(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2008 年10 月23 日 (23.10.2008)

PCT

(10) 国際公開番号
WO 2008/126183 A1

(51) 国際特許分類:
G06F 21/20 (2006.01) *G06F 21/24* (2006.01)

(21) 国際出願番号: PCT/JP2007/055281

(22) 国際出願日: 2007 年3 月15 日 (15.03.2007)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通マイクロエレクトロニクス株式会社 (FUJITSU MICROELECTRONICS LIMITED) [JP/JP]; 〒1630722 東京都新宿区西新宿二丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 高橋 信雄 (TAKAHASHI, Nobuo) [JP/JP]; 〒2220033 神奈川県横浜市港北区新横浜二丁目３番９号 富士通マイクロソリューションズ株式会社内 Kanagawa (JP). 淀川 愛 (YODOKAWA, Ai) [JP/JP]; 〒2220033 神奈川県横浜市港北区新横浜二丁目３番９号 富士通マイクロソリューションズ株式会社内 Kanagawa (JP). 阿部 剛 (ABE, Tsuyoshi) [JP/JP]; 〒2220033 神奈川県横浜市港北区新横浜二丁目３番９号 富士通マイクロソリューションズ株式会社内 Kanagawa (JP).

(74) 代理人: 青木 篤, 外 (AOKI, Atsushi et al.); 〒1058423 東京都港区虎ノ門三丁目５番１号 虎ノ門３７森ビル青和特許法律事務所 Tokyo (JP).

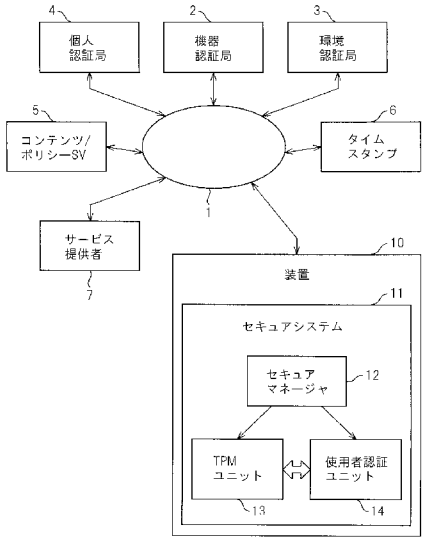
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[続葉有]

(54) Title: SECURE NETWORK SYSTEM, SECURE APPARATUS AND SECURE SYSTEM

(54) 発明の名称: セキュアネットワークシステム、セキュア装置及びセキュアシステム

[図1]



2 EQUIPMENT AUTHENTICATION STATION
3 ENVIRONMENT AUTHENTICATION STATION
4 PERSONAL AUTHENTICATION STATION
5 CONTENTS/POLICY SV
6 TIME STAMP
7 SERVICE PROVIDER
10 APPARATUS
11 SECURE SYSTEM
12 SECURE MANAGER
13 TPM UNIT
14 USER AUTHENTICATION UNIT

(57) Abstract: Security environment increased in reliability is realized in equipment (PC, etc.) needing security on which biometrics and personal authentication using public key system can be mounted. Secure system (11) of one chip mounted on apparatus (10) comprises TPM unit (13), user authentication unit (14) based on biological/password information and secure manager (12) for managing both thereof. The secure manager (12) makes the TPM unit (13) and the user authentication unit (14) cooperate together in the secure system and checks the software environment within the apparatus.

(57) 要約: 公開鍵方式を用いた本人認証、および、生体認証を実装可能なセキュリティを必要とする機器（ＰＣ等）において、より強固なセキュリティ環境を実現する。装置10に搭載される１チップのセキュアシステム11は、ＴＰＭユニット13と、生体／パスワード情報による使用者認証ユニット14と、双方を管理するセキュアマネージャ12と、有する。セキュアマネージャ12はＴＰＭユニット13と使用者認証ユニット14のセキュアシステム内で連携させ、装置内のソフトウェア環境のチェックを実施する。

WO 2008/126183 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明 細 書

セキュアネットワークシステム、セキュア装置及びセキュアシステム

技術分野

[0001] 本発明は、セキュリティを必要とするシステム及び装置全般に関する。

背景技術

[0002] 昨今、情報家電のデジタル化／ネットワーク化が加速される中、コンテンツ配信、遠隔医療等の多種多様サービスにおいては、情報家電の基盤技術としてセキュリティ技術がより一層不可欠なものになっている。そこで、特許文献1から4に記載されるように、カードの認証、生体認証方式による個人の認証、署名鍵による送信元の装置の認証など、各種の認証方法が提案されている。

[0003] 今後のセキュリティ技術を担う代表としてTCG(Trusted Computing Group)が規格化したセキュリティチップであるTPM(Trusted Platform Module)が挙げられ、パーソナル・コンピュータ(PC)の分野では、2007年から2008年にかけてTPMが標準搭載されるようになる予定である。

[0004] TPMによるセキュリティ方式では、その装置(機器)がTPM対応機であり、それを証明するための"RSA非対称鍵(秘密鍵:EK)"と、EK証明書が一般的には工場出荷前に事前に装置に注入され、それによる「装置の信頼」に基づいて、大きく以下の3つの機能を実現している。

[0005] (1)ハードウェアベースのセキュリティ(装置認証機能):プラットフォームに搭載(固定)されたTPMを信頼の拠点としたハードウェアベースのセキュリティを提供する。

[0006] (2)信頼できるプラットフォーム環境の実現(環境認証機能):ソフトウェアの機能的完全性保証により、アプリケーションの安全な実行環境を提供し、プラットフォーム認証を実現する。(PCR制御)

(3)安全なデータ保護:ハードウェアの堅牢性を利用し、ソフトウェアによる攻撃や物理的窃盗による危険からデータ、パスワード、鍵などの情報資産を保護する。

[0007] 前述した通り、以上の機能は、認証局が証明した装置を信頼の基点としている。

[0008] 一方、上記のTPMとは異なり、"個人(自然人)"を対象として、個人認証局が装置

の使用者の正当性を証明(証明を発行)し、それを起点としてサービスを展開することが行われている。ここでは、これを個人認証と呼ぶ。個人認証には、いわゆるキャッシュカード／クレジットカード等のICカード系サービスと生体認証がある。

[0009] ICカード系サービスでは、使用者が提示するカードの情報とパスワードを認証局に送信して照合する。一般に、パスワード入力などによる個人認証はPKI(Public Key Infrastructure)と呼ばれるので、ここでもこの語を使用する。通常、パスワードは正規のICカード所有者が容易に記憶していられるように簡単な番号の組合せになっており、ICカードが盗難または紛失して第三者の手に渡り、その第三者が何らかの方法でパスワードを知った時には、悪用されるという問題を生じる。また、ICカードには、ICカードの紛失、ICカードの不携帯時にはサービスを受けられないといった不都合もある。

[0010] 生体認証は、一般に信頼性が高く、特許文献3及び4に記載されるように正当な使用者を認証する上での基点として使用されている。

[0011] 特許文献1:特開2002－042102

特許文献2:特開2001－197055

特許文献3:特開2003－143136

特許文献4:特開2002－368737

発明の開示

発明が解決しようとする課題

[0012] 現状では、TPMと個人認証を行う装置(システム)は、別の装置であり、ICカード・リーダー・ライター(R／W)や指紋検出装置のような個人認証を行う装置とTPMを連携させたり、ネットワークを介してTPMと個人認証を行う装置とを連携させることは可能であるが、装置間やネットワークでのデータのやりとりが発生するため、データをモニタ可能であり、セキュリティ上好ましくないという問題があった。

[0013] 上記の問題に加えて、さらに以下に示すような問題があった。

[0014] (1)サービス利用者が使用する機器(PC等)内に実装されたTPMによる装置認証及び環境認証のための情報チェック等では、ネットワーク経由で認証局アクセスしてこれらの情報を送信することが必要であり、スタンドアローンの装置内で個人認証す

る場合は、TPM機能を使った環境情報等のチェックができないという問題があった。

[0015] (2)ネットワークを介してのTPM認証局、個人認証局(ICカード認証局、生体認証局)などの各認証局間の連携では、多数の連携用コマンドが発行される為、すべての処理をネットワークを介して実施したのでは、処理遅延という問題を生じる。また、ネットワークを介しての認証シーケンスの途中で失敗した場合には、確実な認証ができないという問題があった。

[0016] (3)認証情報運用管理セキュアシステムは、TPM機能単体でも動作できるアッパーコンパチであることが要求され、プログラムのローダブル機能もTPM、パスワードの入力による本人認証(PKI)、生体認証(BIO)のそれぞれのソフトウェアを単体で機器にインストールできることが要求されるが、このような要求を満たす装置が現状ではないという問題があった。

[0017] (4)従来の装置に搭載されるTPM機能は、その装置の利用者と1対1の関係にあり、複数の利用者を管理することができないという問題があった。

[0018] 本発明は、上記のような問題を解決して、耐タンパ(Tampering)・セキュリティ性を強化したセキュアシステム、セキュアシステムを搭載した装置、そのような装置が接続されるセキュアネットワークシステムの実現を目的とする。

課題を解決するための手段

[0019] 上記目的を実現するため、本発明のセキュアシステムは、TPM対応機器であるかの認証処理を行うTPMユニットと、装置の使用者の認証処理を行う使用者認証ユニットと、TPMユニット及び使用者認証ユニットを管理するセキュアマネージャと、を1チップの半導体チップに搭載して構成する。そして、このような半導体チップを搭載して装置を実現し、そのような装置をネットワークに接続することでセキュアネットワークシステムを実現する。使用者認証ユニットは、PKIやBIOである。

[0020] 本発明によれば、TPMユニットと使用者認証ユニットが1チップの半導体チップ内に設けられるので、外部からのアクセスが難しくなり、TPMユニットと使用者認証ユニット間でのデータのやりとりを外部からモニタできなくなる。

[0021] また、生体認証(BIO)及び/またはパスワード認証(PKI)による個人認証とTPM認証を連携することにより、正規の装置での正規の使用者であることを、より高い信頼

性で認証可能になる。

[0022] 例えば、ネットワークを介しての認証局への認証データの送信は暗号化して行われることが望ましい。そのため、本発明のセキュアシステムは、TPMユニットが収集したTPM認証情報及び使用者認証ユニットが収集したPKI認証情報を暗号化する暗号化ユニットを備える。暗号化する場合、個人認証とTPM認証を連携することにより、暗号の解読が難しくなる。具体的には、TPM機能にて計算したPCR値をAIK(Attestation Identity Register)(署名鍵)で署名したものと、PKI機能にて管理している個人鍵や受益者認証鍵で署名した平文を統合し、更に、認証サーバが公開している公開鍵で暗号化し、ネットワーク経由で認証サーバへ送信する。認証サーバは認証サーバで保持している秘密鍵で復号化した後、署名検証を行い、更に、認証サーバで保持しているPCR値と比較チェックを行う。これにより、正規の使用者が、プログラム等が改竄されていない正規の装置を使用していることを確実に認証できる。

[0023] また、セキュアマネージャ内でPCR値を保持すれば、ネットワークを介してTPM認証局にデータを送らなくてもTPMによる認証が可能である。そのため、セキュアマネージャは、PCRを記憶するPCR記憶ユニットを備え、装置の環境構築完了時にTPMユニットが算出したPCRを記憶し、以降の装置の起動時には、TPMユニットが算出したPCRを、記憶してあるPCRと比較して認証を行う。これにより、ネットワークを介して認証サーバにアクセスすることなく、安全なソフトウェア環境を保証することが可能になる。

[0024] TPM、PKI、BIO認証のためのソフトウェア(プログラム)は、バージョンアップされるのが一般的であり、最新のプログラムを使用することが望ましい。そこで、そのプログラムを記憶するプログラム記憶ユニットを書き換え可能とし、プログラムを各機能単体でセキュア通信にてロード可能とすることが望ましい。

[0025] 本発明によれば、TPMユニットと使用者認証ユニットが同一チップに設けられているので、アプリケーションなどからチップのセキュアマネージャに入力されるコマンドは、TPM用コマンドとTPM用以外のコマンドが混在することになる。そこで、セキュアマネージャへのコマンドは、TPMユニットで実行するプログラムのコマンドの形式に準拠し、TPMコマンドはTPMの規格にて規定されているVフラグが"0"であり、それ以

外のコマンドはVフラグが”1”であるようにし、セキュアマネージャは、Vフラグを識別するVフラグ識別回路の判定結果に応じてコマンドを分けるようにする。

[0026] さらに、使用者認証ユニットが個人認証局により与信を受けた複数の使用者についての情報を記憶可能にし、セキュアマネージャは、装置の管理者から指示された時に、装置を使用可能なユーザを追加登録可能にすることが望ましい。この際、複数の使用者の情報を、グループ化して記憶可能にすることが望ましい。

[0027] 以上説明したように、本発明は以下のような効果を奏する。

[0028] (1)TPMユニットと使用者認証ユニットが同一チップ内に収容され、相互に連携して認証が行われるので、セキュリティが向上する。また、それぞれの認証機能を連携させることも、機能ごとに単独で動作させることが可能である。

[0029] (2)PCRをセキュアシステム内に保持するので、ネットワークアクセス回数が軽減され、従来より強固なセキュリティ環境でのサービス・機能を活用することが可能になる。

[0030] (3)本発明のセキュア装置では使用環境が保証されるので、これまでR／Wなどの所定の装置でしか使用できなかったICカードを使用することも可能であり、それに応じたサービスが受けられるようになる。

[0031] (4)遠隔医療端末などの専用端末及び共通端末では、装置と使用者が1対1の関係にあり、それ以外の者は使用できなかったが、複数ユーザ(複数ICカード)が使用したい場合に対応できるようになる。

図面の簡単な説明

[0032] [図1]本発明に係るセキュアインターネットシステムの概略を示す模式図である。

[図2]本発明の実施形態の認証情報運用管理セキュアシステムのハードウェア構成図である。

[図3]実施形態のセキュアシステムのソフトウェア構成図である。

[図4]本発明の第1の実施形態における統合署名検証実施シーケンスである。

[図5]本発明の第2実施形態におけるソフトウェア環境検証実施シーケンスである。

[図6]本発明の第3実施形態のセキュアシステムにおけるコマンドの内部構成(ビット振り分け)を示す図である。

[図7]本発明の第3実施形態のセキュアシステム内でのコマンド振り分けフローである。

[図8]本発明の第4実施形態のセキュアシステムにおけるプログラムのローダブルプログラム機能の仕組みを示す図である。

[図9]本発明の第4実施形態におけるプログラムロード実施シーケンスである。

[図10]本発明の第5実施形態のセキュアログインシステムにおける初期利用者登録シーケンスである。

[図11]本発明の第5実施形態のセキュアログインシステムにおける利用者登録シーケンスである。

[図12]本発明の第5実施形態のセキュアログインシステムにおけるグループ登録シーケンスである。

[図13]本発明の第5実施形態においてPKIで管理する個人鍵及び受益者認証鍵の状態変化の例を示す。

符号の説明

[0033] 1 ネットワーク
2 機器(装置)認証局
3 環境認証局
4 個人認証局
10 (端末)装置
11 セキュアシステム
12 セキュアマネージャ
13 TPMユニット
14 使用者認証ユニット

発明を実施するための最良の形態

[0034] 以下、本発明の実施形態を添付の図面を参照して説明する。

[0035] 図1は、本発明の実施例のセキュアシステムを搭載した装置と、この装置が接続されるセキュアネットワークシステムの全体構成を説明する図である。図1に示すように、機器(装置)認証局2、環境認証局3、個人認証局4、コンテンツ／ポリシーSV5、タ

イムスタンプ6、サービス提供者7などが、ネットワーク1に接続され、ネットワーク1を介して相互にアクセスできるように構成されている。本発明の認証情報運用管理セキュアシステム11を搭載した装置10は、ネットワーク1に接続され、ネットワーク1に接続された図示の認証局などを含む他の装置との間で相互にアクセス可能である。

[0036] 本発明のセキュアシステム11は、1チップの半導体チップで構成され、TPM対応機器であるかの認証処理を行うTPMユニット12と、装置10の使用者の認証処理を行う使用者認証ユニット14と、TPMユニット13及び使用者認証ユニット14を管理するセキュアマネージャ12と、を有する。

[0037] 図2は、実施例のセキュアシステム11のハードウェア構成図である。図示のように、セキュアシステム11を構成するハードウェアは、内部バス20と、コマンド(命令)を実行するマイクロコントロールユニット(MCU)21と、実行プログラムを記憶する不揮発性のROM22と、ワークエリアとして機能する揮発性のRAM23と、暗号制御モジュール24と、タイマ制御25と、ハッシュ生成器26と、2048ビットのべき乗剰余演算器27と、乱数生成器28と、外部インターフェース29と、メモリコントローラ30と、メモリ専用バス31と、フラッシュメモリ32と、SRAM33と、を有する。暗号制御モジュール24は、例えばDES、3DES、AESなどの暗号方式処理を行う。ハッシュ生成器26は、例えばMD5、SHA1などのハッシュ処理を行う。外部インターフェース29は、例えばLPC、USB、UART、I2Cなどに準拠したインターフェースである。これらのハードウェア構成については広く知られているので詳しい説明は省略する。

[0038] 図2に示したハードウェアは、すべて1チップの半導体チップ内に設けられる。図2に示したハードウェアは、セキュアシステム11の機能を実現するだけでなく、装置10の機能を実現するのにも利用される。

[0039] 図3は、図2のハードウェアにロードされるプログラムにより実現される実施例のセキュアシステム11のソフトウェア構成図である。図示のように、ソフトウェアは、ハードウェア層34と、ソフトウェアインフラストルクチャ層41と、ソフトウェアアプリケーション層51と、で構成される。ハードウェア層34は、図2に示した各種ハードウェアと、各ハードウェアを駆動するためのハードウェアドライバ36と、TPM(Trusted Platform Module)37と、PKI(Public Key Infrastructure)38と、生体認証ハードウェアのBIO(Biometrics)3

9と、セキュアマネージャ40と、を有する。TPM37、PKI38及びBIO39は、機能的に独立した動作が可能である。TPM37、PKI38及びBIO39は、機能的には既存のものを使用し、それらについては広く知られているので説明は省略する。セキュアマネージャ40の動作については後述する。

[0040] ソフトウェアインフラストラクチャ層41は、ブートBIOS(Boot BIOS)42と、PC BIOS TPM／TSS(TCS Software Stack) BIOS－API43と、セキュアマネージャ・ドライバ44と、セキュアマネージャ・ドライバライブラリ(Lib)45と、TSS46と、管理ツール47と、Crypto API48と、TSS対応のCSP49と、TSS対応のPKCS＃11（TSS）50と、を有する。さらに、ソフトウェアアプリケーション層51は、アプリケーション群52を有する。ソフトウェアインフラストラクチャ層41及びソフトウェアアプリケーション層51のソフトウェア構成は、TPMデバイスドライバ及びライブラリの替わりに、セキュアマネージャ・ドライバ44と、セキュアマネージャ・ドライバライブラリ45が設けられている点を除けば、TPMデバイスドライバTCGにより規格化されているソフトウェアスタックと同じであり、説明は省略する。言い換えれば、本実施例では、TCGにより規格化されている構成において、PKI38及びBIO39を設け、セキュアマネージャによりそれらとTPM37を連携して管理する点が異なる。

[0041] 以上のような構成のセキュアシステム11を搭載した装置10をネットワークに接続した場合の実施形態を、以下に説明する。

[0042] 第1の実施形態は、ユーザが装置10を使用してサービスを受けるための認証処理に関係する。第1の実施形態では、図1のネットワーク構成で、個人認証局4はPKI認証を行い、機器（装置）認証局2、環境認証局3、個人認証局4及びタイムスタンプ6は、1つの認証サーバ55に統合されているものとする。

[0043] 図4は、第1の実施形態における署名検証実施シーケンスを示す。第1の実施形態では、TPM、PKIで作成したデータを統合した統合署名が、認証サーバ55で認証され、この統合署名検証により、使用者本人の特定、使用機器の特定、その機器が正しい構成であることの特定がなされたことが保証される。

[0044] 第1の実施形態で使用される鍵は以下の通りであり、事前に生成されているものとする。鍵の生成及び証明書の取得方法は既存の公知の手順に従う。

[0045] AIK(Attestation Identity Key)(署名鍵):プラットフォーム(装置、セキュアシステム)認証に利用され、TPM内部にデジタル署名を施すために利用される。TPM機能のオーナ(所有者)により生成される。

[0046] 機器(装置)認証鍵:サービス側の要求に従い、TPM機能で生成する。

[0047] 個人鍵:セキュアシステム11に登録された利用者ごとに、PKI機能で生成する。

[0048] 受益者認証鍵:セキュアシステム11に登録された利用者ごとに生成可能(複数の利用者での共有も可)で、PKI機能で生成する。

[0049] 図4を参照して、第1の実施形態において、統合署名を生成して認証サーバ55に送信する手順を説明する。

[0050] 装置10は、事前に認証サーバ55よりサーバ側公開鍵及びノンス(乱数によるバイト列の配列)を取得し、認証サーバ55は装置10から機器認証鍵、AIK、個人鍵、受益者認証鍵の公開鍵を取得しているものとする。

[0051] (1)アプリケーションからセキュアシステム(チップ)11のセキュアマネージャ40に対して署名作成要求が出される。

[0052] (2)セキュアマネージャ40は、TPM37から機器認証鍵を取得する。

[0053] (3)セキュアマネージャ40は、TPM37からAIKを取得する。

[0054] (4)セキュアマネージャ40は、PKI38から個人鍵を取得する。

[0055] (5)セキュアマネージャ40は、PKI38から受益者認証鍵を取得する。この場合、複数の受益者認証鍵を取得することも可能である。

[0056] (6)セキュアマネージャ40は、TPM37において、ソフトウェアの測定結果の値であるPCR(Platform Configuration Register)に対してAIKによる署名を作成するように要求して、作成した署名を取得する。PCRはTPM37において随時更新されているものとするが、要求のあった時に測定して算出してもよい。

[0057] (7)セキュアマネージャ40は、PKI38において、任意の平文に対して個人鍵による署名を作成するように要求して、作成した署名を取得する。

[0058] (8)セキュアマネージャ40は、PKI38において、任意の平文に対して受益者認証鍵による署名を作成するように要求して、作成した署名を取得する。

[0059] (9)セキュアマネージャ40は、TPM37において、任意の平文に対して機器認証鍵

による署名を作成するように要求して、作成した署名を取得する。

[0060] (10)セキュアマネージャ40は、セキュアマネージャ40内に保持されているPIR(Physical Information Register)を取り出す。PIRは、物理認証情報レジスタの値であり、本人の生体認証方法の設定またはその変更時の正確なタイムスタンプもしくはその時に生成した乱数を暗号化して保存したものである。

[0061] (11)セキュアマネージャ40は、PKI38において、対象データ、以上のようにして作成したAIK署名データ、個人鍵署名データ、受益者認証鍵署名データ、機器認証鍵署名データ及びノンスを統合した統合署名用平文に対して、個人鍵による署名作成を要求して、作成した署名を取得する。

[0062] 以上の(2)から(11)までの処理はセキュアシステム11のチップ内で行われる。

[0063] (12)上記の(11)で作成した署名データ及び統合署名用平文を含む統合署名をアプリケーションに送る。

[0064] (13)アプリケーションは、取得した署名データをサーバ側公開鍵で暗号化する。

[0065] (14)アプリケーションは、暗号化した署名データ及び統合署名用平文を含む統合署名を認証サーバ55に送信する。

[0066] (15)認証サーバ55は、受信した統合署名をサーバ側秘密鍵で復号し、署名の検証を行い、検証結果をアプリケーションに返信する。検証は、機器(装置)、ソフトウェア、ユーザが正当性について行われ、ソフトウェアの正当性はPCRの値により判定される。

[0067] アプリケーションは、認証に成功したとの返信を受けた場合には、正常のサービスを開始し、認証が不成功の場合にはその旨及びサービスが受けられないなどの表示を行う。

[0068] 図5は、本発明の第2の実施形態におけるソフトウェア環境検証実施シーケンスを示す。第2の実施形態では、AIKで署名したPCRを認証サーバに送信せずに装置(セキュアマネージャ)で検証可能にする。ハードウェア構成及びソフトウェア構成は第1実施例と同じであるが、環境認証局3が認証サーバに含まれる必要がない。

[0069] 装置10の環境構築完了時(ソフトウェアインストール時)、アプリケーション51は、セキュアマネージャ40にPCRの保存を要求する。

[0070] セキュアマネージャ40は、TPM37に対してPCRを生成するように要求し、生成したPCRを取得する。

[0071] セキュアマネージャ40は、取得したPCRをPCR記憶メモリに基準PCRとして記憶する。PCR記憶メモリは、書込み可能な不揮発性ROMであるフラッシュ(Flash)メモリ32などで構成される。

[0072] セキュアマネージャ40は、基準PCRの保存が完了したことをアプリケーションに通知する。

[0073] 環境構築完了後は、装置10が起動されると、アプリケーション51は、セキュアマネージャ40にPCRの比較を要求する。

[0074] セキュアマネージャ40は、TPM37に対してPCRを生成するように要求し、生成したPCRを取得する。

[0075] セキュアマネージャ40は、取得したPCRをPCR記憶メモリに記憶してある基準PCRと比較する。

[0076] セキュアマネージャ40は、PCRの比較結果をアプリケーションに通知する。生成したPCRが記憶してある環境構築完了時の基準PCRと一致すればソフトウェアが改竄されていないことが認証される。一致しない時には、ソフトウェアに対して、何らかの変更が行われたこと、すなわち改竄が行われたことが分かるので、それに応じた動作を起動する。

[0077] 第2の実施形態では、ネットワークを介してPCRの検証を行う必要がないので、使用者の個人認証を装置内で行うスタンドアローン形の装置に適用すれば、ソフトウェア環境を認証することができる。もちろん、機器(装置)の認証は行えないが、機器はネットワークに接続されないので、特に問題は生じない。

[0078] 遠隔医療端末等の専用・共通端末装置においては端末装置の設定を変える(関係のないソフトウェアをインストールする等)ことが許容されない場合があるが、第2の実施形態の機器を使用すれば、TPMで生成されるPCR値を使用しPCの環境が変更されていないか検査することができるので、不適切なソフトウェアを使用することがなくなる。

[0079] 次に、本発明の第3の実施形態を説明する。第3の実施形態は、セキュアマネージ

ャにおいて、コマンドをPKI、BIO、TPMの各機能へ振り分けるためのデータ設定処理に関係する。

[0080] アプリケーションとセキュアシステム11のセキュアマネージャ40間のインターフェースにはコマンドを使用する。コマンドのPKI、BIO、TPMの各機能への振り分けはセキュアマネージャで行う。コマンドは機器内の環境認証を行う際に使用するTPMのコマンド形式に準拠する。

[0081] TPMの規格(TCPA Main Specification)により、TPMコマンドの形式は表1の通り規定されている。

[0082] [表1]

表1．TPMのコマンド形式

Type	Name	Description	Length
TPM_TAG	Tag	識別子	2
UINT32	paramSize	コマンドサイズ	4
TPM_COMMAND_CODE	Ordinal	コマンド種別	4
以下各コマンドのデータ	—	—	X

[0083] また、TPMコマンド内のOrdinalの構成は、図6のように定義されている。ここで、PはProtectedコマンドかどうかを示すビットである。CはTSSとTPMの間を通信するかを示すビットである。Vはベンダ独自拡張コマンドか示すビットである。Reservedはすべて0のビットがたっている。Purviewは機種指定のコマンドであり、TPMメイン仕様、PC、PDA、携帯電話、サーバなどを指定する。Command Ordinal Indexは、コマンドの識別子に相当する。従来、Vフラグは規格に規定されていないTPMの機能を実装するため、ベンダが独自に実装したコマンドを識別するために使用されている。

[0084] 第3の実施形態では、セキュアシステム11がこのVフラグをTPM機能のコマンドとTPM以外の機能のコマンドを識別するためのフラグとして使用する。Vフラグが"0"の場合はTPM機能を実行するコマンド、Vフラグが"1"の場合はTPM以外の機能を実行するコマンドと識別する。第1の実施形態で実施しているPKIとTPMの連携において、前述のVフラグを判定し実現することが可能となる。

[0085] TPMコマンドの定義は規格に従う。その他の機能(セキュアマネージャ・PKI・BIO)

におけるコマンドのヘッダ値は表2のように設定する。

[0086] [表2]

表２．認証情報運用管理セキュアシステム内コマンド振り分け定義

Name		セキュアマネージャ	PKI	BIO	TPM
Tag		0x00C1	0x00C1	0x00C1	規格に従う
Ordinal					
	P	0	0	0	0
	C	0	0	0	0
	V	1	1	1	0
	Purview	0x01	0x01	0x01	0x00
	Command Ordinal Index	0x0001	0x0002	0x0003	規格に従う

[0087] 図7は、第3の実施形態のおけるコマンド振り分け処理フローを示すフローチャートである。振り分けるコマンドは、TPMヘッダとデータで構成される。

[0088] ステップ101では、表2のOrdinal部のVフラグを判定し、Vが"0"であればTPM標準コマンドであるので、ステップ102に進む。このコマンドには、TPMヘッダが付加されたままである。ステップ102では、TPM37でTPMコマンドが処理される。

[0089] Vフラグが"1"であれば、ベンダ独自コマンドであるので、ステップ103に進む。

[0090] ステップ103では、2バイトのCommand Ordinal Index値を判定し、"0x0001"であればマネージャコマンドであるのでステップ104に進み、セキュアマネージャ40のコマンド処理部にて要求内容を解析し処理を実施する。"0x0002"であればPKIコマンドであるのでステップ105に進み、コマンドの先頭からOrdinal部までを削除したコマンドデータをPKI38に渡し、PKI38がそのコマンドを処理する。"0x0003"であればBIOコマンドであるのでステップ106に進み、PKI38にコマンドデータを渡し、PKI38がそのコマンドを処理する。"0x0004"以上であれば、ベンダ独自のTPMコマンドであるので、TPM37にコマンドデータを渡し、TPM37がそのコマンドを処理する。

[0091] 第3の実施形態では、セキュアマネージャ40へのコマンドはTPM規格に準拠しており、TPMコマンドとそれ以外のコマンドの振り分けが容易に行える。

[0092] 次に説明する本発明の第4の実施形態は、TPM、PKI、BIOの各機能を実現する

プログラムを交換可能にするためのローダブルプログラム機能に関係する。第4の実施形態では、各機能は個別に交換することが可能である。

[0093] 図8は、第4の実施形態におけるローダブルプログラム機能の仕組みを示している。

[0094] セキュアマネージャ40は、内部に各機能のプログラムを展開する先頭のアドレスを定義したエントリポイントベクタテーブルを保持する。エントリポイントベクタテーブルに設定される値はプログラム固定で持つか、プログラムがロードされる際に設定される。

[0095] アプリケーション51から、TPM用、PKI用またはBIO用のインストールするプログラム61を受信し、受信したプログラムは一旦保持メモリ62に格納後、ローダブルメモリ領域63にロードされ、更にRAM23へ展開される。保持メモリ62及びローダブルメモリ領域63はRAM23の一部が使用される。プログラムを展開する際はベクタテーブルから対応する機能のエントリポイント値を取得する。図8では、TPM用プログラムは先頭アドレス"0xAAAA"の領域に、PKI用プログラムは先頭アドレス"0xBBBB"の領域に、BIO用プログラムは先頭アドレス"0xCCCC"の領域に格納される。

[0096] 図9は、ローダブルプログラムによるプログラムのロード処理シーケンスを示す。

[0097] アプリケーション51は、セキュア(暗号化された)通信を使用してインストールプログラム受信し、セキュアマネージャ40に保持を要求する。これに応じて、セキュアマネージャ40は、受信したプログラムを保持メモリ62に格納し、格納の可否についてアプリケーション51に知らせる。

[0098] プログラムが保持メモリ62に格納された後に、アプリケーション51は、セキュアマネージャ40に対してプログラムのロード要求を行う。これを受信したセキュアマネージャ40は、保持メモリ62に格納されたデータをローダブルメモリ領域63にロードし、その可否をアプリケーション51に知らせる。

[0099] アプリケーション51は、セキュアマネージャ40に対してプログラムのインストールを実行する要求を行う。これを受信したセキュアマネージャ40は、エントリポイントベクタテーブルより展開を開始するメモリの先頭アドレスを取得し、RAM23への展開を行う。そして、メモリ展開の可否をアプリケーション51に知らせる。

[0100] 次に、アプリケーション51は、セキュアマネージャ40にローダブル機能実行終了要

求を行い、セキュアマネージャ40はこれに応答する。

[0101] 次に、アプリケーション51からセキュアマネージャ40にプログラムのクリア要求が行われ、これを受信したセキュアマネージャ40は、保持メモリ62に保存されているプログラム削除し、その可否をアプリケーション51に知らせる。

[0102] 次に説明する本発明の第5の実施形態は、セキュアシステムに複数の利用者をグループ化して登録する機能に関係する。

[0103] セキュアシステム11に登録された利用者の権限は、表3の3種類である。

[0104] [表3]

表３．利用者種別

種別	定義
スーパーバイザ	機器の初期状態に対して最初に登録された利用者（初期利用者）が獲得できる権限。 １台の機器に対して一名のみ登録可能。 権限取得時は同時に管理者権限も得る。 他の利用者に対して、管理者権限を持つ権利を与えることができる。 他の利用者へスーパーバイザ権を委譲することは不可。
管理者権限保持者	スーパーバイザより管理者権限を委譲された利用者。
ビジタ	スーパーバイザ権及び管理者権限を持たない利用者のこと。

[0105] 表3に示すように、利用者の権限は、スーパーバイザ、管理権限保持者及びビジタの3種類である。スーパーバイザは、機器の初期状態に対して最初に登録された利用者（初期利用者）が獲得できる権限であり、1台の機器に対して1名のみ登録可能である。スーパーバイザの権限を取得すると、同時に管理者権限も得る。スーパーバイザは、他の利用者に対して、管理者権限を持つ権利を与えることができる。他の利用者へスーパーバイザ権限を委譲することはできない。管理者権限保持者は、スーパーバイザから管理者権限を委譲された利用者である。ビジタはスーパーバイザ権限及び管理者権限を持たない利用者のことである。従って、ビジタは、スーパーバイザから管理者権限を与えられると管理者権限保持者になり、管理者権限保持者はスーパーバイザから管理者権限を取り消されるとビジタになる。

[0106] 次に、セキュアマネージャ40で管理する各種データとデータを保持するテーブル構成について説明する。

[0107] システムに登録された利用者の管理は利用者管理テーブルを使用して行う。1利用者ごとに表4に示す利用者管理テーブルの内容を登録する。

[0108] [表4]

表４．利用者管理テーブル

項目	内容
利用者識別子	利用者登録時に一意に割り当てられる識別子 （生体認証情報に割り当てられる識別子も兼ねる）
利用者名	登録時に設定された利用者名
パスワード	登録時に設定されたログインパスワード
Piproof	認証方法が切り替えられるたびに更新される値
Plid	初期登録時に決定される値
認証種別	BIO／パスワードのどちらを使用して認証を行っているかを示す。 認証種別変更要求コマンド実行時にデータが変更される。
認証方法有効種別	ログインするときの認証方法の有効・無効を設定する。
認証状態	認証完了か否かを示す
認証情報登録完了種別	認証情報登録が完了している種別を示す（BIO／パスワード）
グループ識別子	利用者が所属しているグループ識別子。（複数登録可能） 尚、初期登録時及び所属しているグループが削除された場合は「所属グループ無し」となる
スーパーバイザ権限	スーパーバイザ権限情報（昇格状態、権限保持状態、権限無し）
管理者権限	管理者権限情報（委譲状態、取得状態、管理者権限無し）

[0109] 利用者管理テーブルの項目と内容は、表4に示す通りであるので説明は省略する。PI値は本人のBIO情報の設定時、変更のタイムスタンプ(もしくはそのときに生成した乱数)を暗号化し保存したものであり、PlidとPiproofの2種類がある。

[0110] PI値の更新の規則は、表5のPI値の設定に従って行われる。

[0111] [表5]

表５．PI値の設定について

機能	Piproof		Plid	
	BIO	パスワード	BIO	パスワード
利用者生成	０に設定される	設定されない	新UUIDが生成される	新UUIDが生成される
初期利用者生成	新UUIDが設定される	設定されない	新UUIDが生成される	新UUIDが生成される
認証情報の設定	新UUIDが生成される。	設定されない	旧情報が０の以外のとき、保持される。０のとき、新UUIDが生成される	旧情報が０の以外のとき、保持される。０のとき、新UUIDが生成される
認証情報のリセット	０が設定される	設定されない	０が設定される	０が設定される
認証情報の変更	新UUIDが生成される	設定されない	旧情報が保持される	旧情報が保持される
認証方法の設定	新UUIDが生成される	設定されない	旧情報が保持される	旧情報が保持される
認証方法の変更	新UUIDが生成される。 ※BIO＋パスワードへの変更も同じ	設定されない	旧情報が保持される。	旧情報が保持される。

[0112] Piproofは、利用者生成及び認証情報のリセットの時に”0”に設定され、それ以外の初期利用者生成、認証情報の設定、認証情報の変更、認証方法の設定及び認証方法の変更の時に新UUID（十分な長さを持ったユニークな識別情報を表現する値）に設定される。Piproofのパスワードは、いずれの場合も設定されない。

[0113] Plidは、利用者生成の時にユニークなIDが設定され、初期利用者生成の時に新UUIDが生成され、認証情報の設定の時には、旧情報が”0”以外の時には旧情報が保持され、”0”の時には新UUIDが設定され、認証情報のリセットの時に”0”に設定され、認証情報の変更、認証方法の設定及び認証方法の変更の時には旧情報が保持される。

[0114] Plidのパスワードは、利用者生成及び初期利用者生成の時に新UUIDが生成され、それ以外の時には旧情報が保持される。

[0115] システムに登録されたグループの管理はグループ管理テーブルを使用して行う。1グループごとに、表6のグループ管理テーブルの内容を登録する。

[0116] [表6]

表６．グループ管理テーブル

項目	内容
グループ識別子	グループ登録時に一意に割り当てられる識別子
グループ名	登録時に設定されたグループ名
最大登録可能者数	グループに登録することができる最大の利用者数
登録者数	グループに登録されている利用者数

[0117] グループ管理テーブルは、表6に示すように、グループ識別子、グループ名、最大登録可能者数、登録者数の項を有する。以下各データの登録手順を説明する。

[0118] 図10は、初期利用者（スーパーバイザ）登録シーケンスを示す。ここでは、認証方法としてBIO機能を使用するものとする。

[0119] 初期利用者（スーパーバイザ）である機器利用者が、アプリケーションに初期利用者登録を要求すると、アプリケーションは初期利用者登録画面を表示する。

[0120] 機器利用者が画面に従って認証方法を選択すると、アプリケーションは指示された認証方法を選択し、セキュアマネージャに初期利用者登録を行うように要求する。

[0121] セキュアマネージャは、アプリケーションから初期利用者登録要求を受信すると、利用者管理テーブルに情報を登録する。すなわち、利用者管理テーブル更新(新規利用者データ登録)を行う。そして、セキュアマネージャは、Plidを生成し、BIOにバイオ情報登録開始を指示する。

[0122] この間に、アプリケーションは認証情報入力プロンプトを表示し、これに応じて機器利用者は自身のバイオ情報をバイオセンサで入力する。バイオセンサは登録結果をBIOに通知し、BIOは登録結果をセキュアマネージャに通知し、セキュアマネージャはPiproofを生成すると共にアプリケーションに結果を通知する。このようにして、BIO情報の登録が実施される。

[0123] 登録した機器利用者（スーパーバイザ）がアプリケーションにログインを要求すると、アプリケーションがセキュアマネージャにログインを要求し、BIOにバイオ認証の準備を開始するように指示し、認証情報入力プロンプトを表示する。機器利用者がこの表示に応じてバイオセンサに自身のバイオ情報を入力すると、バイオセンサは入力されたバイオ情報を認証して、その認証結果をBIOに通知し、BIOは認証結果をセキュ

アマネージャに通知する。セキュアマネージャは、更にアプリケーションに結果を通知する。これにより、機器利用者が登録された初期利用者(スーパーバイザ)であることが認証される。

[0124] 認証された機器利用者が運用開始をアプリケーションに要求すると、アプリケーションはそれをセキュアマネージャに通知し、セキュアマネージャは機器利用者にスーパーバイザ権限を付与し、スーパーバイザ権限の下での運用を開始し、そのことをアプリケーションに通知する。以下、通常のサービスが開始される。

[0125] 認証された機器利用者が運用開始を要求するまでは、何回でも初期利用者の登録を変更することができる。しかし、運用開始後はスーパーバイザの変更や削除は不可となる。

[0126] 図11は、利用者登録シーケンスを示す。この利用者登録手順は、認証方法としてBIO機能を使用した場合を示す。

[0127] まず、アプリケーションから管理権限を委譲された利用者がログインして管理者権限保持者として登録される処理から説明する。

[0128] そのような機器利用者が、アプリケーションにログインを要求すると、アプリケーションがセキュアマネージャにログインを要求し、BIOにバイオ認証の準備を開始するように指示し、認証情報入力プロンプトを表示する。機器利用者がこの表示に応じてバイオセンサに自身のバイオ情報を入力すると、バイオセンサは入力されたバイオ情報を認証して、その認証結果をBIOに通知し、BIOは認証結果をセキュアマネージャに通知する。セキュアマネージャは、更にアプリケーションに結果を通知する。これにより、機器利用者が登録されたビジタであることが認証される。

[0129] 認証された機器利用者が管理者権限の取得をアプリケーションに要求すると、アプリケーションはそれをセキュアマネージャに通知し、セキュアマネージャは管理テーブルを変更し、結果をアプリケーションに通知する。これにより、ログインした機器利用者が管理者権限保持者として登録される。

[0130] このような管理者権限保持者が、新規の利用者(ビジタ)を登録するようにアプリケーションに要求すると、アプリケーションはそれをセキュアマネージャに通知し、セキュアマネージャは管理テーブルに新規利用者を登録し、Plidを生成し、利用者識別子

をアプリケーションに通知する。

[0131] 新規利用者は選択した認証方法をアプリケーションに通知し、アプリケーションは認証方法を選択した後、セキュアマネージャに認証情報の登録を要求する。セキュアマネージャは利用者管理テーブルに情報を登録し、BIOにバイオ情報の登録開始を準備するように指示する。この間に、アプリケーションは認証情報入力プロンプトを表示し、新規の機器利用者は表示に応じてバイオセンサでバイオ情報を入力する。バイオセンサは入力されたバイオ情報を登録し、登録結果をBIOに通知し、BIOはセキュアマネージャに登録結果を通知する。セキュアマネージャはPiproofを生成して、結果をアプリケーションに通知する。このようにして新規の利用者が登録される。

[0132] 登録された複数の利用者が1台の機器を利用可能な場合、複数の利用者をグループ化すると管理が容易である。次に、グループ登録及び登録されたグループへの利用者の登録手順を説明する。

[0133] 図12はグループ登録シーケンスを示す。ここでの機器利用者は管理者権限を取得している利用者とする。

[0134] 管理者権限を有する機器利用者がアプリケーションにグループ登録を要求すると、アプリケーションはセキュアマネージャにグループ登録を要求する。グループ登録を受信すると、セキュアマネージャは、新規グループデータを登録する。言い換えれば、グループ管理テーブルが更新される。セキュアマネージャは、グループ登録がなされたことをアプリケーションに通知する。

[0135] 機器利用者がアプリケーションに利用者一覧の取得を要求すると、アプリケーションはセキュアマネージャに利用者一覧の取得を要求する。これを受信すると、セキュアマネージャは、利用者管理テーブルから利用者一覧を取得して、それをアプリケーションに通知する。

[0136] 機器利用者がアプリケーションにグループ一覧の取得を要求すると、アプリケーションはセキュアマネージャにグループ一覧の取得を要求する。これを受信すると、セキュアマネージャは、グループ管理テーブルから利用者一覧を取得して、それをアプリケーションに通知する。

[0137] 機器利用者がアプリケーションにグループへの登録を要求すると、アプリケーション

はセキュアマネージャにグループ登録を要求する。これを受信すると、セキュアマネージャは、利用者管理テーブルを変更し(グループ識別子の追加)、グループ管理テーブルを変更し(登録者数カウントアップ)、その結果をアプリケーションに通知する。

[0138] 機器利用者がグループ化されている場合、ログイン認証の実施によりPKIの鍵の状態が変更される。図13は、これを説明する図であり、例として太郎(Aグループに属する)のログイン認証実施による鍵の状態変更を示す。

[0139] 太郎のログイン完了後、太郎が所有している個人鍵と受益者認証鍵、及び所属しているAグループの受益者認証鍵がPIN(鍵へアクセスするためのパスワード)入力待ち状態になる。図では、Aグループに属する"一郎"、"通子"及び"次郎"の受益者認証鍵がPIN入力待ち状態になる。しかし、Aグループに属する"通子"の個人鍵はPIN入力待ち状態にならない。

[0140] 以上説明したように、本発明のセキュアシステム及びそれを搭載した装置によれば、本人認証機能とTPM機能の連携を可能とし、利用者が使用するシステム内のソフトウェア環境を保証することができる。また、従来のTPM実装機器において、PKI機能、TPM機能それぞれでネットワーク認証を行っていたところを、システム内で連携することでネットワークを経由する手順を省き、認証にかかる処理時間の短縮、ネットワーク障害による影響を軽減させることが期待できる。

請求の範囲

[1] ネットワークと、

前記ネットワークに接続され、TPM認証を行うTPM認証局と、

前記ネットワークに接続され、個人認証を行う個人認証局と、

前記ネットワークに接続される装置と、を備えるセキュアネットワークシステムであって、

前記装置は、

TPM対応機器であるかの認証処理を行うTPMユニットと、

前記装置の使用者の認証処理を行う使用者認証ユニットと、

前記TPMユニット及び前記使用者認証ユニットを管理するセキュアマネージャと、を1チップ内に搭載した半導体チップを、備えることを特徴とするセキュアネットワークシステム。

[2] 前記装置は、前記TPMユニットが収集したTPM認証情報及び前記使用者認証ユニットが収集したPKI認証情報を暗号化する暗号化ユニットを備え、

前記装置は、暗号化した前記TPM認証情報及び前記PKI認証情報を、前記ネットワークを介して前記TPM認証局及び前記個人認証局に送り、

前記TPM認証局及び前記個人認証局は、送られてきた暗号化した前記TPM認証情報及び前記PKI認証情報を復号した後認証し、認証結果を前記装置に送信することを特徴とする請求項1に記載のセキュアネットワークシステム。

[3] ネットワークを介してTPM認証を行うTPM認証局と、個人認証を行う個人認証局と、に接続されるセキュア装置であって、

TPM対応機器であるかの認証処理を行うTPMユニットと、

前記装置の使用者の認証処理を行う使用者認証ユニットと、

前記TPMユニット及び前記使用者認証ユニットを管理するセキュアマネージャと、を1チップ内に搭載した半導体チップを、備えることを特徴とするセキュア装置。

[4] 前記TPMユニットが収集したTPM認証情報及び前記使用者認証ユニットが収集したPKI認証情報を暗号化する暗号化ユニットを備え、

暗号化した前記TPM認証情報及び前記PKI認証情報を、前記ネットワークを介し

て前記TPM認証局及び前記個人認証局に送り、

前記TPM認証局及び前記個人認証局から送り返された前記TPM認証情報及び前記PKI認証情報の認証結果を受信することを特徴とする請求項3に記載のセキュア装置。

[5] 前記セキュアマネージャは、当該装置の環境構築完了時に前記TPMユニットが算出したPCRを記憶するPCR記憶ユニットを備え、

当該装置の起動時には、前記TPMユニットが算出したPCRを、前記PCR記憶ユニットに記憶された前記PCRと比較し、比較結果に応じて前記装置のセキュリティ状態レベルを設定することを特徴とする請求項3に記載のセキュア装置。

[6] アプリケーションから前記セキュアマネージャへのコマンドは、前記TPMユニットで実行するプログラムのコマンドの形式に準拠しており、TPMコマンドはVフラグが"0"であり、それ以外のコマンドはVフラグが"1"であり、

前記セキュアマネージャは、Vフラグを識別し、その判定結果に応じてコマンドを前記TPMユニット用コマンドと、前記使用者認証ユニット用コマンドを含むそれ以外のコマンドに分けることを特徴とする請求項3に記載のセキュア装置。

[7] 前記使用者認証ユニットは、前記個人認証局により与信を受けた使用者に関する個人認証情報を、複数の使用者について記憶し、

前記セキュアマネージャは、当該装置の管理者から指示された時に、当該装置を使用可能なユーザを追加登録することを特徴とする請求項3に記載のセキュア装置。

[8] 前記セキュアマネージャは、記憶する複数の使用者の情報を、グループ化して記憶することを特徴とする請求項7に記載のセキュア装置。

[9] 前記使用者認証ユニットは、生体認証を行う請求項3から8のいずれか1項に記載のセキュア装置。

[10] 前記使用者認証ユニットは、カード認証を含むパスワード認証を行う請求項3から9のいずれか1項に記載のセキュア装置。

[11] ネットワークを介してTPM認証を行うTPM認証局と、個人認証を行う個人認証局と、に接続される装置に搭載されるセキュアシステムであって、

TPM対応機器であるかの認証処理を行うTPMユニットと、

前記装置の使用者の認証処理を行う使用者認証ユニットと、

前記TPMユニット及び前記使用者認証ユニットを管理するセキュアマネージャと、を備え、

前記TPMユニット、前記使用者認証ユニット及び前記セキュアマネージャが1チップの半導体チップに搭載されていることを特徴とするセキュアシステム。

[12] 前記TPMユニットが収集したTPM認証情報及び前記使用者認証ユニットが収集したPKI認証情報を暗号化する暗号化ユニットを備えることを特徴とする請求項11に記載のセキュアシステム。

[13] 前記セキュアマネージャは、前記装置の環境構築完了時に前記TPMユニットが算出したPCRを記憶するPCR記憶ユニットを備え、

起動時には、前記TPMユニットが算出したPCRを、前記PCR記憶ユニットに記憶された前記PCRと比較し、比較結果を出力することを特徴とする請求項11に記載のセキュアシステム。

[14] 前記TPMユニット及び前記使用者認証ユニットを動作させるプログラムを記憶するプログラム記憶ユニットを備え、前記プログラム記憶ユニットは書き換え可能であることを特徴とする請求項11に記載のセキュアシステム。

[15] アプリケーションから前記セキュアマネージャへのコマンドは、前記TPMユニットで実行するプログラムのコマンドの形式に準拠しており、TPMコマンドはVフラグが”0”であり、それ以外のコマンドはVフラグが”1”であり、

前記セキュアマネージャは、Vフラグを識別し、その判定結果に応じてコマンドを前記TPMユニット用コマンドと、前記使用者認証ユニット用コマンドを含むそれ以外のコマンドに分けることを特徴とする請求項14に記載のセキュアシステム。

[16] 前記使用者認証ユニットは、前記個人認証局により与信を受けた使用者に関する個人認証情報を、複数の使用者について記憶し、

前記セキュアマネージャは、前記装置の管理者から指示された時に、前記装置を使用可能なユーザを追加登録することを特徴とする請求項11に記載のセキュアシステム。

[17] 前記セキュアマネージャは、記憶する複数の使用者の情報を、グループ化して記

憶することを特徴とする請求項16に記載のセキュアシステム。

[18] 前記使用者認証ユニットは、生体認証を行う請求項11から17のいずれか1項に記載のセキュアシステム。

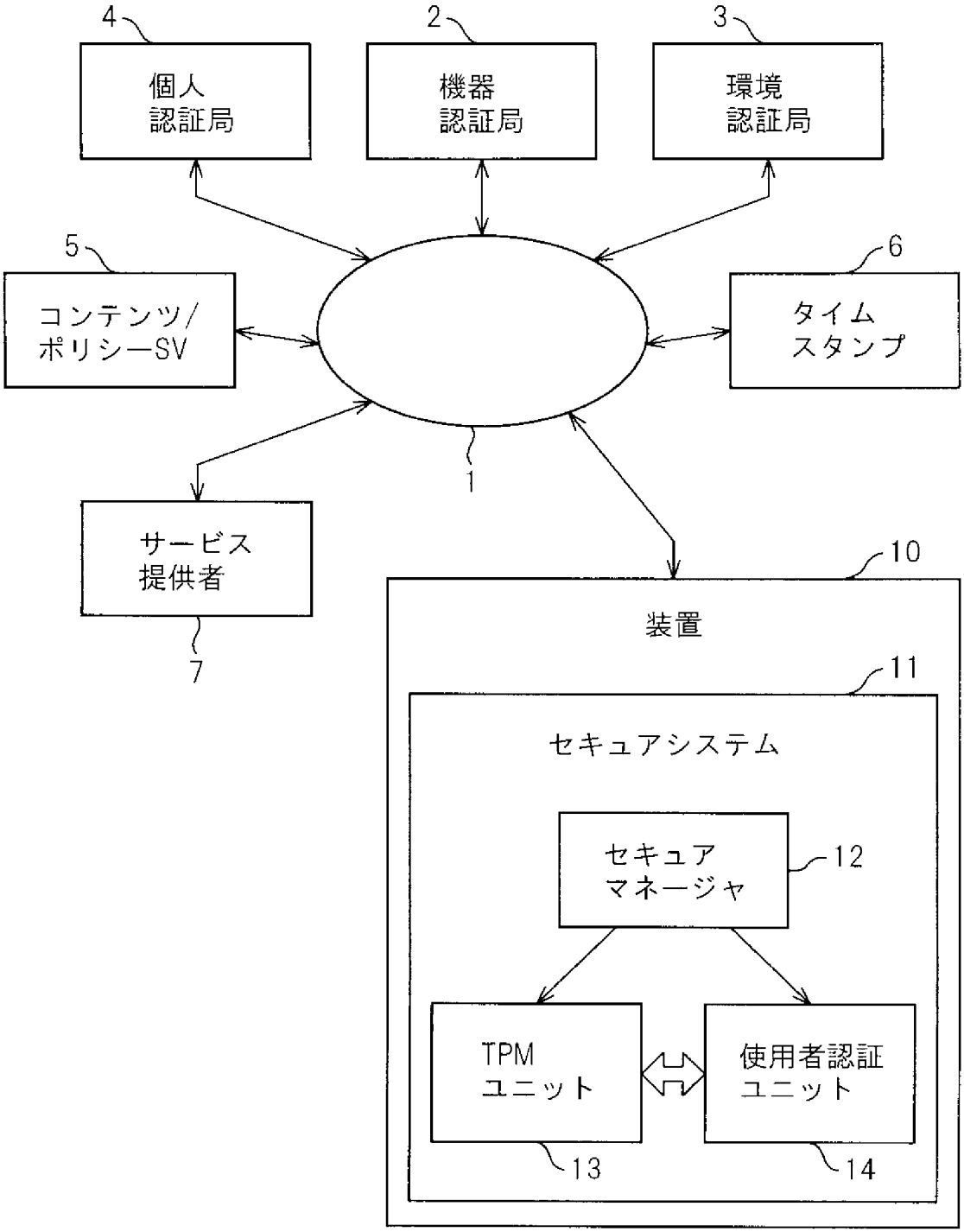
[19] 前記使用者認証ユニットは、カード認証を含むパスワード認証を行う請求項11から18のいずれか1項に記載のセキュアシステム。

[20] 前記使用者認証ユニットは、公開鍵方式を採用したICカード認証を行い、

前記セキュアマネージャは、複数のICカード情報を登録することを特徴とする請求項17に記載のセキュアシステム。

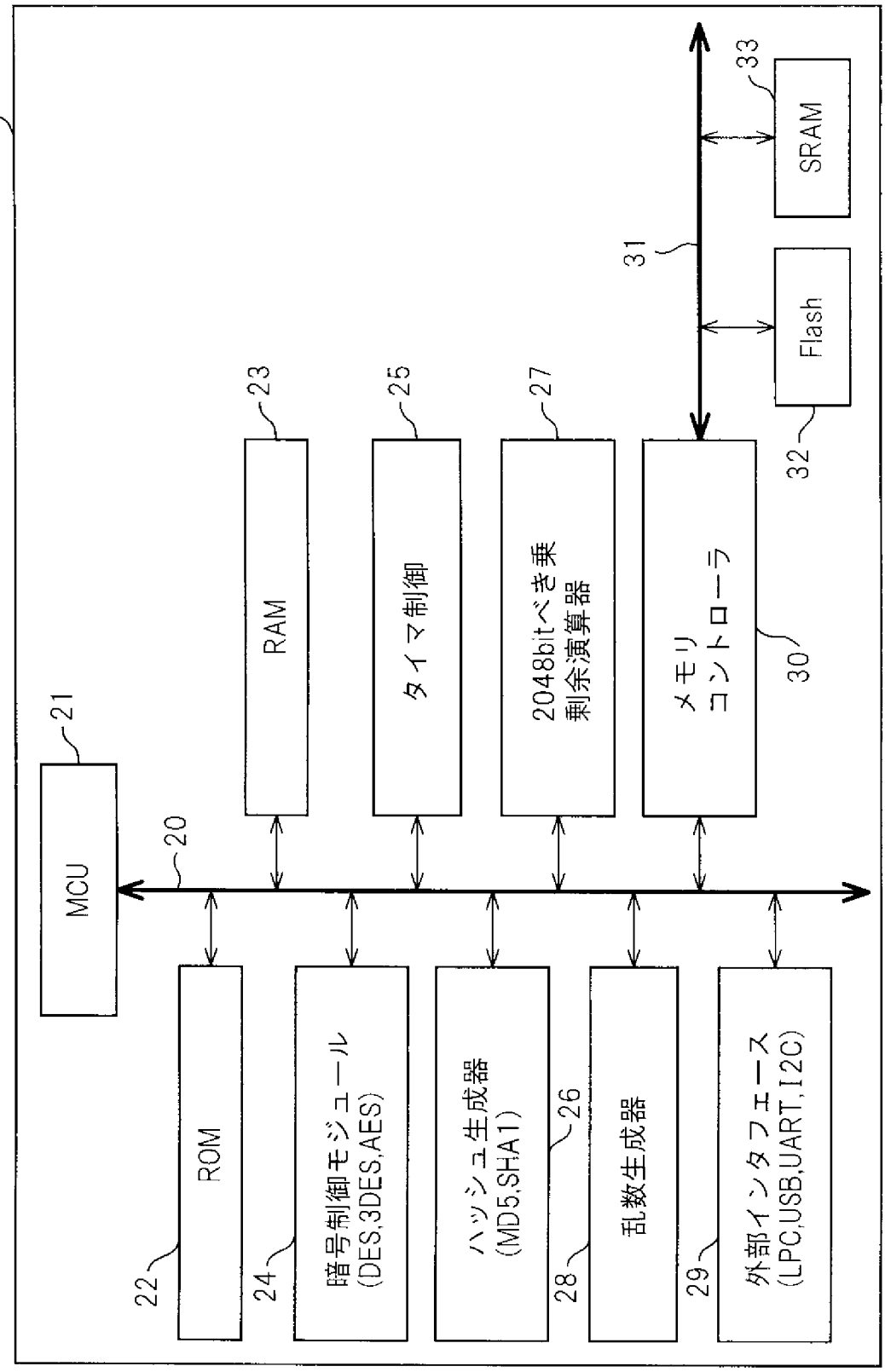
[図1]

Fig.1


4
個人
認証局
2
機器
認証局
3
環境
認証局
5
コンテンツ/
ポリシーSV
6
タイム
スタンプ
1
サービス
提供者
7
10
装置
11
セキュアシステム
セキュア
マネージャ
12
TPM
ユニット
使用者認証
ユニット
13
14

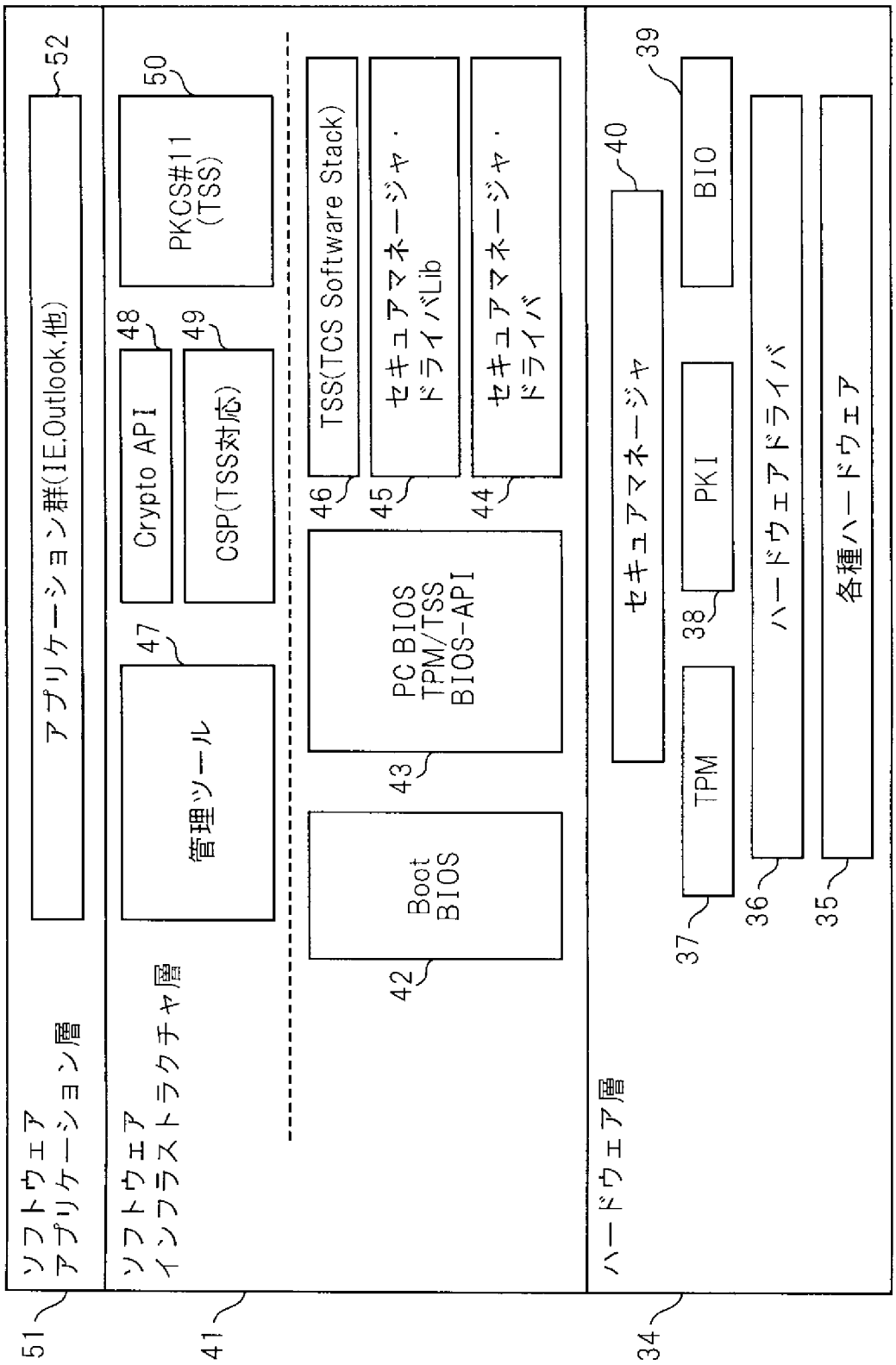
[図2]

Fig.2


11
MCU
21
20
RAM
23
タイマ制御
25
2048bitべき乗
剰余演算器
27
メモリ
コントローラ
30
31
SRAM
33
Flash
32
ROM
22
暗号制御モジュール
(DES,3DES,AES)
24
ハッシュ生成器
(MD5,SHA1)
26
乱数生成器
28
外部インタフェース
(LPC,USB,UART,I2C)
29

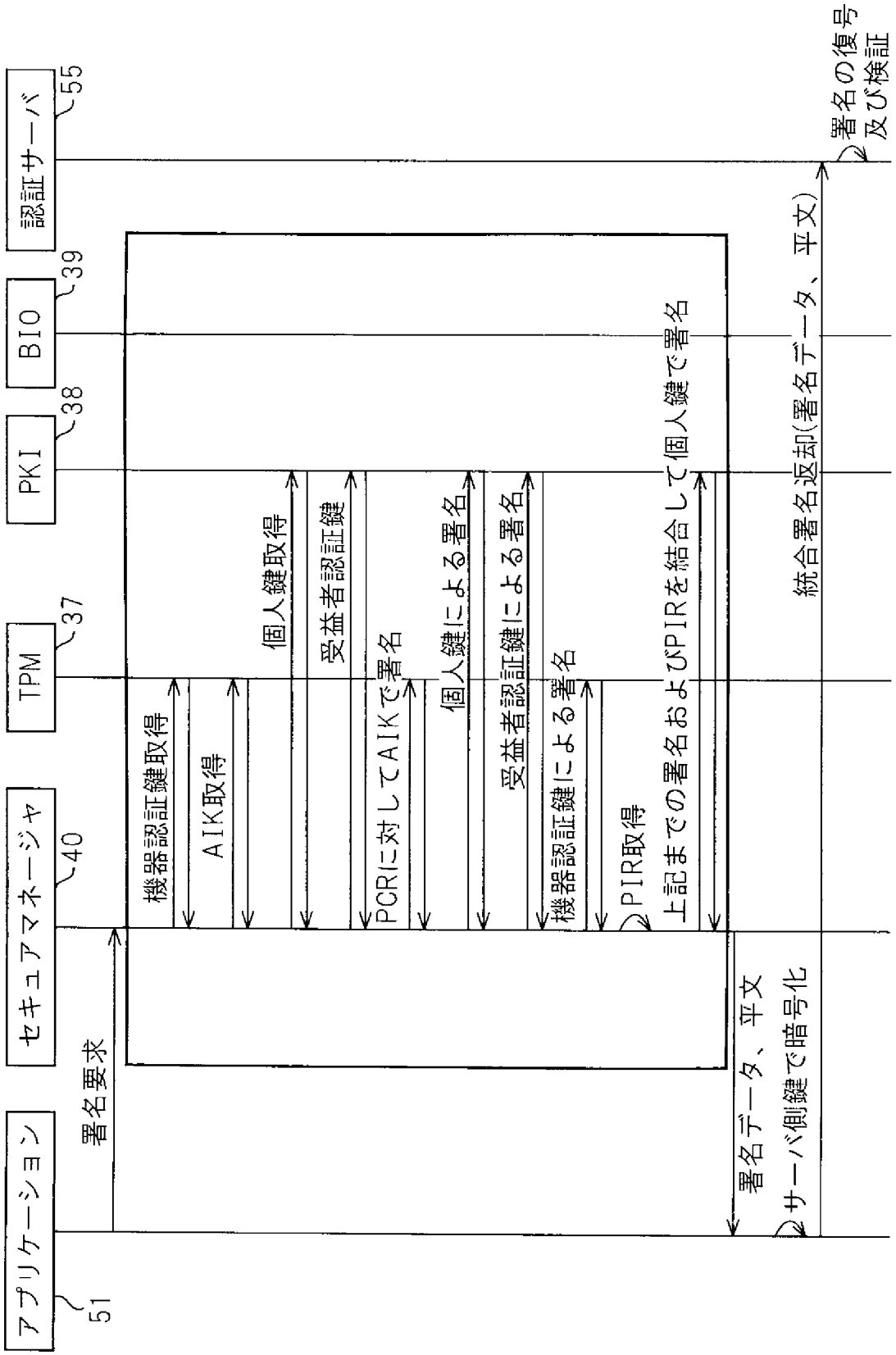
[図3]

Fig.3


ソフトウェア
アプリケーション層
51
アプリケーション群(IE,Outlook,他)
52
ソフトウェア
インフラストラクチャ層
41
管理ツール
47
Crypto API
48
CSP(TSS対応)
49
PKCS#11
(TSS)
50
Boot
BIOS
42
PC BIOS
TPM/TSS
BIOS-API
43
TSS(TCS Software Stack)
46
セキュアマネージャ・
ドライバLib
45
セキュアマネージャ・
ドライバ
44
ハードウェア層
34
セキュアマネージャ
40
TPM
37
PKI
38
BIO
39
ハードウェアドライバ
36
各種ハードウェア
35

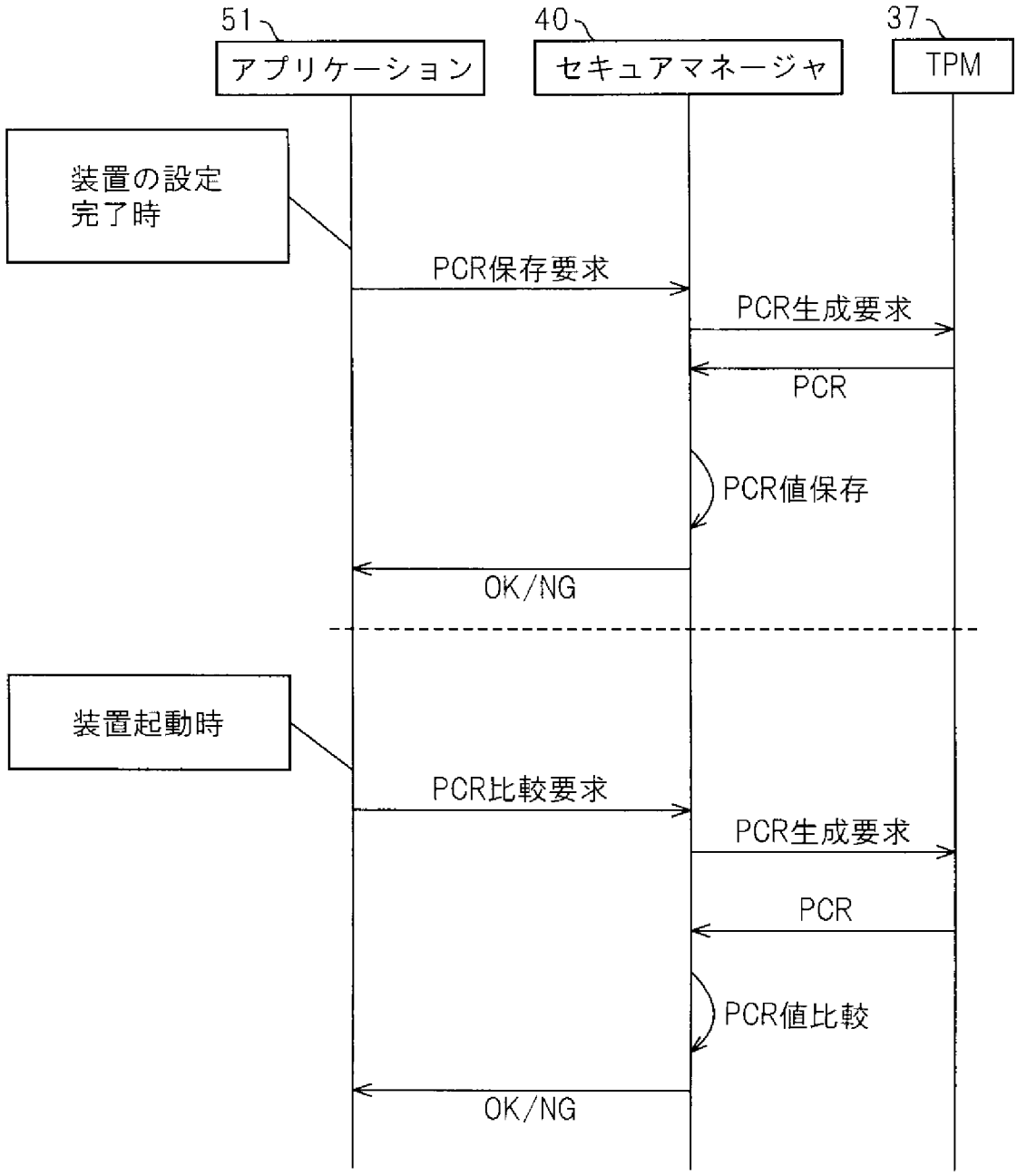
[図4]

Fig.4


アプリケーション
51
セキュアマネージャ
40
TPM
37
PKI
38
BIO
39
認証サーバ
55
署名要求
機器認証鍵取得
AIK取得
個人鍵取得
受益者認証鍵
PCRに対してAIKで署名
個人鍵による署名
受益者認証鍵による署名
機器認証鍵による署名
PIR取得
上記までの署名およびPIRを結合して個人鍵で署名
署名データ、平文
サーバ側鍵で暗号化
統合署名返却(署名データ、平文)
署名の復号
及び検証

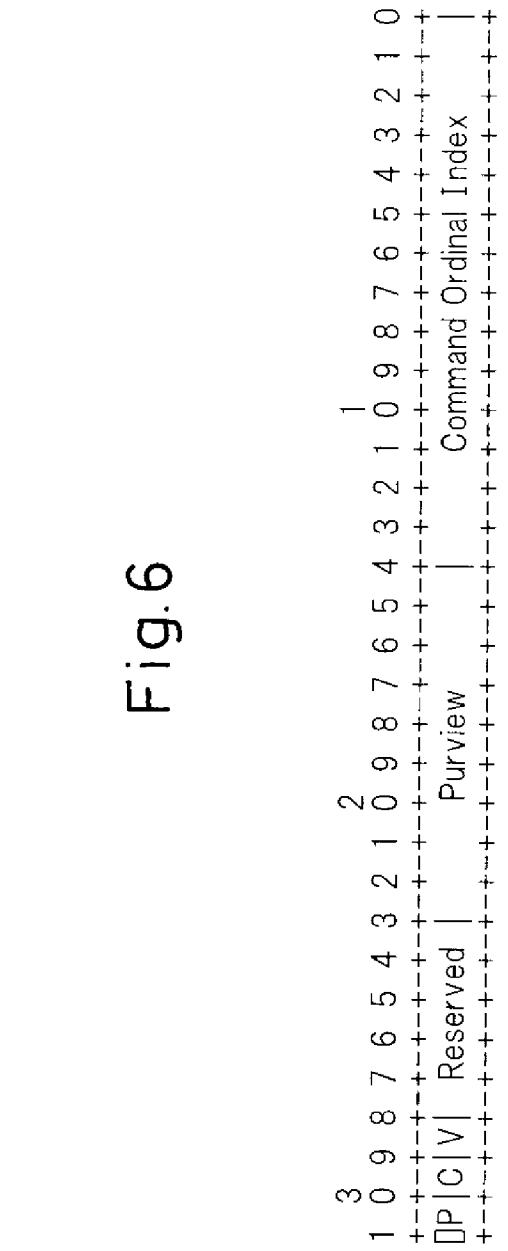
[図5]

Fig.5


51
アプリケーション
40
セキュアマネージャ
37
TPM
装置の設定
完了時
PCR保存要求
PCR生成要求
PCR
PCR値保存
OK/NG
装置起動時
PCR比較要求
PCR生成要求
PCR
PCR値比較
OK/NG

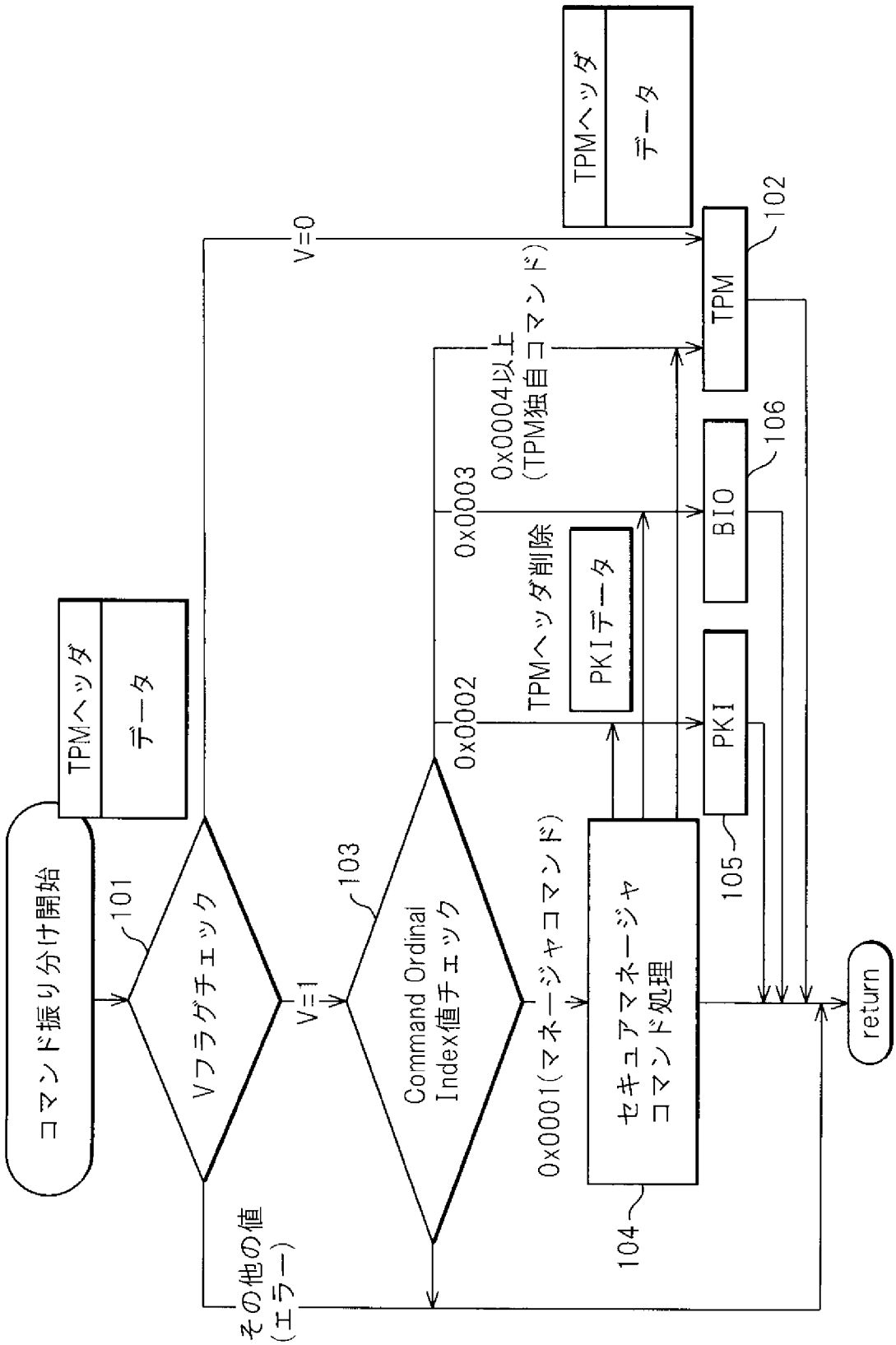
[図6]

Fig.6


3 2 1
1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0
P C V Reserved Purview Command Ordinal Index

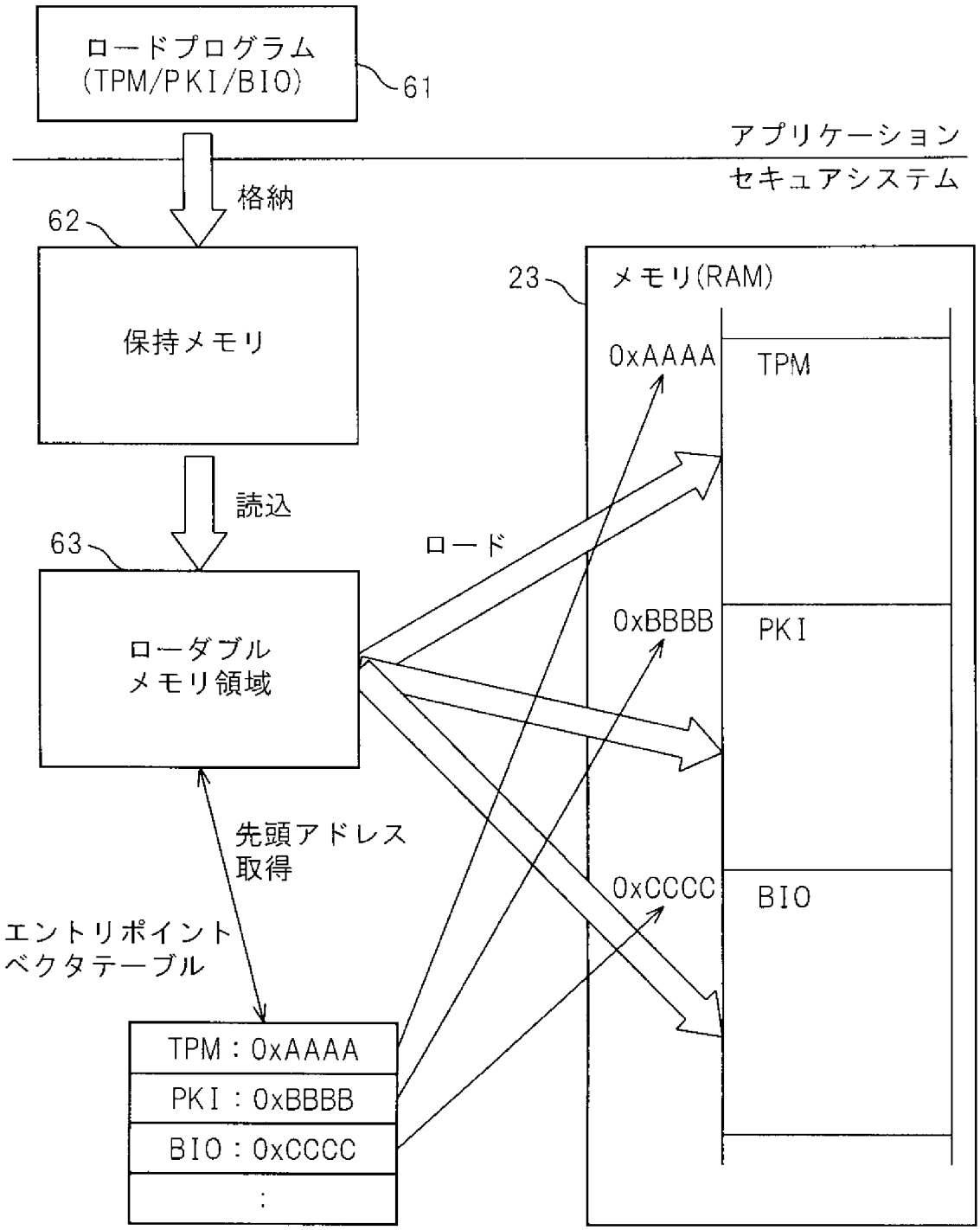
[図7]

Fig.7


コマンド振り分け開始
TPMヘッダ
データ
101
Vフラグチェック
V=0
V=1
その他の値
(エラー)
103
Command Ordinal
Index値チェック
0x0002
0x0003
0x0004以上
(TPM独自コマンド)
TPMヘッダ削除
PKIデータ
0x0001(マネージャコマンド)
セキュアマネージャ
コマンド処理
104
TPMヘッダ
データ
TPM
102
BIO
106
PKI
105
return

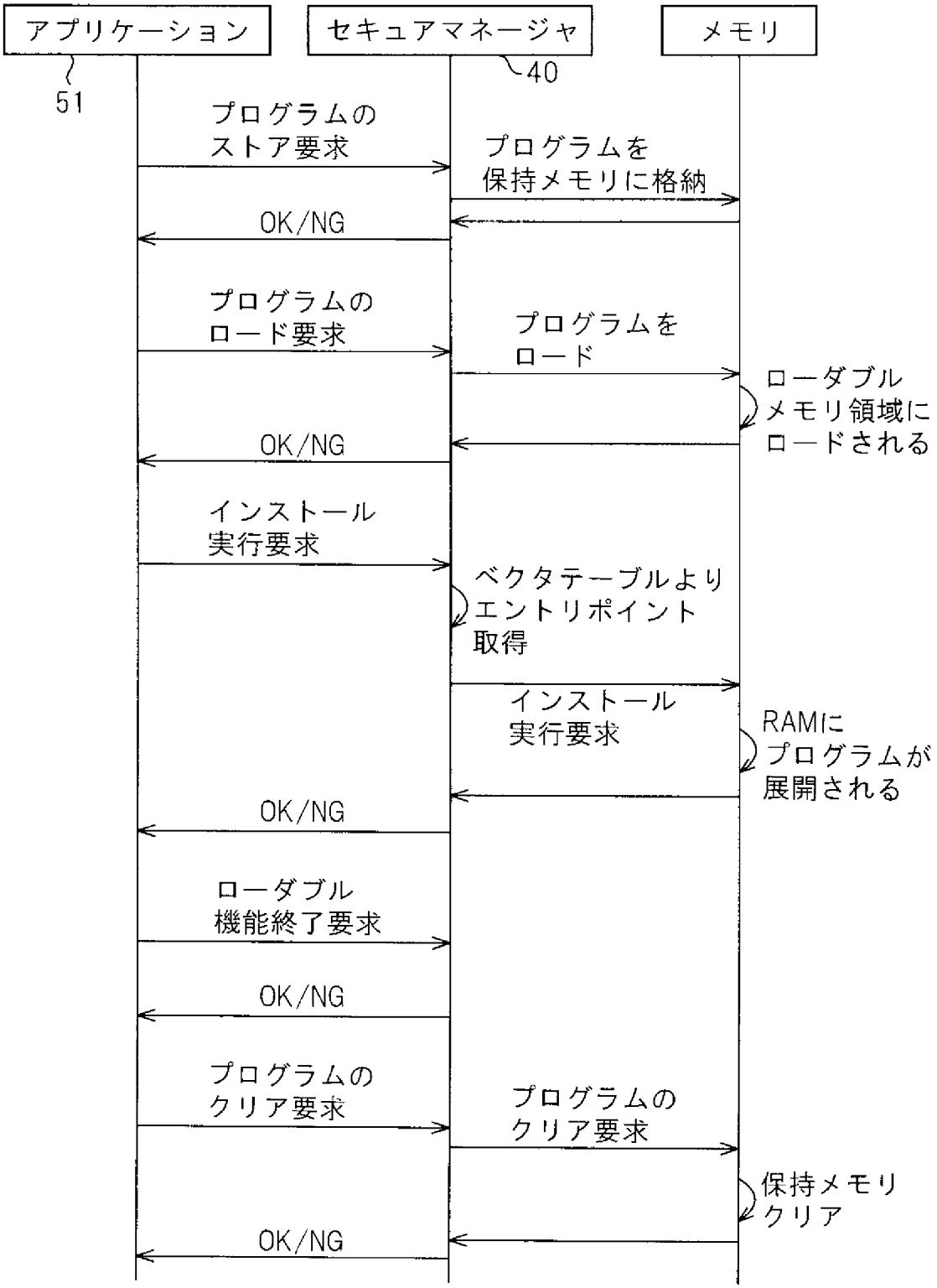
[図8]

Fig. 8


ロードプログラム
(TPM/PKI/BIO)
61
アプリケーション
セキュアシステム
格納
62
保持メモリ
読込
63
ローダブル
メモリ領域
ロード
23
メモリ(RAM)
0xAAAA
TPM
0xBBBB
PKI
0xCCCC
BIO
先頭アドレス
取得
エントリポイント
ベクタテーブル
TPM：0xAAAA
PKI：0xBBBB
BIO：0xCCCC
：

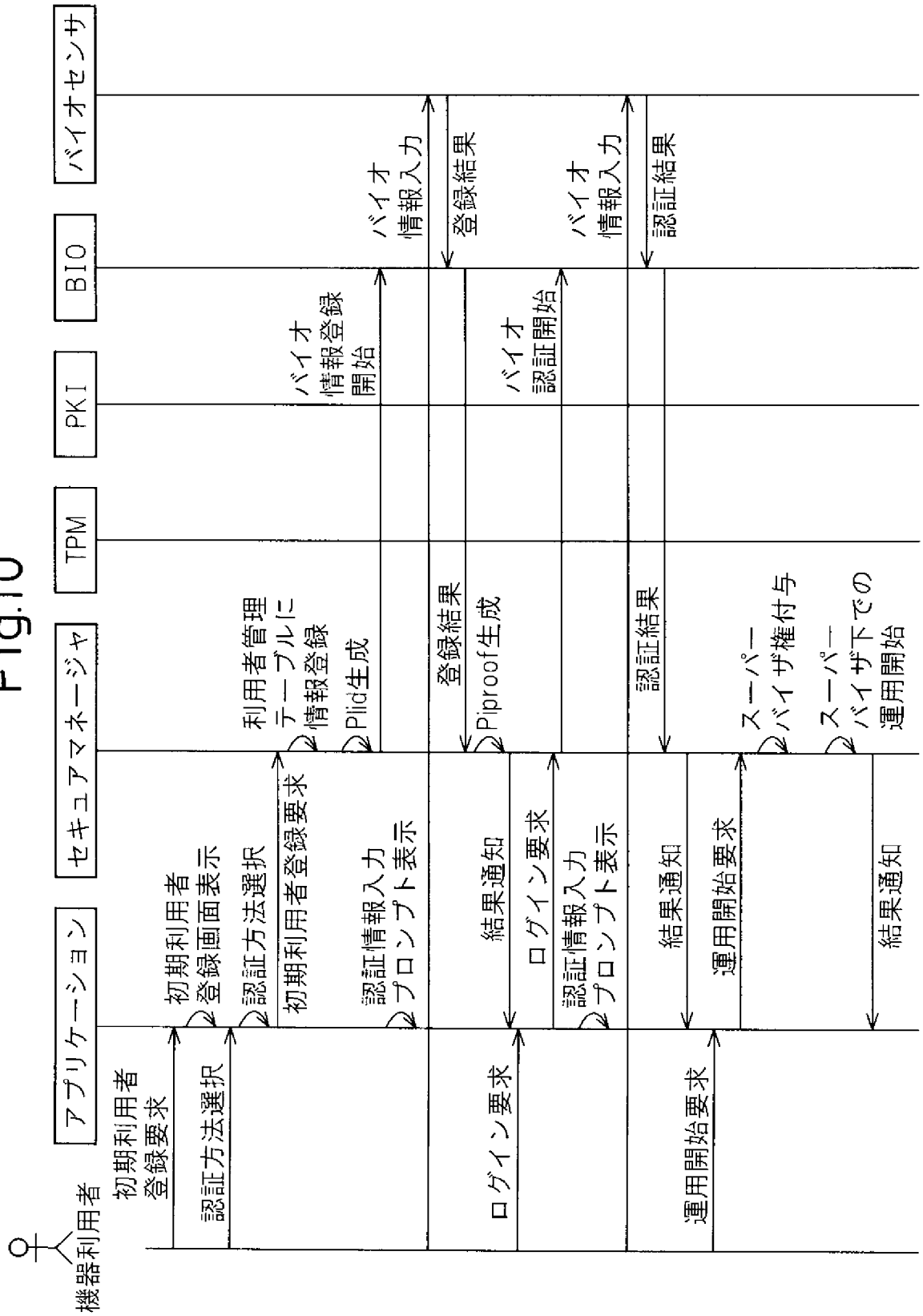
[図9]

Fig.9


アプリケーション
51
セキュアマネージャ
40
メモリ
プログラムの
ストア要求
プログラムを
保持メモリに格納
OK/NG
プログラムの
ロード要求
プログラムを
ロード
ローダブル
メモリ領域に
ロードされる
OK/NG
インストール
実行要求
ベクタテーブルより
エントリポイント
取得
インストール
実行要求
RAMに
プログラムが
展開される
OK/NG
ローダブル
機能終了要求
OK/NG
プログラムの
クリア要求
プログラムの
クリア要求
保持メモリ
クリア
OK/NG

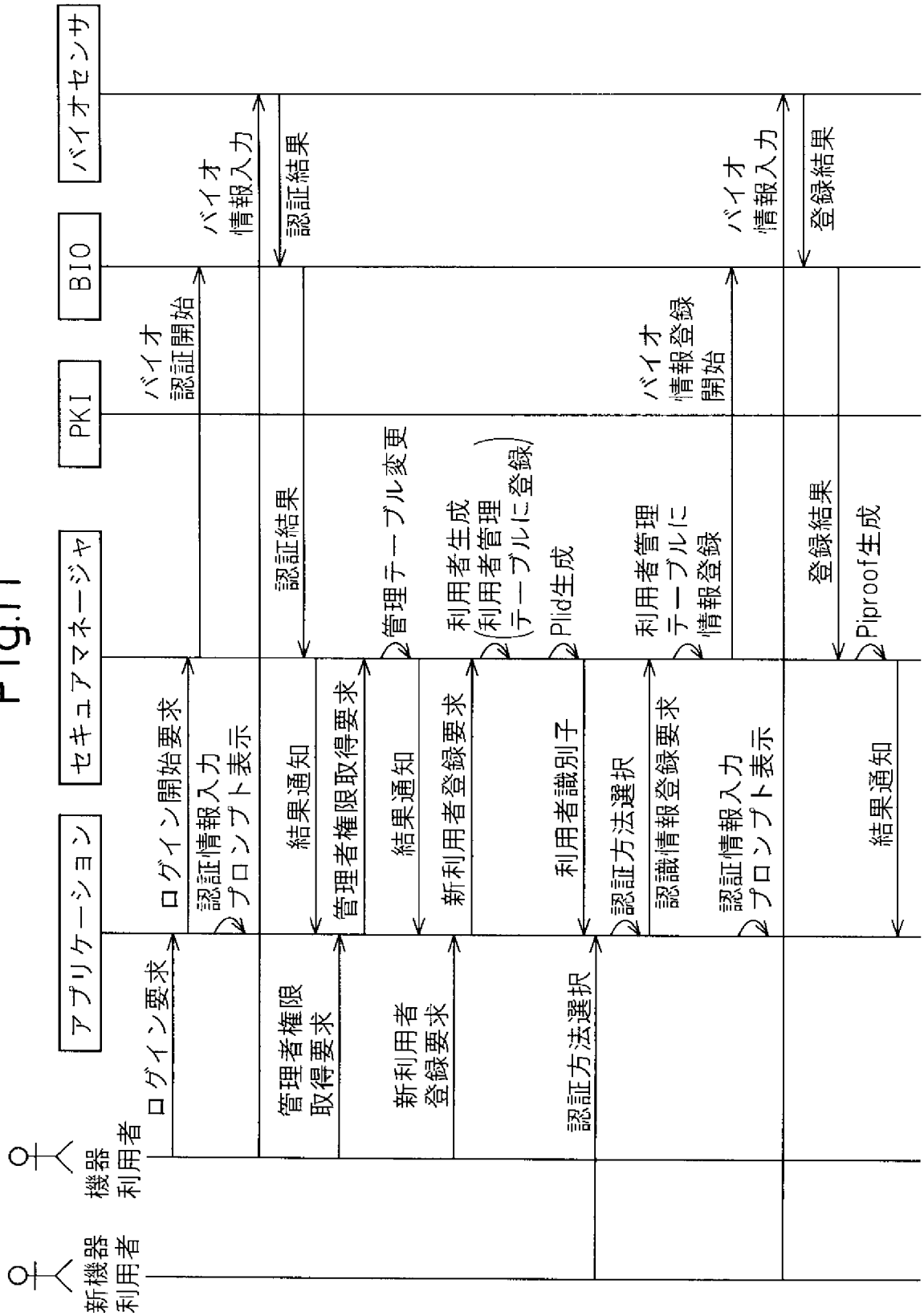
[図10]

Fig.10


機器利用者
アプリケーション
セキュアマネージャ
TPM
PKI
BIO
バイオセンサ
初期利用者登録要求
認証方法選択
初期利用者登録画面表示
認証方法選択
初期利用者登録要求
利用者管理テーブルに情報登録
PIid生成
認証情報入力プロンプト表示
バイオ情報登録開始
バイオ情報入力
登録結果
PIproof生成
結果通知
ログイン要求
バイオ認証開始
バイオ情報入力
認証結果
認証情報入力プロンプト表示
ログイン要求
結果通知
運用開始要求
スーパーバイザ権付与
運用開始要求
スーパーバイザ下での運用開始
結果通知
認証結果

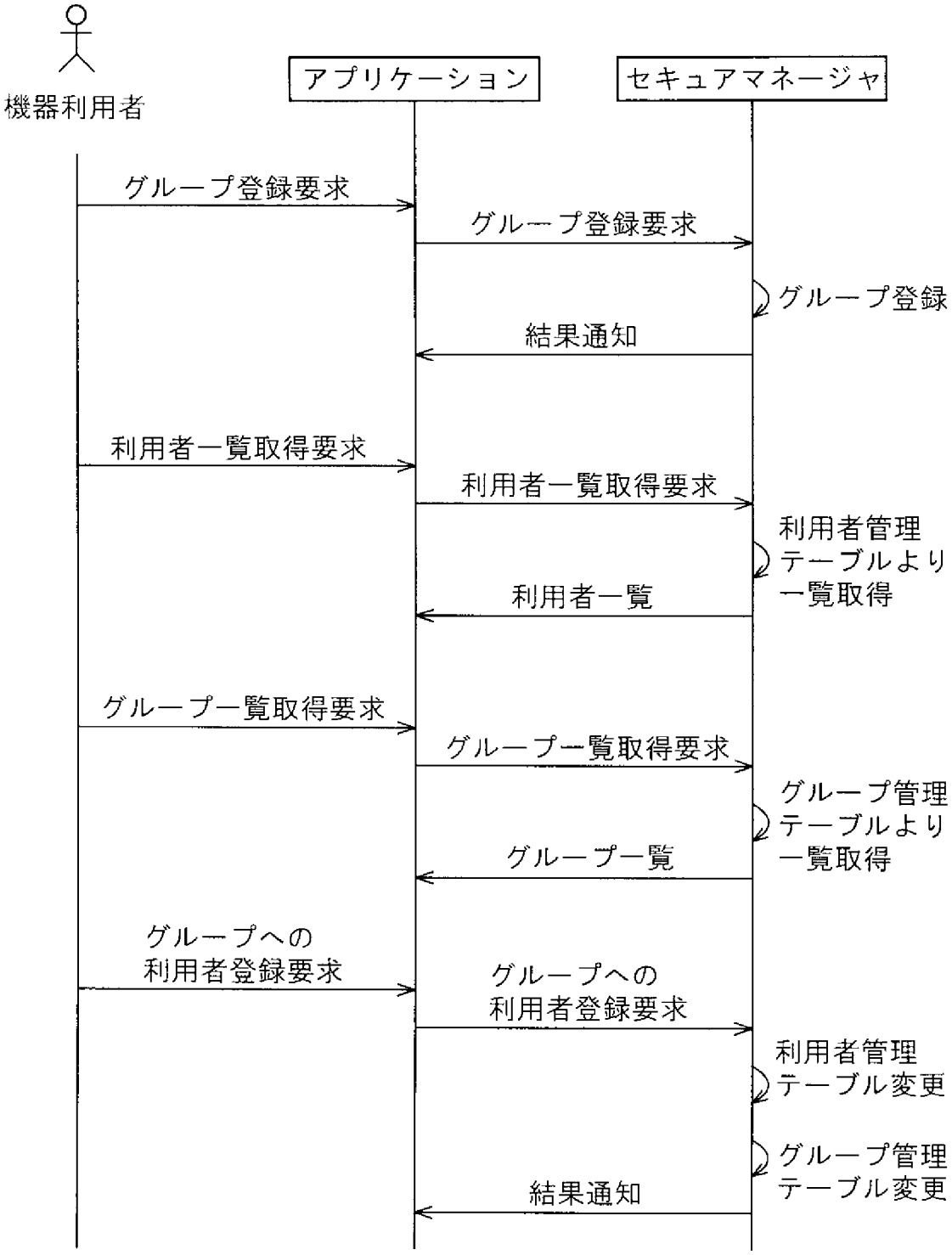
[図11]

Fig.11


新機器利用者
機器利用者
アプリケーション
セキュアマネージャ
PKI
BIO
バイオセンサ
ログイン要求
ログイン開始要求
認証情報入力
プロンプト表示
管理者権限取得要求
結果通知
管理者権限取得要求
新利用者登録要求
結果通知
新利用者登録要求
認証方法選択
バイオ認証開始
バイオ情報入力
認証結果
認証結果
管理テーブル変更
利用者生成
(利用者管理テーブルに登録)
PIid生成
利用者識別子
認証方法選択
バイオ情報登録開始
利用者管理テーブルに情報登録
認識情報登録要求
認証情報入力
プロンプト表示
バイオ情報入力
登録結果
登録結果
Piproof生成
結果通知

[図12]

Fig.12


機器利用者
アプリケーション
セキュアマネージャ
グループ登録要求
グループ登録要求
グループ登録
結果通知
利用者一覧取得要求
利用者一覧取得要求
利用者管理
テーブルより
一覧取得
利用者一覧
グループ一覧取得要求
グループ一覧取得要求
グループ管理
テーブルより
一覧取得
グループ一覧
グループへの
利用者登録要求
グループへの
利用者登録要求
利用者管理
テーブル変更
グループ管理
テーブル変更
結果通知

[図13]

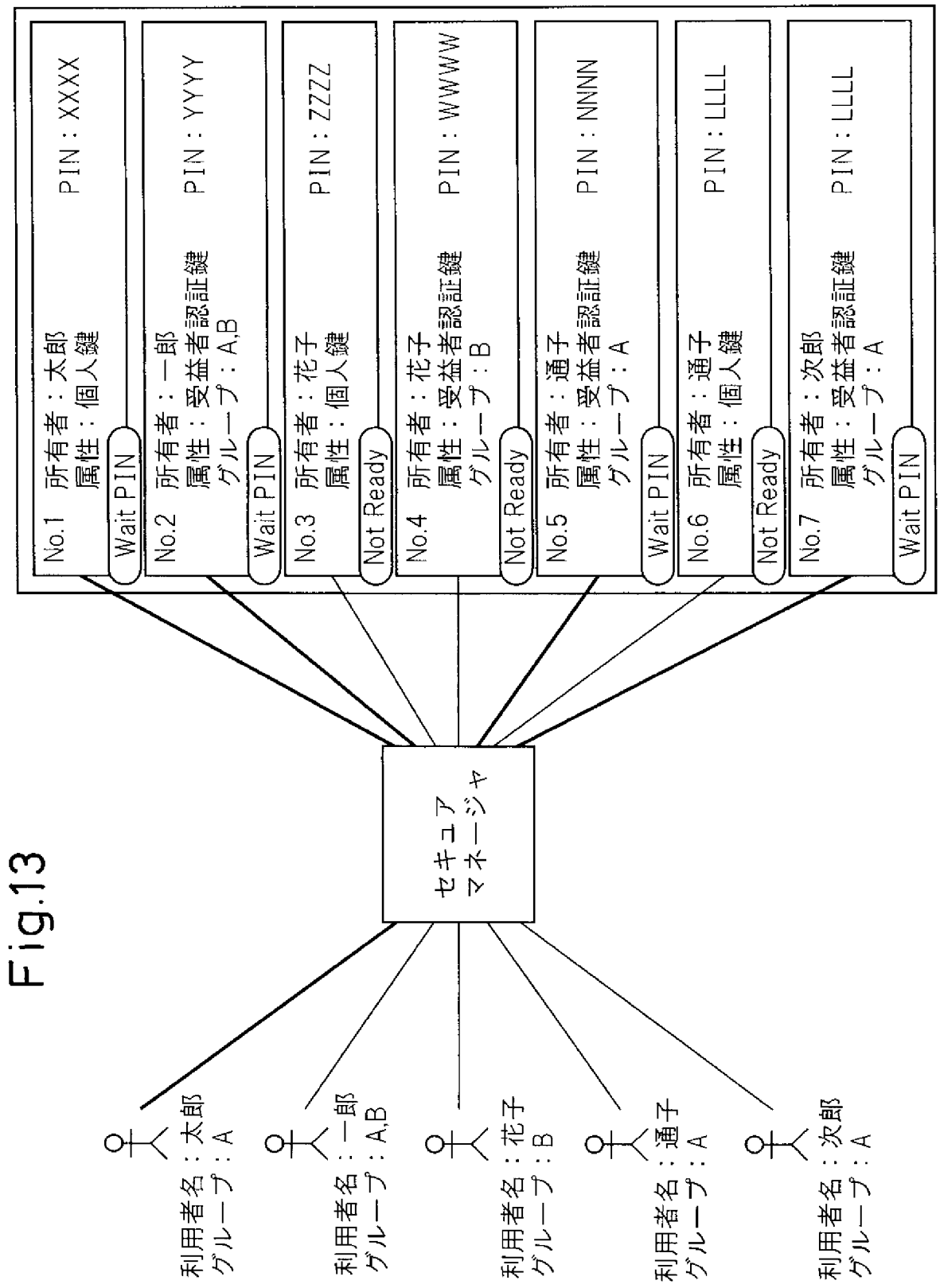

No.1 所有者：太郎
属性：個人鍵
PIN：XXXX
Wait PIN
No.2 所有者：一郎
属性：受益者認証鍵
グループ：A,B
PIN：YYYY
Wait PIN
No.3 所有者：花子
属性：個人鍵
PIN：ZZZZ
Not Ready
No.4 所有者：花子
属性：受益者認証鍵
グループ：B
PIN：WWWW
Not Ready
No.5 所有者：通子
属性：受益者認証鍵
グループ：A
PIN：NNNN
Wait PIN
No.6 所有者：通子
属性：個人鍵
PIN：LLLL
Not Ready
No.7 所有者：次郎
属性：受益者認証鍵
グループ：A
PIN：LLLL
Wait PIN
セキュア
マネージャ
利用者名：太郎
グループ：A
利用者名：一郎
グループ：A,B
利用者名：花子
グループ：B
利用者名：通子
グループ：A
利用者名：次郎
グループ：A

Fig.13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/055281

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/20(2006.01)i, *G06F21/24*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/20, G06F21/24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2007
Kokai Jitsuyo Shinan Koho	1971-2007	Toroku Jitsuyo Shinan Koho	1994-2007

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Patrick George, Gerald Maunier, "Combining User and Platform Trust Properties to Enhance VPN Client Authentication", In SAM'05, [online], 2005, Gemplus, [retrieved on 2007.05.15], Retrieved from the Internet <URL: http://www.gemplus.com/smart/rd/publications/pdf/GM05sam.pdf>	1-8,10-13,15-17,19,20 14,9,18
Y A	Liqun Chen, Siani Pearson, Anthanasios Vamvakas, "A Trusted Biometric System", [online], 2002, Hewlett-Packard, [retrieved on 2007.05.15], Retrieved from the Internet <URL: http://www.hpl.hp.com/techreports/2002/HPL-2002-185.pdf>	9,14,18 1-8,10-13,15-17,19,20

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 May, 2007 (15.05.07)	22 May, 2007 (22.05.07)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/055281

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2005/038635 A2 (International Business Machines Corp.), 28 April, 2005 (28.04.05), Full text; all drawings & EP 1673674 A3	1-20

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０５５２８１

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/20(2006.01)i, G06F21/24(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/20, G06F21/24

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００７年
日本国実用新案登録公報	１９９６－２００７年
日本国登録実用新案公報	１９９４－２００７年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	Patrick George, Gerald Maunier, "Combining User and Platform Trust Properties to Enhance VPN Client Authentication", In SAM'05, [online], 2005, Gemplus, [retrieved on 2007.05.15], Retrieved from the Internet <URL: http://www.gemplus.com/smart/rd/publications/pdf/GM05sam.pdf >	1-8, 10-13, 15-17, 19, 20
Y		14, 9, 18

☑ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１５．０５．２００７	２２．０５．２００７

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｓ	３４４９
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	石川　正二 電話番号　０３－３５８１－１１０１　内線　３５４６		

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	Liqun Chen, Siani Pearson, Anthanasios Vamvakas, "A Trusted Biometric System", [online], 2002, Hewlett-Packard, [retrieved on 2007.05.15], Retrieved from the Internet <URL: http://www.hpl.hp.com/techreports/2002/HPL-2002-185.pdf>	9, 14, 18
A		1-8, 10-13, 15-17, 19, 20
A	WO 2005/038635 A2 (International Business Machines Corporation) 2005.04.28, 全文, 全図 & EP 1673674 A3	1-20