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

特許第4209131号
(P4209131)

(45)発行日　平成21年1月14日(2009.1.14)　(24)登録日　平成20年10月31日(2008.10.31)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	520A
G06F 12/00	(2006.01)	G06F	12/14	560A
G06F 21/20	(2006.01)	G06F	12/00	537A
H04L 9/32	(2006.01)	G06F	15/00	330F
H04N 1/44	(2006.01)	H04L	9/00	675B

請求項の数 14　(全 17 頁)　最終頁に続く

(21)出願番号　特願2002-121080(P2002-121080)
(22)出願日　平成14年4月23日(2002.4.23)
(65)公開番号　特開2003-316651(P2003-316651A)
(43)公開日　平成15年11月7日(2003.11.7)
審査請求日　平成17年4月5日(2005.4.5)

(73)特許権者　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100088155
弁理士　長谷川　芳樹
(74)代理人　100092657
弁理士　寺崎　史朗
(74)代理人　100114270
弁理士　黒川　朋也
(74)代理人　100108213
弁理士　阿部　豊隆
(74)代理人　100113549
弁理士　鈴木　守

最終頁に続く

(54)【発明の名称】携帯端末、及びアクセス制御方法

(57)【特許請求の範囲】
【請求項１】
電話帳データを格納する電話帳データ格納手段と、
前記電話帳データ格納手段に格納されている前記電話帳データを管理する電話帳管理アプリケーションプログラムに対する他のアプリケーションプログラムからのアクセス権認証要求を、当該アプリケーションプログラムの有するアプリケーション認証情報と共に取得する要求取得手段と、
前記要求取得手段により取得された前記アクセス権認証要求に応じて、前記アプリケーション認証情報の正当性を判定する検証手段と、
前記検証手段により前記アプリケーション認証情報が正当であると判定された場合に前記アクセス権認証要求を許可し、前記電話帳データに対するアクセス要求に応じて、前記アプリケーションプログラムに対して前記電話帳データを出力する出力手段と
を備えることを特徴とする携帯端末。
【請求項２】
前記アプリケーション認証情報は、デジタル署名及び公開鍵証明書を含むことを特徴とする請求項１に記載の携帯端末。
【請求項３】
前記アプリケーション認証情報は、属性証明書を更に含むことを特徴とする請求項２に記載の携帯端末。
【請求項４】

本人の身体的特徴を示す身体情報を格納する身体情報格納手段と、
前記身体情報格納手段に格納されている前記身体情報と、前記アクセス権認証要求を指示するユーザの身体情報とを照合して、各身体情報の同一性を判定する判定手段とを更に備え、
前記要求取得手段は、前記判定手段により前記各身体情報が同一であるものと判定された場合に、当該判定結果が反映されたユーザ認証情報を取得し、
前記検証手段は、前記要求取得手段により取得された前記アクセス権認証要求に応じて、前記ユーザ認証情報の正当性を判定し、
前記出力手段は、前記検証手段により前記ユーザ認証情報が正当であると判定された場合に前記アクセス権認証要求を許可し、前記電話帳データに対するアクセス要求に応じて、前記電話帳データを前記アプリケーションプログラムに対して出力することを特徴とする請求項１又は２に記載の携帯端末。
【請求項５】
前記身体情報は、指紋情報であることを特徴とする請求項４に記載の携帯端末。
【請求項６】
前記アクセス権認証要求は、前記電話帳管理アプリケーションプログラムに対する前記電話帳データの表示権認証要求であり、
前記アクセス要求は、前記電話帳データの表示要求であり、
前記出力手段は、前記表示要求に応じて前記電話帳データを表示手段に表示させることを特徴とする請求項１～５の何れか一項に記載の携帯端末。
【請求項７】
前記アクセス権認証要求は、前記電話帳管理アプリケーションプログラムに対する、前記電話帳データに含まれる電話番号への電話発信権認証要求であり、
前記アクセス要求は、前記電話番号への電話発信要求であり、
前記出力手段は、前記電話発信要求に応じて前記電話番号に電話発信させることを特徴とする請求項１～５の何れか一項に記載の携帯端末。
【請求項８】
携帯端末が、アプリケーションプログラムからアクセス要求を取得するアクセス制御方法において、
前記携帯端末が、当該携帯端末の電話帳データ格納手段に格納されている前記電話帳データを管理する電話帳管理アプリケーションプログラムに対する他のアプリケーションプログラムからのアクセス権認証要求を、当該アプリケーションプログラムの有するアプリケーション認証情報と共に取得する要求取得工程と、
前記携帯端末が、前記要求取得工程にて取得された前記アクセス権認証要求に応じて、前記アプリケーション認証情報の正当性を判定する検証工程と、
前記携帯端末が、前記検証工程にて前記アプリケーション認証情報が正当であると判定された場合に前記アクセス権認証要求を許可し、前記電話帳データに対するアクセス要求に応じて、前記アプリケーションプログラムに対して前記電話帳データを出力する出力工程と
を含むことを特徴とするアクセス制御方法。
【請求項９】
前記アプリケーション認証情報は、デジタル署名及び公開鍵証明書を含むことを特徴とする請求項８に記載のアクセス制御方法。
【請求項１０】
前記アプリケーション認証情報は、属性証明書を更に含むことを特徴とする請求項９に記載のアクセス制御方法。
【請求項１１】
前記携帯端末が、当該携帯端末の身体情報格納手段に格納されている本人の身体的特徴を示す身体情報と、前記アクセス権認証要求を指示するユーザの身体情報とを照合して、各身体情報の同一性を判定する判定工程を更に含み、

前記要求取得工程では、前記判定工程にて前記各身体情報が同一であるものと判定された場合に、当該判定結果が反映されたユーザ認証情報を取得し、
前記検証工程では、前記要求取得工程にて取得された前記アクセス権認証要求に応じて、前記ユーザ認証情報の正当性を判定し、
前記出力工程では、前記検証工程にて前記ユーザ認証情報が正当であると判定された場合に前記アクセス権認証要求を許可し、前記電話帳データに対するアクセス要求に応じて、前記電話帳データを前記アプリケーションプログラムに対して出力することを特徴とする請求項８又は９に記載のアクセス制御方法。
【請求項１２】
前記身体情報は、指紋情報であることを特徴とする請求項１１に記載のアクセス制御方法。
【請求項１３】
前記アクセス権認証要求は、前記電話帳管理アプリケーションプログラムに対する前記電話帳データの表示権認証要求であり、
前記アクセス要求は、前記電話帳データの表示要求であり、
前記出力工程では、前記表示要求に応じて前記電話帳データを表示手段に表示させることを特徴とする請求項８～１２の何れか一項に記載のアクセス制御方法。
【請求項１４】
前記アクセス権認証要求は、前記電話帳管理アプリケーションプログラムに対する、前記電話帳データに含まれる電話番号への電話発信権認証要求であり、
前記アクセス要求は、前記電話番号への電話発信要求であり、
前記出力工程では、前記電話発信要求に応じて前記電話番号に電話発信させることを特徴とする請求項８～１２の何れか一項に記載のアクセス制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、携帯端末、及びアクセス制御方法に関する。
【０００２】
【従来の技術】
近年、氏名、電話番号、メールアドレス等の様々な個人情報が電子データ化されて登録された電話帳を有する携帯端末が実用化されている。携帯端末のユーザは電話帳を使用することにより、所望の通信相手の氏名を選択するという容易な操作で、電話番号やメールアドレスを所定の領域に入力できる。通常電話帳は、携帯端末に予め記録されている電話帳管理専用のアプリケーションプログラム（以下、「電話帳管理アプリケーション」）によって管理されている。
【０００３】
【発明が解決しようとする課題】
しかしながら、上記従来技術では以下に示すような問題点があった。すなわち、電話帳には多数の個人情報が登録されているので、登録された情報の漏洩や改竄を防いで一定のセキュリティを確保する必要がある。そこで、ＩＣカード等の耐タンパー性を有する装置の内部に電話帳を格納することにより、電話帳管理アプリケーションからのアクセスのみを許可し、他のアプリケーションプログラムからのアクセスを一括して拒否する方法も考えられる。
【０００４】
ところが、近年では、携帯端末に格納されるデータの大容量化や無線通信技術の発達に伴い、携帯端末にダウンロード可能なアプリケーションプログラムの種類は急速に増加している。この様なアプリケーションプログラムの中には、正当な理由で、電話帳に登録された個人情報を参照すべき機能を有するものもある。この様なアプリケーションプログラムからのアクセスに対してまで、電話帳の参照を拒否するのは、携帯端末及びアプリケーションプログラムの機能を有効に活用して利便性を向上する観点から好ましくない。

【０００５】
そこで、本発明は上記事情に鑑みて、高いセキュリティを維持しつつ、アプリケーションプログラムからの電話帳データに対するアクセスが可能な携帯端末、及びアクセス制御方法を実現することを課題とする。
【０００６】
【課題を解決するための手段】
上記課題を解決すべく、本発明に係る携帯端末は、電話帳データを格納する電話帳データ格納手段と、前記電話帳データ格納手段に格納されている前記電話帳データを管理する電話帳管理アプリケーションプログラムに対する他のアプリケーションプログラムからのアクセス権認証要求を、当該アプリケーションプログラムの有するアプリケーション認証情報と共に取得する要求取得手段と、前記要求取得手段により取得された前記アクセス権認証要求に応じて、前記アプリケーション認証情報の正当性を判定する検証手段と、前記検証手段により前記アプリケーション認証情報が正当であると判定された場合に前記アクセス権認証要求を許可し、前記電話帳データに対するアクセス要求に応じて、前記アプリケーションプログラムに対して前記電話帳データを出力する出力手段とを備える。
【０００７】
本発明に係るアクセス制御方法は、携帯端末が、アプリケーションプログラムからアクセス要求を取得するアクセス制御方法において、前記携帯端末が、当該携帯端末の電話帳データ格納手段に格納されている前記電話帳データを管理する電話帳管理アプリケーションプログラムに対する他のアプリケーションプログラムからのアクセス権認証要求を、当該アプリケーションプログラムの有するアプリケーション認証情報と共に取得する要求取得工程と、前記携帯端末が、前記要求取得工程にて取得された前記アクセス権認証要求に応じて、前記アプリケーション認証情報の正当性を判定する検証工程と、前記携帯端末が、前記検証工程にて前記アプリケーション認証情報が正当であると判定された場合に前記アクセス権認証要求を許可し、前記電話帳データに対するアクセス要求に応じて、前記アプリケーションプログラムに対して前記電話帳データを出力する出力工程とを含む。
【０００８】
これらの発明によれば、電話帳データを管理する電話帳管理アプリケーションプログラムに対する他のアプリケーションプログラムからのアクセス権認証要求と共に取得されたアプリケーション認証情報が正当であると判定された場合に、前記電話帳データに対するアクセス要求に応じて、前記アプリケーションプログラムに対して前記電話帳データが出力される。すなわち、携帯端末は、正当なアプリケーション認証情報を有するアプリケーションプログラムからのアクセス権認証要求を許可し、正当なアプリケーション認証情報を有さないアプリケーションプログラムからのアクセス権認証要求を拒否する。そして、携帯端末は、アクセス権認証要求が許可されたアプリケーションプログラムからの電話帳データに対するアクセス要求を許可する。これにより、携帯端末において、高いセキュリティを維持しつつ、アプリケーションプログラムからの電話帳データに対するアクセスが可能となる。
【０００９】
本発明に係る携帯端末において好ましくは、前記アプリケーション認証情報は、デジタル署名及び公開鍵証明書を含む。
本発明に係るアクセス制御方法において好ましくは、前記アプリケーション認証情報は、デジタル署名及び公開鍵証明書を含む。
【００１０】
これらの発明によれば、アプリケーション認証情報はデジタル署名及び公開鍵証明書を含む。携帯端末は、デジタル署名と公開鍵証明書とを組み合わせて、アクセス権認証を要求したアプリケーションプログラムの正当性の判定を行うことにより、アクセス制御をより高精度に行うことができる。その結果、携帯端末において、より高いセキュリティレベルを維持しつつアプリケーションプログラムからの電話帳データに対するアクセスが可能となる。

【００１１】
本発明に係る携帯端末において好ましくは、前記アプリケーション認証情報は、属性証明書を更に含む。
本発明に係るアクセス制御方法において好ましくは、前記アプリケーション認証情報は、属性証明書を更に含む。
【００１２】
公開鍵証明書の有する権利情報（アプリケーションプログラムの正当性を判定する際に参照される情報）が有効期間内は変更できないのに対して、属性証明書の有する権利情報は公開鍵証明書とは独立した有効期間を設定可能である。したがって、これらの発明によれば、証明書を再発行する手続きを必要とせずに、証明書の有する権利情報を容易に変更できる。
【００１３】
本発明に係る携帯端末は、本人の身体的特徴を示す身体情報を格納する身体情報格納手段と、前記身体情報格納手段に格納されている前記身体情報と、前記アクセス権認証要求を指示するユーザの身体情報とを照合して、各身体情報の同一性を判定する判定手段とを更に備え、前記要求取得手段は、前記判定手段により前記各身体情報が同一であるものと判定された場合に、当該判定結果が反映されたユーザ認証情報を取得し、前記検証手段は、前記要求取得手段により取得された前記アクセス権認証要求に応じて、前記ユーザ認証情報の正当性を判定し、前記出力手段は、前記検証手段により前記ユーザ認証情報が正当であると判定された場合に前記アクセス権認証要求を許可し、前記電話帳データに対するアクセス要求に応じて、前記電話帳データを前記アプリケーションプログラムに対して出力する。
【００１４】
本発明に係るアクセス制御方法は、前記携帯端末が、当該携帯端末の身体情報格納手段に格納されている本人の身体的特徴を示す身体情報と、前記アクセス権認証要求を指示するユーザの身体情報とを照合して、各身体情報の同一性を判定する判定工程を更に含み、前記要求取得工程では、前記判定工程にて前記各身体情報が同一であるものと判定された場合に、当該判定結果が反映されたユーザ認証情報を取得し、前記検証工程では、前記要求取得工程にて取得された前記アクセス権認証要求に応じて、前記ユーザ認証情報の正当性を判定し、前記出力工程では、前記検証工程にて前記ユーザ認証情報が正当であると判定された場合に前記アクセス権認証要求を許可し、前記電話帳データに対するアクセス要求に応じて、前記電話帳データを前記アプリケーションプログラムに対して出力する。
【００１５】
これらの発明によれば、本人（携帯端末の正規の契約者）の身体情報と、アクセス権認証要求を指示するユーザの身体情報とが同一であるものと判定された場合に、アプリケーションプログラムからのアクセス要求に応じて、電話帳データが前記アプリケーションプログラムに対して出力される。すなわち、携帯端末は身体情報を参照して本人確認を行い、本人の指示に基づくアクセス権認証要求を許可し、本人以外の指示に基づくアクセス権認証要求を拒否する。そして、携帯端末は、アクセス権認証要求が許可されたアプリケーションプログラムからの電話帳データに対するアクセス要求を許可する。これにより、アプリケーションプログラム認証とユーザ認証とを組み合わせたアクセス制御が可能となり、電話帳データにアクセスする際のセキュリティレベルを一層向上できる。
【００１６】
本発明に係る携帯端末において好ましくは、前記身体情報は指紋情報である。
本発明に係るアクセス制御方法において好ましくは、前記身体情報は指紋情報である。
【００１７】
これらの発明によれば、アクセス権認証要求を指示するユーザの本人確認を行うにあたり、本人の身体的特徴を示す情報として指紋情報（例えば、指紋の特徴点データ）が使用される。したがって、ユーザが手指の指紋を指紋読取装置に読み取らせるという容易な操作で、携帯端末は、暗証番号やパスワードを利用した認証に比べて精確な本人確認が可能と

なる。なお、ユーザ認証に使用される身体情報としては、指紋情報に限らず、例えば眼球の虹彩や網膜、声紋、顔画像などに関する情報であってもよい。この様な身体情報を利用したユーザ認証は、原理的に極めてなりすましが困難であり、本人確認の精度を一層向上できる。

【００１８】

本発明に係る携帯端末において、より好ましくは、前記アクセス権認証要求は、前記電話帳管理アプリケーションプログラムに対する前記電話帳データの表示権認証要求であり、前記アクセス要求は、前記電話帳データの表示要求であり、前記出力手段は、前記表示要求に応じて前記電話帳データを表示手段に表示させる。

【００１９】

本発明に係るアクセス制御方法において、より好ましくは、前記アクセス権認証要求は、前記電話帳管理アプリケーションプログラムに対する前記電話帳データの表示権認証要求であり、前記アクセス要求は、前記電話帳データの表示要求であり、前記出力工程では、前記表示要求に応じて前記電話帳データを表示手段に表示させる。

【００２０】

電話帳データの中には、氏名やフリガナ等のように、表示手段に表示（可視化）されて初めて、その電話帳データ本来の機能を実現できるものも少なくない。したがって、この様な電話帳データの場合には特に、電話帳データに対するアクセス権認証要求は、電話帳データの表示権認証要求であることが想定される。また、アクセス要求は、電話帳データの表示要求であることが想定される。このため、電話帳データが携帯端末の電話帳データ格納手段から読み出されるのみならず、表示手段に表示されることによって、電話帳データが携帯端末のユーザの閲覧に供される。

【００２１】

本発明に係る携帯端末において、より好ましくは、前記アクセス権認証要求は、前記電話帳管理アプリケーションプログラムに対する、前記電話帳データに含まれる電話番号への電話発信権認証要求であり、前記アクセス要求は、前記電話番号への電話発信要求であり、前記出力手段は、前記電話発信要求に応じて前記電話番号に電話発信させる。

【００２２】

本発明に係るアクセス制御方法において、より好ましくは、前記アクセス権認証要求は、前記電話帳管理アプリケーションプログラムに対する、前記電話帳データに含まれる電話番号への電話発信権認証要求であり、前記アクセス要求は、前記電話番号への電話発信要求であり、前記出力工程では、携帯端末は、前記電話発信要求に応じて前記電話番号に電話発信させる。

【００２３】

電話帳データの中には電話番号が存在するが、電話番号はその電話番号に電話発信されて初めて、その機能本来の効果を奏する場合が多い。したがって、電話番号の場合には特に、電話帳データに対するアクセス権認証要求は、電話番号への電話発信権認証要求であることが想定される。同様に、アクセス要求は、電話番号への電話発信要求であることが想定される。このため、電話番号が携帯端末の電話帳データ格納手段から読み出されるのみならず、発信されることによって、電話番号が携帯端末のユーザの使用に供される。

【００２４】

【発明の実施の形態】

以下、添付図面を参照して本発明に係る携帯端末について説明する。

まず、構成を説明する。図１は、携帯端末１０の機能的構成を示すブロック図である。携帯端末１０は、制御装置１１、入力装置１２、ＲＡＭ１３、表示装置１４、記憶装置１５、無線通信装置１６、指紋読取装置１７、及び音声処理装置１８を備えて構成される。また、これら各装置は、それぞれバス１９を介して電気的に接続されており、相互に各種信号の入出力が可能となっている。

【００２５】

制御装置１１は、記憶装置１５に記憶されているプログラムをＲＡＭ１３に読み出し、当

該プログラムに従って各部を集中制御する。すなわち、制御装置１１は、入力装置１２からの入力信号とＲＡＭ１３に読み出されたプログラムとに従って、後述の電話帳データベース１５１に格納されている電話帳データ（例えば、電話番号）に対するアクセス制御処理等の各種処理を実行し、その処理結果をＲＡＭ１３に一時的に記憶する。そして、ＲＡＭ１３に記憶された処理結果を必要に応じて記憶装置１５内部の所定の領域に格納させる。

【００２６】

入力装置１２は、データ及び処理の選択、電源のON/OFF等を指示する各種操作釦を備えて構成され、これら各種操作釦は、単独で又は組み合せて押下されることにより、指示内容に応じた入力信号を制御装置１１に出力する。また、入力装置１２は、手指や専用ペンによる接触を感知する素子を、表示装置１４の表示画面上に配置した透明なスクリーン（所謂、タッチスクリーン）により構成され、接触された位置座標に応じた入力信号を制御装置１１に出力する。接触の感知方式は、押圧力の変化を感知する感圧式、静電気による電気信号を感知する静電式など任意である。

【００２７】

ＲＡＭ（Random Access Memory）１３は、揮発性の半導体メモリにより構成され、制御装置１１により実行される各種処理において、後述する記憶装置１５から読み出されたプログラムやデータを一時的に格納する。また、ＲＡＭ１３は、表示装置１４に表示されるデータを一時的に記憶するＶＲＡＭ（Video RAM）の機能も併有する。

【００２８】

表示装置１４は、ＬＣＤ（Liquid Crystal Display）やＥＬ（Electro Luminescence）等により構成され、制御装置１１から入力される表示信号に従って画面上にデータの表示を行う。また、表示装置１４の画面上には、上述した入力装置１２としてのタッチスクリーンが覆設されている。

【００２９】

記憶装置１５は、ＥＥＰＲＯＭ（Electrically Erasable and Programmable ROM）等の不揮発性の半導体メモリにより構成され、各種処理の実行に際して必要なデータや各種処理の実行の結果生成されたデータ等を記憶する。

【００３０】

記憶装置１５は、電話帳データベース１５１を有する。電話帳データベース１５１には、後述の電話帳管理アプリケーション１５２によって登録された氏名、フリガナ、電話番号、メールアドレス、グループ名等のデータ（以下纏めて「電話帳データ」と記す。）が格納されている。電話帳データは、所定のアプリケーションプログラム（例えば、表示用アプリケーション１５３）により表示装置１４に表示される。好適には、電話帳データは暗号化されている。また、電話帳データベース１５１は、電話帳データに対するアクセスが許可されたアプリケーションプログラムからのアクセスが可能な様に非タンパー領域に存在する。

【００３１】

図２は、電話帳データベース１５１内部のデータ格納例を示す構成図である。図２に示す様に、電話帳データベース１５１は、氏名格納領域１５１ａと、フリガナ格納領域１５１ｂと、電話番号格納領域１５１ｃと、メールアドレス格納領域１５１ｄと、グループ名格納領域１５１ｅとを有する。これら各格納領域には、氏名（例えば、「○○太郎」…）、フリガナ（例えば、「○○タロウ」…）、電話番号（例えば、「090-1234-5678」…）、メールアドレス（例えば、「taro@***.ne.jp」…）、グループ名（例えば、「Ａ」…）の電話帳データが、それぞれ対応付けられて格納されている。

【００３２】

また、記憶装置１５は、電話帳データベース１５１に格納されている電話帳データの登録や呼出などの管理を行うアプリケーションプログラム（以下、「電話帳管理アプリケーション１５２」と記す。）が格納されている。この電話帳管理アプリケーション１５２には、機密性を高めて改竄や不正使用を困難にするために、耐タンパーソフトウェア化が施さ

れている。

【００３３】

図３は、電話帳管理アプリケーション１５２の構成例を示す図である。図３に示す様に、電話帳管理アプリケーション１５２は、アクセスリスト１５２ａと、デジタル署名１５２ｂと、公開鍵証明書１５２ｃとを有する。

【００３４】

アクセスリスト１５２ａは、電話帳データに対するアクセス権限を表す証明書と、アプリケーションプログラムからのアクセス要求に応じて出力可能（すなわちアクセス可能）な情報とを対応付けて格納するデータリストである。ここで、本発明に係るアクセス要求とは、対象となるデータの読出し要求のみならず、データの表示要求や発信要求をも含む。

【００３５】

以下、図４を参照して、アクセスリストの構成例について詳述する。図４は、アクセスリスト１５２ａのデータ格納例を示す図である。図４に示す様に、アクセスリスト１５２ａは、Subject領域１５２ｄと、証明書種別領域１５２ｅと、アクセス可能情報領域１５２ｆとを有する。

【００３６】

Subject領域１５２ｄには、電話帳データに対するアクセス要求が想定されるアプリケーションプログラムの有する証明書のデータ（例えば、CN=aaa…，CN=bbb…）が格納されている。なお、Subject領域１５２ｄに格納されている「＊」は、アクセスを要求したアプリケーションプログラムの有する証明書のデータが、上記例示した証明書のデータ以外のデータであることを示す。

【００３７】

また、証明書種別領域１５２ｅは、Subject領域１５２ｄに格納されている証明書の種別を示すデータ（例えば、「＊」、「証明書１」、「証明書１，２，３，－」）が格納されている。なお、証明書種別領域１５２ｅに格納されている「＊」は、対応する証明書が、電話帳データベース１５１に格納されている全ての電話帳データに対するアクセスが可能な種別の証明書であることを示す。また、「－」は、アクセスを要求したアプリケーションプログラムが何れの証明書ももたないことを示す。

【００３８】

更に、アクセス可能情報領域１５２ｆは、対応する種別の証明書によってアクセス可能な情報（例えば、「全ての電話帳データ」、「グループＢに属する全ての電話帳データ」、「グループＢの電話番号」）が格納されている。これにより、携帯端末１０は、アクセスを要求したアプリケーションプログラムの有する証明書の種別に応じて、当該アプリケーションプログラムからのアクセスが可能な電話帳データを適宜選択できる。

【００３９】

図３に戻り、デジタル署名１５２ｂは、電話帳管理アプリケーション１５２の正当性を保証すると共にその出所を明示するために、第三者である認証機関によって発行及び付加された電子署名である。漏洩防止の観点から好適には、デジタル署名１５２ｂは暗号化されている。

公開鍵証明書１５２ｃは、ＩＴＵ-Ｔによって規定されている所定の仕様（例えば、X.509準拠の仕様）で定義された周知の公開鍵証明書である。

【００４０】

更に、記憶装置１５には、電話帳データ等のデータを表示装置１４に表示するためのアプリケーションプログラム（以下、「表示用アプリケーション１５３」と記す。）が格納されている。以下、図５を参照して、表示用アプリケーション１５３について説明する。図５に示す様に、表示用アプリケーション１５３は、デジタル署名１５３ａ及び公開鍵証明書１５３ｂを有する。

【００４１】

デジタル署名１５３ａは、表示用アプリケーション１５３の正当性を保証すると共にその出所を明示するために、第三者である認証機関によって発行及び付加された電子署名であ

る。漏洩防止の観点から好適には、デジタル署名１５３ａは暗号化されている。

【００４２】

公開鍵証明書１５３ｂは、ＩＴＵ-Ｔによって規定されている所定の仕様（例えば、X.509準拠の仕様）のExtension（拡張領域）１５３ｃを有する。Extension１５３ｃには、上述した電話帳管理アプリケーション１５２の有するアクセスリスト１５２ａと照合される権利情報１５３ｄが記録されている。

【００４３】

再び図１に戻り、記憶装置１５には、後述する指紋読取装置１７を実行制御するための指紋認証アプリケーション１５４が格納されている。この指紋認証アプリケーション１５４は、高い機密性を確保して改竄や悪用を困難にするために、耐タンパーソフトウェア化が施されている。

【００４４】

また、身体情報格納手段としての指紋認証アプリケーション１５４には、指紋認証アプリケーション１５４の使用者登録をした本人（通常は携帯端末１０の所有者）の指紋の特徴点が、指紋情報として事前に登録されている。指紋情報とは、本人確認を行うために手指の指紋の画像から抽出された特徴点のデータである。指紋認証アプリケーション１５４は、後述の指紋読取装置１７から出力されたユーザの指紋情報と、本人の指紋情報とを比較照合し、その結果に基づいてユーザと本人との同一性を判定する。これにより、電話帳データに対するアクセス要求（例えば、表示要求、電話発信要求）を指示したユーザの本人確認が行われる。

【００４５】

無線通信装置１６は、基地局Ｂとの無線通信の制御を行う。無線通信の制御には、電話帳データベース１５１から読み出された電話番号への電話発信を含む。詳細には、無線通信装置１６は、信号の変調及び復調を行う変復調部（図示せず）と、信号の符号化及び復号化を行う符復号化部（図示せず）とを有する回路であり、アンテナＡを備える。アンテナＡは、携帯端末１０の筐体上部に伸縮可能に設けられ、基地局Ｂとの間で電波の送受信を行う。

【００４６】

指紋読取装置１７は、読取部と抽出部とから構成される。指紋読取装置１７は、記憶装置１５から読み出された指紋認証アプリケーション１５４に従って、読取部によって読み取られた、ユーザの手指の指紋の画像から特徴点を抽出し、ユーザの指紋情報として指紋認証アプリケーション１５４に出力する。

【００４７】

音声処理装置１８は、変換器、増幅器等により構成され、マイクＭ及びスピーカＳを備える。音声処理装置１８は、通話時に、制御装置１１から入力される音声データを変換器でアナログ信号に変換し、増幅器を介してスピーカＳから放音する。また、音声処理装置１８は、通話時に、マイクＭから入力される音声信号を変換器によりデジタル信号に変換し、制御装置１１に出力する。

【００４８】

次に、本発明に係る携帯端末１０の動作について説明し、併せて、本発明に係るアクセス制御方法について説明する。以下に示す各工程は、図１に示した記憶装置１５に格納されている各種プログラムが、制御装置１１によって実行されることにより実現する。

【００４９】

図６は、携帯端末１０によって実行されるアクセス制御処理の流れを示すフローチャートである。動作説明の前提として、電話帳管理アプリケーション１５２と指紋認証アプリケーション１５４とは所与の秘密鍵（図示せず）を予め共有しているものとする。

【００５０】

まず、電話帳管理アプリケーション１５２に対してアクセス要求が有ると、表示用アプリケーション１５３から指紋認証アプリケーション１５４にユーザ認証要求が出力される（Ｓ１）。上記アクセス要求は、表示用アプリケーション１５３からのアクセス要求である

が、表示用アプリケーション１５３から制御装置１１を経由したアクセス要求は勿論、ユーザが入力装置１２を介して指示したアクセス要求をも含む。

【００５１】

Ｓ１で出力されたユーザ認証要求が指紋認証アプリケーション１５４に入力される（Ｓ２）と、指紋認証アプリケーション１５４は、指紋読取装置１７により携帯端末１０のユーザの指紋の読取りを開始する。読み取られた指紋の画像からは、所定の条件を満たす特徴点が抽出され、ユーザの指紋情報として取得される（Ｓ３）。

【００５２】

Ｓ４では、指紋認証アプリケーション１５４に事前に登録されている本人の指紋情報と、Ｓ３で取得されたユーザの指紋情報とが比較照合され、各指紋情報の同一性が判定される。当該照合の結果、各指紋情報が同一であるものと判定されると、乱数（以下、「Challenge」と記す。）の生成要求が、指紋認証アプリケーション１５４から電話帳管理アプリケーション１５２に出力される（Ｓ５）。出力されたChallenge生成要求は、電話帳管理アプリケーション１５２に入力される（Ｓ６）。

【００５３】

一方、Ｓ４における照合の結果、各指紋情報が同一でないものと判定されると、指紋認証アプリケーション１５４から表示用アプリケーション１５３に対して、メッセージが出力される（Ｓ７）。このメッセージは、ユーザ認証に失敗しアクセス要求が拒否された旨を携帯端末１０のユーザに通知するデータである。

【００５４】

続いて、電話帳管理アプリケーション１５２によってChallengeが生成され、指紋認証アプリケーション１５４に出力される（Ｓ８）。Ｓ８で出力されたChallengeは、指紋認証アプリケーション１５４に入力される（Ｓ９）。

【００５５】

続いて、指紋認証アプリケーション１５４によって、予め電話帳管理アプリケーション１５２と共有している秘密鍵と、所定の一方向関数（例えば、Keyed Hash等）とを用いてChallengeを計算した結果（以下、「Response」と記す。）が生成される。生成されたResponseは、本人確認が正常に完了したことを示すユーザ認証成功通知と共に表示用アプリケーション１５３に出力される（Ｓ１０）。

【００５６】

Ｓ１０で出力された上記ユーザ認証成功通知とResponseとは、表示用アプリケーション１５３に入力される（Ｓ１１）。これに伴い、表示用アプリケーション１５３から電話帳管理アプリケーション１５２に向けて、電話帳管理アプリケーション１５２に対するアクセス権認証要求が出力される。アクセス権認証要求は、表示用アプリケーション１５３から読み出されたデジタル署名１５３ａ及び公開鍵証明書１５３ｂと、上記Responseと共に出力される（Ｓ１２）。

【００５７】

次いで、Ｓ１２で出力されたアクセス権認証要求が、デジタル署名１５３ａ及び公開鍵証明書１５３ｂ並びにResponseと共に、電話帳管理アプリケーション１５２に入力される（Ｓ１３）と、電話帳管理アプリケーション１５２によってResponseの検証が開始される（図７に移りＳ１４）。Responseの検証は、電話帳管理アプリケーション１５２が指紋認証アプリケーション１５４と予め共有している上述の秘密鍵を参照して行われる。

【００５８】

Ｓ１４の検証の結果、Responseが正当であるもの、すなわち電話帳管理アプリケーション１５２が生成したChallengeに基づいて生成されたものと判定されると、次に電話帳管理アプリケーション１５２によってデジタル署名１５３ａの検証が行われる（Ｓ１５）。一方、Ｓ１４における検証の結果、Responseが正当でないものと判定されると、電話帳管理アプリケーション１５２から表示用アプリケーション１５３に対して、メッセージが出力される（Ｓ１６）。このメッセージは、アプリケーションプログラム認証に失敗しアクセス要求が拒否された旨をユーザに通知するものである。

【００５９】
また、Ｓ１５における検証の結果、デジタル署名１５３ａが正当であるものと判定されると、電話帳管理アプリケーション１５２によって、Ｓ１３で入力された公開鍵証明書１５３ｂと、アクセスリスト１５２ａのSubject領域１５２ｄに格納されている証明書との比較照合が行われる（Ｓ１７）。一方、Ｓ１５の検証の結果、デジタル署名１５３ａが正当でないものと判定されると、Ｓ１６の処理と同様に、アクセス要求が拒否された旨を示すメッセージがユーザに通知される（Ｓ１８）。
【００６０】
更に、Ｓ１７における照合の結果、公開鍵証明書１５３ｂがSubject領域１５２ｄに格納されている何れかの証明書と一致した場合、電話帳管理アプリケーション１５２によって、アクセス権の確認が正常に完了したことを示すアクセス権認証成功通知が、デジタル署名１５２ｂ及び公開鍵証明書１５２ｃと共に、表示用アプリケーション１５３に出力される（Ｓ１９）。
【００６１】
一方、Ｓ１７の照合の結果、公開鍵証明書１５３ｂがアクセスリスト１５２ａのSubject領域１５２ｄに格納されている何れの証明書とも一致しない場合には、Ｓ２０に示す様に、アクセス要求が拒否された旨を示すメッセージが表示用アプリケーション１５３に出力される。
【００６２】
Ｓ１９で出力された上記アクセス権認証成功通知、デジタル署名１５２ｂ、及び公開鍵証明書１５２ｃが入力される（Ｓ２１）と、表示用アプリケーション１５３によって、デジタル署名１５２ｂ及び公開鍵証明書１５２ｃの検証が行われる（Ｓ２２）。当該検証の結果、デジタル署名１５２ｂが存在し、かつ、公開鍵証明書１５２ｃが正当であるものと判定されると、表示用アプリケーション１５３によって、電話帳管理アプリケーション１５２にアクセス要求が出力される（Ｓ２３）。
【００６３】
Ｓ２３で出力されたアクセス要求が電話帳管理アプリケーション１５２に入力される（Ｓ２４）と、電話帳管理アプリケーション１５２によって、アクセスを要求された電話帳データの中から選択されたアクセス可能な情報を読み出す要求が、電話帳データベース１５１に対して出力される（Ｓ２５）。アクセス可能な情報の選択は、アクセス可能情報領域１５２ｆに格納されているデータを参照して行われる。
【００６４】
例えば、公開鍵証明書１５３ｂがアプリケーションＢの有する証明書と同一のデータである場合、対応するアクセス可能な情報は「グループＢに属する全ての電話帳データ」である。したがって、電話帳データベース１５１（図２参照）に格納されているデータの内、グループ名格納領域１５１ｅ内の"Ｂ"に対応する全てのデータ、すなわち氏名"△△次郎"及び"××三郎"の氏名、フリガナ、電話番号、及びメールアドレスを読み出す要求が出力される。
【００６５】
Ｓ２５で出力されたアクセス可能情報の読出し要求が、電話帳データベース１５１に入力される（Ｓ２６）と、Ｓ２５で選択された電話帳データ（アクセス可能情報）が、表示対象データとして電話帳データベース１５１から読み出される。次いで、読み出された電話帳データは、表示用アプリケーション１５３に出力される（Ｓ２７）。
【００６６】
そして、Ｓ２７で電話帳データベース１５１から出力された電話帳データは、表示用アプリケーション１５３に入力され、表示用アプリケーション１５３によって携帯端末１０の表示装置１４に表示される（Ｓ２８）。なお、電話帳データに電話番号が含まれる場合には、無線通信装置１６によって、当該電話番号への電話発信が行われるものとしてもよい。更に、電話帳データにメールアドレスが含まれる場合には、無線通信装置１６によって、当該メールアドレス宛に電子メールが発信されるものとしてもよい。

【００６７】
以上説明した様に、本発明に係る携帯端末１０は、電話帳データ格納手段としての電話帳データベース１５１と、要求取得手段、検証手段、及び出力手段としての制御装置１１とを備える。要求取得手段は、電話帳データベース１５１に格納されている電話帳データを管理する電話帳管理アプリケーション１５２に対する表示用アプリケーション１５３からのアクセス権認証要求を、表示用アプリケーション１５３の有するデジタル署名１５３ａ及び公開鍵証明書１５３ｂ（アプリケーション認証情報に対応）と共に取得する。検証手段は、アクセス権認証要求に応じてアプリケーション認証情報の正当性を判定する。出力手段は、アプリケーション認証情報が正当であると判定された場合にアクセス権認証要求を許可し、電話帳データに対するアクセス要求に応じて、表示用アプリケーション１５３に対して電話帳データを出力する。
【００６８】
すなわち、携帯端末１０は、正当なデジタル署名及び公開鍵証明書を有するアプリケーションプログラムからのアクセス権認証要求を許可し、正当なアプリケーション認証情報を有さないアプリケーションプログラムからのアクセス権認証要求を拒否する。そして、携帯端末１０は、アクセス権認証要求が許可されたアプリケーションプログラムからの電話帳データに対するアクセス要求を許可する。これにより、携帯端末１０において、高いセキュリティを維持しつつ、アプリケーションプログラムからの電話帳データに対するアクセスが可能となる。
【００６９】
具体的には、電話帳管理アプリケーション１５２にアクセスリスト１５２ａをもたせることで、電話帳データ単位でアクセス権を設定した場合と同様のアクセス制御（排他制御を含む）が可能となる。また、表示用アプリケーション１５３にデジタル署名１５３ａ及び公開鍵証明書１５３ｂをもたせることで、アプリケーションプログラム単位でアクセス権を設定した場合と同様のアクセス制御が可能となる。更に、指紋情報の同一性判定結果が反映されたResponseをユーザ認証に使用することで、ユーザ単位でアクセス権を設定した場合と同様のアクセス制御が可能となる。
【００７０】
電話帳データベース１５１は、データ単位、アプリケーション単位、ユーザ単位などの個別のアクセス制御が通常困難な非タンパー領域に存在するが、この様な非タンパー領域に存在する電話帳データに関しても、木目細やかなアクセス制御が可能となる。
【００７１】
なお、本実施形態における記述内容は、本発明に係る携帯端末の好適な一例であり、これに限定されるものではない。以下、図９を参照して、本実施形態の変形態様である携帯端末１０の記憶装置１５に格納された表示用アプリケーション１５３について説明する。図９に示す様に、表示用アプリケーション１５３は、デジタル署名１５３ａ及び公開鍵証明書１５３ｂの他に、属性証明書１５３ｅを新たに有する。
【００７２】
デジタル署名１５３ａ及び公開鍵証明書１５３ｂは、図５を参照して説明したデジタル署名１５３ａ及び公開鍵証明書１５３ｂと同様であるので、同一の構成部分には同一の符号を付すと共にその説明は省略する。属性証明書１５３ｅは、公開鍵証明書１５３ｂの発行者とは異なる認証機関によって発行され、Extension１５３ｃと同様にＩＴＵ‐Ｔによって規定されている所定の仕様（例えば、X.509準拠の仕様）で定義されている周知の属性証明書である。属性証明書１５３ｅには、公開鍵証明書１５３ｂを参照可能な情報が記載されている。
【００７３】
携帯端末１０は、証明書とアクセスリストとの照合処理（図７のＳ１７）の実行に際して、属性証明書１５３ｅの有する権利情報１５３ｆを参照する。権利情報がExtension１５３ｃに記述されている場合には、公開鍵証明書１５３ｂの有効期間内は権利情報を変更できない。このため、権利情報の記述内容を変更する為には、公開鍵証明書を再発行する手

続きが必要になる。これに対して、属性証明書１５３ｅは、公開鍵証明書１５３ｂとは独立に有効期間を設定できるので、記述されている権利情報の変更が容易である。

【００７４】

また、携帯端末１０は携帯電話に限らず、ＰＨＳ（Personal Handyphone System）等、通信機能を有する電子機器であればよい。

【００７５】

最後に、本発明に係るアクセス制御技術を実現するためのプログラム、及び当該プログラムを記録したコンピュータ読取り可能な記録媒体（以下、単に「記録媒体」と記す。）について説明する。記録媒体とは、汎用コンピュータ等のハードウェア資源に備えられている読取り装置に対して、プログラムの記述内容に応じて、磁気、光、電気等のエネルギーの変化状態を引き起こし、それに対応する信号の形式で、読取り装置にプログラムの記述内容を伝達できるものである。かかる記録媒体としては、例えば、ＵＩＭ（User Identity Module）等のＩＣカード、磁気ディスク、光ディスク、光磁気ディスクの様にコンピュータ（携帯端末、ＰＨＳ等を含む）に着脱可能に装着されるものの他に、コンピュータに固定的に内蔵されるＨＤ（Hard Disk）や一体に固着されたファームウェア等の不揮発性半導体メモリなどが該当する。

【００７６】

また、上記プログラムは、その一部若しくは全部を他の機器から通信回線等の伝送媒体を介して、本発明に係る携帯端末が備える無線通信装置により受信され、記録される構成にしてもよい。反対に、上記プログラムは、本発明に係る携帯端末から伝送媒体を介して他の機器に伝送され、インストールされる構成としてもよい。

【００７７】

【発明の効果】

本発明によれば、電話帳データを管理する電話帳管理アプリケーションプログラムに対する他のアプリケーションプログラムからのアクセス権認証要求と共に取得されたアプリケーション認証情報が正当であると判定された場合に、前記電話帳データに対するアクセス要求に応じて、前記アプリケーションプログラムに対して前記電話帳データが出力される。すなわち、携帯端末は、正当なアプリケーション認証情報を有するアプリケーションプログラムからのアクセス権認証要求を許可し、正当なアプリケーション認証情報を有さないアプリケーションプログラムからのアクセス権認証要求を拒否する。そして、携帯端末は、アクセス権認証要求が許可されたアプリケーションプログラムからの電話帳データに対するアクセス要求を許可する。これにより、携帯端末において、高いセキュリティを維持しつつ、アプリケーションプログラムからの電話帳データに対するアクセスが可能となる。

【図面の簡単な説明】

【図１】携帯端末の構成を示す図である。

【図２】電話帳データベースの構成例を示す図である。

【図３】電話帳管理アプリケーションの構成例を示す概念図である。

【図４】アクセスリストの構成を示す概念図である。

【図５】表示用アプリケーションの一の構成例を示す概念図である。

【図６】携帯端末によって実行されるアクセス制御処理の一部分を示すフローチャートである。

【図７】携帯端末によって実行されるアクセス制御処理の一部分を示すフローチャートである。

【図８】携帯端末によって実行されるアクセス制御処理の一部分を示すフローチャートである。

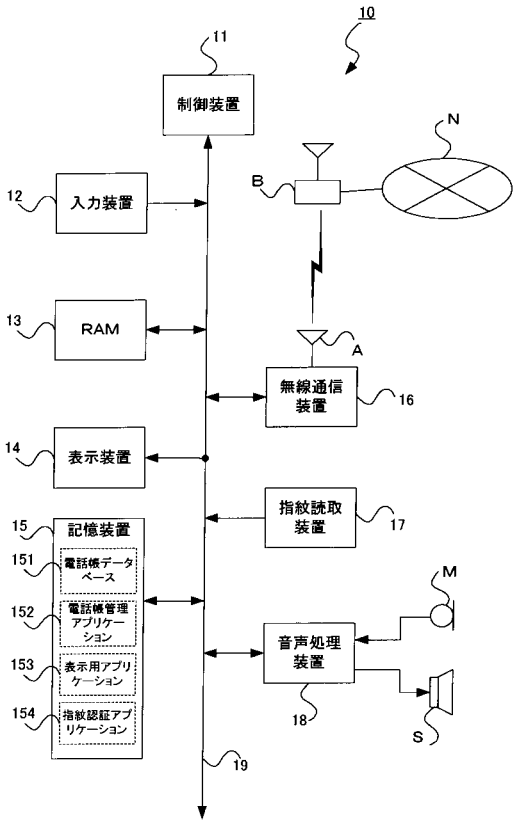
【図９】表示用アプリケーションの他の構成例を示す概念図である。

【符号の説明】

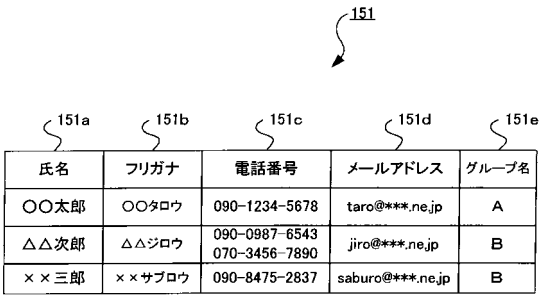
１０…携帯端末、１４…表示装置、１５…記憶装置、１５１…電話帳データベース、１５２…電話帳管理アプリケーション、１５２ａ…アクセスリスト、１５３…表示用アプリケ

ーション、１５３ａ…デジタル署名、１５３ｂ…公開鍵証明書、１５３ｅ…属性証明書、１５４…指紋認証アプリケーション、１６…無線通信装置、１７…指紋読取装置

【図１】



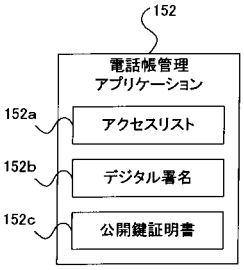
【図２】



151

151a 氏名	151b フリガナ	151c 電話番号	151d メールアドレス	151e グループ名
○○太郎	○○タロウ	090-1234-5678	taro@***.ne.jp	A
△△次郎	△△ジロウ	090-0987-6543 070-3456-7890	jiro@***.ne.jp	B
××三郎	××サブロウ	090-8475-2837	saburo@***.ne.jp	B

【図３】

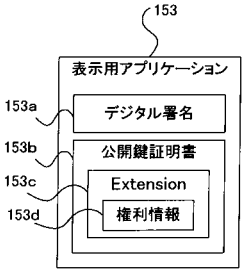


【図４】

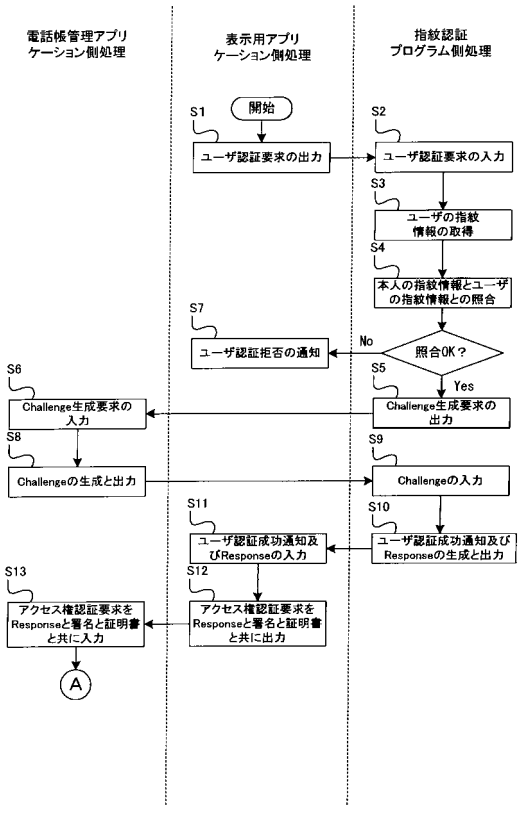
152a

152d Subject	152e 証明書の種別	152f アクセス可能な情報
アプリケーションAの有する証明書(CN=aaa, …)	*	全ての電話帳データ
アプリケーションBの有する証明書(CN=bbb, …)	証明書1	グループBに属する全ての電話帳データ
*	証明書1 証明書2 証明書3 —	グループBの電話番号 グループBの全電話帳データ メールアドレス 無し

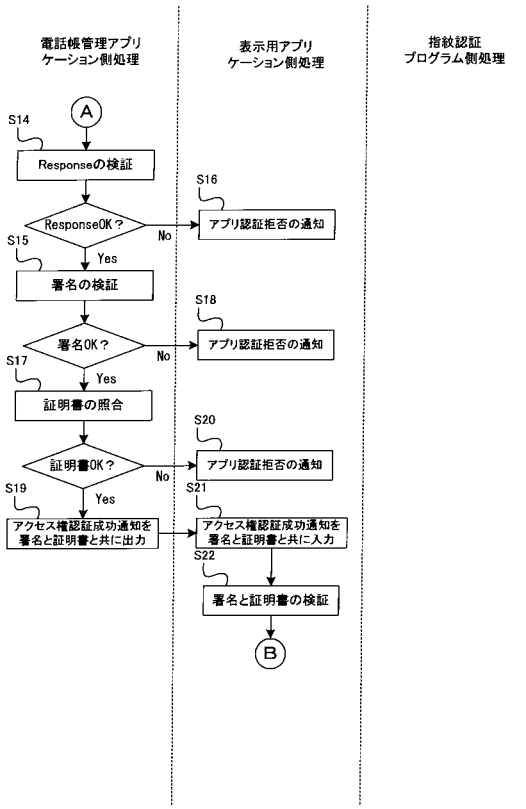
【図５】



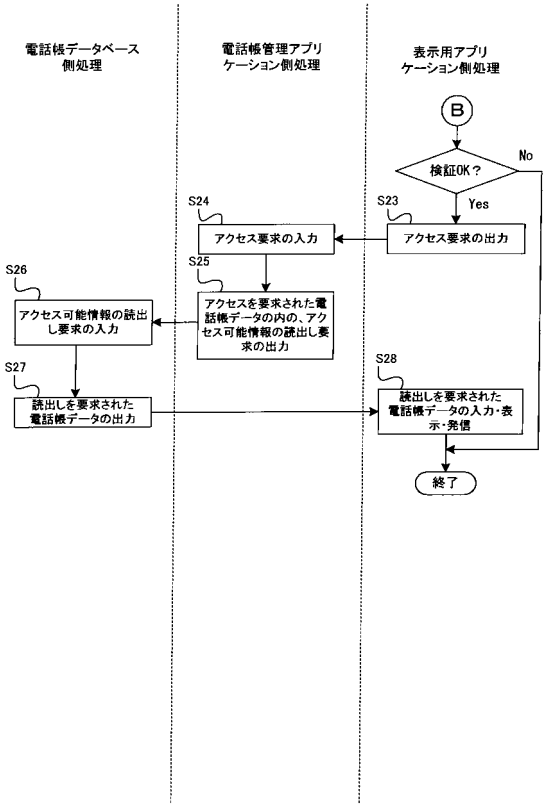
【図６】



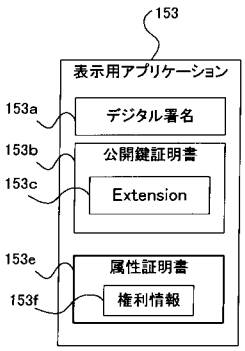
【図７】


電話帳管理アプリケーション側処理
表示用アプリケーション側処理
指紋認証プログラム側処理
A
S14
Responseの検証
S16
ResponseOK？
No
アプリ認証拒否の通知
S15
Yes
署名の検証
S18
署名OK？
No
アプリ認証拒否の通知
S17
Yes
証明書の照合
S20
証明書OK？
No
アプリ認証拒否の通知
S19
Yes
アクセス権認証成功通知を署名と証明書と共に出力
S21
アクセス権認証成功通知を署名と証明書と共に入力
S22
署名と証明書の検証
B

【図８】


電話帳データベース側処理
電話帳管理アプリケーション側処理
表示用アプリケーション側処理
B
検証OK？
No
Yes
S24
アクセス要求の入力
S23
アクセス要求の出力
S26
アクセス可能情報の読出し要求の入力
S25
アクセスを要求された電話帳データの内の、アクセス可能情報の読出し要求の出力
S27
読出しを要求された電話帳データの出力
S28
読出しを要求された電話帳データの入力・表示・発信
終了

【図９】


153
表示用アプリケーション
153a
デジタル署名
153b
公開鍵証明書
153c
Extension
153e
属性証明書
153f
権利情報

フロントページの続き

(51)Int.Cl. F I
H04L 9/00 673D
H04N 1/44

(72)発明者 青野 博
東京都千代田区永田町二丁目１１番１号 株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者 森 謙作
東京都千代田区永田町二丁目１１番１号 株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者 石井 一彦
東京都千代田区永田町二丁目１１番１号 株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者 本郷 節之
東京都千代田区永田町二丁目１１番１号 株式会社エヌ・ティ・ティ・ドコモ内

審査官 宮司 卓佳

(56)参考文献 特開平８－１８６３３（ＪＰ，Ａ）
特開２０００－２４２４９１（ＪＰ，Ａ）
国際公開第０２／２１２４３（WO，Ａ２）
特開昭６３－０７３３４８（ＪＰ，Ａ）
特開２０００－１５１７９８（ＪＰ，Ａ）
特開２００２－４１１７０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/24
G06F 12/00
G06F 21/20
H04L 9/32
H04N 1/44
H04M 1/00