(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
2023年2月9日(09.02.2023)

WIPO | PCT

(10) 国際公開番号
WO 2023/013102 A1

(51) 国際特許分類:
G06F 21/62 (2013.01) *G06F 21/44* (2013.01)

(21) 国際出願番号： PCT/JP2022/003807

(22) 国際出願日： 2022年2月1日(01.02.2022)

(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 2021-129455 2021年8月6日(06.08.2021) JP

(71) 出願人: フェリカネットワークス株式会社 (**FELICA NETWORKS, INC.**) [JP/JP]; 〒1410032 東京都品川区大崎１丁目１１番１号 Tokyo (JP).

(72) 発明者: 野中 章裕 (**NONAKA, Akihiro**); 〒1410032 東京都品川区大崎１丁目１１番１号 フェリカネットワークス株式会社内 Tokyo (JP). 加藤 晋一(**KATO, Shinichi**); 〒1410032 東京都品川区大崎１丁目１１番１号 フェリカネットワークス株式会社内 Tokyo (JP). 松崎 雄基(**MATSUZAKI, Yuki**); 〒1410032 東京都品川区大崎１丁目１１番１号 フェリカネットワークス株式会社内 Tokyo (JP).

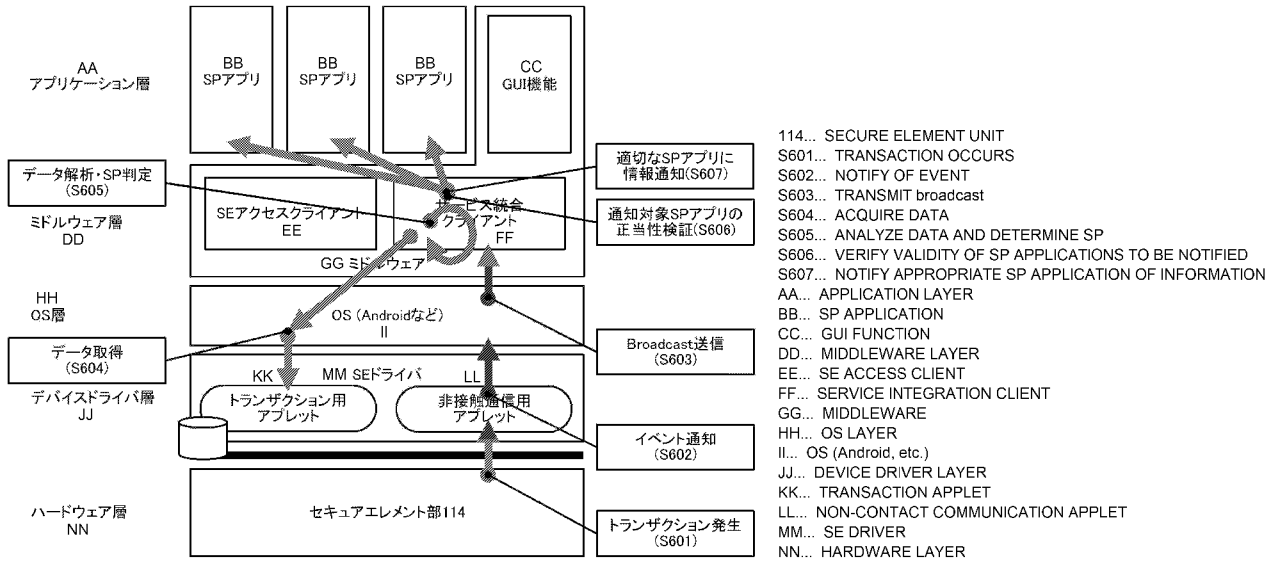
(74) 代理人: 山田 英治, 外 (**YAMADA, Eiji** et al.); 〒1040032 東京都中央区八丁堀三丁目２５番９号 Ｄａｉｗａ八丁堀駅前ビル西館８階 特許業務法人 大同特許事務所 Tokyo (JP).

(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, AO, AT, AU, AZ,

(54) **Title:** INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND COMPUTER PROGRAM

(54) 発明の名称： 情報処理装置及び情報処理方法、並びにコンピュータプログラム

[図6]



(57) **Abstract:** Provided is an information processing apparatus equipped with a secure element. In the present invention, an external information processing apparatus is provided with: a detection unit that detects when a transaction occurs between a device mounted on a main body and an external apparatus; an acquisition unit that acquires data from the device in response to the detection of the occurrence of the transaction by the detection unit; a determination unit that analyzes the data acquired by the acquisition unit to determine applications to be notified; a verification unit that verifies the validity of the applications to be notified; and a notification unit that notifies an appropriate application that is among the applications to be notified and the validity of which has been confirmed, of the data acquired by the acquisition unit.

WO 2023/013102 A1

［続葉有］

BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

— 国際調査報告（条約第21条(3)）

(57) 要約：セキュアエレメントを搭載する情報処理装置を提供する。 外情報処理装置は、本体に搭載するデバイスと外部装置間でトランザクションが発生したことを検知する検知部と、前記検知部が前記トランザクションの発生を検知したことに応じて、前記デバイスからデータを取得する取得部と、前記取得部が取得したデータを解析して、通知対象のアプリケーションを判定する判定部と、前記通知対象のアプリケーションの正当性を検証する検証部と、前記通知対象のうち正当性が確認された適切なアプリケーションに、前記取得部が取得したデータを通知する通知部を具備する。

明　細　書

発明の名称 ：

情報処理装置及び情報処理方法、並びにコンピュータプログラム

技術分野

[0001] 本明細書で開示する技術（以下、「本開示」とする）は、外部装置とトランザクションを行うデバイスを搭載する情報処理装置及び情報処理方法、並びにコンピュータプログラムに関する。

背景技術

[0002] ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）チップ又はＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）タグ、ＩＣカードなどのセキュアエレメント（ＳＥ）を利用したサービスは広く普及している。セキュアエレメントは、耐タンパ性のあるハードウェアで保護されたデバイスであり、リーダライタとの間では相互認証と暗号化を用いてセキュアな非接触通信が可能である。なお、非接触通信には、近距離無線通信規格であるＮＦＣ（Ｎｅａｒ　Ｆｉｅｌｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ）などに則った通信方式を利用することができるが、本明細書では詳細な説明を省略する。

[0003] 最近では、セキュアエレメントを搭載するスマートフォンなどの情報端末が増えてきている。この種の情報端末をリーダライタにかざすと、情報端末内のセキュアエレメントとリーダライタ間でトランザクション（セキュアエレメント内のメモリに対するデータの読み出し及び書き込みなど）が行われることにより、公共交通機関の乗車券機能、電子マネー又は決済機能、クレジットカード機能、映画や劇場などの娯楽施設のチケット機能、個人認証機能といった、セキュアエレメントを利用したサービス機能（以下、単に「サービス機能」とも呼ぶ）を実現することができる。

[0004] 情報端末上では、各サービス機能の提供元であるプロバイダ（サービスプロバイダ：ＳＰ）から配布されるアプリケーションプログラム（以下、「Ｓ

Ｐアプリ」とも呼ぶ）をインストールし、ＳＰアプリを起動することによって、該当するサービス機能に関するサービスプロバイダへの手続き（電子マネーのチャージなど）や、サービス機能に対する操作（利用履歴や残高の表示など）を行うことができる。他方、情報端末内のセキュアエレメントとリーダライタ間のトランザクションは、例えばユーザが情報端末をリーダライタにかざすという手動操作によって発生し、その際にＳＰアプリの起動が不要で、ＳＰアプリへの予告もない。このため、ＳＰアプリにおいて残高表示などを実施するには、ＳＰアプリがセキュアエレメントとリーダライタ間で行われたトランザクションの情報を把握する必要がある。

[0005] 例えば、トランザクションに関する情報をセキュアエレメント内の第２の記憶部に格納し、情報処理装置側のデータ取得部が第２の記憶部から読み出した情報に基づいてトランザクションが実施されたタイミングでの当該装置の位置や周辺状況、使用者、当該装置の動作や使用者の動作などを解析する情報処理装置が提案されている（特許文献１を参照のこと）。しかしながら、データ取得部において行われるトランザクション情報の解析処理はミドルウェアで実施されると思料され、この情報処理装置上ではＳＰアプリがセキュアエレメントとリーダライタ間で行われたトランザクションの情報を把握することはできない。

先行技術文献

特許文献

[0006] 特許文献1：ＷＯ２０１９／１２３８５１

発明の概要

発明が解決しようとする課題

[0007] 本開示の目的は、本体内のデバイスと外部装置間で実施されたトランザクションに関する情報を処理する情報処理装置及び情報処理方法、並びにコンピュータプログラムを提供することにある。

課題を解決するための手段

[0008] 本開示は、上記課題を参酌してなされたものであり、その第１の側面は、外部装置とトランザクションを行うデバイスを搭載する情報処理装置であって、

前記デバイスと前記外部装置間でトランザクションが発生したことを検知する検知部と、

前記検知部が前記トランザクションの発生を検知したことに応じて、前記デバイスからデータを取得する取得部と、

前記取得部が取得したデータを解析して、通知対象のアプリケーションを判定する判定部と、

前記通知対象のアプリケーションの正当性を検証する検証部と、

前記通知対象のうち正当性が確認された適切なアプリケーションに、前記取得部が取得したデータを通知する通知部と、

を具備する情報処理装置である。

[0009] 前記取得部は、前記トランザクションの処理対象データ及び前記トランザクションの処理に関するデータを取得する。また、前記判定部は、前記取得部が取得したデータに基づいて前記トランザクションに関連するサービスＩＤを特定し、前記サービスＩＤに基づいて通知対象のアプリケーションを判定する。

[0010] 前記検証部は、サーバから取得したアプリケーションの検証情報とオペレーティングシステムから取得したアプリケーションの情報に基づいて、アプリケーションの正当性を検証する。検証情報は、アプリケーションのパッケージ名及び署名値を含む。

[0011] 前記通知部は、サーバから取得したアプリケーション毎の情報に基づいて前記適切なアプリケーションへの通知を行う。サーバから取得したアプリケーション毎の前記情報は、通知の優先度、通知期限、通知期限を超過時の動作のうち少なくとも１つを含む。

[0012] また、本開示の第２の側面は、外部装置とトランザクションを行うデバイスを搭載する機器における情報処理方法であって、

前記デバイスと前記外部装置間でトランザクションが発生したことを検知する検知ステップと、

前記検知ステップにおいて前記トランザクションの発生を検知したことに応じて、前記デバイスからデータを取得する取得ステップと、

前記取得ステップにおいて取得したデータを解析して、通知対象のアプリケーションを判定する判定ステップと、

前記通知対象のアプリケーションの正当性を検証する検証ステップと、

前記通知対象のうち正当性が確認された適切なアプリケーションに、前記取得において取得したデータを通知する通知ステップと、

を有する情報処理方法である。

[0013] また、本開示の第３の側面は、外部装置とトランザクションを行うデバイスを搭載する情報処理装置を、

前記デバイスの前記外部装置間でトランザクションが発生したことを検知する検知部、

前記検知部が前記トランザクションの発生を検知したことに応じて、前記デバイスからデータを取得する取得部、

前記取得部が取得したデータを解析して、通知対象のアプリケーションを判定する判定部、

前記通知対象のアプリケーションの正当性を検証する検証部、

前記通知対象のうち正当性が確認された適切なアプリケーションに、前記取得部が取得したデータを通知する通知部、

として機能させるようにコンピュータ可読形式で記述されたコンピュータプログラムである。

[0014] 本開示の第３の側面に係るコンピュータプログラムは、コンピュータ上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータプログラムを定義したものである。換言すれば、本開示の第３に係るコンピュータプログラムをコンピュータにインストールすることによって、コンピュータ上では協働的作用が発揮され、本開示の第１の側面に係る情報処理

装置と同様の作用効果を得ることができる。

[0015] また、本開示の第４の側面は、外部装置とトランザクションを行うデバイスを搭載するとともに、前記トランザクションに関連するサービスを提供するアプリケーションをインストールした情報処理装置であって、

前記アプリケーションに前記トランザクションの処理対象データを通知する通知部と、

前記アプリケーションが受信した処理対象データに関する前記情報を提示する提示部と、

を具備する情報処理装置である。

[0016] また、本開示の第５の側面は、外部装置とトランザクションを行うデバイスを搭載するとともに、前記トランザクションに関連するサービスを提供するアプリケーションをインストールした機器において、前記アプリケーションによって実行される情報処理方法であって、

前記トランザクションの処理対象データを受信する受信ステップと、

前記受信した処理対象データに関する情報を提示する提示ステップと、

を有する情報処理方法である。

[0017] また、本開示の第６の側面は、外部装置とトランザクションを行うデバイスを搭載するとともに、前記トランザクションに関連するサービスを提供するアプリケーションをインストールした情報処理装置を、

前記トランザクションの処理対象データを受信する受信部、

前記受信した処理対象データに関する情報を提示する提示部、

として機能させるようにコンピュータ可読形式で記述されたコンピュータプログラムである。

発明の効果

[0018] 本開示によれば、本体内のデバイスと外部装置間で実施されたトランザクションに関する情報を適切なアプリケーションに通知する情報処理装置及び情報処理方法、並びにコンピュータプログラムを提供することができる。

[0019] なお、本明細書に記載された効果は、あくまでも例示であり、本開示によ

りもたらされる効果はこれに限定されるものではない。また、本開示が、上記の効果以外に、さらに付加的な効果を奏する場合もある。

[0020] 本開示のさらに他の目的、特徴や利点は、後述する実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

図面の簡単な説明

[0021] [図1]図１は、情報処理装置１００のハードウェア構成例を示した図である。

[図2]図２は、セキュアエレメント部１１４の内部構成を示した図である。

[図3]図３は、セキュアエレメント部１１４内のメモリ２０４においてトランザクションの処理対象データを格納するデータ構造を示した図である。

[図4]図４は、トランザクション処理に関するデータの構成例を示した図である。

[図5]図５は、情報処理装置１００上で動作するソフトウェアのスタック構造を示した図である。

[図6]図６は、トランザクションの情報をＳＰアプリに通知する際のソフトウェアレイヤ間の動作例を示した図である。

[図7]図７は、セキュアエレメント部１１４とリーダライタ１２０間のトランザクションの情報をＳＰアプリに通知するための処理手順を示したフローチャートである。

[図8]図８は、ＳＰアプリの正当性を検証する際のソフトウェアレイヤ間の概略的な動作例を示した図である。

[図9]図９は、トランザクションの通知対象となったＳＰアプリの正当性を検証するための処理シーケンス例を示した図である。

[図10]図１０は、ＳＩＭサーバから取得するＳＰアプリの属性情報のデータ構造を示した図である。

[図11]図１１は、トランザクションの一意性を特定するヘッダ部分のデータ構造を示した図である。

[図12]図１２は、決済に関するトランザクションの情報のペイロードのデータ構造を示した図である。

[図13]図１３は、決済以外に関するトランザクションの情報のペイロードのデータ構造を示した図である。

[図14]図１４は、トランザクションの発生に応じて画面を更新する一例を示した図である。

[図15]図１５は、トランザクションの発生に応じて画面を更新する他の例を示した図である。

発明を実施するための形態

[0022] 以下、図面を参照しながら本開示について、以下の順に従って説明する。

[0023] Ａ．装置構成

Ｂ．セキュアエレメントの機能的構成

Ｃ．ソフトウェア構成

Ｄ．トランザクションの通知機能

Ｅ．ＳＰアプリの正当性の検証処理

Ｆ．効果

[0024] Ａ．装置構成

図１には、本開示が適用される情報処理装置１００のハードウェア構成例を模式的に示している。情報処理装置１００として、例えばセキュアエレメントを搭載したスマートフォンやタブレットなどの多機能情報端末を想定しているが、パーソナルコンピュータ（ＰＣ）などその他のタイプの情報機器でもよい。

[0025] 図示の情報処理装置１００は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１０１と、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１０２と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１０３と、ホストバス１０４と、ブリッジ１０５と、拡張バス１０６と、インターフェース部１０７と、入力部１０８と、出力部１０９と、ストレージ部１１０と、ドライブ１１１と、通信部１１３と、セキュアエレメント（ＳＥ）部１１４を含んでいる。

[0026] ＣＰＵ１０１は、演算処理装置及び制御装置として機能し、各種プログラ

ムに従って情報処理装置１００の動作全般を制御する。ＲＯＭ１０２は、ＣＰＵ１０１が使用するプログラム（基本入出力システムなど）や演算パラメータなどを不揮発的に格納している。ＲＡＭ１０３は、ＣＰＵ１０１の実行において使用するプログラムをロードしたり、プログラム実行において適宜変化する作業データなどのパラメータを一時的に格納したりするのに使用される。ＲＡＭ１０３にロードしてＣＰＵ１０１において実行するプログラムは、例えば各種アプリケーションプログラムやオペレーティングシステム（ＯＳ）、ミドルウェア（MW）などである。

[0027] ＣＰＵ１０１とＲＯＭ１０２とＲＡＭ１０３は、ＣＰＵバスなどから構成されるホストバス１０４により相互に接続されている。そして、ＣＰＵ１０１は、ＲＯＭ１０２及びＲＡＭ１０３の協働的な動作により、ＯＳが提供する実行環境下で各種アプリケーションプログラムを実行して、さまざまな機能やサービスを実現することができる。情報処理装置１００がスマートフォンやタブレットの場合、ＯＳは例えば米グーグル社のＡｎｄｒｏｉｄである。また、アプリケーションプログラムには、セキュアエレメントのサービス機能に関するＳＰプロバイダから配布されるＳＰアプリが含まれるものとする。

[0028] ホストバス１０４は、ブリッジ１０５を介して拡張バス１０６に接続されている。但し、情報処理装置１００がホストバス１０４、ブリッジ１０５及び拡張バス１０６によって回路コンポーネントを分離される構成する必要はなく、単一のバス（図示しない）によってほぼすべての回路コンポーネントが相互接続される実装であってもよい。

[0029] インターフェース部１０７は、拡張バス１０６の規格に則って、入力部１０８、出力部１０９、ストレージ部１１０、ドライブ１１１、通信部１１３、及びセキュアエレメント（ＳＥ）部１１４といった周辺装置を接続する。但し、情報処理装置１００がスマートフォンやタブレットといった情報端末として動作するために、図１に示す周辺装置がすべて必須であるとは限らず、また図示しない周辺装置を情報処理装置１００がさらに含んでもよい。ま

た、周辺装置は情報処理装置１００の本体に内蔵されていてもよいし、一部の周辺装置は情報処理装置１００本体に外付け接続されていてもよい。

[0030] 入力部１０８は、ユーザからの入力に基づいて入力信号を生成し、ＣＰＵ１０１に出力する入力制御回路などから構成される。情報処理装置１００がスマートフォンやタブレットなどの情報端末の場合、入力部１０８は、例えばタッチパネルやマイクロホンであるが、ボタンなどのその他の機械式の操作子を含んでもよい。また、情報処理装置１００がスマートフォンやタブレットなどの情報端末の場合、情報端末に搭載されるカメラを入力部１０８に含んでいてもよい。

[0031] 出力部１０９は、例えば、液晶ディスプレイ（ＬＣＤ）装置、有機ＥＬ（Ｅｌｅｃｔｒｏ－Ｌｕｍｉｎｅｓｃｅｎｃｅ）ディスプレイ装置、及びＬＥＤ（Ｌｉｇｈｔ Ｅｍｉｔｔｉｎｇ Ｄｉｏｄｅ）などの表示装置を含み、映像データなどの各種データをイメージ又はテキストで表示したり、ＧＵＩ（Ｇｒａｐｈｉｃａｌ Ｕｓｅｒ Ｉｎｔｅｒｆａｃｅ）画面を表示したりする。また、出力部１０９は、スピーカ及びヘッドホンなどの音声出力装置を含み、音声データなどを音声に変換して出力する。

[0032] ストレージ部１１０は、ＣＰＵ１０１で実行されるプログラム（アプリケーション、ＯＳ、ミドルウェアなど）や各種データなどのファイルを格納する。ストレージ部１１０は、例えば、ＳＳＤ（Ｓｏｌｉｄ Ｓｔａｔｅ Ｄｒｉｖｅ）などの大容量記憶装置で構成されるが、ＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）のような外付けの記憶装置を含んでもよい。

[0033] リムーバブル記憶媒体１１２は、例えばｍｉｃｒｏＳＤカードのようなカートリッジ式で構成される記憶媒体である。ドライブ１１１は、装填したリムーバブル記憶媒体１１３に対して読み出し及び書き込み動作を行う。ドライブ１１１は、リムーバブル記録媒体１１２から読み出したデータ（例えば静止画や動画など）をＲＡＭ１０３に出力したり、ＲＡＭ１０３上のデータをリムーバブル記録媒体１１２に書き込んだりする。

[0034] 通信部１１３は、４Ｇや５Ｇなどのセルラー通信網や、Ｗｉ－Ｆｉ（登録

商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）などの無線通信を行うデバイスである。また、通信部１１３は、ＨＤＭＩ（登録商標）（Ｈｉｇｈ－Ｄｅｆｉｎｉｔｉｏｎ　Ｍｕｌｔｉｍｅｄｉａ　Ｉｎｔｅｒｆａｃｅ）などの端子を備え、ディスプレイなどとのＨＤＭＩ（登録商標）通信を行う機能をさらに備えていてもよい。

[0035] セキュアエレメント（ＳＥ）部１１４は、ＩＣチップ又はＲＦＩＤタグと呼ばれる、耐タンパ性のあるハードウェアで保護されたデバイスである。耐タンパ性とは、内部解析（リバースエンジニアリング）や改変が極めて困難なことを意味し、解析できないように難読化するといった論理的な手段や、保護層を剥がすと回路が破壊されてしまうといった物理的な手段によって実現される。また、セキュアエレメント部１１４は、リーダライタ１２０との間では相互認証と暗号化を用いてセキュアな非接触通信が可能である。非接触通信は、リーダライタ１２０から発される電磁波を利用して行われる。通信は、副搬送波を利用しない対称通信であり、１３．５６ＭＨｚの周波数帯を利用して、２１２ｋｂｐｓ／４２４ｋｂｐｓの速度で行われる。

[0036] Ｂ．セキュアエレメントの機能的構成

セキュアエレメント部１１４は、単一のセキュアエレメントモジュール内で多目的のデータを管理することができる。セキュアエレメント部１１４内のメモリの各々のデータには個別のアクセス権を設定することが可能で、これによってアプリケーション間の安全な相互運用が実現される。

[0037] 情報処理装置１００をリーダライタ１２０にかざして、セキュアエレメント部１１４がリーダライタ１２０からの搬送波が届く範囲に入ると、情報処理装置１００本体の動作とは非同期に（又は、アプリケーションの起動不要で予告なく）、セキュアエレメント部１１４とリーダライタ１２０間でトランザクションが実施される。ここで言うトランザクションは、クレジットカード機能、チケット機能、個人認証機能、乗車券機能、電子マネー又は決済機能といった各種のサービス機能に関する処理である。セキュアエレメント部１１４の耐タンパ性を利用して、トランザクションを安全に行うことがで

きる。

[0038] セキュアエレメント部１１４内では、トランザクションの処理対象データ（電子マネーなど）は、外部からの直接のアクセスを排除することでデータの改ざんやデータの漏洩、データの不正利用を防ぐことができる安全なメモリ領域（後述）に格納される。さらに本実施形態では、トランザクション処理に関するデータも、セキュアエレメント部１１４内で併せて格納されるようになっている。トランザクション処理に関するデータは、「サービスＩＤＸＸの処理が発生した」など）を認識できる情報を含むものとする。

[0039] 図２には、セキュアエレメント部１１４の内部構成を模式的に示している。セキュアエレメント部１１４は、アンテナ部２０１と、アンテナ部２０１に接続されたアナログ部２０２と、デジタル制御部２０３と、メモリ２０４と、外部インターフェース（外部ＩＦ）２０５で構成され、情報処理装置１００に搭載されている。セキュアエレメント部１１４は、１チップの半導体集積回路で構成してもよいし、ＲＦアナログフロントエンドとロジック回路部を分離して２チップの半導体集積回路で構成してもよい。

[0040] アンテナ部２０１及びアナログ部２０２は、セキュアエレメント部１１４とリーダライタ１２０間の非接触インターフェースを構成する。アンテナ部２０１は、リーダライタ１２０との間で非接触データの送受信を行なう。アナログ部２０２は、検波、変復調、クロック抽出など、アンテナ部２０１から送受信されるアナログ信号の処理を行なう。リーダライタ１２０からは、データ読み出し要求又はデータ書き込み要求を含んだ変調搬送波と、セキュアエレメント部１１４からの返信用の無変調搬送波が送信される。アナログ部２０２は、無変調搬送波に返信用データを重畳した搬送波を、アンテナ部２０１から反射送信する。リーダライタ１２０との非接触通信には、例えばＮＦＣ通信方式が利用される。また、リーダライタ１２０との間では相互認証と暗号化を用いてセキュアな非接触通信が可能である。

[0041] デジタル制御部２０３は、リーダライタ１２０間の送受信データの処理やその他のセキュアエレメント部１１４内の動作を統括的にコントロールする

。また、デジタル制御部２０３は、アドレス可能なメモリ２０４をローカルに接続している。メモリ２０４は、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）などの不揮発性記憶装置で構成され、乗車券機能、電子マネー又は決済機能、クレジットカード機能、チケット機能、個人認証機能といった各種のサービス機能に関する（すなわち、トランザクションの処理対象の）データを格納するために使用される。デジタル制御部２０３は、メモリ２０４のメモリ空間に階層構造（図３を参照のこと）を構築して、トランザクションの処理対象のデータを格納している。さらに本実施形態では、トランザクション処理に関するデータ（図４を参照のこと）もメモリ２０４内で併せて格納している。また、メモリ２０４にはデジタル制御部２０３が実行するプログラムコードを書き込んだり、プログラム実行中の作業データを保存するために使用したりしてもよい。

[0042] 外部インターフェース２０５は、情報処理装置１００側のインターフェース部１０７と接続するためのインターフェースプロトコルに則って、デジタル制御部２０３が情報処理装置１００本体とを有線接続するための機能モジュールである。メモリ２０４に書き込まれたデータは、外部インターフェース２０５を経由して、情報処理装置１００本体（ＣＰＵ１０１又はＲＡＭ１０３）に転送することができる。また、情報処理装置１００側（例えば、ＣＰＵ１０１が実行するソフトウェアプログラム）は、外部インターフェース２０５及びデジタル制御部２０３を介して、メモリ２０４に対するデータ読み出し及びデータ書き込みなどの動作を行うことができる。

[0043] 図３には、セキュアエレメント部１１４内のメモリ２０４に構築される、トランザクションの処理対象データを格納するメモリ領域におけるデータ構造を模式的に示している。このメモリ領域は、デジタル制御部２０３の制御下でアクセス可能なメモリ領域であり、外部からの直接のアクセスを排除することで、データの改ざんやデータの漏洩、データの不正利用などを防ぐことができる安全なメモリ領域である。図示のメモリ領域では、「エリア」、

「サービス」、及び「ユーザブロックデータ」という単位で、階層構造によってデータが管理される。

[0044] 「エリア」は、「ディレクトリ」又は「フォルダ」に相当し、エリアの下にさらに階層的にエリアを作成することも可能である。エリアは、例えばサービスプロバイダ単位でエリアが形成されるが、セキュアエレメント部１１４が複数のサービスプロバイダに対応している場合にはメモリ２０４内に複数個のエリアが形成され得る。もちろん、１つのサービスプロバイダに対して複数個のエリアが形成され得るし、複数のサービスプロバイダで１つのエリアが共有され得る。

[0045] 「サービス」は、データに対するアクセス権限又は暗号化方式などを管理する概念である。具体的には、サービスの配下に格納されたデータには、サービスに定められたアクセス権限又は暗号化方式などに基づく制御が行われる。例えば、図３中のサービスＡが暗号化されていないデータを格納し、サービスＢが所定の暗号化方式によって暗号化されたデータを格納するものとする。この場合、相対的に重要度の低いデータであるユーザブロックデータＡ－１及びユーザブロックデータＡ－２は、暗号化されることなくサービスＡの配下に格納され得る。一方、相対的に重要度の高いデータであるユーザブロックデータＢ－１は、サービスＢによって定められた暗号化方式で暗号化され、サービスＢの配下に格納され得る。サービスも１階層構造につき複数個存在し得る。

[0046] 「ユーザブロックデータ」は、セキュアエレメント部１１４の処理に用いられるデータ（すなわち処理対象データ）を格納する記憶領域又はデータ自体であり、１階層構造につき複数個存在し得る。

[0047] 本実施形態では、トランザクション処理に関するデータ（図４を参照のこと）もメモリ２０４内で併せて格納している。図４には、トランザクション処理に関するデータの構成例を示している。

[0048] 図４に示す例では、各トランザクション処理に関するデータは、メモリ領域（図３を参照のこと）における処理対象データのパスと、処理対象データ

自体と、処理対象データのハッシュ値などを含んでいる。

[0049] デジタル制御部２０３は、リーダライタ１２０との間でトランザクションを実施する際に、処理対象データと、メモリ領域（図３を参照のこと）における処理対象データのパスを、そのトランザクションの処理に関するデータとして格納する。さらに、デジタル制御部２０３は、処理対象データのハッシュ値を計算して、そのハッシュ値もそのトランザクションの処理に関するデータとして併せて格納する。

[0050] なお、デジタル制御部２０３は、図４に示したデータ以外のデータを適宜追加してもよい。例えば、デジタル制御部２０３は、処理対象データの属性（例えば、内容、種別又は重要度など）に関するデータを追加してもよい。また、デジタル制御部２０３は、図４に示したデータを、それに相当する別のデータに置換してもよい。例えば、デジタル制御部２０３は、処理対象データのパスを、当該処理対象データを特定可能な任意のデータに置換してもよい。また、デジタル制御部２０３は、処理対象データだけでなく、処理対象データ以外のデータ（例えば、処理対象データのパス）も含めたハッシュ値を算出してもよい。これによって、情報処理装置１００本体側では、処理対象データだけでなく、処理対象データ以外のデータも含めデータの完全性を検証することができる。

[0051] Ｃ．ソフトウェア構成

図５には、情報処理装置１００上で動作するソフトウェアのスタック構造を模式的に示している。ソフトウェアスタックは、最下層から順に、デバイスドライバ層、ＯＳ層、ミドルウェア層、アプリケーション層で構成される。

[0052] デバイスドライバ層：

最下層のデバイスドライバ層は、情報処理装置１００に含まれる各ハードウェアを個別に制御するデバイスドライバの集合で構成される。ここで言う、「ハードウェア」には、入力部１０８、出力部１０９、ストレージ部１１０、ドライブ１１１、通信部１１３などを構成する個々のハードウェアコン

ポネント毎に、駆動制御用のデバイスドライバが装備される。本実施形態では、セキュアエレメント部１１４用のデバイスドライバ（図５中では、「ＳＥドライバ」と表記）も装備される。但し、ＳＥドライバ以外のデバイスドライバは一般的であり、本開示に直接関連しないので、本明細書では最低限の説明にとどめる。

[0053] デバイスドライバは、対応するデバイスにおいてイベントが発生すると、ＯＳに対してイベントの通知を行う機能を有する。イベントの通知は、例えば割り込みの発生やポーリングなどの処理によって行われる。ＳＥドライバの場合、例えば、セキュアエレメント部１１４内の外部インターフェース部２０５から割り込み信号を受信したり、外部インターフェース部２０５内のステータスレジスタのポーリングを行ったりして、イベントの発生を検出することができる。具体的には、ＳＥドライバは、「非接触通信アプレット」の機能により、セキュアエレメント部１１４とリーダライタ１２０との非接触通信が開始及び終了したイベント（又は、セキュアエレメント部１１４がリーダライタ１２０からの搬送波のオン及びオフのイベント）を検出すると、ＯＳに通知する。

[0054] また、デバイスドライバは、対応するデバイスに対するデータの入出力動作やデバイスの駆動動作などデバイス固有のハードウェア動作の制御を行う。例えばＳＥドライバは、上位層からセキュアエレメント部１１４へのアクセス要求（具体的には、ミドルウェアを介したアプリケーション（ＳＰアプリ）からのアクセス要求）に応じて、セキュアエレメント部１１４内の外部インターフェース部２０５を通じて、メモリ２０４に対するデータ読み出しやデータ書き込みなどのトランザクションを行う機能を有する。この機能は「トランザクション用アプレット」によって実現されるものとする。ＯＳやミドルウェアは、ＯＭＡＰＩ（Ｏｐｅｎ　ｍｏｂｉｌｅ　ＡＰＩ）を介してトランザクション用アプレットにアクセスすることができる。トランザクション用アプレットは、トランザクションの処理対象のデータを保管する。トランザクションの処理対象のデータはＡＰＤＵ（Ａｐｐｌｉｃａｔｉｏｎ

Ｐｒｏｔｏｃｏｌ　Ｄａｔａ　Ｕｎｉｔ）という単位で扱われる。

[0055] セキュアエレメント部１１４内のメモリ２０４において、トランザクションの処理対象のデータを記憶するメモリ空間の構造は、図３を参照しながら既に説明した通りである。本実施形態では、リーダライタ１２０からメモリ２０４に書き込みが発生したときに処理の内容（例えば、「サービスＩＤＸＸの処理が発生した」など）を認識できる仕組みが導入されている。

[0056] ＯＳ層：

ＯＳは、多くのアプリケーションで共通して利用される機能やハードウェアの基本的な制御機能などからなる実行環境をアプリケーションに提供する。例えば情報処理装置１００がスマートフォンやタブレットなどの情報端末の場合、米グーグル社のＡｎｄｒｏｉｄなどがＯＳに相当する。ＯＳがＡｎｄｒｏｉｄの場合、デバイスドライバからのイベント通知などシステム全体に関わる情報を、「ＢｒｏａｄｃａｓｔＩｎｔｅｎｔ」という仕組みを使って、すべてのアプリケーションへ向けて発信する。なお、Ｉｎｔｅｎｔは、Ａｎｄｒｏｉｄ上で動作するアプリケーションに含まれる１以上のアクティビティ又はサービス間でやり取りされるメッセージオブジェクトである。

[0057] ミドルウェア層：

ミドルウェアは、ＯＳとアプリケーションの中間に位置し、さまざまなソフトウェアから共通して利用される機能を提供する。例えば、分野や用途が限定された具体的又は個別的な機能は、ＯＳではなくミドルウェアで提供される。スマートフォンやタブレットなどの情報端末の全機種がセキュアエレメントを装備しているとは限らないので、本実施形態ではセキュアエレメント部１１４の使用に関連する機能はミドルウェアとして提供されるものとする。また、ＧＵＩ機能などがミドルウェアとして提供されている。但し、セキュアエレメント部１１４に関連しないミドルウェアの機能は、本開示に直接関連しないので、本明細書では最低限の説明にとどめる。

[0058] 本実施形態では、ミドルウェアによって提供されるセキュアエレメント部１１４の使用に関連する機能として、「ＳＥアクセスクライアント」と「サ

ービス統合クライアント」を含むものとする。「ＳＥアクセスクライアント」は、セキュアエレメント部１１４へのアクセス動作を行う機能である。また、「サービス統合クライアント」は、セキュアエレメント部１１４において使用中のサービスに関する情報をサーバ（以下、「サービス統合サーバ」とする）（図５には図示しない）との連携により管理する機能である。

[0059] アプリケーション層：

最上位のアプリケーション層は、それぞれ作業目的に応じて使用されるアプリケーションソフトウェアの集合で構成される。各アプリケーションソフトウェアは、ＯＳやミドルウェアが提供する機能を使用して、それぞれの作業目的を実現する。例えば、電話やメール、カメラ、カレンダー・スケジュール管理などのアプリケーションソフトウェアが情報処理装置１００にインストールされていることが想定される。これらの一般的なアプリケーションソフトウェアは、本開示に直接関連しないので、本明細書では最小限の説明にとどめる。

[0060] また、本実施形態では、セキュアエレメント部１１４を利用してサービス機能（乗車券機能、電子マネー又は決済機能、クレジットカード機能、チケット機能、個人認証機能など）を提供する１又は複数のＳＰアプリが情報処理装置１００にインストールされているものとする。このようなＳＰアプリをインストールした情報処理装置１００は、該当するサービス機能を提供するＩＣカードとして動作することができる。サービス統合クライアントは、情報処理装置１００にインストールされているＳＰアプリ毎に、利用するサービスを識別するサービスＩＤと、ＳＰアプリから参照可能なカードを識別するカードＩＤ（ＣＩＤ）を管理する。

[0061] ＳＰアプリがセキュアエレメント部１１４内の情報を能動的にアクセスする場合、ＳＰアプリがセキュアエレメント部１１４の利用権を占有する状態となる必要がある。一般に、ＳＰアプリはサービス統合クライアントに対して利用申請手続きを行い、サービス統合クライアントがＳＰアプリの正当性（身元）確認やＳＰアプリに許可されているセキュアエレメントへの操作な

どのサービス統合サーバへの問い合わせを経て、ＳＰアプリがセキュアエレメント部１１４の利用権を占有する状態となる。したがって、ＳＰアプリがセキュアエレメント部１１４にアクセスしようとすると、セキュアエレメント部１１４の利用権の占有に伴う処理時間、ネットワーク負荷、及びサーバ負荷を要する。

[0062] セキュアエレメント部１１４の利用権を占有する状態となったＳＰアプリは、ミドルウェアの機能であるＳＥアクセスクライアントを通じてセキュアエレメント部１１４へのアクセス、すなわちセキュアエレメント部１１４内のメモリ２０４に対するデータ読み出し又はデータ書き込み動作を行うことができる。

[0063] なお、セキュアエレメント部１１４のセキュリティを担保する上で、ＳＰアプリが無制限にアクセスできるのは好ましくない。このため、ＳＥアクセスクライアントは、セキュアエレメント部１１４にアクセスを要求するＳＰアプリの検証を行うことや、複数のＳＰアプリによるセキュアエレメント部１１４への同時アクセスを禁止することなどのアクセス制限を行うようにしている。

[0064] Ｄ．トランザクションの通知機能

ＳＰアプリをインストールした情報処理装置１００は、該当するサービス機能を提供するＩＣカードとして動作することができる。例えば、ユーザが情報処理装置１００をリーダライタ１２０にかざすという手動操作によって、情報処理装置１００に搭載されたセキュアエレメント部１１４とリーダライタ１２０間のトランザクションが発生する。

[0065] このようなトランザクションは、ＳＰアプリの起動が不要で、ＳＰアプリへの予告もなく発生する。このため、ＳＰアプリにおいて残高表示などを実施するには、ＳＰアプリはセキュアエレメント部１１４内のメモリ２０４に格納されている最新の情報を把握する必要がある。

[0066] 上記Ｃ項で説明したように、ミドルウェア内のＳＥアクセスクライアントは、セキュリティの担保のため、セキュアエレメント部１１４へのアクセス

制限（ＳＰアプリの検証や、複数のＳＰアプリによる同時アクセス禁止など）を行っている。このようなアクセス制限下で、各ＳＰアプリが最新の情報を把握するために、定期的及び能動的にセキュアエレメント部１１４内のメモリ２０４にアクセスしようとすると、複数のＳＰアプリからのアクセスの競合が起き易いという問題がある。

[0067] また、ＳＰアプリは定期的にアクセスするだけでは、予告なく発生するメモリ２０４内の情報変化を即時的に検知できないので、ＳＰアプリがメモリ２０４から取得する情報のリアルタイム性に欠ける。さらに、メモリ２０４内の情報変化が起きていなくても、ＳＰアプリは定期的にアクセスを行う必要があり、無駄な処理を実施することになる。ＳＰアプリがセキュアエレメント部１１４にアクセスする際に、サービス統合クライアントはサービス統合サーバにアクセスして、ＳＰアプリの正当性検証やＳＰアプリから参照可能なカード一覧を取得する必要がある。このため、情報処理装置１００がネットワーク接続する処理負荷があり、且つサーバ負荷が増大する。

[0068] そこで、本開示では、セキュアエレメント部１１４とリーダライタ１２０間のトランザクションが発生すると、主にミドルウェア内のサービス統合クライアントの機能によって、トランザクションの情報を必要なＳＰアプリに通知する機能を提示する方法について提案する。ただ単に通知する機能を追加するだけでは、不正なＳＰアプリや関係のないアプリに通知してしまうおそれがあり、センシティブな決済情報が漏洩する可能性がある。そこで、本開示では、情報の通知が必要なＳＰアプリの判定とＳＰアプリの正当性の検証とを併せて行って、ＳＰアプリへのトランザクションの情報の通知を行うようにしている。

[0069] 図６には、セキュアエレメント部１１４とリーダライタ１２０間のトランザクションの情報をＳＰアプリに通知する際のソフトウェアレイヤ間の動作例を示している。

[0070] まず、ユーザが情報処理装置１００をリーダライタ１２０にかざすという手動操作によって、情報処理装置１００に搭載されたセキュアエレメント部

１１４とリーダライタ１２０間のトランザクションが発生する（Ｓ６０１）。このようなトランザクションは、関連するＳＰアプリに予告なく発生する。トランザクションでは、リーダライタ１２０から搬送波が送信される。搬送波は、リーダライタ１２０からのデータ読み出し要求又はデータ書き込み要求を含んだ変調搬送波と、セキュアエレメント部１１４からの返信用の無変調搬送波を含む。その際、トランザクションのデータは、トランザクション用アプレットに保管される。

[0071] ＳＥドライバの非接触通信用アプレットは、セキュアエレメント部１１４とリーダライタ１２０間でトランザクションが発生したことを検知すると、ＯＳに対してイベントを通知する（Ｓ６０２）。そして、ＯＳは、イベントを検知すると、Ｂｒｏａｄｃａｓｔを発信して、上位層に対してシステムの状態が変化したことを通知する（Ｓ６０３）。

[0072] ミドルウェア内のサービス統合クライアントは、ＯＳからイベントを通知するＢｒｏａｄｃａｓｔを受信すると、ＯＭＡＰＩを介してトランザクション用アプレットにアクセスする。そして、サービス統合クライアントは、該当するトランザクションの処理対象のデータ（ＡＰＤＵ）を、トランザクション用アプレットを通じてセキュアエレメント部１１４から取得する（Ｓ６０４）。その際、サービス統合クライアントは、トランザクションの処理対象データと併せて、トランザクション処理に関するデータも取得する。

[0073] 次いで、サービス統合クライアントは、取得したデータをＳＰ（サービスプロバイダ）毎に解析して、トランザクションの情報の通知が必要なＳＰアプリを判定する（Ｓ６０５）。トランザクションの処理対象データと併せて取得した、トランザクション処理に関するデータは、「サービスＩＤ　ＸＸの処理が発生した」など）を認識できる情報を含んでいる。したがって、サービス統合クライアントは、トランザクション処理に関するデータを解析することによって、そのトランザクションに関連するサービスＩＤを特定することができ、そのサービスＩＤに基づいて通知対象のＳＰアプリを判定することができる。

[0074] 次いで、サービス統合クライアントは、通知対象として判定された各ＳＰアプリの正当性を検証する（Ｓ６０６）。サービス統合クライアントは、サーバから事前に取得した検証情報に基づいて、ＳＰアプリの正当性を検証する。具体的には、ＳＰアプリのパッケージ名やＳＰアプリの署名値を検証情報に用いる。サービス情報管理（Ｓｅｒｖｉｃｅ Ｉｎｆｏｒｍａｔｉｏｎ Ｍａｎａｇｅｍｅｎｔ：ＳＩＭ）サーバが、ＳＰアプリ毎の検証情報を含む情報を管理している。通知対象ＳＰアプリの正当性の検証処理の詳細については後述に譲る。

[0075] そして、サービス統合クライアントは、正当性が検証された適切なＳＰアプリへ、トランザクションの情報を通知する（Ｓ６０７）。ＳＰアプリに通知するトランザクションの情報の詳細については、後述に譲る。

[0076] なお、複数のＳＰアプリに通知を行う場合には、ＳＰアプリ間で所定の時間間隔を置いて情報通知を行うようにする。何故なら、ＳＰアプリがトランザクションの情報の通知を受けてセキュアエレメント部１１４へのアクセスを開始する可能性があるからである。アクセスを行う原因として、トランザクション後の残高低下によるオートチャージや決済に伴うポイント残高の読み込み処理などを挙げることができる。

[0077] 図７には、情報処理装置１００内で実施される、セキュアエレメント部１１４とリーダライタ１２０間で実施されたトランザクションの情報をＳＰアプリに通知するための処理手順をフローチャートの形式で示している。図示の処理手順は、ミドルウェア層に含まれるサービス統合クライアントが中心となって実現する。

[0078] サービス統合クライアントには、セキュアエレメント部１１４とリーダライタ１２０間でトランザクションが実施されたことを示すイベントが、ＯＳを介して通知される（ステップＳ７０１のＹｅｓ）。

[0079] サービス統合クライアントは、このイベント通知に応答して、ＳＥドライバ内のトランザクション用アプレットにＯＭＡＰＩを介してアクセスして、トランザクションの処理対象データと、そのトランザクション処理に関する

データを取得する（ステップＳ７０２）。

[0080] 次いで、サービス統合クライアントは、取得したデータをＳＰ（サービスプロバイダ）毎に解析して、トランザクションの情報の通知が必要なＳＰアプリを判定する（ステップＳ７０３）。トランザクション処理に関するデータは、「サービスＩＤ　ＸＸの処理が発生した」など）を認識できる情報を含んでいるので、サービス統合クライアントは、データ解析により該当するサービスＩＤを特定することができ、そのサービスＩＤに基づいて通知対象のＳＰアプリを判定することができる。

[0081] 次いで、サービス統合クライアントは、ＳＩＭサーバから事前に取得したＳＰアプリ毎の検証情報に基づいて、通知対象として判定された各ＳＰアプリの正当性を検証する（ステップＳ７０４）。通知対象ＳＰアプリの正当性の検証処理の詳細については後述に譲る。

[0082] そして、サービス統合クライアントは、正当性が検証された適切なＳＰアプリへ、トランザクションの情報を通知する（ステップＳ７０５）。ＳＰアプリに通知するトランザクションの情報の詳細については、後述に譲る。

[0083] Ｅ．ＳＰアプリの正当性の検証処理

このＥ項では、上記Ｄ項で説明したトランザクションの通知機能において、通知対象のＳＰアプリを判定した際に実施される、ＳＰアプリの正当性の検証処理について詳細に説明する。

[0084] 図８には、トランザクションの通知対象となったＳＰアプリの正当性を検証する際のソフトウェアレイヤ間の概略的な動作例を示している。

[0085] サービス統合クライアントは、事前処理として、情報処理装置１００にインストールされている各ＳＰアプリの検証情報を、ＳＩＭサーバから事前に取得しておく（Ｓ８０１）。検証情報は、パッケージ名などのＳＰアプリを一意に特定する情報と、ＳＰアプリ署名値（アプリ署名者証明書ハッシュなど）などで構成される。

[0086] その後、セキュアエレメント部１１４とリーダライタ１２０間のトランザクションが発生すると、サービス統合クライアントは、ＯＳからのＢｒｏａ

ｄｃａｓｔの受信を通じてそのイベントを検知することができる。

[0087] サービス統合クライアントは、トランザクション用アプレットを通じて取得したデータをＳＰ毎に解析して、トランザクションの情報の通知対象となるＳＰアプリを判定すると、続いて、ＳＩＭサーバから事前に取得しておいた検証情報を用いて、通知対象の各ＳＰアプリの正当性を検証する（Ｓ８０２）。そして、サービス統合クライアントは、正当性の検証に成功した各ＳＰアプリに、トランザクションの情報を通知する。

[0088] ＳＰアプリは、サービス統合クライアントから通知されたトランザクションの情報を用いて、残高表示などトランザクションによって変化した情報を速やかに提示することができる。また、ＳＰアプリは、ＳＰサーバと連携して、ユーザ通知や、セキュアエレメント部１１４へのアクセスを行う（Ｓ８０３）。具体的には、ＳＰアプリは、ＳＰサーバと連携して、セキュアエレメント部１１４にアクセスして、トランザクション後の残高低下によるオートチャージや決済に伴うポイント残高の読み込み処理など、該当するサービス機能に関するサービスプロバイダへの手続きを行う。

[0089] 図９には、トランザクションの通知対象となったＳＰアプリの正当性を検証するための、ソフトウェアモジュール間の処理シーケンス例を示している。図９では、紙面の都合により、トランザクションの通知対象をＳＰアプリＡ及びＳＰアプリＢの２つのアプリケーションのみとしている。また、説明の簡素化のため、ＳＰアプリＡ及びＳＰアプリＢのいずれも正当性の検証に成功するものとする。

[0090] サービス統合クライアントは、情報処理装置１００にインストールされている各ＳＰアプリの属性情報をＳＩＭサーバに要求する（ＳＥＱ９０１）。これに対し、ＳＩＭサーバは要求された各ＳＰアプリの属性情報を返信する（ＳＥＱ９０２）。ＳＰアプリの属性情報は検証情報を含んでおり、ＳＩＭサーバからの属性情報の取得はＳＰアプリの正当性を検証するための事前処理となる。例えばミドルウェアが起動される度に定期的に（例えば、３０日に１回、１００回に１度など）、サービス統合クライアントは、ＳＩＭサー

バに更新情報を確認して、インストール済みの各ＳＰアプリの最新の属性情報を事前に取得するようにする。

[0091] 図１０には、参考として、サービス統合クライアントがＳＩＭサーバから取得するＳＰアプリの属性情報のデータ構造を例示している。正確には、サービス統合クライアントは、ＳＩＭサーバから、図１０に示すようなデータのリストをＳＰアプリ毎に取得する。以下、各データについて説明しておく。

[0092] 「サービスＩＤ」は、ＳＰアプリが実施するサービスを一意に表す値からなる。例えば決済を行うＳＰアプリであれば、決済サービスを一意に表す値である。一般には、サービスＩＤは、ミドルウェアの開発主体（セキュアエレメントを提供するプラットフォーマー）が払い出す、”ＳＶ１２３４５６”といった英数値である。

[0093] 「ＳＰアプリを一意に特定する情報」は、”ｃｏｍ．ｓｐａｐｐ．ａｐｐ”などの、ＳＰアプリのパッケージ名である。「署名値」は、例えば１６進数のＳＰアプリ署名者証明書ハッシュである。ＯＳからＳＰアプリの署名者証明書を取得してハッシュ値を計算し、そのハッシュ値とＳＰアプリの属性情報に含まれる署名値と照合して、ＳＰアプリの正当性を検証することができる。

[0094] 「優先度」、「通知期限」、「通知期限超過時の動作」は、複数のＳＰアプリが正当な通知対象となった場合の通知動作を規定するパラメータである。「優先度」はトランザクションの情報を通知する優先度を１～１０の値で示す。複数のＳＰアプリが正当な通知対象となった場合には、優先度が高いＳＰアプリから順番にトランザクションの情報の通知が行われる。「通知期限」は、ＳＰアプリが通知の遅延を許容する時間を０～３の数値で示す。「通知期限超過時の動作」は、「通知期限」で指定した遅延時間を超過したときに通知を諦めるか通知を敢行するかを０又は１の値で示す。

[0095] 再び図９を参照して、ＳＰアプリの正当性を検証するための処理シーケンスについて説明する。

[0096] その後、セキュアエレメント部１１４とリーダライタ１２０間のトランザクションが発生時に、サービス統合クライアントは、通知対象となるＳＰアプリを特定して、通知対象の各ＳＰアプリ（図９に示す例では、ＳＰアプリＡ及びＳＰアプリＢ）の正当性の検証処理を行う。

[0097] この正当性の検証処理では、サービス統合クライアントは、まず通知対象のＳＰアプリを特定する。サービス統合クライアントは、トランザクション処理に関するデータを解析してサービスＩＤを特定すると、事前処理であらかじめ取得した各ＳＰアプリの属性情報（図１０を参照のこと）と照合して、サービスＩＤが一致するＳＰアプリを通知対象として特定することができる。図９に示す処理シーケンス例では、ＳＰアプリＡ及びＳＰアプリＢの２つのアプリケーションが通知対象として特定されている。

[0098] 次いで、サービス統合クライアントは、各ＳＰの通知対象となるＳＰアプリの検証情報を要求し（ＳＥＱ９０３）、これに対し、ＯＳは各ＳＰアプリの検証情報を返信する（ＳＥＱ９０４）。米グーグル社のＡｎｄｒｏｉｄなどのスマートフォン向けのＯＳは、アプリケーションのインストール時に実施する相互認証手続きを通じて、各ＳＰアプリの検証情報を把握している。したがって、サービス統合クライアントは、ＯＳに問い合わせることによって、通知対象の各ＳＰアプリの検証情報を取得することができる。

[0099] 次いで、サービス統合クライアントは、通知対象の各ＳＰアプリの正当性を検証する（ＳＥＱ９０５）。サービス統合クライアントは、通知対象の各ＳＰアプリの属性情報に含まれる検証情報を、ＯＳから取得した対応ＳＰアプリの検証情報と照合することによって検証を行い、一致すればそのＳＰアプリは正当性があると判定することができる。図９に示す処理シーケンス例では、通知対象に特定されたＳＰアプリＡ及びＳＰアプリＢの両方について正当性が確認されている。

[0100] 例えばＯＳとしてＡｎｄｒｏｉｄを使用するスマートフォンは、公式アプリストア以外からもアプリケーションをインストールすることができる。このような場合、外観やパッケージ名を本物のように偽装して作成されたアプ

リケーションを、ユーザが正当なアプリケーションと誤認して自端末にインストールしてしまい、その結果、アプリケーションを通じてセキュアエレメント部１１４内の情報が漏洩、不正使用、改ざんされるおそれがある。これに対し、本実施形態では、ＳＰアプリのパッケージ名とＳＰアプリの署名値を組み合わせた検証情報を用いてＳＰアプリの正当性を検証するので、不正なＳＰアプリを排除して、セキュアエレメント部１１４内の情報が漏洩、不正使用、改ざんなどを防ぐことができる。

[0101] そして、サービス統合クライアントは、正当性を確認できた通知対象のＳＰアプリに対して、トランザクションの処理対象データを通知する。図９に示す処理シーケンス例では、ＳＰアプリＡ及びＳＰアプリＢの両方について正当性が確認されたので、まずＳＰアプリＡに通知処理を行い（ＳＥＱ９０６）、次いでＳＰアプリＢに通知処理を行う（ＳＥＱ９０７）。

[0102] 複数のＳＰアプリに通知を行う場合には、各ＳＰアプリの属性情報に含まれている優先度が高い順に通知を行う。図９に示す例では、ＳＰアプリＡの方がＳＰアプリＢよりも高優先度である。

[0103] また、ＳＰアプリＡに通知処理（ＳＥＱ９０６）を行った後、所定の時間間隔（Ｔ）を置いてから、ＳＰアプリＢへの通知処理（ＳＥＱ９０７）を行うようにする。何故ならば、通知を受けたＳＰアプリＡとＳＰアプリＢがともにトランザクションの情報の通知を受けてセキュアエレメント部１１４へのアクセスを開始する可能性があるからである。アクセスを行う原因として、トランザクション後の残高低下によるオートチャージや決済に伴うポイント残高の読み込み処理などを挙げることができる。ＳＰアプリ間で通知を受ける時間間隔が十分長くないと、前後に通知を受けたＳＰアプリＡとＳＰアプリＢの間でセキュアエレメント部１１４へのアクセスなどの処理が競合するおそれがある。

[0104] 前後に通知を受けるＳＰアプリ間で競合が発生した場合には、先に通知を受けたＳＰアプリの処理が終了した後に、次のＳＰアプリの処理を開始するようにする。この場合、通知順が後のＳＰアプリにおいて通知の遅延が発生

する。遅延を容認する通知期限や通知期限を超過してしまった場合については、各ＳＰの属性情報に含まれるパラメータ（図１０を参照のこと）に従うようにしてもよい。

[0105] 続いて、サービス統合クライアントからＳＰアプリに通知するトランザクションの情報のデータ構造について説明する。このデータ構造は、トランザクションの一意性を特定するヘッダ部分と、トランザクションの種別の応じたペイロードで構成される。

[0106] 図１１には、トランザクションの一意性を特定するヘッダ部分のデータ構造を示している。トランザクションの一意性を特定するヘッダ部分は、トランザクションの利用種別（決済、又は決済以外か）に依らない共通のデータ構造である。

[0107] サービスＩＤは、トランザクションによって処理されたサービス（例えば、決済が行われたサービス）を一意に特定する識別情報である。ＣＩＤは、カードを識別するための識別情報である。Ｒ／Ｗ　ＩＤは、トランザクションの相手となったリーダライタ固有の識別情報である。Ｒ／Ｗ　ＩＤを基に利用された場所を特定することができる。Ｒ／W利用日時は、リーダライタを利用した日時（又は、トランザクションが実施された日時）である。Ｒ／Ｗトランザクション ＩＤは、リーダライタで発生したトランザクションの識別情報である。利用種別は、支払い、チャージ、スタンプ、クーポン、チケットなど、トランザクションの種別を示す。ペイロードは、利用種別に応じたデータ構造からなる。

[0108] 図１２には、トランザクションの利用種別に応じたペイロードのデータ構造の一例として、決済に関するトランザクションの情報のペイロードのデータ構造を示している。決済の場合のペイロードは、利用金額、残高、ポイント増減、ポイント残高など、トランザクションによって更新されるデータを含む。

[0109] 図１３には、トランザクションの利用種別に応じたペイロードのデータ構造の他の例として、決済以外に関するトランザクションの情報のペイロード

のデータ構造を示している。この場合のペイロードは、サービス固有特定ＩＤと、券面・デザイン情報を含む。サービス固有特定ＩＤは、サービス事業者で定義できる固有ＩＤであり、例えばチケット特定ＩＤやクーポン特定ＩＤなどである。券面・デザイン情報は、スタンプや券面デザインを定義する情報であり、例えば取引先のＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）の一部に利用するＩＤなどを含む。なお、決済の関するトランザクションの情報のペイロードも、サービス固有特定ＩＤと、券面・デザイン情報を含んでいてもよい。

[0110] Ｆ．効果

（１）トランザクションは情報処理装置１００をリーダライタ１２０にかざすという手動操作によって発生し、その際にＳＰアプリの起動が不要で、ＳＰアプリへの予告もない。従来、ＳＰアプリは、セキュアエレメント部１１４に能動的にアクセスして、トランザクションによって変化した最新のデータ（利用金額や残高、ポイント増減やポイント残高など）を取得する必要があった。これに対し、本開示に係るトランザクション情報の通知機能によれば、トランザクションによってセキュアエレメント部１１４内のデータが変化したことを、関連するすべてのＳＰアプリが即時に検知することができる。このようなＳＰアプリへの通知機能は、具体的には、ミドルウェア内のサービス統合クライアントに図６に示した機能を実装することによって実現される。したがって、本開示に係る通知機能によれば、ＳＰアプリは、セキュアエレメント部１１４へのアクセスなしにトランザクションの情報を把握して、残高表示などトランザクションによって変化した最新の情報を速やかに提示することができる。

[0111] また、本開示に係るトランザクション情報の通知機能によれば、ＳＰアプリによるセキュアエレメント部１１４へのアクセス回数は最小限となるので、アプリの起動時間の短縮が見込めるとともに、複数のＳＰアプリによるアクセス競合の発生率を低減することができる。複数のＳＰアプリによるセキュアエレメント部１１４への同時アクセスが禁止されるという状況下におい

ては、アクセス競合を抑制できることはとりわけ有効である。セキュアエレメント部１１４へアクセス回数が最小限となることにより、ＳＰアプリがセキュアエレメント部１１４の利用権を占有するためのサービス統合クライアントへの申請及びサービス統合サーバへの問い合わせが不要になるので、ネットワーク負荷及びサーバ負荷の低減にもなる。

[0112] 本開示に係るトランザクション情報の通知機能によれば、ＳＰアプリは、チャージなどのトランザクションによってセキュアエレメント部１１４内のデータが変化すると、関連するＳＰアプリは即時に残高などの情報を更新して、常に最新の情報を情報処理装置１００の画面などで提示することができる。

[0113] 図１４には、トランザクションの発生によってセキュアエレメント部１１４内のデータが変化したことに応じて画面を更新する一例を示している。図１４では、具体的には、トランザクション（支払いやチャージなど）が発生したことにより、スマートフォンの画面に提示中の電子マネーの残高が最新の情報に即時更新される様子を示している。

[0114] 情報処理装置１００（スマートフォン）をリーダライタ１２０にかざして、支払いやチャージなどのトランザクションが発生すると、セキュアエレメント部１１４内の情報が変化する。本開示に係る通知機能によって、通知対象のＳＰアプリの判定及び正当性検証を経て、通知対象のＳＰアプリにセキュアエレメント部１１４内の最新の情報が通知される。その結果、図１４右に示すように、通知対象のＳＰアプリは画面上の電子マネーの残高を、トランザクション前の金額（１，２３４円）からトランザクション後の金額（５，６７８円）へ、即座に更新して提示することができる。提示金額を更新する際、ＳＰアプリを起動するといったユーザ操作や、ＳＰアプリによるセキュアエレメント部１１４の利用権占有は不要である。

[0115] また、図１５には、トランザクションの発生によってセキュアエレメント部１１４内のデータが変化したことに応じて画面を更新する他の例を示している。図１５では、具体的には、複数種類の電子マネーを使用可能なＷａｌ

ｌｅｔアプリの統合残高表示画面において、トランザクション（支払いやチャージなど）の発生により変化した一部の電子マネーの残高が即時更新される様子を示している。

[0116] 情報処理装置１００（スマートフォン）をリーダライタ１２０にかざして、電子マネーＣを使った支払いやチャージなどのトランザクションが発生すると、セキュアエレメント部１１４内で電子マネーＣの情報が変化する。本開示に係る通知機能によって、電子マネーＣのサービスに関連するＳＰアプリが通知対象に判定され且つそのＳＰアプリの正当性検証を経て、通知対象のＳＰアプリにセキュアエレメント部１１４内の電子マネーＣの最新の情報が通知される。その結果、図１５右に示すように、Ｗａｌｌｅｔアプリの統合残高表示画面では、電子マネーＣの残高を即座に更新して提示することができる。提示金額を更新する際、電子マネーＣに対応するＳＰアプリを起動するといったユーザ操作や、そのＳＰアプリによるセキュアエレメント部１１４の利用権占有は不要である。なお、通知を受けたＳＰアプリは、画面更新処理のバックグラウンドで、電子マネーＣの利用情報に基づいてクーポンを取得して表示したり、むしろＳＰアプリの起動にユーザを誘引したりするといったＵＸ（Ｕｓｅｒ　Ｅｘｐｅｒｉｅｎｃｅ）を実現することもできる。

[0117] ちみなに、従来通りに、ＳＰアプリがセキュアエレメント部１１４内の情報を能動的に取得する場合、一般に、ＳＰアプリはサービス統合クライアントに対して利用申請手続きを行い、サービス統合クライアントがＳＰアプリの正当性（身元）確認やＳＰアプリに許可されているセキュアエレメントへの操作などの問い合わせを経て、ＳＰアプリがセキュアエレメント部１１４の利用権を占有する状態となる。したがって、従来通りに、ＳＰアプリを起動してセキュアエレメント部１１４内の最新のデータの提示（残高提示など）を行おうとすると、セキュアエレメント部１１４の利用権の占有に伴う処理時間、ネットワーク負荷、及びサーバ負荷を要する。

[0118] （２）本開示に係るトランザクション情報の通知機能によれば、トランザク

ションの処理対象データなどの情報を、関連する複数のＳＰアプリに通知することができる。このような複数のＳＰアプリへの同時通知機能は、具体的には、ミドルウェア内のサービス統合クライアントに、図６に示したデータ解析及びＳＰ判定機能を実装することによって実現される。トランザクションの情報を複数のＳＰアプリに通知することが可能となる結果、例えば同じ電子マネーを利用する複数のＳＰアプリがそれぞれ情報を最新化することができる。

[0119] 本開示に係るトランザクションの情報の通知機能は、通知先のＳＰアプリを制御可能であるということもできる。セキュアエレメント部１１４とリーダライタ１２０間でトランザクションが発生したとしても、その結果として変化した情報が必要なＳＰアプリのみを通知対象に判定し、通知すべきでないＳＰアプリには情報を通知しないようにすることができる。

[0120] （３）本開示に係るトランザクション情報の通知機能によれば、通知対象と判定されたＳＰアプリの正当性を検証して、不正なアプリにトランザクションの情報を渡さないようにすることができる。例えば外観やパッケージ名を本物のように偽装した不正なＳＰアプリが作成される場合がある。本開示では、ＳＰアプリのパッケージ名とＳＰアプリの署名値を組み合わせた検証情報を用いてＳＰアプリの正当性を検証するので、不正なＳＰアプリを排除して、セキュアエレメント部１１４内の情報が漏洩、不正使用、改ざんなどを防ぐことができる。

産業上の利用可能性

[0121] 以上、特定の実施形態を参照しながら、本開示について詳細に説明してきた。しかしながら、本開示の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。

[0122] 本明細書では、非接触通信を行うＩＣチップなどのセキュアエレメントを搭載したスマートフォンに本開示を適用した実施形態を中心に説明してきたが、本開示の要旨はこれに限定されるものではない。非接触通信以外の無線又は有線を通じて外部装置とトランザクションを行うデバイスを搭載したさ

まざまなタイプの情報処理装置にも本開示を適用して、デバイスと外部装置間で実施されたトランザクションに関する情報を適切なアプリケーションに通知することができる。

[0123] 要するに、例示という形態により本開示について説明してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本開示の要旨を判断するためには、特許請求の範囲を参酌すべきである。

[0124] なお、本開示は、以下のような構成をとることも可能である。

[0125] （１）外部装置とトランザクションを行うデバイスを搭載する情報処理装置であって、

前記デバイスと前記外部装置間でトランザクションが発生したことを検知する検知部と、

前記検知部が前記トランザクションの発生を検知したことに応じて、前記デバイスからデータを取得する取得部と、

前記取得部が取得したデータを解析して、通知対象のアプリケーションを判定する判定部と、

前記通知対象のアプリケーションの正当性を検証する検証部と、

前記通知対象のうち正当性が確認された適切なアプリケーションに、前記取得部が取得したデータを通知する通知部と、

を具備する情報処理装置。

[0126] （２）前記検知部は、オペレーティングシステムからの発信に基づいて前記トランザクションの発生を検知する、

上記（１）に記載の情報処理装置。

[0127] （３）前記取得部は、ＯＭＡＰＩを介して前記デバイスからデータを取得する、

上記（１）又は（２）のいずれかに記載の情報処理装置。

[0128] （４）前記取得部は、前記トランザクションの処理対象データ及び前記トランザクションの処理に関するデータを取得する、

上記（１）乃至（３）のいずれかに記載の情報処理装置。

[0129] （５）前記判定部は、前記取得部が取得したデータに基づいて前記トランザクションに関連するサービスＩＤを特定し、前記サービスＩＤに基づいて通知対象のアプリケーションを判定する、

上記（１）乃至（４）のいずれかに記載の情報処理

[0130] （６）前記判定部は、前記取得部が取得した前記トランザクションの処理に関するデータを解析して前記トランザクションに関連するサービスＩＤを特定する、

上記（５）に記載の情報処理装置。

[0131] （７）前記検証部は、サーバから取得したアプリケーションの検証情報とオペレーティングシステムから取得したアプリケーションの情報に基づいて、アプリケーションの正当性を検証する、

上記（１）乃至（６）のいずれかに記載の情報処理装置。

[0132] （８）検証情報は、アプリケーションのパッケージ名及び署名値を含む、

上記（７）に記載の情報処理装置。

[0133] （９）前記通知部は、前記適切なアプリケーションに対して前記トランザクションの処理対象データを通知する、

上記（１）乃至（８）のいずれかに記載の情報処理装置。

[0134] （１０）前記通知部は、前記適切なアプリケーションが複数ある場合には、アプリケーション間で所定の時間間隔を置いて通知を行う、

上記（１）乃至（９）のいずれかに記載の情報処理装置。

[0135] （１１）前記通知部は、サーバから取得したアプリケーション毎の情報に基づいて前記適切なアプリケーションへの通知を行う、

上記（１）乃至（１０）のいずれかに記載の情報処理装置。

[0136] （１２）サーバから取得したアプリケーション毎の前記情報は、通知の優先度、通知期限、通知期限を超過時の動作のうち少なくとも１つを含む、

上記（１１）に記載の情報処理装置。

[0137] （１３）前記デバイスは非接触通信を通じて前記外部装置とのトランザクションを行う、

上記（１）乃至（１２）のいずれかに記載の情報処理装置。

[0138] （１３-１）前記非接触通信は、相互認証及び暗号化を行う通信である、

上記（１３）に記載の情報処理装置。

[0139] （１４）前記トランザクションは、前記情報処理装置にインストールされたアプリケーションの起動不要で予告なく発生する、

上記（１）乃至（１３）のいずれかに記載の情報処理装置。

[0140] （１５）外部装置とトランザクションを行うデバイスを搭載する機器における情報処理方法であって、

前記デバイスと前記外部装置間でトランザクションが発生したことを検知する検知ステップと、

前記検知ステップにおいて前記トランザクションの発生を検知したことに応じて、前記デバイスからデータを取得する取得ステップと、

前記取得ステップにおいて取得したデータを解析して、通知対象のアプリケーションを判定する判定ステップと、

前記通知対象のアプリケーションの正当性を検証する検証ステップと、

前記通知対象のうち正当性が確認された適切なアプリケーションに、前記取得において取得したデータを通知する通知ステップと、

を有する情報処理方法。

[0141] （１６）外部装置とトランザクションを行うデバイスを搭載する情報処理装置を、

前記デバイスの前記外部装置間でトランザクションが発生したことを検知する検知部、

前記検知部が前記トランザクションの発生を検知したことに応じて、前記デバイスからデータを取得する取得部、

前記取得部が取得したデータを解析して、通知対象のアプリケーションを判定する判定部、

前記通知対象のアプリケーションの正当性を検証する検証部、

前記通知対象のうち正当性が確認された適切なアプリケーションに、前記

取得部が取得したデータを通知する通知部、

として機能させるようにコンピュータ可読形式で記述されたコンピュータプログラム。

[0142] （１７）外部装置とトランザクションを行うデバイスを搭載するとともに、前記トランザクションに関連するサービスを提供するアプリケーションをインストールした情報処理装置であって、

前記アプリケーションに前記トランザクションの処理対象データを通知する通知部と、

前記アプリケーションが受信した処理対象データに関する前記情報を提示する提示部と、

を具備する情報処理装置。

[0143] （１８）前記アプリケーションとサーバとの連携により、前記セキュアエレメントにアクセスするアクセス部をさらに備える、

上記（１７）に記載の情報処理装置。

[0144] （１９）外部装置とトランザクションを行うデバイスを搭載するとともに、前記トランザクションに関連するサービスを提供するアプリケーションをインストールした機器において、前記アプリケーションによって実行される情報処理方法であって、

前記トランザクションの処理対象データを受信する受信ステップと、

前記受信した処理対象データに関する情報を提示する提示ステップと、

を有する情報処理方法。

[0145] （２０）外部装置とトランザクションを行うデバイスを搭載するとともに、前記トランザクションに関連するサービスを提供するアプリケーションをインストールした情報処理装置を、

前記トランザクションの処理対象データを受信する受信部、

前記受信した処理対象データに関する情報を提示する提示部、

として機能させるようにコンピュータ可読形式で記述されたコンピュータプログラム。

符号の説明

[0146] １００…情報処理装置、１０１…ＣＰＵ、１０２…ＲＯＭ
１０３…ＲＡＭ、１０４…ホストバス、１０５…ブリッジ
１０６…拡張バス、１０７…インターフェース部、１０８…入力部、
１０９…出力部、１１０…ストレージ部、１１１…ドライブ
１１２…リムーバブル記録媒体、１１３…通信部
１１４…セキュアエレメント部、１２０…リーダライタ
２０１…アンテナ部、２０２…アナログ部、２０３…デジタル部
２０４…メモリ、２０５…外部インターフェース（外部ＩＦ）

請求の範囲

[請求項1] 外部装置とトランザクションを行うデバイスを搭載する情報処理装置であって、

前記デバイスと前記外部装置間でトランザクションが発生したことを検知する検知部と、

前記検知部が前記トランザクションの発生を検知したことに応じて、前記デバイスからデータを取得する取得部と、

前記取得部が取得したデータを解析して、通知対象のアプリケーションを判定する判定部と、

前記通知対象のアプリケーションの正当性を検証する検証部と、

前記通知対象のうち正当性が確認された適切なアプリケーションに、前記取得部が取得したデータを通知する通知部と、

を具備する情報処理装置。

[請求項2] 前記検知部は、オペレーティングシステムからの発信に基づいて前記トランザクションの発生を検知する、

請求項１に記載の情報処理装置。

[請求項3] 前記取得部は、ＯＭＡＰＩ（Ｏｐｅｎ　ｍｏｂｉｌｅ　ＡＰＩ）を介して前記デバイスからデータを取得する、

請求項１に記載の情報処理装置。

[請求項4] 前記取得部は、前記トランザクションの処理対象データ及び前記トランザクションの処理に関するデータを取得する、

請求項１乃至３のいずれかに記載の情報処理装置。

[請求項5] 前記判定部は、前記取得部が取得したデータに基づいて前記トランザクションに関連するサービスＩＤを特定し、前記サービスＩＤに基づいて通知対象のアプリケーションを判定する、

請求項１に記載の情報処理

[請求項6] 前記判定部は、前記取得部が取得した前記トランザクションの処理に関するデータを解析して前記トランザクションに関連するサービス

ＩＤを特定する、

請求項５に記載の情報処理装置。

[請求項7] 前記検証部は、サーバから取得したアプリケーションの検証情報とオペレーティングシステムから取得したアプリケーションの情報に基づいて、アプリケーションの正当性を検証する、

請求項１に記載の情報処理装置。

[請求項8] 検証情報は、アプリケーションのパッケージ名及び署名値を含む、

請求項７に記載の情報処理装置。

[請求項9] 前記通知部は、前記適切なアプリケーションに対して前記トランザクションの処理対象データを通知する、

請求項１に記載の情報処理装置。

[請求項10] 前記通知部は、前記適切なアプリケーションが複数ある場合には、アプリケーション間で所定の時間間隔を置いて通知を行う、

請求項１に記載の情報処理装置。

[請求項11] 前記通知部は、サーバから取得したアプリケーション毎の情報に基づいて前記適切なアプリケーションへの通知を行う、

請求項１に記載の情報処理装置。

[請求項12] サーバから取得したアプリケーション毎の前記情報は、通知の優先度、通知期限、通知期限を超過時の動作のうち少なくとも１つを含む、

請求項１１に記載の情報処理装置。

[請求項13] 前記デバイスは非接触通信を通じて前記外部装置とのトランザクションを行う、

請求項１に記載の情報処理装置。

[請求項14] 前記トランザクションは、前記情報処理装置にインストールされたアプリケーションの起動不要で予告なく発生する、

請求項１に記載の情報処理装置。

[請求項15] 外部装置とトランザクションを行うデバイスを搭載する機器におけ

る情報処理方法であって、

前記デバイスと前記外部装置間でトランザクションが発生したことを検知する検知ステップと、

前記検知ステップにおいて前記トランザクションの発生を検知したことに応じて、前記デバイスからデータを取得する取得ステップと、

前記取得ステップにおいて取得したデータを解析して、通知対象のアプリケーションを判定する判定ステップと、

前記通知対象のアプリケーションの正当性を検証する検証ステップと、

前記通知対象のうち正当性が確認された適切なアプリケーションに、前記取得において取得したデータを通知する通知ステップと、

を有する情報処理方法。

[請求項16] 外部装置とトランザクションを行うデバイスを搭載する情報処理装置を、

前記デバイスの前記外部装置間でトランザクションが発生したことを検知する検知部、

前記検知部が前記トランザクションの発生を検知したことに応じて、前記デバイスからデータを取得する取得部、

前記取得部が取得したデータを解析して、通知対象のアプリケーションを判定する判定部、

前記通知対象のアプリケーションの正当性を検証する検証部、

前記通知対象のうち正当性が確認された適切なアプリケーションに、前記取得部が取得したデータを通知する通知部、

として機能させるようにコンピュータ可読形式で記述されたコンピュータプログラム。

[請求項17] 外部装置とトランザクションを行うデバイスを搭載するとともに、前記トランザクションに関連するサービスを提供するアプリケーションをインストールした情報処理装置であって、

前記アプリケーションに前記トランザクションの処理対象データを通知する通知部と、

前記アプリケーションが受信した処理対象データに関する前記情報を提示する提示部と、

を具備する情報処理装置。

[請求項18] 前記アプリケーションとサーバとの連携により、前記セキュアエレメントにアクセスするアクセス部をさらに備える、

請求項１７に記載の情報処理装置。

[請求項19] 外部装置とトランザクションを行うデバイスを搭載するとともに、前記トランザクションに関連するサービスを提供するアプリケーションをインストールした機器において、前記アプリケーションによって実行される情報処理方法であって、

前記トランザクションの処理対象データを受信する受信ステップと、

前記受信した処理対象データに関する情報を提示する提示ステップと、

を有する情報処理方法。

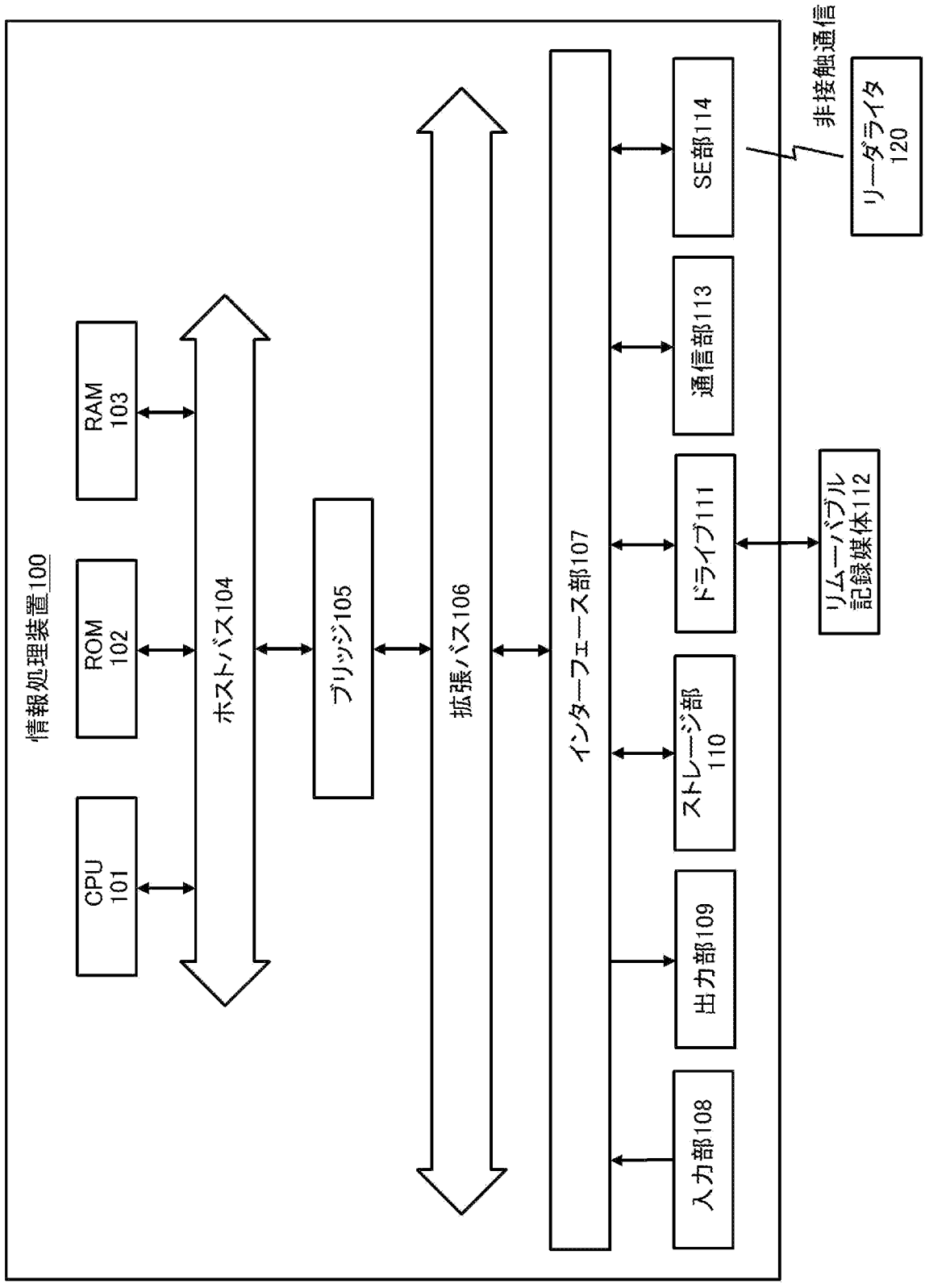
[請求項20] 外部装置とトランザクションを行うデバイスを搭載するとともに、前記トランザクションに関連するサービスを提供するアプリケーションをインストールした情報処理装置を、

前記トランザクションの処理対象データを受信する受信部、

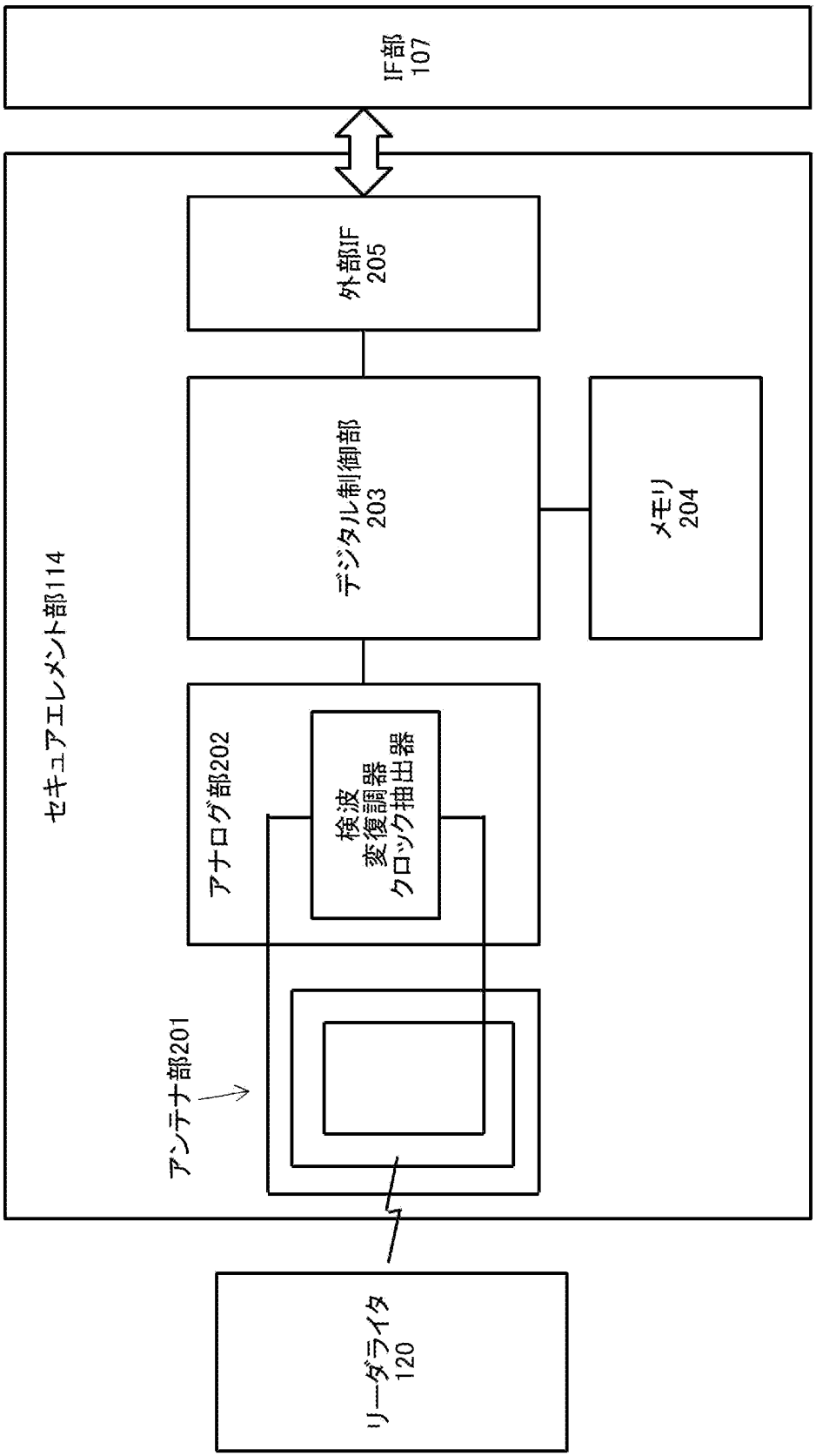
前記受信した処理対象データに関する情報を提示する提示部、

として機能させるようにコンピュータ可読形式で記述されたコンピュータプログラム。

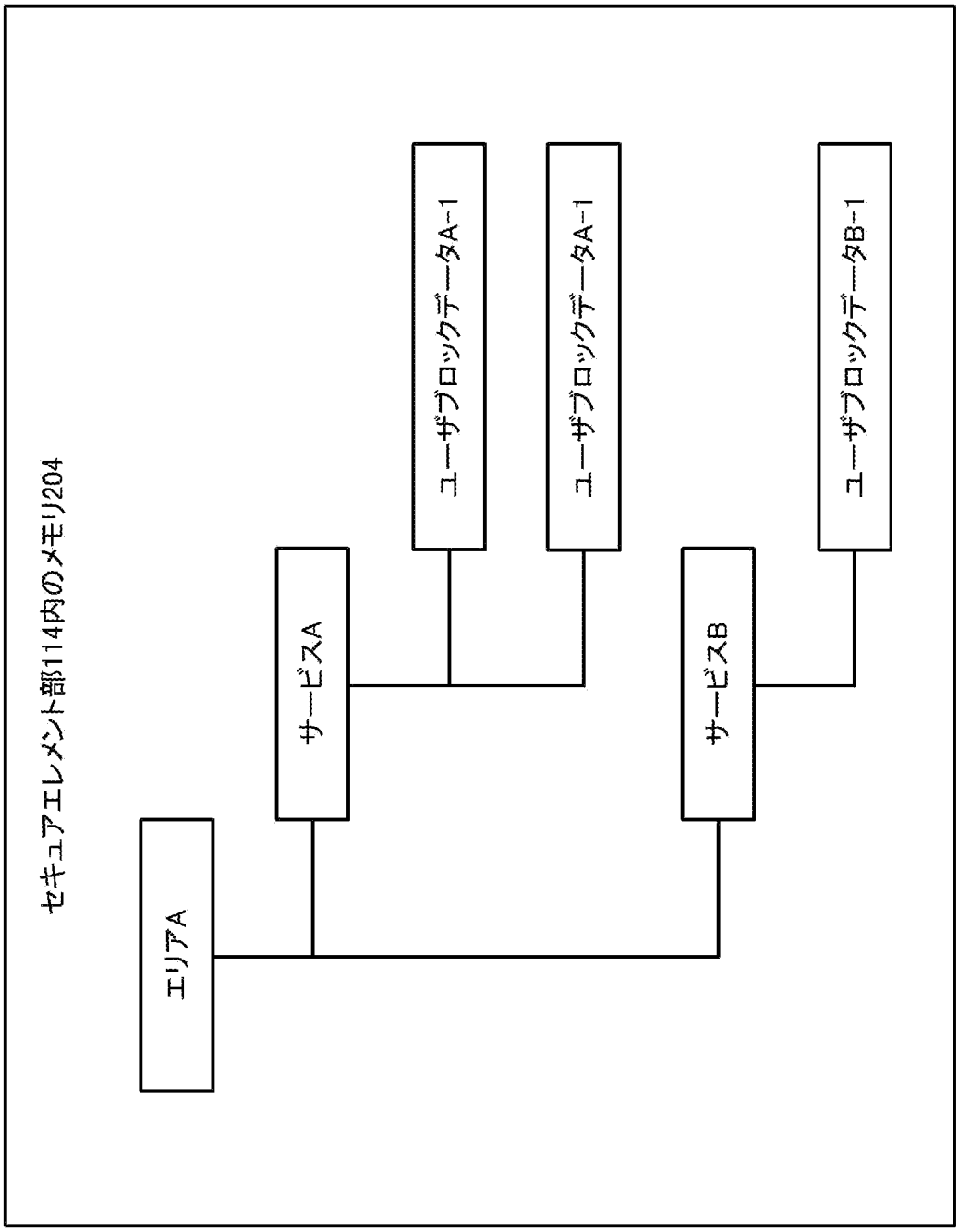
[図1]


情報処理装置100
CPU 101
ROM 102
RAM 103
ホストバス104
ブリッジ105
拡張バス106
インターフェース部107
入力部108
出力部109
ストレージ部 110
ドライブ111
リムーバブル記録媒体112
通信部113
SE部114
非接触通信
リーダライタ 120

[図2]


IF部
107
外部IF
205
デジタル制御部
203
メモリ
204
セキュアエレメント部114
アナログ部202
検波
変復調器
クロック抽出器
アンテナ部201
リーダライタ
120

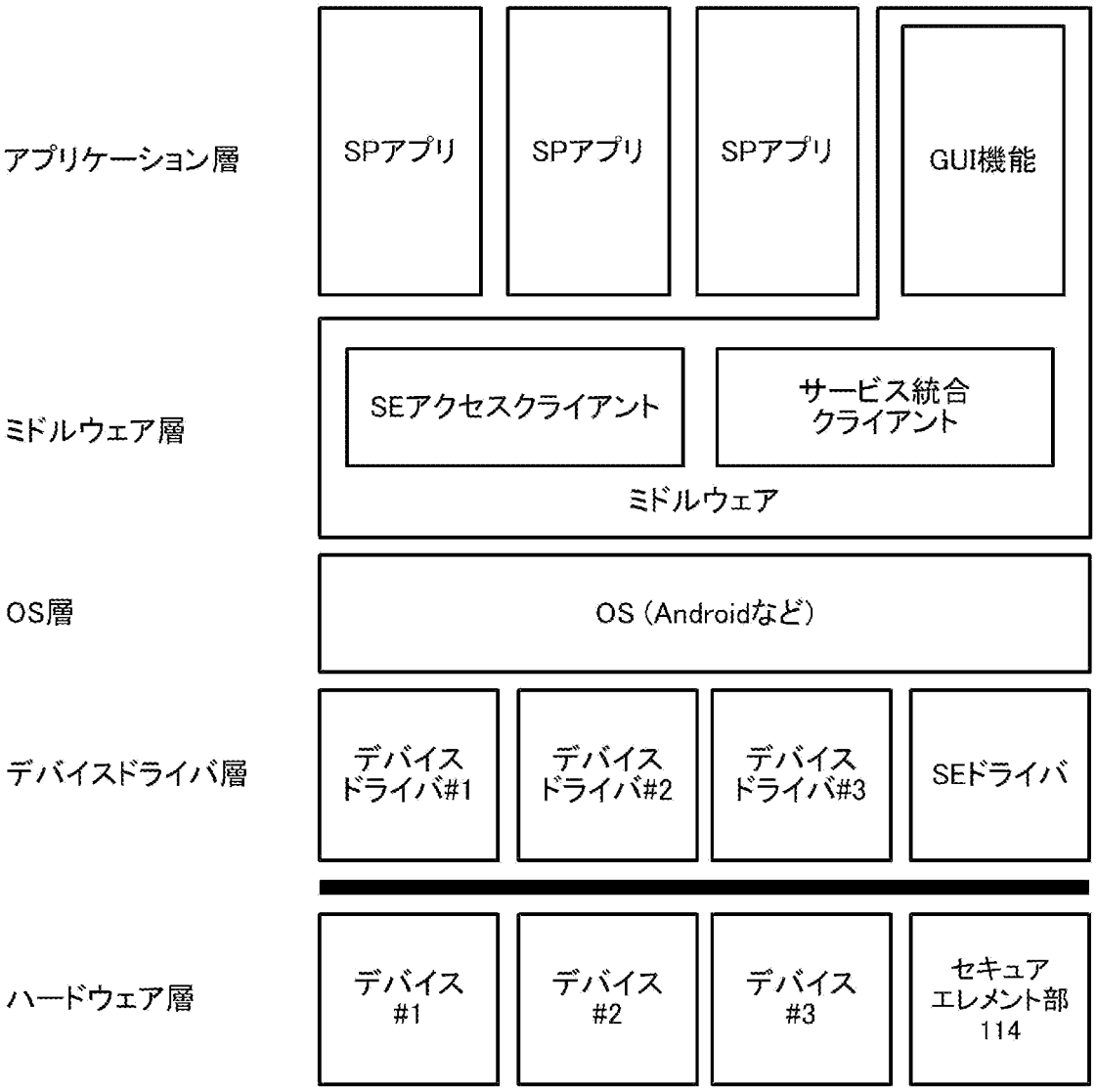
[図3]


セキュアエレメント部114内のメモリ204
エリアA
サービスA
サービスB
ユーザブロックデータA-1
ユーザブロックデータA-1
ユーザブロックデータB-1

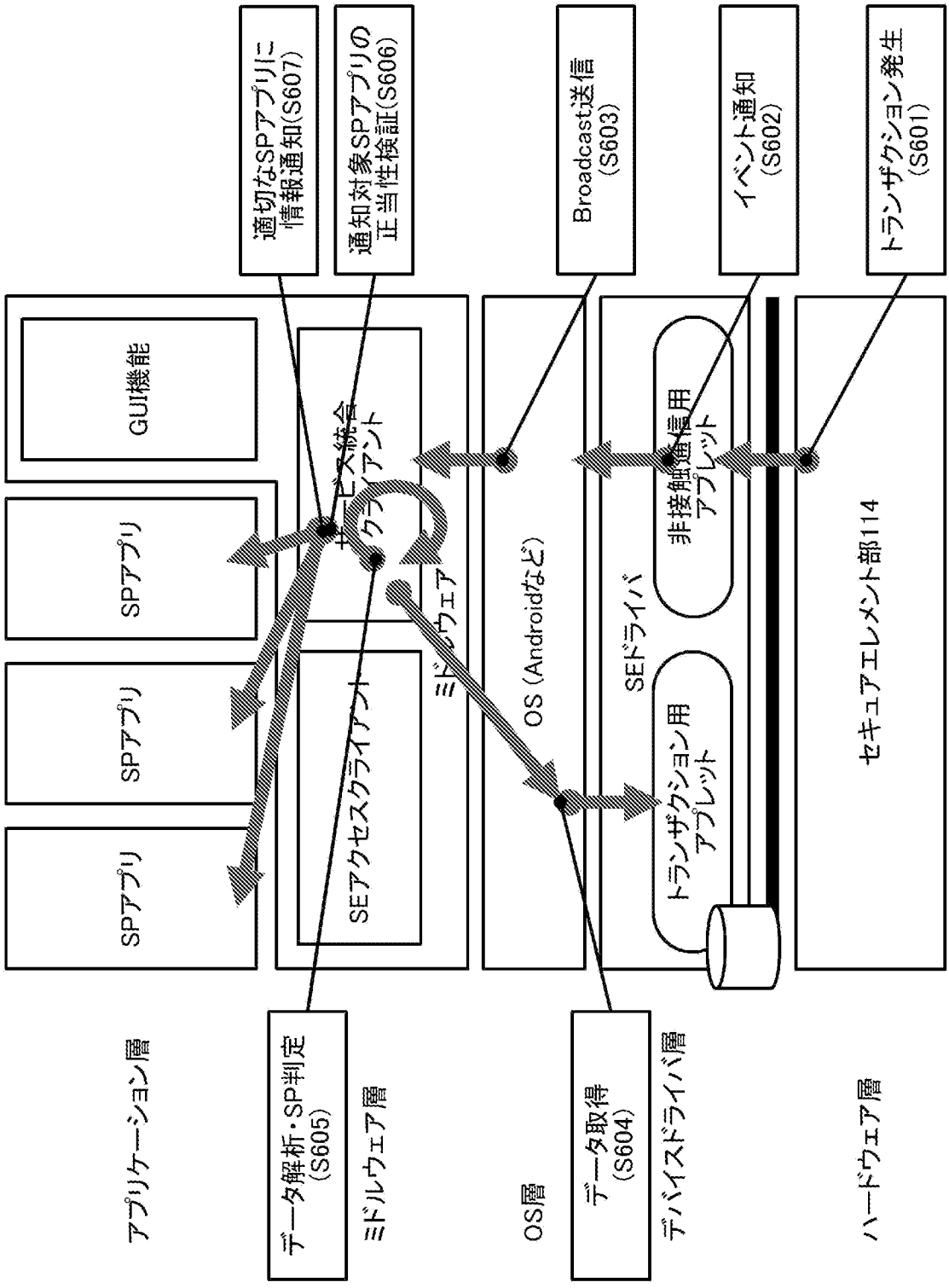
[図4]

No.	パス	処理対象データ	ハッシュ値
1	エリアA/サービスA/ユーザブロックデータA-1	データA	2035FA…93CF
2	エリアA/サービスA/ユーザブロックデータA-1	データB	A157CB…BB3A
3	エリアA/サービスA/ユーザブロックデータA-1	データC	7DC80F…ABFF
…	…	…	…

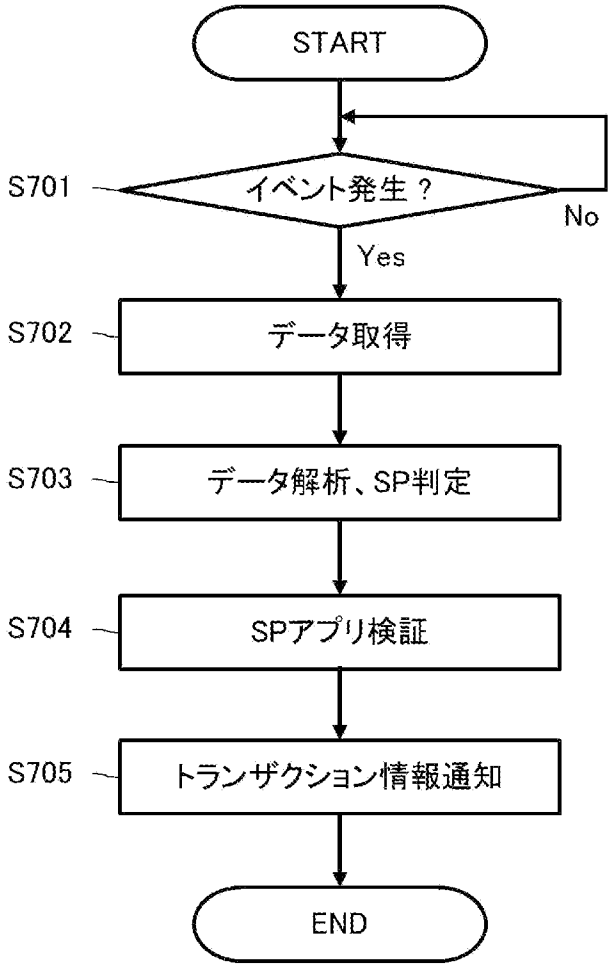
[図5]


アプリケーション層
SPアプリ
SPアプリ
SPアプリ
GUI機能
ミドルウェア層
SEアクセスクライアント
サービス統合
クライアント
ミドルウェア
OS層
OS (Androidなど)
デバイスドライバ層
デバイス
ドライバ#1
デバイス
ドライバ#2
デバイス
ドライバ#3
SEドライバ
ハードウェア層
デバイス
#1
デバイス
#2
デバイス
#3
セキュア
エレメント部
114

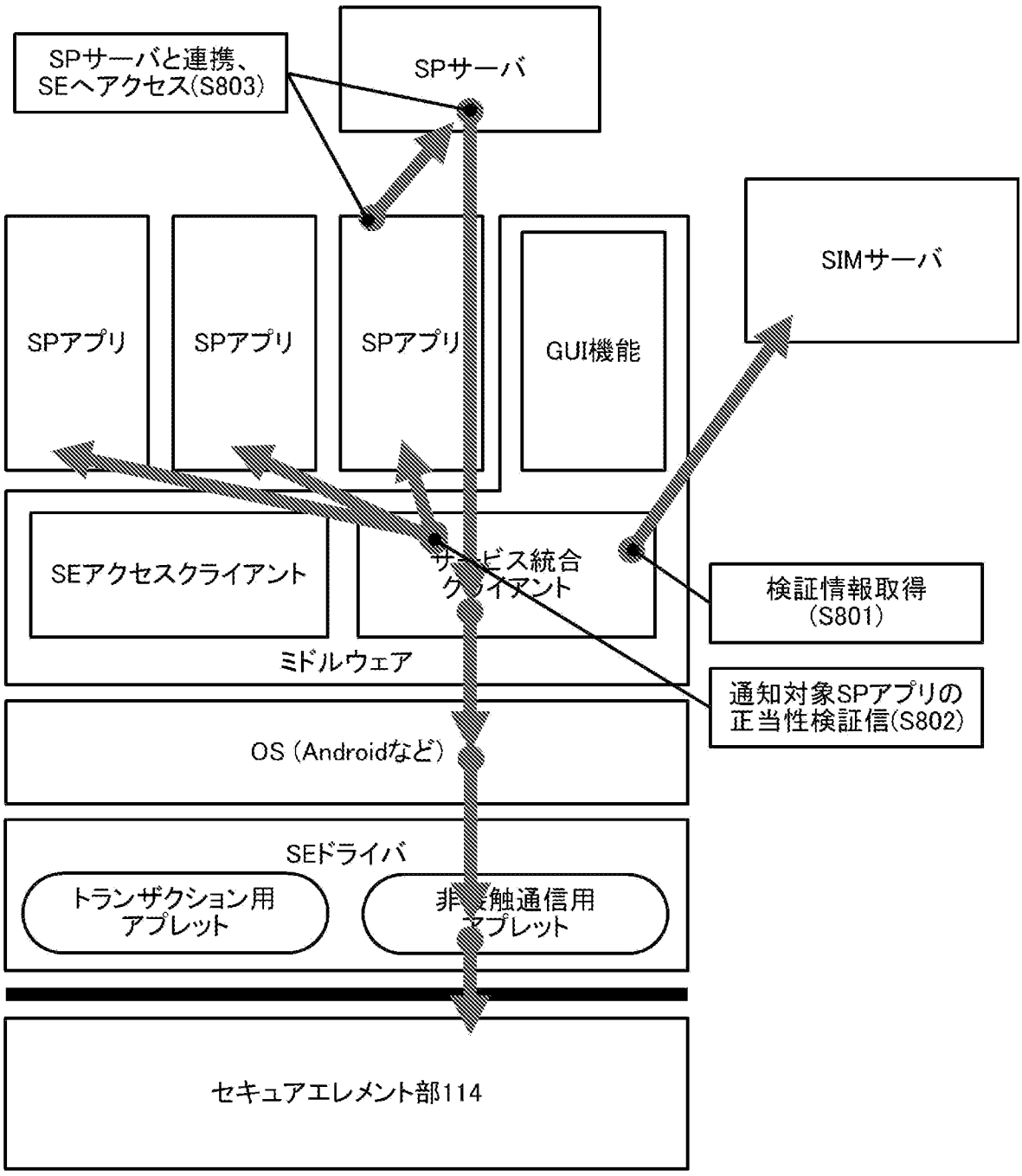
[図6]


適切なSPアプリに情報通知(S607)
通知対象SPアプリの正当性検証(S606)
Broadcast送信(S603)
イベント通知(S602)
トランザクション発生(S601)
GUI機能
SPアプリ
SPアプリ
SPアプリ
サービス統合クライアント
SEアクセスクライアント
ミドルウェア
OS (Androidなど)
SEドライバ
非接触通信用アプレット
トランザクション用アプレット
セキュアエレメント部114
データ解析・SP判定(S605)
データ取得(S604)
アプリケーション層
ミドルウェア層
OS層
デバイスドライバ層
ハードウェア層

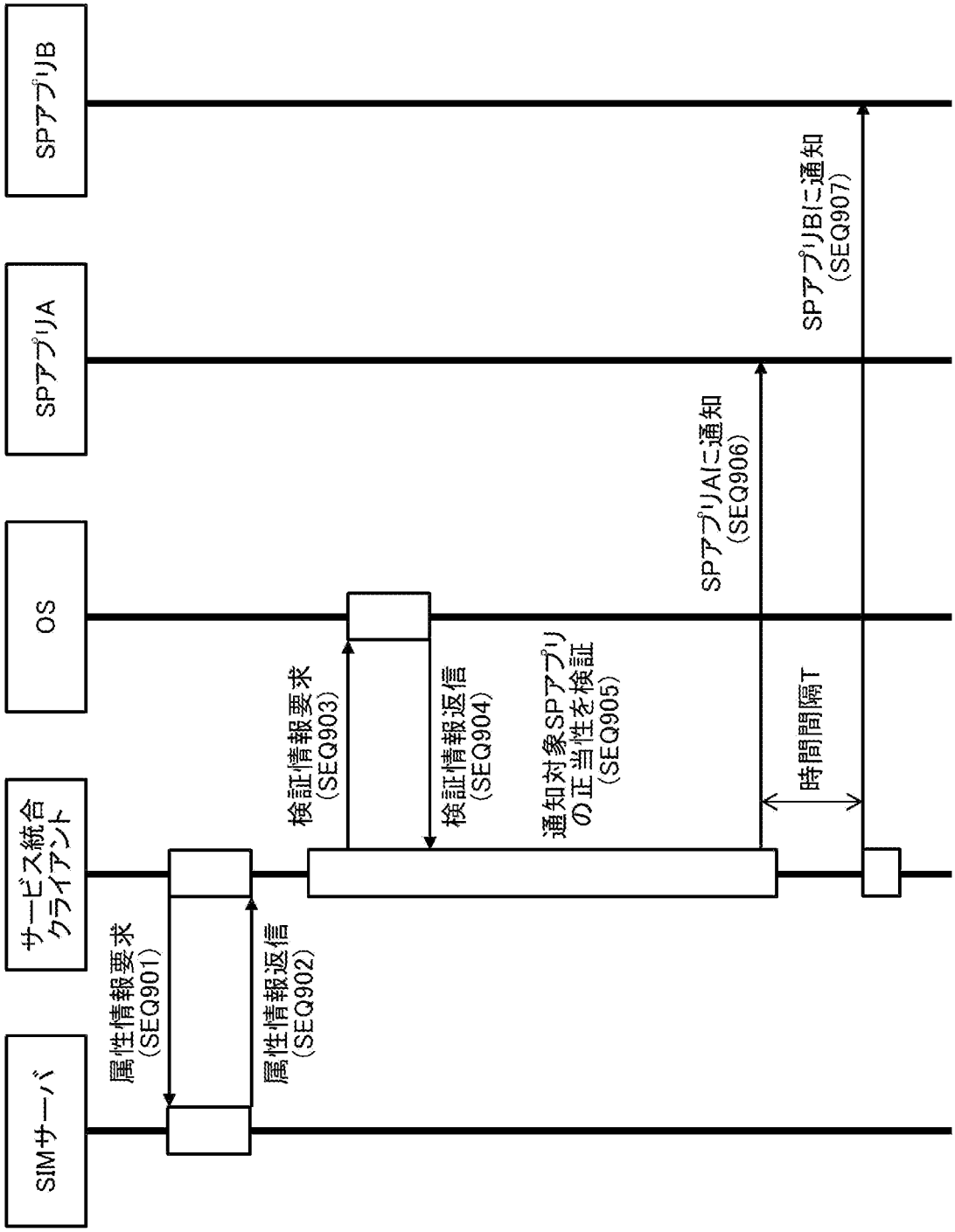
[図7]


START
S701
イベント発生？
No
Yes
S702
データ取得
S703
データ解析、SP判定
S704
SPアプリ検証
S705
トランザクション情報通知
END

[図8]


SPサーバと連携、
SEへアクセス(S803)
SPサーバ
SIMサーバ
SPアプリ
SPアプリ
SPアプリ
GUI機能
SEアクセスクライアント
サービス統合
クライアント
検証情報取得
(S801)
ミドルウェア
通知対象SPアプリの
正当性検証信(S802)
OS (Androidなど)
SEドライバ
トランザクション用
アプレット
非接触通信用
アプレット
セキュアエレメント部114

[図9]


SIMサーバ
サービス統合クライアント
OS
SPアプリA
SPアプリB
属性情報要求 (SEQ901)
属性情報返信 (SEQ902)
検証情報要求 (SEQ903)
検証情報返信 (SEQ904)
通知対象SPアプリの正当性を検証 (SEQ905)
SPアプリAに通知 (SEQ906)
SPアプリBに通知 (SEQ907)
時間間隔T

[図10]

No.	項目	データ
1	サービスID	"SV123456"などの英数で、サービスを一意に特定する値 ミドルウェア開発主体が払い出す
2	SPアプリを一意に特定する情報	"com.spapp.app"などのパッケージ名など 通知先SPアプリを一意に特定する値
3	SPアプリの検証情報	16進数 アプリ署名者証明書ハッシュ値など
4	優先度	1(優先度高)～10(優先度低)
5	通知期限	0：リアルタイム 1：遅延容認(10分以内) 2：遅延容認(60分以内) 3：遅延容認(1日以内)
6	通知期限超過時の動作	0：通知を諦める 1：期限に関わらず、その時点で通知する

[図11]

No.	項目	データ
1	サービスID	トランザクションが行われたサービスのID
2	CID	カードを識別するためのID
3	R/W ID	利用された場所を特定するR/Wの固有ID
4	R/W 利用日時	R/Wを利用した日時
5	R/W トランザクションID	R/Wで発生したトランザクションID
6	利用種別	支払い、チャージ、スタンプ、クーポン、チケットなどの種別
7	ペイロード	利用種別に応じたデータ構造

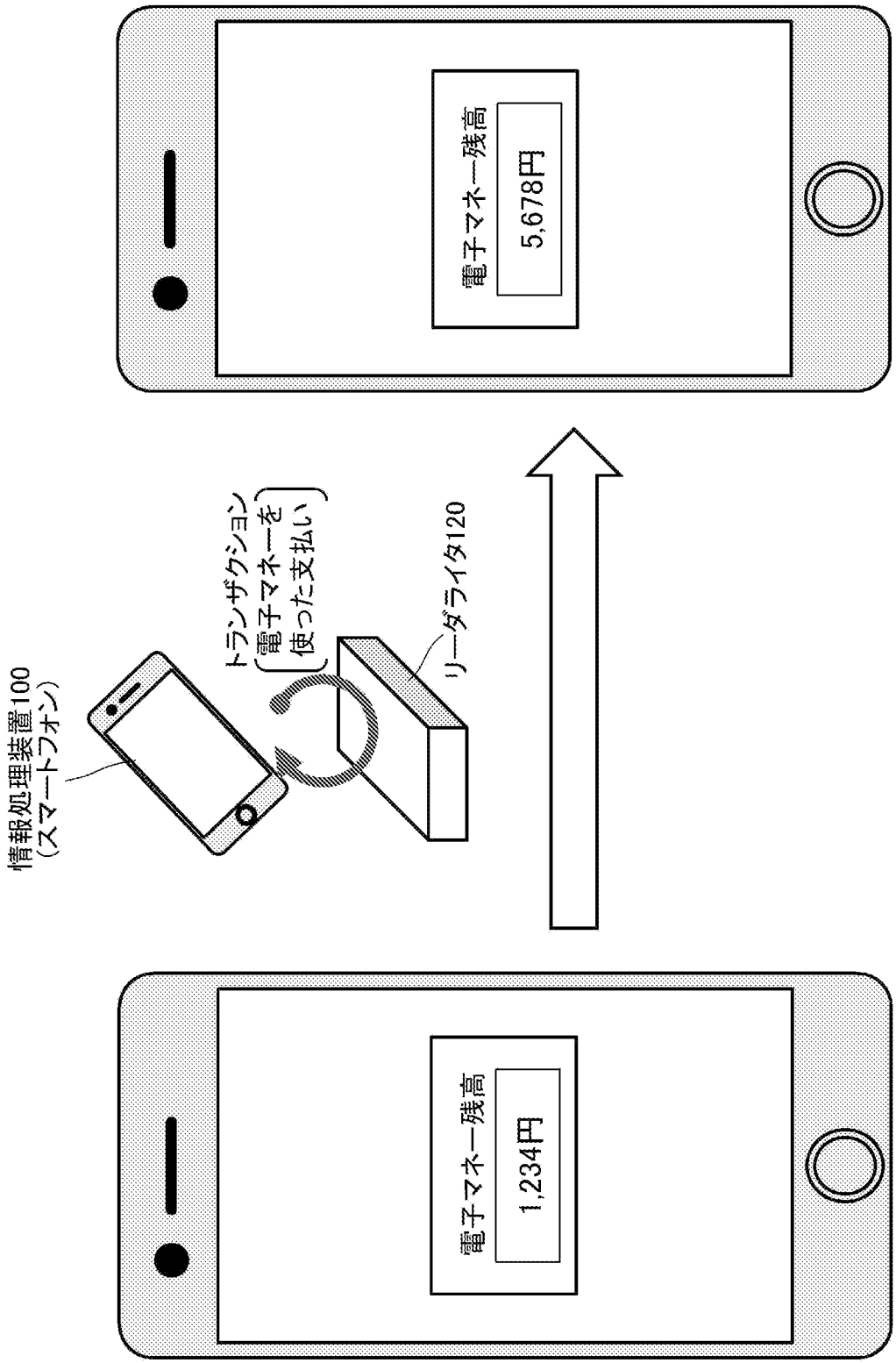
[図12]

No.	項目	データ
8	利用金額	123円の「123」など
9	残高	345円の「345」など
10	ポイント増減	±678Pの「±678」など
11	ポイント残高	910Pの「910」など

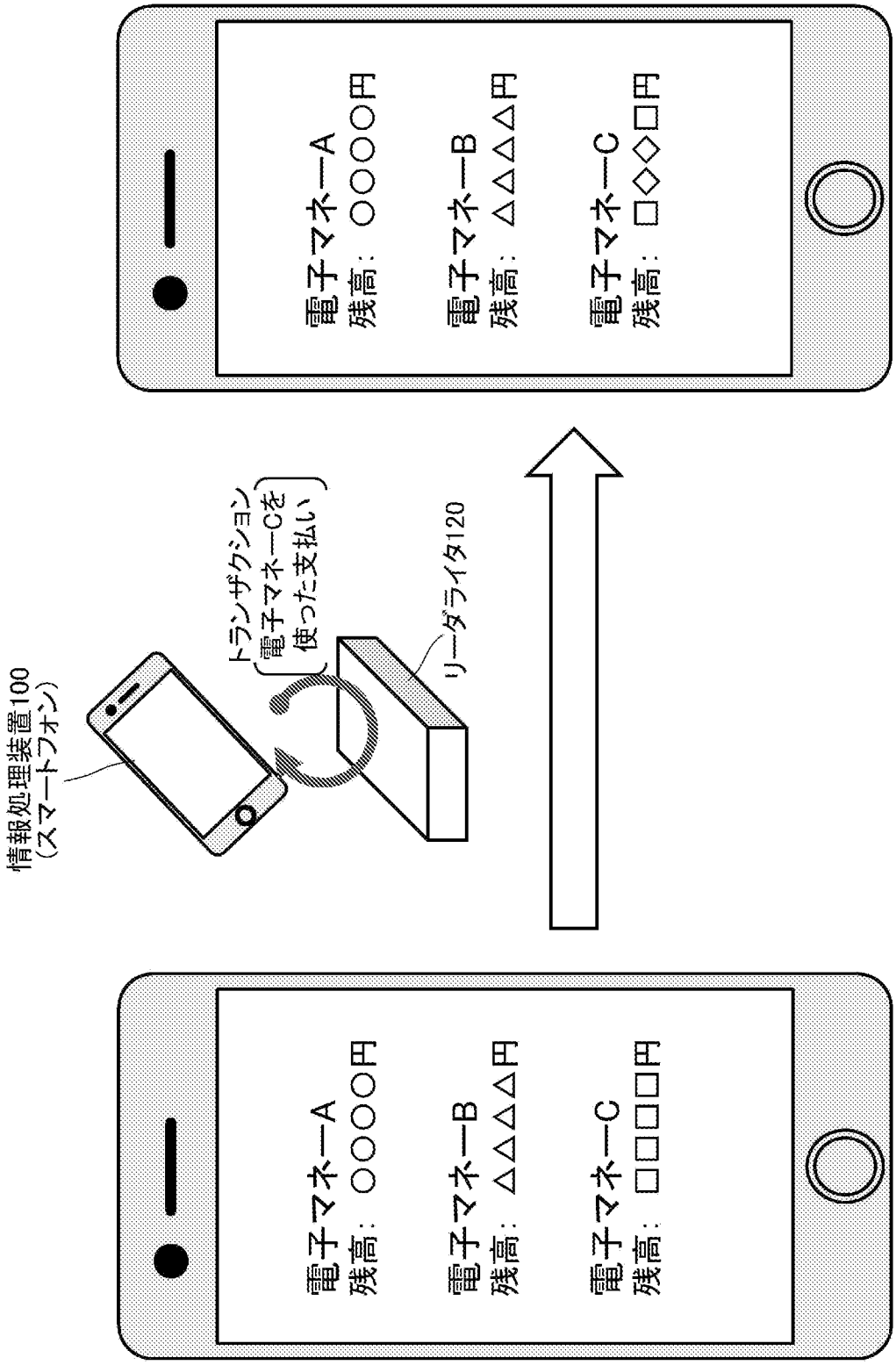
[図13]

No.	項目	データ
8	サービス固有特定ID	サービス事業者で定義できる固有ID (チケット特定ID、クーポン特定IDなど)
9	券面・デザイン情報	スタンプや券面デザインを定義する情報 (取得先URLの一部に利用するIDなど

[図14]


電子マネー残高
1,234円
情報処理装置100
(スマートフォン)
トランザクション
(電子マネーを
使った支払い)
リーダライタ120
電子マネー残高
5,678円

[図15]


電子マネーA
残高：○○○○円
電子マネーB
残高：△△△△円
電子マネーC
残高：□□□□円
情報処理装置100
（スマートフォン）
トランザクション
（電子マネーCを
使った支払い）
リーダライタ120
電子マネーA
残高：○○○○円
電子マネーB
残高：△△△△円
電子マネーC
残高：□◇◇□円

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2022/003807

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62(2013.01)i; ***G06F 21/44***(2013.01)i
FI: G06F21/62; G06F21/44

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)

G06F21/62; G06F21/44; G06K19/00

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2022
Registered utility model specifications of Japan 1996-2022
Published registered utility model applications of Japan 1994-2022

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	JP 2005-050262 A (MATSUSHITA ELECTRIC IND CO LTD) 24 February 2005 (2005-02-24) paragraphs [0049]-[0052], [0060]-[0061], fig. 1, 3	17, 19-20
Y		18
A		1-16
Y	JP 2011-028688 A (FELICA NETWORKS INC) 10 February 2011 (2011-02-10) paragraphs [0053]-[0060], fig. 2, 5	18

☐ 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
07 April 2022	**19 April 2022**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2022/003807

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2005-050262 A	24 February 2005	US 2005/0023345 A1 paragraphs [0107]-[0110], [0118]-[0119], fig. 1, 3 EP 1503352 A1 CN 1591452 A	
JP 2011-028688 A	10 February 2011	US 2011/0029779 A1 paragraphs [0084]-[0092], fig. 2, 5 EP 2336962 A2 CN 101989982 A	

国際調査報告

国際出願番号
PCT/JP2022/003807

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06F 21/62(2013.01)i; G06F 21/44(2013.01)i
FI: G06F21/62; G06F21/44

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））

G06F21/62; G06F21/44; G06K19/00

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	１９７１－２０２２年
日本国実用新案登録公報	１９９６－２０２２年
日本国登録実用新案公報	１９９４－２０２２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	関連する請求項の番号
X	JP 2005-050262 A (松下電器産業株式会社) 24.02.2005 (2005-02-24) 段落[0049]-[0052],[0060]-[0061], 図1,3	17,19-20
Y		18
A		1-16
Y	JP 2011-028688 A (フェリカネットワークス株式会社) 10.02.2011 (2011-02-10) 段落[0053]-[0060], 図2,5	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抵触するものではなく、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
07.04.2022	19.04.2022

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
田名網　忠雄 5S 6306

電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2022/003807

引用文献	公表日	パテントファミリー文献	公表日
JP 2005-050262 A	24.02.2005	US 2005/0023345 A1 段落[0107]-[0110],[0118]-[0119], 図1,3 EP 1503352 A1 CN 1591452 A	
JP 2011-028688 A	10.02.2011	US 2011/0029779 A1 段落[0084]-[0092], 図2,5 EP 2336962 A2 CN 101989982 A	