(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2005-135072
(P2005-135072A)
(43)公開日　平成17年5月26日(2005.5.26)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 17/21	G06F 17/21	570M	5B009
G06F 12/00	G06F 17/21	596Z	5B017
G06F 12/14	G06F 12/00	537A	5B082
	G06F 12/14	310K	
	G06F 12/14	310Z	

審査請求 未請求　請求項の数 7　ＯＬ　（全 12 頁）

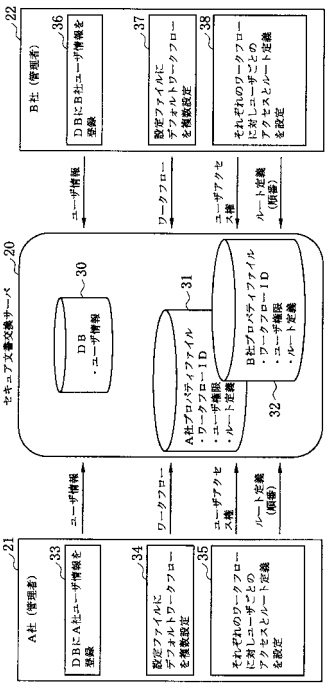
(21)出願番号　特願2003-368810 (P2003-368810)
(22)出願日　平成15年10月29日 (2003.10.29)

(71)出願人　396017453
リコーシステム開発株式会社
東京都中央区勝どき３－１２－１
(74)代理人　100077274
弁理士　磯村　雅俊
(74)代理人　100102587
弁理士　渡邊　昌幸
(72)発明者　木須　智章
東京都中央区勝どき３－１２－１フォアフロントタワー　リコーシステム開発株式会社内

Ｆターム(参考)　5B009 TB13　VC03
5B017 AA01　AA08　BA06　CA07　CA16
5B082 AA11　EA11

(54)【発明の名称】セキュア文書交換システム、文書承認方法、文書交換管理方法およびそのプログラム

(57)【要約】
【課題】秘密性のある文書に対して、紙ベースで行われている文書処理フローと同等に柔軟なフロー制御を行い、自動でのルート制御や署名検証などを自動化して、人手によるミスや手間を大幅に削減させる。
【解決手段】クライアント２１，２２間で取り交わされる文書の原本を保管するユーザ情報データベース３０と、各クライアント２１，２２ごとにワークフローＩＤ、アクセス権限、および保管された文書に対して承認や否決などの処理を行うノードの集合であるルートの定義を含む各情報を登録するプロパティファイル３１，３２と、ユーザ情報データベース３０と上記プロパティファイル３１，３２とを保持し、各クライアント２１，２２との間で文書の交換を行って、文書登録、該文書の参照、文書の内容変更時に自動的にワークフローの設定を実行し、文書のアクセス権限や改ざん検知などのセキュリティを確保するセキュア文書交換サーバ２０とを備える。
【選択図】図３



【特許請求の範囲】
【請求項１】
複数のクライアントをインターネットを介して接続するセキュア文書交換システムにおいて、
上記クライアント間で取り交わされる文書の原本を保管するユーザ情報データベースと、　各クライアントごとにワークフローＩＤ、アクセス権限、および保管された文書に対して承認や否決などの処理を行うノードの集合であるルートの定義を含む各情報を登録するプロパティファイルと、
上記ユーザ情報データベースと上記プロパティファイルとを保持し、各クライアントとの間で文書の交換を行って、文書登録、該文書の参照、文書の内容変更時に自動的にワークフローの設定を実行し、文書のアクセス権限や改ざん検知などのセキュリティを確保するセキュア文書交換サーバと
を有することを特徴とするセキュア文書交換システム。
【請求項２】
請求項１に記載のセキュア文書交換システムにおいて、
前記ワークフローは、電子ファイルであるコンテンツに対して承認や否決などの処理を行うノードの集合であるルートと、複数のコンテンツから構成されるドキュメントと、該コンテンツにアクセスできる権限とから構成されることを特徴とするセキュア文書交換システム。
【請求項３】
登録文書の承認行為を実施する文書承認方法であって、
コンテンツに対して承認や否決などの処理を行うノードの集合であるルートを形成する各ノード、複数のノードの集合およびルートの部分集合を形成する各ステージにおいて、
電子署名の付与を行う承認行為を実施し、上記コンテンツの正しさ、上記ルート経過の正しさを、サーバ側で検証することを特徴とする文書承認方法。
【請求項４】
各クライアントとの間でドキュメントの交換を行う文書交換管理方法であって、
上記ドキュメントを構成するコンテンツに対して承認や否決などの処理を行うノードの集合であるルートの各ノードおよび該ルートの部分集合を形成する各ステージにおいて、
ドキュメント毎にルートの随時設定あるいは変更を可能とし、かつ、
ドキュメント毎にアクセス権、承認行為の随時設定あるいは変更を可能とすることを特徴とした文書交換管理方法。
【請求項５】
請求項４に記載の文書交換管理方法において、
前記ドキュメントに対するルート設定では、特に企業間のルート設定について送信側企業と受信側企業の異なるルートを相手側企業に知られることなく連結、かつ挿入が可能であり、
該ドキュメントの属性情報および該ドキュメントを構成するコンテンツの内容によって、ドキュメント間のつながり、およびルートが自動設定されることを特徴とする文書交換管理方法。
【請求項６】
請求項４に記載の文書交換管理方法において、
前記ルートが設定されている場合でも、将来、該当ノードに回って来るであろうドキュメントについて、後方のノードの担当者端末は状況によって前方のいくつかのノード、ステージを飛ばして先取りすることを可能とし、
該ルートの各ノードにおいて、担当者端末のスケジュールと連動して設定されているルートが自動制御されることを特徴とする文書交換管理方法。
【請求項７】
複数の企業間におけるセキュア文書交換サーバの文書交換用プログラムであって、
該セキュア文書交換サーバのコンピュータに、１番目の企業の担当者端末によりドキュ

メントを作成し、該ドキュメントを構成する各コンテンツに対して電子署名を付与し、作成者の正当性と各コンテンツの改ざん検知の情報を施して、該ドキュメントを登録する手順、先に定義したワークフローの定義をプロパティファイルから取得し、文書内容、プロパティ情報から企業間のワークフロとして連結し、登録したドキュメントとリンクさせる手順、取得した該ドキュメントの電子署名検証から、該ドキュメントの改ざん検知、作成者の正しさの確認を行う手順、該ドキュメントを検証した後、原本保管データベースに電子原本として保管する手順、上記ワークフローに定義した通りに、該ドキュメントをインターネット上を流れて、２番目の企業に転送するとともに、該企業の担当者端末に通知メールを送る手順、該担当者端末から読み出しの指示があることで、ドキュメントを原本保管データベースから該担当者端末にダウンロードする手順、電子署名検証処理を行う手順、原本の更新または更新することなく該ドキュメントの電子原本を保管する手順を、それぞれ実施するための文書交換用プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、クライアント端末およびサーバを使用したインターネットあるいはイントラネット上ではコンテンツセキュリティ技術、電子文書長期保存技術あるいは電子文書交換技術を用いたセキュア文書交換システム、文書承認方法、文書交換管理方法およびそのプログラムに関する。
【背景技術】
【０００２】
従来、ワークフローの各段階で生成、変更された履歴情報を管理し、所定のクライアントに提供するワークフローシステム（例えば、特開２００２－２１５８５６号公報（特許文献１参照））、複数のシステム間で文書情報を連携させ、ドキュメントとその属性をデータベースに登録する文書情報連携システム（例えば、特開平１０－２６０９６２号公報（特許文献２参照））、あるいは、ワークフロー作業のタスクと作業対象物のドキュメントとの結び付きを管理操作するインターフェースを用いて、クライアント側でドキュメント管理操作を行えるワークフロー管理システム（例えば、特開平１１－７３４５９号公報（特許文献３参照））などがある。
【０００３】
しかしながら、これら従来のワークフロー管理システムでは、ノード毎にコンテンツが改竄されていないことが保証されていないワークフローシステムであった。また、これらは、主として１つの社内で作成されたドキュメントの管理であるため、文書交換されているコンテンツが原本として保管されていないため、最終的なコンテンツとしての信頼性が確保されていない文書管理システムであった。
【０００４】
【特許文献１】特開２００２－２１５８５６号公報
【特許文献２】特開平１０－２６０９６２号公報
【特許文献３】特開平１１－７３４５９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
従来の電子文書交換・業務フロー方法としての問題点は下記の通りである。
１）ノード毎にコンテンツが『改ざんされていない』ということを保証していないものが多かった。すなわち、前のノードの担当者を『改ざんしないものである』と無条件に信頼して、ルートが成立されていることが多い。これは、従来の電子文書交換システムが、社内だけで構築されるものが殆んどであるため、インターネット上に文書を送出したり、社外からアクセスされて読み込まれることもないため、上記のことが成り立っていた。
２）通常、各ノードにおいては、変更がかかる（つまり、変更が追記される）のが普通で

あるので、各ノード毎にそれ以前のノードの結果が保証されていないならば、誰がどのルートで承認したのか判明できず、事故調査などを行う際には不都合が出ていた。
３）文書交換されているコンテンツが原本として保管されていないため、最終的なコンテンツとしての信頼性が確保されていないものが多かった。
【０００６】
４）予めルートが定義されており、ドキュメントはそのルートに従って交換されているが、担当者の出欠、期限などの状況に応じてルートや処理を変更する必要が生じたときなど、対処できなかった。また、ルートの変更ができるものもあるが、予め想定された状況に対してしか対応できないなどの不都合があった。
５）予めアクセス権限が定義されており、ドキュメントはそのアクセス権限に従って管理されているが、担当者の出欠、期限などの状況に応じてアクセスや処理を変更する必要が生じたときなど対処できなかった。アクセス権限の変更ができるものもあるが、予め想定された状況に対してしか対応できないなどの不都合があった。
【０００７】
（目的）
本発明の目的は、これら従来の問題を解消し、秘密性のある文書に対して、紙ベースで行われている文書処理フローと同等に柔軟なフロー制御が可能であり、自動でのルート制御や署名検証などを自動化することで、人手によるミスや手間を大幅に削減させることができ、ネットワークを使用して企業間で文書を電子化し、交換する際に、コンテンツの改ざん、盗聴、原本性の確保に対する蔽害をなくすことが可能なセキュア文書交換システム、文書承認方法、文書交換管理方法を提供することである。
【課題を解決するための手段】
【０００８】
本発明のセキュア文書交換システムは、複数のクライアントをインターネットを介して接続するセキュア文書交換システムにおいて、上記クライアント間で取り交わされる文書の原本を保管するユーザ情報データベースと、各クライアントごとにワークフローＩＤ、アクセス権限、および保管された文書に対して承認や否決などの処理を行うノードの集合であるルートの定義を含む各情報を登録するプロパティファイルと、上記ユーザ情報データベースと上記プロパティファイルとを保持し、各クライアントとの間で文書の交換を行って、文書登録、該文書の参照、文書の内容変更時に自動的にワークフローの設定を実行し、文書のアクセス権限や改ざん検知などのセキュリティを確保するセキュア文書交換サーバとを有することを特徴としている。
また、前記ワークフローは、電子ファイルであるコンテンツに対して承認や否決などの処理を行うノードの集合であるルートと、複数のコンテンツから構成されるドキュメントと、該コンテンツにアクセスできる権限とから構成されることも特徴としている。
【０００９】
本発明の文書承認方法は、コンテンツに対して承認や否決などの処理を行うノードの集合であるルートを形成する各ノード、複数のノードの集合およびルートの部分集合を形成する各ステージにおいて、電子署名の付与を行う承認行為を実施し、上記コンテンツの正しさ、上記ルート経過の正しさを、サーバ側で検証することを特徴としている。
【００１０】
本発明の文書交換管理方法は、上記ドキュメントを構成するコンテンツに対して承認や否決などの処理を行うノードの集合であるルートの各ノードおよび該ルートの部分集合を形成する各ステージにおいて、ドキュメント毎にルートの随時設定あるいは変更を可能とし、かつ、ドキュメント毎にアクセス権、承認行為の随時設定あるいは変更を可能とすることを特徴としている。
【００１１】
また、前記ドキュメントに対するルート設定では、特に企業間のルート設定について送信側企業と受信側企業の異なるルートを相手側企業に知られることなく連結、かつ挿入が可能であり、該ドキュメントの属性情報および該ドキュメントを構成するコンテンツの内

容によって、ドキュメント間のつながり、およびルートが自動設定されることも特徴としている。

また、前記ルートが設定されている場合でも、将来、該当ノードに回って来るであろうドキュメントについて、後方のノードの担当者端末は状況によって前方のいくつかのノード、ステージを飛ばして先取りすることを可能とし、該ルートの各ノードにおいて、担当者端末のスケジュールと連動して設定されているルートが自動制御されることも特徴としている。

【発明の効果】

【００１２】

本発明によれば、秘密性のある文書について、紙ベースで行われている文書処理フローと同等に柔軟かつ電子化による制御が可能であり、特に企業間で文書を電子化して、それを交換する際の弊害（コンテンツの改ざん、盗聴、原本の確保の欠除）をなくし、自動化することで、ミスや手間を大幅に減少させることが可能となる。

【発明を実施するための最良の形態】

【００１３】

以下、本発明の実施例を、図面により詳細に説明する。

（システム構成）

図１は、本発明の一実施例に係るセキュア文書交換システムの構成を示す図である。

ここでは、Ａ社とＢ社の２つが連携する場合の説明を行うが、Ａ，Ｂ，Ｃの３社であっても、４社以上の場合であっても適用が可能である。

図１に示すように、本実施例のセキュア文書交換システムは、Ａ社側クライアント端末１４，１５が接続されているネットワーク（例えば、インターネット）１１と、Ｂ社側クライアント端末１６，１７が接続されているネットワーク１３と、セキュア文書交換サーバ１９および原本保管サーバ１８が接続されているネットワーク１２と、全体のネットワーク１１，１２，１３と接続しているネットワーク１０とで構成されている。

【００１４】

（文書交換の流れ）

図２は、本発明の一実例に係る文書交換の流れを表す図である。

Ａ社側クライアント端末１４とセキュア文書交換サーバ１９との交換を(1)、Ａ社側クライアント端末１５とセキュア文書交換サーバ１９との交換を(2)、Ｂ社側クライアント端末１６とセキュア文書交換システム１９との交換を(3)、Ｂ社側クライアント端末１７とセキュア文書交換サーバ１９との交換を(4)とすると、そのルートは、セキュア文書交換サーバ１９にルート定義を行うことで、様々に設定することができる。例えば、(1)→(2)→(3)→(4)、(1)→(3)→(2)→(4)などのセキュア文書交換サーバ１９を使用する業務により、どのようなルートの設定も可能となる。

【００１５】

(セキュア文書交換システムのマスターデータ登録手順)

図３は、本発明の一実施例に係るＡ社、Ｂ社のマスターデータ登録手順を表す図である。 図３においては、セキュア文書交換サーバ２０に対して、非同期にＡ社の管理端末２１とＢ社の管理端末２２から管理者が以下の順番で、セキュア文書交換サーバ２０にマスターデータ（ワークフロー、およびそのワークフローに設定されるユーザのアクセス権限、ルート定義）を設定する手順が示される。セキュア文書交換サーバ２０には、ユーザ情報ＤＢ（データベース）３０、ワークフローＩＤ、ユーザ権限、ルート定義などを登録したＡ社プロパティファイル３１およびＢ社プロパティファイル３２が配置される。

ステップ３３の処理によりＡ社の管理端末からセキュア文書交換サーバ２０のユーザ情報ＤＢ３０に対して、セキュア文書交換サーバ２０を使用するユーザの基本情報が登録される。その時、Ｂ社などの他社のユーザ情報は、参照することはできない。次に、ステップ３４の処理により、Ａ社のプロパティファイル３１にワークフローを複数設定することができる。この時もまた、Ａ社の管理端末からは、Ｂ社のプロパティファイル３２にアクセスすることは不可能である。次に、ステップ３５の処理により、ワークフローに設定さ

れるユーザのアクセス権限、ルート定義（順番）を設定する。
全く同じようにして、Ｂ社の管理端末２２により、ステップ３６～３８の処理を行うことによって、様々なルートを定義するマスターデータ（ユーザ情報、ワークフロー、ユーザアクセス権、ルート定義）を登録することができる。
【００１６】
（セキュア文書交換システムの文書交換手順）
図４－Ａ，Ｂ，Ｃは、Ａ社とＢ社間の企業間におけるセキュア文書交換サーバの文書交換手順を表す図である。
なお、ワークフローとは、ドキュメントのルート定義（移動の順序を定義したもの）であり、ドキュメントとは、ワークフローに１対１に対応している物（オブジェクト）であって、実ファイルに紐付けられているものである。コンテンツとは、実ファイルのことで、コピーファイルと区別される。また、ノードとは、この場合Ａ社，Ｂ社のことである。
図４－Ａにおいて、（１）Ａ社担当者端末４１で、ドキュメント（コンテンツ群とプロパティ情報）を作成する（ステップ１１０）。
（２）Ａ社任当者端末は、コンテンツに対して電子署名を付与し、作成者の正当性とコンテンツの改ざん検知の情報を施す（ステップ１１１）。
（３）次に、そのドキュメントを、セキュア文書交換サーバ４０に登録する。ドキュメントがセキュア文書交換サーバ４０に登録された時、先に定義したワークフローの定義をプロパティファイル４３から取得し、文書内容、プロパティ情報から自動的にＡ，Ｂ社間の企業間のワークフローとして連結し、登録したドキュメントとリンクさせる（ステップ１１２）。
【００１７】
（４）この時、アクセス権、ルート定義のカスタマイズが行われるので、ユーザは設定されたルート、ユーザアクセス権限を変更することができる（ステップ１１３）。
（５）ドキュメントの電子署名検証から、ドキュメントの改ざん検知、作成者の正しさの確認が行われる（ステップ１１４）。
（６）ドキュメントを検証した後、外部の原本保管サーバ４４に電子原本として保管する（ステップ１１５）。
（７）以後、ワークフローに定義した通り、ドキュメントがネット（インターネット、イントラネット）上を流れて、ワークフローの次のノードに転送される。
しかし、ドキュメントが次のノードの担当者端末に送られる訳ではない。すなわち、ドキュメントは、常に文書交換サーバ４０に保管・管理されているので、以下のような処理となる。
まず、ドキュメントが来ているという通知メールが該当ノード（Ｂ社端末）に届く（ステップ１１６）。
【００１８】
図４－Ｂ、図４－Ｃにおいて、ノードの担当者端末から読み出しの指示が送出されることにより、初めてドキュメントがセキュア文書交換サーバ４０から該当端末にダウンロード可能となる（ステップ１１７，１１８，１１９）。
（８）Ｂ社担当者端末４２の該当ノードで、承認または承認拒否（電子署名の付与）の操作（ステップ１２０，１２１）をすれば、ドキュメントはセキュア文書交換サーバ４０に戻る。以下、Ａ社が行ったステップ１１３～１１６と同様の処理が繰り返される（ステップ１２２～１２５）。
【００１９】
（文書承認方法）
図５は、本発明の一実施例に係る文書署名方法の動作フローチャートである。
ここでは、本システムを使用して電子署名を施す方法として、端末側のファイルフォーマットにより署名方式を選択できるものとする。例えば、以下のような方法で、ファイルに署名を施すことが可能である。
（１）ドキュメントを開く（ステップ５０）。

（２）電子署名イメージ画像（サインなど、それに類するもの、電子押印したことを示す記号）を表示するエリア（領域）をドラッグして指定する（ステップ５１）。
（３）登録してある鍵（自己の秘密鍵）の名前を選択する（ステップ５２）。
（４）署名理由や署名者名や署名場所などの署名条件を入力する（ステップ５３）。
（５）上記（２）で指定したエリア内に表示する署名イメージデータを選択する（ステップ５４）。
（６）署名ＯＫを押下すると、上記（１）のドキュメントのハッシュ値（メッセージダイジェスト）が計算され、担当者の秘密鍵で暗号化され、電子署名の生成が行われる（ステップ５５，５６）。
（７）上記（１）で選択されたドキュメントのファイルフォーマット固有の方式で、上記（６）で作成して署名データを付与する（ステップ５７）。
（８）画面には、対応する電子署名イメージ画像が、上記（２）で指定したエリアに表示される（ステップ５８）。
（９）ファイルを保存する（ステップ５９）。

【００２０】

（端末側の署名検証方法）

図６は、本発明の一実施例に係る文書承認検証方法（端末署名検証）の動作フローチャートである。

ここでは、電子署名検証する方法として、端末側のファイルフォーマットによって署名方式を選択可能とする。例えば、以下のような方法で、ファイルの署名検証が可能である。（１）ドキュメントを開く（ステップ６０）。
（２）電子署名イメージ画像（サインなど、それに類するもの、電子押印したことを示す記号）が表示されているエリア（領域）をクリックして、メニューから署名検証を選択する（ステップ６１）。
（３）上記（１）で選択されたファイルフォーマット固有の方式で署名データをファイルから取得する（ステップ６２）。
（４）取得した署名データから証明書（相手の公開鍵証明書）の有効性を失効リストや信頼チェーンの検証によって確認する（ステップ６３）。
（５）有効性の確認できた証明書で、電子署名を復号化する（ハッシュ値の抽出）（ステップ６４）。
（６）上記（１）でオープンしてファイルのハッシュ値（メッセージダイジェスト）を再度計算する（ステップ６５）。
（７）上記（５）で取得したハッシュ値と上記（６）で取得したハッシュ値とを比較する（ステップ６６）。
（８）上記（４）の証明書の有効性確認結果と、上記（７）の比較結果と、署名、証明書の情報を、プロパティ画面より表示する（ステップ６７）。

【００２１】

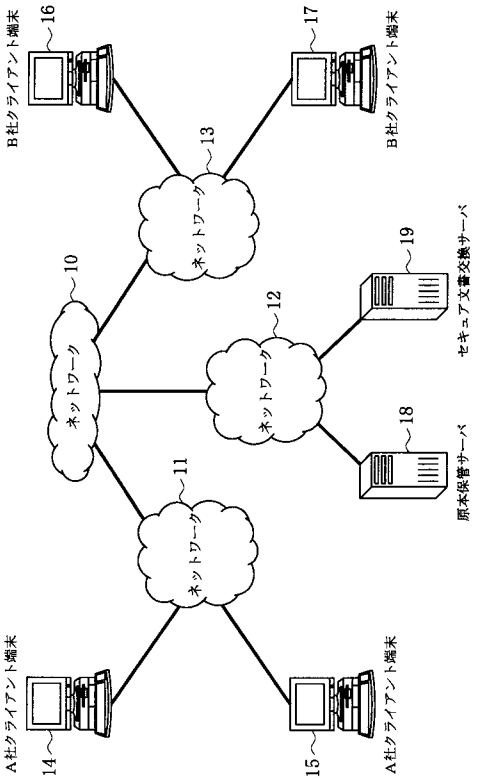
（サーバ側の署名検証方法）

図７は、本発明の一実施例に係るサーバ側の署名検証方法の動作フローチャートである。　ここでは、システムを使って電子署名検証する方法として、サーバ側の署名検証方式を端末側の署名方式と合わせることにより、様々な署名フォーマットの検証に対応することができる。例えば、以下のような方法で、ファイルの署名検証が可能である。
（１）文書プロパティよりファイルフォーマットを自動判別する（ステップ７０）。
（２）上記（１）で選択されたファイルフォーマット固有の方式で署名データをファイルから取得する（ステップ７１）。
（３）取得した署名データから証明書（相手の公開鍵証明書）の有効性を失効リストや信頼チェーンの検証によって確認する（ステップ７２）。
（４）有効性の確認できた証明書で、電子署名を復号化する（ハッシュ値の抽出）（ステップ７３）。
（５）ファイルのハッシュ値（メッセージダイジェスト）を再計算する（ステップ７４）

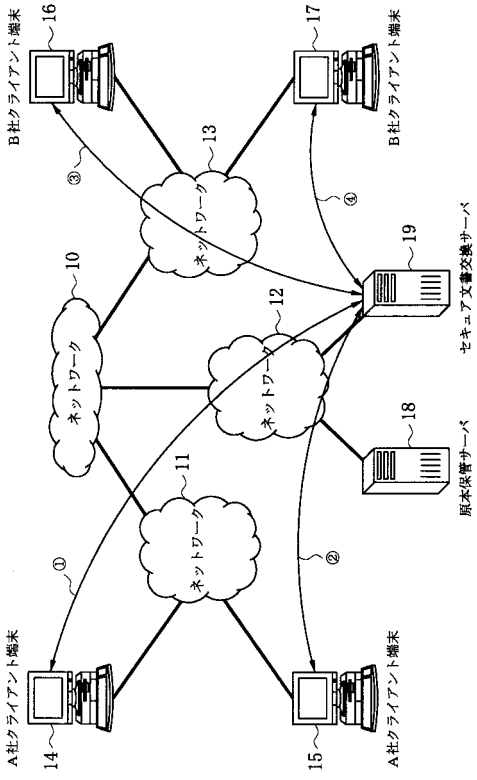
。（６）上記（４）で取得したハッシュ値と上記（５）で取得したハッシュ値とを比較する（ステップ７５）。
（７）上記（３）の証明書の有効性確認結果と、上記（６）の比較結果から、登録されたファイルの正当性を判断する（ステップ７６）。
【００２２】
（文書交換管理方法）
（ワークフロー自動設定方法）
図８は、本発明の一実施例に係るワークフロー自動設定方法のシーケンスチャートである。
電子文書をセキュア文書交換サーバに登録する時に行われる自動ワークフロー設定機能は、以下のような方法がある。
（１）図８において、文書のプロパティ情報８１（文書種別、作成者など）を参照し、予め決められた条件によりマスターテーブル８０からワークフローを自動選択する。
（２）図８の文書の内容８２を参照し（例えば、金額など）、予め決められた条件によりマスターテーブル８０からワークフローを自動選択する。例えば、ドキュメントの種類が契約書であり、ドキュメントの内容８２の金額が１０万円以上の場合には、部長決済のルートを自動設定し、契約書で、金額が１００万円以上の場合には、取締役決済のルートを自動設定する、などが可能である。
（３）図８において、文書のプロパティ情報８１（文書種別）を参照し、予め決められた条件によりマスターテーブル８０から、次に回覧される文書種別を自動選択し、担当者に表示させる。
【００２３】
（ワークフロー制御方式）
図９は、本発明の一実施例に係るワークフロー制御方法の説明図である。
電子文書を交換する際のワークフローの情報には、次のものがあり、それにより以下のような制御方法がある。
☆ワークフロー承認期限（全体期限と各ノード期限）
☆各ノード担当者のアクセス権（先取り権限）
☆各ノードのルート定義（例えば、ルートが４人に回覧、６人に回覧など）
（１）図９において、文書登録日９１と次の担当者のスケジュールデータ９０を参照し、ワークフローが期限通りに駆動するように、欠席承認者の飛越しなどのルートの制御（例えば、フロー(1)）を行う。例えば、図９に示すように、４人に回覧する場合に、１２月５日に文書登録が行われ、その日に回覧したが、次の承認者のスケジュールデータが１２月３日から１２月１２日まで欠席の場合には、３番目の承認者は、全体期限が７日であるならば、スケジュールを参照し、先取りすることができる。
（２）図９において、期限の関係上、ワークフローの上位者が、自己が承認者に設定されているワークフローを承認順番より事前に参照でき（例えば、フロー(2))、文書を下位の承認者より早く承認することを可能とする。例えば、図９に示すように、４人の最後の上位者が、社外秘の文書を２番目と３番目の承認者よりも先に参照することができる。
【００２４】
なお、図４－Ａ，Ｂ，Ｃのセキュア文書交換システムの文書交換手順をプログラムコード化し、ＣＤ－ＲＯＭなどの記録媒体に格納しておけば、本発明のプログラムの販売や貸付の際に便利であり、また、記録媒体をセキュア文書交換サーバに装着して、プログラムをサーバコンピュータにインストールして実行させることにより、本発明を容易に実現させることが可能である。
【産業上の利用可能性】
【００２５】
これまで述べてきた各実施例を含む本発明は、例えば、企業間電子契約書締結業務、社内電子稟議書交換業務あるいは企業間電子技術文書交換業務に利用が可能である。
【図面の簡単な説明】

【００２６】
【図１】本発明の一実施例に係るセキュア文書交換システムの構成図である。
【図２】図１におけるセキュア文書交換システムの文書交換の流れを示す図である。
【図３】本発明の一実施例に係るセキュア文書交換システムのマスターデータ登録手順を示すシーケンスチャートである。
【図４－Ａ】本発明の一実施例に係るセキュア文書交換システムの文書交換手順（その１）を示すフローチャートである。
【図４－Ｂ】本発明の一実施例に係るセキュア文書交換システムの文書交換手順（その２）を示すフローチャートである。
【図４－Ｃ】本発明の一実施例に係るセキュア文書交換システムの文書交換手順（その２）を示すフローチャートである。
【図５】本発明の一実施例に係るセキュア文書交換システムの署名方法（端末署名）の動作フローチャートである。
【図６】本発明の一実施例に係るセキュア文書交換システムの文書承認検証方法（端末署名検証）の動作フローチャートである。
【図７】本発明の一実施例に係るセキュア文書交換システムの文書承認検証方法（サーバ署名検証）の動作フローチャートである。
【図８】本発明の一実施例に係るワークフロー自動設定方法のシーケンスチャートである。
【図９】本発明の一実施例に係るワークフロー制御方法のシーケンスチャートである。
【符号の説明】
【００２７】
１０，１１，１２，１３…ネットワーク、１４，１５…Ａ社クライアント端末、
１６，１７…Ｂ社クライアント端末、１８…原本保管サーバ、
１９…セキュア文書交換サーバ、２０，３０，４０…セキュア文書交換サーバ、
２１，４１…Ａ社クライアント端末、２２，４２…Ｂ社クライアント端末、
３０…ユーザ情報ＤＢ、３１…Ａ社プロパティファイル、
３２…Ｂ社プロパティファイル、４３…プロパティファイル群、４４…原本保管サーバ、　８２…ドキュメント（コンテンツファイル）、８１…ドキュメントプロパティ情報、
８３…プロパティファイル群、８０…マスターテーブル、９１…文書登録、
９０…スケジュールデータ、９２…先取り権限あり。

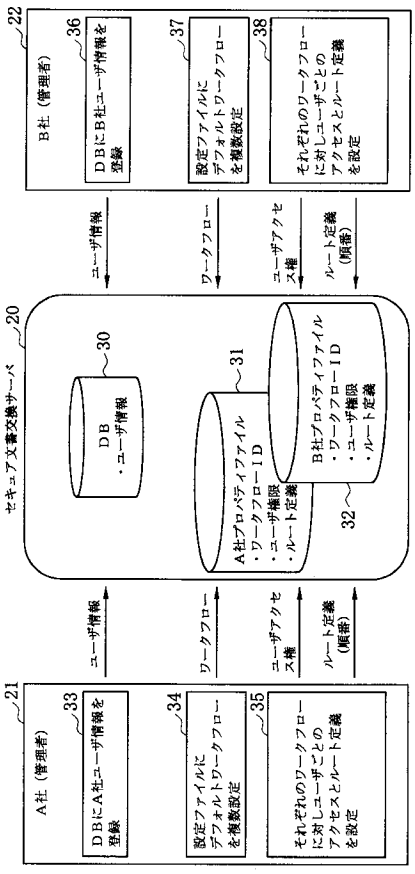
【図１】


B社クライアント端末
16
17
B社クライアント端末
ネットワーク
13
ネットワーク
10
12
19
セキュア文書交換サーバ
ネットワーク
18
原本保管サーバ
11
A社クライアント端末
14
15
A社クライアント端末

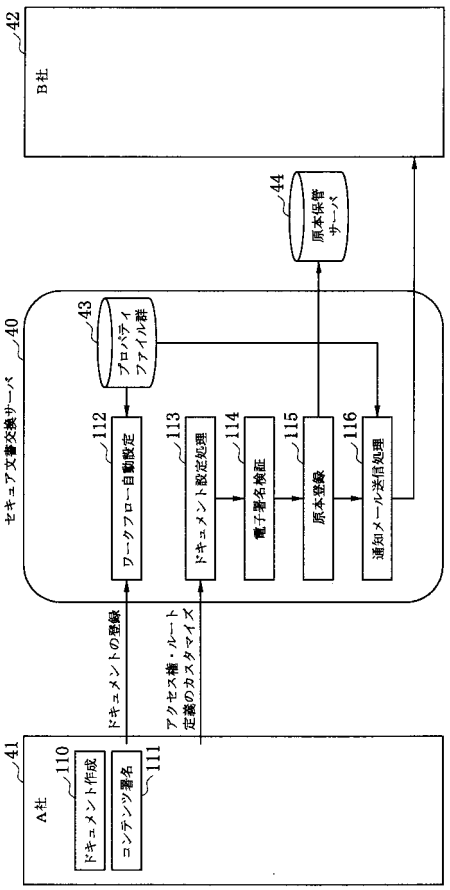
【図２】


B社クライアント端末
16
17
B社クライアント端末
③
④
ネットワーク
13
ネットワーク
10
12
19
セキュア文書交換サーバ
ネットワーク
18
原本保管サーバ
11
①
②
A社クライアント端末
14
15
A社クライアント端末

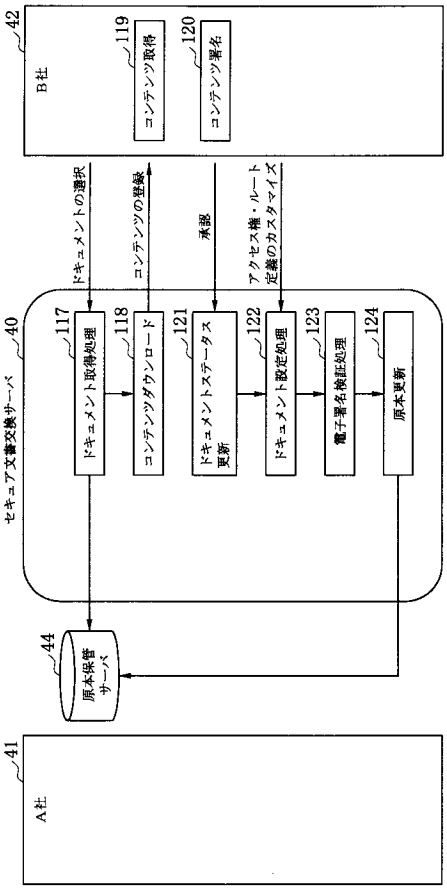
【図３】


22
B社（管理者）
36
DBにB社ユーザ情報を登録
37
設定ファイルにデフォルトワークフローを複数設定
38
それぞれのワークフローに対しユーザごとのアクセスとルート定義を設定
ユーザ情報
ワークフロー
ユーザアクセス権
ルート定義（順番）
20
セキュア文書交換サーバ
30
DB
・ユーザ情報
31
A社プロパティファイル
・ワークフローID
・ユーザ権限
・ルート定義
32
B社プロパティファイル
・ワークフローID
・ユーザ権限
・ルート定義
21
A社（管理者）
33
DBにA社ユーザ情報を登録
34
設定ファイルにデフォルトワークフローを複数設定
35
それぞれのワークフローに対しユーザごとのアクセスとルート定義を設定

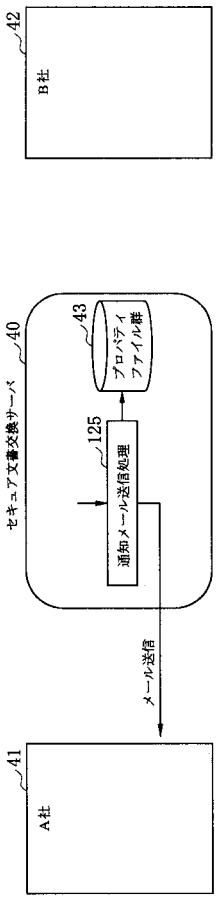
【図４－Ａ】


42
B社
44
原本保管サーバ
43
プロパティファイル群
40
セキュア文書交換サーバ
112
ワークフロー自動設定
113
ドキュメント設定処理
114
電子署名検証
115
原本登録
116
通知メール送信処理
ドキュメントの登録
アクセス権・ルート定義のカスタマイズ
41
A社
110
ドキュメント作成
111
コンテンツ署名

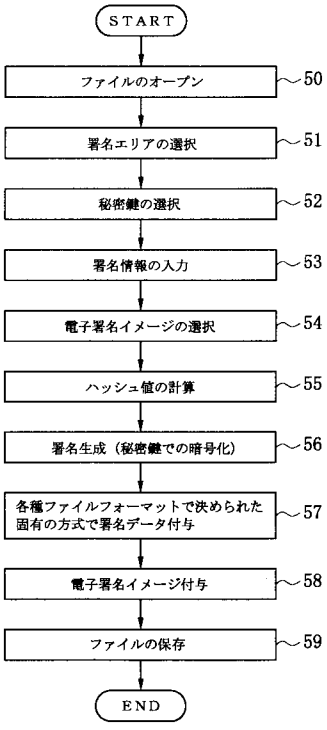
【図４－Ｂ】


42
B社
119
コンテンツ取得
120
コンテンツ署名
ドキュメントの選択
コンテンツの登録
承認
アクセス権・ルート定義のカスタマイズ
40
セキュア文書交換サーバ
117
ドキュメント取得処理
118
コンテンツダウンロード
121
ドキュメントステータス更新
122
ドキュメント設定処理
123
電子署名検証処理
124
原本更新
44
原本保管サーバ
41
A社

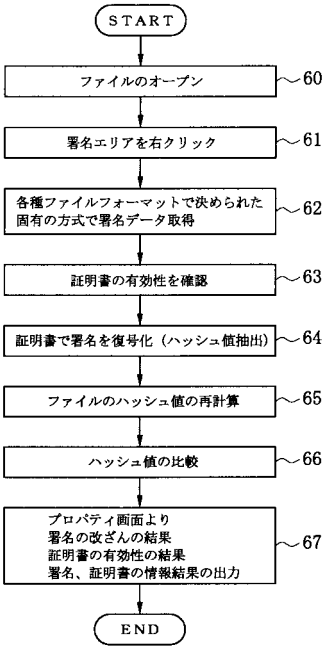
【図４－Ｃ】


42
B社
40
セキュア文書交換サーバ
43
プロパティファイル群
125
通知メール送信処理
メール送信
41
A社

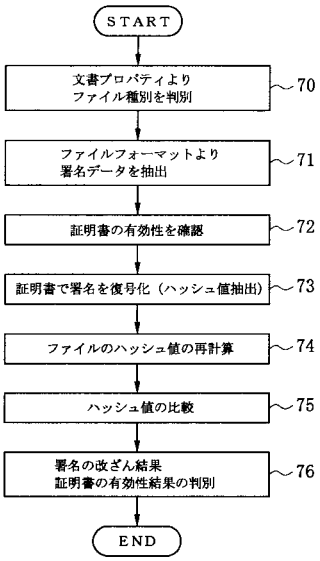
【図５】


START
ファイルのオープン
50
署名エリアの選択
51
秘密鍵の選択
52
署名情報の入力
53
電子署名イメージの選択
54
ハッシュ値の計算
55
署名生成（秘密鍵での暗号化）
56
各種ファイルフォーマットで決められた固有の方式で署名データ付与
57
電子署名イメージ付与
58
ファイルの保存
59
END

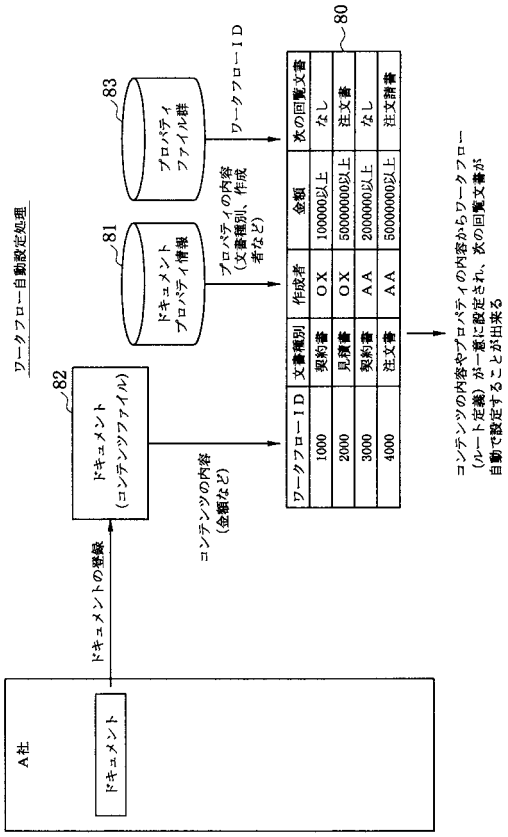
【図６】


START
ファイルのオープン
60
署名エリアを右クリック
61
各種ファイルフォーマットで決められた固有の方式で署名データ取得
62
証明書の有効性を確認
63
証明書で署名を復号化（ハッシュ値抽出）
64
ファイルのハッシュ値の再計算
65
ハッシュ値の比較
66
プロパティ画面より
署名の改ざんの結果
証明書の有効性の結果
署名、証明書の情報結果の出力
67
END

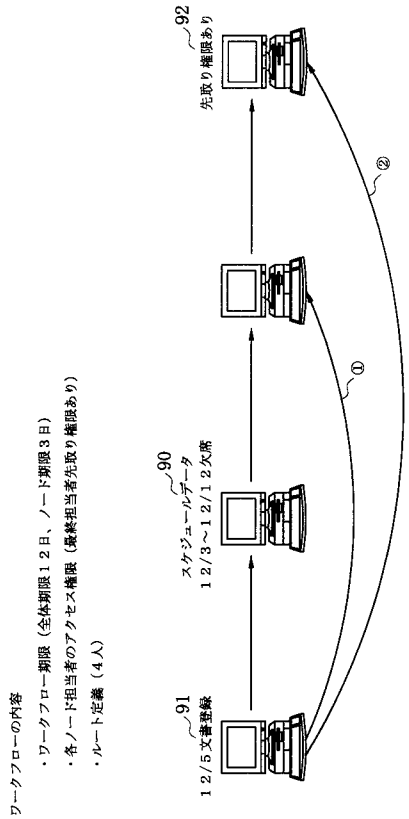
【図７】


START
文書プロパティより
ファイル種別を判別
70
ファイルフォーマットより
署名データを抽出
71
証明書の有効性を確認
72
証明書で署名を復号化（ハッシュ値抽出）
73
ファイルのハッシュ値の再計算
74
ハッシュ値の比較
75
署名の改ざん結果
証明書の有効性結果の判別
76
END

【図８】


ワークフロー自動設定処理
83
プロパティ
ファイル群
ワークフローID
81
ドキュメント
プロパティ情報
プロパティの内容
（文書種別、作成
者など）
80
82
ドキュメント
（コンテンツファイル）
コンテンツの内容
（金額など）
ドキュメントの登録
A社
ドキュメント
ワークフローID
文書種別
作成者
金額
次の回覧文書
1000
契約書
OX
100000以上
なし
2000
見積書
OX
50000000以上
注文書
3000
契約書
AA
20000000以上
なし
4000
注文書
AA
50000000以上
注文請書
コンテンツの内容やプロパティの内容からワークフロー
（ルート定義）が一意に設定され、次の回覧文書が
自動で設定することが出来る

【図９】


ワークフローの内容
・ワークフロー期限（全体期限１２日、ノード期限３日）
・各ノード担当者のアクセス権限（最終担当者先取り権限あり）
・ルート定義（４人）
91
１２/５文書登録
90
スケジュールデータ
１２/３～１２/１２欠席
92
先取り権限あり
①
②