(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4794125号
(P4794125)
(45)発行日　平成23年10月19日(2011.10.19)　(24)登録日　平成23年8月5日(2011.8.5)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 12/14 520D

請求項の数 1 (全 14 頁)

(21)出願番号　特願2003-375727(P2003-375727)
(22)出願日　平成15年11月5日(2003.11.5)
(65)公開番号　特開2004-164638(P2004-164638A)
(43)公開日　平成16年6月10日(2004.6.10)
審査請求日　平成18年10月30日(2006.10.30)
(31)優先権主張番号　289528
(32)優先日　平成14年11月6日(2002.11.6)
(33)優先権主張国　米国(US)

(73)特許権者　596170170
ゼロックス　コーポレイション
ＸＥＲＯＸ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国、コネチカット州　０６８５６、ノーウォーク、ピーオーボックス　４５０５、グローバー・アヴェニュー　４５
(74)代理人　100079049
弁理士　中島　淳
(74)代理人　100084995
弁理士　加藤　和詳
(72)発明者　ダイアナ　ケイ.　スメターズ
アメリカ合衆国　９４１３１　カリフォルニア州　サンフランシスコ　シーザー　チャヴェス　ストリート　４３１９　１／２
最終頁に続く

(54)【発明の名称】安全な共有リソース管理方法

(57)【特許請求の範囲】
【請求項１】
ネットワークにおける複数の計算装置間の安全な共有リソースを管理する方法であって、
共有スペースに含まれる少なくとも一つの共有リソースを示す少なくとも一つのデータ構造の第１セットによって定義される該共有スペースの第１の表示を該第１のメンバー計算装置に生成し、
前記第１の表示は、第２の表示および第３の表示とは異なり、前記第１のメンバー計算装置に独自であり、
前記第１のメンバー計算装置から前記共有スペースに含まれる少なくとも１つの共有リソースの第１のセットへのアクセスの提供を受けるために、前記第１の表示および第３の表示とは異なる、第２のメンバー計算装置に独自の、該共有スペースの前記第２の表示を第２のメンバー計算装置に形成するために、第２のメンバー計算装置は前記第１のメンバー計算装置から前記第１の表示で示される前記共有スペースに関する第１の証明書のコピーおよび該第１のメンバー計算装置で生成された第２の証明書のコピーを受信し、
前記第２のメンバー計算装置は、前記第２の表示にもとづいて前記共有スペースへのアクセスを提供するための前記第３の表示を第３のメンバー計算装置に形成するために、該第３のメンバー計算装置に前記第１の証明書のコピー、該第２の表示で示される前記共有スペースに関する第２の証明書のコピー、該第２のメンバー計算装置で生成された第３の証明書のコピーを該第３のメンバー計算装置に提供し、

前記第３の表示は、前記第１の表示および第２の表示とは異なり、前記第３のメンバー計算装置に独自であり、
前記共有スペースは前記共有リソースへのアクセス権限を所有する前記第１のメンバー計算装置に含まれており、
前記第１のメンバー計算装置、第２のメンバー計算装置、第３のメンバー計算装置および少なくとも一つの共有リソースはネットワークを介して接続されており、
前記共有スペースは該共有スペースに含まれる少なくとも一つの共有リソースの第１セットを有し、
前記第２のメンバー計算装置は、前記第１の証明書および第２の証明書のコピー、および、該第２の証明書から第１の証明書へのリンク、を含む第１の証明書チェーンを前記第１のメンバー計算装置に提示することにより、前記少なくとも一つの共有リソースにアクセスすることができ、
前記第３のメンバー計算装置は、前記第１の証明書、第２の証明書および第３の証明書のコピー、および、該第３の証明書から第２の証明書へのリンク、および、該第２の証明書から第１の証明書へのリンクを含む第２の証明書チェーンを前記第１のメンバー計算装置に提示することにより、前記少なくとも一つの共有リソースにアクセスすることができる、
安全な共有リソース管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はデジタル処理システムの中のデジタルデータ処理に係り、より詳しくは、共有リソースにアクセスしようとするデジタルデータ処理システムの複数のコンポーネントのうち、所定基準に基づいていずれのコンポーネントにアクセス権限を付与するかを決定する方法及びシステムに関する。
【背景技術】
【０００２】
メディアストリーム、カメラ、ファイル、プリンタ等の任意のリソースへの安全なアクセスを簡易に行う方法はない。また、リソースへの安全なアクセスをいかなる方法で行うかをエンドユーザに直観的に指定させるシステムはない。システムによっては、アクセス制御リストを作成し、これに基づいてユーザにアクセス権限を付与するものもある。アクセス制御リストを利用すれば、システムリソースへのアクセスを許可し、特定のアクセス権限を付与するユーザを指定できる。例えば、特定のユーザグループが閲覧及び編集の目的で共有ファイルにアクセスできるようにする。しかし、多くのシステムでは、任意のユーザグループにアクセス権限を付与するだけでも、システム管理責任者への介入要請等の煩雑な手続きを要する。例えばユニックス(ＵＮＩＸ（Ｒ）)環境では、ユーザはシステムグループを新規に形成することはできない。マイクロソフト社のウィンドウズ（Ｒ）環境では、ユーザが任意のドメインユーザのリストをアクセス制御リストに追加し、これを１つのファイルに適用することは可能であるが、このアクセス制御リストを多数のファイルに適用するためにはファイル毎に明示的なリストを作成する必要がある。また、ユーザは、セキュリティドメインのメンバーでない特定の個人に対し、明示的なアクセスを許可することはできない。メンバー以外の個人がアクセスを許可されるのは、アクセス制限が設けられていない場合のみである。
【０００３】
リソース管理方法の従来技術として、例えば、非特許文献１乃至３がある。
【０００４】
【非特許文献１】ロペス・Ｃ(Lopes, C)ら著、「空中音声通信(Aerial Acoustic Communication)」、音声への信号処理の応用に関するＩＥＥＥワークショップ(IEEE Workshop on Applications of Signal Processing to Audio and Acoustics)、2001年、p. 21-24
【非特許文献２】フィルディング・Ｒ(Fielding, R)ら著、「複雑な情報プロダクツのウ

ェブベース開発(Web-Based Development of Complex Information Products)」、ＡＣＭ通信(Communications of The ACM)、第41巻、Ｎｏ．８、1998年、p. 84-92
【非特許文献３】ホワイトヘッド・Ｊ(Whitehead, J)ら、”ＷｅｂＤＡＶ、ウェブ上の遠隔協調オーサリングのためのネットワークプロトコル(WebDAC, A Network Protocol for Remote Collaborative Authoring on the Web)”、1999年、[2003年3月11日検索]、インターネット<ＵＲＬ：http://citeseer.nj.nec.com/whitehead99onlinedav.html>

【発明の開示】
【発明が解決しようとする課題】
【０００５】
送信者が第一のセキュリティドメインに、受信者が第二のセキュリティドメインにいる場合、ファイルを電子メールに添付して送信する方法がある。しかしこの方法ではファイルの安全な交換を保証するために鍵や証明書の交換が必要となり、ユーザ構成が複雑となる。また、送信側も受信側もそれぞれのメールサーバにアクセスしなければならないため、リアルタイムでの送受信が必ずしも可能でない。更に、ファイルの移動に伴う遅延や帯域幅に関する要求は、ネットワークの混雑緩和の観点から是認されない場合もある。従ってこの例では、目的とするファイル交換以前の問題としてセキュリティ技術の構築に多大な努力が費やされることになる。
【０００６】
更に、ユーザにとって、共有しているリソースやその共有メンバーを容易に把握することは概ね困難あるいは不可能である。例えば、システム上で明示的なファイル検索を行わない限り、ユーザはあるファイルに対し誰がアクセス権限を持っているかを判断できない。また、例えば、あるファイルに一時的なアクセスを許可されたユーザが誤って無期限のアクセス権限を付与されたり、意図されたものでないファイルへのアクセス権限を付与されたりすることもあり得る。
【課題を解決するための手段】
【０００７】
本発明は、オペレータが安全な共有リソース（ドキュメント、データ、サービス、デバイス等）に容易にアクセスできるようにする等、数多の利益をもたらす。また、本発明により、クライアントは任意のリソースへの安全なアクセスを簡易に行うことができる。オペレータはリソースへの安全なアクセスをいかなる方法で行うかを直観的に指定することができる。更に、本発明で用いられる基礎的なセキュリティシステムの詳細は、オペレータに意識されることはない。本発明では、リソースの共有に関するセキュリティ権の設定は暗黙裡に行われるため、オペレータが共有を希望するリソース毎のセキュリティ権の明示的な設定に関する懸念は不要である。
【０００８】
本発明では、可視性とアクセスとを結び付けているので、オペレータが可視性とアクセスとに別々のアクセス権限を明示的に付与する必要がない。オペレータはリソースの存在を認識するだけでこのリソースにアクセスできる。ユーザは、いかなるリソースを他のユーザと共有しているかを簡単に、即時に把握できる。また、共有リソースグループのメンバーは共通するタスクの達成を目的として活動していることが多く、相互の活動に関する情報を得、それを共有することを望むことから、メンバーは、他のメンバーがいかなるリソースを共有しているかを把握できるとしても関心をもたない。
【発明を実施するための最良の形態】
【０００９】
本発明の諸実施形態の、安全なリソース管理方法及びシステム１０を図１乃至図６に示す。本発明の諸実施形態では、システム１０は、ラップトップ１２（１）、１２（２）、ネットワーク１４及びプリンタ１６を備える。本発明の一実施形態の方法は、共有スペース２０の構築の際に暗号化及び認証技術を利用するラップトップ１２（１）を含む。ラップトップ１２（１）は１つ以上のリソース２２、２４をスペース２０と関連付け、１つ以上のメンバー（ラップトップ１２（２）、１２（３）等）をスペース２０に参加させ、１

つ以上の証明書３０、４０、５０を提示することでメンバー資格を証明できる１つ以上のメンバーに、スペース２０に関連付けられたリソースへのアクセスを許可する。

【００１０】

図１を参照すると、各ラップトップ１２（１）、１２（２）はファイル管理、ワードプロセッシング、情報処理及び表示、電子通信、電話及びファクシミリ通信、ネットワーキング等の種々の機能を実行するポータブルコンピューティングデバイスで構成されている。本発明のデバイスタイプやデバイス数はこれらに限定されない。各ラップトップ１２（１）、１２（２）はプロセッサ、入出力ユニット、メモリ、及びメモリに記憶されたデータを読み出すメカニズムを含む。これらの要素は１つ以上のバスで相互接続されているが、他の結合技術も利用できる。各ラップトップ１２（１）、１２（２）はこれらの要素を用いて、後述するように本発明の諸実施形態のインストラクションを記憶、処理する。

【００１１】

メモリは揮発性メモリ及び不揮発性メモリからなる。ここでは揮発性メモリはランダムアクセスメモリであるが、ダイナミックランダムアクセスメモリやフラッシュメモリも利用できる。不揮発性メモリはハードディスク等の固定データ記憶媒体であるが、フロッピー（Ｒ）ディスク、コンパクトディスク、デジタルビデオディスク、磁気テープ、光ディスク等のポータブルデータ記憶媒体も利用できる。メモリは本発明を実施するためのインストラクション及びデータを記憶し、記憶されたインストラクション及びデータはプロセッサで実行される。インストラクション及びデータの一部もしくは全部を他の場所に記憶させてもよい。

【００１２】

各ラップトップ１２（１）、１２（２）の入出力ユニットは、ＲＦ等の範囲限定(range-limited)信号の送受信が可能な１つ以上のポートを具備し、これにより各ラップトップ１２（１）、１２（２）は信号で相互に通信できる。この他に赤外線信号、コンタクト信号、音声信号等も利用できる。ネットワーク１４との間でデータをやりとりするための１つ以上の別のポートを入出力ユニットに設けてもよい。この実施形態では、各ラップトップ１２（１）、１２（２）は１つ以上のこれらのポートでネットワーク１４に接続されている。ラップトップ１２（１）、１２（２）のようなデバイスは当該技術では周知であり、その構成要素や配置、作用についての説明は割愛する。

【００１３】

ネットワーク１４は、ブルートゥース（Bluetooth：登録商標）ネットワークなどのワイヤレスネットワークの他、タイプの異なるインターネット等のワイヤレスネットワークや、ワイヤベースのネットワークとすることもできる。また、ネットワーク１４により、ラップトップ１２（１）、１２（２）間の相互通信や、ネットワーク１４にアクセスする任意の他のデバイス（コンピュータやプリンタ（図示せず）等）との通信が可能となる。

【００１４】

プリンタ１６は、グラフィカル表示や文章表示を印刷媒体上にレンダリングできるネットワーク印刷デバイスの他、タイプや数の異なるデバイスとすることもできる。プリンタ１６はネットワーク１４に接続されており、ネットワーク１４上のデバイスと通信して印刷要求を受信、処理することが可能である。プリンタ１６等のデバイスは当該技術では周知であり、その構成要素や配置、作用についての説明は割愛する。

【００１５】

ラップトップ１２（１）、１２（２）やプリンタ１６等のデバイスはあくまで例示目的で供される。後述するように、本発明の諸実施形態では、これらのデバイスは本発明の１つ以上の方法を実施するためのインストラクションを記憶、処理、実行できる、タイプの異なるデバイスやシステムを具備してもよい。例えば、図１のデバイスは携帯情報端末（ＰＤＡ）、スキャナ、携帯電話、ビデオカメラレコーダ、音声入出力デバイス、複写デバイス、遠隔操作デバイス、アプライアンス、コンピュータシステムに組み込まれたファイルシステム又はデータベースを具備してもよい。

【００１６】

図２乃至図６を参照して、本発明の諸実施形態の、安全なリソース管理システム１０の作用を説明する。まず、図２及び図３を参照する。ステップ１００で、例えばラップトップ１２（１）のユーザが共有スペース２０の構築を開始する。ラップトップ１２（１）は共有スペース２０へのアクセス権限を有し、また指定された他のデバイスグループ（例えば、ラップトップ１２（２））と共有スペース２０を共有することを希望している。ラップトップ１２（１）、１２（２）は、共有スペース２０の表示をそれぞれ有し、この表示はデバイス毎に変更でき、また異なっていてもよい。共有スペース２０に関連付けられたリソースのセットは動的であり、いったんスペース２０とその認定証(credential)とが作成されると（後述のステップ１２０を参照）、そのメンバーはスペース２０にリソースを追加して共有化し、また所望により削除し、共有を解除できる。リソースは、図３のファイルディレクトリリソース２２等の１つ以上のサービス、ドキュメント、データとすることができる。ファイルディレクトリ２２は、ラップトップ１２（１）に関するローカルファイルリストを表し、この実施形態ではラップトップ１２（２）がこのリストにアクセスできる。

【００１７】

図４を参照する。ステップ１１０で、ラップトップ１２（１）が共有スペース２０を定義する情報を記憶するためのデータ構造のセットを生成し、このデータ構造をラップトップ１２（１）のメモリ内で組織化する。詳細には、データ構造は共有スペース２０に関連付けられた各リソース２２を記述する情報を含む。ステップ１２０で、ラップトップ１２（１）はデバイスに共有スペース２０へのアクセス権限を付与する目的で認証と暗号化に使用されるルート鍵の対を生成する。ラップトップ１２（１）は既存のルート鍵の対を選択して使用してもよい。ステップ１３０で、ラップトップ１２（１）は新しいスペース２０に関するルート証明書３０を生成し、これにデジタル署名する。ステップ１２０で生成されたルート鍵等の必要な任意の秘密や鍵、あるいはシステム１０が利用する後述の特定の認定証付与機構(credentialing mechanism)が必要とする補助情報は、ラップトップ１２（１）がルート証明書３０を作成する際に利用される。

【００１８】

システム１０は標準的な暗号化認証技術を採用しており、後述の方法で公開鍵インフラストラクチャ（ＰＫＩ）を構築する。これにより、共有スペース２０のメンバーはメンバー資格を相互に証明できる。グループ署名方式、識別ベースの暗号化、公開鍵リストや既存の証明書リストの保管、秘密の共有、匿名の認定証等の認証及び暗号化技術も利用できる。ここではＸ．５０９を利用した鍵証明書を例示するが、本発明の諸実施形態では、ＸＭＬ証明書、ＳＰＫＩ証明書、ＷＴＬＳ証明書、属性証明書等を使用してもよい。

【００１９】

Ｘ．５０９を利用した「BasicConstraints」拡張や他の指示子を、ルート証明書３０や、後述の如くルートにより発行される他の指定されたメンバー証明書に追加し、証明書の保持者が他のユーザに共有スペース２０へのアクセス権限を付与するための証明書を発行する権限を有することを示すことができる。これについては後述する。上述のタイプの異なる証明書中の対応する拡張をこの目的で使用してもよい。ルート証明書３０をグループ証明書として指定し、イニシエータ（ここではラップトップ１２（１））によって指定されるグループのフレンドネーム(friendly name)を提供する拡張をルート証明書３０に追加してもよい。また、この拡張は必要に応じてランダム数字等のグループのバイナリ識別子を含んでいてもよい。ルート証明書３０はラップトップ１２（１）のメモリに記憶され、後述のように後続処理に利用される。

【００２０】

図２のステップ２００を参照すると、ラップトップ１２（１）、１２（２）は図５に示すように相互間に安全な通信チャネルを確立する。ラップトップ１２（１）は、入出力ユニットの１つ以上のポートから範囲限定信号を送信する。既述の如く、信号はコンタクト信号、赤外線信号、音声信号及び将来開発される任意の媒体であってもよい。ラップトップ１２（２）が最初に信号を送信する構成も可能である。本発明の諸実施形態では、この

実施形態のネットワーク１４で利用しているBlueTooth（登録商標）等の汎用ワイヤレスチャネルは、検出されない「アクティブな中間者(active man in the middle attacks)の攻撃」を受けやすく、ラップトップ１２（２）や他のデバイスに対して不安定であることから、このような用途には不適当である。これらの範囲限定信号は、ワイヤレスネットワークにおいてラップトップ１２（１）、１２（２）が相互に位置を確認するための情報、例えばラップトップ１２（１）、１２（２）のネットワークアドレスを表す符号化デジタルデータを含む。

【００２１】

メッセージは、ラップトップ１２（１）、１２（２）毎の公開鍵へのコミットメントや暗号化ダイジェスト等の暗号化情報を含んでもよい。この情報は、ステップ３００乃至７００に関連する箇所で詳述するが、ラップトップ１２（１）、１２（２）間に更なる通信を確保するために利用される。次いでラップトップ１２（１）、１２（２）は、公開鍵の交換のためにハンドシェイク方式のプロトコル（例えば、ＳＳＬ／ＴＬＳ）を実行する。他のタイプのハンドシェイク方式のプロトコルを実行してもよい。本発明の諸実施形態において、認証は、上述の安全な通信チャネル確立の際にコミットメントされた公開鍵に対応する秘密鍵を所有していることを相互に証明する、ラップトップ１２（１）、１２（２）のようなデバイスとして定義される。

【００２２】

ステップ３００で、ラップトップ１２（１）はインビテーションメッセージをラップトップ１２（２）に送信し、共有スペース２０へのアクセスを受け入れるようラップトップ１２（２）に要請する。ラップトップ１２（２）はこれに応答してグラフィックユーザインタフェースウィンドウ等のユーザインタフェースを生成、表示し、ラップトップ１２（２）のユーザにこのインビテーションを受けるか否かを問い合わせるようプログラムされることができる。ラップトップ１２（２）のオペレータはマウスやキーボード等のユーザ入力デバイスを操作し、ラップトップ１２（１）からのインビテーションを受けるか否かを示し、共有スペース２０へのアクセス権限を取得する。

【００２３】

ラップトップ１２（２）のオペレータがスペース２０に参加することで共有スペース２０へのアクセス権限を取得しない意思を表明した場合、デシジョンボックス４００では否定（ＮＯ）に進み、スペース２０へのアクセス取得に関してはラップトップ１２（２）の処理が終了する。ラップトップ１２（２）のオペレータが共有スペース２０へのアクセス権限を取得する意思を表明した場合、処理は肯定（ＹＥＳ）に進む。ステップ５００で、スペース２０におけるラップトップ１２（２）のメンバー資格を明示するために、ラップトップ１２（１）は、第二のラップトップ証明書４０に情報を含ませることにより、ラップトップ１２（２）のための第二のラップトップメンバー証明書４０を作成する。本発明の諸実施形態では、ここに記載したことを除けば、第二のラップトップ証明書４０はルート証明書３０と同様である。

【００２４】

図６と（図６の）デシジョンボックス５１０を参照する。第二のラップトップメンバー証明書４０の一部を作成する際に、ラップトップ１２（２）がラップトップ１２（１）に、特定の公開鍵の使用を希望するか否かを、ラップトップ１２（２）に問い合わせるよう、ラップトップ１２（１）をプログラムすることができる。この問い合わせは、ラップトップ１２（１）、１２（２）のオペレータに意識されない形で実行してもよい。この場合、ラップトップ１２（１）、１２（２）は、相互に通信するよう構成される。ラップトップ１２（２）は、所望の鍵を使用する旨を示すようオペレータを促す構成としてもよい。いずれの場合でも、ラップトップ１２（２）が特定の公開鍵の使用を求める旨を表示すれば、処理は肯定に進む。ステップ５２０で、ラップトップ１２（２）は、使用を希望する特定の公開鍵をラップトップ１２（１）に送信する。あるいは、ラップトップ１２（２）は上述のステップ２００の交換時に使用された公開鍵と同一の公開鍵の使用を希望する旨を表示してもよい。次いで、ステップ５５０が後述の方法で実行される。

【００２５】
デシジョンボックス５１０で、ラップトップ１２（２）がラップトップ１２（１）に対し、特定の公開鍵の使用を希望しない旨を表示する場合、処理は否定に進む。ステップ５３０で、ラップトップ１２（１）は公開鍵と秘密鍵の対を生成する。鍵の対の一部は、後述のように第二のラップトップメンバー証明書４０の作成時に使用される。ステップ５４０で、ラップトップ１２（１）は、ステップ５３０で生成された鍵の対に対応する秘密鍵を、ステップ２００で確立され図５に示された安全な通信チャネルを通してラップトップ１２（２）に送信する。

【００２６】
ステップ５５０で、ラップトップ１２（１）は、ステップ５２０でラップトップ１２（２）から送信された公開鍵、又はステップ５３０で自らが作成した公開鍵のいずれかを用いて、第二のラップトップメンバー証明書４０の作成を完了する。また、ラップトップ１２（１）は共有スペース２０の場所を示す情報（例えばＵＲＬ）と、識別された場所において共有スペース２０へのアクセス時に必要なパスワードとを証明書４０に追加する。ラップトップ１２（２）はそのリソース（例えばファイルディレクトリリソース２２）へのアクセスを許可される。ラップトップ１２（１）はこの証明書４０の保持者であるラップトップ１２（２）が他のユーザを共有スペース２０に招待し、アクセス権限を付与するか否かに関する情報を更に追加してもよい。

【００２７】
図２のステップ６００、及び図５を参照する。ラップトップ１２（１）はルート証明書３０と第二のラップトップメンバー証明書４０の両方をラップトップ１２（２）に送信する。ラップトップ１２（２）は証明書３０及び４０をメモリに記憶する。証明書３０及び４０はラップトップ１２（２）の「証明書チェーン」を形成する。ラップトップ１２（２）はこの証明書チェーンを用いて、スペース２０を共有する他のメンバーに対し、自らがスペース２０のメンバーであり、スペース２０へのアクセス権限を付与されていることを証明する。これについてはステップ７００に関連する箇所で詳述する。例えばラップトップ１２（１）の場合、「証明書チェーン」はルート証明書３０のみである。ステップ１１０に関連する箇所で説明したように、ラップトップ１２（２）はラップトップ１２（１）と同様にして共有スペース２０の定義に必要なデータ構造を生成することで、共有スペース２０の独自の表示を生成する。これでラップトップ１２（１）、１２（２）は共有スペース２０のメンバーとなった。

【００２８】
ステップ７００で、ラップトップ１２（２）は、共有スペース２０の内容をラップトップ１２（２）のオペレータに提示するためのグラフィカルユーザインタフェースウィンドウ（図示せず）を生成するためのプログラムインストラクションを実行する。音声インタフェースやテキストベースのインタフェース等も利用できる。ラップトップ１２（２）は、ステップ６００に関連する箇所で説明したように証明書３０及び４０の受信に応答して、これらのインストラクションを実行してもよい。本発明の諸実施形態では、ユーザインタフェースウィンドウを生成するためのインストラクションをラップトップ１２（２）のメモリに記憶しているが、メモリ以外の場所（例えば、他のデバイス）に記憶しておき、ラップトップ１２（２）に動的に提供する構成としてもよい。

【００２９】
共有スペース２０のメンバー（例えばラップトップ１２（２））は、後述のようにスペース２０に対し追加あるいは削除できる。リソース（例えばファイルディレクトリリソース２２）も、後述のようにスペース２０に対し追加あるいは削除できる。従って、ラップトップ１２（２）は表示されたユーザインタフェースウィンドウを、共有スペース２０の状態における変化を反映させて、一定時間毎に更新してもよい。あるいは、後述するように、ラップトップ１２（２）で機能する更新プロトコルから受け取る通知信号に応答して、ラップトップ１２（２）がインタフェースウィンドウを動的に更新するようにしてもよい。

【００３０】
この実施形態では、共有スペース２０は、ステップ１００に関連する箇所で説明したように、ラップトップ１２（１）から提供されるファイルディレクトリリソース２２を含む。このため、ラップトップ１２（２）は共有スペース２０を表すユーザインタフェースウィンドウを、ファイルディレクトリリソース２２等のリソース（図示せず）を表す１つ以上のアイコンと共にモニタに表示できる。既述の如く、ラップトップ１２（２）はスペース２０を表すインタフェースウィンドウを表示することができるため、ラップトップ１２（２）は共有スペース２０に関連付けられたリソース（この実施形態ではファイルディレクトリリソース２２）へのアクセスが可能である。この実施形態では、ラップトップ１２（２）のオペレータは、ラップトップ１２（１）を通じてアクセス可能な、ファイルディレクトリリソース２２へのアクセスを希望することができる。
【００３１】
ラップトップ１２（２）のオペレータは、マウスやキーボード等の入力デバイスを使用して、ファイルディレクトリリソース２２を表す、表示されたグラフィカルアイコン（図示せず）を選択できる。ラップトップ１２（２）は、コンテキストデータにアクセスしたり、選択されたリソース（ここでは、ファイルリソース２２）との間でデータの授受を行ったりするデータ通信セッションを開始するため、記憶されたインストラクションを実行してアイコン選択を検出し、これに応答する構成としてもよい。
【００３２】
後述するように、ラップトップ１２（２）はファイルリソース２２にアクセスすべくラップトップ１２（２）と通信する。ラップトップ１２（２）はラップトップ１２（１）を検出し、ラップトップ１２（１）に対して自らを認証すべく、ステップ２００で生成された暗号化情報をＳＳＬ／ＴＬＳ等のキー交換プロトコルの一部として交換する。詳細には、ラップトップ１２（２）は、共有スペース２０のメンバーであることを証明すべく、ラップトップ１２（１）に対し、秘密部分を所有している公開鍵を証明する、ルート証明書３０及びメンバー証明書４０を所有していることを示す。ラップトップ１２（２）又は他の任意のデバイスが、ラップトップ１２（１）に対し、自らが共有スペース２０のメンバーであることを証明できない場合、ラップトップ１２（１）は共有スペース２０リソースへのアクセス要求を拒絶する。この実施形態では、ラップトップ１２（２）はメンバー証明書４０、及びメンバー証明書４０が他のメンバーをスペースに追加する権限を付与されたスペースの正当なメンバーにより発行されたことを示す証明書を含む、「証明書チェーン」をラップトップ１２（１）に送信する。この実施形態では、証明チェーンはスペース２０に関してはルート証明書３０で終了する。
【００３３】
また、ラップトップ１２（２）は、ラップトップ１２（１）に対し、メンバー証明書４０に提示された公開鍵に対応する秘密鍵を所有していることを証明するに足る情報を送るべきである。この証明は、新鮮さを保証するため、ラップトップ１２（１）、１２（２）間でのメッセージ交換時の署名（例えばランダム値や一時の目的のための値(nonce)）を含んでいてもよい。あるいは、証明はメンバー証明書４０に記された公開鍵により暗号化された値を復号する能力を実証するものであってもよい。ここで、ラップトップ１２（１）はルート証明書３０を作成し、更に第二のメンバー証明書４０を作成してこれをラップトップ１２（２）に付与した。上述のように、ラップトップ１２（２）が第二のメンバー証明書４０における公開鍵に対応する秘密鍵を所有していることを証明するために提供する署名や他の情報を利用することで、ラップトップ１２（１）は他の不審者とではなくラップトップ１２（２）と通信していると判断できる。このように、ラップトップ１２（１）はラップトップ１２（２）が共有スペース２０のメンバーであると結論付ける。
【００３４】
同様に、ラップトップ１２（１）はラップトップ１２（２）に対し、自らのメンバー証明書チェーン（ここでは、ルート証明書３０）と、対応する秘密鍵を所有していることの証明を提示する。これにより、ラップトップ１２（２）は他の不審者とではなくスペース

２０の正当なメンバーと通信し、リソースを要求していることを確認できる。鍵交換プロトコルの一部として、ラップトップ１２（１）、１２（２）は更に、後述するように暗号化、認証及び通信の統合性によって、交換のための更なる通信を確実に行うための共有セッション鍵を生成してもよい。

【００３５】

この結果、ラップトップ１２（１）は認証されたラップトップ１２（２）が、例えば、ラップトップ１２（１）内にあるディレクトリのファイルリストを受け取るべくファイルディレクトリリソース２２にアクセスすることを許可する。ラップトップ１２（１）は、上述のキー交換プロトコルの際にラップトップ１２（１）、１２（２）間に確立されたセッション鍵を用いてこのファイルリストを暗号化する。このため、共有スペース２０のメンバー外のデバイスがラップトップ１２（１）、１２（２）間の通信を傍受したとしても、この実施形態ではファイルリストを復号することは不可能である。

【００３６】

図７を参照しながらシステム１０の別の実施形態を説明する。図７中の参照番号は図１乃至図３のそれと同様である。この実施形態のシステム１０は、更にラップトップ１２（３）を備える。ラップトップ１２（３）は後述するオペレーションが異なる他はラップトップ１２（１）、１２（２）と同様である。共有スペース２０を構築し、ラップトップ１２（２）にスペース２０へのアクセスを許可するステップ１００乃至７００は上述の如く実行される。図７、及び図２、４、６を参照すると、ラップトップ１２（１）の機能をラップトップ１２（２）が実行する他はステップ２００乃至７００が反復される。ラップトップ１２（３）はラップトップ１２（２）の機能を実行する。ゆえに、この実施形態ではラップトップ１２（２）がラップトップ１２（３）に共有スペース２０へのアクセス権限を付与する。

【００３７】

かくして、ステップ２００で、ラップトップ１２（２）、１２（３）は安全な通信チャネルを相互間に確立する。ステップ３００で、ラップトップ１２（２）はインビテーションメッセージをラップトップ１２（３）に送信し、共有スペース２０へのアクセスを受け入れるようラップトップ１２（３）に要請する。デシジョンボックス４００で、ラップトップ１２（３）はラップトップ１２（２）からの要請を受ける。ラップトップ１２（２）がラップトップ１２（３）のための第三のメンバー証明書５０を作成する他はステップ５００乃至５５０が上述の如く実行される。ステップ６００で、ラップトップ１２（２）は「証明書チェーン」をラップトップ１２（３）に送信する。この実施形態では、証明チェーンはルート証明書３０、第二のメンバー証明書４０及び第三のメンバー証明書５０からなっている。この実施形態ではファイルディレクトリリソース２２はラップトップ１２（１）内に存在するため、ステップ７００で、ラップトップ１２（３）はファイルディレクトリリソース２２にアクセスすべく、ラップトップ１２（１）と安全な通信を行う。更に、後述するように、ラップトップ１２（３）は、ラップトップ１２（１）と通信する代わりに、ステップ７００で述べた方法と同様にしてラップトップ１２（２）と通信することにより、ラップトップ１２（２）によって共有スペースに追加される任意のリソースにアクセスしてもよい。

【００３８】

図１乃至図７を参照しながら、システム１０の更に別の実施形態を説明する。共有スペース２０を構築し、ラップトップ１２（２）、１２（３）にスペース２０へのアクセス権限を付与すべくステップ１００乃至７００が上述の如く実行され、ステップ２００乃至７００が反復される。あくまで例であるが、ラップトップ１２（１）のオペレータは別のリソース（例えば、図３のプリンタリソース２４）を、共有スペース２０のメンバー（この実施形態ではラップトップ１２（２）、１２（３）を含む）と共有することを決定する。プリンタリソース２４はネットワーク１４のプリンタ１６を表し、この実施形態ではラップトップ１２（１）がプリンタリソース２４へのアクセス権限を有する。後述するように、ラップトップ１２（１）は、プリンタリソース２４へのアクセス権限を管理すべく個々

にアクセス制御権限を特定したり、アクセス制御リストを作成したりする必要はない。

【００３９】

各ラップトップ１２（１）、１２（２）、１２（３）は、それぞれがスペース２０の状態を記述した情報をエピデミック(epidemic)方式で相互に更新できるようにするプログラムインストラクションを実行してもよい。あるいは、ディスカバリサービスや電子掲示板システムにおいて、暗号化で安全を確保したブロードキャストやマルチキャスト送信、暗号化で安全を確保したアナウンスメントを利用することができる。マルチキャストのように、安全なポイントツーグループ(point-to-group)送信方式が利用される場合、グループイニシエータ（この実施形態では、ラップトップ１２（１））が生成する特定の共有鍵が共有スペース２０の新メンバーに伝達され、使用される。スペース２０のメンバーのみが算出できる鍵を利用することもできる。

【００４０】

この実施形態のようにエピデミック方式で更新を行う場合、スペース２０のメンバーはメンバー資格を得た時点でこれらのインストラクションを実行してもよいし、メンバー資格を保有する期間の任意の時点で実行してもよい。従って、この実施形態では、ラップトップ１２（１）は、スペース２０を詳述する情報（スペース２０のメンバー、メンバーの場所、スペース２０で利用できるリソース、現在オンライン又はオフライン中のメンバー等）を、スペース２０の通信可能な別のメンバー（例えばラップトップ１２（２））に伝える。更に、ラップトップ１２（１）は、スペース２０におけるプリンタリソース２４の利用可能性を示す情報をラップトップ１２（２）に送信する。そして、ラップトップ１２（２）は共有スペース２０の状態に関する自らの更新した情報を、安全な通信が可能な別のメンバー（例えばラップトップ１２（３））に伝える。従って、ステップ７００が実行されると、スペース２０の１つ以上のメンバーがユーザインタフェースウィンドウでプリンタリソース２４を「閲覧」し、アクセスすることが可能となる。

【００４１】

スペース２０の状態に関する情報は、ステップ２００に関連する箇所で述べたタイプの各デバイス間で、ポイントツーポイント(point-to-point)の同期化を行うことで、ラップトップ１２（１）からラップトップ１２（２）、そしてラップトップ１２（３）へと安全に交換され得る。また、この同期化により、スペース２０の更新を行うラップトップ１２（１）、１２（２）、１２（３）がスペース２０の正当なメンバーであり、認証されていないメンバーや非メンバーでないことが確実となる。ラップトップ１２（１）、１２（２）、１２（３）は、スペース２０のメンバー資格を得た際に各々が受け取る認定証(credential)を用いて、ＳＳＬ／ＴＬＳチャネル等の安全なチャネル上で相互に通信する。

【００４２】

１つ以上の証明書３０、４０、５０からの情報を含むこれらの認定証により、メンバーは共有スペース２０のメンバー資格を相互に確認することができる。提示された証明書が共有スペース２０に関連付けられれば、確認は成功である。ステップ１３０に関連する箇所で述べたように、証明書が共有スペース２０独自の識別子を正しく含んでいれば証明書は有効とみなされ、有効な「証明書チェーン」が提示される。有効なチェーンは、共有スペース２０に関するメンバーの証明書（例えば、第三のメンバー証明書５０）からルート証明書３０への間断のないリンクを実証する。また、後述するように、メンバーは共有スペース２０が削除メカニズムを実行した場合、チェーンに含まれるいずれの証明書も削除されていないことを確認してもよい。

【００４３】

ラップトップ１２（１）のオペレータは、共有スペース２０への更なるメンバーの追加を望まず、メンバーの削除を希望することがある。この場合、ラップトップ１２（１）は削除リスト情報を生成し、上記エピデミック方式の更新処理を通じて共有スペース２０のメンバーに伝達する。

【００４４】

共有スペース２０のメンバーは、削除リストを調査し、スペース２０の開始者（ここで

は、ラップトップ１２（１））のデジタル署名の有無を判断することで、削除リストの有効性を確認するよう構成されていてもよい。所定数（例えば、定足数）のメンバーが削除リストにデジタル署名しているか否かを判断すべくリストを調査することもできる。システム１０は、削除リストを利用せず、有効期限の短い認定証を利用することも可能である。同時に、共有スペース２０の指定された、信任されたメンバーだけが新規メンバーを参加させるための新しい認定証を作成できるようにし、削除されたメンバーは認定証の再交付を受けることができないよう要求する。削除リストを利用する別の方法では、共有スペース２０を消滅させ、削除されるメンバーを参加させずにスペース２０を再度構築してもよい。

【００４５】

共有スペース２０のあるメンバー（例えばラップトップ１２（１））が全メンバーから相互に信任を受けたとみなし、このメンバーを共有スペース２０のホスト機能を有するサーバとして機能させる構成も可能である。従って、この実施形態では、共有スペース２０にアクセスを許可されるメンバーに関するアクセス制御はラップトップ１２（１）に委ねられる。これは、ネットワーク接続されたサーバに記憶されたコンポーネント集合体にアクセス制御を行うサービスを各メンバーが実行することとは性質が異なる。

【００４６】

相互に信任された一メンバーではなく、相互に信任されていないメンバー（例えばラップトップ１２（３））を共有スペース２０のホストとしてもよい。この場合、受動的ドキュメント等のリソースはラップトップ１２（３）によってホストされ得る。この実施形態では、各ドキュメントはスペース２０の他のメンバーがアクセスできる鍵で暗号化される。更に、ラップトップ１２（３）はスペース２０の他のメンバーに、ドキュメント自体ではなく、ドキュメントの場所（この例ではラップトップ１２（３））を記述した情報を送信する。この情報は既述のエピデミック方式で更新され、メンバーに送られる。あるいは情報を暗号化し、電子掲示板に送信してもよい。

【００４７】

各ラップトップ１２（１）、１２（２）、１２（３）は、共有スペース２０のコンテンツをコピーし保持できる。コンテンツはドキュメント、データ、ソフトウェア等である。これにより、スペース２０のメンバーはネットワーク１４にアクセスできない場合でも、共有スペース２０の内容に即時にアクセスできる。また、メンバーがスペース２０の現在の状態に関する情報を受信したことを保証する上記更新プロトコルは、ラップトップ１２（１）、１２（２）、１２（３）上で実行される。あるいは、ピアツーピア(peer-to-peer)プロトコル、上記エピデミック方式の更新処理、及び共有スペース２０のコンテンツの指定された「マスタ」コピーに対して同期化されるプロトコル等の他の処理を行ってもよい。

【００４８】

スペース２０の各メンバーは、共有スペース２０への参加を認識するため、それぞれのオペレーションメモリにレコードログ（例えば、リソース（リソース２２、２４等）の追加及び削除に関する情報やスペース２０のメンバーの追加及び削除に関する情報）を保持してもよい。この情報はスペース２０の履歴を提示する際に利用できる。また、スペース２０のロールバックすなわち操作を元に戻す際にも利用できる。この情報の一部を、アクセスを要求するメンバーに限定された日時情報とし、メンバーが要求すれば、このメンバーがメンバー資格を有した期間の履歴情報にのみアクセスを許可するようにしてもよい。更に、履歴情報は暗号化又は署名されてもよく、そのための指定された鍵のセットをメンバーに与えてもよい。

【００４９】

１つ以上の共有リソースグループを共有スペース２０とは別の場所で生成し、同時に存在せしめてもよい。また、１つのグループ（共有スペース２０等）のメンバー（ラップトップ１２（１）等）は、同時に他のグループと関連付けられることができる。同様に、リソース（プリンタリソース２４等）は１つ以上のグループに関連付けられることができる

。

【図面の簡単な説明】

【００５０】

【図１】本発明の諸実施形態に従って安全なリソース管理を提供するシステムを示す図である。

【図２】本発明の諸実施形態に従って安全なリソース管理を提供するプロセスのフローチャートである。

【図３】本発明の諸実施形態に従って安全なリソース管理を提供するシステムの一部を示す機能ブロック図である。

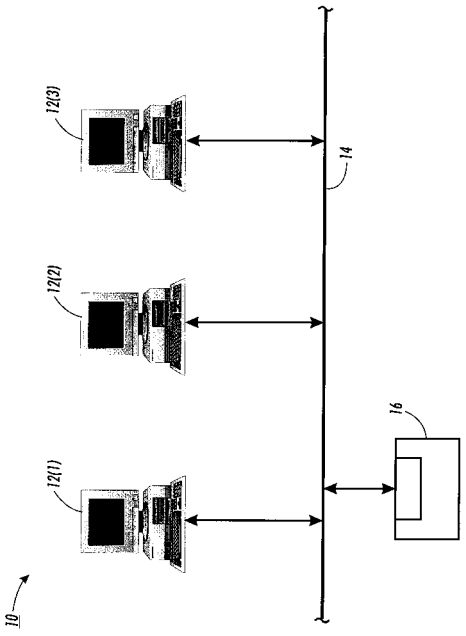
【図４】本発明の諸実施形態に従って、安全なリソース管理を提供するシステム内の共有スペースを構築するプロセスのフローチャートである。

【図５】本発明の諸実施形態に従って、共有スペースへのアクセス権限をメンバーに付与するシステムの一部を示す機能ブロック図である。

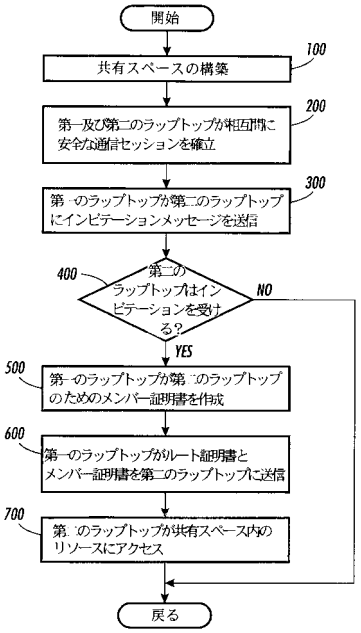
【図６】本発明の諸実施形態に従った、メンバー証明書の作成プロセスを示すフローチャートである。

【図７】本発明の諸実施形態に従って、共有スペースへのアクセス権限をメンバーに付与するシステムの一部を示す機能ブロック図である。

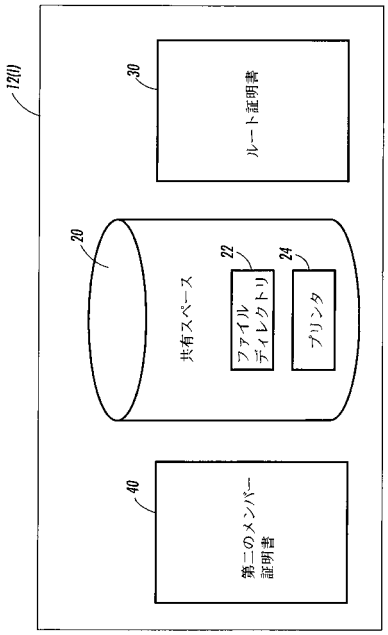
【図１】



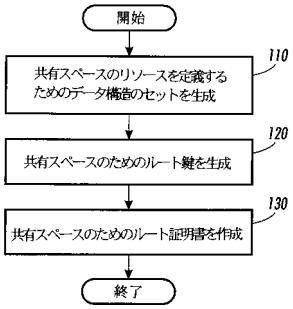
【図２】



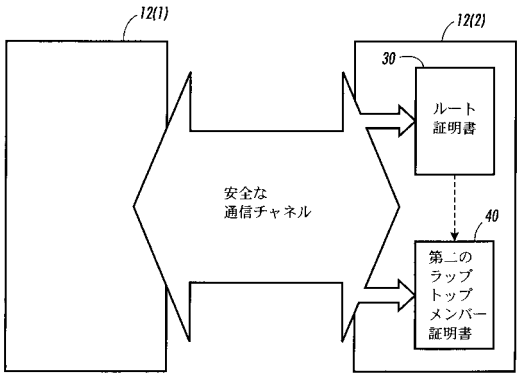
【図３】


12(1)
30
ルート証明書
20
共有スペース
22
ファイルディレクトリ
24
プリンタ
40
第二のメンバー証明書

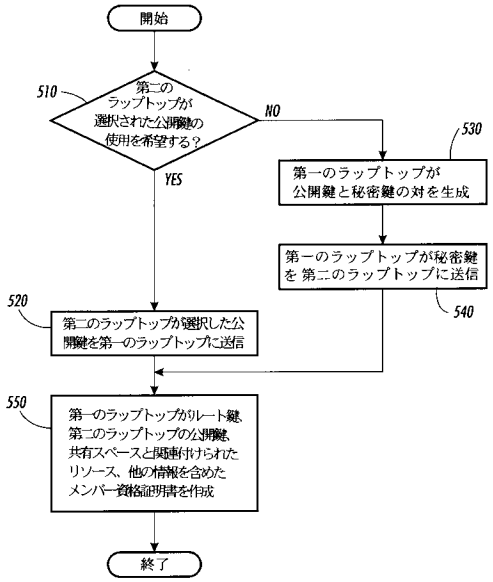
【図４】


開始
共有スペースのリソースを定義するためのデータ構造のセットを生成
110
共有スペースのためのルート鍵を生成
120
共有スペースのためのルート証明書を作成
130
終了

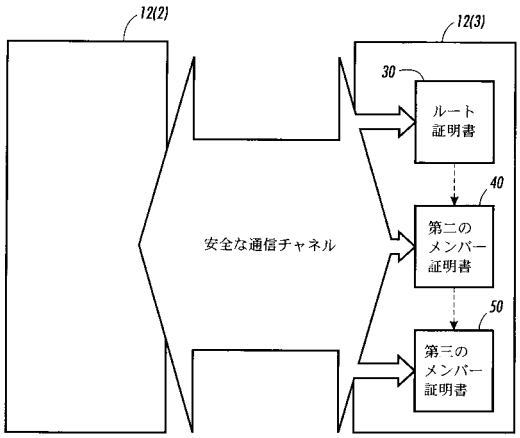
【図５】


12(1)
12(2)
30
ルート証明書
安全な通信チャネル
40
第二のラップトップメンバー証明書

【図６】


開始
510
第二のラップトップが選択された公開鍵の使用を希望する？
NO
YES
530
第一のラップトップが公開鍵と秘密鍵の対を生成
第一のラップトップが秘密鍵を第二のラップトップに送信
540
520
第二のラップトップが選択した公開鍵を第一のラップトップに送信
550
第一のラップトップがルート鍵、第二のラップトップの公開鍵、共有スペースと関連付けられたリソース、他の情報を含めたメンバー資格証明書を作成
終了

【図７】


12(2)
12(3)
30
ルート証明書
40
第二のメンバー証明書
安全な通信チャネル
50
第三のメンバー証明書

フロントページの続き

(72)発明者 ダブリュ. キース エドワーズ
アメリカ合衆国 ９４１１０ カリフォルニア州 サンフランシスコ ウィンフィールド ストリート ８３
(72)発明者 ディルク バルファンツ
アメリカ合衆国 ９４０２５ カリフォルニア州 メンロ パーク シャロン パーク ドライブ ３５０ アパートメント ディー－１
(72)発明者 ハオ－チ ウォン
アメリカ合衆国 ９４０７０ カリフォルニア州 サン カーロス シーダー ストリート ３６８
(72)発明者 マーク ダブリュ. ニューマン
アメリカ合衆国 ９４１１０ カリフォルニア州 サンフランシスコ ボカナ ストリート １６４
(72)発明者 ジャナ ゼット. セディヴィー
アメリカ合衆国 ９４３０６ カリフォルニア州 パロ アルト カートナー アヴェニュー ２５０ ナンバー２２
(72)発明者 トレバー エフ. スミス
アメリカ合衆国 ９４１１０ カリフォルニア州 サンフランシスコ エルシ ストリート ９３
(72)発明者 シャーラム イザディ
イギリス国 オーエックス２５ １キューエイチ オクソン バイセスター アーンコット マーコット ロード ３０

審査官 宮司 卓佳

(56)参考文献 国際公開第０１／０２４０５９（WO，Ａ１）
特開平０６－１８７１１７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２４