(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2012-10052
(P2012-10052A)
(43)公開日　平成24年1月12日(2012.1.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601Z	5B017
H04L 9/14	(2006.01)	H04L	9/00	601C	5J104
G06F 21/24	(2006.01)	H04L	9/00	641	
		G06F	12/14	510F	

審査請求 未請求　請求項の数 17　ＯＬ　（全 46 頁）

(21)出願番号　特願2010-143399 (P2010-143399)
(22)出願日　平成22年6月24日 (2010.6.24)

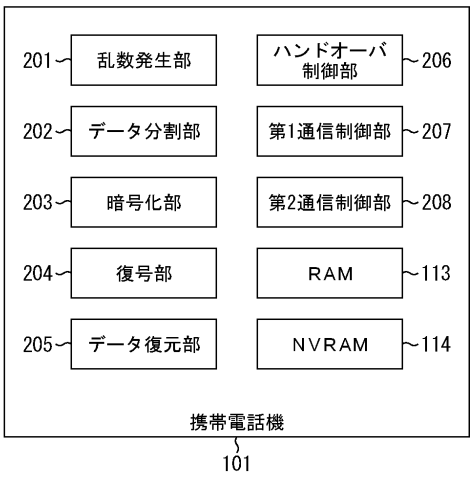
(71)出願人　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100082131
弁理士　稲本　義雄
(74)代理人　100121131
弁理士　西川　孝
(72)発明者　米田　好博
東京都港区港南１丁目７番１号　ソニー株式会社内

Ｆターム(参考)　5B017 AA03 BA10 BB02 CA16
5J104 AA16 AA32 AA44 EA02 EA04 EA08 EA13 EA16 JA03 NA02 NA37 PA14

(54)【発明の名称】情報処理装置および方法、プログラム、並びに、情報処理システム

(57)【要約】
【課題】より便利かつより安全にデータを保存する。
【解決手段】乱数発生部２０１は、自身が使用する暗号鍵である自暗号鍵、および、通信相手が使用する暗号鍵である他暗号鍵を生成し、第１通信制御部２０７は、生成された暗号鍵の全てを、第１の通信により通信相手に送信し、データ分割部２０２は、データを分割し、暗号化部２０３は、分割されたデータのうち、自身が保存すべきデータである自データを、自暗号鍵で暗号化し、第２通信制御部２０８は、分割されたデータのうち、通信相手が保存すべきデータである他データを、第２の通信により通信相手に送信し、NVRAM１１４は、暗号化部２０３によって暗号化された自データ、および他暗号鍵を記憶し、暗号化部２０３は、自データを暗号化した後、暗号化に使用した自暗号鍵を消去する。本発明は、例えば、携帯電話機から構成される通信システムに適用することができる。
【選択図】図３

図3



【特許請求の範囲】
【請求項１】
１以上の通信相手とデータを共有する情報処理装置において、
自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵を生成する生成手段と、
前記生成手段によって生成された前記暗号鍵の全てを、第１の通信により、前記通信相手に送信する第１の通信手段と、
前記データを分割する分割手段と、
前記分割手段によって分割された前記データのうち、自身が保存すべきデータである自データを、前記自暗号鍵で暗号化する暗号化手段と、
前記分割手段によって分割された前記データのうち、前記通信相手が保存すべきデータである他データを、第２の通信により、前記通信相手に送信する第２の通信手段と、
前記暗号化手段によって暗号化された前記自データ、および前記他暗号鍵を記憶する記憶手段と
を備える情報処理装置。
【請求項２】
前記暗号化手段は、前記自データを暗号化した後、暗号化に使用した前記自暗号鍵を消去する
請求項１に記載の情報処理装置。
【請求項３】
前記第１の通信手段は、前記通信相手によって記憶され、前記第１の通信により送信されてくる前記自暗号鍵を受信し、
前記第２の通信手段は、前記通信相手によって保存され、前記第２の通信により送信されてくる前記他データを受信し、
前記記憶手段に記憶されている前記自データを、前記第１の通信手段によって受信された前記自暗号鍵で復号する復号手段と、
前記復号手段によって復号された前記自データと、前記第２の通信手段によって受信された前記他データとから、前記データを復元する復元手段とをさらに備える
請求項２に記載の情報処理装置。
【請求項４】
前記記憶手段は、前記データを共有する自身および前記通信相手に関する管理情報をさらに記憶し、
前記管理情報に基づいて、
前記分割手段は、前記データを分割し、
前記第２の通信手段は、前記他データを前記通信相手に送信し、
前記暗号化手段は、前記自データを暗号化する
請求項２に記載の情報処理装置。
【請求項５】
１以上の通信相手とデータを共有する情報処理装置の情報処理方法において、
自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵を生成する生成ステップと、
前記生成ステップの処理によって生成された前記暗号鍵の全てを、第１の通信により、前記通信相手に送信する第１の通信ステップと、
前記データを分割する分割ステップと、
前記分割ステップの処理によって分割された前記データのうち、自身が保存すべきデータである自データを、前記自暗号鍵で暗号化する暗号化ステップと、
前記分割ステップの処理によって分割された前記データのうち、前記通信相手が保存すべきデータである他データを、第２の通信により、前記通信相手に送信する第２の通信ステップと、
前記暗号化ステップの処理によって暗号化された前記自データ、および前記他暗号鍵を

記憶する記憶ステップと
を含む情報処理方法。
【請求項６】
１以上の通信相手とデータを共有する情報処理装置の処理をコンピュータに実行させるプログラムにおいて、
自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵を生成する生成ステップと、
前記生成ステップの処理によって生成された前記暗号鍵の全ての、第１の通信による、前記通信相手への送信を制御する第１の通信制御ステップと、
前記データを分割する分割ステップと、
前記分割ステップの処理によって分割された前記データのうち、自身が保存すべきデータである自データを、前記自暗号鍵で暗号化する暗号化ステップと、
前記分割ステップの処理によって分割された前記データのうち、前記通信相手が保存すべきデータである他データの、第２の通信による、前記通信相手への送信を制御する第２の通信制御ステップと、
前記暗号化ステップの処理によって暗号化された前記自データ、および前記他暗号鍵の記憶を制御する記憶制御ステップと
を含む処理をコンピュータに実行させるプログラム。
【請求項７】
通信相手とデータを共有する情報処理装置において、
前記通信相手から、第１の通信により送信されてくる、自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵を受信する第１の通信手段と、
前記通信相手から、第２の通信により送信されてくる、前記通信相手において分割された前記データのうち、自身が保存すべきデータである自データを受信する第２の通信手段と、
前記第２の通信手段によって受信された前記自データを、前記第１の通信手段によって受信された前記自暗号鍵で暗号化する暗号化手段と、
前記暗号化手段によって暗号化された前記自データ、および前記他暗号鍵を記憶する記憶手段と
を備える情報処理装置。
【請求項８】
前記暗号化手段は、前記自データを暗号化した後、暗号化に使用した前記自暗号鍵を消去する
請求項７に記載の情報処理装置。
【請求項９】
前記第１の通信手段は、前記通信相手によって記憶され、前記第１の通信により送信されてくる前記自暗号鍵を受信し、
前記記憶手段に記憶されている前記自データを、前記第１の通信手段によって受信された前記自暗号鍵で復号する復号手段をさらに備え、
前記第２の通信手段は、前記復号手段によって復号された前記自データを、前記第２の通信により、前記通信相手に送信する
請求項７に記載の情報処理装置。
【請求項１０】
前記記憶手段は、前記データを共有する自身および前記通信相手に関する管理情報をさらに記憶し、
前記管理情報に基づいて、
前記第２の通信手段は、前記通信相手から送信されてくる前記自データを受信し、
前記暗号化手段は、前記自データを暗号化する
請求項７に記載の情報処理装置。

【請求項１１】
通信相手とデータを共有する情報処理装置の情報処理方法において、
前記通信相手から、第１の通信により送信されてくる、自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵を受信する第１の通信ステップと、
前記通信相手から、第２の通信により送信されてくる、前記通信相手において分割された前記データのうち、自身が保存すべきデータである自データを受信する第２の通信ステップと、
前記第２の通信ステップの処理によって受信された前記自データを、前記第１の通信ステップの処理によって受信された前記自暗号鍵で暗号化する暗号化ステップと、
前記暗号化ステップの処理によって暗号化された前記自データ、および前記他暗号鍵を記憶する記憶ステップと
を含む情報処理方法。
【請求項１２】
通信相手とデータを共有する情報処理装置の処理をコンピュータに実行させるプログラムにおいて、
前記通信相手から、第１の通信により送信されてくる、自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵の受信を制御する第１の通信制御ステップと、
前記通信相手から、第２の通信により送信されてくる、前記通信相手において分割された前記データのうち、自身が保存すべきデータである自データの受信を制御する第２の通信制御ステップと、
前記第２の通信制御ステップの処理によって受信された前記自データを、前記第１の通信制御ステップの処理によって受信された前記自暗号鍵で暗号化する暗号化ステップと、
前記暗号化ステップの処理によって暗号化された前記自データ、および前記他暗号鍵の記憶を制御する記憶制御ステップと
を含む処理をコンピュータに実行させるプログラム。
【請求項１３】
第１の情報処理装置および１以上の第２の情報処理装置からなる情報処理システムにおいて、
前記第１の情報処理装置は、
前記第１の情報処理装置が使用する暗号鍵である第１の暗号鍵、および、前記第２の情報処理装置が使用する暗号鍵である第２の暗号鍵を生成する生成手段と、
前記生成手段によって生成された前記暗号鍵の全てを、第１の通信により、前記第２の情報処理装置に送信する第１の通信手段と、
前記第１の情報処理装置および前記第２の情報処理装置に共有されるデータを分割する分割手段と、
前記分割手段によって分割された前記データのうち、前記第１の情報処理装置が保存すべきデータである第１のデータを、前記第１の暗号鍵で暗号化する第１の暗号化手段と、
前記分割手段によって分割された前記データのうち、前記第２の情報処理装置が保存すべきデータである第２のデータを、第２の通信により、前記通信相手に送信する第２の通信手段と、
前記第１の暗号化手段によって暗号化された前記第１のデータ、および前記第２の暗号鍵を記憶する第１の記憶手段と
を備え、
前記第２の情報処理装置は、
前記第１の情報処理装置から、前記第１の通信により送信されてくる前記第１の暗号鍵および前記第２の暗号鍵を受信する第３の通信手段と、
前記第１の情報処理装置から、前記第２の通信により送信されてくる前記第２のデー

タを受信する第４の通信手段と、
　前記第４の通信手段によって受信された前記第２のデータを、前記第３の通信手段によって受信された前記第２の暗号鍵で暗号化する第２の暗号化手段と、
　前記第２の暗号化手段によって暗号化された前記第２のデータ、および前記第１の暗号鍵を記憶する第２の記憶手段と
　を備える情報処理システム。
【請求項１４】
　他の情報処理装置とデータを共有する情報処理装置において、
　前記データを複数に分割する分割手段と、
　前記分割手段によって分割された複数のデータを暗号化するための複数の暗号鍵を生成する生成手段と、
　前記生成手段によって生成された複数の暗号鍵のうちの少なくとも２つの暗号鍵を、第１の通信により、前記他の情報処理装置に送信する第１の通信手段と、
　前記第１の通信手段によって送信された暗号鍵のうちの第１の暗号鍵で、前記分割手段によって分割された前記データのうちの１のデータを暗号化する暗号化手段と、
　前記分割手段によって分割された前記データのうち、前記他の情報処理装置に保存されるデータである他データを、第２の通信により、前記他の情報処理装置に送信する第２の通信手段と、
　前記暗号化手段によって暗号化された前記データ、および前記他の情報処理装置に送信された暗号鍵のうちの、前記第１の暗号鍵以外の暗号鍵を記憶する記憶手段と
　を備える情報処理装置。
【請求項１５】
　他の情報処理装置とデータを共有する情報処理装置の情報処理方法において、
　前記データを複数に分割する分割ステップと、
　前記分割ステップの処理によって分割された複数のデータを暗号化するための複数の暗号鍵を生成する生成ステップと、
　前記生成ステップの処理によって生成された複数の暗号鍵のうちの少なくとも２つの暗号鍵を、第１の通信により、前記他の情報処理装置に送信する第１の通信ステップと、
　前記第１の通信ステップの処理によって送信された暗号鍵のうちの第１の暗号鍵で、前記分割手段によって分割された前記データのうちの１のデータを暗号化する暗号化ステップと、
　前記分割ステップの処理によって分割された前記データのうち、前記他の情報処理装置に保存されるデータである他データを、第２の通信により、前記他の情報処理装置に送信する第２の通信ステップと、
　前記暗号化ステップの処理によって暗号化された前記データ、および前記他の情報処理装置に送信された暗号鍵のうちの、前記第１の暗号鍵以外の暗号鍵を記憶する記憶ステップと
　を含む情報処理方法。
【請求項１６】
　他の情報処理装置とデータを共有する情報処理装置において、
　前記他の情報処理装置から、第１の通信により送信されてくる少なくとも２つの暗号鍵を受信する第１の通信手段と、
　前記他の情報処理装置から、第２の通信により送信されてくる、前記他の情報処理装置において分割された前記データのうち、自身が保存すべきデータである自データを受信する第２の通信手段と、
　前記第２の通信手段によって受信された前記自データを、前記第１の通信手段によって受信された暗号鍵のうちの第１の暗号鍵で暗号化する暗号化手段と、
　前記暗号化手段によって暗号化された前記自データ、および前記他の情報処理装置から送信されてくる暗号鍵のうちの、前記第１の暗号鍵以外の暗号鍵を記憶する記憶手段と
　を備える情報処理装置。

【請求項１７】
第１の情報処理装置および第２の情報処理装置からなる情報処理システムにおいて、
前記第１の情報処理装置は、
前記データを複数に分割する分割手段と、
前記分割手段によって分割された複数のデータを暗号化するための複数の暗号鍵を生成する生成手段と、
前記生成手段によって生成された複数の暗号鍵のうちの少なくとも２つの暗号鍵を、第１の通信により、前記第２の情報処理装置に送信する第１の通信手段と、
前記第１の通信手段によって送信された暗号鍵のうちの第１の暗号鍵で、前記分割手段によって分割された前記データのうちの第１のデータを暗号化する第１の暗号化手段と、
前記分割手段によって分割された前記データのうち、前記第２の情報処理装置に保存されるデータである第２のデータを、第２の通信により、前記第２の情報処理装置に送信する第２の通信手段と、
前記第１の暗号化手段によって暗号化された前記第１のデータ、および前記第２の情報処理装置に送信された暗号鍵のうちの、前記第１の暗号鍵以外の暗号鍵を記憶する記憶手段と
を備え、
前記第２の情報処理装置は、
前記第１の情報処理装置から、第１の通信により送信されてくる少なくとも２つの前記暗号鍵を受信する第３の通信手段と、
前記第１の情報処理装置から、第２の通信により送信されてくる前記第２のデータを受信する第４の通信手段と、
前記第４の通信手段によって受信された前記第２のデータを、前記第３の通信手段によって受信された暗号鍵のうちの第２の暗号鍵で暗号化する第２の暗号化手段と、
前記第２の暗号化手段によって暗号化された前記第２のデータ、および前記第１の情報処理装置から送信されてくる暗号鍵のうちの、前記第２の暗号鍵以外の暗号鍵を記憶する記憶手段と
を備える情報処理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置および方法、プログラム、並びに、情報処理システムに関し、特に、より便利かつより安全にデータを保存するようにする情報処理装置および方法、プログラム、並びに、情報処理システムに関する。
【背景技術】
【０００２】
従来、３台以上の携帯電話機の間で無線通信を行って情報を共有する際に、互いの認証や通信設定等の処理を簡潔にするために、第１の通信から第２の通信にハンドオーバしてデータを共有するようにした情報処理装置が提案されている（特許文献１参照）。
【０００３】
また、一般的に、LAN（Local Area Network）等の、複数の機器が接続されるネットワークにおいて、共有サーバやファイルサーバ等を設けることによって、複数の機器で１つのファイルを共有することが行われている。
【０００４】
LANのようなネットワークにおいては、例えば、共有ファイルのセキュリティレベルを設定することによって、そのネットワークに接続されている機器を使用するユーザが、記録媒体にファイルをコピーして持ち出すことを防ぐことで、情報の流出を避けることができた。
【先行技術文献】

【特許文献】
【０００５】
【特許文献１】特開２０１０－７３１０５号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、携帯電話機の間で行われる無線通信によって授受されるデータは、携帯電話機のユーザによって、簡単に情報が流出してしまう恐れがあった。
【０００７】
本発明は、このような状況に鑑みてなされたものであり、特に、より便利かつより安全にデータを保存するようにするものである。
【課題を解決するための手段】
【０００８】
本発明の第１の側面の情報処理装置は、１以上の通信相手とデータを共有する情報処理装置であって、自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵を生成する生成手段と、前記生成手段によって生成された前記暗号鍵の全てを、第１の通信により、前記通信相手に送信する第１の通信手段と、前記データを分割する分割手段と、前記分割手段によって分割された前記データのうち、自身が保存すべきデータである自データを、前記自暗号鍵で暗号化する暗号化手段と、前記分割手段によって分割された前記データのうち、前記通信相手が保存すべきデータである他データを、第２の通信により、前記通信相手に送信する第２の通信手段と、前記暗号化手段によって暗号化された前記自データ、および前記他暗号鍵を記憶する記憶手段とを備える。
【０００９】
前記暗号化手段には、前記自データを暗号化した後、暗号化に使用した前記自暗号鍵を消去させることができる。
【００１０】
前記第１の通信手段には、前記通信相手によって記憶され、前記第１の通信により送信されてくる前記自暗号鍵を受信させ、前記第２の通信手段には、前記通信相手によって保存され、前記第２の通信により送信されてくる前記他データを受信させ、前記情報処理装置には、前記記憶手段に記憶されている前記自データを、前記第１の通信手段によって受信された前記自暗号鍵で復号する復号手段と、前記復号手段によって復号された前記自データと、前記第２の通信手段によって受信された前記他データとから、前記データを復元する復元手段とをさらに設けることができる。
【００１１】
前記記憶手段には、前記データを共有する自身および前記通信相手に関する管理情報をさらに記憶させ、前記管理情報に基づいて、前記分割手段には、前記データを分割させ、前記第２の通信手段には、前記他データを前記通信相手に送信させ、前記暗号化手段には、前記自データを暗号化させることができる。
【００１２】
本発明の第１の側面の情報処理方法は、１以上の通信相手とデータを共有する情報処理装置の情報処理方法であって、自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵を生成する生成ステップと、前記生成ステップの処理によって生成された前記暗号鍵の全てを、第１の通信により、前記通信相手に送信する第１の通信ステップと、前記データを分割する分割ステップと、前記分割ステップの処理によって分割された前記データのうち、自身が保存すべきデータである自データを、前記自暗号鍵で暗号化する暗号化ステップと、前記分割ステップの処理によって分割された前記データのうち、前記通信相手が保存すべきデータである他データを、第２の通信により、前記通信相手に送信する第２の通信ステップと、前記暗号化ステップの処理によって暗号化された前記自データ、および前記他暗号鍵を記憶する記憶ステップとを含む。
【００１３】

本発明の第１の側面のプログラムは、１以上の通信相手とデータを共有する情報処理装置の処理をコンピュータに実行させるプログラムであって、自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵を生成する生成ステップと、前記生成ステップの処理によって生成された前記暗号鍵の全ての、第１の通信による、前記通信相手への送信を制御する第１の通信制御ステップと、前記データを分割する分割ステップと、前記分割ステップの処理によって分割された前記データのうち、自身が保存すべきデータである自データを、前記自暗号鍵で暗号化する暗号化ステップと、前記分割ステップの処理によって分割された前記データのうち、前記通信相手が保存すべきデータである他データの、第２の通信による、前記通信相手への送信を制御する第２の通信制御ステップと、前記暗号化ステップの処理によって暗号化された前記自データ、および前記他暗号鍵の記憶を制御する記憶制御ステップとを含む処理をコンピュータに実行させる。

【００１４】

本発明の第１の側面においては、自身が使用する暗号鍵である自暗号鍵、および、通信相手が使用する暗号鍵である他暗号鍵が生成され、生成された暗号鍵の全てが、第１の通信により、通信相手へ送信され、データが分割され、分割されたデータのうち、自身が保存すべきデータである自データが、自暗号鍵で暗号化され、分割されたデータのうち、通信相手が保存すべきデータである他データが、第２の通信により、通信相手に送信され、暗号化された自データ、および他暗号鍵が記憶される。

【００１５】

本発明の第２の側面の情報処理装置は、通信相手とデータを共有する情報処理装置であって、前記通信相手から、第１の通信により送信されてくる、自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵を受信する第１の通信手段と、前記通信相手から、第２の通信により送信されてくる、前記通信相手において分割された前記データのうち、自身が保存すべきデータである自データを受信する第２の通信手段と、前記第２の通信手段によって受信された前記自データを、前記第１の通信手段によって受信された前記自暗号鍵で暗号化する暗号化手段と、前記暗号化手段によって暗号化された前記自データ、および前記他暗号鍵を記憶する記憶手段とを備える。

【００１６】

前記暗号化手段には、前記自データを暗号化した後、暗号化に使用した前記自暗号鍵を消去させることができる。

【００１７】

前記第１の通信手段には、前記通信相手によって記憶され、前記第１の通信により送信されてくる前記自暗号鍵を受信させ、前記情報処理装置には、前記記憶手段に記憶されている前記自データを、前記第１の通信手段によって受信された前記自暗号鍵で復号する復号手段をさらに設け、前記第２の通信手段には、前記復号手段によって復号された前記自データを、前記第２の通信により、前記通信相手に送信させることができる。

【００１８】

前記記憶手段には、前記データを共有する自身および前記通信相手に関する管理情報をさらに記憶させ、前記管理情報に基づいて、前記第２の通信手段には、前記通信相手から送信されてくる前記自データを受信させ、前記暗号化手段には、前記自データを暗号化させることができる。

【００１９】

本発明の第２の側面の情報処理方法は、通信相手とデータを共有する情報処理装置の情報処理方法であって、前記通信相手から、第１の通信により送信されてくる、自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵を受信する第１の通信ステップと、前記通信相手から、第２の通信により送信されてくる、前記通信相手において分割された前記データのうち、自身が保存すべきデータである自データを受信する第２の通信ステップと、前記第２の通信ステップの処理によって受信された前記自データを、前記第１の通信ステップの処理によって受信された前記自暗号鍵で暗号

化する暗号化ステップと、前記暗号化ステップの処理によって暗号化された前記自データ、および前記他暗号鍵を記憶する記憶ステップとを含む。

【００２０】

本発明の第２の側面のプログラムは、通信相手とデータを共有する情報処理装置の処理をコンピュータに実行させるプログラムであって、前記通信相手から、第１の通信により送信されてくる、自身が使用する暗号鍵である自暗号鍵、および、前記通信相手が使用する暗号鍵である他暗号鍵の受信を制御する第１の通信制御ステップと、前記通信相手から、第２の通信により送信されてくる、前記通信相手において分割された前記データのうち、自身が保存すべきデータである自データの受信を制御する第２の通信制御ステップと、前記第２の通信制御ステップの処理によって受信された前記自データを、前記第１の通信制御ステップの処理によって受信された前記自暗号鍵で暗号化する暗号化ステップと、前記暗号化ステップの処理によって暗号化された前記自データ、および前記他暗号鍵の記憶を制御する記憶制御ステップとを含む処理をコンピュータに実行させる。

【００２１】

本発明の第２の側面においては、通信相手から、第１の通信により送信されてくる、自身が使用する暗号鍵である自暗号鍵、および、通信相手が使用する暗号鍵である他暗号鍵が受信され、通信相手から、第２の通信により送信されてくる、通信相手において分割されたデータのうち、自身が保存すべきデータである自データが受信され、受信された自データが、受信された自暗号鍵で暗号化され、暗号化された自データ、および他暗号鍵が記憶される。

【００２２】

本発明の第３の側面の情報処理システムは、第１の情報処理装置および１以上の第２の情報処理装置からなる情報処理システムであって、前記第１の情報処理装置が、前記第１の情報処理装置が使用する暗号鍵である第１の暗号鍵、および、前記第２の情報処理装置が使用する暗号鍵である第２の暗号鍵を生成する生成手段と、前記生成手段によって生成された前記暗号鍵の全てを、第１の通信により、前記第２の情報処理装置に送信する第１の通信手段と、前記第１の情報処理装置および前記第２の情報処理装置に共有されるデータを分割する分割手段と、前記分割手段によって分割された前記データのうち、前記第１の情報処理装置が保存すべきデータである第１のデータを、前記第１の暗号鍵で暗号化する第１の暗号化手段と、前記分割手段によって分割された前記データのうち、前記第２の情報処理装置が保存すべきデータである第２のデータを、第２の通信により、前記通信相手に送信する第２の通信手段と、前記第１の暗号化手段によって暗号化された前記第１のデータ、および前記第２の暗号鍵を記憶する第１の記憶手段とを備え、前記第２の情報処理装置が、前記第１の情報処理装置から、前記第１の通信により送信されてくる前記第１の暗号鍵および前記第２の暗号鍵を受信する第３の通信手段と、前記第１の情報処理装置から、前記第２の通信により送信されてくる前記第２のデータを受信する第４の通信手段と、前記第４の通信手段によって受信された前記第２のデータを、前記第３の通信手段によって受信された前記第２の暗号鍵で暗号化する第２の暗号化手段と、前記第２の暗号化手段によって暗号化された前記第２のデータ、および前記第１の暗号鍵を記憶する第２の記憶手段とを備える。

【００２３】

本発明の第３の側面においては、第１の情報処理装置が使用する暗号鍵である第１の暗号鍵、および、第２の情報処理装置が使用する暗号鍵である第２の暗号鍵が生成され、暗号鍵の全てが、第１の通信により、第２の情報処理装置に送信され、第１の情報処理装置および第２の情報処理装置に共有されるデータが分割され、分割されたデータのうち、第１の情報処理装置が保存すべきデータである第１のデータが、第１の暗号鍵で暗号化され、分割されたデータのうち、第２の情報処理装置が保存すべきデータである第２のデータが、第２の通信により、通信相手に送信され、暗号化された第１のデータ、および第２の暗号鍵が記憶される。また、第１の情報処理装置から、第１の通信により送信されてくる第１の暗号鍵および第２の暗号鍵が受信され、第１の情報処理装置から、第２の通信によ

り送信されてくる第２のデータが受信され、受信された第２のデータが、受信された第２の暗号鍵で暗号化され、暗号化された第２のデータ、および第１の暗号鍵が記憶される。

【００２４】

本発明の第４の側面の情報処理装置は、他の情報処理装置とデータを共有する情報処理装置であって、前記データを複数に分割する分割手段と、前記分割手段によって分割された複数のデータを暗号化するための複数の暗号鍵を生成する生成手段と、前記生成手段によって生成された複数の暗号鍵のうちの少なくとも２つの暗号鍵を、第１の通信により、前記他の情報処理装置に送信する第１の通信手段と、前記第１の通信手段によって送信された暗号鍵のうちの第１の暗号鍵で、前記分割手段によって分割された前記データのうちの１のデータを暗号化する暗号化手段と、前記分割手段によって分割された前記データのうち、前記他の情報処理装置に保存されるデータである他データを、第２の通信により、前記他の情報処理装置に送信する第２の通信手段と、前記暗号化手段によって暗号化された前記データ、および前記他の情報処理装置に送信された暗号鍵のうちの、前記第１の暗号鍵以外の暗号鍵を記憶する記憶手段とを備える。

【００２５】

本発明の第４の側面の情報処理方法は、他の情報処理装置とデータを共有する情報処理装置の情報処理方法であって、前記データを複数に分割する分割ステップと、前記分割ステップの処理によって分割された複数のデータを暗号化するための複数の暗号鍵を生成する生成ステップと、前記生成ステップの処理によって生成された複数の暗号鍵のうちの少なくとも２つの暗号鍵を、第１の通信により、前記他の情報処理装置に送信する第１の通信ステップと、前記第１の通信ステップの処理によって送信された暗号鍵のうちの第１の暗号鍵で、前記分割手段によって分割された前記データのうちの１のデータを暗号化する暗号化ステップと、前記分割ステップの処理によって分割された前記データのうち、前記他の情報処理装置に保存されるデータである他データを、第２の通信により、前記他の情報処理装置に送信する第２の通信ステップと、前記暗号化ステップの処理によって暗号化された前記データ、および前記他の情報処理装置に送信された暗号鍵のうちの、前記第１の暗号鍵以外の暗号鍵を記憶する記憶ステップとを含む。

【００２６】

本発明の第４の側面においては、データが複数に分割され、分割された複数のデータを暗号化するための複数の暗号鍵が生成され、生成された複数の暗号鍵のうちの少なくとも２つの暗号鍵が、第１の通信により、他の情報処理装置に送信され、送信された暗号鍵のうちの第１の暗号鍵で、分割されたデータのうちの１のデータが暗号化され、分割されたデータのうち、他の情報処理装置に保存されるデータである他データが、第２の通信により、他の情報処理装置に送信され、暗号化されたデータ、および他の情報処理装置に送信された暗号鍵のうちの、第１の暗号鍵以外の暗号鍵が記憶される。

【００２７】

本発明の第５の側面の情報処理装置は、他の情報処理装置とデータを共有する情報処理装置であって、前記他の情報処理装置から、第１の通信により送信されてくる少なくとも２つの暗号鍵を受信する第１の通信手段と、前記他の情報処理装置から、第２の通信により送信されてくる、前記他の情報処理装置において分割された前記データのうち、自身が保存すべきデータである自データを受信する第２の通信手段と、前記第２の通信手段によって受信された前記自データを、前記第１の通信手段によって受信された暗号鍵のうちの第１の暗号鍵で暗号化する暗号化手段と、前記暗号化手段によって暗号化された前記自データ、および前記他の情報処理装置から送信されてくる暗号鍵のうちの、前記第１の暗号鍵以外の暗号鍵を記憶する記憶手段とを備える。

【００２８】

本発明の第５の側面においては、他の情報処理装置から、第１の通信により送信されてくる少なくとも２つの暗号鍵が受信され、他の情報処理装置から、第２の通信により送信されてくる、他の情報処理装置において分割されたデータのうち、自身が保存すべきデータである自データが受信され、受信された自データが、受信された暗号鍵のうちの第１の

暗号鍵で暗号化され、暗号化された自データ、および他の情報処理装置から送信されてくる暗号鍵のうちの、第１の暗号鍵以外の暗号鍵が記憶される。

【００２９】

本発明の第６の側面の情報処理システムは、第１の情報処理装置および第２の情報処理装置からなる情報処理システムであって、前記第１の情報処理装置が、前記データを複数に分割する分割手段と、前記分割手段によって分割された複数のデータを暗号化するための複数の暗号鍵を生成する生成手段と、前記生成手段によって生成された複数の暗号鍵のうちの少なくとも２つの暗号鍵を、第１の通信により、前記第２の情報処理装置に送信する第１の通信手段と、前記第１の通信手段によって送信された暗号鍵のうちの第１の暗号鍵で、前記分割手段によって分割された前記データのうちの第１のデータを暗号化する第１の暗号化手段と、前記分割手段によって分割された前記データのうち、前記第２の情報処理装置に保存されるデータである第２のデータを、第２の通信により、前記第２の情報処理装置に送信する第２の通信手段と、前記第１の暗号化手段によって暗号化された前記第１のデータ、および前記第２の情報処理装置に送信された暗号鍵のうちの、前記第１の暗号鍵以外の暗号鍵を記憶する記憶手段とを備え、前記第２の情報処理装置が、前記第１の情報処理装置から、第１の通信により送信されてくる少なくとも２つの前記暗号鍵を受信する第３の通信手段と、前記第１の情報処理装置から、第２の通信により送信されてくる前記第２のデータを受信する第４の通信手段と、前記第４の通信手段によって受信された前記第２のデータを、前記第３の通信手段によって受信された暗号鍵のうちの第２の暗号鍵で暗号化する第２の暗号化手段と、前記第２の暗号化手段によって暗号化された前記第２のデータ、および前記第１の情報処理装置から送信されてくる暗号鍵のうちの、前記第２の暗号鍵以外の暗号鍵を記憶する記憶手段とを備える。

【００３０】

本発明の第６の側面においては、データが複数に分割され、分割された複数のデータを暗号化するための複数の暗号鍵が生成され、生成された複数の暗号鍵のうちの少なくとも２つの暗号鍵が、第１の通信により、第２の情報処理装置に送信され、送信された暗号鍵のうちの第１の暗号鍵で、分割されたデータのうちの第１のデータが暗号化され、分割されたデータのうち、第２の情報処理装置に保存されるデータである第２のデータが、第２の通信により、第２の情報処理装置に送信され、暗号化された第１のデータ、および第２の情報処理装置に送信された暗号鍵のうちの、第１の暗号鍵以外の暗号鍵が記憶される。また、第１の情報処理装置から、第１の通信により送信されてくる少なくとも２つの暗号鍵が受信され、第１の情報処理装置から、第２の通信により送信されてくる第２のデータが受信され、受信された第２のデータが、受信された暗号鍵のうちの第２の暗号鍵で暗号化され、暗号化された第２のデータ、および第１の情報処理装置から送信されてくる暗号鍵のうちの、第２の暗号鍵以外の暗号鍵が記憶される。

【発明の効果】

【００３１】

本発明の第１乃至第６の側面によれば、より便利かつより安全にデータを保存することが可能となる。

【図面の簡単な説明】

【００３２】

【図１】通信システムの構成例を示す図である。

【図２】図１の携帯電話機の構成例を示すブロック図である。

【図３】携帯電話機の機能構成例を示すブロック図である。

【図４】携帯電話機のディスプレイの表示について説明する図である。

【図５】携帯電話機のディスプレイの表示について説明する図である。

【図６】図１の通信システムのデータ保存処理について説明するフローチャートである。

【図７】携帯電話機のデータの授受について説明する図である。

【図８】データ情報テーブルの例を示す図である。

【図９】ユーザ情報テーブルの例を示す図である。

【図１０】携帯電話機のディスプレイの表示について説明する図である。
【図１１】携帯電話機のディスプレイの表示について説明する図である。
【図１２】携帯電話機のディスプレイの表示について説明する図である。
【図１３】携帯電話機のディスプレイの表示について説明する図である。
【図１４】図１の通信システムのデータ復元処理について説明するフローチャートである。
【図１５】携帯電話機のデータの授受について説明する図である。
【図１６】携帯電話機のディスプレイの表示について説明する図である。
【図１７】通信システムの他の構成例を示す図である。
【図１８】図１７の装置Ａのディスプレイの表示について説明する図である。
【図１９】装置Ａのディスプレイの表示について説明する図である。
【図２０】図１７の通信システムのデータ保存処理について説明するフローチャートである。
【図２１】図１７の通信システムのデータ保存処理について説明するフローチャートである。
【図２２】鍵データについて説明する図である。
【図２３】ユーザ情報について説明する図である。
【図２４】アプリケーションデータ情報について説明する図である。
【図２５】ユーザ情報テーブルの例を示す図である。
【図２６】データ情報テーブルの例を示す図である。
【図２７】分散処理および暗号化処理の例について説明する図である。
【図２８】分散処理および暗号化処理の他の例について説明する図である。
【図２９】装置Ａ，Ｂ，Ｃのディスプレイの表示について説明する図である。
【図３０】図１７の通信システムのデータ復元処理について説明するフローチャートである。
【図３１】図１７の通信システムのデータ復元処理について説明するフローチャートである。
【図３２】装置Ａ，Ｂ，Ｃのディスプレイの表示について説明する図である。
【図３３】鍵データについて説明する図である。
【図３４】装置Ａ，Ｂ，Ｃのディスプレイの表示について説明する図である。
【図３５】装置Ａ，Ｂ，Ｃのディスプレイの表示について説明する図である。
【図３６】復号処理および復元処理の例について説明する図である。
【発明を実施するための形態】
【００３３】
以下、本発明の実施の形態について図を参照して説明する。なお、説明は以下の順序で行うが、第２の実施の形態における３台の装置間での通信の方式を、第１の実施の形態における２台の装置間での通信に適用するようにしてもよい。
１．第１の実施の形態（２台の装置間で通信を行う例）
２．第２の実施の形態（３台の装置間で通信を行う例）
【００３４】
＜１．第１の実施の形態＞
［通信システムの構成例について］
図１は、通信システムの構成例を示す図である。図１において、通信システム１００は、複数の装置間で無線通信を行わせ、データの授受を行い、そのデータに基づいてアプリケーションを実行するシステムである。図１に示されるように、通信システム１００は、例えば、携帯電話機１０１および携帯電話機１０２を有する。
【００３５】
携帯電話機１０１および携帯電話機１０２は、第１通信と第２通信の２つの方法で互いに通信を行う。第１通信は、データの授受に必要な情報を授受するために行われる通信である。例えば、第１通信として近接無線通信が利用される。第２通信は、携帯電話機１０

１および携帯電話機１０２のそれぞれにおいて実行されるアプリケーションを動作させるためのデータを授受するために行われる通信である。例えば、第２通信として近距離無線通信が利用される。

【００３６】

なお、ここで近接無線通信とは、携帯電話機１０１および携帯電話機１０２の筐体を互いに接触させるか、若しくは、例えば数センチメートル程度のように、通信相手を視覚的に特定可能な距離まで近接させた状態で通信可能な無線通信方式のことを示す。例えば、非接触IC（Integrated Circuit）カードのような、電磁誘導を利用した無線通信方式がある。なお、以下においては、特に必要の無い限り、上述したような「接触」と「近接」を区別せずに説明する。すなわち、以下において、「近接」と説明する行為には、「接触」も含まれるものとする。また、その逆も同様である。

【００３７】

また、近距離無線通信とは、携帯電話機１０１および携帯電話機１０２の筐体を近距離（例えば数十メートル以下程度）に位置させた状態で通信可能な無線通信方式のことを示す。例えば、ブルートゥース（Bluetooth（登録商標））方式やWiFi（Wireless Fidelity）方式（WiFi認定されたIEEE（Institute of Electrical and Electronic Engineers）８０２．１１ｘ）がある。

【００３８】

一般的に、第１通信として使用される近接無線通信の場合、その通信範囲の物理的制限から通信相手の特定が容易であり、その分、通信接続を確立させるための設定作業が、近距離無線通信の場合よりも容易である。例えば、近距離無線通信の場合、通信可能範囲に複数のデバイスが存在する場合、どのデバイスと通信を行うかをユーザが指定する必要がある。これに対して近接無線通信の場合、その通信可能範囲が狭いため、基本的に通信相手が１台に制限される。したがってこの場合、ユーザは、自分自身が操作するデバイスを通信相手となるデバイスに近接させる必要があるが、その行為自体が通信相手を指定することになるので、改めて通信相手の指定等を入力する必要がない。

【００３９】

ただし、近接無線通信は、一般的に近距離無線通信よりもデータ転送レートが低く、大容量のデータ転送に不向きである。また、通信中はデバイス同士を近接させておかなければならないが、その姿勢（デバイス同士の位置関係）維持が困難な場合も考えられる。さらに３台以上のデバイス間通信も困難になる。

【００４０】

以上のような点から、通信システム１００においては、アプリケーション（携帯電話機１０１と携帯電話機１０２のそれぞれで実行されるアプリケーション）を動作させるためのデータの授受は、第２通信（近距離無線通信）により行い、第１通信（近接無線通信）は、データの授受に必要な情報を授受するために利用される。つまり、携帯電話機１０１と携帯電話機１０２は、まず、第１通信を行い、データの授受に必要な情報を授受することにより第２通信の接続の準備を行う。第２通信の接続が確立されると、携帯電話機１０１と携帯電話機１０２は、その第２通信を利用してアプリケーションを動作させるためのデータの授受を行う。

【００４１】

なお、通信システム１００を構成する通信装置は、第１通信と第２通信の両方を行うことができる装置であればどのような通信装置であっても良い。例えば、通信時のデバイスの位置関係において通信相手を視覚的に特定可能な距離で通信を行う第１通信、並びに、通信可能範囲が第１通信よりも広く、通信時のデバイスの位置関係において通信相手を視覚的に特定することが困難な距離で通信を行う第２通信の両方を行うことができる通信装置であってもよい。

【００４２】

つまり、通信システム１００を構成する通信装置は、上述した携帯電話機１０１および携帯電話機１０２以外であっても良い。例えば、テレビジョン受像機、ビデオレコーダ、

メディアプレーヤ、オーディオアンプ、オーディオコンポ、プリンタ、ファクシミリ、車載用オーディオシステム、またはカーナビゲーションシステム等であってもよい。もちろん、これら以外の装置であっても良い。また、例えば携帯電話機とオーディオコンポのように、通信システム１００を構成する各通信装置が互いに異なる機能を有する装置であっても良い。

【００４３】

さらに通信システム１００を構成する通信装置の数は任意であり、３台以上であってもよい。なお、第１通信は近接無線通信でなくてもよい。また、第２通信も近距離無線通信である必要はない。さらに、この第１通信および第２通信は、中継装置やネットワークを介して行われるようにしてもよい。また、第１通信および第２通信は、有線を介して行われる有線通信であってもよい。ただし、上述したように第１通信は、第２通信で行われるデータの授受に必要な情報を授受するための通信であるので、通信相手を容易に特定可能である等、通信開始のための設定作業が容易または不要なものであるのが望ましい。

【００４４】

図２は、図１の携帯電話機１０１の内部の構成例を示すブロック図である。

【００４５】

図２において、携帯電話機１０１のCPU（Central Processing Unit）１１１は、ソフトウェアプログラムを実行することにより、各種の処理を実行する演算処理部である。CPU１１１は、バス１１５を介してROM（Read Only Memory）１１２、RAM（Random Access Memory）１１３、およびNVRAM（Non Volatile RAM）１１４と相互に接続される。ROM１１２には予めソフトウェアプログラムやデータが格納される。RAM１１３およびNVRAM１１４には、ROM１１２や記憶部１２３に格納されているソフトウェアプログラムやデータがロードされる。RAM１１３およびNVRAM１１４にはまた、CPU１１１が各種の処理を実行する上において必要なデータなども適宜記憶される。

【００４６】

このバス１１５にはまた、入出力インタフェース１２０も接続される。入出力インタフェース１２０には、キーボード、マウスなどよりなる入力部１２１が接続される。また入出力インタフェース１２０には、CRT（Cathode Ray Tube）ディスプレイや、LCD（Liquid Crystal Display）などよりなるディスプレイ、並びにスピーカなどよりなる出力部１２２も接続される。さらに入出力インタフェース１２０には、フラッシュメモリやハードディスクなどより構成される記憶部１２３が接続される。

【００４７】

入出力インタフェース１２０にはまた、必要に応じてドライブ１２４が接続され、磁気ディスク、光ディスク、光磁気ディスク、或いは半導体メモリなどのリムーバブルメディア１３１が適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部１２３にインストールされる。

【００４８】

さらに、入出力インタフェース１２０には、第１通信を行う第１通信部１４１と第２通信を行う第２通信部１４２が接続される。また、入出力インタフェース１２０には、モデムなどより構成され、公衆電話回線網を介して他の装置と音声通信、または、パケット通信を行う電話回線網通信部１４３が接続される。さらに、入出力インタフェース１２０には、被写体を撮影し、その画像データを得るデジタルカメラ機能を有するカメラ部１４４が接続される。

【００４９】

第１通信部１４１は、上述したような近接無線通信を行う無線通信部である。第１通信部１４１は、非接触ICカードに利用される通信方式で通信を行う無線通信部であるモバイル機器用IC通信チップ１５１（以下、モバイルIC通信チップ１５１と称する）を有する。また、第１通信部１４１は、ディジタル家電用IC通信チップ１５２（以下、CE（Consumer Electronics）用IC通信チップ１５２と称する）を有する。モバイルIC通信チップ１５１およびCE用IC通信チップ１５２は、互いに異なる通信規格に基づいて通信を行う。第１通

信部１４１は、これらのうち、いずれか一方を選択的に使用する。
【００５０】
第２通信部１４２は、上述したような近距離無線通信を行う無線通信部である。第２通信部１４２は、ブルートゥース方式で無線通信を行う無線通信部であるブルートゥース（Bluetooth（登録商標））１６１を有する。また、第２通信部１４２は、IEEE８０２．１１ｘ方式で無線通信を行う、WiFi認定された無線通信部であるワイファイ（WiFi）１６２を有する。第２通信部１４２は、これらのうち、いずれか一方を選択的に使用する。
【００５１】
なお、図２においては、第１通信部１４１および第２通信部１４２のそれぞれにおいて２種類の通信部が設けられるように説明したが、それぞれが有する通信部の数（種類）はいくつであってもよい。また、第１通信部１４１は第１通信を行うものであればよく、第２通信部１４２は第２通信を行うものであればよい。つまり、第１通信部１４１および第２通信部１４２が有する通信部の通信方式は任意であり、上述した以外のものであってもよい。
【００５２】
また、携帯電話機１０１が上述した以外の構成を有するようにしてももちろんよい。また、カメラ部１４４等一部の機能は省略可能である。
【００５３】
携帯電話機１０１の通信相手となる携帯電話機１０２も、図２を参照して説明した携帯電話機１０１の構成と基本的に同様の構成を有するので、携帯電話機１０２の構成についての説明は省略する。つまり、図２の説明は、携帯電話機１０２にも適用することができ、携帯電話機１０２の構成を説明する場合も、携帯電話機１０１と同様に、図２を用いて説明する。以下においては、ハンドオーバ処理を要求する側を携帯電話機１０１とし、それに応答する側を携帯電話機１０２として説明しているが、状況に応じて同一の装置が要求側になる場合も応答側になる場合も考えられ、要求側と応答側で構成が互いに異なる必要はない。したがって、以下においても、携帯電話機１０１および携帯電話機１０２の構成は、基本的に互いに同一であるものとして説明する。つまり、携帯電話機１０１の構成についての説明は、携帯電話機１０２の説明にも適用可能である。
【００５４】
［携帯電話機の機能構成例について］
次に、図３を参照して、携帯電話機１０１の機能構成例について説明する。
【００５５】
図３の携帯電話機１０１は、RAM１１３、NVRAM１１４、乱数発生部２０１、データ分割部２０２、暗号化部２０３、復号部２０４、データ復元部２０５、ハンドオーバ制御部２０６、第１通信制御部２０７、および第２通信制御部２０８から構成される。
【００５６】
なお、図３において、RAM１１３およびNVRAM１１４は、図２の携帯電話機１０１におけるRAM１１３およびNVRAM１１４と同一であるので、その説明は省略する。
【００５７】
乱数発生部２０１は、暗号化部２０３によって行われるデータの暗号化に使用される暗号鍵となる、乱数を発生する。
【００５８】
データ分割部２０２は、第２通信を利用して授受される、アプリケーションを動作させるためのデータ（以下、適宜、アプリケーションデータという）を、所定のアルゴリズム（分散方式）を用いて分割する。
【００５９】
暗号化部２０３は、所定のアルゴリズム（暗号方式）を用いて、データ分割部２０２によって分割されたデータを暗号化する。
【００６０】
復号部２０４は、暗号化されたデータを、暗号化されたときのアルゴリズムと同一のア

ルゴリズムで復号する。

【００６１】

データ復元部２０５は、分割されたデータを、分割されたときのアルゴリズムと同一のアルゴリズムで復元する。

【００６２】

ハンドオーバ制御部２０６は、第１通信制御部２０７および第２通信制御部２０８を制御して、通信相手との第１通信を確立した後、その通信相手との第２通信を確立する処理（ハンドオーバ処理）を行う。

【００６３】

第１通信制御部２０７は、第１通信部１４１を制御し、第１通信に関する処理を行う。

【００６４】

第２通信制御部２０８は、第２通信部１４２を制御し、第２通信に関する処理を行う。

【００６５】

［通信システムにおけるデータの保存について］

次に、通信システム１００におけるデータの保存について説明する。

【００６６】

通信システム１００において、携帯電話機１０１および携帯電話機１０２は、互いに通信を行うことにより、アプリケーションデータを共有して保存することができる。

【００６７】

例えば、携帯電話機１０１および携帯電話機１０２のRAM１１３に、同一のアプリケーションデータが保持されているとすると、例えば、図４に示されるように、携帯電話機１０１のディスプレイ２３１および携帯電話機１０２のディスプレイ２３２には、携帯電話機１０１および携帯電話機１０２それぞれに保持されているアプリケーションデータ（画像データ）により表示される画像と、ユーザがその画像データの保存を指示するためのGUI（Graphical User Interface）としての「保存」ボタンとが表示される。

【００６８】

図４の状態から、携帯電話機１０１および携帯電話機１０２のいずれかのユーザ（この場合、携帯電話機１０１のユーザ）が、「保存」ボタンを選択すると、携帯電話機１０１のディスプレイ２３１には、図５の左側に示されるように、画像データの保存先をユーザに確認させるためのメッセージ「どこに保存しますか？」と、その保存先の候補を選択させるための「ＳＤメモリ」ボタンおよび「共有メモリ」ボタンとが表示される。

【００６９】

ここで、携帯電話機１０１のユーザが「ＳＤメモリ」ボタンを選択した場合、携帯電話機１０１のRAM１１３に保持されている画像データは、携帯電話機１０１のNVRAM１１４に保存される。一方、携帯電話機１０１のユーザが「共有メモリ」ボタンを選択した場合、携帯電話機１０１のディスプレイ２３１には、図５の右側に示されるように、「タッチしてください。」というメッセージが表示され、携帯電話機１０１のユーザに、携帯電話機１０１の筐体を携帯電話機１０２の筐体に近接または接触させることを促す。

【００７０】

そして、携帯電話機１０１の筐体と携帯電話機１０２の筐体とが近接または接触されると、通信システム１００において、携帯電話機１０１と携帯電話機１０２とがデータを共有して保存するデータ保存処理が実行される。

【００７１】

［データ保存処理について］

図６のフローチャートを参照して、通信システム１００における携帯電話機１０１および携帯電話機１０２のデータ保存処理について説明する。

【００７２】

ステップＳ１１において、携帯電話機１０１のハンドオーバ制御部２０６は、第１通信制御部２０７を制御して、携帯電話機１０２との間に第１通信を確立する。一方、ステップＳ４１において、携帯電話機１０２のハンドオーバ制御部２０６は、第１通信制御部２

０７を制御して、携帯電話機１０１との間に第１通信を確立する。
【００７３】
第１通信が確立されると、ステップＳ１２において、携帯電話機１０１の乱数発生部２０１は、乱数を発生することで、暗号鍵である鍵Ａを生成する。また、ステップＳ４２において、携帯電話機１０２の乱数発生部２０１は、乱数を発生することで、暗号鍵である鍵Ｂを生成する。
【００７４】
鍵Ａが生成されると、ステップＳ１３において、携帯電話機１０１の第１通信制御部２０７は、第１通信部１４１を制御して、乱数発生部２０１において生成された鍵Ａを携帯電話機１０２に送信する。一方、ステップＳ４３において、携帯電話機１０２の第１通信制御部２０７は、第１通信部１４１を制御して、携帯電話機１０１から送信されてくる鍵Ａを受信する。
【００７５】
また、ステップＳ４４において、携帯電話機１０２の第１通信制御部２０７は、第１通信部１４１を制御して、乱数発生部２０１において生成された鍵Ｂを携帯電話機１０１に送信する。一方、ステップＳ１４において、携帯電話機１０１の第１通信制御部２０７は、第１通信部１４１を制御して、携帯電話機１０２から送信されてくる鍵Ｂを受信する。
【００７６】
すなわち、図７の矢印３０１に示されるように、携帯電話機１０１の乱数発生部２０１において生成された鍵Ａは携帯電話機１０２に供給され、携帯電話機１０２の乱数発生部２０１において生成された鍵Ｂは携帯電話機１０１に供給される。
【００７７】
図７は、携帯電話機１０１と携帯電話機１０２との間のデータの授受について説明する図である。
【００７８】
図７に示されるように、携帯電話機１０１および携帯電話機１０２のRAM１１３には、それぞれ、同一のアプリケーションデータAPDが保持されている。また、携帯電話機１０１のNVRAM１１４には、後述する管理テーブルT1および暗号化データd1が記憶（保存）され、携帯電話機１０２のNVRAM１１４には、後述する管理テーブルT1および暗号化データd2が記憶されるようになる。
【００７９】
図６のフローチャートに戻り、ステップＳ１５において、携帯電話機１０１のハンドオーバ制御部２０６は、第２通信制御部２０８を制御して、携帯電話機１０２との間に第２通信を確立する。一方、ステップＳ４５において、携帯電話機１０２のハンドオーバ制御部２０６は、第２通信制御部２０８を制御して、携帯電話機１０１との間に第２通信を確立する。
【００８０】
このとき、携帯電話機１０１と携帯電話機１０２とは、図７の矢印３０２で示されるように、それぞれを第２通信で接続するとともに、互いの通信相手に関する情報を含む管理テーブルT1を同期させる。
【００８１】
管理テーブルT1は、アプリケーションデータを共有して保存する装置（携帯電話機）のグループ、およびそのグループに共有され保存されるアプリケーションデータについての情報から構成されるデータ情報テーブルと、アプリケーションデータを共有して保存するグループを構成する装置についての情報から構成されるユーザ情報テーブルとに分けられる。
【００８２】
図８は、データ情報テーブルの例を示している。
【００８３】
データ情報テーブルは、アプリケーションデータを共有するグループを特定する情報で

あるGroup ID、そのグループの名称であるGroup Name、共有されるアプリケーションデータの種別を表すデータ種別、そのアプリケーションデータのファイルとしてのファイル名を表すファイル名称、そのアプリケーションデータが共有されるように分割する際に用いられるアルゴリズムを表す割符アルゴリズム、分割されたアプリケーションデータを暗号化する際に用いられるアルゴリズムを表す暗号アルゴリズム、および、分割されたアプリケーションデータが復元される際の妥当性のチェックに用いられるハッシュ値から構成される。

【００８４】

図８においては、Group IDは「１」とされ、Group Nameは「ともだち」とされ、データ種別は、写真であることを示す「Photo」とされ、ファイル名称は「箱根の写真」とされている。また、割符アルゴリズムは「単純ｎ分割完全秘密分散法」とされ、暗号アルゴリズムは「3DES（Data Encription Standard）(トリプルDESともいう)」とされ、ハッシュ値は「389fc14d-39c06de3」とされている。

【００８５】

なお、割符アルゴリズムおよび暗号アルゴリズムは、グループ内のいずれかの装置において予め設定されていてもよいし、また、ユーザによって設定されるようにしてもよい。また、ハッシュ値は、例えば、第２通信が確立されたときに、RAM１１３に保持されているアプリケーションデータに基づいて得られるものとする。

【００８６】

携帯電話機１０１および携帯電話機１０２は、このようなデータ情報テーブルにより、そのグループにおいて分割して保存されるアプリケーションデータについての情報を共有することができる。

【００８７】

図９は、ユーザ情報テーブルの例を示している。

【００８８】

ユーザ情報テーブルは、自身を含む装置が属するグループを特定するGroup ID、そのグループでの通信において各装置を管理するための情報である管理ID、そのグループ内で、各装置を使用するユーザを特定するUser ID、そのユーザの名称を表すUser Name、そのユーザを表すアイコンを表示するためのファイル名を表すUser Icon、および、グループ内の各装置に保存されるアプリケーションデータのバージョンを表すRev.（Revision）から構成される。

【００８９】

図９においては、Group IDが「１」であるグループに属する２つの装置（携帯電話機１０１および携帯電話機１０２）についての情報が示されている。具体的には、携帯電話機１０１については、管理IDは「１」とされ、User IDは「89abcdef-00000001」とされ、User Nameは「たろう」とされ、User Iconは「a01.png」とされ、Rev.は「１」とされている。また、携帯電話機１０２については、管理IDは「２」とされ、User IDは「89abcdef-00000002」とされ、User Nameは「はなこ」とされ、User Iconは「a02.png」とされ、Rev.は「１」とされている。

【００９０】

この場合、管理IDが「１」である携帯電話機１０１が通信システム１００におけるマスタとされ、管理IDが「２」である携帯電話機１０２が通信システム１００におけるスレーブとされる。

【００９１】

携帯電話機１０１および携帯電話機１０２は、このようなユーザ情報テーブルにより、自身の属するグループの通信相手についての情報を共有することができる。

【００９２】

また、図６のフローチャートのステップＳ１５およびＳ４５において、第２通信が確立されたとき、携帯電話機１０１のディスプレイ２３１および携帯電話機１０２のディスプレイ２３２には、図１０に示されるように、互いの装置とアプリケーションデータを共有

して保存するか否かをそれぞれのユーザに選択を促すためのメッセージと、ユーザがアプリケーションデータを共有して保存するか否かを選択するための「はい」ボタンおよび「いいえ」ボタンが表示される。

【００９３】

ここで、携帯電話機１０１を使用するユーザである「たろう」、および、携帯電話機１０２を使用するユーザである「はなこ」の両方またはいずれかが、「いいえ」ボタンを選択した場合、図６のフローチャートの処理は終了する。

【００９４】

一方、「たろう」および「はなこ」の両方が、「はい」ボタンを選択した場合、携帯電話機１０１のディスプレイ２３１および携帯電話機１０２のディスプレイ２３２には、図１１に示されるように、「保存中・・・」というメッセージが表示され、図６のフローチャートのステップＳ１５およびＳ４５以降の処理が進められる。

【００９５】

さて、図６のフローチャートに戻り、ステップＳ１５の後、処理はステップＳ１６に進み、携帯電話機１０１のデータ分割部２０２は、RAM１１３に保持されているアプリケーションデータを、管理テーブルT1のデータ情報テーブルの割符アルゴリズムに設定されている方法で分割する。同様に、ステップＳ４５の後、処理はステップＳ４６に進み、携帯電話機１０２のデータ分割部２０２は、RAM１１３に保持されているアプリケーションデータを、管理テーブルT1のデータ情報テーブルの割符アルゴリズムに設定されている方法で分割する。例えば、図７の携帯電話機１０１および携帯電話機１０２のそれぞれのRAM１１３に保持されているアプリケーションデータAPDが、白抜きの四角形で示される部分（データ）と、網かけの四角形で示される部分（データ）とに分割される。

【００９６】

ステップＳ１７において、携帯電話機１０１の暗号化部２０３は、分割したアプリケーションデータのうちの一方を、携帯電話機１０２から送信（供給）されてきた鍵Ｂで、管理テーブルT1のデータ情報テーブルの暗号アルゴリズムに設定されている方法で暗号化する。具体的には、図７の矢印３０３に示されるように、携帯電話機１０１において分割されたアプリケーションデータAPDのうちの、白抜きの四角形で示されるデータが鍵Ｂで暗号化される。このとき、白抜きの四角形で示されるデータには、管理テーブルT1のデータ情報テーブルに設定されているハッシュ値が付与されて、そのデータが暗号化される。暗号化されたデータ（暗号化データd1）は、NVRAM１１４に供給され、保存（記憶）される。

【００９７】

ステップＳ１８において、携帯電話機１０１の暗号化部２０３は、ステップＳ１７における暗号化で用いた鍵Ｂを消去する。このとき、暗号化部２０３は、分割されたアプリケーションデータのうちの、ステップＳ１７において暗号化されなかったデータ（図７の網かけの四角形で示される部分）も、鍵Ｂとともに消去する。

【００９８】

そして、ステップＳ１９において、携帯電話機１０１の乱数発生部２０１は、図７の矢印３０４に示されるように、ステップＳ１２で生成した鍵ＡをNVRAM１１４に供給し、保存（記憶）させる。

【００９９】

一方、ステップＳ４７において、携帯電話機１０２の暗号化部２０３は、分割したアプリケーションデータのうちの他方を、携帯電話機１０１から送信（供給）されてきた鍵Ａで、管理テーブルT1のデータ情報テーブルの暗号アルゴリズムに設定されている方法で暗号化する。具体的には、図７の矢印３０５に示されるように、携帯電話機１０２において分割されたアプリケーションデータAPDのうちの、網かけの四角形で示されるデータが鍵Ａで暗号化される。このとき、網かけの四角形で示されるデータには、管理テーブルT1のデータ情報テーブルに設定されているハッシュ値が付与されて、そのデータが暗号化される。暗号化されたデータ（暗号化データd2）は、NVRAM１１４に供給され、保存（記憶）

される。

【０１００】

ステップＳ４８において、携帯電話機１０２の暗号化部２０３は、ステップＳ４７における暗号化で用いた鍵Ａを消去する。このとき、暗号化部２０３は、分割されたアプリケーションデータのうちの、ステップＳ４７において暗号化されなかったデータ（図７の白抜きの四角形で示される部分）も、鍵Ａとともに消去する。

【０１０１】

そして、ステップＳ４９において、携帯電話機１０２の乱数発生部２０１は、図７の矢印３０６に示されるように、ステップＳ４２で生成した鍵ＢをNVRAM１１４に供給し、保存（記憶）させる。

【０１０２】

以上の処理によれば、通信システム１００においては、携帯電話機１０１および携帯電話機１０２のそれぞれに保持されているアプリケーションデータが同じように分割され、分割されたデータが携帯電話機１０１と携帯電話機１０２とに分散された上で、それぞれの通信相手によって生成された暗号鍵で暗号化されて保存される。これにより、通信システム１００で共有されたアプリケーションデータを復元する場合、携帯電話機１０１および携帯電話機１０２のいずれか一方だけでは、暗号化されたデータを復号することも、復号後のデータから元のアプリケーションデータを復元することもできない。また、通信システム１００においては、携帯電話機１０１および携帯電話機１０２は、第１通信から第２通信にハンドオーバしてデータを授受するようになされている。したがって、より便利かつより安全にデータを保存することが可能となる。

【０１０３】

以上においては、通信システム１００において、アプリケーションデータを共有して保存する処理について説明してきたが、以下においては、保存されたアプリケーションデータを復元する処理について説明する。

【０１０４】

［通信システムにおけるデータの復元について］

上述したデータ保存処理によって、携帯電話機１０１および携帯電話機１０２のNVRAM１１４に、アプリケーションデータが分割（分散）されて保存されている場合、ユーザにより所定の操作がされると、例えば、図１２に示されるように、携帯電話機１０１のディスプレイ２３１および携帯電話機１０２のディスプレイ２３２には、携帯電話機１０１および携帯電話機１０２それぞれに記憶されている管理テーブルT1のデータ情報テーブルおよびユーザ情報テーブルに基づいて、自身の属するグループの名称「ともだち」、そのグループに属する装置を使用するユーザ（「たろう」および「はなこ」）を表すアイコン、および共有されているアプリケーションデータのファイルとしてのファイル名「箱根の写真」と、ユーザがそのアプリケーションデータを復元するための接続（通信の開始）を指示するためのGUIとしての「接続」ボタンとが表示される。

【０１０５】

なお、図１２においては、自身のユーザを表すアイコンには、そのアイコンを強調させる枠が表示されている。すなわち、携帯電話機１０１のディスプレイ２３１においては、携帯電話機１０１のユーザである「たろう」を表すアイコンに枠が表示され、携帯電話機１０２のディスプレイ２３２においては、携帯電話機１０２のユーザである「はなこ」を表すアイコンに枠が表示されている。

【０１０６】

図１２の状態から、携帯電話機１０１および携帯電話機１０２の両方が「接続」ボタンを選択すると、携帯電話機１０１のディスプレイ２３１および携帯電話機１０２のディスプレイ２３２には、図１３に示されるように、それぞれのユーザに、自身の筐体を通信相手の筐体に近接または接触させることを促すメッセージが表示される。すなわち、携帯電話機１０１のディスプレイ２３１には、携帯電話機１０１の筐体を携帯電話機１０２の筐体に近接または接触させることを促す「「はなこ」さんとタッチしてください。」という

メッセージが表示され、携帯電話機１０２のディスプレイ２３２には、携帯電話機１０２の筐体を携帯電話機１０１の筐体に近接または接触させることを促す「「たろう」さんとタッチしてください。」というメッセージが表示される。

【０１０７】

そして、図１３に示される状態から、携帯電話機１０１の筐体と携帯電話機１０２の筐体とが近接または接触されると、通信システム１００において、携帯電話機１０１と携帯電話機１０２とが分散して保存しているデータを復元するデータ復元処理が実行される。

【０１０８】

［データ復元処理について］

そこで、図１４のフローチャートを参照して、通信システム１００における携帯電話機１０１および携帯電話機１０２のデータ復元処理について説明する。

【０１０９】

ステップＳ１１１において、携帯電話機１０１のハンドオーバ制御部２０６は、第１通信制御部２０７を制御して、携帯電話機１０２との間に第１通信を確立する。一方、ステップＳ１４１において、携帯電話機１０２のハンドオーバ制御部２０６は、第１通信制御部２０７を制御して、携帯電話機１０１との間に第１通信を確立する。

【０１１０】

第１通信が確立されると、ステップＳ１１２において、携帯電話機１０１の第１通信制御部２０７は、第１通信部１４１を制御して、NVRAM１１４に記憶されている鍵Ａを携帯電話機１０２に送信する。一方、ステップＳ１４２において、携帯電話機１０２の第１通信制御部２０７は、第１通信部１４１を制御して、携帯電話機１０１から送信されてくる鍵Ａを受信する。

【０１１１】

また、ステップＳ１４３において、携帯電話機１０２の第１通信制御部２０７は、第１通信部１４１を制御して、NVRAM１１４に記憶されている鍵Ｂを携帯電話機１０１に送信する。一方、ステップＳ１１３において、携帯電話機１０１の第１通信制御部２０７は、第１通信部１４１を制御して、携帯電話機１０２から送信されてくる鍵Ｂを受信する。

【０１１２】

すなわち、図１５の矢印３１１に示されるように、携帯電話機１０１のNVRAM１１４に保存されている鍵Ａは携帯電話機１０２に供給され、携帯電話機１０２のNVRAM１１４に保存されている鍵Ｂは携帯電話機１０１に供給される。

【０１１３】

図１４は、携帯電話機１０１と携帯電話機１０２との間のデータの授受について説明する図である。

【０１１４】

図１４に示されるように、携帯電話機１０１のNVRAM１１４には、管理テーブルT1および暗号化データd1が記憶され、携帯電話機１０２のNVRAM１１４には、管理テーブルT1および暗号化データd2が記憶されている。また、携帯電話機１０１のRAM１１３には、後述する復号データD1が保持され、携帯電話機１０２のRAM１１３には、後述する復号データD2が保持されるようになる。

【０１１５】

図６のフローチャートに戻り、ステップＳ１１４において、携帯電話機１０１の復号部２０４は、NVRAM１１４に記憶されている暗号化データを、携帯電話機１０２から送信（供給）されてきた鍵Ｂで、管理テーブルT1のデータ情報テーブルの暗号アルゴリズムに設定されている方法で復号する。具体的には、図１５の矢印３１２に示されるように、携帯電話機１０１のNVRAM１１４に記憶されている暗号化データd1が鍵Ｂで復号される。復号されたデータ（復号データD1）は、RAM１１３に供給され、保持される。このとき、暗号化データd1に付与されていたハッシュ値も、復号データD1とともにRAM１１３に保持される。

【０１１６】

一方、ステップＳ１４４において、携帯電話機１０２の復号部２０４は、NVRAM１１４に記憶されている暗号化データを、携帯電話機１０１から送信（供給）されてきた鍵Ａで、管理テーブルT1のデータ情報テーブルの暗号アルゴリズムに設定されている方法で復号する。具体的には、図１５の矢印３１３に示されるように、携帯電話機１０２のNVRAM１１４に記憶されている暗号化データd2が鍵Ａで復号される。復号されたデータ（復号データD2）は、RAM１１３に供給され、保持される。このとき、暗号化データd2に付与されていたハッシュ値も、復号データD2とともにRAM１１３に保持される。

【０１１７】

ステップＳ１１５において、携帯電話機１０１のハンドオーバ制御部２０６は、第２通信制御部２０８を制御して、携帯電話機１０２との間に第２通信を確立する。一方、ステップＳ１４５において、携帯電話機１０２のハンドオーバ制御部２０６は、第２通信制御部２０８を制御して、携帯電話機１０１との間に第２通信を確立する。

【０１１８】

このとき、携帯電話機１０１と携帯電話機１０２とは、図１５の矢印３１４で示されるように、それぞれを第２通信で接続するとともに、管理テーブルT1を同期させる。

【０１１９】

第２通信が確立されると、管理テーブルT1のユーザ情報テーブルにおいて、管理IDの数字が大きい装置が、管理IDの数字が小さい装置に対して、復号データを送信する。

【０１２０】

すなわち、ステップＳ１４６において、管理IDが「２」である携帯電話機１０２（スレーブ）の第２通信制御部２０８は、第２通信部１４２を制御して、図１５の矢印３１５に示されるように、RAM１１３に保持されている復号データD2を、管理IDが「１」である携帯電話機１０１（マスタ）に送信する。一方、ステップＳ１１６において、携帯電話機１０１の第２通信制御部２０８は、第２通信部１４２を制御して、携帯電話機１０２から送信されてくる復号データD2を受信する。

【０１２１】

復号データD2を受信した携帯電話機１０１のデータ復元部２０５は、RAM１１３に保持されている復号データD1と、携帯電話機１０２から受信した復号データD2とから、管理テーブルT1のデータ情報テーブルの割符アルゴリズムに設定されているアルゴリズムに対応する方法で、アプリケーションデータAPDを復元する。このとき、データ復元部２０５は、RAM１１３に保持されているハッシュ値に基づいて、復元されたアプリケーションデータAPDの妥当性をチェックする。これにより、信頼性の高いアプリケーションデータAPDを復元することができる。

【０１２２】

なお、ステップＳ１１７において、携帯電話機１０１のデータ復元部２０５がアプリケーションデータAPDの復元を開始すると、携帯電話機１０１のディスプレイ２３１には、図１６の左側に示されるように、グループ「ともだち」に属する「たろう」および「はなこ」が使用する装置それぞれに分散され保存されていたデータが復元中であることを表す画像が表示される。そして、アプリケーションデータAPDの復元が完了されると、携帯電話機１０１のディスプレイ２３１には、図１６の右側に示されるように、アプリケーションデータAPDの復元が完了したことを示すメッセージ「復元完了」と、復元されたデータ（画像）が表示される。

【０１２３】

アプリケーションデータの復元が完了されると、ステップＳ１１８において、携帯電話機１０１の第２通信制御部２０８は、第２通信部１４２を制御し、図１５の矢印３１６に示されるように、復元されたアプリケーションデータAPDを、携帯電話機１０２に送信する。一方、ステップＳ１４７において、携帯電話機１０２の第２通信制御部２０８は、第２通信部１４２を制御して、携帯電話機１０２から送信されてくるアプリケーションデータAPDを受信する。

【０１２４】

以上の処理によれば、通信システム１００において、携帯電話機１０１と携帯電話機１０２とに分散されて保存されたアプリケーションデータが、それぞれの通信相手が有する暗号鍵で復号され、復号データのそれぞれからアプリケーションデータが復元される。このように、アプリケーションデータ保存時に、アプリケーションデータを分散させて保存した装置が揃わない限り、そのデータを復元することができない。したがって、より安全に、分散されて保存されたデータを復元することが可能となる。

【０１２５】

以上においては、２台の装置から構成される通信システムにおいて、データを分散して保存する構成について説明してきたが、３台以上の装置から構成される通信システムにおいて、データを分散して保存させるようにすることもできる。

【０１２６】

以下においては、３台以上の装置から構成される通信システムにおいて、データを分散して保存する構成について説明する。

【０１２７】

＜２．第２の実施の形態＞

［通信システムの他の構成例について］

図１７は、通信システムの他の構成例を示す図である。図１７において、通信システム４００は、複数の装置間で無線通信を行わせ、データの授受を行い、そのデータに基づいてアプリケーションを実行するシステムである。図１７に示されるように、通信システム４００は、例えば、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２を有する。

【０１２８】

なお、図１７において、装置Ａ１０１は、図１の通信システム１００における携帯電話機１０１と同一であるので、同一の符号を付するものとする。そして、装置Ａ１０１の内部の構成例および機能構成例は、図２および図３を参照して説明した構成と同一であり、装置Ａ１０１の通信相手となる装置Ｂ４０１および装置Ｃ４０２の内部の構成例および機能構成例も、図２および図３を参照して説明した携帯電話機１０１の構成と基本的に同様の構成を有するので、装置Ｂ４０１および装置Ｃ４０２の構成についての説明は省略する。

【０１２９】

通信システム４００においては、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２は、それぞれ、上述した第１通信と第２通信の２つの方法で互いに通信を行う。

【０１３０】

［通信システムにおけるデータの保存について］

次に、通信システム４００におけるデータの保存について説明する。

【０１３１】

通信システム４００において、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２は、互いに通信を行うことにより、アプリケーションデータを共有して保存することができる。

【０１３２】

例えば、装置Ａ１０１のRAM１１３に、所定のアプリケーションデータが保持されているとする。装置Ａ１０１のディスプレイ２３１には、図１８の左側に示されるように、装置Ａ１０１に保持されているアプリケーションデータ（表データ）により表示される画像と、ユーザがそのアプリケーションデータの保存を指示するためのGUIとしての「保存」ボタンとが表示される。

【０１３３】

図１８の左側の状態から、装置Ａ１０１のユーザが、「保存」ボタンを選択すると、装置Ａ１０１のディスプレイ２３１には、図１８の中央に示されるように、アプリケーションデータの保存先をユーザに確認させるためのメッセージ「どこに保存しますか？」と、その保存先の候補を選択させるための「ＳＤメモリ」ボタンおよび「共有メモリ」ボタンとが表示される。

【０１３４】
ここで、装置Ａ１０１のユーザが「ＳＤメモリ」ボタンを選択した場合、装置Ａ１０１のRAM１１３に保持されているアプリケーションデータは、装置Ａ１０１のNVRAM１１４に保存される。一方、装置Ａ１０１のユーザが「共有メモリ」ボタンを選択した場合、装置Ａ１０１のディスプレイ２３１には、図１８の右側に示されるように、アプリケーションデータを共有する装置の数をユーザに選択させるためのメッセージ「何人で共有しますか？」と、共有されて保存されたアプリケーションデータを復元するのに必要な装置の数をユーザに選択させるためのメッセージ「データの復元に何人必要ですか？」とが表示される。また、それぞれのメッセージの下側には、ユーザが、そのメッセージに対する入力を行うための、例えばテキストボックス（またはドロップダウンリスト）等が表示される。図１８において、それぞれのテキストボックスには、「３人」と入力されているので、３台の装置でアプリケーションデータが共有され、そのアプリケーションデータは、３台の装置によって復元されるようになる。

【０１３５】
アプリケーションデータを共有する装置の数、および、共有されたアプリケーションデータを復元する装置の数がユーザにより入力（決定）されると、装置Ａ１０１のディスプレイ２３１には、図１９の左側に示されるように、「１人目にタッチしてください」というメッセージが表示され、装置Ａ１０１のユーザに、装置Ａ１０１の筐体を、装置Ｂ４０１および装置Ｃ４０２のいずれか一方の筐体に近接または接触させることを促す。

【０１３６】
そして、例えば、装置Ａ１０１の筐体と装置Ｂ４０１の筐体とが近接または接触されると、通信システム４００において、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２がデータを共有して保存するデータ保存処理が実行される。

【０１３７】
［データ保存処理について］
図２０および図２１のフローチャートを参照して、通信システム４００における装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２のデータ保存処理について説明する。

【０１３８】
ステップＳ３１１において、装置Ａ１０１の乱数発生部２０１は、乱数を発生することで、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２のそれぞれで使用される暗号鍵である鍵Ａ，Ｂ，Ｃを生成する。ここでは、鍵Ａは装置Ａ１０１に使用され、鍵Ｂは装置Ｂ４０１に使用され、鍵Ｃは装置Ｃ４０２に使用されるものとする。

【０１３９】
鍵Ａ，Ｂ，Ｃが生成されると、ステップＳ３１２において、装置Ａ１０１のハンドオーバ制御部２０６は、第１通信制御部２０７を制御して、装置Ｂ４０１との間に第１通信を確立する。一方、ステップＳ３４１において、装置Ｂ４０１のハンドオーバ制御部２０６は、第１通信制御部２０７を制御して、装置Ａ１０１との間に第１通信を確立する。

【０１４０】
装置Ａ１０１と装置Ｂ４０１との間で第１通信が確立されると、ステップＳ３１３において、装置Ａ１０１の第１通信制御部２０７は、第１通信部１４１を制御して、乱数発生部２０１において生成された鍵Ａ，Ｂ，Ｃを装置Ｂ４０１に送信する。一方、ステップＳ３４２において、装置Ｂ４０１の第１通信制御部２０７は、第１通信部１４１を制御して、装置Ａ１０１から送信されてくる鍵Ａ，Ｂ，Ｃを受信する。

【０１４１】
ここで、図２２を参照して、装置Ａ１０１から第１通信により送信される鍵を表す鍵データについて説明する。

【０１４２】
鍵データは、送信される鍵それぞれの情報を表すKey部、鍵の送信元となる装置（以下、単に、送信元という）のユーザの情報を表すMy User Information部、および、送信元と鍵Ａ，Ｂ，Ｃの送信先となる装置（以下、単に、送信先という）との間で行われる第２

通信についての情報である2ndキャリア部の、大きく３つの情報部から構成される。

【０１４３】

Key部は、送信される鍵それぞれのデータから構成され、図２２においては、鍵Ａは「000102030405060708090a0b0c0d0e0f」、鍵Ｂは「0101020304050607080 90a0b0c0d0e0f」、鍵Ｃは「02010203040506070 8090a0b0c0d0e0f」で示されている。

【０１４４】

My User Information部は、そのユーザの名称を表すUser Nameと、そのユーザを特定するUser IDとから構成され、図２２においては、User Nameは「たろう」とされ、User IDは「01234567-00000001」とされている。

【０１４５】

そして、2ndキャリア部は、第２通信の通信方式（通信方法）を表す方法、鍵データの送信元が第２通信においてマスタであるかスレーブであるかを表す機器種別、および、第２通信における送信元の識別情報であるアドレスから構成される。図２２においては、方法は、Bluetoothバージョン2.0を表す「BT2.0」とされ、種別は、マスタを表す「Master」とされ、アドレスは「fedcba9876543210」とされる。

【０１４６】

図２０のフローチャートに戻り、ステップＳ３４３において、装置Ｂ４０１の第１通信制御部２０７は、受信した鍵Ａ，Ｂ，Ｃの鍵データが正しいか否かを判定する。

【０１４７】

ステップＳ３４３において、受信した鍵Ａ，Ｂ，Ｃの鍵データが正しくないと判定された場合、装置Ｂ４０１は、送信元である装置Ａ１０１に対して、鍵Ａ，Ｂ，Ｃの再送信を要求し、処理はステップＳ３４２に戻る。そして、受信した鍵Ａ，Ｂ，Ｃの鍵データが正しいと判定されるまで、ステップＳ３４２およびステップＳ３４３の処理が繰り返される。

【０１４８】

一方、ステップＳ３４３において、受信した鍵Ａ，Ｂ，Ｃの鍵データが正しいと判定された場合、装置Ｂ４０１は、送信元である装置Ａ１０１に対して、鍵データが正しかった旨の情報を送信し、処理は、後述するステップＳ３４４に進む。

【０１４９】

さて、ステップＳ３１３の後、装置Ａ１０１が装置Ｂ４０１から鍵データが正しかった旨の情報を受信すると、装置Ａ１０１のディスプレイ２３１には、図１９の右側に示されるように、「２人目にタッチしてください」というメッセージが表示され、装置Ａ１０１のユーザに、装置Ａ１０１の筐体を装置Ｃ４０２の筐体に近接または接触させることを促す。

【０１５０】

そして、装置Ａ１０１の筐体と装置Ｃ４０２の筐体とが近接または接触されると、ステップＳ３１４において、装置Ａ１０１のハンドオーバ制御部２０６は、第１通信制御部２０７を制御して、装置Ｃ４０２との間に第１通信を確立する。一方、ステップＳ３７１において、装置Ｃ４０２のハンドオーバ制御部２０６は、第１通信制御部２０７を制御して、装置Ａ１０１との間に第１通信を確立する。

【０１５１】

装置Ａ１０１と装置Ｃ４０２との間で第１通信が確立されると、ステップＳ３１５において、装置Ａ１０１の第１通信制御部２０７は、第１通信部１４１を制御して、鍵Ａ，Ｂ，Ｃを装置Ｃ４０２に送信する。一方、ステップＳ３７２において、装置Ｃ４０２の第１通信制御部２０７は、第１通信部１４１を制御して、装置Ａ１０１から送信されてくる鍵Ａ，Ｂ，Ｃを受信する。

【０１５２】

ここでも、図２２を参照して説明した鍵データが、装置Ａ１０１から装置Ｃ４０２に送信される。

【０１５３】

そして、ステップＳ３７３において、装置Ｃ４０２の第１通信制御部２０７は、受信した鍵Ａ，Ｂ，Ｃの鍵データが正しいか否かを判定する。

【０１５４】

ステップＳ３７３において、受信した鍵Ａ，Ｂ，Ｃの鍵データが正しくないと判定された場合、装置Ｃ４０２は、送信元である装置Ａ１０１に対して、鍵Ａ，Ｂ，Ｃの再送信を要求し、処理はステップＳ３７２に戻る。そして、受信した鍵Ａ，Ｂ，Ｃの鍵データが正しいと判定されるまで、ステップＳ３７２およびステップＳ３７３の処理が繰り返される。

【０１５５】

一方、ステップＳ３７３において、受信した鍵Ａ，Ｂ，Ｃの鍵データが正しいと判定された場合、装置Ｃ４０２は、送信元である装置Ａ１０１に対して、鍵データが正しかった旨の情報を送信し、処理は、後述するステップＳ３７４に進む。

【０１５６】

さて、ステップＳ３１５の後、装置Ａ１０１が装置Ｃ４０２から鍵データが正しかった旨の情報を受信すると、ステップＳ３１６において、装置Ａ１０１のハンドオーバ制御部２０６は、第２通信制御部２０８を制御して、装置Ｂ４０１および装置Ｃ４０２との間に第２通信を確立する。

【０１５７】

一方、ステップＳ３４４において、装置Ｂ４０１のハンドオーバ制御部２０６は、第２通信制御部２０８を制御して、装置Ａ１０１との間に第２通信を確立する。また、ステップＳ３７４において、装置Ｃ４０２のハンドオーバ制御部２０６は、第２通信制御部２０８を制御して、装置Ａ１０１との間に第２通信を確立する。

【０１５８】

このとき、装置Ａ１０１と装置Ｂ４０１および装置Ｃ４０２とは、互いを第２通信で接続して、それぞれのNVRAM１１４に記憶されている管理テーブルT1を同期させるための情報を授受することにより、管理テーブルT1を同期させる。なお、装置Ａ１０１と装置Ｂ４０１および装置Ｃ４０２とが、既に第２通信で接続されている場合には、管理テーブルT1を同期させるための情報の授受、および、管理テーブルT1の同期が行われる。

【０１５９】

まず、装置Ａ１０１と装置Ｂ４０１および装置Ｃ４０２とは、それぞれのユーザを表すユーザ情報の授受を行う。具体的には、装置Ａ１０１は、図２３の左側のユーザ情報User A Informationを、装置Ｂ４０１および装置Ｃ４０２に送信する。ユーザ情報UserA Informationは、装置Ａ１０１のユーザの名称を表すUser Name「たろう」およびそのユーザを特定するUser ID「01234567-00000001」から構成されている。

【０１６０】

また、装置Ｂ４０１は、図２３の中央のユーザ情報UserB Informationを、装置Ａ１０１に送信し、装置Ｃ４０２は、図２３の右側のユーザ情報UserC Informationを、装置Ａ１０１に送信する。ユーザ情報UserB Informationは、装置Ｂ４０１のユーザの名称を表すUser Name「もも」およびそのユーザを特定するUser ID「01234567-00000002」から構成され、ユーザ情報UserC Informationは、装置Ｃ４０２のユーザの名称を表すUser Name「てつじ」およびそのユーザを特定するUser ID「01234567-00000003」から構成されている。

【０１６１】

装置Ａ１０１は、装置Ｂ４０１からユーザ情報を受信すると、装置Ｂ４０１からのユーザ情報を装置Ｃ４０２に送信し、装置Ｃ４０２からユーザ情報を受信すると、装置Ｃ４０２からのユーザ情報を装置Ｂ４０１に送信する。これにより、図２３に示される装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２それぞれのユーザについてのユーザ情報が、各装置によって共有されるようになる。

【０１６２】

次に、装置Ａ１０１は、RAM１１３に保持されていて、装置Ａ１０１、装置Ｂ４０１、

および装置Ｃ４０２に共有されて保存されるアプリケーションデータについてのアプリケーションデータ情報を、装置Ｂ４０１および装置Ｃ４０２に送信する。具体的には、装置Ａ１０１は、図２４に示されるアプリケーションデータ情報を、装置Ｂ４０１および装置Ｃ４０２に送信する。

【０１６３】

アプリケーションデータ情報は、図２４に示されるように、グループ内の各装置に保存されるアプリケーションデータのバージョンを表すData Revision、そのグループの名称であるGroup Name、共有されるアプリケーションデータの種別を表すデータ種別、そのアプリケーションデータのファイルとしてのファイル名を表すファイル名称、そのアプリケーションデータが共有されるように分割する際に用いられるアルゴリズムを表す割符アルゴリズム、および、分割されたアプリケーションデータを暗号化する際に用いられるアルゴリズムを表す暗号アルゴリズムから構成される。

【０１６４】

図２４においては、Data Revisionは「１」とされ、Group Nameは「テニスサークル」とされ、データ種別は、文字データであることを示す「Text」とされ、ファイル名称は「住所録」とされている。また、割符アルゴリズムは「単純ｎ分割完全秘密分散法」とされ、暗号アルゴリズムは「AES（Advanced Encryption Standard）128bit」とされている。

【０１６５】

このようなアプリケーションデータ情報が、装置Ａ１０１から装置Ｂ４０１および装置Ｃ４０２に送信されることにより、図２４に示されるアプリケーションデータ情報が、各装置によって共有されるようになる。

【０１６６】

そして、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２は、上述したユーザ情報およびアプリケーションデータ情報に基づいて、それぞれのNVRAM１１４に記憶されている管理テーブルT1を同期させる。

【０１６７】

具体的には、図２３を参照して説明したユーザ情報に基づいて、管理テーブルT1のユーザ情報テーブルが同期される。

【０１６８】

図２５は、装置Ａ１０１のNVRAM１１４に記憶されているユーザ情報テーブルの例を示している。

【０１６９】

上述したように、装置Ａ１０１は、図１の通信システム１００の携帯電話器１０１と同一であるので、図２５のユーザ情報テーブルにおいては、図９を参照して説明した情報に加え、Group IDが「２」であるグループに属する３つの装置としての装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２についての情報が示されている。具体的には、装置Ａ１０１については、管理IDは「１」とされ、User IDは「01234567-00000001」とされ、User Nameは「たろう」とされ、User Iconは「b01.png」とされ、Rev.は「１」とされている。装置Ｂ４０１については、管理IDは「２」とされ、User IDは「01234567-00000002」とされ、User Nameは「もも」とされ、User Iconは「b02.png」とされ、Rev.は「１」とされている。また、装置Ｃ４０２については、管理IDは「３」とされ、User IDは「01234567-00000003」とされ、User Nameは「てつじ」とされ、User Iconは「b03.png」とされ、Rev.は「１」とされている。この場合、管理IDが「１」である装置Ａ１０１が通信システム４００におけるマスタとされ、管理IDが「２」である装置Ｂ４０１および管理IDが「３」である装置Ｃ４０２が通信システム４００におけるスレーブとされる。

【０１７０】

なお、装置Ｂ４０１および装置Ｃ４０２のユーザ情報テーブルにおいては、少なくとも、Group IDが「２」であるグループに属する３つの装置についての情報が含まれるようになる。

【０１７１】

装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２は、このようなユーザ情報テーブルにより、自身の属するグループの通信相手についての情報を共有することができる。

【０１７２】

また、上述したアプリケーションデータ情報に基づいて、管理テーブルT1のデータ情報テーブルが同期される。

【０１７３】

図２６は、装置Ａ１０１のNVRAM１１４に記憶されているデータ情報テーブルの例を示している。

【０１７４】

図２６のデータ情報テーブルにおいては、図９を参照して説明した情報に加え、Group IDが「２」であるグループに属する３つの装置としての装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２により共有されるアプリケーションデータについての情報が示されている。具体的には、Group IDは「２」とされ、Group Nameは「テニスサークル」とされ、データ種別は、文字データであることを示す「Text」とされ、ファイル名称は「住所録」とされている。また、割符アルゴリズムは「単純ｎ分割完全秘密分散法」とされ、暗号アルゴリズムは「AES128bit」とされ、ハッシュ値は「154359a5-52abca12」とされている。

【０１７５】

なお、装置Ｂ４０１および装置Ｃ４０２のデータ情報テーブルにおいては、少なくともGroup IDが「２」であるグループに属する３つの装置により共有されるアプリケーションデータについての情報が含まれるようになる。

【０１７６】

装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２は、このようなデータ情報テーブルにより、そのグループにおいて分割して保存されるアプリケーションデータについての情報を共有することができる。

【０１７７】

図２１のフローチャートに戻り、ステップＳ３４５において、装置Ｂ４０１の第２通信制御部２０８は、装置Ａ１０１から受信したデータ（ユーザ情報およびアプリケーションデータ情報）が正しいか否かを判定する。

【０１７８】

ステップＳ３４５において、受信したデータが正しくないと判定された場合、装置Ｂ４０１は、装置Ａ１０１に対して、データの再送信を要求し、処理はステップＳ３４４に戻る。そして、受信したデータが正しいと判定されるまで、ステップＳ３４４およびステップＳ３４５の処理が繰り返される。

【０１７９】

一方、ステップＳ３４５において、受信したデータが正しいと判定された場合、装置Ｂ４０１は、送信元である装置Ａ１０１に対して、データが正しかった旨の情報を送信し、処理は、後述するステップＳ３４６に進む。

【０１８０】

また、ステップＳ３７５において、装置Ｃ４０２の第２通信制御部２０８は、装置Ａ１０１から受信したデータが正しいか否かを判定する。

【０１８１】

ステップＳ３７５において、受信したデータが正しくないと判定された場合、装置Ｃ４０２は、装置Ａ１０１に対して、データの再送信を要求し、処理はステップＳ３７４に戻る。そして、受信したデータが正しいと判定されるまで、ステップＳ３７４およびステップＳ３７５の処理が繰り返される。

【０１８２】

一方、ステップＳ３７５において、受信したデータが正しいと判定された場合、装置Ｃ４０２は、送信元である装置Ａ１０１に対して、データが正しかった旨の情報を送信し、処理は、後述するステップＳ３７６に進む。

【０１８３】

そして、ステップＳ３１７において、装置Ａ１０１の第２通信制御部２０８は、装置Ｂ４０１および装置Ｃ４０２から送信されてくる情報に基づいて、装置Ｂ４０１および装置Ｃ４０２からのレスポンスがＯＫであるか否かを判定する。

【０１８４】

ステップＳ３１７において、レスポンスがＯＫではないと判定された場合、すなわち、装置Ｂ４０１および装置Ｃ４０２から送信されてくる情報のうち、少なくともいずれかがデータの再送信を要求する内容である場合、処理はステップＳ３１６に戻り、装置Ｂ４０１および装置Ｃ４０２それぞれから、データが正しかった旨の情報が送信されるまで、ステップＳ３１６およびステップＳ３１７の処理が繰り返される。

【０１８５】

一方、ステップＳ３１７において、レスポンスがＯＫであると判定された場合、処理はＳ３１８に進み、装置Ａ１０１のデータ分割部２０２は、RAM１１３に保持されているアプリケーションデータを、管理テーブルT1のデータ情報テーブルの割符アルゴリズムに設定されている方法で分割する。

【０１８６】

例えば、装置Ａ１０１のデータ分割部２０２は、RAM１１３に保持されているアプリケーションデータを、単純ｎ分割完全秘密分散法で分割する。

【０１８７】

具体的には、図２７に示されるように、装置Ａ１０１のデータ分割部２０２は、アプリケーションデータAPDをデータ１乃至９に分割し、そのうちのデータ１，４，７、データ２，５，８、データ３，６，９を、それぞれ１まとまりの分割データとする。

【０１８８】

ステップＳ３１９において、装置Ａ１０１の第２通信制御部２０８は、第２通信部１４２を制御して、データ分割部２０２によって分割されたアプリケーションデータ（分割データ）を、装置Ｂ４０１および装置Ｃ４０２に送信する。具体的には、装置Ｂ４０１には、図２７で説明した分割データのうちのデータ２，５，８からなる分割データが送信され、装置Ｃ４０２には、図２７で説明した分割データのうちのデータ３，６，９からなる分割データが送信される。

【０１８９】

そして、ステップＳ３４６において、装置Ｂ４０１の第２通信制御部２０８は、第２通信部１４２を制御して、装置Ａ１０１から送信されてくる分割データを受信する。また、ステップＳ３７６において、装置Ｃ４０２の第２通信制御部２０８は、第２通信部１４２を制御して、装置Ａ１０１から送信されてくる分割データを受信する。

【０１９０】

分割データを装置Ｂ４０１および装置Ｃ４０２に送信した装置Ａ１０１の暗号化部２０３は、ステップＳ３２０において、分割したアプリケーションデータ（分割データ）を、鍵Ａで、管理テーブルT1のデータ情報テーブルの暗号アルゴリズムに設定されている方法で暗号化する。具体的には、図２７に示されるように、データ１，４，７からなる分割データD1（平文）が鍵Ａで暗号化される。このとき、分割データD1には、分割データD1に基づいて得られるハッシュ値が付与されて、そのデータが暗号化される。暗号化されたデータ１’，４’，７’からなる暗号化データd1（暗号文）は、NVRAM１１４に供給され、保存（記憶）される。

【０１９１】

ステップＳ３２１において、装置Ａ１０１の暗号化部２０３は、ステップＳ３２０における暗号化で用いた鍵Ａを消去する。

【０１９２】

そして、ステップＳ３２２において、装置Ａ１０１の乱数発生部２０１は、ステップＳ３１１で生成した鍵Ａ，Ｂ，Ｃのうち、暗号化に使用されていない鍵Ｂ，ＣをNVRAM１１４に供給し、保存（記憶）させる。

【０１９３】

一方、装置Ａ１０１からの分割データを受信した装置Ｂ４０１の暗号化部２０３は、ステップＳ３４７において、装置Ａ１０１からの、分割されたアプリケーションデータ（分割データ）を、鍵Ｂで、管理テーブルT1のデータ情報テーブルの暗号アルゴリズムに設定されている方法で暗号化する。具体的には、図２７に示されるように、データ２，５，８からなる分割データD2（平文）が鍵Ｂで暗号化される。このとき、分割データD2には、分割データD2に基づいて得られるハッシュ値が付与されて、そのデータが暗号化される。暗号化されたデータ２’，５’，８’からなる暗号化データd2（暗号文）は、NVRAM１１４に供給され、保存（記憶）される。

【０１９４】

ステップＳ３４８において、装置Ｂ４０１の暗号化部２０３は、ステップＳ３４７における暗号化で用いた鍵Ｂを消去する。

【０１９５】

そして、ステップＳ３４９において、装置Ｂ４０１の第１通信制御部２０７は、ステップＳ３４２で受信した鍵Ａ，Ｂ，Ｃのうち、暗号化に使用されていない鍵Ｃ，ＡをNVRAM１１４に供給し、保存（記憶）させる。

【０１９６】

さらに、装置Ａ１０１からの分割データを受信した装置Ｃ４０２の暗号化部２０３は、ステップＳ３７７において、装置Ａ１０１からの、分割されたアプリケーションデータ（分割データ）を、鍵Ｃで、管理テーブルT1のデータ情報テーブルの暗号アルゴリズムに設定されている方法で暗号化する。具体的には、図２７に示されるように、データ３，６，９からなる分割データD3（平文）が鍵Ｃで暗号化される。このとき、分割データD3には、分割データD3に基づいて得られるハッシュ値が付与されて、そのデータが暗号化される。暗号化されたデータ３’，６’，９’からなる暗号化データd3（暗号文）は、NVRAM１１４に供給され、保存（記憶）される。

【０１９７】

ステップＳ３７８において、装置Ｃ４０２の暗号化部２０３は、ステップＳ３７７における暗号化で用いた鍵Ｃを消去する。

【０１９８】

そして、ステップＳ３７９において、装置Ｃ４０２の第１通信制御部２０７は、ステップＳ３７２で受信した鍵Ａ，Ｂ，Ｃのうち、暗号化に使用されていない鍵Ａ，ＢをNVRAM１１４に供給し、保存（記憶）させる。

【０１９９】

以上の処理によれば、通信システム４００においては、装置Ａ１０１に保持されているアプリケーションデータが分割され、分割されたアプリケーションデータが装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２に分散された上で、それぞれの装置において暗号化されて保存される。また、それぞれの装置で使用された暗号鍵は、暗号化後に消去される。これにより、通信システム４００で共有されたアプリケーションデータを復元する場合、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２の全てが揃わない限り、暗号化されたデータを復号することも、復号後のデータから元のアプリケーションデータを復元することもできない。また、通信システム４００においては、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２は、第１通信から第２通信にハンドオーバしてデータを授受するようになされている。したがって、より便利かつより安全にデータを保存することが可能となる。

【０２００】

なお、上述した説明においては、アプリケーションデータを分割する際に、割符アルゴリズムとして完全秘密分散法を用いているので、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２の全てが揃わない限り、元のアプリケーションデータを復元することができない。すなわち、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２のいずれか１つが破壊される等した場合、元のアプリケーションデータを復元することは完全に不可能になってしまう。

【０２０１】
そこで、割符アルゴリズムとして、分割データのいくつかが揃えば元のアプリケーションデータを復元することができる、k-out-of-nしきい値秘密分散法を用いるようにしてもよい。ここで、ｎは分散させる分割データの数を表し、ｋはデータの復元に必要な分割データの数を表している。ｎ，ｋは、図１８の右側に示されるディスプレイ２３１に表示される入力画面において、ユーザにより決定されるようにできる。
【０２０２】
図２８は、2-out-of-3しきい値秘密分散法を用いた秘密分散処理および暗号化処理について説明する図である。
【０２０３】
図２８においては、アプリケーションデータAPDは、2-out-of-3しきい値秘密分散法で、３つのデータ１乃至３に分割される。データ１である分割データD1（平文）は、装置Ａ１０１において、ハッシュ値が付与され、鍵Ａで暗号化され、暗号化されたデータ１’である暗号化データd1（暗号文）が保存される。データ２である分割データD2（平文）は、装置Ｂ４０１において、ハッシュ値が付与され、鍵Ｂで暗号化され、暗号化されたデータ２’である暗号化データd2（暗号文）が保存される。また、データ３である分割データD3（平文）は、装置Ｃ４０２において、ハッシュ値が付与され、鍵Ｃで暗号化され、暗号化されたデータ３’である暗号化データd3（暗号文）が保存される。
【０２０４】
図２８における分割データD1乃至D3は、2-out-of-3しきい値秘密分散法で分割されているので、元のアプリケーションデータを復元する場合、３つの分割データのうち、２つの分割データがあれば、元のアプリケーションデータを復元することができる。また、通信システム４００においては、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２は、それぞれ、自身で使用した暗号鍵以外の暗号鍵を全て保存しているので、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２のいずれか１つが破壊される等した場合であっても、元のアプリケーションデータを復元することができるようになる。したがって、可用性高く、より安全にデータを保存することが可能となる。
【０２０５】
なお、上述した説明においては、アプリケーションデータは、装置Ａ１０１によって分割されるものとしたが、装置Ａ１０１がアプリケーションデータを分割する前に装置Ｂ４０１および装置Ｃ４０２に送信するようにして、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２のそれぞれがアプリケーションデータを分割し、対応する分割データのみを、それぞれが暗号化するようにしてもよい。
【０２０６】
以上においては、通信システム４００において、アプリケーションデータを共有して保存する処理について説明してきたが、以下においては、保存されたアプリケーションデータを復元する処理について説明する。
【０２０７】
［通信システムにおけるデータの復元について］
上述したデータ保存処理によって、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２のNVRAM１１４に、アプリケーションデータが分散されて保存されている場合、ユーザにより所定の操作がされると、例えば、図２９に示されるように、装置Ａ１０１のディスプレイ２３１、装置Ｂ４０１のディスプレイ４３１、および装置Ｃ４０２のディスプレイ４３２には、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２それぞれに記憶されている管理テーブルのデータ情報テーブルおよびユーザ情報テーブルに基づいて、自身の属するグループの名称「テニスサークル」、そのグループに属する装置を使用するユーザ（「たろう」、「もも」、および「てつじ」）を表すアイコン、および共有されているアプリケーションデータのファイルとしてのファイル名「住所録」と、ユーザがそのアプリケーションデータを復元するための接続（通信の開始）を指示するためのGUIとしての「接続」ボタンとが表示される。

【０２０８】
なお、図２９においては、自身のユーザを表すアイコンには、そのアイコンを強調させる枠が表示されている。すなわち、装置Ａ１０１のディスプレイ２３１においては、装置Ａ１０１のユーザである「たろう」を表すアイコンに枠が表示され、装置Ｂ４０１のディスプレイ４３１においては、装置Ｂ４０１のユーザである「もも」を表すアイコンに枠が表示され、装置Ｃ４０２のディスプレイ４３２においては、装置Ｃ４０２のユーザである「てつじ」を表すアイコンに枠が表示されている。
【０２０９】
さらに、それぞれの装置のユーザのアイコンが表示されている下側には、それぞれの装置自身の筐体を、他の装置の筐体に近接または接触させることを促す「「接続」ボタンを押し、タッチしてください。」というメッセージが表示されている。
【０２１０】
そして、図２９に示される状態から、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２それぞれのユーザが「接続」ボタンを選択し、例えば、装置Ａ１０１の筐体と装置Ｂ４０１の筐体とが近接または接触されると、通信システム４００において、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２が分散して保存しているデータを復元するデータ復元処理が実行される。
【０２１１】
［データ復元処理について］
図３０および図３１のフローチャートを参照して、通信システム４００における装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２のデータ復元処理について説明する。
【０２１２】
ステップＳ４１１において、装置Ａ１０１のハンドオーバ制御部２０６は、第１通信制御部２０７を制御して、装置Ｂ４０１との間に第１通信を確立する。一方、ステップＳ４４１において、装置Ｂ４０１のハンドオーバ制御部２０６は、第１通信制御部２０７を制御して、装置Ａ１０１との間に第１通信を確立する。
【０２１３】
第１通信が確立されると、図３２に示されるように、装置Ａ１０１のディスプレイ２３１には、装置Ａ１０１のユーザである「たろう」を表すアイコンと、装置Ｂ４０１のユーザである「もも」を表すアイコンとの間に、第１通信が確立したことを示すラインが表示される。同様に、装置Ｂ４０１のディスプレイ４３１には、装置Ｂ４０１のユーザである「もも」を表すアイコンと、装置Ａ１０１のユーザである「たろう」を表すアイコンとの間に、第１通信が確立したことを示すラインが表示される。
【０２１４】
ステップＳ４１２において、装置Ａ１０１の第１通信制御部２０７は、第１通信部１４１を制御して、NVRAM１１４に記憶されている鍵Ｂ，Ｃを装置Ｂ４０１に送信する。一方、ステップＳ４４２において、装置Ｂ４０１の第１通信制御部２０７は、第１通信部１４１を制御して、装置Ａ１０１から送信されてくる鍵Ｂ，Ｃを受信する。
【０２１５】
ここで、装置Ａ１０１から装置Ｂ４０１に送信される鍵を表す鍵データは、図３３の上側に示されるような構成となる。この鍵データは、基本的には図２２を参照して説明した鍵データと同様の構成とされるが、Key部においては、装置Ａ１０１において暗号化後に消去された鍵Ａのデータが存在しない。
【０２１６】
図３０のフローチャートに戻り、ステップＳ４４３において、装置Ｂ４０１の第１通信制御部２０７は、受信した鍵Ｂ，Ｃの鍵データが正しいか否かを判定する。
【０２１７】
ステップＳ４４３において、受信した鍵Ｂ，Ｃの鍵データが正しくないと判定された場合、装置Ｂ４０１は、送信元である装置Ａ１０１に対して、鍵Ｂ，Ｃの再送信を要求し、処理はステップＳ４４２に戻る。そして、受信した鍵Ｂ，Ｃの鍵データが正しいと判定さ

れるまで、ステップＳ４４２およびステップＳ４４３の処理が繰り返される。

【０２１８】

一方、ステップＳ４４３において、受信した鍵Ｂ，Ｃの鍵データが正しいと判定された場合、装置Ｂ４０１は、送信元である装置Ａ１０１に対して、鍵データが正しかった旨の情報を送信し、処理はステップＳ４４４に進む。

【０２１９】

ステップＳ４４４において、装置Ｂ４０１の第１通信制御部２０７は、第１通信部１４１を制御して、NVRAM１１４に記憶されている鍵Ｃ，Ａを装置Ａ１０１に送信する。一方、ステップＳ４１３において、装置Ａ１０１の第１通信制御部２０７は、第１通信部１４１を制御して、装置Ｂ４０１から送信されてくる鍵Ｃ，Ａを受信する。

【０２２０】

ここで、装置Ｂ４０１から装置Ａ１０１に送信される鍵を表す鍵データは、図３３の下側に示されるような構成となる。この鍵データは、My User Information部において、User Nameが「もも」、User IDが「01234567-00000002」とされ、2ndキャリア部において、種別が、スレーブを表す「Slave」とされている他、Key部においては、装置Ｂ４０１において暗号化後に消去された鍵Ｂのデータが存在しない。

【０２２１】

装置Ａ１０１と装置Ｂ４０１との間で鍵が授受された後、装置Ａ１０１の筐体と装置Ｃ４０２の筐体とが近接または接触されると、ステップＳ４１４において、装置Ａ１０１のハンドオーバ制御部２０６は、第１通信制御部２０７を制御して、装置Ｃ４０２との間に第１通信を確立する。一方、ステップＳ４７１において、装置Ｃ４０２のハンドオーバ制御部２０６は、第１通信制御部２０７を制御して、装置Ａ１０１との間に第１通信を確立する。

【０２２２】

ステップＳ４１５において、装置Ａ１０１の第１通信制御部２０７は、第１通信部１４１を制御して、NVRAM１１４に記憶されている鍵Ｂ，Ｃを装置Ｃ４０２に送信する。一方、ステップＳ４７２において、装置Ｃ４０２の第１通信制御部２０７は、第１通信部１４１を制御して、装置Ａ１０１から送信されてくる鍵Ｂ，Ｃを受信する。

【０２２３】

ステップＳ４７３において、装置Ｃ４０２の第１通信制御部２０７は、受信した鍵Ｂ，Ｃの鍵データが正しいか否かを判定する。

【０２２４】

ステップＳ４７３において、受信した鍵Ｂ，Ｃの鍵データが正しくないと判定された場合、装置Ｃ４０２は、送信元である装置Ａ１０１に対して、鍵Ｂ，Ｃの再送信を要求し、処理はステップＳ４７２に戻る。そして、受信した鍵Ｂ，Ｃの鍵データが正しいと判定されるまで、ステップＳ４７２およびステップＳ４７３の処理が繰り返される。

【０２２５】

一方、ステップＳ４７３において、受信した鍵Ｂ，Ｃの鍵データが正しいと判定された場合、装置Ｃ４０２は、送信元である装置Ａ１０１に対して、鍵データが正しかった旨の情報を送信し、処理はステップＳ４７４に進む。

【０２２６】

ステップＳ４７４において、装置Ｃ４０２の第１通信制御部２０７は、第１通信部１４１を制御して、NVRAM１１４に記憶されている鍵Ａ，Ｂを装置Ａ１０１に送信する。一方、ステップＳ４１６において、装置Ａ１０１の第１通信制御部２０７は、第１通信部１４１を制御して、装置Ｃ４０２から送信されてくる鍵Ａ，Ｂを受信する。

【０２２７】

さて、ステップＳ４１６において、装置Ａ１０１が装置Ｃ４０２から鍵Ａ，Ｂを受信した後、ステップＳ４１７において、装置Ａ１０１のハンドオーバ制御部２０６は、第２通信制御部２０８を制御して、装置Ｂ４０１および装置Ｃ４０２との間に第２通信を確立する。

【０２２８】
ステップＳ４４５において、装置Ｂ４０１のハンドオーバ制御部２０６は、第２通信制御部２０８を制御して、装置Ａ１０１との間に第２通信を確立する。また、ステップＳ４７５において、装置Ｃ４０２のハンドオーバ制御部２０６は、第２通信制御部２０８を制御して、装置Ａ１０１との間に第２通信を確立する。
【０２２９】
このとき、装置Ａ１０１と装置Ｂ４０１および装置Ｃ４０２とは、互いを第２通信で接続して、それぞれのNVRAM１１４に記憶されている管理テーブルT1を同期させるための情報（ユーザ情報およびアプリケーションデータ情報）を授受することにより、管理テーブルT1を同期させる。なお、装置Ａ１０１と装置Ｂ４０１および装置Ｃ４０２とが、既に第２通信で接続されている場合には、管理テーブルT1を同期させるための情報の授受、および、管理テーブルT1の同期が行われる。特に、データ復元処理においては、アプリケーションデータ情報のData Revisionにより、復元しようとするアプリケーションデータのバージョンをチェックすることができる。
【０２３０】
また、装置Ａ１０１と装置Ｂ４０１および装置Ｃ４０２とが、互いに第２通信を確立している間、装置Ａ１０１のディスプレイ２３１、装置Ｂ４０１のディスプレイ４３１、および装置Ｃ４０２のディスプレイ４３２には、図３４に示されるように、それぞれのユーザのアイコンの間に、第２通信を確立することを示すラインと、「接続中・・・」のメッセージが表示される。
【０２３１】
そして、装置Ａ１０１と装置Ｂ４０１および装置Ｃ４０２とが、互いに第２通信の確立を完了させると、装置Ａ１０１のディスプレイ２３１、装置Ｂ４０１のディスプレイ４３１、および装置Ｃ４０２のディスプレイ４３２には、図３５に示されるように、「たろう」のアイコンと「もも」のアイコンの間、および、「たろう」のアイコンと「てつじ」のアイコンの間に、第２通信を確立したことを示すラインと、「接続されました」のメッセージが表示されるようになる。
【０２３２】
図３１のフローチャートに戻り、ステップＳ４４６において、装置Ｂ４０１の第２通信制御部２０８は、受信したデータ（ユーザ情報およびアプリケーションデータ情報）が正しいか否かを判定する。
【０２３３】
ステップＳ４４６において、受信したデータが正しくないと判定された場合、装置Ｂ４０１は、装置Ａ１０１に対して、データの再送信を要求し、処理はステップＳ４４５に戻る。そして、受信したデータが正しいと判定されるまで、ステップＳ４４５およびステップＳ４４６の処理が繰り返される。
【０２３４】
一方、ステップＳ４４６において、受信したデータが正しいと判定された場合、装置Ｂ４０１は、送信元である装置Ａ１０１に対して、データが正しかった旨の情報を送信し、処理は、後述するステップＳ４４７に進む。
【０２３５】
また、ステップＳ４７６において、装置Ｃ４０２の第２通信制御部２０８は、受信したデータが正しいか否かを判定する。
【０２３６】
ステップＳ４７６において、受信したデータが正しくないと判定された場合、装置Ｃ４０２は、装置Ａ１０１に対して、データの再送信を要求し、処理はステップＳ４７５に戻る。そして、受信したデータが正しいと判定されるまで、ステップＳ４７５およびステップＳ４７６の処理が繰り返される。
【０２３７】
一方、ステップＳ４７６において、受信したデータが正しいと判定された場合、装置Ｃ

４０２は、送信元である装置Ａ１０１に対して、データが正しかった旨の情報を送信し、処理は、後述するステップＳ４７７に進む。

【０２３８】

そして、ステップＳ４１８において、装置Ａ１０１の第２通信制御部２０８は、装置Ｂ４０１および装置Ｃ４０２から送信されてくる情報に基づいて、装置Ｂ４０１および装置Ｃ４０２からのレスポンスがＯＫであるか否かを判定する。

【０２３９】

ステップＳ４１８において、レスポンスがＯＫではないと判定された場合、すなわち、装置Ｂ４０１および装置Ｃ４０２から送信されてくる情報のうち、少なくともいずれかがデータの再送信を要求する内容である場合、処理はステップＳ４１７に戻り、装置Ｂ４０１および装置Ｃ４０２それぞれから、データが正しかった旨の情報が送信されるまで、ステップＳ４１７およびステップＳ４１８の処理が繰り返される。

【０２４０】

一方、ステップＳ４１８において、レスポンスがＯＫであると判定された場合、処理はステップＳ４１９に進み、装置Ａ１０１の復号部２０４は、NVRAM１１４に記憶されている暗号化データを、装置Ｂ４０１および装置Ｃ４０２から送信（供給）されてきた暗号鍵のうちの鍵Ａで、管理テーブルT1のデータ情報テーブルの暗号アルゴリズムに設定されている方法で復号する。具体的には、図３６に示されるように、装置Ａ１０１のNVRAM１１４に記憶されている暗号化データd1が鍵Ａで復号される。復号された復号データD1（平文）は、RAM１１３に供給され、保持される。このとき、復号部２０４は、暗号化データd1に付与されていたハッシュ値に基づいて、復号データD1の妥当性をチェックする。これにより、信頼性の高い復号データD1を得ることができる。

【０２４１】

また、ステップＳ４４７において、装置Ｂ４０１の復号部２０４は、NVRAM１１４に記憶されている暗号化データを、装置Ａ１０１および装置Ｃ４０２から送信（供給）されてきた暗号鍵のうちの鍵Ｂで、管理テーブルT1のデータ情報テーブルの暗号アルゴリズムに設定されている方法で復号する。具体的には、図３６に示されるように、装置Ｂ４０１のNVRAM１１４に記憶されている暗号化データd2が鍵Ｂで復号される。復号された復号データD2（平文）は、RAM１１３に供給され、保持される。このとき、復号部２０４は、暗号化データd2に付与されていたハッシュ値に基づいて、復号データD2の妥当性をチェックする。これにより、信頼性の高い復号データD2を得ることができる。

【０２４２】

ステップＳ４４８において、装置Ｂ４０１の第２通信制御部２０８は、第２通信部１４２を制御して、RAM１１３に保持されている復号データD2を、装置Ａ１０１に送信する。

【０２４３】

そして、ステップＳ４７７において、装置Ｃ４０２の復号部２０４は、NVRAM１１４に記憶されている暗号化データを、装置Ａ１０１および装置Ｂ４０１から送信（供給）されてきた暗号鍵のうちの鍵Ｃで、管理テーブルT1のデータ情報テーブルの暗号アルゴリズムに設定されている方法で復号する。具体的には、図３６に示されるように、装置Ｃ４０２のNVRAM１１４に記憶されている暗号化データd3が鍵Ｃで復号される。復号された復号データD3（平文）は、RAM１１３に供給され、保持される。このとき、復号部２０４は、暗号化データd3に付与されていたハッシュ値に基づいて、復号データD3の妥当性をチェックする。これにより、信頼性の高い復号データD3を得ることができる。

【０２４４】

ステップＳ４７８において、装置Ｃ４０２の第２通信制御部２０８は、第２通信部１４２を制御して、RAM１１３に保持されている復号データD3を、装置Ａ１０１に送信する。

【０２４５】

ステップＳ４２０において、装置Ａ１０１の第２通信制御部２０８は、第２通信部１４２を制御して、装置Ｂ４０１から送信されてくる復号データD2、および、装置Ｃ４０２から送信されてくる復号データD3を受信し、処理はステップＳ４２１に進む。

【０２４６】
ステップＳ４２１において、装置Ａ１０１のデータ復元部２０５は、RAM１１３に保持されている復号データD1、装置Ｂ４０１から受信した復号データD2、および、装置Ｃ４０２から受信した復号データD3から、管理テーブルT1のデータ情報テーブルの割符アルゴリズムに設定されているアルゴリズムに対応する方法（例えば、単純ｎ分割完全秘密分散法に対応する方法）で、アプリケーションデータAPDを復元する。
【０２４７】
具体的には、図３６に示されるように、装置Ａ１０１のデータ復元部２０５は、復号データD1をデータ１，４，７に、復号データD2をデータ２，５，８に、復号データD3をデータ３，６，９にそれぞれ分割し、分割されたデータ１乃至９から、アプリケーションデータAPDを復元する。このとき、データ復元部２０５は、管理テーブルT1のデータ情報テーブルに設定されているハッシュ値に基づいて、復元されたアプリケーションデータAPDの妥当性をチェックする。これにより、信頼性の高いアプリケーションデータAPDを復元することができる。
【０２４８】
データの復元が完了されると、ステップＳ４２２において、装置Ａ１０１の第２通信制御部２０８は、第２通信部１４２を制御し、復元されたアプリケーションデータAPDを、装置Ｂ４０１および装置Ｃ４０２に送信する。
【０２４９】
ステップＳ４４９において、装置Ｂ４０１の第２通信制御部２０８は、第２通信部１４２を制御して、装置Ａ１０１から送信されてくるアプリケーションデータAPDを受信する。また、ステップＳ４７９において、装置Ｃ４０２の第２通信制御部２０８は、第２通信部１４２を制御して、装置Ａ１０１から送信されてくるアプリケーションデータAPDを受信する。
【０２５０】
以上の処理によれば、通信システム４００において、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２に分散されて保存されたアプリケーションデータが、それぞれの装置が有する暗号鍵以外の暗号鍵で復号され、復号されたデータそれぞれからアプリケーションデータが復元される。このように、アプリケーションデータ保存時に、アプリケーションデータを分散させて共有した装置が揃わない限り、そのアプリケーションデータを復元することができない。したがって、より安全に、保存されたデータを復元することが可能となる。
【０２５１】
また、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２に分散されて保存されたアプリケーションデータが、図２８を参照して説明した2-out-of-3しきい値秘密分散法で分割されている場合には、元のアプリケーションデータを復元する場合、３つの分割データのうち、２つの分割データがあれば、元のアプリケーションデータを復元することができる。そして、通信システム４００においては、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２は、それぞれ、自身で使用した暗号鍵以外の暗号鍵を全て保存しているので、装置Ａ１０１、装置Ｂ４０１、および装置Ｃ４０２のいずれか１つが破壊される等した場合であっても、元のアプリケーションデータを復元することができる。したがって、可用性高く、より安全に、分散されて保存されたデータを復元することが可能となる。
【０２５２】
以上においては、通信システム４００において、装置Ａ１０１がマスタであり、装置Ｂ４０１および装置Ｃ４０２がスレーブであるものとしたが、いずれの装置がマスタになり、いずれの装置がスレーブになるようにしてもよい。
【０２５３】
上述した一連の処理は、ハードウェアにより実行させることもできるし、ソフトウェアにより実行させることもできる。上述した一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、ネットワークや記録媒体からインス

トールされる。

【０２５４】

この記録媒体は、例えば、図２に示されるように、装置本体とは別に、プログラムが記録されている磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROMおよびDVDを含む）、光磁気ディスク（MDを含む）、もしくは半導体メモリなどよりなるリムーバブルメディア１３１により構成されるだけでなく、装置本体に予め組み込まれた状態で提供される、プログラムが記録されているROM１１２や、記憶部１２３に含まれるハードディスクなどで構成される。

【０２５５】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２５６】

また、本明細書において、システムとは、複数のデバイス（装置）により構成される装置全体を表わすものである。

【０２５７】

なお、以上において、１つの装置として説明した構成を分割し、複数の装置として構成するようにしてもよい。逆に、以上において複数の装置として説明した構成をまとめて１つの装置として構成されるようにしてもよい。また、各装置の構成に上述した以外の構成を付加するようにしてももちろんよい。さらに、システム全体としての構成や動作が実質的に同じであれば、ある装置の構成の一部を他の装置の構成に含めるようにしてもよい。つまり、本発明の実施の形態は、上述した実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲において種々の変更が可能である。

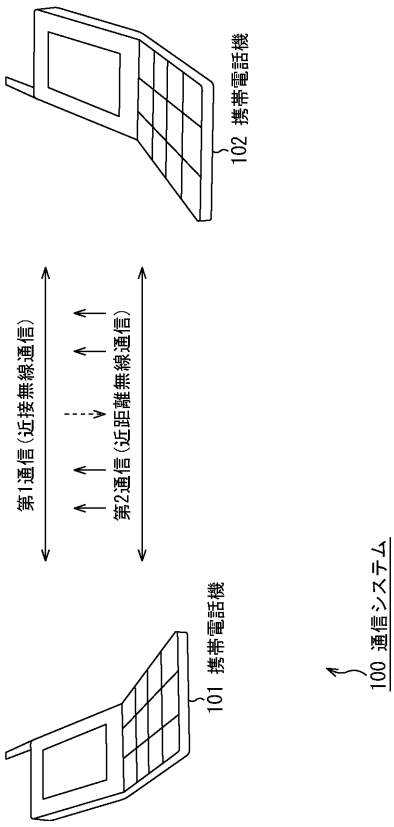
【符号の説明】

【０２５８】

１００　通信システム，　１０１　携帯電話機，　１０２　携帯電話機，　１１３　RAM，　１１４　NVRAM，　１４１　第１通信部，　１４２　第２通信部，　２０１　乱数発生部，　２０２　データ分割部，　２０３　暗号化部，　２０４　復号部，　２０５　データ復元部，　２０６　ハンドオーバ制御部，　２０７　第１通信制御部，　２０８　第２通信制御部，　４００　通信システム，　４０１　装置Ｂ，　４０２　装置Ｃ

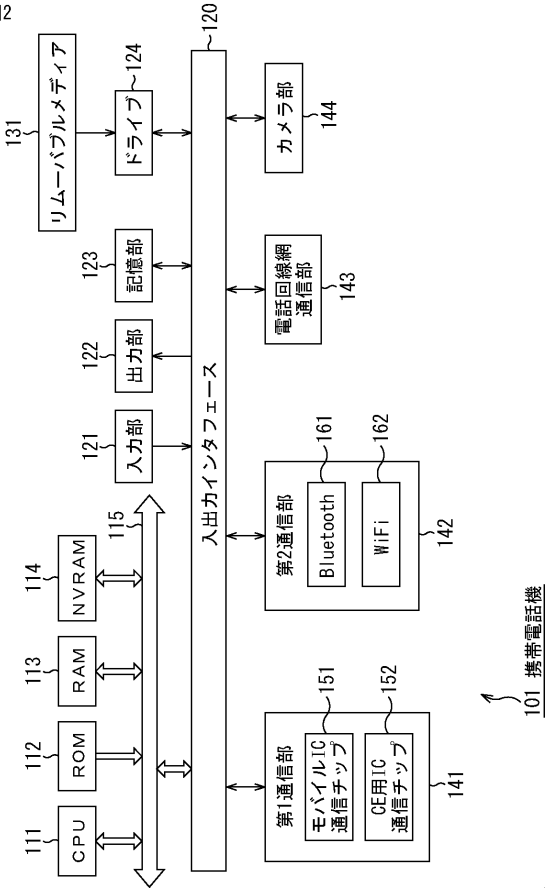
【図１】

図1



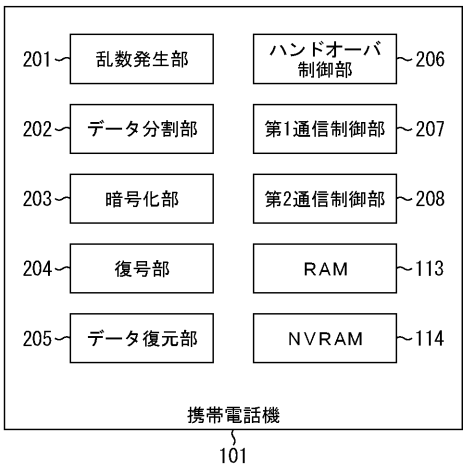
【図２】

図2



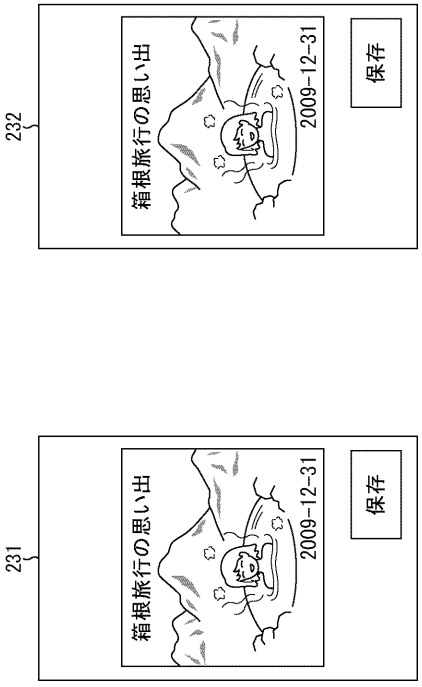
【図３】

図3

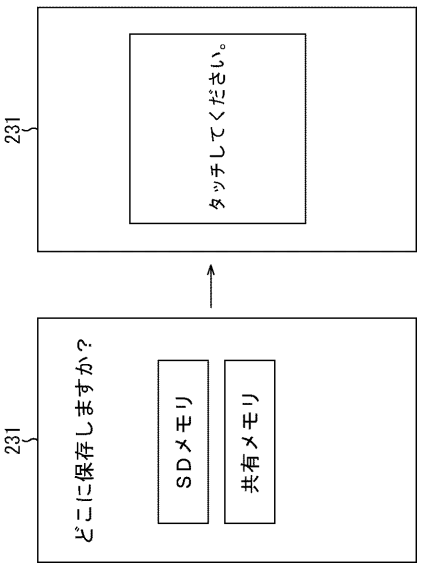


【図４】

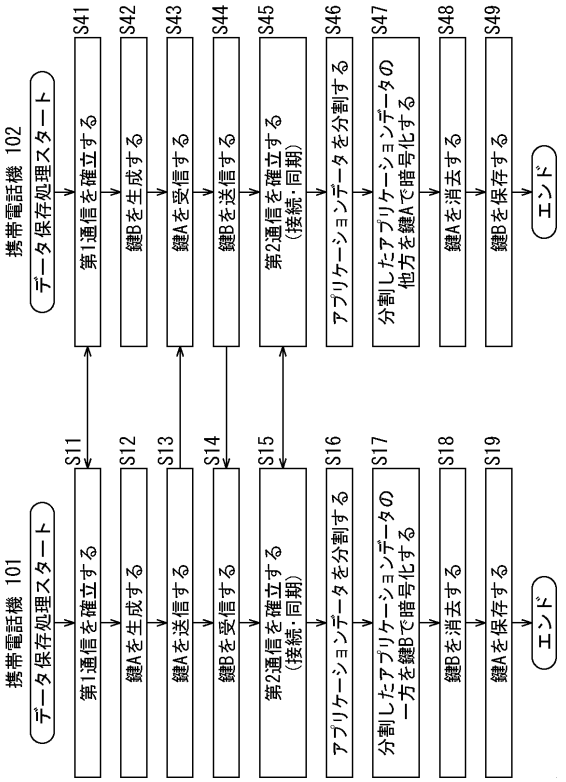
図4



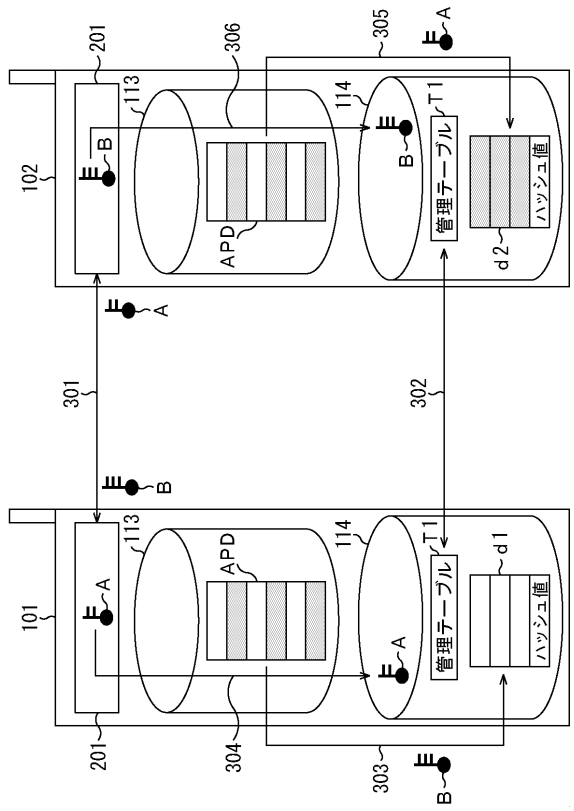
【図５】
図5



【図６】
図6



【図７】
図7



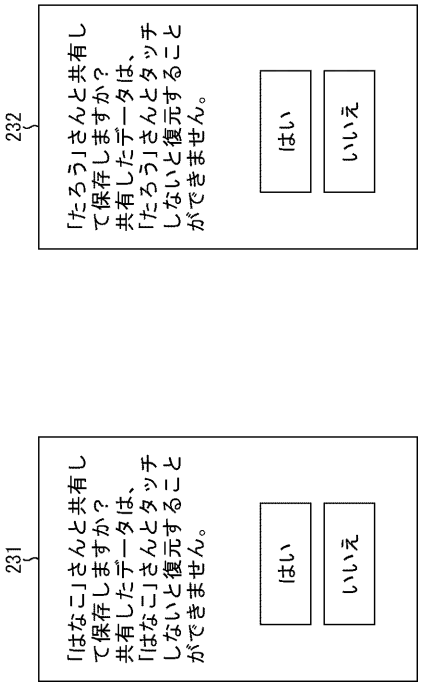
【図８】
図8

Group ID	Group Name	データ種別	ファイル名称	割符アルゴリズム	暗号アルゴリズム	ハッシュ値
1	ともだち	Photo	箱根の写真	単純n分割 完全秘密分散法	3DES	389fc14d-39c06de3

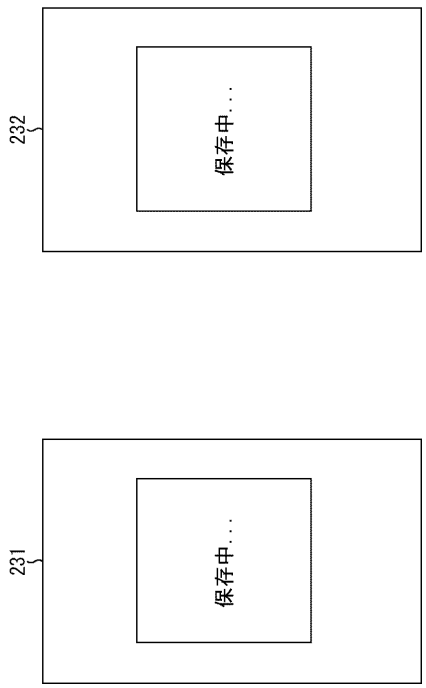
【図９】
図9

Group ID	管理ID	User ID	User Name	User Icon	Rev.
1	1	89abcdef-00000001	たろう	a01.png	1
1	2	89abcdef-00000002	はなこ	a02.png	1

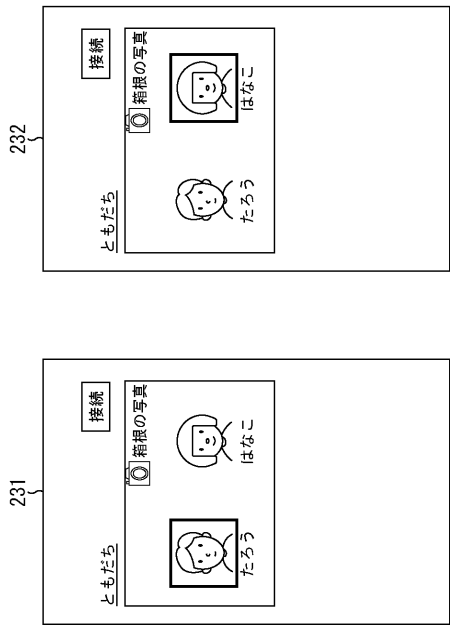
【図１０】
図10



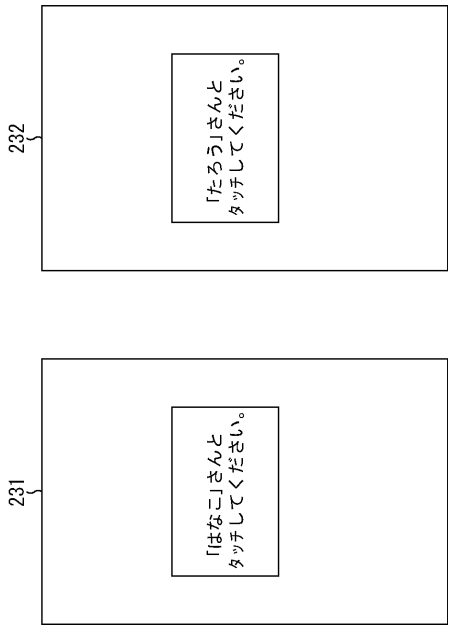
【図１１】
図11



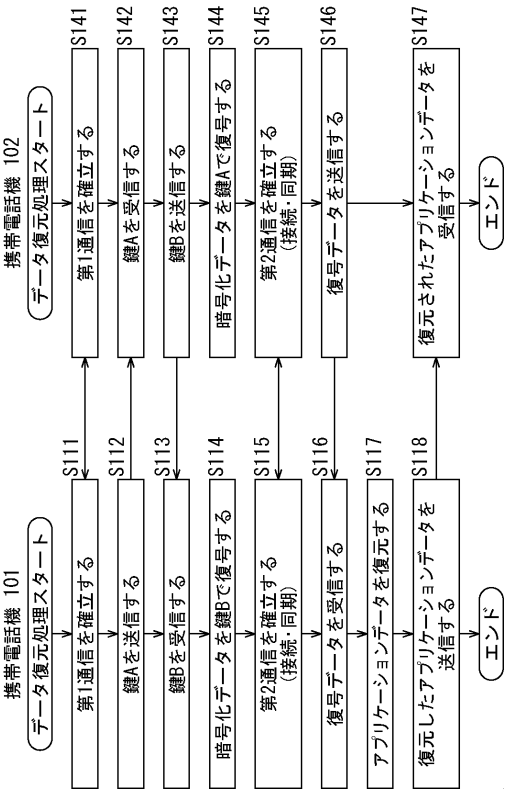
【図１２】
図12



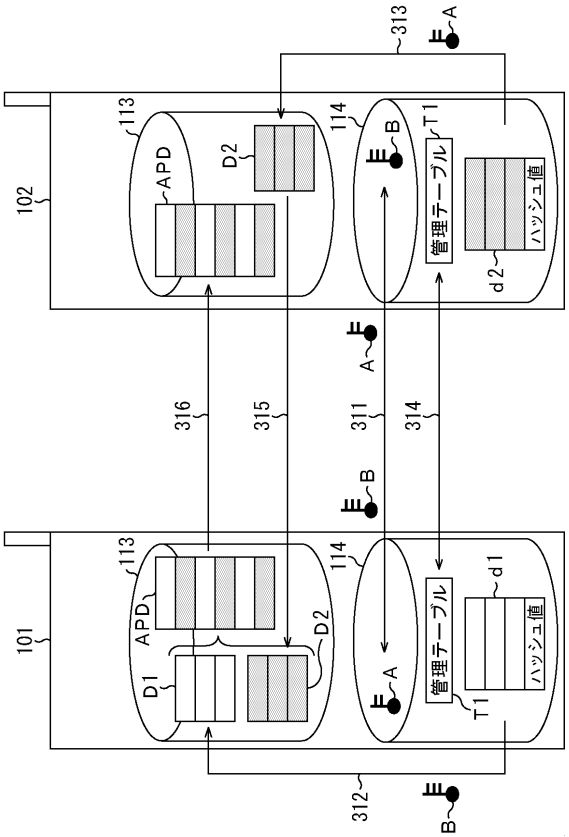
【図１３】
図13



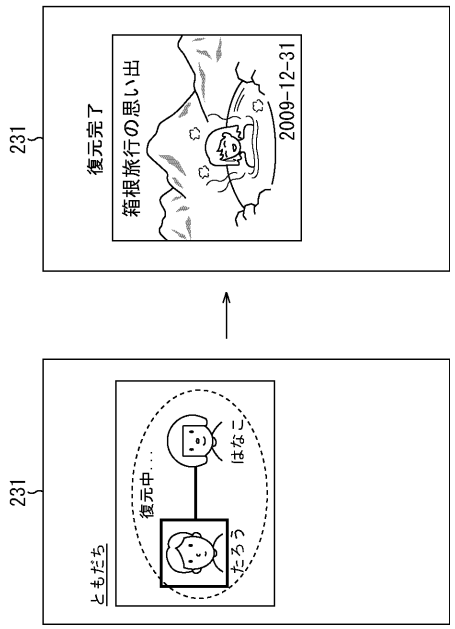
【図１４】
図14



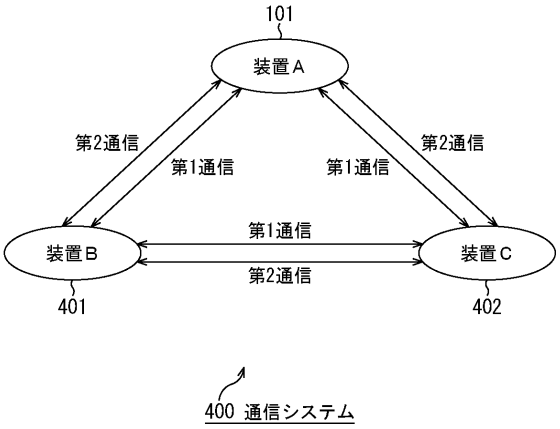
【図１５】
図15



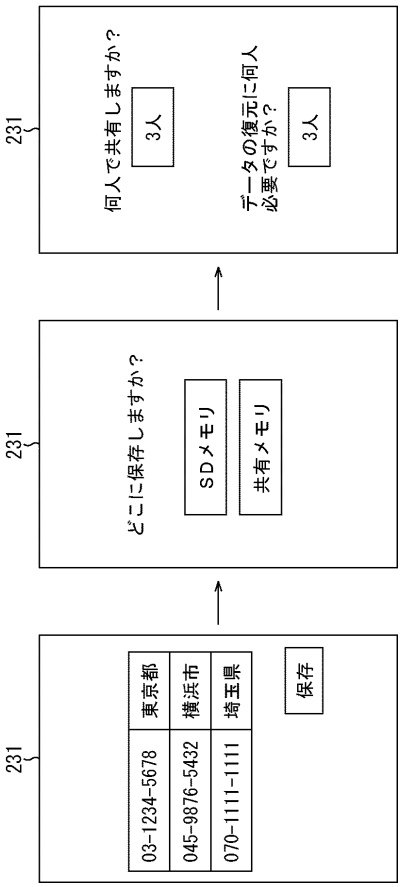
【図１６】
図16



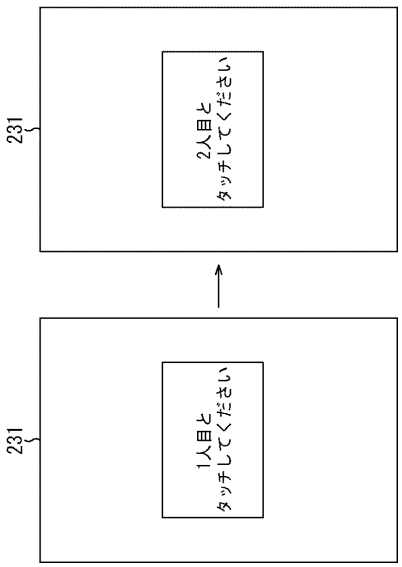
【図１７】
図17



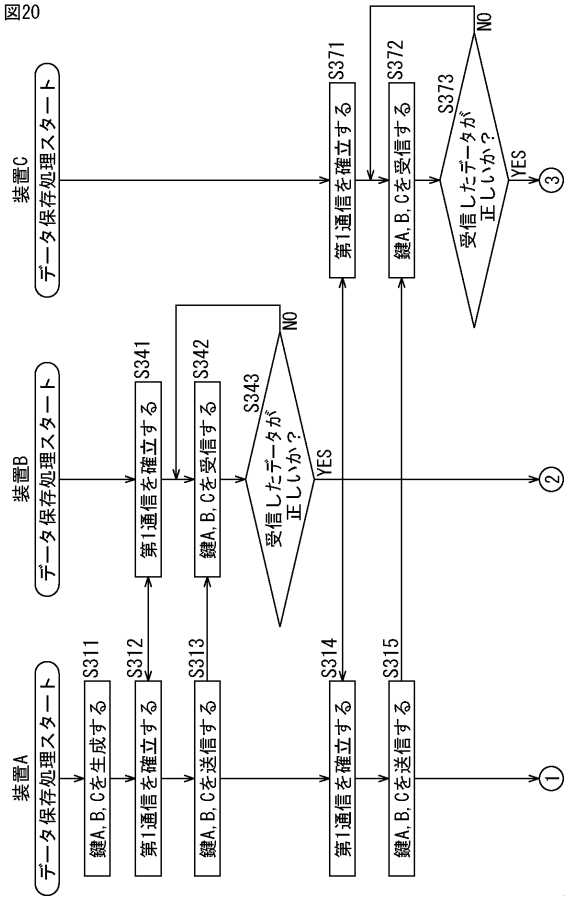
【図１８】
図18



【図１９】
図19

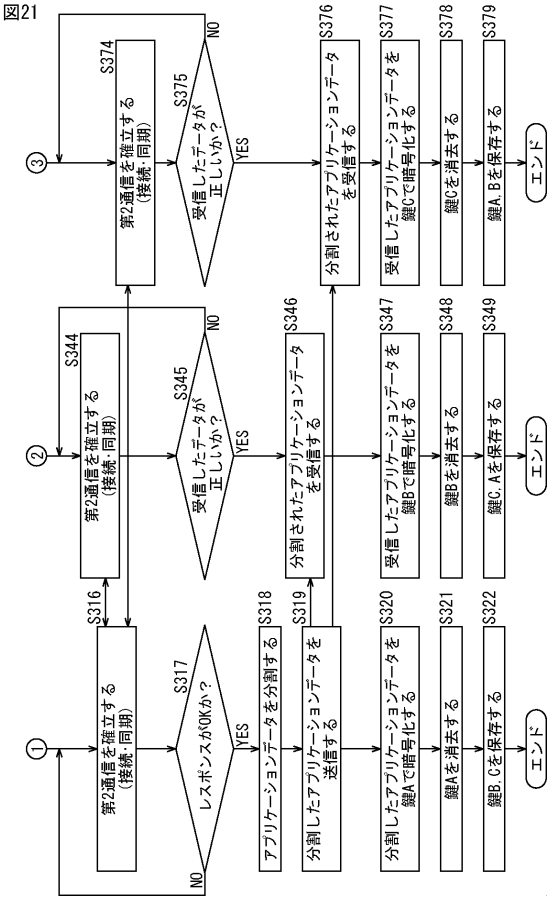


【図２０】
図20



【図２１】

図21



【図２２】

図22

Key			My User Information		2ndキャリア		
A	B	C	User Name	User ID	方法	種別	アドレス
00010203 04050607 08090a0b 0c0d0e0f	01010203 04050607 08090a0b 0c0d0e0f	02010203 04050607 08090a0b 0c0d0e0f	たろう	01234567- 00000001	BT2.0	Master	fedcba987 6543210

【図２３】

図23

UserA Information		UserB Information		UserC Information	
User Name	User ID	User Name	User ID	User Name	User ID
たろう	01234567- 00000001	もも	01234567- 00000002	てつじ	01234567- 00000003

【図２４】

図24

アプリケーションデータ情報						
Data Revision	Group Name	データ種別	ファイル名称	割符アルゴリズム	暗号アルゴリズム
1	テニスサークル	Text	住所録	単純n分割 完全秘密分散法	AES 128bit

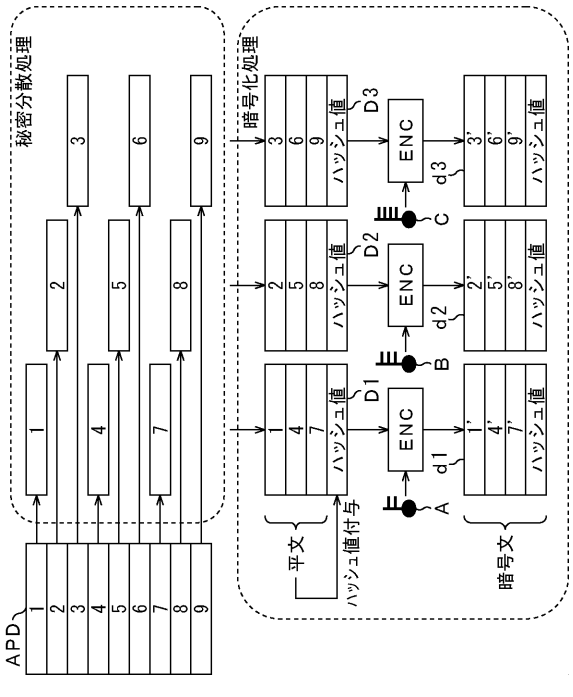
【図２５】
図25

Group ID	管理ID	User ID	User Name	User Icon	Rev.
1	1	89abcdef-00000001	たろう	a01.png	1
1	2	89abcdef-00000002	はなこ	a02.png	1
2	1	01234567-00000001	たろう	b01.png	1
2	2	01234567-00000002	もも	b02.png	1
2	3	01234567-00000003	てつじ	b03.png	1

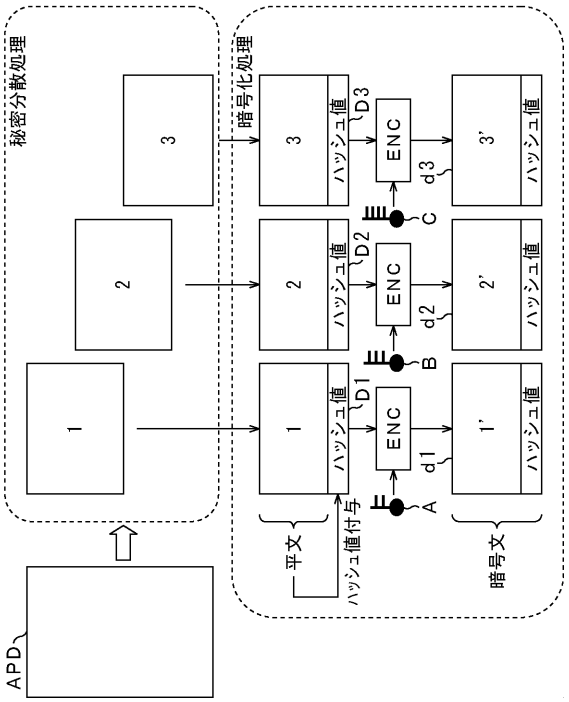
【図２６】
図26

Group ID	Group Name	データ種別	ファイル名称	割符アルゴリズム	暗号アルゴリズム	ハッシュ値
1	ともだち	Photo	箱根の写真	単純n分割 完全秘密分散法	3DES	389fc14d-39c06de3
2	テニスサークル	Text	住所録	単純n分割 完全秘密分散法	AES128bit	154359a5-52abca12

【図２７】
図27

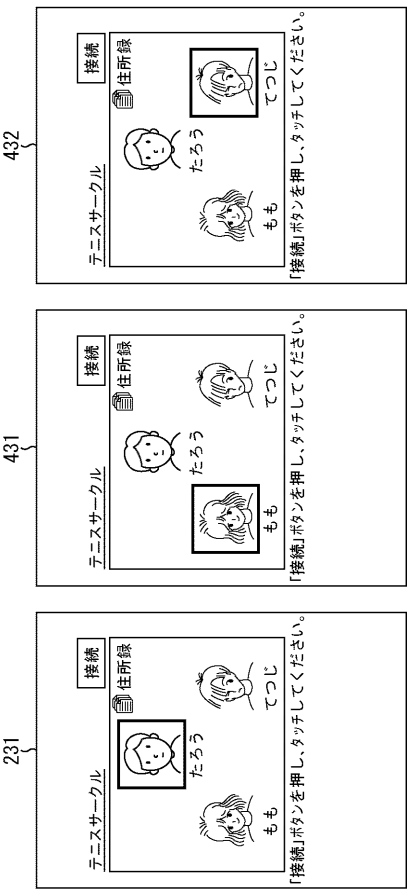


【図２８】
図28



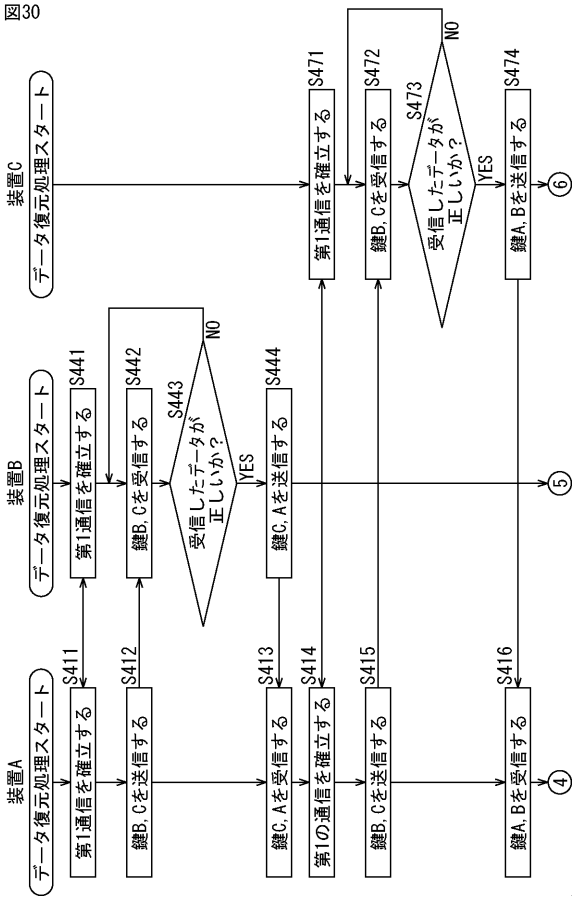
【図２９】

図29



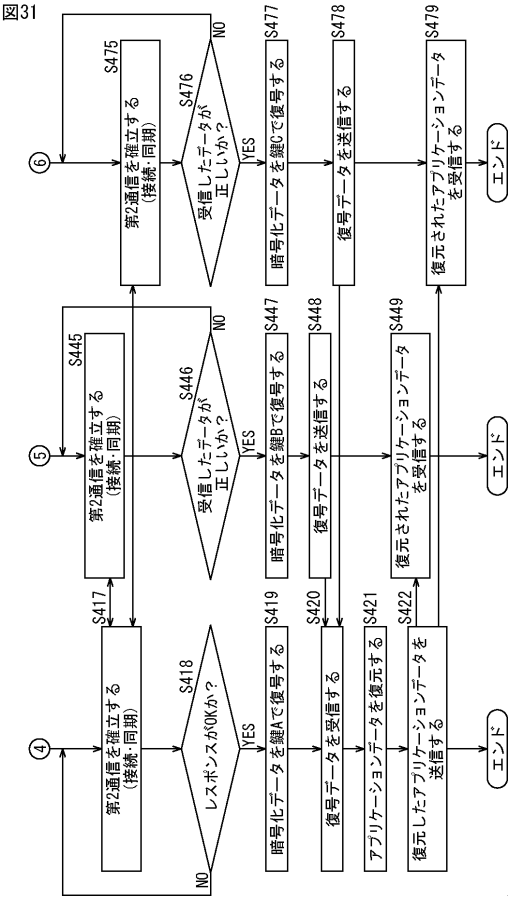
【図３０】

図30



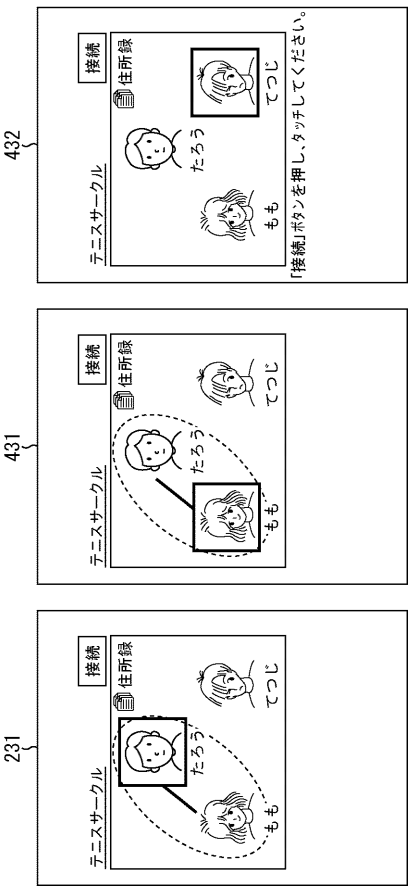
【図３１】

図31



【図３２】

図32



【図３３】

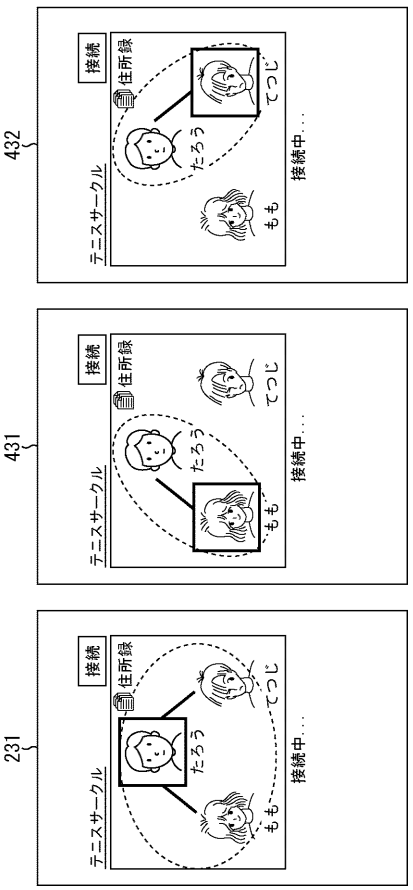
図33

Key		My User Information		2ndキャリア		
B	C	User Name	User ID	方法	種別	アドレス
01010203 04050607 08090a0b 0c0d0e0f	02010203 04050607 08090a0b 0c0d0e0f	たろう	01234567- 00000001	BT2.0	Master	fedcba98 76543210

Key		My User Information		2ndキャリア		
A	C	User Name	User ID	方法	種別	アドレス
00010203 04050607 08090a0b 0c0d0e0f	02010203 04050607 08090a0b 0c0d0e0f	もも	01234567- 00000002	BT2.0	Slave	fedcba98 76543211

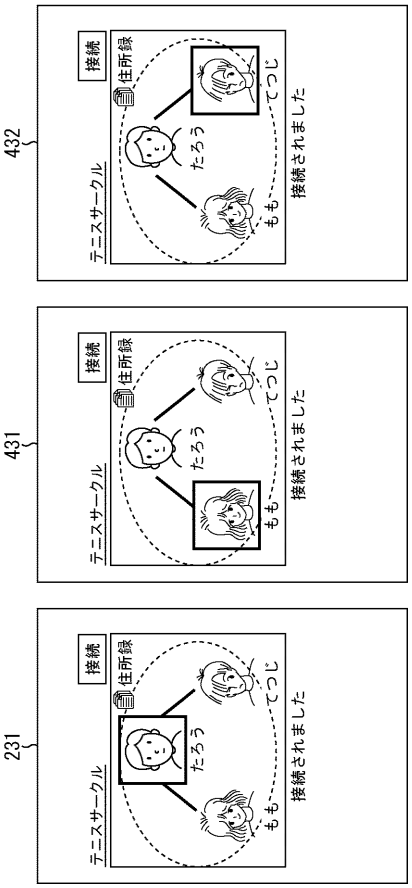
【図３４】

図34



【図３５】

図35



【図３６】

図36