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

特許第6079875号
(P6079875)

(45)発行日　平成29年2月15日(2017.2.15)　(24)登録日　平成29年1月27日(2017.1.27)

(51)Int.Cl.		F I		
G06F 9/445	(2006.01)	G06F	9/06	640A
G06F 21/62	(2013.01)	G06F	9/06	610Q
G06F 13/00	(2006.01)	G06F	21/62	
		G06F	21/62	309
		G06F	13/00	530A

請求項の数 9　(全 21 頁)

(21)出願番号　特願2015-519513 (P2015-519513)
(86)(22)出願日　平成25年5月27日 (2013.5.27)
(86)国際出願番号　PCT/JP2013/064642
(87)国際公開番号　WO2014/192063
(87)国際公開日　平成26年12月4日 (2014.12.4)
審査請求日　平成27年10月29日 (2015.10.29)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100094525
弁理士　土井　健二
(74)代理人　100094514
弁理士　林　恒徳
(72)発明者　矢崎　孝一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　伊藤　栄信
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】アプリケーション実行プログラム，アプリケーション実行方法及びアプリケーションを実行する情報処理端末装置

(57)【特許請求の範囲】

【請求項１】

端末装置のメモリに保存されているアプリケーションを実行するアプリケーション実行処理をプロセッサに実行させるアプリケーション実行プログラムであって，前記アプリケーション実行処理は，

前記メモリに保存されているアプリケーションに前記端末装置内で未使用のＵＲＬである外部アドレスを対応付ける工程と，

前記外部アドレスが割り当てられた内部ウエブサーバを起動する工程と，

ブラウザに，前記外部アドレスの内部ウエブサーバにアクセスさせて前記アプリケーションを取得させる工程と，

前記ブラウザに，前記アプリケーションを実行させて，前記外部アドレスに対応付けられた前記メモリのデータストレージ領域内のデータにアクセスさせる工程とを有するアプリケーション実行プログラム。

【請求項２】

請求項１において，

さらに，

前記外部アドレスに対応付けられたデータストレージ領域を前記メモリ内に確保する初期化処理を行う工程と，

前記データストレージ領域に，前記メモリ内に保存されているアプリケーションに対するデータを書き込む工程とを有するアプリケーション実行プログラム。

【請求項３】
請求項１または２において，
さらに，前記データストレージ領域内のデータを退避する工程と，
前記データの退避後に，前記ブラウザに前記アプリケーションの実行を終了させて前記データストレージ領域内のデータを消去させる工程と，
前記退避したデータをセキュリティファイルシステムに保存する工程とを有するアプリケーション実行プログラム。
【請求項４】
請求項１または２において，
さらに，前記端末装置がアプリケーションサーバと通信可能なオンライン状態において，前記アプリケーションサーバから前記アプリケーションと当該アプリケーションのデータとをダウンロードして，前記端末装置のメモリに保存する工程とを有するアプリケーション実行プログラム。
【請求項５】
請求項２において，
前記初期化処理を行う工程で，前記データストレージ領域への読み出し処理を読み出しデータを復号して行い，書き込み処理をデータを暗号化して行う読み出し書き込み関数を，前記外部アドレスに対応付けて登録し，
前記ブラウザが前記アプリケーションを実行中に行う前記データストレージ領域へのアクセスが，前記読み出し書き込み関数を介して行われるアプリケーション実行プログラム。
【請求項６】
請求項２において，
さらに，前記端末装置がアプリケーションサーバと通信可能なオンライン状態において，前記アプリケーションサーバから，前記アプリケーション及び当該アプリケーションのデータの暗号化コンテンツと，前記アプリケーションのデータに対応する端末装置状況を有する第１のポリシーファイルとをダウンロードして，前記暗号化コンテンツと第１のポリシーファイルとを前記端末装置のメモリに保存する工程と，
前記端末装置が前記アプリケーションサーバと通信不能なオフライン状態において，前記アプリケーションの起動時の前記端末装置状況が前記第１のポリシーファイル内の端末装置状況と一致する場合に，前記暗号化コンテンツを復号して前記アプリケーションのデータを前記データストレージ領域に保存する工程とを有するアプリケーション実行プログラム。
【請求項７】
請求項６において，
さらに，前記データストレージ領域内のデータを退避する工程と，
前記データの退避後に，前記ブラウザに前記アプリケーションの実行を終了させて前記データストレージ領域内のデータを消去させる工程と，
前記アプリケーションの実行を終了させる時の前記端末装置状況を有する第２のポリシーファイルを生成する工程と，
前記退避したデータと前記生成した第２のポリシーファイルを前記アプリケーションサーバにアップロードする工程とを有するアプリケーション実行プログラム。
【請求項８】
端末装置のメモリに保存されているアプリケーションを実行するアプリケーション実行方法であって，
前記メモリに保存されているアプリケーションに前記端末装置内で未使用のＵＲＬである外部アドレスを対応付ける工程と，
前記外部アドレスが割り当てられた内部ウエブサーバを起動する工程と，
ブラウザに，前記外部アドレスの内部ウエブサーバにアクセスさせて前記アプリケーションを取得させる工程と，

前記ブラウザに，前記アプリケーションを実行させて，前記外部アドレスに対応付けられた前記メモリのデータストレージ領域内のデータにアクセスさせる工程とを有するアプリケーション実行方法。

【請求項９】

端末装置のメモリに保存されているアプリケーションを実行する情報処理端末装置であって，

前記メモリに保存されているアプリケーションに前記端末装置内で未使用のＵＲＬである外部アドレスを対応付ける対応付け手段と，

前記外部アドレスが割り当てられた内部ウエブサーバを起動する起動手段と，

ブラウザに，前記外部アドレスの内部ウエブサーバにアクセスさせて前記アプリケーションを取得させる取得手段と，

前記ブラウザに，前記アプリケーションを実行させて，前記外部アドレスに対応付けられた前記メモリのデータストレージ領域内のデータにアクセスさせるアクセス手段とを有する情報処理端末装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は，アプリケーション実行プログラム，アプリケーション実行方法及びアプリケーションを実行する情報処理端末装置に関する。

【背景技術】

【０００２】

３Ｇ／ＬＴＥ（Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ）／ホットスポットの充実に伴い，例えばスマートフォンなどの情報処理端末装置（以下，単に端末または端末装置と称する）が，常時ネットワークに接続できる環境が整ってきている。

【０００３】

このような環境を利用して，アプリケーションサーバ（以下，単にアプリサーバと称する）から端末に必要なタイミングでアプリケーションプログラム（以下，単にアプリと称する）を配信して，端末に実行させる情報処理システムが提案されている。このようなシステムでは，端末を携帯するユーザの時間や場所に応じて必要となるアプリやデータについて，端末に配信，実行，消去などの一連の動作を自動で行う。例えば，サーバが端末の状況を端末が内蔵するセンサの出力から取得し，必要なアプリやデータを端末に配信する。そして，端末でアプリの実行が終了すると，そのデータが消去される。このシステムを利用することで，ユーザが事前にアプリやデータを端末にセットアップしておかなくても，必要なときに必要な場所で，端末でそのときその場所で必要なアプリを実行することができるようになる。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２０１０－１８２３０９号公報

【特許文献２】特開２０１０－１６０８０８号公報

【特許文献１】特表２０１０－５３４８７５号公報

【特許文献２】国際公開第２００３／０５０６６２号パンフレット

【非特許文献】

【０００５】

【非特許文献１】プレスリリース（技術）”時間や場所に応じて必要なアプリケーションが自動配信・自動実行される情報端末技術を開発”，平成２３年７月１９日，株式会社富士通，（平成２４年８月７日検索），http://pr.fujitsu.com/jp/news/2011/07/19-1.html

【発明の概要】

【発明が解決しようとする課題】

【０００６】
上記のような情報処理システムにおいて，データのセキュリティは重要な技術的課題である。端末は，オンライン状態でアプリサーバから必要なアプリとデータをダウンロードし，アプリサーバと接続できないオフライン環境で，そのデータに対してアプリを実行する。そして，このような情報処理システムにおけるアプリとして，ＨＴＭＬで記述されたアプリケーションプログラムであるHTMLアプリが利用される。
【０００７】
オンライン環境でHTMLアプリを利用すると，端末上に一時的な情報を保存するためのストレージ領域を持つことができる。そのストレージ領域は，ブラウザによりインターネットアドレスであるURLに対して割り当てられ，それぞれ隔離されるので，各ストレージ領域内のデータは保護される。そして，ウインドウやタブが開いている間のみデータが保存され，閉じるとデータは失われる。例えば，セッションストレージと呼ばれているストレージ領域である。したがって，異なるHTMLアプリについてのデータは，それぞれ隔離されたストレージ領域に保存され，HTMLアプリの終了と共にそのストレージ領域内のデータはクリアされる。このように，オンライン環境でサーバからダウンロードして実行されるHTMLアプリを，ウエブアプリと称する。
【０００８】
一方，HTMLアプリは，端末内（ローカル内）の記憶領域内に保存することで，オフライン環境下で実行することができる。いわゆるオフライン閲覧が可能である。このように，オフライン環境で実行されるローカルに保存したHTMLアプリを，ローカルアプリと称する。しかし，この場合は，ブラウザがローカルファイル（Localfile)という同一のインターネットアドレスに対してデータのストレージ領域を割り当てるので，全てのローカルなHTMLアプリが同じストレージ領域を共有する。さらに，HTMLアプリを終了してもストレージ領域内のデータはクリアされない。
【０００９】
したがって，ローカルアプリの場合は，悪意のあるHTMLアプリによって共有されるストレージ領域内のデータが漏洩する問題がある。
【００１０】
そこで，本発明の目的は，セキュリティ性の高いアプリケーション実行プログラム，アプリケーション実行方法及びアプリケーションを実行する情報処理端末装置を提供することにある。
【課題を解決するための手段】
【００１１】
実施の形態の第１の側面は，端末装置のメモリに保存されているアプリケーションを実行するアプリケーション実行処理をプロセッサに実行させるアプリケーション実行プログラムであって，前記アプリケーション実行処理は，
前記メモリに保存されているアプリケーションに前記端末装置外の外部アドレスを対応付ける工程と，
前記外部アドレスが割り当てられた内部ウエブサーバを起動する工程と，
ブラウザに，前記外部アドレスの内部ウエブサーバにアクセスさせて前記アプリケーションを取得させる工程と，
前記ブラウザに，前記アプリケーションを実行させて，前記外部アドレスに対応付けられたデータストレージ領域内のデータにアクセスさせる工程とを有する。
【発明の効果】
【００１２】
第１の側面によれば，アプリケーションのデータのセキュリティ性を高めることができる。
【図面の簡単な説明】
【００１３】
【図１】本実施の形態におけるアプリプッシュの情報処理システムの全体構成を示す図で

ある。
【図２】本実施の形態におけるアプリサーバの構成図である。
【図３】アプリプッシュ制御プログラム２１１の機能を示す図である。
【図４】本実施の形態における端末装置の構成図である。
【図５】図４の端末装置のハードウエアとソフトウエアの関係を示す図である。
【図６】第１の実施の形態におけるアプリ実行シーケンスの概略を示すフローチャート図である。
【図７】第１の実施の形態におけるアプリ実行シーケンスのフローチャート図である。
【図８】第１の実施の形態におけるアプリ実行シーケンスのフローチャート図である。
【図９】第１の実施の形態におけるアプリ実行シーケンスのフローチャート図である。
【図１０】第２の実施の形態におけるアプリの実行シーケンスを示すフローチャート図である。
【図１１】第２の実施の形態におけるアプリの実行シーケンスを示すフローチャート図である。
【図１２】第２の実施の形態におけるアプリの実行シーケンスを示すフローチャート図である。
【図１３】ブラウザエンジン内の読み出し書き込み関数テーブルを示す図である。
【図１４】アプリサーバが保持するデータ管理テーブルと各端末装置が保持するデータ管理テーブルの例を示す図である。
【図１５】アプリサーバ２０と端末装置１０内の鍵管理部１３１とが生成するポリシーファイルPFの例を示す図である。
【図１６】第３の実施の形態におけるアプリ実行シーケンスのフローチャート図である。
【図１７】第３の実施の形態におけるアプリ実行シーケンスのフローチャート図である。
【図１８】第３の実施の形態におけるアプリ実行シーケンスのフローチャート図である。
【発明を実施するための形態】
【００１４】
図１は，本実施の形態におけるアプリプッシュの情報処理システムの全体構成を示す図である。この情報処理システムは，アプリケーション，例えばHTMLアプリ（HTMLで記述されたアプリケーションプログラム），を実行する複数の端末装置１０と，アプリを端末装置１０に送信するアプリサーバ２０と，複数の端末装置１０とアプリサーバ２０とを通信可能にするネットワークNETとを有する。このネットワークNETは，ユーザが属する企業内のイントラネットや，企業外のインターネットや，その他企業外の無線LAN，公衆電話回線などが含まれる。
【００１５】
この情報処理システムの概略的な動作は次の通りである。アプリサーバ２０は，各端末装置１０を所有するユーザのスケジュールや行動範囲に関するデータを保持している。一方，各端末装置１０は，端末装置の位置を検出をするGPSセンサや，無線通信を行う通信装置を有する。それにより，端末装置１０は，アプリサーバ２０と通信可能なオンライン状態で，端末装置の位置情報や，WiFi通信のアクセスポイントの識別子であるSSID（Service Set Identifier)や，IPアドレスなどをアプリサーバ２０に送信する。
【００１６】
そして，アプリサーバ２０は，端末装置１０から送信されてきた各種情報と，保持しているスケジュールなどに基づいて，現在の端末装置の状況（以下，シーンと称する場合がある）と近い将来における状況（シーン）に応じて必要なアプリとアプリのデータとを，端末装置１０に送信する。例えば，アプリサーバ２０が，必要なアプリのダウンロード先情報，例えばURL，を有するメッセージを端末装置１０にプッシュ送信する。すると，端末装置１０が，そのダウンロード先情報に基づいて，現在必要なまたは近い将来必要になるアプリをアプリサーバ２０からダウンロードし，端末装置内の内部メモリに保存する。
【００１７】
その後，オフライン状態において，端末装置１０は，内部メモリに保存したアプリを実

行しデータを更新する。端末装置１０は，アプリの実行を終了させる時に，内部メモリに保存している更新されたデータを，セキュアなストレージシステムであるアプリサーバ２０にアップロードする。端末装置１０は，アプリの実行が終了すると，その更新されたデータを内部メモリから消去する。

【００１８】

上記のように，端末装置１０は，必要なときに必要な場所で必要なアプリを実行し，不要になると端末装置内からアプリ実行で更新されたデータを消去する。したがって，ユーザは，出先の顧客先においても，オフラインで業務やプライベートについてのアプリを実行させることができ，そのアプリ実行により生成されたデータを端末装置から削除することができるので，端末装置を紛失した場合のデータに対するセキュリティを高めることができる。

【００１９】

図２は，本実施の形態におけるアプリサーバの構成図である。アプリサーバ２０は，CPU２０１と，メインメモリであるRAM２０２と，表示装置２０３と，入力装置２０４と，ネットワークNETを介して外部と通信する通信装置２０５と，ハードディスクやフラッシュメモリなどの大容量メモリ２０６とを有する。

【００２０】

大容量メモリ２０６には，OS２１０と，アプリプッシュ制御プログラム２１１と，ユーザのスケジュールや端末情報を有するユーザ・端末データベース２１２が保存されている。さらに，大容量メモリ２０６には，端末装置にダウンロードされるHTMLアプリのプログラム２２１，２２３と，そのデータ２２２，２２４と，HTMLアプリを実行するランタイムライブラリ２２５と，各HTMLアプリに対応するデータについて，アプリサーバ２０と端末装置１０間で共有する暗号鍵や，そのデータが端末装置のどのシーンに対応するものかなどの情報を格納したデータ管理データベース２２６とが保存されている。

【００２１】

HTMLアプリはランタイムライブラリによって解釈され実行され，そして，ランタイムライブラリはOSによって解釈され実行される。したがって，HTMLアプリを端末装置に送信して端末装置上で実行させるためには，そのHTMLアプリを実行するランタイムライブラリも端末装置に送信する必要がある。但し，端末装置に既にランタイムライブラリが保存され実行可能になっている場合は，ランタイムライブラリを端末装置に送信する必要はない。

【００２２】

図３は，アプリプッシュ制御プログラム２１１の機能を示す図である。アプリプッシュ制御プログラム２１１を実行することにより実現される機能には，ユーザ・端末情報ＤＢ２１２を管理するユーザ・端末管理部２３０と，端末装置からアップロードされるセンサ値（位置情報，ＳＳＩＤ，ＩＰアドレスなど）と，ユーザのスケジュールなどに基づいて，端末装置の現在及び近い未来のシーンを検出する端末シーン検出部２３１とが含まれる。

【００２３】

さらに，アプリプッシュ制御プログラム２１１の機能には，検出した端末装置のシーンに基づいて，どのアプリとデータを端末装置にプッシュ送信すべきかを決定するアプリ・データ選択部２３２と，決定したアプリとデータ及びその暗号鍵などを端末装置に送信するアプリ送信制御部２３３と，データ管理ＤＢ２２６を管理するアプリ用データ管理部２３４とが含まれる。

【００２４】

図４は，本実施の形態における端末装置の構成図である。図４の端末装置１０は，スマートフォンやタブレット端末などである。端末装置１０は，CPU１０１と，メインメモリであるRAM１０２と，表示装置１０３と，操作入力を行うためのタッチスクリーン１０４と，無線通信を行う通信装置１０５と，端末装置の位置検出するGPSなどの各種センサ１０６とを有する。

【００２５】

さらに，端末装置１０は，ハードディスク（HDD)やフラッシュメモリなどのＳＳＤなど，大容量の補助メモリ１０７を有する。そして，補助メモリ１０７内には，OS１１０と，ブラウザ１１１と，アプリケーションプログラム群１１２とが保存されている。さらに，補助メモリ１０７には，アプリサーバ２０からダウンロードしたHTMLアプリ１２１，１２３と，それらのアプリを実行するランタイムライブラリ１１３とが保存され，HTMLアプリを起動するときに生成されたHTMLアプリのデータを保存するデータストレージ領域１２２，１２４を有する。

【００２６】

図５は，図４の端末装置のハードウエアとソフトウエアの関係を示す図である。端末装置１０は，CPU１０１やRAM１０２などのその他ハードウエア群１２０の上でOS１１０が動作する。そして，補助メモリ１０７に保存されているアプリケーションプログラム１１２がOS１１０上で実行され所定の機能を実現する。

【００２７】

一方，ブラウザ１１によりアプリサーバ２０からダウンロードされたHTMLアプリ１２１，１２３は，ランタイムライブラリ１１３により，端末装置内のローカルメモリである補助メモリ１０７内に保存される。そして，補助メモリ１０７内には，ランタイムライブラリに割り当てられたメモリ領域１４０が生成され，ランタイムライブラリ１１３のストレージ管理部１３２により管理される。

【００２８】

ランタイムライブラリ１１３は，アプリサーバ２０からブラウザ１１１を介してダウンロードされたHTMLアプリを起動制御するランチャ１３０と，暗号鍵を管理する鍵管理部１３１と，ランタイムライブラリに割り当てられたメモリ領域１４０を管理するストレージ管理部１３２とを有する。

【００２９】

ダウンロードされたHTMLアプリ１２１，１２３は，ランタイムライブラリ１１３によりメモリ領域１４０内に保存される。ここで，HTMLアプリ１２１は，HTMLアプリ１であり，HTMLアプリ１２３は，HTMLアプリ２であり，それぞれ異なるHTMLアプリである。そして，ランチャ１３０がメモリ領域１４０内のHTMLアプリを起動する時に，起動するHTMLアプリのデータを保存するデータストレージ領域１２２，１２４がメモリ領域１４０内に確保され，そこに，ダウンロードしたデータが保存される。

【００３０】

HTMLアプリ１２１，１２３がブラウザ１１１とランタイムライブラリ１１３により実行されると，実行中のデータの読み出しと書き込みが，HTMLアプリ１２１，１２３それぞれに関連付けられたデータストレージ領域１２２，１２４に対して実行される。特に，後述するとおり，HTMLアプリがウエブサーバからダウンロードされた場合は，そのウエブサーバのURLに関連付けられたデータストレージ領域にデータが保存され，各データストレージ領域のデータは隔離して管理される。

【００３１】

［第１の実施の形態］

図６は，第１の実施の形態におけるアプリ実行シーケンスの概略を示すフローチャート図である。図６にしたがってアプリ実行シーケンスの概略を説明した後に，詳細な説明を行う。

【００３２】

図６において，端末装置がアプリサーバと通信可能なオンライン状態において（S0)，端末装置１０は，端末装置の状況であるシーン（例えばプライベートまたは業務）に応じて必要なアプリとそのデータをアプリサーバからダウンロードし，それぞれ補助メモリ１０７内に保存する（S51)。この場合，アプリとそのデータが暗号化されている場合は，端末装置１０は，暗号鍵も併せてダウンロードする。

【００３３】

そして，オンライン状態中にウエブサーバからダウンロードしたアプリ（ウエブアプリ

）を実行した場合は，ブラウザが，ウエブサーバのURLに対応したストレージ領域を確保し，アプリの実行に伴ってデータを更新しストレージ領域内に書き込み，アプリの実行の終了に伴ってストレージ領域内のデータをアプリサーバにアップロードして，端末装置内のデータを削除する。オンライン状態中のアプリの実行は，図６には示されていない。

【００３４】

本実施の形態では，その後のオフライン状態（S5）において，端末装置１０が，ダウンロードして内部の補助メモリ内に保存したアプリ（ローカルアプリ）を実行する実行シーケンスを説明する。ランタイムライブラリ１１３は，アプリを起動する時に，端末装置内で未使用の外部アドレスであるURLを決定し，起動するアプリと関連付ける（S52)。起動するアプリとURLとの関連付けはデータベース化されて補助メモリ１０７内に保存される。

【００３５】

そして，ランタイムライブラリ１１３は，URLに対応するデータストレージ領域を補助メモリ内に確保する初期化処理を行い，ダウンロードしたアプリのデータをデータストレージ領域に書き込んで復元する（S53)。

【００３６】

次に，ランタイムライブラリ１１３が，URLを有するウエブサーバを起動し，そのURLと，アプリが保存されているアドレスとを指定してブラウザ１１１にアプリをダウンロードするよう指示する。この指示に応答して，ブラウザがそのURLにアクセスし，アプリをダウンロードする（S54）。このように，ブラウザ１１１に，見せかけの外部アドレスであるURLを有するウエブブラウザにアクセスさせることで，ブラウザにウエブアプリをダウンロードして実行するよう制御させる。その結果，ブラウザは，アプリの実行中のデータの読み出し及び書き込み動作を，そのURLに対応付けられたデータストレージ領域に対して実行する（S55)。しかも，ブラウザは，このデータストレージ領域をURL毎に隔離してアクセス管理する。

【００３７】

最後に，ブラウザは実行中のアプリを終了し，データストレージ領域内のデータをクリア，すなわち削除する。そして，ランタイムライブラリは，アプリ終了前にデータストレージ領域内のデータを退避し，アプリが終了した後，退避したデータをセキュリティ性の高いセキュアファイルシステム，例えばアプリサーバにアップロードして保存する（S56)。

【００３８】

そして，その後，再度，オンライン状態になると，アプリサーバ２０から端末装置１０にメッセージがプッシュ送信され，端末装置１０は，必要なアプリとそのデータの暗号化コンテンツと，暗号鍵とをアプリサーバ２０からダウンロードし，内部メモリである補助メモリ内に保存する。以下，上記と同様に，オフライン状態では，ブラウザが内部メモリに保存されているアプリをウエブアプリとして実行する。

【００３９】

上記のアプリ実行シーケンスで概略的に示したとおり，端末装置内の内部メモリである補助メモリ内に保存しているアプリ，つまりローカルアプリを起動するときに，端末装置内に未使用の外部アドレスであるURLを選択し，ブラウザにそのURLにアクセスして端末装置内のメモリに保存されているローカルアプリをダウンロードさせる。このようにフェイクの外部アドレスであるURLからダウンロードさせることで，ブラウザはローカルアプリをウエブアプリとして実行する。その結果，そのURLに対応して生成されたデータストレージ領域は，他のアプリのデータストレージ領域とは隔離して管理される。したがって，データストレージ領域内のデータを盗み取られることを抑制することができる。また，アプリの実行が終了すると，そのアプリのURLに対応するデータストレージ領域内のデータは削除される。これにより，端末装置を紛失した場合でも，端末装置内にはアプリが更新したデータが保存されないので，セキュリティ性を高めることができる。

【００４０】

［第１の実施の形態の詳細］

図７，図８，図９は，第１の実施の形態におけるアプリ実行シーケンスのフローチャート図である。

【００４１】

前述したとおり，前提として，アプリサーバ２０は，端末装置１０から送信されてきた位置情報，IPアドレス，SSIDなどの端末装置１０のシーンを類推するための各種情報と，保持している端末装置１０のユーザのスケジュールなどに基づいて，端末装置の現在の状況と近い将来におけるシーン（状況）を類推する。そして，アプリサーバ２０は，その端末装置のシーンに応じて必要なアプリとアプリのデータとを，端末装置１０に送信する。例えば，アプリサーバ２０が，必要なアプリのダウンロード先情報，例えばURL，を有するメッセージを端末装置１０に送信する。

【００４２】

図７参照

これに応答して，端末装置１０のランタイムライブラリのランチャ１３０は，そのダウンロード先情報URLにアクセスして，現在必要なまたは近い将来必要になるアプリとそのアプリのデータを暗号化した暗号化コンテンツと，暗号鍵の送信をアプリサーバ２０に要求し（S1)，アプリサーバ２０はそれらを端末装置１０に送信する（S2)。この暗号鍵は，例えば，アプリサーバと端末装置間で共有される共有鍵により暗号化されていてもよい。そして，ランチャ１３０は，鍵管理部１３１に暗号鍵の保存を要求し，鍵管理部１３１は暗号鍵を補助メモリ１０７内に保存する（S3)。さらに，ランチャ１３０は，ストレージ管理部１３２に暗号化コンテンツの保存を要求し，ストレージ管理部１３２はその暗号化コンテンツを補助メモリ１０７内に保存する（S4)。これで，端末装置１０は，その後のオフライン状態において，補助メモリ１０７に保存したアプリを実行可能状態になる。

【００４３】

その後，端末装置１０がアプリサーバ２０と通信不能のオフライン状態になる（S5)。このオフライン状態で，ランチャ１３０は，ユーザによるアプリ１の起動操作などのアプリ起動イベントを検知したり，現在の端末装置のシーンに基づいてアプリ１を起動することを決定すると，アプリ１に対応する外部アドレスであるURLを決定する（S6)。この外部アドレスは，端末装置内で未使用のアドレスである。以下の例では，この外部アドレスURLがURL1であるとする。そして，ランチャ１３０は，アプリ１とその外部アドレスURL1とが対応付けられたデータベースDB１を，例えば補助メモリ１０７内に保存する。ランチャ１３０がアプリ１に割り当てるURL1は，例えば，次のようなアドレスである。

http://171.0.0.1:5289/path/index.html

そして，ランチャ１３０は，アプリ１のデータの復元をストレージ管理部１３２に要求する（S7)。これに応答して，ストレージ管理部１３２は，アプリ１の暗号鍵を鍵管理部１３１から取得し，補助メモリ１０７に保存しているアプリ１のデータの暗号化コンテンツを暗号鍵により復号する（S9)。さらに，ストレージ管理部１３２は，アプリ１とその外部アドレスURL1の対応付けを有するデータベースDB1を参照して，URL1のデータストレージ領域を確保する初期化処理を，ブラウザ１１１に要求し（S11)，ブラウザはURL1のデータストレージ領域を補助メモリ１０７内に確保する（S12)。

【００４４】

図８参照

ブラウザ１１１がURL1のデータストレージ領域を初期化すると（S12)，ストレージ管理部１３２は，復号したアプリ１のデータを初期化したデータストレージ領域DSに書き込んで復元する（S13)。すなわち，後でブラウザ１１１がローカルアプリであるアプリ１をウエブアプリとして実行するので，アプリ１の復号データをデータストレージ領域DSに予め書き込んでおく必要がある。

【００４５】

次に，ランチャ１３０は，アプリ１の暗号化コンテンツをストレージ管理部１３２から取得し（S14)，更に，アプリ１の暗号鍵を鍵管理部１３１から取得する（S15)。そして，

ランチャ１３０は，アプリ１を暗号鍵により復号する（S16)。復号されたアプリ１は，端末装置内のいずれかの領域に保存される。

【００４６】

そして，ランチャ１３０は，URL1のWebサーバ１３３を起動し（S17)，ブラウザ１１１に，URL1のウエブサーバ１３３からアプリ１をURL1のWebサーバ１３３からダウンロードするよう指示する（S18)。このダウンロード指示には，URL1とアプリ１が保存されている端末装置内の領域情報とが含まれる。これに応答して，ブラウザ１１１は，URL1のWebサーバにアクセスし，アプリ１のダウンロードを要求する（S19）。それに応答して，Webサーバ１３３は，復号されているアプリ１をブラウザ１１１に送信し（S20)，ブラウザ１１１は，ダウンロードしたアプリ１をWebアプリケーションとして実行する（S21)。

【００４７】

図９参照

ブラウザ１１１は，アクセスしたURL1でそれに対応付けられたデータストレージ領域DSを検索し，検出すれば，アプリ１の実行中に，そのデータストレージ領域DS内のデータにアクセスし，データの読み出し処理と，アプリ実行による更新データの書き込み処理を行う。検索して検出できなければ，ブラウザ１１１は，URL1に対するデータストレージ領域を初期化してアプリ１を実行する。

【００４８】

上記のWebサーバ１３３は，端末装置内に設けられ，HTTPプロトコルでブラウザと通信することができる。したがって，ブラウザ１１１がURL1にアクセスすると，ブラウザ１は起動してWebサーバ１３３と接続状態になり，ブラウザ１１１が指定した端末装置内の領域情報内のアプリ１をダウンロードすることができる。これにより，ブラウザ１１１は，端末装置内に保存されたローカルアプリを外部のインターネット上のWebブラウザからダウンロードしたウエブアプリとして認識させられ，そのURL1に対応して確保されたデータストレージ領域DSに対してデータの読み出し，書き込み動作を実行する。このURL1に対応するデータストレージ領域DSに対してデータを書き込むのは，例えば，HTML5の規格でも規定されている動作である。

【００４９】

アプリ１の実行後，ランチャ１３０がアプリ１の終了を検知すると（S22)。アプリ１のデータの暗号化とアプリ１の実行の終了とをストレージ管理部１３２に要求する（S23)。これに応答して，ストレージ管理部１３２は，まず，アプリ１のデータをURL1のデータストレージ領域DSから退避（読み出して一時保存）する（S24)。さらに，ストレージ管理部１３２が，ブラウザ１１１にアプリ１の終了処理要求を行うと（S25)，ブラウザ１１１は，アプリ１を終了し，アプリ１に関連付けられているURL1のストレージ領域DS内のデータを消去する。ブラウザ１１１は，ウエブアプリの終了と認識しているので，上記のように，アプリ１の終了と共にURL1のストレージ領域DS内のデータを消去する。

【００５０】

ストレージ管理部１３２は，アプリ１の暗号鍵を鍵管理部１３１から取得し，退避していたアプリ１のデータを暗号化し，一時記憶する（S27)。その後，ランチャ１３０は，一定時間アプリ１の実行が行われない場合に，ストレージ管理部１３２からアプリ１の暗号化したデータを取得し（S29)，よりセキュアなファイルシステムであるアプリサーバ２０に，アップロードする（S30)。セキュアなファイルシステムは，アプリサーバ２０以外のファイルシステムでも良い。

【００５１】

以上の通り，ランチャ１３０がURL1のWebサーバ１３３を起動した状態で，ブラウザ１１１にURL1にアクセスしてアプリ１をダウンロードさせることで，ブラウザ１１１は，ローカルアプリであるアプリ１をウエブアプリと認識し，URL1に対応するデータストレージ領域DSにデータの読み出し書き込みを実行し，データストレージ領域DSへの他のアプリからのアクセスを制限し，アプリ１の終了時にそのデータストレージ領域DS内のデータを消去する。さらに，ランチャ１３０は，アプリ１の終了時にデータストレージ領域DSからデ

ータを退避し，適切なタイミングで暗号化してセキュアなファイルシステムであるアプリサーバ２０にアップロードする。

【００５２】

したがって，端末装置を紛失したとしても，端末装置内にはアプリ１により更新されたデータは消去されているし，アプリ１のデータストレージ領域DSは，他のアプリのデータストレージ領域とは隔離されて管理されるので，データに対するセキュリティを向上させることができる。

【００５３】

［第２の実施の形態］

第１の実施の形態において，アプリ１の実行中にURL1に対応付けられたデータストレージ領域に更新したデータが暗号化されずに書き込まれる。それに対して，第２の実施の形態におけるアプリ実行シーケンスでは，アプリ１の実行中にURL1に対応付けられたデータストレージ領域に更新したデータをリアルタイムで暗号化して保存する。そのために，読み出したデータを復号し書き込みデータを暗号化して書き込む処理を行う暗号・復号読み出し書き込み関数を，アプリ１の実行が開始されるときに登録し，アプリ１実行中のURL1のデータストレージ領域への読み出し書き込み処理を，その暗号・復号読み出し書き込み関数で処理させる。

【００５４】

図１０，図１１，図１２は，第２の実施の形態におけるアプリの実行シーケンスを示すフローチャート図である。以下，図７，図８，図９のアプリ実行シーケンスと異なる処理について主に説明する。

【００５５】

図１０参照

オンライン状態S0での処理S1-S4は，図７と同じである。さらに，オフライン状態S5での処理S6-S11も図７と同じである。

【００５６】

そして，ストレージ管理部１３２からのURL1に対応するデータストレージ領域の初期化要求に応答して，ブラウザ１１１は，URL1に対応するデータストレージ領域を補助メモリ１０７内に確保する初期化処理を行い（S12），さらに，ブラウザ１１１は，URL1に対応するデータストレージ領域への暗号・復号読み出し書き込み関数を，ブラウザエンジン内の読み出し書き込み関数テーブルに登録する（S12A）。

【００５７】

図１３は，ブラウザエンジン内の読み出し書き込み関数テーブルを示す図である。ブラウザ１１１は，URL1への読み出し書き込み命令を実行すると，ブラウザエンジン１１１Ｅ内の読み出し書き込み（Ｒ／Ｗ）関数テーブル内のURL1に対応するR/W関数のアドレス２が参照され，ミドルエウアMW内のアドレス２に対応する暗号・復号読み出し書き込み（R/W）関数が，コールバック関数（Call Back Function）として呼び出されて，読み出し書き込み命令の処理が行われる。このアドレス２に対応する暗号・復号読み出し書き込み（R/W）関数は，一種のAPI(Application Program Interface)である。

【００５８】

なお，図１３では，URL2への読み出し書き込み命令に対してもアドレス２の暗号・復号読み出し書き込み（R/W)関数が呼び出されるように登録されている。また，ブラウザ１１１によるURL3に対するデータ領域への通常の読み出し書き込み命令が実行されると，ブラウザエンジン１１１Ｅ内のアドレス３に登録されている通常読み出し書き込み関数が読み出される。

【００５９】

図１１参照

ストレージ管理部１３２は，復号したデータを，初期化したURL1のデータストレージ領域SDに復元する（S13A)。この復元処理は，URL1のデータストレージ領域SDへのデータの書き込み処理であり，登録された暗号・復号読み出し書き込み関数が呼び出されて，その

関数により復号データは暗号化されてURL1のデータストレージ領域SDに書き込まれる。

【００６０】

図１２参照

ブラウザ１１１がアプリ１を実行すると（S21），実行中のデータの読み出し，書き込み処理は，登録された暗号・復号読み出し書き込み関数で処理される（S21A)。したがって，更新されたデータは，この暗号・復号読み出し書き込み関数で暗号化されてデータストレージ領域SDに書き込まれ，データストレージ領域SDから読み出されたデータは復号される。これによりブラウザ１１１によるアプリ１の実行中のデータアクセスは，この関数を呼び出すことで実行され，データはリアルタイムで暗号化されてURL1のデータストレージ領域SDに書き込まれる。

【００６１】

そして，アプリ１の終了時には，図９のようにストレージ管理部１３２がデータストレージ領域SD内のデータを暗号化する処理は不要になる。そのため，図１２では，ランチャ１３０がアプリ１の終了を検知すると（S22)，ストレージ管理部１３２に対して，アプリ１のデータの退避とアプリ１の終了を要求し（S23A)，それに応答して，ストレージ管理部１３２は，アプリ１の暗号化済みのデータをURL1のデータストレージ領域から退避しておくだけであり，改めて暗号化処理を行う必要はない。そして，一定時間アプリ１の実行がない場合に，ランチャ１３０は，退避した暗号化データをストレージ管理部１３２から取得して，アプリサーバ２０にアップロードする（S30)。

【００６２】

このように，ブラウザエンジン１１１Ｅ内に，URL1に対するデータストレージ領域SDへの読み出しと書き込み処理を専用に行う暗号・復号読み出し書き込み関数を登録しておくことで，ブラウザ１１１がURL1のアプリ１のデータアクセス処理を実行するとき，この登録した関数がフックされて呼び出されるので，リアルタイムにデータを暗号化してデータストレージ領域SD内に保存することができる。これにより，オフライン状態で端末装置１０を紛失しても，アプリ実行中のデータを盗まれることが抑制され，データのセキュリティを高めることができる。

【００６３】

［第３の実施の形態］

第３の実施の形態では，HTMLアプリのデータを，端末装置１０の状況に応じて，すなわちプライベートや業務などの状況（シーン）に応じて，区別して管理する。それを行うために，アプリサーバ２０と端末装置１０とは，アプリケーションと，データと，そのデータのシーンと，そのシーンでのアプリのデータについての暗号鍵の情報を有するデータ管理DBを共有する。そして，オンライン状態で，アプリサーバ２０が端末装置１０のシーンを検出して，アプリサーバ２０が，検出したシーンに対するアプリとデータと暗号鍵と，そのアプリやデータの使用条件を記載したポリシーファイルとを，端末装置１０に送信する。アプリサーバ２０は，データ管理DBを参照して，アプリとシーン毎にポリシーファイルを作成する。

【００６４】

そして，オフライン状態で，ダウンロードされたアプリとデータに対する起動を行う時に，端末装置１０内の鍵管理部が，ポリシーファイルを参照して，起動しようとするアプリとデータの使用がアプリサーバにより許可されていたかを確認する。これにより，不正に端末装置を取得した第三者が，端末装置のセンサに虚偽のシーン状態（例えばプライベートであるにもかかわらず業務のシーン状態）を検出させ，内部メモリに保存されているアプリとデータ（業務のデータ）を不正に使用する試みを，防止できる。

【００６５】

さらに，アプリの終了時に，再度，鍵管理部が現在のシーンを検出し，アップロードするデータをどのアプリのどのシーンに対して保管すべきかの情報を有するポリシーファイルを作成し，アプリサーバ２０に暗号化データとポリシーファイルとを共にアップロードする。アプリサーバ２０は，このポリシーファイルを参照して，アプリと正しいシーンに

対するデータを保存することができる。

【００６６】

図１４は，アプリサーバが保持するデータ管理テーブルと各端末装置が保持するデータ管理テーブルの例を示す図である。図１４に示されるとおり，アプリサーバは，全ての端末１０－１，１０－２，１０－３それぞれについて，データ管理DBを保持している。端末１０－１についてのデータ管理DBは，アプリ１について，端末のシーンがプライベートの場合の鍵名KEY1と，端末のシーンが業務の場合の鍵名KEY2と，それぞれについての，端末内の保存状態の情報とを有する。この鍵名KEY1は，例えば，アプリ名とシーンとを有するデータ名でもある。同様に，端末１０－１についてのデータ管理DBは，アプリ２についても，同様に，端末のシーンがプライベートの場合の鍵名KEY3と，業務の場合の鍵名KEY4とを有する。

【００６７】

上記の鍵名は，アプリケーションがword（wordは登録商標）で，そのデータがプライベートに対するものであれば，word-private_xxx.keyなどである。鍵名には，アプリ名とシーンの情報が含まれている。

【００６８】

一方，各端末装置は，それぞれの端末装置に保存されたデータのデータ管理DBを保持している。図１４の例では，端末装置１０－１が保持するデータ管理DBは，アプリサーバが端末装置１０－１について保持するデータ管理DBと，アプリ名，鍵名，シーンが一致している。ただし，端末装置１０－１が保持するデータ管理DBは，端末内の保存場所のデータを有している。

【００６９】

図１４で示したとおり，アプリサーバと端末装置は，特定のアプリの特定のシーンについての鍵情報を共有する。これにより，アプリサーバと端末装置間だけでデータの暗号化と復号とが可能になる。

【００７０】

図１５は，アプリサーバ２０と端末装置１０内の鍵管理部１３１とが生成するポリシーファイルPFの例を示す図である。アプリ１についてのポリシーファイルは，端末のシーンがプライベートの場合のデータに添付されるポリシーファイルPF1と，端末のシーンが業務の場合のデータに添付されるポリシーファイルPF2とが生成される。ポリシーファイルPF1の鍵名は，アプリ１とシーン１の情報を有する，word-private_xxx.keyであり，署名hijklmが付加される。ポリシーファイルPF2の鍵名は，アプリ１とシーン２の情報を有する，word-business_xxx.keyであり，署名opqrstが付加される。また，ポリシーファイルPF3の鍵名は，アプリ２とシーン１の情報を有する，exel-private_xxx.keyであり，署名uwxyzが付加される。ポリシーファイルPF4の鍵名は，アプリ２とシーン２の情報を有する，exel-business_xxx.keyであり，署名abcdeが付加される。

【００７１】

端末装置１０は，アプリサーバ２０からアプリとそのデータをダウンロードするときに，それらの利用条件（アプリとシーン）を記述したポリシーファイルもダウンロードする。そして，オフライン状態で，端末のあるシーンが検出されると，あるアプリが起動されそのシーンについてのデータが使用される。その際に，端末装置１０の鍵管理部がこのポリシーファイルPFを参照して，アプリサーバ２０がオンライン状態で許可した特定のアプリの特定のシーンに対するデータであるか否かをチェックする。したがって，悪意のある第三者が，不正に端末装置を盗みたいデータに対するシーンにおいた場合に，シーンが異なるためそのデータの使用が許可されず，データについてのセキュリティ性を高めることができる。

【００７２】

また，端末装置１０は，アプリを終了する時に，鍵管理部に端末装置のシーンを検出させてポリシーファイルPFを生成させ，退避させた暗号化データにそのポリシーファイルPFを添付して，アプリサーバなどのセキュアなファイルシステムにアップロードする。これ

により，アプリサーバは，どのアプリのどのシーンのデータかをポリシーファイルから検出して，そのデータを正しいシーンに対するデータとして更新することができる。

【００７３】

図１６，図１７，図１８は，第３の実施の形態におけるアプリ実行シーケンスのフローチャート図である。以下，図７，図８，図９のアプリ実行シーケンスと異なる処理について主に説明する。

【００７４】

図１６参照

オンライン状態S0で，アプリサーバ２０は，端末装置から端末のシーンに対応するセンサ情報を取得し，端末装置のユーザのスケジュール情報などを参照して，端末装置の現在のシーン及び近い将来のシーンに対応したアプリとそのデータを選択する(S40）。さらに，アプリサーバ２０は，図１４のデータ管理DBを参照して，図１５に示したデータ毎のポリシーファイルを作成する（S41)。

【００７５】

そして，アプリサーバ２０は，例えば，選択した現在のシーン及び近い将来のシーンに対応したアプリとそのデータをダウンロードするよう要求するメッセージを，端末１０にプッシュ送信する。これに応答して，端末装置のランチャ１３０は，プッシュ送信されたメッセージに記述されているアプリサーバのURLにアクセスして，ダウンロードするよう要求されているアプリの鍵，暗号化コンテンツの送信を要求する（S1)。これに応答して，アプリサーバ２０は，暗号鍵と，暗号化コンテンツ（アプリとそのデータ）と，ポリシーファイルPFを端末装置１０に送信する。そして，ランチャ１３０は，鍵管理部１３１に暗号鍵とポリシーファイルPFを補助メモリ１０７内に保存させ（S3)，ストレージ管理部１３２に暗号化コンテンツを補助メモリ１０７内に保存させる（S4)。

【００７６】

その後，オフライン状態S5で，ランチャ１３０は，現在の端末のシーン１からアプリ１の起動を決定し，アプリ１とシーン１（以下AP1+SC1)に対応するURL1を決定し，ランチャ１３０は，アプリ１及びシーン１（AP1+SC1)とその外部アドレスURLとが対応付けられたデータベースDB1を，例えば補助メモリ１０７内に保存する（S6A)。そして，ランチャ１３０は，ストレージ管理部１３２に，アプリ１及びシーン１（AP1+SC1)に対するデータの復元を要求する（S7A)。

【００７７】

ストレージ管理部１３２は，データ管理DBを参照して，アプリ１及びシーン１（AP1+SC1)のデータを検出し（S42)，その鍵名の暗号鍵を鍵管理部１３１に要求する（S8A)。これに応答して，鍵管理部１３１は，ポリシーファイルPFを参照し，現在の端末のシーン１でアプリ１のデータの利用を許可できるかチェックする（S43)。もし，端末装置を取得した悪意の第三者が，実際のシーンと異なる状況に端末装置を制御して，アプリ１及びシーン１（例えば業務）のデータへのアクセスを試みている場合に，オンライン状態でアプリサーバ２０が作成したポリシーファイルPFにアプリ１及びシーン１のデータの使用を許可するものがなければ，データへの不正なアクセスを抑制することができる。ポリシーファイルPFを参照してデータの使用を許可できないと判断した場合は，鍵管理部１３１は，ユーザに認証情報の入力を要求して，データの使用許可を求めるようにしてもよい。

【００７８】

鍵管理部１３１は，アプリ１及びシーン１（AP1+SC1)のデータの使用を許可する場合は，ストレージ管理部１３２に暗号鍵を渡し，これにより，ストレージ管理部１３２は，保存していた暗号化コンテンツからデータを復号する（S9)。そして，ストレージ管理部１３２は，ブラウザ１３３にURL1のデータストレージ領域の初期化要求を行い，ブラウザ１１１は，URL1に対するデータストレージ領域を補助メモリ１０７内に確保する初期化処理を行う（S12)。

【００７９】

図１７参照

図８と異なる処理は，ランチャ１３０が，アプリ１及びシーン１（AP1+SC1)の暗号化コンテンツと，暗号鍵をストレージ領域１３２から取得する処理S14A,S15Aである。

【００８０】

図１８参照

ブラウザ１１１は，アプリ１を実行し（S21)，更新したデータをデータストレージ領域SDに書き込む。そして，ランチャがアプリ１の終了を検知すると（S22)，ランチャ１３０は，アプリ１及びシーン１（AP1+SC1)のデータの暗号化と終了をストレージ管理部１３２に要求する（S23A)。これに応答して，ストレージ管理部１３２は，アプリ１及びシーン１のデータをURL1のデータストレージ領域SDから退避し，ブラウザ１１１にアプリ１の終了処理を要求する（S25)。これにより，ブラウザ１１１は，アプリ１を終了し，データストレージ領域SDのデータを消去する。

【００８１】

そして，ストレージ管理部１３２は，アプリ１及びシーン１（AP1+SC1）の暗号鍵を取得し（S26A)，データを暗号化して一時記憶する（S27)。さらに，ストレージ管理部１３２は，端末のシーンに基づきポリシーファイルPFを生成することを鍵管理部１３１に依頼する（S44)。鍵管理部１３１は，現在の端末のシーンを検出し，ポリシーファイルPFを生成し，ストレージ管理部１３２に返信する（S45)。このポリシーファイルPFは一時記憶される。

【００８２】

一定時間アプリ１の実行がない場合に，ランチャ１３０は，アプリ１及びシーン１（AP1+SC1)の暗号化データと鍵管理部が生成したポリシーファイルPFとを，ストレージ管理部１３２に要求し取得する（S29A)。そして，ランチャ１３０は，シーン１（AP1+SC1)の暗号化データとポリシーファイルPFを，アプリサーバ２０にアップロードする（S30A)。これに応答して，アプリサーバ２０は，ポリシーファイルPFの情報に基づいて，アップロードされてきた暗号化データをポリシーファイルPF内のアプリ１及びシーン１に対応するデータとして保存する（S46)。さらに，アプリサーバ２０は，ポリシーファイルPFに基づいて，データ管理DBを更新する。

【００８３】

これにより，アプリサーバ２０は，次回，端末装置１０がアプリ１及びシーン１の暗号化データのダウンロードを要求した場合に，その暗号化データとポリシーファイルPFとを端末装置に送信することができる。

【００８４】

アプリ名とシーン名が含まれているポリシーファイルPFがアプリサーバ２０にアップロードされるので，業務用の暗号化データがプライベート用の暗号化データとして保存され，その後，プライベートのシーン下で業務用の暗号化データが悪意の第三者に覗かれることを抑制できる。また，ポリシーファイルPFによりデータ管理DBも更新されるので，その後のオンライン状態で，データ管理DBを参照してポリシーファイルPFを作成することができる。

【００８５】

以上の通り，第３の実施の形態では，アプリと端末のシーンとの組み合わせによりデータを管理し，ポリシーファイルを利用することで，オンライン状態でアプリサーバが許可したデータの利用を，オフライン状態で端末装置の鍵管理部が確認することができる。これにより，悪意の第三者が端末装置のシーンを意図的に実際とは異なるシーンに変更して，秘密データをのぞき見るようにすることを防止することができる。また，ポリシーファイルを利用して，セキュアなファイルシステムであるアプリサーバに，アプリとシーンに対応したデータとして安全に保存させることができる。

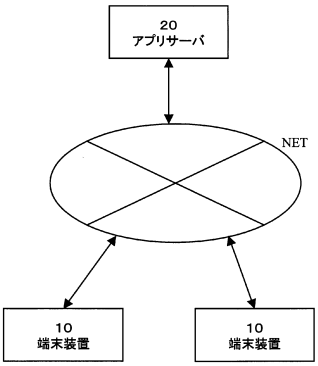
【産業上の利用可能性】

【００８６】

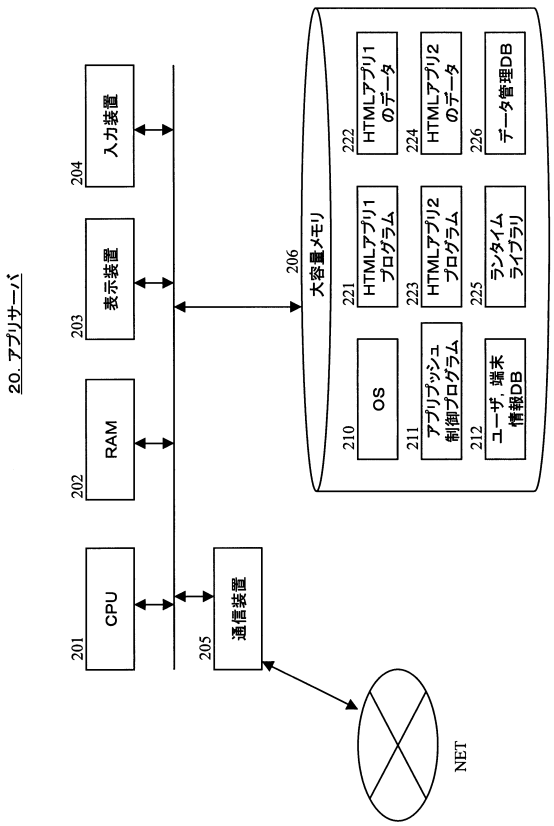
本実施の形態によれば，アプリプッシュシステムにおいて，ローカルアプリが実行中に更新するデータのセキュリティ性を高めることができる。

【符号の説明】
【００８７】
１０：端末装置
２０：アプリサーバ
１０７：補助メモリ
１１１：ブラウザ
１１３：ランタイムライブラリ
１３０：ランチャ
１３１：鍵管理部
１３２：ストレージ管理部

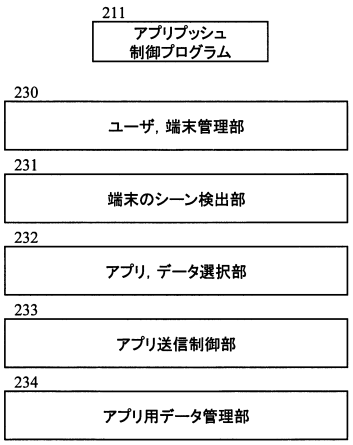
【図１】



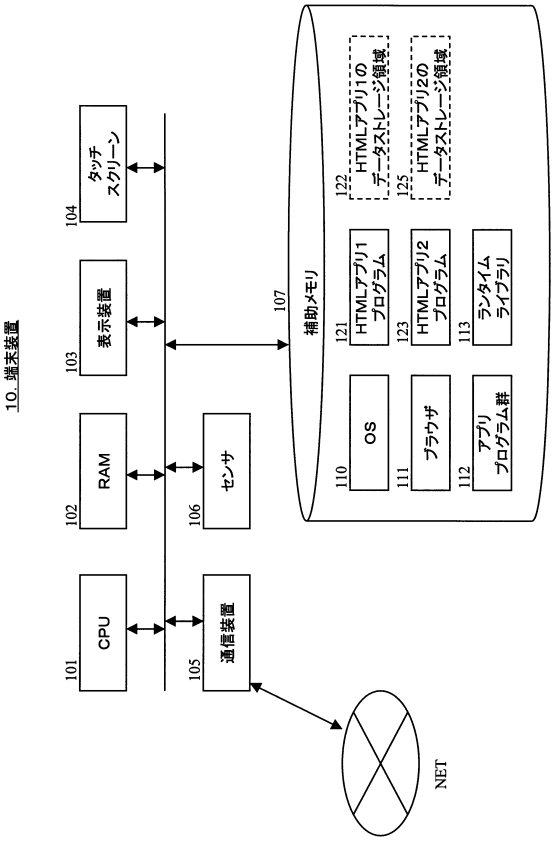
【図２】



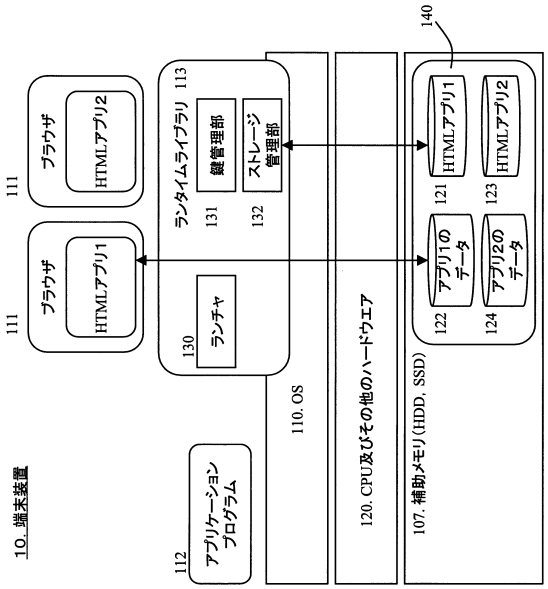
【図３】


211
アプリプッシュ
制御プログラム
230
ユーザ，端末管理部
231
端末のシーン検出部
232
アプリ，データ選択部
233
アプリ送信制御部
234
アプリ用データ管理部

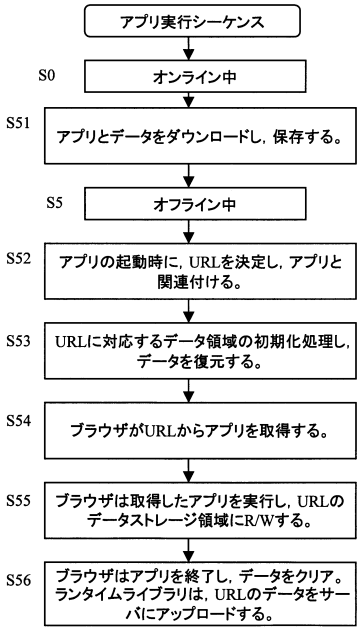
【図４】


10. 端末装置
101 CPU
102 RAM
103 表示装置
104 タッチスクリーン
105 通信装置
106 センサ
107 補助メモリ
110 OS
111 ブラウザ
112 アプリプログラム群
113 ランタイムライブラリ
121 HTMLアプリ1プログラム
122 HTMLアプリ1のデータストレージ領域
123 HTMLアプリ2プログラム
125 HTMLアプリ2のデータストレージ領域
NET

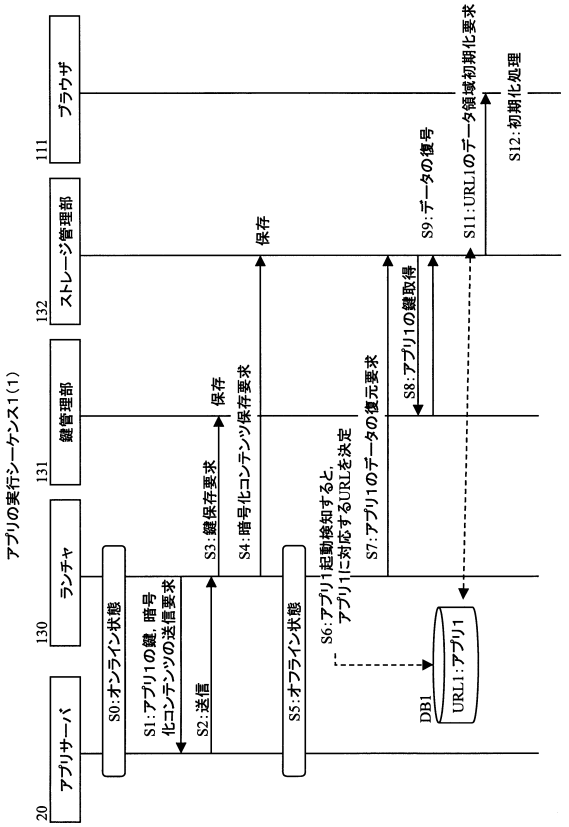
【図５】


10. 端末装置
111 ブラウザ
HTMLアプリ2
111 ブラウザ
HTMLアプリ1
ランタイムライブラリ 113
鍵管理部 131
ストレージ管理部 132
ランチャ 130
アプリケーションプログラム 112
110. OS
120. CPU及びその他のハードウエア
140
107. 補助メモリ(HDD, SSD)
HTMLアプリ1 121
HTMLアプリ2 123
アプリ1のデータ 122
アプリ2のデータ 124

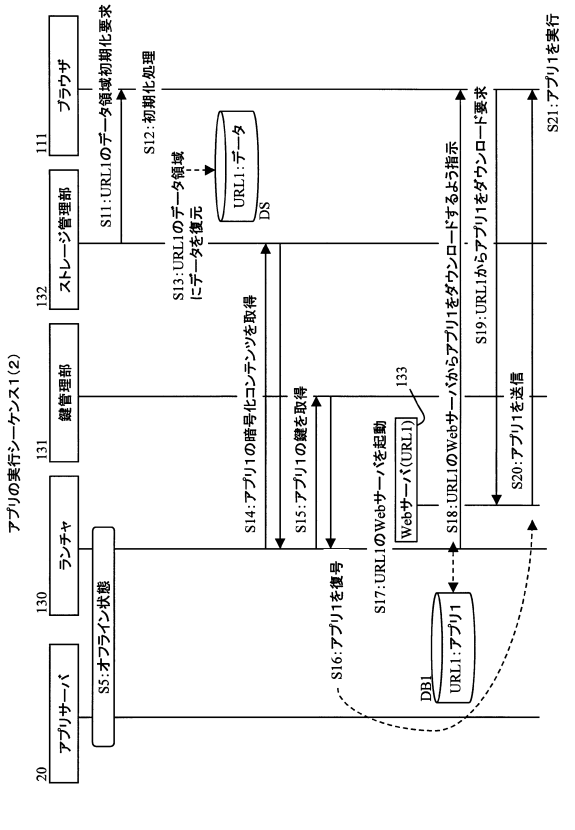
【図６】


アプリ実行シーケンス
S0
オンライン中
S51
アプリとデータをダウンロードし，保存する。
S5
オフライン中
S52
アプリの起動時に，URLを決定し，アプリと関連付ける。
S53
URLに対応するデータ領域の初期化処理し，データを復元する。
S54
ブラウザがURLからアプリを取得する。
S55
ブラウザは取得したアプリを実行し，URLのデータストレージ領域にR/Wする。
S56
ブラウザはアプリを終了し，データをクリア。ランタイムライブラリは，URLのデータをサーバにアップロードする。

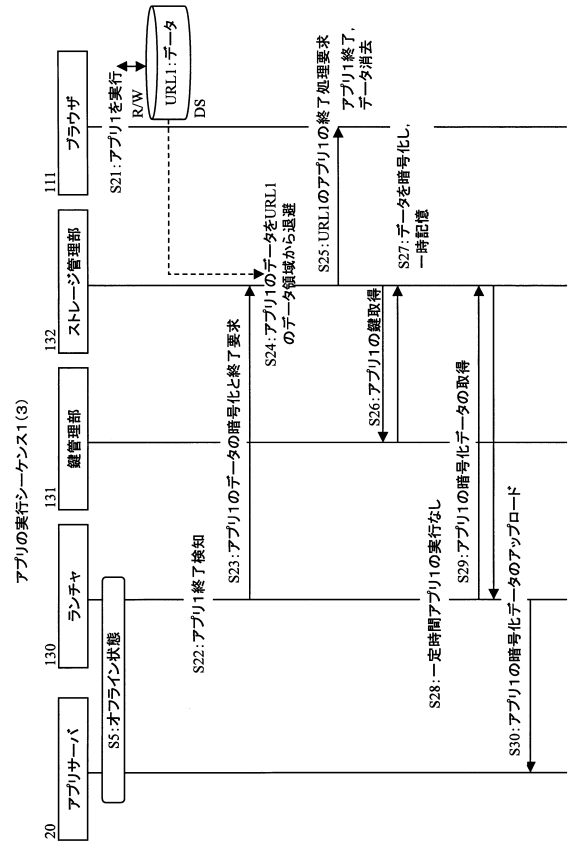
【図７】


アプリの実行シーケンス1(1)
20 アプリサーバ
130 ランチャ
131 鍵管理部
132 ストレージ管理部
111 ブラウザ
S0:オンライン状態
S1:アプリ1の鍵，暗号化コンテンツの送信要求
S2:送信
S3:鍵保存要求
保存
S4:暗号化コンテンツ保存要求
保存
S5:オフライン状態
S6:アプリ1起動検知すると，アプリ1に対応するURLを決定
S7:アプリ1のデータの復元要求
S8:アプリ1の鍵取得
S9:データの復号
S11:URL1のデータ領域初期化要求
S12:初期化処理
DB1
URL1:アプリ1

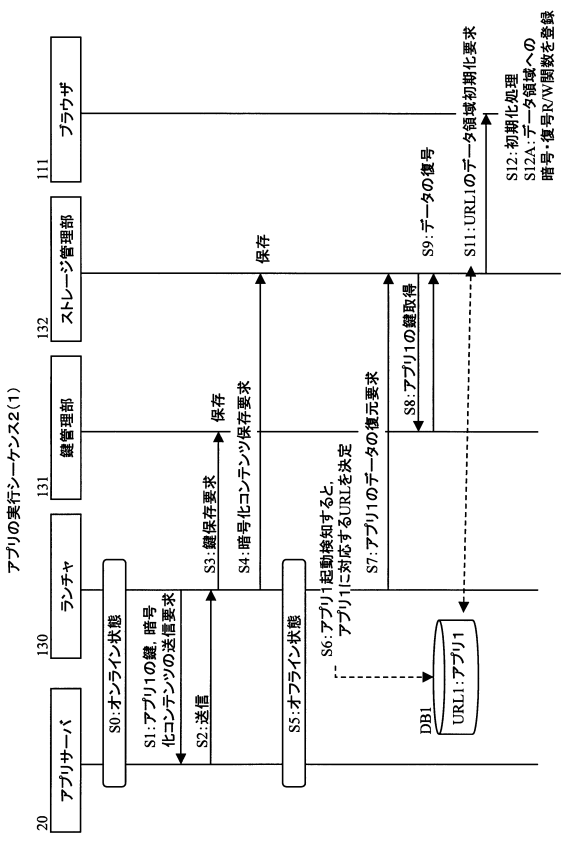
【図８】


アプリの実行シーケンス1(2)
20 アプリサーバ
130 ランチャ
131 鍵管理部
132 ストレージ管理部
111 ブラウザ
S5:オフライン状態
S11:URL1のデータ領域初期化要求
S12:初期化処理
S13:URL1のデータ領域にデータを復元
URL1:データ
DS
S14:アプリ1の暗号化コンテンツを取得
S15:アプリ1の鍵を取得
133
S16:アプリ1を復号
S17:URL1のWebサーバを起動
Webサーバ(URL1)
S18:URL1のWebサーバからアプリ1をダウンロードするよう指示
S19:URL1からアプリ1をダウンロード要求
S20:アプリ1を送信
S21:アプリ1を実行
DB1
URL1:アプリ1

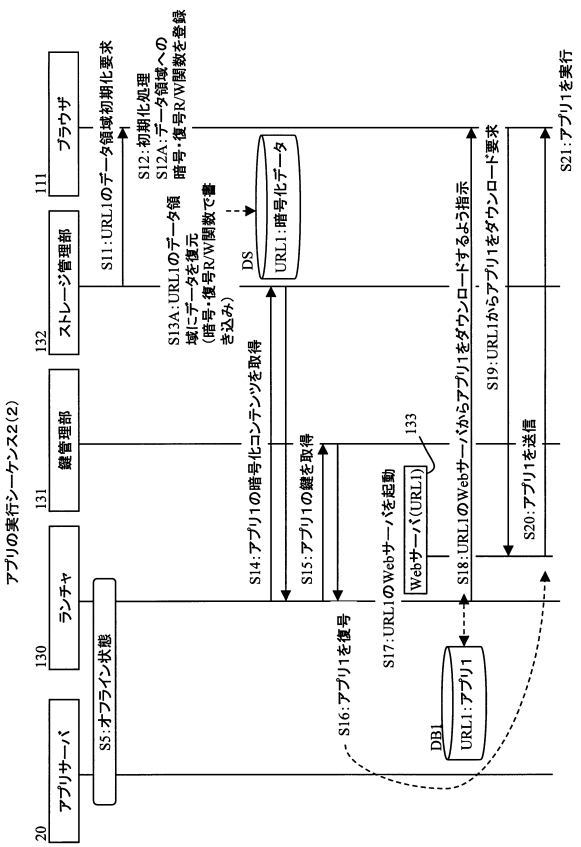
【図９】


アプリの実行シーケンス1(3)
20 アプリサーバ
130 ランチャ
131 鍵管理部
132 ストレージ管理部
111 ブラウザ
S5:オフライン状態
S21:アプリ1を実行
R/W
URL1:データ
DS
S22:アプリ1終了検知
S23:アプリ1のデータの暗号化と終了要求
S24:アプリ1のデータをURL1のデータ領域から退避
S25:URL1のアプリ1の終了処理要求
アプリ1終了，データ消去
S26:アプリ1の鍵取得
S27:データを暗号化し，一時記憶
S28:一定時間アプリ1の実行なし
S29:アプリ1の暗号化データの取得
S30:アプリ1の暗号化データのアップロード

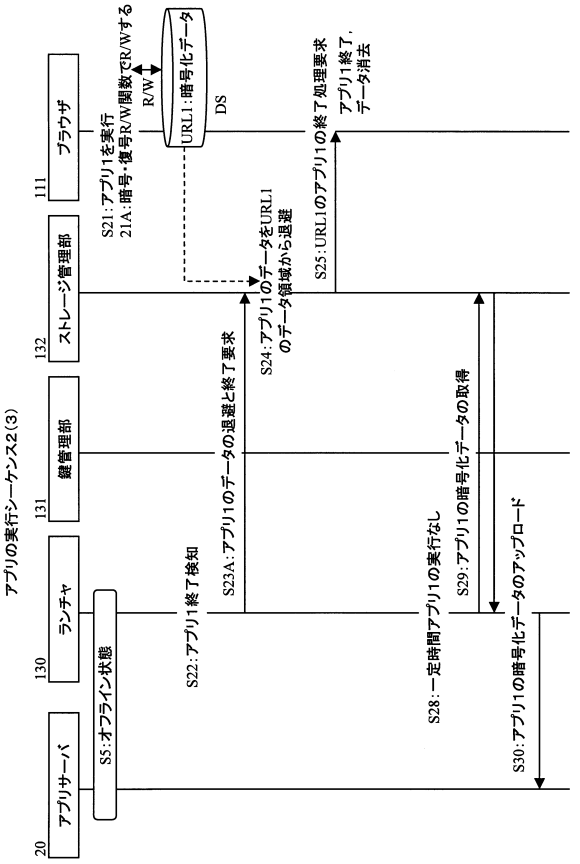
【図１０】


アプリの実行シーケンス2(1)
20 アプリサーバ
130 ランチャ
131 鍵管理部
132 ストレージ管理部
111 ブラウザ
S0:オンライン状態
S1:アプリ1の鍵，暗号化コンテンツの送信要求
S2:送信
S3:鍵保存要求
保存
S4:暗号化コンテンツ保存要求
保存
S5:オフライン状態
S6:アプリ1起動検知すると，アプリ1に対応するURLを決定
S7:アプリ1のデータの復元要求
S8:アプリ1の鍵取得
S9:データの復号
S11:URL1のデータ領域初期化要求
S12:初期化処理
S12A:データ領域への暗号・復号R/W関数を登録
DB1
URL1:アプリ1

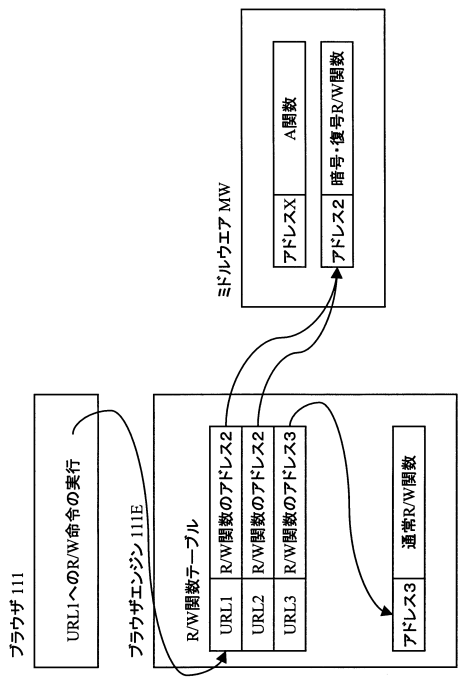
【図１１】



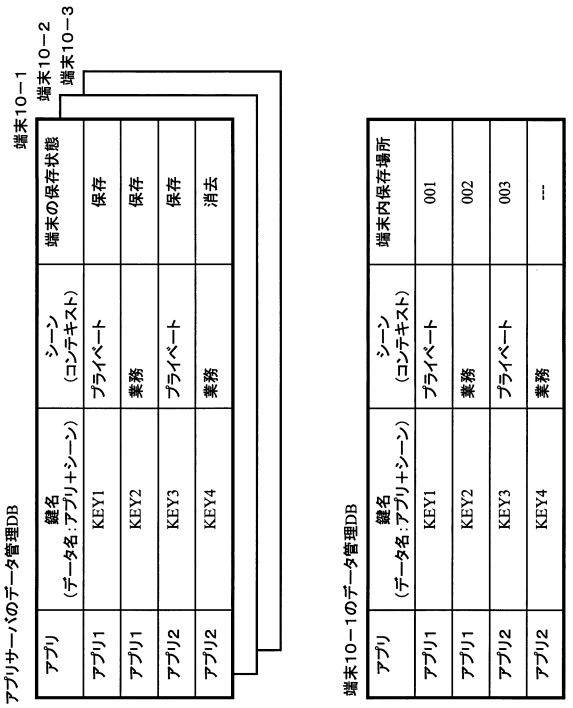
【図１２】



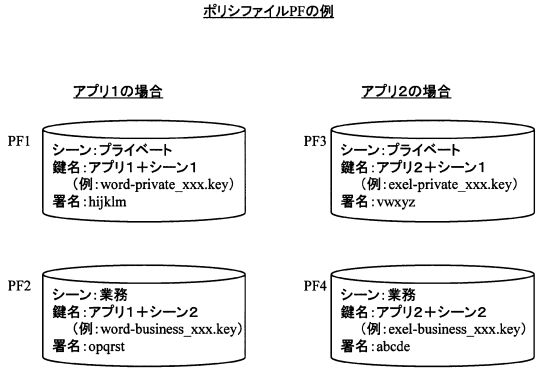
【図１３】



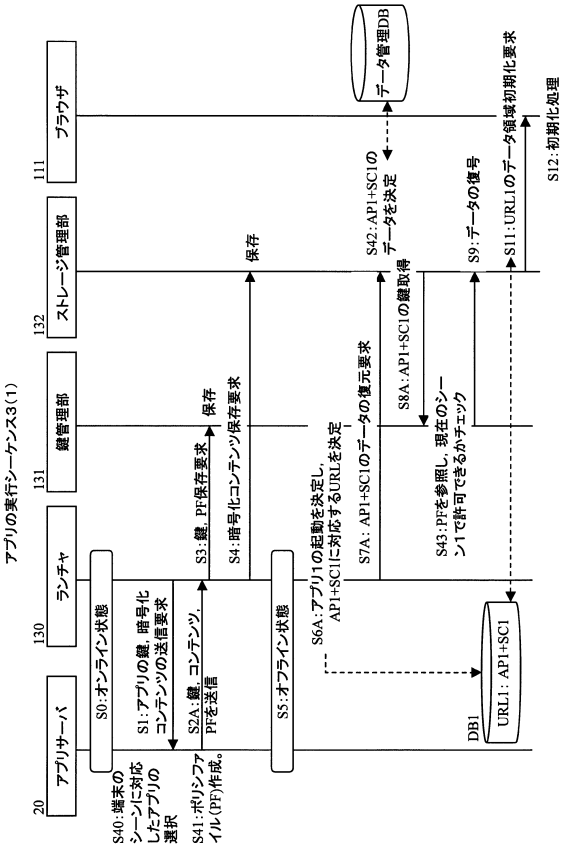
【図１４】



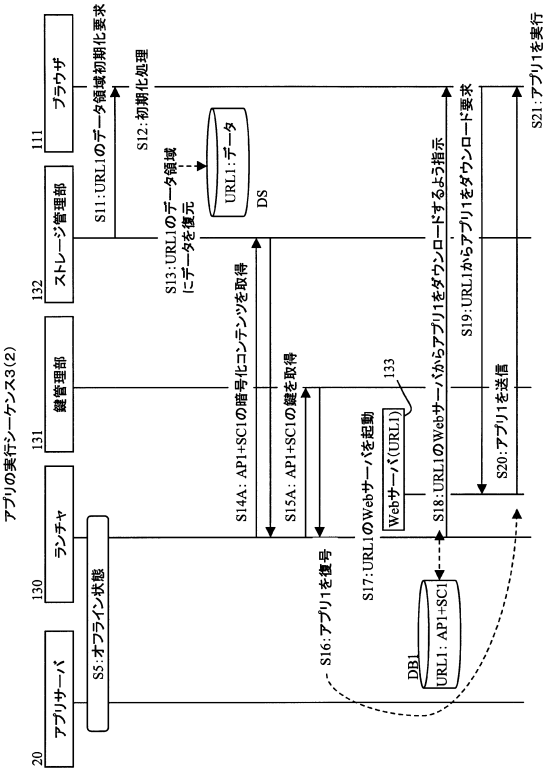
【図１５】



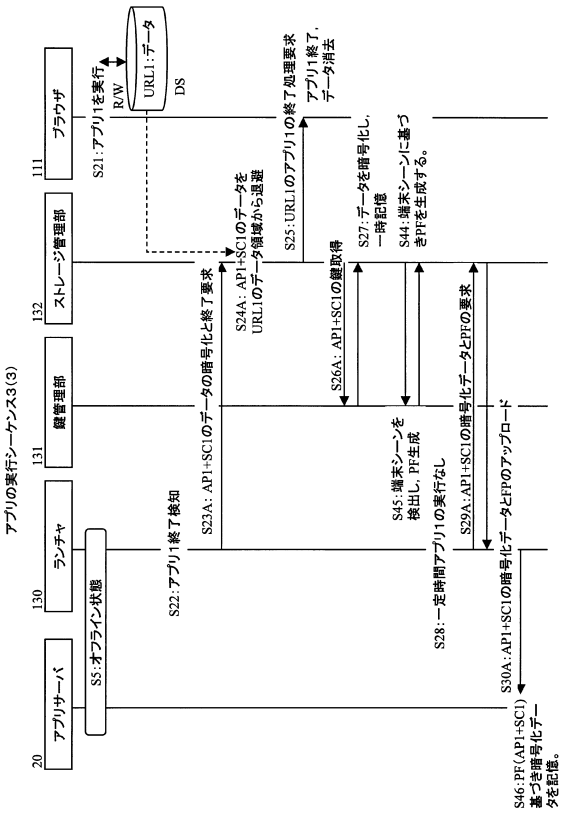
【図１６】



【図１７】



【図１８】



フロントページの続き

(72)発明者　中村　洋介
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　坂本　拓也
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　二村　和明
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　石川　亮

(56)参考文献　特開２００５－２３５０５５（ＪＰ，Ａ）
特開２００４－０９４６８２（ＪＰ，Ａ）
国際公開第２０１３／０４２４１１（WO，Ａ１）
菅原 英治，僕にも作れるソーシャル・ネットワークの世界 続・Ｗｉｎｄｏｗｓ Ａｚｕｒｅ上にＦａｃｅｂｏｏｋアプリを開発しよう！，Ｇ－ＣＬＯＵＤ Ｍａｇａｚｉｎｅ ２０１１ Ｓｕｍｍｅｒ，日本，（株）技術評論社，２０１１年　8月　1日，pp.78-109
Web Storage，W3C，２０１３年　4月　9日，W3C Proposed Recommendation 9 April 2013，ＵＲＬ，http://www.w3.org/TR/2013/PR-webstorage-20130409/

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　９／４４５
Ｇ０６Ｆ　１３／００
Ｇ０６Ｆ　１５／００
Ｇ０６Ｆ　２１／６２
Ｈ０４Ｌ　　９／０８