

(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7月21日(21.07.2022)



(10) 国際公開番号

WO 2022/153455 A1

(51) 国際特許分類:

H04N 7/15 (2006.01)

(21) 国際出願番号:

PCT/JP2021/001111

(22) 国際出願日:

2021年1月14日(14.01.2021)

(25) 国際出願の言語:

日本語

(26) 国際公開の言語:

日本語

(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).

(72) 発明者: 村上 啓造 (**MURAKAMI, Keizo**); 〒1808585 東京都武蔵野市緑町3丁目9-11 N T T 知的財産センタ内 Tokyo

(JP). 岡野 裕樹(**OKANO, Yuki**); 〒1808585 東京都武蔵野市緑町3丁目9-11 N T T 知的財産センタ内 Tokyo (JP). 小林 鉄太郎(**KOBAYASHI, Tetsutaro**); 〒1808585 東京都武蔵野市緑町3丁目9-11 N T T 知的財産センタ内 Tokyo (JP).

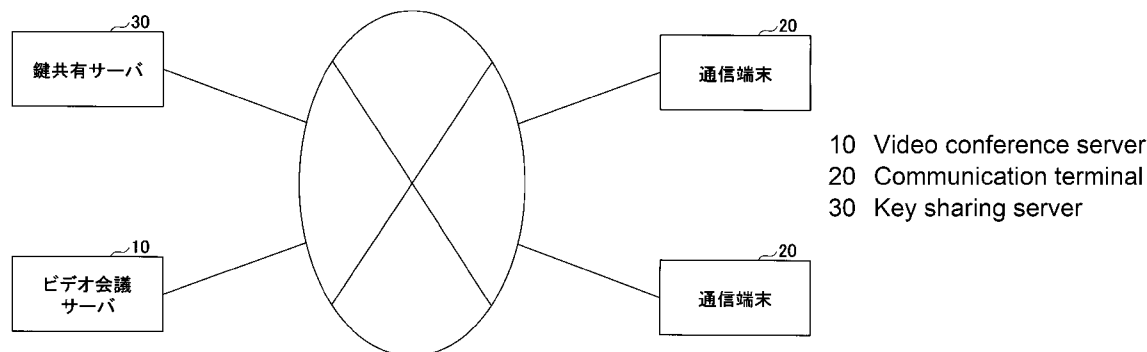
(74) 代理人: 伊東 忠重, 外(**ITO, Tadashige et al.**); 〒1000005 東京都千代田区丸の内二丁目1番1号 丸の内 M Y P L A Z A (明治安田生命ビル) 16階 Tokyo (JP).

(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,

(54) **Title:** COMMUNICATION SYSTEM, INFORMATION PROCESSING DEVICE, COMMUNICATION METHOD, AND PROGRAM

(54) 発明の名称: 通信システム、情報処理装置、通信方法及びプログラム

[図1]



(57) **Abstract:** This communication system includes an information processing device which provides a video conferencing service, and a plurality of communication terminals which utilize the video conferencing service, wherein: the information processing device includes a recording unit which records communication data relating to a video conference, encrypted and transmitted from each communication terminal, separately for each communication terminal in a first storage unit, a first transmitting unit which transmits, to the communication terminals, encrypted text obtained by encrypting, in such a way as to capable of being decrypted by the communication terminals, an encryption key capable of decrypting each set of communication data recorded in the first storage unit, and a second transmitting unit which transmits the communication data recorded in the first storage unit to the communication terminals; each communication terminal includes a decrypting unit which uses the result of decrypting the encrypted text to decrypt the communication data specific to the communication terminal, and a reproducing unit which synchronizes and reproduces video and audio included in the communication data decrypted specifically for the communication terminal, on the basis of control data

HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH,
KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
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))

included in each set of communication data. The invention thereby achieves a video-recording function for end-to-end encrypted communication data.

(57) 要約：ビデオ会議サービスを提供する情報処理装置と、ビデオ会議サービスを利用する複数の通信端末とを含む通信システムであって、情報処理装置は、各通信端末から暗号化されて送信されるビデオ会議に関する通信データを通信端末別に第1の記憶部に記録する記録部と、第1の記憶部に記録された各通信データを復号可能な暗号鍵が通信端末によって復号可能なように暗号化された暗号文を通信端末へ送信する第1の送信部と、第1の記憶部に記録された通信データを当該通信端末へ送信する第2の送信部と、を有し、通信端末は、通信端末別の通信データを暗号文の復号結果を用いて復号する復号部と、通信端末別に復号された通信データに含まれる映像及び音声を、それぞれの通信データに含まれている制御用のデータに基づいて同期させて再生する再生部と、を有することで、エンドツーエンドで暗号化された通信データの録画機能を実現する。

明 細 書

発明の名称：

通信システム、情報処理装置、通信方法及びプログラム

技術分野

[0001] 本発明は、通信システム、情報処理装置、通信方法及びプログラムに関する。

背景技術

[0002] ビジネスでの使用を前提とするメッセージ送信システムとしてパソコンやスマートフォン等のマルチデバイスに対応可能なシステムが存在する。マルチデバイスに対応可能なシステムのうち、企業の機密情報漏えいを考慮し、通信端末にデータを残さないクラウドベース型のビデオ会議システムが存在する。

[0003] このようなビデオ会議システムにおいては、通信路を暗号化することで通信経路上の盗聴防止がなされていたり、既に述べたように、通信端末にデータを残さないことによって通信端末の紛失や不正な持ち出しに起因する情報漏えい防止がなされていたりする。このように、従来のビデオ会議システムは「通信経路」と「通信端末」に対する脅威に対処している一方、サーバ装置に対する脅威への対処は不十分である。

[0004] ここでいうサーバ装置に対する脅威として、「サーバ装置に対する外部からの攻撃」や「サーバ管理者等による内部不正」等が挙げられる。

[0005] サーバ装置に対する脅威に対する１つの対策として、サーバ装置に対してビデオ会議の映像や音声データを秘匿し、通信端末でのみ復号可能なエンドツーエンドの暗号化通信を実現することが考えられる。但し、この場合、通信端末間で用いる共通鍵をどのように共有するかが問題となる。この問題の解決策が、例えば、非特許文献１が開示されている。非特許文献１では、中央に認証サーバをもつスター型のネットワークにおいて、認証サーバに対していかなる情報も漏らさずに利用者間で鍵（以下、「セッション鍵」という

。)を共有するプロトコルが提案されている。

[0006] これによって、サーバ装置に対してビデオ会議データを秘匿したまま通信端末間でのやりとりを可能とすることができる。また、現在参加している通信端末でのみビデオ会議データを利用できるようにセッション鍵の共有が行われるため、ユーザの追加・削除等のイベントによりセッション鍵が更新される。

[0007] 特許文献1によれば、セッション鍵更新にともない、サーバ装置のデータを最新のセッション鍵で復号できるよう再暗号化するとともに、セッションが途切れた後もセッション再開時に新セッションの通信端末に旧セッションのセッション鍵を共有する仕組みがある。

先行技術文献

特許文献

[0008] 特許文献1：特開2020-53772号公報

非特許文献

[0009] 非特許文献1：小林鉄太郎、米山一樹、吉田麗生、川原祐人、富士仁、山本具英「スケーラブルな動的多者鍵配布プロトコル」、SCIS2016-暗号と情報セキュリティシンポジウム-講演論文集、一般社団法人電子情報通信学会、平成28年1月、4E2-3

発明の概要

発明が解決しようとする課題

[0010] ビデオ会議システムでは、ビデオ会議データをサーバ装置で録画しておき、事後に再生できる録画機能が用意されていることが多い。録画機能においては、ビデオ会議システムの各参加者の通信端末から送信される、通信端末別の複数のビデオ会議データを、サーバ装置が一つに合成することで録画データが生成される。通信端末は、このような録画データをダウンロードすることで、ビデオ会議後の任意のタイミングで、ビデオ会議の全参加者の各通信端末から送信された映像データ及び音声データを再生することができる。

[0011] しかしながら、ビデオ会議においてエンドツーエンドの暗号化が実施された場合、サーバ装置では、複数の通信端末のビデオ会議データを合成できなくなってしまうため、録画機能の実現が困難である。

[0012] 本発明は、上記の点に鑑みてなされたものであって、エンドツーエンドで暗号化された通信データの録画機能を実現することを目的とする。

課題を解決するための手段

[0013] そこで上記課題を解決するため、ビデオ会議サービスを提供する情報処理装置と、前記ビデオ会議サービスを利用する複数の通信端末とを含む通信システムであって、前記情報処理装置は、前記各通信端末から暗号化されて送信されるビデオ会議に関する通信データを、前記通信端末別に第１の記憶部に記録する記録部と、前記第１の記憶部に記録された前記各通信データを復号可能な暗号鍵が前記通信端末によって復号可能なように暗号化された暗号文を前記通信端末へ送信する第１の送信部と、前記第１の記憶部に記録された前記通信データを当該通信端末へ送信する第２の送信部と、を有し、前記通信端末は、前記通信端末別の前記通信データを前記暗号文の復号結果を用いて復号する復号部と、前記通信端末別に復号された前記通信データに含まれる映像及び音声を、それぞれの前記通信データに含まれている制御用のデータに基づいて同期させて再生する再生部と、を有する。

発明の効果

[0014] エンドツーエンドで暗号化された通信データの録画機能を実現することができる。

図面の簡単な説明

[0015] [図1]本発明の実施の形態におけるビデオ会議システムの構成例を示す図である。

[図2]本発明の実施の形態におけるビデオ会議サーバ１０のハードウェア構成例を示す図である。

[図3]本発明の実施の形態におけるビデオ会議サーバ１０の機能構成例を示す図である。

[図4]ビデオ会議システムにおいて実行される処理手順の一例を説明するためのシーケンス図である。

[図5]ビデオ会議システムにおいて実行される処理手順の一例を説明するためのシーケンス図である。

[図6]ビデオ会議システムにおいて実行される処理手順の一例を説明するためのシーケンス図である。

[図7]通信端末20の通信データ取得機能の機能構成例を示す図である。

[図8]通信端末20の送信機能の機能構成例を示す図である。

[図9]通信端末20の再生権要求機能の機能構成例を示す図である。

[図10]通信端末20の鍵更新機能の機能構成例を示す図である。

[図11]通信端末20の旧セッション鍵暗号化機能の機能構成例を示す図である。

[図12]通信端末20の再生機能の機能構成例を示す図である。

発明を実施するための形態

[0016] 以下、図面に基づいて本発明の実施の形態を説明する。図1は、本発明の実施の形態におけるビデオ会議システムの構成例を示す図である。図1に示されるビデオ会議システムにおいて、鍵共有サーバ30、ビデオ会議サーバ10、及び複数の通信端末20は、インターネット等のネットワークを介して接続される。

[0017] 鍵共有サーバ30は、ID-DMKDプロトコル (ID-based Dynamic Multi-key Distribution Protocol) における鍵共有サーバとして機能する1以上のコンピュータである。鍵共有サーバ30は、各通信端末20とスター型トポロジを構成し、その中心に位置する。なお、鍵共有の方法について、ID-DMKDは一例であり、他の方法によって鍵共有が実現されてもよい。例えば、一台の通信端末20が鍵を生成し、公開鍵暗号方式によって他の通信端末20に鍵を配布する方法などで鍵共有が実現されてもよい。また、必ずしもスター型トポロジが構成されなくてもよい。

[0018] ビデオ会議サーバ10は、ビデオ会議サービスを提供する1以上のコンピ

ユータである。ビデオ会議サーバ１０は、通信端末２０から送信される、暗号化された通信データ（ビデオ会議データ）を記憶し、セッション鍵の更新時には、再暗号化を実施する。

[0019] 通信端末２０は、ビデオ会議サービスのユーザがビデオ会議の際に利用する通信端末である。

[0020] 図２は、本発明の実施の形態におけるビデオ会議サーバ１０のハードウェア構成例を示す図である。図２のビデオ会議サーバ１０は、それぞれバスＢで相互に接続されているドライブ装置１００、補助記憶装置１０２、メモリ装置１０３、ＣＰＵ１０４、及びインタフェース装置１０５等を有する。

[0021] ビデオ会議サーバ１０での処理を実現するプログラムは、ＣＤ－ＲＯＭ等の記録媒体１０１によって提供される。プログラムを記憶した記録媒体１０１がドライブ装置１００にセットされると、プログラムが記録媒体１０１からドライブ装置１００を介して補助記憶装置１０２にインストールされる。但し、プログラムのインストールは必ずしも記録媒体１０１より行う必要はなく、ネットワークを介して他のコンピュータよりダウンロードするようにしてもよい。補助記憶装置１０２は、インストールされたプログラムを格納すると共に、必要なファイルやデータ等を格納する。

[0022] メモリ装置１０３は、プログラムの起動指示があった場合に、補助記憶装置１０２からプログラムを読み出して格納する。ＣＰＵ１０４は、メモリ装置１０３に格納されたプログラムに従ってビデオ会議サーバ１０に係る機能を実行する。インタフェース装置１０５は、ネットワークに接続するためのインタフェースとして用いられる。

[0023] 図３は、本発明の実施の形態におけるビデオ会議サーバ１０の機能構成例を示す図である。図３において、ビデオ会議サーバ１０は、暗号文受信部１１１、暗号文送信部１１２、鍵更新用データ受信部１１３、再暗号化部１１４、セットアップ処理部１１５、再生権要求受信部１１６、公開鍵リスト送信部１１７、旧セッション鍵暗号文受信部１１８、旧セッション鍵暗号文送信部１１９及び旧セッション鍵暗号文分割部１２０等を有する。これら各部

は、ビデオ会議サーバ１０にインストールされた１以上のプログラムが、ＣＰＵ１０４に実行させる処理により実現される。ビデオ会議サーバ１０は、また、暗号文記憶部１３１、サーバ用鍵ペア記憶部１３２、公開鍵リスト記憶部１３３、旧セッション鍵暗号文記憶部１３４等を利用する。これら各記憶部は、例えば、メモリ装置１０３、補助記憶装置１０２、又はビデオ会議サーバ１０にネットワークを介して接続可能な記憶装置等を用いて実現可能である。

[0024] 以下、ビデオ会議システムにおいて実行される処理手順について説明する。図４～図６は、ビデオ会議システムにおいて実行される処理手順の一例を説明するためシーケンス図である。

[0025] ビデオ会議（以下、単に「会議」という。）の開始前の任意のタイミングにおいて、各通信端末２０は、鍵共有サーバ３０装置と通信して、セッション鍵 K_1 を共有する（Ｓ１０１～Ｓ１０３）。なお、セッション鍵の共有は、例えば、非特許文献１に開示されている方法に基づいて実行されてもよい。

[0026] 会議が開始されると、通信データを送信する各通信端末２０は、当該通信端末２０の通信データ取得機能を利用して通信データの構成要素を取得し、当該通信端末２０の送信機能を利用して当該通信データを暗号化して、暗号文をビデオ会議サーバ１０へ送信する（Ｓ１１１～Ｓ１１３）。

[0027] 図７は、通信端末２０の通信データ取得機能の機能構成例を示す図である。図７に示されるように、通信データ取得機能を有する通信端末２０は、画面情報取得部２１１、映像データ取得部２１２、音声データ取得部２１３、時刻データ取得部２１４、画面表示位置情報取得部２１５及びデータ収集部２１６等を有する。これら各部は、通信端末２０にインストールされた１以上のプログラムが、通信端末２０のＣＰＵに実行させる処理により実現される。

[0028] 通信データは、メディアデータ及び制御用メタデータを含む。メディアデータは、画面共有データ、映像データ及び音声データを含む。画面共有のデータとは、映像データや音声データとは別に、画面共有や資料共有を行った

際の画面を示すデータをいう。映像データとは、通信端末20に接続されたカメラから入力される映像（例えば、会議への参加者の画像）を示すデータをいう。音声データとは、通信端末20に接続されたマイクから入力される音声（例えば、会議への参加者が発話した音声）を示すデータをいう。

[0029] 制御用メタデータは、時刻データ、映像のオンオフ情報、音声のオンオフ情報、画面共有のオンオフ情報、及び画面上の表示位置を含む。時刻データとは、メディアデータの記録時刻を示すデータをいう。なお、時刻データは、他の通信端末20のメディアデータとの同期のために利用される。したがって、斯かる同期が可能であれば、時刻データはどのような形式であってもよい。

[0030] 映像のオンオフ情報とは、映像データの送信（共有）についてのオンオフを示す情報をいう。音声のオンオフ情報とは、音声データの送信（共有）についてのオンオフを示す情報をいう。画面共有のオンオフ情報とは、画面共有のデータの送信（共有）についてのオンオフを示す情報をいう。画面上の表示位置とは、画面共有の対象とされる資料等の表示位置をいう。なお、各データのオンオフや、画面上の表示位置は、時間の経過に伴って変化する可能性が有る。したがって、これらのデータは、各時刻における値と当該時刻とを時系列に含むデータであってもよい。

[0031] 画面情報取得部211は、ビデオ会議時の画面共有のデータ、及び画面共有のオンオフ情報を取得する。映像データ取得部212は、ビデオ会議時の映像データを取得する。音声データ取得部213は、ビデオ会議時の音声データを取得する。時刻データ取得部214は、時刻データを取得する。画面表示位置情報取得部215は、画面上の表示位置等を取得する。データ収集部216は、各部によって取得されたデータ群を収集し、当該データ群を含む通信データ（の平文）mを出力する。

[0032] 図8は、通信端末20の送信機能の機能構成例を示す図である。図8に示されるように、送信機能を有する通信端末20は、共通鍵暗号文生成部221、関数演算部222及び暗号文送信部223を有する。これら各部は、通

信端末 20 にインストールされた 1 以上のプログラムが、通信端末 20 の CPU に実行させる処理により実現される。送信機能を有する通信端末 20 は、また、共通鍵記憶部 291 及びセッション鍵記憶部 292 を利用する。これら各記憶部は、通信端末 20 のメモリ装置又は補助記憶装置等を用いて実現可能である。

[0033] 共通鍵暗号文生成部 221 は、通信データ取得機能から出力される通信データ m を、共通鍵記憶部 291 に記憶されている共通鍵 K を用いて暗号化することで、暗号文 C_DEM を生成する。共通鍵 K は、予め所定の方法によって各通信端末 20 間で共有される。なお、本実施の形態において、「 X_Y 」（ X 、 Y は任意の記号）という表記は、図面において Y が X に対する下付き文字である記号を表す。

[0034] 関数演算部 222 は、ステップ $S101 \sim S103$ において共有され、セッション鍵記憶部 292 に記憶されているセッション鍵と、共通鍵 K とに関数 f_K_1 を適用した演算を実行することで、通信データ m を暗号化した共通鍵 K をその時点でのセッション鍵（この時点では K_1 ）で暗号化した結果である暗号文 $f_k_1 (K, K_1)$ を生成する。

[0035] 暗号文送信部 223 は、共通鍵暗号文生成部 221 が生成した C_DEM と、関数演算部 222 が生成した $f_k_1 (K, K_1)$ との組である（ $C_DEM, f_k_1 (K, K_1)$ ）をビデオ会議サーバ 10 へ送信する。すなわち、ステップ $S111 \sim S113$ では、各通信端末 20 から（ $C_DEM, f_k_1 (K, K_1)$ ）がビデオ会議サーバ 10 へ送信される。

[0036] ビデオ会議サーバ 10 の暗号文受信部 111 は、（ $C_DEM, f_k_1 (K, K_1)$ ）を受信すると、当該（ $C_DEM, f_k_1 (K, K_1)$ ）を暗号文記憶部 131 へ記録する。この際、暗号文受信部 111 は、（ $C_DEM, f_k_1 (K, K_1)$ ）を通信端末 20 別に記録する。 C_DEM は暗号化されているため、ビデオ会議サーバ 10 では合成できないからである。

[0037] ステップS 1 1 1～S 1 1 3は、会議中において継続的に実行される。

[0038] なお、各通信端末20は、会議中において、ビデオ会議サーバ10から他の通信端末20の(C__DEM, f__k__1 (K, K__1))を受信し、その時点のセッション鍵K__1で、f__k__1 (K, K__1)を復号し、得られた共通鍵Kで、C__DEMを復号することで、他の通信端末20からの通信データmを得ることができる。

[0039] その後、会議の途中において、例えば、通信端末20iがセッション（会議）から離脱する場合において、通信端末20iのユーザU__iが会議終了後に録画内容の再生を希望する場合には、再生権要求処理（S 1 2 1～S 1 2 4）が実行される。再生権とは、会議終了後の任意の時点において当該会議に関する通信データを復号し、再生する権利をいう。再生権要求処理において、通信端末20の再生権要求機能が利用される。

[0040] 図9は、通信端末20の再生権要求機能の機能構成例を示す図である。図9に示されるように、再生権要求機能は、セットアップ処理部231及び再生権要求送信部232を含む。これら各部は、通信端末20にインストールされた1以上のプログラムが、通信端末20のCPUに実行させる処理により実現される。通信端末20は、また、鍵ペア記憶部293を利用する。鍵ペア記憶部293は、例えば、通信端末20のメモリ装置又は補助記憶装置等を用いて実現可能である。

[0041] セットアップ処理部231は、ステップS 1 2 1（図4）において、ビデオ会議サーバ10のセットアップ処理部115（図3）との間でセットアップ処理（事前準備処理）を実行する。セットアップ処理において、ビデオ会議サーバ10のセットアップ処理部115（図3）は、ビデオ会議サーバ10用の公開鍵Params及び秘密鍵mskを生成し、公開鍵Params及び秘密鍵mskをサーバ用鍵ペア記憶部132に記録する（S 1 2 1）。セットアップ処理部115は、また、部分秘密鍵導出アルゴリズムに対して、公開鍵Params、秘密鍵msk及び通信端末20iの識別子（以下、「ID」という。）U__iを入力することで、部分秘密鍵psk__iを生成

し、部分秘密鍵 $p s k_i$ を通信端末 20 i へ送信する (S 1 2 2)。

[0042] 一方、通信端末 20 i のセットアップ処理部 231 (図 9) は、ビデオ会議サーバ 10 から部分秘密鍵 $p s k_i$ を受信すると、公開鍵 $P a r a m s$ 、部分秘密鍵 $p s k_i$ 及び秘密値を完全秘密鍵生成アルゴリズムに入力することで、完全秘密鍵 $c s k_i$ と完全公開鍵 $c p k_i$ とを生成し、完全秘密鍵 $c s k_i$ 及び完全公開鍵 $c p k_i$ の組を鍵ペア記憶部 293 へ記録する (S 1 2 3)。

[0043] 続いて、通信端末 20 i の再生権要求送信部 232 は、完全公開鍵 $c p k_i$ 及び通信端末 20 i の ID (U_i) を含む再生権要求をビデオ会議サーバ 10 に送信する (S 1 2 4)。ビデオ会議サーバ 10 の再生権要求受信部 116 (図 3) は、当該再生権要求を受信すると、当該再生権要求に含まれている通信端末 20 i の $c p k_i$ を U_i に関連付けて公開鍵リスト記憶部 133 へ記録する。 $c p k_i$ が U_i に関連付けられて公開鍵リスト記憶部 133 へ記録されることで、通信端末 20 i が再生権を要求したことがビデオ会議サーバ 10 において記憶される。

[0044] その後、通信端末 20 i はセッション (ビデオ会議) から離脱する (S 1 2 5)。

[0045] 通信端末 20 i の離脱 (参加メンバ U_i の離脱) に応じ、他の通信端末 20 間は、鍵共有サーバ 30 装置と通信して、セッション鍵を更新し、更新後のセッション鍵 K_2 を共有する (S 1 3 1、S 1 3 2)。更新後のセッション鍵 K_2 は、当該各通信端末 20 のセッション鍵記憶部 292 に記憶される。なお、セッション鍵の更新は、参加メンバの追加や一定時間経過等の他のタイミングにおいて行われてもよい。

[0046] セッション鍵が更新されると、鍵更新処理 (S 1 4 1 ~ S 1 4 3) が実行される。鍵更新処理では、更新後のセッション鍵 K_2 を有する通信端末 20 のうちの一つ (図 4 では通信端末 20 j) の鍵更新機能が利用される。

[0047] 図 10 は、通信端末 20 の鍵更新機能の機能構成例を示す図である。図 10 に示されるように、鍵更新機能は、鍵更新用数演算部 241 及び鍵更新用

データ送信部242を含む。

[0048] 鍵更新用数演算部241は、セッション鍵記憶部292に記憶されているセッション鍵 $K_{_1}$ 及びセッション鍵 $K_{_2}$ に対して関数 $f_{_K_{_1}}$ を適用した演算を実行することで、当該演算の結果（更新後のセッション鍵 $K_{_2}$ によって更新前のセッション鍵 $K_{_1}$ を暗号化して結果）である再暗号化鍵 $f_{_k_{_1}}(K_{_1}, K_{_2})$ を生成する（S141）。

[0049] 続いて、鍵更新用データ送信部242は、再暗号化鍵 $f_{_k_{_1}}(K_{_1}, K_{_2})$ をビデオ会議サーバ10へ送信する（S142）。

[0050] ビデオ会議サーバ10の鍵更新用データ受信部113（図3）が再暗号化鍵 $f_{_k_{_1}}(K_{_1}, K_{_2})$ を受信すると、再暗号化部114（図3）は、 $f_{_k_{_1}}(K_{_1}, K_{_2})$ を用いて、暗号文記憶部131に通信端末20別に記録している各録画データ（ $C_DEM, f_{_k_{_1}}(K, K_{_1})$ ）の $f_{_k_{_1}}(K, K_{_1})$ を $f_{_k_{_1}}(K, K_{_2})$ へと再暗号化する（S143）。その結果、各録画データ（ $C_DEM, f_{_k_{_1}}(K, K_{_1})$ ）は、（ $C_DEM, f_{_k_{_1}}(K, K_{_2})$ ）へ更新され、更新後のセッション鍵 $K_{_2}$ によってのみ復号可能となる。なお、再暗号化については、特許文献1に詳しい。

[0051] その後、更新後のセッション鍵 $K_{_2}$ が用いられて会議が進行される。すなわち、セッション鍵 $K_{_1}$ の代わりにセッション鍵 $K_{_2}$ が用いられて、ステップS112及びS113と同様の処理が実行されて、通信端末20j及び通信端末20kのそれぞれの（ $C_DEM, f_{_k_{_1}}(K, K_{_2})$ ）がビデオ会議サーバ10の暗号文記憶部131に通信端末20別に記録（録画）される（S151、S152）。

[0052] また、会議が終了する際に、通信端末20iのユーザ $U_{_j}$ が会議終了後に録画内容の再生を希望する場合には、ステップS121～S124と同様に、再生権要求処理（図5のS161～S163）が実行される。その結果、（ $U_{_j}, c_{pk_{_j}}$ ）がビデオ会議サーバ10の公開鍵リスト記憶部133に記録される。但し、ビデオ会議サーバ10は、ステップS122にお

いて、既に $Params$ 及び msk を生成しているため、これらを改めて生成しなくてよい。

[0053] また、会議（セッション）が終了し、全員が会議から離脱すると、代表となる通信端末 $20j$ の旧セッション鍵暗号化機能は、旧セッション鍵暗号文生成処理を実行する。なお、代表となる通信端末 20 は、例えば、ランダムに決定される。

[0054] 図 11 は、通信端末 20 の旧セッション鍵暗号化機能の機能構成例を示す図である。図 11 に示されるように、旧セッション鍵暗号化機能は、公開鍵リスト受信部 251 、旧セッション鍵暗号化処理部 252 及び旧セッション鍵暗号文送信部 253 を含む。

[0055] 公開鍵リスト受信部 251 は、当該会議において実行された再生権要求処理においてビデオ会議サーバ 10 の公開鍵リスト記憶部 133 に記憶された、完全公開鍵のリスト $\{(U_i, cpk_i), (U_j, cpk_j)\}$ をビデオ会議サーバ 10 の公開鍵リスト送信部 117 から受け取り ($S171$)、当該完全公開鍵のリストを旧セッション鍵暗号化処理部 252 へ入力する。なお、本実施の形態では、 U_i に係る通信端末 $20i$ と、 U_j に係る通信端末 $20j$ とによって再生権要求処理が実行されている（再生権が要求されている）ため、 (U_i, cpk_i) 及び (U_j, cpk_j) が、当該リストに含まれる。

[0056] 旧セッション鍵暗号化処理部 252 は、 $\{(U_i, cpk_i), (U_j, cpk_j)\}$ と、会議終了時点のセッション鍵 K_2 とを暗号化アルゴリズムへ入力することで、 $\{(U_i, cpk_i), (U_j, cpk_j)\}$ によってセッション鍵 K_2 を暗号化した結果である暗号文 CT_oid, ij を生成する。

[0057] 旧セッション鍵暗号文送信部 253 は、ステップ $S172$ において、暗号文 CT_oid, ij をビデオ会議サーバ 10 に送信する。なお、暗号文 CT_oid, ij は、 ID のリスト $\{U_i, U_j\}$ が関連付けられたデータである。ビデオ会議サーバ 10 の旧セッション鍵暗号文受信部 118 は

、暗号文CT__o l d, i jを受信すると、暗号文CT__o l d, i jを旧セッション鍵暗号文記憶部134へ記録する。

[0058] その後、ユーザU__iが会議の録画内容の再生指示を通信端末20iへ入力すると、通信端末20iは、鍵共有サーバ30と通信して新規セッションを開始し、新規セッション鍵K__3を生成する（図6のS181）。セッション鍵K__3は、通信端末20iのセッション鍵記憶部292に記録される。

[0059] 続いて、通信端末20iは、再生機能を用いて再生処理を実行する。

[0060] 図12は、通信端末20の再生機能の機能構成例を示す図である。図12に示されるように、再生機能を有する通信端末20は、旧セッション鍵暗号文受信部261、旧セッション鍵復号部262、暗号文受信部263、暗号文復号部264及び再生部265を有する。これら各部は、通信端末20にインストールされた1以上のプログラムが、通信端末20のCPUに実行させる処理により実現される。

[0061] 旧セッション鍵暗号文受信部261は、ステップS182において、暗号化された旧セッション鍵をビデオ会議サーバ10に要求する。

[0062] ビデオ会議サーバ10の旧セッション鍵暗号文送信部119（図3）が、暗号化された旧セッション鍵の要求を受信すると、旧セッション鍵暗号文分割部120（図3）は、通信端末20iのID（U__i）に関連付くCT__o l dを検索し、該当するCT__o l dが有る場合、当該CT__o l d（本実施の形態ではCT__o l d, i j）を通信端末20iの秘密鍵c s k__iでのみ（すなわち、通信端末20iのみが）が復号できるようにCT__o l d, iに変換する（S183、S184）。すなわち、旧セッション鍵暗号文分割部120は、CT__o l d, i jを分割して、U__iに対応する部分をCT__o l d, iとして生成する。なお、暗号文の分割は、例えば、特許文献1に開示されている方法を用いて実行されてもよい。旧セッション鍵暗号文送信部119は、変換後のデータであるCT__o l d, iを通信端末20iに送信する（S185）。

- [0063] 旧セッション鍵暗号文受信部261がCT__old, iを受信すると、旧セッション鍵復号部262は、CT__old, iを通信端末20iの秘密鍵csk__iで復号することで、K__2を得る(S186)。
- [0064] 続いて、暗号文受信部263が、暗号文送信部112から、通信端末20別に暗号文記憶部131に記録されている各(C__DEM, f__k__1(K, K__2))を受信すると(S187)、暗号文復号部264は、K__2を用いて各(C__DEM, f__k__1(K, K__2))を復号することで、各通信データm(例えば、m__i、m__j、m__k)を得る(S188)。より詳しくは、暗号文復号部264は、K__2を用いてf__k__1(K, K__2)からKを復号し、復号されたKを用いてC__DEMをmへ復号する。なお、m__iは、通信端末20iの通信データmである。m__jは、通信端末20jの通信データmである。m__kは、通信端末20kの通信データmである。
- [0065] 続いて、再生部265は、各通信データm(m__i, m__j, m__k)に含まれている制御用メタデータに従って、各通信データmに含まれているメディアデータを再生する。すなわち、再生部265は、各通信データmを、それぞれに含まれている時刻データに基づいて同期させてそれぞれに含まれているメディアデータを再生する。この際、再生部265は、各メディアデータのオンオフを、各通信データに含まれているオンオフ情報に基づいて制御する。また、再生部265は、画面共有の対象とされる資料等の表示位置についても、各通信データmの制御用メタデータに含まれている画面上の表示位置に基づいて再現する。すなわち、再生部265は、通信端末20別にビデオ会議サーバ10に記録されていた各通信データを合成する。その結果、通信端末20iのユーザU__iは、会議時と同様の形態にて、会議の様子を確認することができる。すなわち、ユーザU__iは、実質的に、録画機能を利用することができる。
- [0066] 続いて、旧セッション鍵K__2が漏洩してもビデオ会議サーバ10上の通信データが復号されないようにするための処理が実行される。

- [0067] まず、ビデオ会議サーバ10の公開鍵リスト送信部117は、公開鍵リスト記憶部133に記憶されている公開鍵のリスト {c p k__i、c p k__j} を通信端末20iへ送信する(S191)。
- [0068] 通信端末20iの公開鍵リスト受信部251(図11)は、公開鍵のリスト {c p k__i、c p k__j} を受信すると、当該公開鍵のリストを旧セッション鍵暗号化処理部252へ入力する。旧セッション鍵暗号化処理部252は、{(U__i, c p k__i), (U__j, c p k__j)}と、現時点のセッション鍵K__3とを暗号化アルゴリズムへ入力することで、{(U__i, c p k__i), (U__j, c p k__j)}によってセッション鍵K__3を暗号化した結果である暗号文C T__new, i jを生成する。旧セッション鍵暗号文送信部253は、ステップS192において、暗号文C T__new, i jをビデオ会議サーバ10に送信する。
- [0069] ビデオ会議サーバ10の旧セッション鍵暗号文受信部118は、暗号文C T__new, i jを受信すると、暗号文C T__new, i jを旧セッション鍵暗号文記憶部134へ記録する。
- [0070] 続いて、通信端末20iの鍵更新用数演算部241が、K__2及びK__3から再暗号化鍵f__k__1(K__2, K__3)を生成すると(S193)、鍵更新用データ送信部242は、再暗号化鍵f__k__1(K__2, K__3)をビデオ会議サーバ10へ送信する(S194)。
- [0071] ビデオ会議サーバ10の鍵更新用データ受信部113(図3)が再暗号化鍵f__k__1(K__2, K__3)を受信すると、再暗号化部114(図3)は、f__k__1(K__2, K__3)を用いて、暗号文記憶部131に記録されている各録画データ(C__DEM, f__k__1(K, K__2))のf__k__1(K, K__2)をf__k__1(K, K__3)へと再暗号化する(S195)。その結果、各録画データ(C__DEM, f__k__1(K, K__2))は、(C__DEM, f__k__1(K, K__3))となり、更新後のセッション鍵K__3によってのみ復号可能となる。
- [0072] なお、ステップS191～S195は、ステップS181～S189と並

行して実行されてもよい。

[0073] 上述したように、本実施の形態によれば、セッション鍵によって暗号化されてビデオ会議サーバ10に記録されている通信端末20別の録画データが或る通信端末20において再生される際に、ビデオ会議サーバ10は、当該通信データを復号可能なセッション鍵が当該或る通信端末20によって復号可能なように暗号化された暗号文と、各録画データとを当該或る通信端末20へ送信する。その結果、当該或る通信端末は、各録画データを復号し、各復号結果に含まれる各メディアデータと、各復号結果に含まれる制御用メタデータに基づいて再生することで、各メディアデータを同期させて再生することができる。したがって、通信データの経由地点（ビデオ会議サーバ10）に対して通信データの内容を秘匿しつつ通信データの録画機能を実現することができる。

[0074] また、本実施の形態によれば、再生権を要求した通信端末20のみが、録画データの復号を行うことができる。その結果、例えば、不特定の者が参加可能なビデオ会議において、不正者であるとして途中で離脱させた参加者によって、ビデオ会議全体の録画内容が閲覧されるのを防止することができる。なお、再生権の要求の際には、再生権の要求元の通信端末20のユーザについてビデオ会議サーバ10が認証を行うようにしてもよい。そうすることで、不正者による再生権の要求を防止することができる。

[0075] なお、非特許文献1では、現在の参加メンバのみでセッション鍵を共有するため、セッション鍵はログイン・ログアウトイベントのようなユーザの追加・削除に伴って更新されたり、それ以外にも定期的に更新されたりすることがある。特許文献1によれば、セッション鍵更新にともない、データを再暗号化し、セッション鍵を非同期で新規セッションの通信端末20に共有することが可能だが、通信端末20の指定については未解決であるという課題がある。本実施の形態によれば、斯かる課題についても解決することができる。

[0076] なお、本実施の形態において、ビデオ会議サーバ10は、情報処理装置の

一例である。ビデオ会議サーバ 10 と通信端末 20 とが構成するシステムは、通信システムの一例である。セッション鍵は、暗号鍵の一例である。暗号文受信部 111 は、記録部の一例である。暗号文記憶部 131 は、第 1 の記憶部の一例である。セッション鍵は、第 1 の暗号鍵の一例である。旧セッション鍵暗号文送信部 119 は、第 1 の送信部の一例である。暗号文送信部 112 は、第 2 の送信部の一例である。暗号文復号部 264 は、復号部の一例である。再生権要求受信部 116 は、第 2 の受信部の一例である。公開鍵リスト記憶部 133 は、第 2 の記憶部の一例である。旧セッション鍵暗号文受信部 118 は、第 3 の受信部の一例である。旧セッション鍵暗号文分割部 120 は、変換部の一例である。

[0077] 以上、本発明の実施の形態について詳述したが、本発明は斯かる特定の実施形態に限定されるものではなく、請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

符号の説明

[0078]	10	ビデオ会議サーバ
	20	通信端末
	30	鍵共有サーバ
	100	ドライブ装置
	101	記録媒体
	102	補助記憶装置
	103	メモリ装置
	104	CPU
	105	インタフェース装置
	111	暗号文受信部
	112	暗号文送信部
	113	鍵更新用データ受信部
	114	再暗号化部
	115	セットアップ処理部

1 1 6	再生権要求受信部
1 1 7	公開鍵リスト送信部
1 1 8	旧セッション鍵暗号文受信部
1 1 9	旧セッション鍵暗号文送信部
1 2 0	旧セッション鍵暗号文分割部
1 3 1	暗号文記憶部
1 3 2	サーバ用鍵ペア記憶部
1 3 3	公開鍵リスト記憶部
1 3 4	旧セッション鍵暗号文記憶部
2 1 1	画面情報取得部
2 1 2	映像データ取得部
2 1 3	音声データ取得部
2 1 4	時刻データ取得部
2 1 5	画面表示位置情報取得部
2 1 6	データ収集部
2 2 1	共通鍵暗号文生成部
2 2 2	関数演算部
2 2 3	暗号文送信部
2 3 1	セットアップ処理部
2 3 2	再生権要求送信部
2 4 1	鍵更新用数演算部
2 4 2	鍵更新用データ送信部
2 5 1	公開鍵リスト受信部
2 5 2	旧セッション鍵暗号化処理部
2 5 3	旧セッション鍵暗号文送信部
2 6 1	旧セッション鍵暗号文受信部
2 6 2	旧セッション鍵復号部
2 6 3	暗号文受信部

2 6 4	暗号文復号部
2 6 5	再生部
2 9 1	共通鍵記憶部
2 9 2	セッション鍵記憶部
2 9 3	鍵ペア記憶部
B	バス

請求の範囲

[請求項1]

ビデオ会議サービスを提供する情報処理装置と、前記ビデオ会議サービスを利用する複数の通信端末とを含む通信システムであって、
前記情報処理装置は、
前記各通信端末から暗号化されて送信されるビデオ会議に関する通信データを、前記通信端末別に第1の記憶部に記録する記録部と、
前記第1の記憶部に記録された前記各通信データを復号可能な暗号鍵が前記通信端末によって復号可能なように暗号化された暗号文を前記通信端末へ送信する第1の送信部と、
前記第1の記憶部に記録された前記通信データを当該通信端末へ送信する第2の送信部と、
を有し、
前記通信端末は、
前記通信端末別の前記通信データを前記暗号文の復号結果を用いて復号する復号部と、
前記通信端末別に復号された前記通信データに含まれる映像及び音声、それぞれの前記通信データに含まれている制御用のデータに基づいて同期させて再生する再生部と、
を有することを特徴とする通信システム。

[請求項2]

前記情報処理装置は、
いずれかの前記通信端末から、当該通信端末が生成した公開鍵を受信すると、当該公開鍵を第2の記憶部へ記録する第2の受信部と、
前記ビデオ会議において前記第2の記憶部に記録された全ての前記公開鍵を用いて暗号化された前記暗号鍵の前記暗号文を、いずれかの前記通信端末から受信する第3の受信部と、
いずれかの前記通信端末からの要求に応じ、当該通信端末の前記公開鍵に対する秘密鍵によって復号可能なように前記暗号文を変換する変換部と、

を有し、

前記第 1 の送信部は、変換後の前記暗号文を当該通信端末へ送信する、

ことを特徴とする請求項 1 記載の通信システム。

[請求項3]

前記情報処理装置は、

前記暗号鍵が更新されると、前記第 1 の記憶部に記録された前記通信データを、更新後の暗号鍵によってのみ復号できるように再暗号化する再暗号化部を有し、

前記第 3 の受信部は、前記ビデオ会議において前記第 2 の記憶部に記録された全ての前記公開鍵を用いて暗号化された前記ビデオ会議の終了時の前記暗号鍵の前記暗号文を、いずれかの前記通信端末から受信する、

ことを特徴とする請求項 2 記載の通信システム。

[請求項4]

ビデオ会議サービスを提供する情報処理装置であって、

前記ビデオ会議サービスを利用する前記各通信端末から暗号化されて送信されるビデオ会議に関する通信データを、前記通信端末別に第 1 の記憶部に記録する記録部と、

前記第 1 の記憶部に記録された前記各通信データを復号可能な暗号鍵が前記通信端末によって復号可能なように暗号化された暗号文を前記通信端末へ送信する第 1 の送信部と、

前記第 1 の記憶部に記録された前記通信データを当該通信端末へ送信する第 2 の送信部と、

を有することを特徴とする情報処理装置。

[請求項5]

ビデオ会議サービスを提供する情報処理装置と、前記ビデオ会議サービスを利用する複数の通信端末とが実行する通信方法であって、

前記情報処理装置が、

前記各通信端末から暗号化されて送信されるビデオ会議に関する通信データを、前記通信端末別に第 1 の記憶部に記録する記録手順と、

前記第 1 の記憶部に記録された前記各通信データを復号可能な暗号鍵が前記通信端末によって復号可能なように暗号化された暗号文を前記通信端末へ送信する第 1 の送信手順と、

前記第 1 の記憶部に記録された前記通信データを当該通信端末へ送信する第 2 の送信手順と、

を実行し、

前記通信端末が、

前記通信端末別の前記通信データを前記暗号文の復号結果を用いて復号する復号手順と、

前記通信端末別に復号された前記通信データに含まれる映像及び音声、それぞれの前記通信データに含まれている制御用のデータに基づいて同期させて再生する再生手順と、

を実行することを特徴とする通信方法。

[請求項6]

ビデオ会議サービスを提供する情報処理装置に、

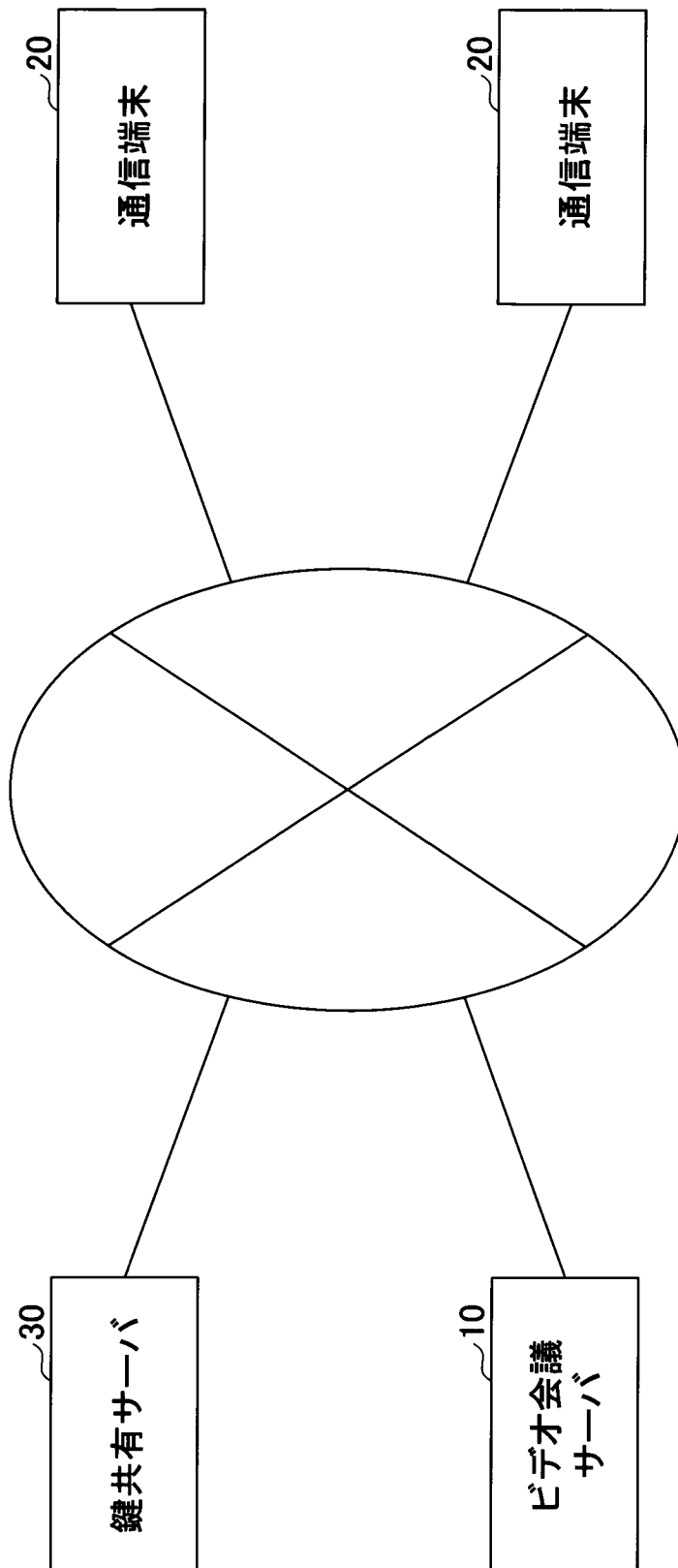
前記ビデオ会議サービスを利用する前記各通信端末から暗号化されて送信されるビデオ会議に関する通信データを、前記通信端末別に第 1 の記憶部に記録する記録手順と、

前記第 1 の記憶部に記録された前記各通信データを復号可能な暗号鍵が前記通信端末によって復号可能なように暗号化された暗号文を前記通信端末へ送信する第 1 の送信手順と、

前記第 1 の記憶部に記録された前記通信データを当該通信端末へ送信する第 2 の送信手順と、

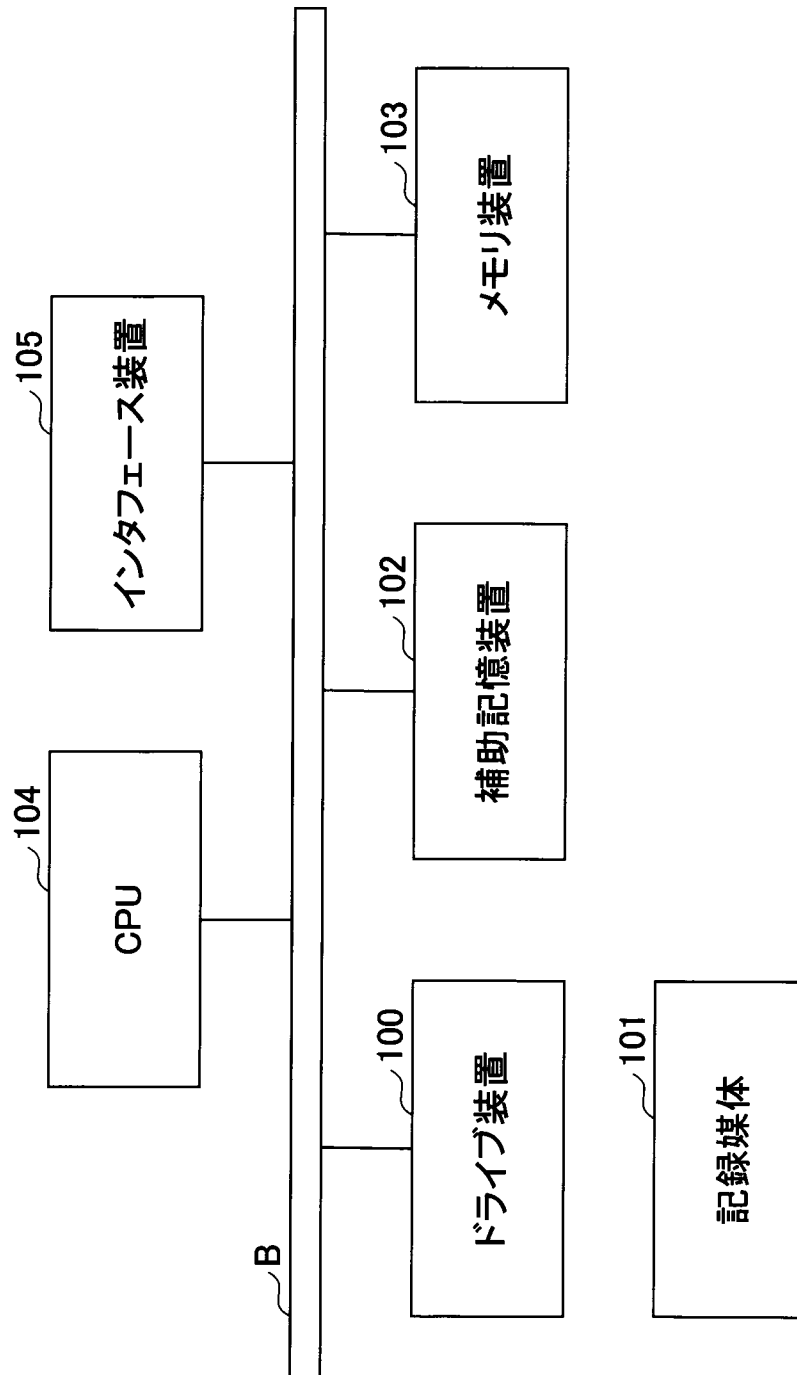
を実行させることを特徴とするプログラム。

[図1]

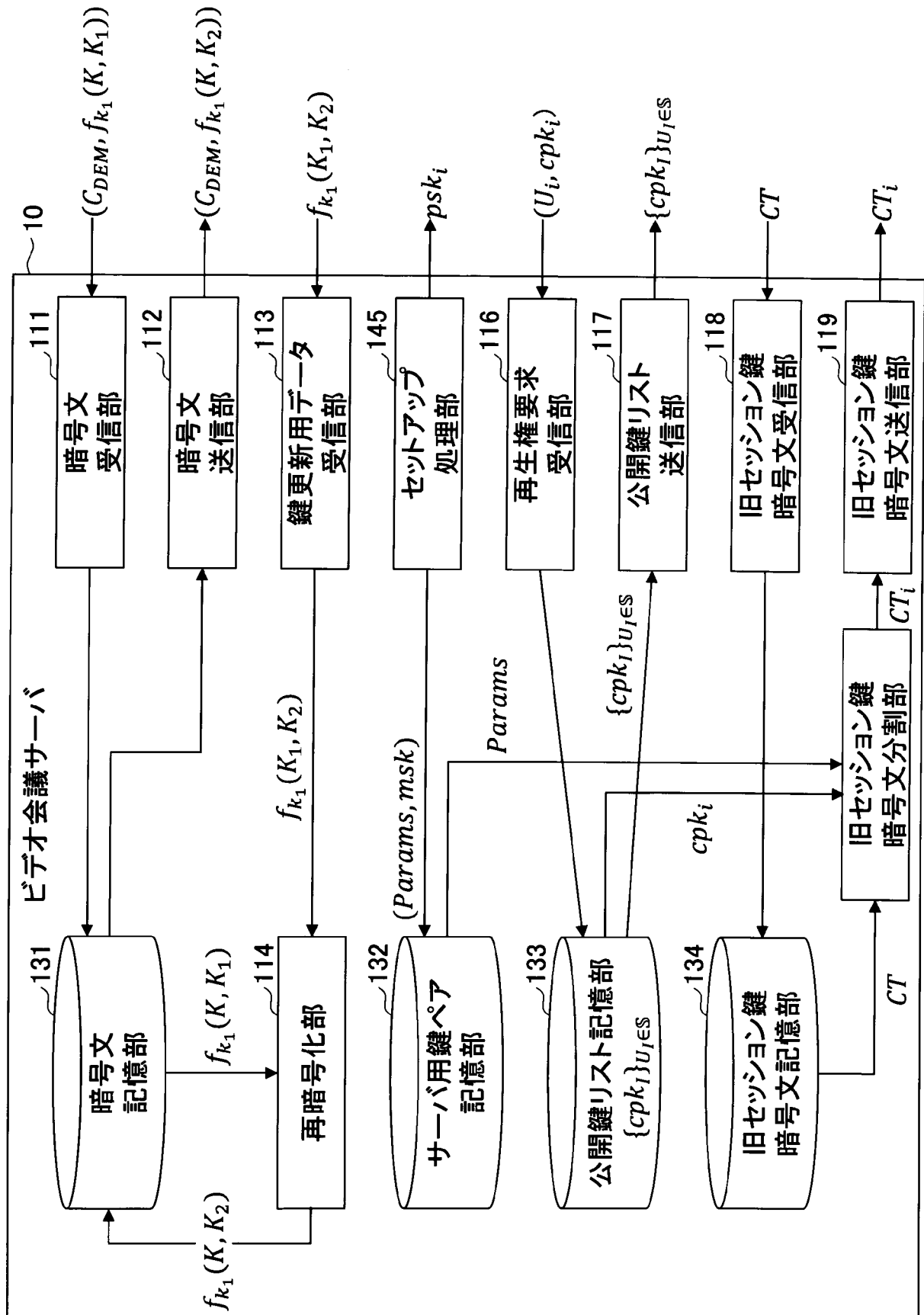


[図2]

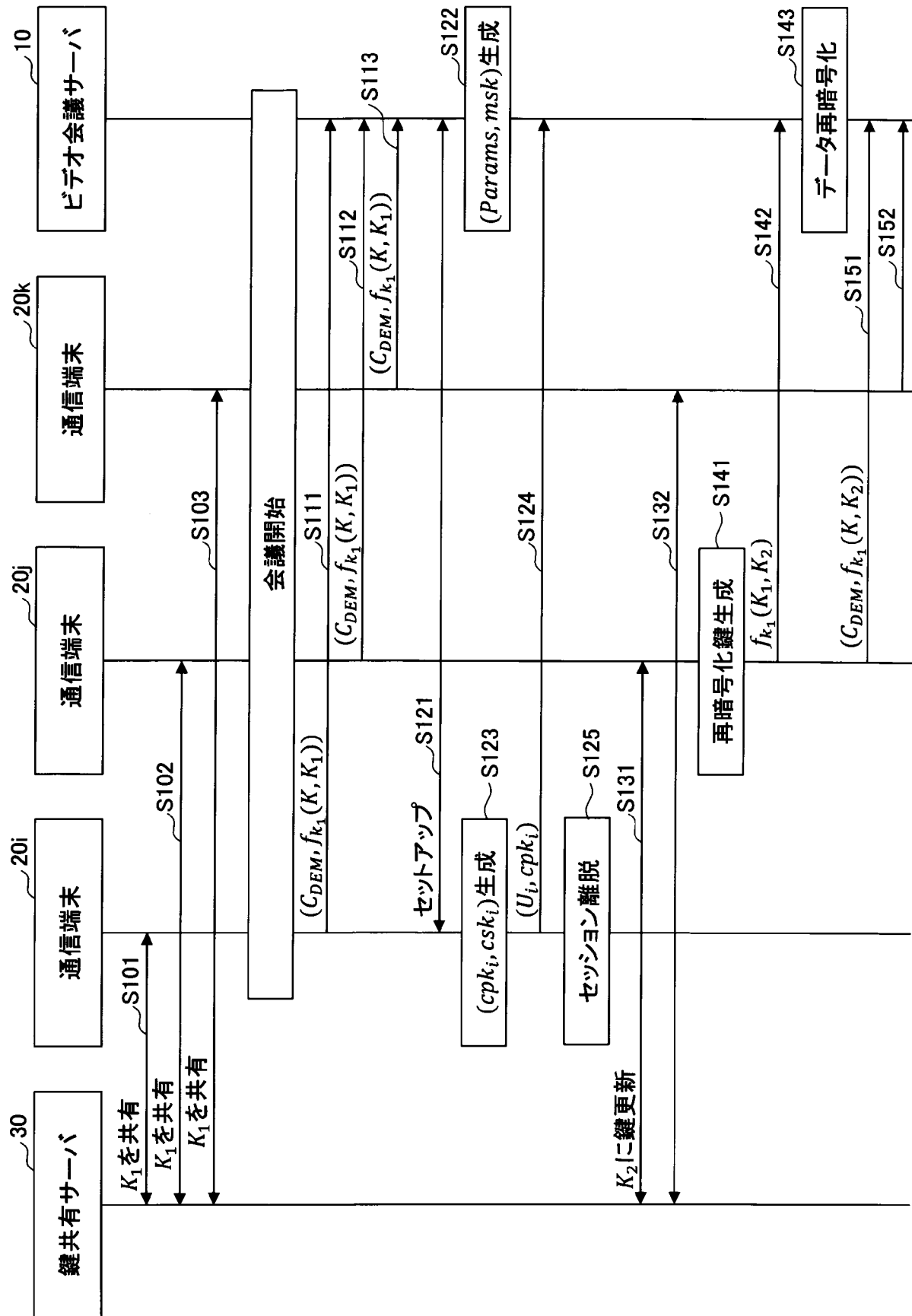
10



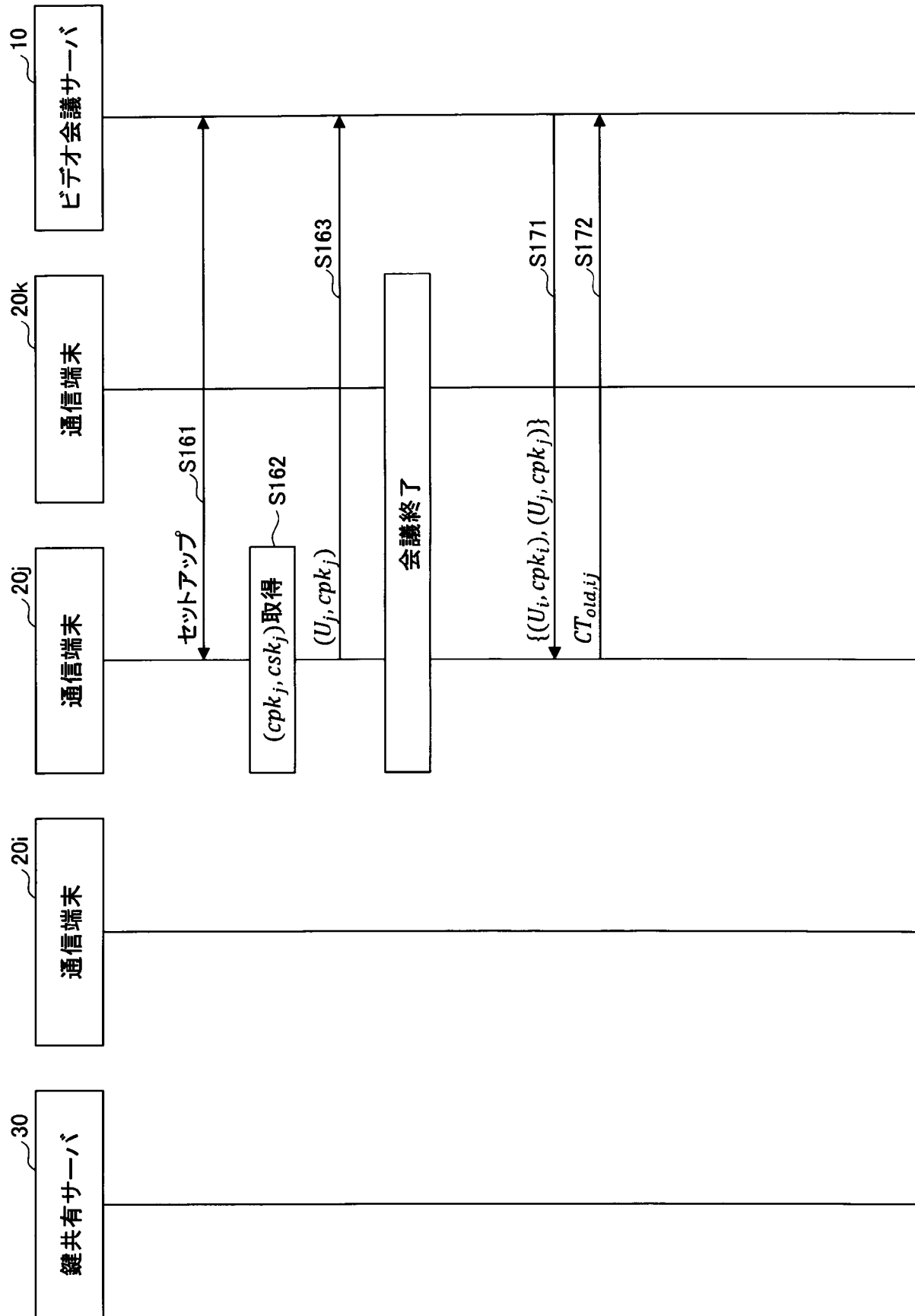
[図3]



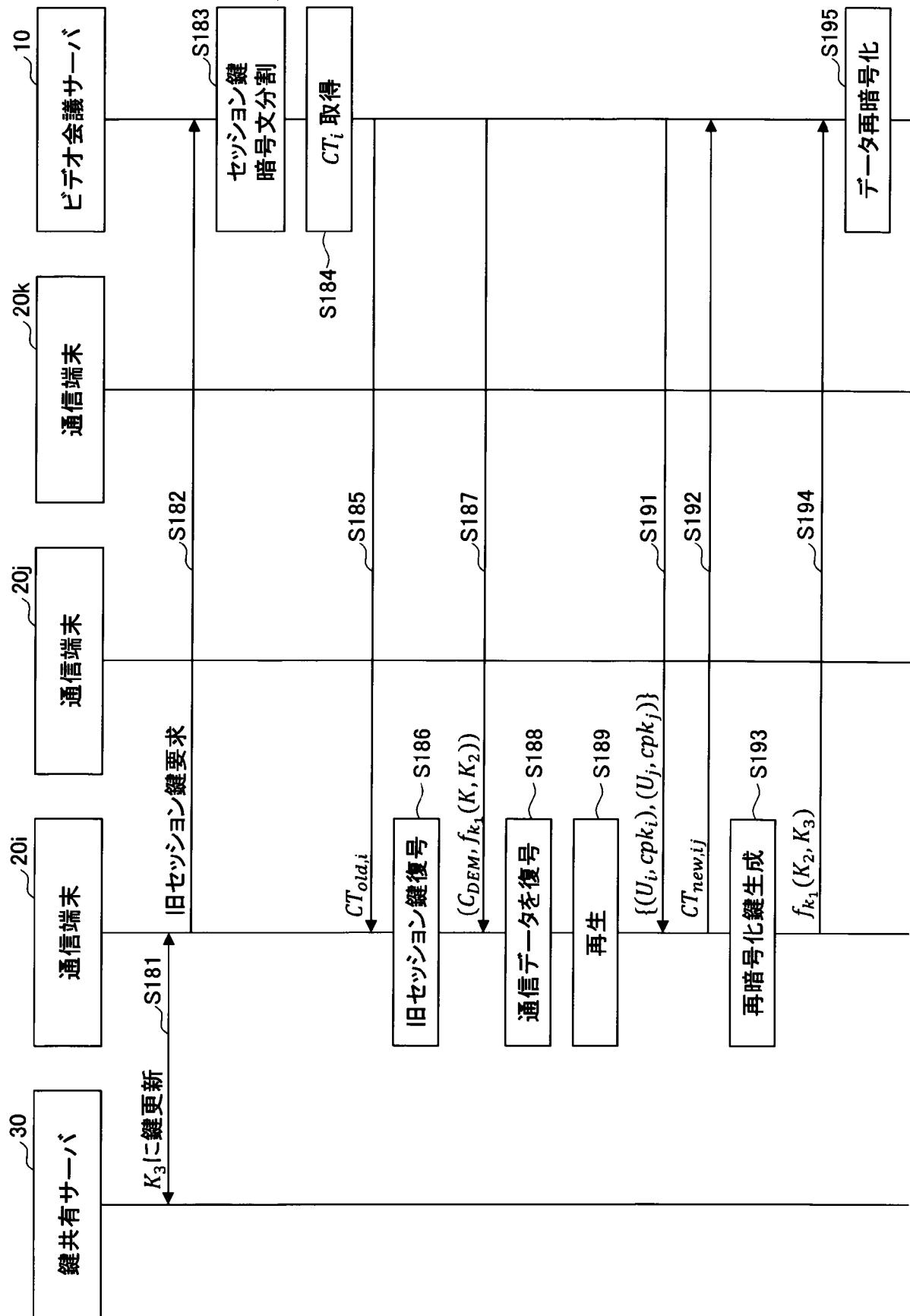
[図4]



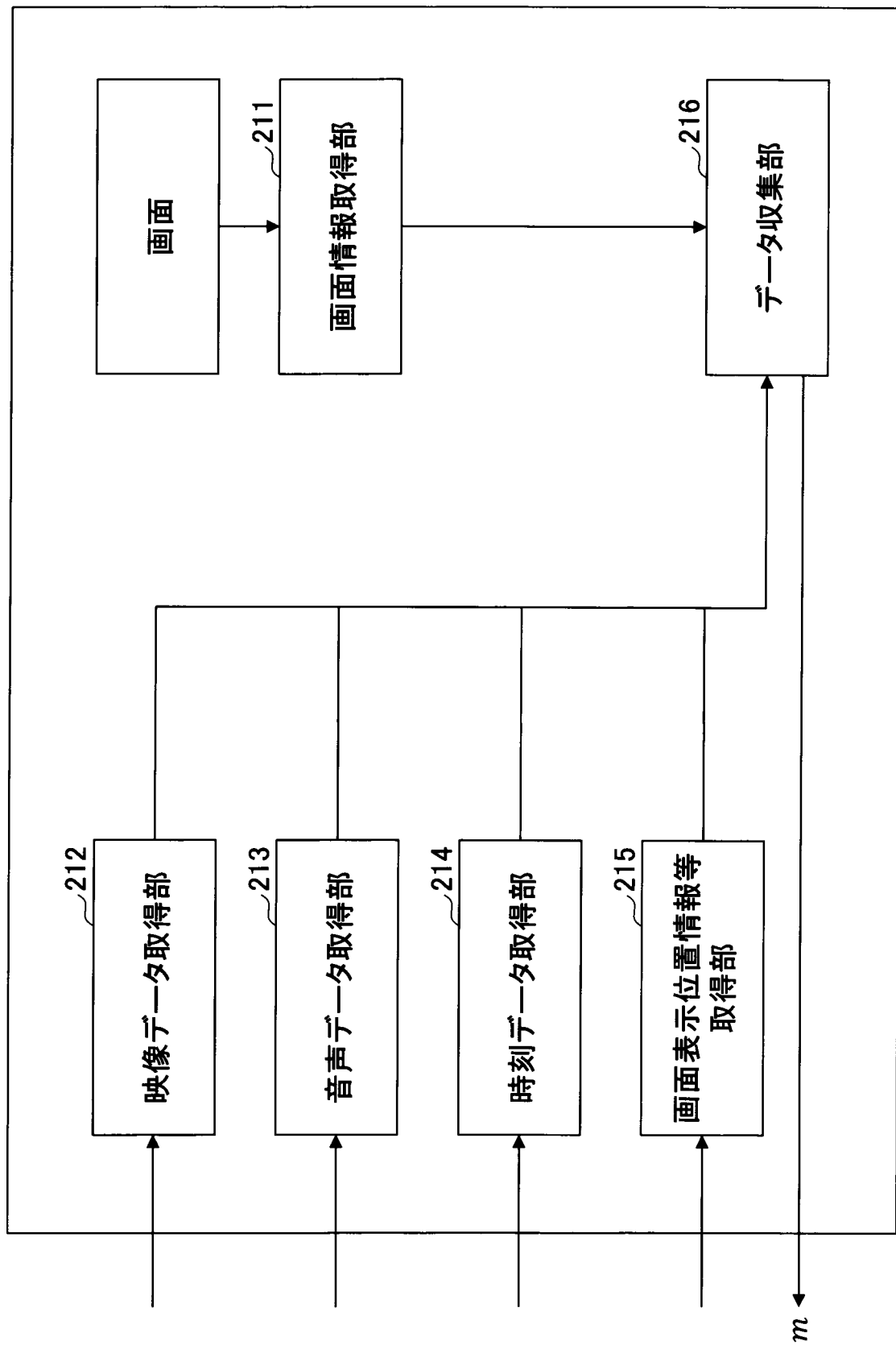
[図5]



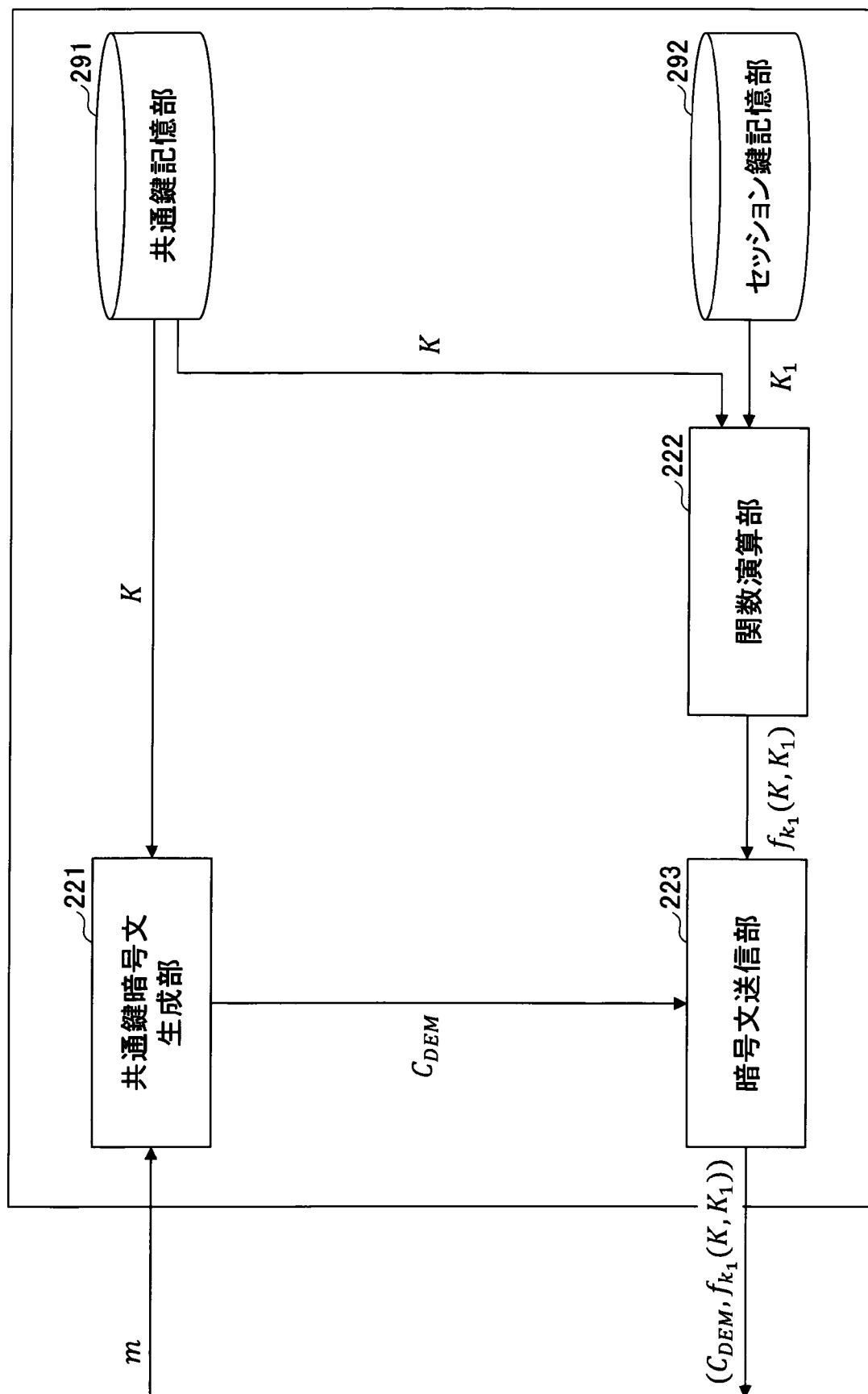
[図6]



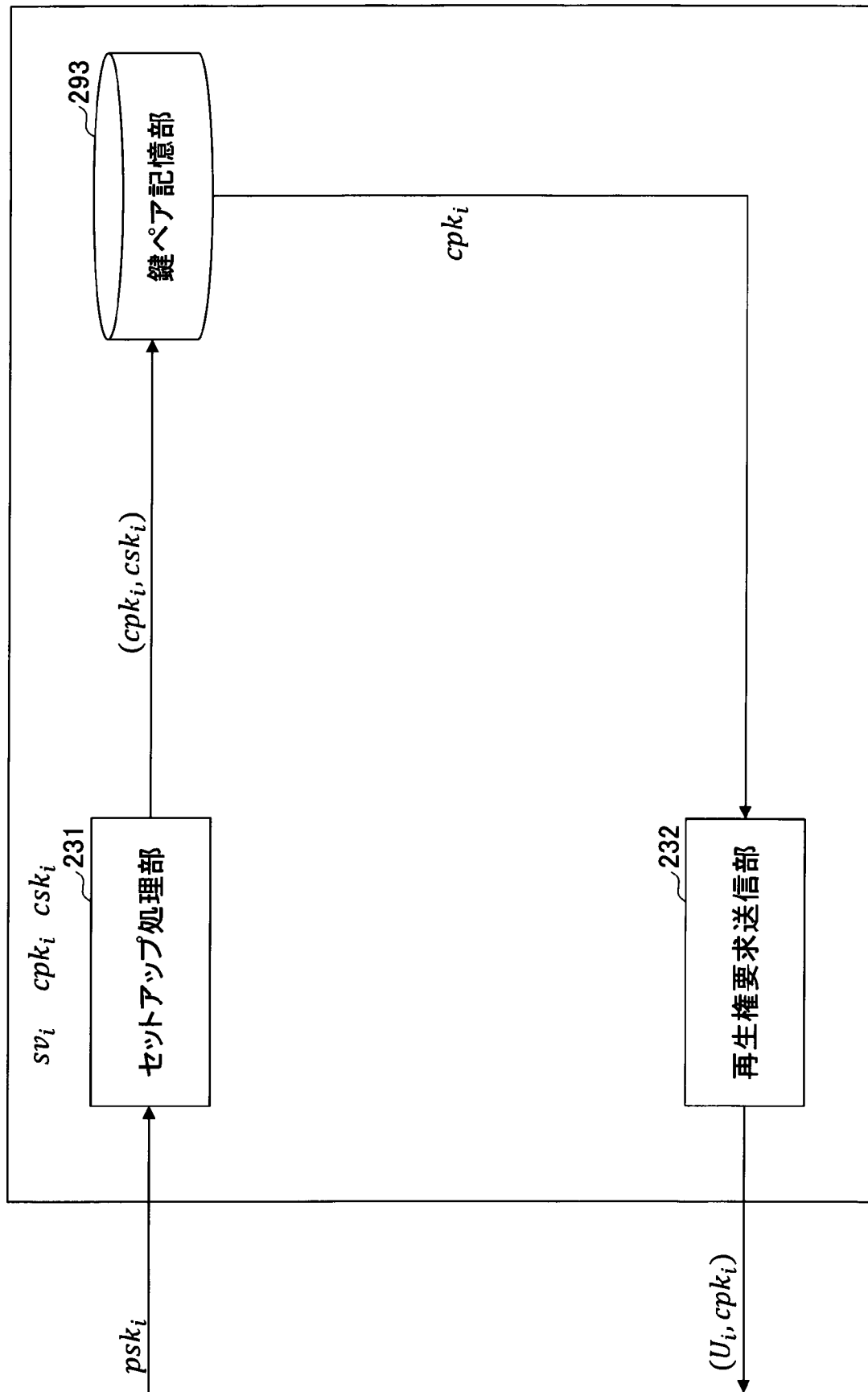
[図7]



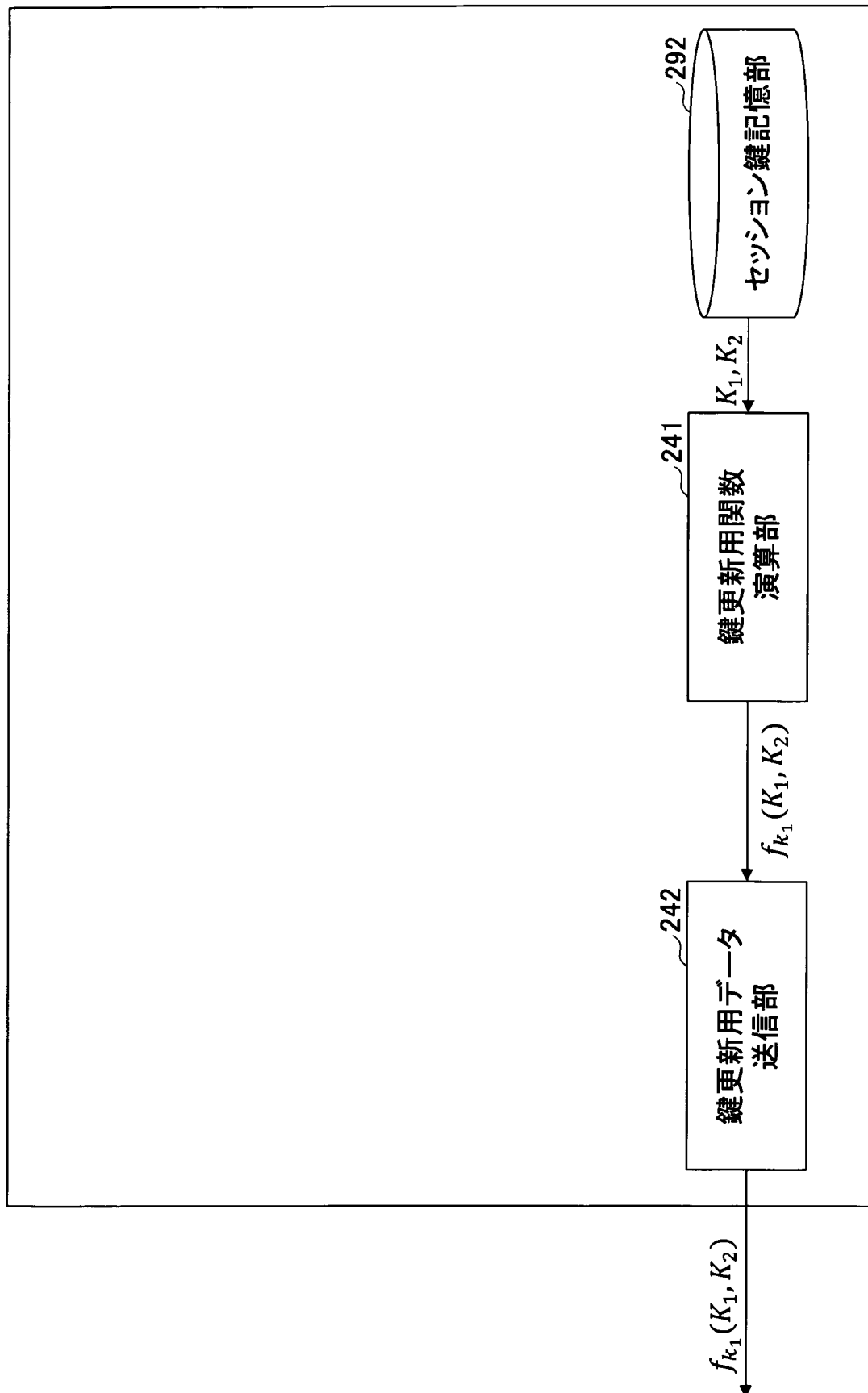
[図8]



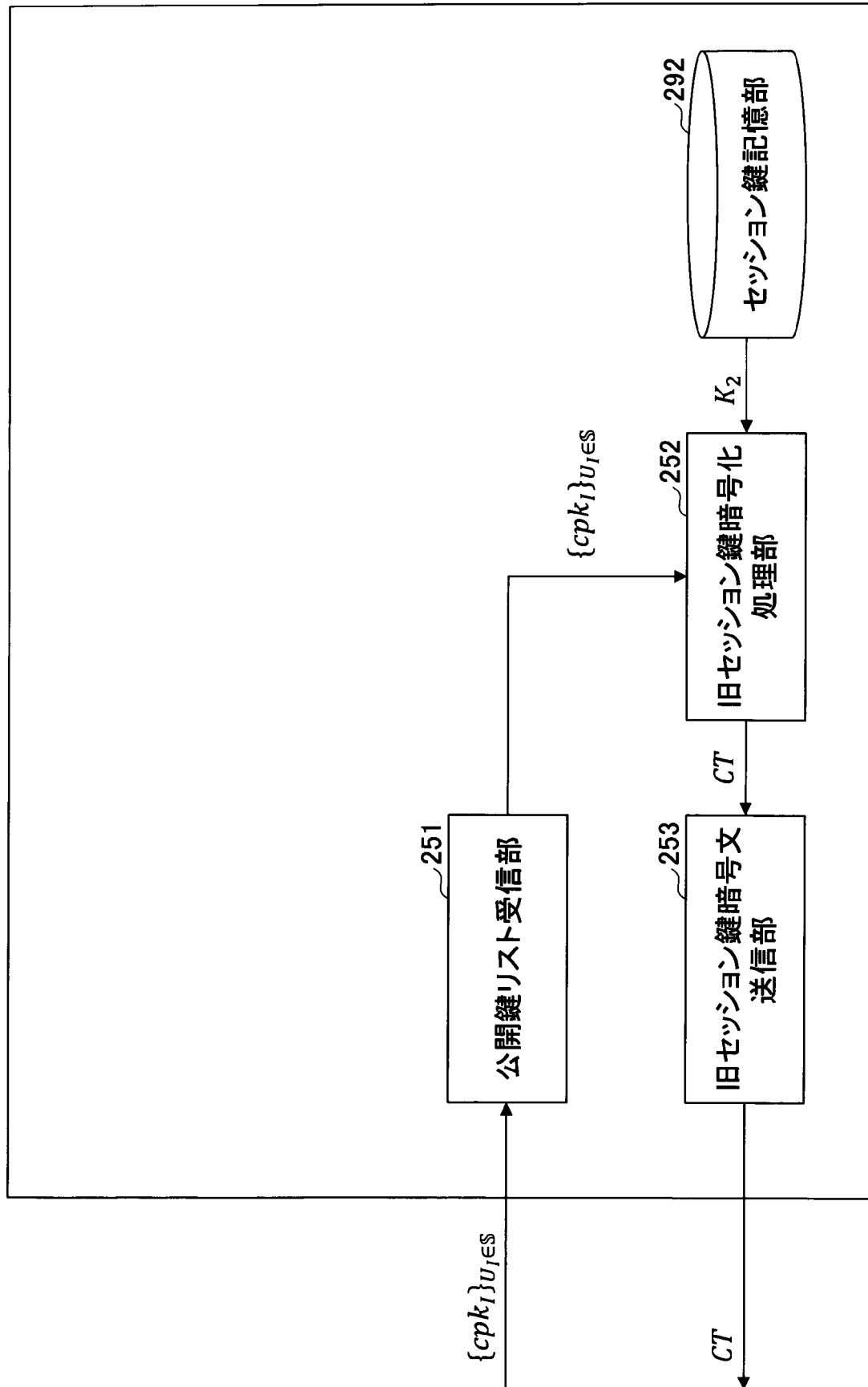
[図9]



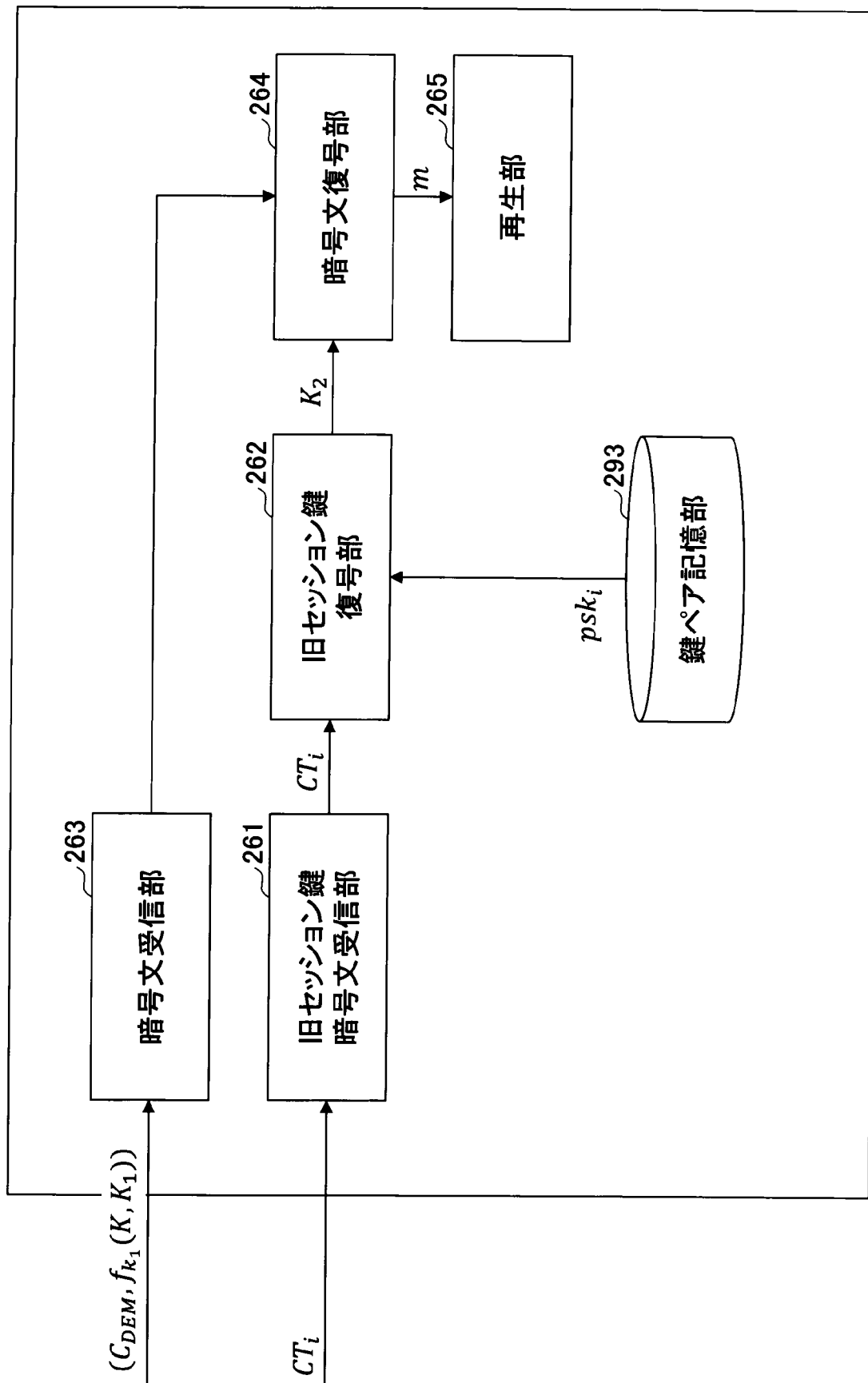
[図10]



[図11]



[図12]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/001111

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. H04N7/15 (2006.01) i

FI: H04N7/15 150

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)

Int. Cl. H04N7/15

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 1971-2021

Registered utility model specifications of Japan 1996-2021

Published registered utility model applications of Japan 1994-2021

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	WO 2020/085151 A1 (NIPPON TELEGRAPH AND TELEPHONE	4, 6
A	CORP.) 30 April 2020 (2020-04-30), paragraphs [0054], [0056], [0079]-[0096]	1-3, 5
A	JP 2010-219733 A (BROTHER INDUSTRIES, LTD.) 30 September 2010 (2010-09-30), paragraphs [0061], [0073]	1-3, 5

☐ 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
14.04.2021

Date of mailing of the international search report
27.04.2021

Name and mailing address of the ISA/
Japan Patent Office
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/JP2021/001111

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
WO 2020/085151 A1	30.04.2020	(Family: none)	
JP 2010-219733 A	30.09.2010	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） H04N 7/15(2006.01)i FI: H04N7/15 150														
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）） H04N7/15 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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2021年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2021年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2021年</td> </tr> </table> 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）			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2021年	日本国実用新案登録公報	1996 - 2021年	日本国登録実用新案公報	1994 - 2021年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2021年													
日本国実用新案登録公報	1996 - 2021年													
日本国登録実用新案公報	1994 - 2021年													
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	WO 2020/085151 A1（日本電信電話株式会社）30.04.2020（2020 - 04 - 30） 段落[0054], [0056], [0079]-[0096]	4, 6												
A		1-3, 5												
A	JP 2010-219733 A（ブラザー工業株式会社）30.09.2010（2010 - 09 - 30） 段落[0061], [0073]	1-3, 5												
☐ 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。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“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</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的技術水準を示すもの</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“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</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“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	“A” 特に関連のある文献ではなく、一般的技術水準を示すもの	“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	“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	“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	“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）	“&” 同一パテントファミリー文献	“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	
* 引用文献のカテゴリー	“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													
“A” 特に関連のある文献ではなく、一般的技術水準を示すもの	“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													
“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	“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													
“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）	“&” 同一パテントファミリー文献													
“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														
国際調査を完了した日 14.04.2021	国際調査報告の発送日 27.04.2021													
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） 富樫 明 5C 5890 電話番号 03-3581-1101 内線 3541													

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/JP2021/001111

引用文献			公表日	パテントファミリー文献	公表日
WO	2020/085151	A1	30.04.2020	(ファミリーなし)	
JP	2010-219733	A	30.09.2010	(ファミリーなし)	