(19)日本国特許庁(JP)

再 公 表 特 許(A1)

(11)国際公開番号
WO2017/065209

発行日　平成30年8月30日(2018.8.30)

(43)国際公開日　平成29年4月20日(2017.4.20)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/60	(2013.01)	G06F	21/60		5J104
G06F 21/62	(2013.01)	G06F	21/62	318	
G06F 21/31	(2013.01)	G06F	21/31		
G06F 12/00	(2006.01)	G06F	12/00	545A	
G09C 1/00	(2006.01)	G09C	1/00	660D	

審査請求 未請求　予備審査請求 未請求　（全 49 頁）

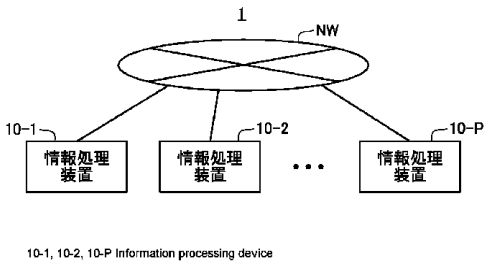
出願番号　特願2017-545453 (P2017-545453)
(21)国際出願番号　PCT/JP2016/080351
(22)国際出願日　平成28年10月13日(2016.10.13)
(31)優先権主張番号　特願2015-204607 (P2015-204607)
(32)優先日　平成27年10月16日(2015.10.16)
(33)優先権主張国　日本国(JP)

(71)出願人　504157024
国立大学法人東北大学
宮城県仙台市青葉区片平二丁目１番１号
(74)代理人　100092978
弁理士　真田　有
(72)発明者　長谷川　真吾
宮城県仙台市青葉区片平二丁目１番１号
国立大学法人東北大学内
(72)発明者　岩崎　淳也
宮城県仙台市青葉区片平二丁目１番１号
国立大学法人東北大学内
(72)発明者　酒井　正夫
宮城県仙台市青葉区片平二丁目１番１号
国立大学法人東北大学内

最終頁に続く

(54)【発明の名称】情報処理システム、情報処理装置、情報処理方法、及び、プログラム

(57)【要約】
情報処理システム（１）は、複数の記憶装置（１０）を備える。情報処理システム（１）は、複数の異なる時点と関連付けられた複数の異なる装置群の中から、現在の時点を含む所定の期間に含まれる時点と関連付けられた１つの装置群を選択し、選択された装置群に含まれるＮ個の記憶装置に、秘密データから秘密分散法に従って生成されたＮ個の分散データを保存する。情報処理システム（１）は、上記複数の装置群のうちの１つの装置群に対して復元処理を実行し、復元が失敗した場合、上記複数の装置群のうちの、上記失敗の基となった装置群と関連付けられた時点よりも前の時点と関連付けられた装置群に対して上記復元処理を実行する。



10-1, 10-2, 10-P Information processing device

【特許請求の範囲】
【請求項１】
Ｍ（Ｍは、２以上の整数を表す）個の記憶装置を備える情報処理システムであって、
秘密データから、秘密分散法に従って、Ｎ（Ｎは、２以上且つＭ以下の整数を表す）個の分散データを生成する生成手段と、
複数の異なる時点とそれぞれ関連付けられた複数の異なる装置群の中から、現在の時点と前記現在の時点よりも所定の時間だけ前の時点との間の期間に含まれる時点と関連付けられた１つの装置群を選択し、前記複数の装置群のそれぞれが、前記Ｍ個の記憶装置の中から選択されたＣ（Ｃは、Ｎ以上且つＭ以下の整数を表す）個の記憶装置を含み、前記選択された装置群に含まれるＮ個の記憶装置に前記生成されたＮ個の分散データをそれぞれ保存する保存手段と、
前記複数の装置群のうちの１つの装置群に対して復元処理を実行し、前記復元処理が、前記装置群に含まれるＮ個の記憶装置の少なくとも一部の記憶装置のそれぞれに前記分散データを要求することと、前記要求に応じて提供された提供データから前記秘密分散法に従って前記秘密データを復元することと、を含み、前記復元が失敗した場合、前記複数の装置群のうちの、前記失敗の基となった装置群と関連付けられた時点よりも前の時点と関連付けられた装置群に対して前記復元処理を実行する復元手段と、
を備える、情報処理システム。
【請求項２】
請求項１に記載の情報処理システムであって、
前記保存手段は、ユーザによって入力された入力情報と関連付けて保存要求を受け付けるとともに、前記保存要求が受け付けられた場合、前記複数の装置群を前記保存要求と関連付けられた前記入力情報に基づいて設定し、
前記復元手段は、ユーザによって入力された入力情報と関連付けて復元要求を受け付けるとともに、前記復元要求が受け付けられた場合、前記複数の装置群を前記復元要求と関連付けられた前記入力情報に基づいて設定する、情報処理システム。
【請求項３】
請求項１又は請求項２に記載の情報処理システムであって、
前記複数の装置群は、前記複数の時点とそれぞれ関連付けられた複数の異なる装置順位情報と、前記入力情報とＣ個の異なる順位との予め定められた情報順位関係と、に基づいて設定され、前記装置順位情報が、前記Ｍ個の記憶装置の少なくとも一部の記憶装置と、前記少なくとも一部の記憶装置のそれぞれに付与された順位と、を表す情報である、情報処理システム。
【請求項４】
請求項１又は請求項２に記載の情報処理システムであって、
前記複数の装置群は、前記Ｍ個の記憶装置の少なくとも一部の記憶装置と、前記少なくとも一部の記憶装置のそれぞれに付与された順位と、を表す装置順位情報と、前記複数の時点とそれぞれ関連付けられた複数の異なる情報順位関係と、に基づいて設定され、前記情報順位関係が、前記入力情報とＣ個の異なる順位との予め定められた関係である、情報処理システム。
【請求項５】
請求項１乃至請求項４のいずれか一項に記載の情報処理システムであって、
前記秘密データは、前記秘密データと異なる他の秘密データから秘密分散法に従って生成された複数の分散データがそれぞれ保存された複数の記憶装置を表す情報を含むデータである、情報処理システム。
【請求項６】
請求項１乃至請求項５のいずれか一項に記載の情報処理システムであって、
前記復元手段は、ユーザによって入力され且つ期間を表す期間情報を受け付けるとともに、前記復元処理を実行する対象となる装置群を、前記複数の装置群の中で、前記受け付けられた期間情報が表す期間に含まれる時点と関連付けられた装置群に限定する、情報処

理システム。
【請求項７】
請求項１乃至請求項６のいずれか一項に記載の情報処理システムであって、
前記保存手段は、前記選択された装置群と関連付けられた時点に基づいて識別情報を生成するとともに、前記Ｎ個の分散データのそれぞれを、前記生成された識別情報と関連付けて保存する、情報処理システム。
【請求項８】
請求項７に記載の情報処理システムであって、
前記保存手段は、前記選択された装置群に含まれるＮ個の記憶装置に対して、記憶装置毎に異なる情報を前記識別情報として生成する、情報処理システム。
【請求項９】
請求項１乃至請求項８のいずれか一項に記載の情報処理システムであって、
前記装置群に含まれる記憶装置の数Ｃは、ユーザの認証に用いられるパスワードが特定されやすいほど多い数に設定され、
前記保存手段は、前記選択された装置群に含まれるＣ個の記憶装置の中からＮ個の記憶装置をランダムに選択し、前記選択されたＮ個の記憶装置に前記生成されたＮ個の分散データをそれぞれ保存し、
前記復元処理は、前記装置群に含まれるＣ個の記憶装置のそれぞれに前記分散データを要求することと、前記要求に応じて提供されたＣ個の提供データから選択されるＮ個の提供データの組み合わせのそれぞれに対して、当該組み合わせを構成するＮ個の提供データから前記秘密分散法に従って前記秘密データを復元することと、を含む、情報処理システム。
【請求項１０】
請求項１乃至請求項９のいずれか一項に記載の情報処理システムであって、
前記記憶装置に対する前記分散データの要求は、情報処理装置が前記記憶装置へ、時点を識別する時点識別情報と、ユーザによって入力された入力情報又は前記入力情報に基づいて生成された生成情報と、を含む提供要求を送信することにより行なわれ、
前記情報処理装置から、前記時点識別情報が共通し、且つ、前記入力情報又は前記生成情報が相違する、所定の閾値数以上の提供要求が所定の判定時間内に送信された場合、前記情報処理装置からの前記要求に応じた前記提供データの提供を禁止する禁止手段を備える、情報処理システム。
【請求項１１】
Ｍ（Ｍは、２以上の整数を表す）個の記憶装置と通信可能に接続された情報処理装置であって、
秘密データから、秘密分散法に従って、Ｎ（Ｎは、２以上且つＭ以下の整数を表す）個の分散データを生成する生成手段と、
複数の異なる時点とそれぞれ関連付けられた複数の異なる装置群の中から、現在の時点と前記現在の時点よりも所定の時間だけ前の時点との間の期間に含まれる時点と関連付けられた１つの装置群を選択し、前記複数の装置群のそれぞれが、前記Ｍ個の記憶装置の中から選択されたＣ（Ｃは、Ｎ以上且つＭ以下の整数を表す）個の記憶装置を含み、前記選択された装置群に含まれるＮ個の記憶装置に前記生成されたＮ個の分散データをそれぞれ保存する保存手段と、
前記複数の装置群のうちの１つの装置群に対して復元処理を実行し、前記復元処理が、前記装置群に含まれるＮ個の記憶装置の少なくとも一部の記憶装置のそれぞれに前記分散データを要求することと、前記要求に応じて提供された提供データから前記秘密分散法に従って前記秘密データを復元することと、を含み、前記復元が失敗した場合、前記複数の装置群のうちの、前記失敗の基となった装置群と関連付けられた時点よりも前の時点と関連付けられた装置群に対して前記復元処理を実行する復元手段と、
を備える、情報処理装置。
【請求項１２】

Ｍ（Ｍは、２以上の整数を表す）個の記憶装置を用いる情報処理方法であって、
秘密データから、秘密分散法に従って、Ｎ（Ｎは、２以上且つＭ以下の整数を表す）個の分散データを生成し、
複数の異なる時点とそれぞれ関連付けられた複数の異なる装置群の中から、現在の時点と前記現在の時点よりも所定の時間だけ前の時点との間の期間に含まれる時点と関連付けられた１つの装置群を選択し、前記複数の装置群のそれぞれが、前記Ｍ個の記憶装置の中から選択されたＣ（Ｃは、Ｎ以上且つＭ以下の整数を表す）個の記憶装置を含み、前記選択された装置群に含まれるＮ個の記憶装置に前記生成されたＮ個の分散データをそれぞれ保存し、
前記複数の装置群のうちの１つの装置群に対して復元処理を実行し、前記復元処理が、前記装置群に含まれるＮ個の記憶装置の少なくとも一部の記憶装置のそれぞれに前記分散データを要求することと、前記要求に応じて提供された提供データから前記秘密分散法に従って前記秘密データを復元することと、を含み、前記復元が失敗した場合、前記複数の装置群のうちの、前記失敗の基となった装置群と関連付けられた時点よりも前の時点と関連付けられた装置群に対して前記復元処理を実行する、情報処理方法。
【請求項１３】
Ｍ（Ｍは、２以上の整数を表す）個の記憶装置と通信可能に接続された情報処理装置に、
秘密データから、秘密分散法に従って、Ｎ（Ｎは、２以上且つＭ以下の整数を表す）個の分散データを生成し、
複数の異なる時点とそれぞれ関連付けられた複数の異なる装置群の中から、現在の時点と前記現在の時点よりも所定の時間だけ前の時点との間の期間に含まれる時点と関連付けられた１つの装置群を選択し、前記複数の装置群のそれぞれが、前記Ｍ個の記憶装置の中から選択されたＣ（Ｃは、Ｎ以上且つＭ以下の整数を表す）個の記憶装置を含み、前記選択された装置群に含まれるＮ個の記憶装置に前記生成されたＮ個の分散データをそれぞれ保存し、
前記複数の装置群のうちの１つの装置群に対して復元処理を実行し、前記復元処理が、前記装置群に含まれるＮ個の記憶装置の少なくとも一部の記憶装置のそれぞれに前記分散データを要求することと、前記要求に応じて提供された提供データから前記秘密分散法に従って前記秘密データを復元することと、を含み、前記復元が失敗した場合、前記複数の装置群のうちの、前記失敗の基となった装置群と関連付けられた時点よりも前の時点と関連付けられた装置群に対して前記復元処理を実行する、処理を実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理システム、情報処理装置、情報処理方法、及び、プログラムに関する。
【背景技術】
【０００２】
複数の記憶装置を備える情報処理システムが知られている。この種の情報処理システムの一つとして、特許文献１に記載の情報処理システムは、秘密データから、秘密分散法に従って、Ｎ（Ｎは、２以上の整数を表す）個の分散データを生成する。更に、情報処理システムは、Ｎ個の記憶装置に、生成されたＮ個の分散データをそれぞれ保存する。
【０００３】
上記情報処理システムにおいては、例えば、秘密データを不正に取得することを意図するユーザは、当該秘密データから生成されたＮ個の分散データのうちの、ｋ（ｋは、２以上且つＮよりも小さい整数を表す）個の分散データを取得しない限り、秘密データを復元できない。更に、上記情報処理システムは、秘密データを保存する毎に所定の方式に従ってＮ個の分散データの保存先としての記憶装置を変更する。
【先行技術文献】

【特許文献】
【０００４】
【特許文献１】特開２０１３－２０３１４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ところで、上記情報処理システムが、秘密データを識別する情報と、分散データの保存先を特定する情報と、を関連付けて記憶し、秘密データの復元が要求された場合に、当該秘密データを復元するために用いられる分散データの保存先を、記憶された情報に基づいて特定することが考えられる。
【０００６】
しかしながら、この場合、当該情報が、秘密データを不正に取得することを意図するユーザに漏洩することがある。この場合、当該ユーザによって、当該秘密データを復元するために用いられる分散データの保存先が特定されやすい。このため、秘密データが不正に取得される虞があった。
【０００７】
また、情報処理システムが、秘密データを識別する情報と、分散データの保存先を特定する情報と、を関連付けて記憶しない場合、秘密データの復元が要求された場合に、当該秘密データを復元するために用いられる分散データの保存先を特定するための処理の負荷が高くなりやすい。
【０００８】
本発明の目的の一つは、秘密データが不正に取得されることを抑制しながら、分散データの保存先を特定するための処理の負荷を低減することにある。
【課題を解決するための手段】
【０００９】
一つの側面では、情報処理システムは、Ｍ（Ｍは、２以上の整数を表す）個の記憶装置を備える。
更に、この情報処理システムは、
秘密データから、秘密分散法に従って、Ｎ（Ｎは、２以上且つＭ以下の整数を表す）個の分散データを生成する生成手段と、
複数の異なる時点とそれぞれ関連付けられた複数の異なる装置群の中から、現在の時点と上記現在の時点よりも所定の時間だけ前の時点との間の期間に含まれる時点と関連付けられた１つの装置群を選択し、上記複数の装置群のそれぞれが、上記Ｍ個の記憶装置の中から選択されたＣ（Ｃは、Ｎ以上且つＭ以下の整数を表す）個の記憶装置を含み、上記選択された装置群に含まれるＮ個の記憶装置に上記生成されたＮ個の分散データをそれぞれ保存する保存手段と、
上記複数の装置群のうちの１つの装置群に対して復元処理を実行し、上記復元処理が、上記装置群に含まれるＮ個の記憶装置の少なくとも一部の記憶装置のそれぞれに上記分散データを要求することと、上記要求に応じて提供された提供データから上記秘密分散法に従って上記秘密データを復元することと、を含み、上記復元が失敗した場合、上記複数の装置群のうちの、上記失敗の基となった装置群と関連付けられた時点よりも前の時点と関連付けられた装置群に対して上記復元処理を実行する復元手段と、
を備える。
【００１０】
他の一つの側面では、情報処理装置は、Ｍ（Ｍは、２以上の整数を表す）個の記憶装置と通信可能に接続される。
更に、この情報処理装置は、
秘密データから、秘密分散法に従って、Ｎ（Ｎは、２以上且つＭ以下の整数を表す）個の分散データを生成する生成手段と、
複数の異なる時点とそれぞれ関連付けられた複数の異なる装置群の中から、現在の時点

と上記現在の時点よりも所定の時間だけ前の時点との間の期間に含まれる時点と関連付けられた１つの装置群を選択し、上記複数の装置群のそれぞれが、上記Ｍ個の記憶装置の中から選択されたＣ（Ｃは、Ｎ以上且つＭ以下の整数を表す）個の記憶装置を含み、上記選択された装置群に含まれるＮ個の記憶装置に上記生成されたＮ個の分散データをそれぞれ保存する保存手段と、

上記複数の装置群のうちの１つの装置群に対して復元処理を実行し、上記復元処理が、上記装置群に含まれるＮ個の記憶装置の少なくとも一部の記憶装置のそれぞれに上記分散データを要求することと、上記要求に応じて提供された提供データから上記秘密分散法に従って上記秘密データを復元することと、を含み、上記復元が失敗した場合、上記複数の装置群のうちの、上記失敗の基となった装置群と関連付けられた時点よりも前の時点と関連付けられた装置群に対して上記復元処理を実行する復元手段と、

を備える。

【００１１】

他の一つの側面では、情報処理方法は、Ｍ（Ｍは、２以上の整数を表す）個の記憶装置を用いる。

更に、この情報処理方法は、

秘密データから、秘密分散法に従って、Ｎ（Ｎは、２以上且つＭ以下の整数を表す）個の分散データを生成し、

複数の異なる時点とそれぞれ関連付けられた複数の異なる装置群の中から、現在の時点と上記現在の時点よりも所定の時間だけ前の時点との間の期間に含まれる時点と関連付けられた１つの装置群を選択し、上記複数の装置群のそれぞれが、上記Ｍ個の記憶装置の中から選択されたＣ（Ｃは、Ｎ以上且つＭ以下の整数を表す）個の記憶装置を含み、上記選択された装置群に含まれるＮ個の記憶装置に上記生成されたＮ個の分散データをそれぞれ保存し、

上記複数の装置群のうちの１つの装置群に対して復元処理を実行し、上記復元処理が、上記装置群に含まれるＮ個の記憶装置の少なくとも一部の記憶装置のそれぞれに上記分散データを要求することと、上記要求に応じて提供された提供データから上記秘密分散法に従って上記秘密データを復元することと、を含み、上記復元が失敗した場合、上記複数の装置群のうちの、上記失敗の基となった装置群と関連付けられた時点よりも前の時点と関連付けられた装置群に対して上記復元処理を実行する。

【００１２】

他の一つの側面では、プログラムは、Ｍ（Ｍは、２以上の整数を表す）個の記憶装置と通信可能に接続された情報処理装置に処理を実行させる。

上記処理は、

秘密データから、秘密分散法に従って、Ｎ（Ｎは、２以上且つＭ以下の整数を表す）個の分散データを生成し、

複数の異なる時点とそれぞれ関連付けられた複数の異なる装置群の中から、現在の時点と上記現在の時点よりも所定の時間だけ前の時点との間の期間に含まれる時点と関連付けられた１つの装置群を選択し、上記複数の装置群のそれぞれが、上記Ｍ個の記憶装置の中から選択されたＣ（Ｃは、Ｎ以上且つＭ以下の整数を表す）個の記憶装置を含み、上記選択された装置群に含まれるＮ個の記憶装置に上記生成されたＮ個の分散データをそれぞれ保存し、

上記複数の装置群のうちの１つの装置群に対して復元処理を実行し、上記復元処理が、上記装置群に含まれるＮ個の記憶装置の少なくとも一部の記憶装置のそれぞれに上記分散データを要求することと、上記要求に応じて提供された提供データから上記秘密分散法に従って上記秘密データを復元することと、を含み、上記復元が失敗した場合、上記複数の装置群のうちの、上記失敗の基となった装置群と関連付けられた時点よりも前の時点と関連付けられた装置群に対して上記復元処理を実行する、ことを含む。

【発明の効果】

【００１３】

秘密データが不正に取得されることを抑制しながら、分散データの保存先を特定するための処理の負荷を低減することができる。

【図面の簡単な説明】

【００１４】

【図１】第１実施形態の情報処理システムの構成を表すブロック図である。

【図２】図１の情報処理装置の構成を表すブロック図である。

【図３】図１の情報処理装置がユーザノードとして動作するための機能を表すブロック図である。

【図４】図１の情報処理装置が保存ノードとして動作するための機能を表すブロック図である。

【図５】図１の情報処理装置がユーザデータを保存するために実行する処理を表すフローチャートである。

【図６】図１の情報処理装置がユーザデータを復元するために実行する処理を表すフローチャートである。

【図７】第２実施形態の情報処理装置がユーザデータを保存するために実行する処理の一部を表すフローチャートである。

【図８】第２実施形態の情報処理装置がユーザデータを復元するために実行する処理の一部を表すフローチャートである。

【図９】第３実施形態の情報処理装置が保存ノードとして動作するための機能を表すブロック図である。

【図１０】第３実施形態の情報処理装置が分散データを提供するために実行する処理を表すフローチャートである。

【発明を実施するための形態】

【００１５】

以下、本発明の、情報処理システム、情報処理装置、情報処理方法、及び、プログラム、に関する各実施形態について図１乃至図１０を参照しながら説明する。

【００１６】

＜第１実施形態＞

（構成）

図１に表されるように、第１実施形態の情報処理システム１は、通信網ＮＷを介して、互いに通信可能に接続されたＰ（Ｐは、３以上の整数を表す）個の情報処理装置１０－１，…，１０－Ｐを備える。本例では、通信網ＮＷは、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）網である。また、以下において、情報処理装置１０－ｐは、区別する必要がない場合、情報処理装置１０と表されてよい。ｐは、１からＰの各整数を表す。本例では、情報処理システム１は、Ｐ２Ｐ（Ｐｅｅｒ　ｔｏ　Ｐｅｅｒ）方式に従った通信を行なう。情報処理装置１０－ｐは、ノード１０－ｐと表されてよい。

【００１７】

図２に表されるように、情報処理装置１０－ｐは、バスＢＵを介して互いに接続された、処理装置１１、記憶装置１２、通信装置１３、入力装置１４、及び、出力装置１５、を備える。

【００１８】

処理装置１１は、記憶装置１２に記憶されたプログラムを実行することにより、情報処理装置１０－ｐを構成する各要素を制御する。これにより、情報処理装置１０－ｐは、後述する機能を実現する。本例では、処理装置１１は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）を含む。なお、処理装置１１は、ＭＰＵ（Ｍｉｃｒｏ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）、又は、ＤＳＰ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ）を含んでもよい。

【００１９】

記憶装置１２は、情報を読み書き可能に記憶する。例えば、記憶装置１２は、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖ

ｅ）、ＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）、半導体メモリ、及び、有機メモリの少なくとも１つを備える。なお、記憶装置１２は、フレキシブルディスク、光ディスク、光磁気ディスク、及び、半導体メモリ等の記録媒体と、記録媒体から情報を読み取り可能な読取装置と、を備えていてもよい。

【００２０】

通信装置１３は、有線又は無線により他の情報処理装置１０－ｑと通信する。ｑは、ｐと異なる、１からＰの各整数を表す。本例では、通信装置１３は、他の情報処理装置１０－ｑとの間の通信として、送信元及び送信先の少なくとも一方が秘匿された匿名通信を行なう。例えば、匿名通信は、Ｔｏｒ（Ｔｈｅ　Ｏｎｉｏｎ　Ｒｏｕｔｅｒ）、又は、Ｉ２Ｐ（Ｔｈｅ　Ｉｎｖｉｓｉｂｌｅ　Ｉｎｔｅｒｎｅｔ　Ｐｒｏｊｅｃｔ）と呼ばれる技術を用いて実現されてよい。

【００２１】

なお、通信装置１３は、他の情報処理装置１０－ｑとの通信のうちの少なくとも一部として、非匿名通信を行なってもよい。非匿名通信は、送信元及び送信先の両方が公開された通信である。

【００２２】

入力装置１４は、情報処理装置１０－ｐの外部から情報を入力する。本例では、入力装置１４は、キーボード、及び、マウスを備える。なお、入力装置１４は、マイクロフォン、又は、カメラを備えてもよい。

出力装置１５は、情報処理装置１０－ｐの外部に情報を出力する。本例では、出力装置１５は、ディスプレイを備える。なお、出力装置１５は、スピーカを備えてもよい。

なお、情報処理装置１０－ｐは、入力装置１４及び出力装置１５の両方を構成するタッチパネル式のディスプレイを備えてもよい。

【００２３】

（機能）

図３及び図４に表されるように、情報処理装置１０－ｐは、情報処理装置１０－ｐがユーザノード１００として動作するための機能と、情報処理装置１０－ｐが保存ノード２００として動作するための機能と、を有する。

【００２４】

本例では、情報処理装置１０－ｐは、第１状態、第２状態、及び、第３状態から選択された１つの状態にて動作する。第１状態は、情報処理装置１０－ｐがユーザノード１００として動作するとともに、情報処理装置１０－ｐが保存ノード２００として動作しない状態である。第２状態は、情報処理装置１０－ｐが保存ノード２００として動作するとともに、情報処理装置１０－ｐがユーザノード１００として動作しない状態である。第３状態は、情報処理装置１０－ｐがユーザノード１００として動作するとともに、情報処理装置１０－ｐが保存ノード２００としても動作する状態である。

【００２５】

また、ユーザノード１００として動作している情報処理装置１０－ｐは、ユーザノード１００と表されてよい。保存ノード２００として動作している情報処理装置１０－ｐは、保存ノード２００と表されてよい。

なお、Ｐ個の情報処理装置１０－１，…，１０－Ｐのうちの少なくとも一部の情報処理装置１０は、ユーザノード１００の機能と、保存ノード２００の機能と、のうちの一方のみを有してもよい。

【００２６】

（機能：ユーザノード）

図３に表されるように、ユーザノード１００の機能は、ユーザ認証受付部１０１と、ユーザデータ保存要求受付部１０２と、保存ノードリスト取得部１０３と、ノード群決定部１０４と、分散データ生成部１０５と、分散データ保存要求送信部１０６と、ユーザデータ復元要求受付部１０７と、提供データ取得部１０８と、秘密データ復元部１０９と、を含む。

【００２７】
本例では、分散データ生成部１０５は、生成手段を構成する。本例では、ユーザデータ保存要求受付部１０２、保存ノードリスト取得部１０３、ノード群決定部１０４、及び、分散データ保存要求送信部１０６は、保存手段を構成する。本例では、保存ノードリスト取得部１０３、ノード群決定部１０４、ユーザデータ復元要求受付部１０７、提供データ取得部１０８、及び、秘密データ復元部１０９は、復元手段を構成する。
【００２８】
ユーザ認証受付部１０１は、ユーザ認証情報を受け付ける。本例では、ユーザ認証受付部１０１は、情報処理装置１０－ｐのユーザによって、入力装置１４を介して入力された入力情報をユーザ認証情報として受け付ける。本例では、入力情報は、ユーザを識別するユーザ識別子（換言すると、ユーザＩＤ）と、ユーザの認証に用いられるパスワードとしての文字列と、を含む。
【００２９】
ユーザデータ保存要求受付部１０２は、ユーザによって、入力装置１４を介して入力されたユーザデータ保存要求を受け付ける。
【００３０】
ユーザによって入力されたユーザデータ保存要求は、ユーザによって入力された入力情報と関連付けられている、と捉えられてよい。ユーザデータ保存要求は、ユーザデータを含むとともに、当該ユーザデータの保存を要求することを表す。
【００３１】
ユーザデータ保存要求受付部１０２は、受け付けられたユーザデータ保存要求に含まれるユーザデータを暗号化する。なお、ユーザデータ保存要求受付部１０２は、ユーザデータを暗号化しなくてもよい。
【００３２】
保存ノードリスト取得部１０３は、ユーザデータ保存要求が受け付けられた場合、保存ノードリストを取得する。保存ノードリストは、Ｐ個の情報処理装置１０－１，…，１０－Ｐのうちの、保存ノード２００のそれぞれと、Ｐ個の情報処理装置１０－１，…，１０－Ｐのうちの、保存ノード２００のそれぞれに付与された順位と、を表す情報である。換言すると、保存ノードリストは、Ｐ個の情報処理装置１０－１，…，１０－Ｐのうちの保存ノード２００が備える記憶装置１２のそれぞれと、Ｐ個の情報処理装置１０－１，…，１０－Ｐのうちの保存ノード２００が備える記憶装置１２のそれぞれに付与された順位と、を表す情報である。
【００３３】
本例では、保存ノードリストは、先頭から末尾へ向かって順位が低くなるように、保存ノード２００を識別するノード識別子（換言すると、ノードＩＤ）が順に並ぶ情報である。本例では、保存ノードリストは、装置順位情報を構成する。
【００３４】
後述するように、保存ノードリストは、リスト生成時点が到来する毎に生成される。換言すると、リスト生成時点は、保存ノードリストが生成される時点である。本例では、リスト生成時点は、情報処理システム１において予め定められる。換言すると、Ｐ個の情報処理装置１０－１，…，１０－Ｐは、リスト生成時点を共有する。本例では、リスト生成時点は、基準時点（例えば、２０１５年１月１日０時０分０秒）から、所定の変化時間（例えば、１分）が経過する毎に到来する時点である。変化時間は、変動してもよい。
【００３５】
後述するように、少なくとも１つの保存ノード２００は、複数のリスト生成時点にてそれぞれ生成された複数の異なる保存ノードリストを、当該複数のリスト生成時点とそれぞれ関連付けて保持している。例えば、保存ノードリストは、当該保存ノードリストが生成されたリスト生成時点を表す時点情報を含む。
【００３６】
本例では、保存ノードリストの取得は、以下のようにして行なわれる。保存ノードリス

ト取得部１０３は、ユーザデータ保存要求が受け付けられた場合、現在の時点を取得する。そして、保存ノードリスト取得部１０３は、情報処理システム１において予め定められたリスト生成時点のうちの、所定の選択期間に含まれる少なくとも１つのリスト生成時点の中から１つのリスト生成時点を選択する。本例では、選択期間は、取得された現在の時点と、当該現在の時点よりも所定の時間（例えば、５分）だけ前の時点と、の間の期間である。

【００３７】

具体的には、保存ノードリスト取得部１０３は、当該選択期間に含まれる少なくとも１つのリスト生成時点の中から１つのリスト生成時点をランダムに選択する。本例では、ランダムな選択は、疑似乱数を用いて行なわれる。

【００３８】

保存ノードリスト取得部１０３は、選択されたリスト生成時点を表す時点情報を含む保存ノードリスト要求を、保存ノードリストを保持する保存ノード２００へ送信する。保存ノードリスト要求は、保存ノードリストを要求することを表す。保存ノードリスト取得部１０３は、当該保存ノードリスト要求に応じて当該保存ノード２００によって送信された保存ノードリストを受信（換言すると、取得）する。これにより、保存ノードリストの取得が行なわれる。

【００３９】

分散データ生成部１０５は、ユーザデータ保存要求受付部１０２により暗号化されたユーザデータである秘密データから、秘密分散法に従って、Ｓ個の分散データを生成する。Ｓは、２以上且つＭ以下の整数を表す。Ｍは、Ｐから１を減じた値Ｐ－１を表す。Ｍは、Ｐと等しい値を表してもよい。ユーザデータから生成されたＳ個の分散データは、第１分散データ群を構成する。分散データは、シェアと表されてもよい。

【００４０】

本例では、秘密分散法は、下記非特許文献１に記載のシャミアの秘密分散法である。なお、秘密分散法は、シャミアの秘密分散法と異なる方式であってもよい。本例では、ユーザデータに対する秘密分散法は、Ｓ個の分散データのうちの、ｔ以上の数の分散データから秘密データを復元可能であり、Ｓ個の分散データのうちの、ｔよりも少ない数の分散データから秘密データを復元不能である。ｔは、２以上且つＳよりも小さい整数を表す。

非特許文献１：Ａ．Ｓｈａｍｉｒ、「Ｈｏｗ ｔｏ ｓｈａｒｅ ａ ｓｅｃｒｅｔ」、Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ ｏｆ ｔｈｅ ＡＣＭ、第２２巻、第１１号、ｐ．６１２－６１３、１９７９年

【００４１】

ノード群決定部１０４は、ユーザデータ保存要求が受け付けられた場合に保存ノードリスト取得部１０３により取得された保存ノードリストに基づいて、ユーザデータから生成された第１分散データ群に対するノード群を決定する。第１分散データ群に対するノード群は、Ｓ個の保存ノード２００からなる。

【００４２】

本例では、第１分散データ群に対するノード群の決定は、以下のようにして行なわれる。ノード群決定部１０４は、ユーザデータ保存要求が受け付けられた場合に保存ノードリスト取得部１０３により取得された保存ノードリストに含まれるノードＩＤの中からランダムにＳ個のノードＩＤを選択する。ノード群決定部１０４は、選択されたＳ個のノードＩＤによりそれぞれ識別されるＳ個の保存ノード２００からなるノード群を、第１分散データ群に対するノード群として決定する。これにより、第１分散データ群に対するノード群の決定が行なわれる。

【００４３】

分散データ保存要求送信部１０６は、ユーザデータ保存要求が受け付けられた場合にノード群決定部１０４により決定された、第１分散データ群に対するノード群に含まれるＳ個の保存ノード２００に、Ｓ個の第１分散データ保存要求をそれぞれ送信する。Ｓ個の第１分散データ保存要求は、分散データ生成部１０５により生成された、第１分散データ群

を構成するＳ個の分散データをそれぞれ含む。更に、各第１分散データ保存要求は、分散データを保存先の保存ノード２００において識別する第１データ識別子（換言すると、第１データＩＤ）を含むとともに、分散データの記憶装置１２への保存を要求することを表す。

【００４４】

更に、ノード群決定部１０４は、分散データ保存要求送信部１０６により第１分散データ保存要求が送信された場合、メタデータを生成する。メタデータは、ユーザデータから生成されたＳ個の分散データがそれぞれ保存されたＳ個の保存ノード２００（換言すると、保存先）を表す情報を含む。本例では、メタデータは、更に、暗号化されたユーザデータを復号するために用いられる情報と、第１データＩＤと、を含む。

【００４５】

ノード群決定部１０４は、生成されたメタデータを暗号化する。具体的には、ノード群決定部１０４は、メタデータの基となったユーザデータ保存要求と関連付けられた入力情報の、所定のハッシュ関数に対するハッシュ値を取得し、取得されたハッシュ値を用いてメタデータを所定の暗号化方式に従って暗号化する。例えば、ハッシュ関数は、ＭＤ５、ＳＨＡ－０、ＳＨＡ－１、ＳＨＡ－２、又は、ＳＨＡ－３と呼ばれるハッシュ関数である。例えば、暗号化方式は、３－ｋｅｙ　Ｔｒｉｐｌｅ　ＤＥＳ、ＡＥＳ、又は、Ｃａｍｅｌｌｉａ等の共通鍵暗号方式である。ＤＥＳは、Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ａｌｇｏｒｉｔｈｍの略記である。ＡＥＳは、Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄの略記である。なお、ノード群決定部１０４は、メタデータを暗号化しなくてもよい。

【００４６】

分散データ生成部１０５は、ノード群決定部１０４により暗号化されたメタデータである秘密データから、秘密分散法に従って、Ｎ個の分散データを生成する。Ｎは、２以上且つＭ以下の整数を表す。Ｎは、Ｓと等しい値を表してもよいし、Ｓと異なる値を表してもよい。メタデータから生成されたＮ個の分散データは、第２分散データ群を構成する。

【００４７】

本例では、メタデータに対する秘密分散法は、Ｎ個の分散データのうちの、ｋ以上の数の分散データから秘密データを復元可能であり、Ｎ個の分散データのうちの、ｋよりも少ない数の分散データから秘密データを復元不能である。ｋは、２以上且つＮよりも小さい整数を表す。

【００４８】

ノード群決定部１０４は、ユーザデータ保存要求が受け付けられた場合に保存ノードリスト取得部１０３により取得された保存ノードリストに基づいて、メタデータから生成された第２分散データ群に対するノード群を決定する。第２分散データ群に対するノード群は、Ｎ個の保存ノード２００からなる。

【００４９】

本例では、第２分散データ群に対するノード群の決定は、以下のようにして行なわれる。ノード群決定部１０４は、ユーザデータ保存要求が受け付けられた場合に保存ノードリスト取得部１０３により取得された保存ノードリストと、入力情報とＮ個の異なる順位との予め定められた情報順位関係と、当該ユーザデータ保存要求と関連付けられた入力情報と、に基づいて、当該保存ノードリストに含まれるノードＩＤの中からＮ個のノードＩＤを選択する。

【００５０】

具体的には、ノード群決定部１０４は、当該ユーザデータ保存要求と関連付けられた入力情報と、当該情報順位関係と、に基づいて、Ｎ個の異なる順位を取得し、当該保存ノードリストに含まれるノードＩＤの中から、取得されたＮ個の順位にそれぞれ対応するＮ個のノードＩＤを選択する。

【００５１】

本例では、情報順位関係において、Ｎ個の順位のうちのｎ番目の順位は、ｎを表す情報

を入力情報に付加した情報の、ハッシュ値が整数である所定のハッシュ関数に対するハッシュ値を、保存ノードリストに含まれる保存ノード２００の数により除した場合における剰余に１を加えた値と等しいと定められる。ｎは、１からＮの各整数を表す。

【００５２】

加えて、ノード群決定部１０４は、選択されたＮ個のノードＩＤによりそれぞれ識別されるＮ個の保存ノード２００からなるノード群を、第２分散データ群に対するノード群として決定する。これにより、第２分散データ群に対するノード群の決定が行なわれる。

【００５３】

本例では、ノード群は、当該ノード群に含まれるＮ個の保存ノード２００が備えるＮ個の記憶装置１２からなる装置群に対応する。

また、本例では、ノード群決定部１０４により決定される、第２分散データ群に対するノード群は、保存ノードリストと入力情報とが変化しない場合、変化しない。従って、保存ノードリストの選択は、第２分散データ群に対するノード群の選択に対応する。

【００５４】

また、本例では、第２分散データ群に対するノード群の決定に用いられる保存ノードリストは、保存ノードリスト要求に含まれる時点情報が表すリスト生成時点と関連付けられた保存ノードリストである。従って、本例では、保存ノードリスト要求に含まれる時点情報が表すリスト生成時点の選択は、第２分散データ群に対するノード群の選択に対応する。

【００５５】

分散データ保存要求送信部１０６は、ユーザデータ保存要求が受け付けられた場合にノード群決定部１０４により決定された、第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００に、Ｎ個の第２分散データ保存要求をそれぞれ送信する。

【００５６】

Ｎ個の第２分散データ保存要求は、分散データ生成部１０５により生成された、第２分散データ群を構成するＮ個の分散データをそれぞれ含む。更に、各第２分散データ保存要求は、分散データを保存先の保存ノード２００において識別する第２データ識別子（換言すると、第２データＩＤ）を含むとともに、分散データの記憶装置１２への保存を要求することを表す。本例では、第２データＩＤは、第２分散データ群の基となったユーザデータ保存要求と関連付けられた入力情報に含まれるユーザＩＤである。

【００５７】

ユーザデータ復元要求受付部１０７は、ユーザによって、入力装置１４を介して入力されたユーザデータ復元要求を受け付ける。

【００５８】

ユーザによって入力されたユーザデータ復元要求は、ユーザによって入力された入力情報と関連付けられている、と捉えられてよい。ユーザデータ復元要求は、ユーザデータの復元を要求することを表す。

【００５９】

保存ノードリスト取得部１０３は、ユーザデータ復元要求が受け付けられた場合、保存ノードリストを取得する。本例では、保存ノードリストの取得は、以下のようにして行なわれる。保存ノードリスト取得部１０３は、ユーザデータ復元要求が受け付けられた場合、現在の時点を取得する。そして、保存ノードリスト取得部１０３は、情報処理システム１において予め定められたリスト生成時点の中から、取得された現在の時点に最も近いリスト生成時点を選択する。

【００６０】

保存ノードリスト取得部１０３は、選択されたリスト生成時点を表す時点情報を含む保存ノードリスト要求を、保存ノードリストを保持する保存ノード２００へ送信する。保存ノードリスト取得部１０３は、当該保存ノードリスト要求に応じて当該保存ノード２００によって送信された保存ノードリストを受信（換言すると、取得）する。これにより、保存ノードリストの取得が行なわれる。

【００６１】
ノード群決定部１０４は、ユーザデータ復元要求が受け付けられた場合に保存ノードリスト取得部１０３により取得された保存ノードリストに基づいて、メタデータから生成された第２分散データ群に対するノード群を決定する。第２分散データ群に対するノード群は、Ｎ個の保存ノード２００からなる。
【００６２】
本例では、第２分散データ群に対するノード群の決定は、以下のようにして、ユーザデータ保存要求が受け付けられた場合と同様に行なわれる。ノード群決定部１０４は、ユーザデータ復元要求が受け付けられた場合に保存ノードリスト取得部１０３により取得された保存ノードリストと、上記情報順位関係と、当該ユーザデータ復元要求と関連付けられた入力情報と、に基づいて、当該保存ノードリストに含まれるノードＩＤの中からＮ個のノードＩＤを選択する。
【００６３】
加えて、ノード群決定部１０４は、選択されたＮ個のノードＩＤによりそれぞれ識別されるＮ個の保存ノード２００からなるノード群を、第２分散データ群に対するノード群として決定する。これにより、第２分散データ群に対するノード群の決定が行なわれる。
【００６４】
提供データ取得部１０８は、ユーザデータ復元要求が受け付けられた場合にノード群決定部１０４により決定された、第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００に、Ｎ個の第２分散データ提供要求をそれぞれ送信する。各第２分散データ提供要求は、当該ユーザデータ復元要求と関連付けられた入力情報に含まれるユーザＩＤを第２データＩＤとして含むとともに、記憶装置１２に保存されている分散データの提供を要求することを表す。
【００６５】
なお、提供データ取得部１０８は、ユーザデータ復元要求が受け付けられた場合にノード群決定部１０４により決定された、第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００のうちの、ｖ個の保存ノード２００のみに、ｖ個の第２分散データ提供要求をそれぞれ送信してもよい。ｖは、Ｎよりも小さく且つｋ以上である整数を表す。
【００６６】
提供データ取得部１０８は、送信された第２分散データ提供要求に応じて保存ノード２００によって送信された（換言すると、提供された）提供データを受信する。第２分散データ提供要求に対して受信された提供データは、第２提供データ群を構成する。これにより、提供データ取得部１０８は、第２提供データ群を取得する。なお、保存ノード２００は、第２分散データ提供要求に応じて提供データを送信しないことがある。従って、第２提供データ群を構成する提供データの数は、Ｎよりも小さいことがある。また、保存ノード２００は、第２分散データ提供要求に応じて所定のダミーデータを送信することがある。従って、第２提供データ群には、第２分散データ群を構成する分散データと異なるデータが含まれることがある。
【００６７】
秘密データ復元部１０９は、提供データ取得部１０８により取得された第２提供データ群を構成する提供データである分散データから、秘密分散法に従って、秘密データを復元する。
【００６８】
保存ノードリスト取得部１０３は、秘密データ復元部１０９による、第２提供データ群に対する秘密データの復元が失敗した場合、保存ノードリストを再び取得する。本例では、保存ノードリストの取得は、以下のようにして行なわれる。保存ノードリスト取得部１０３は、第２提供データ群に対する秘密データの復元が失敗した場合、当該失敗の基となった保存ノードリストと関連付けられた（換言すると、保存ノードリストが生成された）リスト生成時点よりも、上記変化時間だけ前のリスト生成時点を取得する。
【００６９】

そして、保存ノードリスト取得部１０３は、取得されたリスト生成時点を表す時点情報を含む保存ノードリスト要求を、保存ノードリストを保持する保存ノード２００へ送信する。保存ノードリスト取得部１０３は、当該保存ノードリスト要求に応じて当該保存ノード２００によって送信された保存ノードリストを受信（換言すると、取得）する。これにより、保存ノードリストの取得が行なわれる。

【００７０】

ノード群決定部１０４は、第２提供データ群に対する秘密データの復元が失敗した場合に保存ノードリスト取得部１０３により取得された保存ノードリストに基づいて、メタデータから生成された第２分散データ群に対するノード群を決定する。本例では、第２分散データ群に対するノード群の決定は、上述したように、ユーザデータ保存要求が受け付けられた場合と同様に行なわれる。

【００７１】

提供データ取得部１０８は、第２提供データ群に対する秘密データの復元が失敗した場合にノード群決定部１０４により決定された、第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００に、Ｎ個の第２分散データ提供要求をそれぞれ送信する。提供データ取得部１０８は、送信された第２分散データ提供要求に応じて保存ノード２００によって送信された（換言すると、提供された）提供データを受信する。

【００７２】

秘密データ復元部１０９は、第２提供データ群に対する秘密データの復元が成功した場合、ユーザデータ復元要求と関連付けられた入力情報の、メタデータの暗号化に用いられたハッシュ関数に対するハッシュ値を取得する。更に、秘密データ復元部１０９は、復元された秘密データであるメタデータを、取得されたハッシュ値を用いて、上記暗号化方式に対応する復号方式に従って復号する。

【００７３】

提供データ取得部１０８は、第２提供データ群に対する秘密データの復元が成功した場合、秘密データ復元部１０９により復号されたメタデータにより表される、ユーザデータから生成されたＳ個の分散データがそれぞれ保存されたＳ個の保存ノード２００に、Ｓ個の第１分散データ提供要求をそれぞれ送信する。各第１分散データ提供要求は、秘密データ復元部１０９により復号されたメタデータにより表される第１データＩＤを含むとともに、記憶装置１２に保存されている分散データの提供を要求することを表す。

【００７４】

なお、提供データ取得部１０８は、復号されたメタデータにより表される、ユーザデータから生成されたＳ個の分散データがそれぞれ保存されたＳ個の保存ノード２００のうちの、ｕ個の保存ノード２００のみに、ｕ個の第１分散データ提供要求をそれぞれ送信してもよい。ｕは、Ｓよりも小さく且つｔ以上である整数を表す。

【００７５】

提供データ取得部１０８は、送信された第１分散データ提供要求に応じて保存ノード２００によって送信された（換言すると、提供された）提供データを受信する。第１分散データ提供要求に対して受信された提供データは、第１提供データ群を構成する。これにより、提供データ取得部１０８は、第１提供データ群を取得する。なお、保存ノード２００は、第１分散データ提供要求に応じて提供データを送信しないことがある。従って、第１提供データ群を構成する提供データの数は、Ｓよりも小さいことがある。また、保存ノード２００は、第１分散データ提供要求に応じて所定のダミーデータを送信することがある。従って、第１提供データ群には、第１分散データ群を構成する分散データと異なるデータが含まれることがある。

【００７６】

秘密データ復元部１０９は、提供データ取得部１０８により取得された第１提供データ群を構成する提供データである分散データから、秘密分散法に従って、秘密データを復元する。秘密データ復元部１０９は、第１提供データ群に対する秘密データの復元が成功した場合、復号されたメタデータにより表される、暗号化されたユーザデータを復号するた

めに用いられる情報に基づいて、復元された秘密データであるユーザデータを復号する。
【００７７】
（機能：保存ノード）
図４に表されるように、保存ノード２００の機能は、保存要求処理部２０１と、分散データ記憶部２０２と、提供要求処理部２０３と、動作通知処理部２０４と、動作通知記憶部２０５と、保存ノードリスト生成部２０６と、保存ノードリスト記憶部２０７と、保存ノードリスト要求処理部２０８と、を含む。
【００７８】
保存要求処理部２０１は、第１分散データ保存要求、又は、第２分散データ保存要求をユーザノード１００から受信する。
【００７９】
保存要求処理部２０１は、第１分散データ保存要求が受信された場合、当該第１分散データ保存要求に含まれる、第１データＩＤ及び分散データを互いに関連付けて分散データ記憶部２０２に記憶させる。これにより、分散データ記憶部２０２は、当該分散データを当該第１データＩＤと関連付けて保持する。
【００８０】
同様に、保存要求処理部２０１は、第２分散データ保存要求が受信された場合、当該第２分散データ保存要求に含まれる、第２データＩＤ及び分散データを互いに関連付けて分散データ記憶部２０２に記憶させる。これにより、分散データ記憶部２０２は、当該分散データを当該第２データＩＤと関連付けて保持する。
【００８１】
提供要求処理部２０３は、第１分散データ提供要求、又は、第２分散データ提供要求をユーザノード１００から受信する。
【００８２】
提供要求処理部２０３は、第１分散データ提供要求が受信された場合、当該第１分散データ提供要求に含まれる第１データＩＤと関連付けて分散データ記憶部２０２に保持されている分散データを、当該第１分散データ提供要求の送信元であるユーザノード１００へ送信する。
【００８３】
提供要求処理部２０３は、第１分散データ提供要求が受信された場合において、当該第１分散データ提供要求に含まれる第１データＩＤと関連付けられた分散データが分散データ記憶部２０２に保持されていないとき、当該第１分散データ提供要求の送信元であるユーザノード１００へデータを送信しない。このとき、提供要求処理部２０３は、当該第１分散データ提供要求の送信元であるユーザノード１００へ、当該第１分散データ提供要求に対応する分散データが保持されていないことを表す通知を送信してもよい。また、このとき、提供要求処理部２０３は、当該第１分散データ提供要求の送信元であるユーザノード１００へ、所定のダミーデータを送信してもよい。
【００８４】
同様に、提供要求処理部２０３は、第２分散データ提供要求が受信された場合、当該第２分散データ提供要求に含まれる第２データＩＤと関連付けて分散データ記憶部２０２に保持されている分散データを、当該第２分散データ提供要求の送信元であるユーザノード１００へ送信する。
【００８５】
提供要求処理部２０３は、第２分散データ提供要求が受信された場合において、当該第２分散データ提供要求に含まれる第２データＩＤと関連付けられた分散データが分散データ記憶部２０２に保持されていないとき、当該第２分散データ提供要求の送信元であるユーザノード１００へデータを送信しない。このとき、提供要求処理部２０３は、当該第２分散データ提供要求の送信元であるユーザノード１００へ、当該第２分散データ提供要求に対応する分散データが保持されていないことを表す通知を送信してもよい。また、このとき、提供要求処理部２０３は、当該第２分散データ提供要求の送信元であるユーザノー

ド１００へ、所定のダミーデータを送信してもよい。

【００８６】

動作通知処理部２０４は、情報処理装置１０－ｐが保存ノード２００としての動作を開始した場合、所定の通知周期が経過する毎に、動作通知を他の情報処理装置１０－ｑのそれぞれへ送信するとともに、当該動作通知を、当該動作通知が送信された時点と関連付けて動作通知記憶部２０５に記憶させる。情報処理システム１は、少なくとも１つの保存ノード２００のそれぞれをリスト生成ノードとして設定する。各リスト生成ノードは、保存ノードリストの候補である保存ノードリスト候補を生成する。

【００８７】

本例では、保存ノードリスト候補は、当該保存ノードリスト候補を生成したリスト生成ノードの電子署名を含む。各リスト生成ノードは、生成された保存ノードリスト候補を、他の情報処理装置１０－ｑのそれぞれへ送信する。

【００８８】

保存ノードリスト候補を受信した情報処理装置１０－ｑのそれぞれは、当該保存ノードリスト候補が真正であるか否かを検証する。例えば、保存ノードリスト候補が真正であるか否かは、保存ノードリスト候補に含まれる電子署名によって検証されてよい。保存ノードリスト候補を受信した情報処理装置１０－ｑのそれぞれは、当該保存ノードリスト候補が真正である場合、当該保存ノードリスト候補を承認する。

【００８９】

情報処理システム１は、承認の結果に基づいて、リスト生成時点にて生成された保存ノードリスト候補の中から１つの保存ノードリスト候補を保存ノードリストとして選択する。例えば、情報処理システム１は、保存ノードリスト候補が真正であることを承認した情報処理装置１０の数が、情報処理システム１が備える情報処理装置１０の総数の過半数となる時点が最も早い保存ノードリスト候補を保存ノードリストとして選択してよい。情報処理システム１によって選択される保存ノードリストを生成するリスト生成ノードは、リスト生成時点が経過する毎に変化してよい。

【００９０】

保存ノードリストは、情報処理装置１０間で送受信されることにより、保存ノード２００間で共有される。例えば、保存ノードリストを受信した保存ノード２００は、当該保存ノードリストを保持する。なお、保存ノード２００は、当該保存ノードリストを保持しなくてもよい。

【００９１】

本例では、保存ノードリストは、当該保存ノードリストが生成されたリスト生成時点を表す時点情報を含む。保存ノードリストが、当該保存ノードリストが生成されたリスト生成時点を表す時点情報を含むことは、当該保存ノードリストが当該リスト生成時点と関連付けられることの一例である。

【００９２】

動作通知は、情報処理装置１０－ｐを識別するノードＩＤを含むとともに、情報処理装置１０－ｐが保存ノード２００として動作していることを表す。動作通知は、情報処理装置１０－ｐが保存ノード２００としての動作を開始した時点を表す時点情報を含んでいてもよい。また、動作通知は、情報処理装置１０－ｐの電子署名を含んでいてもよい。

【００９３】

動作通知処理部２０４は、情報処理装置１０－ｐがリスト生成ノードとして設定されている場合、他の情報処理装置１０－ｑにより送信された動作通知を受信し、受信された動作通知を、当該動作通知が受信された時点と関連付けて動作通知記憶部２０５に記憶させる。これにより、動作通知記憶部２０５は、動作通知を当該動作通知が受信された時点と関連付けて保持する。

【００９４】

動作通知記憶部２０５は、保持している動作通知の中から、現在の時点から上記通知周期だけ前の時点以前の時点と関連付けられた動作通知を消去する（換言すると、当該動作

通知の保持を終了する）。

【００９５】

なお、保存ノード２００の動作通知記憶部２０５に保持されている動作通知は、他の保存ノード２００の少なくとも１つにより共有されてよい。動作通知の共有と、保存ノードリスト候補の生成と、保存ノードリストの共有と、の少なくとも１つは、下記非特許文献２に記載のブロックチェーンと呼ばれる技術を用いて実現されてよい。また、リスト生成時点毎の、保存ノードリスト候補からの保存ノードリストの選択は、下記非特許文献２に記載のプルーフ・オブ・ワークと呼ばれる技術を用いて実現されてよい。また、複数の保存ノード２００により動作通知が共有されている場合、動作通知処理部２０４により送信される動作通知の送信先は、動作通知を共有する複数の保存ノード２００の中から選択されてよい。

非特許文献２：Ｓａｔｏｓｈｉ　Ｎａｋａｍｏｔｏ、「Ｂｉｔｃｏｉｎ：Ａ　Ｐｅｅｒ－ｔｏ－Ｐｅｒｒｔ　Ｅｌｅｃｔｒｏｎｉｃ　Ｃａｓｈ　Ｓｙｓｔｅｍ」、Ｂｉｔｃｏｉｎ、［online］、２００８年、［２０１５年１０月２日検索］、インターネット〈URL：https://bitcoin.org/bitcoin.pdf〉

【００９６】

保存ノードリスト生成部２０６は、情報処理装置１０－ｐがリスト生成ノードとして設定されている場合、リスト生成時点が到来する毎に、動作通知記憶部２０５に保持されている動作通知に基づいて保存ノードリスト候補を生成する。

【００９７】

保存ノードリスト記憶部２０７は、情報処理装置１０－ｐが保存ノード２００として動作している場合、保存ノードリストが選択される毎に、選択された保存ノードリストを記憶する。上述したように、本例では、保存ノードリストは、当該保存ノードリストが生成されたリスト生成時点を表す時点情報を含む。なお、保存ノードリストが時点情報を含まない場合、保存ノードリスト記憶部２０７は、保存ノードリストと、当該保存ノードリストが生成されたリスト生成時点と、を関連付けて記憶してよい。

【００９８】

本例では、複数の異なるリスト生成時点にてそれぞれ生成される複数の保存ノードリスト候補が互いに異なるように、保存ノードリスト候補の生成は、以下のようにして行なわれる。

保存ノードリスト生成部２０６は、動作通知記憶部２０５に保持されている動作通知に含まれるノードＩＤにより識別される保存ノード２００のそれぞれに、ランダムに決定された順位を付与する。本例では、ランダムな決定は、疑似乱数を用いて行なわれる。保存ノードリスト生成部２０６は、先頭から末尾へ向かって、付与された順位が低くなるように、動作通知記憶部２０５に保持されている動作通知に含まれるノードＩＤを並べた情報を、保存ノードリスト候補として生成する。これにより、保存ノードリスト候補の生成が行なわれる。

【００９９】

本例では、保存ノードリスト取得部１０３により送信される保存ノードリスト要求の送信先は、保存ノードリストを共有する複数の保存ノード２００の中から選択されてよい。

【０１００】

保存ノードリスト要求処理部２０８は、保存ノードリスト要求をユーザノード１００から受信する。保存ノードリスト要求処理部２０８は、保存ノードリスト要求が受信された場合、当該保存ノードリスト要求に含まれる時点情報を含むとともに保存ノードリスト記憶部２０７に保持されている保存ノードリストを、当該保存ノードリスト要求の送信元であるユーザノード１００へ送信する。

【０１０１】

（動作）

次に、情報処理システム１の動作について説明する。

本例では、情報処理装置１０－１が第１状態にて動作するとともに、情報処理装置１０

－２，…，１０－Ｐが第２状態にて動作する場合を想定する。換言すると、情報処理装置１０－１がユーザノード１００として動作するとともに、情報処理装置１０－２，…，１０－Ｐが保存ノード２００として動作する場合を想定する。更に、本例では、各保存ノード２００がリスト生成ノードとして設定されている場合を想定する。

【０１０２】

以下の動作の説明において、情報処理装置１０－１は、ユーザノード１０－１と表されてもよい。同様に、情報処理装置１０－２，…，１０－Ｐは、保存ノード１０－２，…，１０－Ｐとそれぞれ表されてもよい。同様に、情報処理装置１０－２，…，１０－Ｐは、リスト生成ノード１０－２，…，１０－Ｐとそれぞれ表されてもよい。

【０１０３】

保存ノード１０－２，…，１０－Ｐのそれぞれは、上記通知周期が経過する毎に、動作通知を他の情報処理装置１０－ｑのそれぞれへ送信するとともに、送信された動作通知を、当該動作通知が送信された時点と関連付けて記憶装置１２に記憶させる。

保存ノード２００は、保存ノード１０－２，…，１０－Ｐのそれぞれにより送信された動作通知を受信し、受信された動作通知を、当該動作通知が受信された時点と関連付けて記憶装置１２に記憶させる。

【０１０４】

リスト生成ノード１０－２，…，１０－Ｐのそれぞれは、リスト生成時点が到来する毎に、保持されている動作通知に基づいて保存ノードリスト候補を生成する。リスト生成ノード１０－２，…，１０－Ｐのそれぞれは、生成した保存ノードリスト候補を、他の情報処理装置１０－ｑのそれぞれへ送信する。情報処理システム１は、保存ノードリスト候補の中から１つの保存ノードリスト候補を保存ノードリストとして選択する。保存ノード２００は、選択された保存ノードリストを記憶装置１２に記憶させる。

【０１０５】

ユーザノード１０－１は、図５にフローチャートにより表される処理を、以下のようにして実行する。

ユーザノード１０－１は、入力情報をユーザ認証情報として受け付ける（図５のステップＳ１０１）。

【０１０６】

次いで、ユーザノード１０－１は、ユーザデータ保存要求を受け付けるまで待機する（図５のステップＳ１０２の「Ｎｏ」ルート）。

ユーザノード１０－１のユーザによってユーザデータ保存要求が入力された場合、ユーザノード１０－１は、入力されたユーザデータ保存要求を受け付ける。従って、ユーザノード１０－１は、「Ｙｅｓ」と判定し、リスト生成時点を選択する（図５のステップＳ１０３）。

【０１０７】

本例では、ユーザノード１０－１は、現在の時点を取得する。更に、ユーザノード１０－１は、情報処理システム１において予め定められたリスト生成時点のうちの、上記選択期間に含まれる少なくとも１つのリスト生成時点の中から１つのリスト生成時点をランダムに選択する。上記選択期間は、上述したように、取得された現在の時点と、当該現在の時点よりも所定の時間（例えば、５分）だけ前の時点と、の間の期間である。

【０１０８】

そして、ユーザノード１０－１は、選択されたリスト生成時点を表す時点情報を含む保存ノードリスト要求を、少なくとも１つの保存ノード２００のそれぞれへ送信する（図５のステップＳ１０４）。次いで、ユーザノード１０－１は、保存ノード２００から保存ノードリストを受信するまで待機する（図５のステップＳ１０５の「Ｎｏ」ルート）。

【０１０９】

一方、保存ノード２００は、ユーザノード１０－１から保存ノードリスト要求を受信する。保存ノード２００は、受信された保存ノードリスト要求に含まれる時点情報を含むとともに保持されている保存ノードリストをユーザノード１０－１へ送信する。

【０１１０】
これにより、ユーザノード１０－１は、保存ノード２００から少なくとも１つの保存ノードリストを受信する。ユーザノード１０－１は、受信した保存ノードリストが真正であるか否かを検証することにより、不正又は改竄がない保存ノードリストを選択し、選択した保存ノードリストを保持する。従って、ユーザノード１０－１は、「Ｙｅｓ」と判定し、受け付けられたユーザデータ保存要求に含まれるユーザデータに対する第１分散データ群を生成する（図５のステップＳ１０６）。
【０１１１】
本例では、ユーザノード１０－１は、受け付けられたユーザデータ保存要求に含まれるユーザデータを暗号化し、暗号化されたユーザデータである秘密データから、秘密分散法に従って、Ｓ個の分散データからなる第１分散データ群を生成する。
【０１１２】
次いで、ユーザノード１０－１は、保存ノードリストに基づいて、生成された第１分散データ群に対するノード群を決定する（図５のステップＳ１０７）。
本例では、ユーザノード１０－１は、保存ノードリストに含まれるノードＩＤの中からランダムにＳ個のノードＩＤを選択し、選択されたＳ個のノードＩＤによりそれぞれ識別されるＳ個の保存ノード２００からなるノード群を、第１分散データ群に対するノード群として決定する。
【０１１３】
そして、ユーザノード１０－１は、決定された、第１分散データ群に対するノード群に含まれるＳ個の保存ノード２００に、Ｓ個の第１分散データ保存要求をそれぞれ送信する（図５のステップＳ１０８）。Ｓ個の第１分散データ保存要求は、生成された第１分散データ群を構成するＳ個の分散データをそれぞれ含む。更に、各第１分散データ保存要求は、分散データを保存先の保存ノード２００において識別する第１データＩＤを含む。
【０１１４】
第１分散データ群に対するノード群に含まれるＳ個の保存ノード２００のそれぞれは、ユーザノード１０－１から第１分散データ保存要求を受信し、受信された第１分散データ保存要求に含まれる分散データ及び第１データＩＤを互いに関連付けて記憶装置１２に記憶させる。
【０１１５】
その後、ユーザノード１０－１は、メタデータを生成する（図５のステップＳ１０９）。メタデータは、第１分散データ群を構成するＳ個の分散データがそれぞれ保存されたＳ個の保存ノード２００を表す情報と、暗号化されたユーザデータを復号するために用いられる情報と、第１データＩＤと、を含む。
【０１１６】
次いで、ユーザノード１０－１は、生成されたメタデータに対する第２分散データ群を生成する（図５のステップＳ１１０）。
本例では、ユーザノード１０－１は、図５のステップＳ１０１にて受け付けられた入力情報の、上記ハッシュ関数に対するハッシュ値を取得し、取得されたハッシュ値を用いてメタデータを上記暗号化方式に従って暗号化する。更に、ユーザノード１０－１は、暗号化されたメタデータである秘密データから、秘密分散法に従って、Ｎ個の分散データからなる第２分散データ群を生成する。
【０１１７】
そして、ユーザノード１０－１は、保存ノードリストに基づいて、生成された第２分散データ群に対するノード群を決定する（図５のステップＳ１１１）。
本例では、ユーザノード１０－１は、図５のステップＳ１０５にて保持された保存ノードリストと、上記情報順位関係と、図５のステップＳ１０１にて受け付けられた入力情報と、に基づいて、当該保存ノードリストに含まれるノードＩＤの中からＮ個のノードＩＤを選択し、選択されたＮ個のノードＩＤによりそれぞれ識別されるＮ個の保存ノード２００からなるノード群を、第２分散データ群に対するノード群として決定する。

【０１１８】
次いで、ユーザノード１０－１は、決定された、第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００に、Ｎ個の第２分散データ保存要求をそれぞれ送信する（図５のステップＳ１１２）。
Ｎ個の第２分散データ保存要求は、生成された第２分散データ群を構成するＮ個の分散データをそれぞれ含む。更に、各第２分散データ保存要求は、分散データを保存先の保存ノード２００において識別する第２データＩＤを含む。
【０１１９】
第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００のそれぞれは、ユーザノード１０－１から第２分散データ保存要求を受信し、受信された第２分散データ保存要求に含まれる分散データ及び第２データＩＤを互いに関連付けて記憶装置１２に記憶させる。
そして、ユーザノード１０－１は、図５の処理を終了する。
【０１２０】
その後、ユーザノード１０－１は、図６にフローチャートにより表される処理を、以下のようにして実行する。
ユーザノード１０－１は、図５のステップＳ１０１と同様に、入力情報をユーザ認証情報として受け付ける（図６のステップＳ２０１）。
【０１２１】
次いで、ユーザノード１０－１は、ユーザデータ復元要求を受け付けるまで待機する（図６のステップＳ２０２の「Ｎｏ」ルート）。
ユーザノード１０－１のユーザによってユーザデータ復元要求が入力された場合、ユーザノード１０－１は、入力されたユーザデータ復元要求を受け付ける。従って、ユーザノード１０－１は、「Ｙｅｓ」と判定し、リスト生成時点を選択する（図６のステップＳ２０３）。
【０１２２】
本例では、ユーザノード１０－１は、現在の時点を取得し、情報処理システム１において予め定められたリスト生成時点の中から、取得された現在の時点に最も近いリスト生成時点を選択する。
【０１２３】
そして、ユーザノード１０－１は、選択されたリスト生成時点を表す時点情報を含む保存ノードリスト要求を、少なくとも１つの保存ノード２００のそれぞれへ送信する（図６のステップＳ２０４）。次いで、ユーザノード１０－１は、保存ノード２００から保存ノードリストを受信するまで待機する（図６のステップＳ２０５の「Ｎｏ」ルート）。
【０１２４】
一方、保存ノード２００は、ユーザノード１０－１から保存ノードリスト要求を受信する。保存ノード２００は、受信された保存ノードリスト要求に含まれる時点情報を含むとともに保持されている保存ノードリストをユーザノード１０－１へ送信する。
【０１２５】
これにより、ユーザノード１０－１は、保存ノード２００から少なくとも１つの保存ノードリストを受信する。ユーザノード１０－１は、受信した保存ノードリストが真正であるか否かを検証することにより、不正又は改竄がない保存ノードリストを選択し、選択した保存ノードリストを保持する。従って、ユーザノード１０－１は、「Ｙｅｓ」と判定し、図５のステップＳ１１１と同様に、保存ノードリストに基づいて、第２分散データ群に対するノード群を決定する（図６のステップＳ２０６）。
【０１２６】
本例では、ユーザノード１０－１は、図６のステップＳ２０５にて保持された保存ノードリストと、上記情報順位関係と、図６のステップＳ２０１にて受け付けられた入力情報と、に基づいて、当該保存ノードリストに含まれるノードＩＤの中からＮ個のノードＩＤを選択し、選択されたＮ個のノードＩＤによりそれぞれ識別されるＮ個の保存ノード２０

０からなるノード群を、第２分散データ群に対するノード群として決定する。

【０１２７】

次いで、ユーザノード１０－１は、決定された、第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００に、Ｎ個の第２分散データ提供要求をそれぞれ送信する（図６のステップＳ２０７）。

各第２分散データ提供要求は、図６のステップＳ２０１にて受け付けられた入力情報に含まれるユーザＩＤを第２データＩＤとして含む。

【０１２８】

第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００のそれぞれは、ユーザノード１０－１から第２分散データ提供要求を受信し、受信された第２分散データ提供要求に含まれる第２データＩＤと関連付けられた分散データが記憶装置１２に保持されているか否かを判定する。

【０１２９】

第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００のそれぞれは、当該分散データが記憶装置１２に保持されている場合、当該分散データをユーザノード１０－１へ送信し、当該分散データが記憶装置１２に保持されていない場合、ユーザノード１０－１へダミーデータを送信する。

【０１３０】

その後、ユーザノード１０－１は、図６のステップＳ２０７にて送信された第２分散データ提供要求に応じて保存ノード２００によって送信された提供データを受信する（図６のステップＳ２０８）。上述したように、第２分散データ提供要求に対して受信された提供データは、第２提供データ群を構成する。

【０１３１】

次いで、ユーザノード１０－１は、受信された第２提供データ群を構成する提供データである分散データから、秘密分散法に従って、秘密データであるメタデータを復元する（図６のステップＳ２０９）。

【０１３２】

そして、ユーザノード１０－１は、図６のステップＳ２０９にてメタデータの復元が成功したか否かを判定する（図６のステップＳ２１０）。

メタデータの復元が失敗した場合、ユーザノード１０－１は、「Ｎｏ」と判定し、図６のステップＳ２０４にて送信された最新の保存ノードリスト要求に含まれる時点情報が表すリスト生成時点（換言すると、メタデータの復元の失敗の基となった保存ノードリストと関連付けられたリスト生成時点）よりも、上記変化時間だけ前のリスト生成時点を取得する（図６のステップＳ２１１）。

【０１３３】

そして、ユーザノード１０－１は、図６のステップＳ２１１にて取得されたリスト生成時点を表す時点情報を含む保存ノードリスト要求を、少なくとも１つの保存ノード２００のそれぞれへ送信する（図６のステップＳ２０４）。次いで、ユーザノード１０－１は、上述したように、図６のステップＳ２０５からステップＳ２１０までの処理を実行する。

【０１３４】

ユーザノード１０－１は、図６のステップＳ２０９にてメタデータの復元が成功するまで、図６のステップＳ２０４からステップＳ２１１までの処理を繰り返し実行する。

本例では、図６のステップＳ２０４からステップＳ２０９までの処理は、復元処理と表されてもよい。

【０１３５】

図６のステップＳ２０９にてメタデータの復元が成功した場合、ユーザノード１０－１は、図６のステップＳ２１０にて「Ｙｅｓ」と判定し、図６のステップＳ２０１にて受け付けられた入力情報の、メタデータの暗号化に用いられたハッシュ関数に対するハッシュ値を取得する。そして、ユーザノード１０－１は、復元されたメタデータを、取得されたハッシュ値を用いて、メタデータの暗号化に用いられた暗号化方式に対応する復号方式に

従って復号する。

【０１３６】

次いで、ユーザノード１０－１は、復号されたメタデータにより表されるＳ個の保存ノード２００に、Ｓ個の第１分散データ提供要求をそれぞれ送信する（図６のステップＳ２１２）。各第１分散データ提供要求は、復号されたメタデータに含まれる第１データＩＤを含む。

【０１３７】

復号されたメタデータにより表されるＳ個の保存ノード２００のそれぞれは、ユーザノード１０－１から第１分散データ提供要求を受信し、受信された第１分散データ提供要求に含まれる第１データＩＤと関連付けられた分散データが記憶装置１２に保持されているか否かを判定する。

【０１３８】

復号されたメタデータにより表されるＳ個の保存ノード２００のそれぞれは、当該分散データが記憶装置１２に保持されている場合、当該分散データをユーザノード１０－１へ送信し、当該分散データが記憶装置１２に保持されていない場合、ユーザノード１０－１へダミーデータを送信する。

【０１３９】

その後、ユーザノード１０－１は、図６のステップＳ２１２にて送信された第１分散データ提供要求に応じて保存ノード２００によって送信された提供データを受信する（図６のステップＳ２１３）。上述したように、第１分散データ提供要求に対して受信された提供データは、第１提供データ群を構成する。

【０１４０】

次いで、ユーザノード１０－１は、受信された第１提供データ群を構成する提供データである分散データから、秘密分散法に従って、秘密データであるユーザデータを復元する（図６のステップＳ２１４）。そして、ユーザノード１０－１は、復号されたメタデータにより表される、暗号化されたユーザデータを復号するために用いられる情報に基づいて、復元されたユーザデータを復号する。

そして、ユーザノード１０－１は、図６の処理を終了する。

【０１４１】

以上、説明したように、第１実施形態の情報処理システム１は、複数の異なる時点とそれぞれ関連付けられた複数の異なる装置群の中から、現在の時点と当該現在の時点よりも所定の時間だけ前の時点との間の期間に含まれる時点と関連付けられた１つの装置群を選択する。複数の装置群のそれぞれは、Ｍ個の記憶装置１２の中から選択されたＣ（Ｃは、Ｎ以上且つＭ以下の整数を表す。本例では、Ｃは、Ｎと等しい値を表す）個の記憶装置１２を含む。更に、情報処理システム１は、選択された装置群に含まれるＮ個の記憶装置１２に、生成されたＮ個の分散データをそれぞれ保存する。

【０１４２】

加えて、情報処理システム１は、上記複数の装置群のうちの１つの装置群に対して復元処理を実行する。復元処理は、装置群に含まれるＮ個の記憶装置１２の少なくとも一部の記憶装置１２のそれぞれに分散データを要求することと、当該要求に応じて提供された提供データから秘密分散法に従って秘密データを復元することと、を含む。更に、情報処理システム１は、当該復元が失敗した場合、上記複数の装置群のうちの、当該失敗の基となった装置群と関連付けられた時点よりも前の時点と関連付けられた装置群に対して上記復元処理を実行する。

【０１４３】

これによれば、時間の経過に伴って選択される装置群が変化する。これにより、分散データが保存される記憶装置１２が時間の経過に伴って変化する。この結果、秘密データを不正に取得することを意図するユーザによって、当該秘密データを復元するために用いられる分散データの保存先が特定される確率を低減できる。従って、秘密データが不正に取得されることを抑制できる。

【０１４４】
更に、情報処理システム１は、秘密データ（本例では、メタデータ）を識別する情報（本例では、第２データＩＤ）と、分散データの保存先を特定する情報と、を関連付けて記憶しない。従って、秘密データを不正に取得することを意図するユーザによって、当該秘密データを復元するために用いられる分散データの保存先が特定される確率を低減できる。従って、秘密データが不正に取得されることを抑制できる。
【０１４５】
加えて、情報処理システム１は、秘密データの復元が失敗した場合、失敗の基となった装置群と関連付けられた時点よりも前の時点と関連付けられた装置群に対して、当該復元のための復元処理を実行する。従って、秘密データの復元が失敗した場合において無作為（ランダム）に選択された装置群に対して当該復元処理を実行する場合よりも、秘密データの復元が成功する確率を高めることができる。この結果、秘密データの復元が要求された場合に、当該秘密データを復元するために用いられる分散データの保存先を特定するための処理の負荷を抑制できる。
【０１４６】
更に、秘密データが保存されてから、当該秘密データの復元が要求されるまでの時間が短くなるほど、当該秘密データの保存に用いられた装置群の候補の数が少なくなる。従って、当該時間が短くなるほど、情報処理システム１が当該秘密データを復元するために用いられる分散データの保存先を特定するまでに要する時間が短くなりやすい。この結果、ユーザの利便性を向上できる。
【０１４７】
更に、第１実施形態の情報処理システム１は、ユーザによって入力された入力情報と関連付けて保存要求を受け付けるとともに、保存要求が受け付けられた場合、上記複数の装置群を当該保存要求と関連付けられた入力情報に基づいて設定する。加えて、情報処理システム１は、ユーザによって入力された入力情報と関連付けて復元要求を受け付けるとともに、復元要求が受け付けられた場合、上記複数の装置群を当該復元要求と関連付けられた入力情報に基づいて設定する。
【０１４８】
これによれば、秘密データの保存が要求される場合と、秘密データの復元が要求される場合と、の２つの場合に共通する入力情報をユーザが入力することにより、情報処理システム１は、当該２つの場合に共通する装置群を設定する。従って、ユーザからの要求に応じて保存された秘密データが、当該ユーザと異なるユーザからの要求に応じて復元される確率を低減できる。
【０１４９】
更に、第１実施形態の情報処理システム１において、秘密データとしてのメタデータは、秘密データとしてのユーザデータから秘密分散法に従って生成された複数の分散データがそれぞれ保存された複数の記憶装置１２を表す情報を含むデータである。
【０１５０】
これによれば、ユーザデータから生成された複数の分散データの保存先を特定する情報の保存先が、複数の記憶装置１２に分散される。従って、ユーザデータから生成された複数の分散データの保存先が特定される確率を低減できる。従って、ユーザデータが不正に取得されることを抑制できる。
【０１５１】
なお、メタデータのサイズは、一定の値（例えば、１メガバイト、１０メガバイト、又は、１０メガバイト等）を有してよい。この場合、第２分散データ提供要求に応じて送信されるダミーデータのサイズは、メタデータのサイズと等しいことが好適である。これによれば、ユーザノード１００が、第２分散データ提供要求に応じて受信した提供データのサイズに基づいて、当該提供データが、分散データ及びダミーデータのいずれであるかを知ることを防止できる。
【０１５２】

また、ユーザデータは、複数のデータブロックを含んでよい。例えば、データブロックは、ファイルである。この場合、メタデータは、各データブロックを識別するための情報（例えば、データブロックの名称、データブロックが作成された日時、又は、データブロックが更新された日時等）を含んでよい。更に、この場合、ユーザノード１００は、メタデータが復号された場合、当該メタデータに含まれる情報に基づいて、ユーザデータに含まれるデータブロックの一覧を出力装置１５を介して出力してよい。加えて、この場合、ユーザノード１００は、ユーザノード１００のユーザによって入力装置１４を介して入力され、且つ、当該ユーザによって選択されたデータブロックを識別するための情報を受け付けてよい。この場合、ユーザノード１００は、当該受け付けた情報により識別されるデータブロックに対する分散データを保存ノード２００に要求してよい。

なお、情報処理システム１は、ユーザ認証情報をユーザデータ復元要求として用いてもよい。この場合、図６のステップＳ２０２の処理は省略されてよい。

【０１５３】

＜第１実施形態の第１変形例＞

次に、第１実施形態の第１変形例の情報処理システムについて説明する。第１実施形態の第１変形例の情報処理システムは、第１実施形態の情報処理システムに対して、復元処理を実行する対象となる装置群を制限する点において相違している。以下、相違点を中心として説明する。なお、第１実施形態の第１変形例の説明において、第１実施形態にて使用した符号と同じ符号を付したものは、同一又はほぼ同様のものである。

【０１５４】

本例では、ユーザデータ復元要求は、期間を表す期間情報を含む。期間情報は、期間が開始する時点と、期間が終了する時点と、を含む。なお、期間情報は、期間が開始する時点及び期間が終了する時点のうちの１つの時点と、期間の長さと、を含んでもよい。

例えば、ユーザノード１００のユーザは、ユーザデータ保存要求を入力した時点を含む期間を表す期間情報を含むユーザデータ復元要求を入力する。

【０１５５】

保存ノードリスト取得部１０３は、ユーザデータ復元要求が受け付けられた場合、情報処理システム１において予め定められたリスト生成時点のうちの、当該ユーザデータ復元要求に含まれる期間情報が表す期間に含まれるリスト生成時点の中で最新のリスト生成時点を選択する。

【０１５６】

なお、期間情報が期間を開始する時点を表す時点情報を含まない場合、保存ノードリスト取得部１０３は、保存ノード２００により保持されている保存ノードリストと関連付けられたリスト生成時点のうちの最も古いリスト生成時点を、期間情報が表す期間が開始する時点として用いてもよい。また、期間情報が期間が終了する時点を表す時点情報を含まない場合、保存ノードリスト取得部１０３は、保存ノード２００により保持されている保存ノードリストと関連付けられたリスト生成時点のうちの最も新しいリスト生成時点を、期間情報が表す期間が終了する時点として用いてもよい。

【０１５７】

保存ノードリスト取得部１０３は、選択されたリスト生成時点を表す時点情報を含む保存ノードリスト要求を、保存ノードリストを保持する保存ノード２００へ送信する。保存ノードリスト取得部１０３は、当該保存ノードリスト要求に応じて当該保存ノード２００によって送信された保存ノードリストを受信（換言すると、取得）する。

【０１５８】

更に、本例では、保存ノードリスト取得部１０３は、秘密データ復元部１０９による、第２提供データ群に対する秘密データの復元が失敗した場合、当該失敗の基となった保存ノードリストと関連付けられた（換言すると、保存ノードリストが生成された）リスト生成時点よりも、上記変化時間だけ前のリスト生成時点を取得する。

【０１５９】

そして、保存ノードリスト取得部１０３は、取得されたリスト生成時点が、当該第２提

供データ群の基となったユーザデータ復元要求に含まれる期間情報が表す期間に含まれるか否かを判定する。

【０１６０】

取得されたリスト生成時点が当該期間に含まれる場合、保存ノードリスト取得部１０３は、取得されたリスト生成時点を表す時点情報を含む保存ノードリスト要求を、保存ノードリストを保持する保存ノード２００へ送信する。保存ノードリスト取得部１０３は、当該保存ノードリスト要求に応じて当該保存ノード２００によって送信された保存ノードリストを受信（換言すると、取得）する。

【０１６１】

取得されたリスト生成時点が当該期間に含まれない場合、保存ノードリスト取得部１０３は、保存ノードリストを取得する処理を終了する。これにより、ユーザノード１００は、ユーザデータを取得する処理を終了する。この場合、ユーザノード１００は、当該処理が終了したことを表す情報を出力装置１５を介して出力してもよい。当該情報は、保存ノードリストの取得に失敗したことを表す情報を含んでもよい。また、当該情報は、ユーザデータの取得に失敗したことを表す情報を含んでもよい。

【０１６２】

以上、説明したように、第１実施形態の第１変形例の情報処理システム１は、第１実施形態の情報処理システム１と同様の作用及び効果を奏することができる。

更に、第１実施形態の第１変形例の情報処理システム１は、ユーザによって入力され且つ期間を表す期間情報を受け付ける。更に、情報処理システム１は、復元処理を実行する対象となる装置群を、複数の装置群の中で、当該受け付けられた期間情報が表す期間に含まれる時点と関連付けられた装置群に限定する。

【０１６３】

これによれば、秘密データの復元が成功する確率を高めることができる。この結果、秘密データを復元する際に、当該秘密データを復元するために用いられる分散データの保存先を特定するための処理の負荷を抑制できる。また、ユーザがユーザ認証情報を誤って入力した場合に、秘密データの復元の失敗を確定させるための処理の負荷を抑制できる。

【０１６４】

＜第１実施形態の第２変形例＞

次に、第１実施形態の第２変形例の情報処理システムについて説明する。第１実施形態の第２変形例の情報処理システムは、第１実施形態の情報処理システムに対して、第２分散データ群に対するノード群を決定する方式において相違している。以下、相違点を中心として説明する。なお、第１実施形態の第２変形例の説明において、第１実施形態にて使用した符号と同じ符号を付したものは、同一又はほぼ同様のものである。

【０１６５】

本例では、ノード群決定部１０４による第２分散データ群に対するノード群の決定は、以下のようにして行なわれる。

ノード群決定部１０４は、複数の異なるリスト生成時点とそれぞれ関連付けられた複数の異なる情報順位関係の中から、取得された保存ノードリストと関連付けられたリスト生成時点と関連付けられた情報順位関係を選択する。

【０１６６】

各情報順位関係は、入力情報とＮ個の異なる順位との予め定められた関係である。

本例では、各情報順位関係において、Ｎ個の順位のうちのｎ番目の順位は、ｎを表す情報、及び、当該情報順位関係と関連付けられたリスト生成時点を表す時点情報を入力情報に付加した情報の、ハッシュ値が整数である所定のハッシュ関数に対するハッシュ値を、保存ノードリストに含まれる保存ノード２００の数により除した場合における剰余に１を加えた値と等しいと定められる。ｎは、１からＮの各整数を表す。

【０１６７】

ノード群決定部１０４は、取得された保存ノードリストと、選択された情報順位関係と、ユーザデータ保存要求又はユーザデータ復元要求と関連付けられた入力情報と、に基づ

いて、当該保存ノードリストに含まれるノードＩＤの中からＮ個のノードＩＤを選択する。

【０１６８】

加えて、ノード群決定部１０４は、選択されたＮ個のノードＩＤによりそれぞれ識別されるＮ個の保存ノード２００からなるノード群を、第２分散データ群に対するノード群として決定する。これにより、第２分散データ群に対するノード群の決定が行なわれる。

【０１６９】

以上、説明したように、第１実施形態の第２変形例の情報処理システム１は、第１実施形態の情報処理システム１と同様の作用及び効果を奏することができる。

更に、第１実施形態の第２変形例の情報処理システム１において、複数の装置群は、複数のリスト生成時点とそれぞれ関連付けられた複数の異なる装置順位情報（本例では、保存ノードリスト）と、当該複数のリスト生成時点とそれぞれ関連付けられた複数の異なる情報順位関係と、に基づいて設定される。

【０１７０】

これによれば、時間の経過に伴って選択される装置群をより一層確実に変化させることができる。この結果、秘密データを不正に取得することを意図するユーザによって、当該秘密データを復元するために用いられる分散データの保存先が特定される確率を低減できる。従って、秘密データが不正に取得されることを抑制できる。

【０１７１】

なお、保存ノードリスト生成部２０６による保存ノードリスト候補の生成は、以下のようにして行なわれてもよい。

保存ノードリスト生成部２０６は、動作通知記憶部２０５に保持されている動作通知に含まれるノードＩＤにより識別される保存ノード２００のそれぞれに、ノードＩＤが所定のアルゴリズムに従って（例えば、昇順又は降順に）並ぶように順位を付与する。保存ノードリスト生成部２０６は、先頭から末尾へ向かって、付与された順位が低くなるように、動作通知記憶部２０５に保持されている動作通知に含まれるノードＩＤを並べた情報を、保存ノードリスト候補として生成する。

【０１７２】

この場合、動作通知記憶部２０５に保持されている動作通知が変化しないとき、生成される保存ノードリスト候補も変化しない。従って、複数の異なるリスト生成時点にてそれぞれ生成される複数の保存ノードリスト候補が一致することがある。しかしながら、第１実施形態の第２変形例の情報処理システム１においては、第２分散データ群に対するノード群の決定に用いられる情報順位関係が、時間の経過に伴って変化する。従って、時間の経過に伴って選択される装置群を変化させることができる。

【０１７３】

この場合、保存ノードリスト間で、情報は変化しにくい。従って、情報処理システム１は、複数の保存ノードリストとして、当該複数の保存ノードリストに含まれる１つの保存ノードリストと、当該１つの保存ノードリストと当該複数の保存ノードリストに含まれる他の保存ノードリストのそれぞれとの差を表す情報と、を伝達することが好適である。これにより、保存ノードリストを伝達するための通信の負荷を抑制できる。

【０１７４】

＜第１実施形態の第３変形例＞

次に、第１実施形態の第３変形例の情報処理システムについて説明する。第１実施形態の第３変形例の情報処理システムは、第１実施形態の情報処理システムに対して、第２データＩＤとしてユーザＩＤと異なる識別情報を用いる点において相違している。以下、相違点を中心として説明する。なお、第１実施形態の第３変形例の説明において、第１実施形態にて使用した符号と同じ符号を付したものは、同一又はほぼ同様のものである。

【０１７５】

本例では、分散データ保存要求送信部１０６により送信される第２分散データ保存要求に含まれる第２データＩＤは、ワンタイム識別子（換言すると、ワンタイムＩＤ）である

。本例では、ワンタイムＩＤは、識別情報を構成する。分散データ保存要求送信部１０６は、当該第２分散データ保存要求の基となったユーザデータ保存要求と関連付けられた入力情報に含まれるユーザＩＤ及びパスワードと、第２分散データ群に対するノード群の決定に用いられた保存ノードリストに関連付けられたリスト生成時点と、に基づいて当該ワンタイムＩＤを生成する。

【０１７６】

具体的には、分散データ保存要求送信部１０６は、当該リスト生成時点を表す時点情報を当該入力情報に付加した情報の、所定のハッシュ関数に対するハッシュ値を当該ワンタイムＩＤとして用いる。例えば、ハッシュ関数は、ＭＤ５、ＳＨＡ－０、ＳＨＡ－１、ＳＨＡ－２、又は、ＳＨＡ－３と呼ばれるハッシュ関数である。

【０１７７】

同様に、提供データ取得部１０８により送信される第２分散データ提供要求に含まれる第２データＩＤも、ワンタイムＩＤである。提供データ取得部１０８は、分散データ保存要求送信部１０６と同様に、当該第２分散データ提供要求の基となったユーザデータ復元要求と関連付けられた入力情報に含まれるユーザＩＤ及びパスワードと、第２分散データ群に対するノード群の決定に用いられた保存ノードリストに関連付けられたリスト生成時点と、に基づいて当該ワンタイムＩＤを生成する。

【０１７８】

具体的には、提供データ取得部１０８は、分散データ保存要求送信部１０６と同様に、当該リスト生成時点を表す時点情報を当該入力情報に付加した情報の、上記ハッシュ関数に対するハッシュ値を当該ワンタイムＩＤとして用いる。

【０１７９】

以上、説明したように、第１実施形態の第３変形例の情報処理システム１は、第１実施形態の情報処理システム１と同様の作用及び効果を奏することができる。

更に、第１実施形態の第３変形例の情報処理システム１は、選択された装置群と関連付けられた時点に基づいて識別情報（本例では、ワンタイムＩＤ）を生成するとともに、Ｎ個の分散データのそれぞれを、生成された識別情報と関連付けて保存する。

【０１８０】

これによれば、例えば、ユーザを識別する情報と関連付けて秘密データを保存する場合と比較して、秘密データの保存を要求したユーザが特定される確率を低減できる。従って、例えば、ユーザを識別する情報に基づいて秘密データが暗号化されている場合には、秘密データが復号される確率を低減できる。

【０１８１】

なお、ワンタイムＩＤは、リスト生成時点を表す時点情報を入力情報に付加した情報の、上記ハッシュ関数に対するハッシュ値を、第１のパラメータにより除した場合における剰余であってよい。第１のパラメータは、正の整数である。本例では、第１のパラメータは、情報処理システム１において予め定められる。これによれば、ワンタイムＩＤを生成する基となった情報が特定される確率を低減できる。

【０１８２】

なお、第１のパラメータは、変動してもよい。この場合、第１のパラメータは、保存ノードリストに含まれるノードＩＤの数が大きくなるほど大きくなるように定められてよい。この場合、例えば、保存ノードリストに含まれるノードＩＤの数と、第１のパラメータと、の関係を定める第１のパラメータ関数が、情報処理システム１において予め定められる。

【０１８３】

＜第１実施形態の第４変形例＞

次に、第１実施形態の第４変形例の情報処理システムについて説明する。第１実施形態の第４変形例の情報処理システムは、第１実施形態の情報処理システムに対して、第２データＩＤとしてユーザＩＤと異なる識別情報を用いる点において相違している。以下、相違点を中心として説明する。なお、第１実施形態の第４変形例の説明において、第１実施

形態にて使用した符号と同じ符号を付したものは、同一又はほぼ同様のものである。

【０１８４】

本例では、分散データ保存要求送信部１０６により送信される第２分散データ保存要求に含まれる第２データＩＤは、ワンタイム識別子（換言すると、ワンタイムＩＤ）である。本例では、ワンタイムＩＤは、識別情報を構成する。分散データ保存要求送信部１０６は、第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００に対して、保存ノード２００毎に異なる情報をワンタイムＩＤとして生成する。

【０１８５】

本例では、第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００のうちのｎ番目の保存ノード２００に対するワンタイムＩＤは、当該Ｎ個の保存ノード２００のうちのｒ番目の保存ノード２００を識別するノードＩＤを、当該第２分散データ保存要求の基となったユーザデータ保存要求と関連付けられた入力情報に含まれるユーザＩＤに付加した情報の、所定のハッシュ関数に対するハッシュ値である。ｒは、ｎが１からＮ－１の各整数を表す場合、ｎ＋１を表すとともに、ｎがＮを表す場合、１を表す。例えば、ハッシュ関数は、ＭＤ５、ＳＨＡ－０、ＳＨＡ－１、ＳＨＡ－２、又は、ＳＨＡ－３と呼ばれるハッシュ関数である。

【０１８６】

同様に、提供データ取得部１０８により送信される第２分散データ提供要求に含まれる第２データＩＤも、ワンタイムＩＤである。提供データ取得部１０８は、分散データ保存要求送信部１０６と同様に、第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００に対して、保存ノード２００毎に異なる情報をワンタイムＩＤとして生成する。

【０１８７】

具体的には、提供データ取得部１０８は、分散データ保存要求送信部１０６と同様に、当該Ｎ個の保存ノード２００のうちのｎ番目の保存ノード２００に対するワンタイムＩＤとして、当該Ｎ個の保存ノード２００のうちのｒ番目の保存ノード２００を識別するノードＩＤを、当該第２分散データ提供要求の基となったユーザデータ復元要求と関連付けられた入力情報に含まれるユーザＩＤに付加した情報の、上記ハッシュ関数に対するハッシュ値を用いる。

【０１８８】

以上、説明したように、第１実施形態の第４変形例の情報処理システム１は、第１実施形態の情報処理システム１と同様の作用及び効果を奏することができる。

更に、第１実施形態の第４変形例の情報処理システム１は、選択された装置群と関連付けられた時点に基づいて識別情報（本例では、ワンタイムＩＤ）を生成するとともに、Ｎ個の分散データのそれぞれを、生成された識別情報と関連付けて保存する。

【０１８９】

これによれば、例えば、ユーザを識別する情報と関連付けて秘密データを保存する場合と比較して、秘密データの保存を要求したユーザが特定される確率を低減できる。従って、例えば、ユーザを識別する情報に基づいて秘密データが暗号化されている場合には、秘密データが復号される確率を低減できる。

【０１９０】

更に、第１実施形態の第４変形例の情報処理システム１は、選択された装置群に含まれるＮ個の記憶装置１２に対して、記憶装置１２毎に異なる情報を識別情報として生成する。

【０１９１】

これによれば、秘密データを復元するために用いられる分散データが、識別情報に基づいて特定される確率を低減できる。

【０１９２】

なお、上記Ｎ個の保存ノード２００のうちのｎ番目の保存ノード２００に対するワンタイムＩＤは、当該Ｎ個の保存ノード２００のうちのｒ番目の保存ノード２００を識別する

ノードＩＤを、入力情報に含まれるユーザＩＤに付加した情報の、上記ハッシュ関数に対するハッシュ値を、第１のパラメータにより除した場合における剰余であってよい。第１のパラメータは、正の整数である。本例では、第１のパラメータは、情報処理システム１において予め定められる。これによれば、ワンタイムＩＤを生成する基となった情報が特定される確率を低減できる。

【０１９３】

なお、第１のパラメータは、変動してもよい。この場合、第１のパラメータは、保存ノードリストに含まれるノードＩＤの数が大きくなるほど大きくなるように定められてよい。この場合、例えば、保存ノードリストに含まれるノードＩＤの数と、第１のパラメータと、の関係を定める第１のパラメータ関数が、情報処理システム１において予め定められる。

【０１９４】

＜第２実施形態＞

次に、第２実施形態の情報処理システムについて説明する。第２実施形態の情報処理システムは、第１実施形態の情報処理システムに対して、ユーザの認証に用いられるパスワードの強度に応じて、秘密データの復元に要する時間が変化する点において相違している。以下、相違点を中心として説明する。なお、第２実施形態の説明において、第１実施形態にて使用した符号と同じ符号を付したものは、同一又はほぼ同様のものである。

【０１９５】

本例では、ノード群決定部１０４による、ユーザデータ保存要求が受け付けられた場合における第２分散データ群に対するノード群の決定は、以下のようにして行なわれる。

【０１９６】

ノード群決定部１０４は、ユーザデータ保存要求が受け付けられた場合、当該ユーザデータ保存要求と関連付けられた入力情報に含まれるパスワードに基づいて候補数Ｃを決定する。候補数Ｃは、Ｎよりも大きく且つＭ以下の範囲において、パスワードが特定されやすい（換言すると、パスワードの強度が低い）ほど多い数に設定される。

【０１９７】

本例では、候補数Ｃの決定は、以下のようにして行なわれる。ノード群決定部１０４は、パスワードに基づいて、当該パスワードが特定されやすくなるほど小さくなる値を有するパラメータを算出する。

例えば、ノード群決定部１０４は、パスワードを構成する文字の数が、所定の閾値以上である場合、当該パラメータに所定の増分値を加算する。また、例えば、ノード群決定部１０４は、パスワードが数字を含む場合、当該パラメータに所定の増分値を加算する。また、例えば、ノード群決定部１０４は、パスワードがアルファベットの小文字を含む場合、当該パラメータに所定の増分値を加算する。また、例えば、ノード群決定部１０４は、パスワードがアルファベットの大文字を含む場合、当該パラメータに所定の増分値を加算する。また、例えば、ノード群決定部１０４は、パスワードが記号（例えば、数字、及び、アルファベット以外の文字）を含む場合、当該パラメータに所定の増分値を加算する。また、例えば、ノード群決定部１０４は、パスワードがユーザＩＤに含まれる文字列を含まない場合、当該パラメータに所定の増分値を加算する。また、例えば、ノード群決定部１０４は、パスワードが辞書に含まれる文字列を含まない場合、当該パラメータに所定の増分値を加算する。

【０１９８】

ノード群決定部１０４は、Ｎよりも大きく且つＭ以下の範囲において、算出されたパラメータが小さくなるほど多くなるように、候補数Ｃを決定する。これにより、候補数Ｃの決定が行なわれる。

【０１９９】

ノード群決定部１０４は、ユーザデータ保存要求が受け付けられた場合に保存ノードリスト取得部１０３により取得された保存ノードリストと、決定された候補数Ｃの異なる順位と入力情報との予め定められた情報順位関係と、当該ユーザデータ保存要求と関連付け

られた入力情報と、に基づいて、当該保存ノードリストに含まれるノードＩＤの中から、決定された候補数Ｃのノードを選択（換言すると、決定）する。選択された候補数Ｃのノードによりそれぞれ識別される候補数Ｃの保存ノード２００は、候補ノード群を構成する。

【０２００】

具体的には、ノード群決定部１０４は、当該ユーザデータ保存要求と関連付けられた入力情報と、当該情報順位関係と、に基づいて、候補数Ｃの異なる順位を取得し、当該保存ノードリストに含まれるノードＩＤの中から、取得された候補数Ｃの順位にそれぞれ対応する候補数Ｃのノードを選択する。

【０２０１】

本例では、情報順位関係において、候補数Ｃの順位のうちのｃ番目の順位は、ｃを表す情報を入力情報に付加した情報の、ハッシュ値が整数である所定のハッシュ関数に対するハッシュ値を、保存ノードリストに含まれる保存ノード２００の数により除した場合における剰余に１を加えた値と等しいと定められる。ｃは、１からＣの各整数を表す。

【０２０２】

更に、ノード群決定部１０４は、選択された候補数Ｃのノードの中から、Ｎ個のノードＩＤをランダムに選択する。加えて、ノード群決定部１０４は、ランダムに選択されたＮ個のノードＩＤによりそれぞれ識別されるＮ個の保存ノード２００からなるノード群を、第２分散データ群に対するノード群として決定する。これにより、第２分散データ群に対するノード群の決定が行なわれる。

【０２０３】

また、ノード群決定部１０４は、ユーザデータ復元要求が受け付けられた場合、ユーザデータ保存要求が受け付けられた場合と同様に、当該ユーザデータ復元要求と関連付けられた入力情報に含まれるパスワードに基づいて候補数Ｃを決定する。パスワードと、ノード群決定部１０４により決定される候補数Ｃと、の関係は、ユーザデータ保存要求が受け付けられた場合と、ユーザデータ復元要求が受け付けられた場合と、に共通する。

【０２０４】

ノード群決定部１０４は、ユーザデータ保存要求が受け付けられた場合と同様に、ユーザデータ復元要求が受け付けられた場合に保存ノードリスト取得部１０３により取得された保存ノードリストと、上記情報順位関係と、当該ユーザデータ復元要求と関連付けられた入力情報と、に基づいて、当該保存ノードリストに含まれるノードＩＤの中から、決定された候補数Ｃのノードを選択（換言すると、決定）する。選択された候補数Ｃのノードによりそれぞれ識別される候補数Ｃの保存ノード２００は、候補ノード群を構成する。

【０２０５】

本例では、提供データ取得部１０８は、ユーザデータ復元要求が受け付けられた場合にノード群決定部１０４により決定された、候補ノード群に含まれる候補数Ｃの保存ノード２００に、候補数Ｃの第２分散データ提供要求をそれぞれ送信する。なお、提供データ取得部１０８は、ユーザデータ復元要求が受け付けられた場合にノード群決定部１０４により決定された、候補ノード群に含まれる候補数Ｃの保存ノード２００のうちの、一部の保存ノード２００のそれぞれに、第２分散データ提供要求を送信してもよい。この場合、提供データ取得部１０８は、秘密データの復元に失敗した場合に、候補ノード群に含まれる候補数Ｃの保存ノード２００のうちの残余の保存ノード２００に第２分散データ提供要求を送信してよい。

【０２０６】

提供データ取得部１０８は、送信された第２分散データ提供要求に応じて保存ノード２００によって送信された（換言すると、提供された）提供データを受信する。第２分散データ提供要求に対して受信された提供データは、第２提供データ群を構成する。これにより、提供データ取得部１０８は、第２提供データ群を取得する。なお、保存ノード２００は、第２分散データ提供要求に応じて提供データを送信しないことがある。従って、第２

提供データ群を構成する提供データの数は、Ｃよりも小さいことがある。また、保存ノード２００は、第２分散データ提供要求に応じて所定のダミーデータを送信することがある。従って、第２提供データ群には、第２分散データ群を構成する分散データと異なるデータが含まれることがある。

【０２０７】

秘密データ復元部１０９は、ノード群決定部１０４により決定された候補ノード群に含まれる候補数Ｃの保存ノード２００から選択されるＮ個の保存ノード２００の組み合わせのすべてを生成する。Ｎ個の保存ノード２００の組み合わせのそれぞれは、ノード群候補を構成する。換言すると、各ノード群候補は、Ｎ個の保存ノード２００により構成される。

【０２０８】

秘密データ復元部１０９は、生成されたノード群候補のそれぞれに対して、提供データ取得部１０８により取得された第２提供データ群を構成する提供データのうちの、当該ノード群候補に含まれるＮ個の保存ノード２００により提供された提供データである分散データから、秘密分散法に従って、秘密データを復元する。

【０２０９】

次に、第２実施形態の情報処理システム１の動作について説明を加える。

ユーザノード１０－１は、図５の処理に代えて、図５の処理におけるステップＳ１１１の処理を、図７のステップＳ１２１からステップＳ１２３までの処理に置換した処理を実行する。

【０２１０】

具体的には、ユーザノード１０－１は、図５のステップＳ１１０の処理を実行した後、図５のステップＳ１０１にて受け付けられた入力情報に含まれるパスワードに基づいて候補数Ｃを決定する（図７のステップＳ１２１）。

【０２１１】

次いで、ユーザノード１０－１は、図５のステップＳ１０５にて保持された保存ノードリストと、図７のステップＳ１２１にて決定された候補数Ｃと、に基づいて、図５のステップＳ１１０にて生成された第２分散データ群に対する候補ノード群を決定する（図７のステップＳ１２２）。

【０２１２】

本例では、ユーザノード１０－１は、図５のステップＳ１０５にて保持された保存ノードリストと、上記情報順位関係と、図５のステップＳ１０１にて受け付けられた入力情報と、に基づいて、当該保存ノードリストに含まれるノードＩＤの中から、図７のステップＳ１２１にて決定された候補数ＣのノードＩＤを選択することにより候補ノード群を決定する。

【０２１３】

次いで、ユーザノード１０－１は、決定された候補ノード群を構成する候補数Ｃの保存ノード２００からランダムにＮ個の保存ノード２００を選択し、選択されたＮ個の保存ノード２００からなるノード群を、第２分散データ群に対するノード群として決定する（図７のステップＳ１２３）。その後、ユーザノード１０－１は、図５のステップＳ１１２以降の処理を実行する。

【０２１４】

また、ユーザノード１０－１は、図６の処理に代えて、図６の処理におけるステップＳ２０４からステップＳ２１１までの処理を、図８のステップＳ２２１からステップＳ２３２までの処理に置換した処理を実行する。

【０２１５】

具体的には、ユーザノード１０－１は、図６のステップＳ２０３の処理を実行した後、図６のステップＳ２０１にて受け付けられた入力情報に含まれるパスワードに基づいて候補数Ｃを決定する（図８のステップＳ２２１）。次いで、ユーザノード１０－１は、図６のステップＳ２０４及びステップＳ２０５と同様に、図８のステップＳ２２２及びステッ

プＳ２２３の処理を実行する。

【０２１６】

そして、ユーザノード１０－１は、図７のステップＳ１２２と同様に、図８のステップＳ２２３にて保持された保存ノードリストと、図８のステップＳ２２１にて決定された候補数Ｃと、に基づいて、第２分散データ群に対する候補ノード群を決定する（図８のステップＳ２２４）。

【０２１７】

本例では、ユーザノード１０－１は、図８のステップＳ２２３にて保持された保存ノードリストと、上記情報順位関係と、図６のステップＳ２０１にて受け付けられた入力情報と、に基づいて、当該保存ノードリストに含まれるノードＩＤの中から、図８のステップＳ２２１にて決定された候補数Ｃのノードを選択することにより候補ノード群を決定する。

【０２１８】

次いで、ユーザノード１０－１は、決定された候補ノード群に含まれる候補数Ｃの保存ノード２００に、候補数Ｃの第２分散データ提供要求をそれぞれ送信する（図８のステップＳ２２５）。

【０２１９】

候補ノード群に含まれる候補数Ｃの保存ノード２００のそれぞれは、ユーザノード１０－１から第２分散データ提供要求を受信し、受信された第２分散データ提供要求に含まれる第２データＩＤと関連付けられた分散データが記憶装置１２に保持されているか否かを判定する。

【０２２０】

候補ノード群に含まれる候補数Ｃの保存ノード２００のそれぞれは、当該分散データが記憶装置１２に保持されている場合、当該分散データをユーザノード１０－１へ送信し、当該分散データが記憶装置１２に保持されていない場合、ユーザノード１０－１へダミーデータを送信する。

【０２２１】

その後、ユーザノード１０－１は、図８のステップＳ２２５にて送信された第２分散データ提供要求に応じて保存ノード２００によって送信された提供データを受信する（図８のステップＳ２２６）。上述したように、第２分散データ提供要求に対して受信された提供データは、第２提供データ群を構成する。

【０２２２】

次いで、ユーザノード１０－１は、図８のステップＳ２２４にて決定された候補ノード群に含まれる候補数Ｃの保存ノード２００から選択されるＮ個の保存ノード２００の組み合わせのすべてを生成する（図８のステップＳ２２７）。上述したように、当該組み合わせのそれぞれは、ノード群候補を構成する。

【０２２３】

そして、ユーザノード１０－１は、生成されたノード群候補のそれぞれに対するループ処理を順次に実行する。当該ループ処理の始端及び終端は、それぞれ、図８のステップＳ２２８及びステップＳ２３１である。なお、ユーザノード１０－１は、複数のループ処理を並列に実行してもよい。

【０２２４】

ループ処理において、ユーザノード１０－１は、図８のステップＳ２２６にて受信された第２提供データ群を構成する提供データのうちの、当該ループ処理の対象であるノード群候補に含まれるＮ個の保存ノード２００により提供された提供データである分散データから、秘密分散法に従って、秘密データであるメタデータを復元する（図８のステップＳ２２９）。

【０２２５】

次いで、ループ処理において、ユーザノード１０－１は、図８のステップＳ２２９にてメタデータの復元が成功したか否かを判定する（図８のステップＳ２３０）。

メタデータの復元が成功した場合、ユーザノード１０－１は、「Ｙｅｓ」と判定し、生成されたノード群候補のそれぞれに対するループ処理のすべてを終了し、図６のステップＳ２１２以降の処理を実行する。

【０２２６】

メタデータの復元が失敗した場合、ユーザノード１０－１は、「Ｎｏ」と判定し、図８のステップＳ２３１へ進む。

このようにして、ユーザノード１０－１は、生成されたノード群候補のそれぞれに対するループ処理を実行する。

【０２２７】

生成されたノード群候補のそれぞれに対するループ処理が終了するまでに、メタデータの復元が成功しなかった場合、ユーザノード１０－１は、図８のステップＳ２２２にて送信された最新の保存ノードリスト要求に含まれる時点情報が表すリスト生成時点（換言すると、メタデータの復元の失敗の基となった保存ノードリストと関連付けられたリスト生成時点）よりも、上記変化時間だけ前のリスト生成時点を取得する（図８のステップＳ２３２）。

【０２２８】

そして、ユーザノード１０－１は、図８のステップＳ２３２にて取得されたリスト生成時点を表す時点情報を含む保存ノードリスト要求を、少なくとも１つの保存ノード２００のそれぞれへ送信する（図８のステップＳ２２２）。次いで、ユーザノード１０－１は、上述したように、図８のステップＳ２２３からステップＳ２３１までの処理を実行する。

【０２２９】

ユーザノード１０－１は、図８のステップＳ２２９にてメタデータの復元が成功するまで、図８のステップＳ２２２からステップＳ２３２までの処理を繰り返し実行する。

【０２３０】

以上、説明したように、第２実施形態の情報処理システム１は、第１実施形態の情報処理システム１と同様の作用及び効果を奏することができる。

更に、第２実施形態の情報処理システム１において、装置群（本例では、候補ノード群）に含まれる記憶装置１２の数Ｃは、ユーザの認証に用いられるパスワードが特定されやすいほど多い数に設定される。

【０２３１】

加えて、情報処理システム１は、選択された装置群（本例では、候補ノード群）に含まれるＣ個の記憶装置１２の中からＮ個の記憶装置１２をランダムに選択し、選択されたＮ個の記憶装置１２に、生成されたＮ個の分散データをそれぞれ保存する。更に、情報処理システム１は、装置群（本例では、候補ノード群）に含まれるＣ個の記憶装置１２のそれぞれに分散データを要求する。加えて、情報処理システム１は、当該要求に応じて提供されたＣ個の提供データから選択されるＮ個の提供データの組み合わせのそれぞれに対して、当該組み合わせを構成するＮ個の提供データから秘密分散法に従って秘密データを復元する。

【０２３２】

これによれば、装置群（本例では、候補ノード群）に含まれる記憶装置１２の数Ｃが、ユーザの認証に用いられるパスワードが特定されやすいほど多い数に設定される。従って、ユーザの認証に用いられるパスワードが特定されやすいほど、秘密データの復元が失敗しやすくなる。このため、ユーザの認証に用いられるパスワードが特定されやすいほど、秘密データを復元するために用いられる分散データの保存先を特定するために要する時間が長くなりやすい。これにより、ユーザの認証に用いられるパスワードとして、特定されにくいパスワードを設定する動機をユーザに与えることができる。また、ユーザの認証に用いられるパスワードが特定されやすい場合に、当該ユーザの秘密データを不正に取得することを意図するユーザによって、当該ユーザの秘密データを復元するために用いられる分散データの保存先を特定するための処理の負荷を増大できる。従って、当該ユーザの秘密データが不正に取得されることを抑制できる。

【０２３３】
＜第３実施形態＞
次に、第３実施形態の情報処理システムについて説明する。第３実施形態の情報処理システムは、第１実施形態の情報処理システムに対して、所定の条件が満足された場合にユーザノードへの提供データの提供を禁止する点において相違している。以下、相違点を中心として説明する。なお、第３実施形態の説明において、第１実施形態にて使用した符号と同じ符号を付したものは、同一又はほぼ同様のものである。
【０２３４】
本例では、ユーザノード１００による、第２分散データ提供要求の送信は、送信元が公開された通信として行なわれる。第２分散データ提供要求の送信は、非匿名通信として行なわれてよく、例えば、ＴＬＳ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）と呼ばれる技術を用いて行なわれてよい。
【０２３５】
本例では、分散データ保存要求送信部１０６により送信される第２分散データ保存要求に含まれる第２データＩＤは、ワンタイムＩＤと、リスト生成時点を表す生成時点情報と、を含む。当該生成時点情報は、第２分散データ群に対するノード群の決定に用いられた保存ノードリストに関連付けられたリスト生成時点を表す。なお、第２データＩＤは、ワンタイムＩＤに代えて、ユーザＩＤを含んでいてもよい。また、第２データＩＤは、ワンタイムＩＤに代えて、入力情報を含んでいてもよい。
本例では、生成時点情報は、時点を識別する時点識別情報を構成する。
【０２３６】
分散データ保存要求送信部１０６は、当該第２分散データ保存要求の基となったユーザデータ保存要求と関連付けられた入力情報に含まれるユーザＩＤ及びパスワードと、第２分散データ群に対するノード群の決定に用いられた保存ノードリストに関連付けられたリスト生成時点を表す生成時点情報と、に基づいて当該ワンタイムＩＤを生成する。本例では、ワンタイムＩＤは、入力情報に基づいて生成された生成情報を構成する。
【０２３７】
具体的には、分散データ保存要求送信部１０６は、当該リスト生成時点を表す生成時点情報を当該入力情報に付加した情報の、所定のハッシュ関数に対するハッシュ値を当該ワンタイムＩＤとして用いる。例えば、ハッシュ関数は、ＭＤ５、ＳＨＡ－０、ＳＨＡ－１、ＳＨＡ－２、又は、ＳＨＡ－３と呼ばれるハッシュ関数である。
【０２３８】
同様に、提供データ取得部１０８により送信される第２分散データ提供要求に含まれる第２データＩＤも、ワンタイムＩＤと、リスト生成時点を表す生成時点情報と、を含む。当該生成時点情報は、第２分散データ群に対するノード群の決定に用いられた保存ノードリストに関連付けられたリスト生成時点を表す。提供データ取得部１０８は、分散データ保存要求送信部１０６と同様に、当該第２分散データ提供要求の基となったユーザデータ復元要求と関連付けられた入力情報に含まれるユーザＩＤ及びパスワードと、第２分散データ群に対するノード群の決定に用いられた保存ノードリストに関連付けられたリスト生成時点を表す生成時点情報と、に基づいて当該ワンタイムＩＤを生成する。
【０２３９】
具体的には、提供データ取得部１０８は、分散データ保存要求送信部１０６と同様に、当該リスト生成時点を表す生成時点情報を当該入力情報に付加した情報の、上記ハッシュ関数に対するハッシュ値を当該ワンタイムＩＤとして用いる。
【０２４０】
図９に表されるように、保存ノード２００の機能は、第１実施形態の保存ノード２００の機能に加えて、不保持通知処理部２０９と、不保持通知記憶部２１０と、拒否ノードリスト生成部２１１と、拒否ノードリスト記憶部２１２と、を含む。本例では、提供要求処理部２０３、及び、拒否ノードリスト生成部２１１は、禁止手段を構成する。
【０２４１】

不保持通知処理部２０９は、第２分散データ提供要求が受信された場合において、当該第２分散データ提供要求に含まれる第２データＩＤと関連付けられた分散データが分散データ記憶部２０２に保持されていないとき、不保持通知を他の保存ノード２００のそれぞれへ送信するとともに、当該不保持通知を、当該不保持通知が送信された時点と関連付けて不保持通知記憶部２１０に記憶させる。

【０２４２】

不保持通知は、当該第２分散データ提供要求の送信元である情報処理装置１０を識別する送信元識別情報と、当該第２分散データ提供要求に含まれる第２データＩＤに含まれるワンタイムＩＤ及び生成時点情報と、当該不保持通知が送信された時点を表す送信時点情報と、を含む。本例では、送信元識別情報は、ＩＰアドレスである。なお、不保持通知は、ワンタイムＩＤに代えて、ワンタイムＩＤの、所定のハッシュ関数に対するハッシュ値を含んでいてもよい。また、不保持通知は、当該不保持通知を送信する情報処理装置１０－ｐの電子署名を含んでいてもよい。

【０２４３】

不保持通知処理部２０９は、情報処理装置１０－ｐが保存ノード２００として動作している場合、他の情報処理装置１０－ｑにより送信された不保持通知を受信し、受信された不保持通知を、当該不保持通知が受信された時点と関連付けて不保持通知記憶部２１０に記憶させる。これにより、不保持通知記憶部２１０は、不保持通知を当該不保持通知が受信された時点と関連付けて保持する。

【０２４４】

なお、保存ノード２００の不保持通知記憶部２１０に保持されている不保持通知は、他の保存ノード２００の少なくとも１つにより共有されてよい。不保持通知の共有は、ブロックチェーンと呼ばれる技術を用いて実現されてよい。また、複数の保存ノード２００により不保持通知が共有されている場合、不保持通知処理部２０９により送信される不保持通知の送信先は、不保持通知を共有する複数の保存ノード２００の中から選択されてよい。

【０２４５】

拒否ノードリスト生成部２１１は、情報処理装置１０－ｐが保存ノード２００として動作している場合、所定の生成周期が経過する毎に、不保持通知記憶部２１０に保持されている不保持通知に基づいて拒否ノードリストを生成し、生成された拒否ノードリストを拒否ノードリスト記憶部２１２に記憶させる。これにより、拒否ノードリスト記憶部２１２は、拒否ノードリストを保持する。

【０２４６】

拒否ノードリストは、Ｐ個の情報処理装置１０－１，…，１０－Ｐのうちの、第２分散データ提供要求に対する保存ノード２００からの提供データの提供が禁止された情報処理装置１０を表す情報である。本例では、拒否ノードリストは、当該提供データの提供が禁止された情報処理装置１０が有するＩＰアドレスを含む。

【０２４７】

本例では、拒否ノードリストの生成は、以下のようにして行なわれる。

拒否ノードリスト生成部２１１は、不保持通知記憶部２１０に保持されている不保持通知のうちの、生成時点情報が共通し、ワンタイムＩＤが相違し、且つ、送信時点情報が表す時点が所定の判定期間に含まれる不保持通知の数を、送信元識別情報毎に取得する。本例では、当該判定期間は、現在の時点から、所定の判定時間だけ前の時点までの期間である。

【０２４８】

拒否ノードリスト生成部２１１は、取得された不保持通知の数が、所定の閾値数以上である送信元識別情報を含む拒否ノードリストを生成する。これにより、拒否ノードリストの生成が行なわれる。

【０２４９】

なお、保存ノード２００の拒否ノードリスト記憶部２１２に保持されている拒否ノード

リストは、他の保存ノード２００の少なくとも１つにより共有されてよい。拒否ノードリストの共有は、ブロックチェーンと呼ばれる技術を用いて実現されてよい。

【０２５０】

提供要求処理部２０３は、第２分散データ提供要求が受信された場合、当該第２分散データ提供要求の送信元であるユーザノード１００を識別する送信元識別情報が、拒否ノードリスト要求処理部２１３により取得された拒否ノードリストに含まれるか否かを判定する。

【０２５１】

提供要求処理部２０３は、当該第２分散データ提供要求の送信元であるユーザノード１００を識別する送信元識別情報が拒否ノードリストに含まれる場合、当該第２分散データ提供要求の送信元であるユーザノード１００へダミーデータを送信する。ダミーデータの送信は、分散データの提供の禁止の一例である。なお、提供要求処理部２０３は、この場合、当該第２分散データ提供要求の送信元であるユーザノード１００へデータを送信しなくてもよい。

【０２５２】

提供要求処理部２０３は、当該第２分散データ提供要求の送信元であるユーザノード１００を識別する送信元識別情報が拒否ノードリストに含まれない場合、当該第２分散データ提供要求に含まれる第２データＩＤと関連付けて分散データ記憶部２０２に保持されている分散データを、当該第２分散データ提供要求の送信元であるユーザノード１００へ送信する。

【０２５３】

なお、提供要求処理部２０３は、第１分散データ提供要求が受信された場合においても、第２分散データ提供要求が受信された場合と同様に、拒否ノードリストに基づいて分散データの提供を禁止してもよい。

【０２５４】

次に、第３実施形態の情報処理システム１の動作について説明を加える。

保存ノード１０－ｗは、図１０にフローチャートにより表される処理を、以下のようにして実行する。ｗは、２からＰの各整数を表す。

【０２５５】

保存ノード１０－ｗは、第２分散データ提供要求をユーザノード１０－１から受信するまで待機する（図１０のステップＳ３０３の「Ｎｏ」ルート）。

【０２５６】

その後、第２分散データ提供要求がユーザノード１０－１から受信されると、保存ノード１０－ｗは、「Ｙｅｓ」と判定し、送信元ノードが、保持された拒否ノードリストに存在するか否かを判定する（図１０のステップＳ３０４）。送信元ノードは、第２分散データ提供要求の送信元である。本例では、送信元ノードは、ユーザノード１０－１である。

【０２５７】

送信元ノードが拒否ノードリストに存在する場合、保存ノード１０－ｗは、「Ｙｅｓ」と判定し、分散データ及び不保持通知をいずれも送信せずに、図１０の処理を終了する。

送信元ノードが拒否ノードリストに存在しない場合、保存ノード１０－ｗは、「Ｎｏ」と判定し、図１０のステップＳ３０３にて受信された第２分散データ提供要求に含まれる第２データＩＤと関連付けられた分散データが記憶装置１２に保持されているか否かを判定する（図１０のステップＳ３０５）。

【０２５８】

当該第２分散データ提供要求に含まれる第２データＩＤと関連付けられた分散データが記憶装置１２に保持されている場合、保存ノード１０－ｗは、「Ｙｅｓ」と判定し、第２分散データ提供要求の送信元であるユーザノード１０－１へ、当該分散データである提供データを送信する（図１０のステップＳ３０６）。そして、保存ノード１０－ｗは、図１０の処理を終了する。

【０２５９】

一方、当該第２分散データ提供要求に含まれる第２データＩＤと関連付けられた分散データが記憶装置１２に保持されていない場合、保存ノード１０－ｗは、「Ｎｏ」と判定し、他の保存ノード２００のそれぞれへ不保持通知を送信する（図１０のステップＳ３０７）。

【０２６０】

当該不保持通知は、当該第２分散データ提供要求の送信元であるユーザノード１０－１を識別する送信元識別情報と、当該第２分散データ提供要求に含まれる第２データＩＤに含まれるワンタイムＩＤ及び生成時点情報と、当該不保持通知が送信された時点としての現在の時点を表す送信時点情報と、を含む。

そして、保存ノード１０－ｗは、図１０の処理を終了する。

【０２６１】

以上、説明したように、第３実施形態の情報処理システム１は、第１実施形態の情報処理システム１と同様の作用及び効果を奏することができる。

更に、第３実施形態の情報処理システム１において、メタデータから生成された分散データの要求は、ユーザノード１００が保存ノード２００へ、ワンタイムＩＤと生成時点情報とを含む第２分散データ提供要求を送信することにより行なわれる。

【０２６２】

加えて、情報処理システム１は、ユーザノード１００から、生成時点情報が共通し、且つ、ワンタイムＩＤが相違する、所定の閾値数以上の第２分散データ提供要求が所定の判定時間内に送信された場合、ユーザノード１００からの上記要求に応じた提供データの提供を禁止する。

【０２６３】

秘密データの保存を要求したユーザが、当該秘密データの復元を要求する場合、生成時点情報が共通し、且つ、ワンタイムＩＤが相違する、複数の第２分散データ提供要求が送信されることが少ない。従って、生成時点情報が共通し、且つ、ワンタイムＩＤが相違する、多数の第２分散データ提供要求が送信された場合、秘密データの保存を要求したユーザと異なるユーザが当該秘密データを不正に取得することを試行している確率が高い。

【０２６４】

そこで、上記のように、情報処理システム１は、生成時点情報が共通し、且つ、ワンタイムＩＤが相違する、所定の閾値数以上の第２分散データ提供要求が所定の判定時間内に送信された場合、ユーザノード１００からの要求に応じた提供データの提供を禁止する。これによれば、秘密データが不正に取得されることを抑制できる。

【０２６５】

なお、各保存ノード２００は、他の保存ノード２００により生成された拒否ノードリストを用いずに、自ノードが生成した拒否ノードリストのみを用いてもよい。これによれば、不正な拒否ノードリストによるサービス提供不能（ＤｏＳ）攻撃を適切に抑制できる。ＤｏＳは、Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅの略記である。

【０２６６】

また、拒否ノードリスト生成部２１１は、拒否ノードリストに含まれる送信元識別情報を、取得された不保持通知の数が所定の閾値通知数以上である送信元識別情報の中で、不保持通知の送信元である保存ノード２００の数が所定の閾値ノード数以上（例えば、保存ノード２００の総数の過半数）である送信元識別情報に制限してもよい。これによれば、不正な拒否ノードリストによるサービス提供不能（ＤｏＳ）攻撃を適切に抑制できる。

【０２６７】

また、拒否ノードリスト生成部２１１は、拒否ノードリストに含まれる送信元識別情報を、取得された不保持通知の数が所定の閾値通知数以上である送信元識別情報の中で、自ノードに対する不正なアクセスが検知された送信元識別情報に制限してもよい。これによれば、不正な拒否ノードリストによるサービス提供不能（ＤｏＳ）攻撃を適切に抑制できる。

【０２６８】

＜第３実施形態の第１変形例＞

次に、第３実施形態の第１変形例の情報処理システムについて説明する。第３実施形態の第１変形例の情報処理システムは、第３実施形態の情報処理システムに対して、ワンタイムＩＤとして用いる情報が相違している。以下、相違点を中心として説明する。なお、第３実施形態の第１変形例の説明において、第３実施形態にて使用した符号と同じ符号を付したものは、同一又はほぼ同様のものである。

【０２６９】

本例では、第２データＩＤに含まれるワンタイムＩＤは、第１実施形態の第４変形例と同様に、第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００に対して、保存ノード２００毎に異なる情報である。本例では、ワンタイムＩＤは、入力情報に基づいて生成された生成情報を構成する。

【０２７０】

本例では、第２分散データ群に対するノード群に含まれるＮ個の保存ノード２００のうちのｎ番目の保存ノード２００に対するワンタイムＩＤは、当該Ｎ個の保存ノード２００のうちのｒ番目の保存ノード２００を識別するノードＩＤを、入力情報に含まれるユーザＩＤに付加した情報の、所定のハッシュ関数に対するハッシュ値である。ｒは、ｎが１からＮ－１の各整数を表す場合、ｎ＋１を表すとともに、ｎがＮを表す場合、１を表す。例えば、ハッシュ関数は、ＭＤ５、ＳＨＡ－０、ＳＨＡ－１、ＳＨＡ－２、又は、ＳＨＡ－３と呼ばれるハッシュ関数である。

【０２７１】

以上、説明したように、第３実施形態の第１変形例の情報処理システム１は、第３実施形態の情報処理システム１と同様の作用及び効果を奏することができる。

更に、第３実施形態の第１変形例の情報処理システム１は、選択された装置群に含まれるＮ個の記憶装置１２に対して、記憶装置１２毎に異なる情報を識別情報として生成する。

【０２７２】

これによれば、秘密データを復元するために用いられる分散データが、識別情報に基づいて特定される確率を低減できる。

【０２７３】

なお、上記Ｎ個の保存ノード２００のうちのｎ番目の保存ノード２００に対するワンタイムＩＤは、当該Ｎ個の保存ノード２００のうちのｒ番目の保存ノード２００を識別するノードＩＤを、入力情報に含まれるユーザＩＤに付加した情報の、上記ハッシュ関数に対するハッシュ値を、第１のパラメータにより除した場合における剰余であってよい。第１のパラメータは、正の整数である。本例では、第１のパラメータは、情報処理システム１において予め定められる。これによれば、ワンタイムＩＤを生成する基となった情報が特定される確率を低減できる。

【０２７４】

なお、第１のパラメータは、変動してもよい。この場合、第１のパラメータは、保存ノードリストに含まれるノードＩＤの数が大きくなるほど大きくなるように定められてよい。この場合、例えば、保存ノードリストに含まれるノードＩＤの数と、第１のパラメータと、の関係を定める第１のパラメータ関数が、情報処理システム１において予め定められる。

【０２７５】

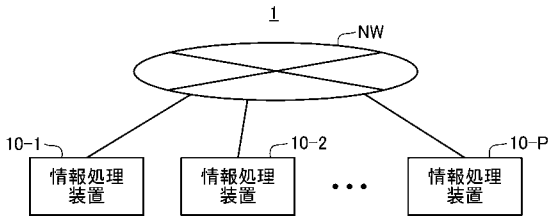
＜第３実施形態の第２変形例＞

次に、第３実施形態の第２変形例の情報処理システムについて説明する。第３実施形態の第２変形例の情報処理システムは、第３実施形態の第１変形例の情報処理システムに対して、第２データＩＤが、生成時点情報に代えて、生成時点情報のハッシュ値を含む点において相違している。以下、相違点を中心として説明する。なお、第３実施形態の第２変形例の説明において、第３実施形態の第１変形例にて使用した符号と同じ符号を付したものは、同一又はほぼ同様のものである。

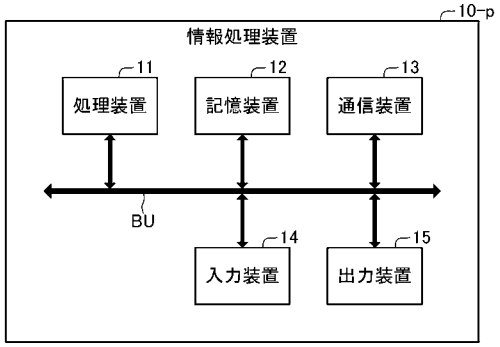
【０２７６】
本例では、第２データＩＤは、生成時点情報に代えて、生成時点識別情報を含む。本例では、生成時点識別情報は、生成時点情報の、所定のハッシュ関数に対するハッシュ値である。本例では、生成時点識別情報は、時点を識別する時点識別情報を構成する。例えば、ハッシュ関数は、ＭＤ５、ＳＨＡ－０、ＳＨＡ－１、ＳＨＡ－２、又は、ＳＨＡ－３と呼ばれるハッシュ関数である。
【０２７７】
以上、説明したように、第３実施形態の第２変形例の情報処理システム１は、第３実施形態の第１変形例の情報処理システム１と同様の作用及び効果を奏することができる。
更に、第３実施形態の第２変形例の情報処理システム１によれば、リスト生成時点が特定される確率を低減できる。
【０２７８】
なお、生成時点識別情報は、生成時点情報の、上記ハッシュ関数に対するハッシュ値を、第２のパラメータにより除した場合における剰余であってよい。第２のパラメータは、正の整数である。本例では、第２のパラメータは、情報処理システム１において予め定められる。これによれば、リスト生成時点が特定される確率を低減できる。
【０２７９】
なお、第２のパラメータは、変動してもよい。この場合、第２のパラメータは、保存ノードリストが選択される対象の保存ノードリスト候補の数、所定の期間にて生成される保存ノードリスト候補の数、又は、保存ノード２００として動作する情報処理装置１０の数が大きくなるほど大きくなるように定められてよい。この場合、例えば、保存ノードリストが選択される対象の保存ノードリスト候補の数、所定の期間にて生成される保存ノードリスト候補の数、又は、保存ノード２００として動作する情報処理装置１０の数と、第２のパラメータと、の関係を定める第２のパラメータ関数が、情報処理システム１において予め定められる。
【０２８０】
なお、上記各実施形態において、データを保存する時点の変化に伴って分散データの保存先を変更する技術は、メタデータに適用されている。ところで、当該技術は、メタデータと異なるデータ（例えば、ユーザデータ）に適用されてもよい。
【０２８１】
また、上記各実施形態において、情報処理システム１は、Ｐ２Ｐ方式に従った通信を行なう。ところで、情報処理システム１は、Ｐ２Ｐ方式と異なる方式（例えば、クライアント・サーバ方式等）に従った通信を行なってもよい。
【０２８２】
なお、本発明は、上述した実施形態に限定されない。例えば、上述した実施形態に、本発明の趣旨を逸脱しない範囲内において当業者が理解し得る様々な変更が加えられてよい。例えば、本発明の趣旨を逸脱しない範囲内において、上述した実施形態の他の変形例として、上述した実施形態及び変形例の任意の組み合わせが採用されてもよい。
【符号の説明】
【０２８３】
１　　情報処理システム
１０　情報処理装置
１１　処理装置
１２　記憶装置
１３　通信装置
１４　入力装置
１５　出力装置
１００　ユーザノード
１０１　ユーザ認証受付部
１０２　ユーザデータ保存要求受付部

１０３　保存ノードリスト取得部
１０４　ノード群決定部
１０５　分散データ生成部
１０６　分散データ保存要求送信部
１０７　ユーザデータ復元要求受付部
１０８　提供データ取得部
１０９　秘密データ復元部
２００　保存ノード
２０１　保存要求処理部
２０２　分散データ記憶部
２０３　提供要求処理部
２０４　動作通知処理部
２０５　動作通知記憶部
２０６　保存ノードリスト生成部
２０７　保存ノードリスト記憶部
２０８　保存ノードリスト要求処理部
２０９　不保持通知処理部
２１０　不保持通知記憶部
２１１　拒否ノードリスト生成部
２１２　拒否ノードリスト記憶部
ＢＵ　バス
ＮＷ　通信網

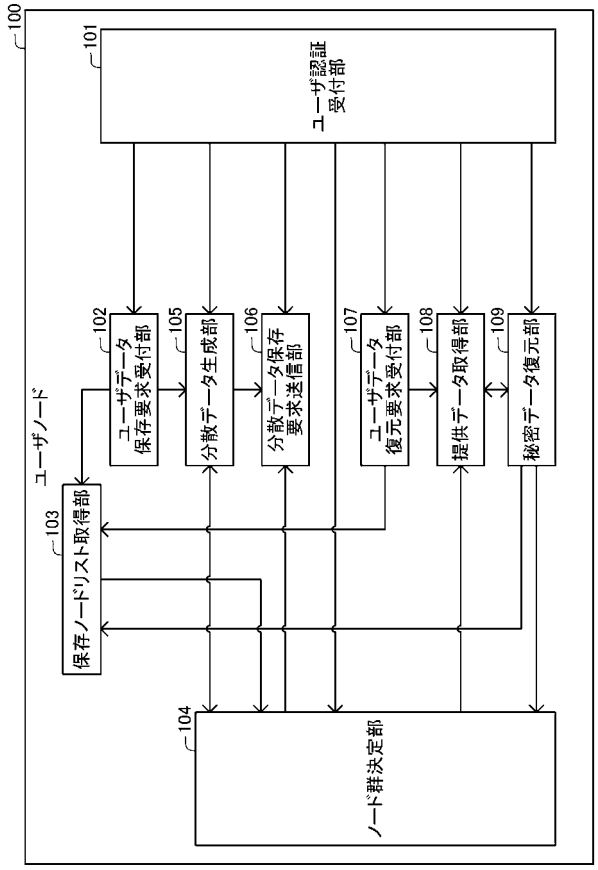
【図１】



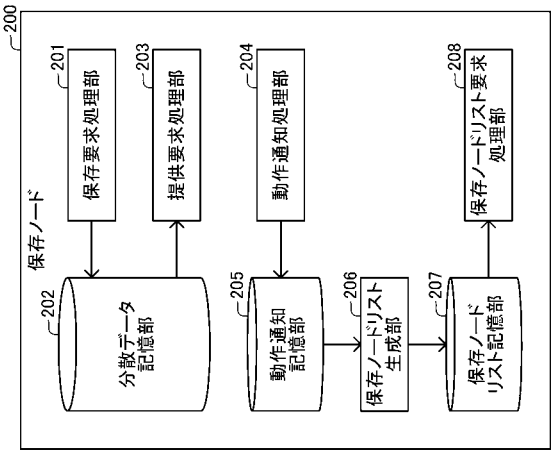
【図２】



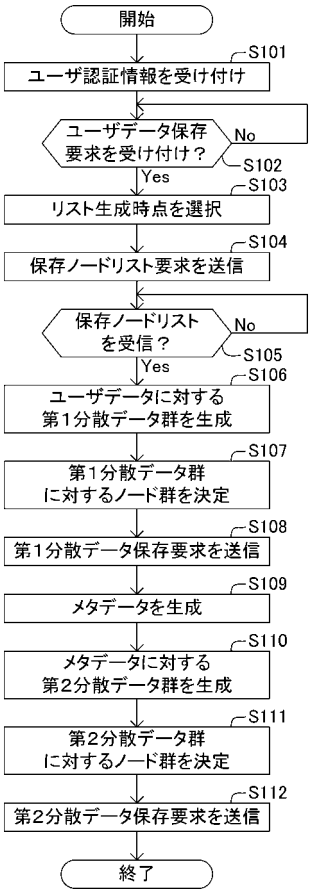
【図３】



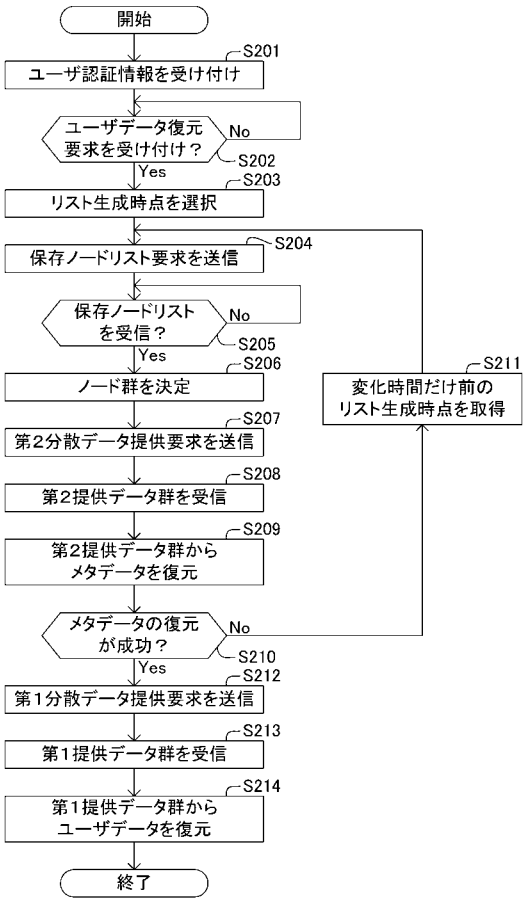
【図４】


200
保存ノード
201
保存要求処理部
203
提供要求処理部
204
動作通知処理部
208
保存ノードリスト要求処理部
202
分散データ記憶部
205
動作通知記憶部
206
保存ノードリスト生成部
207
保存ノードリスト記憶部

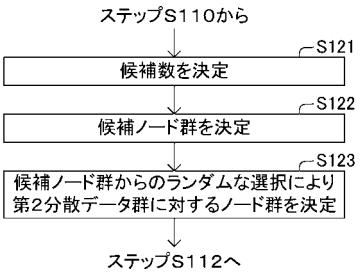
【図５】


開始
S101
ユーザ認証情報を受け付け
ユーザデータ保存要求を受け付け？
No
S102
Yes
S103
リスト生成時点を選択
S104
保存ノードリスト要求を送信
保存ノードリストを受信？
No
S105
Yes
S106
ユーザデータに対する第1分散データ群を生成
S107
第1分散データ群に対するノード群を決定
S108
第1分散データ保存要求を送信
S109
メタデータを生成
S110
メタデータに対する第2分散データ群を生成
S111
第2分散データ群に対するノード群を決定
S112
第2分散データ保存要求を送信
終了

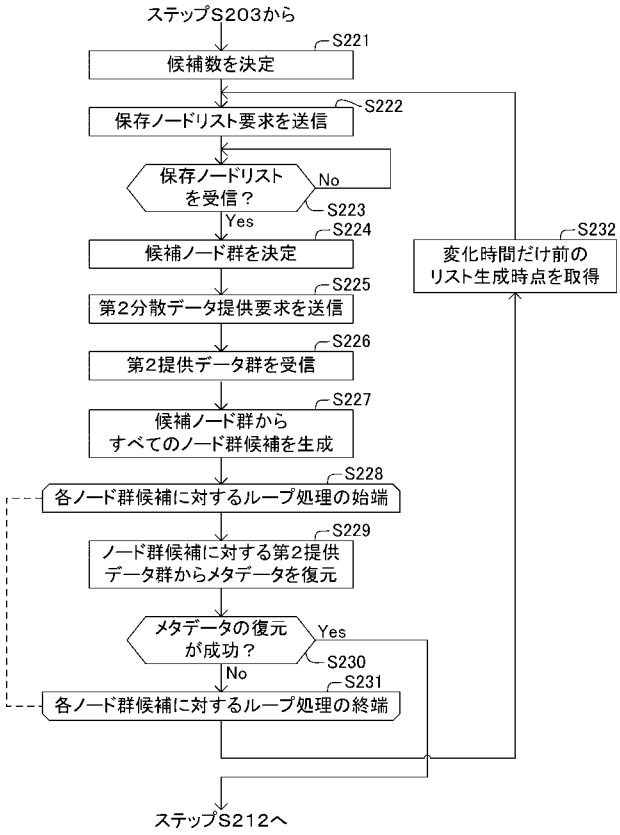
【図６】


開始
S201
ユーザ認証情報を受け付け
ユーザデータ復元要求を受け付け？
No
S202
Yes
S203
リスト生成時点を選択
S204
保存ノードリスト要求を送信
保存ノードリストを受信？
No
S205
Yes
S206
ノード群を決定
S211
変化時間だけ前のリスト生成時点を取得
S207
第2分散データ提供要求を送信
S208
第2提供データ群を受信
S209
第2提供データ群からメタデータを復元
メタデータの復元が成功？
No
S210
Yes
S212
第1分散データ提供要求を送信
S213
第1提供データ群を受信
S214
第1提供データ群からユーザデータを復元
終了

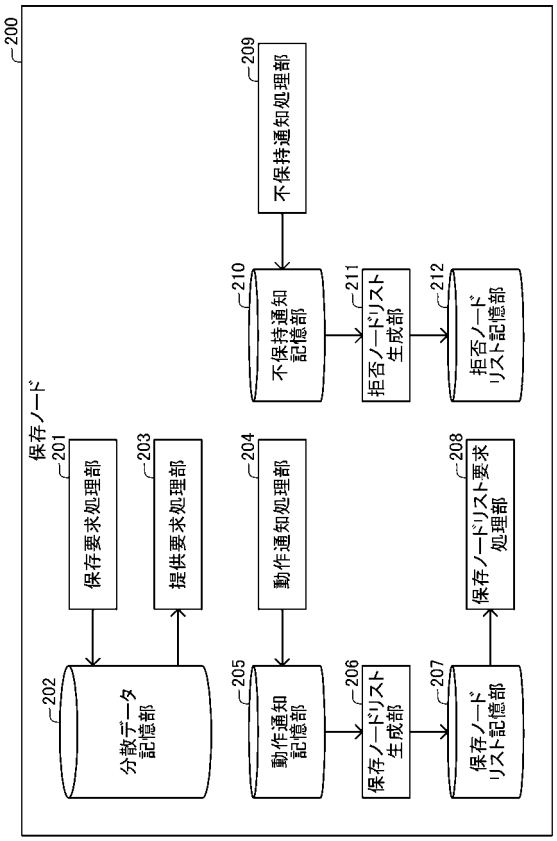
【図７】


ステップS110から
S121
候補数を決定
S122
候補ノード群を決定
S123
候補ノード群からのランダムな選択により第2分散データ群に対するノード群を決定
ステップS112へ

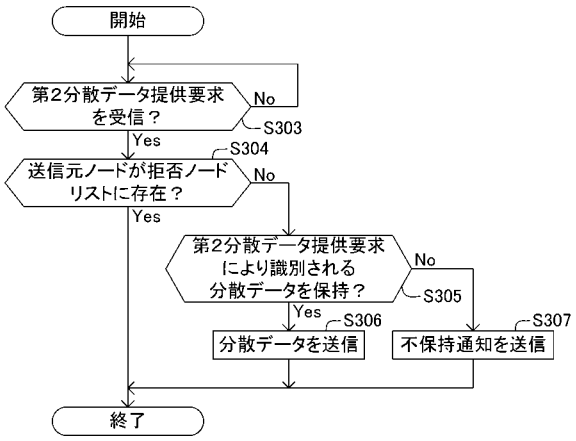
【図８】


ステップS203から
S221
候補数を決定
S222
保存ノードリスト要求を送信
保存ノードリスト
を受信？
No
S223
Yes
S224
候補ノード群を決定
S225
第2分散データ提供要求を送信
S226
第2提供データ群を受信
S227
候補ノード群から
すべてのノード群候補を生成
S228
各ノード群候補に対するループ処理の始端
S229
ノード群候補に対する第2提供
データ群からメタデータを復元
メタデータの復元
が成功？
Yes
S230
No
S231
各ノード群候補に対するループ処理の終端
S232
変化時間だけ前の
リスト生成時点を取得
ステップS212へ

【図９】


200
保存ノード
201
保存要求処理部
202
分散データ
記憶部
203
提供要求処理部
204
動作通知処理部
205
動作通知
記憶部
206
保存ノードリスト
生成部
207
保存ノード
リスト記憶部
208
保存ノードリスト要求
処理部
209
不保持通知処理部
210
不保持通知
記憶部
211
拒否ノードリスト
生成部
212
拒否ノード
リスト記憶部

【図１０】


開始
第2分散データ提供要求
を受信？
No
S303
Yes
S304
送信元ノードが拒否ノード
リストに存在？
No
Yes
第2分散データ提供要求
により識別される
分散データを保持？
No
S305
Yes
S306
分散データを送信
S307
不保持通知を送信
終了

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/080351

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/60(2013.01)i, *G06F12/00*(2006.01)i, *G09C1/00*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/60, G06F12/00, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2016
Kokai Jitsuyo Shinan Koho 1971-2016 Toroku Jitsuyo Shinan Koho 1994-2016

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamIII), IEEE Xplore, Secret sharing

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-147218 A (NTT Communications Corp.), 20 May 2004 (20.05.2004), paragraphs [0001] to [0048]	1-13
A	JP 2005-167794 A (Nippon Telegraph and Telephone Corp.), 23 June 2005 (23.06.2005), paragraphs [0001] to [0067]	1-13
A	JP 2007-73004 A (Canon Inc.), 22 March 2007 (22.03.2007), paragraphs [0001] to [0122]	1-13
A	US 5625692 A (INTERNATIONAL BUSINESS MACHINES CORP.), 29 April 1997 (29.04.1997), column 1, line 7 to column 18, line 22	1-13

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 December 2016 (13.12.16)	20 December 2016 (20.12.16)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/080351

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 7577689 B1 (ADOBE SYSTEMS INC.), 18 August 2009 (18.08.2009), column 1, line 3 to column 18, line 27	1-13
A	GANGER, G. R. et al., Survivable Storage Systems, Proceedings of the DARPA Information Survivability Conference & Exposition II, Vol. II, 2001.06, p.184-195, especially 2.PASIS	1-13

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2016/080351

JP 2004-147218 A	2004.05.20	(Family: none)	
JP 2005-167794 A	2005.06.23	(Family: none)	
JP 2007-73004 A	2007.03.22	(Family: none)	
US 5625692 A	1997.04.29	JP 8-251157 A EP 723348 A2	1996.09.27 1996.07.24
US 7577689 B1	2009.08.18	(Family: none)	

国際調査報告	国際出願番号 PCT／JP2016／080351

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06F21/60(2013.01)i, G06F12/00(2006.01)i, G09C1/00(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. G06F21/60, G06F12/00, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2016年
日本国実用新案登録公報	1996－2016年
日本国登録実用新案公報	1994－2016年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus/JMEDPlus/JST7580 (JDreamIII), IEEE Xplore
Secret sharing

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2004-147218 A (エヌ・ティ・ティ・コミニュケーションズ) 2004.05.20, 段落[0001]-[0048]	1-13
A	JP 2005-167794 A (日本電信電話株式会社) 2005.06.23, 段落[0001]-[0067]	1-13
A	JP 2007-73004 A (キヤノン株式会社) 2007.03.22, 段落[0001]-[0122]	1-13
A	US 5625692 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 1997.04.29, 1欄7行-18欄22行	1-13

☒ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
13. 12. 2016	20. 12. 2016

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5S	9364
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	中里 裕正 電話番号 03－3581－1101 内線 3546		

国際調査報告 国際出願番号 ＰＣＴ／ＪＰ２０１６／０８０３５１

C（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	US 7577689 B1 (ADOBE SYSTEMS INCORPORATED) 2009.08.18, 1欄3行-18欄27行	1-13
A	GANGER, G. R. et al., Survivable Storage Systems, Proceedings of the DARPA Information Survivability Conference & Exposition II, Vol. II, 2001.06, p.184-195, especially 2.PASIS	1-13

国際調査報告
パテントファミリーに関する情報

国際出願番号 ＰＣＴ／ＪＰ２０１６／０８０３５１

JP 2004-147218 A	2004.05.20	ファミリーなし	
JP 2005-167794 A	2005.06.23	ファミリーなし	
JP 2007-73004 A	2007.03.22	ファミリーなし	
US 5625692 A	1997.04.29	JP 8-251157 A	1996.09.27
		EP 723348 A2	1996.07.24
US 7577689 B1	2009.08.18	ファミリーなし	

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA

(72)発明者 高橋 大樹
宮城県仙台市青葉区片平二丁目１番１号 国立大学法人東北大学内
(72)発明者 福光 正幸
宮城県仙台市青葉区片平二丁目１番１号 国立大学法人東北大学内

Ｆターム(参考) 5J104 AA12 AA16 EA02 EA08 EA17 JA03 NA05 NA12 PA07

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。