

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第6567683号
(P6567683)

(45) 発行日 令和1年8月28日(2019.8.28)

(24) 登録日 令和1年8月9日(2019.8.9)

(51) Int.Cl.	F I
G06F 21/60 (2013.01)	G06F 21/60
G06F 21/62 (2013.01)	G06F 21/62 318
G06F 16/182 (2019.01)	G06F 16/182
G09C 1/00 (2006.01)	G09C 1/00 660D

請求項の数 13 (全 43 頁)

(21) 出願番号	特願2017-545453 (P2017-545453)	(73) 特許権者	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
(86) (22) 出願日	平成28年10月13日(2016.10.13)	(74) 代理人	100092978 弁理士 真田 有
(86) 国際出願番号	PCT/JP2016/080351	(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
(87) 国際公開番号	W02017/065209	(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
(87) 国際公開日	平成29年4月20日(2017.4.20)	(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
審査請求日	平成31年3月6日(2019.3.6)		
(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・地域又は機関	日本国(JP)		

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) 【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、前記保存要求を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、前記復元要求を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。

10

【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。

20

【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。

30

【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。

40

【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

50

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。

10

【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、

20

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】

30

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。

40

【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、

50

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。

10

【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。

20

【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】

30

【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。

40

【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。

50

【 0 0 0 8 】

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 】

【 0 0 0 9 】

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。

【 0 0 1 0 】

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。

【 0 0 1 1 】

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

10

20

30

40

50

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。

10

【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、

20

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。

30

【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。

40

【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。

50

【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。

10

【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。

20

【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 Drive)、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。

30

【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。

40

【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

50

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】

10

20

30

40

50

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。

10

【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。

20

【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。

30

【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。

40

【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。

50

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

10

【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。

20

【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。

30

【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。

40

【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

50

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。

10

【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。

20

【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。

30

【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。

40

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】

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

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、 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。

10

【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。

20

【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。

30

【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。

40

【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

50

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。

10

【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、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。

20

【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。

30

【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。

40

【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。

50

【 0 0 8 1 】

提供要求処理部 2 0 3 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 1 0 0 から受信する。

【 0 0 8 2 】

提供要求処理部 2 0 3 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 2 0 2 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 1 0 0 へ送信する。

【 0 0 8 3 】

提供要求処理部 2 0 3 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 2 0 2 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 1 0 0 へデータを送信しない。このとき、提供要求処理部 2 0 3 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 1 0 0 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 2 0 3 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 1 0 0 へ、所定のダミーデータを送信してもよい。

10

【 0 0 8 4 】

同様に、提供要求処理部 2 0 3 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 2 0 2 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 1 0 0 へ送信する。

20

【 0 0 8 5 】

提供要求処理部 2 0 3 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 2 0 2 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 1 0 0 へデータを送信しない。このとき、提供要求処理部 2 0 3 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 1 0 0 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 2 0 3 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 1 0 0 へ、所定のダミーデータを送信してもよい。

30

【 0 0 8 6 】

動作通知処理部 2 0 4 は、情報処理装置 1 0 - p が保存ノード 2 0 0 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 1 0 - 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 2 0 5 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 2 0 0 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。

【 0 0 8 7 】

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 1 0 - q のそれぞれへ送信する。

40

【 0 0 8 8 】

保存ノードリスト候補を受信した情報処理装置 1 0 - 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 1 0 - 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。

【 0 0 8 9 】

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

50

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

10

【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

20

【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）。

30

【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に記載のブルーフ・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

40

非特許文献2：Satoshi Nakamoto、「Bitcoin：A Peer-to-Peer 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】

50

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。

10

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。

20

【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。

30

【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】

40

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

50

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）。 10

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。 20

【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。 30

【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。 40

【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 50

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(

10

20

30

40

50

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。

【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

10

20

30

40

50

のステップS 2 0 8)。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S 2 0 9)。

【0132】

そして、ユーザノード10-1は、図6のステップS 2 0 9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S 2 1 0)。

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S 2 0 4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S 2 1 1)。

【0133】

そして、ユーザノード10-1は、図6のステップS 2 1 1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S 2 0 4)。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S 2 0 5からステップS 2 1 0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S 2 0 9にてメタデータの復元が成功するまで、図6のステップS 2 0 4からステップS 2 1 1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S 2 0 4からステップS 2 0 9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S 2 0 9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S 2 1 0にて「Yes」と判定し、図6のステップS 2 0 1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S 2 1 2)。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S 2 1 2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S 2 1 3)。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

10

20

30

40

50

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。

10

【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。

20

【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。

30

【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。

40

【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。

50

【 0 1 4 7 】

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。

【 0 1 4 8 】

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。

10

【 0 1 4 9 】

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。

【 0 1 5 0 】

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。

20

【 0 1 5 1 】

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が防止できる。

【 0 1 5 2 】

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。

30

40

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。

【 0 1 5 3 】

< 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。

【 0 1 5 4 】

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

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

10

20

30

40

50

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。

10

【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。

20

【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нтаイム識別子（換言すると、ワнтаイム ID）である。本例では、ワнта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нтаイム ID を生成する。

30

【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нта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。

40

【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нта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нта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

50

に対するハッシュ値を当該ワнта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нта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。

10

【0181】

なお、ワнта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нта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、の関係を決める第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。

20

【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。

30

【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нтаイム識別子(換言すると、ワнтаイムID)である。本例では、ワнта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нта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нта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。

40

【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нта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

50

ード200に対して、保存ノード200毎に異なる情報をワнта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нта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нта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нта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нта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

10

20

30

40

50

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ID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ID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ID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ID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。

10

20

30

40

50

【 0 2 0 3 】

また、ノード群決定部 1 0 4 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 1 0 4 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。

【 0 2 0 4 】

ノード群決定部 1 0 4 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 1 0 3 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 ID 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 ID によりそれぞれ識別される候補数 C の保存ノード 2 0 0 は、候補ノード群を構成する。

10

【 0 2 0 5 】

本例では、提供データ取得部 1 0 8 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 1 0 4 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 2 0 0 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 1 0 8 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 1 0 4 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 2 0 0 のうちの、一部の保存ノード 2 0 0 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 1 0 8 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 2 0 0 のうちの残余の保存ノード 2 0 0 に第 2 分散データ提供要求を送信してよい。

20

【 0 2 0 6 】

提供データ取得部 1 0 8 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 2 0 0 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 1 0 8 は、第 2 提供データ群を取得する。なお、保存ノード 2 0 0 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 2 0 0 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。

30

【 0 2 0 7 】

秘密データ復元部 1 0 9 は、ノード群決定部 1 0 4 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 2 0 0 から選択される N 個の保存ノード 2 0 0 の組み合わせのすべてを生成する。N 個の保存ノード 2 0 0 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 2 0 0 により構成される。

40

【 0 2 0 8 】

秘密データ復元部 1 0 9 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 1 0 8 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 2 0 0 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。

【 0 2 0 9 】

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 1 0 - 1 は、図 5 の処理に代えて、図 5 の処理におけるステップ S 1 1 1 の処理を、図 7 のステップ S 1 2 1 からステップ S 1 2 3 までの処理に置換した処理を実行する。

50

【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。

10

【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。

20

【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。

30

【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IDを選択することにより候補ノード群を決定する。

40

【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

50

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。

10

【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行う。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行ってもよい。

20

【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)。

30

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)。

40

【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。

50

【 0 2 2 9 】

ユーザノード 1 0 - 1 は、図 8 のステップ S 2 2 9 にてメタデータの復元が成功するまで、図 8 のステップ S 2 2 2 からステップ S 2 3 2 までの処理を繰り返し実行する。

【 0 2 3 0 】

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 1 2 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。

【 0 2 3 1 】

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 1 2 の中から N 個の記憶装置 1 2 をランダムに選択し、選択された N 個の記憶装置 1 2 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 1 2 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。

【 0 2 3 2 】

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 1 2 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。

【 0 2 3 3 】

< 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。

【 0 2 3 4 】

本例では、ユーザノード 1 0 0 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、T L S (T r a n s p o r t L a y e r S e c u r i t y) と呼ばれる技術を用いて行なわれてよい。

【 0 2 3 5 】

本例では、分散データ保存要求送信部 1 0 6 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。

10

20

30

40

50

【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нтаイムIDを生成する。本例では、ワнта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нтаイムIDとして用いる。例えば、ハッシュ関数は、MD5、SHA-0、SHA-1

10

、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нта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нтаイムIDを生成する。

20

【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нта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。

30

【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нта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нтаイムIDに代えて、ワнта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。

40

【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】

50

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。

10

【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。

20

【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。

30

【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。

40

【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。

50

【 0 2 5 3 】

なお、提供要求処理部 2 0 3 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。

【 0 2 5 4 】

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 1 0 - w は、図 1 0 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。

【 0 2 5 5 】

保存ノード 1 0 - w は、第 2 分散データ提供要求をユーザノード 1 0 - 1 から受信するまで待機する（図 1 0 のステップ S 3 0 3 の「No」ルート）。

10

【 0 2 5 6 】

その後、第 2 分散データ提供要求がユーザノード 1 0 - 1 から受信されると、保存ノード 1 0 - 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 1 0 のステップ S 3 0 4）。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 1 0 - 1 である。

【 0 2 5 7 】

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 1 0 - 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 1 0 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 1 0 - w は、「No」と判定し、図 1 0 のステップ S 3 0 3 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 1 2 に保持されているか否かを判定する（図 1 0 のステップ S 3 0 5）。

20

【 0 2 5 8 】

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 1 2 に保持されている場合、保存ノード 1 0 - 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 1 0 - 1 へ、当該分散データである提供データを送信する（図 1 0 のステップ S 3 0 6）。そして、保存ノード 1 0 - w は、図 1 0 の処理を終了する。

【 0 2 5 9 】

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 1 2 に保持されていない場合、保存ノード 1 0 - w は、「No」と判定し、他の保存ノード 2 0 0 のそれぞれへ不保持通知を送信する（図 1 0 のステップ S 3 0 7）。

30

【 0 2 6 0 】

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 1 0 - 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нта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 1 0 - w は、図 1 0 の処理を終了する。

40

【 0 2 6 1 】

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 1 0 0 が保存ノード 2 0 0 へ、ワнта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。

【 0 2 6 2 】

加えて、情報処理システム 1 は、ユーザノード 1 0 0 から、生成時点情報が共通し、且つ、ワнта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 1 0 0 からの上記要求に応じた提供データの提

50

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нта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нта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нта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、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нта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нта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нта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нта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】

10

20

30

40

50

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нта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нта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。

10

【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、の関係性を定める第1の関数が、情報処理システム1において予め定められる。

20

【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。

30

【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。

40

【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

50

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、の関係性を定める第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。

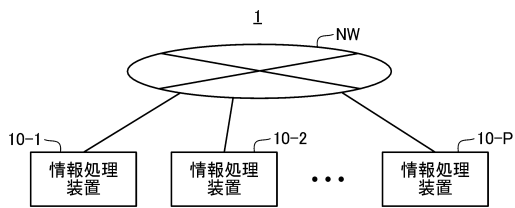
【符号の説明】

【0283】

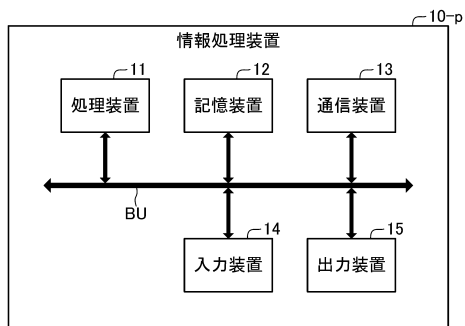
1	情報処理システム	
10	情報処理装置	
11	処理装置	
12	記憶装置	
13	通信装置	
14	入力装置	
15	出力装置	
100	ユーザノード	
101	ユーザ認証受付部	
102	ユーザデータ保存要求受付部	30
103	保存ノードリスト取得部	
104	ノード群決定部	
105	分散データ生成部	
106	分散データ保存要求送信部	
107	ユーザデータ復元要求受付部	
108	提供データ取得部	
109	秘密データ復元部	
200	保存ノード	
201	保存要求処理部	
202	分散データ記憶部	40
203	提供要求処理部	
204	動作通知処理部	
205	動作通知記憶部	
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	50

B U バス
N W 通信網

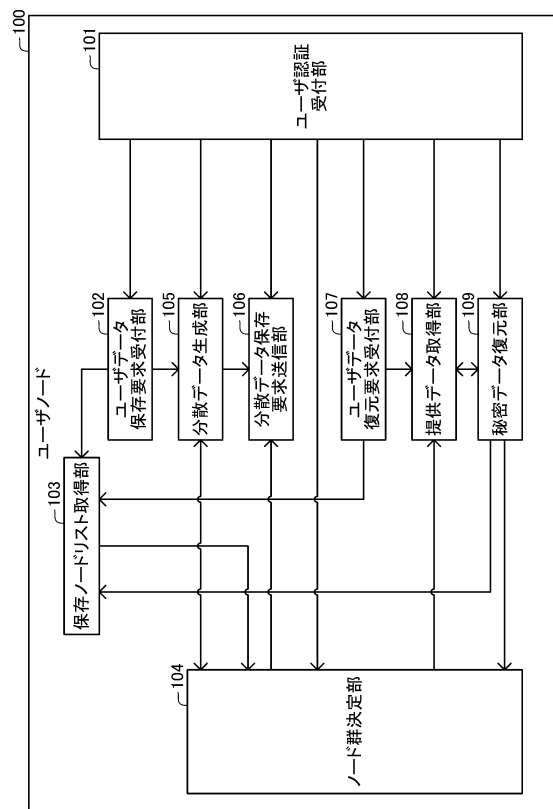
【図1】



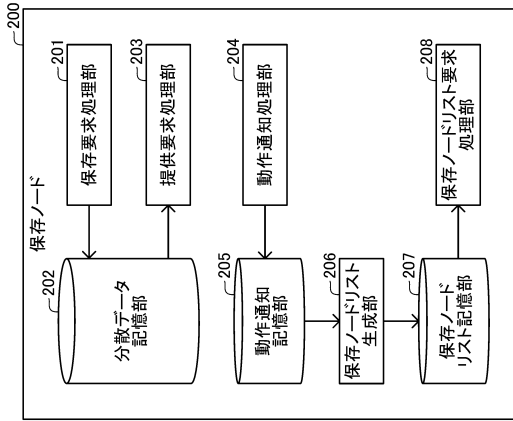
【図2】



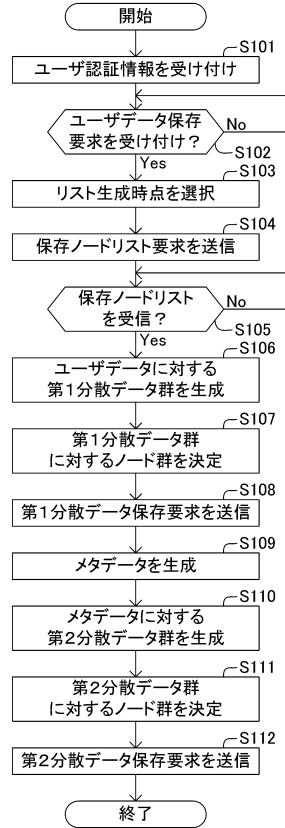
【図3】



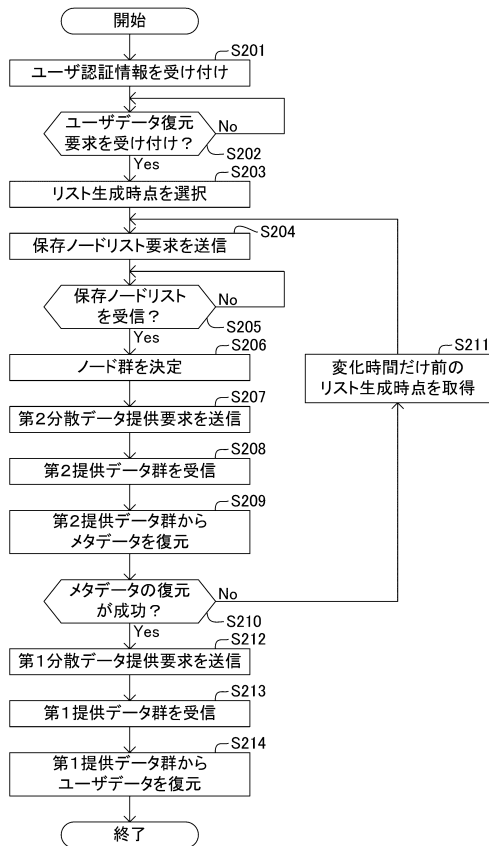
【図4】



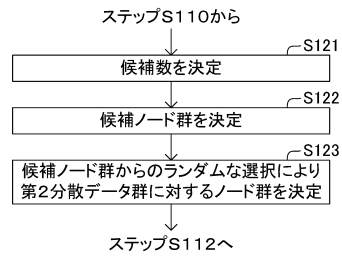
【図5】



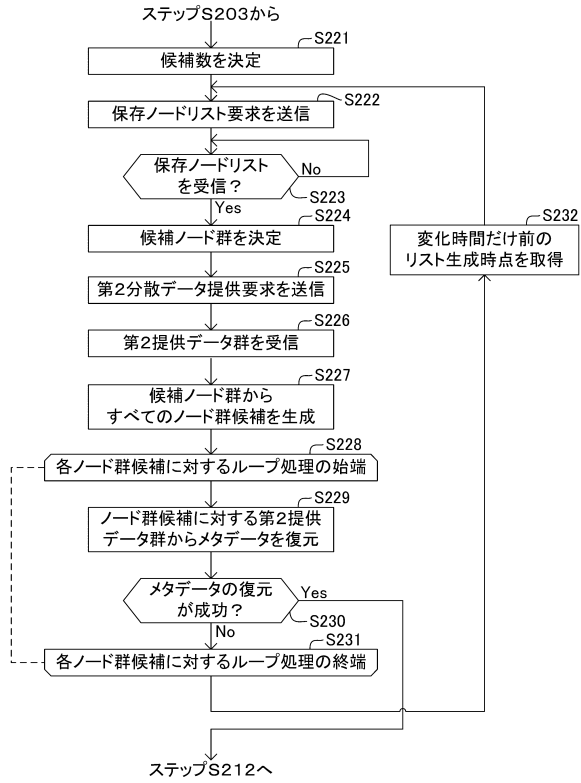
【図6】



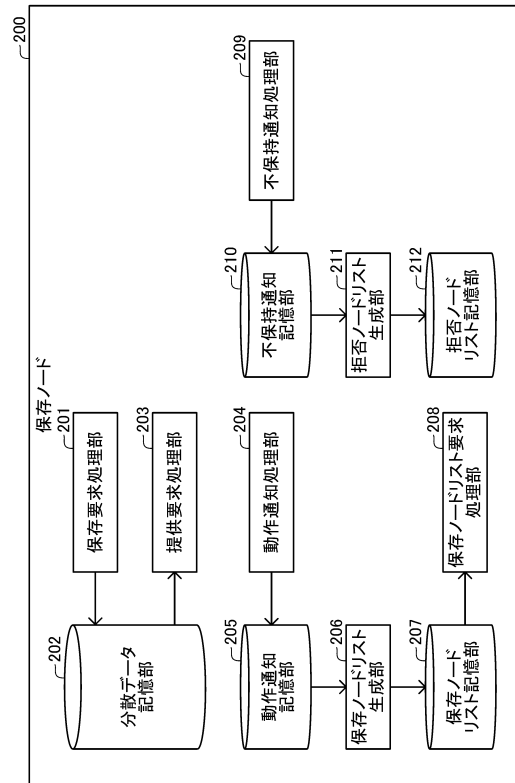
【図7】



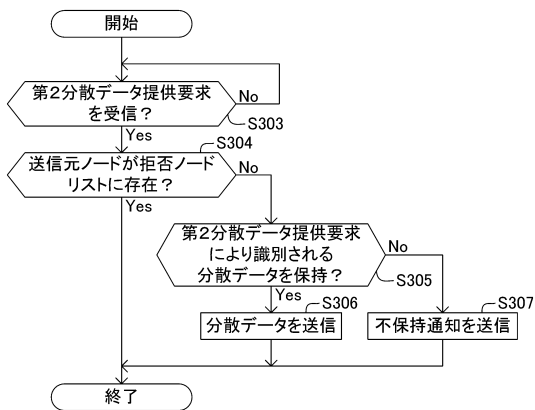
【図8】



【図9】



【図10】



フロントページの続き

- (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

審査官 中里 裕正

- (56)参考文献 特開2004-147218(JP,A)
特開2005-167794(JP,A)
特開2007-73004(JP,A)
米国特許第5625692(US,A)
米国特許第7577689(US,B1)
GANGER, G. R. et al., Survivable Storage Systems, Proceedings of the DARPA Information Survivability Conference & Exposition II, 2001年 6月, Vol. II, p.184-195

(58)調査した分野(Int.Cl., DB名)

G06F 21/60
G06F 16/182
G06F 21/62
G09C 1/00
JSTPlus/JMEDPlus/JST7580(JDreamIII)
IEEE Xplore