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

特許第4099070号
(P4099070)

(45)発行日　平成20年6月11日(2008.6.11)　(24)登録日　平成20年3月21日(2008.3.21)

(51)Int.Cl.		F I		
G06F 21/22	(2006.01)	G06F	9/06	660J
G06F 9/445	(2006.01)	G06F	9/06	640A
H04Q 7/38	(2006.01)	H04B	7/26	109R

請求項の数 12　(全 56 頁)

(21)出願番号　特願2002-589970 (P2002-589970)
(86)(22)出願日　平成14年5月14日 (2002.5.14)
(86)国際出願番号　PCT/JP2002/004643
(87)国際公開番号　WO2002/093361
(87)国際公開日　平成14年11月21日 (2002.11.21)
審査請求日　平成14年10月25日 (2002.10.25)
(31)優先権主張番号　特願2001-143810 (P2001-143810)
(32)優先日　平成13年5月14日 (2001.5.14)
(33)優先権主張国　日本国(JP)

(73)特許権者　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100098084
弁理士　川▲崎▼　研二
(72)発明者　夏野　剛
東京都千代田区永田町二丁目１１番１号
山王パークタワー　株式会社エヌ・ティ・ティ・ドコモ　知的財産部内
(72)発明者　山本　正明
東京都千代田区永田町二丁目１１番１号
山王パークタワー　株式会社エヌ・ティ・ティ・ドコモ　知的財産部内

最終頁に続く

(54)【発明の名称】移動体端末の記憶部に格納されたプログラムを管理するシステム

(57)【特許請求の範囲】
【請求項１】
端末装置が有する１以上のメモリエリアの各々に格納されているアプリケーションの識別情報を含む管理データを記憶する記憶手段と、
サーバ装置から通信網を介しアプリケーションを受信する受信手段と、
前記管理データに基づき前記端末装置が有する前記１以上のメモリエリアのうちアプリケーションを格納すべきメモリエリアを決定する決定手段と、
前記受信手段により取得されたアプリケーションと、当該アプリケーションに関し前記決定手段により決定されたメモリエリアに当該アプリケーションの格納を指示する格納要求とを、通信網を介し前記端末装置に送信する送信手段と、
前記送信手段により送信されたアプリケーションが前記送信手段により送信された格納要求により指示されるメモリエリアに格納されていることを示すように前記管理データを更新する更新手段と
を備える中継装置。
【請求項２】
前記送信手段は、前記管理データにより前記端末装置が有する前記１以上のメモリエリアのうちいずれかのメモリエリアに格納されていることが示される一のアプリケーションの削除を指示する削除要求を、通信網を介し前記端末装置に送信し、
前記更新手段は、前記一のアプリケーションが前記端末装置が有する前記１以上のメモリエリアのいずれにも格納されていないことを示すように前記管理データを更新する

請求項１に記載の中継装置。
【請求項３】
前記決定手段は、前記管理データに基づき、前記端末装置が有する前記１以上のメモリエリアに新たなアプリケーションを格納するための空き容量があるか否かを判定し、
前記送信手段は、前記決定手段が前記新たなアプリケーションを格納するための空き容量がないと判定した場合、前記端末装置に削除すべきアプリケーションの指定を促す指定要求を送信し、
前記受信手段は、前記指定要求に応じて前記端末装置から送信される削除すべきアプリケーションを指定する指定情報を受信し、
前記決定手段は、前記指定情報により指定されるアプリケーションが格納されているメモリエリアを、前記新たなアプリケーションを格納すべきメモリエリアとして決定し、
前記送信手段は、前記指定情報により指定されるアプリケーションの削除を指示する削除要求と、前記新たなアプリケーションと、当該新たなアプリケーションに関し前記決定手段により決定されたメモリエリアに当該新たなアプリケーションの格納を指示する格納要求とを送信する
請求項２に記載の中継装置。
【請求項４】
前記管理データは、前記端末装置における一のアプリケーションの利用に対する料金についての課金処理が既になされているか否かを示す購入情報を含み、
前記送信手段により、一のアプリケーションの削除を指示する削除要求が前記端末装置に送信された場合、前記更新手段は、前記端末装置における当該一のアプリケーションの利用に対する料金についての課金処理が既になされていることを示すように前記管理データを更新する
請求項２に記載の中継装置。
【請求項５】
前記管理データは、前記端末装置が有する１以上のメモリエリアの各々に格納されているアプリケーションが、利用可能な状態とされているか否かを示す活性化情報を含み、
前記送信手段は、前記管理データにより前記端末装置が有する前記１以上のメモリエリアのうちいずれかのメモリエリアに格納されており利用可能な状態とされていないことが示される一のアプリケーションを利用可能な状態とする処理を指示する活性化要求を、通信網を介し前記端末装置に送信し、
前記更新手段は、前記一のアプリケーションが利用可能な状態とされていることを示すように前記管理データを更新する
請求項１に記載の中継装置。
【請求項６】
前記管理データは、前記端末装置が有する１以上のメモリエリアの各々に格納されているアプリケーションが、利用可能な状態とされているか否かを示す活性化情報を含み、
前記送信手段は、前記管理データにより前記端末装置が有する前記１以上のメモリエリアのうちいずれかのメモリエリアに格納されており利用可能な状態とされていることが示される一のアプリケーションを利用可能でない状態とする処理を指示する不活性化要求を、通信網を介し前記端末装置に送信し、
前記更新手段は、前記一のアプリケーションが利用可能でない状態とされていることを示すように前記管理データを更新する
請求項１に記載の中継装置。
【請求項７】
前記記憶手段は、前記受信手段により受信されたアプリケーションの各々について当該アプリケーションの信頼性の程度を示す信頼度情報を記憶し、
前記送信手段は、一のアプリケーションを前記端末装置に送信する場合、当該一のアプリケーションについて前記記憶手段に記憶されている信頼度情報を前記端末装置に送信する

請求項１に記載の中継装置。
【請求項８】
各々１のアプリケーションを格納可能な１以上のメモリエリアと、
前記１以上のメモリエリアに格納されているアプリケーションの各々を実行する実行手段と、
中継装置から通信網を介しアプリケーションと、前記１以上のメモリエリアのうち一のメモリエリアへの当該アプリケーションの格納を指示する格納要求とを受信する受信手段と、
前記１以上のメモリエリアと前記実行手段との間の全てのデータの受け渡しを制御するメモリコントローラと
を備え、
前記メモリコントローラは、前記受信手段により受信された格納要求に従う場合にのみ前記受信手段により受信されたアプリケーションを前記１以上のメモリエリアのうちの一のメモリエリアへ格納する
端末装置。
【請求項９】
前記受信手段は、前記中継装置から通信網を介し前記１以上のメモリエリアのうちいずれかのメモリエリアに格納されている一のアプリケーションの削除を指示する削除要求を受信し、
前記メモリコントローラは、前記受信手段により受信された削除要求に従う場合にのみ前記１以上のメモリエリアのうちいずれかのメモリエリアに格納されている一のアプリケーションを削除する
請求項９に記載の端末装置。
【請求項１０】
前記受信手段は、前記中継装置から通信網を介し前記１以上のメモリエリアのうちいずれかのメモリエリアに格納されている一のアプリケーションを利用可能な状態とする処理を指示する活性化要求を受信し、
前記メモリコントローラは、前記受信手段により一のアプリケーションに関する活性化要求を受信した後に限り当該一のアプリケーションが格納されているメモリエリアと前記実行手段との間のデータの受け渡しを行う
請求項９に記載の端末装置。
【請求項１１】
前記受信手段は、前記中継装置から通信網を介し前記１以上のメモリエリアのうちいずれかのメモリエリアに格納されている一のアプリケーションを利用可能でない状態とする処理を指示する不活性化要求を受信し、
前記メモリコントローラは、前記受信手段により一のアプリケーションに関する不活性化要求を受信した後は当該一のアプリケーションが格納されているメモリエリアと前記実行手段との間のデータの受け渡しを行わない
請求項９に記載の端末装置。
【請求項１２】
前記受信手段は、前記中継装置から通信網を介し一のアプリケーションを受信する場合、当該一のアプリケーションの信頼性の程度を示す信頼度情報を受信し、
前記メモリコントローラは、前記実行手段から、前記１以上のメモリエリアのうちいずれかのメモリエリアに格納されている一のアプリケーションの実行により前記１以上のメモリエリアのうちいずれかのメモリエリアに格納されている他のアプリケーションもしくは当該他のアプリケーションに関するデータの利用要求を受け取った場合、当該一のアプリケーションの信頼度情報および当該他のアプリケーションの信頼度情報に基づき、前記利用要求に従い前記他のアプリケーションを格納しているメモリエリアと前記実行手段との間のデータの受け渡しを行うか否かを決定する
請求項９に記載の端末装置。

【発明の詳細な説明】
【０００１】
移動体端末の記憶部に格納されたプログラムを管理するシステム
【０００２】
［技術分野］
本発明は、移動体端末に内蔵あるいは装着された記憶部に格納されたプログラム（アプレットを含む）の管理システムに関する。
【０００３】
［背景技術］
近年、比較的記憶容量の大きい不揮発性メモリを内蔵し、その不揮発性メモリに出荷時には組み込まれていないアプリケーションプログラムを購入後に書き込み、そのアプリケーションプログラムを実行することのできる移動体端末が開発されている。そのような移動体端末のユーザは、不要になったアプリケーションプログラムを不揮発性メモリから消去し、新たに別のアプリケーションプログラムを不揮発性メモリに書き込むことにより、移動体端末を買い換えることなく、新しいアプリケーションプログラムを利用することができる。
【０００４】
このようなアプリケーションプログラムの書き込み可能な移動体端末として、例えばＪａｖａバーチャルマシンを搭載したものがある。Ｊａｖａバーチャルマシンを搭載した移動体端末は、Ｊａｖａアプリケーション（Ｊａｖａアプレットを含む）を移動通信網経由でダウンロードし、不揮発性メモリに書き込んだ後、ダウンロードしたＪａｖａアプリケーションを実行することができる。（以下、アプレットを含むアプリケーションプログラムを「アプリケーション」と呼ぶ。）
【０００５】
上記のような移動体端末において、移動体端末が実行するアプリケーションの管理を移動体端末が独自に行うと不便な場合があった。
【０００６】
その一例は、移動体端末にダウンロードされるアプリケーションの利用代金に関するものである。
例えば、移動体端末に過去にダウンロードされたアプリケーションが移動体端末のメモリ不足等の理由により削除された後、再度、移動体端末にダウンロードされる場合がある。この場合に、ダウンロードされるアプリケーションの利用代金が二重に課金されると不都合な場合がある。
また、例えば、移動体端末にダウンロードされたアプリケーションが所定期間のみ利用可能となれば便利な場合がある。この場合に、アプリケーションが利用できない期間に関して課金されると不都合な場合がある。
【０００７】
移動体端末が実行するアプリケーションの管理を移動体端末が独自に行うと不都合が生じる他の一例は、互いに機能が関連する複数のアプリケーションの利用に関するものである。
例えば、高い価値を有する情報を扱う第１のアプリケーションと連係する第２のアプリケーションがある場合、たとえ第１のアプリケーションの信頼性が高くても、第２のアプリケーションの信頼性が低いと、第２のアプリケーションに従った処理により高い価値を有する情報がユーザの意図しない利用のされ方をする危険性がある。
【０００８】
［発明の開示］
上述した従来技術による移動体端末の不便な点を克服するために、本発明は、端末装置が有する１以上のメモリエリアの各々に格納されているアプリケーションの識別情報を含む管理データを記憶する記憶手段と、サーバ装置から通信網を介しアプリケーションを受信する受信手段と、前記管理データに基づき前記端末装置が有する前記１以上のメモリエ

リアのうちアプリケーションを格納すべきメモリエリアを決定する決定手段と、前記受信手段により取得されたアプリケーションと、当該アプリケーションに関し前記決定手段により決定されたメモリエリアに当該アプリケーションの格納を指示する格納要求とを、通信網を介し前記端末装置に送信する送信手段と、前記送信手段により送信されたアプリケーションが前記送信手段により送信された格納要求により指示されるメモリエリアに格納されていることを示すように前記管理データを更新する更新手段とを備える中継装置を提供する。

【０００９】

また、本発明は、各々１のアプリケーションを格納可能な１以上のメモリエリアと、前記１以上のメモリエリアに格納されているアプリケーションの各々を実行する実行手段と、中継装置から通信網を介しアプリケーションと、前記１以上のメモリエリアのうち一のメモリエリアへの当該アプリケーションの格納を指示する格納要求とを受信する受信手段と、前記１以上のメモリエリアと前記実行手段との間の全てのデータの受け渡しを制御するメモリコントローラとを備え、前記メモリコントローラは、前記受信手段により受信された格納要求に従う場合にのみ前記受信手段により受信されたアプリケーションを前記１以上のメモリエリアのうちの一のメモリエリアへ格納する端末装置を提供する。

【００１０】

［図面の簡単な説明］

図１は、本発明の第１実施形態および第２実施形態に係るアプリケーション配信システムの全体構成を示すブロック図である。

図２は、本発明の第１実施形態および第２実施形態に係る移動体端末の外観図である。

図３は、本発明の第１実施形態および第２実施形態に係る移動体端末の概要構成ブロック図である。

図４は、本発明の第１実施形態および第２実施形態に係る移動体端末のメモリの構成図である。

図５は、本発明の第１実施形態および第２実施形態に係る管理サーバの概要構成を示すブロック図である。

図６は、本発明の第１実施形態および第２実施形態に係るアプリケーションの情報管理システムの構成を示す図である。

図７は、本発明の第１実施形態および第２実施形態に係る、ユーザ情報格納部に格納されるデータ例を示す図である。

図８は、本発明の第１実施形態に係る、アプリケーション情報格納部の登録アプリケーション領域に格納されるデータ例を示す図である。

図９は、本発明の第１実施形態および第２実施形態に係る、アプリケーション情報格納部の一時保管アプリケーション領域に格納されるデータ例を示す図である。

図１０および図１１は、本発明の第１実施形態および第２実施形態に係る管理サーバにおけるアプリケーションの格納処理のフローを示す図である。

図１２および図１３は、本発明の第１実施形態および第２実施形態に係る、管理サーバに公開されているアプリケーションの購入の際に移動体端末に表示される画面を示す図である。

図１４および図１５は、本発明の第１実施形態および第２実施形態に係る、管理サーバに公開されているアプリケーションの購入処理のフローを示す図である。

図１６および図１７は、本発明の第１実施形態および第２実施形態に係る、信頼度を付されているが管理サーバに公開されていないアプリケーションの購入処理のフローを示す図である。

図１８、図１９、および図２０は、本発明の第１実施形態および第２実施形態に係る、信頼度を与えられていないアプリケーションの購入処理のフローを示す図である。

図２１および図２２は、本発明の第１実施形態および第２実施形態に係る、アプリケーションのダウンロードの際に移動体端末に表示される画面を示す図である。

図２３、図２４、および図２５は、本発明の第１実施形態および第２実施形態に係る、

アプリケーションのダウンロード処理のフローを示す図である。
図２６は、本発明の第１実施形態および第２実施形態に係る、アプリケーションの起動操作の際に移動体端末に表示される画面を示す図である。
図２７、図２８、図２９、図３０、および図３１は、本発明の第１実施形態に係る、複数のアプリケーションが連係できない場合に移動体端末に表示される画面を示す図である。
図３２、図３３、および図３４は、本発明の第１実施形態に係る、複数のアプリケーションが連係して動作する場合に移動体端末に表示される画面を示す図である。
図３５は、本発明の第２実施形態に係る、アプリケーション間の権限情報を例示した図である。
図３６は、本発明の第２実施形態に係る、アプリケーション情報格納部の登録アプリケーション領域に格納されるデータ例を示す図である。
図３７は、本発明の第３実施形態に係る、アプリケーション情報格納部の登録アプリケーション領域に格納されるデータ例を示す図である。
図３８は、本発明の第３実施形態に係るアプリケーションの情報管理システムの構成を示す図である。
図３９は、本発明の第３実施形態に係る、ユーザ情報格納部に格納されるデータ例を示す図である。
図４０、図４１、および図４２は、本発明の第３実施形態に係る、アプリケーションの購入処理およびダウンロード処理のフローを示す図である。
【００１１】
［発明を実施するための最良の形態］
次に本発明の望ましい実施形態について説明する。
［１］第１実施形態
［１．１］構成
［１．１．１］アプリケーション配信システムの全体構成
図１は本発明の実施形態に係るアプリケーション配信システムの全体構成の概要を示すブロック図である。
【００１２】
アプリケーション配信システムは、複数の移動体端末１１－１、１１－２、・・・と、複数の基地局１３－１、１３－２、・・・と、複数の交換局１４と、移動体通信網１５と、管理サーバ１６と、認証サーバ１７と、ゲートウェイサーバ１８と、インターネット１９と、複数のコンテンツサーバ２０－１、２０－２、・・・とにより構成されている。なお、以下では、特に区別する必要がない場合に、各移動体端末を移動体端末１１と、各基地局を基地局１３と、また各コンテンツサーバをコンテンツサーバ２０と総称する。
【００１３】
移動体端末１１は、例えば携帯電話、ＰＨＳ（Ｐｅｒｓｏｎａｌ　Ｈａｎｄｙｐｈｏｎｅ　Ｓｙｓｔｅｍ；登録商標）等の無線通信機能を有する情報処理装置である。移動体端末１１は、アプリケーションを記憶可能な不揮発性メモリを内蔵しているか、もしくはアプリケーションを記憶可能な外部の不揮発性メモリを装着することができる。移動体端末１１は、管理サーバ１６より移動体通信網１５、交換局１４、および基地局１３を介してアプリケーションをダウンロードし、ダウンロードしたアプリケーションを不揮発性メモリに書き込む。移動体端末１１のユーザは、望む時に不揮発性メモリに書き込まれたアプリケーションを実行することができる。
【００１４】
基地局１３は有線により交換局１４を介して移動体通信網１５に接続されている。基地局１３は、割り当てられた無線ゾーン内に存在する移動体端末１１のいずれかが移動体通信網１５に対して発呼する場合、もしくは割り当てられた無線ゾーン内に存在する移動体端末１１のいずれかに対して移動体通信網１５から発呼がされた場合、該当する移動体端末１１との間で無線接続を確立し、移動体端末１１と移動体通信網１５との間の通信を中

継する。なお、基地局１３は割り当てられた無線ゾーン内の移動体端末１１との間で頻繁に無線による制御信号をやりとりを行うことにより、割り当てられた無線ゾーン内にどの移動体端末１１が存在するかを把握し、その情報を移動体端末１１の位置情報として移動体通信網１５に送信する。

【００１５】

交換局１４は、基地局１３および移動体通信網１５とそれぞれ有線により接続されており、基地局１３と無線接続を確立した移動体端末１１と、移動体通信網１５との間に利用可能な通信経路を確立する装置である。なお、移動体通信網１５との間に通信状態を確立した移動体端末１１が、ある交換局１４の管理する無線ゾーンから他の交換局１４の管理する無線ゾーンに移動した場合には、交換局１４は、確立されている通信状態を維持しつつ、交換局間の通信接続切替制御を行う。

【００１６】

移動体通信網１５は、交換局１４を関門交換局（図示略）を介して有線により相互に接続した通信網である。移動体通信網１５は、交換局１４および基地局１３を介して複数の移動体端末１１間の通信経路を確立する。また、移動体通信網１５は固定電話網等の他の通信網（図示略）と接続されている。さらに、移動体通信網１５はゲートウェイサーバ１８を介してインターネット１９に接続されている。なお、移動体通信網１５内には位置登録メモリ（図示略）が設けられており、この位置登録メモリには各基地局１３から得られる移動体端末１１の位置情報が記録される。移動体通信網１５は、特定の移動体端末１１に対する発呼を行う場合には、位置登録メモリに記録された情報を用いて、該当する移動体端末１１と無線接続の可能な基地局１３に対し接続要求を行う。

【００１７】

管理サーバ１６は、移動体端末１１の要求に応じて、アプリケーションを移動体端末１１に配信するサーバである。管理サーバ１６は、アプリケーションの移動体端末１１への配信に先立ち、アプリケーションの配信元であるコンテンツサーバ２０からアプリケーションの送信を受け、送信されたアプリケーションをデータベースに格納する。

【００１８】

管理サーバ１６の管理事業者は、コンテンツサーバ２０の管理事業者の希望があれば、コンテンツサーバ２０が管理しているアプリケーションの内容を審査し、そのアプリケーションに対し、移動体端末１１における動作の安全性等の観点から信頼度を決定する。決定された信頼度は、管理サーバ１６のデータベースに記録される。管理サーバ１６は、信頼度の与えられたアプリケーションの配信要求を移動体端末１１から受けると、移動体端末１１に対し、アプリケーションと共にその信頼度を送信する。

【００１９】

移動体端末１１がアプリケーションを利用するには、アプリケーションの購入、アプリケーションの移動体端末１１に対するダウンロード、およびダウンロードされたアプリケーションを利用可能な状態にする処理（以下、「アクティベーション処理」と呼ぶ）が必要である。管理サーバ１６は、移動体端末１１のユーザによってアプリケーションの購入が要求されると、要求されたアプリケーションの配信準備を行う。また、管理サーバ１６は、移動体端末１１にアプリケーションがダウンロードされる際、移動体端末１１のメモリにおけるアプリケーションの書き込み領域を決定し、移動体端末１１に対しアプリケーションの書き込みを許可する。さらに、管理サーバ１６は、移動体端末１１に対し、移動体端末１１におけるアプリケーションのアクティベーション処理の指示を行う。管理サーバ１６はアプリケーションの配信準備およびアクティベーション処理を行うと、それらの処理に関する情報を、移動体通信網１５に接続された課金管理サーバ（図示略）に送信する。課金管理サーバは管理サーバ１６より配信準備およびアクティベーション処理に関する情報を受信すると、それらの情報を用いて、処理の対象の移動体端末１１に対する、アプリケーションの利用料金算出を行う。

【００２０】

認証サーバ１７は、各移動体端末１１、管理サーバ１６、各コンテンツサーバ２０、お

よび認証サーバ１７自身の公開鍵方式における公開鍵を管理するサーバである。認証サーバ１７は、任意の移動体端末１１、管理サーバ１６、および任意のコンテンツサーバ２０からの要求に応じて、送信要求のされた公開鍵を送信要求を行った装置に送信する。

コンテンツサーバ２０は、移動体端末１１の仕様に応じて開発されたアプリケーションを１または複数管理しており、管理サーバ１６からの要求に応じて、該当するアプリケーションを管理サーバ１６に送信する。なお、コンテンツサーバ２０の管理事業者は、希望すればアプリケーションを管理サーバ１６の管理事業者に送信し、その内容の審査を依頼し、審査結果に応じて管理サーバ１６の管理事業者からアプリケーションに対応する信頼度を取得することができる。

【００２１】

［１．１．２］移動体端末の構成

次に移動体端末１１の構成について説明する。なお、ここでは移動体端末１１－１を例に説明する。

【００２２】

図２は移動体端末１１－１の外観図である。また、図３は移動体端末１１－１の概要構成を示したブロック図である。図３に示すように、移動体端末１１－１は、ディスプレイ部２１、操作部２２、アンテナ３４Ａ、制御部３１、制御用メモリ３２、通信部３４、メモリコントローラ３５、メモリ１２および音声入出力部３６を備えている。

【００２３】

ディスプレイ部２１は、移動体端末１１－１のユーザに移動体端末１１－１の制御部がメッセージを表示するための構成部である。ディスプレイ部２１には、図２に示されているアプリケーション実行のための処理メニューの他、種々の処理メニュー、情報サイトから得られる情報を表示するブラウザ画面、電波強度や電話番号等の各種情報が表示される。

【００２４】

操作部２２は、制御部３１に対し、指示を与える構成部である。操作部２２には、数字等の示された操作ボタンおよびアプリボタン２３が設けられている。アプリボタン２３はアプリケーションの操作を簡便に行うための機能が割り当てられた操作ボタンである。

【００２５】

アンテナ３４Ａは、移動体端末１１－１が無線通信を行う際、電波を物理的に出力および入力する構成部である。

【００２６】

制御部３１は、移動体端末１１－１において、メモリ１２を除く各構成部の制御を行うマイクロプロセッサである。制御部３１は、制御用メモリ３２に記憶されている制御用プログラムに従って各構成部の制御を行う。また、制御部３１は、メモリコントローラ３５を介してメモリ１２からアプリケーションを読み出し、読み出したアプリケーションを実行する。制御部３１は、実行中の制御用プログラムおよびアプリケーションからの要求により、メモリ１２に書き込まれているアプリケーションもしくはデータを利用することがある。その場合、制御部３１はメモリコントローラ３５にアプリケーションもしくはデータの利用要求とこの利用要求の発信元である制御用プログラムもしくはアプリケーションの識別情報を送信する。この識別情報は、メモリコントローラ３５が利用要求に応じるか否かを判定する際に利用される。制御部３１は制御用プログラムもしくはアプリケーションを複数同時に実行することがあるが、制御用プログラムとアプリケーションの間、もしくは複数のアプリケーションの間でデータの受け渡しを直接行うことはなく、必ずメモリコントローラ３５を介してデータの受け渡しを行う。

【００２７】

制御用メモリ３２は制御部３１の制御用プログラムおよび制御用プログラムが管理するデータを記録するための揮発性メモリおよび不揮発性メモリである。また、制御用メモリ３２は、制御部３１が制御用プログラムを実行する際の作業領域としても利用される。なお、制御用プログラムには、移動体端末１１－１が出荷時に有している電話番号記録機能

等の基本機能を実現するプログラムも含まれている。

【００２８】

通信部３４は、アンテナ３４Ａを介して基地局１３との間で電波による信号の送受信を行う構成部である。通信部３４は、移動体端末１１－１が基地局１３に送信したい情報を持つ場合、制御部３１の制御のもとで、ベースバンド信号を送信したいデジタルデータを示す信号により変調した後、アンテナ３４Ａに印加することにより、電波信号を基地局１３に送信する。また、通信部３４はアンテナ３４Ａを介して基地局１３より電波を受信すると、受信した電波からアプリケーションまたはデータを復調し、アプリケーションについてはメモリコントローラ３５に、復調されたデータのうちデジタル音声データについては音声入出力部３６に、制御データ等のその他のデータは制御部３１に、それぞれ送信する。

【００２９】

音声入出力部３６は移動体端末１１－１のユーザが他の移動体端末１１や固定電話等のユーザとの間で会話をする際、音声の入出力処理を行う。音声入出力部３６はマイク（図示略）、Ａ／Ｄコンバータ（図示略）、Ｄ／Ａコンバータ（図示略）、スピーカ（図示略）等を有している。移動体端末１１－１のユーザが話す場合、音声入出力部３６はマイクから移動体端末１１－１のユーザの声をアナログ信号として取り込み、取り込んだアナログ信号をＡ／Ｄコンバータによりデジタル信号に変換後、通信部３４に送信する。一方、移動体端末１１－１のユーザの会話の相手が話す場合、通信部３４から送信されるデジタル音声データをＤ／Ａコンバータによりアナログ信号に変換し、スピーカから発音する。

【００３０】

メモリコントローラ３５はメモリ１２と制御部３１および通信部３４との間のデータの送受信を制御するためのマイクロプロセッサである。メモリコントローラ３５は、通信部３４からアプリケーションが送信されると、アプリケーションをメモリ１２に書き込む。通信部３４から送信されるアプリケーションには、管理サーバ１６からの書き込み要求と共に、メモリ１２においてアプリケーションを書き込むべきメモリエリアが指定されており、メモリコントローラ３５は指定されたメモリエリアにアプリケーションを書き込む。また、メモリコントローラ３５が通信部３４から受信するアプリケーションが、ある程度以上の信頼度が与えられているアプリケーションである場合、メモリコントローラ３５はアプリケーションと共にその信頼度も受信する。その場合、メモリコントローラ３５はアプリケーションを書き込むメモリエリアに、受信した信頼度も書き込む。

【００３１】

メモリコントローラ３５は、制御部３１からメモリ１２に書き込まれているアプリケーションもしくはデータの利用要求、すなわち読み取り要求、書き込み要求、もしくは削除要求を受信すると、その利用要求を承諾するべきかどうかを判定し、その判定の結果に基づいてメモリ１２に対する処理を行う。制御部３１のメモリ１２に書き込まれているアプリケーションもしくはデータの利用要求は、利用要求を行っているプログラムの識別情報を伴っている。メモリコントローラ３５は利用要求を受信すると、まずその利用要求を行っているプログラムの信頼度を確認する。利用要求を行っているプログラムが制御部３１の管理する制御用プログラムである場合、制御用プログラムには最も高い信頼度が与えられているため、メモリコントローラ３５は無条件に利用要求を承諾し、利用要求に従ったメモリ１２に対する処理を行う。利用要求を行っているプログラムがメモリ１２から読み出されたアプリケーションである場合、メモリコントローラ３５は識別情報から、利用要求を行っているアプリケーションの書き込まれているメモリエリアを特定し、そのアプリケーションに与えられている信頼度を読み出す。なお、アプリケーションの信頼度が不明である場合、メモリコントローラ３５は、そのアプリケーションを信頼度が最も低いものとして扱う。続いて、メモリコントローラ３５は、利用要求の対象となっているアプリケーションもしくはデータの書き込まれているメモリエリアから同様に信頼度を読み出す。メモリコントローラ３５はこうして得られる２つの信頼度を比較し、利用要求を行っているアプリケーションの信頼度が、利用要求の対象となっているアプリケーション、もしく

は利用要求の対象となっているデータを管理しているアプリケーションの信頼度より高いか、もしくは同等の場合に限り、利用要求を承諾し、利用要求に従ったメモリ１２に対する処理を行う。この信頼度を用いた制御処理については、具体例を挙げて後述する。

【００３２】

また、メモリコントローラ３５は、移動体端末１１－１の秘密鍵および公開鍵の生成、および秘密鍵を用いたデータの暗号化および復号化を行う。メモリコントローラ３５は、制御部３１の制御のもとで、移動体端末１１のユーザの入力するキーワードに基づいて秘密鍵および公開鍵の対を作成する。メモリコントローラ３５は生成した公開鍵を通信部３４を介して認証サーバ１７に送信し、一方、秘密鍵については容易に移動体端末１１－１に漏洩しないようプロテクト処理を施した後、記録する。メモリコントローラ３５は、通信部３４を介して外部より移動体端末１１－１の公開鍵で暗号化されたデータを受信すると、移動体端末１１－１の秘密鍵を用いて暗号化されたデータを復号する。また、メモリコントローラ３５は、メモリ１２のデータを通信部３４を介して外部に送信する際、必要に応じて送信するデータを移動体端末１１－１の秘密鍵で暗号化する。

【００３３】

メモリ１２は、通信部３４を介して外部より受信されるアプリケーションおよびそれらのアプリケーションが管理するデータを記憶するための不揮発性メモリである。図４はメモリ１２の構成を示した図である。

【００３４】

メモリ１２は複数のメモリエリアに区画されている。これらのメモリエリアには管理エリア４０とフリーエリア４１がある。管理エリア４０は管理サーバ１６によりある程度以上の信頼度を与えられているアプリケーション用の領域であり、フリーエリア４１は管理サーバ１６によりある程度以上の信頼度を与えられていないアプリケーション用の領域である。管理エリア４０は複数の管理エリア４０－１～管理エリア４０－ｎ（ｎは任意の正の整数）からなり、またフリーエリア４１は複数のフリーエリア４１－１～フリーエリア４１－ｍ（ｍは任意の正の整数）からなる。以下、管理エリア４０－１およびフリーエリア４１－１を例として説明する。

【００３５】

管理エリア４０－１は、アプリケーション領域４０Ａ－１、データ領域４０Ｄ－１、および信頼情報領域４０Ｒ－１に区画されている。アプリケーション領域４０Ａ－１にはアプリケーション本体が格納される。データ領域４０Ｄ－１には、アプリケーション領域４０Ａ－１に格納されるアプリケーションが管理するデータが格納される。信頼情報領域４０Ｒ－１には、アプリケーション領域４０Ａ－１に格納されるアプリケーションに与えられている信頼度が格納される。

【００３６】

フリーエリア４１－１は、アプリケーション領域４１Ａ－１およびデータ領域４１Ｄ－１に分かれている。アプリケーション領域４１Ａ－１にはアプリケーション本体が格納される。データ領域４１Ｄ－１には、アプリケーション領域４１Ａ－１に格納されるアプリケーションが管理するデータが格納される。

【００３７】

アプリケーション領域４０Ａ－１およびアプリケーション領域４１Ａ－１におけるアプリケーションの書き込みおよび削除、および信頼情報領域４０Ｒ－１における信頼度の書き込みおよび削除は、メモリコントローラ３５が管理サーバ１６からの指示のみに従って行う。一方、アプリケーション領域４０Ａ－１およびアプリケーション領域４１Ａ－１におけるアプリケーションの読み出し、信頼情報領域４０Ｒ－１における信頼度の読み出し、データ領域４０Ｄ－１およびデータ領域４１Ｄ－１のデータの書き込み、読み出し、および削除は、メモリコントローラ３５の管理のもとで、制御部３１の要求により行われる。

【００３８】

［１．１．３］管理サーバの構成

図５は管理サーバ１６の概要構成を示したブロック図である。管理サーバ１６は、暗号鍵格納部５１、アプリケーション情報格納部５２、ユーザ情報格納部５３、および制御部５４を備えている。

【００３９】

暗号鍵格納部５１は、制御部５４により生成される管理サーバ１６の秘密鍵、認証サーバ１７から取得される各移動体端末１１および各コンテンツサーバ２０の公開鍵を格納するデータベースである。

【００４０】

アプリケーション情報格納部５２は、各コンテンツサーバ２０から送信されるアプリケーション本体もしくはアプリケーションの保管場所情報をアプリケーションの名称等の情報と共に格納しているデータベースである。

【００４１】

ユーザ情報格納部５３は、各移動体端末１１のメモリ１２に書き込まれているアプリケーションに関する情報、および移動体端末１１のユーザにより購入され、移動体端末１１のユーザが望む時に移動体端末１１にダウンロードし、メモリ１２に書き込み可能なアプリケーションに関する情報を格納しているデータベースである。

【００４２】

制御部５４は、管理サーバ１６の各構成部の制御を行うマイクロプロセッサである。制御部５４は認証サーバ１７からの公開鍵の取得、コンテンツサーバ２０からのアプリケーションの取得と暗号化されているアプリケーションの復号化、および移動体端末１１へ配信するアプリケーションの暗号化および配信の制御を行う。また、それらの処理に伴う暗号鍵格納部５１、アプリケーション情報格納部５２、およびユーザ情報格納部５３の各データベースのデータ更新を行う。

【００４３】

管理サーバ１６の各データベースの構成およびアプリケーションの配信動作の詳細については後述する。

【００４４】

［１．１．４］アプリケーションの情報管理システムの構成

図６は移動体端末１１、管理サーバ１６、およびコンテンツサーバ２０におけるアプリケーションに関する情報管理のシステムを示す図である。

【００４５】

ユーザ情報格納部５３は、移動体端末１１－１、移動体端末１１－２、・・・、移動体端末１１－ｋ（ｋは移動体端末１１の数を表す整数）に対応するデータ格納領域として、ユーザ情報格納部５３－１、ユーザ情報格納部５３－２、・・・、ユーザ情報格納部５３－ｋを持っている。各ユーザ情報格納部５３－ｉ（ｉ＝１～ｋ）は、既配信アプリケーション領域５３Ａ－ｉと配信可能アプリケーション領域５３Ｂ－ｉに区画されている。あるユーザ情報格納部５３－ｉの既配信アプリケーション領域５３Ａ－ｉは、移動体端末１１－ｉのメモリ１２の管理エリア４０またはフリーエリア４１に現在書き込まれているアプリケーションの情報を格納する領域である。一方、ユーザ情報格納部５３－ｉの配信可能アプリケーション領域５３Ｂ－ｉは、現在は移動体端末１１－ｉのメモリ１２に書き込まれていないが、移動体端末１１－ｉのユーザにより購入済みであり、移動体端末１１の要求により、いつでも移動体端末１１への配信が可能なアプリケーションの情報を格納する領域である。既配信アプリケーション領域５３Ａおよび配信可能アプリケーション領域５３Ｂには、アプリケーションの名称、バージョン番号、各アプリケーションを識別する識別番号、アプリケーションのサイズ、アクティベーション処理の完了／未完了の別、アプリケーションの保管番号等の情報が格納されている。図７は移動体端末１１－１に対応したユーザ情報格納部５３－ｉに格納されているデータを例示したもので、簡略化のため、対応するメモリエリア、アプリケーションの識別番号、アクティベーション、および保管番号に関する項目のみを示している。

【００４６】

図７に示す例では、移動体端末１１－１の管理エリア４０－１におけるアプリケーション領域４０Ａ－１には、現在、識別番号が「ＡＰ－３５６８」であるアプリケーションが書き込まれており、アクティベーション処理がされている。保管番号は、配信準備のなされているアプリケーションの、アプリケーション情報格納部５２における一時的保管場所を特定するための情報である。従って、既に移動体端末１１－１に配信されているアプリケーションに関しては、保管番号は不要であるため、既配信アプリケーション領域５３Ａにおけるアプリケーションに関しては、保管番号は与えられない。

【００４７】

また、図７に示す例において、移動体端末１１－１のフリーエリア４１－１におけるアプリケーション領域４１Ａ－１には、現在、識別番号が「Ｆ－０３２５」であるアプリケーションが書き込まれており、アクティベーション処理がされている。

【００４８】

さらに、図７に示す例において、移動体端末１１－１のユーザは、現在、メモリ１２に書き込んではいないが、既に購入しており、いつでもダウンロード可能なアプリケーションとして、４つのアプリケーションを持っている。例えば、それらのアプリケーションの１つである識別番号が「ＡＰ－４１２５」であるアプリケーションはその本体が、現在、アプリケーション情報格納部５２において保管番号「Ｔ－７８５１」で識別される領域に格納されている。それに対し、識別番号が「ＡＰ－３０２１」であるアプリケーションは、保管番号に「削除済み」との記録があることから、アプリケーション情報格納部５２には現在、アプリケーション本体が格納されていない。さらに、識別番号が「ＡＰ－４５１３」であるアプリケーションは、保管番号にデータが与えられていないことから、このアプリケーションは管理サーバ１６の登録アプリケーション領域５２Ｒに格納されているアプリケーションであり、そもそも保管番号を持つ必要がないものである。なお、配信可能アプリケーション領域５３Ｂに情報の格納されているアプリケーションは、現在移動体端末１１－１のメモリ１２に書き込まれていないことから、当然ながらアクティベーション処理は行われておらず、従ってアクティベーションに関する項目にはデータが与えられていない。

【００４９】

アプリケーション情報格納部５２は、図６に示すように、登録アプリケーション領域５２Ｒおよび一時保管アプリケーション領域５２Ｔから構成されている。登録アプリケーション領域５２Ｒには、移動体端末１１用に開発された様々なアプリケーションに関して、アプリケーションの名称、バージョン番号、各アプリケーションの識別番号、アプリケーションのサイズ、利用料金、アプリケーションの機能概要等の情報がアプリケーション本体もしくはアプリケーションの保管場所情報と共に格納されている。また、ある程度以上の信頼度が与えられているアプリケーションに関しては、信頼度、アプリケーションの公開／非公開の別、料金徴収の管理サーバ１６の管理事業者による代行／非代行の別等の情報も格納されている。なお、ある程度以上の信頼度の与えられていないアプリケーションに関しては、登録アプリケーション領域５２Ｒの信頼度の項目には、信頼度として「０」が格納されている。図８は登録アプリケーション領域５２Ｒに格納されるデータを例示したもので、簡略化のため、アプリケーションの識別番号、信頼度、公開、料金徴収、および保管場所に関する項目のみが示されている。アプリケーションの保管場所情報としては、目的のアプリケーションを含むファイルの所在を特定可能な情報であれば何でもよいが、例えばインターネットにおいて広く利用されているＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）が利用可能である。

【００５０】

図８に例示した登録アプリケーション領域５２Ｒの情報によれば、例えば識別番号が「ＡＰ－３５６８」のアプリケーションの信頼度は「３」、アプリケーションは管理サーバ１６において公開し、料金徴収は管理サーバ１６の管理事業者が代行し、そのアプリケーション本体は登録アプリケーション領域５２Ｒ内に格納されていることが分かる。一方、識別番号が「ＡＰ－３７１２」のアプリケーションの信頼度は「５」、アプリケーション

は公開し、料金徴収は管理サーバ１６の管理事業者が代行せず、そのアプリケーションはアプリケーション情報格納部５２内には格納されておらず、ｆｔｐ：／／ｆｔｐ．ａｂｃ＿ｓｏｆｔｗａｒｅ．ｃｏｍ／ａｐｐｌｉｃａｔｉｏｎという場所に、ａｐ＿０３０６．ｅｘｅというファイル名で保管されていることが分かる。また、識別番号が「Ｆ－３２５１」であるアプリケーションは、信頼度が与えられていないアプリケーションであり、従って公開および料金徴収に関する項目にはデータが与えられていない。なお、アプリケーションの公開／非公開、料金徴収の代行／非代行、およびアプリケーションの保管場所の違いについては後述する。

【００５１】

一時保管アプリケーション領域５２Ｔには、登録アプリケーション領域５２Ｒにおいてアプリケーションの保管場所情報が登録されているアプリケーションに関し、移動体端末１１より配信の要求があった際、それらのアプリケーションの配信元であるコンテンツサーバ２０からアプリケーション本体を受信した後、移動体端末１１に配信が行われるまでの間、それらのアプリケーション本体が一時的に格納されている。図９は一時保管アプリケーション領域５２Ｔに格納されるデータ構造を例示したもので、アプリケーション本体は一時保管アプリケーション領域５２Ｔにおいてそれらを特定するための保管番号と関連づけて格納されている。

【００５２】

［１．２］配信処理の概要

続いて、アプリケーションの配信処理の流れを説明する。

［１．２．１］アプリケーション購入前の処理

［１．２．１．１］暗号鍵の発行

本発明の実施形態に係るアプリケーション配信システムにおいては、移動体通信網１５の管理事業者、管理サーバ１６の管理事業者、およびコンテンツサーバ２０の管理事業者のいずれからも独立した事業者により管理される認証サーバ１７により、公開鍵方式による公開鍵の管理が行われる。

【００５３】

まず、認証サーバ１７は、認証サーバ１７自身の秘密鍵「ＳＫ－ＡＳ」（Ｓｅｃｒｅｔ Ｋｅｙ ｆｏｒ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｓｅｒｖｅｒ）および公開鍵「ＰＫ－ＡＳ」（Ｐｕｂｌｉｃ Ｋｅｙ ｆｏｒ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｓｅｒｖｅｒ）の対を生成し、秘密鍵「ＳＫ－ＡＳ」については外部に漏洩することのないよう保管し、公開鍵「ＰＫ－ＡＳ」に関しては任意の外部の装置からの要求に応じて送信を行う。

【００５４】

各移動体端末１１においては、ユーザの操作に応じて秘密鍵「ＳＫ－ＭＴ」（Ｓｅｃｒｅｔ Ｋｅｙ ｆｏｒ Ｍｏｂｉｌｅ Ｔｅｒｍｉｎａｌ）および公開鍵「ＰＫ－ＭＴ」（Ｐｅｃｒｅｔ Ｋｅｙ ｆｏｒ Ｍｏｂｉｌｅ Ｔｅｒｍｉｎａｌ）の対が作成される。秘密鍵「ＳＫ－ＭＴ」については各移動体端末１１のメモリコントローラ３５により外部に漏洩がないよう管理されている。一方、各移動体端末１１は、作成した公開鍵「ＰＫ－ＭＴ」を移動体通信網１５を介して認証サーバ１７に送信する。認証サーバ１７は、移動体端末１１から公開鍵「ＰＫ－ＭＴ」を受信すると、受信した公開鍵「ＰＫ－ＭＴ」を各移動体端末１１の識別番号と関連づけてデータベースに格納する。この公開鍵「ＰＫ－ＭＴ」は、認証サーバ１７の公開鍵「ＰＫ－ＡＳ」と同様に、任意の装置からの要求に応じて、認証サーバ１７により送信される。

【００５５】

個々の移動体端末１１の秘密鍵および公開鍵を区別する場合には、上記の呼称に移動体端末１１の添字番号を付ける。例えば、移動体端末１１－１の秘密鍵は「ＳＫ－ＭＴ－１」と呼ぶ。

【００５６】

管理サーバ１６および各コンテンツサーバ２０は、各移動体端末１１と同様に、秘密鍵および公開鍵の対を作成し、秘密鍵については外部に漏洩することのないよう保管する一

方、公開鍵に関しては認証サーバ１７に送信する。認証サーバ１７は、管理サーバ１６から公開鍵を受信すると、受信した公開鍵を管理サーバ１６の識別番号と関連づけてデータベースに格納する。コンテンツサーバ２０から公開鍵が受信された場合も同様である。管理サーバ１６やコンテンツサーバ２０の公開鍵は、認証サーバ１７および移動体端末１１の公開鍵と同様に、任意の装置からの要求に応じて、認証サーバ１７により送信される。この明細書では管理サーバ１６およびコンテンツサーバ２０用の秘密鍵および公開鍵を以下のように呼ぶこととする。

管理サーバ１６の秘密鍵：「ＳＫ－ＭＳ」（Ｓｅｃｒｅｔ Ｋｅｙ ｆｏｒ Ｍａｎａｇｅｍｅｎｔ Ｓｅｒｖｅｒ）

管理サーバ１６の公開鍵：「ＰＫ－ＭＳ」（Ｐｕｂｌｉｃ Ｋｅｙ ｆｏｒ Ｍａｎａｇｅｍｅｎｔ Ｓｅｒｖｅｒ）

コンテンツサーバ２０の秘密鍵：「ＳＫ－ＣＳ」（Ｓｅｃｒｅｔ Ｋｅｙ ｆｏｒ Ｃｏｎｔｅｎｔｓ Ｓｅｒｖｅｒ）

コンテンツサーバ２０の公開鍵：「ＰＫ－ＣＳ」（Ｐｕｂｌｉｃ Ｋｅｙ ｆｏｒ Ｃｏｎｔｅｎｔｓ ｓｅｒｖｅｒ）

【００５７】

また、個々のコンテンツサーバ２０用の秘密鍵および公開鍵を区別する場合には、移動体端末１１の場合と同様に、上記の呼称にコンテンツサーバ２０の添字番号を付ける。例えば、コンテンツサーバ２０－１用の秘密鍵は「ＳＫ－ＣＳ－１」と呼ぶ。

【００５８】

なお、認証サーバ１７、各移動体端末１１、管理サーバ１６および各コンテンツサーバ２０は、それぞれの秘密鍵を用いた暗号化アルゴリズムと、公開鍵を用いた復号化アルゴリズムとが共通しているため、それぞれの装置は鍵を交換することにより、相互にデータの暗号化および復号化が可能である。

【００５９】

［１．２．１．２］アプリケーションの審査

コンテンツサーバ２０の管理事業者は、自分が管理をしているアプリケーションが他のアプリケーションとの連係を行う必要がある場合や、高い価値を有する情報を扱うものである場合には、それらのアプリケーションにある程度以上の信頼度を与えるよう、管理サーバ１６の管理事業者に対しアプリケーションの内容審査を依頼することができる。

【００６０】

管理サーバ１６の管理事業者は、コンテンツサーバ２０の管理事業者よりアプリケーションの内容審査の依頼を受けると、そのアプリケーションの利用目的、アプリケーションの動作内容、コンテンツサーバ２０の管理事業者によるアプリケーションの管理体制等を審査し、その結果に応じて審査したアプリケーションに対し信頼度を与える。信頼度の区分方法にはさまざまな方法が考えられるが、以下の説明においては簡単化のため、審査によって与えられる信頼度は「１」、「２」、「３」、「４」、「５」の５段階とし、数が大きいほど信頼度が高いものとする。なお、審査が行われていないアプリケーションに関しては、信頼度「０」が与えられるものとする。

【００６１】

例えば、信頼度「５」の与えられたアプリケーションは、管理サーバ１６の管理事業者により、コンテンツサーバ２０の管理事業者による管理体制やアプリケーションの動作の安定性等が検証され、必要に応じて、移動体端末１１の制御用プログラム、制御用メモリ３２に格納されているデータ、メモリ１２に格納されているアプリケーションおよびデータを利用できる。それらのデータの中には、移動体端末１１のユーザの個人情報やクレジットカード番号等の高い価値を有する情報が含まれている可能性がある。

【００６２】

それに対し、例えば信頼度「１」の与えられたアプリケーションは、アプリケーションの動作は安定しているが、そのアプリケーションがそもそも個人情報や金銭情報等の高い価値を持ったデータの利用を目的としていないため、低い信頼度で動作上の問題がない、

と判断されたアプリケーションや、コンテンツサーバ２０の管理事業者によるデータ管理体制が不十分等の理由で、高い価値を持ったデータを扱うとデータ漏洩等の危険性がある、と判断されたアプリケーションである。信頼度「１」の与えられたアプリケーションは、他の信頼度「１」を与えられたアプリケーション、もしくは信頼度が「０」であるアプリケーションとの間では連係動作を行うことができる。しかしながら、信頼度「１」の与えられたアプリケーションは、信頼度が「２」、「３」、「４」、もしくは「５」であるアプリケーションに対してデータを渡したり、機能を提供することはできるが、それらのアプリケーションからデータを受け取ったり、それらのアプリケーションの機能を利用することはできない。また、移動体端末１１の制御用プログラムの機能を利用したり、制御用メモリ３２に格納されたデータを利用することも一切できない。

【００６３】

管理サーバ１６の管理事業者は、アプリケーションに対して「１」以上の信頼度を与えた場合には、管理サーバ１６の登録アプリケーション領域５２Ｒに、そのアプリケーションの識別番号等と共に信頼度を登録する。

【００６４】

［１．２．１．３］管理サーバに対するアプリケーションの公開依頼

コンテンツサーバ２０の管理事業者は、「１」以上の信頼度の与えられたアプリケーションの移動体端末１１に対する公開を管理サーバ１６に依頼することができる。公開を依頼されたアプリケーションは、管理サーバ１６の登録アプリケーション領域５２Ｒにおける公開に関する項目が「Ｙｅｓ」と登録される。管理サーバ１６は各移動体端末１１から購入可能なアプリケーション情報一覧の送信要求を受信すると、登録アプリケーション領域５２Ｒにおける公開に関する項目が「Ｙｅｓ」であるアプリケーションの情報を移動体端末１１に送信する。その結果、移動体端末１１のユーザは公開依頼のされているアプリケーションを容易に見つけることができ、また容易に購入の手続きを行うことができる。

【００６５】

一方、公開されていないアプリケーションに関しては、移動体端末１１のユーザは例えば配信元のコンテンツサーバ２０内のホームページを介して、直接コンテンツサーバ２０の管理事業者に対し申込みを行うことにより、購入を行う。従って、コンテンツサーバ２０の管理事業者が、自ら定めた一定の条件を満たす移動体端末１１に対してのみ、アプリケーションの配信を行いたいような場合には、アプリケーションの公開を管理サーバ１６に対して依頼しない方が好都合である。なお、アプリケーションが管理サーバ１６において公開されない場合も、アプリケーションは管理サーバ１６経由で移動体端末１１に配信され、管理サーバ１６によりアプリケーション情報の管理が行われる点には変わりがない。

【００６６】

［１．２．１．４］管理サーバに対する料金徴収代行依頼

コンテンツサーバ２０の管理事業者は、「１」以上の信頼度の与えられたアプリケーションに関して、管理サーバ１６に対し、その利用料金の徴収代行を依頼することができる。利用料金の徴収代行の依頼をされたアプリケーションは、管理サーバ１６の登録アプリケーション領域５２Ｒにおける料金徴収に関する項目が「Ｙｅｓ」と登録される。

【００６７】

管理サーバ１６は各移動体端末１１から料金徴収に関する項目が「Ｙｅｓ」であるアプリケーションの購入要求を受けると、アプリケーションの情報が管理サーバ１６の配信可能アプリケーション領域５３Ｂに書き込まれた時点で、アプリケーションの識別番号、移動体端末１１の識別番号、および購入日時等の情報を移動体通信網１５に接続された課金管理サーバに送信する。同様に、管理サーバ１６は、、ある移動体端末１１について、料金徴収に関する項目が「Ｙｅｓ」であるアプリケーションのアクティベーション処理を行うと、その時点で、アプリケーションの識別番号、その移動体端末１１の識別番号、および購入日時等の情報を移動体通信網１５に接続された課金管理サーバに送信する。課金管理サーバは管理サーバ１６から送信されるこれらの情報に基づき、該当する移動体端末１

１のアプリケーションの利用料金を算出する。アプリケーションの利用料金が購入時から課金されるか、アクティベーション処理の時点から課金されるかは、コンテンツサーバ２０の管理事業者と管理サーバ１６もしくは移動体通信網１５の管理事業者の間で取り決められており、課金管理サーバに課金に関する情報として記録されている。課金管理サーバにより算出されるアプリケーションの利用料金は、同じく課金管理サーバにより算出される移動体端末１１の通信料金と共に、移動体通信網１５の管理事業者により移動体端末１１のユーザから徴収される。その後、移動体通信網１５の管理事業者は各アプリケーションの提供元であるコンテンツサーバ２０の管理事業者に対し、徴収したアプリケーションの利用料金から一定の徴収代行手数料を差し引いた金額を送金する。さらに、移動体通信網１５の管理事業者は、得られた徴収代行手数料の一定部分を管理サーバ１６の管理事業者に課金のための情報提供サービス料として送金する。

【００６８】

［１．２．１．５］管理サーバに対するアプリケーション格納依頼

コンテンツサーバ２０の管理事業者は、「１」以上の信頼度の与えられたアプリケーションに関して、管理サーバ１６に対し、アプリケーションを管理サーバ１６の登録アプリケーション領域５２Ｒに格納するよう依頼することができる。あるアプリケーションの格納依頼が行われた場合、登録アプリケーション領域５２Ｒの保管場所に関する項目には、そのアプリケーションの保管場所情報ではなく、アプリケーション本体が格納される。

【００６９】

登録アプリケーション領域５２Ｒにおいて、アプリケーション本体を格納するか、それともアプリケーションの保管場所情報を格納するかは、管理サーバ１６とコンテンツサーバ２０との間の通信速度や、アプリケーションの内容等に応じて、コンテンツサーバ２０の管理事業者により決定される。アプリケーション本体を登録アプリケーション領域５２Ｒに格納しておくと、移動体端末１１から管理サーバ１６に対しアプリケーションの配信要求があった場合、管理サーバ１６はアプリケーション本体をその都度コンテンツサーバ２０から送信してもらう必要がないため、迅速に移動体端末１１にアプリケーションの配信を行うことができる。従って、例えば管理サーバ１６とコンテンツサーバ２０との間の通信速度が遅い場合、コンテンツサーバ２０の管理事業者はアプリケーションを登録アプリケーション領域５２Ｒに格納することを依頼するメリットが大きい。一方、アプリケーション本体を登録アプリケーション領域５２Ｒに格納せず、移動体端末１１から管理サーバ１６に対しアプリケーションの配信要求がある毎にアプリケーション本体をコンテンツサーバ２０から管理サーバ１６に送信するようにすると、コンテンツサーバ２０は各移動体端末１１に応じたアプリケーションの配信を行うことが可能となる。例えば、コンテンツサーバ２０は同じアプリケーションに関して、各移動体端末１１に対し個別のアクセスキーを設定して、正しい移動体端末１１のユーザ以外の者によるそのアプリケーションの利用を禁止することができる。

【００７０】

コンテンツサーバ２０－１が、あるアプリケーションの格納を管理サーバ１６に依頼する際の処理を、図１０および図１１のフロー図を用いて説明する。まず、コンテンツサーバ２０－１は管理サーバ１６に対し、アプリケーションの格納依頼を送信する（ステップＳ１０１）。この格納依頼にはアプリケーションの識別番号が含まれている。

【００７１】

管理サーバ１６はアプリケーションの格納依頼を受信すると、格納依頼に含まれている識別番号を用いて、登録アプリケーション領域５２Ｒのデータを読み出し、対象のアプリケーションに信頼度が与えられていることを確認する。対象のアプリケーションに信頼度が与えられていることが確認できた場合、管理サーバ１６はコンテンツサーバ２０－１に対し、格納依頼の受諾通知を送信する（ステップＳ１０２）。

【００７２】

コンテンツサーバ２０－１は格納依頼の受諾通知を受信すると、認証サーバ１７に対し、管理サーバ１６の公開鍵「ＰＫ－ＭＳ」の送信要求を行う（ステップＳ１０３）。認証

サーバ１７はこの公開鍵の送信要求に応じ、コンテンツサーバ２０－１に対し「ＰＫ－ＭＳ」を送信する（ステップＳ１０４）。

【００７３】

コンテンツサーバ２０－１は「ＰＫ－ＭＳ」を受信すると、アプリケーションを「ＰＫ－ＭＳ」を用いて暗号化する（ステップＳ１０５）。この暗号化処理により、アプリケーションがコンテンツサーバ２０－１から管理サーバ１６に送信される際、第３者がこれを傍受しても内容を解読することができず、アプリケーションが第３者により不正に使用されることが防がれる。

【００７４】

続いて、コンテンツサーバ２０－１はコンテンツサーバ２０－１の秘密鍵「ＳＫ－ＣＳ－１」を用いて、既に暗号化されているアプリケーションをさらに暗号化する（ステップＳ１０６）。この暗号化処理により、管理サーバ１６はこのアプリケーションが間違いなくコンテンツサーバ２０－１から送信されたものであることを確認することができる。すなわち、この暗号化処理は管理サーバ１６がアプリケーションの送信元を確認するための証明書の役割を果たす。

【００７５】

コンテンツサーバ２０－１は二重に暗号化されたアプリケーションを管理サーバ１６に対し送信する（ステップＳ１０７）。

【００７６】

管理サーバ１６は二重に暗号化されたアプリケーションを受信すると、管理サーバ１６の暗号鍵格納部５１のデータを読み出し、コンテンツサーバ２０－１の公開鍵「ＰＫ－ＣＳ－１」が登録されているかどうかを確認する。管理サーバ１６は、「ＰＫ－ＣＳ－１」が暗号鍵格納部５１に登録されていない場合、認証サーバ１７に対し「ＰＫ－ＣＳ－１」の送信要求を行う（ステップＳ１０８）。認証サーバ１７はこの公開鍵の送信要求に応じ、管理サーバ１６に対し「ＰＫ－ＣＳ－１」を送信する（ステップＳ１０９）。管理サーバ１６は、「ＰＫ－ＣＳ－１」が暗号鍵格納部５１に登録されている場合、改めて「ＰＫ－ＣＳ－１」を取得する必要はないので、ステップＳ１０８およびステップＳ１０９は行わず、次のステップＳ１１０に進む。

【００７７】

続いて、管理サーバ１６は、二重に暗号化されたアプリケーションを「ＰＫ－ＣＳ－１」を用いて復号化する（ステップＳ１１０）。ここでアプリケーションの復号化に失敗した場合、管理サーバ１６の受信したアプリケーションは送信途中に改竄が行われたか、何らかの理由で破損しているか、コンテンツサーバ２０－１以外のサーバから送信されたものであるので、管理サーバ１６はこのアプリケーションの格納処理を中止し、コンテンツサーバ２０－１に正しいアプリケーションの再送要求を行う。一方、「ＰＫ－ＣＳ－１」を用いたアプリケーションの復号化が成功した場合、アプリケーションはコンテンツサーバ２０－１から問題なく送信されたことが確認されるので、管理サーバ１６は続いて、このアプリケーションを管理サーバ１６の秘密鍵「ＳＫ－ＭＳ」を用いて復号化する（ステップＳ１１１）。管理サーバ１６は上記の処理により、平文となったアプリケーションを取得できるので、その内容にコンテンツサーバ２０－１による改竄等が行われていないことを確認できる。

【００７８】

なお、上記の処理のうち、ステップＳ１０３からステップＳ１１１までの一連の処理は、以下の説明において「管理サーバへのアプリケーション送信処理１」と呼ぶ。

【００７９】

管理サーバ１６は、ステップＳ１１１の処理を終えると、アプリケーションそのアプリケーションを登録アプリケーション領域５２Ｒに格納し（ステップＳ１１２）、コンテンツサーバ２０－１に対し格納処理の完了通知を送信する（ステップＳ１１３）。

【００８０】

［１．２．２］アプリケーションの購入

アプリケーションの配信は、移動体端末１１のユーザがアプリケーションを購入することにより可能となる。移動体端末１１のユーザが希望するアプリケーションを購入する方法としては、管理サーバ１６によって公開されているアプリケーションを購入する方法と、コンテンツサーバ２０内のホームページ等を介して、移動体端末１１のユーザがコンテンツサーバ２０の管理事業者と直接購入契約を結ぶ方法がある。さらに、移動体端末１１のユーザがコンテンツサーバ２０の管理事業者と直接購入契約を結ぶ方法には、「１」以上の信頼度を与えられたアプリケーションを購入する場合と、信頼度が「０」であるアプリケーションを購入する場合がある。以下、それぞれの場合について、購入処理の流れを説明する。

【００８１】

［１．２．２．１］管理サーバにおいて公開されているアプリケーションの購入

移動体端末１１のユーザが管理サーバ１６において公開されているアプリケーションを購入する場合の例として、移動体端末１１－１のユーザが管理サーバ１６を介してコンテンツサーバ２０－１が配信元であるアプリケーションを購入する場合の処理を図１２および図１３および図１４および図１５を用いて説明する。

【００８２】

移動体端末１１－１のユーザは、移動体端末１１－１のアプリボタン２３を押下して、画面Ｄ１１に示すアプリケーションメニューを表示させる。続いて、移動体端末１１－１のユーザは、操作部２２のボタン「１」を押下して「１．アプリケーションの新規購入」を選択する。ボタン「１」が押下されると、移動体端末１１－１は管理サーバ１６に対し、アプリケーション情報一覧の送信要求を行う（ステップＳ２０１）。

【００８３】

管理サーバ１６はアプリケーション情報一覧の送信要求を受信すると、登録アプリケーション領域５２Ｒのデータを読み出し、公開に関する項目が「Ｙｅｓ」であり、かつユーザ情報格納部５３－１に登録されていないアプリケーションの情報を抽出する。続いて、管理サーバ１６は抽出された情報から、アプリケーションの識別番号、名称、機能、利用料金、料金徴収の代行の別、配信元のコンテンツサーバ２０内の所定のホームページのＵＲＬ等の情報を、アプリケーション情報一覧として移動体端末１１－１に送信する（ステップＳ２０２）。

【００８４】

移動体端末１１－１はアプリケーション情報一覧を受信すると、画面Ｄ１２を表示させる。これに対し、移動体端末１１－１のユーザは購入希望のアプリケーションに対応する番号のボタンを押下する。例えばユーザが画面Ｄ１２においてボタン「１」を押下すると、「スケジュール管理　Ｖｅｒ．２」が選択され、移動体端末１１－１はディスプレイ部２１に画面Ｄ１３を表示する。画面Ｄ１３には指定されたアプリケーションの機能に関する情報および利用料金が示されており、ユーザはこれらの情報に基づきこのアプリケーションの購入の判断を行う。

【００８５】

移動体端末１１－１のユーザが画面Ｄ１３においてアプリケーションの購入を決定し、ボタン「９」を押下すると、移動体端末１１－１は指定されたアプリケーションの識別番号を管理サーバ１６に送信する（ステップＳ２０３）。その後、移動体端末１１－１はディスプレイ部２１に画面Ｄ１４を表示させる。

【００８６】

管理サーバ１６はアプリケーションの識別番号を受信すると、登録アプリケーション領域５２Ｒのデータを読み出し、対応するアプリケーションの保管場所を確認する（ステップＳ２０４）。

【００８７】

ここで指定されたアプリケーション本体が登録アプリケーション領域５２Ｒに格納されていない場合、管理サーバ１６は登録アプリケーション領域５２Ｒのデータよりアプリケーションの保管場所情報としてコンテンツサーバ２０－１内のＵＲＬを取得し、コンテン

ツサーバ２０－１に対しアプリケーションの送信要求を送信する（ステップＳ２０５）。
【００８８】
コンテンツサーバ２０－１はアプリケーションの送信要求を受信すると、前述の「管理サーバへのアプリケーション送信処理１」を開始し、管理サーバ１６、認証サーバ１７、およびコンテンツサーバ２０－１の間において図１０および図１１におけるステップＳ１０３からステップＳ１１１までの処理と同様の処理が行われる。その結果、管理サーバ１６は該当するアプリケーションを取得する（ステップＳ２０６）。
【００８９】
管理サーバ１６は取得したアプリケーションに保管番号を与え、その保管番号と共にアプリケーションを一時保管アプリケーション領域５２Ｔに格納する（ステップＳ２０７）。この保管番号は管理サーバ１６が取得したアプリケーションを一時保管アプリケーション領域５２Ｔにおいて識別するためのものであり、同じ内容のアプリケーションであっても配信先の移動体端末が異なると異なる保管番号となる。
【００９０】
一方、移動体端末１１－１により指定されたアプリケーションが管理サーバ１６の登録アプリケーション領域５２Ｒに格納されている場合、管理サーバ１６は既にアプリケーションを取得しているので、上記のステップＳ２０５からステップＳ２０７までの処理は行わず、次のステップＳ２０８の処理に進む。
【００９１】
続いて、管理サーバ１６はユーザ情報格納部５３－１における配信可能アプリケーション領域５３Ｂにコンテンツサーバ２０－１から取得したアプリケーションに関する情報、すなわちアプリケーションの識別番号、信頼度等を登録する（ステップＳ２０８）。この登録処理により、移動体端末１１－１のユーザは希望する時にこの既登録のアプリケーションを移動体端末１１－１にダウンロードすることが可能となる。なお、この登録処理において、アクティベーションに関する項目に関しては、この時点ではまだコンテンツサーバ２０－１から取得したアプリケーションは移動体端末１１－１にダウンロードされておらず、従ってアクティベーション処理も行われていないので、「Ｎｏ」が登録される。さらに、登録されるアプリケーションが一時保管アプリケーション領域５２Ｔに格納されている場合には、配信可能アプリケーション領域５３Ｂには保管番号も登録される。この登録処理が完了すると、管理サーバ１６は移動体端末１１－１に対し、アプリケーション購入処理の完了通知を送信する（ステップＳ２０９）。
【００９２】
移動体端末１１－１はアプリケーション購入処理の完了通知を受信すると、画面Ｄ１５もしくは画面Ｄ１６を表示する。画面Ｄ１５は、新たに購入されたアプリケーションの利用に関し、料金徴収の代行依頼が行われている場合に表示される画面の例であり、移動体端末１１－１のユーザに対し利用料金が通信料金と共に請求されることが通知される。一方、画面Ｄ１６は、料金徴収の代行依頼が行われていない場合に表示される画面の例であり、移動体端末１１－１のユーザに対し利用料金の支払手続を別途行うよう連絡がなされる。画面Ｄ１６において、移動体端末１１－１のユーザはボタン「０」を押下して、コンテンツサーバ２０－１の管理事業者の運営する所定のホームページに移動し、そのホームページにおいて、購入したアプリケーションの料金支払に関する手続を行うことができる。
【００９３】
移動体端末１１－１のユーザが、画面Ｄ１５もしくは画面Ｄ１６においてボタン「９」を押下してアプリケーションの新規購入の処理を終了すると、移動体端末１１－１はディスプレイ部２１に画面Ｄ１７を表示する。画面Ｄ１７は移動体端末１１－１の通常の画面であるが、上部に「α」が表示されている。この「α」の表示は、移動体端末１１－１のユーザに対し、新たにダウンロードが可能となったアプリケーションがあることを知らせるための表示である。なお、移動体端末１１－１のユーザに対し、新たにダウンロードが可能となったアプリケーションがあることを知らせるための方法は「α」の表示に限られ

ず、他の文字や画像の表示、および音や振動による通知であってもよい。

【００９４】

一方、ステップＳ２０９においてアプリケーション購入処理の完了通知を行った管理サーバ１６は、続いてコンテンツサーバ２０－１に対し移動体端末１１－１によってアプリケーションの購入が行われたことを通知する（ステップＳ２１０）。また、新たに移動体端末１１－１によって購入処理が行われたアプリケーションの料金徴収の代行依頼がなされている場合には、管理サーバ１６は購入されたアプリケーションの識別番号、移動体端末１１－１の識別番号、購入日時等の情報を課金管理サーバに送信する（ステップＳ２１１）。

【００９５】

［１．２．２．２］「１」以上の信頼度を与えられ、かつ公開されていないアプリケーションの購入

【００９６】

移動体端末１１のユーザが、「１」以上の信頼度を与えられているが、管理サーバ１６において公開されていないアプリケーションを購入する場合の例として、移動体端末１１－１のユーザが、コンテンツサーバ２０－１が配信元であるアプリケーションを購入する場合の処理を図１６および図１７を用いて説明する。

【００９７】

移動体端末１１－１のユーザが、管理サーバ１６において公開されていないアプリケーションを購入する場合、移動体端末１１－１のユーザは、例えば移動体端末１１－１を用いてコンテンツサーバ２０－１内のホームページを開き、そのホームページにおいて目的のアプリケーションの購入申請を行う（ステップＳ３０１）。その際、必要であれば、移動体端末１１－１のユーザは購入するアプリケーションの利用料金の支払手続も行うものとする。

【００９８】

コンテンツサーバ２０－１は移動体端末１１－１の購入申請の内容が所定の条件を満たしていることを確認した後、移動体端末１１－１に対しアプリケーションの購入承諾通知を送信する（ステップＳ３０２）。この購入承諾通知にはアプリケーションの識別番号が含まれている。なお、コンテンツサーバ２０－１は購入承諾通知を送信する際、購入承諾を行った移動体端末１１－１の識別番号を記録する。

【００９９】

移動体端末１１－１は、アプリケーションの購入承諾通知を受信すると、管理サーバ１６に対し購入したアプリケーション情報の登録要求を送信する（ステップＳ３０３）。この登録要求には、新たに購入されたアプリケーションの識別番号が含まれている。

【０１００】

管理サーバ１６は、移動体端末１１－１から購入アプリケーション情報の登録要求を受信すると、登録アプリケーション領域５２Ｒのデータを読み出し、登録要求のされたアプリケーションの識別番号からそのアプリケーションの配信元情報としてコンテンツサーバ２０－１内のＵＲＬを取得する。続いて、管理サーバ１６はそのＵＲＬを用いて、コンテンツサーバ２０－１に対し、移動体端末１１－１に対する購入アプリケーション情報の登録を行ってよいかどうかを確認するための登録許可を要求する（ステップＳ３０４）。この登録許可の要求には、移動体端末１１－１の識別番号が含まれている。

【０１０１】

コンテンツサーバ２０－１は管理サーバ１６よりアプリケーション情報の登録許可の要求を受信すると、管理サーバ１６がアプリケーション情報を登録しようとしている移動体端末の識別番号が、ステップＳ３０２においてアプリケーションの購入承諾を行った移動体端末の識別番号と一致することを確認する。コンテンツサーバ２０－１は、それらの識別番号が一致すると、管理サーバ１６に対しアプリケーション情報の登録許可を通知する（ステップＳ３０５）。

【０１０２】

管理サーバ１６はコンテンツサーバ２０－１よりアプリケーション情報の登録許可を受信すると、登録アプリケーション領域５２Ｒのデータを読み出し、移動体端末１１－１から登録要求のあったアプリケーションの保管場所を確認する（ステップＳ３０６）。

【０１０３】

ステップＳ３０６において、登録要求のあったアプリケーション本体が登録アプリケーション領域５２Ｒに格納されていない場合、管理サーバ１６は登録アプリケーション領域５２Ｒの保管場所に関する情報を用いて、コンテンツサーバ２０－１に対し対応するアプリケーションの送信要求を送信する（ステップＳ３０７）。コンテンツサーバ２０－１はアプリケーションの送信要求を受信すると、前述の「管理サーバへのアプリケーション送信処理１」を開始し、管理サーバ１６、認証サーバ１７、およびコンテンツサーバ２０－１の間において図１０および図１１におけるステップＳ１０３からステップＳ１１１までの処理と同様の処理が行われる。その結果、管理サーバ１６は該当するアプリケーションを取得する（ステップＳ３０８）。管理サーバ１６は取得したアプリケーションに保管番号を与え、その保管番号と共にアプリケーションを一時保管アプリケーション領域５２Ｔに格納する（ステップＳ３０９）。

【０１０４】

一方、移動体端末１１－１により登録要求のあったアプリケーションが登録アプリケーション領域５２Ｒに格納されている場合、管理サーバ１６は上記のステップＳ３０７からステップＳ３０９までの処理を行わず、次のステップＳ３１０の処理に進む。

【０１０５】

続いて、管理サーバ１６はユーザ情報格納部５３－１における配信可能アプリケーション領域５３Ｂに、移動体端末１１－１により登録要求のあったアプリケーションの情報、すなわちアプリケーションの識別番号、信頼度等を登録する（ステップＳ３１０）。なお、アクティベーションに関する項目については、まだアクティベーション処理が行われていないため、「Ｎｏ」が登録される。また、アプリケーションが一時保管アプリケーション領域５２Ｔに格納されている場合、配信可能アプリケーション領域５３Ｂには保管番号も登録される。この登録処理により、移動体端末１１－１のユーザは希望する時に新たに登録されたアプリケーションを移動体端末１１－１にダウンロードすることが可能となる。従って、管理サーバ１６は移動体端末１１－１に対し、アプリケーション購入処理の完了通知を送信する（ステップＳ３１１）。

【０１０６】

移動体端末１１－１は、アプリケーション購入処理の完了通知を受信すると、ディスプレイ部２１に「α」を表示し、購入されたアプリケーションが管理サーバ１６よりダウンロード可能となったことをユーザに知らせる。

【０１０７】

ここで、コンテンツサーバ２０－１により管理サーバ１６に対して、新たに登録が行われたアプリケーションの料金徴収の代行依頼がされている場合には、管理サーバ１６はアプリケーションの識別番号、移動体端末１１－１の識別番号、購入日時等の情報を課金管理サーバに送信する（ステップＳ３１２）。

【０１０８】

［１．２．２．３］信頼度が「０」であるアプリケーションの購入

移動体端末１１のユーザが、信頼度が「０」であるアプリケーションを購入する場合の例として、移動体端末１１－１のユーザがコンテンツサーバ２０－１が配信元であるアプリケーションを購入する場合の処理を図１８、図１９、および図２０を用いて説明する。以下の処理は図１６および図１７を用いて説明したステップＳ３０１以下の処理と類似しているが、「１」以上の信頼度を与えられていないため、管理サーバ１６はアプリケーションの内容を平文として取得する必要はない。従って、アプリケーションがコンテンツサーバ２０－１から管理サーバ１６に送信される際、アプリケーションは管理サーバ１６の公開鍵ではなく、配信先の移動体端末１１－１の公開鍵で暗号化される。その結果、移動体端末１１－１のユーザ以外がアプリケーションの送信を傍受してもその内容を解読でき

ないため、アプリケーションの不正使用が防止されるとともに、その内容の秘匿性が確保される。

【０１０９】

まず、移動体端末１１－１のユーザは、例えば移動体端末１１－１を用いてコンテンツサーバ２０－１内のホームページを開き、そのホームページにおいて目的のアプリケーションの購入を申請する（ステップＳ４０１）。その際、移動体端末１１－１のユーザは購入するアプリケーションの利用料金の支払手続も行うものとする。

【０１１０】

コンテンツサーバ２０－１は移動体端末１１－１の購入申請の内容が一定の条件を満たしていることを確認した後、移動体端末１１－１に対しアプリケーションの購入承諾通知を送信する（ステップＳ４０２）。この購入承諾通知にはアプリケーションの識別番号が含まれている。また、コンテンツサーバ２０－１は購入承諾通知を送信する際、購入承諾を行った移動体端末１１－１の識別番号を記録する。

【０１１１】

移動体端末１１－１は、アプリケーションの購入承諾通知を受信すると、管理サーバ１６に対し、新たに購入したアプリケーション情報の登録要求を送信する（ステップＳ４０３）。この登録要求には、アプリケーションの識別番号およびアプリケーションの保管場所情報としてコンテンツサーバ２０－１内のＵＲＬが含まれている。

【０１１２】

管理サーバ１６は、移動体端末１１－１からアプリケーション情報の登録要求を受信すると、コンテンツサーバ２０－１に対し、アプリケーションの送信要求を行う（ステップＳ４０４）。この送信要求には、移動体端末１１－１の識別番号が含まれている。

【０１１３】

コンテンツサーバ２０－１は管理サーバ１６よりアプリケーションの送信要求を受信すると、送信要求を行っている移動体端末の識別番号が、ステップＳ４０２においてアプリケーションの購入承諾を行った移動体端末の識別番号と一致するかどうかを確認する。これらの識別番号が一致する場合、コンテンツサーバ２０－１は、認証サーバ１７に対し移動体端末１１－１の公開鍵「ＰＫ－ＭＴ－１」の送信を要求する（ステップＳ４０５）。認証サーバ１７は「ＰＫ－ＭＴ－１」の送信要求を受信すると、コンテンツサーバ２０－１に対し「ＰＫ－ＭＴ－１」を送信する（ステップＳ４０６）。

【０１１４】

コンテンツサーバ２０－１は「ＰＫ－ＭＴ－１」を受信すると、送信要求のされたアプリケーションを「ＰＫ－ＭＴ－１」を用いて暗号化する（ステップＳ４０７）。

【０１１５】

続いて、コンテンツサーバ２０－１はコンテンツサーバ２０－１の秘密鍵「ＳＫ－ＣＳ－１」を用いて、既に暗号化されているアプリケーションをさらに暗号化する（ステップＳ４０８）。この暗号化処理により、管理サーバ１６はこのアプリケーションが間違いなくコンテンツサーバ２０－１から送信されたものであることを確認することができる。

【０１１６】

コンテンツサーバ２０－１は二重に暗号化されたアプリケーションを管理サーバ１６に対し送信する（ステップＳ４０９）。

【０１１７】

管理サーバ１６は二重に暗号化されたアプリケーションを受信すると、管理サーバ１６の暗号鍵格納部５１のデータを読み出し、コンテンツサーバ２０－１の公開鍵「ＰＫ－ＣＳ－１」が登録されているかどうかを確認する。管理サーバ１６は、「ＰＫ－ＣＳ－１」が暗号鍵格納部５１に登録されていない場合、認証サーバ１７に対し「ＰＫ－ＣＳ－１」の送信要求を行う（ステップＳ４１０）。認証サーバ１７はこの公開鍵の送信要求に応じ、管理サーバ１６に対し「ＰＫ－ＣＳ－１」を送信する（ステップＳ４１１）。管理サーバ１６は、「ＰＫ－ＣＳ－１」が暗号鍵格納部５１に登録されている場合、改めて「ＰＫ－ＣＳ－１」を取得する必要はないので、ステップＳ４１０およびステップＳ４１１は行

わず、次のステップＳ４１２に進む。

【０１１８】

続いて、管理サーバ１６は、二重に暗号化されたアプリケーションを「ＰＫ－ＣＳ－１」を用いて復号化する（ステップＳ４１２）。ここでアプリケーションの復号化に失敗した場合、管理サーバ１６の受信したアプリケーションは送信途中に改竄が行われたか、何らかの理由で破損しているか、コンテンツサーバ２０－１以外のサーバから送信されたものであるので、管理サーバ１６はこのアプリケーションの格納処理を中止し、コンテンツサーバ２０－１に正しいアプリケーションの再送要求を行う。一方、「ＰＫ－ＣＳ－１」を用いたアプリケーションの復号化が成功した場合、アプリケーションはコンテンツサーバ２０－１から問題なく送信されたことが確認される。

【０１１９】

なお、以下の説明において、上記のステップＳ４０５からステップＳ４１２までの一連の処理を、「管理サーバへのアプリケーション送信処理２」と呼ぶ。

【０１２０】

続いて、管理サーバ１６はそのアプリケーションに保管番号を与え、その保管番号と共にアプリケーションを一時保管アプリケーション領域５２Ｔに格納する（ステップＳ４１３）。なお、この場合、一時保管アプリケーション領域５２Ｔに格納されるアプリケーションは移動体端末１１－１の公開鍵「ＰＫ－ＭＴ－１」により暗号化されたままであり、管理サーバ１６の管理事業者等から内容を解読されることはない。

【０１２１】

続いて、管理サーバ１６は、登録アプリケーション領域５２Ｒにアプリケーションの識別番号およびアプリケーションの保管場所情報としてコンテンツサーバ２０－１内のＵＲＬを登録する（ステップＳ４１４）。この登録は、管理サーバ１６が移動体端末１１－１からの要求に応じ、同じアプリケーションを再度コンテンツサーバ２０－１から取得する際に必要な情報の登録処理である。なお、このアプリケーションに関する登録アプリケーション領域５２Ｒにおける信頼度は「０」、公開および料金徴収に関する項目は空欄（「－」）となる。

【０１２２】

次に、管理サーバ１６はユーザ情報格納部５３－１における配信可能アプリケーション領域５３Ｂに、移動体端末１１－１により登録要求のあったアプリケーション情報、すなわちアプリケーションの識別番号、保管番号等を登録する（ステップＳ４１５）。なお、アクティベーションに関する項目については、「Ｎｏ」が登録され、信頼度に関する項目については、「０」が登録される。この登録処理により、移動体端末１１－１のユーザは希望する時に新たに登録されたアプリケーションを移動体端末１１－１にダウンロードすることが可能となる。管理サーバ１６はこの登録処理を完了すると、移動体端末１１－１に対し、アプリケーションの購入処理の完了通知を送信する（ステップＳ４１６）。

【０１２３】

移動体端末１１－１は、アプリケーション購入処理の完了通知を受信すると、ディスプレイ部２１に「α」を表示し、購入されたアプリケーションが管理サーバ１６よりダウンロード可能となったことをユーザに知らせる。

【０１２４】

［１．２．３］移動体端末によるアプリケーションのダウンロード

移動体端末１１のユーザはアプリケーションを購入した後、購入したアプリケーションをダウンロードする必要がある。以下、アプリケーションのダウンロードの処理を、移動体端末１１－１を例として図２１および図２２および図２３、図２４、および図２５を用いて説明する。

【０１２５】

移動体端末１１－１のユーザは、まず移動体端末１１－１のアプリボタン２３を押下して、画面Ｄ２１のアプリケーションメニューを表示させる。画面Ｄ２１において、移動体端末１１－１のユーザは、操作部２２のボタン「２」を押下して「２．アプリケーション

のダウンロード」を選択する。ボタン「２」が押下されると、移動体端末１１－１は管理サーバ１６に対し、ダウンロードの可能なアプリケーション情報一覧の送信要求を行う（ステップＳ５０１）。

【０１２６】

管理サーバ１６はアプリケーション情報一覧の送信要求を受信すると、ユーザ情報格納部５３－１の配信可能アプリケーション領域５３Ｂに登録されているアプリケーションの名称を、アプリケーションの識別番号と共にアプリケーション情報一覧として移動体端末１１－１に送信する（ステップＳ５０２）。

【０１２７】

移動体端末１１－１はアプリケーション情報一覧を受信すると、画面Ｄ２２を表示させる。これに対し、移動体端末１１－１のユーザは対応する番号のボタンを押下することにより、ダウンロードするアプリケーションの指定を行う。例えばユーザが画面Ｄ２２においてボタン「１」を押下すると、「スケジュール管理　Ｖｅｒ．２」という名称のアプリケーションが選択される。移動体端末１１－１のユーザによるボタン操作によりアプリケーションが指定されると、移動体端末１１－１は管理サーバ１６に対し、指定されたアプリケーションの識別番号を送信する（ステップＳ５０３）。

【０１２８】

管理サーバ１６は指定されたアプリケーションの識別番号を受信すると、配信可能アプリケーション領域５３Ｂのデータを読み出し、指定されたアプリケーションが信頼度の与えられたものであるか否かを確認する。続いて、管理サーバ１６は既配信アプリケーション領域５３Ａのデータを読み出し、移動体端末１１－１のメモリ１２において、指定されたアプリケーションを書き込むために必要な空き容量があるかどうかを確認する（ステップＳ５０４）。その際、指定されたアプリケーションに信頼度が与えられている場合は、管理エリア４０に空き容量があるかどうかが確認される。一方、指定されたアプリケーションに信頼度が与えられていない場合は、フリーエリア４１に空き容量があるかどうかが確認される。

【０１２９】

ステップＳ５０４において、移動体端末１１－１のメモリ１２に指定されたアプリケーションを書き込むための空き容量が十分でない場合、管理サーバ１６は移動体端末１１－１に対し、メモリ１２上から削除すべきアプリケーションの指定要求を送信する（ステップＳ５０５）。この指定要求には、ダウンロードの指定のされたアプリケーションが信頼度の与えられたものであるか否かの情報が含まれている。移動体端末１１－１はこの指定要求を受信すると、画面Ｄ２３をディスプレイ部２１に表示させる。移動体端末１１－１のユーザがこの画面に対しボタン「９」を押下して実行の指示を行うと、移動体端末１１－１はさらに画面Ｄ２４をディスプレイ部２１に表示させる。ダウンロードの指定のされたアプリケーションが信頼度の与えられたものである場合、画面Ｄ２４には管理エリア４０に書き込まれているアプリケーションの名称が表示され、ダウンロードの指定のされたアプリケーションが信頼度の与えられていないものである場合、画面Ｄ２４にはフリーエリア４１に書き込まれているアプリケーションの名称が表示される。この画面において、移動体端末１１－１のユーザは対応するボタンを押下することにより、メモリ１２から削除するアプリケーションを指定する。移動体端末１１－１は指定されたアプリケーションの識別番号を管理サーバ１６に送信する（ステップＳ５０６）。なお、ステップＳ５０６の処理の後、移動体端末１１－１はディスプレイ部２１に画面Ｄ２５を表示させる。

【０１３０】

一方、ステップＳ５０４において、指定されたアプリケーションを書き込むための空き容量が移動体端末１１－１のメモリ１２に十分ある場合、ステップＳ５０５およびステップＳ５０６の処理は行われず、管理サーバ１６は次のステップＳ５０７の処理に進む。また、移動体端末１１－１はディスプレイ部２１に画面Ｄ２５を表示させる。

【０１３１】

続いて、管理サーバ１６は配信可能アプリケーション領域５３Ｂのデータを読み出し、

移動体端末１１－１によりダウンロードの指定のされたアプリケーションがアプリケーション情報格納部５２に格納されているか否かを確認する（ステップＳ５０７）。図７を用いて、アプリケーションがアプリケーション情報格納部５２に格納されている場合とそうでない場合の例を示す。

【０１３２】

移動体端末１１－１によりダウンロードの指定のされたアプリケーションの識別番号が「ＡＰ－４１２５」であった場合、図７の例によれば対応するアプリケーションの保管場所が「Ｔ－７８５１」であることが分かる。これは目的のアプリケーションが一時保管アプリケーション領域５２Ｔに格納されていることを意味する。また、移動体端末１１－１によりダウンロードの指定のされたアプリケーションの識別番号が「ＡＰ－４５１３」であった場合、図７の例によれば対応するアプリケーションの保管場所のデータが与えられていない。これは対応するアプリケーションが登録アプリケーション領域５２Ｒに格納依頼がなされているアプリケーションであることを意味する。従って、目的のアプリケーションは登録アプリケーション領域５２Ｒに格納されている。

【０１３３】

これらに対し、移動体端末１１－１によりダウンロードの指定のされたアプリケーションの識別番号が「ＡＰ－３０２１」であった場合、図７の例によれば対応するアプリケーションの保管場所が「削除済み」となっている。これは対応するアプリケーションが、一時保管アプリケーション領域５２Ｔにも、登録アプリケーション領域５２Ｒにも格納されていないことを意味する。このように、配信可能アプリケーション領域５３Ｂに登録されているアプリケーションが、アプリケーション情報格納部５２に格納されていない状況が発生する理由は、以下のステップＳ５２３において説明するように、登録アプリケーション領域５２Ｒにおける格納依頼のされていないアプリケーションであって、一度ダウンロードされたアプリケーションに関しては、ダウンロードされた時点で一時保管アプリケーション領域５２Ｔに格納されていたアプリケーションが削除されるためである。

【０１３４】

上記の識別番号「ＡＰ－３０２１」のアプリケーションの例のように、ステップＳ５０７において、ダウンロードの指定のされたアプリケーションがアプリケーション情報格納部５２に格納されていない場合、管理サーバ１６は登録アプリケーション領域５２Ｒのデータを読み出し、ダウンロードの指定のされたアプリケーションの識別番号に対応する保管場所としてコンテンツサーバ２０－１内のＵＲＬを取得し、コンテンツサーバ２０－１に対しアプリケーションの送信要求を送信する（ステップＳ５０８）。

【０１３５】

ダウンロードの指定のされたアプリケーションが信頼度の与えられたアプリケーションである場合、ステップＳ５０８に続いて、コンテンツサーバ２０、認証サーバ１７、および管理サーバ１６の間で、「管理サーバへのアプリケーション送信処理１」と同様の処理が行われる。一方、ダウンロードの指定のされたアプリケーションが信頼度の与えられていないアプリケーションである場合、ステップＳ５０８に続いて、コンテンツサーバ２０、認証サーバ１７、および管理サーバ１６の間で、「管理サーバへのアプリケーション送信処理２」と同様の処理が行われる。その結果、管理サーバ１６は該当するアプリケーションを取得する（ステップＳ５０９）。

【０１３６】

続いて、管理サーバ１６はステップＳ５０９の処理により取得したアプリケーションを、一時保管アプリケーション領域５２Ｔに格納する（ステップＳ５１０）。

【０１３７】

これに対して、ステップＳ５０７において、上記の識別番号が「ＡＰ－４１２５」もしくは「ＡＰ－４５１３」のアプリケーションの例のように、ダウンロードの指定のされたアプリケーションがアプリケーション情報格納部５２に格納されている場合、管理サーバ１６はステップＳ５０８からステップＳ５１０までの処理は行わず、次のステップＳ５１１に進む。

【０１３８】
続いて、管理サーバ１６はアプリケーション情報格納部５２に格納されているダウンロードの指定のされたアプリケーションが、暗号化されているかどうかを確認する（ステップＳ５１１）。ダウンロードの指定のされたアプリケーションが信頼度の与えられたアプリケーションである場合、アプリケーション情報格納部５２には平文のアプリケーションが格納されている。一方、ダウンロードの指定のされたアプリケーションが信頼度の与えられていないアプリケーションである場合、アプリケーション情報格納部５２には移動体端末１１－１の公開鍵を用いて暗号化されたアプリケーションが格納されている。
【０１３９】
ステップＳ５１１において、アプリケーション情報格納部５２に格納されているダウンロードの指定のされたアプリケーションが暗号化されていない場合、管理サーバ１６は、認証サーバ１７に対し、移動体端末１１－１の公開鍵「ＰＫ－ＭＴ－１」の送信要求を行う（ステップＳ５１２）。認証サーバ１７はこの公開鍵の送信要求に応じ、管理サーバ１６に対し「ＰＫ－ＭＴ－１」を送信する（ステップＳ５１３）。
【０１４０】
管理サーバ１６は「ＰＫ－ＭＴ－１」を受信すると、移動体端末１１－１のメモリ１２においてアプリケーションを書き込むべき場所を示す情報をアプリケーションに添付する。また、アプリケーションに信頼度が与えられている場合、管理サーバ１６はアプリケーションにその信頼度も添付する。その後、管理サーバ１６はアプリケーションを「ＰＫ－ＭＴ－１」を用いて暗号化する（ステップＳ５１４）。この暗号化処理により、アプリケーションが管理サーバ１６から移動体端末１１－１に送信される際、第３者がこれを傍受しても、移動体端末１１－１以外はこれを復号化することができず、アプリケーションが第３者により不正に使用されることが防がれる。
【０１４１】
これに対し、ステップＳ５１１において、アプリケーション情報格納部５２に格納されているダウンロードの指定のされたアプリケーションが暗号化されている場合、管理サーバ１６は上記のステップＳ５１２からステップＳ５１４までの処理を行わず、次のステップＳ５１５に進む。
【０１４２】
続いて、管理サーバ１６は管理サーバ１６の秘密鍵「ＳＫ－ＭＳ」を用いて、既に暗号化されているアプリケーションをさらに暗号化する（ステップＳ５１５）。この暗号化処理により、移動体端末１１－１はこのアプリケーションが間違いなく管理サーバ１６から送信されたものであることを確認することができる。すなわち、この暗号化処理は移動体端末１１－１がアプリケーションの出所を確認するための証明書の役割を果たす。
【０１４３】
管理サーバ１６は二重に暗号化されたアプリケーションを、移動体端末１１－１に対し送信する（ステップＳ５１６）。
【０１４４】
移動体端末１１－１は二重に暗号化されたアプリケーションを受信すると、認証サーバ１７に対し管理サーバ１６の公開鍵「ＰＫ－ＭＳ」の送信要求を行う（ステップＳ５１７）。認証サーバ１７はこの公開鍵の送信要求に応じ、移動体端末１１－１に対し「ＰＫ－ＭＳ」を送信する（ステップＳ５１８）。
【０１４５】
移動体端末１１－１は「ＰＫ－ＭＳ」を受信すると、二重に暗号化されたアプリケーションをまず「ＰＫ－ＭＳ」を用いて復号化する（ステップＳ５１９）。ここで復号化に失敗した場合、移動体端末１１－１の受信したアプリケーションは途中で改竄が行われたか、何らかの理由で破損しているか、管理サーバ１６以外のサーバから送信されたものであるので、移動体端末１１－１は管理サーバ１６に正しいアプリケーションの再送要求を行う。一方、「ＰＫ－ＭＳ」を用いた復号化が成功した場合、アプリケーションは管理サーバ１６から問題なく送信されたものであると確認されるので、移動体端末１１－１は続い

てこのアプリケーションを移動体端末１１－１の秘密鍵「ＳＫ－ＭＴ－１」を用いて復号化する（ステップＳ５２０）。

【０１４６】

移動体端末１１－１は上記の処理により、平文となったアプリケーションを、移動体端末１１－１のメモリ１２においてアプリケーションを書き込むべき場所を示す情報とともに取得する。移動体端末１１－１は、受信したアプリケーションを、書き込みべき場所に関する情報により指定されたメモリエリアのアプリケーション領域４０Ａもしくはアプリケーション領域４１Ａに書き込む（ステップＳ５２１）。ここで、受信したアプリケーションに信頼度が添付されている場合には、移動体端末１１－１は、アプリケーションを書き込んだ管理エリア４０における信頼情報領域４０Ｒに、信頼度を書き込む。この際、指定された領域にステップＳ５０６において移動体端末１１－１のユーザが削除を指定したアプリケーションがある場合には、そのアプリケーションは新たなアプリケーションで上書きされる。続いて、移動体端末１１－１は管理サーバ１６に対しアプリケーションの書き込み完了通知を送信する（ステップＳ５２２）。移動体端末１１－１はステップＳ５２２の処理を終えると、ディスプレイ部２１に通常の画面である画面Ｄ２６を表示させる。

【０１４７】

管理サーバ１６はアプリケーションの書き込み完了通知を受信すると、ユーザ情報格納部５３およびアプリケーション情報格納部５２のデータの更新を行う（ステップＳ５２３）。具体的には、まず移動体端末１１のメモリ１２より削除されたアプリケーションがある場合、そのアプリケーションの情報を既配信アプリケーション領域５３Ａから配信可能アプリケーション領域５３Ｂに移動する。次に、新たにメモリ１２に書き込まれたアプリケーションの情報を、配信可能アプリケーション領域５３Ｂから既配信アプリケーション領域５３Ａの対応する場所に移動する。さらに、書き込まれたアプリケーションが一時保管アプリケーション領域５２Ｔに一時的に格納されていたアプリケーションである場合は、一時保管アプリケーション領域５２Ｔからそのアプリケーションを削除する。

【０１４８】

［１．２．４］アプリケーションのアクティベーション

上記のように移動体端末１１がアプリケーションをダウンロードしても、移動体端末１１のユーザがそのアプリケーションを利用するにはアクティベーション処理を行う必要がある。

【０１４９】

アクティベーション処理とは、管理サーバ１６が、ダウンロードされたアプリケーションの利用許可通知を、移動体端末１１のメモリコントローラ３５に対し与える処理である。移動体端末１１のメモリ１２にダウンロードされたアプリケーションが、特にアプリケーションの利用期間に制限のないアプリケーションである場合には、アクティベーション処理はアプリケーションのダウンロード処理の後、引き続き実行される。しかしながら、アプリケーションの利用期間に制限のあるアプリケーション関しては、アプリケーションのダウンロードの後、利用期間が開始されるまでの間はアクティベーション処理は行われず、利用開始期間が訪れた際、アクティベーション処理が行われる。

【０１５０】

例えば、移動体端末１１－１が４月１日より有効な定期乗車券の機能を持つアプリケーションを３月１５日に購入し、そのアプリケーションを３月２０日に移動体端末１１－１にダウンロードした場合、３月２０日から３月３１日までの間は、そのアプリケーションは移動体端末１１－１のメモリ１２に書き込まれているが、利用できない。３月３１日から４月１日に日付が変わる時点で、このアプリケーションに関するアクティベーション処理が行われ、移動体端末１１－１のユーザは４月１日以降にこのアプリケーションを利用することができる。

【０１５１】

ダウンロード処理とアクティベーション処理とを別個に行うことにより、移動体端末１１のユーザは、アプリケーションの有効期限に拘束されることなく望む時間にアプリケー

ションをダウンロードすることができる。また、同じ利用開始日を持つアプリケーションを多くの移動体端末１１が利用する必要がある場合、もし利用開始日にダウンロード処理を行う必要があれば、多くの人が一斉にそれらのアプリケーションをダウンロードするため、管理サーバ１６、コンテンツサーバ２０、および移動体端末１１の間の通信経路において、データの輻輳を引き起こしやすい。しかしながら、アクティベーション処理におけるデータ通信量はダウンロード処理におけるデータ通信量と比較して極めて小さいため、上記のような場合において、各移動体端末１１のユーザがダウンロード処理をアクティベーション処理に先んじて自由な時間に行っておくことにより、アプリケーションの利用開始日に通信経路におけるデータの輻輳の発生を抑制することができる。以下にアクティベーション処理の流れを説明する。

【０１５２】

アクティベーション処理が発生するのは、利用期間に制限のないアプリケーションが移動体端末１１－１にダウンロードされた場合、既に移動体端末１１－１にダウンロードされているアプリケーションに対し利用開始の時期が訪れた場合、もしくはアプリケーションの配信元であるコンテンツサーバ２０からアクティベーションの指示が管理サーバ１６に対しなされた場合などである。以下に例として、移動体端末１１－１の管理エリア４０－１に書き込まれているアプリケーションに対し、アクティベーション処理が行われる場合の処理の流れを説明する。

【０１５３】

まず、管理サーバ１６は移動体端末１１－１に対しアクティベーション命令を送信する。このアクティベーション命令には、メモリ１２における対象のアプリケーションの特定情報として、管理エリア４０－１の識別番号が含まれている。

【０１５４】

移動体端末１１－１の通信部３４はアクティベーション命令を受信すると、その命令をメモリコントローラ３５に送る。メモリコントローラ３５は、このアクティベーション命令を受信するまでの間、管理エリア４０－１のアプリケーション領域４０Ａ－１およびデータ領域４０Ｄ－１内のアプリケーションやデータに対する、移動体端末１１－１の制御部３１による利用要求を全て拒否する。従って、その間、移動体端末１１－１のユーザは管理エリア４０－１のアプリケーションを利用することができない。

【０１５５】

これに対し、メモリコントローラ３５がアクティベーション命令を受信した後は、管理エリア４０－１のアプリケーション領域４０Ａ－１およびデータ領域４０Ｄ－１内のアプリケーションやデータに対する、制御部３１の利用要求を受信すると、メモリコントローラ３５はまず、管理エリア４０－１の信頼情報領域４０Ｒ－１に書き込まれている信頼度を読み出す。続いて、メモリコントローラ３５は利用要求と共に制御部３１から送信される、利用要求元のプログラムの信頼度と、信頼情報領域４０Ｒ－１から読み出した信頼度とを比較する。そして、メモリコントローラ３５は、利用要求元のプログラムの信頼度が信頼情報領域４０Ｒ－１から読み出した信頼度より高い場合、もしくは２つの信頼度が等しい場合にのみ、利用要求に従った処理を行う。この信頼度を用いた制御処理については、既に移動体端末１１の構成におけるメモリコントローラ３５の機能説明において述べたとおりである。

【０１５６】

管理サーバ１６は、アクティベーション命令を移動体端末１１－１に送信した後、ユーザ情報格納部５３－１における既配信アプリケーション領域５３Ａのアクティベーションに関する項目を「Ｙｅｓ」に更新する。続いて、管理サーバ１６は、登録アプリケーション領域５２Ｒのデータを読み出し、アクティベーション処理の対象のアプリケーションの料金徴収に関する項目が「Ｙｅｓ」である場合には、アプリケーションの識別番号、移動体端末１１－１の識別番号、アクティベーション処理のなされた日時等の情報を課金管理サーバに送信する。

【０１５７】

一方、移動体端末１１－１は新たにアクティベーション命令を受信した場合、ディスプレイ部２１に「α」を表示させ、移動体端末１１－１のユーザに新たなアプリケーションが利用可能となったことを知らせる（図２６、画面Ｄ３１）。なおこの「α」の文字は、先に説明したアプリケーション購入処理の完了通知と区別するために「β」等の他の文字や、図形、音、振動等の他の方法を用いてもよい。

【０１５８】

以上がアクティベーション処理である。なお、移動体端末１１－１のユーザがアクティベーション処理が行われたアプリケーションを起動する場合、まず移動体端末１１－１のユーザは、アプリボタン２３を押下し、アプリケーションメニューを表示させる（画面Ｄ３２）。続いて、移動体端末１１－１のユーザはボタン「３」を押下することにより「３．アプリケーションの起動」を指定し、利用可能なアプリケーションの選択画面を表示させる（画面Ｄ３３）。アプリケーションの選択画面において、移動体端末１１－１が例えばボタン「１」を押下し、「１．スケジュール管理　Ｖｅｒ．２」を選択すると、選択されたアプリケーションが起動される（画面Ｄ３４）。

【０１５９】

［１．２．５］アプリケーションのディアクティベーション

移動体端末１１－１において、既にアクティベーション処理が行われたアプリケーションに対し、その利用を一時的に停止させる必要が生じる場合がある。例えば、移動体端末１１－１が紛失もしくは盗難に遭った場合には、移動体端末１１－１のユーザの要求により、移動体端末１１－１にダウンロードされている全てのアプリケーションの利用を禁止する必要がある。また、移動体端末１１－１のユーザによりアプリケーションの利用料金が滞納された場合や移動体端末１１－１のユーザによる利用条件違反があった場合、コンテンツサーバ２０－１もしくは管理サーバ１６の管理事業者の要求により、移動体端末１１－１にダウンロードされている特定のアプリケーションに関し、利用を一時的に停止させる必要がある。

【０１６０】

上記のような場合、ディアクティベーション処理が行われる。以下に例として、移動体端末１１－１の管理エリア４０－１に書き込まれているアプリケーションに対し、ディアクティベーション処理が行われる場合の処理の流れを説明する。

【０１６１】

まず、管理サーバ１６は移動体端末１１－１に対しディアクティベーション命令を送信する。このディアクティベーション命令には、メモリ１２における対象のアプリケーションの特定情報として、管理エリア４０－１の識別番号が含まれている。

【０１６２】

移動体端末１１－１の通信部３４はディアクティベーション命令を受信すると、その命令をメモリコントローラ３５に送る。メモリコントローラ３５は、このディアクティベーション命令を受信すると、それ以降、管理エリア４０－１のアプリケーション領域４０Ａ－１およびデータ領域４０Ｄ－１内のアプリケーションやデータに対する、移動体端末１１－１の制御部３１による利用要求を全て拒否する。従って、移動体端末１１－１のユーザは管理エリア４０－１のアプリケーションを利用することができなくなる。

【０１６３】

管理サーバ１６はディアクティベーション命令を移動体端末１１－１に送信した後、ユーザ情報格納部５３－１における既配信アプリケーション領域５３Ａのアクティベーションに関する項目を「Ｎｏ」に更新する。続いて、管理サーバ１６は、登録アプリケーション領域５２Ｒのデータを読み出し、ディアクティベーション処理の対象のアプリケーションの料金徴収に関する項目が「Ｙｅｓ」である場合には、アプリケーションの識別番号、移動体端末１１－１の識別番号、ディアクティベーション処理のなされた日時等の情報を課金管理サーバに送信する。

【０１６４】

以上がディアクティベーション処理である。移動体端末１１－１はディアクティベーシ

ョン命令を受信した場合、利用可能なアプリケーションの選択画面において該当するアプリケーションの名称を表示しなくなる。なお、一度ディアクティベーション処理のされたアプリケーションを再度利用したい場合には、既に説明したアクティベーション処理を行う。例えば、紛失していた移動体端末１１－１が見つかったり、移動体端末１１－１のユーザによるアプリケーションの利用料金の滞納が解消したりした際、再度アクティベーション処理が行われるが、その場合、既に移動体端末１１－１のメモリ１２にダウンロードされていたアプリケーションやそのアプリケーションが管理していたデータはディアクティベーション処理のされた時点の状態で、再度利用可能となる。

【０１６５】

［１．２．６］アプリケーションの削除

移動体端末１１－１において、アプリケーションの利用を完全に中止させる必要が生じる場合がある。例えば、移動体端末１１－１のユーザがアプリケーションの購入契約を解約する場合、予め定められていたアプリケーションの利用可能期間が満了した場合、移動体端末１１－１のユーザが深刻なアプリケーションの利用条件違反を行った場合などである。そのような場合、以下の削除処理によって、アプリケーションを移動体端末１１－１のメモリ１２から削除すると同時に、ユーザ情報格納部５３－１の配信可能アプリケーション領域５３Ｂからも、削除対象のアプリケーションに関するデータを削除する。以下に例として、移動体端末１１－１の管理エリア４０－１に書き込まれているアプリケーションに対し、削除処理が行われる場合の処理の流れを説明する。

【０１６６】

まず、管理サーバ１６はユーザ情報格納部５３－１の既配信アプリケーション領域５３Ａのデータを読み出し、削除の対象となるアプリケーションが移動体端末１１－１のメモリ１２に書き込まれているかどうかを確認する。

【０１６７】

対象のアプリケーションが移動体端末１１－１のメモリ１２に書き込まれている場合、管理サーバ１６は移動体端末１１－１に対し削除命令を送信する。この削除命令には、対象のアプリケーションの特定情報として、管理エリア４０－１の識別番号が含まれている。移動体端末１１－１の通信部３４は削除命令を受信すると、その命令をメモリコントローラ３５に送る。メモリコントローラ３５は削除命令を受信すると、識別番号により指定された管理エリア４０－１内のアプリケーションおよびデータを消去する。移動体端末１１－１のメモリコントローラ３５はこの消去処理を終えると、管理サーバ１６に対し消去完了通知を送信する。管理サーバ１６は消去完了通知を受信すると、ユーザ情報格納部５３－１における既配信アプリケーション領域５３Ａから、該当するアプリケーションの情報を削除する。

【０１６８】

一方、対象のアプリケーションが移動体端末１１－１のメモリ１２に書き込まれていない場合、管理サーバ１６はユーザ情報格納部５３－１における配信可能アプリケーション領域５３Ｂから、該当するアプリケーションの情報を削除する。

【０１６９】

続いて、管理サーバ１６は登録アプリケーション領域５２Ｒのデータを読み出し、対象のアプリケーションの料金徴収に関する項目が「Ｙｅｓ」である場合には、アプリケーションの識別番号、移動体端末１１－１の識別番号、削除処理のなされた日時等の情報を課金管理サーバに送信する。

【０１７０】

以上が削除処理である。この削除処理により、移動体端末１１－１の利用可能なアプリケーションの選択画面およびダウンロード可能なアプリケーションの表示画面において、該当するアプリケーションの名称は表示されなくなる。

【０１７１】

［１．３］信頼度を用いたアプリケーション間の連係

続いて、信頼度を用いたアプリケーション間の連係方法について、具体例を用いて説明

する。
【０１７２】
既に説明したように、移動体端末１１－１のメモリ１２には複数のアプリケーションが書き込まれるが、管理エリア４０に書き込まれているアプリケーションに関しては、信頼情報領域４０Ｒに、それぞれのアプリケーションに対して与えられている信頼度が、「１」から「５」までの数値で格納されている。信頼度はその数値が大きいほど信頼性が高いことを示し、信頼度が高いアプリケーションは信頼度が低いアプリケーションの機能や、信頼度が低いアプリケーションの管理するデータを利用することが可能であるが、信頼度が低いアプリケーションからは信頼度の高いアプリケーションの機能や、信頼度が高いアプリケーションの管理するデータを利用することはできない。なお、移動体端末１１の制御部３１が管理し、制御用メモリ３２に書き込まれている制御用プログラムに関しては、信頼度「５」が与えられている。一方、フリーエリア４１に書き込まれているアプリケーションに関しては、信頼度は与えられておらず、フリーエリア４１に書き込まれているアプリケーションと他のプログラムとの信頼度の比較を行う必要がある場合には、フリーエリア４１に書き込まれているアプリケーションには信頼度として「０」が適用される。
【０１７３】
［１．３．１］アプリケーション間の連係が許可されない場合
以下に説明する例は、信頼度が低いアプリケーションから信頼度が高いアプリケーションの機能の呼び出しおよびデータの利用を行うことができないことを示す例である。なお、以下の説明には図２７、図２８、図２９、図３０、および図３１を用いる。
【０１７４】
まず、移動体端末１１－１の管理エリア４０－１におけるアプリケーション領域４０Ａに、定期乗車券機能を持ったアプリケーション（以下、「定期券アプリケーション」と呼ぶ）が書き込まれており、アクティベーション処理がなされ利用可能となっている。定期券アプリケーションを用いると、移動体端末１１－１のユーザは「ａｂｃ鉄道」のホームページを開き、そのホームページにおいて時刻表を閲覧したり、定期乗車券の購入を行ったりすることができる。なお、定期乗車券を購入した場合、例えば移動体端末１１－１が「ａｂｃ鉄道」の改札機に近づくと、改札機より発信されている電波信号に応じて移動体端末１１－１からは所定の信号が発信され、改札機がゲートを開くようになっており、移動体端末１１－１自体が定期乗車券の役割をする。この定期券アプリケーションの信頼度は「３」である。
【０１７５】
一方、管理エリア４０－２におけるアプリケーション領域４０Ａには、代金決済機能を持ったアプリケーション（以下、「決済アプリケーション」と呼ぶ）が書き込まれており、アクティベーション処理がなされ利用可能となっている。決済アプリケーションを用いると、移動体端末１１－１のユーザは「ｘｘ銀行」のホームページを開き、そのホームページにおいて移動体端末１１－１のユーザの保有する口座から任意の口座に送金を行うことができる。この決済アプリケーションの信頼度は「５」である。
【０１７６】
移動体端末１１－１のユーザは、アプリボタン２３を押下し、アプリケーションメニュー（画面Ｄ４１）をディスプレイ部２１に表示させる。続いて、ユーザは画面Ｄ４１においてボタン「３」を押下し、起動するアプリケーションの選択画面（画面Ｄ４２）を表示する。ユーザは画面Ｄ４２においてボタン「１」を押下し、定期券アプリケーションを選択する。移動体端末１１－１は定期券アプリケーションを起動し、定期券アプリケーションは「ａｂｃ鉄道」のホームページを開く（画面Ｄ４３）。
【０１７７】
画面Ｄ４３において、ユーザがボタン「３」を押下して「３．定期乗車券購入」を選択すると、移動体端末１１－１は画面Ｄ４４を表示する。画面Ｄ４４において、ユーザは購入する定期乗車券の利用区間および利用期間を操作部２２を用いて入力し、ボタン「９」を押下して「ａｂｃ鉄道」のホームページに対し、購入指示を送信する。

【０１７８】
ここで、定期券アプリケーションは移動体端末１１－１のメモリ１２の他のアプリケーションの中で代金決済を行うことのできるアプリケーションを検索する。より具体的には、定期券アプリケーションを実行している制御部３１は、定期券アプリケーションの書き込まれている管理エリア４０－１の識別番号と共に、他の管理エリア４０およびフリーエリア４１に書き込まれているアプリケーションに対する読み取り要求を、メモリコントローラ３５に対し送信する。
【０１７９】
メモリコントローラ３５は、各管理エリア４０およびフリーエリア４１に対する制御部３１からの読み取り要求を受信すると、まず制御部３１から読み取り要求と共に送信された管理エリア４０－１の識別情報を用いて、管理エリア４０－１の信頼情報領域４０Ｒから信頼度を読み出す。この場合、読み出される信頼度は「３」である。以下、これを「要求元信頼度」と呼ぶ。
【０１８０】
続いて、メモリコントローラ３５は、読み取り要求の対象となっている管理エリア４０－２、管理エリア４０－３、・・・、管理エリア４０－ｎのそれぞれに関して、信頼情報領域４０Ｒから信頼度を読み出す。また、フリーエリア４０－１、フリーエリア４０－１、・・・、フリーエリア４０－ｍに関しては、信頼度は与えられていないため、信頼度は「０」として扱われる。このようにして得られる信頼度を、以下、「要求先信頼度」と呼ぶ。
【０１８１】
続いて、メモリコントローラ３５は、要求元信頼度と各要求先信頼度とを比較し、要求元信頼度が要求先信頼度より高いか等しい場合、すなわち要求先信頼度が「３」以下である場合に限り、読み取り要求を実行し、それ以外の場合に関しては、制御部３１に対し読み取り要求の拒否通知を送信する。
【０１８２】
ここで、管理エリア４０－２には代金決済の可能な決済アプリケーションがあるが、その要求先信頼度は「５」であるため、メモリコントローラ３５は定期券アプリケーションからの決済アプリケーションに対する読み取り要求を拒否する。その結果、定期券アプリケーションは決済アプリケーションの存在を認識できない。従って、定期券アプリケーションはメモリ１２内に代金決済を行うことのできるアプリケーションを見つけることができず、移動体端末１１－１は画面Ｄ４５を表示する。画面Ｄ４５において、ユーザは別途代金の送金手続を行うよう要求される。ユーザは画面Ｄ４５の情報をメモ用紙等に書き取った後、ボタン「９」を押下して定期券アプリケーションを終了させる。その結果、ディスプレイ部２１には通常画面である画面Ｄ４６が表示される。
【０１８３】
続いて、ユーザは画面Ｄ４６において、再度アプリボタン２３を押下し、アプリケーションメニュー（画面Ｄ４７）を表示させる。ユーザは画面Ｄ４７においてボタン「３」を押下し、起動するアプリケーションの選択画面（画面Ｄ４８）を表示する。ユーザは画面Ｄ４８においてボタン「２」を押下し、決済アプリケーションを選択する。移動体端末１１－１は決済アプリケーションを起動し、決済アプリケーションは「ｘｘ銀行」のホームページを開く（画面Ｄ４９）。
【０１８４】
画面Ｄ４９において、ユーザは暗証番号を入力し、処理の選択画面である画面Ｄ５０を表示させる。画面Ｄ５０において、ユーザはボタン「３」を押下して、「３．送金」を選択し、画面Ｄ５１を表示させる。画面Ｄ５１において、ユーザは先に書き取った「ａｂｃ鉄道」への送金情報を入力し、ボタン「９」を押下して送金情報を「ｘｘ銀行」のホームページに対し送信する。「ｘｘ銀行」は、この送金情報をホームページ経由で移動体端末１１－１から受信し、指定された送金処理を「ａｂｃ鉄道」の口座に対して行った後、移動体端末１１－１のディスプレイ部２１に画面Ｄ５２を表示させる。一方、「ａｂｃ鉄道

」は「ｘｘ銀行」からの送金を確認し、移動体端末１１－１による定期乗車券購入の処理を完了し、移動体端末１１－１に関する購入履歴情報を更新する。

【０１８５】

画面Ｄ５２において、ボタン「９」が押下されると、移動体端末１１－１は通常の画面である画面Ｄ５３を表示する。続いて、ユーザは画面Ｄ５３において、再度アプリボタン２３を押下し、アプリケーションメニュー（画面Ｄ５４）を表示させる。ユーザは画面Ｄ５４においてボタン「３」を押下し、起動するアプリケーションの選択画面（画面Ｄ５５）を表示する。ユーザは画面Ｄ５５においてボタン「１」を押下し、定期券アプリケーションを起動する（画面Ｄ５６）。

【０１８６】

画面Ｄ５６において、ユーザがボタン「４」を押下して「４．購入履歴閲覧」を選択すると、移動体端末１１－１は画面Ｄ５７を表示する。画面Ｄ５７において、ユーザがボタン「１」を押下すると、移動体端末１１－１は、先に購入した定期乗車券の購入履歴明細を表示する（画面Ｄ５８）。ユーザは画面Ｄ５８において、先に購入した定期乗車券に対する送金が「ａｂｃ鉄道」により確認され、定期乗車券の購入処理が無事完了したことを確認する。その後、ユーザがボタン「９」を押下すると、移動体端末１１－１はディスプレイ部２１に通常の画面である画面Ｄ５９を表示させる。

【０１８７】

［１．３．２］アプリケーション間の連係が許可される場合

以下に説明する例は、信頼度が高いアプリケーションから信頼度が低いアプリケーションもしくは信頼度が同じアプリケーションの機能の呼び出しおよびデータの利用を行うことができることを示す例である。なお、以下の説明には図３２、図３３、および図３４を用いる。

【０１８８】

まず、移動体端末１１－１の管理エリア４０－１におけるアプリケーション領域４０Ａに、通信販売機能を持つアプリケーション（以下、「通信販売アプリケーション」と呼ぶ）が書き込まれており、アクティベーション処理がなされ利用可能となっている。通信販売アプリケーションを用いると、移動体端末１１－１のユーザは「サイバー商店ｚｚ」のホームページを開き、そのホームページにおいて商品を購入することができる。この通信販売アプリケーションの信頼度は「４」である。

【０１８９】

一方、管理エリア４０－２におけるアプリケーション領域４０Ａには、先の例と同様に、決済アプリケーションが書き込まれており、アクティベーション処理がなされ利用可能となっている。以下、この決済アプリケーションを「決済アプリケーション１」と呼ぶ。決済アプリケーション１の信頼度は「４」である。

【０１９０】

また、管理エリア４０－３におけるアプリケーション領域４０Ａには、クレジットカードによる代金決済機能を持つアプリケーション（以下、「クレジットアプリケーション」と呼ぶ）が書き込まれており、アクティベーション処理がなされ利用可能となっている。クレジットアプリケーションを用いると、移動体端末１１－１のユーザは「ｃｃ信販」のホームページを開き、そのホームページにおいてクレジットカードによる代金決済の手続を行うことができる。このクレジットアプリケーションの信頼度は「４」である。

【０１９１】

また、管理エリア４０－４におけるアプリケーション領域４０Ａには、決済アプリケーション１と同様の機能を持つが、「ｘｘ銀行」ではなく、「ｋｋ銀行」のホームページを開き、送金等の処理を行うことができるアプリケーションが書き込まれており、アクティベーション処理がなされ利用可能となっている。以下、この決済アプリケーションを「決済アプリケーション２」と呼ぶ。決済アプリケーション２の信頼度は「５」である。

【０１９２】

移動体端末１１－１のユーザは、アプリボタン２３を押下し、アプリケーションメニュ

ー（画面Ｄ７１）をディスプレイ部２１に表示させる。続いて、ユーザは画面Ｄ７１においてボタン「３」を押下し、起動するアプリケーションの選択画面（画面Ｄ７２）を表示する。ユーザは画面Ｄ７２においてボタン「１」を押下し、通信販売アプリケーションを選択する。移動体端末１１－１は通信販売アプリケーションを起動し、通信販売アプリケーションは「サイバー商店ｚｚ」のホームページを開く（画面Ｄ７３）。

【０１９３】

画面Ｄ７３において、ユーザがボタン「２」を押下して牛肉の購入を選択すると、通信販売アプリケーションは、続いて購入申込のされた商品の配送先の入力画面を表示する（画面Ｄ７４）。画面Ｄ７４において、ユーザが購入する商品の配送先を入力し、ボタン「９」を押下すると、通信販売アプリケーションは移動体端末１１－１のメモリ１２の他のアプリケーションの中で代金決済を行うことのできるアプリケーションを検索する。なお、以下の説明のため、ユーザは商品の配送先として、「東京都新宿区１－１－１」を入力したものとする。代金決済を行うことのできるアプリケーションの検索処理の具体的な流れは、定期券アプリケーションの例において説明したものと同様である。

【０１９４】

代金決済を行うことのできるアプリケーションの検索処理において、通信販売アプリケーションによるメモリ１２の他のアプリケーションの読み取り要求が行われる際、要求元である通信販売アプリケーションの信頼度は「４」である。一方、この読み取り要求の要求先の一つである決済アプリケーション１の信頼度は「４」であるため、メモリコントローラ３５は通信販売アプリケーションからの決済アプリケーション１に対する読み取り要求を承諾し、決済アプリケーション１の機能情報を通信販売アプリケーションを実行している制御部３１に送信する。同様に、クレジットアプリケーションの信頼度も「４」であるため、メモリコントローラ３５はクレジットアプリケーションの機能情報を制御部３１に送信する。それに対し、決済アプリケーション２の信頼度は「５」であり、要求元の通信販売アプリケーションの信頼度「４」よりも高いため、メモリコントローラ３５は制御部３１の決済アプリケーション２に対する読み取り要求を拒否し、通信販売アプリケーションには決済アプリケーション２の機能情報が送信されない。その結果、通信販売アプリケーションは、代金決済を行うことができるアプリケーションとして、決済アプリケーション１およびクレジットアプリケーションの２つが利用可能である、と判断し、画面Ｄ７５を表示する。

【０１９５】

画面Ｄ７５において、ユーザが代金決済の方法として決済アプリケーション１を利用することを選び、ボタン「１」を押下すると、通信販売アプリケーションはメモリコントローラ３５に対して、決済アプリケーション１の読み取り要求を送信する。また、通信販売アプリケーションは決済アプリケーション１に対し、決済アプリケーション１を読み出す目的およびその目的を実行するために必要な情報を渡す。より具体的には、通信販売アプリケーションを実行している制御部３１は、メモリコントローラ３５に対し、決済アプリケーション１が管理している管理エリア４０－２のデータ領域４０Ｄ－２に、読み出しの目的が「サイバー商店ｘｘ」における牛肉１ｋｇの購入に対する５，０００円の送金であり、送金先が「ｎｎ銀行」の口座番号が「４１２５６３７８」である「普通口座」であり、購入商品の配送先が「東京都新宿区１－１－１」である、という情報の書き込み要求を送信する。

【０１９６】

メモリコントローラ３５はアプリケーション読み出しおよびデータ書き込みの要求元信頼度と要求先信頼度の比較を行い、アプリケーションの読み出しとデータの書き込みを承諾する。その結果、制御部３１は決済アプリケーション１を起動する。

続いて、決済アプリケーション１は画面Ｄ７６を表示し、移動体端末１１－１のユーザに本人確認のための暗証番号の入力を求める。画面Ｄ７６において、移動体端末１１－１のユーザが正しい暗証番号を入力すると、決済アプリケーション１は画面Ｄ７７を表示する。この際、送金に必要な情報は、決済アプリケーション１により管理エリア４０－２の

データ領域４０Ｄ－２より読み出され、既に画面Ｄ７７に入力されている。従って、ユーザがそれらの情報を入力する必要はない。

【０１９７】

画面Ｄ７７において、ユーザが送金情報を確認し、ボタン「９」を押下すると、決済アプリケーション１は「ｘｘ銀行」のホームページに対して送金依頼を送信する。その際、決済アプリケーション１は購入商品情報および購入商品の配送先情報も「ｘｘ銀行」のホームページに対し送信する。

【０１９８】

「ｘｘ銀行」は、ホームページを介して移動体端末１１－１から送金依頼、購入商品情報、および購入商品の配送先情報を受信すると、「サイバー商店ｚｚ」に対して指定された送金を行うとともに、「サイバー商店ｚｚ」に対して、購入商品情報および購入商品の配送先情報も送信する。「サイバー商店ｚｚ」は「ｘｘ銀行」からの送金を確認するとともに、その送金により牛肉１ｋｇの購入がなされ、その牛肉１ｋｇの配送先が「東京都新宿区１－１－１」である、という情報を受け取る。その結果、「サイバー商店ｚｚ」は購入された商品の配送処理を行うとともに、移動体端末１１－１に対して、商品の配送日および注文番号とともに、入金確認通知を送信する。

【０１９９】

移動体端末１１－１の制御部３１において実行されている決済アプリケーション１は、「サイバー商店ｚｚ」より入金確認通知を受信すると、メモリコントローラ３５に対し、決済アプリケーション１の呼び出し元である通信販売アプリケーションの読み出しと、通信販売アプリケーションが管理しているデータ領域４０Ｄ－１への、商品の配送日および注文番号に関するデータの書き込みの要求を行う。この場合においても、メモリコントローラ３５は要求元信頼度と要求先信頼度の比較を行い、これらの要求を承諾する。その結果、制御部３１は処理途中で待機していた通信販売アプリケーションを再度起動し、通信販売アプリケーションはデータ領域４０Ｄ－１に書き込まれた商品の配送日および注文番号に関するデータを読み出し、画面Ｄ７８を表示する。画面Ｄ７８において、ユーザが「サイバー商店ｚｚ」からの送信確認の内容を確認し、ボタン「９」を押下すると、移動体端末１１－１は通常の画面である画面Ｄ７９を表示し、処理を終了する。

【０２００】

このように、信頼度の高いアプリケーションは金銭情報や個人情報のような価値の高い情報を直接、他のアプリケーションから受け取ったり、価値の高い情報を扱う他のアプリケーションの機能を呼び出したりすることができる。また、信頼度が「５」であるアプリケーションであれば、制御用メモリ３２に格納されている制御用プログラムを呼び出したり、それらのプログラムが管理しているデータを利用することもできる。従って、ユーザの操作は簡便化される。しかしながら、既に説明したように、アプリケーションが高い信頼度を得るには管理サーバ１６の管理事業者による審査が必要であり、また信頼度の与えられたアプリケーションに関しては、管理サーバ１６の管理事業者により、必要に応じてアプリケーションの改竄がないことが確認されているため、ユーザは安心して価値の高い情報を扱うアプリケーションを利用することができる。

【０２０１】

［２］第２実施形態

第２実施形態は、上述した第１実施形態と比較し、以下に説明するように第１実施形態における信頼度の代わりに信頼関係情報を用いる点が異なっている。その他の点に関しては全て第１実施形態と同様である。従って、以下の説明においては第２実施形態が第１実施形態と異なる点のみを説明する。また、以下の説明においては、各構成要素を特定するために、第１実施形態において用いた名称および符号をそのまま用いる。

【０２０２】

［２．１］権限情報の構成および機能

第２実施形態において、コンテンツサーバ２０により管理サーバ１６の管理事業者に対しアプリケーションの内容審査の依頼がなされた場合、管理サーバ１６の管理事業者は新

たに内容審査を行ったアプリケーションと、既に内容審査が行われているアプリケーションのそれぞれとの間に、アプリケーションの読み取り、データの読み取り、データの書き込み、およびデータの削除についての権限を設定する。

【０２０３】

以下、識別番号が「ＡＰ－３５６８」であるアプリケーションに関し、新たに内容審査が行われた場合を例とし、具体例を説明する。また、例えば識別番号が「ＡＰ－３５６８」であるアプリケーションを呼ぶ際には、アプリケーション「ＡＰ－３５６８」と呼ぶ。図３５はアプリケーション「ＡＰ－３５６８」に関して与えられた権限を示すデータ例である。なお、以下の説明では図３５に示す形式のデータを「権限情報」と呼ぶ。

【０２０４】

図３５の第１列は、アプリケーション「ＡＰ－３５６８」が読み取りを許可されているアプリケーションのリストである。例えば、アプリケーション「ＡＰ－３５６８」を実行している制御部３１が、アプリケーション「ＡＰ－３７１２」の機能を利用したい場合、制御部３１はメモリコントローラ３５に対し、アプリケーション「ＡＰ－３７１２」の読み取り要求を送信する。アプリケーション「ＡＰ－３７１２」はアプリケーション「ＡＰ－３５６８」に対応した権限情報の第１列に含まれている。従って、メモリコントローラ３５はアプリケーション「ＡＰ－３７１２」の読み取り要求を受信すると、その読み取り要求を承諾する。そして、メモリコントローラ３５はこの読み取り要求を承諾すると、管理エリア４０のアプリケーション領域４０Ａからアプリケーション「ＡＰ－３７１２」を読み出し、読み出したアプリケーションを制御部３１に対し送信する。

【０２０５】

また、図３５の第２列は、アプリケーション「ＡＰ－３５６８」がデータの読み取りを許可されているアプリケーションのリストである。例えば、アプリケーション「ＡＰ－３５６８」を実行している制御部３１が、アプリケーション「ＡＰ－８１２５」の管理するデータの読み取りを行いたい場合、制御部３１はメモリコントローラ３５に対し、アプリケーション「ＡＰ－８１２５」の管理するデータの読み取り要求を送信する。ここで、アプリケーション「ＡＰ－８１２５」はアプリケーション「ＡＰ－３５６８」の権限情報の第２列に含まれている。従って、メモリコントローラ３５はアプリケーション「ＡＰ－８１２５」の管理するデータの読み取り要求を受信すると、その読み取り要求を承諾する。そして、メモリコントローラ３５は読み取り要求を承諾すると、アプリケーション「ＡＰ－８１２５」が格納されている管理エリア４０のデータ領域４０Ｄから要求されたデータを読み出し、読み出したデータを制御部３１に対し送信する。

図３５の第３列および第４列は、それぞれ、アプリケーション「ＡＰ－３５６８」が、データの書き込みを許可されているアプリケーションのリスト、およびデータの削除を許可されているアプリケーションのリストである。

【０２０６】

一方、図３５の第５列は、アプリケーション「ＡＰ－３５６８」を読み取ることが許可されているアプリケーションのリストである。例えば、アプリケーション「ＡＰ－４３１５」を実行している制御部３１が、アプリケーション「ＡＰ－３５６８」の機能を利用したい場合、制御部３１はメモリコントローラ３５に対し、アプリケーション「ＡＰ－３５６８」の読み取り要求を送信する。ここで、アプリケーション「ＡＰ－４３１５」はアプリケーション「ＡＰ－３５６８」の権限情報の第５列に含まれている。従って、メモリコントローラ３５はアプリケーション「ＡＰ－４３１５」によるアプリケーション「ＡＰ－３５６８」の読み取り要求を受信すると、その読み取り要求を承諾する。そして、メモリコントローラ３５は読み取り要求を承諾すると、管理エリア４０のアプリケーション領域４０Ａからアプリケーション「ＡＰ－３５６８」を読み出し、読み出したアプリケーションを制御部３１に対し送信する。

【０２０７】

同様に、権限情報の第６列、第７列、および第８列は、それぞれ、アプリケーション「ＡＰ－３５６８」が管理するデータを、読み取ることが許可されているアプリケーション

のリスト、書き込むことが許可されているアプリケーションの一覧、および削除することが許可されているアプリケーションのリストである。

【０２０８】

［２．２］信頼関係情報の登録および更新

管理サーバ１６のアプリケーション情報格納部５２の登録アプリケーション領域５２Ｒには、図３６に示すように、第１実施形態における信頼度の項目の代わりに、信頼関係情報の項目が設けられている。管理サーバ１６の管理事業者は、新たにアプリケーション「ＡＰ－３５６８」の内容審査を行うと、図３５に示した権限情報を管理サーバ１６に入力する。管理サーバ１６は、権限情報が入力されると、登録アプリケーション領域５２Ｒにアプリケーション「ＡＰ－３５６８」に対応するデータを新たに作成し、その信頼関係情報に関する項目に、権限情報の第５列から第８列までを格納する。

【０２０９】

続いて、管理サーバ１６は、権限情報の第１列から第４列のそれぞれに含まれる全てのアプリケーションに関し、登録アプリケーション領域５２Ｒにおいて対応するデータの信頼関係情報に関する項目を更新する。例えば、アプリケーション「ＡＰ－３７１２」はアプリケーション「ＡＰ－３５６８」の権限情報の第１列に含まれているので、管理サーバ１６は登録アプリケーション領域５２Ｒにおけるアプリケーション「ＡＰ－３７１２」に対応するデータの信頼関係情報に関する項目の、アプリケーション読み取りの項目に、アプリケーション「ＡＰ－３５６８」を追加する。

【０２１０】

次に、管理サーバ１６は、ユーザ情報格納部５３－１、ユーザ情報格納部５３－２、・・・、ユーザ情報格納部５３－ｋの既配信アプリケーション領域５３Ａのデータを読み出し、上記において信頼関係情報が更新されたアプリケーション、すなわちアプリケーション「ＡＰ－３５６８」の権限情報の第１列から第４列に含まれるアプリケーションの識別番号を含むユーザ情報格納部５３を、アプリケーション「ＡＰ－３５６８」の権限情報の各列ごとに抽出する。続いて管理サーバ１６は、抽出されたユーザ情報格納部５３の信頼関係情報の対応する項目に、アプリケーション「ＡＰ－３５６８」を追加する。その後、管理サーバ１６は、アプリケーション「ＡＰ－３５６８」の追加を行ったユーザ情報格納部５３に対応する移動体端末１１に対し、ユーザ情報格納部５３における信頼関係情報の対応する項目にアプリケーション「ＡＰ－３５６８」が追加されたことを通知する。例えば、ユーザ情報格納部５３－１のデータ例を示す図７によれば、移動体端末１１－１はメモリ１２の管理エリア４０－２のアプリケーション領域４０Ａ－２にアプリケーション「ＡＰ－０１２３」を書き込んでいる。アプリケーション「ＡＰ－０１２３」は図３５に示した権限情報の第１列に含まれ、新たに内容審査の行われたアプリケーション「ＡＰ－３５６８」にはアプリケーション「ＡＰ－０１２３」に対するアプリケーションの読み取り権限が与えられている。従って、管理サーバ１６は移動体端末１１－１に対し、ユーザ情報格納部５３－１のアプリケーション「ＡＰ－０１２３」の信頼関係情報のアプリケーション読み取りに関する項目に、新たにアプリケーション「ＡＰ－３５６８」が追加されたことを通知する。

【０２１１】

各移動体端末１１においては、内容審査の行われているアプリケーションをメモリ１２にダウンロードする場合、アプリケーションとともに対応する信頼関係情報が添付されてダウンロードされる。移動体端末１１のメモリコントローラ３５は、ダウンロードしたアプリケーションに添付されている信頼関係情報を、アプリケーションを書き込む管理エリア４０の信頼情報領域４０Ｒに書き込む。

【０２１２】

従って、例えば移動体端末１１－１が、先に示した例のように管理サーバ１６より、ユーザ情報格納部５３－１のアプリケーション「ＡＰ－０１２３」の信頼関係情報のアプリケーション読み取りに関する項目に、新たにアプリケーション「ＡＰ－３５６８」が追加されたことに関する通知を受信すると、移動体端末１１－１のメモリコントローラ３５は

、アプリケーション「ＡＰ－０１２３」が書き込まれている管理エリア４０－２の信頼情報領域４０Ｒ－２のデータにおける、アプリケーション読み取りの項目に、アプリケーション「ＡＰ－３５６８」を追加する。

【０２１３】

以上の処理により、アプリケーション情報格納部５２の登録アプリケーション領域５２Ｒ、および各移動体端末１１における管理エリア４０の信頼情報領域４０Ｒのデータは常に最新のものに更新される。

【０２１４】

［２．３］信頼関係情報を用いたアプリケーション連係動作の制御

各移動体端末１１において、あるアプリケーションが他のアプリケーションの機能を利用したり、他のアプリケーションの管理するデータを利用する場合には、制御部３１は処理要求と共に、処理の要求先のアプリケーションの書き込まれているメモリエリアの識別番号（以下、「要求先エリア番号」と呼ぶ）、および処理の要求元のアプリケーションの識別番号をメモリコントローラ３５に送信する。

【０２１５】

要求先エリア番号により指定されたメモリエリアが管理エリア４０である場合、メモリコントローラ３５は制御部３１より処理要求を受信すると、その管理エリア４０の信頼情報領域４０Ｒから信頼関係情報を読み出す。続いて、メモリコントローラ３５は要求元のアプリケーションの識別番号が、読み出した信頼関係情報において、処理要求の内容に対応する項目に含まれているかどうかを確認する。例えば、アプリケーション「ＡＰ－２５６８」を実行している制御部３１が、メモリコントローラ３５に対し、アプリケーション領域４０Ａ－２に書き込まれている「ＡＰ－０１２３」に対するアプリケーションの読み取り要求を送信した場合、メモリコントローラ３５は信頼情報領域４０Ｒ－２から信頼関係情報を読み出し、そのアプリケーションの読み取りが許可されているアプリケーションのリストにアプリケーション「ＡＰ－２５６８」が含まれているかどうかを確認する。要求元のアプリケーションがこのリストに含まれている場合、メモリコントローラ３５は制御部３１の処理要求を承諾し、要求に従った処理を行う。一方、要求元のアプリケーションが、読み取りが許可されているアプリケーションのリストに含まれていない場合、メモリコントローラ３５は制御部３１の処理要求を拒否する。

【０２１６】

このようなメモリコントローラ３５による信頼関係情報を利用した制御により、アプリケーション間の連係動作において、きめ細かい管理が可能となる。

【０２１７】

［３］第３実施形態

第３実施形態は、上述した第１実施形態と比較し、以下に説明するようにアプリケーションの配信の流れが異なっている。その他の点に関しては全て第１実施形態と同様である。従って、以下の説明においては第３実施形態が第１実施形態と異なる点のみを説明する。また、以下の説明においては、各構成要素を特定するために、第１実施形態において用いた名称および符号をそのまま用いる。

【０２１８】

［３．１］アプリケーション配信システムの構成

まず、第１実施形態と同様に、コンテンツサーバ２０の管理事業者が希望する場合、アプリケーションの内容は管理サーバ１６の管理事業者により審査され、信頼度が与えられる。その際、第３実施形態においては、管理サーバ１６の管理事業者は、アプリケーションに対しハッシュ関数を用いて、メッセージダイジェストを作成する。ハッシュ関数は元となるデータから、不可逆的なデータを作成するので、このメッセージダイジェストからは、それに対応するアプリケーションを復元することはできない。また、わずかでも内容の異なるアプリケーションからは、同じメッセージダイジェストが作成されることは極めて稀であり、実用上、アプリケーションの内容がわずかでも変更されれば、同じハッシュ関数を用いてそのアプリケーションから作成されるメッセージダイジェストは、変更前の

アプリケーションに対応するメッセージダイジェストとは一致しない。なお、メッセージダイジェストはそれに対応するアプリケーションのサイズと比較して小さく、格納容量が少なくて済む上、送受信が容易である。管理サーバ１６の管理事業者は、作成したメッセージダイジェストを信頼度とともにアプリケーション情報格納部５２に格納する。図３７は、第３実施形態においてアプリケーション情報格納部５２に格納されるデータ例を示す図である。

【０２１９】

なお、第３実施形態においては、説明の簡易化のため、内容審査の行われたアプリケーションに関し、管理サーバ１６において移動体端末１１に対し、アプリケーションの一覧を公開することは行わないものとする。従って、図３７において、公開に関する項目は設けられていない。

【０２２０】

第３実施形態においては、第１実施形態と異なり、アプリケーション本体はアプリケーション情報格納部５２に格納されることはなく、全て配信元である各コンテンツサーバ２０に格納される。従って、図３７において、保管場所に関する項目にアプリケーション本体が格納されているアプリケーションはなく、全てのアプリケーションについて、保管場所を示すＵＲＬが格納されている。

【０２２１】

第３実施形態においては、第１実施形態と異なり、アプリケーション本体は全て、直接、配信元である各コンテンツサーバ２０から各移動体端末１１に配信される。従って、管理サーバ１６のアプリケーション情報格納部５２において、一時保管アプリケーション領域５２Ｔは不要であるため、設けられていない。また、管理サーバ１６のユーザ情報格納部５３においても、第１実施形態において、一時保管アプリケーション領域５２Ｔに格納されるアプリケーションの保管場所を特定するために設けられていた保管番号の項目は不要であるため、設けられていない。図３８は第３実施形態におけるアプリケーションの情報管理システムの構成を示す図であり、図３９は第３実施形態におけるユーザ情報格納部５３に格納されるデータ例を示す図である。

【０２２２】

また、第３実施形態においては、移動体端末１１－１のメモリコントローラ３５は、管理サーバ１６からメッセージダイジェストを受信するとそれを一時的に格納する。また、移動体端末１１－１のメモリコントローラ３５は、通信部３４を介して「１」以上の信頼度の与えられたアプリケーションを受信すると、受信したアプリケーションのメッセージダイジェストを作成し、その新たに作成されたメッセージダイジェストを、管理サーバ１６から受信されるメッセージダイジェストと照合する。

【０２２３】

［３．２］アプリケーションの配信

移動体端末１１のユーザが、「１」以上の信頼度を与えられているアプリケーションの購入およびダウンロードを行う処理の例として、移動体端末１１－１のユーザが、コンテンツサーバ２０－１が配信元であるアプリケーションを購入し、ダウンロードする場合の処理を図４０、図４１、および図４２を用いて説明する。また、以下の処理の流れに伴い、移動体端末１１－１のディスプレイ部２１に表示される表示は、第１実施形態におけるアプリケーションのダウンロード処理において用いた図２１と同様であるので、それを用いる。

【０２２４】

移動体端末１１－１のユーザは、例えば移動体端末１１－１を用いてコンテンツサーバ２０－１内のホームページを開き、そのホームページにおいて目的のアプリケーションの購入申請を行う（ステップＳ６０１）。その際、移動体端末１１－１のユーザは購入するアプリケーションの利用料金の支払手続も行うものとする。

【０２２５】

コンテンツサーバ２０－１は移動体端末１１－１の購入申請の内容が所定の条件を満た

していることを確認した後、管理サーバ１６に対しアプリケーションの購入承諾通知を送信する（ステップＳ６０２）。この購入承諾通知にはアプリケーションの購入を行った移動体端末１１－１の識別番号と、購入されたアプリケーションの識別番号が含まれている。また、コンテンツサーバ２０－１は購入承諾通知を送信する際、購入承諾を行った移動体端末１１－１の識別番号を記録する。

【０２２６】

管理サーバ１６は、コンテンツサーバ２０－１から購入承諾通知を受信すると、受信した購入承諾通知に含まれている移動体端末の識別番号からアプリケーションを購入した移動体端末を特定する。続いて管理サーバ１６は、移動体端末１１－１に対応するユーザ情報格納部５３－１における配信可能アプリケーション領域５３Ｂに、購入承諾通知に含まれているアプリケーションの識別番号を登録する（ステップＳ６０３）。

【０２２７】

続いて、管理サーバ１６は、移動体端末１１－１に対し、アプリケーションの購入処理の完了通知を送信する（ステップＳ６０４）。移動体端末１１－１は、アプリケーションの購入処理の完了通知を受信すると、ディスプレイ部２１の上部に「α」を表示する。この「α」の表示は、移動体端末１１－１のユーザに対し、新たにダウンロードが可能となったアプリケーションがあることを知らせるための表示である。

【０２２８】

ここで、コンテンツサーバ２０－１により管理サーバ１６に対して、新たに購入が行われたアプリケーションの料金徴収の代行依頼がされている場合には、管理サーバ１６はアプリケーションの識別番号、移動体端末１１－１の識別番号、購入日時等の情報を課金管理サーバに送信する（ステップＳ６０５）。

【０２２９】

移動体端末１１－１のユーザは、移動体端末１１－１のアプリボタン２３を押下して、画面Ｄ２１のアプリケーションメニューを表示させる。画面Ｄ２１において、移動体端末１１－１のユーザは、操作部２２のボタン「２」を押下して「２．アプリケーションのダウンロード」を選択する。ボタン「２」が押下されると、移動体端末１１－１は管理サーバ１６に対し、ダウンロードの可能なアプリケーション情報一覧の送信要求を行う（ステップＳ６０６）。

【０２３０】

管理サーバ１６はアプリケーション情報一覧の送信要求を受信すると、ユーザ情報格納部５３－１の配信可能アプリケーション領域５３Ｂに登録されているアプリケーションの名称を、アプリケーションの識別番号と共にアプリケーション情報一覧として移動体端末１１－１に送信する（ステップＳ６０７）。

【０２３１】

移動体端末１１－１はアプリケーション情報一覧を受信すると、画面Ｄ２２を表示させる。これに対し、移動体端末１１－１のユーザは対応する番号のボタンを押下することにより、ダウンロードするアプリケーションの指定を行う。例えばユーザが画面Ｄ２２においてボタン「１」を押下すると、「スケジュール管理　Ｖｅｒ．２」という名称のアプリケーションが選択される。移動体端末１１－１のユーザによるボタン操作によりアプリケーションが指定されると、移動体端末１１－１は管理サーバ１６に対し、指定されたアプリケーションの識別番号を送信する（ステップＳ６０８）。

【０２３２】

管理サーバ１６は指定されたアプリケーションの識別番号を受信すると、管理サーバ１６は既配信アプリケーション領域５３Ａのデータを読み出し、移動体端末１１－１のメモリ１２の管理エリア４０に、指定されたアプリケーションを書き込むために必要な空き容量があるかどうかを確認する（ステップＳ６０９）。

【０２３３】

ステップＳ６０９において、移動体端末１１－１のメモリ１２に指定されたアプリケーションを書き込むための空き容量が十分でない場合、管理サーバ１６は移動体端末１１－

１に対し、メモリ１２上から削除すべきアプリケーションの指定要求を送信する（ステップＳ６１０）。移動体端末１１－１はこの指定要求を受信すると、画面Ｄ２３をディスプレイ部２１に表示させる。移動体端末１１－１のユーザがこの画面に対しボタン「９」を押下して実行の指示を行うと、移動体端末１１－１はさらに画面Ｄ２４をディスプレイ部２１に表示させる。画面Ｄ２４には管理エリア４０に書き込まれているアプリケーションの名称が表示される。この画面において、移動体端末１１－１のユーザは対応するボタンを押下することにより、メモリ１２から削除するアプリケーションを指定する。移動体端末１１－１は指定されたアプリケーションの識別番号を管理サーバ１６に送信する（ステップＳ６１１）。なお、ステップＳ６１１の処理の後、移動体端末１１－１はディスプレイ部２１に画面Ｄ２５を表示させる。

【０２３４】

一方、ステップＳ６０９において、指定されたアプリケーションを書き込むための空き容量が移動体端末１１－１のメモリ１２に十分ある場合、ステップＳ６１０およびステップＳ６１１の処理は行われず、管理サーバ１６は次のステップＳ６１２の処理に進む。また、移動体端末１１－１はディスプレイ部２１に画面Ｄ２５を表示させる。

【０２３５】

続いて、管理サーバ１６は、移動体端末１１－１により指定されたアプリケーションの識別番号を用いて、アプリケーション情報格納部５２から指定されたアプリケーションに対応する内容証明書、信頼度、およびアプリケーションの保管場所に関する情報を読み出し、それらを移動体端末１１－１に送信する（ステップＳ６１２）。

【０２３６】

移動体端末１１－１は、管理サーバ１６よりアプリケーションの内容証明書、信頼度、およびアプリケーションの保管場所に関する情報を受信すると、受信したアプリケーションの保管場所に関する情報を用いて、コンテンツサーバ２０－１に対し、アプリケーションの送信要求を送信する（ステップＳ６１３）。このアプリケーションの送信要求には、移動体端末１１－１の識別番号およびアプリケーションの識別番号が含まれている。

【０２３７】

コンテンツサーバ２０－１は、アプリケーションの送信要求を受信すると、受信した送信要求に含まれる移動体端末の識別番号が、ステップＳ６０２においてアプリケーションの購入承諾を行った移動体端末の識別番号と一致するかどうかを確認する。これらの識別番号が一致する場合、コンテンツサーバ２０－１は、認証サーバ１７に対し移動体端末１１－１の公開鍵「ＰＫ－ＭＴ－１」の送信を要求する（ステップＳ６１４）。認証サーバ１７は「ＰＫ－ＭＴ－１」の送信要求を受信すると、コンテンツサーバ２０－１に対し「ＰＫ－ＭＴ－１」を送信する（ステップＳ６１５）。

【０２３８】

コンテンツサーバ２０－１は「ＰＫ－ＭＴ－１」を受信すると、送信要求のされたアプリケーションを「ＰＫ－ＭＴ－１」を用いて暗号化する（ステップＳ６１６）。この暗号化処理により、アプリケーションがコンテンツサーバ２０－１から移動体端末１１－１に配信される際、第３者がこれを傍受しても内容を解読することができず、アプリケーションが第３者により不正に使用されることが防がれる。

【０２３９】

コンテンツサーバ２０－１は暗号化されたアプリケーションを移動体端末１１－１に対し送信する（ステップＳ６１７）。

【０２４０】

移動体端末１１－１は暗号化されたアプリケーションを受信すると、そのアプリケーションを移動体端末１１－１の秘密鍵「ＳＫ－ＭＴ－１」を用いて復号化する（ステップＳ６１８）。

【０２４１】

続いて、移動体端末１１－１は、ステップＳ６０８の処理により平文となったアプリケーションのメッセージダイジェストを作成し、作成したメッセージダイジェストと、ステ

ップＳ６１２において管理サーバ１６より受信した内容証明書との照合を行う（ステップＳ６１９）。ここで、管理サーバ１６においてアプリケーションの内容審査直後に作成されたメッセージダイジェストである内容証明書と、新たに作成されたメッセージダイジェストが一致すると、移動体端末１１－１がコンテンツサーバ２０－１より受信したアプリケーションが、内容審査後に変更されていないことが証明される。もしこれらのメッセージダイジェストが一致しない場合、アプリケーションの内容が変更されているので、移動体端末１１－１は、そのアプリケーションのメモリ１２への書き込みを行わず、管理サーバ１６に対し、正しいアプリケーションの受信に失敗したことを通知する。

【０２４２】

ステップＳ６１９において、２つのメッセージダイジェストが一致した場合、移動体端末１１－１は、アプリケーションをメモリ１２の管理エリア４０のアプリケーション領域４０Ａのいずれかに書き込む（ステップＳ６２０）。ここで、ステップＳ６０９においてメモリ空き容量が残っていなかった場合は、ステップＳ６１１において削除の指定を行ったアプリケーションが書き込まれている管理エリア４０に、新たに受信されたアプリケーションが書き込まれる。また、ステップＳ６０９においてメモリ空き容量が残っていた場合は、空いている管理エリア４０のいずれかに、新たに受信されたアプリケーションが書き込まれる。

【０２４３】

移動体端末１１－１は、アプリケーションの書き込みを完了すると、管理サーバ１６に対し、アプリケーションの書き込み完了通知を送信する（ステップＳ６２１）。移動体端末１１－１はステップＳ６２１の処理を終えると、ディスプレイ部２１に通常の画面である画面Ｄ２６を表示させる。

【０２４４】

管理サーバ１６は、アプリケーションの書き込み完了通知を受信すると、ユーザ情報格納部５３のデータの更新を行う（ステップＳ６２２）。具体的には、まず移動体端末１１のメモリ１２より削除されたアプリケーションがある場合、そのアプリケーションの情報を既配信アプリケーション領域５３Ａから配信可能アプリケーション領域５３Ｂに移動する。次に、新たにメモリ１２に書き込まれたアプリケーションの情報を、配信可能アプリケーション領域５３Ｂから既配信アプリケーション領域５３Ａの対応する場所に移動する。

【０２４５】

以上が、移動体端末１１のユーザが、「１」以上の信頼度を与えられているアプリケーションの購入およびダウンロードを行う処理の流れである。これに対し、移動体端末１１のユーザが、信頼度「０」のアプリケーションの購入およびダウンロードを行う場合は、管理サーバ１６による移動体端末１１－１に対する内容証明書および信頼度の送信は不要である。従って、図４０におけるステップＳ６０１～ステップＳ６０４、ステップＳ６０６～ステップＳ６１１、ステップＳ６１３～ステップＳ６１８、ステップＳ６２０～ステップＳ６２２のみが行われる。なお、この場合、ステップＳ６１０およびステップＳ６１１において、削除候補のアプリケーションの一覧は管理エリア４０に書き込まれたアプリケーションではなく、フリーエリア４１に書き込まれたアプリケーションの一覧となる。

【０２４６】

以上により、アプリケーションが移動体端末１１－１のメモリ１２に書き込まれるが、そのアプリケーションはアクティベーション処理がなされていない。従って、移動体端末１１－１のユーザは、続いてアクティベーション処理を行うことにより新たに購入したアプリケーションを利用することができるようになる。その場合のアクティベーション処理は、第１実施形態において説明したアクティベーション処理と同様である。また、第３実施形態においても、第１実施形態と同様にディアクティベーション処理、および削除処理を行うことができる。

【０２４７】

［４］実施形態の変形例

［４．１］第１変形例
第１変形例においては、アプリケーション配信システムには複数の管理サーバが含まれている。これらの複数の管理サーバは、例えば互いに同期が取られ、常時データベースのデータが更新されているため、各移動体端末および各コンテンツサーバは管理サーバとの間で処理を行う場合、応答の速い管理サーバを自由に選択することができる。第１変形例においては、管理サーバにより分散処理が可能となるので、アプリケーション配信システム全体の処理速度の向上と、管理サーバの障害発生に対する信頼性の向上が実現される。
【０２４８】
［４．２］第２変形例
第２変形例においては、移動体端末においてアプリケーションを書き込む場所として、移動体端末に内蔵されたメモリに加え、各種のＩＣカードメモリ、ＵＩＭ（Ｕｓｅｒ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｍｏｄｕｌｅ）、および移動体端末に装着可能な外部記憶装置がユーザにより自由に選択できる。従って、第２変形例においては、移動体端末間でアプリケーションの記録媒体を交換することにより、アプリケーションを共有したり、移動させたりすることが容易である。
【０２４９】
［４．３］第３変形例
第３変形例においては、移動体端末は他の情報端末と有線もしくは無線で移動体通信網を介さずに接続可能な入出力インタフェースを持っている。従って、移動体端末はその入出力インタフェースを介して他の情報端末からアプリケーションを取得することができる。
【０２５０】
［４．４］第４変形例
第４変形例においては、管理サーバはアプリケーション情報格納部において、内容が同一のアプリケーションであっても、配信元が異なるものについては異なるアプリケーション識別番号を与え、必要に応じて異なる信頼性に関する情報を与えている。従って、例えば、信頼度の高いコンテンツプロバイダから送信されるアプリケーションには高い信頼度が与えられ、信頼度の低いコンテンツプロバイダから配信されるアプリケーションには低い信頼度が与えられており、同じアプリケーションであっても加える制限を変更可能である。
【０２５１】
［４．５］第５変形例
第５変形例においては、移動体端末のメモリにおいて、１つのアプリケーションが複数のメモリエリアを利用することができる。従って、移動体端末において、プログラムサイズの大きいアプリケーションの実行が可能である。
【０２５２】
［４．６］第６変形例
第６変形例においては、内容審査の行われているアプリケーションの書き込まれる管理エリアと、内容審査の行われていないアプリケーションの書き込まれるフリーエリアの領域を自由に変更することができる。メモリーコントローラは各メモリエリアに書き込まれているアプリケーションに信頼性に関する情報が与えられているかどうかを管理しているため、管理エリアのアプリケーションとフリーエリアのアプリケーションが混同されることはない。従って、例えば管理エリアの空き容量が不足した場合、フリーエリアの空き容量を管理エリアに切り換えることにより、メモリエリアの効率的利用ができる。
【０２５３】
［４．７］第７変形例
第７変形例においては、アプリケーションの内容審査および信頼性に関する情報の付与は管理サーバの管理事業者とは異なる第３者機関が行う。第３者機関により付与されるアプリケーションの信頼性に関する情報は、随時管理サーバに送信され、管理サーバおよび移動体端末により利用される。

【０２５４】
また、この第３者機関が管理する内容認証サーバは、コンテンツサーバから管理サーバにアプリケーションが送信される際、アプリケーションの内容に対しコンテンツサーバによる改竄等が行われていないことを証明するための証明書を、管理サーバに対し発行する。

【０２５５】
より具体的には、第３者機関はアプリケーションの内容審査を行った後、そのアプリケーションに対しハッシュ関数を用いてメッセージダイジェストを作成する。管理サーバはコンテンツサーバからアプリケーションを受信すると、内容認証サーバに対し、そのアプリケーションに対応するメッセージダイジェストの送信を要求する。内容認証サーバは要求に応じてメッセージダイジェストを管理サーバに送信する。管理サーバはメッセージダイジェストを受信すると、アプリケーションに対し第３者機関が用いたものと同じハッシュ関数を用いてメッセージダイジェストを作成し、内容認証サーバから受信したメッセージダイジェストと、新たに作成したメッセージダイジェストを照合する。この照合処理により、管理サーバは受信したアプリケーションの内容が正しいことを確認できる。

【０２５６】
第７変形例においては、第３者機関が内容の保証を行うので、管理サーバは平文のアプリケーションを取得する必要はない。従って、コンテンツサーバは、例えば移動体端末の公開鍵で暗号化したアプリケーションを管理サーバ経由で移動体端末に配信することができる。また、管理サーバはアプリケーションの内容そのものに変更のないことを確認できるので、そのアプリケーションの送信元を確認する必要がない。従って、コンテンツサーバは、コンテンツサーバの秘密鍵でアプリケーションを暗号化することなく、管理サーバに送信することができる。

【０２５７】
［４．８］第８変形例
第８変形例においては、あるアプリケーションが、他のアプリケーションもしくは制御用プログラムの機能を利用したり、他のアプリケーションもしくは制御用プログラムの管理するデータを利用したりする場合、アプリケーションもしくは制御用プログラムにおける機能単位、およびデータの種別単位に利用の許可もしくは拒否を判定するための信頼関係情報が設定されている。

【０２５８】
従って、第８実施例においては、例えば、移動体端末において、アプリケーションＡがアプリケーションＢの機能１は利用できるが、アプリケーションＢの機能２は利用できない、といったきめ細かい制御を行うことができる。

【図１】

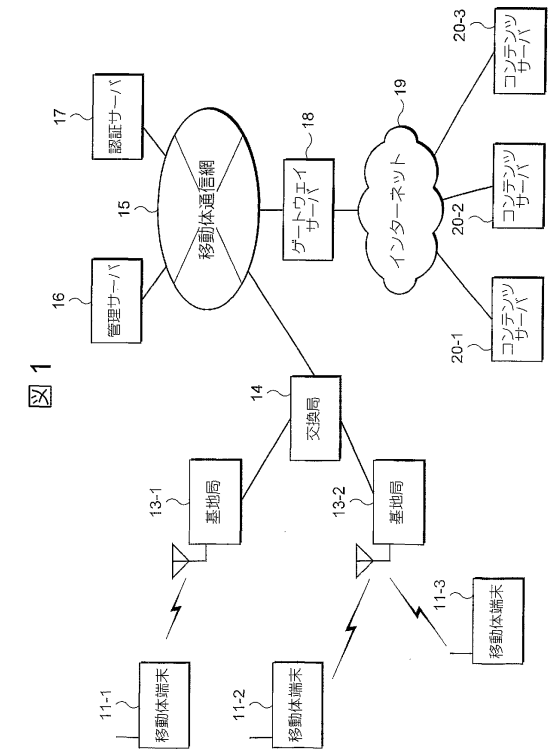
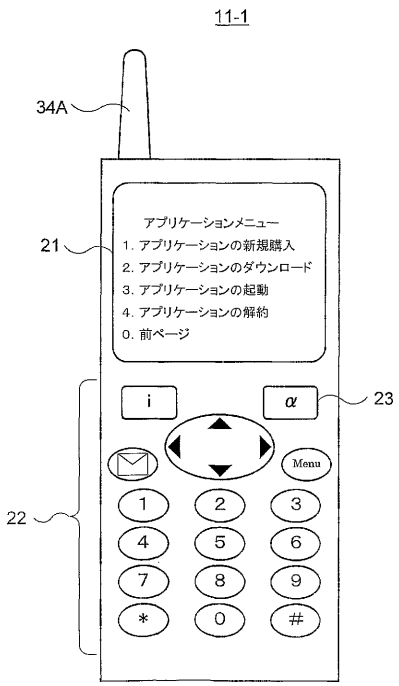


図１

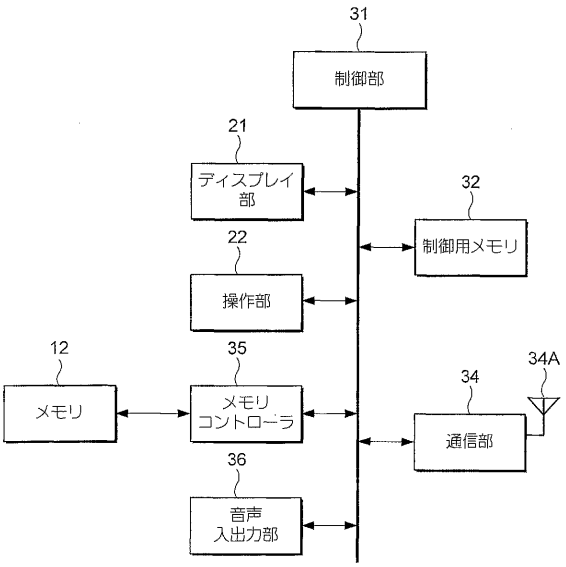
【図２】

図２



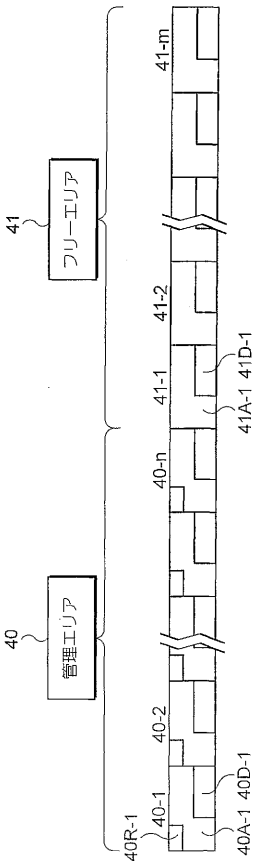
【図３】

図３



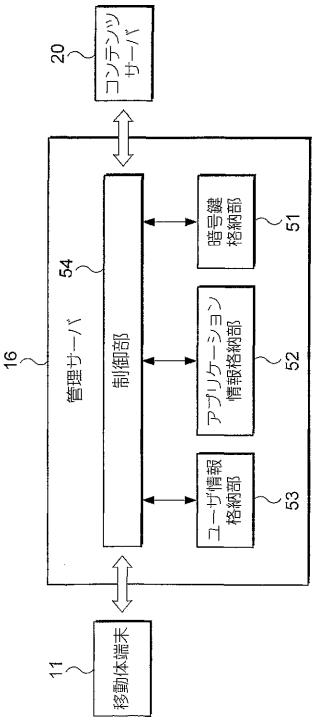
【図４】

図４



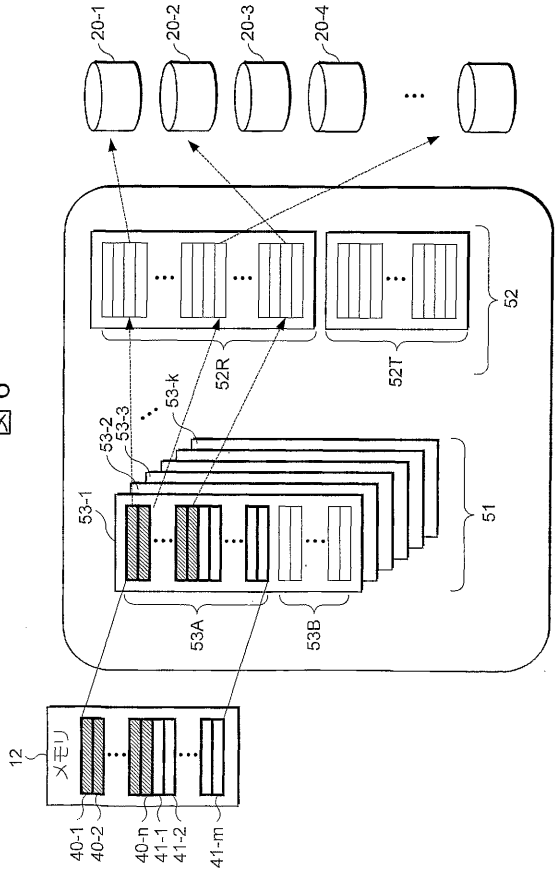
【図５】

図５



【図６】

図６



【図７】

図７

	メモリエリア		アプリケーション識別番号	アクティベーション	保管番号
既配信アプリケーション領域	固定エリア	1	AP-2568	Yes	—
		2	AP-0123	No	—
		3	AP-1015	Yes	—
		⋮	⋮	⋮	⋮
		n	未使用	—	—
	フリーエリア	1	F-0325	Yes	—
		2	F-7485	Yes	—
		3	未使用	—	—
		⋮	⋮	⋮	⋮
		m	未使用	—	—
配信可能アプリケーション領域		1	AP-4125	—	T-7851
		2	F-5963	—	T-3256
		3	AP-3021	—	削除済み
		4	AP-4513	—	—
		5	未使用	—	—
		6	未使用	—	—
		7	未使用	—	—
		8	未使用	—	—
		9	未使用	—	—
		⋮	⋮	⋮	⋮

【図８】

図８

アプリケーション識別番号	信頼度	公開	料金徴収	保管場所
AP-2568	3	Yes	Yes	アプリケーション本体を格納
AP-3712	5	Yes	No	ftp://ftp.abc_software.com/application/ap_0306.exe
AP-4513	2	No	Yes	アプリケーション本体を格納
AP-3021	1	No	No	ftp://ftp.software_world.com/software/app_view.exe
F-3251	0	—	—	ftp://ftp. softpocket.com/root/app/miracle.exe
…	…	…	…	…

【図９】

保管番号	
T-1025	アプリケーション本体
T-7851	アプリケーション本体
T-3639	アプリケーション本体
T-7142	アプリケーション本体
T-3256	アプリケーション本体
…	…

図９

【図１０】

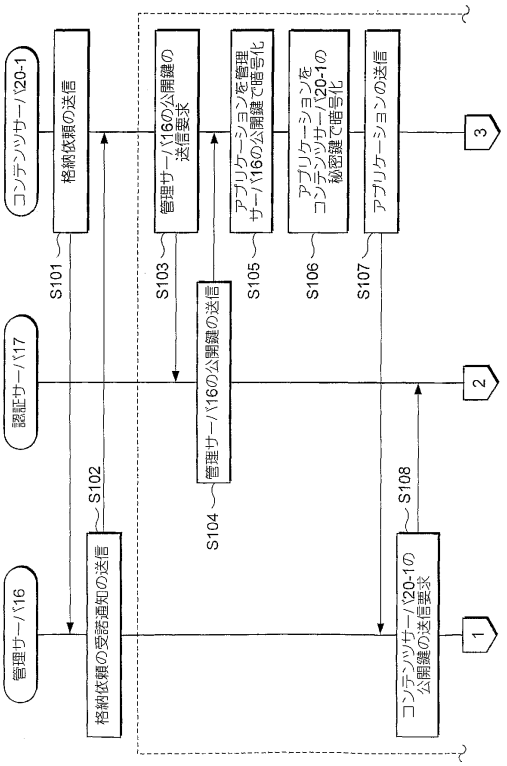


図10

【図１１】

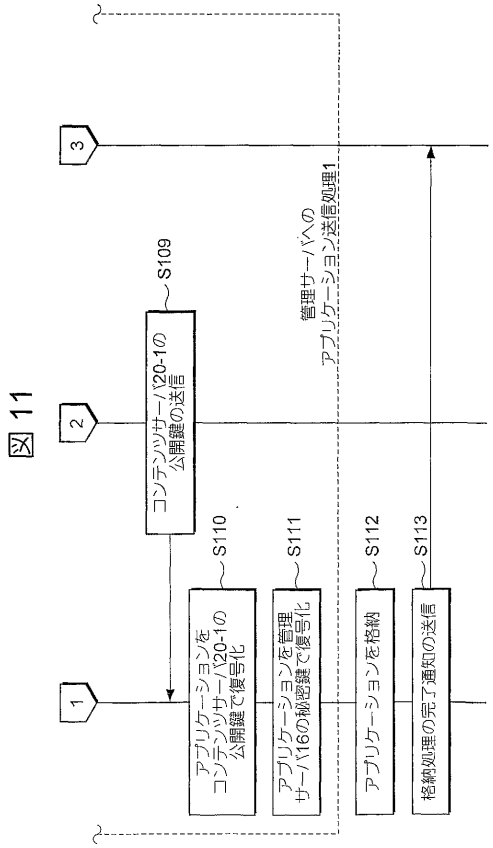


図11

【図１２】

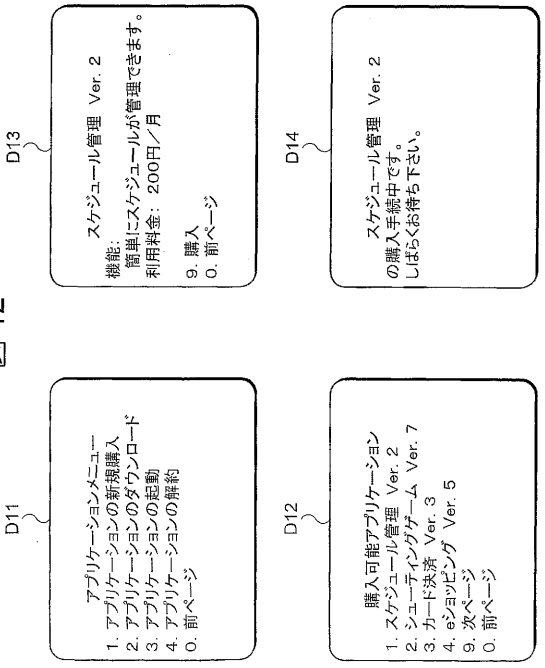
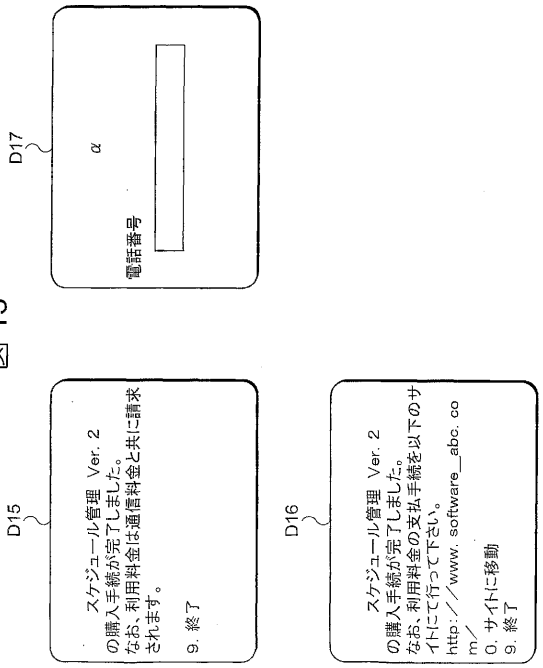


図12

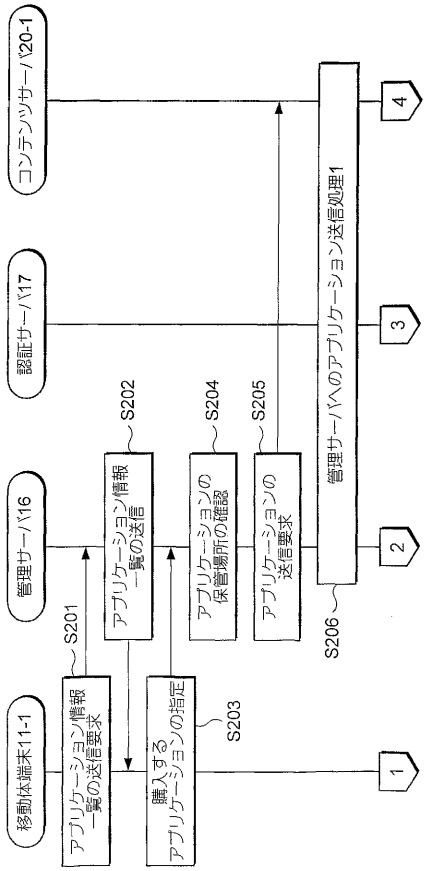
【図１３】

図 13



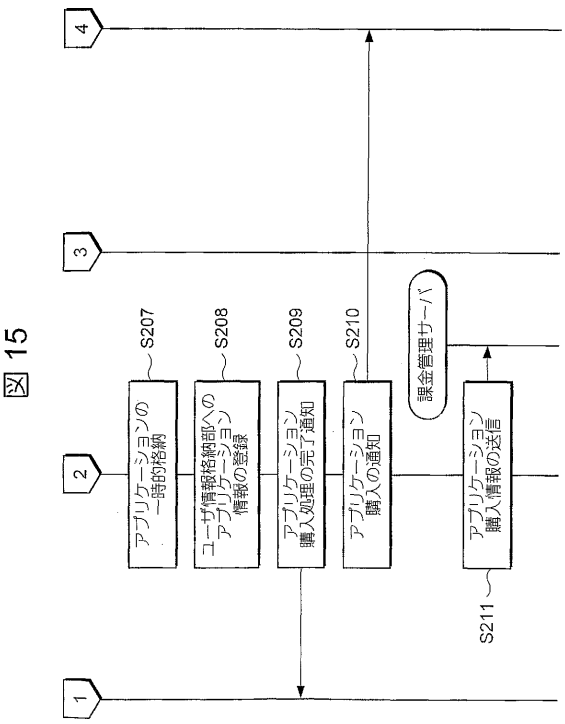
【図１４】

図 14



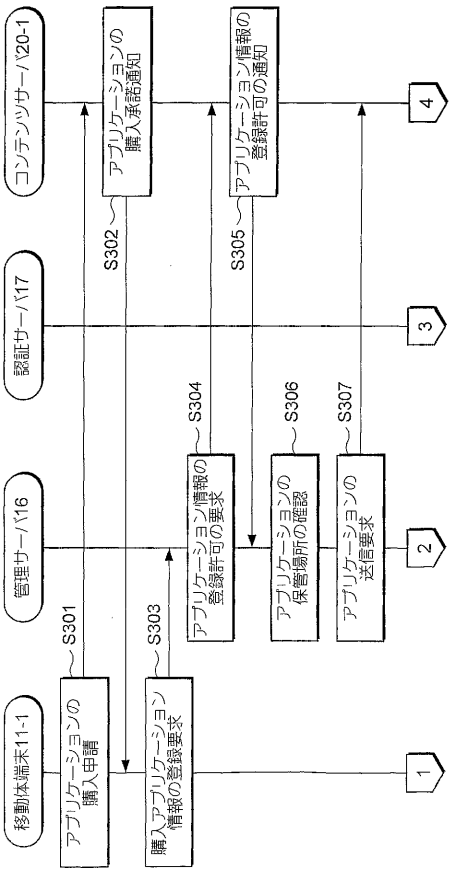
【図１５】

図 15

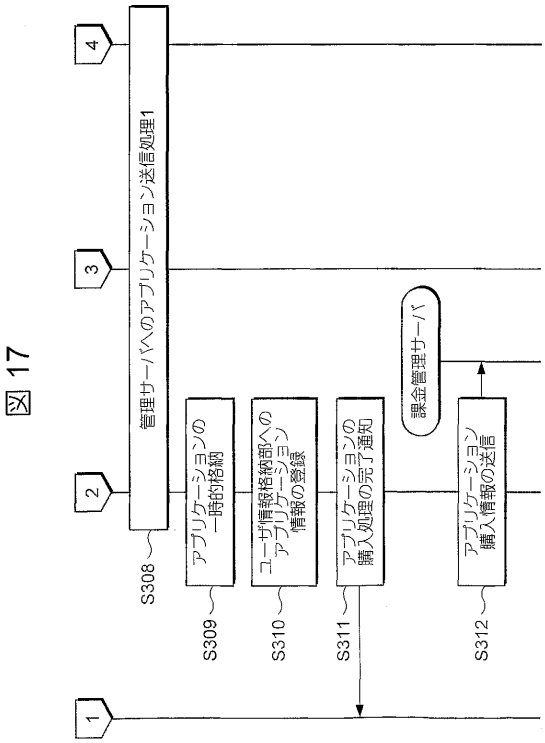


【図１６】

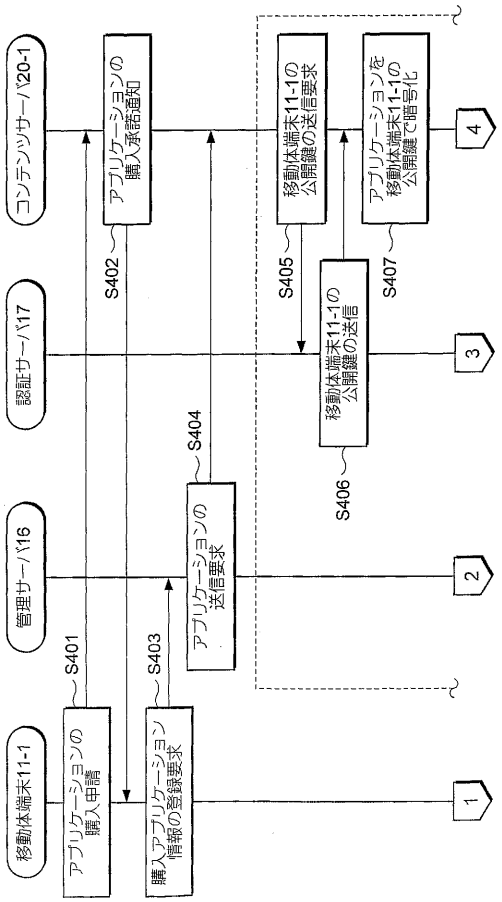
図 16



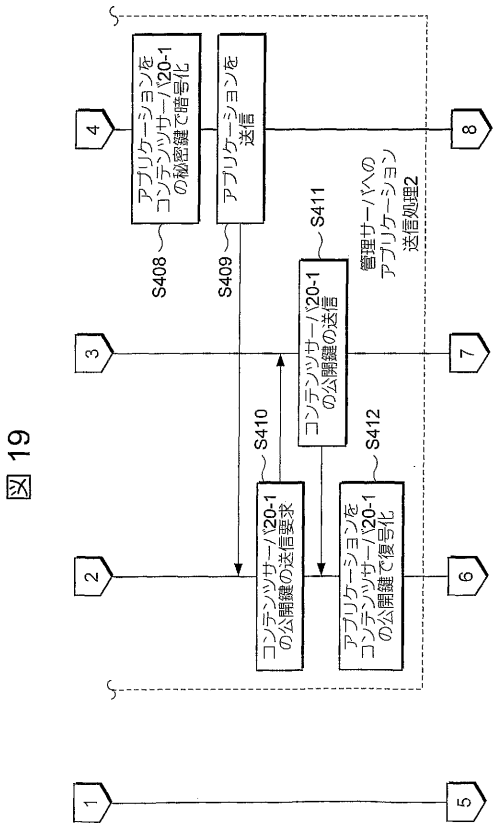
【図１７】



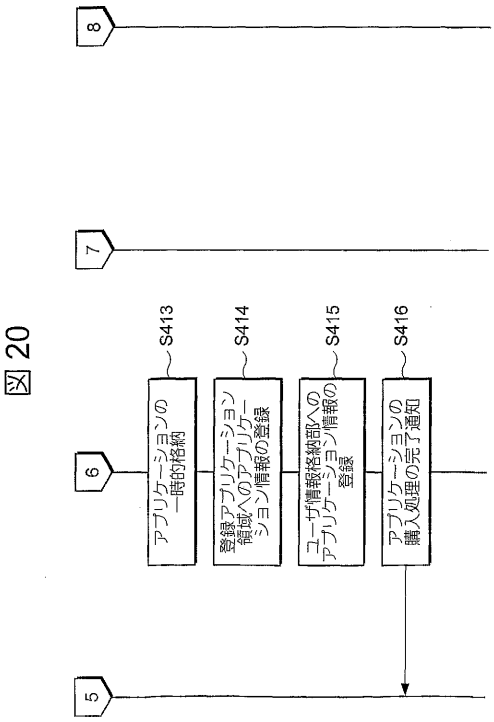
【図１８】



【図１９】

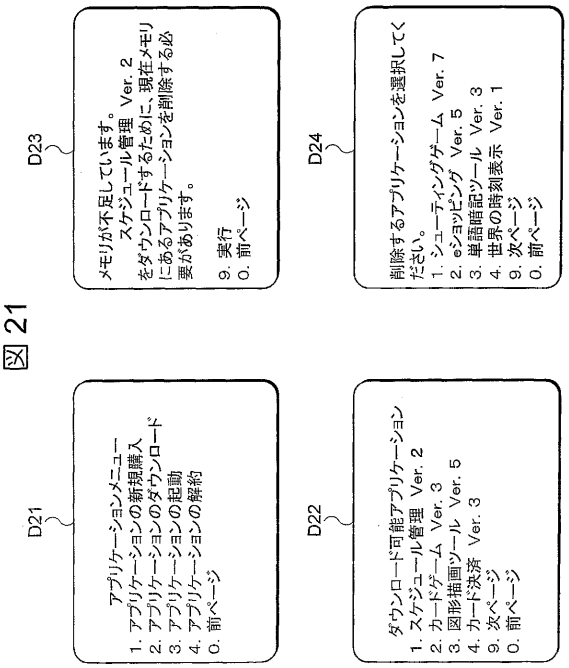


【図２０】



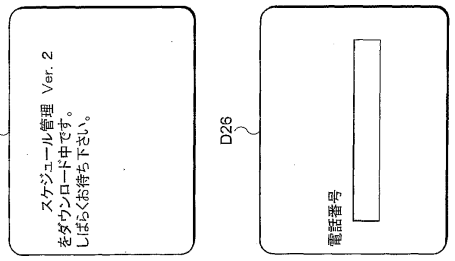
【図２１】

図21



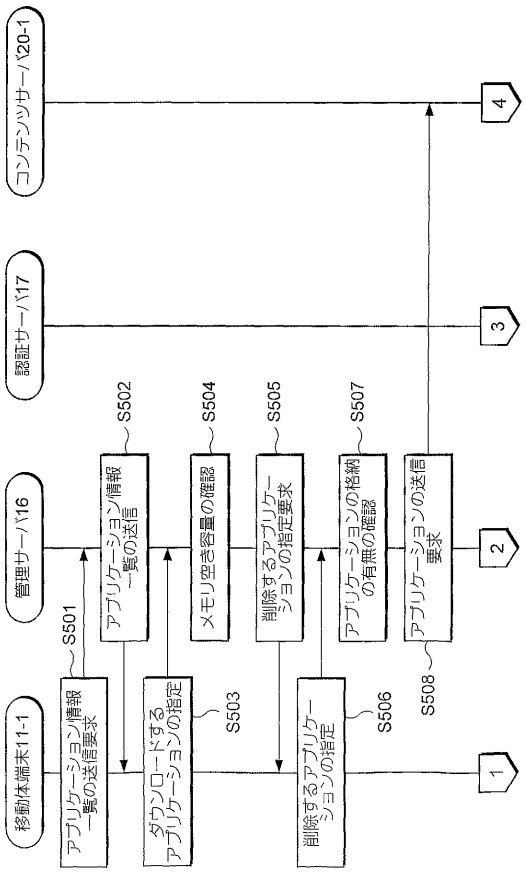
【図２２】

図22



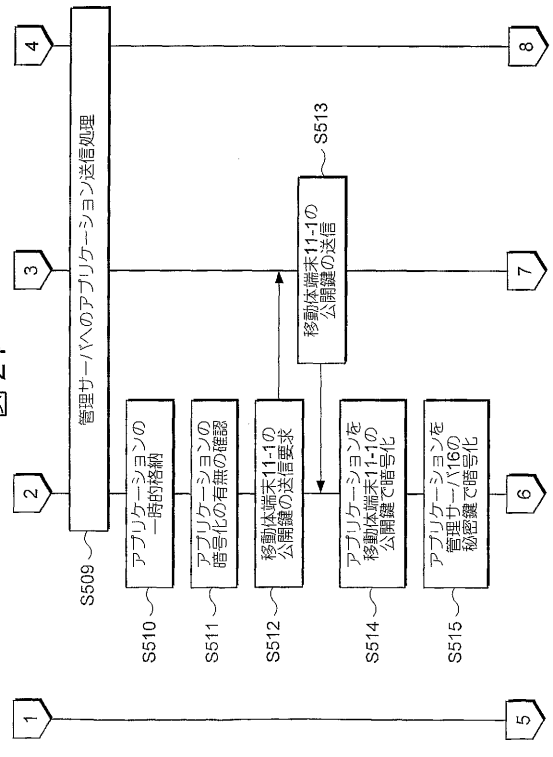
【図２３】

図23

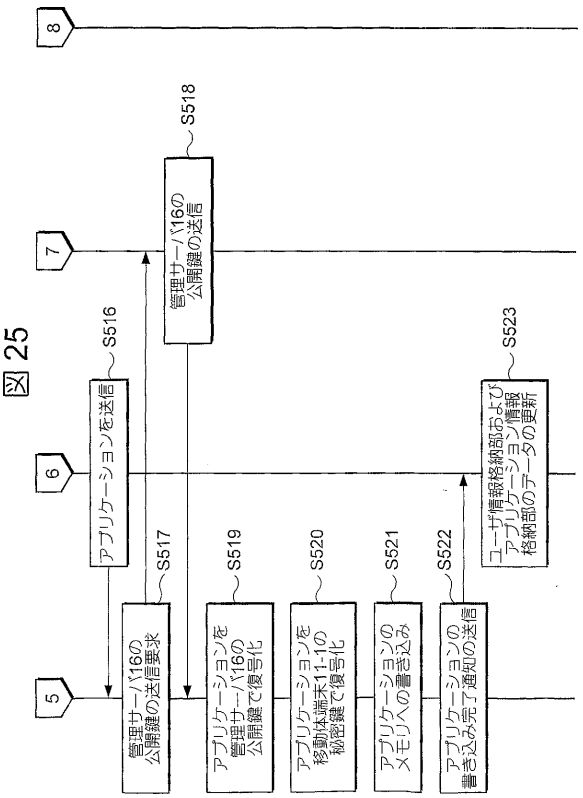


【図２４】

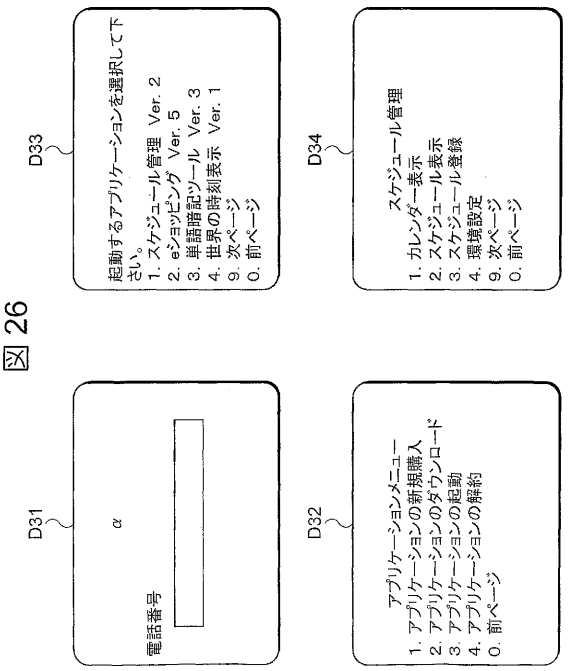
図24



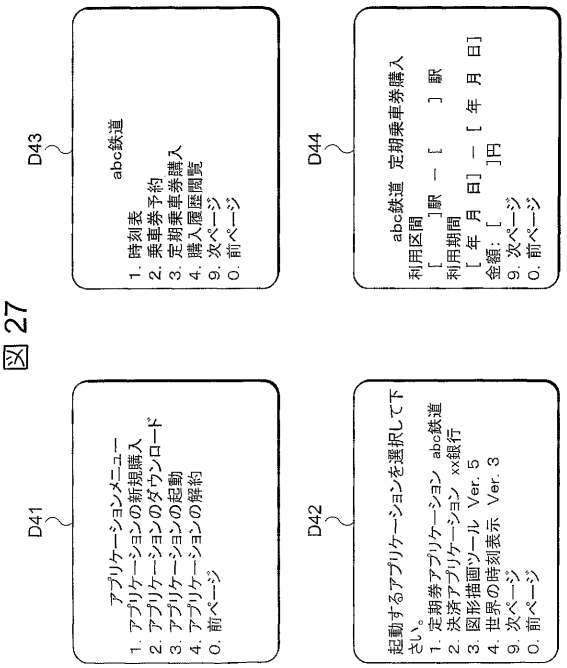
【図２５】



【図２６】



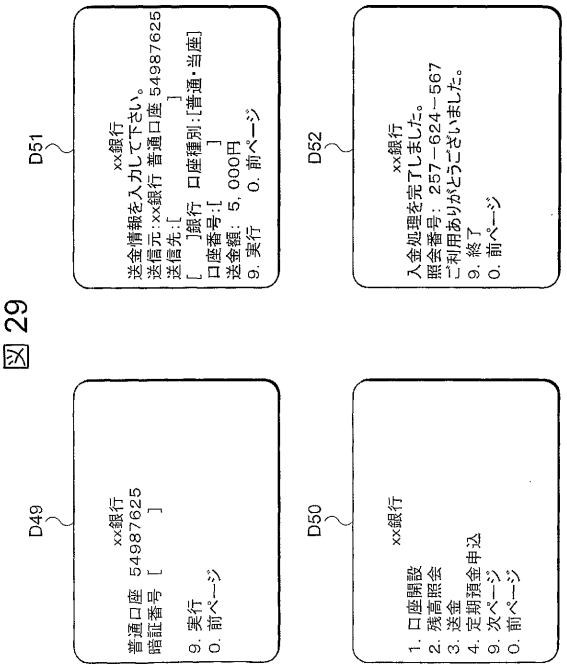
【図２７】



【図２８】

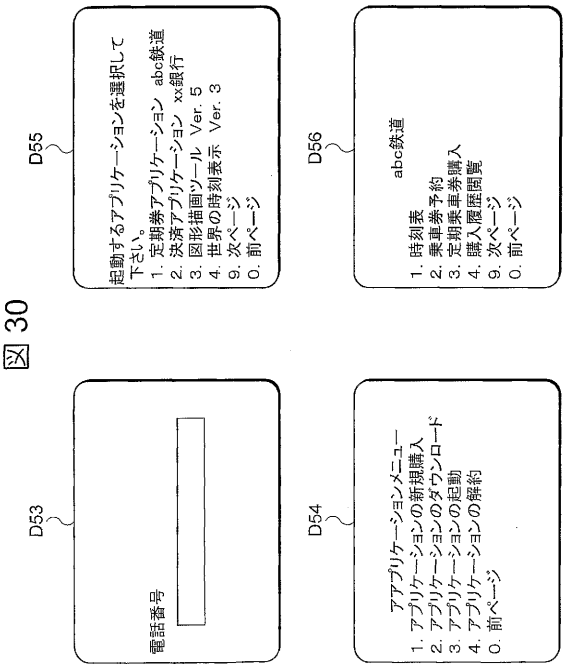
【図２９】

図 29



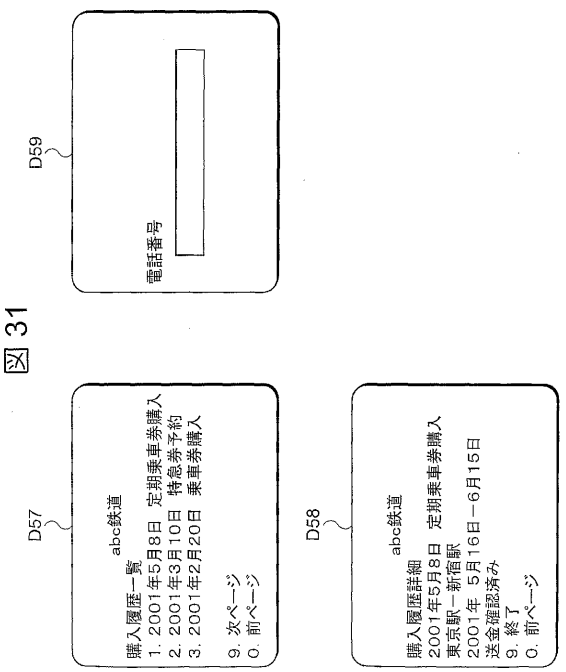
【図３０】

図 30



【図３１】

図 31

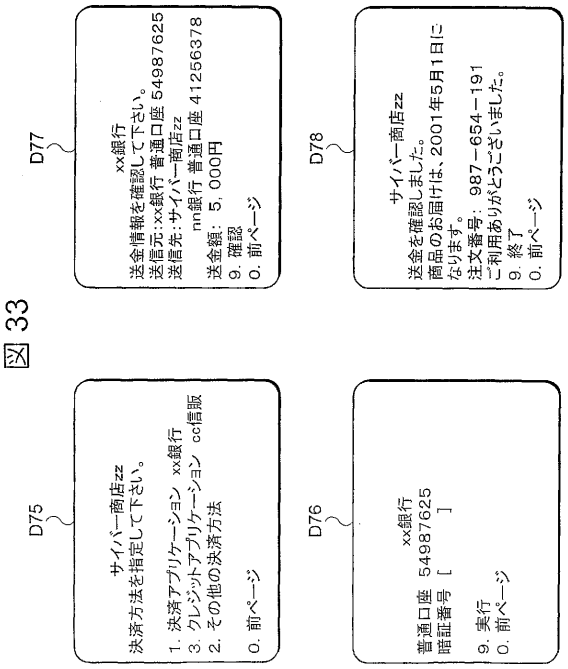


【図３２】

図 32

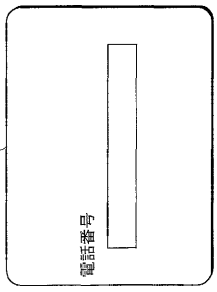
【図３３】

図 33



【図３４】

図 34



【図３５】

図 35

AP-3568からの要求			
アプリケーション読み取り	データ読み取り	データ書き込み	データ削除
AP-3712	AP-8125	AP-1346	AP-2349
AP-0123	AP-5724	AP-2349	AP-1272
…	…	…	…

AP-3568への要求			
アプリケーション読み取り	データ読み取り	データ書き込み	データ削除
AP-4315	AP-1523	AP-2349	AP-3125
AP-2349	AP-0312	AP-8125	AP-6789
…	…	…	…

【図３６】

図 36

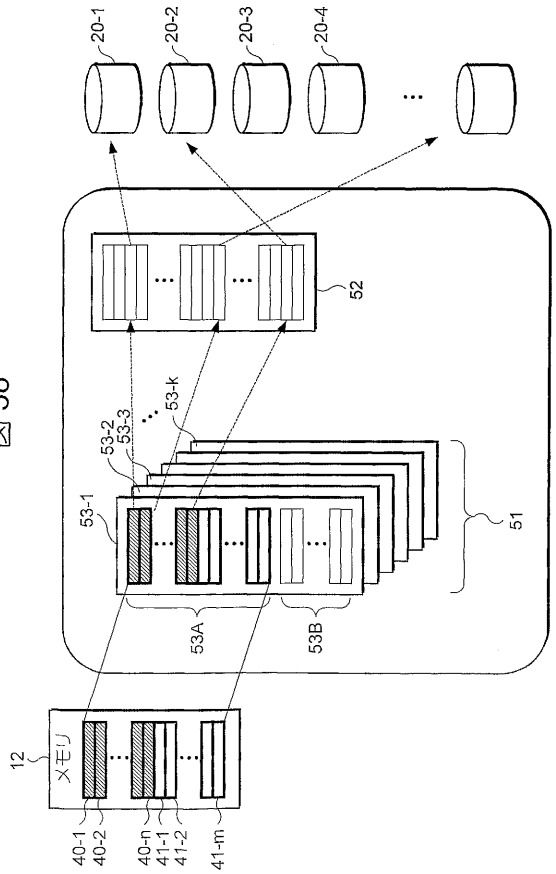
アプリケーション識別番号	信頼関係情報				公開	料金徴収	保管場所
	アプリケーション読み取り	データ読み取り	データ書き込み	データ削除			
AP-2568	AP-4315	AP-1523	AP-2349	AP-3125	Yes	Yes	アプリケーション本体を格納
	AP-2349	AP-0312	AP-8125	AP-6789			
	…	…	…	…			
AP-3712	AP-2436	AP-1297	AP-2635	AP-3251	Yes	No	ftp://ftp.abc_software.com/application/ap_0306.exe
	AP-9870	AP-0879	AP-8187	AP-6789			
	…	…	…	…			
AP-4513	AP-9870	AP-9009	AP-7614	AP-1231	No	Yes	アプリケーション本体を格納
	AP-1121	AP-0012	AP-8198	AP-6763			
	…	…	…	…			
AP-3021	AP-4121	AP-1231	AP-1213	AP-9809	No	No	ftp://ftp.software_world.com/software/app_view.exe
	AP-5454	AP-8192	AP-8125	AP-1265			
	…	…	…	…			
F-3251	—	—	—	—	—	—	ftp://ftp.softpocket.com/root/app/miracle.exe
…	…	…	…	…	…	…	…

【図３７】

図 37

アプリケーション識別番号	信頼度	料金徴収	保管場所	
AP-2568	3	Yes	ftp://ftp.neonetwonk.com/public/apbinder.exe	内容証明書
AP-3712	5	No	ftp://ftp.abc_software.com/application/ap_0306.exe	内容証明書
AP-4513	2	Yes	ftp://ftp.humantec.com/mobile/application007.jar	内容証明書
AP-3021	1	No	ftp://ftp.software_world.com/software/app_view.exe	内容証明書
F-3251	0	—	ftp://ftp. softpocket.com/root/app/miracle.exe	内容証明書
…	…	…	…	…

【図３８】

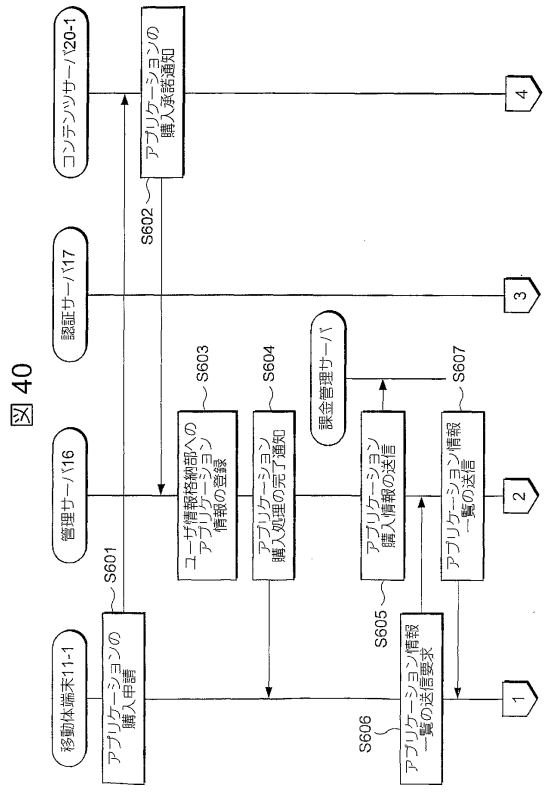


【図３９】

図 39

		メモリエリア	アプリケーション識別番号	アクティベーション
既に配置されているアプリケーション領域	常駐エリア	1	AP-2568	Yes
		2	AP-0123	No
		3	AP-1015	Yes
		…	…	…
		n	未使用	—
	フリーエリア	1	F-0325	Yes
		2	F-7485	Yes
		3	未使用	—
		…	…	…
		m	未使用	—
配置可能アプリケーション領域		1	AP-4125	—
		2	F-5963	—
		3	AP-3021	—
		4	AP-4513	—
		5	未使用	—
		6	未使用	—
		7	未使用	—
		8	未使用	—
		9	未使用	—
		…	…	…

【図４０】



【図４１】

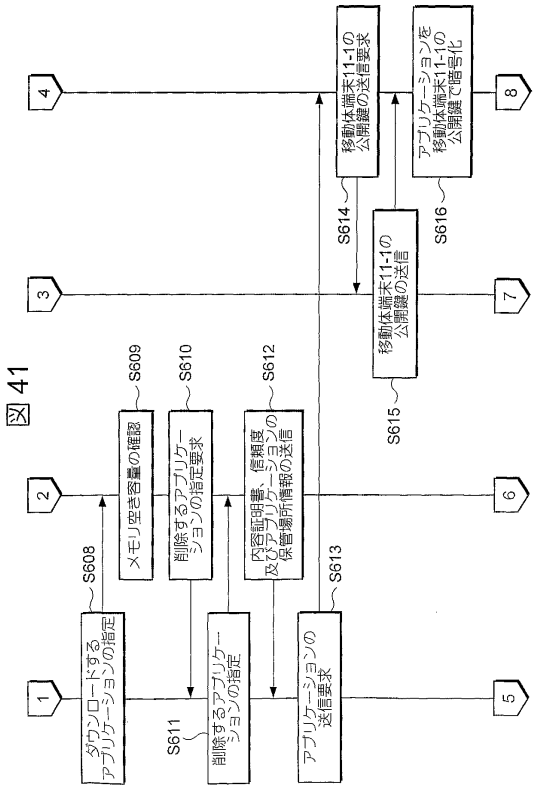


図41
1
2
3
4
5
6
7
8
ダウンロードするアプリケーションの指定
S608
メモリ空き容量の確認
S609
削除するアプリケーションの指定要求
S610
削除するアプリケーションの指定
S611
内容証明書、信頼度及びアプリケーションの保管場所情報の送信
S612
アプリケーションの送信要求
S613
移動体端末11-1の公開鍵の送信要求
S614
移動体端末11-1の公開鍵の送信
S615
アプリケーションを移動体端末11-1の公開鍵で暗号化
S616

【図４２】

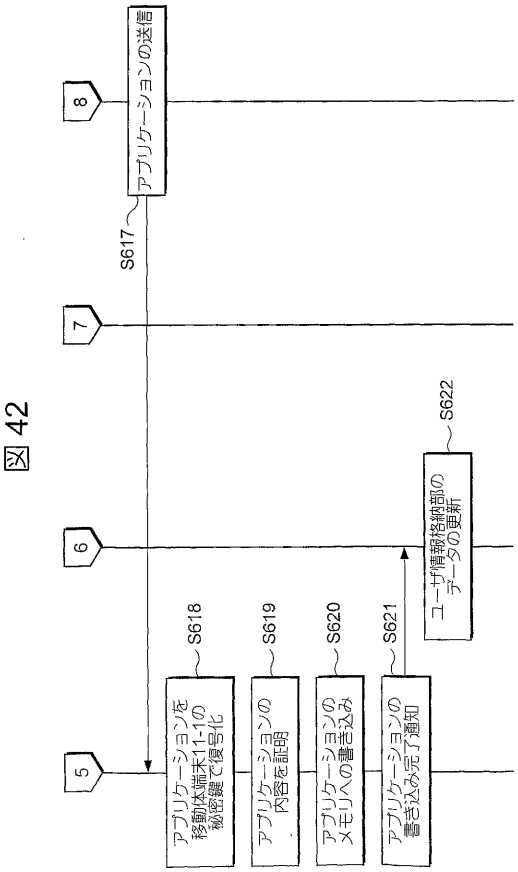


図42
5
6
7
8
アプリケーションの送信
S617
アプリケーションを移動体端末11-1の秘密鍵で復号化
S618
アプリケーションの内容を証明
S619
アプリケーションのメモリへの書き込み
S620
アプリケーションの書き込み完了通知
S621
ユーザ情報格納部のデータの更新
S622

フロントページの続き

(72)発明者　鷲尾　諭
東京都千代田区永田町二丁目１１番１号　山王パークタワー　株式会社エヌ・ティ・ティ・ドコモ
知的財産部内
(72)発明者　川端　博史
東京都千代田区永田町二丁目１１番１号　山王パークタワー　株式会社エヌ・ティ・ティ・ドコモ
知的財産部内

審査官　宮司　卓佳

(56)参考文献　特開２０００－０１０７８２（ＪＰ，Ａ）
特開平１０－０６９３８２（ＪＰ，Ａ）
特開平０９－２４４９００（ＪＰ，Ａ）
特開２００１－１２５７９１（ＪＰ，Ａ）
特開平０６－５００８７８（ＪＰ，Ａ）
特開２０００－３０５７７６（ＪＰ，Ａ）
特開平１０－２６０８７３（ＪＰ，Ａ）
特開平１１－２１２７７０（ＪＰ，Ａ）
特開２００１－０６７２２５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/22
G06F　 9/445
H04Q　 7/38