

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5411500号
(P5411500)

(45) 発行日 平成26年2月12日(2014.2.12)

(24) 登録日 平成25年11月15日(2013.11.15)

(51) Int.Cl.

F I

H04L 9/32 (2006.01)
G09C 1/00 (2006.01)H04L 9/00 675B
G09C 1/00 640D

請求項の数 15 (全 22 頁)

(21) 出願番号	特願2008-530138 (P2008-530138)	(73) 特許権者	500046438
(86) (22) 出願日	平成18年9月6日(2006.9.6)		マイクロソフト コーポレーション
(65) 公表番号	特表2009-508405 (P2009-508405A)		アメリカ合衆国 ワシントン州 9805
(43) 公表日	平成21年2月26日(2009.2.26)		2-6399 レッドモンド ワン マイ
(86) 国際出願番号	PCT/US2006/034581		クロソフト ウェイ
(87) 国際公開番号	W02007/032968	(74) 代理人	100140109
(87) 国際公開日	平成19年3月22日(2007.3.22)		弁理士 小野 新次郎
審査請求日	平成21年8月6日(2009.8.6)	(74) 代理人	100075270
(31) 優先権主張番号	11/223, 255		弁理士 小林 泰
(32) 優先日	平成17年9月9日(2005.9.9)	(74) 代理人	100101373
(33) 優先権主張国	米国 (US)		弁理士 竹内 茂雄
前置審査		(74) 代理人	100118902
			弁理士 山本 修
		(74) 代理人	100138759
			弁理士 大房 直樹

最終頁に続く

(54) 【発明の名称】 デジタル署名ポリシー

(57) 【特許請求の範囲】

【請求項 1】

文書を複数の個別部分として格納する手段であって、前記文書は、前記文書にどの個別部分が含まれるかを示す、全ての前記個別部分をリストする文書シーケンス、及び、少なくとも1つの前記個別部分の内容に関するデータを有する、手段と、

デジタル署名ポリシーに基づいて前記文書シーケンス及び前記データに対して個別にデジタル署名を適用する手段と、

前記文書に1つ又は複数の個別部分が追加され又は前記文書から1つ又は複数の個別部分が削除されることにより前記文書シーケンスが後に変更された場合に、前記文書シーケンスに対して適用された前記デジタル署名を無効にする手段と、

前記データが後に変更された場合に、前記文書シーケンスに対して適用された前記デジタル署名が有効であり、前記データに対して適用された前記デジタル署名が無効であることを示す手段とを含むシステム。

【請求項 2】

前記格納手段が、X P S 文書フォーマットを含む、請求項 1 に記載のシステム。

【請求項 3】

前記デジタル署名ポリシーは、サブセットの個々の個別部分が変更された場合に前記文書の構成が変更されたと見なされるように、前記構成に寄与する前記個別部分の前記サブセットを定義する、請求項 1 に記載のシステム。

【請求項 4】

前記デジタル署名ポリシーは、サブセットの個々の個別部分が変更された場合に前記文書の構成が変更されたと見なされるように、前記構成に寄与する前記個別部分の第1のサブセット、および前記構成を変更せずに変更され得る部分の第2のサブセットを定義する、請求項1に記載のシステム。

【請求項5】

表示手段が、前記文書シーケンスが変更される場合に前記デジタル署名が無効であると示すように構成されたインターフェースを含む、請求項1に記載のシステム。

【請求項6】

コンピュータに、

複数の個別部分として格納された文書であって、前記文書にどの個別部分が含まれるかを示す、全ての前記個別部分をリストする文書シーケンス、及び、少なくとも1つの前記個別部分の内容に関するデータを有する文書の、前記文書シーケンス及び前記データに対して、デジタル署名ポリシーに従って個別にデジタル署名を適用するステップと、

前記文書に1つ又は複数の個別部分が追加され又は前記文書から1つ又は複数の個別部分が削除されることにより前記文書シーケンスが後に変更された場合に、前記文書シーケンスに対して適用された前記デジタル署名を無効にするステップと、

前記データが後に変更された場合に、前記文書シーケンスに対して適用された前記デジタル署名が有効であり、前記データに対して適用された前記デジタル署名が無効であることを示すステップと

を実行させるためのコンピュータ実行可能命令を記憶したコンピュータ読取り可能媒体。

【請求項7】

前記個別部分が、すべての固定文書部分および関連する関係部分と、すべての固定ページ部分および関連する固定ページ関係部分と、すべてのリソース部分と、前記文書に含まれたすべてのデジタル署名定義部分とを更に含む、請求項6に記載のコンピュータ読取り可能媒体。

【請求項8】

前記コンピュータ実行可能命令は、コアプロパティおよび注釈のうちの1つまたはいずれかが、前記デジタル署名を無効にせずに変更され得るかどうかがユーザが指定することを可能にするステップをさらに含む、請求項6に記載のコンピュータ読取り可能媒体。

【請求項9】

前記適用ステップは、前記ユーザがコアプロパティの変更によって前記ユーザのデジタル署名が無効になると指定し、またコアプロパティ部分が存在する場合は、前記ユーザのデジタル署名を前記コアプロパティ部分に適用する、請求項8に記載のコンピュータ読取り可能媒体。

【請求項10】

前記適用ステップは、前記ユーザがコアプロパティの変更によって前記ユーザのデジタル署名が無効にならないと指定し、またコアプロパティ部分が存在する場合は、前記デジタル署名を前記コアプロパティ部分に適用しない、請求項8に記載のコンピュータ読取り可能媒体。

【請求項11】

前記コンピュータ実行可能命令は、前記ユーザがコアプロパティの変更によって前記ユーザのデジタル署名が無効にならないと指定し、またコアプロパティ部分が存在しない場合は、デジタル署名の前に前記コアプロパティ部分を作成するステップをさらに含む、請求項8に記載のコンピュータ読取り可能媒体。

【請求項12】

プロセッサと、

前記プロセッサによって実行可能な命令を格納するメモリと、

を含むシステムであって、

前記命令は、

複数の個別部分として格納された文書であって、前記文書にどの個別部分が含まれるか

10

20

30

40

50

を示す、全ての前記個別部分をリストする文書シーケンス、及び、少なくとも1つの前記個別部分の内容に関するデータを有する文書の、前記文書シーケンス及び前記データに対して、デジタル署名ポリシーに従って個別にデジタル署名を適用するステップと、

前記文書に1つ又は複数の個別部分が追加され又は前記文書から1つ又は複数の個別部分が削除されることにより前記文書シーケンスが後に変更された場合に、前記文書シーケンスに対して適用された前記デジタル署名を無効にするステップと、

前記データが後に変更された場合に、前記文書シーケンスに対して適用された前記デジタル署名が有効であり、前記データに対して適用された前記デジタル署名が無効であることを示すステップと

を含む行為を実施する、
システム。

10

【請求項13】

前記デジタル署名ポリシーが、サブセットの個々の個別部分が変更された場合に前記文書の構成が変更されたと見なされるように、前記構成に寄与する前記個別部分の前記サブセットを定義する、請求項12に記載のシステム。

【請求項14】

個々の個別部分を変更すると前記デジタル署名が無効になるように前記デジタル署名が前記サブセットの各個別部分に有効に適用される、請求項13に記載のシステム。

【請求項15】

前記デジタル署名ポリシーが、前記文書の変更を引き起こさずに前記文書に加えられ得るデータをユーザが任意選択で指定することを可能にする、請求項13に記載のシステム。

20

【発明の詳細な説明】

【背景技術】

【0001】

ペーパーレス技術の採用は、多くのユーザが文書を署名するのにデジタル署名を使用しただけでなく、また、ユーザが文書を署名する際にデジタル署名を使用しないことによって妨げられてきた。これらのユーザの多くは、文書のデジタル署名が実際に何を意味するかについて混乱している。ユーザは、文書がユーザの直接制御から離れると、署名された文書に対する制御を欠くことも認識している。例えば、文書がユーザのデジタル署名を有する間に、不正な第三者が文書进行操作することがある。その結果、デジタル文書はしばしば、印刷され、次いで、通常のペン書きで署名される。その時点で、文書がスキャンされようが、ハードコピーとして扱われようが、潜在的な利点の多くが失われる。

30

【発明の開示】

【0002】

指示されたデジタル署名ポリシーに関する技術について述べられる。ある場合では、システムが、文書を複数の論理部分として格納するための手段を含む。このシステムは、文書にデジタル署名が適用されるときに文書構成を確立する手段と、文書構成がその後に変更されるかどうかを示す手段とを含む。

【0003】

この要約は、以下の詳細な説明でさらに述べられる選択された概念を簡略化された形で述べるために提供される。この要約は、特許請求の範囲中に記載された主題の主なまたは本質的な特徴を識別するためのものではなく、また特許請求の範囲中に記載された主題の範囲を定める助けとして使用するためのものでもない。

40

【0004】

述べられた技術は、電子文書をデジタル署名付きで維持するためのデジタル署名ポリシーに関する。例えば、発行側ユーザは、文書を構成し、その構成に満足するときに文書にデジタル署名することを決定してもよい。デジタル署名ポリシーは、ユーザによって署名された構成で文書を維持するために文書のどの部分をデジタル署名で包含するか確立するように、基礎となるデータレベルで機能する。デジタル署名がデジタル署名ポリシーに従

50

って適用される場合、ポリシーに違反する文書のどんな後続の操作によってもデジタル署名が無効になる。したがって、デジタル署名が存在し続けることは、文書がデジタル署名されてから変更されていないという証拠となる。したがって、デジタル署名ポリシーは、署名された文書の内容に関する確実性のレベルの向上を容易にし、すなわち、文書は、デジタル署名が適用されまたは適用されなかったときに有していたのと同じ構成を有する。文書構成に関する確実性のレベルの向上は、契約交渉および共同作業による文書作成と同じように多様なシナリオにおいて生産性を向上させることに寄与することができる。

【 0 0 0 5 】

記述された署名ポリシーは、文書のデータを個別の論理エンティティまたは部分に格納する文書パッケージおよび/または文書タイプで利用される。こうした構成の一例は、識別可能なルート部分と、ルート部分の有効な処理のための関連部分とを有するツリー構造である。こうした構成では、一部の部分は、内容に関するデータベースを格納し、ルート部分などの他の部分は、他の部分の相互関係を伝えるデータを格納する。例えば、ある部分は、所与のページの内容に関することがあり、別の部分は、所与のページの他のページに対する位置に関することがある。これを考慮して、デジタル署名ポリシーは、ユーザに提示された文書構成の維持のために、文書またはパッケージのどの基礎部分が包含されるか指定する。別の言い方をすると、デジタル署名ポリシーは、文書への後の変更を検出するために構成を利用することができるように、文書がデジタル署名されたときの文書の構成を有効に記録するように機能する。デジタル署名ポリシーは、こうした変更を検出し、それに応答してユーザの署名を無効にすることができる。少なくとも一部の実装形態は、将来のユーザによって文書の他のどの部分が、またどんなやり方で変更され得るかユーザが指定することをさらに可能にする。例えば、発行側ユーザは、文書に署名するときに、消費側ユーザが例えば、発行側ユーザの署名を無効にせずに文書に注釈を加えることができることを指定してもよい。

【 0 0 0 6 】

例示的なシステム

図 1 は、電子文書 1 0 1 が、それがデジタル署名されたときの文書の構成に一致したままかどうか判断するための署名ポリシーを実施するように構成された例示的なシステム 1 0 0 を示す。システム 1 0 0 は、デジタルデータ交換プラットフォーム 1 0 6 を介してコンシューマ 1 0 4 に結合されたパブリッシャ 1 0 2 を含む。デジタルデータ交換プラットフォームは、デジタルデータを転送するいずれかの手段を含むことができる。例えば、電子文書 1 0 1 を転送するために様々なタイプのネットワークが使用されてもよい。別の実施例では、電子文書は、ディスクやフラッシュデバイスなど、何らかのタイプの記憶媒体内に格納され、ある人から別の人に物理的に渡されてもよい。この場合、パブリッシャ 1 0 2 は、発行側ユーザ 1 1 4 のためのユーザインターフェースを作成するように物理的なコンピューティング装置上で動作するプログラムまたはソフトウェアを含む。同様に、コンシューマ 1 0 4 は、消費側ユーザ 1 2 4 のためのユーザインターフェースを作成するように物理的なコンピューティング装置上で動作するプログラムまたはソフトウェアを含む。

【 0 0 0 7 】

システム 1 0 0 は、後に消費側ユーザ 1 2 4 に提示され得る文書 1 0 1 を生成するために発行側ユーザ 1 1 4 がパブリッシャ 1 0 2 と対話することを可能にするように構成される。文書作成プロセスの間のある時点で、発行側ユーザは、発行側ユーザがデジタル署名したいと望む文書構成に達することがある。パブリッシャ 1 0 2 上で動作するデジタル署名ポリシーは、文書 1 0 1 の構成を維持するのに十分な発行側ユーザのデジタル署名によってどの基礎文書部分が包含されるか指定する。消費側ユーザ 1 2 4 は、その後に文書 1 0 1 にアクセスすることができる。コンシューマ 1 0 4 は、文書 1 0 1 を開き、デジタル署名ポリシーに従って文書を検査する。発行側ユーザのデジタル署名が有効なままである場合では、有効な署名が存在することによって、文書が発行側ユーザの意図した構成と一致したままであることが消費側ユーザに保証される。デジタル署名が無効にされた場合で

は、消費側ユーザは、文書が変更されたという知識に基づいてそれに応じて行動することができる。同様に、文書がその後に発行側ユーザに戻される場合、パブリッシャは、発行側ユーザのデジタル署名が依然として有効かどうか査定することができる。次いで、発行側ユーザは、文書が変更されたかどうか知り、それに応じて行動することができる。

【 0 0 0 8 】

図 2 は、一実装形態に従ってデジタル署名ポリシーが実施され得る例示的な文書フォーマット 2 0 0 の一般的な例を示している。この場合、文書フォーマット 2 0 0 は、データを複数の個別の論理部分に格納する。パブリッシャまたはコンシューマによって解析されるとき、論理部分はまとめて、2 0 2 で全体が示されるようにユーザに提示される文書の構成を作成する。文書は、テキスト、画像および / または他の通常の文書コンテンツを含んでもよい。この場合、論理部分は、第 1 の文書部分 2 0 4、第 2 の文書部分 2 0 6 および第 3 の文書部分 2 0 8 として例示されている。もちろん、この実施例のほかに、他の例示的な文書フォーマットが、論理部分を別のやり方で編成してもよい。例えば、論理部分のツリータイプ編成の実施例について、下記に述べられる。

【 0 0 0 9 】

説明のために、作成者または発行側ユーザが文書 2 0 2 にデジタル署名をその現在の形または構成で適用することを望むシナリオについて考慮されたい。デジタル署名ポリシーは、現在の構成を確立するために、文書のどの部分がデジタル署名によって包含されるか指定する。例えば、この実施例では、デジタル署名ポリシーが、デジタル署名を伴う 3 つのすべての文書部分 2 0 4、2 0 6 および 2 0 8 を包含すると仮定する。指定された部分のいずれかの後のどんな変更によっても、発行側ユーザのデジタル署名が無効になる。したがって、有効なデジタル署名は、文書が、それが署名されたときの構成で存在することを示す。一部の实装形態では、デジタル署名ポリシーは、発行側ユーザが、デジタル署名を無効にせずに文書に加えられ得る追加のデータを指定することを可能にしてもよい。こうした実装形態の例について、図 4 に関して下記に述べられる。あるいはまたはさらに、一部の实装形態では、デジタル署名ポリシーは、文書の構成が変更されるときには必ず署名側ユーザのデジタル署名が無効にされることを保証するために、デジタル署名によって包含される必要のある減少した数または最小数の文書部分を定義する。

【 0 0 1 0 】

図 3 ~ 4 は、一実装形態に従ってデジタル署名ポリシーが実施され得る文書フォーマットを例示する文書を示している。これらの文書が実施され得るこうした 1 つの文書フォーマットは、ワシントン州 Redmond の Microsoft Corporation 社によって開発された XML 文書仕様 (X P S : X M L P a p e r S p e c i f i c a t i o n) 文書フォーマットである。X P S 文書フォーマットに関する詳細は、少なくとも <http://www.microsoft.com/whdc/Device/print/metro.mspx> で公的に入手可能である。

【 0 0 1 1 】

この特定の实施例では、デジタル署名ポリシーは、文書が署名付きと見なされるように、どの文書部分がデジタル署名によって包含されるか示す。デジタル署名が指定された文書部分より少ない部分を包含する場合は、文書は、デジタル署名を無効にせずに後に変更され、したがって、デジタル署名が適用されたときの文書の構成に関する曖昧さをもたらすことがある。別の言い方をすると、デジタル署名ポリシーの機能は、署名時の文書構成のスナップショットを有効に作成するために、デジタル署名によってどの部分が包含されるか指定することである。図 3 ~ 4 は、特定のシナリオにおいてデジタル署名ポリシーがどのように実施され得るかについての具体的な実施例を示している。当業者には、他のシナリオが当然認識されよう。

【 0 0 1 2 】

図 3 は、パッケージ関係部分 3 0 1 と、文書シーケンス部分 3 0 2 と、関連文書シーケンス (D S : d o c u m e n t s e q u e n c e) 関係部分 3 0 3 と、少なくとも 1 つの固定文書部分とを含む文書 3 0 0 を示している。個々の固定文書の部分は、個々の固定

文書 (FD: fixed document) 関係部分に関連付けられる。この実施例では、3つの固定文書部分304、306および308が示されているが、他の実施例は、任意の数の固定文書部分を有し得る。図3が現れる文書の物理的な制約により、FD関係部分309は、固定文書部分304についてだけ示されている。

【0013】

パッケージ関係301は、そのターゲットが一部分であり、そのソースがパッケージ全体である関係である。文書シーケンス部分302は、固定文書部分304、306および308を参照するマークアップを含む。別の言い方をすると、文書シーケンスは、文書300内にどの固定文書が含まれるかリストする部分である。固定文書部分304、306または308のうちの1つまたは複数のどんな削除も、文書シーケンス部分302に反映される。同様に、新しい固定文書部分のどんな追加も、文書シーケンス部分に反映される。

10

【0014】

個々の固定文書部分は、固定ページ部分を参照する。別の言い方をすると、固定文書部分は、その個々の固定ページのリストを含む。図3が現れる物理的ページのスペースの制約により、固定ページ部分は、固定文書部分304との関連付けでのみ示されている。この場合では、2つの固定ページ部分310および312が示されているが、個々の固定文書部分によって任意の数の固定ページ部分が参照され得る。固定ページ部分のいずれの削除または追加も、関連する固定文書部分に反映される。

【0015】

20

個々の固定ページ部分は、個々のページがリンクされるリソースのすべてを指定する関係部分を通してそのリソース部分にリンクされる。例えば、固定ページ部分310は、固定ページ(FP: fixed page)関係部分320を通してリソース部分322、324に関連付けられる。図面ページの物理的制約により、関係部分およびリソース部分は、固定ページ部分312に関しては示されていない。固定ページ部分からの内容のいずれの削除または追加も、固定ページ部分および/または関連する関係部分に反映される。さらに、所与のリソースへのどんな変更も、そのリソースに反映される。

【0016】

デジタル署名ポリシーは、デジタル署名が適用されるときに文書300の構成または内容を確認する働きをする。この特定の実施例では、デジタル署名ポリシーは、デジタル署名がパッケージ関係部分301、文書シーケンス部分302、固定文書部分304、306および308、固定ページ部分310、312、リソース部分322、324、関連する関係部分303、309および320を包含しなければならないことを指定する。デジタル署名ポリシー規則は、データを複数の論理部分として格納する文書が、ユーザによってデジタル署名された構成で維持されることを保証するための機構を提供する。文書が論理部分として格納される場合では、文書構成は、部分の相互関係、ならびに部分内のデータから確立される。したがって、デジタル署名ポリシーは、部分相互関係と部分内データの両方を確立する働きをする。文書構成が部分相互関係または部分内データ、あるいはその両方によって変更される場合には、デジタル署名ポリシーは、デジタル署名を無効にさせる。こうしたデジタル署名ポリシー機構は、作成者または後続のユーザが、文書がデジタル署名に関連する構成と一致したままかどうか判断することを可能にする。

30

40

【0017】

説明するために、文書300が発行側ユーザによって、上記で指定されたデジタル署名ポリシーに従って、デジタル署名がパッケージ関係部分301、文書シーケンス部分302、ならびにその文書シーケンス関係部分303、固定文書部分304、306、308、およびその各々の固定文書関係部分(FD関係部分309だけが具体的に指定されている)、固定ページ部分310、312、ならびに固定ページ関係部分320およびリソース部分322、324を包含するようにデジタル署名されると仮定する。こうした場合、署名時に発行側ユーザのために表される文書構成は、デジタル署名ポリシーによって指定された署名付き部分によって有効に包含される。後続のユーザが文書300に新しい固定

50

文書を追加することを試みるとさらに仮定する。新しい文書は、文書シーケンス部分 3 0 2 に表される。文書シーケンス部へのこの変更によって、発行側ユーザのデジタル署名は、デジタル署名ポリシーに従って無効にされる。この特定の実装形態では、デジタル署名が無効にされるという事実は、ユーザが容易に気づくやり方で視覚的に表されてもよい。他の実装形態は、ユーザが実施しようとしている行為によって文書のデジタル署名が無効になることの警告をユーザに提供してもよい。しかし、この実装形態では、デジタル署名ポリシーは、消費側ユーザが新しい文書を追加してデジタル署名を無効することを回避しない。そうではなく、こうした行為によって、単にデジタル署名が無効になり、このシステムは、ユーザが適切と思うように行動するように、ユーザにこの情報を与える。例えば、消費側ユーザは、発行側ユーザの無効にされた署名を伴う文書を受け取る場合、その文書を改ざんされていると見なし、署名された新しい文書を発行側ユーザに要求してもよい。

10

【 0 0 1 8 】

上記実施例と同様に、後続のユーザが特定の固定ページ部分によって参照されたリソースを削除して、そのリソースを異なるリソースで置き換えようとするシナリオについて考慮されたい。例えば、リソースは、ユーザが第 2 の異なる画像で置き換えようとする画像であり得る。こうした行為は、変更（この場合は、文書の署名付きの部分を削除）しようとしているので、発行側ユーザのデジタル署名を無効にさせる。この実施例では、参照された画像の変更に応答してデジタル署名を無効にすることは、デジタル署名ポリシーの機能に一致する。例示するために、文書 3 0 0 は、所与の価格で家を建築することの建築者による提案であると仮定する。参照された画像が、提案に含まれた家の青写真であるとさらに仮定する。提案の価格は、その特定の青写真を前提とするものである。したがって、建築者は、代わりの青写真に基づいて建築者が提案を作成したように見えるように、家主などの誰かが異なる青写真を代用できることを望まない。デジタル署名ポリシーは、提案が、建築者によって提案に署名された構成のままであること、または提案が、建築者によって署名された構成ともやは一致しないように変更されていることを建築者および/または家主に通知するように機能する。

20

【 0 0 1 9 】

図 4 は、文書が署名されていると見なされるにはどの文書部分がデジタル署名によって包含されるべきかデジタル署名ポリシーが指定する、別の文書 4 0 0 を示している。文書がデジタル署名ポリシーに従ってデジタル署名される場合、デジタル署名は、それがデジタル署名されたときの文書の構成をキャプチャする。別の言い方をすると、この実装形態では、デジタル署名ポリシーは、内容が元のままの状態であると見なされるにはパッケージのどの部分が変化してはいけなしか指定する。有効性を保証するために、一部のクライアントアプリケーションおよび/またはユーザは、パッケージ内の部分および関係のすべてが署名され、有効にされることを求めることがある。他のクライアントは、コンテンツが変化していないことを示すために、選択された部分または関係だけが署名され有効にされることを求めることがある。デジタル署名ポリシーは、パッケージの部分が変更可能なままであることを可能にしながら、署名される内容を定義する柔軟性を提供する。文書 4 0 0 は、署名側ユーザが、ユーザのデジタル署名を壊さずに文書の特定の内容が変更され得る場合を指定してもよいシナリオの一例を提供している。

30

40

【 0 0 2 0 】

文書 4 0 0 は、パッケージ関係部分 4 0 2 と、デジタル署名定義部分 4 0 4 と、コアプロパティ部分 4 0 6 とを含む。この場合、デジタル署名定義部分、コアプロパティ部分 4 0 6 およびパッケージ関係部分 4 0 2 は、パッケージレベルで定義され、したがって、文書レベルで継承され、デジタル署名ポリシーによって維持される。パッケージ関係 4 0 2 は、そのターゲットが一部分であり、そのソースがパッケージ全体である関係である。デジタル署名定義部 4 0 4 は、発行側ユーザが、文書にデジタル署名するように要求される 1 組の人、および要求された各デジタル署名に関連する条件または定義を定義することを可能にする。コアプロパティ部分は、ユーザが文書内で定義することができる 1 つまたは

50

複数のプロパティに関する。例えば、1つのこうしたコアプロパティは、ユーザが希望する任意の名前または偽名を用いて自由に指定できる「文書作成者」であり得る。

【0021】

文書400はさらに、関連する文書シーケンス(DS)関係部分412を伴う文書シーケンス部410と、関連する固定文書(FD)関係部分416を伴う固定文書部分414とを含む。固定文書部分414は、固定ページ部分418および注釈部分420を参照する。固定ページ部分418は、固定ページ(FP)関係部分422に示されるように、リソース部分424にリンクされる。この特定の実装形態は、下記により詳細に論じられるサムネイル部分426をも含む。

【0022】

デジタル署名ポリシーは、デジタル署名が適用されときの文書400の内容を確立するように機能する。この実装形態では、デジタル署名ポリシーは、文書がデジタル署名ポリシーに従うように、デジタル署名がパッケージ関係部分402、文書シーケンス部410およびそのDS関係部分412、固定文書部分414およびそのFD関係部分416、固定ページ部分418およびそのFP関係部分422、ならびにリソース部分424を包含することを指定する。デジタル署名ポリシーはさらに、デジタル署名が、存在する場合にはサムネイル426を包含することを示す。もちろん、上記部分のそれぞれの単一の例だけが示されているが、多くの実装形態が部分414~426の複数の例を有する。

【0023】

この場合、パッケージ関係402に署名すると、後続のユーザが署名側ユーザのデジタル署名を無効にせずにパッケージ関係を変更することができなくなる。同様に、文書シーケンス部410およびそのDS関係部分412に署名すると、デジタル署名を無効にせずに既存の固定文書の削除または新しい固定文書の追加を行うことができなくなる。固定文書部分414およびそのFD関係部分416に署名すると、固定文書のページ順の変更、あるいは固定ページの削除または追加ができなくなる。固定ページ部分418およびそのFP関係部分422への署名は、ページの内容が変更されることを防ぐ働きをする。リソース部分424に署名すると、リソース部分を削除または置き換えることができなくなる。同様に、図示された実装形態のように、存在する場合にサムネイル部分に署名すると、署名を壊さずにサムネイル426を置き換えまたは削除することができなくなる。同様に、ここで示されるようにデジタル署名定義部分404が存在する場合、デジタル署名ポリシーは、デジタル署名を伴うデジタル署名定義部分を包含する。デジタル署名ポリシーは機能上、署名された構成から文書が変更されているかどうかに関する表示を集合的に提供するために、これらのコンポーネントのそれぞれに署名する。

【0024】

この実装形態では、デジタル署名ポリシーは、署名側ユーザが、署名側ユーザのデジタル署名を無効にせずに文書の特定の部分の内容が操作され得るかどうか決定することを可能にする。例えば、署名側ユーザは、後続のユーザが、署名側ユーザのデジタル署名を無効にせず文書に内容を追加できることを望むであろうか。こうした1つの場合では、署名側ユーザは、後続ユーザが文書にデジタル署名を追加することを可能にするかどうか決定することができる。別の場合では、署名ユーザは、後続のユーザが文書へのコアプロパティ変更を行うことを可能にするかどうか決定することができる。別の場合では、署名側ユーザは、後続のユーザが文書に注釈を加えることを可能にするかどうか決定することができる。これらのオプションはそれぞれ、他とは独立したものであり、署名側ユーザは、文書へのオプションの追加も、いずれかの所望の組合せも可能にしないことがある。

【0025】

図5は、コアプロパティに関する論理テーブル500の形のデジタル署名ポリシーの一例を示している。論理テーブル500は、相互排他的な2つのシナリオに関する。第1のシナリオでは、502に示されるように、署名側ユーザは、コアプロパティの変更を可能にすることを望む。第2のシナリオでは、504に示されるように、署名側ユーザは、コアプロパティの変更を可能にすることを望まない。2つのシナリオ502、504に関し

10

20

30

40

50

て、2つの状況のうちの1つが存在する。506に示されるようにコアプロパティ部分が存在し、あるいは508に示されるようにコアプロパティ部分が存在しない。

【0026】

510に示されるように、署名側ユーザがコアプロパティの変更を可能にすることを望み、コアプロパティが存在する場合は、デジタル署名ポリシーは、ユーザが文書にデジタル署名するときにコアプロパティ部分を無署名のままにしておくが、ポリシーは、図4に関して述べたパッケージ関係にユーザのデジタル署名を適用する。パッケージ関係は、コアプロパティ部分へのリンクを含み、したがって、後続のユーザは、ユーザの署名を無効にせずコアプロパティを変更することができる。

【0027】

512に示されるように、署名側ユーザがコアプロパティ変更を可能にすることを望み、またコアプロパティが存在しない場合は、デジタル署名ポリシーは、ユーザが文書にデジタル署名する前にコアプロパティ部分を作成する。コアプロパティ部分は、この時点では空であり得るが、署名の前にそれを作成することによって、後に内容が追加されることが可能になる。次いで、コアプロパティ部分は、コアプロパティへの後続の変更が行われ得るように無署名のままにされる。上記のように、ユーザのデジタル署名は、要素(material)が変更されまたは削除されないようにするために、パッケージ関係に適用される。

【0028】

514に示されるように、署名側ユーザがコアプロパティの追加を可能にすることを望まず、またコアプロパティが存在する場合は、デジタル署名ポリシーは、ユーザのデジタル署名でコアプロパティ部分、ならびにパッケージ関係に署名する。こうしたシナリオでは、ユーザのデジタル署名は、コアプロパティ部分へのどんな変更によってもユーザの署名が無効になるように、コアプロパティ部分を包含する。

【0029】

最後に、516に示されるように、署名側ユーザがコアプロパティの追加を可能にすることを望まず、またコアプロパティ部分が存在しない場合は、デジタル署名ポリシーは、ユーザが文書にデジタル署名する前にコアプロパティ部分を作成しない。他のシナリオと同様に、デジタル署名は、パッケージ関係に適用される。このシナリオでは、次にコアプロパティを追加するには、コアプロパティ部分の追加が必要である。コアプロパティ部分を追加すると、パッケージ関係部分に変更され、それによって、ユーザの署名が無効になる。

【0030】

図4～5をまとめて参照すると、デジタル署名ポリシーは、コアプロパティに関して上述されたのと同じやり方で注釈を扱うことができる。注釈は、固定文書部分414によって参照される注釈部分420に追加される。注釈部分がユーザのデジタル署名によって包含される場合は、注釈を加えると署名が無効になる。注釈部分が存在しない場合は、デジタル署名が適用された後に注釈部分を作成すると、固定文書部分に変更され、署名が無効になる。署名側ユーザが、注釈が追加されることを可能にしたい場合は、注釈部分が署名時に存在すべきであり、また無署名にしておかれるべきである。注釈部分は、文書にデジタル署名する前に作成されてもよい。こうした場合では、新しく作成された注釈部分は、ユーザのデジタル署名が適用されるときに空であることがある。

【0031】

図6は、図4に表された文書400に関連付けられ得るようなデジタル署名部分に関する。この実装形態では、デジタル署名部分は、署名起点部分602と、署名部分と、証明書部分とを含む。この場合、2つの署名部分604、606が、2つの証明書部分608、610と同様に表されている。この実装形態は、証明書部分608および610を別々の個別の部分として明示している。他の実装形態では、証明書部分は、関連する署名部分に組み込まれてもよい。署名起点部分602は、文書の使用可能なデジタル署名上を移動して見る(navigate)ための始点を提供する。デジタル署名ポリシーによって指

10

20

30

40

50

定された部分を包含するデジタル署名を含んでおり、また適切に検証される606や608などの署名部分は、有効であると見なされ得る。例えば、このシステムは、正確な部分がデジタル署名ポリシーに従って署名されていることを検証する。このシステムはさらに、上記のコアプロパティなど、任意選択で署名された部分の状況、および任意選択で署名された部分の状態がどのようにユーザに影響を及ぼしているか検証する。このシステムは、署名された部分について、署名が有効であることをも検証する。例えば、このシステムは、当業者に当然認識されるように、ハッシュ計算が一致するかどうかチェックする。

【0032】

別の言い方をすると、署名部分がデジタル署名ポリシーと一致する文書部分を包含し、また署名検証が成功する場合は、文書は、XPS文書など、有効な署名付き文書と見なされ得る。こうした場合では、ユーザは、こうした文書が、有効なデジタル署名が適用されたときに存在したのと同じ構成を有していると見なすことができる。

【0033】

デジタル署名ポリシーは、追加の要素が文書に追加され得るかどうかに関する柔軟な解決策を提供する。この解決策は、発行側ユーザが、もしあるならばどんなオプションの要素が、デジタル署名を無効にせずに追加され得るか指定することを可能にする。次いで、デジタル署名ポリシーは、文書の現在の構成を考慮に入れ、それに応じて、図4～6に上述されたように部分を作成しまたはそれに署名するように働く。少なくとも一部の実装形態は、スイッチに類似する。例えば、作成者が署名保護をオンにし、誰かがデジタル署名を追加する場合は、デジタル署名ポリシーは、作成者のデジタル署名を壊す。作成者が署名保護を望まない場合は、作成者のデジタル署名に影響を及ぼさず、誰かがデジタル署名を追加することができる。同じ原理が、注釈およびコアプロパティなどの他のオプションの追加に適用される。したがって、この解決策は、それが署名側ユーザにポリシーパラメータを定義させ、デジタル署名ポリシーがそれに応じて、後続のユーザが署名側ユーザのデジタル署名を壊さずに内容を追加することを可能にするという点で、非常に柔軟である。しかし、その柔軟性にもかかわらず、デジタル署名ポリシーは、消費側ユーザのデジタル署名を壊さずに文書構成を誰かが変更することを防止し続ける。エンドユーザレベルでは、述べられたデジタル署名ポリシーは、ユーザのデジタル署名を有する文書が、ユーザによってデジタル署名された構成に一致したままであることの信頼性を向上させる。デジタル署名ポリシーは、デジタル署名ポリシーに従う文書および文書フォーマットと対話することができる他のソフトウェア製品に適合し、かつ/またはそれによって理解され得るデジタル署名ポリシーを確立するのにも有用である。デジタル署名ポリシーは、署名付き文書によって実際に何が包含されるか、デジタル署名ポリシーに従う署名付き文書をどのように生成するか、かつ/または文書のデジタル署名が有効かどうか判断するために、受信された文書をどのように評価するかについての規格を定義する。要約すると、デジタル署名ポリシーは、デジタル署名された文書が実際に何を意味するか定義する。

【0034】

例示的なコンピューティング環境

図7は、デジタル署名ポリシーが実施され得る、例示的なシステムまたはコンピューティング環境700を表している。システム700は、第1のマシン701および第2のマシン702の形の汎用コンピューティングシステムを含む。

【0035】

第1のマシン701の構成要素は、それだけに限らないが、1つまたは複数のプロセッサ704（例えばマイクロプロセッサ、コントローラなどのいずれか）、システムメモリ706と、様々なシステム構成要素を結合するシステムバス708とを含み得る。1つまたは複数のプロセッサ704は、第1のマシン701の動作を制御し、また他の電子およびコンピューティング装置と通信するための様々なコンピュータ実行可能命令を処理する。システムバス708は、メモリバスまたはメモリコントローラ、周辺バス、アクセラレイテッドグラフィックポートおよびプロセッサ、または様々なバス構造のいずれかを使用したローカルバスを含めて、任意の数の複数のタイプのバス構造のいずれかを表す。

【 0 0 3 6 】

システム 7 0 0 は、第 1 のマシン 7 0 1 によってアクセス可能である任意の媒体であり得る様々なコンピュータ読取り可能媒体を含み、揮発性と不揮発性、取外し可能と取外し不可能の両方の媒体を含む。システムメモリ 7 0 6 は、ランダムアクセスメモリ (RAM : random access memory) 7 1 0 などの揮発性メモリ、および / または読取り専用メモリ (ROM : read only memory) 7 1 2 などの不揮発性メモリの形のコンピュータ読取り可能媒体を含む。基本入出力システム (BIOS : basic input/output system) 7 1 4 は、起動時などに第 1 のマシン 7 0 1 内の構成要素間の情報転送を円滑に進める基本ルーチンを維持し、ROM 7 1 2 に格納される。RAM 7 1 0 は一般に、プロセッサ 7 0 4 のうちの 1 つまたは複数から直ぐにアクセス可能であり、かつ / またはそれによる操作を現在受けているデータおよび / またはプログラムモジュールを含む。

10

【 0 0 3 7 】

第 1 のマシン 7 0 1 は、他の取外し可能 / 取外し不可能、揮発性 / 不揮発性のコンピュータ記憶媒体を含んでもよい。例を挙げると、ハードディスクドライブ 7 1 6 は、取外し不可能な不揮発性の磁気媒体 (図示せず) から読み出し、かつそこに書き込み、磁気ディスクドライブ 7 1 8 は、取外し可能な不揮発性の磁気ディスク 7 2 0 (例えば「フロッピー (登録商標) ディスク」) から読み出し、かつそこに書き込み、光ディスクドライブ 7 2 2 は、CD-ROM、デジタル多用途ディスク (DVD : digital versatile disk) または他のいずれかのタイプの光学媒体など、取外し可能な不揮発性の光ディスク 7 2 4 から読み出し、かつ / またはそこに書き込む。この実施例では、ハードディスクドライブ 7 1 6、磁気ディスクドライブ 7 1 8 および光ディスクドライブ 7 2 2 はそれぞれ、1 つまたは複数のデータメディアインターフェース 7 2 6 によってシステムバス 7 0 8 に接続される。ディスクドライブおよび関連するコンピュータ読取り可能媒体は、コンピュータ読取り可能命令、データ構造体、プログラムモジュール、および第 1 のマシン 7 0 1 のための他のデータの揮発性記憶域を提供する。

20

【 0 0 3 8 】

例を挙げると、オペレーティングシステム 7 2 6、1 つまたは複数のアプリケーションプログラム 7 2 8、他のプログラムモジュール 7 3 0 およびプログラムデータ 7 3 2 を含めて、任意の数のプログラムモジュールが、ハードディスク 7 1 6、磁気ディスク 7 2 0、光ディスク 7 2 4、ROM 7 1 2 および / または RAM 7 1 0 に格納され得る。こうしたオペレーティングシステム 7 2 6、アプリケーションプログラム 7 2 8、他のプログラムモジュール 7 3 0 およびプログラムデータ 7 3 2 (またはその何らかの組合せ) は、本明細書で述べられたシステムおよび方法の一実施形態を含んでもよい。

30

【 0 0 3 9 】

ユーザは、キーボード 7 3 4 およびポインティング装置 7 3 6 (例えば「マウス」) など、任意の数の異なる入力装置を介して第 1 のマシン 7 0 1 とインターフェースすることができる。他の入力装置 7 3 8 (具体的には図示せず) は、マイクロホン、ジョイスティック、ゲームパッド、コントローラ、衛星放送アンテナ、シリアルポート、スキャナおよび / または同類物を含んでもよい。これらおよび他の入力装置は、システムバス 7 0 8 に結合された入出力インターフェース 7 4 0 を介してプロセッサ 7 0 4 に結合されるが、パラレルポート、ゲームポートおよび / またはユニバーサルシリアルバス (USB : universal serial bus) など、他のインターフェースおよびバス構造によって接続されてもよい。

40

【 0 0 4 0 】

モニタ 7 4 2 または他のタイプの表示装置が、ビデオアダプタ 7 4 4 などのインターフェースを介してシステムバス 7 0 8 に接続され得る。モニタ 7 4 2 に加えて、他の出力周辺装置は、入出力インターフェース 7 4 0 を介して第 1 のマシン 7 0 1 に接続され得るスピーカ (図示せず) およびプリンタ 7 4 6 などの構成要素を含むことができる。

【 0 0 4 1 】

50

第1のマシン701は、第2のマシン702などの1つまたは複数のリモートコンピュータへの論理接続を使用して、ネットワーク化された環境内で動作することができる。例を挙げると、第2のマシン702は、パーソナルコンピュータ、携帯型コンピュータ、サーバ、ルータ、ネットワークコンピュータ、ピアデバイスまたは他の共通ネットワークノードなどであり得る。第2のマシン702は、第1のマシン701に関して本明細書で述べられた要素および特徴の多くまたはすべてを含み得るポータブルコンピュータとして示される。

【0042】

第1のマシン701と第2のマシン702の間の論理接続は、ローカルエリアネットワーク(LAN: local area network)750および一般的な広域ネットワーク(WAN: wide area network)752として示される。こうしたネットワーキング環境は、オフィス、企業規模のコンピュータネットワーク、イントラネットおよびインターネットでは一般的である。LANネットワーキング環境内で実施されるとき、第1のマシン701は、ネットワークインターフェースまたはアダプタ754を介してローカルネットワーク750に接続される。WANネットワーキング環境内で実施されるとき、第1のマシン701は一般に、モデム756、または広域ネットワーク752を介して通信を確立する他の手段を含む。第1のマシン701の内部にあることも、外部にあることもあるモデム756は、入出力インターフェース740または他の適切な機構を介してシステムバス708に接続され得る。示されたネットワーク接続は例示的なものであり、第1と第2のマシン701、702間の通信リンクを確立する他の手段が利用され得る。

【0043】

システム700で示されたようなネットワーク化された環境では、第1のマシン701に関して示されたプログラムモジュール、またはその一部は、リモートメモリ記憶装置内に格納されてもよい。例を挙げると、リモートアプリケーションプログラム758は、第2のマシン702のメモリ装置で維持される。例示するため、アプリケーションプログラム、およびオペレーティングシステム726などの他の実行可能プログラムコンポーネントは、本明細書では個別のブロックとして示されているが、こうしたプログラムおよびコンポーネントは、様々なときに第1のマシン701のそれぞれ異なる記憶コンポーネント内に常駐し、第1のマシンのプロセッサ704によって実行されることが認識されよう。

【0044】

例示的なプロセス

図8は、デジタル署名ポリシーに関連する例示的なプロセス800を示している。プロセスが示される順序は、限定と見なされるものではなく、任意の数の示されたプロセスブロックが、プロセスを実施する任意の順序で組み合わせられ得る。さらに、プロセスは、任意の適切なハードウェア、ソフトウェア、ファームウェアまたはその組合せで実施され得る。

【0045】

ブロック802で、プロセスは、デジタル署名ポリシーに従ってユーザのデジタル署名で包含する文書の部分を決定する。一部の実装形態では、デジタル署名ポリシーは、文書のすべての部分がデジタル署名されることを指定することができる。他の実装形態では、デジタル署名ポリシーは、デジタル署名される部分のサブセットを指定することができる。例えば、一実装形態では、デジタル署名ポリシーは、署名時に表された文書構成に寄与する部分に適用される。こうした場合では、デジタル署名ポリシーは、署名の後に文書が、ユーザが署名した文書構成から文書構成を変更するようなやり方で変更されているかどうかユーザおよび/または他のユーザに通知するように機能する。

【0046】

ブロック804で、プロセスは、ブロック802で決定された部分にデジタル署名を適用する。ユーザのデジタル署名は、部分のうちのいずれかが変更される場合にはデジタル署名が壊されまたは無効にされるように、デジタル署名ポリシーによって指定されたすべ

ての部分に有効に適用される。部分のいずれかに関するデジタル署名を壊すと、文書のデジタル署名全体が壊される。基礎となるその論理的根拠は、指定された部分のいずれかを変更すると文書構成が変更され得ることである。

【 0 0 4 7 】

このプロセスは、ユーザおよび / または後続のユーザが文書の扱い方についてより十分な知識を得たうえで決定することができるように、デジタル署名が有効のままかどうか表すことができる。デジタル署名ポリシーは、ユーザへの信頼性の度合いが増した環境を有効にもたす。例えば、発行側ユーザが特定の文書構成に満足しており、その文書をデジタル署名する場合、デジタル署名ポリシーは、ユーザのデジタル署名が有効なままである限り、発行側ユーザと、いずれかの消費側ユーザの両方が、発行側ユーザによってデジタル署名された文書構成を見ているという確信をもって行動できることを保証する。これは、発行側ユーザが所望の文書構成にデジタル署名し、次いで、契約交渉において遭遇し得るような、相反する消費側に文書を送るシナリオにおいて特に有用であり得る。次いで、消費側ユーザが発行側ユーザに文書を返送する場合、発行側ユーザは、消費側が、検出するのは難しいが重要な何らかの変更を文書に加えたことに非常に用心することがある。デジタル署名ポリシーの機能性によって、発行側ユーザは、戻された文書が発行側ユーザがデジタル署名した同じ構成を有するか容易に判断することができる。デジタル署名ポリシーがユーザへのより高いレベルの信頼性をもたらすので、それは、特にユーザによって重要と見なされる事柄において、デジタル文書の受入れのレベルの向上を促し得る。さらに、システム面から見ると、デジタル署名ポリシーは、デジタル署名ポリシーに従う文書と対話し、またはそれをサポートすることができるソフトウェア製品間の相互運用性を促進する。

【 0 0 4 8 】

デジタル署名ポリシーに関する実装形態について、構造的特徴および / または方法に特有の言語で述べられたが、添付の特許請求の範囲の主題は、示された特定の特徴または方法に必ずしも限定されないことを理解されたい。そうではなく、特定の特徴および方法は、上記および下記に示された概念についての実装形態の例を提供するものである。

【図面の簡単な説明】

【 0 0 4 9 】

【図 1】一実装形態に従ってデジタル署名ポリシーが実施され得る例示的なシステムを示す図である。

【図 2】一実装形態に従ってデジタル署名ポリシーが実施され得る例示的な文書構成を示す図である。

【図 3】一実装形態に従ってデジタル署名ポリシーが実施され得る例示的な文書構成を示す図である。

【図 4】一実装形態に従ってデジタル署名ポリシーが実施され得る例示的な文書構成を示す図である。

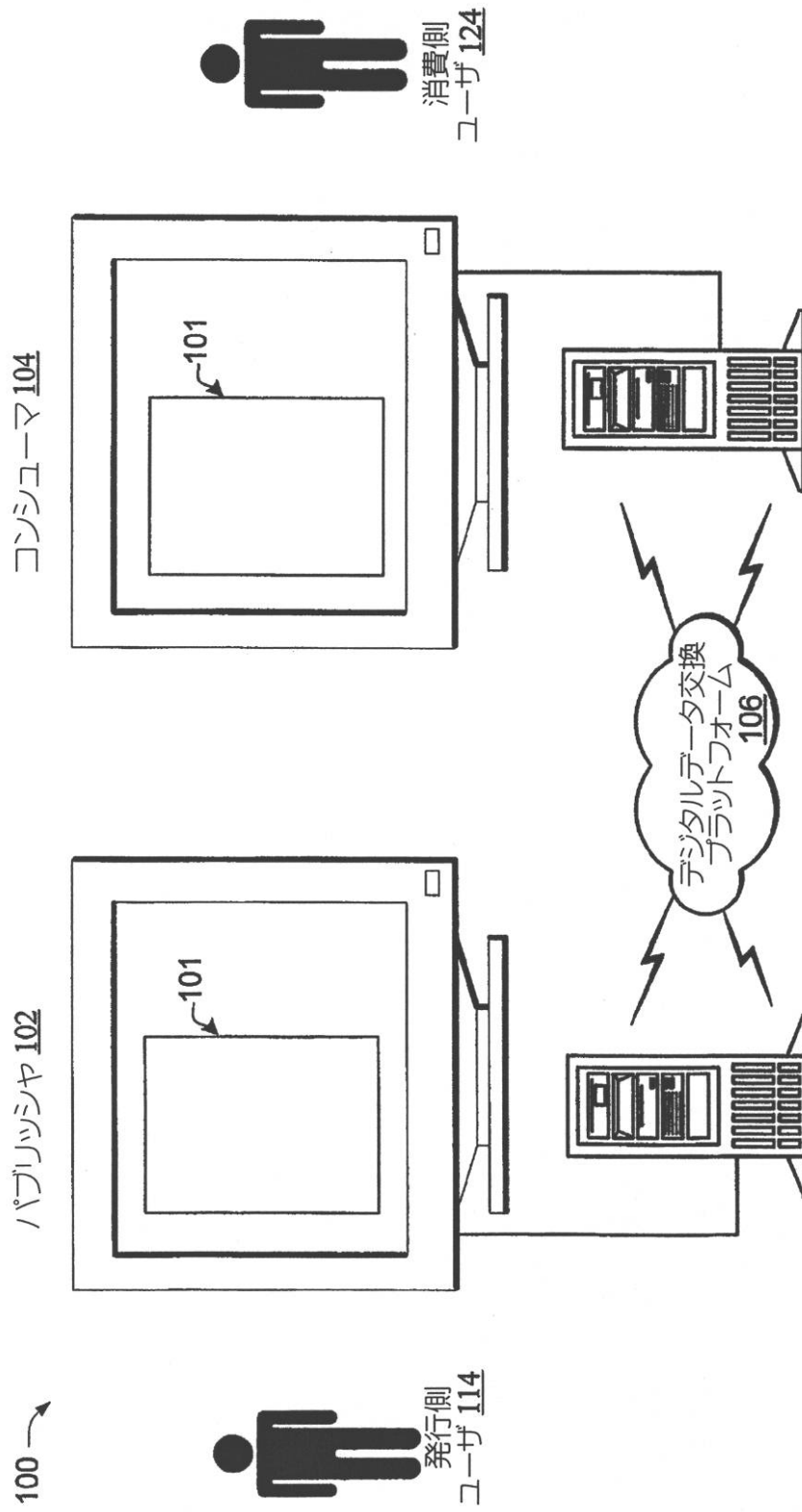
【図 5】一実装形態に従ってデジタル署名ポリシーが実施され得る例示的な文書構成を示す図である。

【図 6】一実装形態に従ってデジタル署名ポリシーが実施され得る例示的な文書構成を示す図である。

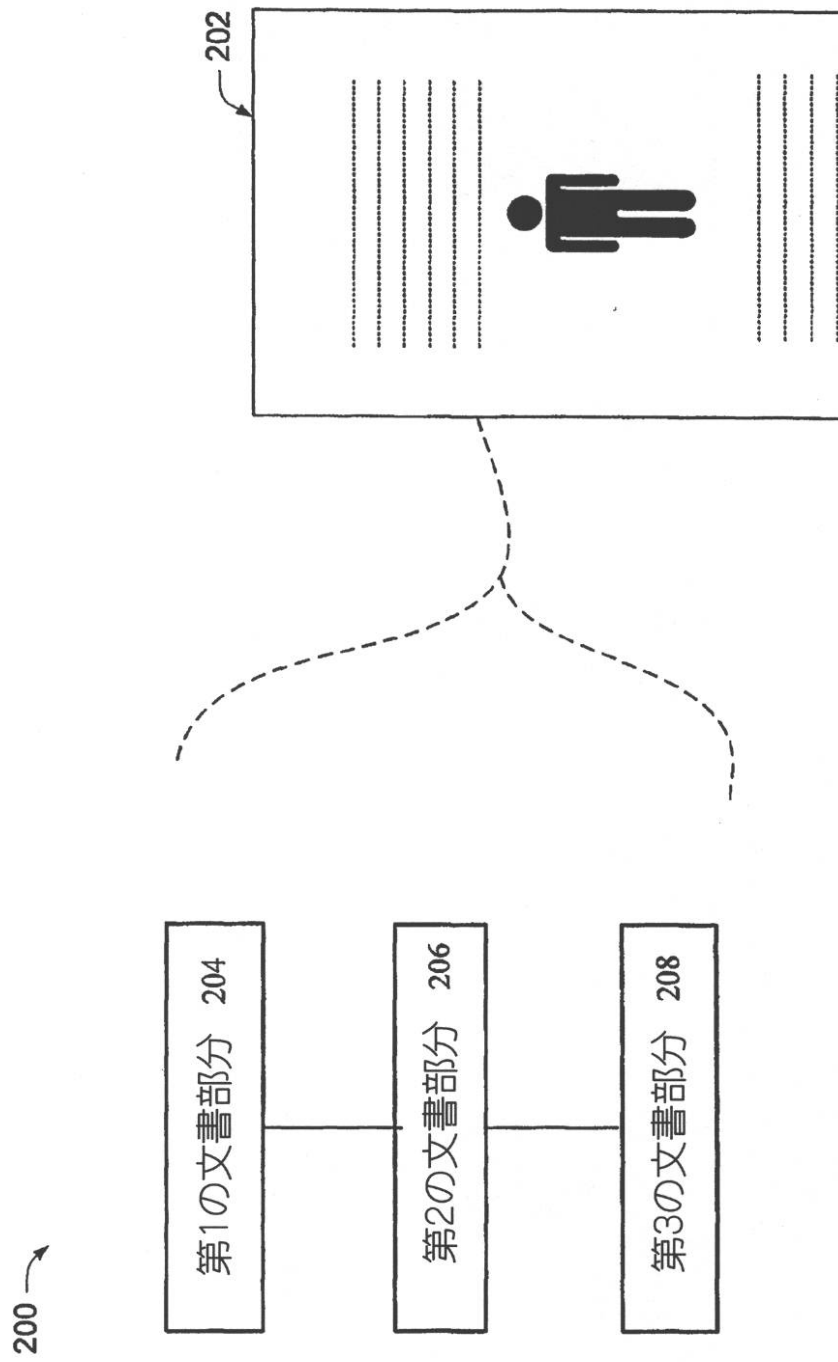
【図 7】一実装形態に従ってデジタル署名ポリシーが実施され得る例示的なシステム、装置、および環境内の構成要素を示す図である。

【図 8】一実装形態による、デジタル署名ポリシーに関する例示的なプロセス図である。

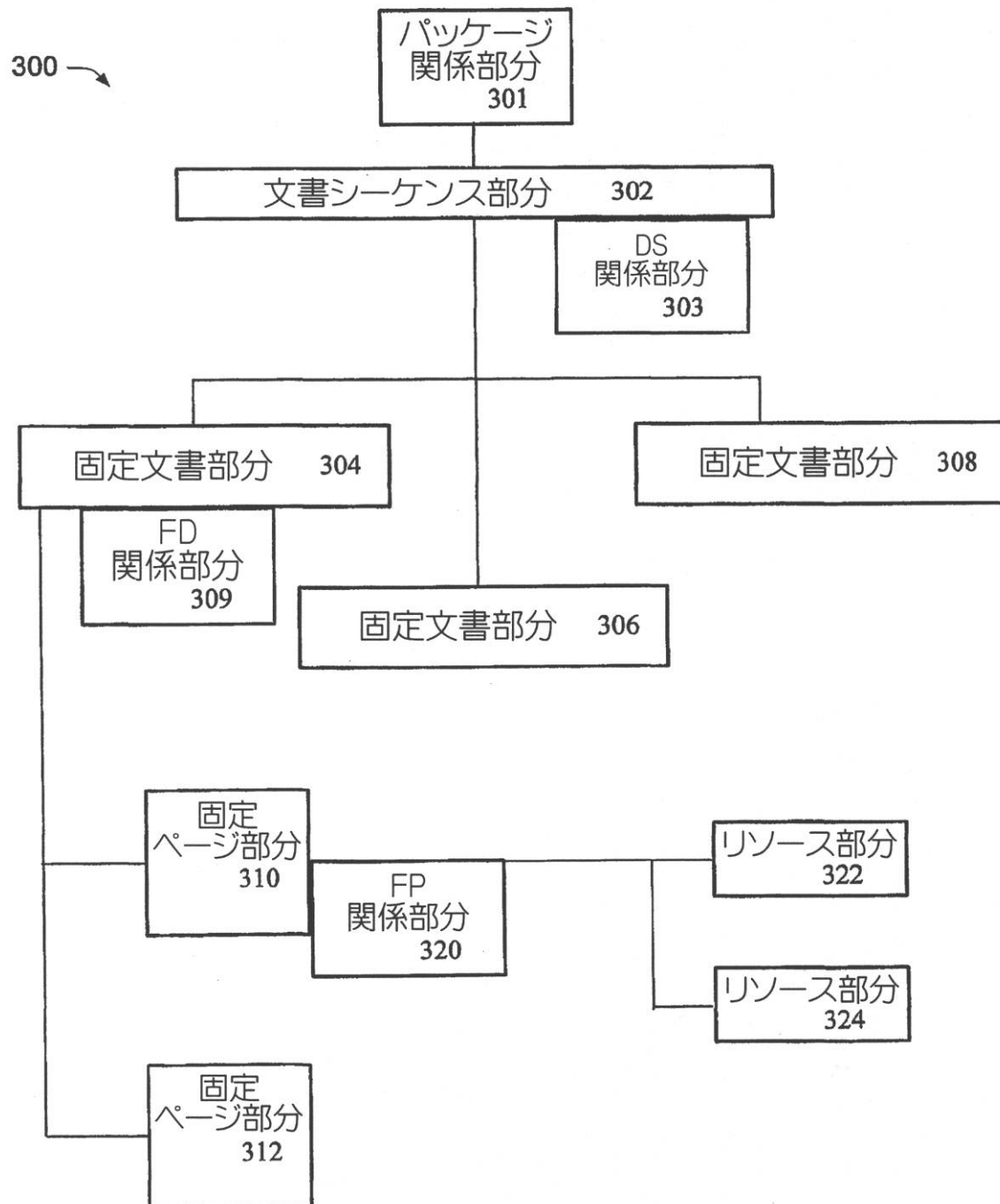
【図 1】



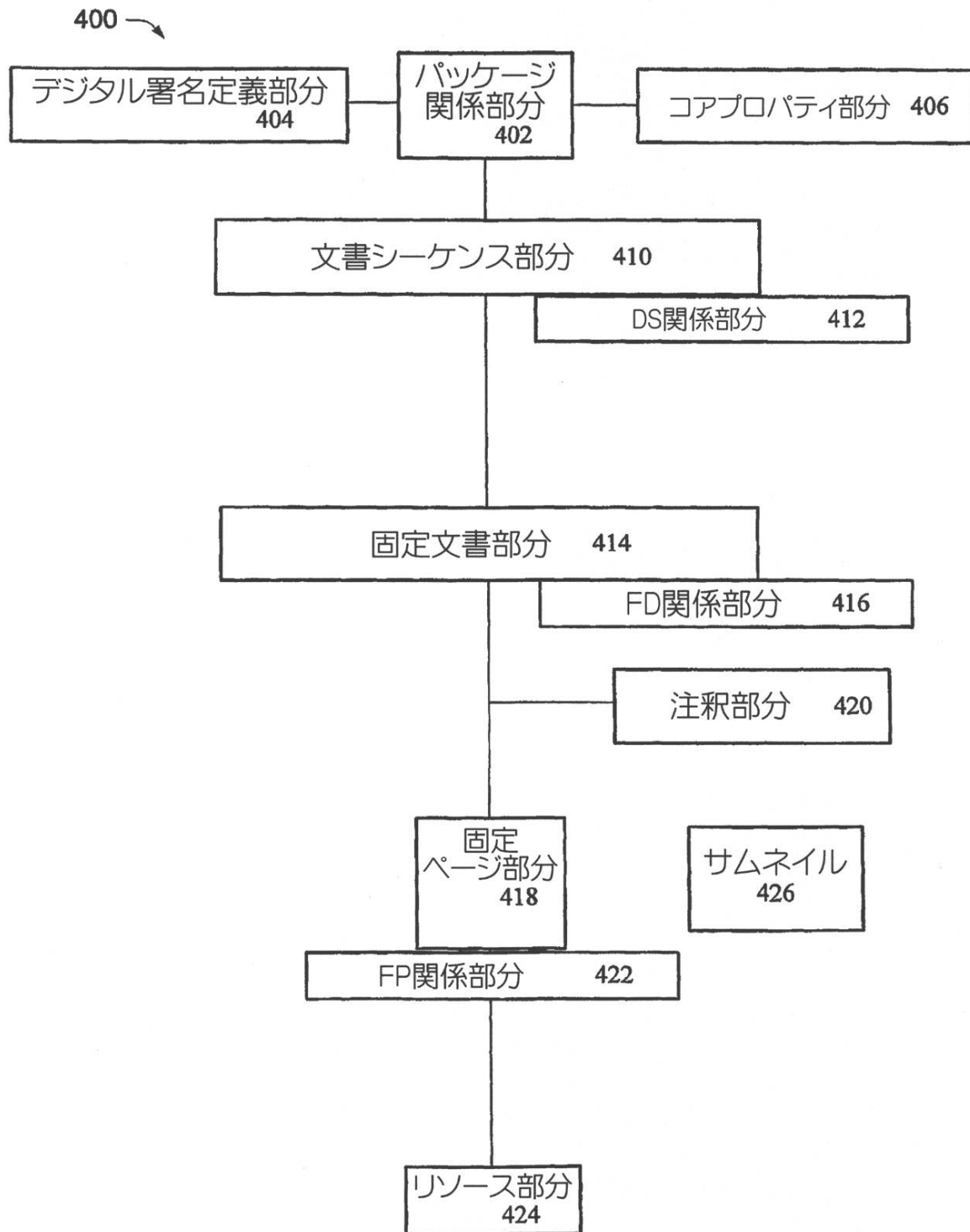
【図 2】



【図 3】



【図4】

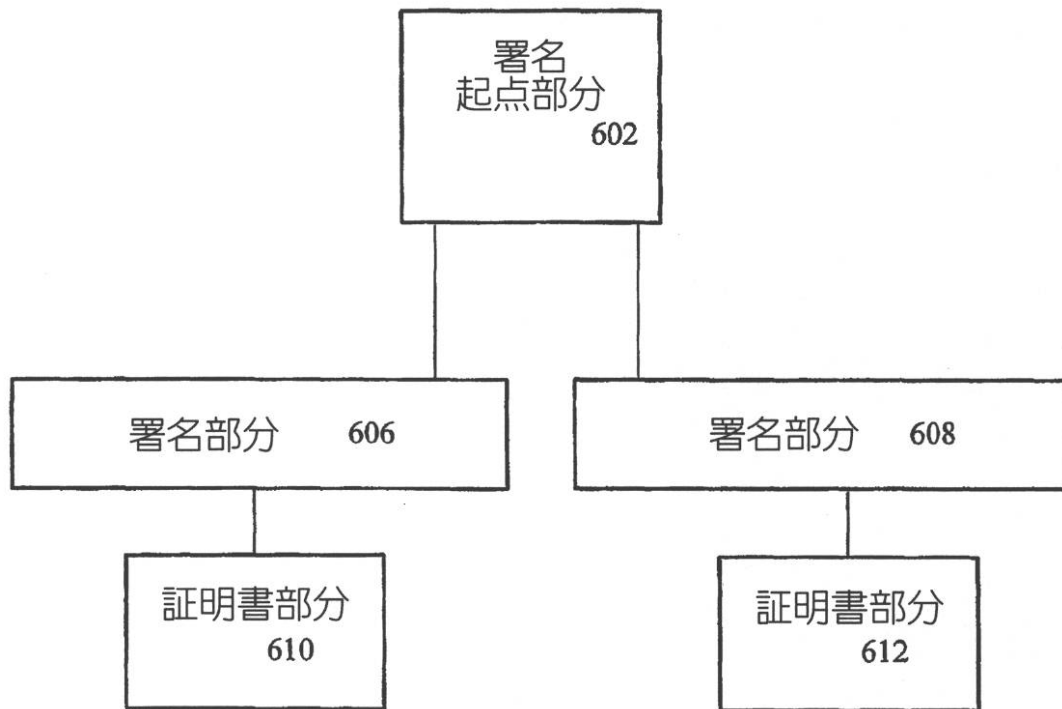


【図5】

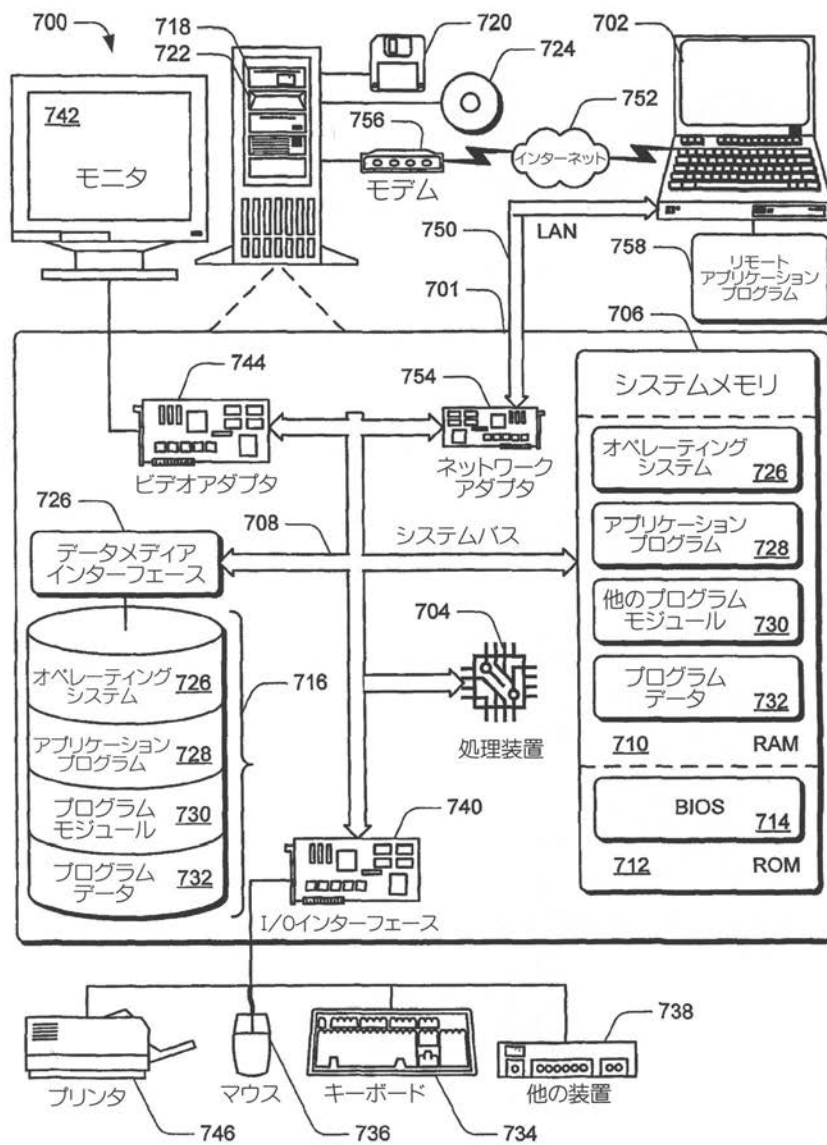
500 →

	コアプロパティ部分が 存在する 506	コアプロパティ部分が 存在しない 508
署名側ユーザが コアプロパティの 変更を可能にする ことを望む 502	コアプロパティ部分を 未署名のままにする 510	コアプロパティ部分を 作成する 512
署名側ユーザが コアプロパティの 変更を可能にする ことを望まない 504	コアプロパティ部分に 署名する 514	コアプロパティ部分を 作成しない 516

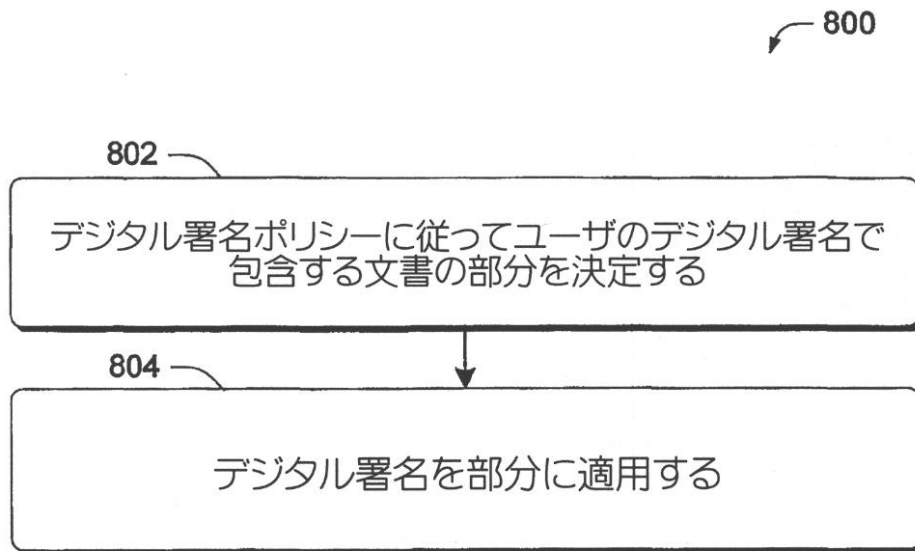
【図 6】



【図 7】



【図 8】



フロントページの続き

(72)発明者 デ・メッロ, マルシオ

アメリカ合衆国ワシントン州 9 8 0 5 2, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ

(72)発明者 ドハラ, マハムード・エイ

アメリカ合衆国ワシントン州 9 8 0 5 2, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ

審査官 松平 英

(56)参考文献 特開平 0 2 - 2 9 1 0 4 3 (J P , A)

特開 2 0 0 5 - 1 8 2 5 4 6 (J P , A)

特表 2 0 0 4 - 5 3 7 0 9 4 (J P , A)

特表 2 0 0 2 - 5 0 1 2 2 7 (J P , A)

特表 2 0 0 9 - 5 0 8 4 0 6 (J P , A)

特開平 0 8 - 0 7 7 1 1 7 (J P , A)

特開平 1 0 - 0 4 0 1 0 0 (J P , A)

特開 2 0 0 1 - 1 6 7 0 8 6 (J P , A)

特開 2 0 0 2 - 0 9 1 2 9 9 (J P , A)

特開 2 0 0 5 - 0 5 1 7 3 4 (J P , A)

Jerry Duniets - XML Paper Specification, [online], 2 0 0 5 年 8 月 8 日, p.1, [平成 2 4 年 3 月 2 1 日検索], インターネット<URL: <http://channel9.msdn.com/Blogs/scobleizer/Jerry-Dunietz-XML-Paper-Specification>>XML Paper Specification(XPS) - Windows Vista(Longhorn), [online], 2 0 0 5 年 7 月 3 0 日, p.1, [平成 2 4 年 3 月 2 1 日検索], インターネット<URL: [http://www.ailight.jp/Blog/sha256/archive/2005/7/30/XML%20Paper%20Specification%20\(XPS\)%20-%20Windows%20Vista%20\(Longhorn\)>](http://www.ailight.jp/Blog/sha256/archive/2005/7/30/XML%20Paper%20Specification%20(XPS)%20-%20Windows%20Vista%20(Longhorn)>)>

北野 宗之 他, Word 2 0 0 3 XML 文書への情報ハイディングシステム, 情報処理学会研究報告, 日本, 社団法人情報処理学会, 2 0 0 5 年 7 月 2 1 日, Vol. 2 0 0 5 No. 7 0, p. 2 0 5 ~ 2 1 2

マクラフリン プレット, Java & XML 第 2 版, 株式会社オライリー・ジャパン, 2 0 0 2 年 5 月 2 5 日, 初版, p. 5 3 9 ~ 5 4 0

斎藤 伸雄, 中央省庁における電子公文書の標準化に関する検討, 情報処理学会研究報告, 日本, 社団法人情報処理学会, 1 9 9 8 年 7 月 1 7 日, Vol. 9 8 No. 5 9, p. 3 9 ~ 4 6

金井 洋一 他, 原本性保証電子保存システム(Trusty Cabinet TM)の開発, R I C O H T E C H N I C A L R E P O R T, 株式会社リコー, 2 0 0 0 年 1 1 月 3 0 日, NO. 2 6, p.97-103

(58)調査した分野(Int.Cl., DB名)

G 0 9 C 1 / 0 0

H 0 4 L 9 / 0 0

G 0 6 F 2 1 / 2 0

G 0 6 Q 5 0 / 0 0