(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
2007 年10 月25 日 (25.10.2007)

PCT

(10) 国際公開番号
WO 2007/119594 A1

(51) 国際特許分類:
G06K 19/07 (2006.01) *G06K 17/00* (2006.01)
G06F 21/24 (2006.01) *G06K 19/10* (2006.01)

(21) 国際出願番号: PCT/JP2007/056982

(22) 国際出願日: 2007 年3 月29 日 (29.03.2007)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2006-098865 2006 年3 月31 日 (31.03.2006) JP
特願2007-075217 2007 年3 月22 日 (22.03.2007) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

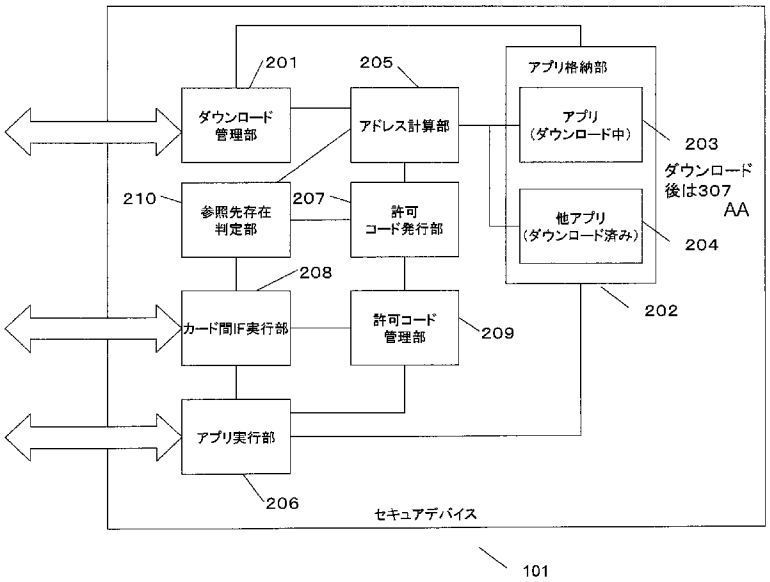
(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 田靡 雅基 (TANABIKI, Masamoto). 竹内 康雄 (TAKEUCHI, Yasuo). 鶴切 恵美 (TSURUKIRI, Emi). 徳田 泰久 (TOKUDA, Yasuhisa).

(74) 代理人: 高松 猛, 外(TAKAMATSU, Takeshi et al.); 〒1050003 東京都港区西新橋一丁目７番１３号 栄光特許事務所 Tokyo (JP).

[続葉有]

(54) **Title:** SECURE DEVICE AND READ/WRITE DEVICE

(54) **発明の名称:** セキュアデバイス及び読み書き装置



201 DOWNLOAD MANAGING UNIT
210 REFERENCE DESTINATION EXISTENCE JUDGING UNIT
208 INTER-CARD IF EXECUTION UNIT
206 APPLICATION EXECUTION UNIT
205 ADDRESS CALCULATION UNIT
207 ALLOWANCE CODE ISSUING UNIT
209 ALLOWANCE CODE MANAGING UNIT
202 APPLICATION STORAGE UNIT
203 APPLICATION (DOWNLOAD IN PROGRESS)
204 OTHER APPLICATION (DOWNLOAD COMPLETED)
AA 307 AFTER DOWNLOAD
101 SECURE DEVICE

(57) Abstract: It is possible to solve the problem that a server application owned by a secure device cannot be used by a client application owned by other secure device. A secure device includes: an application storage unit (202) for storing a client application as an application performing data processing; an address calculation unit (205) for judging whether the application storage unit (202) has a server application for passing data to/from the client; and a reference destination existence judging unit (210) for judging whether other secure device has a first server application when the address calculation unit (205) has judged that the application storage unit (202) does not have the first server application for passing data to/from the first client application.

(57) 要約: 本発明は、セキュアデバイスが有するサーバアプリを、他のセキュアデバイスが有するクライアントアプリが利用することができないという課題を解決するためのものである。 本発明に係るセキュアデバイスは、データ処理を行うアプリケーションである、クライアントアプリを格納するアプリ格納部２０２と、クライアントアプリとデータのやり取りを行う、サーバアプリを前記アプリ格納部２０２が有しているか否かを判定するアドレス計算部２０５と、前記アドレス計算部２０５により、前記アプリ格納部２０２は、第1のクライアントアプリとデータのやり取りを

[続葉有]

WO 2007/119594 A1

(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, BH, 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, 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.

(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

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

行う第1のサーバアプリを有していないと判定されたとき、他のセキュアデバイスが前記第1のサーバアプリを有しているか否かを判定する参照先存在判定部２１０と、を有する。

明 細 書

セキュアデバイス及び読み書き装置

技術分野

[0001] 本発明は、セキュアデバイス並びに、セキュアデバイスに接続される外部機器に関するものである。

背景技術

[0002] 現在セキュリティデバイスとしてICカードが着目されている。ユーザの利便性の向上、ICカードによるサービスを提供したい事業者の参入障壁を下げることを目的に、カード発行後にアプリをダウンロードすることが可能なマルチアプリ対応カードの開発が行われている。

[0003] また最近では、ICチップに大容量メモリを備えることで、この大容量メモリをICカード拡張メモリ保護領域として利用可能なデバイス(以下、セキュアメモリカード)が提案され、ICカードアプリデータの大容量化ニーズに対応可能となる。セキュアメモリカードは、モバイル機器の大きさに適合できることから、スロットつきのモバイル機器に直接挿入し、モバイル機器を利用したEC(Electronic Commerce)サービス利用への展開が期待されている。

[0004] ここで、ICカードのハードウェア構成について概観する。

[0005] 図30は、ICカードのハードウェアに関する機能ブロック図である。ICカード3001は、CPU(Central Processing Unit)3002、ROM(Read Only Memory)3003、揮発性メモリ(例:RAM:Random Access Memory)3004、揮発性メモリ(例:EEPROM:Electrically Erasable Programmable Read Only Memory)3005、I/O IF3006を備えている。CPU3002は、演算を行う。ROM3003は書き換えができない読み出し専用のメモリである。ROM3003に格納される内容は、ICカード製造時に決定され、その後変更することはできない。RAM3004は読み書きが可能なメモリである。EEPROM3005は電源が切断されても内容が保持されるようになっている。I/O IF3006は、ICカードと外部とのデータ交換を担当する。CPU3002で実行されるプログラムは、通常「アプリケーション」(以下、アプリと称する。)と呼

ばれる。アプリの実行のためのコードは、ROM3003やEEPROM3005に格納される。また図30に示す以外に、ICカードが暗号操作のため暗号用コプロセッサを備える場合もある。

[0006] ICカードに登載されるアプリと外部(リーダ)は、ISO／IEC7816－4で規定されているAPDU(Application Protocol Data Unit)を使ってデータを交換する。APDUは、リーダがICカードに与えるコマンドと、ICカードからリーダに返すレスポンスの2つの構成からなる。

[0007] 図31はAPDUコマンド3101を示しており、ヘッダと本体から構成される。本体は、任意の長さで、空白の場合はなくてもよい。ヘッダは、クラス(CLA)、命令(INS)とパラメータ1と2(P1, P2)で構成されている。

[0008] 図32はAPDUレスポンスコマンド3201を示しており、データ部とStatusWord(SW)から構成される。

[0009] ICカードの特徴としてアプリケーションファイアウォールがある。アプリケーションファイアウォールとは、ICカード内に複数のアプリが並存する場合に、他のアプリが明示的にアクセスするためのインタフェースを与えない限り、アプリは他のアプリの関数呼び出しやオブジェクトへのデータアクセスができないことを意味する。

[0010] ここでアプリ間のオブジェクト共有方法としてShareable Interface Object(SIO)が知られている。(特許文献1参照)

[0011] 以下、SIOを提供するアプリをサーバアプリ、SIOを利用するアプリをクライアントアプリと称する。

[0012] 例えば、携帯電話に2種類のアプリが搭載されたICカード(チップ)を挿入し、改札機と改札アプリが非接触通信を行って改札を通過し、カード内で改札アプリが表示アプリに結果を渡し、携帯電話が表示アプリと接触通信を行って携帯電話の画面に表示することにより、表示装置を持たないICカードの利用結果を表示するのに有効な方法が提案されている。

[0013] この例において、改札アプリがクライアントアプリ、表示アプリがサーバアプリとして機能することになる。

特許文献1:特表2003－522988号公報

発明の開示

発明が解決しようとする課題

[0014] ICカードのようなデバイスが改札の通過や入退出チェックに利用される場合には、処理全体が1秒以下～数秒程度で完結することが期待される。ICカードのCPU処理能力が一般のPCやモバイル機器に比べて低いため、ダウンロード時にリンクを実施し、アドレス参照先として即値を設定することが多い。Dynamic Link Libraryのように必要に応じてメモリに呼び出して利用するような手法は、リンク処理自体がボトルネックとなりICカードアプリに利用できない。

[0015] したがって、サーバアプリが搭載されていない状態でクライアントアプリをダウンロードするとリンクエラーとして失敗するICカードが多い。

[0016] そのため、既存技術においてサーバアプリとクライアントアプリは同一カード内に存在する必要がある。

[0017] しかし、サーバアプリによっては複数のクライアントアプリから利用されるものもあり、所有するカード全てに同じサーバアプリを搭載することは、ICカードの限られたメモリを有効活用できていない。

[0018] 本発明はこうした従来の問題点を解決するものであり、クライアントアプリをダウンロードするときに同一カード内にサーバアプリが存在しない場合にもダウンロードを許可し、クライアントアプリの実行時に別のカードに搭載されたサーバアプリと連携する方法(以下、カード間IF利用と称する。)を提供することを目的とする。

課題を解決するための手段

[0019] 本願発明は、データ処理を行うアプリケーションであるクライアントアプリを格納するアプリ格納部と、クライアントアプリとデータのやり取りを行うサーバアプリを前記アプリ格納部が有しているか否かを判定するアドレス計算部と、前記アドレス計算部により、前記アプリ格納部は、第1のクライアントアプリとデータのやり取りを行う第1のサーバアプリを有していないと判定されたとき、他のセキュアデバイスが前記第1のサーバアプリを有しているか否かを判定する参照先存在判定部と、を有する、セキュアデバイスである。

[0020] これにより、自己のセキュアデバイスにサーバアプリがない場合にも、他のセキュア

デバイスのサーバアプリにより、自己のセキュアデバイスのクライアントアプリを実行することが出来るかを確認できる。

発明の効果

[0021] 本発明により、セキュアデバイス内のメモリ領域の削減を図ることが出来るという効果を有する。

図面の簡単な説明

[0022] [図1]本発明の実施の形態1におけるシステム構成図

[図2]本実施の形態1におけるセキュアデバイスのブロック図

[図3]ダウンロード中と終了後のアプリ領域を示す図

[図4]本実施の形態1における他のセキュアデバイスのブロック図

[図5]本実施の形態1における読み書き装置のブロック図

[図6]カード内に参照先が存在する場合の処理フロー図

[図7]カード内に参照先が存在しない場合の処理フロー図

[図8]本実施の形態1におけるアドレス空間を示す図

[図9]許可コードテーブルの一例を示す図

[図10]許可コードを付与されたアプリの処理フロー図

[図11a]コマンドとレスポンスの一例を示す図(a)

[図11b]コマンドとレスポンスの一例を示す図(b)

[図12]本実施の形態2におけるセキュアデバイスのブロック図

[図13]本実施の形態2における他のセキュアデバイスのブロック図

[図14]読み書き装置への入力と出力の関係図

[図15]本実施の形態3における読み書き装置のブロック図

[図16]本実施の形態3における処理フロー図

[図17]本実施の形態4における読み書き装置のブロック図

[図18]本実施の形態4における処理フロー図

[図19]本実施の形態5における処理フロー図

[図20]本実施の形態5における許可コードテーブルの例

[図21]本実施の形態5における許可コード発行フロー図

[図22]指示書の一例を示す図

[図23]仮許可コード管理テーブルの一例を示す図

[図24]本実施の形態7におけるセキュアデバイスのブロック図

[図25]本実施の形態7における他のセキュアデバイスのブロック図

[図26]アプリ実行部が扱うフレームの一例を示す図

[図27]スタック制御部が作成するデータの一例を示す図

[図28]参照先のアプリが同じセキュアデバイス内に存在する場合のアプリのダウンロードフロー図

[図29]本実施の形態2におけるセキュリティ確保フロー図

[図30]ICカードのハードウェアに関する機能ブロック図

[図31]APDUコマンドのフォーマット図

[図32]APDUレスポンスのフォーマット図

[図33a]読み書き装置が扱うデータ型定義を示す図(1)

[図33b]読み書き装置が扱うデータ型定義を示す図(2)

符号の説明

[0023] 101 セキュアデバイス

102 他のセキュアデバイス

103 読み書き装置

201 ダウンロード管理部

202 アプリ格納部

203 アプリ(ダウンロード中)

204 他アプリ(ダウンロード済み)

205 アドレス計算部

206 アプリ実行部

207 許可コード発行部

208 カード間IF実行部

209 許可コード管理部

210 参照先存在判定部

301　ダウンロード中のアプリ

302　アプリコード用データ領域

303　アプリ計算用データ領域

304　アプリデータ領域

305　アプリコード用データ

306　アプリ計算用データ

307　ダウンロード後のアプリ

308　アプリコード

309　ダウンデータ

401　サーバアプリ

501　排他制御通信部

502　アプリ制御部

801　メモリ空間

802　アプリに許可された領域

803　システム領域

901　許可コードテーブル

1101、1103、1105、1107　レスポンス、

1102　選択コマンド

1104、1108　共有コマンド

1106　INVOKEコマンド

1201　セキュアデバイス

1202　セキュリティ管理部

1301　セキュアデバイス

1302　カード間IF実行部

1303　セキュリティ管理部

1401　読み書き装置への入力(セキュアデバイスからのレスポンス)

1402　読み書き装置からの出力(他のセキュアデバイスへのコマンド)

1403　読み書き装置への入力(他のセキュアデバイスからのレスポンス)

1404 読み書き装置からの出力(セキュアデバイスへのコマンド)

1501 読み書き装置

1502 所有者管理部

1701 読み書き装置

1702 所有者確認情報入力部

1703 ダウンロード条件判定部

2001 許可コードテーブル

2201 指示書

2301 仮許可コード管理テーブル

2401 セキュアデバイス

2402 クライアントアプリ

2403 スタック操作部

2501 他のセキュアデバイス

2502 スタック制御部

2601 アプリの一部

2602 フレーム1

2603 フレーム2ROM

2604 スタック

2605 ローカル変数

2701 レスポンスデータ

3001 ICカード

3002 CPU

3003 ROM

3004 RAM

3005 EEPROM

3006 I/O IF

3101 APDUコマンド

3201 APDUレスポンス

3301 読み書き装置が扱うデータ構造定義書

発明を実施するための最良の形態

[0024] 本発明は、クライアントアプリをダウンロードするときに同一カード内にサーバアプリが存在しない場合にもダウンロードを許可し、クライアントアプリの実行時に別のカードに搭載されたサーバアプリと連携するセキュアデバイスに関するものである。

[0025] 実施の形態1は、クライアントアプリをダウンロードするときに同一カード内にサーバアプリが存在しない場合にもダウンロードを許可し、クライアントアプリの実行時に別のカードに搭載されたサーバアプリと連携するセキュアデバイスに関する発明である。

[0026] 実施の形態2は、連携時にセキュリティを確保するシステムに関する発明である。

[0027] 実施の形態3は、連携時にセキュアデバイスと、他のセキュアデバイスの所有者の同一性を確認するシステム(その1)に関する発明である。

[0028] 実施の形態4は、連携時にセキュアデバイスと、他のセキュアデバイスの所有者の同一性を確認するシステム(その2)に関する発明である。

[0029] 実施の形態5は、サーバアプリが搭載されたセキュアデバイスのライフサイクルに連動したクライアントアプリの利用制御方法に関する発明である。

[0030] 実施の形態6は、同一カード内にサーバアプリが存在しない場合のクライアントアプリの条件付きダウンロード方法と、条件のチェック方法に関する発明である。

[0031] 実施の形態7は、他のセキュアデバイスに搭載されたサーバアプリに処理を依頼し、サーバアプリの処理データをクライアントアプリで利用する方法に関する発明である。

[0032] 以下、本発明の実施形態について図を用いて説明する。なお、本発明はこれら実施形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実施しうる。

[0033] (実施の形態1)

本実施例に記載の発明は、クライアントアプリをダウンロードするときに同一カード内にサーバアプリが存在しない場合にもダウンロードを許可し、クライアントアプリの実行時に別のカードに搭載されたサーバアプリと連携するセキュアデバイスである。

[0034] たとえば、携帯電話の画面にクライアントアプリの処理結果を表示する表示アプリをサーバアプリとし、定期券アプリ、プリペイドアプリをクライアントアプリとしたセキュアデバイスに適用する場合が考えられる。

[0035] あるいは、視聴権のチェックを行うサーバアプリと、視聴権と視聴コンテンツを格納するクライアントアプリの関係において、クライアントアプリが視聴権をサーバアプリに渡し、サーバアプリによる視聴権に付随する年齢、回数、有効期限、総再生時間などの条件チェックに合格しないと視聴できない例にも適用できる。

[0036] 本実施の形態について図1から図11、図28を用いて説明する。

[0037] 図1は本実施の形態におけるセキュアデバイスと、他のセキュアデバイスとの連携システムを示した図であり、セキュアデバイス101と他のセキュアデバイス102と読み書き装置103とから構成される。

[0038] 図2、図4、図5は、それぞれ図1に示す、セキュアデバイス101、他のセキュアデバイス102、読み書き装置103の構成図である。

[0039] 図2は、上記のように、セキュアデバイス101の構成を示したブロック図である。

[0040] ダウンロード管理部201は、読み書き装置103と通信を行い、セキュアデバイス101にアプリをダウンロードする場合の動作を管理する。

[0041] アプリ格納部202は、ダウンロード中のアプリ203とダウンロード済みのアプリ204とを含む。

[0042] 図3は、図2のアプリ格納部202中で、アプリが占有する領域を示したものである。

[0043] ダウンロード中のアプリ301(203)が確保する領域は、アプリコード用データ領域302とアドレス計算用データ領域303とアプリデータ領域304である。

[0044] アプリコード用データ領域302にはアプリコード用データ305が格納され、アドレス計算用データ領域303には、アドレス計算用データ306が格納される。

[0045] ダウンロード後のアプリ307が占有する領域は、アプリコード用データ領域302とアプリデータ領域304である。ア プリコード用データ領域302には、アプリコード308が格納され、アプリデータ領域304には、アプリデータ309が格納される。

[0046] アドレス計算部205は、ダウンロード中のアプリ203中のアプリコード用データ305とアプリ計算用データ306と、ダウンロード済みの他アプリ204を利用して、ダウンロ

ード対象のアプリ203の「アドレス解決」を行う。

[0047] 「アドレス解決」とは、関数呼び出しやオブジェクトアクセス時の参照先のアドレスを直接的なデータに更新することをいう。

[0048] また、アドレス解決後に アドレス計算用データ領域303は削除され、ダウンロードが完了した後にはアプリコード308とアプリデータ309とからなるアプリ307がダウンロード済みアプリとしてアプリ格納部202に格納される。

[0049] ダウンロード済みのアプリ307は、読み書き装置103からのコマンドによって、セキュアデバイス101のアプリ実行部206により実行される。

[0050] 例えば、アプリ格納部202には、アプリコード308としてバイトコードが格納され、アプリデータ309としてオブジェクトが格納され、アプリ実行部206として仮想マシンが上記バイトコードを解釈し処理を行う技術が広く知られている。

[0051] 本実施の形態1をはじめ本文中の実施の形態において、このような処理系を用いて説明する。また、仮想マシンが管理するメモリ空間におけるアドレスを16ビット(2バイト)で表記することにする。

[0052] 許可コード発行部207は、アドレス解決中のアドレス計算部205からの依頼を受けて「許可コード」を発行する。「許可コード」については後述する。

[0053] このとき参照先存在判定部210が、“参照先が他のセキュアデバイス内に存在するか”を確認する。この動作については後述する。

[0054] また、カード間IF実行部208は、アドレス解決中の参照先存在判定部210からの依頼や、アプリ307の実行時にアプリ実行部206からの依頼を受けて、他のセキュアデバイス102との通信を行う。

[0055] 図4は、上記のように、他のセキュアデバイス102の構成を示したブロック図である。

[0056] 他のセキュアデバイス102には、他のアプリ204が明示的にアクセスするためのインタフェースを提供するアプリ(以下、サーバアプリ401と称する。一方インタフェースを利用するアプリをクライアントアプリ307と称する(図2におけるダウンロード後のアプリ307)。)がアプリ格納部402に格納され、アプリ実行部403により実行される。

[0057] 図5は、上記のように、読み書き装置103の構成を示したブロック図である。

[0058] 読み書き装置103は、セキュアデバイス101、他のセキュアデバイス102等の複数

のセキュアデバイスと通信が可能であり、通信を実施するセキュアデバイス101、他のセキュアデバイス102を個別に認識する。

[0059] 読み書き装置103は、上記動作を行うために、セキュアデバイス101に送信するデータを誤って別のセキュアデバイス102に送信すること(あるいはその逆)を防止する排他制御通信部501と、セキュアデバイス101内のアプリ307, 他のセキュアデバイス内のサーバアプリ401にコマンドを送り、レスポンスを処理するアプリ制御部502と、から構成される。

[0060] 例えば、複数スロットを設け、各スロットに挿入したセキュアデバイスに接触して通信する読み書き装置や、電波の届く範囲内にある複数のセキュアデバイスに対して非接触通信を行う読み書き装置などが知られている。

[0061] また、アプリ制御部502は、1)すべてが読み書き装置103内にある場合と、2)その一部が読み書き装置103内に、残りがネットワークを介した別の装置内にある場合と、があるが、いずれの場合も本文中において同様に扱う。

[0062] 以下、本実施例では上記構成要素を有する、セキュアデバイス101、他のセキュアデバイス102、読み書き装置103とのデータのやり取りについて説明する。

[0063] なお、本実施例を含む本願では、データ等のやり取りは、明示しない限り、基本的に制御部(図示なし)が行うこととする。

[0064] 本実施例の特徴部分を説明する前に、まず、参照先のアプリが同じセキュアデバイス内に存在する場合のアプリのダウンロードについて図7、図28を用いて説明する。

[0065] 読み書き装置103から送信されたアプリのダウンロード用のコマンドをセキュアデバイス101中のダウンロード管理部201が受信し、処理結果をレスポンスとして読み書き装置103に送信する。基本的に、アプリのダウンロードはこれ を繰り返すことによって実行される。

[0066] (STEP1(S2801))

読み書き装置103から送信されたダウンロード用のコマンドで指定されたサイズに応じて、セキュアデバイス101では、アプリコード用データ領域302とアドレス計算用データ領域303とアプリデータ領域304とを確保し、上記ダウンロード用のコマンドからアプリコード用データ305とアドレス計算用データ306を抽出してそれぞれの領域

に格納する。

[0067] (STEP2(S2802))

セキュアデバイス101では、アプリコード用データ305とアドレス計算用データ306とが抽出された後、ダウンロード管理部201からの依頼を受けてアドレス計算部205がアドレス解決を実行する。

[0068] アドレス計算部205はアプリコード用データ305の先頭からバイト単位で解釈していく。例えば、図6に示すように アドレス計算部205は、他のアプリ204が提供するIF(インターフェイス)を経由して関数を呼び出す命令コードである「invokeinterface」を読み出したときに「invokeinterface」に応じた処理をおこなう。

[0069] 上記「応じた処理」とは、「invokeinterface」といった種々の命令コードが定義されており、それぞれの処理内容が異なっていることを意味する。

[0070] 「invokeinterface」の直後の1バイトは、呼び出す引数を制御するものであり、その後の2バイト“0002”がアドレス計算用データ306のインデックスである。アドレス計算部205は、このアドレス計算用データ306のインデックスに基づいて該当するアドレス計算用データ306を参照する。

[0071] 図6に示す、参照先“01800000”は、パッケージ、クラストークン、メソッドの識別番号などから構成されており、アドレス計算部205はこれらを用いて呼び出す関数の先頭位置を示すアドレスを抽出し、インデックス“0002”を呼び出し先のアドレス“a000”に変換する。

[0072] (STEP3(S2803))

セキュアデバイス101では、アドレス計算部205が、アプリコード用データ305のすべてを解釈した後、アドレス計算が完了した旨を、ダウンロード管理部201に通知する。

[0073] (STEP4(S2804))

セキュアデバイス101では、ダウンロード管理部201は不要になったアドレス計算用データを格納した領域303を開放する。ただし、カードのメモリリソースを鑑みると本ステップは非常に有効であるが、オプションとしてもよい。

[0074] (STEP5(S2805))

ダウンロード管理部201は、読み書き装置103から「アプリの初期化」を依頼するコマンドを受信したときに、アプリを初期化する。

[0075] 「アプリの初期化」とは、アプリのインスタンスを生成し、オブジェクトに初期値を設定することである。これらデータはアプリデータ309としてアプリデータ領域304に格納される。

[0076] 以後、読み書き装置103からのコマンドに対してアプリ実行部206によるアプリ307、204の選択や実行が可能となる。

[0077] 以上、アドレス解決が成功する場合の処理について説明した。

[0078] 次に、参照するアプリがカード内に存在しないためにアドレス解決ができない場合について図7を用いて説明する。

[0079] 図7において前述の(STEP2(S2802))と同様に他のアプリの関数呼び出しをアドレス解決する場合に、アドレス計算部205は参照先がセキュアデバイス101内に存在しないことを認識する。

[0080] アドレス計算部205は参照先存在判定部210に“他のセキュアデバイス102内に該当する参照先が存在するかどうか”を確認するよう依頼する。

[0081] そのときに、アドレス計算部205は、参照先存在判定部210に対して、参照先アプリの識別子Application Identification Data(AID)やメソッドIDや引数の数などを含む存在確認情報を渡す。

[0082] カード間IF実行部208は、参照先存在判定部210から存在確認情報を渡され、読み書き装置103を介して 他のセキュアデバイス102に、存在確認情報を転送する。

[0083] 他のセキュアデバイス102は、存在確認情報で示される関数が存在することを確認したのち、使用許可もしくは使用拒絶を意味する許可確認情報をセキュアデバイス101に転送する。

[0084] セキュアデバイス101のカード間IF実行部208が受信した、許可確認情報は参照先存在判定部210に渡され、参照先存在判定部210により許可確認情報が確認された結果、他のセキュアデバイス102のサーバアプリ401の使用が許可された場合に許可コードの発行を許可コード発行部207に依頼する。また使用が拒絶された場合は、許可コード発行部207は、エラーを発行する。

[0085] エラーが発行された場合は、ダウンロード管理部201を通じて読み書き装置103に“参照先がないためダウンロードに失敗した”旨を意味するSWが返却される。

[0086] 許可コードの長さは本来アドレスとして更新する場合と同じ長さであり、例えばアドレスが2バイトで示される場合は許可コードも2バイトとする。

[0087] また、許可コードは、アプリの配置が許可されないアドレス領域を示す情報と、許可コード管理部で管理するテーブルのインデックスと、から構成される。

[0088] 図8はセキュアデバイス101内のメモリ空間を示す。

[0089] メモリ空間801の中でアプリの配置に許可されるメモリ空間802が0000h～EFFFhで示されるとき、アプリに許可されない領域(例えばシステム領域)803はF000h～FFFFhである。

[0090] 例えば、許可コードとして、アプリに許可されない領域803の範囲内であって、かつ後半の1バイトによってテーブルのインデックス“2”を示すFF02hが付与される。この場合には、許可コード発行後に、許可コード管理部209で管理する許可コードテーブル901のインデックス“2”の行に参照先アプリ(サーバアプリ401)の識別子、メソッドID、引数の数など、が格納される。

[0091] 次に、許可コードが付与されたアプリ(クライアントアプリ307)の実行動作について図10、図11を用いて説明する。

[0092] 図10は動作フロー、図11はセキュアデバイス101、他のセキュアデバイス102と読み書き装置103との間で通信するコマンドおよびレスポンスの一例を示したものである。

[0093] 以下、図10の動作フローを用いて、セキュアデバイス101、他のセキュアデバイス102、読み書き装置103の動作について説明する。

[0094] 図33は、読み書き装置103が扱うデータの構造を記述した定義書3301を示すものである。なお、定義書3301は、図33aに示すデータ列から図33bの左側に示すデータ列へと続き、さらに同図の右側に示すデータ列へと連続するものである。ここでは、標準を定義するための言語であるASN. 1(Abstract Sytax Notation One)を使用して記述している。さらにC言語においてtypedefキーワードによるデータ型の定義も可能である。

[0095] また本実施の形態における定義書と実装の関係、すなわち定義されたデータ型が、どのようなコマンド／レスポンスに反映されているかを、定義書3301内のコメントに追加している。ここではAPDUの送受信について説明しているが、HTTP(HyperText Transfer Protocol)に基づいたデータの送受信でもよい。

[0096] このように読み書き装置103におけるデータ型の定義、ICカードに登載されるアプリ(クライアントアプリ307、サーバアプリ401)と読み書き装置103とが交換するデータの構造は種々なる態様で実施しうる。以下、実施の形態2から7における同様の説明は省略する。

[0097] (実行動作STEP1(S1001))

既にセキュアデバイス101内のクライアントアプリ307が起動されているものとする(図示は省略)。

[0098] 読み書き装置103から送信されたコマンド1に対応する処理が、セキュアデバイス101のアプリ実行部206により実行される。

[0099] コマンド1は、映像コンテンツ視聴時の許可条件の確認を求めるといった、クライアントアプリが提供する機能ごとに種々の形式が存在しうる。

[0100] アプリ実行部206が、メソッド呼び出しを意味する命令コードを読み出した後、直後のアドレス情報を取り出す。

[0101] アドレス情報により示される領域が、アプリ実行部206によって、「アプリに許可された領域」かどうかが判断され、許可された領域であればアドレス先を呼び出す。

[0102] 許可された領域でなければ、アプリ実行部206は、許可コードであることを認識し、許可コードを許可コード管理部209に渡し、メソッドで利用するパラメータをカード間IF実行部208に渡す。

[0103] 許可コード管理部209は、許可コードに含まれるインデックスを読み出し、許可コードテーブル901に含まれる参照先アプリのAIDを取り出してカード間IF実行部208に渡す。

[0104] カード間IF実行部208は、参照先アプリのAIDをレスポンス1101のデータ部に設定し、カード間IF利用を依頼する旨を意味するデータをレスポンス1101のSWに設定し、このレスポンス1101を読み書き装置103に送信する。

[0105] （実行動作STEP2（S1002））

読み書き装置103の排他制御通信部501が、セキュアデバイス101からのレスポンス1101を受信すると、アプリ制御部502がレスポンスを解析し、セキュアデバイス101がカード間IF利用を希望している旨を認識する。

[0106] アプリ制御部502は、セキュアデバイス101から受け取ったレスポンスがカード間IF利用完了を意味することを認識するまで、セキュアデバイス101から受信したデータ（セキュアデバイス101からのレスポンス）を加工して、他のセキュアデバイス102へのコマンドとして転送し、他のセキュアデバイス102から受信したデータ（他のセキュアデバイス102からのレスポンス）を加工してセキュアデバイス101へのコマンドとして転送する。

[0107] 読み書き装置103は、セキュアデバイス101から、最初にカード間IF利用を希望している旨を含むレスポンスを受け取った場合は、このセキュアデバイス101からのレスポンスを、図11に示す、選択コマンド1102に加工し、他のセキュアデバイス102に送信する。

[0108] この選択コマンド1102によって、他のセキュアデバイス102のアプリ格納部402に格納されているサーバアプリ401が起動する。

[0109] 以下、サーバアプリ401がRemote Method Invocation（RMI）を実装している場合を例に説明する。

[0110] RMIはJava（登録商標）CardTMで定義されている技術であり、読み書き装置側で動くアプリケーションがカードのリモートオブジェクトのメソッドを呼び出すメカニズムである。

[0111] RMIを実装したサーバアプリ401は、読み書き装置103からの選択コマンド1102に対して、INSとオブジェクトIDを含むレスポンス1103を、読み書き装置103へ返却する。

[0112] （実行動作STEP3（S1003））

読み書き装置103は、サーバアプリ401からのレスポンス1103を、図11（a）に示す、共有コマンド1104中のデータ部に設定し、この共有コマンド1104をセキュアデバイス101のカード間IF実行部208に送信する。

[0113] ここで、共有コマンド1104は、セキュアデバイス101がカード間IF利用を希望している場合における、読み書き装置103からセキュアデバイス101に送信されるコマンドに特化したものであり、固有のINSが割り当てられることが望ましい。

[0114] セキュアデバイス101のカード間IF実行部208は、サーバアプリ401から渡されたINSとオブジェクトIDと、許可コードテーブル901に格納されたメソッドIDと、セキュアデバイス101のアプリ実行部206から渡されたパラメータと、を含むリクエストデータを、図11(b)に示す、レスポンス1105のデータ部に設定し、カード間IF利用を依頼する旨をレスポンス1105のSWに設定し、このレスポンス1105を読み書き装置103に返却する。

[0115] (実行動作STEP4(S1004))

読み書き装置103は、カード間IF利用を依頼する旨を解釈し、レスポンス1105のデータ部に格納されたデータをもとに作成したINVOKEコマンド1106をサーバアプリ401に送信する。

[0116] サーバアプリ401は、メソッドIDとパラメータを使用して処理を行い、レスポンス1107を読み書き装置103に返却する。

[0117] (実行動作STEP5(S1005))

読み書き装置103は、INVOKEコマンドに対するサーバアプリの処理結果(例えば、レスポンス1107で図示されるSWのみ)を、図11(b)に示す、共有コマンド1108のデータ部に設定し、この共有コマンド1108を、セキュアデバイス101のカード間IF実行部208に送信する。

[0118] カードIF実行部208は、INVOKEコマンドに対するサーバアプリの処理結果をアプリ実行部206に渡す。

[0119] 以後、アプリ実行部206はINVOKEコマンドに対するサーバアプリの処理結果に対する処理を継続し、コマンド1に対するレスポンス1109を読み書き装置103に送信する。

[0120] コマンド1に対するレスポンス1109には、成功を意味する9000hが含まれており、カード間IF利用を希望している旨を含むSWが含まれていない。

[0121] したがって、読み書き装置103は、カード間IF利用完了を意味することを認識し、

以後のセキュアデバイス101、セキュアデバイス102　間の転送を中止する。

[0122] もしくは、セキュアデバイス101から明示的にカード間IF利用完了を意味するSWを送信してもよい。

[0123] 以上、本実施の形態により、セキュアデバイス内に搭載されたサーバアプリへのアクセスだけでなく、他のセキュアデバイスに搭載されたサーバアプリへのアクセスも可能とした。

[0124] これにより、共通的に利用されるサーバアプリを、所持するセキュアデバイスごとに搭載する必要がなく、メモリリソースの乏しいセキュアデバイスにとって有効である。

[0125] すなわち、2枚目以降のカードにはサーバアプリ分、他のアプリを搭載することができるユーザメリットが発生する。

[0126] さらに、同じセキュアデバイス内に搭載されたサーバアプリを利用する場合と、他のセキュアデバイスに搭載されたサーバアプリを利用する場合のいずれにおいてもクライアントアプリのソースコードは同じとなる。

[0127] これにより、一般的にユーザの利便性が向上し、利用シーンが拡大する場合には開発側の負担も拡大する傾向にあるが、一方で、アプリ開発者にとっては、本方式においてはユーザ利用シーン拡大の影響を受けることなく、従来どおりの開発が可能である。

[0128] また、既に開発済みのアプリのダウンロードや実行にも影響をあたえない(バックワードコンパチビリティが確保されている)。

[0129] そのため、従来のセキュアデバイスから、本実施の形態で提案するセキュアデバイスへの移行が容易となる。

[0130] (実施の形態2)

本実施の形態2は、セキュアデバイスと、他のセキュアデバイスとが連携するときにセキュリティ確保について説明する。

[0131] 本実施の形態2について図12から図14を用いて説明する。

[0132] 図12は、本実施の形態におけるセキュアデバイス1201の構成を示したブロック図である。

[0133] 図12におけるダウンロード管理部201、アプリ格納部202、ダウンロード中アプリ20

3(ダウンロード後はクライアントアプリ307)、ダウンロード済みアプリ204、アドレス計算部205、アプリ実行部206、許可コード発行部207、カード間IF実行部208、許可コード管理部209、参照先存在判定部201は、それぞれ図2におけるものと同様である。

[0134] 図2におけるセキュアデバイス101の構成要素と同一のものは、同一の番号を付してある。

[0135] 実施の形態1で説明した図2におけるセキュアデバイス101と、本実施の形態で説明する図12におけるセキュアデバイス1201と、の差異部分である、セキュリティ管理部1202を中心に、以下、詳述する。

[0136] セキュリティ管理部1202は、本実施の形態1で述べた許可コードを発行する段階や、アプリ実行中に他のセキュアデバイスを参照する段階での「セキュリティを確保」する。

[0137] ここで、「セキュリティを確保」とは、自身(セキュアデバイス)が通信相手(他のセキュアデバイス)を認証する外部認証、通信相手が自身を認証する内部認証(以下、外部認証と内部認証を合わせて相互認証と称する。)、通信するデータの秘匿、改ざん検知等を実施することであり、実現のために暗号技術が用いられる。

[0138] 本実施の形態では、“サーバアプリは、このサーバアプリを利用するための事前登録がされていない不特定多数のクライアントアプリからも利用される可能性がある。”ことを前提にして、上記「セキュリティの確保」について、公開鍵暗号技術を用いて説明する。

[0139] 公開鍵暗号技術は、一般的に処理速度の点で共通鍵暗号技術に劣る。

[0140] したがって、公開鍵暗号技術を利用して外部認証や内部認証と、セッション鍵(もしくはセッション鍵の種)の共有と、を行い、セッション鍵を使った共通鍵暗号技術により通信データの暗復号や改ざん検知が行われる。

[0141] 本実施の形態に、上記公開鍵、セッション鍵暗号化技術を適用すると、以下の3つの「セキュリティの確保」の方法が考えられる。

[0142] 方法1:許可コードを発行する段階で外部認証、内部認証を実施して、セッション鍵を共有し、アプリ実行中に他のセキュアデバイスを参照する際、セッション鍵を利用す

る。

[0143] 方法2:許可コードを発行する段階で外部認証、内部認証を実施して、セッション鍵の種を共有し、アプリ実行中にセキュアデバイス、他のセキュアデバイスが互いに同じアルゴリズムでセッション鍵の種からセッション鍵を作成し、セッション鍵を利用する。

[0144] 方法3:許可コードを発行する段階も、アプリ実行中に他のセキュアデバイスを参照する段階も、外部認証、内部認証を実施し、セッション鍵を共有する。

[0145] 処理をするタイミングや、通信するデータに若干の差があるものの、基本的な考え方はいずれも同じである。

[0146] したがって、本実施の形態では、上記3つの方法の中で、例として、方法1について説明する。

[0147] 図13は、本実施の形態における他のセキュアデバイス1301の構成を示したブロック図である。

[0148] 図13におけるアプリ実行部206、アプリ格納部202、サーバアプリ401は、それぞれ図4におけるものと同様である。

[0149] 図4における他のセキュアデバイス102と異なる構成は、カード間IF実行部1302と、セキュリティ管理部1303である。

[0150] カード間IF実行部1302は、セキュアデバイス1301が許可コードを発行する段階や、アプリ実行中に他のセキュアデバイスを参照する段階の通信を実行する。

[0151] セキュリティ管理部1303は、セキュリティ管理部1202と同様の機能を有し、セキュリティを確保する。

[0152] 以下、上記構成を有する、セキュアデバイス1201と他のセキュアデバイス1301との動作について説明する。

[0153] 最初に、許可コードを発行する段階について説明する。

[0154] 実施の形態1で述べた(STEP2)と同様に他のアプリの関数呼び出しをアドレス解決する場合に、セキュアデバイス1201のアドレス計算部205は、参照先がカード内に存在しないことを認識する。

[0155] 次に、アドレス計算部205は参照先存在判定部210に“他のセキュアデバイス102

内に該当する参照先が存在するかどうか”を確認するよう依頼する。

[0156] 以下の動作フローを図29に示す。

[0157] （セキュリティ確保ステップ1（S2901））

セキュアデバイス1201のカード間IF実行部208は、参照先存在判定部210からの依頼を受けて、セキュリティ管理部1202が有するセキュアデバイス1201のカード公開鍵証明書Aと、セキュリティ管理部1202が生成した乱数aと、を取得する。

[0158] セキュアデバイス1201のカード間IF実行部208は、カード間IF実行部1302にカード公開鍵証明書Aと乱数aとを、他のセキュアデバイス1301に対して送信する。

[0159] （セキュリティ確保ステップ2（S2902））

他のセキュアデバイス1301のカード間IF実行部1302は、セキュリティ管理部1303にカード公開鍵証明書Aと、乱数aと、を渡し、セキュリティ管理部1303において証明書検証を実施し、セキュリティデバイス1201のカードIDと、カード公開鍵Aと、を取得する。

[0160] 次に、他のセキュアデバイス1301のセキュリティ管理部1303は、乱数bを生成し、乱数aをカード秘密鍵Bで暗号化する。

[0161] 続いて乱数bと、暗号化された乱数aと、セキュアデバイス1301のカード公開鍵証明書Bと、をカード間IF実行部1302に渡す。

[0162] 他のセキュアデバイス1301のカード間IF実行部1302は、乱数bと、暗号化された乱数aと、セキュアデバイス1301のカード公開鍵証明書Bと、をセキュアデバイス1201のカード間IF実行部208に送信する。

[0163] （セキュリティ確保ステップ3（S2903））

セキュアデバイス1201のカード間IF実行部208は、乱数bと、暗号化された乱数aと、セキュアデバイス1301のカード公開鍵証明書Bと、をセキュリティ管理部1202に渡し、セキュリティ管理部1202において証明書検証を実施し、他のセキュアデバイスのカードIDと、カード公開鍵Bと、を取得する。

[0164] 次に、セキュリティ管理部1202は、暗号化された乱数aをカード公開鍵Bで復号して、生成した乱数aと一致するかを確かめる（外部認証が完了）。

[0165] 続いて、セキュリティ管理部1202は、乱数bをカード秘密鍵Aで暗号化し、カード間

IF実行部208に渡す。

[0166] カード間IF実行部208は、他のセキュアデバイス1301のカード間IF実行部1302に暗号化された乱数bを送信する。

[0167] (セキュリティ確保ステップ4(S2904))

他のセキュアデバイス1301のカード間IF実行部1302は、暗号化された乱数bをセキュリティ管理部1303に渡し、セキュリティ管理部1303は、暗号化された乱数bを、カード秘密鍵Bで復号して、生成した乱数bと一致するかを確かめる(内部認証が完了)。

[0168] (セキュリティ確保ステップ5(S2905))

次に、他のセキュアデバイス1301のセキュリティ管理部1303は、セッション鍵を作成し、セッション鍵をカード公開鍵Aで暗号化し、暗号化されたセッション鍵をカード間IF実行部1302に渡す。

[0169] カード間IF実行部1302は、暗号化されたセッション鍵を、セキュアデバイス1201のカード間IF実行部208に送信する。

[0170] カード間IF実行部208は、セキュリティ管理部1202に対して、暗号化されたセッション鍵を渡し、セキュリティ管理部1202は、暗号化されたセッション鍵をカード秘密鍵Aで復号化し、セッション鍵を取得する(セッション鍵の共有が完了)。

[0171] この段階で、上記ステップ中に交換や生成によって新たに保持したデータのうち、セキュリティ管理部1202はセッション鍵を、セキュリティ管理部1303はセキュアデバイス1201のカードIDとセッション鍵を、少なくとも保持しておく必要がある。

[0172] 上記セキュリティ確保ステップ5が完了した後、セキュアデバイス1201のカード間IF実行部208には、参照先存在判定部210から参照先アプリの識別子やメソッドIDや引数の数などを含む存在確認情報が渡され、これらの存在確認情報は、カード間IF実行部208が読み書き装置103を介して、他のセキュアデバイス1301に転送する。

[0173] このとき、セキュアデバイス1201のセキュリティ管理部1202においてセッション鍵を用いた送信データの暗号化や改ざん検知用データの付与が実施される。

[0174] 他のセキュアデバイス1301は、存在確認情報で示される関数が存在することを確認したのち、使用許可を意味する情報をセキュアデバイス1201に転送する。

[0175] この場合も、他のセキュアデバイス1301のセキュリティ管理部1303においてセッション鍵を用いた送信データの暗号化や改ざん検知用データの付与が実施される。

[0176] セキュアデバイス1201のカード間IF実行部208が受信した情報は、セキュリティ管理部1202においてセッション鍵を用いた復号化や改ざんチェックが実施された後に参照先存在判定部210に渡される。

[0177] 参照先存在判定部210は、使用が許可された場合に許可コードの発行を許可コード発行部207に依頼する。

[0178] また、使用が拒絶された場合にエラーを発行し、ダウンロード管理部201を通じて読み書き装置103に“参照先がないためダウンロードに失敗した”旨を意味するSWが返却される。

[0179] 次に、許可コードが付与されたクライアントアプリの実行について説明する。基本的に実施の形態1と同様であり、差分は以下のとおりとなる。

[0180] 第一に、セキュアデバイス1201、他のセキュアデバイス1301からのレスポンスはセキュリティ管理部1202、1303によって管理されるセッション鍵を用いて暗号化される。

[0181] 第二に、セキュアデバイス1201、他のセキュアデバイス1301からのレスポンスは暗号化されているため、読み書き装置103がデータを解釈し、必要なデータを抽出して、コマンドを作成することはできない。

[0182] したがって読み書き装置103は、レスポンスのデータ部から必要なデータを抽出し、それをコマンドに組み込んで、セキュアデバイス1201、他のセキュアデバイス1301に送信する必要がある。

[0183] 次に、セキュアデバイス1201、他のセキュアデバイス1301、読み書き装置103によるクライアントアプリ実行中の動作フローについて図10を用いて説明する。

[0184] 以下の説明では、図10におけるセキュアデバイス101をセキュアデバイス1201に、他のセキュアデバイス102を他のセキュアデバイス1301としてそのまま適用するものとする。

[0185] また、前提として、既にセキュアデバイス1201内のクライアントアプリ307が起動されているものとする。

[0186] （実行動作STEP1（S1001））

読み書き装置103から送信されたコマンド1に対応する処理が、セキュアデバイス1201のアプリ実行部206により実行される。

[0187] アプリ実行部206が、メソッド呼び出しを意味するコードを読み出した後、直後のアドレス情報を取り出す。

[0188] アドレス情報がアプリに許可された領域かどうかを判断し、許可された領域であればアドレス先を呼び出す。

[0189] “否”であれば許可コードであることを認識し、許可コードを許可コード管理部209に渡す。

[0190] 許可コード管理部209は、許可コードに含まれるインデックスを読み出し、テーブル901に含まれる参照先アプリのAIDを取り出して、この参照アプリのAIDをカード間IF実行部208に渡す。

[0191] カード間IF実行部208は、参照先アプリのAIDをレスポンスのデータ部に設定し、カード間IF利用を依頼する旨を意味するデータをレスポンスのSWに設定し、このレスポンスを読み書き装置103に送信する。

[0192] （実行動作STEP2（S1002））

読み書き装置103の排他制御通信部501がレスポンスを受信すると、アプリ制御部502がレスポンスを解析し、セキュアデバイス1201がカード間IF利用を希望している旨を認識する。

[0193] アプリ制御部502は、セキュアデバイス1201から受け取ったデータがカード間IF利用完了を意味することを認識するまで、セキュアデバイス1201から受信したデータ（セキュアデバイス1201からのレスポンス）を加工して、他のセキュアデバイス1301へのコマンドとして、他のセキュアデバイス1301に転送し、他のセキュアデバイス1301から受信したデータ（セキュアデバイス1301からのレスポンス）を加工してセキュアデバイス1201へのコマンドとして、セキュアデバイス1201へ転送する。

[0194] 読み書き装置103は、セキュアデバイス1201から、最初にカード間IF利用を希望している旨を含むレスポンスを受け取った場合は、選択コマンドに加工し、他のセキュアデバイス1301に送信する。

[0195] 選択コマンドによって、他のセキュアデバイス1301のサーバアプリ401が起動する。

[0196] 以下、サーバアプリ401がRemote Method Invocation(RMI)を実装している場合を例に説明する。

[0197] RMIを実装したサーバアプリ401は、選択コマンドに対する応答として、読み書き装置103に、INSとオブジェクトIDを含むレスポンスを返却する。

[0198] (実行動作STEP3(S1003))

読み書き装置103は、サーバアプリ401からのレスポンスを、共有コマンドのデータ部に設定し、この共有コマンドをセキュアデバイス1201のカード間IF実行部208に送信する。

[0199] カード間IF実行部208は、サーバアプリ401から渡されたINSとオブジェクトIDと、を保持する。

[0200] このINSとオブジェクトIDとを保持方法については、特に図示していないが、セキュアデバイス1201の内部にメモリを設けて、保持する形が考え得る。

[0201] 以降、セキュアデバイス1201、他のセキュアデバイス1301からのレスポンスは、それぞれのセキュリティ管理部1202、1303にてセッション鍵を用いて暗号化されている。

[0202] また、相手から受信したデータをセキュリティ管理部1202、1303でセッション鍵を用いて復号した後、それぞれのカードIF実行部208、1302で処理を行う。

[0203] 図14は、読み書き装置103への入力と出力の関係を示したものである。

[0204] 読み書き装置103は、セキュアデバイス1201からのレスポンス1401のデータ部をそのままコマンド1402として他のセキュアデバイス1301に送信する。

[0205] また他のセキュアデバイス1301からのレスポンス1403をそのままコマンド1404のデータ部に設定し、共有コマンド用のヘッダをつけてセキュアデバイス1201に送信する。

[0206] セキュアデバイス1201のカード間IF実行部208は、他のセキュアデバイス1301のサーバアプリ401から渡されたINSとオブジェクトIDと、セキュアデバイス1201のアプリ実行部206が指定したメソッドIDとアプリ実行部から渡されたパラメータを含むリ

クエストデータをレスポンスのデータ部に設定し、カード間IF利用を依頼する旨をSWに設定し、読み書き装置103に返却する。

[0207] (実行動作STEP4(S1004))

読み書き装置103は、セキュアデバイス1201からのカード間IF利用を依頼する旨を解釈し、レスポンスのデータ部に格納されたデータ(暗号化ずみのINVOKEコマンド)を抽出し、それをコマンドとして、他のセキュアデバイス1301のサーバアプリ401に送信する。

[0208] サーバアプリ401は、INVOKEコマンドで指定されたメソッドIDとパラメータを使用して処理を行い、処理結果を読み書き装置103に返却する。

[0209] (実行動作STEP5(S1005))

読み書き装置103は上記処理結果をデータ部に設定した共有コマンドを、セキュアデバイス1201のカード間IF実行部208に送信する。

[0210] カードIF実行部208は、結果をアプリ実行部206に渡す。

[0211] 以後、アプリ実行部206は結果に対する処理を継続し、コマンド1に対するレスポンスを読み書き装置103に送信する。

[0212] コマンド1に対するレスポンスには、一般的にカード間IF利用を希望している旨を含むSWが含まれない。

[0213] したがって、読み書き装置103は、カード間IF利用完了を意味することを認識し、以後のセキュアデバイス1201、他のセキュアデバイス1301間の転送を中止する。

[0214] もしくは、セキュアデバイス1201から明示的にカード間IF利用完了を意味するSWを送信してもよい。

[0215] 本実施の形態2では、セキュリティ管理部1202、1303によって、参照先の存在確認や、アプリ実行中の他セキュアデバイスへの参照においてセキュリティを確保するシステムについて説明した。

[0216] 上記構成を用いることで、セキュアデバイスの成りすまし防止や、セキュアデバイス間で交換されるデータの盗聴防止、改ざん検知が可能となる。

[0217] (実施の形態3)

本実施の形態3は、セキュアデバイスと、他のセキュアデバイスの所有者が一致す

ることを確認するシステム(その1)について説明する。

[0218] 本実施の形態3について図12、図13、図15、図16を用いて説明する。

[0219] 図12は、本実施の形態におけるセキュアデバイス1201の構成を示したブロック図であり、実施の形態2で説明したものと同様である。

[0220] 図13は、本実施の形態における他のセキュアデバイス1301の構成を示したブロック図であり、実施の形態2で説明したものと同様である。

[0221] 図15は、本実施の形態における読み書き装置1501の構成を示したブロック図である。

[0222] 図15における排他制御部501、アプリ制御部502は、それぞれ図5における排他制御部501、アプリ制御部502と同様である。

[0223] 本実施の形態の特徴は、読み書き装置にあり、上記実施の形態1、実施の形態2との差異は、所有者管理部1502と、ダウンロード条件判定部1503とを有する点である。

[0224] 所有者管理部1502は、セキュアデバイス1201の所有者と、セキュアデバイス1201に設定したカードIDを管理する。

[0225] ダウンロード条件判定部1503は、クライアントアプリのダウンロードに際しての条件を定義したダウンロード条件情報を管理する。

[0226] ユーザがクライアントアプリのダウンロードを希望した場合に、読み書き装置1501は、該当するダウンロード条件情報をアプリ制御部502に渡し、アプリ制御部502はダウンロード条件を満足しているかを確認するための処理を実行する。

[0227] 本実施の形態では、以下で、セキュアデバイス1201と他のセキュアデバイス1301と読み書き装置1501からなるシステムについて説明する。

[0228] 上記実施の形態1、2では、クライアントアプリがアドレス解決をする際、同じセキュアデバイス内にサーバアプリがない場合に、他のセキュアデバイス内に存在するサーバアプリを利用する方法について説明した。

[0229] その際、クライアントアプリを利用してサービスを享受する「クライアントアプリ所有者(＝セキュアデバイスの所有者)」と、サーバアプリを利用してサービスを享受する「サーバアプリ所有者(＝他のセキュアデバイスの所有者)」との同一性等については考

慮していない。

[0230] 本実施の形態では、クライアントアプリ所有者とサーバアプリ所有者に何らかの関係が要求される場合に、要求された関係を確認し、確保する方法について言及する。

[0231] 例えば、サーバアプリがクレジットアプリで、クライアントアプリがコンテンツ購入アプリであると仮定する。

[0232] この場合、クレジットカード業者にとって“どのユーザがどのコンテンツをいくらで購入したか”を正しく把握する必要があるため、クライアントアプリの所有者とサーバアプリの所有者とは同一人物であることが望ましいと考えられる状況が起こりうる。

[0233] 本実施の形態では、このような状況を想定して、クライアントアプリがアドレス解決を実行するときにサーバアプリ所有者とクライアントアプリ所有者の同一性を確認する方法を説明する。

[0234] このサーバアプリ所有者とクライアントアプリ所有者との同一性確保の方法として下記2パターンが考えられる。

[0235] (1)同一性確認を読み書き装置で確認した後に、セキュアデバイスで、クライアントアプリをダウンロードする。

[0236] (2)ダウンロードの段階で、各セキュアデバイスを個人認証する(例:PIN照合)ことで同一性を確認する。

[0237] 実施の形態3では、上記(1)について説明する。

[0238] また、上記(2)については、実施の形態4で説明する。

[0239] 上記(1)について説明するにあたって、以下を前提とする。(図16の“Start”)

[0240] ・読み書き装置1501は、サーバアプリがダウンロードされた他のセキュアデバイス1301と、これからクライアントアプリをダウンロードするセキュアデバイス1201と通信可能な状態になっている。

[0241] ・クライアントアプリをダウンロードする条件として、“他のセキュアデバイスの参照が可能でその場合にサーバアプリ所有者とクライアントアプリ所有者が同一であること”と定義されている。

[0242] ・読み書き装置1501はセキュアデバイス1201内にサーバアプリが存在しないことを把握済みである。

[0243] 前提の実現は一般的な技術で可能であり、図では省略する。以下、図16に示すフロー図を用いて、上記(1)に関するシステムの動作を説明する。

[0244] 最初に、図16に示されるように、読み書き装置1501はSELECTコマンドを他のセキュアデバイス1301に送信し、サーバアプリが、他のセキュアデバイス内に存在するか否かを確認する。

[0245] 次に、GETDATAコマンドにより他のセキュアデバイス1301に付与されたカードIDを取得する。

[0246] ここで、「カードID」とはセキュアデバイスを一意に特定するための情報で、例えばカード発行者に一意となるIssuer Identification Numberとカード発行者が発行したカードを一意に特定するCard Identification Numberとから成る。

[0247] 同様に、読み書き装置1501は、セキュアデバイス1201からもカードIDを取得する。

[0248] 読み書き装置1501のアプリ制御部502は、所有者管理部1502に依頼して、上記のように取得した、セキュアデバイス1201と他のセキュアデバイス1301それぞれのカードIDで関連付けられたセキュアデバイスの所有者が一致することを確かめる。

[0249] 所有者管理部1502が、セキュアデバイス1201の所有者と他のセキュアデバイス1301の所有者とが一致しているか否かを判定した結果、両セキュアデバイスの所有者が一致している場合、読み書き装置1501は、クライアントアプリのダウンロードを開始する。

[0250] ここで少なくともセキュアデバイス1201のアドレス計算部205がアドレス解決を実施する前に、読み書き装置1501は他のセキュアデバイス1301のカードIDをセキュアデバイス1201に送信する必要がある。

[0251] セキュアデバイス1201は、カードIDを許可コード管理部209に保存しておく。

[0252] セキュアデバイス1201がアドレス解決を実施するときに、自己のセキュアデバイス内である、セキュアデバイス1201内にサーバアプリがないことを認識し、他のセキュアデバイス1301に存在するかを確かめる。

[0253] ここでは、実施の形態2で述べたセキュリティ確保ステップ1からステップ5までを同様に実施する。

[0254] ただし、この途中で他のセキュアデバイス1301のカード公開鍵証明書から取得したカードIDと、許可コード管理部209に保存されたカードIDとが一致しているかを確かめる必要がある。

[0255] カードIDと所有者の一致は既に読み書き装置1501で確認されているため、省略することも可能である。

[0256] ただし、カードIDを送信した後に他のセキュアデバイス1301がすりかえられる脅威に対して、事前の確認に加えてアドレス解決中に再確認することでセキュリティレベルが向上する。

[0257] 本実施の形態3では、サーバアプリとクライアントアプリがそれぞれ異なるセキュアデバイスに搭載されている場合に、サーバアプリ所有者とクライアント所有者の同一性を確保する方法について述べた。

[0258] 同一性を確認することによって、なりすましによるクライアントアプリのダウンロードを防止することができる。

[0259] 本手法は、所有者の同一性だけでなく、クライアントアプリ所有者が、サーバアプリ所有者の家族か、同じグループに所属しているか、などにも適用できる。

[0260] 以上により、サーバアプリ所有者とクライアントアプリ所有者の関係を柔軟に設定、確認可能なシステムを提供することができる。

[0261] (実施の形態4)

本実施の形態4は、セキュアデバイスと、他のセキュアデバイスの所有者が一致することを確認するシステム(その2)について説明する。

[0262] 本実施の形態4について図12、図13、図17、図18を用いて説明する。

[0263] 図12は、本実施の形態におけるセキュアデバイス1201の構成を示したブロック図であり、実施の形態2で説明したものと同様である。

[0264] 図13は、本実施の形態における他のセキュアデバイス1301の構成を示したブロック図であり、実施の形態2で説明したものと同様である。

[0265] 図17は、本実施の形態における読み書き装置1701の構成を示したブロック図である。

[0266] 図17における排他制御部501、アプリ制御部502は、それぞれ図5における排他

制御部501、アプリ制御部502と同様である。

[0267] また所有者管理部1502は、図15における所有者管理部1502と同様である。

[0268] 上記実施の形態3との差異は、所有者情報確認入力部1702を有する点である。

[0269] 所有者情報確認入力部1702は、セキュアデバイス所有者の正当性を判定するための情報(例:PIN)を入力するためのものである。

[0270] 所有者情報確認入力部1702の例として、入力画面が考えられる。

[0271] ただし、本画面は、セキュアデバイス1201からPIN入力画面を提供するように依頼する旨のレスポンスが返却された後、アプリ制御部502がその旨を解釈し、所有者確認情報入力部1702に画面出力を依頼した場合のみ表示される。

[0272] 本実施の形態では、セキュアデバイス1201と他のセキュアデバイス1301と読み書き装置1701からなるシステムについて説明する。

[0273] 実施の形態1、2では、セキュアデバイス内のクライアントアプリがアドレス解決をする際に、自己のセキュアデバイス内にサーバアプリがない場合には、他のセキュアデバイス内に存在するサーバアプリを利用するシステムについて説明した。

[0274] その際、クライアントアプリを利用してサービスを享受する「クライアントアプリ所有者(=セキュアデバイスの所有者)」と、サーバアプリを利用してサービスを享受する「サーバアプリ所有者(=他のセキュアデバイスの所有者)」との同一性等については考慮していない。

[0275] 本実施の形態では、上記実施の形態3と同様、クライアントアプリ所有者とサーバアプリ所有者に何らかの関係が要求される場合に、要求された関係を確認し、確保する方法について言及する。

[0276] 例えば、サーバアプリがクレジットアプリで、クライアントアプリがコンテンツ購入アプリであると仮定する。この場合、クレジットカード業者にとって“どのユーザがどのコンテンツをいくらで購入したか”を正しく把握する必要があるため、クライアントアプリの所有者とサーバアプリの所有者とは同一人物であることが望ましいと考えられる状況が起こりうる。

[0277] したがって、このような状況を想定して、本実施の形態ではクライアントアプリがアドレス解決を実行するときにサーバアプリ所有者とクライアントアプリ所有者の同一性を

確認する方法を、図18を用いて説明する。

[0278] 本実施の形態に記載の発明を説明するにあたって、まずは前提を述べる。(図18の“Start”)

[0279] ・読み書き装置は、サーバアプリがダウンロードされた他のセキュアデバイスと、これからクライアントアプリをダウンロードするセキュアデバイスと通信可能な状態になっている。

[0280] ・クライアントアプリをダウンロードする条件として、“他のセキュアデバイスの参照が可能でその場合にサーバアプリ所有者とクライアントアプリ所有者が同一であること”と定義されている。

[0281] ・読み書き装置はセキュアデバイス内にサーバアプリが存在しないことを把握済みである。

[0282] 前提の実現は一般的な技術で実現可能であり、図では省略する。

[0283] 以下、図18に示すフロー図を用いて、本実施の形態に記載の発明に関するシステムの動作を説明する。

[0284] 最初に、読み書き装置1701はダウンロード条件をセキュアデバイス1201に送信する。

[0285] ダウンロード管理部1201はダウンロード条件を受信し、セキュリティ管理部1202に渡し、セキュリティ管理部1202で保存する。

[0286] 次にクライアントアプリのダウンロードを開始する。

[0287] セキュアデバイス1201がアドレス解決を実施するときに、自己のセキュアデバイス内である、セキュアデバイス1201内にサーバアプリがないことを認識し、他のセキュアデバイス1301に、サーバアプリが存在するかを確かめる。

[0288] ここでは、実施の形態2で述べたセキュリティ確保ステップ1からステップ5までを同様に実施する。

[0289] ただし、この途中で、セキュアデバイス1201のカード間IF実行部208はセキュリティ管理部1202に保存されたダウンロード条件を満足しているかを確認するための処理を読み書き装置1701と連携して実行する。

[0290] カード間IF実行部208は、ダウンロード条件に応じて条件を満足しているかを確認

するための処理を切り替えることができる。

[0291] 本実施の形態における“他のセキュアデバイスの参照が可能でその場合にサーバアプリ所有者とクライアントアプリ所有者が同一であること”がダウンロード条件である場合には、PINの入力を依頼する旨のレスポンスを読み書き装置1701に送信する。

[0292] 読み書き装置1701は、排他制御通信部501においてレスポンスを受信し、レスポンスをアプリ制御部502に渡す。

[0293] アプリ制御部502は、PINの入力を依頼されていることを解釈し、所有者確認情報入力部1702に画面を表示するように依頼する。

[0294] 次に所有者情報入力部1702によって表示された画面に所有者がPINを入力する。

[0295] 入力されたPINは、排他制御通信部501から他のセキュアデバイス1301に送信され、カード間IF実行部1302が受信する。

[0296] カード間IF実行部1302からの依頼を受けてセキュリティ管理部1303においてPIN照合を実施し、その結果を、読み書き装置1701を経由してセキュアデバイス1201に送信する。

[0297] このPIN照合は、必ずしも、セキュリティ管理部1303で行う必要はなく、例えば、PIN照合部などの構成を設けても良い。

[0298] セキュアデバイス1201のカード間IF実行部208は、結果が“OK”であった場合に、他のセキュアデバイスの所有者が、ダウンロード対象のセキュアデバイスの所有者と同一であると判定し、アドレス解決を継続する。

[0299] ここで、他のセキュアデバイスの所有者が、セキュアデバイスの所有者と異なるにもかかわらず、それぞれの所有者が連携することで他のセキュアデバイスのPIN照合に成功する脅威が存在する。

[0300] そこで、ダウンロード終了後に、他のセキュアデバイスのカード証明書をセキュアデバイスから読み書き装置に送信し、読み書き装置で所有者の同一性をチェックする。この結果、なりすましを検知できる。

[0301] 以上より、本実施の形態4では、サーバアプリとクライアントアプリがそれぞれ異なるセキュアデバイスに搭載されている場合に、サーバアプリ所有者とクライアント所有者

の同一性を確保する方法について述べた。

[0302] 特に、所有者情報データベースから切り離された環境でダウンロードを実行する場合に、本手法は最適である。

[0303] (実施の形態5)

本実施の形態5は、サーバアプリが搭載されたセキュアデバイスのライフサイクルに連動したクライアントアプリの利用制御に関するものである。

[0304] 本実施の形態5について図2、図4、図5、図19、図20を用いて説明する。

[0305] 図2は、本実施の形態におけるセキュアデバイス101の構成を示したブロック図であり、各構成要素は実施の形態1で説明したものと同様である。

[0306] 図4は、本実施の形態における他のセキュアデバイス102の構成を示したブロック図であり、各構成要素は実施の形態1で説明したものと同様である。

[0307] 図5は、本実施の形態における読み書き装置103の構成を示したブロック図であり、各構成要素は実施の形態1で説明したものと同様である。

[0308] 図20は、許可コード管理部209に含まれる許可コードテーブル2001であり、図9におけるインデックス、参照先アプリの識別子、メソッドID、引数の数に加えて、クライアントアプリの識別子が含まれる。

[0309] 本実施の形態では、このクライアントアプリの識別子が含まれる点が、他の実施の形態に記載の発明と異なる点である。

[0310] 本実施の形態では、セキュアデバイス101と他のセキュアデバイス102と読み書き装置103からなるシステムについて説明する。

[0311] サーバアプリとクライアントアプリが同一セキュアデバイスに搭載されている場合には、両アプリのライフサイクルはセキュアデバイスのライフサイクルに連動する。

[0312] すなわち、セキュアデバイスが利用可能な状態であれば両アプリは利用可能であり、セキュアデバイスが一時停止や廃棄状態であれば両アプリも利用不可となる。

[0313] ここで、これまでの実施の形態で述べた、サーバアプリとクライアントアプリが別々のセキュアデバイスに搭載されている場合について、セキュアデバイスが一時停止、廃棄状態のときに、どのようになるのかを述べる。

[0314] サーバアプリが搭載されている他のセキュアデバイス(以下、サーバ側デバイス)が

利用可能で、クライアントアプリが搭載されているセキュアデバイス(以下、クライアント側デバイス)が利用不可の場合は、そもそもクライアント側が実行できないので問題ない。

[0315] 一方でサーバ側デバイスが利用不可でクライアント側デバイスが利用可能な場合、従来と異なる処理が必要である。

[0316] すなわち、“サーバ側デバイスが一時停止であるためクライアントアプリは利用できません。”という内容を読み書き装置に返却する必要がある。

[0317] また、返却するタイミングはできるだけ早いことが望ましい。

[0318] したがって、本実施の形態では他のセキュアデバイスに登録されたサーバアプリを参照するクライアントアプリを実行するときに他のセキュアデバイスのライフサイクルを確認する処理について図19を用いて説明する。

[0319] 読み書き装置103はクライアントアプリを選択するSELECTコマンドを、セキュアデバイス101に送信する。

[0320] セキュアデバイス101のアプリ実行部206が、SELECTコマンドを受信し、データ部に設定されたクライアントアプリのAIDをカード間IF実行部208に渡す。

[0321] カード間IF実行部208は、許可コード管理部209に格納された許可コードテーブル2001を参照する。

[0322] 許可コードテーブル2001中に、該当するクライアントアプリのAIDが存在しない場合は、アプリ実行部206にその旨を通知し、アプリ実行部206は通常のSELECTコマンド処理を実行する。

[0323] 該当するクライアントアプリのAIDが存在する場合は、許可コードテーブル2001から他のセキュアデバイスに搭載されたサーバアプリのAIDを抽出し、サーバアプリのAIDと、“SELECTコマンドを他のセキュアデバイスに送信することを依頼する”旨のデータとからなるレスポンスを、読み書き装置103に返却する。

[0324] 読み書き装置103は、セキュアデバイス101のカード間IF実行部208から受信したデータからSELECTコマンドを作成し、他のセキュアデバイス102に送信する。

[0325] 次に、他のセキュアデバイス102からのレスポンスをセキュアデバイス101に渡す。

[0326] セキュアデバイス101のカード間IF実行部208は、レスポンスを解析し、他のセキュ

アデバイス102の利用可能状態を把握する。

[0327] 他のセキュアデバイス102が利用可能な場合は、アプリ実行部208にその旨を伝え、アプリ実行部208は、通常のSELECTコマンド処理を実行する。

[0328] 他のセキュアデバイス102が利用不可な場合は、アプリ実行部208にその旨を伝え、アプリ実行部は、“他のセキュアデバイスが利用不可であるためクライアントアプリは使用できない”旨を示すSWを設定したレスポンスを読み書き装置103に返却する。

[0329] 本実施の形態5では、サーバアプリとクライアントアプリがそれぞれ異なるセキュアデバイスに搭載されている場合に起こりうる、サーバアプリが搭載されているセキュアデバイスが一時停止もしくは廃棄状態にあるときのクライアントアプリが搭載されているセキュアデバイスの振舞について述べた。

[0330] クライアントアプリのSELECT時にサーバアプリの状態を確認することで、クライアントアプリの処理実行中にサーバアプリの状態を確認する場合に比べてカード内や読み書き装置側におけるリカバリ処理のような余分な処理をなくすことができる。

[0331] また、サーバアプリの機能を利用しない範囲に限ってクライアントアプリを実行するように切り替えることもできる。

[0332] 以上、従来のサーバアプリとクライアントアプリが揃って利用可能あるいは利用不可であった従来技術に対してクライアントアプリを実行するサーバ側で、サーバアプリの状態に応じた処理を選択可能となり、柔軟なサービス提供が実現できる。

[0333] (実施の形態6)

実施の形態6は、同一カード内にサーバアプリが存在しない場合のクライアントアプリの条件付きダウンロード方法と、条件のチェック方法に関する発明である。

[0334] 例えば、サーバアプリが搭載されたセキュアデバイスを携帯するのを忘れた場合においても、実際にクライアントアプリを使うまでにサーバアプリを参照することを条件に、クライアントアプリのダウンロードを許可するシステムに適用できる。

[0335] 本実施の形態6について図2、図4、図5、図9、図10、図21、図22、図23を用いて説明する。

[0336] 図2は、本実施の形態におけるセキュアデバイス101の構成を示したブロック図であり、各構成要素は実施の形態1で説明したものと同様である。

[0337] 図4は、本実施の形態における他のセキュアデバイス102の構成を示したブロック図であり、各構成要素は実施の形態1で説明したものと同様である。

[0338] 図5は、本実施の形態における読み書き装置103の構成を示したブロック図であり、各構成要素は実施の形態1で説明したものと同様である。

[0339] 図9は、許可コードテーブル901の一例を示したものであり、各構成要素は実施の形態1で説明したものと同様である。

[0340] 図22、図23に示す、許可コード又は仮許可コード等が本実施例の特徴となりものである。

[0341] 図22は、許可コード発行部207が許可コードを発行する際のルールを定義した指示書である。

[0342] 図23は、アプリ実行部206が管理する仮許可コード管理テーブル2301の一例を示すものである。仮許可コード管理テーブル2301は、インデックス、クライアントアプリの識別子、サーバアプリの識別子、アドレス計算用データからなる。

[0343] 本実施の形態では、セキュアデバイス101と他のセキュアデバイス102と読み書き装置103からなるシステムについて説明する。

[0344] 本実施の形態1では、サーバアプリのIFを利用するクライアントアプリのダウンロードにおいて、他のセキュアデバイスに搭載されたサーバアプリを参照可能な場合に許可コードを発行する方法について説明した。

[0345] これに対して、本実施の形態では、種々の許可コードの発行と、発行した許可コードの活用方法について図21を用いて説明する。

[0346] 事前に、許可コード発行部207には、読み書き装置103から送信されたアプリの属性を設定するコマンドにより、「アプリの種類」や「仮許可コード発行許可」などが設定されている。

[0347] ここで「アプリの種類」とは、例えば、アプリが利用回数や利用期間などを制限した一時的なアプリであったり、制限を課さない正式なアプリであったり、アプリに対する様々な制限で分類されたものである。

[0348] そのため、「アプリの種類」は、アプリがどのような制限が課されたものであるのかを識別するために用いられる。

[0349] 「仮許可コード発行許可」とは、アドレス解決時に参照先存在判定部210がサーバアプリへの参照を確認した際に、参照先がないにもかかわらずダウンロードエラーとして扱わずに仮許可コードを発行することを許可するものでありアプリ実行部206にとっては、仮許可コードの解釈において「まだ参照先を確かめてない状態であることを判別できる」かつ「いつまでその状態が許容されるかを判別できる」必要がある。

[0350] 例えば、サーバアプリが搭載されたセキュアデバイスを所持しない(たとえば、携帯するのを忘れた等)場合でも仮にクライアントアプリのダウンロードを実行し、その後サーバアプリが搭載されたセキュアデバイスを確認し許可コードを発行する場面を想定される。

[0351] 本実施の形態では、この想定される状況でのシステムの動作について説明する。

[0352] 図21において「許可コードを発行する」までのフローは実施の形態1と同様であり、その後の処理が、本実施の形態において記載する発明の特徴部分となる。

[0353] (制限付き許可コードの発行)

ここでは、制限付き許可コードの発行について説明する。

[0354] 事前に、参照先存在判定部201には、読み書き装置103から送信されたアプリの属性を設定するコマンドにより、「アプリの種類」が設定されている。

[0355] ここでは、利用回数の上限を3回とする一時的なアプリとして設定されていると仮定する。

[0356] アプリのダウンロード時にアドレス解決を開始し、他のセキュアデバイス102が使用許可を意味する情報をセキュアデバイス101に転送するまでは実施の形態1と同様である。

[0357] 参照先存在判定部210はカード間IF実行部208が受信した情報を解析することで“OK”と判定した後、許可コード発行部207に「アプリの種類」を用いた制限付き許可コードの発行を依頼する。

[0358] 許可コード発行部207は、アプリの種類が一時的なアプリであること、利用回数が3回であることから指示書2201にしたがったFCB1hを制限付き許可コードとして発行する。

[0359] 指示書2201によれば、アプリの配置に許可されないアドレス領域を示す情報のう

ちFC～FDhが先頭1バイトに割り当てられ、次の4ビットで制限の種類や内容が表現され、最後の4ビットで許可コードテーブル901のインデックスが付与されることになる。

[0360] また、制限付き許可コード発行後に、許可コード管理部209で管理する許可コードテーブル901には、参照先アプリ(サーバアプリ)の識別子、メソッドID、引数の数などが格納される。

[0361] 次に、制限付き許可コードが付与されたクライアントアプリの実行中の動作について図10を利用して説明する。

[0362] ここでは実施の形態1と差異のあるSTEP10－1についてのみ詳述する。

[0363] (STEP10－1)

既にセキュアデバイス101内のクライアントアプリ307が起動されているものとする。

[0364] 読み書き装置103から送信されたコマンド1に対応する処理が、セキュアデバイス101のアプリ実行部206により実行される。

[0365] アプリ実行部206が、メソッド呼び出しを意味する命令コードを読み出した後、直後のアドレス情報を取り出す。

[0366] アドレス情報がアプリに許可された領域かどうかを判断し、許可された領域であればアドレス先を呼び出す。

[0367] “否”であれば許可コードであることを認識し、さらに許可コードの種類を判別する。

[0368] 判別した結果が制限付き許可コードであれば、次に制限の種類や内容を満足するかどうかを判定する。

[0369] 例えば、利用制限がある場合に残りの試行回数が0に到達していれば“これ以上の利用は不可”を意味するエラーを発行する。

[0370] まだ試行回数が残されている場合は、制限付き許可コードを許可コード管理部209に渡す。

[0371] 残りの試行回数の確認は、利用時に制限付き許可コードを更新してもよいし、利用回数を許可コード管理部209に保存しておいて制限付き許可コードに含まれる利用回数と比較してもよい。

[0372] 許可コード管理部209は、制限付き許可コードに含まれるインデックスを読み出し、

テーブル901に含まれる参照先アプリのAIDを取り出してカード間IF実行部208に渡す。

[0373] カード間IF実行部208は、参照先アプリのAIDをレスポンスのデータ部に設定し、カード間IF利用を依頼する旨を意味するデータをレスポンスのSWに設定し、このレスポンス1101を読み書き装置103に送信する。

[0374] STEP10－2以降は、許可コードを発行した実施の形態1と同様であり、ここでは、省略する。

[0375] (仮許可コードの発行)

最後に仮許可コードの発行について説明する。

[0376] 事前に、クライアントアプリがダウンロード後に選択されるまで仮許可状態を許可する旨のアプリ属性が参照先存在判定部210に設定されていると仮定する。

[0377] これにより、サーバアプリが搭載されたセキュアデバイスを携帯するのを忘れた場合においても、実際にクライアントアプリを使うまでにサーバアプリを参照する許可コードを発行すればよい。

[0378] アプリのダウンロード時にアドレス解決を開始し、他のセキュアデバイス102が使用許可を意味する情報をセキュアデバイス101に転送するまでは実施の形態1と同様である。

[0379] この場合、セキュアデバイス101のカード間IF実行部208は参照するアプリが存在しない旨を含む情報を受信し、参照先存在判定部210は“NG”と判定した後、「仮許可コード発行許可」が設定されていることを確認し、仮許可コードの発行を許可コード発行部207に依頼する。

[0380] 許可コード発行部207は、指示書2201に従った“FA02h”を仮許可コードとして発行する。

[0381] 指示書2201によれば、アプリの配置に許可されないアドレス領域を示す情報のうちFA～FBhが先頭1バイトに割り当てられ、後半の1バイトで仮状態が許可される条件が表現されることになる。

[0382] また、制限付き許可コード発行後に、アプリ実行部206が保持する仮許可コード管理テーブル2301が更新される。

[0383] 仮許可状態管理テーブル2301は、仮許可コードを発行した場合に更新される。

[0384] SELECTコマンドにてアプリの選択を試みたとき、アプリ実行部206は仮許可コード管理テーブル2301を参照し、選択対象のアプリがまだサーバアプリとのアドレス解決が実行されていないことを確認し、アプリ使用不可を意味するエラーを発行する。

[0385] アプリを選択可能とするためには、1)サーバアプリを同じセキュアデバイスにダウンロードする、あるいは2)サーバアプリが搭載された別のセキュアデバイスとリンク処理を実行する、のいずれかが必要となる。

[0386] 上記1)サーバアプリを同じセキュアデバイスにダウンロードする場合は、公知の技術にてサーバアプリをダウンロードした後、アドレス計算部205はアプリ実行部206が管理する仮許可コード管理テーブル2301を参照し、サーバアプリとのリンク処理待ちのクライアントアプリの存在を確認する。

[0387] クライアントアプリが存在する場合、仮許可コード管理テーブルで保持されているアドレス計算用データを利用してアドレス解決を実行する。

[0388] この後、仮許可コード管理テーブルからリンクを完了したクライアントアプリに関する行を削除する。

[0389] 上記2)サーバアプリが搭載された別のセキュアデバイスとリンク処理を実行する場合は、読み書き装置103から、リンク専用コマンドを送信する。

[0390] リンク専用コマンドは、リンク専用コマンドであることを解釈可能なヘッダ部と、サーバアプリの識別子を含むデータ部からなる。

[0391] ダウンロード管理部201がリンク専用コマンドを受信すると、アドレス計算部205は、アプリ実行部206が管理する仮許可コード管理テーブル2301を参照し、サーバアプリとのリンク処理待ちのクライアントアプリの存在を確認する。

[0392] リンク処理待ちのクライアントアプリが存在する場合、仮許可コード管理テーブル2301で保持しているアドレス計算用データと、サーバアプリの識別子とを、カード間IF実行部208に渡し、カード間IF実行部208と他のセキュアデバイス102間で参照先の存在を確認する。

[0393] 使用許可を意味する情報をカード間IF実行部208が受信すると、参照先存在判定部210が許可コードの発行を許可コード発行部207に依頼する。

[0394] 許可コード発行部207は、許可コードを発行し、許可コードテーブル901を更新する。

[0395] また参照先存在判定部210は、アプリ実行部206に依頼して仮許可コード管理テーブルからリンクを完了したクライアントアプリに関する行を削除する。

[0396] 以上1)、2)いずれかの処理を行うことにより、以降のクライアントアプリの選択、実行が実現できる。

[0397] 本実施の形態6では、実施の形態1で詳述した許可コード以外にも、制限付き許可コードや仮許可コードの発行と、それら許可コードを付与されたアプリの動作について説明した。

[0398] 制限付き許可コードにより、サーバアプリ側を変更すること無く、利用回数などを制限できるため、お試し版のような一時的なアプリの発行に適用できる。

[0399] 仮許可コードにより、クライアントアプリをダウンロードするときにサーバアプリが搭載されたセキュアデバイスを所有しなくても、後でリンク処理を行うことができる。これにより、ユーザがクライアントアプリのダウンロードを希望するにもかかわらず、その時点でサーバアプリが搭載されたセキュアデバイスを持ち合わせていないために断念せざるを得ない場面がなくなる。

[0400] したがって、サービス提供者からみた事業機会の損失、ユーザから見たサービス利用機会の損失に対する有効な対策となる。

[0401] (実施の形態7)

実施の形態7は、他のセキュアデバイスに搭載されたサーバアプリに処理を依頼し、サーバアプリの処理データをクライアントアプリで利用する方法に関する発明である。

[0402] 本実施の形態7について図5、図24～図27を用いて説明する。

[0403] 図24は、本実施の形態におけるセキュアデバイス2401の構成を示したブロック図である。

[0404] ダウンロード管理部201、アプリ格納部202、アプリ203、204、アドレス計算部205、アプリ実行部206、許可コード発行部207、カード間IF実行部208、許可コード管理部209は、それぞれ実施の形態1で説明したものと同様である。

[0405] 図2に示す、セキュアデバイス101との差異は、クライアントアプリ2402と、スタック操作部2403である。

[0406] クライアントアプリ2402は、他のセキュアデバイス2501に搭載されたサーバアプリが提供するIFを利用する。

[0407] スタック操作部2403は、サーバアプリが提供するIFを利用する際のクライアントアプリが扱うスタックを操作する。

[0408] 図25は、本実施の形態における他のセキュアデバイス2501の構成を示したブロック図である。アプリ格納部202、アプリ実行部206、サーバアプリ401は実施の形態1で説明したものと同様である。

[0409] 図4に示す、セキュアデバイス102との差異は、スタック制御部2502である。

[0410] スタック制御部2502は、同一のセキュアデバイスに搭載されたクライアントアプリからの呼び出しと、別のセキュアデバイスに搭載されたクライアントアプリからの呼び出しと、に対してのサーバアプリが同じ動作をするための制御を行う。

[0411] 図5は、本実施の形態における読み書き装置103であり、実施の形態1と同様である。

[0412] 本実施の形態では、セキュアデバイス2401と他のセキュアデバイス2501と読み書き装置103からなるシステムについて説明する。

[0413] 本実施の形態1では、サーバアプリからのレスポンスにSW以外のデータを含まないケースについて述べた。(図11(a)のレスポンス1103参照)

[0414] もしもレスポンスがデータとSWから構成され、以降のクライアントアプリの処理でデータを利用するならば、そのデータはスタック上に積まれている必要がある。

[0415] 同一セキュアデバイス上にサーバアプリが存在する場合には、サーバアプリでの処理結果である戻り値がスタック上に積まれて呼び出し元であるクライアントアプリに戻ってくることが知られている。

[0416] しかしながら、サーバアプリが同一セキュアデバイス上に存在せず、他のセキュアデバイス上のサーバアプリを利用した場合の戻り値は、セキュアデバイス間の通信プロトコルに従ってAPDU(Application Protocol Data Unit)に内蔵される。

[0417] したがって、サーバアプリがどのセキュアデバイス上にあるかに関係なくクライアント

アプリに同じ動作をさせるためには、APDUから戻り値を抽出し、クライアントアプリのスタック上に積む操作が必要になる。

[0418] 本実施の形態7では、サーバアプリからの戻り値を、以降のクライアントアプリの処理で利用する方法について説明する。

[0419] これに際し、以下に前提を述べる。

[0420] ・サーバアプリは他のセキュアデバイスに搭載され、クライアントアプリのアドレス解決は完了している。

[0421] ・クライアントアプリが実行され、図10のSTEP10－3までは完了している。

[0422] この前提は、実施の形態1に記載のシステムの動作と同様にして実施される。

[0423] 図26に示すように“method__1”が“method__2”を呼び出している場合について説明する。

[0424] アプリ実行部206は関数単位でフレームを作成し、処理を実行する。フレームとは、関数が値を返したり、例外の処置を行ったり、データと結果の一部をストアするために使用する作業エリアのことである。“method__1”にはフレーム1が、“method__2”はフレーム2が割り当てられる。また各フレームは、ローカル変数とスタックからなる。

[0425] “method__1”が“method__2”を呼び出した直後に、フレーム2が生成される。“method__2”は、フレーム2を用いて処理を行い、最後に“b”を返却する。

[0426] “b”の返却とは、“b”の値が“sreturn”という命令コードによって直接フレーム1のスタックに積まれることを意味する。また、“b”を返却した後にフレーム2は消去される。

[0427] その後、“method__1”が処理を継続する。

[0428] このようにして、関数同士の呼び出しが成立する。

[0429] しかしながら、“method__1”と“method__2”が異なるセキュアデバイス上にある場合には、本来“method__1”のフレームに積まれているはずの“method__2”のフレームが他のセキュアデバイス管理下にあるため、“method__2”による処理結果を、呼び出し側の“method__1”のスタックに直接積むことはできない。

[0430] したがって、本来“method__2”が処理結果を“method__1”のスタックに直接積む操作と同等の処理を、“method__2”が直接積むことができない状況で実現可能な仕組みが必要になる。

[0431] したがって、スタック制御部2502は、別のセキュアデバイスに搭載されたクライアントアプリからの参照時に限って、戻り値の操作に関係する命令コード(例:sreturn)に対して通常と異なる処理を実行する。

[0432] 別のセキュアデバイスに搭載されたクライアントアプリからの呼び出される際、アプリ実行部403には呼び出し元のフレームがない。

[0433] この場合に、"sreturn"の処理はスタック制御部2502が担当する。

[0434] スタック制御部2502は、呼び出し元フレームのスタックへの書き込みを中止し、代わりに図27に示すデータを作成する。

[0435] 本実施の形態に記載の発明では、図27のようなデータを生成し、利用することで、クライアントアプリが、サーバアプリを有するセキュアデバイス内に存在しない場合にも、スタックに積むことができる。

[0436] 図27は、"sreturn"であることを意味するTAGと、戻り値の長さを意味するLEGNTHと、戻り値を表すValueから構成される。

[0437] これが、サーバアプリから送信されるレスポンスのデータ部に設定され、呼び出し結果として、クライアントアプリを実行するセキュアデバイス101に渡されることになる。

[0438] 次に、データを受信した後のセキュアデバイス2401の動作について図10を用いて説明する。

[0439] 本実施の形態においては、図10におけるセキュアデバイス101をセキュアデバイス2401に、他のセキュアデバイス102を他のセキュアデバイス2501に置き換えて説明する。

[0440] また、クライアントアプリ2402がサーバアプリを参照するときの複数ステップのうちSTEP10－1から10－4までは実施の形態1と同様であるため説明を省略し、サーバアプリの処理結果が戻ってくるSTEP10－5について説明する。

[0441] セキュアデバイス2401のカード間IF実行部208が共有コマンドを受信し、スタック操作部2403に共有コマンドのデータ部を渡す。

[0442] スタック操作部2403は、"sreturn"であることを意味するTAGを解釈し、呼び出し元(クライアントアプリ)のフレームのスタック上にValueを積む。

[0443] この後、クライアントアプリも、サーバアプリが同一セキュアデバイスに搭載されてい

る場合と同様に処理を継続することができる。

[0444] 本実施の形態6では、セキュアデバイス2401にスタック操作部2403を、他のセキュアデバイス2501にスタック制御部2502を備えることにより、サーバアプリとクライアントアプリのコードに特殊な加工をすることなく、他のセキュアデバイスに搭載されたサーバアプリからの戻り値をクライアントアプリが利用できる方法について述べた。

[0445] サーバアプリの戻り値を、クライアントアプリで確認・利用する場面は多く、本方式の効果は大きい。

[0446] 本発明を詳細にまた特定の実施態様を参照して説明したが、本発明の精神と範囲を逸脱することなく様々な変更や修正を加えることができることは当業者にとって明らかである。

本出願は、2006年3月31日出願の日本特許出願(特願2006－098865)、2007年3月22日出願の日本特許出願(特願2007-075217)に基づくものであり、その内容はここに参照として取り込まれる。

産業上の利用可能性

[0447] 本発明のセキュアデバイス、読み書き装置により、セキュアデバイスのメモリ領域の削減を図ることが出来るという効果を有するシステムを提供することができる。

請求の範囲

[1] データ処理を行うアプリケーションである、クライアントアプリを格納するアプリ格納部と、

クライアントアプリとデータのやり取りを行う、サーバアプリを前記アプリ格納部が有しているか否かを判定するアドレス計算部と、

前記アドレス計算部により、前記アプリ格納部は、第1のクライアントアプリとデータのやり取りを行う第1のサーバアプリを有していないと判定されたとき、他のセキュアデバイスが前記第1のサーバアプリを有しているか否かを判定する参照先存在判定部と、

を有する、セキュアデバイス。

[2] さらに、他のセキュアデバイスへアクセスするカード間IF実行部を備え、

前記参照先存在判定部は、前記カード間IF実行部による結果に基づき、他のセキュアデバイスが前記第1のサーバアプリを有しているか否かを判定する、請求項1記載のセキュアデバイス。

[3] さらに、前記参照先存在判定部により、他のセキュアデバイスが前記第1のサーバアプリを有していると判定されたとき、前記第1のサーバアプリを参照することを許可する許可コードを発行する許可コード発行部と、

前記許可コードに基づき、前記第1のクライアントアプリを実行するアプリ実行部と、を備える、請求項2記載のセキュアデバイス。

[4] さらに、少なくとも、前記他のセキュアデバイスの有する第1のサーバアプリのアプリ識別子を含む管理情報を管理する、許可コード管理部を備え、

前記アプリ実行部は、前記第1のクライアントアプリを実行するとき、前記管理情報を基に前記アプリ識別子と参照先と前記参照先に渡すパラメータとの中で、少なくとも1つをレスポンスとして、前記参照先に送信する、請求項3記載のセキュアデバイス。

[5] 前記カード間IF実行部により送受信されるデータのセキュリティを確保するセキュリティ管理部を備える、請求項2記載のセキュアデバイス。

[6] さらに、前記許可コード発行部が、第1のクライアントアプリの利用制限に応じた利用制限付き許可コードを発行するとき、

前記アプリ実行部は、前記許可コードに基づいて、前記第1のクライアントアプリからの前記第1のサーバアプリへの参照を制限する、請求項3記載のセキュアデバイス。

[7] さらに、第2のクライアントアプリをダウンロードするダウンロード管理部を備え、

前記カード間IF実行部が前記第2のサーバアプリを参照できない場合、

前記許可コード発行部は、前記ダウンロード管理部が前記第2のクライアントアプリをダウンロードすることを許可する仮許可コードを発行する、請求項3記載のセキュアデバイス。

[8] 前記カード間IF実行部が前記第2のサーバアプリを参照することができるとき、

前記第2のサーバアプリと、前記仮許可コードによりダウンロードが許可された前記第2のクライアントアプリと、によるデータ通信を行う、請求項7記載のセキュアデバイス。

[9] さらに、前記他のセキュアデバイスが有する第1のサーバアプリによる処理の指示と、前記処理による戻り値とに基づき、前記第1のクライアントアプリの実行をアプリ実行部に行わせるスタック操作部を備える、請求項1記載のセキュアデバイス。

[10] サーバアプリを有するセキュアデバイスであって、

前記サーバアプリの参照要求を受信するカード間IF実行部と、

前記サーバアプリを実行するアプリ実行部と、

前記アプリ実行部が前記サーバアプリを実行するときに、クライアントアプリを有するセキュアデバイスから前記参照要求がある場合、前記サーバアプリによる処理の判定と、前記処理による戻り値とを、前記クライアントアプリを有するセキュアデバイスに送るデータを作成するスタック制御部と、を備える、セキュアデバイス。

[11] サーバアプリを有する第1のセキュアデバイスと、クライアントアプリを実行する第2のセキュアデバイスとのデータのやり取りを制御する、読み書き装置であって、

前記第1のセキュアデバイスと前記第2のセキュアデバイスと、データ通信を行う排他制御通信部と、

前記第1のセキュアデバイスと前記第2のセキュアデバイスとに送信するコマンドを管理するとともに、前記第1のセキュアデバイスと前記第2のセキュアデバイスとからのレスポンスを解析するアプリ制御部と、を備え、

前記排他制御通信部が、前記第1のセキュアデバイスからのカード間IF利用を示すデータを受信してから、前記カード間IF利用の完了を示すデータを受信するまで、

前記アプリ制御部は、前記第2のセキュアデバイスからのレスポンスをコマンドとして、前記排他制御通信部に前記第1のセキュアデバイスへ送信させ、

前記第1のセキュアデバイスからのレスポンスをコマンドとして前記排他制御通信部に前記第2のセキュアデバイスへ送信させる、読み書き装置。

[12] 前記第1のセキュアデバイスを識別する第1のカードIDと前記第1のセキュアデバイスの所有者との第1の関連情報と、前記第2のセキュアデバイスを識別する第2のカードIDと前記第1のセキュアデバイスの所有者との第2の関連情報と、を管理する所有者管理部と、

前記第1の関連情報と前記第2の関連情報とが所定要件を満たすとき、前記第2のセキュアデバイスに、前記クライアントアプリのダウンロードを許可するダウンロード条件判定部とを備える、請求項11記載の読み書き装置。

[13] 前記所定要件は、前記第1のセキュアデバイスの所有者情報と、前記第2のセキュアデバイスの所有者情報とが、同じ所有者を示す情報であるということである、請求項12記載の読み書き装置。

[14] 前記アプリ実行部は、前記第1のサーバアプリを有する他のセキュアデバイスの利用状態を、前記カード間IF実行部に取得させ、

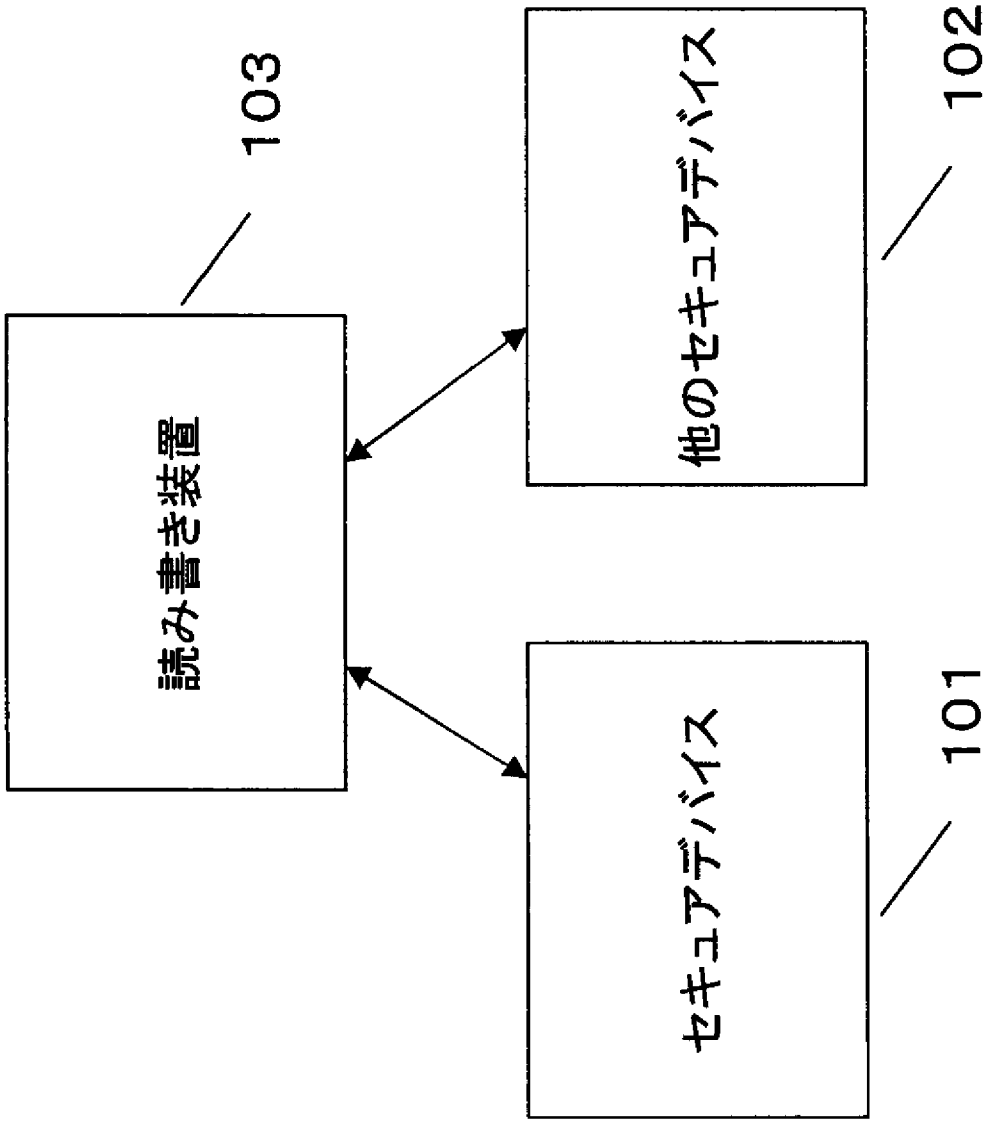
前記利用状態が前記他のセキュアデバイスが利用できない状態であることを示すときに、前記カード間IF実行部による、前記他のセキュアデバイスが利用できないことを示すデータを受信する、請求項3記載のセキュアデバイス。

[15] 前記クライアントアプリは、視聴権および視聴コンテンツを含み、

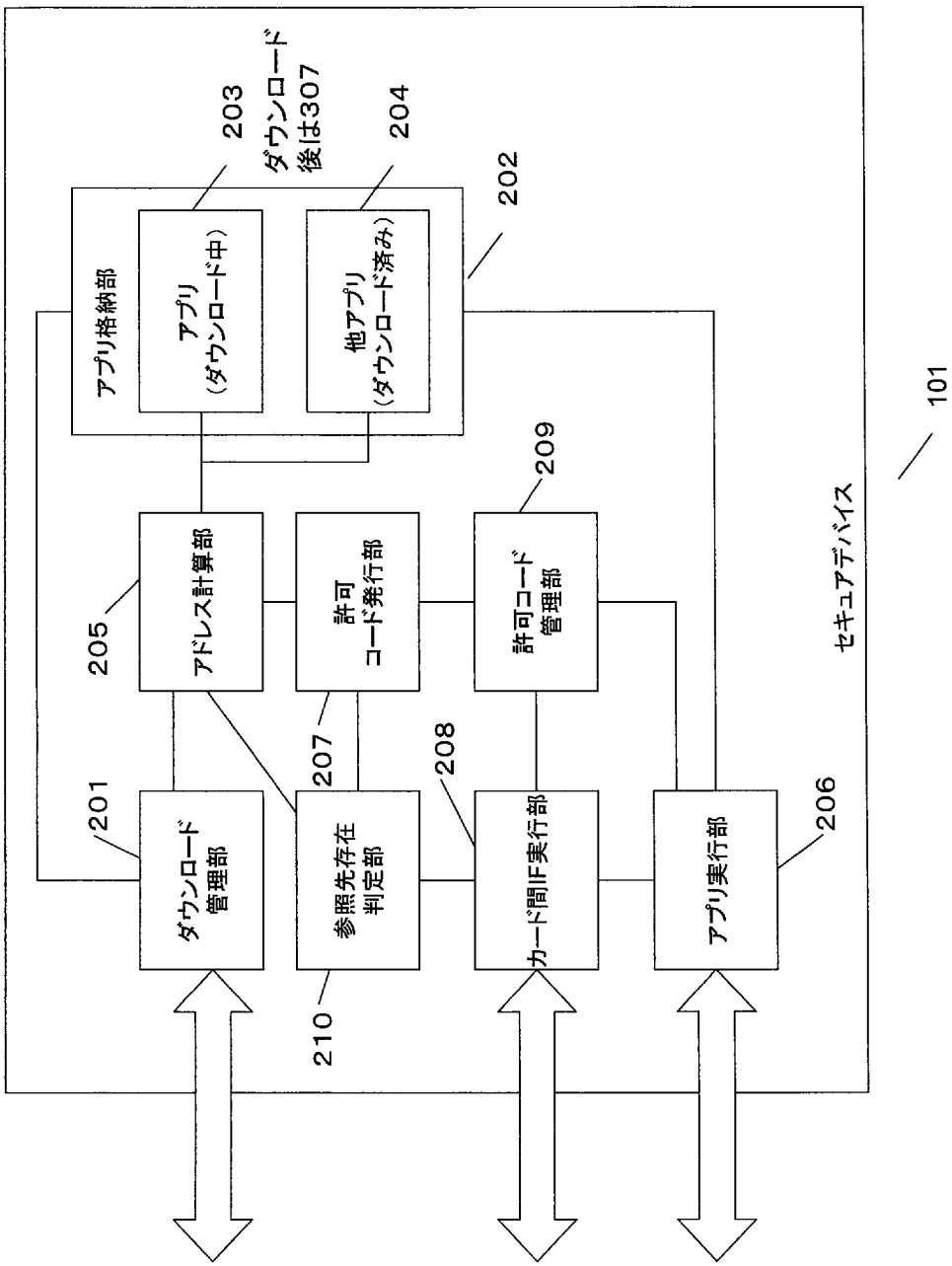
前記サーバアプリは、前記クライアントアプリから渡された前記視聴権に付随する条件をチェックする、請求項1記載のセキュアデバイス。

[16] セキュアデバイス所有者の正当性を判定するための情報を入力する所有者情報確認入力部を備える、請求項12記載の読み書き装置。

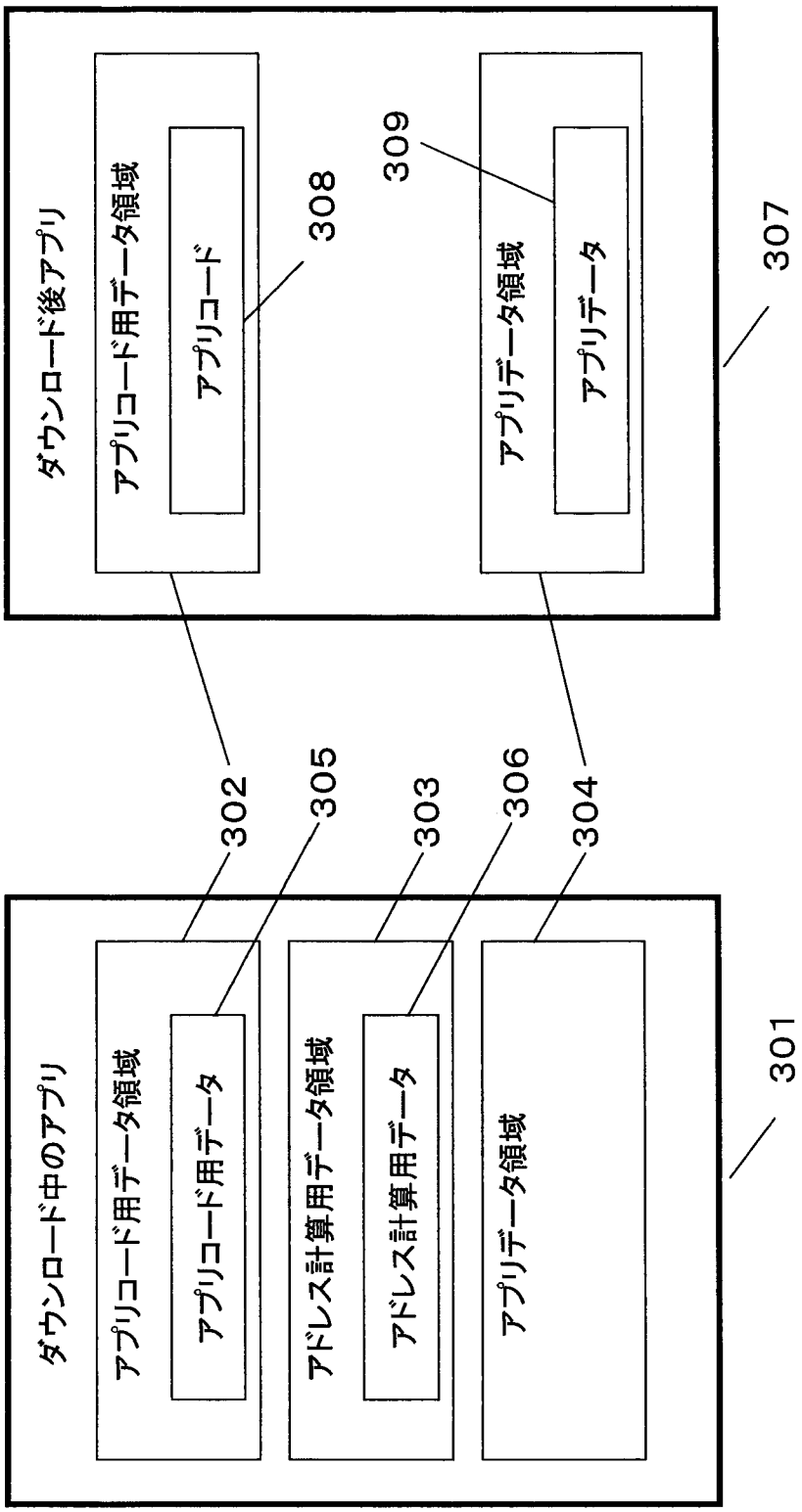
[図1]



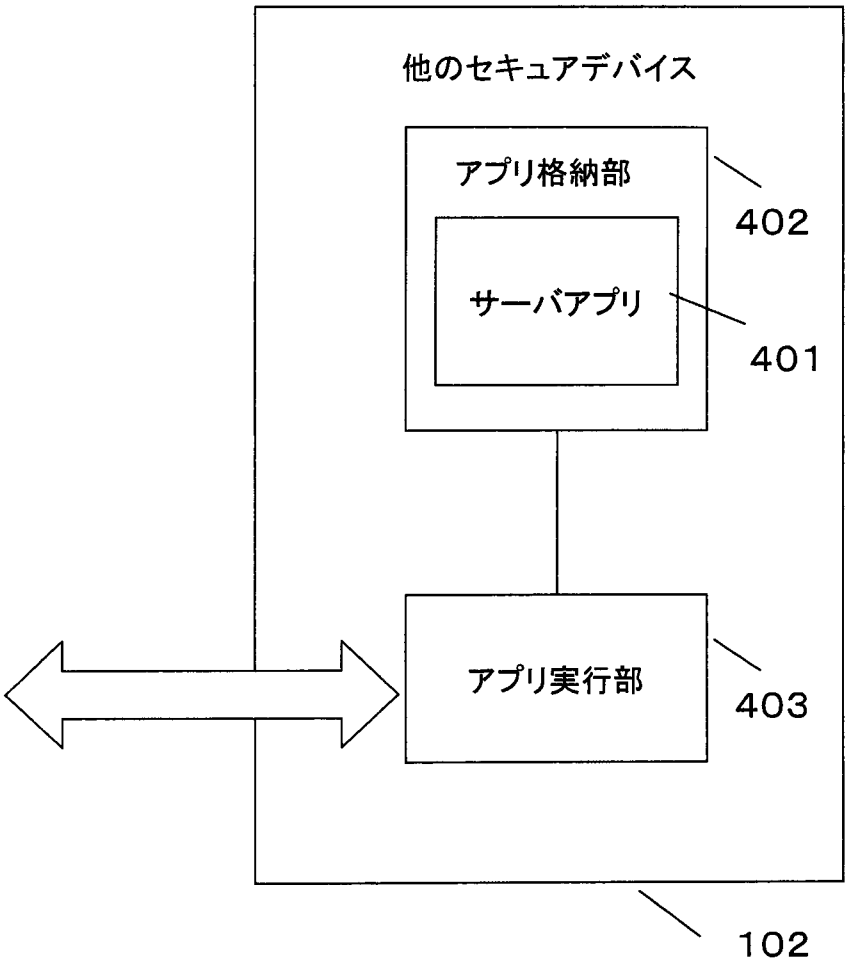
[図2]


101
セキュアデバイス
アプリ格納部
203
ダウンロード後は307
アプリ（ダウンロード中）
204
他アプリ（ダウンロード済み）
202
205
アドレス計算部
許可コード発行部
209
許可コード管理部
201
ダウンロード管理部
207
参照先存在判定部
208
カード間IF実行部
アプリ実行部
206
210

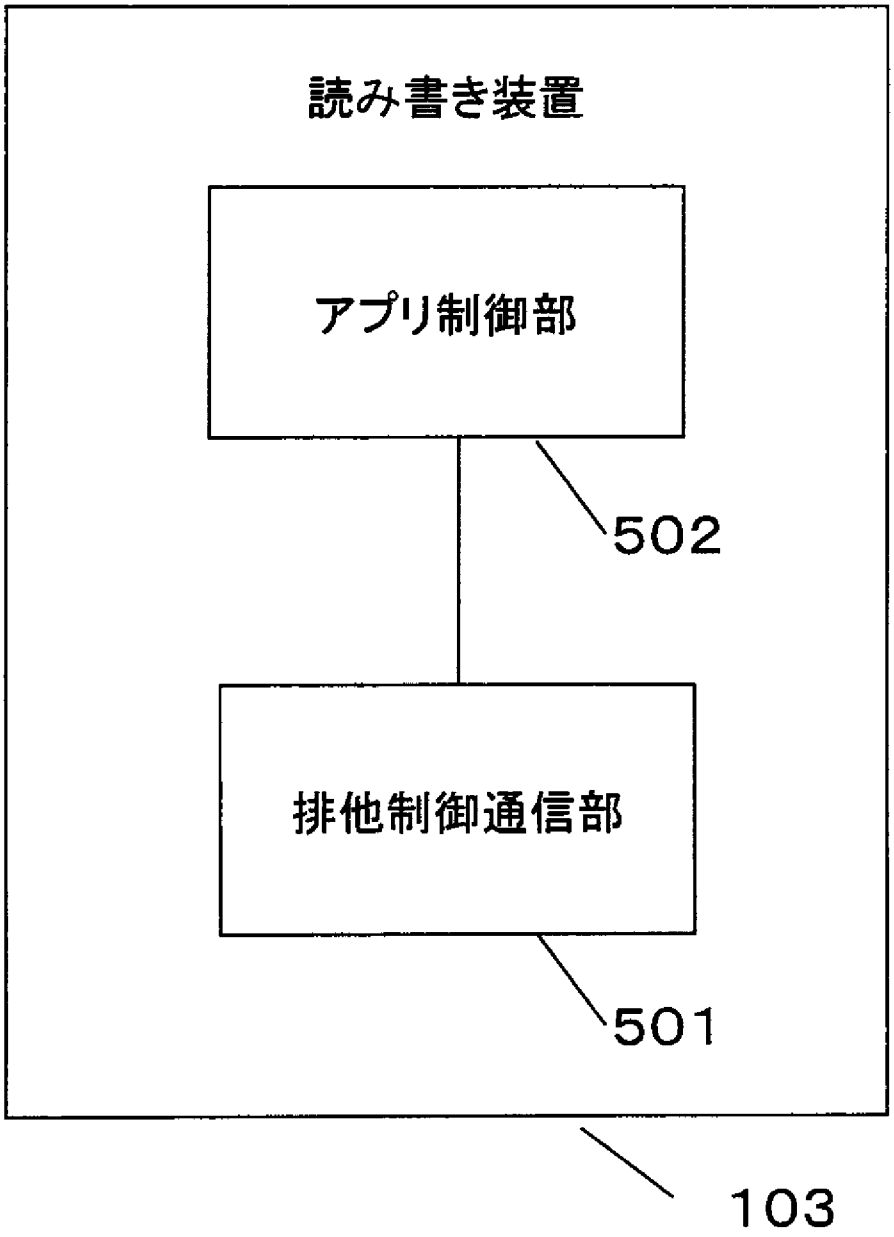
[図3]


ダウンロード後アプリ
アプリコード用データ領域
アプリコード
アプリデータ領域
アプリデータ
307
308
309
ダウンロード中のアプリ
アプリコード用データ領域
アプリコード用データ
アドレス計算用データ領域
アドレス計算用データ
アプリデータ領域
301
302
303
304
305
306

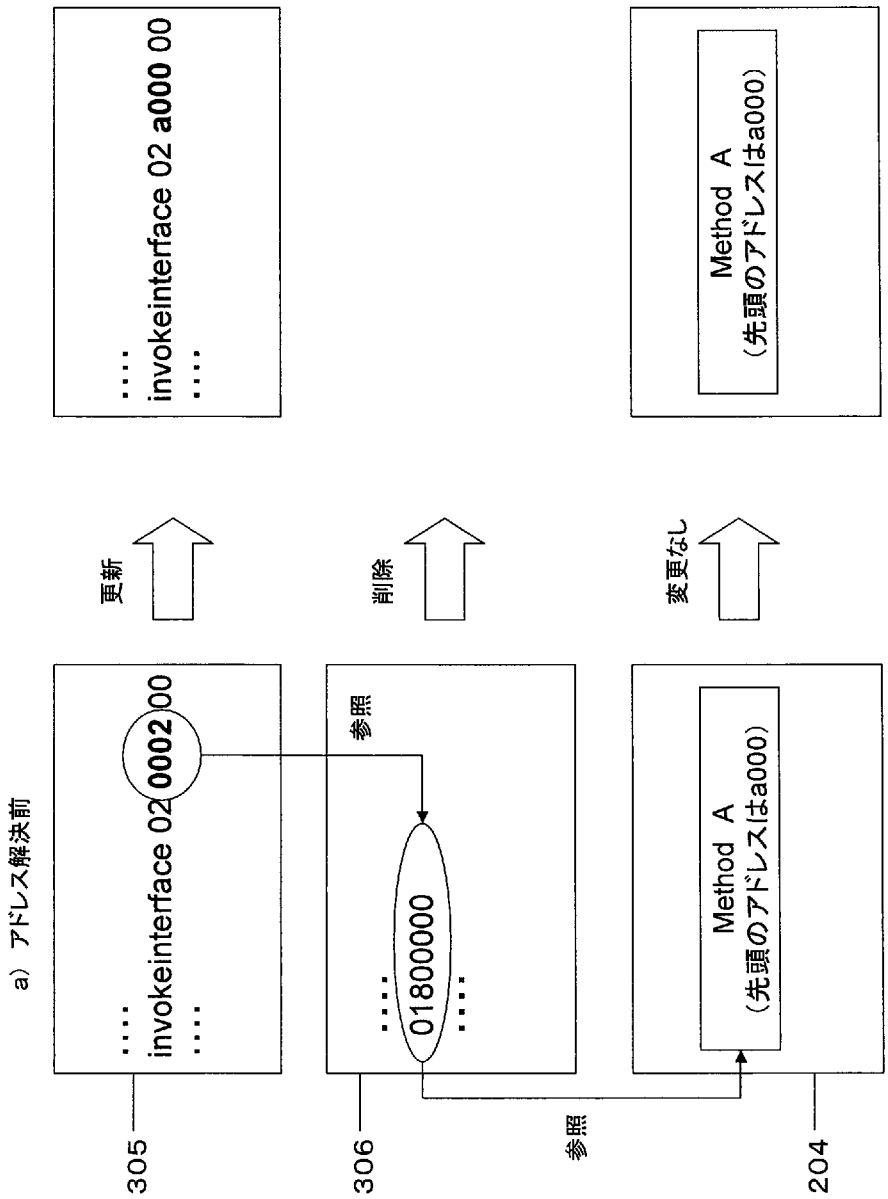
[図4]



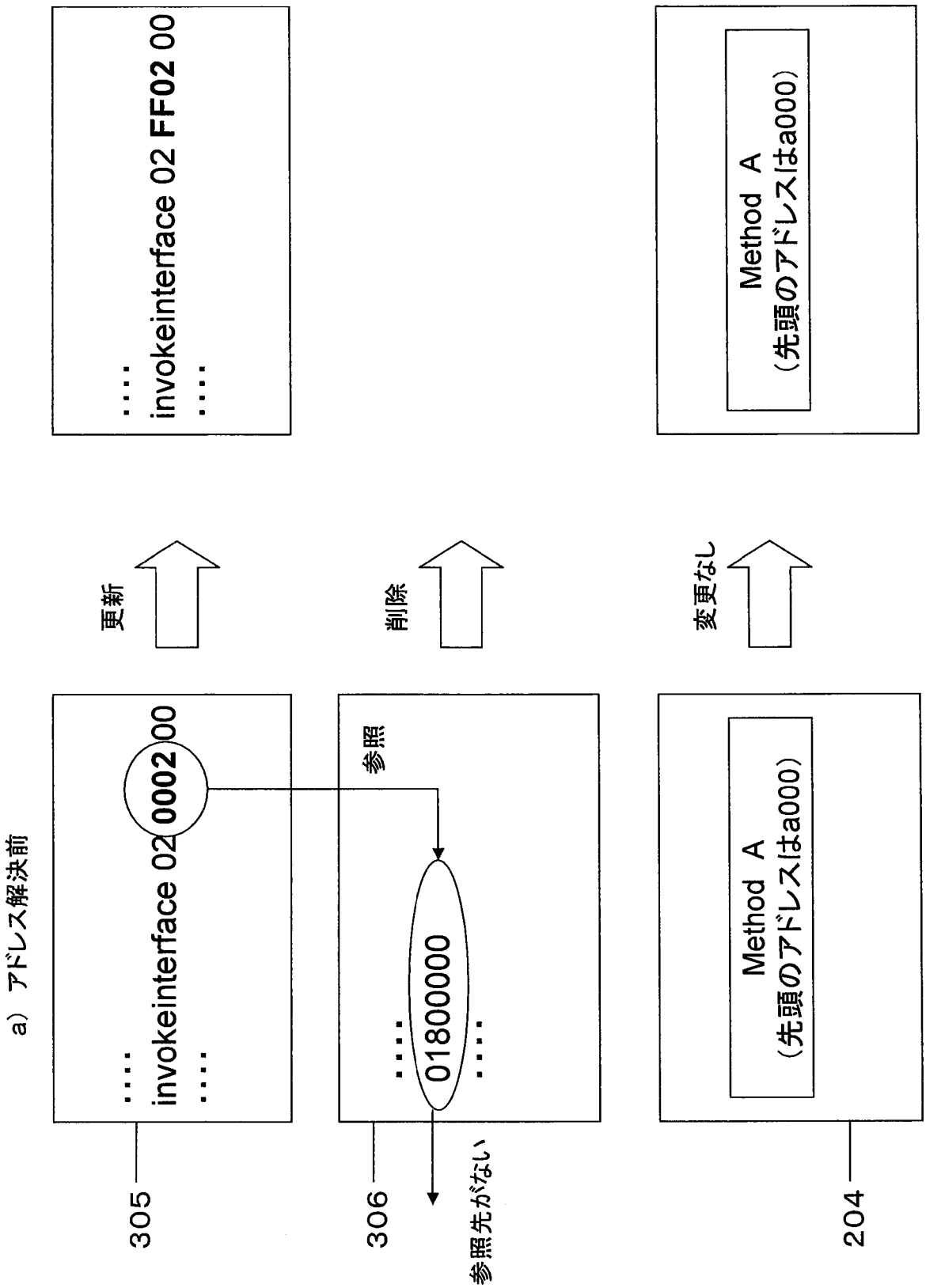
[図5]



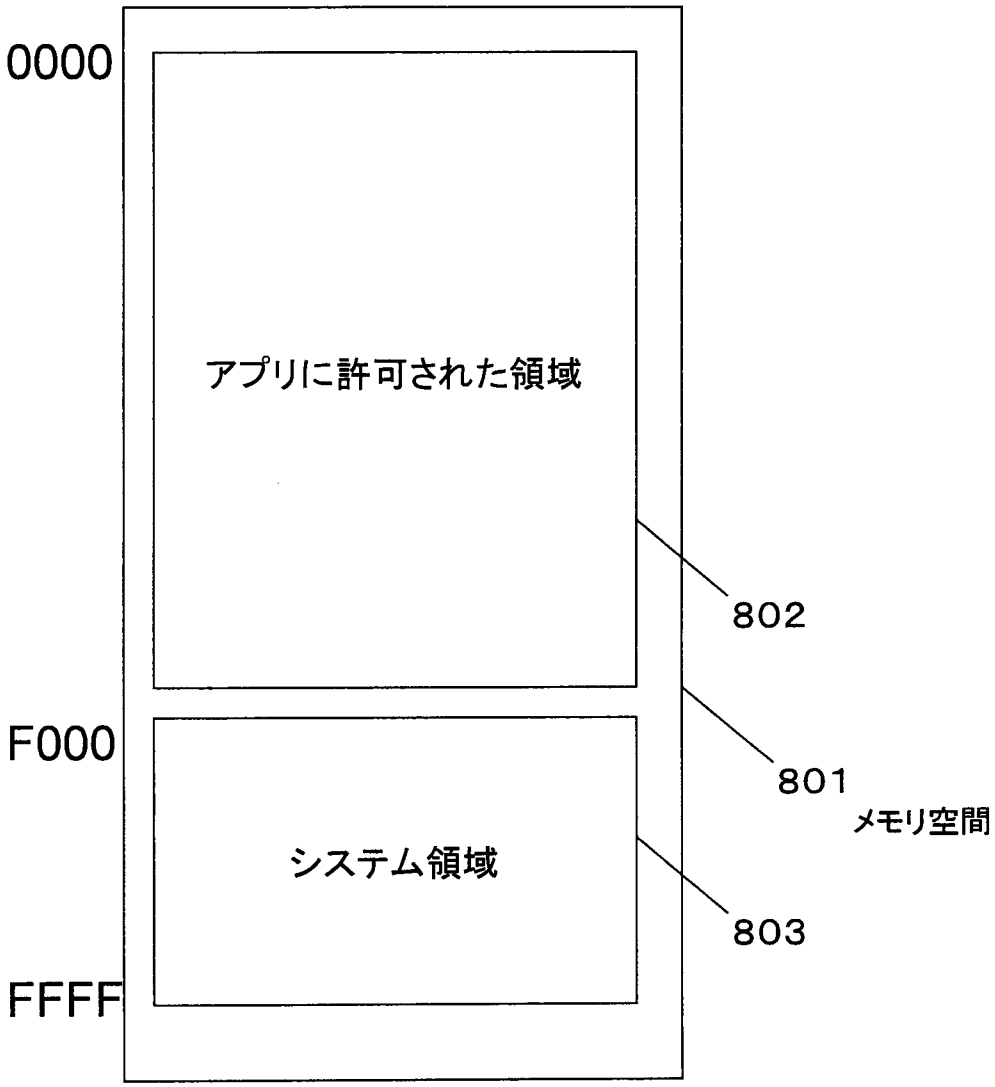
[図6]


a) アドレス解決前
invokeinterface 02 0002 00
01800000
Method A
(先頭のアドレスはa000)
参照
参照
更新
削除
変更なし
invokeinterface 02 a000 00
Method A
(先頭のアドレスはa000)
305
306
204

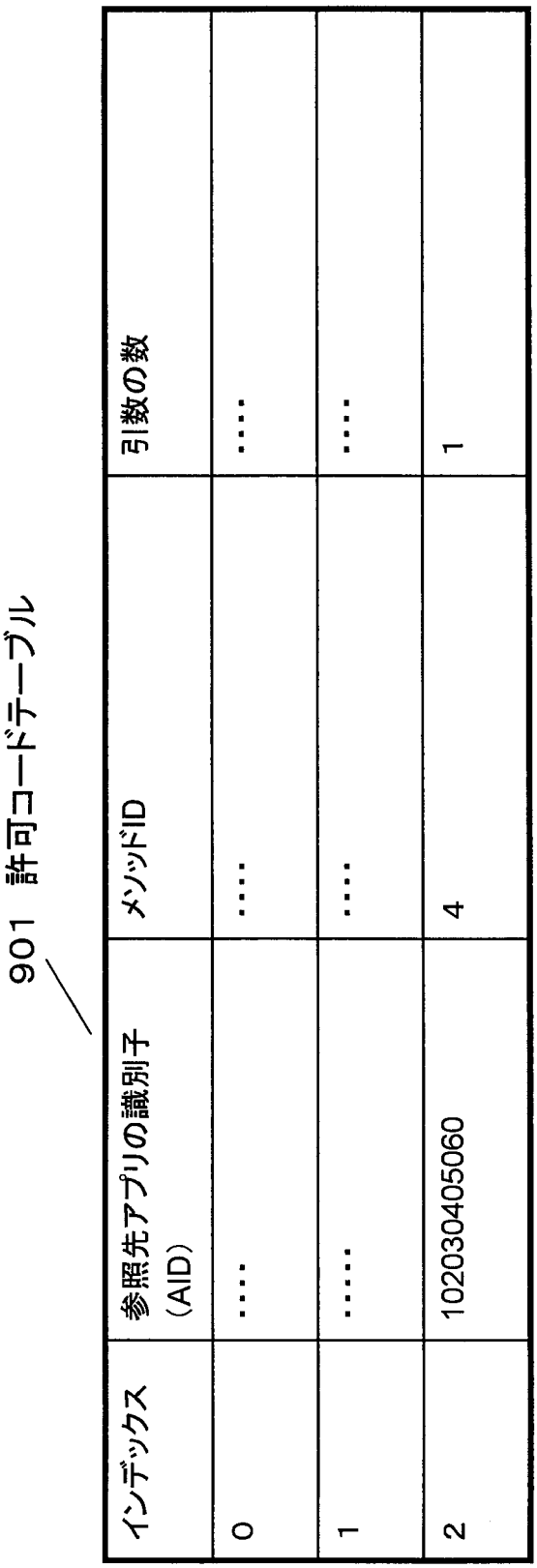
[図7]


a) アドレス解決前
invokeinterface 02 0002 00
305
参照
01800000
306
参照先がない
Method A
(先頭のアドレスはa000)
204
更新
削除
変更なし
invokeinterface 02 FF02 00
Method A
(先頭のアドレスはa000)

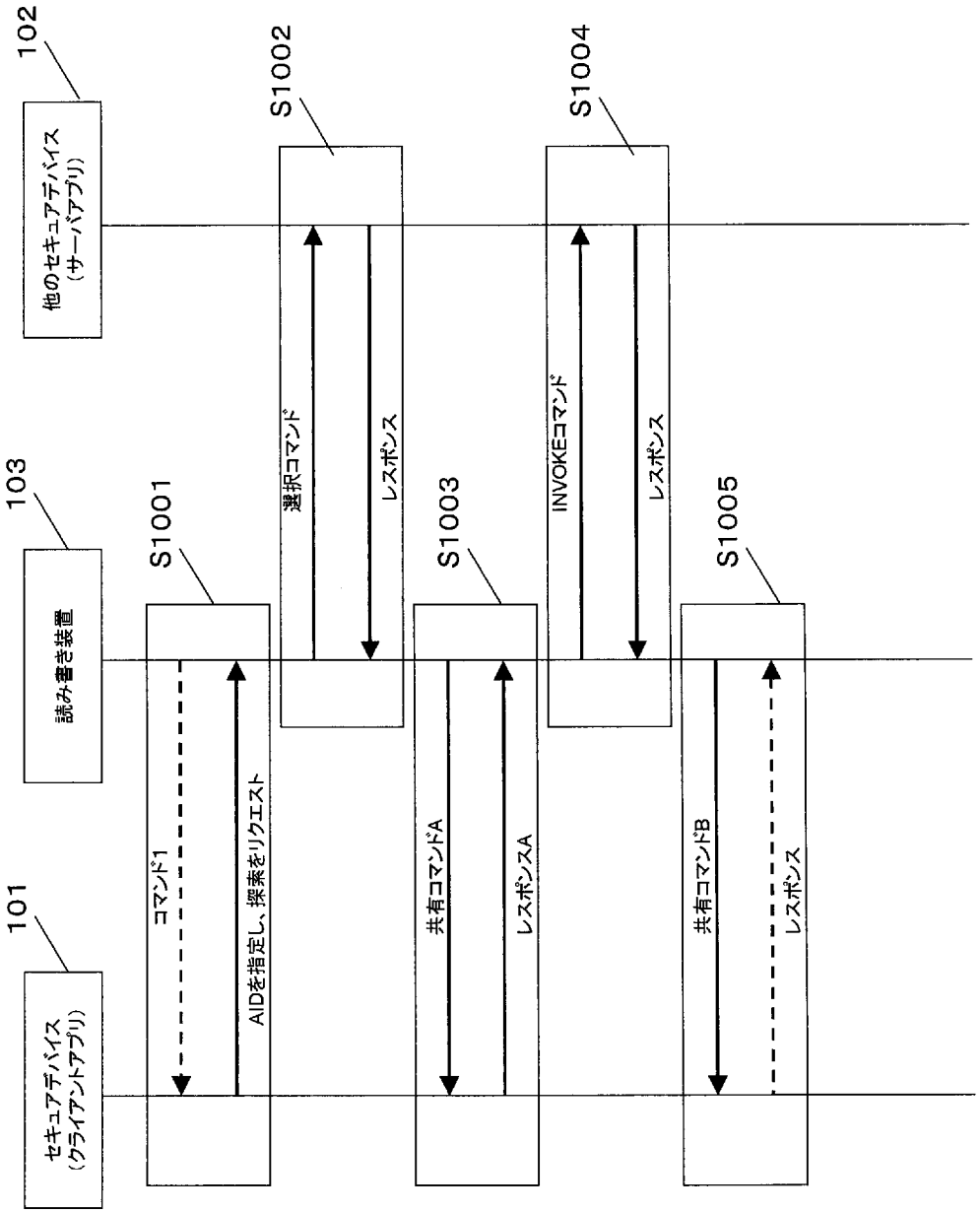
[図8]



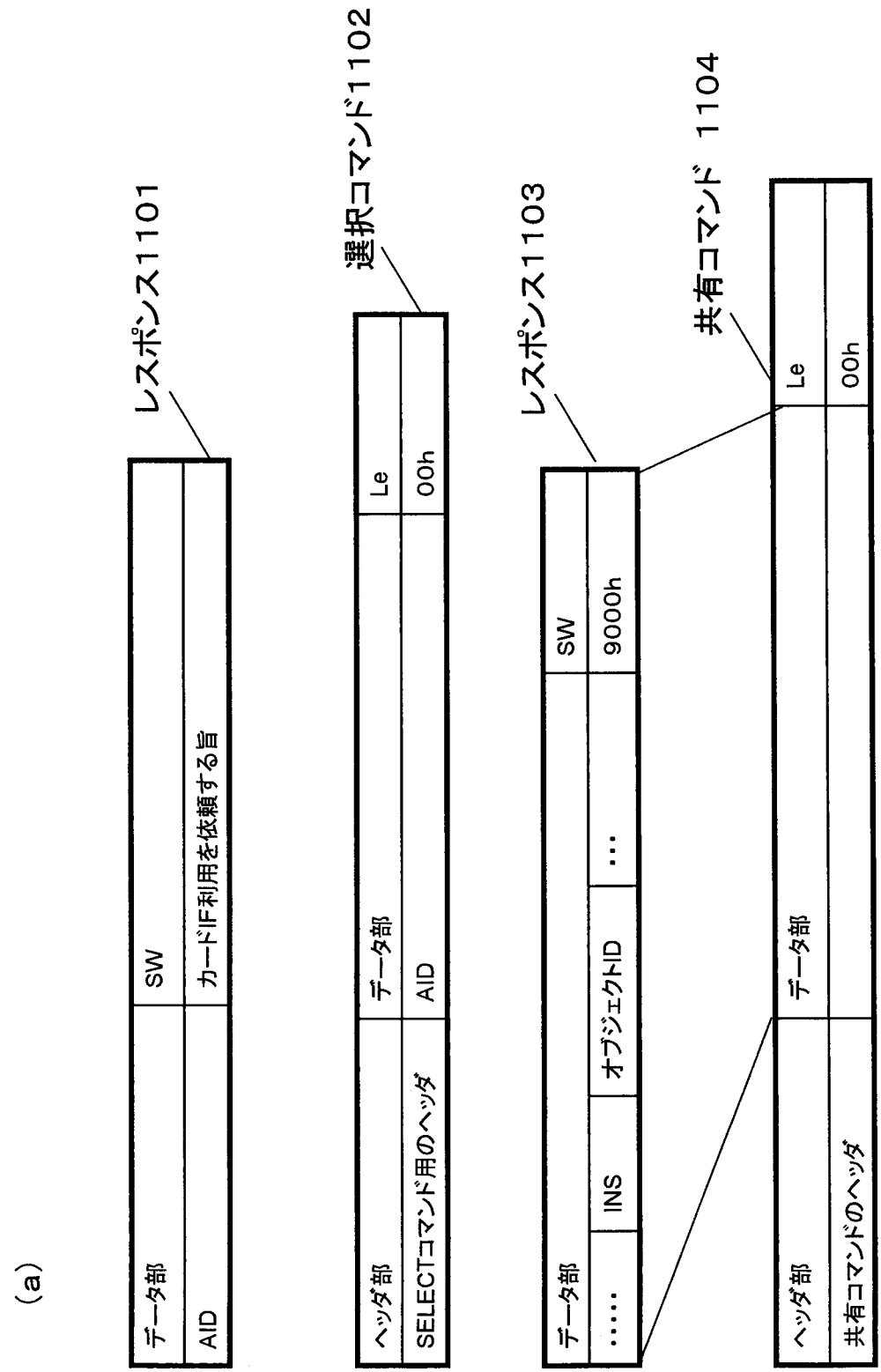
[図9]


901 許可コードテーブル
インデックス
参照先アプリの識別子 (AID)
メソッドID
引数の数
0
.....
.....
.....
1
.....
.....
.....
2
102030405060
4
1

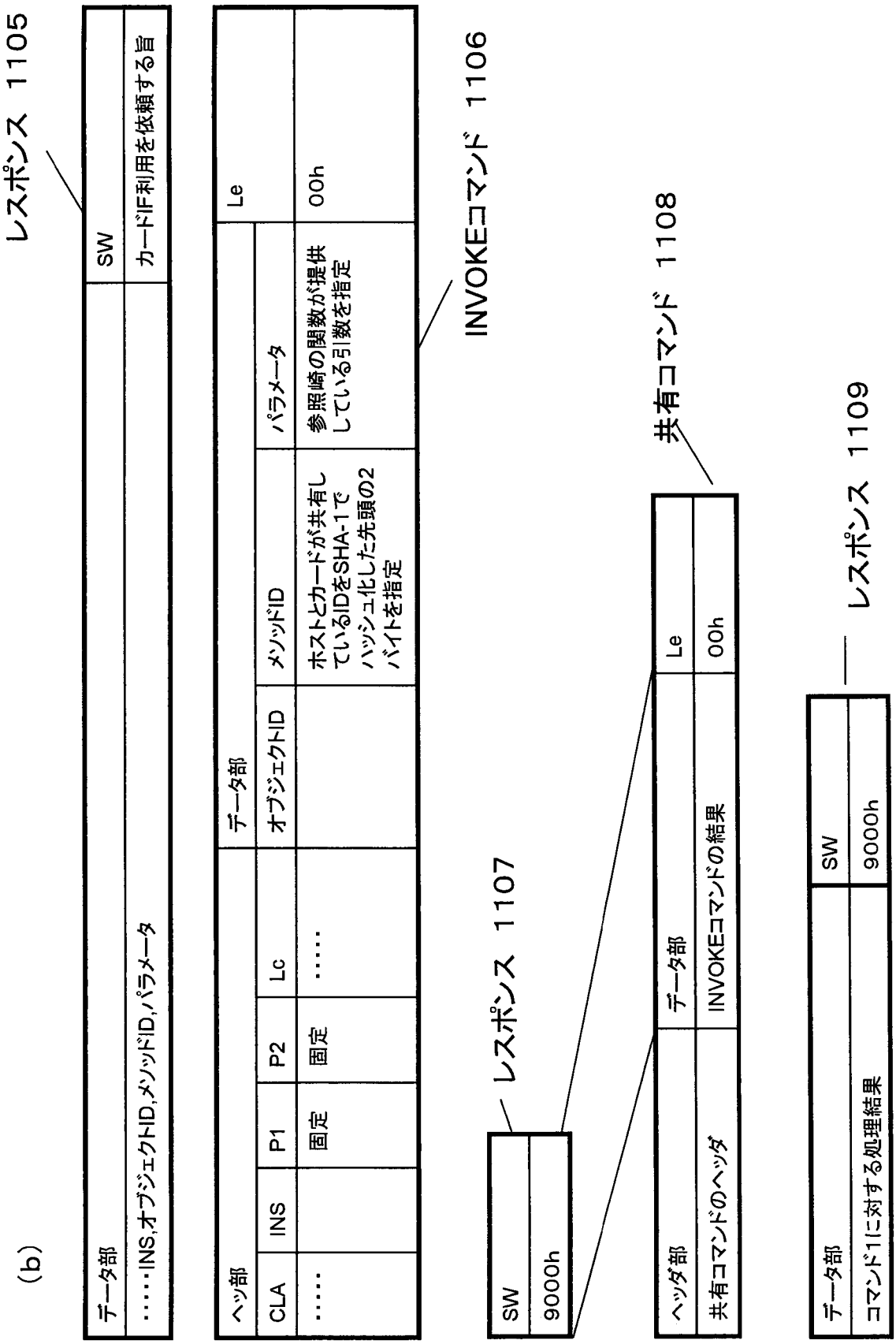
[図10]


102
他のセキュアデバイス
(サーバアプリ)
S1002
S1004
選択コマンド
レスポンス
INVOKEコマンド
レスポンス
103
読み書き装置
S1001
S1003
S1005
コマンド1
AIDを指定し、探索をリクエスト
共有コマンドA
レスポンスA
共有コマンドB
レスポンス
101
セキュアデバイス
(クライアントアプリ)

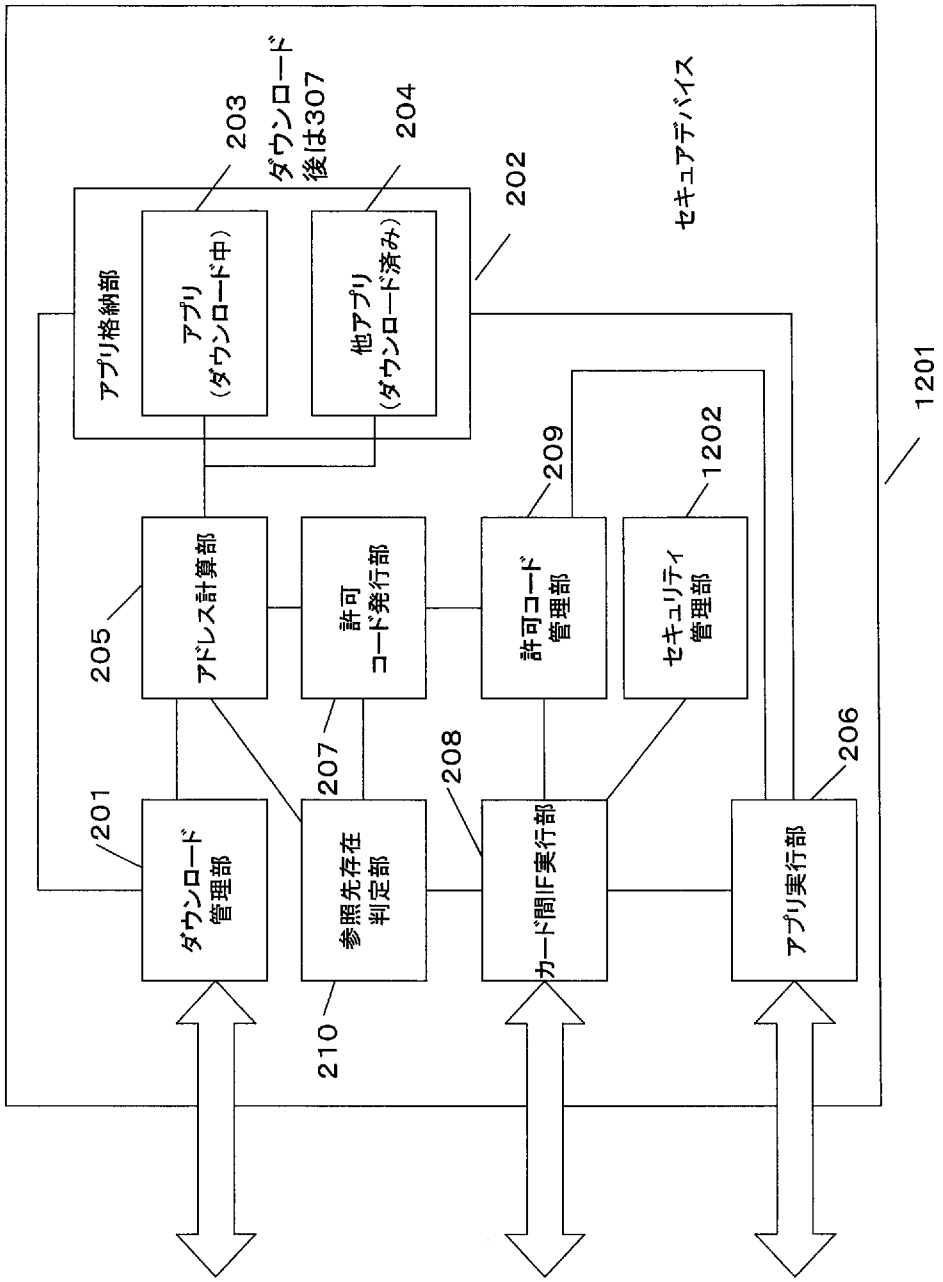
[図11a]


(a)
レスポンス1101
データ部
AID
SW
カードIF利用を依頼する旨
選択コマンド1102
ヘッダ部
SELECTコマンド用のヘッダ
データ部
AID
Le
00h
レスポンス1103
データ部
.....
INS
オブジェクトID
...
SW
9000h
共有コマンド 1104
ヘッダ部
共有コマンドのヘッダ
データ部
Le
00h

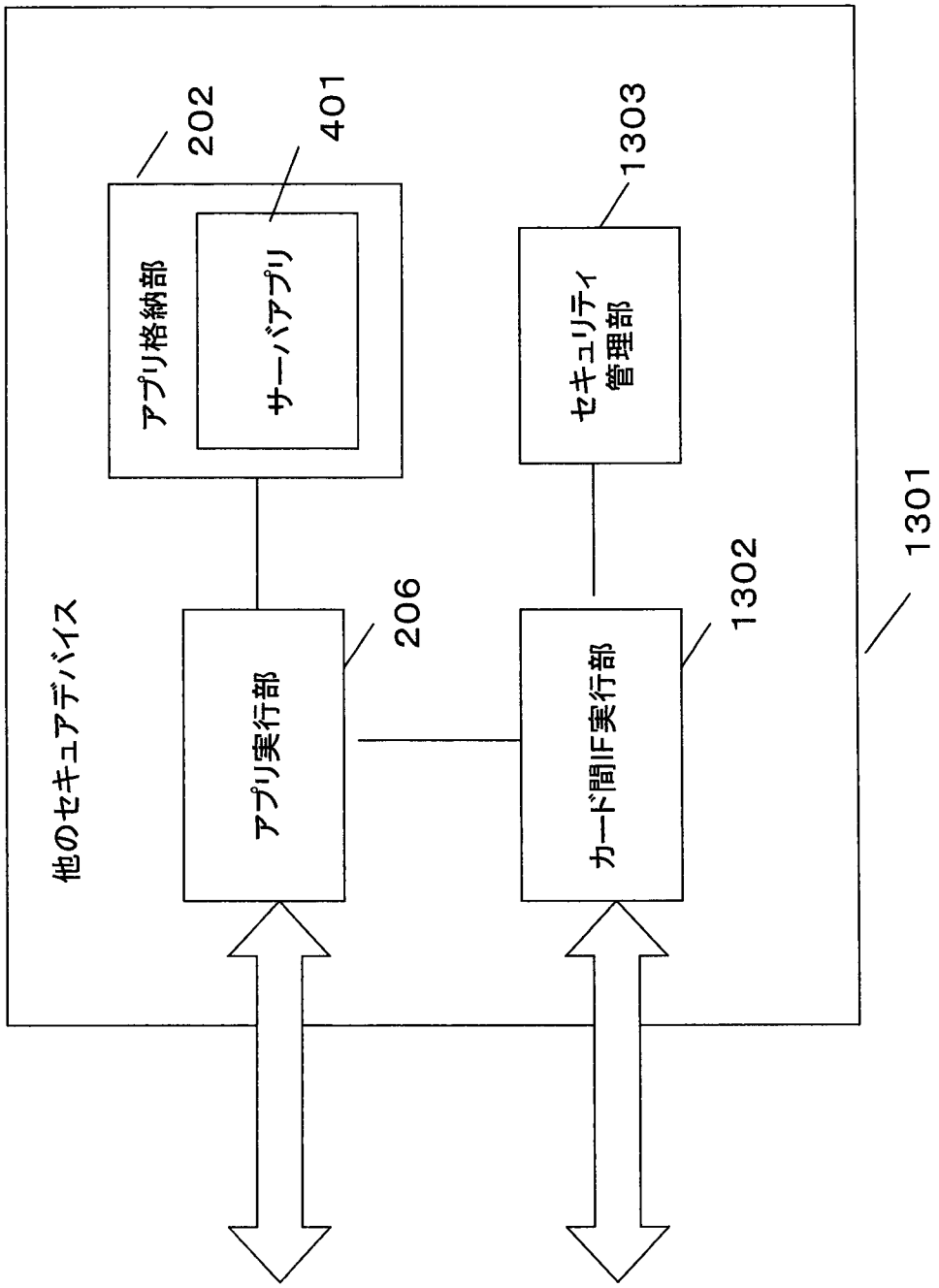
[図11b]


(b)
レスポンス 1105
データ部
・・・・・INS,オブジェクトID,メソッドID,パラメータ
SW
カードIF利用を依頼する旨
ヘッダ部
データ部
Le
CLA
INS
P1
P2
Lc
オブジェクトID
メソッドID
パラメータ
・・・・・
固定
固定
・・・・・
ホストとカードが共有しているIDをSHA-1でハッシュ化した先頭の2バイトを指定
参照崎の関数が提供している引数を指定
00h
INVOKEコマンド 1106
SW
9000h
レスポンス 1107
ヘッダ部
データ部
Le
共有コマンドのヘッダ
INVOKEコマンドの結果
00h
共有コマンド 1108
データ部
SW
コマンド1に対する処理結果
9000h
レスポンス 1109

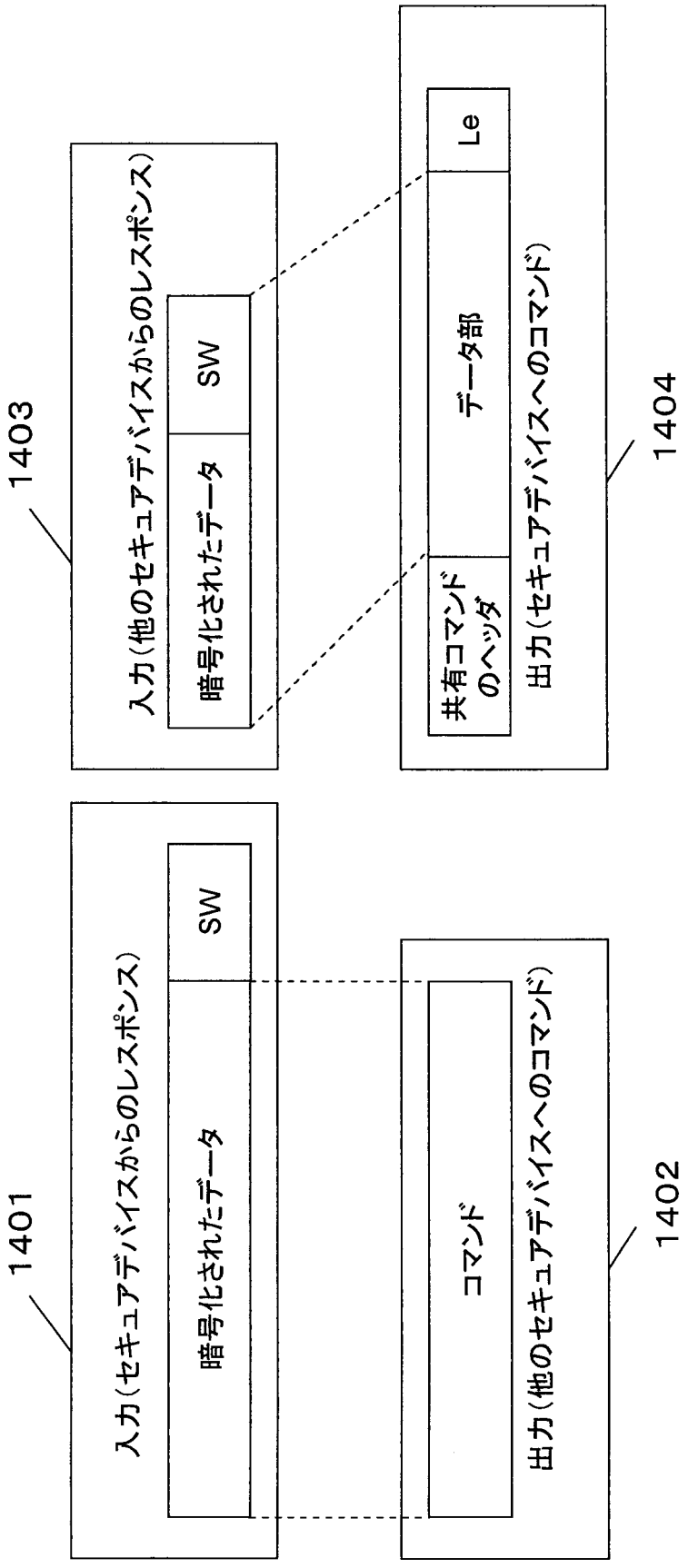
[図12]


セキュアデバイス
1201
アプリ格納部
202
アプリ
(ダウンロード中)
203
ダウンロード
後は307
他アプリ
(ダウンロード済み)
204
アドレス計算部
205
許可
コード発行部
207
許可コード
管理部
209
セキュリティ
管理部
1202
ダウンロード
管理部
201
参照先存在
判定部
208
カード間IF実行部
アプリ実行部
206
210

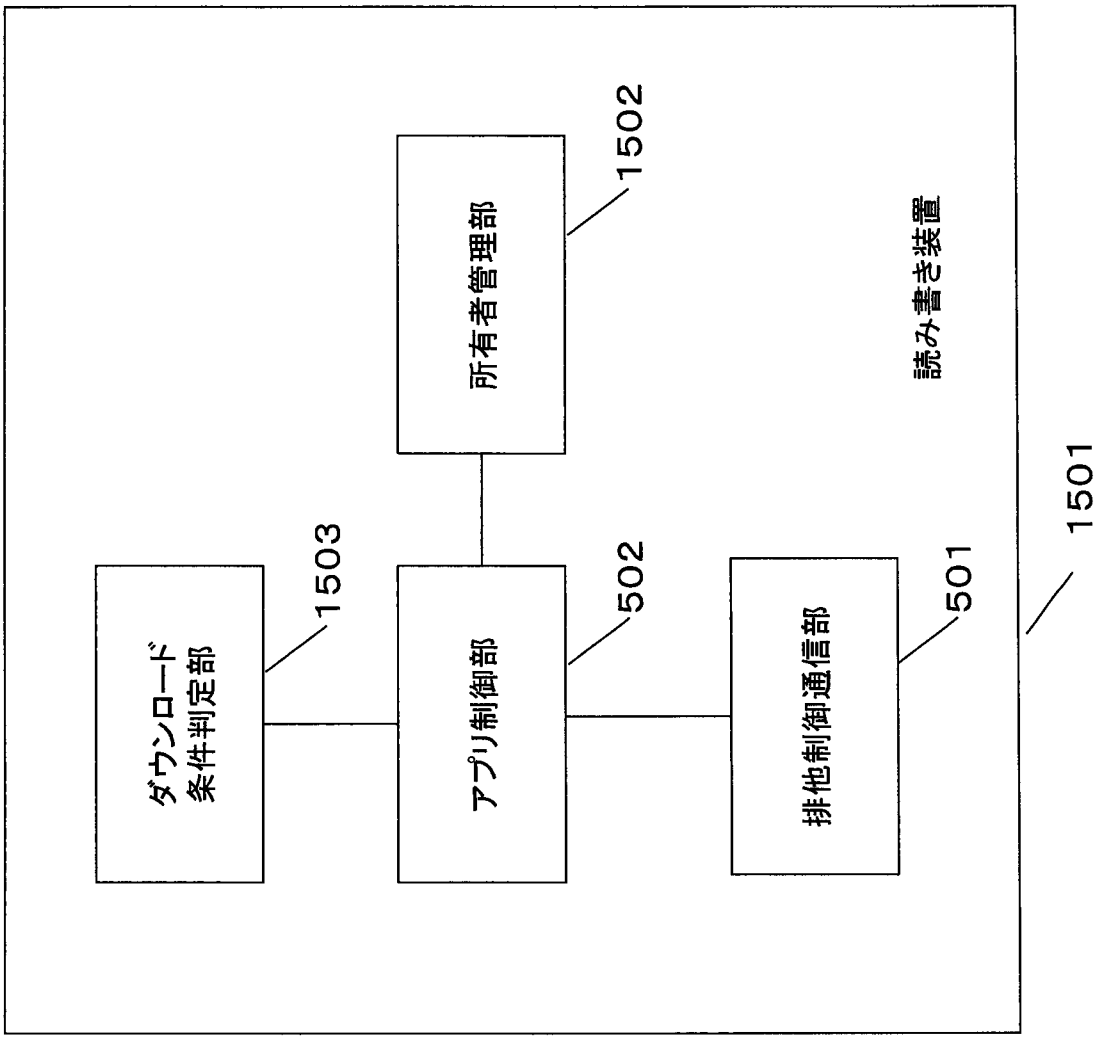
[図13]


202
401
1303
アプリ格納部
サーバアプリ
セキュリティ管理部
1301
206
1302
他のセキュアデバイス
アプリ実行部
カード間IF実行部

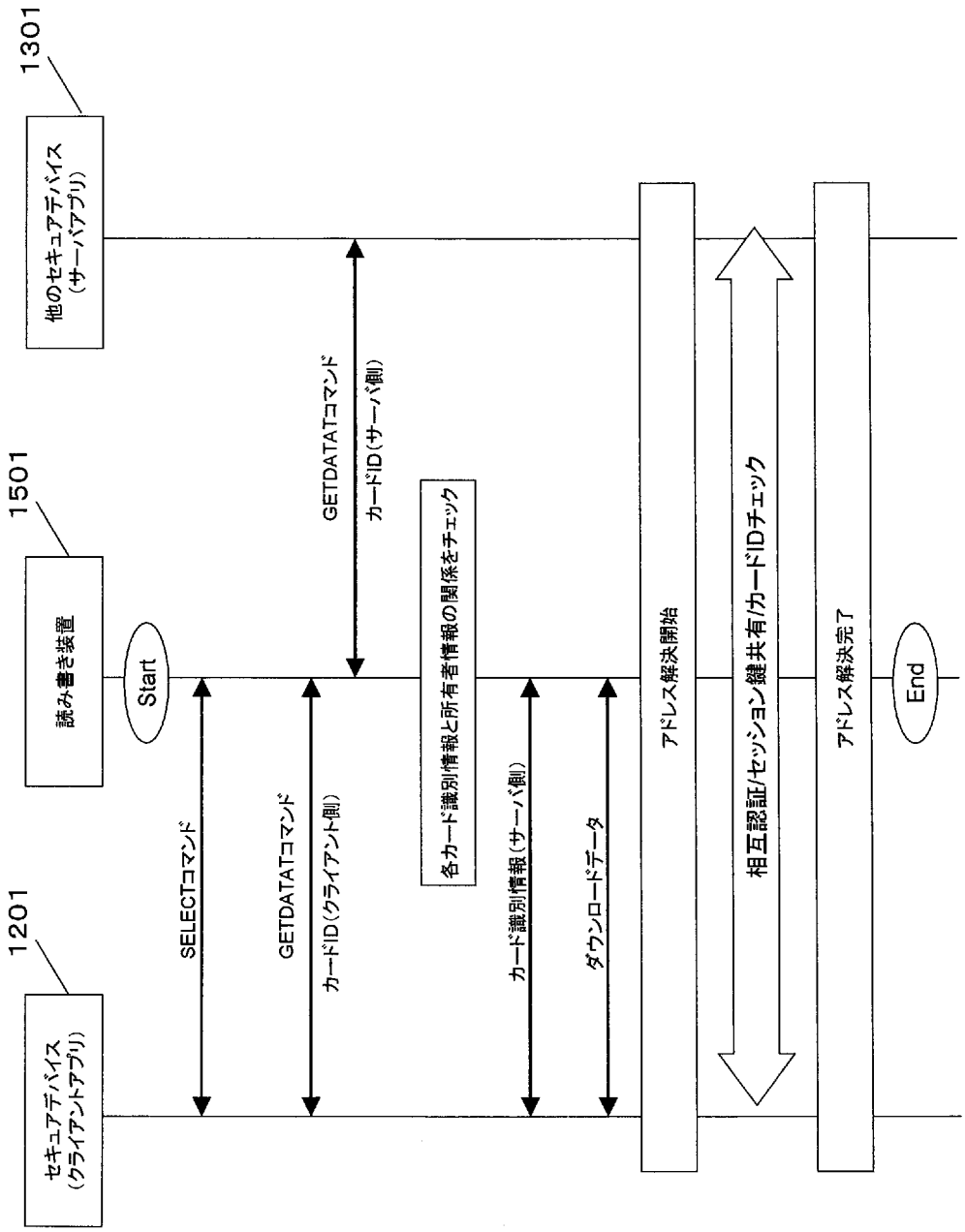
[図14]


1401
入力(セキュアデバイスからのレスポンス)
暗号化されたデータ
SW
1402
出力(他のセキュアデバイスへのコマンド)
コマンド
1403
入力(他のセキュアデバイスからのレスポンス)
暗号化されたデータ
SW
1404
出力(セキュアデバイスへのコマンド)
共有コマンドのヘッダ
データ部
Le

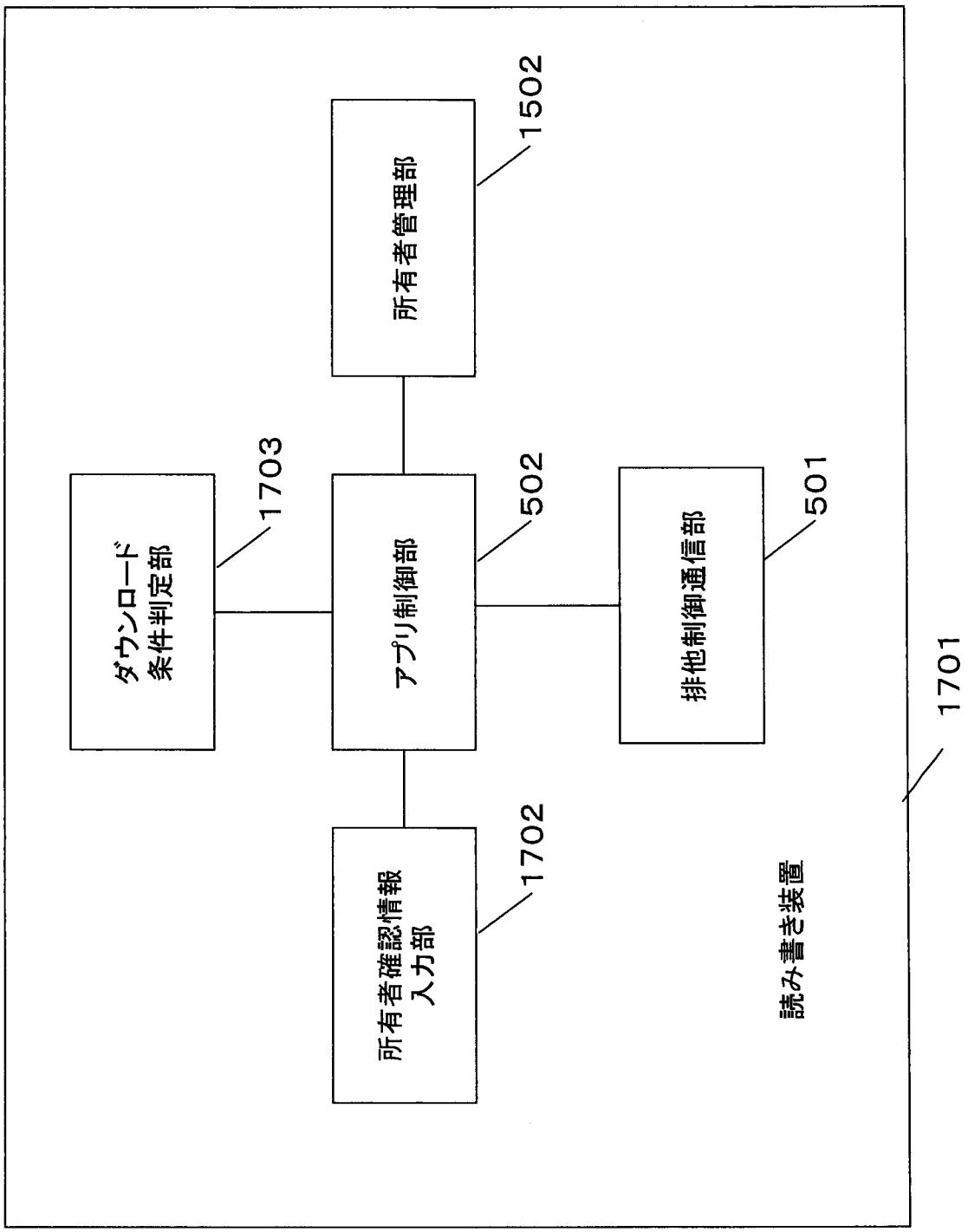
[図15]


読み書き装置
1501
所有者管理部
1502
ダウンロード
条件判定部
1503
アプリ制御部
502
排他制御通信部
501

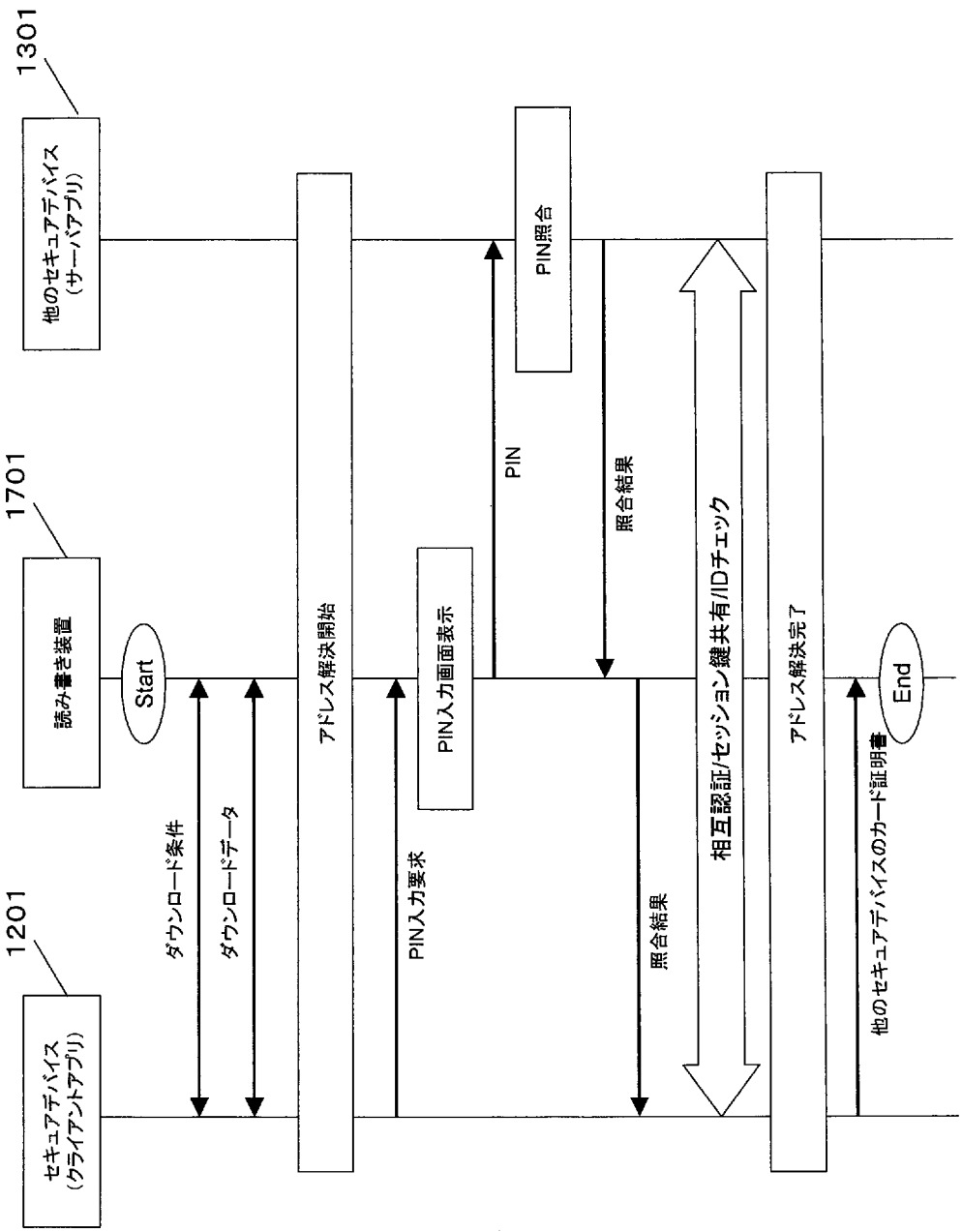
[図16]


1301
他のセキュアデバイス
(サーバアプリ)
1501
読み書き装置
Start
1201
セキュアデバイス
(クライアントアプリ)
SELECTコマンド
GETDATATコマンド
カードID(クライアント側)
GETDATATコマンド
カードID(サーバ側)
各カード識別情報と所有者情報の関係をチェック
カード識別情報(サーバ側)
ダウンロードデータ
アドレス解決開始
相互認証/セッション鍵共有/カードIDチェック
アドレス解決完了
End

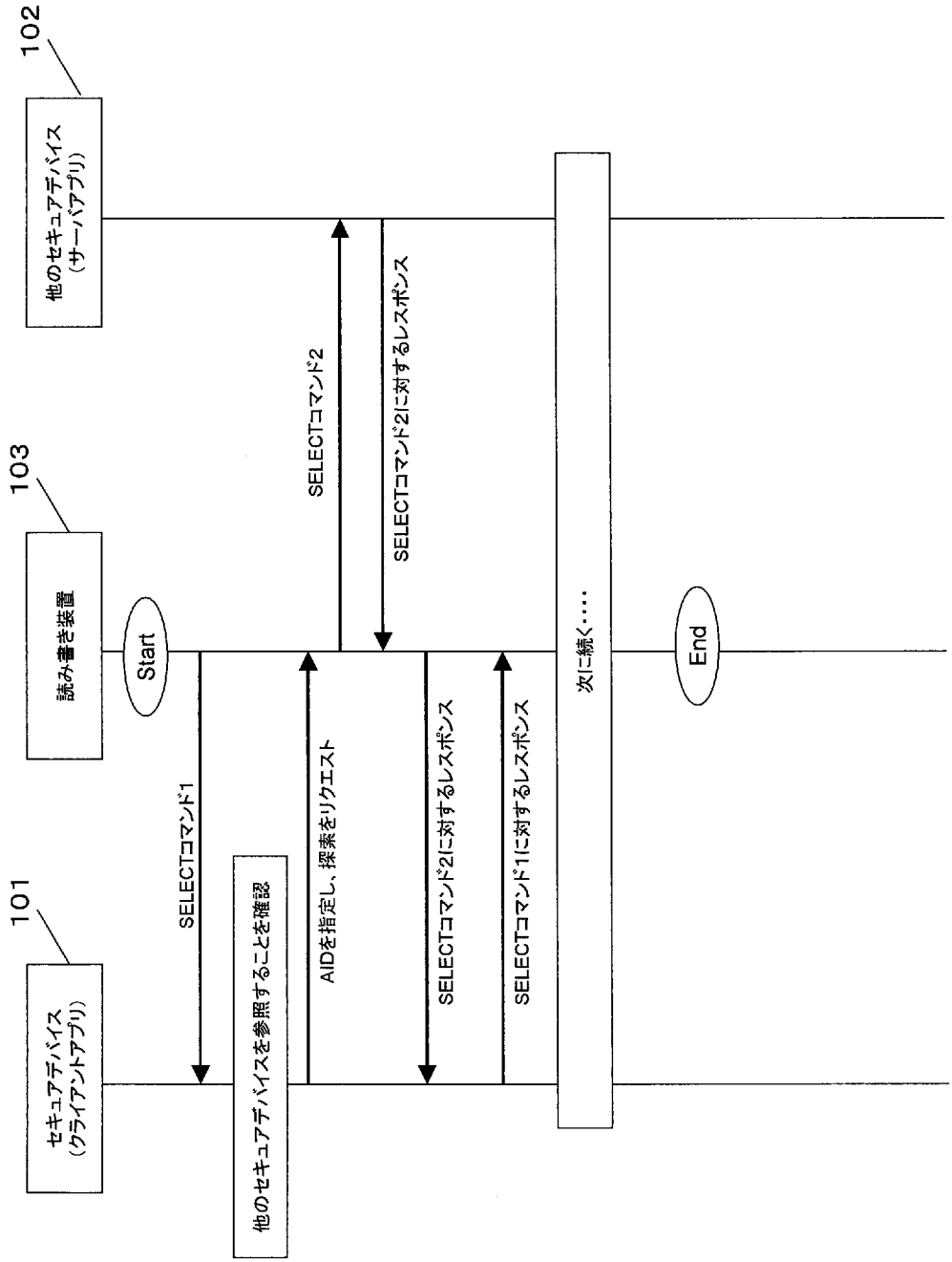
[図17]


所有者管理部
1502
ダウンロード
条件判定部
1703
アプリ制御部
502
排他制御通信部
501
所有者確認情報
入力部
1702
読み書き装置
1701

[図18]


1301
他のセキュアデバイス
(サーバアプリ)
1701
読み書き装置
1201
セキュアデバイス
(クライアントアプリ)
Start
End
ダウンロード条件
ダウンロードデータ
アドレス解決開始
PIN入力画面表示
PIN入力要求
PIN
PIN照合
照合結果
照合結果
相互認証/セッション鍵共有/IDチェック
アドレス解決完了
他のセキュアデバイスのカード証明書

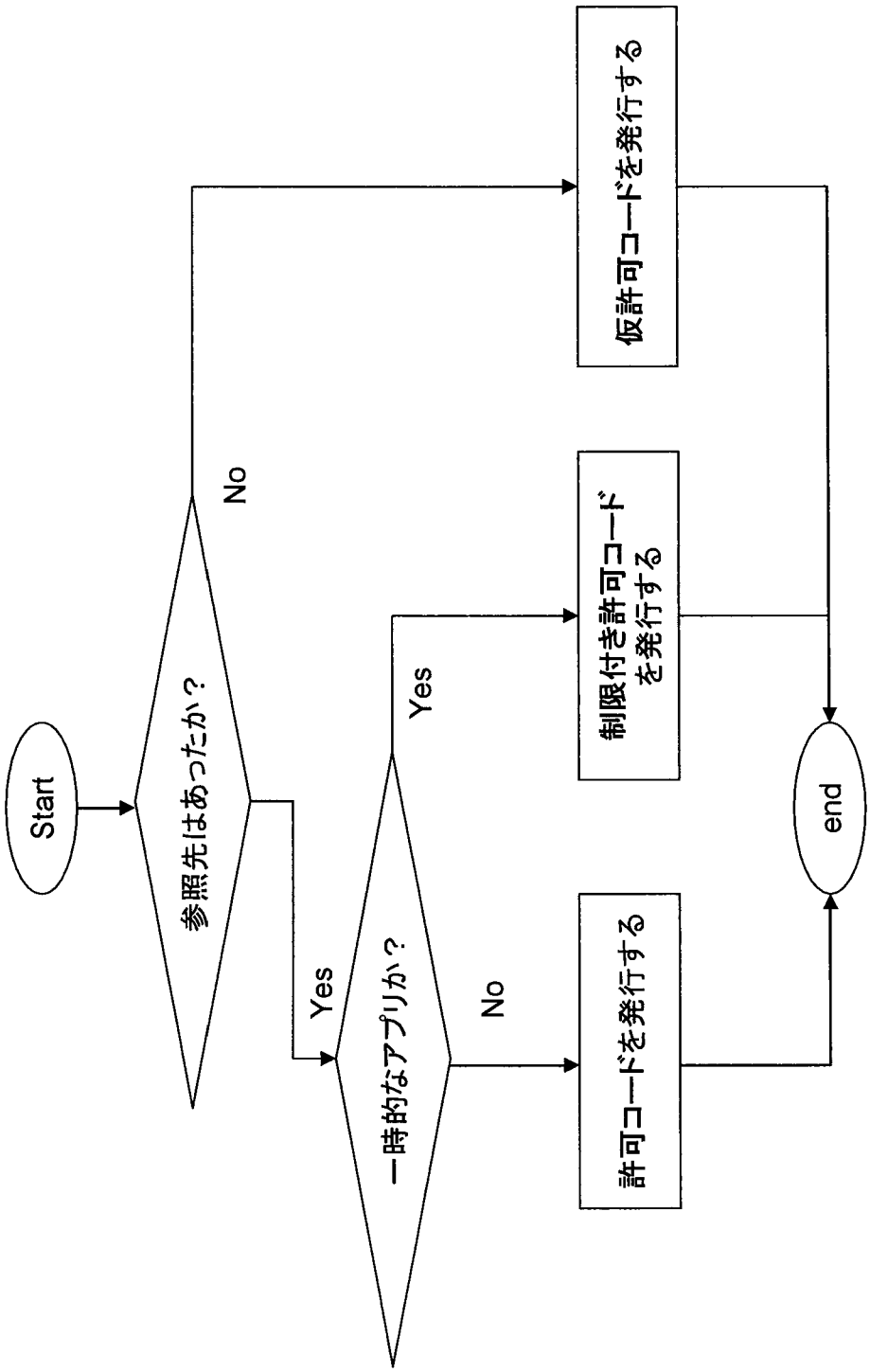
[図19]


102
他のセキュアデバイス
(サーバアプリ)
103
読み書き装置
101
セキュアデバイス
(クライアントアプリ)
Start
End
SELECTコマンド1
SELECTコマンド2
SELECTコマンド2に対するレスポンス
AIDを指定し、探索をリクエスト
SELECTコマンド2に対するレスポンス
SELECTコマンド1に対するレスポンス
他のセキュアデバイスを参照することを確認
次に続く・・・・

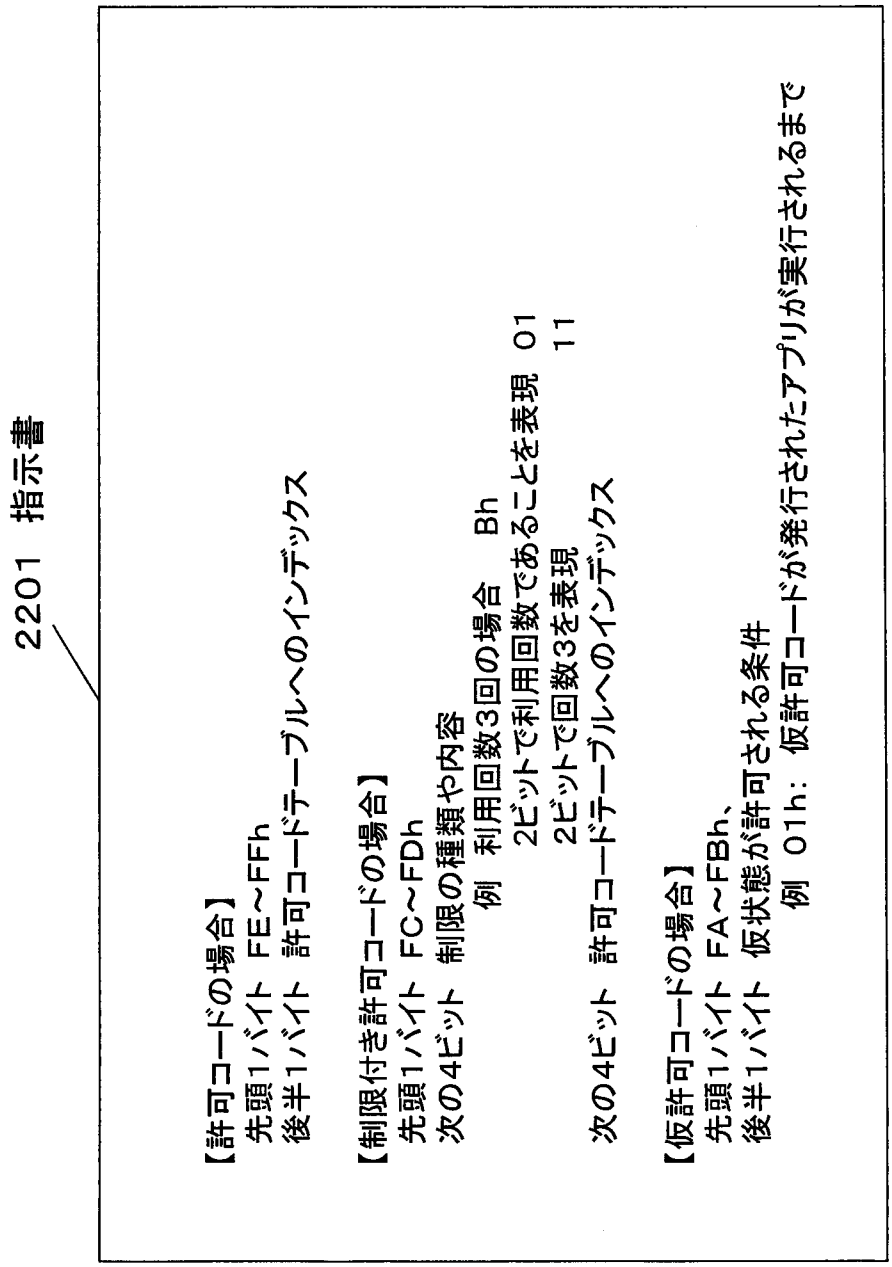
[図20]

インデックス	クライアントアプリの識別子	参照先アプリの識別子	メソッドID	引数の数
0	0102030405	102030405060	02	02
1	060708090a	102030405060	02	02
2	0b0c0d0e0f10	102030405060	02	02

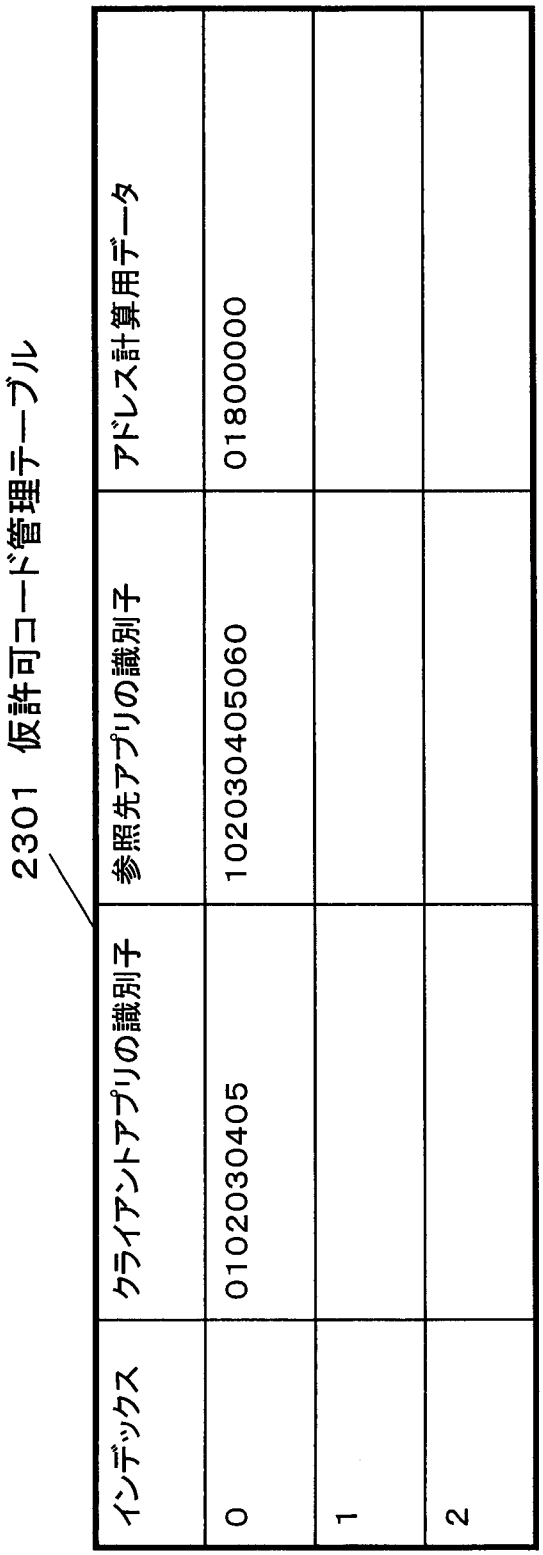
[図21]


Start
参照先はあったか？
No
Yes
一時的なアプリか？
Yes
No
仮許可コードを発行する
制限付き許可コードを発行する
許可コードを発行する
end

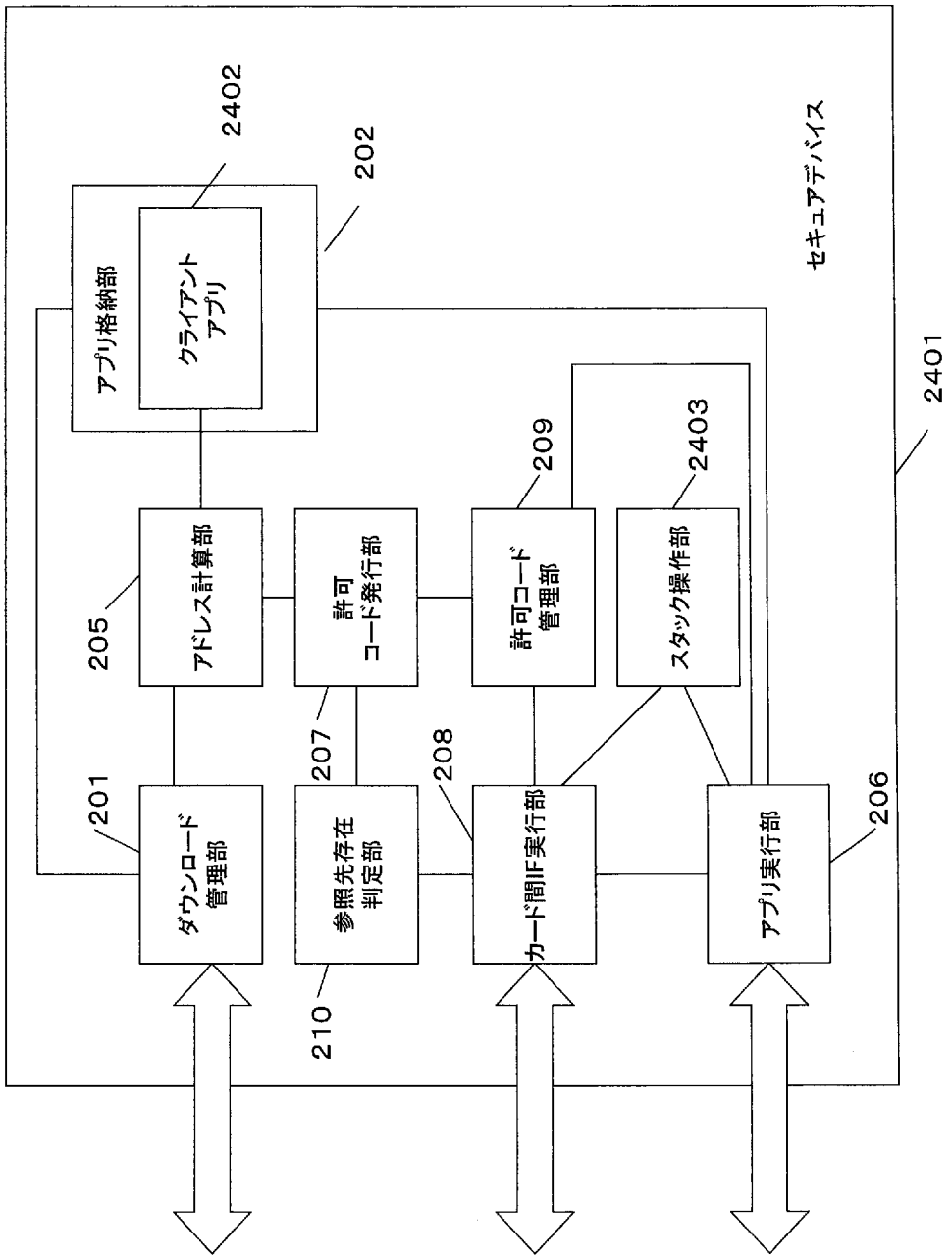
[図22]


2201 指示書
【許可コードの場合】
先頭1バイト FE～FFh
後半1バイト 許可コードテーブルへのインデックス
【制限付き許可コードの場合】
先頭1バイト FC～FDh
次の4ビット 制限の種類や内容
例 利用回数3回の場合 Bh
2ビットで利用回数であることを表現 01
2ビットで回数3を表現 11
次の4ビット 許可コードテーブルへのインデックス
【仮許可コードの場合】
先頭1バイト FA～FBh、
後半1バイト 仮状態が許可される条件
例 01h: 仮許可コードが発行されたアプリが実行されるまで

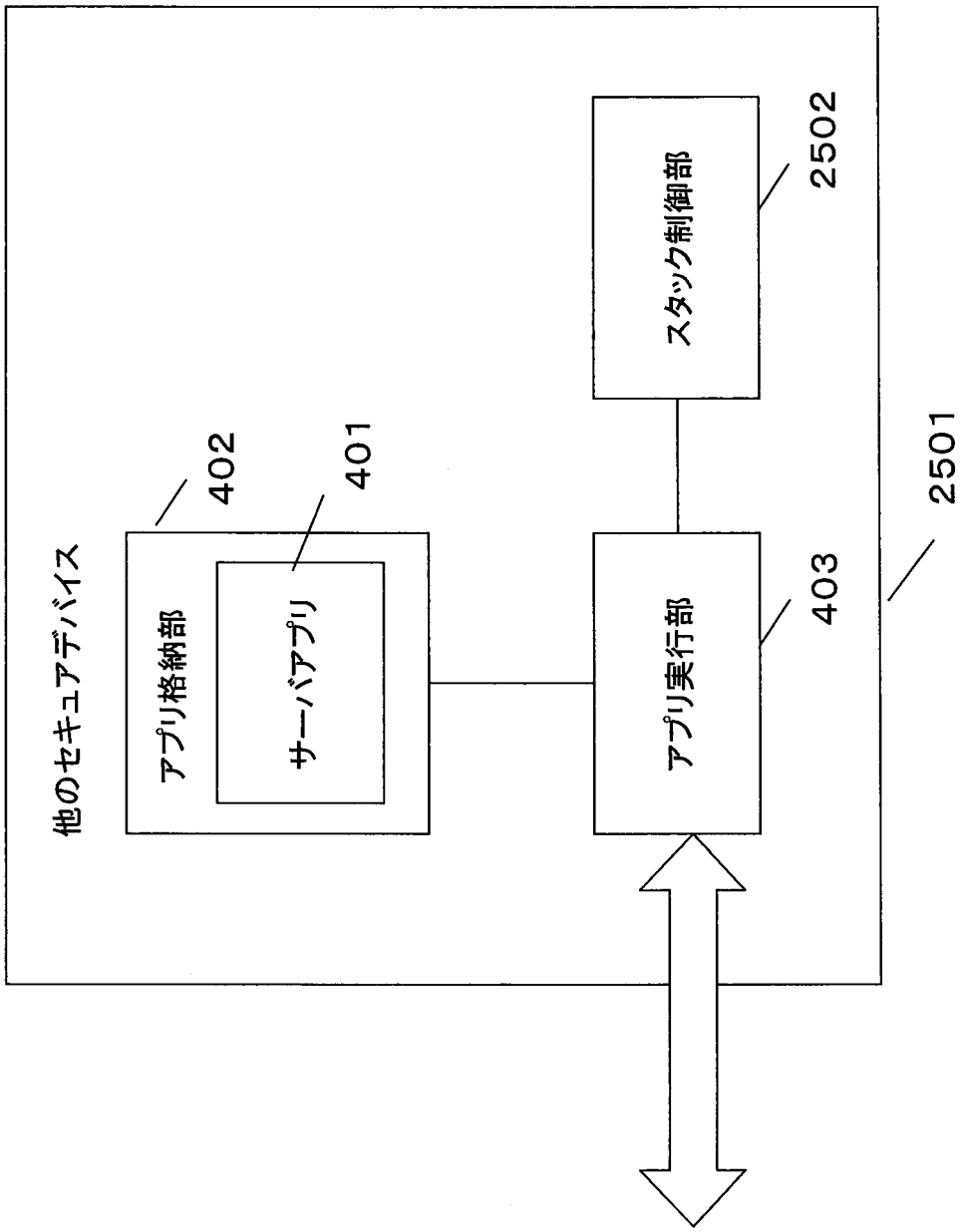
[図23]


2301 仮許可コード管理テーブル
インデックス
クライアントアプリの識別子
参照先アプリの識別子
アドレス計算用データ
0
0102030405
102030405060
01800000
1
2

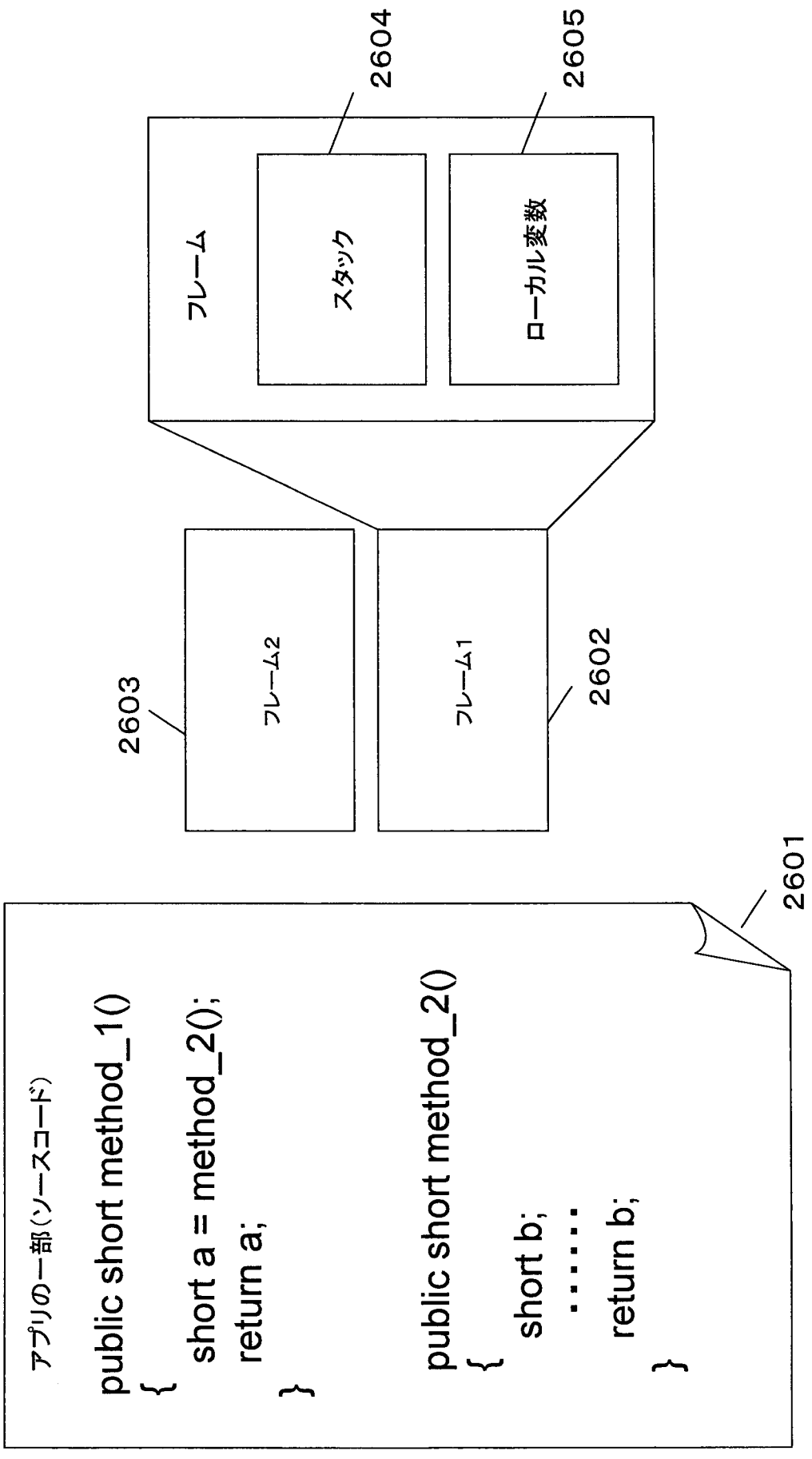
[図24]


セキュアデバイス
2401
アプリ格納部
クライアントアプリ
2402
202
アドレス計算部
205
許可コード発行部
許可コード管理部
209
スタック操作部
2403
ダウンロード管理部
201
参照先存在判定部
207
210
カード間IF実行部
208
アプリ実行部
206

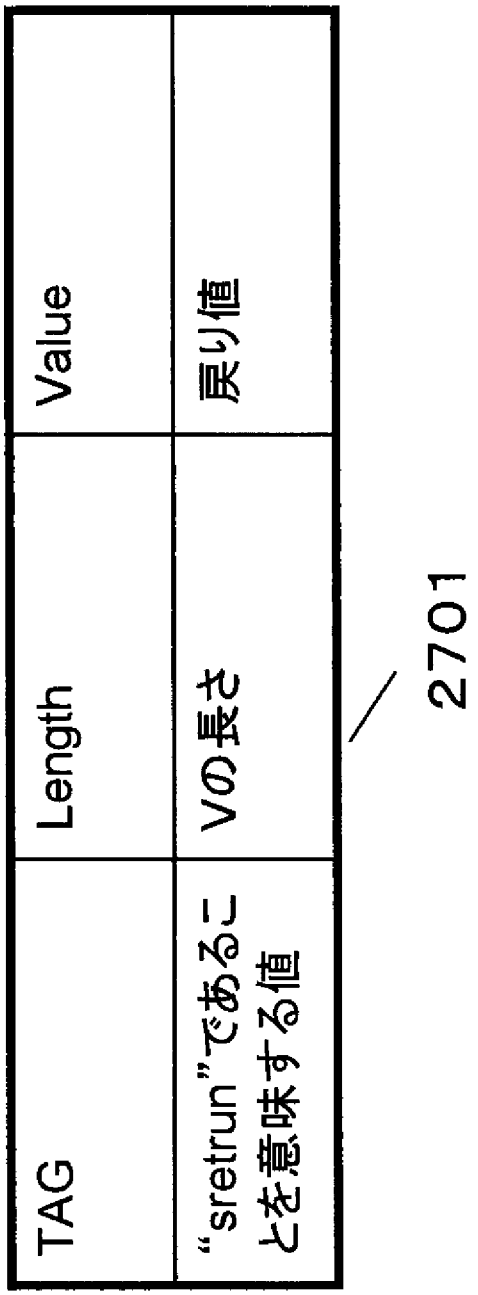
[図25]


他のセキュアデバイス
アプリ格納部
402
サーバアプリ
401
スタック制御部
2502
アプリ実行部
403
2501

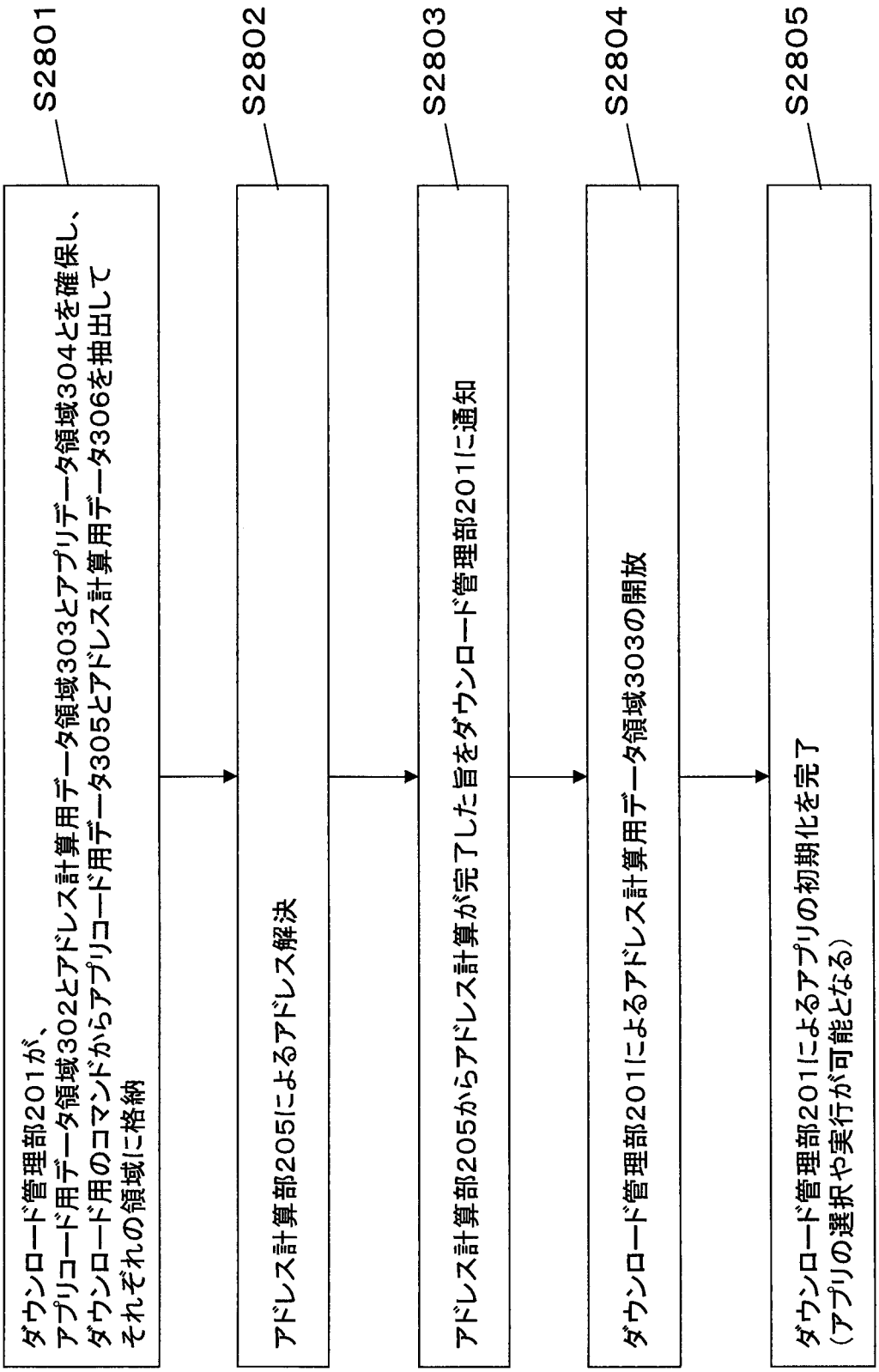
[図26]


アプリの一部(ソースコード)
public short method_1()
{
short a = method_2();
return a;
}
public short method_2()
{
short b;
……
return b;
}
2601
フレーム1
フレーム2
2602
2603
フレーム
スタック
ローカル変数
2604
2605

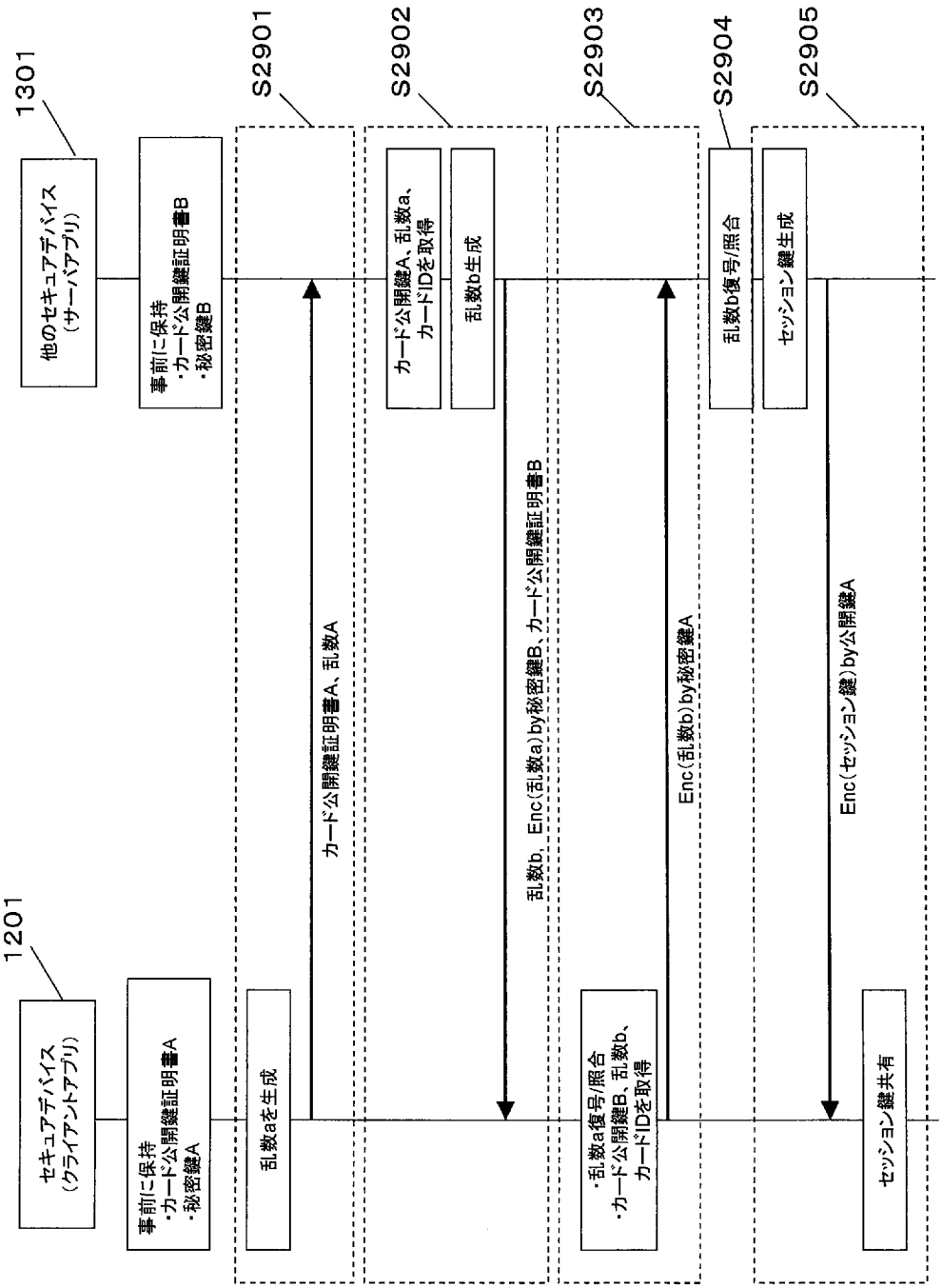
[図27]



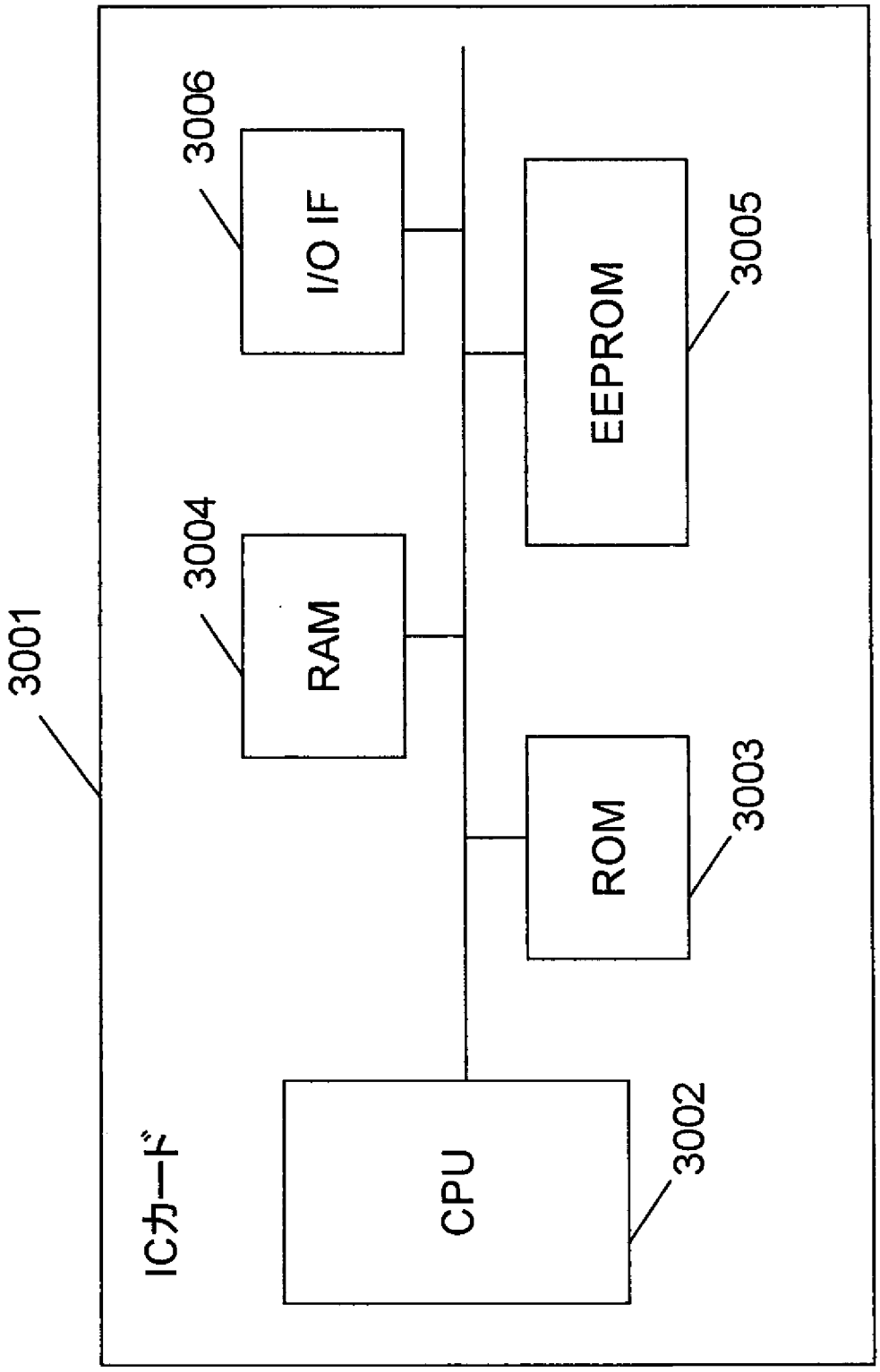
[図28]


S2801
ダウンロード管理部201が、
アプリコード用データ領域302とアドレス計算用データ領域303とアプリデータ領域304とを確保し、
ダウンロード用のコマンドからアプリコード用データ305とアドレス計算用データ306を抽出して
それぞれの領域に格納
S2802
アドレス計算部205によるアドレス解決
S2803
アドレス計算部205からアドレス計算が完了した旨をダウンロード管理部201に通知
S2804
ダウンロード管理部201によるアドレス計算用データ領域303の開放
S2805
ダウンロード管理部201によるアプリの初期化を完了
(アプリの選択や実行が可能となる)

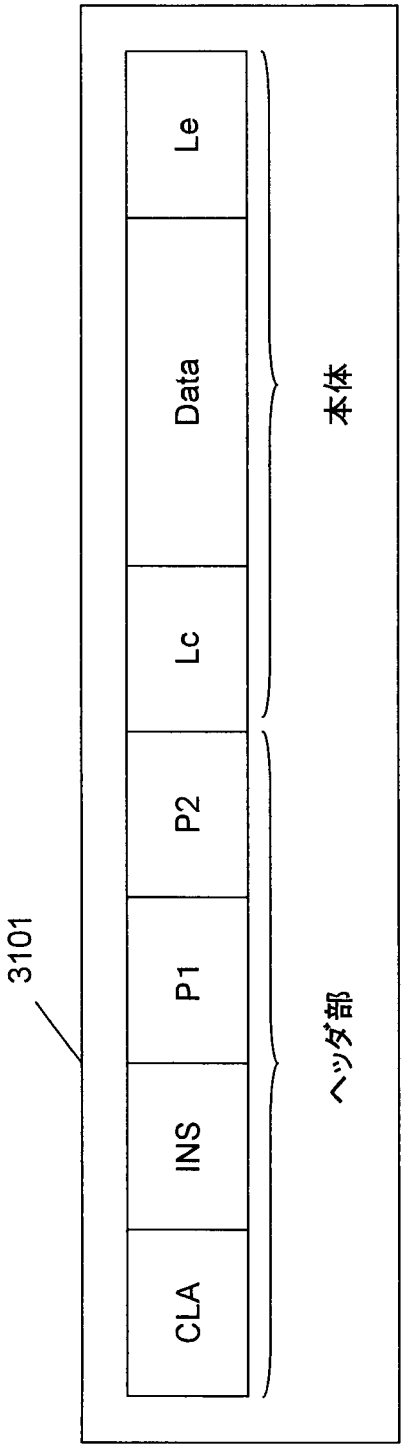
[図29]


1301
他のセキュアデバイス
(サーバアプリ)
事前に保持
・カード公開鍵証明書B
・秘密鍵B
S2901
S2902
S2903
S2904
S2905
カード公開鍵証明書A、乱数A
カード公開鍵A、乱数a、
カードIDを取得
乱数b生成
乱数b、Enc(乱数a)by秘密鍵B、カード公開鍵証明書B
乱数b復号/照合
セッション鍵生成
Enc(乱数b)by秘密鍵A
Enc(セッション鍵)by公開鍵A
1201
セキュアデバイス
(クライアントアプリ)
事前に保持
・カード公開鍵証明書A
・秘密鍵A
乱数aを生成
・乱数a復号/照合
・カード公開鍵B、乱数b、
カードIDを取得
セッション鍵共有

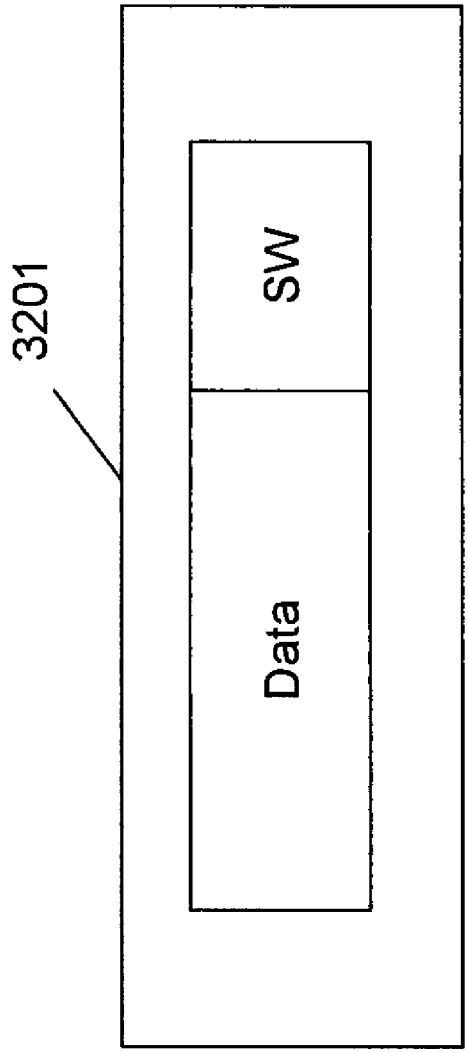
[図30]



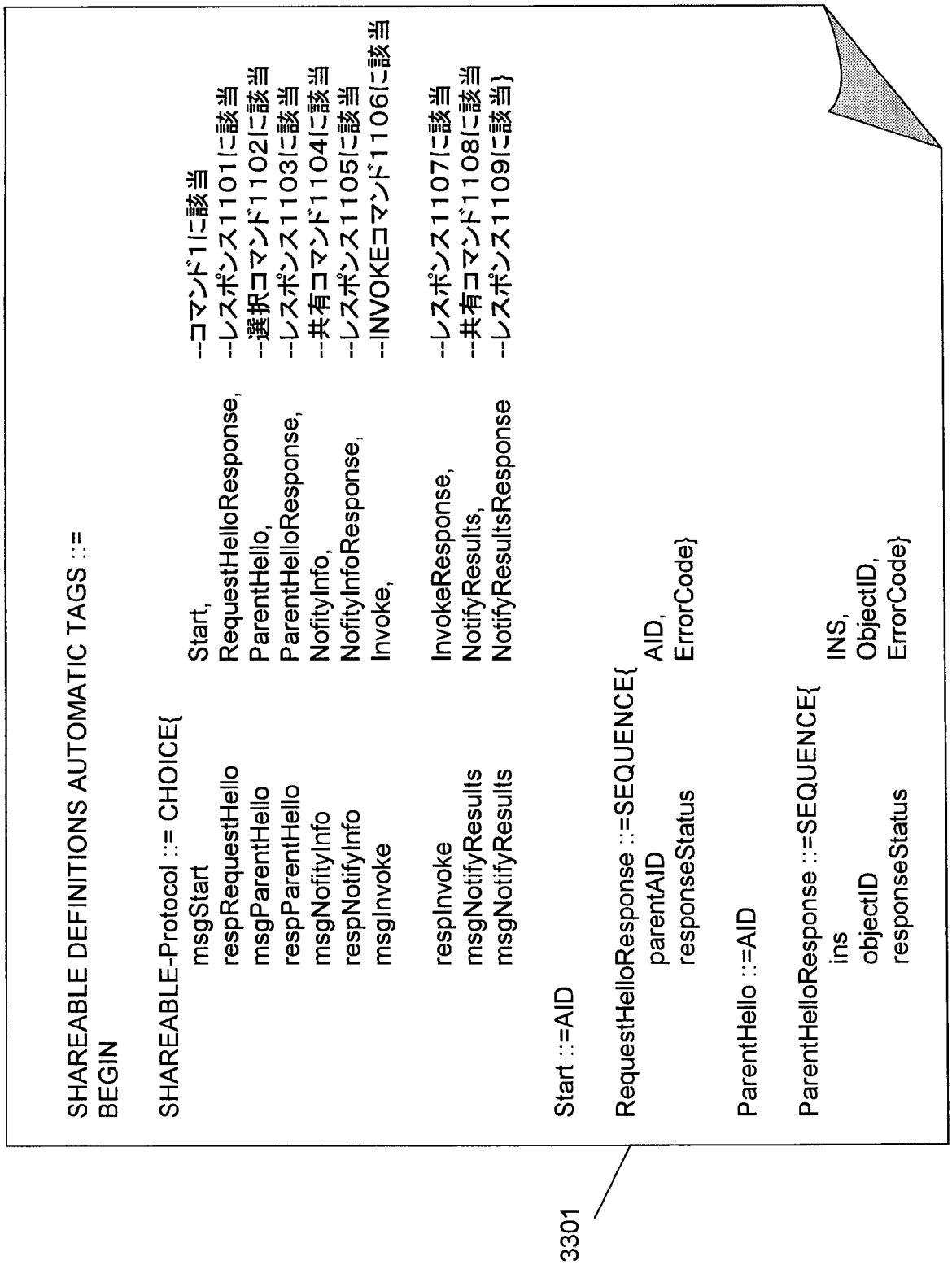
[図31]



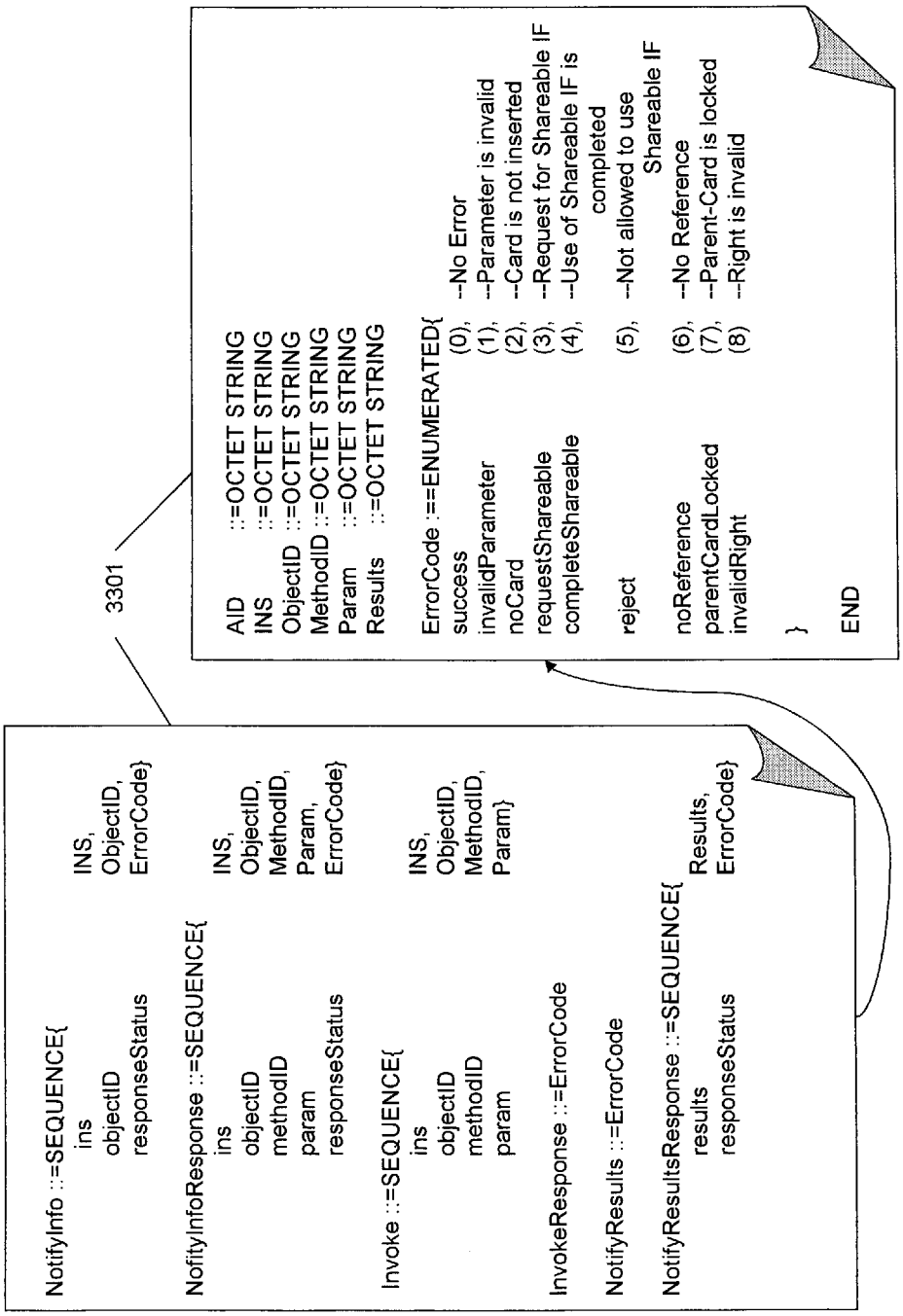
[図32]



[図33a]


SHAREABLE DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
SHAREABLE-Protocol ::= CHOICE{
msgStart Start, --コマンド1に該当
respRequestHello RequestHelloResponse, --レスポンス1101に該当
msgParentHello ParentHello, --選択コマンド1102に該当
respParentHello ParentHelloResponse, --レスポンス1103に該当
msgNofityInfo NofityInfo, --共有コマンド1104に該当
respNotifyInfo NofityInfoResponse, --レスポンス1105に該当
msgInvoke Invoke, --INVOKEコマンド1106に該当
respInvoke InvokeResponse, --レスポンス1107に該当
msgNotifyResults NotifyResults, --共有コマンド1108に該当
msgNotifyResults NotifyResultsResponse --レスポンス1109に該当}
Start ::=AID
RequestHelloResponse ::=SEQUENCE{
parentAID AID,
responseStatus ErrorCode}
ParentHello ::=AID
ParentHelloResponse ::=SEQUENCE{
ins INS,
objectID ObjectID,
responseStatus ErrorCode}
3301

[図33b]


NotifyInfo ::=SEQUENCE{
ins INS,
objectID ObjectID,
responseStatus ErrorCode}
NotifyInfoResponse ::=SEQUENCE{
ins INS,
objectID ObjectID,
methodID MethodID,
param Param,
responseStatus ErrorCode}
Invoke ::=SEQUENCE{
ins INS,
objectID ObjectID,
methodID MethodID,
param Param}
InvokeResponse ::=ErrorCode
NotifyResults ::=ErrorCode
NotifyResultsResponse ::=SEQUENCE{
results Results,
responseStatus ErrorCode}
3301
AID ::=OCTET STRING
INS ::=OCTET STRING
ObjectID ::=OCTET STRING
MethodID ::=OCTET STRING
Param ::=OCTET STRING
Results ::=OCTET STRING
ErrorCode ::=ENUMERATED{
success (0), --No Error
invalidParameter (1), --Parameter is invalid
noCard (2), --Card is not inserted
requestShareable (3), --Request for Shareable IF
completeShareable (4), --Use of Shareable IF is completed
reject (5), --Not allowed to use Shareable IF
noReference (6), --No Reference
parentCardLocked (7), --Parent-Card is locked
invalidRight (8) --Right is invalid
}
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/056982

A. CLASSIFICATION OF SUBJECT MATTER
G06K19/07(2006.01)i, *G06F21/24*(2006.01)i, *G06K17/00*(2006.01)i, *G06K19/10*(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)
G06K19/07, G06F21/24, G06K17/00, G06K19/10

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 A	JP 2001-188884 A (Nippon Telegraph And Telephone Corp.), 10 July, 2001 (10.07.01), Par. Nos. [0016] to [0031] (Family: none)	1,15 2-14,16
A	JP 2002-216085 A (Hitachi, Ltd.), 02 August, 2002 (02.08.02), Par. Nos. [0060] to [0065] & US 2002/134843 A1	1,2
A	JP 2002-73196 A (Dainippon Printing Co., Ltd.), 12 March, 2002 (12.03.02), Par. Nos. [0008] to [0024] (Family: none)	3,4,5

☒ 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
04 July, 2007 (04.07.07)	17 July, 2007 (17.07.07)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/056982

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-196625 A (Dainippon Printing Co., Ltd.), 11 July, 2003 (11.07.03), Par. No. [0026] (Family: none)	6

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０５６９８２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06K19/07(2006.01)i, G06F21/24(2006.01)i, G06K17/00(2006.01)i, G06K19/10(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.　G06K19/07, G06F21/24, G06K17/00, G06K19/10

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 A	ＪＰ　２００１－１８８８８４　Ａ（日本電信電話株式会社）、２００１．０７．１０，【００１６】－【００３１】（ファミリーなし）	1, 15 2-14, 16
A	ＪＰ　２００２－２１６０８５　Ａ（株式会社日立製作所）、２００２．０８．０２，【００６０】－【００６５】＆　ＵＳ　２００２／１３４８４３　Ａ１	1, 2
A	ＪＰ　２００２－７３１９６　Ａ（大日本印刷株式会社）、２００２．０３．１２，【０００８】－【００２４】（ファミリーなし）	3, 4, 5

☑　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
０４．０７．２００７	１７．０７．２００７

国際調査機関の名称及びあて先
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

特許庁審査官（権限のある職員）　５Ｎ　８６２７
大塚　良平
電話番号　０３－３５８１－１１０１　内線　３５８６

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
Ａ	ＪＰ　２００３－１９６６２５　Ａ（大日本印刷株式会社）、２００３．０７．１１，【００２６】（ファミリーなし）	６