

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号  
特許第7462922号  
(P7462922)

(45)発行日 令和6年4月8日(2024.4.8)

(24)登録日 令和6年3月29日(2024.3.29)

(51)国際特許分類

F I

G 0 6 F 16/182(2019.01)

G 0 6 F 16/182

請求項の数 7 (全35頁)

(21)出願番号	特願2020-19041(P2020-19041)	(73)特許権者	519442829
(22)出願日	令和2年2月6日(2020.2.6)		株式会社ブルーキャッスル
(62)分割の表示	特願2019-223803(P2019-223803) の分割		東京都港区新橋 6 - 5 - 3 山田屋ビル 4 F
原出願日	令和1年12月11日(2019.12.11)	(74)代理人	100134430
(65)公開番号	特開2021-93104(P2021-93104A)		弁理士 加藤 卓士
(43)公開日	令和3年6月17日(2021.6.17)	(72)発明者	李 晨
審査請求日	令和4年12月12日(2022.12.12)		東京都港区新橋 6 - 5 - 3 山田屋ビル 4 F 株式会社ブルーキャッスル内
		(72)発明者	曲 衛東
			東京都港区新橋 6 - 5 - 3 山田屋ビル 4 F 株式会社ブルーキャッスル内
		審査官	成瀬 博之

最終頁に続く

(54)【発明の名称】 ブロックチェーン技術と分散ストレージ技術とにより実現した分散型ストレージプラットフォームおよびアプリケーションプログラム

(57)【特許請求の範囲】

【請求項 1】

ファイルを分散保存するための複数の保存用ノードを含む保存用ネットワークと、  
前記複数の保存用ノードの識別情報を含む識別情報リストをブロックチェーン化しつつ  
保存する検索用ノードを複数含む、前記保存用ネットワークとは別の検索用ネットワーク  
と、  
前記ファイルを複数の部分データに分割し、前記複数の部分データのそれぞれを前記保  
存用ネットワークに含まれる少なくとも2つの保存用ノードに送信して保存させる保存処  
理部と、  
前記少なくとも2つの保存用ノードから前記複数の部分データのそれぞれを取得し、前  
記複数の部分データを合成して前記ファイルを復元する復元処理部と、

10

を備え、  
前記保存処理部は、前記複数の保存用ノードから、各々の保存用ノードの信頼性を考慮  
して前記少なくとも2つの保存用ノードを選択する情報処理システム。

【請求項 2】

前記保存処理部は、さらに、前記ファイルの重要度および前記ファイルの保存を要求し  
たクライアントの重要度の少なくともいずれかを考慮して前記少なくとも2つの保存用ノ  
ードを選択する請求項 1 に記載の情報処理システム。

【請求項 3】

前記保存処理部は、さらに、前記複数の部分データに対応して生成された複数の冗長デ

20

ータのそれぞれを、前記複数の保存用ノードに含まれる少なくとも2つの保存用ノードに送信して保存させる請求項1に記載の情報処理システム。

【請求項4】

前記検索用ノードは、前記識別情報リストに基づいて、前記複数の部分データのそれぞれが保存されている前記少なくとも2つの保存用ノードを検索する検索処理部を備えた請求項1に記載の情報処理システム。

【請求項5】

ファイルを分散保存するための複数の保存用ノードを含む保存用ネットワークと、  
前記複数の保存用ノードの識別情報を含む識別情報リストをブロックチェーン化しつつ保存する検索用ノードを複数含む前記保存用ネットワークとは別の検索用ネットワークと、  
を備える情報処理システムを用いた情報処理方法であって、

前記ファイルを複数の部分データに分割し、前記複数の部分データのそれぞれを前記保存用ネットワークに含まれる少なくとも2つの保存用ノードに送信して保存させる保存処理ステップと、

前記少なくとも2つの保存用ノードから前記複数の部分データのそれぞれを取得し、前記複数の部分データを合成して前記ファイルを復元する復元処理ステップと、

を含み、

前記保存処理ステップにおいては、前記複数の保存用ノードから、各々の保存用ノードの信頼性を考慮して前記少なくとも2つの保存用ノードを選択する情報処理方法。

【請求項6】

ファイルを分散保存するための複数の保存用ノードを含む保存用ネットワークと、  
前記複数の保存用ノードの識別情報を含む識別情報リストをブロックチェーン化しつつ保存する検索用ノードを複数含む、前記保存用ネットワークとは別の検索用ネットワークと、

を備える情報処理システムにおいて、ファイルの分割により生成された複数の部分データのそれぞれを、前記保存用ネットワークに含まれる少なくとも2つの保存用ノードに分散して前記ファイルが復元可能となるように保存するためのアプリケーションプログラムであって、

前記ファイルを複数の部分データに分割し、前記複数の部分データのそれぞれを前記少なくとも2つの保存用ノードに送信して保存させる保存処理ステップと、

前記少なくとも2つの保存用ノードから前記複数の部分データのそれぞれを取得し、前記複数の部分データを合成して前記ファイルを復元する復元処理ステップと、

をコンピュータに実行させ、

前記保存処理ステップにおいては、前記複数の保存用ノードから、各々の保存用ノードの信頼性を考慮して前記少なくとも2つの保存用ノードを選択するアプリケーションプログラム。

【請求項7】

前記ファイルのハッシュ値をファイルハッシュとして生成するファイルハッシュ生成ステップと、

前記ファイルを複数の部分データに分割するファイル分割ステップと、

前記複数の部分データのそれぞれのハッシュ値を部分ハッシュとして生成する部分ハッシュ生成ステップと、

前記ファイルハッシュと前記部分ハッシュとの組み合わせをブロックチェーン化しつつ複数の前記検索用ノードに保存すると共に、前記ファイルハッシュと前記部分データと前記部分ハッシュとの組合せのそれぞれを前記少なくとも2つの保存用ノードに保存するように指示する分散保存指示ステップと、

をコンピュータに実行させる請求項6に記載のアプリケーションプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ブロックチェーン技術と分散ストレージ技術とにより実現した分散型ストレージプラットフォームおよびアプリケーションプログラムに関する。

【背景技術】

【0002】

上記技術分野において、特許文献1には、データの分散保存における冗長性の技術が開示されている。

【先行技術文献】

【特許文献】

【0003】

【文献】米国特許第10127108号公報

10

【発明の概要】

【発明が解決しようとする課題】

【0004】

しかしながら、上記文献に記載の技術では、中央集中型のデータセンタを前提としており、安全性が十分とは言えなかった。複数のデータセンタが同時にダウンしてしまうと、データが消えてしまうことがあった。

【0005】

本発明の目的は、上述の課題を解決する技術を提供することにある。

【課題を解決するための手段】

【0006】

20

上記目的を達成するため、本発明に係る情報処理システムは、  
ファイルを分散保存するための複数の保存用ノードを含む保存用ネットワークと、  
前記複数の保存用ノードの識別情報を含む識別情報リストをブロックチェーン化しつつ保存する検索用ノードを複数含む、前記保存用ネットワークとは別の検索用ネットワークと、

前記ファイルを複数の部分データに分割し、前記複数の部分データのそれぞれを前記保存用ネットワークに含まれる少なくとも2つの保存用ノードに送信して保存させる保存処理部と、  
前記少なくとも2つの保存用ノードから前記複数の部分データのそれぞれを取得し、前記複数の部分データを合成して前記ファイルを復元する復元処理部と、

30

を備え、

前記保存処理部は、前記複数の保存用ノードから、各々の保存用ノードの信頼性を考慮して前記少なくとも2つの保存用ノードを選択する情報処理システムである。

【0008】

上記目的を達成するため、本発明に係る情報処理方法は、  
ファイルを分散保存するための複数の保存用ノードを含む保存用ネットワークと、  
前記複数の保存用ノードの識別情報を含む識別情報リストをブロックチェーン化しつつ保存する検索用ノードを複数含む前記保存用ネットワークとは別の検索用ネットワークと、  
を備える情報処理システムを用いた情報処理方法であって、

前記ファイルを複数の部分データに分割し、前記複数の部分データのそれぞれを前記保存用ネットワークに含まれる少なくとも2つの保存用ノードに送信して保存させる保存処理ステップと、  
前記少なくとも2つの保存用ノードから前記複数の部分データのそれぞれを取得し、前記複数の部分データを合成して前記ファイルを復元する復元処理ステップと、

40

を含み、

前記保存処理ステップにおいては、前記複数の保存用ノードから、各々の保存用ノードの信頼性を考慮して前記少なくとも2つの保存用ノードを選択する情報処理方法である。

【0010】

上記目的を達成するため、本発明に係るアプリケーションプログラムは、  
ファイルを分散保存するための複数の保存用ノードを含む保存用ネットワークと、

50

前記複数の保存用ノードの識別情報を含む識別情報リストをブロックチェーン化しつつ保存する検索用ノードを複数含む前記保存用ネットワークとは別の検索用ネットワークと、を備える情報処理システムにおいて、ファイルの分割により生成された複数の部分データのそれぞれを、前記保存用ネットワークに含まれる少なくとも2つの保存用ノードに分散して前記ファイルが復元可能となるように保存するためのアプリケーションプログラムであって、前記ファイルを複数の部分データに分割し、前記複数の部分データのそれぞれを前記少なくとも2つの保存用ノードに送信して保存させる保存処理ステップと、前記少なくとも2つの保存用ノードから前記複数の部分データのそれぞれを取得し、前記複数の部分データを合成して前記ファイルを復元する復元処理ステップと、

10

をコンピュータに実行させ、

前記保存処理ステップにおいては、前記複数の保存用ノードから、各々の保存用ノードの信頼性を考慮して前記少なくとも2つの保存用ノードを選択するアプリケーションプログラムである。

【発明の効果】

【0012】

本願発明によれば、高い安全性を担保しつつ、小規模ストレージの集合により大規模データサーバと同様の機能を実現することができる。

【図面の簡単な説明】

【0013】

20

【図1A】本発明の第1実施形態に係る情報処理システムの構成を示すブロック図である。

【図1B】本発明の第2実施形態に係る情報処理システムの構成を示すブロック図である。

【図2】本発明の第3実施形態に係る情報処理システムの構成を示すブロック図である。

【図3A】本発明の第3実施形態に係る情報処理システムの、ファイルを分散して保存する動作手順を示す図である。

【図3B】本発明の第3実施形態に係る情報処理システムの、ファイルを合成して再現する動作手順を示す図である。

【図4】本発明の第3実施形態に係る情報処理システムの、保存用ノードまたは検索用ノードに参加する動作手順を示す図である。

【図5】本発明の第3実施形態に係るクライアントアプリケーションの構成を示す図である。

30

【図6】本発明の第3実施形態に係るクライアントアプリケーションを含むクライアント端末のハードウェア構成を示すブロック図である。

【図7】本発明の第3実施形態に係るクライアントアプリケーションの処理手順を示すフローチャートである。

【図8】本発明の第3実施形態に係るファイル保存処理部の機能構成を示すブロック図である。

【図9】本発明の第3実施形態に係るファイル保存処理部で使用するデータの構成を示す図である。

【図10】本発明の第3実施形態に係るファイル保存処理部の処理手順を示すフローチャートである。

40

【図11A】本発明の第3実施形態に係るデータの分割処理の手順を示すフローチャートである。

【図11B】本発明の第3実施形態に係る保存先ノードの選定処理の手順を示すフローチャートである。

【図12】本発明の第3実施形態に係るリスト検索処理部の機能構成を示すブロック図である。

【図13】本発明の第3実施形態に係るリスト検索処理部で使用するデータの構成を示す図である。

【図14】本発明の第3実施形態に係るリスト検索処理部の処理手順を示すフローチャー

50

トである。

【図 1 5】本発明の第 3 実施形態に係るファイル取得処理部の機能構成を示すブロック図である。

【図 1 6】本発明の第 3 実施形態に係るファイル取得処理部で使用するデータの構成を示す図である。

【図 1 7】本発明の第 3 実施形態に係るデータ取得処理部の処理手順を示すフローチャートである。

【図 1 8】本発明の第 3 実施形態に係る報酬処理部の機能構成を示すブロック図である。

【図 1 9】本発明の第 3 実施形態に係る報酬処理部で使用するデータの構成を示す図である。

10

【図 2 0】本発明の第 3 実施形態に係る報酬処理部の処理手順を示すフローチャートである。

【図 2 1】本発明の第 3 実施形態に係る保存用ノードの機能構成を示すブロック図である。

【図 2 2】本発明の第 3 実施形態に係る保存用ノードの処理手順を示すフローチャートである。

【図 2 3】本発明の第 3 実施形態に係る検索用ノードの機能構成を示すブロック図である。

【図 2 4】本発明の第 3 実施形態に係る検索用ノードの処理手順を示すフローチャートである。

【図 2 5】本発明の第 3 実施形態に係る保存用ノードまたは検索用ノードとなるクライアント装置のハードウェア構成を示すブロック図である。

20

【図 2 6】本発明の第 4 実施形態に係る情報処理システムの構成を示すブロック図である。

【図 2 7】本発明の第 5 実施形態に係る情報処理システムの構成を示すブロック図である。

【発明を実施するための形態】

【0014】

以下に、図面を参照して、本発明の実施の形態について例示的に詳しく説明する。ただし、以下の実施の形態に記載されている構成要素は単なる例示であり、本発明の技術範囲をそれらのみに限定する趣旨のものではない。

【0015】

[第 1 実施形態]

本発明の第 1 実施形態としての情報処理システム 110 について、図 1 A を用いて説明する。

30

【0016】

図 1 A に示すように、情報処理システム 110 は、保存用ネットワーク 101 と、検索用ネットワーク 102 と、保存処理部 103 と、を含む。保存用ネットワーク 101 は、ファイル 130 を分散保存するための複数の保存用ノード 111 を含む。検索用ネットワーク 102 は、複数の保存用ノード 111 のロケーションを含むロケーションリスト 122 をブロックチェーン化しつつ保存する検索用ノード 121 を複数含む。保存処理部 103 は、ファイル 130 を複数の部分データ 131 ~ 13n に分割し、複数の部分データ 131 ~ 13n のそれぞれを複数の保存用ノード 111 に含まれる少なくとも 2 つの保存用ノードに送信して保存させる。更新処理部 123 は、検索用ノード 121 に含まれ、部分データを保存した保存用ノード 111 の識別情報を用いて、ロケーションリスト 122 を更新する。

40

【0017】

本実施形態によれば、高い安全性を担保しつつ、小規模ストレージの集合により大規模データサーバと同様の機能を実現することができる。

【0018】

[第 2 実施形態]

本発明の第 2 実施形態に係る情報処理システム 120 について図 1 B を用いて説明する。

【0019】

図 1 B に示すように、情報処理システム 120 は、保存用ネットワーク 101 と、検索

50

用ネットワーク 105 と、復元処理部 104 とを含む。検索用ネットワーク 105 は、複数の保存用ノードのロケーションを含むロケーションリスト 152 をブロックチェーン化しつつ保存する検索用ノード 151 を複数含む。また、各検索用ノード 151 は、検索処理部 153 を含む。検索処理部 153 は、ロケーションリスト 122 に基づいて、複数の部分データ 141 ~ 14n が保存されている保存用ノード 111 を検索する。復元処理部 104 は、保存用ノード 111 から複数の部分データ 141 ~ 14n を取得し、複数の部分データ 141 ~ 14n を合成してファイル 140 を復元する。

#### 【0020】

本実施形態によれば、高い安全性を担保しつつ、小規模ストレージの集合により大規模データサーバと同様の機能を実現することができる。

10

#### 【0021】

##### [ 第3実施形態 ]

本発明の第3実施形態に係る情報処理システム 200 について図2以降を用いて説明する。

本実施形態の情報処理システム 200 は、ファイルおよびその分割された部分データがハッシュ化（以下、ハッシュをHash、ハッシュ値をHash値と表す）されて、検索用ネットワークと保存用ネットワークとの独立した二層構造で管理される。そして、ファイルのアップロードでは、ファイルから分割した複数の部分データを、複数の保存用ノードから複数の部分データのそれぞれの保存先として選定した保存用ノードに保存させる。そして、複数の部分データをそれぞれ保存する選定された保存用ノードを示すロケーションリストをブロックチェーン化しつつ生成し、複数の検索用ノードに共有させる。一方、ファイルのダウンロードでは、複数の検索用ノードに共有されたロケーションリストをいずれか1つの検索用ノードから取得して、ファイルに対応するロケーションリストを検索する。そして、検索したロケーションリストに従って、ファイルから分割された複数の部分データをそれぞれ保存する複数の保存用ノードから取得し、複数の部分データを合成して取得対象のファイルを生成する。

20

#### 【0022】

ファイルをアップロードする際には、ファイルを暗号化し、暗号化されたファイルから分割した複数の部分データを保存先として選定した保存用ノードに保存させる。また、ファイルをダウンロードする際には、暗号化ファイルから分割された複数の部分データをそれぞれ保存する複数の保存用ノードから取得し、暗号化ファイルを構成する。そして、暗号化ファイルからファイルを復号する。なお、検索用ノードおよび保存用ノードは、ノードを識別するノード識別情報のHash値により識別されることが望ましい。

30

#### 【0023】

##### 《情報処理システム》

以下、図2～図4に従って、本実施形態の情報処理システム 200 の構成および動作について説明する。

#### 【0024】

##### （ブロック構成）

図2は、本実施形態に係る情報処理システム 200 の構成を示すブロック図である。

40

#### 【0025】

情報処理システム 200 は、保存用ネットワーク 201 と、検索用ネットワーク 202 と、クライアント端末 203 とを有する。クライアント端末 203 は、ファイル保存処理、リスト検索処理およびファイル取得処理を実現するクライアントアプリケーション 232 を実行するよう構成されている。

#### 【0026】

保存用ネットワーク 201 は、P2P通信を行う複数の保存用ノード 211 を含む。複数の保存用ノード 211 のそれぞれは、クライアントアプリケーション 232 からのファイルの保存要求において、ファイルから分割された部分データを、ファイルHash（ファイルハッシュ）と部分Hash（部分ハッシュ）を検索キーとして保存する。また、複数の保存

50

用ノード211は、クライアントアプリケーション232からのファイルの取得要求において、検索用ノード221がロケーションリストからファイルのHash値によって検索したファイルリストに含まれる部分Hashを用いて、部分データを検索して読出し、クライアント端末203に送信する。

【0027】

検索用ネットワーク202は、P2P通信を行う複数の検索用ノード221を含む。検索用ノード221は、ファイルが複数の保存用ノード211に保存された場合に、そのファイルのHash値によって特定されたファイルリストを含むロケーションリストを生成して複数の検索用ノード221で共有する。また、検索用ノード221は、クライアント端末203からのファイルの取得要求において、最新のロケーションリストから、取得要求されたファイルに対応するファイルHashと部分Hashと保存用ノードIDとから構成されるファイルリストを検索して、クライアント端末203に提供する。

10

【0028】

クライアントアプリケーション232は、ファイルの保存要求に対しては、ファイルを分割して部分データを部分Hashを検索キーとして、複数の保存用ノード211から選択された保存用ノードに保存する。部分データの保存が完了すると、保存用ノード211は、ファイルHashと部分Hashと部分データを保存した保存用ノードIDとを検索用ノード221に通知する。そして、検索用ノード221が、ファイルHashと、部分Hash値と、保存用ノードIDと、から構成されたファイルリストを生成して、ロケーションリストを更新する。更新されたロケーションリストは、全ての検索用ノード221で共有される。

20

【0029】

クライアントアプリケーション232は、ファイルの取得要求に対しては、ファイルHashを検索キーとして、近傍の検索用ノード221に送り、最新のロケーションリストに含まれるファイルのファイルリストを取得する。取得したファイルリストには、ファイルHashと、部分Hashと、保存用ノードIDと、が含まれている。クライアントアプリケーション232は、ファイルリストから抽出した部分Hashと保存用ノードIDとの組合せを用いて、部分データを保存用ノードから読出す。

【0030】

以下、図3A、図3Bおよび図4を参照して、情報処理システム200の動作手順を示す。

30

【0031】

(ファイルの保存手順)

図3Aは、実施形態に係る情報処理システム200の、ファイルを分散して保存する動作手順を示す図である。

【0032】

ファイルの保存を要求するクライアント301は、クライアント端末203にファイル名によりファイルデータの保存を指示する。ファイルデータ311は、クライアント端末203のクライアントアプリケーション232に渡される。

【0033】

クライアントアプリケーション232は、ファイルデータ311を暗号化し、暗号化ファイルデータ312を生成する。そして、クライアントアプリケーション232は、ファイルハッシュ生成処理として、暗号化ファイルデータ312からファイルHash313を算出する。クライアントアプリケーション232は、ファイルHash313を検索用ノード221に送信する。なお、送信先の検索用ノード221は、ロケーションリスト317の検索用ノードリスト324を参照して、例えば、KAD(Kademlia)ネットワークにおけるノード検索の再帰アルゴリズムを用いて、最も近い検索用ノードを見付けることが望ましい。また、本実施形態においては、ファイルの暗号化後にファイルHashを算出したが、ファイルHashを算出した後にファイルHashを含んでファイルを暗号化してもよい。

40

【0034】

検索用ノード221は、保持するロケーションリスト317に、ファイルHash313を

50

検索キーとして有する空のファイルリストを生成して追加する。そして、検索用ネットワーク 202 に含まれる全ての検索用ノードは、P2P 通信により空のファイルリストが追加された最新のロケーションリストを保持することができる。なお、ファイル名と検索キーとなるファイル Hash 313 との対応データ 314 を生成してアプリケーションに保持しておくことによって、ファイルの取得を行う場合のクライアントからの要求を簡易にすることができる。

#### 【0035】

一方、クライアントアプリケーション 232 は、暗号化ファイルデータ 312 を、クライアントやファイルの重要性、さらに、復元可能な冗長性を考慮して複数の部分データ 315 に分割する。そして、クライアントアプリケーション 232 は、部分ハッシュ生成処理として、複数の部分データ 315 のそれぞれの Hash 値を算出して、部分 Hash 316 を生成する。部分 Hash 316 は、部分データ 315 の先頭から順に、前の部分 Hash 316 に次の部分データ 315 を加えて Hash 値を算出することによりブロックチェーン化する。ブロックチェーン化して Hash 値を算出するので、ファイルリストに保持された部分 Hash や保存用ノードから読み出した部分 Hash から部分データの合成順を知ることができる。なお、部分 Hash 316 は、各部分データ 315 に対して独立して算出してもよい。独立して部分 Hash を算出する場合には、ファイルの読み出し時に部分データを合成する順序を保持する必要がある。例えば、ロケーションリストのファイルリスト 322 に保持する、あるいは、保存用ノードに保存された部分データや部分 Hash 内に保持することができる。

#### 【0036】

クライアントアプリケーション 232 は、検索用ノード 221 のロケーションリスト 317 から保存用ネットワーク 201 に参加する保存用ノードリスト 318 を取得する。なお、クライアントアプリケーション 232 から検索用ノード 221 へのファイル Hash 313 の送信と、検索用ノード 221 からクライアントアプリケーション 232 への保存用ノードリスト 318 の送信とは、一緒に行われてもよい。また、検索用ノード 221 のロケーションリスト 317 には検索用ノードリスト 324 も保持されており、クライアントアプリケーション 232 からアクセスする検索用ノードを選定する場合に参照され、クライアント端末の検索用ノードとしての参加や離脱時には、最新データに更新される。

#### 【0037】

クライアントアプリケーション 232 は、受信した保存用ノードリスト 318 から、分割された複数の部分データ 315 の数に相当する保存ノードを識別する保存用ノード ID 319 を選定する。なお、保存用ノード ID 319 は、保存用ノードに関連する属性から算出された Hash 値であるのが望ましい。また、選定される保存用ノード ID 319 の数は、保存時のエラーを考慮して分割された複数の部分データ 315 の数より多く選定する。

#### 【0038】

クライアントアプリケーション 232 は、ファイル Hash 313 と部分データ 315 と部分 Hash 316 との組合せと、選定された保存用ノード ID 319 とを組み合わせ、選定された保存用ノードに対して保存を指示する保存用メッセージ 320 を生成する。ここで、ファイル Hash 313 と部分データ 315 と部分 Hash 316 との組合せ、あるいは、少なくとも部分データ 315 は各データごとに暗号鍵で暗号化される。そして、クライアントアプリケーション 232 は、各保存用メッセージ 320 を各保存用ノードに送信する。なお、保存用メッセージ 320 の送信は、保存相手の複数の保存用ノードに一斉送信するのが高速化の面で望ましい。

#### 【0039】

保存相手の保存用ノード 211 では、保存用ノード ID 319 を確認して、ファイル Hash と部分 Hash とを検索キーとした部分データ 321 を保存する。そして、保存がエラーなく完了すると、保存用ノード 211 は検索用ノードに保存完了報告を行う。この保存完了報告には、ファイル Hash と部分 Hash と保存用ノード ID との組合せが含まれる。なお、保存完了報告は、全検索用ノードに一斉送信されても、先にクライアントアプリケーション 232 がアクセスした検索用ノードであってもよい。なお、検索用ネットワーク 20

10

20

30

40

50



2では、全検索用ノードがP2P通信により空のファイルリストを含む最新のロケーションリストを保持している。図示されていないが、保存完了報告を行った保存用ノードには、保存対価の報酬が支払われる。

【0040】

エラーなしに保存完了した保存用ノードからの保存完了報告を受信した検索用ノードは、保存完了報告に含まれる部分Hashと保存用ノードIDとの組合せを、ファイルHashを検索キーとする空のファイルリストに順次に記憶する。冗長を含む保存対象のファイルが再生可能な数の部分データが保存されると、新たなファイルリスト322が追加された最新のロケーションリストが完成する。

【0041】

図示されていないが、ファイルの保存用ネットワーク201の保存用ノードへの保存が完了すると、ファイルの保存を要求したクライアント301から通常は保存料金が徴収される。

【0042】

(ファイルの再現手順)

図3Bは、本実施形態に係る情報処理システム200の、ファイルを合成して復元する動作手順を示す図である。なお、図3Bにおいては、図3Aで保存したファイルを読み出す例を説明するが、他のファイルであっても動作手順は同様である。

【0043】

ファイルの取得を要求するクライアント303からのクライアント端末203に対して入力されたファイル名は、クライアントアプリケーション232に渡される。クライアントアプリケーション232は、ファイルハッシュ取得処理として、対応データ314を参照してファイル名に対応付けて保持されているファイルHash313を取得する。そして、取得したファイルHash313を検索用ノードに送信する。なお、ファイルの保存時と同様に、送信先の検索用ノードは、ロケーションリスト317の検索用ノードリストを参照して、例えば、KAD(Kademlia)ネットワークにおけるノード検索の再帰アルゴリズムを用いて、最も近い検索用ノードを見付けることが望ましい。

【0044】

検索用ノードは、受信したファイルHash313を検索キーとして、ファイルのファイルリスト322を検索する。そして、ファイルHash313を有するファイルリスト325を見つける。そして、検索用ノードは、見つけたファイルリスト325をクライアントアプリケーション232に送信する。

【0045】

クライアントアプリケーション232は、保存用ノード情報取得処理として、受信したファイルリスト325に含まれる、ファイルの分割数だけの部分Hashと保存用ノードIDとの組合せ326をそれぞれ抽出する。そして、クライアントアプリケーション232は、保存用ノードIDが示す保存用ノードに対してファイルHashと部分Hashとを送信する。なお、保存用ノードIDとファイルHashと部分Hashとは、保存用ネットワーク201の保存用ノードに対してP2P送信される。

【0046】

送信された各保存用ノードIDを有する保存用ノード211は、受信したファイルHashと部分Hashとを検索キーとして部分データを検索する。そして、保存用ノード211は、見つけた部分データを、ファイルHashと部分Hashと共にクライアントアプリケーション232に送信する。図示されていないが、本実施形態においては、部分データを読み出してクライアントアプリケーション232に送信した保存用ノード211には、保存時の報酬よりも高い読出の報酬が支払われる。

【0047】

クライアントアプリケーション232は、それぞれの保存用ノード211からファイルHashと部分Hashと部分データとの組合せ321を受信して、その数がファイルを復元できる数を越えた場合、保存用ネットワーク201からのファイルの読み出しが成功したと

10

20

30

40

50

する。クライアントアプリケーション 2 3 2 は、受信したデータを部分データを暗号化した暗号鍵に対応する復号鍵で復号し、部分Hashと部分データとの組合せ 3 2 1 に含まれる各部分Hashを照合して、部分データ 3 1 5 を分割した順序で合成して、暗号化ファイルデータ 3 1 2 を復元する。なお、複数の部分データの合成については、先にファイルの保存処理で説明したように、部分データを分割順にブロックチェーン化して部分Hashを算出しているため、合成順序を持つ必要はない。ただし、各部分データから独立に部分Hashを算出する場合は、部分データの合成順序を保持する必要がある。

【 0 0 4 8 】

クライアントアプリケーション 2 3 2 は、復元された暗号化ファイルデータからファイルを暗号化した暗号鍵に対応する復号鍵でファイルデータを復号して、クライアント端末 2 0 3 によりクライアント 3 0 3 に提供する。なお、図示していないが、クライアント 3 0 3 にファイルが提供されると、普通はクライアント 3 0 3 からファイルを提供した料金が徴収される。

10

【 0 0 4 9 】

( 保存用ノードまたは検索用ノードの動作手順 )

図 4 は、本実施形態に係る情報処理システム 2 0 0 の、保存用ノードまたは検索用ノードの動作手順を示す図である。

【 0 0 5 0 】

( 保存用ノード )

クライアント端末が保存用ネットワーク 2 0 1 の保存用ノード 2 1 1 として参加する場合、クライアント端末は、ステップ S 4 5 1 において、保存用ノードアプリケーション 4 1 1 をダウンロードして駆動する。保存用ノードアプリケーション 4 1 1 は、ステップ S 4 5 2 において、電子キャッシュ保存部を設定する。

20

【 0 0 5 1 】

クライアント端末は、ステップ S 4 5 3 において、保存用ノードへの参加を申し込み、ステップ S 4 5 4 において、クライアント情報としてストレージサイズやクライアント属性などを保存用ノードアプリケーション 4 1 1 に送出する。保存用ノードアプリケーション 4 1 1 は、ステップ S 4 5 5 において、クライアント情報に基づいて保存用ノード 2 1 1 の選定時に考慮されるノードの信頼性を示すノードランクが初期設定され、保存用ノード 2 1 1 を識別するHash ID が設定される。そして、保存用ノードの登録は、検索用ノードに伝えられて検索用ノードに保持されたロケーションリスト内の保存用ノードリストが最新状態に更新される。

30

【 0 0 5 2 】

保存用ノード 2 1 1 が部分ファイルを保存する場合、保存用ノードアプリケーション 4 1 1 は、ステップ S 4 5 6 において、クライアントアプリケーション 2 3 2 から保存用ノード ID を送信先として ( ファイルHash、部分Hash、部分データ ) の組合せを取得して保存する。そして、保存用ノードアプリケーション 4 1 1 は、ステップ S 4 5 7 において、保存報酬を取得する。

【 0 0 5 3 】

保存用ノード 2 1 1 が部分データを読出す場合、保存用ノードアプリケーション 4 1 1 は、ステップ S 4 5 8 において、クライアントアプリケーション 2 3 2 から保存用ノード ID を送信先としてファイルHashと部分Hashとを取得する。そして、保存用ノードアプリケーション 4 1 1 は、ファイルHashと部分Hashとを検索キーとして部分データを検索して読み出し、クライアントアプリケーション 2 3 2 に送る。保存用ノードアプリケーション 4 1 1 は、ステップ S 4 5 9 において、保存報酬より多い読出報酬を取得する。

40

【 0 0 5 4 】

( 検索用ノード )

クライアント端末が検索用ネットワーク 2 0 2 の検索用ノード 2 2 1 として参加する場合、クライアント端末は、ステップ S 4 6 1 において、検索用ノードアプリケーション 4 2 1 をダウンロードして駆動する。検索用ノードアプリケーション 4 2 1 は、ステップ S

50

4 6 2 において、電子キャッシュ保存部を設定する。

【 0 0 5 5 】

クライアント端末は、ステップ S 4 6 3 において、検索用ノードへの参加を申し込み、ステップ S 4 6 4 において、クライアント情報としてクライアント属性や参加料金などを検索用ノードアプリケーション 4 2 1 に送出する。検索用ノードアプリケーション 4 2 1 は、ステップ S 4 6 5 において、検索用ノードから選ばれた管理グループに対して、参加可否の判定要求をして、判定結果を取得する。なお、参加可否の判定は、検索用ネットワーク 2 0 2 に参加する検索用ノードの投票で行われる。そして、検索用ノードアプリケーション 4 2 1 は、ステップ S 4 6 6 において、クライアント情報に基づいて検索用ノード 2 2 1 の投票時に考慮されるノードの信頼性を示すノードランクが設定され、検索用ノード 2 2 1 を識別する Hash ID が設定される。そして、検索用ノードの登録は、検索用ノードが保持するロケーションリスト内の検索用ノードリストを最新状態に更新する。

10

【 0 0 5 6 】

検索用ノード 2 2 1 がロケーションリストを保存して共有する場合、検索用ノードアプリケーション 4 2 1 は、ステップ S 4 6 7 において、クライアント端末からファイル Hash を受信すると、ファイル Hash を検索キーとする空のファイルリストをロケーションリストに追加する。そして、各保存用ノードから部分データの保存完了報告を受信すると、検索用ノードアプリケーション 4 2 1 は、ステップ S 4 6 8 において、空のファイルリストに、部分 Hash と、部分データを保存した保存用ノード ID との組合せを書き込む。また、ファイルの取得要求として、クライアント端末からファイル Hash を受信すると、検索用ノードアプリケーション 4 2 1 は、ステップ S 4 6 9 において、ロケーションリストからファイル Hash を含むファイルリストを読み出して、クライアントアプリケーション 2 3 2 に送信する。

20

【 0 0 5 7 】

検索用ノード 2 2 1 が検索用ネットワーク 2 0 2 における投票に参加する場合、検索用ノードアプリケーション 4 2 1 は、ステップ S 4 7 0 において、各投票に参加すると、ステップ S 4 7 1 において、参加に対する報酬を取得する。

【 0 0 5 8 】

《クライアントアプリケーション》

以下、図 5 ～図 7 に従って、クライアントアプリケーション 2 3 2 の構成および動作について説明する。

30

【 0 0 5 9 】

図 5 は、本実施形態に係るクライアントアプリケーション 2 3 2 の構成を示す図である。

【 0 0 6 0 】

クライアントアプリケーション 2 3 2 は、通信制御部 5 0 0 ～ 5 0 2 と、ファイル保存処理部 5 0 3 と、リスト検索処理部 5 0 5 と、ファイル取得処理部 5 0 6 と、を備える。

【 0 0 6 1 】

通信制御部 5 0 0 は、クライアント端末 2 0 3 との通信を制御する。通信制御部 5 0 1 は、保存用ネットワーク 2 0 1 との間で P 2 P トンネルによる（ファイル Hash、部分 Hash、部分データ）の組合せや報酬などの通信を制御する。通信制御部 5 0 2 は、検索用ネットワーク 2 0 2 との間で保存用ノードリストまたはファイルリストをやり取りする独立した P 2 P ネットワークを制御する。

40

【 0 0 6 2 】

ファイル保存処理部 5 0 3 は、クライアント端末 2 0 3 から通信制御部 5 0 0 を介して取得したファイルを暗号化して Hash 値であるファイル Hash を生成する。また、ファイル保存処理部 5 0 3 は、暗号化したファイルを部分データに分割して、各部分データの Hash 値である部分 Hash を生成する。さらに、ファイル保存処理部 5 0 3 は、検索用ノードから取得した保存用ノードリストに記載された複数の保存用ノードから、部分データの分割数と冗長数を加えたブロック数の保存用ノードを選定する。そして、ファイル保存処理部 5 0 3 は、通信制御部 5 0 1 を介して、選定された保存用ノードに（ファイル Hash、部分 H

50

ash、部分データ)の組合せを送信して、ファイルHashと部分Hashとを検索キーとして部分データを保存させる。

【0063】

リスト検索処理部505は、クライアント端末203から取得を望むファイルを表す取得対象情報、例えば、文書名、ファイル名、動画タイトルなどを取得し、取得対象情報をファイルに対応付けられた検索キーとしてのファイルHashを生成する。リスト検索処理部505は、通信制御部502を介して、検索用ネットワーク202内の近傍にある検索用ノードから、ファイルHashを検索キーとして検索された、最新のロケーションリスト内のファイルリストを取得する。

【0064】

ファイル取得処理部506は、リスト検索処理部505から取得したファイルリストから各部分データの(部分Hash、保存用ノードID)の組合せを抽出する。そして、ファイル取得処理部506は、通信制御部501を介して、(ファイルHash、部分Hash、保存用ノードID)の組合せを用いて、各部分データに対応する保存用ノードから検索して読み出す。ファイル取得処理部506は、各部分データを復号して、正しく読み出された部分データのブロック数が所定数以上の場合には、部分データを合成して暗号化ファイルを再生する。ファイル取得処理部506は、再生された暗号化ファイルを暗号化鍵に対応する復号鍵で復号してクライアント端末203に送出する。

【0065】

図6は、本実施形態に係るクライアントアプリケーション232を含むクライアント端末203のハードウェア構成を示すブロック図である。

【0066】

図6で、CPU610は演算制御用のプロセッサであり、プログラムを実行することで図5の構成を実現する。CPU(Central Processing Unit)610は1つであっても複数であってもよい。ROM(Read Only Memory)620は、初期データおよびプログラムなどの固定データおよびプログラムを記憶する。ネットワークインタフェース630は、保存用ネットワーク201や検索用ネットワーク202との通信を制御する。

【0067】

RAM(Random Access Memory)640は、CPU610が一時記憶のワークエリアとして使用するランダムアクセスメモリである。RAM640には、本実施形態の実現に必要なデータを記憶する領域が確保されている。保存すべきファイル641は、保存用ネットワーク201の保存用ノード211に部分データとして分散保存するためのファイルである。取得したファイル642は、保存用ネットワーク201の保存用ノード211に分散保存された部分データを合成して復元されたファイルである。ロケーションリスト643は、検索用ネットワーク202の全ての検索用ノードに共有された分散保存の構成を示すリストである。ファイルHash644は、保存すべきファイル641あるいは取得したファイル642のHash値である。検索用ノードID645は、クライアント端末203がアクセスしているロケーションリストを保持する検索用ノードを識別するためのIDである。部分Hashと部分データと保存用ノードID646は、分割されて各保存用ノードに保存される部分データと、その部分データのHash値と、保存先ノードのIDである。なお、保存用ノードIDは保存用ノードを識別する識別情報のHash値であることが望ましい。電子キャッシュデータ647は、ファイル保存や取得に対応する料金の支払い、あるいは、ファイル保存や読出しの報酬の受取りのためのブロックチェーンされたデータである。送受信データ648は、ネットワークインタフェース630を介して送受信されるデータである。入出力データ649は、入出力インタフェース660を介して入出力機器と入出力するデータである。

【0068】

ストレージ650は、CPU610が使用する、本実施形態の実現に必要な以下のデータまたはプログラムが記憶されている。データベース651は、本実施形態の実現に必要な基本データを保持する。各種アルゴリズム652は、本実施形態の実現に必要なアルゴ

10

20

30

40

50

リズムを保持する。各種パラメータ 6 5 3 は、各種アルゴリズム 6 5 2 が用いる本実施形態の実現に必要なアルゴリズムを保持する。電子キャッシュ保持部 6 5 4 は、電子サイフとして、本実施形態の処理に必要な料金の支払い、あるいは、処理により得られる報酬をブロックチェーンされた電子キャッシュで保持する。

#### 【 0 0 6 9 】

ストレージ 6 5 0 には、以下のプログラムが格納される。クライアント端末制御プログラム 6 5 5 は、クライアント端末 2 0 3 の全体を制御するプログラムである。クライアントアプリケーション 2 3 2 は、クライアント端末 2 0 3 にダウンロードされて、あるいは、ブラウザ機能を伴ってクライアント端末 2 0 3 で実行されるアプリケーションである。クライアントアプリケーション 2 3 2 は、以下のモジュールを有する。

10

#### 【 0 0 7 0 】

ファイル保存処理部 5 0 3 として機能するファイル保存処理モジュールは、図 5 に図示された、保存すべきファイル 6 4 1 を分割した部分データを保存用ノードに分散保存させるモジュールである。リスト検索処理部 5 0 5 として機能するリスト検索処理モジュールは、図 5 に図示された、1つの検索用ノードが保持するロケーションリストからファイル Hash を検索キーとして検索したファイルリストを受信モジュールである。ファイル取得処理部 5 0 6 として機能するファイル取得処理モジュールは、図 5 に図示された、リスト検索処理モジュールにより受信したファイルリストが保持するファイル Hash と部分 Hash と保存用ノード ID との組合せを用いて部分データを読み出して合成して、取得したファイル 6 4 2 を復元するモジュールである。報酬処理部として機能する報酬処理モジュールは、

20

ファイル保存完了通知や、ファイル取得完了通知に回答して、参加ノード特に保存用ノードに対する報酬を提供するためのモジュールである。各種通信制御部 5 0 0、5 0 1、5 0 2 として機能する通信制御モジュールは、図 5 に図示された、各通信制御を行うモジュールである。

#### 【 0 0 7 1 】

入出力インタフェース 6 6 0 は、入出力デバイスとのデータ入出力を制御するためのインタフェースを行なう。本実施形態においては、入出力インタフェース 6 6 0 には、表示部 6 6 1、操作部 6 6 2、音声入出力部 6 6 3、記憶媒体 6 6 4 などが接続される。

#### 【 0 0 7 2 】

なお、図 6 の RAM 6 4 0 やストレージ 6 5 0 には、クライアント端末 2 0 3 が有する汎用の機能や他の実現可能な機能に関連するプログラムやデータは図示されていない。

30

#### 【 0 0 7 3 】

図 7 は、本実施形態に係るクライアントアプリケーション 2 3 2 の処理手順を示すフローチャートである。このフローチャートは、図 6 の CPU 6 1 0 が RAM 6 4 0 を用いて実行し、図 5 の機能構成を実現する。

#### 【 0 0 7 4 】

クライアント端末 2 0 3 は、ステップ S 7 1 1 において、ファイルの保存であるか否かを判定する。ファイルの保存であれば、クライアント端末 2 0 3 は、ステップ S 7 1 3 において、ファイルを分割して、分割された部分データを保存用ノード 2 1 1 に保存するデータ保存処理を実行する。

40

#### 【 0 0 7 5 】

ファイルの保存でないと判定された場合、クライアント端末 2 0 3 は、ステップ S 7 2 1 において、ファイルの取得（または閲覧）であるか否かを判定する。ファイルの取得であれば、クライアント端末 2 0 3 は、ステップ S 7 2 3 において、1つの検索用ノードが保持するロケーションリストから、ファイルを識別するファイル Hash に一致するファイルリストを受信するリスト検索処理を実行する。そして、クライアント端末 2 0 3 は、ステップ S 7 2 5 において、ファイルから分割された部分データを、ファイルリストに含まれる部分 Hash と保存用ノード ID とに基づいて読み出し、部分データからファイルを合成して復元するファイル取得処理を実行する。

#### 【 0 0 7 6 】

50

( ファイル保存処理部 )

図 8 は、本実施形態に係るファイル保存処理部 5 0 3 の機能構成を示すブロック図である。

【 0 0 7 7 】

ファイル保存処理部 5 0 3 は、ファイル暗号化部 8 3 1 と、ファイルHash生成部 8 3 2 と、部分データ生成部 8 3 3 と、部分Hash生成部 8 3 4 と、保存用ノード選定部 8 3 5 と、分散保存指示部 8 3 6 と、を備える。

【 0 0 7 8 】

ファイル暗号化部 8 3 1 は、暗号化アルゴリズムと暗号化鍵とを有し、クライアントから保存を指示されたファイルを暗号化する。なお、使用される暗号化アルゴリズムや暗号化鍵は限定されないが、クライアントに対応する暗号化鍵が配布されているとする。ファイルHash生成部 8 3 2 は、ファイル暗号化部 8 3 1 において暗号化されたファイルのHash値を算出する。なお、Hash値の算出方法は、その認証方法と対応していれば限定されない。部分データ生成部 8 3 3 は、分割アルゴリズムと分割アルゴリズムで算出された分割数とを有し、データ分割部として、ファイル暗号化部 8 3 1 において暗号化されたファイルを算出された分割数に基づいて分割する。なお、部分データ生成部 8 3 3 の分割アルゴリズムは、ファイルに対応して部分データの数を制御すると共に、保存時や取得時のエラーによってもデータ復元が可能ないように、分割における冗長のための処理が含まれる。部分Hash生成部 8 3 4 は、部分データ生成部 8 3 3 で分割された部分データのHash値を算出する。なお、Hash値の算出方法は、その認証方法と対応していれば限定されない。保存用ノード選定部 8 3 5 は、選定アルゴリズムと選定アルゴリズムで選定された保存先ノードIDとを有し、部分データ生成部 8 3 3 で冗長を含めて分割された分割数の部分データを保存する保存用ノードを、各々の保存用ノードの信頼性も考慮して選定する。なお、保存用ノードの識別は、保存用ノードに関連する情報のHash値であるのが望ましい。かかる保存用ノードを識別するHash値は、保存用ノードとして保存用ネットワーク 2 0 1 に参加する時に付与される。

【 0 0 7 9 】

分散保存指示部 8 3 6 は、保存データテーブル 8 3 7 を有し、ファイルHashと、部分Hash生成部 8 3 4 で生成された部分Hashを部分データを識別する識別子として部分データと組み合わせ、保存用ノード選定部 8 3 5 が選定した各保存用ノードへ保存を指示する。なお、図示しないが、部分データは暗号化鍵により暗号化される。

【 0 0 8 0 】

図 9 は、本実施形態に係るファイル保存処理部 5 0 3 で使用する保存データテーブル 8 3 7 の構成を示す図である。保存データテーブル 8 3 7 には、分散保存指示部 8 3 6 で保存用ノードに部分データを保存するための情報が保持される。

【 0 0 8 1 】

保存データテーブル 8 3 7 は、ファイルHash 9 2 1 に対応付けて、分割数 9 1 2 の各々の部分データ 9 2 3 について、部分Hash 9 2 2 と、対応する部分データ 9 2 3 と、選定された保存用ノードID 9 2 4 とを記憶する。

【 0 0 8 2 】

図 1 0 は、実施形態に係るファイル保存処理部 5 0 3 の処理手順を示すフローチャートである。このフローチャートは、図 6 のCPU 6 1 0 がRAM 6 4 0 を用いて実行し、図 8 のファイル保存処理部 5 0 3 の機能構成部を実現する。

【 0 0 8 3 】

ファイル保存処理部 5 0 3 は、ステップS 1 0 0 1 において、保存すべきファイルを取得したか否かを判定する。ファイルを取得した場合、ファイル保存処理部 5 0 3 は、ステップS 1 0 0 3 において、ファイルの暗号化処理を実行する。ファイル保存処理部 5 0 3 は、ステップS 1 0 0 5 において、暗号化されたファイルのHash値を算出する。

【 0 0 8 4 】

ファイル保存処理部 5 0 3 は、ステップS 1 0 0 7 において、暗号化されたファイルの

10

20

30

40

50

部分データへの分割処理を実行する。ファイル保存処理部 503 は、ステップ S1009 において、分割された部分データを保存する保存先の保存用ノードを選定する。

【0085】

ファイル保存処理部 503 は、ステップ S1011 において、選定された各保存用ノードに（ファイルHash、部分Hash、部分データ）により保存を指示する。

【0086】

図 11A は、本実施形態に係るファイル分割処理 S1007 の手順を示すフローチャートである。

【0087】

ファイル保存処理部 503 は、ステップ S1171 において、ファイルのサイズを取得する。ファイル保存処理部 503 は、ステップ S1173 において、データブロック数を、（データブロック数 = サイズ / 部分データサイズ）の式により算出する。次に、ファイル保存処理部 503 は、ステップ S1175 において、冗長ブロック数を、（冗長ブロック数 = データブロック数 / 所定数）の式により算出する。所定数は、本実施形態では例えば、3 が用いられる。次に、ファイル保存処理部 503 は、ステップ S1177 において、分割数を、（分割数 = データブロック数 + 冗長ブロック数）の式により算出する。そして、ファイル保存処理部 503 は、ステップ S1179 において、ステップ S1003 で暗号化されたファイルを算出された分割数に分割する。

【0088】

図 11B は、本実施形態に係る保存先ノードの選定処理 S1009 の手順を示すフローチャートである。

【0089】

ファイル保存処理部 503 は、ステップ S1191 において、ステップ S1177 で算出された分割数を取得する。次に、ファイル保存処理部 503 は、ステップ S1193 において、保存用ネットワーク 201 に参加する保存用ノードのリストを 1 つの検索用ノードから取得する。そして、ファイル保存処理部 503 は、ステップ S1195 において、ファイルの重要度や保存要求クライアントの重要度などを取得する。ファイル保存処理部 503 は、ステップ S1197 において、取得したファイルの重要度、および / または、保存要求クライアントの重要度を考慮して、クライアント端末により近い分割数に相当する保存用ノードを選定する。

【0090】

図 11B には、ステップ S1195 および S1197 における処理で用いられる保存用ノードのテーブル 1110 が図示されている。保存用ノードのテーブル 1110 は、各保存用ノード ID（Hash 値）1111 に対応付けて、保存用ノードの属性 1112、保存用ノードの信頼度（レベル）1113、保存用ノードの位置 1114 を記憶する。そして、各保存用ノード ID（Hash 値）1111 に対応付けて、選択結果 1115 を記憶する。

【0091】

（リスト検索処理部）

図 12 は、本実施形態に係るリスト検索処理部 505 の機能構成を示すブロック図である。

【0092】

リスト検索処理部 505 は、ファイルHash取得部 1251 と、ファイルHash送信部（ファイルハッシュ送信部）1252 と、ファイルリスト取得部 1253 と、ファイルリスト通知部 1255 と、を備える。ファイルHash取得部 1251 は、取得対象情報、例えば、取得対象のファイル名や文書名、動画題名などから、ファイルの保存時にあらかじめ保持された対応するファイルHashを取得する。ファイルHash送信部 1252 は、検索用ネットワーク 202 中の近接する 1 つの検索用ノードから、ファイルのHash値を検索キーとして最新のロケーションリストから検索したファイルリストを取得する。ファイルリスト通知部 1255 は、ファイルリスト 1256 を有し、ファイルリスト取得部 1253 が取得したファイルリストをファイル取得処理部 506 に通知する。

10

20

30

40

50

## 【 0 0 9 3 】

図 1 3 は、本実施形態に係るリスト検索処理部 5 0 5 で使用するファイルリスト 1 2 5 6 の構成を示す図である。図 1 3 には、ファイルリスト通知部 1 2 5 5 がファイル取得処理部 5 0 6 に通知するファイルリスト 1 2 5 6 の構成を図示する。

## 【 0 0 9 4 】

図 1 4 は、本実施形態に係るリスト検索処理部 5 0 5 の処理手順を示すフローチャートである。このフローチャートは、図 6 の C P U 6 1 0 が R A M 6 4 0 を用いて実行し、図 1 2 の機能構成を実現する。

## 【 0 0 9 5 】

リスト検索処理部 5 0 5 は、ステップ S 1 4 0 1 において、クライアント端末 2 0 3 からファイルを示す取得対象情報を取得する。リスト検索処理部 5 0 5 は、ステップ S 1 4 0 3 において、取得した取得対象情報に対応して保持されたファイル Hash を取得する。

10

## 【 0 0 9 6 】

リスト検索処理部 5 0 5 は、ステップ S 1 4 0 5 において、検索用ネットワーク 2 0 2 中の近くの検索用ノードにファイル Hash を送信する。そして、リスト検索処理部 5 0 5 は、ステップ S 1 4 0 7 において、検索用ノードから返信される、ファイル Hash を探索キーとして最新のロケーションリストを検索して得られたファイルリストの受信を待つ。ファイルリストが受信されれば、リスト検索処理部 5 0 5 は、ステップ S 1 4 1 1 において、ファイルリストをファイル取得処理部 5 0 6 に通知する。

## 【 0 0 9 7 】

20

( ファイル取得処理部 )

図 1 5 は、本実施形態に係るファイル取得処理部 5 0 6 の機能構成を示すブロック図である。

## 【 0 0 9 8 】

ファイル取得処理部 5 0 6 は、ファイルリスト取得部 1 5 6 1 と、部分データ情報抽出部 1 5 6 2 と、部分データ取得部 1 5 6 3 と、部分データ合成部 1 5 6 4 と、を備える。さらに、ファイル取得処理部 5 0 6 は、ファイル復号部 1 5 6 6 と、ファイル送出部 1 5 6 7 と、を備える。

## 【 0 0 9 9 】

ファイルリスト取得部 1 5 6 1 は、リスト検索処理部 5 0 5 からファイルリストを取得する。部分データ情報抽出部 1 5 6 2 は、ファイルリストに含まれる分割された部分データのロケーションを示す部分データ情報である保存用ノード I D と部分 hash とを抽出する。部分データ取得部 1 5 6 3 は、保存用ノード I D とファイル Hash と各部分データの部分 Hash とを用いて、保存用ノード I D が示す保存用ノードから一斉に部分データを取得する。

30

## 【 0 1 0 0 】

部分データ合成部 1 5 6 4 は、データ合成テーブル 1 5 6 5 を有し、部分データ取得部 1 5 6 3 が取得した部分データの数 が所定数以上になれば、部分データを合成して暗号化ファイルを復元する。すなわち、部分データの取得にエラーが生じた場合であっても、所定数以上の部分データの取得があればファイルを復元可能である。なお、部分データ合成部 1 5 6 4 では、保存用ノードから取得した部分データを保存時に暗号鍵に対応する復号鍵で復号する処理も行う。

40

## 【 0 1 0 1 】

ファイル復号部 1 5 6 6 は、復元された暗号化ファイルを保存時に暗号化した暗号鍵に対応する復号鍵で復号する。なお、かかる復号鍵は、クライアントに対応して配布された暗号化鍵に対応するものである。このように構成することにより、クライアント以外の人 は復号鍵をいずれかの方法で取得しない限り、ファイルを復号して復元することができない。ファイル送出部 1 5 6 7 は、復号されたファイルをクライアント端末 2 0 3 に送出する。ファイルの取得完了通知を報酬処理部に通知して、読出報酬を取得してもよい。

## 【 0 1 0 2 】

50



図16は、本実施形態に係るファイル取得処理部506で使用するデータ合成テーブル1565の構成を示す図である。データ合成テーブル1565は、部分データ合成部1564が取得した部分データから暗号化されたファイルを合成するために使用される。

【0103】

データ合成テーブル1565は、部分Hash1601と、読出された部分データ1602と、部分データ1602の所定数以上から合成された、暗号化されたファイルである合成ファイル1603と、復号されたファイルである復号ファイル1604とを記憶する。なお、部分データ1602の合成順序は、ブロックチェーン化された部分Hash1601から知ることができる。ブロックチェーン化されない部分Hash1601においては、合成順序を別途保存しておく必要がある。

10

【0104】

図17は、本実施形態に係るファイル取得処理部506の処理手順を示すフローチャートである。このフローチャートは、図6のCPU610がRAM640を用いて実行し、図15のファイル取得処理部506の機能構成を実現する。

【0105】

ファイル取得処理部506は、ステップS1701において、リスト検索処理部505からファイルリストを取得する。ファイル取得処理部506は、ステップS1703において、ファイルリストから分割されて保存された部分データを取得するための（部分Hash、保存用ノードID）の組合せを抽出する。ファイル取得処理部506は、ステップS1705において、（ファイルHash、部分Hash、保存用ノードID）の組合せを用いて、保存用ネットワーク201の保存用ノードから分割数の部分データを取得する。

20

【0106】

ファイル取得処理部506は、ステップS1707において、正しく取得した部分データの取得数を数える。例えば、保存用ノードの故障、保存用ノードの部分データの削除、改ざんやエラー、通信状況によるエラーなど、その一部は部分Hashにより検証可能である。ファイル取得処理部506は、ステップS1709において、正しく取得した部分データの取得数が所定数以上である、復元可能な数であるか否かを判定する。

【0107】

部分データの取得数が所定数以上である場合、ファイル取得処理部506は、ステップS1711において、正しく取得した部分データを合成する。ファイル取得処理部506は、ステップS1713において、合成ファイルを復号する。ファイル取得処理部506は、ステップS1715において、部分データから合成され復号されたファイルをクライアント端末203から送出する。

30

【0108】

部分データの取得数が所定数未満である場合、ファイル取得処理部506は、ステップS1719において、データ取得エラーをクライアント端末203に通知する。

【0109】

（報酬処理部）

図18は、本実施形態に係る報酬処理部1800の機能構成を示すブロック図である。なお、報酬処理部1800は、検索用サーバに搭載されていても、クライアントアプリケーション232に組み込まれていても、あるいは、検索用ノードアプリケーションや保存用ノードアプリケーションなどに分散されていてもよい。また、報酬処理部1800を含む管理サーバを別途設ける構成であってもよい。

40

【0110】

報酬処理部1800は、保存完了通知取得部1871と、取得完了通知取得部1872と、報酬算出アルゴリズム取得部1873と、報酬算出部1874と、報酬提供部1876と、を備える。

【0111】

保存完了通知取得部1871は、保存完了した各保存用ノードから部分データの保存完了通知を取得する。取得完了通知取得部1872は、ファイル取得処理部506からファ

50

イルの取得完了通知を取得する。

【 0 1 1 2 】

報酬算出アルゴリズム取得部 1 8 7 3 は、情報処理システム 2 0 0 における、保存用ネットワーク 2 0 1 に保存用ノードとして参加したクライアント、あるいは、検索用ネットワーク 2 0 2 に検索用ノードとして参加したクライアントに、どのように報酬を提供するかのアルゴリズムを取得する。本実施形態においては、例えば、ファイルの保存時に徴収する料金の内から総額 2 割程度の比較的少ない初期報酬を保存用ノードに提供し、その後は、所定期間でゼロとなる下降曲線で残りの 8 割をファイルの読み出し時に還元する報酬提供アルゴリズムを採用している。このようなアルゴリズムを用いることにより、保存用ノードの参加者が保存された部分データを削除しないように誘導している。しかしながら、報酬の提供アルゴリズムはこれに限定されない。

10

【 0 1 1 3 】

報酬算出部 1 8 7 4 は、報酬テーブル 1 8 7 5 を有し、報酬提供アルゴリズムに従って、部分データの保存完了時および部分データの読出し完了時に保存用ノードに対して提供する報酬を算出する。報酬提供部 1 8 7 6 は、報酬算出部 1 8 7 4 が算出した報酬を、部分データを保存あるいは読出した保存用ノードに提供する。

【 0 1 1 4 】

なお、図 1 8 には、検索用ネットワーク 2 0 2 の検索用ノードへの報酬については図示されてない。本実施形態においては、例えば、検索用ネットワーク 2 0 2 への新規参加時、あるいは、保存用ノードに対して提供する報酬の算出アルゴリズムなどの決定あるいは変更時などに行われる保存用ノードによる投票への参加に対して、報酬を提供する。

20

【 0 1 1 5 】

図 1 9 は、本実施形態に係る報酬処理部 1 8 0 0 で使用する報酬テーブル 1 8 7 5 の構成を示す図である。報酬テーブル 1 8 7 5 は、報酬算出部 1 8 7 4 が本実施形態のアルゴリズムで保存用ノードに報酬を提供する場合に用いる。

【 0 1 1 6 】

報酬テーブル 1 8 7 5 は、保存対象あるいは取得対象のファイル Hash によるファイル ID 1 9 1 0 に対応付けて、保存料金 1 9 0 2 と取得または閲覧料金 × 回数 1 9 0 3 とを考慮して算出された、データ保存時の報酬 1 9 0 4 とデータ読出し時の報酬 1 9 0 5 とを記憶する。なお、データ読出し時の報酬 1 9 0 5 の変化は、初期値と減少する変化曲線とを含む。

30

【 0 1 1 7 】

図 2 0 は、本実施形態に係る報酬処理部 1 8 0 0 の処理手順を示すフローチャートである。このフローチャートは、報酬処理部 1 8 0 0 の C P U が R A M を用いて実行し、図 1 8 の報酬処理部 1 8 0 0 の機能構成部を実現する。

【 0 1 1 8 】

報酬処理部 1 8 0 0 は、ステップ S 2 0 0 1 において、各保存用ノードからの保存完了通知、または、ファイル取得処理部 5 0 6 からの取得完了通知を待つ。保存完了通知、または、取得完了通知があれば、報酬処理部 1 8 0 0 は、ステップ S 2 0 0 3 において、部分データの保存であるかファイルの取得であるかを判定する。

【 0 1 1 9 】

部分データの保存完了であれば、報酬処理部 1 8 0 0 は、ステップ S 2 0 0 5 において、保存料金から各保存用ノードへの報酬 X を算出する。そして、報酬処理部 1 8 0 0 は、ステップ S 2 0 0 7 において、部分データを保存した保存用ノードに報酬 X を提供する。

40

【 0 1 2 0 】

一方、ファイルを取得した場合、報酬処理部 1 8 0 0 は、ステップ S 2 0 0 9 において、保存料金 ( + 取得料金 ) から各保存用ノードへの報酬 Y を算出する。ここで、報酬 Y は報酬 X よりも多い。そして、報酬処理部 1 8 0 0 は、ステップ S 2 0 1 1 において、ファイルの部分データを正しく読出した保存用ノードに報酬 Y を提供する。

【 0 1 2 1 】

《 保存用ノード 》

50

図 2 1 は、本実施形態に係る保存用ノード 2 1 1 の機能構成を示すブロック図である。

【 0 1 2 2 】

保存用ノード 2 1 1 は、P 2 P の通信制御部 2 1 0 1 と、入出力インタフェース 2 1 0 2 と、保存用ノードアプリケーションダウンロード部 2 1 0 3 と、保存用ノードアプリケーション実行部 2 1 0 4 と、を備える。

【 0 1 2 3 】

P 2 P の通信制御部 2 1 0 1 は、クライアント端末 2 0 3 や保存用ネットワーク 2 0 1 の他の保存用ノードとの P 2 P 通信を制御する。入出力インタフェース 2 1 0 2 は、保存用ノード 2 1 1 に接続する入出力機器である、表示部 2 1 2 1、操作部 2 1 2 2、音声入出力部 2 1 2 3、記憶媒体 2 1 2 4 などとの入出力を制御する。保存用ノードアプリケーションダウンロード部 2 1 0 3 は、種々のクライアント端末が保存用ノードとして保存用ネットワーク 2 0 1 に参入するために保存用ノードアプリケーションをダウンロードする。保存用ノードアプリケーション実行部 2 1 0 4 は、保存用ノードアプリケーションダウンロード部 2 1 0 3 がダウンロードした保存用ノードアプリケーションを実行し、保存用ノードとして機能する。

【 0 1 2 4 】

保存用ノードアプリケーション実行部 2 1 0 4 は、Hash I D 記憶部 2 1 4 1 と、保存用部分データ受信部 2 1 4 2 と、ストレージ 2 1 4 3 と、部分データ保存完了通知部 2 1 4 4 と、を有する。さらに、保存用ノードアプリケーション実行部 2 1 0 4 は、部分データ要求受信部 2 1 4 5 と、部分データ送信部 2 1 4 6 と、電子キャッシュ保存部 2 1 4 7 と、料金送信部 2 1 4 8 と、報酬受信部 2 1 4 9 と、を有する。

【 0 1 2 5 】

Hash I D 記憶部 2 1 4 1 は、保存用ノードとして保存用ネットワーク 2 0 1 に参入した時に付与される保存用ノード情報の Hash 値である I D を記憶する。この保存用ノード Hash I D は、保存用ノード I D として使用される。保存用部分データ受信部 2 1 4 2 は、ファイル保存処理部 5 0 3 からの保存用の部分データをファイル Hash および部分 Hash と共に受信する。ストレージ 2 1 4 3 は、保存用部分データ受信部 2 1 4 2 が受信した（ファイル Hash、部分 Hash、部分データ）を、ファイル Hash と部分 Hash とを検索キーとして保存する。部分データ保存完了通知部 2 1 4 4 は、ストレージ 2 1 4 3 へのファイル Hash と部分 Hash とを検索キーとした部分データの保存が完了した場合に、その旨を（ファイル Hash、部分 Hash、保存用ノード I D）の組合せと共に検索用ノードに通知する。部分データ要求受信部 2 1 4 5 は、ファイル取得処理部 5 0 6 からのファイル hash と部分 Hash とを検索キーとする部分データの読み出し要求を受信する。部分データ送信部 2 1 4 6 は、ファイル Hash と部分 Hash との検索キーにより検索された部分データをストレージ 2 1 4 3 から読出して、ファイル取得処理部 5 0 6 に送信する。

【 0 1 2 6 】

電子キャッシュ保存部 2 1 4 7 は、保存用ノードとして保存用ネットワーク 2 0 1 に参入する場合に、設定される電子キャッシュの記憶部である。料金送信部 2 1 4 8 は、保存用ノードとして参入する場合、あるいは、他の料金支払いが必要な場合に、電子キャッシュ保存部 2 1 4 7 から電子キャッシュを送金する。報酬受信部 2 1 4 9 は、報酬処理部 1 8 0 0 からの報酬を受信して、電子キャッシュ保存部 2 1 4 7 に保存する。

【 0 1 2 7 】

図 2 2 は、本実施形態に係る保存用ノード 2 1 1 の動作手順を示すフローチャートである。このフローチャートは、保存用ノード 2 1 1 となるクライアント端末の C P U が R A M を用いて実行し、図 2 1 の機能構成を実現する。

【 0 1 2 8 】

保存用ノード 2 1 1 は、ステップ S 2 2 1 1 において、保存用の部分データの受信か否かを判定する。保存用の部分データの受信であると判定する場合、保存用ノード 2 1 1 は、ステップ S 2 2 1 3 において、取得した（ファイル hash、部分 Hash、部分データ）の組合せをストレージ 2 1 4 3 に保存する。そして、ストレージ 2 1 4 3 への保存が完了す

10

20

30

40

50

ると、保存用ノード211は、ステップS2215において、保存完了を（ファイルhash、部分Hash、保存用ノードID）の組合せと共に、検索用ノードに通知する。

【0129】

保存用の部分データの受信でないと判定する場合、保存用ノード211は、ステップS2221において、部分データの読み出し要求が否かを判定する。部分データの読み出し要求であると判定された場合、保存用ノード211は、ステップS2223において、読み出し要求に伴うファイルHashと部分Hashとを受け取り、ファイルHashと部分Hashとを検索キーとしてストレージ2143に保存された部分データを検索する。保存用ノード211は、ステップS2225において、部分データがストレージ2143内に有るか否かを判定する。部分データが見つかった場合、保存用ノード211は、ステップS2227において、部分データをファイルHashおよび部分Hashと共にファイル取得処理部506に送信する。部分データが見つからなかった場合、保存用ノード211は、ステップS2229において、エラー処理を行う。

10

【0130】

保存用の部分データの受信でもなく、部分データの要求でもないとして判定する場合、保存用ノード211は、ステップS2231において、料金の送信が否かを判定する。料金の送信と判定された場合、保存用ノード211は、ステップS2233において、電子キャッシュ保存部2147から電子キャッシュを取得し、ステップS2235において、取得した電子キャッシュを送信する。保存用の部分データの受信でもなく、部分データの要求でもなく、料金の送信でもないとして判定する場合、保存用ノード211は、ステップS2241において、報酬の受信が否かを判定する。報酬の受信と判定された場合、保存用ノード211は、ステップS2243において、報酬処理部1800からの報酬を受信し、ステップS2245において、受信した報酬を電子キャッシュ保存部2147に保存する。

20

【0131】

《検索用ノード》

図23は、本実施形態に係る検索用ノード221の機能構成を示すブロック図である。なお、図23には、検索用ノード221が行う、ロケーションリスト317内の検索用ノードリストや保存用ノードリストを作成あるいは更新するための機能構成については、図面が煩雑となるため図示していない。

【0132】

検索用ノード221は、P2Pの通信制御部2301と、入出力インタフェース2302と、検索用ノードアプリケーションダウンロード部2303と、検索用ノードアプリケーション実行部2304と、を備える。

30

【0133】

P2Pの通信制御部2301は、クライアント端末203や検索用ネットワーク202の他の検索用ノードとのP2P通信を制御する。入出力インタフェース2302は、検索用ノード221に接続する入出力機器である、表示部2321、操作部2322、音声入出力部2323、記憶媒体2324などとの入出力を制御する。検索用ノードアプリケーションダウンロード部2303は、種々のクライアント端末が検索用ノードとして検索用ネットワーク202に参入するために検索用ノードアプリケーションをダウンロードする。検索用ノードアプリケーション実行部2304は、検索用ノードアプリケーションダウンロード部2303がダウンロードした検索用ノードアプリケーションを実行し、検索用ノードとして機能する。

40

【0134】

検索用ノードアプリケーション実行部2304は、検索用ノードHashID記憶部2341と、ロケーションリスト更新指示受信部2342と、ロケーションリスト保存ストレージ2343と、部分データ保存完了通知受信部2344と、を有する。さらに、検索用ノードアプリケーション実行部2304は、ファイルリスト要求受信部2345と、ファイルリスト送信部2346と、電子キャッシュ保存部2347と、料金送信部2348と、報酬受信部2349と、を有する。

50

## 【 0 1 3 5 】

検索用ノードHash I D記憶部 2 3 4 1 は、検索用ノードとして検索用ネットワーク 2 0 2 に参入した時に付与される検索用ノード情報のHash値である I D を記憶する。この検索用ノードHash I D は、検索用ノードを特定する I D として使用される。ロケーションリスト更新指示受信部 2 3 4 2 は、ファイル保存要求の場合に、クライアント端末 2 0 3 からファイルHashを受信して、ロケーションリストにファイルHashを検索キーとする空のファイルリストを追加する。ロケーションリスト保存ストレージ 2 3 4 3 は、ロケーションリスト更新指示受信部 2 3 4 2 により更新された最新のロケーションリストを保存し、他の検索用ノードと共有する。部分データ保存完了通知受信部 2 3 4 4 は、部分データの保存が完了した保存用ノードから保存完了通知を、（ファイルHash、部分Hash、保存用ノード I D ）の組合せと共に受信して、ロケーションリスト保存ストレージ 2 3 4 3 内の空のファイルリストに挿入する。ファイルリスト要求受信部 2 3 4 5 は、ファイル取得要求の場合に、クライアント端末 2 0 3 のリスト検索処理部 5 0 5 から、ファイルHashを検索キーとする最新ロケーションリストからのファイルリストの読み出し要求を受信する。ファイルリスト送信部 2 3 4 6 は、ロケーションリスト保存ストレージ 2 3 4 3 に保持されたロケーションリストを、ファイルHashを検索キーとして検索し、見つけたファイルリストをリスト検索処理部 5 0 5 に送信する。

10

## 【 0 1 3 6 】

電子キャッシュ保存部 2 3 4 7 は、検索用ノードとして検索用ネットワーク 2 0 2 に参入する場合に、設定される電子キャッシュの記憶部である。料金送信部 2 3 4 8 は、検索用ノードとして参入する場合、あるいは、投票の参加するなどによる他の料金支払いが必要な場合に、電子キャッシュ保存部 2 3 4 7 から電子キャッシュを送金する。報酬受信部 2 3 4 9 は、報酬処理部 1 8 0 0 からの報酬を受信して、電子キャッシュ保存部 2 3 4 7 に保存する。

20

## 【 0 1 3 7 】

図 2 4 は、本実施形態に係る検索用ノード 2 2 1 の動作手順を示すフローチャートである。このフローチャートは、検索用ノード 2 2 1 となるクライアント端末の C P U が R A M を用いて実行し、図 2 3 の機能構成を実現する。なお、図 2 4 においても、検索用ノード 2 2 1 が行う、ロケーションリスト 3 1 7 の検索用ノードリストや保存用ノードリストを作成あるいは更新するための動作手順については、図面が煩雑となるため図示していない。

30

## 【 0 1 3 8 】

検索用ノード 2 2 1 は、ステップ S 2 4 1 1 において、ロケーションリスト更新指示の受信か否かを判定する。ロケーションリスト更新指示の受信であると判定する場合、検索用ノード 2 2 1 は、ステップ S 2 4 1 3 において、ロケーションリスト更新指示に付随して送信されたファイルHashを取得する。そして、検索用ノード 2 2 1 は、ステップ S 2 4 1 3 において、取得したファイルHashを検索キーとする空のファイルリストをロケーションリストに追加し、最新のロケーションリストをロケーションリスト保存ストレージ 2 3 4 3 に保存する。

## 【 0 1 3 9 】

40

ロケーションリスト更新指示の受信でないと判定する場合、検索用ノード 2 2 1 は、ステップ S 2 4 2 1 において、部分データの保存完了通知か否かを判定する。部分データの保存完了通知であると判定された場合、検索用ノード 2 2 1 は、ステップ S 2 4 2 3 において、保存完了通知に付随するファイルHashによりロケーションリスト内の空の（あるいは未完の）ファイルリストを検索する。そして、検索用ノード 2 2 1 は、ステップ S 2 4 2 5 において、空の（あるいは未完の）ファイルリストに保存完了通知と共に受信した（部分Hash、保存用ノード I D ）の組合せを挿入する。

## 【 0 1 4 0 】

ロケーションリストの受信でなく、部分データの保存完了通知でもないとは判定する場合、検索用ノード 2 2 1 は、ステップ S 2 4 3 1 において、ファイルリストの読み出し要求

50

か否かを判定する。ファイルリストの読み出し要求であると判定された場合、検索用ノード221は、ステップS2433において、ロケーションリスト保存ストレージ2343に保持された最新のロケーションリストから、読み出し要求と共に受信したファイルHashを検索キーとしてファイルリストを検索する。そして、検索用ノード221は、ステップS2435において、ファイルリストを読み出し要求元のリスト検索処理部505に送信する。

【0141】

ロケーションリストの受信でもなく、部分データの保存完了通知でもなく、ロケーションリストの要求でもないとは判定する場合、検索用ノード221は、ステップS2441において、料金の送信か否かを判定する。料金の送信と判定された場合、検索用ノード221は、ステップS2433において、電子キャッシュ保存部2347から電子キャッシュを取得し、ステップS2445において、取得した電子キャッシュを送信する。

10

【0142】

ロケーションリストの受信でもなく、部分データの保存完了通知でもなく、ロケーションリストの要求でもなく、料金の送信でもないとは判定する場合、検索用ノード221は、ステップS2451において、報酬の受信か否かを判定する。報酬の受信と判定された場合、検索用ノード221は、ステップS2453において、報酬処理部1800からの報酬を受信し、ステップS2455において、受信した報酬を電子キャッシュ保存部2347に保存する。

【0143】

20

(クライアント端末のハードウェア構成)

図25は、本実施形態に係る保存用ノード211または検索用ノード221となるクライアント端末のハードウェア構成を示すブロック図である。

【0144】

図25で、CPU2510は演算制御用のプロセッサであり、プログラムを実行することで図21または図23の機能構成部を実現する。CPU(Central Processing Unit)2510は1つであっても複数であってもよい。ROM(Read Only Memory)2520は、初期データおよびプログラムなどの固定データおよびプログラムを記憶する。ネットワークインタフェース2530は、クライアント端末203や、保存用ネットワーク201や検索用ネットワーク202の他の保存用ノードや検索用ノードとの通信を制御する。

30

【0145】

RAM(Random Access Memory)2540は、CPU2510が一時記憶のワークエリアとして使用するランダムアクセスメモリである。RAM2540には、本実施形態の実現に必要なデータを記憶する領域が確保されている。保存用ノードのデータ2541は、保存用ノードとして動作する場合のデータである。保存用ノードのデータ2541には、部分Hashや部分データが含まれる。検索用ノードのデータ2542は、検索用ノードとして動作する場合のデータである。検索用ノードのデータ2542には、ファイルHashや、ファイルHashを検索キーとするファイルリストや、登録されている保存用ノードの一覧である保存用ノードリストが含まれる。電子キャッシュデータ2543は、送金あるいは報酬受信されるデータである。送受信データ2544は、ネットワークインタフェース2530を介して送受信されるデータである。入出力データ2545は、入出力インタフェース2102や2302を介して入出力機器と入出力するデータである。

40

【0146】

ストレージ2550は、CPU2510が使用する、本実施形態の実現に必要な以下のデータまたはプログラムが記憶されている。データベース2551は、本実施形態の実現に必要な基本データを保持する。保存用ノードまたは検索用ノードのHashID記憶部2141/2341は、ノード参入時に配布されるノードIDである。ストレージ2143/2343は、部分データやロケーションリストを保存するストレージである。電子キャッシュ保存部2147/2347は、電子キャッシュを保存するストレージである。

【0147】

50

ストレージ 2 5 5 0 には、以下のプログラムが格納される。クライアント端末制御プログラム 2 5 5 2 は、保存用ノードや検索用ノードに参入したクライアント端末の全体を制御するプログラムである。保存用ノードアプリケーションプログラム 2 5 5 3 は、保存用ノードとして機能する場合のアプリケーションプログラムである。検索用ノードアプリケーションプログラム 2 5 5 4 は、検索用ノードとして機能する場合のアプリケーションプログラムである。

【 0 1 4 8 】

入出力インタフェース 2 1 0 2 / 2 3 0 2 は、入出力デバイスとのデータ入出力を制御するためのインタフェースを行なう。本実施形態においては、入出力インタフェース 2 1 0 2 / 2 3 0 2 には、表示部 2 1 2 1 / 2 3 2 1、操作部 2 1 2 2 / 2 3 2 2、音声入出力部 2 1 2 3 / 2 3 2 3、記憶媒体 2 1 2 4 / 2 3 2 4 などが接続される。

10

【 0 1 4 9 】

なお、図 2 5 の R A M 2 5 4 0 やストレージ 2 5 5 0 には、保存用ノードや検索用ノードとして機能するクライアント端末が有する汎用の機能や他の実現可能な機能に関連するプログラムやデータは図示されていない。

【 0 1 5 0 】

本実施形態によれば、データおよびその分割された部分データが Hash 化されて、検索用ネットワークと保存用ネットワークとの独立した二層構造で管理されるため、高い安全性を担保しつつ、小規模ストレージの集合により大規模データサーバと同様の機能を実現することができる。

20

【 0 1 5 1 】

また、本実施形態によれば、ファイルは暗号化されて部分データに分割され、ファイルは部分データから合成されて復号されるので、機密性を高めることができる。また、保存するブロック数に冗長性を持たせて保存するので、所定数以上の正常なブロックがあればデータを再現できる。また、保存時の報酬と読出時の報酬とを制御することにより、保存用ノードでの部分データの喪失を防ぐことができる。

【 0 1 5 2 】

また、本実施形態によれば、インターネット上で第三者がストレージ容量を提供し、それに対して報酬を支払うことによって、効率的なインセンティブシステムによりシステム全体を維持および管理することができる。したがって、ユーザはハードディスクの空きスペースを十分に活用し、収益を得ることができる。すなわち、膨大なデータ量が発生し、これらのデータをどのように保存して、よりよいデータをどのように利用していくという問題がある中で、世界中に存在するハードディスクの大半が使用されておらず、価値のある資源が知らない間に消費されている。本実施形態においては、ユーザがソフトウェア（保存用ノードアプリケーションや検索用ノードアプリケーション）を、パソコンやスマートフォンにダウンロードあるいはインストールした後、ネットワークノード（保存用ノードおよび/または検索用ノード）になれる。したがって、ユーザは、専用のマイニングマシンを自宅に設置することで報酬を得られることになる。

30

【 0 1 5 3 】

また、本実施形態によれば、システムは 2 層の保存用ネットワークと検索用ネットワークとに分離されて構成され、ネットワーク効率を高める同時に、マイニング閾値を下げる。マイニングマシンはストレージと検索の要求にとって異なり、検索には、高価なコンピュータティングパワーとエネルギー消費が必要だが、ストレージには、空きストレージリソースと帯域幅資源とが必要である。ストレージと検索との分離は、低コストのマイニングマシンを使ってシステムの運営に貢献するのに役に立つ。さらに、2 層ネットワークの保存と検索とが分離されることによって、ネットワークの効率を向上させる。なお、実施形態では言及されていないが、検索用ノードは、P 2 P ネットワーク全体の中で最も見つけられ攻撃され易い部分であるので、検索ノード用に対する保護を強化する必要がある、検索用ノードの I P アドレスを暗号化して保護している。

40

【 0 1 5 4 】

50

本実施形態によれば、ユーザのファイルデータを一定数に分割して保存し、分割された部分データが異なるノードに保存されていることを保証する。あるノードの部分データが異常な状況で消えても、他のノードのバックアップを通じて、ユーザのファイルデータを完全に復元することができる。また、保存されたデータのセキュリティを保証することができる。分散型ストレージは、戦争、自然災害、あるいは人為的な原因で発生するデータの損失を減らし、価値のあるデータを永久に保存できるように有利になる。すなわち、ファイルデータは破片に分割し、異なったノードに分布するので、データの安全性はより高く、同時に覗きされたりコピーされたりはしない。さらに、データの冗長技術を加えることによって、分割された破片データが失われた場合や、ノードがオフラインになったとしても、完全にファイルを復元することができる。同時にある破片が復元されても、一部のデータだけなのでファイルデータ全体は保護される。なお、ノードに障害が発生してアクセス不能な場合、システムはネットワークの既存の副本を新しいノードに転送することによって、ネットワーク複製プロセスを開始して、ファイルデータを復元する。

10

#### 【0155】

また、本実施形態によれば、保存されたデータは、デバイスによってブロックされ、暗号化されるなどの過程を経て、さらに分散型ストレージに配布され、これにより、安全性は非常に高いレベルにまで向上させて、ユーザのファイルデータはネットワーク内の他のいかなる人も覗くことができない。また、各ノードが実際に保存しているデータは、ファイルの一部であり、その上で暗号化された方法で保存されているので、データはより安全に保護できる。ストレージノードを提供したユーザが、ファイルデータの一部を見る機会があったとしても、意味のないデータだけであり、秘密キーを得るユーザのみが、正常にダウンロードを行うことができる。

20

#### 【0156】

本実施形態によれば、ファイルデータをダウンロード中に、分割された破片データが再編成されるので、速度が集中型ストレージよりもはるかに速くなる。すなわち、1つのファイルが多く破片に分散されて世界各地のストレージノードに保存されており、ユーザがファイルをダウンロードしようとする、該当するアドレス（ハッシュ値）のみ検索するだけで、各ストレージノードから同時にデータを取得することができる。そのため、集中型ストレージよりスピードが速くなります。また、データ伝送速度に関しても、ユーザがデータを読み取る必要がある場合、全ての保存者が同時にユーザのために自分の保存したデータを送信し、アプリケーションが受信した後自動的に合成を行う。したがって、ユーザのダウンロード速度は、主にネットワークのダウンロード帯域幅により決まる。そのため、今後急激な成長を遂げる5G技術などにより更なるデータ伝送速度が達成される。

30

#### 【0157】

また、本実施形態によれば、基準化された基盤技術のプラットフォームの提供を通じて、サポート基準ツールを、分散式資源を必要としているユーザに提供できる。このプラットフォームにより自分のDAPP（decentralized application：分散型アプリケーション）を開発することができる。そして、サーバやPC、モバイルストレージなどの集中型ストレージと比較して、本実施例のP2P分散型ストレージは、ストレージとインターネットの効率を向上させ、分散型技術を通じてストレージの容量とネットワークリソースの浪費を解決した。すなわち、データの自動分配、柔軟な拡張の実現、運営コストの低減、資源浪費を避けることができた。例えば、それに対するコストは従来のクラウドストレージだと10TM（Translation Memory）あたり月間コストは100ドルだが、本実施形態のP2P分散型ストレージに移行することによって月間コストを1/5に抑えることができた。

40

#### 【0158】

さらに詳細には、例えば、DHT（Distributed Hash Table：分散型ハッシュテーブル）を用いることで、Hashキー値によってユニークと識別することできる情報を、ある条件/プロトコルに従って複数のノードに保存される。これにより中央集権型サーバなどの単一故障状態でネットワーク全体が麻痺することを効果的に避けることができる。中央ノー

50



ドサーバと違って、DHTによるネットワーク内の各ノードはネットワーク全体の情報を維持する必要がなく、隣接する後続ノード情報を保存するだけなので、帯域幅の占有および資源消費を大幅に減少する。また、DHTによるネットワークはキーワードの最も近いノードに冗長データもバックアップし、単一ノードの障害を回避できる。

【0159】

[第4実施形態]

次に、本発明の第4実施形態に係る情報処理システムについて説明する。本実施形態に係る情報処理システムは、上記第3実施形態と比べると、それぞれ独立したクライアント端末とクライアントアプリケーションを有するアプリケーションサーバとを有する点で異なる。その他の構成および動作は、第2実施形態と同様であるため、同じ構成および動作については同じ符号を付してその詳しい説明を省略する。

10

【0160】

《情報処理システムの構成》

図26は、本実施形態に係る情報処理システム2600の構成を示すブロック図である。図26においては、情報処理システム2600がアプリケーションサーバ2633を備え、アプリケーションサーバ2633が、データ保存処理、リスト保存処理、リスト検索処理およびデータ取得処理を含む処理を実行する。

【0161】

図26においては、クライアントアプリケーション232がアプリケーションサーバ2633に変更されている。

20

【0162】

なお、図2や図26においては、クライアントアプリケーション232やアプリケーションサーバ2633のそれぞれがファイルの保存や取得の全機能を果たすように図示しているが、これらの機能をクライアント端末203の処理能力に応じて振り分けるよう構成してもよい。

【0163】

本実施形態によれば、処理能力の比較的低いクライアント端末であっても、あるいは、通信能力が比較的低いシステムであっても、ファイルの分散保存とその読み出し再生を行う情報処理システムが実現できる。

【0164】

30

[第5実施形態]

次に、本発明の第5実施形態に係る情報処理システムについて説明する。本実施形態に係る情報処理システムは、上記第3実施形態および第4実施形態と比べると、クライアント端末、保存用ノードおよび検索用ノードが既存のIPアドレスを用いたHTTPに代わるHashアドレスを用いたプロトコルで通信する点で異なる。その他の構成および動作は、第3実施形態または第4実施形態と同様であるため、同じ構成および動作については同じ符号を付してその詳しい説明を省略する。

【0165】

《情報処理システムの構成》

図27は、本実施形態に係る情報処理システム2700の構成を示すブロック図である。図27においては、Hashアドレスを用いたプロトコルをIPWBで示している。すなわち、プロトコルとしてIPWB://...を用いている。

40

【0166】

図27の情報処理システム2700においては、保存用ネットワーク2701と、検索用ネットワーク2702と、クライアントアプリケーション2732との間において、IPWB://...で表現されるHashアドレスによるP2P通信が可能となっている。

【0167】

本実施形態によれば、非集権分散ネットワークによる分散型ストレージが実現される。すなわち、本実施形態は、多数のP2P接続を同時に転送することができる。このような動的な柔軟性と展延性により、システムのスケーラビリティが拡張上限なしに実現する。

50

そして、将来的に、本実施形態のシステムは、P 2 P 分散型クラウドストレージのみの提供だけではなく、そのストレージを利用したWebページを開設することも可能になる。すなわち、本実施形態が提供するプラットフォームにおいては、ユーザ自らがP 2 P 分散ストレージのサービス事業者になることができる。サービス事業者は、本実施形態のブロックチェーンを利用し、独自サービスの決済で利用するトークンを発行することができる。そして、トークンの発行者は、ストレージの利用料金体系や、ストレージ容量提供者への報酬体系を自由に設定することにより、サービスにオリジナリティを出すこともできる。

【 0 1 6 8 】

〔 他の実施形態 〕

以上、実施形態を参照して本願発明を説明したが、本願発明は上記実施形態に限定されるものではない。本願発明の構成や詳細には、本願発明の技術的範囲で当業者が理解し得る様々な変更をすることができる。また、それぞれの実施形態に含まれる別々の特徴を如何様に組み合わせたシステムまたは装置も、本発明の技術的範囲に含まれる。

【 0 1 6 9 】

また、本発明は、複数の機器から構成されるシステムに適用されてもよいし、単体の装置に適用されてもよい。さらに、本発明は、実施形態の機能を実現する情報処理プログラムが、システムあるいは装置に供給され、内蔵されたプロセッサによって実行される場合にも適用可能である。したがって、本発明の機能をコンピュータで実現するために、コンピュータにインストールされるプログラム、あるいはそのプログラムを格納した媒体、そのプログラムをダウンロードさせるWWW(World Wide Web)サーバも、プログラムを実行するプロセッサも本発明の技術的範囲に含まれる。特に、少なくとも、上述した実施形態に含まれる処理ステップをコンピュータに実行させるプログラムを格納した非一時的コンピュータ可読媒体 ( non-transitory computer readable medium ) は本発明の技術的範囲に含まれる。

10

20

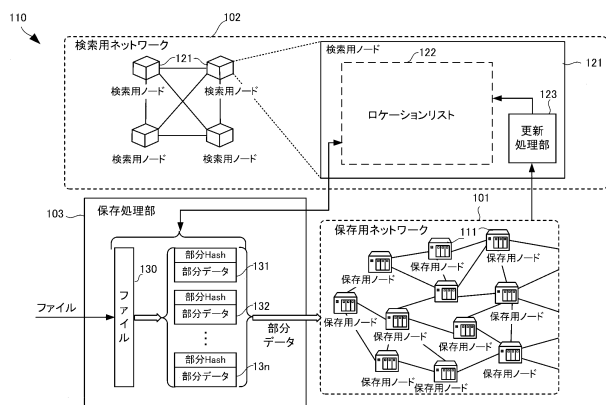
30

40

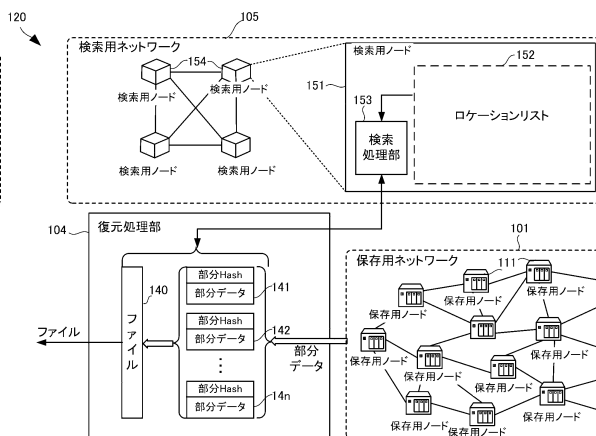
50

【図面】

【 図 1 A 】



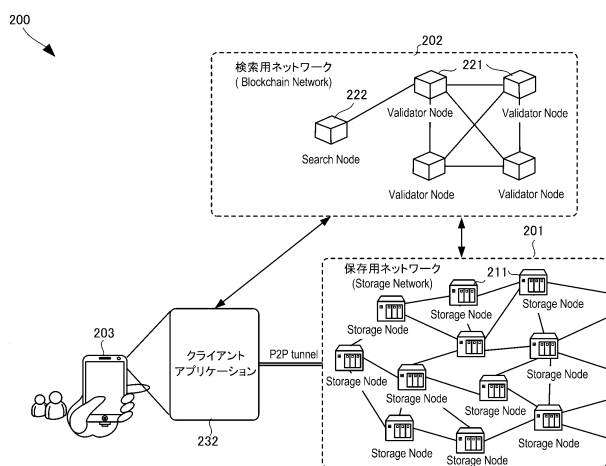
【 図 1 B 】



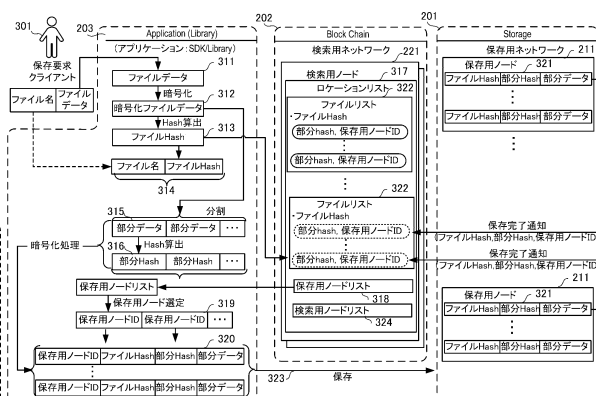
10

20

【圖 2】



【 図 3 A 】

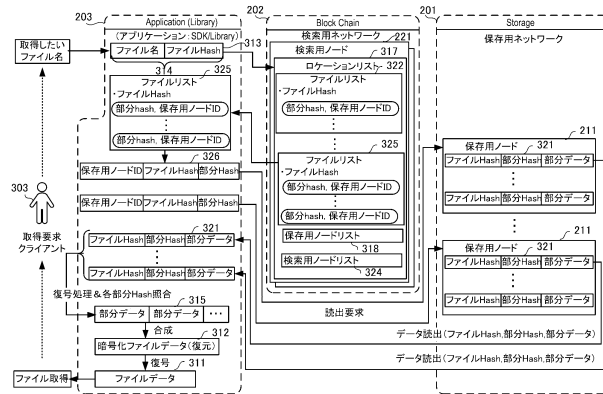


30

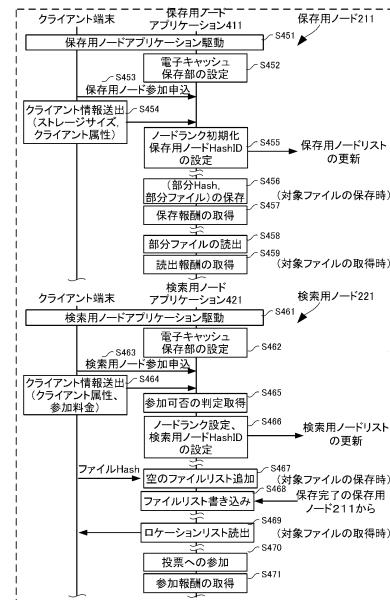
40

50

【図 3 B】

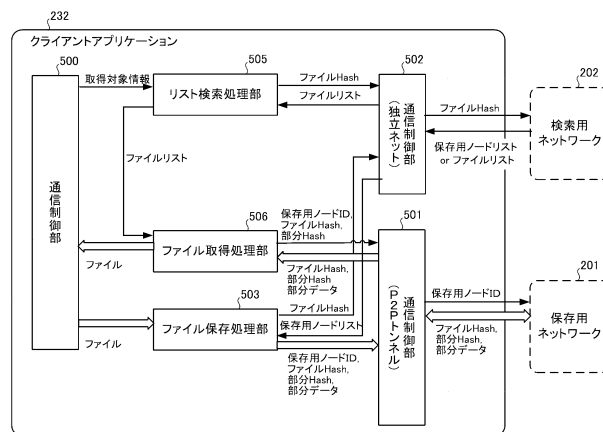


【図 4】

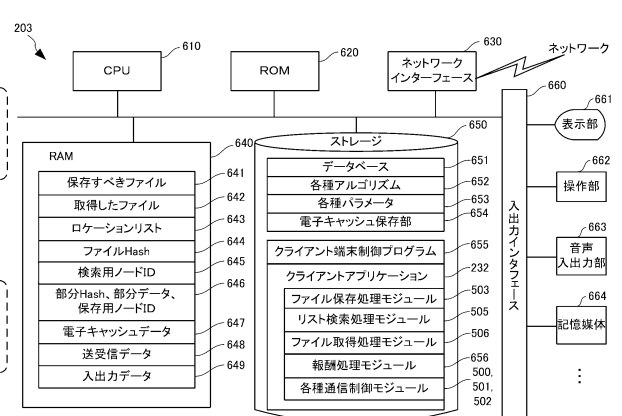


10

【図 5】



【図 6】



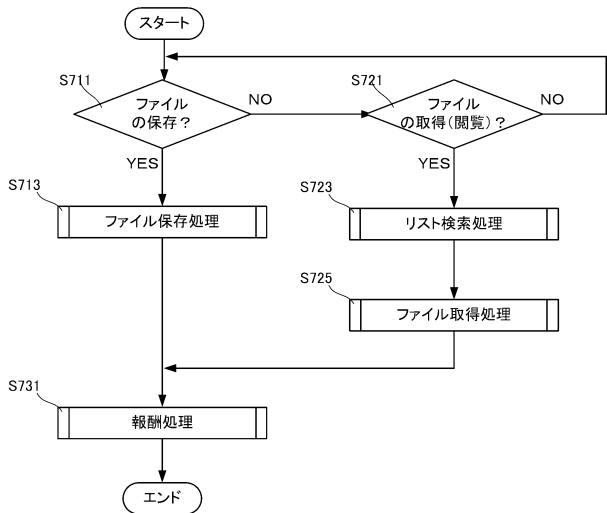
20

30

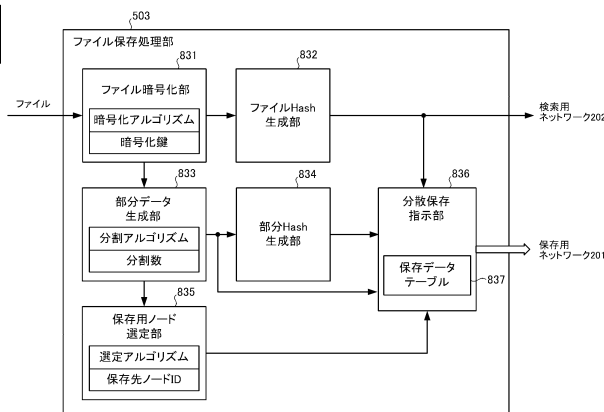
40

50

【図 7】

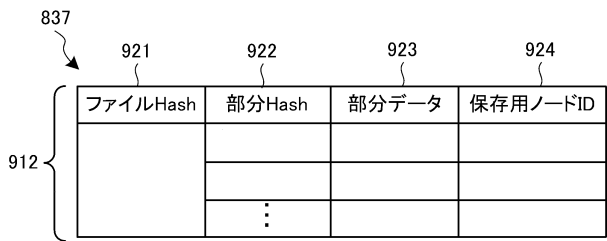


【図 8】

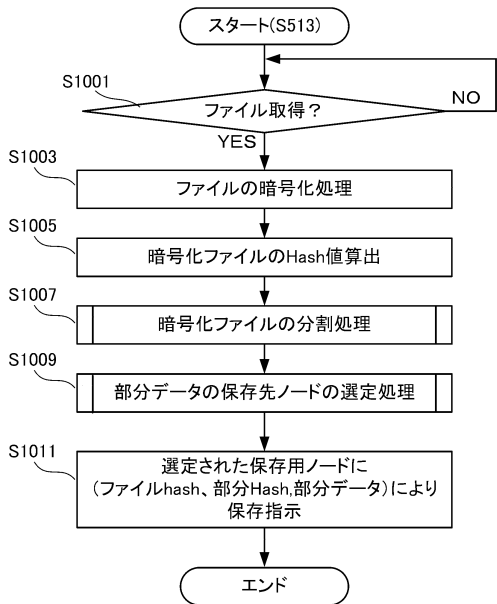


10

【図 9】



【図 10】



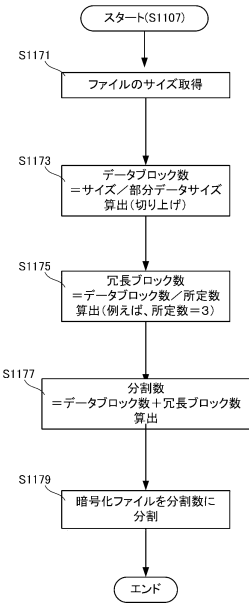
20

30

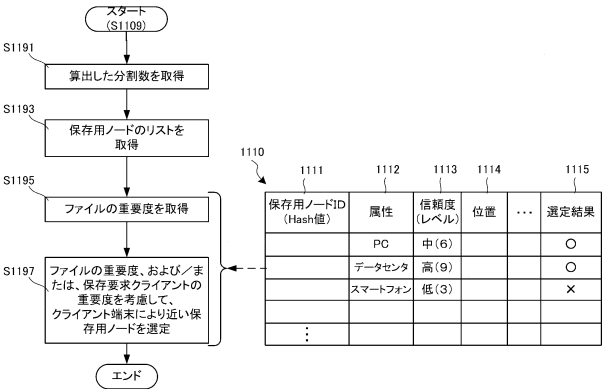
40

50

【図 1 1 A】

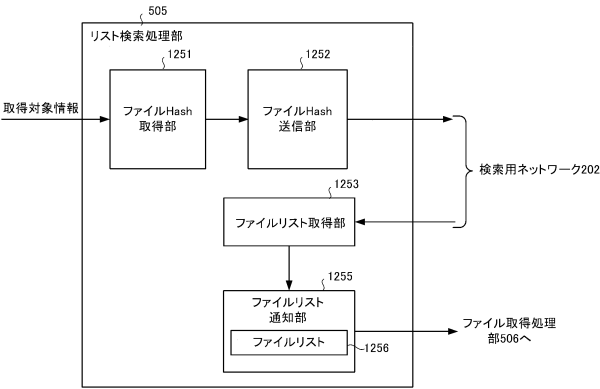


【図 1 1 B】



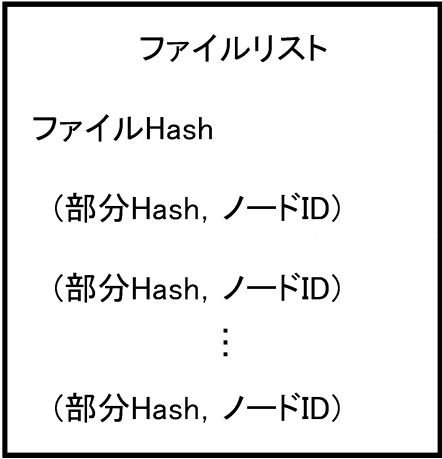
10

【図 1 2】



【図 1 3】

1256

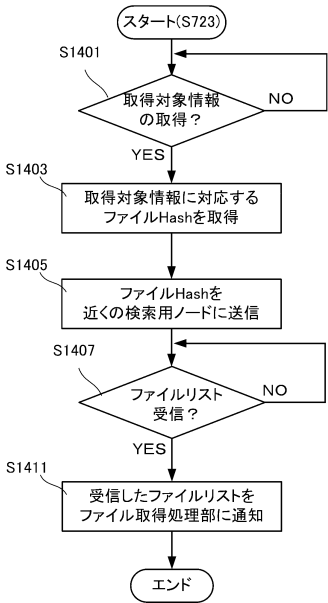


30

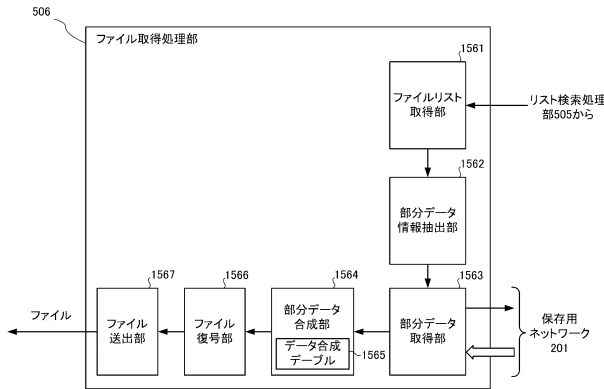
40

50

【図 14】



【図 15】



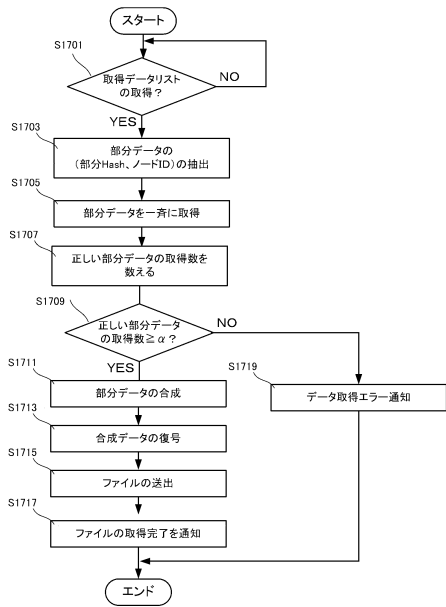
10

【図 16】

1565

1601 部分Hash	1602 部分データ	1603 合成ファイル	1604 復号されたファイル
⋮			

【図 17】



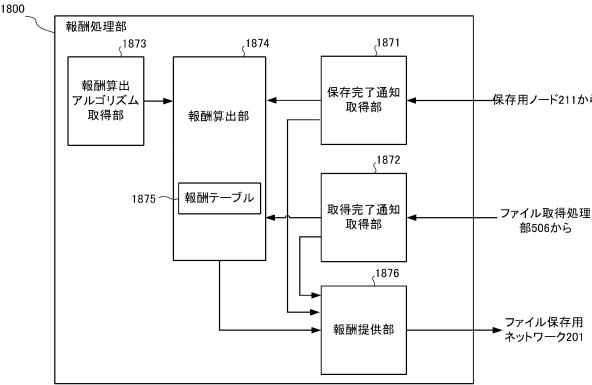
20

30

40

50

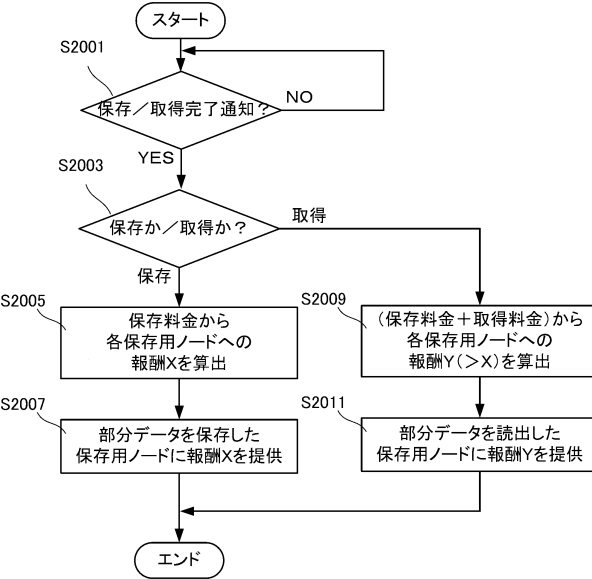
【図 18】



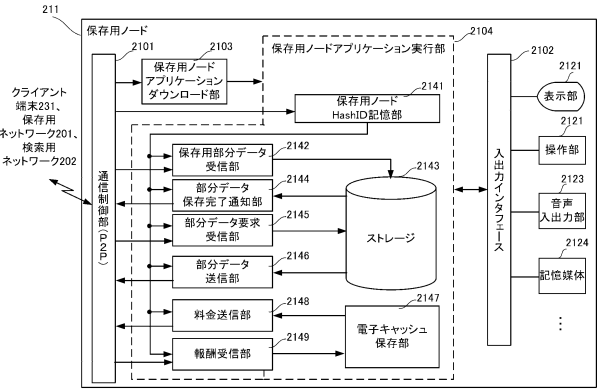
【図 19】

データID (Hash)	保存料金	(取得(閲覧)料金 × 回数)	データ保存時 報酬	データ読出時報酬 初期値	変化曲線	...
⋮						

【図 20】



【図 21】



10

20

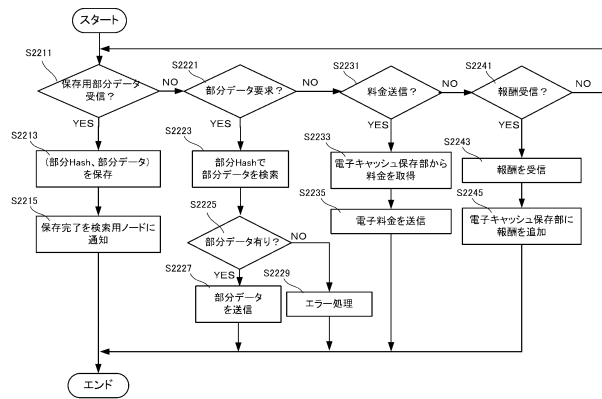
30

40

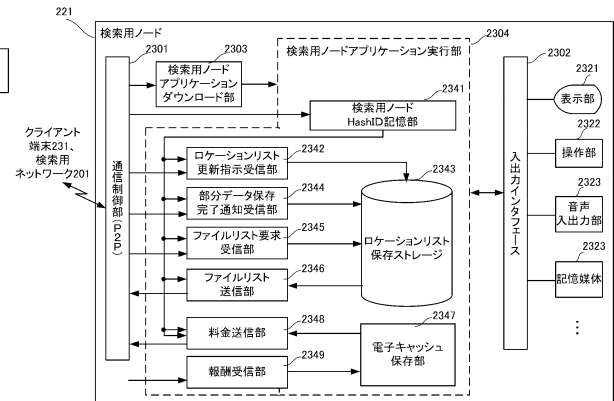
50



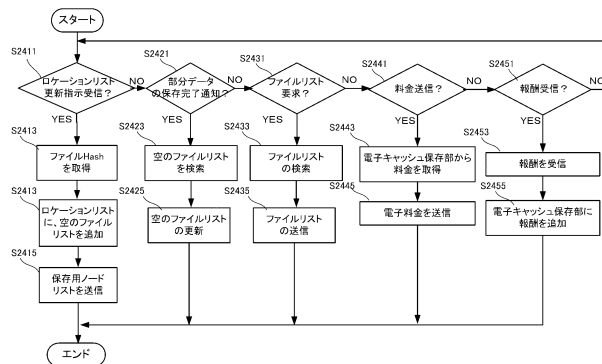
【図 2 2】



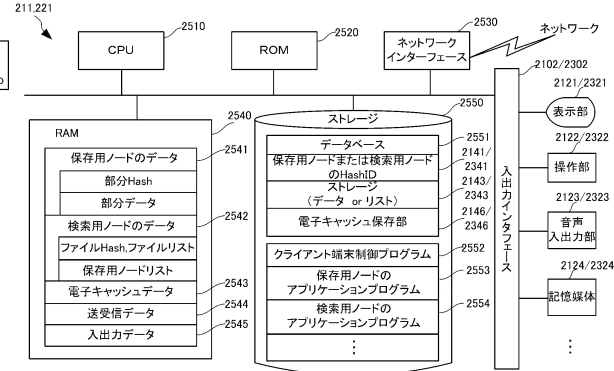
【図 2 3】



【図 2 4】



【図 2 5】



10

20

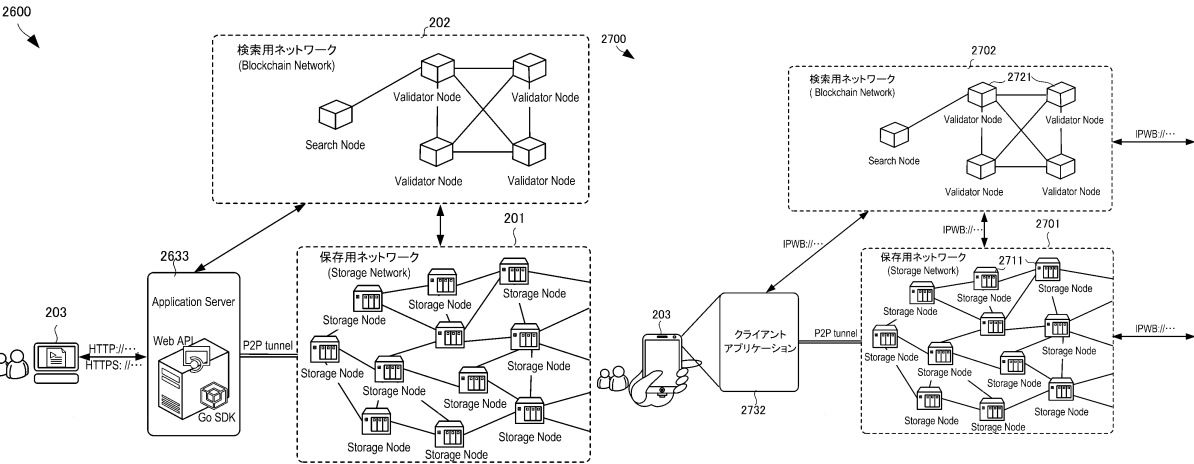
30

40

50

【図 26】

【図 27】



10

20

30

40

50

フロントページの続き

(56)参考文献 特開 2 0 1 8 - 1 9 0 2 2 7 ( J P , A )  
特開 2 0 0 4 - 1 7 1 2 2 4 ( J P , A )  
(58)調査した分野 (Int.Cl. , D B 名)  
G 0 6 F 1 6 / 0 0 - 1 6 / 9 5 8