(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2005-310096
(P2005-310096A)
(43)公開日　平成17年11月4日(2005.11.4)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 17/60	G06F	17/60　174	5B017
G06F 12/00	G06F	17/60　506	5B058
G06F 12/14	G06F	17/60　510	5B082
G06F 15/00	G06F	17/60　514	5B085
G06K 17/00	G06F	12/00　537D	5B185

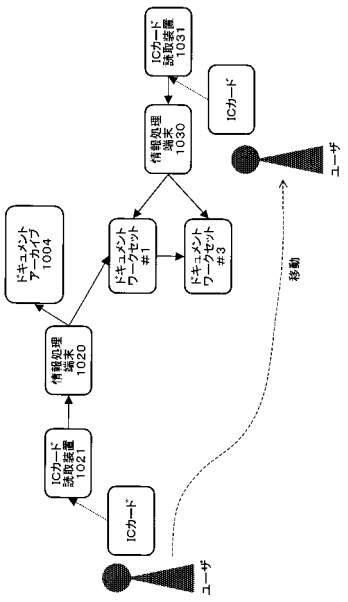
審査請求 未請求　請求項の数 30　ＯＬ　（全 36 頁）　最終頁に続く

(21)出願番号　特願2004-206507 (P2004-206507)
(22)出願日　平成16年7月13日 (2004.7.13)
(31)優先権主張番号　特願2004-88083 (P2004-88083)
(32)優先日　平成16年3月24日 (2004.3.24)
(33)優先権主張国　日本国(JP)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目１７番２２号
(74)代理人　100086531
弁理士　澤田　俊夫
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(72)発明者　堀切　和典
東京都港区赤坂二丁目１７番２２号　富士ゼロックス株式会社内
(72)発明者　山崎　誠
東京都港区赤坂二丁目１７番２２号　富士ゼロックス株式会社内
最終頁に続く

(54)【発明の名称】情報処理システム及び情報処理方法、並びにコンピュータ・プログラム

(57)【要約】
【課題】　ドキュメントやその他のさまざまなメディアなど、会合においてプレゼンテーションに使用される情報資源を好適に管理する。
【解決手段】　ＩＣカードをかざして個人を特定し、情報処理端末経由でシステムにログインした後、個人が所有する情報群すなわち情報アセットの中から今回必要な情報（ドキュメント・ワークセット）を取り出し、表示する。さらに、特定された情報をさらに情報アセットに追加することができる。勿論、このようにして追加された情報アセットは、個人認証を介して別の情報処理端末上でも表示したり、他の参加者へ情報転送を行なったりすることもできる。
【選択図】　図９



【特許請求の範囲】
【請求項１】
複数のユーザの情報アセットを管理する情報処理システムであって、
それぞれユーザ認証装置を備えた複数の情報処理端末と、
各ユーザが所有するドキュメント・ワークセットをユーザの情報アセットとして保持する情報アセット保持装置とを備え、
ユーザはユーザ認証装置による個人認証を経て使用が可能となった情報処理端末を介して前記情報アセット保持装置内の自分のドキュメント・ワークセットにアクセスするとともに、ユーザ認証装置による個人認証を経た他の情報処理端末からのドキュメント・ワークセットへのアクセスを許可する、
ことを特徴とする情報処理システム。
【請求項２】
ユーザは、ユーザ認証装置による個人認証を経て使用が可能となった情報処理端末を介して、所定のドキュメント・アーカイブに蓄積されているドキュメントを利用してドキュメント・ワークセットを作成又は編集し、
前記情報アセット保持装置は、実データからなるドキュメント・ワークセット、又は各ドキュメントに対するドキュメント・アーカイブへのリファレンス情報からなるドキュメント・ワークセットを保持する、
ことを特徴とする請求項１に記載の情報処理システム。
【請求項３】
ユーザは、第１のユーザ認証装置による個人認証を経て使用可能となった第１の情報処理端末上でドキュメント・ワークセットを作成又は編集し、第２のユーザ認証装置による個人認証を経て使用可能となった第２の情報処理端末から該ドキュメント・ワークセットを取り出す、
ことを特徴とする請求項１に記載の情報処理システム。
【請求項４】
第１のユーザが第１のユーザ認証装置による個人認証を経て使用可能となった第１の情報処理端末上でドキュメント・ワークセットを作成又は編集し、
第２のユーザが第２のユーザ認証装置による個人認証を経て使用可能となった第２の情報処理端末から該ドキュメント・ワークセットにアクセスする、
ことを特徴とする請求項１に記載の情報処理システム。
【請求項５】
前記第１の情報処理端末は前記第１のユーザの認証情報を発信する発信機を備えるとともに、前記第２の情報処理端末は受信機を備え、
前記第２の情報処理端末は、受信した第１のユーザの認証情報を用いて前記ドキュメント・ワークセットにアクセスする、
ことを特徴とする請求項４に記載の情報処理システム。
【請求項６】
前記第１の情報処理端末は前記ドキュメント・ワークセットを発信する発信機を備えるとともに、前記第２の情報処理端末はドキュメント・ワークセットを受信する受信機を備える、
ことを特徴とする請求項４に記載の情報処理システム。
【請求項７】
前記第２の情報処理端末は前記ドキュメント・ワークセットへのアクセスを要求する要求信号を発信する発信機を備えるとともに、前記第１の情報処理端末は受信機を備え、
前記第１の情報処理端末は、要求信号を受信したことに応答して前記ドキュメント・ワークセットへのアクセスを許可する、
ことを特徴とする請求項４に記載の情報処理システム。
【請求項８】
前記第２の情報処理端末は、元のドキュメント・ワークセットのコピーをとり、該コピ

ーを操作する、
ことを特徴とする請求項４に記載の情報処理システム。
【請求項９】
ユーザは、認証媒体と該認証媒体に対する書き込み機能を持つ携帯端末を保持し、ユーザが所有するドキュメント・ワークセットへのリファレンス情報と前記情報アセット保持装置内のユーザが所有するドキュメント・ワークセットにアクセスするためのユーザ認証情報とを前記携帯端末から前記認証媒体へ書き込み、
前記情報処理端末は、前記認証媒体からリファレンス情報とユーザ認証情報を読み出し、前記情報アセット保持装置に対するユーザ認証情報を使った個人認証を経て、リファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセットへアクセスする、
ことを特徴とする請求項１に記載の情報処理システム。
【請求項１０】
前記携帯端末は前記認証媒体を内蔵し、前記携帯端末から前記認証媒体へ認証情報を安全に書き込むことができる、
ことを特徴とする請求項９に記載の情報処理システム。
【請求項１１】
前記携帯端末は、ユーザが所有するドキュメント・ワークセット又はその一部にアクセスするための一時的なユーザ認証情報を前記情報アセット保持装置から得て、前記認証媒体に書き込み、
前記情報処理端末は、前記認証媒体からリファレンス情報と一時的なユーザ認証情報を読み出し、前記情報アセット保持装置に対する一時的なユーザ認証情報を使った個人認証を経て、リファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセット又はその中のアクセスが許可されている一部へアクセスする、
ことを特徴とする請求項９に記載の情報処理システム。
【請求項１２】
前記情報処理端末は、認証情報を生成するための素情報を前記認証媒体に書き込み、
前記携帯端末は、前記素情報を基に前記情報処理端末用の認証情報を生成するとともに、前記情報処理端末に対しアクセスを許可するドキュメント・ワークセット又はその一部に対するリファレンス情報を、前記認証情報とともに前記認証媒体に書き込み、
前記情報処理端末は、前記認証媒体からリファレンス情報とユーザ認証情報を読み出し、前記情報アセット保持装置に対するユーザ認証情報を使った個人認証を経て、リファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセット又はその一部へアクセスする、
ことを特徴とする請求項９に記載の情報処理システム。
【請求項１３】
前記携帯端末は、前記情報処理端末とのチャレンジ応答を経て、前記情報処理端末用の認証情報を生成するとともに、前記情報処理端末に対しアクセスを許可するドキュメント・ワークセット又はその一部に対するリファレンス情報を前記認証情報とともに前記認証媒体に書き込み、
前記情報処理端末は、前記認証媒体からリファレンス情報とユーザ認証情報を読み出し、前記情報アセット保持装置に対するユーザ認証情報を使った個人認証を経て、リファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセット又はその一部へアクセスする、
ことを特徴とする請求項９に記載の情報処理システム。
【請求項１４】
前記携帯端末は、前記情報処理端末用の認証情報と、前記情報処理端末に対しアクセスを許可するドキュメント・ワークセット又はその一部に対するリファレンス情報とを前記認証媒体に書き込む前に、前記情報アセット保持装置に対し、前記情報処理端末によるドキュメント・ワークセットに対するアクセス許可を要求する、

ことを特徴とする請求項１２又は１３のいずれかに記載の情報処理システム。
【請求項１５】
前記携帯端末は、前記情報アセット保持装置に対し、前記情報処理端末によるドキュメント・ワークセットに対するアクセス許可を要求し、許可されたことを示す許可情報と許可が得られたドキュメント・ワークセット又はその一部にアクセスするためのリファレンス情報とを前記認証媒体に書き込み、
前記情報処理端末は、前記認証媒体から許可情報とリファレンス情報を読み出し、許可情報とリファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセット又はその中のアクセスが許可されている一部へアクセスする、
ことを特徴とする請求項９に記載の情報処理システム。
【請求項１６】
複数のユーザの情報アセットを管理する情報処理方法であって、
各ユーザが所有するドキュメント・ワークセットをユーザの情報アセットとして管理するステップと、
ユーザが個人認証を経て使用が可能となった情報処理端末を介して自分のドキュメント・ワークセットにアクセスするステップと、
ユーザが個人認証を経た他の情報処理端末からのドキュメント・ワークセットへのアクセスを許可するステップと、
を具備することを特徴とする情報処理方法。
【請求項１７】
ユーザが、個人認証を経て使用が可能となった情報処理端末を介して、所定のドキュメント・アーカイブに蓄積されているドキュメントを利用してドキュメント・ワークセットを作成又は編集するステップをさらに備え、
前記の情報アセットを管理するステップでは、実データからなるドキュメント・ワークセット、又は各ドキュメントに対するドキュメント・アーカイブへのリファレンス情報からなるドキュメント・ワークセットを保持する、
ことを特徴とする請求項１６に記載の情報処理方法。
【請求項１８】
ユーザは、第１のユーザ認証装置による個人認証を経て使用可能となった第１の情報処理端末上でドキュメント・ワークセットを作成又は編集するステップと、
ユーザが、第２のユーザ認証装置による個人認証を経て使用可能となった第２の情報処理端末から該ドキュメント・ワークセットを取り出すステップと、
を備えることを特徴とする請求項１６に記載の情報処理方法。
【請求項１９】
第１のユーザが第１のユーザ認証装置による個人認証を経て使用可能となった第１の情報処理端末上でドキュメント・ワークセットを作成又は編集するステップと、
第２のユーザが第２のユーザ認証処理装置による個人認証を経て使用可能となった第２の情報処理端末から該ドキュメント・ワークセットにアクセスするステップと、
を備えることを特徴とする請求項１６に記載の情報処理方法。
【請求項２０】
前記第１の情報処理端末は前記第１のユーザの認証情報を発信する発信機を備えるとともに、前記第２の情報処理端末は受信機を備え、
前記第２の情報処理端末は、受信した第１のユーザの認証情報を用いて前記ドキュメント・ワークセットにアクセスするステップを備える、
ことを特徴とする請求項１９に記載の情報処理方法。
【請求項２１】
前記第１の情報処理端末は前記ドキュメント・ワークセットを発信する発信機を備えるとともに、前記第２の情報処理端末はドキュメント・ワークセットを受信する受信機を備え、
前記第１の情報処理端末から前記第２の情報処理端末へドキュメント・ワークセットを

転送するステップをさらに備える、
ことを特徴とする請求項１９に記載の情報処理方法。
【請求項２２】
前記第２の情報処理端末は前記ドキュメント・ワークセットへのアクセスを要求する要求信号を発信する発信機を備えるとともに、前記第１の情報処理端末は受信機を備え、
前記第１の情報処理端末が、要求信号を受信したことに応答して前記ドキュメント・ワークセットへのアクセスを許可するステップをさらに備える、
ことを特徴とする請求項１９に記載の情報処理方法。
【請求項２３】
前記第２の情報処理端末は、元のドキュメント・ワークセットのコピーをとるステップをさらに備え、前記第２のユーザは該コピーされたドキュメント・ワークセットを操作する、
ことを特徴とする請求項１９に記載の情報処理方法。
【請求項２４】
ユーザは、認証媒体と該認証媒体に対する書き込み機能を持つ携帯端末を保持しており、
ユーザが所有するドキュメント・ワークセットへのリファレンス情報と、前記情報アセット保持装置内のユーザが所有するドキュメント・ワークセットにアクセスするためのユーザ認証情報とを、前記携帯端末から前記認証媒体へ書き込むステップをさらに備え、
前記のドキュメント・ワークセットへのアクセスを許可するステップでは、前記情報処理端末から、前記認証媒体からリファレンス情報とユーザ認証情報を読み出し、前記情報アセット保持装置に対するユーザ認証情報を使った個人認証を経て、リファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセットへアクセスする、
ことを特徴とする請求項１６に記載の情報処理方法。
【請求項２５】
前記の認証媒体へ書き込むステップでは、前記携帯端末は、ユーザが所有するドキュメント・ワークセット又はその一部にアクセスするための一時的なユーザ認証情報を前記情報アセット保持装置から得て、前記認証媒体に書き込み、
前記のドキュメント・ワークセットへのアクセスを許可するステップでは、前記情報処理端末は、前記認証媒体からリファレンス情報と一時的なユーザ認証情報を読み出し、前記情報アセット保持装置に対する一時的なユーザ認証情報を使った個人認証を経て、リファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセット又はその中のアクセスが許可されている一部へアクセスする、
ことを特徴とする請求項２４に記載の情報処理方法。
【請求項２６】
前記の認証媒体へ書き込むステップでは、前記携帯端末は、前記情報処理端末が前記認証媒体に書き込んだ素情報を基に前記情報処理端末用の認証情報を生成するとともに、前記情報処理端末に対しアクセスを許可するドキュメント・ワークセット又はその一部に対するリファレンス情報を、前記認証情報とともに前記認証媒体に書き込み、
前記のドキュメント・ワークセットへのアクセスを許可するステップでは、前記情報処理端末は、前記認証媒体からリファレンス情報とユーザ認証情報を読み出し、前記情報アセット保持装置に対するユーザ認証情報を使った個人認証を経て、リファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセット又はその一部へアクセスする、
ことを特徴とする請求項２４に記載の情報処理方法。
【請求項２７】
前記の認証媒体へ書き込むステップでは、前記携帯端末は、前記情報処理端末とのチャレンジ応答を経て、前記情報処理端末用の認証情報を生成するとともに、前記情報処理端末に対しアクセスを許可するドキュメント・ワークセット又はその一部に対するリファレンス情報を前記認証情報とともに前記認証媒体に書き込み、

前記のドキュメント・ワークセットへのアクセスを許可するステップでは、前記情報処理端末は、前記認証媒体からリファレンス情報とユーザ認証情報を読み出し、前記情報アセット保持装置に対するユーザ認証情報を使った個人認証を経て、リファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセット又はその一部へアクセスする、
ことを特徴とする請求項２４に記載の情報処理方法。
【請求項２８】
前記携帯端末は、前記情報アセット保持装置に対し、前記情報処理端末によるドキュメント・ワークセットに対するアクセス許可を要求するステップをさらに備える、
ことを特徴とする請求項２６又は２７のいずれかに記載の情報処理方法。
【請求項２９】
前記の認証媒体へ書き込むステップでは、前記携帯端末は、前記情報アセット保持装置に対し、前記情報処理端末によるドキュメント・ワークセットに対するアクセス許可を要求し、許可されたことを示す許可情報と許可が得られたドキュメント・ワークセット又はその一部にアクセスするためのリファレンス情報とを前記認証媒体に書き込み、
前記のドキュメント・ワークセットへのアクセスを許可するステップでは、前記情報処理端末は、前記認証媒体から許可情報とリファレンス情報を読み出し、許可情報とリファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセット又はその中のアクセスが許可されている一部へアクセスする、
ことを特徴とする請求項２４に記載の情報処理方法。
【請求項３０】
複数のユーザの情報アセットを管理するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、
各ユーザが所有するドキュメント・ワークセットをユーザの情報アセットとして管理するステップと、
ユーザが個人認証を経て使用が可能となった情報処理端末を介して自分のドキュメント・ワークセットにアクセスするステップと、
ユーザが個人認証を経た他の情報処理端末からのドキュメント・ワークセットへのアクセスを許可するステップと、
を具備することを特徴とするコンピュータ・プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークを介した複数人による協業的作業を実現する情報処理システム及び情報処理方法、並びにコンピュータ・プログラムに係り、特に、複数の参加者で構成され、ドキュメントやその他のさまざまなメディアを利用したプレゼンテーションが展開される会議の円滑な運営を実現する情報処理システム及び情報処理方法、並びにコンピュータ・プログラムに関する。
【０００２】
さらに詳しくは、本発明は、ドキュメントやその他のさまざまなメディアなど、会合においてプレゼンテーションに使用される情報アセットを管理する情報処理システム及び情報処理方法、並びにコンピュータ・プログラムに係り、特に、会合の各参加者が利用した情報アセットの保管、利用、共有、分配・転送を実現する情報処理システム及び情報処理方法、並びにコンピュータ・プログラムに関する。
【背景技術】
【０００３】
昨今のコンピューティング技術の発展に伴い、コンピュータがオフィスや一般家庭内に深く浸透してきている。これと相俟って、さまざまな適用業務はコンピュータの支援を受けることができるようになってきている。
【０００４】

例えば、企業における産業活動やその他のさまざまに日常生活において、会議が頻繁に行なわれているが、会議室にコンピュータを取り込むことで、会議の運用を支援することができる。

【０００５】

会議支援システムの一例として、遠隔会議システムを取り上げることができる。遠隔会議システムによれば、遠隔に位置する複数の会議室において、カメラやマイクなどの画像・音声入力装置や、モニタやスピーカなどの画像・音声出力装置を設置し、通信回線を利用して、各会議室において行なわれる発言や質疑応答などのイベントを共有し、遠隔地間で議事を同期して進行させることができる。

【０００６】

例えば、複数のユーザが端末装置のネットワーク接続によって対話を可能とした会議システムとしての対話システム制御方式がある（例えば、特許文献１を参照のこと）。この方式によれば、各端末装置において対話への参加、参加者の離脱を処理することによって、自由な参加や離脱を可能にして会議に相当する対話をすることができる。

【０００７】

また、会議の進行上、会議の参加者を撮影した映像や、参加者の初全内容などの音声だけでなく、会議で使用されるホワイトボードや、スライドその他のプレゼンテーション資料など、会議に関連するさまざまな資料を会議室間で共有し、保管することができる。

【０００８】

会議に用いられる共有の資料などの用意や保管を容易に行なうことができる会議システムについて提案がなされている（例えば、特許文献２を参照のこと）。この場合、インターネット上の会議支援ウェブサイトを運営する情報提供装置によりＴＶ電話会議のサービスを提供する第１の工程と、会議参加者（ユーザ）が通信端末を用いるとともに、この情報提供装置を通し、共有資料を用いてリアルタイムで会議を行なう第２の工程とを備え、会議に用いられる共有の資料などの用意や保管を容易に行なうことができ、その場で資料などに書き込みを行なうこともでき、さらにはアプリケーションソフトの違いやバージョンの違いによる不具合も解消することができる。

【０００９】

さらに、会議システムでは、映像や音声などの会議の進行上で発生するさまざまなデータをデジタル化して保存し、さらに、ホワイトボードや、スライドその他のプレゼンテーション資料など、会議に関連するさまざまなメディア・データを、映像や音声すなわち会議の進行と同期させて保管することができる。このように会議に関連するデータを保存しておくことにより、これらを次回の会議において再利用することが可能となる（例えば、非特許文献１を参照のこと）。

【００１０】

会議は、ほぼ毎日、複数の会議において時間毎に開催される。このため、会議毎に捕捉され、蓄積された会議データは膨大であり、その数は日々増加していく。ここで言う会議データは、ドキュメントやその他のさまざまなメディアで構成されるプレゼンテーション資料、さらには議事録などを指し、デジタル化することによりコンピュータ・データベース上で保管することが可能である。

【００１１】

ここで、プレゼンタを始め、プレゼンテーションを聴講した各参加者は、会議での決定事項を見返す、あるいは次回のプレゼンテーションに活用するなどさまざまな目的で、会議データを再利用したいことがある。

【００１２】

会合自体が複数の構成員による協働作業である。したがって、プレゼンテーションで使用されるドキュメントや会議の議事録などの情報資源は、協働作業の１つの成果物、若しくは共有の資産（アセット）であり、構成員がその利益を互いに享受すべきという性質を本来持っている筈である。しかしながら、従来は、この種の会議ベースのシステムにおいては、情報アセットの移動や情報の共有、分配は十分実現されていない。例えば、プレゼ

ンタは、プレゼンテーション資料を書き込んだディスクや機器を持ち運ばなければならない。また、プレゼンテーションを受講した聴衆は、必要に応じてプレゼンタに資料の配布を適宜依頼しなければならない。プレゼンタはこの依頼に個別に応答してディスクのコピーや添付メールの送信など、手作業により情報の分配を行なわなければならない。

【００１３】

一方、これからのコンピュータやネットワークのめざす方向として、「ユビキタス（Ｕｂｉｑｕｉｔｏｕｓ）」が提唱されている。例えば、すべての知識を場所や時間を問わず、取り出すことが望まれている。

【００１４】

「ユビキタス」若しくは「ユビキタス・コンピューティング」という語は、米ゼロックス社のパロアルト研究所の故マーク・ワイザー（Ｍａｒｋ Ｗｅｉｓｅｒ）氏が提唱したことに端を発し、「利用者がどこに移動しても、同じような性能の計算機の能力を利用できる環境」を指している。“コンピューティング”とは言っても、情報へのアクセスに際しＰＣやＰＤＡなどのコンピュータの機器を所持するかは特に問われず、日常の作業空間と渾然一体となってコンピュータが導入され、情報の収集・管理、情報解析やその他の演算処理、情報表示、情報配布といった計算機能力が、ユーザの無意識のうちに提供される。

【００１５】

かかるユビキタス技術が会議システムに適用されることにより、コンピュータ・ファイルなどの形式化された情報はもとより、個々の暗黙的な知識までもすなわち、作業空間のフレキシビリティが高まり、オフィス、企業、国籍といった枠組みを超えたコラボレーションが実現し、ビジネスの可能性が拡大すると本発明者らは思料する。例えば、プレゼンテーションで使用されるドキュメントや会議の議事録などの情報アセットは、会合に加わった協業者間ではほぼ透過的な利用が実現することが期待できよう。

【００１６】

例えば、ファイル共有に関し、一時的に構成されるネットワーク上において各移動型計算機が保有するファイルを各計算機間で共有することができるネットワーク・システムについて提案がなされている（例えば、特許文献３を参照のこと）。この場合、移動型計算機間のメッセージ通信は送信元アドレスと送信先アドレスを指定して行なわれ、ネットワーク上の固定アドレスとネットワークに接続される移動型計算機のアドレスをアドレス変換することで達成される。しかしながら、アドレス変換機と移動型計算機を相互接続する機構と、ファイル共有の可否をあらかじめ定めておく必要がある。ファイル共有に際し意識的な事前手続きが必要であるとともに、形式化されていない情報までも共有することはできない。

【００１７】

また、会議に用いられる共有の資料などの用意や保管を容易に行なうことができる会議システムについて提案がなされている（例えば、特許文献４を参照のこと）。この場合、インターネット・ポータルサイトによりテレビ電話会議のサービスを提供し、会議参加者は通信端末を用いてインターネット・ポータルサイトを通して、共有資料を用いてリアルタイムで会議を行なう。しかしながら、会議参加者の端末にあらかじめアプリケーションをダウンロードしておく必要がある。

【００１８】

【特許文献１】特開平３－１９２８４５号公報
【特許文献２】特開２００２－４１４２９号公報
【特許文献３】特開平８－７０３００号公報
【特許文献４】特開２００２－４１４２９号公報
【非特許文献１】特願２００３－２０１６７３号明細書

【発明の開示】

【発明が解決しようとする課題】

【００１９】

本発明の目的は、複数の参加者で構成され、ドキュメントやその他のさまざまなメディアを利用したプレゼンテーションが展開される会議の円滑な運営を好適に実現することができる、優れた情報処理システム及び情報処理方法、並びにコンピュータ・プログラムを提供することにある。

【００２０】

本発明のさらなる目的は、ドキュメントやその他のさまざまなメディアなど、会合においてプレゼンテーションに使用される情報アセットを好適に管理することができる、優れた情報処理システム及び情報処理方法、並びにコンピュータ・プログラムを提供することにある。

【００２１】

本発明のさらなる目的は、会合の各参加者が利用した情報アセットの保管、利用、共有、分配・転送を好適に実現することかできる、優れた情報処理システム及び情報処理方法、並びにコンピュータ・プログラムを提供することにある。

【課題を解決するための手段】

【００２２】

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、複数のユーザの情報アセットを管理する情報処理システムであって、それぞれユーザ認証装置を備えた複数の情報処理端末と、各ユーザが所有するドキュメント・ワークセットをユーザの情報アセットとして保持する情報アセット保持装置とを備え、ユーザはユーザ認証装置による個人認証を経て使用が可能となった情報処理端末を介して前記情報アセット保持装置内の自分のドキュメント・ワークセットにアクセスするとともに、ユーザ認証装置による個人認証を経た他の情報処理端末からのドキュメント・ワークセットへのアクセスを許可することを特徴とする情報処理システムである。ここで言うユーザ認証装置は、例えばユーザの認証情報を担持するＩＣカードを読み取るＩＣカード読取装置で構成することができる。

【００２３】

本発明に係る情報処理システムは、ネットワーク接続されたネットワーク・コンピューティング環境により実装される。本発明は、例えば遠隔会議システムに適用することができる。この場合、会議システムとして、複数の情報処理端末と参加者が存在する分散型会議室を構成することができる。

【００２４】

この種の分散型会議室においては、ドキュメントやその他のさまざまなメディアなど、会合においてプレゼンテーションに使用される情報資源の好適な管理が必須である。例えば、参加者間においてプレゼンテーションに用いられる資料の情報交換が円滑に行なわれることが好ましい。

【００２５】

本発明によれば、例えばＩＣカードのような認証媒体を導入して、会議の各参加者の認証処理を行なう。そして、ＩＣカードをかざして個人を特定し、情報処理端末経由でシステムにログインした後、個人が所有する情報群すなわち情報アセットの中から今回必要な情報（ドキュメント・ワークセット）を取り出し、表示する。さらに、特定された情報をさらに情報アセットに追加することができる。各ユーザの情報アセットは、情報アセット保持装置としてのドキュメント・アーカイブに蓄積若しくは管理され、情報アセットへのアクセスは所有者であるユーザの個人認証により制限される。勿論、このようにしてドキュメント・アーカイブに蓄積された情報アセットは、個人認証を介して別の情報処理端末上でも表示したり、他の参加者へ情報転送を行なったりすることも可能である。

【００２６】

従来の分散型会議室では、参加者間での情報のコピーが煩雑であった。これに対し、本発明によれば、個人を特定するＩＣカードを各参加者が保持し、最寄りの情報処理端末でカード読み取りによる認証処理を経ることにより、自分の情報（ドキュメント・ワークセット）を表示出力する端末を簡単に変更することができ、また、簡易な操作により参加者

間での情報の転送を行なうことができる。

【００２７】

ここで、ユーザは、ユーザ認証装置による個人認証を経て使用が可能となった情報処理端末を介して、所定のドキュメント・アーカイブに蓄積されているドキュメントを利用してドキュメント・ワークセットを作成又は編集することができる。ここで言うドキュメント・アーカイブは、例えば当該会議システムにおける固有資産としてのドキュメントやさまざまなメディア・データを格納するプライベートなデータ・サーバであってもよいし、あるいはインターネットなどの広域ネットワーク上に構築されたＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）などの広大な情報提供空間がその実体であってもよい。後者の場合、情報提供空間上で公開若しくは使用許諾されているドキュメントやメディア・データを利用してドキュメント・ワークセットを作成又は編集することができる。

【００２８】

また、ドキュメント・ワークセットは、ドキュメントの実データの集合として構成される他、各ドキュメントに対するドキュメント・アーカイブへのリファレンス情報のみで構成されることもある。

【００２９】

本発明に係る情報処理システムによれば、例えば、ユーザは、第１のユーザ認証装置による個人認証を経て使用可能となった第１の情報処理端末上でドキュメント・ワークセットを作成又は編集した後、場所を移動して、第２のユーザ認証処理装置による個人認証を経て使用可能となった第２の情報処理端末から該ドキュメント・ワークセットを取り出すことができる。

【００３０】

また、第１のユーザが第１のユーザ認証装置による個人認証を経て使用可能となった第１の情報処理端末上で作成又は編集したドキュメント・ワークセットを、第２のユーザが第２のユーザ認証処理装置による個人認証を経て使用可能となった第２の情報処理端末からアクセスすることができる。

【００３１】

例えば、前記第１の情報処理端末は前記第１のユーザの認証情報を発信する発信機を備えるとともに、前記第２の情報処理端末は受信機を備え、前記第２の情報処理端末は、受信した第１のユーザの認証情報を用いて前記ドキュメント・ワークセットにアクセスするようにしてもよい。

【００３２】

あるいは、前記第１の情報処理端末は前記ドキュメント・ワークセットを発信する発信機を備えるとともに、前記第２の情報処理端末はドキュメント・ワークセットを受信する受信機を備え、認証処理を経て使用可能状態となっている情報処理端末間でドキュメント・ワークセットそのものを直接伝送するようにしてもよい。

【００３３】

あるいは、前記第２の情報処理端末は前記ドキュメント・ワークセットへのアクセスを要求する要求信号を発信する発信機を備えるとともに、前記第１の情報処理端末は受信機を備え、前記第１の情報処理端末は、要求信号を受信したことに応答して前記ドキュメント・ワークセットへのアクセスを許可するようにしてもよい。

【００３４】

また、前記第２の情報処理端末では、アクセスが許可された元のドキュメント・ワークセットを操作するのではなく、そのコピーをとり、コピーされたドキュメント・ワークセットを操作するようにしてもよい。

【００３５】

なお、認証情報やドキュメント・ワークセット、あるいは要求信号の送受信に用いられる発信機及び受信機は、不正なユーザによる傍受を避けるためには、赤外線やその他の指向性の強い電磁波による通信を適用することが好ましい。

【００３６】

上述したように、認証媒体としてＩＣカードを導入することにより、会議の参加者など個々のユーザの認証処理を安全且つ効率的に行なうことができる。ユーザがＩＣカードのみを携行する場合には、ユーザが自らＩＣカード内の記憶内容を書き換えることができない。これに対し、携帯電話機やＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔ）などの携帯機器にＩＣカード機能が内蔵されている場合には、携帯機器側の演算機能やユーザ・インターフェースを用いてＩＣカード内の記憶内容をユーザがその場で直接書き換えることができることから、上述したような認証を利用したドキュメント・ワークセットへのアクセス手続をより柔軟に運用することができる。

【００３７】

例えば、ユーザは、ＩＣカード機能を内蔵した携帯電話機を保持しているとする。この場合、ユーザ自身が所有するドキュメント・ワークセットの所在を表すＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）などのリファレンス情報を、ドキュメント・ワークセットへアクセスするために必要となるユーザ認証情報とともに、ＩＣカードへ書き込む。ＩＣカードへの書き込みは、携帯電話機のユーザ・インターフェースを用いて行なわれるので、操作性がよい。例えば、携帯電話機上でドキュメント・アーカイブのサイトへ訪れ、所望のドキュメント・ワークセットのＵＲＬを取得し、ＩＣカードへの書き込みを直接指示することができる。

【００３８】

そして、ユーザは、情報処理端末のユーザ認証装置すなわちＩＣカード・リーダへ携帯電話機をかざす。情報処理端末は、ＩＣカードからリファレンス情報とユーザ認証情報を読み出すことができる。そして、ドキュメント・アーカイブに対して、ユーザ認証情報を使った個人認証を行ない、その後、読み出したリファレンス情報を用いることにより、ユーザが所有する（若しくはユーザが指定した）ドキュメント・ワークセットへアクセスすることができる。

【００３９】

このような利用形態では、携帯端末内のＩＣカードには、ユーザが所有するドキュメント・ワークセットへのアクセスを定常的に許可する認証情報、又は一時的に許可する一時的若しくは臨時の認証情報をＩＣカードに書き込むようにすることができる。また、アクセスを許可する対象として、ユーザが所有するドキュメント・ワークセット全体ではなく、その一部のみのリファレンス情報をＩＣカードに書き込むようにすることができる。そして、情報処理端末側では、ＩＣカードからリファレンス情報と一時的なユーザ認証情報を読み出すと、ドキュメント・アーカイブに対し定常的又は一時的若しくは臨時に個人認証を行なうことができ、リファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセット又はその中のアクセスが許可されている一部へアクセスすることができる。

【００４０】

また、ドキュメント・ワークセットにアクセスするための定常的又は一時的若しくは臨時のユーザ認証情報を発行する際に、認証情報を生成するための素情報として、例えば情報処理端末のＵＲＬや情報処理端末自身の証明書を利用することができる。この場合、情報処理端末は、ＩＣカードに自身のＵＲＬや証明書を書き込むことで、ユーザの携帯端末に素情報を渡すことができる。そして、携帯端末側では、このような素情報を基に前記情報処理端末用の認証情報を生成し、情報処理端末に対しアクセスを許可するドキュメント・ワークセット又はその一部に対するリファレンス情報を、作成した認証情報とともにＩＣカードに書き込む。

【００４１】

そして、ユーザは、情報処理端末のユーザ認証装置すなわちＩＣカード・リーダへ携帯電話機をかざす。情報処理端末は、ＩＣカードからリファレンス情報とユーザ認証情報を読み出すと、ドキュメント・アーカイブに対するユーザ認証情報を使った個人認証を経て、リファレンス情報を用いて前記情報アセット保持装置内のドキュメント・ワークセット又はその一部へアクセスすることができる。

【００４２】
また、ユーザが情報処理端末に対し、自分のドキュメント・ワークセットに対するアクセスに必要な認証情報を渡す際に、ユーザの携帯端末と情報処理端末との間で認証手続きを行なうようにしてもよい。例えば、チャレンジ応答に基づく手続により、携帯端末と情報処理端末間で認証を行なうことができる。この場合、携帯端末は、情報処理端末とのチャレンジ応答を経て、前記情報処理端末用の認証情報を生成するとともに、情報処理端末に対しアクセスを許可するドキュメント・ワークセット又はその一部に対するリファレンス情報を認証情報とともにＩＣカードに書き込む。そして、情報処理端末は、ＩＣカードからリファレンス情報とユーザ認証情報を読み出すと、ドキュメント・アーカイブに対してはユーザ認証情報を使った個人認証を行なった後、リファレンス情報を用いてドキュメント・ワークセット又はその一部へアクセスすることができる。

【００４３】
また、上記の場合において、携帯端末は、情報処理端末用の認証情報とドキュメント・ワークセット又はその一部に対するリファレンス情報をＩＣカードに書き込む前に、ドキュメント・アーカイブに対し、情報処理端末によるドキュメント・ワークセットに対するアクセス許可を要求するという手続を付加してもよい。

【００４４】
また、携帯端末は、ドキュメント・アーカイブに対し、情報処理端末によるドキュメント・ワークセットに対するアクセス許可を事前に要求するようにしてもよい。そして、許可されたことを示す許可情報と許可が得られたドキュメント・ワークセット又はその一部にアクセスするためのリファレンス情報を、ＩＣカードに書き込む。この場合、情報処理端末は、ＩＣカードから許可情報とリファレンス情報を読み出すと、許可情報とリファレンス情報を用いてドキュメント・ワークセット又はその中のアクセスが許可されている一部へアクセスすることができる。

【００４５】
また、本発明の第２の側面は、複数のユーザの情報アセットを管理するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、各ユーザが所有するドキュメント・ワークセットをユーザの情報アセットとして管理するステップと、ユーザが個人認証を経て使用が可能となった情報処理端末を介して自分のドキュメント・ワークセットにアクセスするステップと、ユーザが個人認証を経た他の情報処理端末からのドキュメント・ワークセットへのアクセスを許可するステップとを具備することを特徴とするコンピュータ・プログラムである。

【００４６】
本発明の第２の側面に係るコンピュータ・プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第２の側面に係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第１の側面に係る情報処理システムと同様の作用効果を得ることができる。

【発明の効果】

【００４７】
本発明によれば、複数の参加者で構成され、ドキュメントやその他のさまざまなメディアを利用したプレゼンテーションが展開される会議の円滑な運営を好適に実現することができる、優れた情報処理システム及び情報処理方法、並びにコンピュータ・プログラムを提供することができる。

【００４８】
また、本発明によれば、ドキュメントやその他のさまざまなメディアなど、会合においてプレゼンテーションに使用される情報アセットを好適に管理することができる、優れた情報処理システム及び情報処理方法、並びにコンピュータ・プログラムを提供することができる。

【００４９】
また、本発明によれば、会合の各参加者が利用した情報アセットの保管、利用、共有、分配・転送を好適に実現することかできる、優れた情報処理システム及び情報処理方法、並びにコンピュータ・プログラムを提供することができる。
【００５０】
本発明を会議システムに適用して、複数の情報処理端末と参加者が存在する分散型会議室を構成した場合、参加者間における情報アセットの交換を円滑に行なうことができる。例えば、ＩＣカードをかざして個人を特定し、個人が所有する情報群すなわち情報アセットの中から今回必要な情報を取り出し、表示する。さらに、特定された情報をさらに情報アセットに追加することができる。勿論、このようにして追加された情報アセットは、個人認証を介して別の情報処理端末上でも表示したり、他の参加者へ情報転送を行なったりすることもできる。
【００５１】
また、ドキュメント・ワークセットへのアクセス権限を示す認証情報を担持する認証媒体としてＩＣカードを導入する場合、携帯電話機やＰＤＡなどの携帯機器にＩＣカード機能を内蔵することにより、携帯機器側の演算機能やユーザ・インターフェースを用いてＩＣカード内の記憶内容をユーザがその場で直接書き換えることができることから、ドキュメント・ワークセットへのアクセス手続をより柔軟に運用することができるようになる。
【００５２】
本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。
【発明を実施するための最良の形態】
【００５３】
以下、図面を参照しながら本発明の実施形態について詳解する。
【００５４】
図１には、本発明の一実施形態に係る遠隔会議システム１の構成を模式的に示している。同図に示すように、遠隔会議システム１は、複数（図示の例では２つ）の拠点システム１０及び２０が、共有ワークスペース・サーバ３０によって相互接続された構成となっている。同図に示す例では、共有ワークスペース・サーバ３０は、図面の簡素化のため、２つの拠点（すなわち会議システム）を接続するように描かれているが、１対１接続に限定されるものではなく、３地点以上の拠点を相互接続することができるものであると理解されたい。
【００５５】
共有ワークスペース・サーバ３０は、システム間を電話回線などの回線交換系の通信路を用いてスター型結合の中心として位置付けられる多地点接続装置とは異なる。後述するように、共有ワークスペース・サーバ３０は、会議システム間の接続を管理するセッション、会議中に使用したり会議の記録として生成されたりするファイル、会議に関連するリソースへのリファレンス情報、会議の参加者によって行なわれるファイルなどへのアクセスの履歴情報を管理するように構成されている。
【００５６】
拠点システム１０及び２０は、それぞれ独立して動作する会議システムに相当し、拠点毎に会議が運営されている。これら拠点システムは従来のテレビ会議システムをベースにして構成することができる。例えば、映像・音声サーバ１１及び２１が装備され、カメラ、マイクロフォン、モニタ、スピーカなどの画像や音声の入出力を行ない、画像及び音声の符号化及び復号化して他の拠点システムとの間で送受信して、参加者の動作・振る舞いなどを各拠点で共有することができる。
【００５７】
また、双方の会議室に電子黒板１２及び２２を用意して、それぞれの拠点において書き込みを行なったりする。また、各拠点システム間でアプリケーションを共有して操作したりする。本実施形態では、電子黒板１２及び２２上に、共有ワークスペースによって提供

されるグラフィカルなユーザ・インターフェース（ＧＵＩ）が提示され、会議の参加者はこれを操作することによって、マルチメディア通信会議システムへの接続を行なったり、会議に関連するファイルなどの情報にアクセスしたりすることができる（後述）。

【００５８】

各拠点における会議の参加者が、本遠隔会議システム１のユーザとなる。会議の参加者は、共有ワークスペースによって提供されるグラフィカルなユーザ・インターフェースを操作することによって、個々のマルチメディア通信会議システムの呼び出しを行なうので、ユーザはアドレスを意識することなくマルチメディア通信会議システムの接続を行ない、会議に関連するファイルなどの情報に会議システムから容易にアクセスすることができる。

【００５９】

また、各拠点システム１０及び２０には、会議の参加者を認証するための認証装置がそれぞれ装備されている。本実施形態では、各参加者は、個人認証媒体としてのＩＣカードを携行しており、拠点システム１０及び２０は、ＩＣカードにアクセスするカード読取装置１３及び２３を装備して、認証処理や権限の確認などを行なうことができる。なお、ユーザが携行する個人認証媒体は、ＩＣカード単体に限定されず、ＩＣカード機能を内蔵した携帯電話機やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）などの携帯端末であってもよい。

【００６０】

図１に示すような共有ワークスペース型の遠隔会議システム１においては、以下の事柄を実現して、遠隔地間の協働作業を支援することができる。

【００６１】

（１）協業の相手とすぐに接続する。
（２）協業に必要なドキュメントをすぐに取り出す。
（３）協業の結果をすぐに次の工程につなげる。

【００６２】

本実施形態に係る遠隔会議システム１では、各拠点に対して協働作業に必要なモダリティとモダリティのコンビネーションを提供することができる。例えば、音声、プレゼンテーション資料などのファイル、電子黒板、顔の映像の配信と遠隔協働編集をパッケージ化して利用を可能にする。

【００６３】

また、遠隔会議システム１では、協働作業に関連するドキュメントの提示や協働作業に参加するメンバーへの自動接続を行なうことにより、協働作業を行なう空間を個々のグループワーク（拠点）へ個別適応させる。

【００６４】

また、遠隔会議システム１では、リアルタイム協業と非リアルタイム協業の連携を行なう。すなわち、リアルタイム協業を記録（例えば、電子黒板や使用したプレゼンテーション資料を保存）して非リアルタイム協業に連携させたり、ドキュメントをリアルタイム協業に関連付けて非リアルタイム協業を連携させたりする。

【００６５】

本実施形態に係る共有ワークスペース型の遠隔会議システム１の概略的な動作手順を以下に示しておく。

【００６６】

（１）ユーザは、会議システムを利用するときに、共有ワークスペースを選択する（ワークスペースへのログイン又は認識付きアクセス）。

例えば、共有ワークスペースに１対１に対応したＩＣカードを使ってシステムにＩＤを入力する。あるいは、個人でログインしてワークスペースをＧＵＩ操作により選択する。
（２）共有ワークスペースをオープンすることで、現在誰がワークスペースを共有しているか、誰が会議システムで通信中であるかを認識する。
（３）共有ワークスペース内で「会議」を選択すると、その拠点から遠隔会議に参加する

ことができる（全体会議と個人を特定した会議など複数の会議が共有ワークスペースで開かれていてもよい）。
（４）共有ワークスペースにはドキュメントも置くことができ、会議中に文書を参照したり会議の電子黒板上のイメージを保存したりする。
（５）共有ワークスペースは階層化されており、相互のリンクはハイパーリンクによって行なわれる。
（６）共有ワークスペースに参加しつつサブ・ワークスペースを参照することができる。
（７）サブ・ワークスペースを操作して共有ワークスペースに情報を開示する（個人ワークスペースからのドラッグ・アンド・ドロップ）。

【００６７】

ユーザは、自分の所在する拠点システム１０に対し、ＩＣカードをかざすことによって、所定の認証処理を経てシステムにログインすることができる。ログイン後、拠点システム１０では当該ユーザに関連する（権限のある）ワークスペースの一覧が提示される。ここで言うワークスペースは、１つの会議に相当する。また、同じ拠点システム１０に対し、続けて他のユーザがＩＣカードをかざしてログインを要求すると、同様の認証処理を経てログインが許可されると、先にログインしているユーザと共通するワークスペースの一覧が提示される。ここで、特定のワークスペースが選択されると、このワークスペースに紐付けされている共有ドキュメント（ファイル）の一覧が提示される。一方、遠隔の拠点システムにおいて同じワークスペースが選択されると、これら拠点システム間でワークスペースのコネクションが確立し、ローカル拠点システムと同様の動作が行なわれる。そして、ワークスペース内での共有ドキュメントに対するファイル・オープン、編集などの操作の履歴が保持され、検索キーとして後に利用される。ワークスペース内での活動にローカル又はリモートの区別はない。

【００６８】

図２には、拠点システム１０における会議（テレビ会議など）を運営するための拠点サーバ１００の機能構成を模式的に示している。なお、図示しないが、他の拠点システム２０における拠点サーバ２００も同様の構成であると理解されたい。

【００６９】

拠点サーバ１００は、拠点において認証のステップの一部を実行する認証モジュールと、拠点に設置された電子黒板や映像・音声サーバなどの拠点システムを構成するサブシステムのネットワーク・アドレスなどを管理するサブシステム管理モジュール及びこれらを管理する拠点サーバ・マネージャを備えている。

【００７０】

拠点サーバ１００は、接続されたカード読取装置１３を用いて、会議の参加者が持つＩＣカードから読み出される認証情報や権限情報に基づいて、共有ワークスペース・サーバ３０と通信を行ない、ワークスペースの利用を実現する。

【００７１】

各ワークスペースでは、拠点すなわち会議システム間の接続を管理するセッション、会議中に使用したり会議の記録として生成されたりするファイル、会議に関連するリソースへのリファレンス情報、会議の参加者によって行なわれるファイルやリソースなどへのアクセスの履歴情報が管理される。

【００７２】

拠点システム１０内ではグラフィカルなユーザ・インターフェースが提供されている。会議の参加者は、このユーザ・インターフェースを用いてワークスペースに設けられた同一のセッションを指定することで、協業の呼び設定と情報の共有を行なうことができる。また、会議に関連するリソースは、例えば当該拠点システム１０内に存在していてもよいし、拠点内の他の保管場所、又は拠点外のサーバに保管されていてもよく、例えばＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ：資源識別子）形式で記述される。また、アクセス履歴は、アクセスが発生した場所、アクセスしたユーザ（人）、アクセスした時刻などの情報で構成される。

【００７３】
ワークスペース内のそれぞれのセッション、ファイル、リファレンス情報、アクセス履歴情報にはアクセス制御リスト（ＡＣＬ）が割り当てられている。したがって、ワークスペース・マネージャ３１は、ワークスペース単位で利用を管理又は制限することができる他、ワークスペース内のセッション単位、ファイル単位、リファレンス情報単位、あるいはアクセス履歴情報単位という、細かい粒度でアクセス制御を行なうことができる。
【００７４】
拠点サーバ１００は、例えば、ネットワーク接続されるパーソナル・コンピュータ（ＰＣ）やワークステーション（ＷＳ）などの一般的な計算機システム上で所定のサーバ・アプリケーションを起動するという形態で実現される。
【００７５】
図３には、拠点システム１０の実装例を示している。図示の拠点システム１０は、会議参加者などのユーザが情報端末のユーザ・インターフェース（図示しない）経由でアクセスするためのＷｅｂインターフェース１００１と、個人データを管理するディレクトリ・サービス１００２と、ユーザのログインや共有ドキュメント配布時などの認証処理を行なうＩＣカード認証部１００３と、当該拠点内での共有ドキュメントを保管するドキュメント・アーカイブ１００４と、共有ドキュメントに対するアクセス履歴やログイン中のユーザが拠点内で行なったその他の行動履歴をメタデータとして取得し管理するメタデータ・マネージャ１００５と、プレゼンテーション・コントローラ１００６で構成される。
【００７６】
Ｗｅｂインターフェース１００１は、会議参加者などのユーザが情報端末のユーザ・インターフェース（図示しない）経由でアクセスするためのエントリを提供する。
【００７７】
ディレクトリ・サービス１００２は、当該拠点内におけるユーザ（会議参加者）についての個人データを管理する。
【００７８】
ＩＣカード認証部１００３は、ＩＣカードによる超近距離通信技術と耐タンパ性の認証技術（周知）を利用して、ユーザのログインや共有ドキュメント配布時などの認証処理を行なう。
【００７９】
ドキュメント・アーカイブ１００４は、会議で使用するプレゼンテーションファイルなど、当該拠点内での共有ドキュメントを保管する。
【００８０】
メタデータ・マネージャ１００５は、共有ドキュメントに対するアクセス履歴やログイン中のユーザが拠点内で行なったその他の行動履歴、さらには共有ドキュメントの配布（持ち帰り）などの情報を、ワークスペースのバックグラウンドで取得し、メタデータとして管理する。
【００８１】
プレゼンテーション・コントローラ１００６は、会議などのワークスペース上において、ユーザ（すなわち会議参加者）同士でコラボレーションを実現するためのインターフェースを提供する。プレゼンテーション・コントローラ１００６の構成方法はさまざまである。例えば、ディスプレイとキーボードやマウス、タブレットなどの一般的なコンピュータのユーザ・インターフェースをそのまま会議室に設置してもよい。あるいは、プロジェクタによる壁への投影画面と、この投影画面に対するユーザ操作を捕捉するカメラ、ホワイトボードの組み合わせでユーザ・インターフェースを構成する。また、壁面に、共有ドキュメントの印刷、表示、一覧表示などのアプリケーション操作用ボタンを配設する（後述）。勿論、会議室内にユーザの無意識のうちにユーザ・コマンドを検出するプローブを配設するようにしてもよい。
【００８２】
プレゼンテーション・コントローラ１００６の構成次第で、情報へのアクセスに際し、

ＰＣやＰＤＡなどのコンピュータの機器を所持するかは特に問われなくなる。図４には、本発明の一実施形態に係る会議室の概観を示している。図示の作業空間では、会議室と渾然一体となってコンピュータが導入され、情報の収集・管理、情報解析やその他の演算処理、情報表示、情報配布といった計算機能力が、ユーザの無意識のうちに提供されている。すなわち、コンピュータ・ファイルなどの形式化された情報はもとより、個々の暗黙的な知識までもすなわち、作業空間のフレキシビリティが高まり、オフィス、企業、国籍といった枠組みを超えたコラボレーションが実現し、ビジネスの可能性が拡大する。

【００８３】

図１を参照しながら既に説明したように、拠点システム１０及び２０間は、共有ワークスペース・サーバ３０によって相互接続されている。図５には、共有ワークスペース・サーバ３０の機能構成を模式的に示している。

【００８４】

共有ワークスペース・サーバ３０は、協業の単位となるタスクを管理したり利用したりするためのオフジェクトであるワークスペースを各拠点間において共有するために配設される。

【００８５】

ワークスペース・マネージャ３１は、当該遠隔会議システム１内の各拠点において生成されたワークスペースの管理を行なう。

【００８６】

ワークスペース毎にアクセス制御リスト（ＡＣＬ）が設けられており、ワークスペース・マネージャ３１は、会議の参加者が持つＩＣカードから読み出される認証情報や権限情報に基づいて、複数の拠点にまたがるワークスペースの利用を管理又は制限する。

【００８７】

各ワークスペースでは、拠点すなわち会議システム間の接続を管理するセッション、会議中に使用したり会議の記録として生成されたりするファイル、会議に関連するリソースへのリファレンス情報、会議の参加者によって行なわれるファイルやリソースなどへのアクセスの履歴情報が管理される。

【００８８】

ワークスペース内のそれぞれのセッション、ファイル、リファレンス情報、アクセス履歴情報にはアクセス制御リスト（ＡＣＬ）が割り当てられている。したがって、ワークスペース・マネージャ３１は、ワークスペース単位で利用を管理又は制限することができる他、ワークスペース内のセッション単位、ファイル単位、リファレンス情報単位、あるいはアクセス履歴情報単位という、細かい粒度で拠点をまたいだアクセス制御を行なうことができる。

【００８９】

共有ワークスペース・サーバ３０は、例えば、ネットワーク接続されるパーソナル・コンピュータ（ＰＣ）やワークステーション（ＷＳ）などの一般的な計算機システム上で所定のサーバ・アプリケーションを起動するという形態で実現される。

【００９０】

なお、このような遠隔会議システムの仕組み自体については、例えば本出願人に既に譲渡されている特願２００３－３１６４７３号明細書を参照されたい。

【００９１】

次に、会議の参加者としてのユーザが、会合において自分が使用するプレゼンテーション資料を作成するための仕組みについて説明する。

【００９２】

プレゼンテーション資料は、ドキュメントやその他のさまざまなメディアなどで構成される。ここで、ユーザがドキュメントやメディアなどを取り扱うデータ単位のことを「ドキュメント・ワークセット」と呼ぶことにする。例えば１回のプレゼンテーションでは、１つのドキュメント・ワークセットを持ち出し、これをスクリーンなどに表示したり、参加者へ配布したりする。

【００９３】
各ユーザは１以上のドキュメント・ワークセットを所有することができる。一人のユーザが所有するドキュメント・ワークセットの集合を、本明細書では「情報アセット」と呼ぶ。また、システムのユーザ全体（すなわち、すべての会議参加者）の情報アセットのエンティティは、ドキュメント・アーカイブ１００４で保管される。
【００９４】
ドキュメント・ワークセットは、ユーザが編集したドキュメント（データ・エンティティ）を綴じて構成される実ファイルであってもよいし、ドキュメント・アーカイブ１００４に格納されている各ドキュメント（データ・エンティティ）へのリファレンス（ＵＲＬ）の集合であってもよい。あるいは、ドキュメントとリファレンスの組み合わせでドキュメント・ワークセットを構成することもできる。勿論、ドキュメント・アーカイブ１００４も、ファイルやコンテンツのエンティティの保管庫である必要はなく、Ｗｅｂなどの広大な情報空間に散在しているファイルやコンテンツへのリファレンス情報を記録しているだけであってもよい。
【００９５】
ユーザがドキュメント・ワークセットを作成する仕組みについて、図６を参照しながら説明する。
【００９６】
例えば、拠点システム１０毎に、ドキュメント・ワークセットを編集するためのドキュメント・ワークセット・マネージャ１０１０が配設されている。
【００９７】
また、拠点システム１０内には１台以上の情報処理端末１０２０が設置されている。情報処理端末１０２０は、ドキュメント・ワークセット・マネージャ１０１０とはＬＡＮなどを経由して相互接続されているとともに、ＩＣカードの読み取り動作を行なうＩＣカード・リーダ１０２１をローカル接続している。
【００９８】
会議参加者としてのユーザは、自分の認証情報を担持したＩＣカードを所有しており、ＩＣカード・リーダ１０２１にＩＣカードをかざすことにより個人認証が行なわれ、かかる認証処理を経てシステム１０にログインすることができる。そして、ログインに成功したユーザは、情報処理端末１０２０が持つキーボードやマウスなどの入力装置や表示モニタなどの出力装置の使用が許可され、これらユーザ入出力装置を介してドキュメント・ワークセット・マネージャ１０１０によるドキュメント・ワークセットの作成・編集処理を行なうことができる。
【００９９】
ドキュメント・ワークセット・マネージャ１０１０は、ドキュメント・アーカイブ１００４に蓄積されているドキュメントを使用して、ドキュメント・ワークセットを作成することができる。ドキュメント・アーカイブ１００４は、例えば、当該遠隔会議システムの固有資産としてのドキュメントやさまざまなメディア・データを格納するプライベートなデータ・サーバである。あるいは、インターネットなどの広域ネットワーク上に構築されたＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）などの広大な情報提供空間がドキュメント・アーカイブ１００４の実体であってもよい。後者の場合、ドキュメント・ワークセット・マネージャ１０１０は、情報提供空間上で公開若しくは使用許諾されているドキュメントやメディア・データを利用することができる。
【０１００】
また、ドキュメント・ワークセット・マネージャ１０１０は、作成した各ユーザのドキュメント・ワークセットをローカルに蓄積する。各ユーザは１以上のドキュメント・ワークセットを所有することができる。一人のユーザが所有するドキュメント・ワークセットの集合を「情報アセット」と呼ぶ。また、システムのユーザ全体（すなわち、すべての会議参加者）の情報アセットのエンティティは、ドキュメント・アーカイブ１００４で保管される。

【０１０１】
作成されたドキュメント・ワークセットは、ユーザが編集したドキュメント（データ・エンティティ）を綴じて構成される実ファイルであってもよいし、ドキュメント・アーカイブ１００４に格納されている各ドキュメント（データ・エンティティ）へのリファレンス（ＵＲＬ）の集合であってもよい。あるいは、ドキュメントとリファレンスの組み合わせでドキュメント・ワークセットを構成することもできる。
【０１０２】
図７には、ドキュメント・アーカイブ１００４を操作するためのユーザ・インターフェース画面の構成例を示している。図示の例では、ユーザ個人並びに共有それぞれについてのドキュメント・アーカイブを閲覧するためのワークシートが用意されており、ユーザは該当するタブを選択することでワークシートを開くことができる。また、同画面には、「ウォール制御」、「利用者を切り替える」、「会議終了」などの操作ボタンが用意されている。
【０１０３】
また、図８には、ドキュメント・ワークセットを操作するためのユーザ・インターフェースの画面構成例を示している。同図に示す画面では、ユーザが所有するドキュメント・ワークセットが一覧される。ユーザが所有するドキュメント・ワークセットには、ユーザ自身が作成・編集したドキュメント・ワークセットの以外に、他のユーザとの情報交換により得られたものが含まれる。また、同画面には、「先頭」、「最後」、「前頁」、「次頁」、「画面保存」、「画面印刷」、「ファイル印刷」、「閉じる」などの操作ボタンが用意されている。
【０１０４】
続いて、本実施形態に係る会議システムにおいて、情報アセットを移動するための動作手順について説明する。ここでは、会議参加者が、ある情報処理端末上でプレゼンテーション資料を作成し、これをドキュメント・ワークセットとしてシステムに保管しておくとともに、自分の順番が到来したときに、演壇にある情報処理端末上で所望のドキュメント・ワークセットを取り出して表示し、これをスクリーンなどに投影する、といった場面を想定している。
【０１０５】
図９には、この場合のユーザの挙動を図解している。但し、拠点システム１０には、情報処理端末１０２０並びに情報処理端末１０３０が設置され、それぞれ個人認証用のＩＣカード読取装置１０２１並びに１０３１をローカル接続しているものとする。各情報処理端末１０２０並びに情報処理端末１０３０からはドキュメント・アーカイブ１００４並びに認証ユーザのドキュメント・ワークセットにアクセスすることができるものとする。
【０１０６】
まず、ユーザは、情報処理端末１０２０のＩＣカード読取装置１０２１に自分のＩＣカードをかざすことにより、個人認証が行なわれる。そして、認証処理に成功すると、情報処理端末１０２０の使用が可能となり、そのユーザ・インターフェースを介して自分のドキュメント・アーカイブ並びにドキュメント・ワークセットにアクセスすることができる状態となる。
【０１０７】
そして、ユーザは、ドキュメント・アーカイブから必要なファイルを選択し、ドキュメント・ワークセットに配置することで、ドキュメント・ワークセット＃１を作成する。
【０１０８】
さらに、ユーザは、ドキュメント・ワークセットを操作することにより、ドキュメント・ワークセット上のファイルの配置を編集することができる。
【０１０９】
そして、ユーザは、ドキュメント・ワークセットの作成又は編集が終了すると、ＩＣカード読取装置１０２１から自分のＩＣカードを引き離す、あるいは所定のログアウト手順を経て、情報処理端末１０２０からログアウトする。この結果、使用していたユーザ・イ

ンターフェースはクローズする。

【０１１０】

その後、ユーザは、情報処理端末１０３０のところ（例えば演壇）まで移動し、そのＩＣカード読取装置１０３１に自分のＩＣカードをかざすことにより、個人認証が行なわれる。そして、認証処理に成功すると、情報処理端末１０３０の使用が可能となり、そのユーザ・インターフェースを介して自分のドキュメント・アーカイブ並びにドキュメント・ワークセットにアクセスすることができる状態となる。図示の例では、ユーザは、既にドキュメント・ワークセット＃１を所有しているので、情報処理端末１０２０及び１０３０の間でドキュメント・ワークセット＃１が共有する。あるいは、情報処理端末１０３０では、ドキュメント・ワークセット＃１のコピーであるドキュメント・ワークセット＃３を作成し、これを操作する。

【０１１１】

そして、ユーザは、情報処理端末１０３０のユーザ・インターフェースを介してドキュメント・ワークセット＃３を参照することにより、その参照先であるドキュメント・アーカイブにアクセスを行ない、対象となるドキュメントを表示出力することができる。

【０１１２】

複数の端末と参加者が存在する分散型会議室において、従来は、情報を表示する端末の変更や、参加者間の情報のコピーや移動などの操作が煩雑であった。これに対し、図９に示すようなシステムによれば、個人を特定するＩＣカードを各参加者が端末に読み取らせることにより、ドキュメント・ワークセットの表示端末の変更や、参加者間の情報の転送を簡便な手続で行なうことができる。

【０１１３】

なお、上述において、情報処理端末１０３０にログインするのは、ドキュメント・ワークセット＃１を作成したユーザ自身である以外に、ドキュメント・ワークセットのオーナーであるユーザから使用許可を得た他のユーザであってもよい。

【０１１４】

図１０には、上述したような情報アセットを移動するための動作手順を図解している。

【０１１５】

ユーザは、情報処理端末１０２０のＩＣカード読取装置１０２１に自分のＩＣカードをかざすことにより、個人認証が行なわれ、情報処理端末１０２０のユーザ・インターフェースを介して自分のドキュメント・アーカイブ並びにドキュメント・ワークセットにアクセスすることができる。

【０１１６】

そして、ユーザは、ドキュメント・アーカイブから必要なファイルを選択し、ドキュメント・ワークセットに配置することで、ドキュメント・ワークセット＃１を作成する。

【０１１７】

その後、ユーザは、情報処理端末１０２０を離れ、情報処理端末１０３０のところ（例えば演壇）まで移動し、そのＩＣカード読取装置１０３１に自分のＩＣカードをかざすことにより、個人認証が行なわれる。

【０１１８】

そして、ユーザは、情報処理端末１０３０のユーザ・インターフェースを介して自分のドキュメント・アーカイブ並びにドキュメント・ワークセットにアクセスすることができる。ここでは、ドキュメント・ワークセット＃１のコピーであるドキュメント・ワークセット＃３を作成し、これを操作する。

【０１１９】

続いて、本実施形態に係る会議システムにおいて、参加者間で情報アセットを交換するための動作手順について説明する。ここでは、会議参加者が、ある情報処理端末上でプレゼンテーション資料を作成し、これをドキュメント・ワークセットとしてシステムに保管しておくとともに、プレゼンテーション終了後は希望する参加者にドキュメント・ワークセットを転送する、といった場面を想定している。

【０１２０】
図１１には、この場合のユーザの挙動を図解している。但し、拠点システム１０には、情報処理端末１０２０並びに情報処理端末１０４０が設置され、それぞれ個人認証用のＩＣカード読取装置１０２１並びに１０４１をローカル接続しているものとする。各情報処理端末１０２０並びに情報処理端末１０４０からはドキュメント・アーカイブ１００４並びに認証ユーザのドキュメント・ワークセットにアクセスすることができるものとする。
【０１２１】
まず、ユーザは、情報処理端末１０２０のＩＣカード読取装置１０２１に自分のＩＣカードをかざすことにより、個人認証が行なわれる。そして、認証処理に成功すると、情報処理端末１０２０の使用が可能となり、そのユーザ・インターフェースを介して自分のドキュメント・アーカイブ並びにドキュメント・ワークセットにアクセスすることができる状態となる。
【０１２２】
そして、ユーザは、ドキュメント・アーカイブから必要なファイルを選択し、ドキュメント・ワークセットに配置することで、ドキュメント・ワークセット＃１を作成する。さらに、ユーザは、ドキュメント・ワークセットを操作することにより、ドキュメント・ワークセット上のファイルの配置を編集することができる。
【０１２３】
ここで、ドキュメント・ワークセット＃１のオーナーシップを持つユーザは、情報交換を許可するユーザを特定するための情報を、例えばドキュメント・ワークセット・マネージャに与えておく。
【０１２４】
情報交換先となるユーザは、情報処理端末１０４０のところまで移動し、そのＩＣカード読取装置１０４１に自分のＩＣカードをかざすことにより、個人認証が行なわれる。そして、認証処理に成功すると、情報処理端末１０３０の使用が可能となり、そのユーザ・インターフェースを介してドキュメント・アーカイブ並びに情報交換されたドキュメント・ワークセット＃１にアクセスすることができる状態となる。あるいは、情報処理端末１０４０では、ドキュメント・ワークセット＃１のコピーであるドキュメント・ワークセット＃４を作成し、これを操作する。
【０１２５】
そして、情報交換の相手であるユーザは、情報処理端末１０４０のユーザ・インターフェースを介してドキュメント・ワークセット＃４を参照することにより、その参照先であるドキュメント・アーカイブにアクセスを行ない、対象となるドキュメントを表示出力することができる。
【０１２６】
図１２には、上述したような情報アセットを交換するための動作手順を図解している。
【０１２７】
ユーザは、情報処理端末１０２０のＩＣカード読取装置１０２１に自分のＩＣカードをかざすことにより、個人認証が行なわれ、情報処理端末１０２０のユーザ・インターフェースを介して自分のドキュメント・アーカイブ並びにドキュメント・ワークセットにアクセスすることができる。
【０１２８】
そして、ユーザは、ドキュメント・アーカイブから必要なファイルを選択し、ドキュメント・ワークセットに配置することで、ドキュメント・ワークセット＃１を作成する。
【０１２９】
その後、プレゼンテーションの聴講などによりドキュメント・ワークセットの交換を希望するユーザは、情報処理端末１０４０のところまで移動し、そのＩＣカード読取装置１０４１に自分のＩＣカードをかざすことにより、個人認証が行なわれる。
【０１３０】
そして、ユーザは、情報処理端末１０４０のユーザ・インターフェースを介してドキュ

メント・アーカイブ並びに情報交換されたドキュメント・ワークセット＃１にアクセスすることができる。ここでは、ドキュメント・ワークセット＃１のコピーであるドキュメント・ワークセット＃４を作成し、これを操作する。

【０１３１】

上述した例では、ドキュメント・ワークセット＃１のオーナーシップを持つユーザは、情報交換を許可するユーザを特定するための情報を、例えばドキュメント・ワークセット・マネージャに与えておくようにしたが、その他の形態により情報交換先を指定することができる。例えば、ドキュメント・ワークセット＃１のオーナーシップを持つユーザは、情報交換先となるユーザにその使用許可を表す認証情報を送信するようにしてもよい。

【０１３２】

図１３に示す例では、ユーザ間でドキュメント・ワークセットの使用許可を表した認証情報を送受信することにより情報交換を実現するための挙動を図解している。

【０１３３】

ドキュメント・ワークセット＃１のオーナーシップを持つユーザは、使用許可を表した認証情報を発信する発信機１０２２を備えた情報処理端末１０２０を操作する。また、情報交換の相手となる他のユーザは、この認証情報を受信する受信機１０５２を備えた情報処理端末１０５０を操作するものとする。

【０１３４】

ここで、発信機１０２２並びに受信機１０５２間では、例えば電磁波を媒体とする無線通信により認証情報の交換を行なうものとする。但し、傍受などにより不正なユーザが認証情報を取得することを避けるためには、赤外線やその他の指向性の強い電磁波による通信を適用することが好ましい。

【０１３５】

まず、ユーザは、情報処理端末１０２０のＩＣカード読取装置１０２１に自分のＩＣカードをかざすことにより、個人認証が行なわれる。そして、認証処理に成功すると、情報処理端末１０２０の使用が可能となり、そのユーザ・インターフェースを介して自分のドキュメント・アーカイブ並びにドキュメント・ワークセットにアクセスすることができる状態となる。

【０１３６】

そして、ユーザは、ドキュメント・アーカイブから必要なファイルを選択し、ドキュメント・ワークセットに配置することで、ドキュメント・ワークセット＃１を作成する。さらに、ユーザは、ドキュメント・ワークセットを操作することにより、ドキュメント・ワークセット上のファイルの配置を編集することができる。

【０１３７】

ここで、ドキュメント・ワークセット＃１のオーナーシップを持つユーザは、情報交換の相手となる情報処理端末１０５０の受信機１０５２を目掛けて、ドキュメント・ワークセット＃１の使用許可を表す情報を発信する。この使用許可を示す情報は、ＩＣカードの認証情報であってもよいし、ドキュメント・アーカイブからドキュメント・ワークセットを取り出すためのリファレンス情報（ＵＲＬなど）であってもよい。あるいは、ドキュメント・ワークセットのシリアライズ・データ自体を発信するようにしてもよい。

【０１３８】

そして、情報交換先となるユーザは、情報処理端末１０５０のところまで移動し、そのＩＣカード読取装置１０５１に自分のＩＣカードをかざすことにより、個人認証が行なわれる。認証処理に成功すると、情報処理端末１０５０の使用が可能となり、そのユーザ・インターフェースを介してドキュメント・アーカイブ並びに情報交換されたドキュメント・ワークセット＃１にアクセスすることができる状態となる。あるいは、情報処理端末１０５０では、ドキュメント・ワークセット＃１のコピーであるドキュメント・ワークセット＃５を作成し、これを操作する。

【０１３９】

そして、情報交換の相手であるユーザは、情報処理端末１０５０のユーザ・インターフ

ェースを介してドキュメント・ワークセット＃５を参照することにより、その参照先であるドキュメント・アーカイブにアクセスを行ない、対象となるドキュメントを表示出力することができる。

【０１４０】

図１４には、上述したような情報アセットを交換するための動作手順を図解している。

【０１４１】

ユーザは、情報処理端末１０２０のＩＣカード読取装置１０２１に自分のＩＣカードをかざすことにより、個人認証が行なわれ、情報処理端末１０２０のユーザ・インターフェースを介して自分のドキュメント・アーカイブ並びにドキュメント・ワークセットにアクセスすることができる。

【０１４２】

そして、ユーザは、ドキュメント・アーカイブから必要なファイルを選択し、ドキュメント・ワークセットに配置することで、ドキュメント・ワークセット＃１を作成する。

【０１４３】

ここで、ドキュメント・ワークセット＃１のオーナーシップを持つユーザは、情報交換の相手となる情報処理端末１０５０の受信機１０５２を目掛けて、ドキュメント・ワークセット＃１の使用許可を表す情報を発信する。この使用許可を示す情報は、ＩＣカードの認証情報であってもよいし、ドキュメント・アーカイブからドキュメント・ワークセットを取り出すためのリファレンス情報（ＵＲＬなど）であってもよい。あるいは、ドキュメント・ワークセットのシリアライズ・データ自体を発信するようにしてもよい。

【０１４４】

その後、プレゼンテーションの聴講などによりドキュメント・ワークセットの交換を希望するユーザは、情報処理端末１０５０のところまで移動し、そのＩＣカード読取装置１０５１に自分のＩＣカードをかざすことにより、個人認証が行なわれる。

【０１４５】

そして、ユーザは、情報処理端末１０５０のユーザ・インターフェースを介してドキュメント・アーカイブ並びに情報交換されたドキュメント・ワークセット＃１にアクセスすることができる。ここでは、ドキュメント・ワークセット＃１のコピーであるドキュメント・ワークセット＃５を作成し、これを操作する。

【０１４６】

上述した例では、ドキュメント・ワークセット＃１のオーナーシップを持つユーザは、情報交換先となるユーザにその使用許可を表す認証情報を送信することにより情報交換先を指定するようにしている。これとは逆に、情報交換先が情報交換を要求し、これに応答して認証情報の送信を行なうように構成することも可能である。

【０１４７】

図１５には、この場合のユーザ間でドキュメント・ワークセットの情報交換を実現するための挙動を図解している。

【０１４８】

ドキュメント・ワークセット＃１のオーナーシップを持つユーザは情報処理端末１０２０を操作し、情報交換の相手となる他のユーザは情報処理端末１０６０を操作するものとする。ここで、情報処理端末１０６０はドキュメント・ワークセットを要求する信号を発信する発信機１０６３を備え、これに対し、情報処理端末１０２０はこの要求信号を受信する受信機１０２３を備えている。

【０１４９】

発信機１０６３並びに受信機１０２３間では、例えば電磁波を媒体とする無線通信により認証情報の交換を行なうものとする。但し、傍受などにより不正なユーザが認証情報を取得することを避けるためには、赤外線やその他の志向性の強い電磁波による通信を適用することが好ましい。

【０１５０】

まず、ユーザは、情報処理端末１０２０のＩＣカード読取装置１０２１に自分のＩＣカ

ードをかざすことにより、個人認証が行なわれる。そして、認証処理に成功すると、情報処理端末１０２０の使用が可能となり、そのユーザ・インターフェースを介して自分のドキュメント・アーカイブ並びにドキュメント・ワークセットにアクセスすることができる状態となる。

【０１５１】

そして、ユーザは、ドキュメント・アーカイブから必要なファイルを選択し、ドキュメント・ワークセットに配置することで、ドキュメント・ワークセット＃１を作成する。さらに、ユーザは、ドキュメント・ワークセットを操作することにより、ドキュメント・ワークセット上のファイルの配置を編集することができる。

【０１５２】

一方、情報交換先となるユーザは、情報処理端末１０５０のところまで移動し、そのＩＣカード読取装置１０５１に自分のＩＣカードをかざすことにより、個人認証が行なわれる。認証処理に成功すると、情報処理端末１０６０の使用が可能となる。

【０１５３】

そして、情報交換先となるユーザは、ドキュメント・ワークセットを要求する信号を発信機１０６３から発信させる。この要求信号は、情報処理端末１０２０側の受信機１０２３で受信される。

【０１５４】

この要求信号に応答して、情報処理端末１０６０からドキュメント・ワークセット＃１へのアクセスが許可される。そして、情報交換先となるユーザは、情報処理端末１０６０の使用が許可された状態であり、そのユーザ・インターフェースを介してドキュメント・アーカイブ並びに情報交換されたドキュメント・ワークセット＃１にアクセスすることができる。あるいは、情報処理端末１０６０では、ドキュメント・ワークセット＃１のコピーであるドキュメント・ワークセット＃６を作成し、これを操作する。

【０１５５】

そして、情報交換の相手であるユーザは、情報処理端末１０６０のユーザ・インターフェースを介してドキュメント・ワークセット＃６を参照することにより、その参照先であるドキュメント・アーカイブにアクセスを行ない、対象となるドキュメントを表示出力することができる。

【０１５６】

図１６には、上述したような情報アセットを交換するための動作手順を図解している。

【０１５７】

ユーザは、情報処理端末１０２０のＩＣカード読取装置１０２１に自分のＩＣカードをかざすことにより、個人認証が行なわれ、情報処理端末１０２０のユーザ・インターフェースを介して自分のドキュメント・アーカイブ並びにドキュメント・ワークセットにアクセスすることができる。

【０１５８】

そして、ユーザは、ドキュメント・アーカイブから必要なファイルを選択し、ドキュメント・ワークセットに配置することで、ドキュメント・ワークセット＃１を作成する。

【０１５９】

一方、情報交換先となるユーザは、情報処理端末１０５０のところまで移動し、そのＩＣカード読取装置１０５１に自分のＩＣカードをかざすことにより、個人認証が行なわれる。認証処理に成功すると、情報処理端末１０６０の使用が可能となる。そして、情報交換先となるユーザは、ドキュメント・ワークセットを要求する信号を発信機１０６３から発信させる。この要求信号は、情報処理端末１０２０側の受信機１０２３で受信される。

【０１６０】

この要求信号に応答して、情報処理端末１０６０からドキュメント・ワークセット＃１へのアクセスが許可される。そして、情報交換先となるユーザは、情報処理端末１０６０の使用が許可された状態であり、そのユーザ・インターフェースを介してドキュメント・アーカイブ並びに情報交換されたドキュメント・ワークセット＃１にアクセスすることが

できる。あるいは、情報処理端末１０６０では、ドキュメント・ワークセット＃１のコピーであるドキュメント・ワークセット＃６を作成し、これを操作する。

【０１６１】

上述したように、認証媒体としてＩＣカードを導入することにより、会議の参加者など個々のユーザの認証処理を安全且つ効率的に行なうことができる。ユーザがＩＣカードのみを携行する場合には、ユーザが自らＩＣカード内の記憶内容を書き換えることができない。これに対し、携帯電話機やＰＤＡなどの携帯機器にＩＣカード機能が内蔵されている場合には、携帯機器側の演算機能やユーザ・インターフェースを用いてＩＣカード内の記憶内容をユーザがその場で直接書き換えることができることから、上述したような認証を利用したドキュメント・ワークセットへのアクセス手続をより柔軟に運用することができる。以下では、このような場合の幾つかの実施形態について、図面を参照しながら説明する。但し、以下の各実施形態では、ユーザは図９に示したような挙動を行なうものとする。

【０１６２】

図１７には、携帯端末に内蔵されたＩＣカードを経由して認証処理を行なうことにより情報アセットの移動を行なう動作手順の一例を図解している。

【０１６３】

ユーザは、任意の情報処理端末上でドキュメント・ワークセットの作成又は編集を終了しているものとする。その後、情報処理端末１０３０のところ（例えば演壇）まで移動し、自分が所有するドキュメント・ワークセットを利用したいとする。

【０１６４】

ユーザは、ＩＣカード機能を内蔵した携帯電話機を保持している。この場合、ユーザ自身が所有するドキュメント・ワークセットの所在を表すＵＲＬなどのリファレンス情報を、ドキュメント・ワークセットへアクセスするために必要となるユーザ認証情報とともに、ＩＣカードへ書き込む。

【０１６５】

ＩＣカードへの書き込みは、携帯電話機のユーザ・インターフェースを用いて行なわれるので、操作性がよい。また、携帯電話機上でドキュメント・アーカイブのサイトへ訪れ、所望のドキュメント・ワークセットのＵＲＬを取得し、ＩＣカードへの書き込みを直接指示することができる。

【０１６６】

ここで、携帯電話機と、内蔵ＩＣカードとの接続は、携帯電話機がＩＣカード読み書き機能を備え、非接触ＩＣカード・インターフェース経由で行なわれてもよいし、ＩＣカード・インターフェース以外の有線インターフェースで接続されていてもよい。いずれの場合であっても、携帯電話機と内蔵ＩＣカードとの通信は、セキュアなＩＣカード・プロトコルに従って行なわれるので、データの読み書き動作は耐タンパ性がある（以下同様）。

【０１６７】

そして、ユーザは、ドキュメント・ワークセットを利用する情報処理端末１０３０のところまで移動し、そのＩＣカード読取装置１０３１に自分の携帯電話機をかざす。情報処理端末１０３０は、ＩＣカードからリファレンス情報とユーザ認証情報を読み出すことができる。

【０１６８】

次いで、情報処理端末１０３０は、取得したユーザ認証情報を用いてドキュメント・ワークセット・マネージャ１０１０と個人認証を行なう。そして、認証処理に成功すると、ＩＣカードから取得したファレンス情報を用いて、ドキュメント・アーカイブ１００４内の当該ユーザが所有する（若しくはユーザが指定した）ドキュメント・ワークセットへアクセスする。

【０１６９】

図１７に示したような実施形態の変形例として、携帯端末内のＩＣカードには、ユーザが所有するドキュメント・ワークセットへのアクセスを一時的に許可するための一時的若

しくは臨時の認証情報をＩＣカードに書き込むようにすることができる。また、アクセスを許可する対象として、ユーザが所有するドキュメント・ワークセット全体ではなく、その一部のみのリファレンス情報をＩＣカードに書き込むようにすることができる。図１８には、この場合の情報アセットの移動を行なう動作手順を図解している。

【０１７０】

ユーザは、任意の情報処理端末上でドキュメント・ワークセットの作成又は編集を終了しているものとする。その後、情報処理端末１０３０のところ（例えば演壇）まで移動し、自分が所有するドキュメント・ワークセットを利用したいとする。

【０１７１】

ユーザは、ＩＣカード機能を内蔵した携帯電話機を保持している。この携帯電話機上で、ユーザが所有するドキュメント・ワークセットへのアクセスを一時的に許可する一時的若しくは臨時の認証情報を生成する。そして、この一時的若しくは臨時の認証情報を、ドキュメント・ワークセットのうちアクセスを許可する部分についての所在を表すＵＲＬとともに、ＩＣカードへ書き込む。

【０１７２】

ＩＣカードへの書き込みは、携帯電話機のユーザ・インターフェースを用いて行なわれるので、操作性がよい。また、携帯電話機上でドキュメント・アーカイブのサイトへ訪れ、所望のドキュメント・ワークセットのＵＲＬを取得し、ＩＣカードへの書き込みを直接指示することができる。ここで、携帯電話機と内蔵ＩＣカードとの通信は、セキュアなＩＣカード・プロトコルに従って行なわれるので、データの読み書き動作は耐タンパ性がある（同上）。

【０１７３】

そして、ユーザは、ドキュメント・ワークセットを利用する情報処理端末１０３０のところまで移動し、そのＩＣカード読取装置１０３１に自分の携帯電話機をかざす。情報処理端末１０３０は、ＩＣカードからリファレンス情報とユーザ認証情報を読み出すことができる。

【０１７４】

情報処理端末側では、ＩＣカードからリファレンス情報と一時的なユーザ認証情報を読み出すと、ドキュメント・ワークセット・マネージャ１０１０に対し一時的若しくは臨時に個人認証を行なう。そして、認証処理に成功すると、取得したリファレンス情報を用いて、ドキュメント・アーカイブ１００４内の該当するドキュメント・ワークセットへアクセスすることができる。

【０１７５】

また、ドキュメント・ワークセットにアクセスするための一時的若しくは臨時のユーザ認証情報を発行する際に、認証情報を生成するための素情報として、例えば情報処理端末のＵＲＬや情報処理端末自身の証明書を利用することができる。図１９には、この場合の情報アセットの移動を行なう動作手順を図解している。

【０１７６】

ユーザのドキュメント・ワークセットを使用しようとする情報処理端末１０３０側では、自身の証明書を発行する。そして、ＩＣカード読取装置１０３１にユーザの携帯電話機がかざされると、内蔵されているＩＣカードに、自身のＵＲＬ並びに証明書を書き込む。

【０１７７】

携帯端末側では、情報処理端末１０３０の証明書を基に、情報処理端末用の認証情報を生成する。そして、情報処理端末に対しアクセスを許可するドキュメント・ワークセット又はその一部に対するリファレンス情報とともに、作成した認証情報をＩＣカードに書き込む。

【０１７８】

これに対し、情報処理端末１０３０は、ＩＣカードからリファレンス情報とユーザ認証情報を読み出すと、ドキュメント・ワークセット・マネージャ１０１０に対し、ＩＣカードから読み取ったユーザ認証情報を使い、個人認証を行なう。そして、個人認証に成功す

ると、今度はＩＣカードから読み取ったリファレンス情報を用いてドキュメント・アーカイブ１００４内の該当するドキュメント・ワークセット又はその一部へアクセスする。

【０１７９】

また、ユーザが情報処理端末に対し、自分のドキュメント・ワークセットに対するアクセスに必要な認証情報を渡す際に、ユーザの携帯端末と情報処理端末との間で認証手続きを行なうようにしてもよい。例えば、チャレンジ応答に基づく手続により、携帯端末と情報処理端末間で認証を行なうことができる。図２０には、この場合の情報アセットの移動を行なう動作手順を図解している。

【０１８０】

この場合、ユーザが携帯端末を情報処理端末１０３０のＩＣカード読取装置１０３１にかざすと、チャレンジ応答を経て、情報処理端末用の認証情報を生成する。そして、情報処理端末１０３０に対しアクセスを許可するドキュメント・ワークセット又はその一部に対するリファレンス情報を、生成した認証情報とともにＩＣカードに書き込む。

【０１８１】

そして、情報処理端末１０３０は、ＩＣカードからリファレンス情報とユーザ認証情報を読み出すと、ドキュメント・ワークセット・マネージャ１０１０に対し、ユーザ認証情報を使った個人認証を行なう。この個人認証に成功すると、情報処理端末１０３０は、同じくＩＣカードから読み取ったリファレンス情報を用いて、ドキュメント・アーカイブ１００４から該当するドキュメント・ワークセット又はその一部へアクセスする。

【０１８２】

また、図１９並びに図２０に示した動作手順において、携帯端末は、情報処理端末用の認証情報とドキュメント・ワークセット又はその一部に対するリファレンス情報をＩＣカードに書き込む前に、ドキュメント・アーカイブに対し、情報処理端末によるドキュメント・ワークセットに対するアクセス許可を要求するという手続を付加してもよい。図２１には、この場合の情報アセットの移動を行なう動作手順を図解している。

【０１８３】

ユーザのドキュメント・ワークセットを使用しようとする情報処理端末１０３０側では、自身の証明書を発行する。そして、ＩＣカード読取装置１０３１にユーザの携帯電話機がかざされると、内蔵されているＩＣカードに、自身のＵＲＬ並びに証明書を書き込む。

【０１８４】

携帯端末側では、情報処理端末１０３０の証明書を基に、ドキュメント・ワークセット・マネージャ１０１０に対し、情報処理端末１０３０用のアクセス許可要求を発行する。そして、ドキュメント・ワークセット・マネージャ１０１０は、情報処理端末１０３０に対する許可確認を返信する。

【０１８５】

次いで、携帯端末は、ドキュメント・ワークセット・マネージャ１０１０から取得した許可確認を基に、認証情報を生成する。そして、情報処理端末に対しアクセスを許可するドキュメント・ワークセット又はその一部に対するリファレンス情報とともに、作成した認証情報をＩＣカードに書き込む。

【０１８６】

これに対し、情報処理端末１０３０は、ＩＣカードからリファレンス情報とユーザ認証情報を読み出すと、ドキュメント・ワークセット・マネージャ１０３１に対し、ＩＣカードから読み取ったユーザ認証情報を使い、個人認証を行なう。そして、個人認証に成功すると、今度はＩＣカードから読み取ったリファレンス情報を用いてドキュメント・アーカイブ１００４内の該当するドキュメント・ワークセット又はその一部へアクセスする。

【０１８７】

また、携帯端末は、ドキュメント・アーカイブに対し、情報処理端末によるドキュメント・ワークセットに対するアクセス許可を事前に要求するようにしてもよい。図２１には、この場合の情報アセットの移動を行なう動作手順を図解している。

【０１８８】

携帯端末は、ドキュメント・ワークセット・マネージャ１０１０に対し、情報処理端末１０３０用のアクセス許可要求を発行する。そして、ドキュメント・ワークセット・マネージャ１０１０は、情報処理端末１０３０に対する許可確認を返信する。

【０１８９】

次いで、携帯端末は、ドキュメント・ワークセット・マネージャ１０１０から取得した許可確認を、情報処理端末に対しアクセスを許可するドキュメント・ワークセット又はその一部に対するリファレンス情報とともに、ＩＣカードに書き込む。

【０１９０】

そして、情報処理端末は、ＩＣカードから許可情報とリファレンス情報を読み出すと、許可情報とリファレンス情報を用いてドキュメント・ワークセット又はその中のアクセスが許可されている一部へアクセスすることができる。

【産業上の利用可能性】

【０１９１】

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。

【０１９２】

本明細書では、遠隔会議システムにおけるユーザの情報アセットの移動や共有などの操作を行なう場合を例にとって、本発明の実施形態について説明してきたが、本発明の要旨はこれに限定されるものではなく。各ユーザが情報アセットを所有し、ドキュメント・アーカイブにおいて格納されているという他の形態のシステムにおいても、個人認証をベースに情報アセットの移動や共有を行なうという局面においては、同様に本発明を適用し、作用効果を奏することができる。

【０１９３】

要するに、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、特許請求の範囲を参酌すべきである。

【図面の簡単な説明】

【０１９４】

【図１】図１は、本発明の一実施形態に係る遠隔会議システム１の構成を模式的に示した図である。

【図２】図２は、拠点システム１０における会議（テレビ会議など）を運営するための拠点サーバ１００の機能構成を模式的に示した図である。

【図３】図３は、拠点システム１０の実装例を示した図である。

【図４】図４は、本発明の一実施形態に係る会議室の概観を示した図である。

【図５】図５は、共有ワークスペース・サーバ３０の機能構成を模式的に示した図である。

【図６】図６は、ユーザがドキュメント・ワークセットを作成する仕組みを説明するための図である。

【図７】図７は、ドキュメント・アーカイブ１００４を操作するためのユーザ・インターフェース画面の構成例を示した図である。

【図８】図８は、ドキュメント・ワークセットを操作するためのユーザ・インターフェースの画面構成例を示した図である。

【図９】図９は、ユーザが情報アセットを移動する挙動を説明するための図である。

【図１０】図１０は、情報アセットを移動するための動作手順を示したシーケンス図である。

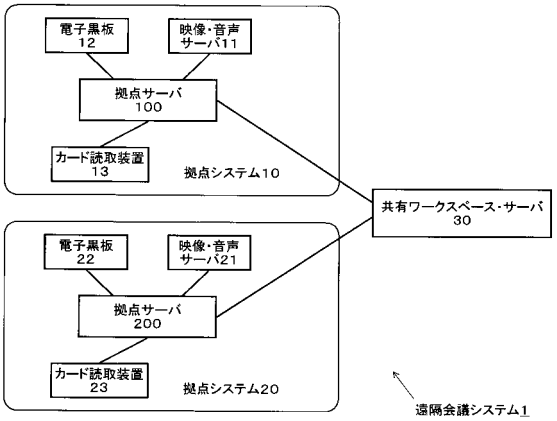
【図１１】図１１は、ユーザが情報アセットを交換する挙動を説明するための図である。

【図１２】図１２は、情報アセットを交換するための動作手順を示したシーケンス図である。

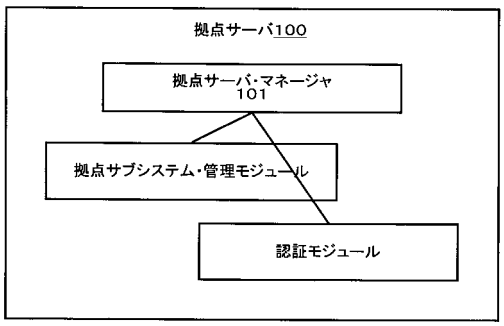
【図１３】図１３は、ユーザが情報アセットを交換する相手を指定して情報交換を行なう

挙動を説明するための図である。
【図１４】図１４は、ユーザが情報アセットを交換する相手を指定して情報交換を行なうための動作手順を示したシーケンス図である。
【図１５】図１５は、ユーザが情報アセットを交換する相手を指定して情報交換を行なう挙動を説明するための図である。
【図１６】図１６は、ユーザが情報アセットを交換する相手を指定して情報交換を行なうための動作手順を示したシーケンス図である。
【図１７】図１７は、携帯端末に内蔵されたＩＣカードを経由して認証処理を行なうことにより情報アセットの移動を行なう動作手順を説明するための図である。
【図１８】図１８は、携帯端末に内蔵されたＩＣカードを経由して認証処理を行なうことにより情報アセットの移動を行なう動作手順を説明するための図である。
【図１９】図１９は、携帯端末に内蔵されたＩＣカードを経由して認証処理を行なうことにより情報アセットの移動を行なう動作手順を説明するための図である。
【図２０】図２０は、携帯端末に内蔵されたＩＣカードを経由して認証処理を行なうことにより情報アセットの移動を行なう動作手順を説明するための図である。
【図２１】図２１は、携帯端末に内蔵されたＩＣカードを経由して認証処理を行なうことにより情報アセットの移動を行なう動作手順を説明するための図である。
【図２２】図２２は、携帯端末に内蔵されたＩＣカードを経由して認証処理を行なうことにより情報アセットの移動を行なう動作手順を説明するための図である。
【符号の説明】
【０１９５】
１…遠隔会議システム
１０，２０…拠点システム
１１，２１…映像・音声サーバ
１２，２２…電子黒板
１３，２３…カード読取装置
１００，２００…拠点サーバ
１０１…ワークスペース・マネージャ
１００１…Ｗｅｂインターフェース
１００２…ディレクトリ・サービス
１００３…ＩＣカード認証部
１００４…ドキュメント・アーカイブ
１００５…メタデータ・マネージャ
１００６…プレゼンテーション・コントローラ

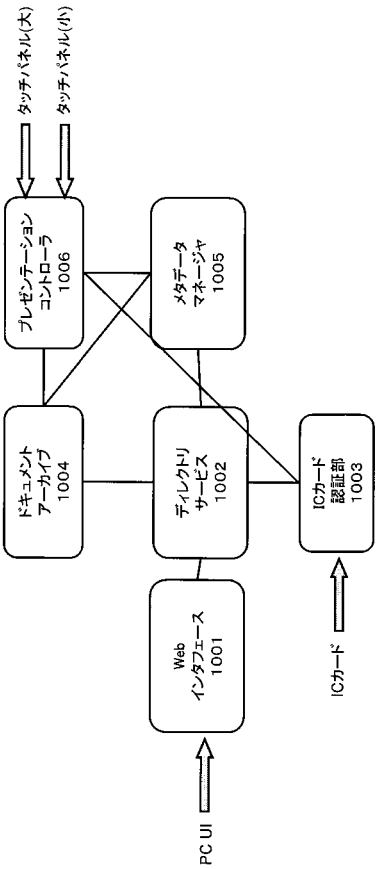
【図１】


電子黒板
12
映像・音声
サーバ11
拠点サーバ
100
カード読取装置
13
拠点システム10
共有ワークスペース・サーバ
30
電子黒板
22
映像・音声
サーバ21
拠点サーバ
200
カード読取装置
23
拠点システム20
遠隔会議システム1

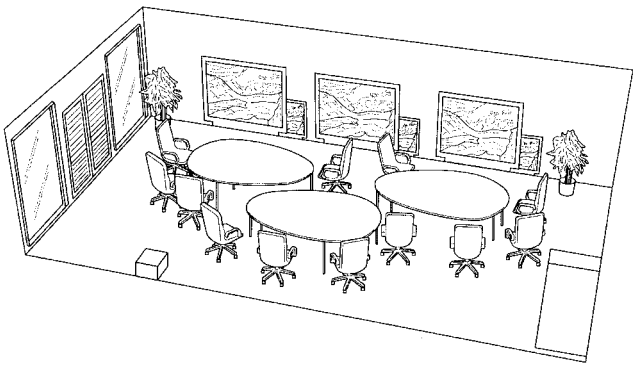
【図２】


拠点サーバ100
拠点サーバ・マネージャ
101
拠点サブシステム・管理モジュール
認証モジュール

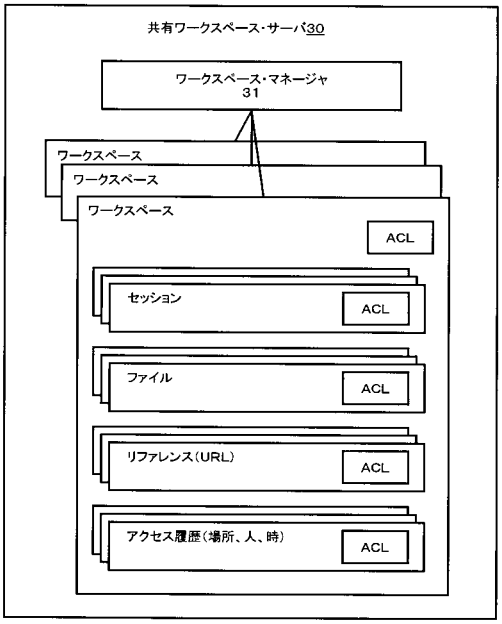
【図３】


タッチパネル(大)
タッチパネル(小)
プレゼンテーション
コントローラ
1006
メタデータ
マネージャ
1005
ドキュメント
アーカイブ
1004
ディレクトリ
サービス
1002
ICカード
認証部
1003
Web
インタフェース
1001
ICカード
PC UI

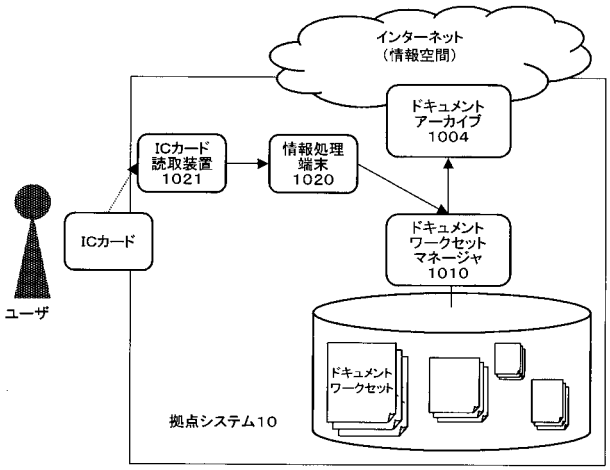
【図４】



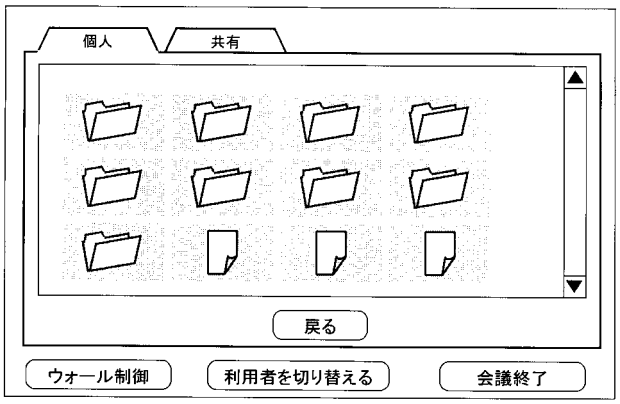
【図５】


共有ワークスペース・サーバ30
ワークスペース・マネージャ
31
ワークスペース
ワークスペース
ワークスペース
ACL
セッション
ACL
ファイル
ACL
リファレンス(URL)
ACL
アクセス履歴(場所、人、時)
ACL

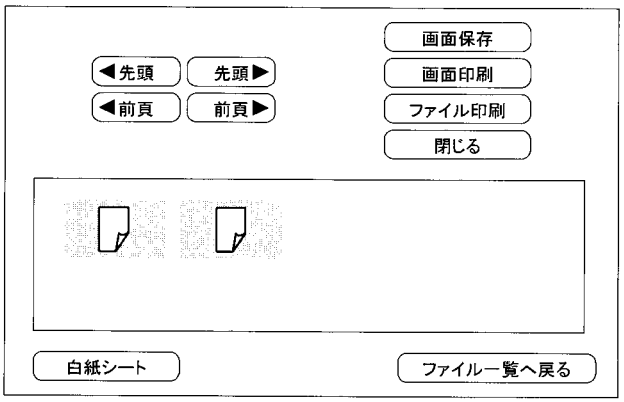
【図６】


インターネット
(情報空間)
ドキュメント
アーカイブ
1004
ICカード
読取装置
1021
情報処理
端末
1020
ICカード
ユーザ
ドキュメント
ワークセット
マネージャ
1010
ドキュメント
ワークセット
拠点システム10

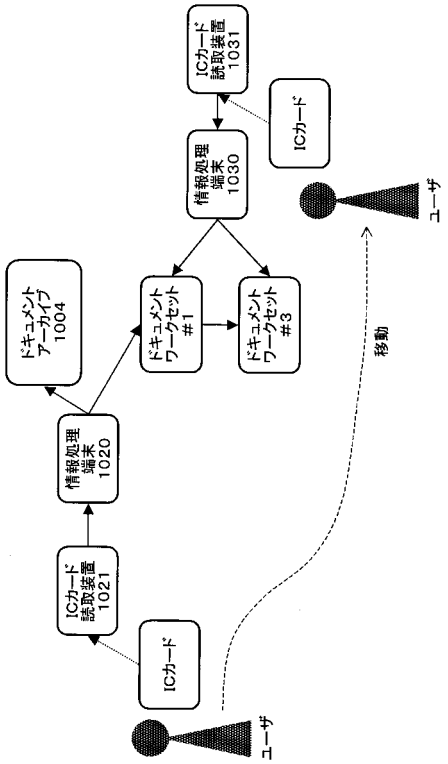
【図７】


個人
共有
戻る
ウォール制御
利用者を切り替える
会議終了

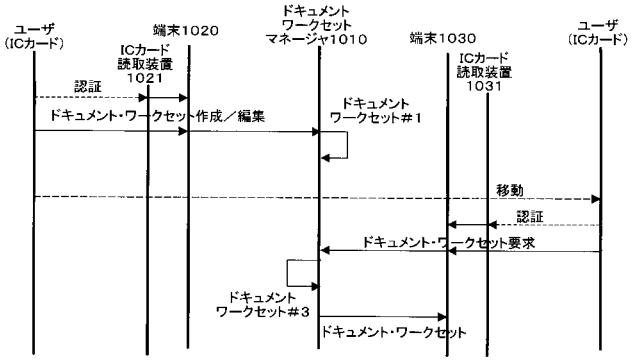
【図８】


◀先頭
先頭▶
◀前頁
前頁▶
画面保存
画面印刷
ファイル印刷
閉じる
白紙シート
ファイル一覧へ戻る

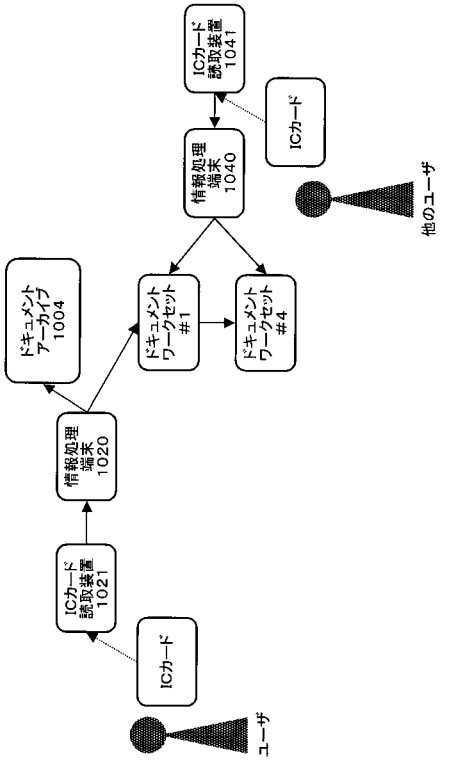
【図９】



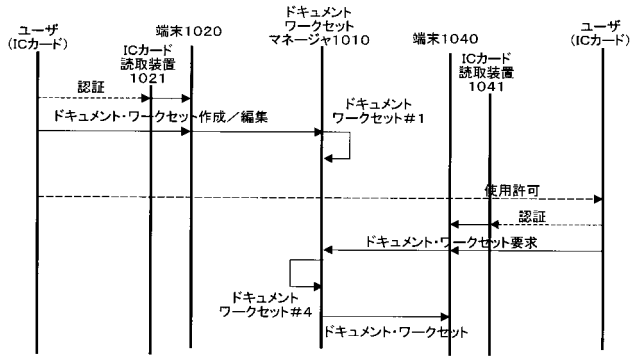
【図１０】



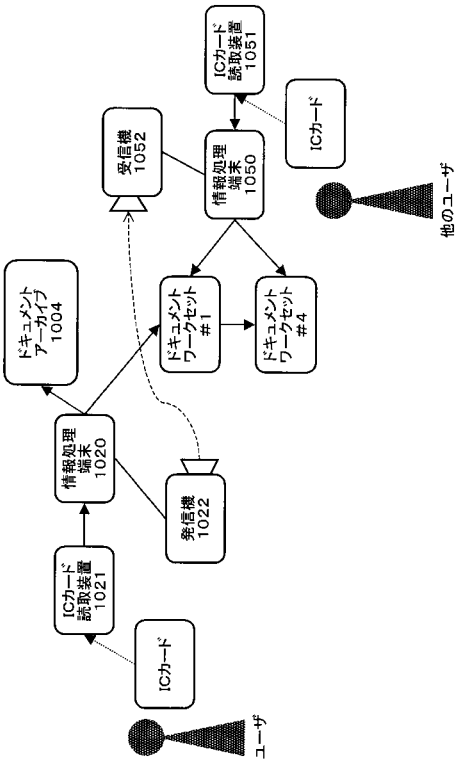
【図１１】



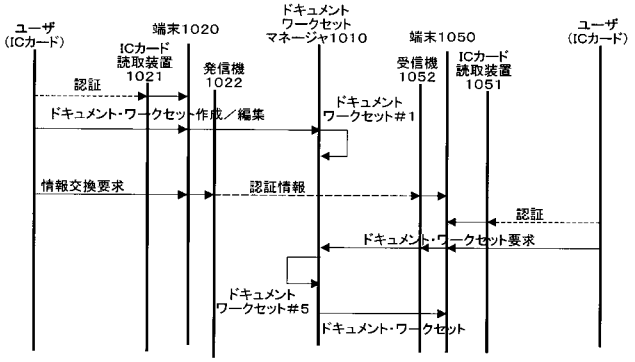
【図１２】



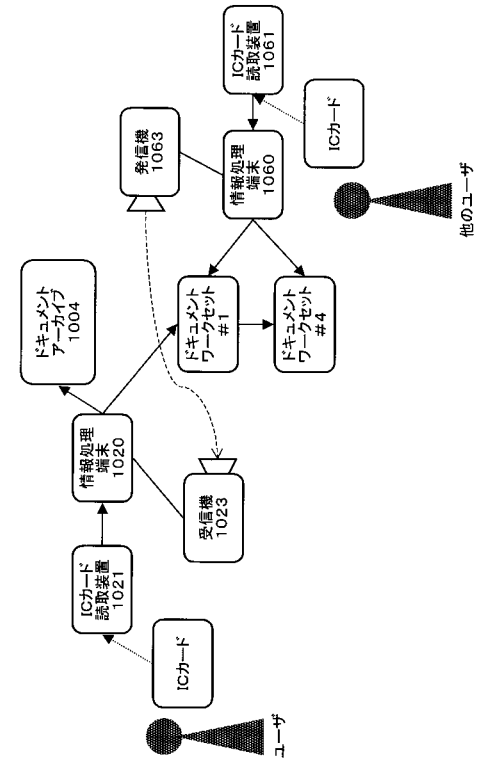
【図１３】



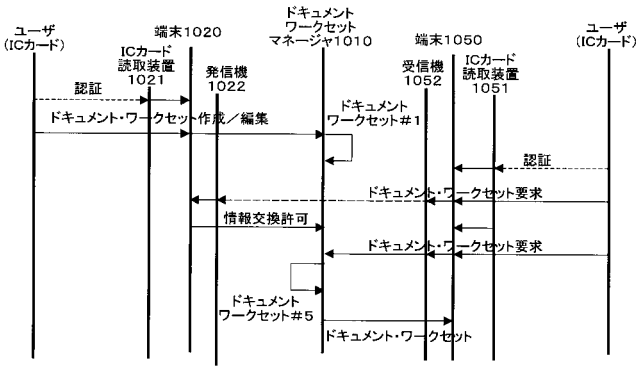
【図１４】



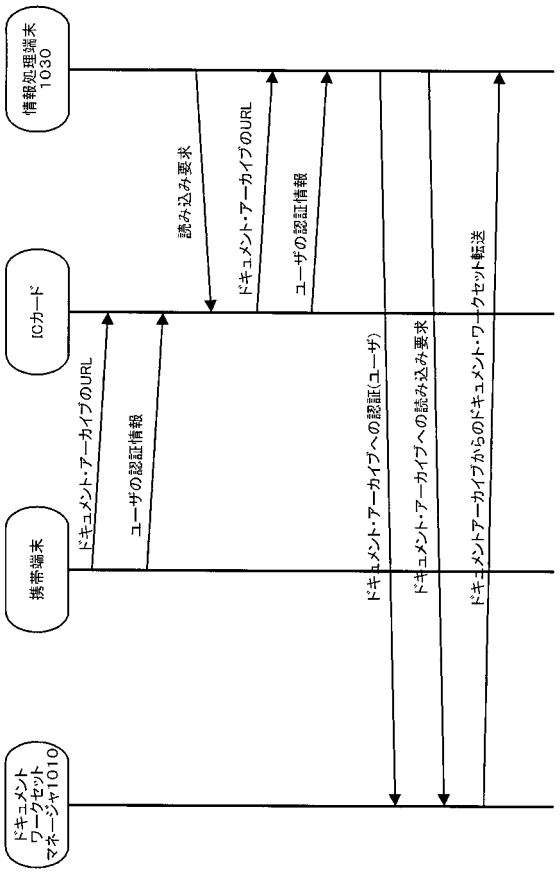
【図１５】



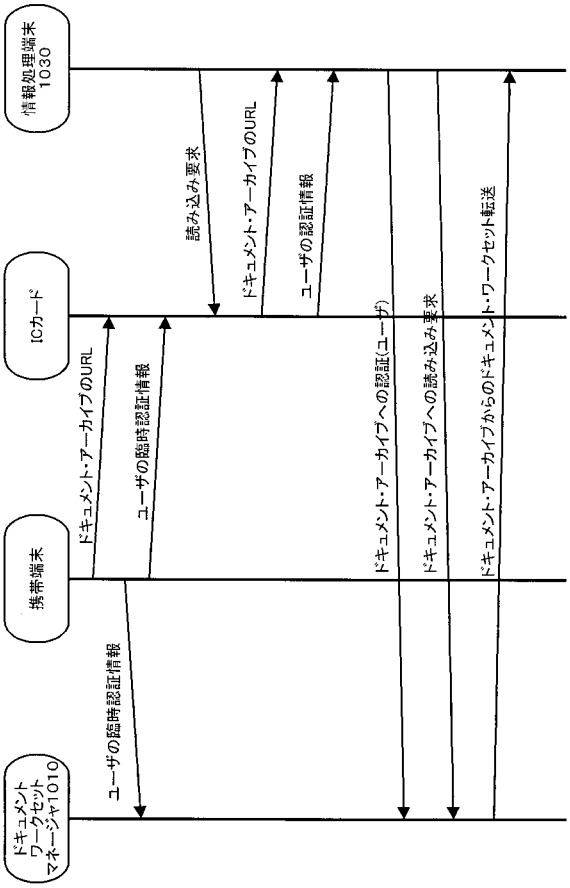
【図１６】



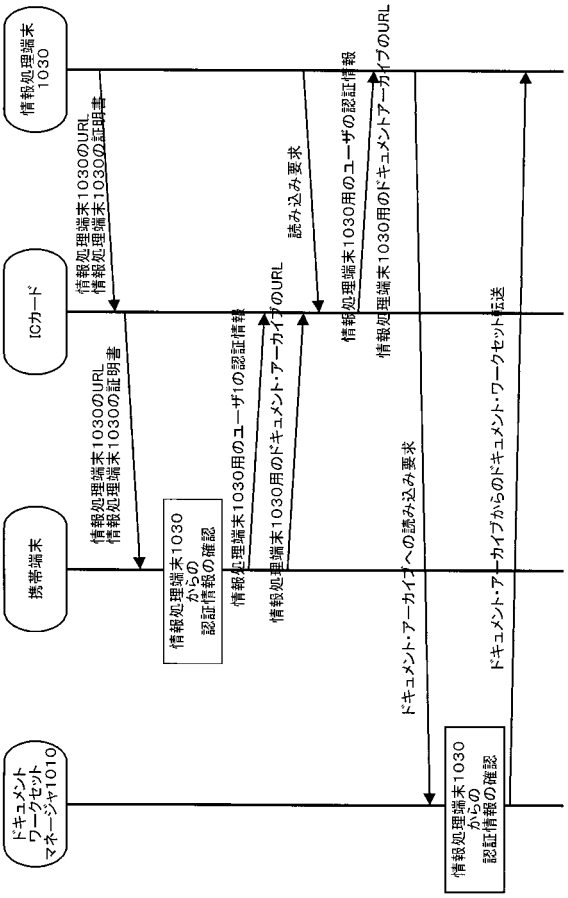
【図１７】



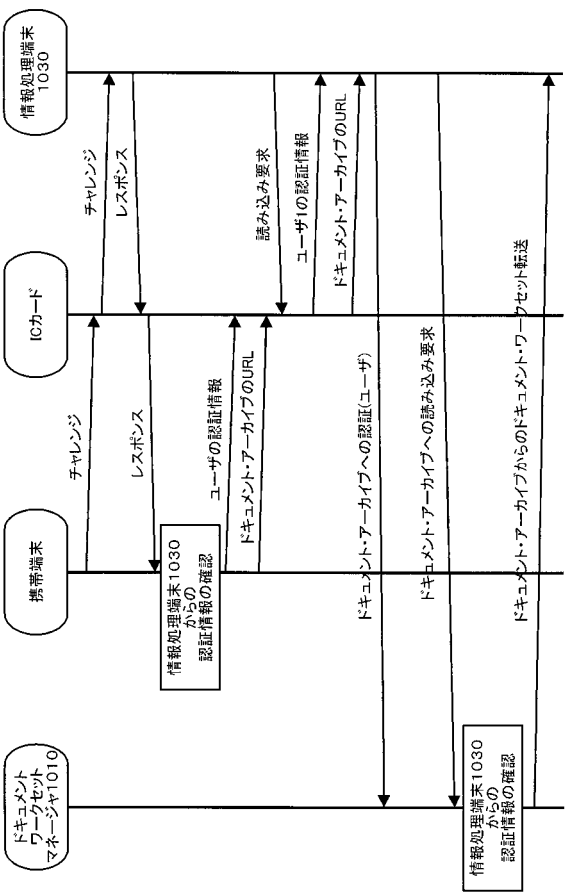
【図１８】



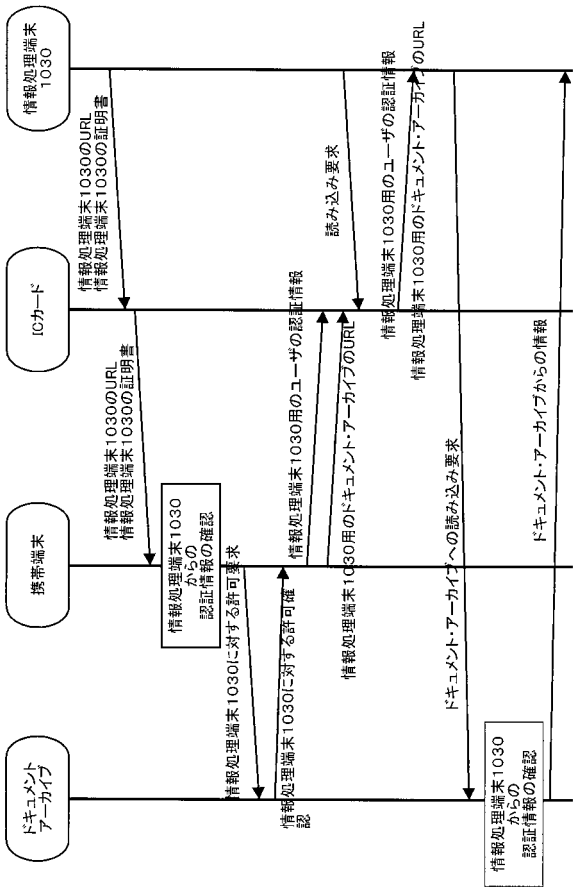
【図１９】



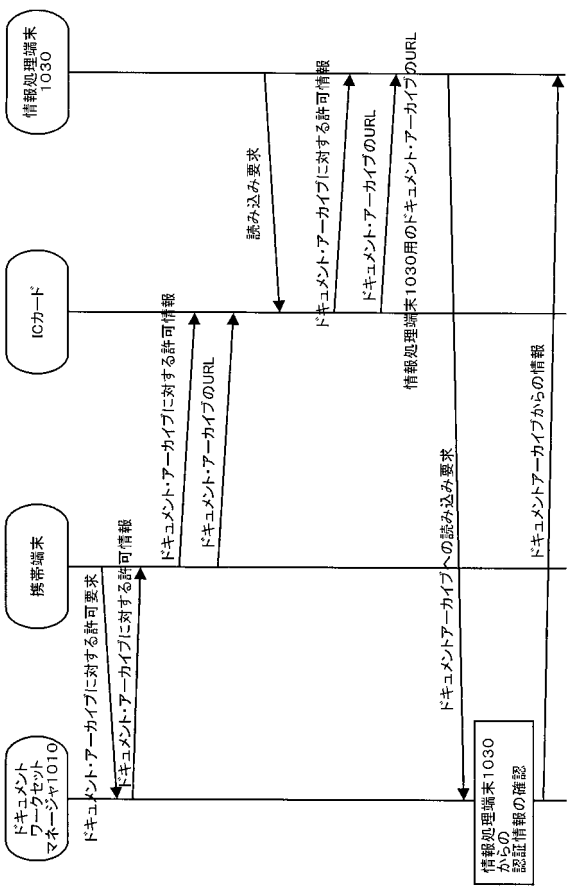
【図２０】



【図２１】


情報処理端末1030
ICカード
携帯端末
ドキュメントアーカイブ
情報処理端末1030のURL
情報処理端末1030の証明書
情報処理端末1030のURL
情報処理端末1030の証明書
情報処理端末1030からの認証情報の確認
情報処理端末1030に対する許可要求
情報処理端末1030に対する許可確認
情報処理端末1030用のユーザの認証情報
情報処理端末1030用のドキュメント・アーカイブのURL
読み込み要求
情報処理端末1030用のユーザの認証情報
情報処理端末1030用のドキュメント・アーカイブのURL
ドキュメント・アーカイブへの読み込み要求
ドキュメント・アーカイブからの情報
情報処理端末1030からの認証情報の確認

【図２２】


情報処理端末1030
ICカード
携帯端末
ドキュメントワークセットマネージャ1010
読み込み要求
ドキュメント・アーカイブに対する許可情報
ドキュメント・アーカイブのURL
ドキュメント・アーカイブに対する許可要求
ドキュメント・アーカイブに対する許可情報
ドキュメント・アーカイブのURL
情報処理端末1030用のドキュメント・アーカイブのURL
ドキュメントアーカイブへの読み込み要求
ドキュメントアーカイブからの情報
情報処理端末1030からの認証情報の確認

フロントページの続き

(51)Int.Cl.[7]	FI		テーマコード（参考）
Ｈ０４Ｌ 9/32	Ｇ０６Ｆ 12/14	５３０Ｄ	５Ｊ１０４
	Ｇ０６Ｆ 15/00	３９０	
	Ｇ０６Ｋ 17/00	Ｔ	
	Ｈ０４Ｌ 9/00	６７３Ｅ	

(72)発明者 阿部 仁
東京都港区赤坂二丁目１７番２２号 富士ゼロックス株式会社内
(72)発明者 上野 裕一
神奈川県足柄上郡中井町境４３０グリーンテクなかい 富士ゼロックス株式会社内
(72)発明者 水梨 豪
神奈川県足柄上郡中井町境４３０グリーンテクなかい 富士ゼロックス株式会社内
(72)発明者 坂本 彰司
神奈川県足柄上郡中井町境４３０グリーンテクなかい 富士ゼロックス株式会社内
(72)発明者 鷹合 基行
神奈川県川崎市高津区坂戸３丁目２番１号 ＫＳＰ Ｒ＆Ｄ ビジネスパークビル 富士ゼロックス株式会社内

Ｆターム(参考) 5B017 AA03 BA05 CA16
5B058 CA01 KA02 KA37
5B082 EA12
5B085 AA08 AE00 AE12
5B185 AA08 AE00 AE12
5J104 AA07 KA01 NA36 NA38 PA07