明　細　書

発明の名称 ： 情報処理装置および情報処理方法

技術分野

[0001] 本開示は、情報処理装置および情報処理方法に関する。

背景技術

[0002] スマートフォンを含む携帯電話端末においては、非接触ＩＣ（Integrated Circuit）タグやＲＦＩＤ（Radio Frequency Identification）タグ等を備えることで、近距離（近接）無線通信機能を有し、例えば数センチ程度に近接したリーダライタとの間で無線通信が可能な端末が開発されている。例えば、非接触ＩＣタグに備えられるセキュアエレメントが、近距離無線通信に伴って任意の処理を行うことで、当該携帯電話端末は、交通機関の乗車券機能、電子マネー機能、クレジットカード機能、個人認証用カード機能を実現することができる。

[0003] また、これらの各種機能の処理に用いられたデータを有効活用する技術も開発されている。例えば、以下の特許文献１には、近距離無線通信を介した代金決済処理が行われた場合に、代金決済処理の履歴データと、ユーザによって別個に入力されたデータとを対応付けて有効活用する技術が開示されている。

先行技術文献

特許文献

[0004] 特許文献1：特開２００８－１４１４００号公報

発明の概要

発明が解決しようとする課題

[0005] しかし、特許文献１に記載の技術等によっては、携帯電話端末が、セキュアエレメント（保護記憶部）による処理のタイミングを把握し、有効活用することができなかった。より具体的に説明すると、セキュアエレメントは、携帯電話端末（または携帯電話端末に接続する外部装置）に備えられる時刻

取得機能にアクセスすることができないため、処理のタイミングに関するデータを記録しておくことができない。したがって、処理後に、携帯電話端末が当該処理に関するデータをセキュアエレメントから取得しても、取得したデータの中に処理のタイミングに関するデータが含まれないため、携帯電話端末は、セキュアエレメントによる処理のタイミングを把握し、有効活用することができない。

[0006] そこで、本開示は、上記に鑑みてなされたものであり、本開示は、携帯電話端末等の情報処理装置が、セキュアエレメント等の保護記憶部による処理のタイミングを把握し、有効活用することが可能な、新規かつ改良された情報処理装置および情報処理方法を提供する。

課題を解決するための手段

[0007] 本開示によれば、保護記憶部からの通知に基づいて、前記保護記憶部による処理のタイミングに関するデータを取得するデータ取得部と、前記処理のタイミングに関するデータと前記処理に関するデータとを対応付ける制御部と、を備える、情報処理装置が提供される。

[0008] また、本開示によれば、保護記憶部からの通知に基づいて、前記保護記憶部による処理のタイミングに関するデータを取得することと、前記処理のタイミングに関するデータと前記処理に関するデータとを対応付けることと、を有する、コンピュータにより実行される情報処理方法が提供される。

発明の効果

[0009] 以上説明したように本開示によれば、情報処理装置が、保護記憶部による処理のタイミングを把握し、有効活用することが可能となる。

[0010] なお、上記の効果は必ずしも限定的なものではなく、上記の効果とともに、または上記の効果に代えて、本明細書に示されたいずれかの効果、または本明細書から把握され得る他の効果が奏されてもよい。

図面の簡単な説明

[0011] [図1]本実施形態に係る情報処理システムの構成例を示す図である。

[図2]情報処理装置１００の機能構成例を示すブロック図である。

[図3]第１の記憶部１２２が有するデータ構造について説明する図である。

[図4]第２の記憶部１２３が記憶するデータの一例について説明する図である。

[図5]記憶部１１３が記憶するデータの一例について説明する図である。

[図6]情報処理装置１００とリーダライタ３００との近距離無線通信に伴って行われる処理フローの例を示すシーケンス図である。

[図7]情報処理装置１００とサーバ２００との通信に伴って行われる処理フローの例を示すシーケンス図である。

[図8]情報処理装置１００のハードウェア構成例を示すブロック図である。

発明を実施するための形態

[0012] 以下に添付図面を参照しながら、本開示の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

[0013] なお、説明は以下の順序で行うものとする。

１．背景

２．実施形態

２．１．システム構成例

２．２．セキュアエレメント１２０の機能構成例

２．３．デバイスホスト１１０の機能構成例

２．４．処理フローの例

２．５．情報処理装置１００のハードウェア構成例

３．まとめ

[0014] ＜１．背景＞

まず、本開示の背景について説明する。

[0015] 上記のとおり、スマートフォンを含む携帯電話端末においては、例えば、非接触ＩＣタグに備えられるセキュアエレメントが、近距離無線通信に伴って任意の処理を行う。これによって、当該携帯電話端末は、交通機関の乗車

券機能、電子マネー機能、クレジットカード機能、個人認証用カード機能を実現することができる。

[0016] ここで、セキュアエレメントは、処理のタイミングに関するデータ（例えば、処理が行われた日時のデータ等）を取得し、記録することができない。より具体的に説明すると、セキュアエレメントは、携帯電話端末（または携帯電話端末に接続する外部装置）に備えられる時刻取得機能にアクセスすることができないため、処理のタイミングに関するデータを取得することができない。したがって、セキュアエレメントは、処理のタイミングに関するデータを処理対象データに対応付けて記憶しておくことができない。

[0017] また、セキュアエレメントには、処理のタイミングに関するデータ以外にも取得することができないデータが存在する。例えば、セキュアエレメントは、セキュアエレメント外に備えられた各種センサまたは各種装置に対してアクセスできないことを理由に、処理が行われた際の携帯電話端末の位置に関するデータ、当該位置の周辺状況に関するデータ、携帯電話端末の使用者に関するデータ、または、携帯電話端末の動作もしくは使用者の動作に関するデータ等を取得することができない。したがって、セキュアエレメントは、これらのデータを処理対象データに対応付けて記憶することができない。

[0018] また、近距離無線通信によってセキュアエレメントと外部装置との間で行われる処理は、基本的に、セキュアエレメントと外部装置との間で完結するため、携帯電話端末に備えられるデバイスホストは、当該処理の内容を知ることができない。

[0019] また、セキュアエレメントに記憶されているデータの更新処理が行われた場合、デバイスホストが、セキュアエレメント内に記憶されている処理対象データを取得したとしても、当該更新処理の内容を知ることができない場合がある。例えば、デバイスホストが処理対象データを取得する前に、セキュアエレメントに記憶されているデータの更新処理が複数回行われた場合、デバイスホストは各更新処理の内容を把握することができない。

[0020] 本件の開示者は、上記事情に鑑みて、本開示の技術を創作するに至った。

以降では、本開示の一実施形態について説明していく。

[0021] ＜２．実施形態＞

上記では、本開示の背景について説明した。続いて、本開示の一実施形態について説明する。

[0022] （２．１．システム構成例）

まず、図１および図２を参照して、本実施形態に係る情報処理システムの構成例について説明する。

[0023] 図１に示すように、本実施形態に係る情報処理システムは、情報処理装置１００と、サーバ２００と、リーダライタ３００と、を備える。また、図２に示すように、情報処理装置１００は、デバイスホスト１１０と、セキュアエレメント１２０と、ＣＬＦ（Contactless Front End）１３０と、を備える。

[0024] （情報処理装置１００）

情報処理装置１００は、所定の基地局と無線通信を行うことで通話やデータの送受信を行うことができる装置である。また、情報処理装置１００は、非接触ＩＣタグを内蔵しており、その非接触ＩＣタグを用いて、所定の場所（例えば、店頭、改札または出入口等）に設置されたリーダライタ３００との非接触通信（例えば、近距離無線通信等）を行うことで、様々な処理を行うことができる。なお、当該処理の内容は特に限定されない。例えば、情報処理装置１００は、非接触ＩＣタグを用いて、代金決済処理、電子マネーチャージ処理、個人認証処理または行動管理処理等を行うことができる。また、情報処理装置１００とリーダライタ３００間の通信方式は特に限定されない。例えば、情報処理装置１００とリーダライタ３００間の通信方式は、非接触通信ではなく、接触通信であってもよい。

[0025] また、情報処理装置１００は、サーバ２００と通信を行うことでデータの送受信を行うこともできる。例えば、情報処理装置１００は、代金決済処理等の履歴データ等をサーバ２００へ送信することができる。また、情報処理装置１００は、チャージされた電子マネーに関するデータをサーバ２００か

ら受信することで、当該データを自装置に反映させることができる。なお、情報処理装置１００とサーバ２００間で送受信されるデータの内容は特に限定されない。また、情報処理装置１００とサーバ２００間の通信方式は特に限定されない。

[0026] また、上記は、情報処理装置１００がスマートフォンを含む携帯電話端末であることを想定して記載したものであるが、情報処理装置１００の種類はこれに限定されない。例えば、情報処理装置１００は、汎用コンピュータ、ＰＣ（Personal Computer）、ノート型ＰＣ、タブレット型ＰＣ、任意のウェアラブル端末、携帯型メディア再生機器または携帯型ゲーム機器等を含む任意の情報処理装置であってもよい。

[0027] （デバイスホスト１１０）

デバイスホスト１１０は、ＣＰＵ（Central Processing Unit）、ＲＯＭ（Read Only

Memory）、及びＲＡＭ（Random Access Memory）等を搭載した集積回路を備える情報処理装置である。そして、デバイスホスト１１０は、ＲＯＭが記憶している１または２以上のプログラムを用いて、オペレーティングシステムによる各種処理等を実行する。当該オペレーティングシステムの例としては、Ａｎｄｒｏｉｄ（登録商標）、ｉＯＳ、Ｗｉｎｄｏｗｓ（登録商標）等が挙げられるがこれらに限定されない。

[0028] （セキュアエレメント１２０）

セキュアエレメント１２０は、保護記憶部として機能する機能構成である。より具体的には、セキュアエレメント１２０は、耐タンパ性を有するセキュリティモジュール（例えば、セキュリティチップ等）であり、自ら備える記憶部（例えば、メモリ等）に記憶されているデータ、当該記憶部へのアクセス、自ら実行する処理等を保護することができる。さらに、セキュアエレメント１２０は、暗号機能を有し、重要データを暗号化して記憶部に記憶させることができる。

[0029] また、セキュアエレメント１２０は、外部装置との近距離無線通信に伴っ

て任意の処理を行うことができる。例えば、セキュアエレメント１２０は、外部装置からの要求に応じて自ら備える記憶部からデータを読み取ったり、データの更新を行ったりすることができる。なお、セキュアエレメント１２０による処理はこれらに限定されない。例えば、セキュアエレメント１２０は、サーバ２００またはデバイスホスト１１０との通信に伴って任意の処理を実行してもよい。例えば、セキュアエレメント１２０は、サーバ２００からの要求に応じて自ら備える記憶部からデータを読み取ったり、データの更新を行ったりしてもよい。

[0030] セキュアエレメント１２０は、情報処理装置１００内のＳＩＭ（Subscriber Identity Module）カード等に備えられ得るが、これに限定されない。例えば、セキュアエレメント１２０は、情報処理装置１００内の、ＳＩＭカード以外の任意の構成に備えられてもよいし、情報処理装置１００以外の任意の装置（例えば、サーバ２００等）に備えられてもよい。

[0031] （ＣＬＦ１３０）

ＣＬＦ１３０は、ＮＦＣ（Near Field Communication）コントローラとも呼称され、リーダライタ３００とのＮＦＣ規格に基づいた通信を行う。より具体的には、ＣＬＦ１３０は、近距離無線通信により、通信可能範囲（０～１０ｃｍの範囲）内に存在するリーダライタ３００とデータの送受信を行う。例えば、ＣＬＦ１３０は、リーダライタ３００から無線信号を受信した場合、当該無線信号に含まれるデータをデバイスホスト１１０またはセキュアエレメント１２０へ提供する。また、ＣＬＦ１３０は、デバイスホスト１１０またはセキュアエレメント１２０から提供されたデータを用いて送信用の無線信号を生成し、当該無線信号をリーダライタ３００に対して送信する。なお、ＣＬＦ１３０は、上記と同様の機能を有する別の構成に置換されてもよい。

[0032] （サーバ２００）

サーバ２００は、情報処理装置１００、または、情報処理装置１００を介して提供されるサービス等を管理するサーバである。サーバ２００は、情報

処理装置１００との所定の通信に伴って各種処理を行う。例えば、サーバ２００は、情報処理装置１００からセキュアエレメント１２０に記憶されている各種データを受信する。そして、サーバ２００は、当該データを蓄積し統計分析すること等によって、情報処理装置１００を使用するユーザの行動履歴データや嗜好データ等を出力し、これらのデータに基づいて各種サービスを提供することができる。なお、サーバ２００によって行われる処理または提供されるサービスの内容は特に限定されない。また、サーバ２００と情報処理装置１００間の通信方式は特に限定されない。

[0033] （リーダライタ３００）

リーダライタ３００は、ユーザによって情報処理装置１００がかざされた際に、情報処理装置１００と近距離無線通信を行う情報処理装置である。また、図示していないが、リーダライタ３００は、任意の情報処理装置（情報処理装置１００以外の装置）と通信することも可能である。例えば、リーダライタ３００は、店舗に備えられた任意の情報処理装置（以降、「店舗装置」と呼称する）と接続されることで、情報処理装置１００から取得した各種データ（例えば、情報処理装置１００の識別データ、電子マネーデータまたはクーポンデータ等）を店舗装置に提供することもできるし、店舗装置から提供された各種データ（例えば、レシートデータ等）を情報処理装置１００に提供することもできる。

[0034] なお、リーダライタ３００と情報処理装置１００間の通信方式は、近距離無線通信であることを想定しているが、これに限定されない。例えば、リーダライタ３００と情報処理装置１００間の通信方式は、Ｗｉ－Ｆｉ（Wireless Fidelity）、または、Ｂｌｕｅｔｏｏｔｈ（登録商標）等を含む任意の非接触通信方式であってもよいし、任意の接触通信であってもよい。また、リーダライタ３００と店舗装置間の通信方式も特に限定されない。

[0035] （２．２．セキュアエレメント１２０の機能構成例）

上記では、本実施形態に係る情報処理システムの構成例について説明した。続いて、セキュアエレメント１２０の機能構成例について説明する。

[0036] 図２に示すように、セキュアエレメント１２０は、制御部１２１と、第１の記憶部１２２と、第２の記憶部１２３と、を備える。

[0037] （第１の記憶部１２２）

第１の記憶部１２２は、制御部１２１の制御に基づいてアクセス可能な記憶領域であり、外部装置からの直接のアクセスを排除することで、外部装置によるデータの改ざん等を防ぐことができる記憶領域である。また、第１の記憶部１２２は、制御部１２１の処理に用いられるデータを記憶する記憶領域でもある。より具体的には、第１の記憶部１２２は、制御部１２１の処理に用いられる処理対象データ、プログラムまたは設定ファイル等を記憶する。

[0038] ここで、図３を参照して、第１の記憶部１２２が有するデータ構造について説明する。図３に示すように、第１の記憶部１２２は、所定の階層構造によってデータを管理する。より具体的には、第１の記憶部１２２は、「エリア」、「サービス」または「ユーザブロックデータ」という単位でデータを管理している。「エリア」とは、ディレクトリとも呼ばれ、配下のデータを束ねる概念であり、１階層構造につき複数個存在し得る。エリアは、基本的に、情報処理システム単位で形成されるため、セキュアエレメント１２０が複数の情報処理システムに対応している場合には、エリアは複数個形成され得る。しかし、これに限定されず、１つの情報処理システムで複数のエリアが形成されてもよいし、複数の情報処理システムで１つのエリアが共有されてもよい。

[0039] 「サービス」とは、データに対するアクセス権限または暗号化方式等を管理する概念である。より具体的には、サービス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または暗号化方式等に基づく制御が行われる。例えば、図３におけるサービスＡが暗号化されていないデータが格納されるものであり、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が格納されるものであるとする。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およ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。

[0040] 「ユーザブロックデータ」は、セキュアエレメント１２０の処理に用いられるデータを格納する記憶領域また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。

[0041] なお、第１の記憶部１２２のデータ構造は上記に限定されない。例えば、第１の記憶部１２２のデータ構造は、「エリア」、「サービス」または「ユーザブロックデータ」に相当する別の概念によって実現されてもよい。

[0042] （制御部１２１）

制御部１２１は、セキュアエレメント１２０が行う処理全般を統括的に制御する機能構成である。より具体的には、情報処理装置１００と外部装置との近距離無線通信により、外部装置からの要求情報がＣＬＦ１３０によって受信された場合、制御部１２１は、当該要求情報に基づく処理を行う。例えば、制御部１２１は、当該要求情報に基づいて、第１の記憶部１２２に記憶されているデータ（例えば、ユーザブロックデータ内のデータ、または、ユーザブロックデータ自体）の読み取り、または、更新等を行う。なお、制御部１２１が制御する処理は上記に限定されず、例えば、制御部１２１は、サーバ２００またはデバイスホスト１１０との通信に伴って任意の処理を制御してもよい。

[0043] そして、制御部１２１は、上記の処理が終了した後に、処理に関するデータを第２の記憶部１２３へ格納する。より具体的には、制御部１２１は、処理後の第１の記憶部１２２に記憶されている処理対象データを第２の記憶部１２３へ格納する。

[0044] ここで、図４を参照して、制御部１２１が第２の記憶部１２３に格納するデータの一例について説明する。制御部１２１は、図４に示すように、処理対象データおよび第１の記憶部１２２における処理対象データのパスを第２

の記憶部１２３に格納する。さらに、制御部１２１は、処理対象データのハッシュ値を算出し、当該ハッシュ値も併せて第２の記憶部１２３に格納する。

[0045] これによって、デバイスホスト１１０は、第２の記憶部１２３からこれらのデータを取得することで、処理の内容を適切に知ることができる。例えば、デバイスホスト１１０がこれらのデータを取得する前に、第１の記憶部１２２内のデータの更新処理が複数回行われたとしても、全処理対象データが上書きされることなく第２の記憶部１２３に格納されているため、デバイスホスト１１０は、第２の記憶部１２３からこれらのデータを取得し、全ての処理の内容を適切に知ることができる（換言すると、本開示の技術は、データの更新処理が頻繁に発生する場合に特に有効である）。また、デバイスホスト１１０は、取得した処理対象データを用いてハッシュ値を算出し、当該ハッシュ値と第２の記憶部１２３から取得したハッシュ値との一致を確認することによって、処理対象データの完全性を検証することができる。例えば、セキュアエレメント１２０内の第２の記憶部１２３から取得されたデータの完全性をサーバ２００において検証する例として、ＭＡＣ（Message Authentication Code）または電子署名による検証等が考えられる。

[0046] なお、制御部１２１が第２の記憶部１２３に格納するデータは上記に限定されない。より具体的には、制御部１２１は、図４に示したデータの一部を適宜省略してもよい。例えば、制御部１２１は、パスまたはハッシュ値等を省略してもよい。また、制御部１２１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、制御部１２１は、処理対象データの属性（例えば、内容、種別または重要度等）に関するデータを追加してもよい。また、制御部１２１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、制御部１２１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、制御部１２１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、デバイスホスト１１０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。

[0047] また、制御部１２１は、処理が終了した後に必ず、処理に関するデータを第２の記憶部１２３へ格納するとは限らず、処理に関するデータを第２の記憶部１２３へ格納するか否かを制御することができる。

[0048] 例えば、制御部１２１は、処理の内容に基づいて、処理に関するデータを第２の記憶部１２３へ格納するか否かを制御することができる。より具体的には、処理の内容が、第１の記憶部１２２に記憶されているデータの更新を含む場合、制御部１２１は、上記のように、当該処理に関するデータを第２の記憶部１２３に格納してもよい。一方、例えば、処理の内容が、第１の記憶部１２２に記憶されているデータの読み取りだけである場合、制御部１２１は、当該処理に関するデータを第２の記憶部１２３に格納しなくてもよい。換言すると、処理の内容がデータの読み取りだけである場合には、データが変更されないため、デバイスホスト１１０は当該処理対象データを把握しなくてもよい場合（または、既に把握済である場合）があるため、制御部１２１は、当該処理に関するデータを第２の記憶部１２３に格納しなくてもよい。

[0049] また、制御部１２１は、処理対象データが記憶されている記憶領域に基づいて、処理に関するデータを第２の記憶部１２３へ格納するか否かを制御してもよい。より具体的には、処理対象データが、図３に示したデータ構造において暗号化されたデータ用のサービス配下に格納されている場合、制御部１２１は、当該処理対象データの重要度が相対的に高いと判断して、処理に関するデータを第２の記憶部１２３に格納しなくてもよい。換言すると、制御部１２１は、処理対象データの暗号化の有無（または、重要度を示す何らかの指標値）に基づいて、処理に関するデータを第２の記憶部１２３へ格納するか否かを制御してもよい。

[0050] 上記の制御によって、制御部１２１は、第２の記憶部１２３に格納されるデータ量の無駄を削減することができる。なお、処理に関するデータを第２

の記憶部１２３へ格納するか否かの制御方法は上記に限定されない。また、上記では、制御部１２１が、第１の記憶部１２２のデータを用いて処理を行った後に、当該処理に関するデータを第２の記憶部１２３に格納する旨について説明したが、制御部１２１が当該処理に関するデータを第２の記憶部１２３に格納するタイミングはこれに限定されない。例えば、制御部１２１は、処理の途中に、当該処理に関するデータを第２の記憶部１２３に格納してもよい。また、制御部１２１は、処理に関するデータを、セキュアエレメント１２０外の記憶部に格納してもよい。例えば、制御部１２１は、処理に関するデータを、デバイスホスト１１０の記憶部１１３に格納してもよい。これによって、デバイスホスト１１０が第２の記憶部１２３から処理に関するデータを取得する処理が省略可能となる。

[0051] 加えて、制御部１２１は、第１の記憶部１２２のデータを用いて処理を行った場合には、処理が終了したタイミングでデバイスホスト１１０に対して処理終了の通知を行う。これによって、デバイスホスト１１０は、処理が終了したタイミングを認識することができる。なお、処理が終了したタイミングとは、リーダライタ３００からの搬送波が受信されなくなったタイミングを指してもよいし、制御部１２１によって一連の処理が全て終了したと認識されたタイミングを指してもよい。ここで、制御部１２１による処理時間は短い（例えば、１秒未満～数秒程度）ため、処理が終了したタイミングとは、「処理が行われたタイミング」と解釈されてもよい。換言すると、当該通知によって、デバイスホスト１１０は、処理が行われたタイミングを認識することができる。デバイスホスト１１０は、処理が行われたタイミングを認識したことをトリガとして、第２の記憶部１２３に格納されている処理に関するデータを取得することができる。詳細については後述する。

[0052] なお、制御部１２１が当該通知を行うタイミングは上記に限定されない。例えば、制御部１２１は、処理が開始されたタイミングでデバイスホスト１１０に対して通知を行ってもよい。なお、処理が開始されたタイミングとは、リーダライタ３００からの搬送波が検出されたタイミングを指してもよい

し、制御部１２１によって一連の処理が開始されたタイミングを指してもよい。上記のとおり、制御部１２１による処理時間は短いため、処理が開始されたタイミングとは、「処理が行われたタイミング」と解釈されてもよい。この場合、デバイスホスト１１０は、通知を受けてから、処理に関するデータが第２の記憶部１２３に格納されたと予測されるタイミングに当該データの取得を試みる。詳細については後述する。

[0053] また、制御部１２１は、処理の実施が予想されるタイミングに、デバイスホスト１１０に対して通知を行ってもよい。例えば、ユーザ認証処理が所定の方法（例えば、指紋認証、虹彩認証もしくは静脈認証等の生体認証またはパスワード認証等）で行われた後には、代金決済処理等を含む任意の処理が行われる可能性がある。したがって、制御部１２１は、デバイスホスト１１０等からユーザ認証処理が成功した旨を通知された場合、デバイスホスト１１０に対して上記の通知を行ってもよい。

[0054] また、制御部１２１は、第１の記憶部１２２のデータを用いた処理を行う場合に必ず、デバイスホスト１１０に対して通知を行うとは限らず、デバイスホスト１１０に対して通知を行うか否かを制御することができる。例えば、制御部１２１は、処理に関するデータを第２の記憶部１２３に格納しない場合、デバイスホスト１１０が取得すべきデータが第２の記憶部１２３に存在しないため、制御部１２１は、デバイスホスト１１０に対して通知を行わなくてもよい。なお、デバイスホスト１１０に対する通知の制御方法はこれに限定されない。

[0055] また、当該通知は、その通知タイミングによって、処理が行われたタイミング（または、処理が終了したタイミング、処理が開始されたタイミング）等を伝えるだけでなく、他のデータを伝えてもよい（換言すると、通知の内容は特に限定されない）。例えば、通知は、処理の内容に関するデータ（例えば、処理の種別または重要度等）を含むことで、これらのデータをデバイスホスト１１０へ伝えてもよい。これによって、デバイスホスト１１０は、通知に含まれるデータに基づいて第２の記憶部１２３からのデータの取得処

理等を制御することができる。

[0056] そして、デバイスホスト１１０が当該通知に基づいて第２の記憶部１２３からのデータの取得を要求した場合、制御部１２１は、当該要求に応じて第２の記憶部１２３からデータを取得し、デバイスホスト１１０へ提供する。このとき、制御部１２１は、デバイスホスト１１０へ提供済のデータを第２の記憶部１２３から削除する。これによって、制御部１２１は、第２の記憶部１２３の空き容量を増やすことができる。なお、制御部１２１が第２の記憶部１２３に記憶されているデータを削除するタイミング（換言すると、第２の記憶部１２３のデータ保持期間）はこれに限定されない。

[0057] なお、制御部１２１の制御内容は上記に限定されない。例えば、制御部１２１は、汎用コンピュータ、ＰＣ、ノート型ＰＣ、タブレット型ＰＣ、任意のウェアラブル端末、携帯型メディア再生機器または携帯型ゲーム機器等を含む任意の情報処理装置において一般的に行われる処理を制御してもよい。

[0058] （第２の記憶部１２３）

第２の記憶部１２３は、図４を参照して説明した、処理に関するデータを記憶する記憶領域である。より具体的には、第２の記憶部１２３は、図４に示すように、処理対象データ、第１の記憶部１２２における処理対象データのパス、および、処理対象データのハッシュ値等を記憶する。なお、第２の記憶部１２３の個数、データ構造等は特に限定されない。

[0059] 以上、セキュアエレメント１２０の機能構成例について説明した。なお、図２を用いて説明した上記の機能構成はあくまで一例であり、セキュアエレメント１２０の機能構成は係る例に限定されない。また、セキュアエレメント１２０の機能構成は、仕様や運用に応じて柔軟に変形可能である。

[0060] （２．３．デバイスホスト１１０の機能構成例）

上記では、セキュアエレメント１２０の機能構成例について説明について説明した。続いて、デバイスホスト１１０の機能構成例について説明する。

[0061] 図２に示すように、デバイスホスト１１０は、制御部１１１と、データ取得部１１２と、記憶部１１３と、入力部１１４と、出力部１１５と、通信部

１１６と、を備える。

[0062] （データ取得部１１２）

データ取得部１１２は、セキュアエレメント１２０の制御部１２１から提供された通知に応じて、第２の記憶部１２３に記憶されている処理に関するデータを取得する機能構成である。より具体的には、データ取得部１１２は、制御部１２１からの通知を受信した場合には、処理に関するデータの要求情報を生成して、当該情報を制御部１２１へ提供する。これによって、制御部１２１は、第２の記憶部１２３に記憶されている処理に関するデータを全て取得してデータ取得部１１２へ提供し、第２の記憶部１２３に記憶されているデータを削除する。なお、これはあくまで一例であり、データ取得部１１２は、第２の記憶部１２３に記憶されている処理に関するデータの一部だけを取得してもよい。例えば、データ取得部１１２は、何らかの方法（例えば、第２の記憶部１２３のインデックス情報、または、通知に含まれる情報等）で第２の記憶部１２３に記憶されているデータの内容を把握し、必要なデータまたはより重要度の高いデータを優先的に取得してもよい。また、データ取得部１１２は、制御部１２１からの通知が無い場合であっても、自発的に第２の記憶部１２３から処理に関するデータを取得することを試みてもよい。

[0063] また、データ取得部１１２は、制御部１２１から提供された通知に応じて、セキュアエレメント１２０による処理のタイミングに関するデータをセキュアエレメント１２０外から取得する。より具体的には、情報処理装置１００が、時刻データを出力可能な機能構成（図示なし）を備えている（または、時刻データを出力可能な装置と通信可能である）ことによって、データ取得部１１２は、通知を受信した場合に、その受信タイミングの時刻データを当該機能構成から取得することができる。上記のとおり、当該通知は、セキュアエレメント１２０によって処理が行われたタイミングで行われるため、データ取得部１１２は、この処理によって、セキュアエレメント１２０による処理のタイミングに関するデータを取得することができる。上記のとおり

、セキュアエレメント１２０は、処理のタイミングに関するデータを取得することができないが、データ取得部１１２が当該処理によって処理のタイミングに関するデータを取得することによって様々な機能が可能となる。詳細については後述する。なお、時刻データを出力可能な機能構成とは、例えば、時計等であり得るがこれに限定されない。また、データ取得部１１２は、通知の受信タイミングの時刻データを取得するのではなく、通知が制御部１２１によって送信されたと予測されるタイミングの時刻データ、または、（通知が処理のタイミングに関するデータを含む場合には）通知に含まれるデータに基づいて時刻データを取得してもよい。

[0064] また、データ取得部１１２は、処理のタイミングに関するデータだけに限らず、セキュアエレメント１２０が取得することができない任意のデータをセキュアエレメント１２０外から取得してもよい。例えば、情報処理装置１００が、自装置の位置に関するデータ、当該位置の周辺状況に関するデータ（例えば、環境音データまたは周辺画像データ等）、自装置の使用者に関するデータ、または、自装置の動作もしくは使用者の動作に関するデータ等を出力可能な機能構成（図示なし）を備えている（または、これらのデータを出力可能な装置と通信可能である）ことによって、データ取得部１１２は、通知を受信した場合に、その受信タイミングにおけるこれらのデータを当該機能構成から取得することができる。

[0065] これによって、データ取得部１１２は、セキュアエレメント１２０によって処理が行われたタイミングにおける、自装置の位置、当該位置の周辺状況、自装置の使用者、または、自装置の動作もしくは使用者の動作等を知ることができる。上記のとおり、セキュアエレメント１２０は、これらのデータを取得することができないが、データ取得部１１２が当該処理によってこれらのデータを取得することによって様々な機能が可能となる。なお、データ取得部１１２によって取得されるデータは上記に限定されない。また、データ取得部１１２は、セキュアエレメント１２０が上記の各データを取得可能か否かについて判断し、セキュアエレメント１２０が上記の各データを取得

できないと判断した場合にのみ各データを取得してもよい。

[0066] ここで、情報処理装置１００の位置に関するデータを出力可能な機能構成とは、例えば、緯度データ、経度データまたは高度データを出力可能なＧＮＳＳ（Global Navigation Satellite System）センサ（ＧＰＳ（Global Positioning System）センサを含む）、または、高度データを出力可能な気圧センサ等であり得るがこれに限定されない。例えば、モーションセンサ（加速度センサまたはジャイロセンサ等を含む）等のセンシングデータに基づいて情報処理装置１００の位置を推定可能な機能構成であってもよい。また、情報処理装置１００の位置の周辺状況に関するデータを出力可能な機能構成とは、例えば、周辺の環境音を取得可能なマイクロホン、または、周辺画像を出力可能なカメラ等であり得るがこれらに限定されない。また、自装置の使用者に関するデータを出力可能な機能構成とは、例えば、所定の方法によるユーザ認証（例えば、指紋認証、虹彩認証もしくは静脈認証等の生体認証またはパスワード認証等）を実施可能な機能構成、または、所定の方法によるユーザ推定（例えば、脈拍データ等を含む生体データに基づくユーザ推定）を実施可能な機能構成であり得るがこれに限定されない。また、自装置の動作もしくは使用者の動作に関するデータを出力可能な機能構成とは、例えば、モーションセンサ（加速度センサまたはジャイロセンサ等を含む）等であり得るがこれに限定されない。

[0067] データ取得部１１２は、セキュアエレメント１２０から取得した処理に関するデータ、および、セキュアエレメント１２０外から取得した処理のタイミング等に関するデータを制御部１１１に提供する。

[0068] （制御部１１１）

制御部１１１は、セキュアエレメント１２０から取得された処理に関するデータと、セキュアエレメント１２０外から取得された処理のタイミング等に関するデータとを対応付けることで、これらのデータを様々な処理に用いる。

[0069] より具体的に説明すると、セキュアエレメント１２０から取得された処理

に関するデータには、図４に示したように、処理対象データのハッシュ値が含まれる。したがって、制御部１１１は、まず、取得された処理対象データを用いてハッシュ値を算出し、当該ハッシュ値と第２の記憶部１２３から取得されたハッシュ値との一致を確認することによって、処理対象データの完全性を検証する。仮に、処理対象データを用いて算出されたハッシュ値が第２の記憶部１２３から取得されたハッシュ値と一致しない場合には、制御部１１１は、処理対象データが改ざんされている可能性があると判断して後段の処理を中止してもよい。

[0070] 制御部１１１は、処理対象データの完全性の検証に成功した場合、セキュアエレメント１２０から取得された処理に関するデータと、セキュアエレメント１２０外から取得された処理のタイミング等に関するデータとを対応付けて記憶部１１３に格納する。ここで、図５を参照して、記憶部１１３に格納されるデータの一例について説明する。図５において、データ１０が、セキュアエレメント１２０から取得された処理に関するデータであり、制御部１１１は、当該データ１０に対して、セキュアエレメント１２０外から取得された処理のタイミング等に関するデータ２０を対応付けて記憶部１１３に格納する。

[0071] そして、制御部１１１は、例えば、所定の方法で出力部１１５に処理対象データを出力させる。より具体的には、セキュアエレメント１２０によって行われた処理が代金決済処理である場合、制御部１１１は、処理対象データに含まれる代金決済金額もしくは残高に関するデータを出力部１１５に出力させてもよい。また、セキュアエレメント１２０によって行われた処理がクーポンの使用処理もしくは取得処理である場合、制御部１１１は、処理対象データに含まれるクーポンに関するデータを出力部１１５に出力させてもよい。また、セキュアエレメント１２０によって行われた処理が電子マネーのチャージ処理である場合、制御部１１１は、処理対象データに含まれるチャージ額に関するデータを出力部１１５に出力させてもよい。また、セキュアエレメント１２０によって行われた処理がキャンペーンデータの取得処理で

ある場合、制御部１１１は、処理対象データに含まれるキャンペーンデータを出力部１１５に出力させてもよい。

[0072] これらの処理によって、ユーザは、例えば、情報処理装置１００をリーダライタ３００にかざすことによって情報処理装置１００に各種処理を行わせた後に、出力部１１５からの出力によって当該処理の結果等を確認することができる。なお、制御部１１１による制御は上記に限定されない。例えば、制御部１１１は、処理対象データの完全性の検証に失敗した場合であっても、後段の処理を中止することなく、出力部１１５による出力等を制御してもよい。

[0073] また、制御部１１１は、処理対象データだけでなく、セキュアエレメント１２０外から取得された処理のタイミング等に関するデータも用いて上記の処理を行ってもよい。より具体的には、制御部１１１は、出力部１１５に出力を行わせる際に、併せて、処理のタイミングに関するデータ、自装置の位置に関するデータ、当該位置の周辺状況に関するデータ、自装置の使用者に関するデータ、または、自装置の動作もしくは使用者の動作に関するデータ等を出力させたり、これらのデータを用いた所定の処理結果を出力させたりしてもよい。例えば、制御部１１１は、処理対象データに含まれる代金決済金額もしくは残高に関するデータだけでなく、セキュアエレメント１２０外から取得された代金決済処理が行われたタイミング（例えば、日時）または位置（例えば、店舗）等を併せて出力部１１５に出力させてもよい。

[0074] これらの処理によって、ユーザは、より豊富な情報を知ることができる。また、制御部１１１は、上記以外の、セキュアエレメント１２０外から取得された任意のデータを併せて出力部１１５に出力させてもよい。

[0075] また、制御部１１１は、セキュアエレメント１２０から取得された処理に関するデータと、セキュアエレメント１２０外から取得された処理のタイミング等に関するデータとを対応付けたデータをサーバ２００へ提供してもよい。これによって、サーバ２００は、これらのデータを蓄積し統計分析すること等によって、情報処理装置１００の使用者の行動履歴データや嗜好デー

タ等を出力し、これらのデータに基づいて各種サービスを提供することができる。

[0076] また、制御部１１１は、汎用コンピュータ、ＰＣ、ノート型ＰＣ、タブレット型ＰＣ、任意のウェアラブル端末、携帯型メディア再生機器または携帯型ゲーム機器等を含む任意の情報処理装置において一般的に行われる処理を制御してもよい。

[0077] （記憶部１１３）

記憶部１１３は、各種データを記憶する機能構成である。例えば、記憶部１１３は、図５を参照して説明したように、セキュアエレメント１２０から取得された処理に関するデータと、セキュアエレメント１２０外から取得された処理のタイミング等に関するデータとが対応付けられたデータ等を記憶する。また、記憶部１１３は、デバイスホスト１１０の各機能構成によって使用されるプログラムまたはパラメータ等を記憶する。なお、記憶部１１３が記憶するデータの内容はこれらに限定されない。

[0078] （入力部１１４）

入力部１１４は、ユーザによる入力を受ける機能構成である。例えば、入力部１１４は、ユーザが各種入力手段（図示なし。例えば、マウス、キーボード、タッチパネル、ボタン、スイッチまたはマイクロホン等）を用いて行った入力を受ける。入力部１１４は、入力された内容を制御部１１１に提供することで、制御部１１１による各種処理を実現する。なお、入力手段は上記に限定されない。

[0079] （出力部１１５）

出力部１１５は、各種データを出力する機能構成である。例えば、出力部１１５は、各種出力手段（図示なし。例えば、ディスプレイ等の表示手段またはスピーカ等の音声出力手段）に各種データを出力させることができる。より具体的には、上記のとおり、出力部１１５は、制御部１１１の制御に基づいて、処理対象データまたはセキュアエレメント１２０外から取得された処理のタイミング等に関するデータ等を出力する（ディスプレイ表示または

音声出力等）。なお、出力手段は上記に限定されない。

[0080] （通信部１１６）

通信部１１６は、サーバ２００を含む外部装置との各種通信を行う機能構成である。例えば、通信部１１６は、セキュアエレメント１２０から取得された処理に関するデータと、セキュアエレメント１２０外から取得された処理のタイミング等に関するデータとが対応付けられたデータを含む無線信号をサーバ２００へ送信してもよい。また、通信部１１６は、デバイスホスト１１０またはセキュアエレメント１２０による処理に用いられる任意のデータを含む無線信号をサーバ２００から受信してもよい。なお、通信部１１６が通信するデータおよび通信するケースはこれらに限定されない。また、上記のとおり、通信部１１６とサーバ２００間の通信方式は特に限定されない。

[0081] 以上、デバイスホスト１１０の機能構成例について説明した。なお、図２を用いて説明した上記の機能構成はあくまで一例であり、デバイスホスト１１０の機能構成は係る例に限定されない。例えば、デバイスホスト１１０は、図２に示す構成の全てを必ずしも備えなくてもよい。また、デバイスホスト１１０の機能構成は、仕様や運用に応じて柔軟に変形可能である。

[0082] （２．４．処理フローの例）

上記では、デバイスホスト１１０の機能構成例について説明した。続いて、情報処理システムにおける処理フローの例について説明する。

[0083] まず、図６を参照して、情報処理装置１００とリーダライタ３００との近距離無線通信に伴って行われる処理フローの例について説明する。

[0084] まず、ユーザが情報処理装置１００をリーダライタ３００にかざすことで、情報処理装置１００がリーダライタ３００の発する搬送波を受信可能な範囲に入る。そして、ステップＳ１０００では、リーダライタ３００が、セキュアエレメント１２０の第１の記憶部１２２に記憶されているデータの更新要求情報を含む無線信号を送信する。ステップＳ１００４では、ＣＬＦ１３０が、リーダライタ３００からの無線信号を受信し、当該無線信号に含まれ

る更新要求情報をセキュアエレメント１２０に提供する。そして、セキュアエレメント１２０の制御部１２１は、当該更新要求情報に基づいて第１の記憶部１２２に記憶されているデータを更新する。そして、制御部１２１は、ステップＳ１００８にて、第１の記憶部１２２から更新完了の通知を受信したことに基づいて、ステップＳ１０１２にて、処理に関するデータを第２の記憶部１２３に格納する。ステップＳ１０１６では、制御部１２１が、第２の記憶部１２３から格納完了の通知を受信する。

[0085] ステップＳ１０２０では、リーダライタ３００が搬送波の発信を停止する（または、情報処理装置１００がリーダライタ３００の発する搬送波を受信可能な範囲から外れる）。これによって、ステップＳ１０２４では、セキュアエレメント１２０の制御部１２１が処理の終了を認識して、デバイスホスト１１０に対して処理終了の通知を行う。

[0086] ステップＳ１０２８では、デバイスホスト１１０のデータ取得部１１２が、処理終了の通知に基づいてセキュアエレメント１２０が取得することができない各種データ（例えば、処理のタイミングに関するデータ等）の取得を、時計または各種センサ等に対して要求する。ステップＳ１０３２では、時計または各種センサ等が、当該要求に応じて各種データを取得し、データ取得部１１２へ提供する。

[0087] ステップＳ１０３６では、データ取得部１１２が、処理に関するデータの要求情報を生成して、当該情報をセキュアエレメント１２０へ提供する。ステップＳ１０４０およびステップＳ１０４４では、セキュアエレメント１２０の制御部１２１が、当該情報に基づいて第２の記憶部１２３に記憶されている処理に関するデータを全て取得する。ステップＳ１０４８では、制御部１２１が、処理に関するデータをデバイスホスト１１０へ提供する。

[0088] ステップＳ１０５２では、デバイスホスト１１０の制御部１１１が、処理に関するデータに含まれる処理対象データの完全性を検証する。より具体的には、制御部１１１が、処理対象データを用いてハッシュ値を算出し、当該ハッシュ値と処理に関するデータに含まれるハッシュ値との一致を確認する

ことによって、処理対象データの完全性を検証する。制御部１１１は、処理対象データの完全性の検証に成功した場合、ステップＳ１０５６にて、セキュアエレメント１２０から取得された処理に関するデータと、セキュアエレメント１２０外から取得された各種データとを対応付け、記憶部１１３に格納する。ステップＳ１０６０では、制御部１１１が、記憶部１１３から格納完了の通知を受信することで、一連の処理が終了する。なお、図示していないが、制御部１１１は、互いに対応付けられた処理に関するデータ、または、セキュアエレメント１２０外から取得された各種データを用いて上記で説明した各種処理を行ってもよい。

[0089] これによって、情報処理装置１００は、有用なデータをユーザに提供することができる。より具体的には、情報処理装置１００は、処理対象データだけでなく、セキュアエレメント１２０が取得することができない、処理のタイミングに関するデータ等を併せてユーザに提供することができる。

[0090] 続いて、図７を参照して、情報処理装置１００とサーバ２００との通信に伴って行われる処理フローの例について説明する。

[0091] ステップＳ１１００では、サーバ２００が、セキュアエレメント１２０の第１の記憶部１２２に記憶されているデータの更新要求情報を含む無線信号をデバイスホスト１１０に対して送信する。例えば、サーバ２００は、電子マネーのチャージに関する要求情報を含む無線信号をデバイスホスト１１０に対して送信する。

[0092] ステップＳ１１０４では、デバイスホスト１１０の制御部１１１が、受信された無線信号に含まれる、データの更新要求情報をセキュアエレメント１２０に対して提供する。ステップＳ１１０８では、セキュアエレメント１２０の制御部１２１が、当該更新要求情報に基づいて第１の記憶部１２２に記憶されているデータを更新することで、電子マネーのチャージ等を実現する。そして、制御部１２１は、ステップＳ１１１２にて、第１の記憶部１２２から更新完了の通知を受信したことに基づいて、ステップＳ１１１６にて、処理に関するデータを第２の記憶部１２３に格納する。ステップＳ１１２０

では、制御部１２１が、第２の記憶部１２３から格納完了の通知を受信する。

[0093] ステップＳ１１２４では、制御部１２１が処理の終了を認識して、デバイスホスト１１０に対して処理終了の通知を行う。以降に行われるステップＳ１１２８～ステップＳ１１６０の処理は、図６のステップＳ１０２８～ステップＳ１０６０の処理と同一であるため説明を省略する。

[0094] なお、図６および図７に示したシーケンス図における各ステップは、必ずしも記載された順序に沿って時系列に処理する必要はない。すなわち、シーケンス図における各ステップは、記載された順序と異なる順序で処理されても、並列的に処理されてもよい。

[0095] （２．５．情報処理装置１００のハードウェア構成例）

上記では、情報処理システムにおける処理フローの例について説明した。続いて、図８を参照して、情報処理装置１００のハードウェア構成例について説明する。上記で説明してきた各種処理は、ソフトウェアと、以下に説明するハードウェアとの協働により実現される。

[0096] 図８は、情報処理装置１００のハードウェア構成例を示すブロック図である。情報処理装置１００は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）９０１と、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）９０２と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）９０３と、ホストバス９０４と、ブリッジ９０５と、外部バス９０６と、インタフェース９０７と、入力装置９０８と、出力装置９０９と、ストレージ装置（ＨＤＤ）９１０と、ドライブ９１１と、通信装置９１２とを備える。

[0097] ＣＰＵ９０１は、演算処理装置およ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。また、ＣＰＵ９０１は、マイクロプロセッサであってもよい。ＲＯＭ９０２は、ＣＰＵ９０１が使用するプログラムや演算パラメータ等を記憶する。ＲＡＭ９０３は、ＣＰＵ９０１の実行において使用するプログラムや、その実行において適宜変化するパラメータ等を一時記憶する。これらはＣＰＵバスなどから構成され

るホストバス９０４により相互に接続されている。当該ＣＰＵ９０１、ＲＯＭ９０２およびＲＡＭ９０３の協働により、デバイスホスト１１０の制御部１１１もしくはデータ取得部１１２、または、セキュアエレメント１２０の制御部１２１の機能が実現される。

[0098] ホストバス９０４は、ブリッジ９０５を介して、ＰＣＩ（Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ／Ｉｎｔｅｒｆａｃｅ）バスなどの外部バス９０６に接続されている。なお、必ずしもホストバス９０４、ブリッジ９０５および外部バス９０６を分離構成する必要はなく、１つのバスにこれらの機能を実装してもよい。

[0099] 入力装置９０８は、マウス、キーボード、タッチパネル、ボタン、マイクロホン、スイッチおよびレバー等を備え、ユーザが各種データを入力するために用いられる。入力装置９０８は、ユーザからの入力に基づいて入力信号を生成し、ＣＰＵ９０１に出力する入力制御回路などから構成されている。デバイスホスト１１０の入力部１１４には、入力装置９０８によって生成された入力信号が入力されることになる。

[0100] 出力装置９０９は、例えば、ＣＲＴ（Ｃａｔｈｏｄｅ Ｒａｙ Ｔｕｂｅ）ディスプレイ装置、液晶ディスプレイ（ＬＣＤ）装置、ＯＬＥＤ（Ｏｒｇａｎｉｃ Ｌｉｇｈｔ Ｅｍｉｔｔｉｎｇ Ｄｉｏｄｅ）装置およびランプなどの表示装置を含む。さらに、出力装置９０９は、スピーカおよびヘッドホンなどの音声出力装置を含む。出力装置９０９は、映像データ等の各種データをイメージまたはテキストで表示する。一方、音声出力装置は、音声データ等を音声に変換して出力する。当該出力装置９０９により、デバイスホスト１１０の出力部１１５の機能が実現される。

[0101] ストレージ装置９１０は、デバイスホスト１１０の記憶部１１３またはセキュアエレメント１２０の第１の記憶部１２２もしくは第２の記憶部１２３の一例として構成されたデータ格納用の装置である。ストレージ装置９１０は、記憶媒体、記憶媒体にデータを記録する記録装置、記憶媒体からデータを読み出す読出し装置および記憶媒体に記録されたデータを削除する削除装

置などを含んでもよい。ストレージ装置９１０は、例えば、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）で構成される。このストレージ装置９１０は、ハードディスクを駆動し、ＣＰＵ９０１が実行するプログラムや各種データを格納する。

[0102] ドライブ９１１は、記憶媒体用リーダライタであり、情報処理装置１００に内蔵、あるいは外付けされる。ドライブ９１１は、装着されている磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリ等のリムーバブル記憶媒体９１３に記録されている情報を読み出して、ＲＡＭ９０３に出力する。また、ドライブ９１１は、リムーバブル記憶媒体９１３に情報を書き込むこともできる。

[0103] 通信装置９１２は、例えば、通信網９１４に接続するための通信デバイス等で構成された通信インタフェースである。当該通信装置９１２により、デバイスホスト１１０の通信部１１６またはＣＬＦ１３０の機能が実現される。

[0104] なお、情報処理装置１００のハードウェア構成は、図８に示す構成に限られない。例えば、情報処理装置１００は、接続されている外部の通信デバイスを介して通信を行う場合には、通信装置９１２を備えていなくてもよい。また、通信装置９１２は、複数の通信方式によって通信を行うことが可能な構成であってもよい。

[0105] ＜３．まとめ＞

以上で説明してきたように、本開示に係る、セキュアエレメント１２０は、第１の記憶部１２２のデータを用いて処理を行った場合に、処理に関するデータを第２の記憶部１２３へ格納し、所定の通知をデバイスホスト１１０に対して提供する。そして、デバイスホスト１１０は、当該通知に基づいて第２の記憶部１２３から処理に関するデータを取得することで、処理の内容を適切に知ることができる。

[0106] また、デバイスホスト１１０は、当該通知に基づいて、セキュアエレメント１２０が取得することができない、処理のタイミングに関するデータ等を

含む任意のデータをセキュアエレメント１２０外から取得する。これによって、デバイスホスト１１０は、セキュアエレメント１２０から取得した処理に関するデータ、および、セキュアエレメント１２０外から取得した処理のタイミングに関するデータ等を用いて様々な処理を行うことができる。

[0107] 以上、添付図面を参照しながら本開示の好適な実施形態について詳細に説明したが、本開示の技術的範囲はかかる例に限定されない。本開示の技術分野における通常の知識を有する者であれば、請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本開示の技術的範囲に属するものと了解される。

[0108] また、本明細書に記載された効果は、あくまで説明的または例示的なものであって限定的ではない。つまり、本開示に係る技術は、上記の効果とともに、または上記の効果に代えて、本明細書の記載から当業者には明らかな他の効果を奏しうる。

[0109] なお、以下のような構成も本開示の技術的範囲に属する。

（１）

保護記憶部からの通知に基づいて、前記保護記憶部による処理のタイミングに関するデータを取得するデータ取得部と、

前記処理のタイミングに関するデータと前記処理に関するデータとを対応付ける制御部と、を備える、

情報処理装置。

（２）

前記データ取得部は、前記処理のタイミングに関するデータを前記保護記憶部外から取得する、

前記（１）に記載の情報処理装置。

（３）

前記データ取得部は、前記処理のタイミングにおける前記保護記憶部の位置に関するデータ、前記位置の周辺状況に関するデータ、前記保護記憶部の

使用者に関するデータ、または、前記保護記憶部の動作もしくは前記使用者の動作に関するデータも併せて前記保護記憶部外から取得する、

前記（２）に記載の情報処理装置。

（４）

前記データ取得部は、前記処理に関するデータを前記保護記憶部から取得する、

前記（１）から（３）のいずれか１項に記載の情報処理装置。

（５）

前記保護記憶部は、前記処理の対象データを記憶する第１の記憶部と、前記処理に関するデータを記憶する第２の記憶部と、を備え、

前記データ取得部は、前記処理に関するデータを前記第２の記憶部から取得する、

前記（４）に記載の情報処理装置。

（６）

前記保護記憶部は、前記処理後の前記第１の記憶部に記憶されている前記処理の対象データを、前記処理に関するデータとして前記第２の記憶部へ格納する、

前記（５）に記載の情報処理装置。

（７）

前記保護記憶部は、前記処理の内容に基づいて、前記第２の記憶部への前記処理に関するデータの格納を制御する、

前記（６）に記載の情報処理装置。

（８）

前記処理の内容が、データの更新を含む場合、

前記保護記憶部は、前記第２の記憶部へ前記処理に関するデータを格納する、

前記（７）に記載の情報処理装置。

（９）

前記処理の内容が、データの読み取りだけである場合、

前記保護記憶部は、前記第２の記憶部へ前記処理に関するデータを格納しない、

前記（７）に記載の情報処理装置。

（１０）

前記保護記憶部は、前記処理の対象データが記憶されている記憶領域、または、前記処理の対象データの暗号化の有無に基づいて、前記第２の記憶部への前記処理に関するデータの格納を制御する、

前記（６）に記載の情報処理装置。

（１１）

前記処理の対象データが前記第１の記憶部において暗号化されたデータ用の記憶領域に記憶されている場合、または、前記処理の対象データが暗号化されている場合、

前記保護記憶部は、前記第２の記憶部へ前記処理に関するデータを格納しない、

前記（１０）に記載の情報処理装置。

（１２）

前記保護記憶部は、前記処理の対象データのハッシュ値を算出し、前記処理の対象データと前記ハッシュ値を前記処理に関するデータとして前記第２の記憶部に格納する、

前記（６）から（１１）のいずれか１項に記載の情報処理装置。

（１３）

前記保護記憶部は、外部装置との近距離無線通信に伴って前記処理を行う、

前記（１）から（１２）のいずれか１項に記載の情報処理装置。

（１４）

前記通知は、前記処理が終了したタイミング、前記処理が開始されたタイミング、または、前記処理の実施が予想されるタイミングに行われる、

前記（１）から（１３）のいずれか１項に記載の情報処理装置。

（１５）

前記保護記憶部は、セキュアエレメントを含み、

前記情報処理装置は、デバイスホストを含む、

前記（１）から（１４）のいずれか１項に記載の情報処理装置。

（１６）

保護記憶部からの通知に基づいて、前記保護記憶部による処理のタイミングに関するデータを取得することと、

前記処理のタイミングに関するデータと前記処理に関するデータとを対応付けることと、を有する、

コンピュータにより実行される情報処理方法。

符号の説明

[0110]

１００	情報処理装置
１１０	デバイスホスト
１１１	制御部
１１２	データ取得部
１１３	記憶部
１１４	入力部
１１５	出力部
１１６	通信部
１２０	セキュアエレメント
１２１	制御部
１２２	第１の記憶部
１２３	第２の記憶部
１３０	ＣＬＦ
２００	サーバ
３００	リーダライタ