 に格納されて C P U 951 によって処理されるか、あるいはハードディスクに格納され H D D 954 を介して C P U 951 に供給されて実行される。

【 0 6 2 6 】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

40

【 0 6 2 7 】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【 0 6 2 8 】

例えば、プログラムは記録媒体としてのハードディスクや R O M (Read Only Memory) に

50

予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、C D - R O M (Compact Disc Read Only Memory)、M O (Magneto optical) ディスク、D V D (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

【0629】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、L A N (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

10

【0630】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0631】

【発明の効果】

以上、説明したように、本発明のデータ処理権限管理システム、情報処理装置、および方法によれば、暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、暗号化実行命令の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス（A d）情報とを格納データとして有する実行属性証明書をサービス受領デバイスであるユーザデバイスに対して提供し、ユーザデバイスにおいて、実行属性証明書に格納されたアドレス（A d）情報に従って、ユーザデバイスのメモリから取得した登録鍵を適用して、実行属性証明書に格納された暗号化実行命令の復号を行ない、復号結果に基づくデータ処理を実行する構成としたので、登録鍵を実行属性証明書に格納したアドレスに従って取得可能なユーザデバイスにおいてのみ実行属性証明書に格納した実行命令を実行することが可能となり、サービス利用権限を有するユーザに対して厳格に限定したサービスの提供が可能となる。

20

【0632】

さらに、本発明のデータ処理権限管理システム、情報処理装置、および方法によれば、サービス提供実行属性証明書に適用する登録鍵の格納を登録鍵生成実行属性証明書に従って実行する構成としたので、不正な登録鍵の格納が防止され、不正なサービス受領を確実に防止できる。

30

【0633】

さらに、本発明のデータ処理権限管理システム、情報処理装置、および方法によれば、リセット鍵の書き込みによる登録鍵の破棄処理を実行する構成としたので、不正な登録鍵の保持を防止することが可能となる。

【0634】

さらに、本発明のデータ処理権限管理システム、情報処理装置、および方法では、実行命令に適用可能回数識別値を格納し、実行命令の実行に応じて適用可能回数識別値を更新して、更新された適用可能回数識別値を含む新たな実行属性証明書の生成を行なう構成としたので、利用回数制限のあるサービスの受領を確実な回数制限の下に実行可能となる。

40

【0635】

さらに、本発明のデータ処理権限管理システム、情報処理装置、および方法によれば、譲渡用実行属性証明書の生成処理命令、審査代行属性証明書の発行処理命令、代理署名属性証明書の発行処理命令等の各種の実行命令を実行属性証明書に格納することにより、様々な属性証明書の利用形態が実現される。

【図面の簡単な説明】

【図1】権限管理システムにおける公開鍵基盤、権限管理基盤構成について説明する図で

50

ある。

【図 2】公開鍵証明書フォーマットの示す図である。

【図 3】公開鍵証明書フォーマットの示す図である。

【図 4】公開鍵証明書フォーマットの示す図である。

【図 5】権限情報証明書としての属性証明書のフォーマットの示す図である。

【図 6】グループ属性証明書（グループ A C）の発行者、所有者、検証者、属性情報の構成例を示す図である。

【図 7】グループ属性証明書の発行ポリシーテーブルを示す図である。

【図 8】権限管理システムに参加する各エンティティの信頼関係構成を説明するトラストモデルを示す図である。

10

【図 9】ユーザデバイスとしてのエンドエンティティ（E E）とユーザ識別デバイス（U I D）に構成されるセキュリティチップの構成例を示す図である。

【図 10】ユーザデバイスのセキュリティチップの格納データ例を示す図である。

【図 11】グループ属性証明書の発行申請、発行処理、利用処理の流れの概略を説明する図である。

【図 12】サービスプロバイダ（S P）と、属性認証局（A A）または属性証明書登録局（A R A）のグループ情報共有化処理について説明する図である。

【図 13】公開鍵暗号方式の 1 つの認証処理方式であるハンドシェイクプロトコル（T L S 1 . 0）について示す図である。

【図 14】メッセージ認証コード：M A C（Message Authentication Code）の生成構成を示す図である。

20

【図 15】発行ポリシーテーブル、グループ情報データベースの情報構成例を示す図である。

【図 16】ユーザデバイスであるエンドエンティティ（E E）のセキュリティチップ（S C）がグループ属性証明書の発行要求主体である場合の処理シーケンスを示す図である。

【図 17】電子署名の生成処理を説明するフロー図である。

【図 18】電子署名の検証処理を説明するフロー図である。

【図 19】ユーザ識別デバイス（U I D）内のユーザセキュリティチップ（U S C）対応のグループ属性証明書を発行する手順について説明するシーケンス図である。

【図 20】グループ属性証明書を利用したサービス利用権限確認を含むサービス開始までの処理について説明するシーケンス図である。

30

【図 21】公開鍵証明書（P K C）と属性証明書（A C）との関連について説明する図である。

【図 22】属性証明書（A C）の検証処理フローを示す図である。

【図 23】公開鍵証明書（P K C）の検証処理フローを示す図である。

【図 24】グループ属性証明書を利用したサービス利用権限確認を含むサービス開始までの処理について説明するシーケンス図である。

【図 25】グループ属性証明書（G p . A C）の審査処理を説明するシーケンス図である。

。

【図 26】サービスを提供条件として、ユーザあるいはユーザ機器が異なる複数のグループに属することが条件とされる場合の概念を説明する図である。

40

【図 27】ユーザ識別デバイス（U I D）内のユーザセキュリティチップ（U S C）に対応して発行されたグループ属性証明書に基づくサービス提供までの処理について説明するシーケンス図である。

【図 28】ユーザ識別デバイス（U I D）内のユーザセキュリティチップ（U S C）に対応して発行されたグループ属性証明書に基づくサービス提供までの処理について説明するシーケンス図である。

【図 29】ユーザデバイス間においてグループ属性証明書を発行し、格納する処理について説明するシーケンス図である。

【図 30】アクセス許可情報を属性として持つグループ属性証明書の発行処理シーケンス

50

について説明する図である。

【図 3 1】アクセス許可情報をグループ情報として持つグループ属性証明書と、他のグループ属性証明書との対応例について説明する図である。

【図 3 2】アクセス要求先ユーザデバイスが、自ら属性証明書の発行処理を実行せずに属性証明書の発行処理を他のユーザデバイスに依頼して実行する処理シーケンスについて説明する図である。

【図 3 3】アクセス許可情報をグループ情報として定義したグループ属性証明書を利用したアクセス可否判定処理を伴うサービス利用シーケンスについて説明する図である。

【図 3 4】各サービスにおいて利用されるグループ属性証明書の例を示す図である。

【図 3 5】第 1 のグループ属性証明書 A に基づいて、コンテンツの利用許可情報をグループ情報として含む第 2 のグループ属性証明書 B を発行する処理について説明するシーケンス図である。

10

【図 3 6】グループ属性証明書 B をサービスプロバイダに提示して、コンテンツ利用権限のあることの確認を行なって、サービス提供、すなわちコンテンツ配信サービスを受領する処理について説明するシーケンス図である。

【図 3 7】複数の異なる属性証明書を適用してユーザあるいはユーザ機器のコンテンツ利用権を確認してサービスを提供する処理に適用する属性証明書例を説明する図である。

【図 3 8】異なるグループ属性証明書を適用したコンテンツ利用権限確認および、サービス提供処理について説明するフロー図である。

【図 3 9】サービス提供条件として設定されるグループ属性証明書の組み合わせテーブルデータ構成例を示す図である。

20

【図 4 0】複数のグループ属性証明書を適用した利用権限確認処理を説明する図である。

【図 4 1】医療処理において適用するグループ属性証明書の例を示す図である。

【図 4 2】医療処理を行なうリモートコントロールのシステムにおいて、各機器に格納される属性証明書について説明する図である。

【図 4 3】ユーザ識別デバイスに格納されたグループ属性証明書を適用して医療診断プログラムの実行サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する図である。

【図 4 4】グループ属性証明書を適用して医療診断プログラムの実行結果としての診断データ引き取り処理サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する図である。

30

【図 4 5】リモートメンテナンス処理において適用するグループ属性証明書の例を示す図である。

【図 4 6】メンテナンスサービスを行なうシステムにおいて、各機器に格納される属性証明書を説明する図である。

【図 4 7】サービス実行時におけるサービス属性証明書およびコントロール属性証明書の利用形態について説明する図である。

【図 4 8】家電機器 (E E) に格納されたサービス属性証明書、サービスプロバイダに格納されたコントロール属性証明書を適用したメンテナンス等のサービス処理を説明するシーケンス図である。

40

【図 4 9】サービス属性証明書の審査処理について説明する図である。

【図 5 0】コントロール属性証明書に基づくサービス、例えば家電機器に対するメンテナンス処理を実行するシーケンスについて説明する図である。

【図 5 1】メンテナンス実行プログラムをメーカー側機器 (S P) からユーザ側家電機器 (E E) に対して送信する処理とした例を説明する図である。

【図 5 2】メンテナンス実行プログラムをメーカー側機器 (S P) から、逐次コマンドを家電機器 (E E) に送信し、コマンド実行に基づく応答を家電機器 (E E) から受信しながらレスポンス対応の処理を実行する例を説明する図である。

【図 5 3】サービス提供要求時にサービス属性証明書、コントロール属性証明書をメーカー側 (S P) に提示する処理例を説明する図である。

50

【図 5 4】コミュニケーションサービスにおいて適用するグループ属性証明書の例を説明する図である。

【図 5 5】コミュニケーションサービスにおいて適用するグループ属性証明書の格納構成例を示す図である。

【図 5 6】グループ属性証明書を適用してチャットルーム参加サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する図である。

【図 5 7】グループ属性証明書を適用してアクセス権限確認処理を行ない、コミュニケーションを開始する処理シーケンスについて説明する図である。

【図 5 8】実行属性証明書の概要について説明する図である。

【図 5 9】実行属性証明書の利用手続き概要を説明するフロー図である。

10

【図 6 0】実行属性証明書の発行シーケンス図である。

【図 6 1】実行属性証明書の発行シーケンス図である。

【図 6 2】実行 A C テーブルの構成例を示す図である。

【図 6 3】セキュリティモジュール (S M) における登録鍵生成実行 A C の生成処理を説明する図である。

【図 6 4】セキュリティチップで実行される登録鍵生成実行 A C に基づく登録鍵生成処理について、説明する図である。

【図 6 5】セキュリティモジュール (S M) によるサービス提供実行 A C の生成処理を説明する図である。

【図 6 6】サービス提供実行 A C のユーザデバイス側における適用シーケンスをまとめた図である。

20

【図 6 7】セキュリティチップ (S C) におけるサービス提供処理における処理詳細を説明する図である。

【図 6 8】セキュリティチップ (S C) 登録鍵破棄処理について説明する図である。

【図 6 9】リセット要求に基づく登録鍵の破棄処理としてのリセット処理を説明する図である。

【図 7 0】実行属性証明書をサービスプロバイダ (S P) の承認の下に破棄し、破棄が間違いなく実行されたことをサービスプロバイダに通知する実行属性証明書リセット (破棄) 処理について説明する図である。

【図 7 1】実行属性証明書をサービスプロバイダ (S P) の承認の下に破棄し、破棄が間違いなく実行されたことをサービスプロバイダに通知する実行属性証明書リセット (破棄) 処理について説明する図である。

30

【図 7 2】リセット確認結果生成処理の詳細について説明する図である。

【図 7 3】実行 A C に基づく登録鍵の破棄処理について説明する図である。

【図 7 4】回数制限付きサービス提供実行属性証明書をユーザデバイスにおいて適用してサービスを適用する処理を説明する図である。

【図 7 5】回数制限付きサービス提供実行属性証明書をユーザデバイスにおいて適用してサービスを適用する処理を説明する図である。

【図 7 6】更新後の残利用回数 1 の場合のセキュリティチップ (S C) における処理を説明する図である。

40

【図 7 7】更新後の残利用回数 = 0 の場合のセキュリティチップ (S C) における処理を説明する図である。

【図 7 8】譲渡機能付きサービス提供実行属性証明書の適用処理を説明する図である。

【図 7 9】譲渡機能付きサービス提供実行属性証明書の復号処理以降の処理詳細を説明する図である。

【図 8 0】譲渡機能付きサービス提供実行属性証明書の復号処理以降の処理詳細を説明する図である。

【図 8 1】譲渡機能付きサービス提供実行属性証明書を適用した暗号化データ復号処理を説明する図である。

【図 8 2】審査代行実行属性証明書の概要を説明する図である。

50

【図 8 3】審査代行実行属性証明書を適用した処理を説明する図である。

【図 8 4】審査代行グループ属性証明書を生成、発行する処理について説明する図である。

【図 8 5】審査代行実行属性証明書を入力して審査代行グループ属性証明書を生成する処理を説明する図である。

【図 8 6】代理署名実行属性証明書の概要を説明する図である。

【図 8 7】代理署名実行属性証明書を適用した処理を説明する図である。

【図 8 8】サービスプロバイダ (S P) 等の検証者からの代理署名グループ属性証明書の提示要求に際して実行する処理を説明する図である。

【図 8 9】ユーザデバイス、サービスプロバイダ等、各エンティティの情報処理装置構成例を示す図である。 10

【符号の説明】

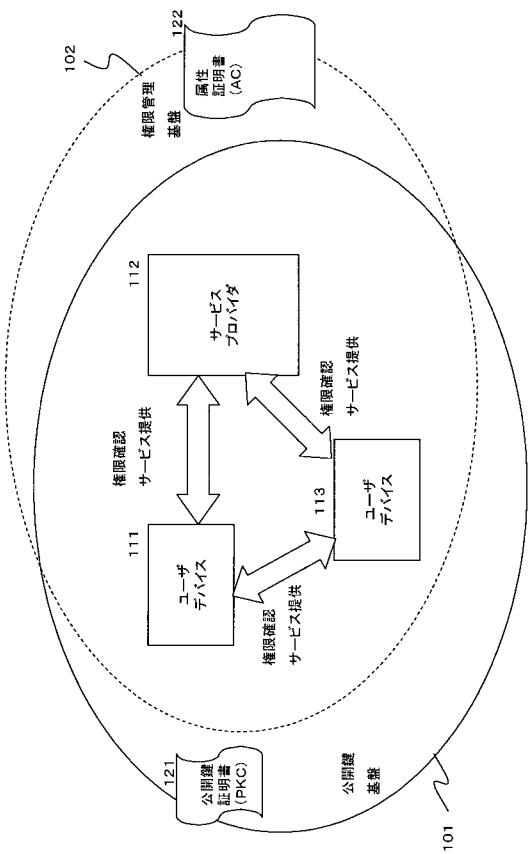
1 0 1	公開鍵基盤	
1 0 2	権限管理基盤	
1 1 1 , 1 1 3	ユーザデバイス	
1 1 2	サービスプロバイダ	
1 2 1	公開鍵証明書	
1 2 2	属性証明書	
1 3 0	システムホルダ	
1 3 1	ルート認証局 (C A)	20
1 3 2	認証局 (C A)	
1 3 3	登録局 (R A)	
1 4 0	属性認証局 (A A)	
1 5 0	属性証明書登録局 (A R A)	
1 5 1	ポリシーテーブル	
1 6 0	サービスプロバイダ (S P)	
1 7 0	ユーザデバイス	
1 7 1	ユーザ識別デバイス (U I D)	
1 7 2	エンドエンティティ (E E)	
2 0 0	ユーザデバイス	30
2 0 1	C P U (Central processing Unit)	
2 0 2	インタフェース	
2 0 3	R O M (Read-Only-Memory)	
2 0 4	R A M (Random Access Memory)	
2 0 5	暗号処理部	
2 0 6	メモリ部	
2 0 7	共通鍵メモリ領域	
2 1 0	セキュリティチップ	
2 2 1	ユーザデバイス側制御部	
2 2 2	外部メモリ部	40
2 3 1	接続機器インタフェース	
2 3 2	ネットワークインタフェース	
3 1 1	ユーザデバイス	
3 1 2	属性証明書登録局 (A R A)	
3 1 3	発行ポリシーテーブル	
3 1 4	サービスプロバイダ	
3 1 5	グループ情報データベース	
3 1 6	グループ属性証明書	
4 0 1	病院側医療機器 (S P)	
4 0 2	グループ属性証明書 A C 0 2	50

4 0 3	セキュリティモジュール	
4 1 1	自宅側医療機器 (E E)	
4 1 2	セキュリティチップ	
4 2 1	ユーザ識別デバイス	
4 2 2	グループ属性証明書 A C 0 1	
4 2 3	ユーザセキュリティチップ	
4 5 1	メーカー側機器 (S P)	
4 5 2	コントロール属性証明書	
4 5 3	セキュリティモジュール	
4 6 1	ユーザ側家電機器 (E E)	10
4 6 2	サービス属性証明書	
4 6 3	セキュリティチップ	
4 7 1	ユーザ識別デバイス	
4 7 2	ユーザセキュリティチップ	
4 8 1	ユーザデバイス	
4 8 2	メーカー側機器 (S P)	
4 8 3	サービス情報データベース	
4 8 4	サービス属性証明書	
4 8 5	コントロール属性証明書	
4 9 1	ユーザデバイス	20
4 9 2	メーカー側機器 (S P)	
4 9 3	サービス属性証明書	
4 9 4	コントロール属性証明書	
5 0 1	チャットルーム提供サービスプロバイダ (S P)	
5 0 2	セキュリティモジュール	
5 1 1	甲さん通信端末 (E E)	
5 1 2	セキュリティチップ	
5 2 1	ユーザ識別デバイス	
5 2 2	ユーザセキュリティチップ	
5 2 3	グループ属性証明書 A C 0 1	30
5 2 4	グループ属性証明書 A C 0 2	
5 3 1	乙さん通信端末 (E E)	
5 3 2	セキュリティチップ	
5 3 3	ユーザ識別デバイス (U I D)	
5 3 4	ユーザセキュリティチップ (U S C)	
6 0 1	セキュリティモジュール	
6 0 2	公開鍵暗号エンジン	
6 0 3	共通鍵暗号エンジン	
6 0 5	セキュリティチップ	
6 0 6	公開鍵暗号エンジン	40
6 0 7	共通鍵暗号エンジン	
6 0 8	共通鍵メモリ領域	
6 1 1	登録鍵生成実行属性証明書 (A C)	
6 1 2	登録鍵生成実行結果	
6 1 3	実行命令	
6 1 4	サービス提供実行属性証明書 (A C)	
6 1 5	暗号化データ	
6 1 6	データ	
6 1 7	リセット処理命令	
6 2 1	リセット確認実行属性証明書 (A C)	50

6 2 2	リセット確認結果	
6 2 3	登録鍵破棄実行属性証明書 (A C)	
7 0 1	回数制限付きサービス提供実行属性証明書 (A C)	
7 0 2	暗号化データ	
7 0 3	データ	
7 0 4	回数制限付きサービス提供実行属性証明書 (A C)	
7 0 5	回数制限付きサービス提供実行属性証明書 (A C)	
7 0 6	暗号化データ	
7 0 7	データ	
7 1 1	譲渡機能付きサービス提供実行属性証明書 (A C)	10
7 1 2	譲渡実行トリガ	
7 1 3	グループ属性証明書	
7 1 4	データ	
7 1 5	登録鍵生成実行属性証明書 (A C)	
7 2 1	登録鍵生成実行結果	
7 2 2	譲渡機能付きサービス提供実行属性証明書 (A C)	
7 3 1	譲渡機能付きサービス提供実行属性証明書 (A C)	
7 3 2	暗号化データトリガ	
7 3 3	暗号化データ	
7 3 4	データ	20
8 0 1	グループ属性証明書	
8 0 2	審査代行グループ属性証明書	
8 0 3	審査代行実行属性証明書	
8 0 4	代理署名鍵証明書	
8 1 1	発行者	
8 1 2	審査代行者	
8 1 3	A C 利用者 (属性保持者)	
8 1 4	検証者	
8 2 1	代理署名鍵証明書	
8 2 2	審査代行実行属性証明書	30
8 2 3	審査代行グループ属性証明書	
8 5 1	審査代行実行属性証明書 (代理署名実行属性証明書)	
8 5 2	グループ属性証明書	
8 5 3	付加情報	
8 5 4	審査代行グループ属性証明書 (代理署名グループ属性証明書)	
9 2 1	グループ属性証明書	
9 2 2	代理署名グループ属性証明書	
9 2 3	代理署名実行属性証明書	
9 2 4	代理署名鍵証明書	
9 3 1	発行者	40
9 3 2	A C 利用者 (属性保持者)	
9 3 3	検証者	
9 4 1	代理署名鍵証明書	
9 4 2	代理署名実行属性証明書	
9 4 3	代理署名グループ属性証明書	
9 5 1	C P U (Central processing Unit)	
9 5 2	R O M (Read-Only-Memory)	
9 5 3	R A M (Random Access Memory)	
9 5 4	H D D	
9 5 5	入力部	50

- 9 5 6 出力部
- 9 5 7 通信部
- 9 5 8 ドライブ
- 9 5 9 リムーバブル記録媒体
- 9 6 0 バス
- 9 6 1 入出力インタフェース
- 9 6 2 セキュリティチップ

【 図 1 】



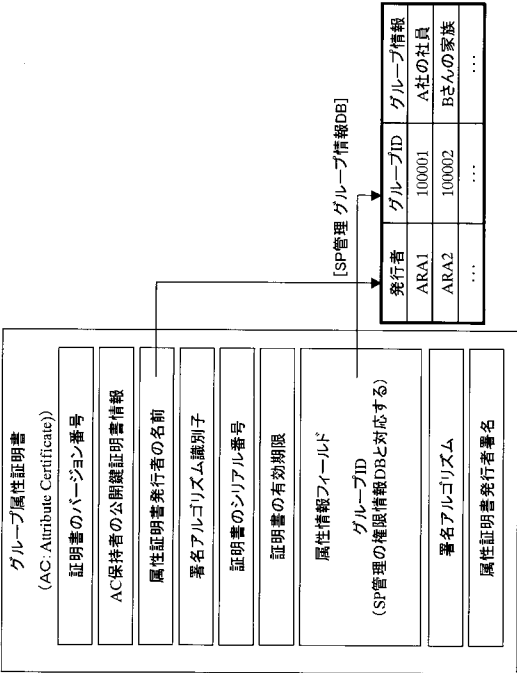
【 図 2 】

Ver sion	項目	説明
V-1	version	証明書のフォーマットのバージョン
	serialNumber	証明書発行者によって割り当てられる証明書番号
	signature	証明書の署名アルゴリズム
	issuer	証明書発行者名(Distinguished Name形式)
	validity notBefore notAfter	証明書の有効期限 開始日時 終了日時
	subject	証明書所有者名
	subjectPublicKeyInfo algorithm subjectPublicKey	証明書所有者の公開鍵情報 鍵のアルゴリズム 鍵

【図 3】

V-3	<div> <div>authorityKeyIdentifier keyIdentifier authorityCertIssuer authorityCertSerialNumber</div> <div>署名検証に用いる証明書発行者の鍵識別子 鍵識別子 機関証明書発行者名 (General Name 形式) 機関証明書シリアルナンバー</div> </div>	<div> <div>subjectKeyIdentifier keyIdentifier</div> <div>複数の鍵の中から目的の鍵を明確に識別</div> </div>
	<div> <div>key usage (1) digitalSignature (2) nonRepudiation (3) keyEncipherment (4) dataEncipherment (5) keyAgreement (6) keyCertSign</div> <div>鍵の使用目的を指定 (0) デジタル署名用 (1) 否認防止用 (2) 鍵の暗号化用 (3) メッセージの暗号化用 (4) 共通鍵配送用 (5) 認証の署名確認用 (6) 失効リストの署名確認</div> </div>	<div> <div>privateKeyUsagePeriod notBefore notAfter</div> <div>証明書中の公開鍵に対応する秘密鍵の有効期限</div> </div>
	<div> <div>certificatePolicies policyIdentifier policyQualifiers</div> <div>証明書発行者が承認した証明書ポリシー ポリシーID (ISO/IEC8334-1 準拠) 認証基準</div> </div>	
	<div> <div>policyMappings issuerDomainPolicy subjectDomainPolicy</div> <div>認証パス中のポリシーの関係を制限 (CA 証明書にのみ必要)</div> </div>	

【図 5】



【図 4】

V-3	<div>subjectAltName</div> <div>証明書所有者の別名 (GN 形式)</div>	<div>issuerAltName</div> <div>証明書発行者の別名 (GN 形式)</div>
	<div>subjectDirectoryAttributes</div> <div>証明書所有者のために必要とされるディレクトリの属性</div>	
	<div>basicConstraints ca pathLenConstraint</div> <div>証明対象の公開鍵が認証局の署名用が、証明書所有者のものかを区別</div>	
	<div>nameConstraints permittedSubtrees base minimum maximum ExcludedSubtrees</div> <div>発行者が発行する証明書の名前を制限</div>	
	<div>policyConstraints requireExplicitPolicy inhibitPolicyMapping</div> <div>認証パス中のポリシーの関係を制限</div>	
	<div>cRLDistributionPoints</div> <div>証明書所有者が証明書を利用する際に、証明書が失効していないかどうかを確認するための失効リストの参照点を記述</div>	
	<div>signatureAlgorithm</div> <div>証明書への署名付けに用いるアルゴリズム</div>	
	<div>signatureValue</div> <div>証明書発行者の秘密鍵による署名</div>	

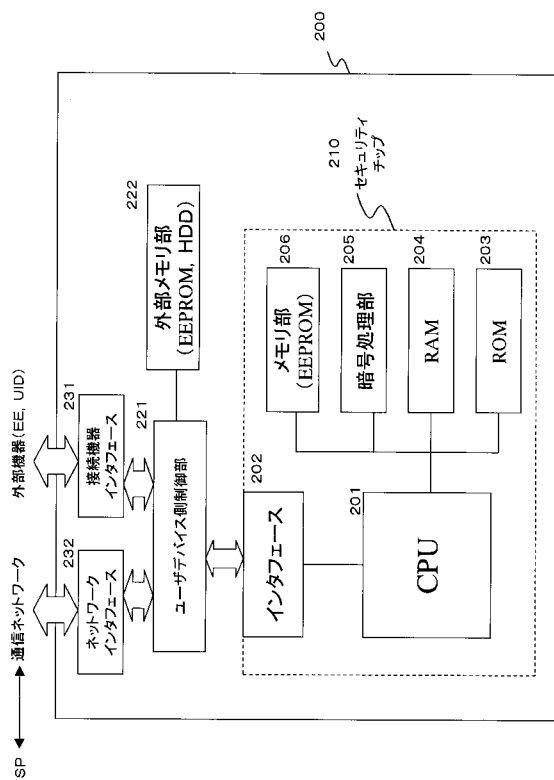
【図 6】

発行者	所有者	検証者	属性情報
グループ ARA	SC, USC	SP, SM	グループ ID

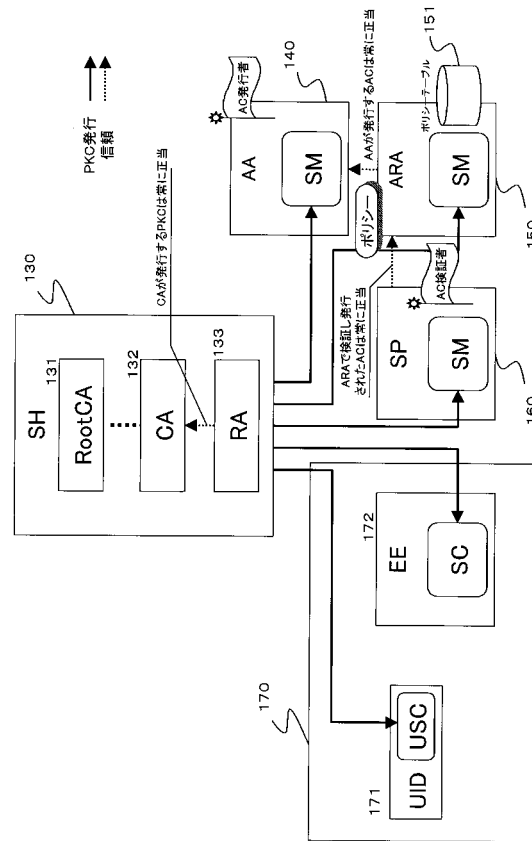
【 図 7 】

グループID	グループ情報	発行ポリシー
1234-0	ゲーム配信サービス会員	<ul style="list-style-type: none"> •正格のゲーム機を所有 •EE PKC等で確認 •ゲーム配信サービス入会金を支払済
1234-5-10	ゲーム10回利用会員	<ul style="list-style-type: none"> •ゲーム配信サービスに加入済 ゲーム配信サービス会員ACを所有 •10回制限に同意
...

【 図 9 】



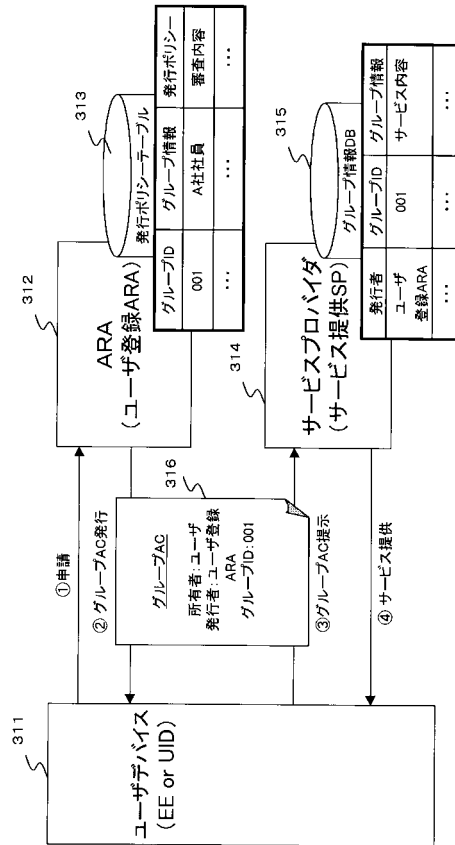
【 図 8 】



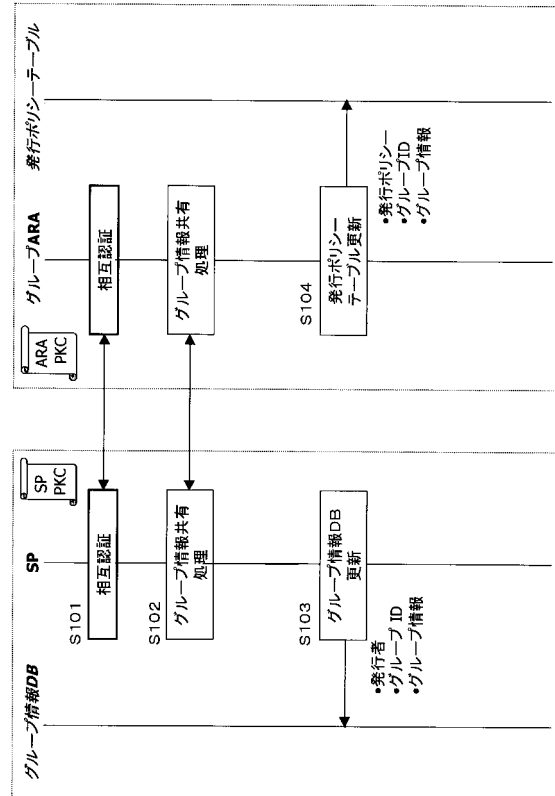
【 図 1 0 】

データ種別	データ内容
公開鍵証明書	<ul style="list-style-type: none"> ・ルート認証局公開鍵証明書 ・サービスプロバイダ公開鍵証明書
グループ属性証明書	<ul style="list-style-type: none"> ・機器の属するまたはユーザの属するグループ対応の属性証明書
実行属性証明書	<ul style="list-style-type: none"> ・暗号化実行命令、暗号化実行命令の復号用発行者鍵を格納したメモリアドレスデータを含む属性証明書
鍵データ	<ul style="list-style-type: none"> ・セキユリティチップ公開鍵、秘密鍵ペア ・登録鍵 ・リセット鍵 ・乱数生成用鍵、相互認証用鍵
識別情報	<ul style="list-style-type: none"> ・セキユリティチップID ・サービスプロバイダID ・ユーザID ・アプリケーションID
その他	<ul style="list-style-type: none"> ・乱数シード(Seed) ・サービス利用情報等

【図 1 1】



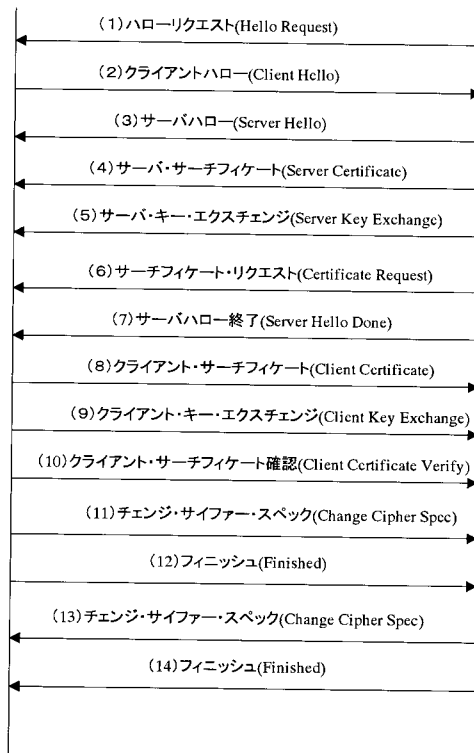
【図 1 2】



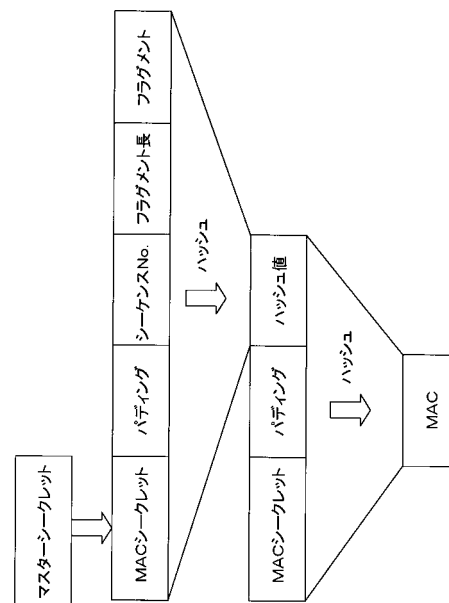
【図 1 3】

エンティティA
(クライアント)

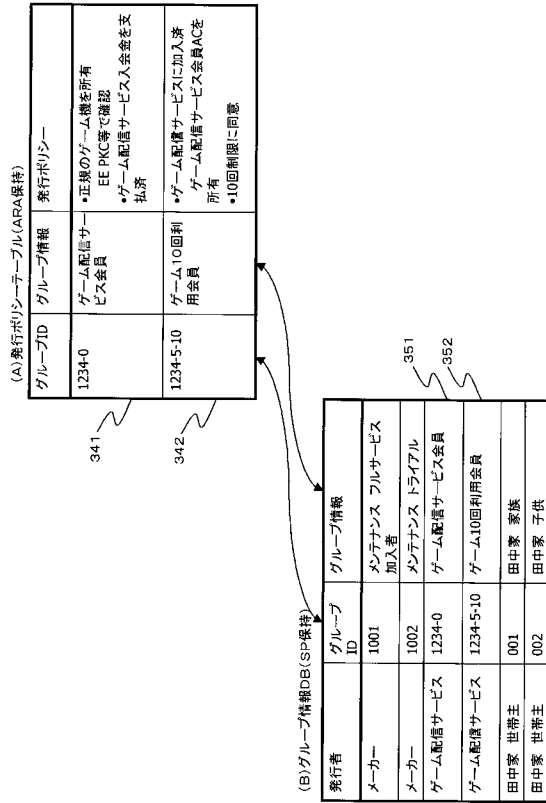
エンティティB
(サーバ)



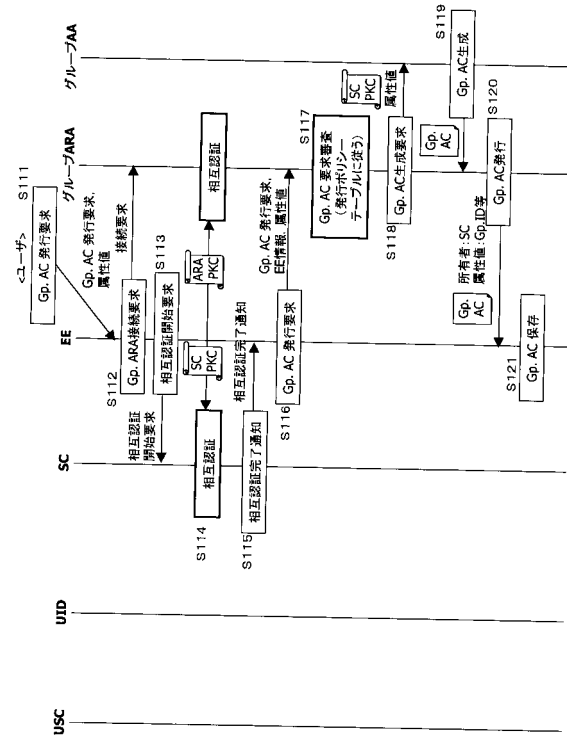
【図 1 4】



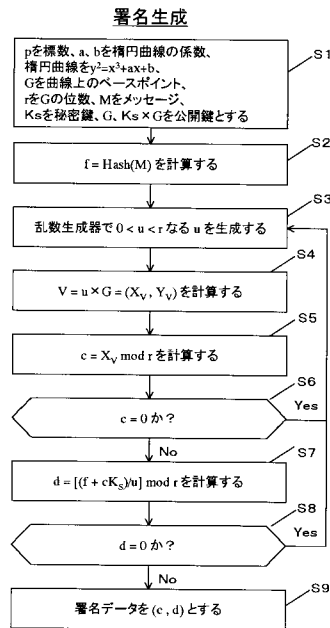
【図 15】



【図 16】

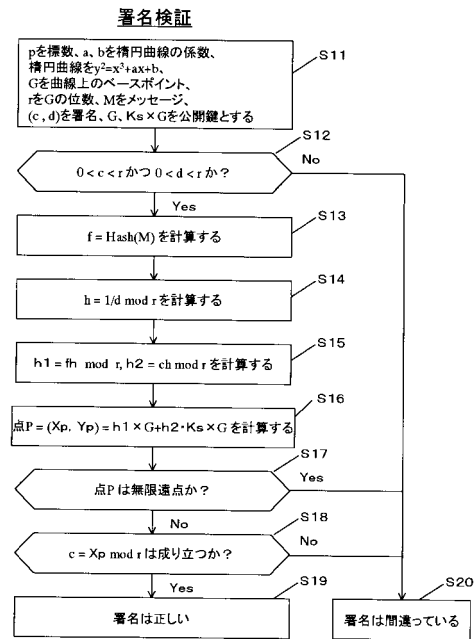


【図 17】



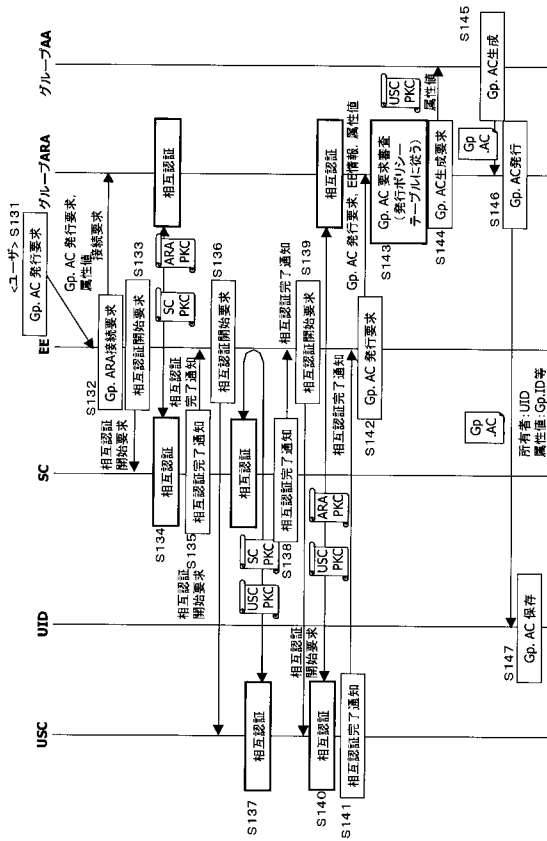
署名生成(IEEE P1363/D13)

【図 18】

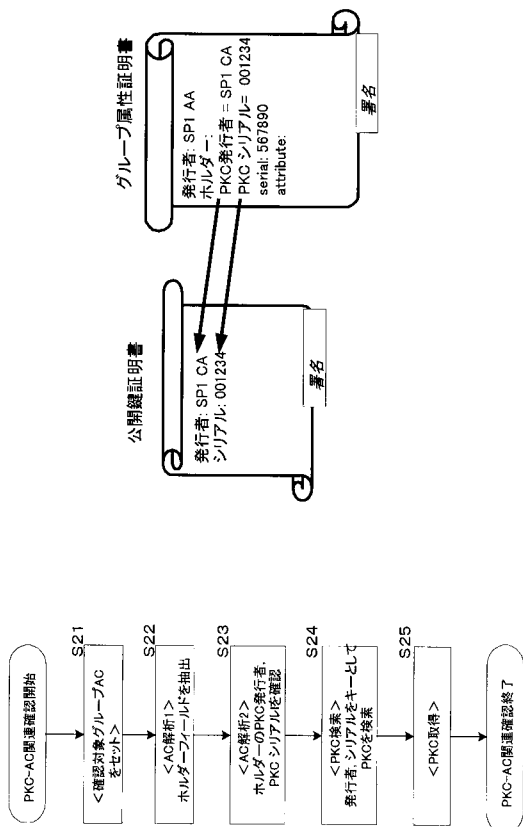


署名検証(IEEE P1363/D13)

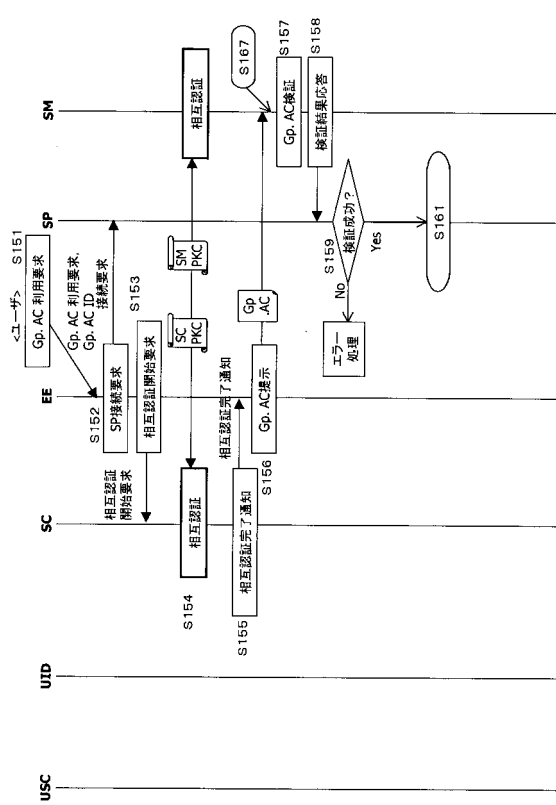
【図 19】



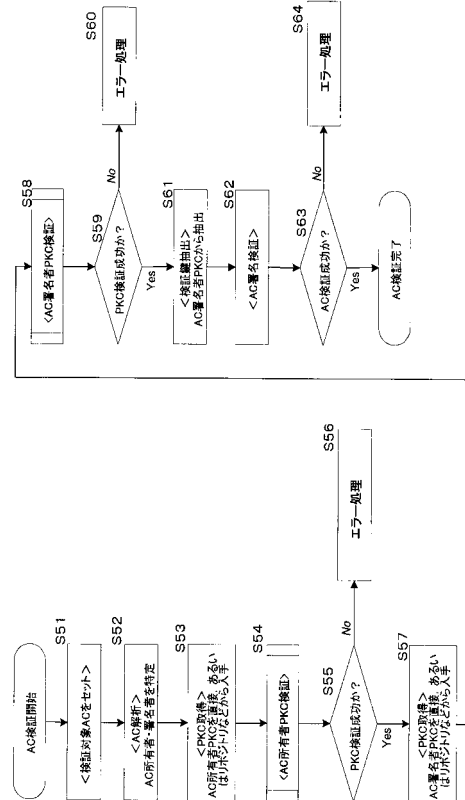
【図 21】



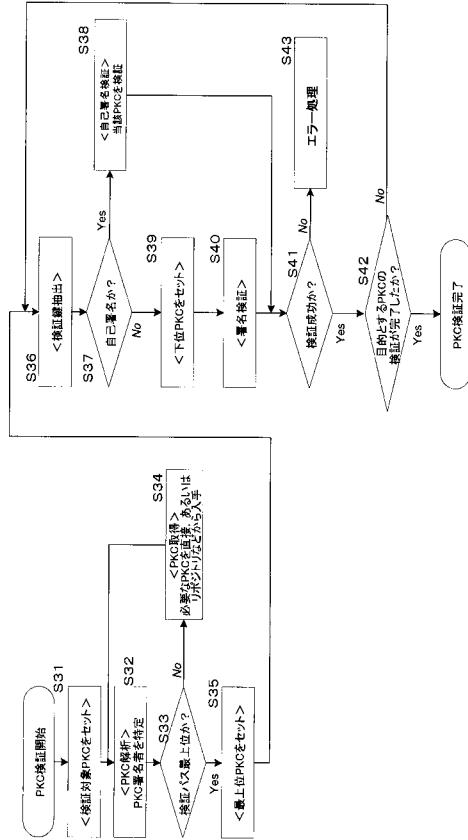
【図 20】



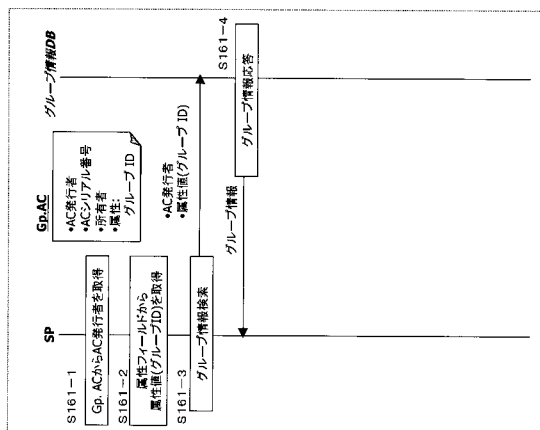
【図 22】



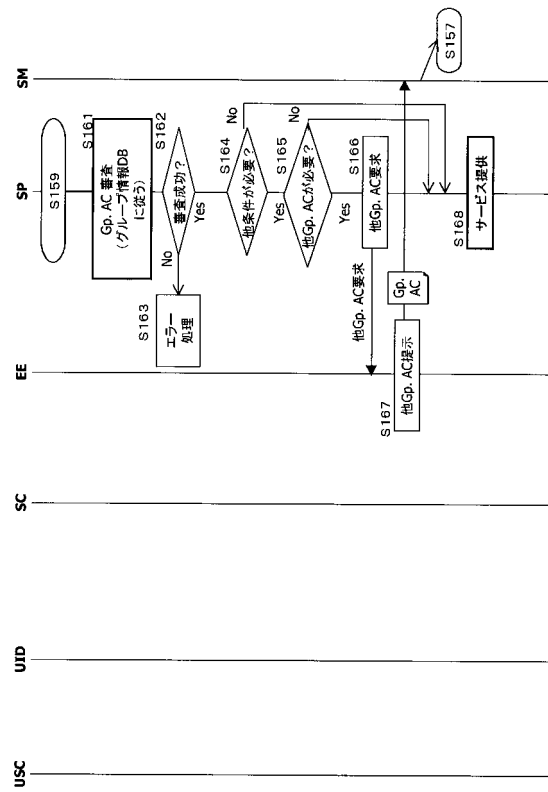
【図 23】



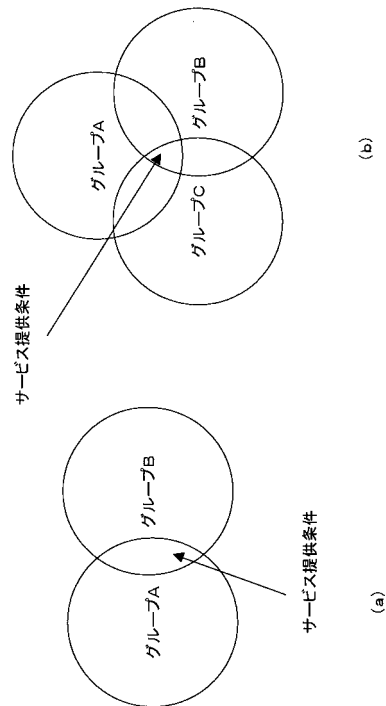
【図 25】



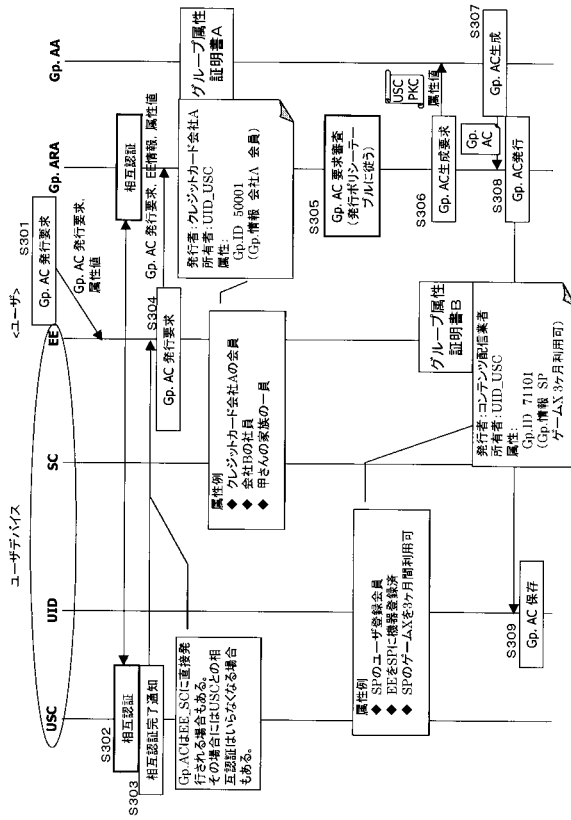
【図 24】



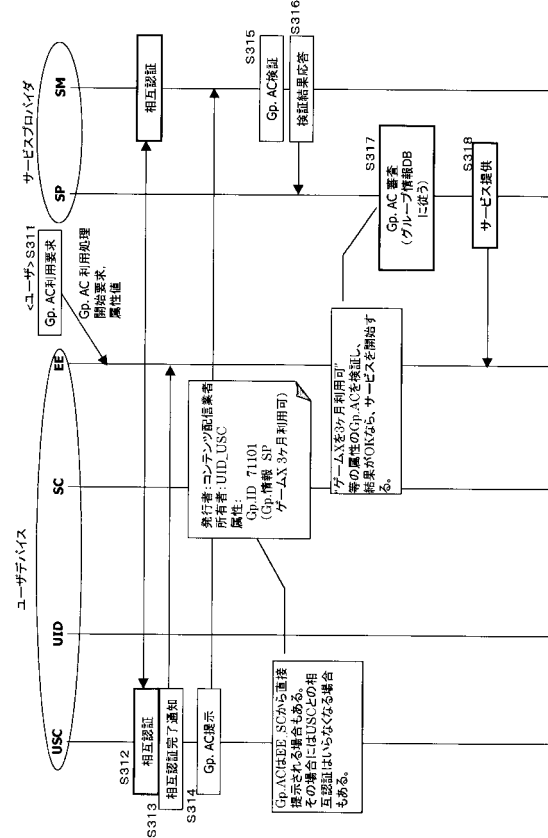
【図 26】



【図 35】



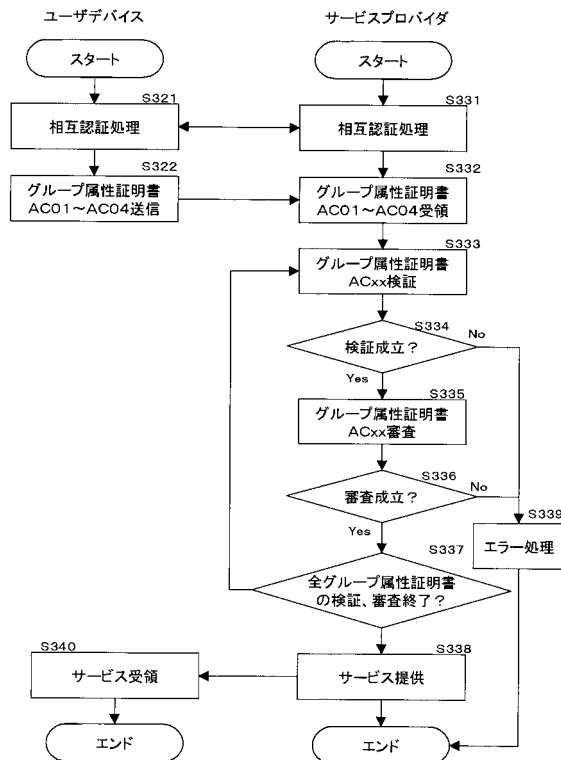
【図 36】



【図 37】

AC名称	属性情報 (=発行ポリシー)	発行者(グループ AA,ARA)	所有者
1. 学生証 AC01	発行者の学生である	A大学の運営(管理)するAA)	ユーザC君のUIDの USC
2. 美術講座受講証 AC02	発行者の開催する美術 講座受講権利者である	A大学の運営(管理)するAA)	ユーザC君のUIDの USC
3. 管理機器証明書 AC03	発行者の管理する機器 である	A大学の運営(管理)するAA)	エンドエンティティ(EE) としてのテレビDのSC
4. 教育用機器証明書 AC04	教育使用目的の機器で ある	文部科学省(の運営 (管理)するAA)	エンドエンティティ(EE) としてのテレビDのSC

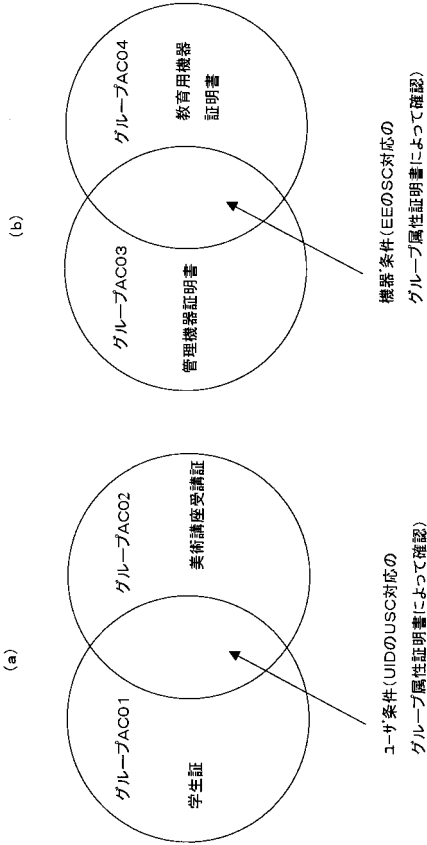
【図 38】



【図 39】

サービス	AC発行者、AC	...	AC以外の情報	...
コンテンツB視聴	A大卒、学生証		文部科学省、教育用機器証明書	
コンテンツB視聴				
...				
コンテンツG視聴				

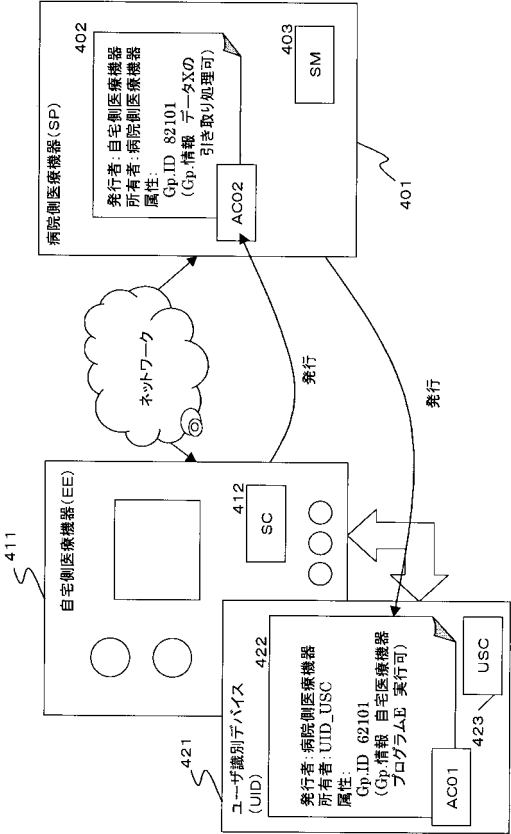
【図 40】



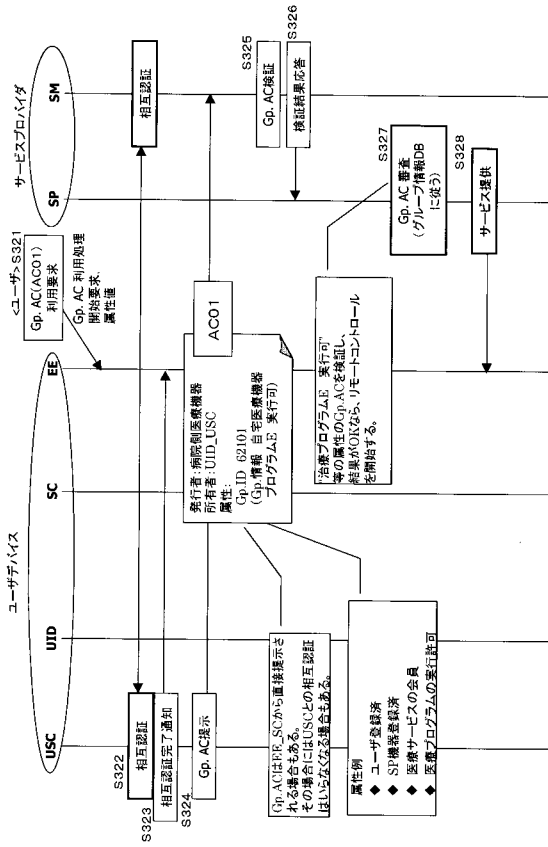
【図 41】

	発行者	所有者	検証者	属性
AC01	病院側医療機器 (SP)	甲さんUID_USC or EE_SC	病院側医療機器 (SP_SM)	プログラムE実行可
AC02	自宅側医療機器 (EE)	病院側医療機器 (SP_SM)	自宅側医療機器 (EE_SC)	データXの引き取り処理可

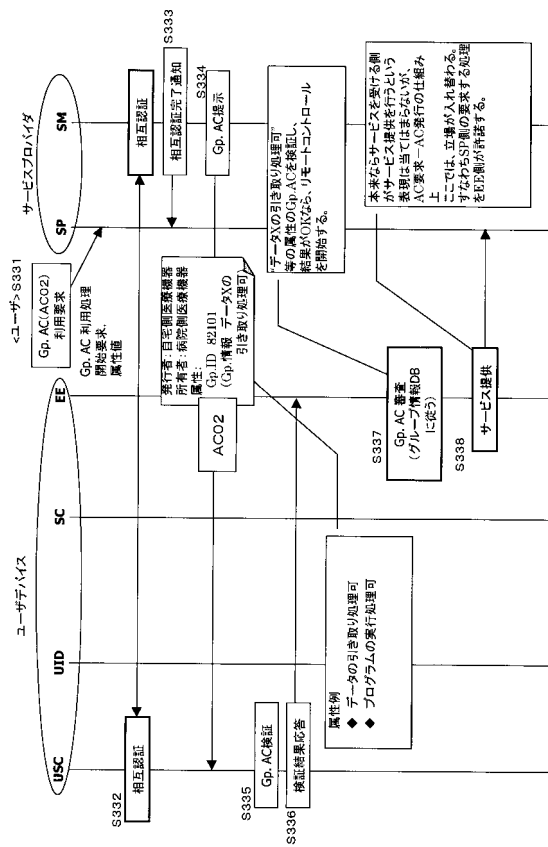
【図 42】



【 図 4 3 】



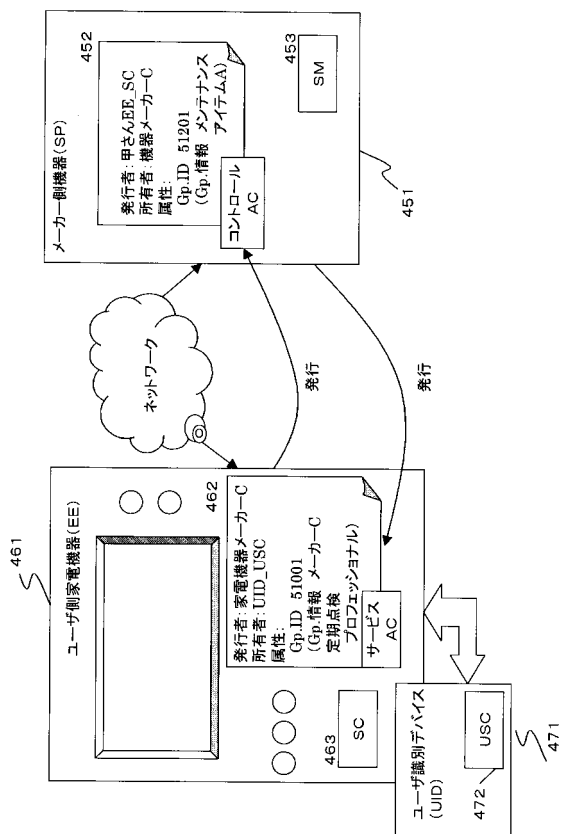
【 図 4 4 】



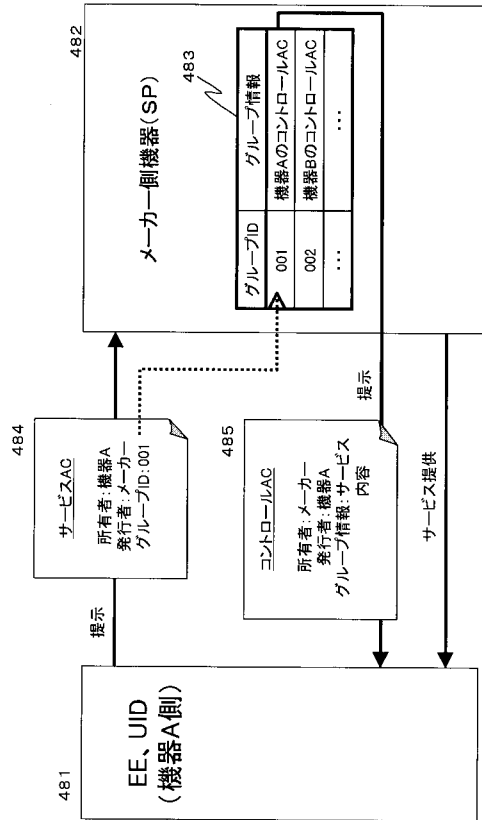
【 図 4 5 】

発行者	発行タイミング	所有者	検証者	属性
サービスAC	家電機器メーカー (SP)	甲さん、 UTD、USC or EE、SC	SP、SM	EE：メンテナンス サービス内容
コントロール AC	家電機器 (EE)	事相or自動メンテナンス時	SP、SM	家電機器 コントロール制限 範囲 X

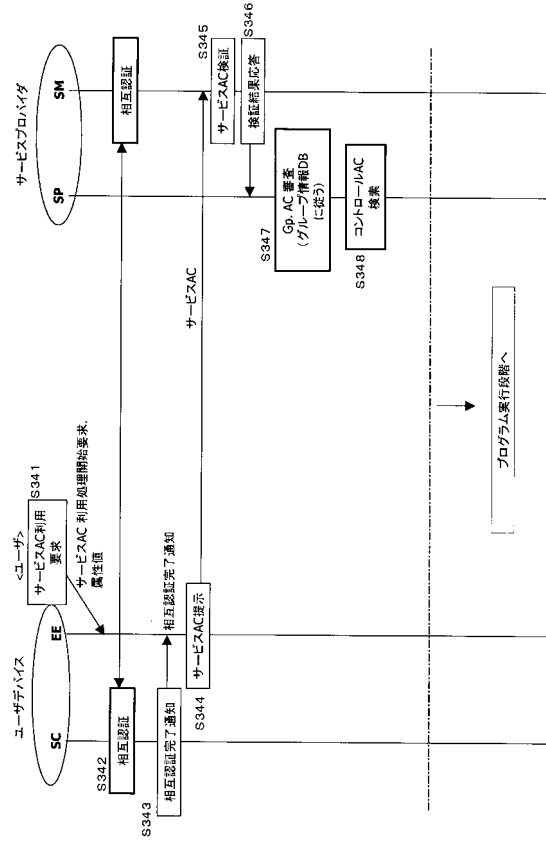
【 図 4 6 】



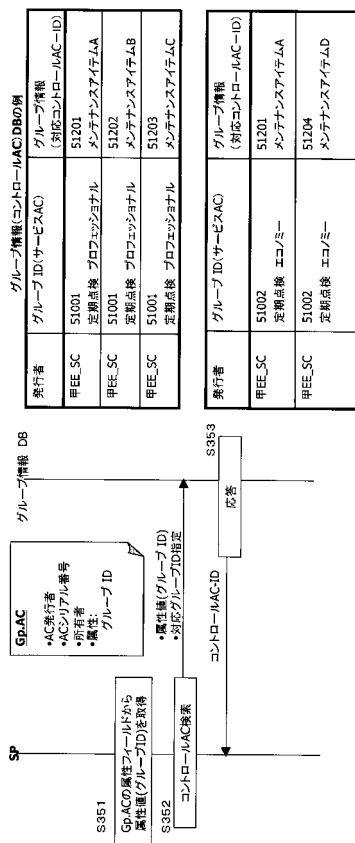
【 図 4 7 】



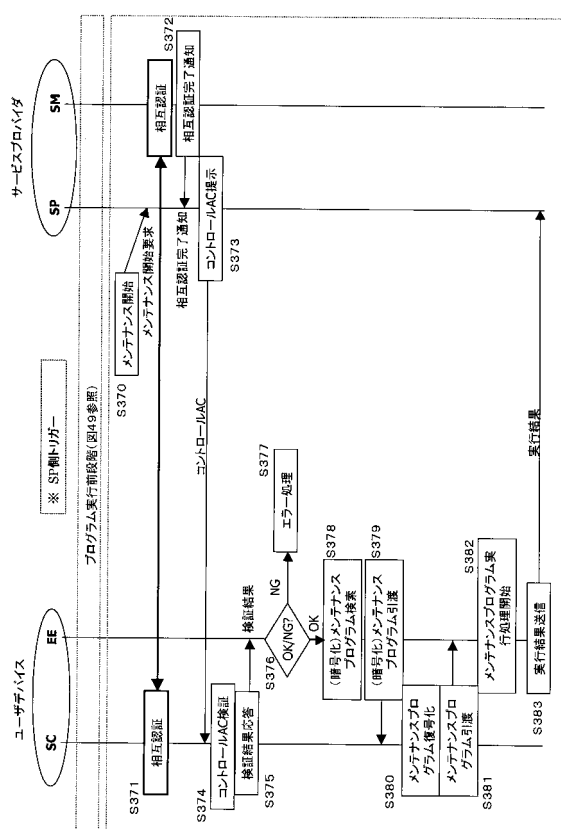
【 図 4 8 】



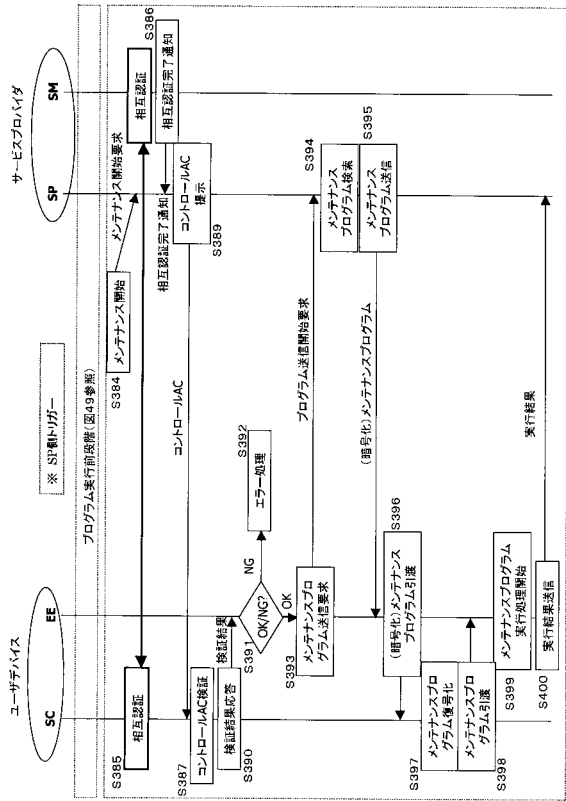
【 図 4 9 】



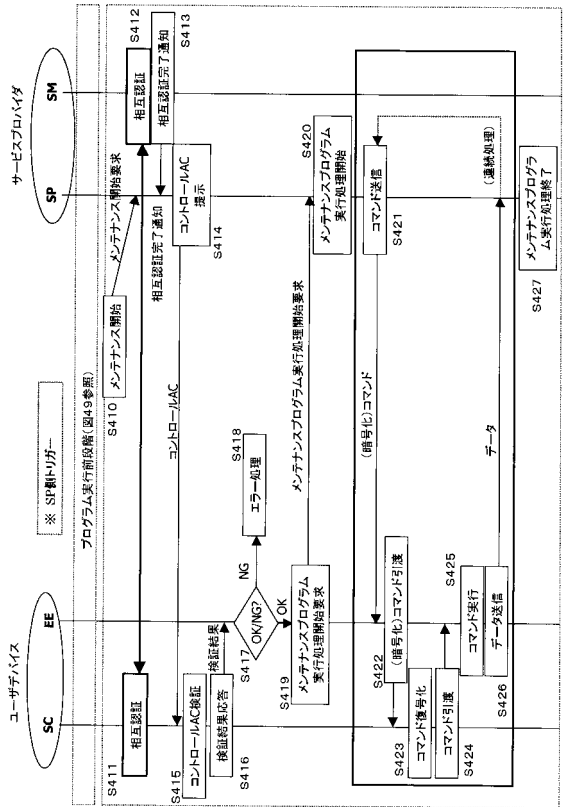
【 図 5 0 】



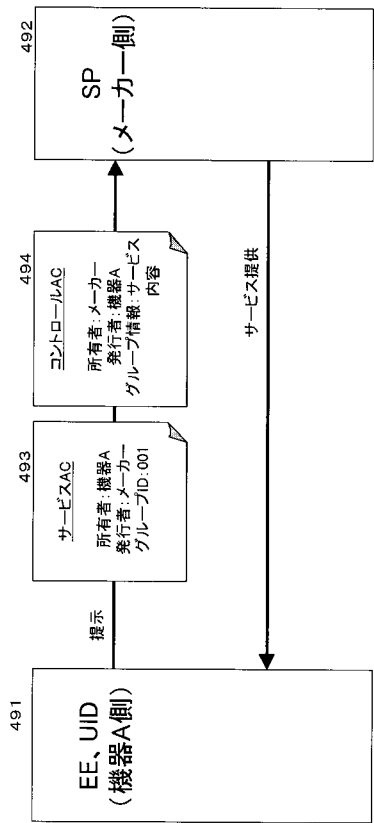
【図 5 1】



【図 5 2】



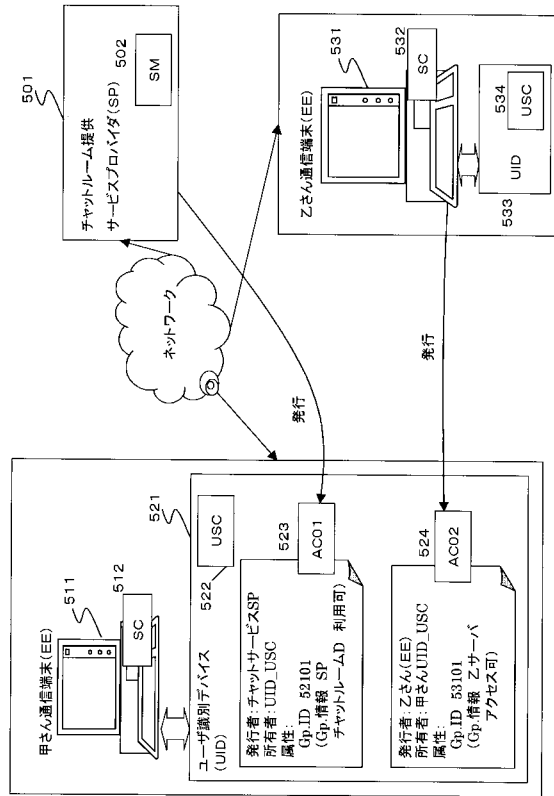
【図 5 3】



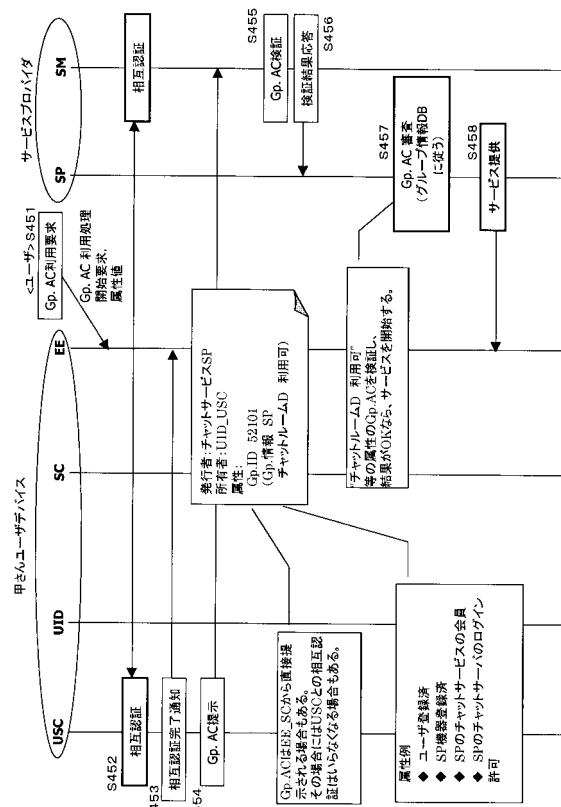
【図 5 4】

発行者	発行タイミング	所有者	検証者	属性
AC01	チャット 運営者(SP)	甲さん UID_USC or EE_SC	SP_SM	SP サーバアクセス権
AC02	乙さん(SP)	甲さん UID_USC or EE_SC	乙さん UID_USC or EE_SC	乙 サーバアクセス権

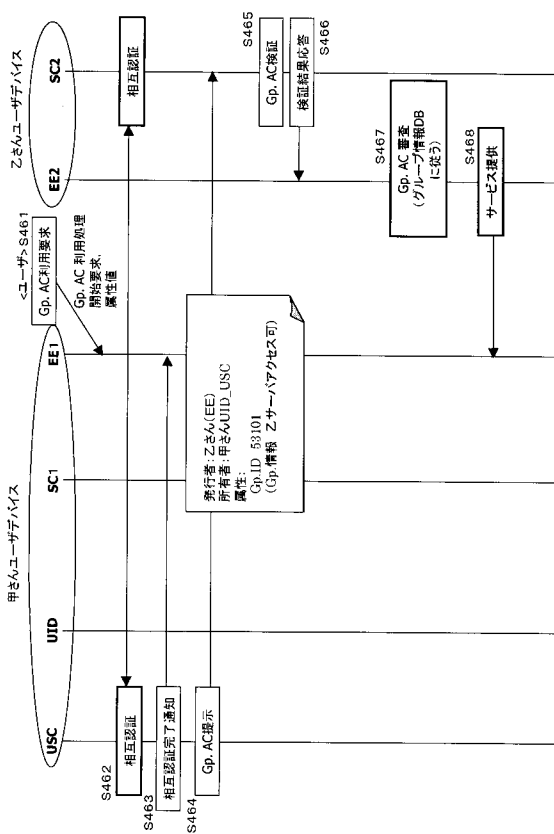
【図 55】



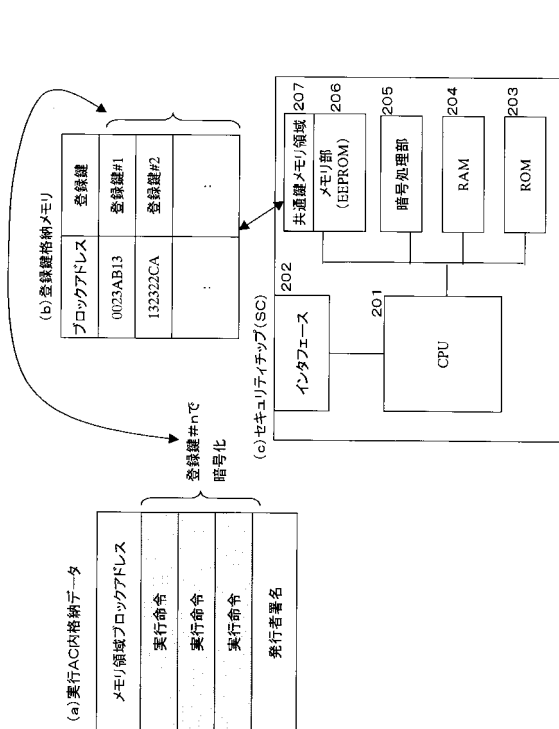
【図 56】



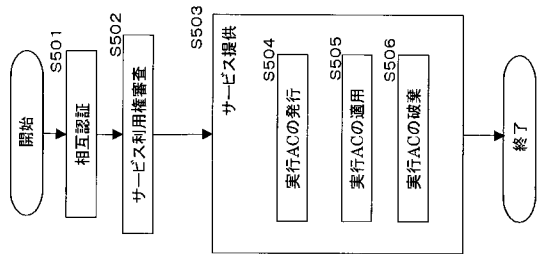
【図 57】



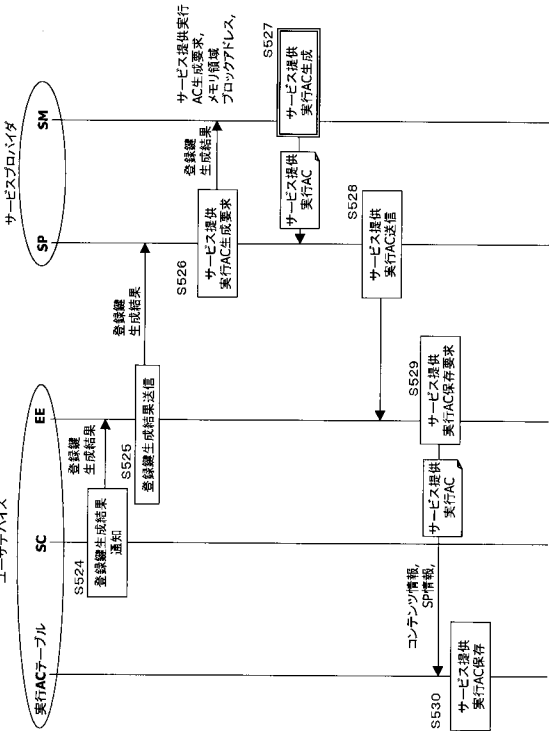
【図 58】



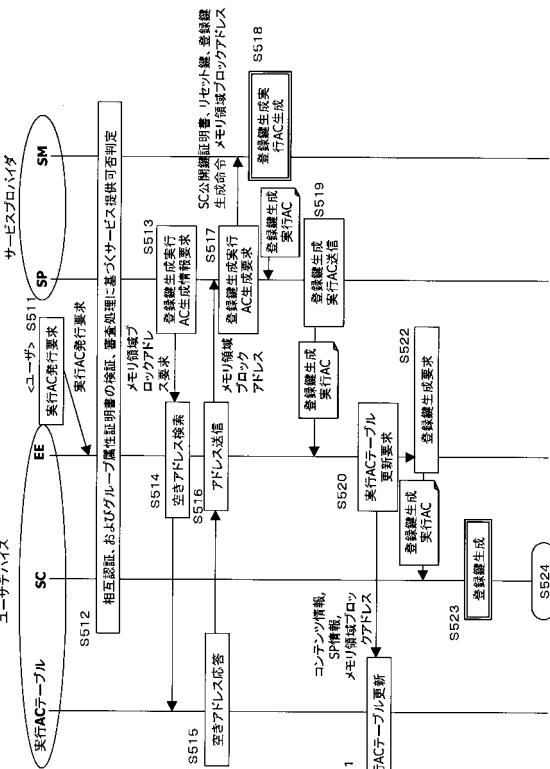
【図 59】



【図 61】



【図 60】

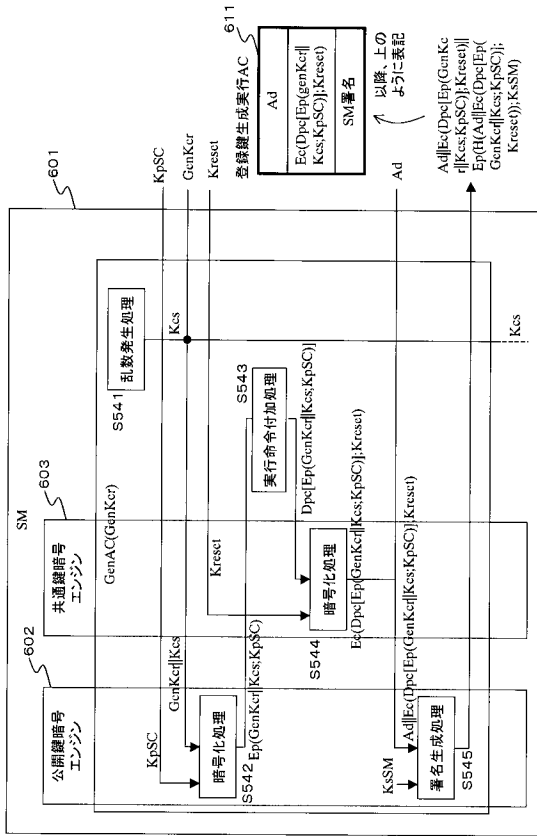


【図 62】

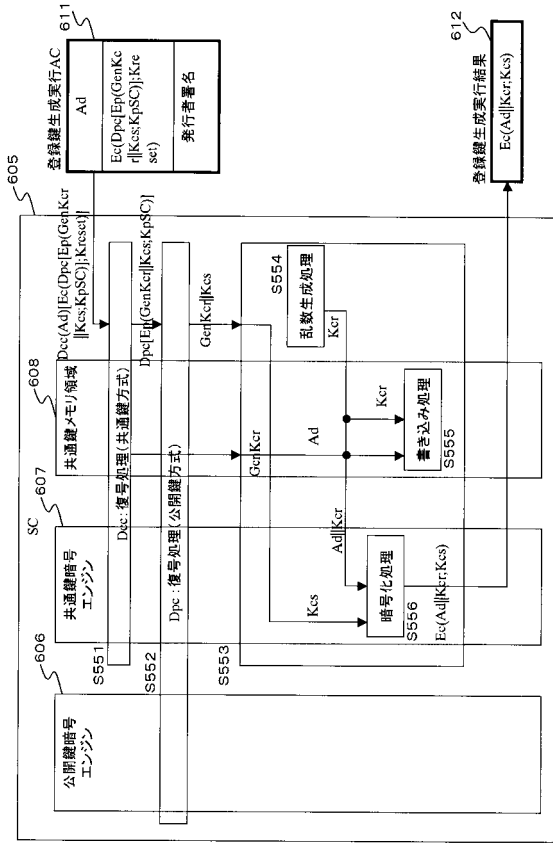
SP 情報	暗号化データ (ex. コンテンツ)情報	暗号化データ(コンテンツ) 復号処理適用実行AC
SP_1	暗号化データ1	実行AC0001
	暗号化データ2	実行AC0002

	暗号化データ11	...
SP_2	暗号化データ12	...
	暗号化データ13	...

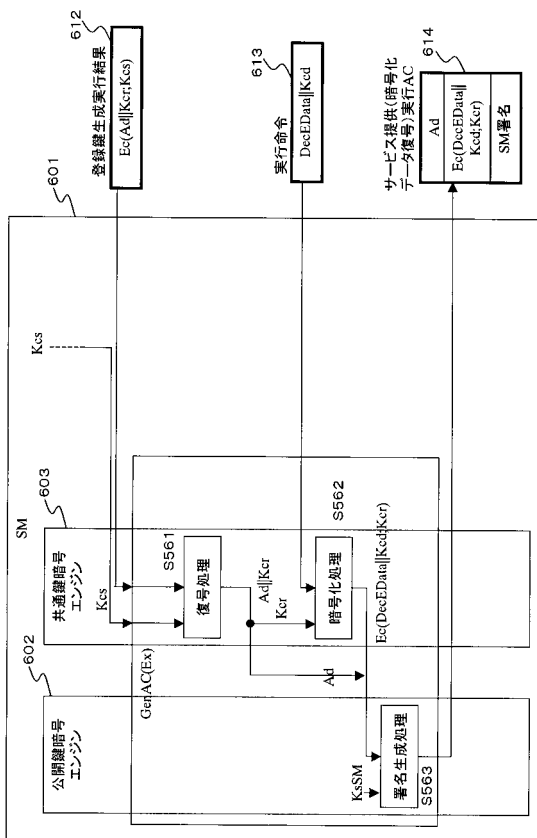
【 図 6 3 】



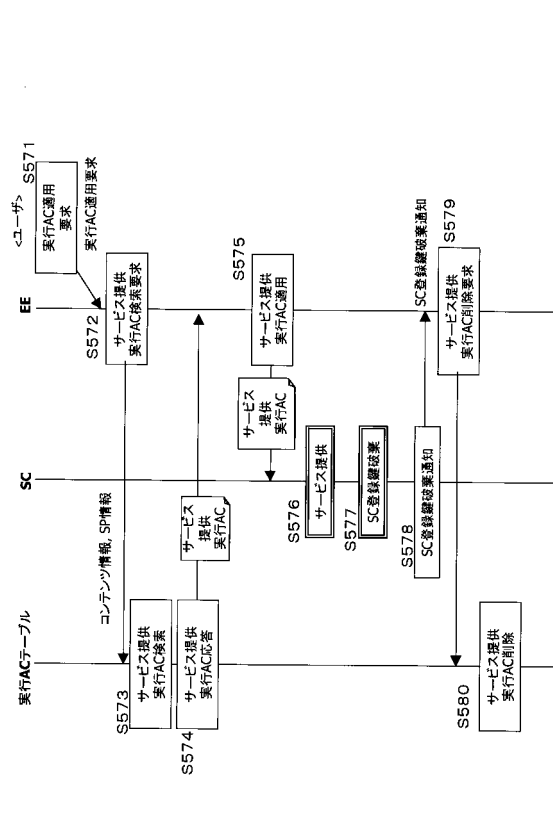
【 図 6 4 】



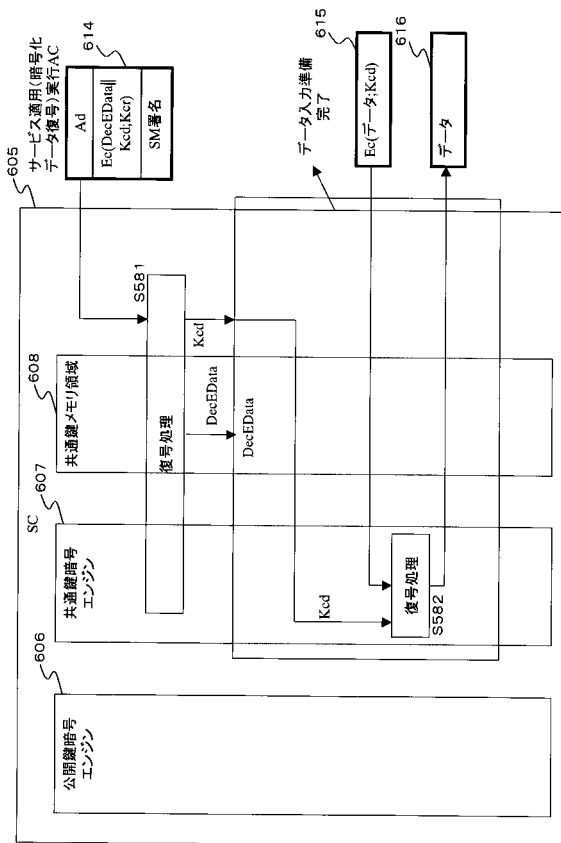
【 図 6 5 】



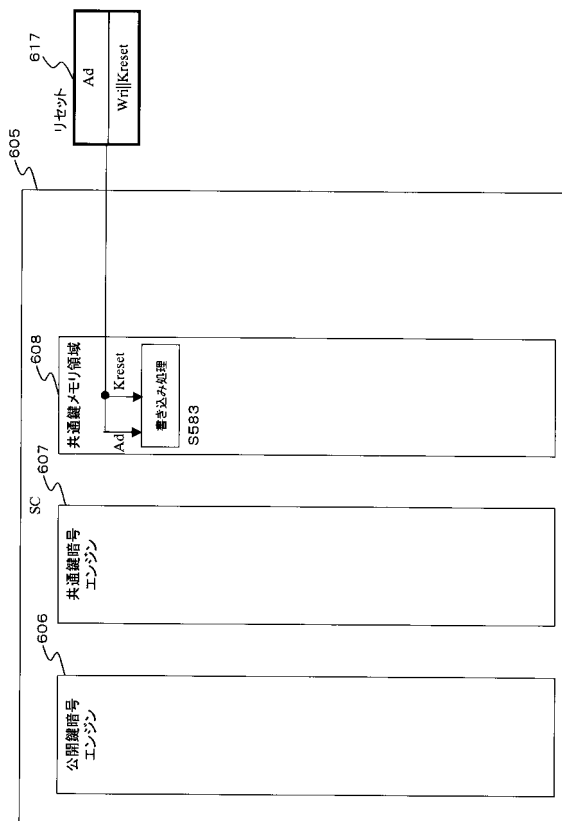
【 図 6 6 】



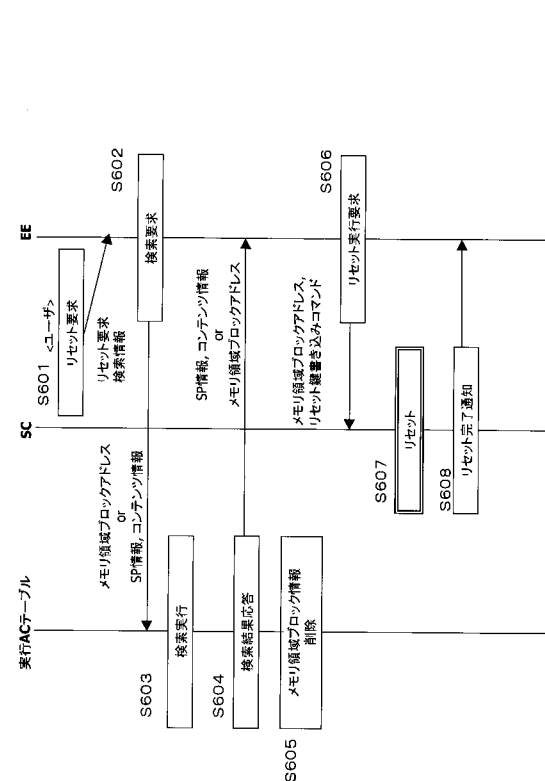
【 図 6 7 】



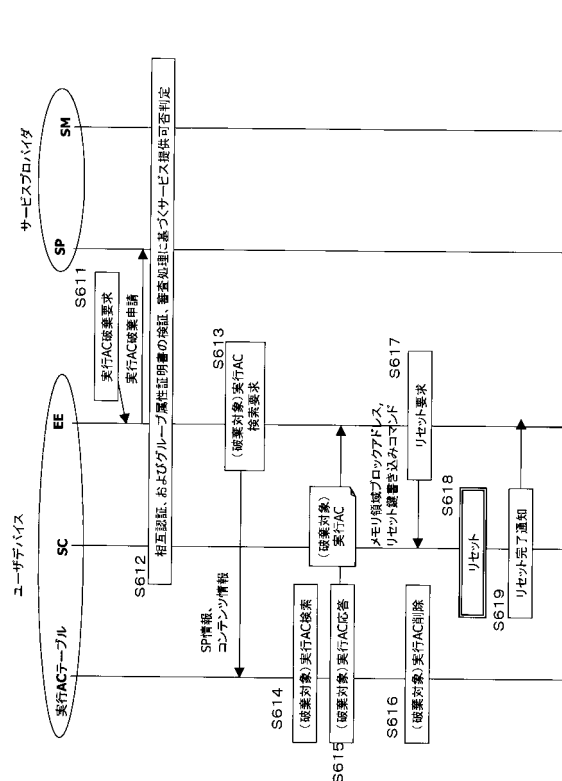
【圖 68】



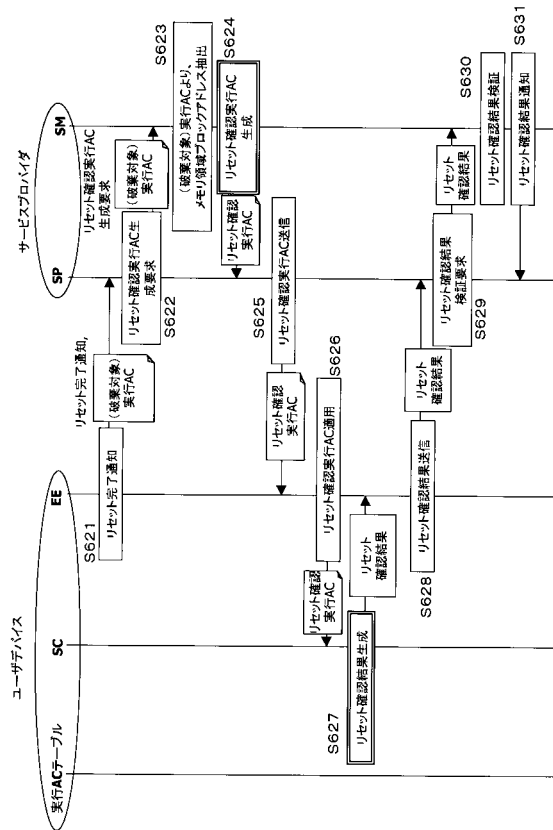
【 図 6 9 】



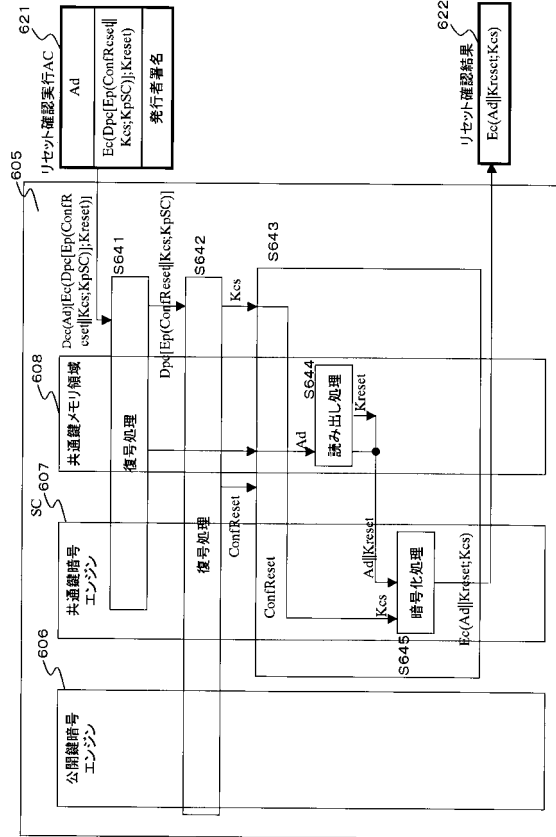
【 図 7 0 】



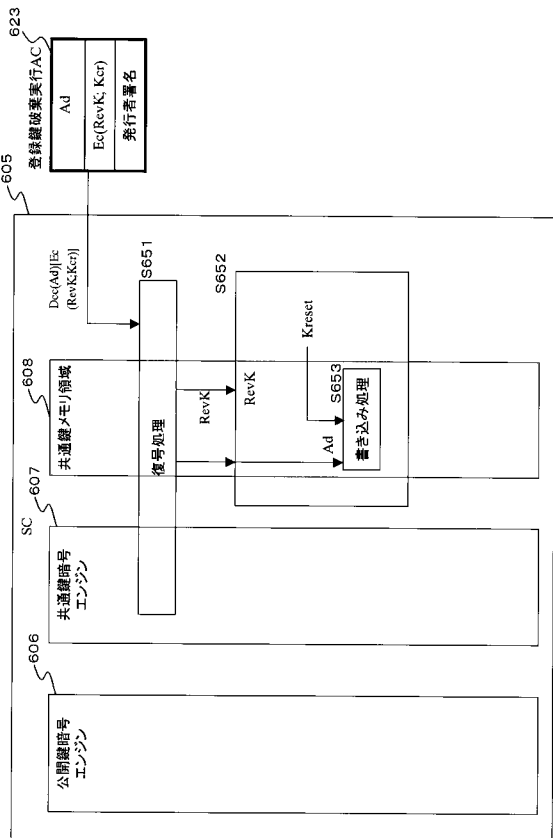
【圖 7 1】



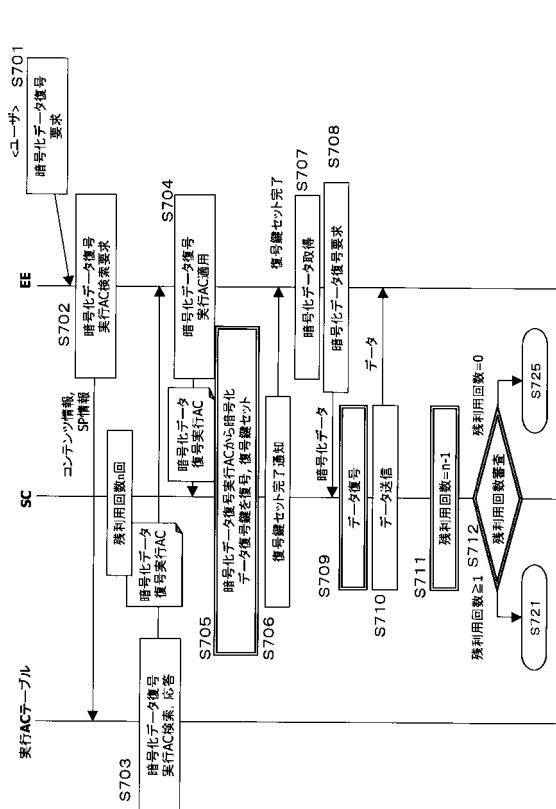
【圖 7 2】



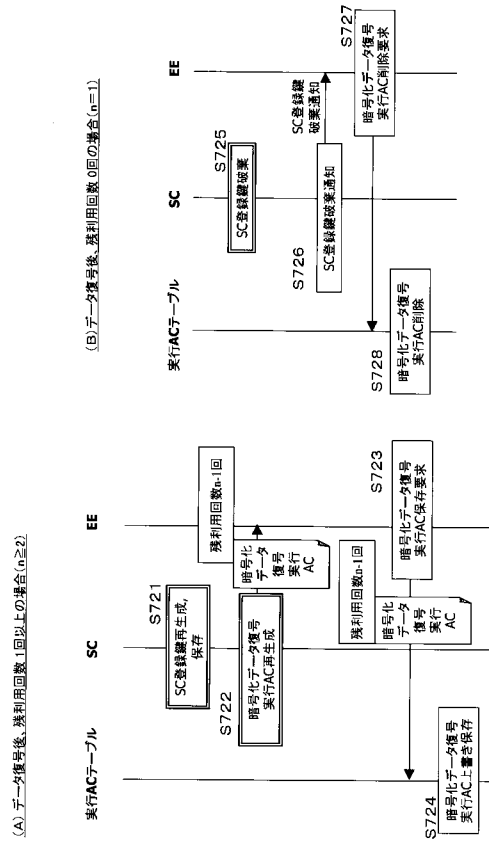
【 図 7 3 】



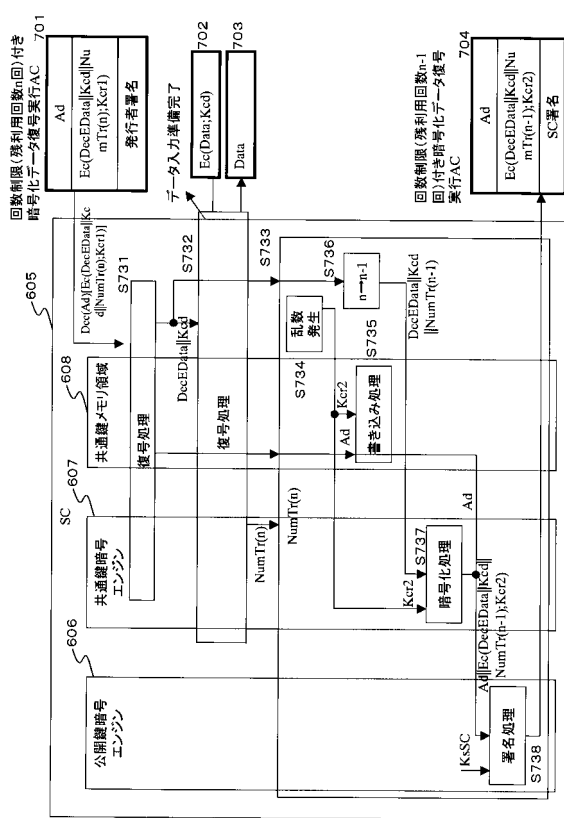
【 図 7 4 】



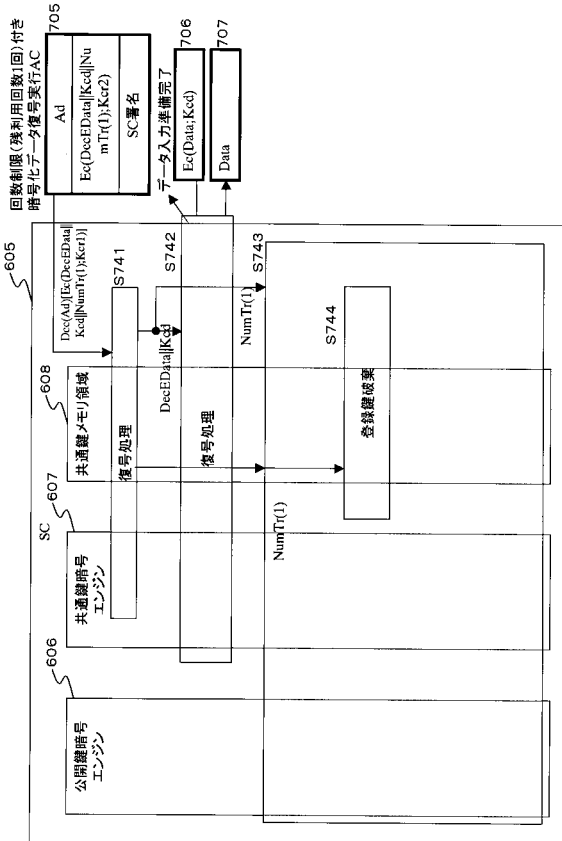
【図 75】



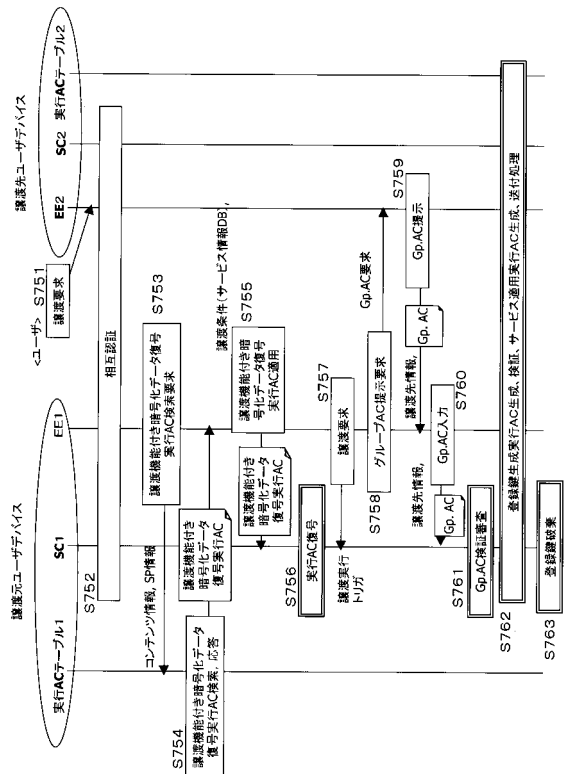
【図 76】



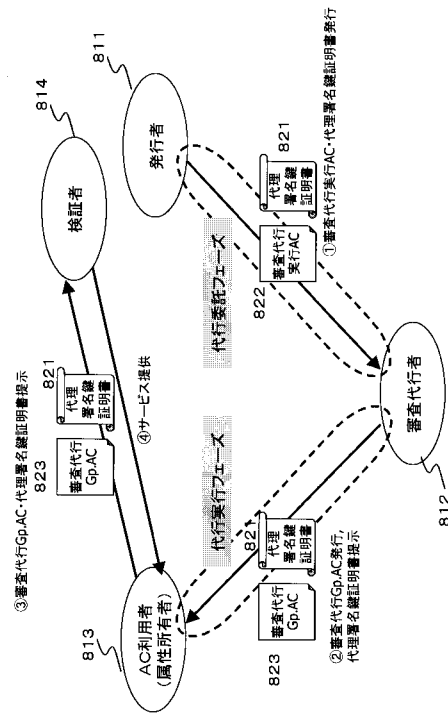
【図 77】



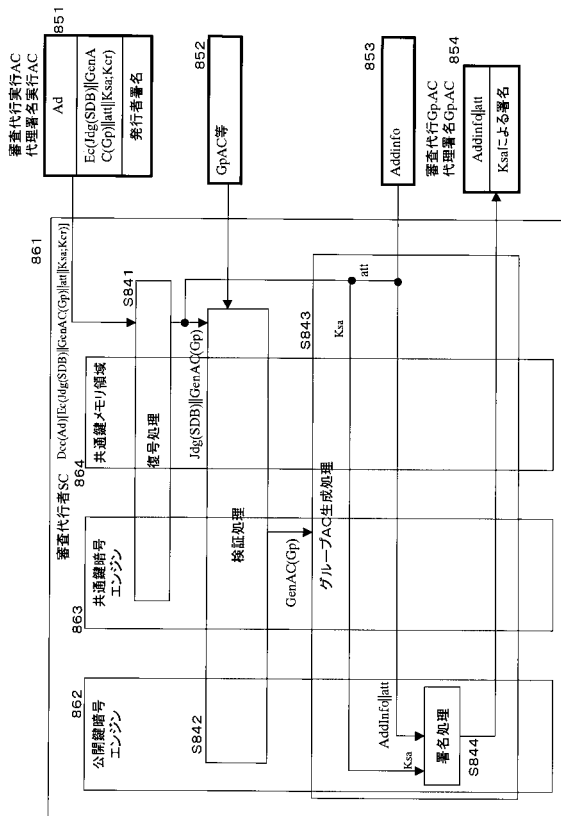
【図 78】



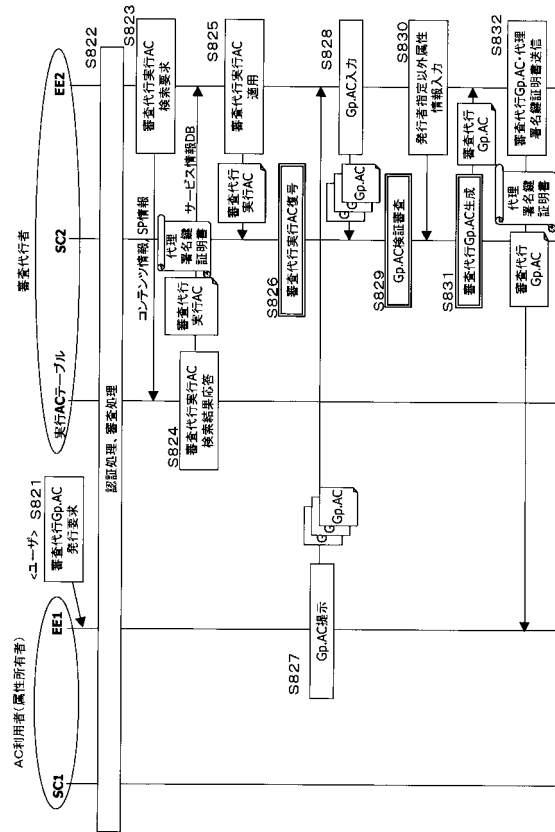
【図 8 3】



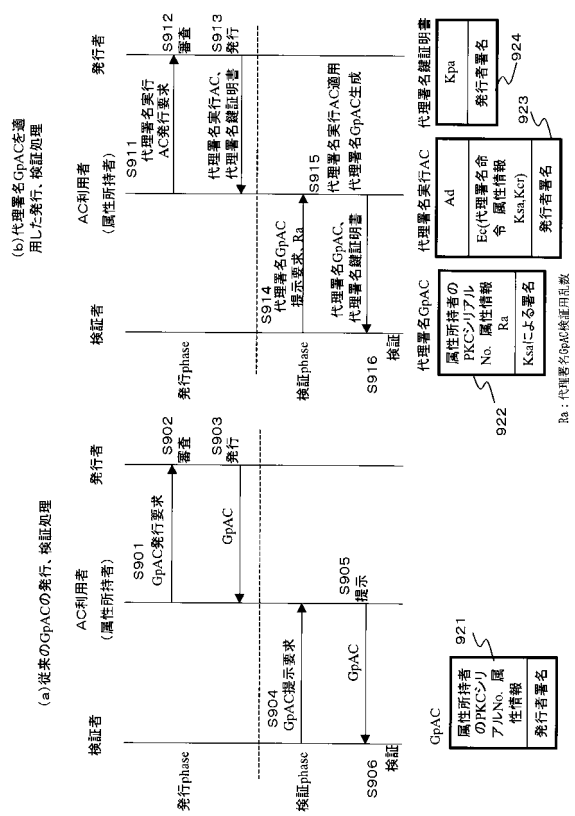
【図 8 5】



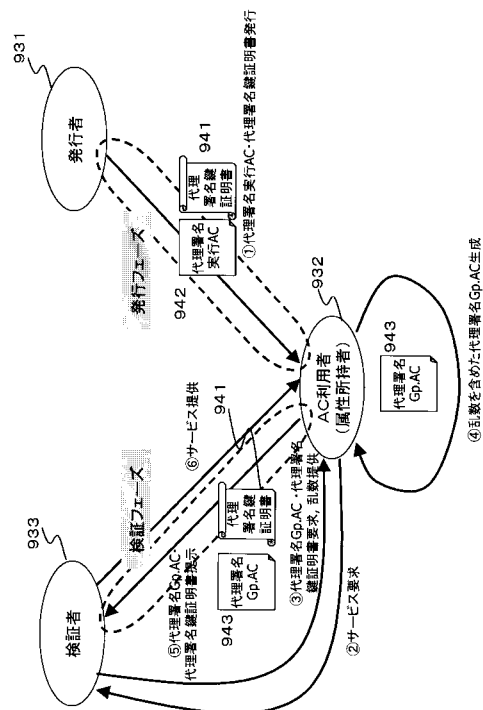
【図 8 4】



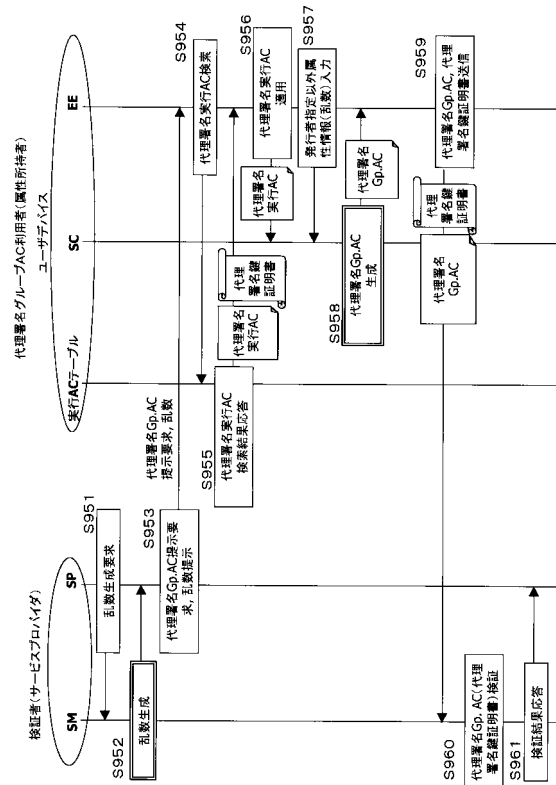
【図 8 6】



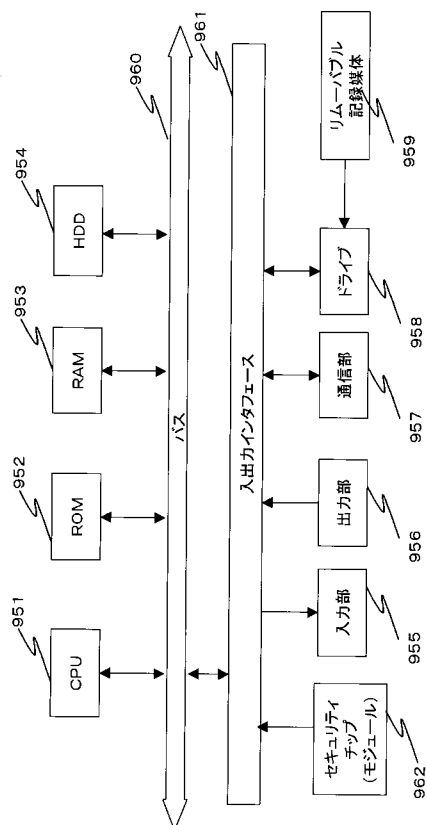
【図 87】



【図 88】



【図 89】



フロントページの続き

- (72)発明者 岡 誠
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 間杉 円
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 石橋 義人
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 阿部 博
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 豊島 信隆
東京都品川区北品川6丁目7番35号 ソニー株式会社内

審査官 速水 雄太

- (56)参考文献 特開2001-237827(JP,A)
特開平5-81204(JP,A)
特開昭55-34520(JP,A)

(58)調査した分野(Int.Cl., DB名)

H04L 9/08

H04L 9/32