

(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2006-24218

(P2006-24218A)

(43) 公開日 平成18年1月26日(2006.1.26)

(51) Int. Cl.

G06F 12/00 (2006.01)

F I

G06F 12/00 533F

テーマコード (参考)

5B082

審査請求 未請求 請求項の数 31 O L (全 31 頁)

(21) 出願番号 特願2005-198824 (P2005-198824)
 (22) 出願日 平成17年7月7日(2005.7.7)
 (31) 優先権主張番号 887, 998
 (32) 優先日 平成16年7月9日(2004.7.9)
 (33) 優先権主張国 米国 (US)

(71) 出願人 000006747
 株式会社リコー
 東京都大田区中馬込1丁目3番6号
 (74) 代理人 100070150
 弁理士 伊東 忠彦
 (72) 発明者 グレグ ウォルフ
 アメリカ合衆国、カリフォルニア 940
 25, メンロ・パーク, サンド・ヒル・ロ
 ード 2882番, スイート 115 リ
 コー イノベーション インク内
 (72) 発明者 カート ダブリュー ピアソル
 アメリカ合衆国、カリフォルニア 940
 25, メンロ・パーク, サンド・ヒル・ロ
 ード 2882番, スイート 115 リ
 コー イノベーション インク内
 Fターム(参考) 5B082 GB01 GB07

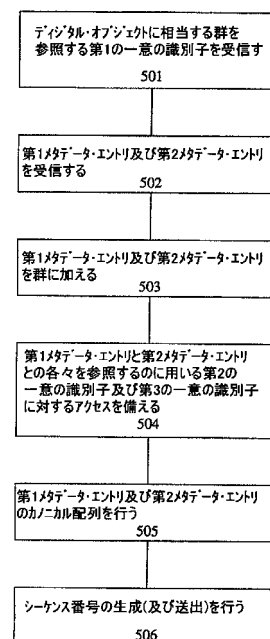
(54) 【発明の名称】 情報処理方法、情報処理装置、情報処理システム並びに記録媒体

(57) 【要約】

【課題】 配布される作品を同期化させる方法及び装置を開示する。

【解決手段】 一実施例では、方法は、第1メタデータ・エントリ並びに第2メタデータ・エントリを受信する工程、第1メタデータ・エントリ並びに第2メタデータ・エントリをデジタル・オブジェクトに相当する群に加える工程、及び第1メタデータ・エントリ並びに第2メタデータ・エントリ各々を参照するのに用いる第1の一意の識別子並びに第2の一意の識別子に対するアクセスを備える工程を備え、第1の一意の識別子並びに第2の一意の識別子は、第1のメタデータ・エントリのコンテンツ及び第2のメタデータ・エントリのコンテンツ各々に基づくものである。

【選択図】 図5



【特許請求の範囲】**【請求項 1】**

情報処理方法であって、

第 1 メタデータ・エントリと第 2 メタデータ・エントリとを受信する工程と、

該第 1 メタデータ・エントリと該第 2 メタデータ・エントリとをデジタル・オブジェクトに相当する群に加える工程と、

該第 1 メタデータ・エントリと該第 2 メタデータ・エントリとの各々を参照するのに用いる第 1 の一意の識別子と第 2 の一意の識別子とに対するアクセスを備える工程とを備え、該第 1 の一意の識別子と該第 2 の一意の識別子が、該第 1 のメタデータ・エントリのコンテンツと該第 2 のメタデータ・エントリのコンテンツとの各々に基づいていることを特徴とする情報処理方法。

10

【請求項 2】

コンピュータによって実行される場合に該コンピュータに情報処理方法を行わせる命令を記憶する記録可能な媒体であって、該情報処理方法が、

第 1 メタデータ・エントリと第 2 メタデータ・エントリとを受信する工程と、

該第 1 メタデータ・エントリと該第 2 メタデータ・エントリとをデジタル・オブジェクトに相当する群に加える工程と、

該第 1 メタデータ・エントリと該第 2 メタデータ・エントリとの各々を参照するのに用いる第 1 の一意の識別子と第 2 の一意の識別子とに対するアクセスを備える工程とを備え、該第 1 の一意の識別子と該第 2 の一意の識別子が、該第 1 のメタデータ・エントリのコンテンツと該第 2 のメタデータ・エントリのコンテンツとの各々に基づいていることを特徴とする媒体。

20

【請求項 3】

情報処理システムであって、

第 1 メタデータ・エントリと第 2 メタデータ・エントリとを受信する入力と、

該第 1 メタデータ・エントリと該第 2 メタデータ・エントリとをデジタル・オブジェクトに相当する群に加える文書処理装置と、

該第 1 メタデータ・エントリと該第 2 メタデータ・エントリとを記憶させるメモリと、

該メモリに結合されて、該第 1 メタデータ・エントリと該第 2 メタデータ・エントリとの各々を参照するのに用いる第 1 の一意の識別子と第 2 の一意の識別子とに対するアクセスを備えるアクセス処理装置とを備え、該第 1 の一意の識別子と該第 2 の一意の識別子が、該第 1 のメタデータ・エントリのコンテンツと該第 2 のメタデータ・エントリのコンテンツとの各々に基づいていることを特徴とする情報処理システム。

30

【請求項 4】

情報処理装置であって、

第 1 メタデータ・エントリと第 2 メタデータ・エントリとを受信する手段と、

該第 1 メタデータ・エントリと該第 2 メタデータ・エントリとをデジタル・オブジェクトに相当する群に加える手段と、

該第 1 メタデータ・エントリと該第 2 メタデータ・エントリとを記憶させる記憶手段と

40

、
前記記憶手段に記憶された該第 1 メタデータ・エントリと該第 2 メタデータ・エントリとの各々を参照するのに用いる第 1 の一意の識別子と第 2 の一意の識別子とに対するアクセスを備える手段とを備え、該第 1 の一意の識別子と該第 2 の一意の識別子が、該第 1 のメタデータ・エントリのコンテンツと該第 2 のメタデータ・エントリのコンテンツとの各々に基づいていることを特徴とする情報処理装置。

【請求項 5】

情報処理方法であって、

デジタル・オブジェクトに相当する群を参照する第 1 の一意の識別子を送る工程と、

該群におけるメタデータ・エントリ毎の、シーケンス番号と第 1 の一意の識別子との対を受信する工程とを備えることを特徴とする情報処理方法。

50

【請求項 6】

コンピュータによって実行される場合に該コンピュータに情報処理方法を行わせる命令を記憶する記録可能な媒体であって、該情報処理方法が、

デジタル・オブジェクトに相当する群を参照する第 1 の一意の識別子を送る工程と、
該群におけるメタデータ・エントリ毎の、シーケンス番号と一意の識別子との対を受信する工程とを備えることを特徴とする媒体。

【請求項 7】

情報処理装置であって、

デジタル・オブジェクトに相当する群を参照する第 1 の一意の識別子を送る処理装置と、

該処理装置に結合されて、該群におけるメタデータ・エントリ毎の、シーケンス番号と第 1 の一意の識別子との対を受信する入力装置とを備えることを特徴とする情報処理装置。

【請求項 8】

情報処理装置であって、

デジタル・オブジェクトに相当する群を参照する第 1 の一意の識別子を送る手段と、
該群におけるメタデータ・エントリ毎の、シーケンス番号と一意の識別子との対を受信する手段とを備えることを特徴とする情報処理装置。

【請求項 9】

情報処理方法であって、

デジタル・オブジェクトに相当する動的に修正可能なメタデータ・エントリ群に対してアクセスする工程を備え、該メタデータ・エントリ群は第 1 のメタデータ・エントリ及び第 2 のメタデータ・エントリを備え、更に、

更なるメタデータ・エントリを該エントリ群に基準に基づいて加えるよう、アクセスを制限する工程を備えることを特徴とする情報処理方法。

【請求項 10】

コンピュータによって実行される場合に該コンピュータに情報処理方法を行わせる命令を記憶する記録可能な媒体であって、該情報処理方法が、

デジタル・オブジェクトに相当する動的に修正可能なメタデータ・エントリ群に対してアクセスする工程を備え、該メタデータ・エントリ群は第 1 のメタデータ・エントリ及び第 2 のメタデータ・エントリを備え、該情報処理方法が更に、

更なるメタデータ・エントリを該エントリ群に基準に基づいて加えるよう、アクセスを制限する工程を備えることを特徴とする媒体。

【請求項 11】

情報処理装置であって、

デジタル・オブジェクトに相当する動的に修正可能なメタデータ・エントリ群に対してアクセスする手段を備え、該メタデータ・エントリ群は第 1 のメタデータ・エントリ及び第 2 のメタデータ・エントリを備え、更に、

更なるメタデータ・エントリを該エントリ群に基準に基づいて加えるよう、アクセスを制限する手段を備えることを特徴とする情報処理装置。

【請求項 12】

情報処理方法であって、

サーチの範囲がハッシュ値と、該サーチのコンテキストとを規定することによって定義される、コンテンツのサーチ要求を受信する工程と、

該サーチを行う工程とを備えることを特徴とする情報処理方法。

【請求項 13】

コンピュータによって実行される場合に該コンピュータに情報処理方法を行わせる命令を記憶する記録可能な媒体であって、該情報処理方法が、

サーチの範囲がハッシュ値と、該サーチのコンテキストとを規定することによって定義される、コンテンツのサーチ要求を受信する工程と、

10

20

30

40

50

該サーチを行う工程とを備えることを特徴とする媒体。

【請求項 14】

情報処理装置であって、

サーチの範囲がハッシュ値と、該サーチのコンテキストとを規定することによって定義される、コンテンツのサーチ要求を受信する入力と、

該サーチを行う処理装置とを備えることを特徴とする情報処理装置。

【請求項 15】

情報処理装置であって、

サーチの範囲がハッシュ値と、該サーチのコンテキストとを規定することによって定義される、コンテンツのサーチ要求を受信する手段と、

該サーチを行う手段とを備えることを特徴とする情報処理装置。

【請求項 16】

情報処理方法であって、

ディジタル・オブジェクトから計算される第 1 の一意の識別子を受信する工程を備え、該ディジタル・オブジェクトに相当する群が少なくとも、第 1 メタデータ・エントリと第 2 メタデータ・エントリとを有し、更に、

該ディジタル・オブジェクトと、該第 1 メタデータ・エントリと、該第 2 メタデータ・エントリとのうちの少なくとも 1 つを、該ディジタル・オブジェクトのコンテンツの関数である暗号化鍵を用いて暗号化する工程を備えることを特徴とする情報処理方法。

【請求項 17】

コンピュータによって実行される場合に該コンピュータに情報処理方法を行わせる命令を記憶する記録可能な媒体であって、該情報処理方法が、

ディジタル・オブジェクトから計算される第 1 の一意の識別子を受信する工程を備え、該ディジタル・オブジェクトに相当する群が少なくとも、第 1 メタデータ・エントリと第 2 メタデータ・エントリとを有し、該情報処理方法が更に、

該ディジタル・オブジェクトと、該第 1 メタデータ・エントリと、該第 2 メタデータ・エントリとのうちの少なくとも 1 つを、該ディジタル・オブジェクトのコンテンツの関数である暗号化鍵を用いて暗号化する工程を備えることを特徴とする媒体。

【請求項 18】

情報処理装置であって、

ディジタル・オブジェクトから計算される第 1 の一意の識別子を受信する入力装置を備え、該ディジタル・オブジェクトに相当する群が少なくとも、第 1 メタデータ・エントリと第 2 メタデータ・エントリとを有し、更に、

該ディジタル・オブジェクトと、該第 1 メタデータ・エントリと、該第 2 メタデータ・エントリとのうちの少なくとも 1 つを、該ディジタル・オブジェクトのコンテンツの関数である暗号化鍵を用いて暗号化する暗号化装置を備えることを特徴とする情報処理装置。

【請求項 19】

情報処理装置であって、

ディジタル・オブジェクトから計算される第 1 の一意の識別子を受信する手段を備え、該ディジタル・オブジェクトに相当する群が少なくとも、第 1 メタデータ・エントリと第 2 メタデータ・エントリとを有し、更に、

該ディジタル・オブジェクトと、該第 1 メタデータ・エントリと、該第 2 メタデータ・エントリとのうちの少なくとも 1 つを、該ディジタル・オブジェクトのコンテンツの関数である暗号化鍵を用いて暗号化する手段を備えることを特徴とする情報処理装置。

【請求項 20】

情報処理方法であって、

ディジタル・オブジェクトに相当する、動的に修正可能な 1 つ又は複数のエントリ群を保持する工程を備え、動的に修正可能なログを保持する工程が、

識別子を、該ディジタル・オブジェクトのコンテンツに基づいて計算する工程と、

暗号化を、該識別子を暗号化鍵として用いて行う工程とを備えることを特徴とする情報

10

20

30

40

50

処理方法。

【請求項 2 1】

コンピュータによって実行される場合に該コンピュータに情報処理方法を行わせる命令を記憶する記録可能な媒体であって、該情報処理方法が、

デジタル・オブジェクトに相当する、動的に修正可能な1つ又は複数のエントリ群を保持する工程を備え、動的に修正可能なログを保持する工程が、

識別子を、該デジタル・オブジェクトのコンテンツに基づいて計算する工程と、

暗号化を、該識別子を暗号化鍵として用いて行う工程とを備えることを特徴とする媒体

。

【請求項 2 2】

情報処理装置であって、

デジタル・オブジェクトに相当する、動的に修正可能な1つ又は複数のエントリ群を保持するメモリと、

情報処理方法を行う処理装置を備え、該情報処理方法が、

識別子を該デジタル・オブジェクトのコンテンツに基づいて計算する工程と、

暗号化を、該識別子を暗号化鍵として用いて行う工程とを備えることを特徴とする情報処理装置。

【請求項 2 3】

情報処理装置であって、

デジタル・オブジェクトに相当する、動的に修正可能な1つ又は複数のエントリ群を保持する情報処理方法を行う手段を備え、動的に修正可能なログを保持する情報処理方法が、

識別子を該デジタル・オブジェクトのコンテンツに基づいて計算する工程と、

暗号化を、該識別子を暗号化鍵として用いて行う工程を備えることを特徴とする情報処理装置。

【請求項 2 4】

情報処理方法であって、

デジタル・オブジェクトに相当する群を参照する第1の一意の識別子を受信する工程と、

第1メタデータ・エントリと第2メタデータ・エントリとを受信する工程とを備え、該第1メタデータ・エントリは売り手による売り出し物件の記述に相当し、該第2メタデータ・エントリは該第1メタデータ・エントリに関する追加情報を取得し、

更に、該第1メタデータ・エントリと該第2メタデータ・エントリとを該群に加える工程と、

該第1メタデータ・エントリと該第2メタデータ・エントリとの各々を参照するのに用いる第2の一意の識別子と第3の一意の識別子とに対するアクセスを備える工程とを備え、該第2の一意の識別子と該第3の一意の識別子が、該第1メタデータ・エントリのコンテンツと該第2メタデータ・エントリのコンテンツとの各々に基づいていることを特徴とする情報処理方法。

【請求項 2 5】

コンピュータによって実行される場合に該コンピュータに情報処理方法を行わせる命令を記憶する記録可能な媒体であって、該情報処理方法が、

デジタル・オブジェクトに相当する群を参照する第1の一意の識別子を受信する工程と、

第1メタデータ・エントリと第2メタデータ・エントリとを受信する工程とを備え、該第1メタデータ・エントリは売り手による売り出し物件の記述に相当し、該第2メタデータ・エントリは該第1メタデータ・エントリに関する追加情報を取得し、

該情報処理方法が更に、該第1メタデータ・エントリと該第2メタデータ・エントリとを該群に加える工程と、

該第1メタデータ・エントリと該第2メタデータ・エントリとの各々を参照するのに用

10

20

30

40

50

いる第2の一意の識別子と第3の一意の識別子とに対するアクセスを備える工程とを備え、該第2の一意の識別子と該第3の一意の識別子が、該第1メタデータ・エントリのコンテンツと該第2メタデータ・エントリのコンテンツとの各々に基づいていることを特徴とする媒体。

【請求項26】

情報処理装置であって、

デジタル・オブジェクトに相当する群を参照する第1の一意の識別子を受信し、第1メタデータ・エントリと第2メタデータ・エントリとを受信する入力装置を備え、該第1メタデータ・エントリは売り手による売り出し物件の記述に相当し、該第2メタデータ・エントリは該第1メタデータ・エントリに関する追加情報を取得し、

10

更に、該第1メタデータ・エントリと該第2メタデータ・エントリとを該群に加える処理装置と、

該第1メタデータ・エントリと該第2メタデータ・エントリとの各々を参照するのに用いる第2の一意の識別子と第3の一意の識別子とに対するアクセスを備えるアクセス処理装置とを備え、該第2の一意の識別子と該第3の一意の識別子が、該第1メタデータ・エントリのコンテンツと該第2メタデータ・エントリのコンテンツとの各々に基づいていることを特徴とする情報処理装置。

【請求項27】

情報処理装置であって、

デジタル・オブジェクトに相当する群を参照する第1の一意の識別子を受信する手段と、

20

第1メタデータ・エントリと第2メタデータ・エントリとを受信する手段とを備え、該第1メタデータ・エントリは売り手による売り出し物件の記述に相当し、該第2メタデータ・エントリは該第1メタデータ・エントリに関する追加情報を取得し、

更に、該第1メタデータ・エントリと該第2メタデータ・エントリとを該群に加える手段と、

該第1メタデータ・エントリと該第2メタデータ・エントリとの各々を参照するのに用いる第2の一意の識別子と第3の一意の識別子とに対するアクセスを備える手段とを備え、該第2の一意の識別子と該第3の一意の識別子が、該第1メタデータ・エントリのコンテンツと該第2メタデータ・エントリのコンテンツとの各々に基づいていることを特徴とする情報処理装置。

30

【請求項28】

オンライン・オークションにおける入札の情報処理方法であって、

デジタル・オブジェクトに相当する群に加える対象のメタデータを作成する工程を備え、該メタデータは、ネットワーク化された環境に接続されていない状態でありながら作成され、

更に、該メタデータを、ネットワーク化された環境に接続されていない状態でありながら記憶させる工程と、

該メタデータを該群に、ネットワーク化された環境に接続されている場合に送る工程とを備えることを特徴とする情報処理方法。

40

【請求項29】

情報処理方法であって、

第1検証ハッシュ値を作成する工程と、

該第1検証ハッシュを第1文書ログに加える工程と、

該第1文書ログに加える対象のコメントに対する第2検証ハッシュ値を作成する工程と、

該第2検証ハッシュ値を該第1文書ログに加える工程と、

該第1文書ログを参照する、第2文書ログにおけるエントリを、該第1文書ログにおけるエントリの該第2検証ハッシュ値を含めることによって作成する工程と、

該第1文書ログにおけるエントリを、該第2検証ハッシュ値を含む、前記第2文書にお

50

けるエントリをアクセスすることによって検証する工程とを備えることを特徴とする情報処理方法。

【請求項 3 0】

コンピュータによって実行される場合に該コンピュータに情報処理方法を行わせる命令を記憶する記録可能な媒体であって、該情報処理方法が、

第 1 検証ハッシュ値を作成する工程と、

該第 1 検証ハッシュを第 1 文書ログに加える工程と、

該第 1 文書ログに加える対象のコメントに対する第 2 検証ハッシュ値を作成する工程と

、
該第 2 検証ハッシュ値を該第 1 文書ログに加える工程と、

該第 1 文書ログを参照する、第 2 文書ログにおけるエントリを、該第 1 文書ログにおけるエントリの該第 2 検証ハッシュ値を含めることによって作成する工程と、

該第 1 文書ログにおけるエントリを、該第 2 検証ハッシュ値を含む、前記第 2 文書におけるエントリをアクセスすることによって検証する工程とを備えることを特徴とする媒体

。

【請求項 3 1】

情報処理装置であって、

第 1 検証ハッシュ値を作成する手段と、

該第 1 検証ハッシュを第 1 文書ログに加える手段と、

該第 1 文書ログに加える対象のコメントに対する第 2 検証ハッシュ値を作成する手段と

、
該第 2 検証ハッシュ値を該第 1 文書ログに加える手段と、

該第 1 文書ログを参照する、第 2 文書ログにおけるエントリを、該第 1 文書ログにおけるエントリの該第 2 検証ハッシュ値を含めることによって作成する手段と、

該第 1 文書ログにおけるエントリを、該第 2 検証ハッシュ値を含む、前記第 2 文書におけるエントリをアクセスすることによって検証する手段とを備えることを特徴とする情報処理装置。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は一般的にデジタル・オブジェクトの配布の分野に関し、特にデジタル・オブジェクトに相当する情報を同期化させる情報処理方法に関する。

【背景技術】

【0 0 0 2】

何百万もの文書が毎日、やりとりされている。相当な労力や時間がこれらの文書のアドレス（所在）を指定するオーバーヘッドに費やされている。職場では、この相当な時間や労力が費用や経費の増加をもたらしている。

【発明の開示】

【発明が解決しようとする課題】

【0 0 0 3】

文書に関してよくみられる 1 つの課題に、配布されるデジタル・オブジェクトを同期化させることが含まれる。配布されるデジタル・オブジェクトを同期化させることはデジタル・オブジェクトを配置させることを伴う。デジタル・オブジェクトが文書を含む場合、そのような同期化は文書に相当する情報を連係させることを含み得る。例えば、複数の関係者が文書に関するコメントを作成する場合、コメントは、より良い理解を備えるか、文書の査読のより完全な状態を備えるよう配置及び/又は配列させる場合がある。

【0 0 0 4】

多くの文書管理システムが過去に提案され、導入されてきた。これらの文書管理システムは、文書を記憶させ、要求と応答との連係を処理するシステムを含む。しかし、これらのシステムは組織の境界をまたがるものでなく、必要な同期化を行うものでない。

10

20

30

40

50

【0005】

ウェブ・ログは情報を記録するのに用いるオンライン文書管理ツールである。ウェブ・ログは、クライアント・サーバのフレームワークを用いて、コンテンツを、ウェブ・ログをホスティングするサーバに加えるか、1つ又は複数のクライアント側から取り去ることを可能にする。1つのサーバが各ウェブ・ログをホスティングしているので、ウェブ・ログは通常、特定のHTTPの位置にアンカされている。

【課題を解決するための手段】

【0006】

本明細書及び特許請求の範囲では、配布されるデジタル・オブジェクトを同期化させる情報処理方法及び情報処理装置を開示している。一実施例では、該情報処理方法は、第1メタデータ・エントリ並びに第2メタデータ・エントリを受信する工程、該第1メタデータ・エントリ並びに該第2メタデータ・エントリをデジタル・オブジェクトに相当する群に加える工程、及び該第1メタデータ・エントリと該第2メタデータ・エントリとの各々を参照するのに用いる第1の一意の識別子並びに第2の一意の識別子に対するアクセスを備える工程を備え、該第1の一意の識別子並びに該第2の一意の識別子は、該第1メタデータ・エントリのコンテンツと該第2メタデータ・エントリの内容コンテンツとに基づくものである。

10

【発明を実施するための最良の形態】

【0007】

本発明は、以下に表す詳細説明と本発明の種々の実施例を示す添付図面とから更に全面的に分かることになる。しかし、それらは、本発明を特定の実施例に限定するものとして解されないこととし、説明及び理解の目的のためのものに過ぎない。

20

【実施例】

【0008】

任意のサイズのグループすなわち群までスケーリングする、デジタル・オブジェクト（例えば、文書）を中心としたデータを同期化させる情報処理方法及び情報処理装置。一実施例では、同期化は、本明細書及び特許請求の範囲では「文書ログ」と表す概念的フレームワークを用いて行われる。文書ログはウェブ・ログに類似している。文書ログは、ウェブ・ログをアンカするHTTPの位置ではなく、特定の文書にアンカされているという点でウェブ・ログとは異なっている。

30

【0009】

一実施例では、文書ログはログ・エントリを有する。個々のログ・エントリはメタデータから構成される。メタデータは、1人若しくは複数人、又は1つ若しくは複数の自動化システムによって入力される短いテキスト・メッセージ及び/又は任意のリンクを備え得る。この文書ログは配布させ得ることができる。一実施例では、文書ログはXMLとして配布される。

【0010】

ウェブ・ログのクライアント/サーバのフレームワークと違って、文書ログの配布及び処理は、ネットワークにおいて接続されているノード（例えば、装置、機器など）の間で分散される処理である。この処理は任意にスケーリングすることが可能である。1つのネットワーク化されている環境では、各ノードは最低限、ログ・エントリに対するキャッシング並びに同期化、及び他のノードとログ・エントリを交換する機能を備える。更に、ユーザ・インタフェース・ノード（例えば、クライアント）は、ログ・エントリと、アンカされている文書ログとのビューを、新たなエントリを追加する機構及び/又はリンクをたどる機構とともに備える。

40

【0011】

一実施例では、何れかの所定の文書ログ又は文書ログ群に対して、単一ノードが、ログ・エントリを同期化させる役割を果たすものとして指定される。この「同期化」ノードの役割は、ドメイン名を位置（IPアドレス）に変換するドメイン名サーバ（DNS）と同様に、配布されるデジタル・オブジェクトを同期化させるというものである。同期化ノードは

50

サーバであり得る。特に、同期化ノードは、文書ログ毎にエントリのカノニカル・オーダリング（正規順序）を備える。別の実施例では、そのような同期化は、単一のワークグループを処理することによって局所で行ってもよく、ルート・ドメイン名サーバに相当するウェブ・サービスを介してグローバルに行ってもよい。同じ同期化ノードを用いることに合意する２つのノードはその場合、エントリに対する同じカノニカル・オーダリングを有することに依拠することが可能である。

【００１２】

システムのアーキテクチャ及び動作を説明することに加えて、グローバルなランデブーポイントサービス（マルチキャストによるデータ送信サービス）を用いて取引を処理する情報処理方法及び情報処理装置を説明する。本質的に、文書に対するエントリのカノニカル・シーケンスにそのログ・エントリを加えさせたいその実体は、このサービスに対して取引手数料を支払う。支払いが受け取られた旨を示す表示が生成されると、ログ・エントリを加え得る。

10

【００１３】

一実施例では、文書ログは暗号化とともに用いられて第三者機関なしでセキュアな、文書の交換を備える。

【００１４】

併せて、文書ログ処理及び関連した処理は、バージョン追跡、柔軟なファイル共有、同期化などを含むコンテンツ管理及びコンテンツ配布に有用な基本構成ブロックを備える。既存の文書管理システム、ソース・コードのレポジトリ、又はこれらの目標を達成するうえでその他の既存の機構と違って、一実施例では、文書ログは、ソフトウェアのインストールも管理保守も何ら必要でない。更に、文書ログは、ユーザが効率的に協働するうえでの柔軟性を備える。

20

【００１５】

以下の記載では、多くの詳細を表して本発明をより徹底的に説明している。しかし、本発明をこれらの特定の詳細なしで実施し得るということは当業者に分かるものである。他の場合には、周知の構造及び装置を詳細に示すのではなく構成図形式で示して、本発明を分かりにくくすることがないようにしている。

【００１６】

以下の詳細説明の一部は、コンピュータ・メモリ内のデータ・ビットに対する演算のアルゴリズム及び記号表現によって表している。これらのアルゴリズムの記述及び表現は、データ処理の技術分野における当業者が自らの作品を他の当業者に最も効果的に伝えるうえで用いられている手段である。アルゴリズムは、本明細書及び特許請求の範囲においてかつ一般的には、所望の結果につながる首尾一貫した工程シーケンスとして考えられている。これらの工程は、物理的数量の物理的な操作を必要とするものである。必然的なものではないが通常は、これらの数量は、記憶や転送や合成や比較やその他の方法での操作を行うことができる電気信号又は磁気信号の形式を呈する。これらの信号をビット、値、要素、記号、文字、項、数などとして表すことが、主に慣例の理由で、場合によっては、好都合であることが明らかとなった。

30

【００１７】

しかし、これらや同様な用語は全て、適切な物理的数量と関連付けることとし、これらの数量に付される好都合な呼び名に過ぎない。以下の記載から明らかであるように別途記載しない限り、本願の記載を通じて、「処理」や「計算」や「算出」や「判定」や「表示」などの用語を利用する記載は、コンピュータ・システムのレジスタ内やメモリ内で物理的（電子的）数量として表されるデータを、操作して、コンピュータ・システムのメモリ内若しくはレジスタ内又は他のそのような情報記憶装置、情報伝送装置又は情報表示装置に変換する、コンピュータ・システム又は同様な電子計算機装置の動作及び処理を表す。

40

【００１８】

本発明は、本明細書及び特許請求の範囲記載の処理を行う装置にも関する。この装置は、必要な目的で特別に構成されてもよく、コンピュータにおいて記憶されているコンピュ

50

ータ・プログラムによって選択的に起動されるか再構成される汎用コンピュータを備えてもよい。そのようなコンピュータ・プログラムは、電子的な命令を記憶させるのに適しており、その各々がコンピュータ・システム・バスに結合されている、フロッピー（登録商標）・ディスク、光ディスク、CD-ROM及び光磁気ディスクを含む何れかの種類のディスク、読み取り専用メモリ（ROM）、ランダム・アクセス・メモリ（RAM）、EPROM、EEPROM、磁気カード若しくは光カード、又は何れかの種類の媒体に限定されないがそれらなどの、そのコンピュータ判読可能記憶媒体において記憶させ得る。

【0019】

本明細書及び特許請求の範囲記載のアルゴリズム及び表示は、何れの特定のコンピュータやその他の装置にも本来的に関係するものでない。種々の汎用システムを本明細書及び特許請求の範囲記載の教示によるプログラムとともに用いる場合もあり、必要な方法工程を行うよう、より専門的な装置を構築することが好都合であることが明らかになる場合もある。種々のこれらのシステムに必要な構造は以下の記載から明らかとなる。更に、本発明は何れの特定のプログラミング言語も参照して記載していない。なお、種々のプログラミング言語を用いて本明細書及び特許請求の範囲記載の本発明の教示を実施するのに用い得るということが分かる。

10

【0020】

マシン判読可能媒体は、マシン（例えば、コンピュータ）によって判読可能な形式における情報を記憶させるか伝送する何れかの機構を含む。例えば、マシン判読可能媒体は、読み取り専用メモリ（「ROM」）、ランダム・アクセス・メモリ（「RAM」）、磁気ディスク記憶媒体、光記憶媒体、フラッシュ・メモリ装置、伝搬信号（例えば、搬送波、赤外線信号、デジタル信号など）の電気形式や光形式や音響形式やその他の形式などを含む。

20

【0021】

一般的な文書ログ

ログ（例えば、文書ログ）は、デジタル・オブジェクトと、1つ又は複数のメタデータ群とからなる。デジタル・オブジェクトはバイト・シーケンスとして表すことが可能である。デジタル・オブジェクトは文書である場合があり、メタデータは文書と関連したコメント群に相当し得る。よって、文書毎に、その文書に関連したコメント群が存在する。コメントは、一般的にはテキスト列からなり、それ自体が文書である場合があり、任意のバイト列からなり得る。コメントは、他の文書を表し得る単純なテキスト・エントリである場合があり、何れかの人又は何れかのものによって作成することが可能である。技術文書の草稿のコンテキストでは、コメント群は種々の査読者からの意見を表し得る。写真（例えば、jpegファイル）のコンテキストでは、コメント群は、誕生日パーティーなどの、写真に描かれるイベントに関する話を含み得る。患者のカルテのコンテキストでは、コメント群は、患者にとっての個々の予約又は訪問についての記載を含み得る。

30

【0022】

文書に関連したコメントのリストを交換し、（競合なしで）お互いにマージする手法が本明細書及び特許請求の範囲に記載されている。

【0023】

一実施例では、文書ログは、「アンカ」文書及びエントリ・リストを規定する単純なXML形式を用いて表す。例えば、単純なシンディケーション（RSS）形式などの形式を容易に適合させて同じ目的を果たすようにすることが可能である。

40

【0024】

一実施例では、交換機構を用いて、2つのノードがエントリ・リストを交換することを可能にする。一実施例では、ノードはHTTP GET方法を用いて文書ログに相当するXMLファイルを取り出し、HTTP POSTのコマンドを用いて（新たな）エントリを備えているXMLをノードに送る。本明細書及び特許請求の範囲の目的では、GETは、HTTPの一部として用いても用いなくても、ロケータに関連したコンテンツを取り出す動作を表すこととする。あるいは、単純なファイル複製処理を含む別の交換機構を用い得る。

【0025】

50

ノードは、個人が文書ログ・エントリを見て、このエントリに追加することを可能にするユーザ・インタフェースを含み得る。文書ログを見て追加する、多くのユーザ・インタフェースが考えられる。例示的なユーザ・インタフェースを図1に表す。図1を参照すれば、右側には画像101が表されており、左側には文書ログ・エントリ102が表されている。左側の最下部には、ユーザが新たなエントリを入力することを可能にするテキスト・ボックス103がある。

【0026】

図1は文書ログを見るためのプロトタイプ・ユーザ・インタフェースである。この例では、文書は（例えば、患者に相当する）画像であり、エントリはその患者に関する情報に相当する。このエントリは、予約や、手順の結果などの他の文書へのリンクと、それに関連したログを含む。よって、図1のユーザ・インタフェースは、患者情報を追跡するうえでの仮説的な利用を容易にする。図1の右側には、写真、この場合には患者の写真がある。ログ・エントリ102は患者に関連したエントリである。これらのエントリの一部は職員、医師、又は患者自身によって手入力され、その他のエントリは、スケジューリング・システム又はx線透視撮像マシンなどの関連システムによって自動的に作成される。そのような文書ログにおけるエントリ毎に、別の文書リンクに対するリンクをエントリに含み得る。関連文書の小サムネール104をそのエントリの右側に示す。

【0027】

一実施例では、カーソルの下にある「アクティブな」コメントは、単一リスト内の多くのコメントをすばやくブラウジングすることを可能にするフィッシュアイなどの視覚効果によって拡大される。1つの例示的なユーザ・インタフェースでは、マウス・カーソルの下にあるエントリ105は容易に視ることができるよう拡大される。当該例では、強調されたエントリはマシンによって当該技術分野において周知の方法で自動的に生成された場合がある。図示する文書ログの識別子は、この文書ログの印刷バージョン上のバー・コード又は別の機構を用いることによってマシンに入力された場合がある。元の文書ログに自動的に入力されたアイテムは、撮像マシンによって自動的に作成された撮像結果を含む文書ログに対するリンクを含む。何れかのエントリ102上をクリックすることによってユーザはそのエントリに関連した文書ログまで案内される。関連文書を指し示すリンクに関連付けられたコメント上をクリックすることによってユーザは文書と、参照される文書に関連付けられたログとのビューに案内される。図2は図1において強調されているコメントによって参照されたx線透視画像に関連したログのビューを示す。図2を参照すれば、x線マシンによって自動的に生成された文書及びその文書と関連付けられたコメントが示されている。

【0028】

一部の場合では、そのログは、元のログをもう一度指し示すエントリを有することになるが、多くの場合は、そのようなエントリを有しないことになる。このプロトタイプ・ビューアの最上部にあるナビゲーション・ツールは、標準的なウェブ・ブラウザと同様な前送り機能及び後送り機能を備える。

【0029】

画像に加えて、文書の種類は、ワードプロセッシング・ファイル、フラッシュ・ペーパー、エクセル・ファイル、テキスト文書やその他の種類のデータを含み得る。現行システムでは、何れかの単一のファイル（又は個々にアドレス指定可能な単位）を「文書」として用いることが可能である。

【0030】

位置としての文書

概念的には、文書ログは、仮想の空間又は仮想の（ファイル）階層を表し得る。空間の起点、すなわち「ルート」ノードは文書自体によって定義される。ディレクトリ名を用いて仮想空間の位置を規定することが可能である。しかし、一実施例では、ディレクトリ名を用いて位置を規定する代わりに、文書自体のハッシュ値を用いて仮想の空間上又は仮想のファイル階層上の文書の位置とコメントの位置とを規定する。例えば、/A/Cは、文書（

10

20

30

40

50

A=SHA1(a)であるa)に関するコメント(C=SHA1(c)であるc)を表し、その場合、SHA1は任意のバイト・シーケンスを固定サイズのシーケンスにマッピングするハッシュ関数である。すなわち、文字AはオブジェクトaのハッシュであるA=SHA1(a)を示すのに用いられ、その場合、Aは何れかのバイト・シーケンスを表す。例えば、列「This is a character string.」は、(16進表記を用いれば)「97d981dad06b03622cbf8e1a5642724cbcae64f8」にマッピングされる。

【0031】

この表現に関連した記憶機構は、例えば、Aをディレクトリ名とし、Cをaに関するコメントを含むファイルの名前とする標準的なディレクトリ構造であり得る。ハッシュ値を1次鍵として用いるデータベースなどのその他の記憶機構は同様にうまく機能することになり、何れかのノードが1つ又は複数のそのような記憶機構を用い得る。分かりにくい場合として、aの値自体が、パス又はユニフォーム・リソース・ロケータ(URL)として解釈することが可能な列である場合がある。a=「http://foo.com/path/to/file.ext」の場合、cが当該位置に関するコメントであるか、コンテンツが変わり得るウェブ・ページに関するコメントであるか、ある特定の時点でのそのウェブ・ページのコンテンツに関するコメントであるかが曖昧であり得る。このような場合には、(コンテンツのハッシュがある場合には)コンテンツのハッシュをアンカ文書として用いるほうが参照列のハッシュをアンカとして用いるよりも安全である。

【0032】

なお、aが列でありかつ有効なURLである場合、個々のノードは、列に関するコメントと、そのURLから得られた「既知の」コンテンツに関するコメントとを合成するよう選択し得る。なお慣例によって、aの文書ログは、aから入手可能であるコンテンツと、この特定のコンテンツに関連した文書ログへのポインタとの各々にエントリを含み得る。

【0033】

本明細書及び特許請求の範囲記載の目的で、一実施例では、文書は特定のバイト・シーケンスと同一である不変オブジェクトであり、文書のハッシュ値はその文書に対する参照として用いられる。文書の別々のバージョンは異なるハッシュ値を有するので、別々のバージョンは異なる文書としてみなす(慣例によって、D2が文書D1の新たなバージョンである場合、文書D1のログはD2を指し示すエントリを有することになり、D2のログはD1をもう一度指し示すエントリを有することになる)。

【0034】

特に、ハッシュ関数と、例えば、JPEGファイル、ワード文書、ポストスクリプト文書、テキスト列などの、ディレクトリ構造と利用に関しては、auは、http://www.server.com/path/a.jpg又はfile://path/to/a.jpgなどの、オブジェクトaの位置(例えば、URL)を示し、

a=GET(au)

である(aはauを参照解除した結果である)。

【0035】

AuはSHA1(GET(au))=Aである、位置群auを表すこととする。

【0036】

なお、AuはAの列表現を戻した位置を示す。

【0037】

新たな「仮想的な」SHA1プロトコルは：

A、B及びCと、それらに相当する値a、値b及び値cとの間の関係を表す、SHA1://host.name/A/B/C

として規定し得る。値bはaに関するコメント(又は文書ログのエントリ)である一方、cはbに関するコメントである。

【0038】

何れかのURLと同様に、GET(SHA1://host.name/A/B/C)がうまくいく場合、それによって、特定のコンテンツがバイト列として戻される。他のプロトコルと違って、このコンテン

10

20

30

40

50

ツはcであり、したがって、何れのホストについても同一であるのみならず、不変でもある。すなわち、SHA1(GET(SHA1://.../C))がcに等しくない場合、それはエラーである。よって、ノードは、cの複製を有する場合、GET(SHA1://.../C)を戻すうえでの通信を何ら行わなくてよい（クライアントがSHA1(c)を計算し、結果と何れかのルックアップ・テーブルとを、Cを鍵として用いて記憶させるということを仮定する）。

【0039】

なお、同じ画像ファイルをいくつかの場所で位置特定される場合があることと同様に、同じコメントがいくつかの文書に関する場合がある。Cがbに関するコメントである場合、SHA1:///A/B/CもSHA1:///B/Cも有効なURLである。コメントcは文書Xに関するコメントでもある場合があり、その場合には、SHA1:///X/Cも有効となる。この意味合いにおいて有効であるということは、何れかの人又は何れかの処理によって実際にcが文書xや文書bに関するコメントとして加えられたということを意味する。

10

【0040】

文書ログ・リスト

慣例によって、末尾のスラッシュを用いて、文書に関連したコメントのリストを示す。一実施例では、GET(SHA1://host.com/A/)はhost.comから（標準的なXML形式で）文書aに関するコメントのリストを戻す。同様に、SHA1://foo.com/A/はホストfoo.comからのリストを表す。/A/は、局所で既知のaに関するコメントに対する参照である。SHA1://host.com/A/Cはhost.comなどからのコメントaに関するコメントのリストを表す。

【0041】

H/A/Cのルック・アップを行う例示的なアルゴリズムは：

a)局所記憶機構にCがあるかを確認する（記憶機構はハッシュ・テーブル、データベース、ファイル・ディレクトリなどであり得る）。

【0042】

b)入手可能なものとして存在する場合、その関連した値を取得して、戻す（なお、群C/がルック・アップされている場合、関連した群を結果に加え、（任意的には）局所記憶機構にAがあるかを確認、見つかった場合には、関連したコメント群を取得する。）

c)コメントのハッシュを計算する

d)何れかのコメントがハッシュCを有する場合、そのコメントを戻す

e)（以下で処理される、URLに相当する列のハッシュでもあり得る）ドメイン名Hをルック・アップする

30

f)GET要求をHに対してA/Cとともに送る

g)結果を戻す（更に、任意的には有効なハッシュがあるかを確認する）

h)要求を1つ又は複数の予め構成されたサーバに送る（なお、サーバは、A又はaを取得するうえでの先行する位置であった場合がある）。

【0043】

i)Hが、aのURLのハッシュであるhである場合、aを戻すものである、通常のGET要求におけるそのURLを用いる、というものである。

【0044】

h/若しくはh.xml又はhに関する同様な標準的な変形をクライアントによってサーバに対するコメント（例えば、XMLファイル）のリストの要求として用いることが可能であり、それは、Cを計算するのに用いることが可能である（例えば、cがそのファイルにおけるエントリのうちの1つである場合）。

40

【0045】

クライアントは、Aをu1及びu2にマッピングするリストを保持している場合もあり、u1はクライアントがa（又はaに基づく情報）を得た位置群であり、u2は、aに関するコメント（例えば、XMLファイル）を含む位置である。別の実施例では、クライアントは、単にu2をルック・アップし、関連したコメント群を取り出し、Cを計算しようとする場合がある。

【0046】

50

SHA1：のURLとHTTP：のURLとのマッピング

一実施例では、クライアントは、特定のコンテンツから場所までの自らのマッピングを規定しており、保持している。例えば、rがリコー・イノベーション社のホームページのコンテンツであることとする。その場合、ruは、<http://www.rii.ricoh.com/>であり、R=（この例の場合、[index.html](http://www.rii.ricoh.com/index.html)=rのコンテンツ全体である「Welcome to RII」のハッシュ値である）'c2c0bfe479dd6da1d58ec4d0c42c5c7c10a1acfe'である。

【0047】

この場合、クライアントは以下のエントリを備えている内部テーブルを保持し得る。

【0048】

【表1】

10

SHA1 (R)	HTTP: (r _u)	備考
c2c0bfe479dd	http://www.rii.ricoh.com/	「元の」URL。(なお、この値はスペースを節減するよう切捨てられている。) 文書コンテンツの局所の複製 特定のウェブ・サイトと関連したコメントを見つける通常の場合 この文書上の既知のエントリの局所のリスト
	/cache/c2c0bfe479dd/file.html	
/c2c0bfe479dd/	http://www.rii.ricoh.com/rss.xml	
	/cache/c2c0bfe479dd/rss.xml	

20

なお、ハッシュ値は同じ長さのものでなくてよい。特に、より多くの、ハッシュ値のビットが規定されているほど、値はより「セキュアな」ものになる。したがって、本明細書及び特許請求の範囲において暗号化鍵Kをコンテンツ及び識別子に基づいているものとして記載し、識別子Iをコンテンツに基づいているものとして記載している場合、K及びIは、同じアルゴリズムの出力の別々の部分であり得るか、別々のアルゴリズムの出力であり得る。すなわち、Iがxのハッシュであっても、KがIのハッシュであるということである。同様に、Iは、同じハッシュ計算の最初の80ビットであり得るものであり、Kは、そのビット81乃至160であり得る。

30

【0049】

なお、Aがコンテンツaに対するアクセスを実際に有するうえで、文書ログに記憶するか、文書ログを処理するか、文書ログに提示するか加えるノード又はサーバに対する要件は何ら存在するものでない。しかし、慣例によって、文書のコンテンツのキャッシュ又は複製を実際に有するサーバ、例えばcache.com、の場合、<http://cache.com/A>などの、文書の要求に応じてそのコンテンツを備え、<http://cache.com/A>に応じてリスト・ログ・エントリを備えることが可能である。この場合、同じ文書を表すHTTP：のURLのパス構成部分とSHA1：のURLのパス構成部分は同一であり得る。

40

【0050】

個々のコメントを取り出すよう、クライアントは<http://cache.com/A/C>を要求し得る（この場合も又、cache.comは、aに対するアクセスを有しない場合でも、cにアクセスし、cを戻す場合がある。）。cが別の文書bを（例えば、[HREF=HTTP://foo.com/b.html](http://foo.com/b.html)であるので**bu**=[HTTP://foo.com/b.html](http://foo.com/b.html)である）位置によって表す場合、クライアントは、bを**bu**から取り出し、Bを計算し、Bに関連した文書ログ・エントリを、GET(SHA1://B/)を介して位置特定することができる場合がある。一実施例では、指定されない場合は規定値によ

50

って、クライアントは、ランデブーポイントサーバ、その局所キャッシュ、foo.com/b.html.xmlなどを含むいくつかの位置からのログ・エントリを検査し、統合する。

【0051】

当然、cはSHA1:URL(例えば、bu=SHA1:/B)によってそのリンクを規定する場合もあり、その場合には、クライアントは、既にbもbuの別のHTTP:のバージョンも有しているものでない場合に実際のコンテンツbをダウンロードする位置を識別する特定の機構を用いる。

【0052】

2つのノード間の同期化

一実施例では、個々のクライアントは、文書毎にエントリの局所キャッシュを保持する。これらはハッシュ・テーブルに記憶されている場合がある。局所キャッシュは、何れかのメモリ空間すなわち記憶場所であり得る。一実施例では、ハッシュ毎のエントリは2つの部分からなる。第1部分は、実際のコンテンツ自体を含む列及び/又は実際のコンテンツに対する1つ又は複数のポインタ(利用可能なものとして存在する場合)を含む列であり、第2部分は、この文書に関するコメントに相当するハッシュ値のリストである。クライアントは、エントリ・リストがあるかについて1つ又は複数の場所を確かめるよう構成することが可能である。一実施例では、デフォルト位置は、ランデブーポイントサーバ又は同期化サーバであり、それは、例えば、ユーザが文書を見る都度など、定期的に検査し得る。

【0053】

クライアントが追加のエントリ、例えば、GET処理の結果を得る場合、それらのエントリは局所キャッシュに加えられ(整合性検査を行ってコンテンツがハッシュ値に等しくなるようにする場合がある。)、局所エントリ・リストが、新たなエントリを反映するように更新される(同期化サーバから得られるシーケンス番号などの情報を用いて、提示するようこのリストを配列させ得る。)。

【0054】

なお、交換のシステムの一実施例におけるノードは対称である。クライアントとサーバとの唯一の違いは、クライアントが、通信、すなわちGETを用いたエントリ・リストの取り出し、又はHTTPPOSTを用いたリストの送出、を開始させるマシンとして定義されているという点である。当然、別々のノード(特に、サーバとしての役割を果たすもの)はそれらの構成においても、特に、特定のノード(クライアント)からのエントリを受け入れるか否かにおいて、異なる場合がある。

【0055】

ノードは別のノード(別のクライアント又はサーバ)との通信を把握し、「新たな」エントリのみを別のノードに(HTTPPOSTを介してかGETに応じて)送る場合がある。

【0056】

更に、同じ文書ログを参照する2つのXMLファイルのコンテンツを単に複製して単一のファイルに添付するなどの、別の交換プロトコルを用い得る。

【0057】

何れかのXML表現を文書ログ・エントリに用いることが可能である。図3は、文書Aに関連したログを表すXMLファイルの例示的な見取り図を示す。コンテンツ(「文書A上の第1コメント」)に加えて、各エントリは、エントリの発信元又は別のノードによって割り当て得るいくつかの属性を有する。図3では、SEQ属性はランデブーポイントサーバによって割り当てられる。このXML文書自体は、Aに関連した文書ログに対する照会に応じて戻されることになり、慣例によってこの照会は//rp.com/A/の形式を呈し、その場合、「rp.com」はランデブーポイントのホスト名である。(別のサーバ/ホストは、このリストのそれ自体のバージョンを戻すことになる。ランデブーポイントによって備えられるシーケンス番号は「カノニカルな(正規順序)」ものとして指定される。)なお、エントリ上のHREF属性はアンカのHREF属性、すなわち、アンカ! a href=... ? HTMLにおけるタグ、と同様な、別の文書に対するリンクを規定する。同様に、SRCタグはHTMLのIMGタ

グのSRC属性と類似のものであり、参照される文書を表すサムネール画像のソースを規定する。

【0058】

もう1つ考えられることとしては、既存の非常に単純なシンディケーション (Rich Site Summary) のスキーマを用いるということがある。RSSフィードのベース文書 (「アンカ」) を識別する、RSSに対する単純な拡張によって本明細書及び特許請求の範囲記載の利用が可能になる。あるいは、RSSを拡張するかわりに、RSSにおける既存フィールドを用い得る。

【0059】

コメントをマージすることが課題となっているが、これは、コメントがそのハッシュ値によって記憶されるからである。(テキスト) 値に加えて、例えば、著者及び日付などの属性はハッシュ値Cの計算に用いられる。

【0060】

図4は、特定の文書のランデブーポイントにエントリを提出するクライアントの構成を描いた図である。図4を参照すれば、この全体図はクライアントからランデブーポイントへのエントリの提出を示している。なお、一部のクライアントはエントリをランデブーポイントに直接ポスティングする場合がある一方、他のものは中間ノードを経由し得る。エントリはそのハッシュ値によって参照され、記憶されるので、何れかのノードは、競合を心配することなく、何れかの別のノードと直接エントリを交換することが可能である。個々のノードは自らの順序をエントリ・シーケンスに割り当てることも可能である。ランデブーポイントによって備えられる順序は、慣例によって、カノニカルオーダリングとして扱われる。なお、文書の元の作成者は、当初の! doc...? エレメントのルート属性すなわちrp属性を規定することによって、その文書に関連したログ・エントリのランデブーポイントすなわち「ルート」を規定し得る、しかし、文書ログは、必ずしも文書の作成者だけでなく、誰によっても作成し得る。(文書の作成者は、文書上に当初のログ・エントリを登録する最初の機会を有する。) 別のノードは、文書エレメントに規定されているルート属性を用いることを選んでも選ばなくてもよい。文書エントリはオフライン状態にある間に行い、そのエントリは1つ又は複数のサーバと後に自動的に同期化させ得る。

【0061】

ランデブーポイントが見るエントリのカノニカルオーダリングは、(特に一部のクライアントが作成時にオフライン状態にある場合に) 実際の作成順序とは異なり得る。更に、中間ノードは複数の別のノードからのエントリを集約して、提出する場合がある。

【0062】

ランデブーポイントのサーバ側では、一実施例においては、シーケンス番号が、受信された順番で割り当てられる。ユーザの識別情報(例えば、ポスティング権限)の別個の構成及び確認をいくつかの方法のうちの何れか1つにおいて処理することが可能である。これらは、ユーザ名並びにパスワードの検証、IPアドレスの検査、セッション識別子などを含む。暗号化コンテンツの一部の場合には、ユーザは、暗号化鍵A(及び/又はコンテンツa)が実際に分かっているということを(暗号手法によって)証明しなければならない場合がある。

【0063】

ランデブーポイント及びグローバル同期化

前述のように、上記のノードの配置は、分散化された、スケーラブルな、ピア・ツー・ピアの配置において文書ログを交換するうえで非常にうまく機能する。コメントはオフライン状態又はオンライン状態で作成し、局所の交換によって解決することが可能である。

【0064】

しかし、複数クライアント間で作品を連係しようとする場合に重大な問題が発生する場合がある。多くの場合、それらのクライアントはエントリの配列すなわち順序について合意しなければならない。同時作成と通信遅延時間との理由で、そのエントリの一意の配列を構成することが可能でない場合がある。その代わりに、各ノードは自らの一意の配列を

10

20

30

40

50

有し得る。

【0065】

一実施例では、本明細書及び特許請求の範囲においてランデブーポイント(RP.net)(RP.netは利用可能なものとして存在するドメイン名ではなく、単に例として用いている)として表すウェブ・サービスは、何れかの文書ログのグローバルな配列を備える。例えばPOST(http://RP.net/A/C)などのPOST要求に応じて、RP.netは、文書aのコンテキストでコメントcにシーケンス番号を割り当てる。GET要求に応じて、RP.netは、既知のコメントのリストによってGET(http://RP.net/A/)に応答し、コメント毎のシーケンス番号を規定する。

【0066】

ルート・ドメイン名サーバ以外のサーバがDNS関数を備えることが可能であるのと同様に、一実施例では、RP.net以外のサーバはシーケンス番号を備えることが可能である。しかし、1つのサービスのみが、シーケンス番号を割り当てるカノニカル・サービスとしての役割を果たすことが可能である。一実施例では、権限は別のサービスに委譲されるが、責任はRP.netの組織に残る。

【0067】

よって、サーバはメタデータ(例えば、コメント)と、デジタル・オブジェクト(例えば、コメントされる文書)に関するハッシュ又は別の値であり得る識別子とを受け入れ、一実施例では、サーバはシーケンス番号をそのメタデータ・エントリに割り当て、シーケンス番号及び関連したメタデータ・エントリの更新リストを公表する。サーバは、エントリのコンテンツ又は、エントリのコンテンツに基づいて計算された識別子を公表することが可能である。更に、一実施例では、サーバは公表リストをデジタル形式で署名する。

【0068】

図5は、同期化処理の一実施例の流れ図である。当該処理は、ハードウェア(回路、専用ロジックなど)、(汎用コンピュータ・システム上若しくは専用マシン上で実行する)ソフトウェア又は両方の組み合わせを備え得る処理ロジックによって行われる。

【0069】

図5を参照すれば、当該処理は、デジタル・オブジェクトに相当する群を参照する第1の一意の識別子を受信する処理ロジックによって開始される(処理ブロック501)。一実施例では、第1の一意の識別子がデジタル・オブジェクトのコンテンツに基づいて計算される。一実施例では、第1の一意の識別子は、デジタル・オブジェクトと関連した任意のバイト・シーケンスを固定サイズのシーケンスにマッピングするハッシュ関数を適用した結果であるハッシュ値である。あるいは、ハッシュ値は、ハッシュ関数をデジタル・オブジェクトのコンテンツに対して適用した結果である。

【0070】

なお、デジタル・オブジェクトは第1の一意の識別子によって索引付けされる場合がある。

【0071】

処理ロジックは、第1メタデータ・エントリ及び第2メタデータ・エントリも受信する(処理ブロック502)。なお、第1メタデータ・エントリのソースと第2メタデータ・エントリのソースは異なり得る。

【0072】

第1メタデータ・エントリと第2メタデータ・エントリとを受信した後、処理ロジックは第1メタデータ・エントリと第2メタデータ・エントリとを群に加える(処理ブロック503)。

【0073】

加えられると、処理ロジックは、第1メタデータ・エントリ及び第2メタデータ・エントリ各々を参照するのに用いる第2の一意の識別子及び第3の一意の識別子に対するアクセスを備える(処理ブロック504)。第2の一意の識別子及び第3の一意の識別子は、第

10

20

30

40

50

1のメタデータ・エントリのコンテンツ及び第2のメタデータ・エントリのコンテンツ各々に基づくものである。一実施例では、第2の一意の識別子及び第3の一意の識別子は、第1のメタデータ・エントリのコンテンツ及び第2のメタデータ・エントリのコンテンツ各々に基づいてハッシュ値を計算した結果である。

【0074】

一実施例では、第2の一意の識別子及び第3の一意の識別子に対するアクセスを備える工程は、第2の一意の識別子と第3の一意の識別子とのカノニカルオーダリングを送る工程を備える。別の実施例では、第2の一意の識別子及び第3の一意の識別子に対するアクセスを備える工程は、第2の一意の識別子及び第3の一意の識別子と関連したシーケンス番号を送る工程を備え、シーケンス番号の各々は、第2の一意の識別子及び第3の一意の識別子の1つのみに関連している。なお、コンテンツに基づいて計算される識別子を送るかわりに、コンテンツ自体を送ることが可能である。

10

【0075】

一実施例では、当該処理は更に本明細書及び特許請求の範囲記載のように、第1のメタデータ・エントリ及び第2のメタデータ・エントリのカノニカルオーダリングを行い（処理ブロック505）、シーケンス番号の生成（及び送出）を行う（処理ブロック506）。

【0076】

一実施例では、当該処理は更に、第1の一意の識別子及び第2の一意の識別子を指数として用いて第1のメタデータ・エントリ及び第2のメタデータ・エントリにアクセスする工程を備える。一実施例では、指数はハッシュ値である。

20

【0077】

一実施例では、第1メタデータ・エントリは売り手による売り出し物件の記述に相当し、第2メタデータ・エントリは物を購入する意思を表示する買い手からの表示に相当する。一実施例では、そのような場合には、図5の当該処理は更に、第1メタデータ・エントリと第2メタデータ・エントリとの一方又は両方を参照する情報を含む第3のメタデータ・エントリを受信する。図5の当該処理は、例えば、発送情報（例えば、発送日付、追跡番号、並びに受領日付）及び支払情報などの情報を含む、物を購入する取引に関する情報を含む第3メタデータ・エントリを（ソースすなわち、第1メタデータ及び第2メタデータを備える者以外の、例えば、エスクロウエージェントなどの関係者から）受信する工程も含み得る。

30

【0078】

一実施例では、図5の当該処理は更に、追加メタデータ・エントリの追加をエントリ群に、基準（例えば、文書上に公表されているメタデータ・エントリの数）に基づいて制限するアクセス制限処理を含む。一実施例では、アクセスを制限する工程は、更なるコメントを加える要求を拒否する工程によって行われる。別の実施例では、アクセスを制限する工程は、群に第2メタデータ・エントリを加える工程、手数料を課す工程、及び、第2メタデータ・エントリに関連したシーケンス番号の公表を、群における1つ又は複数のエントリに関連した1つ又は複数の別のシーケンス番号が公表される場合に、支払いが受領されたという表示を受領するまで妨げる工程によって行われる。そのようなアクセス制限処理は更に、更なるメタデータ・エントリの追加を妨げる一方で、群におけるエントリに相当するシーケンス番号を公表する工程を備え得る。アクセス制限処理は以下に更に詳細に説明する。

40

【0079】

一実施例では、図5の当該処理は更に、特定の暗号化処理を含む。暗号化処理は、デジタル・オブジェクトのハッシュを計算する工程及び、デジタル・オブジェクトのコンテンツの関数である暗号化鍵を用いてデジタル・オブジェクトと第2メタデータ・エントリとの一方又は両方を暗号化する工程を含み得る。一実施例では、暗号化鍵は、デジタル・オブジェクトのハッシュである。別の実施例では、暗号化鍵は、デジタル・オブジェクトの暗号化バージョンの関数である。一実施例では、暗号化はDESを用いて行われる。一実施例では、暗号化処理は、デジタル・オブジェクトのハッシュを暗号化鍵とし

50

て用いてDESアルゴリズムをデジタル・オブジェクトに適用することによってデジタル・オブジェクトの暗号化バージョンを作成する工程も含む。暗号化処理は以下に更に詳細に説明する。

【0080】

図6は、データ処理の一実施例の流れ図である。当該処理は、ハードウェア（回路、専用ロジックなど）、（汎用コンピュータ・システム上若しくは専用マシン上で実行されるような）ソフトウェア、又は両方の組み合わせを備え得る処理ロジックによって行われる。

【0081】

図6を参照すれば、当該処理は、デジタル・オブジェクトに相当する群を参照する第1の一意の識別子を送る処理ロジックによって開始される（処理ロジック601）。処理ロジックは更に、群におけるメタデータ・エントリ毎のシーケンス番号と一意の識別子との対を受信する（処理ブロック602）。一実施例では、当該対における一意の識別子はハッシュ値である。

【0082】

一実施例では、当該処理は更に、別の関係者から1つ又は複数の追加エントリを受信する工程（処理ブロック603）、追加エントリに対する一意の識別子を生成する工程（処理ブロック604）、及び生成された一意の識別子を受信された一意の識別子と比較して、群における1つ又は複数の追加エントリとその他のエントリとのカノニカルオーダリングを識別する工程（処理ブロック605）を備える。

【0083】

一実施例では、当該処理は更に、群における一意の識別子のうちの第1の一意の識別子の時間的位置を識別する工程を含み得る。

【0084】

ビジネス・モデル

ログ・エントリを特定の文書コンテンツに結びつけることによって、新たな取引上のビジネス・モデルの可能性がもたらされる。各識別子は空間に相当する。サーバは、個々のユーザが更新エントリを受け入れ、公表するうえで課金し得る。例えば、当初識別子及び特定数NのエントリがユーザAによって支払われていることとする。N番目のエントリの後、一実施例では、支払いが受領されるまでシーケンスがロックされる（シーケンス・リストはなお公表されているが、更新は何ら可能でない。）。ユーザBがエントリを登録しようとする場合、サーバは、追加の支払いが（A、B又は関心のあるその他の関係者から）受領されるまで要求を拒否する（か、割り当てられたシーケンス番号を公表しない）。

【0085】

特に、RP.netは「文書空間」単位で課金して新たなコメントを受け入れ、それをその空間に割り当てる。例えば、RP.netは最初の100の登録コメントに対して一料金（例えば、ゼロ）を課金し得る。その後、追加の登録によってある程度の少額費用がかかり得る。この料金は文書オーナー（例えば、第1エントリを加えた個人）によって支払われる可能性があり、コメント提出者（コメントを加えたい個人若しくは組織）又は関心のあるその他の関係者によって支払われる可能性がある。

【0086】

通常のシナリオでは、元の提出者は、例えば、誕生日パーティーの特定の写真に関する議論を開始したい場合がある。写真は友人に回覧され、最初の100のコメントに対してRP.netに支払いが行われる。結局は、興味を失い、もはやその議論を行いたくない場合がある。ある別の個人、例えば、上記誕生日の子どもの親が、自分たちの写真アルバムへのリンクを追加するほど単純なことを場合によっては行って、議論を継続したい場合がある。その親はその場合、101番目のコメントに対する支払いを行い得るものであり、101番目のコメントを登録し得る。当然、親は、単に、祖父母などの他の人達がコメントを出し続け、別のブロック（例えば、100）のコメントの登録に対する支払いを行うことを可能にしたい場合もある。

10

20

30

40

50

【 0 0 8 7 】

一実施例では、RP.netは現在登録されているコメントを無料で提供する。（当初のコメントに対して支払われる手数料は、本質的には、シーケンス番号と場合によっては共通コンテンツとを備える継続的な義務を備える。）このことは、既存のコメントを目に見えるかたちにさせて、このコメントを見る人々が自らのものを追加する需要（更にはそれに対する支払いを行う需要）を創出する。本明細書及び特許請求の範囲記載の暗号化手法とともに、このサービス及びビジネス・モデルは、公的文書及びコメント、更には私的文書及び私的コメントに同様にうまく機能する（全て、RP.netを何れかの私的情報によって認証させることなく、私的文書に関する公的コメントが存在し得るものであり、逆も同様である）。

10

【 0 0 8 8 】

このモデルに関する多くの別の変形が考えられる。最も明らかなものとしては、登録アクセスを文書単位及びユーザ/組織単位で制限することがある（例えば、文書ログにおける当初のコメントは、識別されているユーザ群にポスティング・アクセスを限定する情報である場合があるか、そのような構成情報は文書ログ機構自体の外で処理することが可能である）。

【 0 0 8 9 】

図7は、アクセス処理の一実施例の流れ図である。当該処理は、ハードウェア（回路、専用ロジックなど）、（汎用コンピュータ・システム上若しくは専用マシン上で実行されるような）ソフトウェア、又は両方の組み合わせを備え得る処理ロジックによって行われる。

20

【 0 0 9 0 】

図7を参照すれば、当該処理は、デジタル・オブジェクトに相当する動的に修正可能なメタデータ・エントリ群をアクセスする処理ロジックによって開始する（処理ブロック701）。メタデータ・エントリ群は、第1メタデータ・エントリ及び第2メタデータ・エントリを備える。

【 0 0 9 1 】

一実施例では、当該処理は、更なるコメントのシーケンス番号を含めることなく、群におけるエントリに相当するシーケンス番号を公表する処理ロジックを含む（処理ブロック702）。なお、これは必須でない。

30

【 0 0 9 2 】

メタデータ・エントリ群をアクセスした後、処理ロジックは、更なるメタデータ・エントリをエントリ群に基準に基づいて加えるよう、アクセスを制限する（処理ブロック703）。アクセスを制限する工程は、特定の基準が満たされるまで第2メタデータ・エントリを受け入れない工程を備えてもよく、更なるコメントを加える要求を拒否する工程を備えてもよい。

【 0 0 9 3 】

一実施例では、当該基準は、文書に関して登録されるメタデータ・エントリ数を備える。別の実施例では、当該基準は、更なるメタデータ・エントリが登録される予定の時点

40

【 0 0 9 4 】

一実施例では、アクセスを制限する工程は、第2メタデータ・エントリを群に加える工程、手数料を課金する工程、及び、第2メタデータ・エントリに関連したシーケンス番号の公表を、群における1つ又は複数のエントリに関連した1つ又は複数の別のシーケンス番号が公表される場合に、支払いが受信された旨の表示を受信するまで妨げる工程を含む。

【 0 0 9 5 】

一実施例では、アクセスを制限する工程は、アクセスに対する課金を行う工程、及び支払いが関係者から受信された旨の表示を受信した後、アクセスを許可する工程を含み得る。

【 0 0 9 6 】

50

フラッシュ・クライアント

図1及び図2に表す例は、ユーザ・インタフェース・クライアントのプラットフォームとしてマクロメディア社のフラッシュを用いている。フラッシュは、非常に高い携帯性を有し（非常に多くの数のプラットフォーム上で利用可能なものとして存在し）、（例えば、大きなリストにおけるエントリにズームインするなどの）動的な機能を含み、（テキストや画像のみならず、ビデオやオーディオや「フラッシュ」ペーパーも含む）多数の文書の種類をネイティブで表示する利点を有する。

【0097】

フラッシュ・プレイヤは、ブラウザの内部で実行し、局所のファイル・システムからセグメント化される局所キャッシュを保持する利点も有する。キャッシュによって、オフライン状態にある間に文書エントリを加え、このエントリを1つ又は複数のサーバと後に自動的に同期化させる機能を含む、スムーズなオンライン処理及びオフライン処理を可能にする。例として、例えばジャバスクリプトなどの、動的なスクリプトを備えているか備えていない標準的なHTMLを含む多くの別のクライアントが考えられる。

10

【0098】

暗号化文書

文書ログの1つの変形として、aのコンテンツを参照するうえでの1つの間接的な方法レベルを用いることがある。aに関する文書ログの起点として $A = \text{SHA1}(a)$ を用いる代わりに、 $AA = \text{SHA1}(\text{ENC}(a, A))$ を用い、その場合、 $A = \text{SHA1}(a)$ はaを符号化する暗号化鍵として用いる。ENCは、暗号化アルゴリズム、例えば、DESである。Aは、秘密を符号化し、Aをaと秘密コメントcとの暗号化鍵として用いる暗号化鍵として用いることも可能である。仮想プロトコルは本明細書及び特許請求の範囲ではcを表す $\text{DES}://A/AC$ として定義され、その場合ACは、DESアルゴリズムの適用において鍵Aを用いた、cの暗号化バージョンのハッシュである。（同様な表記をRSAやその他のアルゴリズムに用いることが可能である。）よって、 $\text{GET}(\text{SHA1}://AA/)$ は $\text{DES}://A/AA$ によって表すAの暗号化バージョンを戻す。 $\text{GET}(\text{DES}://A/AA)$ はaを戻すが、クライアントが既にAが分かっている場合のみ計算することが可能である。大半の場合、クライアントは、まずaを得て次にAを計算することによってAを得る。

20

【0099】

クライアントが、aを別のチャネルから取得し（例えば、文書を作成したか、それを添付として電子メールによって受信し）、Aの暗号化バージョンを実際に復号する必要が何らない場合には、しかし、Aを用いて、aに関連したコメントを暗号化し、復号することが可能であり、aに関連したコメントを暗号化し、復号する。Aに関する平文のテキスト・コメントをなお、 $\text{SHA1}://A/C$ として局所で記憶させることが可能である一方、クライアントは、何れかの別のノードと直接このコメントを交換したくないものである（クライアントは他の、潜在的に許可されていないノードにAを明らかにすべきでない）。その代わりに、クライアントは $\text{SHA1}://AA/C$ を交換する。すなわち、クライアントは、（Aを暗号化鍵として用いて）aの暗号化バージョンのハッシュに関するコメントを用い、交換する。秘密コメントは、コメント「位置」に対するAC（Aを暗号化鍵として用いたcの暗号化バージョンのハッシュ）を用いることによって用いることも可能である。

30

40

【0100】

このようにして、同じオブジェクト（例えば、電子メールの添付として交換したjpgファイルから、面と向かって伝達した秘密のパスフレーズまでの何れかのもの）を共有する二者は、そのオブジェクトに関して全く認証されていない第3者を介してセキュアに通信することが可能である。

【0101】

図8は暗号化処理の一実施例の流れ図である。当該処理は、ハードウェア（回路、専用ロジックなど）、（汎用コンピュータ・システム上若しくは専用マシン上で実行するものなどの）ソフトウェア、又は両方の組み合わせを備え得る処理ロジックによって行われる。

50

【0102】

図8を参照すれば、当該処理は、デジタル・オブジェクトから計算される第1の一意の識別子を受信する処理ロジックによって開始する（処理ブロック801）。群は少なくとも第1のメタデータ・エントリ及び第2のメタデータ・エントリを有する。

【0103】

デジタル・オブジェクトの識別子を用いて、処理ロジックは、デジタル・オブジェクトと、第1メタデータ・エントリと、第2メタデータ・エントリとのうちの少なくとも1つを、デジタル・オブジェクトのコンテンツの関数である暗号化鍵を用いて暗号化する（処理ブロック803）。一実施例では、暗号化鍵はデジタル・オブジェクトのハッシュである。一実施例では、暗号化鍵はデジタル・オブジェクトの暗号化バージョンの関数である。一実施例では、デジタル・オブジェクトと第2のメタデータ・エントリとのうちの一方又は両方がDESを用いて行われる。

10

【0104】

一実施例では、当該処理は、デジタル・オブジェクトのハッシュを暗号化鍵として用いたDESを適用することによってデジタル・オブジェクトの暗号化バージョンを作成する処理ロジックも含む（処理ロジック804）。

【0105】

別の実施例では、暗号化処理は、デジタル・オブジェクトに相当する1つ又は複数の動的に修正可能なエントリ群を保持する工程を含む場合があり、その場合、動的に修正可能ログを保持する工程は、デジタル・オブジェクトのコンテンツに基づいた識別子（例えば、ハッシュ値）を計算する工程及び、識別子を暗号化鍵として用いた暗号化を行う工程による。識別子を暗号化鍵として用いた暗号化を行う工程は、デジタル・オブジェクトを識別子によって暗号化する工程を含み得る。別の実施例では、識別子を暗号化鍵として用いて暗号化を行う工程は、デジタル・オブジェクトのハッシュを識別子によって暗号化する工程を備える。

20

【0106】

一実施例では、識別子は、デジタル・オブジェクトのコンテンツにハッシュ関数を適用することによって計算されるハッシュ値であり、暗号化を行う工程は、ハッシュ値が暗号化鍵であるDESを用いてデジタル・オブジェクトを暗号化する工程を備える。そのような処理は、暗号化デジタル・オブジェクトのハッシュを生成する工程及びハッシュを指数として用いてデジタル・オブジェクトをアクセスする工程又はエントリのコンテンツを、識別子を用いて暗号化する工程も含み得る。一実施例では、識別子はデジタル・オブジェクトのハッシュである。

30

【0107】

エンタングルメント（ログの複雑化）

当該記載手法は、文書ログにエントリの偽造を行うことを任意的に困難するのに用い得る。一実施例では、同期化サーバSAはコメントxをaのログ、SHA1:/SA/A/Eに加える。aのログは検証ハッシュVAによって開始され、検証ハッシュは、SAによって保持されている秘密qaを知ることによってのみ生成することが可能である。例えば、シードを、秘密qと連結される、文書aのコンテンツのMD5のハッシュをとることによって構成し得る。このシード値VA1は第1エントリとしてaのログにおいて記載される。コメントxがaのログに加えられる場合、検証ハッシュVA2は、VAと、コメントxのハッシュXを追加し、結果列のMD5のハッシュをとることによって作成される。同様に、次のコメントyの場合、検証ハッシュ値VA3は、VA2と、コメントyのハッシュYを追加し、結果の連結列のハッシュをとることによって作成される（例えば、VA3=MD5(VA2&SHA1(y))。特定の配列で追加されているということを各エントリが検証することになり、エントリは何ら省略されていないということが分かる。何れかの検査機関は、特定のログが有効であり、正しい順序の配列になっていることを検証することが可能である。追加のセキュリティを、サーバSAによって保持される公開鍵/秘密鍵対を用いて、各検証ハッシュをデジタル形式で署名することによって備えることが可能である。

40

50

【0108】

新たなハッシュを計算することによってそのようなログ自体を最初から書き換えることが可能であるということは明らかである。しかし、このようにして検証可能なログのエンタングルメントを行うことが可能である、つまり、ログはエントリにおけるお互いの状態を参照することが可能である。同期化サーバがSBである、文書bに関連した第2文書ログBを検討する。エントリは、Bに加えられるにつれ、直前に述べた連続ハッシュ機構によっても検証される。Bにおけるエントリが文書aを参照する場合、検証ハッシュVA2を含む、ログAの最後のエントリを含み得る。これによって2つのログのエンタングルメントが行われる。

【0109】

その場合、攻撃者は、ログSHA1:/SA/Aにおけるエントリを置き換えたいか取り除きたい場合、ログSHA1:/SB/Bが存在することが分かっているはず、そのログも置き換えなければならない。ログSHA1:/SA/AにおいてはログSHA1:/SB/Bへの参照を何ら見つけることが可能でない、検知不能な修正をログAに対して行うことは任意的に困難である。文書ログ間の相互参照は少数しかないので、所定のログを参照し得るログ・エントリ全てを見つけ、置き換えることが事実上不可能となる。更に、悪意のサーバは、それ自身のログに悪意のログ・エントリを作成することが可能でなく、有効な検証ハッシュと一致するものでないが、それは、そのようなエントリが正しいデジタル署名を有しないことになるからである。

【0110】

図9は、エンタングルメント処理の一実施例の流れ図である。当該処理は、ハードウェア（回路、専用ロジックなど）、（汎用コンピュータ・システム上若しくは専用マシン上で実行するものなどの）ソフトウェア、又は両方の組み合わせを備え得る処理ロジックによって行われる。

【0111】

図9を参照すれば、当該処理は、第1検証ハッシュ値（処理ブロック901）を作成することによって開始する。一実施例では、第1検証ハッシュ値は、秘密qを文書aのコンテンツと連結した結果の列のハッシュ値を計算することによって作成される。一実施例では、文書aは文書ログの文書に相当する。

【0112】

第1検証ハッシュが作成されると、処理ロジックは第1検証ハッシュを第1文書ログに加える（処理ブロック902）。

【0113】

後に、処理ロジックは、第1文書ログに加える対象のコメントに対する第2検証ハッシュ値を作成する（処理ブロック903）。一実施例では、第2検証ハッシュ値は、第1検証ハッシュ値を、加える対象のコメントのハッシュと連結した結果の列のハッシュ値を計算することによって作成される。

【0114】

第2検証ハッシュ値を作成した後、処理ロジックは第2検証ハッシュ値を第1文書ログに加える（処理ブロック904）。

【0115】

その後、処理ロジックは、第1文書ログを参照するエントリを第2文書において、第1文書ログにおけるエントリの第2検証ハッシュ値を含めることによって作成する（処理ブロック905）。

【0116】

一定時間経過後に、処理ロジックは、第1文書ログにおけるエントリを、第2検証ハッシュ値を含む、第2文書ログにおけるエントリをアクセスすることによって検証する（処理ブロック906）。

【0117】

ハッシュ・ベースのサーチ

10

20

30

40

50

ハッシュ・ベースのサーチは本明細書及び特許請求の範囲記載の手法を用いて行い得る。SHA1://host.com/A/Bを前提とすれば、未だコンテンツbを有していないノードはbをサーチしたい場合がある。前述のように、ノードは局所テーブルにおいてサーチしてもよく、他のサーバ（例えば、host.com又は汎用サーチ・サーバ）から情報を要求することによってサーチしてもよい。サーバは同様に、追加の要求をなお別のサーバに送出し得る。大半のサーチ・エンジンがコンテンツ（例えば、キーワード）又は識別子（例えば、ファイル名）に依拠する一方、ハッシュ値によってサーチする機能を備えるものはほとんどない。このような機能を備えるもののうちでは、一般的に、単純なグローバル・サーチ機能が提供されている。フリーネットなどのシステムは、サーバSに対するクライアント要求が、Sの構成に応じて追加サーバS'に転送される、ハッシュ値に基づいたフェデレーテッド・サーチを備える。対照的に、サーチの限定及び/又は指示を行ううえでの追加の因子としてコンテキストA及びhost.comを用いることが可能である。一例として、クライアントがaを知っていることを、サーチを行うか、Bに対してサーチの結果を戻す前に示すということをサーバSが要求する場合を検討する。なお、クライアントはBに対する要求にaを用いて署名しなければならない場合があるが、その場合、その署名は、Bに対する要求を表す列と連結されるaのハッシュ値を計算する工程とそのハッシュ値をサーバに供給する工程からなる。

10

【0118】

図10は、ハッシュ・ベースのサーチ処理の一実施例の流れ図である。当該処理は、ハードウェア（回路、専用ロジックなど）、（汎用コンピュータ・システム上若しくは専用マシン上で実行するものなどの）ソフトウェア、又は両方の組み合わせを備え得る処理ロジックによって行われる。図10を参照すれば、当該処理は、ハッシュ値とサーチのコンテキストとを規定することによってサーチ範囲が定義される、コンテンツのサーチ要求を受信する処理ロジックによって開始する（処理ブロック1001）。更に、処理ロジックはサーチを行う（処理ブロック1002）。

20

【0119】

取引システムにおける利用

このシーケンス処理は、配布される作品を管理する基本構成ブロックである。そういうものとして、多くの潜在的な利用シナリオが存在する。多くのそのようなシナリオは、アイテムのオークションなどの取引を巡る。単純化した場合では、物品の売り手がその目的物のログにコメントを入れ、買い手は購入する意思を表示するコメントを入れ、1者以上の第3者が、発送日付、追跡番号、受領日付や支払い情報などの、取引に関するコメントを入れる。これらの第3者の一部は、エスクロウエージェントとしての役割を果たす、例えば、先行するコメントに対する「正式シーケンス」番号が同期化サービスによって割り当てられてのみコメントを入れる、場合がある（例えば、支払いサービスは、配達を受領されたという配列されたコメントを見るまで支払いを完遂した旨のコメントを公表しない場合がある）。当該処理中の何れの時点でも、何れかの関係者は、現行のコメント（更には、まだ配列されていない自らの「保留」コメント）のリストを見ることが可能である。同期化サービスはこの種の取引を、各関係者がその他の関係者と事前に別個に交渉することを必要とすることなく可能にする。これは、現行のシステムよりも高い柔軟性及び可視性を備える一方で、間接費、管理費及び統合費用を大いに削減する。

30

40

【0120】

図11は取引処理の一実施例の流れ図である。当該処理は、ハードウェア（回路、専用ロジックなど）、（汎用コンピュータ・システム上若しくは専用マシン上で実行するものなどの）ソフトウェア、又は両方の組み合わせを備え得る処理ロジックによって行われる。

【0121】

図11を参照すれば、当該処理は、デジタル・オブジェクトに相当する群を参照する第1の一意の識別子を受信する処理ロジックによって開始する（処理ブロック1101）。

【0122】

次に、処理ロジックは第1メタデータ・エントリ及び第2メタデータ・エントリを受信

50

する（処理ブロック1102）。第1メタデータ・エントリは、売り手による売り出し物件の記述に相当し、第2メタデータ・エントリは、第1メタデータ・エントリに関する追加情報を得よう企図されている。一実施例では、追加情報は、第1メタデータ・エントリに相当するシーケンス番号を備える。別の実施例では、第1メタデータ・エントリは、売り手による売り出し物件の記述に相当し、第2メタデータ・エントリは、物件を購入する意思を表示する買い手からの表示に相当する。

【0123】

受信された後、処理ロジックは第1メタデータ・エントリ及び第2メタデータ・エントリを群に加える（処理ブロック1103）。

【0124】

群に加えられると、処理ロジックは、第1メタデータ・エントリ及び第2メタデータ・エントリ各々を参照するのに用いる第2の一意の識別子及び第3の一意の識別子に対するアクセスを備える（処理ブロック1104）。第2の一意の識別子及び第3の一意の識別子は、第1のメタデータ・エントリのコンテンツ及び第2のメタデータ・エントリのコンテンツ各々に基づくものである。

【0125】

一実施例では、当該処理は、第1メタデータ・エントリと第2メタデータ・エントリとの一方又は両方を参照する情報を含む第3のメタデータ・エントリを受信する処理ロジックも含む（処理ブロック1105）。一実施例では、第3のメタデータ・エントリは、第1メタデータ・エントリ及び第2メタデータ・エントリのソースでない別の関係者からのものである。そのような関係者は例えば、エスクロウエージェントであり得る。第3のメタデータ・エントリは、発送情報（例えば、発送日付、追跡番号並びに受領日付）及び支払情報を含む、物件を購入する取引に関する情報を含み得る。一実施例では、第3者のメタデータ・エントリは、1つ又は複数の先行するメタデータ・エントリに対するシーケンス番号が割り当てられた後にしか、加えられるものでない。

【0126】

例示的なコンピュータ・システム

図12は、本明細書及び特許請求の範囲記載の1つ又は複数の動作を行い得る例示的なコンピュータ・システムの構成図である。図12を参照すれば、コンピュータ・システム1200は例示的なクライアント1250又はサーバ1200のコンピュータ・システムを備え得る。コンピュータ・システム1200は、情報を通信する通信機構すなわちバス1211、及びバス1211に結合されて情報を処理するプロセッサ1212を備える。プロセッサ1212は、例えばペンティアム（登録商標）TAなどのマイクロプロセッサを含むが、これに限定されるものでない。

【0127】

システム1200は更に、バス1211に結合されて、情報と、プロセッサ1212によって実行される対象の命令とを記憶させる（主メモリと呼ぶ）ランダム・アクセス・メモリ（RAM）やその他の動的記憶装置1204を備える。主メモリ1204は、プロセッサ1212による命令の実行中に一時変数やその他の中間情報を記憶させるのにも用いる場合がある。

【0128】

コンピュータ・システム1200は、バス1211に結合されて、静的情報やプロセッサ1212用命令を記憶させる読み取り専用メモリ（ROM）並びに/若しくはその他の静的記憶装置1206及び、磁気ディスク若しくは光ディスク並びにそれに相当するディスク・ドライブなどのデータ記憶装置1207も備える。データ記憶装置1207は、バス1211に結合されて、情報及び命令を記憶させる。

【0129】

コンピュータ・システム1200は、バス1211に結合されて情報をコンピュータ・ユーザに表示させる、陰極線管（CRT）ディスプレイ又は液晶ディスプレイ（LCD）などのディスプレイ装置1221に更に結合し得る。英数字キーやその他のキーを含む英数字入力装置1222は、情報とコマンド選択をプロセッサ1212に通信するよう、バス1211に結合される場合もある。その他のユーザ入力装置としては、バス1211に結合されて、方向情報及びコマンド選択

10

20

30

40

50

をプロセッサ1212に通信し、ディスプレイ1221上のカーソル移動を制御する、マウス、トラックボール、トラックパッド、スタイラス又はカーソル方向キーなどのカーソル制御1223がある。

【0130】

バス1211に結合し得る別の装置には、紙上、フィルム上や同様な種類の媒体上などの媒体上に命令、データやその他の情報を印刷するのに用い得るハードコピー装置1224がある。更に、スピーカ及び/又はマイクロフォンなどの、音の記録再生装置を任意的にバス1211に結合してコンピュータ・システム1200とのオーディオ・インタフェースを行う場合がある。バス1211に結合し得る別の装置は、電話またはハンドヘルド型パーム装置に通信する有線/無線通信機能1225である。

10

【0131】

なお、システム1200及び関連したハードウェアの構成部分の何れか又は全部を本発明に用い得る。しかし、コンピュータ・システムのその他の構成は上記装置の一部又は全部を含み得るということが分かり得る。

【0132】

本発明の多くの改変及び修正は、当業者が上記記載を検討した後に疑いなく明らかとなる一方で、説明する目的で表し、記載した何れかの特定の実施例は限定的なものとみなされることを何ら意図しているものでないこととする。したがって、種々の実施例の詳細に対する参照は、それ自体が本発明に重要なものとしてみなされる特徴のみを記載しているその本特許請求の範囲に記載された範囲を限定することを意図するものでない。

20

【図面の簡単な説明】

【0133】

【図1】例示的なユーザ・インタフェースを示す図である。

【図2】図1において強調されたコメントによって参照されたX線透視画像に関連したログのビューを示す図である。

【図3】文書に関連したログを表すXMLファイルの例示的な見取り図を示す図である。

【図4】特定の文書に対するランデブーポイントに対してエントリを提出するクライアントの構成を描く図である。

【図5】同期化処理の一実施例の流れ図である。

【図6】データ処理の一実施例の流れ図である。

30

【図7】アクセス処理の一実施例の流れ図である。

【図8】暗号化処理の一実施例の流れ図である。

【図9】エンタングルメント処理の一実施例の流れ図である。

【図10】ハッシュ・ベースのサーチ処理の一実施例の流れ図である。

【図11】取引処理の一実施例の流れ図である。

【図12】例示的なコンピュータ・システムの構成図である。

【符号の説明】

【0134】

101 画像

102 ログ・エントリ

40

103 テキスト・ボックス

104 小サムネール

105 エントリ

1200 コンピュータ・システム

1204 主メモリ

1206 静的メモリ

1207 大容量記憶メモリ

1211 バス

1212 プロセッサ

1221 ディスプレイ

50

- 1222 キーボード
- 1223 カーソル制御装置
- 1224 ハードコピー装置
- 1225 無線/電話インタフェース

【 図 3 】

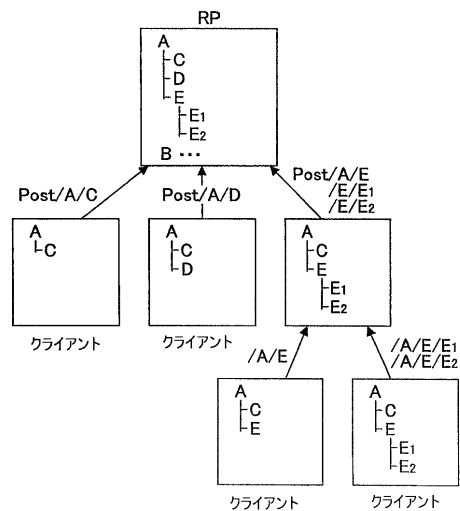
```

<doc SHA1=A...>
  <entry SEQ=1
    SHA1=C...>
    文書A上の第1のコメント
  </entry>
  <entry SEQ=2
    SHA1=D...
    HREF=URL
    SRC=URL>
    別のコメント
  </entry>
  ...
</doc>

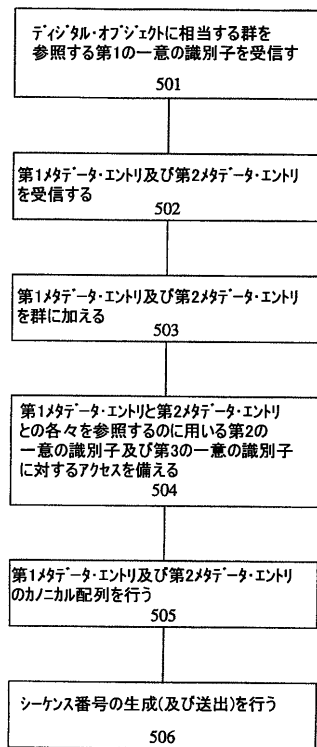
```

http://RP.net/A/
文書「A」上のコメントのXMLリスト

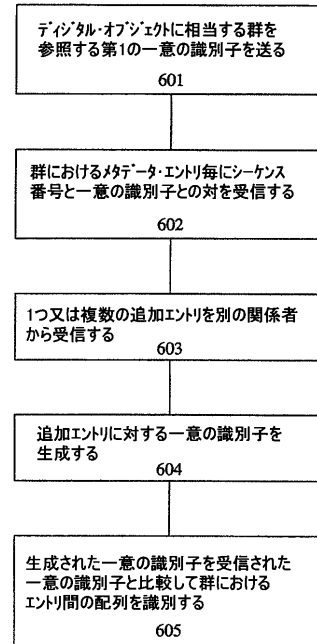
【 図 4 】



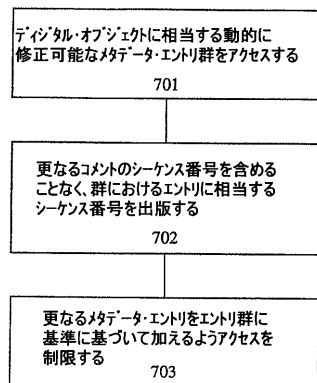
【 図 5 】



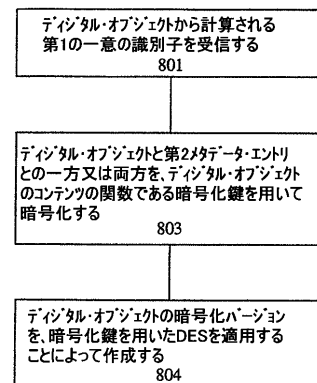
【 図 6 】



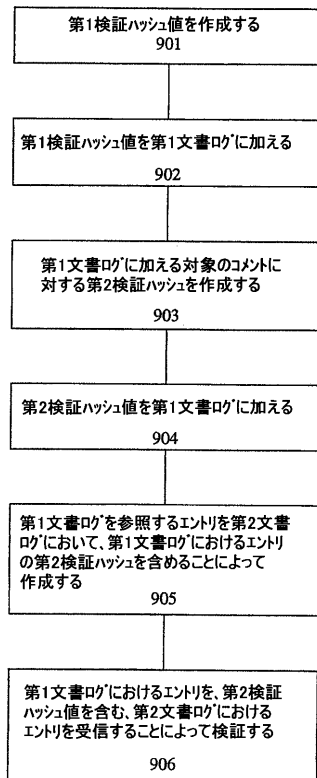
【 図 7 】



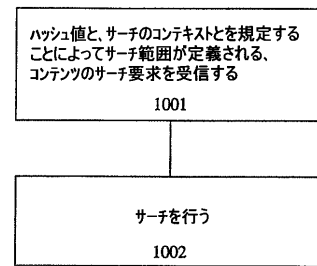
【 図 8 】



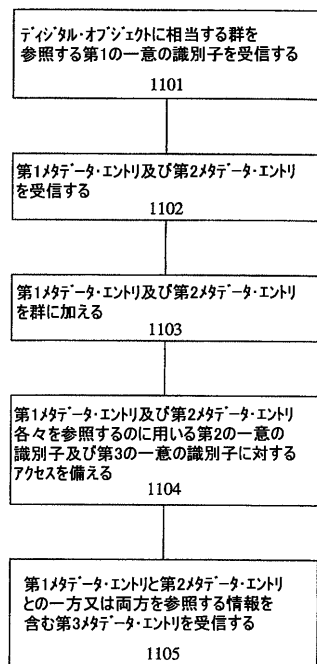
【 図 9 】



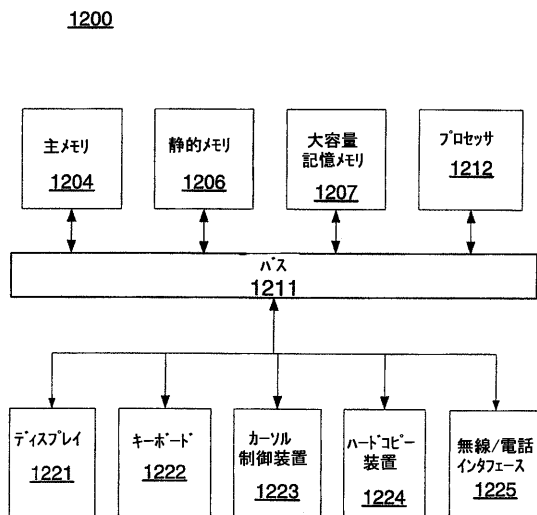
【 図 10 】



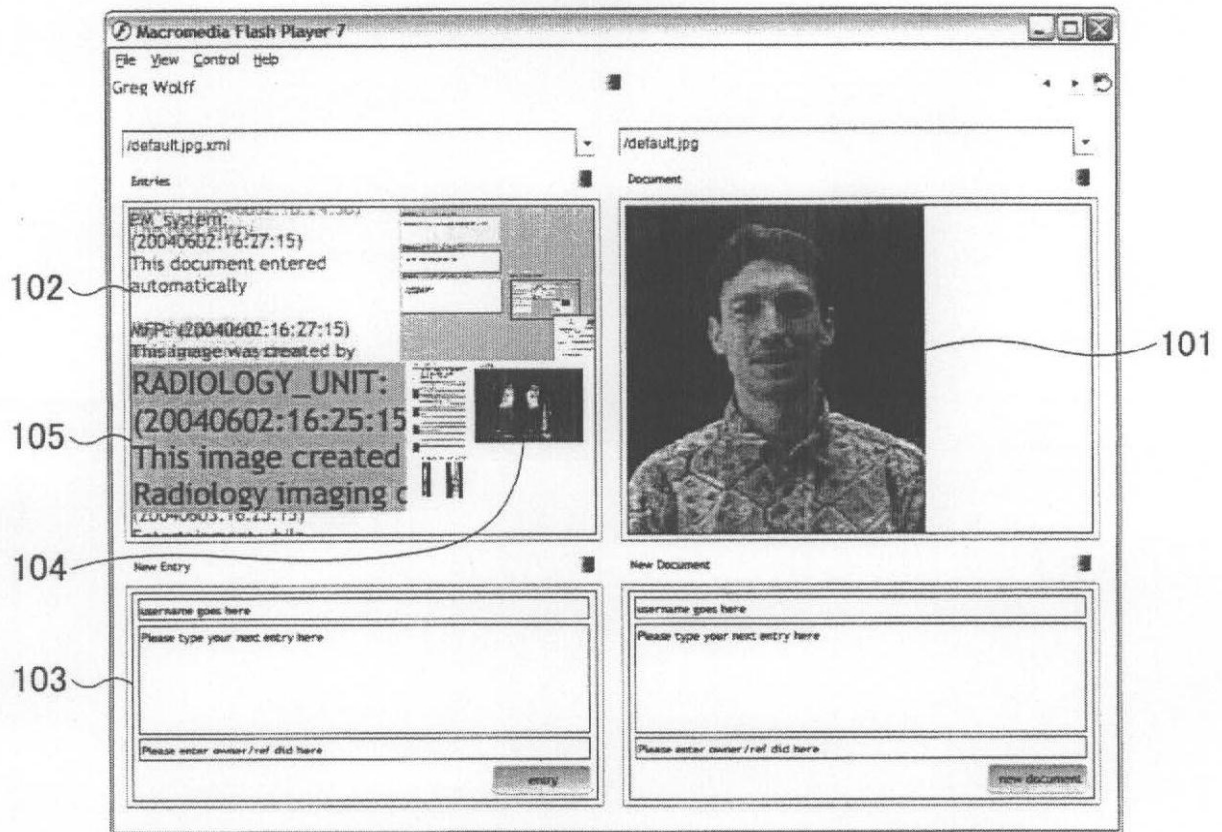
【 図 11 】



【 図 12 】



【 図 1 】



【 図 2 】

