

(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
2024年12月12日(12.12.2024)



(10) 国際公開番号

WO 2024/252681 A1

(51) 国際特許分類:

G06F 21/57 (2013.01) H04L 9/32 (2006.01)
G06F 21/64 (2013.01)

(21) 国際出願番号: PCT/JP2023/021612

(22) 国際出願日: 2023年6月9日(09.06.2023)

(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).

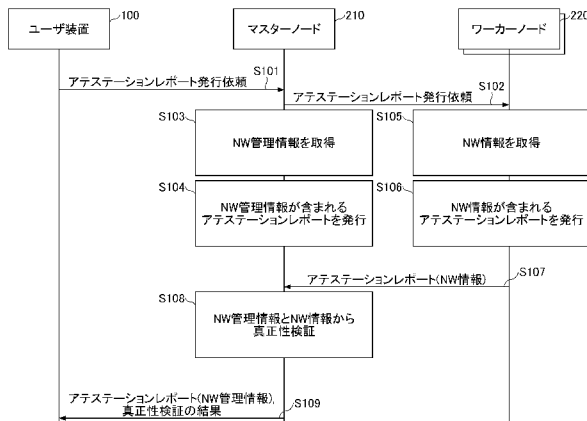
(72) 発明者: 奥田 哲矢(OKUDA, Tetsuya); 〒1808585 東京都武蔵野市緑町3丁目9-11 N T T 知的財産センタ内 Tokyo (JP). 井上 知洋

(INOUE, Tomohiro); 〒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). 馬越 健治(UMAKOSHI, Kenji); 〒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). 柏木 啓一郎(KASHIWAGI, Keiichiro); 〒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). 泉 雅巳(IZUMI, Masami); 〒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). 神谷 弘樹(MITANI, Koki); 〒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). 横関 大子郎(YOKOZEKI, Daigoro); 〒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).

(54) Title: AUTHENTICITY VERIFICATION SYSTEM, AUTHENTICITY VERIFICATION METHOD, AND PROGRAM

(54) 発明の名称: 真正性検証システム、真正性検証方法、及びプログラム

[図5]



100... User device
210... Master node
220... Worker node
S101, S102... Attestation report issuance request
S103... Acquire NW management information
S104... Issue attestation report including NW management information
S105... Acquire NW information
S106... Issue attestation report including NW information
S107... Attestation report (NW information)
S108... Verify authenticity from NW management information and NW information
S109... Attestation report (NW management information), authenticity verification result

(57) Abstract: An authenticity verification system according to one aspect of the present disclosure includes a platform that realizes a cluster configured from a plurality of nodes each provided with an isolated execution environment, and a user device that uses a service provided by the cluster, the authenticity verification system verifying the authenticity of the cluster, wherein the user device has a first transmission unit that transmits an attestation report issuance request to the nodes, and the nodes each have an issuing unit that issues an attestation report including unique information pertaining to the nodes upon receiving the issuance request.

(57) 要約: 本開示の一態様による真正性検証システムは、隔離実行環境をそれぞれ備える複数のノードで構成されるクラスタを実現するプラットフォームと、前記クラスタによって提供されるサービスを利用するユーザ装置とが含まれ、前記クラスタの真正性を検証する真正性検証システムであって、前記ユーザ装置は、前記ノードに対してアステーションレポートの発行依頼を送信する第1の送信部、を有し、前記ノードは、前記発行依頼を受信すると、前記ノードの固有情報が含まれるアステーションレポートを発行する発行部、を有する。

[続葉有]

(74) 代理人: 伊東 忠重, 外 (ITOH, 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, 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:

— 国際調査報告 (条約第21条(3))

明 細 書

発明の名称：

真正性検証システム、真正性検証方法、及びプログラム

技術分野

[0001] 本開示は、真正性検証システム、真正性検証方法、及びプログラムに関する。

背景技術

[0002] クラウド事業者にはデータ（プログラムも含む。）を秘匿したまま計算を行う従来技術として、例えば、Confidential Computing（非特許文献1）やConfidential VM（非特許文献2）等がある。これらの技術により機密性の高いデータの秘密性を保ったまま計算可能な隔離実行環境を構築することが可能となり、例えば、そのデータの秘密性を保ったままクラウド上で何等かの計算処理をするサービスを実現することができる。

先行技術文献

非特許文献

[0003] 非特許文献1：Microsoft Azure Confidential Computing 公式ページ<https://docs.microsoft.com/ja-jp/azure/confidential-computing/overview>
非特許文献2：Google Confidential VM 公式ページ<https://cloud.google.com/compute/confidential-vm/docs?hl=ja>

発明の概要

発明が解決しようとする課題

[0004] しかしながら、複数のノードで構成されるクラスタ（例えば、Kubernetesクラスタ）上で上記のサービスを実現する場合、クラスタ全体の真正性を検証することができない。このため、例えば、或るノードの設定情報の改ざん等を検知できず、安全性を確保することができない。

[0005] 本開示は、上記の点に鑑みてなされたもので、隔離実行環境を備える複数

のノードで構成されるクラスタ全体の真正性を検証可能な技術を提供する。

課題を解決するための手段

[0006] 本開示の一態様による真正性検証システムは、隔離実行環境をそれぞれ備える複数のノードで構成されるクラスタを実現するプラットフォームと、前記クラスタによって提供されるサービスを利用するユーザ装置とが含まれ、前記クラスタの真正性を検証する真正性検証システムであって、前記ユーザ装置は、前記ノードに対してアステーションレポートの発行依頼を送信する第1の送信部、を有し、前記ノードは、前記発行依頼を受信すると、前記ノードの固有情報が含まれるアステーションレポートを発行する発行部、を有する。

発明の効果

[0007] 隔離実行環境を備える複数のノードで構成されるクラスタ全体の真正性を検証可能な技術を提供すること。

図面の簡単な説明

[0008] [図1]本発明の一実施形態におけるシステム構成例を示す図である。
[図2]ユーザ装置の機能構成例を示す図である。
[図3]マスターノードの機能構成例を示す図である。
[図4]ワーカーノードの機能構成例を示す図である。
[図5]実施例1における真正性検証処理の流れを示すシーケンス図である。
[図6]実施例2における真正性検証処理の流れを示すシーケンス図である。
[図7]実施例1におけるデータ分配処理の流れを示すシーケンス図である。
[図8]実施例2におけるデータ分配処理の流れを示すシーケンス図である。
[図9]実施例3におけるデータ分配処理の流れを示すシーケンス図である。
[図10]コンピュータのハードウェア構成例を示す図である。

発明を実施するための形態

[0009] 以下、本発明の一実施形態について説明する。以下で説明する実施形態は一例に過ぎず、本発明が適用される実施形態は以下の実施形態に限定される

ものではない。なお、以下では、隔離実行環境上でデータ（プログラムも含む。）の秘密性を保ったまま何等かの計算処理を実行するサービスのことを「秘匿実行サービス」と呼ぶことにする。ここで、隔離実行環境は、例えば、`Confidential Computing`（非特許文献1）や`Confidential VM`（非特許文献2）等の技術により実現可能である。隔離実行環境は`TEE`（Trusted Execution Environment）等と呼ばれ、データ処理を既存の`OS`（Operating System）から独立して実行可能な環境のことである。`TEE`は、例えば、`AMD`（登録商標）の`SEV`、`Intel`（登録商標）の`SGX`や`TDX`、`Arm`（登録商標）の`TrustZone`（登録商標）、`ARM Confidential Compute Architecture`等といった`CPU`（Central Processing Unit）が備えている。なお、隔離実行環境は、例えば、秘密計算機構、秘匿計算機構、サンドボックス等と呼ばれてもよい。

[0010] <システム構成例>

一実施形態におけるシステムの構成例を図1に示す。図1に示すシステムには、ユーザ装置100と、プラットフォーム200とが含まれる。また、ユーザ装置100とプラットフォーム200は、例えば、インターネット等を含む通信ネットワーク300に接続される。

[0011] ユーザ装置100は、秘匿実行サービスのユーザが利用する各種装置（例えば、`PC`（パーソナルコンピュータ）、スマートフォン、タブレット端末、ウェアラブルデバイス等）である。秘匿実行サービスのユーザは、当該秘匿実行サービスに用いられるデータ（プログラムも含む。）の所有者であってもよいし、そのサービスの実行結果のみを取得又は利用する者であってもよい。

[0012] プラットフォーム200は、隔離実行環境をそれぞれ備える複数のノードで構成されるクラスタを実現する物理マシン又は物理マシン群である。ここで、クラスタを構成する各ノードは、例えば、仮想マシン（`VM` : Virtual Machine）、コンテナ、ポッド等で実現される。以下では、一例として、クラ

スタを構成するノードはKubernetesノードであり、各ノードはポッドで実現されることを想定する。ただし、クラスタ及びそれを構成する各ノードの実現方法はこれに限られるものではない。

[0013] また、クラスタを構成するノードには、マスターノードとワーカーノードとが存在するものとする。図1に示す例では、マスターノード210と、3つのワーカーノード220とが図示されている。ただし、これは一例であって、マスターノードとワーカーノードの区別がなくてもよい。

[0014] マスターノード210及び各ワーカーノード220はいずれも隔離実行環境を実現しており、TEEが提供するアテステーションレポート (Attestation Report) と呼ばれるレポートを発行することができる。アテステーションレポートとは、任意の属性情報を含めることが可能な署名付きの情報である。そこで、本実施形態では、このアテステーションレポートを利用してユーザがクラスタの真正性を検証する場合について説明する。より具体的には、ノード固有の情報をアテステーションレポートに含めることにより、ユーザがクラスタの真正性を検証可能とする。

[0015] <前提>

以下、本実施形態の前提となる事項について説明する。

[0016] ・各ノードはその生成（起動）時に任意の公開鍵暗号方式により公開鍵と秘密鍵の鍵ペアを作成する。これは、ユーザ装置100とノード間、各ノード間は必ずしもセキュアであるとは限らないため、それらの間でデータを送信する際の暗号化するため等に用いられる。以下、上記の鍵をサンドボックス鍵と呼び、それぞれサンドボックス秘密鍵、サンドボックス公開鍵と呼ぶことにする。なお、例えば、マスターノード210で各ワーカーノード220の鍵ペアを生成し、それらの鍵ペアを各ワーカーノード220に分配してもよい。

[0017] ・各ノード及びユーザ装置100は通信相手にデータを送信する際の暗号化に必要なサンドボックス公開鍵を所持しているものとする。

[0018] ・各ノードに保管されるデータのアクセス制御等のためのポリシーが予め

合意され、各ノードは必要なポリシー（ポリシー全体又はその一部）を所持しているものとする。例えば、マスターノード210はポリシー全体を所持しており、各ワーカーノード220はそのワーカーノード220に保管されるデータのアクセス制御等のための部分的なポリシーを所持している。以下、マスターノード210が持つポリシーを全体ポリシーと呼び、各ワーカーノード220が持つポリシーを部分ポリシーと呼ぶことにする。なお、部分ポリシーは、例えば、マスターノード210から各ワーカーノード220に配布（分配）される。

[0019] <ユーザ装置100の機能構成例>

ユーザ装置100の機能構成例を図2に示す。図2に示すように、ユーザ装置100は、アテステーションレポート発行依頼部101と、アテステーションレポート受信部102と、データ提供部103とを有する。これら各部は、例えば、ユーザ装置100にインストールされた1以上のプログラムが、CPU等のプロセッサに実行させる処理により実現される。

[0020] アテステーションレポート発行依頼部101は、クラスタの真正性を検証するために、マスターノード210に対してアテステーションレポート発行依頼を送信する。

[0021] アテステーションレポート受信部102は、ノード固有情報が含まれるアテステーションレポートをマスターノード210から受信する。また、このとき、アテステーションレポート受信部102は、マスターノード210がワーカーノード220のアテステーションレポートに含まれるノード固有情報を検証した結果（真正性検証の結果）も受信する。

[0022] データ提供部103は、秘匿実行サービスに用いられるデータをマスターノード210に送信する。このとき、データ提供部103は、マスターノード210のサンドボックス公開鍵で当該データを暗号化した上で、その暗号化データをマスターノード210に送信する。

[0023] <マスターノード210の機能構成例>

マスターノード210の機能構成例を図3に示す。図3に示すように、マ

スターノード２１０は、オーケストレーション機能部２１１と、アテステーションレポート発行部２１２と、アテステーションレポート発行依頼部２１３とを有する。これら各部は、例えば、プラットフォーム２００にインストールされた１以上のプログラムが、ＣＰＵ等のプログラムに実行させる処理により実現される。

[0024] オーケストレーション機能部２１１は、ワーカーノード２２０を制御したり、自身のノード固有情報を取得したり、各ワーカーノード２２０からのアテステーションレポートに含まれるノード固有情報を検証したり、他の各部に処理を依頼したりする。

[0025] アテステーションレポート発行部２１２は、ＴＥＥによりアテステーションレポートを発行する。このとき、アテステーションレポート発行部２１２は、自身（マスターノード２１０）のノード固有情報が含まれるアテステーションレポートを発行する。

[0026] アテステーションレポート発行依頼部２１３は、各ワーカーノード２２０に対してアテステーションレポート発行依頼を送信する。

[0027] ＜ワーカーノード２２０の機能構成例＞

ワーカーノード２２０の機能構成例を図４に示す。図４に示すように、ワーカーノード２２０は、エージェント機能部２２１と、アテステーションレポート発行部２２２とを有する。これら各部は、例えば、プラットフォーム２００にインストールされた１以上のプログラムが、ＣＰＵ等のプログラムに実行させる処理により実現される。

[0028] エージェント機能部２２１は、自身のノード固有情報を取得したり、他の各部に処理を依頼したりする。

[0029] アテステーションレポート発行部２２２は、ＴＥＥによりアテステーションレポートを発行する。このとき、アテステーションレポート発行部２２２は、自身（ワーカーノード２２０）のノード固有情報が含まれるアテステーションレポートを発行する。

[0030] ＜真正性検証処理＞

以下、マスターノード210及び各ワーカーノード220で構成されるクラスタの真正性をユーザが検証とする真正性検証処理の実施例1及び2について説明する。

[0031] 《真正性検証処理（実施例1）》

実施例1における真正性検証処理の流れについて、図5を参照しながら説明する。

[0032] ユーザ装置100のアテステーションレポート発行依頼部101は、マスターノード210に対してアテステーションレポート発行依頼を送信する（ステップS101）。

[0033] マスターノード210のアテステーションレポート発行依頼部213は、オーケストレーション機能部211によってアテステーションレポート発行依頼を受信すると、各ワーカーノード220に対してアテステーションレポート発行依頼をそれぞれ送信する（ステップS102）。

[0034] マスターノード210のオーケストレーション機能部211は、自身のノード固有情報としてNW管理情報を取得する（ステップS103）。ここで、NW管理情報とはクラスタ全体のネットワークに関する情報であり、例えば、各ワーカーノード220のIP（Internet Protocol）アドレス、ポート番号、FW設定、タスク名、イメージ名等が含まれる。NW管理情報は、例えば、Kubernetesが提供するコマンド等の機能により取得可能である。

[0035] マスターノード210のアテステーションレポート発行部212は、上記のステップS103で取得されたNW管理情報が含まれるアテステーションレポートを発行する（ステップS104）。

[0036] 各ワーカーノード220のエージェント機能部221は、自身のノード固有情報としてNW情報を取得する（ステップS105）。ここで、NW情報とは当該ワーカーノード220のネットワークに関する情報であり、例えば、当該ワーカーノード220のIPアドレス、ポート番号、FW設定、タスク名、イメージ名等が含まれる。NW情報は、例えば、Kubernet

s が提供するコマンド等の機能により取得可能である。

[0037] 各ワーカーノード 220 のアテストーションレポート発行部 222 は、上記のステップ S 105 で取得された NW 情報が含まれるアテストーションレポートを発行する（ステップ S 106）。

[0038] 各ワーカーノード 220 のアテストーションレポート発行部 222 は、上記のステップ S 106 で発行されたアテストーションレポートをマスターノード 210 に送信する（ステップ S 107）。

[0039] マスターノード 210 のオーケストレーション機能部 211 は、上記のステップ S 103 で取得された NW 管理情報と、各ワーカーノード 220 から受信したアテストーションレポートに含まれる NW 情報とを用いて、各ワーカーノード 220 の真正性を検証する（ステップ S 108）。すなわち、オーケストレーション機能部 211 は、NW 管理情報を正解として、各ワーカーノード 220 の NW 情報が正しいこと（つまり、改ざんされていないこと）を検証する。

[0040] マスターノード 210 のアテストーションレポート発行部 212 は、上記のステップ S 104 で発行したアテストーションレポートと、上記のステップ S 108 における真正性検証の結果とをユーザ装置 100 に送信する（ステップ S 109）。

[0041] 以上により、ユーザは、真正性検証の結果から各ワーカーノード 220 の真正性を確認することができる。また、アテストーションレポートに含まれる NW 管理情報を用いて、クラスタ全体の真正性を確認することができる。

[0042] ≪真正性検証処理（実施例 2）≫

実施例 2 における真正性検証処理の流れについて、図 6 を参照しながら説明する。

[0043] ユーザ装置 100 のアテストーションレポート発行依頼部 101 は、マスターノード 210 に対してアテストーションレポート発行依頼を送信する（ステップ S 201）。

[0044] マスターノード 210 のアテストーションレポート発行依頼部 213 は、

オーケストレーション機能部 211 によってアステーションレポート発行依頼を受信すると、各ワーカーノード 220 に対してアステーションレポート発行依頼をそれぞれ送信する（ステップ S202）。

[0045] マスターノード 210 のオーケストレーション機能部 211 は、自身のノード固有情報として全体ポリシーを取得する（ステップ S203）。全体ポリシーには、例えば、各ワーカーノード 220 が保管するデータとそのデータに対するアクセス制御に関する情報等が定義されている。なお、全体ポリシーは、例えば、ポリシー表現言語である ODR L（Open Digital Rights Language）等で定義された情報である。ただし、これは一例であって、全体ポリシーはどのような言語で定義されていてもよい。

[0046] マスターノード 210 のアステーションレポート発行部 212 は、上記のステップ S203 で取得された全体ポリシーが含まれるアステーションレポートを発行する（ステップ S204）。

[0047] 各ワーカーノード 220 のエージェント機能部 221 は、自身のノード固有情報として部分ポリシーを取得する（ステップ S205）。部分ポリシーには、例えば、当該ワーカーノード 220 が保管するデータとそのデータに対するアクセス制御に関する情報等が定義されている。なお、部分ポリシーは、全体ポリシーの一部の情報である。

[0048] 各ワーカーノード 220 のアステーションレポート発行部 222 は、上記のステップ S205 で取得された部分ポリシーが含まれるアステーションレポートを発行する（ステップ S206）。

[0049] 各ワーカーノード 220 のアステーションレポート発行部 222 は、上記のステップ S206 で発行されたアステーションレポートをマスターノード 210 に送信する（ステップ S207）。

[0050] マスターノード 210 のオーケストレーション機能部 211 は、上記のステップ S203 で取得された全体ポリシーと、各ワーカーノード 220 から受信したアステーションレポートに含まれる部分ポリシーとを用いて、各ワーカーノード 220 の真正性を検証する（ステップ S208）。すなわち

、オーケストレーション機能部 211 は、全体ポリシーを正解として、各ワーカーノード 220 の部分ポリシーが正しいこと（つまり、改ざんされていないこと）を検証する。

[0051] マスターノード 210 のアテステーションレポート発行部 212 は、上記のステップ S204 で発行したアテステーションレポートと、上記のステップ S208 における真正性検証の結果とをユーザ装置 100 に送信する（ステップ S209）。

[0052] 以上により、ユーザは、真正性検証の結果から各ワーカーノード 220 の真正性を確認することができる。また、アテステーションレポートに含まれる NW 管理情報を用いて、クラスタ全体の真正性を確認することができる。

[0053] <データ分配処理>

以下、秘匿実行サービスに利用するデータをユーザ装置 100 からマスターノード 210 に送信すると共に、更にそのデータを利用するワーカーノード 220 に対して当該データを送信（分配）するデータ分配処理の実施例 1～3 について説明する。

[0054] <<データ分配処理（実施例 1）>>

実施例 1 におけるデータ分配処理の流れについて、図 7 を参照しながら説明する。

[0055] ユーザ装置 100 のデータ提供部 103 は、マスターノード 210 のサンドボックス公開鍵を用いて、送信対象のデータを暗号化する（ステップ S301）。以下、本ステップで暗号化されたデータを暗号化データと呼ぶ。

[0056] ユーザ装置 100 のデータ提供部 103 は、上記のステップ S301 で暗号化された暗号化データをマスターノード 210 に送信する（ステップ S302）。

[0057] マスターノード 210 のオーケストレーション機能部 211 は、暗号化データを受信すると、自身のサンドボックス秘密鍵を用いて、当該暗号化データを復号する（ステップ S303）。

[0058] マスターノード 210 のオーケストレーション機能部 211 は、ワーカー

ノード２２０のサンドボックス公開鍵を用いて、上記のステップＳ３０３で復号されたデータを暗号化する（ステップＳ３０４）。以下、本ステップで暗号化されたデータを再暗号化データと呼ぶ。

[0059] マスターノード２１０のオーケストレーション機能部２１１は、上記のステップＳ３０４で暗号化された再暗号化データを当該ワーカーノード２２０に送信する（ステップＳ３０５）。

[0060] ワーカーノード２２０のエージェント機能部２２１は、再暗号化データを受信すると、自身のサンドボックス秘密鍵を用いて、当該再暗号化データを復号する（ステップＳ３０６）。これにより、ワーカーノード２２０は当該データを保管し、秘匿実行サービスで利用することができる。

[0061] ≪データ分配処理（実施例２）≫

実施例２におけるデータ分配処理の流れについて、図８を参照しながら説明する。

[0062] マスターノード２１０のオーケストレーション機能部２１１とワーカーノード２２０のエージェント機能部２２１は、セキュアチャネルを確立する（ステップＳ４０１）。セキュアチャネルとしては、例えば、ＴＬＳ（Transport Layer Security）、ＩＰｓｅｃ、ＶＸＬＡＮ（ＶＸＬＡＮ ｏｖｅｒ ＩＰｓｅｃ）等を確立すればよい。また、このとき、認証又は相互認証が必要な場合にはアテステーションレポートの真正性検証で代替してもよい。

[0063] 例えば、セキュアチャネルとしてＴＬＳを確立する場合、マスターノード２１０をサーバ、ワーカーノード２２０をクライアントとして、マスターノード２１０がワーカーノード２２０を認証する際には、図５のステップＳ１０７又は図６のステップＳ２０７のアテステーションレポートの真正性検証をクライアント認証とみなしてもよい。一方で、ワーカーノード２２０がマスターノード２１０を認証する際には、通常と同様に、サーバ証明書（又はそのハッシュ値）を用いる。この場合、マスターノード２１０から当該ワーカーノード２２０に対して、サーバ証明書（又はそのハッシュ値）が含まれるアテステーションレポートを送信すればよい。サーバ証明書（又はそのハ

ッシュ値)をアテステーションレポートに含めることにより、ワーカーノード220は、正当なマスターノード210からのサーバ証明書であることを検証することが可能となる。

[0064] ユーザ装置100のデータ提供部103は、マスターノード210のサンドボックス公開鍵を用いて、送信対象のデータを暗号化する(ステップS402)。以下、本ステップで暗号化されたデータを暗号化データと呼ぶ。

[0065] ユーザ装置100のデータ提供部103は、上記のステップS402で暗号化された暗号化データをマスターノード210に送信する(ステップS403)。

[0066] マスターノード210のオーケストレーション機能部211は、暗号化データを受信すると、自身のサンドボックス秘密鍵を用いて、当該暗号化データを復号する(ステップS404)。

[0067] マスターノード210のオーケストレーション機能部211は、上記のステップS401で確立したセキュアチャネルを用いて、上記のステップS404で復号されたデータを当該ワーカーノード220に送信する(ステップS405)。これにより、ワーカーノード220は当該データを保管し、秘匿実行サービスで利用することができる。

[0068] なお、実施例2におけるデータ分配処理では、セキュアチャネルを利用してマスターノード210からワーカーノード220に対してデータを送信するため、マスターノード210はワーカーノード220のサンドボックス公開鍵を保持する必要がない。このため、例えば、実施例1におけるデータ分配処理と比較して、ワーカーノード220の起動と削除が頻繁に行われる場合等に鍵管理の煩雑さを削減することが可能となる。

[0069] ≪データ分配処理(実施例3)≫

実施例3におけるデータ分配処理の流れについて、図9を参照しながら説明する。

[0070] マスターノード210のオーケストレーション機能部211とワーカーノード220のエージェント機能部221は、図8のステップS401と同様

に、セキュアチャネルを確立する（ステップS501）。

[0071] マスターノード210のオーケストレーション機能部211は、上記のステップS501で確立したセキュアチャネルを用いて、自身のサンドボックス秘密鍵をワーカーノード220に送信する（ステップS502）。

[0072] ユーザ装置100のデータ提供部103は、マスターノード210のサンドボックス公開鍵を用いて、送信対象のデータを暗号化する（ステップS503）。以下、本ステップで暗号化されたデータを暗号化データと呼ぶ。

[0073] ユーザ装置100のデータ提供部103は、上記のステップS503で暗号化された暗号化データをマスターノード210に送信する（ステップS504）。

[0074] マスターノード210のオーケストレーション機能部211は、暗号化データを受信すると、当該暗号化データを当該ワーカーノード220に送信する（ステップS505）。

[0075] ワーカーノード220のエージェント機能部221は、暗号化データを受信すると、マスターノード210のサンドボックス秘密鍵を用いて、当該暗号化データを復号する（ステップS506）。これにより、ワーカーノード220は当該データを保管し、秘匿実行サービスで利用することができる。

[0076] なお、実施例3におけるデータ分配処理では、セキュアチャネルを利用してマスターノード210からワーカーノード220に対して、マスターノード210のサンドボックス秘密鍵を送信するため、マスターノード210はワーカーノード220のサンドボックス公開鍵を保持する必要がない。このため、例えば、実施例1におけるデータ分配処理と比較して、ワーカーノード220の起動と削除が頻繁に行われる場合等に鍵管理の煩雑さを削減することが可能となる。

[0077] ＜ハードウェア構成例＞

上記のユーザ装置100やプラットフォーム200を実現する物理マシンは、例えば、図10に示すコンピュータ500のハードウェア構成により実現可能である。図10に示すコンピュータ500は、入力装置501と、表

示装置５０２と、外部Ｉ／Ｆ５０３と、通信Ｉ／Ｆ５０４と、ＲＡＭ（Random Access Memory）５０５と、ＲＯＭ（Read Only Memory）５０６と、補助記憶装置５０７と、プロセッサ５０８とを有する。これらの各ハードウェアは、それぞれがバス５０９を介して通信可能に接続される。

[0078] 入力装置５０１は、例えば、キーボード、マウス、タッチパネル、物理ボタン等である。表示装置５０２は、例えば、ディスプレイ、表示パネル等である。なお、コンピュータ５００は、例えば、入力装置５０１及び表示装置５０２のうちの少なくとも一方を有していなくてもよい。

[0079] 外部Ｉ／Ｆ５０３は、記録媒体５０３ａ等の外部装置とのインタフェースである。記録媒体５０３ａとしては、例えば、ＣＤ（Compact Disc）、ＤＶＤ（Digital Versatile Disk）、ＳＤメモリカード（Secure Digital memory card）、ＵＳＢ（Universal Serial Bus）メモリカード等が挙げられる。

[0080] 通信Ｉ／Ｆ５０４は、コンピュータ５００を通信ネットワークに接続するためのインタフェースである。ＲＡＭ５０５は、プログラムやデータを一時保持する揮発性の半導体メモリ（記憶装置）である。ＲＯＭ５０６は、電源を切ってもプログラムやデータを保持することができる不揮発性の半導体メモリ（記憶装置）である。補助記憶装置５０７は、例えば、ＨＤＤ（Hard Disk Drive）、ＳＳＤ（Solid State Drive）、フラッシュメモリ等のストレージ装置（記憶装置）である。プロセッサ５０８は、例えば、ＣＰＵ等の各種演算装置である。

[0081] なお、図１０に示すコンピュータ５００のハードウェア構成は一例であって、これに限られるものではない。例えば、コンピュータ５００は、複数の補助記憶装置５０７や複数のプロセッサ５０８を有していてもよいし、図示したハードウェアの一部を有していなくてもよいし、図示したハードウェア以外の種々のハードウェアを有していてもよい。

[0082] <変形例>

以下、上記の実施形態の変形例について説明する。

[0083] ・変形例１

実施例 1 における真正性検証処理と実施例 2 における真正性検証処理とを組み合わせ、ネットワークに関する情報（NW管理情報及びNW情報）とポリシー（全体ポリシー及び部分ポリシー）の両方により複数のノードで構成されるクラスタの真正性が検証されてもよい。

[0084] ・変形例 2

実施例 1 における真正性検証処理ではマスターノード 210 のユーザ固有情報として NW 管理情報、ワーカーノード 220 のユーザ固有情報として NW 情報をそれぞれ用いたが、これ以外にも、プラットフォーム 200 上の OS やプラットフォーム 200 を実現する情報処理装置（例えば、PC、サーバ等の物理マシン）等が持つ様々な固有情報が用いられてもよい。例えば、ユーザ固有情報としてスナップショット等が用いられてもよい。ユーザ固有情報としてスナップショットが用いられる場合、例えば、マスターノード 210 が持つスナップショットを正解として、各ワーカーノード 220 が持つスナップショットにより真正性が検証される。ここで、スナップショットとしては、例えば、CPU のスナップショットやストレージのスナップショット等を用いることが考えられる。なお、上記の変形例 1 で説明したように、更にポリシーも用いて真正性が検証されてもよい。

[0085] なお、CPU のスナップショットの具体例としては、CPU のレジスタ情報等のスナップショットが挙げられる。また、ストレージのスナップショットの具体例としては、ネットワークカードやストレージのデバイス情報のスナップショット、ネットワーク接続しているストレージのネットワーク情報（iSCSI、FiberChannel、NAS 等）のスナップショット等が挙げられる。更に、OS や情報処理装置が持つ固有情報の具体例としては、OS のビルド番号、情報処理装置のシリアル番号、ファームウェア（例えば、OVMF 等）のバイナリや初期 RAM ディスク（例えば、initrd や initramfs）のハッシュ値等が挙げられる。

[0086] ・変形例 3

実施例 2 における真正性検証処理において、マスターノード 210 が各ワ

ーカーノード２２０の部分ポリシーを検証し、それにより真正性が検証された場合、マスターノード２１０は、その部分ポリシーに対して、当該部分ポリシーを持つワーカーノード２２０のサンドボックス公開鍵を対応付けて保持してもよい。同様に、ユーザが全体ポリシーを検証し、それにより真正性が検証された場合、ユーザ装置１００は、全体ポリシーに対して、マスターノード２１０のサンドボックス公開鍵を対応付けて保持してもよい。これにより、マスターノード２１０は真正性が確認された各ワーカーノード２２０の部分ポリシーとそのサンドボックス公開鍵とを対応付けて保持することができる。同様に、ユーザ装置１００は、真正性が確認されたクラスタに含まれるマスターノード２１０の全体ポリシーとそのサンドボックス公開鍵とを対応付けて保持することができる。このため、データ分配処理で真正性が確認されたノードのサンドボックス公開鍵を利用することが可能となる。

[0087] ・変形例４

上記の実施形態では、マスターノードとワーカーノードとを区別したが、マスターとワーカーの区別がなくてもよい。この場合、ユーザ装置１００は各ノードに対してアステーションレポート発行依頼をそれぞれ送信し、各ノードは自身のノード固有情報が含まれるアステーションレポートを当該ユーザ装置１００に送信する。これにより、ユーザは、各ノードからのアステーションレポートに含まれるノード固有情報からそのノードの真正性を検証することができる。

[0088] ・変形例５

ワーカーノード２２０間で通信可能な場合には、ワーカーノード２２０間で真正性の検証が行われてもよい。例えば、或るワーカーノード２２０から別のワーカーノード２２０に対してアステーションレポート発行依頼を送信し、当該別のワーカーノード２２０が自身のノード固有情報が含まれるアステーションレポートを当該或るワーカーノード２２０に送信してもよい。これにより、当該或るワーカーノード２２０は、当該別のワーカーノード２２０の真正性を検証することができる。

[0089] ここで、各ワーカーノード２２０は、自身がアテストレーションレポート発行依頼を送信する他のワーカーノード２２０の部分ポリシー及び公開鍵をマスターノード２１０からアテストレーションレポートにより取得すればよい。このとき、各ワーカーノード２２０は、例えば、当該他のワーカーノード２２０を一意に識別する名称等を用いて、当該他のワーカーノード２２０の部分ポリシー及び公開鍵をマスターノード２１０に要求すればよい。

[0090] なお、各ワーカーノード２２０は、自身がアテストレーションレポート発行依頼を送信する他のワーカーノード２２０の部分ポリシー及び公開鍵をマスターノード２１０から都度取得してもよいし、その部分ポリシー及び公開鍵が事前にマスターノード２１０から配布されてもよい。

[0091] ・変形例６

上記の実施形態のデータ分配処理（実施例１～３）では、ユーザ装置１００のデータ提供部１０３がマスターノード２１０にデータ（暗号化データ）を送信する場合について説明したが、データ提供部１０３は、例えば、ワーカーノード２２０に対して、そのワーカーノード２２０の公開鍵で暗号化した暗号化データを送信してもよい。

[0092] また、ユーザ装置１００のデータ提供部１０３から暗号化データを送信する場合だけでなく、各ノードがデータ提供部１０３からデータ（暗号化データ）を取得するものであってもよい。

[0093] ・変形例７

上記の実施形態では、各ワーカーノード２２０は自身に保管されるデータのアクセス制御等のための部分ポリシーを所持しているものとしたが、これに限られず、例えば、各ワーカーノード２２０が全体ポリシーとすべてのワーカーノード２２０の鍵ペアとを所持していてもよい。なお、この場合、全体ポリシーとすべてのワーカーノード２２０の鍵ペアは、マスターノード２１０から各ワーカーノード２２０に配布される。

[0094] ＜まとめ＞

以上のように、本実施形態に係るユーザ装置１００と隔離実行環境をそれ

ぞれ備える複数のノードで構成されるクラスタを実現するプラットフォーム 200で構成されるシステムによれば、ユーザは、当該クラスタの真正性（つまり、当該クラスタの設定情報等が改ざんされていないこと）を検証することができる。このため、当該クラスタによって提供される秘匿実行サービスを利用する際に、ユーザは、その安全性を確認した上で利用することが可能となる。

[0095] 本発明は、具体的に開示された上記の実施形態に限定されるものではなく、請求の範囲の記載から逸脱することなく、種々の変形や変更、既知の技術との組み合わせ等が可能である。

符号の説明

[0096]	100	ユーザ装置
	101	アステーションレポート発行依頼部
	102	アステーションレポート受信部
	103	データ提供部
	200	プラットフォーム
	210	マスターノード
	211	オーケストレーション機能部
	212	アステーションレポート発行部
	213	アステーションレポート発行依頼部
	220	ワーカーノード
	221	エージェント機能部
	222	アステーションレポート発行部
	300	通信ネットワーク
	500	コンピュータ
	501	入力装置
	502	表示装置
	503	外部 I/F
	503a	記録媒体

5 0 4	通信 I ／ F
5 0 5	R A M
5 0 6	R O M
5 0 7	補助記憶装置
5 0 8	プロセッサ
5 0 9	バス

請求の範囲

- [請求項1] 隔離実行環境をそれぞれ備える複数のノードで構成されるクラスタを実現するプラットフォームと、前記クラスタによって提供されるサービスを利用するユーザ装置とが含まれ、前記クラスタの真正性を検証する真正性検証システムであって、
- 前記ユーザ装置は、
- 前記ノードに対してアステーションレポートの発行依頼を送信する第1の送信部、を有し、
- 前記ノードは、
- 前記発行依頼を受信すると、前記ノードの固有情報が含まれるアステーションレポートを発行する発行部、を有する、
- 真正性検証システム。
- [請求項2] 前記複数のノードは、1つのマスターノードと、前記マスターノード以外の1以上のワーカーノードとで構成されており、
- 前記第1の送信部は、
- 前記マスターノードに対してアステーションレポートの発行依頼を送信し、
- 前記マスターノードは、
- 前記発行依頼を受信すると、前記ワーカーノードに対してアステーションレポートの発行依頼を送信する第2の送信部と、
- 前記マスターノードの固有情報を用いて、前記ワーカーノードから受信したアステーションレポートに含まれる前記固有情報の真正性を検証する検証部と、
- 前記マスターノードの固有情報が含まれるアステーションレポートと、前記真正性の検証結果とを前記ユーザ装置に送信する第3の送信部と、を有する、請求項1に記載の真正性検証システム。
- [請求項3] 前記検証部は、
- 前記マスターノードの固有情報を正解として、前記ワーカーノード

から受信したアテストレーションレポートに含まれる前記固有情報の改ざん有無を検証する、請求項2に記載の真正性検証システム。

[請求項4] 前記固有情報は、ネットワークに関する情報、前記ノードが保持するデータのアクセス制御に関するポリシー、前記プラットフォーム上のOSの固有情報、前記プラットフォームを実現する情報処理装置の固有情報、の少なくとも1つである、請求項1乃至3の何れか一項に記載の真正性検証システム。

[請求項5] 前記ユーザ装置は、
前記ノードの公開鍵により暗号化した暗号化データを前記ノードに送信するデータ提供部、を有し、
前記ノードは、
他のノードから受信したアテストレーションレポートを前記他のノードの認証とみなして事前に確立したセキュアチャネルを介して、前記暗号化データを自身の秘密鍵で復号したデータを前記他のノードに送信する第4の送信部、を有する、請求項1に記載の真正性検証システム。

[請求項6] 前記ユーザ装置は、
前記ノードの公開鍵により暗号化した暗号化データを前記ノードに送信するデータ提供部、を有し、
前記ノードは、
他のノードから受信したアテストレーションレポートを前記他のノードの認証とみなして事前に確立したセキュアチャネルを介して、前記暗号化データを復号するための自身の秘密鍵を前記他のノードに送信する第5の送信部と、
前記暗号化データを前記他のノードに送信する第6の送信部と、を有する、請求項1に記載の真正性検証システム。

[請求項7] 隔離実行環境をそれぞれ備える複数のノードで構成されるクラスタを実現するプラットフォームと、前記クラスタによって提供されるサ

ービスを利用するユーザ装置とが含まれ、前記クラスタの真正性を検証する真正性検証システムにおける真正性検証方法であって、

前記ユーザ装置が、

前記ノードに対してアステーションレポートの発行依頼を送信する第1の送信手順、を実行し、

前記ノードが、

前記発行依頼を受信すると、前記ノードの固有情報が含まれるアステーションレポートを発行する発行手順、を実行する、

真正性検証方法。

[請求項8]

隔離実行環境をそれぞれ備える複数のノードで構成されるクラスタを実現するプラットフォームと、前記クラスタによって提供されるサービスを利用するユーザ装置とが含まれ、前記クラスタの真正性を検証する真正性検証システムを実現するプログラムであって、

前記ユーザ装置に、

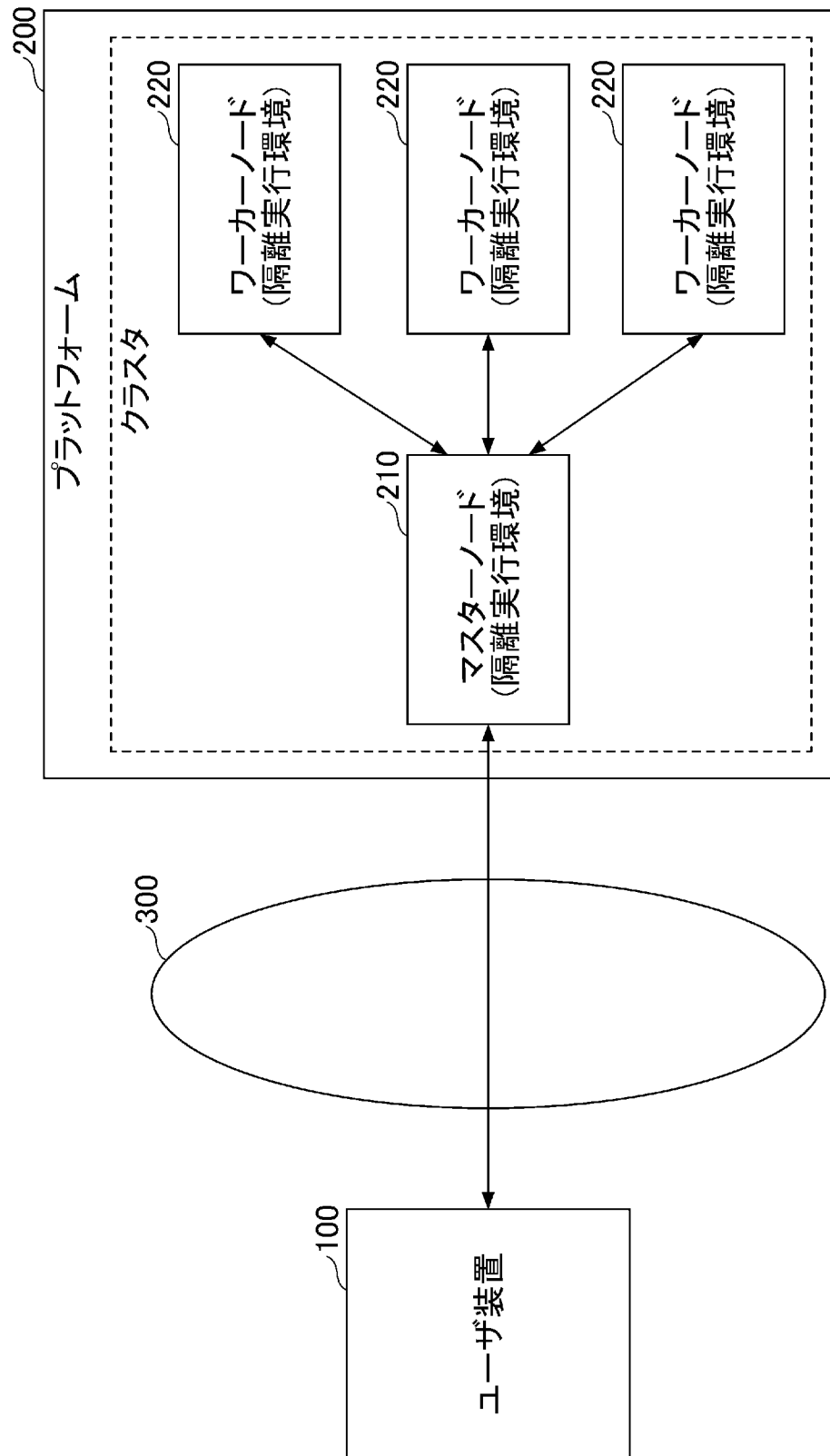
前記ノードに対してアステーションレポートの発行依頼を送信する第1の送信手順、を実行させ、

前記ノードに、

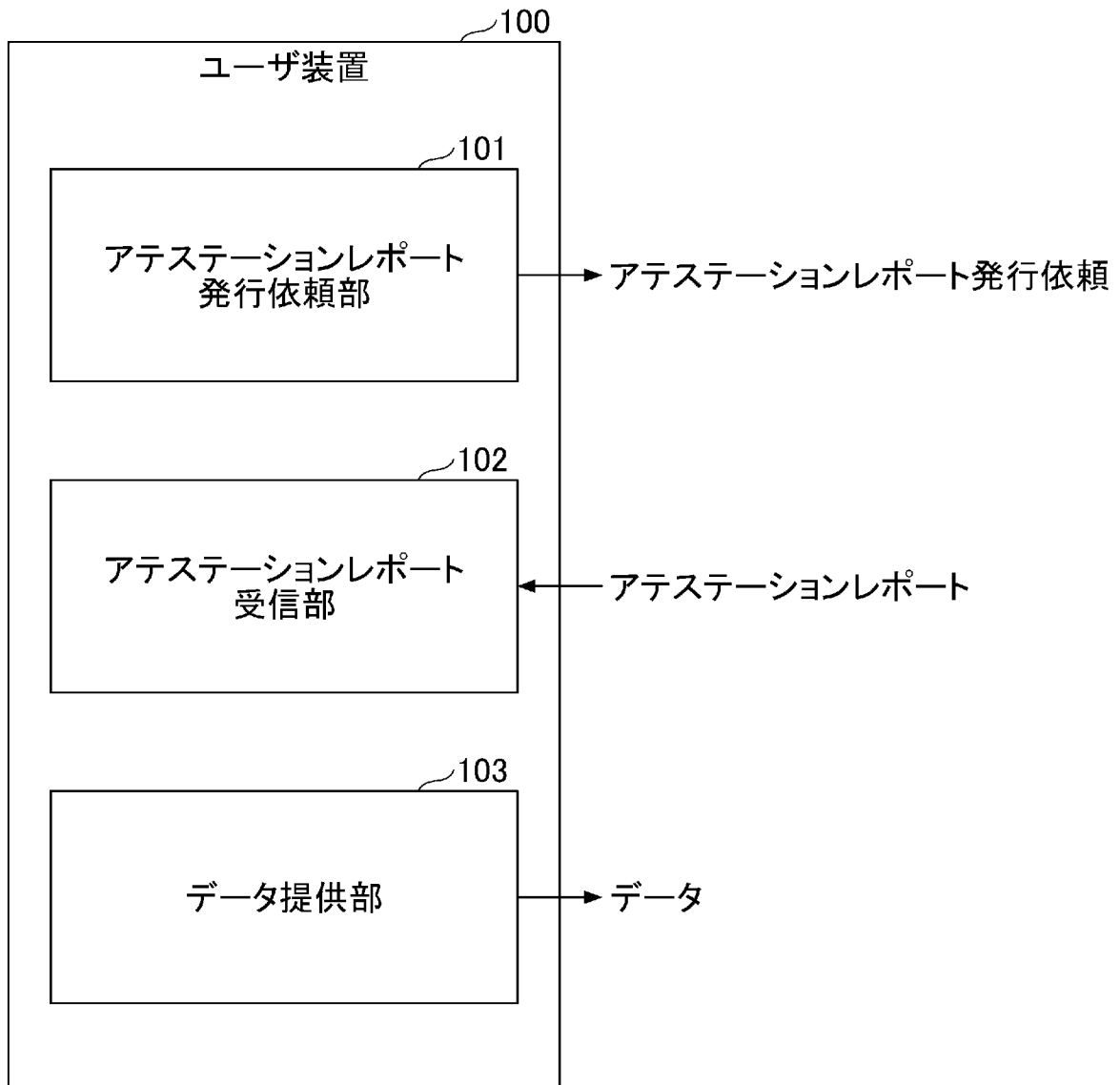
前記発行依頼を受信すると、前記ノードの固有情報が含まれるアステーションレポートを発行する発行手順、を実行させる、

プログラム。

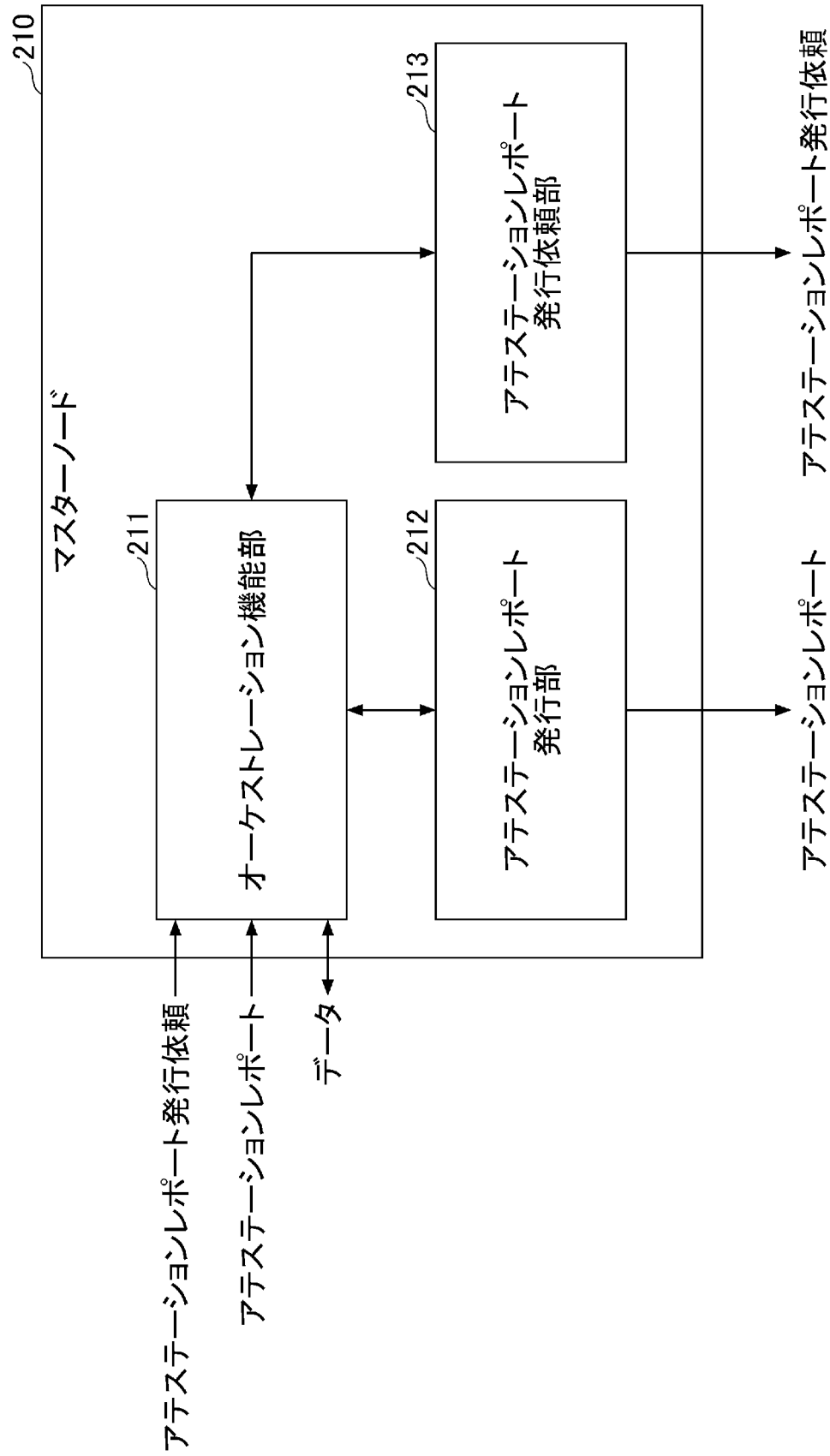
[図1]



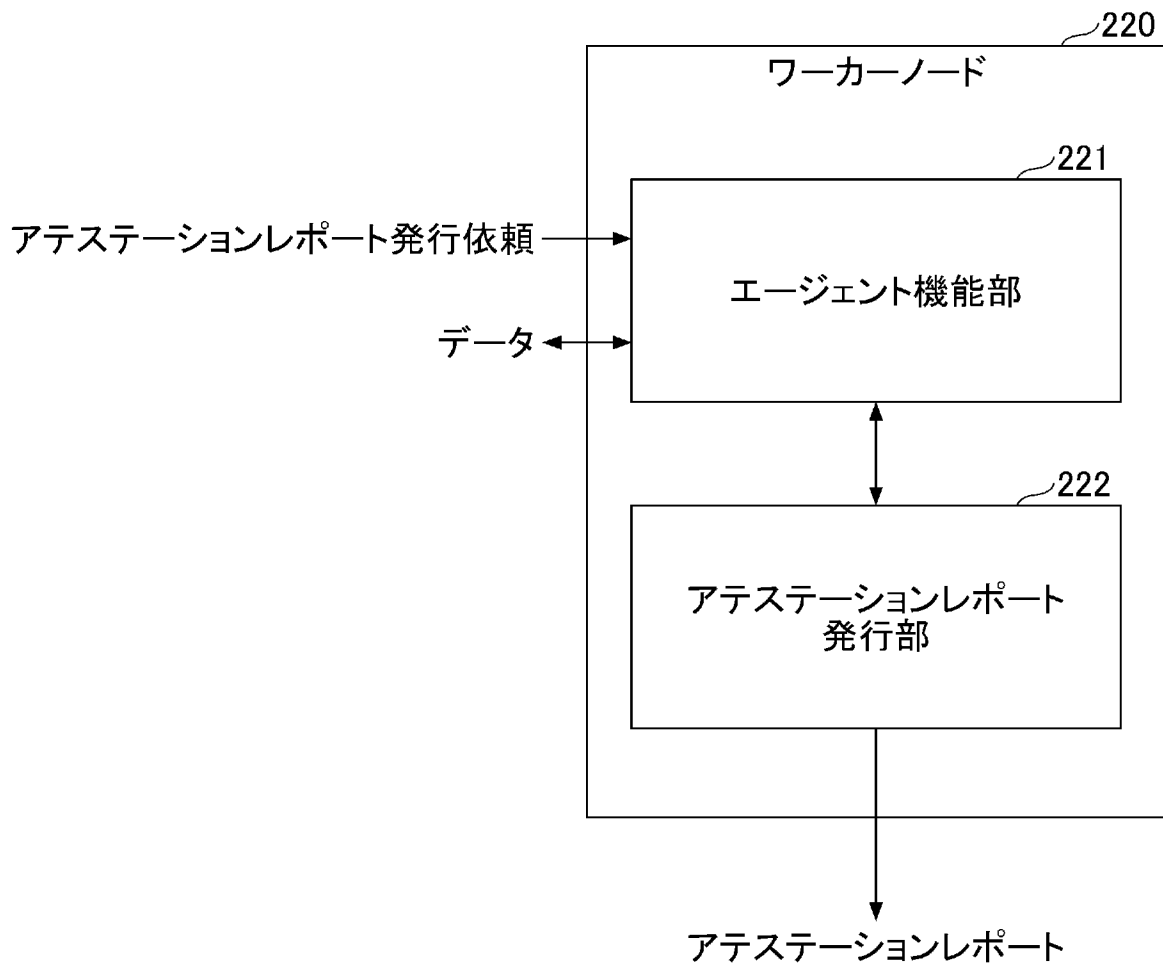
[図2]



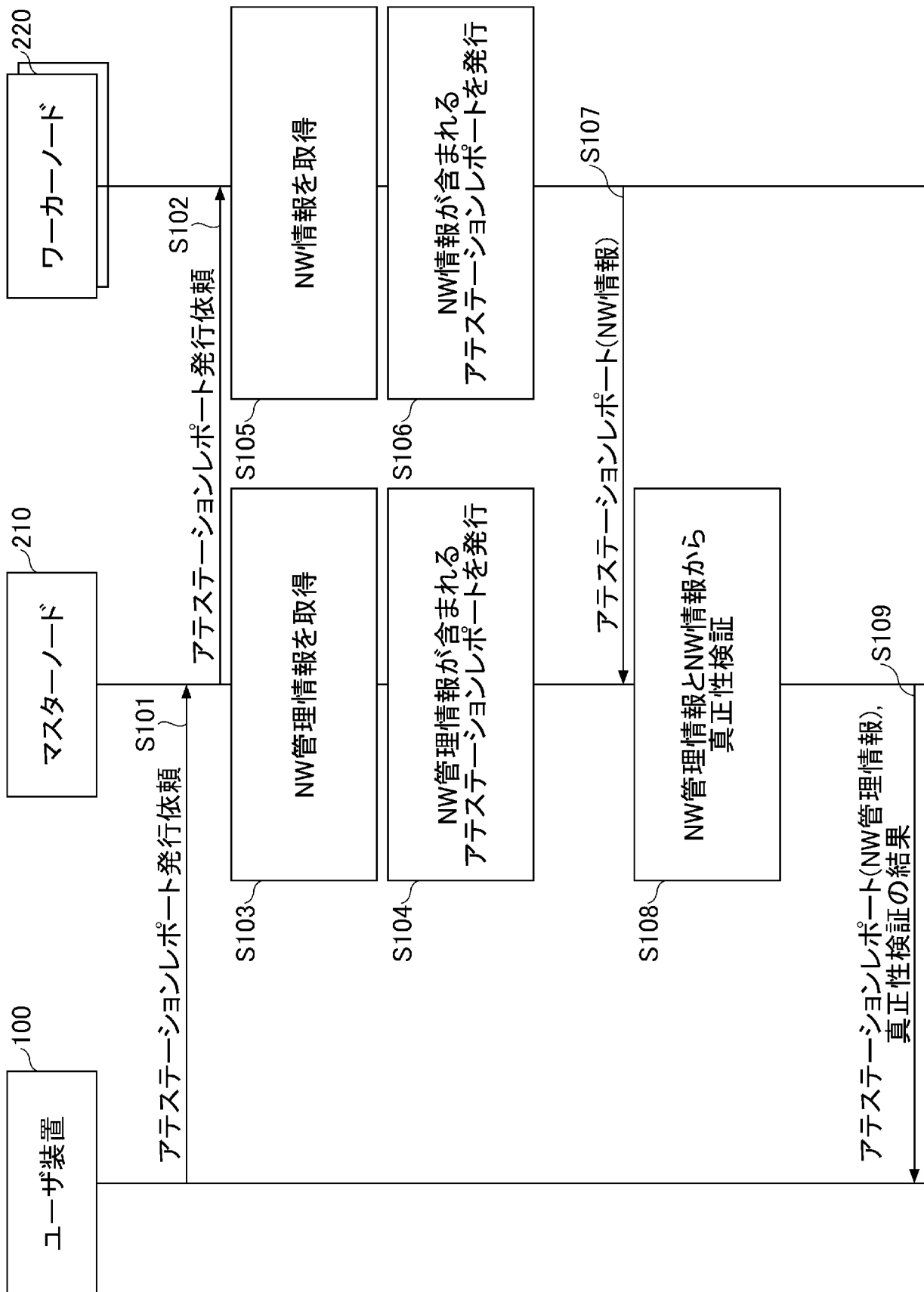
[図3]



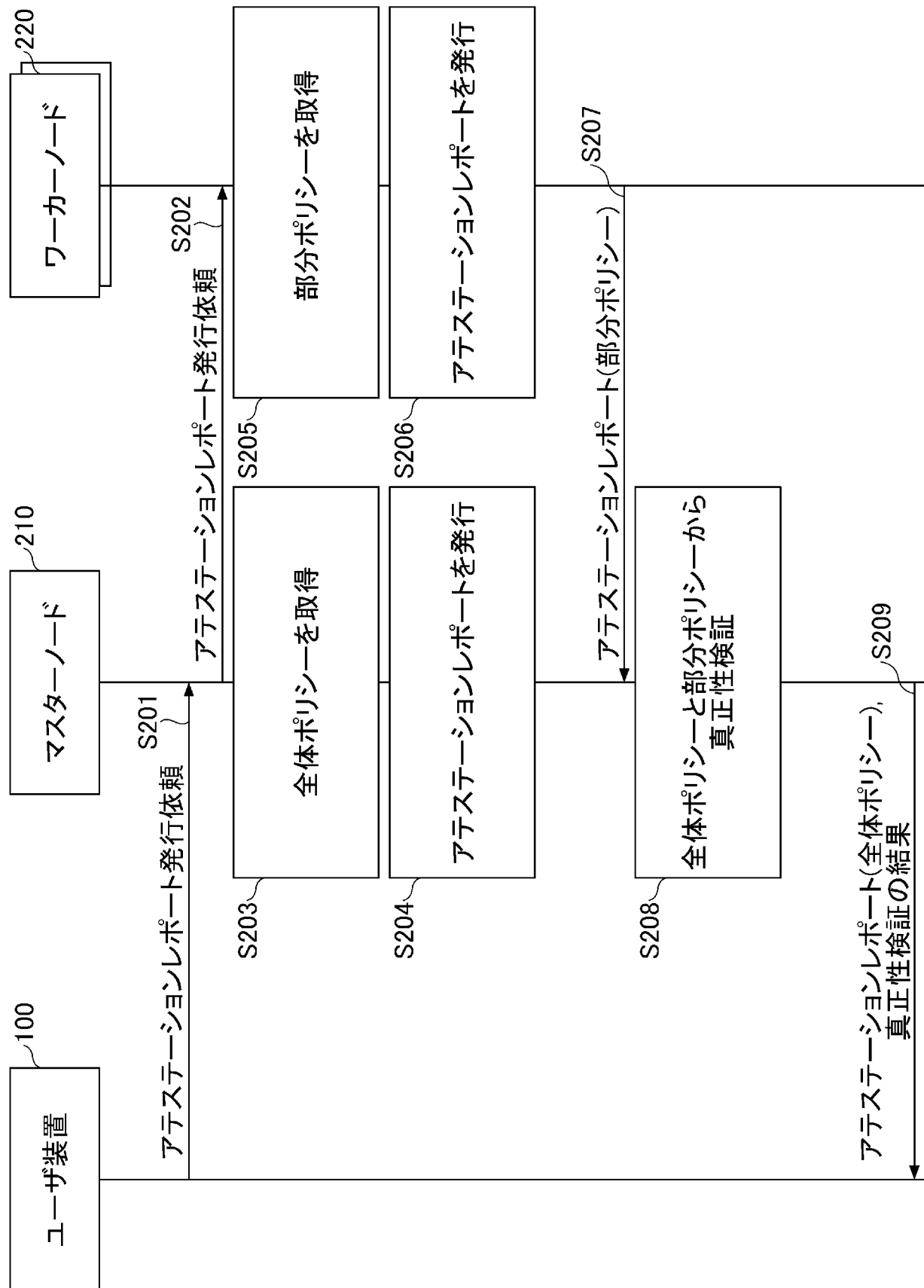
[図4]



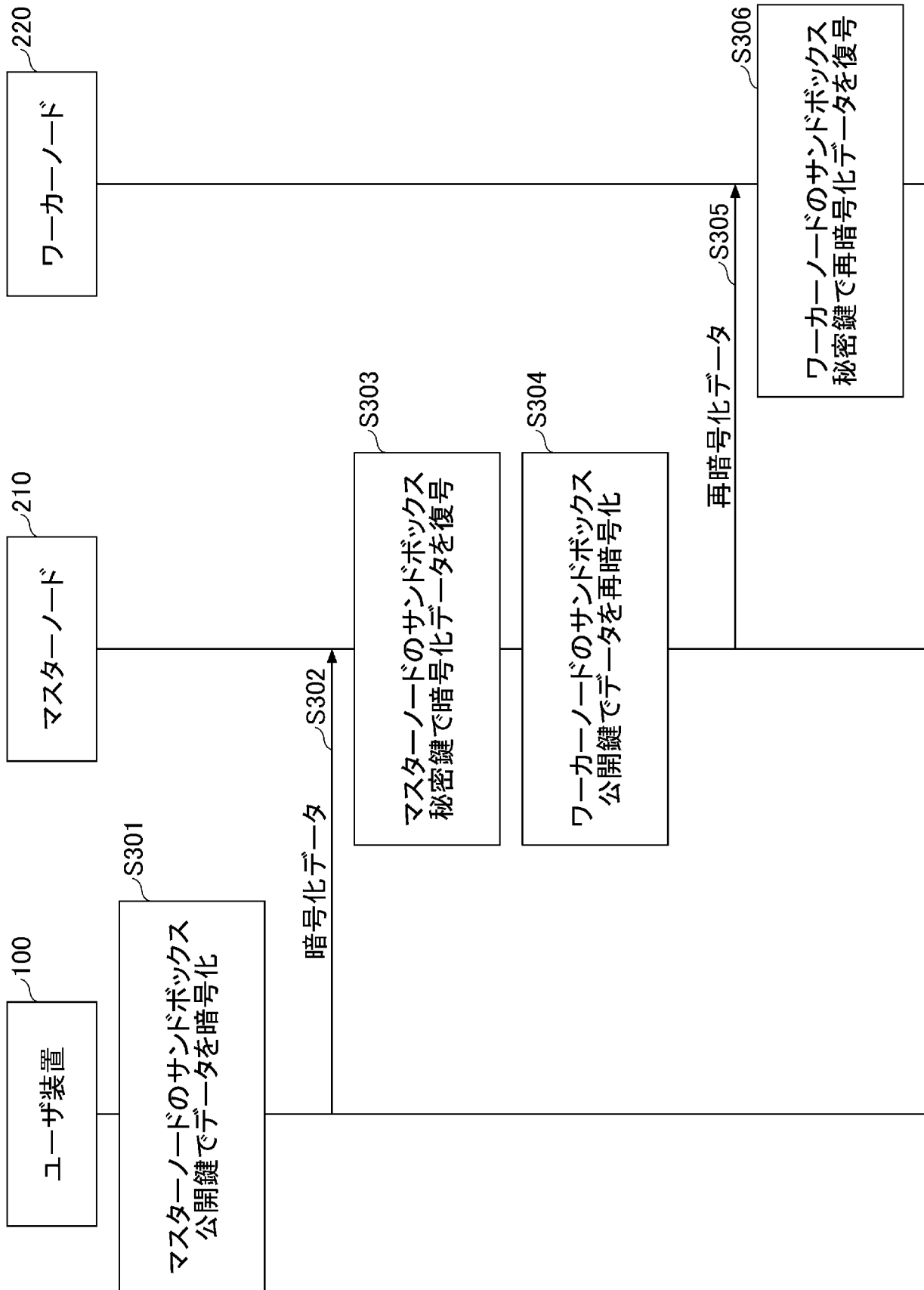
[図5]



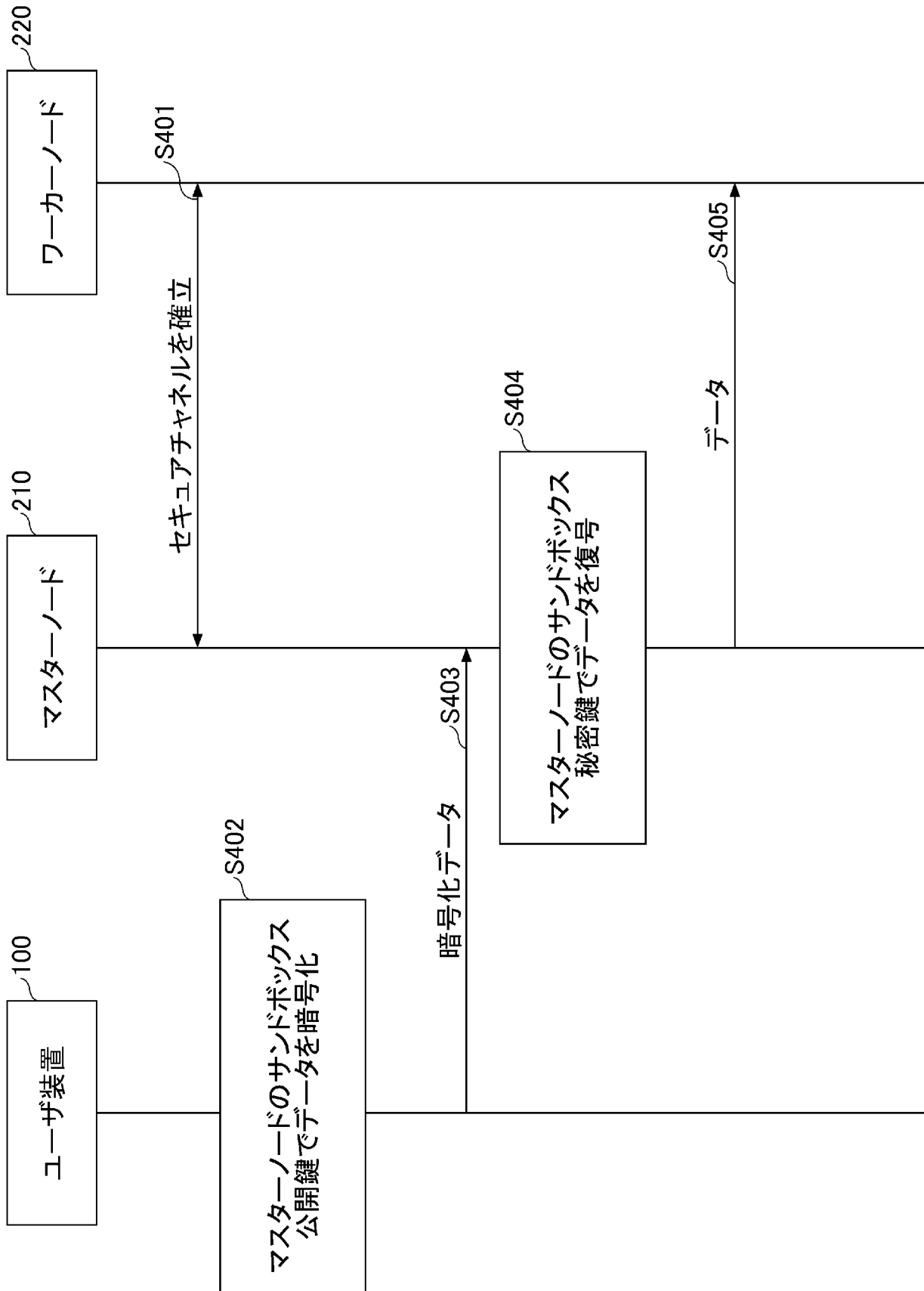
[図6]



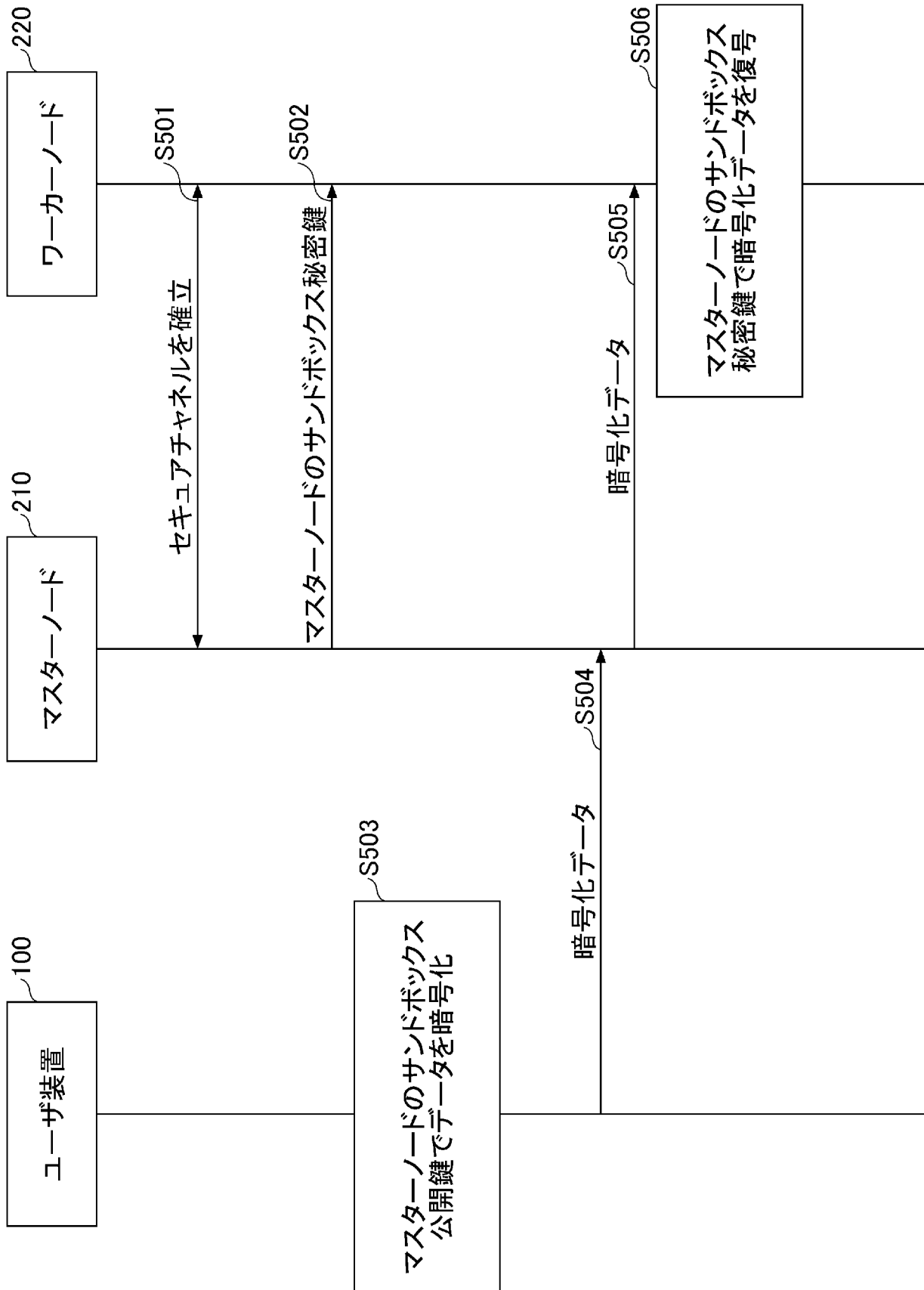
[図7]



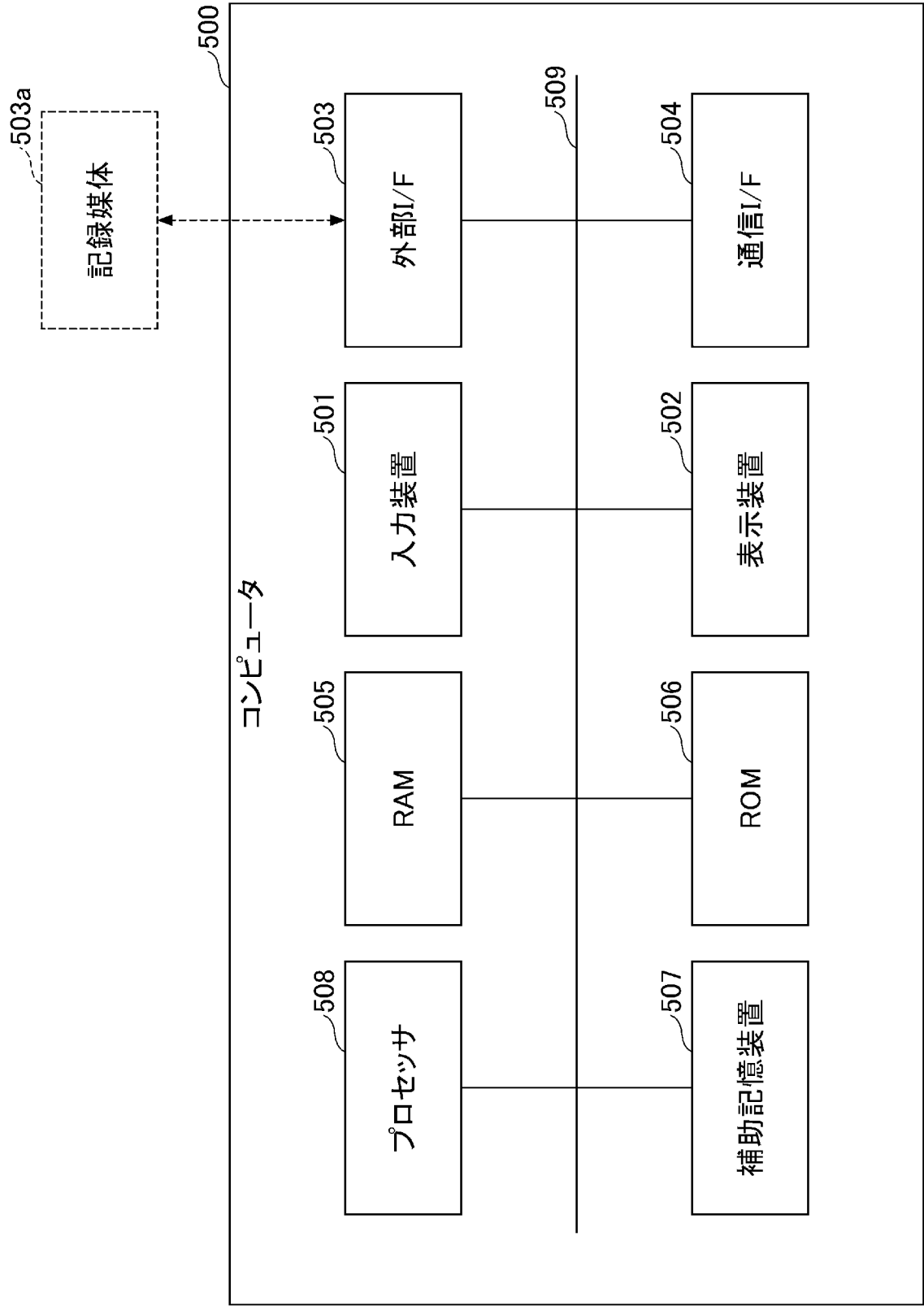
[図8]



[図9]



[図10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2023/021612

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/57**(2013.01)i; **G06F 21/64**(2013.01)i; **H04L 9/32**(2006.01)i

FI: G06F21/57; G06F21/64; H04L9/32 100B

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)

G06F21/57; G06F21/64; H04L9/32

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 1971-2023
 Registered utility model specifications of Japan 1996-2023
 Published registered utility model applications of Japan 1994-2023

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.
Y	奥田 哲矢 ほか, Confidential Program Executionの提案と安全性評価, 研究報告コンピュータセキュリティ (CSEC), 1 November 2021, vol. 2021-CSEC-95, no. 17, pp. 1-8, ISSN 2188-8655 (OKUDA, Tetsuya et al., Proposition and Security Evaluation of Confidential Program Execution), non-official translation (Technical Report, Computer Security (CSEC)) in particular, section 2.4	1, 4, 5-8
A	in particular, section 2.4	2-3
Y	JP 2022-537739 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 29 August 2022 (2022-08-29) paragraphs [0017]-[0082], fig. 1, 7	1, 4, 5-8
A	paragraphs [0017]-[0082], fig. 1, 7	2-3

☒ 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

10 August 2023

Date of mailing of the international search report

22 August 2023

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

International application No.

PCT/JP2023/021612

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	内匠 真也 ほか, ファームウェア更新に対する I E T F R A T S 準拠リモートアテステーションの設計, 2 0 2 2 年 暗号と情報セキュリティシンポジウム予稿集, 18 January 2022, pp. 1-7 (TAKUMI, Shinya et al., A Design for Remote Attestation based on IETF RATS to protect firmware update, SCIS 2022)	1, 4, 5-8
A	in particular, section 2.1, table 1	2-3
Y	須藤 欧佑 ほか, A n o n i f y : プライバシーを保護した検証可能な状態遷移モジュール, 2 0 2 1 年 暗号と情報セキュリティシンポジウム予稿集, 19 January 2021, pp. 1-8 (SUDO, Osuke et al., Anonify: A Module for Privacy-preserving State Transitions with Verifiability, SCIS 2021)	5-6
A	in particular, section 3	2-3
A	US 2023/0068880 A1 (EMC IP HOLDING CO. LLC.) 02 March 2023 (2023-03-02) paragraphs [0066]-[0073], fig. 8	1-8

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2023/021612

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2022-537739	A	29 August 2022	US 2020/0403784 A1 paragraphs [0016]-[0081], fig. 1, 7 WO 2020/260026 A1 EP 3987712 A1 CN 113826352 A KR 10-2022-0002616 A	
US	2023/0068880	A1	02 March 2023	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/57(2013.01)i; G06F 21/64(2013.01)i; H04L 9/32(2006.01)i FI: G06F21/57; G06F21/64; H04L9/32 100B										
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）） G06F21/57; G06F21/64; H04L9/32										
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>1971-2023年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2023年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2023年</td> </tr> </table>			日本国実用新案公報	1922-1996年	日本国公開実用新案公報	1971-2023年	日本国実用新案登録公報	1996-2023年	日本国登録実用新案公報	1994-2023年
日本国実用新案公報	1922-1996年									
日本国公開実用新案公報	1971-2023年									
日本国実用新案登録公報	1996-2023年									
日本国登録実用新案公報	1994-2023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								
Y	奥田 哲矢 ほか, Confidential Program Executionの 提案と安全性評価, 研究報告コンピュータセキュリティ (CSEC), 2021.11.01, vol. 2021-CSEC-95, no. 17, pp.1-8, ISSN 2188-8655	1, 4, 5-8								
A	特に, 2.4節	2-3								
Y	JP 2022-537739 A (インターナショナル・ビジネス・マシーンズ・コーポレーショ ン) 29.08.2022 (2022-08-29)	1, 4, 5-8								
A	段落0017-0082, 図1, 7	2-3								
Y	内匠 真也 ほか, ファームウェア更新に対する I E T F R A T S 準拠リモートア テステーションの設計, 2022年 暗号と情報セキュリティシンポジウム予稿集, 2022.01.18, pp.1-7	1, 4, 5-8								
A	特に, 2.1節、表1	2-3								
	特に, 2.1節、表1									
☒ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。										
* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技術水準を示すもの “E” 国際出願日前の出願または特許であるが、国際出願日以後に 公表されたもの “L” 優先権主張に疑義を提起する文献又は他の文献の発行日若し くは他の特別な理由を確立するために引用する文献（理由を 付す） “O” 口頭による開示、使用、展示等に言及する文献 “P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の 後に公表された文献 “T” 国際出願日又は優先日後に公表された文献であって出願と抵 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 10.08.2023	国際調査報告の発送日 22.08.2023									
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） 行田 悦資 5S 6304 電話番号 03-3581-1101 内線 3546									

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	須藤 欧佑 ほか, Anonify: プライバシーを保護した検証可能な状態遷移モジュール, 2021年 暗号と情報セキュリティシンポジウム予稿集, 2021.01.19, pp.1-8	5-6
A	特に、3節	2-3
A	US 2023/0068880 A1 (EMC IP HOLDING COMPANY LLC) 02.03.2023 (2023 - 03 - 02) 段落0066-0073, 図8	1-8

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/JP2023/021612

引用文献			公表日	パテントファミリー文献	公表日
JP	2022-537739	A	29.08.2022	US 2020/0403784 A1 段落0016-0081, 図1, 7 WO 2020/260026 A1 EP 3987712 A1 CN 113826352 A KR 10-2022-0002616 A	
US	2023/0068880	A1	02.03.2023	(ファミリーなし)	