(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-275839
(P2005-275839A)
(43)公開日　平成17年10月6日(2005.10.6)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 1/00	G06F 9/06	660G	5B017
G06F 12/14	G06F 12/14	530B	5B035
G06K 17/00	G06K 17/00	E	5B058
G06K 19/073	G06F 9/06	660J	5B076
	G06K 19/00	P	

審査請求 未請求　請求項の数 50　ＯＬ　（全 36 頁）

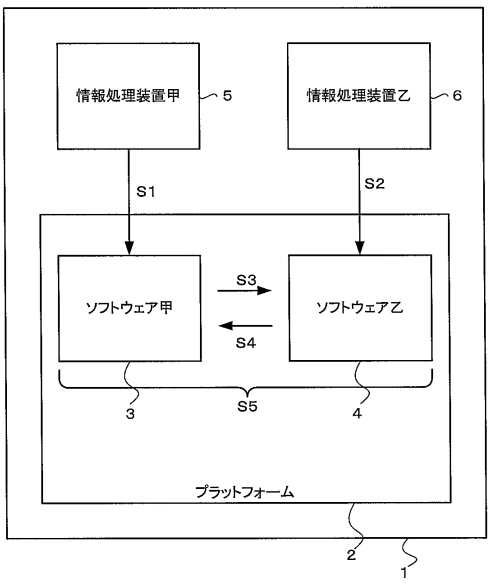
(21)出願番号　特願2004-88452(P2004-88452)
(22)出願日　平成16年3月25日(2004.3.25)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100077838
弁理士　池田　憲保
(74)代理人　100082924
弁理士　福田　修一
(74)代理人　100129023
弁理士　佐々木　敬
(72)発明者　樋口　直志
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B017 AA08 BB09 CA15
5B035 AA06 BB09 CA11
5B058 CA25 KA08 KA31
5B076 FA13 FB02

(54)【発明の名称】ソフトウェア利用許可方法及びシステム

(57)【要約】
【課題】プラットフォームの信頼性に影響されることなく、或いは、プラットフォームの信頼性を確認した上で、複数のソフトウェアを組み合わせて利用する際の組み合わせ相手となるソフトウェア毎に、ソフトウェアの利用の可否を制限することができる技術を提供すること。
【解決手段】　ソフトウェア本体甲を提供する際、ソフトウェア本体甲と組み合わせる予定のソフトウェア本体乙が、組み合わせ相手として認められるか否かを判定するためのコンピュータプログラムを用意して、ソフトウェア本体甲と共に提供する。組み合わせての利用に先立って、判定プログラム甲をプラットフォームが実行し、判定結果が認める旨である場合に限り許可する。
【選択図】図１



【特許請求の範囲】
【請求項１】
デジタル電子情報としての複数のソフトウェア、即ち、コンピュータプログラム及びデジタルデータのいずれかを複数組み合わせて、コンピュータを含んでなるプラットフォーム上で利用することを許否する方法において、
デジタル電子情報であるソフトウェア本体甲を提供する際に、ソフトウェア本体甲と組み合わせて利用しようとしているソフトウェアであって、デジタル電子情報である他のソフトウェア本体乙が、組み合わせ相手として認められるか否かを判定するためのコンピュータプログラムである判定プログラム甲を用意して、ソフトウェア本体甲と共にソフトウェア甲としてコンピュータ甲を介して提供し、
ソフトウェア本体甲をソフトウェア乙と組み合わせて前記プラットフォーム上で利用するのに先立って、判定プログラム甲を前記プラットフォームが実行し、
判定プログラム甲による判定結果が認める旨である場合に限り、ソフトウェア本体甲と組み合わせて利用するソフトウェアとして、ソフトウェア本体乙を許可する処理を前記プラットフォームが実行する
ことを特徴とするソフトウェア利用許可方法。
【請求項２】
請求項１に記載のソフトウェア利用許可方法において、
ソフトウェア本体乙は、前記判定プログラムである判定プログラム乙と共にソフトウェア乙としてコンピュータ乙を介して提供され、
判定プログラム甲及び乙による判定結果の両方が認める旨である場合に限り、ソフトウェア本体甲及び乙を組み合わせて利用することを許可する処理を、当該コンピュータが実行する
ことを特徴とするソフトウェア利用許可方法。
【請求項３】
請求項１に記載のソフトウェア利用許可方法において、
ソフトウェア本体甲の提供を要求するメッセージ甲にデジタル署名Ｓを施したものが前記プラットフォームにて生成されてコンピュータ甲に通知されると共に、ソフトウェア本体乙の提供を要求するメッセージ乙にデジタル署名Ｓを施したものが前記プラットフォームにて生成されてコンピュータ乙に通知される段階１と、
コンピュータ甲がデジタル署名Ｓに基づいて前記プラットフォームの認証に成功した場合に限り、コンピュータ甲にてデジタル署名甲を施されたソフトウェア甲が、前記プラットフォームに提供される段階２と、
コンピュータ乙がデジタル署名Ｓに基づいて前記プラットフォームの認証に成功した場合に限り、コンピュータ乙にてデジタル署名乙を施されたソフトウェア乙が、前記プラットフォームに提供される段階３と、
提供されたソフトウェア甲及び乙のそれぞれに施されたデジタル署名甲及び乙に基づいて、前記プラットフォームがコンピュータ甲及び乙を認証する段階４と、
段階４でのコンピュータ甲及び乙の認証が両方とも成功した場合に限り、前記プラットフォームが判定プログラム甲及び乙を実行する段階５と、
段階５での判定プログラム甲及び乙の実行結果が両方とも認める旨である場合に限り、ソフトウェア本体甲及び乙を組み合わせて利用することを許可する段階６と
を含むことを特徴とするソフトウェア利用許可方法。
【請求項４】
請求項１に記載のソフトウェア利用許可方法において、判定プログラム甲に従って、前記プラットフォームは、データ通信ネットワークを介して他のコンピュータとデータ通信を行い、当該他のコンピュータによる判定に従って判定を行うことを特徴とするソフトウェア利用許可方法。
【請求項５】
請求項４に記載のソフトウェア利用許可方法において、前記他のコンピュータはコンピ

ュータ甲であることを特徴とするソフトウェア利用許可方法。
【請求項６】
請求項２に記載のソフトウェア利用許可方法において、
判定プログラム甲に従って、前記プラットフォームは、ソフトウェア乙の少なくとも一部を、データ通信ネットワークを介して予め定められた他のコンピュータＡに送信し、
コンピュータＡは、送信されたソフトウェア乙の一部乃至全部に基づいて、ソフトウェア甲に対してソフトウェア乙を組み合わせることの可否を判定して、その判定結果甲を、データ通信ネットワークを介して前記プラットフォームに送信し、
判定プログラム甲に従って、前記プラットフォームは、受信した判定結果甲に従って判定し、
判定プログラム乙に従って、前記プラットフォームは、ソフトウェア甲の少なくとも一部を、データ通信ネットワークを介して予め定められた他のコンピュータＢに送信し、
コンピュータＢは、送信されたソフトウェア乙の一部乃至全部に基づいて、ソフトウェア甲に対してソフトウェア乙を組み合わせることの可否を判定して、その判定結果乙を、データ通信ネットワークを介して前記プラットフォームに送信し、
判定プログラム乙に従って、前記プラットフォームは、受信した判定結果乙に従って判定する
ことを特徴とするソフトウェア利用許可方法。
【請求項７】
請求項６に記載のソフトウェア利用許可方法において、コンピュータＡはコンピュータ甲であること、及び、コンピュータＢはコンピュータ乙であることのうち、少なくとも一方が成り立つことを特徴とするソフトウェア利用許可方法。
【請求項８】
請求項１に記載のソフトウェア利用許可方法において、判定プログラム甲は、予めソフトウェア乙に添付されたデジタル署名による認証の結果に基づいて、ソフトウェア本体甲と組み合わせて利用するソフトウェアとして、ソフトウェア乙を許可することを特徴とするソフトウェア利用許可方法。
【請求項９】
請求項１に記載のソフトウェア利用許可方法において、
コンピュータ甲は、前記プラットフォームにて生成された公開暗号方式の暗号鍵を用いて暗号化したソフトウェアを提供し、
ソフトウェアの提供を受けた前記プラットフォームは、前記暗号鍵と対になって生成した復号鍵を用いてソフトウェアを復号する処理を実行する
ことを特徴とするソフトウェア利用許可方法。
【請求項１０】
請求項１に記載のソフトウェア利用許可方法において、
コンピュータ甲は、前記プラットフォームにて生成されたメッセージに応じてソフトウェア甲を提供し、
メッセージは前記プラットフォームの所在を示すアドレス情報を含む
ことを特徴とするソフトウェア利用許可方法。
【請求項１１】
請求項１０に記載のソフトウェア利用許可方法において、アドレス情報は前記プラットフォームのデータ通信ネットワーク上でのアドレス情報であることを特徴とするソフトウェア利用許可方法。
【請求項１２】
請求項１０に記載のソフトウェア利用許可方法において、アドレス情報は前記プラットフォームの地理上の所在地を示すことを特徴とするソフトウェア利用許可方法。
【請求項１３】
請求項１に記載のソフトウェア利用許可方法において、
前記プラットフォーム及びコンピュータ甲はデータ通信ネットワークに接続され、

前記プラットフォームにて生成され、データ通信ネットワークを介してコンピュータ甲に送信されたメッセージに応じて、コンピュータ甲は前記プラットフォームにソフトウェア甲を提供する
ことを特徴とするソフトウェア利用許可方法。
【請求項１４】
請求項１に記載のソフトウェア利用許可方法において、
前記プラットフォーム及びコンピュータ甲はデータ通信ネットワークに接続され、
コンピュータ甲は、データ通信ネットワークを介して前記プラットフォームにソフトウェア甲を送信して提供する
ことを特徴とするソフトウェア利用許可方法。
【請求項１５】
請求項１に記載のソフトウェア利用許可方法において、
前記プラットフォーム及びコンピュータ甲は、コンピュータ読み取り可能であって取り外し可能な記録媒体を読み書きする装置を備え、
前記プラットフォームはメッセージを生成して記録媒体に書き込み、コンピュータ甲は、当該記録媒体から読み出したメッセージに応じて、前記プラットフォームにソフトウェア甲を提供する
ことを特徴とするソフトウェア利用許可方法。
【請求項１６】
請求項１に記載のソフトウェア利用許可方法において、
前記プラットフォーム及びコンピュータ甲は、コンピュータ読み取り可能であって取り外し可能な記録媒体を読み書きする装置を備え、
ソフトウェア甲の提供は、コンピュータ甲が記録媒体にソフトウェア甲を書き込み、前記プラットフォームが当該記録媒体からソフトウェア甲を読み出すことにより行われる
ことを特徴とするソフトウェア利用許可方法。
【請求項１７】
請求項１６に記載のソフトウェア利用許可方法において、記録媒体はＩＣカードが備えるＲＡＭ（ｒａｎｄｏｍ－ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）であることを特徴とするソフトウェア利用許可方法。
【請求項１８】
請求項１７に記載のソフトウェア利用許可方法において、前記ＩＣカードはＭＰＵ（ｍｉｃｒｏ　ｐｒｏｃｅｓｓｉｎｇ　ｕｎｉｔ）を備え、前記プラットフォームとして動作することを特徴とするソフトウェア利用許可方法。
【請求項１９】
請求項１に記載のソフトウェア利用許可方法において、ソフトウェア本体甲は、判定プログラム甲の一部として組み込まれ、ソフトウェア本体甲の呼び出しは判定プログラム甲を介して実行されることを特徴とするソフトウェア利用許可方法。
【請求項２０】
請求項１に記載のソフトウェア利用許可方法において、
前記プラットフォームはコンピュータからなり、
ソフトウェア甲は当該コンピュータ上で動作するオペレーティングシステムまたは当該オペレーティングシステム上で動作するコンピュータプログラムであり、
ソフトウェア乙は前記オペレーティングシステム上で動作する当該他のコンピュータプログラムである
ことを特徴とするソフトウェア利用許可方法。
【請求項２１】
請求項１に記載のソフトウェア利用許可方法において、
前記プラットフォームはコンピュータからなり、
ソフトウェア甲は当該コンピュータ上で動作するオペレーティングシステムまたは当該オペレーティングシステム上で動作するコンピュータプログラムであり、

ソフトウェア乙は当該コンピュータプログラムにより読み込まれるデータである
ことを特徴とするソフトウェア利用許可方法。
【請求項２２】
請求項１に記載のソフトウェア利用許可方法において、
前記プラットフォームはコンピュータ及び当該コンピュータ上で動作するオペレーティングシステムからなり、
ソフトウェア甲及び乙は当該オペレーティングシステム上で動作するコンピュータプログラムである
ことを特徴とするソフトウェア利用許可方法。
【請求項２３】
請求項１に記載のソフトウェア利用許可方法において、
前記プラットフォームはコンピュータ及び当該コンピュータ上で動作するオペレーティングシステムからなり、
ソフトウェア甲及び乙は、当該オペレーティングシステムまたはオペレーティングシステム上で動作するコンピュータプログラムにより読み込まれるデータである
ことを特徴とするソフトウェア利用許可方法。
【請求項２４】
請求項１に記載のソフトウェア利用許可方法において、
前記プラットフォームはコンピュータ、当該コンピュータ上で動作するオペレーティングシステム、及び当該オペレーティングシステム上で動作する第１のコンピュータプログラムからなり、
ソフトウェア甲及び乙は、前記第１のコンピュータプログラムから呼び出されるコンピュータプログラムである
ことを特徴とするソフトウェア利用許可方法。
【請求項２５】
デジタル電子情報としての複数のソフトウェア、即ち、コンピュータプログラム及びデジタルデータのいずれかを複数組み合わせて、コンピュータを含んでなるプラットフォーム上で利用することを許否する方法において、
前記複数のソフトウェアは３つ以上であって、
前記複数のソフトウェアのうちの２つのソフトウェアからなる組み合わせのうち、少なくとも１つの組み合わせの許否を請求項２に記載の方法で行う
ことを特徴とするソフトウェア利用許可方法。
【請求項２６】
デジタル電子情報としての複数のソフトウェア、即ち、コンピュータプログラム及びデジタルデータのいずれかを複数組み合わせて、コンピュータを含んでなるプラットフォーム上で利用することを許否するシステムにおいて、
前記プラットフォームと、
前記プラットフォーム上で組み合わせて利用することの許否を判定されるソフトウェアであるソフトウェア本体甲及び乙と、
ソフトウェア本体乙が、ソフトウェア甲の組み合わせ相手として認められるか否かを判定するためのコンピュータプログラムであり、前記プラットフォーム上で実行される判定プログラム甲と、
ソフトウェア本体甲及び判定プログラム甲をソフトウェア甲として前記プラットフォームに提供するコンピュータ甲と、
ソフトウェア本体乙を前記プラットフォームに提供するコンピュータ乙とを備え、
判定プログラム甲による判定結果が認める旨である場合に限り、ソフトウェア本体甲と組み合わせて利用するソフトウェアとして、ソフトウェア本体乙を許可する処理を前記プラットフォームが実行する
ことを特徴とするソフトウェア利用許可システム。
【請求項２７】

請求項２６に記載のソフトウェア利用許可システムにおいて、
ソフトウェア本体乙は、前記判定プログラムである判定プログラム乙と共にソフトウェア乙としてコンピュータ乙を介して提供され、
判定プログラム甲及び乙による判定結果の両方が認める旨である場合に限り、ソフトウェア本体甲及び乙を組み合わせて利用することを許可する処理を、当該コンピュータが実行する
ことを特徴とするソフトウェア利用許可システム。
【請求項２８】
請求項２６に記載のソフトウェア利用許可システムにおいて、
前記プラットフォームは、コンピュータ甲に対してソフトウェア本体甲の提供を要求するメッセージ甲にデジタル署名Ｓを施したもの、及び、コンピュータ乙に対してソフトウェア本体乙の提供を要求するメッセージ乙にデジタル署名Ｓを施したものを生成し、
コンピュータ甲は、デジタル署名Ｓに基づいて前記プラットフォームの認証に成功した場合に限り、ソフトウェア甲にデジタル署名甲を施して前記プラットフォームに宛てて提供する処理を実行し、
コンピュータ乙は、デジタル署名Ｓに基づいて前記プラットフォームの認証に成功した場合に限り、ソフトウェア乙にデジタル署名乙を施して前記プラットフォームに宛てて提供する処理を実行し、
前記プラットフォームは、提供されたソフトウェア甲及び乙のそれぞれに施されたデジタル署名甲及び乙に基づいて、コンピュータ甲及び乙を認証する処理を実行し、
コンピュータ甲及び乙の認証が両方とも成功した場合に限り、前記プラットフォームは判定プログラム甲及び乙を実行し、
前記プラットフォームは、判定プログラム甲及び乙の実行結果が両方とも認める旨である場合に限り、ソフトウェア本体甲及び乙を組み合わせて利用することを許可する処理を実行する
ことを特徴とするソフトウェア利用許可システム。
【請求項２９】
請求項２６に記載のソフトウェア利用許可システムにおいて、
前記プラットフォームとデータ通信ネットワークを介してデータ通信可能な他のコンピュータを更に備え、
前記プラットフォームは、判定プログラム甲に従ってデータ通信ネットワークを介して他のコンピュータとデータ通信を行い、当該他のコンピュータによる判定に従って判定を行う
ことを特徴とするソフトウェア利用許可システム。
【請求項３０】
請求項２９に記載のソフトウェア利用許可システムにおいて、前記他のコンピュータはコンピュータ甲であることを特徴とするソフトウェア利用許可システム。
【請求項３１】
請求項２７に記載のソフトウェア利用許可システムにおいて、
前記プラットフォームとデータ通信ネットワークを介してデータ通信可能な他のコンピュータＡ及びＢを更に備え、
前記プラットフォームは、判定プログラム甲に従って、ソフトウェア乙の少なくとも一部を、前記データ通信ネットワークを介して、コンピュータＡに送信し、
コンピュータＡは、送信されたソフトウェア乙の一部乃至全部に基づいて、ソフトウェア甲に対してソフトウェア乙を組み合わせることの可否を判定して、その判定結果甲を、前記データ通信ネットワークを介して前記プラットフォームに送信し、
前記プラットフォームは、判定プログラム甲に従って受信した判定結果甲に応じて判定し、
前記プラットフォームは、判定プログラム乙に従って、ソフトウェア甲の少なくとも一部を、前記データ通信ネットワークを介して、コンピュータＢに送信し、

コンピュータＢは、送信されたソフトウェア乙の一部乃至全部に基づいて、ソフトウェア甲に対してソフトウェア乙を組み合わせることの可否を判定して、その判定結果乙を、データ通信ネットワークを介して前記プラットフォームに送信し、
前記プラットフォームは、判定プログラム乙に従って、受信した判定結果乙に応じて判定する
ことを特徴とするソフトウェア利用許可システム。
【請求項３２】
請求項３１に記載のソフトウェア利用許可システムにおいて、コンピュータＡはコンピュータ甲であること、及び、コンピュータＢはコンピュータ乙であることのうち、少なくとも一方が成り立つことを特徴とするソフトウェア利用許可システム。
【請求項３３】
請求項２６に記載のソフトウェア利用許可システムにおいて、判定プログラム甲は、予めソフトウェア乙に添付されたデジタル署名による認証の結果に基づいて、ソフトウェア本体甲と組み合わせて利用するソフトウェアとして、ソフトウェア乙を許可する処理を、前記プラットフォームに実行させることを特徴とするソフトウェア利用許可システム。
【請求項３４】
請求項２６に記載のソフトウェア利用許可システムにおいて、
コンピュータ甲は、前記プラットフォームにて生成された公開暗号方式の暗号鍵を用いて暗号化したソフトウェアを提供する処理を実行し、
ソフトウェアの提供を受けた前記プラットフォームは、前記暗号鍵と対になって生成した復号鍵を用いてソフトウェアを復号する処理を実行する
ことを特徴とするソフトウェア利用許可システム。
【請求項３５】
請求項２６に記載のソフトウェア利用許可システムにおいて、
コンピュータ甲は、前記プラットフォームにて生成されたメッセージに応じてソフトウェア甲を提供する処理を実行し、
メッセージは前記プラットフォームの所在を示すアドレス情報を含む
ことを特徴とするソフトウェア利用許可システム。
【請求項３６】
請求項３５に記載のソフトウェア利用許可システムにおいて、
アドレス情報は前記プラットフォームのデータ通信ネットワーク上でのアドレス情報であり、
当該アドレス情報に基づいてデータ通信ネットワーク上の前記プラットフォームにソフトウェア甲を送信する
ことを特徴とするソフトウェア利用許可システム。
【請求項３７】
請求項３５に記載のソフトウェア利用許可システムにおいて、アドレス情報は前記プラットフォームの地理上の所在地を示すことを特徴とするソフトウェア利用許可システム。
【請求項３８】
請求項２６に記載のソフトウェア利用許可システムにおいて、
前記プラットフォーム及びコンピュータ甲はデータ通信ネットワークに接続され、
前記プラットフォームにて生成され、データ通信ネットワークを介してコンピュータ甲に送信されたメッセージに応じて、コンピュータ甲は前記プラットフォームにソフトウェア甲を提供する
ことを特徴とするソフトウェア利用許可システム。
【請求項３９】
請求項２６に記載のソフトウェア利用許可システムにおいて、
前記プラットフォーム及びコンピュータ甲はデータ通信ネットワークに接続され、
コンピュータ甲は、データ通信ネットワークを介して前記プラットフォームにソフトウェア甲を送信して提供する

ことを特徴とするソフトウェア利用許可システム。
【請求項４０】
請求項２６に記載のソフトウェア利用許可システムにおいて、
前記プラットフォーム及びコンピュータ甲は、コンピュータ読み取り可能であって取り外し可能な記録媒体を読み書きする装置を備え、
前記プラットフォームはメッセージを生成して記録媒体に書き込み、コンピュータ甲は、当該記録媒体から読み出したメッセージに応じて、前記プラットフォームにソフトウェア甲を提供する
ことを特徴とするソフトウェア利用許可システム。
【請求項４１】
請求項２６に記載のソフトウェア利用許可システムにおいて、
前記プラットフォーム及びコンピュータ甲は、コンピュータ読み取り可能であって取り外し可能な記録媒体を読み書きする装置を備え、
ソフトウェア甲の提供は、コンピュータ甲が記録媒体にソフトウェア甲を書き込み、前記プラットフォームが当該記録媒体からソフトウェア甲を読み出すことにより行われる
ことを特徴とするソフトウェア利用許可システム。
【請求項４２】
請求項４１に記載のソフトウェア利用許可システムにおいて、記録媒体はＩＣカードが備えるＲＡＭ（ｒａｎｄｏｍ－ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）であることを特徴とするソフトウェア利用許可システム。
【請求項４３】
請求項４２に記載のソフトウェア利用許可システムにおいて、前記ＩＣカードはＭＰＵ（ｍｉｃｒｏ　ｐｒｏｃｅｓｓｉｎｇ　ｕｎｉｔ）を備え、前記プラットフォームとして動作することを特徴とするソフトウェア利用許可システム。
【請求項４４】
請求項２６に記載のソフトウェア利用許可システムにおいて、ソフトウェア本体甲は、判定プログラム甲の一部として組み込まれ、ソフトウェア本体甲の呼び出しは判定プログラム甲を介して実行されることを特徴とするソフトウェア利用許可システム。
【請求項４５】
請求項２６に記載のソフトウェア利用許可システムにおいて、
前記プラットフォームはコンピュータからなり、
ソフトウェア甲は当該コンピュータ上で動作するオペレーティングシステムまたは当該オペレーティングシステム上で動作するコンピュータプログラムであり、
ソフトウェア乙は前記オペレーティングシステム上で動作する当該他のコンピュータプログラムである
ことを特徴とするソフトウェア利用許可システム。
【請求項４６】
請求項２６に記載のソフトウェア利用許可システムにおいて、
前記プラットフォームはコンピュータからなり、
ソフトウェア甲は当該コンピュータ上で動作するオペレーティングシステムまたは当該オペレーティングシステム上で動作するコンピュータプログラムであり、
ソフトウェア乙は当該コンピュータプログラムにより読み込まれるデータである
ことを特徴とするソフトウェア利用許可システム。
【請求項４７】
請求項２６に記載のソフトウェア利用許可システムにおいて、
前記プラットフォームはコンピュータ及び当該コンピュータ上で動作するオペレーティングシステムからなり、
ソフトウェア甲及び乙は当該オペレーティングシステム上で動作するコンピュータプログラムである
ことを特徴とするソフトウェア利用許可システム。

【請求項４８】
請求項２６に記載のソフトウェア利用許可システムにおいて、
前記プラットフォームはコンピュータ及び当該コンピュータ上で動作するオペレーティングシステムからなり、
ソフトウェア甲及び乙は、当該オペレーティングシステムまたはオペレーティングシステム上で動作するコンピュータプログラムにより読み込まれるデータである
ことを特徴とするソフトウェア利用許可システム。
【請求項４９】
請求項２６に記載のソフトウェア利用許可システムにおいて、
前記プラットフォームはコンピュータ、当該コンピュータ上で動作するオペレーティングシステム、及び当該オペレーティングシステム上で動作する第１のコンピュータプログラムからなり、
ソフトウェア甲及び乙は、前記第１のコンピュータプログラムから呼び出されるコンピュータプログラムである
ことを特徴とするソフトウェア利用許可システム。
【請求項５０】
デジタル電子情報としての複数のソフトウェア、即ち、コンピュータプログラム及びデジタルデータのいずれかを複数組み合わせて、コンピュータを含んでなるプラットフォーム上で利用することを許否するシステムにおいて、
前記複数のソフトウェアは３つ以上であって、
前記複数のソフトウェアのうちの２つのソフトウェアからなる組み合わせのうち、少なくとも１つの組み合わせの許否を行う請求項２７に記載のシステムを備える
ことを特徴とするソフトウェア利用許可システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータプログラム及びデジタルデータを含むソフトウェアの利用を、ソフトウェア提供者等が制限する技術に関する。
【背景技術】
【０００２】
パーソナルコンピュータの普及に伴って、コンピュータプログラム（以下プログラムと記す）やデジタルデータ（以下データと記す）といったソフトウェアを提供するビジネスが盛んであるが、最近では、携帯電話端末を含む携帯情報端末や、ＩＣカードが備えるＣＰＵ、ＭＰＵ等の処理装置の処理能力向上に伴い、これら装置を対象とするソフトウェアが加わって、ビジネスは一層盛んになるものと予想される。
【０００３】
こうした状況の中でソフトウェア提供者等がソフトウェアの利用に制限を課す技術が求められている。特に、複数のソフトウェアを組み合わせて利用する際に、ソフトウェア提供者の立場から見ると、認めてよい組み合わせと、望ましくない組み合わせがあり、ソフトウェアの組み合わせを制限する技術が求められている。
【０００４】
関連した従来技術としは、ソフトウェア利用プラットフォームに耐タンパ性のあるＩＣカードを利用することにより、ソフトウェア利用が正当に行われることへの信頼性を高めたものがある（例えば特許文献１を参照）。
【０００５】
特許文献１によれば、ソフトウェア提供者が、ソフトウェアの正当な利用が阻害されないような、特定のソフトウェア利用プラットフォーム(ＩＣカード等)上でのみ動作可能な形式・手法でソフトウェアを提供する一方、ソフトウェア利用者は、この特定のソフトウェア利用プラットフォーム上でソフトウェアを利用することにより、信頼性向上を図って

いる。
【０００６】
関連する他の従来技術には、デジタル署名を施してソフトウェアを配信し、配信を受けたソフトウェア利用プラットフォームは、デジタル署名情報に基づいてソフトウェアの信頼性を確認するといった技術がある。このような技術の具体例にはＭｉｃｒｏｓｏｆｔ社のＡｃｔｉｖｅＸ配信技術が挙げられる。
【０００７】
この種の従来技術では、ソフトウェア配信者がソフトウェアに自身のデジタル署名を施して配信する。配信を受けたソフトウェア利用プラットフォームは、デジタル署名情報に基づいてソフトウェア配信者を特定し、特定されたソフトウェア配信者を信頼するならば、配信されたソフトウェアも信頼して利用するといった手順により、ソフトウェアの利用に制限を課している。
【０００８】
更に他の従来技術として、ソフトウェアが相互に信頼性を確認するステップを含むことにより、不正な組み合わせでソフトウェアが利用されることを回避する技術がある（例えば特許文献２を参照）。
【０００９】
特許文献２には、ソフトウェア利用プラットフォームを介して、ソフトウェアＡがソフトウェアＢの信頼性を確認する一方で、同じくソフトウェア利用プラットフォームＰを介して、ソフトウェアＢがソフトウェアＡの信頼性を確認し、相互に信頼性があると確認された場合のみ、ソフトウェアＡ及びＢを組み合わせて利用する技術が開示されている。
【００１０】
【特許文献１】特開平１０－２０９５８号公報
【特許文献２】特開平９－２３１０６８号公報
【発明の開示】
【発明が解決しようとする課題】
【００１１】
特許文献１に記載の技術に代表されるタイプの従来技術によれば、ソフトウェア提供者は、自らが提供するソフトウェアを特定のプラットフォーム上で利用することの可否について制限を課すことができるものの、あるソフトウェアと組み合わせて利用することを許可する一方で、別のソフトウェアと組み合わせて利用することを禁止するといったことはできなかった。これは、個々のソフトウェアがソフトウェア利用プラットフォームの信頼性は確認できるが、組み合わせ相手となるソフトウェアの信頼性を確認する手段が用意されていないからである。
【００１２】
また、ＡｃｔｉｖｅＸ配信技術に代表されるタイプの従来技術によっても、ソフトウェアの組み合わせ相手を制限することはできない。また、ソフトウェアの利用者の立場から見ての利用制限は可能であるが、ソフトウェア提供者の立場から見ての利用制限、即ち、ソフトウェア提供者が、望まないソフトウェア利用プラットフォーム上で、ソフトウェアを利用することを禁止できない。これは、ソフトウェア利用プラットフォームの信頼性を、ソフトウェア提供者が確認する手段が用意されていないからである。
【００１３】
また、特許文献２に記載の技術に代表されるタイプの従来技術によれば、ソフトウェアの組み合わせ相手に制限を課すことができるものの、ソフトウェア利用プラットフォームが不正な場合、不正な組み合わせでソフトウェアＡ及びＢが利用されるのを防ぐことができないといった問題がある。この従来技術では、ソフトウェアの信頼性を確認する際に、ソフトウェア利用プラットフォームが介入しているため、ソフトウェア利用プラットフォームが信頼性の確認を故意にスキップする、或いは、信頼性についての検証結果を改ざんする等の可能性があるからである。
【００１４】

このような状況に鑑みて、本発明が解決しようとする課題は、プラットフォームの信頼性に影響されることなく、或いは、プラットフォームの信頼性を確認した上で、複数のソフトウェアを組み合わせて利用する際の組み合わせ相手となるソフトウェア毎に、ソフトウェアの利用の可否を制限することができる技術を提供することである。

【課題を解決するための手段】

【００１５】

上述の課題を解決するため、本発明は次のようなソフトウェアの利用許可方法及びシステムを提供する。

【００１６】

本発明は、デジタル電子情報としての複数のソフトウェア、即ち、コンピュータプログラム及びデジタルデータのいずれかを複数組み合わせて、コンピュータを含んでなるプラットフォーム上で利用することを許否する方法及びシステムとして、次のようなものを提供する。まず、デジタル電子情報であるソフトウェア本体甲を提供する際に、ソフトウェア本体甲と組み合わせて利用しようとしているソフトウェアであって、デジタル電子情報である他のソフトウェア本体乙が、組み合わせ相手として認められるか否かを判定するためのコンピュータプログラムである判定プログラム甲を用意して、ソフトウェア本体甲と共にソフトウェア甲としてコンピュータ甲を介して提供する。次に、ソフトウェア本体甲をソフトウェア乙と組み合わせてプラットフォーム上で利用するのに先立って、判定プログラム甲をプラットフォームが実行する。そして、判定プログラム甲による判定結果が認める旨である場合に限り、ソフトウェア本体甲と組み合わせて利用するソフトウェアとして、ソフトウェア本体乙を許可する処理をプラットフォームが実行する。

【００１７】

ソフトウェア本体乙は、判定プログラムである判定プログラム乙と共にソフトウェア乙としてコンピュータ乙を介して提供され、判定プログラム甲及び乙による判定結果の両方が認める旨である場合に限り、ソフトウェア本体甲及び乙を組み合わせて利用することを許可する処理を、当該コンピュータが実行することとすれば、ソフトウェア本体甲及び乙を提供する双方の立場から、組み合わせ相手のソフトウェア本体の妥当性を評価することができる。

【００１８】

更に詳しくは、ソフトウェア本体甲の提供を要求するメッセージ甲にデジタル署名Ｓを施したものがプラットフォームにて生成されてコンピュータ甲に通知されると共に、ソフトウェア本体乙の提供を要求するメッセージ乙にデジタル署名Ｓを施したものがプラットフォームにて生成されてコンピュータ乙に通知される段階１と、コンピュータ甲がデジタル署名Ｓに基づいてプラットフォームの認証に成功した場合に限り、コンピュータ甲にてデジタル署名甲を施されたソフトウェア甲が、プラットフォームに提供される段階２と、コンピュータ乙がデジタル署名Ｓに基づいてプラットフォームの認証に成功した場合に限り、コンピュータ乙にてデジタル署名乙を施されたソフトウェア乙が、プラットフォームに提供される段階３と、提供されたソフトウェア甲及び乙のそれぞれに施されたデジタル署名甲及び乙に基づいて、プラットフォームがコンピュータ甲及び乙を認証する段階４と、段階４でのコンピュータ甲及び乙の認証が両方とも成功した場合に限り、プラットフォームが判定プログラム甲及び乙を実行する段階５と、段階５での判定プログラム甲及び乙の実行結果が両方とも認める旨である場合に限り、ソフトウェア本体甲及び乙を組み合わせて利用することを許可する段階６とを含むこととしてもよい。

【００１９】

判定プログラム甲に従って、プラットフォームは、データ通信ネットワークを介して他のコンピュータとデータ通信を行い、当該他のコンピュータによる判定に従って判定を行うこととしてもよい。この場合、許否の判定を実際に行うコンピュータはプラットフォームではなく他のコンピュータであるので、不正なプラットフォームであっても偽の許可判定を行うのが困難となる。ここでいう他のコンピュータは例えばコンピュータ甲であってもよい。

【００２０】
判定プログラム甲及び乙による判定結果を参照する場合であれば、判定プログラム甲に従って、プラットフォームは、ソフトウェア乙の少なくとも一部を、データ通信ネットワークを介して予め定められた他のコンピュータＡに送信し、コンピュータＡは、送信されたソフトウェア乙の一部乃至全部に基づいて、ソフトウェア甲に対してソフトウェア乙を組み合わせることの可否を判定して、その判定結果甲を、データ通信ネットワークを介してプラットフォームに送信し、判定プログラム甲に従って、プラットフォームは、受信した判定結果甲に従って判定し、判定プログラム乙に従って、プラットフォームは、ソフトウェア甲の少なくとも一部を、データ通信ネットワークを介して予め定められた他のコンピュータＢに送信し、コンピュータＢは、送信されたソフトウェア乙の一部乃至全部に基づいて、ソフトウェア甲に対してソフトウェア乙を組み合わせることの可否を判定して、その判定結果乙を、データ通信ネットワークを介してプラットフォームに送信し、判定プログラム乙に従って、プラットフォームは、受信した判定結果乙に従って判定することとしてもよい。この場合、コンピュータＡはコンピュータ甲であること、及び、コンピュータＢはコンピュータ乙であることのうち、少なくとも一方が成り立つこととしてもよい。
【００２１】
判定プログラム甲は、予めソフトウェア乙に添付されたデジタル署名による認証の結果に基づいて、ソフトウェア本体甲と組み合わせて利用するソフトウェアとして、ソフトウェア乙を許可することとしてもよい。
【００２２】
コンピュータ甲は、プラットフォームにて生成された公開暗号方式の暗号鍵を用いて暗号化したソフトウェアを提供し、ソフトウェアの提供を受けたプラットフォームは、暗号鍵と対になって生成した復号鍵を用いてソフトウェアを復号する処理を実行することとしてもよい。このようにすれば、プラットフォームはコンピュータ甲の詐称や、ソフトウェア甲の内容の改竄を検出することができる。
【００２３】
コンピュータ甲は、プラットフォームにて生成されたメッセージに応じてソフトウェア甲を提供し、メッセージはプラットフォームの所在を示すアドレス情報を含むこととしてもよい。このとき、アドレス情報はプラットフォームのデータ通信ネットワーク上でのアドレス情報であってもよいし、或いは、プラットフォームの地理上の所在地を示すこととしてもよい。
【００２４】
プラットフォーム及びコンピュータ甲はデータ通信ネットワークに接続され、プラットフォームにて生成され、データ通信ネットワークを介してコンピュータ甲に送信されたメッセージに応じて、コンピュータ甲はプラットフォームにソフトウェア甲を提供することとしてもよい。
【００２５】
プラットフォーム及びコンピュータ甲はデータ通信ネットワークに接続され、コンピュータ甲は、データ通信ネットワークを介してプラットフォームにソフトウェア甲を送信して提供することとしてもよい。
【００２６】
プラットフォーム及びコンピュータ甲は、コンピュータ読み取り可能であって取り外し可能な記録媒体を読み書きする装置を備え、プラットフォームはメッセージを生成して記録媒体に書き込み、コンピュータ甲は、当該記録媒体から読み出したメッセージに応じて、プラットフォームにソフトウェア甲を提供することとしてもよい。
【００２７】
プラットフォーム及びコンピュータ甲は、コンピュータ読み取り可能であって取り外し可能な記録媒体を読み書きする装置を備え、ソフトウェア甲の提供は、コンピュータ甲が記録媒体にソフトウェア甲を書き込み、プラットフォームが当該記録媒体からソフトウェア甲を読み出すことにより行われることとしてもよい。このとき、記録媒体は例えばＩＣ

カードが備えるＲＡＭ（ｒａｎｄｏｍ－ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）であってもよい。また、ＩＣカードはＭＰＵ（ｍｉｃｒｏ　ｐｒｏｃｅｓｓｉｎｇ　ｕｎｉｔ）を備え、プラットフォームとして動作することとしてもよい。

【００２８】

ソフトウェア本体甲は、判定プログラム甲の一部として組み込まれ、ソフトウェア本体甲の呼び出しは判定プログラム甲を介して実行されることとしてもよい。

【００２９】

プラットフォームはコンピュータからなり、ソフトウェア甲は当該コンピュータ上で動作するオペレーティングシステムまたは当該オペレーティングシステム上で動作するコンピュータプログラムであり、ソフトウェア乙はオペレーティングシステム上で動作する当該他のコンピュータプログラムであることとしてもよい。

【００３０】

プラットフォームはコンピュータからなり、ソフトウェア甲は当該コンピュータ上で動作するオペレーティングシステムまたは当該オペレーティングシステム上で動作するコンピュータプログラムであり、ソフトウェア乙は当該コンピュータプログラムにより読み込まれるデータであることとしてもよい。

【００３１】

プラットフォームはコンピュータ及び当該コンピュータ上で動作するオペレーティングシステムからなり、ソフトウェア甲及び乙は当該オペレーティングシステム上で動作するコンピュータプログラムであることとしてもよい。

【００３２】

プラットフォームはコンピュータ及び当該コンピュータ上で動作するオペレーティングシステムからなり、ソフトウェア甲及び乙は、当該オペレーティングシステムまたはオペレーティングシステム上で動作するコンピュータプログラムにより読み込まれるデータであることとしてもよい。

【００３３】

プラットフォームはコンピュータ、当該コンピュータ上で動作するオペレーティングシステム、及び当該オペレーティングシステム上で動作する第１のコンピュータプログラムからなり、ソフトウェア甲及び乙は、第１のコンピュータプログラムから呼び出されるコンピュータプログラムであることとしてもよい。

【００３４】

デジタル電子情報としての複数のソフトウェア、即ち、コンピュータプログラム及びデジタルデータのいずれかを複数組み合わせて、コンピュータを含んでなるプラットフォーム上で利用することを許否する方法において、複数のソフトウェアは３つ以上であって、複数のソフトウェアのうちの２つのソフトウェアからなる組み合わせのうち、少なくとも１つの組み合わせの許否を上述の方法で行うこととしてもよい。

【発明の効果】

【００３５】

本発明によれば、ソフトウェア本体と共に判定プログラムを提供し、判定プログラムが許可する判定結果を出力した場合に限り、ソフトウェア本体と他のソフトウェア本体とを組み合わせて利用することを許可する。この許可は、例えばソフトウェア本体を提供する処理を実行するコンピュータ等のソフトウェア本体を利用するプラットフォーム以外のコンピュータにより実行される。また例えば、公開鍵暗号方式を利用したデジタル署名により正当性を確認して行う。このため、プラットフォーム側での不正により偽の許可を行うことが困難である。

【発明を実施するための最良の形態】

【００３６】

本発明の実施の形態であるソフトウェア利用許可システム１について図１を参照して説明する。まずソフトウェア利用許可システム１の構成要素それぞれについて説明する。

【００３７】

ソフトウェア利用許可システム１は、プラットフォーム２、ソフトウェア３、４（以下ソフトウェア甲、乙と記す場合もあり）、情報処理装置５、６（以下情報処理装置甲、乙と記す場合もあり）からなる。

【００３８】

プラットフォーム２は少なくともハードウェアを含み、実施例によっては、更に、ハードウェア上で動作するオペレーティングシステム（以下ＯＳと記す）を含む場合や、ＯＳに加えてＯＳ上で動作するコンピュータプログラム（以下単にプログラムと記す）をも含む場合がある。ソフトウェア３及び４はプラットフォーム２上で利用される。

【００３９】

プラットフォーム２のハードウェアは耐タンパ性を有するように構成される。耐タンパ性を有するハードウェアとは、筐体をこじ開けるなど、外部からの不正な手続による秘密情報の漏洩や改竄、不正なアクセス等を防ぐための物理的・論理的機能を有するハードウェアをいう。より具体的には、プラットフォーム２は、物理的・電気的に耐タンパ性を有するコンピュータと、その上で動作するＯＳ及びプログラムからなる。或いは、プラットフォーム２は、物理的・電気的に耐タンパ性を有するＩＣカードからなる。或いは、厳格なプロセス管理・ユーザ管理によって、不正なソフトウェアが、他のソフトウェアに干渉することを防止する機構を備えたオペレーティングシステムを含んで構成される。また、例えば、コンピュータ上にＪａｖａ（登録商標）ＶＭ（ＶｉｒｔｕａｌＭａｃｈｉｎｅ）等に代表される仮想マシンをつくり、仮想マシンの外のソフトウェアからの干渉を困難にしたシステムとして構成される、また、それ以外にも、利用ソフト群の正当な利用を妨げる、様々な要因を排除できるようなハードウェア、もしくはソフトウェア、もしくはそれらの複合したシステムとして構成される。

【００４０】

ソフトウェア３及び４は、プログラム及びデータの両方を指すものとする。「ソフトウェアを利用する」とは、そのソフトウェアがプログラムであればプラットフォーム上で実行することを指す。そのソフトウェアがデータであればプラットフォーム上で実行されたプログラムやＯＳにより読み込まれることや書き換えられることを指す。ソフトウェア３はソフトウェア提供者甲により提供され、ソフトウェア４はソフトウェア提供者甲とは異なる乙により提供される。

【００４１】

情報処理装置５はソフトウェア提供者甲により管理され、ソフトウェア３を他のソフトウェアと組み合わせて利用することの可否を判断する処理を自動的に行う。同様に、情報処理装置６はソフトウェア提供者乙により管理され、ソフトウェア４を他のソフトウェアと組み合わせて利用することの可否を判断する処理を自動的に行う。

【００４２】

このような構成からなるソフトウェア利用許可システム１において、プラットフォーム２上でソフトウェア３とソフトウェア４とを組み合わせて利用する際、これに先立って、プラットフォーム２－ソフトウェア３、プラットフォーム２－ソフトウェア４、ソフトウェア３－ソフトウェア４のそれぞれの間で信頼性を確認し、これら全ての間で信頼性が確認された場合に限って、プラットフォーム２上でソフトウェア３及び４を組み合わせて利用することを許可する。

【００４３】

この利用許可は次のステップＡ～Ｅを経て実行される。

【００４４】

まず、ソフトウェア提供者甲及び乙のそれぞれの立場から、情報処理装置甲及び乙がプラットフォーム２を認証し、認証に成功した場合に限り、それぞれがプラットフォーム２に対してソフトウェア甲及び乙を供給する。

【００４５】

（ステップＡ）情報処理装置甲がプラットフォーム２を認証することにより、ソフトウェア提供者甲の立場からプラットフォーム２の信頼性の有無を確認する。

【００４６】
具体的には、例えばプラットフォーム２によるデジタル署名を情報処理装置甲が認証することにより行う。
【００４７】
または、固有の識別符号を書き込んだ書き換え不能な記録媒体を備えるプラットフォーム２と情報処理装置甲とを接続し、この識別符号を読み込むことにより、情報処理装置甲がプラットフォーム２を認証してもよい。
【００４８】
認証に成功して信頼性が確認されたならば、ソフトウェア提供者甲は、プラットフォーム２以外では利用不可能もしくは困難な形式で、ソフトウェア甲をプラットフォーム２に対して供給する。
【００４９】
プラットフォーム２以外では利用不可能もしくは困難な形式で供給するとは、例えばソフトウェア甲を暗号化して提供することである。ここでの暗号化方式として公開暗号方式を用いる場合、情報処理装置甲にプラットフォーム２の暗号化鍵を予め渡しておく。
【００５０】
ソフトウェア甲の供給経路としては、ネットワークを介したデータ通信にてプラットフォーム２がソフトウェア甲を受信する経路や、ソフトウェア甲を格納したＣＤ－ＲＯＭ等のリムーバブルメディアの記録媒体から、プラットフォーム２の読み込み装置を使って読み込む経路がある。
【００５１】
（ステップＢ）ステップＡと同様に、情報処理装置乙がプラットフォーム２を認証することにより、ソフトウェア提供者乙の立場からプラットフォーム２の信頼性の有無を確認する。信頼性が確認されたならば、ソフトウェア提供者乙は、プラットフォーム２以外には利用不可能もしくは困難な形式で、ソフトウェア乙をプラットフォーム２に対して提供する。ソフトウェアの提供形式及び供給経路について詳しくはステップＡと同様である。
【００５２】
次に、ソフトウェア甲及び乙が、他方のソフトウェアを信頼するか否かを判定するための処理がプラットフォーム２で実行される。
【００５３】
（ステップＣ）プラットフォーム２はソフトウェア甲にソフトウェア乙を認証させることにより、ソフトウェア甲がソフトウェア乙を信頼するか否か確認する。
【００５４】
ソフトウェア甲によるソフトウェア乙の認証は、例えば、組み合わせ相手のソフトウェアを認証する処理をプラットフォーム２に実行させる認証プログラムをソフトウェア甲に組み込み、プラットフォーム２が、この認証プログラムをソフトウェア甲の利用に先立って実行することにより行う。認証プログラムは、認証に必要な情報をソフトウェア乙から取得し、認証の可否を判定し、その判定結果に応じて信頼の可否を確認する。
【００５５】
或いは、認証プログラムは、必要な情報を取得すると他の情報処理装置、例えば情報処理装置甲に取得した情報を渡して、認証の可否の判定は情報処理装置甲から受け取ることとしてもよい。この場合、認証の可否を判定するのは情報処理装置甲である。
【００５６】
（ステップＤ）ステップＣと同様に、プラットフォーム２はソフトウェア乙にソフトウェア甲を認証させることにより、ソフトウェア乙がソフトウェア乙を信頼するか否か確認する。
【００５７】
（ステップＥ）ステップＣ及びＤの両方で信頼可能と判定された場合に限り、プラットフォーム上でソフトウェア甲及び乙を組み合わせて利用することが許可され、必要に応じて実際に組み合わせて利用される。

【００５８】
ここでソフトウェア甲及び乙を組み合わせて利用するとは次のような意味である。ソフトウェア甲及び乙が共にプログラムである場合、例えば一方の出力を他方の入力としてコンピュータが処理を行うことをいう。ソフトウェア甲及び乙の一方がプログラムであって他方がデータである場合、コンピュータはそのプログラムに従ってそのデータを読み込んで所定の処理を実行し、更に必要に応じてそのデータを書き換えることをいう。ソフトウェア甲及び乙の両方がデータである場合、ＯＳ或いはＯＳ上で動作するプログラムが両方のデータを読み込んで所定の処理を実行し、必要に応じてデータの一方或いは両方を書き換えることをいう。
【００５９】
ソフトウェア甲及び乙は、ＯＳ、ＯＳを含むプログラム、或いは、ＯＳを含むプログラム上で実行される他のプログラム及びデータのいずれかである。これらの組み合わせについて図２を参照して説明する。図中の矢印は、信頼が相互に確認され、組み合わせて利用されるソフトウェア甲及び乙を結んでいる。斜線部はプラットフォームを表す。
【００６０】
（ａ）ではハードウェアがプラットフォームであり、ＯＳ及びプログラムがソフトウェア甲及び乙にあたる。ここで組み合わせて利用するとは、ＯＳ上でプログラムを実行することをさす。
【００６１】
（ｂ）ではハードウェアがプラットフォームであり、ＯＳ及びデータがソフトウェア甲及び乙にあたる。組み合わせ利用とは、ＯＳがデータにアクセスすること、即ち、データの読み込み、更新、削除等をさす。
【００６２】
（ｃ）ではＯＳ及びハードウェアがプラットフォームにあたり、ＯＳ上で実行される２つのプログラムがソフトウェア甲及び乙にあたる。ここで組み合わせ利用とは、一方のプログラムの指示に応じて他方のプログラムが動作することをさす。具体的には、アプリケーションプログラムと、このアプリケーションプログラムへの課金用ソフトウェアがある。例えば、プレイ時間によって料金の変わるゲームプログラムと、クレジットカード会社への課金情報通知を行う通信プログラムの組み合わせである。また、他の具体例としては、画像編集プログラムと、画像フォーマット毎に用意された読み込み／書き出しライブラリとの組み合わせがある。
【００６３】
（ｄ）ではＯＳ及びハードウェアがプラットフォームにあたり、ＯＳが参照する２つのデータがソフトウェア甲及び乙にあたる。ここで組み合わせ利用とは、ＯＳが２つのデータの両方を読み込んで、一方の内容を他方にコピーする、一方の内容を元に他方の内容を変更する、両方のデータを合体する等をさす。
【００６４】
（ｅ）ではＯＳ及びハードウェアがプラットフォームにあたり、ＯＳ上で実行されるプログラムと、プログラムが参照するデータとがソフトウェア甲及び乙にあたる。ここで組み合わせ利用とは、プログラムがデータを参照して動作することを指し、例えばデータを表示・再生・編集・更新・変換等することをいう。具体例としては音楽データと、それを再生するプレイヤープログラムの組み合わせがある。
【００６５】
（ｆ）ではプログラム、ＯＳ、ハードウェアがプラットフォームにあたり、プログラムが参照する２つのデータがソフトウェア甲及び乙にあたる。ここで組み合わせ利用とは、プログラムが２つのデータの両方を読み込んで、一方の内容を他方にコピーする、一方の内容を元に他方の内容を変更する、両方のデータを合体する等をさす。具体例としては、カーナビゲーションシステムにおける地図データと、渋滞情報データの組み合わせがある。
【００６６】

このようなソフトウェア利用許可システム１によれば、ソフトウェア提供者甲がソフトウェア提供者乙を信頼していないにも関わらず、ソフトウェア本体甲の組み合わせ相手としてソフトウェア本体乙が認められて利用されることを防止することができる。逆に、ソフトウェア提供者乙がソフトウェア提供者甲を信頼していないにも関わらず、ソフトウェア本体乙の組み合わせ相手としてソフトウェア本体甲が認められて利用されることを防止することもできる。

【００６７】

また、ソフトウェア提供者甲がプラットフォームの安全性を信頼していないにも関わらず、ソフトウェア本体甲がプラットフォーム上で利用されることを防止することができる。同様に、ソフトウェア提供者乙がプラットフォームの安全性を信頼していないにも関わらず、ソフトウェア本体乙がプラットフォーム上で利用されることを防止することができる。

【００６８】

尚、ソフトウェアの配信や書き込みを要求するメッセージが、プラットフォームから情報処理装置に伝送される経路と、情報処理装置からプラットフォームにソフトウェアが伝送される経路とは、同じであっても異なっていてもよい。例えば、両方ともネットワーク経由、一方をネットワーク経由で他方を記録媒体経由、或いは両方とも記録媒体経由とすることが考えられる。また、両方ともネットワークを経由する場合、メッセージとソフトウェアが伝送されるネットワークは同じであっても異なっていてもよい。

【実施例１】

【００６９】

図３を参照して実施例１のソフトウェア利用許可システム３００について説明する。ソフトウェア利用許可システム３００は、ソフトウェア利用プラットフォーム３１０、ソフトウェア配信サーバ３２０、３３０、及びこれらを接続するネットワーク３４０からなる。ソフトウェア利用プラットフォーム３１０は、メッセージ３５０及び３６０を動作プロセス中に作成し、ネットワーク３４０を介して、それぞれソフトウェア配信サーバ３２０及び３３０に送信する。これに応答して、ソフトウェア配信サーバ３２０及び３３０は、それぞれソフトウェア３７０及び３８０をソフトウェア利用プラットフォーム３１０に配信する。ソフトウェア３７０はソフトウェア認証プログラム３７１及びソフトウェア本体３７２を内包し、ソフトウェア３８０はソフトウェア認証プログラム３８１及びソフトウェア本体３８２を内包する。また、ソフトウェア３７０及び３８０はそれぞれ提供元を示すデジタル署名が施された上で暗号化されている。

【００７０】

以下、対応関係を明瞭にするため、ソフトウェア配信サーバ３２０、メッセージ３５０、ソフトウェア３７０、ソフトウェア認証プログラム３７１及びソフトウェア本体３７２をそれぞれ、ソフトウェア配信サーバ甲、メッセージ甲、ソフトウェア甲、ソフトウェア認証プログラム甲及びソフトウェア本体甲と呼び、ソフトウェア配信サーバ３３０、メッセージ３６０、ソフトウェア３８０、ソフトウェア認証プログラム３８１及びソフトウェア本体３８２をそれぞれ、ソフトウェア配信サーバ乙、メッセージ乙、ソフトウェア乙、ソフトウェア認証プログラム乙及びソフトウェア本体乙と呼ぶこともある。また、ソフトウェア甲及び乙の提供者をそれぞれソフトウェア提供者甲及び乙と呼ぶ。

【００７１】

ソフトウェア利用プラットフォーム３１０は図１のプラットフォーム２に相当し、メッセージ作成部３１１、メッセージ電子署名部３１２、メッセージ送信部３１３、ソフトウェア受信部３１４、ソフトウェア復号化部３１５、ソフトウェア認証部３１６、ソフトウェア認証機能起動部３１７、ソフトウェア本体機能利用部３１８からなる。これらはネットワーク接続のためのインタフェース装置を備えるパーソナルコンピュータ、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄａｔａ　Ａｓｓｉｓｔａｎｔ）、携帯電話端末等のコンピュータ及びＯＳから実現されるか、更にＯＳ上で動作するプログラムが機能を提供することにより実現される。ソフトウェア利用プラットフォーム３１０のハードウェアは、物理的・電気的

に耐タンパ性を有する。

【００７２】

メッセージ作成部３１１は、ソフトウェア配信サーバ甲及び乙に対して所望のソフトウェア甲及び乙の配信を依頼するメッセージ３５０及び３６０（甲及び乙）を作成する。メッセージ３５０及び３６０は電子情報であり、ネットワーク３４０を介して伝送可能である。

【００７３】

メッセージ３５０は公開暗号鍵３５１及びアドレス情報３５２からなる電子情報である。公開暗号鍵３５１は公開暗号方式の暗号鍵である。アドレス情報３５２はソフトウェア利用プラットフォーム３１０に対してソフトウェア甲を配信する際の配信先を示すアドレス情報であり、ネットワーク３４０上のアドレス情報である。例えばネットワーク３４０がインターネットである場合、アドレス情報３５２はソフトウェア利用プラットフォーム３００のＩＰアドレスとなる。

【００７４】

メッセージ３６０は公開暗号鍵３６１及びアドレス情報３６２からなる電子情報である。公開暗号鍵３６１は公開暗号方式の暗号鍵である。アドレス情報３６２はソフトウェア利用プラットフォーム３１０に対してソフトウェア乙を配信する際の配信先を示すアドレス情報であり、ネットワーク３４０上のアドレス情報である。例えばネットワーク３４０がインターネットである場合、アドレス情報３５２はソフトウェア利用プラットフォーム３１０のＩＰアドレスとなる。

【００７５】

メッセージ電子署名部３１２は、メッセージ３５０及び３６０に対し、ソフトウェア利用プラットフォーム３００またはその利用者によるデジタル署名を施す。デジタル署名とは公開鍵方式を応用した署名方式であり、データの作成者を証明すると共に、データの改竄がなされていないことを保障する技術である。

【００７６】

メッセージ送信部３１３は、メッセージ電子署名部３１２にてデジタル署名済みのメッセージ３５０及び３６０を、ネットワーク３４０を介したデータ通信にて、ソフトウェア配信サーバ甲及び乙に送信する。

【００７７】

ソフトウェア受信部３１４は、ネットワーク３４０を介して、ソフトウェア３７０及び３８０を受信する。

【００７８】

ソフトウェア復号化部３１５は、公開暗号鍵３５１と対になる不図示の秘密復号鍵３５１Ｄを用いて、ソフトウェア配信サーバ３２０が暗号化したソフトウェア３７０を復号化する。また、公開暗号鍵３６１と対になる不図示の秘密復号鍵３６１Ｄを用いて、ソフトウェア配信サーバ３２０が暗号化したソフトウェア３８０を復号化する。

【００７９】

ソフトウェア認証部３１６は、施されたデジタル署名に基づいて、ソフトウェア甲及び乙の提供元を特定すると共に、ソフトウェア甲及び乙が改竄されていないことを確認する。これにより、ソフトウェア認証部３１６はソフトウェア甲及び乙の信頼性を確認する。

【００８０】

ソフトウェア認証機能起動部３１７は、ソフトウェア認証プログラム３７１、即ちソフトウェア認証プログラム甲を起動する。ソフトウェア認証プログラム甲は、ソフトウェア３８０、即ちソフトウェア乙を表すバイナリーコードの一部乃至全体を入力とする処理であり、その出力に応じてソフトウェア乙の信頼性を確認する。同様に、ソフトウェア認証機能起動部３１７は、ソフトウェア認証プログラム３８１、即ちソフトウェア認証プログラム乙を起動する。ソフトウェア認証プログラム乙は、ソフトウェア３７０、即ちソフトウェア甲を表すバイナリーコードの一部乃至全体を入力とする処理であり、その出力に応じてソフトウェア甲の信頼性を確認する。

【００８１】
ソフトウェア本体機能利用部３１８は、ソフトウェア甲及び乙を組み合わせて利用する。ソフトウェアを組み合わせて利用することについては図２を参照して既に説明したのでここでは説明を省略する。
【００８２】
ソフトウェア配信サーバ３２０は図１の情報処理装置５に相当し、メッセージ受信部３２１、ソフトウェア利用プラットフォーム認証部３２２、ソフトウェア電子署名部３２３、ソフトウェア暗号化部３２４、ソフトウェア送信部３２５、及び、組み合わせ信頼性判定部３２６からなる。ソフトウェア配信サーバ３２０はネットワーク接続のためのインタフェース装置を備え、ネットワーク３４０に接続されたコンピュータ、コンピュータ上で実行されるＯＳ、ＯＳ上で実行される各種のプログラムにより実現される。ソフトウェア配信サーバ３２０はセキュリティが保たれた場所に設置されることが望ましい。
【００８３】
メッセージ受信部３２１は、メッセージ送信部３１３からネットワーク３４０を介してメッセージ３５０を受信する。
【００８４】
ソフトウェア利用プラットフォーム認証部３２２は、メッセージ受信部３２１が受信したメッセージ３５０を受け取り、メッセージ３５０に対してメッセージ電子署名部３１２にて施されたデジタル署名に基づいて、ソフトウェア利用プラットフォーム３００またはその利用者を認証すると共に、メッセージ３５０が改竄されていないことを確認する。これにより、ソフトウェア利用プラットフォーム３００の信頼性を確認する。
【００８５】
ソフトウェア電子署名部３２３はソフトウェア甲に対して公開鍵方式を利用したデジタル署名を施す。
【００８６】
ソフトウェア暗号化部３２４は、公開暗号鍵３５１を用いてデジタル署名済みのソフトウェア甲を暗号化する。
【００８７】
ソフトウェア送信部３２５は、デジタル署名を施して暗号化したソフトウェア甲を、アドレス情報３５２に従って、ネットワーク３４０を介してソフトウェア受信部３１４に送信する。
【００８８】
組み合わせ信頼性判定部３２６は、ソフトウェア本体甲と組み合わせて利用されようとしているソフトウェアの信頼の可否を判定する。
【００８９】
ソフトウェア配信サーバ３３０は図１の情報処理装置６に相当し、メッセージ受信部３３１、ソフトウェア利用プラットフォーム認証部３３２、ソフトウェア電子署名部３３３、ソフトウェア暗号化部３３４、ソフトウェア送信部３３５、及び、組み合わせ信頼性判定部３３６からなる。ソフトウェア配信サーバ３３０はネットワーク接続のためのインタフェース装置を備え、ネットワーク３４０に接続されたコンピュータ、コンピュータ上で実行されるＯＳ、ＯＳ上で実行される各種のプログラムにより実現される。ソフトウェア配信サーバ３３０はセキュリティが保たれた場所に設置されることが望ましい。
【００９０】
メッセージ受信部３３１は、メッセージ送信部３１３からネットワーク３４０を介してメッセージ３６０を受信する。
【００９１】
ソフトウェア利用プラットフォーム認証部３３２は、メッセージ受信部３３１が受信したメッセージ３６０を受け取り、メッセージ３６０に対してメッセージ電子署名部３１２にて施されたデジタル署名に基づいて、ソフトウェア利用プラットフォーム３００またはその利用者を認証すると共に、メッセージ３６０が改竄されていないことを確認する。こ

れにより、ソフトウェア利用プラットフォーム３００の信頼性を確認する。

【００９２】

ソフトウェア電子署名部３３３はソフトウェア乙に対してデジタル署名を施す。

【００９３】

ソフトウェア暗号化部３３４は、公開暗号鍵３６１を用いてデジタル署名済みのソフトウェア乙を暗号化する。

【００９４】

ソフトウェア送信部３３５は、デジタル署名を施して暗号化したソフトウェア乙を、アドレス情報３６２に従って、ネットワーク３４０を介してソフトウェア受信部３１４に送信する。

【００９５】

組み合わせ信頼性判定部３３６は、ソフトウェア本体甲と組み合わせて利用されようとしているソフトウェアの信頼の可否を判定する。

【００９６】

ネットワーク３４０はデータ通信可能な情報通信網であり、インターネット、ＬＡＮ（ｌｏｃａｌ　ａｒｅａ　ｎｅｔｗｏｒｋ）、公衆電話回線網、移動通信回線網等、或いはこれらを組み合わせたネットワークである。

【００９７】

ソフトウェア３７０、即ちソフトウェア甲は、ソフトウェア認証プログラム３７１及びソフトウェア本体３７２からなる。ソフトウェア認証プログラム３７１はソフトウェア認証機能起動部３１７にて起動され、実行されるコンピュータプログラムであり、ソフトウェア認証プログラム３７１は、ソフトウェア３８０、即ちソフトウェア乙を表すバイナリーコードの一部乃至全体を入力とする処理であり、その出力に応じてソフトウェア乙の信頼性を確認する。

【００９８】

同様に、ソフトウェア３８０、即ちソフトウェア乙は、ソフトウェア認証プログラム３８１及びソフトウェア本体３８２からなる。ソフトウェア認証プログラム３８１はソフトウェア認証機能起動部３１７にて起動され、実行されるコンピュータプログラムであり、ソフトウェア認証プログラム３８１は、ソフトウェア３７０、即ちソフトウェア甲を表すバイナリーコードの一部乃至全体を入力とする処理であり、その出力に応じてソフトウェア甲の信頼性を確認する。

【００９９】

続いて、異なるソフトウェア提供者甲及び乙がそれぞれ提供するソフトウェア本体３７２（甲）及びソフトウェア本体３８２（乙）を、ソフトウェア利用プラットフォーム３１０上にて組み合わせて利用することを許可する際の、ソフトウェア利用許可システム３００の動作について説明する。

【０１００】

予め、ソフトウェア利用プラットフォーム３１０、ソフトウェア配信サーバ３２０（甲）、及び、ソフトウェア配信サーバ３３０（乙）には、ネットワーク３４０上にてユニークなネットワークアドレスが割り当てられているものとする。

【０１０１】

ソフトウェア利用プラットフォーム３１０が、ソフトウェア配信サーバ甲に対して、ソフトウェア３５０（甲）の配信を要求し、配信を受けるまでの過程について図４を参照して以下に説明する。

【０１０２】

ソフトウェア利用プラットフォーム３１０にて、メッセージ作成部３１１が、公開暗号鍵３５１（甲）及びアドレス情報３５２（甲）を含む電子情報であるメッセージ３５０（甲）を作成する（ステップＳ４１）。公開暗号鍵３５１と共に生成される秘密復号鍵３５１Ｄはソフトウェア復号化部３１５に渡される。

【０１０３】

作成されたメッセージ甲はメッセージ電子署名部３１２に渡され、ここでデジタル署名を施される（ステップＳ４２）。

【０１０４】

デジタル署名済みのメッセージ甲は、メッセージ送信部３１３からネットワーク３４０を介してソフトウェア配信サーバ甲のメッセージ受信部３２１（甲）に送信される（ステップＳ４３）。

【０１０５】

メッセージ受信部甲にて受信されたデジタル署名済みメッセージ甲（ステップＳ４４）はソフトウェア利用プラットフォーム認証部３２２（甲）に渡される。ソフトウェア利用プラットフォーム認証部甲は、メッセージ甲に施されたデジタル署名に基づいて、送信元であるソフトウェア利用プラットフォーム３１０の信頼の可否を判定する（ステップＳ４５）。

【０１０６】

ここで信頼できないと判定した場合、ソフトウェア配信サーバ甲はソフトウェア甲の送信を行わない。代わりに他の応答メッセージをソフトウェア利用プラットフォーム３１０に対して送信することとしてもよい。または、ソフトウェア本体甲の代わりに、ソフトウェア本体甲の機能を制限したバージョンを含むソフトウェア甲をソフトウェア利用プラットフォーム３１０に送信することとしてもよい。

【０１０７】

ソフトウェア利用プラットフォーム３１０が信頼可能であると判定された場合、ソフトウェア配信サーバ甲はソフトウェア甲を配信するための準備を開始する。

【０１０８】

まず、ソフトウェア配信サーバ甲の不図示の外部記憶装置、例えば固定磁気ディスク装置等には、ソフトウェア認証プログラム３７１（甲）及びソフトウェア本体３７２（甲）からなるソフトウェア甲が予め格納されている。ソフトウェア電子署名部３２３（甲）は、この外部記憶装置からソフトウェア甲をコピーして、これに対し、ソフトウェア提供者甲またはソフトウェア配信サーバ甲を示すデジタル署名を施す（ステップＳ４６）。

【０１０９】

次に、ソフトウェア暗号化部３２４（甲）は、ステップＳ４４にて受信したメッセージ甲に含まれていた公開暗号鍵３５１を用いて、デジタル署名済みのソフトウェア甲を暗号化する（ステップＳ４７）。

【０１１０】

そして、ソフトウェア送信部３２５は、デジタル署名済みかつ暗号化したソフトウェア甲を、ネットワーク３４０を介してソフトウェア利用プラットフォーム３１０に送信する（ステップＳ４８）。

【０１１１】

ソフトウェア受信部３１４にてソフトウェア甲を受信したソフトウェア利用プラットフォーム３１０（ステップＳ４９）は、ソフトウェア復号化部３１５にてソフトウェア甲を復号する（ステップＳ５０）。復号の際に用いる秘密復号鍵は、ステップＳ４１にて生成された公開暗号鍵３５１と対になって生成された秘密復号鍵３５１Ｄである。

【０１１２】

ソフトウェア利用プラットフォーム３１０が、ソフトウェア配信サーバ乙に対して、ソフトウェア３６０（乙）の配信を要求し、配信を受けるまでの過程について図５を参照して以下に説明する。甲乙が逆転するのみで基本的には同じ動作である。

【０１１３】

ソフトウェア利用プラットフォーム３１０にて、メッセージ作成部３１１が、公開暗号鍵３６１（乙）及びアドレス情報３６２（乙）を含む電子情報であるメッセージ３６０（乙）を作成する（ステップＳ５１）。公開暗号鍵３６１と共に生成される秘密復号鍵３６１Ｄはソフトウェア復号化部３１５に渡される。

【０１１４】

作成されたメッセージ乙はメッセージ電子署名部３１２に渡され、ここでデジタル署名を施される（ステップＳ５２）。

【０１１５】

デジタル署名済みのメッセージ乙は、メッセージ送信部３１３からネットワーク３４０を介してソフトウェア配信サーバ乙のメッセージ受信部３３１（乙）に送信される（ステップＳ５３）。

【０１１６】

メッセージ受信部乙にて受信されたデジタル署名済みメッセージ乙（ステップＳ５４）はソフトウェア利用プラットフォーム認証部３３２（乙）に渡される。ソフトウェア利用プラットフォーム認証部乙は、メッセージ乙に施されたデジタル署名に基づいて、送信元であるソフトウェア利用プラットフォーム３１０の信頼の可否を判定する（ステップＳ５５）。

【０１１７】

ここで信頼できないと判定した場合、ソフトウェア配信サーバ乙はソフトウェア乙の送信を行わない。代わりに他の応答メッセージをソフトウェア利用プラットフォーム３１０に対して送信することとしてもよい。または、ソフトウェア本体乙の代わりに、ソフトウェア本体乙の機能を制限したバージョンを含むソフトウェア乙をソフトウェア利用プラットフォーム３１０に送信することとしてもよい。

【０１１８】

ソフトウェア利用プラットフォーム３１０が信頼可能であると判定された場合、ソフトウェア配信サーバ乙はソフトウェア乙を配信するための準備を開始する。

【０１１９】

まず、ソフトウェア配信サーバ乙の不図示の外部記憶装置、例えば固定磁気ディスク装置等には、ソフトウェア認証プログラム３８１（乙）及びソフトウェア本体３８２（乙）からなるソフトウェア乙が予め格納されている。ソフトウェア電子署名部３３３（乙）は、この外部記憶装置からソフトウェア乙をコピーして、これに対し、ソフトウェア提供者乙またはソフトウェア配信サーバ乙を示すデジタル署名を施す（ステップＳ５６）。

【０１２０】

次に、ソフトウェア暗号化部３３４（乙）は、ステップＳ５４にて受信したメッセージ乙に含まれていた公開暗号鍵３５１を用いて、デジタル署名済みのソフトウェア乙を暗号化する（ステップＳ５７）。

【０１２１】

そして、ソフトウェア送信部３３５は、デジタル署名済みかつ暗号化したソフトウェア乙を、ネットワーク３４０を介してソフトウェア利用プラットフォーム３１０に送信する（ステップＳ５８）。

【０１２２】

ソフトウェア受信部３１４にてソフトウェア乙を受信したソフトウェア利用プラットフォーム３１０（ステップＳ５９）は、ソフトウェア復号化部３１５にてソフトウェア乙を復号する（ステップＳ６０）。復号の際に用いる秘密復号鍵は、ステップＳ５１にて生成された公開暗号鍵３６１と対になって生成された秘密復号鍵３６１Ｄである。

【０１２３】

最後に、ソフトウェア甲及び乙を受信したソフトウェア利用プラットフォーム３１０にて、ソフトウェア本体甲及び乙を組み合わせて利用することを認証する過程について図６を参照して以下に説明する。

【０１２４】

ソフトウェア甲及び乙を受信して復号化したソフトウェア利用プラットフォーム３１０は、ソフトウェア認証部３１６にて、ソフトウェア甲及び乙に施されたデジタル署名に基づいてそれぞれのソフトウェアの信頼性を確認する（ステップＳ６１、６２）。

【０１２５】

この段階で信頼性が確認できないソフトウェアに含まれるソフトウェア本体については

、ソフトウェア利用プラットフォーム３１０は利用に制限を課す。そのソフトウェアがプログラムであれば、例えば、実行を許可しない、実行は許可するがそのプログラムによるデータの書き換えを認めない、本発明による信頼性の判定を要求しないソフトウェアと組み合わせる場合や或いは単体での実行であれば制限なく利用できるが本発明による信頼性の判定を要求するソフトウェアと組み合わせて実行することは禁じる等の制限が考えられる。また、そのソフトウェアがデータであれば、例えば、一切のアクセスを禁じる、読み込みのみ許可して書き換えや消去を禁じる等の制限が考えられる。

【０１２６】

ソフトウェア甲及び乙の両方の信頼性が確認された場合、ソフトウェア認証機能起動部３１７は、ソフトウェア利用プラットフォーム３１０上にてソフトウェア認証プログラム甲を起動する（ステップＳ６３）。起動されたソフトウェア認証プログラム甲に従って、ソフトウェア利用プラットフォーム３１０は、ステップＳ６０にて復号したソフトウェア乙を読み込んで、その一部乃至全部をソフトウェア配信サーバ甲に送信する。ソフトウェア乙の一部を読み込む場合、例えば、ソフトウェア本体乙だけを送信することや、ソフトウェア乙を構成するバイナリーコードの中から、一乃至複数の範囲のビット列を予め指定し、そのビット列を送信することが考えられる。

【０１２７】

ソフトウェア乙の一部乃至全部を受信したソフトウェア配信サーバ甲において、組み合わせ信頼性判定部３２６は、ソフトウェア乙が、ソフトウェア甲と組み合わせて利用するソフトウェアとして認められるか否かの判定を行う（ステップＳ６４）。

【０１２８】

予め、或いは、ソフトウェア利用プラットフォーム３１０からのソフトウェア乙の受信に応じて、ソフトウェア配信サーバ甲は、ソフトウェア配信サーバ乙とデータ通信を行い、判定の基準となるソフトウェア乙の一部乃至全部を受信しておく。ここで判定基準となるソフトウェア乙を含むその他のソフトウェアは、ソフトウェア配信サーバ甲がアクセス可能なデータベースに予め登録しておき、このデータベースから取得してもよい。

【０１２９】

このようにして得た判定基準となるソフトウェア乙と、ソフトウェア利用プラットフォーム３１０から受信したソフトウェア乙とを比較して、一致した場合、組み合わせ信頼性判定部３２６は、ソフトウェア利用プラットフォーム３１０に対して、ソフトウェア本体乙をソフトウェア本体甲と組み合わせて利用することを許可することを示す信号を送信する。この許可は、ソフトウェア提供者甲が、ソフトウェア本体甲の組み合わせ利用の対象として、ソフトウェア本体乙を認めたことを意味する。他方、比較結果が不一致の場合、組み合わせ信頼性判定部３２６は、ソフトウェア利用プラットフォーム３１０に対して、不許可を示す信号を送信する。

【０１３０】

許可信号を受信した場合、ソフトウェア認証機能起動部３１７は、ソフトウェア本体乙が、ソフトウェア本体甲の組み合わせ対象として認められたと判定する（ステップＳ６５）。また、不許可信号を受信した場合は認められなかったと判定する。このとき、ステップＳ６１にて信頼性が確認されているのであれば、ソフトウェア利用プラットフォーム３１０は、ソフトウェア本体甲の単体での利用には制限を課さないが、ソフトウェア本体乙と組み合わせての利用には制限を課す。

【０１３１】

ここでソフトウェア利用プラットフォーム３１０が課す制限は、ソフトウェア甲及び乙が共にプログラムの場合、例えば、ソフトウェア利用プラットフォーム３１０上で実行されたソフトウェア甲及び乙の間でのプログラム間の通信のうち、ソフトウェア乙からソフトウェア甲に向けて発信されるものの一部乃至全部を禁止することが考えられる。また、ソフトウェア甲がプログラムでソフトウェア乙がデータの場合、例えば、ソフトウェア甲がソフトウェア乙を開くのを禁止したり、書き換えを禁止することが考えられる。また、ソフトウェア甲がデータでソフトウェア乙がプログラムの場合、例えば、ソフトウェア乙

によるソフトウェア甲の読み込み、書き換え等の一部乃至全部を禁止することが考えられる。

【０１３２】

続いて、ソフトウェア認証機能起動部３１７は、同様の処理をソフトウェア甲及び乙の立場を入れ替えて実行する。即ち、ソフトウェア認証機能起動部３１７は、ソフトウェア利用プラットフォーム３１０上にてソフトウェア認証プログラム乙を起動する（ステップＳ６６）。起動されたソフトウェア認証プログラム乙に従って、ソフトウェア利用プラットフォーム３１０は、ステップＳ５０にて復号したソフトウェア甲を読み込んで、その一部乃至全部をソフトウェア配信サーバ乙に送信する。ソフトウェア甲の一部を読み込む場合、例えば、ソフトウェア本体甲だけを送信することや、ソフトウェア甲を構成するバイナリーコードの中から、一乃至複数の範囲のビット列を予め指定し、そのビット列を送信することが考えられる。

【０１３３】

ソフトウェア甲の一部乃至全部を受信したソフトウェア配信サーバ乙において、組み合わせ信頼性判定部３３６は、ソフトウェア甲が、ソフトウェア乙と組み合わせて利用するソフトウェアとして認められるか否かの判定を行う（ステップＳ６７）。

【０１３４】

予め、或いは、ソフトウェア利用プラットフォーム３１０からのソフトウェア甲の受信に応じて、ソフトウェア配信サーバ乙は、ソフトウェア配信サーバ甲とデータ通信を行い、判定の基準となるソフトウェア甲の一部乃至全部を受信しておく。ここで判定基準となるソフトウェア甲を含むその他のソフトウェアは、ソフトウェア配信サーバ乙がアクセス可能なデータベースに予め登録しておき、このデータベースから取得してもよい。

【０１３５】

このようにして得た判定基準となるソフトウェア甲と、ソフトウェア利用プラットフォーム３１０から受信したソフトウェア甲とを比較して、一致した場合、組み合わせ信頼性判定部３３６は、ソフトウェア利用プラットフォーム３１０に対して、ソフトウェア本体甲をソフトウェア本体乙と組み合わせて利用することを許可することを示す信号を送信する。この許可は、ソフトウェア提供者乙が、ソフトウェア本体乙の組み合わせ利用の対象として、ソフトウェア本体甲を認めたことを意味する。他方、比較結果が不一致の場合、組み合わせ信頼性判定部３３６は、ソフトウェア利用プラットフォーム３１０に対して、不許可を示す信号を送信する。

【０１３６】

許可信号を受信した場合、ソフトウェア認証機能起動部３１７は、ソフトウェア本体甲が、ソフトウェア本体乙の組み合わせ対象として認められたと判定する（ステップＳ６８）。また、不許可信号を受信した場合は認められなかったと判定する。このとき、ステップＳ６２にて信頼性が確認されているのであれば、ソフトウェア利用プラットフォーム３１０は、ソフトウェア本体乙の単体での利用には制限を課さないが、ソフトウェア本体甲と組み合わせての利用には制限を課す。制限の内容についてはステップＳ６５に関連して説明したものと同様であり、説明を省略する。

【０１３７】

このようにして、ソフトウェア認証機能起動部３１７がソフトウェア本体甲及び乙の信頼の可否を判定した後、ソフトウェア本体機能利用部３１８は、その判定結果に従ってソフトウェア本体甲及び乙を利用する（ステップＳ６９）。ステップＳ６５及びＳ６８の両方で許可信号を受信しているのであれば、ソフトウェア本体機能利用部３１８は、ソフトウェア甲及び乙を組み合わせて利用することに制限を課さない。ステップＳ６５及びＳ６８のいずれか一方、または両方で不許可信号を受信した場合、ソフトウェア本体機能利用部３１８は、ソフトウェア甲及び乙を組み合わせて利用することに対し、前述の制限を課す。

【０１３８】

次に、ソフトウェア利用許可システム３００の効果について説明する。

【０１３９】
ソフトウェア配信サーバ甲及び乙は、メッセージ甲及び乙に施されたデジタル署名に基づいてソフトウェア利用プラットフォーム３１０を認証し、認証に成功した場合に限り、ソフトウェア甲及び乙を配信している。このため、ソフトウェア利用プラットフォーム３１０になりすました他のコンピュータにソフトウェア本体甲及び乙を配信することを防止することができる。
【０１４０】
尚、デジタル署名による認証と共に、そのデジタル署名で識別されるユーザが、ソフトウェア甲及び乙の正規ユーザとして登録された者であるか否かを、予め正規ユーザを登録したデータベースに問い合わせて確認し、正規ユーザと確認できた場合に限り、ソフトウェア甲及び乙を送信することとしてもよい。こうすれば、不正なユーザによる利用をこの段階で排除することができる。
【０１４１】
また、ソフトウェア甲及び乙は、公開暗号方式により暗号化をされてソフトウェア配信サーバ甲及び乙からソフトウェア利用プラットフォーム３１０に送信される。このため、ネットワーク３４０の伝送過程における改竄があっても、ソフトウェア利用プラットフォーム３１０は改竄を検出することができる。また、ソフトウェア利用プラットフォーム３１０以外のコンピュータでソフトウェア甲及び乙が利用されるのを防止することができる。
【０１４２】
更に、ソフトウェア本体甲の利用に先立って、ソフトウェア認証プログラム甲が実行されて、ソフトウェア本体乙が、ソフトウェア本体甲の組み合わせ相手として認められるか否かを判定する。この判定処理はソフトウェア配信サーバ甲にて実行されるため、ソフトウェア利用プラットフォーム３１０にて判定処理をスキップされるのを防止することができる。ソフトウェア本体乙についても同様である。
【０１４３】
上述の実施例１では、２つのソフトウェア本体甲及び乙を組み合わせる場合に適用することを前提として説明したが、３つ以上のソフトウェアを組み合わせる場合に適用することも可能であることは、当業者には明らかだろう。
【０１４４】
実施例１では、２つのソフトウェア本体甲及び乙に対応して、２つのソフトウェア配信サーバ甲及び乙が、ソフトウェア利用プラットフォーム３１０に対して、それぞれステップＳ４１～Ｓ５０及びステップＳ５１～Ｓ６０によりソフトウェア本体甲及び乙を配信する。この後、ソフトウェア認証プログラム甲及び乙に従って、ソフトウェア利用プラットフォーム３１０が、組み合わせ対象となるソフトウェア本体の信頼性を判定するための処理を行い、どちらのソフトウェア本体の視点（即ち、ソフトウェア提供者の視点）からも相手ソフトウェアが信頼できる場合に限り、２つのソフトウェア本体甲及び乙を組み合わせて利用することを許可する。
【０１４５】
同様に、３つ以上のソフトウェアを組み合わせる場合は、組み合わせるソフトウェアと同数のソフトウェア配信サーバを用意して、それぞれのソフトウェア配信サーバとソフトウェア利用プラットフォームとの間でステップＳ４１～Ｓ５０と同様の処理を行う。また、各ソフトウェアのソフトウェア認証プログラムは、そのソフトウェア本体と組み合わされる他の全てのソフトウェア本体の信頼性を判定するための処理を行う。どのソフトウェア本体の視点から見ても他の全てのソフトウェア本体が信頼できる場合に限り、これらソフトウェア本体を組み合わせて利用することを許可する。
【０１４６】
また、実施例１では、ソフトウェア提供者甲及び乙がそれぞれ一種類のソフトウェア甲及び乙のみを提供しているとの前提で説明したが、それぞれが複数種類のソフトウェアを提供することとしてもよい。その場合、メッセージ甲及び乙には更にソフトウェア種別を

指定する情報が含まれることとなる。

【０１４７】

また、実施例１では、ソフトウェア送信部３２５、３３５、ネットワーク３４０、及びソフトウェア受信部３１４の経路にて、ソフトウェア３７０及び３８０を配信したが、他の配信経路であってもよい。例えば、ＣＤ－ＲＯＭ等の取り外し可能で書き換え不可能な記録媒体に書き込み、この記録媒体をこの記録媒体をソフトウェア利用プラットフォーム３００に読み込ませることにより、ソフトウェア利用プラットフォーム３００にソフトウェア３７０及び３８０を配信することとしてもよい。この場合、アドレス情報３５２及び３６２は、ソフトウェア利用プラットフォーム３１０の現実の所在地を示す都道府県・市町村・番地等となる。

【実施例２】

【０１４８】

次に本発明の実施例２のソフトウェア利用許可システム７００について図７を参照して説明する。ソフトウェア利用許可システム７００は、ＩＣカード利用端末７１０、ＩＣカード７２０、キオスク端末７３０、及びキオスク端末７４０からなる。キオスク端末７３０は、ソフトウェア提供者甲が提供するソフトウェア７５０を配布し、キオスク端末７４０はソフトウェア提供者乙が提供するソフトウェア７６０を配布する。以下、キオスク端末７３０及び７４０をそれぞれキオスク端末甲及び乙と呼ぶこともある。また、ソフトウェア７５０及び７６０をそれぞれソフトウェア甲及び乙と呼ぶこともある。ＩＣカード利用端末７１０、キオスク端末７３０及び７４０は、インターネット等の不図示のデータ通信ネットワークを介して互いにデータ通信可能な端末装置である。

【０１４９】

ＩＣカード利用端末７１０は、図１に示したプラットフォーム２に相当する装置であり、キーボード、マウス等の入力装置、ＩＣカードリーダライタ、インターネット等のデータ通信ネットワークに接続するためのネットワークインタフェース装置、固定磁気ディスク装置等の外部記憶装置を備えるコンピュータと、コンピュータ上で動作するＯＳ、プログラム等により実現される装置である。ＩＣカード利用端末７１０は、ＩＣカード挿抜部７１１、メッセージ作成部７１２、メッセージ書込部７１３、ソフトウェア利用開始部７１４、ソフトウェア入力データ書込部７１５、及び、ソフトウェア出力データ読出部７１６からなる。

【０１５０】

ＩＣカード挿抜部７１１は、ＩＣカードリーダライタにＩＣカード７２０が装着されると、これを検出してＩＣカード利用端末７１０がＩＣカード７２０を読み書きできる状態にする。

【０１５１】

メッセージ作成部７１２は、ＩＣカード利用端末７１０にて利用しようとするソフトウェアを指定して、そのソフトウェアをＩＣカード７２０に書き込むことを、そのソフトウェアを配布するキオスク端末に対して要求するメッセージを電子情報として作成する。

【０１５２】

メッセージ書込部７１３は、メッセージ作成部７１２にて作成したメッセージを、ＩＣカードリーダライタを用いてＩＣカード７２０のメモリに書き込む。

【０１５３】

ソフトウェア利用開始部７１４は、ＩＣカード７２０に書き込まれているソフトウェアを利用する際に、これをＩＣカード７２０に通知する。

【０１５４】

ソフトウェア入力データ書込部７１５は、ＩＣカード７２０に書き込まれているソフトウェアを利用する際に、入力するデータをＩＣカード７２０に書き込む。

【０１５５】

ソフトウェア出力データ読出部７１６は、ＩＣカード７２０に書き込まれているソフトウェアを利用する際に、ソフトウェアから出力されるデータをＩＣカード７２０から読み

出す。

【０１５６】

ＩＣカード７２０は、プラットフォーム２の一部を構成すると共に、情報処理装置５及び６とプラットフォーム２との間におけるソフトウェアの媒体としての役割を有する。ＩＣカード７２０は、ＭＰＵ（Ｍｉｃｒｏ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）と、ＭＰＵの動作を制御するためのＯＳを格納するＲＯＭと、ＭＰＵを介してアクセスされるＲＡＭを少なくとも備える所謂スマートカードにより実現される装置であり、メッセージ記憶部７２１、キオスク端末認証部７２２、ソフトウェア記憶部７２３、ソフトウェア認証部７２４、ソフトウェア認証機能起動部７２５、ソフトウェア本体機能利用部７２６、ソフトウェア入力データ記憶部７２７、及びソフトウェア出力データ記憶部７２８からなる。

【０１５７】

メッセージ記憶部７２１は、メッセージ書込部７１３によって書き込まれるメッセージを保持する。

【０１５８】

キオスク端末認証部７２２は、ＩＣカード７２０がキオスク端末甲或いは乙に装着されたときに、キオスク端末が正当なものであるか否かを判定し、判定結果に応じてキオスク端末によるＩＣカード７２０への読み書きを許可或いは禁止する。認証は例えば３パス相互認証方式（ＩＳＯ／ＩＥＣ９７９８－３）により行われる。

【０１５９】

ソフトウェア記憶部７２３は、キオスク端末甲及び乙が書き込んだソフトウェア甲及び乙を保持する。尚、ソフトウェア記憶部７２３は、ＩＣカード利用端末７１０を含む他の端末によって読み出すことができないように構成されている。即ち、ソフトウェア記憶部７２３は耐タンパ性を有するものとする。

【０１６０】

ソフトウェア認証部７２４は、ソフトウェア甲及び乙に施されたデジタル署名に基づいてソフトウェア提供者甲及び乙を特定すると共に、ソフトウェア甲及び乙が改竄されていないことを確認する。これにより、ソフトウェア甲及び乙の信頼の可否を判定する。

【０１６１】

ソフトウェア認証機能起動部７２５は、ソフトウェア甲及び乙にそれぞれ内包されているコンピュータプログラムであるソフトウェア認証プログラム７５１及び７６１（以下それぞれソフトウェア認証プログラム甲及び乙と呼ぶこともある）を起動して、ＩＣカード７２０のＭＰＵに実行させる。また、起動後のソフトウェア認証プログラム甲に対してソフトウェア乙を入力して応答を受け取る。同様に、起動後のソフトウェア認証プログラム乙に対してソフトウェア甲を入力して応答を受け取る。

【０１６２】

ソフトウェア本体機能利用部７２６は、ソフトウェア甲及び乙にそれぞれ内包されているソフトウェア本体７５２及び７６２（以下それぞれソフトウェア本体甲及び乙と呼ぶこともある）を組み合わせて利用する。

【０１６３】

ソフトウェア入力データ記憶部７２７は、ソフトウェア本体機能利用部７２６上にて組み合わせて利用されているソフトウェア本体７５２及び７６２に対し、入力するデータを保持する。

【０１６４】

ソフトウェア出力データ記憶部７２８は、ソフトウェア本体機能利用部７２６上にて組み合わせて利用されているソフトウェア本体７５２及び７６２が、出力したデータを保持する。

【０１６５】

キオスク端末７３０は、ＩＣカード挿抜部７３１、ＩＣカード認証部７３２、メッセージ読込部７３３、ソフトウェア保持部７３４、ソフトウェア電子署名部７３５、ソフトウェア書込部７３６、及び、ソフトウェア信頼性判定部７３７からなる。以下、参照符号７

３０～７３７の代わりに甲を用いることもある。キオスク端末甲は、図１に示した情報処理装置甲に相当する装置であり、街頭設置型のキオスク端末であり、耐タンパ性を有するとする。キオスク端末甲は、キーボード、マウス、タッチパネル等の入力装置、ＩＣカードリーダライタ、インターネット等のデータ通信ネットワークに接続するためのネットワークインタフェース装置、固定磁気ディスク装置等の外部記憶装置を備えるコンピュータと、コンピュータ上で動作するＯＳ、プログラム等により実現される装置である。

【０１６６】

ＩＣカード挿抜部７３１は、ＩＣカードリーダライタにＩＣカード７２０が装着されると、これを検出してＩＣカード利用端末７１０がＩＣカード７２０を読み書きできる状態にする。

【０１６７】

ＩＣカード認証部７３２は、ＩＣカード挿抜部７３１にて読み書き可能となったＩＣカード７２０が、ＩＣカード７２０が正当なものであるか否かを判定し、判定結果に応じてＩＣカード７２０への読み書きを許可或いは禁止する。認証は例えば３パス相互認証方式（ＩＳＯ／ＩＥＣ９７９８－３）により行われる。

【０１６８】

メッセージ読込部７３３は、メッセージ記憶部７２１からメッセージを読み出す。

【０１６９】

ソフトウェア保持部７３４は、ソフトウェア甲を保持する。

【０１７０】

ソフトウェア電子署名部７３５は、ソフトウェア保持部７３４から受け取ったソフトウェア甲に対し、公開鍵暗号方式を利用したデジタル署名を施す。

【０１７１】

ソフトウェア書込部７３６は、ソフトウェア電子署名部７３５にてデジタル署名を施されたソフトウェア甲を、ソフトウェア記憶部７２３に書き込む。

【０１７２】

組み合わせ信頼性判定部７３７は、ソフトウェア本体甲と組み合わせて利用されようとしているソフトウェアの信頼の可否を判定する。

【０１７３】

キオスク端末７４０、即ちキオスク端末乙は、ソフトウェア甲とソフトウェア乙の立場を入れ替わるだけで他の点は同じなので説明を省略する。以下、参照符号７４０～７４７の代わりに乙を用いることもあるのも同様である。

【０１７４】

ソフトウェア７５０、即ちソフトウェア甲は、ソフトウェア認証プログラム７５１及びソフトウェア本体７５２からなる。ソフトウェア認証プログラム７５１はソフトウェア認証機能起動部７２５にて起動されて実行されるコンピュータプログラムであり、ソフトウェア認証プログラム７５１は、ソフトウェア７６０、即ちソフトウェア乙を表すバイナリーコードの一部乃至全体を入力とする処理であり、その出力に応じてソフトウェア乙の信頼性を確認する。

【０１７５】

同様に、ソフトウェア７６０、即ちソフトウェア乙は、ソフトウェア認証プログラム７６１及びソフトウェア本体７６２からなる。ソフトウェア認証プログラム７６１はソフトウェア認証機能起動部７２５にて起動さて実行されるコンピュータプログラムであり、ソフトウェア認証プログラム７６１は、ソフトウェア７５０、即ちソフトウェア甲を表すバイナリーコードの一部乃至全体を入力とする処理であり、その出力に応じてソフトウェア甲の信頼性を確認する。

【０１７６】

ソフトウェア利用許可システム７００により、ソフトウェア甲及び乙を組み合わせて利用することを許可する動作を以下に説明する。

【０１７７】

図８を参照して説明する。ＩＣカード７２０の利用者が、ＩＣカード利用端末７１０のＩＣカードリーダライタにＩＣカード７２０を装着すると、ＩＣカード挿抜部７１１がＩＣカード７２０を検出し、検出に応じてＩＣカード７２０をＩＣカード利用端末７１０から読み書き可能な状態にする（ステップＳ８１）。

【０１７８】

次に、ＩＣカード利用端末７１０は、ソフトウェア甲をＩＣカード７２０に書き込むように、キオスク端末７３０に対して依頼するメッセージを、メッセージ作成部７１２にて作成（ステップＳ８２）し、作成したメッセージをメッセージ書込部７１３にてメッセージ記憶部７２１に書き込む（ステップＳ８３、Ｓ８４）。

【０１７９】

同様に、ＩＣカード利用端末７１０は、ソフトウェア乙をＩＣカード７２０に書き込むように、キオスク端末７４０に対して依頼するメッセージを、メッセージ作成部７１２にて作成（ステップＳ８５）し、作成したメッセージをメッセージ書込部７１３にてメッセージ記憶部７２１に書き込む（ステップＳ８６、Ｓ８７）。

【０１８０】

この後、利用者は、メッセージを書き込んだＩＣカード７２０をＩＣカード利用端末７１０から外し、キオスク端末甲の元に持ち運んで、キオスク端末甲のＩＣカードリーダライタに装着する。図９を参照してＩＣカード７２０を装着したキオスク端末甲での処理を説明する。

【０１８１】

ＩＣカード７２０の装着に応じて、ＩＣカード挿抜部７３１は、ＩＣカード７２０を検出し、検出に応じてＩＣカード７２０をキオスク端末甲から読み書き可能な状態にした（ステップＳ９１）後、ＩＣカード７２０とキオスク端末甲とは、相互に相手の信頼性を確認する（ステップＳ９２、Ｓ９３）。少なくとも一方の装置から相手の装置の信頼性が確認できなかった場合、処理は中断される。

【０１８２】

お互いに相手装置の信頼性が確認できた場合、メッセージ読込部７３３は、ステップＳ８４にて保持したメッセージを、メッセージ記憶部７２１から読み出す（ステップＳ９４）。ソフトウェア保持部７３４は、保持しているソフトウェアの中から、読み出したメッセージが指定するソフトウェア甲を検索（ステップＳ９５）し、該当するソフトウェア甲をソフトウェア電子署名部７３５に渡す。

【０１８３】

ソフトウェア甲は、ソフトウェア本体７５２と、ソフトウェア７５２と組み合わせて利用しようとしている他のソフトウェアが、ソフトウェア提供者甲の視点から見て組み合わせて利用してもよいソフトウェアであるか否かを判定するための処理をコンピュータに実行させるソフトウェア認証プログラム７５１とを内包する。

【０１８４】

ソフトウェア甲の受け渡しに応じて、ソフトウェア電子署名部７３５は、ソフトウェア甲に対して公開鍵方式を利用したデジタル署名を施して（ステップＳ９６）ソフトウェア書込部７３６に渡す。これに応じて、ソフトウェア書込部７３６は、ソフトウェア記憶部７２３に、デジタル署名済みのソフトウェア甲を書き込む（ステップＳ９７、Ｓ９８）。

【０１８５】

デジタル署名済みのソフトウェア甲を書き込んだＩＣカード７２０は、キオスク端末甲から外されて、次にキオスク端末乙に装着される。ＩＣカード７２０を装着したキオスク端末乙での処理が図１０に示すようにして行われるが、ここでの処理ステップＳ１００１～Ｓ１００８は、基本的に上述のステップＳ９１～Ｓ９８と同様であるので、ここでは説明を省略する。

【０１８６】

このようにしてデジタル署名済みのソフトウェア甲及び乙が、ソフトウェア記憶部７２３に保持されたＩＣカード７２０を、再びＩＣカード利用端末７１０に装着する。

【０１８７】
即ち、ＩＣカード７２０の利用者が、ＩＣカード利用端末７１０のＩＣカードリーダライタにＩＣカード７２０を装着すると、ＩＣカード挿抜部７１１がＩＣカード７２０を検出し、検出に応じてＩＣカード７２０をＩＣカード利用端末７１０から読み書き可能な状態にする（ステップＳ１１０１）。
【０１８８】
利用者による操作に応じて、または、ＩＣカード利用端末７１０上で動作するＯＳやプログラムの指示に応じて、ソフトウェア甲及び乙を組み合わせて利用しようとすると、ソフトウェア利用開始部７１４は、ＩＣカード７２０に対してその旨を通知する（ステップＳ１１０２）。
【０１８９】
ソフトウェア記憶部７２３に保持されているソフトウェア甲及び乙にはデジタル署名が施されている。ステップＳ１１０２の通知を受けると、このデジタル署名に基づいて、ソフトウェア認証部７２４はキオスク端末甲及び乙の信頼性を確認する（ステップＳ１１０３、Ｓ１１０４）。ここで、少なくとも一方の信頼性が確認できなかった場合、以後の処理は中断される。
【０１９０】
両方の信頼性が確認できた場合、ＩＣカード７２０は、実施例１にて説明したステップＳ６３～Ｓ６８と同様の処理を実行し、ソフトウェア甲とソフトウェア乙の間での信頼性の確認を行う（ステップＳ１１０５～Ｓ１１１０）。このとき、ＩＣカード７２０とキオスク端末甲の間のデータ通信は、ＩＣカード利用端末７１０及び不図示のデータ通信ネットワークを介して実行される。ＩＣカード７２０とキオスク端末乙の間のデータ通信も同様である。ここで、ソフトウェア甲から見たときのソフトウェア乙の信頼性、及び、ソフトウェア乙から見たときのソフトウェア甲の信頼性のうち、少なくとも一方が確認できない場合、以後の処理は中断される（ステップＳ１１１１）。ソフトウェア甲及び乙の間の信頼性が双方向で確認できた場合、ＩＣカード７２０は、ソフトウェア本体甲及び乙を組み合わせて利用することを許可する（ステップＳ１１１２）。
【０１９１】
組み合わせ利用が許可されると、ＩＣカード７２０は、ソフトウェア本体甲及び乙に入力されるべきデータを受け付けるようになる。ＩＣカード利用端末７１０からこうしたデータが入力される（ステップＳ１２０１）と、このデータはソフトウェア入力データ書込部７１５によりソフトウェア入力データ記憶部７２７に保持される（ステップＳ１２０２）。ソフトウェア本体甲及び乙は、このデータが入力されて利用される。また、キオスク端末甲及び乙では、データ通信ネットワークを介して、それぞれソフトウェア本体甲及び乙と連携して動作する処理が実行され（ステップＳ１２０３）、処理結果がソフトウェア本体甲及び乙の出力データとしてソフトウェア出力データ記憶部７２８に保持される（ステップＳ１２０４）。ソフトウェア出力データ記憶部７２８に保持されたデータは適宜ソフトウェア出力データ読出部７１６により読み出され、ＩＣカード利用端末７１０で実行される他の処理に渡されたり、ＩＣカード利用端末７１０の画像表示装置にて表示される。
【０１９２】
次に、ソフトウェア利用許可システム７００の効果について説明する。
【０１９３】
キオスク端末甲及び乙とＩＣカード７２０は、例えば３パス相互認証方式（ＩＳＯ／ＩＥＣ９７９８－３）のような認証方式によって互いを認証し、認証した場合に限り、キオスク端末甲及び乙はＩＣカード７２０にソフトウェア甲及び乙を書き込んでいる。このため、偽造されたＩＣカードにソフトウェア本体甲及び乙を書き込むことを防止することができる。
【０１９４】
尚、デジタル署名の認証と共に、そのデジタル署名で識別されるユーザが、ソフトウェ

ア甲及び乙の正規ユーザとして登録された者であるか否かを、予め正規ユーザを登録したデータベースに問い合わせて確認し、正規ユーザと確認できた場合に限り、ソフトウェア甲及び乙を送信することとしてもよいのは実施例１と同様である。

【０１９５】

また、ソフトウェア本体甲の利用に先立って、ソフトウェア認証プログラム甲が実行されて、ソフトウェア本体乙が、ソフトウェア本体甲の組み合わせ相手として認められるか否かを判定する。この判定処理はキオスク端末甲にて実行されるため、ＩＣカード７２０やＩＣカード利用端末７１０にて判定処理をスキップされるのを防止することができる。ソフトウェア本体乙についても同様である。

【０１９６】

実施例１と同様に、上述の実施例２でも、２つのソフトウェア本体甲及び乙を組み合わせる場合に適用することを前提として説明したが、３つ以上のソフトウェアを組み合わせる場合に適用することも可能であることは、当業者には明らかだろう。

【０１９７】

尚、上述の実施例１及び２では、ソフトウェア認証プログラム３７１、３８１、７５１、７６１はいずれも、情報処理装置甲及び乙に相当する装置である、ソフトウェア配信サーバ甲及び乙、または、キオスク端末甲及び乙と通信を行い、これら装置で行われた判定結果に基づいて、組み合わせ対象となるソフトウェア本体甲及び乙の信頼の可否を判定した。つまり、判定処理は情報処理装置甲及び乙上で実行されていた。

【０１９８】

しかし、本発明はこれに限定されるものではなく、例えば、組み合わせ対象となるソフトウェアに施されたデジタル署名に基づいて、プラットフォーム２上で判定処理を実行することとしてもよい。この場合、実施例１であれば、組み合わせ信頼性判定部３２６、３３６で行われていた判定処理はソフトウェア認証機能起動部３１７にて実行され、組み合わせ信頼性判定部３２６、３３６は不要となる。同様に、実施例２であれば、組み合わせ信頼性判定部７３７、７４７で行われていた判定処理はソフトウェア認証機能起動部７２５にて実行され、組み合わせ信頼性判定部７３７、７４７は不要となる。

【０１９９】

以上、本発明を実施の形態及び実施例に基づいて説明したが、本発明はこれに限定されるものではなく、当業者の通常の知識の範囲内でその変更や改良が可能であることは勿論である。

【図面の簡単な説明】

【０２００】

【図１】本発明の実施の形態であるソフトウェア利用許可システム１の機能ブロック図である。

【図２】本発明におけるプラットフォームの種類、及び、組み合わせて利用するソフトウェアの種類について説明するための図である。

【図３】本発明の実施例１であるソフトウェア利用許可システム３００の機能ブロック図である。

【図４】ソフトウェア利用許可システム３００の動作を説明するためのフローチャートである。

【図５】ソフトウェア利用許可システム３００の動作を説明するためのフローチャートである。

【図６】ソフトウェア利用許可システム３００の動作を説明するためのフローチャートである。

【図７】ソフトウェア利用許可システム３００の動作を説明するためのフローチャートである。

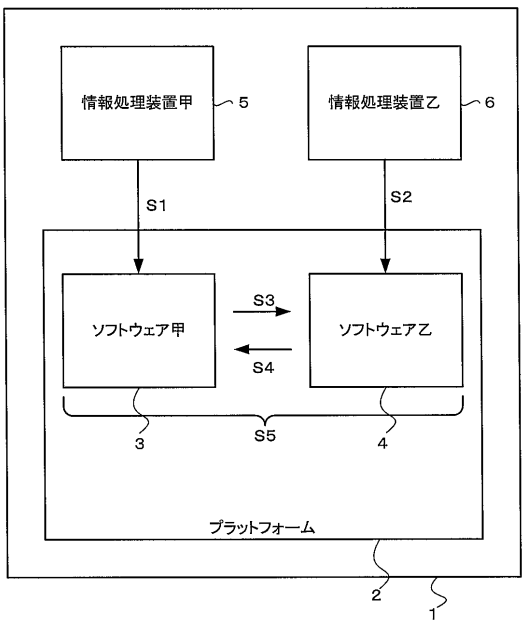
【図８】本発明の実施例２であるソフトウェア利用許可システム７００の機能ブロック図である。

【図９】ソフトウェア利用許可システム７００の動作を説明するためのフローチャートで

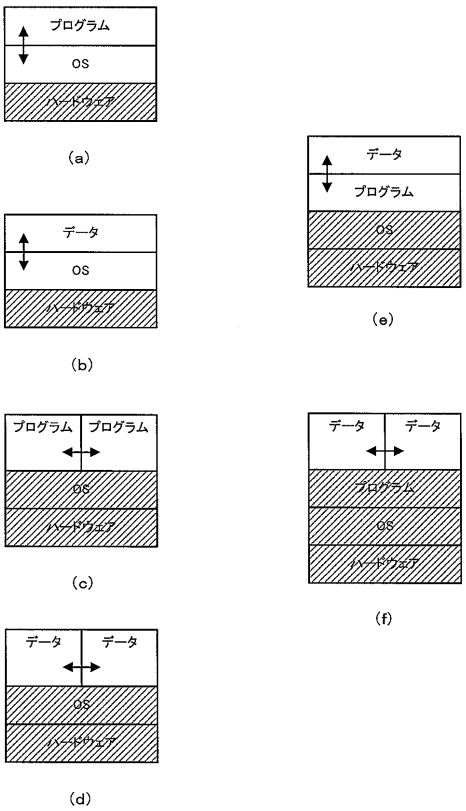
ある。
【図１０】ソフトウェア利用許可システム７００の動作を説明するためのフローチャートである。
【図１１】ソフトウェア利用許可システム７００の動作を説明するためのフローチャートである。
【図１２】ソフトウェア利用許可システム７００の動作を説明するためのフローチャートである。
【符号の説明】
【０２０１】
１、３００、７００　ソフトウェア利用許可システム
２　プラットフォーム
３　ソフトウェア甲
４　ソフトウェア乙
５　情報処理装置甲
６　情報処理装置乙
３１０　ソフトウェア利用プラットフォーム
３１１　メッセージ作成部
３１２　メッセージ電子署名部
３１３　メッセージ送信部
３１４　ソフトウェア受信部
３１５　ソフトウェア復号化部
３１６　ソフトウェア認証部
３１７　ソフトウェア認証機能起動部
３１８　ソフトウェア本体機能利用部
３２０、３３０　ソフトウェア配信サーバ
３２１、３３１　メッセージ受信部
３２２、３３２　ソフトウェア利用プラットフォーム認証部
３２３、３３３　ソフトウェア電子署名部
３２４、３３４　ソフトウェア暗号化部
３２５、３３５　ソフトウェア送信部
３２６、３３６、７３７、７４７　組み合わせ信頼性判定部
３４０　ネットワーク
３５０、３６０　メッセージ
３５１、３６１　公開暗号鍵
３５２、３６２　アドレス情報
３７０、３８０、７５０、７６０　ソフトウェア
３７１、３８１、７５１、７６１　ソフトウェア認証プログラム
３７２、３８２、７５２、７６２　ソフトウェア本体
７１０　ＩＣカード利用端末
７１１、７３１、７４１　ＩＣカード挿抜部
７１２　メッセージ作成部
７１３　メッセージ書込部
７１４　ソフトウェア利用開始部
７１５　ソフトウェア入力データ書込部
７１６　ソフトウェア出力データ読出部
７２０　ＩＣカード
７２１　メッセージ記憶部
７２２　キオスク端末認証部
７２３　ソフトウェア記憶部
７２４　ソフトウェア認証部

７２５　　ソフトウェア認証機能起動部
７２６　　ソフトウェア本体機能利用部
７２７　　ソフトウェア入力データ記憶部
７２８　　ソフトウェア出力データ記憶部
７３０、７４０　　キオスク端末
７３２、７４２　　ＩＣカード認証部
７３３、７４３　　メッセージ読込部
７３４、７４４　　ソフトウェア保持部
７３５、７４５　　ソフトウェア電子署名部
７３６、７４６　　ソフトウェア書込部

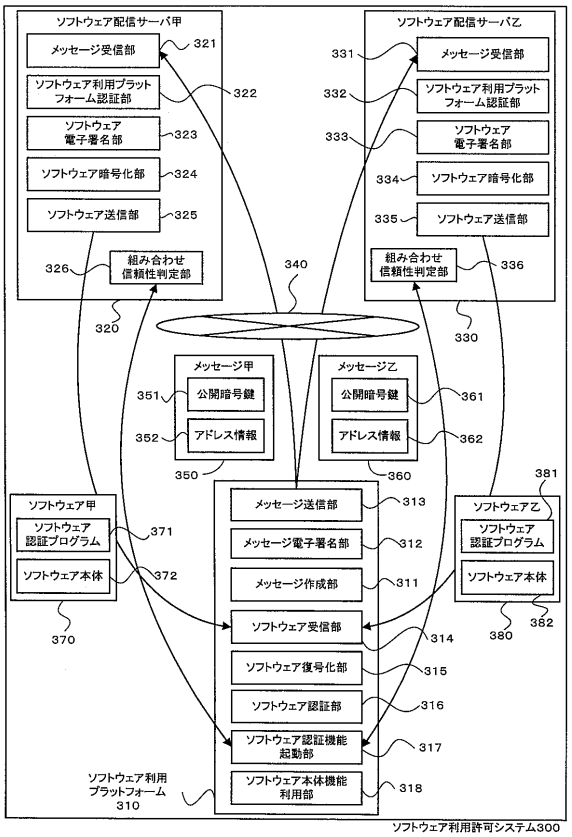
【図１】



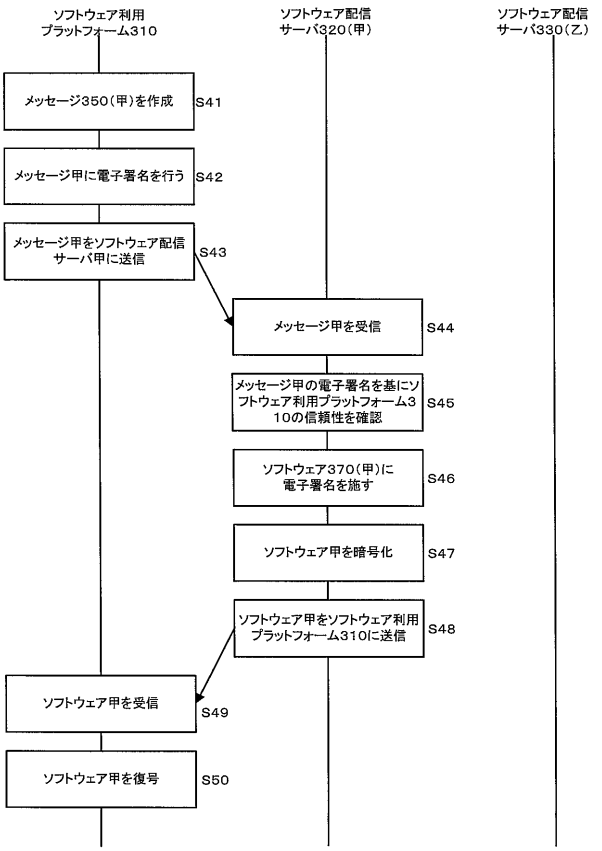
【図２】



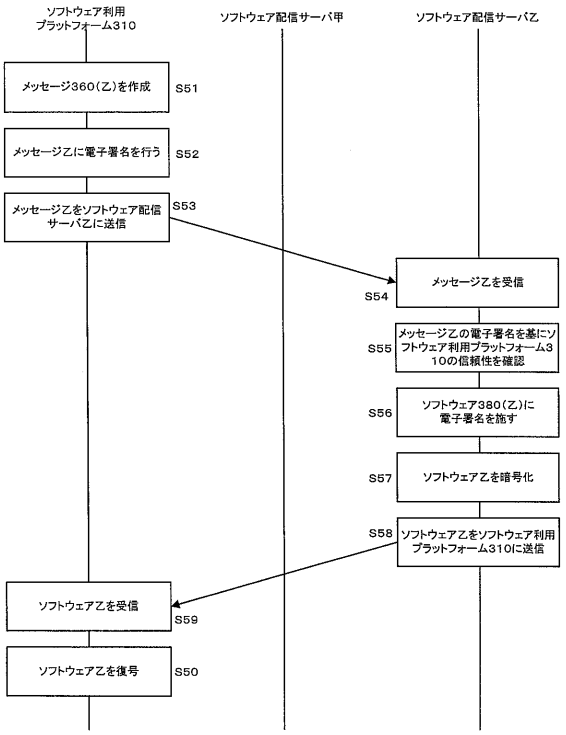
【図３】


ソフトウェア配信サーバ甲
メッセージ受信部
321
ソフトウェア利用プラットフォーム認証部
322
ソフトウェア電子署名部
323
ソフトウェア暗号化部
324
ソフトウェア送信部
325
326
組み合わせ信頼性判定部
320
ソフトウェア配信サーバ乙
331
メッセージ受信部
332
ソフトウェア利用プラットフォーム認証部
333
ソフトウェア電子署名部
334
ソフトウェア暗号化部
335
ソフトウェア送信部
336
組み合わせ信頼性判定部
330
340
メッセージ甲
351
公開暗号鍵
352
アドレス情報
350
メッセージ乙
361
公開暗号鍵
362
アドレス情報
360
ソフトウェア甲
ソフトウェア認証プログラム
371
ソフトウェア本体
372
370
381
ソフトウェア乙
ソフトウェア認証プログラム
ソフトウェア本体
382
380
メッセージ送信部
313
メッセージ電子署名部
312
メッセージ作成部
311
ソフトウェア受信部
314
ソフトウェア復号化部
315
ソフトウェア認証部
316
ソフトウェア認証機能起動部
317
ソフトウェア本体機能利用部
318
ソフトウェア利用プラットフォーム310
ソフトウェア利用許可システム300

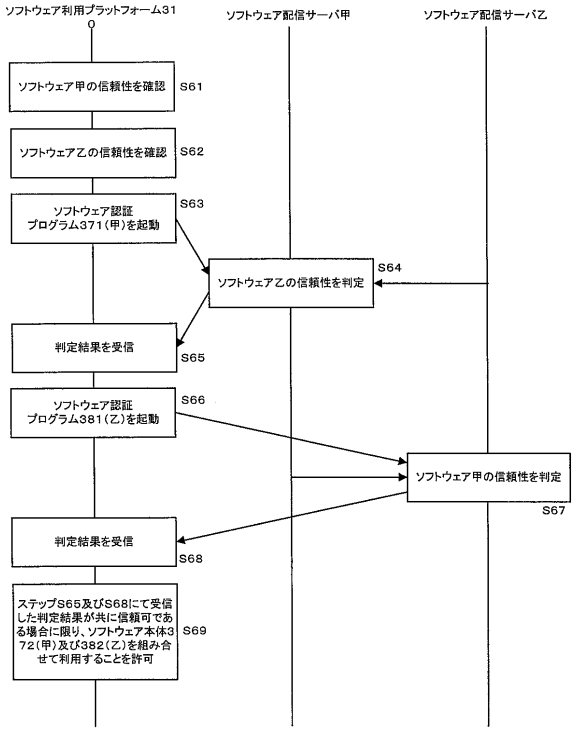
【図４】


ソフトウェア利用プラットフォーム310
ソフトウェア配信サーバ320(甲)
ソフトウェア配信サーバ330(乙)
メッセージ350(甲)を作成
S41
メッセージ甲に電子署名を行う
S42
メッセージ甲をソフトウェア配信サーバ甲に送信
S43
メッセージ甲を受信
S44
メッセージ甲の電子署名を基にソフトウェア利用プラットフォーム310の信頼性を確認
S45
ソフトウェア370(甲)に電子署名を施す
S46
ソフトウェア甲を暗号化
S47
ソフトウェア甲をソフトウェア利用プラットフォーム310に送信
S48
ソフトウェア甲を受信
S49
ソフトウェア甲を復号
S50

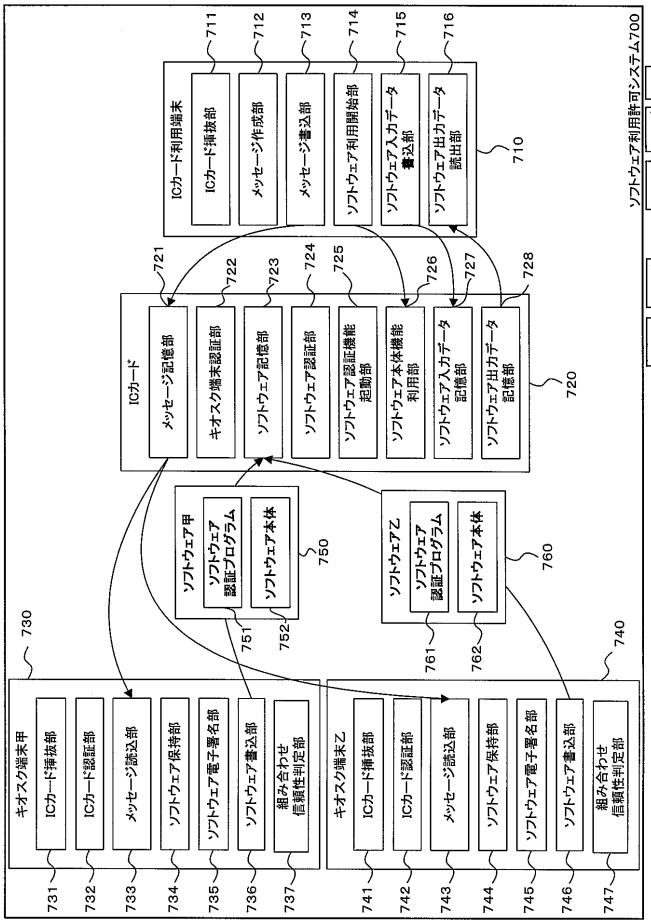
【図５】


ソフトウェア利用プラットフォーム310
ソフトウェア配信サーバ甲
ソフトウェア配信サーバ乙
メッセージ360(乙)を作成
S51
メッセージ乙に電子署名を行う
S52
メッセージ乙をソフトウェア配信サーバ乙に送信
S53
メッセージ乙を受信
S54
メッセージ乙の電子署名を基にソフトウェア利用プラットフォーム310の信頼性を確認
S55
ソフトウェア380(乙)に電子署名を施す
S56
ソフトウェア乙を暗号化
S57
ソフトウェア乙をソフトウェア利用プラットフォーム310に送信
S58
ソフトウェア乙を受信
S59
ソフトウェア乙を復号
S50

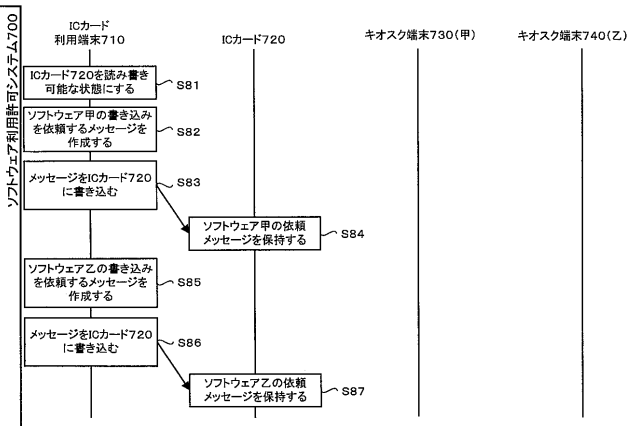
【図６】


ソフトウェア利用プラットフォーム310
ソフトウェア配信サーバ甲
ソフトウェア配信サーバ乙
ソフトウェア甲の信頼性を確認
S61
ソフトウェア乙の信頼性を確認
S62
ソフトウェア認証プログラム371(甲)を起動
S63
ソフトウェア乙の信頼性を判定
S64
判定結果を受信
S65
ソフトウェア認証プログラム381(乙)を起動
S66
ソフトウェア甲の信頼性を判定
S67
判定結果を受信
S68
ステップS65及びS68にて受信した判定結果が共に信頼可である場合に限り、ソフトウェア本体372(甲)及び382(乙)を組み合せて利用することを許可
S69

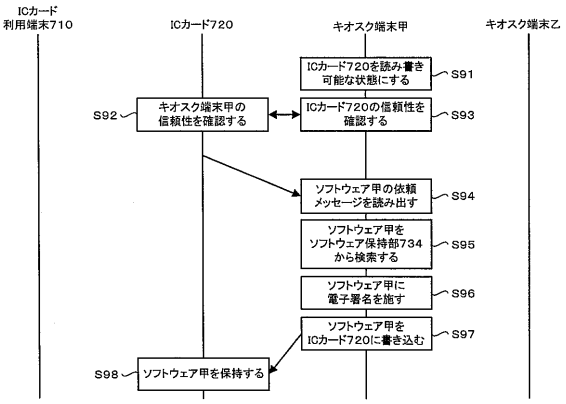
【図７】


ICカード利用端末
ICカード挿抜部
メッセージ作成部
メッセージ書込部
ソフトウェア利用開始部
ソフトウェア入力データ書込部
ソフトウェア出力データ読出部
710
ICカード
メッセージ記憶部
キオスク端末認証部
ソフトウェア記憶部
ソフトウェア認証部
ソフトウェア認証機能起動部
ソフトウェア本体機能利用部
ソフトウェア入力データ記憶部
ソフトウェア出力データ記憶部
720
ソフトウェア甲
ソフトウェア認証プログラム
ソフトウェア本体
750
ソフトウェア乙
ソフトウェア認証プログラム
ソフトウェア本体
760
キオスク端末甲
ICカード挿抜部
ICカード認証部
メッセージ読込部
ソフトウェア保持部
ソフトウェア電子署名部
ソフトウェア書込部
組み合わせ信頼性判定部
730
キオスク端末乙
ICカード挿抜部
ICカード認証部
メッセージ読込部
ソフトウェア保持部
ソフトウェア電子署名部
ソフトウェア書込部
組み合わせ信頼性判定部
740

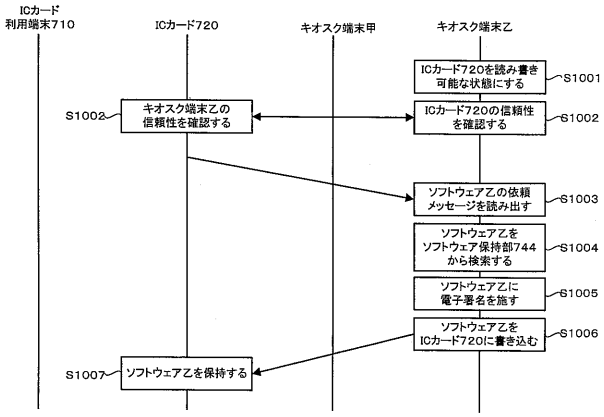
【図８】


ソフトウェア利用許可システム700
ICカード利用端末710
ICカード720
キオスク端末730(甲)
キオスク端末740(乙)
ICカード720を読み書き可能な状態にする
S81
ソフトウェア甲の書き込みを依頼するメッセージを作成する
S82
メッセージをICカード720に書き込む
S83
ソフトウェア甲の依頼メッセージを保持する
S84
ソフトウェア乙の書き込みを依頼するメッセージを作成する
S85
メッセージをICカード720に書き込む
S86
ソフトウェア乙の依頼メッセージを保持する
S87

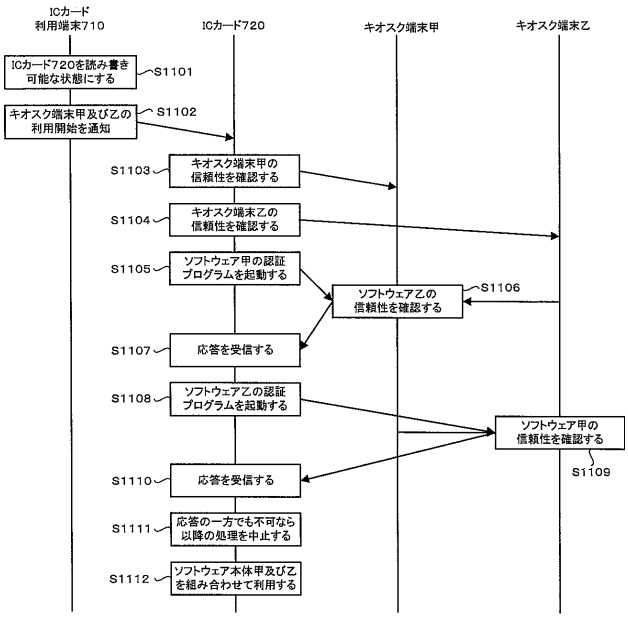
【図９】


ICカード利用端末710
ICカード720
キオスク端末甲
キオスク端末乙
ICカード720を読み書き可能な状態にする
S91
キオスク端末甲の信頼性を確認する
S92
ICカード720の信頼性を確認する
S93
ソフトウェア甲の依頼メッセージを読み出す
S94
ソフトウェア甲をソフトウェア保持部734から検索する
S95
ソフトウェア甲に電子署名を施す
S96
ソフトウェア甲をICカード720に書き込む
S97
S98
ソフトウェア甲を保持する

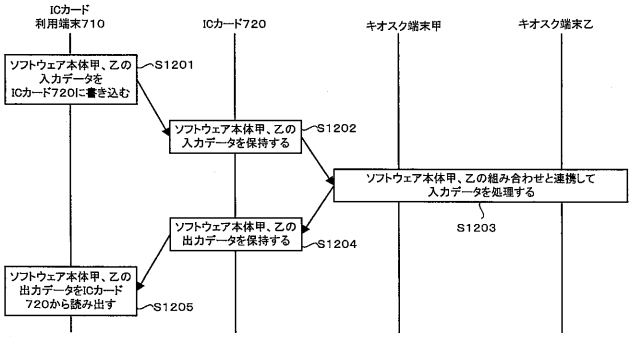
【図１０】


ICカード利用端末710
ICカード720
キオスク端末甲
キオスク端末乙
ICカード720を読み書き可能な状態にする
S1001
S1002
キオスク端末乙の信頼性を確認する
ICカード720の信頼性を確認する
S1002
ソフトウェア乙の依頼メッセージを読み出す
S1003
ソフトウェア乙をソフトウェア保持部744から検索する
S1004
ソフトウェア乙に電子署名を施す
S1005
ソフトウェア乙をICカード720に書き込む
S1006
S1007
ソフトウェア乙を保持する

【図１１】


ICカード
利用端末710
ICカード720
キオスク端末甲
キオスク端末乙
ICカード720を読み書き
可能な状態にする
S1101
キオスク端末甲及び乙の
利用開始を通知
S1102
S1103
キオスク端末甲の
信頼性を確認する
S1104
キオスク端末乙の
信頼性を確認する
S1105
ソフトウェア甲の認証
プログラムを起動する
ソフトウェア乙の
信頼性を確認する
S1106
S1107
応答を受信する
S1108
ソフトウェア乙の認証
プログラムを起動する
ソフトウェア甲の
信頼性を確認する
S1109
S1110
応答を受信する
S1111
応答の一方でも不可なら
以降の処理を中止する
S1112
ソフトウェア本体甲及び乙
を組み合わせて利用する

【図１２】


ICカード
利用端末710
ICカード720
キオスク端末甲
キオスク端末乙
ソフトウェア本体甲、乙の
入力データを
ICカード720に書き込む
S1201
ソフトウェア本体甲、乙の
入力データを保持する
S1202
ソフトウェア本体甲、乙の組み合わせと連携して
入力データを処理する
S1203
ソフトウェア本体甲、乙の
出力データを保持する
S1204
ソフトウェア本体甲、乙の
出力データをICカード
720から読み出す
S1205