(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4121278号
(P4121278)
(45)発行日　平成20年7月23日(2008.7.23)　(24)登録日　平成20年5月9日(2008.5.9)

(51)Int.Cl.　　F I
G06F 21/22 (2006.01)　　G06F 9/06 660G
G06F 15/00 (2006.01)　　G06F 15/00 310A

請求項の数 5　(全 17 頁)

(21)出願番号　特願2002-7929(P2002-7929)
(22)出願日　平成14年1月16日(2002.1.16)
(65)公開番号　特開2002-318635(P2002-318635A)
(43)公開日　平成14年10月31日(2002.10.31)
審査請求日　平成16年9月22日(2004.9.22)
(31)優先権主張番号　特願2001-11253(P2001-11253)
(32)優先日　平成13年1月19日(2001.1.19)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100098291
弁理士　小笠原　史朗
(72)発明者　稲見　聡
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　水山　正重
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　加藤　淳展
神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内

最終頁に続く

(54)【発明の名称】通信端末

(57)【特許請求の範囲】
【請求項１】
ネットワークを介してサーバとデータの送受信を行う通信端末であって、
アプリケーションの実行と関連づけられるアプリケーションデータを少なくとも含む起動用データの取得要求を前記サーバに対して行う取得要求部と、
前記取得要求に応じて前記サーバから送信されてくる、前記起動用データを受信するデータ受信部と、
アプリケーションと、それに関連づけられる前記アプリケーションデータの認証に用いる認証方式との対応を示すアプリケーション情報を格納するアプリケーション情報格納部と、
前記データ受信部により受信された前記起動用データについて、前記アプリケーション情報に示されている認証方式によってデータ認証を行う認証部と、
前記認証部による認証が成功した場合、当該認証がなされたアプリケーションデータを読み込んで、前記アプリケーションを起動するアプリケーション起動部と、
前記アプリケーションデータに加え、当該アプリケーションデータの認証に用いる認証方式を示す認証タイプデータが前記起動用データに含まれる場合であって、かつ、前記認証部による認証が成功した場合、前記アプリケーション情報格納部に格納されている前記アプリケーション情報の内、前記アプリケーション起動部により起動されたアプリケーションに対応する認証方式を、当該認証がなされた認証タイプデータの示す認証方式に更新するアプリケーション情報更新部とを備える、通信端末。

【請求項２】
前記取得要求部は、Ｗｅｂブラウザを用いて、前記サーバに格納されている前記起動用データを指定することにより、当該起動用データの取得要求を行うことを特徴とする、請求項１に記載の通信端末。
【請求項３】
サーバと、ネットワークを介して当該サーバとデータの送受信を行う通信端末とを含むネットワークシステムであって、
前記サーバは、
アプリケーションの実行と関連づけられるアプリケーションデータを少なくとも含む起動用データを格納する起動用データ格納部と、
前記通信端末から送信されてくる前記起動用データの取得要求に応じて、前記起動用データ格納部に格納されている起動用データを送信するデータ送信部とを備え、
前記通信端末は、
前記起動用データの取得要求を行う取得要求部と、
前記取得要求に応じて前記サーバから送信されてくる起動用データを受信するデータ受信部と、
アプリケーションと、それに関連づけられる前記アプリケーションデータの認証に用いる認証方式との対応を示すアプリケーション情報を格納するアプリケーション情報格納部と、
前記データ受信部により受信された前記起動用データについて、前記アプリケーション情報に示されている認証方式によってデータ認証を行う認証部と、
前記認証部による認証が成功した場合、当該認証がなされた前記アプリケーションデータを読み込んで、前記アプリケーションを起動するアプリケーション起動部と、
前記アプリケーションデータに加え、当該アプリケーションデータの認証に用いる認証方式を示す認証タイプデータが前記起動用データに含まれる場合であって、かつ、前記認証部による認証が成功した場合、前記アプリケーション情報格納部に格納されている前記アプリケーション情報の内、前記アプリケーション起動部により起動されたアプリケーションに対応する認証方式を、当該認証がなされた認証タイプデータの示す認証方式に更新するアプリケーション情報更新部とを備える、ネットワークシステム。
【請求項４】
ネットワークを介してサーバとデータの送受信を行う通信端末において用いられるコンピュータで実行可能なデータ認証プログラムであって、
前記通信端末には、アプリケーションと、それに関連づけられるアプリケーションデータの認証に用いる認証方式との対応を示すアプリケーション情報が予め用意されており、
アプリケーションの実行と関連づけられるアプリケーションデータを少なくとも含む起動用データの取得要求を前記サーバに対して行う取得要求ステップと、
前記取得要求に応じて前記サーバから送信されてくる、前記起動用データを受信するデータ受信ステップと、
前記データ受信ステップで受信された前記起動用データについて、前記アプリケーション情報に示されている認証方式によってデータ認証を行う認証ステップと、
前記認証ステップの認証が成功した場合、当該認証がなされたアプリケーションデータを読み込んで、前記アプリケーションを起動するアプリケーション起動ステップと、
前記アプリケーションデータに加え、当該アプリケーションデータの認証に用いる認証方式を示す認証タイプデータが前記起動用データに含まれる場合であって、かつ、前記認証ステップの認証が成功した場合、前記予め用意されているアプリケーション情報の内、前記アプリケーション起動ステップで起動されたアプリケーションに対応する認証方式を、当該認証がなされた認証タイプデータの示す認証方式に更新するアプリケーション情報更新ステップとを前記コンピュータに実行させる、データ認証プログラム。
【請求項５】
ネットワークを介してサーバとデータの送受信を行う通信端末によって実行されるデー

タ認証方法であって、
前記通信端末には、アプリケーションと、それに関連づけられるアプリケーションデータの認証に用いる認証方式との対応を示すアプリケーション情報が予め用意されており、
アプリケーションの実行と関連づけられるアプリケーションデータを少なくとも含む起動用データの取得要求を前記サーバに対して行う取得要求ステップと、
前記取得要求に応じて前記サーバから送信されてくる、前記起動用データを受信するデータ受信ステップと、
前記データ受信ステップで受信された前記起動用データについて、前記アプリケーション情報に示されている認証方式によってデータ認証を行う認証ステップと、
前記認証ステップの認証が成功した場合、当該認証がなされたアプリケーションデータを読み込んで、前記アプリケーションを起動するアプリケーション起動ステップと、
前記アプリケーションデータに加え、当該アプリケーションデータの認証に用いる認証方式を示す認証タイプデータが前記起動用データに含まれる場合であって、かつ、前記認証ステップの認証が成功した場合、前記予め用意されているアプリケーション情報の内、前記アプリケーション起動ステップで起動されたアプリケーションに対応する認証方式を、当該認証がなされた認証タイプデータの示す認証方式に更新するアプリケーション情報更新ステップとを前記通信端末が実行する、データ認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信端末に関し、より特定的には、通信端末内部のアプリケーションの起動に関連づけられるデータをサーバから取得し、取得したデータについてデータ認証を行う通信端末に関する。

【０００２】

【従来の技術】

従来から、サーバと端末とからなるシステムにおいて、端末のアプリケーションを実行する際に、サーバから端末へデータを送信するシステムが考えられている。例えば、アプリケーションがゲームであって、端末側でゲームを開始するとき、サーバが他のユーザ情報やゲームの設定等のデータを送信するシステムが考えられる。この場合、サーバ側でデータを格納しておき、端末側でゲームを開始するときにデータを入手するので、ユーザは、常に最新のデータでゲームをすることができる。

【０００３】

上記のシステムにおいては、サーバから送信されてくるデータが改ざんされていないかどうかをチェックするため、データ認証を行う必要がある。このようなデータ認証システムにおいて、端末は、電子署名や電子透かしによって、サーバから送信されてきたデータが正しいサーバから送信されたかどうか、データが改ざんされていないかどうか等を判定する。

【０００４】

例えば、データ認証を行うものとして、特開２０００－２２７７５７号公報には、Ｗｅｂページの真正性確認システムが記載されている。上記公報には、Ｗｅｂブラウザによってサーバから取得されるコンテンツについてデータ認証を行うことが記載されている。

【０００５】

【発明が解決しようとする課題】

従来において、データ認証の処理を行うプログラムは、アプリケーションに組み込まれていたり、または、特定のアプリケーションに関連づけられている。従って、アプリケーションとデータ認証処理のプログラムとは一対一に対応するものであり、従来においては、データ認証処理のプログラムとそれを用いるアプリケーションとの関係は、固定的なものであった。

【０００６】

そのため、アプリケーションについて認証方式を変更することは、非常に面倒であった。

例えば、特定のアプリケーションにおいて用いられる認証方式を変更しようとすると、新たに別のデータ認証処理のプログラムをインストールしなければならない。また、データ認証を行うプログラムがアプリケーション内部に組み込まれている場合、アプリケーション自体をインストールし直さなければならない。以上のように、従来のデータ認証システムでは、アプリケーションに対して一度設定された認証方式を変更することは、非常に面倒であった。

【０００７】

それ故に、本発明の目的は、データ認証の方式を容易に変更することが可能なデータ認証システムを提供することである。

【０００８】

【課題を解決するための手段および発明の効果】

第１の発明は、ネットワークを介してサーバとデータの送受信を行う通信端末であって、

アプリケーションの実行と関連づけられるアプリケーションデータを少なくとも含む起動用データの取得要求をサーバに対して行う取得要求部と、

取得要求に応じてサーバから送信されてくる、起動用データを受信するデータ受信部と、

アプリケーションと、それに関連づけられるアプリケーションデータの認証に用いる認証方式との対応を示すアプリケーション情報を格納するアプリケーション情報格納部と、

データ受信部により受信された起動用データについて、アプリケーション情報に示されている認証方式によってデータ認証を行う認証部と、

認証部による認証が成功した場合、認証がなされたアプリケーションデータを読み込んで、アプリケーションを起動するアプリケーション起動部と、

アプリケーションデータに加え、アプリケーションデータの認証に用いる認証方式を示す認証タイプデータが起動用データに含まれる場合であって、かつ、認証部による認証が成功した場合、アプリケーション情報格納部に格納されているアプリケーション情報の内、アプリケーション起動部により起動されたアプリケーションに対応する認証方式を、認証がなされた認証タイプデータの示す認証方式に更新するアプリケーション情報更新部とを備えている。

上記第１の発明によれば、アプリケーションデータとともに、認証タイプデータがサーバから送信される。通信端末は、予め格納されているアプリケーション情報に従って認証を行った結果、認証が成功した場合、認証タイプデータに従いアプリケーション情報を変更する。従って、次回起動用データを受信する際には、認証方式が変更されていることとなる。以上より、上記第１の発明によれば、認証タイプデータによって、認証方式の変更を容易に行うことができる。

【００１３】

第２の発明は、第１の発明に従属する発明であって、

取得要求部は、Ｗｅｂブラウザを用いて、サーバに格納されているアプリケーションデータを指定することにより、アプリケーションデータの取得要求を行う。

【００１４】

上記第２の発明によれば、ユーザは、Ｗｅｂブラウザに対して、リンク情報をクリックする等の単純な動作を行うだけで、サーバに対して取得要求処理を行うことができる。特に通信端末が移動体通信端末の場合、入力装置が簡易であることが多いので、単純な操作によりサーバに対する送信処理が実行可能であることは有効である。

【００１８】

第３の発明は、サーバと、ネットワークを介してサーバとデータの送受信を行う通信端末とを含むネットワークシステムであって、

サーバは、

アプリケーションの実行と関連づけられるアプリケーションデータを少なくとも含む起動用データを格納する起動用データ格納部と、

通信端末から送信されてくる起動用データの取得要求に応じて、起動用データ格納部に格納されている起動用データを送信するデータ送信部とを備え、
通信端末は、
起動用データの取得要求を行う取得要求部と、
取得要求に応じてサーバから送信されてくる起動用データを受信するデータ受信部と、
アプリケーションと、それに関連づけられるアプリケーションデータの認証に用いる認証方式との対応を示すアプリケーション情報を格納するアプリケーション情報格納部と、
データ受信部により受信された起動用データについて、アプリケーション情報に示されている認証方式によってデータ認証を行う認証部と、
認証部による認証が成功した場合、認証がなされたアプリケーションデータを読み込んで、アプリケーションを起動するアプリケーション起動部と、
アプリケーションデータに加え、アプリケーションデータの認証に用いる認証方式を示す認証タイプデータが起動用データに含まれる場合であって、かつ、認証部による認証が成功した場合、アプリケーション情報格納部に格納されているアプリケーション情報の内、アプリケーション起動部により起動されたアプリケーションに対応する認証方式を、認証がなされた認証タイプデータの示す認証方式に更新するアプリケーション情報更新部とを備える、通信端末。

【００２０】

第４の発明は、ネットワークを介してサーバとデータの送受信を行う通信端末において用いられるコンピュータで実行可能なデータ認証プログラムであって、
通信端末には、アプリケーションと、それに関連づけられるアプリケーションデータの認証に用いる認証方式との対応を示すアプリケーション情報が予め用意されており、
アプリケーションの実行と関連づけられるアプリケーションデータを少なくとも含む起動用データの取得要求をサーバに対して行う取得要求ステップと、
取得要求に応じてサーバから送信されてくる、起動用データを受信するデータ受信ステップと、
データ受信ステップで受信された起動用データについて、アプリケーション情報に示されている認証方式によってデータ認証を行う認証ステップと、
認証ステップの認証が成功した場合、認証がなされたアプリケーションデータを読み込んで、アプリケーションを起動するアプリケーション起動ステップと、
アプリケーションデータに加え、アプリケーションデータの認証に用いる認証方式を示す認証タイプデータが起動用データに含まれる場合であって、かつ、認証ステップの認証が成功した場合、予め用意されているアプリケーション情報の内、アプリケーション起動ステップで起動されたアプリケーションに対応する認証方式を、認証がなされた認証タイプデータの示す認証方式に更新するアプリケーション情報更新ステップとをコンピュータに実行させる、データ認証プログラムである。

【００２２】

第５の発明は、ネットワークを介してサーバとデータの送受信を行う通信端末によって実行されるデータ認証方法であって、
通信端末には、アプリケーションと、それに関連づけられるアプリケーションデータの認証に用いる認証方式との対応を示すアプリケーション情報が予め用意されており、
アプリケーションの実行と関連づけられるアプリケーションデータを少なくとも含む起動用データの取得要求をサーバに対して行う取得要求ステップと、
取得要求に応じてサーバから送信されてくる、起動用データを受信するデータ受信ステップと、
データ受信ステップで受信された起動用データについて、アプリケーション情報に示されている認証方式によってデータ認証を行う認証ステップと、
認証ステップの認証が成功した場合、認証がなされたアプリケーションデータを読み込

んで、アプリケーションを起動するアプリケーション起動ステップと、
アプリケーションデータに加え、アプリケーションデータの認証に用いる認証方式を示す認証タイプデータが起動用データに含まれる場合であって、かつ、認証ステップの認証が成功した場合、予め用意されているアプリケーション情報の内、アプリケーション起動ステップで起動されたアプリケーションに対応する認証方式を、認証がなされた認証タイプデータの示す認証方式に更新するアプリケーション情報更新ステップとを通信端末が実行する、データ認証方法である。

【００２３】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を用いて詳細に説明する。図１は、本発明の実施形態に係るデータ認証システムの構成を示すブロック図である。図１において、データ認証システムは、サーバ１と、ネットワーク２と、通信端末３とから構成される。サーバ１と通信端末３とは、ネットワーク２を介して接続されており、相互に通信可能である。なお、ネットワーク２は、有線であっても、無線であってもよい。

【００２４】

図２は、図１に示すサーバ１のハードウェア構成を示すブロック図である。サーバ１は、いわゆるWWW（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）サーバである。図２に示すように、サーバ１は、記憶装置１１と、ＣＰＵ１２と、ＲＡＭ１３と、通信装置１４とを備えている。

【００２５】

記憶装置１１は、ハードディスクドライブやＲＯＭからなり、少なくとも１つのインストールデータ１１１および起動用データ１１２を記憶している。インストールデータ１１１とは、通信端末３がダウンロードしてインストールするプログラムと、プログラムについての情報とを含むデータである。起動用データ１１２は、アプリケーションの起動と関連づけられるデータである。すなわち、起動用データ１１２とは、通信端末３のアプリケーションが起動する際に通信端末３へ送信されるデータである。通信端末３は、アプリケーションを実行する際、起動用データの取得をサーバ１に対して要求する。

【００２６】

また、記憶装置１１は、取得要求処理プログラム１１３を記憶している。取得要求処理プログラム１１３とは、通信端末３によって起動用データ１１２の取得が要求された場合、要求に応じて起動用データ１１２を通信端末３へ送信するためのプログラムである。なお、記憶装置１１は、上記の他にも、本実施形態において必要となる処理を行うために実行されるプログラムを記憶している。

【００２７】

ＣＰＵ１２は、ＲＡＭ１３を作業領域として使いつつ、記憶装置１１に格納されているプログラムを実行する。通信装置１４は、ネットワーク２を通じて通信端末３との間で通信を行う。

【００２８】

図３は、図１に示す通信端末３のハードウェア構成を示すブロック図である。図３のように、通信端末３は、記憶装置３１と、ＣＰＵ３２と、ＲＡＭ３３と、入力装置３４と、表示装置３５と、通信装置３６とを備えている。

【００２９】

記憶装置３１は、Ｗｅｂブラウザ３１１と、アプリケーション３１２と、認証処理プログラム３１３と、アプリケーション起動処理プログラム３１４と、アプリケーション情報テーブル３１５とを記憶している。なお、記憶装置３１は、上記の他にも、本実施形態において必要となる処理を行うために実行されるプログラムを記憶している。

【００３０】

Ｗｅｂブラウザ３１１は、サーバ１が保持しているコンテンツを取得し、表示等の処理を行うためのプログラムである。本実施形態において、通信端末３は、Ｗｅｂブラウザ３１１によってネットワーク２にアクセスし、サーバ１との間でデータの送受信を行う。

【００３１】
アプリケーション３１２は、通信端末３において実行されるプログラムである。なお、記憶装置３１は、アプリケーション３１２の他にも複数のアプリケーションを記憶している。ここで、記憶装置３１に記憶されているアプリケーションは、起動時に何らかのデータをサーバ１から取得する必要があるものとする。例えば、ゲームのアプリケーションであれば、他のユーザの情報、ゲームの難易度等のデータをサーバ１から取得する。また、スケジュール管理のアプリケーションであれば、ユーザのスケジュール情報のデータをサーバ１から取得する。
【００３２】
認証処理プログラム３１３は、サーバ１から送信されてくるデータについて、データ認証を行うためのプログラムである。ここで、データ認証とは、データが改ざんされていないか、および、データ発信元であるサーバが正当なサーバであるかについての認証をいう。なお、記憶装置３１は、認証処理プログラム３１３の他にも複数の認証処理プログラムを記憶している。
【００３３】
アプリケーション起動処理プログラム３１４は、アプリケーションを起動する際の処理を行うためのプログラムである。アプリケーション情報テーブル３１５は、アプリケーションと、アプリケーションの起動時に読み込まれるデータの種別と、アプリケーションを起動する際に行われる認証方式とを対応付けるテーブルである。
【００３４】
ＣＰＵ３２は、ＲＡＭ３３を作業領域として使いつつ、記憶装置３１に格納されているプログラムを実行する。入力装置３４は、例えばキーボードから構成され、アプリケーションの実行等の際にユーザの指示を入力する。表示装置３５は、例えば液晶ディスプレイで構成され、Ｗｅｂブラウザによって取得されるＷｅｂページや、アプリケーションの実行結果等を表示する。通信装置３６は、ネットワーク２を通じてサーバ１との間で通信を行う。
【００３５】
次に、本実施形態に係るデータ認証システムにおける、通信端末３のアプリケーションを実行する動作について説明する。本実施形態において、通信端末３のＣＰＵ３２は、Ｗｅｂブラウザ３１１を実行することによってネットワーク２にアクセスし、サーバ１との間でデータの送受信を行うものとする。従って、アプリケーションの実行時には、Ｗｅｂブラウザ３１１が起動されているものとする。すなわち、アプリケーションの実行動作の開始時には、Ｗｅｂブラウザ３１１によって、サーバ１から受信したＷｅｂページが表示装置３５に表示されている。以下、実行されるアプリケーションがアプリケーション３１２であり、データ認証処理のため認証処理プログラム３１３が実行される場合について説明する。
【００３６】
図４は、図１に示す通信端末３におけるアプリケーションの起動処理を示すフローチャートである。アプリケーションの起動処理は、アプリケーション起動処理プログラム３１４を実行する通信端末３のＣＰＵ３２によって行われる。まず、ＣＰＵ３２は、前述の起動用データの取得をサーバ１に対して要求する（ステップＳ４０１）。起動用データの取得要求は、ユーザが入力装置３４を用いて、Ｗｅｂページ上にリンクとして表示されるアンカー情報を選択することにより行われる。すなわち、ＣＰＵ３２は、ユーザによるアンカー情報の選択操作を契機として、ステップＳ４０１の処理を行う。ここで、ステップＳ４０１における取得要求には、起動用データの位置を示すＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）が含まれている。また、アンカー情報は、Ｗｅｂページ上にアプリケーションの名前として表示されており、そのアプリケーションについての起動用データと関連づけられているものとする。
【００３７】
ステップＳ４０１における取得要求は、通信装置３６によってネットワーク２を介してサ

ーバ１へ送信される。サーバ１で受信された取得要求は、通信装置１４によってＣＰＵ１２に転送される。これにより、ＣＰＵ１２は、通信端末３からの取得要求に対する処理を開始する。

【００３８】

図５は、図２に示すＣＰＵ１２の、取得要求に対する処理の流れを示すフローチャートである。取得要求に対する処理は、取得要求処理プログラム１１３を実行するサーバ１のＣＰＵ１２によって行われる。まず、ＣＰＵ１２は、上記の取得要求を受信する（ステップＳ５１）。次に、ＣＰＵ１２は、取得要求を行った通信端末３に対して送信すべき起動用データを決定する（ステップＳ５２）。前述のように、サーバ１の記憶装置１１には、アプリケーションに対応する起動用データが予め格納されている。ステップＳ５２において、送信すべき起動用データは、記憶装置１１に記憶されている起動用データの中から、取得要求に含まれているＵＲＬに基づいて決定される。以下に起動用データの具体例を説明する。

【００３９】

図６は、本実施形態における起動用データの一例を示す図である。図６において、起動用データ１１２は、アプリケーションデータ１１２１と、アプリケーションデータについての署名１１２２と、認証タイプデータ１１２３と、認証タイプデータについての署名１１２４と、公開鍵１１２５を含んでいる。アプリケーションデータ１１２１とは、アプリケーション３１２を起動する際にアプリケーション３１２に読み込まれるデータである。アプリケーションデータ１１２１の具体例として、例えば、アプリケーション３１２がゲームの場合、他のユーザの情報、ゲームの難易度等が考えられる。また、アプリケーションデータ１１２１は、アプリケーション３１２がスケジュール管理ソフトである場合、ユーザのスケジュール情報であってもよい。アプリケーションデータについての署名１１２２は、サーバ１から送信されてきたアプリケーションデータ１１２１が改ざんされたものでないことを証明するものである。なお、アプリケーションデータについての署名１１２２は、サーバ１においてアプリケーションデータ１１２１のハッシュ値を計算したものである。また、アプリケーションデータについての署名１１２２は、暗号化されて送信される。

【００４０】

認証タイプデータ１１２３とは、アプリケーションデータ１１２１の認証方式を示すデータである。上記のアプリケーションデータ１１２１は、認証タイプデータ１１２３により示される認証方式に適合した暗号化等が行われている。認証タイプデータについての署名１１２４とは、サーバ１から送信されてきた認証タイプデータ１１２３が改ざんされたものでないことを証明するものである。認証タイプデータについての署名１１２４は、サーバ１において認証タイプデータのハッシュ値を計算したものである。また、認証タイプデータについての署名１１２４は、暗号化されて送信される。

【００４１】

ここで、アプリケーションデータ１１２１の認証方式は、認証タイプデータ１１２３によって変更されるものであるのに対して、認証タイプデータ１１２３の認証方式は、予め定められている点で異なっている。なお、ここでは、認証タイプデータ１１２３は、公開鍵暗号方式を用いた署名を行うことを示すものとする。従って、起動用データ１１２には、暗号解読に必要な公開鍵１１２５が含まれている。

【００４２】

図５の説明に戻り、ステップＳ５２の後、ＣＰＵ１２は、記憶装置１１に記憶されている起動用データ１１２を読み出し、通信端末３へ送信する（ステップＳ５３）。具体的には、ＣＰＵ１２は、起動用データ１１２を通信装置１４に転送する。通信装置１４は、転送された起動用データ１１２を、ネットワーク２を介して通信端末３に対して送信する。

【００４３】

図４の説明に戻り、サーバ１から送信された起動用データ１１２は、通信端末３の通信装置３６によって受信される。ＣＰＵ３２は、通信装置３６から起動用データ１１２を受け

取る（ステップＳ４０２）。具体的には、ＣＰＵ３２は、通信装置３６が受信した起動用データ１１２をＲＡＭ３３に展開する。次に、ＣＰＵ３２は、起動用データ１１２の解析を行う（ステップＳ４０３）。ステップＳ４０３において、ＣＰＵ３２は、起動用データ１１２のどの部分が上記のそれぞれのデータ（アプリケーションデータ１１２１～公開鍵１１２５）にあたるのかを判定する。また、ＣＰＵ３２は、アプリケーションデータ１１２１のファイル種別も判定する。

【００４４】

次に、ＣＰＵ３２は、ステップＳ４０３の解析結果に基づいて、起動用データ１１２に認証タイプデータ１１２３が含まれているかどうかを判定する（ステップＳ４０４）。認証タイプデータ１１２３が含まれていない場合、ＣＰＵ３２は、ステップＳ４０７の処理を行う。一方、認証タイプデータ１１２３が含まれている場合、ＣＰＵ３２は、認証タイプデータ１１２３についてデータ認証を行う（ステップＳ４０５）。

【００４５】

図７は、図４のサブルーチンステップＳ４０５の詳細を示すフローチャートである。図７に示すデータ認証処理は、記憶装置３１に記憶されている認証処理プログラムから、予め定められた一の認証処理プログラムをＣＰＵ３２が実行することにより行われる。まず、ＣＰＵ３２は、認証タイプデータ１１２３のハッシュ値を算出する（ステップＳ４５０１）。ここで、ハッシュ値を算出するためのハッシュ関数は、サーバ１において認証タイプデータ１１２３についての署名を算出する際に用いられるものと同一のものである。次に、ＣＰＵ３２は、認証タイプデータについての署名１１２４を復号化する（ステップＳ４５０２）。

【００４６】

次に、ＣＰＵ３２は、ステップＳ４５０１において算出したハッシュ値と、ステップＳ４５０２において復号化された署名とを比較する（ステップＳ４５０３）。ステップＳ４５０３は、認証タイプデータ１１２３が改ざんされていないかどうか、すなわち、通信端末３で受信した認証タイプデータが、サーバ１から送信された認証タイプデータと一致するか否かについて判定するものである。このように、サーバ１において認証タイプデータ１１２３のハッシュ値を計算した結果である署名と、通信端末３において認証タイプデータ１１２３のハッシュ値の計算結果とを比較することにより、認証タイプデータ１１２３が改ざんされていないかどうかを判断することができる。

【００４７】

次に、ＣＰＵ３２は、ステップＳ４５０３の比較の結果、上記のハッシュ値と署名とが一致するか否かを判定する（ステップＳ４５０４）。ハッシュ値と署名とが一致する場合、ＣＰＵ３２は、データ認証が成功したものと判断して（ステップＳ４５０５）、処理を終了する。一方、ハッシュ値と署名とが一致しない場合、ＣＰＵ３２は、データ認証が失敗したものと判断して（ステップＳ４５０６）、処理を終了する。

【００４８】

再び図４の説明に戻り、ＣＰＵ３２は、ステップＳ４０５のデータ認証処理が成功したか否かを判定する（ステップＳ４０６）。データ認証処理が失敗した場合、ＣＰＵ３２は、ステップＳ４１０の処理を行う。一方、データ認証処理が成功した場合、ＣＰＵ３２は、アプリケーションデータについてデータ認証を行う（ステップＳ４０７）。

【００４９】

図８は、図４のサブルーチンステップＳ４０７の詳細を示すフローチャートである。まず、ＣＰＵ３２は、認証方式を決定する（ステップＳ４７０１）。認証方式は、ステップＳ４０４において認証タイプデータが含まれていると判定された場合、その認証タイプデータの示す認証方式に決定される。また、ステップＳ４０４において認証タイプデータが含まれていないと判定された場合、記憶装置３１に格納されているアプリケーション情報テーブル３１５を参照して決定される。

【００５０】

図９は、図３に示すアプリケーション情報テーブル３１５の一例を示す図である。図９の

ように、アプリケーション情報テーブル３１５には、アプリケーション名と、アプリケーションデータのファイル種別と、認証方式とが対応付けて格納されている。前述のように、ステップＳ４０３においてアプリケーションデータのファイル種別が判定される。アプリケーション情報テーブル３１５を参照することによって、ファイル種別に基づいて、実行されるアプリケーションおよびアプリケーションデータの認証方式を決定することができる。例えば、アプリケーションデータのファイル種別が“Ｃ”で表現されるものである場合、起動するアプリケーションは名前が“Ａ１”のアプリケーションに決定され、認証方式はＤＥＳ暗号を用いたものに決定される。

【００５１】

以上のようにステップＳ４７０１の認証方式の決定が行われ、続いて、ステップＳ４７０２～Ｓ４７０７の処理が行われる。ステップＳ４７０２～ステップＳ４７０７の一連のデータ認証処理は、記憶装置３１に記憶されている認証処理プログラムの内、ステップＳ４７０１によって決定された認証方式に対応する認証処理プログラムをＣＰＵ３２が実行することにより行われる。

【００５２】

図８の説明に戻り、ＣＰＵ３２は、アプリケーションデータ１１２１のハッシュ値を算出する（ステップＳ４７０２）。ここで、ハッシュ値を算出するためのハッシュ関数は、サーバ１においてアプリケーションデータ１１２１についての署名を算出する際に用いられるものと同一のものである。次に、ＣＰＵ３２は、アプリケーションデータについての署名１１２２を復号化する（ステップＳ４７０３）。ステップＳ４０７３において、アプリケーションデータについての署名１１２２は、公開鍵暗号方式により暗号化されているので、公開鍵１１２５を用いて復号化される。次に、ＣＰＵ３２は、ステップＳ４７０２において算出したハッシュ値と、ステップＳ４７０３において復号化された署名とを比較する（ステップＳ４７０４）。最後に、ＣＰＵ３２は、ステップＳ４７０４の比較の結果、上記のハッシュ値と署名とが一致するか否かを判定する（ステップＳ４７０５）。ハッシュ値と署名とが一致する場合、ＣＰＵ３２は、データ認証が成功したものと判断して（ステップＳ４７０６）、処理を終了する。一方、ハッシュ値と署名とが一致しない場合、ＣＰＵ３２は、データ認証が失敗したものと判断して（ステップＳ４７０７）、処理を終了する。

【００５３】

再び図４の説明に戻り、ＣＰＵ３２は、ステップＳ４０７のデータ認証処理が成功したか否かを判定する（ステップＳ４０８）。データ認証処理が成功した場合、ＣＰＵ３２は、アプリケーションを起動して（ステップＳ４０９）、処理を終了する。なお、ステップＳ４０９において、ＣＰＵ３２は、アプリケーション情報テーブル３１５の内容を認証タイプデータ１１２３に基づいて変更してもよい。この場合、次回に起動用データが送信される際の認証方式が変更されることとなる。一方、データ認証処理が失敗した場合、ＣＰＵ３２は、起動用データを破棄して（ステップＳ４１０）、処理を終了する。以上の処理により、アプリケーションの起動処理が完了する。

【００５４】

なお、本実施形態においては、起動用データに含まれるアプリケーションデータと、認証タイプデータとのそれぞれについて、独立して認証を行うこととした。ここで、他の実施形態においては、起動用データに認証タイプデータが含まれている場合、次回に送信される起動用データについて、認証方式を変更するようにしてもよい。以下、アプリケーションの起動処理の他の例を説明する。

【００５５】

図１０は、図４に示すアプリケーションの起動処理の変形例を示すフローチャートである。ここで、ステップＳ６０１～Ｓ６０３については、図４のステップＳ４０１～Ｓ４０３の処理と同様であるので、説明を省略する。図１０において、ステップＳ６０３の後、ＣＰＵ３２は、データ認証を行う（ステップＳ６０４）。ここで、本変形例においては、起動用データ全体についてデータ認証を行う。データ認証の方式は、アプリケーション情報

テーブルに基づいて決定される。すなわち、ステップＳ６０４のデータ認証における認証方式は、起動用データに含まれている認証タイプデータにより示される方式とは無関係である。

【００５６】

ＣＰＵ３２は、ステップＳ４０５のデータ認証処理が成功したか否かを判定する（ステップＳ６０５）。データ認証処理が成功した場合、ＣＰＵ３２は、アプリケーションを起動する（ステップＳ６０６）。さらに、ＣＰＵ３２は、アプリケーション情報テーブルを更新して（ステップ６０７）、処理を終了する。具体的には、ＣＰＵ３２は、起動用データに含まれている認証タイプデータにより示される認証方式に、アプリケーション情報テーブルの内容を更新する。より具体的には、アプリケーション情報テーブルにおける、ステップＳ６０６において起動されたアプリケーションに対応する認証方式が更新される。一方、ステップＳ６０５において、データ認証処理が失敗した場合、ＣＰＵ３２は、起動用データを破棄して（ステップＳ６０８）、処理を終了する。以上の処理により、アプリケーションの起動処理が完了する。なお、図１０に示す処理では、次回に起動用データが送信されたとき、認証方式が変更されていることとなる。

【００５７】

なお、起動用データ１１２は、どのような形式で記述されてもよく、ハイパーテキスト、ＸＭＬ（ｅＸｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）形式、または、ＳＧＭＬ（Ｓｔａｎｄａｒｄ Ｇｅｎｅｒａｌｉｚｅｄ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）等を用いて記述してもよい。あるいは、単にテーブルを用いて記述してもよい。

【００５８】

なお、本実施例においては、認証方式として公開鍵暗号方式による方式を挙げたが、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）等、他の暗号方式を用いてもよい。また、認証方式は、データ認証を行うものであればよく、署名によるものであってもよいし、電子透かしや証明書によるものであってもよい。ここで、データ認証とは、データが改ざんされていないか、および、データ発信元であるサーバが正当なサーバであるかについての認証をいう。

【００５９】

なお、本実施形態において、通信端末３は、アプリケーションをサーバ１からインストールする。以下、通信端末３におけるアプリケーションを組み込む際の動作を説明する。

【００６０】

図１１は、通信端末３におけるアプリケーションの組み込み処理の流れを示すフローチャートである。なお、アプリケーションの組み込み処理時には、Ｗｅｂブラウザが起動されているものとする。すなわち、アプリケーションの実行動作の開始時には、Ｗｅｂブラウザによって、サーバ１から受信したＷｅｂページが表示装置３５に表示されていることが前提となる。

【００６１】

まず、通信端末３のＣＰＵ３２は、インストールデータ１１１の送信をサーバ１に対して要求する（ステップＳ７０１）。インストールデータ１１１の送信要求は、ユーザが入力装置３４を用いて、Ｗｅｂページ上にリンクとして表示されるアンカー情報を選択することにより行われる。すなわち、ＣＰＵ３２は、ユーザによるアンカー情報の選択操作を契機として、ステップＳ７０１の処理を行う。ここで、ステップＳ７０１における送信要求には、サーバ１に記憶されているアプリケーションプログラム１１１１の位置を示すＵＲＬが含まれている。また、アンカー情報は、Ｗｅｂページ上にアプリケーションの名前として表示されているものとする。

【００６２】

ステップＳ７０１における送信要求は、ネットワーク２を介して、サーバ１により受信される。サーバ１の通信装置１４は、ネットワーク２から受信した送信要求をＣＰＵ１２に転送する。ＣＰＵ１２は、送信要求を受信すると、送信要求に含まれるＵＲＬに基づいて、送信すべきインストールデータの内容を決定する。本実施形態では、インストールデー

タ１１１が送信すべきインストールデータであるとする。

【００６３】

図１２は、図１に示すインストールデータ１１１の一例を示す図である。図１２において、インストールデータ１１１は、アプリケーションプログラム１１１１と、認証タイプデータ１１１２と、ファイル種別データ１１１３とを含んでいる。アプリケーションプログラム１１１１は、通信端末３においてインストールされるアプリケーションのプログラムである。認証タイプデータ１１１２は、アプリケーションプログラム１１１１を起動する場合に行われる認証の方式を示す。ファイル種別データ１１１３は、アプリケーションプログラム１１１１を起動する際に読み込まれるアプリケーションデータのファイルの種類を示す。本実施形態において、インストールデータ１１１の内容は、サーバ１の記憶装置１１において予め記憶されているテーブルを参照することによって決定される。ここで、テーブルは、アプリケーションプログラムと、認証タイプデータと、ファイル種別データとを対応付けて格納するものとする。また、インストールデータ１１１は、専用のプログラムを実行することにより、生成されてもよい。プログラムは、例えば、アプリケーションプログラムに、それに対応する認証タイプデータおよびファイル種別データを結合してインストールデータを生成する処理を行うものである。

【００６４】

ＣＰＵ１２は、上記のように決定されたインストールデータ１１１を記憶装置１１から読み出し、通信装置１４に転送する。通信装置１４は、転送されたインストールデータ１１１を、ネットワーク２に送出する。

【００６５】

サーバ１から送信されたインストールデータ１１１は、ネットワーク２を経由して通信端末３の通信装置３６により受信される。通信装置３６は、受信したデータをＲＡＭ３３に展開する。これによって、ＣＰＵ３２は、インストールデータ１１１の解析を行う（ステップＳ７０２）。ＣＰＵ３２は、インストールデータ１１１からどの部分が上記のそれぞれのデータ（アプリケーションプログラム１１１１、認証タイプデータ１１１２、ファイル種別データ１１１３）にあたるのかを判定する。

【００６６】

次に、ＣＰＵ３２は、インストールデータ１１１に含まれるアプリケーションプログラム１１１１を記憶装置３１に保存する（ステップＳ７０３）。さらに、アプリケーションプログラム１１１１以外の認証タイプデータ１１１２およびファイル種別データ１１１３をアプリケーション情報テーブル３１５に保存する（ステップＳ７０４）。以上の動作により、通信端末３にアプリケーションプログラム１１１１がインストールされる。

【００６７】

なお、サーバから通信端末へ送信されるインストールデータについても、起動用データと同様、データ認証が行われることが好ましい。データ認証の方式は、図４のステップＳ４０５における認証タイプデータについての認証方式と同様、予め定められた固定的なものであってもよいし、図１０のステップＳ６０４における起動用データについての認証方式と同様、変更可能なものであってもよい。

【００６８】

以上のように、アプリケーションをインストールする場合においても、アプリケーションとデータ認証処理を行うプログラムとを分割することができる。従って、端末にインストールされる前に、サーバ側でアプリケーションに対応するデータ認証処理の方式を変更する場合においても、変更を容易に行うことができる。

【００６９】

なお、インストールデータ１１１は、１つのファイルとして説明したが、アプリケーションプログラム１１１１と、認証タイプデータ１１１２およびファイル種別データ１１１３とを別のファイルに記述し、別個のファイルとしてインストール処理を行ってもよい。

【００７０】

なお、通信端末３におけるアプリケーションのインストール方法は、サーバからダウンロ

ードする方法の他、ＣＤ－ＲＯＭ等の記録媒体からインストールされる形態であってもよい。

【００７１】

また、本発明は、プログラムによって実現することが可能であり、これを記録媒体に記録して移送することにより、独立した他のコンピュータシステムで容易に実施することができる。

【図面の簡単な説明】

【図１】本発明の実施形態に係るデータ認証システムの構成を示すブロック図である。

【図２】図１に示すサーバ１のハードウェア構成を示すブロック図である。

【図３】図１に示す通信端末３のハードウェア構成を示すブロック図である。

【図４】図１に示す通信端末３におけるアプリケーションの起動処理を示すフローチャートである。

【図５】図２に示すＣＰＵ１２の、取得要求に対する処理の流れを示すフローチャートである。

【図６】本実施形態における起動用データの一例を示す図である。

【図７】図４のサブルーチンステップＳ４０５の詳細を示すフローチャートである。

【図８】図４のサブルーチンステップＳ４０７の詳細を示すフローチャートである。

【図９】図３に示すアプリケーション情報テーブルの一例を示す図である。

【図１０】図４に示すアプリケーションの起動処理の変形例を示すフローチャートである。

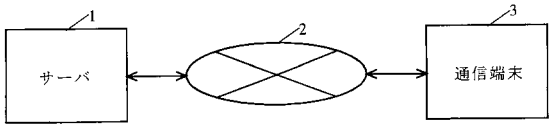
【図１１】通信端末３におけるアプリケーションの組み込み処理の流れを示すフローチャートである。

【図１２】図１に示すインストールデータ１１１の一例を示す図である。

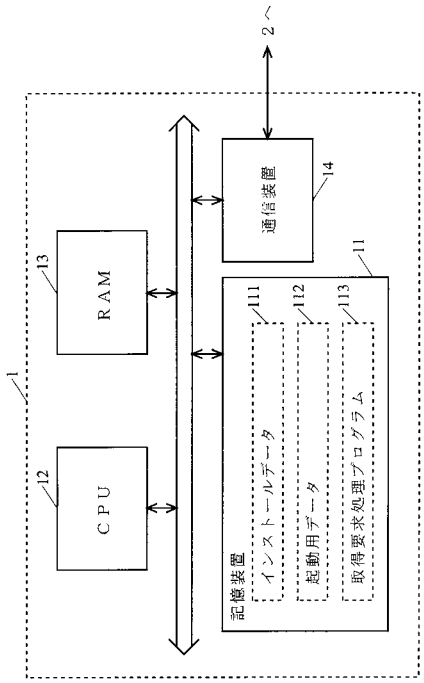
【符号の説明】

１　サーバ
２　ネットワーク
３　通信端末
１１，３１　記憶装置
１２，３２　ＣＰＵ
１３，３３　ＲＡＭ
１４，３６　通信装置
３４　入力装置
３５　表示装置
１１１　インストールデータ
１１２　起動用データ
１１３　取得要求処理プログラム
３１１　Ｗｅｂブラウザ
３１２　アプリケーション
３１３　認証処理プログラム
３１４　起動処理プログラム
３１５　アプリケーション情報テーブル
１１１１　アプリケーションプログラム
１１１２，１１２３　認証タイプデータ
１１１３　ファイル種別データ
１１２１　アプリケーションデータ
１１２２　アプリケーションデータについての署名
１１２４　認証タイプデータについての署名
１１２５　公開鍵

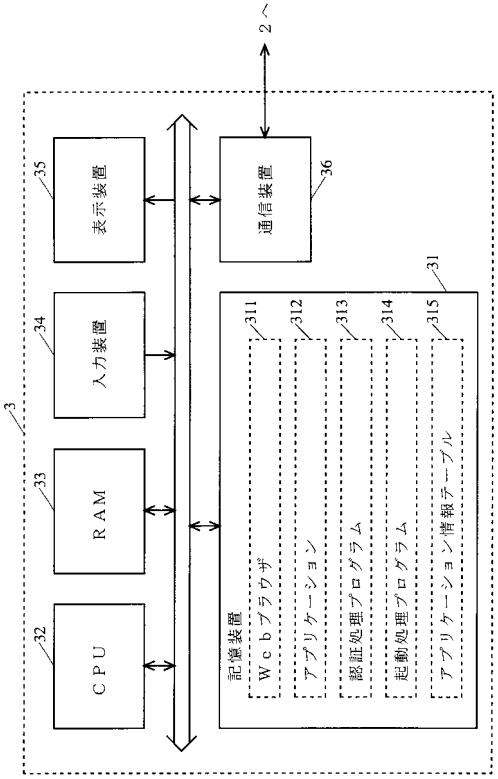
【図１】


1
サーバ
2
3
通信端末

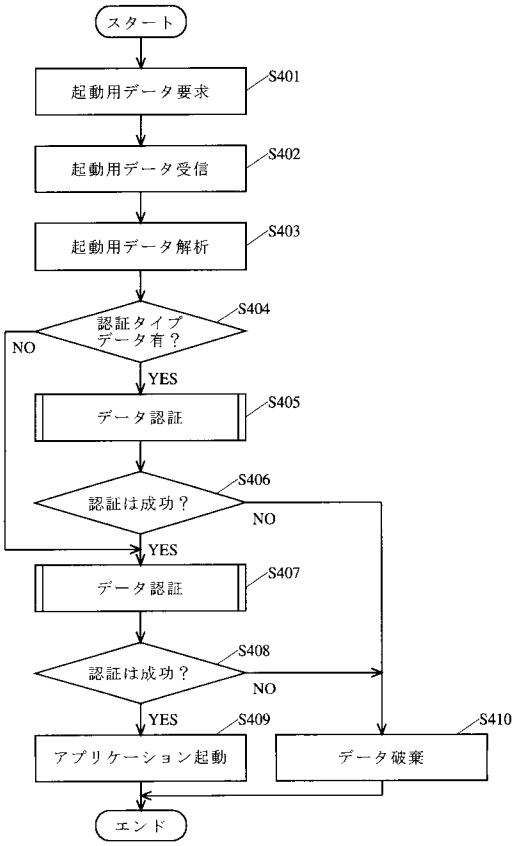
【図２】


2へ
通信装置
14
RAM
13
CPU
12
11
記憶装置
111
インストールデータ
112
起動用データ
113
取得要求処理プログラム
1

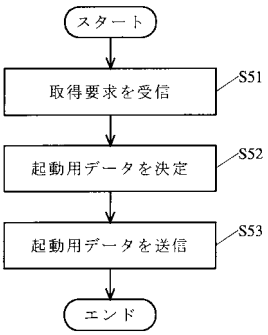
【図３】


2へ
表示装置
35
通信装置
36
入力装置
34
RAM
33
CPU
32
3
31
記憶装置
311
Webブラウザ
312
アプリケーション
313
認証処理プログラム
314
起動処理プログラム
315
アプリケーション情報テーブル

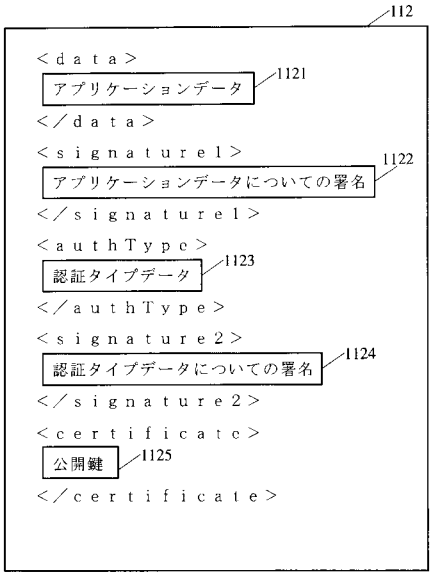
【図４】


スタート
起動用データ要求
S401
起動用データ受信
S402
起動用データ解析
S403
認証タイプデータ有？
S404
NO
YES
データ認証
S405
認証は成功？
S406
NO
YES
データ認証
S407
認証は成功？
S408
NO
YES
S409
アプリケーション起動
S410
データ破棄
エンド

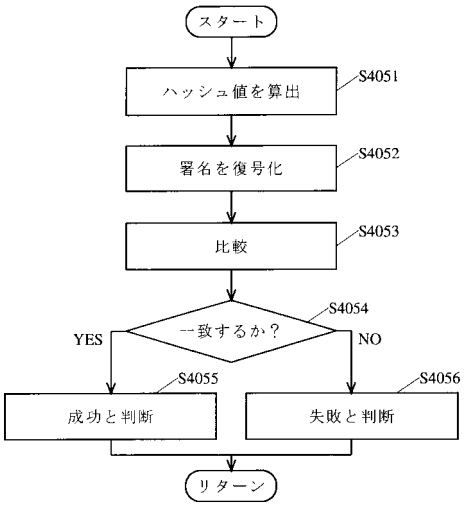
【図５】


スタート
取得要求を受信
S51
起動用データを決定
S52
起動用データを送信
S53
エンド

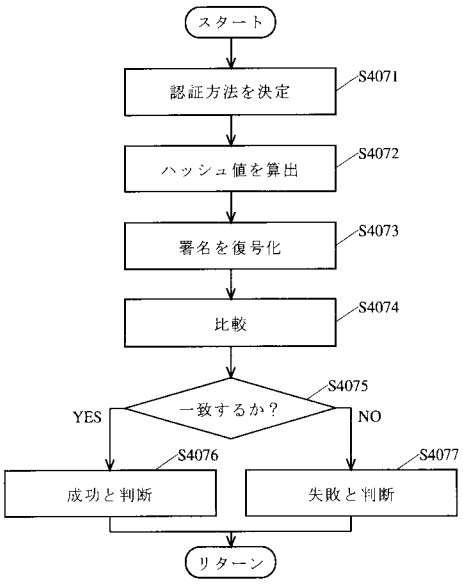
【図６】



【図７】



【図８】

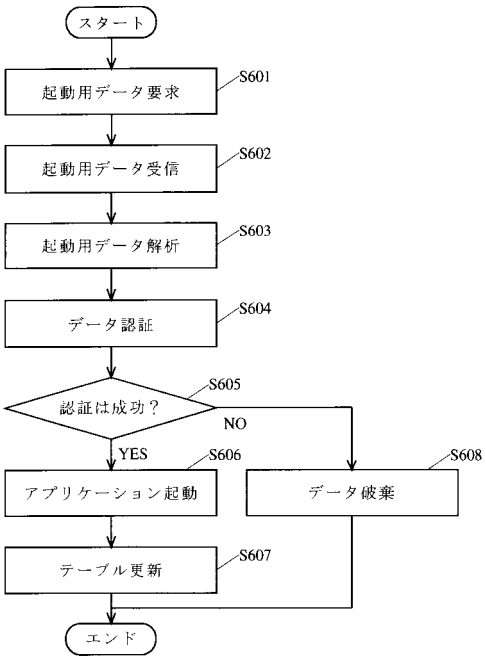


【図９】

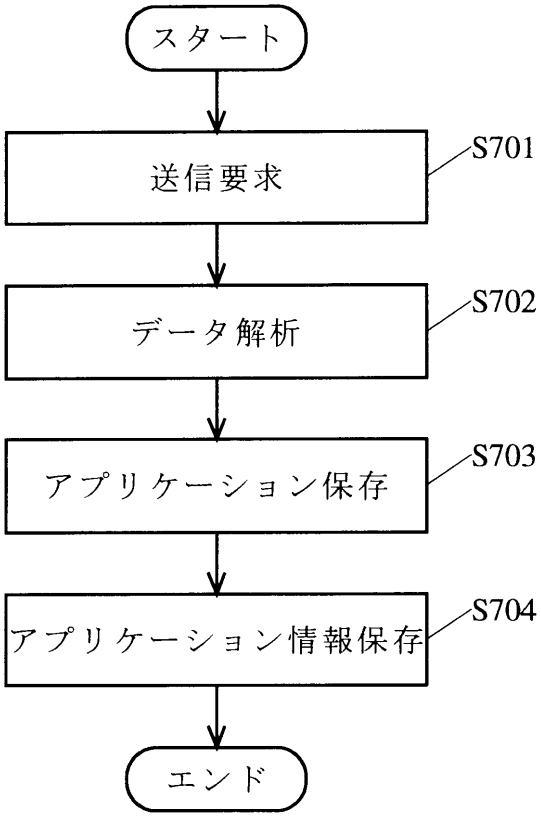
315

アプリケーション名	種別	認証方式
Ａ１	Ｃ	ＤＥＳ暗号
Ａ２	Ｐ	証明書
Ａ３	Ｊ	電子透かし
・ ・ ・	・ ・ ・	・ ・ ・

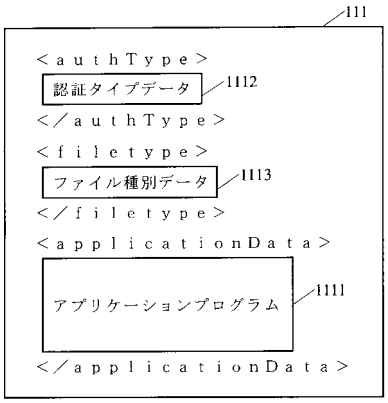
【図１０】



【図１１】


スタート
送信要求
S701
データ解析
S702
アプリケーション保存
S703
アプリケーション情報保存
S704
エンド

【図１２】


111
<authType>
認証タイプデータ
1112
</authType>
<filetype>
ファイル種別データ
1113
</filetype>
<applicationData>
アプリケーションプログラム
1111
</applicationData>

フロントページの続き

審査官　小林　秀和

(56)参考文献　国際公開第９８／０２１６８３（WO，Ａ１）
特開２０００－１６３３７９（ＪＰ，Ａ）
欧州特許出願公開第００８１１９４２（ＥＰ，Ａ１）
国際公開第９８／０５４６４４（WO，Ａ１）
David Walker, “A Type System for Expressive Security Policies”, Proceedings of the 27th ACM SIGPLAN-SIGACT symposium on Principles of programming languages, 米国, ACM, ２０００年, p.254-p.267, ISBN: 1-58113-125-9

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/22
G06F 15/00