(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2007-202064
(P2007-202064A)
(43)公開日　平成19年8月9日(2007.8.9)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	673B	5J104
H04Q	7/38	(2006.01)	H04B	7/26	109S	5K027
H04B	7/26	(2006.01)	H04B	7/26	M	5K067
H04M	1/67	(2006.01)	H04M	1/67		5K201
H04M	1/00	(2006.01)	H04M	1/00	V	

審査請求 未請求　請求項の数 5　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願2006-21064(P2006-21064)
(22)出願日　平成18年1月30日(2006.1.30)

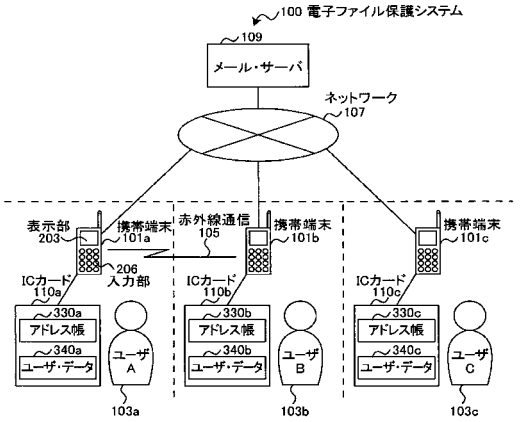
(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100096091
弁理士　井上　誠一
(72)発明者　大野　毅
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

Ｆターム(参考)　5J104 AA07 AA12 AA16 EA04 EA15
EA16 JA03 KA02 KA04 NA02
NA05 NA27 NA37 NA38 PA01
PA14
5K027 AA11 BB09 HH23 HH26 MM03

最終頁に続く

(54)【発明の名称】通信システム及び携帯端末

(57)【要約】
【課題】データの閲覧制限のできる通信システム及び携帯端末を提供する。
【解決手段】通信システム（電子ファイル保護システム）１００は、メール・サーバ１０９と、複数の携帯端末１０１ａ、１０１ｂ、１０１ｃ等がネットワーク１０７を介して接続されて構成される。携帯端末１０１ａ、１０１ｂ、１０１ｃは、それぞれユーザＡ１０３ａ、ユーザＢ１０３ｂ、ユーザＣ１０３ｃに所有される。
携帯端末１０１にはプラグイン型のＩＣカード１１０が搭載されており、アドレス帳３３０等のデータが保持される。
送受信する双方の携帯端末１０１を使用して個人情報データ３１０をやりとりする場合には、電話番号やメール・アドレ等の情報の他に電子証明書３１１が付加され、送信先の携帯端末１０１のアドレス帳３３０に、送信元ユーザの電子証明書３１１が保存される。
【選択図】図１



【特許請求の範囲】
【請求項１】
複数の携帯端末間で通信を行う通信システムであって、
第１の携帯端末は、
第１の携帯端末を特定する個人情報と、第１の携帯端末固有の鍵を含む認証情報とを、サーバを介さずに第２の携帯端末に対して通信する通信手段を有し、
第２の携帯端末は、
前記第１の携帯端末から送られる前記個人情報と前記認証情報を保持する保持手段を有し、
前記第１の携帯端末は、
データを前記鍵で暗号化して、サーバを介して前記第２の携帯端末に送信する第２の送信手段を有し、
前記第２の携帯端末は、
前記第１の携帯端末からサーバを介してデータが送られると、前記保持手段から前記第１の携帯端末に関する鍵を含む認証情報を抽出する手段と、前記データを前記鍵で復号する手段と、
を具備することを特徴とする通信システム。
【請求項２】
前記第１の携帯端末は、
前記データを生成する際に、生成者を特定する第２の認証情報を前記データに付加する手段を有し、
前記第２の認証情報が付加された前記データが、前記第２の携帯端末に送られ、
前記第２の携帯端末は、前記データの生成者と前記第２の携帯端末の所有者を比較し、一致しない場合、前記データの転送を禁止する手段を有することを特徴とする請求項１記載の通信システム。
【請求項３】
前記第１の携帯端末は、
前記データを生成する際に、コピー制限回数を前記データに付加する手段を有し、
前記コピー制限回数が付加された前記データが前記第２の携帯端末に送られ、
前記第２の携帯端末は、前記データを保存する際に前記コピー制限回数を「１」減らす手段を有することを特徴とする請求項１記載の通信システム。
【請求項４】
前記第１の通信手段は、赤外線通信であることを特徴とする請求項１記載の通信システム。
【請求項５】
第１の携帯端末と通信を行う第２の携帯端末であって、
第１の携帯端末から、第１の携帯端末を特定する個人情報と、第１の携帯端末固有の鍵を含む認証情報とを、サーバを介さずに第２の携帯端末に対して通信されると、
前記第１の携帯端末から送られる前記個人情報と前記認証情報を保持する保持手段と、
前記第１の携帯端末からデータを前記鍵で暗号化して、サーバを介して前記第２の携帯端末に送信されると、
前記第１の携帯端末から、サーバを介してデータが送られると、前記保持手段から前記第１の携帯端末に関する鍵を含む認証情報を抽出する手段と、
前記データを前記鍵で復号する手段と、
を具備することを特徴とする携帯端末。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信システム及び携帯端末に関するものである。
【背景技術】

【０００２】
昨今、デジタルカメラやカメラ付携帯電話の普及に伴い、個人で撮影した画像等の電子ファイルをネットワーク経由で送受信することが多くなっている。同時にネットワーク環境の拡大に伴い、画像の撮影者や被撮影者の意図に反して電子ファイルがネットワーク上に流出するといった問題点もある。
【０００３】
このように、ネットワーク上への電子ファイルの流出が行われることへの対策として、プロが作成したデジタルコンテンツのデータ保護や閲覧制限（コピーワンス等）は存在するが、一般のユーザが作成したデジタルコンテンツのデータ保護や閲覧制限の仕組みは整備されていない。
【０００４】
一方、電子ファイル、即ちデジタルカメラ等で撮影された画像や、その他のあらゆる種類のデジタルコンテンツを含む電子ファイルに対して個人情報を埋め込む技術はすでに存在している。また、このような電子ファイルを読み出す技術も存在している（例えば「特許文献１」参照。）。
【特許文献１】特開２００５－７１０５４号公報
【０００５】
しかしながら、個人情報を読み出し、電子ファイルの作成者が特定できるとしても、電子ファイルそのものがインターネット上に流出してしまった場合、不特定多数の第三者から当該ファイルを閲覧されてしまう危険性は依然として存在する。
【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明は、前述した問題点に鑑みてなされたもので、その目的とすることはデータの閲覧制限のできる通信システム及び携帯端末を提供することにある。
【課題を解決するための手段】
【０００７】
前述した目的を達成するために第１の発明は、複数の携帯端末間で通信を行う通信システムであって、第１の携帯端末は、第１の携帯端末を特定する個人情報と、第１の携帯端末固有の鍵を含む認証情報とを、サーバを介さずに第２の携帯端末に対して通信する通信手段を有し、第２の携帯端末は、前記第１の携帯端末から送られる前記個人情報と前記認証情報を保持する保持手段を有し、前記第１の携帯端末は、データを前記鍵で暗号化して、サーバを介して前記第２の携帯端末に送信する第２の送信手段を有し、前記第２の携帯端末は、前記第１の携帯端末からサーバを介してデータが送られると、前記保持手段から前記第１の携帯端末に関する鍵を含む認証情報を抽出する手段と、前記データを前記鍵で復号する手段と、を具備することを特徴とする通信システムである。
【０００８】
前記第１の携帯端末は、前記データを生成する際に、生成者を特定する第２の認証情報を前記データに付加する手段を有し、前記第２の認証情報が付加された前記データが、前記第２の携帯端末に送られ、前記第２の携帯端末は、前記データの生成者と前記第２の携帯端末の所有者を比較し、一致しない場合、前記データの転送を禁止する手段を有する。
【０００９】
前記第１の携帯端末は、前記データを生成する際に、コピー制限回数を前記データに付加する手段を有し、前記コピー制限回数が付加された前記データが前記第２の携帯端末に送られ、前記第２の携帯端末は、前記データを保存する際に前記コピー制限回数を「１」減らす手段を有する。
【００１０】
前記第１の送信手段は、赤外線通信である。
【００１１】
第２の発明は、第１の携帯端末と通信を行う第２の携帯端末であって、第１の携帯端末

から、第１の携帯端末を特定する個人情報と、第１の携帯端末固有の鍵を含む認証情報とを、サーバを介さずに第２の携帯端末に対して通信されると、前記第１の携帯端末から送られる前記個人情報と前記認証情報を保持する保持手段と、前記第１の携帯端末からデータを前記鍵で暗号化して、サーバを介して前記第２の携帯端末に送信されると、前記第１の携帯端末から、サーバを介してデータが送られると、前記保持手段から前記第１の携帯端末に関する鍵を含む認証情報を抽出する手段と、前記データを前記鍵で復号する手段と、を具備することを特徴とする携帯端末である。

【発明の効果】

【００１２】

本発明によれば、データの閲覧制限のできる通信システム及び携帯端末を提供することができる。

【発明を実施するための最良の形態】

【００１３】

以下添付図面に基づいて、本発明の実施形態に係る通信システム（電子ファイル保護システム）１００について詳細に説明する。

【００１４】

図１は、電子ファイル保護システム１００の構成を示すブロック図である。図１に示すように、電子ファイル保護システム１００は、メール・サーバ１０９と、複数の携帯端末１０１ａ、１０１ｂ、１０１ｃ等がネットワーク１０７を介して接続されて構成される。携帯端末１０１ａ、１０１ｂ、１０１ｃは、それぞれユーザＡ１０３ａ、ユーザＢ１０３ｂ、ユーザＣ１０３ｃに所有される。

【００１５】

携帯端末１０１は、携帯電話（特に第３世代３ＧＰＰ）、アナログＴＶやデジタルＴＶの受信機器であるセットトップボックス（ＳＴＢ）、車載案内装置やＧＰＳ等の位置信号受発信機器である車載端末等である。

【００１６】

携帯端末１０１は、それぞれ、表示部２０３や入力部２０６等を有し、ユーザ１０３によって操作される。また携帯端末１０１にはプラグイン型のＩＣカード１１０が搭載されており、アドレス帳３３０等のデータが保持される。

【００１７】

ネットワーク１０７は、インターネット、ローカルエリアネットワーク（ＬＡＮ）等のネットワークであり、有線、無線を問わない。

【００１８】

メール・サーバ１０９は、サーバコンピュータ等であり、携帯端末１０１におけるメールの送受信を管理するサーバである。メール・サーバ１０９は、携帯端末１０１のサービスプロバイダが有する。

【００１９】

次に、図２を参照しながら、携帯端末１０１のハードウェア構成を説明する。図２は、携帯端末１０１のハードウェア構成図である。本発明に関連した構成要素のみを図示しており、送受話部等の図示は省略してある。

【００２０】

携帯端末１０１は、制御部２０１、記憶部２０２、表示部２０３、カメラ２０４、送受信部２０５、入力部２０６、マイク２０７、記録媒体Ｉ／Ｆ部２０８、暗号化・復号回路２０９、赤外線通信部２１０、アンテナ２１１等が、バス２１２を介して接続され、構成される。

【００２１】

制御部２０１は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ　）、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ　）、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等で構成される。

【００２２】

ＣＰＵは、記憶部２０２、ＲＯＭ、暗号化・復号回路２０９、ＩＣカード２２０やメモリカード２３０等の記録媒体等に格納されるプログラムをＲＡＭ上のワークメモリ領域に呼び出して実行し、システムバスを介して接続された各装置を駆動制御し、携帯端末１０１が行う各種処理を実現する。

ＲＯＭは、不揮発性メモリであり、コンピュータのブートプログラムやＢＩＯＳ等のプログラム、データ等を恒久的に保持している。

ＲＡＭは、揮発性メモリであり、記憶部２０２、ＲＯＭ、記録媒体等からロードしたプログラム、データ等を一時的に保持するとともに、制御部２０１が各種処理を行う為に使用するワークエリアを備える。

【００２３】

記憶部２０２は、制御部２０１が実行するプログラム、プログラム実行に必要なデータ、ＯＳ（オペレーティングシステム）等が格納される。

これらの各プログラムコードは、制御部２０１により必要に応じて読み出されてＲＡＭに移され、ＣＰＵに読み出されて各種の手段として実行される。

【００２４】

表示部２０３は、ＣＲＴモニタ、液晶パネル等のディスプレイ装置である。カメラ２０４は、画像データ、映像データ等を取得する。

【００２５】

送受信部２０５は、携帯端末１０１とネットワーク１０７間の通信を媒介する通信インタフェースであり、ネットワーク１０７を介して、メール・サーバ１０９と、携帯端末１０１間の通信制御を行う。送受信部２０５は、アンテナ２１１と接続される。

【００２６】

入力部２０６は、データの入力を行い、例えば、キーボード、テンキー等の入力装置である。マイク２０７は、音声データを取得する。

【００２７】

記録媒体Ｉ／Ｆ部２０８は、記録媒体へのデータの授受を行う。記録媒体は、ＩＣカード２２０、メモリカード２３０等である。

暗号化・復号回路２０９は、暗号化したデータに対する復号、及びデータの暗号化を行う。

【００２８】

赤外線通信部２１０は、赤外線による通信を行う。赤外線通信部２１０では、受信した赤外線を制御信号に変換する等の処理を行う。赤外線による通信は、メール・サーバ１０９を介さずに行われる。赤外線のほかに、電磁波や超音波等を用いた他の近距離無線通信方式を用いてもよい。

【００２９】

図３は、ＩＣカード１１０を示す図である。

図３に示すように、ＩＣカード１１０は、接触型ＩＣカードであり、ＩＣモジュール端子とリーダ／ライタの端子が接触することで電力供給や通信を行う。

ＩＣカード１１０は、ＣＰＵ３０１、ＲＯＭ３０３、ＲＡＭ３０５、ＥＥＰＲＯＭ３０７（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）等を有する。

【００３０】

ＲＯＭ３０３は、プログラム領域３０９を有し、アプリケーションの追加・削除が可能なプラットフォーム型のＯＳ３６０を格納する。またアプリケーション・プログラムの一部を格納する。電子ファイル保護システム１００における保護アプリケーション・プログラム３５０等が格納される。

【００３１】

ＥＥＰＲＯＭ３０７は、ユーザ領域を有し、プラットフォーム型ＯＳに対応したアプリケーションを複数搭載可能とする。例えば、アプリケーションとして、契約端末の認証を行う認証アプリケーション・プログラム、正当使用者／端末を特定するための認証情報（

例えば、契約者識別情報等）を搭載、格納する。また、アドレス帳３３０や、ユーザ・データ３４０等が格納される。
尚、ＩＣカード１１０は、この構成に限られるものではない。
【００３２】
次に、図４を参照しながら、携帯端末１０１における個人情報データ３１０について説明を行う。図４は個人情報データ３１０の一態様を示す図である。個人情報データ３１０は携帯端末１０１のＩＣカード１１０中に保存され、ユーザ１０３間で赤外線通信１０５を介して送受信されるデータである。個人情報データ３１０は、他のユーザ１０３の携帯端末１０１より受信し、赤外線通信部２１０経由で入力され、アドレス帳３３０に保存される。
【００３３】
電子証明書３１１は、各携帯端末１０１に固有の識別情報である。暗号鍵３１４及びＩＭＳＩ（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｍｏｂｉｌｅ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ：加入者識別番号）３１５を含む。暗号鍵３１４は、携帯端末１０１を所有するユーザ１０３が、自分の作成した電子ファイルを暗号化するときに使用するデータである。即ち、ユーザＡ１０３ａが、自分が撮影した画像データを携帯端末１０１中で暗号化して、ユーザＢ１０３ｂに送信する。このとき、暗号鍵３１４が使用される。ユーザＢ１０３ｂは、自分の携帯端末１０１ｂで受信した電子ファイルを同じ暗号鍵３１４で復号して初めて参照が可能となる。ＩＭＳＩ３１５は加入者識別番号であり、携帯端末
の各ユーザに固有の番号である。即ち、ＩＭＳＩ３１５は携帯端末１０１のＩＣカード１１０毎に設定される番号である。
【００３４】
電子ファイル保護システム１００において、電子証明書３１１は、電子ファイルの作成者、すなわち画像データを撮影、取得した携帯端末１０１等を特定する際にも使用される。
【００３５】
電話番号３１２は、携帯端末１０１の電話番号、メール・アドレス３１３は、携帯端末１０１のメール・アドレスである。個人情報データ３１０には、電子証明書３１１、電話番号３１２、メール・アドレス３１３の他、ユーザ１０３の氏名等任意のデータを含むことができる。
【００３６】
次に、図５を参照しながら、送信データ３２０について説明を行う。図５は送信データ３２０の一態様を示す図である。
送信データ３２０は、画像データ等のデータを送信する際の送信内容を示す。
送信データ３２０は、アドレス帳３３０とユーザ・データ３４０を参照して作成され、メール・サーバ１０９を経由し、他の携帯端末１０１に送信される。
送信先電子証明書３２１は、ユーザ・データ３４０を送信しようとする相手の携帯端末１０１の電子証明書である。アドレス帳３３０より、ユーザ６０１に対応する電子証明書６０２が参照されて付加される。
【００３７】
電子証明書３２２は図４の電子証明書３１１と同様のもので、ユーザ・データ３４０に含まれるものである。即ち、送信しようとするデータ部３２５の作成者、すなわち画像データの撮影者等の保有する識別情報である。
コピー回数３２３は、送信しようとするデータ部３２５に対して許可されたコピーの回数である。
特定ユーザ３２４は、送信しようとするデータ部３２５の閲覧を許可されたユーザのＩＤである。特定ユーザ３２４には、ＩＭＳＩを使用してもよいし、メール・アドレスや電話番号を使用してもよい。
【００３８】
データ部３２５は送信しようとする画像や映像などのデジタルコンテンツのデータであ

る。送信時には、送信する携帯端末１０１で暗号化を行う。

【００３９】

次に、図６を参照しながら、アドレス帳３３０について説明を行う。図６は、アドレス帳３３０の一態様を示す図である。アドレス帳３３０は、携帯端末１０１のＩＣカード１１０に保持される。アドレス帳３３０のデータの取得は、ユーザ１０３の入力、又は赤外線通信による他の携帯端末１０１からのデータの受信によって行われる。

【００４０】

ユーザ６０１は、送信先となるユーザ１０３を識別する情報である。電子証明書６０２はユーザ６０１に対応する携帯端末１０１の暗号鍵、ＩＭＳＩ等の情報である。電子証明書６０２がアドレス帳に３３０に含まれる場合は、赤外線通信１０５によって個人情報データ３１０を取得したユーザ１０３に限られる。

電話番号６０３はユーザ６０１に対応する電話番号、メール・アドレス６０４はユーザ６０１に対応するメール・アドレスである。

尚、アドレス帳３３０に含まれるデータ項目は、この構成に限られるものではない。

【００４１】

次に、図７を参照しながら、ユーザ・データ３４０について説明を行う。図７はユーザ・データ３４０の一態様を示す図である。ユーザ・データ３４０は、携帯端末１０１のＩＣカード１１０に保持される。ユーザ・データ３４０の取得は、カメラ２０４で撮影を行ったときや、他の携帯端末１０１から送信されたデータを受信したときに行われる。

【００４２】

ＩＤ７０１は、データを識別するＩＤである。属性７０２はデータ部３２５のデータの種類を示す。コピー回数３２３及び特定ユーザ３２４は、図５のコピー回数３２３、特定ユーザ３２４と同様のものである。電子証明書３２２は該当データの作成者を識別する情報である。図５の電子証明書３２２と同様のものである。データ部３２５は、画像データ、音楽データ、映像データ等のデジタルコンテンツそのものを示し、図５のデータ部３２５と同様のものである。

【００４３】

次に、図８を参照しながら、携帯端末１０１ａより、携帯端末１０１ｂに個人情報データ３１０を送信する際の動作について説明を行う。図８は携帯端末１０１ａ、携帯端末１０１ｂの動作を示すフローチャートである。

例えば、ユーザＡ１０３ａと、ユーザＢ１０３ｂが互いの携帯端末１０１を使用して、電話番号等の情報を交換するときの動作である。

【００４４】

最初に、携帯端末１０１ａの制御部２０１は、メール・アドレス等の個人情報のデータに携帯端末１０１ａの電子証明書３１１を付加し、個人情報データ３１０を生成し、赤外線通信部２１０を介して、携帯端末１０１ｂに送信する（ステップ８０１）。

【００４５】

携帯端末１０１ｂの制御部２０１は携帯端末１０１ａから受信した個人情報データ３１０をアドレス帳３３０ｂに書き込む（ステップ８０２）。

【００４６】

以上のようにして、送受信する双方の携帯端末１０１を使用して個人情報データ３１０をやりとりする場合には、電話番号３１２やメール・アドレス３１３等の情報の他に電子証明書３１１が付加され、送信先の携帯端末１０１のアドレス帳３３０に、電子証明書３１１が保存される。

【００４７】

具体的に、ユーザＡ１０３ａとユーザＢ１０３ｂが知り合ってお互いにアドレスの交換を行う場合を例にとる。ユーザＡ１０３ａは、ユーザＢ１０３ｂに自分の携帯端末１０１ａに保存された自分のプロフィール、即ち、電話番号３１２やメール・アドレス３１３などの情報を赤外線通信１０５経由で送信するための操作を行う。すると、携帯端末１０１ａの制御部２０１が電子証明書３１１を付加して個人情報データ３１０として送信する。

【００４８】
ユーザＢ１０１ｂも同様に、携帯端末１０１ｂに保存されたプロフィールを携帯端末１０１ｂに送るための操作を行う。相互に送受信された個人情報データ３１０には、電子証明書３１１が含まれている。携帯端末１０１ａのアドレス帳３３０ａには、ユーザＢ１０３ｂの情報として、電話番号６０３、メール・アドレス６０４の他に電子証明書６０２が保存される。この電子証明書６０２は、携帯端末１０１ｂから送られる暗号化された電子ファイルを復号する際に用いられる。
【００４９】
同様に、ユーザＢ１０３ｂの携帯端末１０１ｂのアドレス帳３３０ｂには、ユーザＡ１０３ａの電子証明書６０２が保存される。前述と同様、この電子証明書６０２は、携帯端末１０１Ａから送られる暗号化された電子ファイルを復号する際に用いられる。
【００５０】
以上のように、実際に面識があって、直接個人情報データ３１０を受信した相手のユーザ１０３のみ、アドレス帳３３０に電子証明書６０２が保存される。
【００５１】
次に、図９を参照しながら、ユーザ・データ３４０を保存する際の動作について説明を行う。図９はデータ部３２５の取得から、ユーザ・データ３４０の保存における携帯端末１０１ａの動作を示すフローチャートである。
【００５２】
まず、携帯端末１０１ａの制御部２０１はデータ部３２５を取得する（ステップ９０１）。データ部３２５の取得は携帯端末１０１ａのカメラ２０４による撮影や、音楽作成ツールを用いた音楽データの入力等によって行われる。
【００５３】
データ部３２５を取得したユーザＡ１０３ａ、即ち携帯端末１０１ａの所有者はユーザ・データ３４０ａに取得したデータ部３２５を保存するための操作を行う。このときに、コピー回数や、送信先等、任意に制限項目を指定して保存する。この情報は入力部２０６より入力される。制御部２０１は、入力部２０６より受け取ったコピー回数３２３、特定ユーザ３２４等の入力項目、及び携帯端末１０１ａの電子証明書３３２を付加してＩＣカード１１０中のユーザ・データ３４０ａに書き込む（ステップ９０２）。
【００５４】
この他に、ユーザ・データ３４０に含まれるデータには、他の携帯端末１０１ら送信されてきたものや、公のウェブ・サイトからダウンロードしたものも含まれる。自分で作成したデータ以外は、自分以外の作成者の携帯端末１０１の電子証明書３２２が付加されている。また、電子証明書３２２を含まないものもある。
【００５５】
また、データ部３２５を取得したユーザＡ１０１ａ、即ち画像データの撮影者であれば、自分の携帯端末１０１ａに対するオペレーションによってのみ、ユーザ・データ３４０ａの内容を変更できるようにしてもよい。即ち、例えば撮影日以降の後日、特定ユーザ３２４を追加したり、コピー回数３２３を変更したりすることができるようなユーザ・インターフェースを設けることもできる。この場合、さらにユーザ・データ３４０の安全性を高めるためにパスワード機能を持たせて第三者が携帯端末１０１ａを用いて属性の変更を行わないようにしておいてもよい。
【００５６】
次に、図１０、図１１及び図１２を参照しながら、携帯端末１０１ａから携帯端末１０１ｂに対して、電子ファイルを送信する際の処理について説明を行う。図１０は、ユーザ・データ３４０ａの送信に伴う携帯端末１０１ａの動作を示す。
【００５７】
最初に、制御部２０１は、送信しようとするユーザ・データ３４０の電子証明書３２２を参照する（ステップ１００１）。電子証明書３２２は、ユーザ・データ３４０のデータ部３２５の作成者、例えば写真等の画像データであれば、撮影者等の情報である。次に、

電子証明書３２２が送信しようとする携帯端末１０１ａのものであるか検査を行う（ステップ１００２）。携帯端末１０１ａのＩＣカード１１０中にあるＩＭＳＩを参照し、電子証明書３２２のＩＭＳＩと照合し、一致するかどうかを調べる。即ち、送信しようとするユーザ・データ３４０は自分が作成したデータかどうかの検証を行う。

【００５８】

電子証明書３２２が携帯端末１０１ａのものでなければ（ステップ１００２のＮｏ）、制御部２０１は、エラーメッセージを出力して（ステップ１００３）、直ちに処理を終了する。これは、ユーザＡ１０３ａが作成した電子ファイル、例えばユーザＡ１０３ａが、携帯端末１０１のカメラ２０４を使用して撮影した画像データでなければ、送信ができないことを意味する。

【００５９】

電子証明書３２２が自分のもの、すなわち携帯端末１０１ａのものであれば（ステップ１００２のＹｅｓ）、次に、制御部２０１はユーザ・データ３４０ａのコピー回数３２３を参照する（ステップ１００４）。コピー回数３２３を検査することによって、許可されたコピー回数を超えてコピーが行われないようにする。コピー回数３２３が０であれば（ステップ１００５のＮｏ）、制御部２０１は、エラーメッセージを出力して（ステップ１００６）、直ちに処理を終了する。

【００６０】

コピー回数３２３が０より大きければ（ステップ１００５のＹｅｓ）、次に制御部２０１は、アドレス帳３３０ａの送信しようとする先のユーザ６０１と、ユーザ・データ３４０ａの特定ユーザ３２４を照合する（ステップ１００７）。照合のステップの中で、まず、制御部２０１は、ユーザＡ１０３ａが指定した送信先ユーザ６０１を取得する。次に送信しようとするユーザ・データ３４０ａの特定ユーザ３２４を取得し、比較する。特定ユーザ３２４に複数のユーザ１０３が指定されていた場合には、送信先のユーザ６０１がその中に含まれるものであるかを検査する。即ち、送信しようとする先のユーザ１０３が、ユーザ・データ３４０の保存時に設定した送信対象のユーザ１０３と一致するかどうかを検査する。

【００６１】

ユーザ６０１と特定ユーザ３２４が一致しなかった場合（ステップ１００８のＮｏ）、制御部２０１は、エラーメッセージを出力して（ステップ１００９）、直ちに処理を終了する。

【００６２】

ユーザ６０１と特定ユーザ３２４が一致した場合（ステップ１００８のＹｅｓ）、制御部２０１は、ユーザ・データ３４０のコピー回数３２３のカウントを１減らす（ステップ１０１０）。次に、制御部２０１は、送信処理を開始する（ステップ１０１１）。

【００６３】

尚、ステップ１００３、ステップ１００６、ステップ１００９のエラーメッセージは、携帯端末１０１の表示部２０３に表示される。

図１２は、エラーメッセージ１２０１の画面表示の一態様を示したものである。エラーメッセージ１２０１には、「送信できません」等の送信失敗を示すメッセージ及び送信失敗の理由１２０２が表示される。例えば、ステップ１００９に示すように、ユーザ・データ３４０を特定ユーザ３２４以外の携帯端末１０１に送信しようとした場合、図１２に示すように「このデータは第三者に転送できません」等の表示を行う。

【００６４】

図１０のステップ１００２，ステップ１００５及びステップ１００８の検査については、ユーザ・データ３４０の設定によって行われ、設定のないものについては行われない。例えば、コピー回数３２３の設定がなければ、ステップ１００４、ステップ１００５の処理は実行されない。

【００６５】

図１１は、送信処理（図１０のステップ１０１１）における、携帯端末１０１ａ及び携

帯端末１０１ｂの動作を示すフローチャートである。

【００６６】

まず、携帯端末１０１ａの制御部２０１は、アドレス帳３３０中の送信先の電子証明書６０２を、ユーザ・データ３４０に付加し、携帯端末１０１ａの電子証明書３２２の暗号鍵で暗号化して送信データ３２０とする（ステップ１１０１）。

【００６７】

次に、制御部２０１は、送信データ３２０を送信先ユーザＢ１０３ｂの携帯端末１０１ｂに送信する（ステップ１１０２）。

【００６８】

携帯端末１０１ｂの制御部２０１は、携帯端末１０１ａより送られた送信データ３２０を受信する（ステップ１１０３）。

【００６９】

携帯端末１０１ｂの制御部２０１は、アドレス帳３３０ｂを参照し、暗号鍵を用いて認証を行う（ステップ１１０４）。即ち、送信元のユーザＡ１０３ａのデータをアドレス帳３３０ｂ中から、当該データの電子証明書６０２を参照し、電子証明書中の暗号鍵の情報を読み取る。アドレス帳３３０ｂに含まれる電子証明書６０２の暗号鍵が、携帯端末１０１ａから送信されてきた送信データ３２０を復号できる暗号であるかの認証を行う。

【００７０】

暗号鍵による認証に失敗した場合（ステップ１１０５のＮｏ）、制御部２０１は、送信データ３２０の内容を無効にし（ステップ１１０６）、処理を終了する。即ち、予め電子証明書を交換した携帯端末１０１からの送信データ３２０のみ、復号して読み取ることができる。

【００７１】

暗号鍵による認証に成功した場合（ステップ１１０５のＹｅｓ）、制御部２０１は、携帯端末１０１ａからの送られた送信データ３２０を復号して、携帯端末１０１ｂのユーザ・データ３４０に保存する（ステップ１１０７）。

【００７２】

以上のように、送り手の携帯端末１０１ａでは、ユーザ・データ３４０の作成者の電子証明書３２２、コピー回数３２３、特定ユーザ３２４等を参照し、携帯端末１０１ｂに送信してもよいデータであるか否かを検査した後、送信データ３２０を作成し、携帯端末１０１ｂに送信する。受け手の携帯端末１０１ｂでは暗号認証を行い、認証が成功すれば携帯端末１０１ａからの送信データ３２０を参照することができる。

【００７３】

従って、画像データ等のデジタルコンテンツを含む電子ファイルの送信元と送信先のそれぞれの携帯端末１０１が互いに電子証明書を用いて個人情報を交換していなければ、電子ファイルの送受信の実行は制限される。これにより、第三者に対して自分の作成した電子ファイルを転送されることはなくなる。

【００７４】

また、電子ファイルの作成時、即ち画像を撮影して保存するときなどに、任意の閲覧制限を付加することができるので、電子ファイルの種類によって転送の制限やユーザの制限を変えることが可能である。

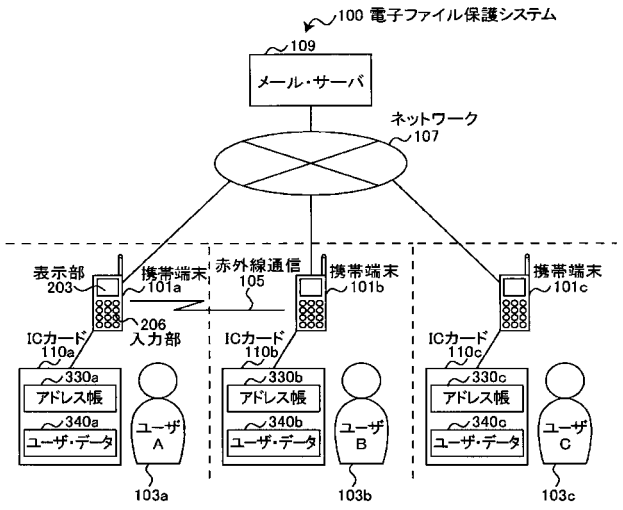
【００７５】

具体的には、ユーザＡ１０３ａから画像データを含む送信データ３２０を受信したユーザＢ１０３ｂは、その送信データ３２０を他のユーザ、例えばユーザＣに送信することに対し、制限を受ける。例えば、携帯端末１０１ｂのユーザ・データ３４０ｂに、携帯端末１０１ａから送信された画像データを保存したとする。撮影者はユーザＡ１０３ａ自身である。電子証明書３２２には、携帯端末１０１ａのＩＭＳＩ、暗号鍵が含まれる。仮に、ユーザＢ１０１ｂが、ユーザＣ１０１ｃに送信しようとした場合、当該ユーザ・データ３４０の電子証明書３２２はユーザＢ１０１ｂの携帯端末１０１ｂのものではないから、図１０のステップ１００２の処理でエラーとなる。

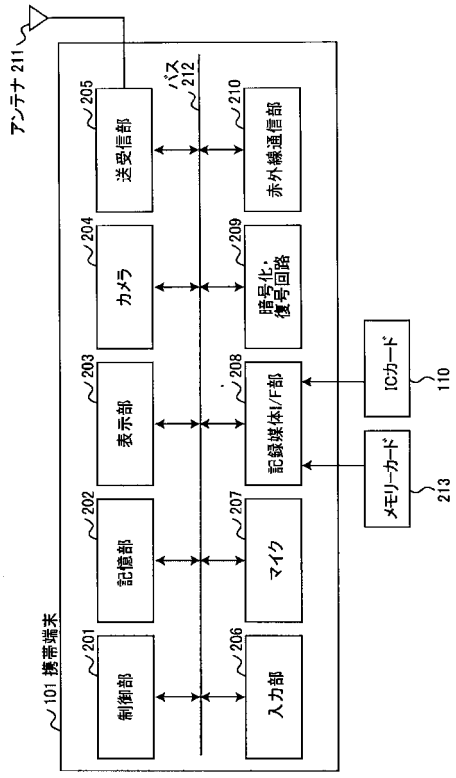
【００７６】
例えば、撮影者ではないユーザＢ１０３ｂが当該ユーザ・データ３４０を転送する許可を与えられていたとしても、暗号化することによって、携帯端末１０１ｂの電子証明書を持たない携帯端末１０１では閲覧ができない。このように、転送や閲覧に関して多重のチェックを行うことも可能である。
【００７７】
また、ユーザ・データ３４０のコピー回数３２３をカウンタとして使用することによって、コピーの回数を制限することができる。
例えば、ユーザＡ１０３ａは画像を撮影し、ユーザ・データ３４０にコピー回数３２３を指定して保存する。当該データを、ユーザＢ１０３ｂに送信する。最初のコピー回数３２３を「１」とした場合、図１０のステップ１０１１に示すように、送信時にコピー回数３２３は「１」減算され、「０」となる。次にユーザＡ１０３ａは、当該データを他のユーザ１０３に送信しようとすると、コピー回数３２３が０であるので、ステップ１００５でエラーとなる。
【００７８】
また、記録媒体経由やケーブル経由で携帯端末１０１以外の装置にデータをコピーする場合においても、同様にコピー回数３２３をカウンタとして用いることによって、無制限にユーザ・データ３４０がコピーされることを防ぐことができる。
【００７９】
以上、添付図面を参照しながら、本発明に係る通信システム等の好適な実施形態について説明したが、本発明はかかる例に限定されない。当業者であれば、本願で開示した技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。
【図面の簡単な説明】
【００８０】
【図１】電子ファイル保護システム１００の構成を示すブロック図
【図２】携帯端末１０１のハードウェア構成図
【図３】ＩＣカード１１０のデータ構造の一態様を示す図
【図４】個人情報データ３１０の一態様を示す図
【図５】送信データ３２０の一態様を示す図
【図６】アドレス帳３３０の一態様を示す図
【図７】ユーザ・データ３４０の一態様を示す図
【図８】個人情報データ３１０送信処理の動作を示すフローチャート
【図９】ユーザ・データ３４０書込み処理の動作を示すフローチャート
【図１０】ユーザ・データ３４０の送信前処理の動作を示すフローチャート
【図１１】送信データ３２０の送信処理の動作を示すフローチャート
【図１２】エラーメッセージの一態様を示す図
【符号の説明】
【００８１】
１００……電子ファイル保護システム
１０１……携帯端末
１０３……ユーザ
１１０……ＩＣカード
２０１……制御部
２０２……記憶部
２０３……表示部
２０４……カメラ
２０５……送受信部
２０６……入力部
２０７……マイク

２０８……記録媒体Ｉ／Ｆ部
２０９……暗号化復号回路
２１０……赤外線通信部
２１１……アンテナ
２１３……メモリカード

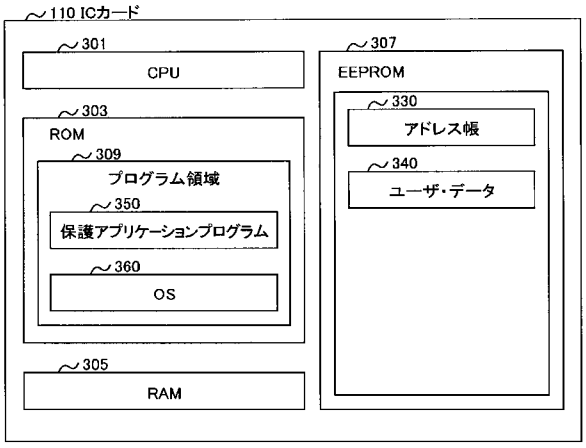
【図１】



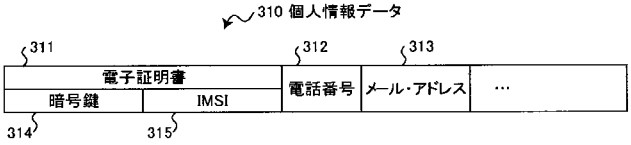
【図２】



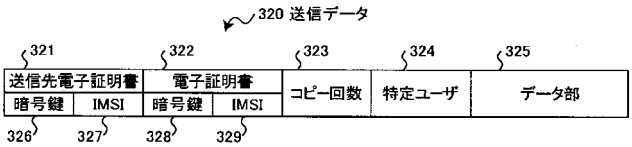
【図３】



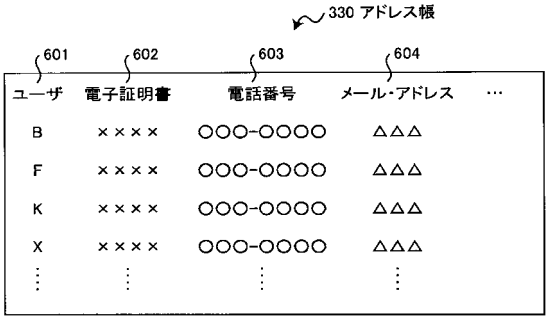
【図４】



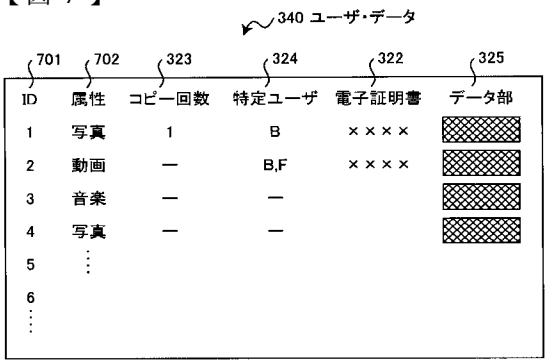
【図５】



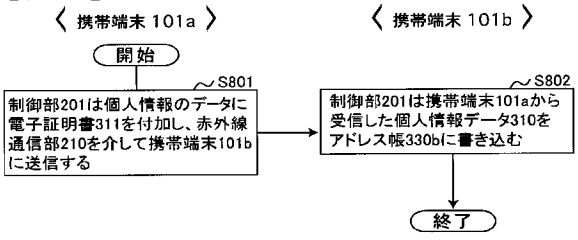
【図６】



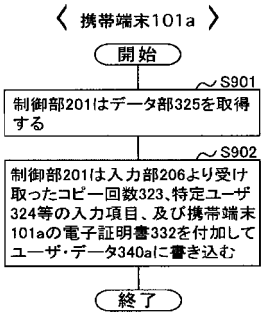
【図７】



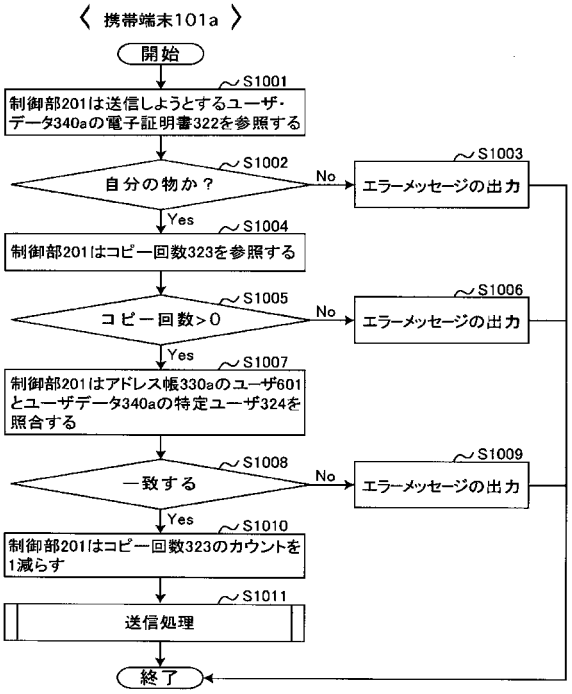
【図８】



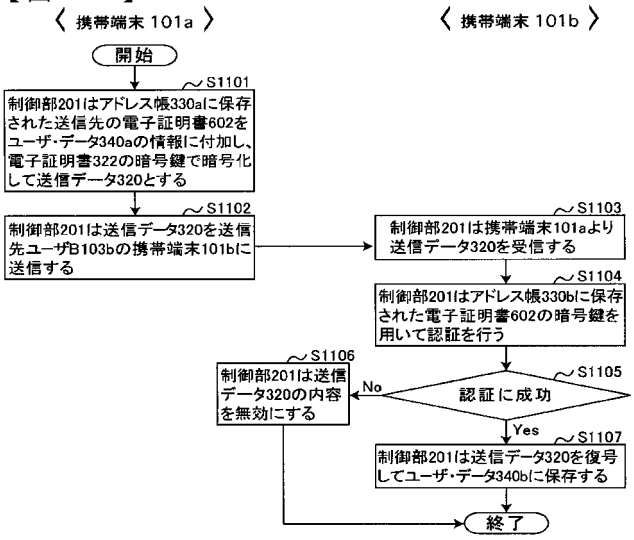
【図９】



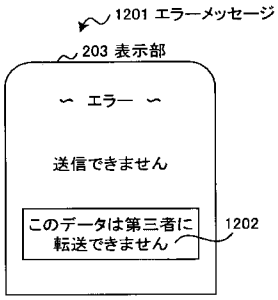
【図１０】


〈 携帯端末101a 〉
開始
S1001
制御部201は送信しようとするユーザ・データ340aの電子証明書322を参照する
S1002
自分の物か？
No
S1003
エラーメッセージの出力
Yes
S1004
制御部201はコピー回数323を参照する
S1005
コピー回数＞0
No
S1006
エラーメッセージの出力
Yes
S1007
制御部201はアドレス帳330aのユーザ601とユーザデータ340aの特定ユーザ324を照合する
S1008
一致する
No
S1009
エラーメッセージの出力
Yes
S1010
制御部201はコピー回数323のカウントを1減らす
S1011
送信処理
終了

【図１１】


〈 携帯端末 101a 〉
〈 携帯端末 101b 〉
開始
S1101
制御部201はアドレス帳330aに保存された送信先の電子証明書602をユーザ・データ340aの情報に付加し、電子証明書322の暗号鍵で暗号化して送信データ320とする
S1102
制御部201は送信データ320を送信先ユーザB103bの携帯端末101bに送信する
S1103
制御部201は携帯端末101aより送信データ320を受信する
S1104
制御部201はアドレス帳330bに保存された電子証明書602の暗号鍵を用いて認証を行う
S1105
認証に成功
No
S1106
制御部201は送信データ320の内容を無効にする
Yes
S1107
制御部201は送信データ320を復号してユーザ・データ340bに保存する
終了

【図１２】


1201 エラーメッセージ
203 表示部
エラー
送信できません
このデータは第三者に転送できません
1202

フロントページの続き

(51)Int.Cl.		F I		テーマコード（参考）
H04M 11/00	***(2006.01)***	Ｈ０４Ｍ 11/00	３０２	
H04L 9/08	***(2006.01)***	Ｈ０４Ｌ 9/00	６０１Ｃ	
		Ｈ０４Ｌ 9/00	６０１Ｅ	

Ｆターム(参考) 5K067 AA30 BB04 BB21 DD17 DD51 EE02 EE16 EE25 EE37 FF02
HH22 HH23 HH24 HH36
5K201 AA08 BA06 BB07 BC23 BD06 CB12 CB20 ED05 EE09