

(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
2025年2月6日(06.02.2025)



(10) 国際公開番号

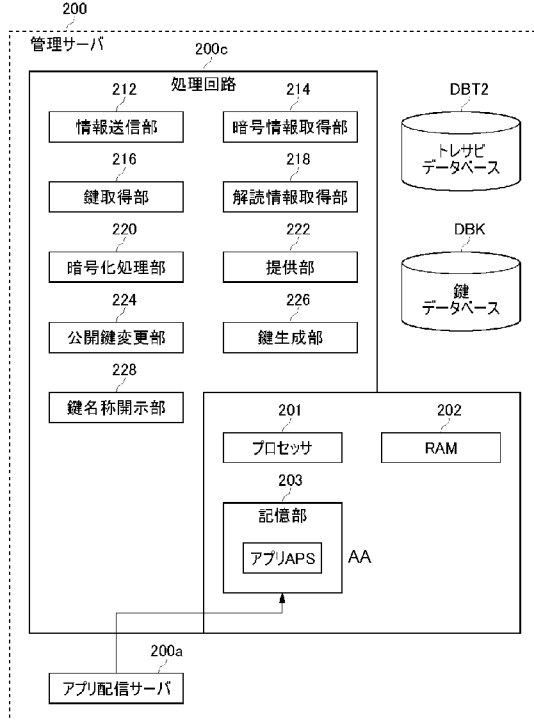
WO 2025/027967 A1

(51) 国際特許分類:
H04L 9/14 (2006.01) H04L 9/30 (2006.01)
(21) 国際出願番号: PCT/JP2024/017189
(22) 国際出願日: 2024年5月9日(09.05.2024)
(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 2023-125000 2023年7月31日(31.07.2023) JP
(71) 出願人: 株式会社デンソー (DENSO CORPORATION) [JP/JP]; 〒4488661 愛知県刈谷市昭和町1丁目1番地 Aichi (JP).

(72) 発明者: 岡部 達哉(OKABE Tatsuya); 〒4488661 愛知県刈谷市昭和町1丁目1番地 株式会社デンソー内 Aichi (JP). 並木 陽彦(NAMIKI Haruhiko); 〒4488661 愛知県刈谷市昭和町1丁目1番地 株式会社デンソー内 Aichi (JP). 中仙道 太郎(NAKASENDO Taro); 〒1100005 東京都台東区上野1丁目1-10 株式会社メイテック内 Tokyo (JP). 野吹 恭信(NOBUKI Yasunobu); 〒1100005 東京都台東区上野1丁目1-10 株式会社メイテック内 Tokyo (JP). 柿木 慎里仁(KAKINOKI Marito); 〒1100005 東京都台東区上野1丁目1-10 株式会社メイテック内 Tokyo (JP). 雲雀 恵太(HIBARI Keita); 〒1100005 東京都台東区上野1丁目1-10 株式会社メイテック内 Tokyo (JP).

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

(54) 発明の名称: 情報処理装置、情報処理システムおよび情報処理方法



200 Management server
200a Application distribution server
200c Processing circuit
201 Processor
203 Storage unit
212 Information transmission unit
214 Encrypted information acquisition unit
216 Key acquisition unit
218 Decrypted information acquisition unit
220 Encryption processing unit
222 Provision unit
224 Public key change unit
226 Key generation unit
228 Key name disclosure unit
DBK Key database
DBT2 Traceability database
AA Application APS

(57) Abstract: An information processing device (200) for managing item-related information relating to an item handled by a plurality of traders constituting a supply chain (SC) comprises: a database (DBK) in which each of multiple sets of secret keys based on homomorphic encryption and public keys corresponding to the respective secret keys is associated with a key name and stored; an encrypted information acquisition unit (214) that acquires, from a trader terminal (100) of a trader, encrypted information obtained by encrypting the item-related information using a public key, and the key

(74) 代理人: 鈴木 守, 外 (SUZUKI Mamoru et al.);
〒1500031 東京都渋谷区桜丘町 22-14
N. E. SビルS棟4F K S I パートナ
ーズ法律特許事務所 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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC,
EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,
HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG,
KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU,
LY, MA, MD, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS,
MW, MZ, NA, RW, SC, 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, ME, 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))

name of the public key used for encrypting the item-related information; a key acquisition unit (216) that acquires a secret key corresponding to the key name from the database; a decrypted information acquisition unit (218) that acquires decrypted information by decrypting the encrypted information using the secret key; an encryption processing unit (220) that encrypts the decrypted information to acquire re-encrypted information; and a provision unit (222) that provides the re-encrypted information obtained by encryption by the encryption processing unit to the trader terminal.

(57) 要約: サプライチェーン (SC) を構成する複数の取引者が扱うアイテムに関するアイテム関連情報を管理する情報処理装置 (200) は、準同型暗号に基づく秘密鍵および該秘密鍵に対応する公開鍵の複数セットのそれぞれを、鍵名称と紐づけて記憶しているデータベース (DBK) と、取引者の取引者端末 (100) から、公開鍵を用いてアイテム関連情報を暗号化した暗号情報と、アイテム関連情報の暗号化に用いた公開鍵の鍵名称とを取得する暗号情報取得部 (214) と、鍵名称に対応する秘密鍵をデータベースから取得する鍵取得部 (216) と、該秘密鍵を用いて暗号情報を解読することで解読情報を取得する解読情報取得部 (218) と、解読情報を暗号化して再暗号情報を取得する暗号化処理部 (220) と、暗号化処理部により暗号化された再暗号情報を取引者端末に提供する提供部 (222) と、を有する。

明 細 書

発明の名称：

情報処理装置、情報処理システムおよび情報処理方法

関連出願の相互参照

[0001] 本出願は、2023年7月31日に出願された日本出願番号2023-125000号に基づくもので、ここにその記載内容を援用する。

技術分野

[0002] この明細書による開示は、情報処理装置に関する。

背景技術

[0003] 消費者やユーザの環境、デューデリジェンス、トレーサビリティに関する意識の高まりにより、製品の原材料、リサイクル率、カーボンフットプリント（CFP）、環境負荷物質などの開示要求や開示義務化の流れが強まっている。一方で、開示要求をされる企業にとっては、原材料、リサイクル率、CFP等の情報開示は、競争の源泉であるトレードシークレットを開示することに等しく、開示への抵抗感が強い。

[0004] 特に、欧州電池法規などを代表例として、まずはCFPの開示要求が高まっている。CFPは一件、単なる二酸化炭素排出量だけの情報には見えるが、同業他社にとってはCFP値が分かることで、大まかな原材料や加工方法なども推定がつく為に、トレードシークレットとなっているケースが多い。また、CFP値が購買行動に直接影響を及ぼし、値切りなどにもつながる可能性がある為、開示を嫌がるケースが多い。

[0005] 特許文献1には、複数の取引者を含んで構築されるサプライチェーンにおいて、各取引者間での取引記録を管理するサプライチェーン管理方法が開示されている。

[0006] また、特許文献2には、ユーザ公開鍵により暗号化された暗号化データに対して準同型演算を行い、準同型演算の演算結果を、マスタ秘密鍵を用いて復号可能な暗号システムが開示されている。

先行技術文献

特許文献

[0007] 特許文献1：国際公開第2021/002226号公報

特許文献2：特開2018-36418号公報

発明の概要

[0008] しかしながら、特許文献2に開示された通常の暗号システムをサプライチェーンの情報管理に単に利用しただけでは、監督官庁やサプライチェーン管理団体等とサーバ等で秘密鍵のやり取りや、解読した値のやり取りなどがネットワーク上で必要となる。ネットワーク自体のセキュリティが担保されていたとしても、悪意のあるハッカーなどが傍受をし、不正に入手した秘匿鍵などで解読した値などを見られてしまう可能性があるため、さらなるセキュリティの強化を図る必要がある。

[0009] 本開示は、ネットワーク上で秘密鍵及び解読した値のやり取りを一切行わない、セキュリティの強化された情報処理装置、情報処理システム及び情報処理方法の提供を目的とする。

[0010] 上記目的を達成するため、開示された一つの態様は、サプライチェーンを構成する複数の取引者が扱うアイテムに関するアイテム関連情報を管理する情報処理装置であって、準同型暗号に基づく秘密鍵および該秘密鍵に対応する公開鍵の複数セットのそれぞれを、鍵名称と紐づけて記憶しているデータベースと、取引者の取引者端末から、公開鍵を用いてアイテム関連情報を暗号化した暗号情報と、アイテム関連情報の暗号化に用いた公開鍵の鍵名称とを取得する暗号情報取得部と、鍵名称に対応する秘密鍵を前記データベースから取得する鍵取得部と、該秘密鍵を用いて暗号情報を解読することで解読情報を取得する解読情報取得部と、解読情報を暗号化して再暗号情報を取得する暗号化処理部と、暗号化処理部により暗号化された再暗号情報を取引者端末に提供する提供部と、を有する情報処理装置とされる。

[0011] また開示された一つの態様は、上記情報処理装置と、取引者の取引者端末と、を備える情報処理システムとされる。

[0012] また開示された一つの態様は、サプライチェーンを構成する複数の取引者が扱うアイテムに関するアイテム関連情報を管理する情報処理方法であって、準同型暗号に基づく秘密鍵および該秘密鍵に対応する公開鍵の複数セットのそれぞれを、鍵名称と紐づけてデータベースに記録するステップと、取引者の取引者端末から、公開鍵を用いてアイテム関連情報を暗号化した暗号情報と、アイテム関連情報の暗号化に用いた公開鍵の鍵名称とを取得するステップと、鍵名称に対応する秘密鍵をデータベースから取得するステップと、該秘密鍵を用いて暗号情報を解読することで解読情報を取得するステップと、解読情報を暗号化して再暗号情報を取得するステップと、再暗号情報を取引者端末に提供するステップと、を有する情報処理方法とされる。

[0013] これらの態様では、公開鍵を用いて暗号化された暗号情報と、暗号化に用いた鍵名称とを取引者端末から取得し、取得した鍵名称から秘密鍵を検索し暗号情報を解読し、解読した情報に基づく再暗号情報を取引者端末に提供する処理を行う。以上によれば、情報処理装置内で秘密鍵を使用することにより、秘密鍵の配布を行う必要がない。このため、ネットワーク自体のセキュリティが担保されていたとしても、悪意のあるハッカーなどが傍受をし、不正に入手した秘密鍵で解読した値を見られてしまう事態を防ぐことができ、セキュリティを向上することができる。さらに、情報処理装置から取引者端末へ送信される情報は暗号化されているため、ハッカーに傍受されたとしても実際の値を知られることはなく、セキュリティを向上することができる。

[0014] 尚、上記及び特許請求の範囲における括弧内の参照番号は、後述する実施形態における具体的な構成との対応関係の一例を示すものにすぎず、技術的範囲を何ら制限するものではない。また、特に組み合わせに支障が生じなければ、特許請求の範囲において明示していない請求項同士の組み合わせも可能である。

図面の簡単な説明

[0015] 本開示についての上記目的およびその他の目的、特徴や利点は、添付の図面を参照しながら下記の詳細な記述により、より明確になる。その図面は、

- [図1]図1は、本開示の実施形態でのサプライチェーンの例を示す図であり、
- [図2]図2は、サプライチェーン管理システムの全体像を示す図であり、
- [図3]図3は、取引者端末の構成を示すブロック図であり、
- [図4]図4は、管理サーバの構成を示すブロック図であり、
- [図5]図5は、監督官庁・CFP管理団体サーバの構成を示すブロック図であり、
- [図6]図6は、異なる公開鍵で暗号化されている数値の四則演算の詳細を示すフローチャートであり、
- [図7]図7は、ブートストラッピング処理の詳細を示すフローチャートであり、
- [図8]図8は、データ開示要求の詳細を示すフローチャートであり、
- [図9]図9は、秘密鍵及び公開鍵の生成の詳細を示すフローチャートであり、
- [図10]図10は、鍵名称の配布の詳細を示すフローチャートであり、
- [図11]図11は、前工程がない場合における追加・統合工程時の準同型暗号を用いたCFP計算の詳細を示すフローチャートであり、
- [図12]図12は、前工程がある場合における追加・統合工程時の準同型暗号を用いたCFP計算の詳細を示すフローチャートであり、
- [図13]図13は、分岐工程時の準同型暗号を用いたCFP計算の詳細を示すフローチャートであり、
- [図14]図14は、前工程の公開鍵が異なる場合における準同型暗号を用いたCFP計算の詳細を示すフローチャートであり、
- [図15]図15は、乗算・除算回数が上限値に到達したときの準同型暗号を用いたCFP計算の詳細を示すフローチャートであり、
- [図16]図16は、乗算・除算の計算回数をクリアしたいときの準同型暗号を用いたCFP計算の詳細を示すフローチャートであり、
- [図17]図17は、監督官庁・CFP管理団体からのCFP値の開示要求があった場合の処理の詳細を示すフローチャートであり、
- [図18]図18は、監督官庁・CFP管理団体以外からのCFP値の開示要求

があった場合の処理の詳細を示すフローチャートである。

発明を実施するための形態

[0016] 以下、本開示の実施形態を図面に基づいて説明する。尚、実施形態において対応する構成要素には同一の符号を付すことにより、重複する説明を省略する場合がある。

[0017] 図1は、本開示の実施形態でのサプライチェーンの例を示す図である。図1に示すサプライチェーンSCは、工業製品、農業製品及び水産物等をエンドユーザに届けるための取引者同士の繋がりである。サプライチェーンSCは、多数の取引者（図1 企業A～F参照）によって構築されている。サプライチェーンSCによって供給される最終製品は、例えば自動車、バッテリー、半導体、生鮮食品、水産物、食品、花き類、医薬品、及び化学薬品等、種々の物品であってよい。

[0018] 図1の例では、企業Cは、企業Aから製品Aを仕入れ、企業Bから製品Bを仕入れ、最終製品Cを製造する。企業Cは、製品Cを消費者であるユーザに届け、ユーザは企業Dにリサイクル品として製品Cを売る。企業Dは、製品Cを修理し製品Dを製造し、企業Eと企業Fに製品Dの一部をそれぞれ納品し、企業Eと企業Fはそれぞれ製品Eと製品Fを製造する。

[0019] 図2は、サプライチェーン管理システム1の全体像を示す図である。本開示の実施形態によるサプライチェーン管理システム1は、サプライチェーンSCにおいて、各取引者間にて取引されるアイテムの取引記録を、各取引者に紐づく情報として管理する。取引記録は、取引者間で取引されるアイテムのトレーサビリティ（以下、トレサビと称する場合がある）を実現する履歴情報であり、取引が発生した時間及び場所等を示す多数の情報を含んでいる。

[0020] サプライチェーン管理システム1は、取引記録に加えて、取引対象となるアイテムに関連するアイテム関連情報をさらに管理する。例えば、原材料に関わる情報、加工及び組立に関わる情報、並びに流通に関わる情報等が、アイテム関連情報として管理される。さらに、サプライチェーン管理システム

1 は、アイテム関連情報の一つとして、アイテムの製造及び流通の各過程において排出される温室効果ガスの排出量（以下、カーボンフットプリント）（C F P）に関連する情報の収集及び蓄積を行う。

[0021] サプライチェーン管理システム 1 は、各取引者の C F P 値を取得し、ユーザ、監督官庁及び C F P 管理団体等に提示可能である。C F P には、アイテムの原材料の採掘及びリサイクル等の工程でのカーボンリリース量、並びにアイテムの焼却及び埋め立て等の廃棄に関連する工程でのカーボンリリース量が含まれていてもよい。

[0022] 尚、排出量が記録される温室効果ガスは、二酸化炭素のみであってもよく、二酸化炭素以外の温室効果ガス、具体的には、メタン、亜酸化窒素、ハイドロフルオロカーボン類、パーフルオロカーボン類及び六フッ化硫黄等を適宜含んでいてもよい。この場合、二酸化炭素以外の温室効果ガスの排出量は、二酸化炭素の排出量に換算されて、提示されるカーボンフットプリントの値に算入される。

[0023] ここで、C F P 値は、各取引者 T R におけるトレードシークレットであることが多い。これは、C F P 値から、大まかな原材料及び加工方法等が類推され得るためである。故に、C F P 値を他の取引者及び消費者等へ開示したくないという企業が多くなる。こうした背景を受けて、サプライチェーン管理システム 1 は、ネットワーク上で、秘密鍵及び各取引者の C F P 値を解読した数値のやり取りを一切しない秘密計算を行う。以下、サプライチェーン管理システム 1 の詳細を、図 2 ～図 5 に基づき説明する。

[0024] サプライチェーン管理システム 1 は、多数の取引者端末 1 0 0、管理サーバ 2 0 0、アプリ配信サーバ 2 0 0 a、及び監督官庁・C F P 管理団体サーバ 3 0 0 によって構成されている。サプライチェーン管理システム 1 を構成する各要素は、それぞれ一つのノードとしてネットワークに接続されており、互いに通信可能である。

[0025] <取引者端末 1 0 0>

図 3 は、取引者端末 1 0 0 の構成を示すブロック図である。取引者端末 1

１００は、個々の取引者によって運用される情報処理装置である。例えば、スマートフォン、タブレット端末、及びパーソナルコンピュータ等が取引者端末１００として利用可能である。取引者端末１００は、個々の企業Ａ～Ｆ（図１参照）にそれぞれ紐づいている。取引者端末１００は、各取引者において利用され、取引記録及びアイテム関連情報の収集及び蓄積を行う。取引者端末１００は、どのような取引者から原材料又は部品等を購入しているか、いつ取得したものなのか等の納入情報、及びどのような取引者へ向けていつ出荷したのか等の出荷情報を、取引記録として記録する。さらに、取引者端末１００は、コストに関連する情報及びＣＦＰ値等を少なくともアイテム関連情報として記録する。

[0026] 取引者端末１００は、処理回路１００ｃを主体とする構成である。処理回路１００ｃは、プロセッサ１０１、ＲＡＭ（Random Access Memory）１０２、記憶部１０３、入出力インターフェース及びこれらを接続するバス等を備え、演算処理を実施するコンピュータとして機能する。プロセッサ１０１は、ＲＡＭ１０２と結合された演算処理のためのハードウェアである。記憶部１０３には、本開示による情報処理方法を処理回路１００ｃに実行させるためのアプリケーションプログラム（情報管理アプリＡＰＴ）が格納されている。入出力インターフェースには、ディスプレイ、コードリーダー（又はカメラ）、及びプリンタ等が電氣的に接続されている。ディスプレイ、コードリーダー、及びプリンタは、取引者端末１００と一体的な構成であってもよく、取引者端末１００に有線又は無線によって電気接続される構成であってもよい。

[0027] 取引者端末１００は、記憶部１０３に格納された情報管理アプリＡＰＴをプロセッサ１０１が実行することにより、鍵名称管理部１１２、ＵＩＤ読込部１１４、情報取得部１１６、情報演算部１１８、情報送信部１２０、専用鍵生成部１２２、送付要求送信部１２４、コード生成部１２６等の機能部を有する。

[0028] 鍵名称管理部１１２は、準同型暗号に基づく秘密鍵及び公開鍵のセットの

鍵名称を管理する。本実施形態の取引者端末100では、秘密鍵及び公開鍵のセットを管理せず、鍵名称のみを管理する。秘密鍵及び公開鍵は、トレードシークレットに相当するアイテム関連情報の暗号化及び復号に用いられる。準同型暗号は、暗号化したデータを復号することなく、暗号化したままデータの処理を行うことが可能な暗号方式である。準同型暗号の一つとして、例えばFHE (Fully Homomorphic Encryption) 等の完全準同型暗号を利用する。完全準同型暗号は、暗号化したままの加算、減算、乗算及び除算を可能にする。完全準同型暗号に替えて、RSA暗号及びElGamal暗号等の乗法準同型暗号、並びにGoldwasser-Micali暗号、Paillier暗号等の加法準同型暗号が、後述する秘密計算の処理内容に応じて利用可能である。

[0029] UID読込部114は、アイテムに添付される1次元コードまたは2次元コード等のコード（例えば、QRコード（登録商標））を読み込むコードリーダーである。コードには、取引記録及びアイテム関連情報から生成される固有の識別ID（以下、UID）が記録されている。

[0030] 情報取得部116は、UID読込部114によって読み取られUIDを引数として、管理サーバ200にアイテムの取引記録、アイテム関連情報及び鍵名称を含む情報（以下、トレサビ情報）を要求する。そして、情報取得部116は、読み取ったUIDに対応するトレサビ情報を管理サーバ200から取得する。アイテム関連情報には、取引者がアイテムに行う処置（例えば、加工、組み立て、輸送、及び保管等）に関連した情報に加えて、上述したCFP値に関する情報が含まれる。

[0031] 情報取得部116は、アイテムの各UIDに紐づけた状態で、トレサビ情報をトレサビデータベースDBT1に格納する。情報取得部116は、UIDを検索のキーとすることで、UIDに対応するトレサビ情報を、トレサビデータベースDBT1に蓄積されたデータの中から抽出する。尚、トレサビデータベースDBT1は、取引者の拠点に設けられたローカルな記憶装置であってもよく、又はクラウド上のストレージであってもよい。

[0032] 情報演算部118は、トレサビ情報に関連する種々の演算を実施する。情

報演算部 118 の具体的な処理については後述する。

[0033] 情報送信部 120 は、取引者端末 100 にて収集されたトレサビ情報を管理サーバ 200 に送信する。情報送信部 120 は、コード生成部 126 にて生成された U I D に紐づけて、トレサビ情報を管理サーバ 200 に送信する。

[0034] 専用鍵生成部 122 は、取引者端末 100 を扱う取引者専用の秘密鍵及び公開鍵のセットを生成する。取引者専用の秘密鍵及び公開鍵のセットは、管理サーバ 200 の鍵データベース D B K 内には含まれない。生成した取引者専用の秘密鍵及び公開鍵のセットは、専用鍵データベース D B S K 1 に記録される。

[0035] 送付要求送信部 124 は、管理サーバ 200 に対して種々の送付要求を送信する。

[0036] コード生成部 126 は、プリンタと接続されている。コード生成部 126 は、2次元コード等が印刷されたラベルをプリンタに出力させる。ラベルは、出荷アイテムに添付され、出荷アイテムと共に次工程の取引者に流通する。尚、2次元コードは、アイテムに直接的にレーザー刻印又は印字等されていてもよい。この場合、プリンタに替えて、レーザーマーカ―又はインクジェットプリンタ等が出力機器として利用可能である。

[0037] <管理サーバ 200>

図 4 は、管理サーバ 200 の構成を示すブロック図である。管理サーバ 200 及びアプリ配信サーバ 200 a は、サプライチェーン S C の管理者によって運用されるサーバ装置である。管理者は、例えばサプライチェーン S C によって供給される最終製品の提供者（完成品メーカー）から管理業務を委託された代行業者である。管理者は、最終製品の属するカテゴリに対し監督権限を持つ監督官庁から管理及び監査の業務を委託された代行機関であってもよい。管理サーバ 200 及びアプリ配信サーバ 200 a は、管理者又はシステムサプライヤ等によって物理的に管理されるオンプレミスな構成であってもよく、クラウド上に設けられた仮想のサーバ構成であってもよい。

[0038] 管理サーバ200は、処理回路200cを主体とする情報処理装置である。処理回路200cは、プロセッサ201、RAM202、記憶部203、入出力インターフェース及びこれらを接続するバス等を備え、演算処理を実施するコンピュータとして機能する。プロセッサ201は、RAM202と結合された演算処理のためのハードウェアであり、記憶部203に格納されたプログラムを実行する。

[0039] 管理サーバ200は、サプライチェーンSCを構成する複数の取引者が扱うアイテムに関するアイテム関連情報を管理する管理者側の情報処理装置である。記憶部203には、本開示による情報処理方法を処理回路200cに実施させるためのアプリケーションプログラム（情報管理アプリAPS）が格納されている。管理サーバ200は、プロセッサ201による情報管理アプリAPSの実行により、情報送信部212、暗号情報取得部214、鍵取得部216、解読情報取得部218、暗号化処理部229、提供部222、公開鍵変更部224、鍵生成部226、鍵名称開示部228等の機能部を有する。管理サーバ200は、準同型暗号に基づく秘密鍵および該秘密鍵に対応する公開鍵の複数セットのそれぞれを、鍵名称と紐づけて記憶している鍵データベースDBKを備える。

[0040] 情報送信部212は、取引者端末100から要求されたトレサビ情報をトレサビデータベースDBT2から抽出し、取引者端末100に送信する。

[0041] 暗号情報取得部214は、取引者端末100から、公開鍵を用いてアイテム関連情報を暗号化した暗号情報と、該アイテム関連情報の暗号化に用いた公開鍵の鍵名称とを取得する。なお、暗号情報取得部214は、取引者端末100から、トレサビ情報を取得する情報取得部としても機能する。暗号情報取得部214が取得したトレサビ情報は、トレサビデータベースDBT2にてUIDに紐づけて記録される。

[0042] 鍵取得部216は、鍵名称に対応する秘密鍵を鍵データベースDBKから取得する。

[0043] 解読情報取得部218は、秘密鍵を用いて、アイテム関連情報を暗号化し

た暗号情報を解読することで解読情報を取得する。

[0044] 暗号化処理部 220 は、解読情報を暗号化して再暗号情報を取得する。

[0045] 提供部 222 は、暗号化処理部 220 により暗号化され再暗号情報を取り引者端末 100 に提供する。

[0046] 公開鍵変更部 224 は、公開鍵 A で暗号化された暗号情報を、公開鍵 A とは異なる公開鍵 B で暗号化した暗号情報に変更する。

[0047] 鍵生成部 226 は、監督官庁・CFP 管理団体から作成を要求された秘密鍵及び公開鍵のセットを生成する。

[0048] 鍵名称開示部 228 は、作成した秘密鍵及び公開鍵のセットの鍵名称を開示する。例えば、鍵名称開示部 228 は、鍵の作成を要求した監督官庁・CFP 管理団体に作成した鍵の鍵名称を開示する。

[0049] <監督官庁・CFP 管理団体サーバ 300>

図 5 は、監督官庁・CFP 管理団体サーバ 300 の構成を示すブロック図である。監督官庁・CFP 管理団体サーバ 300 は、監督官庁または CFP 管理団体によって運用されるサーバ装置である。監督官庁・CFP 管理団体サーバ 300 は、監督官庁または CFP 管理団体によって物理的に管理されるオンプレミスな構成であってもよく、クラウド上に設けられた仮想のサーバ構成であってもよい。

[0050] 監督官庁・CFP 管理団体サーバ 300 は、処理回路 300c を主体とする情報処理装置である。処理回路 300c は、プロセッサ 301、RAM 302、記憶部 303、入出力インターフェース及びこれらを接続するバス等を備え、演算処理を実施するコンピュータとして機能する。プロセッサ 301 は、RAM 302 と結合された演算処理のためのハードウェアであり、記憶部 303 に格納されたプログラムを実行する。

[0051] 監督官庁・CFP 管理団体サーバ 300 は、監督官庁または CFP 管理団体の情報処理装置である。記憶部 203 には、本開示による情報処理方法を処理回路 300c に実施させるためのアプリケーションプログラム（情報管理アプリ APR）が格納されている。監督官庁・CFP 管理団体サーバ 300

0は、プロセッサ301による情報管理アプリAPRの実行により、UID読込部312、情報取得部314、情報演算部316、鍵生成要求部318、専用鍵生成部320、送付要求送信部322等の機能部を有する。

[0052] UID読込部312は、アイテムに添付される1次元コードまたは2次元コード等のコード（例えば、QRコード（登録商標））を読み込むコードリーダーである。コードには、取引記録及びアイテム関連情報から生成される固有のUIDが記録されている。

[0053] 情報取得部314は、UID読込部312によって読み取られたUIDを引数として管理サーバ200にトレサビ情報を要求し、読み取ったUIDに対応するトレサビ情報を管理サーバ200から取得する。

[0054] 情報演算部316は、トレサビ情報に関連する種々の演算を実施する。情報演算部316の具体的な処理については後述する。

[0055] 鍵生成要求部318は、管理サーバ200に対して、秘密鍵及び公開鍵のセットの生成を要求する。

[0056] 専用鍵生成部320は、監督官庁・CFP管理団体サーバ300が扱う監督官庁又はCFP管理団体専用の秘密鍵及び公開鍵のセットを生成する。監督官庁またはCFP管理団体専用の秘密鍵及び公開鍵のセットは、管理サーバ200の鍵データベースDBK内には含まれない。生成した監督官庁またはCFP管理団体専用の秘密鍵及び公開鍵のセットは、専用鍵データベースDBSK2に記録される。

[0057] 次に、本実施形態のサプライチェーン管理システム1にて実行される準同型暗号を用いた処理について説明する。秘密鍵及び暗号化されていないアイテム関連情報の実際の値をネットワーク上でやり取りするのは、セキュリティ面でも問題がある。そこで、本実施形態では、暗号化された数値さえあれば暗号の鍵がなくても平文情報の数値を足すことが可能であるという準同型暗号の性質を利用する。

[0058] ただし、準同型暗号には、次の制約がある。

制約1：暗号化された数値同士を足し合わせるには、同じ暗号鍵で暗号

化されていることが必要

制約 2：乗算・除算は、計算回数に制限があり、計算誤差がたまるのを防止する為にブートストラッピング処理（一旦解読し、その後再度暗号化する）が必要であるが、ブートストラッピング処理時に必要な解読の為に秘密鍵が必要

制約 3：暗号化された数値の実際の値を知るには秘密鍵が必要

[0059] 制約 2 及び制約 3 の解決には秘密鍵 $K_{\text{prv}}^{\text{Adm}}$ が必要であるが、秘密鍵 $K_{\text{prv}}^{\text{Adm}}$ をネットワーク上でやり取りするわけにはいかない。このため、一つの管理サーバ（本実施形態の管理サーバ 200）上で秘密鍵 $K_{\text{prv}}^{\text{Adm}}$ を用いた処理を行えばよい。

[0060] 制約 3 に関して、1 つの管理サーバ上で解読を行うと、解読により得られた実際の値を他のサーバへ送信するには、解読により得られた実際の値をネットワーク上でやり取りする必要があるが生じてしまう。これを避けるため、解読を要求する端末で独自に秘密鍵 K_{prv} および公開鍵 K_{pub} のセットを作成し、0 の値を公開鍵 K_{pub} で暗号化（ $\text{Enc}(0, K_{\text{pub}})$ ）し、0 の暗号化データ $\text{Enc}(0, K_{\text{pub}})$ と解読したい暗号化データ（ $\text{Enc}(x_1, K_{\text{pub}}^{\text{Adm}})$ ）を管理サーバに送信する。そして、管理サーバ側で $\text{Enc}(x_1, K_{\text{pub}}^{\text{Adm}})$ を解読して x_1 を得た上で、 $\text{Enc}(0, K_{\text{pub}})$ に足し合わせて、解読を要求する端末に $\text{Enc}(0+x_1, K_{\text{pub}})$ を送信する。解読を要求した端末は独自の秘密鍵 K_{prv} で $\text{Enc}(0+x_1, K_{\text{pub}})$ を解読する。

[0061] 制約 2 のブートストラッピング処理に関しては、上記アイデアと同様に、 $\text{Enc}(x_1, K_{\text{pub}}^{\text{Adm}})$ を管理サーバに送信し、管理サーバで秘密鍵 $K_{\text{prv}}^{\text{Adm}}$ を使って解読し、解読した値を再度公開鍵 $K_{\text{pub}}^{\text{Adm}}$ により暗号化した後に、ブートストラッピング処理の要求者端末に返す。

[0062] 制約 1 に関して、異なる暗号鍵を使った暗号化の値を足し合わせるには、全ての暗号化された数値（ $\text{Enc}(x_1, K_{\text{pub}}^{\text{Adm}1})$ 、 $\text{Enc}(x_2, K_{\text{pub}}^{\text{Adm}2})$ ）を管理サーバに送り、秘密鍵 $K_{\text{prv}}^{\text{Adm}1}$ と秘密鍵 $K_{\text{prv}}^{\text{Adm}2}$ でそれぞれを解読し x_1 と x_2 を取得した後に、 x_1+x_2 を $K_{\text{pub}}^{\text{Adm}3}$ で再度暗号化して $\text{Enc}(x_1+x_2, K_{\text{pub}}^{\text{Adm}3})$ を暗号情報の演算を要求した要求者端末に返す。

[0063] 以下、図6～図8を用いて、秘密鍵及び暗号化されていないアイテム関連情報の実際の値をネットワーク上でやり取りせずに、上記の制約1～3を解決するためのサプライチェーン管理システム1の処理について詳細に説明する。以下に、説明のために用いる記号を定義する。なお、業界とは、取引者の企業を分類したものである。

$K_{\text{prv}}^{\text{Adm}1}$: 業界1で使われている暗号化の元となる秘密鍵

$K_{\text{pub}}^{\text{Adm}1}$: 業界1で使われている公開鍵

$N^{\text{Adm}1}$: 業界1で使われている鍵の鍵名称

$K_{\text{prv}}^{\text{Adm}2}$: 業界2で使われている暗号化の元となる秘密鍵

$K_{\text{pub}}^{\text{Adm}2}$: 業界2で使われている公開鍵

$N^{\text{Adm}2}$: 業界2で使われている鍵の鍵名称

$K_{\text{prv}}^{\text{Adm}3}$: 業界3で使われている暗号化の元となる秘密鍵

$K_{\text{pub}}^{\text{Adm}3}$: 業界3で使われている公開鍵

$N^{\text{Adm}3}$: 業界3で使われている鍵の鍵名称

x_1 : 数値 (例: 業界1である製品を作るために必要だったCFP値)

x_2 : 数値 (例: 業界2である製品を作るために必要だったCFP値)

x_3 : 数値 (例: 業界3である製品を作るために必要だったCFP値)

$\text{Enc}(x, K_{\text{pub}}^{\text{Adm}1})$: 数値 x を業界1で使われている公開鍵で暗号化したもの

$\text{Enc}(x, K_{\text{pub}}^{\text{Adm}2})$: 数値 x を業界2で使われている公開鍵で暗号化したもの

$\text{Enc}(x, K_{\text{pub}}^{\text{Adm}3})$: 数値 x を業界3で使われている公開鍵で暗号化したもの

[0064] 図6は、異なる公開鍵で暗号化されている数値の四則演算の詳細を示すフローチャートである。図6を用いて、制約1に対応する異なる公開鍵で暗号化されている数値の四則演算について説明する。業界3の取引者の取引者端末100が管理サーバ200に対してログインを行い、管理サーバ200がログインの認証を行うことにより処理が開始される。

[0065] S601において、UID読込部114は、業界1の取引者と業界2の取引者それぞれから納品された製品に付されたUIDを読み込む。なお、図6において、業界1の取引者の取引者端末100と業界2の取引者の取引者端

末100から、業界3の取引者の取引者端末100への納品を点線で示しているのは、製品の納品は信号のやりとりではなく、製品という現物の移動を示しているからである。

[0066] S602において、送付要求送信部124は、管理サーバ200に読み込んだUIDを引数として、トレサビ情報の送付要求を送信する。

[0067] S603において、管理サーバ200の情報送信部212は、読み込んだUIDに対応するトレサビ情報を取引者端末100に送信する。

[0068] S604において、情報演算部118は、取得したトレサビ情報内の $Enc(x_1, K_{pub}^{Adm1})$ 、 N^{Adm1} 、 $Enc(x_2, K_{pub}^{Adm2})$ 、 N^{Adm2} 及び N^{Adm3} と共に、 $Enc(x_1, K_{pub}^{Adm1})$ と $Enc(x_2, K_{pub}^{Adm2})$ の加算のリクエストを、管理サーバ200の暗号情報取得部214に送信する。

[0069] S605において、鍵取得部216は、暗号情報取得部214が取得した鍵名称 N^{Adm1} 、 N^{Adm2} 、 N^{Adm3} にそれぞれ対応する秘密鍵および公開鍵のセット（ $(K_{prv}^{Adm1}, K_{pub}^{Adm1})$ 、 $(K_{prv}^{Adm2}, K_{pub}^{Adm2})$ 、 $(K_{prv}^{Adm3}, K_{pub}^{Adm3})$ ）を検索して、鍵データベースDBKから秘密鍵および公開鍵のセット（ $(K_{prv}^{Adm1}, K_{pub}^{Adm1})$ 、 $(K_{prv}^{Adm2}, K_{pub}^{Adm2})$ 、 $(K_{prv}^{Adm3}, K_{pub}^{Adm3})$ ）を取得する。さらに、解読情報取得部218は、取得した秘密鍵 K_{prv}^{Adm1} 、 K_{prv}^{Adm2} で $Enc(x_1, K_{pub}^{Adm1})$ 、 $Enc(x_2, K_{pub}^{Adm2})$ を解読し x_1 、 x_2 を得る。さらに、暗号化処理部220は、 x_1 と x_2 および K_{pub}^{Adm3} を用いて暗号情報 $Enc(x_1+x_2, K_{pub}^{Adm3})$ を計算する。

[0070] S606において提供部222は、業界3の取引者の取引者端末100に暗号情報 $Enc(x_1+x_2, K_{pub}^{Adm3})$ を送信する。

[0071] S607において、情報演算部118は、暗号情報 $Enc(x_1+x_2, K_{pub}^{Adm3})$ に x_3 を足す秘密計算を行い、暗号情報 $Enc(x_1+x_2+x_3, K_{pub}^{Adm3})$ を取得する。このように、情報演算部118は、暗号情報及びアイテム関連情報の平文情報を用いた秘密計算により暗号情報を生成する秘密計算部として機能を有する。

[0072] 以上の処理により、異なる公開鍵で暗号化された数値の四則演算を1つの管理サーバ200上で行うことができる。ネットワーク上でやり取りされる情報は、鍵名称と暗号化された情報のみであり、秘密鍵や解読された実際の

数値がネットワーク上でやり取りされないため、セキュリティを向上することができる。さらに、公開鍵は配布されてもよいが、本実施形態では、公開鍵すら配布する必要がなく、秘密鍵及び公開鍵のセットが一つの管理サーバ200の鍵データベースDBKで管理される。

[0073] 図7は、ブートストラッピング処理の詳細を示すフローチャートである。

図7を用いて、制約2に対応するブートストラッピング処理について説明する。業界3の取引者の取引者端末100が管理サーバ200に対してログインを行い、管理サーバ200がログインの認証を行うことにより処理が開始される。

[0074] S701において、情報演算部118は、 $Enc(x_3, K_{pub}^{Adm3})$ 及び N^{Adm3} を用意する。

[0075] S702において、情報送信部120は、 $Enc(x_3, K_{pub}^{Adm3})$ 及び N^{Adm3} と共に、 $Enc(x_3, K_{pub}^{Adm3})$ のブートストラッピング処理のリクエストを管理サーバ200に送信する。

[0076] S703において、鍵取得部216は、暗号情報取得部214が取得した鍵名称 N^{Adm3} に対応する秘密鍵および公開鍵のセット(K_{prv}^{Adm3} 、 K_{pub}^{Adm3})を検索して、鍵データベースDBKから秘密鍵および公開鍵のセット(K_{prv}^{Adm3} 、 K_{pub}^{Adm3})を取得する。さらに、解読情報取得部218は、取得した秘密鍵 K_{prv}^{Adm3} で $Enc(x_3, K_{pub}^{Adm3})$ を解読し x_3 を得る。さらに、暗号化処理部220は、 x_3 および K_{pub}^{Adm3} を用いて暗号情報 $Enc(x_3, K_{pub}^{Adm3})$ を計算（ブートストラッピング処理）する。

[0077] S704において、提供部222は、業界3の取引者の取引者端末100に暗号情報 $Enc(x_3, K_{pub}^{Adm3})$ を送信する。

[0078] S705において、情報演算部118は、乗算・除算回数を更新($M^{Adm3}=0$)し、暗号情報 $Enc(x_3, K_{pub}^{Adm3})$ に乗算・除算を実施する。

[0079] 以上の処理により、ブートストラッピング処理を1つの管理サーバ200上で行うことができる。ネットワーク上でやり取りされる情報は、鍵名称と暗号化された情報のみであり、秘密鍵や解読された実際の数値がネットワー

ク上でやり取りされないため、セキュリティを向上することができる。

[0080] 図8は、データ開示要求の詳細を示すフローチャートである。図8を用いて、制約3に対応するデータ開示要求について説明する。業界3の取引者の取引者端末100が管理サーバ200に対してログインを行い、管理サーバ200がログインの認証を行うことにより処理が開始される。

[0081] S801において、情報演算部118は、解読対象の暗号情報 $\text{Enc}(x_3, K_{\text{pub}}^{\text{Adm}3})$ 及び $N^{\text{Adm}3}$ を用意する。

[0082] S802において、専用鍵生成部122は、専用の秘密鍵 K_{prv} および公開鍵 K_{pub} のセットを作成し用意する。

[0083] S803において、情報演算部118は、公開鍵 K_{pub} を用いて数値0の暗号化を行い、暗号情報 $\text{Enc}(0, K_{\text{pub}})$ を計算する。

[0084] S804において、情報送信部120は、 $\text{Enc}(x_3, K_{\text{pub}}^{\text{Adm}3})$ 、 $N^{\text{Adm}3}$ 及び $\text{Enc}(0, K_{\text{pub}})$ と共に $\text{Enc}(x_3, K_{\text{pub}}^{\text{Adm}3})$ のデータ開示要求を管理サーバ200に送信する。

[0085] S805において、鍵取得部216は、取得した鍵名称 $N^{\text{Adm}3}$ に対応する秘密鍵および公開鍵のセット($K_{\text{prv}}^{\text{Adm}3}$ 、 $K_{\text{pub}}^{\text{Adm}3}$)を検索して、鍵データベースDBKから秘密鍵および公開鍵のセット($K_{\text{prv}}^{\text{Adm}3}$ 、 $K_{\text{pub}}^{\text{Adm}3}$)を取得する。さらに、解読情報取得部218は、取得した秘密鍵 $K_{\text{prv}}^{\text{Adm}3}$ で $\text{Enc}(x_3, K_{\text{pub}}^{\text{Adm}3})$ を解読し x_3 を得る。さらに、暗号化処理部220は、 x_3 に $\text{Enc}(0, K_{\text{pub}})$ を足す秘密計算により、暗号情報 $\text{Enc}(x_3, K_{\text{pub}})$ を計算する。

[0086] S806において、提供部222は、業界3の取引者の取引者端末100に暗号情報 $\text{Enc}(x_3, K_{\text{pub}})$ を送信する。

[0087] S807において、情報演算部118は、暗号情報 $\text{Enc}(x_3, K_{\text{pub}})$ を専用の秘密鍵 K_{prv} を用いて解読し x_3 を取得する。

[0088] 以上の処理により、データの開示要求を1つの管理サーバ200上で行うことができる。ネットワーク上でやり取りされる情報は、鍵名称と暗号化された情報のみであり、秘密鍵や解読された実際の数値がネットワーク上でやり取りされないため、セキュリティを向上することができる。なお、S80

4において、取引者端末100は、数値0の暗号情報 $Enc(0, K_{pub})$ を管理サーバ200に送信しているが、0ではない所定値の暗号情報を管理サーバ200に送信してもよい。この場合、取引者は所定値を把握しておき、S806にて管理サーバ200から送信される暗号情報を解読した値から所定値を差し引けばよい。

[0089] 次に、本実施形態のサプライチェーン管理システム1を実装した際の基本的なフローについて、図9～図18を用いて説明する。以下に、説明のために用いる記号を定義する。

$K_{prv}^{AdmY}(n)$: 業界Yで使われている暗号化の元となる秘密鍵 (n個目)

$K_{pub}^{AdmY}(n)$: 業界Yで使われている公開鍵 (n個目)

$N^{AdmY}(n)$: 業界Yで使われている鍵の鍵名称 (n個目)

$M^{AdmY}(n)$: 業界Yで使われているn個目の鍵の現在の乗算・除算回数

n:業界ごとの鍵の発行回数 (別番号を示す際はn1, n2, ...と表記)

Y:業界ごとに割り振られる固有名称 (別業界を示す際はY1, Y2, ...と表記)

$K_{prv}^{Adm}(n)$: 暗号化の元となる秘密鍵 (n個目) (業界を分けて議論する必要がない場合)

$K_{pub}^{Adm}(n)$: 暗号化の元となる公開鍵 (n個目) (業界を分けて議論する必要がない場合)

$N^{Adm}(n)$: 暗号化の元となる鍵の鍵名称 (n個目) (業界を分けて議論する必要がない場合)

K_{prv} : ある業界内の会社が独自に作成した秘密鍵 (使い捨て)

K_{pub} : K_{prv} に対応する公開鍵 (使い捨て)

x_m : 数値 (例: 会社mでのCFP値)

x: 数値 (例: 会社を分けて議論する必要がない場合の会社でのCFP値)

$Enc(x, K_{pub}^{AdmY}(n))$: 数値xを業界Yで使われているn個目の公開鍵で暗

号化したもの

$\text{Enc}(x, K_{\text{pub}}^{\text{Adm}}(n))$: 数値 x を n 個目の公開鍵で暗号化したもの（業界を分けて議論する必要がない場合）

$\text{Enc}(x, K_{\text{pub}})$: 数値 x をある業界内の会社が独自に作成した公開鍵で暗号化したもの

R : 分岐割合

[0090] 図9は、秘密鍵及び公開鍵の生成の詳細を示すフローチャートである。図9を用いて、秘密鍵及び公開鍵のセットを生成する処理のフローについて説明する。監督官庁・CFP管理団体サーバ300が管理サーバ200に対してログインを行い、管理サーバ200がログインの認証を行うことにより処理が開始される。

[0091] S901において、鍵生成要求部318は、業界情報Yを引数として管理サーバ200の鍵生成部226に鍵作成要求を送信する。

[0092] S902において、鍵生成部226は、業界情報Yの鍵の作成要求回数nを設定し、秘密鍵及び公開鍵のセット $(K_{\text{prv}}^{\text{AdmY}}(n), K_{\text{pub}}^{\text{AdmY}}(n))$ 及びこれらの鍵の鍵名称 $N^{\text{AdmY}}(n)$ を生成する。

[0093] S903において、鍵生成部226は、業界情報Y及び作成要求回数nを含め、秘密鍵及び公開鍵のセット $(K_{\text{prv}}^{\text{AdmY}}(n), K_{\text{pub}}^{\text{AdmY}}(n))$ 及びこれらの鍵の鍵名称 $N^{\text{AdmY}}(n)$ を鍵データベースDBKに記録する。

[0094] S904において、鍵名称開示部228は、監督官庁・CFP管理団体サーバ300に、鍵名称 $N^{\text{AdmY}}(n)$ を送信する。

[0095] 上述した処理により、管理サーバ200内の鍵データベースDBKに業界ごとに秘密鍵及び公開鍵のセット $(K_{\text{prv}}^{\text{AdmY}}(n), K_{\text{pub}}^{\text{AdmY}}(n))$ 及びこれらの鍵の鍵名称 $N^{\text{AdmY}}(n)$ が記録される。

[0096] 図10は、鍵名称の配布の詳細を示すフローチャートである。図10を用いて、鍵名称を配布する処理のフローについて説明する。鍵名称の配布は2通りの方法がある。図10(a)に示す方法では、監督官庁・CFP管理団体サーバ300は鍵名称をダイレクトに取引者端末100に開示する。例え

ば、監督官庁・CFP管理団体が監督官庁・CFP管理団体サーバ300で作成したホームページHPに鍵名称を掲載し、取引者端末100を使用する管理者は、HPから自身が所属する業界の鍵名称を探して取得すればよい。図10(b)に示す方法では、取引者端末100がダイレクトに管理サーバ200から鍵名称を取得する。以下具体的に説明する。まず、取引者端末100が管理サーバ200に対してログインを行い、管理サーバ200がログインの認証を行う。S1001において、取引者端末100の送付要求送信部124は、業界情報Y及び発行回数nを引数として鍵名称の送付要求を管理サーバ200に対して送信する。S1002において、鍵取得部216は、鍵データベースDBKから鍵名称 $N^{AdmY}(n)$ を検索し取得する。S1003において、鍵名称開示部228は、取得した鍵名称 $N^{AdmY}(n)$ を取引者端末100に送信する。これにより、取引者端末100を使用する管理者は、自身が所属する業界の鍵名称を取得することができる。

[0097] 図11は、前工程がない場合における追加・統合工程時の準同型暗号を用いたCFP計算の詳細を示すフローチャートである。図11を用いて、追加・統合工程時において前工程がない場合における準同型暗号を用いたCFP計算について説明する。鍵名称 $N^{AdmY}(n)$ の取引者端末100が管理サーバ200に対してログインを行い、管理サーバ200がログインの認証を行うことにより処理が開始される。

[0098] S1101において、取引者端末100の送付要求送信部124は、自社の鍵名称 $N^{AdmY}(n)$ を引数としてOCFP送付要求を管理サーバ200に対して送信する。ここで、OCFP送付要求とは、CFP値が0の状態で暗号化された暗号情報である。なお、引数として鍵名称 $N^{AdmY}(n)$ ではなく、業界情報Yと発行回数nを指定してもよい。

[0099] S1102において、鍵取得部216は、鍵データベースDBKから鍵名称 $N^{AdmY}(n)$ を用いて公開鍵 $K_{pub}^{AdmY}(n)$ を検索し取得する。

[0100] S1103において、暗号化処理部220は、取得した公開鍵 $K_{pub}^{AdmY}(n)$ を用いて数値0を暗号化(OCFP暗号化)した暗号情報 $Enc(0, K_{pub}^{AdmY}(n))$

)を計算する。

[0101] S 1 1 0 4 において、提供部 2 2 2 は、暗号情報 $\text{Enc}(O, K_{\text{pub}}^{\text{AdmY}}(n))$ を取引者端末 1 0 0 に送信する。

[0102] S 1 1 0 5 において、情報演算部 1 1 8 は、測定した自社製品に関する C F P 値 x_1 を暗号情報 $\text{Enc}(O, K_{\text{pub}}^{\text{AdmY}}(n))$ に足す秘密計算を行い、暗号情報 $\text{Enc}(x_1, K_{\text{pub}}^{\text{AdmY}}(n))$ を取得する。

[0103] S 1 1 0 6 において、取引者端末 1 0 0 は、U I D、C F P 値 x_1 、鍵名称 $N^{\text{AdmY}}(n)$ 、暗号化 C F P ($\text{Enc}(x_1, K_{\text{pub}}^{\text{AdmY}}(n))$)、乗算・除算回数 $M^{\text{AdmY}}(n) = 0$ を含むトレサビ情報をトレサビデータベース D B T 1 に記録する。

[0104] S 1 1 0 7 において、情報送信部 1 2 0 は、管理サーバ 2 0 0 にトレサビデータベース D B T 1 に記録したトレサビ情報を送信する。その後、U I D を付けた製品が次工程の会社へ納品される。

[0105] S 1 1 0 8 において、管理サーバ 2 0 0 は、取引者端末 1 0 0 から送信されたトレサビ情報をトレサビデータベース D B T 2 に記録する。

[0106] 図 1 2 は、前工程がある場合における追加・統合工程時の準同型暗号を用いた C F P 計算の詳細を示すフローチャートである。図 1 2 を用いて、追加・統合工程時において前工程がある場合における準同型暗号を用いた C F P 計算について説明する。鍵名称 $N^{\text{AdmY}}(n)$ の現工程会社の取引者端末 1 0 0 が管理サーバ 2 0 0 に対してログインを行い、管理サーバ 2 0 0 がログインの認証を行うことにより処理が開始される。

[0107] S 1 2 0 1 において、現工程会社における取引者端末 1 0 0 の U I D 読込部 1 1 4 は、前工程会社から納品された製品に付された U I D を読み込む。

[0108] S 1 2 0 2 において、情報取得部 1 1 6 は、管理サーバ 2 0 0 に読み込んだ U I D を引数としたトレサビ情報の送付要求を送信する。

[0109] S 1 2 0 3 において、情報送信部 2 1 2 は、読み込んだ U I D に対応するトレサビ情報を取引者端末 1 0 0 の情報取得部 1 1 6 に送信する。

[0110] S 1 2 0 4 において、情報演算部 1 1 8 は取得したトレサビ情報内の前工程会社の鍵名称 $N^{\text{AdmY}}(n)$ と、自社の鍵名称 $N^{\text{AdmY}}(n)$ とを比較し、両社の鍵名

称が一致するのを確認する。

[0111] S 1 2 0 5 において、情報演算部 1 1 8 は、取得したトレサビ情報内の暗号情報 $\text{Enc}(x_1, K_{\text{pub}}^{\text{AdmY}}(n))$ に自社製品に関する C F P 値 x_2 を足す秘密計算を行い、暗号情報 $\text{Enc}(x_1 + x_2, K_{\text{pub}}^{\text{AdmY}}(n))$ を取得する。

[0112] S 1 2 0 6 において、取引者端末 1 0 0 は、U I D、C F P 値 x_2 、鍵名称 $N^{\text{AdmY}}(n)$ 、暗号化 C F P ($\text{Enc}(x_2, K_{\text{pub}}^{\text{AdmY}}(n))$ 、 $\text{Enc}(x_1 + x_2, K_{\text{pub}}^{\text{AdmY}}(n))$)、乗算・除算回数 $M^{\text{AdmY}}(n)$ を含むトレサビ情報をトレサビデータベース D B T 1 に記録する。

[0113] S 1 2 0 7 において、情報送信部 1 2 0 は、管理サーバ 2 0 0 にトレサビデータベース D B T 1 に記録したトレサビ情報を送信する。その後、U I D を付けた製品が次工程の会社へ納品される。

[0114] S 1 2 0 8 において、管理サーバ 2 0 0 は、取引者端末 1 0 0 から送信されたトレサビ情報をトレサビデータベース D B T 2 に記録する。

[0115] 図 1 3 は、分岐工程時の準同型暗号を用いた C F P 計算の詳細を示すフローチャートである。図 1 3 を用いて、分岐工程時における準同型暗号を用いた C F P 計算について説明する。鍵名称 $N^{\text{AdmY}}(n)$ の現工程会社の取引者端末 1 0 0 が管理サーバ 2 0 0 に対してログインを行い、管理サーバ 2 0 0 がログインの認証を行うことにより処理が開始される。

[0116] S 1 3 0 1 において、現工程会社における取引者端末 1 0 0 の U I D 読込部 1 1 4 は、前工程会社から納品された製品に付された U I D を読み込む。

[0117] S 1 3 0 2 において、情報取得部 1 1 6 は、管理サーバ 2 0 0 に読み込んだ U I D を引数としたトレサビ情報の送付要求を送信する。

[0118] S 1 3 0 3 において、情報送信部 2 1 2 は、読み込んだ U I D に対応するトレサビ情報を取引者端末 1 0 0 の情報取得部 1 1 6 に送信する。

[0119] S 1 3 0 4 において、情報演算部 1 1 8 は取得したトレサビ情報内の前工程会社の鍵名称 $N^{\text{AdmY}}(n)$ と、自社の鍵名称 $N^{\text{AdmY}}(n)$ とを比較し、両社の鍵名称が一致するのを確認する。

[0120] S 1 3 0 5 において、情報演算部 1 1 8 は、取得したトレサビ情報内の暗

号情報 $\text{Enc}(x_1, K_{\text{pub}}^{\text{AdmY}}(n))$ に自社製品に関するCFP値 x_2 を足す秘密計算を行い、暗号情報 $\text{Enc}(x_1+x_2, K_{\text{pub}}^{\text{AdmY}}(n))$ を取得する。さらに、情報演算部118は、暗号情報 $\text{Enc}(x_1+x_2, K_{\text{pub}}^{\text{AdmY}}(n))$ に分岐割合 R を乗じ、乗算・除算回数 $M^{\text{AdmY}}(n)$ に1を加える。なお、分岐割合 R を乗じるとは、製品の分岐割合 R 分を次工程会社に納品する場合の計算処理である。

[0121] S1306において、取引者端末100は、UID、CFP値 x_2 、鍵名称 $N^{\text{AdmY}}(n)$ 、暗号化CFP($\text{Enc}(x_2, K_{\text{pub}}^{\text{AdmY}}(n))$ 、 $\text{Enc}(x_1+x_2, K_{\text{pub}}^{\text{AdmY}}(n))$)、乗算・除算回数 $M^{\text{AdmY}}(n)$ を含むトレサビ情報をトレサビデータベースDBT1に記録する。

[0122] S1307において、情報送信部120は、管理サーバ200にトレサビデータベースDBT1に記録したトレサビ情報を送信する。その後、UIDを付けた製品が次工程の会社へ納品される。

[0123] S1308において、管理サーバ200は、取引者端末100から送信されたトレサビ情報をトレサビデータベースDBT2に記録する。

[0124] 図14は、前工程の公開鍵が異なる場合における準同型暗号を用いたCFP計算の詳細を示すフローチャートである。図14を用いて、前工程会社の公開鍵と現工程会社の公開鍵が異なる場合における準同型暗号を用いたCFP計算について説明する。鍵名称 $N^{\text{AdmY}2}(n_2)$ の現工程会社の取引者端末100が管理サーバ200に対してログインを行い、管理サーバ200がログインの認証を行うことにより処理が開始される。

[0125] S1401において、現工程会社における取引者端末100のUID読込部114は、前工程会社から納品された製品に付されたUIDを読み込む。

[0126] S1402において、情報取得部116は、管理サーバ200に読み込んだUIDを引数としたトレサビ情報の送付要求を送信する。

[0127] S1403において、情報送信部212は、読み込んだUIDに対応するトレサビ情報を取引者サーバ100の情報取得部116に送信する。

[0128] S1404において、情報演算部118は、取得したトレサビ情報内の前工程会社の鍵名称 $N^{\text{AdmY}1}(n_1)$ と、自社の鍵名称 $N^{\text{AdmY}2}(n_2)$ とを比較し、両社

の鍵名称が一致していないのを確認する。

[0129] 両社の鍵名称が一致していない場合、S 1 4 0 5において、情報演算部 1 1 8 は、前工程会社の暗号情報 $\text{Enc}(x_1, K_{\text{pub}}^{\text{AdmY } 1}(n_1))$ の公開鍵 $K_{\text{pub}}^{\text{AdmY } 1}(n_1)$ の変更要求を送信する。このとき、引数として、 $N^{\text{AdmY } 1}(n_1)$ 、 $\text{Enc}(x_1, K_{\text{pub}}^{\text{AdmY } 1}(n_1))$ 、 $N^{\text{AdmY } 2}(n_2)$ を指定する。

[0130] S 1 4 0 6において、鍵取得部 2 1 6 は、変更要求内の鍵名称 $N^{\text{AdmY } 1}(n_1)$ に対応する秘密鍵 $K_{\text{prv}}^{\text{AdmY } 1}(n_1)$ および鍵名称 $N^{\text{AdmY } 2}(n_2)$ に対応する公開鍵 $K_{\text{pub}}^{\text{AdmY } 2}(n_2)$ を鍵データベース D B K から検索して取得する。さらに、解読情報取得部 2 1 8 は、取得した秘密鍵 $K_{\text{prv}}^{\text{AdmY } 1}(n_1)$ で $\text{Enc}(x_1, K_{\text{pub}}^{\text{AdmY } 1}(n_1))$ を解読し x_1 を得る。さらに、暗号化処理部 2 2 0 は、 x_1 および $K_{\text{pub}}^{\text{AdmY } 2}(n_2)$ を用いて暗号情報 $\text{Enc}(x_1, K_{\text{pub}}^{\text{AdmY } 2}(n_2))$ を計算する。

[0131] S 1 4 0 7において、提供部 2 2 2 は、取引者端末 1 0 0 に暗号情報 $\text{Enc}(x_1, K_{\text{pub}}^{\text{AdmY } 2}(n_2))$ を送信する。

[0132] S 1 4 0 8において、情報演算部 1 1 8 は、取得した暗号情報 $\text{Enc}(x_1, K_{\text{pub}}^{\text{AdmY } 2}(n_2))$ に測定した自社製品に関する C F P 値 x_2 を足す秘密計算を行い、暗号情報 $\text{Enc}(x_1 + x_2, K_{\text{pub}}^{\text{AdmY } 2}(n_2))$ を取得し、乗算・除算回数 $M^{\text{AdmY } 2}(n_2)$ を 0 に更新する。

[0133] S 1 4 0 9において、取引者端末 1 0 0 は、U I D、C F P 値 x_2 、鍵名称 $N^{\text{AdmY } 2}(n_2)$ 、暗号化 C F P ($\text{Enc}(x_2, K_{\text{pub}}^{\text{AdmY } 2}(n_2))$ 、 $\text{Enc}(x_1 + x_2, K_{\text{pub}}^{\text{AdmY } 2}(n_2))$)、乗算・除算回数 $M^{\text{AdmY } 2}(n_2)$ を含むトレサビ情報をトレサビデータベース D B T 1 に記録する。

[0134] S 1 4 1 0において、情報送信部 1 2 0 は、管理サーバ 2 0 0 にトレサビデータベース D B T 1 に記録したトレサビ情報を送信する。その後、U I D を付けた製品が次工程の会社へ納品される。

[0135] S 1 4 1 1において、管理サーバ 2 0 0 は、取引者端末 1 0 0 から送信されたトレサビ情報をトレサビデータベース D B T 2 に記録する。

[0136] 図 1 5 は、乗算・除算回数が上限値に到達したときの準同型暗号を用いた C F P 計算の詳細を示すフローチャートである。図 1 5 を用いて、乗算・除

算回数が上限値に到達したときの準同型暗号を用いたCFP計算について説明する。なお、図15の処理は、図11～図14に記載の処理と併用することが可能である。現工程会社の取引者端末100が管理サーバ200に対してログインを行い、管理サーバ200がログインの認証を行うことにより処理が開始される。

[0137] S1501において、現工程会社における取引者端末100のUID読込部114は、前工程会社から納品された製品に付されたUIDを読み込む。

[0138] S1502において、情報取得部116は、管理サーバ200に読み込んだUIDを引数としたトレサビ情報の送付要求を送信する。

[0139] S1503において、情報送信部212は、読み込んだUIDに対応するトレサビ情報を取引者端末100の情報取得部116に送信する。

[0140] S1504において、情報演算部118は、取得したトレサビ情報内の乗算・除算回数 $M^{AdmY}(n)$ が上限値を超過しているか確認する。なお、上限値は外部から事前に指定することができる。

[0141] 乗算・除算回数 $M^{AdmY}(n)$ が上限値を超過している場合、S1505において、取引者端末100の情報演算部118は、管理サーバ200に前工程会社の暗号情報 $Enc(x_1, K_{pub}^{AdmY}(n))$ のブートストラッピング要求を送信する。このとき、引数として、 $N^{AdmY}(n)$ 、 $Enc(x_1, K_{pub}^{AdmY}(n))$ を指定する。

[0142] S1506において、鍵取得部216は、ブートストラッピング要求内の鍵名称 $N^{AdmY}(n)$ に対応する秘密鍵 $K_{prv}^{AdmY}(n)$ および公開鍵 $K_{pub}^{AdmY}(n)$ を鍵データベースDBKから検索して取得する。さらに、解読情報取得部218は、取得した秘密鍵 $K_{prv}^{AdmY}(n)$ で $Enc(x_1, K_{pub}^{AdmY}(n))$ を解読し x_1 を得る。さらに、暗号化処理部220は、 x_1 および $K_{pub}^{AdmY}(n)$ を用いて暗号情報 $Enc(x_1, K_{pub}^{AdmY}(n))$ を計算する。

[0143] S1507において、提供部222は、取引者端末100に暗号情報 $Enc(x_1, K_{pub}^{AdmY}(n))$ を送信する。

[0144] S1508において、情報演算部118は、取得した暗号情報 $Enc(x_1, K_{pub}^{AdmY}(n))$ に測定した自社製品に関するCFP値 x_2 を足す秘密計算を行い、暗号

情報 $\text{Enc}(x_1+x_2, K_{\text{pub}}^{\text{AdmY}}(n))$ を取得し、乗算・除算回数 $M^{\text{AdmY}}(n)$ を0に更新する。

[0145] S1509において、取引者端末100は、UID、CFP値 x_2 、鍵名称 $N^{\text{AdmY}}(n)$ 、暗号化CFP($\text{Enc}(x_2, K_{\text{pub}}^{\text{AdmY}}(n))$ 、 $\text{Enc}(x_1+x_2, K_{\text{pub}}^{\text{AdmY}}(n))$)、乗算・除算回数 $M^{\text{AdmY}}(n)$ を含むトレサビ情報をトレサビデータベースDBT1に記録する。

[0146] S1510において、情報送信部120は、管理サーバ200にトレサビデータベースDBT1に記録したトレサビ情報を送信する。その後、UIDを付けた製品が次工程の会社へ納品される。

[0147] S1511において、管理サーバ200は、取引者端末100から送信されたトレサビ情報をトレサビデータベースDBT2に記録する。

[0148] 図16は、乗算・除算の計算回数をクリアしたいときの準同型暗号を用いたCFP計算の詳細を示すフローチャートである。図16を用いて、乗算・除算の計算回数をクリアしたいときの準同型暗号を用いたCFP計算について説明する。なお、図16の処理は、図11～図14に記載の処理と併用することが可能である。現工程会社の取引者端末100が管理サーバ200に対してログインを行い、管理サーバ200がログインの認証を行うことにより処理が開始される。

[0149] S1601において、現工程会社における取引者端末100のUID読込部114は、前工程会社から納品された製品に付されたUIDを読み込む。

[0150] S1602において、情報取得部116は、管理サーバ200に読み込んだUIDを引数としたトレサビ情報の送付要求を送信する。

[0151] S1603において、情報送信部212は、読み込んだUIDに対応するトレサビ情報を取引者端末100の情報取得部116に送信する。

[0152] S1604において、取引者端末100の取引者は、取得したトレサビ情報内の乗算・除算回数 $M^{\text{AdmY}}(n)$ をクリアするクリア要求を取引者端末100に入力する。

[0153] S1605において、取引者端末100の情報演算部118は、クリア要

求に基づいて、管理サーバ200に前工程会社の暗号情報 $Enc(x_1, K_{pub}^{AdmY}(n))$ のブートストラッピング要求を送信する。このとき、引数として、 $N^{AdmY}(n)$ 、 $Enc(x_1, K_{pub}^{AdmY}(n))$ を指定する。

[0154] S1606において、鍵取得部216は、ブートストラッピング要求内の鍵名称 $N^{AdmY}(n)$ に対応する秘密鍵 $K_{prv}^{AdmY}(n)$ および公開鍵 $K_{pub}^{AdmY}(n)$ を鍵データベースDBKから検索して取得する。さらに、解読情報取得部218は、取得した秘密鍵 $K_{prv}^{AdmY}(n)$ で $Enc(x_1, K_{pub}^{AdmY}(n))$ を解読し x_1 を得る。さらに、暗号化処理部220は、 x_1 および $K_{pub}^{AdmY}(n)$ を用いて暗号情報 $Enc(x_1, K_{pub}^{AdmY}(n))$ を計算する。

[0155] S1607において、提供部222は、取引者端末100に暗号情報 $Enc(x_1, K_{pub}^{AdmY}(n))$ を送信する。

[0156] S1608において、情報演算部118は、取得した暗号情報 $Enc(x_1, K_{pub}^{AdmY}(n))$ に測定した自社製品に関するCFP値 x_2 を足す秘密計算を行い、暗号情報 $Enc(x_1+x_2, K_{pub}^{AdmY}(n))$ を取得し、乗算・除算回数 $M^{AdmY}(n)$ を0に更新する。

[0157] S1609において、取引者端末100は、ID、CFP値 x_2 、鍵名称 $N^{AdmY}(n)$ 、暗号化CFP($Enc(x_2, K_{pub}^{AdmY}(n))$ 、 $Enc(x_1+x_2, K_{pub}^{AdmY}(n))$)、乗算・除算回数 $M^{AdmY}(n)$ を含むトレサビ情報をトレサビデータベースDBT1に記録する。

[0158] S1610において、情報送信部120は、管理サーバ200にトレサビデータベースDBT1に記録したトレサビ情報を送信する。その後、UIDを付けた製品が次工程の会社へ納品される。

[0159] S1611において、管理サーバ200は、取引者端末100から送信されたトレサビ情報をトレサビデータベースDBT2に記録する。

[0160] 図17は、監督官庁・CFP管理団体からのCFP値の開示要求があった場合の処理の詳細を示すフローチャートである。図17を用いて、監督官庁・CFP管理団体からCFPの実際の値の開示要求があった場合の処理について説明する。監督官庁・CFP管理団体サーバ300が管理サーバ200

に対してログインを行い、管理サーバ200がログインの認証を行うことにより処理が開始される。

[0161] S1701において、監督官庁・CFP管理団体サーバ300のUID読込部312は、CFP値の開示対象である製品に付されたUIDを読み込む。

[0162] S1702において、情報取得部314は、管理サーバ200に読み込んだUIDを引数としたトレサビ情報の送付要求を送信する。

[0163] S1703において、情報送信部212は、読み込んだUIDに対応するトレサビ情報を監督官庁・CFP管理団体サーバ300の情報取得部314に送信する。

[0164] S1704において、監督官庁・CFP管理団体サーバ300の専用鍵生成部320は、専用の秘密鍵 K_{prv} および公開鍵 K_{pub} のセットを作成し準備する。さらに、情報演算部316は、専用の公開鍵 K_{pub} を用いて数値0の暗号化を行い、暗号情報 $\text{Enc}(0, K_{\text{pub}})$ を計算する。

[0165] S1705において、送付要求送信部322は、管理サーバ200にCFPの実際の値の開示要求を送信する。このとき、引数として、 $N^{\text{Adm}}(n)$ 、 $\text{Enc}(x, K_{\text{pub}}^{\text{Adm}}(n))$ 、 $\text{Enc}(0, K_{\text{pub}})$ を指定する。なお、 $\text{Enc}(x, K_{\text{pub}}^{\text{Adm}}(n))$ は、取得したトレサビ情報内の開示対象の暗号化されたCFP値である。

[0166] S1706において、鍵取得部216は、引数として指定された鍵名称 $N^{\text{Adm}}(n)$ に対応する秘密鍵 $K_{\text{prv}}^{\text{Adm}}(n)$ を鍵データベースDBKから検索して取得する。さらに、解読情報取得部218は、取得した秘密鍵 $K_{\text{prv}}^{\text{Adm}}(n)$ で $\text{Enc}(x, K_{\text{pub}}^{\text{Adm}}(n))$ を解読し x を得る。さらに、暗号化処理部220は、 x に $\text{Enc}(0, K_{\text{pub}})$ を足す秘密計算により、暗号情報 $\text{Enc}(x, K_{\text{pub}})$ を計算する。

[0167] S1707において、提供部222は、監督官庁・CFP管理団体サーバ300に暗号情報 $\text{Enc}(x, K_{\text{pub}})$ を送信する。

[0168] S1708において、情報演算部316は、暗号情報 $\text{Enc}(x, K_{\text{pub}})$ を専用の秘密鍵 K_{prv} を用いて解読し x を取得する。

[0169] 図18は、監督官庁・CFP管理団体以外からのCFP値の開示要求があ

った場合の処理の詳細を示すフローチャートである。図18を用いて、監督官庁・CFP管理団体以外の開示要求者からCFPの実際の値の開示要求があった場合の処理について説明する。監督官庁・CFP管理団体以外の開示要求者（以下、CFP開示要求者）とは、例えば消費者、企業の従業員等である。CFP開示要求者が、自身が使用する端末で管理サーバ200に対してログインを行い、管理サーバ200がログインの認証を行うことにより処理が開始される。ここで、CFP開示要求者が使用する端末は、例えば、スマートフォン、タブレット端末、及びパーソナルコンピュータ等の情報処理装置であって、取引者端末100と同様の構成を有する。したがって、以下では、CFP開示要求者が使用する端末を取引者サーバ100として説明する。

[0170] S1801において、取引者端末100のUID読込部114は、CFP値の開示対象である製品に付されたUIDを読み込む。

[0171] S1802において、情報取得部116は、管理サーバ200に読み込んだUIDを引数としたトレサビ情報の送付要求を送信する。

[0172] S1803において、情報送信部120は、読み込んだUIDに対応するトレサビ情報を取引者端末100の情報取得部116に送信する。

[0173] S1804において、取引者端末100の専用鍵生成部122は専用の秘密鍵 K_{prv} および公開鍵 K_{pub} のセットを作成し準備する。さらに、情報演算部118は、専用の公開鍵 K_{pub} を用いて数値0の暗号化を行い、暗号情報 $\text{Enc}(0, K_{\text{pub}})$ を計算する。

[0174] S1805において、送付要求送信部124は、管理サーバ200にCFPの実際の値の開示要求を送信する。このとき、引数として、 $N^{\text{Adm}}(n)$ 、 $\text{Enc}(x, K_{\text{pub}}^{\text{Adm}}(n))$ 、 $\text{Enc}(0, K_{\text{pub}})$ を指定する。なお、 $\text{Enc}(x, K_{\text{pub}}^{\text{Adm}}(n))$ は、取得したトレサビ情報内の開示対象の暗号化されたCFP値である。

[0175] S1806において、管理サーバ200は、監督官庁・CFP管理団体サーバ300にメッセージを送信し、CFP開示要求者からCFP値の開示要求があったことを伝え、開示してよいか確認を行う。

[0176] S 1 8 0 7 において、監督官庁・C F P 管理団体サーバ 3 0 0 は、開示要求に対して承認または否認を行う。開示要求を否認する場合は、監督官庁・C F P 管理団体サーバ 3 0 0 は、否認メッセージを取引者端末 1 0 0 に送信する。開示要求を承認する場合は、監督官庁・C F P 管理団体サーバ 3 0 0 は、承認の旨を管理サーバ 2 0 0 に送信し、フローは S 1 8 0 8 に進む。

[0177] S 1 8 0 8 において、鍵取得部 2 1 6 は、引数として指定された鍵名称 $N^{Adm}(n)$ に対応する秘密鍵 $K_{prv}^{Adm}(n)$ を鍵データベース D B K から検索して取得する。さらに、解読情報取得部 2 1 8 は、取得した秘密鍵 $K_{prv}^{Adm}(n)$ で $Enc(x, K_{pub}^{Adm}(n))$ を解読し x を得る。さらに、暗号化処理部 2 2 0 は、 x に $Enc(0, K_{pub})$ を足す秘密計算により、暗号情報 $Enc(x, K_{pub})$ を計算する。

[0178] S 1 8 0 9 において、提供部 2 2 2 は、取引者端末 1 0 0 に暗号情報 $Enc(x, K_{pub})$ を送信する。

[0179] S 1 8 1 0 において、情報演算部 1 1 8 は、暗号情報 $Enc(x, K_{pub})$ を専用の秘密鍵 K_{prv} を用いて解読し、 x を取得する。

[0180] (他の実施形態)

以上、本開示の複数の実施形態について説明したが、本開示は、上記実施形態に限定して解釈されるものではなく、本開示の要旨を逸脱しない範囲内において種々の実施形態及び組み合わせに適用することができる。

[0181] 上記実施形態では、アイテム関連情報として各工程の C F P 値を用いたが、各工程にてアイテムに行う処理に関連して使用される電力又はエネルギー資源の使用量情報をアイテム関連情報として用いてもよい。電力の使用量情報には、例えば、水力、火力、風力、地熱、原子力及び太陽光等の発電方法を示す種別情報が紐づけられている。同様に、エネルギー資源の使用量情報には、例えば原油、石炭、天然ガス及び水素等の燃料の種別を示す情報が紐づけられている。また、アイテム関連情報として、レアメタルの使用量または規制対象とされる特定の有害物質の発生量を使用することもできる。

[0182] 以上の例のように、法規的に記録を義務付けられた情報に、本開示によるサプライチェーン管理システム 1 は、特に好適となる。

[0183] 上記実施形態にて、取引者端末１００、管理サーバ２００及び監督官庁・ＣＦＰ管理団体サーバ３００によって提供されていた各機能は、ソフトウェア及びそれを実行するハードウェア、ソフトウェアのみ、ハードウェアのみ、あるいはそれらの複合的な組合せによっても提供可能である。こうした機能がハードウェアとしての電子回路によって提供される場合、各機能は、多数の論理回路を含むデジタル回路、又はアナログ回路によっても提供可能である。

[0184] 本開示は、実施例に準拠して記述されたが、本開示は当該実施例や構造に限定されるものではないと理解される。本開示は、様々な変形例や均等範囲内の変形をも包含する。加えて、様々な組み合わせや形態、さらには、それらに一要素のみ、それ以上、あるいはそれ以下、を含む他の組み合わせや形態をも、本開示の範疇や思想範囲に入るものである。

請求の範囲

[請求項1]

サプライチェーン（SC）を構成する複数の取引者が扱うアイテムに関するアイテム関連情報を管理する情報処理装置（200）であって、

準同型暗号に基づく秘密鍵および該秘密鍵に対応する公開鍵の複数セットのそれぞれを、鍵名称と紐づけて記憶しているデータベース（DBK）と、

前記取引者の取引者端末（100）から、公開鍵を用いてアイテム関連情報を暗号化した暗号情報と、前記アイテム関連情報の暗号化に用いた前記公開鍵の鍵名称とを取得する暗号情報取得部（214）と、

前記鍵名称に対応する秘密鍵を前記データベースから取得する鍵取得部（216）と、

該秘密鍵を用いて前記暗号情報を解読することで解読情報を取得する解読情報取得部（218）と、

前記解読情報を暗号化して再暗号情報を取得する暗号化処理部（220）と、

前記暗号化処理部により暗号化された前記再暗号情報を前記取引者端末に提供する提供部（222）と、を有する情報処理装置。

[請求項2]

前記暗号情報取得部は、前記取引者端末から、第1公開鍵を用いて第1アイテム関連情報を暗号化した第1暗号情報および前記第1アイテム関連情報の暗号化に用いた前記第1公開鍵の第1鍵名称と、第2公開鍵を用いて第2アイテム関連情報を暗号化した第2暗号情報および前記第2アイテム関連情報の暗号化に用いた前記第2公開鍵の第2鍵名称とを取得し、

前記鍵取得部は、前記第1鍵名称に対応する第1秘密鍵と、前記第2鍵名称に対応する第2秘密鍵とを前記データベースから取得し、

前記解読情報取得部は、前記第1秘密鍵を用いて前記第1暗号情報

を解読することで第1解読情報を取得するとともに、前記第2秘密鍵を用いて前記第2暗号情報を解読することで第2解読情報を取得し、

前記暗号化処理部は、前記第1解読情報および前記第2解読情報を用いて得られた計算結果を暗号化して前記再暗号情報を取得する、請求項1に記載の情報処理装置。

[請求項3] 前記暗号情報取得部は、前記取引者の取引者端末から、前記第1鍵名称および前記第2鍵名称とも異なる、第3鍵名称をさらに取得し、

前記鍵取得部は、前記第3鍵名称に対応する公開鍵を前記データベースから取得し、

前記暗号化処理部は、前記第3鍵名称に対応する公開鍵により前記計算結果を暗号化して前記再暗号情報を取得する、請求項2に記載の情報処理装置。

[請求項4] 前記暗号情報取得部は、前記取引者の取引者端末から、第1公開鍵を用いて第1アイテム関連情報を暗号化した第1暗号情報、前記第1アイテム関連情報の暗号化に用いた前記第1公開鍵の第1鍵名称、および前記第1鍵名称とは異なる、第3鍵名称を取得し、

前記鍵取得部は、前記第1鍵名称に対応する第1秘密鍵を前記データベースから取得し、

前記解読情報取得部は、前記第1秘密鍵を用いて前記第1暗号情報を解読することで第1解読情報を取得し、

前記暗号化処理部は、前記第3鍵名称に対応する公開鍵により前記第1解読情報を暗号化して前記再暗号情報を取得する、請求項1に記載の情報処理装置。

[請求項5] 前記鍵取得部は、前記鍵名称に対応する公開鍵を前記データベースから取得し、

前記暗号化処理部は、前記公開鍵により前記解読情報を暗号化して前記再暗号情報を取得する、請求項1に記載の情報処理装置。

[請求項6] 前記暗号情報取得部は、前記取引者の取引者端末から、準同型暗号

に基づく公開鍵であって前記データベースにて管理している公開鍵とは異なる公開鍵を用いて暗号化された暗号情報をさらに取得し、

前記暗号化処理部は、該暗号情報および前記解読情報を用いた秘密計算により前記再暗号情報を取得する、請求項 1 に記載の情報処理装置。

[請求項7] 前記アイテム関連情報は、温室効果ガスの排出量情報を含む、請求項 1 に記載の情報処理装置。

[請求項8] 前記アイテム関連情報は、電力またはエネルギー資源の種別ごとの使用量情報を含む、請求項 1 に記載の情報処理装置。

[請求項9] 請求項 1 から 8 のいずれか一項に記載の情報処理装置（200）と、
前記取引者の取引者端末（100）と、を備える情報処理システム（1）。

[請求項10] 前記取引者端末は、前記提供部により提供された前記再暗号情報およびアイテム関連情報の平文情報を用いた秘密計算により暗号情報を生成する秘密計算部（118）を有する、請求項 9 に記載の情報処理システム。

[請求項11] 前記取引者端末は、前記秘密計算により生成された暗号情報を示すコードを生成するコード生成部（126）を有する、請求項 10 に記載の情報処理システム。

[請求項12] 前記取引者端末は、前記情報処理装置に対して、所定値の暗号情報の送付要求を送信する送付要求送信部（124）を有し、

前記情報処理装置は、

前記暗号化処理部により、前記所定値を暗号化して暗号所定値情報を生成し、

前記提供部により、前記取引者端末に前記暗号所定値情報を提供する請求項 10 に記載の情報処理システム。

[請求項13] 前記取引者端末の前記秘密計算部は、前記暗号所定値情報およびア

アイテム関連情報の平文情報を用いた秘密計算により暗号情報を生成する請求項 1 2 に記載の情報処理システム。

[請求項14] 前記取引者端末は、前記秘密計算により得られた暗号情報を示すコードを生成するコード生成部（1 2 6）をさらに有する、請求項 1 3 に記載の情報処理システム。

[請求項15] サプライチェーンを構成する複数の取引者が扱うアイテムに関するアイテム関連情報を管理する情報処理方法であって、

準同型暗号に基づく秘密鍵および該秘密鍵に対応する公開鍵の複数セットのそれぞれを、鍵名称と紐づけてデータベースに記録するステップと、

前記取引者の取引者端末から、公開鍵を用いてアイテム関連情報を暗号化した暗号情報と、前記アイテム関連情報の暗号化に用いた前記公開鍵の鍵名称とを取得するステップと、

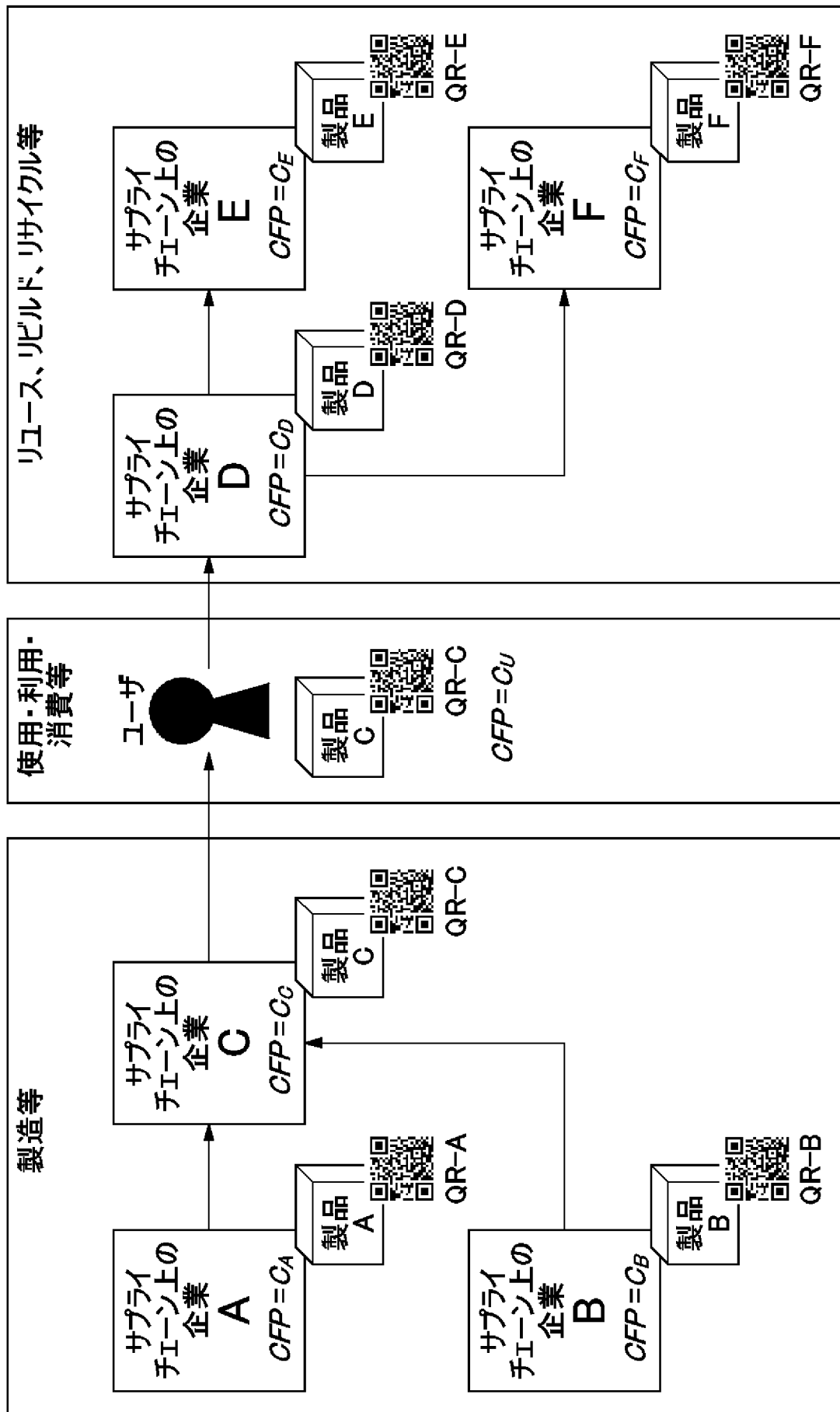
前記鍵名称に対応する秘密鍵を前記データベースから取得するステップと、

該秘密鍵を用いて前記暗号情報を解読することで解読情報を取得するステップと、

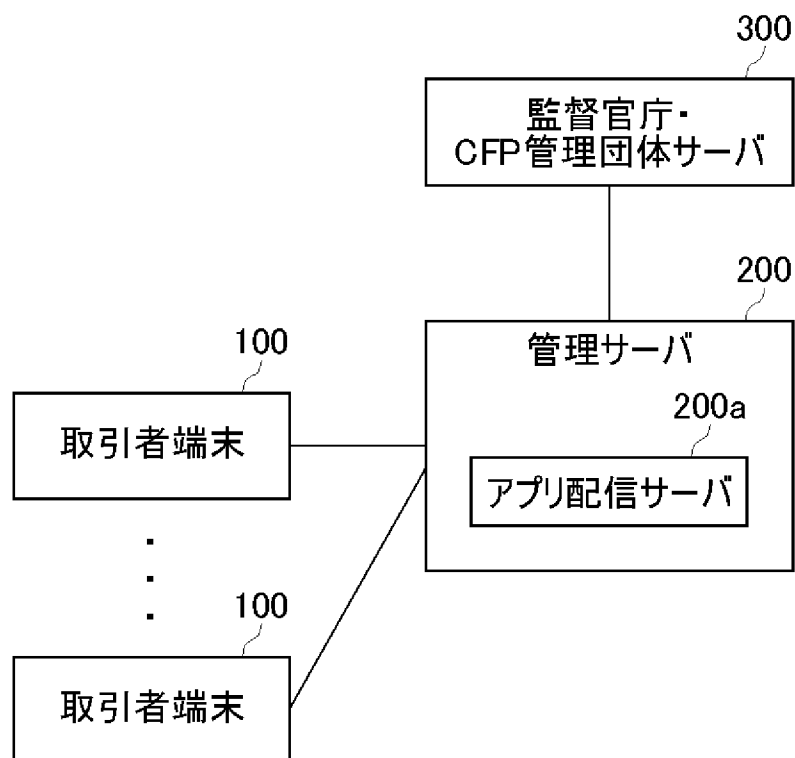
前記解読情報を暗号化して再暗号情報を取得するステップと、

前記再暗号情報を前記取引者端末に提供するステップと、を有する情報処理方法。

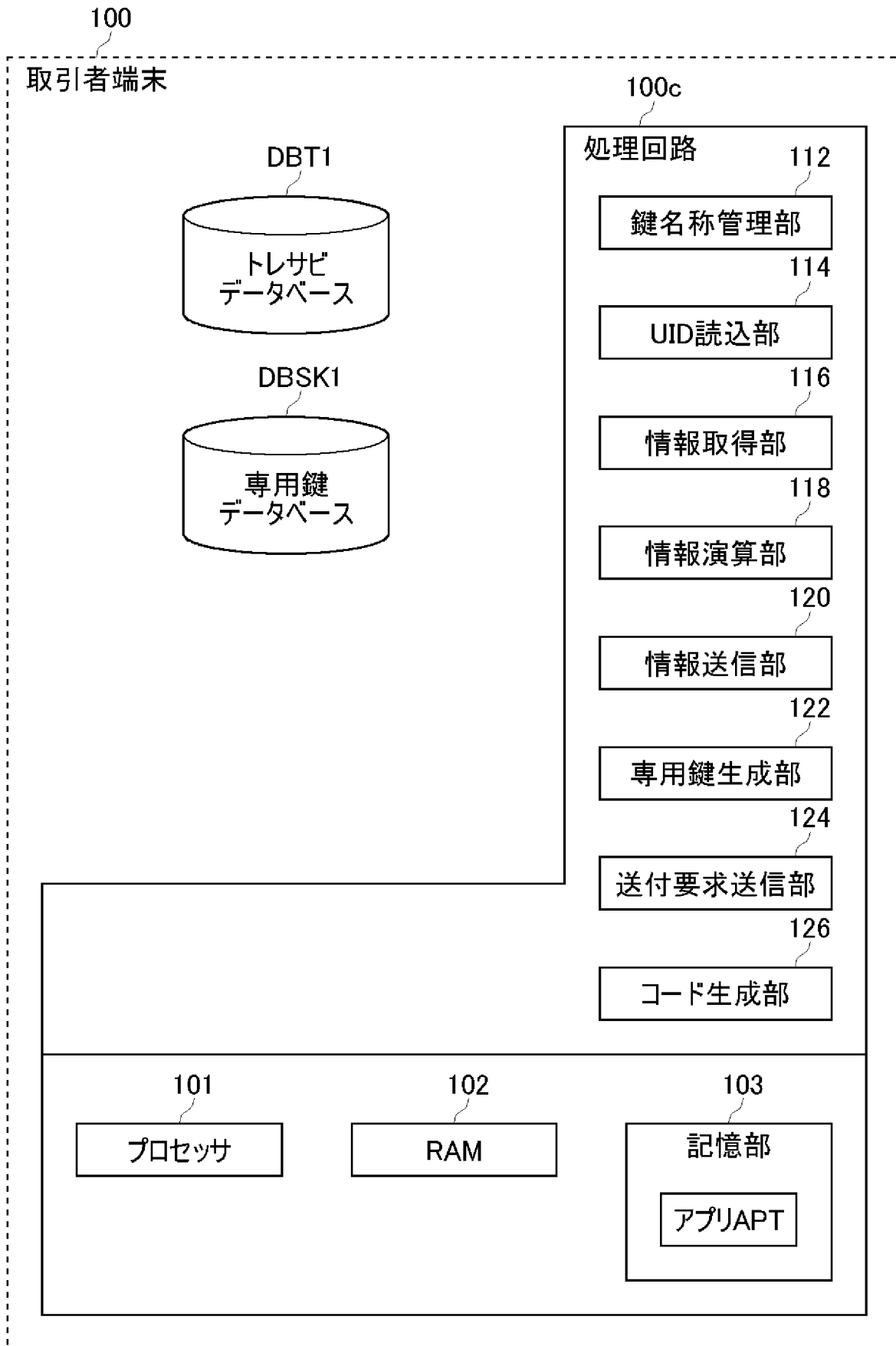
[図1]



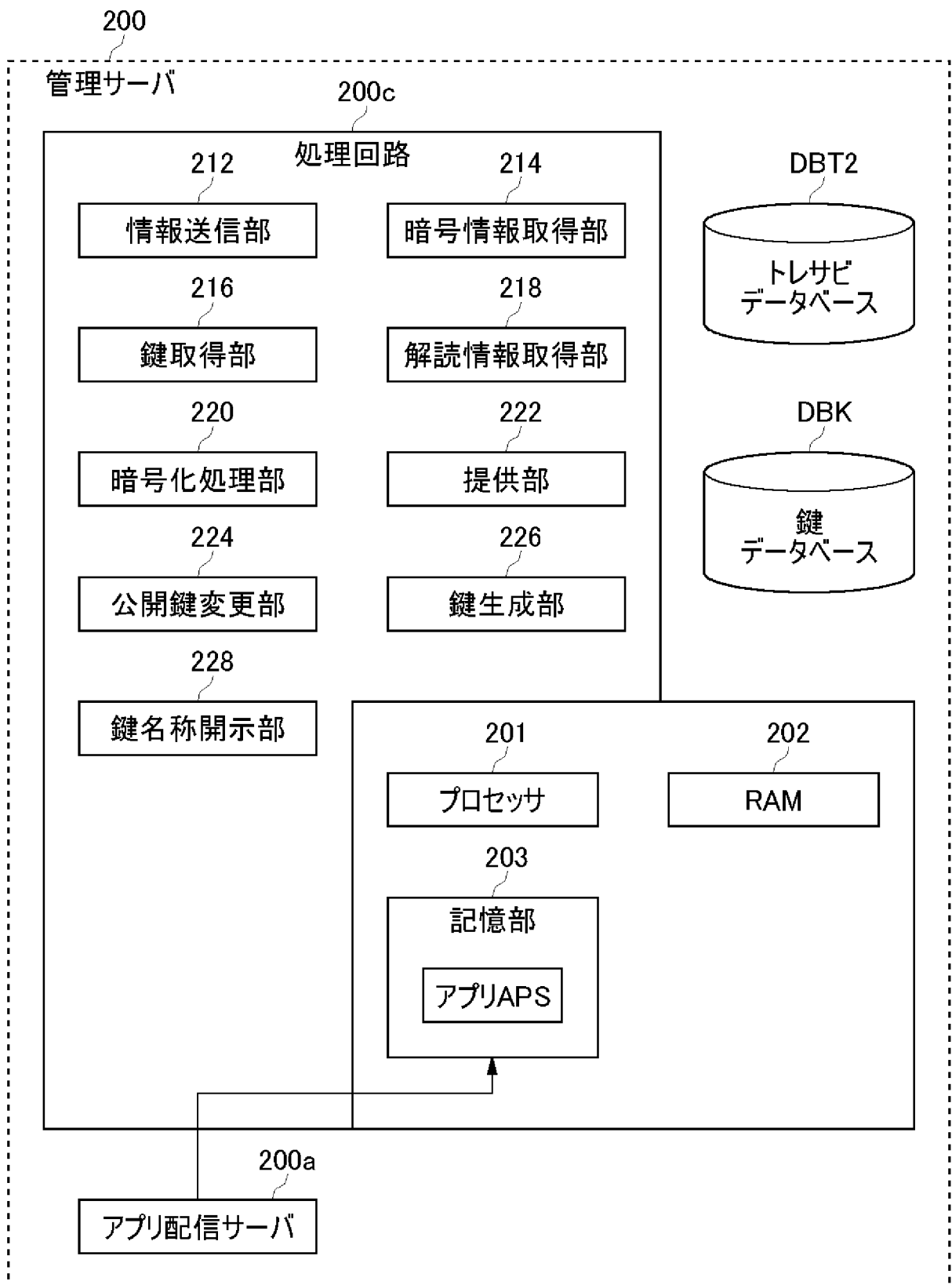
[図2]



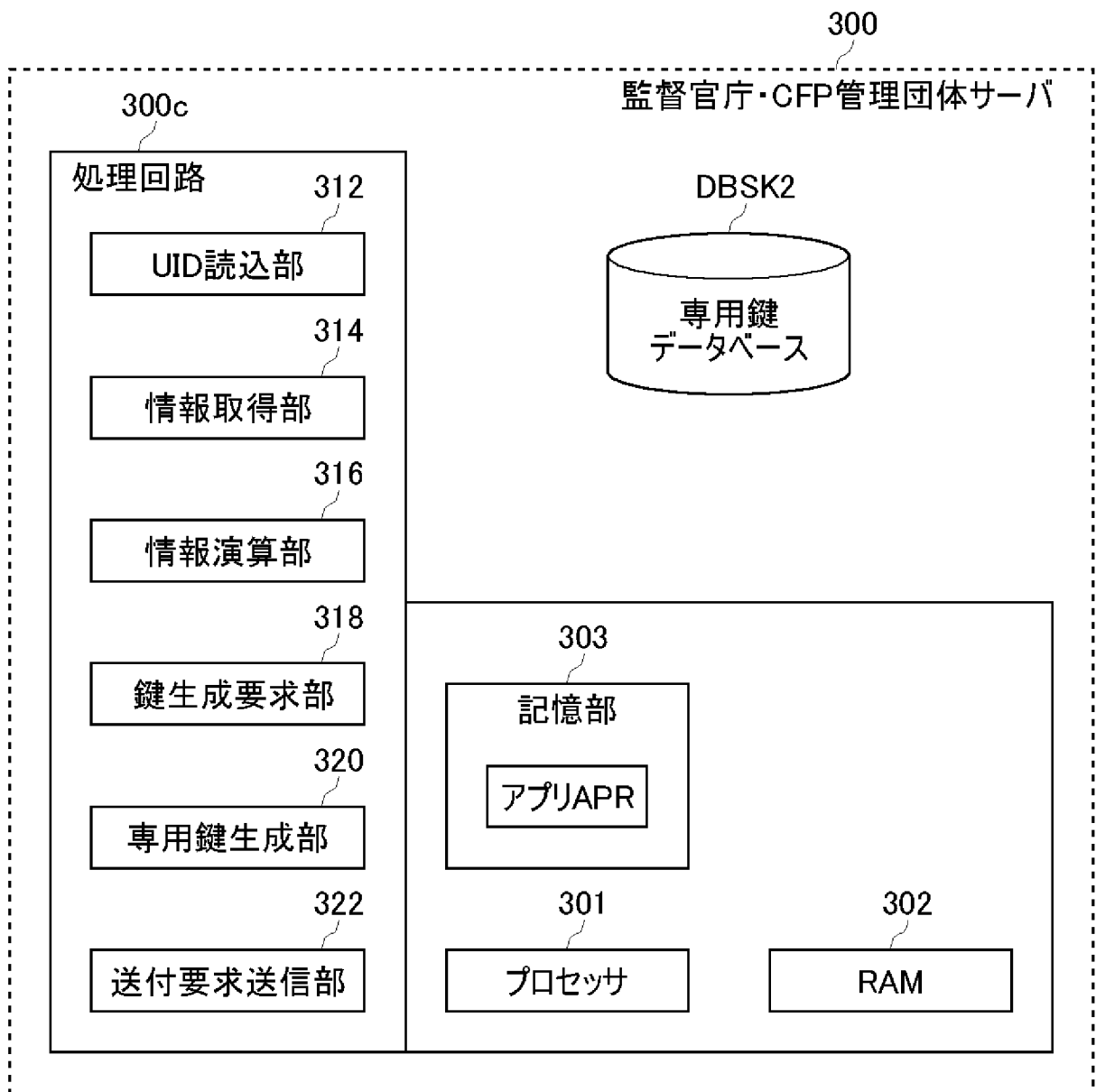
[図3]



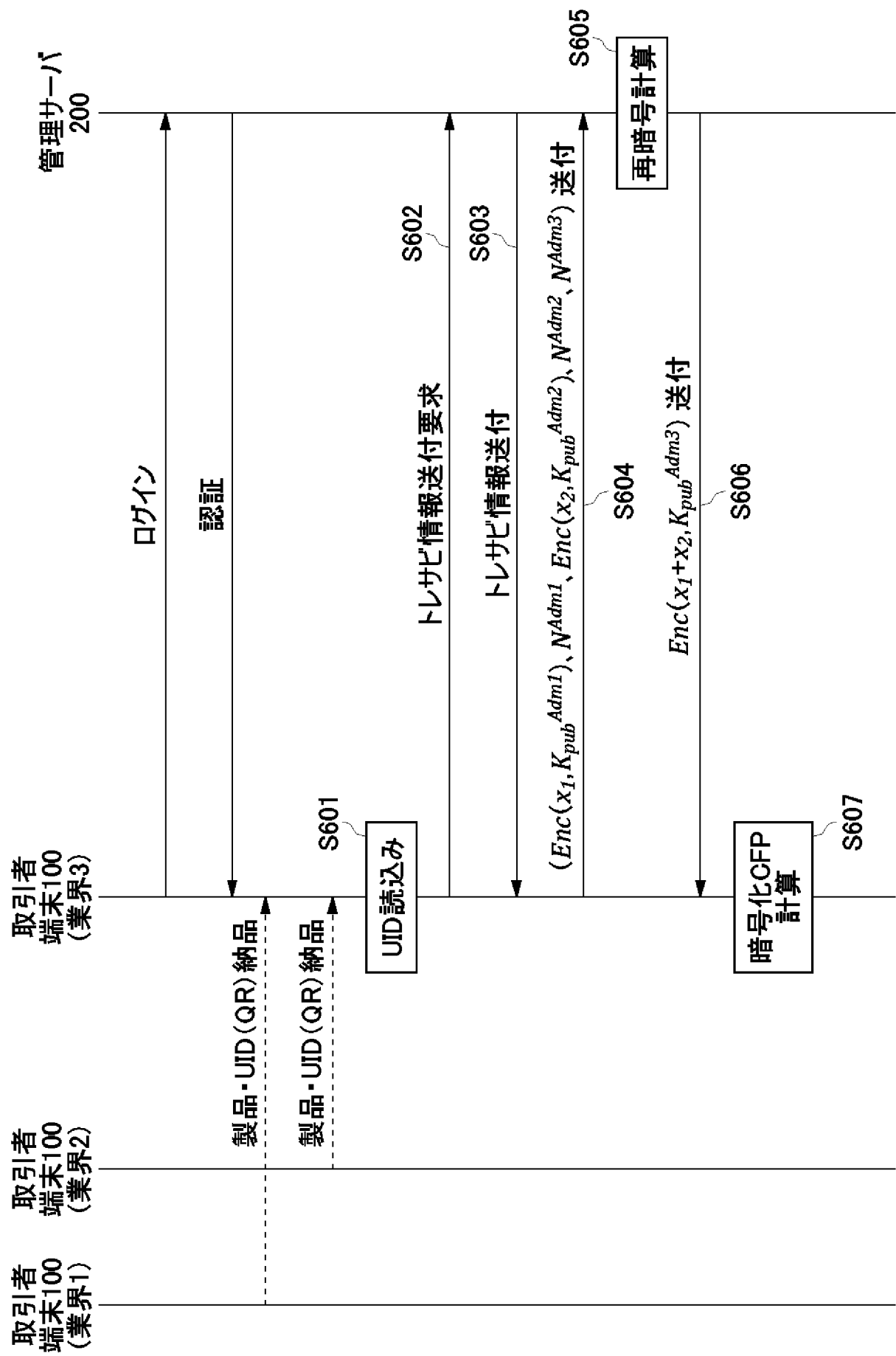
[図4]



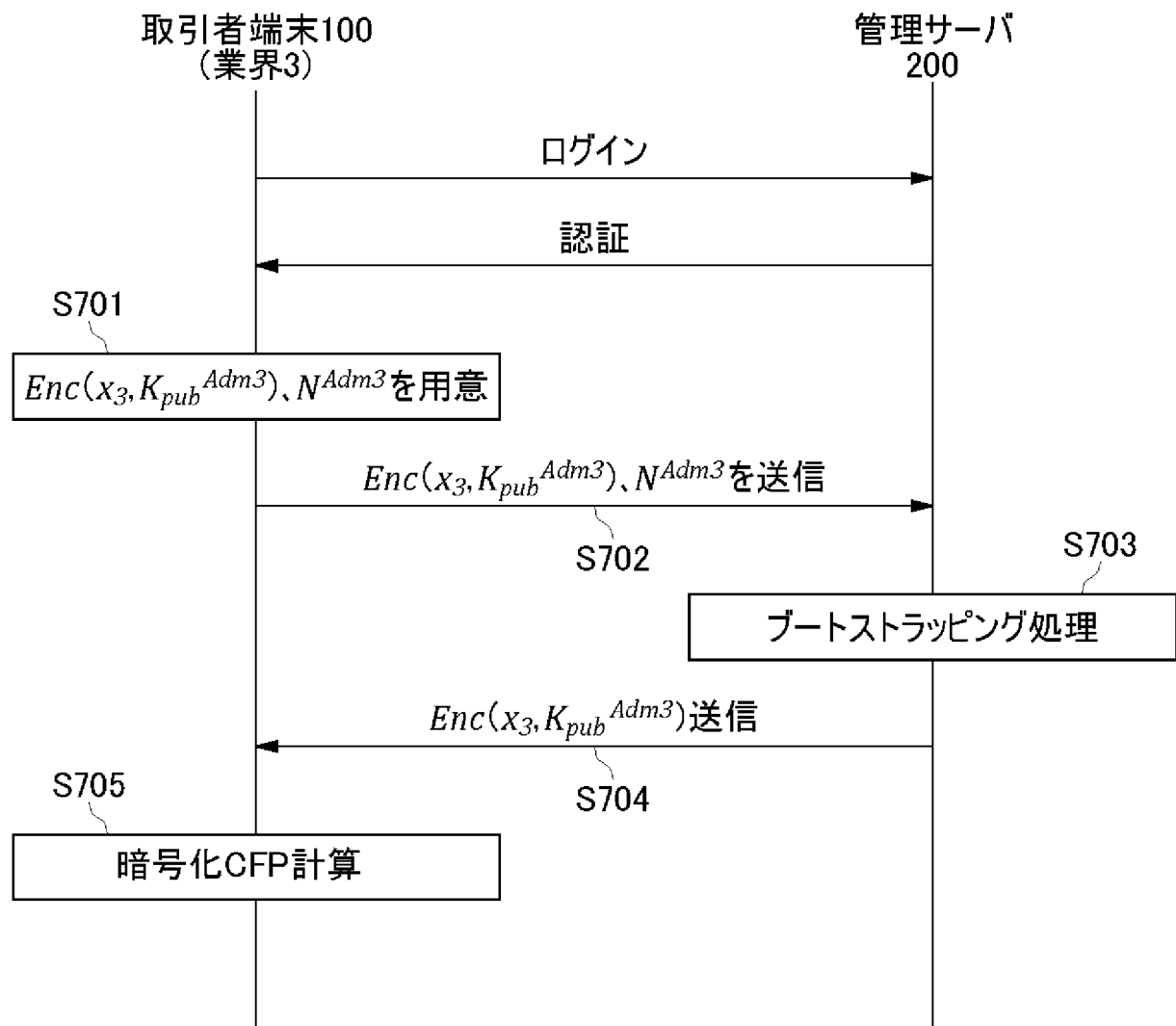
[図5]



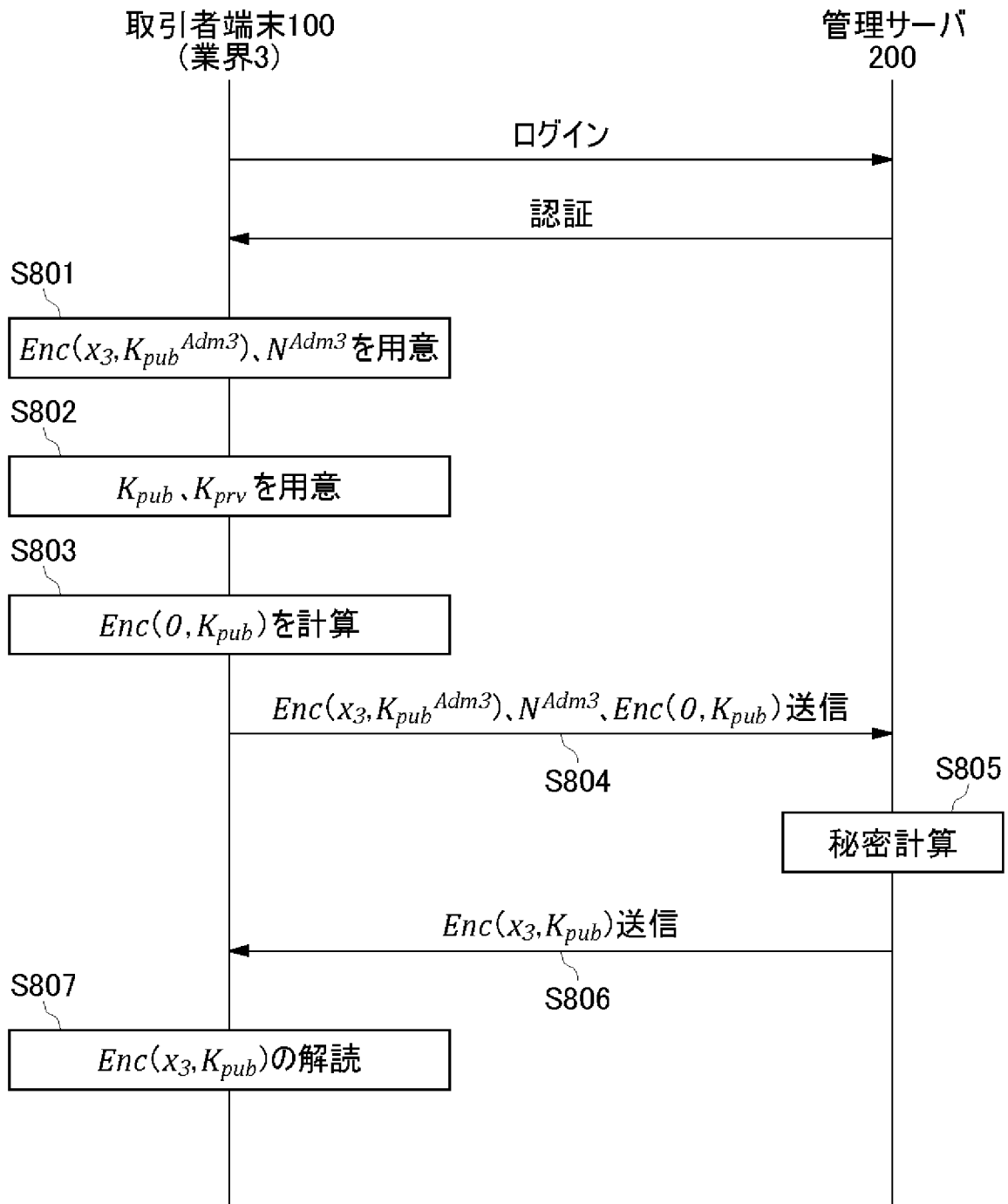
[図6]



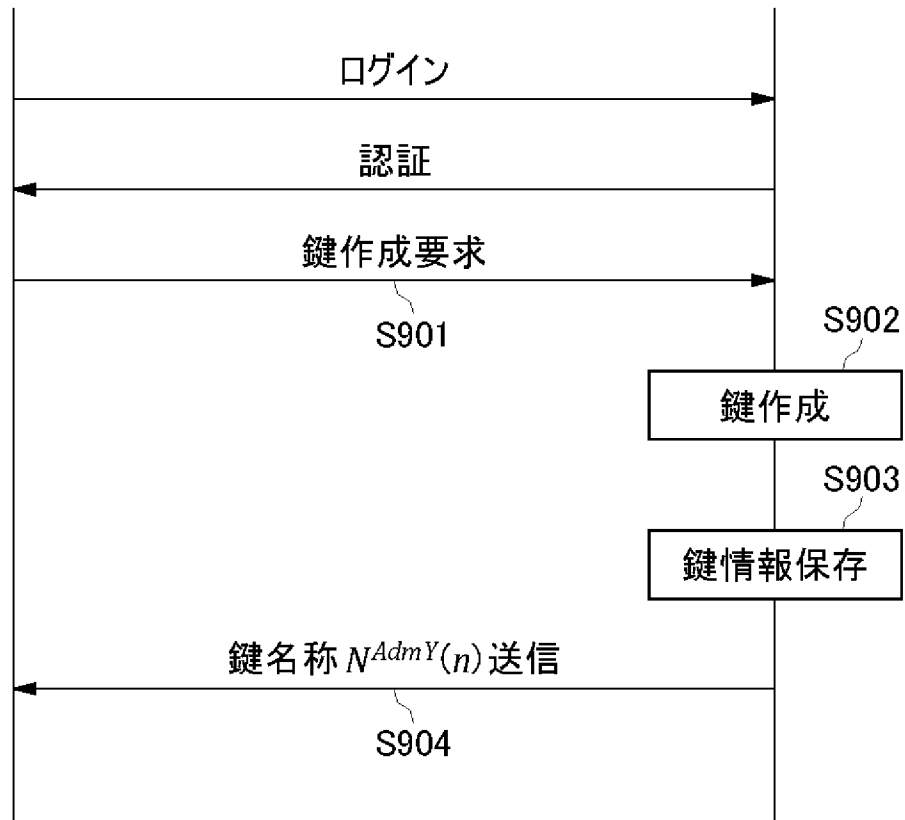
[図7]



[図8]

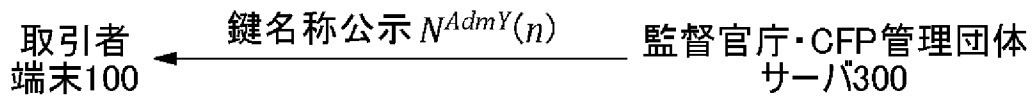


[図9]

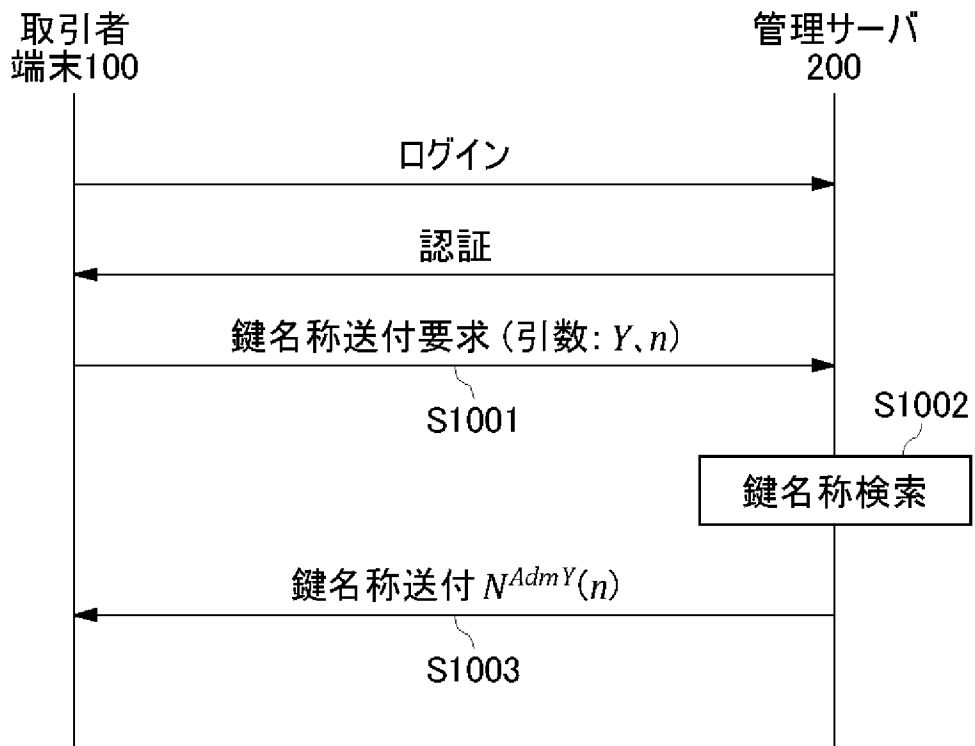
監督官庁・CFP管理団体
サーバ300管理サーバ
200

[図10]

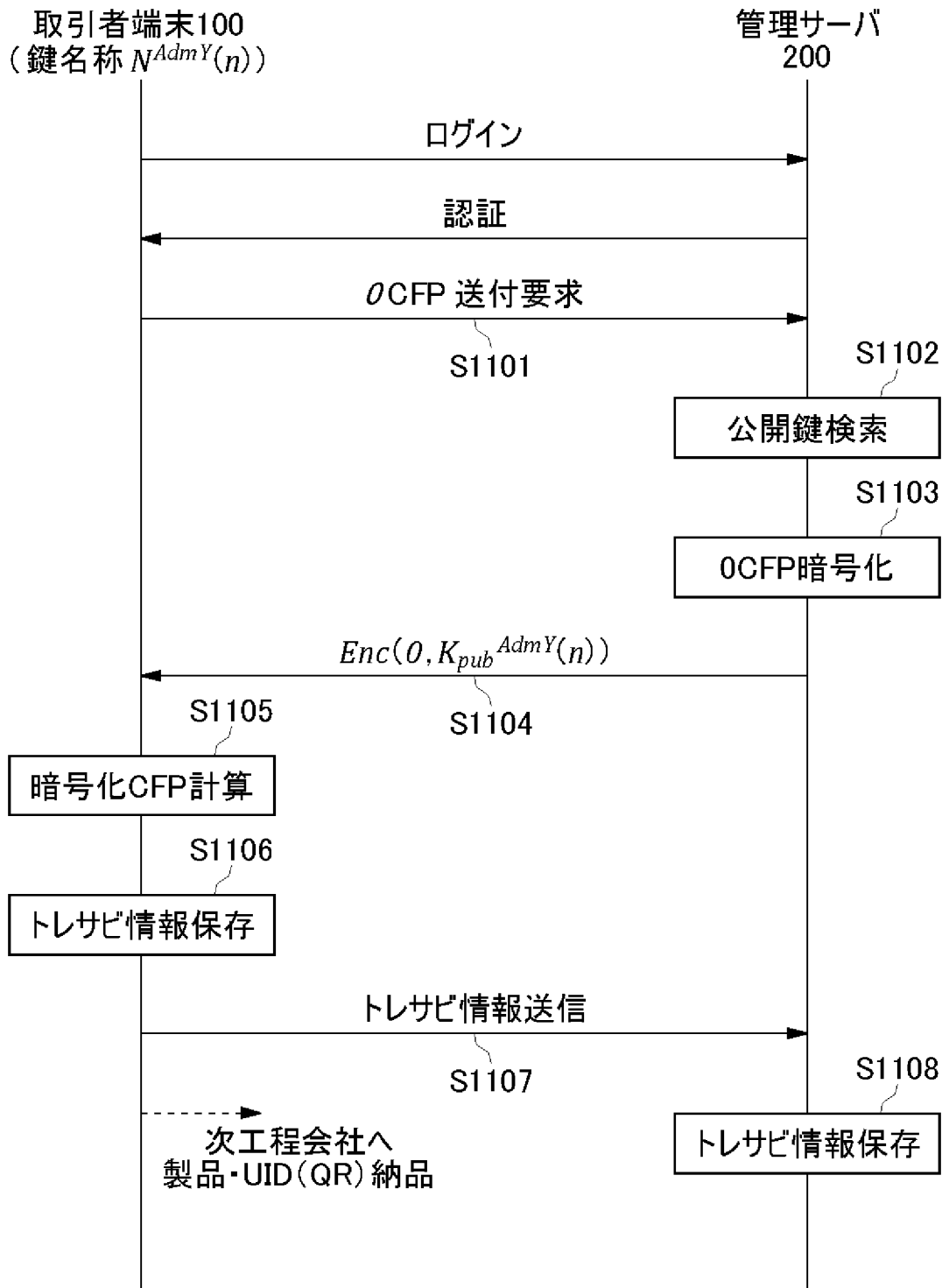
(a)



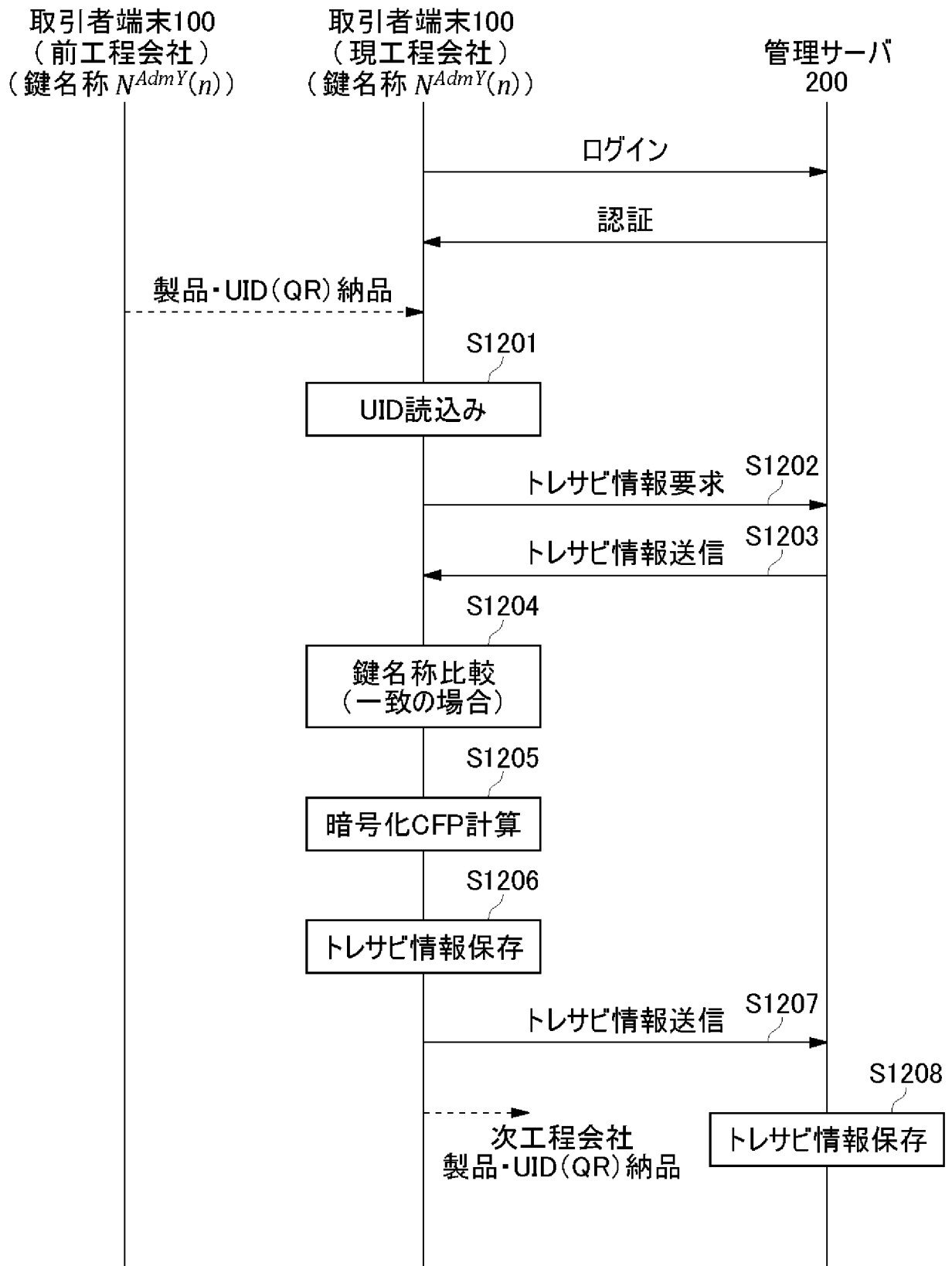
(b)



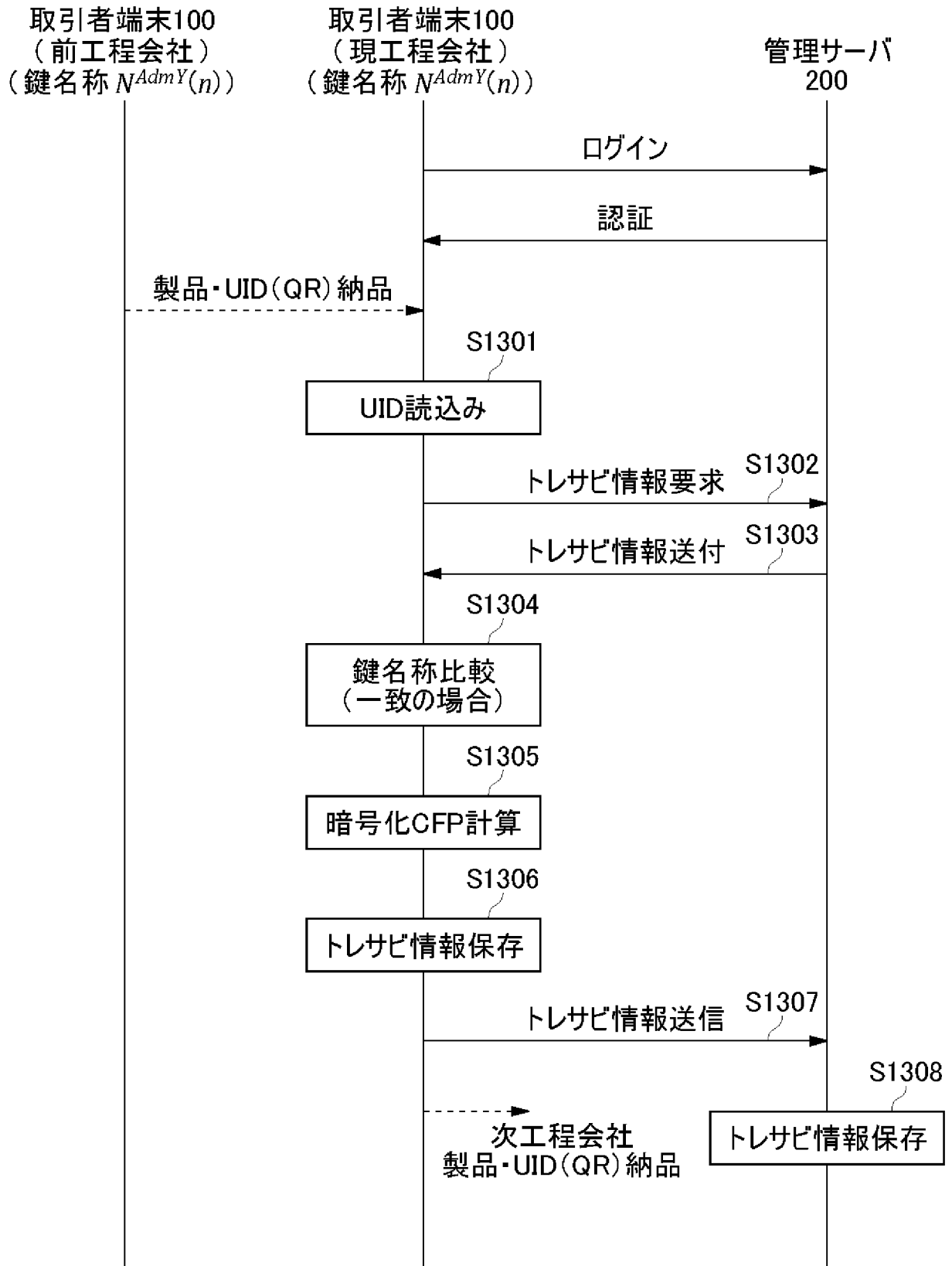
[図11]



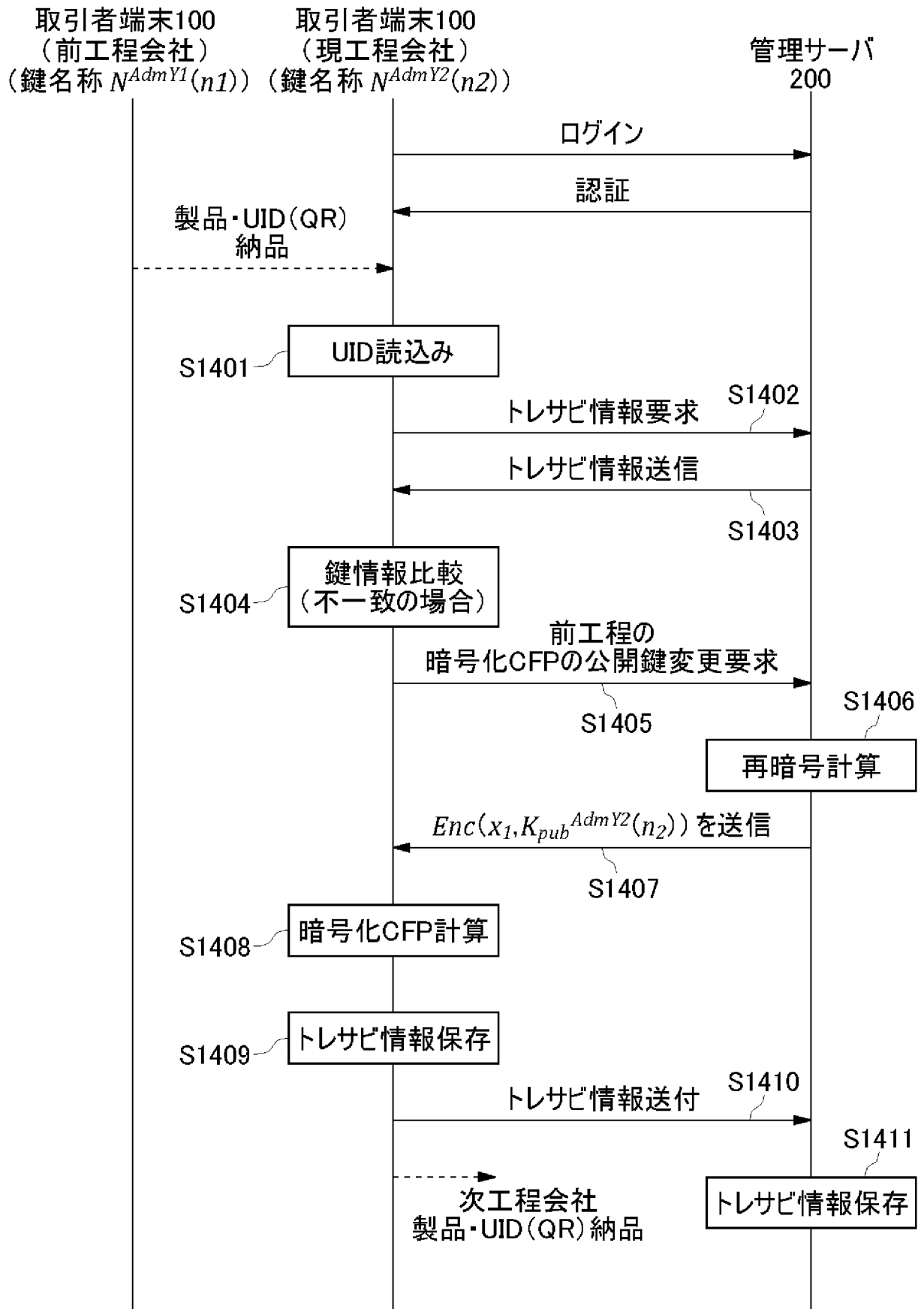
[図12]



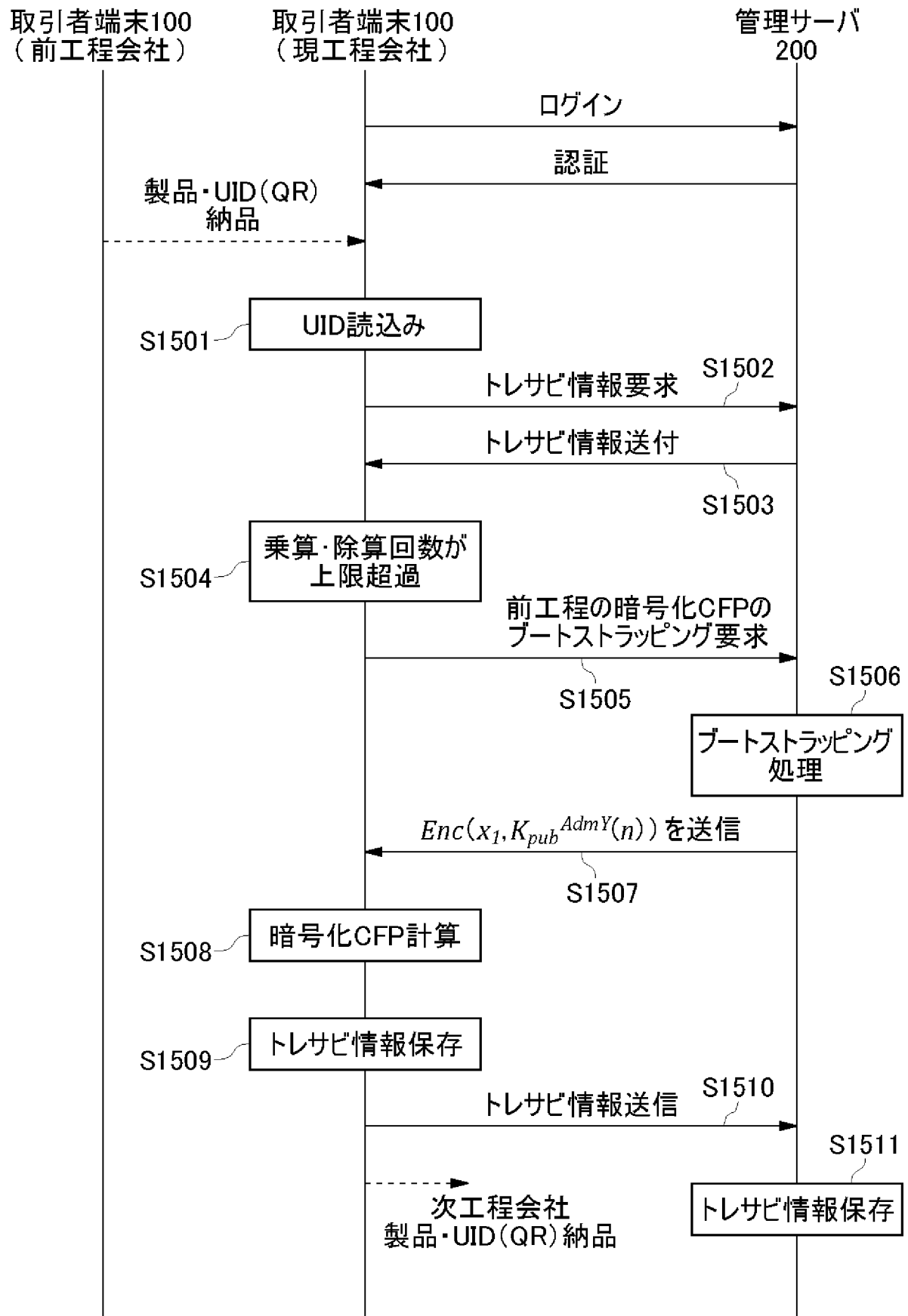
[図13]



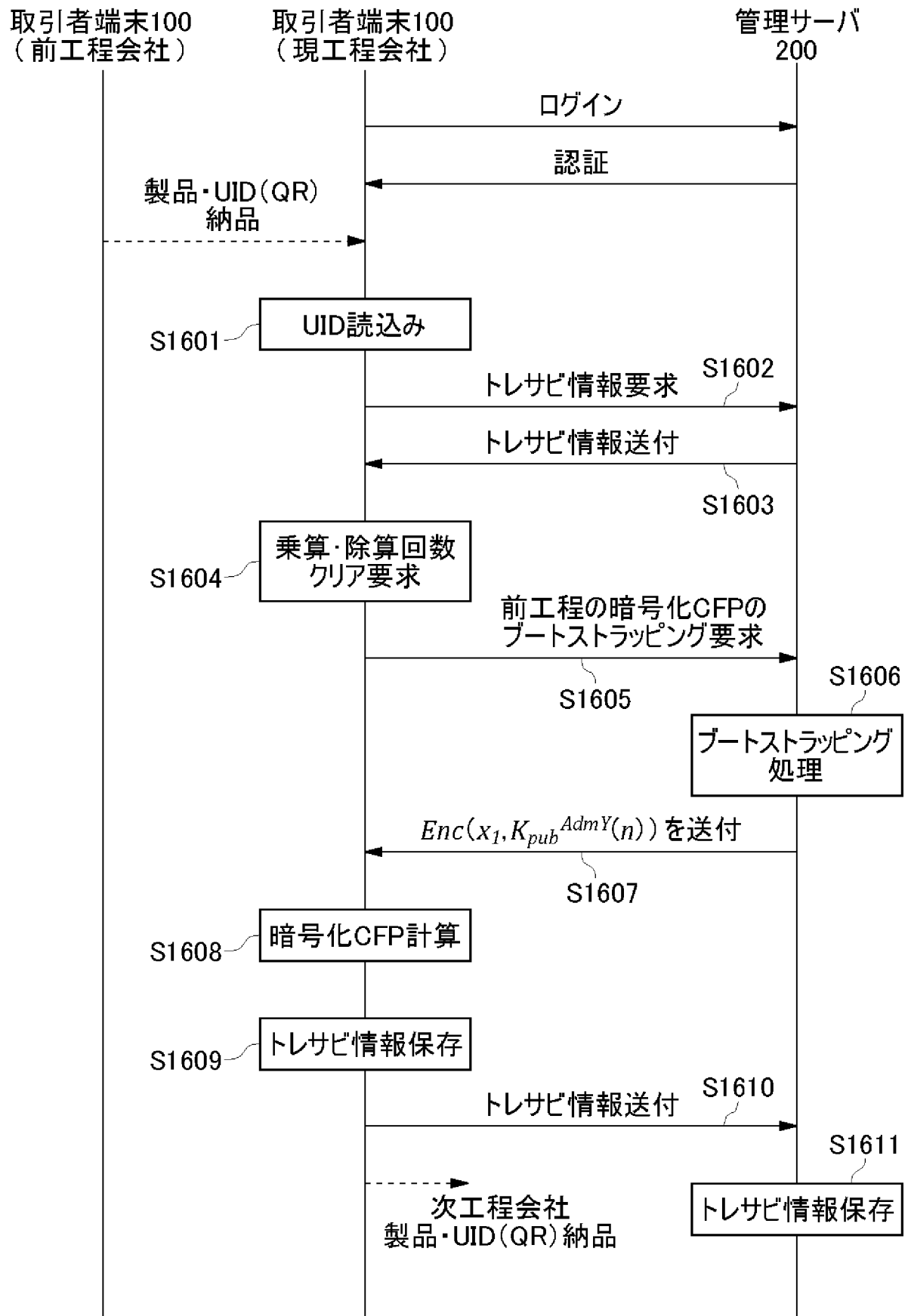
[図14]



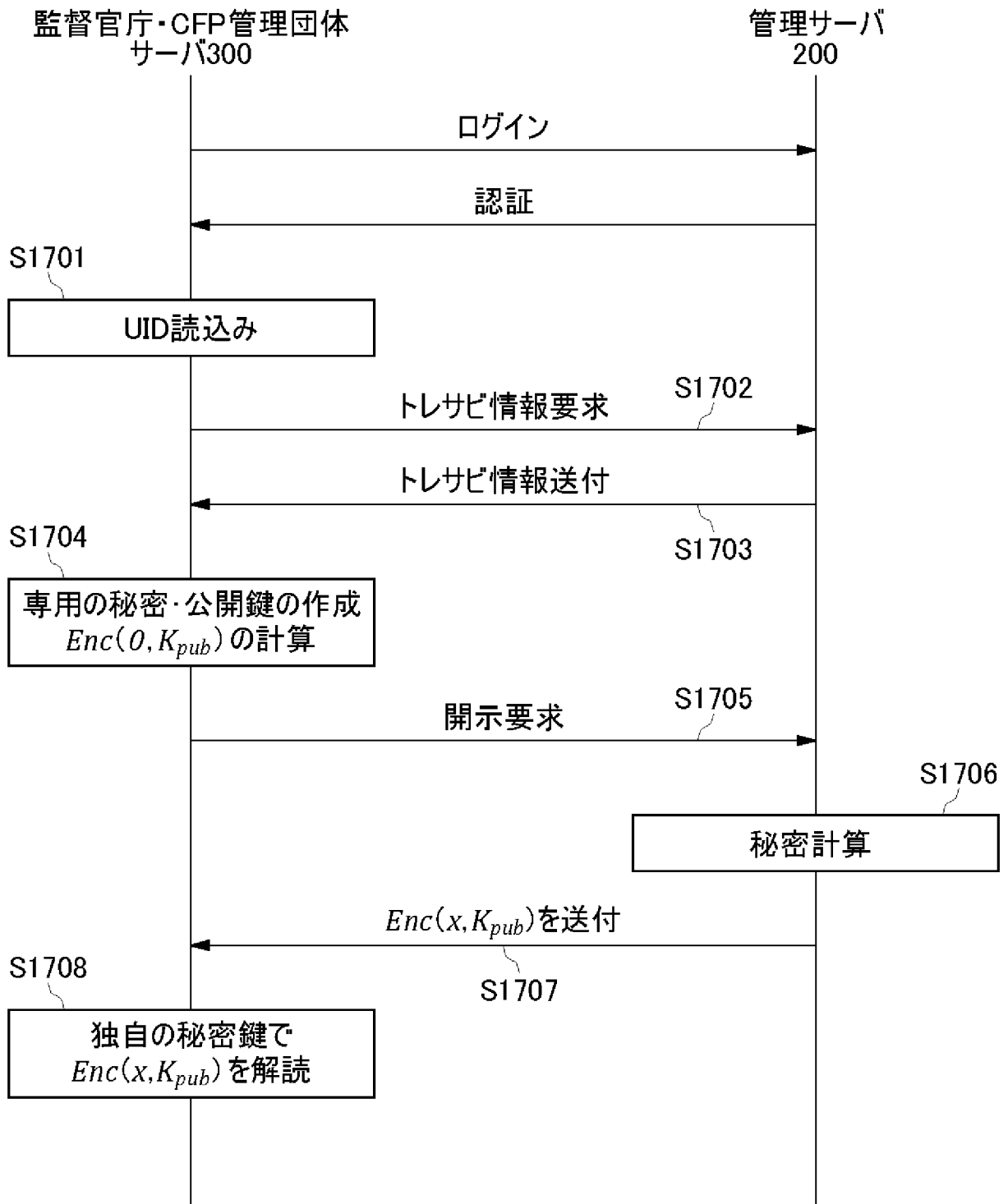
[図15]



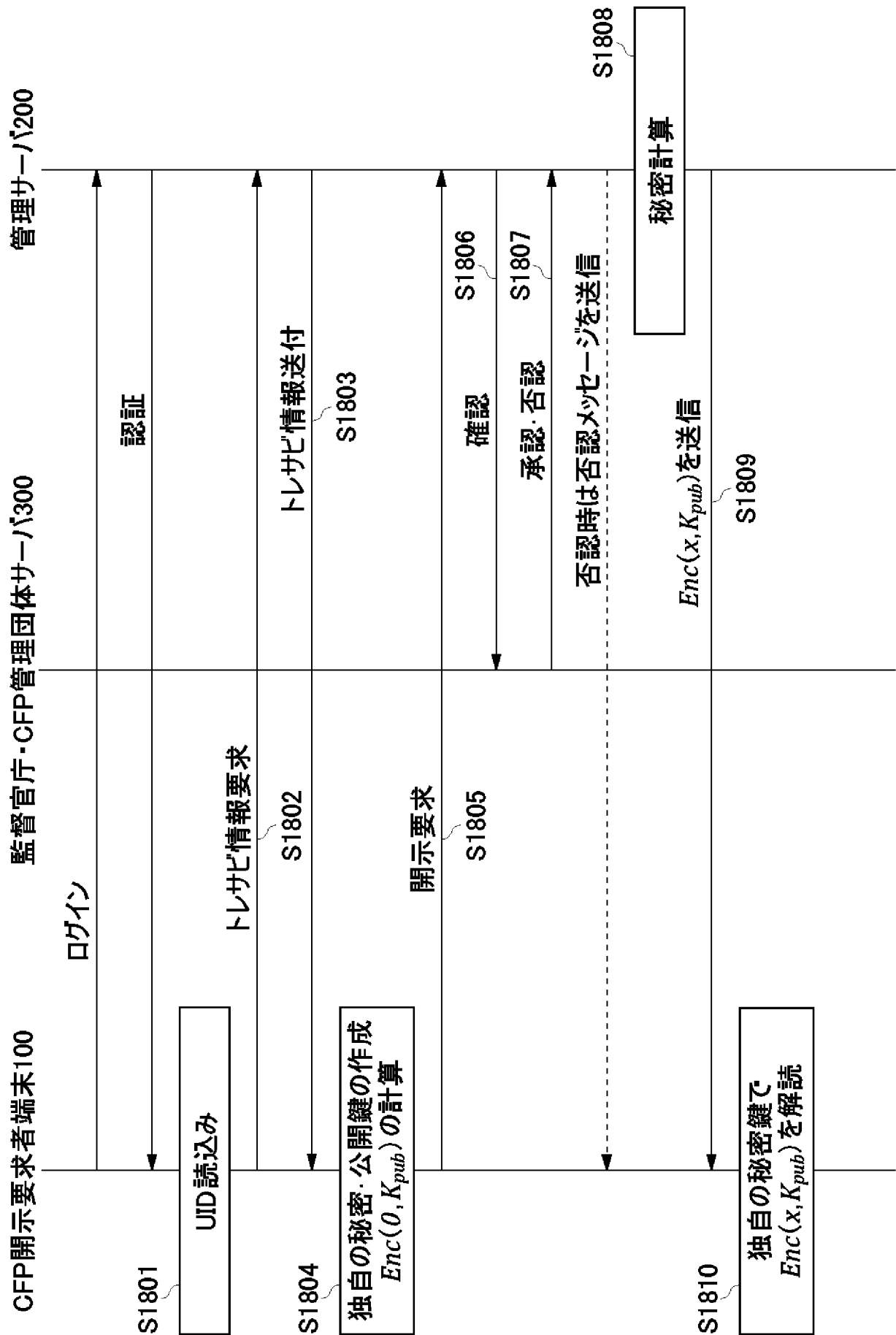
[図16]



[図17]



[図18]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2024/017189

A. CLASSIFICATION OF SUBJECT MATTER H04L 9/14 (2006.01)i; H04L 9/30 (2006.01)i FI: H04L9/14; H04L9/30 Z 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) H04L9/14; H04L9/30 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 1971-2024 Registered utility model specifications of Japan 1996-2024 Published registered utility model applications of Japan 1994-2024 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) JSTPlus/JMEDPlus/JST7580 (JDreamIII); IEEE Xplore homomorphic encryption, carbon footprint		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2021-132323 A (EAGLYS INC.) 09 September 2021 (2021-09-09) paragraphs [0002]-[0167]	1-5, 7-9, 15
A		6, 10-14
Y	KERSCHBAUM, F., STRUKER, J. and KOSLOWSKI, T., Confidential Information-Sharing for Automated Sustainability Benchmarks, 32nd International Conference on Information Systems (ICIS), 2011, pp. 1-17 pp. 4, 5, ERP Systems as a Solution to the Manual Data Gathering Problem, pp. 7-13, A Confidential SBS	1-5, 7-9, 15
Y	JP 2011-164907 A (HITACHI SOLUTIONS, LTD.) 25 August 2011 (2011-08-25) paragraphs [0023]-[0044]	1-5, 7-9, 15
Y	JP 2016-189527 A (MITSUBISHI ELECTRIC CORPORATION) 04 November 2016 (2016-11-04) paragraphs [0036]-[0045]	1-5, 7-9, 15
☒ 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 “D” document cited by the applicant in the international application “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 08 July 2024		Date of mailing of the international search report 16 July 2024
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.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2023-46341 A (EAGLYS INC.) 04 April 2023 (2023-04-04) paragraphs [0013]-[0016], [0135]-[0152]	1-15
A	US 2022/0129847 A1 (SAP SE) 28 April 2022 (2022-04-28) paragraphs [0026]-[0114]	1-15
A	TRONCOSO-PASTORIZA, J. A. and CAPUTO, S., Bootstrap-based Proxy Reencryption for Private Multi-user Computing, 2014 IEEE International Workshop on Information Forensics and Security (WIFS), December 2014, pp. 107-112 IV. PROPOSED SECURE SYSTEM	1-15

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2024/017189

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2021-132323	A	09 September 2021	US 2022/0385455 A1 paragraphs [0002]-[0192] WO 2021/166787 A1 EP 4096146 A1	
JP	2011-164907	A	25 August 2011	(Family: none)	
JP	2016-189527	A	04 November 2016	(Family: none)	
JP	2023-46341	A	04 April 2023	US 2023/0318824 A1 paragraphs [0026]-[0029], [0156]-[0175] WO 2023/047926 A1 EP 4250163 A1	
US	2022/0129847	A1	28 April 2022	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC））

H04L 9/14(2006.01)i; H04L 9/30(2006.01)i

FI: H04L9/14; H04L9/30 Z

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））

H04L9/14; H04L9/30

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

1971-2024年

日本国実用新案登録公報

1996-2024年

日本国登録実用新案公報

1994-2024年

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

JSTPlus/JMEDPlus/JST7580 (JDreamIII); IEEE Xplore homomorphic encryption, carbon footprint

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
Y	JP 2021-132323 A (EAGLYS株式会社) 09.09.2021 (2021 - 09 - 09)	1-5, 7-9, 15
A	段落[0002]-[0167]	6, 10-14
Y	KERSCHBAUM, F., STRUKER, J. and KOSLOWSKI, T., Confidential Information-Sharing for Automated Sustainability Benchmarks, 32nd International Conference on Information Systems (ICIS), 2011, pp.1-17	1-5, 7-9, 15
	pp.4-5 ERP Systems as a Solution to the Manual Data Gathering Problem, pp.7-13 A Confidential SBS	
Y	JP 2011-164907 A (株式会社日立ソリューションズ) 25.08.2011 (2011 - 08 - 25)	1-5, 7-9, 15
	段落[0023]-[0044]	
Y	JP 2016-189527 A (三菱電機株式会社) 04.11.2016 (2016 - 11 - 04)	1-5, 7-9, 15
	段落[0036]-[0045]	
A	JP 2023-46341 A (EAGLYS株式会社) 04.04.2023 (2023 - 04 - 04)	1-15
	段落[0013]-[0016], [0135]-[0152]	

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

* 引用文献のカテゴリー

“A” 特に関連のある文献ではなく、一般的技术水準を示すもの

“D” 国際出願で出願人が先行技術文献として記載した文献

“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

08.07.2024

国際調査報告の発送日

16.07.2024

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）

中里 裕正 5S 9364

電話番号 03-3581-1101 内線 3529

C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	US 2022/0129847 A1 (SAP SE) 28.04.2022 (2022 - 04 - 28) 段落[0026]-[0114]	1-15
A	TRONCOSO-PASTORIZA, J. A. and CAPUTO, S., Bootstrap-based Proxy Reencryption for Private Multi-user Computing, 2014 IEEE International Workshop on Information Forensics and Security (WIFS), 2014.12, pp.107-112 IV. PROPOSED SECURE SYSTEM	1-15

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/JP2024/017189

引用文献			公表日	パテントファミリー文献	公表日
JP	2021-132323	A	09.09.2021	US 2022/0385455 A1 段落[0002]-[0192] WO 2021/166787 A1 EP 4096146 A1	
JP	2011-164907	A	25.08.2011	(ファミリーなし)	
JP	2016-189527	A	04.11.2016	(ファミリーなし)	
JP	2023-46341	A	04.04.2023	US 2023/0318824 A1 段落[0026]-[0029], [0156]-[0175] WO 2023/047926 A1 EP 4250163 A1	
US	2022/0129847	A1	28.04.2022	(ファミリーなし)	