(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2004-252584
(P2004-252584A)
(43)公開日　平成16年9月9日(2004.9.9)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 12/14	G06F	12/14	310K	5B017
G06F 12/00	G06F	12/00	537A	5B082

審査請求 有　請求項の数 7　OL　（全 14 頁）

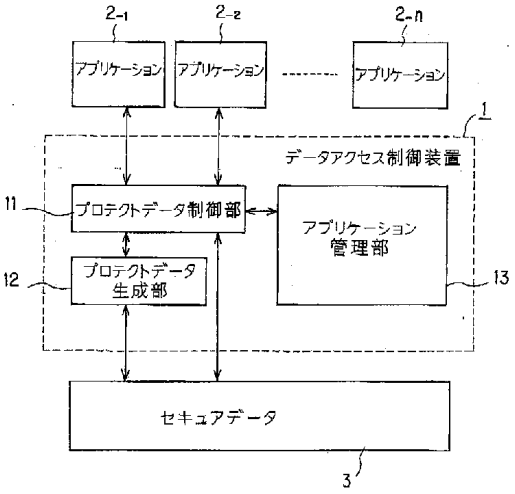
(21)出願番号　特願2003-40151(P2003-40151)
(22)出願日　平成15年2月18日(2003.2.18)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100071526
弁理士　平田　忠雄
(72)発明者　中山　義孝
東京都港区芝五丁目７番１号　日本電気株式会社内

Fターム(参考)　5B017 AA07　BA06　CA16
5B082 EA11

(54)【発明の名称】データアクセス制御装置

(57)【要約】
【課題】複数のアプリケーションの何れからアクセスされても、秘匿性を持つデータの安全性が高められるようにしたデータアクセス制御装置を提供する。
【解決手段】アクセス元のアプリケーションからセキュアデータ３の取得（又は参照、設定）要求があると、プロテクトデータ制御部１１はアプリケーション管理部１３からアプリケーション情報を取得し、この情報を基にアクセス元アプリケーションのアクセス権限の有無を検証する。アクセス権限有りのとき、プロテクトデータ制御部１１はプロテクトデータ生成部１２にアクセス制限情報を付与したプロテクトデータＰＤを生成させ、アクセス制限情報に基づく許容レベル内のデータについて、セキュアデータ３に対するアクセス元のアプリケーションによる取得、参照、又は設定を許可する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
アクセス制限の必要なセキュアデータに対し、アクセス権限を有するアプリケーションとアクセス権限を有しないアプリケーションとを含む複数のアプリケーションの何れから行われるアクセスを制御するデータアクセス制御装置において、
前記複数のアプリケーションについての情報を格納すると共に、前記複数のアプリケーションの何れかから前記セキュアデータがアクセスされたとき、そのアクセス元のアプリケーションのアプリケーション情報を検索するアプリケーション管理部と、
前記アクセス元のアプリケーションから前記セキュアデータの取得要求があったとき、アクセス制限情報を前記セキュアデータに付与してプロテクトデータを生成するプロテクトデータ生成部と、
前記アクセス元のアプリケーションが前記セキュアデータをアクセスした際、前記アプリケーション管理部から取得した前記アプリケーション情報に基づいて前記アクセス元のアプリケーションが前記セキュアデータをアクセスする権限の有無を検証し、アクセス権限有りを判定したとき、前記アクセス元のアプリケーションからの前記セキュアデータの取得、参照、又は設定を前記アクセス制限情報に基づいて許可するプロテクトデータ制御部を備えることを特徴とするデータアクセス制御装置。
【請求項２】
前記アプリケーション情報は、前記複数のアプリケーションの名称と、前記アプリケーションのそれぞれのアクセス許容度を示すアクセス権限とを含み、
前記アクセス制限情報は、前記セキュアデータの種別と、前記セキュアデータの提供レベルを示すセキュアレベルとを含むことを特徴とする請求項１記載のセキュアデータアクセス制御装置。
【請求項３】
前記アプリケーション管理部は、前記複数のアプリケーションのアプリケーション情報が格納されたアプリケーション属性データベースと、
指定されたアプリケーションのアプリケーション情報を前記アプリケーション属性データベースを検索して取得し、前記プロテクトデータ制御部に提供するアプリケーション情報参照手段を備えること特徴とする請求項１記載のデータアクセス制御装置。
【請求項４】
前記プロテクトデータ生成部は、前記プロテクトデータ制御部からの前記セキュアデータの提供要求に応じて前記セキュアデータを取得するセキュアデータ取得手段と、
前記セキュアデータにアクセス制限情報を付与して前記プロテクトデータを生成するプロテクトデータ生成手段を備えることを特徴とする請求項１記載のデータアクセス制御装置。
【請求項５】
前記プロテクトデータ生成手段は、前記アクセス制限情報として、データの種類を表すセキュアデータ種別、扱うデータの重要度を表すセキュアレベルの情報を含むことを特徴とする請求項４記載のデータアクセス制御装置。
【請求項６】
前記プロテクトデータ制御部は、前記アクセス元のアプリケーションのアプリケーション情報を取得し、前記アプリケーションの前記セキュアデータに対するアクセス権限の有無を検証するプロテクトデータ参照手段と、
前記プロテクトデータ参照手段が前記アクセス元のアプリケーションにアクセス権限が有ることを検証したとき、前記アプリケーションから前記セキュアデータに対する情報の設定を許可するプロテクトデータ設定手段と、
前記プロテクトデータ参照手段が前記アクセス元のアプリケーションにアクセス権限を有することを検証したとき、前記セキュアデータを前記アクセス元のアプリケーションに取得させるプロテクトデータ取得手段を備えることを特徴とする請求項１記載のデータアクセス制御装置。

【請求項７】
前記プロテクトデータ制御部は、前記プロテクトデータが前記アクセス元のアプリケーションから他のアプリケーションに引き渡されたとき、前記アクセス元及び前記引き渡し先のアプリケーションのそれぞれのアプリケーション情報を前記アプリケーション管理部から取得し、前記アクセス元のアプリケーションと前記引き渡し先のアプリケーションの両方に前記セキュアデータをアクセスする権限があるときにのみ前記プロテクトデータの引き渡し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アクセス制御装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、データアクセス制御装置に関し、特に、セキュリティレベルの異なる複数のアプリケーションが同時に実行可能な環境において、秘匿性を有するデータへのアクセスに対し、安全性が高められるようにするデータアクセス制御装置に関する。
【０００２】
【従来の技術】
ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）などの携帯端末装置においては、同時に複数のアプリケーションを実行可能なものがある。このような携帯端末装置において、秘匿性を有し、アクセス制限が必要となるデータ（以下、セキュアデータという）の１つがアドレス帳であり、各アプリケーションが無制限にセキュアデータを参照できてしまうことは、個人情報（特定情報）の流出につながり、好ましくない。
【０００３】
また、企業では、メーカーサイドが末端の消費者に至るまで、製品の流れを把握し、生産計画や販売計画に役立てたい場合があり、そのために物流システムが構築されている。この物流システムは、例えば、物流に関する情報を格納する開示データベース（ＤＢ）、この開示データＤＢに接続されたサーバにより構成され、或るレコードのアクセス許可会社欄にＡ社、Ｂ社、Ｃ社が記述されている場合、Ａ社、Ｂ社、Ｃ社の何れか又は３社を経由して検索要求が与えられたときにのみ前記レコード内の物流情報が要求元に送られるようにし、また、Ａ社、Ｂ社、Ｃ社以外のＩＤが含まれていた場合には検索条件を満たしていても物流情報が送信されないように制御し、第三者による不正アクセスを防止している（例えば、特許文献１参照）。
【０００４】
しかし、かかる構成では、第三者による不正アクセスの防止は可能であるが、複数のアプリケーションが存在し、その内のアクセス権限の無いアプリケーションからセキュアデータがアクセスされるような装置への適用は困難である。このようなケースに対応した構成について、次に図を示して説明する。
【０００５】
図７は、従来のデータアクセス制御装置を示す。
ここに示すデータアクセス制御装置１００は、ＰＤＡに代表される携帯端末装置１１０に搭載されている。データアクセス制御装置１００は、セキュアデータ制御部１０１と、このセキュアデータ制御部１０１に接続されたアプリケーション属性データ管理部１０２と、アプリケーション１０３，１０４と、及びセキュアデータ１０５とを備えている。セキュアデータ制御部１０１は、アプリケーションデータ側がセキュアデータ１０５（秘匿性を有するためにアクセス制限が必要なデータ）をアクセスする際、そのアクセスを制御する。アプリケーション属性データ管理部１０２は、〔表１〕のように、各アプリケーションの情報（アプリケーション名、アクセス権限など）を属性データとして格納している。
【０００６】
【表１】

アプリケーション名	アクセス権限
アプリケーションＡ	有り
アプリケーションＢ	無し

【０００７】
この制御装置１００は、同時に実行可能なのは１つのアプリケーションのみであり、アプリケーションデータ１０３又は１０４がセキュアデータ１０５を参照しようとするとき、アプリケーション属性データ管理部１０２の表１に示す属性データに基づいてセキュアデータ制御部１０１によりアクセス権限が検証され、検証できたときにはアプリケーションデータ１０３又は１０４からセキュアデータ１０５をアクセスすることができる。アプリケーション１０３，１０４は、ＪＡＶＡ（登録商標）アプリケーション、ｉアプリケーションなどである。

【０００８】
アクセス権限が〔表１〕のように設定されているとき、アプリケーション属性データ管理部１０２はアプリケーションデータ１０３にアクセス権限が有ることを検証する（図７のＡで示す丸印）。この検証を受けて、セキュアデータ制御部１０１は、アプリケーションデータ１０３によるセキュアデータ１０５へのアクセスを許可する。一方、アプリケーションデータ１０４は〔表１〕に示されるようにアクセス権限が無いので、セキュアデータ制御部１０１はアプリケーションデータ１０４によるセキュアデータ１０５へのアクセスを許可しない（図７の×印）。このようにして、アクセス権限を有するアプリケーションデータ１０３のみにセキュアデータ１０５に対するアクセスが許可されるので、セキュアデータ１０５が不用意に読み出され、インターネットなどに流出することがない。

【０００９】
【特許文献１】
特開２０００－２６７９５９号公報

【００１０】
【発明が解決しようとする課題】
しかし、従来のデータアクセス制御装置によると、１つのアプリケーションのみが実行可能で、同時に複数のアプリケーションを起動することができないように作られており、１つのアプリケーションのみが実行している限り、セキュリティは確立できる。しかし、携帯端末装置の機能が向上し、複数のアプリケーションを同時に実行できる環境が整った場合、アプリケーション１０３がアプリケーション１０４にセキュアなデータを渡すことにより（図７のＢの丸印）、アクセス権限のないアプリケーション１０４がセキュア１０５を参照することが可能になり、安全性が脅かされる。

【００１１】
本発明の目的は、複数のアプリケーションの何れからアクセスされても、秘匿性を持つデータの安全性が高められるようにしたデータアクセス制御装置を提供することにある。

【００１２】
【課題を解決するための手段】
本発明は、上記の目的を達成するため、アクセス制限の必要なセキュアデータに対し、アクセス権限を有するアプリケーションとアクセス権限を有しないアプリケーションとを含む複数のアプリケーションの何れから行われるアクセスを制御するデータアクセス制御装

置において、前記複数のアプリケーションについての情報を格納すると共に、前記複数のアプリケーションの何れかから前記セキュアデータがアクセスされたとき、そのアクセス元のアプリケーションのアプリケーション情報を検索するアプリケーション管理部と、前記アクセス元のアプリケーションから前記セキュアデータの取得要求があったとき、アクセス制限情報を前記セキュアデータに付与してプロテクトデータを生成するプロテクトデータ生成部と、前記アクセス元のアプリケーションが前記セキュアデータをアクセスした際、前記アプリケーション管理部から取得した前記アプリケーション情報に基づいて前記アクセス元のアプリケーションが前記セキュアデータをアクセスする権限の有無を検証し、アクセス権限有りを判定したとき、前記アクセス元のアプリケーションからの前記セキュアデータの取得、参照、又は設定を前記アクセス制限情報に基づいて許可するプロテクトデータ制御部を備えることを特徴とするデータアクセス制御装置を提供する。

【００１３】

この構成によれば、アプリケーションからセキュアデータに対するアクセスがあったとき、プロテクトデータ生成部で前記セキュアデータにアクセス制限情報を付加することによりプロテクトデータが生成され、アプリケーション管理部から提供されるアプリケーション情報とに基づいてセキュアデータをアクセスしたアプリケーションのアクセス権限有りが検証されたとき、セキュアデータのアクセス制限情報に応じたレベルのデータのみについて、取得、参照、又は設定が許可される。したがって、セキュリティレベルの異なる複数のアプリケーションが同時に実行可能な携帯端末装置の環境においても、アクセス権限の無いアプリケーションからセキュアデータをアクセスすることはできないので、セキュアデータの安全かつ容易な扱いが可能になる。

【００１４】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。

図１は、本発明の実施の形態に係るデータアクセス制御装置を示す。

データアクセス制御装置１は、プロテクトデータ制御部１１、プロテクトデータ生成部１２、及びアプリケーション管理部１３を備えて構成されており、携帯端末装置に内蔵される。更に、携帯端末装置はＲＡＭなどのメモリを内蔵しており、このメモリにアプリケーション２－１，２－２，・・・２－ｎ及びセキュアデータ３が格納されている。アプリケーション２－１～２－ｎはメーカー出荷時にインストールされたもの、ユーザーが作成したもの、ユーザーがインターネットなどからダウンロードしたものが含まれる。また、セキュアデータ３は、ユーザーが作成し、又は使用する過程で記録に残されたものが含まれる。

【００１５】

プロテクトデータ制御部１１は、アプリケーション２－１，２－２・・・２－ｎの何れかがセキュアデータ３にアクセスするための機能を有しており、アプリケーション２－１～２－ｎの何れかがセキュアデータ３の取得、参照、或いはセキュアデータ３に情報の設定を行う場合、プロテクトデータ制御部１１が提供する機能を通して行い、アプリケーションがセキュアデータ３にアクセスする権限を有するか否かを検証し、アクセス権限を有しない場合にはセキュアデータ３の取得、参照、設定を拒否する。検証は、セキュアデータ３に付加されている付与情報としてのアクセス制限情報（或いはセキュリティ情報）と、アプリケーション管理部１３が提供するアプリケーション情報とに基づいて判別する。〔表２〕はアプリケーション情報の一例を示し、〔表３〕はアクセス制限情報の一例を示す。

【００１６】

【表２】

アプリケーション名	アクセス権限
アプリケーション２－１	高
アプリケーション２－２	低
アプリケーション２－３	無
・ ・ ・	・ ・ ・

【００１７】
アプリケーション情報は、〔表２〕に示すように、アクセス権限が、アプリケーション２－１～２－ｎのそれぞれに対し、高、中、低、無の複数のレベルによりアクセス許容度が設定されている。このアプリケーション情報とアクセス制限情報の組み合わせにより、後述するようにアプリケーション２－１～２－ｎからセキュアデータ３（又はプロテクトデータＰＤ）の取得、参照、又は設定に対する安全性が保証される。
【００１８】
【表３】

アプリケーション種別	セキュアレベル	セキュアデータ
アドレス帳	高	神奈川県横浜市・・・
着信履歴	低	０４５（１２３）４５・・
・ ・ ・	・ ・ ・	・ ・ ・

【００１９】

アクセス制限情報は、〔表３〕に示すように、セキュアデータ種別（アドレス帳、着信履歴など）とセキュアレベル（高、中、低など）を含み、１つのセキュアデータ種別とセキュアレベルの組み合わせは、１つのセキュアデータ３に対応している。セキュアデータ３は、住所、電話番号などを含んでいる。

【００２０】

プロテクトデータ生成部１２は、アプリケーション２－１～２－ｎがセキュアデータ３を読み出す際に、セキュアデータ３に〔表３〕に示すアクセス制限情報を付与してプロテクトデータＰＤを生成する。すなわち、〔表３〕の全体がプロテクトデータＰＤを表している。

【００２１】

アプリケーション管理部１３は、プロテクトデータＰＤにアクセスするアプリケーション（２－１～２－ｎの何れか）についての情報をアプリケーション属性データベース内に保持しており、この情報はプロテクトデータ制御部１１のプロテクトデータ参照機能により参照することができる。アプリケーション管理部１３は、アプリケーション２－１～２－ｎがプロテクトデータＰＤにアクセスする際、そのアプリケーションにセキュアデータ３へのアクセス権が有るか否かを検証するために必要な情報をプロテクトデータ制御部１１に提供する。

【００２２】

例えば、アプリケーション２－１がアクセス権限を有し、このアプリケーション２－１がセキュアデータ３をアクセスする要求をプロテクトデータ制御部１１に行うと、プロテクトデータ制御部１１はアプリケーション管理部１３にアプリケーション２－１のアプリケーション情報の提供を要求する。アプリケーション管理部１３はアプリケーション２－１に関するアプリケーション情報を検索し、検索結果をプロテクトデータ制御部１１に提供する。プロテクトデータ制御部１１は、〔表２〕に示すアプリケーション２－１のアクセス権限「高」を参照し、アクセス権限が有ることを判定する。

【００２３】

プロテクトデータ制御部１１は、アクセス権限「高」の判定結果から、プロテクトデータ生成部１２に対してセキュアデータ３の取得を要求する。プロテクトデータ生成部１２はセキュアデータ３を読み出し、このセキュアデータ３に〔表３〕に示すアクセス制限情報を付与してプロテクトデータＰＤを生成した後、このプロテクトデータＰＤをプロテクトデータ制御部１１に送る。

【００２４】

プロテクトデータ制御部１１は、アクセス権限が「高」のレベルであることから、アクセス制限情報が「高」のレベルにあるものを抽出する。〔表３〕で「高」のセキュアレベルにあるものは「アドレス帳」であるので、セキュアデータ３の内、「アドレス帳」に対応するデータのみをアプリケーション２－１に対して、取得、参照、又は設定のいずれか、要求時の１つを許可する。なお、アクセス元のアプリケーションのアクセス権限が「低」のレベルであった場合、〔表３〕のセキュアレベルが「低」に対応するセキュアデータ種別及びセキュアデータ内容がアクセス元のアプリケーションに提供され、「高」や「低」のレベルのセキュアデータ３が提供されることは無い。したがって、セキュアデータ３の安全性が高められる。

【００２５】

このように、セキュアデータ３に対してアクセス制限情報を付与したデータ（＝プロテクトデータ）を生成し、セキュアデータ３そのものにアクセス制限情報を持たせることにより、セキュアデータ３がどのようなケースでアクセスされようとも、アクセス権限のないアプリケーションに対しては取得、参照、及び設定を制限することが可能になる。

【００２６】

図２は、セキュアデータ３内のアドレス帳をアプリケーションが参照する場合のアクセス状況を示す。

セキュアデータ３は、着信履歴３ａ、アドレス帳３ｂ、及び、その他のプライベート情報

３ｃを備えている。ここで、アプリケーションは２－１，２－２の２つとし、アプリケーション２－１にアクセス権限があり、アプリケーション２－２にはアクセス権限が無いものとする。

【００２７】

アプリケーション２－１，２－２からセキュアデータ３のアドレス帳３ｂにアクセスが行われたとすると、データアクセス制御装置１はアプリケーション２－１に対してはアドレス帳３ｂの情報を提供するが、アプリケーション２－２に対してはアドレス帳３ｂの情報を提供しない。更に、アドレス帳３ｂの情報をアプリケーション２－１がアプリケーション２－２に受け渡そうとした場合、データアクセス制御装置１が情報の引き渡しを行うために必要な機能を提供し、この機能を使用する時点でアプリケーション２－１と２－２の間のアドレス帳３ｂの情報の引き渡しを禁止する。

【００２８】

図３は、図１に示したデータアクセス制御装置１の詳細構成を示す。

プロテクトデータ制御部１１は、プロテクトデータ参照機能１１ａ（プロテクトデータ参照手段）、プロテクトデータ設定機能１１ｂ（プロテクトデータ設定手段）、プロテクトデータ取得機能１１ｃ（プロテクトデータ取得手段）、及びアプリケーション情報取得機能１１ｄ（アプリケーション情報取得手段）を備えて構成されている。プロテクトデータ制御部１１は、アプリケーション２－１～２－ｎがセキュアデータ３をアクセスする際、アプリケーション２－１～２－ｎのアクセス権限の検証、セキュアデータ３の取得依頼の受け付け、及びセキュアデータ３の設定依頼の受け付けを処理する。

【００２９】

プロテクトデータ参照機能１１ａは、アプリケーション情報取得機能１１ｄを使用してセキュアデータ３への参照を試みるアプリケーション（２－１～２－ｎの何れか）のアプリケーション情報１３ｃ（表２に示す内容）を取得し、アクセス元のアプリケーションがアクセス権限（参照権限）を有するか否かを検証する。検証の結果、参照権限有りが判定された場合、プロテクトデータＰＤを保持するセキュアデータ３は、プロテクトデータ制御部１１が提供するインタフェース機能を介して、アクセス制限情報のセキュアレベルに応じた情報の参照をアクセス元のアプリケーションに許可する。

【００３０】

また、プロテクトデータＰＤそのものを他のアプリケーションに受け渡す場合（図７のＢのケース）、引き渡し先のアプリケーション情報も取得し、その引き渡し先のアプリケーションにセキュアデータ３を参照する権限が有るか否かを検証する。そして、引き渡し元のアプリケーションと引き渡し先のアプリケーションの両方にセキュアデータ３を参照する権限がある場合にのみ、プロテクトデータＰＤの引き渡しを行う。

【００３１】

プロテクトデータ設定機能１１ｂは、アプリケーション情報取得機能１１ｄを使用してセキュアデータ３への設定を試みるアプリケーションの情報を取得し、そのアプリケーションがセキュアデータ３へのアクセス権限を有するか否かを検証する。検証の結果、アクセス権限（設定権限）があると判定された場合、アプリケーションが使用したプロテクトデータ制御部１１の提供するインタフェース機能を介してセキュアデータ３に対してアクセス制限情報のセキュアレベルに応じた情報の設定を実行する。

【００３２】

セキュアデータ取得機能１１ｃは、アプリケーション情報取得機能１１ｄを使用してセキュアデータ３から取得を試みるアプリケーション（＝アクセス元）の情報を取得し、そのアプリケーションがセキュアデータ３へのアクセス権を有するか否かを検証する。検証の結果、アクセス権限（取得権限）有りが判定された場合、アプリケーションが使用したプロテクトデータ制御部１１の提供するインタフェース機能を介してセキュアデータ３からアクセス制限情報のセキュアレベルに応じた情報の取得を実行する。

【００３３】

プロテクトデータ生成部１２は、プロテクトデータ生成機能１２ａ（プロテクトデータ生

成手段）、セキュアデータ取得機能１２ｂ（セキュアデータ取得手段）を持ち、プロテクトデータ制御部１１からセキュアデータ３の提供を依頼された際、セキュアデータ取得機能１２ｂによりセキュアデータ３を取得する。その時、プロテクトデータ生成部１２は、プロテクトデータ生成機能１２ａを使用してセキュアデータ３にアクセス制限情報（表３の内容）を付与したうえで提供する。

【００３４】

アプリケーション管理部１３は、アプリケーション情報参照機能１３ａとアプリケーション属性データベース１３ｂとを備え、セキュアデータ３をアクセスしようとするアプリケーション２－１（アクセス元）のアプリケーション情報をプロテクトデータ制御部１１のセキュアデータ参照機能１１ａに提供する。

【００３５】

次に、図３の構成によるデータアクセス制御装置１の動作について、図４～図６を参照して説明する。図４～図６においては、ステップをＳで表している。

図４は、アプリケーションがプロテクトデータＰＤを取得するための処理を示す。以下においては、アクセス元はアプリケーション２－１であるとする。

【００３６】

アプリケーション２－１がセキュアデータ３の取得を行う際、プロテクトデータ制御部１１は、プロテクトデータ取得機能１１ｃを使用してプロテクトデータ生成部１２にセキュアデータ３の取得を依頼する（Ｓ４０１）。次に、プロテクトデータ制御部１１が持つアプリケーション情報取得機能１１ｄを使用してセキュアデータ３の取得を依頼してきたアプリケーション２－１のアプリケーション情報１３ｃ（表２）をアプリケーション管理部１３から取得する（Ｓ４０２）。アプリケーション管理部１３は、プロテクトデータ制御部１１からアプリケーション情報１３ｃの提供を依頼されたとき（Ｓ４０２）、アプリケーション情報参照機能１３ａによりアプリケーション２－１のアプリケーション情報を検索し、アプリケーション情報１３ｃを取得する（Ｓ４１１）。アプリケーション管理部１３は、Ｓ４１１で取得したアプリケーション情報１３ｃをプロテクトデータ制御部１１に提供する（Ｓ４１２）。

【００３７】

次に、プロテクトデータ制御部１１は、アプリケーション管理部１３より提供されたアプリケーション情報１３ｃ内のアクセス権限情報に基づいてセキュアデータ３のアクセス権限の有無を判定する（Ｓ４０３）。具体的には、〔表２〕に示されるように、アプリケーション２－１のアクセス権限は「高」であるので、アクセス権限有りを判定する（Ｓ４０４）。なお、アプリケーションがアプリケーション２－１以外のときで、Ｓ４０４による検証結果がアクセス権限無しが判定されたときには、アクセス元のアプリケーション２－１にエラーコードを返送する（Ｓ４０５）。

【００３８】

Ｓ４０４のアクセス権限有りの判定結果に応じて、プロテクトデータ生成部１２はセキュアデータ取得機能１２ｂを使用してセキュアデータ３を取得し（Ｓ４２１）、更に、セキュアデータ取得機能１２ｂ及びプロテクトデータ生成機能１２ａを使用して、取得したセキュアデータ３に〔表３〕のアクセス制限情報を付与してプロテクトデータＰＤを生成し（Ｓ４２２）、これをプロテクトデータ制御部１１に提供する。プロテクトデータ制御部１１のプロテクトデータ取得機能１１ｃでは、アクセス制限情報を参照し、そのセキュアレベル「高」に対応するセキュアデータ３の内容を含むプロテクトデータＰＤをアプリケーション２－１に提供する（Ｓ４０６）。ここで、セキュアデータ３ではなく、プロテクトデータＰＤをアプリケーション２－１に提供する理由は、〔００３０〕のケースに対応させるにはアクセス制限情報が必要になるためである。

【００３９】

上記実施の形態によれば、以下に列挙する効果を得ることができる。

（１）セキュアデータ３にアクセス制限情報を付与してプロテクトデータを生成し、このプロテクトデータにアプリケーションがアクセスするため、アクセス権限のないアプリケ

ーションにプロテクトデータが渡されるの防止することができる。
（２）プロテクトデータ制御部１１及びプロテクトデータ生成部１２を介してのみプロテクトデータ内のセキュアデータ３にアクセス可能としているため、参照するセキュアデータ自身の情報（保持する情報の種類、フォーマット、その他）などの内容の解析を困難なものにすることができる。
（３）セキュアデータ３にアクセス制限情報を付与してプロテクトデータとして提供することにより、セキュリティの検証が行えるため、ユーザがセキュアデータ３を取り扱うことを容易にすることができる。
（４）データアクセス制御装置１がセキュアデータ３として扱う要素を判断するため、セキュリティを考慮しなければならないデータに関する保守性の向上が期待できる。

【００４０】
図５は、アプリケーションから提供されたプロテクトデータＰＤを参照する処理を示す。
アプリケーションがセキュアデータ３の参照を行う際、プロテクトデータ制御部１１が持つプロテクトデータ参照機能１１ａを使用してプロテクトデータＰＤの取得を依頼する（Ｓ５０１）。ついで、アプリケーション情報取得機能１１ｄを使用してアクセス元であるアプリケーション２－１のアプリケーション情報１３ａを取得する（Ｓ５０２）。更に、プロテクトデータ参照機能１１ａの内、データを他のアプリケーションに受け渡す機能を使用する場合、引き渡し先のアプリケーションのアプリケーション情報１３ａも取得する。

【００４１】
プロテクトデータ制御部１１からのアプリケーション情報１３ｃの提供依頼（Ｓ４０２）に対し、アプリケーション管理部１３は、アプリケーション管理部１３が持つアプリケーション情報参照機能１３ａを使用して、アプリケーション２－１のアプリケーション情報１３ａを検索し、アプリケーション属性データベース１３ｂから〔表２〕のアプリケーション情報１３ｃを取得する（Ｓ５１１）。アプリケーション管理部１３は、Ｓ５１１で取得したアプリケーション情報１３ｃをプロテクトデータ制御部１１に提供する（Ｓ５１２）。

【００４２】
プロテクトデータ制御部１１は、アプリケーション管理部１３から取得したアプリケーション情報１３ｃに含まれるアクセス権限情報を参照し、アプリケーション２－１のアクセス権限の有無を検証する（Ｓ５０３）。〔表２〕のアプリケーション情報１３ｃに示すように、アプリケーション２－１のアクセス権限は「高」であるので、アクセス権限有りが判定される（Ｓ５０４）。尚、アプリケーションがアプリケーション２－１以外のときで、アクセス権限無しが判定された場合には、アクセス元のアプリケーションにエラーコードを返送する（Ｓ５０５）。

【００４３】
Ｓ５０４でアクセス権限有りが判定されると、プロテクトデータ制御部１１のプロテクトデータ参照機能１１ａは、プロテクトデータＰＤに含まれているセキュアデータ３をアクセス制限情報に応じ（ここでは、〔表３〕に示すようにセキュアレベル「高」のセキュアデータ３の内容をアプリケーション２－１へ提供（参照のみ）する（Ｓ５０６）。その提供方法は、アプリケーションが使用するプロテクトデータ参照機能１１ａのインタフェースによって異なるものになる。

【００４４】
図６は、セキュアデータに対するアプリケーションからの設定処理を示す。
アプリケーションからセキュアデータ３の設定を行う場合、プロテクトデータ制御部１１は、プロテクトデータ設定機能１１ｂを使用してセキュアデータ３の設定要求を依頼する（Ｓ６０１）。また、アプリケーション情報取得機能１１ｄを使用し、アクセス元であるアプリケーション２－１に関する情報の取得をアプリケーション管理部１３に依頼する（Ｓ６０２）。

【００４５】

プロテクトデータ制御部１１からのアプリケーション情報の提供依頼（Ｓ６０２）に対し、アプリケーション管理部１３は、アプリケーション管理部１３が持つアプリケーション情報参照機能１３ａを使用して、アプリケーション２－１のアプリケーション情報を検索し、アプリケーション属性データベース１３ｂからアプリケーション情報１３ｃ（〔表２〕の内容）を取得する（Ｓ６１１）。アプリケーション管理部１３は、Ｓ６１１で取得したアプリケーション情報１３ｃをプロテクトデータ制御部１１に提供する（Ｓ６１２）。

【００４６】

プロテクトデータ制御部１１では、アプリケーション管理部１３から取得したアプリケーション情報１３ｃに含まれるアクセス権限情報に基づいて、そのアプリケーションがセキュアデータ３を設定できるか否かを検証する（Ｓ６０３）。アプリケーション２－１のアクセス権限は「高」であるので、アクセス権限有りが判定される（Ｓ６０４）。尚、アプリケーションがアプリケーション２－１以外のときで、アクセス権限無しが判定された場合には、アクセス元のアプリケーションにエラーコードを返送する（Ｓ６０５）。Ｓ６０４のアクセス権限有りの判定結果に基づいて、プロテクトデータ設定機能１１ｂはアクセス制限情報のセキュアレベル（ここでは「高」のセキュアレベル）に応じたセキュアデータ３の内容（アドレス帳のデータ）に対し、アプリケーション２－１による設定を許可する（Ｓ６０６）。

【００４７】

上記実施の形態においては、アプリケーション管理部１３が提供するアプリケーション情報１３ｃには、アクセス権限だけでなく、そのアプリケーションの属するグループ（システムアプリケーション、一般アプリケーションなど）、アクセス可能なデータ種別、実行される地域などの情報を追加することができる。これにより、プロテクトデータ制御部１１におけるセキュアデータ３のアクセス権限の検証を、より細かな条件で判定することが可能になる。このように、本実施の形態では、プロテクトデータＰＤのアクセス権限の検証を行う際に参照する条件をデータアクセス制御装置１１で保持することにより、より詳細な判断をすることが可能となり、さらにユーザはそのことに気を使うことなくセキュアデータ３を扱うことが可能になる。

【００４８】

また、上記実施の形態においては、携帯端末装置に適用した場合について説明したが、本発明は携帯端末装置に限定されるものではなく、アクセス権限を有するアプリケーションとアクセス権限を有しないアプリケーションを含む複数のアプリケーションの何れかからアクセス制限の必要なセキュアデータがアクセスされる際、前記セキュアデータをアクセス権限に応じて制御する必要のある電子機器に広く適用可能である。

【００４９】

【発明の効果】

以上より明らかなように、本発明のデータアクセス制御装置によれば、セキュアデータに対するアプリケーションからのアクセスの際、プロテクトデータ生成部によりアクセス制限情報をセキュアデータに付与してプロテクトデータを生成し、アプリケーション管理部から提供されるアプリケーション情報によりアクセス権限有りが判定されたとき、セキュアデータのアクセス制限情報に応じたレベルのデータのみについて、取得、参照、又は設定が許可される構成にしたので、セキュリティレベルの異なる複数のアプリケーションが同時に実行可能な携帯端末装置の環境においても、アクセス権限の無いアプリケーションにセキュアデータが制限無く渡されるのを防止できる。また、セキュアデータの安全が高められると共に解析を困難にし、プロテクトデータにすることでユーザによるセキュアデータの取り扱いを容易にすることができる。

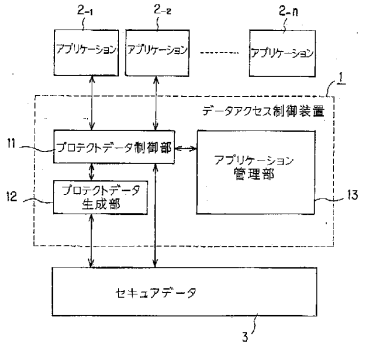
【図面の簡単な説明】

【図１】本発明の実施の形態に係るデータアクセス制御装置の構成を示すブロック図である。

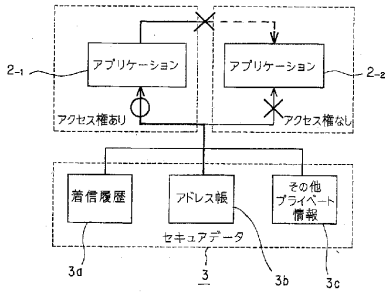
【図２】セキュアデータであるアドレス帳をアプリケーションが参照する場合のアクセス状況を示す説明図である。

【図３】図１に示したデータアクセス制御装置の詳細構成を示すブロック図である。
【図４】アプリケーションがプロテクトデータを取得するための処理を示すフローチャートである。
【図５】アプリケーションから提供されたプロテクトデータを参照する処理を示すフローチャートである。
【図６】セキュアデータに対するアプリケーションからの設定処理を示すフローチャートである。
【図７】従来のセキュアデータの制御装置を示すブロック図である。
【符号の説明】
１　データアクセス制御装置
２－１，２－２・・・２－ｎ　アプリケーション
３　セキュアデータ
３ａ　着信履歴
３ｂ　アドレス帳
３ｃ　プライベート情報
１１　プロテクトデータ制御部
１１ａ　セキュアデータ参照機能
１１ｂ　プロテクトデータ設定機能
１１ｃ　セキュアデータ取得機能
１１ｄ　アプリケーション情報取得機能
１２　プロテクトデータ生成部
１２ａ　プロテクトデータ生成機能
１２ｂ　セキュアデータ取得機能
１３　アプリケーション管理部
１３ａ　アプリケーション情報参照機能
１３ｂ　アプリケーション属性データベース
１００　制御装置
１０１　セキュアデータ制御部
１０２　アプリケーション属性データ管理部
１０３，１０４　アプリケーション
１０５　セキュアデータ

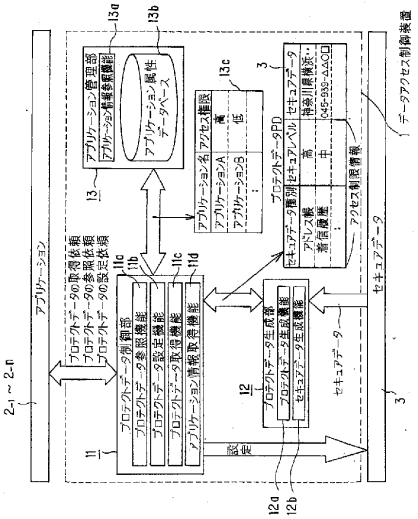
【図１】


2-1
2-2
2-n
アプリケーション
アプリケーション
アプリケーション
1
データアクセス制御装置
11
プロテクトデータ制御部
アプリケーション管理部
12
プロテクトデータ生成部
13
セキュアデータ
3

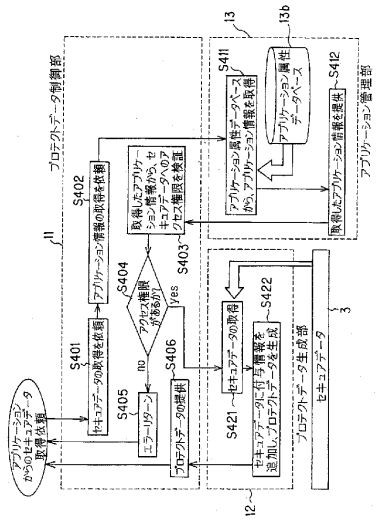
【図２】


2-1
アプリケーション
アプリケーション
2-2
アクセス権あり
アクセス権なし
着信履歴
アドレス帳
その他プライベート情報
セキュアデータ
3
3a
3b
3c

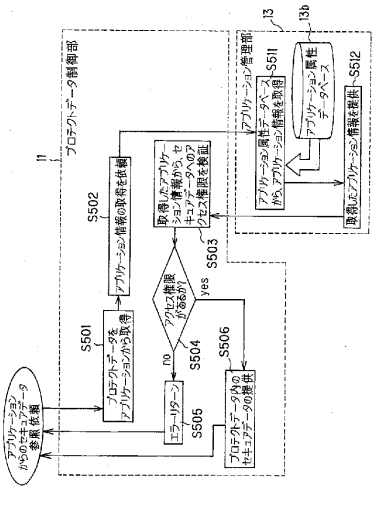
【図３】


13a
13b
アプリケーション管理部
アプリケーション情報参照機能
アプリケーション属性データベース
13
13c
アプリケーション名
アクセス権限
アプリケーションA
高
アプリケーションB
低
3
プロテクトデータPID
セキュアレベル
セキュアデータ
神奈川県横浜...
045-555-△△○○
アクセス制限情報
データアクセス制御装置
アプリケーション
11c
11b
11c
11d
プロテクトデータの取得依頼
プロテクトデータの参照依頼
プロテクトデータの設定依頼
プロテクトデータ制御部
プロテクトデータ参照機能
プロテクトデータ設定機能
プロテクトデータ取得機能
アプリケーション情報取得機能
2-1 ～ 2-n
11
12
プロテクトデータ生成部
プロテクトデータ生成機能
セキュアデータ生成機能
セキュアデータ
3
12a
12b

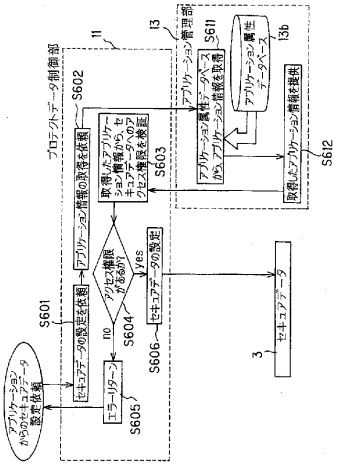
【図４】


プロテクトデータ制御部
11
13
13b
アプリケーション管理部
アプリケーション属性データベース
S411
S412
S401
S402
S403
S404
S405
S406
S421
S422
yes
no
アプリケーションからのセキュアデータ取得依頼
セキュアデータの取得を依頼
アプリケーション情報の取得を依頼
取得したアプリケーション情報から、セキュアデータへのアクセス権限を検証
アクセス権限があるか
エラーリターン
プロテクトデータの提供
セキュアデータに付与情報を追加したプロテクトデータを生成
プロテクトデータ生成部
セキュアデータ
3
12

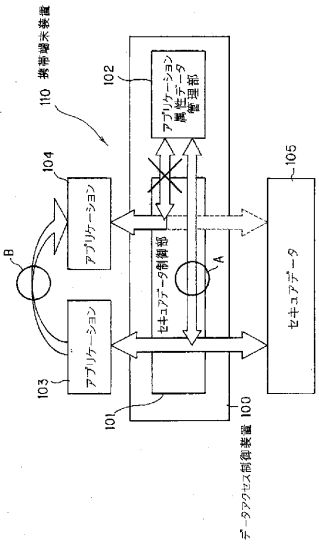
【図５】


プロテクトデータ制御部
11
13
13b
アプリケーション管理部
アプリケーション属性データベース
S511
S512
S501
S502
S503
S504
S505
S506
yes
no
アプリケーションからのセキュアデータ参照依頼
プロテクトデータをアプリケーションから取得
アプリケーション情報の取得を依頼
取得したアプリケーション情報から、セキュアデータへのアクセス権限を検証
アクセス権限があるか
エラーリターン
プロテクトデータ内のセキュアデータの提供

【図６】


プロテクトデータ制御部
11
アプリケーション管理部
13
アプリケーション属性データベース
13b
アプリケーション属性データベースから、アプリケーション情報を取得
S611
取得したアプリケーション情報を提供
S612
アプリケーションからのセキュアデータ設定依頼
セキュアデータの設定を依頼
S601
アプリケーション情報の取得を依頼
S602
取得したアプリケーション情報から、セキュアデータへのアクセス情報を検索
S603
アクセス権限があるか
S604
no
yes
エラーリターン
S605
セキュアデータの設定
S606
セキュアデータ
3

【図７】


携帯端末装置
110
アプリケーション
104
アプリケーション
103
セキュアデータ制御部
101
アプリケーション属性データ管理部
102
セキュアデータ
105
データアクセス制御装置 100
A
B