(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4759513号
(P4759513)

(45)発行日　平成23年8月31日(2011.8.31)　(24)登録日　平成23年6月10日(2011.6.10)

(51)Int.Cl.　　F I
G06F 21/24 (2006.01)　　G06F 12/14 520B
G06F 21/20 (2006.01)　　G06F 12/14 560B
　　G06F 15/00 330D

請求項の数 33　(全 39 頁)

(21)出願番号　特願2006-515002 (P2006-515002)
(86)(22)出願日　平成16年5月27日 (2004.5.27)
(65)公表番号　特表2006-526851 (P2006-526851A)
(43)公表日　平成18年11月24日 (2006.11.24)
(86)国際出願番号　PCT/US2004/016848
(87)国際公開番号　WO2004/109443
(87)国際公開日　平成16年12月16日 (2004.12.16)
審査請求日　平成19年4月16日 (2007.4.16)
(31)優先権主張番号　60/475,109
(32)優先日　平成15年6月2日 (2003.6.2)
(33)優先権主張国　米国 (US)

(73)特許権者　505444765
リキッド・マシンズ・インコーポレーテッド
ＬＩＱＵＩＤ　ＭＡＣＨＩＮＥＳ，ＩＮＣ．
アメリカ合衆国，マサチューセッツ州　０２４２１，レキシントン，スイート　１１０，マグァイア　ロード　１０
(74)代理人　100087941
弁理士　杉本　修司
(74)代理人　100086793
弁理士　野田　雅士
(74)代理人　100112829
弁理士　堤　健郎

最終頁に続く

(54)【発明の名称】動的、分散的および協働的な環境におけるデータオブジェクトの管理

(57)【特許請求の範囲】

【請求項１】

制御ポリシー・サーバおよびクライアント装置を含む分散的な環境におけるデータオブジェクトの制御をコンピュータで維持および管理する方法であって、

前記制御ポリシー・サーバに格納されている制御ポリシーについての識別子を、前記クライアント装置に記憶されたデータオブジェクトに添付された制御ポリシータグに記録することによって、各データオブジェクトに、制御ポリシーの識別子を前記クライアント装置が付ける工程であって、各制御ポリシーが、少なくとも、

（ｉ）前記データオブジェクトにアクセスできるユーザのリスト、

（ｉｉ）前記リストのユーザの前記データオブジェクトに対する使用権限、および

（ｉｉｉ）当該制御ポリシーを編集できるユーザのリストである追加リストを含む、制御ポリシー識別子付加工程と、

ユーザがデータオブジェクトへの特定の操作によるアクセスを要求すると、このユーザがその特定の操作で前記データオブジェクトにアクセスできるユーザであるか否かを、前記アクセスされたデータオブジェクトの前記制御ポリシーの識別子が示す制御ポリシーに含まれている、前記データオブジェクトにアクセスできるユーザの前記リスト(i)および前記リストのユーザの前記データオブジェクトに対する前記使用権限(ii)に基づいて、前記クライアント装置のリファレンス・モニタがチェックする、チェック工程と、

前記追加リスト(iii)に含まれているユーザに対して、制御ポリシーを編集するためのインタフェースを前記制御ポリシー・サーバが提供する、インタフェース提供工程とを備

えたデータオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項２】
請求項１において、さらに、
前記ユーザがその特定の操作で前記データオブジェクトにアクセスできるユーザであると前記チェック工程において判断された場合に、前記特定の操作による前記データオブジェクトへのアクセスを前記ユーザに許可するように、前記クライアント装置の前記リファレンス・モニタが前記データオブジェクトを復号化する、復号化工程を備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項３】
請求項１において、さらに、
前記チェック工程よりも前に、前記制御ポリシー・サーバにネットワーク接続している間に、前記制御ポリシーを前記制御ポリシー・サーバから前記クライアント装置がキャッシュする、制御ポリシーキャッシュ工程と、
前記制御ポリシー・サーバにおける制御ポリシーを前記ユーザが利用できるか否かを、前記制御ポリシー・サーバへのネットワーク接続に基づいて、前記クライアント装置が決定する、利用可能性決定工程と、
前記制御ポリシーが利用不可能である場合は、前記キャッシュした制御ポリシーに格納されている、この制御ポリシーの鍵暗号鍵の有効期間および前記キャッシュした制御ポリシーの有効期間に基づいて、前記データオブジェクトに対する前記ユーザのアクセス権が有効である時間期間を前記クライアント装置が決定する、時間期間決定工程と、
前記データオブジェクトに対する前記ユーザのアクセス権が有効である時間期間が満了していない場合には、前記特定の操作による前記データオブジェクトへのアクセスを前記ユーザに許可するように、前記クライアント装置の前記リファレンス・モニタが前記データオブジェクトを復号化する、復号化工程と、を備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項４】
請求項３において、
前記クライアント装置に記憶された前記データオブジェクトの複製を第２のユーザに提供することで、前記データオブジェクトは第２のユーザと共有される、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項５】
請求項４において、前記制御ポリシー・サーバにおける制御ポリシーが利用不可能である間、前記データオブジェクトは、前記キャッシュされた制御ポリシーを用いて、前記ユーザによって生成される、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項６】
請求項１において、前記制御ポリシーは、さらに、データオブジェクトに添付された前記制御ポリシータグにおける制御ポリシー識別子を未管理にして、前記データオブジェクトを前記制御ポリシーによる保護範囲から外すことができるユーザのリストと、新たに生成したデータオブジェクトに添付された前記制御ポリシータグに制御ポリシー識別子を設定することによって、または既存のデータオブジェクトに添付された前記制御ポリシータグにおける制御ポリシー識別子を変更することによって、データオブジェクトに前記制御ポリシーを割り当てできるユーザのリストとを含む、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項７】
請求項１において、前記制御ポリシー内の複数のロール内に登場するユーザの前記使用権限は、そのユーザの個々のロールの明確な使用権限であり、これら明確な使用権限は、そのユーザの個々のロールの明確な使用権限を全て含む一式の使用権限に集約される、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項８】

請求項１において、前記データオブジェクトは暗号化されている、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項９】
請求項８において、前記データオブジェクトは、前記データオブジェクトに対応する制御ポリシーの鍵暗号鍵で暗号化されたコンテンツ暗号鍵で暗号化されている、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項１０】
請求項１において、さらに、
前記制御ポリシー識別子付加工程よりも後に、前記データオブジェクトに添付された前記制御ポリシータグにおける制御ポリシー識別子を変更することによって、前記データオブジェクトを前記制御ポリシーから第２の制御ポリシーに前記クライアント装置が転換させる、転換工程を備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項１１】
請求項１０において、前記第２の制御ポリシーは、
データオブジェクトが保護されていない状態であって、前記データオブジェクトに添付された制御ポリシータグにおける制御ポリシー識別子が未管理に設定されている、保護されていない状態と、
当該第２の制御ポリシーに含まれる前記追加リストのユーザが、そのポリシーにデータオブジェクトを割り当てる特権を有している、制御ポリシーとのうちの少なくとも１つである、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項１２】
請求項１において、さらに、
前記制御ポリシー識別子付加工程よりも後に、予め決められたイベントが発生したときに、前記データオブジェクトを１つの制御ポリシーから第２の制御ポリシーに前記クライアント装置が転換させる転換工程であって、前記第２の制御ポリシーは、
当該第２の制御ポリシーに含まれる前記追加リストのユーザが、そのポリシーにデータオブジェクトを割り当てる特権を有している、制御ポリシーと、
データオブジェクトが保護されていない状態であって、前記データオブジェクトに添付された制御ポリシータグにおける制御ポリシー識別子が未管理に設定されている、保護されていない状態とのうちの少なくとも１つである、転換工程を備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項１３】
請求項１２において、前記予め決められたイベントが、前記制御ポリシーの生成者によって決定されるビジネス・イベントである、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項１４】
請求項１２において、さらに、
前記転換工程よりも後に、データオブジェクトの制御ポリシーの転換を前記クライアント装置がアクティビティ・ログに記録して、データオブジェクトの変更の監査を可能にする、記録工程を備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項１５】
請求項１において、制御ポリシーに含まれている、前記データオブジェクトにアクセスできるユーザの前記リスト(i)および前記リストのユーザの前記データオブジェクトに対する前記使用権限(ii)に応じて、前記制御ポリシーがビジネス・プロセスに分類されている、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項１６】
請求項１５において、特定のビジネス結果の達成を系統立てることを目的とした、制御された段階またはアクティビティに基づいて、ビジネス・プロセスが階層的に体系化され

ている、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項１７】
請求項１６において、前記制御ポリシーは、前記ビジネス・プロセスにおける前記段階または前記アクティビティを表しており、前記階層が、データオブジェクトの制御ポリシーの転換の範囲の限定に使用される、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項１８】
請求項１において、さらに、
前記チェック工程よりも後に、ビジネス・プロセスの１つまたは複数の制御ポリシー内で許可または拒絶されたアクティビティのログを前記クライアント装置が記録する工程と、
前記制御ポリシー・サーバがこの記録されたログを検査および調査することで、ビジネス・プロセスの監査またはフォレンジックを可能にする工程とを備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項１９】
請求項１において、さらに、
前記制御ポリシー識別子付加工程よりも後に、クライアント・コンピュータ上に、前記制御ポリシーに含まれる、前記データオブジェクトにアクセスできるユーザの前記リストに存在するユーザによってアクセスされた前記データオブジェクトに対応する制御ポリシーを前記クライアント装置が表示する、表示工程を備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項２０】
請求項１９において、さらに、
前記データオブジェクトにアクセスできるユーザの前記リスト(i)に、前記ユーザが存在している、制御ポリシーのリストを、前記制御ポリシー・サーバに、前記クライアント装置が要求する、要求工程と、
前記データオブジェクトの制御ポリシーを、前記データオブジェクトを表示するウインドウのタイトルバーに位置するドロップダウン・ウインドウに前記クライアント装置が表示する表示工程であって、このドロップダウン・ウインドウは、前記サーバからの制御ポリシーのリストを、このリストに含まれている、前記データオブジェクトの制御ポリシーが識別可能であるように表示する、表示工程とを備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項２１】
請求項１９において、前記ドロップダウン・ウインドウは、前記ユーザが前記データオブジェクトを転換できる転換先の制御ポリシーを示す、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項２２】
請求項２０において、前記ドロップダウン・ウインドウは、前記制御ポリシーのビジネス・プロセス階層を示す、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項２３】
請求項１において、１つまたは複数のデータオブジェクトが、同一の制御ポリシーを使用する、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項２４】
請求項１において、さらに、
前記データオブジェクトに対応する制御ポリシーを、このデータオブジェクトにアクセスすることなく前記制御ポリシー・サーバが変更させる、変更工程を備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項２５】
請求項１において、さらに、

前記制御ポリシー識別子付加工程よりも後に、前記データオブジェクトに対応する制御ポリシーに対して使用権限を有するユーザが行った変更を、制御ポリシー・サーバが記録する記録工程と、
前記使用権限を有するユーザが行った前記変更に従って、データオブジェクトに対応する制御ポリシーを前記制御ポリシー・サーバが変更する変更工程と、
前記記録された、前記使用権限を有するユーザが行った前記変更を取消すことにより、元の制御ポリシー構成に前記制御ポリシー・サーバが復帰させる復帰工程とを備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項２６】
請求項１において、さらに、
データオブジェクトの対応する制御ポリシーに、使用権限を有するユーザによって決定された変更を前記制御ポリシー・サーバが適用する適用工程であって、前記変更は前記使用権限を有するユーザが設定した所定の時間において適用される、適用工程を備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項２７】
請求項２６において、前記制御ポリシーが関連付けられているビジネス・プロセス内に、前記使用権限を有するユーザによって決定された前記変更が示されている、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項２８】
請求項１において、前記制御ポリシーについての前記識別子は、ポリシーの参照先および前記制御ポリシー・サーバの指定を含む、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項２９】
請求項１において、さらに、
前記チェック工程よりも後に、クライアント装置が、データオブジェクトへのアクセス要求を記録し、アクティビティ・ログに含める工程を備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項３０】
請求項２９において、さらに、
前記アクティビティ・ログ内の前記データオブジェクトのアクティビティを、固有の文書識別子に基づいて特定する特定工程を備えた、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項３１】
請求項１において、
前記制御ポリシータグが、有効期限を有する鍵暗号化鍵によって暗号化されているコンテンツ暗号化鍵を含み、
前記データオブジェクトは、前記コンテンツ暗号化鍵によって暗号化されており、
前記有効期限を越えると、前記データオブジェクトがアクセス不可能になることより、前記データオブジェクトが一時的なものである、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項３２】
請求項１において、
前記制御ポリシータグが、コンテンツ暗号化鍵を含み、
前記データオブジェクトは、前記制御ポリシー・サーバのマスター鍵暗号化鍵によって暗号化されている前記コンテンツ暗号化鍵によって暗号化されていることりより、前記データオブジェクトが永久的なものであり、アクセス提示される際には常に復号化可能である、データオブジェクトの制御のコンピュータでの維持および管理方法。
【請求項３３】
分散的な環境におけるデータオブジェクトの制御を維持および管理するコンピュータ実装されたクライアント装置であって、

前記データオブジェクトを記憶する記憶装置であって、前記データオブジェクトは、前記分散的な環境の制御ポリシー・サーバに格納されている制御ポリシーについての識別子を前記データオブジェクトに添付された制御ポリシータグに記録しており、各制御ポリシーは、少なくとも、

（i）前記データオブジェクトにアクセスできるユーザのリスト、

（ii）前記リストのユーザの前記データオブジェクトに対する使用権限、および

（iii）当該制御ポリシーを編集できるユーザのリストである追加リストを含む、記憶装置と、

ユーザからのデータオブジェクトへの特定の操作によるアクセス要求を受けると、このデータオブジェクトに添付された制御ポリシータグに記録された制御ポリシー識別子が示す制御ポリシーを取得するように、前記制御ポリシー・サーバと通信する通信モジュールと、

このユーザがその特定の操作で前記データオブジェクトにアクセスできるユーザであるか否かを、前記通信モジュールが前記制御ポリシー・サーバとの通信によって取得した前記制御ポリシーに含まれている、前記データオブジェクトにアクセスできるユーザの前記リスト(i)および前記リストのユーザの前記データオブジェクトに対する使用権限(ii)に基づき判断する、ポリシー・チェッカーと、

前記追加リスト(iii)に含まれているユーザに対して、制御ポリシーを編集するためのインタフェースを提供する、ユーザ・インタフェースとを備えた、コンピュータ実装されたクライアント。

【発明の詳細な説明】

【関連出願】

【０００１】

本出願は、２００３年６月２日付の米国特許仮出願第６０／４７５，１０９号の利益を主張するものであり、前記出願の全内容は参照により本明細書に引用したものとする。

【背景技術】

【０００２】

本発明は、デジタル的に符号化された文書およびデータの使用権限の行使および管理の分野に関する。

【０００３】

デジタル・フォーマットでのオーディオ、ビデオ、グラフィック、および著述作品の符号化および配布は、最近のビジネスにおける基本的部分となってきている。しかしながら、オリジナルと同一の複製を容易に作成できること、およびインターネットによって可能になった配布の速度により、そのような作品の所有者は、デジタル符号化データに使用権限を関連付けして行使する技法を採用するようになってきている。そのような技法の関係者の例としては、音楽、映画、または他の娯楽コンテンツの提供者、電子新聞、雑誌、または書籍の発行者、ならびに秘密の、固有の、または他の機密情報を有する企業が含まれる。一般性を欠くことなく、説明を容易にするため、この種のデジタル符号化された作品のすべてを、ここではデータオブジェクトと称することにする。

【０００４】

使用権限をデータオブジェクトに関連付けて行使するための多くの手法が存在する。一般的な手法の１つは、データオブジェクトについて、オブジェクトを保持する物理的媒体からの無許可の複製を防止しようする技法を基本としている。米国特許第５，５１３，２６０号が、そのような複製防止方式の一例である。

【０００５】

複製防止技法は、特定の分野においては適正であるが、それら技法が行使できる使用権限の種類は、一般的解決策となるにはあまりにも粗い分類である。例えば、固有かつ秘密の文書の所有者は、保護対象の文書を、個人の１グループについては読み出しのみを可能にし、他のグループについては読み出しおよび書き込みを許可したいと望むことがある。複製防止技法は、このような使用ポリシーを記述するには、性能的に不十分である。

【０００６】
許可されたユーザの各クラスすなわちグループに対して指定されたルールのセットに従って、許可ユーザのみがオブジェクトにアクセスし、使用できるようにデータオブジェクトを保護する、より汎用的な手法が存在する。この手法は、典型的には暗号化技術に依拠して、許可ユーザのみが実際のデータオブジェクトへのアクセス権を有することを保証する。詳細には、許可ユーザには、保護されているオブジェクトを復号化して実際のデータオブジェクトを生成するのに必要な秘密鍵へのアクセスが与えられる。使用権限は、典型的には、秘密鍵へのアクセスを許可されるユーザ、および許可ユーザが復号化されたデータオブジェクトを用いて実行できる内容を指定する。この基本的手法は、デジタル著作権管理（ＤＲＭ）および関連の権限管理技法におけるワークの大部分を含む。この手法は、暗号化されたビットの複製は防止しないが、無許可ユーザは秘密鍵なしでは保護されているデータオブジェクトにアクセスできないため、複製防止と同じ最終結果を達成している。

【０００７】
権限管理システムが効果的に機能するには、使用権限を暗号化データオブジェクトに緊密に結び付けて、使用権限が常に関連のオブジェクトとともに現れるようにしなければならない。この結合は、オブジェクトの所有者でない者または他の無許可のユーザが、データオブジェクトを使用権限から分離することをきわめて困難にし、理想的には不可能にしていなければならない。

【０００８】
データオブジェクトを使用権限から分離しようとする攻撃は、２つのカテゴリーに分類される。第１のカテゴリーは、使用権限と暗号化データオブジェクトとの結合に対する攻撃から成る。このカテゴリーの攻撃の一例は、ある１つのファイルの使用権限を他のファイルの使用権限に置き替えることである。第２のカテゴリーは、データオブジェクトが復号化されて、許可ユーザによって使用されるときに企てられる攻撃から成る。この目的は、使用権限を直接回避して、復号化されたデータオブジェクトの保護されない複製を入手することにある。権限管理システムが効果的に機能するには、両カテゴリーの攻撃を防御する機構を備えていなければならない。

【０００９】
第２のカテゴリーの攻撃は、暗号化データオブジェクトであっても、許可ユーザがアクセスするには、最終的には復号化する必要があるという事実を明示している。権限管理システムは、ユーザが直接データオブジェクトを復号化することを許可するか、あるいは権限管理対応アプリケーションの装備および使用を要求する。多くの商業的状況においては、保護されたデータオブジェクトの所有者は、エンドユーザに暗号化工程および復号化工程を明示することでエンドユーザを困惑させることは望まない。また、保護されたデータオブジェクトの所有者は、使用権限の順守に関してエンドユーザを信用しない。したがって、好ましい方法は、データオブジェクトを許可ユーザに対して透過的に復号化し、このオブジェクトに付された使用ルールを行使する権限管理対応アプリケーションを使用する。権限管理対応アプリケーションは、権限管理システムについての信頼エージェントとして機能し、保護されたデータオブジェクトの所有者によって指定されたルールを行使する。権限管理対応アプリケーションの例としては、暗号化フォーマットの音楽ファイルを再生できるメディアプレーヤがある。

【００１０】
結合の緊密性および信頼アプリケーション・エージェントへの依拠が、権限管理システムと暗号化ファイルシステム技法の基本的な相違を構成する。暗号化ファイルシステム（例えば、マイクロソフト社のＥＦＳ、米国特許第６，２４９，８６６号）においては、使用権限はデータオブジェクト（例えば、ファイル）を保持するコンピュータ構造にのみ関連付けられ、データオブジェクトそのものには関連付けられていない。アプリケーションが暗号化ファイルシステムによって行使される使用権限を認識していないため、オブジェクトへのアクセスを許可されているが使用権限の変更は認められていないユーザにとって

、権利を伝達しない方式でデータオブジェクトを保存することは、かなり容易である。詳細には、暗号化ファイルシステム内で保護されているファイルの許可ユーザは、保護ファイルの複製を妨害されることなく生成するためには、ファイルを暗号化ファイルシステムの外部のディレクトリに保存するだけでよい。

【００１１】

権限管理対応アプリケーションを使用することにより、権限管理システムは、暗号化されたデータオブジェクトとそれに関する使用権限の間の緊密な結合を行使できる。設計者によっては、使用権限を暗号化データオブジェクトと共に格納することによりこの緊密な結合を実現することを選択し、多くの場合セキュアコンテナと称される新しいデータオブジェクトを生成している（例えば、米国特許第６，４２７，１４０号）。この手法においては、使用権限は保護されたデータオブジェクトの特定の複製に明確に結び付けられる。この手法が優れた機能を示すのは、例えば、オンライン音楽などの商業市場においては、データオブジェクトの所有者が読み出し専用のコンテンツを発行し、このコンテンツの使用および配布に関する管理を維持することをとにかく望む場合である。このような権限管理システムを、「発行専用配布モデルのサポート」と称する。

【００１２】

発行専用配布モデルの基本的な特性は、セキュアコンテナ内の使用権限が時間とともに変化することを想定していない。あるいは、変化する場合でも、変化は低速であり、変化によって同時に影響を受けるエンドユーザは１人のみであるとしている。発行専用配布モデルにおいて使用権限を変更するには、所有者は、使用権限を保持するセキュアコンテナにアクセスしなければならない。セキュアコンテナへのアクセスによって、権限管理システムは、コンテナ内に保存された使用権限を変更できるようになる。セキュアコンテナが利用でない場合、所有者は、元のセキュアコンテナにアクセスするためのエンドユーザ許可権を（例えば、このコンテナについての復号鍵を破壊することによって）削除し、同一の保護されたデータオブジェクトであるが新しい使用権限を有するエンドユーザに対して、新しいセキュアコンテナを再発行できる。この後者の手法は、権限管理システムが新しいセキュアコンテナをエンドユーザに通知することを必要とし、さらに権限管理システムが、新しいセキュアコンテナ内に入れるデータオブジェクトの複製を有することを必要とする。

【００１３】

これらの要件は、オンライン音楽などの分野においては負担とならないが、動的な環境、すなわちデータオブジェクトを保護している使用権限が頻繁に変更され、かつおそらくは多くの方法で変更される可能性がある環境に対しては、重大な障害になる。さらに、これらの要件は、多数のユーザが保護データオブジェクトの複製を種々のコンピュータ装置および記憶媒体上に個々に有する可能性があり、それらコンピュータ装置および記憶媒体のいくつかがオンラインでなく、あるいは保護オブジェクトの所有者がアクセスできない可能性がある分散的な環境に対しても、重大な障害になる。このような環境においては、所有者が保護オブジェクトの使用権限を変更することを望む場合に、保護オブジェクトのすべての複製に権限管理システムがアクセスできないことは明白である。さらに、保護データオブジェクトを複数のユーザからなるグループに新しく再発行することも、使用権限の変更が少数のユーザにのみ作用し、残りのユーザに通知されない（気付かれない）可能性があるため、望ましくない。さらに、所有者が使用権限を制御するがオブジェクトの最新バージョンの複製を有していない分散的な環境においては、保護データオブジェクトの再発行の可能性すらもない。

【００１４】

極めて協働的な環境においては、協働的な資料の単一の「発行者」を特定することが困難であることが多く、不可能なこともある。しかし、企業データについては、企業のビジネス目的で生成された協働的な資料について、「所有者」を識別することが可能である。所有者は、著作者または協働作品の著作者らを雇用している企業である。したがって、協働的な環境においては、機密資料を作成した者とこの資料の使用権限を決定する者との間

を区別することは、明らかに必要である。

【００１５】

オーセンティカ社（Authentica）は、動的および分散的な環境におけるデジタル・データオブジェクトの使用権限の行使および管理についての部分的な解決策に関する特許を得ている（米国特許第６，４４９，７２１号）。この手法によれば、保護オブジェクトがエンドユーザに配布された後であっても、デジタル・データオブジェクトの所有者が、使用権限についての制御を維持できる。詳細には、この手法は、保護オブジェクトの使用権限を単一の中央位置に格納し、したがって保護データオブジェクトの所有者は、このデータオブジェクトのあらゆる（おそらくは多数の）複製に同時にアクセスする必要なく、オブジェクトの使用権限を変更できる。理想的には、この手法は、オブジェクトの使用権限の唯一の正式な複製を保持するのに対して、データオブジェクトの多数の分散された複製の存在を可能にする。オブジェクトの使用権限の唯一の正式な複製を持つことで、使用権限の管理が簡単になる。

【００１６】

オーセンティカ社の手法は、保護情報の各セグメントについて、固有の識別子を生成する。オーセンティカ社の鍵サーバは、固有のセグメント識別子と、それらセグメントについての使用権限と、各セグメントの保護およびアクセスに使用される暗号鍵との間の関連性を保持する。保護セグメントにアクセスするには、エンドユーザは、サーバに対して本人であることを証明し、アクセスを希望する保護セグメントの識別子を提示しなければならない。ユーザが保護セグメントへのアクセスを許可されているならば、サーバは、そのセグメントに対する復号鍵およびそのセグメントとユーザの組み合わせについての使用権限を用いて応答する。エンドユーザ装置上の権限管理対応アプリケーションがサーバの応答を使用し、その保護セグメントに対する所有者が指定したアクセスレベルをエンドユーザに提供する。

【００１７】

オーセンティカ社のような手法は、保護データオブジェクトの所有者が、保護データオブジェクトを収集または再配布の必要なしに、配布情報の使用を制御して使用情報を動的に変更することを可能にするが、協働的な環境における使用権限の行使および管理に関する問題については、完全な解決策ではない。詳細には、協働的な環境についての解決策は、既存の協働モデルに無理なく適合するようにして、協働の生成物の保護に焦点を合わせる必要がある。例えば、民間企業においては、協働作業によって、すべて同一使用権限によって保護される複数の文書が生成されることが頻繁にあり、したがって真に協働的な解決策は、一式の使用権限の下での複数の文書の容易なグループ化を可能しなければならない。さらに、多くの場合、協働作業において生成された派生的な作品も協働の使用権限によって保護されると予測され、それらの権限についての変更は、作品を新しい協働の設定に移すための既存のプロセスと一致することが予想される。最後に、現在の権限管理システムのすべて、特に発行専用配布モデルに焦点を合わせた権限管理システムでは、協働的な対話を含むデータオブジェクトを適正に保護するために、保護文書の生成、変更、および配布を厳重に管理しすぎている。適正な解決策は、「著作者」の保持する権限と「所有者」の保持する権限との間を明示的に区別しなければならない。

【発明の開示】

【００１８】

任意、必須、またはロールに基づくアクセス制御のモデルを含むこの分野におけるさまざまな技法および発明、ならびにＤＲＭ（デジタル著作権管理）関連の技法が、前記要件のうちの１つまたは別の要件に対応してきた。しかし、本発明の実施形態は、動的、分散的、かつ協働的な環境を対象とする権限管理システムに関する必要なすべての形態に対応する独自の手法を提供する。

【００１９】

本発明の構成は、ユーザによって動的、分散的、かつ協働的な環境で起草、アクセス、および変更されるデータオブジェクト全体にわたる制御を維持および管理する方法および

システムを含む。

【００２０】

データオブジェクトは、デジタル形式で符号化され、コンピュータ構造内にカプセル化されているあらゆるオーディオ、グラフィック、ビデオ、または著述作品であって、例えば、ソフトウェア・プログラムによってアクセスおよび操作可能であるファイル、メッセージ、または共有メモリ・オブジェクトなどである。

【００２１】

分散的および協働的な環境（context）とは、１人または複数のユーザからなるグループが、少なくとも間欠的な接続を有しているコンピュータのネットワーク上で、特定の共通目的を達成するために、１つまたは複数のデータオブジェクトの集合に個々にまたは協働的に取り組む環境のことをいう。本発明においては、この共通目的をビジネス・プロセスと称する。

【００２２】

ビジネス・プロセスにおいては、異なる一式の権限および責任を有するユーザのクラスが存在しうる。本発明においては、それらのクラスをロールと称する。

【００２３】

本発明では、システムの特性がビジネス・プロセスの寿命の間に変化しうる場合に、環境が動的であると考える。例えば、システムはビジネス・プロセスの最中に、あるロールに属するユーザの組の変更を可能にし、あるいはあるデータオブジェクトに付された制御の種類の変更を可能にできる。本発明は、保護データオブジェクトの発行および変更を、それらデータオブジェクトの使用を制御しているポリシーの所有権および操作から分離している。

【００２４】

データオブジェクトに関する制御は、特定のロールに属するコンピュータ・ユーザによって作動されるソフトウェア・プログラムが、オブジェクトにアクセスして操作できる方法を記述する一式のルールよって指定される。本発明においては、これらのルールを使用権限と称する。

【００２５】

制御ポリシーは、使用権限が許可される条件を記載する署名付きの表明である。制御ポリシーは、少なくとも、データオブジェクトにアクセスできるユーザのリスト、それらアクセスを有するユーザの権限、および制御ポリシーを定義または編集できるユーザの追加リストを含んでいる。さらに、本発明におけるポリシーは、その制御のもとにあるオブジェクトに適用する補足的な特性を定義して、それらオブジェクトの信頼性、完全性、および秘密性を保証できる。

【００２６】

先のパラグラフで述べたとおり、本発明において使用される用語の「制御」は、通常は、無許可ユーザおよびそれらユーザのアプリケーションによるアクセスに対抗する保護を意味する。

【００２７】

本発明の別の目的は、ビジネス・プロセス内への可視性を得るシステムおよび方法を提供することにある。そのような可視性を、それらのデータオブジェクトの実際のデジタル表現の暗号化またはその他の変更によってデータオブジェクトを保護する上でのリスクを犯すことなく、達成できる。制御が保護を含んでいなければ、悪意のある相手、すなわち保護データオブジェクトを保護された環境の外から操作する者に対抗して、確実に制御を維持することを保証できないことは明白である。しかし、この制御レベルは、企業がデータオブジェクトを平文に維持すると同時に、ビジネス・プロセス内への可視性を望むようなビジネス状況において、依然として望まれる。

【００２８】

本発明の別の目的は、制御ポリシーを１つまたは複数の中央サーバに格納する方法およびシステムを提供することにある。

【００２９】
本発明の別の目的は、制御ポリシーを編集できるユーザの表示およびそれらのユーザが実行できる変更の種類に基づいて、制御ポリシーを編集する方法およびシステムを提供することにある。制御ポリシーの変更は、制御ポリシーを格納しているサーバ上で実行される。
【００３０】
本発明の別の目的は、１つまたは複数の制御ポリシーを一時的に変更し、次いで将来のある時点において元の設定に自動的に復帰させる方法およびシステムを提供することにある。
【００３１】
本発明の別の目的は、１つのボタンのクリックで実行し、その後別のボタンのクリックで元に戻すことができる１つまたは複数のあらかじめ設定された一時的な変更を有する方法およびシステムを提供することにある。
【００３２】
本発明の別の目的は、各データオブジェクトに１つの（すなわち、それぞれの）制御ポリシーの識別名を付与する方法およびシステムを提供することにある。本発明においては、その識別名がデータオブジェクトに付与されている制御ポリシーを、そのデータオブジェクトを保護する制御ポリシーと称する。さらに、そのようなデータオブジェクトを、保護データオブジェクトと称する。
【００３３】
本発明の別の目的は、複数のデータオブジェクトが同一制御ポリシーを参照できるようにすることにある。
【００３４】
本発明の別の目的は、制御ポリシーの識別名が、そのネーム空間において実際の制御ポリシー識別子を定義しているサーバを特定する方法およびシステムを提供することにある。好ましい実施形態においては、データオブジェクトに付されたポリシー参照は、サーバのＵＲＬおよびサーバにとって既知の数値を含んでいる。
【００３５】
本発明の別の目的は、制御ポリシーによって保護されるデータオブジェクトの生成、アクセス、または変更を試みるユーザが、データオブジェクトに関してそのアクションを実行する権限を有していることを、ポリシー・サーバに間欠的に接続される可能性のあるクライアントによってチェックする、方法およびシステムを提供することにある。ユーザが権限を有している場合、クライアントは要求されたアクションの続行を許可する。ユーザが権限を有していない場合、クライアントは適切なエラーメッセージによって応答する。言い換えると、ビジネス・プロセス手法によって提供される保護は、所有され、極秘の、または別の慎重を期するデータオブジェクトを、ディスクに格納される間、または通信リンクを介して伝送される間に、保護するだけでなく、データオブジェクトが許可ユーザのソフトウェア・アプリケーションによって操作される際およびアプリケーション間の通信（例えば、マイクロソフト社のＷｉｎｄｏｗｓ（登録商標）オペレーティング・システムにおけるクリップボード操作）の際にもこれらデータオブジェクトを保護する。
【００３６】
本発明の別の目的は、装置、場所、アクセス時間、またはネットワーク接続の制約を特定する条件を含む制御ポリシーを有する方法およびシステムを提供することにある。
【００３７】
本発明の別の目的は、制御ポリシーの編集を許可されたユーザが、このポリシーによって保護されているすべてのデータオブジェクトに物理的または電子的にアクセスすることなく、ポリシーを変更できる方法およびシステムを提供することにある。
【００３８】
本発明の別の目的は、保護データオブジェクトの正式の１つまたは複数の複製だけを、データオブジェクトを保護する制御ポリシーの変更の権限を有さないユーザのコンピュー

タ装置または媒体上に置くことができる方法およびシステムを提供することにある。

【００３９】

本発明の一実施形態においては、保護データオブジェクトを他のユーザに配布する前に、保護データオブジェクトをポリシー・サーバに登録する概念は存在しない。これは、オフラインである可能性のある許可ユーザの装置上でデータオブジェクトの生成および変更を含む協働的作業をサポートするのに必要とされる本発明の主要な側面である。

【００４０】

本発明の別の目的は、許可ユーザが彼らの作業しているクライアントが指定された制御ポリシーのサーバとの接続を失っている場合であっても、新しい保護データオブジェクトを生成できるようにする方法およびシステムを提供することにある。この状況における許可ユーザは、制御ポリシーの下でデータオブジェクトを生成する権限を有するユーザである。好ましい実施形態においては、ユーザは、ある程度最近のポリシー・サーバへのアクセスを有する必要があり、ここでの「最近」とは、そのポリシーについて指定されたキャッシュの時間切れ期間内を意味している。

【００４１】

本発明の別の目的は、２人またはそれ以上の許可ユーザが保護データオブジェクトを閲覧し、新規または既存の保護データオブジェクトについて協働的に作業する方法およびシステムであって、それらユーザのクライアントのうちの１以上が協働的データオブジェクトを保護する制御ポリシーの単一または複数のサーバへの接続を失う場合でも、そのような協働的な作業が可能である方法およびシステムを提供することにある。保護データオブジェクトは、サーバに接続されているときには未だ閲覧されていなくてもよい。共有のデータオブジェクトは新しく生成、すなわち、ユーザがサーバとの接続を有していないときに生成されてよい。

【００４２】

本発明の別の目的は、ポリシー・サーバの記憶装置が、決められた制御ポリシーの数に比例して拡大収縮する方法およびシステムを提供することにある。記憶装置は、固有の保護データオブジェクトの数に応じて拡大収縮すべきではなく、それら保護データオブジェクトの複製の数に応じて拡大収縮すべきでもない。

【００４３】

本発明の別の目的は、制御ポリシーをビジネス・プロセスにグループ化する方法およびシステムを提供することにある。

【００４４】

本発明の別の目的は、制御ポリシーに含まれる１つまたは複数のロールを定義することによって制御ポリシーを構成する方法およびシステムを提供することにある。各ロールは、それぞれの一式の使用権限およびユーザのリストを含む。

【００４５】

本発明の別の目的は、１つの制御ポリシーに含まれる複数のロールに登場するユーザの使用権限を集約する方法およびシステムを提供することにある。

【００４６】

本発明の別の目的は、ビジネス・プロセスおよびそれらが包含する制御ポリシーを管理（生成、編集、および削除）する特権を有するユーザと、制御ポリシーの１つまたは複数のロールのユーザのリストのみを変更する特権を有するユーザとを区別する方法およびシステムを提供することにある。

【００４７】

本発明の別の目的は、データオブジェクトについての制御ポリシーの識別名を変更できる方法およびシステムを提供することにある。この変更により、データオブジェクトをそのシステムによって管理されないようにしてもよい。

【００４８】

本発明の別の目的は、適正な使用権限を有するユーザがデータオブジェクトについての制御ポリシーの識別子を変更できる方法およびシステムを提供することにある。オブジェ

クトの制御ポリシー識別子を「非管理」または同等の状態に変更することによって、ユーザに、データオブジェクトを被保護にする権限を付与することもできる。

【００４９】

本発明の別の目的は、データオブジェクトを制御ポリシーの外に移動できるユーザのリストと、ポリシーをデータオブジェクトに割り当てることができるユーザの別個のリストとを決定する制御ポリシーを有する方法およびシステムを提供することにある。これらのアクションは両方とも、データオブジェクトに付された制御ポリシー識別子の変更を含む。これらのリストについて、ユーザをまったく含まない時点が存在してもよい。

【００５０】

本発明の別の目的は、手動で移動および割り当てを行なう権限を有するユーザに対して、制御ポリシー間のデータオブジェクトの移動を自動化する方法およびシステムを提供することにある。この構成の好ましい実施形態は、ツールを既存の電子ビジネス・プロセスのソフトウェア・コンポーネントに統合することを含む。

【００５１】

本発明の別の目的は、ビジネス・プロセスの管理者が制御ポリシー間のデータオブジェクトの自動移動を生じさせるイベントを決定できる方法およびシステムを提供することにある。

【００５２】

本発明の別の目的は、ビジネス・プロセスを階層方式に体系化する方法およびシステムを提供することにある。そのような階層を用いて、制御ポリシー間のデータオブジェクトの移動の範囲を制限できる。さらに、階層を用いて、単一の位置にある複数のビジネス・プロセスに共通の制御ポリシーまたは他の特性を決定できる。

【００５３】

本発明の別の目的は、保護データオブジェクトの制御ポリシーを表示および変更する方法およびシステム（例えば、グラフィカル・ユーザ・インタフェース）を提供することにある。一実施形態においては、これは、データオブジェクトを表示するウインドウのタイトルバーに位置するドロップダウン・ウインドウとして実現される。このドロップダウン・ウインドウは、ドロップレット・コントロールと称される。ユーザがドロップレット・コントロールをクリックすると、ウインドウが開き、ユーザにより選択される複数のポリシーおよびオプションが表示される。

【００５４】

本発明の別の目的は、ユーザがドロップレット・コントロールを起動したときに、ユーザが現在のデータオブジェクトを移動できる可能な制御ポリシーのリストを表示する方法およびシステムを提供することにある。

【００５５】

本発明の別の目的は、ユーザがデータオブジェクトの起動されたドロップレット・コントロールウインドウ内で新しい制御ポリシーを選択したときに、データオブジェクトの制御ポリシーを変更する方法およびシステムを提供することにある。

【００５６】

本発明の別の目的は、起動されたドロップレット・コントロール・ウインドウ内にビジネス・プロセスの制御ポリシーの階層構造を表示する方法およびシステムを提供することにある。

【００５７】

本発明の別の目的は、データオブジェクトをコンテンツ暗号化鍵（ＣＥＫ）で暗号化する方法およびシステムであって、このＣＥＫは、データオブジェクトに関連付けられた制御ポリシーの鍵暗号化鍵（ＫＥＫ）で暗号化される。

【００５８】

本発明の別の目的は、制御ポリシーによって保護されるデータオブジェクトを一時的または永久的なオブジェクトのいずれとして取り扱うべきかを指示する方法およびシステムを提供することにある。一時的なデータオブジェクトは、将来の特定の指定された時間ま

でアクセス可能であり、その時間後に、アクセス不可能および復元不可能になる。永久的なデータオブジェクトは、権限管理システムまたはそのエージェントに提示されたときには、常にアクセス可能または復元可能である。

【００５９】

本発明の別の目的は、制御ポリシーによって保護されるデータオブジェクトのすべてを、将来の指定時間よりも前に強制的にアクセス不可能かつ復元不可能にする方法およびシステムを提供することにある。ビジネス・プロセスの管理者は、計画よりも早くアクセスを永久的に無効にすることができる。

【００６０】

本発明の別の目的は、制御ポリシー識別子を、（おそらくは暗号化された）保護データオブジェクトのビットと共に格納されるデータ構造内に記録する方法およびシステムを提供することにある。好ましい実施形態においては、このデータ構造を制御ポリシー・タグ（ＣＰＴ）と称する。

【００６１】

本発明の別の目的は、ＣＰＴを保護データオブジェクトの開始端または終端に付ける方法およびシステムを提供することにある。

【００６２】

本発明の別の目的は、保護データオブジェクトのＣＰＴを、クライアントまたはサーバ装置上のいずれかの上に構成する方法およびシステムを提供することにある。

【００６３】

本発明の別の目的は、ＣＥＫをＣＰＴ内に安全に格納する方法およびシステムを提供することにある。ＣＰＴがＣＥＫを含んでいるため、クライアントはキャッシュしたポリシーおよび鍵（ＫＥＫ）情報のみを用いて、オフラインで保護データオブジェクトにアクセスできる。

【００６４】

本発明の別の目的は、保護データオブジェクトの有効期限切れのＣＰＴを自動的に置換する方法およびシステムを提供することにある。ＣＰＴの期限切れは、ＣＰＴフォーマットが変更されることによって、あるいはＣＰＴの制御ポリシーＫＥＫが期限切れとなる（すなわち、その有効期限を越える）ことによって生じる。

【００６５】

本発明の別の目的は、権限管理システムの信頼できるクライアントは古いＣＰＴフォーマットを解釈するためのコードを必要としない方法およびシステムを提供することにある。

【００６６】

本発明の別の目的は、制御ポリシーが読み出し専用のまたは読み出し専用コンピュータ媒体上に格納されたデータオブジェクトを保護することを示す方法およびシステムを提供することにある。

【００６７】

本発明の別の目的は、無許可ユーザにデータオブジェクトを保護しているシステムにアクセスしたことを通告する方法およびシステムを提供することにある。好ましい実施形態は、ＣＰＴにテキスト・メッセージを含む。

【００６８】

本発明の別の目的は、改ざんに対してＣＰＴの完全性を守る方法およびシステムを提供することにある。好ましい実施形態は、ＣＰＴのフィールド全体にわたりセキュア・ハッシュ（secure hash）を使用する。

【００６９】

本発明の別の目的は、データオブジェクトのＣＥＫがＣＰＴ内に格納されている間、そのＣＥＫの秘密性を守る方法およびシステムを提供することにある。好ましい実施形態は、ＣＥＫを制御ポリシーのＫＥＫで暗号化する。暗号化されたＣＥＫは、データオブジェクトが変更されたときにランダムなシード値を用いてＣＥＫを変更することによって、既

知平文攻撃（すなわち、２つの類似文書の同一部分を知ることに基づく攻撃）に対して保護される。

【００７０】

本発明の別の目的は、サーバおよびクライアント通信をネットワークに基づく攻撃に対して保護する方法およびシステムを提供することにある。好ましい実施形態は、クライアントとサーバとの間の通信に、ハイパーテキスト・トランスファ・プロトコル・オーバ・セキュア・ソケット・レイヤー（ＨＴＴＰＳ）接続を使用する。

【００７１】

本発明の別の目的は、ビジネス・プロセスの１つまたは複数の制御ポリシー内で許可および拒絶されたアクティビティに基づいて、ビジネス・プロセスの監査またはフォレンジックを可能にする方法およびシステムを提供することにある。

【００７２】

本発明の別の目的は、ＣＰＴ内に保持された固有の文書識別子に基づいてアクティビティ・ログ内のデータオブジェクトを識別する方法およびシステムを提供することにある。

【００７３】

本発明の別の目的は、ユーザ・ログイン時にクライアントがサーバにアクセスして、そのユーザ名が挙げられている制御ポリシーを取得してキャッシュできるようにする方法およびシステムを提供することにある。この実施形態により、間欠的な接続、保護データオブジェクトのオフラインでの使用、および制御ポリシーにおいて名称が挙げられている他のユーザとのオフラインでの協働など、協働的かつ分散的な環境において生じる問題に対応する。

【００７４】

本発明の別の目的は、クライアントがサーバによりキャッシュされたポリシーを確認するポーリングの頻度を変更する方法およびシステムを提供することにある。この頻度の設定は、アクセスを許可する前に、クライアントがキャッシュ・ポリシーを常に確認する必要があるように設定できる。

【００７５】

本発明の別の目的は、ネットワーク・アクセスが復元されたときに、クライアントがキャッシュされたポリシーを確認および更新できる方法およびシステムを提供することにある。

【００７６】

本発明の別の目的は、サーバがクライアントに対し彼らのキャッシュされたポリシーを更新するよう促す方法およびシステムを提供することにある。

【００７７】

本発明の別の目的は、キャッシュされた制御ポリシーの有効期間を指定する方法およびシステムを提供することにある。

【００７８】

本発明の別の目的は、制御ポリシーのＫＥＫの有効期限を指定する方法およびシステムを提供することにある。

【００７９】

本発明の別の目的は、サーバがクライアントに制御ポリシーのＫＥＫの履歴の一部を供給できる方法およびシステムを提供することにある。保護データオブジェクト内の期限切れポリシーＫＥＫの使用は、クライアントがオブジェクトにアクセスする前にサーバと交信することを強制しない。たとえユーザがオンラインで保護データオブジェクトにアクセスしなくても、オフラインのアクセスがデータオブジェクトの制御ポリシーのキャッシュの時間切れ期間内に行なわれている限りは、ユーザは期限切れのＫＥＫを理由にアクセスを拒否されることはない。

【００８０】

本発明の前記の目的、特徴および利点、ならびに他の目的、特徴および利点は、添付の図面に示されている本発明の好ましい実施の形態についての以下のさらに詳しい説明から

、明らかになるであろう。添付の図面においては、同一の参照符号は異なる図であっても同一部分を示す。図面は必ずしも縮尺通りではなく、本発明の原理を示すことに重点がおかれている。

【発明を実施するための最良の形態】

【００８１】

本発明の好ましい実施形態を以下に説明する。

【００８２】

本発明は、ビジネスの重要なプロセスを反映する構造において体系化された使用権限の集中管理から出発する。図１は、本発明の一実施形態において使用されるポリシーの体系化構造１０を示している。ビジネス・プロセス１２は、特定のビジネス結果の達成に向けて系統的に誘導される制御段階またはアクティビティに基づく前進的に継続する手順を表わしている。階層的体系化構造１０内のビジネス・プロセス１２は、１つまたは複数の制御ポリシー１４を保有するコンテナとして作用する。制御ポリシー１４は、保護データオブジェクトを誰がどのように使用できるのかを管理する使用ルールを指定している。ポリシーは、典型的には、ビジネス・プロセスにおける段階およびアクティビティを表わしており、データのクラス分け（例えば、企業秘密、幹部専用等）をサポートするのに充分な順応性を有する。保護データオブジェクト（文書として図示されている）のそれぞれは、ビジネス・プロセス１２内の単一の制御ポリシー１４に関連付けられ、この制御ポリシー１４の制御下にある。制御ポリシー１４のそれぞれは、１つまたは複数のロール１６を指定している。ロール１６は、ユーザの組（すなわち、グループ）、およびポリシー１４によって管理されるデータについてのユーザの権限を記述している。

【００８３】

図１の体系化構造１０を使用し、本発明の以下の実施形態によって、体系化構造はそれ自体のデータオブジェクトの使用および流れの制御を維持して、権限管理動作をデータオブジェクトの複製への物理的アクセスから分離できる。例えば、一式のデータオブジェクトが与えられ、それらのすべてが単一の制御ポリシーによって保護されると仮定する。なお、この一式のデータオブジェクトは、１つのデータオブジェクだけを含んでいてもよい。本発明および本発明の好ましい実施形態は、制御ポリシーの変更がエンドユーザに伝達され、最終的に、次にユーザが変更されたポリシーによって保護されたデータオブジェクトにアクセスするときに、制御ポリシーの変更を認識することを保証する。この保証は、変更時に保護データオブジェクトの所有者がオブジェクトのいずれかまたはすべての複製にアクセスすることが現実的でなく、あるいは不可能である場合でさえも、維持される。

【００８４】

好ましい実施形態では、多数のユーザが種々のコンピュータ装置または記憶媒体上で保護データオブジェクトの個々の複製を変更し、それらコンピュータ装置または記憶媒体のいくつかがオンラインではなく、あるいは保護データオブジェクトの所有者によってアクセス不可能である動的、分散的、および協働的な環境において、本発明が保護データオブジェクトの透過的な使用をサポートする方法を説明する。この説明は、本発明が情報の著作者と所有者の区別をサポートすることを明瞭に示す。さらに、本発明はポリシーとデータオブジェクトの結合を攻撃しようと試みる敵対者に対する防御を備えていることも示す。

【００８５】

データオブジェクトを保護すると同時に、ポリシー・モデルの制約内でそれら保護データオブジェクトを生成し、変更し、配布する能力を提供する必要がある、動的、分散的、かつ協働的な環境の例として、投資銀行において銀行家とリサーチ・アナリストの間の情報の明確かつ監査可能な分離を要求する規則であるＮＡＳＤ　２７１１に準拠したデータオブジェクトの管理および保護を望む企業を考える。図２～図５は、そのような動的、分散的、かつ協働的なプロセスにおける仮想の工程を列挙している。

【００８６】

「ＮＡＳＤ　２７１１」のビジネス・プロセス１５０は３つの制御ポリシー１４、すな

わち「バックグラウンド・リサーチ」１５２（図２）、「業界再調査」１５４（図３および４）、ならびに「発行」１５６（図５）を含む。「ＶＰコンプライアンス」が、このビジネス・プロセスを所有し、そのすべての側面を管理する。図２の「バックグラウンド・リサーチ」ポリシー１５２に対して、ＶＰコンプライアンスは、２つのロール、すなわち「アナリスト」および「ディレクター」を設置する。「アナリスト」ロールに挙げられた各人は、「バックグラウンド・リサーチ」ポリシー内でレポートを作成し、読み出しでき、書き込むことができる。「ディレクター」ロールに挙げられた各人は、レポートを読み出すことができ（書き込みはできない）、そのようなレポートの複製を「業界再調査」ポリシー１５４に移すことができる。

【００８７】

図２に示した例は、「ＮＡＳＤ　２７１１」ビジネス・プロセス１５０によって保護および制御される「ビッグ・モーター社（Big Motor Co.）」についてのアナリスト・レポートの生成を示している。図が示すとおり、アナリストは、このポリシー１５２内でレポート（データオブジェクト）に関してドラフトを作成し、協働でき（共同で作成でき）、レポートが完成したとき、それをロール「ディレクター」のメンバーである「リサーチ・ディレクター」に送り、審査し、最終的にコンプライアンスに移す。「バックグラウンド・リサーチ」ポリシー１５２の下でのロールのいずれにも挙げられていない者は、このポリシーによって保護されているレポートにアクセスできない。

【００８８】

図３は、このビジネス・プロセス１５０の動的「業界再調査」部分１５４の最初の部分を示している。「業界再調査」は、３つのロールを有するポリシーを含む。すなわち、「ディレクター」ロールは、このポリシー１５４の保護データオブジェクトを読み出すことができ、データオブジェクトをポリシー１５４内に移すことができる。「コンプライアンス」ロールは、保護データオブジェクトを読み出すことができ、データオブジェクトの複製を「発行」ポリシー１５６（図５）に移すことができ、さらに、「外部再調査者」ロールの構成員を管理できる。「外部再調査者」ロールは、保護データオブジェクトを編集できる。「コンプライアンス」ロールのメンバーである「ＶＰコンプライアンス」は、「業界再調査」ポリシー１５４の「ディレクター」ロールのメンバーである「リサーチ・ディレクター」から保護データオブジェクトを受け取ったとき、「外部再調査者」ロールの構成員を編成して、「ＢＭＣｏの最高財務責任者」および「自動車関連の投資銀行家」が保護されたアナリスト・レポートを監査して編集できるようにする。「外部再調査者」ロールのメンバーらは、協働的な相互活動を行ない、更新したデータオブジェクトを「ＶＰコンプライアンス」に送り返す。次に「ＶＰコンプライアンス」は、図４に示すとおり「ＢＭＣｏの最高財務責任者」および「自動車関連の投資銀行家」を「外部再調査者」ロールの構成員から（したがって、「業界再調査」ポリシー１５４から）削除し、彼らが「業界再調査」ポリシーの下で保護されているレポート（対象のデータオブジェクト）を閲覧できないようにすることができる。このような削除は、本発明の動的な性質の一態様を示している。

【００８９】

図５では、「ＮＡＳＤ　２７１１」ビジネス・プロセス１５０に制約されるビッグ・モーター社アナリスト・レビューの各段階を経てアナリスト・レポートの進行を完了する。図５は、「発行」ポリシー１５６内の３つのロールを示しており、それらはすべて、保護データオブジェクトの読み出しは可能であるが、書き込みはできない。さらに、「コンプライアンス」ロールは、データオブジェクトをポリシー１５６に移すことができ、「ディレクター」ロールは、「閲覧者」ロールの構成員を管理できる。「コンプライアンス」ロールの「ＶＰコンプライアンス」が、アナリストのレポートの複製を「発行」ポリシー１５６に移すとき、「ディレクター」ロールの「リサーチ・ディレクター」が、必要な参加者（例えば、販売グループおよびＢＭＣｏの最高財務責任者）を「閲覧者」ロールに追加し、保護されるアナリスト・レポートを外界から利用可能にする。

【００９０】

図６のブロック図は、本発明の実施形態の主要な構造的な構成要素、およびそれら構造的な構成要素間の主な相互作用を示す。ユーザ２０は権限管理対応アプリケーション２１を使用して、保護データオブジェクト３２を操作する。保護データオブジェクト３２は、暗号化されたデータオブジェクト２２およびタグ２３を含んでいる。実施形態によっては、データオブジェクト３２が暗号化されていなくてもよい。

【００９１】

クライアント・エージェント２６内のリファレンス・モニタ２４が、権限管理対応アプリケーション２１による、保護データオブジェクト３２のデータに対する操作要求を捕捉する。このモニタは、保護データオブジェクト３２のタグ２３を使用し、ユーザ２０に対してこのデータオブジェクト２２を保護するポリシー内の使用権限を得る。クライアント・エージェント２６はポリシー・サーバ２９上のポリシー・マネージャ２７と通信して、タグ２３によって特定されている制御ポリシーの詳細を取得する必要がある。ユーザ２０が要求操作を実行する権限を有すると仮定すると、クライアント・エージェント２６内の暗号エンジン２５が、データオブジェクト２２について要求された操作について適切な暗号化操作を実行する。この操作の実行に必要な暗号鍵は、ポリシー・サーバ２９上の鍵マネージャ２８から、制御ポリシーの要求および応答作用の一部として最初に得られている。

【００９２】

ポリシー・サーバ２９に格納されている制御ポリシーは、適切に許可されたユーザ３０によって、ポリシー・サーバ２９上のポリシー・マネージャ２７と相互作用するポリシー管理アプリケーション３１を使用して、生成および編集される。

【００９３】

特定の実施形態においては、複数のポリシー・サーバを使用できる。複数のサーバは、信頼性の向上および負荷平衡を目的として使用できる。

【００９４】

特定の実施形態においては、クライアント・エージェント２６は、ポリシー・サーバ２９との間で間欠的に接続されていてもよい。本発明は、変更された使用権限について、影響されるデータオブジェクトの複製への適時の伝達をサポートするが、「適時」の定義は、ポリシーの管理を許可されているユーザ３０によって設定される。例えば、特定の商業的状況においては、適時とは、使用権限の変更後のデータオブジェクトへのすべてのアクセスが新しい権限によって管理されることを意味することもある。商業環境が保護データオブジェクトへの制限された「オフライン」アクセスを要求するような別の状況においては、適時とは、権限管理システムのローカル・エージェントがオンラインに復帰したときに使用権限が更新されることを意味することもある。

【００９５】

権限管理対応アプリケーション

図６のクライアント・アプリケーション２１は、ポリシー・サーバ２９上に格納されたポリシーを行使するために、権限管理システムのクライアント・エージェント２６と協働する権限管理対応アプリケーションとして示されている。このような権限管理対応アプリケーションを生成するのに多くの方法が存在する。クライアント・エージェント２６と直接相互作用するようにアプリケーション２１をコード化することができる。あるいは、一式の権限管理ライブラリを標準インタフェースでロードして使用するようにアプリケーション２１をコード化することができる。次いで、クライアント・エージェント２６とのすべての相互作用を管理するこれらの権限管理ライブラリの一バージョンを実装できる。最後に、アプリケーション２１を実行するシステムは、発明の名称「コンテンツ保護エージェントを自動的かつ動的に一体化することによって非認証の使用からデジタル・コンテンツを保護する方法（METHOD FOR PROTECTING DIGITAL CONTENT FROM UNAUTHORIZED USE BY AUTOMATICALLY AND DYNAMICALLY INTEGRATING A CONTENT-PROTECTION AGENT）」のバーラ（Ｂａｌａ）およびスミス（Ｓｍｉｔｈ）による２００２年７月１１日付の米国特許出願第１０／１９４，６５５号に記載のとおり、クライアント・エージェント２６を、権限

管理対応アプリケーションを生成するアプリケーションに挿入できる。前記の米国特許出願は、参照により本明細書に引用したものとする。

【００９６】

一般に、図６に示したようなリファレンス・モニタリングに基づくクライアント中心の処理は、アプリケーションが権限管理システムのトラスト・エージェントとなることを可能にし、したがってクライアント装置が権限管理システムの残りの部分から切断されても、指定された使用権限のローカルな行使を可能にする。動的な投入を採用する実施形態は、既存および新規のアプリケーションを即座に、権限管理システムに組み込むことを可能にする。

【００９７】

ポリシーおよびポリシー管理

以下に説明する実施形態においては、制御ポリシー１４は、ポリシーによって保護データオブジェクトへのアクセスが許可されているユーザの少なくとも１つのリスト、この許可リスト内の各ユーザに与えられた権限のダイジェスト、現在の鍵暗号鍵（ＫＥＫ）、および固有の識別子（すなわち、タグ２３に使用されているポリシーＩＤ）を含む。さらに、制御ポリシー１４は、これらの特権についての条件を含むことができ、それら条件は、追加の装置、場所、アクセス時間、またはネットワーク接続の制約を指定できる。

【００９８】

本発明は、（前述の）ポリシーによって保護されたデータオブジェクトへのアクセスを許可されているユーザ２０の集合と、制御ポリシーおよび周囲のビジネス・プロセスを管理（すなわち、生成、編集、および削除）するユーザ３０の集合とを区別する。なお、ユーザは両方のユーザ集合２０、３０のメンバーであってもよい。

【００９９】

企業のビジネス・プロセスのニーズに、より適切に対処するために、好ましい実施形態は３つの明示的な種類の管理者ユーザ、すなわち情報技術（ＩＴ）管理者、ビジネス・プロセス所有者、およびビジネスロール管理者をサポートする。ＩＴ管理者は、図６のポリシー・サーバ２９への管理アクセスを有しているユーザである。彼らの役目は、ポリシー・サーバが必要とするコンピュータ・インフラを維持することにあり、ＩＴ管理者は、ポリシー管理のビジネス関連の管理的側面については実行する必要はない。ビジネス・プロセス所有者は、特定のビジネス・プロセスを管理する権限を有するユーザである。ビジネス・プロセス所有者は、所有しているビジネス・プロセス内の制御ポリシー１４のすべての側面を編集できるが、他のビジネス・プロセスを変更することはできない（このユーザが、それら他のビジネス・プロセスのビジネス・プロセス所有者である場合を除く）。ビジネスロール管理者は、特定の制御ポリシー１４のロール内のユーザのリストを変更できるユーザである。ビジネスロール管理者は、ビジネスロール管理者が指名されたビジネス・プロセスのビジネス・プロセス所有者に与えられる特権の一部を有する。

【０１００】

企業のビジネス・プロセスのカテゴリー化をさらに容易にし、ビジネス・プロセス管理の階層的特性を直接的に反映するために、好ましい一実施形態は、定義されたビジネス・プロセスの階層的方式での体系化をサポートする。例えば、ツリーとして体系化されたビジネス・プロセスの集合を考える。ツリーの根にあるビジネス・プロセスは、最上位の環境を表わしており、ツリーの葉にあるビジネス・プロセスは、根にあるビジネス・プロセスの個々の構成要素である。付加的な内部ツリー・ノードを用いて、ビジネス・プロセス全体内の主要なカテゴリーを表わすことができる。

【０１０１】

ツリーとして体系化されたこのような階層構造を用いて、階層構造のサブツリー内のビジネス・プロセスのすべてを管理できるユーザを指定できる。同様に、指定されたユーザは、サブツリー内のロールのみを管理できる。

【０１０２】

図７は、図６のポリシー管理アプリケーション３１のロジックを示している。このプロ

セスは、ステップ４０で始まり、ここで、ユーザはポリシー管理アプリケーション３１を開始し、ポリシー・サーバ２９に接続する。一実施形態においては、ポリシー管理アプリケーション３１は、Ｊ２ＥＥウェブ・アプリケーションである。ステップ４１において、システムは、ユーザが許可された管理者であることを確認し、ユーザがどの種類の管理者であるかを特定し、ユーザがポリシー・データベースについて実行できる操作の種類を決定する。ユーザが、いずれのアクションの実行も許可されず、あるいはデータベースを閲覧することも許可されていない場合、ステップ４２においてエラーメッセージが表示される。ステップ４３は、ビジネス・プロセス、それらの制御ポリシー、および許可ユーザが許可されたロールの表示を提示するが、この表示は許可ユーザの権限に応じて決まる。次いで、ステップ４３は、ユーザがビジネス・プロセスのデータベースを変更するアクションを選択するのを待つ。

【０１０３】

許可ユーザは、ステップ４４に示されているとおり、ビジネス・プロセス、制御ポリシー１４、またはロールリストの生成もしくは編集を選択できる。ユーザによって実行された変更はすべて、ステップ４６において記録され、確定される。次いで、この変更が、ステップ４３においてユーザに表示される。

【０１０４】

変更を記録することによって、システムは、許可ユーザがポリシー・サーバ２９上のデータベースに関する先の変更を取り消すことを可能にする。詳細には、ステップ４３はさらに、ステップ４５に示されているとおり、ユーザが確定された一式の変更を元の状態に復帰させることを可能にする。このアクションも、ステップ４６において記録および確定される。ステップ４３～４６は、ユーザがポリシー管理アプリケーション３１を出るまで繰り返される。これらのステップはすべて、ポリシー・サーバ２９上の変更されたビジネス・プロセスおよびポリシーによって保護される正確なデータオブジェクトにアクセスすることなく、またそれらデータオブジェクトについての認識なしで、実行できる。

【０１０５】

セキュリティ・ノブ（security knob）

本発明の好ましい一実施形態は前記ロールバック（元の状態に復帰）機能を用いて、動的に有効または無効にできるワンクリックのセキュリティ設定を実現できる。このワンクリックのセキュリティ設定を、俗称でセキュリティ・ノブと称する。

【０１０６】

最も単純な場合においては、２つのセキュリティ警報、すなわち通常および停止を有するビジネス・プロセスを考える。「通常」はデフォルトのセキュリティ状態であり、企業は、このビジネス・プロセスの通常の日々のワークフローにおいて行使されるポリシーの範囲外の特別な考慮を払うことなく手続きを進める。ビジネス・プロセスが「攻撃下」にあり、あるいは脆弱である（例えば、特定され割り出された敵対者に対して脆弱であり、あるいは特定の重大な時間期間において政府規制の潜在的侵害について脆弱である）際には、このビジネス・プロセスが効果を発揮するように、セキュリティ担当者およびビジネス・プロセス所有者は共にこのビジネス・プロセスへの一式の変更を決定する。ビジネス・プロセスの適切な一部に適用されると、これらの一式の変更は、システム「停止」のセキュリティ状態になる。

【０１０７】

この形態の主要な側面は、企業またはビジネス・プロセス所有者が、この「停止」のセキュリティ状態に即座に、かつ一時的な時間期間だけ入りたいと望む可能性があるという点にある。脅威または無防備状態が過ぎ去ると、システムは、「通常」のセキュリティ状態に対して定義されたポリシー特徴に復帰すべきである。企業またはビジネス・プロセス所有者が「停止」のセキュリティ状態に入るか、または出ることを望むたびにビジネス・プロセスの各部分を編集するのでは、低速になり、エラーが発生しやすく、時間を要するであろう。

【０１０８】

この能力を実現するため、一実施形態は、セキュリティ・ノブが所定の設定にされたときに自動的に適用される一式のログ・イベントを生成する。前記「停止」のセキュリティ状態のログ・イベントは、許可された管理者に現在のビジネス・プロセス（すなわち、「通常」のセキュリティ状態）への変更を単に実行させ、システムにそれらの変更を適切なセキュリティ設定識別子（すなわち、「停止」）の下で記録および格納させ、さらにそれらの変更を決定した時点においては実際にデータベースに適用しないことによって、捕捉できる。「停止」から「通常」への移行のためのログ・イベントは、単に「停止」変更からの復帰に使用される。

【０１０９】

セキュリティ設定の整合性を保つため、システムはユーザに対し、例えば許可ユーザが「通常」のセキュリティ状態にあるビジネス・プロセスについて変更を行なっているときに、さらに「停止」のセキュリティ状態を変更したいと望むか否かを問う。

【０１１０】

この２設定のセキュリティ・ノブの例および具体化を、２よりも大きい任意の特定のｎについて、ｎ個の設定を有するセキュリティ・ノブを実現する事例に拡張する方法は、当業者であれば理解できるであろう。

【０１１１】

ポリシー削除

ポリシーが変更されるとき、システムは制御ポリシー１４によって保護されるデータオブジェクト３２のすべてにアクセスできないため、制御ポリシーを「削除する」際には注意する必要がある。第１に、「削除された」ポリシーによって保護されるあらゆるデータオブジェクト３２は、その後に新しい制御ポリシーの一部となり現れるため、新しいポリシーの代わりに「削除された」制御ポリシーからの制御ポリシー識別子を再使用することはできない。さらに、特定の特権ユーザが「削除された」制御ポリシーからデータオブジェクトを回復できることが望まれることもある。

【０１１２】

好ましい実施形態においては、制御ポリシー１４についての識別子として、完全に固有の識別子（ＧＵＩＤ）を使用して、２つの制御ポリシー１４が決して同一識別子を得ることがないようにする。許可された管理者ユーザが制御ポリシーを削除するとき、システムは制御ポリシーをシステムから削除し（おそらくは、このアクションおよび削除された情報を記録する）、「削除された」制御ポリシーによって保護されるデータオブジェクトが、ユーザによるアクセスが許可されないデータオブジェクトとして現れるようにする。保護データオブジェクトの回復は、後述する「災害時回復」機構によりなされる。

【０１１３】

暗号化および制御ポリシー・タグ（ＣＰＴ）

データオブジェクト２２全体にわたる継続的な保護および管理を保証するために、本発明の好ましい実施形態は、権限管理対応アプリケーションによってアクセスされていないときに、データオブジェクト２２を暗号化する。暗号化データオブジェクト２２のそれぞれに対し、システムは、制御ポリシー・タグ（ＣＰＴ）を付ける。図８は、図６の保護データオブジェクト３２の制御ポリシー・タグ２３の抽象的な表示である。ＣＰＴは、データオブジェクト２２を暗号化するのに使用されるコンテンツ暗号鍵（ＣＥＫ）を含んでいる（ＣＰＴの全フィールドについては、後述する）。ＣＰＴは、権限管理システムにおけるポリシーをデータオブジェクトに関連付ける機構でもある。暗号化された（または、暗号化可能な）データオブジェクト２２とそのＣＰＴの組み合わせは、保護データオブジェクト３２と呼ばれる。

【０１１４】

各データオブジェクト２２について、権限管理システムは擬似乱数を生成し、この疑似乱数を、データオブジェクト２２を暗号化および復号化するための対称鍵として使用する。このプロセスは、各データオブジェクトの固有ＣＥＫを効果的に生成する。図８の制御ポリシー・タグ２３は、識別情報、暗号化情報、および完全性情報を提供するフィールド

を備えるデータ構造である。フィールドは、任意の順序で現れることができるが、クライアント・エージェント２６は常に、ＣＰＴのバージョン・フィールド５１および長さフィールド５２を見出し解釈できなければならない。

【０１１５】

バージョン・フィールド５１は、使用されているＣＰＴ構造のバージョンを特定する。このフィールドにより、システム設計者は、将来的にＣＰＴのフォーマットまたはコンテンツを変更でき、さらに古いＣＰＴ構造ならびに新しいＣＰＴ構造によって保護されたコンテンツにアクセスできる（図１４および以下の関連説明を参照）。

【０１１６】

バージョン・フィールド５１は、コンテンツ・フィルタリング・アプリケーションがデータオブジェクト３２を本発明により暗号化され保護されたものとして識別するのに使用できる、「マジック・ナンバー」で開始できる。この「マジック・ナンバー」は、例えば、保護データオブジェクト３２が暗号化されていること（さらに、暗号化前のスキャンによりウイルスを含まないと予測される）を知るためのウイルス対策スキャン・アプリケーションによって使用できる。

【０１１７】

長さフィールド５２は、ＣＰＴのサイズをバイトで指定している。

【０１１８】

テキスト・メッセージ・フィールド５３は、無許可ユーザ（または、権限管理システムの制御の下にないプログラムを実行しているユーザ）に、添付のデータオブジェクト３２が保護されていること、およびどこでさらに詳しい情報を得ることができるのかを説明するオプション・フィールドである。このフィールドは任意であり、実施形態によっては、操作の容易性（ユーザに、権限管理システムの一部となることができる方法を知らせる）よりも機密性を高めること（無許可ユーザには情報を提供しない）を選択できる。

【０１１９】

制御ポリシーＩＤフィールド５４は、添付のデータオブジェクトを保護する制御ポリシー１４を特定する。このフィールドは、完全な固有の識別子（ＧＵＩＤ）を含んでいる。さらに、制御ポリシーＩＤフィールド５４は、そのネーム空間内でＧＵＩＤが知られているポリシー・サーバ２９を指定（例えば、ＵＲＬによって）することができる。

【０１２０】

オブジェクトＩＤフィールド５５もオプション・フィールドであり、各データオブジェクト２２について固有識別子を指定する。

【０１２１】

保護データオブジェクト３２はそれぞれ、コンテンツ暗号化鍵（ＣＥＫ）と呼ばれる秘密鍵によって暗号化され、この鍵はＣＰＴ構造２３内の少なくとも２つの場所、すなわち暗号化ＣＥＫ５６および５７と記された場所に格納されている。これら２つのフィールド５６、５７のうちの一方は、ポリシー・サーバのＫＥＫで暗号化されたＣＥＫを含む。他方のフィールドは、制御ポリシーＩＤフィールド５４内で特定されたポリシーの鍵暗号鍵（ＫＥＫ）で暗号化されたＣＥＫを含む。ＫＥＫは、対称鍵であっても、非対称鍵であってもよい。好ましい実施形態についての説明の残りの部分では、ＫＥＫが公開鍵／秘密鍵の対を含むと仮定する。

【０１２２】

別の実施形態は、ロールに基づくＫＥＫをサポートする追加のＫＥＫフィールドを含むことができる。このような方法では、管理者は、特定のロールについて固有の鍵特性（例えば、短いオフライン・アクセスなど）を指定できる。

【０１２３】

本発明の実施形態は１つまたは複数の異なるコンテンツ暗号化アルゴリズムを使用できるため、暗号化アルゴリズムＩＤフィールド５８は、データオブジェクトをＣＥＫで暗号化するのに用いられる実際のアルゴリズムおよび別の定義可能な特性（例えば、鍵長さ）を特定する。

【０１２４】
最後のフィールドである完全性チェック・フィールド５９を用いて、何者もＣＰＴ２３内のフィールドを改ざんしていないことを保証する。完全性チェック・フィールド５９には、例えば、ＣＰＴ全体のセキュア・ハッシュを含む。
【０１２５】
データオブジェクトが、タグ付けされているが暗号化はされていない場合、２つの暗号化ＣＥＫフィールド５６および５７ならびに暗号化アルゴリズムＩＤフィールド５８はゼロにされる。
【０１２６】
制御ポリシー１４は、保護データオブジェクト３２の不可欠な部分と考えられ、コンピュータおよびそれらの内部構造体（例えば、ファイルシステムおよびメモリバッファ）の間を移動するときでさえも、データオブジェクトに付随している。ＣＰＴは、制御ポリシーＩＤフィールド５４によって管理している制御ポリシーを参照し、また制御ポリシーのＫＥＫにより保護されるＣＥＫを含んでいるが、本発明の権限管理システムの実施形態によって、許可ユーザがＣＰＴを明示的に削除しない限り、暗号化データオブジェクト２２とともに伝達される。
【０１２７】
本発明の明確な結論は、複数のデータオブジェクト３２が単一の制御ポリシー１４により、参照可能となり、かつ保護されることである。前述のＣＰＴ構造は、明らかにこの結論を裏付けている。さらに、この実施形態は、ＣＰＴの制御ポリシーＩＤフィール５４内の値が文書を一意に特定しない（これは固有の文書識別子と異なる）ことに重点をおいている。
【０１２８】
図６のポリシー・サーバ２９は、制御ポリシー１４の詳細のみを格納し、データオブジェクト３２と制御ポリシー１４との間の関連付けは格納しない。このデータオブジェクトと制御ポリシーとの間の関連付けは、保護データオブジェクト３２のＣＰＴ２３にのみ格納される。この構成は、ポリシー１４用に設けられたポリシー・サーバ２９の記憶領域が、定義される制御ポリシー１４の数に比例して拡大縮小することを意味している。ポリシー・サーバの記憶領域は、個々の保護データオブジェクトの数に影響されない。それら保護データオブジェクトの複製の数にも影響されない。
【０１２９】
本発明の好ましい実施形態は、データオブジェクト３２の前に配置されたＣＰＴ２３を備える（すなわち、保護データオブジェクト３２のスキャンがこの保護データオブジェクトの第１バイトから開始されるときに、データオブジェクトよりも先にＣＰＴを検知する）。他の実施形態においては、ＣＰＴを保護データオブジェクト３２の末端、または他の任意の明確な位置に置くことができる。
【０１３０】
好ましい実施形態により、図６のポリシー・サーバ２９およびクライアント・エージェント２６の両者がＣＰＴ２３を構築できる。
【０１３１】
リファレンス・モニタリング
図９は、保護データオブジェクト３２へのアクセス操作において、図６のリファレンス・モニタ２４が従うロジックを示す。ある特定の操作が行われると、まずステップ６１においてリファレンス・モニタ２４は、その操作が保護データオブジェクト３２にアクセスする操作であるか否かを判断する。このチェックは、データオブジェクト上のＣＰＴ２３を探索することを含む。ＣＰＴが存在しない場合、リファレンス・モニタ２４は、ステップ６２においてアプリケーション２１の続行を許可する。ＣＰＴ２３が存在する場合、ステップ６３においてモニタ２４は、ＣＰＴのバージョン・フィールド５１をチェックし、ＣＰＴのバージョンが現在のバージョンであるか否かを判断する。ＣＰＴ２３が存在しない場合、リファレンス・モニタはステップ６４に進む。ステップ６４については図１４で

説明する。

【０１３２】

モニタ２４がＣＰＴ２３を解釈できる場合、モニタは進行し、ステップ６５において、フィールド５９（図８）によりＣＰＴの完全性をチェックする。ＣＰＴが改ざんされている場合、モニタ２４は、ステップ６６においてエラーメッセージを表示し、改ざんが無い場合、この保護データオブジェクト３２についてのユーザの使用権限を決定するために、ステップ６７においてＣＰＴ内の制御ポリシーＩＤ（図８のフィールド５４）をユーザの認証信任状とともに使用する。一式の使用権限が決定されると、ステップ６８においてモニタは、そのユーザが要求した操作を実行することを許可されているか否かを判断する。許可されていない場合、ステップ６９においてモニタ２４は、アプリケーション２１が要求された操作を実行することを禁止し、適切なエラーメッセージを表示する。

【０１３３】

ユーザが、対応する（関連付けられた）制御ポリシー１４の下で複数のロールに登場する場合、好ましい実施形態は、そのユーザを含むロールのそれぞれについての使用権限を集約する。この集約によって、ユーザの個々のロールの明確な権利をすべて含む一式の使用権限が得られる。明らかに、別の実施形態においては、別の集約方法を用いることができる。

【０１３４】

操作が許可される場合、ステップ７０においてモニタ２４は、ＣＰＴで特定される制御ポリシー１４のＫＥＫを使用し、対象の保護データオブジェクト３２のコンテンツを暗号化および復号化するのに用いられたＣＥＫを復号化する。特定の実施形態におけるステップ７０の処理の間に発生する可能性のある、いくつかの例外的な状況は、以下のＣＰＴ更新および災害時回復に関連するセクションで説明される。

【０１３５】

最後に、復号化されたＣＥＫが得られると、ステップ７２においてモニタ２４はこのＣＥＫを使用して、読み出し操作時に暗号化されたコンテンツを復号化するか、あるいは書込み操作時に新しいコンテンツを暗号化する。

【０１３６】

クライアント・エージェント２６のアーキテクチャ

図１０は、本発明のクライアントのアーキテクチャの好ましい実施形態の詳細を示している。この実施形態は、図６のクライアント・エージェント２６を、クライアント・ハンドラ・プロセス８２および統合バンドル８４に分割している。ユーザ装置ごとに、クライアント・ハンドラ・プロセス８２が１つずつ存在している。統合バンドル８４は、ユーザの装置上で動作している各プロセス内にロードされる単一のダイナミック・リンク・ライブラリとして実現できる。統合バンドル８４は、リファレンス・モニタ８３および暗号エンジン８５を含み、両者は図６においてすでに述べた２４、２５に相当する。

【０１３７】

クライアント・ハンドラ・プロセス８２は、図６のポリシー・サーバ２９のローカル・プロキシとして動作する。クライアント・ハンドラ・プロセス８２は、図６のポリシー・マネージャ２７から受け取る制御ポリシー１４をキャッシュし管理するポリシー・サービスおよびキャッシュ８６と、図６の鍵マネージャ２８からのＫＥＫを確実にキャッシュし管理する鍵サービスおよびキャッシュ８７とを含む。

【０１３８】

この実施形態では、リファレンス・モニタ８３は、保護データオブジェクトのＣＥＫをそのＣＰＴから抽出する（図９のステップ７０）ために、クライアント・ハンドラ・プロセス８２内の鍵サービスおよびキャッシュ８７にポリシーＫＥＫを要求する。ＣＥＫが得られると、統合バンドル８４は自身のメモリからＫＥＫを取り消し、ＣＥＫを暗号エンジンに送る。

【０１３９】

クライアント・ハンドラ・プロセス８２はさらに、各統合バンドル８４からログ情報を

収集し、そのログ情報を最終的に図６のポリシー・サーバ２９に送り返す、ログ・サービス８８を含む。

【０１４０】

図１１は、図１０のクライアント・ハンドラ・プロセス８２が従うロジックを示している。このハンドラは、ステップ９０の出力端に表記されているいくつかのイベントのうちの１つを待機するイベント・ループ内にある。新しいユーザがクライアント装置にログインし、本人であることを立証すると、クライアント・ハンドラ・プロセス８２は、ステップ９１に記されているとおり、そのユーザに関するポリシー・サーバ２９上のすべてのポリシー１４を要求する。ステップ９２では、クライアント・ハンドラ・プロセス８２は、一定のポーリング間隔で、ログイン・ユーザに関する新たなポリシー１４について、あるいはキャッシュしたポリシー１４の変更について、ポリシー・サーバ２９をチェックする。

【０１４１】

いくつかの制御ポリシー１４は、それらをどれだけ長くキャッシュでき、オフラインで使用できるかを記載している。そのようなポリシーが時間切れになったとき、ステップ９３においてハンドラ・プロセス８２は、期限切れしたポリシー１４をポリシー・サーバ２９から再度取り出す。制御ポリシーＫＥＫも期限切れになる可能性があり、この期限切れ状態に対する実施形態の取り扱いは、以下で「期限切れＫＥＫおよびＣＰＴ更新」と表記されたセクションで説明される。

【０１４２】

好ましい実施形態は、このとき、３段階切替トグル（基本、標準、および高と記されている）を実装し、制御ポリシーＫＥＫの有効期間およびキャッシュ時間切れ値を設定する。ポリシーＫＥＫの有効期間およびキャッシュしたポリシーの時間切れまでの時間の長さは、「低」設定では「中間」設定よりも長い。これにより、ＫＥＫが損なわれるか、あるいは制御ポリシーが変更される場合により大きな危険性をもたらす。「高」設定は、最も高いレベルのセキュリティ、したがって最も低いレベルの危険性をもたらす。これはまた、ユーザがオフラインで作業できる時間期間がより短いことを意味する。本発明の実施形態のそれぞれは、制御ポリシーＫＥＫ有効期間およびキャッシュ時間切れ値を、それらのリスク許容レベルおよび保護データオブジェクト３２のオフライン使用の必要性に応じて選択する。

【０１４３】

最後に、ポリシー・サーバ２９は、ステップ９４に記されているとおり、オンラインのクライアントのハンドラ・プロセス８２に対し、それらがキャッシュしているポリシーを削除して、リフレッシュするように促すことができる。オフラインのクライアントは、それらがキャッシュしているポリシー記憶を、再度接続したときにポリシー・サーバ２９と同期させる。

【０１４４】

ステップ９１～９４については、クライアント・ハンドラ・プロセス８２はステップ９５で、必要なネットワーク通信が形成されたことを確認するチェックを行なう。すべてに問題がない場合、ハンドラ・プロセス８２はステップ９６において、受け取った制御ポリシー１４を安全な記憶装置にキャッシュする。クライアントが、ポリシー・サーバ２９とのネットワーク接続を有していなかった場合、ステップ９７においてハンドラ・プロセス８２は、その失敗したイベントを記録し、後にネットワーク接続が回復した後にステップ９８および９９で再実行する。

【０１４５】

期限切れＫＥＫおよびＣＰＴ更新

保護データオブジェクト３２のＣＰＴ２３は、本発明における唯一の構造体であり、データオブジェクト３２を暗号化するのに用いられるＣＥＫを含む。先に述べたとおり、ＣＥＫは、図８の制御ポリシーＩＤフィールド５４で特定される制御ポリシー１４のＫＥＫで暗号化されている。ＫＥＫが有効でなくなることに伴うリスクを抑えるために、本シス

テムは、そのような暗号鍵の寿命を制限する。しかし、これは制御ポリシーＫＥＫが期限切れになると、フィールド内の保護データオブジェクト３２にアクセスできなくなることを意味する。ポリシーのＫＥＫが期限切れになったとき、システムは制御ポリシー１４によって保護されるすべてのデータオブジェクトへのアクセスを持たないため、期限切れしたＫＥＫによって保護されるデータオブジェクトへのアクセスを可能にし、最終的には、遅れてそれらデータオブジェクトのＣＰＴ２３を制御ポリシーの現在のＫＥＫで更新可能にする機構を有する必要がある。

【０１４６】

図６のポリシー・サーバ２９は、各制御ポリシーＫＥＫの寿命の定義および管理を担当する。

【０１４７】

本発明の好ましい実施形態は、制御ポリシー１４内の各ＫＥＫに固有の識別子を割り当てる。ポリシー・サーバ２９は、鍵マネージャ２８を使用して、アクティブな制御ポリシー１４のそれぞれについて現在のＫＥＫを格納し、ＫＥＫの履歴を保持する。この履歴は、制御ポリシー１４についてこれまでに生成されたすべてのＫＥＫを含むことができ、あるいはポリシー１４について最も新しく期限切れしたＫＥＫを限定数だけ含むことができる。

【０１４８】

図６のクライアント・エージェント２６が、保護データオブジェクト３２のＣＥＫを復号化するための正しいＫＥＫを有するか否かを決定できるようにするために、図８の暗号化ＣＥＫフィールド５６および５７は、ＣＥＫを暗号化するのに使用されるＫＥＫ固有の識別子の（平文の）値を含む。許可ユーザのクライアントが、保護データオブジェクト３２のＣＥＫを復号化するのに必要なＫＥＫを有している確率を高めるために、本発明の好ましい実施形態（例えば、ポリシー・サーバ２９）は、制御ポリシー１４の現在のＫＥＫだけでなく、制御ポリシーのＫＥＫについて最も新しく格納された履歴の一部分も、クライアント・エージェント２６に配布する。配布される履歴の長さは、鍵マネージャ２８によってポリシー・サーバ２９上に保持されている履歴の長さよりも短いか、あるいは等しい。

【０１４９】

次に、期限切れの制御ポリシーＫＥＫによって暗号化されたＣＥＫによって保護されるデータオブジェクト３２にアクセスする試みについて、２つの事例を考える。さらに、後のセクションの表題「災害回復およびＣＰＴバージョン管理」についての事例を考える。この事例は両方共、ポリシー・サーバ２９が期限切れのＫＥＫについて完全な履歴を維持すると共に、最も新しく期限切れとなった鍵のうちの限定された数のみをクライアント・エージェント２６に配布していると仮定する。ポリシー・サーバ２９が期限切れになったＫＥＫの完全な履歴をすべてのクライアント・エージェント２６に配布することは、現実的でない。図１２は、現在および過去の３つの期限切れＫＥＫ１２５をクライアント・エージェント２６に配布する実施形態についてのシナリオを説明しており、この図は、ＫＥＫが鍵の対１２１ａ、ｂを含むと仮定している。

【０１５０】

第１の事例においては、期限切れの制御ポリシーＫＥＫが、配布された履歴内のサーバ２９によって送られた制御ポリシーＫＥＫのうちの１つである場合は、クライアント・エージェント２６は、ＣＥＫを復号化し、このＣＥＫを用いて保護データオブジェクト３２にアクセスし、制御ポリシーの現在のＫＥＫを使用する保護データオブジェクト３２について新しいＣＰＴを生成できる。これはすべて、ユーザが介入することなく、かつポリシー・サーバ２９と通信も行なうことなくなされ、したがってクライアントがオフラインである場合でも実現する。

【０１５１】

第２の事例は、期限切れのＫＥＫがクライアント・エージェント２６に配布された履歴の一部ではない問題を解決する。この状態から回復するには、ポリシー・サーバが保護デ

ータオブジェクト３２の制御ポリシー１４に関する期限切れＫＥＫの完全な履歴を保持しているため、クライアント・エージェント２６はオンラインになって、ポリシー・サーバ２９と通信可能にならなければならない。好ましい実施形態においては、単に、クライアント・エージェント２６が対象の制御ポリシー１４の特定の期限切れのＫＥＫを要求するだけである。ポリシー・サーバ２９は、保存されている適切なＫＥＫで応答すると、クライアントは前述のとおりに（期限切れのＫＥＫを配布された履歴内で見出す場合と同様に）続行する。

【０１５２】

さらに、図１２は、現在のＫＥＫの期限切れのために、制御ポリシー１４が現在のＫＥＫを有していない時間が存在する可能性を示している。本発明の好ましい実施形態は、クライアント・エージェント２６がユーザごとの使用ルールおよび制御ポリシーの現在のＫＥＫを要求したとき（図１１のステップ９１）にのみ、ポリシーについての新しいＫＥＫを生成する。クライアント・エージェント２６が、図１１のステップ９１が完了するのに極めて長時間待たなくてもよいようにするために、ポリシー・サーバ２９は、あらかじめ生成した一式のＫＥＫをキャッシュする。このＫＥＫのキャッシュを使用して、現在のＫＥＫを有さない制御ポリシー１４に対するクライアント・エージェント２６の要求に応じ、新たな現在のＫＥＫの要求を満足させる。あらかじめ生成されるＫＥＫのキャッシュは、当業者にとって公知である単純な高低ウォーターマーク方式によって管理される。好ましい実施形態におけるこの手法は、ポリシー・サーバ２９が、長期間無活動である保護データオブジェクト３２を有する制御ポリシー１４について保存する必要がある、多数の未使用のＫＥＫを生成しないことを保証する。

【０１５３】

保護データオブジェクトの持続性モデル

本発明は、保護データオブジェクト３２の２つの明確な持続性モデルをサポートする。一般に、制御ポリシー１４の保護データオブジェクト３２は、永久的または一時的な資産のいずれかであると考えられる。

【０１５４】

「永久」モデルにおいては、制御ポリシー１４内の保護データオブジェクト３２は、保護され、失われてはならない永久的資産であると考えられる。好ましい実施形態では、各保護データオブジェクト３２のＣＥＫをポリシー・サーバ２９の公開マスターＫＥＫで暗号化することによって、このモデルを実現する。この暗号化された値が、暗号化ＣＥＫフィールドの一方に（例えば、図８のフィールド５６）格納され、他方のフィールド（図８のフィールド５７）は、図８のフィールド５４内で特定された制御ポリシーの現在のＫＥＫで暗号化されたＣＥＫを含む。

【０１５５】

表題「災害時回復およびＣＰＴバージョン管理」の次のセクションは、好ましい実施の形態が、秘密マスター鍵を使用して、保護データオブジェクト３２のＣＥＫを常に回復できる方法を説明している。ここでは、マスターＫＥＫの有効期限が通常は制御ポリシーＫＥＫに割り当てられるそれよりも長いという点を除き、ポリシー・サーバ２９のマスターＫＥＫもまた有効期限を有しているとだけ述べておく。有効期間は、次のセクションで説明するとおり、マスターＫＥＫの秘密部分がクライアント・エージェント２６に配布されることがない（すなわち、ポリシー・サーバ２９においてのみ使用される）ため、より長くすることができる。マスターＫＥＫが有効期間を有しているため、好ましい実施形態は、同様に固有の識別子をポリシー・サーバ２９の生成されたマスターＫＥＫのそれぞれに関連付け、この識別子が、図８のフィールド５６に暗号化ＣＥＫと共に格納される。したがって、図８のフィールド５６および５７の格納場所に格納されるコンテンツは、同一である。

【０１５６】

「一時」モデルにおいては、制御ポリシー１４内の保護データオブジェクト３２は、ある所定の時間期間にわたって保護されなければならず、その後に破壊する必要がある一時

的資産であると考えられる。「破壊される」とは、保護データオブジェクト３２の平文を回復することが理論的に不可能であることを意味する。

【０１５７】

好ましい実施形態は、ＣＰＴ２３内のＣＥＫを、ポリシー・サーバのマスターＫＥＫで暗号化するのではなく、「ポリシー・マスター」ＫＥＫ（図８のフィールド５６）で暗号化することによって、「一時」モデルを実現する。システムが保護データオブジェクト３２のＣＥＫをサーバのマスターＫＥＫで暗号化することはない。ポリシー・マスターＫＥＫは、サーバ・マスターＫＥＫと同一の属性をすべて有している（例えば、極めて長い有効期間を有しており、サーバ２９を離れることがなく、それが保存されている限りＣＥＫの回復をサポートする）。

【０１５８】

一時ポリシーの所有者は、そのポリシー１４に関連するすべてのデータオブジェクトを永久的に破壊すべき時であると判断したとき、単にそのポリシーに関連するポリシー・マスターＫＥＫの記録されているすべての複製をポリシー・サーバ２９上において削除するように要求するだけでよい。

【０１５９】

災害時回復およびＣＰＴバージョン制御

本発明の実施形態が保護および回復しなければならない多くの種類の災害（例えば、ポリシーの記憶の喪失およびバックアップからのこの記憶の回復）が存在する。このセクションでは、本発明の災害時回復機構の２つの特有の側面に焦点を当てる。第１は、制御ポリシーＫＥＫについて限られた履歴のみを維持する（あるいは、ある種の破滅的な事象によって、１つまたは複数の制御ポリシー１４について保存されたＫＥＫのすべてが失われた）実施形態に関する。第２は、ＣＰＴフォーマットの上位および下位互換性に関する、本発明によるサポートを説明する。この形態は、企業のセキュリティ空間の動的な特性に対処し、何年にもわたって参照されていない可能性のある保護データオブジェクト３２のＣＰＴ２３内に格納されているＣＥＫをシステムが常に回復できることを保証するために、やはり必要である。

【０１６０】

図１３は、図９のステップ７０において図６のリファレンス・モニタ２４が従うロジックの拡張である。ここで、モニタ２４は、保護データオブジェクト３２（図６）のＣＥＫをＣＰＴ２３（図６）から取り出すことを試みる。クライアント・エージェント２６は、対象の制御ポリシー１４について、現在のＫＥＫおよび期限切れしたＫＥＫのいくつか（ゼロでもよい）を、すでに有している。モニタ２４は、現在のＫＥＫの固有の識別子を、ＣＥＫの暗号化に使用されたＫＥＫの固有の識別子（図８のフィールド５７に保存されている）と比較する（ステップ１１０）。識別子が一致すると、モニタ２４は、図１３のステップ１１５に記載のとおり、暗号化されたＣＥＫの復号化に進む。

【０１６１】

前述のとおり、制御ポリシーのＫＥＫは期限切れになる可能性があり、この実施形態は、その発生を、格納されたＫＥＫの固有の識別子のいずれもがＣＥＫの暗号化に使用されたＫＥＫの固有の識別子と一致しないことを検知することによって特定する。回復のために、ステップ１１１において、モニタ２４がＣＰＴを抽出し、それをポリシー・サーバ２９に、ＣＥＫを現在のポリシーＫＥＫで暗号化するように求めるサーバへの要求と共に送信する。ステップ１１２においてサーバ２９は、暗号化ＣＥＫと共に格納されている固有の識別子によって示されているとおり、適切なマスターＫＥＫ（サーバまたはポリシー）を使用することによってＣＥＫを回復する。ステップ１１３においてサーバ２９は、更新されたＣＰＴをクライアント・エージェント２６に送り返す。ステップ１１４においてクライアント・エージェント２６は、受け取ったＣＰＴからＣＥＫを取り出し、新しいＣＥＫを生成し、それを更新されたＣＰＴに加え、さらに、保護データオブジェクト３２が読み出し専用と表記されておらず、あるいは読み出し専用媒体に格納されていない場合、元のＣＰＴ２３を置き換え、更新されたＣＰＴを使用してステップ１１５に進む。クライア

ントは、データオブジェクト３２に読み出し専用と表記されている場合、取り出したＣＰＴをキャッシュしてもよい。

【０１６２】

好ましい実施形態は、ＣＰＴフォーマットのバージョン変更を、災害時回復問題として取り扱う。この手法により、この実施形態では、現在のＣＰＴフォーマットを解釈する方法、および災害から回復する方法のみを知るコードを、クライアント・エージェント２６に配布できる。

【０１６３】

図１４は、図６のリファレンス・モニタ２４が図９のステップ６４に達したときに従うロジックを説明している。モニタ２４は、保護データオブジェクト３２（図６）のＣＰＴ２３（図６）のバージョンがモニタ２４のサポートするＣＰＴのバージョンと一致しないときに、このロジックに達する。ステップ１００においてクライアント・エージェント２６内のリファレンス・モニタ２４は、保護データオブジェクト３２からＣＰＴ全体を取り出す。ステップ１０１においてクライアント・エージェント２６は、取り出したＣＰＴをポリシー・サーバ２９に、ＣＰＴをクライアント・エージェント２６のサポートする指定のバージョンに変換することを求める要求と共に送る。ステップ１０２においてサーバ２９は、ＣＰＴのバージョン・フィールド５１を使用して、適切なコンバータ・ルーチンを選択し、このコンバータ・ルーチンが、単純に所定のバージョンのＣＰＴデータ構造内の各フィールドを指定のバージョンの各フィールドに写像する（標準的な中間形態を使用すると予測される）。サーバ２９のみが、コンバータ・コードの全セットを有していればよいことに、注目すべきである。この変換において、ステップ１０３でサーバ２９は、示された制御ポリシーＫＥＫまたはマスターＫＥＫを使用してＣＥＫを復号化し、このＣＥＫを現在の制御ポリシーＫＥＫおよびマスターＫＥＫで再度暗号化する。ステップ１０４においてサーバ２９は、更新したＣＰＴをクライアント・エージェント２６に送り返す。ステップ１０５においてクライアントは、現在のＣＥＫを取り出し、ＣＥＫを新しくして受け取ったＣＰＴを更新し、更新したＣＰＴをキャッシュし、保護データオブジェクト３２に読み出し専用と表記されておらず、あるいは読み出し専用媒体上に格納されていない場合は、元のＣＰＴと置き換え、更新されたＣＰＴを使用して図９のステップ６５に進む。

【０１６４】

読み出し専用の保護データオブジェクト

ここまでの説明は、一般に、保護データオブジェクト３２の生成および変更を含む協働的な環境を仮定していた。好ましい実施形態はさらに、文書の生成および配布についての発行専用モデルもサポートする。詳細には、好ましい実施形態により、ビジネス・プロセス管理者は、制御ポリシー１４についてのＫＥＫが常に有効に保たれるべきであることを指示できる。このオプションは、制御ポリシー１４によって保護されるデータオブジェクトが読み出し専用であり、あるいは読み出し専用のコンピュータ媒体上に格納されていることを、管理者が認識している場合に望ましい。システムが読み出し専用データオブジェクト３２のＣＰＴ２３を更新できない場合でも、読み出し専用データオブジェクトのオフライン閲覧可能時間の長さを制限するために、クライアントのポリシー・キャッシュ８６にある読み出し専用文書に関するポリシー１４を期限切れにすることを望むことは、依然としてありうる。

【０１６５】

ポリシーの識別およびデータオブジェクトの移動

図１５は、好ましい実施形態が、コンピュータのウインドウに表示されたデータオブジェクトを現在保護している制御ポリシー１４の名称を、どのように表示するのかを示している。対象の制御ポリシー名（ここでは、"Product Launch"）が、ドロップレット・コントロール１２０と呼ばれるドロップダウン式のウインドウ・オブジェクトに表示される。有効にされると、このドロップダウン・ウインドウは、アクティブの制御ポリシー１２４を含むビジネス・プロセスの名称１２２、ならびにユーザが保護データオブジェクトを移動できる他のビジネス・プロセス１２および制御ポリシー１４を表示する。

【０１６６】
一実施形態においては、ActiveX Windowが、ドロップレット・コントロール１２０をサポートする。その内容および階層は、以下でさらに説明するとおり、キャッシュ８６、タグ２３、および／またはクライアント・ハンドラ８２を介してポリシー・サーバ２９から得られる。
【０１６７】
図１６は、制御ポリシー１４間でのデータオブジェクト（文書で代表される）の移動に含まれるロジックを示している。１つの制御ポリシー１４から別の制御ポリシーへの保護データオブジェクト３２の移動は、図２～図５に関してすでに説明したとおり、動的、分散的、および協働的な環境の重要な側面である。詳細には、好ましい実施形態は、ビジネス・プロセス１２内またはビジネス・プロセス１２間の制御ポリシー１４間の情報の流れを、ビジネス・プロセス所有者（すなわち、ビジネス管理者）が指定できるようにする。ビジネス・プロセス所有者が流れを決める一方で、許可ユーザは、保護データオブジェクトの実際の移動を実行する。移動は、通常のワークフローの一部としてしばしば生じる。
【０１６８】
ステップ１３０において許可ユーザは、権限管理対応アプリケーション２１で文書を開く。これは、新規の文書（データオブジェクト）２２であってよく、その場合には、ステップ１３２においてクライアント・エージェント２６は、ドロップレット・コントロール１２０にデフォルトの「未管理」制御ポリシーを表示する。あるいは、これが既存の保護文書であってよく、その場合には、ステップ１３２でエージェント２６は、文書２２を保護している制御ポリシーの名称をドロップレット・コントロール１２０に表示する。ステップ１３４においてユーザは、制御ポリシー１４によって指定されたユーザ使用権限の範囲内で、開いた文書を編集し、さらに操作する。ロジックは、ステップ１３４からステップ１３４自体に戻るように流れ、このような編集がある長さの非特定の、長い時間期間にわたり継続できることを示している。
【０１６９】
ある時点において、ステップ１３６でユーザは、ドロップレット・コントロール１２０を起動し、新しい制御ポリシー１４を選択して、そのポリシーに保護文書を移動することを決定できる。選択の後、ステップ１３８においてエージェント２６は、選択された制御ポリシーの識別子を内部に含む新しいＣＰＴ２３を生成し、これを文書２２にタグ付けする。制御ポリシー１４に定められているならば、許可ユーザは、ステップ１３６において「未管理」の制御ポリシーを選択してもよく、その場合、ステップ１３８においてエージェント２６は、新しいＣＰＴを生成せず、既存のＣＰＴを削除し、文書２２を復号化する。ステップ１３８の後、ユーザは、新しい制御ポリシー１４の制約の下で文書２２の編集を続行できる。
【０１７０】
システムの各制御ポリシー１４は、データオブジェクト２２をその制御ポリシーによって実現される保護の外に移動する権限を有するユーザのリストを記録する。さらに、制御ポリシー１４は、新しいデータオブジェクト２２を制御ポリシーに割り当てる権限を有するユーザのリストを記録する。ユーザは、データオブジェクト２２を現在の制御ポリシー１４から新しい制御ポリシーに移動するには、現在の制御ポリシー１４の「送出側」リストのメンバーでなければならず、新しい制御ポリシー１４の「指定先」リストのメンバーでなければならない。
【０１７１】
「移動」の権限は必須ではなく、すなわち制御ポリシー１４の「送出側」および「指定先」リストは、空白であってもよい。ただし、本発明の好ましい実施形態においては、制御ポリシー１４内のロールのうちの少なくとも１つは、ユーザがデータオブジェクト２２をポリシー１４に割り当てできるようにしている。いずれのロールも割り当ての特権を有していない場合、ポリシー１４は何ら意味を持たなくなる（すなわち、関連付けられるオブジェクトが存在しない）。「指定先」リストは、この特権がデータオブジェクトを制御

ポリシー１４に割り当てるために、最初だけ必要とされる理由から空白になってもよい。例えば、メンバーが、ポリシーの最初の生成およびポリシーへのデータオブジェクトの割り当ての際に、「指定先」の特権を有してもよい。この初期化の後、「指定先」の特権が削除され、ポリシー１４は固定の一式のオブジェクトを管理する。

【０１７２】

一般に、好ましい実施形態は、ビジネス・プロセス１２の階層内の３種類の「移動」をサポートする（図１）。

（ａ）許可ユーザには、単一のビジネス・プロセス１２内においてデータオブジェクト２２とその制御ポリシー１４との間の関連付けを変更する特権が付与される。

（ｂ）さらに、ユーザには、ビジネス・プロセス１２間でデータオブジェクト２２を移動する特権が付与される。

（ｃ）さらに、ユーザには、データオブジェクト２２を権限管理システムの外に移動する特権が付与される。この移動の結果として、データオブジェクト２２は管理または保護されないことになる。

【０１７３】

上記の種類の移動は、前述のドロップレット・コントロール１２０を通して、許可ユーザによって明示的に開始することができ、あるいは移動を、許可ユーザによってなされる他の何らかの電子的作用の副産物として、暗黙のうちに開始することもできる。この後者のカテゴリーを、「自動移動」と称する。

【０１７４】

データオブジェクト２２に関連付けられたポリシー１４は、マージ操作（例えば、カット／ペースト操作）を通して自動的に変更できる。本発明の好ましい実施形態は、マージ操作について以下の種類の自動移動を実現する。すなわち、保護データオブジェクト３２が非管理のデータオブジェクトにペーストされる場合には、対象となるデータオブジェクトはペーストされたオブジェクトのポリシー１４を引き継ぐ。保護データオブジェクト３２が、別のポリシー１４を有する保護データオブジェクトにペーストされる場合には、対象となるデータオブジェクトは自身のポリシーを維持し、ペーストの完了は、ソースのデータオブジェクトのポリシーが移動を許容しており、かつ対象のデータオブジェクトのポリシーが割り当てを許容している場合にのみ完了を許される。

【０１７５】

本発明の好ましい実施形態は、スタンドアロンの移動ツールを既存の電子ビジネス・プロセスのソフトウェア・コンポーネントに統合することによって、「自動移動」を実現する。例えば、あらかじめ設定された制御ポリシー１４の下でデータオブジェクト３２としてレポートを生成するためにスタンドアロンの移動ツールを使用するように、大きなデータベース・システム用のレポート生成部を改変できる。他の例としては、電子メールサービスを、スタンドアロンの移動ツールを一種のフィルタとして使用し（すなわち、アンチウィルスフィルタとして利用されるこのようなインタフェースを活用し）、電子メールの「宛先」または「差出人」フィールド内の個人またはグループに基づいてデータオブジェクトを１つの制御ポリシー１４から別の制御ポリシーに自動的に移動するように構成できる。自動移動は、電子メールの差出人が適切な移動の権限を有している場合にのみ生じる。そのような実施形態は、さらに、デジタル署名を使用して、電子メール・メッセージが確かに「差出人」フィールドに指定されている個人から届いたことを確認することを望むことができる。

【０１７６】

オフラインでの協働

動的かつ分散的な環境における協働は、保護データオブジェクト３２の唯一の正式の複製が、ポリシー・サーバ２９を離れて、フィールド内の、ビジネス・プロセス所有者がアクセスできない場所に常駐できることを意味する。動的、分散的、かつ協働的な環境をサポートするシステムは、２人（または、それ以上）の許可ユーザが、オンラインおよびオフラインの両方で容易に保護データオブジェクト３２を生成および共有できるようにしな

ければならない。本発明の好ましい実施形態は、そのような目標を、許可ユーザがごく最近にポリシー・サーバ２９にアクセスしていなくてはならないという唯一の基準によりサポートする。ここで「最近」とは、ユーザが希望する協働を管理する制御ポリシー１４についてのキャッシュの時間切れの期間内を意味する。言い換えると、協働はあらかじめ定められたビジネス・プロセス１２によって推進され、あらかじめ登録されたデータオブジェクト３２によって推進されるものではない。

【０１７７】

図１７は、本発明に基づく権限管理システム２００における２人のユーザ間の協働を示したフローチャートを表わしており、ここでは協働は、ポリシー・サーバ２９にとって未知である文書（データオブジェクト２２）を介して生じている。ステップ１４０は、管理者がユーザＡおよびＢの両者をロールに含んでいる制御ポリシーＰを生成することによって開始される。ステップ１４１においてユーザＡおよびＢは、ポリシー・サーバ２９が位置する企業のネットワークに接続されているユーザのラップトップにログインする。ステップ１４２において、ユーザのラップトップのクライアント・ハンドラ・プロセス８２が、制御ポリシーＰとそのＫＥＫをキャッシュする。次いで、ステップ１４３においてユーザＡおよびＢは、企業のネットワークから離れ、ユーザのラップトップをオフラインのミーティングに持ち出す。この時点で、クライアント・ハンドラ・プロセス８２は、キャッシュした制御ポリシー１４の範囲内であらゆる協働的アクティビティを許可する準備ができており、すなわちクライアント・ハンドラ・プロセス８２は、権限管理システム２００のトラスト・エージェントとして機能する。

【０１７８】

オフラインの間、ステップ１４４においてユーザＡは、機密のデータオブジェクトＤ（この例では、文書である）を生成し、制御ポリシーＰで保護する。このアクションは、ユーザＡがポリシー・サーバ２９に接続していない状態で生じる。ユーザＡは、制御ポリシーＰが自身のラップトップにキャッシュされているため、文書Ｄを生成して保護することができる。ステップ１４５においてユーザＡは、文書Ｄの複製をユーザＢに与える。ステップ１４６においてユーザＢは、やはりポリシー・サーバ２９に接続していない状態で、自身のラップトップ上で保護文書Ｄを編集できる。文書Ｄ（または、制御ポリシーＰによって保護された他のあらゆる文書）に関するユーザＡおよびＢの協働は、期限切れが生じない限り、ステップ１４７において継続する。

【０１７９】

監査、フォレンジック、およびコンプライアンス

本発明の好ましい実施形態は、図６のクライアント・エージェント２６によって監視および制御されたアクティビティ（許可および拒否されたアクティビティ）の記録をサポートする。図１０のログ・サービス８８は、個々の権限管理対応アプリケーション２１からログ・データを収集し、それらデータをポリシー・サーバ２９に送り返す。その後、ビジネス・プロセス所有者は、監査、フォレンジック、およびコンプライアンスなどのビジネス上の必要事項をサポートするために、収集された情報を検査し、調査できる。

【０１８０】

ビジネス・プロセス１２のデータオブジェクト３２に関するアクティビティの監査は、特定されたデータオブジェクト３２の暗号化を必ずしも必要としない。本発明の一実施形態においては、特定されたデータオブジェクト３２が、単に「管理」されており「保護」されていなくてもよい。言い換えると、監査は、特定されたデータオブジェクト３２がＣＰＴ２３を有していることのみを必要とし、データオブジェクト３２のコンテンツ２２が暗号化されていることを必要としない。

【０１８１】

ＣＰＴ２３のオブジェクトＩＤフィールド５５（図８）は、監査、フォレンジック、およびコンプライアンスを支援する。クライアント・エージェント２６が最初に保護データオブジェクト３２を生成したときに、完全な固有の識別子が生成される。新しいデータオブジェクト３２が既存の保護データオブジェクトから（例えば「名前をつけて保存」コマ

ンドによって）作り出されたとき、新規および既存のデータオブジェクトを結び付けるログ記録が、それらのオブジェクト識別子５５の値を使用して書かれる。そうでない場合、システム２００は、新しい保護データオブジェクト３２が最初から作られたか、あるいは非管理のデータオブジェクト２２から作られたことを記録する。

【０１８２】

この例は、本発明の好ましい実施形態が、オブジェクト識別子を監査、フォレンジック、およびコンプライアンスの目的のためだけに使用することを強調している。この実施形態は、保護データオブジェクト３２のオブジェクト識別子５５を、制御ポリシー１４または関連の使用ルールの決定には使用しない。

【０１８３】

以上、本発明を、本発明の好ましい実施の形態に関して詳細に示し説明してきたが、添付の特許請求の範囲に包含される本発明の範囲から逸脱することなく、これらの実施形態における形態および細部についてさまざまな変更が可能であることは、当業者であれば理解できるであろう。

【図面の簡単な説明】

【０１８４】

【図１】権利制御ポリシーについての体系化構造の概略図である。

【図２】ビジネス・プロセスおよび制御ポリシーのアプリケーションを示す図である。

【図３】ビジネス・プロセスおよび制御ポリシーのアプリケーションを示す図である。

【図４】ビジネス・プロセスおよび制御ポリシーのアプリケーションを示す図である。

【図５】ビジネス・プロセスおよび制御ポリシーのアプリケーションを示す図である。

【図６】本発明の一実施形態の主な構成要素の構造ブロック図である。

【図７】ポリシー管理のロジックを説明したフローチャートである。

【図８】制御ポリシー・タグの概略を示す図である。

【図９】保護データオブジェクトへのアクセスのフローチャートである。

【図１０】本発明の別の実施形態におけるクライアント・エージェントの構造ブロック図である。

【図１１】クライアント・ハンドラ・プロセシングのフローチャートである。

【図１２】鍵暗号化、鍵配布および期限切れの説明図である。

【図１３】保護データオブジェクトへのアクセスの第２のフローチャートである。

【図１４】保護データオブジェクトへのアクセスの第３のフローチャートである。

【図１５】制御ポリシー表示の図である。

【図１６】ポリシー移動ロジックのフローチャートである。

【図１７】２人のユーザ間でのオフライン協働のフローチャートである。

【符号の説明】

【０１８５】

１４　制御ポリシー

【図１】

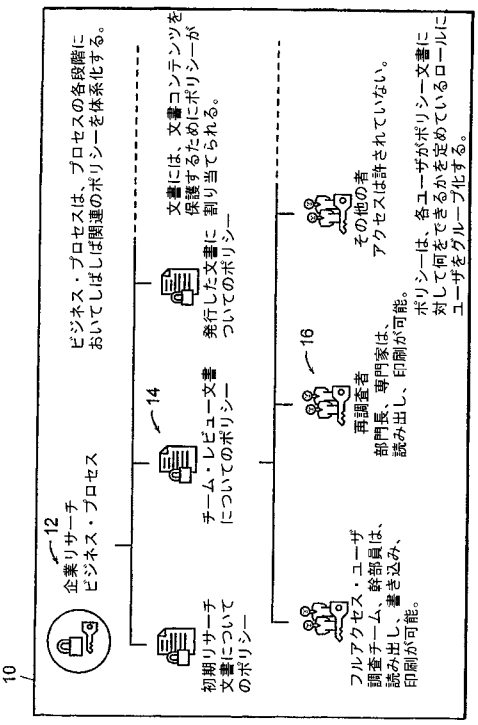

FIG. 1

【図２】

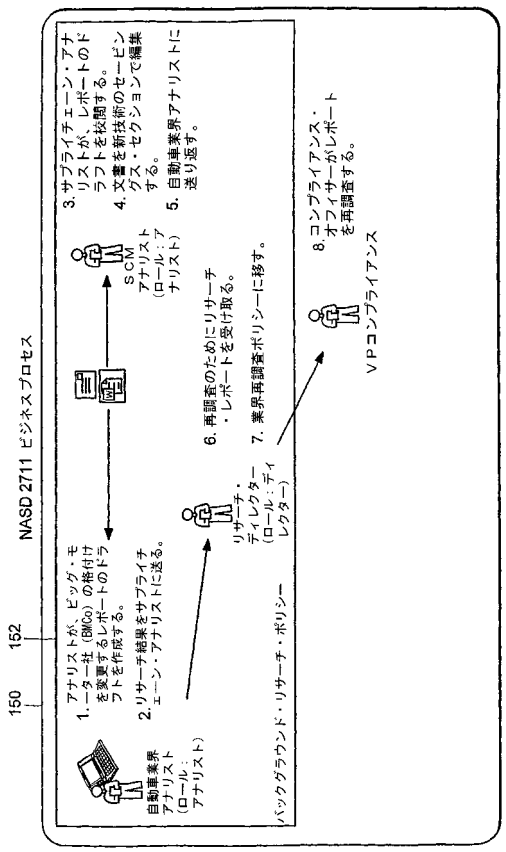

FIG. 2

【図３】

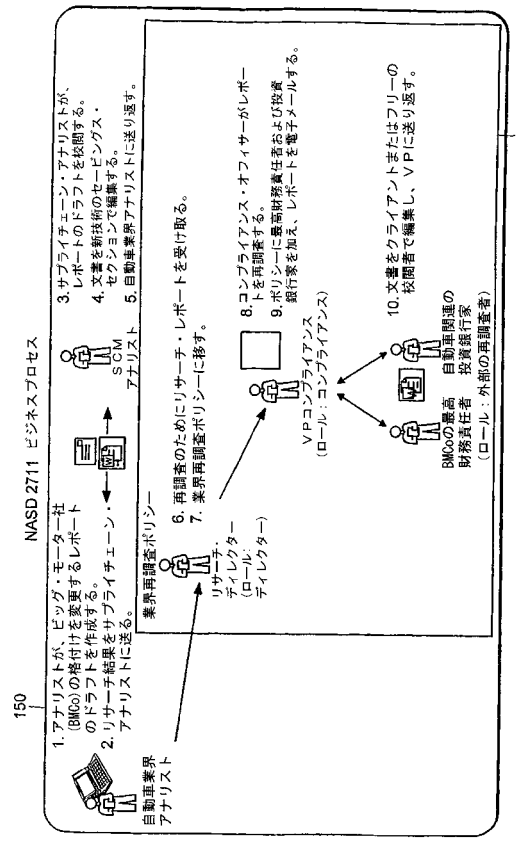

FIG. 3

【図４】

FIG. 4

【図５】

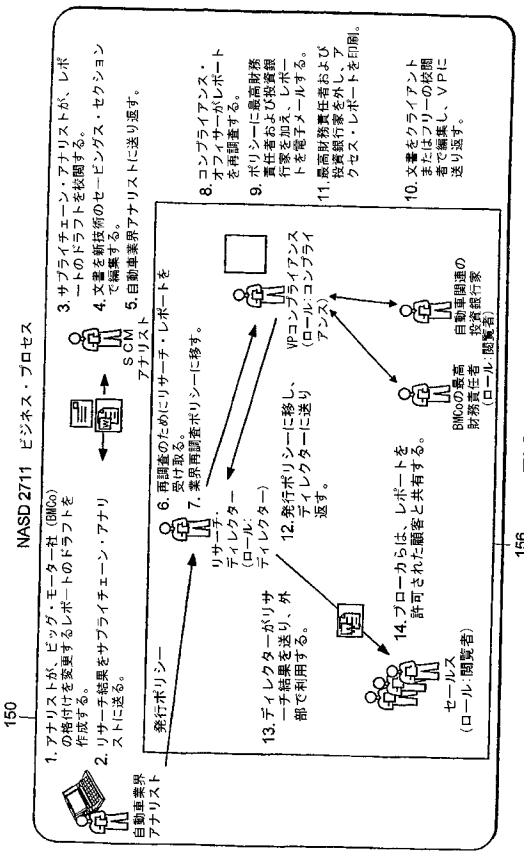

FIG. 5

【図６】

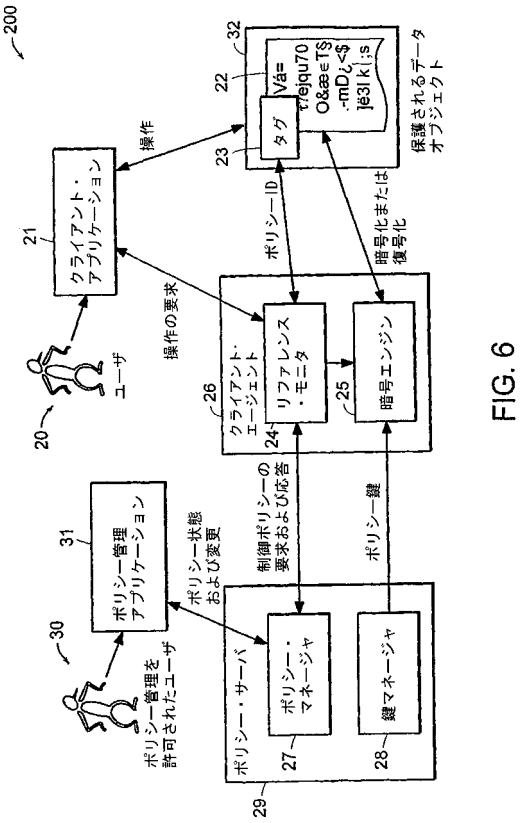

FIG. 6

【図７】

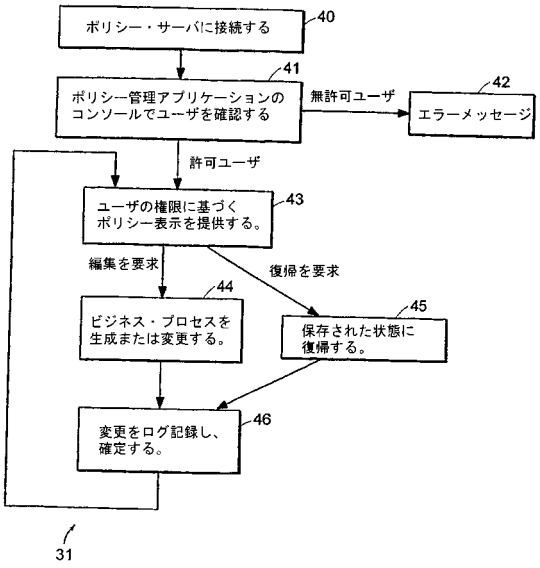

FIG. 7

【図８】

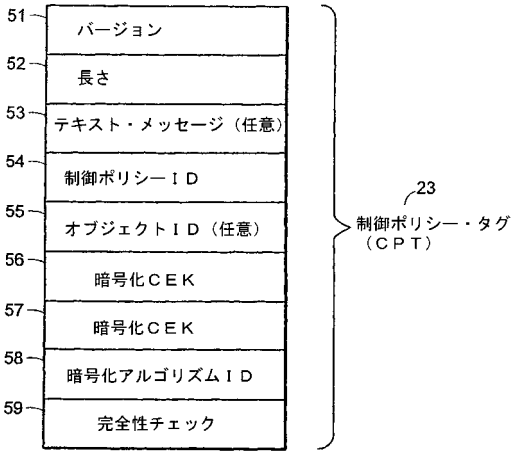

FIG. 8

【図９】

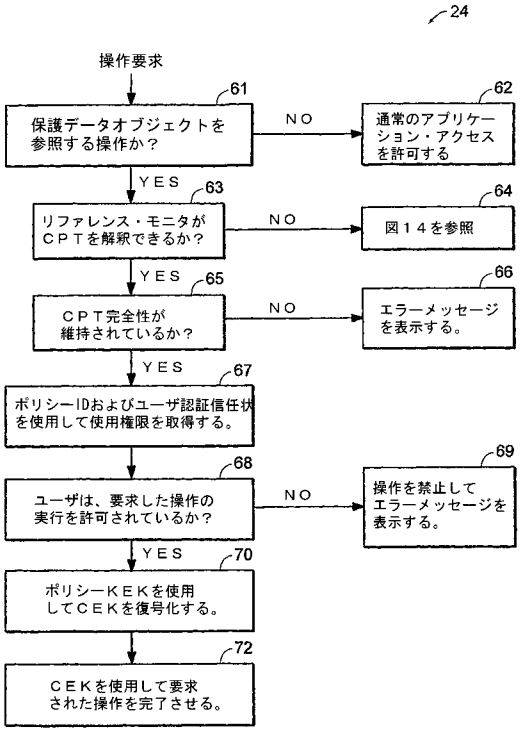

FIG. 9

【図１０】

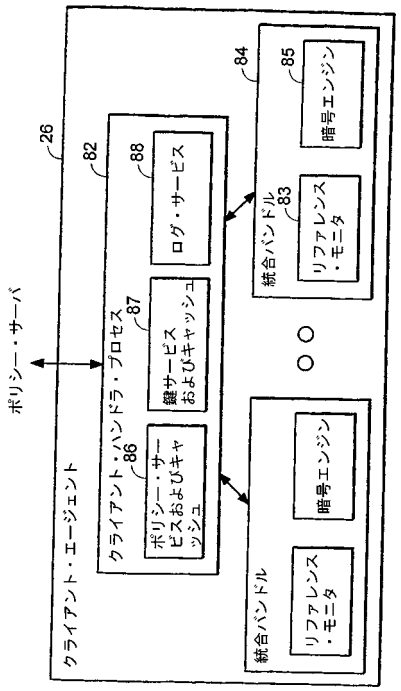

FIG. 10

【図１１】

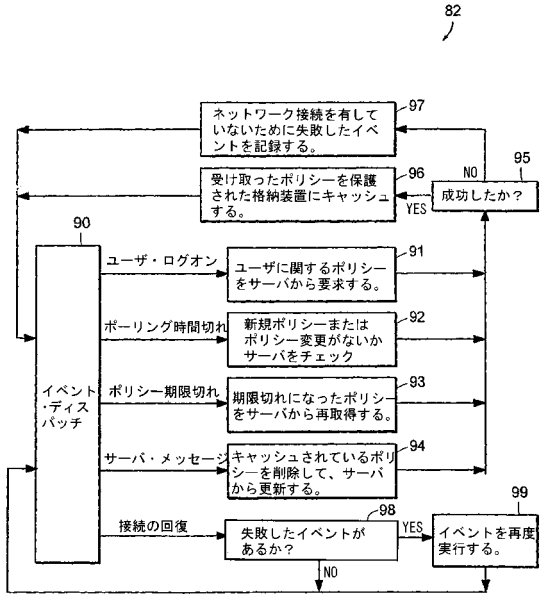

FIG. 11

【図１２】

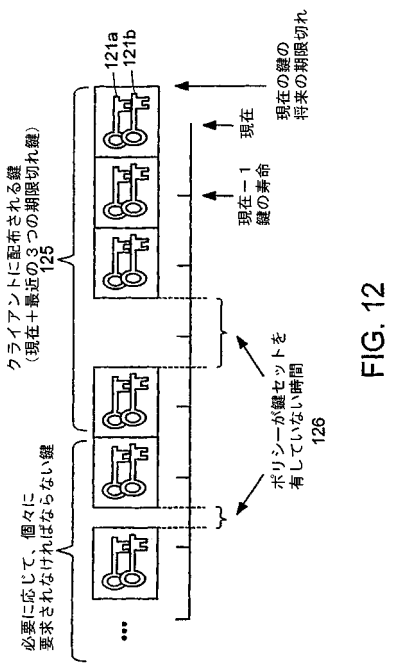

FIG. 12

【図１３】

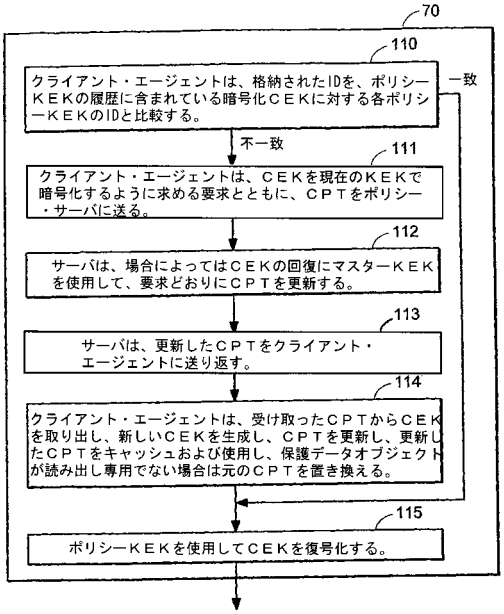

FIG. 13

【図１４】

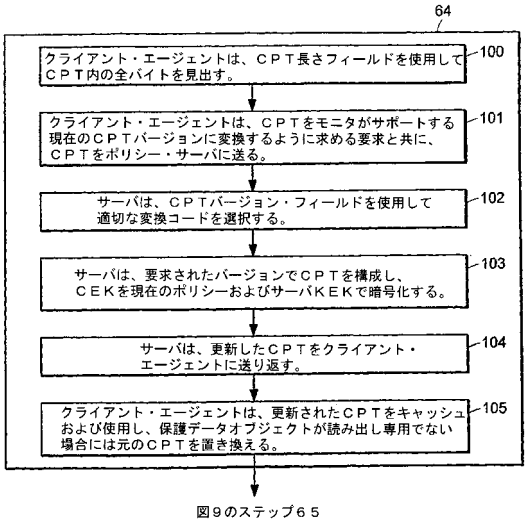

FIG. 14

【図１５】

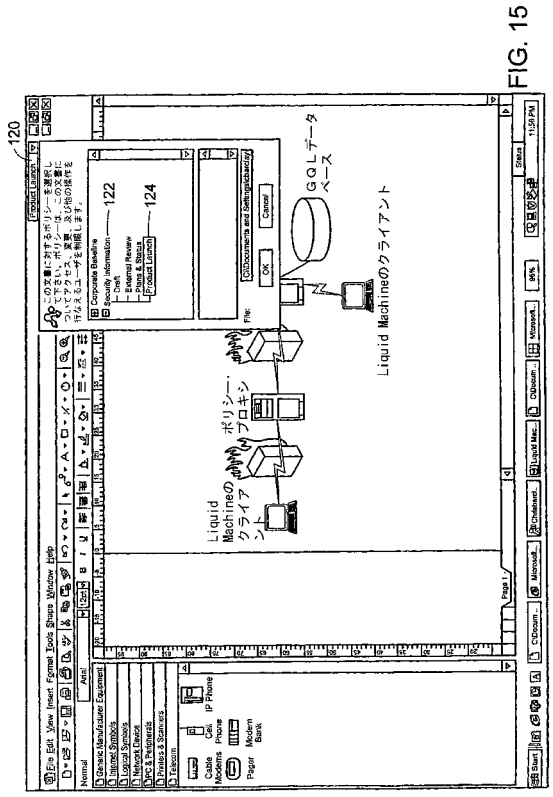

FIG. 15

【図１６】

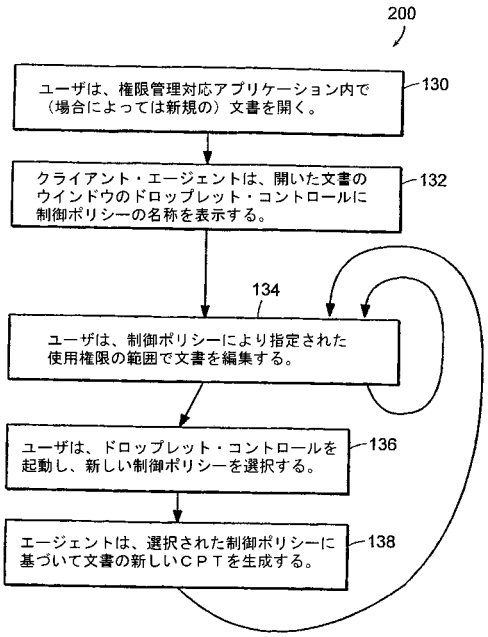

FIG. 16

【図１７】

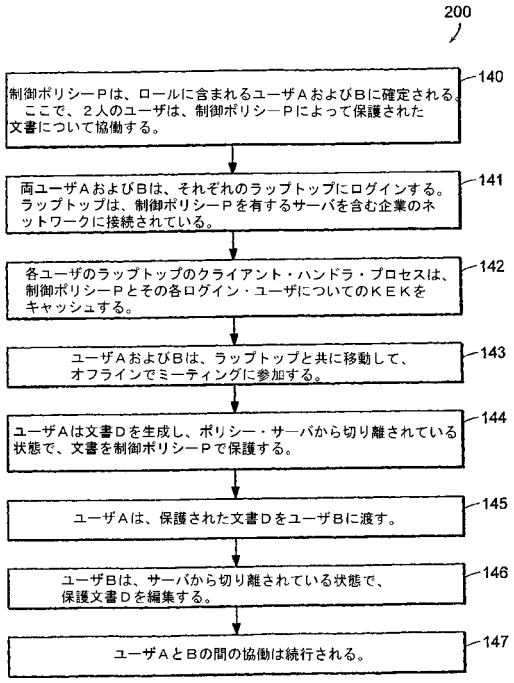
200
制御ポリシーＰは、ロールに含まれるユーザＡおよびＢに確定される。ここで、２人のユーザは、制御ポリシーＰによって保護された文書について協働する。
140
両ユーザＡおよびＢは、それぞれのラップトップにログインする。ラップトップは、制御ポリシーＰを有するサーバを含む企業のネットワークに接続されている。
141
各ユーザのラップトップのクライアント・ハンドラ・プロセスは、制御ポリシーＰとその各ログイン・ユーザについてのＫＥＫをキャッシュする。
142
ユーザＡおよびＢは、ラップトップと共に移動して、オフラインでミーティングに参加する。
143
ユーザＡは文書Ｄを生成し、ポリシー・サーバから切り離されている状態で、文書を制御ポリシーＰで保護する。
144
ユーザＡは、保護された文書ＤをユーザＢに渡す。
145
ユーザＢは、サーバから切り離されている状態で、保護文書Ｄを編集する。
146
ユーザＡとＢの間の協働は続行される。
147

FIG. 17

フロントページの続き

(72)発明者 レッサー・ノーバート
アメリカ合衆国, メーン州 ０４８４３, キャンデン, チェストナット ヒル １０
(72)発明者 カイン・ファジェン
アメリカ合衆国, マサチューセッツ州 ０２１４３, ソマーヴィレ, ナンバー2, ワシントン ストリート ２
(72)発明者 モーガン・ロバート
アメリカ合衆国, マサチューセッツ州 ０１８４５, ノース アンドーバー, ファースト ストリート ２１
(72)発明者 バークレイ・クリストファー・ビー
アメリカ合衆国, マサチューセッツ州 ０２４４６, ブルックライン, ナンバー６０５, ビーコン ストリート １４０１
(72)発明者 ゴーデッド・エドワード・ジェー
アメリカ合衆国, マサチューセッツ州 ０２３３９, ハノーバー, ガードナー ウェイ ５４
(72)発明者 スクーンメーカー・ジェイムス
アメリカ合衆国, マサチューセッツ州 ０２４７６, アーリントン, ノーフォーク ロード ７９
(72)発明者 エプステイン・アーノルド・エス
アメリカ合衆国, マサチューセッツ州 ０１７７６, サドバリー, コンコード ロード ５５５
(72)発明者 スミス・マイケル・ディ
アメリカ合衆国, マサチューセッツ州 ０２４２０, レキシントン, テイラー レイン １

審査官 宮司 卓佳

(56)参考文献 特開平１０－１１１８３３（ＪＰ, Ａ）
特開２００２－２０７７３９（ＪＰ, Ａ）
特開２０００－２９３５８４（ＪＰ, Ａ）
特開２００２－２８８０３０（ＪＰ, Ａ）
特開２００３－００６０２７（ＪＰ, Ａ）
特開２００２－００７９１４（ＪＰ, Ａ）
特開平０９－１４６８４３（ＪＰ, Ａ）
国際公開第００／０１９３２６（WO, Ａ１）

(58)調査した分野(Int.Cl., ＤＢ名)
G06F 21/24
G06F 21/20