(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-79912
(P2005-79912A)
(43)公開日　平成17年3月24日(2005.3.24)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/10	H04L 9/00	621A	5B017
G06F 12/14	G06F 12/14	320A	5B058
G06K 17/00	G06K 17/00	S	5J104
G09C 1/00	G09C 1/00	640D	
	G09C 1/00	660A	

審査請求 未請求　請求項の数 28　ＯＬ　（全 53 頁）

(21)出願番号　特願2003-307863(P2003-307863)
(22)出願日　平成15年8月29日(2003.8.29)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100105050
弁理士　鷲田　公一
(72)発明者　中　健
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　高山　久
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　竹川　視野
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

Ｆターム(参考)　5B017 AA07　BA09　BB09　CA14

最終頁に続く

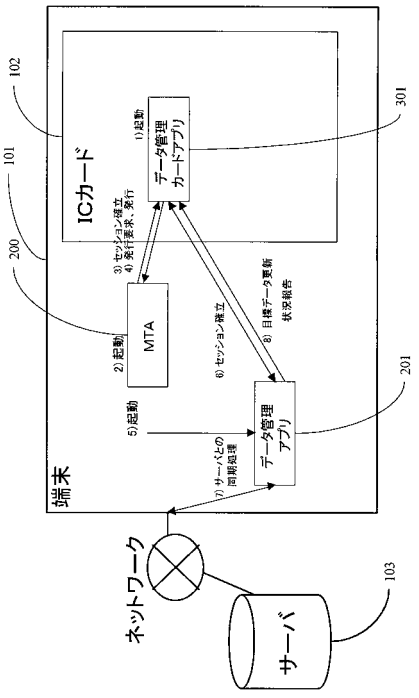
(54)【発明の名称】セキュアデータ管理装置

(57)【要約】

【課題】　情報処理端末上での、サーバとの同期処理の信頼性と確実性の向上、データの安全性と時刻の信頼性の向上を図り、確実で、安全性の高いデータ管理を行うこと。

【解決手段】　ＩＣカード１０２上のデータ管理カードアプリ３０１が、端末１０１上で動作する端末アプリケーションであるＭＴＡ２００（Master Trusted Agent）を端末１０１に対して発行し、ＭＴＡ２００がサーバ１０３とのデータの同期処理を行う端末アプリケーションであるデータ管理アプリ２０１のコードに認証情報を埋め込んで起動し、その認証情報を基にデータ管理カードアプリ３０１がデータ管理アプリ２０１を認証し、データ管理アプリ２０１が同期処理の目標データをＩＣカード１０２に格納し、ＩＣカード１０２に格納した目標データに基づいてデータ管理アプリ２０１がサーバとの間で同期処理を行う。

【選択図】　図４



【特許請求の範囲】
【請求項１】
データの格納、演算を秘匿した状態で実行するセキュアデバイスと情報処理端末によって構成され、前記セキュアデバイスは、前記情報処理端末で動作するアプリケーションの起動を制御するアプリケーションであるＭＴＡ(Master Trusted Agent)を前記情報処理端末に対して発行するカード処理モジュールと、ＭＴＡを格納するカード記憶装置を備え、前記情報処理端末は、実データと前記実データの管理を行うデータ管理アプリを格納する記憶装置とを備え、前記情報処理端末は、前記セキュアデバイスから発行された前記ＭＴＡを起動して、前記ＭＴＡと前記カード処理モジュールとの間で認証処理を行い、前記セキュアデバイスによって認証されたＭＴＡが前記データ管理アプリを起動し、前記データ管理アプリが前記セキュアデバイスと認証処理を行い、サーバとの間で前記実データの同期処理を行うことを特徴とするセキュアデータ管理装置。
【請求項２】
前記ＭＴＡ、または、前記データ管理アプリは、前記情報処理端末に前記セキュアデバイスが装着されているかどうかを確認する調査手段を備え、前記セキュアデバイスが装着されていないことを確認すると、動作を終了することを特徴とする請求項１記載のセキュアデータ管理装置。
【請求項３】
前記カード記憶装置には、前記実データ及び前記データ管理アプリのハッシュ値がそれぞれ格納されており、前記実データまたは前記データ管理アプリが利用される際にそれぞれのハッシュ値を算出し、前記カード記憶装置に格納されたハッシュ値と比較することによって前記実データ及び前記データ管理アプリの改ざんを検出するデータ検証手段を備えることを特徴とする請求項１記載のセキュアデータ管理装置。
【請求項４】
前記データ管理アプリの前記データ検証手段は、同期処理によってサーバから受信した実データのハッシュ値を算出し、前記データ管理アプリの制御手段が、前記算出されたハッシュ値を、前記カード制御手段に送信し、前記カード制御手段が、前記制御手段から受信したハッシュ値を、前記カード記憶装置に格納することを特徴とする請求項３記載のセキュアデータ管理装置。
【請求項５】
前記データ管理アプリが、暗号化手段及び復号化手段を備え、前記実データは、前記カード記憶装置に格納された暗号鍵データを用いて、前記暗号化手段が暗号化した状態で、前記記憶装置に格納され、復号化する場合には、前記カード記憶装置に格納された暗号鍵データを用いて、前記復号化手段が復号することを特徴とする請求項１記載のセキュアデータ管理装置。
【請求項６】
前記カード記憶装置には、前記情報処理端末で起動すべきアプリケーションが記述された起動アプリリストデータが格納されており、前記起動アプリリストデータの中には、前記データ管理アプリが記述されており、前記ＭＴＡのアプリ操作手段が、前記起動アプリリストデータを参照し、常にデータ管理アプリが起動している状態に保つことを特徴とする請求項１記載のセキュアデータ管理装置。
【請求項７】
前記ＭＴＡのアプリ発行手段が前記記憶装置に格納されたデータ管理アプリに、前記セキュアデバイスと認証処理を行う認証情報を埋め込んで起動し、起動された前記データ管理アプリの制御手段が前記セキュアデバイスの認証手段と認証処理を行うことを特徴とする請求項１記載のセキュアデータ管理装置。
【請求項８】
前記データ管理アプリは、サーバとの前記実データの同期処理の内容を記述した目標データを生成決定する目標データ決定手段と、前記カード記憶装置に格納された前記目標データに基づき前記実データに対するサーバとの同期処理を行うデータ同期手段と、前記カ

ード記憶装置に格納された目標データに基づき、前記記憶装置に格納された実データの削除を行うデータ削除手段を備え、前記目標データ決定手段が生成した前記目標データを、前記データ管理アプリが備える制御手段が、前記カード制御手段に送信し、前記カード制御手段が、前記カード記憶装置に格納し、前記カード記憶装置に格納された目標データに基づき、前記データ同期手段が、サーバとの間で前記実データの同期処理を行い、前記データ削除手段が、前記記憶装置に格納された実データの削除を行うことを特徴とする請求項１記載のセキュアデータ管理装置。

【請求項９】

前記カード記憶装置には、前記実データの利用可能な期限を示す有効期限情報が格納されており、目標データ決定手段が、有効期限情報を基に、有効期限が過ぎた削除すべき前記実データを削除されるべきデータとして前記目標データに設定することを特徴とする請求項８記載のセキュアデータ管理装置。

【請求項１０】

ダウンロード、アップロード、削除といった同期処理の種類別の優先度と、各同期処理の種類毎のデータの優先度を記述したデータポリシーデータを前記カード記憶装置に格納し、前記目標データ決定手段が、前記データポリシーデータを基に、目標データを生成することを特徴とする請求項８記載のセキュアデータ管理装置。

【請求項１１】

前記目標データには、各同期処理が処理状況を示す情報が含まれており、前記制御手段が、同期の処理結果情報を前記カード制御手段に通知し、前記カード制御手段が、処理結果情報を基に、前記カード記憶装置に格納された前記目標データを更新することを特徴とする請求項８記載のセキュアデータ管理装置。

【請求項１２】

前記カード記憶装置には、緊急削除処理を促す緊急削除フラグが格納され、前記緊急削除フラグがＯＮの状態になっている場合には、優先的に削除処理を行う目標データを生成することを特徴とする請求項８記載のセキュアデータ管理装置。

【請求項１３】

前記情報処理端末上で動作するアプリケーションが、前記実データに対する参照を要求する場合に、前記データ管理アプリの前記復号化手段が復号した実データに対し、前記データ管理アプリの前記制御手段が、日時やユーザＩＤを電子透かしとして埋め込み、アプリケーションに前記実データを送信することを特徴とする請求項５記載のセキュアデータ管理装置。

【請求項１４】

データの格納、演算を秘匿した状態で実行するセキュアデバイスと情報処理端末によって構成され、前記セキュアデバイスは、前記情報処理端末で動作するアプリケーションの起動を制御するアプリケーションであるＭＴＡ(Master Trusted Agent)を前記情報処理端末に対して発行するカード処理モジュールと、ＭＴＡを格納するカード記憶装置を備え、前記ＭＴＡは、ネットワーク上のサーバから現在時刻を取得する時刻取得手段と、前記情報処理端末上での現在時刻をカウントする時刻カウント手段を備え、前記情報処理端末は、前記セキュアデバイスから発行された前記ＭＴＡを起動して、前記ＭＴＡと前記カード処理モジュールとの間で認証処理を行い、前記セキュアデバイスによって認証されたＭＴＡの前記時刻取得手段がサーバから現在時刻を取得し、前記時刻カウント手段に設定し、前記時刻カウント手段が、前記時刻カウント手段が示す時刻を現在時刻とすることを特徴とするセキュアデータ管理装置。

【請求項１５】

前記ＭＴＡの前記時刻取得手段がネットワーク上のサーバから複数回現在時刻を取得し、その取得した現在時刻の差分に基づく経過時間と、時刻カウント手段が示す経過時間を、前記ＭＴＡの制御手段が比較することにより、情報処理端末の時刻カウント手段が示す経過時間の正当性を判断し、不正と判断した場合には、前記情報処理端末で動作中のアプリケーションを停止することを特徴とする請求項１４記載のセキュアデータ管理装置。

【請求項１６】
前記セキュアデバイスが、時刻をカウントするカード時刻カウント手段を備え、前記ＭＴＡの制御手段が、前記セキュアデバイスの前記カード時刻カウント手段が示す経過時間と、前記情報処理端末の時刻カウント手段が示す経過時間を比較することにより、情報処理端末の時刻カウント手段が示す経過時間の正当性を判断し、不正と判断した場合には、前記情報処理端末で動作中のアプリケーションを停止することを特徴とする請求項１４記載のセキュアデータ管理装置。
【請求項１７】
前記ＭＴＡの時刻取得手段がネットワーク上のサーバから現在時刻を取得した際に、カード制御手段がカード記憶装置に前記サーバから取得した現在時刻を格納しておき、ＭＴＡが新たに起動した際に、時刻取得手段がネットワーク上のサーバから現在時刻を取得できなかった場合に、前記カード記憶装置に格納した現在時刻と、前記情報処理端末の前記時刻カウント手段が示す現在時刻を、前記ＭＴＡの制御手段が比較することで、情報処理端末の時刻カウント手段が示す現在時刻の正当性を確認し、不正と判断した場合には、前記情報処理端末で動作中のアプリを停止することを特徴とする請求項１４記載のセキュアデータ管理装置。
【請求項１８】
前記ＭＴＡのネットワーク上のサーバから現在時刻情報を取得する時刻取得手段が、時刻情報の取得を失敗した場合に、前記ＭＴＡの制御手段は、カード制御手段に失敗したことを通知し、カード制御手段は、失敗回数をカード記憶装置に格納し、許容回数を越えると前記情報処理端末で動作するアプリを停止することを特徴とする請求項１４記載のセキュアデータ管理装置。
【請求項１９】
データの格納、演算を秘匿した状態で実行するセキュアデバイスと情報処理端末によって構成され、前記セキュアデバイスは、前記情報処理端末で動作するアプリケーションの起動を制御するアプリケーションであるＭＴＡ(Master Trusted Agent)を前記情報処理端末に対して発行するカード処理モジュールと、ＭＴＡと、実データと、前記実データの管理を行うデータ管理アプリを格納するセキュア記憶装置を備え、前記情報処理端末は、前記セキュアデバイスから発行された前記ＭＴＡを起動して前記ＭＴＡと前記カード処理モジュールとの間で認証処理を行い、前記セキュアデバイスによって認証されたＭＴＡが前記データ管理アプリを起動し、前記データ管理アプリが前記セキュアデバイスと認証処理を行い、サーバとの間で前記実データの同期処理を行うことを特徴とするセキュアデータ管理装置。
【請求項２０】
前記ＭＴＡ、または、前記データ管理アプリは、前記情報処理端末に前記セキュアデバイスが装着されているかどうかを確認する調査手段を備え、前記セキュアデバイスが装着されていないことを確認すると、動作を終了することを特徴とする請求項１９記載のセキュアデータ管理装置。
【請求項２１】
前記セキュア記憶装置には、前記情報処理端末処理モジュールで起動すべきアプリケーションが記述された起動アプリリストデータが格納されており、前記起動アプリリストデータの中には、前記データ管理アプリが記述されており、前記ＭＴＡのアプリ操作手段が、前記起動アプリリストデータを参照し、常にデータ管理アプリが起動している状態に保つことを特徴とする請求項１９記載のセキュアデータ管理装置。
【請求項２２】
前記ＭＴＡのアプリ発行手段が前記セキュア記憶装置に格納されたデータ管理アプリに、前記セキュアデバイスと認証処理を行う認証情報を埋め込んで起動し、起動された前記データ管理アプリの制御手段が前記セキュアデバイスの認証手段と認証処理を行うことを特徴とする請求項１９記載のセキュアデータ管理装置。
【請求項２３】

前記データ管理アプリは、サーバとの前記実データの同期処理の内容を記述した目標データを生成する目標データ決定手段と、前記セキュア記憶装置に格納された前記目標データに基づき前記実データに対するサーバとの同期処理を行うデータ同期手段と、前記セキュア記憶装置に格納された目標データに基づき、前記セキュア記憶装置に格納された実データの削除を行うデータ削除手段を備え、前記目標データ決定手段が生成した前記目標データを、前記データ管理アプリが備える制御手段が、前記カード制御手段に送信し、前記カード制御手段が、前記セキュア記憶装置に格納し、前記セキュア記憶装置に格納された目標データに基づき、前記データ同期手段が、サーバとの間で前記実データの同期処理を行い、前記データ削除手段が、前記セキュア記憶装置に格納された実データの削除を行うことを特徴とする請求項１９記載のセキュアデータ管理装置。

【請求項２４】

前記セキュア記憶装置には、前記実データの利用可能な期限を示す有効期限情報が格納されており、目標データ決定手段が、有効期限情報を基に、有効期限が過ぎた実データを削除されるべきデータとして前記目標データに設定することを特徴とする請求項２３記載のセキュアデータ管理装置。

【請求項２５】

ダウンロード、アップロード、削除といった同期処理の種類別の優先度と、各同期処理の種類毎のデータの優先度を記述したデータポリシーデータを前記セキュア記憶装置に格納し、前記目標データ決定手段が、前記データポリシーデータを基に、目標データを生成することを特徴とする請求項２３記載のセキュアデータ管理装置。

【請求項２６】

前記目標データには、各同期処理が処理状況を示す情報が含まれており、前記制御手段が、同期の処理結果情報を前記カード制御手段に通知し、前記カード制御手段が、処理結果情報を基に、前記セキュア記憶装置に格納された前記目標データを更新することを特徴とする請求項２３記載のセキュアデータ管理装置。

【請求項２７】

前記セキュア記憶装置には、緊急削除処理を促す緊急削除フラグが格納され、前記緊急削除フラグがＯＮの状態になっている場合には、優先的に削除処理を行う目標データを生成することを特徴とする請求項２３記載のセキュアデータ管理装置。

【請求項２８】

前記情報処理端末上で動作するアプリケーションが、前記実データに対する参照を要求する場合に、実データに対し、前記データ管理アプリの前記制御手段が、日時やユーザＩＤを電子透かしとして埋め込み、アプリケーションに前記実データを送信することを特徴とする請求項１９記載のセキュアデータ管理装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、データをセキュアに保持するＩＣカード等のセキュアデバイスと、そのセキュアデバイスを搭載する携帯電話やＰＤＡ（Personal Digital Assistant）、パーソナルコンピュータなどの情報処理端末に関する。

【背景技術】

【０００２】

従来から、コンピューターや携帯用の端末装置を利用してフィールドでの営業活動を支援するためのシステムが広く利用されている。その様な中で、データベースサーバとオンライン接続するための通信コストの節約と、オフライン環境下での利便性から、携帯用の端末装置に、データベースの一部を保存し、オフライン環境下でも営業支援活動が行えるようにしたものが普及しつつある。その一例として、特許文献１に挙げた先行技術がある。この先行技術のブロック構成図を図４５に示す。ホストマシン２と携帯端末装置３に、企業情報記憶部６a、１４を備えており、記憶した営業情報を相互交換可能となるように編成されている。ホストマシン２は、営業支援活動で利用する営業情報を企業情報記憶部

６aに保持している。携帯端末装置３は、フロッピー（Ｒ）などの外部記憶媒体４を介して、ホストマシン２と同期処理を行い、ホストマシン２の企業情報記憶部６aの営業情報を、携帯端末装置３の企業情報記憶部１４に保存する。携帯端末装置３は、企業情報記憶部１４を参照することで、単独でも、営業情報を参照し、営業支援活動に利用することが可能である。また、この先行技術を応用して、ホストマシンと携帯端末装置との間を、外部記憶媒体の代わりにネットワークで結び、ホストマシンと携帯端末装置との間で同期処理を行って、ホストマシンの企業情報記憶部に保存された営業情報の一部を携帯端末装置の企業情報記憶部に保存し、携帯端末装置は企業情報記憶部に保存された営業情報を参照することで、オフラインでも営業支援活動を行うことが出来る。

【特許文献１】特開平１１－１７５５９６号公報

【発明の開示】

【発明が解決しようとする課題】

【０００３】

しかしながら、この場合、携帯端末装置上には顧客リストなどの営業情報も格納されるため、例えば、携帯端末装置の盗難や紛失によって顧客データが外部に流出する場合や、携帯端末装置を管理する社員が意図的に機密情報を流出する場合など、大きな損害を被る場合があった。また、不正なアプリケーションのなりすましによって、同期処理などが確実に行えない場合があった。また、同期処理が確実に行えたとしても、古いデータをあらかじめコピーしておき、新しいデータとすり替え、削除されるはずの古いデータを参照させて、顧客情報を参照されてしまう場合があった。また、同期処理の際に利用する現在時刻を、端末の時計を戻すことによって、有効期限が切れていないものとして、処理がなされ、有効期限の切れたデータやアプリケーションを使い続けることが可能になるなどの問題に対処できなかった。

【０００４】

この発明はこのような実状に鑑みてなされたものであり、処理の信頼性、確実性、データの安全性、時刻の信頼性の向上を図り、より確実、安全、信頼できるデータの管理を行うことを目的とする。

【課題を解決するための手段】

【０００５】

上記課題を解決するために本発明は、第一に、データの格納、演算を秘匿した状態で実行するセキュアデバイスと情報処理端末によって構成され、セキュアデバイスは、情報処理端末で動作するアプリケーションの起動を制御するアプリケーションであるＭＴＡ(Master Trusted Agent)を情報処理端末に対して発行するカード処理モジュールと、ＭＴＡを格納するカード記憶装置を備え、情報処理端末は、実データと前記実データの管理を行うデータ管理アプリを格納する記憶装置とを備え、セキュアデバイスから発行された前記ＭＴＡを起動して、ＭＴＡと前記カード処理モジュールとの間で認証処理を行い、セキュアデバイスによって認証されたＭＴＡがデータ管理アプリを起動し、データ管理アプリが前記セキュアデバイスと認証処理を行い、サーバとの間で実データの同期処理を行う。これにより安全で、信頼性の高いデータ管理が行える。

【０００６】

本発明は、第二に、データ管理アプリは、サーバとの実データの同期処理の内容を記述した目標データを生成決定する目標データ決定手段と、カード記憶装置に格納された目標データに基づき実データに対するサーバとの同期処理を行うデータ同期手段と、カード記憶装置に格納された目標データに基づき、記憶装置に格納された実データの削除を行うデータ削除手段を備え、目標データ決定手段が生成した目標データを、データ管理アプリが備える制御手段が、カード制御手段に送信し、カード制御手段が、カード記憶装置に格納し、カード記憶装置に格納された目標データに基づき、データ同期手段が、サーバとの間で実データの同期処理を行い、データ削除手段が、記憶装置に格納された実データの削除を行う。これにより信頼できるデータ管理アプリが、データの同期処理を行うので、安全で、信頼性の高いデータ管理が行える。

【０００７】
本発明は、第三に、カード記憶装置には、実データの利用可能な期限を示す有効期限情報が格納されており、目標データ決定手段が、有効期限情報を基に、有効期限が過ぎた実データを削除されるべきデータとして目標データに設定する。これにより、データの有効期限を信頼できるデータ管理アプリが管理することで、安全で、信頼性の高いデータ管理が行える。
【０００８】
本発明は、第四に、ダウンロード、アップロード、削除といった同期処理の種類別の優先度と、各同期処理の種類毎のデータの優先度を記述したデータポリシーデータをカード記憶装置に格納し、目標データ決定手段が、データポリシーデータを基に、目標データを生成する。これにより、例えば、機密レベルの高い実データから優先的に削除する設定にしておくことで、データ管理の安全性が向上する。また、サーバが接続するたびに更新するデータを決定し、同期処理を主導的に行う場合に比べ、情報処理端末が目標データを決定し、同期処理を行うので、サーバの負荷が低減できる。
【０００９】
本発明は、第五に、セキュアデバイスが、時刻をカウントするカード時刻カウント手段を備え、ＭＴＡの制御手段が、セキュアデバイスのカード時刻カウント手段が示す経過時間と、情報処理端末の時刻カウント手段が示す経過時間を比較することにより、情報処理端末の時刻カウント手段が示す経過時間の正当性を判断し、不正と判断した場合には、情報処理端末で動作中のアプリケーションを停止する。これにより、情報処理端末の時刻の改変による不正行為を防ぐことができる。
【００１０】
本発明は、第六に、ＭＴＡの時刻取得手段がネットワーク上のサーバから現在時刻を取得した際に、カード制御手段がカード記憶装置にサーバから取得した現在時刻を格納しておき、ＭＴＡが新たに起動した際に、時刻取得手段がネットワーク上のサーバから現在時刻を取得できなかった場合に、カード記憶装置に格納した現在時刻と、情報処理端末の時刻カウント手段が示す現在時刻を、ＭＴＡの制御手段が比較することで、情報処理端末の時刻カウント手段が示す現在時刻の正当性を確認し、不正と判断した場合には、情報処理端末で動作中のアプリを停止する。これにより、情報処理端末の時刻の改変による不正行為を防ぐことができる。
【００１１】
本発明は、第七に、ＭＴＡのネットワーク上のサーバから現在時刻情報を取得する時刻取得手段が、時刻情報の取得を失敗した場合に、ＭＴＡの制御手段は、カード制御手段に失敗したことを通知し、カード制御手段は、失敗回数をカード記憶装置に格納し、許容回数を越えると情報処理端末で動作するアプリを停止する。これにより、情報処理端末の時計の改変による不正行為を防ぐことができる。
【００１２】
本発明は、第八に、データの格納、演算を秘匿した状態で実行するセキュアデバイスと情報処理端末によって構成され、セキュアデバイスは、情報処理端末で動作するアプリケーションの起動を制御するアプリケーションであるＭＴＡ(Master Trusted Agent)を情報処理端末に対して発行するカード処理モジュールと、ＭＴＡと、実データと、実データの管理を行うデータ管理アプリを格納するセキュア記憶装置を備え、情報処理端末は、セキュアデバイスから発行されたＭＴＡを起動してＭＴＡとカード処理モジュールとの間で認証処理を行い、セキュアデバイスによって認証されたＭＴＡがデータ管理アプリを起動し、データ管理アプリがセキュアデバイスと認証処理を行い、サーバとの間で実データの同期処理を行う。これにより安全で、信頼性の高いデータ管理が行える。
【発明の効果】
【００１３】
以上説明したように本発明のセキュアデータ管理装置を利用することで、情報処理端末上で動作する、セキュアデバイスと信頼関係のあるアプリケーションを利用することで、

同期処理、データの改ざん検出、データの緊急削除、有効期限の切れたデータの削除、データに対する参照、現在時刻の取得や計測を、信頼ある状態で安全かつ確実に行える。

【発明を実施するための最良の形態】

【００１４】

以下、本発明の実施の形態を、図面を参照しながら説明する。

【００１５】

（実施の形態１）

本発明の実施の形態１におけるセキュアデータ管理装置を示すシステム構成を図１に示す。

【００１６】

セキュアデータ管理装置は、端末１０１、ＩＣカード１０２、サーバ１０３から構成されている。セキュアデータ管理装置は、端末１０１で利用されるデータを、安全に管理するための装置である。端末１０１は、複数台存在しても良い。

【００１７】

セキュアデータ管理装置の処理概要を図４に示す。

【００１８】

セキュアデータ管理装置は、ＩＣカード１０２が、信頼できるアプリケーションであるＭＴＡ２００を端末１０１上で起動し、さらに、ＭＴＡ２００(Master Trusted Agentの略である。以下では、ＭＴＡとする）が端末１０１上で信頼できるアプリケーションを動作させるという仕組みを利用している。本特許では、端末１０１上で起動するアプリケーションとして、データ管理アプリ２０１が起動する（ＭＴＡ２００を利用した信頼できるアプリケーションの起動に仕組みについては後で詳しく説明する）。

【００１９】

データ管理アプリ２０１は、ＩＣカード１０２とデータベースサーバが稼動するサーバ１０３とそれぞれ通信し、端末１０１上で、端末上のデータの同期を行うアプリケーションである。扱うデータの具体例としては、例えば、端末が営業支援用端末の場合には、顧客リストや、契約情報、価格表などが想定され、端末が情報家電端末の場合には、音楽や動画などのコンテンツなどが想定される。

【００２０】

以下、処理フローについて述べる。

【００２１】

端末１０１の電源をオンにし、ＩＣカード１０２を挿入、または、ＩＣカード１０２が既に装着されていると、まず、端末１０１によってＩＣカード１０２のデータ管理カードアプリ３０１が選択されて、データ管理カードアプリ３０１が起動する（図４の1)）。

【００２２】

すると、データ管理カードアプリ３０１は端末１０１にＭＴＡ２００を発行し、ＭＴＡ２００のコードを受信した端末１０１では、データ管理カードアプリ３０１から発行されたＭＴＡ２００が起動する（図４の2)）。ＭＴＡ２００は、データ管理カードアプリ３０１と認証を行い、信頼できるセッションを確立する（図４の3)）。

【００２３】

次に、ＭＴＡ２００は、端末１０１の状態を調べる。この場合、データ管理アプリ２０１は、起動していないので、ＭＴＡ２００は、データ管理カードアプリ３０１に、データ管理アプリ２０１の発行要求を出す。データ管理カードアプリ３０１は、ＭＴＡ２００に対して、データ管理アプリ２０１を発行する（図４の4)）。それを受信したＭＴＡ２００は、データ管理アプリ２０１を起動する（図４の5)）。その際、データ管理アプリ２０１は、データ管理カードアプリ３０１と認証を行い、信頼できるセッションを確立する（図４の6)）。

【００２４】

起動したデータ管理アプリ２０１は、必要に応じて、サーバ１０３との間で、同期の前処理及び同期処理を行う（図４の7)）。データ管理アプリ２０１は、同期の前処理及び同

期処理の結果を、データ管理カードアプリ３０１に対して通知する（図４の8)）。
【００２５】
以上が、セキュアデータ管理装置の処理概要である。以上の処理は四つのタイミングで行われる。例えば、１日１回午前９時に行うといった設定をしておき、定期的に行う場合や、端末１０１でのアプリケーションの動作状況を見てＣＰＵ負荷率の低い時に行う場合や、端末１０１にＩＣカード１０２を挿入した場合や、ユーザがＧＵＩから同期ボタン（同期処理開始を要求するボタン）を押して処理開始を要求した場合である。
【００２６】
次に、端末１０１の内部構成について説明する。
【００２７】
端末１０１は、図１に示すように処理モジュール１０４、記憶装置１０５から構成されている。
【００２８】
端末１０１は、ＩＣカード等のセキュアデバイスを搭載可能な携帯電話、パーソナルコンピュータを想定している。
【００２９】
携帯電話の場合、例えば、端末１０１の処理モジュール１０４は、ＣＰＵとＲＯＭとＲＡＭと、外部と通信するためのアンテナ、ＲＦ部、無線通信制御回部、ＩＣカード１０２と通信するためのスロットを備えている。記憶装置としては、フラッシュメモリなどを備えている。ＲＯＭには、ＯＳやＪａｖａ（Ｒ）ＶＭなどのソフトウェアが格納され、それらが、ＲＡＭを用いてＣＰＵ上で実行されることによって、各種のアプリケーションを実行する処理モジュール１０４が実現される。
【００３０】
パーソナルコンピュータの場合、端末１０１の処理モジュール１０４は、ＣＰＵと、記憶メモリと、外部との通信するためのモデムや、ネットワークカード、ＩＣカード１０２を装着、通信するためのＰＣＩカード、ＳＤカードなどのスロットを備えている。記憶装置としては、ＨＤＤを備えている。ＲＯＭおよびＨＤＤには、ＯＳやＪａｖａ（Ｒ）ＶＭなどのソフトウェアが格納され、それらが、ＲＡＭを用いてＣＰＵ上で実行されることによって、各種のアプリケーションを実行する処理モジュール１０４が実現される。
【００３１】
次に、ＩＣカード１０２の内部構成について説明する。
【００３２】
ＩＣカード１０２は、図１に示すようにカード処理モジュール１０６、カード記憶装置１０７から構成されている。
【００３３】
ＩＣカード１０２のカード処理モジュール１０６は、ＣＰＵとＲＯＭ、ＲＡＭと端末と通信するためのホストＩ／Ｆから構成され、カード記憶装置１０７は、ＥＥＰＲＯＭなどの不揮発性メモリによって構成され、ＩＣカード１０２は全体として耐タンパ性を備え、外部からＩＣカードの内部に直接アクセスできないようになっている。
【００３４】
サーバ１０３は、サーバコンピュータ装置であり、アプリケーションとしてデータベースサーバが稼動している。
【００３５】
本発明の実施形態1におけるセキュアデータ管理装置を示すブロック図を図２、３に示す。
【００３６】
図２は、端末１０１のブロック図である。図３は、ＩＣカード１０２のブロック図である。
【００３７】
処理モジュール１０４は、様々なアプリケーション（以下アプリと略す）を実行する機

能、ネットワークを通してサーバ１０３と通信する機能、ＩＣカード１０２と通信する機能を備えている。

【００３８】

実施の形態１では、処理モジュール１０４で、アプリとしてＭＴＡ２００とデータ管理アプリ２０１を実行する。

【００３９】

ＭＴＡ２００は、ＩＣカード１０２が信頼できるアプリとして端末１０１上で動作し、端末１０１の状態に応じて、アプリの起動、信頼できる時刻の取得、計測を行う。

【００４０】

ＭＴＡ２００は、アプリ操作手段２０３、調査手段２０４、制御手段２０５、時刻取得手段２０６、時刻カウント手段２０７、アプリ発行手段２１８、復号化手段２１９、データ検証手段２２０から構成されている。

【００４１】

ＭＴＡ２００については、後で詳しく説明する。

【００４２】

データ管理アプリ２０１は、ＭＴＡ２００によって起動され、ＩＣカード１０２が信頼できるアプリとして、端末１０１上で動作し、サーバ１０３と通信してデータの同期、端末１０１上のデータの管理を行う。

【００４３】

データ管理アプリ２０１は、データ同期手段２０８、データ削除手段２０９、データ検証手段２１０、目標データ決定手段２１１、調査手段２１２、制御手段２１３、暗号化手段２１４、復号化手段２１５から構成されている。

【００４４】

記憶装置１０５は、データを保存するための装置である。

【００４５】

実施の形態１では、記憶装置１０５は、データ管理アプリ２０１が管理する実データ２１６と、データ管理アプリ２０１の実行コードであるデータ管理アプリデータ２１７を、保存している。

【００４６】

カード処理モジュール１０６は、ＩＣカード１０２上で様々なアプリを実行する機能、端末１０１と通信する機能を備えている。

【００４７】

実施の形態１では、カード処理モジュール１０６は、カードアプリとして、データ管理カードアプリ３０１を実行する。

【００４８】

データ管理カードアプリ３０１は、アプリ発行手段３０２、認証手段３０３、カード制御手段３０４、カード時刻カウント手段３１４から構成されている。

【００４９】

カード記憶装置１０７は、ＩＣカード１０２上に、データを保存するための装置である。

【００５０】

実施の形態１では、カード記憶装置１０７に、構成データ３０５、目標データ３０６、起動アプリリストデータ３０７、前回更新日時データ３０８、ＭＴＡデータ３０９、データポリシーデータ３１１、鍵データ３１２、時刻データ３１３を保存している。

【００５１】

次に、データについて、説明する。

【００５２】

実データ２１６は、本特許のセキュアデータ管理装置によって安全に管理されるデータのことである。実データ２１６は、データ管理アプリ２０１によって管理され、記憶装置１０５に保存されている時は、暗号化されていて、ＩＤで管理され、複数存在する。デー

タの具体的内容としては、顧客リスト、契約情報、価格表、業務マニュアル、アプリケーションなどのデータである。

【００５３】

データ管理アプリデータ２１７は、端末１０１の処理モジュール１０４上で動作するアプリであるデータ管理アプリ２０１の起動前のデータ（実行コード）であり、暗号化されて、記憶装置１０５に保存されている。

【００５４】

構成データ３０５は、実データ２１６とデータ管理アプリデータ２１７に関する情報を記したデータである。構成データ３０５には、どの実データ２１６についての情報であるかを示す識別子ＩＤと、実データ２１６を暗号化する時に利用した鍵を示す情報と、実データ２１６から算出したハッシュ値と、データの種類を示す種別情報と、その実データ２１６の有効期限を示す情報と、その実データ２１６を更新した日時情報と、更新した方法が記されている。

【００５５】

構成データ３０５の具体例を、図１６、１７、１８、１９、２０を用いて説明する。

【００５６】

図１６は、構成データに記載されている各項目の内容を示している。項目としては、ＩＤ、対応鍵番号、ハッシュ値、種別、有効期限、更新日時がある。それぞれの括弧内の数字は、データで表現する場合の値である。

【００５７】

例えば、図１７に示すような内容を実際のデータで表現すると、図１９になり、図１８に示すような内容を実際のデータで表現すると、図２０になる。

【００５８】

本実施の形態では、実データ２１６を端末１０１の記憶装置１０５に保存し、構成データ３０５をＩＣカード１０２のカード記憶装置１０７に保存している。

【００５９】

従来、端末１０１上に保存していたデータを、古いデータとすり替えた場合に、改ざんの検出すらできなかったことに鑑みて、必要最低限のデータのみ、耐タンパなＩＣカード１０２に保存し、利用することによって、改ざんを検出できる仕組みにしている。

【００６０】

目標データ３０６は、同期処理の対象となるデータと同期処理の状態を管理するデータであり、同期、削除を行う時に対象となるデータの識別子ＩＤと、処理が完了したかどうかを示す情報と、処理を開始した日時情報と、処理を中断した日時情報と、処理が終了した日時情報とを処理毎に記録したデータである。

【００６１】

目標データ３０６の具体例を、図２１、２２、２３を用いて説明する。

【００６２】

図２１は、目標データに記載されている各項目の内容を示している。項目としては、処理名、実データのＩＤ（ここの内容には、処理状況も表現される）、開始日時、中断日時、終了日時がある。それぞれの括弧内の数字は、データで表現する場合の値である。

【００６３】

例えば、図２２に示すような内容を実際のデータで表現すると、図２３になる。

【００６４】

起動アプリリストデータ３０７は、端末１０１が起動している際に、処理モジュール１０４で起動しておくべきアプリのリストを示すデータである。

【００６５】

また、起動アプリリストデータ３０７には、緊急時に行うデータの削除を行うべきかどうかを示す緊急削除フラグ情報も示されている。

【００６６】

起動アプリリストデータ３０７の具体例を、図２４、２５、２６を用いて説明する。

【００６７】
図２４は、起動アプリリストデータに記載されている各項目の内容を示している。項目としては、緊急削除フラグ、起動アプリ名がある。それぞれの括弧内の数字は、データで表現する場合の値である。
【００６８】
例えば、図２５に示すような内容を実際のデータで表現すると、図２６になる。
【００６９】
端末１０１上で起動すべきアプリをＩＣカード１０２で管理し、ＭＴＡ２００が、端末１０１の状態に応じて必要なアプリを起動することで、端末１０１でのデータ管理のための処理が確実に実行される。
【００７０】
前回更新日時データ３０８は、目標データ３０６を前回いつ決定したかを示す日時情報を記すデータである。一度サーバ１０３から取得した更新情報を接続のたびに、取得しなおさなくてよいため、通信コストの軽減を図ることができる。また、前回からの更新分だけを調べればよいため、目標決定の処理も速く行うことができる。
【００７１】
前回更新日時データ３０８の具体例を、図２７、２８、２９を用いて説明する。
【００７２】
図２７は、前回更新日時データに記載されている各項目の内容を示している。項目としては、前回更新日時がある。それぞれの括弧内の数字は、データで表現する場合の値である。
【００７３】
例えば、図２８に示すような内容を実際のデータで表現すると、図２９になる。
【００７４】
ＭＴＡデータ３０９は、端末１０１の処理モジュール１０４上で動作するアプリであるＭＴＡ２００の元のデータ（実行コード）である。データ管理カードアプリ３０１が、ＭＴＡデータ３０９から端末１０１に対してＭＴＡを発行することによって、ＭＴＡ２００が起動される。
【００７５】
データポリシーデータ３１１は、各処理の際の実データに対する優先度の情報と、削除と同期のような複数の処理を、同一の実データ２１６に対して行う衝突状態になった場合の優先基準情報を記すデータである。
【００７６】
データポリシーデータ３１１の具体例を、図１３、１４、１５を用いて説明する。
【００７７】
図１３は、データポリシーデータに記載されている各項目の内容を示している。項目としては、処理名、最優先データ、それ以外の決定基準、削除と更新での目標データ衝突の場合の優先基準、更新と更新での目標データ衝突の場合の優先基準がある。それぞれの括弧内の数字は、データで表現する場合の値である。
【００７８】
データポリシーデータに基づき、複数ある実データ２１６に対する処理の順番が決定される。例えば、データポリシーデータを、機密レベルの高い実データから優先的に削除する設定にしておくことで、データ管理の安全性が向上する。
【００７９】
また、サーバが接続するたびに更新するデータを決定し、同期処理を主導的に行う場合に比べ、情報処理端末が目標データを決定し、同期処理を行うので、サーバの負荷が低減できる。
【００８０】
例えば、図１４に示すような内容を実際のデータで表現すると、図１５になる。
【００８１】

鍵データ３１２は、実データ２１６を暗号化または復号化するための共通鍵暗号方式に基く暗号鍵である。複数ある場合には、それぞれの鍵に番号を付け、番号で管理している。

【００８２】

時刻データ３１３には、時刻取得手段２０６がサーバから取得した時刻情報、または、時刻カウント手段２０７が、カウントした時刻情報が保存されている。また、時刻データ３１３には、時刻情報のサーバからの取得に連続して失敗した回数と、その回数の許容最大値が記録されている。

【００８３】

次に、それぞれの手段について説明する。

【００８４】

アプリ操作手段２０３は、端末１０１上で、ＭＴＡ以外のアプリの起動処理を行う手段であり、端末のＯＳとの間でアプリ発行手段２１８が発行したアプリの起動処理を行う。

【００８５】

調査手段２０４は、起動アプリリストデータ３０７を参照して、起動すべきアプリの現在の状態、起動している、起動していないなどを調べる手段である。

【００８６】

制御手段２０５は、調査手段２０４の調査状況報告と、起動アプリリストデータ３０７を基に起動すべきアプリを決定行う手段である。また、制御手段２０５は、ＭＴＡ自体に埋め込まれた認証用の鍵を取得する手段である。また制御手段２０５は、ネットワークを利用するためにプロバイダ、データベースサーバなどに接続するための手段である。

【００８７】

時刻取得手段２０６は、ネットワーク上の信頼できる時刻を保持しているサーバから、時刻を取得する手段である。また、時刻取得手段２０６は、その取得した時刻を、時刻カウント手段２０７とＩＣカード１０２に通知する。

【００８８】

時刻カウント手段２０７は、時刻取得手段２０６からの通知時刻を基に、現在時刻を計測する手段である。また、時刻カウント手段２０６は、その計測した時刻を、ＩＣカード１０２に通知する。

【００８９】

アプリ発行手段２１８は、端末１０１上で起動するアプリデータのコードにセッション鍵を埋め込む手段である。

【００９０】

復号化手段２１９は、鍵データ３１２を利用して、データを復号化する手段である。

【００９１】

データ検証手段２２０は、データのハッシュ値を計算し、さらに必要な場合には、構成データ３０５に記録してあるハッシュ値と比較し、データの改ざんを検証する手段である。

【００９２】

データ同期手段２０８は、サーバ１０３と通信し、目標データ３０６を基に、実データ２１６、データ管理アプリデータ２１７、起動アプリリストデータ３０７、ＭＴＡデータ３０９、データポリシーデータ３１１、などのデータのアップロード、ダウンロードを行う。また、データ同期手段２０８は、処理状況をＩＣカード１０２に通知する。

【００９３】

データ削除手段２０９は、目標データ３０６を基に、実データ２１６、データ管理アプリデータ２１７の削除を行う。また、データ削除手段２０９は、処理状況をＩＣカード１０２に通知する。

【００９４】

データ検証手段２１０は、データのハッシュ値を計算し、さらに必要な場合には、構成データ３０５に記録してあるハッシュ値と比較し、実データ２１６の改ざんを検証する手

段である。信頼できるハッシュ値の計算を、端末１０１上で行えるのは、本特許の特徴の一つである。

【００９５】

目標データ決定手段２１１は、サーバ１０３と通信し、前回更新日時データ３０８と、サーバ１０３のデータの更新情報と、構成データ３０５の更新日時データ、有効期限、データポリシーデータ３１１、目標データ３０６を基に、ダウンロード、アップロード、削除すべきデータを決定する手段である。また、目標データ決定手段２１１は、決定した目標データ３０６をＩＣカード１０２に通知する。

【００９６】

調査手段２１２は、端末１０１の状況情報として、記憶装置１０５の残り記憶容量、ＣＰＵ負荷率などを調べ、制御手段２１３に通知する手段である。

【００９７】

データ管理アプリ２０１の制御手段２１３は、調査手段２１２からの通知情報と、目標データ３０６に基づき、データ管理アプリ２０１の動作を決定する手段である。

【００９８】

また、制御手段２１３は、データ管理アプリ２０１が備える手段であり、ネットワークを利用するためにプロバイダや、データベースサーバに接続するための手段である。

【００９９】

暗号化手段２１４は、鍵データ３１２を利用して、データを暗号化する手段である。

【０１００】

復号化手段２１５は、鍵データ３１２を利用して、データを復号化する手段である。

【０１０１】

アプリ発行手段３０２は、端末１０１上で起動するアプリデータのコードにセッション鍵を埋め込み、アプリを発行する手段である。

【０１０２】

認証手段３０３は、サーバ１０３、端末１０１、ＭＴＡ２００、データ管理アプリ２０１、その他の端末１０１上で起動するアプリとＩＣカード１０２のデータ管理カードアプリ３０１の間で認証を行うための手段である。ＩＣカード１０２が、サーバ１０３との間で、ＳＳＬセッションを確立する際にも利用する。

【０１０３】

カード制御手段３０４は、ＩＣカード１０２のカード記憶装置１０７に保存しているデータの内容を参照、変更、削除する手段である。

【０１０４】

カード時刻カウント手段３１４は、ＩＣカード１０２で、時刻の経過を計るための手段である。

【０１０５】

また、端末１０１上の同一アプリ内の手段同士はメモリ空間を共有しているため、一部の手段が取得、参照したデータは、どの手段も利用できる。

【０１０６】

また、サーバ１０３、端末１０１、ＩＣカード１０２は、認証時に得た鍵を共有し、お互いに通信する場合は、通信路を暗号化している。

【０１０７】

また、本特許で説明している時刻情報、日時データなどは、最低でも年月分秒の単位までを表しており、利用用途に応じて、表現単位を変えても良い。

【０１０８】

次に、セキュアデータ管理装置で行う処理のフローについて順に説明する。

【０１０９】

まず、端末１０１の動作について説明する。

【０１１０】

端末１０１は、パワーオンするとＭＴＡ２００が自動的に起動され、データ管理カード

アプリ３０１などのそれ以外のアプリは、ＭＴＡ２００によって起動される。
【０１１１】
まず、ＭＴＡ２００の起動フローを図５に示す。
【０１１２】
ＭＴＡ２００の起動処理は、端末１０１のＯＳ、ＭＴＡローダ、データ管理カードアプリ３０１の間で行われる。ＭＴＡローダは、ＩＣカード１０２にＭＴＡ２００の発行を依頼し、発行されたＭＴＡ２００の起動を行う端末のアプリである。
【０１１３】
パワーオンすると端末１０１のＯＳは、ＭＴＡ２００を端末１０１上にロードするためのＭＴＡローダを起動する（図５の1)）。
【０１１４】
起動したＭＴＡローダは、データ管理カードアプリ３０１に対して、ＭＴＡ２００の発行要求を送信する（図５の2)）。
【０１１５】
データ管理カードアプリ３０１のアプリ発行手段３０２は、ＭＴＡ２００の起動後の認証と通信用に、ＭＴＡに認証情報を埋め込む（図５の3)）。
【０１１６】
データ管理カードアプリ３０１のアプリ発行手段３０２は、ＭＴＡローダに対して、ＭＴＡデータを発行する（図５の4)）。
【０１１７】
ＭＴＡローダは、端末１０１のＯＳに対して、受信したＭＴＡ２００の起動要求を出す（図５の5)）。
【０１１８】
端末１０１のＯＳは、ＭＴＡデータを受け取り、ＭＴＡ２００を起動する（図５の6)）。
【０１１９】
起動したＭＴＡ２００の制御手段２０５は、埋め込まれた認証情報からセッション鍵を生成する（図５の7)）。
【０１２０】
ＭＴＡ２００の制御手段２０５とデータ管理カードアプリ３０１の認証手段３０３は、データ管理カードアプリ３０１が同様に認証情報からセッション鍵を生成し、その生成したセッション鍵を利用して、認証を行う（図５の8)）。
【０１２１】
以上が、ＭＴＡ２００の起動フローである。
【０１２２】
ＭＴＡ２００以外の端末１０１上で起動するアプリの起動パターンとしては、ＭＴＡ２００の判断で起動する場合と、ユーザの要求によって起動する場合がある。
【０１２３】
ＭＴＡ２００の判断に基づくアプリ起動フローを図６に示す。
【０１２４】
この場合の処理は、ＭＴＡ２００とデータ管理カードアプリ３０１の間で行われる。
【０１２５】
ＭＴＡ２００の制御手段２０５は、データ管理カードアプリ３０１のカード制御手段３０４に起動アプリリストデータ３０７を要求する（図６の1)）。
【０１２６】
データ管理カードアプリ３０１のカード制御手段３０４は、記憶装置１０７に保存している起動アプリリストデータ３０７を参照し、ＭＴＡ２００の制御手段２０５に起動アプリリストデータ３０７を送信する（図６の2)）。
【０１２７】
ＭＴＡ２００の調査手段２０４は、端末１０１の処理モジュール１０４で現在起動中の

アプリを調べ、起動アプリリストデータ３０７に記されているアプリの起動状態を調べる。その結果、ＭＴＡ２００のアプリ操作手段２０３は、起動アプリリストデータ３０７に記されていて、現在起動していないアプリを、起動すべきアプリとして、起動処理を開始する（図６の3)）。

【０１２８】

ＭＴＡ２００の制御手段２０５は、データ管理カードアプリ３０１のカード制御手段３０４に、起動するアプリを復号化するための鍵と、改ざんを検出するためのハッシュ値を記載している構成データ３０５を要求する（図６の4)）。

【０１２９】

データ管理カードアプリ３０１のカード制御手段３０４は、構成データ３０５と、構成データ３０５に記載されている鍵番号を参照し、参照した鍵番号を基に鍵データ３１２を参照し、ＭＴＡ２００の制御手段２０５に、起動するアプリを復号化するための鍵と、改ざんを検出するためのハッシュ値が記載されている構成データ３０５を送信する（図６の5)）。

【０１３０】

ＭＴＡ２００の復号化手段２１９は、鍵データ３１２を利用して、アプリデータを復号化する（図６の6)）。

【０１３１】

ＭＴＡ２００のデータ検証手段２２０は、アプリデータからハッシュ値を計算し、構成データ３０５に記載されているハッシュ値と比較し、アプリデータの改ざんをチェックする（図６の7)）。

【０１３２】

ＭＴＡ２００のアプリ発行手段２１８は、認証用のセッション鍵を生成し、アプリデータに埋め込み、アプリを発行する。そして、ＭＴＡ２００の制御手段２０５は、生成した認証用のセッション鍵を、データ管理カードアプリ３０１のカード制御手段３０４に渡す（図６の8)）。

【０１３３】

ＭＴＡ２００のアプリ操作手段２０３は、発行されたアプリの起動処理を行う（図６の9)）。

【０１３４】

起動したアプリの制御手段（データ管理アプリ２０１の場合ならば、制御手段２１３のこと）は、埋め込まれたセッション鍵を取得し、データ管理カードアプリ３０１の認証手段３０３との間で、セッションを確立する（図６の10)）。

【０１３５】

セッションを確立したアプリの制御手段は、その後の処理に必要な暗号鍵、復号鍵などのデータをデータ管理カードアプリ３０１のカード制御手段３０４に対して、要求し取得する（図６の11)）。尚、アプリデータに埋め込むセッション鍵を生成するのは、アプリ発行手段３０２が行い、図６の5)で、制御手段２０５に渡しても良い。

【０１３６】

また、ＭＴＡ２００によって起動されたアプリケーションは、ＩＣカード１０２とのセッションが確立している間は、正常に動作し、ＩＣカード１０２が抜かれるなどして、セッションが確立していない場合には、調査手段２１２が検知し、アプリケーションを終了する。

【０１３７】

以上がＭＴＡ２００の判断に基づくアプリ起動フローである。

【０１３８】

また、端末１０１は、ユーザによる要求操作に基づいてアプリを起動する場合もある。

【０１３９】

ユーザの要求に基づくアプリ起動フローを図７に示す。

【０１４０】

この場合の処理は、ユーザが利用するＧＵＩなどのインターフェースとＭＴＡ２００とデータ管理カードアプリ３０１の間で行われる。

【０１４１】

ユーザはＧＵＩなどを通して、ＭＴＡ２００のアプリ操作手段２０３に対して、起動したいアプリの起動を要求する（図７の1)）。

【０１４２】

ＭＴＡ２００の制御手段２０５は、データ管理カードアプリ３０１のカード制御手段３０４に、起動するアプリを復号化するための鍵と、改ざんを検出するためのハッシュ値を記した構成データ３０５を要求する（図７の2)）。

【０１４３】

データ管理カードアプリ３０１のカード制御手段３０４は、構成データ３０５と、構成データ３０５に記載されている鍵番号を参照し、参照した鍵番号を基に鍵データ３１２を参照し、ＭＴＡ２００の制御手段２０５に、起動するアプリを復号化するための鍵と、改ざんを検出するためのハッシュ値が記載されている構成データ３０５を送信する（図７の3)）。

【０１４４】

ＭＴＡ２００の復号化手段２１９は、鍵データ３１２を利用して、アプリデータを復号化する（図７の4)）。

【０１４５】

ＭＴＡ２００のデータ検証手段２２０は、アプリデータからハッシュ値を計算し、構成データ３０５に記載されているハッシュ値と比較し、アプリデータの改ざんをチェックする（図７の5)）。

【０１４６】

ＭＴＡ２００のアプリ発行手段２１８は、認証用のセッション鍵を生成し、アプリデータに埋め込み、アプリを発行する（図７の6)）。

【０１４７】

ＭＴＡ２００のアプリ操作手段２０３は、発行されたアプリの起動処理を行う（図７の7)）。

【０１４８】

起動したアプリの制御手段は、埋め込まれたセッション鍵を取得し、データ管理カードアプリ３０１の認証手段３０３との間で、セッションを確立する（図７の8)）。

【０１４９】

セッションを確立したアプリの制御手段は、その後の処理に必要な暗号鍵、復号鍵などのデータをデータ管理カードアプリ３０１のカード制御手段３０４に対して、要求し取得する（図７の9)）。ここでいう制御手段とは、データ管理アプリ２０１の場合では、制御手段２１３のことである。尚、アプリデータに埋め込むセッション鍵を生成するのは、アプリ発行手段３０２が行い、図７の3)で、制御手段２０５に渡しても良い。

【０１５０】

以上がユーザの要求に基づくアプリ起動フローである。

【０１５１】

起動アプリリストデータ３０７には、データ管理アプリ２０１が、起動すべきアプリとして記載されており、データ管理アプリ２０１は、ＭＴＡ２００によって起動され、常に起動状態にある。

【０１５２】

データ管理アプリ２０１は、実データ２１６などのデータの同期処理を行う場合、サーバに接続する。

【０１５３】

サーバへの接続フローを図８に示す。

【０１５４】

この場合の処理は、データベースサーバが稼動しているサーバ１０３とデータ管理アプ

リ２０１とデータ管理カードアプリ３０１の間で行われる。
【０１５５】
データ管理アプリ２０１の制御手段２１３は、サーバとの接続を行うためのＵＲＬなどの情報をデータ管理カードアプリ３０１のカード制御手段３０４に要求し、取得する（図８の1)）。
【０１５６】
データ管理アプリ２０１の制御手段２１３は、取得した情報を基にサーバと接続する（図８の2)）。
【０１５７】
サーバとデータ管理カードアプリ３０１の認証手段３０３は、ＳＳＬセッションを確立する（図８の3)）。
【０１５８】
確立したセッションを利用して、サーバと端末１０１は、は通信することができる（図８の4)）。
【０１５９】
以上が、接続のフローである。
【０１６０】
データ管理アプリ２０１は、データベースサーバと接続したのちに、同期処理を行う対象となるデータを、目標データ３０６に挙げる。
【０１６１】
目標データ３０６を決定するためのフローを図９に示す。
【０１６２】
この場合の処理は、サーバ１０３とデータ管理アプリ２０１とデータ管理カードアプリ３０１の間で行われる。
【０１６３】
データ管理アプリ２０１の制御手段２１３は、データ管理カードアプリ３０１のカード制御手段３０４に対して、同期処理に必要な情報を要求する（図９の1)）。
【０１６４】
データ管理カードアプリ３０１のカード制御手段３０４は、カード記憶装置１０７を参照して、前回更新日時データ３０８、目標データ３０６、構成データ３０５、データポリシーデータ３１１を、データ管理アプリ２０１の制御手段２１３に応答として返す（図９の2)）。
【０１６５】
データ管理アプリ２０１の目標データ決定手段２１１は、更新データ一覧をサーバから取得する。更新データ一覧には、三種類ある。一つには、前回更新日時以後に更新されたデータのＩＤ一覧と、その更新日時と、データサイズで構成される場合、一つには、削除要求と、データのＩＤの一覧で構成される場合、一つには、緊急削除要求で構成される場合である。また、緊急削除要求には、二種類あり、一つには、要求のみの場合、一つには、緊急削除要求と、データのＩＤ一覧の場合がある。（図９の3)。緊急削除の詳細については、後述する）。
【０１６６】
次に、データ管理アプリ２０１の調査手段２１２は、端末１０１の記憶装置１０５を調べ、残り記憶容量を取得する（図９の4)）。
【０１６７】
データ管理アプリ２０１の目標データ決定手段２１１は、前回更新日時データ３０８と、構成データ３０５の更新日時を比較し、前回更新日時以後に、更新されたものを、サーバ１０３へ送信する候補一覧として挙げる（図９の5)）。
【０１６８】
データ管理アプリ２０１の目標データ決定手段２１１は、サーバ１０３からダウンロードする候補、サーバ１０３にアップロードする候補、削除する候補それぞれについて、デ

ータポリシーデータ３１１に基づき、候補を処理順に並べる。最優先データに記されているＩＤを先頭にし、それ以外の決定基準に基づき、それ以外の候補を処理順に並べる（図９の6)）。

【０１６９】

データ管理アプリ２０１の目標データ決定手段２１１は、サーバ１０３からダウンロードする候補、サーバ１０３にアップロードする候補、削除する候補のうち、複数に候補として挙がっており、衝突しているＩＤを検出する（図９の7)）。

【０１７０】

データ管理アプリ２０１の目標データ決定手段２１１は、データポリシーデータ３１１の衝突時の優先度に基づき、衝突しているＩＤに対する処理を決定する（図９の8)）。

【０１７１】

データ管理アプリ２０１の目標データ決定手段は、構成データ３０５とサーバ１０３から取得した更新データ一覧のＩＤを比較し、構成データ３０５として存在しないデータを新規ダウンロード候補として列挙し、サーバ１０３からダウンロードする候補の処理順の早いＩＤから順にデータサイズを加算していき、残り記憶容量内に収まるＩＤまでに絞り込む（図９の9)）。

【０１７２】

データ管理アプリ２０１の目標データ決定手段２１１は、候補一覧から既に、目標データ３０６に挙がっているＩＤを排除する（図９の10)）。

【０１７３】

以上の処理を行うとダウンロード、アップロード、削除の目標データ３０６が決定する。

【０１７４】

データ管理アプリ２０１の目標データ決定手段は、決定した目標データ３０６と、新規データリストをデータ管理カードアプリ３０１に通知する（図９の11)）。

【０１７５】

データ管理カードアプリ３０１のカード制御手段３０４は、ＩＣカード１０２のカード記憶装置１０７に保存している目標データ３０６を更新する（図９の12)）。

【０１７６】

データ管理カードアプリ３０１のカード制御手段３０４は、ＩＣカード１０２のカード記憶装置１０７に新規データリストに挙がっているＩＤの構成データ３０５を用意する（図９の13)）。

【０１７７】

データ管理カードアプリ３０１のカード制御手段３０４は、ＩＣカード１０２のカード記憶装置１０７に保存している前回更新日時データ３０８を更新する（図９の14)）。

【０１７８】

データ管理カードアプリ３０１のカード制御手段３０４は、データ管理アプリ２０１の制御手段２１３に目標データ決定終了を通知し、目標データ３０６を決定する処理を終了する（図９の15)）。

【０１７９】

最優先データ、それ以外の決定基準、衝突時の優先度について、図１３、１４を参照しながら、具体的に説明をしておく。

【０１８０】

削除処理の候補として、ＩＤが５８７,１０７,０８９,００７,００３,００２のデータがリストアップされた場合、図１４に示すデータポリシーデータに基づくと、削除については、００１と００３が、削除候補に挙がっている場合には、優先的に早く削除するように目標データの先頭に挙げることになるので、削除順の先頭は、００３となる。

【０１８１】

次に、それ以外の決定基準について見てみると、ＩＤの小さい順となっているので、ＩＤ００２、００７、０８９、１０７、５８７という順に処理順を決定して行く。その結果

、削除候補に挙がっているＩＤの処理順は、００３、００２、００７、０８９、１０７、５８７となる。

【０１８２】

衝突時の優先度は、図１３では、削除と更新での目標データの衝突の場合の優先基準、更新と更新での目標データの衝突の場合の優先基準と表示しているデータであり、削除目標候補と更新目標候補の両方に挙がり、両方を行うことはできない場合に、どちらを優先するかを決める基準である。図１４ならば、削除と更新の場合には、削除優先であるから、更新する候補からは、排除して、削除目標のみ対象となるデータのＩＤを挙げる。更新と更新の場合には、新規優先なので、サーバから得た更新日時と、対象となるデータに対応する構成データ３０５の更新日時を比較してサーバ側データが新しい場合には、ダウンロードの目標に挙げ、端末側が新しいならば、アップロードの目標に挙げる。

【０１８３】

削除の候補として、００３、００２、００７、０８９、１０７、５８７が挙がっており、ダウンロードの候補として、００５、００２、０５５、１０７、２５８が挙がっている場合について説明する。

【０１８４】

図１４に基づくと削除と更新（ダウンロード）では、削除優先なので、削除候補は、変わらない。ダウンロードの候補は、００２と１０７が排除され、００５、０５５、２５８となる。

【０１８５】

以上が、目標データ３０６を決定するためのフローである。

【０１８６】

同期処理の目標データ３０６が、決定するとデータ管理アプリ２０１は、同期の処理を開始する。

【０１８７】

データ同期処理のフローを図１０に示す。

【０１８８】

この場合の処理は、サーバ１０３とデータ管理アプリ２０１とデータ管理カードアプリ３０１の間で行われる。

【０１８９】

データ管理アプリ２０１の制御手段２１３は、同期処理を行うために必要な情報を、データ管理カードアプリ３０１に要求する（図１０の1)）。

【０１９０】

データ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６のダウンロード、アップロード、削除の目標になっているデータのＩＤを参照する（図１０の2)）。

【０１９１】

データ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６のダウンロードするデータのＩＤに対応する暗号鍵を決定し、鍵データ３１２を参照する。（図１０の3)）。

【０１９２】

データ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６のアップロードするデータの改ざん検出に利用するハッシュ値が記載された構成データ３０５を参照する。そして、また構成データ３０５を参照し、実データ２１６を復号するための鍵を鍵データ３１２から参照する（図１０の4)）。

【０１９３】

データ管理カードアプリ３０１のカード制御手段３０４は、データ管理アプリ２０１に、ダウンロードデータのＩＤリスト、アップロードするデータのＩＤリスト、削除するデータのＩＤリスト、暗号化するための鍵、復号化するための鍵、構成データ３０５を応答として返す（図１０の5)）。

【０１９４】
応答を返した後に、データ管理カードアプリ３０１のカード制御手段３０４は、新たにダウンロードする実データ２１６のＩＤに対応する構成データ３０５の対応鍵番号を更新する（図１０の6)）。
【０１９５】
応答を受けたデータ管理アプリ２０１の制御手段２１３は、ダウンロード、アップロード、削除のいずれかの処理を、適宜開始する。ここでは、ダウンロード、アップロード、削除全ての処理について述べる。
【０１９６】
ダウンロードする場合、データ管理アプリ２０１のデータ同期手段２０８は、データのＩＤを指定して、ダウンロードするデータをサーバ１０３へ要求し、サーバ１０３からデータをダウンロードする（図１０の7)）。この際に、データの更新日時、有効期限もダウンロードする。
【０１９７】
データ管理アプリ２０１のデータ検証手段２１０は、ダウンロードしたデータのハッシュ値を計算する（図１０の8)）。
【０１９８】
データ管理アプリ２０１の暗号化手段２１４は、ＩＤに対応する暗号化するための鍵で、ダウンロードしたデータを暗号化する（図１０の9)）。
【０１９９】
データ管理アプリ２０１の制御手段２１３は、暗号化した実データ２１６を端末１０１の記憶装置１０５に保存する（図１０の10)）。
【０２００】
データ管理アプリ２０１制御手段は、データ管理カードアプリ３０１のカード制御手段３０４に、処理結果と、保存したデータのＩＤと、そのハッシュ値、更新日時、有効期限を通知し、通知を受けたデータ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６を参照して、まだダウンロードすべきデータがあるかどうかを判断する（図１０の15)）。
【０２０１】
データ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６において、ダウンロードした実データ２１６の処理状態を「済み」の状態に更新する（図１０の16))。
【０２０２】
データ管理カードアプリ３０１のカード制御手段３０４は、ダウンロードしたデータのＩＤに対応する構成データ３０５のハッシュ値と、更新日時を更新する（図１０の17))。
【０２０３】
ダウンロードすべきデータが、目標データ３０６に無い場合は目標データ３０６の終了日時を更新する（図１０の18)）。
【０２０４】
データ管理カードアプリ３０１のカード制御手段３０４は、サーバ１０３にダウンロードの処理が終了したことと、ダウンロードしたデータのＩＤを報告する（図１０の19))。
【０２０５】
アップロードする場合には、データ管理アプリ２０１の復号化手段２１５は、実データ２１６のＩＤに対応する復号化するための鍵で、アップロードするデータを復号化する（図１０の11)）。
【０２０６】
データ管理アプリ２０１のデータ検証手段２１０は、アップロードするデータのハッシュ値を計算し、データ管理カードアプリ３０１から取得したハッシュ値と比較して、改ざ

んされていないかを検証する（図１０の12)）。
【０２０７】
従来であると、ハッシュ値の計算を行うアプリ自体に改変を加えられ、ハッシュ値自体が信用できない場合があったが、ＭＴＡ２００によって起動した信頼できるデータ管理アプリ２０１のデータ検証手段２１０が、ハッシュ値の計算を行うため、データの検証結果を信頼することができる。
【０２０８】
データ管理アプリ２０１のデータ同期手段２０８は、実データ２１６のＩＤを指定して、サーバ１０３へデータをアップロードする（図１０の13)）。
【０２０９】
データ管理アプリ２０１の制御手段２１３は、データ管理カードアプリ３０１のカード制御手段３０４に、処理結果とアップロードした実データ２１６のＩＤを通知し、通知を受けたデータ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６を参照して、まだアップロードすべきデータがあるかどうかを判断する（図１０の15)’）。
【０２１０】
データ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６において、アップロードした実データ２１６の処理状態を「済み」の状態に更新する（図１０の16))。
【０２１１】
アップロードすべきデータが、目標データ３０６に、無い場合は目標データ３０６の終了日時を更新する（図１０の18))。
【０２１２】
データ管理カードアプリ３０１のカード制御手段３０４は、サーバ１０３にアップロードの処理が終了したことと、アップロードした実データ２１６のＩＤを報告する（図１０の19))。
【０２１３】
削除する場合は、データ管理アプリ２０１のデータ削除手段２０９は、目標データ３０６に挙がっているＩＤに対応する実データ２１６を端末１０１の記憶装置１０５から削除する（図１０の14))。
【０２１４】
データ管理アプリ２０１の制御手段２１３は、データ管理カードアプリ３０１に、処理結果と削除した実データ２１６のＩＤを通知し、通知を受けたデータ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６を参照して、まだ削除すべきデータがあるかどうかを判断する（図１０の15)’’）。
【０２１５】
データ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６において、削除した実データ２１６データの処理状態を「済み」の状態に更新する（図１０の16))。
【０２１６】
削除する目標データ３０６がまだある場合は処理を継続し、無い場合は目標データ３０６の終了日時を更新する（図１０の18))。
【０２１７】
データ管理カードアプリ３０１のカード制御手段３０４は、サーバ１０３に削除の処理が終了したことを通知する（図１０の19))。尚、削除した実データ２１６のＩＤを報告しても良い。また、処理の終了時には、データ管理アプリ２０１がメモリ上に保持している鍵データ、構成データなどの機密情報は、メモリ上から消去する。
【０２１８】
尚、図１０の16)～19)の処理は、ダウンロード、アップロード、削除それぞれについて、行われる。
【０２１９】

以上が、データの同期処理のフローである。

【０２２０】

また、今までの利用していた複数の端末の内、今まで利用していたユーザが無効になった場合や、端末を紛失した場合や、端末の不正利用を検出した場合に、端末の保存している実データ２１６を緊急に削除する必要がでてくる。

【０２２１】

データの緊急削除時のフローを図１１に示す。

【０２２２】

この場合の処理は、サーバ１０３とデータ管理アプリ２０１とデータ管理カードアプリ３０１の間で行われる。

【０２２３】

サーバ１０３が、データを緊急に削除すべきと判断する（図１１の1)）。

【０２２４】

サーバ１０３は、データ管理アプリ２０１の目標データ３０６決定手段に緊急削除命令を出す（図１１の2)）。

【０２２５】

緊急削除命令のパターンとしては、２パターンある。一つには、緊急削除命令のみを出す場合である。そして、一つには、緊急削除命令と削除するデータのＩＤリストを出す場合である。

【０２２６】

緊急削除命令だけの場合には、命令を受けたデータ管理アプリ２０１の目標データ決定手段２１１は、データ管理カードアプリ３０１のカード制御手段３０４に構成データ３０５と、データポリシーデータ３１１を要求し、緊急削除目標と処理順を決定する（図１１の3)）。

【０２２７】

データ管理アプリ２０１の制御手段２１３は、データ管理カードアプリ３０１のカード制御手段３０４に対して、緊急削除の通知と、目標データ３０６の通知を行う（図１１の4)）。

【０２２８】

データ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６を更新し、緊急削除目標を追加する（図１１の5)）。

【０２２９】

データ管理カードアプリ３０１のカード制御手段３０４は、緊急削除の情報を、起動アプリリストデータに追加する（図１１の6)）。

【０２３０】

データ管理カードアプリ３０１のカード制御手段３０４は、鍵データ３１２を削除する（図１１の7)）。

【０２３１】

一方、データ管理カードアプリ３０１に通知を行った後に、データ管理アプリ２０１のデータ削除手段２０９は、緊急削除を開始する（図１１の8)）。

【０２３２】

データ管理アプリ２０１のデータ削除手段２０９は、緊急削除の目標となるＩＤに対応するデータを端末１０１の記憶装置１０５から削除する（図１１の9)）。

【０２３３】

データ管理アプリ２０１の制御手段２１３は、データ管理カードアプリ３０１のカード制御手段３０４に、処理結果と削除したデータのＩＤを通知し、通知を受けたカード制御手段３０４は、目標データ３０６を参照して、まだ削除すべきデータがあるかどうかを判断する（図１１の10)）。

【０２３４】

データ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６において

、削除した実データ２１６の処理状態を「済み」の状態に更新する（図１１の11)）。
【０２３５】
データ管理カードアプリ３０１のカード制御手段３０４は、必要に応じて構成データ３０５自体を削除する（図１１の12)）。
【０２３６】
緊急削除する目標データ３０６が無い場合は、目標データ３０６の終了日時を更新する（図１１の13)）。
【０２３７】
データ管理カードアプリ３０１のカード制御手段３０４は、起動アプリリストデータ３０７から、緊急削除フラグの情報を、必要に応じて適宜削除（具体例では、ＯＦＦに）する（図１１の14)）。
【０２３８】
データ管理カードアプリ３０１のカード制御手段３０４は、サーバ１０３に緊急削除の処理が終了したことと、削除したデータのＩＤを報告する（図１１の15)）。この場合、データを削除する方法としては、全ての削除対象領域に、１、０など意味の無いデータを書き込むことまで行うとより効果的である。
【０２３９】
また、緊急削除処理の際に、ＩＣカード１０２が抜かれた場合でも削除は続行する。その後、削除を行うアプリが、停止させられても、再びＩＣカード１０２を挿入したならば、起動アプリリストデータ３０７の緊急削除フラグがＯＮになっているため、データを削除し始める。
【０２４０】
以上が、緊急削除時のフローである。
【０２４１】
また、実データ２１６には、利用できる有効期限がついており、有効期限が切れたデータをデータ管理アプリ２０１が、削除することもある。
【０２４２】
有効期限切れデータの削除のフローを図１２に示す。
【０２４３】
この場合の処理は、データ管理アプリ２０１とデータ管理カードアプリ３０１の間で行われる。
【０２４４】
データ管理アプリ２０１の制御手段２１３は、データ管理カードアプリ３０１に要求し、構成データ３０５を取得する（図１２の1)）。
【０２４５】
データ管理アプリ２０１の目標データ３０６決定手段は、構成データ３０５の有効期限情報と現在の日時情報を比較し、有効期限の切れている実データ２１６のＩＤを、削除するデータとして挙げる（図１２の2)）。
【０２４６】
データ管理アプリ２０１の制御手段２１３は、データ管理カードアプリ３０１に目標データ３０６を通知する（図１２の3)）。
【０２４７】
データ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６を更新する（図１２の4)）。
【０２４８】
データ管理アプリ２０１のデータ削除手段２０９は、削除の目標となるＩＤに対応するデータを端末１０１の記憶装置１０５から削除する（図１２の5)）。
【０２４９】
データ管理アプリ２０１の制御手段２１３は、データ管理カードアプリ３０１に、処理結果と削除したデータのＩＤを通知する（図１２の6)）。

【０２５０】
データ管理カードアプリ３０１のカード制御手段３０４は、目標データ３０６の削除したＩＤの処理状態を「済み」にする（図１２の7)）。
【０２５１】
データ管理カードアプリ３０１のカード制御手段３０４は、必要に応じて構成データ３０５自体を削除する（図１２の8)）。
【０２５２】
削除する目標データ３０６がまだある場合は処理を継続し、無い場合は目標データ３０６の終了日時を更新する（図１２の9)）。
【０２５３】
以上が有効期限切れデータの削除のフローである。
【０２５４】
また、実データ２１６が、顧客リストデータ、契約情報などの実データは、データ管理アプリ２０１によって内容を参照され端末１０１のディスプレイに表示される。
【０２５５】
実データ２１６の参照のフローについて説明する。
【０２５６】
この場合の処理は、データ管理アプリ２０１とデータ管理カードアプリ３０１の間で行われる。
【０２５７】
データ管理アプリ２０１の制御手段２１３は、ユーザ操作もしくは、他のアプリからの参照要求と、参照したい実データ２１６のＩＤを受信し、データ管理カードアプリ３０１のカード制御手段３０４にＩＤに対応する復号鍵とハッシュ値を記載している構成データ３０５を要求する。
【０２５８】
データ管理カードアプリ３０１のカード制御手段３０４は、要求された実データ２１６のＩＤに対応する構成データ３０５を参照し、更に対応鍵番号を参照する。
【０２５９】
データ管理カードアプリ３０１のカード制御手段３０４は、対応鍵番号に対応した鍵データ３１２を参照する。
【０２６０】
データ管理カードアプリ３０１のカード制御手段３０４は、データ管理アプリ２０１に、復号化するための鍵と、ハッシュ値が記載されている構成データ３０５を応答として返す。
【０２６１】
データ管理アプリ２０１の復号化手段２１５は、実データ２１６のＩＤに対応する復号化するための鍵で、実データ２１６を復号化する。
【０２６２】
データ管理アプリ２０１のデータ検証手段２１０は、実データ２１６のハッシュ値を計算し、データ管理カードアプリ３０１から取得した構成データ３０５のハッシュ値と比較して、改ざんされていないかを検証する。これによって実データ２１６を参照することができる。
【０２６３】
この時、データ管理アプリ２０１は、参照要求を出した相手に応じて、参照するデータの範囲に制限をかけたり、ユーザＩＤや時刻情報を電子透かしとして入れても良いし、印刷、保存など、参照後のデータに対する処理に制限をかけても良い。
【０２６４】
以上が実データ２１６の参照フローである。
【０２６５】
また、本発明の実施の形態１では、時刻を比較する際の現在時刻は、以下の仕組みを利

用して信頼できる正しい時刻を取得している。

【０２６６】

信頼できる時刻の取得と保存のフローを図３０に示す。

【０２６７】

この場合の処理は、サーバ１０３とＭＴＡ２００とデータ管理カードアプリ３０１と端末１０１上で動作しているアプリの間で行われる。

【０２６８】

サーバ１０３は、ネットワーク上の信頼できる時刻サーバと時刻を同期しており、正確な時刻情報を端末に提供する。本実施形態では、サーバ１０３が、端末１０１に時刻情報を提供するとしたが、同様に時刻情報を提供する機能を備えたサーバまたは時刻サーバから時刻情報を受信するようにしても良い。

【０２６９】

ＭＴＡ２００は、最初、起動するとサーバとＳＳＬの通信セッションを確立することで、サーバが正しい時刻情報を提供するサーバであることを認証し、セキュアセッションを確立する（図３０の1)）。

【０２７０】

ＭＴＡ２００の時刻取得手段２０６は、サーバから時刻情報を取得する（図３０の2)）。

【０２７１】

ＭＴＡ２００の時刻カウント手段２０７は、経過時間を計測し、取得した時刻情報と、合わせて、現在時刻を算出する（図３０の3)）。ＭＴＡ２００の時刻カウント手段２０７は、電源がオフされてＭＴＡ２００が終了するまで時刻をカウントし続ける。時刻カウント手段２０７がカウントする時刻はユーザが変更したり、他のアプリケーションが変更したりすることは出来ない。信頼できるＭＴＡ２００によって時刻がカウントされ続けるので、端末１０１は常に正しい正確な時刻を保つことができる。

【０２７２】

端末１０１上で起動中のデータ管理アプリ２０１やその他のアプリケーションは、現在時刻を利用する場合には、ＭＴＡ２００に問い合わせることで、信頼できる時刻を取得する（図３０の4)）。

【０２７３】

また、ＭＴＡ２００は、サーバから取得した時刻や、カウントした時刻をデータ管理カードアプリ３０１のカード制御手段３０４に通知する（図３０の5)）。

【０２７４】

データ管理カードアプリ３０１のカード制御手段３０４は、通知された時刻をカード記憶装置１０７に時刻データ３１３として保存する（図３０の6)）。

【０２７５】

また、データ管理カードアプリ３０１への時刻情報の通知タイミングは、三種類ある。一つは、サーバから時刻情報を取得した直後であり、一つは、一時間に一回のような定期的なタイミングであり、一つは、他のアプリから時刻取得要求を受けるようなイベント発生時でもある。

【０２７６】

保存した時刻データの利用法としては、次のような方法がある。

【０２７７】

一旦、端末１０１の電源をオフにし、次回、起動した時に、サーバから時刻情報が取得できなかった場合に、ＭＴＡ２００は、端末１０１の時刻をＩＣカード１０２に保存した時刻を用いて検証する。端末の時刻がカード記憶装置１０７の時刻データ３１３が示す時刻よりも過去であった場合、ＭＴＡ２００の制御手段２０５は、時刻が不正に変更されたと判定し、データ管理アプリなどのアプリを起動しない。このようにすることで、時間を前に戻すことで、有効期限の切れた実データ２１６や、アプリを、不正に利用する行為を防ぐことができる。

【０２７８】
　また、端末の時刻がカード記憶装置１０７の時刻データ３１３が示す時刻よりも未来であった場合も、その差が予め設定した閾値よりも大きい場合には、ＭＴＡ２００の制御手段２０５は、時刻が不正に変更されたと判定し、サーバに接続して改めて時刻情報が取得されない限り、オフライン状態ではデータ管理アプリなどのアプリを起動しない。このようにすることで、時間を進めることでまだ利用可能になっていない実データ２１６や、アプリを、不正に利用する行為を防ぐことができる。
【０２７９】
　また、時刻データ３１３には、時刻情報のサーバからの取得に連続して失敗した回数と、その回数の許容最大値が記録されている。連続して失敗した回数は、サーバからの時刻情報が取得に失敗すると１カウントアップし、サーバから時刻情報が取得されるとゼロにリセットされる。その回数が許容最大値を超えると、ＭＴＡ２００はデータ管理アプリ等のアプリを起動しないようになる。
【０２８０】
　時刻情報の取得に失敗すると、ＭＴＡは端末１０１の画面にメッセージを表示するなどしてユーザに通知し、オンライン状態にすることをユーザに促す。このようにすることで、ある頻度で端末１０１とサーバとをオンラインにして、端末１０１上のデータと時刻をサーバと同期が取れた状態に保つようにすることも可能である。
【０２８１】
　また、計測した経過時間が、実際の経過時間より遅くなるように端末１０１のクロックを不正に改造する場合が考えられるが、そのような場合の対処法としては、下記の二つの方法がある。
【０２８２】
　一つには、ネットワーク上のサーバから取得できる時刻を利用する場合である。まず、時刻取得手段２０６は、サーバから時刻情報を取得する。時刻カウント手段２０７は、予め決めた時間、例えば１分として、時刻を図る。時刻カウント手段２０７が計った時間で、１分経過した後に、時刻取得手段２０６は、サーバから時刻情報を取得する。時刻取得手段２０６の取得した時刻の差分が２分であったとして、予め決めた時間が１分であったので比較すると、実際の経過時間が２倍早いことが分かるので、時刻カウント手段２０７の時刻の計り方に補正をかけ、時刻カウント手段２０７の計測した経過時間の２倍が実際の経過時間であるとして、時刻カウント手段２０７が、時刻の経過を正確に計ることが可能になる。また、経過時間に差があった場合、不正な端末であると判断し、アプリの利用を停止、終了する対処法もある。
【０２８３】
　一つには、ＩＣカード１０２を利用することによってオフラインでも、正確な時刻の経過を計る方法が考えられる。時刻カウント手段２０７は、予め決めた時間、例えば１分として、時刻をカウントする。同時に、制御手段２０５は、カード時刻カウント手段３１４に、時刻のカウントの開始を要求する。時刻カウント手段２０７が計測した時間で、あらかじめ決めた時間である１分が経過した後に、制御手段２０５は、カード時刻カウント手段３１４に、経過時刻を要求する。カード時刻カウント手段３１４の計測した経過時刻が２分であったとすると、予め決めた時間（ここでの１分）を比較することによって、時刻カウント手段２０７の計測した時間を２倍した時間が、実際の経過時間であると分かるので、時刻カウント手段２０７の時刻の計り方に補正をかけるにより、時刻カウント手段２０７の計測した経過時間の２倍が実際の経過時間であるとして、オフラインでも、時刻カウント手段２０７が、時刻の経過を正確に計ることが可能になる。また、この場合、カード時刻カウント手段３１４に、計測時間（ここでの１分）をセットし、カード時刻カウント手段３１４からの計測終了通知を受けた後に、補正をかける方法もある。また、この場合も、経過時間に差があった場合、不正な端末であると判断し、アプリの利用を停止、終了する対処法もある。
【０２８４】

（実施の形態２）

本発明の実施の形態２におけるセキュアデータ管理装置を示すシステム構成を図３１に示す。

【０２８５】

実施の形態２では、カードとして、セキュアデータ管理カード３００１を利用する。セキュアデータ管理カード３００１は、通常のＩＣカード１０２に比べて、大きな記憶容量をもっているカードである。実施の形態２では、実施の形態１において、端末１０１の記憶装置１０５に保存していたデータを、セキュアデータ管理カード３００１に保存する。

【０２８６】

セキュアデータ管理装置は、端末１０１、セキュアデータ管理カード３００１、サーバ１０３から構成されている。セキュアデータ管理装置は、端末１０１で利用するデータを、安全に管理するための装置である。

【０２８７】

セキュアデータ管理装置の処理概要を図３４に示す。

【０２８８】

セキュアデータ管理装置の利用目的概要については実施の形態１と同様である。

【０２８９】

以下、処理フローについて述べる。

【０２９０】

端末１０１の電源をオンにし、セキュアデータ管理カード３００１を挿入、または、既に装着されていると、まず、セキュアデータ管理カード３００１で、データ管理カードアプリ３３０１が起動する（図３４の1)）。

【０２９１】

端末１０１では、データ管理カードアプリ３３０１から発行された、ＭＴＡ３２００が起動する（図３４の2)）。ＭＴＡ２００は、データ管理カードアプリ３３０１と認証を行い、信頼できるセッションを確立する（図３４の3)）。

【０２９２】

ＭＴＡ３２００は、端末１０１の状態を調べる。この場合、データ管理アプリ３２０１は、起動していないので、ＭＴＡ３２００は、データ管理カードアプリ３３０１に、データ管理アプリ３２０１の発行要求を出す。データ管理カードアプリ３３０１は、ＭＴＡ３２００に対して、データ管理アプリ３２０１を発行する（図３４の4)）。それを受け取ったＭＴＡ３２００は、データ管理アプリ３２０１を起動する（図３４の5)）。その際、データ管理アプリ３２０１は、データ管理カードアプリ３３０１と認証を行い、信頼できるセッションを確立する（図３４の6)）。

【０２９３】

起動したデータ管理アプリ３２０１は、必要に応じて、サーバ１０３との間で、同期の前処理及び同期処理を行う（図３４の7)）。データ管理アプリ２０１は、同期の前処理結果、同期処理の結果、同期処理で得たデータを、データ管理カードアプリ３３０１に対して通知する（図３４の8)）。データ管理カードアプリ３３０１は、同期によって得たデータに対する更新、削除などの処理を行う（図３４の9)）。

【０２９４】

データ管理カードアプリ３３０１は、処理結果に基づき、状況情報を更新する（図３４の10)）。処理タイミングについては、実施の形態１と同様である。

【０２９５】

以上が、セキュアデータ管理装置の処理概要である。

【０２９６】

端末１０１の構成は、実施の形態１と同様である。

【０２９７】

セキュアデータ管理カード３００１は、カード処理モジュール３００２、セキュア記憶装置３００３、カード記憶装置３００４から構成されている。サーバ１０３は、実施の形

態１と同様である。
【０２９８】
本発明のより具体的なハードウェア構成について述べる。
【０２９９】
端末１０１の内部構成は、実施の形態１と同様である。
【０３００】
セキュアデータ管理カード３００１のセキュア記憶装置３００３、カード記憶装置３００４は、耐タンパ性を持つなど外部からの直接参照が困難な記憶領域で、例えばＥＥＰＲＯＭなどで実装される。
【０３０１】
次に、セキュアデータ管理カード３００１の内部構成について説明する。
【０３０２】
セキュアデータ管理カード３００１は、図３１に示すようにカード処理モジュール３００２、セキュア記憶装置３００３、カード記憶装置３００４から構成されている。
【０３０３】
セキュアデータ管理カード３００１のカード処理モジュール３００２は、ＣＰＵとＲＯＭ、ＲＡＭと端末と通信するためのホストＩ／Ｆから構成され、セキュア記憶装置３００３、カード記憶装置３００４は、ＥＥＰＲＯＭなどの不揮発性メモリによって構成され、セキュアデータ管理カード３００１は全体として耐タンパ性を備えている。セキュア記憶装置３００３へのアクセスは、カード処理モジュール３００２を介してのみ行える。セキュア記憶装置３００３に記録されるデータは、暗号化されており、参照する際に復号化される。暗号化、復号化は、セキュアデータ管理カード３００１のファイルシステムが、行うため、鍵に関する管理を行う必要はない。
【０３０４】
本発明の実施の形態２におけるセキュアデータ管理装置を示すブロック図を図３２、３３に示す。
【０３０５】
図３２は、端末１０１の機能ブロック図である。図３３は、セキュアデータ管理カード３００１の機能ブロック図である。
【０３０６】
処理モジュール１０４の機能は、実施の形態１の場合の機能とほぼ同様である。異なる点は、ＩＣカード１０２ではなく、セキュアデータ管理カード３００１と通信する機能を備えていることである。
【０３０７】
実施の形態２では、処理モジュール１０４で、アプリとしてＭＴＡ３２００とデータ管理アプリ３２０１を実行する。
【０３０８】
ＭＴＡ３２００の機能の概要については、実施の形態１のＭＴＡ２００と同様である。処理フローが多少変わるため、詳細は後述する。
【０３０９】
ＭＴＡ３２００は、アプリ操作手段３２０３、調査手段３２０４、制御手段３２０５、時刻取得手段３２０６、時刻カウント手段３２０７から構成されている。
【０３１０】
データ管理アプリ３２０１の概要については、実施の形態１のデータ管理アプリ２０１と同様である。データ管理アプリ２０１と異なる点は、実データ２１６の保存場所が、端末１０１の記憶装置１０５ではなくなったことによる、処理フローの変化である。詳しくは後述する。
【０３１１】
データ管理アプリ３２０１は、データ同期手段３２０８、目標データ決定手段３２１１、調査手段３２１２、制御手段３２１３から構成されている。

【０３１２】
記憶装置１０５の機能は、実施の形態１と同様である。
【０３１３】
実施の形態２では、記憶装置１０５には、特にデータを保存しない。
【０３１４】
カード処理モジュール３００２は、実施の形態１のカード処理モジュール１０６と同様の機能を備えている。
【０３１５】
実施の形態２では、カード処理モジュール３００２は、アプリとして、データ管理カードアプリ３３０１を実行する。
【０３１６】
データ管理カードアプリ３３０１は、アプリ発行手段３３０２、認証手段３３０３、カード制御手段３３０４、データ削除手段３３０５、カード時刻カウント手段３３１４から構成されている。
【０３１７】
カード記憶装置３００４は、セキュアデータ管理カード３００１上に、データを保存するための装置である。端末１０１側から直接アクセスできることが特徴である。
【０３１８】
カード記憶装置３００４には、データを保存しない。
【０３１９】
セキュア記憶装置３００３は、セキュアデータ管理カード３００１上に、データを保存するための装置である。カード処理モジュール３００２を介してのみ、アクセスできることが特徴である。
【０３２０】
実施の形態２では、セキュア記憶装置３００３には、構成データ３３０６、実データ２１６、データ管理アプリデータ２１７、目標データ３０６、起動アプリリストデータ３０７、前回更新日時データ３０８、ＭＴＡデータ３０９、データポリシーデータ３１１、鍵データ３１２、時刻データ３１３を保存している。
【０３２１】
実データ２１６、データ管理アプリデータ２１７、目標データ３０６、起動アプリリストデータ３０７、前回更新日時データ３０８、ＭＴＡデータ３０９、データポリシーデータ３１１、鍵データ３１２、時刻データ３１３については、実施の形態１と同様である。
【０３２２】
構成データ３３０６は、実施の形態１の構成データ３０５とほぼ同様である。異なる点は、以下の二点である。実データ２１６をセキュアデータカード３００１のセキュア記憶装置３００３に保存しており、改ざん、すり替えの危険がないため、ハッシュ値を記録しない。また、実データ２１６の暗号化、復号化は、セキュアデータ管理カード３００１のファイルシステムが、行うため、鍵に関する管理を行わないため、対応鍵番号についても記録しない。
【０３２３】
構成データ３３０６の具体例を、図３８、３９、４０、４１、４２に示す。
【０３２４】
図３８のように、項目としては、ＩＤ、種別、有効期限、更新日時がある。それぞれの括弧内の数字は、データで表現する場合の値である。
【０３２５】
例えば、図３９をデータで表現すると、図４１になり、図４０をデータで表現すると、図４２になる。
【０３２６】
アプリ操作手段３２０３は、セキュアデータ管理カード３００１を利用して、端末１０１上で、アプリを起動するための手段である。

【０３２７】
調査手段３２０４は、起動アプリリストデータ３０７を参照して、起動すべきアプリの現在の状態、起動している、起動していないなどを調べる手段である。
【０３２８】
制御手段３２０５は、調査手段３２０４の調査状況報告と、起動アプリリストデータ３０７を基に起動すべきアプリを決定行う手段である。また、制御手段３２０５は、埋め込まれた認証用の鍵を取得する手段である。また制御手段３２０５は、ネットワークを利用するためにプロバイダ、データベースサーバなどに接続するための手段である。
【０３２９】
時刻取得手段３２０６は、ネットワーク上の信頼できる時刻を保持しているサーバから、時刻を取得する手段である。また、時刻取得手段３２０６は、その取得した時刻を、時刻カウント手段３２０７とセキュアデータ管理カード３００１に通知する。
【０３３０】
時刻カウント手段３２０７は、時刻取得手段３２０６からの通知時刻を基に、現在時刻を計測する手段である。また、時刻取得手段３２０６は、その計測した時刻を、セキュアデータ管理カード３００１に通知する。
【０３３１】
データ同期手段３２０８は、サーバ１０３と通信し、目標データ３０６を基に、実データ２１６、データ管理アプリデータ２１７、起動アプリリストデータ３０７、ＭＴＡデータ３０９、データポリシーデータ３１１、などのデータのアップロード、ダウンロードを行う。また、データ同期手段３２０８は、処理状況をセキュアデータ管理カード３００１に通知する。
【０３３２】
目標データ決定手段３２１１は、サーバ１０３と通信し、前回更新日時データ３０８と、サーバ１０３のデータの更新情報と、構成データ３３０６の更新日時データ、有効期限、データポリシーデータ３１１、目標データ３０６を基に、ダウンロード、アップロード、削除すべきデータを決定する手段である。また、目標データ決定手段３２１１は、決定した目標データ３０６をセキュアデータ管理カード３００１に通知する。
【０３３３】
調査手段３２１２は、端末１０１の状況情報として、記憶装置１０５、セキュア記憶装置３００３の残り記憶容量、ＣＰＵ負荷率などを調べ、制御手段３２１３に通知する手段である。
【０３３４】
データ管理アプリ３２０１の制御手段３２１３は、調査手段３２１２からの通知情報と、目標データ３０６に基づき、データ管理アプリ３２０１の動作を決定する手段である。
【０３３５】
また、制御手段３２１３は、データ管理アプリ３２０１が備える手段であり、ネットワークを利用するためにプロバイダや、データベースサーバに接続するための手段である。
【０３３６】
アプリ発行手段３３０２は、端末１０１上で起動するアプリデータにセッション鍵を埋め込み、ＭＴＡ３２００に対して送信する手段である。
【０３３７】
認証手段３３０３は、サーバ１０３、端末１０１、ＭＴＡ３２００、データ管理アプリ３２０１、その他の端末１０１上で起動するアプリとセキュアデータ管理カード３００１のデータ管理カードアプリ３３０１の間で認証を行うための手段である。
【０３３８】
カード制御手段３３０４は、セキュアデータ管理カード３００１のカード記憶装置３００４、セキュア記憶装置３００３に保存しているデータの内容を参照、変更する手段である。
【０３３９】

カード時刻カウント手段３３１４は、セキュアデータ管理カード３００１で、時刻の経過を計るための手段である。

【０３４０】

データ削除手段３３０５は、目標データ３０６を基に、実データ２１６の削除を行う。また、データ削除手段３３０５は、カード制御手段３３０４に処理状況を通知する。

【０３４１】

また、同一アプリ内の手段同士はメモリ空間を共有しているため、一部の手段が取得、参照したデータは、どの手段も利用できる。

【０３４２】

また、サーバ１０３、端末１０１、セキュアデータ管理カード３００１は、認証時に得た鍵を共有し、お互いに通信する場合は、通信路を暗号化している。

【０３４３】

ＭＴＡ３２００の起動フローについて、説明する。

【０３４４】

ＭＴＡ３２００の起動処理は、端末１０１のＯＳ、ＭＴＡローダ、データ管理カードアプリ３３０１の間で行われる。実施の形態１で、ＭＴＡ２００が行っていた処理を、ＭＴＡ３２００が行う。実施の形態１で、データ管理カードアプリ３０１が行っていた、処理をデータ管理カードアプリ３３０１が行う。

【０３４５】

以上が、ＭＴＡ３２００の起動フローである。

【０３４６】

ＭＴＡ３２００の判断に基づくアプリ起動フローについて図４３に基づき説明する。

【０３４７】

この場合の処理は、ＭＴＡ３２００とデータ管理カードアプリ３３０１の間で行われる。

【０３４８】

実施の形態１と異なり、起動するアプリの元のデータが、セキュア記憶装置３００３に保存されていることによりフローが異なる。

【０３４９】

ＭＴＡ３２００の制御手段３２０５は、データ管理カードアプリ３３０１のカード制御手段３３０４に起動アプリリストデータを要求する（図４３の1)）。

【０３５０】

データ管理カードアプリ３３０１のカード制御手段３３０４は、セキュア記憶装置３００３に保存している起動アプリリストデータを参照し、ＭＴＡ３２００の制御手段３２０５に起動アプリリストデータを送信する（図４３の2)）。

【０３５１】

ＭＴＡ３２００の調査手段３２０４は、端末１０１の処理モジュール１０４で現在起動中のアプリを調べ、起動アプリリストデータに記されているアプリの起動状態を調べる。その結果、ＭＴＡ２００のアプリ操作手段２０３は、起動アプリリストデータ３０７に記されていて、現在起動していないアプリを、起動すべきアプリとして、起動処理を開始する（図４３の3)）。

【０３５２】

ＭＴＡ３２００のアプリ操作手段３２０３は、データ管理カードアプリ３３０１のアプリ発行手段３３０２にアプリの発行を要求する（図４３の4)）。

【０３５３】

データ管理カードアプリ３３０１のアプリ発行手段３３０２は、認証用のセッション鍵を生成し、アプリデータに埋め込む（図４３の5)）。

【０３５４】

データ管理カードアプリ３３０１のアプリ発行手段３３０２は、ＭＴＡ３２００のアプリ操作手段３２０３に対してアプリを発行する（図４３の6)）。

【０３５５】
ＭＴＡ３２００のアプリ操作手段３２０３は、発行されたアプリの起動処理を行う（図４３の7)）。
【０３５６】
起動したアプリの制御手段（データ管理アプリ３３０１の場合ならば、制御手段３２１３のこと）は、埋め込まれたセッション鍵を取得し、データ管理カードアプリ３３０１の認証手段３３０３との間で、セッションを確立する（図４３の8)）。
【０３５７】
セッションを確立したアプリの制御手段は、その後の処理に必要な暗号鍵、復号鍵などのデータをデータ管理カードアプリ３３０１のカード制御手段３３０４に対して、要求し取得する（図４３の9)）。
【０３５８】
以上がＭＴＡ３２００の判断に基づくアプリ起動フローである。
【０３５９】
ユーザの要求に基づくアプリ起動フローについては、図４４に基づき説明する。
【０３６０】
この場合の処理は、ユーザが利用するＧＵＩなどのインターフェースとＭＴＡ３２００とデータ管理カードアプリ３３０１の間で行われる。
【０３６１】
ユーザはＧＵＩなどを通して、ＭＴＡ３２００のアプリ操作手段３２０３に対して、起動したいアプリの起動を要求する（図４４の1)）。
【０３６２】
ＭＴＡ３２００のアプリ操作手段３２０３は、データ管理カードアプリ３３０１のアプリ発行手段３３０２にアプリの発行を要求する（図４４の2)）。
【０３６３】
データ管理カードアプリ３３０１のアプリ発行手段３３０２は、認証用のセッション鍵を生成し、アプリデータに埋め込む（図４４の3)）。
【０３６４】
データ管理カードアプリ３３０１のアプリ発行手段３３０２は、ＭＴＡ３２００のアプリ操作手段３２０３に対してアプリを発行する（図４４の4)）。
【０３６５】
ＭＴＡ３２００のアプリ操作手段３２０３は、発行されたアプリの起動処理を行う（図４４の5)）。
【０３６６】
起動したアプリの制御手段（データ管理アプリ３３０１の場合ならば、制御手段３２１３のこと）は、埋め込まれたセッション鍵を取得し、データ管理カードアプリ３３０１の認証手段３３０３との間で、セッションを確立する（図４４の6)）。
【０３６７】
セッションを確立したアプリの制御手段は、その後の処理に必要な暗号鍵、復号鍵などのデータをデータ管理カードアプリ３３０１のカード制御手段３３０４に対して、要求し取得する（図４４の7)）。
【０３６８】
以上がユーザの要求に基づくアプリ起動フローである。
【０３６９】
接続のフローについて説明する。
【０３７０】
この場合の処理は、サーバとデータ管理アプリ３２０１とデータ管理カードアプリ３３０１の間で行われる。
【０３７１】
実施の形態１と比較して、異なる点は、制御手段２１３が、制御手段３２１３になって

いる点、カード制御手段３０４が、カード制御手段３２０４になっている点である。
【０３７２】
処理フローについては、実施の形態１と同様である。
【０３７３】
目標データ３０６を決定するためのフローについて説明する。
【０３７４】
この場合の処理は、サーバ１０３とデータ管理アプリ３２０１とデータ管理カードアプリ３３０１の間で行われる。
【０３７５】
実施の形態１と比較して、構成データ３０５が、構成データ３３０６になっている点、制御手段２１３が、制御手段３２１３になっている点、カード制御手段３０４が、カード制御手段３３０４になっている点、カード記憶装置１０７が、セキュア記憶装置３００３になっている点、目標データ決定手段２１１が、目標データ決定手段３２１１になっている点、調査手段２１２が、調査手段３２１２になっている点、調査手段２１２が、端末１０１の記憶装置１０５の残り記憶容量ではなく、セキュアデータ管理カード３００１のセキュア記憶装置３００３の、残り記憶容量を調べる点、が異なる。
【０３７６】
データ同期処理のフローを図３５に示す。
【０３７７】
この場合の処理は、サーバ１０３とデータ管理アプリ３２０１とデータ管理カードアプリ３３０１の間で行われる。
【０３７８】
データ管理アプリ３２０１の制御手段３２１３は、同期処理を行うために必要な情報を、データ管理カードアプリ３３０１に要求する（図３５の1)）。
【０３７９】
データ管理カードアプリ３３０１のカード制御手段３３０４は、目標データ３０６のダウンロード、アップロード、削除の目標になっているデータのＩＤを参照する（図３５の2)）。
【０３８０】
データ管理カードアプリ３３０１のカード制御手段３３０４は、データ管理アプリ３２０１に、ダウンロードデータのＩＤリスト、アップロードするデータのＩＤ、削除するデータのＩＤを応答として返す（図３５の3)）。
【０３８１】
応答を受けたデータ管理アプリ３２０１の制御手段３２１３は、ダウンロード、アップロード、削除のいずれかの処理を、適宜開始する。ここでは、ダウンロード、アップロード、削除全ての処理について述べる。
【０３８２】
ダウンロードする場合、データ管理アプリ３２０１のデータ同期手段３２０８は、データのＩＤを指定して、ダウンロードするデータをサーバ１０３へ要求し、サーバ１０３からデータをダウンロードする（図３５の4)、5)）。この際に、データの更新日時、有効期限もダウンロードする。
【０３８３】
データ管理アプリ３２０１の制御手段３２１３は、受信したデータ、更新日時、有効期限を、データ管理カードアプリ３３０１のカード制御手段３３０４に通知する（図３５の6)）。
【０３８４】
データ管理カードアプリ３３０１のカード制御手段３３０４は、受け取ったデータを実データ２１６として保存する（図３５の7)）。
【０３８５】
データ管理カードアプリ３３０１のカード制御手段３３０４は、目標データ３０６のダ

ウンロードしたＩＤの処理状態を「済み」にする（図３５の13)）。
【０３８６】
データ管理カードアプリ３３０１のカード制御手段３３０４は、ダウンロードしたデータのＩＤに対応する構成データ３３０６の更新日時、有効期限を更新する（図３５の14)）。
【０３８７】
ダウンロードする目標データ３０６がまだある場合は処理を継続し、無い場合は目標データ３０６の終了日時を更新する（図３５の15)）。
【０３８８】
データ管理カードアプリ３３０１のカード制御手段３３０４は、サーバ１０３にダウンロードの処理が終了したことと、ダウンロードしたデータのＩＤを報告する（図３５の16))。
【０３８９】
アップロードする場合には、データ管理アプリ３２０１のデータ同期手段３２０８は、サーバ１０３へ送信する実データ２１６と構成データ３３０６の更新日時を、データ管理カードアプリ３３０１のカード制御手段３３０４に要求し、取得する（図３５の8)）。
【０３９０】
データ管理アプリ３２０１のデータ同期手段３２０８は、実データ２１６のＩＤを指定して、サーバ１０３へデータをアップロードする（図３５の9)）。
【０３９１】
データ管理アプリ３２０１の制御手段３２１３は、データ管理カードアプリ３３０１のカード制御手段３３０４に、処理結果とアップロードした実データ２１６のＩＤを通知する（図３５の11)）。
【０３９２】
データ管理カードアプリ３３０１のカード制御手段３３０４は、目標データ３０６において、アップロードした実データ２１６の処理状態を「済み」の状態に更新する（図３５の13)）。
【０３９３】
アップロードする目標データ３０６がまだある場合は処理を継続し、無い場合は目標データ３０６の終了日時を更新する（図３５の15)）。
【０３９４】
データ管理カードアプリ３３０１のカード制御手段３３０４は、サーバ１０３にアップロードの処理が終了したことと、アップロードした実データ２１６のＩＤを報告する（図３５の16)）。
【０３９５】
削除する場合は、データ管理アプリ３２０１のデータ削除手段３３０５は、目標データ３０６に挙がっているＩＤに対応する実データ２１６をセキュア記憶装置３３０３から削除する（図３５の12)）。
【０３９６】
データ管理カードアプリ３３０１のカード制御手段３３０４は、目標データ３０６において、削除した実データ２１６の処理状態を「済み」の状態に更新する（図３５の13))。また、必要に応じて構成データ３３０６自体を削除する。
【０３９７】
削除する目標データ３０６がまだある場合は処理を継続し、無い場合は目標データ３０６の終了日時を更新する（図３５の15)）。
【０３９８】
データ管理カードアプリ３３０１のカード制御手段３３０４は、サーバ１０３に削除の処理が終了したことを通知する。尚、削除の処理の終了の通知と共に、削除した実データ２１６のＩＤを報告しても良い（図３５の16)）。
【０３９９】

以上が、データの同期処理のフローである。

【０４００】

緊急削除時のフローを図３６に示す。

【０４０１】

この場合の処理は、サーバ１０３とデータ管理アプリ３２０１とデータ管理カードアプリ３３０１の間で行われる。

【０４０２】

サーバ１０３が、データを緊急に削除すべきと判断する（図３６の1)）。

【０４０３】

サーバ１０３は、データ管理アプリ３２０１の目標データ決定手段３２１１に緊急削除命令を出す（図３６の2)）。

【０４０４】

緊急削除命令のパターンとしては、２パターンある。一つには、緊急削除命令のみを出す場合である。そして、一つには、緊急削除命令と削除するデータのＩＤリストを出す場合である。

【０４０５】

緊急削除命令だけの場合には、命令を受けたデータ管理アプリ３２０１の目標データ決定手段３２１１は、データ管理カードアプリ３３０１のカード制御手段３３０４に構成データ３３０６と、データポリシーデータ３１１を要求し、それに基づき、削除目標と処理順を決定する（図３６の3)）。

【０４０６】

データ管理アプリ３２０１の制御手段３２１３は、データ管理カードアプリ３３０１のカード制御手段３３０４に対して、緊急削除の通知と、目標データ３０６の通知を行う（図３６の4)）。

【０４０７】

データ管理カードアプリ３３０１のカード制御手段３３０４は、目標データ３０６を更新し、緊急削除の目標データを追加する（図３６の5)）。

【０４０８】

データ管理カードアプリ３３０１のカード制御手段３３０４は、起動アプリリストデータの緊急削除フラグをＯＮにする（図３６の6)）。削除が行われるのがカード内である点が、実施の形態１と異なる。

【０４０９】

データ管理カードアプリ３３０１のデータ削除手段３３０５は、緊急削除の目標となる実データ２１６をセキュア記憶装置３００３から削除する（図３６の7)）。また、データ管理カードアプリ３３０１のカード制御手段３３０４は、鍵データを削除する。データ管理カードアプリ３３０１のカード制御手段３３０４は、目標データ３０６において、削除した実データ２１６の処理状態を「済み」の状態にする（図３６の8)）。

【０４１０】

データ管理カードアプリ３３０１のカード制御手段３３０４は、構成データ３３０６を削除しても良い（図３６の9)）。

【０４１１】

削除する目標データ３０６がまだある場合は緊急削除処理を継続し、無い場合は目標データ３０６の終了日時を更新する（図３６の10)）。

【０４１２】

データ管理カードアプリ３３０１のカード制御手段３３０４は、起動アプリリストデータ３０７から、緊急削除フラグの情報を、ＯＦＦにする（図３６の11)）。

【０４１３】

データ管理カードアプリ３３０１のカード制御手段３３０４は、サーバ１０３に緊急削除の処理が終了したことと、削除したデータのＩＤを報告する（図３６の12)）。

【０４１４】

実データ２１６が、カードに保存されているため、実施の形態１と処理フローが異なる。

【０４１５】

以上が、緊急削除時のフローである。

【０４１６】

有効期限切れ削除のフローを図３７に示す。

【０４１７】

この場合の処理は、データ管理アプリ３２０１とデータ管理カードアプリ３３０１の間で行われる。

【０４１８】

データ管理アプリ３２０１の制御手段３２１３は、データ管理カードアプリ３３０１に要求し、構成データ３３０６を取得する（図３７の1)）。

【０４１９】

データ管理アプリ３２０１の目標データ３０６決定手段は、構成データ３３０６の有効期限情報と現在の日時情報を比較し、有効期限の切れている実データ２１６のＩＤを、削除する目標データとして挙げる（図３７の2)）。

【０４２０】

データ管理アプリ３２０１の制御手段３２１３は、データ管理カードアプリ３３０１のカード制御手段３３０４に目標データ３０６を通知する（図３７の3)）。

【０４２１】

データ管理カードアプリ３３０１のカード制御手段３３０４は、目標データ３０６を更新する（図３７の4)）。

【０４２２】

データ管理カードアプリ３３０１のデータ削除手段３３０５は、削除の目標となるＩＤに対応するデータをセキュア記憶装置３００３から削除する（図３７の5)）。

【０４２３】

データ管理カードアプリ３３０１のカード制御手段３３０４は、目標データ３０６において、削除した実データ２１６の処理状態を「済み」の状態にする（図３７の6)）。

【０４２４】

データ管理カードアプリ３３０１のカード制御手段３３０４は、構成データ３３０６を削除する（図３７の7)）。

【０４２５】

削除する目標データ３０６がまだある場合は処理を継続し、無い場合は目標データ３０６の終了日時を更新する（図３７の8)）。

【０４２６】

以上が有効期限切れ削除のフローである。

【０４２７】

実データ２１６の参照のフローについて説明する。

【０４２８】

この場合の処理は、データ管理アプリ３２０１とデータ管理カードアプリ３３０１の間で行われる。

【０４２９】

データ管理アプリ３２０１の制御手段３２１３は、ユーザ操作もしくは、他のアプリから参照したい実データ２１６のＩＤを要求として受信し、データ管理カードアプリ３３０１のカード制御手段３３０４に、要求に対応する実データ２１６を要求する。

【０４３０】

データ管理カードアプリ３３０１のカード制御手段３３０４は、セキュア記憶装置３００３の実データ２１６を参照し、ＩＤに対応する実データ２１６を参照する。

【０４３１】

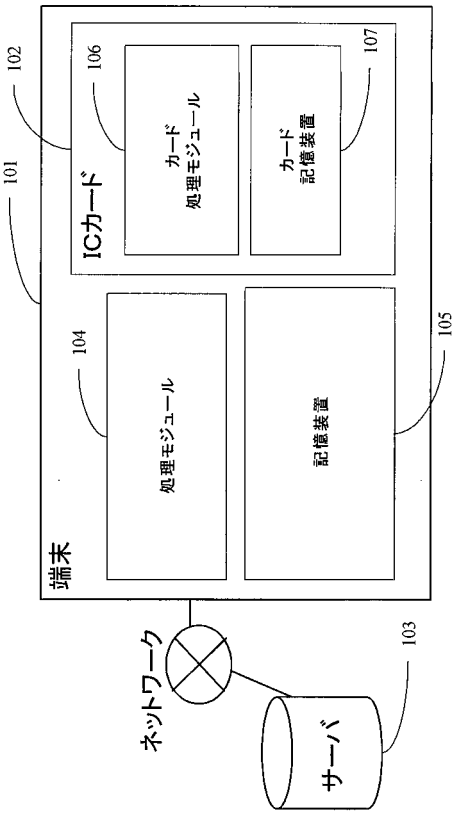
データ管理カードアプリ３３０１のカード制御手段３３０４は、データ管理アプリの制

御手段３２１３に実データ２１６を送信する。
【０４３２】
以上が、実データ２１６の参照のフローである。
【０４３３】
時刻を比較する際の現在時刻は、以下の仕組みを利用して取得している。
【０４３４】
信頼できる時刻の取得と保存のフローについて説明する。
【０４３５】
この場合の処理は、サーバとＭＴＡ３２００とデータ管理カードアプリ３３０１と端末１０１上で動作しているアプリの間で行われる。
【０４３６】
実施の形態１と比較すると、異なる点は、制御手段２０５が、制御手段３２０５になっている点、時刻取得手段２０６が、時刻取得手段３２０６になっている点、時刻カウント手段２０７が、時刻カウント手段３２０７になっている点、カード制御手段３０４が、カード制御手段３３０４になっている点、カード記憶装置１０７が、セキュア記憶装置３００３になっている点、カード時刻カウント手段３１４が、カード時刻カウント手段３３１４になっている点、である。
【０４３７】
なお、本発明はこれらの実施の形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実施し得る。
【産業上の利用可能性】
【０４３８】
本発明は、ＩＣカードなどのセキュアデバイスを装着でき、様々なアプリケーションを実行でき、ネットワーク上のデータベースサーバと同期処理などを行う、携帯電話、携帯情報端末（ＰＤＡ）、パーソナルコンピュータなどの情報処理装置に適用が可能である。
【図面の簡単な説明】
【０４３９】
【図１】本発明の実施の形態１における、セキュアデータ管理装置システム構成図
【図２】本発明の実施の形態１における、端末機能ブロック図
【図３】本発明の実施の形態１における、ＩＣカード機能ブロック図
【図４】本発明の実施の形態１におけるセキュアデータ管理装置処理概要図
【図５】本発明の実施の形態１における、ＭＴＡの起動フロー
【図６】本発明の実施の形態１における、ＭＴＡの判断に基づくアプリ起動フロー
【図７】本発明の実施の形態１における、ユーザの要求操作に基づくアプリ起動フロー
【図８】本発明の実施の形態１における、サーバへの接続フロー
【図９】本発明の実施の形態１における、目標データ決定フロー
【図１０】本発明の実施の形態１における、データの同期処理フロー
【図１１】本発明の実施の形態１における、データの緊急削除フロー
【図１２】本発明の実施の形態１における、有効期限切れデータの削除フロー
【図１３】本発明の実施の形態１における、データポリシーデータのフォーマット
【図１４】本発明の実施の形態１における、データポリシーデータ具体例
【図１５】本発明の実施の形態１における、図１４をデータ形式で表現したデータポリシーデータ
【図１６】本発明の実施の形態１における、構成データフォーマット
【図１７】本発明の実施の形態１における、構成データ具体例その１
【図１８】本発明の実施の形態１における、構成データ具体例その２
【図１９】本発明の実施の形態１における、図１７をデータ形式で表現した構成データ
【図２０】本発明の実施の形態１における、図１８をデータ形式で表現した構成データ
【図２１】本発明の実施の形態１における、目標データフォーマット
【図２２】本発明の実施の形態１における、目標データ具体例

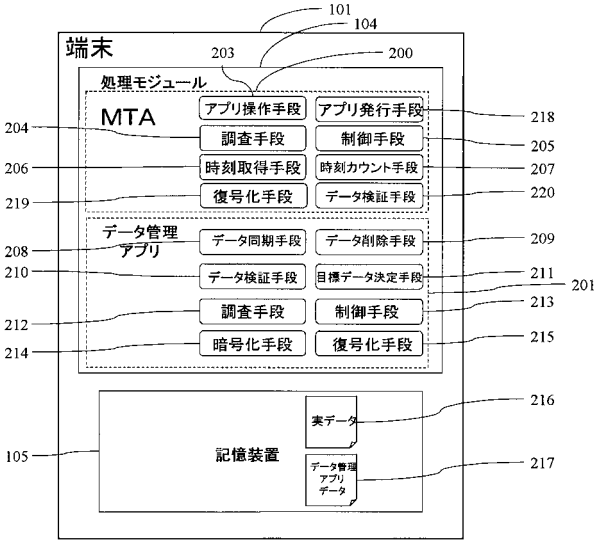
【図２３】本発明の実施の形態１における、図２２をデータ形式で表現した目標データ
【図２４】本発明の実施の形態１における、起動アプリリストデータ
【図２５】本発明の実施の形態１における、起動アプリリストデータ具体例
【図２６】本発明の実施の形態１における、図２５をデータ形式で表現した起動アプリリストデータ
【図２７】本発明の実施の形態１における、前回更新日時データ
【図２８】本発明の実施の形態１における、前回更新日時データ具体例
【図２９】本発明の実施の形態１における、図２８をデータ形式で表現した前回更新日時データ
【図３０】本発明の実施の形態１における、時刻の取得と保存フロー
【図３１】本発明の実施の形態２における、セキュアデータ管理装置システム構成図
【図３２】本発明の実施の形態２における、端末機能ブロック図
【図３３】本発明の実施の形態２における、セキュアデータ管理カード機能ブロック図
【図３４】本発明の実施の形態２におけるセキュアデータ管理装置処理概要図
【図３５】本発明の実施の形態２における、データの同期処理フロー
【図３６】本発明の実施の形態２における、データの緊急削除フロー
【図３７】本発明の実施の形態２における、有効期限切れデータの削除フロー
【図３８】本発明の実施の形態２における、構成データフォーマット
【図３９】本発明の実施の形態２における、構成データ具体例その１
【図４０】本発明の実施の形態２における、構成データ具体例その２
【図４１】本発明の実施の形態２における、図３９をデータ形式で表現した構成データ
【図４２】本発明の実施の形態２における、図４０をデータ形式で表現した構成データ
【図４３】本発明の実施の形態２における、ＭＴＡの判断に基づくアプリ起動フロー
【図４４】本発明の実施の形態２における、ユーザの要求操作に基づくアプリ起動フロー
【図４５】従来例のブロック構成図
【符号の説明】
【０４４０】
１０１　端末
１０２　ＩＣカード
１０３　サーバ
１０４　処理モジュール
１０５　記憶装置
１０６　カード処理モジュール
１０７　カード記憶装置
２００　ＭＴＡ
２０１　データ管理アプリ
２０３　アプリ操作手段
２０４　調査手段
２０５　制御手段
２０６　時刻取得手段
２０７　時刻カウント手段
２０８　データ同期手段
２０９　データ削除手段
２１０　データ検証手段
２１１　目標データ決定手段
２１２　調査手段
２１３　制御手段
２１４　暗号化手段
２１５　復号化手段
２１６　実データ

２１７　データ管理アプリデータ
２１８　アプリ発行手段
２１９　復号化手段
２２０　データ検証手段
３０１　データ管理カードアプリ
３０２　アプリ発行手段
３０３　認証手段
３０４　カード制御手段
３０５　構成データ
３０６　目標データ
３０７　起動アプリリストデータ
３０８　前回更新日時データ
３０９　ＭＴＡデータ
３１１　データポリシーデータ
３１２　鍵データ
３１３　時刻データ
３１４　カード時刻カウント手段
３００１　セキュアデータ管理カード
３００２　カード処理モジュール
３００３　セキュア記憶装置
３００４　カード記憶装置
３２００　ＭＴＡ
３２０１　データ管理アプリ
３２０３　アプリ操作手段
３２０４　調査手段
３２０５　制御手段
３２０６　時刻取得手段
３２０７　時刻カウント手段
３２０８　データ同期手段
３２１１　目標データ決定手段
３２１２　調査手段
３２１３　制御手段
３３０１　データ管理カードアプリ
３３０２　アプリ発行手段
３３０３　認証手段
３３０４　カード制御手段
３３０６　構成データ
３３１４　カード時刻カウント手段

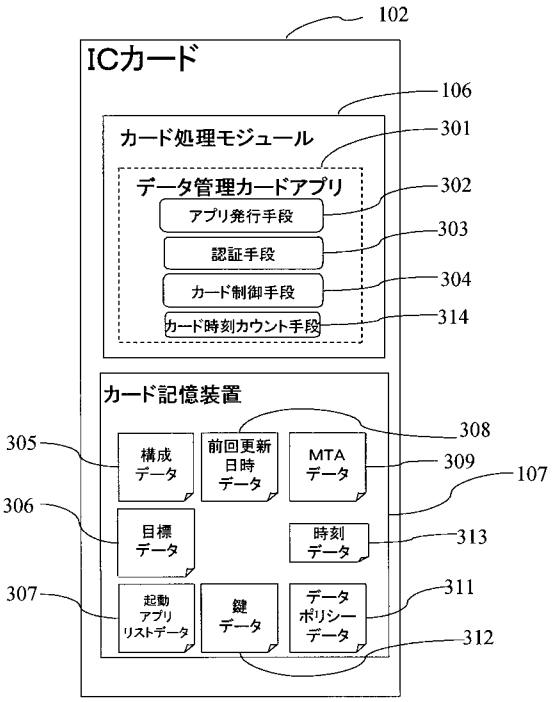
【図１】


102
106
107
101
ICカード
カード
処理モジュール
カード
記憶装置
104
105
処理モジュール
記憶装置
端末
ネットワーク
103
サーバ

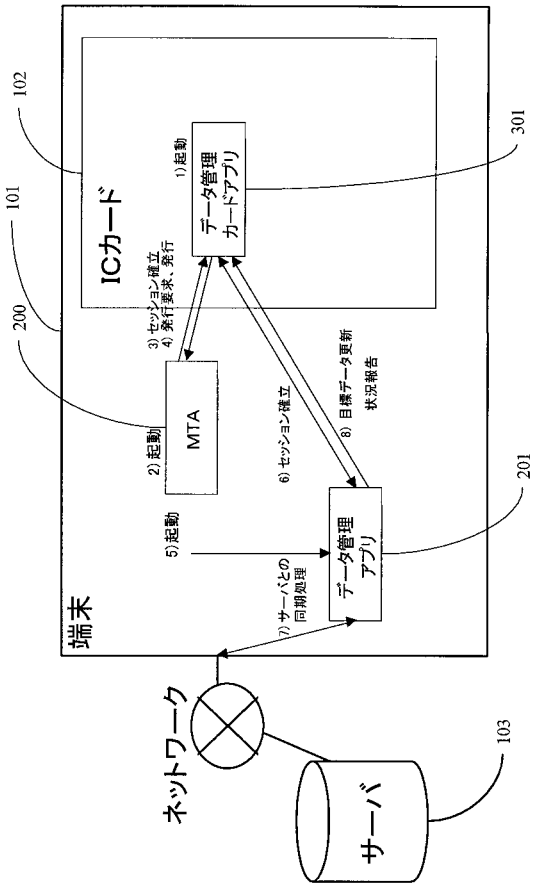
【図２】


101
104
端末
203
200
処理モジュール
MTA
アプリ操作手段
アプリ発行手段
218
204
調査手段
制御手段
205
206
時刻取得手段
時刻カウント手段
207
219
復号化手段
データ検証手段
220
データ管理
アプリ
208
データ同期手段
データ削除手段
209
210
データ検証手段
目標データ決定手段
211
201
212
調査手段
制御手段
213
214
暗号化手段
復号化手段
215
105
記憶装置
実データ
216
データ管理
アプリ
データ
217

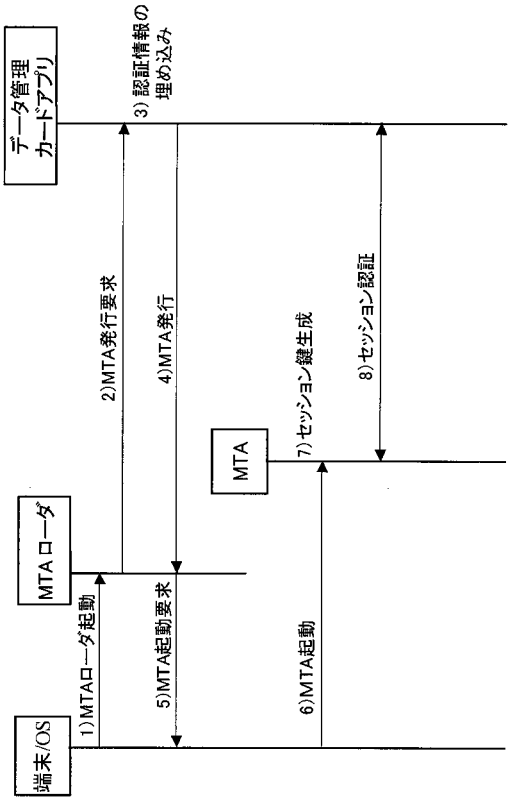
【図３】


102
ICカード
106
カード処理モジュール
301
データ管理カードアプリ
302
アプリ発行手段
303
認証手段
304
カード制御手段
314
カード時刻カウント手段
カード記憶装置
308
305
構成
データ
前回更新
日時
データ
MTA
データ
309
107
306
目標
データ
時刻
データ
313
307
起動
アプリ
リストデータ
鍵
データ
データ
ポリシー
データ
311
312

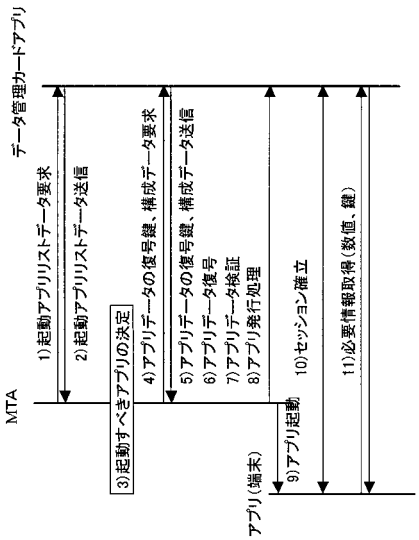
【図４】


102
301
ICカード
1)起動
データ管理
カードアプリ
101
3) セッション確立
4) 発行要求、発行
200
MTA
2) 起動
6) セッション確立
8) 目標データ更新
状況報告
201
5)起動
データ管理
アプリ
7) サーバとの
同期処理
端末
ネットワーク
103
サーバ

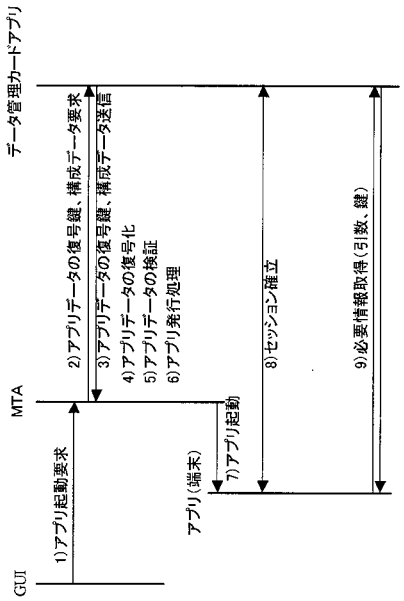
【図５】


データ管理
カードアプリ
3) 認証情報の
埋め込み
2)MTA発行要求
4)MTA発行
MTA ローダ
MTA
7)セッション鍵生成
8)セッション認証
1)MTAローダ起動
5)MTA起動要求
6)MTA起動
端末/OS

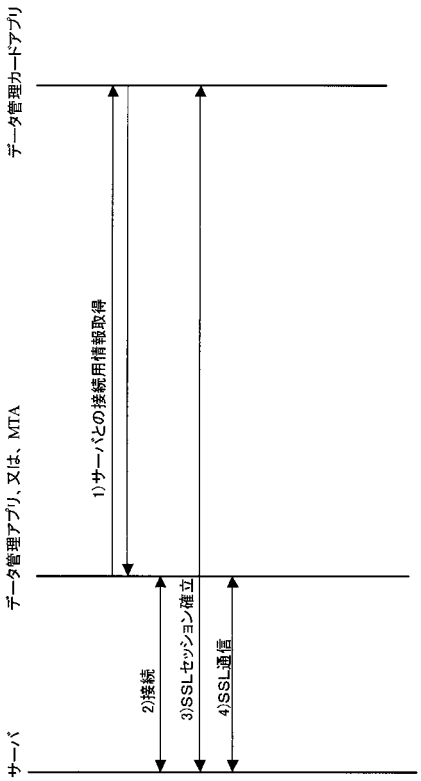
【図６】


データ管理カードアプリ
MTA
1)起動アプリリストデータ要求
2)起動アプリリストデータ送信
3)起動すべきアプリの決定
4)アプリデータの復号鍵、構成データ要求
5)アプリデータの復号鍵、構成データ送信
6)アプリデータ復号
7)アプリデータ検証
8)アプリ発行処理
アプリ(端末)
9)アプリ起動
10)セッション確立
11)必要情報取得(数値、鍵)

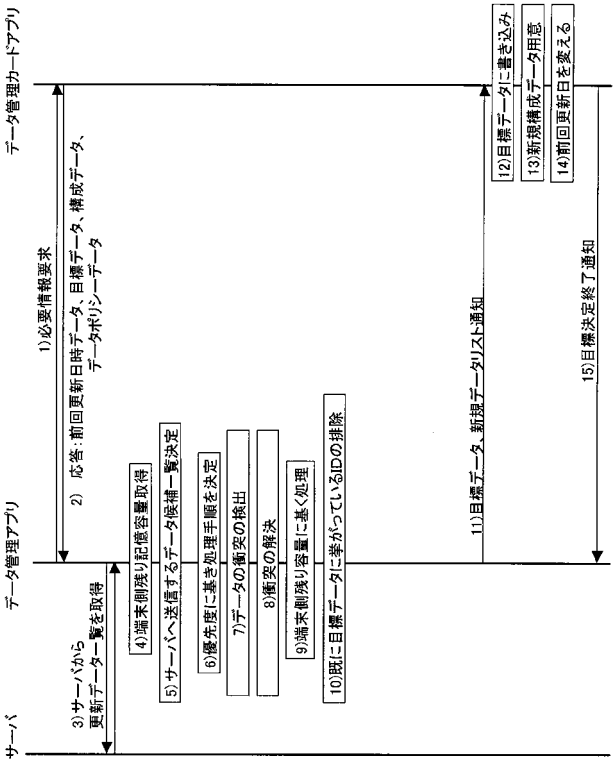
【図７】


データ管理カードアプリ
MTA
2)アプリデータの復号鍵、構成データ要求
3)アプリデータの復号鍵、構成データ送信
4)アプリデータの復号化
5)アプリデータの検証
6)アプリデータ発行処理
1)アプリ起動要求
アプリ(端末)
7)アプリ起動
8)セッション確立
9)必要情報取得(引数、鍵)
GUI

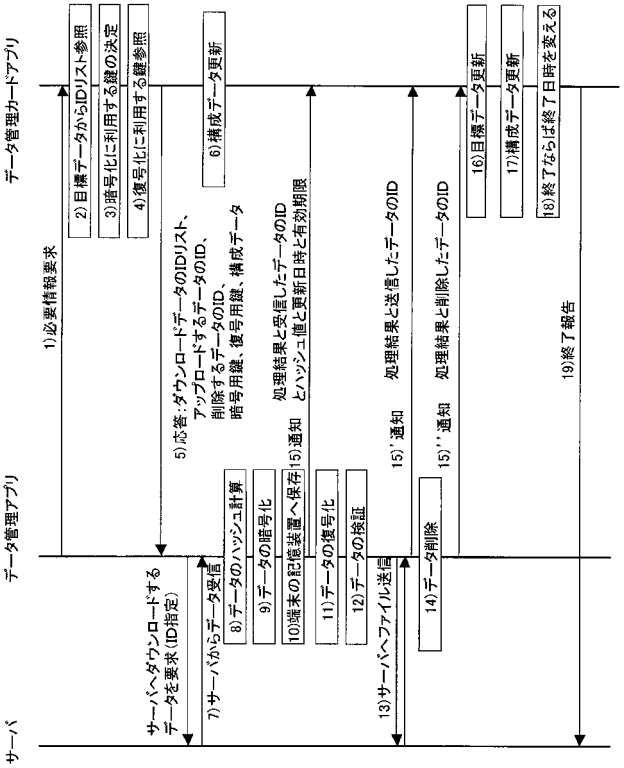
【図８】


データ管理カードアプリ
1)サーバとの接続用情報取得
データ管理アプリ、又は、MTA
2)接続
3)SSLセッション確立
4)SSL通信
サーバ

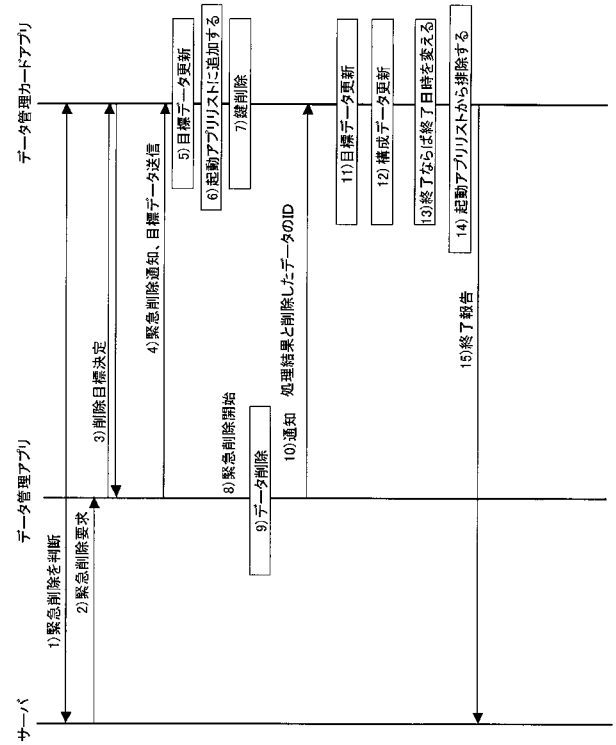
【図９】



【図１０】



【図１１】



【図１２】

【図１３】

項目名	内容
処理名(0)	削除(0)、アップロード(1)、ダウンロード(2)、緊急削除(3)
最優先データ(1)	実データのID
それ以外の決定基準(2)	IDの小さい順(0)、大きい順 更新日の新しい順(1)、古い順(2)
削除と更新での 目標データの衝突の場合の 優先基準(3)	削除優先(0)、更新優先(1)、サーバ側の判断(2)、端末側の判断(3)
更新と更新での 目標データの衝突の場合の 優先基準(4)	更新日の新しい方優先(0)、古い方優先(1)、サーバ優先(2)、端末優先(3)

【図１４】

処理名:削除
最優先削除:001,003
それ以外決定基準:IDの小さい順

処理名:アップロード
最優先:002,004
それ以外の決定基準:更新日の新しい順

処理名:ダウンロード
最優先:005,006
それ以外の決定基準:更新日の古い順

処理名:緊急削除
最優先:001,003,010,111
それ以外の決定基準:IDの小さい順

データの衝突時
削除と更新:削除優先
更新と更新:新規優先

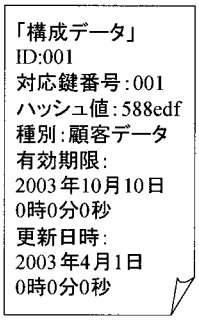
【図１５】

0,0
1,001,003
2,0
0,1
1,002,004
2,2
0,2
1,005,006
2,3
0,3
1,001,003,010,111
2,0
3,0
4,0

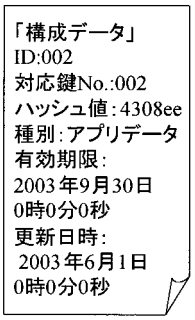
【図１６】

項目名	内容
ID(0)	実データのID
対応鍵番号(1)	鍵番号
ハッシュ値(2)	ハッシュ値
種別(3)	顧客データ(0)、 アプリデータ(1)
有効期限(4)	年月分秒
更新日時(5)	年月分秒

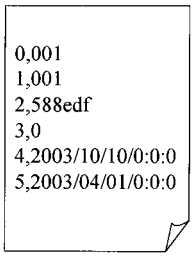
【図１７】



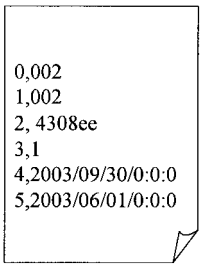
【図１８】



【図１９】



【図２０】



【図２１】

項目名	内容
処理名(0)	削除(0)、アップロード(1)、ダウンロード(2)、緊急削除(3)
実データのID(1)	実データのID、 処理状況(未処理(0)、処理済み(1))
開始日時(2)	年月分秒
中断日時(3)	年月分秒
終了日時(4)	年月分秒

【図２２】

削除:
ID:001　済
ID:002
ID:003
開始日時:
2003月1月1日0時0分0秒
中断日時:
2003月1月2日0時0分0秒
終了日時:
アップロード:
ID:004
ID:005
開始日時:
2003月6月1日0時0分0秒
中断日時:
2003月6月1日0時0分0秒
終了日時:
ダウンロード:
ID:006
開始日時:
2003月6月1日0時0分0秒
中断日時:
2003月6月1日0時0分0秒
終了日時:

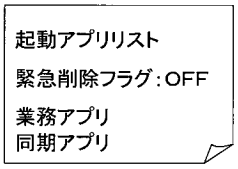
【図２３】

0,0
1,001,1
1,002,0
1,003,0
2,2003/01/01/0:0:0
3,2003/01/02/0:0:0
4,
0,1
1,004,0
1,005,0
2,2003/06/01/0:0:0
3,2003/06/01/0:0:0
4,
0,2
1,006,0
2,2003/06/01/0:0:0
3,2003/06/01/0:0:0
4,

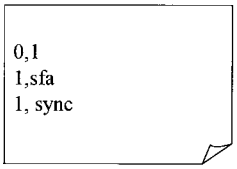
【図２４】

項目名	内容
緊急削除フラグ(0)	緊急削除ON(0)、OFF(1)
起動アプリ名(1)	アプリ名

【図２５】



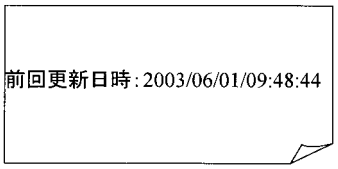
【図２６】



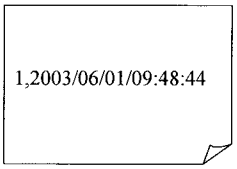
【図２７】

項目名	内容
前回更新日時(1)	年月分秒

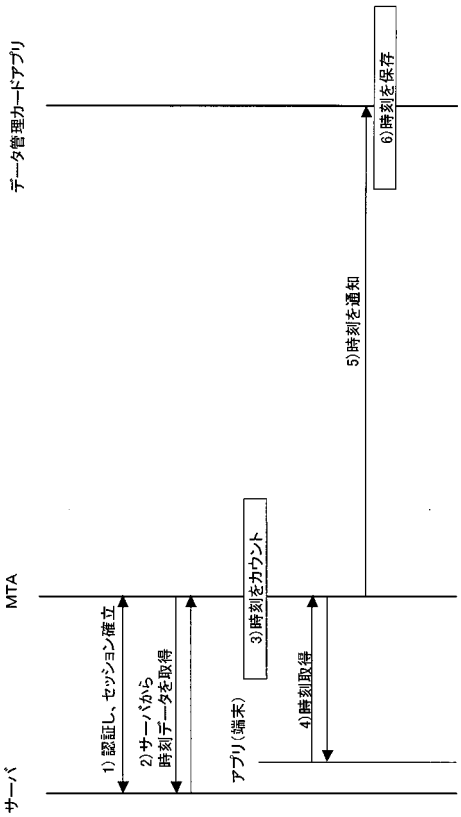
【図２８】



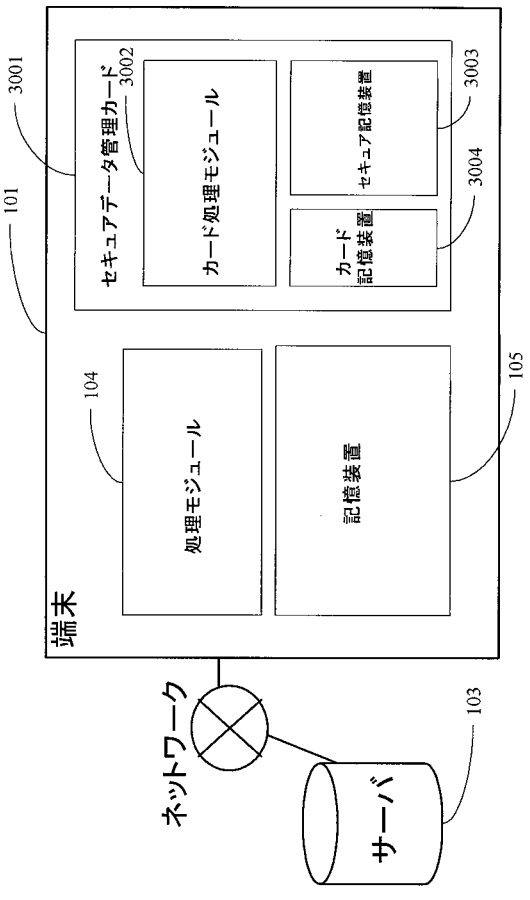
【図２９】



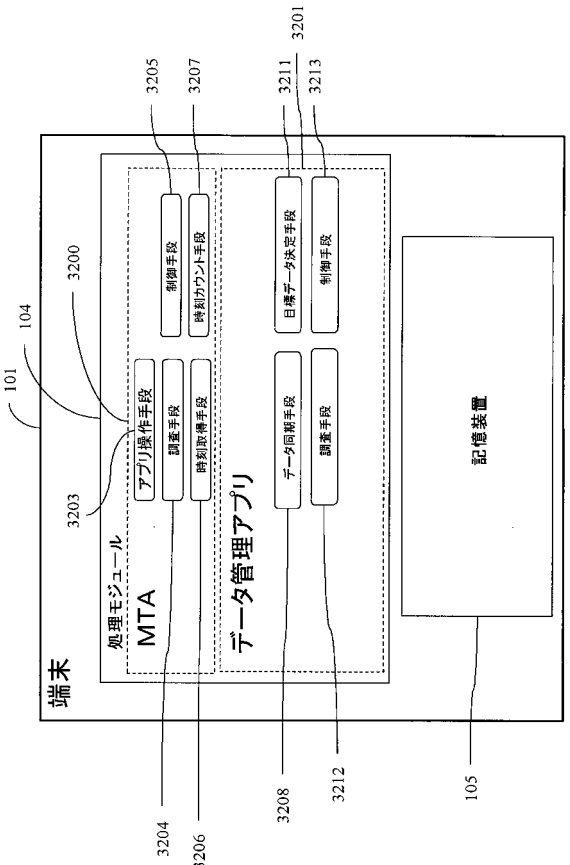
【図３０】



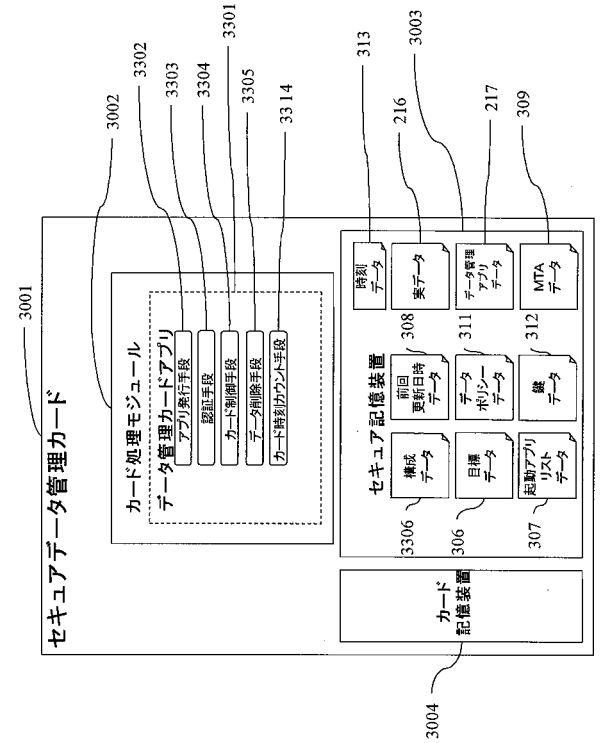
【図３１】



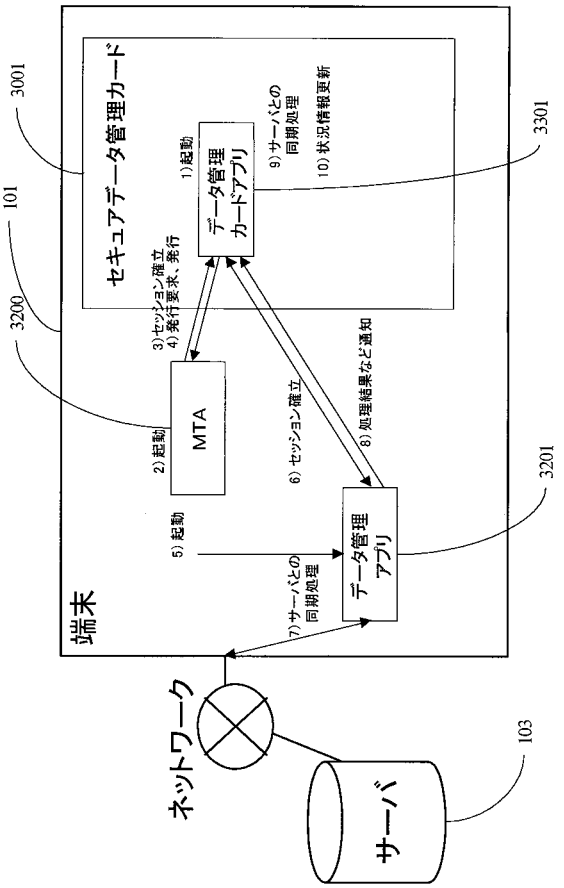
【図３２】



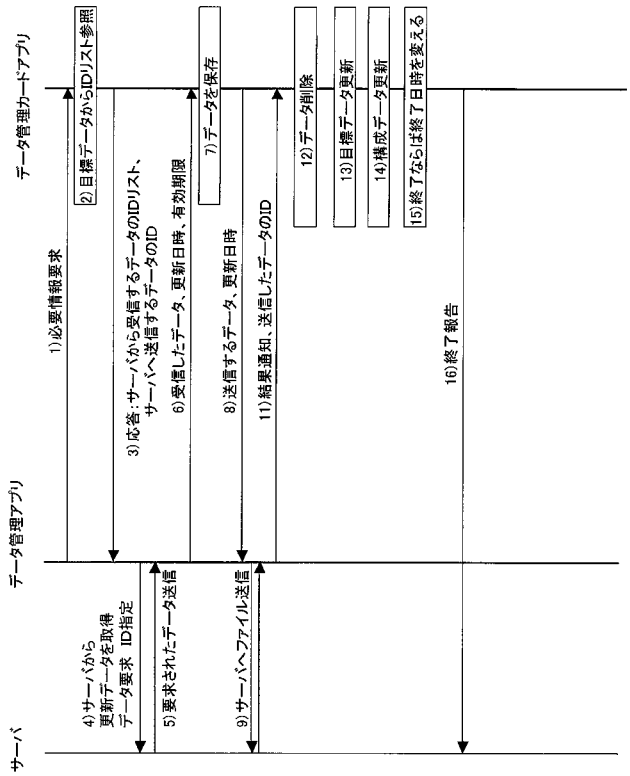
【図３３】



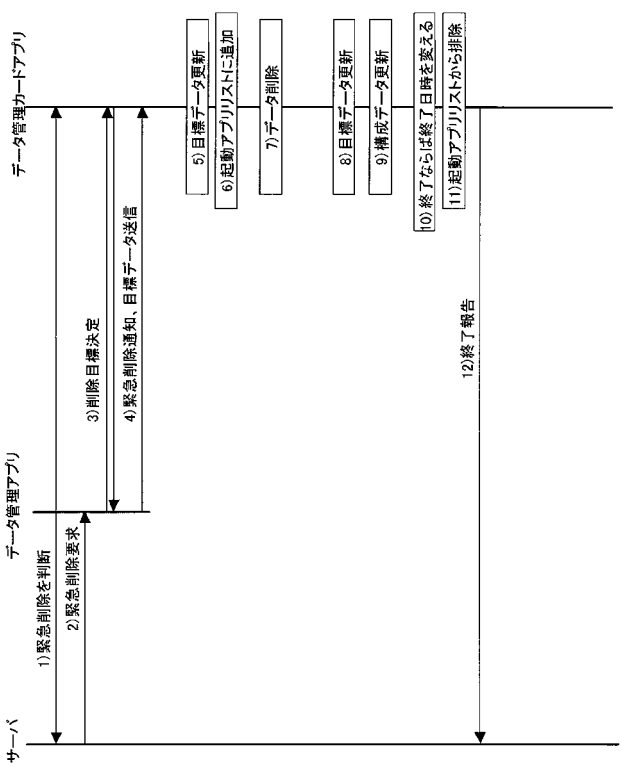
【図３４】



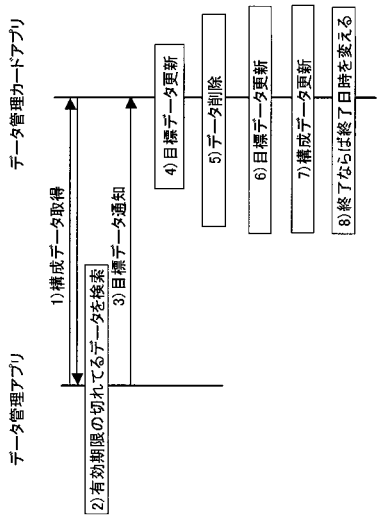
【図３５】



【図３６】



【図３７】



【図３８】

項目名	内容
ID(0)	実データのID
種別(1)	顧客データ(0)、アプリデータ(1)
有効期限(2)	年月分秒
更新日時(3)	年月分秒

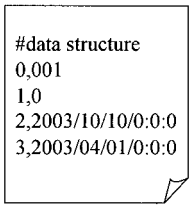
【図３９】

「構成データ」
ID:001
種別:顧客データ
有効期限:
2003年10月10日
0時0分0秒
更新日時:
2003年4月1日
0時0分0秒

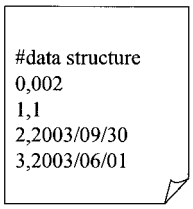
【図４０】

「構成データ」
ID:002
種別:アプリデータ
有効期限:
2003年9月30日
0時0分0秒
更新日時:
2003年6月1日
0時0分0秒

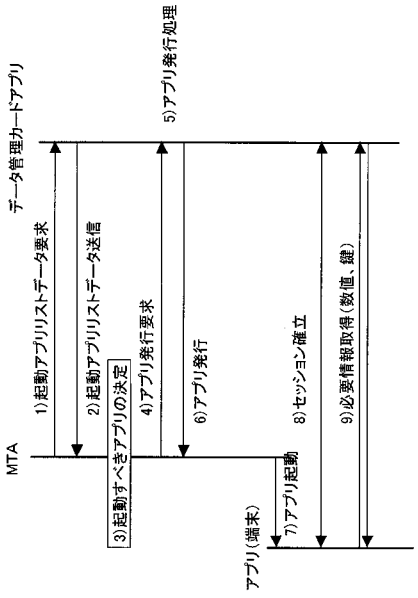
【図４１】



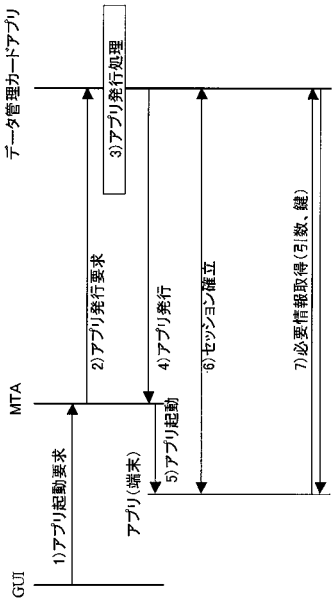
【図４２】



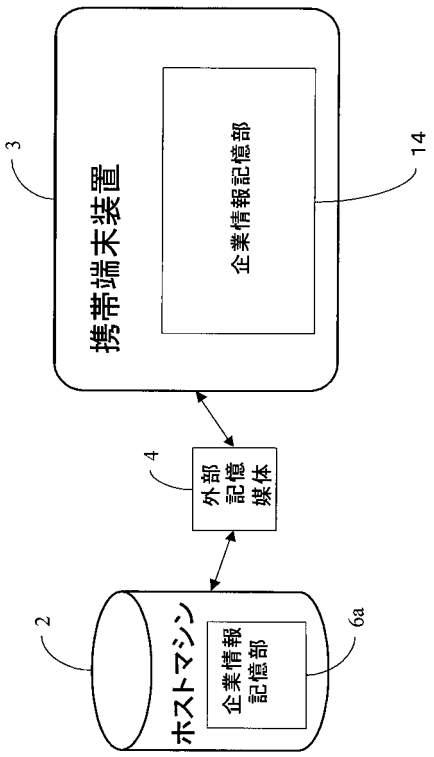
【図４３】



【図４４】



【図４５】



フロントページの続き

Ｆターム(参考) 5B058 CA27 KA32
5J104 LA01 NA37 NA38 NA40 NA41