(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5429880号
(P5429880)

(45)発行日　平成26年2月26日(2014.2.26)　(24)登録日　平成25年12月13日(2013.12.13)

(51)Int.Cl.		F I		
G06F 21/44	(2013.01)	G06F	21/20	144B
G06F 11/00	(2006.01)	G06F	9/06	630B
G06F 9/445	(2006.01)	G06F	9/06	610L
G06F 21/33	(2013.01)	G06F	21/20	144C
		G06F	21/20	133

請求項の数 8　(全 18 頁)

(21)出願番号　特願2010-179404 (P2010-179404)
(22)出願日　平成22年8月10日 (2010.8.10)
(65)公開番号　特開2012-38193 (P2012-38193A)
(43)公開日　平成24年2月23日 (2012.2.23)
審査請求日　平成23年8月9日 (2011.8.9)

(73)特許権者　306029774
ＮＥＣビッグローブ株式会社
東京都品川区大崎一丁目１１番１号
(74)代理人　100123788
弁理士　宮崎　昭夫
(74)代理人　100106138
弁理士　石橋　政幸
(74)代理人　100127454
弁理士　緒方　雅昭
(72)発明者　榎本　敦之
東京都品川区大崎一丁目１１番１号　ＮＥＣビッグローブ株式会社内
(72)発明者　芳賀　康平
東京都品川区大崎一丁目１１番１号　ＮＥＣビッグローブ株式会社内

最終頁に続く

(54)【発明の名称】アプリケーション配布システム、アプリケーション配布方法、端末及びプログラム

(57)【特許請求の範囲】
【請求項１】
インストールされた実行ファイルを実行することによってアプリケーションを起動する端末と、前記実行ファイルに対する更新用の実行ファイルである更新用実行ファイルを前記端末に配布するアプリ配布サーバと、アプリケーションが通信を行うアプリ通信サーバとを有するアプリケーション配布システムであって、
前記端末にプリインストールされた実行ファイルには、前記アプリ通信サーバとの通信時に、前記アプリ通信サーバにアクセスできる端末であることを示す証明書データが内蔵されており、
前記更新用実行ファイルには、前記証明書データが内蔵されておらず、
前記端末は、前記アプリケーションの初回起動時に、前記アプリケーションが、前記プリインストールされた実行ファイル内の証明書データを、特定のアプリケーションからのアクセスでファイルを格納したり読み出したりすることができるアクセス制限がかかった第１の記憶領域に証明書ファイルとして格納しておき、その後、前記アプリ配布サーバから前記更新用実行ファイルが配布された場合、前記プリインストールされた実行ファイルを前記アプリ配布サーバから配布された前記更新用実行ファイルに書き換え、前記証明書データが内蔵されていない前記更新用実行ファイルを実行することによって前記アプリケーションが起動された際に、前記アプリケーションが、前記第１の記憶領域に格納された証明書ファイルを読み出して前記アプリ通信サーバとの通信に用いるアプリケーション配布システム。

【請求項２】
請求項１に記載のアプリケーション配布システムにおいて、
更に、開発者端末を有し、
前記端末は、
前記開発者端末から提供される前記証明書データを含む実行ファイルが含まれるインストールパッケージファイルが格納される第２の記憶領域と、
前記第２の記憶領域に格納されたインストールパッケージファイルのインストール時に、前記第２の記憶領域に格納されたインストールパッケージファイルから取り出した前記実行ファイルが格納される第３の記憶領域とを有し、
前記第３の記憶領域に格納された実行ファイルを実行することによるアプリケーションの初回起動時に、前記アプリケーションが、前記第３の記憶領域に格納された実行ファイル内の証明書データを前記証明書ファイルとして前記第１の記憶領域に格納するアプリケーション配布システム。
【請求項３】
インストールされた実行ファイルを実行することによってアプリケーションを起動する端末と、前記実行ファイルに対する更新用の実行ファイルである更新用実行ファイルを前記端末に配布するアプリ配布サーバと、アプリケーションが通信を行うアプリ通信サーバとを有するアプリケーション配布システムにおけるアプリケーション配布方法であって、
前記端末にプリインストールされた実行ファイルには、前記アプリ通信サーバとの通信時に、前記アプリ通信サーバにアクセスできる端末であることを示す証明書データが内蔵されており、
前記更新用実行ファイルには、前記証明書データが内蔵されておらず、
前記端末が、前記アプリケーションの初回起動時に、前記アプリケーションによって、前記プリインストールされた実行ファイル内の証明書データを、特定のアプリケーションからのアクセスでファイルを格納したり読み出したりすることができるアクセス制限がかかった第１の記憶領域に証明書ファイルとして格納しておく処理と、
前記アプリ配布サーバが、前記更新用実行ファイルを前記端末に配布する処理と、
前記端末が、前記プリインストールされた実行ファイルを前記アプリ配布サーバから配布された前記更新用実行ファイルに書き換える処理と、
前記端末が、前記証明書データが内蔵されていない前記更新用実行ファイルを実行することによって前記アプリケーションが起動された際に、前記アプリケーションによって、前記第１の記憶領域に格納された証明書ファイルを読み出して前記アプリ通信サーバとの通信に用いる処理とを有するアプリケーション配布方法。
【請求項４】
請求項３に記載のアプリケーション配布方法において、
前記端末が、開発者端末から提供された前記証明書データを含む実行ファイルが含まれるインストールパッケージファイルを第２の記憶領域に格納しておく処理と、
前記端末が、前記第２の記憶領域に格納されたインストールパッケージファイルのインストール時に、前記第２の記憶領域に格納されたインストールパッケージファイルから取り出した前記実行ファイルを第３の記憶領域に格納する処理と、
前記端末が、前記第３の記憶領域に格納された実行ファイルを実行することによるアプリケーションの初回起動時に、前記アプリケーションによって、前記第３の記憶領域に格納された実行ファイル内の証明書データを前記証明書ファイルとして前記第１の記憶領域に格納する処理とを有するアプリケーション配布方法。
【請求項５】
インストールされた実行ファイルを実行することによってアプリケーションを起動する端末であって、
前記端末にプリインストールされた実行ファイルには、アプリケーションが通信を行うアプリ通信サーバとの通信時に、前記アプリ通信サーバにアクセスできる端末であることを示す証明書データが内蔵されており、

アプリ配布サーバから配布される、前記実行ファイルに対する更新用の実行ファイルである更新用実行ファイルには、前記証明書データが内蔵されておらず、
前記アプリケーションの初回起動時に、前記アプリケーションが、前記プリインストールされた実行ファイル内の証明書データを、特定のアプリケーションからのアクセスでファイルを格納したり読み出したりすることができるアクセス制限がかかった第１の記憶領域に証明書ファイルとして格納しておき、その後、前記アプリ配布サーバから前記更新用実行ファイルが配布された場合、前記プリインストールされた実行ファイルを前記アプリ配布サーバから配布された前記更新用実行ファイルに書き換え、前記証明書データが内蔵されていない前記更新用実行ファイルを実行することによって前記アプリケーションが起動された際に、前記アプリケーションが、前記第１の記憶領域に格納された証明書ファイルを読み出して前記アプリ通信サーバとの通信に用いる端末。
【請求項６】
請求項５に記載の端末において、
開発者端末から提供される前記証明書データを含む実行ファイルが含まれるインストールパッケージファイルが格納される第２の記憶領域と、
前記第２の記憶領域に格納されたインストールパッケージファイルのインストール時に、前記第２の記憶領域に格納されたインストールパッケージファイルから取り出した前記実行ファイルが格納される第３の記憶領域とを有し、
前記第３の記憶領域に格納された実行ファイルを実行することによるアプリケーションの初回起動時に、前記アプリケーションが、前記第３の記憶領域に格納された実行ファイル内の証明書データを前記証明書ファイルとして前記第１の記憶領域に格納する端末。
【請求項７】
アプリケーションが通信を行うアプリ通信サーバとの通信時に、前記アプリ通信サーバにアクセスできる端末であることを示す証明書データが内蔵された実行ファイルがプリインストールされ、インストールされた実行ファイルを実行することによって前記アプリケーションを起動する端末に、
前記アプリケーションの初回起動時に、前記アプリケーションが、前記プリインストールされた実行ファイル内の証明書データを、特定のアプリケーションからのアクセスでファイルを格納したり読み出したりすることができるアクセス制限がかかった第１の記憶領域に証明書ファイルとして格納しておく手順と、
前記証明書データが内蔵されておらず、前記実行ファイルに対する更新用の実行ファイルである更新用実行ファイルがアプリ配布サーバから配布された場合に、前記プリインストールされた実行ファイルを前記アプリ配布サーバから配布された前記更新用実行ファイルに書き換える手順と、
前記証明書データが内蔵されていない前記更新用実行ファイルを実行することによって前記アプリケーションが起動された際に、前記アプリケーションが、前記第１の記憶領域に格納された証明書ファイルを読み出して前記アプリ通信サーバとの通信に用いる手順とを実行させるためのプログラム。
【請求項８】
請求項７に記載のプログラムにおいて、
前記端末に、
開発者端末から提供された前記証明書データを含む実行ファイルが含まれるインストールパッケージファイルを第２の記憶領域に格納しておく手順と、
前記第２の記憶領域に格納されたインストールパッケージファイルのインストール時に、前記第２の記憶領域に格納されたインストールパッケージファイルから取り出した前記実行ファイルを第３の記憶領域に格納する手順と、
前記第３の記憶領域に格納された実行ファイルを実行することによるアプリケーションの初回起動時に、前記アプリケーションが、前記第３の記憶領域に格納された実行ファイル内の証明書データを前記証明書ファイルとして前記第１の記憶領域に格納する手順とを実行させるためのプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サーバと通信するためのアプリケーションを配布するアプリケーション配布システム、アプリケーション配布方法、端末及びプログラムに関し、特に、アプリケーションを利用する際に必要となる証明書の保護技術に関する。
【背景技術】
【０００２】
近年、スマートフォンやインターネット端末、あるいはタブレット端末等向けに、オープンソースオペレーティングシステム、ミドルウェア及び主要なアプリケーションからなるソフトウェアスタックパッケージを基にしたプラットフォームが発表されている（例えば、非特許文献１参照。）。
【０００３】
また、上述したプラットフォームにおいては、端末のユーザにはｒｏｏｔ権（特権）を渡さず、端末にインストールされたパッケージの各々に一意のＬｉｎｕｘユーザＩＤが割り当てられ、このＬｉｎｕｘユーザＩＤにおいてアプリケーションが実行され、アプリケーションが実行されることによって生成されたファイルが、保護されたデータ記憶領域に格納され、他のアプリケーションや端末のユーザにより読み書きできないようにする機構が設けられている（例えば、非特許文献２参照。）。
【０００４】
また、上述したプラットフォームにおいては、アプリケーションのコピープロテクトを行う機構が設けられており、保護指定を付加してインストールしたアプリケーションは、一般ユーザが読み書きできない保護されたアプリケーション記憶領域にインストールされる（例えば、非特許文献３参照。）。
【０００５】
ところが、アプリケーションに保護指定を付加してインストールした場合においても、パッケージ（．ａｐｋ）に含まれるファイルのうち、アプリケーション実行ファイル（．ｄｅｘ）以外のファイルは、一般ユーザが読み書きできない保護領域にはインストールされず、どのユーザでも読み出せる領域に配置されるため、パッケージファイル内にアプリ実行ファイルとクライアント証明書ファイルとを同梱してインストールした場合、クライアント証明書ファイルは保護領域にはインストールされず、それにより、アプリケーションが利用するクライアント証明書がユーザに抜き取られてしまう虞れがある（例えば、非特許文献４参照。）。
【０００６】
ここで、アプリケーションプログラムの実行ファイル内に証明書を内蔵し、実行ファイルと証明書とを容易にインストールすることを可能とする技術が考えられている（例えば、特許文献１参照。）。この技術を用いれば、証明書も実行ファイルとともに保護領域にインストールされることとなり、アプリケーションが利用するクライアント証明書がユーザに抜き取られることを回避することができる。
【０００７】
また、上述したプラットフォームにおいては、アップデートを可能とすることが好ましい。そのため、アプリケーションの新規インストール並びにアップデートに必要なパッケージをユーザ端末に配布する機構として、マーケットと呼ばれるサーバがインターネット上に用意されている。そして、アプリケーションをアップデートする場合、パッケージファイル内にアプリ実行ファイルとクライアント証明書ファイルや証明書データとを同梱してマーケットと呼ばれるサーバにアップロードし、それにより、アプリケーションをアップデート可能としている（例えば、非特許文献５参照。）
【先行技術文献】
【特許文献】
【０００８】

【特許文献１】特開２００７－２７２６１０号公報
【非特許文献】
【０００９】
【非特許文献１】Ａｎｄｒｏｉｄ－Ｗｉｋｉｐｅｄｉａ http://ja.wikipedia.org/wiki/Android
【非特許文献２】Ａｎｄｒｏｉｄ Ｄｅｖｅｌｏｐｅｒｓ Ｓｅｃｕｒｉｔｙ ａｎｄ Ｐｅｒｍｉｓｓｉｏｎｓ http://developer.android.com/guide/topics/security/security.html#userid
【非特許文献３】Ｆｏｒｗａｒｄ－Ｌｏｃｋｅｄ Ａｐｐｌｉｃａｔｉｏｎｓ http://developer.android.com/guide/appendix/market-filters.html#other-filters
【非特許文献４】Ａｐｐ Ｉｎｓｔａｌｌ Ｌｏｃａｔｉｏｎ http://developer.android.com/guide/appendix/install-location.html
【非特許文献５】Ｐｕｂｌｉｓｈｉｎｇ Ｙｏｕｒ Ａｐｐｌｉｃａｔｉｏｎｓ http://developer.android.com/guide/publishing/publishing.html
【発明の概要】
【発明が解決しようとする課題】
【００１０】
しかしながら、上述したようなアプリケーションのアップデートを行う場合、パッケージファイル内にアプリ実行ファイルとクライアント証明書ファイルや証明書データとを同梱してサーバにアップロードすることとなるため、アプリケーションを配布するサーバの管理者に悪意があった場合、管理者によりパッケージファイルからクライアント証明書ファイルや証明書データが抜き取られてしまう虞れがある。アプリケーションを配布するサーバは、アプリケーションを配布する端末の開発メーカーが設置するとは限らないため、上記のように悪意のある管理者が管理する可能性も否定できない。
【００１１】
本発明は、上述したような技術が有する問題点に鑑みてなされたものであって、更新用のアプリケーションを配布するサーバの管理者にクライアント証明書を触れられないようにしたままアプリケーションのアップデートを行うことができる、アプリケーション配布システム、アプリケーション配布方法、端末及び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】
【００１２】
上記目的を達成するために本発明は、
インストールされた実行ファイルを実行することによってアプリケーションを起動する端末と、前記実行ファイルに対する更新用の実行ファイルである更新用実行ファイルを前記端末に配布するアプリ配布サーバと、アプリケーションが通信を行うアプリ通信サーバとを有するアプリケーション配布システムであって、
前記端末にプリインストールされた実行ファイルには、前記アプリ通信サーバとの通信時に、前記アプリ通信サーバにアクセスできる端末であることを示す証明書データが内蔵されており、
前記更新用実行ファイルには、前記証明書データが内蔵されておらず、
前記端末は、前記アプリケーションの初回起動時に、前記アプリケーションが、前記プリインストールされた実行ファイル内の証明書データを、特定のアプリケーションからのアクセスでファイルを格納したり読み出したりすることができるアクセス制限がかかった第１の記憶領域に証明書ファイルとして格納しておき、その後、前記アプリ配布サーバから前記更新用実行ファイルが配布された場合、前記プリインストールされた実行ファイルを前記アプリ配布サーバから配布された前記更新用実行ファイルに書き換え、前記証明書データが内蔵されていない前記更新用実行ファイルを実行することによって前記アプリケーションが起動された際に、前記アプリケーションが、前記第１の記憶領域に格納された証明書ファイルを読み出して前記アプリ通信サーバとの通信に用いる。

【００１３】
また、インストールされた実行ファイルを実行することによってアプリケーションを起動する端末と、前記実行ファイルに対する更新用の実行ファイルである更新用実行ファイルを前記端末に配布するアプリ配布サーバと、アプリケーションが通信を行うアプリ通信サーバとを有するアプリケーション配布システムにおけるアプリケーション配布方法であって、
前記端末にプリインストールされた実行ファイルには、前記アプリ通信サーバとの通信時に、前記アプリ通信サーバにアクセスできる端末であることを示す証明書データが内蔵されており、
前記更新用実行ファイルには、前記証明書データが内蔵されておらず、
前記端末が、前記アプリケーションの初回起動時に、前記アプリケーションによって、前記プリインストールされた実行ファイル内の証明書データを、特定のアプリケーションからのアクセスでファイルを格納したり読み出したりすることができるアクセス制限がかかった第１の記憶領域に証明書ファイルとして格納しておく処理と、
前記アプリ配布サーバが、前記更新用実行ファイルを前記端末に配布する処理と、
前記端末が、前記プリインストールされた実行ファイルを前記アプリ配布サーバから配布された前記更新用実行ファイルに書き換える処理と、
前記端末が、前記証明書データが内蔵されていない前記更新用実行ファイルを実行することによって前記アプリケーションが起動された際に、前記アプリケーションによって、前記第１の記憶領域に格納された証明書ファイルを読み出して前記アプリ通信サーバとの通信に用いる処理とを有する。
【００１４】
また、インストールされた実行ファイルを実行することによってアプリケーションを起動する端末であって、
前記端末にプリインストールされた実行ファイルには、アプリケーションが通信を行うアプリ通信サーバとの通信時に、前記アプリ通信サーバにアクセスできる端末であることを示す証明書データが内蔵されており、
アプリ配布サーバから配布される、前記実行ファイルに対する更新用の実行ファイルである更新用実行ファイルには、前記証明書データが内蔵されておらず、
前記アプリケーションの初回起動時に、前記アプリケーションが、前記プリインストールされた実行ファイル内の証明書データを、特定のアプリケーションからのアクセスでファイルを格納したり読み出したりすることができるアクセス制限がかかった第１の記憶領域に証明書ファイルとして格納しておき、その後、前記アプリ配布サーバから前記更新用実行ファイルが配布された場合、前記プリインストールされた実行ファイルを前記アプリ配布サーバから配布された前記更新用実行ファイルに書き換え、前記証明書データが内蔵されていない前記更新用実行ファイルを実行することによって前記アプリケーションが起動された際に、前記アプリケーションが、前記第１の記憶領域に格納された証明書ファイルを読み出して前記アプリ通信サーバとの通信に用いる。
【００１５】
また、アプリケーションが通信を行うアプリ通信サーバとの通信時に、前記アプリ通信サーバにアクセスできる端末であることを示す証明書データが内蔵された実行ファイルがプリインストールされ、インストールされた実行ファイルを実行することによって前記アプリケーションを起動する端末に、
前記アプリケーションの初回起動時に、前記アプリケーションが、前記プリインストールされた実行ファイル内の証明書データを、特定のアプリケーションからのアクセスでファイルを格納したり読み出したりすることができるアクセス制限がかかった第１の記憶領域に証明書ファイルとして格納しておく手順と、
前記証明書データが内蔵されておらず、前記実行ファイルに対する更新用の実行ファイルである更新用実行ファイルがアプリ配布サーバから配布された場合に、前記プリインストールされた実行ファイルを前記アプリ配布サーバから配布された前記更新用実行ファイ

ルに書き換える手順と、
前記証明書データが内蔵されていない前記更新用実行ファイルを実行することによって前記アプリケーションが起動された際に、前記アプリケーションが、前記第１の記憶領域に格納された証明書ファイルを読み出して前記アプリ通信サーバとの通信に用いる手順とを実行させるものである。

【発明の効果】

【００１６】

本発明は、実行ファイル内の証明書データを、アクセス制限がかかった第１の記憶領域に証明書ファイルとして格納しておき、その後、証明書データが内蔵されていない実行ファイルが更新用実行ファイルとして配布された場合、その更新用実行ファイルを実行することによってアプリケーションを利用する際に、第１の記憶領域に格納された証明書ファイルを用いる構成としたため、更新用のアプリケーションを配布するサーバの管理者にクライアント証明書を触れられないようにしたままアプリケーションのアップデートを行うことができる。

【図面の簡単な説明】

【００１７】

【図１】本発明のアプリケーション配布システムの実施の一形態を示すブロック図である。

【図２】図１に示したアプリケーションの基本的な動作を説明するためのフローチャートである。

【図３】図１に示した保護アプリ記憶領域に格納されたインストールパッケージファイルの構成を示す図である。

【図４】図１に示したアプリケーション配布システムにおいて図３に示したインストールパッケージファイルをプリインストールする際の動作を説明するためのタイミングチャートである。

【図５】図１に示したアプリケーション配布システムにおいてアプリケーションが通常起動する際の動作を説明するためのタイミングチャートである。

【図６】図１に示したアプリケーション配布システムにおいてユーザがユーザ端末をフルリセット操作した場合の動作を説明するためのタイミングチャートである。

【図７】図１に示したアプリケーション配布システムにおいてアプリケーションをアップデートする際の動作を説明するためのタイミングチャートである。

【図８】図１に示した開発者端末内の出荷製品記憶領域内に置かれたアップデート版のインストールパッケージファイルの構成を示す図である。

【発明を実施するための形態】

【００１８】

以下に、本発明の実施の形態について図面を参照して説明する。

【００１９】

図１は、本発明のアプリケーション配布システムの実施の一形態を示すブロック図である。

【００２０】

本形態は図１に示すように、ユーザ端末１０と、開発者端末２０と、サーバ３０と、アプリ配布サーバ４０とから構成されている。

【００２１】

ユーザ端末１０は、インストールされた実行ファイルを実行することによってサーバ３０にアクセスしてアプリケーションを利用するものであり、保護一部記憶領域１１と、アプリ記憶領域１２と、保護アプリ記憶領域１３と、保護データ記憶領域１４と、デバッグブリッジ１５と、インストーラ１６と、アプリケーション１７と、ダウンローダ１８とから構成されている。このユーザ端末１０としては、例えば、Ａｎｄｒｏｉｄ等のＯＳが搭載された携帯情報端末（ＰＤＡ）や携帯電話端末が考えられる。ユーザ端末１０では、ユーザ端末の利用者にはｒｏｏｔ権（すなわち特権）を渡さず、また、ユーザ端末１０にイ

ンストールされたパッケージの各々に一意のＬｉｎｕｘユーザＩＤが割り当てられ、アプリケーションはこのＬｉｎｕｘユーザＩＤにおいて実行されるようにする。また、ｒｏｏｔ権（すなわち特権）は、ユーザ端末１０の端末メーカーの権限のある人物にのみ与えられている。

【００２２】

開発者端末２０は、ユーザ端末１０に搭載するアプリケーションを開発するためのパーソナルコンピュータ等の端末であり、ユーザ端末１０の製造メーカーの技術者が利用するものである。開発者端末２０は、データ書込ツール２１と、出荷製品記憶領域２２と、ブラウザ２３とから構成されている。

【００２３】

サーバ３０は、ＳＳＬの双方向認証を必要とするＷＥＢサーバである。

【００２４】

アプリ配布サーバ４０は、ユーザ端末１０にアプリケーションを配布するためにインターネット上に設置されたサーバであり、コンテンツ記憶領域４１と、ＷＥＢサーバ４２とから構成されている。アプリ配布サーバ４０は、一般的にはマーケットと呼ばれるサーバである。

【００２５】

まず、ユーザ端末１０の構成要素について説明する。

【００２６】

保護一時記憶領域１１は、本発明における第２の記憶領域となるものであって、開発者端末２０から提供されるファイルを、デバッグブリッジ１５を介して受け取って格納し、デバッグブリッジ１５からの指示もしくはユーザ端末１１の起動時のスクリプトによってインストーラ１６が動作した場合に、ユーザ端末１０のメモリ（不図示）上で動作しているインストーラ１６にそのファイルを渡す。保護一時記憶領域１１は、予め決められたユーザとなるｒｏｏｔ権のあるユーザしかファイルの格納及び読み出しを行うことができない。従って、ユーザ端末１０の端末メーカーの権限のある人物しか、保護一時記憶領域１１に対してファイルを格納して読み出すことができず、ユーザ端末１０の購入者を含む利用者は、保護一時記憶領域１１に格納されているファイルを読み出すことはできない。また、保護一時記憶領域１１に格納されたファイルは、ユーザ端末１０のフルリセット（工場出荷状態に戻すことを指す）を行っても消去されずにそのまま残る。

【００２７】

アプリ記憶領域１２は、インストーラ１６からアプリケーションの実行ファイル及び付属ファイルを受け取って保存し、アプリケーション１７の実行時やアプリケーション１７が要求した場合に、ユーザ端末１０のメモリに保存されているファイルをアプリケーション１７に渡す。アプリ記憶領域１２は、ｒｏｏｔ権のないユーザでもファイルの格納や読み出しが可能である。また、ユーザ端末１０をフルリセットすると、アプリ記憶領域１２に格納されたファイルは消去される。Ａｎｄｒｏｉｄにおいては、／ｄａｔａ／ａｐｐがこのアプリ記憶領域１２にあたる。

【００２８】

保護アプリ記憶領域１３は、本発明の第３の記憶領域となるものであって、インストーラ１６からアプリケーションの実行ファイルを受け取って格納し、そのアプリケーションの実行時にユーザ端末１０のメモリに、格納しているファイルを渡す。保護アプリ記憶領域１３は、ｒｏｏｔ権のあるユーザしかファイルの格納及び読み出しを行うことができない。従って、ユーザ端末１０の端末メーカーの権限のある人物しか、保護アプリ記憶領域１３に対してファイルを格納して読み出すことができず、ユーザ端末１０の購入者を含む利用者は、保護アプリ記憶領域１３に格納されているファイルを読み出すことはできない。また、ユーザ端末１０をフルリセットすると、保護アプリ記憶領域１３に格納されたファイルは消去される。Ａｎｄｒｏｉｄにおいては、／ｄａｔａ／ａｐｐ－ｐｒｉｖａｔｅがこの保護アプリ記憶領域１３にあたる。

【００２９】

保護データ記憶領域１４は、本発明の第１の記憶領域となるものであって、アプリケーション１７からファイルを受け取って格納し、また、アプリケーション１７からの要求により、格納しているファイルを渡す。保護データ記憶領域１４は、ｒｏｏｔ権のあるユーザもしくは、ファイルを生成したアプリケーション、または、ファイルを生成したアプリケーションと同一のコードサイニング証明書で署名されたアプリケーションからのアクセスによってしかファイルを格納したり読み出したりすることができない。従って、例えば、Ａｎｄｒｏｉｄ　ＯＳ搭載端末においては、ユーザ端末１０の端末メーカーの権限のある人物か、もしくはアプリケーション１７しかファイルを格納して読み出すことができず、ユーザ端末１０の購入者を含む利用者は、保護データ記憶領域１４に格納されているファイルを読み出すことはできない。また、ユーザ端末１０をフルリセットすると、保護データ記憶領域１４に格納されたファイルは消去される。Ａｎｄｒｏｉｄにおいては、／ｄａｔａ／ｄａｔａ／アプリケーション名（例：ｊｐ．ｎｅ．ｂｉｇｌｏｂｅ．ａｐｐｌｉｃａｔｉｏｎｎａｍｅ）がこの保護データ記憶領域１４にあたる。

【００３０】

デバッグブリッジ１５は、開発者端末２０内のデータ書き込みツール２１から指示を受け、インストール、アプリ起動、ファイル操作等のコマンドを実行し、また、データ書込ツール２１から受け取ったファイルを保護一時記憶領域１１に渡して格納する。なお、データ書込ツール２１とデバッグブリッジ１５との間は、ＵＳＢケーブル等で接続される。例えば、Ａｎｄｏｒｉｄでは、ａｄｂがデバッグブリッジ１５にあたる。

【００３１】

インストーラ１６は、本発明の第１の処理手段となるものであって、デバッグブリッジ１５からの指示、もしくは起動時スクリプトからの指示により、保護一時記憶領域１１に格納されているインストールパッケージファイルを読み込み、インストールに必要な設定（メニューへの登録等）を行った上で、このインストールパッケージファイルをアプリ記憶領域１２若しくは保護アプリ記憶領域１３に格納する。また、インストーラ１６は、ダウンローダ１８からの指示があった場合は、ダウンローダ１８から受け取ったインストールパッケージファイルを読み込み、インストールに必要な設定（メニューへの登録等）を行った上で、このインストールパッケージファイルをアプリ記憶領域１２若しくは保護アプリ記憶領域１３に格納する。なお、インストーラ１６によるアプリケーションのインストール時に、保護指定（一般的にＦｏｒｗａｒｄ　Ｌｏｃｋという）がされている場合には、実行ファイルのみが保護アプリ記憶領域１３に格納され、実行ファイル以外のファイルはアプリ記憶領域１２に格納される。保護指定がされていない場合は、全てのファイルがアプリ記憶領域１２に格納される。本形態では、全ての場合において保護指定があるものとする。

【００３２】

アプリケーション１７は、本発明の第２の処理手段となるものであって、デバッグブリッジ１５からの指示、起動時スクリプトからの指示、もしくはメニューからの指示により起動する。起動時は、保護アプリ記憶領域１３に格納されたインストールパッケージファイルに含まれるアプリ実行ファイルをユーザ端末１０内のメモリにロードすることで起動する。また、初回起動時には、そのアプリ実行ファイルに含まれる証明書データを証明書ファイルとして展開して保護データ記憶領域１４に格納する。また、アプリケーション１７は、サーバ３０と通信を行う。この際、保護データ記憶領域１４内に証明書ファイル９２が存在する場合は、このファイルを読み出してサーバ３０に対してクライアント証明書として提示し、サーバ３０にアクセスできる端末であることを示す。

【００３３】

ダウンローダ１８は、定期的にアプリ配布サーバ４０内のＷＥＢサーバ４２と通信し、ユーザ端末１０内にインストールされているアプリケーションの更新用実行ファイルが存在するか否かを問い合わせる。もし更新用実行ファイルが存在する場合は、アプリ配布サーバ４０内のＷＥＢサーバ４２からインターネット経由で、更新用実行ファイルを含むインストールパッケージファイルを受信し、インストーラ１６に渡す。

【００３４】
次に、開発者端末２０の構成要素について説明する。
【００３５】
データ書き込みツール２１は、ユーザ端末１０にｒｏｏｔ権のあるユーザとしてログインし、開発者端末２０の操作者による指示に従い、出荷製品記憶領域２２内に記憶されているファイルを、デバッグブリッジ１５経由で保護一時記憶領域１１に転送する。また、デバッグブリッジ１５を介して、ユーザ端末１０に対して、インストール、アプリ起動、ファイル操作等のコマンドを送信する。データ書込ツール２１とデバッグブリッジ１５との間は、ＵＳＢケーブル等で接続される。
【００３６】
出荷製品記憶領域２２は、データ書込ツール２１を経由してユーザ端末１０内の保護一時記憶領域１１に格納するファイルを格納するための領域である。
【００３７】
ブラウザ２３は、アプリ配布サーバ４０内のＷＥＢサーバ４２にアクセスし、出荷製品記憶領域２２内のファイルをアプリ配布サーバ４０にアップロードする。ブラウザ２３とＷＥＢサーバ４２との間は、インターネットで接続されている。
【００３８】
次に、サーバ３０について詳細に説明する。
【００３９】
サーバ３０は、アプリケーション１７から接続要求を受けると、自身のサーバ証明書をアプリケーション１７に提示するとともに、アプリケーション１７に対してクライアント証明書の提示を要求し、正しいクライアント証明書が提示された場合のみ接続を受け付けるサーバである。サーバ３０とユーザ端末１０内のアプリケーション１７との間は、インターネットで接続されている。
【００４０】
次に、アプリ配布サーバ４０の構成要素について説明する。
【００４１】
コンテンツ記憶領域４１は、ＷＥＢサーバ４２から受け取ったファイルを格納し、また、ＷＥＢサーバ４２からの要求に応じてファイルをＷＥＢサーバ４２に送る。
【００４２】
ＷＥＢサーバ４２は、ブラウザ２３からインターネット経由でアップロードされたファイルを受け付けてコンテンツ記憶領域４１に格納し、また、ダウンローダ１８からインターネット経由で要求されたファイルをコンテンツ記憶領域４１から読み出してダウンローダ１８に転送する。
【００４３】
以下に、上記のように構成されたアプリケーション配布システムにおけるアプリケーション配布方法について説明する。
【００４４】
まず、図１に示したアプリケーション１７の基本的な動作について説明する。
【００４５】
図２は、図１に示したアプリケーション１７の基本的な動作を説明するためのフローチャートである。
【００４６】
アプリケーション１７は、デバッグブリッジ１５からの指示、起動時スクリプトからの指示、もしくはメニューからの指示により起動する。起動時は、保護アプリ記憶領域１３に格納されたアプリ実行ファイルをユーザ端末１０内のメモリにロードすることで起動する（ステップ１）。
【００４７】
図３は、図１に示した保護アプリ記憶領域１３に格納されたインストールパッケージファイルの構成を示す図である。

【００４８】
図１に示した保護アプリ記憶領域１３には、保護一時記憶領域１１から読み出されたインストールパッケージファイル９０がインストーラ１６によって格納されている。このインストーラパッケージ９０は、ユーザ端末１０にアプリケーションをプリインストールする場合に利用するインストールパッケージであり、そのため、図３に示すようにアプリ実行ファイル９１を有しており、アプリ実行ファイル９１のインストール時にインストーラ１６によって保護アプリ記憶領域１３に格納される。インストールパッケージファイル９０は、アプリケーションのインストールに必要なファイル類をひとまとめにしたアーカイブであり、Ａｎｄｒｏｉｄの場合は一般的にａｐｋという拡張子が付くファイルである。アプリ実行ファイル９１は、ユーザ端末１０上で動作するアプリケーション１７の実行ファイルであり、内部にクライアント証明書として使用できる証明書データ９２が格納されている。Ａｎｄｒｏｉｄの場合は、一般的にｄｅｘという拡張子が付くファイルである。証明書データ９２は、アプリ実行ファイル９１内に格納されたクライアント証明書データである。
【００４９】
アプリケーション１７が初めて起動された場合で、かつ、アプリ実行ファイル９１に証明書データ９２が内蔵されている場合（つまり、アプリ実行ファイル９１をロードすることで実行されているアプリケーション１７）は（ステップ２）、アプリケーション１７が、保護アプリ記憶領域１３に格納されたインストールパッケージファイル９０に含まれる証明書データ９２を証明書ファイルとして展開して保護データ記憶領域１４に格納する（ステップ３）。なお、証明書ファイルは、サーバ３０との通信時に必要なクライアント証明書データで構成されるファイルであり、開発者端末２０におけるアプリ実行ファイル９１の作成時に証明書データ９２としてアプリ実行ファイル９１内に取り込まれる。
【００５０】
次に、アプリケーション１７は、保護データ記憶領域１４に格納された証明書ファイルを読み出す（ステップ４）。
【００５１】
その後、アプリケーション１７は、サーバ３０との間にて、保護データ記憶領域１４から読み出した証明書ファイルをクライアント証明書として用いて双方向認証つきＳＳＬ通信を行う（ステップ５）。
【００５２】
そして、通信終了後、終了する（ステップ６）。
【００５３】
次に、図１に示したアプリケーション配布システムにおいて図３に示したインストールパッケージファイル９０をプリインストールする際の動作について説明する。
【００５４】
図４は、図１に示したアプリケーション配布システムにおいて図３に示したインストールパッケージファイルをプリインストールする際の動作を説明するためのタイミングチャートである。
【００５５】
ここで、ユーザ端末１０は、製造メーカーの工場等に置かれており、開発者端末２０内のデータ書き込みツール２１とユーザ端末１０内のデバッグブリッジ１５とはＵＳＢケーブルで接続されているものとする。また、開発者端末２０からユーザ端末１０には、ｒｏｏｔ権のあるユーザとしてログインするものとする。
【００５６】
ユーザ端末１０の製造メーカーの技術者（以下、技術者と称する）が、開発者端末２０内の出荷製品記憶領域２２内に、インストールパッケージファイル９０を置く。このインストールパッケージファイル９０内には、図３に示したように、アプリ実行ファイル９１が含まれており、このアプリ実行ファイル９１内には、証明書データ９２が含まれている。

【００５７】
技術者が、データ書込ツール２１を用いて、出荷製品記憶領域２２内に格納されているインストールパッケージファイル９０を、デバッグブリッジ１５を経由して保護一時記憶領域１１に書き込む。この際、ユーザがユーザ端末１０を初めて起動したときに、インストーラ１６が起動してインストールパッケージファイル９０が保護指定つきでインストールされるよう設定する（ステップ１１）。
【００５８】
以上の作業が完了すると、ユーザ端末１０は工場からユーザのもとに発送される。
【００５９】
ユーザは、工場から送付されたユーザ端末１０を受け取り、ユーザ端末１０を起動する。
【００６０】
ユーザ端末１は、初回起動時にインストーラ１６が起動してインストールパッケージファイル９０を保護指定つきでインストールするように設定されているため、インストーラ１６が起動する。インストーラ１６は、保護一時記憶領域１１に格納されたインストールパッケージファイル９０を読み出し、インストールに必要な設定（メニューへの登録等）を行った上で、インストールパッケージファイル９０からアプリ実行ファイル９１を取り出し、保護アプリ記憶領域１３に書き込む（ステップ１２）。なお、このアプリ実行ファイル９１内には、証明書データ９２が含まれている。
【００６１】
以上の動作により、インストールパッケージファイル９０がユーザ端末１０にインストールされた。
【００６２】
次に、ユーザが、ユーザ端末１０のメニューからアプリケーション１７の起動を指示すると、保護アプリ記憶領域１３に格納されているアプリ実行ファイル９１が証明書データ９２ごとメモリ上にロードされ、アプリケーション１７として起動する（ステップ１３）。
【００６３】
アプリケーション１７は、初回起動であり、かつ、アプリ実行ファイル９１が証明書データ９２を内蔵しているため、証明書データ９２を証明書ファイルとして展開して保護データ記憶領域１４に格納する（ステップ１４）。
【００６４】
次に、アプリケーション１７は、保護データ記憶領域１４に格納されている証明書ファイルを読み込み（ステップ１５）、保護アプリ記憶領域１３に格納されているアプリ実行ファイル９１を実行することによってサーバ３０と双方向ＳＳＬによる通信を開始する際に、保護データ記憶領域１４から読み込んだ証明書ファイルのデータをクライアント証明書としてサーバ３０に提示する（ステップ１６）。
【００６５】
アプリケーション１７は、サーバ３０との通信を終了すると、アプリケーションとしての動作を終了する。
【００６６】
以上の動作により、証明書ファイルが保護データ記憶領域１４に書き込まれるとともに、サーバ３０との通信が完了する。
【００６７】
次に、図１に示したアプリケーション配布システムにおいてアプリケーション１７が通常起動（すなわち初回起動ではない）する際の動作について説明する。
【００６８】
図５は、図１に示したアプリケーション配布システムにおいてアプリケーション１７が通常起動する際の動作を説明するためのタイミングチャートである。
【００６９】

ユーザが、ユーザ端末１０のメニューからアプリケーション１７の起動を指示すると、保護アプリ記憶領域１３に格納されているアプリ実行ファイル９１が証明書データ９２ごとメモリ上にロードされ、アプリケーション１７として起動する（ステップ２１）。

【００７０】

アプリケーション１７は、初回起動ではないため、保護データ記憶領域１４に格納されている証明書ファイルを読み込み（ステップ２２）、保護アプリ記憶領域１３に格納されているアプリ実行ファイル９１を実行することによってサーバ３０と双方向ＳＳＬによる通信を開始する際に、保護データ記憶領域１４から読み込んだ証明書ファイルのデータをクライアント証明書としてサーバ３０に提示する（ステップ２３）。

【００７１】

アプリケーション１７は、サーバ３０との通信を終了すると、アプリケーションとしての動作を終了する。

【００７２】

以上の動作により、アプリケーション１７はサーバ３０と正常に通信できた。

【００７３】

次に、図１に示したアプリケーション配布システムにおいてユーザがユーザ端末１をフルリセット操作した場合の動作について説明する。

【００７４】

図６は、図１に示したアプリケーション配布システムにおいてユーザがユーザ端末１０をフルリセット操作した場合の動作を説明するためのタイミングチャートである。

【００７５】

なお、ユーザは既にユーザ端末１０の初回起動を終え、さらにアプリケーション１７の初回起動も終えているものとする。つまり、図４に示したステップ１１～１６の動作を完了しているものとする。

【００７６】

ユーザが、ユーザ端末１０のフルリセット操作を行うと、アプリ記憶領域１２、保護アプリ記憶領域１３及び保護データ記憶領域１４に格納されている全てのファイルが消去される。従って、保護アプリ記憶領域１３に格納されているアプリ実行ファイル９１と、保護データ記憶領域１４に格納されている証明書ファイルが消去されるが、保護一時記憶領域１１内のインストールパッケージファイル９０は消去されずに残る。

【００７７】

ユーザがフルリセット操作の実行後に、初めてユーザ端末１０を起動すると、ユーザ端末１０は、初回起動時にインストールパッケージファイル９０を保護指定つきでインストールするよう設定されているため、インストーラ１６が起動する。インストーラ１６は、保護一時記憶領域１１に格納されているインストールパッケージファイル９０を読み出し、インストールに必要な設定（メニューへの登録等）を行った上で、インストールパッケージファイル９０からアプリ実行ファイル９１を取り出し、保護アプリ記憶領域１３に格納する（ステップ３１）。なお、このアプリ実行ファイル９１内には証明書データ９２が含まれている。

【００７８】

以上の動作により、インストールパッケージファイル９０がユーザ端末１０にインストールされた。

【００７９】

次に、ユーザが、ユーザ端末１０のメニューからアプリケーション１７の起動を指示すると、保護アプリ記憶領域１３に格納されているアプリ実行ファイル９１が証明書データ９２ごとメモリ上にロードされ、アプリケーション１７として起動する（ステップ３２）。

【００８０】

アプリケーション１７は、初回起動であり、かつ、アプリ実行ファイル９１が証明書データ９２を内蔵しているため、証明書データ９２を証明書ファイルとして展開して保護デ

ータ記憶領域１４に格納する（ステップ３３）。

【００８１】

次に、アプリケーション１７は、保護データ記憶領域１４に格納されている証明書ファイルを読み込み（ステップ３４）、保護アプリ記憶領域１３に格納されているアプリ実行ファイル９１を実行することによってサーバ３０と双方向ＳＳＬによる通信を開始する際に、保護データ記憶領域１４から読み込んだ証明書ファイルのデータをクライアント証明書としてサーバ３０に提示する（ステップ３５）。

【００８２】

アプリケーション１７は、サーバ３０との通信を終了すると、アプリケーションとしての動作を終了する。

【００８３】

以上の動作により、証明書データ９２が証明書ファイルとして展開されて保護データ記憶領域１４に格納されるとともに、サーバ３０との通信が完了する。

【００８４】

次に、図１に示したアプリケーション配布システムにおいてアプリケーション１７をアップデートする際の動作について説明する。

【００８５】

図７は、図１に示したアプリケーション配布システムにおいてアプリケーション１７をアップデートする際の動作を説明するためのタイミングチャートである。

【００８６】

なお、ユーザ端末１０はユーザの手元に渡っており、ユーザは、既にユーザ端末１０の初回起動を終え、さらにアプリケーション１７の初回起動も終えているものとする。つまり、図４に示したステップ１１～１６の動作を完了しているものとする。また、開発者端末２０内のデータ書き込みツール２１とユーザ端末１０内のデバッグブリッジ１５とはＵＳＢケーブルで接続されておらず、代わりに開発者端末２０内のブラウザ２３とアプリ配布サーバ４０内のＷＥＢサーバ４２との間、またアプリ配布サーバ４０内のＷＥＢサーバ４２とユーザ端末１０内のダウンローダ１８との間が、インターネットでそれぞれ接続されているものとする。

【００８７】

ユーザ端末１０の製造メーカーの技術者（以下、技術者と称する）が、開発者端末２０内の出荷製品記憶領域２２内に、インストールパッケージファイル９０のアップデート版を置く。この際、アップデート版のインストールパッケージファイルが保護指定つきでインストールされるよう設定する。

【００８８】

図８は、図１に示した開発者端末２０内の出荷製品記憶領域２２内に置かれたアップデート版のインストールパッケージファイルの構成を示す図である。

【００８９】

開発者端末２０内の出荷製品記憶領域２２内に置かれたアップデート版のインストールパッケージファイル９０Ａは、特にユーザ端末１０に既にインストール済みのアプリケーションをアップデートする場合に利用するインストールパッケージであり、そのため、図８に示すように、インストールパッケージファイル９０Ａ内には、更新用のアプリ実行ファイル９１Ａが格納されている。インストールパッケージファイル９０Ａは、アプリケーションのインストールに必要なファイル類をひとまとめにしたアーカイブであり、Ａｎｄｒｏｉｄの場合は一般的にａｐｋという拡張子が付くファイルである。アプリ実行ファイル９１Ａは、ユーザ端末１０上で動作するアプリケーション１７の実行ファイルであり、図３に示したアプリ実行ファイル９１とは異なり、内部にクライアント証明書として使用できる証明書データ９２を格納していない。

【００９０】

技術者が、ブラウザ２３を用いて、出荷製品記憶領域２２内に格納されているインストールパッケージファイル９０Ａを、ＷＥＢサーバ４２を経由してコンテンツ記憶領域４１

に書き込む（ステップ４１）。

【００９１】

ダウンローダ１８は、定期的にアプリ配布サーバ４０内のＷＥＢサーバ４２と通信し、ユーザ端末１０内にインストールされているアプリケーション１７の更新版が存在するか否かを問い合わせる。このとき、ダウンローダ１８はアプリ配布サーバ４０のコンテンツ記憶領域４１内に、アプリケーション１７の更新版のインストールパッケージファイルであるインストールパッケージファイル９０Ａが存在することを知り、ＷＥＢサーバ４２からインターネット経由で更新されたインストールパッケージファイル９０Ａを受信し、保護指定つきでインストーラ１６に渡す。

【００９２】

インストーラ１６は、ダウンローダ１８からインストールパッケージファイル９０Ａを受け取ると、インストールに必要な設定（メニューへの登録等）を行った上で、インストールパッケージファイル９０Ａからアプリ実行ファイル９１Ａを取り出し、保護アプリ記憶領域１３に格納する。このとき、既に保護アプリ記憶領域１３に格納されているアプリ実行ファイル９１を削除することにより、保護アプリ記憶領域１３に格納されているアプリ実行ファイル９１をアプリ実行ファイル９１Ａに書き換える（ステップ４２）。

【００９３】

以上の動作により、保護アプリ記憶領域１３に格納されているアプリ実行ファイル９１がアプリ実行ファイル９１Ａに更新された。

【００９４】

次に、上記のようにして更新されたアプリケーション１７が通常起動する際の動作について説明する。

【００９５】

ユーザが、ユーザ端末１０のメニューからアプリケーション１７の起動を指示すると、保護アプリ記憶領域１３内に格納されているアプリ実行ファイル９１Ａがメモリ上にロードされ、アプリケーション１７として起動する（ステップ４３）。

【００９６】

アプリケーション１７は、アプリ実行ファイル９１Ａに証明書データが内蔵されていないため、保護データ記憶領域１４内に格納されている証明書ファイルを読み込み（ステップ４４）、保護アプリ記憶領域１３に格納されているアプリ実行ファイル９１Ａを実行することによってサーバ３０と双方向ＳＳＬによる通信を開始する際に、保護データ記憶領域１４から読み込んだ証明書ファイルのデータをクライアント証明書としてサーバ３０に提示する（ステップ４５）。

【００９７】

アプリケーション１７は、サーバ３０との通信を終了すると、アプリケーションとしての動作を終了する。

【００９８】

以上の動作により、更新されたアプリケーション１７は、サーバ３０と正常に通信できた。

【００９９】

以下に、本形態の効果について説明する。

【０１００】

本形態においては、開発者端末２０からユーザ端末１０に提供されるインストールパッケージ９０のアプリ実行ファイル９１内に証明書データ９２を埋め込んでいるため、アプリケーションが利用するクライアント証明書をユーザによって触れられないようにしたまま、アプリケーションと証明書のインストールおよびアップデートを行うことができる。

【０１０１】

また、上記のように証明書データ９２を埋め込んだアプリ実行ファイル９１を保護一時領域１１に格納して出荷し、ユーザ端末１０の初回起動時にこのアプリ実行ファイル９１を保護アプリ記憶領域１３にインストールし、アプリケーションの初回起動時に、アプリ

実行ファイル９１に埋め込まれた証明書データ９２を証明書ファイルとして展開して保護データ記憶領域１４に格納し、アップデート版の配布時には証明書データを抜いた更新用のアプリ実行ファイル９１Ａを配布し、このアプリ実行ファイル９１Ａの実行時には、既に保護データ記憶領域１４に格納されている証明書ファイルを用いるため、アプリケーションが利用するクライアント証明書をアプリ配布サーバの管理者に触れられないようにしたまま、更新版アプリケーションの配布とアップデートを行うことができる。

【０１０２】

なお、本発明においては、ユーザ端末１０内の処理は上述の専用のハードウェアにより実現されるもの以外に、その機能を実現するためのプログラムをユーザ端末１０にて読取可能な記録媒体に記録し、この記録媒体に記録されたプログラムをユーザ端末１０に読み込ませ、実行するものであっても良い。ユーザ端末１０にて読取可能な記録媒体とは、ＩＣカードやメモリカード、あるいは、フロッピーディスク（登録商標）、光磁気ディスク、ＤＶＤ、ＣＤ等の移設可能な記録媒体の他、ユーザ端末１０に内蔵されたＨＤＤ等を指す。この記録媒体に記録されたプログラムは、例えば、制御ブロックにて読み込まれ、制御ブロックの制御によって、上述したものと同様の処理が行われる。

【０１０３】

以上、好ましい実施の形態を挙げて本発明を説明したが、本発明は必ずしも上記実施の形態に限定されるものではなく、その技術的思想の範囲内において様々に変形して実施することができる。当然ながら、以上に述べた実施の形態を、相互に組み合わせて実施することもできる。

【産業上の利用可能性】

【０１０４】

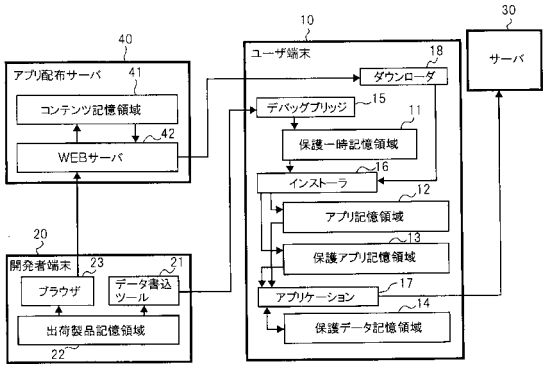
本発明は、ユーザごとのアクセス権を管理できるＯＳを搭載した携帯情報端末（ＰＤＡ）や携帯電話端末（スマートフォン）等に適用できる。

【符号の説明】

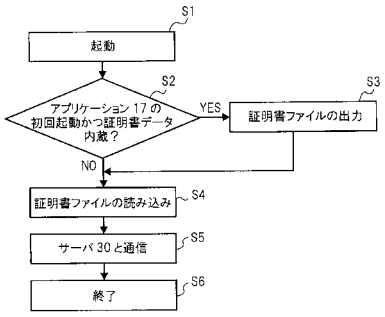
【０１０５】

１０　ユーザ端末
１１　保護一時記憶領域
１２　アプリ記憶領域
１３　保護アプリ記憶領域
１４　保護データ記憶領域
１５　デバッグブリッジ
１６　インストーラ
１７　アプリケーション
１８　ダウンローダ
２０　開発者端末
２１　データ書込ツール
２２　出荷製品記憶領域
２３　ブラウザ
３０　サーバ
４０　アプリ配布サーバ
４１　コンテンツ記憶領域
４２　ＷＥＢサーバ
９０，９０Ａ　インストールパッケージファイル
９１，９１Ａ　アプリ実行ファイル
９２　証明書データ

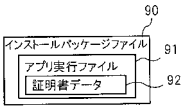
【図１】



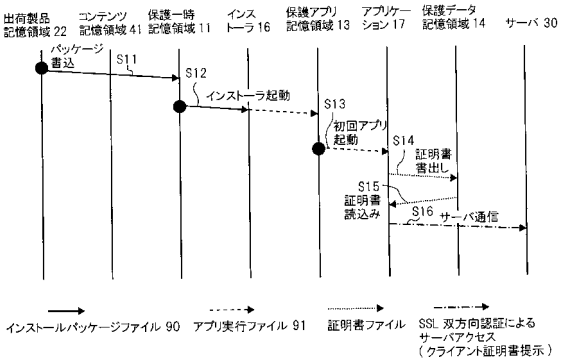
【図２】



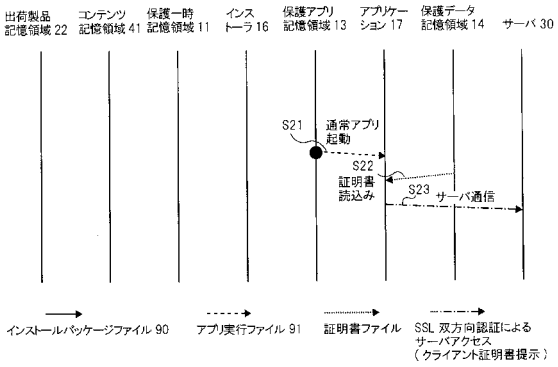
【図３】



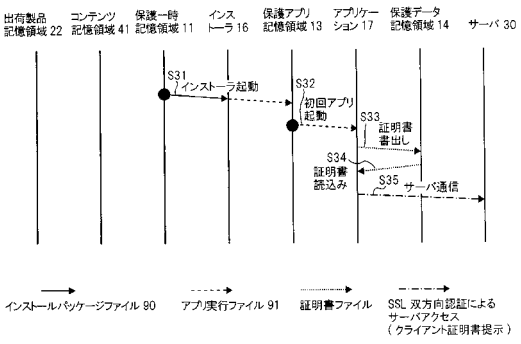
【図４】



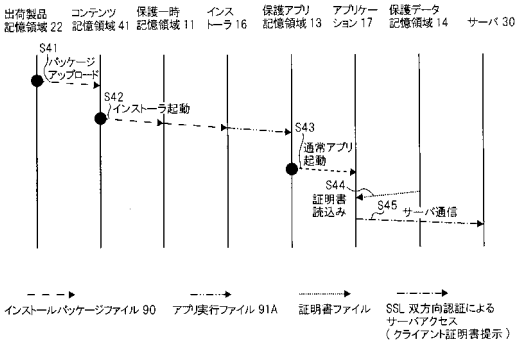
【図５】



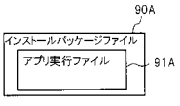
【図６】



【図７】



【図８】



フロントページの続き

(72)発明者　田岡　洋平
東京都品川区大崎一丁目１１番１号　ＮＥＣビッグローブ株式会社内
(72)発明者　廣嶋　隆憲
東京都品川区大崎一丁目１１番１号　ＮＥＣビッグローブ株式会社内

審査官　林　毅

(56)参考文献　特開２００４－２３４５９１（ＪＰ，Ａ）
特開平１０－０８３３１０（ＪＰ，Ａ）
特開２００３－０２２１４０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４４
Ｇ０６Ｆ　９／４４５
Ｇ０６Ｆ　１１／００
Ｇ０６Ｆ　２１／３３