(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2009-5202
(P2009-5202A)
(43)公開日　平成21年1月8日(2009.1.8)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601A	5B017
G06F 21/00	(2006.01)	H04L	9/00	601E	5B285
G06F 21/24	(2006.01)	G06F	15/00	330Z	5J104
		G06F	12/14	560Z	
		G06F	12/14	520D	

審査請求 未請求　請求項の数 9　ＯＬ　（全 23 頁）

(21)出願番号　特願2007-165789 (P2007-165789)
(22)出願日　平成19年6月25日 (2007.6.25)

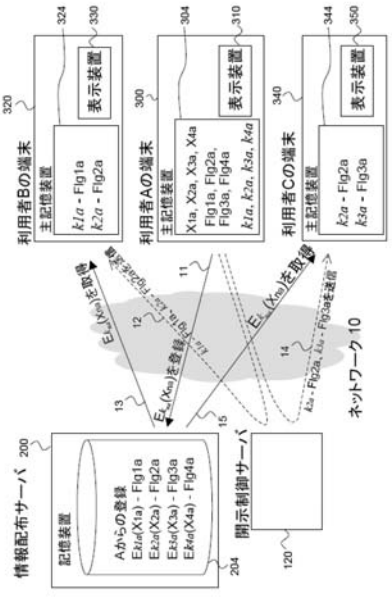
(71)出願人　506183731
リプレックス株式会社
東京都渋谷区神宮前１－２１－１　原宿グリーンランド２０３
(74)代理人　110000408
特許業務法人高橋・林アンドパートナーズ
(72)発明者　直野　典彦
東京都渋谷区神宮前１－２１－１　原宿グリーンランド２０３　リプレックス株式会社内
(72)発明者　太田　智久
東京都渋谷区神宮前１－２１－１　原宿グリーンランド２０３　リプレックス株式会社内

Ｆターム(参考)　5B017 AA03　BA06　BA07　CA16

最終頁に続く

(54)【発明の名称】情報交換装置

(57)【要約】　（修正有）
【課題】情報やその情報の開示先に変更があった場合でも、容易に情報の一貫性を保って情報管理ができる。また、情報の開示制御が容易となり、意図せざる情報流出の防止を図ることができる。
【解決手段】個々の情報または情報の任意の集合ごとに、開示関係を決める秘密鍵で暗号化して、情報配布サーバに記憶し、これとは独立して秘密鍵を開示者端末と被開示者端末の間で授受することによって、開示対象情報と開示関係を独立して制御する。
【選択図】図１



【特許請求の範囲】
【請求項１】
開示者に関する複数の開示用情報を記憶する記憶装置と、
前記複数の開示用情報のそれぞれに対応して用意された複数の秘密鍵を用いて前記複数の開示用情報それぞれを暗号化した暗号情報を複数生成する暗号化装置と、
前記複数の暗号情報および前記複数の秘密鍵を送信する送信装置と、
前記複数の暗号情報から任意に選択された暗号情報と、前記複数の秘密鍵のうち当該選択された暗号情報についての秘密鍵を受信し、当該選択された暗号情報を当該秘密鍵により複合化する復号化装置と、を設けたことを特徴とする情報交換装置。
【請求項２】
前記記憶装置は、前記複数の開示用情報それぞれのフラグ情報を、前記開示用情報と前記フラグ情報とをそれぞれ関連付けた状態でさらに記憶し、
前記暗号化装置は、生成された前記複数の暗号情報それぞれを、対応する開示用情報のフラグ情報と関連付けて前記記憶装置に記憶させ、
前記送信装置は、前記複数の暗号情報を、それぞれの前記フラグ情報と関連付けた状態で送信し、
前記復号化装置は、前記複数の暗号情報から任意に選択された暗号情報についてのフラグ情報を検索キーとした検索によって当該暗号情報を得て復号化を行う請求項１に記載の情報交換装置。
【請求項３】
開示者に関する複数の開示用情報と、これら複数の開示用情報それぞれのフラグ情報と、を、前記開示用情報と前記フラグ情報とをそれぞれ関連付けた状態で記憶する記憶装置と、
前記複数の開示用情報のそれぞれに対応して用意された複数の秘密鍵を用いて前記複数の開示用情報それぞれを暗号化した暗号情報を複数生成し、生成された前記複数の暗号情報を、対応する開示用情報のフラグ情報と関連付けて前記記憶装置に記憶させる暗号化装置と、
前記複数の暗号情報を、それぞれの前記フラグ情報と関連付けた状態で送信する送信装置と、を設けたことを特徴とする情報交換装置。
【請求項４】
前記複数の暗号情報から任意に選択された暗号情報についてのフラグ情報を検索キーとした検索によって当該暗号情報を得るとともに、当該選択された暗号情報についての秘密鍵を受信して暗号情報を当該秘密鍵により当該選択された復号化する復号化装置をさらに設けたことを特徴とする請求項３に記載の情報交換装置。
【請求項５】
前記送信装置は、前記複数の開示用情報それぞれのフラグ情報と当該複数の開示用情報からそれぞれ生成された前記複数の暗号情報とを関連付けた状態で第１のサーバに送信して当該第１のサーバに記憶させ、前記複数の開示用情報それぞれのフラグ情報と当該複数の開示用情報のそれぞれに対応して用意された前記複数の秘密鍵とを関連付けた状態で第２のサーバに送信して当該第２のサーバに記憶させ、
前記復号化装置は、前記複数の暗号情報から任意に選択された暗号情報を前記第１のサーバから受信し、前記複数の秘密鍵のうち当該選択された暗号情報についての秘密鍵を前記第２のサーバから受信する請求項２または４に記載の情報交換装置。
【請求項６】
前記開示用情報と当該開示用情報についての前記秘密鍵とは、互いに独立して設定、変更、および消去されるように構成されている請求項１から５のいずれかに記載の情報交換装置。
【請求項７】
前記複数の開示用情報の少なくとも１以上は、複数のサブ開示情報を含む請求項１から６のいずれかに記載の情報交換装置。

【請求項８】
前記複数の開示用情報が表示され、前記複数の開示用情報のうち前記開示者により被開示者に開示される情報として選択された開示情報が指定される入力装置をさらに設け、
前記送信装置は、前記入力装置に前記開示情報を指定する入力が行われると当該開示情報について生成された暗号情報を、当該開示情報についてのフラグ情報と関連付けて送信する請求項２から７のいずれかに記載の情報交換装置。
【請求項９】
前記入力装置は、前記開示情報を非開示状態に変更する非開示入力機能を備え、
前記送信装置は、前記入力装置に前記開示情報を非開示状態にする入力が行われると当該開示情報、当該開示情報について生成された暗号情報、当該開示情報を暗号化する秘密鍵のいずれか１以上を削除する削除コマンドを生成して生成された削除コマンドと当該開示情報のフラグ情報とを関連付けた状態で送信する請求項８に記載の情報交換装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本願発明は、情報端末間での情報交換装置に関する。
【背景技術】
【０００２】
近年、情報通信技術の発展により、パーソナルコンピュータ（ＰＣ）、携帯型個人情報端末（以下、ＰＤＡと称する）、及び携帯電話など、ネットワークに接続して利用される情報通信機器が普及してきている。また、デジタルカメラ、ビデオカメラ、携帯型音楽プレーヤー、ゲーム機、携帯型ゲーム機、ビデオレコーダなどの様々な民生機器も、ネットワークへの接続が進んでいる。これらの様々な情報機器がインターネットで接続されることで、多様なサービスが生まれ、利便性が向上している。
【０００３】
この種のサービスのなかで最も顕著なものは、情報通信におけるウェブ（ｗｅｂ）をベースとした情報開示である。ウェブ（ｗｅｂ）の普及によって、万人に等しく世界に向けた情報発信の機会が与えられるようになったのみならず、映画や音楽などの有料コンテンツを配信し、さらに決済手段を提供するなど、その用途は急速に拡大している。
【０００４】
しかし一方で、これら各種情報機器のネットワーク化によって、保護されるべき情報が情報所有者の意志に反して流出したり、ネットワーク上で公開されたりする危険性が高まっている。この問題は、個人情報保護に対する関心の高まりや法制化とも相まって、社会的に大きな問題になりつつある。
【０００５】
これは、ウェブ（ｗｅｂ）をベースにとした情報開示技術が、全世界に対する公開を基礎としていることに一因がある。現実に、世界中のウェブサイトの情報のほとんどは、誰でも閲覧が可能である。情報によって閲覧可能な人を限定する必要がある場合には、ユーザ名やパスワードなどの認証手段によってウェブサイトにある情報に対するアクセスを限定する方法が用いられるが、「誰にどの情報を開示するのか」を制御するという観点で情報開示の柔軟性に欠け、管理運営に手間やコストがかかる。そのため、一般のインターネット利用者には運用が困難である。また、ほとんどの場合、その安全性は高くない。現実には、保護すべき情報の実体がウェブサーバにファイルとして存在しているので、様々な技術的、人的手段によってこれが流出する事態が起こっている。
【０００６】
様々な情報機器のネットワーク化によるもう一つの問題は、ネットワークを通じてやりとりされる情報量が急速に増大した結果、利用者による情報の保守、管理が困難になりつつあるという点である。インターネット上で他者が管理し公開している情報の量、および各種情報端末で自らが管理している個人的な情報の量、の両方が爆発的に増大した結果、必要な情報を必要な時に利用することが難しくなっている。

【０００７】
インターネット上で他者が管理し公開している情報に関しては、これら各種情報端末からインターネット上の必要な情報を効率よく検索する技術が提案されており、利用者は、利便性を損なわずにより多くの情報を利用できるようになってきた。現在、検索技術は、情報通信技術の中でも主要な地位を占めるに至っている。（特許文献１）
【０００８】
一方、これら各種の端末で利用者自らが管理している個人的な情報（各種個人情報、私信、写真、ビデオなど）の、インターネットを通じたやりとりのためには、電子メールのやり取りによる個人情報の入手、開示及びそれを基にした各種端末の情報同期方法が一般的である（例えば、特許文献１参照）。しかしながら、この手段には、情報の入手において、他人から更新情報を必ず受け取れるという保障がなく、情報入手の確実性に欠けるという問題があった。また、たとえば電子メールで受領した情報を自らデータベースに入力する必要があるなど、入手した情報の管理に手間がかかるという問題もあった。
【０００９】
これらの問題を解決する手段として、ウェブサーバ上での個人的情報の同期および開示が提案されている（特許文献２）。さらにその延長で、ソーシャル・ネットワーク・サービス（ＳＮＳ）と呼ばれる、個人的な情報をサーバ上で、開示先を限定してやりとりすることのできるサービスが近年普及している（特許文献３）。この手段では、事業者がサーバを立ち上げて会員を募り、ユーザ名及びパスワードの登録、フォルダの共有などの認証手段を確保した上で、前記サーバ上に会員各人が個人情報をアップロードする。この手段によれば、他人の情報が更新されたときに、自分のデータベースが自動的に更新されるため、他人の情報を含めて、常に最新で一貫性のある情報を閲覧することが可能となる。また、自らの知人といった特定人にのみ情報を開示することも可能となる。そして、日記や写真など限られた情報のみを開示することも可能となる。しかしながら、ウェブサーバにあるリモートデータへのアクセスとなるため、動作が遅く不安定であるという問題もあった。そして、すべての個人情報がサーバに集中しているため、それを管理する事業者のリスクが大きいという問題もあった。さらに、ユーザ名とパスワードなど、弱い認証手段が用いられているため、機密性の高い情報には使えないという問題もあった。
【００１０】
更にこのＳＮＳのような、ウェブサーバ上での個人的情報の開示および同期のサービスにおいては、サーバの維持管理のための資金を事業者が得ることが不可欠であり、通常ウェブサイト上に掲載される広告などでその資金をまかなっている。そのために会員数の増大は欠かせない。ところが、一般の（公開されている）ウェブサイトはすべて無料であることから、この種の個人的情報のやりとりのサービスであっても、利用者に課金することは困難である。ここに、この種のサーバを使った個人的情報の開示や同期をおこなうサービスの品質や守秘性が向上しない理由があった。
【特許文献１】米国特許第６，６６５，８３７号明細書
【特許文献２】米国特許第７，０８０，１０４号明細書
【特許文献３】米国特許第７，０６９，３０８号明細書
【発明の開示】
【発明が解決しようとする課題】
【００１１】
様々な情報端末での開示対象情報の入手および開示に関して、現在提案されている電子メールもしくはウェブを前提とした方法の具体的な課題は、以下の６点である。開示対象情報の例としては、個人の電話番号、住所、電子メールアドレスなどの属性情報や、写真、ビデオ、日記、スケジュール、診療履歴、職務経歴、現在いる位置、公開鍵、秘密鍵などの個人が所有する情報、団体や法人の電話番号、電子メールアドレス、人事情報などの団体や法人の構成員に関わる情報、あるいは団体や法人の運営に関わる組織情報、財務情報、営業情報、顧客情報などの団体や法人が所有する情報など、何であっても良い。
【００１２】

第一に端末間の情報一貫性の欠如、第二に他者から開示された情報管理の困難さ、第三に自分の情報開示管理の困難さ、第四に情報開示の柔軟性欠如、第五に開示後の情報制御の困難さ、そして第六にウェブを用いた開示対象情報の開示管理サービスの維持が経済的な面から困難であることである。これらの問題は、既に提案されている、電子メールによる情報交換、あるいはウェブサーバでの情報開示および同期などの方法では経済的合理性のある解決は難しく、またインターネット上で公開された情報から必要な情報を検索することを目的とする、既存の検索技術の精度を向上することでは解決できない問題である。

【００１３】

第一の、端末間の情報一貫性の欠如は、特定の端末にある情報の複製が、ネットワークで接続された他の端末に記憶されている時、前記特定の端末に記憶されている情報が更新されても、他の端末に記憶された情報が、明示的操作をおこなわないと更新されないという問題である。たとえば、利用者Aがその端末にあった電話番号の複製を利用者Bの端末に送信した後、利用者Aの電話番号が変更された場合、利用者Aの端末から利用者Bの端末に、明示的に電子メールを送信するなどの操作が行われない限り、利用者Bの端末に記憶されている利用者Aの電話番号は変更されない。これは、たとえば利用者Aが複数の端末を使っている場合にも起こる問題である。たとえば据置型ＰＣ、携帯型ＰＣ、および携帯電話の三台の端末を使っている利用者Aが、携帯型ＰＣの電話帳を更新しても、据置型ＰＣや携帯電話に対して利用者が入力をおこなうか、明示的に情報同期の操作を行うまでは、これらの端末の電話帳は更新されない。管理する情報や、その複製を送信する相手や端末が増えると、利用者は端末の更新状態を管理し切れなくなり、端末間の情報一貫性が保てない。

【００１４】

第二の、他者の情報管理の困難さは、主として電子メール等で送られてくる他者の開示対象情報を管理しきれないという問題である。たとえば、他者の電話番号の変更があった場合、電子メールで送られてきた情報を自ら住所録などに入力して管理するのが一般的であるが、情報量が多いとその住所録を常に最新の状態に保つには多くの労力を必要し、多くの利用者は、住所録を適切に管理できていない。

【００１５】

第三の、自分の開示管理の困難さは、自分の開示対象情報を更新した場合、明示的に電子メールなどで知人に対して通知を出す必要があるという問題である。たとえば、自分の電話番号や勤務先が変わった場合、新たな情報を電子メール等で知人に知らせるが、通知すべき人や情報が多いと、必要な人に必要な情報をすべて通知しているとは限らず、また誰に通知して誰に通知しなかったかを開示対象情報の所有者自身が把握できなくなる。

【００１６】

第四の、情報開示の柔軟性欠如は、情報所有者の望みどおりに、特定の開示対象情報を特定の相手に開示することが難しいという問題である。ウェブで開示対象情報の開示を行えば、上記の電子メールなどによる情報開示管理の困難は回避できるが、ウェブは基本的にすべての情報を全世界に公開するものであるし、前記ＳＮＳなどのような方法でも、たとえば「日記を友人に開示」といった大まかな区分での開示制御しかできない。電子メールによる情報開示では、開示管理の柔軟性は維持できるが、上に述べたように、開示管理が煩雑となる。つまり、上記の第三の問題と、この第四の問題は相反関係にあり、最適な方法がない。

【００１７】

第五の、開示後の情報制御の困難は、現在の通信方法では、一度開示してしまった開示対象情報は、開示先に所有権が移るため、原則的に情報所有者による制御は不可能である、という問題である。たとえば、電子メールで送ったり、ウェブサイトに入力したりした開示対象情報は、それ以降は開示先の所有する情報として扱われるため、開示先が好きなように利用や再開示することができ、本来の開示対象情報の所有者による制御ができない。これが、個人情報の流出などの様々な社会問題を生む原因となっている。

【００１８】

第六の、ウェブを用いた開示対象情報の開示管理サービスの維持が経済的な面から困難である問題は、現在のインターネット環境において、ほぼすべてのウェブサイトや検索技術が無料で利用できることから、利用者が既に使っている電子メール以外のソフトウェアやサービスに、そこから得られる利便性向上の対価を支払う意志が生まれにくいという事情からくる。ＳＮＳなどのサービスが、ウェブや電子メールほど大きく広がらず、品質も向上しない理由がここにある。これまで述べた具体的問題を解決するためには、個人的情報の開示管理サービスに対して、サービス事業者が充分にその対価を得られるような事業モデルの開発が不可欠であるが、これまでは成功していない。

【課題を解決するための手段】

【００１９】

本発明の第一態様によれば、開示者に関する複数の開示用情報を記憶する記憶装置と、

前記複数の開示用情報のそれぞれに対応して用意された複数の秘密鍵を用いて前記複数の開示用情報それぞれを暗号化した暗号情報を複数生成する暗号化装置と、　前記複数の暗号情報および前記複数の秘密鍵を送信する送信装置と、　前記複数の暗号情報から任意に選択された暗号情報と、前記複数の秘密鍵のうち当該選択された暗号情報についての秘密鍵を受信し、当該選択された暗号情報を当該秘密鍵により複合化する復号化装置と、を設けたことを特徴とする情報交換装置が提供される。

【００２０】

本発明の第二態様によれば、前記第一態様において、前記記憶装置は、前記複数の開示用情報それぞれのフラグ情報を、前記開示用情報と前記フラグ情報とをそれぞれ関連付けた状態でさらに記憶し、　前記暗号化装置は、生成された前記複数の暗号情報それぞれを、対応する開示用情報のフラグ情報と関連付けて前記記憶装置に記憶させ、　前記送信装置は、前記複数の暗号情報を、それぞれの前記フラグ情報と関連付けた状態で送信し、前記復号化装置は、前記複数の暗号情報から任意に選択された暗号情報についてのフラグ情報を検索キーとした検索によって当該暗号情報を得て復号化を行う情報交換装置が提供される。

【００２１】

本発明の第三態様によれば、開示者に関する複数の開示用情報と、これら複数の開示用情報それぞれのフラグ情報と、を、前記開示用情報と前記フラグ情報とをそれぞれ関連付けた状態で記憶する記憶装置と、　前記複数の開示用情報のそれぞれに対応して用意された複数の秘密鍵を用いて前記複数の開示用情報それぞれを暗号化した暗号情報を複数生成し、生成された前記複数の暗号情報を、対応する開示用情報のフラグ情報と関連付けて前記記憶装置に記憶させる暗号化装置と、　前記複数の暗号情報を、それぞれの前記フラグ情報と関連付けた状態で送信する送信装置と、を設けたことを特徴とする情報交換装置が提供される。

【００２２】

本発明の第四態様によれば、前記第三態様において、前記複数の暗号情報から任意に選択された暗号情報についてのフラグ情報を検索キーとした検索によって当該暗号情報を得るとともに、当該選択された暗号情報についての秘密鍵を受信して暗号情報を当該秘密鍵により当該選択された復号化する復号化装置をさらに設けたことを特徴とする情報交換装置が提供される。

【００２３】

本発明の第五態様によれば、前記第二または第三態様において、前記送信装置は、前記複数の開示用情報それぞれのフラグ情報と当該複数の開示用情報からそれぞれ生成された前記複数の暗号情報とを関連付けた状態で第１のサーバに送信して当該第１のサーバに記憶させ、前記複数の開示用情報それぞれのフラグ情報と当該複数の開示用情報のそれぞれに対応して用意された前記複数の秘密鍵とを関連付けた状態で第２のサーバに送信して当該第２のサーバに記憶させ、　前記復号化装置は、前記複数の暗号情報から任意に選択された暗号情報を前記第１のサーバから受信し、前記複数の秘密鍵のうち当該選択された暗号情報についての秘密鍵を前記第２のサーバから受信する情報交換装置が提供される。

【００２４】
本発明の第六態様によれば、前記第一から第五のいずれかにおいて、前記開示用情報と当該開示用情報についての前記秘密鍵とは、互いに独立して設定、変更、および消去されるように構成されている情報交換装置が提供される。
【００２５】
本発明の第七態様によれば、前記第一から第六のいずれかにおいて、前記複数の開示用情報の少なくとも１以上は、複数のサブ開示情報を含む情報交換装置が提供される。
【００２６】
本発明の第八態様によれば、前記第一から第七のいずれかにおいて、前記複数の開示用情報が表示され、前記複数の開示用情報のうち前記開示者により被開示者に開示される情報として選択された開示情報が指定される入力装置をさらに設け、　前記送信装置は、前記入力装置に前記開示情報を指定する入力が行われると当該開示情報について生成された暗号情報を、当該開示情報についてのフラグ情報と関連付けて送信する情報交換装置が提供される。
【００２７】
本発明の第九態様によれば、前記第八において、前記入力装置は、前記開示情報を非開示状態に変更する非開示入力機能を備え、　前記送信装置は、前記入力装置に前記開示情報を非開示状態にする入力が行われると当該開示情報、当該開示情報について生成された暗号情報、当該開示情報を暗号化する秘密鍵のいずれか１以上を削除する削除コマンドを生成して生成された削除コマンドと当該開示情報のフラグ情報とを関連付けた状態で送信する情報交換装置が提供される。
【発明の効果】
【００２８】
本発明によれば、情報やその情報の開示先に変更があった場合でも、容易に情報の一貫性を保って情報管理ができる。また、情報の開示制御が容易となり、意図せざる情報流出の防止を図ることができる。
【発明を実施するための最良の形態】
【００２９】
以下に本願発明を実施するための現在考えられる最善の形態について説明する。本願発明の範囲は、添付特許請求の範囲によって明確に定義されているため、この説明は限定的な意味に解釈すべきではなく、単に発明の一般原理を例示する目的で行う。
【００３０】
図１は、本願発明の実施形態に係る情報交換システムの一例の全体図である。この情報交換システムは、情報配布サーバ２００、開示者である利用者Ａの端末３００、被開示者である利用者Ｂの端末３２０および利用者Ｃの端末３４０、開示制御サーバ１２０、およびこれらの端末とサーバの間を接続するネットワーク１０より構成されている。
【００３１】
図２は、情報配布サーバ２００の構成要素の一例を表す図である。情報配布サーバ２００は、送受信手段２０１、テーブル作成手段２０２、検索手段２０３、および記憶装置２０４を有する。ただし、本願発明における情報配布サーバ２００の構成は図２に示すものに限定されず、本願発明の方法を実行できる構成であればどのようなものであってもよい。また、図２に示す各構成要素は、サーバのハードウェア上で動くオペレーティングシステム、ミドルウェアまたはアプリケーションソフトウェアによって実現されていてもよい。
【００３２】
図３（ａ）は、利用者Ａの端末３００の構成要素を表した図である。利用者Ａの端末３００は、外部記憶装置３０１、演算装置３０３、主記憶装置３０４、通信装置３０６、キーボードによる入力装置３０７、マウスによる入力装置３０８、表示制御装置３０９、表示装置３１０などを具える。また、主記憶装置３０４上には、利用者Ａの端末のオペレーティングシステム３１３、本願発明によるアプリケーションプログラム３０５を有する。ただし、本願発明における利用者Ａの端末の構成は図３（ａ）に示すものに限定されず、本

願発明の方法を実行できる構成であればどのようなものであってもよい。
【００３３】
図３（ｂ）は、利用者Ｂの端末３２０の構成要素を表した図である。利用者Ａの端末３２０は、外部記憶装置３２１、演算装置３２３、主記憶装置３２４、通信装置３２６、キーボードによる入力装置３２７、マウスによる入力装置３２８、表示制御装置３２９、表示装置３３０などを具える。また、主記憶装置３２４上には、利用者Ａの端末のオペレーティングシステム３３３、本願発明によるアプリケーションプログラム３２５を有する。ただし、本願発明における利用者Ｂの端末の構成は図３（ｂ）に示すものに限定されず、本願発明の方法を実行できる構成であればどのようなものであってもよい。
【００３４】
また、図４に本願発明による方法を実現するためのステップの一例を示し、これを用いて、以下に説明する。
【００３５】
はじめに、利用者Ａの端末３００の主記憶装置３０４または外部記憶装置３０１は、開示対象となる４つの情報Ｘ１ａ、Ｘ２ａ、Ｘ３ａ、およびＸ４ａ、ならびにこれらの情報に対応する４つのフラグ情報Ｆｌｇ１ａ、Ｆｌｇ２ａ、Ｆｌｇ３ａ、およびＦｌｇ４ａを各々関連づけられた状態で記憶３１５している（ステップＳ４０１）。ここで関連づけられるフラグ情報どのような情報であってもよく、いくつでもよい。たとえば、第１のフラグ情報として、各々の開示対象情報を特定するための番号または各々の開示対象情報のハッシュ値、第２のフラグ情報として開示者を特定するための認識票、の２つを各々の開示対象情報に関連づけて送信するなどしてもよい。フラグ情報の他の一例としては、開示対象情報を特定することはできないが、開示対象情報の絞り込みに使うことのできるキーワードでもよい。またフラグ情報の他の一例としては、後のステップで被開示者の端末に送られる開示対象情報を、記憶容量の限られた被開示者端末の記憶装置に記憶するか消去するかの優先順位を表す情報であってもよい。
【００３６】
また、同様に利用者Ａの端末３００の主記憶装置上には、開示先データベース３１６として、開示先となる利用者の名前利用者Ｂ、利用者Ｃ、利用者Ｄ、および利用者Ｅと、各々の端末をネットワーク上で一意に特定するために必要な認識票ＩＤｂ、ＩＤｃ、ＩＤｄ、およびＩＤｅが関連づけられた状態で記憶されている。まず、利用者Ａの端末の演算装置３０３が前記４つの情報を各々暗号化するための、ｋ１ａ、ｋ２ａ、ｋ３ａ、およびｋ４ａの４つの秘密鍵３０２を主記憶装置上３０４に生成する。これらは外部記憶装置３０１に記憶されてもよい。また、前記４つの開示対象情報Ｘ１ａ、Ｘ2a、Ｘ３ａ、およびＸ４ａを各々に対応するフラグ情報Ｆｌｇ１ａ、Ｆｌｇ２ａ、Ｆｌｇ３ａ、およびＦｌｇ４ａを各々、さらに前記前記秘密鍵ｋ１ａ、ｋ２ａ、ｋ３ａ、およびｋ４ａを各々、関連づけた状態３１５で主記憶装置にロードする。（ステップＳ４０２）。
【００３７】
次に、利用者Ａの端末の演算装置３０３が、主記憶装置３０４上にある本願発明によるアプリケーションプログラム３０５に定められた手続きに従って、前記４つの情報を前記４つの秘密鍵で各々暗号化し、Ｅｋ１ａ（Ｘ１ａ）、Ｅｋ２ａ（Ｘ２ａ）、Ｅｋ３ａ（Ｘ３ａ）、およびＥｋ４ａ（Ｘ４ａ）を生成した上、これらを主記憶上に一旦記憶する（ステップＳ４０３）。ここで、たとえばＥｋ１ａ（Ｘ１ａ）は情報Ｘ１ａを、暗号化装置としての演算装置３０３によって秘密鍵ｋ１ａで暗号化した演算結果である暗号情報を表す。ここで用いる暗号化のアルゴリズムは、たとえばＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）、三重ＤＥＳ、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）など、いかなる暗号アルゴリズムでもよい。次に、利用者Ａの端末の通信装置３０６が、前記４つの演算結果Ｅｋ１ａ（Ｘ１ａ）、Ｅｋ２ａ（Ｘ２ａ）、Ｅｋ３ａ（Ｘ３ａ）、およびＥｋ４ａ（Ｘ４ａ）の各々に、前記各々のフラグ情報を関連づけた状態で、ネットワーク１０を通じて情報配布サーバ２００に送信する。たとえば、演算結果Ｅｋ１ａ（Ｘ１ａ）は、前記ステップＳ４０１においてＸ１ａと関連づけられた

フラグ情報Ｆｌｇ１ａと関連づけられた上で、サーバ２００に送信される（ステップＳ４０４）。

【００３８】

次に、サーバ２００の送受信手段２０１が前記第２のステップでサーバに送信された、前記４つの演算結果と、各々に関連づけられた前記フラグ情報を受信する。次にサーバ２００のテーブル作成手段２０２が、前記利用者Ａの端末より受信した情報をデータベースとしてサーバの記憶装置２０４に記憶する（ステップＳ４０５）。

【００３９】

次に、利用者Ａの端末では、キーボード３０７やマウス３０８のような入力手段が受け付けた指示に従って、本願発明によるアプリケーションプログラム３０５は、表示制御装置３０９を通じて表示装置３１０に、グラフィカル・ユーザ・インタフェイス（以下ＧＵＩと称する）３１１を表示する。このＧＵＩ３１１上には、本願発明によるアプリケーションプログラム３０５から表示装置３０９を通じて表示装置３１０に送られる信号によって開示制御ウィンドウ３１２が表示される（ステップＳ４０６）。

【００４０】

図５（ａ）には、利用者Ａの端末３００の表示装置３１０に表示された開示制御ウィンドウ３１２の一例を表す。開示制御ウィンドウ３１２は、開示先を表示する欄５００、開示対象情報を表示する欄５０１、および開示状態表示と開示制御を行うチェックボックスの欄５０２よりなる。図３（ａ）乃至図５に示す一例では、開示先５００として、利用者Ｂ、利用者Ｃ、利用者Ｄおよび利用者Ｅの４つの名前が表示されている。また同様に図３（ａ）乃至図５に示す一例では、開示対象情報としてＸ１ａ、Ｘ２ａ、Ｘ３ａ、およびＸ４ａの４つの情報が表示されている。また、開示欄５０２には、前記４つの開示対象情報の各々に対応するチェックボックス５０３、５０４、５０５および５０６が表示されている。たとえば、最上部のチェックボックス５０３は、開示対象情報Ｘ１ａの開示状態表示と開示制御をおこなうためのチェックボックスである。

【００４１】

次に、利用者Ａの端末３００において、キーボート３０７またはマウス３０８が受け付けた入力によって、オペレーティングシステムがＧＵＩ３１１上のカーソル５１０を移動させ、たとえば利用者Ｂが選択されると、利用者Ｂの端末３２０に対する、利用者Ａの端末３００からの開示対象情報の開示制御が可能となる。さらにたとえば、図５（ａ）の状態から、Ｘ１ａおよびＸ２ａの二つの開示対象情報の左側にあるチェックボックス５０３および５０４に、マウス３０８などの入力によってカーソル５１０を移動させ、ボタンを下押しするなどすることで、図５（ｂ）に示すようにチェックマークを表示させるとする。本願発明の一実施形態によれば、この操作は、本願発明によるアプリケーションソフトウェア３０５に対する、利用者Ａの端末３００から利用者Ｂの端末３２０への、情報Ｘ１ａおよびＸ２ａの情報開示の指示である（ステップＳ４０７）。以下では、図４（ｂ）を参照して、利用者Ａの端末３００から利用者Ｂの端末３２０に対する、情報Ｘ１ａおよびＸ２ａの開示を例にとり、本願発明による方法を説明する。

【００４２】

ここで、前記ステップＳ４０７においてＧＵＩ３１１を通じて利用者Ａの端末から利用者Ｂの端末への開示が指示された情報Ｘ１ａおよびＸ２ａについて、利用者Ａの端末においては、本発明によるアプリケーションプログラム３０５の指示に従い、演算装置３０３が、前記第1のステップで情報Ｘ１ａを暗号化するために生成した秘密鍵ｋ１ａと、前記情報Ｘ１ａの検索のために付けられたフラグ情報Ｆｌｇ１ａを関連づけ、また前記第1のステップで情報Ｘ２ａを暗号化するために生成した秘密鍵ｋ２ａと、前記情報Ｘ２ａの検索のために付けられたフラグ情報Ｆｌｇ２ａを関連づけた状態で主記憶装置３０４に一時的に記憶する。次に通信装置３０６は前記一時的に記憶したｋ１ａとＦｌｇ１ａの組およびｋ２ａとＦｌｇ２ａの組の、２組を、前記開示先データベース３１６から利用者Ｂの認識票ＩＤｂを検索した上これを利用して開示制御サーバ１２０を通じて、利用者Ｂの端末３２０に送信（１２）する（ステップＳ４０８）。この時、前記各秘密鍵に関連づけるフラ

グ情報は前記ステップＳ４０４において、利用者Ａの端末が、情報配布サーバ２００に送信した暗号化された情報に関連づけられたフラグ情報のうち開示対象情報を一意に特定することのできるフラグ情報を含む、任意のフラグ情報であってよい。たとえば、前記ステップＳ４０４において、暗号化された情報の各々に、第１のフラグ情報として、各々の開示対象情報を一意に特定するための番号、第２のフラグ情報として開示者を一意に特定するための認識票、の２つを関連づけて情報配布サーバ２００に送信している場合、ここで秘密鍵の各々にこれら第1および第２の２つのフラグを各々関連づけて、開示制御サーバ１２０に送ってもよい。

【００４３】

次に、利用者Ｂの端末３２０において、前記ステップＳ４０８で、利用者Ａの端末３００が開示制御サーバ１２０を通じて利用者Ｂの端末３２０に送信した、ｋ１ａとＦｌｇ１ａの組およびｋ２ａとＦｌｇ２ａの組、の２組の情報を、端末３２０の通信装置３２６が受信し、これを主記憶装置３２４に記憶した上で、さらに必要に応じて外部記憶装置３２１に記憶する（ステップＳ４０９）。

【００４４】

次に、利用者Ｂの端末３２０の主記憶装置３２４上にある本願発明によるアプリケーションプログラム３２５が、通信装置３２６を通じて、サーバ２００に対して、ステップＳ４０８で利用者Ａの端末より送られたフラグ情報Ｆｌｇ１ａおよびＦｌｇ１ｂを送信することで、サーバの記憶装置２０４に記憶されているデータベースに、Ｆｌｇ１ａおよびＦｌｇ１ｂに各々関連づけられた暗号化された情報の検索を依頼する（ステップＳ４１０）。この検索依頼は、いつおこなってもよい。たとえば、前記ステップＳ４０８でＦｌｇ１ａおよびＦｌｇ１ｂを利用者Ａの端末３００から受信した後直ちにおこなってもよいし、利用者Ｂの端末において、キーボード３２７やマウス３２８からの信号によって、サーバからの開示された情報取得の明示的操作が本願発明によるアプリケーションプログラムに対して行われた時に、前記情報配布サーバ２００に対する検索依頼を行ってもよい、さらに、前記ステップＳ４０８より以前に、利用者Ｂの端末３２０が任意の情報を情報配布サーバ２００より取得しておいてもよい。ただしこの場合、Ａの端末より秘密鍵を受領するまでは、情報配布サーバ２００より取得した情報は復号化ができないので、利用者Ｂの端末で利用することはできない。

【００４５】

次に、サーバ２００の検索手段２０３が、記憶装置２０４上のデータベースを検索し、その検索結果として前記ステップＳ４１０で利用者Ｂの端末３２０より検索依頼を受けた、Ｆｌｇ１ａおよびＦｌｇ１ｂに関連づけられた情報である、Ｅｋ１ａ（Ｘ１ａ）およびＥｋ２ａ（Ｘ２ａ）を、検索結果として、送受信手段２０１を通じて利用者Ｂの端末３２０に送信する（ステップＳ４１１）。

【００４６】

次に、利用者Ｂの端末３２０の通信装置が、前記ステップＳ４１１でサーバ２００より送信されたＥｋ１ａ（Ｘ１ａ）およびＥｋ２ａ（Ｘ２ａ）を受信し、これを主記憶装置に記憶する。次に受信した暗号化された情報のうち、Ｅｋ１ａ（Ｘ１ａ）を前記利用者Ａの端末より開示制御サーバ１２０を通じて入手した秘密鍵ｋ１ａで、かつＥｋ２ａ（Ｘ２ａ）を同じく前記利用者Ａの端末より入手した秘密鍵ｋ２ａで、各々復号化し（ステップＳ４１２）、Ｘ１ａおよびＸ２ａを主記憶上に記憶した上で、本願発明によるアプリケーションプログラム３２５が、ＧＵＩ３２３上表示された、開示された情報の表示ウィンドウ３３２上に利用者Ａから開示された情報としてＸ１ａおよびＸ２ａを表示する（ステップＳ４１３）。図３（ｂ）に示す一例では、利用者Ｂの端末３２０の表示装置３３０上に表示されたＧＵＩ３３１に表示された、開示情報表示ウィンドウ３３２には、利用者Ａの端末３００から開示された情報Ｘ１ａおよびＸ２ａが表示されている。

【００４７】

なお、上述した実施態様では、利用者Ａの端末３００の通信装置３０６が暗号情報および秘密鍵を送信する送信装置として機能している。具体的には、通信装置３０６は生成され

た複数の暗号情報（Ｅｋ１ａ（Ｘ１ａ）、Ｅｋ２ａ（Ｘ２ａ）など）を、それぞれのフラグ情報（Ｆｌｇ１ａ、Ｆｌｇ２ａなど）と関連付けた状態で情報配布サーバ２００に送信して情報配布サーバ２００の記憶装置２０４に記憶させる。一方、秘密鍵（ｋ１ａ、ｋ２ａなど）は利用者Ａの端末３００の演算装置３０３で開示用情報（Ｘ１ａ、Ｘ２ａなど）ごとに生成され、それぞれのフラグ情報と関連付けられた状態で、通信装置３０６によって開示制御サーバ１２０に送信される。

【００４８】

そして、利用者Ｂの端末３２０は複合化装置として機能し、利用者Ａの端末３００の通信装置３０６および情報配布サーバ２００の送信手段２０１を介して暗号情報を受信する。また、秘密鍵は、利用者Ａの端末３００の通信装置３０６および開示制御サーバ１２０の送信手段（図示せず）を介して受信する。このように、本実施態様では秘密鍵および暗号情報にはそれぞれのフラグ情報が関連付けられているため、秘密鍵と暗号情報とを別々のサーバに送信して管理して、それぞれのサーバを介して利用者Ｂに送信できるので、安全性が高い。ただし、本発明はこれに限定されず、暗号情報および秘密鍵がサーバを介さずに利用者Ａから利用者Ｂに送信されることも排除されない。

【００４９】

また、本発明による方法によれば、利用者Ａから利用者Ｂの端末への任意の情報開示を取り消すこともできる。たとえば、図５（ｂ）に示す状態、すなわち利用者Ａの端末３００が、これまで説明した本願発明による方法で利用者Ｂの端末に対して情報Ｘ１ａおよびＸ２ａを開示している状態で、利用者Ａの端末のキーボード３０７またはマウス３０８の操作にしたがって、表示装置３１９上に表示されたＧＵＩ３１１上で、カーソル５１０を移動させ、開示対象情報Ｘ２に対応するチェックボックス５０４を、ボタンを下押しするなどして選択する。すると、本発明によるアプリケーションプログラム３０５に定めた手続きに従い、前記チェックボックス５０４からチェックマークを消去する（ステップＳ４２７）。これは、利用者Ａの端末３００から利用者Ｂの端末３２０への、開示対象情報Ｘ２ａの開示取り消しの操作である。以下では図４（ｃ）を参照して開示を取り消す場合のステップについて説明する。

【００５０】

ここで、前記ステップＳ４２７でＧＵＩ３１１を通じて利用者Ａの端末から利用者Ｂの端末への開示が取り消された情報Ｘ２ａについて、利用者Ａの端末の本発明によるアプリケーションプログラム３０５の指示に従い、通信装置３０６が、Ｘ２ａに対応するフラグ情報Ｆｌｇ２ａを、削除要求を表すコマンドやフラグ情報などとともに、開示制御サーバ１２０を通じて利用者Ｂの端末３２０に送る（ステップＳ４２８）。利用者Ｂの端末３２０の通信装置３２６が受信した（ステップＳ４２９）、前記削除要求を表すコマンドやフラグ情報とともに利用者Ａの端末より送られたフラグ情報Ｆｌｇ２ａを、主記憶装置３２４に一時的に記憶し、次に演算装置３２３が主記憶装置３２４または外部記憶装置３２１にあるＦｌｇ２ａを検索したうえ、これに対応する秘密鍵ｋ２ａを削除する（ステップＳ４３０）。また、同様にこのフラグ情報Ｆｌｇ２ａに対応する、復号化された状態で、利用者Ｂの端末３２０の主記憶装置３２４または外部記憶装置３２１に記憶されている、利用者Ａの情報Ｘ２ａを検索した上、これを削除する（ステップＳ４３１）。前記ステップＳ４３０とステップＳ４３１は逆の順番でもよい。このようにすることで、利用者Ｂの端末では利用者Ａの情報を利用できなくなり、開示の取り消しが完了する。

【００５１】

前記ステップＳ４３０およびＳ４３１において、利用者Ｂの端末から、利用者Ａの秘密鍵ｋ２ａおよび開示対象情報Ｘ２ａを削除する際に、前記ステップＳ４０９で開示制御サーバ１２０から受信して記憶したフラグ情報Ｆｌｇ２ａと、前記ステップＳ４１１で情報配布サーバ２００から受信して記憶した暗号情報Ｅｋ２ａ（Ｘ２ａ）は、利用者Ｂの端末の記憶装置から削除しても削除しなくともよい。もし、これらフラグ情報および暗号情報を削除せずに、再び利用者Ａの端末より開示対象情報Ｘ２ａを開示される、すなわち再び前記ステップＳ４０９のように、秘密鍵ｋ２ａとそのフラグ情報Ｆｌｇ２ａを開示制御サー

バから受信した場合には、再度情報配布サーバ２００より暗号化情報を取り寄せる前記ステップＳ４１０およびＳ４１１の各ステップを省略しても、利用者Ｂの端末に復号化した開示対象情報Ｘ２ａを表示することができる。

【００５２】

本願発明で開示される情報は、氏名、住所、電子メールアドレス、各種通信サービスのアカウント情報、パスワードなどを含む個人情報、文書、写真、動画、秘密鍵、公開鍵などに限定されず、ウェブサイト上に掲載されるなどあらゆる情報であってもよい。

【００５３】

また、これまで本実施形態では、情報１つに対して１個の秘密鍵で暗号化する方法を用いたが、複数の情報に対して共通の秘密鍵を利用して、各々の情報を暗号化してもよい。この場合には、開示者端末では、前記共通の秘密鍵とその秘密鍵に関連づけられたフラグ情報を、開示制御サーバ１２０を通じて被開示者端末に送ることで、前記複数の情報を一括して開示することもできる。

【００５４】

また、他の一例として、再び図１を参照すると、利用者Ａの端末３００が前記各ステップを実行することで、利用者Ｂに対して情報Ｘ１ａおよびＸ２ａを開示しながら、さらに利用者Ｃの端末３４０に対して情報Ｘ２ａおよびＸ３ａを開示している一例が示されている。このように、本願発明による方法を用いて、一つの利用者の端末が、複数の利用者の端末へ任意の情報を開示していてもよい。

【００５５】

また、本実施形態では、利用者Ａの端末３００から利用者Ｂ３２０への一方向の開示であったが、これと同時に前記各ステップの方法によって、利用者Ｂの端末３２０から、利用者Ａの端末３００への情報開示が、情報配布サーバ２００および開示制御サーバ１２０を通じて、おこなわれてもよい。またこのような相互開示が複数の利用者の端末の間で相互に行われていてもよい。

【００５６】

図６に示す一例では、相互開示が行われている場合に使われる表示および制御画面の一例として、利用者Ａの端末３００の表示装置３１０上に表示された、情報開示のためのウィンドウと開示された情報の表示のためのウィンドウとの機能を併せ持つ、情報交換ウィンドウ６００の一例を示す。前記情報交換ウィンドウ６００は、情報交換相手の欄６０１、開示対象情報の欄６０２、開示制御の欄６０３、および開示された情報の欄６０４よりなる。この一例では、前記ステップＳ４０４において、利用者Ａの端末３００が、暗号化した開示対象と関連づけて情報配布サーバ２００に送信する、フラグ情報のひとつとして利用者Ａの端末を特定するための認識票を含むとする。また利用者Ａの端末３００から他の利用者の端末への、本願発明による情報開示だけでなく、他の利用者の端末から利用者Ａの端末への本願発明による情報開示についても、同様に前記フラグ情報に開示者の端末を特定できる認識票を含むとする。

【００５７】

ここで図６（ａ）を参照すると、利用者Ａの端末３００のキーボード３０７やマウス３０８などの操作に従って、主記憶装置３０４上にある本願発明によるアプリケーションプログラム３０５の指示により、カーソル６１０を移動させ、表示装置３１０に表示された情報交換ウィンドウ６００の上に表示された情報交換相手である利用者Ｂ６０９を選択が選択されると、開示対象情報欄６０２に、開示対象Ｘ１ａ、Ｘ２ａ、Ｘ３ａ、およびＸ４ａが表示され、さらにこれらの開示対象情報の利用者Ｂの端末に対する開示状態が開示制御欄６０３に、チェックマークによって表示される。図６（ａ）に示す一例では、開示対象情報Ｘ１ａおよびＸ２ａに各々対応するチェックボックス６０５および６０６にチェックマークが付されており、このことによって利用者Ａの端末３００が、利用者Ｂの端末に対して、情報Ｘ１ａおよびＸ２ａを開示していることを示している。またこれと同じウィンドウ６００上では、利用者Ｂが利用者Ａに対して逆方向に開示している情報としてＹ１ｂおよびＹ２ｂが、開示された情報欄６０４に表示されている。ここで表示されている利用

者Ｂの端末３２０が利用者Ａに対して開示している情報も、本発明による前記方法によって開示が行われ、同じＧＵＩ６００上に同時に表示されているものである。

【００５８】

この状態でいつでも、開示制御については、カーソル６１０を表示装置上で移動させ、開示制御欄に表示された任意のチェックボックスを選択することで、任意の開示対象情報の、利用者Ｂの端末３２０への開示状態を変更することができる。たとえば、利用者Ａの端末３００の表示装置３１０において、図６（ａ）に示す状態で、カーソル６１０を開示対象情報Ｘ３ａに対応するチェックボックス６０７まで移動させ、マウスのボタンを下押しするなどして、チェックボックス６０７を選択（ステップＳ４０７に相当）すると、このチェックボックス６０７にチェックマークが表示されると同時に、利用者Ａの端末３００が開示情報Ｘ３ａに対応する秘密鍵ｋ３ａを、開示制御サーバ１２０を通じて、利用者Ｂの端末３２０に送る（ステップＳ４０８に相当）。利用者Ｂの端末３２０は、情報配布サーバ２００から暗号化されたＥｋ３ａ（Ｘ３ａ）を取得し、これを前記秘密鍵ｋ３ａで復号化した上で（ステップＳ４１２に相当）その表示装置上に利用者Ａの端末３００から利用者Ｂの端末３２０に開示された情報Ｘ３ａを表示する。（ステップＳ４１３に相当）。

【００５９】

たとえば、利用者Ａの端末３００の表示装置３１０において、図６（ａ）に示す状態で、カーソル６１０を開示対象情報Ｘ１ａに対応するチェックボックス６０５まで移動させ、マウスのボタンを下押しするなどして、チェックボックス６０５を選択すると、このチェックボックス６０５にチェックマークが消去されると同時に（ステップＳ４２７に相当）、利用者Ａの端末３００が開示情報Ｘ１ａに対応する秘密鍵ｋ１ａおよび開示対象情報Ｘ１ａの消去を、利用者Ｂの端末３２０に依頼する（ステップＳ４２８に相当）。利用者Ｂの端末の本願発明によるアプリケーションソフトウェア３２５は、その主記憶装置および外部記憶装置から前記秘密鍵ｋ１ａおよび開示対象Ｘ１ａの消去をおこなう（ステップＳ４３０およびステップＳ４３１に対応）。こうすることで、利用者Ｂはもはや暗号化された情報Ｅｋ１ａ（Ｘ１ａ）の復号化をできなくなり、利用者Ｂの端末の表示装置上に利用者Ａの開示対象情報Ｘ１ａを表示できなくなる。

【００６０】

この状態で、本願発明によれば、たとえば利用者Ｂの端末３２０に記憶された情報Ｘ１ｂ、Ｘ２ｂ、Ｘ３ｂ、およびＸ４ｂを、前記各ステップによって利用者Ａの端末に開示することができる。この場合、これら各々の情報に対応する秘密鍵ｋ１ｂ、ｋ２ｂ、ｋ３ｂ、およびｋ４ｂと、これら各々の情報に対応するフラグ情報Ｆｌｇ１ｂ、Ｆｌｇ２ｂ、Ｆｌｇ３ｂ、およびＦｌｇ４ｂが使われる。

【００６１】

図６（ｂ）に示す一例は、利用者Ｂの端末の表示装置３３０に表示されたＧＵＩ３３２中に、前記相互開示ウィンドウを表示した状態である。図６（ｂ）に示す一例では、情報交換相手として利用者Ａ６２９が選択されている結果、開示対象情報欄６２２には、利用者Ｂの端末が利用者Ａの端末に開示している情報が開示制御欄６２３に表示されたチェックマークで表示されており、開示された情報欄６２４には、利用者Ｂの端末が利用者Ａの端末より開示されている情報が表示されている。図６に示す一例では、利用者Ａが利用者Ｂに対して情報Ｘ１ａおよびＸ２ａを、また利用者Ｂが利用者Ａに対して情報Ｘ１ｂおよびＸ２ｂをそれぞれ開示している。図６（ａ）はこの状態を利用者Ａの端末から見たものであり、図６（ｂ）は同じ状態を利用者Ｂの端末から見たものである。この状態でいつでも、利用者Ａは開示制御欄６０３の、また利用者Ｂは開示制御欄６２３のチェックボックスを選択することで、前記の方法によって新たな情報を相手に開示したり、開示済の情報の開示を取り消したりすることができる。

【００６２】

これまでの説明は、利用者Ａの端末と利用者Ｂの端末との、２つの端末間の情報の相互開示であったが、これは任意の数の端末間の相互開示であってよい。図７に示す一例は、利用者Ａの端末の表示装置３１０のＧＵＩ３１１上に表示された相互開示ウィンドウ６００

において、情報交換相手として利用者Ｃ６１１が選択された状態である。この状態では利用者Ａの端末３００は利用者Ｃの端末３４０に対して情報Ｘ２ａおよびＸ３ａを、また利用者Ｃの端末３４０は利用者Ａの端末３００に対して情報Ｘ１ｃ、Ｘ２ｃ、およびＸ３ｃを開示している。この状態でいつでも、利用者Ａは、情報交換相手欄６０１で任意の情報交換相手を選択することで、異なる情報交換相手との情報の開示、被開示を表示および制御することができる。

【００６３】

このように複数の端末間の相互開示においては、情報配布サーバ２００には、図８に示すように各々の端末から登録された、暗号化された情報およびその各々に関連づけられたフラグ情報が記憶され、被開示者からの特定のフラグ情報についての検索要求に応じて任意の暗号化された情報を被開示者の端末に送信する。

【００６４】

複数の端末が互いに情報を開示している状態では、各々の端末の記憶装置には、フラグ情報の関連づけられたその端末自身の開示対象情報と、同じようにフラグ情報の関連づけられた他の端末から開示された情報とが記憶されている。この状態で、各々の検索手段は、その端末自身の開示対象情報と開示された情報のなかから、特定のフラグ情報に関連づけられた情報を検索し、それを表示することができる。たとえば、図６（ａ）および図７に示す利用者Ａの端末においては、利用者Ａの端末の記憶装置には、利用者Ａの開示対象情報Ｘ１ａ、Ｘ２ａ、Ｘ３ａ、Ｘ４ａ、利用者Ｂから開示された情報Ｘ１ｂ、Ｘ２ｂ、さらに利用者Ｃから開示された情報Ｘ１ｃ、Ｘ２ｃ、Ｘ３ｃが、各々のフラグ情報と関連づけられて記憶されている。フラグ情報の一つが検索用のキーワードである場合、利用者Ａの端末の、主記憶装置３０４上にある、本願発明によるアプリケーションプログラム３０５の指示によって演算装置３０３が、キーボード３０７などで入力されたキーワードの関連づけられた情報を、上記情報の中から検索するなどして、利用者Ａの望む情報を表示装置３１０上の相互開示ウィンドウ６００上に表示することができる。

【００６５】

本願発明では、開示対象情報と、開示関係を決める秘密鍵は、各々独立して被開示者端末に送られ、各々独立して制御できる。この性質を利用すると、端末における情報のバックアップが可能となる。たとえば、図１を参照すると、利用者Ａの端末３００の主記憶装置３０４および外部記憶装置３０１にある情報が何らかの理由ですべて消失したとする。本願発明による方法では、この時に、情報配布サーバ２００に記憶されている暗号化情報のフラグ情報に、利用者Ａの端末をネットワーク上で特定するための情報が含まれていれば、これらフラグ情報を利用して、情報配布サーバ２００は、暗号化情報Ｅｋ１ａ（Ｘ１ａ）、Ｅｋ２ａ（Ｘ２ａ）、Ｅｋ３ａ（Ｘ３ａ）、およびＥｋ４ａ（Ｘ４ａ）を、利用者Ａの端末３００に送信することができる。さらに秘密鍵ｋ１ａおよびｋ２ａは利用者Ｂの端末３２０に、また秘密鍵ｋ２ａおよびｋ３ａは利用者Ｃの端末３４０に、各々のフラグ情報と関連づけて記憶されているので、利用者ＢおよびＣの端末は、これらフラグ情報を利用して、開示制御サーバ１２０を通じて、利用者Ａの端末３００に秘密鍵ｋ１ａ、ｋ２ａおよびｋ３ａを送信することができる。このようにして、利用者Ａの端末は暗号化情報を情報配布サーバ２００から、また秘密鍵を開示制御サーバ１２０からそれぞれ受領することで、開示対象情報Ｘ１ａ、Ｘ２ａ、およびＸ３ａを復元することができる。

【００６６】

ただし、この時、図１を参照すると、Ａの端末３００で消失した開示対象情報Ｘ４ａ秘密鍵ｋ４ａは、他の端末に一切開示されていない。したがって、利用者Ａの端末３００に記憶された秘密鍵ｋ４ａが消失すると、これを復元する手段がなく、たとえ図１のように情報配布サーバ２００に暗号化情報Ｅｋ４ａ（Ｘ４ａ）が記憶されており、これを利用者Ａの端末に戻せたとしても、利用者Ａの端末３００で、開示対象情報Ｘ４ａを復元することができない。この問題を解決するために、利用者Ａの端末３００が、誰にも開示していない開示対象情報Ｘ４ａに対応する秘密ｋ４ａ鍵は、開示制御サーバ１２０に記憶するか、あるいは他の信頼できる利用者の端末に記憶しておく。利用者Ａの端末３００で情報が消

失した場合には、この秘密鍵を受け取ることで、開示対象情報Ｘ４ａを受け取ることができる。このように本願発明によれば、従来の方法で必要だった明示的なバックアップ操作をあらかじめ行わなくとも、利用者Ａの端末の開示対象情報が消失した時に、これらを復元することができる。

【００６７】

また、本願発明によれば、開示対象情報と、開示関係を決める秘密鍵を各々独立して制御できることを利用して、開示関係を保ったまま、開示制御をおこなう権限を他の端末に移動、または他の端末と共有することができる。たとえば、図１に示す状態で、利用者Ａの端末３００から、情報の開示関係を決める秘密鍵ｋ２ａおよびｋ３ａを利用者Ｃの端末３４０に、開示制御サーバ１２０を通じて移動する。すなわちｋ２ａおよびｋ３ａを利用者Ｃの端末へ送った後に、これらを利用者Ａの端末から削除する。このようにすることで、情報Ｘ２ａおよびＸ３ａの開示権を利用者Ｃの端末に移動させることができる。ただし、この開示権の移動の前後で、たとえば、Ｘ２ａが利用者Ｂの端末３２０に開示されているという、開示状態には変化がない。このようにして、開示関係を保ったまま開示制御をおこなう権限を利用者Ａの端末３００から利用者Ｃの端末３４０に同様に、開示対象ごとに移動させることができる。同様に、秘密鍵とそれを制御する権限を異なる端末との間で共有することで、開示権を共有することもできる。

【００６８】

開示者端末から、他の端末への前記秘密鍵の移動や共有によって、開示対象情報ごとに開示を制御する権限を移動または共有を行えるのと同様に、前記秘密鍵を受け取った被開示者端末から、さらに他の端末への前記秘密鍵の移動や共有をおこなうことによって、被開示者端末での被開示情報の再開示を制御することもできる。

【００６９】

前記バックアップや、開示権の移動や共有は、すべてこれらは、開示対象情報ごとの秘密鍵を用いて、開示対象情報とその開示状態が独立して制御できるという、本願発明の性質を利用したものである。この性質によって、本願発明には以下のような効果がある。

【００７０】

第一の効果は、開示対象情報と開示状態を独立して変更できる点である。従来の方法によれば、たとえば利用者Ａの端末から利用者Ｂおよび利用者Ｃの端末に対して情報Ｘ２ａを開示する場合、利用者Ａの端末はＸ２ａの複製を利用者Ｂおよび利用者Ｃの端末に送信し、利用者Ｂおよび利用者Ｃの端末では、Ｘ２ａの複製を受信した後、各々の記憶装置に記憶し、利用者Ｂまたは利用者Ｃの端末に対する入力装置の指示に従って、各々の端末の記憶装置に保存されているＸ２ａの複製を表示装置に表示していた。この従来の方法によれば、利用者Ａの端末において情報Ｘ２ａがＸ２ａ’に更新された場合、利用者Ａは明示的に利用者Ｂの端末および利用者Ｃの端末にＸ２ａ’の複製を送信する操作をおこなう必要があった。すなわち、従来の方法によれば、情報の開示にあたって、開示者は、開示対象の情報と開示先の両方を明示的に指定した上で被開示者の端末に送信する必要があった。

【００７１】

一方で、本願発明による方法では、開示者である利用者Ａは、対象の情報と、その開示状態（開示先）を独立して変更できる。たとえば、利用者Ａの端末３００において、開示対象となる情報Ｘ２ａがＸ２ａ’に更新された場合でもこれに対応する秘密鍵ｋ２ａおよびフラグ情報Ｆｌｇ２ａは変わらない。したがって、利用者Ａの端末３００がそれを秘密鍵ｋ２ａで暗号化したＥｋ２ａ（Ｘ２ａ’）を情報配布サーバ２００に送信し、情報配布サーバ２００は、情報配布サーバの記憶装置２０４のデータベース上でこのＥｋ２ａ（Ｘ２ａ’）とフラグ情報Ｆｌｇ２ａと関連づけて保持しておくことで、利用者Ａは明示的に利用者Ｂおよび利用者Ｃへ更新されたＸ２ａ’を送信しなくとも、利用者Ｂの端末３２０および利用者Ｃの端末３４０への開示状態を変更することなく、利用者Ｂの端末３２０および利用者Ｃの端末３４０から、更新された情報が利用可能となる。逆に、利用者Ａの端末において、開示対象となる情報Ｘ２ａを変えずに、これまで利用者Ｂの端末と利用者Ｃの端末の両方に開示していたところ、さらに利用者Ｄの端末にも開示をするという、開示状

態の変更をおこなう場合でも、開示対象となる情報Ｘ２ａ、秘密鍵ｋ２ａ、およびフラグ情報Ｆｌｇ２ａには何ら変更を加えることなく、開示制御サーバを通じて秘密鍵ｋ２ａとフラグ情報Ｆｌｇ２ａを利用者Ｄの端末に送るだけで、情報Ｘ２ａの開示状態を変更することができる。このように、本願発明による方法は、開示者である利用者Ａは、開示対象となる情報と、その情報の他者端末への開示関係を独立して変更できるという特徴をそなえる。

【００７２】

第二の効果としては、従来の方法と比較して情報開示制御が容易になる点である。従来の方法によれば、サーバを通じて特定の情報を特定の開示先に限定して開示する場合、情報配布サーバがユーザ名、パスワードなどの方法で利用者を認証した後、開示者があらかじめ設定した開示先に対してのみ限定的に開示対象となる情報を送っていた。この方法では、サービス事業者があらかじめすべての利用者のユーザ名やパスワードをデータベースとして持ち、情報の被開示を求める利用者を認証する必要があった。また、端末においても、個々の情報ごとに開示先を設定するための制御手段や、それを開示者が制御するためのＧＵＩが複雑になるという問題があった。これに対して本願発明による方法は、開示者が被開示者に対して秘密鍵やフラグ情報を被開示者に送信する手段さえあれば、従来の方法で必要であったユーザ名やパスワードの管理が不要となり、さらに端末における開示制御やそのためのＧＵＩが単純になるという特徴を具える。このため、従来の方法に比べて、より柔軟な情報開示が可能となる。

【００７３】

第三の効果としては、秘密保持が容易となる点である。従来の方法によれば、開示対象情報は、平文で情報配布サーバに保管され、被開示者からの要求にしたがって、被開示者の端末に送信される。従来の方法でも、秘密保持を目的として、たとえばＳＳＬ（ＳｅｃｕｒｅＳｏｃｋｅｔ　Ｌａｙｅｒ）などの方法によって、ネットワークの通信経路においての暗号化は行われるが、情報配布サーバでは、平文で保管される。このため、情報開示サーバ自体が何らかの事情で公開されてしまうと、この情報配布サーバ上のすべての情報が公開されてしまうという問題があった。また、一般に被開示者の認証手段は必ずしも充分ではなく、開示者が指定した者以外の被開示者に対して情報が開示される危険もあった。ところが本願発明の方法によれば、すべての開示対象情報は、各々対応する秘密鍵で暗号化された状態で情報配布サーバに記憶されているため、万一情報配布サーバの内容が公開されたとしても、これらを復号化するために必要な秘密鍵を入手しない限り、情報配布サーバの秘密は保持される。本願発明による方法では、これらの秘密鍵は数多くの端末に散在しているため、これらをすべて入手することは事実上困難であり、情報配布サーバ上にある情報の秘密保持は容易である。

【００７４】

第四の効果としては、記憶装置の記憶容量が小さな端末でも、その小さな記憶装置を有効に利用して、情報のやりとりが可能となる点である。従来の方法では、被開示者の端末では、開示者より開示された情報を受け取ると、その記憶装置に受け取った開示された情報を記憶しておく必要があった。このため、端末の記憶装置の容量が小さい場合には、多くの開示された情報を保持できない。他の従来の方法では、被開示者が開示対象情報を要求する毎に情報配布サーバより取得することで、被開示者の端末の記憶装置に開示された情報を記憶する必要がなく、前記被開示者の端末の記憶装置の容量が小さくてもよい。しかし、この場合にはネットワークに接続していない場合に、開示された情報が利用できないという問題があった。本願発明による方法では、被開示者の端末の記憶装置には、開示された情報の秘密鍵を記憶している。前記第一の効果で述べたように、本願発明による方法では、これら開示状態を規定する秘密鍵は、開示される情報とは独立している。したがって、開示される情報は、被開示者の端末の記憶装置にあっても、情報配布サーバにあっても、さらには開示者の端末や、第三者の端末にあってもよい。このため、被開示者がネットワークに接続していない場合にも利用したい情報のみを被開示者の端末の記憶装置に記憶しておき、その他の情報は必要に応じて情報配布サーバから取得するなどの方法で、柔

軟に開示された情報を利用することができる。すなわち、本願発明による方法では、被開示者の端末では、その記憶装置の容量や、開示される情報の性質にあわせて、開示される情報を柔軟に管理できるという特徴を具える。

【００７５】

第五の効果としては、開示される情報のバックアップが容易な点である。従来の方法によれば、開示された情報は、被開示者の端末の記憶装置に、情報配布サーバや開示者の端末に存在する情報とは独立して保存されていた。このため、何らかの事情で被開示者の端末の記憶装置の情報が失われた場合、被開示者は情報を失う。これを防ぐために、被開示者はその端末の記憶装置の内容を他の記憶装置にバックアップをとることが多い。しかし本願発明による方法では、たとえば、被開示者の端末の記憶装置の内容がなんらかの事情で失われたとしても、開示者の端末から、開示される情報に対応する秘密鍵とフラグ情報を受領することで、開示された情報を再び利用可能となる。すなわち、被開示者はその端末の記憶装置のバックアップを明示的にとらなくとも、失われた情報を復元できるという特徴を具える。

【００７６】

第六の効果としては、ネットワーク全体の、複写された情報の量を減らすことができる点である。従来の方法による情報開示では、複数の被開示者に情報を開示する場合、開示者の端末で被開示者の数だけの情報の複製を作り、これをすべての被開示者の端末に送り、すべての被開示者の端末ではこの複製を記憶装置に記憶していた。このため、ネットワーク全体では、同じ情報の複製が数多く作られ、これを複数の端末で重複して記憶していた。しかし、本願発明による方法では、被開示者の端末で必ず保存しておかなければならないのは、開示された情報に対応する秘密鍵である。したがって、ネットワークに接続しない時に必要な情報を除き、被開示者端末で、開示された情報の複写を記憶しておく必要はない。この結果、従来の方法と比べて、ネットワーク全体の複写された情報の量を減らすことができるという特徴を具える。

【図面の簡単な説明】

【００７７】

【図１】情報配布サーバと開示制御サーバによる情報開示システムの説明図。

【図２】情報配布サーバの構成要素の一例を説明する図。

【図３ａ】端末の構成要素の一例を説明する図。

【図３ｂ】端末の構成要素の一例を説明する図。

【図４ａ】本願発明による各ステップを説明するフロー図。

【図４ｂ】本願発明による各ステップを説明するフロー図。

【図４ｃ】本願発明による各ステップを説明するフロー図。

【図５ａ】情報開示の制御をおこなうためのグラフィカル・ユーザ・インタフェイスの一例を説明する図。

【図５ｂ】情報開示の制御をおこなうためのグラフィカル・ユーザ・インタフェイスの一例を説明する図。

【図６ａ】複数の端末間で相互に情報開示の制御をおこなうためのグラフィカル・ユーザ・インタフェイスの一例を説明する図。

【図６ｂ】複数の端末間で相互に情報開示の制御をおこなうためのグラフィカル・ユーザ・インタフェイスの一例を説明する図。

【図７】複数の端末間で相互に情報開示の制御をおこなうためのグラフィカル・ユーザ・インタフェイスの一例を説明する図。

【図８】複数の端末間で相互に情報開示をおこなっている時の、情報配布サーバの記憶装置の状態を説明する図。

【符号の説明】

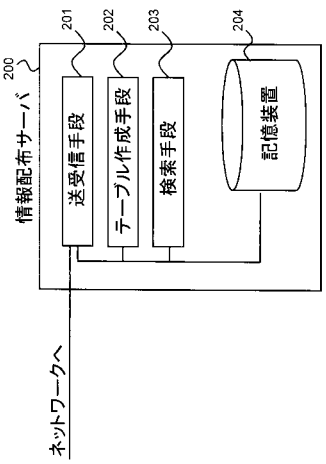
【００７８】

１０　　ネットワーク

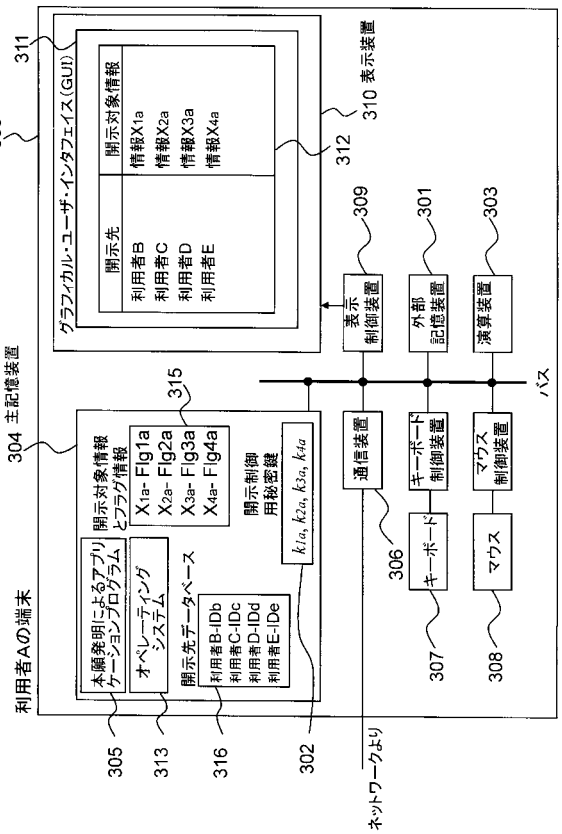
１２０　　開示制御サーバ

２００　　情報配布サーバ
３００、３２０、３４０　利用者端末

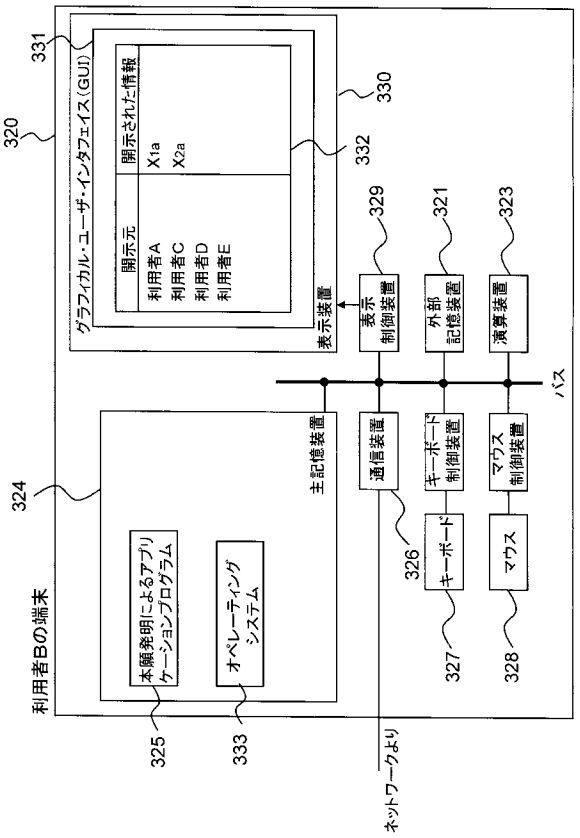
【図２】



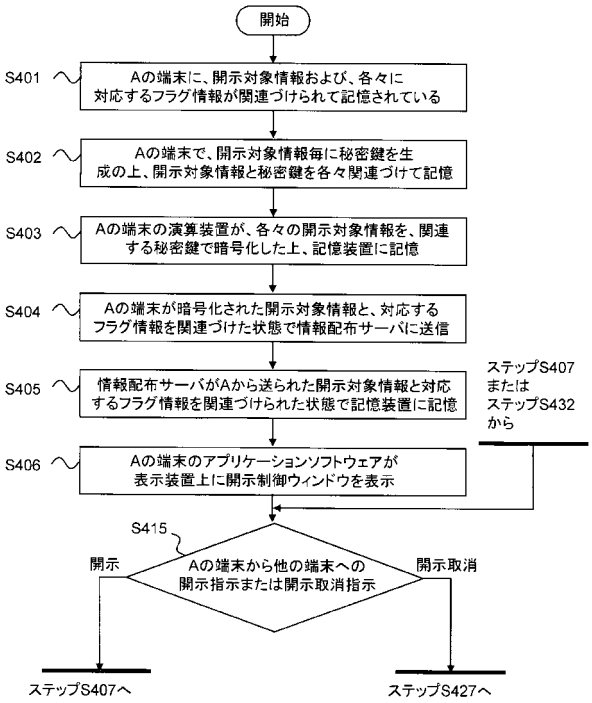
【図３ａ】



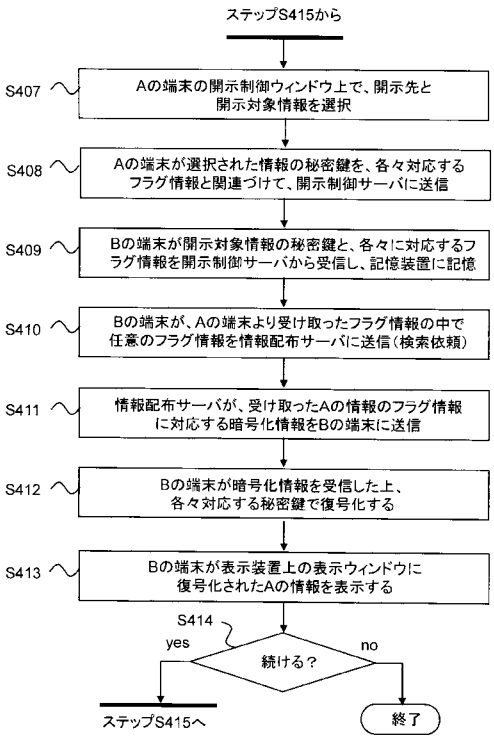
【図３ｂ】



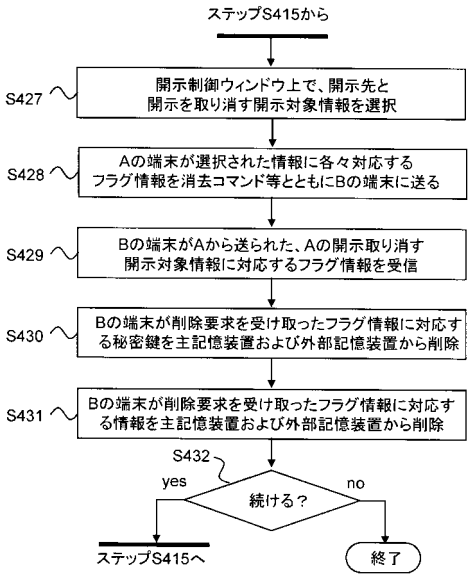
【図４ａ】



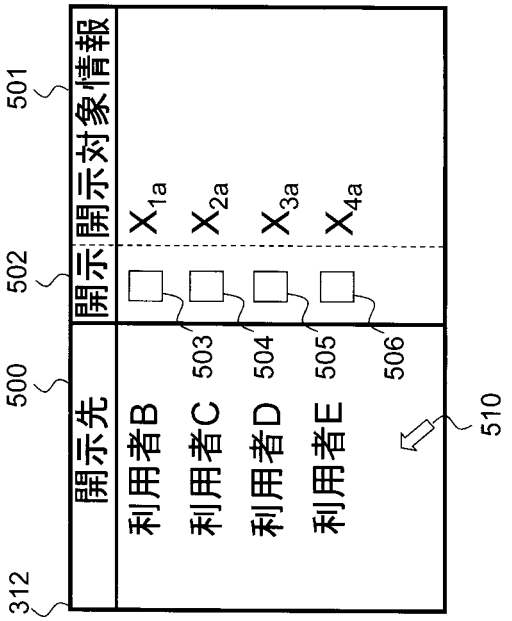
【図４ｂ】



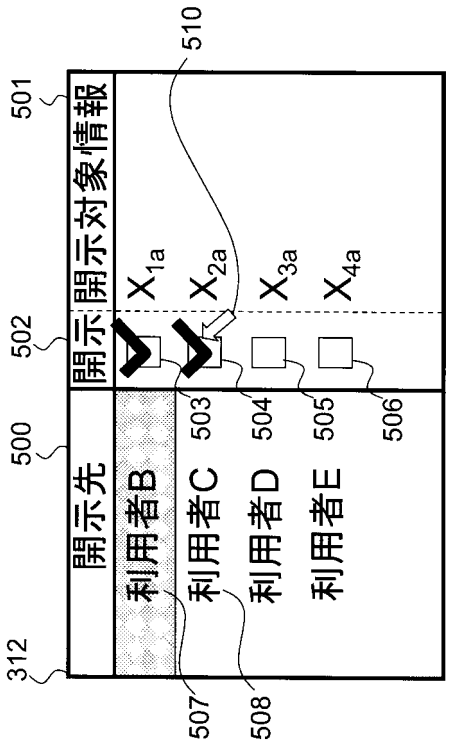
【図４ｃ】



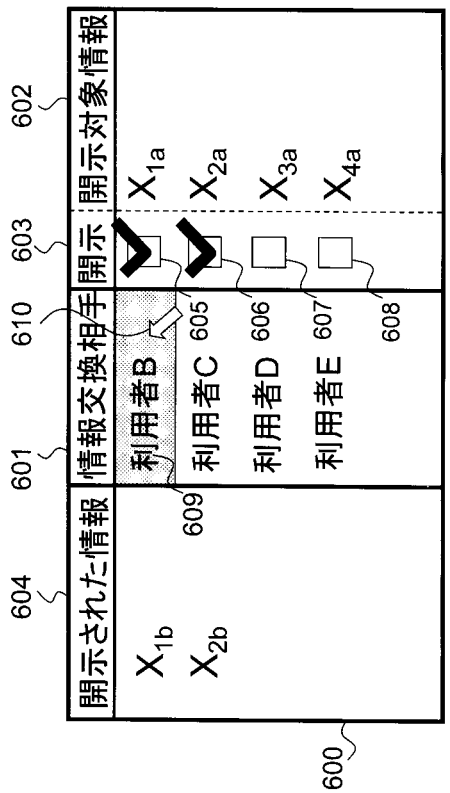
【図５ａ】



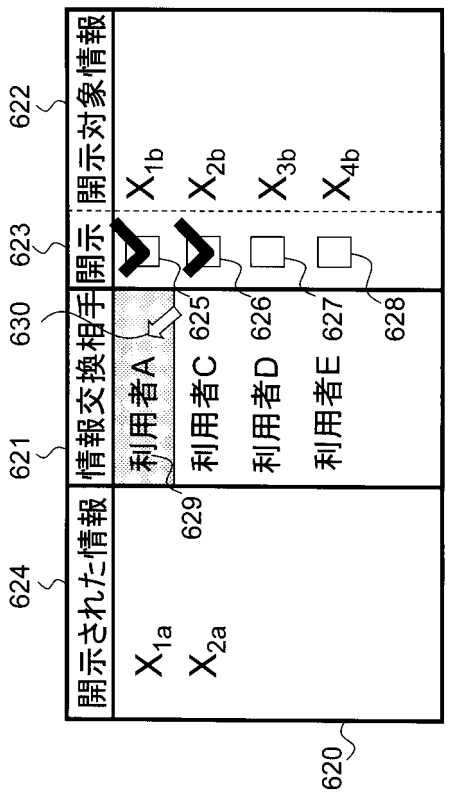
【図５ｂ】



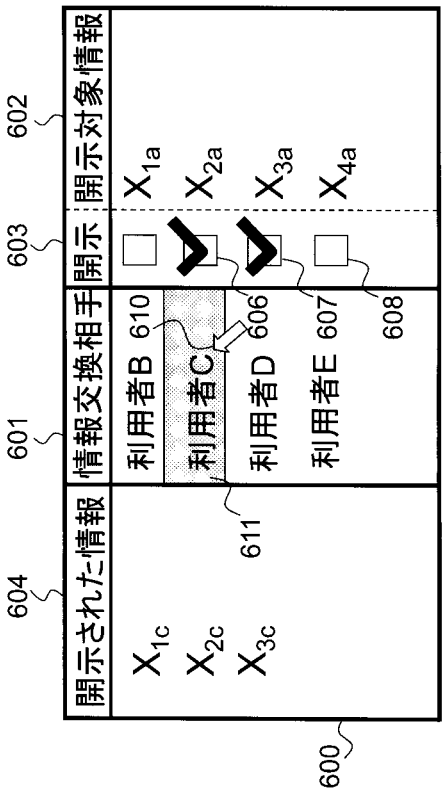
【図６ａ】



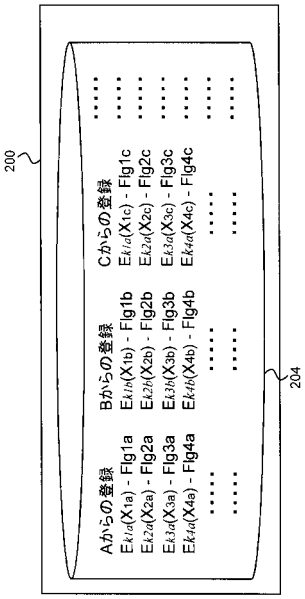
【図６ｂ】



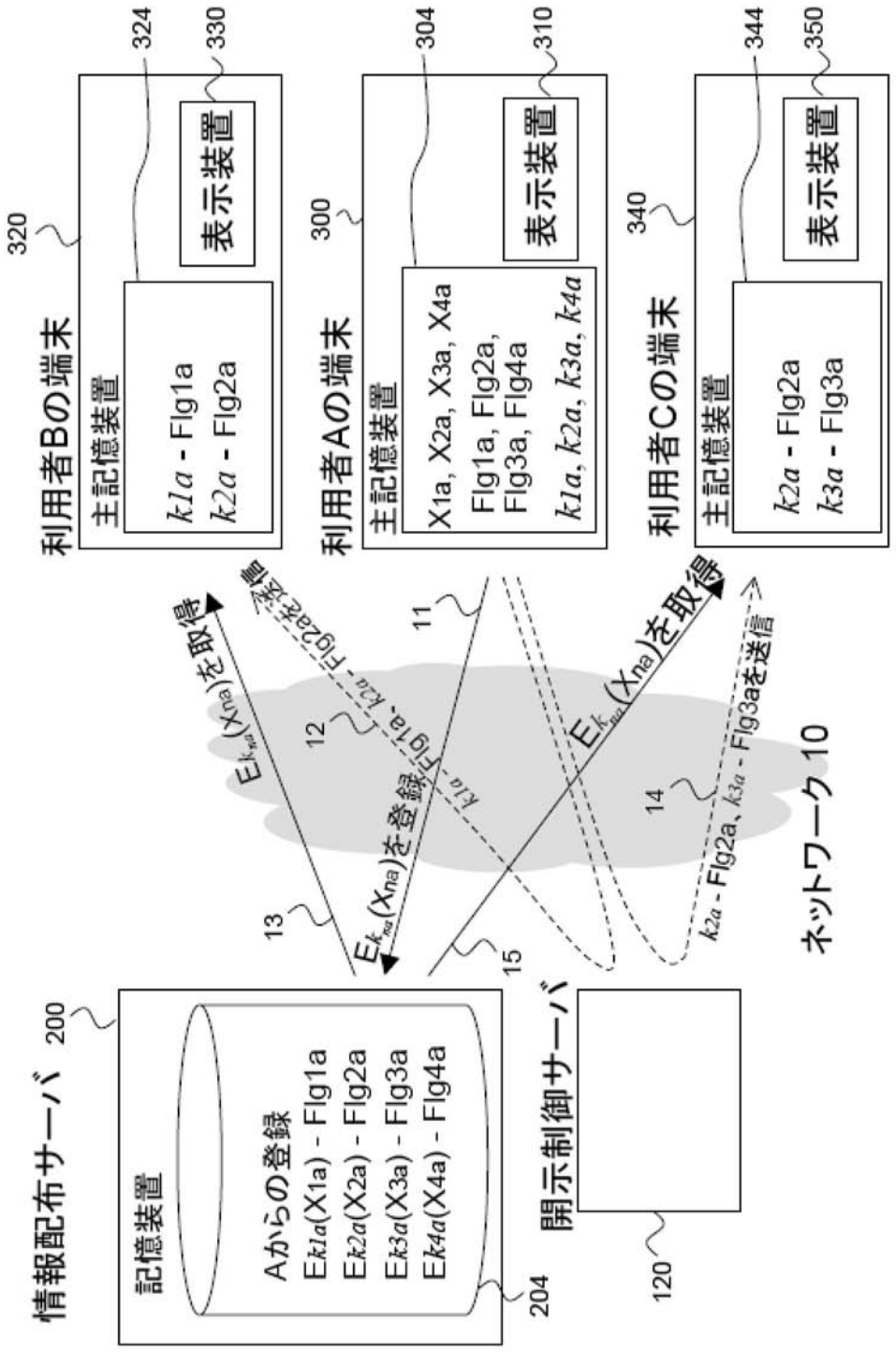
【図７】


開示された情報
情報交換相手
開示
開示対象情報
利用者B
利用者C
利用者D
利用者E
X1c
X2c
X3c
X1a
X2a
X3a
X4a
600
601
602
603
604
606
607
608
610
611

【図８】


200
204
Aからの登録
Bからの登録
Cからの登録
Ek1a(X1a) - Flg1a
Ek2a(X2a) - Flg2a
Ek3a(X3a) - Flg3a
Ek4a(X4a) - Flg4a
Ek1b(X1b) - Flg1b
Ek2b(X2b) - Flg2b
Ek3b(X3b) - Flg3b
Ek4b(X4b) - Flg4b
Ek1c(X1c) - Flg1c
Ek2c(X2c) - Flg2c
Ek3c(X3c) - Flg3c
Ek4c(X4c) - Flg4c

【図１】


情報配布サーバ
200
記憶装置
Aからの登録
Ek1a(X1a) - Flg1a
Ek2a(X2a) - Flg2a
Ek3a(X3a) - Flg3a
Ek4a(X4a) - Flg4a
204
開示制御サーバ
120
ネットワーク 10
利用者Bの端末
320
主記憶装置
324
k1a - Flg1a
k2a - Flg2a
表示装置
330
利用者Aの端末
300
主記憶装置
304
X1a, X2a, X3a, X4a
Flg1a, Flg2a,
Flg3a, Flg4a
k1a, k2a, k3a, k4a
表示装置
310
利用者Cの端末
340
主記憶装置
344
k2a - Flg2a
k3a - Flg3a
表示装置
350
11
12
13
14
15
Ek1a(Xna)を取得
Flg2a - Flg3aを変更
Flg1a - k1aを登録
Ek2a(Xna)を取得
k2a - Flg2a、k3a - Flg3aを送信

フロントページの続き

Ｆターム(参考) 5B285 AA04 BA07 CA02 CA42 CB02 CB63 CB72 DA05
5J104 AA12 AA16 EA01 EA04 EA15 EA16 JA03 MA05 NA02 NA27
NA37 PA07 PA14