

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2003年11月27日 (27.11.2003)

PCT

(10) 国際公開番号  
WO 03/098442 A1

(51) 国際特許分類?: G06F 12/14,  
9/44, H04B 7/26, H04M 1/00, 1/725

[JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目11  
番1号 Tokyo (JP).

(21) 国際出願番号: PCT/JP03/06099

(22) 国際出願日: 2003年5月16日 (16.05.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:  
特願2002-143608 2002年5月17日 (17.05.2002) JP

(71) 出願人(米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.)

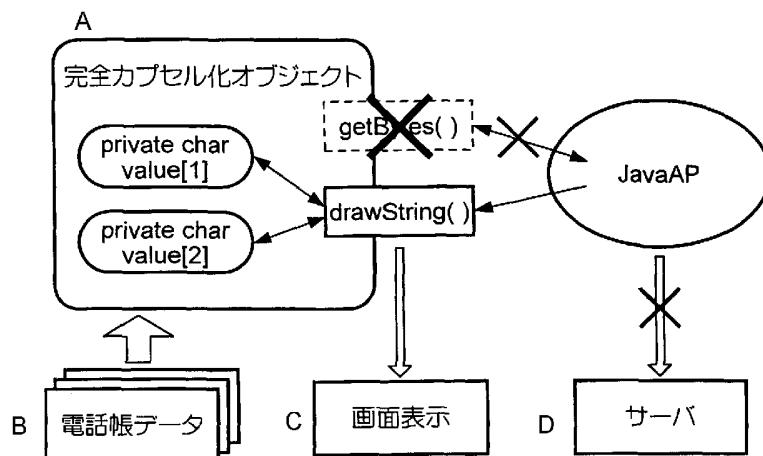
(72) 発明者; および

(75) 発明者/出願人(米国についてのみ): 神谷 大 (KAMIYA,Dai) [JP/JP]; 〒100-6150 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 Tokyo (JP). 山田 和宏 (YAMADA,Kazuhiro) [JP/JP]; 〒100-6150 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 Tokyo (JP). 鶯見 豊 (SUMI,Yutaka) [JP/JP]; 〒106-0044 東京都 港区 東麻布一丁目23-8-502 Tokyo (JP).

[続葉有]

(54) Title: COMMUNICATION DEVICE

(54) 発明の名称: 通信装置



A...COMPLETELY CAPSULATED OBJECT

B...TELEPHONE DIRECTORY DATA

C...SCREEN DISPLAY

D...SERVER

WO 03/098442 A1

(57) Abstract: A cellular phone (40) encapsulates data of high level of importance and contents the copyright of which must be protected, stored in the cellular phone (40) and treats the encapsulated data as a completely capsulated object that has only a method that will not pass the encapsulated data to an operating program. A JavaAP downloaded in the cellular phone (40) issues an instruction to the completely capsulated object to instruct an operation on the encapsulated data in the object using a method provided in the object. This does not lose the convenience of a program provided via a network and ensures the security of such a program.

(57) 要約: 携帯電話機40は、当該携帯電話機40に記憶されている重要度の高いデータや著作権を保護しなければならないコンテンツなどを、これらのデータやコンテンツなどをカプセル化して有する

[続葉有]



(74) 代理人: 川崎 研二 (KAWASAKI,Kenji); 〒103-0027 東京都 中央区 日本橋一丁目 2 番 10 号 東洋ビルディング 7 階 朝日特許事務所 Tokyo (JP).

添付公開書類:  
— 國際調査報告書

(81) 指定国 (国内): AU, BR, CA, CN, ID, IN, KR, NO, NZ, PH, PL, SG, US.

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイド」を参照。

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

---

とともに、当該カプセル化されたデータを操作元のプログラムへ引き渡すことのないメソッドのみを有する完全カプセル化オブジェクトとして扱う。携帯電話機 40 にダウンロードされた Java API は、完全カプセル化オブジェクトに対し、このオブジェクトに備わるメソッドを用いて当該オブジェクト内のカプセル化されたデータに対する操作を指令する。これにより、ネットワークを介して提供されるプログラムの利便性を損なわせることなく、かつ、このようなプログラムに対するセキュリティを確保できる。

## 明細書

## 通信装置

## 5 技術分野

この発明は、通信装置のセキュリティを確保するための技術ならびにコンテンツの著作権を保護するための技術に関する。

## 背景技術

10 例えば、パケット通信機能を有する携帯電話機やパーソナルコンピュータなどの通信装置は、インターネットに接続されているサーバから様々なプログラムをダウンロードすることができる。

ところで、インターネットなどのオープンネットワークでは、世界中の様々な人々が自由に情報の公開やプログラムの提供を行うことができる。オープンネットワークは、このような利点を有する反面、不都合もある。例えば、悪意の有る個人や団体が通信装置内に記憶されているデータを密かに盗み出すプログラムを提供することがある。あるいは悪意は無いものの通信装置において動作させると不具合を引き起こしてしまうプログラムが提供されてしまうことがある。

したがって、ネットワークを介して提供されたプログラムに対して通信装置の内部および外部のリソースを何ら制限することなくアクセスできるようにしてしまうと、問題が起こる可能性がある。例えば、通信装置内に記憶されているユーザの電話番号やメールアドレス、銀行口座番号などが勝手に読み出され、通信装置の外へ流出してしまうといった事態が生じ得る。

このため、例えば、Java（登録商標）言語で記述されたプログラムを実行することが可能な通信装置においては、次のような制限がある。すなわち、ネットワークを介して提供されたJavaプログラムを実行している場合に、このJavaプログラムの実行過程においてアクセスすることのできるリソースをごく限られたものだけに制限している。これにより信頼性を完全に保証することのできないプログラムが、例えば、通信装置内のアドレス帳データやユーザの個人情

報などにアクセスすることを禁じている。

### 発明の開示

上述したアクセス制限の仕組みは、通信装置におけるセキュリティを確保する

5 上で一定の効果を奏するものの、ネットワークを介して提供されるプログラムに  
対して様々な動作制限を課すことになる。すなわち、このようなアクセス制限は  
、ネットワークを介して提供されるプログラムが本来有する、通信装置における  
機能の変更や追加などを自由に行えるという利便性を損なう要因であった。

しかしながら、ネットワークを介して提供されたプログラムの実行に際し、何  
10 10 アクセスの制限を行なわない場合、次のような危険性がある。すなわち、前述  
した悪意の有る個人や団体が提供するプログラムや、通信装置において動作させ  
ると不具合を引き起こしてしまうプログラムなどによる被害が、このプログラム  
を実行した通信装置のみならず、この通信装置と通信を行った他の電子機器にま  
で及んでしまうおそれがある。

15 本発明は、以上説明した事情に鑑みてなされたものであり、ネットワークを介  
して提供されるプログラムの利便性を損なわせることなく、かつ、このようなプロ  
グラムに対するセキュリティを確保することのできる通信装置、プログラムおよび記録媒体を提供することを目的としている。

上記課題を解決するために、この発明は、プログラムを受信する受信手段と、  
20 当該通信装置に記憶されているデータのうち、受信手段により受信されたプロ  
グラムを実行した場合に使用されるデータを特定する特定手段と、特定手段により  
特定され、カプセル化されたデータを有するオブジェクトであって、カプセル化  
されたデータをオブジェクトの外部から操作するためのメソッドであり、かつ、  
そのデータを操作元のプログラムへ引き渡すことのないメソッドのみを有する完  
25 全カプセル化オブジェクトを生成する第1の生成手段と、受信手段により受信さ  
れたプログラムを実行している場合にアクセスすることのできるリソースを制限  
し、当該通信装置に記憶されているデータのうち特定手段により特定されたデー  
タへのアクセスを禁止する一方、生成手段により生成されたオブジェクトへのア  
クセスを許可するアクセス制御手段とを有する通信装置を提供する。

また、この発明は、通信部にプログラムを受信させる受信ステップと、記憶部に記憶されているデータのうち、受信ステップにて受信されたプログラムを実行した場合に使用されるデータを特定する特定ステップと、特定ステップにて特定され、カプセル化されたデータを有するオブジェクトであって、カプセル化されたデータをそのオブジェクトの外部から操作するためのメソッドであり、かつ、そのデータを操作元のプログラムへ引き渡すことのないメソッドのみを有するオブジェクトを生成する生成ステップと、受信ステップにて受信されたプログラムを実行している場合にアクセスすることのできるリソースを制限し、記憶部に記憶されているデータのうち特定ステップにて特定されたデータへのアクセスを禁止する一方、生成ステップにて生成されたオブジェクトへのアクセスを許可するアクセス制御ステップとをコンピュータに実行させるためのプログラムを提供してもよい。

この発明によれば、通信装置は、受信したプログラムに基づく処理の実行中に、当該処理において使用されるデータをカプセル化して有しているオブジェクトにアクセスすることが可能となる。また、通信装置は、受信したプログラムに基づく処理の実行中に、オブジェクト内にカプセル化されているデータそのものを取得することはできないが、このオブジェクトに備わるメソッドを用いてオブジェクト内のデータに対する操作を行うことが可能となる。

また、この発明は、プログラムを受信する受信手段と、当該通信装置に記憶されているデータのうち、受信手段により受信されたプログラムを実行した場合に使用されるデータを特定する特定手段と、特定手段により特定され、カプセル化されたデータを有するオブジェクトであって、カプセル化されたデータを当該オブジェクトの外部から操作するためのメソッドであり、かつ、前記データを操作元のプログラムへ引き渡すことのないメソッドのみを有する完全カプセル化オブジェクトを生成する第1の生成手段と、特定手段により特定され、カプセル化されたデータを有するオブジェクトであって、カプセル化されたデータを当該オブジェクトの外部から操作するためのメソッドであり、かつ、そのデータを操作元のプログラムへ引き渡すメソッドを少なくとも1つ有する非完全カプセル化オブジェクトを生成する第2の生成手段と、データの保護の要否を示す保護要否情報

を記憶する保護情報記憶手段と、保護情報記憶手段に記憶された保護要否情報に基づいて、カプセル化されたデータと、カプセル化されたデータを操作するためのメソッドとを有するオブジェクトを、第1の生成手段または第2の生成手段のいずれが生成するのかを決定する決定手段と、前記受信手段により受信されたプログラムを実行している場合にアクセスすることのできるリソースを制限し、当該通信装置に記憶されているデータのうち前記特定手段により特定されたデータへのアクセスを禁止する一方、前記生成手段により生成されたオブジェクトへのアクセスを許可するアクセス制御手段とを有する通信装置を提供する。

また、この発明は、通信部にプログラムを受信させる受信ステップと、記憶部に記憶されているデータのうち、受信ステップにて受信されたプログラムを実行した場合に使用されるデータを特定する特定ステップと、特定ステップにて特定されたデータに対して予め設定されている当該データの保護の要否を示す保護要否情報に基づいて、カプセル化された前記データと、当該カプセル化されたデータを操作するためのメソッドとを有するオブジェクトを、前記データを操作元のプログラムへ引き渡すメソッドを有する第1のオブジェクトとするのか、前記データを操作元のプログラムへ引き渡すメソッドを有していない第2のオブジェクトとするのかを決定する決定ステップと、前記決定ステップにて決定された第1または第2のオブジェクトを生成する生成ステップと、前記受信ステップにて受信されたプログラムを実行している場合にアクセスすることのできるリソースを制限し、当該通信装置に記憶されているデータのうち前記特定ステップにて特定されたデータへのアクセスを禁止する一方、前記生成ステップにて生成されたオブジェクトへのアクセスを許可するアクセス制御手段とをコンピュータに実行させるためのプログラムを提供してもよい。

この発明によれば、通信装置は、受信したプログラムに基づく処理の実行中に、当該処理において使用されるデータをカプセル化して有しているオブジェクトにアクセスすることが可能となる。また、通信装置は、カプセル化するデータに対して設定されている保護要否情報に基づいて、生成するオブジェクトの種類を決定する。さらに、受信したプログラムに基づく処理の実行中に、オブジェクト内にカプセル化されているデータそのものを取得できるようにするか否かを定め

る。

本発明は、以上挙げたプログラムを電気通信回線を介してユーザに配布し、あるいはこれらのプログラムをF D、C D、M Oディスクといったコンピュータ読み取り可能な記憶媒体に格納して配布するという態様でも実施され得る。

5

#### 図面の簡単な説明

図1 本発明の実施形態に係る通信システムの構成を例示するブロック図である。

図2 同実施形態に係る携帯電話機のハードウェア構成を例示するブロック図  
10 である。

図3 同実施形態に係る携帯電話機において、不揮発性メモリに格納されている型指定テーブルのデータ構成を例示する図である。

図4 同実施形態に係る携帯電話機において、J a v a A P の実行環境を説明するための図である。

15 図5 同実施形態に係る携帯電話機において、カプセル化オブジェクトを説明するための模式図である。

図6 同実施形態に係る携帯電話機において、非完全カプセル化オブジェクトについて例示する模式図である。

20 図7 同実施形態に係る携帯電話機において、完全カプセル化オブジェクトについて例示する模式図である。

図8 同実施形態に係る携帯電話機において、C P Uにより実行されるオブジェクト生成処理の動作を説明するフローチャートである。

図9 同実施形態に係る携帯電話機において、C P Uにより実行されるアクセス管理処理の動作を説明するフローチャートである。

25 図10 同実施形態に係る携帯電話機において、C P Uにより実行されるJ a v a A P 終了処理の動作を説明するフローチャートである。

図11 本発明の変形例6に係り、J a v a 実行環境の変形例を説明するための図である。

図12 本発明の変形例6に係り、通信システムの変形例を例示するブロック

図である。

### 発明を実施するための最良の形態

以下、図面を参照して本発明の実施形態について説明する。なお、各図におい

5 て共通する部分には、同一の符号が付されている。

#### [A-1. 実施形態の構成]

##### <1. 通信システムの構成>

図1は、この発明の実施形態に係る通信システム1の構成を例示するブロック図である。図1に示すように通信システム1は、コンテンツサーバ10と、インターネット20と、移動パケット通信網30と、携帯電話機40とを有している。なお、この通信システム1には、本来、多数の携帯電話機40が収容されるが、図面が煩雑になることを防ぐため、図1には、1つの携帯電話機40のみを図示している。また、同様の理由により、図1には、それぞれ1つのコンテンツサーバ10、ゲートウェイサーバ31および基地局32のみを図示している。

15 コンテンツサーバ10は、インターネット20および移動パケット通信網30を介して携帯電話機40とパケット通信を行う機能を有している。このコンテンツサーバ10には、携帯電話機40に提供するプログラムや画像データ、楽曲データなどの種々のコンテンツが格納されている。これらのコンテンツの中には、携帯電話機40において実行可能なJavaアプリケーションプログラム（以下20、JavaAPPと略称する）が格納されている。このJavaAPPは、JavaアプリレットやJavaアプリケーションなどの、Javaプログラミング言語で記述された携帯電話機40用のアプリケーションプログラムである。

25 移動パケット通信網30は、当該移動パケット通信網30に収容される携帯電話機40に対してパケット通信サービスを提供する通信網であり、ゲートウェイサーバ31と基地局32とを有している。なお、通信システム1は、移動パケット通信網30に加え、図示を省略した移動電話網を有している。この移動電話網は、携帯電話機40に対して一般的な移動電話の通話サービスを提供する。

ゲートウェイサーバ31は、移動パケット通信網30用の通信プロトコルとインターネット20用の通信プロトコルなど、通信プロトコルの異なるデータを相

互に変換し、移動パケット通信網 30 とインターネット 20 とのデータの授受を中継する。また、基地局 32 は、移動パケット通信網 30 の通信サービスエリア内に多数設置されており、自局 32 がカバーする無線セルに在圏している携帯電話機 40 と無線通信を行う。

5 携帯電話機 40 は、自機 40 が在圏している無線セルをカバーする基地局 32 と無線通信を行う。また、この携帯電話機 40 は、移動パケット通信網 30 およびインターネット 20 を介してコンテンツサーバ 10 とパケット通信を行う機能を有しており、コンテンツサーバ 10 から任意のコンテンツをダウンロードすることができる。

10 <2. 携帯電話機の構成>

図 2 は、携帯電話機 40 のハードウェア構成を例示するブロック図である。図 2 に示すように携帯電話機 40 は、無線通信部 401 と、操作入力部 402 と、通話処理部 403 と、通信インターフェース 404 と、CPU 405 と、液晶表示部 406 と、記憶部 407 とを有しており、これらの各部はバス 411 により接続されている。

15 無線通信部 401 は、アンテナ 401a を備え、基地局 32 との間で行われる無線通信を制御する。この無線通信部 401 は、CPU 405 の制御の下、例えば、送話音声に関するデータやパケット通信用のデータなどを搬送波に重畠して送信信号を生成し、この信号を基地局 32 へ送信する。また、無線通信部 401 20 は、基地局 32 から送られてくる無線信号をアンテナ 401a を介して受信し、この信号を復調して自機 40 宛の受話音声に関するデータやパケット通信用のデータなどを得る。

25 操作入力部 402 は、数字や文字、操作指示などを入力するための複数のキーを有しており、これらのキーの操作に応じた操作信号を CPU 405 に出力する。また、通話処理部 403 は、例えば、マイクロフォンやスピーカ、音声処理部などを有しており、CPU 405 の制御の下、呼の接続／切断を含む通話処理を行う。

通信インターフェース 404 は、通信ケーブルを介して接続された電子機器との有線通信を制御する。なお、この通信インターフェース 404 は、赤外線通信や、

HomeRF (Home Radio Frequency)、Bluetooth (登録商標) などの近距離無線通信を制御するものであってもよい。また、CPU 405 は、記憶部 407 に格納されている各種プログラムを実行することにより、バス 411 を介して接続されている装置各部を制御する。また、液晶表示部 406 は、液晶表示パネルと、この液晶表示パネルの表示制御を行う駆動回路とを有している。

記憶部 407 は、ROM 408 と、RAM 409 と、例えば、SRAM (Static-RAM) や EEPROM (Electrically Erasable Programmable-ROM) などの不揮発性メモリ 410 とを有している。ROM 408 には、例えば、携帯電話機 40 用のオペレーティングシステム (以下、OS と略称する) や Web (World Wide Web) ブラウザ、Java 実行環境を構築するためのソフトウェアなどが記憶されている。また、RAM 409 は、CPU 405 のワークエリアとして用いられ、CPU 405 により実行される各種のプログラムやデータが一時的に記憶される。

不揮発性メモリ 410 には、携帯電話機 40 の製品出荷時点から当該携帯電話機 40 に組み込まれているアプリケーションプログラムや、コンテンツサーバ 10 からダウンロードされた Java APP などのコンテンツが格納される。加えて、この不揮発性メモリ 410 には、電話番号やメールアドレスなどの情報が記憶されているアドレス帳データ、受信あるいは送信した電子メールデータ、着信や発信に関する履歴データ、電子決済を行うためのユーザの銀行口座番号やクレジットカード番号などの各種データが格納される。

なお、以下、本明細書では、携帯電話機 40 の製品出荷時点において既に ROM 408 や不揮発性メモリ 410 に格納されているアプリケーションソフトウェアを、ダウンロードされた Java APP と区別するため、ネイティブアプリケーションと記載する。このネイティブアプリケーションには、自身がネイティブアプリケーションであることを示す識別情報が付与されている。

また、不揮発性メモリ 410 は、型指定テーブル 410a と、JAR ストライジ 410b と、個別スクラッチパッド 410c と、共通スクラッチパッド 410d とを有している。まず、型指定テーブル 410a について図 3 を参照して説明

する。図3に示すように、型指定テーブル410aには、不揮発性メモリ410に格納されている各種のデータのうち、アドレス帳データ、電子メールデータ、着信・発信履歴データ、ユーザデータなどの、ダウンロードされたJavaAPPを実行した場合に当該JavaAPPが使用する可能性のあるデータについて、データ名と、型指定情報とが対応付けられて登録されている。型指定情報は、当該データを扱うオブジェクトの型を「完全カプセル化」型とするのか、それとも「非完全カプセル化」型とするのかを指定する情報である。なお、上述したユーザデータとは、携帯電話機40のユーザに関する個人情報であって、例えば、ユーザの氏名や年齢、誕生日、銀行口座番号やクレジットカード番号などである。

図3に示すように、型指定情報は、“1”または“0”的1ビットデータである。型指定情報の値を“1”にセットした場合は、オブジェクトの型が「完全カプセル化」型に指定される一方、型指定情報の値を“0”にセットした場合は、オブジェクトの型が「非完全カプセル化」型に指定される。

なお、カプセル化オブジェクトとは、カプセル化（情報隠蔽）された1以上のデータと、当該カプセル化された各データに対するオブジェクト外部からの操作を可能とするための1以上のメソッドとを有するオブジェクトである。そして、完全カプセル化オブジェクト（tightly encapsulated object）とは、上記カプセル化オブジェクトのうち、オブジェクト内にカプセル化されたデータ自身を当該オブジェクトに対する操作元のプログラム（例えば、ダウンロードされたJavaAPP）へ引き渡すメソッドを一つも持たないよう構成したオブジェクトである。また、非完全カプセル化オブジェクトとは、上記カプセル化オブジェクトのうち、オブジェクト内のデータ自身を当該オブジェクトに対する操作元のプログラムへ引き渡すメソッドを少なくとも一つ以上有しているオブジェクトである。完全カプセル化オブジェクトと非完全カプセル化オブジェクトとの差異は、オブジェクト内のカプセル化されたデータ自身を操作元のプログラムへ引き渡すメソッドを有しているか否かである。

すなわち、図3に示した型指定テーブル410aには、各データ毎に、当該データを完全カプセル化オブジェクトとして扱うのか、それとも非完全カプセル化オブジェクトとして扱うのかが登録されている。例えば、図3において、アドレ

ス帳データ、電子メールデータ、着信・発信履歴データ、ユーザデータは、携帯電話機40に記憶されているデータの中でも特にセキュリティ上の重要度が高いデータである。一方、携帯電話機40にダウンロードされたJava APPは、信頼性を完全に保証することのできないプログラムである。したがって、万一、悪意のある第3者が作成した、データを盗み出すJava APPが携帯電話機40にダウンロードされた場合であっても、このようなJava APPを介して上述したセキュリティ上の重要度が高いデータが携帯電話機40の外部へ流出してしまうような事態は、極力、防がなければならない。

したがって、セキュリティ上の重要度が高いデータは完全カプセル化オブジェクトとして扱い、ダウンロードされたJava APPにデータ自体が引き渡されないようにする必要がある。以上のことから、型指定テーブル410aにおいて、アドレス帳データ、電子メールデータ、着信・発信履歴データ、ユーザデータには、型指定情報の値として“1”（完全カプセル化型）が登録されている。

また、図3に示した型指定テーブル410aにおいて、コンテンツAおよびコンテンツBは、コンテンツサーバ10からダウンロードされた画像データや音楽データなどのコンテンツである。これらのコンテンツには、コンテンツの提供事業者（以下、コンテンツプロバイダと記載する）により著作権保護フラグが付与されている。ここで、著作権保護フラグは、“1”または“0”的1ビットデータである。著作権保護フラグの値が“1”にセットされている場合は、このフラグの付与されているコンテンツの著作権を保護しなければならないことを示している。一方、著作権保護フラグの値が“0”にセットされている場合は、このフラグの付与されているコンテンツの著作権が放棄されていることを示している。

ここで、著作権を保護しなければならないコンテンツの場合、ダウンロードされたJava APPにコンテンツデータ自体を引き渡してしまうと、コンテンツプロバイダが許可を与えていないような利用形態でコンテンツがJava APPにより利用されてしまうおそれや、コンテンツデータがJava APPを介して携帯電話機40の外部へ不正に転送されてしまうおそれがある。したがって、著作権保護フラグの値として“1”が付与されているコンテンツデータは完全カプセル化オブジェクトとして扱い、ダウンロードされたJava APPにコンテンツデータ

自体が引き渡されないようにする必要がある。以上のようなことから、型指定テーブル410aにおいてコンテンツAには、型指定情報の値として“1”（完全力プセル化型）が登録されている。

一方、著作権保護フラグの値として“0”が付与されているコンテンツデータ  
5 は、著作権が放棄されているので、完全カプセル化オブジェクトとして扱う必要  
がない。この場合、ダウンロードされたJ a v a A Pにコンテンツデータ自体を  
引き渡しても何ら問題がなく、また、コンテンツデータ自体を引き渡せるように  
した方がJ a v a A Pの利便性が高くなる。このため、型指定テーブル410a  
10 においてコンテンツBには、型指定情報の値として“0”（非完全カプセル化型）  
が登録されている。

なお、型指定テーブル410aにおいて、アドレス帳データ、電子メールデータ、着信・発信履歴データ、ユーザデータには、予め型指定情報の値として“1”がセットされている。また、ダウンロードされたコンテンツについては、コン  
15 ネンツが携帯電話機40にダウンロードされた際に、このコンテンツに付与され  
ている著作権保護フラグの値に応じた型指定情報の値がC P U 4 0 5により決定  
される。そしてその型指定情報は、コンテンツを識別するコンテンツ識別情報（  
データ名）とともに型指定テーブル410aに登録される。

また、携帯電話機40において作成されたデータやユーザがパソコンなどで作  
成し、通信インターフェース404を介して携帯電話機40に取り込んだ画像データ  
20 や音楽データなどに対しては、このデータを扱うオブジェクトの型を「完全力  
プセル化」型とするのか、それとも「非完全カプセル化」型とするのかをユーザ  
が操作入力により設定することができる。さらに、型指定テーブル410aの内  
容を液晶画面に表示して、著作権保護フラグが付与されたコンテンツを除く各デ  
ータの型指定情報を、ユーザ自身が操作入力により変更可能な構成としてもよい  
25 。

次に、図2に戻り、不揮発性メモリ410は、上述した型指定テーブル410aの他に、J A Rストレージ410bと、個別スクラッチパッド410cと、共通スクラッチパッド410dとを有している。ここで、J A Rストレージ410b、個別スクラッチパッド410cおよび共通スクラッチパッド410dについ

て説明する前に、まず、携帯電話機40にダウンロードされるJavaAPについて説明する。JavaAPは、JavaAPの本体プログラムおよび当該本体プログラムの実行に応じて利用される画像ファイルや音声ファイルなどを1つにまとめたJAR（Java Archive）ファイルと、このJARファイルのインストールや起動、ネットワークアクセスなどを制御するための各種制御情報が記述されたADF（Application Descriptor File）とを有している。

JARストレージ410bおよび個別スクラッチパッド410cには、ダウンロードされたJavaAP毎に当該JavaAP用の記憶領域が設けられる。JARストレージ410b内の各記憶領域には、JavaAPのJARファイルが格納される。また、個別スクラッチパッド410c内の各記憶領域には、例えば、JavaAPがゲームプログラムである場合、今までの得点データやセーブデータなど、JavaAPの利用に応じて発生した当該JavaAP用のデータが格納される。さらに、共通スクラッチパッド410dには、複数のJavaAPが共通して使用するデータが格納される。

また、ダウンロードの後、JavaAPが携帯電話機40において実行される場合、このJavaAPの実行に伴って携帯電話機40がアクセスすることのできるリソースは、このJavaAPのダウンロード元のコンテンツサーバ10（サイト）と、このJavaAPに対して割り当てられたJARストレージ410bおよび個別スクラッチパッド410c内の記憶領域と、共通スクラッチパッド410dと、のみに制限され、それ以外のリソースにアクセスすることはできない。

### <3. Java実行環境>

図4は、携帯電話機40におけるJavaAPの実行環境を説明するための図である。図4に示すように本実施形態に係る携帯電話機40には、JavaAPの実行環境を構築するためのソフトウェアとして、KVM（K Virtual Machine）と、コンフィギュレーションとしてCLDC（Connected Limited Device Configuration）を備える。また、携帯電話機40には、プロファイルとして通信事業者が独自に策定したオ

リジナル Java 拡張プロファイルを備えた J2ME (Java 2 Micro Edition) とが組み込まれている。

KVMは、小型電子機器用に設計変更された JVM (Java Virtual Machine) である。KVMは、Java APの実行ファイル形式であるバイトコードをCPU405がOSを介して解釈／実行可能な命令コードに変換する。また、CLDCクラスライブラリは、CLDC用のクラスライブラリである。

オリジナル Java 拡張ライブラリは、CLDCを基礎として携帯電話機に特化した機能を提供するためのクラスライブラリである。このオリジナル Java 拡張ライブラリには、例えば、ユーザインターフェースAPI (Application Program Interface)、ネットワーキングAPI、スクラッチパッドAPI、完全カプセル化API、非完全カプセル化APIなどが含まれている。

ここで、ユーザインターフェースAPIは、携帯電話機40のユーザインターフェース機能をサポートするAPIである。ネットワーキングAPIは、URL (Uniform Resource Locator) により指定されたネットワークリソースへのアクセスをサポートするAPIである。また、スクラッチパッドAPIは、個別スクラッチパッド410cや共通スクラッチパッド410dに対するデータの書き込みや読み出しをサポートするAPIである。さらに、完全カプセル化APIは、完全カプセル化オブジェクトを生成するためのオブジェクトであり、非完全カプセル化APIは、非完全カプセル化オブジェクトを生成するためのオブジェクトである。

これらプログラムを携帯電話にインストールする態様として種々のものがある。ある態様において、これらプログラムは、工場出荷前に携帯電話にインストールされる。また、別の態様において、これらプログラムは、ネットワーク内のサイトから携帯電話にダウンロードされ、インストールされる。プログラムは、携帯電話以外のPCなどにインストールされる場合もある。この態様では、プログラムは、FD、CD、MOディスクなどのコンピュータ読み取り可能な記憶媒体に格納されてユーザに配布され、ユーザによってPCにインストールされる。

また、携帯電話機 40 は、CLDC クラスライブラリおよびオリジナル Java 拡張ライブラリに加え、メーカ独自拡張ライブラリを有している。このメーカ独自拡張ライブラリは、携帯電話機 40 を製造する各メーカがそれぞれ独自の機能を提供するためのクラスライブラリである。

5 次に、JAM (Java Application Manager) は、OS による制御の下で、携帯電話機 40 にダウンロードされた Java AP や、完全カプセル化オブジェクト、非完全カプセル化オブジェクトなどを管理する機能を有している。例えば、JAM は、Java AP のインストールや更新、削除を行う機能、不揮発性メモリ 410 に格納されている Java AP をリスト表示する機能、Java AP の実行管理（起動や強制終了など）を行う機能、Java AP の実行に伴う携帯電話機 40 のアクセスを制限する機能、完全カプセル化オブジェクトや非完全カプセル化オブジェクトの生成、更新、削除を行なう機能などを有している。

15 また、図 4 に示すように、電話帳機能やブラウザ機能、ネットワーク通信機能などを提供するネイティブアプリケーションは、OS による制御の下で直接動作する。

#### <4. カプセル化オブジェクトの構成>

次に、カプセル化オブジェクトについて説明する。図 5 は、カプセル化オブジェクトについて説明するための模式図である。図 5 に示すように、カプセル化オブジェクトとは、カプセル化された 1 以上のデータと、当該カプセル化された各データに対するオブジェクト外部からの操作を可能とするための 1 以上のメソッドとを有するオブジェクトである。

25 図 5 に示す例では、2 つのデータ 1, 2 と、2 つのメソッド 1, 2 とを有するカプセル化オブジェクトが例示されている。このカプセル化オブジェクト内のデータ 1, 2 は共にカプセル化されているため、オブジェクトの外部からデータ 1, 2 を直接読み書きすることはできない。したがって、例えば、ダウンロードされたプログラムがカプセル化オブジェクト内のデータ 1, 2 に対してアクセスする場合、プログラムは、メソッド 1, 2 を使用して目的のデータ 1 またはデータ 2 に対する操作をカプセル化オブジェクトに指令しなければならない。

ここで、図5に示すメソッド1が、例えば、指定されたデータ自体を操作元のプログラムへ引き渡すメソッドであれば、操作元のプログラムは、メソッド1を使用してカプセル化オブジェクト内の任意のデータ1，2を取得することが可能である。また、図5に示すメソッド2が、例えば、指定されたデータを液晶画面に表示させるメソッドであれば、操作元のプログラムは、メソッド2を使用してカプセル化オブジェクト内の任意のデータ1，2を画面表示させることができある。ここで注目すべき点は、メソッド2を使用してカプセル化オブジェクト内の任意のデータ1，2を画面表示させたプログラムは、表示させるデータやメソッドを指定してカプセル化オブジェクトへ指令を出すものの、表示させるデータ自体を取得していない点である。

つまり、データそのものを操作元のプログラムに引き渡すメソッドを1つも有していないカプセル化オブジェクト（完全カプセル化オブジェクト）であれば、操作元のプログラムは、オブジェクト内のデータそのものを取得することはできないが、このオブジェクトに備わるメソッドを使用してオブジェクト内のデータに対する操作を行うことはできる。

したがって、アドレス帳データや電子メールデータなどを完全カプセル化オブジェクトとして扱うようにすれば、操作元のプログラムがダウンロードされたJava A Pのように信頼性を完全に保証することのできないプログラムであったとしても、当該プログラムにデータ自体を引き渡すことがない。したがって、携帯電話機40におけるセキュリティを確保することができる。また、同時に、このようなプログラムであったとしても、アドレス帳データや電子メールデータなど、従来はセキュリティを確保する観点から一切のアクセスを認めていなかったデータに対し、完全カプセル化オブジェクトが有するメソッドを用いて操作（アクセス）を行うことができる。

以上のようなことから本実施形態では、アドレス帳データ、電子メールデータ、着信・発信履歴データ、ユーザデータなどのセキュリティ上の重要度の高いデータや、著作権を保護しなければならないコンテンツなど、前述した型指定情報の値として“1”がセットされているデータを完全カプセル化オブジェクトとして扱う一方、セキュリティの重要度が低いデータや著作権が放棄されたコンテン

ツなど、型指定情報の値として“0”がセットされているデータを非完全カプセル化オブジェクトとして扱う。また、ダウンロードされたJavaAPに対して、完全カプセル化オブジェクトや非完全カプセル化オブジェクトへのアクセスを許可する。

5 図6は、電話帳データに関する非完全カプセル化オブジェクトについて例示する模式図である。なお、本実施形態において、電話帳データはセキュリティ上の重要度が高いため、本来は必ず完全カプセル化オブジェクトとして扱われるデータであるが、ここでは比較のため、あえて非完全カプセル化オブジェクトとして扱った場合について説明する。

10 Javaプログラミング言語では、「private」というアクセス修飾子を用いてオブジェクト内のフィールドをprivateフィールドに宣言することで、当該privateフィールドに格納されるデータのカプセル化を図る。つまり、オブジェクト内のフィールドが全てprivateフィールドである場合、各privateフィールドに格納されているデータをオブジェクトの外部から直接読み書きすることができなくなる。このようにした場合、各privateフィールドに格納されているデータに対してオブジェクトの外部からアクセスするには、このオブジェクトに備わるメソッドを使用してデータに対する操作を当該オブジェクトに指令しなければならない。

15 図6に示す非完全カプセル化オブジェクトには、2つのprivateフィールドが設けられ、それぞれprivate char value [1]、private char value [2]という電話帳の文字列データが格納されている。また、この非完全カプセル化オブジェクトは、getBytes()、drawString()という2つのメソッドを有している。ここで、getBytes()は、オブジェクト内のデータをバイト配列の形式で操作元のプログラムへ引き渡すメソッドである。したがって、ダウンロードされたJavaAPは、このgetBytes()というメソッドを使用して、非完全カプセル化オブジェクト内の電話帳の文字列データ(private char value [1]、private char value [2])を取得することが可能である。加えて、JavaAPは、取得した電話帳の文字列データを当該Java

APのダウンロード元のサーバ（コンテンツサーバ10）へ送信することなどが  
できる。

また、drawString()は、オブジェクト内のデータを携帯電話機40の液晶画面に表示させるメソッドである。JavaAPは、このdrawString()というメソッドを使用して、非完全カプセル化オブジェクト内の電話帳の文字列データ(private char value[1], private char value[2])を液晶画面に表示させることもできる。

一方、図7は、電話帳データに関する完全カプセル化オブジェクトについて例示する模式図である。図7に示す完全カプセル化オブジェクトが図6に示した非完全カプセル化オブジェクトと異なるのは、完全カプセル化オブジェクトは、上述したgetBytes()のように、オブジェクト内のデータそのものを操作元のプログラムへ引き渡すメソッドを有していない点である。

すなわち、完全カプセル化オブジェクトは、カプセル化された上に、オブジェクト内のデータそのものを操作元のプログラムへ引き渡すメソッドを1つも有していない。したがって、ダウンロードされたJavaAPは、drawString()というメソッドを使用してオブジェクト内の電話帳の文字列データ(private char value[1], private char value[2])を画面表示させることはできるが、電話帳の文字列データそのものを取得することはできない。以上のようなことから、万一、悪意のある第3者が作成した、データを盗み出すJavaAPが携帯電話機40にダウンロードされた場合であっても、このようなJavaAPに電話帳データが引き渡されることはない。当然、電話帳データがサーバなど携帯電話機40の外部へ送信されることもない。

ところで、drawString()というメソッドを使用してオブジェクト内の電話帳の文字列データを画面表示させる場合、完全カプセル化オブジェクトや非完全カプセル化オブジェクトは、ネイティブアプリケーションとしてROM408または不揮発性メモリ410に格納されている表示制御プログラムを使用して液晶画面に電話帳の文字列を表示させる。この表示制御プログラムからJavaAPが表示データを取得してしまうと、完全カプセル化オブジ

エクトや非完全カプセル化オブジェクトを用いた意味がなくなってしまう。

しかしながら、ダウンロードされた Java APP が実行される場合には、前述したように JAM のアクセス制限機能により、Java APP の実行中に携帯電話機 40 がアクセスすることのできるリソースが制限される。ここで、Java APP の実行中に携帯電話機 40 のアクセスが許可されるリソースに表示制御プログラムは含まれていないので、Java APP が表示制御プログラムから表示データを取得するようなことは一切あり得ない。

また、カプセル化は、プログラミング言語レベルでのカプセル化と、実行コード（マシン語またはバイトコード）レベルでのカプセル化とが考えられる。プログラミング言語レベルでのカプセル化が完全であっても、実行コードレベルでのカプセル化が完全でなければ、データを完全にカプセル化したとは言えない。例えば、プログラミング言語である C++ を用いたプログラムでも private フィールドを有するカプセル化オブジェクトを生成することはできる。しかしながら、C++ は、単なるプログラミング言語に過ぎないことから、プログラミング言語レベルでのカプセル化しか達成し得ない。

具体的に説明すると、C++ を用いたプログラムにより、オブジェクト内の全てのフィールドを private フィールドとして宣言し、カプセル化オブジェクトを生成した場合、確かに、このオブジェクト内の private フィールドに格納されているデータを直接読み書きするようなソースコードはコンパイルされないので、当然、実行コードが生成されることもない。

しかしながら、このカプセル化は、コンパイラによって保証されているに過ぎない。したがって、例えば、悪意のある第 3 者がコンパイラを改造することで、オブジェクト内のデータを不正に入手することが可能である。また、コンパイラを改造しなくても、悪意のある第 3 者がハンドアセンブルなどの手段でオブジェクト内のデータを不正に読み出す実行コードを生成するプログラムを作成することも不可能ではない。加えて、ポインタを用いて直接メモリにアクセスしてしまえば、オブジェクト内のデータ入手することができてしまう。

これに対して Java の場合、private 宣言されたフィールドは、private 属性を有するフィールドであることを示す Java のバイトコードへ

コンパイルされる。KVMがクラスファイルをRAM409などへ展開する際も、フィールドのprivate属性は保持されている。したがって、仮にコンパイラを改造してオブジェクト内のprivateフィールドに格納されているデータを不正に読み出すようなバイトコードを生成したとしても、KVMまたはJAMがこれを検知するので、オブジェクト内のデータを入手することはできない。また、Javaはポインタをサポートしていないので、ポインタを用いて直接メモリにアクセスし、オブジェクト内のデータを入手することもできない。

以上のようなことから、Javaでは、プログラミング言語レベルのみに止まらず、バイトコードレベルでの完全なカプセル化を達成することが可能である。

なお、データのカプセル化に際しては、「private」の他に「protected」や「package」などのアクセス修飾子を用いることもできる。

以上が本実施形態に係る通信システム1の構成である。

#### [A-2. 実施形態の動作]

次に、本実施形態の動作について説明する。

なお、携帯電話機40が以下に述べる動作を行う前提として、携帯電話機40は、移動パケット通信網30およびインターネット20を介してコンテンツサーバ10とパケット通信を行い、コンテンツサーバ10からJavaAPをダウンロードして不揮発性メモリ410に格納しているものとする。また、不揮発性メモリ410には、ダウンロードされたJavaAP(コンテンツ)の他に、アドレス帳データや電子メールデータ、ユーザデータなどが格納されており、型指定テーブル410aには、これら各データについて型指定情報が登録されているものとする。

また、型指定テーブル410aにおいて、アドレス帳データ、電子メールデータ、着信・発信履歴データ、ユーザデータに対しては、型指定情報の値として“1”がセットされている。また、ダウンロードされたコンテンツに対しては、コンテンツが携帯電話機40にダウンロードされた際に、このコンテンツに付与されている著作権保護フラグの値に応じた型指定情報の値がCPU405により決定され、当該型指定情報およびコンテンツ名が型指定テーブル410aに登録される。

## &lt;1. オブジェクト生成処理&gt;

まず、携帯電話機40においてCPU405により実行されるオブジェクト生成処理について図8を参照して説明する。このオブジェクト生成処理は、JAMの機能としてCPU405により実行されるものであり、例えば、画面表示されたプログラムの一覧リストの中から、実行するプログラムが操作入力により指定された場合などに実行される。なお、プログラムの実行を指示する形態は、操作入力によるものに限定されず、例えば、予め定められた時間毎にプログラムの実行が指示される場合や、既に実行されている他のプログラムから実行が指示される場合、電子メールなどを用いて携帯電話機40の外部からプログラムの実行が指示される場合などもある。

図8に示すように、まず、携帯電話機40のCPU405は、実行するプログラムとして操作入力により指定されたプログラムを特定する（ステップS101）。次いで、CPU405は、特定したプログラムがダウンロードされたJavaAPであるのか、それともネイティブアプリケーションであるのかを判別する（ステップS102）。前述したようにネイティブアプリケーションには、自身がネイティブアプリケーションであることを示す識別情報が付与されている。したがって、CPU405は、プログラムに上記識別情報が付与されているか否かを判別することで、このプログラムがダウンロードされたJavaAPであるのか、それともネイティブアプリケーションであるのかを判別することができる。

その結果、CPU405は、プログラムがネイティブアプリケーションであると判別した場合は（ステップS102：No）、オブジェクト生成処理を終了するとともに、実行するプログラムとして指定されたネイティブアプリケーションを起動する。そして、CPU405は、起動させたネイティブアプリケーションに基づく処理を行なう。

ここで、実行するプログラムがネイティブアプリケーションである場合は、信頼性が完全に保証できるプログラムであるので、完全カプセル化オブジェクトや非完全カプセル化オブジェクトを用いたり、あるいはネイティブアプリケーションの実行に伴ってJAMのアクセス制限機能を動作させる必要がない。したがって、ネイティブアプリケーションが実行される場合、JAMによるアクセス制限

は一切行われず、ネイティブアプリケーションは、携帯電話機40内の任意のリソースおよびネットワーク上の任意のリソースにアクセスすることができる。

一方、CPU405は、プログラムがダウンロードされたJavaAPであると判別した場合は(ステップS102:Yes)、次いで、不揮発性メモリ410に格納されている各種のデータの中から、このJavaAPを実行した場合に使用されるデータを、例えば、このJavaAPのプログラム内容を解析するなどして特定する(ステップS103)。このとき同時に、そのデータと共にカプセル化するメソッドを特定する。なお、JavaAPが使用するデータを特定する際には、JARストレージ410b内の、このJavaAPのJARファイルに格納されているデータは特定の対象から除外する。これは、JARファイル内に格納されているデータは、このJavaAPを実行する上で必要となるデータとして当該JavaAPを提供するコンテンツプロバイダが用意したデータであるためである。

次いで、CPU405は、型指定テーブル410a(図3)を参照して上記特定したデータの型指定情報の値に基づいて、このデータを扱うオブジェクトの型を「完全カプセル化」型とするのか、それとも「非完全カプセル化」型とするのかを決定する(ステップS104)。例えば、JavaAPの使用するデータがアドレス帳データの場合、CPU405は、型指定テーブル410aを参照し、アドレス帳データを扱うオブジェクトの型を「完全カプセル化」型に決定する。また、JavaAPの使用するデータがコンテンツB(著作権保護フラグ“0”)の場合、CPU405は、コンテンツBを扱うオブジェクトの型を「非完全カプセル化」型に決定する。

この後、CPU405は、上記ステップS103において特定したデータと、上記ステップS104において決定したオブジェクトの型に基づいて、完全カプセル化オブジェクトまたは非完全カプセル化オブジェクトを生成する(ステップS105)。例えば、上記ステップS103において特定したデータがアドレス帳データ(型指定情報“1”)の場合、CPU405は、オリジナルJava拡張ライブラリ内の完全カプセル化APIを起動する。完全カプセル化APIは、完全カプセル化APIに含まれるメソッドの中から、そのデータを特定するとき同

時に特定されたメソッドを選択する。そして、そのデータとメソッドをカプセル化し、アドレス帳データ用の完全カプセル化オブジェクトを生成する。また、上記ステップS 1 0 3において特定したデータがコンテンツBの場合、C P U 4 0 5は、オリジナルJ a v a拡張ライブラリ内の非完全カプセル化A P Iを起動して、コンテンツB用の非完全カプセル化オブジェクトを生成する。

次いで、C P U 4 0 5は、生成した完全カプセル化オブジェクトまたは非完全カプセル化オブジェクトを共通スクラッチパッド4 1 0 dに格納し（ステップS 1 0 6）、オブジェクト生成処理を終了する。なお、上記ステップS 1 0 5において生成された完全カプセル化オブジェクトや非完全カプセル化オブジェクトは、10 共通スクラッチパッド4 1 0 dではなく、個別スクラッチパッド4 1 0 cに格納される形態であってもよい。

また、上記ステップS 1 0 3においてJ a v a A Pの使用するデータが複数特定された場合は、特定した各データ毎に、当該データ用の完全カプセル化オブジェクトまたは非完全カプセル化オブジェクトを生成して共通スクラッチパッド4 1 0 dに格納するため、上記ステップS 1 0 4～S 1 0 6までの処理を各データ毎に繰り返して行う。そして、C P U 4 0 5は、オブジェクト生成処理を終了した後、実行するプログラムとして指定されたJ a v a A Pを起動し、このプログラムに基づく処理を開始する。

## <2. アクセス管理処理>

20 次に、携帯電話機4 0においてC P U 4 0 5により実行されるアクセス管理処理について図9を参照して説明する。このアクセス管理処理は、J A Mの機能としてC P U 4 0 5により実行されるものであり、ダウンロードされたJ a v a A Pの実行過程においてアクセス要求が発生した場合に、割り込み処理として実行される。

25 図9に示すように、まず、携帯電話機4 0のC P U 4 0 5は、J a v a A Pの実行過程において発生したアクセス要求について、アクセスの要求先が予め許可された範囲内のリソースであるか否かを判別し、アクセス要求を許可するか否かを判定する（ステップS 2 0 1）。ここで、アクセス要求の許可有無を判定する仕組みについて具体的に説明する。ダウンロードされたJ a v a A Pが実行される

場合、CPU405は、JavaAPPの実行に伴ってアクセスすることのできるリソースを、このJavaAPPのADFに記述されているURLにより指定される当該JavaAPPのダウンロード元のコンテンツサーバ10（サイト）と、このJavaAPPに対して割り当てられたJARストレージ410bおよび個別スクラッチパッド410c内の記憶領域と、共通スクラッチパッド410dと、のみに制限する。  
5

したがって、CPU405は、アクセスの要求先が上述したリソースのいずれかである場合は、このアクセス要求を許可する一方、アクセスの要求先が上述したりソース以外である場合は、このアクセス要求を許可しない。

10 次いで、CPU405は、アクセス要求の許可有無を示す判定結果を要求元のJavaAPPに通知した後（ステップS202）、アクセス管理処理を終了する。また、実行中のJavaAPPは、JAMによる判定結果を受け取ると、この判定結果に従って、アクセス要求が許可された場合は当該アクセス要求に基づく処理を実行する一方、アクセス要求が許可されなかった場合は当該アクセス要求に基づく処理をキャンセルする。  
15

さて、携帯電話機40のCPU405は、ダウンロードしたJavaAPPを実行する場合、図8に示したオブジェクト生成処理を行った後にJavaAPPを起動する。また、ダウンロードしたJavaAPPの実行過程においてCPU405は、アクセス要求が発生すると、図9に示したアクセス管理処理を行なう。したがって、携帯電話機40は、ダウンロードしたJavaAPPの実行中において必ずJAMによるアクセス制限を受けることとなる。JavaAPPは、例えば、不揮発性メモリ410に格納されているアドレス帳データ、電子メールデータ、着信・発信履歴データ、ユーザデータ、コンテンツなどのデータそのものにアクセスすることができなくなる。  
20

25 このため、携帯電話機40のCPU405は、上述したオブジェクト生成処理において、起動させるJavaAPPが使用するデータを特定し、当該データ用の完全カプセル化オブジェクトまたは非完全カプセル化オブジェクトを生成して共通スクラッチパッド410dに格納する。この共通スクラッチパッド410dは、前述したように、JAMによるアクセス制限が行われている場合であっても携

5 帯電話機 40 のアクセスが許可されるリソースである。また、携帯電話機 40 に  
ダウンロードされる Java APP は、共通スクラッチパッド 410d に格納され  
た完全カプセル化オブジェクトや非完全カプセル化オブジェクトにアクセスし、  
当該オブジェクトに備わるメソッドを使用してこのオブジェクト内のデータに対  
する操作を指令するように作成されている。

10 例えば、アドレス帳データを使用する Java APP が起動される場合、上述し  
たオブジェクト生成処理によりアドレス帳データ用の完全カプセル化オブジェク  
トが生成され、共通スクラッチパッド 410d に格納される。また、この Java  
APP は、上記生成されたアドレス帳データ用の完全カプセル化オブジェクトに  
15 対して、当該オブジェクトに備わるメソッドを用いてこのオブジェクト内のデ  
ータに対する操作を指令する。したがって、完全カプセル化オブジェクトの有する  
アドレス帳データの一部を画面表示させることなどが可能となる一方、完全カプ  
セル化オブジェクトの有するデータそのものが Java APP に引き渡されること  
はない。

20 15 従来は、ダウンロードされた Java APP に対するセキュリティを確保するた  
め、このような Java APP については、アドレス帳データ、電子メールデータ  
、着信・発信履歴データ、ユーザデータなどに一切アクセスすることができなか  
った。これに対して本実施形態によれば、完全カプセル化オブジェクトを用いる  
ことにより、データそのものが Java APP に引き渡されることがないので、ダ  
ウンロードされた Java APP に対するセキュリティを確保しつつ、同時に、従  
来は一切アクセスできなかったデータについて、完全カプセル化オブジェクトを  
介して画面表示を行わせることなどができるようになる。したがって、ダウンロ  
ードされた Java APP が携帯電話機 40 において実現することのできる機能を  
充実させることができる。

25 また、著作権が放棄されたコンテンツや、セキュリティ上の重要度が低く、型  
指定情報として “0” がセットされているデータを使用する Java APP が起動  
される場合、非完全カプセル化オブジェクトが生成されて共通スクラッチパッド  
410d に格納される。この場合は、完全カプセル化オブジェクトの場合と異な  
り、非完全カプセル化オブジェクトの有しているデータそのものを Java APP

に引き渡すこともできる。

すなわち、ダウンロードされたJavaAPは信頼性を完全に保証することのできないプログラムであるが、著作権が放棄されたデータやセキュリティ上の重要度が低いデータについては、非完全カプセル化オブジェクトとして扱うことで  
5 JavaAPにデータそのものを引き渡せるようになる。JavaAPにデータそのものを引き渡せるようにした方が利便性を高くできることは説明をするまでもなく明らかである。このようにカプセル化するデータのセキュリティ上の重要度や著作権の保護の要否などに応じて完全カプセル化オブジェクトと非完全カ  
10 プセル化オブジェクトとを使い分けるようにすると、完全カプセル化オブジェクトのみを用いた場合と比較して、さらに利便性を高めることができる。

### <3. JavaAP終了処理>

次に、携帯電話機40においてCPU405により実行されるJavaAP終了処理について図10を参照して説明する。このJavaAP終了処理は、JAMの機能としてCPU405により実行されるものであり、JavaAPの実行  
15 終了要求が発生した場合に、割り込み処理として実行される。

図10に示すように、携帯電話機40のCPU405は、JavaAPの実行終了要求が発生すると、共通スクラッチパッド410dに格納されている完全カプセル化オブジェクトや非完全カプセル化オブジェクトを削除する（ステップS301）。このステップS301において削除される完全カプセル化オブジェクトや非完全カプセル化オブジェクトは、JavaAPを起動させる際に、上述したオブジェクト生成処理（図8参照）において生成され、共通スクラッチパッド410dに格納されたものである。CPU405は、共通スクラッチパッド410dからオブジェクトを削除すると、JavaAP終了処理を終える。

このようにダウンロードされたJavaAPを起動する際に、完全カプセル化  
25 オブジェクトや非完全カプセル化オブジェクトを生成して共通スクラッチパッド410dに格納する一方、このJavaAPの実行が終了する際に、共通スクラッチパッド410dから完全カプセル化オブジェクトや非完全カプセル化オブジェクトを削除するようにすると、完全カプセル化オブジェクトや非完全カプセル化オブジェクトを共通スクラッチパッド410dに常時保持しておく必要がない

。したがって、携帯電話機40のメモリ資源を効率的に活用することができる。

なお、携帯電話機40は、ROM408または不揮発性メモリ410に記憶されているプログラムに従って、本発明に係る処理（オブジェクト生成処理、アクセス管理処理、JavaAP終了処理）を実行するが、このような処理を実行するためのプログラムを携帯電話機40に対して通信により提供する形態としてもよい。さらに、このような処理を実行するためのプログラムを、例えば、光記録媒体や磁気記録媒体、半導体メモリなどの記録媒体を用いて携帯電話機40へ提供するようにしてもよい。但し、プログラムを記録媒体により携帯電話機40へ提供する場合、携帯電話機40は、記録媒体からプログラムを読み出すための記録媒体ドライブを有する。

#### [B. 変形例]

以上、本発明の実施形態について説明したが、本発明はその主要な特徴から逸脱することなく他の様々な形態で実施することが可能である。上述した実施形態は、本発明の一態様を例示したものに過ぎない。なお、変形例としては、例えば15、以下のようなものが考えられる。

#### <変形例1>

上述した実施形態では、完全カプセル化オブジェクトと非完全カプセル化オブジェクトとを用いる場合について説明したが、完全カプセル化オブジェクトのみを用いるようにしてもよい。すなわち、ダウンロードされたJavaAPが使用するデータを全て完全カプセル化オブジェクトとして扱うようにしてもよい。この場合、型指定情報は不要となる。また、上述した実施形態では、型指定テーブル410aを用いる構成としたが、アドレス帳データ、電子メールデータ、コンテンツなどのデータ自体に型指定情報を付与するようすれば、指定テーブル410aを用いる必要はない。

#### 25 <変形例2>

上述した実施形態では、ダウンロードされたJavaAPの実行が指示された場合に、完全カプセル化オブジェクトまたは非完全カプセル化オブジェクトを生成するようにした。しかしながら、完全カプセル化オブジェクトまたは非完全カプセル化オブジェクトが生成されるタイミングは、JavaAPの実行が指示さ

れたときに限定されるものではない。

例えば、携帯電話機 40 の電源投入時などに、型指定テーブル 410a（図 3）を参照し、各データ用の完全カプセル化オブジェクトや非完全カプセル化オブジェクトを生成して共通スクラッチパッド 410d に格納しておくようにしてもよい。但し、この場合、アドレス帳データ、電子メールデータ、着信・発信履歴データ、ユーザデータなどの元データが更新された場合に、その更新内容に応じて共通スクラッチパッド 410d に格納されている完全カプセル化オブジェクトや非完全カプセル化オブジェクト内のデータを更新する必要がある。

したがって、このような制御を行う場合には、元データの更新に応じてオブジェクト内にカプセル化されているデータを更新する API をオリジナル拡張ライブラリに備えるようにする。また、完全カプセル化オブジェクトや非完全カプセル化オブジェクトを共通スクラッチパッド 410d に常時保持しておく場合は、当然、Java APP の実行終了に応じて共通スクラッチパッド 410d から完全カプセル化オブジェクトや非完全カプセル化オブジェクトを削除する必要はない。

#### <変形例 3>

上述した実施形態において、例えば、“1（重要度「高」）”～“5（重要度「低」）”までのセキュリティ上の重要度を示すセキュリティレベル情報をデータに対して付与し、このセキュリティレベル情報が“1”～“3”までのデータを完全カプセル化オブジェクトとして扱う一方、セキュリティレベル情報が“4”および“5”的データを非完全カプセル化オブジェクトとして扱うようにしてもよい。

#### <変形例 4>

携帯電話機 40 にダウンロードされた Java APP であっても、例えば、移動パケット通信網 30 を運営する通信事業者や CA（C e r t i f i c a t e A u t h o r i t y）のような公正な第 3 者機関により Java APP の内容が審査され、一定の動作基準を満たしていると認定された Java APP であれば、ネイティブアプリケーションと同様に、信頼性を完全に保証することのできるプログラムとみなすことができる。

したがって、第3者機関によって認定されたJavaAPであれば、ダウンロードされたJavaAPであってもネイティブアプリケーションと同様に、使用するデータを不揮発性メモリ410から直接取得できるようにしてもよい。なお、第3者機関により認定されたJavaAPには、当該JavaAPが第3者機  
5 関の認定プログラムであることを示す識別情報が付与されている。したがって、携帯電話機40において、ダウンロードされたJavaAPが第3者機関による認定プログラムであるか否かを識別する場合には、上記識別情報の有無を判別すればよい。

＜変形例5＞

10 上述した実施形態においてコンテンツサーバ10は、インターネット20に接続されている構成とした。しかしながら、コンテンツサーバ10は、専用線を介して移動パケット通信網30のゲートウェイサーバ31に直接接続されている構成であってもよい。また、ゲートウェイサーバ31がコンテンツサーバ10の機能を有する構成であってもよい。さらに、コンテンツサーバ10が移動パケット  
15 通信網30内に設置されている構成であってもよい。

＜変形例6＞

上述した実施形態では、図11においてハッチングで示すように、KVMと、  
20 コンフィギュレーションとしてCLDCを備えるとともにプロファイルとしてオリジナルJava拡張プロファイルを備えるJ2MEとが組み込まれた携帯電話機40に本発明を適用した場合について説明した。しかしながら、Java実行環境は、上述したKVMとJ2MEの組み合わせに限定されるものではない。また、本発明が適用可能な通信装置は、携帯電話機に限定されるものではない。

25 例えば、図11に示すように、J2MEのプロファイルとして、オリジナルJava拡張プロファイルの代わりにMIDP (Mobile Information Device Profile) を有する構成であってもよい。また、KVMの代わりにJVMを有し、J2MEのコンフィギュレーションとしてCLDCの代わりにCDC (Connected Device Configuration) を、また、J2MEのプロファイルとして、例えば、液晶付電話機用プロファイル、TV用プロファイル、カーナビゲーション用プロファイルなどを

有する構成であってもよい。さらには、Hot Spotと、J2SE（Java 2 Standard Edition）またはJ2EE（Java 2 Enterprise Edition）とを有する構成であってもよい。

また、以上説明したJava実行環境の変形例から明らかなように、本発明は  
5 、例えば、PHS（Personal Handy phone System：登録商標）端末やPDA（Personal Digital Assistant）、カーナビゲーション装置、パーソナルコンピュータなどの、通信機能を有する各種電子機器に適用可能である。また、本発明は、移動パケット通信網  
10 30 に収容される通信装置に限定されるものではない。例えば、図12に示すような通信システム2において、LAN50内に設けられたパーソナルコンピュータ70A～70Cに本発明を適用することもできる。

また、上述した実施形態では、Javaプログラミング言語により記述された  
J ava A Pを用いた場合について説明したが、プログラミング言語はJava  
に限定されるものではない。

#### 15 <変形例7>

前述の実施形態においては、電話帳データに関する完全カプセル化オブジェクトについて例示したが、完全カプセル化オブジェクトに含まれるメソッドおよびデータはこれに限定されるものではない。データとして、静止画像、3D画像、動画、Macromedia Flash（登録商標）等の画像データあるいは  
20 動画データ、メソッドとして、そのような画像／動画データを携帯電話機40の画面に表示させるメソッドを用いてもよい。また、データとして、音声データあるいは楽曲データ、メソッドとして、そのような音声／楽曲データを携帯電話機40の再生部で再生させるメソッドを用いてもよい。

#### 25 発明の効果

以上説明したように本発明によれば、受信したプログラムに対する通信装置のセキュリティを確保しつつ、このようなプログラムが通信装置において実現することのできる機能を従来と比較して充実させることができる。

## 請求の範囲

1. プログラムを受信する受信手段と、

当該通信装置に記憶されているデータのうち、前記受信手段により受信された

5 プログラムを実行した場合に使用されるデータを特定する特定手段と、

前記特定手段により特定され、カプセル化されたデータを有するオブジェクトであって、該カプセル化されたデータを当該オブジェクトの外部から操作するためのメソッドであり、かつ、前記データを操作元のプログラムへ引き渡すことのないメソッドのみを有する完全カプセル化オブジェクトを生成する第1の生成手段と、

前記受信手段により受信されたプログラムを実行している場合にアクセスすることのできるリソースを制限し、当該通信装置に記憶されているデータのうち前記特定手段により特定されたデータへのアクセスを禁止する一方、前記生成手段により生成されたオブジェクトへのアクセスを許可するアクセス制御手段と

15 を有することを特徴とする通信装置。

2. 前記特定手段により特定され、カプセル化されたデータを有するオブジェクトであって、該カプセル化されたデータを当該オブジェクトの外部から操作するためのメソッドであり、かつ、前記データを操作元のプログラムへ引き渡すメソッドを少なくとも1つ有する非完全カプセル化オブジェクトを生成する第2の生成手段と、

データの保護の要否を示す保護要否情報を記憶する保護情報記憶手段と、

前記保護情報記憶手段に記憶された保護要否情報に基づいて、前記カプセル化されたデータと、当該カプセル化されたデータを操作するためのメソッドとを有するオブジェクトを、前記第1の生成手段または前記第2の生成手段のいずれが生成するのかを決定する決定手段と、

を有することを特徴とする請求項1に記載の通信装置。

3. 前記決定手段は、前記特定手段により特定されたデータに関連付けられた

保護要否情報が前記データの保護が必要であることを示している場合に、オブジェクトを前記第1の生成手段により生成することを決定する一方、保護要否情報が前記データの保護が不要であることを示している場合に、オブジェクトを前記第2の生成手段により生成することを決定する

5 ことを特徴とする請求項2に記載の通信装置。

4. 前記特定手段は、前記受信手段により受信されたプログラムを実行したときに、当該通信装置に記憶されているデータのうち、前記プログラムを実行した場合に使用されるデータを特定する

10 ことを特徴とする請求項2に記載の通信装置。

5. 前記第1の生成手段あるいは前記第2の生成手段により生成されたオブジェクトを前記プログラムの実行終了に応じて削除する削除手段をさらに有することを特徴とする請求項5に記載の通信装置。

15

6. 当該通信装置に記憶されているデータの重要度を示す情報を記憶する重要度記憶手段と、

前記重要度記憶手段に記憶された重要度が高いデータに対して当該データの保護が必要であることを示す情報を前記保護情報記憶手段に記憶する一方、前記重要度記憶手段に記憶された重要度が低いデータに対して当該データの保護が不要であることを示す情報を前記保護情報記憶手段記憶させる制御手段と  
20 を有することを特徴とする請求項2に記載の通信装置。

7. 当該通信装置に記憶されているデータに対し、そのデータが著作権の保護客体であることを示す情報を記憶する著作権情報記憶手段をさらに有し、

そのデータが著作権の保護客体であることが前記著作権情報記憶手段に記憶されている場合に当該データの保護が必要であることを示す情報を前記保護情報記憶手段に記憶させる一方、そのデータが著作権の保護客体ではないことが前記著作権情報記憶手段に記憶されている場合に当該データの保護が不要であることを

示す情報を前記保護情報記憶手段に記憶させる制御手段と  
を有することを特徴とする請求項 2 に記載の通信装置。

8 . 前記保護要否情報をユーザの操作入力に応じて前記保護情報記憶手段に記  
5 憶させる設定手段をさらに有する  
ことを特徴とする請求項 2 に記載の通信装置。

9 . 当該通信装置に記憶されているデータのうち前記特定手段により特定され  
たデータが更新されると、当該データの更新内容に従って前記生成手段により生  
10 成されたオブジェクト内にカプセル化されているデータを更新する更新手段をさ  
らに有する  
ことを特徴とする請求項 2 に記載の通信装置。

10 . 前記プログラムは、Java プログラミング言語で記述されたプログラ  
15 ムであって、当該通信装置は、前記プログラムを実行するための Java 実行環  
境を有している  
ことを特徴とする請求項 2 に記載の通信装置。

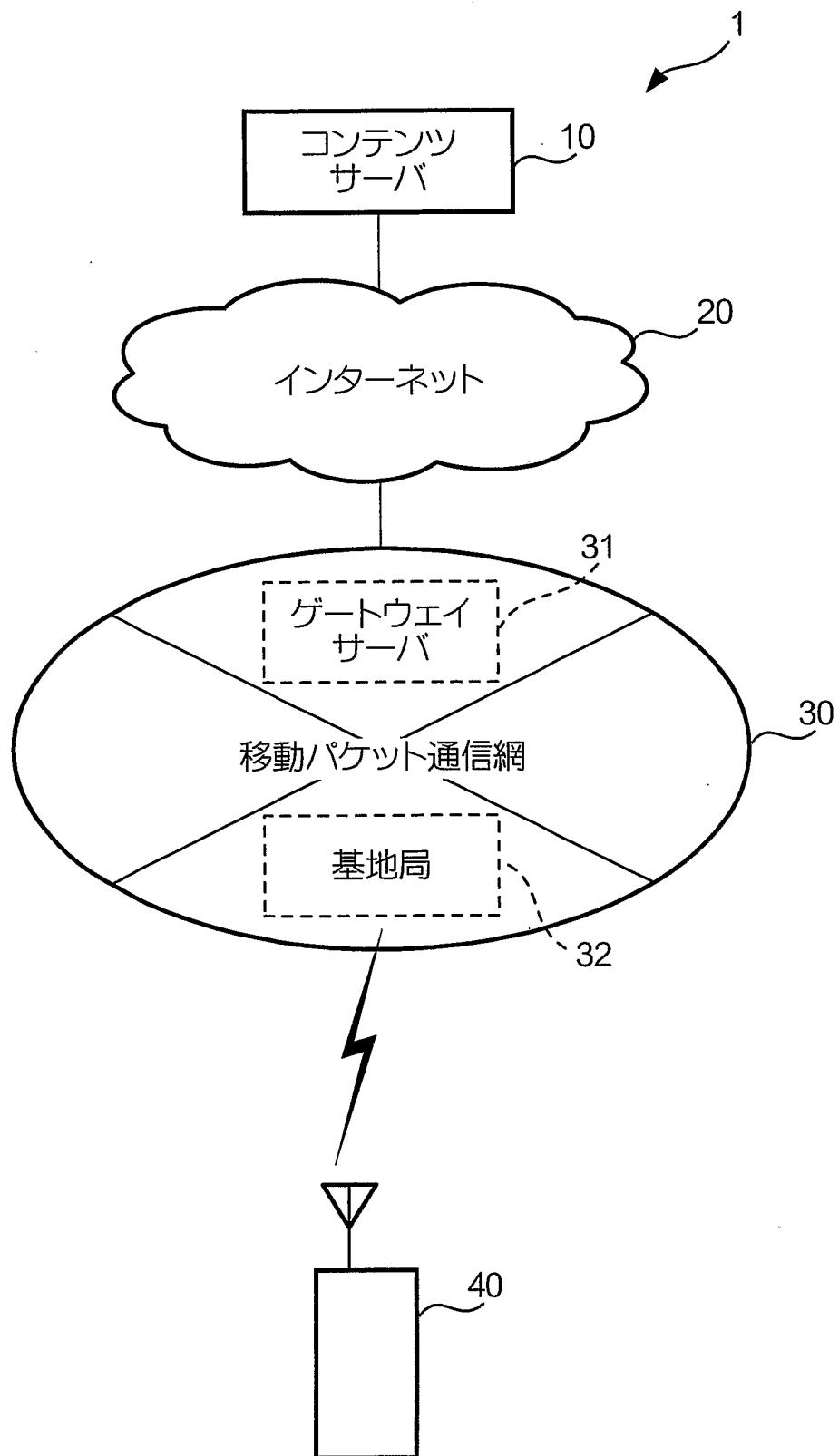
11 . 前記完全カプセル化オブジェクトに含まれるメソッドは、文字列データ  
20 を当該通信装置の表示部に表示するメソッドであることを特徴とする請求項 2 に  
記載の通信装置。

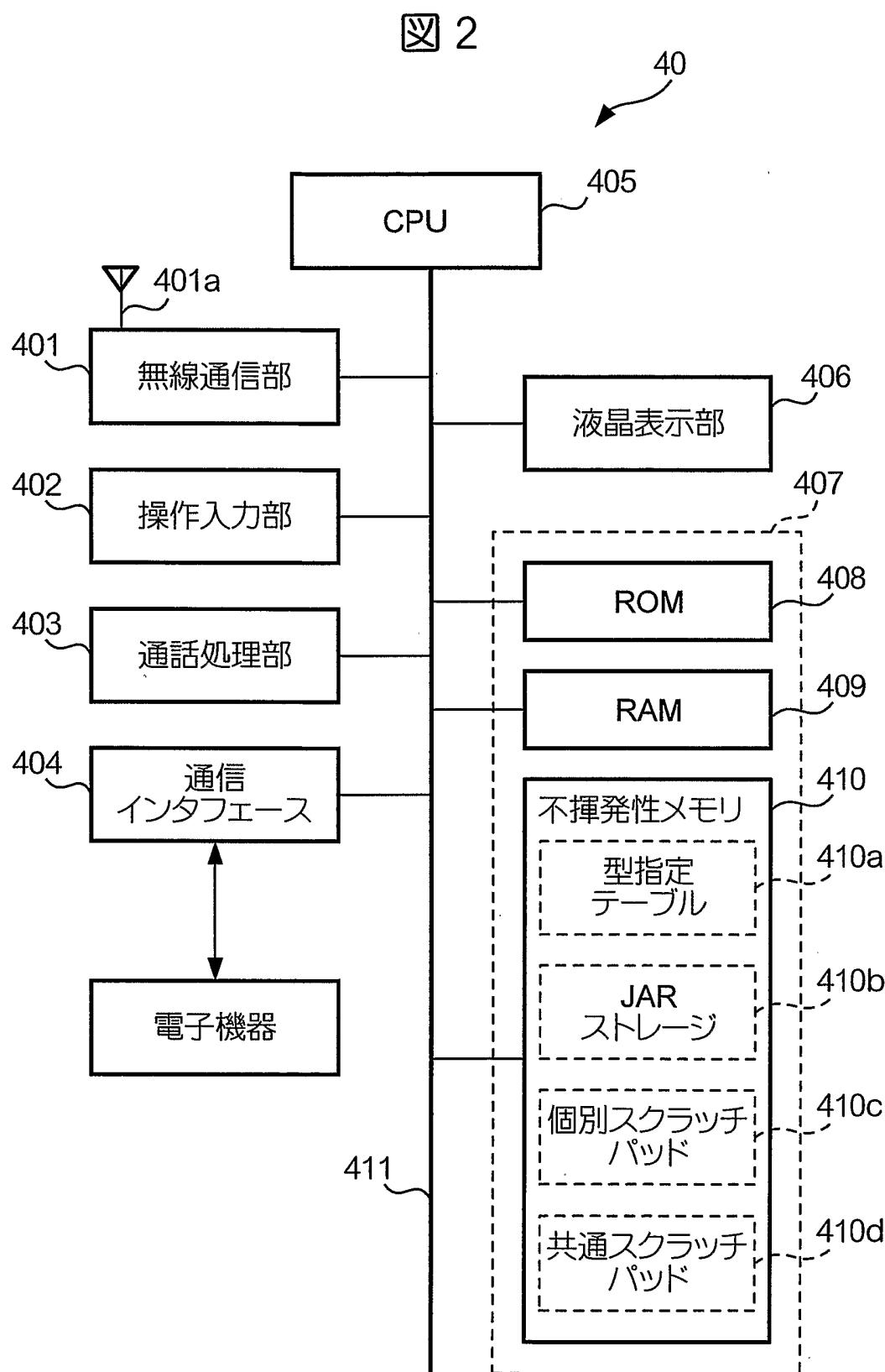
12 . 前記完全カプセル化オブジェクトに含まれるメソッドは、音声データを  
当該通信装置の再生部で再生するメソッドであることを特徴とする請求項 2 に記  
25 載の通信装置。

13 . 前記完全カプセル化オブジェクトに含まれるメソッドは、画像データを  
当該通信装置の表示部に表示するメソッドであることを特徴とする請求項 2 に記  
載の通信装置。

1/10

図 1





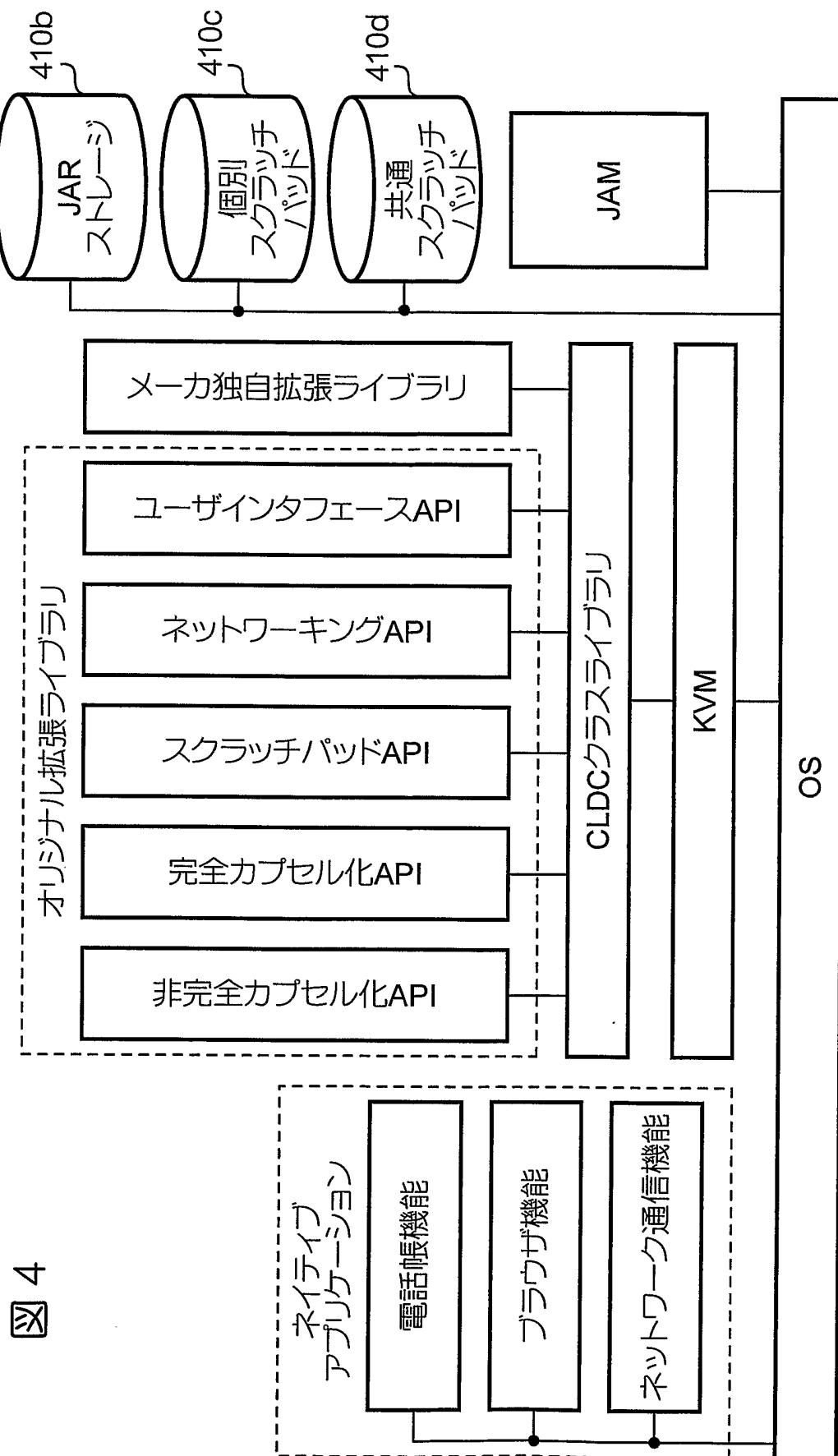
3/10

## 図 3

410a

データ名	型指定情報
アドレス帳データ	1 (完全カプセル化型)
電子メールデータ	1
着信・発信履歴データ	1
ユーザデータ	1
コンテンツA (著作権保護フラグ“1”)	1
コンテンツB (著作権保護フラグ“0”)	0 (非完全カプセル化型)
自作画像データ	0
⋮	⋮

4/10



5/10

図 5

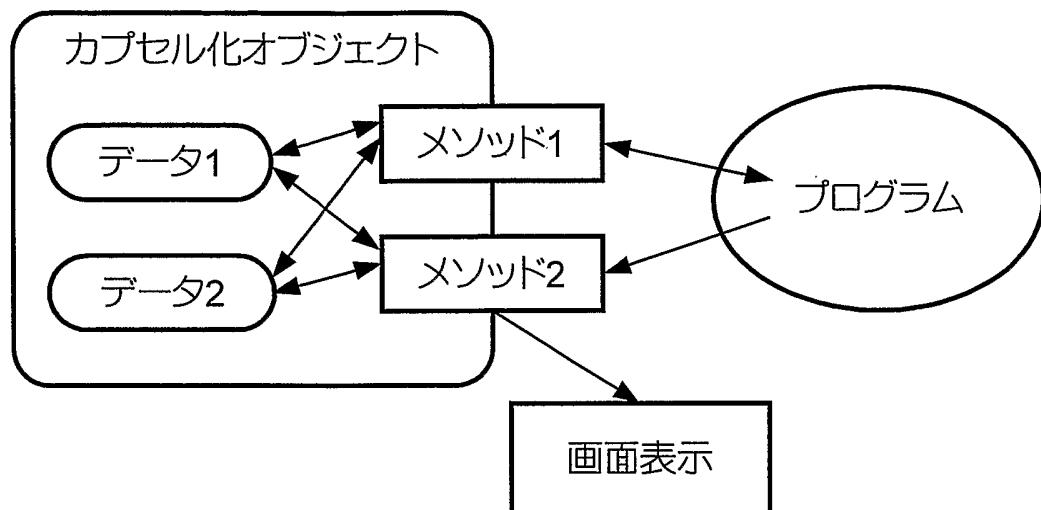


図 6

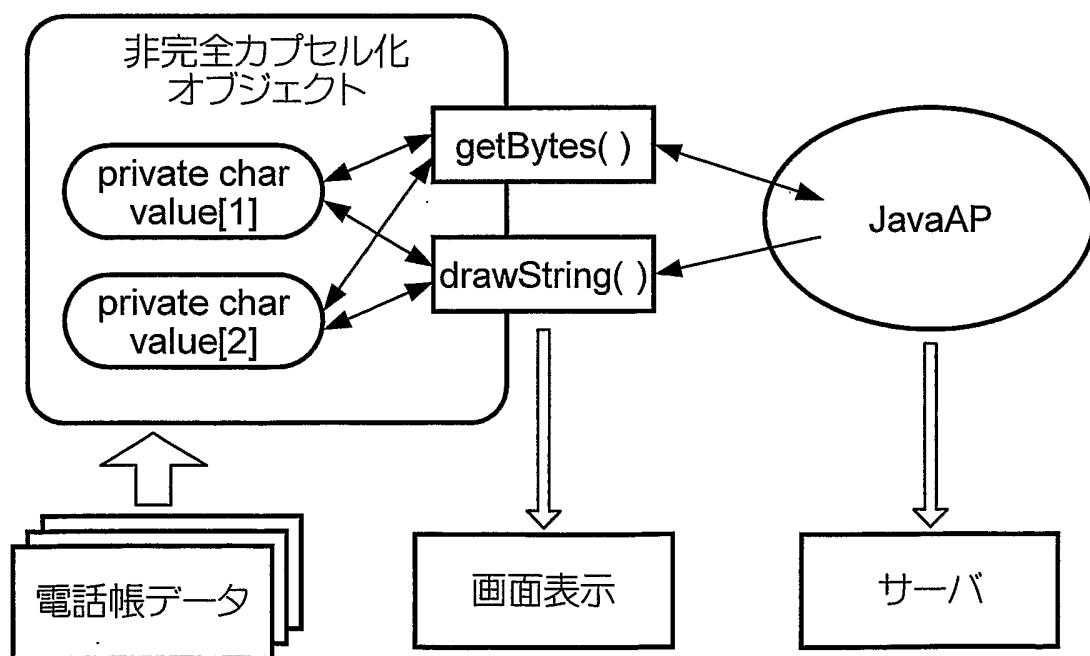


図 7

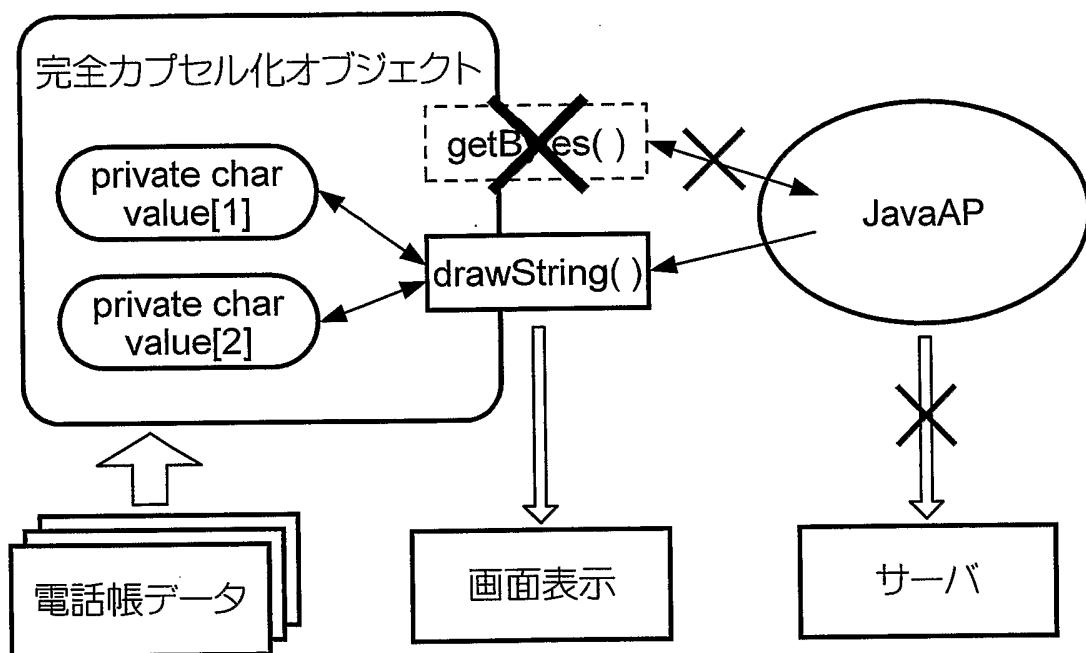
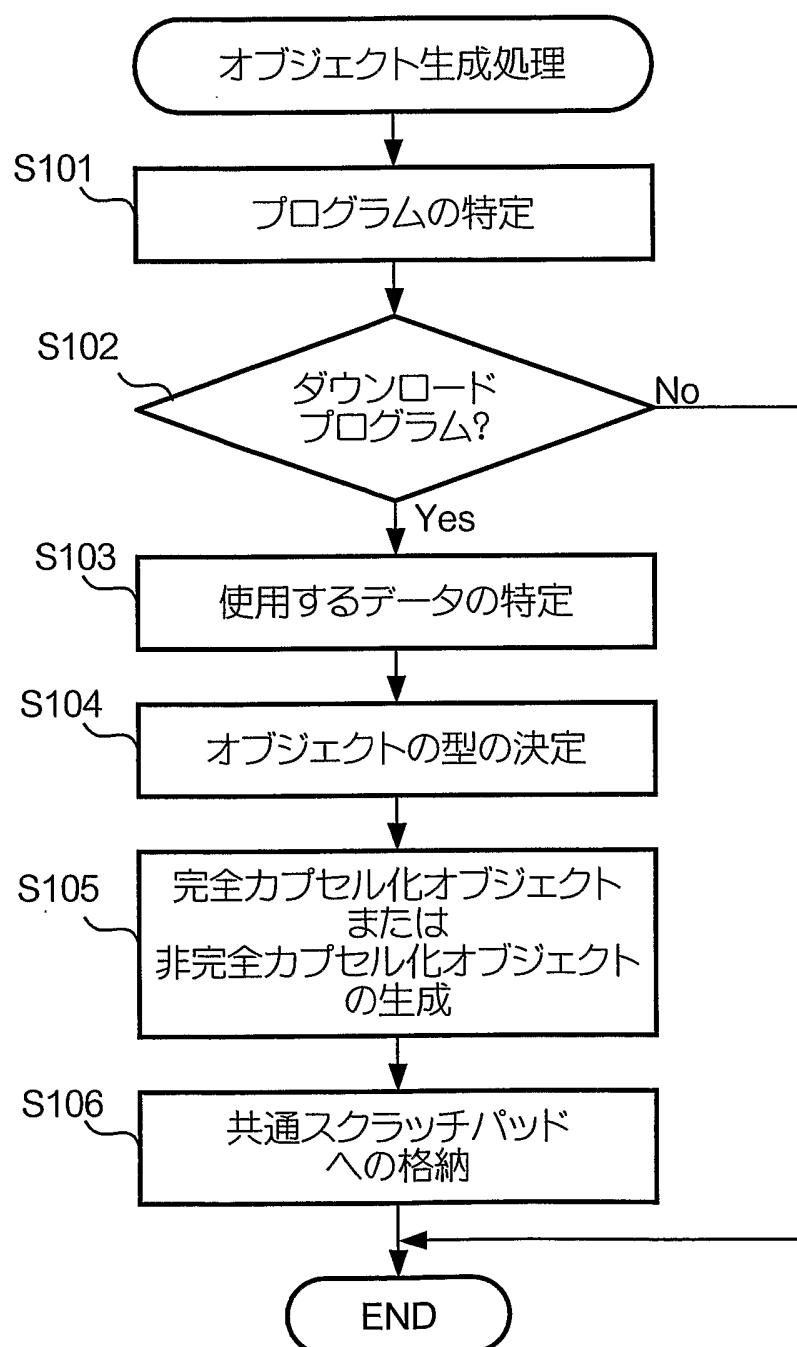


図 8



8/10

図 9

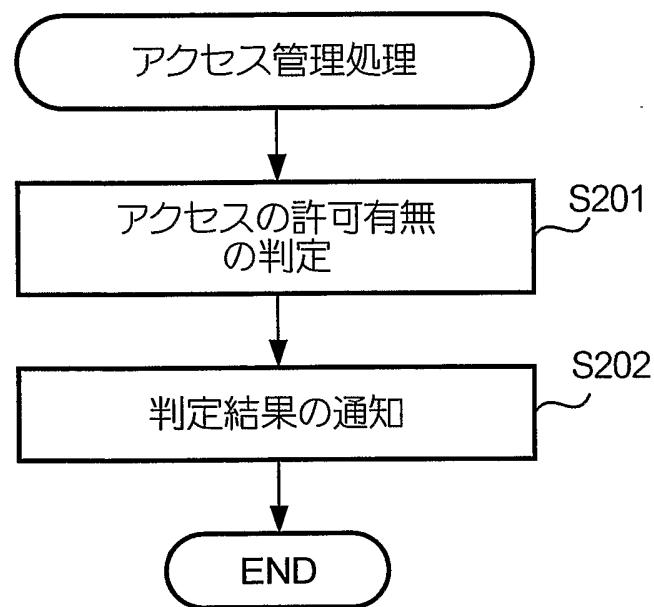
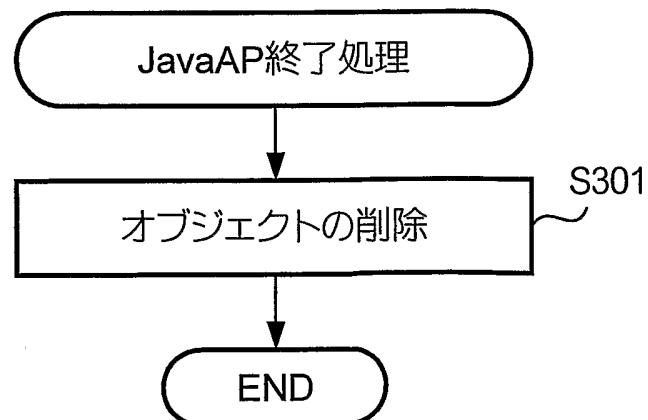
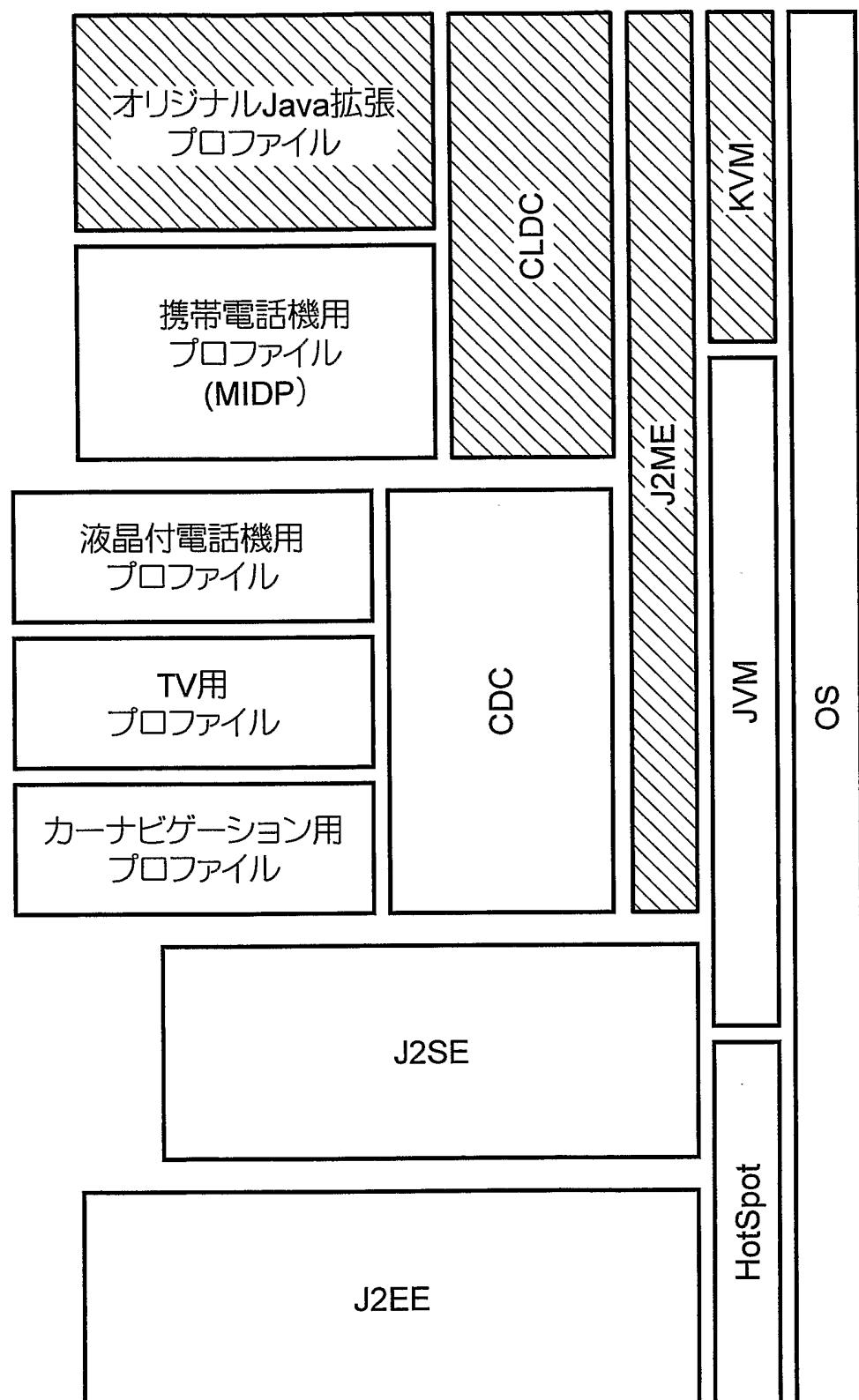


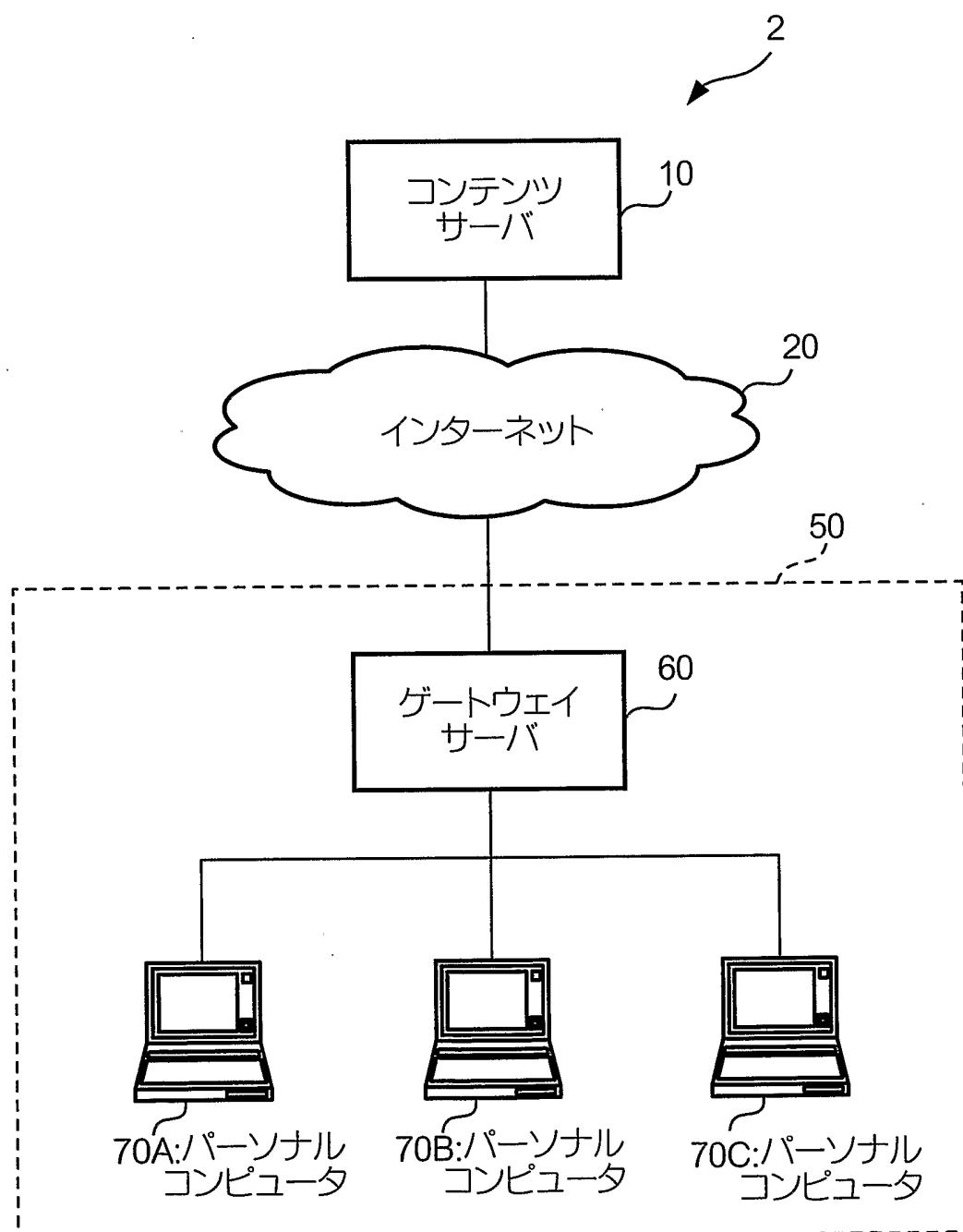
図 10





10/10

図 12



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/06099

**A. CLASSIFICATION OF SUBJECT MATTER**

Int.Cl<sup>7</sup> G06F12/14, G06F9/44, H04B7/26, H04M1/00, H04M1/725

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F12/14, G06F9/44, H04B7/26, H04M1/00, H04M1/725

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Tetsuya KAKU, Masahiro YAMADA, Hiroaki ITO, "Hajimete no i mode Java Programing", Nikkei Business Publications, Inc., 26 March, 2001 (26.03.01), pages 30 to 41	1-13
Y	Scott Oaks, translated under the supervision of Akio SHIMADA, "Java Security", Kabushiki Kaisha Orairi Japan, 28 November, 2001 (28.11.01), pages 19 to 33, 69 to 96	1-13
Y	JP 2001-350664 A (Nippon Telegraph And Telephone Corp.), 21 December, 2001 (21.12.01), All pages; all drawings (Family: none)	1-13

Further documents are listed in the continuation of Box C.  See patent family annex.

* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
---	--

Date of the actual completion of the international search  
18 August, 2003 (18.08.03)

Date of mailing of the international search report  
02 September, 2003 (02.09.03)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP03/06099

**C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-43176 A (Sun Micro Systems Inc.), 16 February, 2001 (16.02.01), All pages; all drawings & EP 1061440 A2	1-13
P,A	"i Appli Contents Kaihatsu Guid for DoJa-3.0 Shosai-Hen", [online], NTT DoCoMo, Inc., 17 April, 2003 (17.04.03), [retrieved on 2003-08-06], Retrieved from the Internet: <URL: http://www.nttdocomo.co.jp/p_s/imode/java/pdf/jguidefordoja3_0_030417.pdf>	1-13
P<A	Tetsu YAMATO, "Ketai Yogo no Kiso Chisiki Dai 132 Kai: i Appli DX towa", [online], Impress Corp., 13 May, 2003 (13.05.03), [retrieved on 2003-08-06], Retrieved from the Internet: <URL: http://k-tai.impress.co.jp/cda/article/keyword/13956.html>	1-13

A. 発明の属する分野の分類（国際特許分類（IPC））  
Int.Cl' G06F12/14, G06F9/44, H04B7/26, H04M1/00, H04M1/725

## B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））  
Int.Cl' G06F12/14, G06F9/44, H04B7/26, H04M1/00, H04M1/725

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926 - 1996
日本国公開実用新案公報	1971 - 2003
日本国登録実用新案公報	1994 - 2003
日本国実用新案登録公報	1996 - 2003

## 国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	加来 徹也, 山田 昌宏, 伊藤 広明, "はじめての i モード Java プログラミング", 日経BP社, 2001.03.26, pp. 30-41	1-13
Y	Scott Oaks 著, 島田 秋雄 監訳, "Java セキュリティ", 株式会社オライリー・ジャパン, 2001.11.28, pp. 19-33, 69-96	1-13
Y	JP 2001-350664 A (日本電信電話株式会社) 2001.12.21, 全頁 (ファミリーなし)	1-13

C 欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）  
 「O」口頭による開示、使用、展示等に言及する文献  
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

## の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」同一パテントファミリー文献

国際調査を完了した日 18.08.03	国際調査報告の発送日 02.09.03
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 奥村 元宏 5 N 3044 電話番号 03-3581-1101 内線 3585

## C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2001-43176 A (サン・マイクロシステムズ・インコーポレーテッド) 2001.02.16, 全頁, 全図 & EP 1061440 A2	1-13
PA	” i アプリコンテンツ開発ガイド for DoJa-3.0 詳細編” , [online], NTT DoCoMo, Inc., 2003.04.17, [retrieved on 2003-08-06], Retrieved from the Internet: <URL: http://www.nttdocomo.co.jp/p_s/imode/java/pdf/jguidefordoja3_0_030417.pdf>	1-13
PA	大和 哲, ” ケータイ用語の基礎知識 第132回： i アプリ DX とは” , [online], Impress Corporation, 2003.05.13, [retrieved on 2003-08-06], Retrieved from the Internet: <URL: http://k-tai.impress.co.jp/cda/article/keyword/13956.htm>	1-13