

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2022年9月9日(09.09.2022)



(10) 国際公開番号

WO 2022/186367 A1

- (51) 国際特許分類:
G06F 21/62 (2013.01) *G06F 21/60* (2013.01)
- (21) 国際出願番号: PCT/JP2022/009291
- (22) 国際出願日: 2022年3月4日(04.03.2022)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2021-034757 2021年3月4日(04.03.2021) JP
- (71) 出願人: N E C ソ リ ュ ー シ ョ ン イ ノ ベ ー タ 株 式 会 社 (NEC SOLUTION INNOVATORS, LTD.) [JP/JP]; 〒1368627 東京都江東区新木場一丁目18番7号 Tokyo (JP).
- (72) 発明者: 坂 本 久 (SAKAMOTO, Hisashi); 〒1368627 東京都江東区新木場一丁目18番7号 N E C ソ リ ュ ー シ ョ ン イ ノ ベ ー タ 株 式 会 社 内 Tokyo (JP).
- (74) 代理人: 特許業務法人ブライタス(BRIGHTAS IP ATTORNEYS); 〒1040061 東京都中央区銀座1丁目19番12号 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): 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, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) **Title:** DATA MANAGEMENT DEVICE, DATA MANAGEMENT SYSTEM, DATA MANAGEMENT METHOD, AND COMPUTER READABLE RECORDING MEDIUM

(54) 発明の名称: データ管理装置、データ管理システム、データ管理方法及びコンピュータ読み取り可能な記録媒体



- 1 Data management device
11 Reception unit
12 Determination unit
13 Acquisition unit
14 Data generation unit
15 Use-rights generation unit
16 Storage unit

(57) **Abstract:** A data management device 1 comprises: a reception unit 11 that receives a request to access first data by a user; a determination unit 12 that determines whether the user can use the first data; an acquisition unit 13 that, if the user can use the first data, acquires the first data and use-rights information relating to use-rights for the first data; a data generation unit 14 that uses the acquired first data to generate second data; a use-rights generation unit 15 that generates use-rights for the second data, including the use-rights for the first data; and a storage unit 16 that stores the second data

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,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (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), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一 国際調査報告(条約第21条(3))

in association with use-rights information relating to the use-rights for the second data.

(57) 要約：データ管理装置1は、利用者による第1データへのアクセス要求を受け付ける受付部11と、利用者が、第1データが利用可能であるかを判定する判定部12と、利用者が、第1データが利用可能である場合、第1データ、及び、第1データの利用権限に係る利用権限情報を取得する取得部13と、取得された第1データを利用して第2データを生成するデータ生成部14と、第1データの利用権限を含めた第2データの利用権限を生成する利用権限生成部15と、第2データと、第2データの利用権限に係る利用権限情報とを対応付けて記憶する記憶部16と、を備える。

明 細 書

発明の名称：

データ管理装置、データ管理システム、データ管理方法及びコンピュータ読み取り可能な記録媒体

技術分野

[0001] 本発明は、データ管理装置、データ管理システム、データ管理方法及び、それらを実現するためのプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

背景技術

[0002] 近年、ネットワークを介してデジタルコンテンツのデータを管理することが行われている。そして、データにパスワードを設定し、又は、アクセス権を設定することで、データの不正利用を防止することが定常的に行われている。例えば、特許文献1には、セキュリティポリシーを電子文書に付与して、電子文書の利用を制限するシステムが開示されている。この特許文献1に記載のシステムは、電子文書の利用権限を所有していない利用者から、電子文書の発行者に対する利用許可の申請を受け付けると、利用者利用権限を付与する構成である。

先行技術文献

特許文献

[0003] 特許文献1：特開2012-212356号公報

発明の概要

発明が解決しようとする課題

[0004] 特許文献1により、利用が許可されたものに対して、電子文書の利用権限を付与することができる。しかしながら、特許文献1では、利用が許可された利用者が電子文書を利用した段階で、電子文書は保護されない状態になってしまうおそれがある。例えば、利用が許可されたデータを複写又は編集し

て新たなデータを生成した場合、新たなデータに元のデータの内容が含まれているにもかかわらず、元のデータの利用が許可されていないものも新たなデータにアクセス可能となることがある。このような場合、結果として、元のデータが保護できていないことになってしまう。

[0005] 本発明の目的の一例は、第2データの生成に利用される第1データの利用権限を、第2データの利用権限に継承させることで、第1データを保護する、データ管理装置、データ管理システム、データ管理方法、及び、それらを実現するためのプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することにある。

課題を解決するための手段

[0006] 上記目的を達成するため、本発明の一側面におけるデータ管理装置は、利用者による第1データへのアクセス要求を受け付ける受付部と、前記利用者が、前記第1データが利用可能であることを判定する判定部と、前記利用者が、前記第1データが利用可能である場合、前記第1データ、及び、前記第1データの利用権限に係る利用権限情報を取得する取得部と、取得された前記第1データを利用して第2データを生成するデータ生成部と、

前記第1データの利用権限を含めた前記第2データの利用権限を生成する利用権限生成部と、

前記第2データと、前記第2データの利用権限に係る利用権限情報とを対応付けて記憶する記憶部と、

を備える、ことを特徴とする。

[0007] また、上記目的を達成するため、本発明の一側面におけるデータ管理システムは、

利用者による第1データへのアクセス要求を受け付ける受付部と、

前記利用者が、前記第1データが利用可能であることを判定する判定部と、

前記利用者が、前記第1データが利用可能である場合、前記第1データ、

及び、前記第1データの利用権限に係る利用権限情報を送信する送信部と、

送信された前記第 1 データ、及び、前記利用権限情報を取得する取得部と、
、
取得された前記第 1 データを利用して第 2 データを生成するデータ生成部と、
前記第 1 データの利用権限を含めた前記第 2 データの利用権限を生成する利用権限生成部と、
前記第 2 データと、前記第 2 データの利用権限に係る利用権限情報とを対応付けて記憶する記憶部と、
を備える、ことを特徴とする。

[0008] また、上記目的を達成するため、本発明の一側面におけるデータ管理方法は、

利用者による第 1 データへのアクセス要求を受け付けるステップと、
前記利用者が、前記第 1 データが利用可能であることを判定するステップと、
、
前記利用者が、前記第 1 データが利用可能である場合、前記第 1 データ、及び、前記第 1 データの利用権限に係る利用権限情報を送信するステップと、
、
送信された前記第 1 データ、及び、前記利用権限情報を取得するステップと、
取得された前記第 1 データを利用して第 2 データを生成するステップと、
前記第 1 データの利用権限を含めた前記第 2 データの利用権限を生成するステップと、
前記第 2 データと、前記第 2 データの利用権限に係る利用権限情報とを対応付けて記憶するステップと、
を備える、ことを特徴とする。

[0009] 更に、上記目的を達成するため、本発明の一側面におけるコンピュータ読み取り可能な記録媒体は、
コンピュータに、

利用者による第 1 データへのアクセス要求を受け付けるステップと、
前記利用者が、前記第 1 データが利用可能であることを判定するステップと、
、
前記利用者が、前記第 1 データが利用可能である場合、前記第 1 データ、
及び、前記第 1 データの利用権限に係る利用権限情報を取得するステップと、
、
取得された前記第 1 データを利用して第 2 データを生成するステップと、
前記第 1 データの利用権限を含めた前記第 2 データの利用権限を生成する
ステップと、
前記第 2 データと、前記第 2 データの利用権限に係る利用権限情報とを対
応付けて記憶するステップと、
を実行させる命令を含むプログラムを記録した、ことを特徴とする。

発明の効果

[0010] 以上のように本発明によれば、第 2 データの生成に利用される第 1 データの利用権限を、第 2 データの利用権限に継承させることで、第 1 データを保護することができる。

図面の簡単な説明

[0011] [図1]図 1 は、実施形態 1 におけるデータ管理装置の構成を示すブロック図である。

[図2]図 2 は、データ管理装置の具体的な構成を示すブロック図である。

[図3]図 3 は、データ管理装置の動作を示すフロー図である。

[図4]図 4 は、実施形態 2 のデータの利用を説明するための図である。

[図5]図 5 は、データ管理システムの具体的な構成を示すブロック図である。

[図6]図 6 は、データ管理装置において、データを登録する際のフロー図である。

[図7]図 7 は、データ管理装置において、データを登録する際のフロー図である。

[図8]図 8 は、データ管理装置において、データを登録する際のフロー図であ

る。

[図9]図9は、本発明の実施形態1、2におけるデータ管理装置を実現するコンピュータの一例を示すブロック図である。

発明を実施するための形態

[0012] (実施形態1)

図1は、本実施形態におけるデータ管理装置1の構成を示すブロック図である。図1に示すように、データ管理装置1は、受付部11と、判定部12と、取得部13と、データ生成部14と、利用権限生成部15と、記憶部16とを備えている。

[0013] 受付部11は、利用者による第1データへのアクセス要求を受け付ける。

[0014] 判定部12は、利用者が、第1データが利用可能であることを判定する。

[0015] 取得部13は、利用者が、第1データが利用可能である場合、第1データ、及び、第1データの利用権限に係る利用権限情報を取得する。

[0016] データ生成部14は、取得された第1データを利用して第2データを生成する。

[0017] 利用権限生成部15は、第1データの利用権限を含めた第2データの利用権限を生成する。

[0018] 記憶部16は、第2データと、第2データの利用権限に係る利用権限情報とを対応付けて記憶する。

[0019] 以上のように本実施形態のデータ管理装置1は、第2データの生成に利用される第1データの利用権限を、第2データの利用権限に継承させることで、第1データを保護することができる。

[0020] 次に、本実施形態のデータ管理装置1の構成について具体的に説明する。

本実施形態では、ユーザAが生成した第1データ（以下、データA）を、ユーザBが利用して、第2データ（以下、データB）を生成するものとして説明する。より詳しくは、ユーザAは、データ管理装置1を用いてデジタルコンテンツであるデータAを生成する。データAには利用権限が設定されている。利用権限は、例えば、データAにアクセス可能なユーザである。データ

Aの利用権限があるユーザBは、データ管理装置1において、データAを取得する。そして、ユーザBは、データ管理装置1を用いて、データAに基づいてデータBを生成する。データBは、データAの複製であってもよいし、データAを編集したものであってもよい。本実施形態では、ユーザBがデータBを生成した場合において、データ管理装置1は、データBの利用権限に、データAに設定された利用権限を含めて、データBの利用権限を生成する。つまり、データBの利用権限には、データAの利用権限が引き継がれるようになっている。

[0021] 図2は、データ管理装置1の具体的な構成を示すブロック図である。

[0022] データ管理装置1は、図1の構成に加え、認証部17、復号化部18、暗号化部19、削除部20、データ記憶部21、鍵記憶部22、及び、利用権限記憶部23、を備える。

[0023] データ記憶部21は、ユーザが生成するデータを記憶する記憶装置である。データ記憶部21は、暗号化されたデータを記憶する。

[0024] 鍵記憶部22は、暗号化されたデータを復号する際に用いられる復号鍵を記憶する記憶装置である。

[0025] 利用権限記憶部23は、生成されたデータに設定された利用権限に係る利用権限情報を記憶する記憶装置である。利用権限情報は、データへのアクセス権限を有するユーザに関する情報である。

[0026] 記憶装置は、例えば、ハードディスクドライブ、フラッシュメモリ等の半導体記憶装置などである。なお、データ、利用権限情報及び復号鍵は、それぞれ同じ記憶装置に記憶されていてもよいし、データ管理装置1の外部の記憶装置に記憶されてもよい。

[0027] また、以下では、ユーザAが生成し、暗号化されたデータAがデータ記憶部21に記憶され、そのデータAを復号する復号鍵が鍵記憶部22に記憶され、データAの利用権限に係る利用権限情報が、利用権限記憶部23に記憶されているものとして説明する。

[0028] 認証部17は、データを生成するユーザを認証する。データ生成時、ユー

ザは、データ管理装置 1 へのログイン操作を行う。認証部 17 は、このときのログイン認証を行う。ログイン認証では、認証部 17 は、データ管理装置 1 が備える記憶装置、又は、外部の記憶装置に記憶されたユーザ情報を参照して、ユーザがデータ管理装置 1 の利用が可能であるかの認証を行う。認証部 17 による認証方法は、パスワード認証又は生体認証など、特に限定されない。

[0029] 受付部 11 は、データ記憶部 21 に記憶されたデータへのアクセス要求を受け付ける。例えば、ユーザ B が、データ記憶部 21 に記憶されたデータ A を利用してデータ B を生成する場合、認証部 17 によるユーザ B の認証が行われると、後述のデータ生成部 14 が、ユーザ B が生成したプログラム環境を実行し、その環境下において、受付部 11 は、ユーザ B によるデータ A へのアクセス要求の受け付けを容認する。

[0030] 判定部 12 は、受付部 11 が受け付けたアクセス要求をするユーザに、アクセスするデータの利用権限があるかを判定する。例えば、受付部 11 が、ユーザ B によるデータ A へのアクセス要求を受け付けた場合、判定部 12 は、データ A に対応付けられた利用権限情報を、利用権限記憶部 23 から取得する。判定部 12 は、その利用権限にユーザ B が含まれているかを判定し、含まれている場合には、ユーザ B にデータ A の利用権限があると判定する。

[0031] 取得部 13 は、判定部 12 がユーザにアクセスするデータの利用権限があると判定すると、そのデータをデータ記憶部 21 から取得する。また、取得部 13 は、そのデータに対応付けられた利用権限情報を利用権限記憶部 23 から取得する。さらに、取得部 13 は、データを復号するための復号鍵を鍵記憶部 22 から取得する。例えば、ユーザ B にデータ A の利用権限があると判定部 12 が判定すると、取得部 13 は、データ A をデータ記憶部 21 から取得する。また、取得部 13 は、データ A に対応付けられた利用権限情報を利用権限記憶部 23 から取得する。さらに、取得部 13 は、データ A を復号するための復号鍵を鍵記憶部 22 から取得する。

[0032] 復号化部 18 は、取得部 13 が取得した復号鍵を用いて、取得部 13 が取

得した、暗号化されているデータを復号する。取得部 13 がデータ A を取得した場合、復号化部 18 は、そのデータ A を復号する。

[0033] データ生成部 14 はデータを生成する。データ生成部 14 は、予めユーザが生成した、保護されたデータを利用できるプログラムをデータ生成部 14 の内部に配置して、それを実行する。そして、データ生成部 14 は、実行した環境下において、ユーザの操作に従い、必要であれば既に生成され保護されている他のデータを参照したりして、データを生成する。例えば、ユーザ B がデータ B を生成する場合、データ生成部 14 は、ユーザ B が生成したプログラム環境を実行し、その環境下において、ユーザ B の操作に従い、復号化部 18 が復号したデータ A に基づいて、データ B を生成する。データ生成部 14 の内部は他の利用者から侵入したり参照したりすることはできず、また、内部のプログラムから外部に通信等でデータを転送する事を制限される。それにより、このプログラム環境下でデータを生成することで、復号化されたデータが他の利用者に不正に伝達されることを抑制する。

[0034] 暗号化部 19 は、生成されたデータを暗号化する。例えば、暗号化部 19 は、データ A に基づいて生成されたデータ B を暗号化する。暗号化されたデータと、このデータを復号する復号鍵は、後述の記憶部 16 によって、データ記憶部 21 及び鍵記憶部 22 に記憶される。

[0035] 利用権限生成部 15 は、ユーザの操作に従い、データ生成部 14 によって生成されたデータの利用権限を生成する。具体的に、データ A を利用してデータ B が生成された場合、利用権限生成部 15 は、取得部 13 が取得したデータ A の利用権限情報に基づいて、生成する利用権限に、利用されたデータ A に設定された利用権限を含める。これにより、利用されるデータ A に設定された利用権限が、新たに生成されたデータ B の利用権限に承継されるようになる。その結果、新たに生成されたデータ B がさらに別のユーザ C に利用される場合、そのユーザ C が、データ B の生成に利用したデータ A の利用権限を有していないと、ユーザ C によるデータ B へのアクセスが拒否されるようになり、データ B に含まれるデータ A をユーザ C から保護することができ

る。生成された利用権限は、記憶部 16 によって、利用権限情報として利用権限記憶部 23 に記憶される。

[0036] 記憶部 16 は、暗号化されたデータをデータ記憶部 21 に記憶する。また、記憶部 16 は、生成された利用権限に係る利用権限情報を、利用権限記憶部 23 に記憶する。また、記憶部 16 は、暗号化されたデータの復号鍵を鍵記憶部 22 に記憶する。

[0037] 削除部 20 は、復号されたデータを削除する。復号されたデータは一時的に RAM などに保存される。削除部 20 は、保存されたデータを削除する。例えば、データ A を利用してデータ B を生成する場合、削除部 20 は、復号されたデータ A を削除する。このように、復号したデータ A を装置内に残さないようにすることで、データ A の保護を行うことができる。なお、削除するタイミングは、データ B を暗号化するタイミングであってもよいし、データ B をデータ記憶部 21 に記憶するタイミングであってもよいし、データ生成部 14 が内部でプログラムを実行し、その実行が終了したタイミングでもよい。

[0038] 次に、本実施形態におけるデータ管理装置 1 の動作について図 3 を用いて説明する。図 3 は、データ管理装置 1 の動作を示すフロー図である。以下の説明においては、適宜図 1 ～図 2 を参酌する。また、本実施形態では、データ管理装置 1 を動作させることによって、データ管理方法が実施される。よって、本実施形態におけるデータ管理方法の説明は、以下のデータ管理装置 1 の動作説明に代える。

[0039] 図 3 は、データ管理装置 1 においてデータ B を生成する際の動作を示すフロー図である。

[0040] 前提として、データ記憶部 21 には、ユーザ A が生成し、暗号化されたデータ A が記憶されているものとする。また、鍵記憶部 22 には、データ A を復号する復号鍵が記憶されているものとする。さらに、利用権限記憶部 23 には、データ A に設定されたデータ A の利用権限に係る利用権限情報が記憶されているものとする。そして、ユーザ B がデータ A を利用して、データ B

を生成するものとする。

[0041] この前提において、ユーザBがデータ管理装置1へのログイン操作を行うと、認証部17はユーザBの認証判定を行う（S1）。認証に失敗した場合（S1：NO）、データ管理装置1は本処理を終了する。認証に成功すると（S1：YES）、データ生成部14は、予めユーザが生成した、保護されたデータを利用できるプログラム環境を実行する（S2）。以下の処理は、このプログラム環境下で実行される。受付部11は、ユーザBにより、データ記憶部21に記憶されたデータAへのアクセス要求を受け付ける（S3）。

[0042] 受付部11がアクセス要求を受け付けると、判定部12は、データAの利用権限情報を利用権限記憶部23から取得して、ユーザBにデータAの利用権限があるか否かを判定する（S4）。ユーザBにデータAの利用権限がない場合（S4：NO）、データ管理装置1は本処理を終了する。ユーザBにデータAの利用権限がある場合（S4：YES）、取得部13は、暗号化されたデータAをデータ記憶部21から取得し、そのデータAを復号する復号鍵を鍵記憶部22から取得し、データAに設定された利用権限に係る利用権限情報を利用権限記憶部23から取得する（S5）。復号化部18は、取得した復号鍵を用いて、取得したデータAを復号する（S6）。復号化部18は、復号したデータを、一時的にRAMなどに保存する。

[0043] データ生成部14は、ユーザBの操作に従い、データAに基づくユーザBを生成する（S7）。利用権限生成部15は、ユーザBの操作に従い、S5で取得した利用権限情報に基づいて、S7で生成されたデータBの利用権限を生成し、設定する（S8）。詳しくは、利用権限生成部15は、新たにデータBに生成する利用権限に、データAの利用権限を含めて、データBの利用権限を設定する。

[0044] 続いて、暗号化部19は、S7で生成されたデータBを暗号化する（S9）。記憶部16は、暗号化したデータBをデータ記憶部21に記憶し、S8で設定した利用権限に係る利用権限情報を利用権限記憶部23に記憶し、暗

号化したデータ B の復号鍵を鍵記憶部 22 に記憶する (S10)。そして、削除部 20 は、S6 で復号し、一時的に記憶したデータ A を削除する (S11)。復号したデータ A を装置内に残さないようにすることで、データ A の保護を行うことができる。

[0045] なお、図 3 に示す動作は一例であり、データ管理装置 1 の動作は適宜変更可能である。例えば、S11 における、復号したデータの削除の処理は、S9 のデータの暗号化の処理の直後に行われてもよい。また、S7 のデータの生成処理と、S8 の利用権限を設定する処理の順序は逆であってもよい。さらに、データ生成部 14 は、S7 でのデータ B の生成時にプログラム環境を実行するようにしてもよい。

[0046] 以上のように本実施形態によれば、利用権限が設定された第 1 データを利用して、第 2 データを生成する場合において、第 2 データの利用権限に、第 1 データの利用権限を承継することができる。これにより、新たに生成する第 2 データのみならず、第 2 データの生成に利用される第 1 データも保護することができる。

[0047] 本発明の実施形態におけるプログラムは、コンピュータに、図 3 に示す各ステップを実行させるプログラムであれば良い。このプログラムをコンピュータにインストールし、実行することによって、本実施形態におけるデータ管理装置とデータ管理方法とを実現することができる。この場合、コンピュータのプロセッサは、受付部 11 と、判定部 12 と、取得部 13 と、データ生成部 14 と、利用権限生成部 15 と、記憶部 16 と、認証部 17 と、復号化部 18 と、暗号化部 19 と、削除部 20 と、として機能し、処理を行なう。

[0048] また、本実施形態におけるプログラムは、複数のコンピュータによって構築されたコンピュータシステムによって実行されても良い。この場合は、例えば、各コンピュータが、それぞれ、受付部 11 と、判定部 12 と、取得部 13 と、データ生成部 14 と、利用権限生成部 15 と、記憶部 16 と、認証部 17 と、復号化部 18 と、暗号化部 19 と、削除部 20 と、のいずれかと

して機能しても良い。

[0049] (実施形態2)

実施形態1では、データAを生成するユーザと、そのデータAを利用してデータBを生成するユーザとは、同じデータ管理装置を利用している。これに対し、本実施形態では、データを提供するユーザと、データを利用する（提供される）ユーザとは、異なる組織に属し、異なるデータ管理装置を利用している点で、実施形態1と相違する。以下では、異なる組織間でデータを利用するデータ管理システムについて説明する。組織とは、例えば、会社、会社内の部署などである。まず、図4を参照して、本実施形態のデータの利用について説明する。図4は、本実施形態のデータの利用を説明するための図である。

[0050] 本実施形態では、ユーザAは組織Aに属し、ユーザBは組織Bに属しているものとする。ユーザAは、組織A内において、データ管理装置1Aを用いてデジタルコンテンツである第1データ（以下、データAという）を生成する。データAには、利用権限Xが設定されている。利用権限Xは、例えば、データAにアクセス可能なユーザである。

[0051] データAの利用権限があるユーザBは、データ管理装置1Bからデータ管理装置1Aにアクセスして、データAを取得する。そして、ユーザBは、データ管理装置1Bを用いて、データAに基づいて第2データ（以下、データBという）を生成する。データBは、データAの複製であってもよいし、データAを編集したものであってもよい。本実施形態では、ユーザBがデータBを生成した場合において、データ管理装置1Bは、データBに生成する利用権限Yに、データAに設定された利用権限Xを含めた、データBの利用権限Y（X）を生成する。つまり、データAの利用権限が、データBの利用権限に引き継がれるようになっている。

[0052] 図5は、データ管理システムの具体的な構成を示すブロック図である。データ管理システムは、データ管理装置1Aと、データ管理装置1Bとを備えていて、互いにデータ通信可能となっている。データ管理装置1Aと、デー

タ管理装置 1 B とは、同じ構成であるため、図 5 におけるデータ管理装置 1 A の構成は省略している。

[0053] データ管理装置 1 A、1 B は、実施形態 1 の構成に加え、送信部 2 4 を備えている。なお、実施形態 1 と同様の構成については、同じ符号を付して、その詳細な説明は省略する。

[0054] データ記憶部 2 1 は、ユーザが生成し、暗号化されたデータを記憶する記憶装置である。鍵記憶部 2 2 は、暗号化されたデータを復号する際に用いられる復号鍵を記憶する記憶装置である。利用権限記憶部 2 3 は、生成されたデータに設定された利用権限に係る利用権限情報を記憶する記憶装置である。

[0055] 以下の説明では、図 4 で説明したように、データ管理装置 1 A のデータ記憶部 2 1 に、データ A が記憶され、そのデータ A を復号する復号鍵がデータ管理装置 1 A の鍵記憶部 2 2 に記憶され、データ A に設定された利用権限に係る利用権限情報が、データ管理装置 1 A の利用権限記憶部 2 3 に記憶されているものとする。

[0056] 受付部 1 1 は、データ記憶部 2 1 に記憶されたデータへのアクセス要求を受け付ける。本実施形態では、データ管理装置 1 A に記憶されたデータ A を利用して、ユーザ B がデータ管理装置 1 B でデータ B を生成する場合、データ管理装置 1 B の受付部 1 1 は、ユーザ B からデータ A へのアクセス要求を受け付けると、データ管理装置 1 A の受付部 1 1 に対してアクセス要求を行う。

[0057] 認証部 1 7 は、データを生成するユーザを認証する。データ生成時、ユーザは、データ管理装置 1 へのログイン操作を行う。認証部 1 7 は、このときのログイン認証を行う。また、本実施形態の認証部 1 7 は、受付部 1 1 が他のデータ管理装置からアクセス要求を受けた場合に、他のデータ管理装置に対してそのユーザの認証を行う。本実施形態では、データ管理装置 1 A の受付部 1 1 がデータ管理装置 1 B の受付部 1 1 からデータ A へのアクセス要求を受け付けた場合、データ管理装置 1 A の認証部 1 7 は、データ管理装置 1

Bに対して、ユーザBがデータ管理装置1Bのユーザであるかの認証を行う。

- [0058] 判定部12は、受付部11が受け付けたアクセス要求をするユーザに、アクセスするデータの利用権限があるかを判定する。本実施形態では、データ管理装置1Aの判定部12は、データ管理装置1BからデータAへのアクセス要求を受け付けた場合、データAに対応付けられた利用権限情報を、データ管理装置1Aの利用権限記憶部23から取得する。データ管理装置1Aの判定部12は、その利用権限にユーザBが含まれているかを判定し、含まれている場合には、ユーザBにデータAの利用権限があると判定する。
- [0059] 取得部13は、判定部12がユーザにアクセスするデータの利用権限があると判定すると、そのデータをデータ記憶部21から取得する。また、取得部13は、そのデータに対応付けられた利用権限情報を利用権限記憶部23から取得する。さらに、取得部13は、データを復号するための復号鍵を鍵記憶部22から取得する。本実施形態では、データ管理装置1Aの判定部12が、ユーザBにデータAの利用権限があると判定すると、データ管理装置1Aの取得部13は、データAをデータ記憶部21から取得し、データAの利用権限に係る利用権限情報を利用権限記憶部23から取得し、データAの復号鍵を鍵記憶部22から取得する。
- [0060] 送信部24は、取得部13が取得した各種データを、アクセス要求をしてきた、他のデータ管理装置へ送信する。本実施形態では、データ管理装置1Aの送信部24は、データ管理装置1Bに対して、データA、データAを復号する復号鍵、及び、データAに設定された利用権限に係る利用権限情報を、送信する。
- [0061] また、本実施形態の取得部13は、他のデータ管理装置の送信部24が送信したデータを取得する。本実施形態では、データ管理装置1Bの取得部13は、データ管理装置1Aの送信部24が送信した、データA、データAを復号する復号鍵、及び、データAに設定された利用権限に係る利用権限情報を取得する。

- [0062] 復号化部 18 は、他のデータ管理装置の送信部 24 が送信し、取得部 13 が取得した復号鍵を用いて、他のデータ管理装置の送信部 24 が送信し、取得部 13 が取得したデータを復号する。
- [0063] データ生成部 14 はデータを生成する。データ生成部 14 は、予めユーザが生成した、保護されたデータを利用できるプログラム環境を実行する。そして、データ生成部 14 は、実行した環境下において、ユーザの操作に従い、データを生成する。本実施形態では、データ生成部 14 は、ユーザ B が生成し、実行したプログラム環境下で、ユーザ B の操作に従い、復号化部 18 が復号したデータ A に基づいて、データ B を生成する。
- [0064] 暗号化部 19 は、生成されたデータを暗号化する。
- [0065] 利用権限生成部 15 は、ユーザの操作に従い、データ生成部 14 によって生成されたデータの利用権限を生成する。本実施形態では、利用権限生成部 15 は、取得部 13 が取得したデータ A の利用権限情報に基づいて、生成するデータ B の利用権限に、利用されたデータ A に設定された利用権限を含める。これにより、利用されるデータ A に設定された利用権限が、新たに生成されたデータ B の利用権限に承継されるようになる。その結果、新たに生成されたデータ B がさらに別のユーザ C に利用される場合、そのユーザ C が、データ B の生成に利用したデータ A の利用権限を有していないと、ユーザ C によるデータ B へのアクセスが拒否されるようになり、データ A をユーザ C から保護することができる。
- [0066] 記憶部 16 は、生成し暗号化されたデータをデータ記憶部 21 に記憶する。また、記憶部 16 は、生成された利用権限に係る利用権限情報を、利用権限記憶部 23 に記憶する。また、記憶部 16 は、復号鍵を鍵記憶部 22 に記憶する。
- [0067] 削除部 20 は、復号されたデータを削除する。
- [0068] 次に、本実施形態におけるデータ管理装置 1A、1B の動作について図 6～図 8 を用いて説明する。図 6～図 8 は、データ管理装置 1A、1B の動作を示すフロー図である。以下の説明においては、適宜図 4～図 5 を参酌する

。また、本実施形態では、データ管理装置 1 A、1 B を動作させることによって、データ管理方法が実施される。よって、本実施形態におけるデータ管理方法の説明は、以下のデータ管理装置 1 A、1 B の動作説明に代える。また、以下の説明では、図 4 で説明したように、データ管理装置 1 A でユーザ A がデータ A を生成し、データ管理装置 1 B でユーザ B がデータ B を生成するものとして説明する。

[0069] 図 6 は、データ管理装置 1 A において、データ A を登録する際のフロー図である。ユーザ A がデータ管理装置 1 A へのログイン操作を行うと、認証部 1 7 はユーザ A の認証判定を行う (S 2 1)。認証に失敗した場合 (S 2 1 : N O)、データ管理装置 1 A は本処理を終了する。認証に成功すると (S 2 1 : Y E S)、データ生成部 1 4 は、ユーザ A が生成した、保護されたデータを利用できるプログラム環境を実行し (S 2 2)、その環境下において、ユーザ A の操作に従い、データ A を生成する (S 2 3)。利用権限生成部 1 5 は、ユーザ A の操作に従い、S 2 3 で生成されたデータ A の利用権限を生成し、設定する (S 2 4)。続いて、暗号化部 1 9 は、S 2 3 で生成されたデータ A を暗号化する (S 2 5)。記憶部 1 6 は、暗号化したデータ A をデータ記憶部 2 1 に記憶し、S 2 4 で設定した利用権限に係る利用権限情報を利用権限記憶部 2 3 に記憶し、S 2 5 で暗号化したデータ A の復号鍵を鍵記憶部 2 2 に記憶する (S 2 6)。

[0070] 図 7 及び図 8 は、データ管理装置 1 B において、データ B を登録する際のフロー図である。図 7 及び図 8 は、データ管理装置 1 A、1 B それぞれでの動作を示すフロー図である。

[0071] ユーザ B がデータ管理装置 1 B へのログイン操作を行うと、データ管理装置 1 B の認証部 1 7 はユーザ B の認証判定を行う (S 3 1)。認証に失敗した場合 (S 3 1 : N O)、データ管理装置 1 B は本処理を終了する。認証に成功すると (S 3 1 : Y E S)、データ生成部 1 4 は、予めユーザが生成した、保護されたデータを利用できるプログラム環境を実行する (S 3 2)。以下のデータ管理装置 1 B での処理は、このプログラム環境下で実行される

。データ管理装置 1 B の受付部 1 1 は、ユーザ B によりデータ A へのアクセス要求を受け付け、さらに、データ管理装置 1 A の受付部 1 1 に対してアクセス要求を行う（S 3 3）。

[0072] データ管理装置 1 A の受付部 1 1 がアクセス要求を受け付けると（S 3 4）、データ管理装置 1 A の認証部 1 7 は、データ管理装置 1 B に対して、ユーザ B の認証を行う（S 3 5）。例えば、データ管理装置 1 A の認証部 1 7 は、組織 B 内のディレクトリサーバと通信してユーザ B を認証する。認証が完了すると、データ管理装置 1 A の判定部 1 2 は、ユーザ B にデータ A の利用権限があるか否かを判定する（S 3 6）。このとき、ユーザ B にデータ A の利用権限がない場合には、データ管理装置 1 A の判定部 1 2 は、データ管理装置 1 B へ通知する。

[0073] ユーザ B にデータ A の利用権限があると、データ管理装置 1 A の取得部 1 3 は、暗号化されたデータ A をデータ記憶部 2 1 から取得し、そのデータ A を復号する復号鍵を鍵記憶部 2 2 から取得し、データ A に設定された利用権限に係る利用権限情報を利用権限記憶部 2 3 から取得する（S 3 7）。そして、データ管理装置 1 A の送信部 2 4 は、暗号化されたデータ A、そのデータ A に設定された利用権限に係る利用権限情報、及び、復号鍵を、データ管理装置 1 B へ送信する（S 3 8）。

[0074] データ管理装置 1 B の取得部 1 3 は、送信された暗号化されたデータ A、そのデータ A に設定された利用権限に係る利用権限情報、及び、復号鍵を、取得する（S 3 9）。データ管理装置 1 B の復号化部 1 8 は、取得した復号鍵を用いて、取得したデータ A を復号する（S 4 0）。復号化部 1 8 は、復号したデータを、一時的に RAM などに保存する。

[0075] データ管理装置 1 B のデータ生成部 1 4 は、ユーザ B の操作に従い、データ A に基づくユーザ B を生成する（S 4 1）。データ管理装置 1 B の利用権限生成部 1 5 は、ユーザ B の操作に従い、S 3 9 で取得した利用権限情報に基づいて、S 4 1 で生成されたデータ B の利用権限を生成し、設定する（S 4 2）。続いて、データ管理装置 1 B の暗号化部 1 9 は、S 3 0 で生成され

たデータ B を暗号化する（S 4 3）。データ管理装置 1 B の記憶部 1 6 は、暗号化したデータ B をデータ記憶部 2 1 に記憶し、S 4 2 で設定した利用権限に係る利用権限情報を利用権限記憶部 2 3 に記憶し、暗号化したデータ B の復号鍵を鍵記憶部 2 2 に記憶する（S 4 4）。そして、削除部 2 0 は、S 4 0 で復号し、一時的に記憶したデータ A を削除する（S 4 5）。復号したデータ A を装置内に残さないようにすることで、データ A の保護を行うことができる。

[0076] なお、図 6 ～ 8 に示す動作は一例であり、データ管理装置 1 の動作は適宜変更可能である。例えば、S 4 3 の暗号化処理の後 S 4 4 の記憶処理を行わず、データ管理装置 1 A など他のデータ管理装置のデータ生成部 1 4 に転送する S 3 8 データ送信の処理に遷移してもよい。また、S 4 5 における、復号したデータの削除の処理は、S 4 3 のデータの暗号化の処理の直後に行われてもよい。また、S 4 1 のデータの生成処理と、S 4 2 の利用権限を設定する処理の順序は逆であってもよい。また、実施形態 1、2 は適宜組み合わせてもよい。

[0077] 以上のように本実施形態によれば、利用権限が設定された第 1 データを利用して、第 2 データを生成する場合において、第 2 データの利用権限に、第 1 データの利用権限を承継することができる。これにより、新たに生成する第 2 データのみならず、第 2 データの生成に利用される第 1 データも保護することができる。

[0078] 本発明の実施形態におけるプログラムは、コンピュータに、図 6 ～ 図 8 に示す各ステップを実行させるプログラムであれば良い。このプログラムをコンピュータにインストールし、実行することによって、本実施形態におけるデータ管理装置とデータ管理方法とを実現することができる。この場合、コンピュータのプロセッサは、受付部 1 1 と、判定部 1 2 と、取得部 1 3 と、データ生成部 1 4 と、利用権限生成部 1 5 と、記憶部 1 6 と、認証部 1 7 と、復号化部 1 8 と、暗号化部 1 9 と、削除部 2 0 と、送信部 2 4 と、として機能し、処理を行なう。

[0079] また、本実施形態におけるプログラムは、複数のコンピュータによって構築されたコンピュータシステムによって実行されても良い。この場合は、例えば、各コンピュータが、それぞれ、受付部 11 と、判定部 12 と、取得部 13 と、データ生成部 14 と、利用権限生成部 15 と、記憶部 16 と、認証部 17 と、復号化部 18 と、暗号化部 19 と、削除部 20 と、送信部 24 と、のいずれかとして機能しても良い。

[0080] ここで、実施形態 1～2 におけるプログラムを実行することによって、データ管理装置を実現するコンピュータについて図 9 を用いて説明する。図 9 は、本発明の実施形態 1、2 におけるデータ管理装置を実現するコンピュータの一例を示すブロック図である。

[0081] 図 9 に示すように、コンピュータ 110 は、CPU 111 と、メインメモリ 112 と、記憶装置 113 と、入力インターフェイス 114 と、表示コントローラ 115 と、データリーダ／ライタ 116 と、通信インターフェイス 117 とを備える。これらの各部は、バス 121 を介して、互いにデータ通信可能に接続される。なお、コンピュータ 110 は、CPU 111 に加えて、又は CPU 111 に代えて、GPU (Graphics Processing Unit)、又は FPGA (Field-Programmable Gate Array) を備えていても良い。

[0082] CPU 111 は、記憶装置 113 に格納された、本実施形態におけるプログラム（コード）をメインメモリ 112 に展開し、これらを所定順序で実行することにより、各種の演算を実施する。メインメモリ 112 は、典型的には、DRAM (Dynamic Random Access Memory) 等の揮発性の記憶装置である。また、本実施形態におけるプログラムは、コンピュータ読み取り可能な記録媒体 120 に格納された状態で提供される。なお、本実施形態におけるプログラムは、通信インターフェイス 117 を介して接続されたインターネット上で流通するものであっても良い。

[0083] また、記憶装置 113 の具体例としては、ハードディスクドライブの他、フラッシュメモリ等の半導体記憶装置が挙げられる。入力インターフェイス 114 は、CPU 111 と、キーボード及びマウスといった入力機器 118

との間のデータ伝送を仲介する。表示コントローラ 115 は、ディスプレイ装置 119 と接続され、ディスプレイ装置 119 での表示を制御する。

[0084] データリーダ／ライタ 116 は、CPU 111 と記録媒体 120 との間のデータ伝送を仲介し、記録媒体 120 からのプログラムの読み出し、及びコンピュータ 110 における処理結果の記録媒体 120 への書き込みを実行する。通信インターフェイス 117 は、CPU 111 と、他のコンピュータとの間のデータ伝送を仲介する。

[0085] また、記録媒体 120 の具体例としては、CF (Compact Flash (登録商標)) 及びSD (Secure Digital) 等の汎用的な半導体記憶デバイス、フレキシブルディスク (Flexible Disk) 等の磁気記録媒体、又はCD-ROM (Compact Disk Read Only Memory) などの光学記録媒体が挙げられる。

[0086] なお、本実施形態におけるデータ管理装置は、プログラムがインストールされたコンピュータではなく、各部に対応したハードウェアを用いることによっても実現可能である。更に、データ管理装置は、一部がプログラムで実現され、残りの部分がハードウェアで実現されていてもよい。

[0087] 上述した実施形態の一部又は全部は、以下に記載する(付記1)～(付記16)によって表現することができるが、以下の記載に限定されるものではない。

[0088] (付記1)

利用者による第1データへのアクセス要求を受け付ける受付部と、
前記利用者が、前記第1データが利用可能であるかを判定する判定部と、
前記利用者が、前記第1データが利用可能である場合、前記第1データ、
及び、前記第1データの利用権限に係る利用権限情報を取得する取得部と、
取得された前記第1データを利用して第2データを生成するデータ生成部と、

前記第1データの利用権限を含めた前記第2データの利用権限を生成する
利用権限生成部と、

前記第2データと、前記第2データの利用権限に係る利用権限情報とを対

応付けて記憶する記憶部と、
を備える、データ管理装置。

[0089] (付記 2)

付記 1 に記載のデータ管理装置であって、
前記第 1 データは暗号化されており、
取得された前記第 1 データを復号する復号化部、
を備え、
前記データ生成部は、復号された前記第 1 データを利用して前記第 2 データを生成し、
前記第 2 データを暗号化する暗号化部、
をさらに備え、
前記記憶部は、暗号化された前記第 2 データを記憶する、
データ管理装置。

[0090] (付記 3)

付記 2 に記載のデータ管理装置であって、
前記第 2 データが生成されると、復号された前記第 1 データを削除する削除部、
を備える、データ管理装置。

[0091] (付記 4)

付記 1 から付記 3 のいずれか一つに記載のデータ管理装置であって、
前記データ生成部は、
予め生成されたプログラム環境を実行し、前記プログラム環境下で前記第 2 データを生成する、
データ管理装置。

[0092] (付記 5)

利用者による第 1 データへのアクセス要求を受け付ける受付部と、
前記利用者が、前記第 1 データが利用可能であることを判定する判定部と、
前記利用者が、前記第 1 データが利用可能である場合、前記第 1 データ、

及び、前記第 1 データの利用権限に係る利用権限情報を送信する送信部と、
送信された前記第 1 データ、及び、前記利用権限情報を取得する取得部と、
、
取得された前記第 1 データを利用して第 2 データを生成するデータ生成部
と、
前記第 1 データの利用権限を含めた前記第 2 データの利用権限を生成する
利用権限生成部と、
前記第 2 データと、前記第 2 データの利用権限に係る利用権限情報とを対
応付けて記憶する記憶部と、
を備える、データ管理システム。

[0093] (付記 6)

付記 5 に記載のデータ管理システムであって、
前記第 1 データは暗号化されており、
取得された前記第 1 データを復号する復号化部、
を備え、
前記データ生成部は、復号された前記第 1 データを利用して前記第 2 デー
タを生成し、
復号された前記第 1 データを利用して生成された第 2 データを暗号化する
暗号化部、
をさらに備え、
前記記憶部は、暗号化された前記第 2 データを記憶する、
データ管理システム。

[0094] (付記 7)

付記 6 に記載のデータ管理システムであって、
前記第 2 データが生成されると、復号された前記第 1 データを削除する削
除部、
を備える、データ管理システム。

[0095] (付記 8)

付記 5 から付記 7 のいずれか一つに記載のデータ管理システムであって、
前記データ生成部は、
予め生成されたプログラム環境を実行し、前記プログラム環境下で前記第
2 データを生成する、
データ管理システム。

[0096] (付記 9)

利用者による第 1 データへのアクセス要求を受け付けるステップと、
前記利用者が、前記第 1 データが利用可能であることを判定するステップと
、
前記利用者が、前記第 1 データが利用可能である場合、前記第 1 データ、
及び、前記第 1 データの利用権限に係る利用権限情報を送信するステップと
、
送信された前記第 1 データ、及び、前記利用権限情報を取得するステップ
と、
取得された前記第 1 データを利用して第 2 データを生成するステップと、
前記第 1 データの利用権限を含めた前記第 2 データの利用権限を生成する
ステップと、
前記第 2 データと、前記第 2 データの利用権限に係る利用権限情報とを対
応付けて記憶するステップと、
を備える、データ管理方法。

[0097] (付記 10)

付記 9 に記載のデータ管理方法であって、
前記第 1 データは暗号化されており、
取得された前記第 1 データを復号するステップ、
を備え、
前記第 2 データを生成するステップでは、復号された前記第 1 データを利
用して前記第 2 データを生成し、
復号された前記第 1 データを利用して生成された第 2 データを暗号化する

ステップ、

をさらに備え、

前記第2データを記憶するステップでは、暗号化された前記第2データを記憶する、

データ管理方法。

[0098] (付記11)

付記10に記載のデータ管理方法であって、

前記第2データが生成されると、復号された前記第1データを削除するステップ、

を備える、データ管理方法。

[0099] (付記12)

付記9から付記11のいずれか一つに記載のデータ管理方法であって、

前記第2データを生成するステップでは、

予め生成されたプログラム環境を実行し、前記プログラム環境下で前記第2データを生成する、

データ管理方法。

[0100] (付記13)

コンピュータに、

利用者による第1データへのアクセス要求を受け付けるステップと、

前記利用者が、前記第1データが利用可能であることを判定するステップと、

前記利用者が、前記第1データが利用可能である場合、前記第1データ、及び、前記第1データの利用権限に係る利用権限情報を取得するステップと、

取得された前記第1データを利用して第2データを生成するステップと、

前記第1データの利用権限を含めた前記第2データの利用権限を生成するステップと、

前記第2データと、前記第2データの利用権限に係る利用権限情報とを対

応付けて記憶するステップと、

を実行させる命令を含むプログラムを記録した、コンピュータ読み取り可能な記録媒体。

[0101] (付記 1 4)

付記 1 3 に記載のコンピュータ読み取り可能な記録媒体であって、

前記第 1 データは暗号化されており、

前記プログラムは、前記コンピュータに、

取得された前記第 1 データを復号するステップ、

を実行させる命令を含み、

前記第 2 データを生成するステップでは、復号された前記第 1 データを利用して前記第 2 データを生成し、

前記プログラムは、前記コンピュータに、

前記第 2 データを暗号化するステップ、

を実行させる命令をさらに含み、

前記第 2 データを記憶するステップでは、暗号化された前記第 2 データを記憶する、

コンピュータ読み取り可能な記録媒体。

[0102] (付記 1 5)

付記 1 4 に記載のコンピュータ読み取り可能な記録媒体であって、

前記プログラムは、

前記コンピュータに、

前記第 2 データが生成されると、復号された前記第 1 データを削除するステップ、

を実行させる命令を含む、コンピュータ読み取り可能な記録媒体。

[0103] (付記 1 6)

付記 1 3 から付記 1 5 のいずれか一つに記載のコンピュータ読み取り可能な記録媒体であって、

前記第 2 データを生成するステップでは、

予め生成されたプログラム環境を実行し、前記プログラム環境下で前記第2データを生成する、

コンピュータ読み取り可能な記録媒体。

[0104] 以上、実施の形態を参照して本開示を説明したが、本開示は上記実施の形態に限定されるものではない。本開示の構成や詳細には、本開示の範囲内で当業者が理解し得る様々な変更をすることができる。

[0105] この出願は、2021年3月4日に提出された日本出願特願2021-034757を基礎とする優先権を主張し、その開示の全てをここに取り込む。

産業上の利用可能性

[0106] 本発明は、利用権限が設定された第1データを利用して第2データを生成する場合において、第1データの利用権限を引き継ぎ、第1データを保護する際に有用である。

符号の説明

[0107] 1、1A、1B データ管理装置

11 受付部

12 判定部

13 取得部

14 データ生成部

15 利用権限生成部

16 記憶部

17 認証部

18 復号化部

19 暗号化部

20 削除部

21 データ記憶部

22 鍵記憶部

23 利用権限記憶部

2 4 送信部

1 1 0 コンピュータ

1 1 1 C P U

1 1 2 メインメモリ

1 1 3 記憶装置

1 1 4 入力インターフェイス

1 1 5 表示コントローラ

1 1 6 データリーダ／ライタ

1 1 7 通信インターフェイス

1 1 8 入力機器

1 1 9 ディスプレイ装置

1 2 0 記録媒体

1 2 1 バス

請求の範囲

- [請求項1] 利用者による第1データへのアクセス要求を受け付ける受付手段と、
- 、
- 前記利用者が、前記第1データが利用可能であることを判定する判定手段と、
- 前記利用者が、前記第1データが利用可能である場合、前記第1データ、及び、前記第1データの利用権限に係る利用権限情報を取得する取得手段と、
- 取得された前記第1データを利用して第2データを生成するデータ生成手段と、
- 前記第1データの利用権限を含めた前記第2データの利用権限を生成する利用権限生成手段と、
- 前記第2データと、前記第2データの利用権限に係る利用権限情報とを対応付けて記憶する記憶手段と、
- を備える、データ管理装置。
- [請求項2] 請求項1に記載のデータ管理装置であって、
- 前記第1データは暗号化されており、
- 取得された前記第1データを復号する復号化手段、
- を備え、
- 前記データ生成手段は、復号された前記第1データを利用して前記第2データを生成し、
- 前記第2データを暗号化する暗号化手段、
- をさらに備え、
- 前記記憶手段は、暗号化された前記第2データを記憶する、データ管理装置。
- [請求項3] 請求項2に記載のデータ管理装置であって、
- 前記第2データが生成されると、復号された前記第1データを削除する削除手段、

を備える、データ管理装置。

[請求項4] 請求項1から請求項3のいずれか一つに記載のデータ管理装置であって、

前記データ生成手段は、

予め生成されたプログラム環境を実行し、前記プログラム環境下で前記第2データを生成する、

データ管理装置。

[請求項5] 利用者による第1データへのアクセス要求を受け付ける受付手段と、

前記利用者が、前記第1データが利用可能であることを判定する判定手段と、

前記利用者が、前記第1データが利用可能である場合、前記第1データ、及び、前記第1データの利用権限に係る利用権限情報を送信する送信手段と、

送信された前記第1データ、及び、前記利用権限情報を取得する取得手段と、

取得された前記第1データを利用して第2データを生成するデータ生成手段と、

前記第1データの利用権限を含めた前記第2データの利用権限を生成する利用権限生成手段と、

前記第2データと、前記第2データの利用権限に係る利用権限情報とを対応付けて記憶する記憶手段と、

を備える、データ管理システム。

[請求項6] 請求項5に記載のデータ管理システムであって、

前記第1データは暗号化されており、

取得された前記第1データを復号する復号化手段、

を備え、

前記データ生成手段は、復号された前記第1データを利用して前記

第2データを生成し、

復号された前記第1データを利用して生成された第2データを暗号化する暗号化手段、

をさらに備え、

前記記憶手段は、暗号化された前記第2データを記憶する、
データ管理システム。

[請求項7]

請求項6に記載のデータ管理システムであって、

前記第2データが生成されると、復号された前記第1データを削除する削除手段、

を備える、データ管理システム。

[請求項8]

請求項5から請求項7のいずれか一つに記載のデータ管理システムであって、

前記データ生成手段は、

予め生成されたプログラム環境を実行し、前記プログラム環境下で前記第2データを生成する、

データ管理システム。

[請求項9]

利用者による第1データへのアクセス要求を受け付け、

前記利用者が、前記第1データが利用可能であることを判定し

前記利用者が、前記第1データが利用可能である場合、前記第1データ、及び、前記第1データの利用権限に係る利用権限情報を送信し、

送信された前記第1データ、及び、前記利用権限情報を取得し

取得された前記第1データを利用して第2データを生成し、

前記第1データの利用権限を含めた前記第2データの利用権限を生成し、

前記第2データと、前記第2データの利用権限に係る利用権限情報とを対応付けて記憶する、

データ管理方法。

- [請求項10] 請求項9に記載のデータ管理方法であって、
前記第1データは暗号化されており、
取得された前記第1データを復号し、
前記第2データを生成する場合、復号された前記第1データを利用して前記第2データを生成し、
復号された前記第1データを利用して生成された第2データを暗号化し、
前記第2データを記憶する場合、暗号化された前記第2データを記憶する、
データ管理方法。
- [請求項11] 請求項10に記載のデータ管理方法であって、
前記第2データが生成されると、復号された前記第1データを削除する、
データ管理方法。
- [請求項12] 請求項9から請求項11のいずれか一つに記載のデータ管理方法であって、
前記第2データを生成する場合、
予め生成されたプログラム環境を実行し、前記プログラム環境下で前記第2データを生成する、
データ管理方法。
- [請求項13] コンピュータに、
利用者による第1データへのアクセス要求を受け付けさせ、
前記利用者が、前記第1データが利用可能であることを判定させ、
前記利用者が、前記第1データが利用可能である場合、前記第1データ、及び、前記第1データの利用権限に係る利用権限情報を取得させ、
取得された前記第1データを利用して第2データを生成させ、
前記第1データの利用権限を含めた前記第2データの利用権限を生

成させ、

前記第2データと、前記第2データの利用権限に係る利用権限情報とを対応付けて記憶させる、

命令を含むプログラムを記録したコンピュータ読み取り可能な記録媒体。

[請求項14]

請求項13に記載のプログラムであって、

前記第1データは暗号化されており、

前記プログラムは、

前記コンピュータに、

取得された前記第1データを復号させる、

命令を含み、

前記第2データを生成させ場合、復号された前記第1データを利用して前記第2データを生成させ、

前記プログラムは、前記コンピュータに、

前記第2データを暗号化させる、

命令をさらに含み、

前記第2データを記憶させる場合、暗号化された前記第2データを記憶させる、

コンピュータ読み取り可能な記録媒体。

[請求項15]

請求項14に記載のコンピュータ読み取り可能な記録媒体であって

、

前記プログラムは、

前記コンピュータに、

前記第2データが生成されると、復号された前記第1データを削除させる、

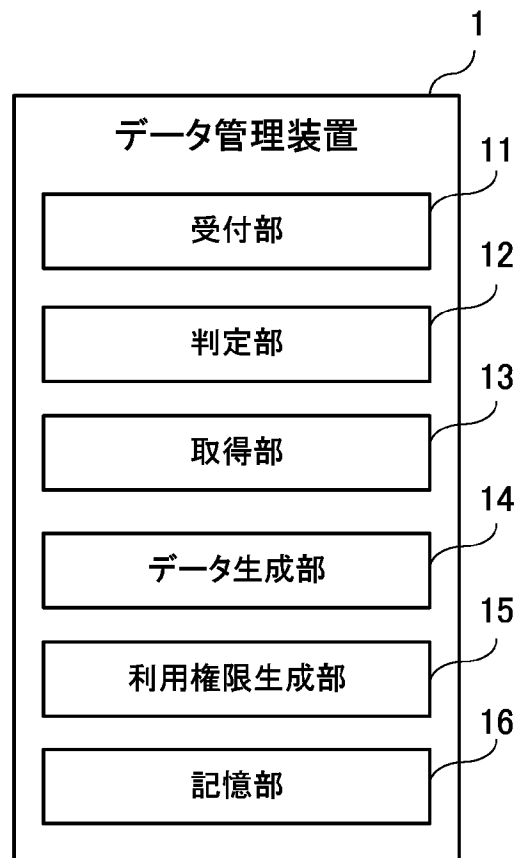
命令を含む、プログラムを記録したコンピュータ読み取り可能な記録媒体。

[請求項16]

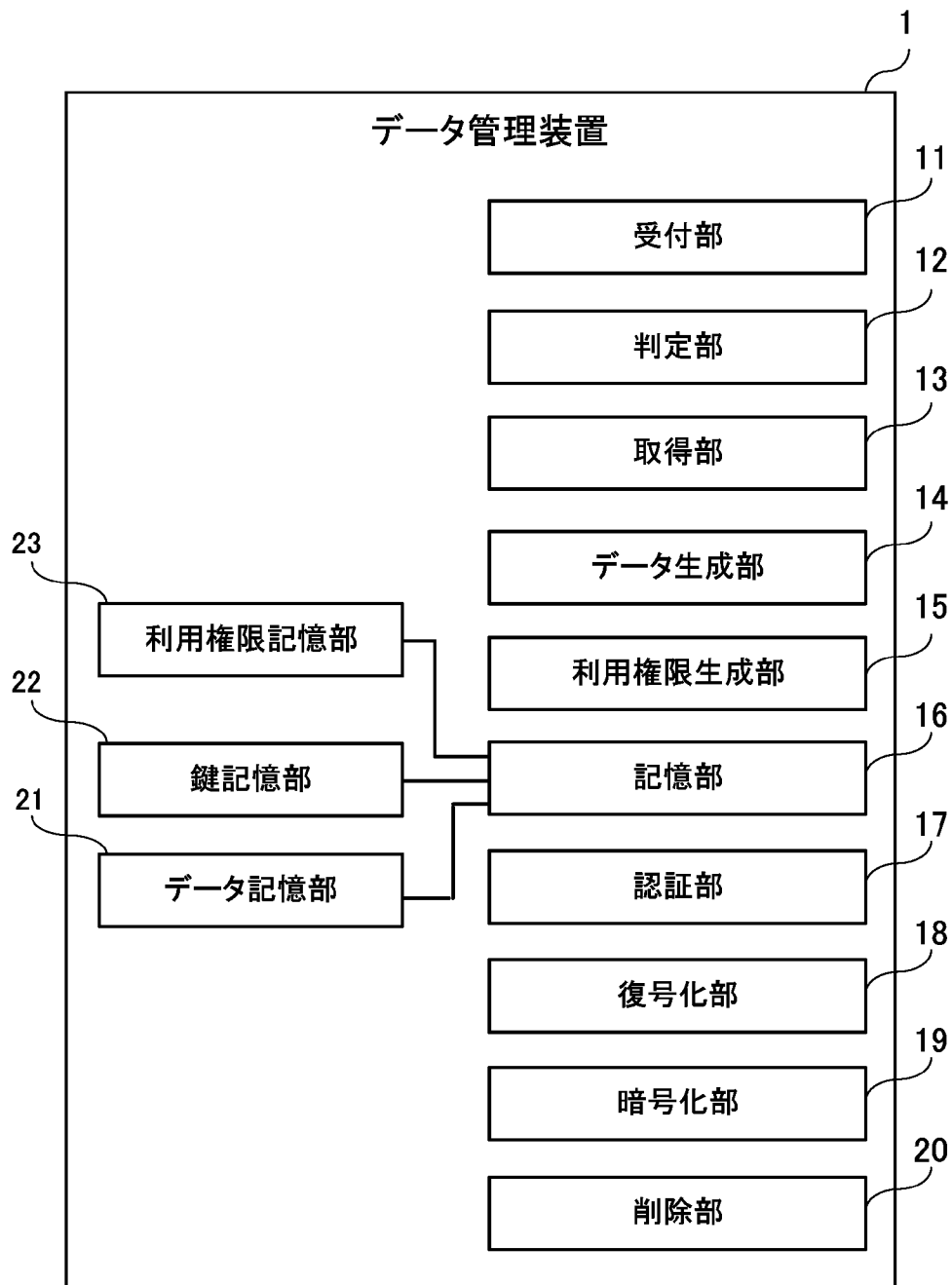
請求項13から請求項15のいずれか一つに記載のコンピュータ読

み取り可能な記録媒体であって、
前記第 2 データを生成させる場合、
予め生成されたプログラム環境を実行し、前記プログラム環境下で
前記第 2 データを生成させる、
コンピュータ読み取り可能な記録媒体。

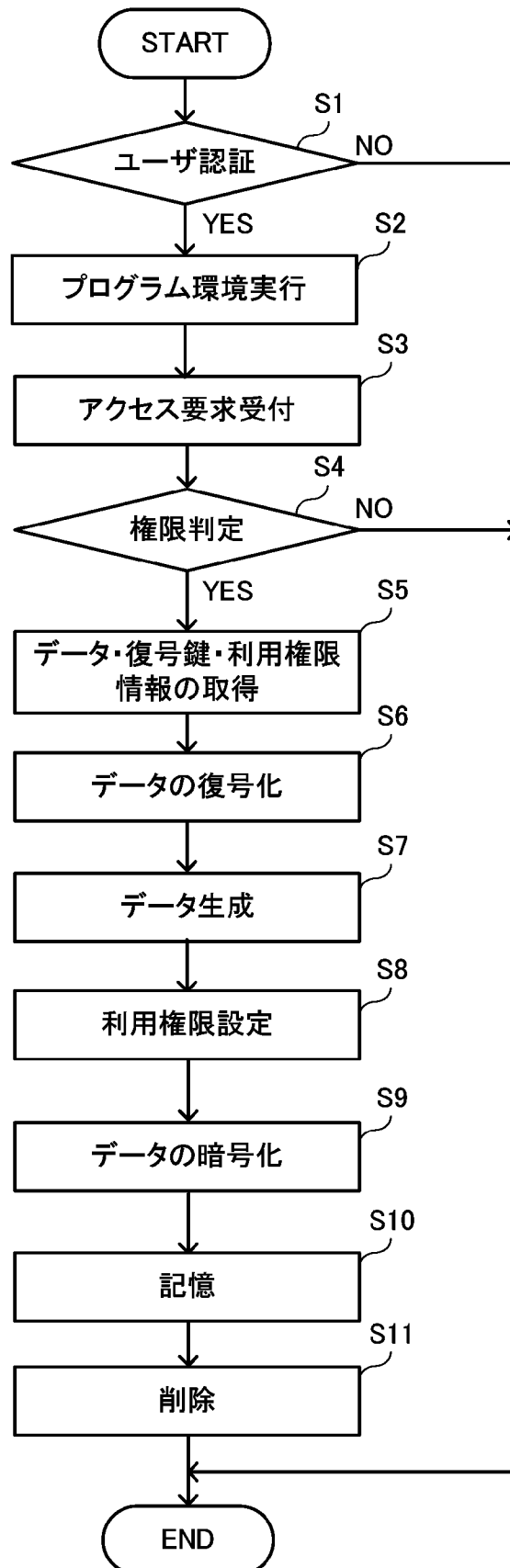
[図1]



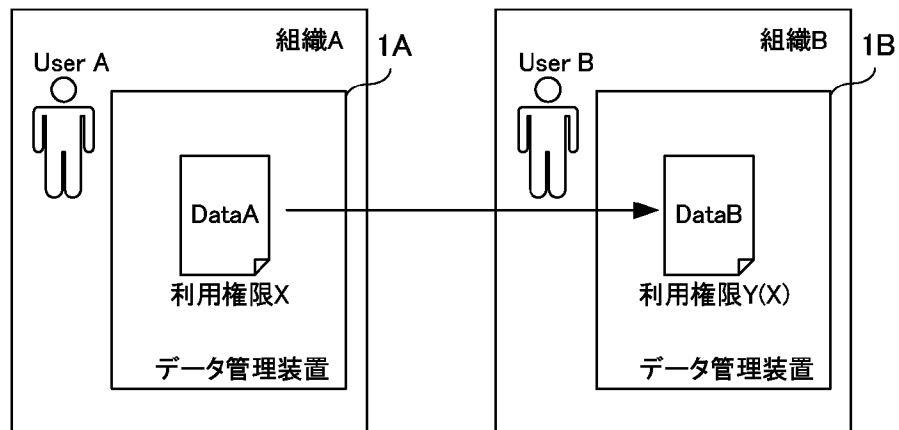
[図2]



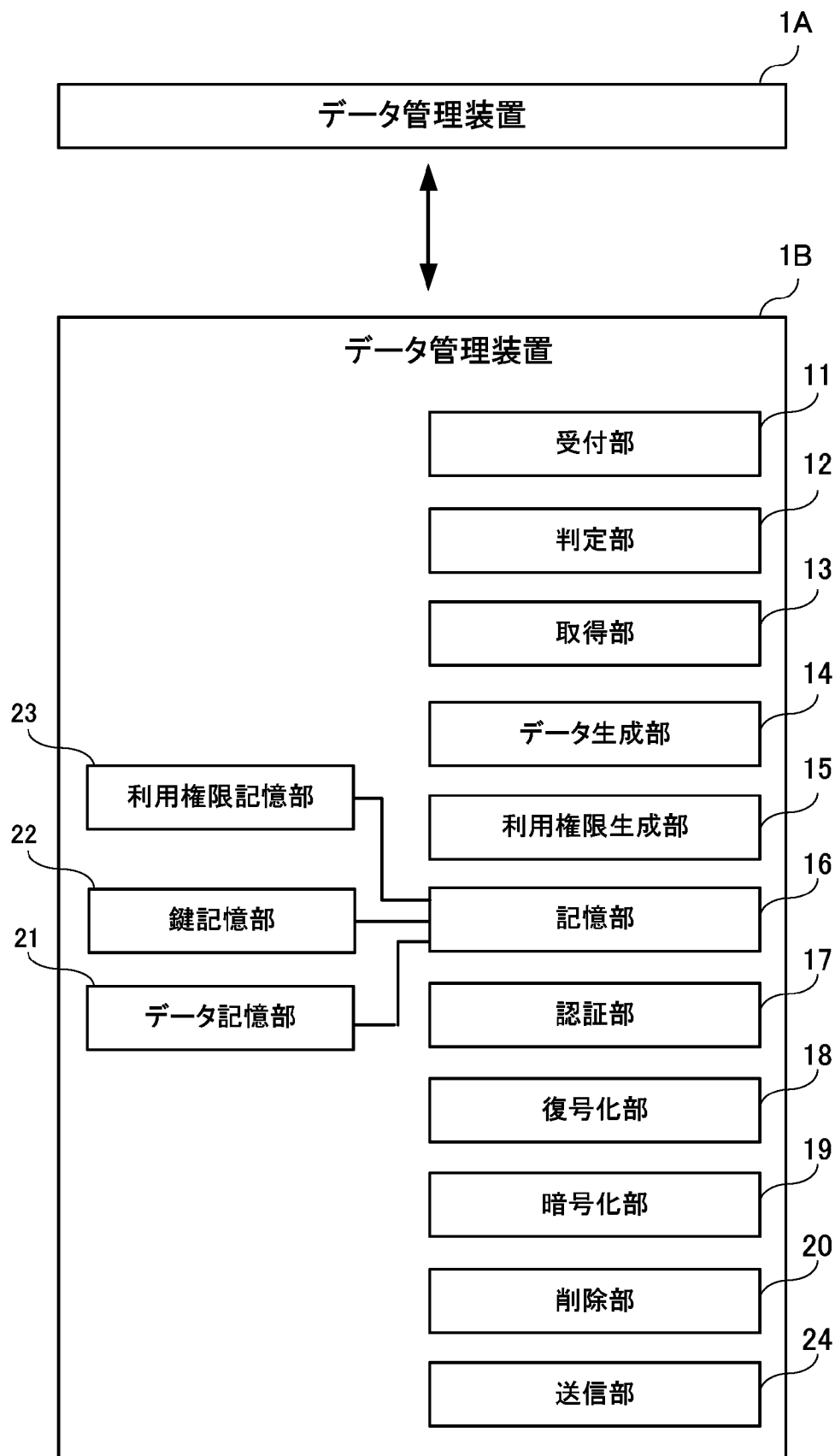
[図3]



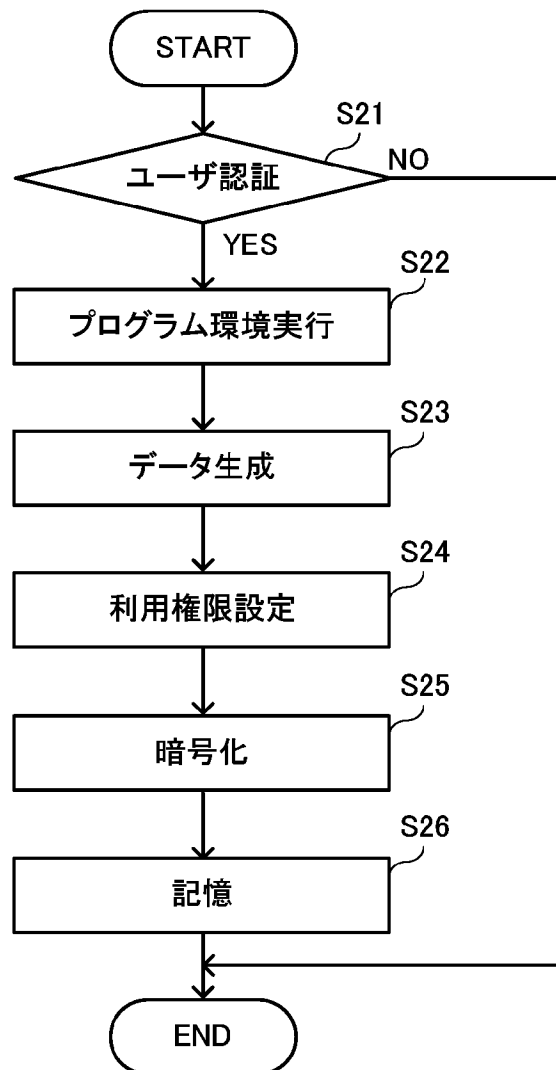
[図4]



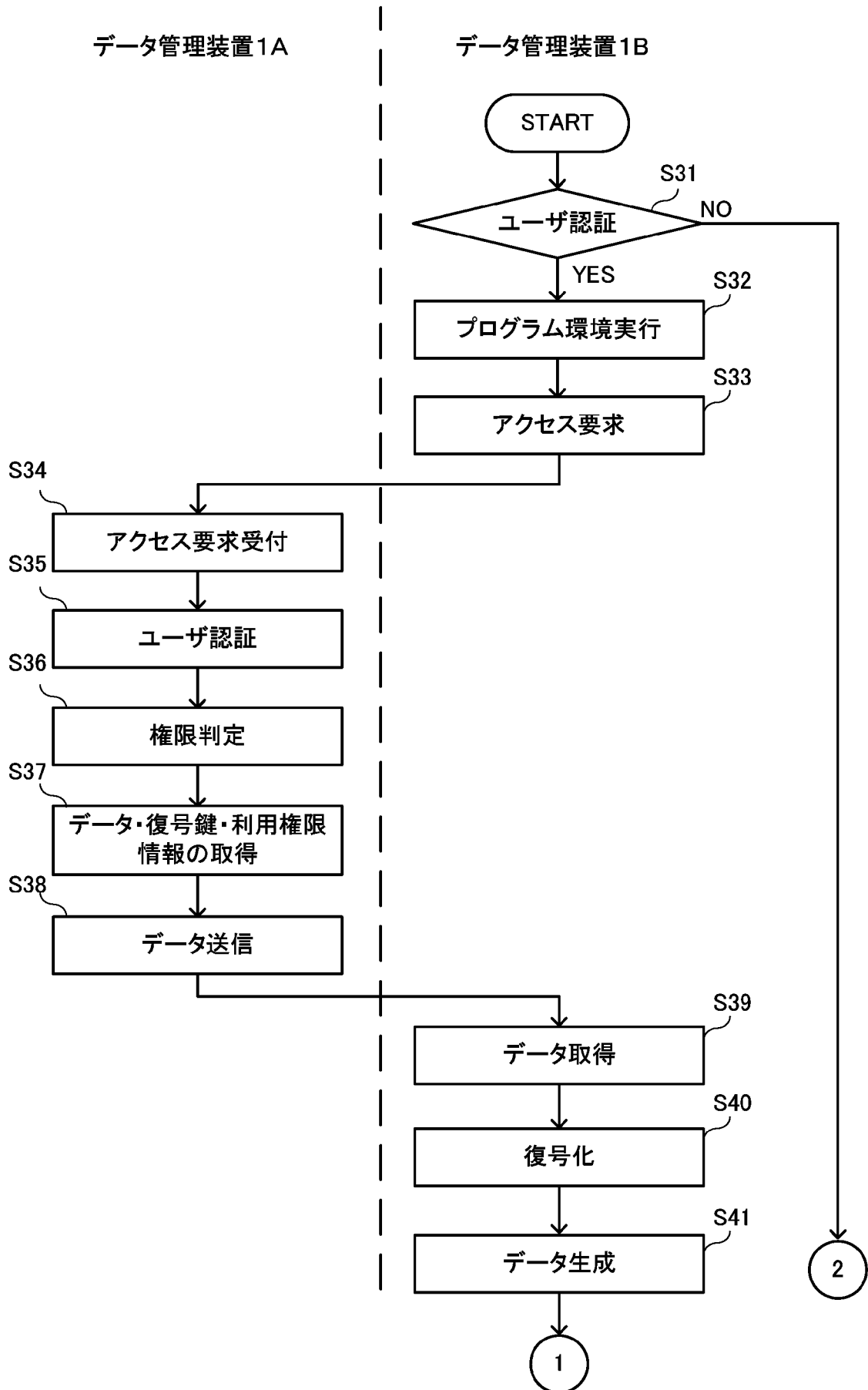
[図5]



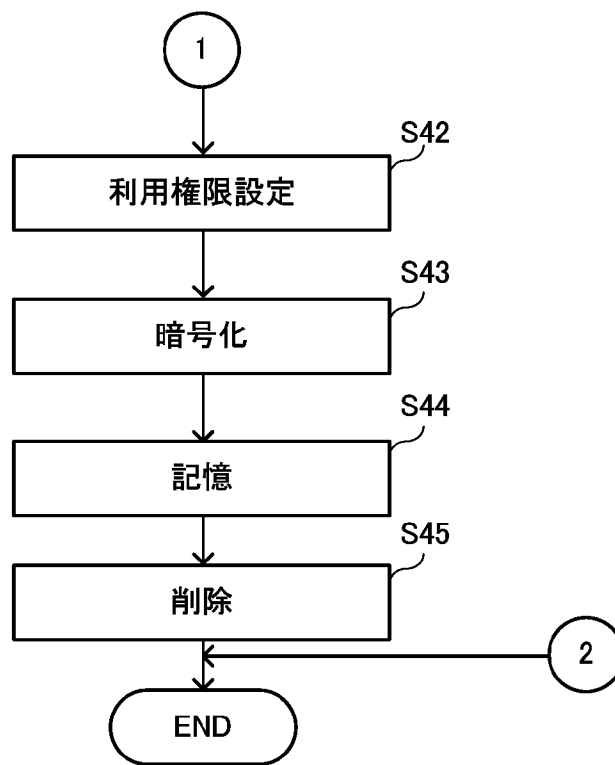
[図6]



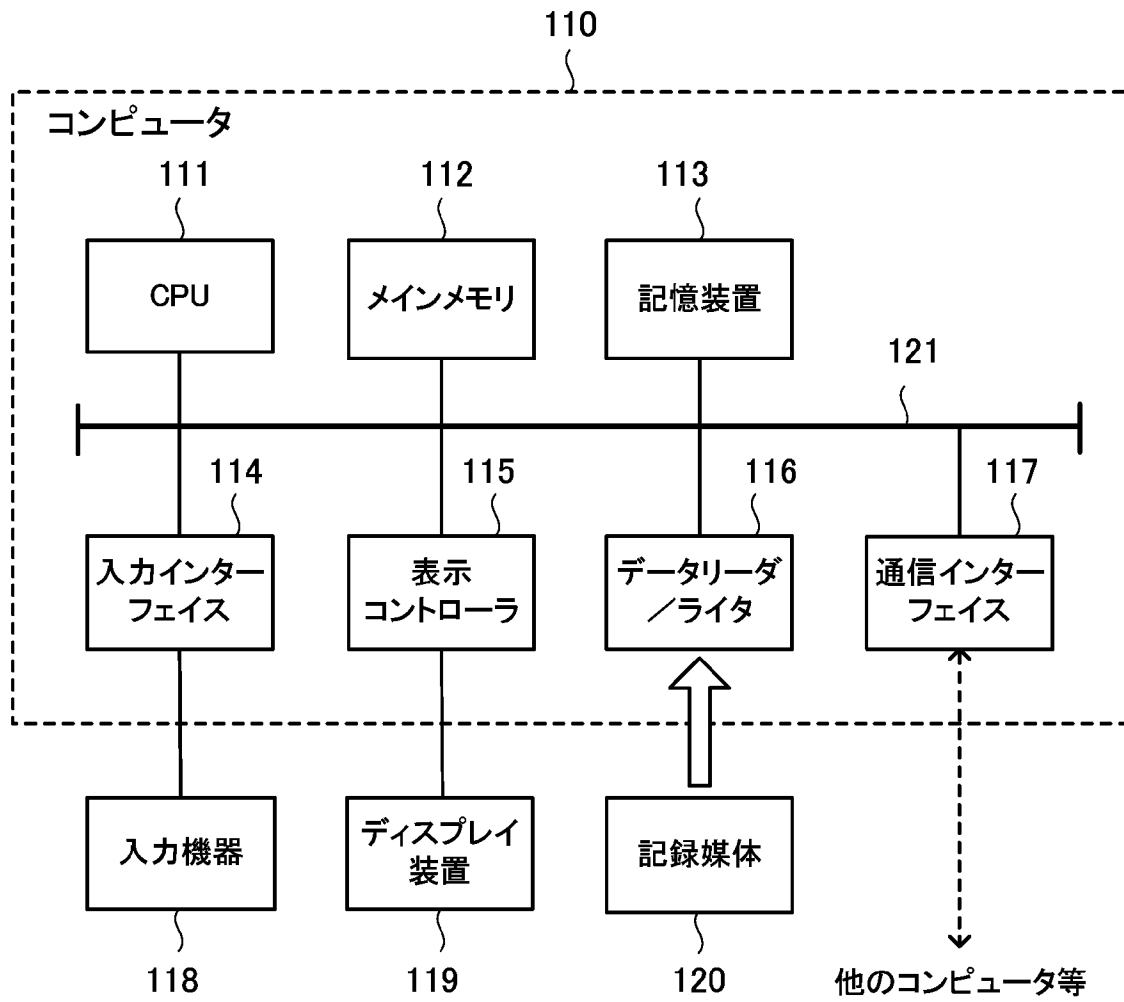
[図7]



[図8]



[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2022/009291

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/62**(2013.01)i; **G06F 21/60**(2013.01)i

FI: G06F21/62 309; G06F21/60 320

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)

G06F21/62; G06F21/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2022
 Registered utility model specifications of Japan 1996-2022
 Published registered utility model applications of Japan 1994-2022

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2020-017308 A (FUJI XEROX CO., LTD.) 30 January 2020 (2020-01-30) paragraphs [0034], [0041]-[0055]	1-3, 5-7, 9-11, 13-15
Y	paragraphs [0034], [0041]-[0055]	4, 8, 12, 16
Y	JP 2010-176431 A (FUJITSU LTD.) 12 August 2010 (2010-08-12) paragraphs [0011], [0016], [0095], [0117]-[0130]	4, 8, 12, 16
A	US 2015/0121089 A1 (KASPERSKY LAB ZAO) 30 April 2015 (2015-04-30) entire text, all drawings	1-16
A	JP 2017-130192 A (INTEL CORP.) 27 July 2017 (2017-07-27) entire text, all drawings	1-16

☐ 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

09 May 2022

Date of mailing of the international search report

17 May 2022

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)
 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915
 Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2022/009291

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
JP	2020-017308	A	30 January 2020	(Family: none)			
JP	2010-176431	A	12 August 2010	(Family: none)			
US	2015/0121089	A1	30 April 2015	EP	2866169	A1	
				DE	202014011089	U	
JP	2017-130192	A	27 July 2017	US	2018/0349610	A1	
				WO	2017/111843	A1	
				CN	109416718	A	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/62(2013.01)i; G06F 21/60(2013.01)i FI: G06F21/62 309; G06F21/60 320		
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）） G06F21/62; G06F21/60		
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 1971-2022年 日本国実用新案登録公報 1996-2022年 日本国登録実用新案公報 1994-2022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）		
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
X	JP 2020-017308 A（富士ゼロックス株式会社）30.01.2020（2020-01-30） 段落0034, 0041-0055	1-3, 5-7, 9-11, 13-15
Y	段落0034, 0041-0055	4, 8, 12, 16
Y	JP 2010-176431 A（富士通株式会社）12.08.2010（2010-08-12） 段落0011, 0016, 0095, 0117-0130	4, 8, 12, 16
A	US 2015/0121089 A1（KASPERSKY LAB ZA0）30.04.2015（2015-04-30） 全文、全図	1-16
A	JP 2017-130192 A（インテル コーポレーション）27.07.2017（2017-07-27） 全文、全図	1-16
☐ 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、一般的な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抵触するものではなく、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 09.05.2022		国際調査報告の発送日 17.05.2022
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号		権限のある職員（特許庁審査官） 吉田 歩 5S 1206 電話番号 03-3581-1101 内線 3546

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/JP2022/009291

引用文献			公表日	パテントファミリー文献			公表日
JP	2020-017308	A	30.01.2020	(ファミリーなし)			
JP	2010-176431	A	12.08.2010	(ファミリーなし)			
US	2015/0121089	A1	30.04.2015	EP	2866169	A1	
				DE	202014011089	U	
JP	2017-130192	A	27.07.2017	US	2018/0349610	A1	
				WO	2017/111843	A1	
				CN	109416718	A	