

(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2010-282529

(P2010-282529A)

(43) 公開日 平成22年12月16日(2010.12.16)

(51) Int.Cl. F I テーマコード (参考)
G06F 21/22 (2006.01) G06F 9/06 660F 5B276

審査請求 有 請求項の数 7 O L (全 17 頁)

(21) 出願番号	特願2009-136867 (P2009-136867)	(71) 出願人	506113602 株式会社コナミデジタルエンタテインメント 東京都港区赤坂九丁目7番2号
(22) 出願日	平成21年6月8日(2009.6.8)	(74) 代理人	100110135 弁理士 石井 裕一郎
		(72) 発明者	森 昌二 東京都港区赤坂九丁目7番2号 株式会社 コナミデジタルエンタテインメント内
		Fターム(参考)	5B276 FB06

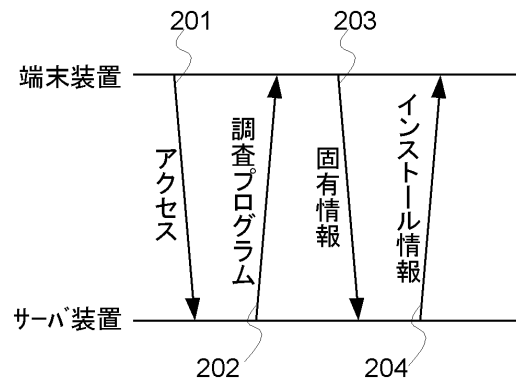
(54) 【発明の名称】 インストールシステム、サーバ装置、インストール方法、ならびに、サーバプログラム

(57) 【要約】

【課題】特定の端末装置のみにインストール可能なアプリケーション情報を適切に提供するインストールシステム等を提供する。

【解決手段】サーバ装置から送信(202)された調査プログラムを端末装置が実行すると、端末装置の固有情報を読み取って、これをサーバ装置へ送信し(203)、サーバ装置は、受信した固有情報を暗号鍵として、アプリケーション情報を暗号化して、暗号化した結果をインストールプログラムとまとめてインストール情報とし、これを端末装置へ送信し(204)、端末装置がインストール情報に含まれるインストールプログラムを実行すると、インストールプログラムは、端末装置の固有情報を読み取り、読み取った固有情報を暗号鍵として、インストール情報に含まれるアプリケーション情報の復号を試み、復号に成功したら、インストールプログラムは、端末装置に、アプリケーション情報をインストールする。

【選択図】 図3



【特許請求の範囲】

【請求項 1】

端末装置と、サーバ装置と、を有するインストールシステムであって、

(a) 前記端末装置は、

当該端末装置の固有情報を読み取って、当該固有情報を前記サーバ装置へ送信する固有
情報送信部

を備え、

(b) 前記サーバ装置は、

前記端末装置から送信された固有情報を受信する固有情報受信部、

前記端末装置にインストールされるべきアプリケーション情報を、前記受信された固有
情報を暗号鍵として暗号化した暗号化済情報を生成する暗号化済情報生成部、

前記生成された暗号化済情報を含むインストール情報を前記端末装置へ送信するインス
トール情報送信部

を備え、

(c) 前記端末装置は、

前記サーバ装置から送信されたインストール情報を受信するインストール情報受信部、

当該端末装置の固有情報を読み取って、当該固有情報を暗号鍵として前記受信されたイ
ンストール情報に含まれる暗号化済情報を復号して、当該端末装置にインストールされる
べきアプリケーション情報を生成するアプリケーション情報生成部、

前記生成されたアプリケーション情報を、当該端末装置にインストールするインストー
ル部

を備えることを特徴とするインストールシステム。

【請求項 2】

請求項 1 に記載のインストールシステムであって、

前記サーバ装置は、端末コンピュータを、前記固有情報送信部として機能させる調査プ
ログラムを、前記端末コンピュータに送信し、当該端末コンピュータは、前記調査プログ
ラムを受信して実行することにより、固有情報送信部として機能し、

前記サーバ装置は、前記端末コンピュータを、前記アプリケーション情報生成部、およ
び、前記インストール部として機能させ、前記暗号化済情報を含むインストールプログラ
ムを、前記インストール情報として、前記端末コンピュータに送信し、

当該端末コンピュータは、前記インストールプログラムを受信して実行することにより
、アプリケーション情報生成部およびインストール部として機能する

ことを特徴とするインストールシステム。

【請求項 3】

請求項 1 または 2 に記載のインストールシステムであって、

前記固有情報は、当該端末装置の固有情報が読み取られた日時を、所定の定数で除算し
た結果を含む情報、もしくは、当該情報のハッシュ値である

ことを特徴とするインストールシステム。

【請求項 4】

請求項 1 から 3 のいずれか 1 項に記載のインストールシステムであって、

前記端末装置は、

前記端末装置にインストールされたアプリケーション情報を識別する識別情報を記憶す
るレジストリ部

をさらに備え、前記固有情報は、前記レジストリ部に記憶される識別情報を含む情報、
もしくは、当該情報のハッシュ値である

ことを特徴とするインストールシステム。

【請求項 5】

端末装置と通信するサーバ装置であって、

端末コンピュータへ調査プログラムを送信する調査プログラム送信部、

前記端末コンピュータから送信された固有情報を受信する固有情報受信部、

	10
	20
	30
	40
	50

前記端末コンピュータにインストールされるべきアプリケーション情報を、前記受信された固有情報を暗号鍵として暗号化した暗号化済情報を生成する暗号化済情報生成部、
前記生成された暗号化済情報と、インストールプログラムと、を含むインストール情報を前記端末コンピュータへ送信するインストール情報送信部

を備え、

前記調査プログラムは、前記端末コンピュータを、

当該端末コンピュータの固有情報を読み取って、当該固有情報を前記サーバ装置へ送信する固有情報送信部

として機能させ、

前記インストールプログラムは、前記端末コンピュータを、

当該端末コンピュータの固有情報を読み取って、当該固有情報を暗号鍵として前記受信されたインストール情報に含まれる暗号化済情報を復号して、当該端末装置にインストールされるべきアプリケーション情報を生成するアプリケーション情報生成部、

前記生成されたアプリケーション情報を、当該端末コンピュータにインストールするインストール部

として機能させることを特徴とするサーバ装置。

10

【請求項 6】

端末装置と、サーバ装置と、が、実行するインストール方法であって、

(a) 前記端末装置が、

当該端末装置の固有情報を読み取って、当該固有情報を前記サーバ装置へ送信する固有情報送信工程

20

を備え、

(b) 前記サーバ装置が、

前記端末装置から送信された固有情報を受信する固有情報受信工程

前記端末装置にインストールされるべきアプリケーション情報を、前記受信された固有情報を暗号鍵として暗号化した暗号化済情報を生成する暗号化済情報生成工程、

前記生成された暗号化済情報を含むインストール情報を前記端末装置へ送信するインストール情報送信工程

を備え、

(c) 前記端末装置が、

前記サーバ装置から送信されたインストール情報を受信するインストール情報受信工程

30

、
当該端末装置の固有情報を読み取って、当該固有情報を暗号鍵として前記受信されたインストール情報に含まれる暗号化済情報を復号して、当該端末装置にインストールされるべきアプリケーション情報を生成するアプリケーション情報生成工程、

前記生成されたアプリケーション情報を、当該端末装置にインストールするインストール工程

を備えることを特徴とするインストール方法。

【請求項 7】

端末コンピュータと通信するサーバコンピュータを、サーバ装置として機能させるサーバプログラムであって、当該サーバプログラムは、当該サーバコンピュータを、

40

前記端末コンピュータへ調査プログラムを送信する調査プログラム送信部、

前記端末コンピュータから送信された固有情報を受信する固有情報受信部、

前記端末コンピュータにインストールされるべきアプリケーション情報を、前記受信された固有情報を暗号鍵として暗号化した暗号化済情報を生成する暗号化済情報生成部、

前記生成された暗号化済情報と、インストールプログラムと、を含むインストール情報を前記端末コンピュータへ送信するインストール情報送信部

として機能させ、

前記調査プログラムは、前記端末コンピュータを、

当該端末装置の固有情報を読み取って、当該固有情報を前記サーバ装置へ送信する固有

50

情報送信部

として機能させ、

前記インストールプログラムは、前記端末コンピュータを、

当該端末コンピュータの固有情報を読み取って、当該固有情報を暗号鍵として前記受信されたインストール情報に含まれる暗号化済情報を復号して、当該端末装置にインストールされるべきアプリケーション情報を生成するアプリケーション情報生成部、

前記生成されたアプリケーション情報を、当該端末コンピュータにインストールするインストール部

として機能させることを特徴とするサーバプログラム。

【発明の詳細な説明】

10

【技術分野】

【0001】

本発明は、特定の端末装置のみにインストール可能なアプリケーション情報を適切に提供するインストールシステム、サーバ装置、インストール方法、ならびに、これらをコンピュータにて実現するプログラムに関する。

【背景技術】

【0002】

従来から、ネットワーク通信機能を持ったコンピュータやゲーム装置などの端末装置に、各種のアプリケーションプログラムやゲームプログラム、当該プログラム用の各種追加データ等を、コンピュータ通信網を介してサーバ装置が提供するインストールシステムが提案されている。

20

【0003】

ここで、以下に掲げる特許文献1においては、端末装置の固有情報を参照して、正当な使用権を有するユーザのみがアプリケーション情報をインストールできるようにする技術が提案されている。

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特許第4011285号公報

【発明の概要】

30

【発明が解決しようとする課題】

【0005】

一方で、インストールシステムにおいては、不正なインストールを簡易に防止するためのさらなる技術が強く求められている。

【0006】

本発明は、上記のような課題を解決するもので、特定の端末装置のみにインストール可能なアプリケーション情報を適切に提供するインストールシステム、サーバ装置、インストール方法、ならびに、これらをコンピュータにて実現するプログラムを提供することを目的とする。

【課題を解決するための手段】

40

【0007】

以上の目的を達成するため、本発明の原理にしたがって、下記の発明を開示する。

【0008】

本発明の第1の観点に係るインストールシステムは、端末装置と、サーバ装置と、を有し、端末装置は、固有情報送信部、インストール情報受信部、アプリケーション情報生成部、インストール部を備え、前記サーバ装置は、固有情報受信部、暗号化済情報生成部、インストール情報送信部を備え、以下のように構成する。

【0009】

まず、端末装置において、固有情報送信部は、当該端末装置の固有情報を読み取って、当該固有情報をサーバ装置へ送信する。

50

【 0 0 1 0 】

端末装置の固有情報としては、端末装置の C P U (Central Processing Unit) の製造番号、端末装置の N I C (Network Interface Card) の M A C (Media Access Control) アドレスや現在割り当てられている I P (Internet Protocol) アドレス、端末装置にインストール済みの他のアプリケーションの情報等、種々の情報をそのまま採用しても良いが、典型的には、これらの情報を並べたバイト列のハッシュ値を利用する。

【 0 0 1 1 】

一方、サーバ装置において、固有情報受信部は、端末装置から送信された固有情報を受信し、暗号化済情報生成部は、端末装置にインストールされるべきアプリケーション情報を、受信された固有情報を暗号鍵として暗号化した暗号化済情報を生成し、インストール情報送信部は、生成された暗号化済情報を含むインストール情報を端末装置へ送信する。

10

【 0 0 1 2 】

インストール情報は、端末装置でインストール時のみに実行されるプログラムであり、その中に上記の暗号化済情報が埋め込まれている。

【 0 0 1 3 】

たとえば、端末装置にゲームプログラムをインストールする態様では、アプリケーション情報としては、音声や画像、動画等のマルチメディア情報ファイルのほか、ゲームプログラム本体として機能する実行可能ファイルなどが含まれる。

【 0 0 1 4 】

さらに、端末装置において、インストール情報受信部は、サーバ装置から送信されたインストール情報を受信し、アプリケーション情報生成部は、当該端末装置の固有情報を読み取って、当該固有情報を暗号鍵として受信されたインストール情報に含まれる暗号化済情報を復号して、当該端末装置にインストールされるべきアプリケーション情報を生成し、インストール部は、生成されたアプリケーション情報を、当該端末装置にインストールする。

20

【 0 0 1 5 】

上記のように、本発明においては、固有情報に基づいて、端末装置を識別することとしており、インストール情報に基づいてアプリケーション情報をインストールする際に、当該端末装置の固有情報を、読み出すこととする。この固有情報は、不正なインストールでなければ、固有情報送信部により読み出された値と一致するはずである。この場合には、暗号化されたアプリケーション情報を復号することが可能である。

30

【 0 0 1 6 】

一方、暗号化済情報が何らかの事情で第三者に流出した場合であっても、端末装置の固有情報が偶然一致する可能性は低い。したがって、被害を最小限に抑えることができるのである。

【 0 0 1 7 】

このように、本発明によれば、特定の端末装置のみにインストール可能なアプリケーション情報を適切に提供することができるようになる。

【 0 0 1 8 】

また、本発明のインストールシステムにおいて、サーバ装置は、調査プログラム、および、インストールプログラムを、端末コンピュータに送信し、以下のように構成することができる。

40

【 0 0 1 9 】

ここで、調査プログラムは、端末コンピュータを、固有情報送信部として機能させ、当該端末コンピュータは、調査プログラムを受信して実行することにより、固有情報送信部として機能する。

【 0 0 2 0 】

たとえば、端末装置からアプリケーションを購入する申し込みをサーバ装置に行うような状況では、調査プログラムは、当該購入申込を実行することとなり、アプリケーション利用の契約条項を提示したり、クレジットカード等を用いた決済を行ったり等の処理に加

50

えて、端末装置の固有情報をサーバ装置に通知する、という役目を果たす。

【0021】

また、インストールプログラムは、暗号化済情報を含み、端末コンピュータを、アプリケーション情報生成部、および、インストール部として機能させ、当該端末コンピュータは、インストールプログラムを受信して実行することにより、アプリケーション情報生成部およびインストール部として機能する。

【0022】

上記の例では、インストールプログラムは、契約が完了した後に提供される実行可能ファイルで、典型的には、setup.exe等のファイル名で提供されるものに相当する。

【0023】

インストールプログラムは、典型的には、自己解凍型圧縮ファイルとして構成されているが、圧縮の際に、上記のように暗号化がなされており、暗号鍵として、当該端末装置のインストール時の固有情報を用いる。

【0024】

本発明は、上記発明の好適実施形態に係るものであり、サーバ装置から2種類のプログラムを端末装置に提供することによって、簡単にアプリケーションのインストールができるようになる。

【0025】

また、本発明のインストールシステムにおいて、固有情報は、当該端末装置の固有情報が読み取られた日時を、所定の定数で除算した結果を含む情報、もしくは、当該情報のハッシュ値であるように構成することができる。

【0026】

インストール情報が流出してしまった場合等の被害を抑えるためには、当該インストール情報からインストールができる有効期限を設けることが望ましいが、有効期限の情報そのものを直接インストール情報に埋め込んでおくと、その部分を直接書き換えられてしまう、等の不正手段がとられる可能性が高まる。

【0027】

本発明では、当該端末装置が有するリアルタイムクロックが計測している日時（典型的には、1970年1月1日0時0分0秒からの経過時間秒数）を有効期間に対応付けられる定数（たとえば、30日間有効とするならば、60日に相当する秒数を採用する等。）で除算して整数化した値が、端末装置の固有情報に反映されるようにしている。

【0028】

本発明では、インストール情報に有効期限を持たせる場合に、日時情報の比較をする必要がないため、不正行為をより一層防止することができるようになる。

【0029】

また、本発明のインストールシステムにおいて、端末装置は、端末装置にインストールされたアプリケーション情報を識別する識別情報を記憶するレジストリ部をさらに備え、固有情報は、レジストリ部に記憶される識別情報を含む情報、もしくは、当該情報のハッシュ値であるように構成することができる。

【0030】

ここで、インストールされたアプリケーション情報とは、プログラムの名称やインストール済のディレクトリ、シリアル番号等の情報である。

【0031】

どのようなアプリケーションをどのようにインストールするかは、端末装置を利用するユーザの利用状況によって大きく変化するため、これらの情報が偶然に一致する可能性は極めて低い。

【0032】

一方で、あるアプリケーションを新たにインストールしようとしている状況では、上記のアプリケーション情報は変化しないと仮定することができる。

【0033】

10

20

30

40

50

本発明によれば、固有情報が、インストール済みのアプリケーション情報を反映するように構成することで、適切に端末装置を識別することができるようになる。

【0034】

本発明のその他の観点に係るサーバ装置は、上記インストールシステムのサーバ装置である。

【0035】

本発明のその他の観点に係るインストール方法は、端末装置と、サーバ装置と、が、実行し、端末装置において、固有情報送信工程、インストール情報受信工程、アプリケーション情報生成工程、インストール工程が実行され、サーバ装置において、固有情報受信工程、暗号化済情報生成工程、インストール情報送信工程が実行され、以下のように構成する。

10

【0036】

すなわち、固有情報送信工程では、端末装置が、当該端末装置の固有情報を読み取って、当該固有情報をサーバ装置へ送信する。

【0037】

一方、固有情報受信工程では、サーバ装置が、端末装置から送信された固有情報を受信し、暗号化済情報生成工程では、サーバ装置が、端末装置にインストールされるべきアプリケーション情報を、受信された固有情報を暗号鍵として暗号化した暗号化済情報を生成し、インストール情報送信工程では、サーバ装置が、生成された暗号化済情報を含むインストール情報を端末装置へ送信する。

20

【0038】

さらに、インストール情報受信工程では、端末装置が、サーバ装置から送信されたインストール情報を受信し、アプリケーション情報生成工程では、端末装置が、当該端末装置の固有情報を読み取って、当該固有情報を暗号鍵として受信されたインストール情報に含まれる暗号化済情報を復号して、当該端末装置にインストールされるべきアプリケーション情報を生成し、インストール工程では、端末装置が、生成されたアプリケーション情報を、当該端末装置にインストールする。

【0039】

本発明のその他の観点に係るサーバプログラムは、コンピュータを上記のサーバ装置として機能させるように構成する。

30

【0040】

本発明のその他の観点に係る調査プログラムおよびインストールプログラムは、コンピュータを、上記の端末装置として機能させるように構成する。

【0041】

また、本発明のプログラムは、コンパクトディスク、フレキシブルディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、半導体メモリ等のコンピュータ読取可能な情報記憶媒体に記録することができる。

【0042】

上記プログラムは、プログラムが実行されるコンピュータとは独立して、コンピュータ通信網を介して配布・販売することができる。また、上記情報記憶媒体は、コンピュータとは独立して配布・販売することができる。

40

【発明の効果】

【0043】

本発明によれば、特定の端末装置のみにインストール可能なアプリケーション情報を適切に提供するインストールシステム、サーバ装置、インストール方法、ならびに、これらをコンピュータにて実現するプログラムを提供することができる。

【図面の簡単な説明】

【0044】

【図1】典型的な情報処理装置の概要構成を示す模式図である。

【図2】本実施形態に係る端末装置とサーバ装置の概要構成を示す模式図である。

50

【図3】端末装置とサーバ装置との間の通信の様子を示すセッション図である。

【図4】サーバ装置におけるサービス処理の制御の流れを示すフローチャートである。

【図5】端末装置における調査処理の制御の流れを示すフローチャートである。

【図6】端末装置におけるインストール処理の制御の流れを示すフローチャートである。

【発明を実施するための形態】

【0045】

以下に本発明の実施形態を説明する。以下では、理解を容易にするため、ゲーム用の情報処理装置を利用して本発明が実現される実施形態を説明するが、以下に説明する実施形態は説明のためのものであり、本願発明の範囲を制限するものではない。

【0046】

したがって、当業者であればこれらの各要素もしくは全要素をこれと均等なものに置換した実施形態を採用することが可能であるが、これらの実施形態も本発明の範囲に含まれる。

【実施例1】

【0047】

図1は、プログラムを実行することにより、本実施形態の端末装置やサーバ装置として機能しうる典型的な情報処理装置の概要構成を示す模式図である。以下、本図を参照して説明する。

【0048】

本図に示す情報処理装置100は、いわゆるコンシューマゲーム機に相当するもので、CPU (Central Processing Unit) 101、ROM (Read Only Memory) 102、RAM (Random Access Memory) 103、インターフェース104、コントローラ105、外部メモリ106、画像処理部107、DVD-ROM (Digital Versatile Disc ROM) ドライブ108、NIC (Network Interface Card) 109、音声処理部110、マイク111、ハードディスク (Hard Disk; HD) 121を有する。各種の入出力装置は、適宜省略することができる。

【0049】

情報処理装置100を典型的なコンシューマゲーム機として機能させる場合には、ゲーム用プログラムおよびデータを記憶したDVD-ROMをDVD-ROMドライブ108に装着し、電源を投入する。すると、当該ゲームプログラムが実行され、ゲームをプレイすることができるようになる。

【0050】

ただし、本実施形態においては、典型的には、DVD-ROMドライブ108に装着されたDVD-ROMから、アプリケーションをHD 121にインストールする。そして、当該HD 121に記憶されたプログラムを実行することによって、ゲームを含む各種のアプリケーションを実行することとする。

【0051】

また、後述するように、端末装置とサーバ装置とでは、実行する情報処理の規模や種類が異なるだけで、本質的には、いずれも、本図に示す情報処理装置100と同様の構成により、実現される。

【0052】

なお、携帯型のゲーム装置においては、携帯可能とするために、DVD-ROMドライブ108を利用するのではなく、ROMカセット用スロットにEEPROM (Electrically Erasable Programmable ROM) カセットを装着して、HD 121を省略したりすることも可能である。この場合、アプリケーション用プログラムをEEPROMカセットに書き込んだ上で、当該プログラムを実行することとなる。このほか、外部メモリ106にアプリケーション用プログラムをインストールすることも可能である。

【0053】

さて、CPU 101は、情報処理装置100全体の動作を制御し、各構成要素と接続され制御信号やデータをやりとりする。また、CPU 101は、レジスタ(図示せず)

10

20

30

40

50

という高速アクセスが可能な記憶域に対してA L U (Arithmetic Logic Unit) (図示せず)を用いて加減乗除等の算術演算や、論理和、論理積、論理否定等の論理演算、ビット和、ビット積、ビット反転、ビットシフト、ビット回転等のビット演算などを行うことができる。さらに、マルチメディア処理対応のための加減乗除等の飽和演算や、三角関数等、ベクトル演算などを高速に行えるように、C P U 1 0 1自身が構成されているものや、コプロセッサを備えて実現するものがある。

【0054】

R O M 1 0 2には、電源投入直後に実行されるI P L (Initial Program Loader)が記録され、これが実行されることにより、D V D - R O Mに記録されたプログラムをR A M 1 0 3に読み出してC P U 1 0 1による実行が開始される。また、R O M 1 0 2には、情報処理装置1 0 0全体の動作制御に必要なオペレーティングシステムのプログラムや各種のデータが記録される。

10

【0055】

R A M 1 0 3は、データやプログラムを一時的に記憶するためのもので、H D 1 2 1やD V D - R O M等から読み出したプログラムやデータ、その他通信対戦ゲームの進行やチャット通信に必要なデータが保持される。また、C P U 1 0 1は、R A M 1 0 3に変数領域を設け、当該変数に格納された値に対して直接A L Uを作用させて演算を行ったり、R A M 1 0 3に格納された値を一旦レジスタに格納してからレジスタに対して演算を行い、演算結果をメモリに書き戻す、などの処理を行う。

【0056】

インターフェース1 0 4を介して接続されたコントローラ1 0 5は、ユーザがゲーム実行の際に行う操作入力を受け付ける。

20

【0057】

なお、コントローラ1 0 5は、必ずしも情報処理装置1 0 0に対して外付けにされている必要はなく、一体に形成されていても良い。携帯可能な端末装置のコントローラ1 0 5は、各種のボタンやスイッチから構成され、これらの押圧操作を操作入力として扱う。このほか、タッチスクリーンを利用した情報処理装置1 0 0では、ユーザがペンや指を利用してタッチスクリーンをなぞった軌跡を操作入力として扱う。

【0058】

インターフェース1 0 4を介して着脱自在に接続された外部メモリ1 0 6には、ゲーム等のプレイ状況(過去の成績等)を示すデータ、ゲームの進行状態を示すデータ、ネットワーク対戦の場合のチャット通信のログ(記録)のデータなどが書き換え可能に記憶される。ユーザは、コントローラ1 0 5を介して指示入力を行うことにより、これらのデータを適宜外部メモリ1 0 6に記録することができる。

30

【0059】

上述の通り、アプリケーションプログラムを外部メモリ1 0 6にインストールして実行するような形態を採用することもできる。これは、外部メモリ1 0 6が大容量である場合に好適である。

【0060】

D V D - R O Mドライブ1 0 8に装着されるD V D - R O Mには、ゲームを実現するためのプログラムとゲームに付随する画像データや音声データが記録される。C P U 1 0 1の制御によって、D V D - R O Mドライブ1 0 8は、これに装着されたD V D - R O Mに対する読み出し処理を行って、必要なプログラムやデータを読み出し、これらはR A M 1 0 3等に一時的に記憶される。

40

【0061】

画像処理部1 0 7は、D V D - R O Mから読み出されたデータをC P U 1 0 1や画像処理部1 0 7が備える画像演算プロセッサ(図示せず)によって加工処理した後、これを画像処理部1 0 7が備えるフレームメモリ(図示せず)に記録する。フレームメモリに記録された画像情報は、所定の同期タイミングでビデオ信号に変換され画像処理部1 0 7に接続されるモニタ(図示せず)へ出力される。これにより、各種の画像表示が可能となる

50

。

【0062】

携帯可能な端末装置のモニタとしては、小型の液晶ディスプレイを利用するのが典型的であり、コントローラ105としてタッチスクリーンを利用する場合には、当該タッチスクリーンの表示パネルがモニタとして機能する。自宅で遊ぶための端末装置やサーバ装置のモニタとしては、CRT (Cathode Ray Tube) やプラズマディスプレイなどの表示装置を利用することも可能である。

【0063】

画像演算プロセッサは、2次元の画像の重ね合わせ演算やブレンディング等の透過演算、各種の飽和演算を高速に実行できる。

【0064】

また、仮想3次元空間に配置され、各種のテクスチャ情報が付加されたポリゴン情報を、Zバッファ法によりレンダリングして、所定の視点位置から仮想3次元空間に配置されたポリゴンを通じた視線の方向へ俯瞰したレンダリング画像を得る演算の高速実行も可能である。

【0065】

さらに、CPU 101と画像演算プロセッサが協調動作することにより、文字の形状を定義するフォント情報にしたがって、文字列を2次元画像としてフレームメモリへ描画したり、各ポリゴン表面へ描画することが可能である。

【0066】

NIC 109は、情報処理装置100をインターネット等のコンピュータ通信網(図示せず)に接続するためのものであり、LANを構成する際に用いられる10BASE-T/100BASE-T規格にしたがうものや、電話回線を用いてインターネットに接続するためのアナログモデム、ISDN (Integrated Services Digital Network) モデム、ADSL (Asymmetric Digital Subscriber Line) モデム、ケーブルテレビジョン回線を用いてインターネットに接続するためのケーブルモデム等と、これらとCPU 101との仲立ちを行うインターフェース(図示せず)により構成される。

【0067】

また、NIC 109経由でコンピュータ通信網から入手した情報を元に、HD 121等にアプリケーションプログラムをインストールすることも可能である。

【0068】

音声処理部110は、HD 121やDVD-ROMから読み出した音声データをアナログ音声信号に変換し、これに接続されたスピーカ(図示せず)から出力させる。また、CPU 101の制御の下、ゲームの進行の中で発生させるべき効果音や楽曲データを生成し、これに対応した音声をスピーカや、ヘッドホン(図示せず)、イヤホン(図示せず)から出力させる。

【0069】

音声処理部110では、HD 121やDVD-ROMに記録された音声データがMIDIデータである場合には、これが有する音源データを参照して、MIDIデータをPCMデータに変換する。また、ADPCM形式やOgg Vorbis形式等の圧縮済音声データである場合には、これを展開してPCMデータに変換する。PCMデータは、そのサンプリング周波数に応じたタイミングでD/A (Digital/Analog) 変換を行って、スピーカに出力することにより、音声出力が可能となる。

【0070】

さらに、情報処理装置100には、インターフェース104を介してマイク111を接続することができる。この場合、マイク111からのアナログ信号に対しては、適当なサンプリング周波数でA/D変換を行い、PCM形式のデジタル信号として、音声処理部110でのミキシング等の処理ができるようにする。

【0071】

本実施形態で利用する情報処理装置100は、上述のように、HD 121等の大容量

10

20

30

40

50

外部記憶装置を用いるのが典型的である。H D 1 2 1 は、R O M 1 0 2、R A M 1 0 3、外部メモリ 1 0 6、D V D - R O M ドライブ 1 0 8 に装着される D V D - R O M 等と同じ機能を果たすこともできる。

【 0 0 7 2 】

このほか、ユーザからの文字列の編集入力を受け付けるためのキーボードや、各種の位置の指定および選択入力を受け付けるためのマウスなどを接続する形態も採用することができる。また、本実施形態の情報処理装置 1 0 0 にかえて、汎用のパーソナルコンピュータやサーバ用コンピュータ等を利用することもできる。

【 0 0 7 3 】

さらに、本実施形態では、リアルタイムクロック（図示せず）もしくは N I C 1 0 9 を介して N T P (Network Time Protocol) サーバに対して時刻を問い合わせる機能を採用して、情報処理装置 1 0 0 を利用している日時の情報を利用することとしている。

【 0 0 7 4 】

以上で説明した情報処理装置 1 0 0 は、コンシューマ向けゲーム装置に相当するものであるが、各種の入出力処理が可能な電子機器であれば、本発明の端末装置やサーバ装置を実現することができる。したがって、携帯電話、携帯ゲーム機器、カラオケ装置、一般的なビジネス用コンピュータなど、種々の計算機上で本発明の端末装置やサーバ装置を実現することが可能である。

【 0 0 7 5 】

たとえば、ビジネス用コンピュータは、上記情報処理装置 1 0 0 と同様に、C P U、R A M、R O M、D V D - R O M ドライブ、および、N I C、H D を構成要素として有するほか、情報処理装置 1 0 0 よりも簡易な機能を備えた画像処理部を備え、外部記憶装置としてフレキシブルディスク、光磁気ディスク、磁気テープ等が利用できるようになっており、コントローラ 1 0 5 ではなく、キーボードやマウスなどを入力装置として利用するのが典型的である。

【 0 0 7 6 】

本実施形態においては、サーバ装置用の情報処理装置 1 0 0 により実現されるサーバ用コンピュータから、端末装置用の情報処理装置 1 0 0 により実現される端末用コンピュータへ、アプリケーションプログラムを提供する際に、当該アプリケーションプログラムをインストールするための各種の情報が何らかの事情で流出したとしても、不正使用をできるだけ抑制するように、以下のような構成を採用する。

【 0 0 7 7 】

図 2 は、本実施形態に係る端末装置とサーバ装置の概要構成を示す模式図である。以下では、本図を参照して、本実施形態における各部の機能について概説する。

【 0 0 7 8 】

端末装置 6 0 1 のユーザがアクセス送信部 6 0 2 を操作して、サーバ装置 6 5 1 に対して、調査プログラムを求めるアクセスを行うと、サーバ装置 6 5 1 のアクセス受信部 6 5 2 は、これを受信する。そして、調査プログラム送信部 6 5 3 に、調査プログラムを端末装置 6 0 1 へ送信させる。

【 0 0 7 9 】

端末装置 6 0 1 の調査プログラム受信部 6 0 3 が調査プログラムを受信すると、C P U 1 0 1 はこれを実行し、固有情報送信部 6 0 4 が、固有情報を読み取って、サーバ装置 6 5 1 へ送信する。

【 0 0 8 0 】

サーバ装置 6 5 1 の固有情報受信部 6 5 4 は、送信された固有情報を受信し、暗号化済情報生成部 6 5 5 は、受信された固有情報でアプリケーション情報を暗号化し、インストール情報送信部 6 5 6 は、暗号化済アプリケーション情報とインストールプログラムをまとめて、インストール情報として、端末装置 6 0 1 に送信する。

【 0 0 8 1 】

端末装置 6 0 1 のインストール情報受信部 6 0 5 は、インストール情報を受信し、イン

10

20

30

40

50

ストール情報に含まれるインストールプログラムを実行すると、アプリケーション情報生成部606は、固有情報を読み取って、これを暗号鍵として用いて、暗号化済アプリケーション情報を復号する。インストール部607は、復号されたアプリケーション情報をHD 121等にインストールする。

【0082】

このように、端末装置601の各部は、CPU 101が、NIC 109や、RAM 103、HD 121等と共働して実現される。

【0083】

サーバ装置651の各部も、CPU 101が、NIC 109や、RAM 103、HD 121等と共働することによって実現される。

10

【0084】

以下では、本実施形態に係るサーバ装置651ならびに端末装置601の構成について、さらに詳細に説明する。図3は、本実施形態に係るサーバ装置651と端末装置601との通信の様子を示すセッション図である。以下、本図を参照して説明する。

【0085】

まず、端末装置601から、所望のアプリケーションプログラムを配布しているサーバ装置651に、アクセスする(201)。

【0086】

すると、サーバ装置651から、端末装置601へ、調査プログラムが送信される(202)。

20

【0087】

端末装置601が調査プログラムを実行すると、調査プログラムは、端末装置601の固有情報を読み取り、その固有情報をサーバ装置651へ送信する(203)。

【0088】

サーバ装置651は、受信した固有情報を暗号鍵として、アプリケーション情報を暗号化して、暗号化した結果をインストールプログラムとまとめてインストール情報とし、これを端末装置601へ送信する(204)。

【0089】

インストール情報を受信した端末装置601が、インストール情報に含まれるインストールプログラムを実行すると、インストールプログラムは、端末装置601の固有情報を読み取る。

30

【0090】

そして、読み取った固有情報を暗号鍵として、インストール情報に含まれるアプリケーション情報の復号を試みる。復号に成功したら、インストールプログラムは、端末装置601に、アプリケーション情報をインストールする。

【0091】

図4は、サーバプログラムを実行することにより実現されるサービス処理の制御の流れを示すフローチャートである。以下、本図を参照して説明する。

【0092】

サーバプログラムがサーバ装置651を実現するサーバ用コンピュータにて実行されると、CPU 101は、各種の初期化を行った後(ステップS301)、端末装置601から送信されるパケットを待機する(ステップS302)。この待機中には、各種の処理をコルーチン的に実行することができる。また、受信割込等を利用して、並行処理により、待機を実現しても良い。

40

【0093】

パケットが到達したら、当該パケットを受信して(ステップS303)、当該パケットの種類を調べる(ステップS304)。当該パケットが、アクセスパケットである場合(ステップS304;アクセス)、当該パケットの送信元の端末装置601へ、調査プログラムを送信して(ステップS305)、ステップS302に戻る。

【0094】

50

以下では一旦、端末装置 601 に提供される調査プログラムの詳細について説明する。図 5 は、調査プログラムを実行することにより実現される調査処理の制御の流れを示すフローチャートである。以下、本図を参照して説明する。

【0095】

調査プログラムが、端末装置 601 を実現する端末用コンピュータにて実行されると、CPU 101 は、当該端末用コンピュータの固有情報を読み取る（ステップ S401）。ここで、固有情報としては、以下のようなものが考えられる。

(1) 端末用コンピュータのリアルタイムクロック等で管理されている現在の日時の情報を、所定の定数で除算して整数化した情報。ここで、所定の定数とは、インストール情報の有効期間に対応する整数であり、有効期間の 2 倍とするのが典型的である。

(2) 端末用コンピュータの HD 121 にインストール済のアプリケーション情報を識別する識別情報。この情報は、HD 121 内のレジストリと呼ばれるデータベースに記憶されるのが典型的であり、アプリケーションプログラムの名称、インストールされたパス名、シリアル番号、インストールの日付などの情報が含まれる。

(3) 端末用コンピュータを利用しているユーザのログイン名。

(4) 端末用コンピュータのハードウェアの固有識別番号。たとえば、CPU 101 の ID や NIC 109 の MAC アドレス、IP アドレス等。

(5) 上記の情報を適宜バイト列として並べた結果のハッシュ値。ハッシュ値の計算には、たとえば、MD5 (Message Digest 5) 値などを利用することができる。

【0096】

上記(1)について、さらに詳細に説明する。端末コンピュータが有するリアルタイムクロック等が計測している日時は、典型的には、1970年1月1日0時0分0秒からの経過時間であり、秒を単位とした整数値で得られる。たとえば有効期間が30日間である場合、所定の定数としては、60日に相当する秒数を採用する。

【0097】

このような構成をとると、経過時間秒数を所定の定数で除算した値は、「現在から少なくとも有効期限が経過するまで」は、変化しない。また、経過時間秒数を所定の定数で除算した値が変化しないのは、「有効期限の 2 倍の長さの期間であって、現在をその中に含む期間」である。

【0098】

したがって、上記(1)の情報を固有情報として採用することにより、インストールできる有効期間を自然に導入することができるのである。

【0099】

ついで、CPU 101 は、アプリケーション利用の契約条項を画面表示し（ステップ S402）、クレジットカード等を用いた決済等を行うための情報の入力をユーザに求め（ステップ S403）、決済情報と固有情報を指定する固有情報バケットを、サーバ装置 651 に送信して（ステップ S404）、本処理を終了する。

【0100】

図 4 に戻り、サーバ装置 651 において、受信したパケットが固有情報パケットである場合（ステップ S304；固有情報）、当該パケットに含まれる決済情報に基づいて、決済処理を行う（ステップ S306）。

【0101】

さらに、提供すべきアプリケーション情報を、当該パケットに含まれる固有情報を暗号鍵として利用して、暗号化する（ステップ S307）。

【0102】

たとえば、端末装置 601 にゲームプログラムをインストールする態様では、アプリケーション情報としては、音声や画像、動画等のマルチメディア情報ファイルのほか、ゲームプログラム本体として機能する実行可能ファイルなどが含まれる。

【0103】

また、暗号化の手法としては、DES (Data Encryption Standard) や AES (Advanc

10

20

30

40

50

ed Encryption Standard) のような共通鍵暗号を使うのが典型的であり、ストリーム暗号やブロック暗号など、各種の技術を適用することも可能である。

【0104】

そして、暗号化されたアプリケーション情報と、インストールプログラムと、を指定するインストール情報を生成し(ステップS308)、これを端末装置601に送信して(ステップS309)、ステップS302に戻る。

【0105】

インストール情報は、自己解凍自動実行型の実行ファイルとして実現されるのが典型的である。以下、この形態を想定して説明する。

【0106】

また、受信されたパケットがその他の種類のものである場合(ステップS304;その他)、対応付けられる処理を実行して(ステップS310)、ステップS302に戻る。

【0107】

図6は、インストール情報を受信した端末装置601にて実行されるインストール処理の制御の流れを示す説明図である。以下、本図を参照して説明する。

【0108】

端末装置601のCPU101は、インストール情報である自己解凍自動実行型の実行ファイルの実行を開始する(ステップS501)。これにより、インストールプログラムと、暗号化されたアプリケーション情報と、を展開する(ステップS502)。

【0109】

ついで、CPU101は、展開されたインストールプログラムの実行を開始する(ステップS503)。当該インストールプログラムの実行により、CPU101は、当該端末装置601の固有情報を読み取る(ステップS504)。ここで読み取る情報は、ステップS401において読み取る情報と同じ種類のものである。

【0110】

また、調査プログラムを実行してから、インストールプログラムを実行するまでの期間が、有効期間以下であるならば、「端末用コンピュータのリアルタイムクロック等で管理されている現在の日時の情報を、所定の定数で除算して整数化した情報」は、ステップS401と、ステップS504と、で同じ値が得られるはずである。

【0111】

このため、同じ端末装置601で、有効期間内に、他のアプリケーションのインストール等を行わずに、本インストールプログラムを実行すれば、同じ固有情報が得られるのである。

【0112】

ついで、CPU101は、得られた固有情報を暗号鍵として用いて、展開された暗号化済アプリケーション情報の復号を試み(ステップS505)、復号に成功したか否かを判断する(ステップS506)。

【0113】

そして、復号に成功した場合(ステップS506;Yes)、CPU101は、復号されたアプリケーション情報を、HD121等にインストールして(ステップS507)、本処理を終了する。

【0114】

上記のように、本実施形態においては、固有情報に基づいて、端末装置601を識別することとしており、この固有情報は、不正なインストールでなければ、固有情報送信部により読み出された値と一致するはずである。この場合には、暗号化されたアプリケーション情報を復号することが可能である。

【0115】

一方、復号に失敗した場合(ステップS506;No)、インストール情報が無効である旨をユーザに提示して(ステップS508)、本処理を終了する。

【0116】

10

20

30

40

50

たとえば、暗号化済情報が何らかの事情で第三者に流出した場合であっても、端末装置 601 の固有情報が偶然一致する可能性は低い。したがって、流出したとしても被害を最小限に抑えることができる。

【0117】

また、有効期間を徒過した場合にも、固有情報は一致しなくなるため、暗号化済アプリケーション情報も変化する。これは、有効期間の情報そのものが、暗号化されて暗号化済アプリケーション情報に埋め込まれている、と見ることができる。このため、有効期限情報を書き換える不正行為を抑制することができる。

【0118】

本発明では、当該端末装置 601 が有するリアルタイムクロックが計測している日時（典型的には、1970年1月1日0時0分0秒からの経過時間秒数）を有効期間に対応付けられる定数（たとえば、30日間有効とするならば、60日に相当する秒数を採用する等。）で除算して整数化した値が、端末装置 601 の固有情報に反映されるようにしている。

【0119】

本発明では、インストール情報に有効期限を持たせる場合に、日時情報の比較をする必要がないため、不正行為をより一層防止することができるようになる。

【0120】

また、本発明のインストールシステムにおいて、端末装置 601 は、端末装置 601 にインストールされたアプリケーション情報を識別する識別情報を記憶するレジストリ部をさらに備え、固有情報は、レジストリ部に記憶される識別情報を含む情報、もしくは、当該情報のハッシュ値であるように構成することができる。

【0121】

ここで、インストールされたアプリケーション情報とは、プログラムの名称やインストール済のディレクトリ、シリアル番号等の情報である。

【0122】

どのようなアプリケーションをどのようにインストールするかは、端末装置 601 を利用するユーザの利用状況によって大きく変化するため、これらの情報が偶然に一致する可能性は極めて低い。

【0123】

このため、本実施形態によれば、特定の端末装置 601 のみにインストール可能なアプリケーション情報を、適切に提供することができるようになる。

【産業上の利用可能性】

【0124】

以上説明したように、本発明によれば、特定の端末装置のみにインストール可能なアプリケーション情報を適切に提供するインストールシステム、サーバ装置、インストール方法、ならびに、これらをコンピュータにて実現するプログラムを提供することができる。

【符号の説明】

【0125】

- 100 情報処理装置
- 101 CPU
- 102 ROM
- 103 RAM
- 104 インターフェース
- 105 コントローラ
- 106 外部メモリ
- 107 画像処理部
- 108 DVD-ROMドライブ
- 109 NIC
- 110 音声処理部

10

20

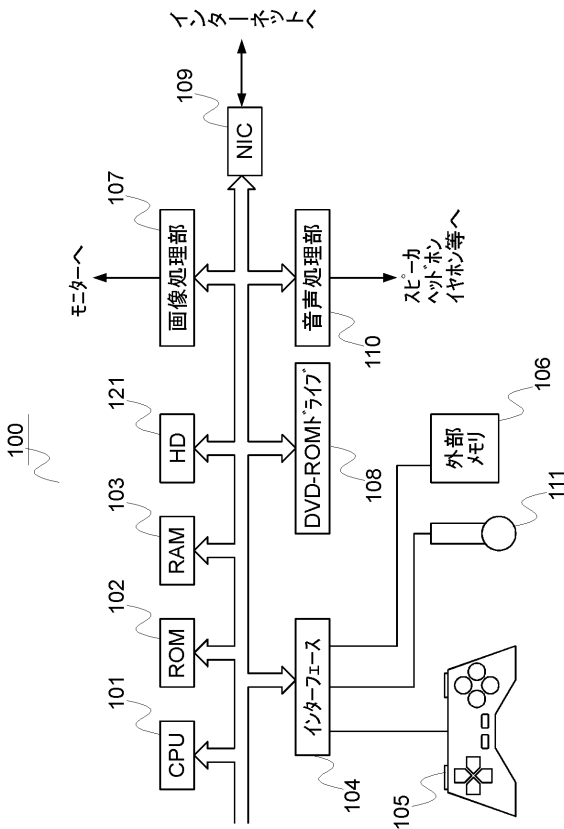
30

40

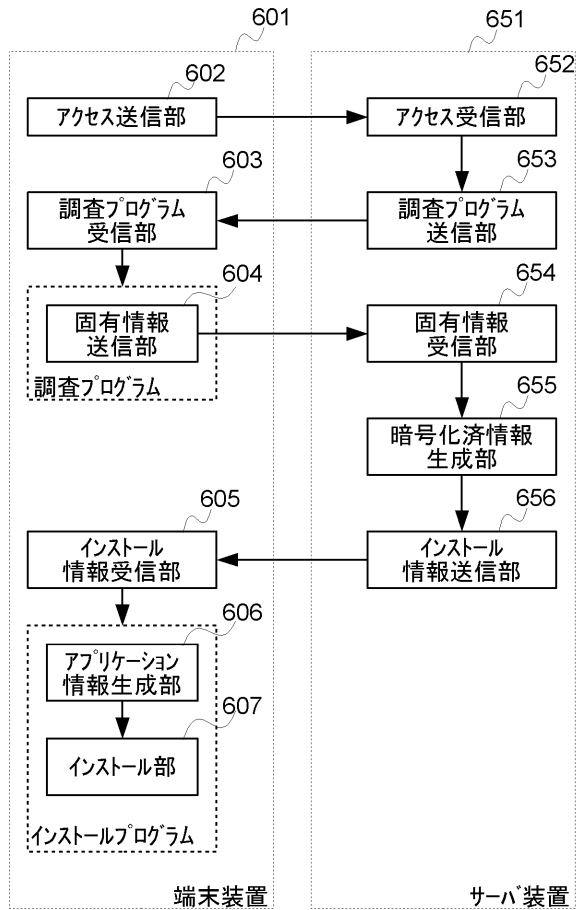
50

- 1 1 1 マイク
- 1 2 1 H D
- 6 0 1 端末装置
- 6 0 2 アクセス送信部
- 6 0 3 調査プログラム受信部
- 6 0 4 固有情報送信部
- 6 0 5 インストール情報受信部
- 6 0 6 アプリケーション情報生成部
- 6 0 7 インストール部
- 6 5 1 サーバ装置
- 6 5 2 アクセス受信部
- 6 5 3 調査プログラム送信部
- 6 5 4 固有情報受信部
- 6 5 5 暗号化済情報生成部
- 6 5 6 インストール情報送信部

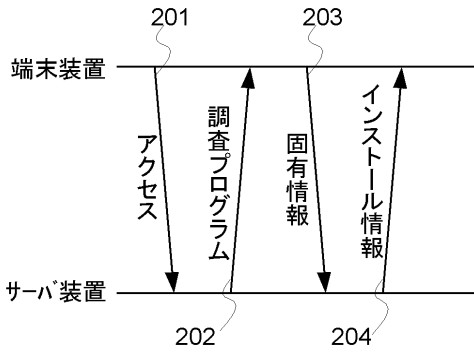
【 図 1 】



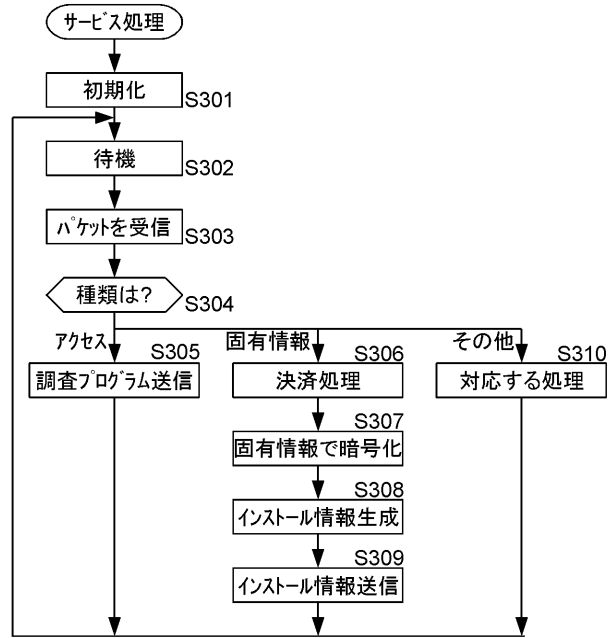
【 図 2 】



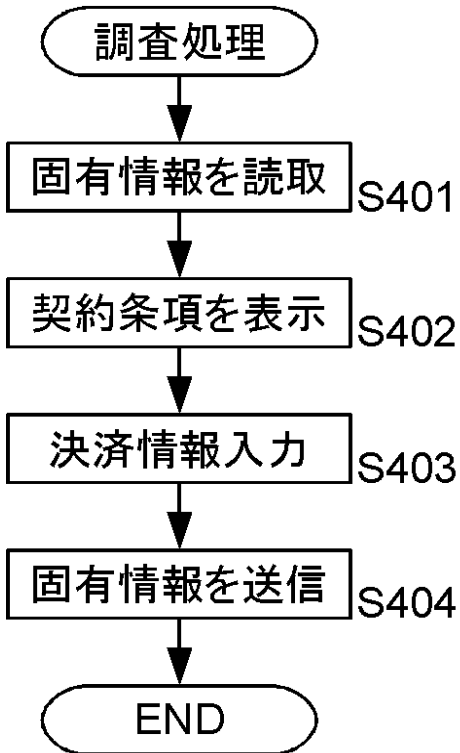
【図3】



【図4】



【図5】



【図6】

