(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2021-52362
(P2021-52362A)
(43)公開日　令和3年4月1日(2021.4.1)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/22	(2006.01)	H04L	12/22		5K030
H04L 12/70	(2013.01)	H04L	12/70	Z	

審査請求 未請求　請求項の数 11　ＯＬ　（全 33 頁）

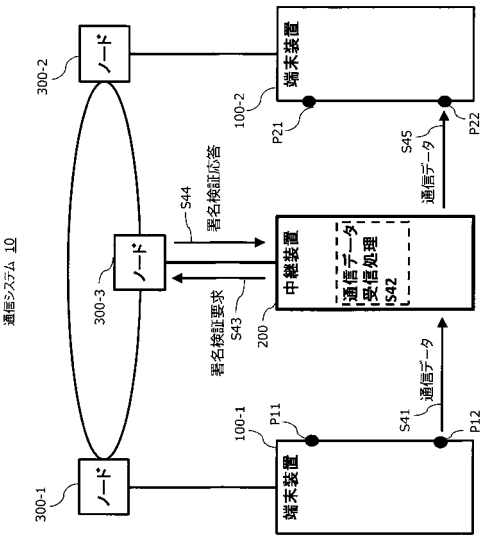
(21)出願番号　特願2019-175822 (P2019-175822)
(22)出願日　令和1年9月26日 (2019.9.26)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100094525
弁理士　土井　健二
(74)代理人　100094514
弁理士　林　恒徳
(72)発明者　鈴木　大
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5K030 GA15　JA11　JL06　KA05

(54)【発明の名称】通信中継プログラム、中継装置、及び通信中継方法

(57)【要約】
【課題】分散台帳機能を有する通信の安全性を向上させること
【解決手段】通信装置の識別子と、前記通信装置が通信に使用する公開鍵を分散台帳に記憶し、前記分散台帳を共有する分散台帳機能を有する複数のノードと、前記ノードのいずれかに接続する前記通信装置と、前記ノードのいずれかに接続する中継装置とを有する通信システムにおける前記中継装置のコンピュータに実行させる通信中継プログラムであって、前記通信装置とメッセージを送受信する送受信処理と、前記ノードから前記メッセージの送信元の通信装置の公開鍵を取得し、前記取得した公開鍵で前記メッセージに含まれる署名を認証する認証処理と、第１通信装置が第２通信装置に送信する通信データを含む通信メッセージを受信したとき、前記通信メッセージに対して前記認証処理を実行し、前記認証が成功した場合、前記通信メッセージを前記第２通信装置に送信する中継処理と、を実行させる。
【選択図】図１８



【特許請求の範囲】
【請求項１】
通信装置の識別子と、前記通信装置が通信に使用する公開鍵を分散台帳に記憶し、前記分散台帳を共有する分散台帳機能を有する複数のノードと、前記ノードのいずれかに接続する前記通信装置と、前記ノードのいずれかに接続する中継装置とを有する通信システムにおける前記中継装置のコンピュータに実行させる通信中継プログラムであって、
前記通信装置とメッセージを送受信する送受信処理と、
前記ノードから前記メッセージの送信元の通信装置の公開鍵を取得し、前記取得した公開鍵で前記メッセージに含まれる署名を認証する認証処理と、
第１通信装置が第２通信装置に送信する通信データを含む通信メッセージを受信したとき、前記通信メッセージに対して前記認証処理を実行し、前記認証が成功した場合、前記通信メッセージを前記第２通信装置に送信する中継処理と、
を実行させる通信中継プログラム。
【請求項２】
さらに、前記第１通信装置が前記第２通信装置と通信を開始するとき送信されるメッセージであって、前記第２通信装置に通信の許可を要求する通信要求メッセージを受信したとき、前記認証処理を実行し、前記認証が成功したとき、前記第２通信装置に前記通信要求メッセージを送信する要求受信処理と、
前記通信要求メッセージに対する応答である通信応答メッセージを前記第２通信装置から受信したとき、前記認証を行い、前記認証が成功したとき、前記第１通信装置に前記通信応答メッセージを送信する応答受信処理と、
を実行させる請求項１記載の通信中継プログラム。
【請求項３】
前記中継装置は、前記通信装置が前記通信メッセージの受信を許可するか否かの受信許可状態を管理する通信管理テーブルを有し、
前記要求受信処理において、前記認証が成功したとき、前記第１通信装置が前記第２通信装置から送信される前記通信メッセージの受信を許可する状態に前記通信管理テーブルを更新する
請求項２記載の通信中継プログラム。
【請求項４】
前記通信応答メッセージは、前記通信を許可するか否かを示す許可情報を含み、
前記応答受信処理において、前記認証が成功し、前記許可情報が前記通信を許可することを示す場合、前記第２通信装置が前記第１通信装置から送信される前記通信メッセージの受信を許可する状態に前記通信管理テーブルを更新する
請求項３記載の通信中継プログラム。
【請求項５】
前記中継装置は、前記通信装置の識別子を登録する制御管理テーブルを有し、
さらに、前記通信装置が前記通信システムに参加したときに送信するメッセージであって、前記通信装置の識別子を含む登録要求メッセージを受信したとき、前記認証処理を実行し、前記認証が成功したとき、前記通信装置の識別子を前記制御管理テーブルに登録する登録処理と、
を実行させる請求項１記載の通信中継プログラム。
【請求項６】
前記制御管理テーブルは、さらに、前記通信装置が前記通信メッセージ以外の制御メッセージを送受信するネットワークアドレス又は通信ポート又はその両方を記憶し、
前記登録要求メッセージは、前記ネットワークアドレス又は通信ポート又はその両方を含み、
前記登録処理において、前記通信装置の識別子を前記制御管理テーブルに登録する場合、前記ネットワークアドレス又は通信ポート又はその両方を前記制御管理テーブルに登録する

請求項５記載の通信中継プログラム。
【請求項７】
さらに、前記第１通信装置から前記第２通信装置に送信されるメッセージであって、前記第２通信装置から送信される前記通信メッセージの受信を拒否することを通知する拒否メッセージを受信したとき、前記認証処理を実行し、前記認証が成功した場合、前記第１通信装置が前記第２通信装置から送信される前記通信メッセージの受信を許可しない状態に前記通信管理テーブルを更新し、前記拒否メッセージを前記第２通信装置に送信する拒否受信処理と、
を実行させる請求項４記載の通信中継プログラム。
【請求項８】
前記通信要求メッセージは、前記第１通信装置と前記第２通信装置間の通信で使用し、前記第１通信装置と前記第２通信装置間の通信以外の通信で使用しない共通鍵を含む、
請求項２記載の通信中継プログラム。
【請求項９】
さらに、前記認証処理において、認証に失敗した場合、受信したメッセージを破棄する破棄処理と、
を実行させる請求項１乃至８記載のいずれか１項記載の通信中継プログラム。
【請求項１０】
通信装置の識別子と、前記通信装置が通信に使用する公開鍵を分散台帳に記憶し、前記分散台帳を共有する分散台帳機能を有する複数のノードと、前記ノードのいずれかに接続する前記通信装置と、前記ノードのいずれかに接続する中継装置とを有する通信システムにおける前記中継装置であって、
前記通信装置とメッセージを送受信する送受信部と、
前記ノードから前記メッセージの送信元の通信装置の公開鍵を取得し、前記取得した公開鍵で前記メッセージに含まれる署名を認証する認証部と、
第１通信装置が第２通信装置に送信する通信データを含む通信メッセージを受信したとき、前記通信メッセージに対する認証を前記認証部に実行させ、前記認証が成功した場合、前記通信メッセージを前記第２通信装置に送信する中継部と、
を有する中継装置。
【請求項１１】
通信装置の識別子と、前記通信装置が通信に使用する公開鍵を分散台帳に記憶し、前記分散台帳を共有する分散台帳機能を有する複数のノードと、前記ノードのいずれかに接続する前記通信装置と、前記ノードのいずれかに接続する中継装置とを有する通信システムにおける前記中継装置における中継方法であって、
前記通信装置とメッセージを送受信する送受信工程と、
前記ノードから前記メッセージの送信元の通信装置の公開鍵を取得し、前記取得した公開鍵で前記メッセージに含まれる署名を認証する認証工程と、
第１通信装置が第２通信装置に送信する通信データを含む通信メッセージを受信したとき、前記通信メッセージに対して前記認証工程を実行し、前記認証が成功した場合、前記通信メッセージを前記第２通信装置に送信する中継工程と、
を有する通信中継方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信中継プログラム、中継装置、及び通信中継方法に関する。
【背景技術】
【０００２】
近年，仮想通貨を実現する基盤として登場した分散台帳技術が注目されている。分散台帳技術における通信システムは、分散台帳機能を持つ複数のノードと、ノードに接続する複数の通信装置で構成される。分散台帳は、ユーザの識別子、公開鍵、通信装置のネット

ワークアドレス情報などが記憶される。
【０００３】
ノードは、自装置配下のネットワークに通信装置が追加されると、通信装置のネットワークアドレスや公開鍵を取得し、分散台帳を更新する。そして、ノードは、他のノードに対しても当該通信装置の情報を分散台帳に追加するように通知する。これにより、各ノードは同じ内容の分散台帳を共有することができる。
【０００４】
通信装置は、ノードから相手装置のネットワークアドレスを取得し、メッセージの送受信を行う。また、通信装置は、ノードから公開鍵を取得し、送信メッセージの署名や受信メッセージに対する署名検証を行う。これにより、通信装置は、安全な通信を行うことができる。
【０００５】
分散台帳に関する技術としては、以下の特許文献１，２に記載されている。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開2018-11191号公報
【特許文献２】特開2006-101414号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
しかし、分散台帳技術における通信システムでは、ノードがネットワークアドレスを管理しているため、第三者に通信装置のネットワークアドレスが漏えいする場合がある。この場合、漏えいしたネットワークアドレスを有する通信装置は、合意しない通信によるサーバー攻撃を受ける可能性がある。
【０００８】
そこで、一開示は、分散台帳機能を有する通信の安全性を向上させる通信中継プログラム、中継装置、及び通信中継方法を提供する。
【課題を解決するための手段】
【０００９】
通信装置の識別子と、前記通信装置が通信に使用する公開鍵を分散台帳に記憶し、前記分散台帳を共有する分散台帳機能を有する複数のノードと、前記ノードのいずれかに接続する前記通信装置と、前記ノードのいずれかに接続する中継装置とを有する通信システムにおける前記中継装置が有するコンピュータに実行させる通信中継プログラムであって、前記通信装置とメッセージを送受信する送受信処理と、前記ノードから前記メッセージの送信元の通信装置の公開鍵を取得し、前記取得した公開鍵で前記メッセージに含まれる署名を認証する認証処理と、
第１通信装置が第２通信装置に送信する通信データを含む通信メッセージを受信したとき、前記通信メッセージに対して前記認証処理を実行し、前記認証が成功した場合、前記通信メッセージを前記第２通信装置に送信する中継処理と、を実行させる。
【発明の効果】
【００１０】
一開示は、分散台帳機能を有する通信の安全性を向上させる。
【図面の簡単な説明】
【００１１】
【図１】図１は、通信システム１０の構成例を示す図である。
【図２】図２は、中継装置２００の構成例を表す図である。
【図３】図３は、端末装置１００の構成例を表す図である。
【図４】図４は、ノード３００の構成例を表す図である。
【図５】図５は、通信システム１０における登録処理のシーケンスの例を示す図である。

【図６】図６は、通信システム１０が有する各装置に関する情報の例を示す図である。
【図７】図７は、ノード３００と、端末装置１００又は中継装置２００との間で送受信されるメッセージの例を示す図である。
【図８】図８は、分散台帳の例を示す図である。
【図９】図９は、端末装置１００と中継装置２００間のメッセージの例を示す図である。
【図１０】図１０は、中継登録要求受信処理Ｓ１５の処理フローチャートの例を示す図である。
【図１１】図１１は、制御用情報管理テーブル及び通信用情報管理テーブルの例を示す図である。
【図１２】図１２は、署名認証処理Ｓ１００の処理フローチャートの例を示す図である。
【図１３】図１３は、通信要求処理のシーケンスの例を示す図である。
【図１４】図１４は、ノード３００と、端末装置１００又は中継装置２００との間で送受信されるメッセージの例を示す図である。
【図１５】図１５は、通信要求受信処理Ｓ２１の処理フローチャートの例を示す図である。
【図１６】図１６は、通信用情報管理テーブルの例を示す図である。
【図１７】図１７は、通信応答受信処理Ｓ２７の処理フローチャートの例を示す図である。
【図１８】図１８は、通信処理のシーケンスの例を示す図である。
【図１９】図１９は、ノード３００と、端末装置１００又は中継装置２００との間で送受信されるメッセージの例を示す図である。
【図２０】図２０は、通信データ受信処理Ｓ４２の処理フローチャートの例を示す図である。
【図２１】図２１は、端末装置１００－２が通信応答（ＮＧ）を送信する場合のシーケンスの例を示す図である。
【図２２】図２２は、ノード３００と、端末装置１００又は中継装置２００との間で送受信されるメッセージの例を示す図である。
【図２３】図２３は、ノード３００と、端末装置１００又は中継装置２００との間で送受信されるメッセージの例を示す図である。
【図２４】図２４は、通信拒否受信処理Ｓ２００の処理フローチャートの例を示す図である。
【図２５】図２５は、通信用情報管理テーブルの例を示す図である。
【図２６】図２６は、通信中に端末装置１００－１が通信拒否を送信する場合のシーケンスの例を示す図である。
【図２７】図２７は、通信用情報管理テーブルの例を示す図である。
【発明を実施するための形態】
【００１２】
［第１の実施の形態］
第１の実施の形態について説明する。
【００１３】
＜通信システムの構成例＞
図１は、通信システム１０の構成例を示す図である。端末装置１００－１，２（以下、端末装置１００と呼ぶ場合がある）、中継装置２００、及びノード３００－１～３（以下、ノード３００とを有する。通信システム１０は、ノード３００が分散台帳を管理する分散台帳機能を有する通信システムである。通信システム１０における各装置は、ネットワークを介して接続されている。ノード３００－１は、端末装置１００－１と接続しており、端末装置１００－１に対応するノードである。言い換えると、端末装置１００－１は、ノード３００－１の配下のネットワークに接続する。同様に、ノード３００－２は、端末装置１００－２と接続しており、ノード３００－３は、中継装置２００と接続する。端末装置１００及び中継装置２００は、接続するノード３００に対して、分散台帳への登録を

要求したり、通信相手端末装置に関する情報の取得を要求したりする。

【００１４】

端末装置１００－１，２（以降、端末装置１００と呼ぶ場合がある）は、通信システム１０のユーザが通信に使用する通信装置であり、例えば、コンピュータやタブレット端末である。端末装置１００は、他の端末装置１００と通信を行う。なお、端末装置１００－１，２は、それぞれ通信ポートＰ１１，Ｐ１２、及び通信ポートＰ２１、Ｐ２２を有する。端末装置１００－１の通信ポートＰ１１は、制御用ポートである。制御用ポートは、端末装置間や中継装置２００との制御用メッセージの送受信に使用する通信ポートである。制御用メッセージについては後述する。また、端末装置１００－１の通信ポートＰ１２は、通信用ポートである。通信用ポートは、端末装置間や中継装置２００を介して他の端末装置１００との通信における、通信データの送受信に使用する通信ポートである。通信用ポートについては後述する。同様に、端末装置１００－２の通信ポートＰ２１は制御用ポートであり、通信ポートＰ２２は通信用ポートである。

【００１５】

中継装置２００は、端末装置間の通信を中継する通信装置である。中継装置２００は、端末装置１００から制御用メッセージを受信すると、受信したメッセージの安全性を確認できた場合、送信先の端末装置１００に受信した制御用メッセージを送信する。中継装置２００は、例えば、受信した制御用メッセージの署名を、公開鍵で検証することで、受信した制御用メッセージの安全性を確認する。

【００１６】

また、中継装置２００は、端末装置１００から通信用メッセージを受信すると、制御用メッセージ受信時の安全性の確認に加え、送信先の端末装置１００と通信が許可されている状態であることを確認し、受信した通信用メッセージを送信先の端末装置１００に送信する。中継装置２００は、端末装置間の通信状態を管理することで、送信先の端末装置１００と通信が許可されている状態であるか否かを確認する。

【００１７】

ノード３００－１～３（以降、ノード３００と呼ぶ場合がある）は、分散台帳を有し、各ボード３００間で分散台帳処理を行う装置である。分散台帳は、例えば、ネットワークに接続する端末装置１００（又は端末装置１００のユーザ）や中継装置２００（又は中継装置２００の管理者やユーザ）の識別子、端末装置１００が通信に使用する公開鍵、及び中継装置２００のネットワークアドレス（例えばＩＰアドレス）などを記憶するテーブルである。ノード３００は、他のノード３００と同内容の分散台帳を保有する状態にするために、分散台帳処理を行う。分散台帳処理は、例えば、あるノード３００が分散台帳を更新したタイミングで、他のノード３００に更新した情報を送信し、分散台帳の更新を指示する処理である。また、分散台帳処理は、各ノード３００が保持している分散台帳が、他のボード３００が保持する分散台帳と同様の内容を記憶しているかを確認するため、定期的または不定期に、ノード間で分散台帳の内容を確認し合う処理を含んでもよい。

【００１８】

通信システム１０では、ノード３００が分散台帳処理を行い、分散台帳を共有する。中継装置２００は、対応する（接続する）ノード３００から、端末装置１００のネットワークアドレスや公開鍵を取得し、受信したメッセージの署名を認証する。端末装置１００は、中継装置２００を介して他の端末装置１００と通信を行うことで、中継装置２００で署名認証した、安全性の高いメッセージを受信することができる。

【００１９】

なお、図１の通信システム１０は、端末装置１００が２台であるが、３台以上であってもよい。また、図１の通信システム１０は、各ノード３００に対して１台の端末装置１００又は中継装置２００が接続しているが、複数台の装置が接続されてもよい。さらに、図１の通信システム１０は、ノード３００が３台であるが、１台又は２台であってもよいし、端末装置１００や中継装置２００が図１よりも多く存在する場合、４台以上であってもよい。

【００２０】
＜中継装置の構成例＞
図２は、中継装置２００の構成例を表す図である。中継装置２００は、例えば、コンピュータやサーバマシンである。
【００２１】
中継装置２００は、ＣＰＵ（Central Processing Unit）２１０、ストレージ２２０、メモリ２３０、通信回路２４０－１～ｎ（ｎは２以上の整数）を有する。
【００２２】
ストレージ２２０は、プログラムやデータを記憶する、フラッシュメモリ、ＨＤＤ（Hard Disk Drive）、又はＳＳＤ（Solid State Drive）などの補助記憶装置である。ストレージ２２０は、ノード側通信プログラム２２１、端末側通信プログラム２２２、中継登録要求受信プログラム２２３、通信要求受信プログラム２２４、通信応答受信プログラム２２５、通信拒否受信プログラム２２６、署名認証プログラム２２７、制御情報管理テーブル２２８、及び通信情報管理テーブル２２９を記憶する。テーブルは、メモリ２３０に記憶されてもよい。
【００２３】
制御情報管理テーブル２２８は、中継装置２００が、通信システム１０に参加する（接続する）端末装置１００を管理するテーブルである。端末装置１００は、通信システム１０に参加し、他の端末装置１００と通信を行う場合、制御情報管理テーブル２２８に自装置（又は自装置のユーザ）の識別子や、通信に使用するネットワークアドレスなどを登録されていることが必要となる。
【００２４】
通信情報管理テーブル２２９は、中継装置２００が、端末装置１００の通信状態を管理するテーブルである。中継装置２００は、通信情報管理テーブル２２９に、どの端末装置１００がどの端末装置１００からの通信メッセージの受信を許容（許可）しているかを記憶する。
【００２５】
メモリ２３０は、ストレージ２２０に記憶されているプログラムをロードする領域である。また、メモリ２３０は、プログラムがデータを記憶する領域としても使用されてもよい。
【００２６】
通信回路２４０－１～ｎ（以降、通信回路２４０と呼ぶ場合がある）は、ネットワークと接続するインターフェースである。通信回路２４０は、それぞれ無線又は有線に対応する。通信回路２４０は、例えば、ネットワークインターフェースカードなどの、インターネットに接続する通信ポートを有するインターフェース機器である。また、中継装置２００は、通信回路２４０を介して、ノード３００－３、端末装置１００と通信を行う。
【００２７】
ＣＰＵ２１０は、ストレージ２２０に記憶されているプログラムを、メモリ２３０にロードし、ロードしたプログラムを実行し、各部を構築し、各処理を実現するプロセッサである。
【００２８】
ＣＰＵ２１０は、ノード側通信プログラム２２１を実行することで、ノード側送受信部を構築し、ノード側通信処理を行う。ノード側通信処理は、接続するノード３００とメッセージの送受信を行う処理である。
【００２９】
ＣＰＵ２１０は、端末側通信プログラム２２２を実行することで、送受信部を構築し、端末側通信処理を行う。端末側通信処理は、端末装置１００とメッセージの送受信を行う処理である。
【００３０】
ＣＰＵ２１０は、中継登録要求受信プログラム２２３を実行することで、登録部を構築

し、中継登録要求受信処理を行う。中継登録要求受信処理は、端末装置１００から中継登録要求を受信したときの処理である。中継装置２００は、中継登録要求受信処理において、受信したメッセージの署名を認証し、端末装置１００（又は端末装置１００のユーザ）の識別子や、端末装置１００が他の端末装置１００との通信に使用するネットワークアドレスや通信ポートの番号などを、制御情報管理テーブル２２８に記憶（登録）する。

【００３１】

ＣＰＵ２１０は、通信要求受信プログラム２２４を実行することで、要求受信部を構築し、通信要求受信処理を行う。通信要求受信処理は、端末装置１００から通信要求を受信したときの処理である。中継装置２００は、通信要求受信処理において、受信したメッセージの署名を認証し、受信した通信要求を通信要求の送信先の端末装置１００に送信する。

【００３２】

ＣＰＵ２１０は、通信応答受信プログラム２２５を実行することで、応答受信部を構築し、通信応答受信処理を行う。通信応答受信処理は、端末装置１００から通信要求の応答メッセージである通信応答を受信したときの処理である。中継装置２００は、通信応答受信処理において、受信したメッセージの署名を認証し、受信した通信応答を、通信要求の送信元の端末装置１００に送信する。

【００３３】

ＣＰＵ２１０は、通信拒否受信プログラム２２６を実行することで、拒否受信部を構築し、通信拒否受信処理を行う。通信拒否受信処理は、端末装置１００から、以降の通信データを含む通信メッセージの受信を拒否する通信拒否を受信したときの処理である。中継装置２００は、通信拒否受信処理において、受信したメッセージの署名を認証し、受信した通信拒否を通信拒否の送信先の端末装置１００に送信する。

【００３４】

ＣＰＵ２１０は、署名認証プログラム２２７を実行することで、認証部を構築し、署名認証処理を行う。署名認証処理は、端末装置１００から受信したメッセージを、メッセージに含まれる署名を用いて認証する処理である。中継装置２００は、署名認証処理に、ノード３００から送信元端末装置１００の公開鍵を取得し、当該メッセージに含まれる署名の認証を行う。

【００３５】

＜端末装置の構成例＞

図３は、端末装置１００の構成例を表す図である。端末装置１００は、ユーザが通信を行うときに使用する通信装置であり、例えば、コンピュータやタブレット端末である。

【００３６】

端末装置１００は、ＣＰＵ１１０、ストレージ１２０、メモリ１３０、通信回路１４０－１～ｎを有する。

【００３７】

ストレージ１２０は、プログラムやデータを記憶する、フラッシュメモリ、ＨＤＤ、又はＳＳＤなどの補助記憶装置である。ストレージ１２０は、ノード側通信プログラム１２１、分散台帳登録プログラム１２２、通信開始プログラム１２３、通信プログラム１２４、及び通信拒否プログラム１２５を記憶する。

【００３８】

メモリ１３０は、ストレージ１２０に記憶されているプログラムをロードする領域である。また、メモリ１３０は、プログラムがデータを記憶する領域としても使用されてもよい。

【００３９】

通信回路１４０－１～ｍ（以降、通信回路１４０と呼ぶ場合がある）は、ネットワークと接続するインターフェースである。通信回路１４０は、例えば、ネットワークインターフェースカードなどの、インターネットに接続する通信ポートを有するインターフェース機器である。また、通信回路１４０は、例えば、アンテナを有し、無線接続を行う無線用

通信回路であってもよい。端末装置１００は、例えば、通信回路１４０－１を制御用ポートとして使用し、通信回路１４０－２を通信用ポートとして使用してもよい。端末装置１００は、通信回路１４０を介して、他の端末装置１００、中継装置２００、ノード３００と通信を行う。

【００４０】

ＣＰＵ１１０は、ストレージ１２０に記憶されているプログラムを、メモリ１３０にロードし、ロードしたプログラムを実行し、各部を構築し、各処理を実現するプロセッサである。

【００４１】

ＣＰＵ１１０は、ノード側通信プログラム２２１を実行することで、ノード側送受信部を構築し、ノード側通信処理を行う。ノード側通信処理は、接続するノード３００とメッセージの送受信を行う処理である。

【００４２】

ＣＰＵ１１０は、分散台帳登録プログラム１２２を実行することで、ノード登録部を構築し、分散台帳登録処理を行う。分散台帳登録処理は、例えば、端末装置１００が通信システム１０に参加したとき、接続又は再接続したときなど、ノード３００の分散台帳に登録する処理である。端末装置１００は、分散台帳登録処理において、ノード３００に分散台帳に登録するよう要求する。端末装置１００は、当該要求時に、自装置の公開鍵、自装置（又はユーザ）の識別子などをノード３００に通知する。そして、ノード３００から分散台帳への登録が完了したことを通知されると、自装置を中継装置２００に登録する処理を行う。

【００４３】

ＣＰＵ１１０は、通信開始プログラム１２３を実行することで、通信開始部を構築し、通信開始処理を行う。通信開始処理は、自装置が中継装置２００に登録されている状態で、端末装置１００が他の通信システムと通信を開始するときに実行する処理である。端末装置１００は、通信開始処理において、中継装置２００に通信要求を送信し、相手の端末装置１００からの応答（通信応答）を待ち受ける。端末装置１００は、相手の端末装置１００からの通信応答を受信すると、通信状態となる。

【００４４】

ＣＰＵ１１０は、通信プログラム１２４を実行することで、通信部を構築し、通信処理を行う。通信処理は、通信状態において、端末装置１００が中継装置２００を介して他の端末装置１００と通信メッセージを送受信する処理である。

【００４５】

ＣＰＵ１１０は、通信拒否プログラム１２５を実行することで、通信拒否部を構築し、通信拒否処理を行う。通信拒否処理は、通信メッセージを受信しないことを他の端末装置１００に通知する処理である。端末装置１００は、例えば、通信を終了するとき、通信拒否を中継装置２００を介して他の端末装置１００に送信し、以降通信を行わないことを通知する。

【００４６】

＜ノードの構成例＞

図４は、ノード３００の構成例を表す図である。ノード３００は、例えば、サーバマシンやコンピュータである。

【００４７】

ノード３００は、ＣＰＵ３１０、ストレージ３２０、メモリ３３０、通信回路３４０－１～ｎを有する。

【００４８】

ストレージ３２０は、プログラムやデータを記憶する、フラッシュメモリ、ＨＤＤ、又はＳＳＤなどの補助記憶装置である。ストレージ３２０は、分散台帳プログラム３２１、端末及び中継装置側通信プログラム３２２、分散台帳３２３を記憶する。

【００４９】

メモリ３３０は、ストレージ３２０に記憶されているプログラムをロードする領域である。また、メモリ３３０は、プログラムがデータを記憶する領域としても使用されてもよい。

【００５０】

通信回路３４０－１～ｎ（以降、通信回路３４０と呼ぶ場合がある）は、ネットワークと接続するインターフェースである。通信回路３４０は、例えば、ネットワークインターフェースカードなどの、インターネットに接続する通信ポートを有するインターフェース機器である。また、ノード３００は、通信回路３４０を介して、他のノード３００、端末装置１００、および中継装置２００と通信を行う。

【００５１】

ＣＰＵ３１０は、ストレージ３２０に記憶されているプログラムを、メモリ３３０にロードし、ロードしたプログラムを実行し、各部を構築し、各処理を実現するプロセッサである。

【００５２】

ＣＰＵ３１０は、分散台帳プログラム３２１を実行することで、分散台帳部を構築し、分散台帳処理を行う。分散台帳処理は、分散台帳への端末装置１００の登録、削除、更新を行い、他のノード３００と分散台帳を共有する処理である。ノード３００は、分散台帳処理において、端末装置１００から識別子や公開鍵を取得し、分散台帳に登録する。そして、更新した分散台帳の内容を、他のノード３００と共有する。

【００５３】

ＣＰＵ３１０は、端末及び中継装置側通信プログラム３２２を実行することで、装置通信部を構築し、端末及び中継装置側通信処理を行う。端末及び中継装置側通信処理は、端末装置１００や中継装置２００と、メッセージを送受信する処理である。

【００５４】

＜端末装置間の通信＞

端末装置間の通信は、登録処理、通信要求処理、及び通信処理を行うことで実現する。それぞれの処理について説明する。

【００５５】

＜１．登録処理＞

登録処理は、例えば、端末装置１００が通信システム１０に参入したタイミングで実行される処理であり、新規参入した端末装置１００に関する情報を、ノード３００（分散台帳）及び中継装置２００に登録する処理である。なお、端末装置１００－１が中継装置２００と送受信するメッセージは、制御用メッセージであり、端末装置１００－１は、中継装置２００とのメッセージの送受信を、通信ポートＰ１１（制御用ポート）を使用して行う。

【００５６】

図５は、通信システム１０における登録処理のシーケンスの例を示す図である。図５は、端末装置１００－１が通信システム１０に新規参入（参加）した場合の例を示す図である。

【００５７】

図６は、通信システム１０が有する各装置に関する情報の例を示す図である。以降、実施例において、各装置のネットワークアドレス、識別子、公開鍵、秘密鍵は、図６に従うものとする。

【００５８】

端末装置１００－１は、接続する（対応する）ノード３００－１にノード登録要求を送信する（Ｓ１１）。ノード登録要求は、端末装置１００に関する情報（例えば、公開鍵、ネットワークアドレス、端末装置１００又は端末装置１００のユーザの識別子を含む）の分散台帳への登録を、ノード３００に要求するメッセージである。

【００５９】

図７は、ノード３００と、端末装置１００又は中継装置２００との間で送受信されるメ

ッセージの例を示す図である。図７（Ａ）は、ノード登録要求Ｓ１１の例を示す図である。

【００６０】

ノード登録要求は、送信元アドレス、送信先アドレス、メッセージ種別、送信元識別子、及び公開鍵を含むメッセージである。

【００６１】

送信元アドレス及び送信先アドレスは、ノード登録要求の送信元の装置のネットワークアドレス及び送信先の装置のネットワークアドレスが掲載される。ノード登録要求Ｓ１１の場合、送信元アドレスは当該メッセージの送信元である端末装置１００－１のネットワークアドレス「ＩＰ１」が掲載され、送信先アドレスは当該メッセージの送信先であるノード３００－１のネットワークアドレス「ＩＰＮ１」が掲載される。

【００６２】

各メッセージにおいて、送信元アドレス及び送信先アドレスは、当該メッセージの送信先アドレス及び送信先アドレスが掲載され、例えば、中継装置２００を介して他の端末装置１００に送信されるメッセージは、送信先アドレスは中継装置２００のネットワークアドレスとなる。また、送信元アドレス及び送信先アドレスは、通信ポート番号まで掲載される場合があるものとする。以降、メッセージの説明において、送信元アドレス及び送信先アドレスについては、省略する場合がある。

【００６３】

メッセージ種別は、当該メッセージが何のメッセージであるかを示す情報が掲載される。ノード登録要求Ｓ１１の場合、メッセージ種別は、当該メッセージの種別である「ノード登録要求」を示す情報が掲載される。以降、メッセージの説明において、メッセージ種別については、説明を省略する場合がある。

【００６４】

送信元識別子は、送信元の装置の識別子又は送信元の装置の識別子のユーザの識別子が掲載される。ノード登録要求Ｓ１１の場合、送信元識別子は、端末装置１００－１の識別子「ａｂｃ」が掲載される。

【００６５】

公開鍵は、ノード登録要求の送信元の端末装置１００が通信に使用する公開鍵に関する情報が掲載される。ノード登録要求Ｓ１１の場合、端末装置１００－１が通信に使用する公開鍵「Ｐｋａ」が掲載される。

【００６６】

図５のシーケンスに戻り、ノード３００－１は、ノード登録要求を受信すると、受信した情報に基づき自装置が有する分散台帳を更新し、他のノード３００－２及びノード３００－３に対して自装置の分散台帳と同様の内容に分散台帳を更新するよう要求（指示）する分散台帳処理を行う（Ｓ１２）。これにより、各ノード３００が有する分散台帳は同様の内容となる。

【００６７】

図８は、分散台帳の例を示す図である。分散台帳は、管理する情報要素として、装置、アドレス、識別子、公開鍵を含む。なお、図８は、すでに中継装置２００及び端末装置１００－２の登録は完了している分散台帳の例である。

【００６８】

装置は、各装置の名称や識別子である。ノード３００－１は、端末装置１００－１からノード登録要求を受信したことに応答し、端末装置１００－１の情報を分散台帳に記憶する。なお、装置は、以降に説明する識別子として管理してもよい。

【００６９】

アドレスは、各装置のネットワークアドレスである。分散台帳は、端末装置１００－１のアドレスとして、何も記憶しない。第１の実施の形態において、ノード３００は、分散台帳に端末装置１００の通信用のネットワークアドレスを記憶しないことで、悪意の第三者が端末装置１００の通信用のネットワークアドレスを取得することを防止し、より安全

な通信を提供することができる。

【００７０】

識別子は、各装置、又は各装置のユーザの識別子である。分散台帳は、端末装置１００－１の識別子として、「ａｂｃ」が記憶される。

【００７１】

公開鍵は、各装置が通信に使用する公開鍵である。分散台帳は、端末装置１００－１の公開鍵として、「Ｐｋａ」が記憶される。

【００７２】

図５のシーケンスに戻り、ノード３００－１は、分散台帳を更新すると、端末装置１００－１にノード登録応答を送信する（Ｓ１３）。ノード登録応答は、分散台帳に装置の情報が登録されたことを通知するメッセージである。

【００７３】

図７（Ｂ）は、ノード登録応答Ｓ１３の例を示す図である。ノード登録応答は、送信元アドレス、送信先アドレス、メッセージ種別、中継装置識別子、及び中継装置アドレスを含むメッセージである。

【００７４】

中継装置識別子は、端末装置間の通信を中継する中継装置の識別子が掲載される。ノード登録応答Ｓ１３の場合、中継装置識別子は、中継装置２００の識別子「ｘｙｚ」が掲載される。

【００７５】

中継装置アドレスは、端末装置間の通信を中継する中継装置のネットワークアドレスが掲載される。ノード登録応答Ｓ１３の場合、中継装置アドレスは、中継装置２００のネットワークアドレス「ＩＰ３」が掲載される。

【００７６】

図５のシーケンスに戻り、端末装置１００－１は、ノード登録応答Ｓ１３を受信し、中継装置２００のネットワークアドレス及び識別子を取得する。なお、端末装置１００は、中継装置２００のネットワークアドレスや識別子を、ノード登録応答から取得せず、他のメッセージ（例えば、通信開始時に送受信するメッセージなど）で取得してもよい。

【００７７】

端末装置１００－１は、ノード登録応答Ｓ１３を受信すると、中継装置２００に中継登録要求を送信する（Ｓ１４）。中継登録要求は、端末装置１００が中継装置２００に、自装置に関する情報を登録するよう要求するメッセージである。

【００７８】

図９は、端末装置１００と中継装置２００間のメッセージの例を示す図である。図９（Ａ）は、中継登録要求Ｓ１４の例を示す図である。中継登録要求は、送信元アドレス、送信先アドレス、タイプ、メッセージ種別、送信元識別子、通信用アドレス、署名を含むメッセージである。

【００７９】

タイプは、メッセージのタイプが制御用であるか通信用であるかを示す情報が掲載される。制御用メッセージは、端末装置１００間の通信の開始や終了などの制御に使用するメッセージである。制御用メッセージは、以降に示す署名認証に成功した場合、送信先の端末装置１００に転送される。一方、通信用メッセージは、端末装置１００間で送受信する通信データを含むメッセージである。通信用メッセージは、署名認証に加え、中継装置２００が管理する通信状態において通信中である場合、送信先の端末装置１００に転送される。中継登録要求Ｓ１４は、制御用メッセージであり、タイプは、制御用メッセージであることを示す「制御」が掲載される。以降、メッセージの説明において、タイプは同様であるものとする。

【００８０】

送信元識別子は、送信元の装置の識別子が掲載される。送信元識別子は、以降に説明する、中継装置２００が実行する署名認証処理において使用される。中継登録要求Ｓ１４の

場合、送信元識別子は、端末装置１００－１の識別子「ａｂｃ」が掲載される。
【００８１】
通信用アドレスは、送信元の装置が通信用メッセージの送受信に使用するネットワークアドレスが掲載される。例えば、通信用アドレスを、制御用メッセージの送受信とはことなるネットワークアドレスとすることで、安全性が向上する。ここでは、通信用アドレスを通信ポートまで指定し、制御用メッセージの送受信の通信ポートと異ならせることで、安全性を向上させるものとする。中継登録要求Ｓ１４の場合、通信用アドレスは、端末装置１００－１のネットワークアドレス及び通信用ポートである「ＩＰ１　ポートＰ１２」が掲載される。
【００８２】
署名は、署名データが掲載される。端末装置１００や中継装置２００は、例えば、秘密鍵で生成された署名データを公開鍵で検証することで、当該署名データの送信元の認証を行う。中継登録要求Ｓ１４の場合、署名は、端末装置１００－１の秘密鍵Ｓｋａで生成された署名データが掲載される。
【００８３】
図５のシーケンスに戻り、中継装置２００は、中継登録要求Ｓ１４を受信すると、中継登録要求受信処理を行う（Ｓ１５）。
【００８４】
図１０は、中継登録要求受信処理Ｓ１５の処理フローチャートの例を示す図である。中継装置２００は、中継登録要求受信処理Ｓ１５において、署名認証処理を行う（Ｓ１００）。署名認証処理Ｓ１００は、受信したメッセージの署名を認証する処理であり、詳細は後述する。
【００８５】
中継装置２００は、署名認証が成功すると（Ｓ１５－１のＹｅｓ）、送信元の端末装置１００に中継登録応答を送信し（Ｓ１５－２）、制御用情報管理テーブル、及び通信用情報管理テーブルを更新する（Ｓ１５－３）。制御用情報管理テーブル、及び通信用情報管理テーブルについては、後述する。
【００８６】
一方、中継装置２００は、署名認証が失敗すると（Ｓ１５－１のＮｏ）、送信元の端末装置１００は、通信システム１０上で正式に認証された端末装置１００ではないと判定し、当該中継装置登録要求を破棄し、処理を終了する。
【００８７】
図１１は、制御用情報管理テーブル及び通信用情報管理テーブルの例を示す図である。図１１（Ａ）は、制御用情報管理テーブルの例を示す図である。制御用情報管理テーブルは、識別子及び制御用アドレスを含む。
【００８８】
識別子は、登録された端末装置１００の識別子である。図１１（Ａ）においては、端末装置１００－１の識別子「ａｂｃ」及び端末装置１００－２の識別子「ｄｅｆ」が登録されている。
【００８９】
制御アドレスは、識別子に対応する端末装置１００の制御用メッセージに使用するネットワークアドレス及びポート番号である。図１１（Ａ）においては、端末装置１００－１のネットワークアドレスと制御用ポート「ＩＰ１　ポートＰ１１」、及び端末装置１００－２のネットワークアドレスと制御用ポート「ＩＰ２　ポートＰ２１」が登録されている。
【００９０】
図１１（Ｂ）は、通信用情報管理テーブルの例を示す図である。通信用情報管理テーブルは、受信側識別子、送信側識別子、受信側通信用アドレスを含む。
【００９１】
受信側識別子は、通信用メッセージの受信を許可する端末装置１００の識別子である。

図１１（Ｂ）においては、端末装置１００－１の識別子「ａｂｃ」及び端末装置１００－２の識別子「ｄｅｆ」が登録されている。

【００９２】

送信側識別子は、受信側識別子に登録されている端末装置１００が受信を許可する送信元の端末装置１００の識別子である。図１１（Ｂ）においては、何も登録されていない。送信側識別子は、通信が行われていない状態では、何も登録されない。

【００９３】

受信側通信用アドレスは、受信側識別子に登録されている端末装置１００が通信用メッセージの送受信に使用するネットワークアドレス及びポート番号である。図１１（Ｂ）においては、端末装置１００－１のネットワークアドレスと通信用ポート「ＩＰ１　ポート１２」、及び端末装置１００－２のネットワークアドレスと通信用ポート「ＩＰ２　ポート２２」が登録されている。

【００９４】

図１２は、署名認証処理Ｓ１００の処理フローチャートの例を示す図である。中継装置２００は、署名認証処理Ｓ１００において、接続するノード３００から署名認証の対象となるメッセージの送信元の識別子を持つ端末装置１００の公開鍵を取得し、当該メッセージの送信元が正当であるかどうか（登録されている端末装置であるか否か）を認証する。

【００９５】

中継装置２００は、署名認証処理Ｓ１００において、接続するノード３００に署名検証要求を送信する（Ｓ１００－１）。署名検証要求は、ノード３００に対して、メッセージに含まれる識別子に対応する公開鍵を送信するよう要求するメッセージである。署名検証要求に含まれる情報については、後述する。

【００９６】

なお、中継装置２００は、端末装置１００からメッセージを受信したときの各処理において、署名認証処理Ｓ１００を実行する。中継装置２００は、署名認証処理Ｓ１００において認証が失敗した場合（認証がエラーとなった場合）、当該受信メッセージを破棄する破棄処理を行う。

【００９７】

中継装置２００は、ノード３００からの署名検証応答を待ち受ける（Ｓ１００－２のＮｏ）。署名検証応答は、中継装置２００に対象の識別子を有する端末装置１００の公開鍵を引き渡すメッセージである。署名検証応答に含まれる情報については、後述する。

【００９８】

中継装置２００は、ノード３００から署名検証応答を受信すると（Ｓ１００－２のＹｅｓ）、対象の識別子に対応する公開鍵を取得できたか否かを確認する（Ｓ１００－３）。例えば、対象の識別子がノード３００の分散台帳に登録されていない場合、ノード３００は、署名検証応答に公開鍵を掲載しない。この場合、中継装置２００は、公開鍵を取得できないと判定する。

【００９９】

中継装置２００は、公開鍵を取得できた場合（Ｓ１００－３のＹｅｓ）、取得した公開鍵で受信したメッセージの署名の認証を行う（Ｓ１００－４）。中継装置２００は、署名認証が成功した場合（Ｓ１００－４のＹｅｓ）、当該メッセージを認証成功と判定し（Ｓ１００－５）、署名認証が失敗した場合（Ｓ１００－４のＮｏ）、当該メッセージを認証失敗と判定し（Ｓ１００－６）、処理を終了する。

【０１００】

一方、中継装置２００は、公開鍵を取得できなかった場合（Ｓ１００－３のＮｏ）、当該識別子は分散台帳に登録されていないとみなし、当該メッセージを認証失敗と判定し（Ｓ１００－６）、処理を終了する。

【０１０１】

図５のシーケンスに戻り、中継装置２００は、中継登録要求受信処理Ｓ１５において、中継装置２００は、署名検証要求をノード３００－３に送信する（Ｓ１６、図１２のＳ１

００－１）。
【０１０２】
図７（Ｃ）は、署名検証要求Ｓ１６の例を示す図である。署名検証要求は、送信元アドレス、送信先アドレス、メッセージ種別、及び識別子を含む。識別子は、署名認証の対象となるメッセージの送信元の識別子である。署名検証要求Ｓ１６の場合、識別子は、中継登録要求Ｓ１４の送信元である端末装置１００－１の識別子「ａｂｃ」が掲載される。
【０１０３】
図５のシーケンスに戻り、ノード３００－１は、署名検証要求Ｓ１６を受信すると、識別子「ａｂｃ」に対応する公開鍵「Ｐｋａ」を分散台帳から検出し、署名検証応答に掲載し、中継装置２００に返信する（Ｓ１７）。
【０１０４】
図７（Ｄ）は、署名検証応答Ｓ１７の例を示す図である。署名検証応答は、送信元アドレス、送信先アドレス、メッセージ種別、識別子検索結果、及び公開鍵を含む。識別子検索結果は、署名検証要求の識別子を分散台帳から検索した結果である。署名検証応答Ｓ１７の場合、識別子検索結果は、識別子「ａｂｃ」が分散台帳に登録済みであり、ノード３００－１が識別子「ａｂｃ」を検出できるため、ＯＫ（検索できた旨を示す）が掲載される。公開鍵は、署名検証要求の識別子に対応する公開鍵である。署名検証応答Ｓ１７の場合、公開鍵は、識別子「ａｂｃ」に対応する公開鍵「Ｐｋａ」が掲載される。
【０１０５】
図５のシーケンスに戻り、中継装置２００は、署名検証応答Ｓ１７を受信すると、中継登録要求受信処理Ｓ１５において実行した署名認証処理Ｓ１００の結果を確認し、認証が成功したことを認識し（図１０のＳ１５－１のＹｅｓ）、端末装置１００－１に中継登録応答を送信する（Ｓ１８、図１０のＳ１５－２）。
【０１０６】
図９（Ｂ）は、中継登録応答Ｓ１８の例を示す図である。中継登録応答は、送信元アドレス、送信先アドレス、タイプ、メッセージ種別、送信元識別子、及び登録結果を含む。送信元識別子は、中継登録応答の送信元である中継装置２００の識別子である。中継登録応答Ｓ１８の場合、送信元識別子は、中継装置２００の識別子「ｘｙｚ」が掲載される。登録結果は、中継登録要求で要求された識別子、通信用アドレスなどが、中継装置２００の内部テーブルに登録されたか否かの結果を示す。中継登録応答Ｓ１８の場合、登録結果は、中継登録要求Ｓ１４の識別子「ａｂｃ」及び通信用ポート「ＩＰ１　ポートＰ１２」が、制御用情報管理テーブル又は通信用情報管理テーブルに登録されているため、ＯＫ（登録できた）が掲載される。
【０１０７】
図５のシーケンスに戻り、端末装置１００－１は、中継登録応答Ｓ１８を受信し、中継装置２００への登録が完了したと認識し、登録処理を完了する。
【０１０８】
＜２．通信要求処理＞
通信要求処理は、例えば、登録処理が完了している端末装置１００が他の端末装置１００と通信を開始するときの処理である。なお、端末装置１００－１及び端末装置１００－２が中継装置２００と送受信するメッセージは、制御用メッセージであり、端末装置１００－１が通信ポートＰ１１（制御用ポート）を使用し、端末装置１００－２が通信ポートＰ２１（制御用ポート）を使用して、中継装置２００と送受信を行う。
【０１０９】
図１３は、通信要求処理のシーケンスの例を示す図である。端末装置１００－１は、端末装置１００－２と通信を開始するとき、中継装置２００に通信要求を送信する（Ｓ２１）。
【０１１０】
図１４は、ノード３００と、端末装置１００又は中継装置２００との間で送受信されるメッセージの例を示す図である。図１４（Ａ）は、通信要求Ｓ２１の例を示す図である。

【０１１１】
通信要求は、送信元アドレス、送信先アドレス、タイプ、メッセージ種別、送信元識別子、送信先識別子、及び署名を含むメッセージである。
【０１１２】
送信元識別子は、通信の開始を要求する端末装置１００の識別子が掲載される。通信要求Ｓ２１の場合、送信元識別子は、端末装置１００－１の識別子「ａｂｃ」が掲載される。
【０１１３】
送信先識別子は、通信の開始を要求される側の端末装置１００の識別子が掲載される。通信要求Ｓ２１の場合、送信先識別子は、端末装置１００－２の識別子「ｄｅｆ」が掲載される。
【０１１４】
署名は、署名データが掲載される。通信要求Ｓ２１の場合、署名は、端末装置１００－１の秘密鍵Ｓｋａで生成された署名データが掲載される。
【０１１５】
図１３のシーケンスに戻り、中継装置２００は、通信要求Ｓ２１を受信すると、通信要求受信処理を行う（Ｓ２２）。
【０１１６】
図１５は、通信要求受信処理Ｓ２１の処理フローチャートの例を示す図である。中継装置２００は、通信要求受信処理Ｓ２１において、署名認証処理Ｓ１００を行う。中継装置２００は、署名認証処理Ｓ１００の結果、受信したメッセージの署名の認証が成功した場合（Ｓ２２－１のＹｅｓ）、当該ユーザが制御用情報管理テーブルに登録済みであるか否かを確認する（Ｓ２２－２）。
【０１１７】
一方、中継装置２００は、署名認証処理Ｓ１００の結果、受信したメッセージの署名の認証が失敗した場合（Ｓ２２－１のＮｏ）、受信したメッセージを破棄し、処理を終了する。
【０１１８】
中継装置２００は、当該ユーザが制御用情報管理テーブルに登録済みである場合（Ｓ２２－２のＹｅｓ）、送信先の端末装置１００に通信要求を送信し（Ｓ２２－３）、通信用情報管理テーブルを更新し（Ｓ２２－４）、処理を終了する。中継装置２００は、処理Ｓ２２－４において、通信要求の送信元の端末装置１００の識別子が記憶された受信側識別子に対応する送信側識別子を、送信先識別子に更新する。通信用情報管理テーブルを上述のように更新することで、少なくとも、通信要求を送信した端末装置１００は、送信先の端末装置１００からの通信用メッセージの受信を許可している状態となる。
【０１１９】
一方、中継装置２００は、当該ユーザが制御用情報管理テーブルに登録済みでない場合（Ｓ２２－２のＮｏ）、送信元の端末装置１００に通信応答（ＮＧ）を送信し（Ｓ２２－５）、処理を終了する。中継装置２００は、未登録の端末装置１００から通信要求を受信した場合、通信応答（ＮＧ）を返信し、当該端末装置１００のノード３００の分散台帳への登録、又は中継装置２００への登録のいずれかが、正しく完了していないことを送信元の端末装置１００に通知する。
【０１２０】
図１３のシーケンスに戻り、中継装置２００は、通信要求受信処理Ｓ２２において、署名認証処理Ｓ１００を行い、ノード３００－３に署名検証要求を送信し（Ｓ２３、図１２のＳ１００－１）、ノード３００－３から署名検証応答を受信し（Ｓ２４、図１２のＳ１００－２）、受信した通信要求Ｓ２１の署名の認証を行う。中継装置２００は、端末装置１００－１は正当な端末装置１００であると認証し（図１２のＳ１００－４）、認証成功と判定する（図１５のＳ２２－１のＹｅｓ）。そして、中継装置２００は、端末装置１００－１が制御情報管理テーブルに登録されていることを確認し（図１５のＳ２２－２のＹ

ｅｓ）、送信先の端末装置１００－２に通信要求を送信する（Ｓ２５、図１５のＳ２２－３）。

【０１２１】

図１４（Ｂ）は、通信要求Ｓ２５の例を示す図である。中継装置２００は、送信元アドレス及び送信先アドレス以外は、受信した通信要求Ｓ２１の内容を載せ替え、通信要求Ｓ２５を端末装置１００－２に送信する。

【０１２２】

図１３のシーケンスに戻り、中継装置２００は、通信用情報管理テーブルを更新し（図１５のＳ２２－４）、通信要求受信処理Ｓ２２を終了し、通信応答を待ち受ける。

【０１２３】

図１６は、通信用情報管理テーブルの例を示す図である。中継装置２００は、通信用情報管理テーブルを、図１１（Ｂ）に示す状態（受信側識別子「ａｂｃ」に対応する送信側識別子「－」）を、図１６（Ａ）に示す状態のように、受信側識別子「ａｂｃ」に対応する送信側識別子を、通信要求に含まれる送信先識別子である「ｄｅｆ」とする。

【０１２４】

図１３のシーケンスに戻り、中継装置２００は、端末装置１００－２から通信応答を受信すると（Ｓ２６）、通信応答受信処理を行う（Ｓ２７）。

【０１２５】

図１４（Ｃ）は、通信応答Ｓ２６の例を示す図である。通信応答は、送信元アドレス、送信先アドレス、タイプ、メッセージ種別、送信元識別子、送信先識別子、通信許可、及び署名を含むメッセージである。

【０１２６】

送信元識別子は、通信の開始を許可（又は不許可）する端末装置１００の識別子が掲載される。通信応答Ｓ２６の場合、送信元識別子は、端末装置１００－２の識別子「ｄｅｆ」が掲載される。

【０１２７】

送信先識別子は、通信の開始を許可（又は不許可）された端末装置１００の識別子が掲載される。通信応答Ｓ２６の場合、送信先識別子は、端末装置１００－１の識別子「ａｂｃ」が掲載される。

【０１２８】

通信許可は、通信を許可するか否か（通信メッセージの受信を許可するか否か）を示す情報である。通信応答Ｓ２６の場合、通信許可は、端末装置１００－２が端末装置１００－１からの通信メッセージの受信を許可する「ＯＫ」が掲載される。

【０１２９】

署名は、署名データが掲載される。通信応答Ｓ２６の場合、署名は、端末装置１００－２の秘密鍵Ｓｋｄで生成された署名データが掲載される。

【０１３０】

図１７は、通信応答受信処理Ｓ２７の処理フローチャートの例を示す図である。中継装置２００は、通信応答受信処理Ｓ２７において、署名認証処理Ｓ１００を行う。中継装置２００は、署名認証処理Ｓ１００の結果、受信したメッセージの署名の認証が成功した場合（Ｓ２７－１のＹｅｓ）、当該ユーザが制御用情報管理テーブルに登録済みであるか否かを確認する（Ｓ２７－２）。

【０１３１】

中継装置２００は、当該ユーザが制御用情報管理テーブルに登録済みである場合（Ｓ２７－２のＹｅｓ）、通信応答の通信許可がＯＫか否かを確認する（Ｓ２７－３）。中継装置２００は、通信応答の通信許可がＯＫである場合（Ｓ２７－３のＹｅｓ）、送信先の端末装置１００（通信要求の送信元の端末装置１００）に通信応答（ＯＫ）を送信し（Ｓ２７－４）、通信用情報管理テーブルを更新し（Ｓ２７－５）、処理を終了する。中継装置２００は、処理Ｓ２７－５において、通信応答（ＯＫ）の送信元の端末装置１００の識別子が記憶された受信側識別子に対応する送信側識別子を、送信先識別子に更新する。通信

用情報管理テーブルを上述のように更新することで、通信応答（ＯＫ）を送信した端末装置１００は、送信先の端末装置１００からの通信用メッセージの受信を許可している状態となる。すなわち、通信要求受信処理Ｓ２２における更新処理Ｓ２２－４及び通信応答受信処理Ｓ２７における更新処理Ｓ２７－５の両方を実施することで、通信する端末装置１００の双方向のメッセージの送受信が許可された状態となる。

【０１３２】

一方、中継装置２００は、通信応答の通信許可がＮＧである場合（Ｓ２７－３のＮｏ）、送信先の端末装置１００（通信要求の送信元の端末装置１００）に通信応答（ＮＧ）を送信し（Ｓ２７－６）、処理を終了する。

【０１３３】

さらに一方、中継装置２００は、署名認証処理Ｓ１００の結果、受信したメッセージの署名の認証が失敗した場合（Ｓ２７－１のＮｏ）、及び当該ユーザが制御用情報管理テーブルに登録済みでない場合（Ｓ２７－２のＮｏ）、受信したメッセージを破棄し、処理を終了する。

【０１３４】

図１３のシーケンスに戻り、中継装置２００は、通信応答受信処理Ｓ２７において、署名認証処理Ｓ１００を行い、ノード３００－３に署名検証要求を送信し（Ｓ２８、図１２のＳ１００－１）、ノード３００－３から署名検証応答を受信し（Ｓ２９、図１２のＳ１００－２）、受信した通信応答Ｓ２６の署名の認証を行う。中継装置２００は、端末装置１００－２は正当な端末装置１００であると認証し（図１２のＳ１００－４）、認証成功と判定する（図１７のＳ２７－１のＹｅｓ）。そして、中継装置２００は、端末装置１００－２が制御情報管理テーブルに登録されていることを確認し（図１７のＳ２７－２のＹｅｓ）、送信先の端末装置１００－１に通信応答（ＯＫ）を送信する（Ｓ３０、図１７のＳ２７－４）。

【０１３５】

図１４（Ｄ）は、通信応答Ｓ３０の例を示す図である。中継装置２００は、送信元アドレス及び送信先アドレス以外は、受信した通信応答Ｓ２６の内容を載せ替え、通信応答Ｓ３０を端末装置１００－１に送信する。

【０１３６】

図１３のシーケンスに戻り、中継装置２００は、通信用情報管理テーブルを更新し（図１７のＳ２７－５）、通信応答受信処理Ｓ２７を終了する。

【０１３７】

中継装置２００は、通信用情報管理テーブルを、図１６（Ａ）に示す状態（受信側識別子「ｄｅｆ」に対応する送信側識別子「－」）を、図１６（Ｂ）に示す状態のように、受信側識別子「ｄｅｆ」に対応する送信側識別子を、通信応答に含まれる送信先識別子である「ａｂｃ」とする。これにより、端末装置１００－１と端末装置１００－２は、互いにメッセージの送受信を許可した状態となる。

【０１３８】

＜３．通信処理＞

通信処理は、例えば、互いに通信メッセージの送受信を許可している端末装置１００が、通信データを送受信する処理である。なお、通信処理において、端末装置１００－１及び端末装置１００－２が中継装置２００と送受信するメッセージは、通信用メッセージであり、端末装置１００－１が通信ポートＰ１２（通信用ポート）を使用し、端末装置１００－２が通信ポートＰ２２（通信用ポート）を使用して、中継装置２００と送受信を行う。

【０１３９】

図１８は、通信処理のシーケンスの例を示す図である。端末装置１００－１は、端末装置１００－２に、中継装置２００を介して通信データを送信する。

【０１４０】

端末装置１００－１は、端末装置１００－２宛ての通信データを、中継装置２００に送

信する（Ｓ４１）。
【０１４１】
図１９は、ノード３００と、端末装置１００又は中継装置２００との間で送受信されるメッセージの例を示す図である。図１９（Ａ）は、通信データＳ４１の例を示す図である。
【０１４２】
通信データは、送信元アドレス、送信先アドレス、タイプ、メッセージ種別、送信元識別子、送信先識別子、ペイロード、及び署名を含むメッセージである。
【０１４３】
送信元識別子は、通信データの送信元の端末装置１００の識別子が掲載される。通信データＳ４１の場合、送信元識別子は、端末装置１００－１の識別子「ａｂｃ」が掲載される。
【０１４４】
送信先識別子は、通信データの送信先の端末装置１００の識別子が掲載される。通信データＳ４５の場合、送信先識別子は、端末装置１００－２の識別子「ｄｅｆ」が掲載される。
【０１４５】
ペイロードは、通信で送受信されるデータ（ユーザデータ）が含まれる。
【０１４６】
署名は、署名データが掲載される。通信データＳ４１の場合、署名は、端末装置１００－１の秘密鍵Ｓｋａで生成された署名データが掲載される。
【０１４７】
図１８のシーケンスに戻り、中継装置２００は、通信データＳ４１を受信すると、通信データ受信処理を行う（Ｓ４２）。
【０１４８】
図２０は、通信データ受信処理Ｓ４２の処理フローチャートの例を示す図である。中継装置２００は、通信データ受信処理Ｓ４２において、署名認証処理Ｓ１００を行う。中継装置２００は、署名認証処理Ｓ１００の結果、受信したメッセージの署名の認証が成功した場合（Ｓ４２－１のＹｅｓ）、当該ユーザが、通信用情報管理テーブルにおいて、通信許可されたユーザであるか否かを確認する（Ｓ４２－２）。
【０１４９】
中継装置２００は、通信データの送信先識別子が通信用情報管理テーブルの受信側識別子に含まれ、通信データの送信元識別子が通信用情報管理テーブルの送信側識別子に含まれている場合、当該通信データのユーザは、通信が許可されていると判定する。
【０１５０】
中継装置２００は、当該ユーザが通信許可されている場合（Ｓ４２－２のＹｅｓ）、通信データを送信先の端末装置に送信し（Ｓ４２－３）、処理を終了する。一方、中継装置２００は、当該ユーザが通信許可されていない場合（Ｓ４２－２のＮｏ）、また認証が失敗した場合（Ｓ４２－１のＮｏ）、通信データを破棄し、処理を終了する。
【０１５１】
図１８のシーケンスに戻り、中継装置２００は、通信データ受信処理Ｓ４２において、署名認証処理Ｓ１００を行い、ノード３００－３に署名検証要求を送信し（Ｓ４３、図１２のＳ１００－１）、ノード３００－３から署名検証応答を受信し（Ｓ４４、図１２のＳ１００－２）、受信した通信データＳ４１の署名の認証を行う。中継装置２００は、端末装置１００－１は正当な端末装置１００であると認証し（図１２のＳ１００－４）、認証成功と判定する（図２０のＳ４２－１のＹｅｓ）。そして、中継装置２００は、端末装置１００－１が通信情報管理テーブルの送信側識別子に登録され、対応する受信側識別子に端末装置１００－２が登録されていることを確認し（図２０のＳ４２－２のＹｅｓ）、送信先の端末装置１００－２に通信データを送信する（Ｓ４５、図２０のＳ４２－３）。
【０１５２】

図１９（Ｂ）は、通信データＳ４５の例を示す図である。中継装置２００は、送信元アドレス及び送信先アドレス以外は、受信した通信データＳ４１の内容を載せ替え、通信データＳ４５Ｓを端末装置１００－２に送信する。

【０１５３】

第１の実施の形態において、中継装置２００は、通信を行う端末装置間のメッセージの送受信を中継する。中継装置２００は、端末装置１００の登録や通信の中継において、ノード３００の分散台帳から公開鍵を取得し、メッセージの署名の認証を行う。これにより、端末装置間で、署名認証が完了している安全性の高いメッセージを送受信することができる。

【０１５４】

［第２の実施の形態］

次に、第２の実施の形態について説明する。第２の実施の形態における通信システム１０は、通信を不許可にすることを通知又は要求する通信拒否メッセージを装置間で送受信する。第２１の実施の形態では、通信中の通信拒否メッセージ受信時の処理、及び通信応答（ＮＧ）受信時の処理について説明する。

【０１５５】

＜１．通信応答（ＮＧ）時の処理＞

図２１は、端末装置１００－２が通信応答（ＮＧ）を送信する場合のシーケンスの例を示す図である。端末装置１００は、例えば、端末装置１００のユーザの操作や、端末装置１００で起動中のアプリケーションの判定などにより、通信を許可しない通信応答（ＮＧ）を送信する場合がある。

【０１５６】

通信要求Ｓ２１から通信要求Ｓ２５までは、図１３のシーケンスにおける通信要求Ｓ２１から通信要求Ｓ２５と同様である。端末装置１００－２は、端末装置１００－１からの通信要求に対して、通信応答（ＮＧ）を送信する。

【０１５７】

図２２は、ノード３００と、端末装置１００又は中継装置２００との間で送受信されるメッセージの例を示す図である。図２２（Ａ）は、通信応答（ＮＧ）Ｓ５０の例を示す図である。

【０１５８】

通信応答は、送信元アドレス、送信先アドレス、タイプ、メッセージ種別、送信元識別子、送信先識別子、ペイロード、及び署名を含むメッセージである。

【０１５９】

送信元識別子は、通信応答の送信元の端末装置１００の識別子が掲載される。通信応答（ＮＧ）Ｓ５０の場合、送信元識別子は、端末装置１００－２の識別子「ｄｅｆ」が掲載される。

【０１６０】

送信先識別子は、通信応答の送信先の端末装置１００の識別子が掲載される。通信応答（ＮＧ）Ｓ５０の場合、送信先識別子は、端末装置１００－１の識別子「ａｂｃ」が掲載される。

【０１６１】

通信許可は、通信を許可するか否か（通信メッセージの受信を許可するか否か）を示す情報である。通信応答Ｓ５０の場合、通信許可は、端末装置１００－２が端末装置１００－１からの通信メッセージの受信を許可しない「ＮＧ」が掲載される。

【０１６２】

署名は、署名データが掲載される。通信応答Ｓ５０の場合、署名は、端末装置１００－２の秘密鍵Ｓｋｄで生成された署名データが掲載される。

【０１６３】

図２１のシーケンスに戻り、中継装置２００は、通信応答（ＮＧ）Ｓ５０を受信すると、通信応答受信処理Ｓ２７を行う。中継装置２００は、通信応答受信処理Ｓ２７において

、署名認証処理Ｓ１００を行い、ノード３００－３に署名検証要求を送信し（Ｓ５１、図１２のＳ１００－１）、ノード３００－３から署名検証応答を受信し（Ｓ５２、図１２のＳ１００－２）、受信した通信応答（ＮＧ）Ｓ５０の署名の認証を行う。中継装置２００は、端末装置１００－２は正当な端末装置１００であると認証し（図１２のＳ１００－４）、認証成功と判定する（図１７のＳ２７－１のＹｅｓ）。そして、中継装置２００は、端末装置１００－２が制御情報管理テーブルに登録されていることを確認する（図１７のＳ２７－２のＹｅｓ）。そして、中継装置２００は、通信応答（ＮＧ）Ｓ５０の通信許可がＮＧであるため（図１７のＳ２７－３）、送信先の端末装置１００－１に通信応答（ＮＧ）を送信する（Ｓ５３、図１７のＳ２７－４）。図２２（Ｂ）は、通信応答Ｓ５３の例を示す図である。送信元アドレス、送信先アドレス以外は、図２２（Ａ）に示す通信応答Ｓ５０と同様である。

【０１６４】

端末装置１００－１は、通信応答（ＮＧ）Ｓ５３を受信すると、自装置の通信要求を、相手装置（端末装置１００－２）が拒否したこと（相手装置が自装置からの通信メッセージの受信を拒否したこと）を認識する。端末装置１００－１は、例えば、自装置が通信を拒否された場合、自装置も、相手装置からの通信メッセージの受信を拒否する。そして、端末装置１００－１は、自装置が通信メッセージの受信を拒否することを意味する通信拒否を、中継装置２００を介して端末装置１００－２に送信する（Ｓ５４）。

【０１６５】

図２３は、ノード３００と、端末装置１００又は中継装置２００との間で送受信されるメッセージの例を示す図である。図２３（Ａ）は、通信拒否Ｓ５４の例を示す図である。

【０１６６】

通信拒否は、送信元アドレス、送信先アドレス、タイプ、メッセージ種別、送信元識別子、送信先識別子、及び署名を含むメッセージである。

【０１６７】

送信元識別子は、通信拒否の送信元の端末装置１００の識別子が掲載される。通信拒否Ｓ５４の場合、送信元識別子は、端末装置１００－１の識別子「ａｂｃ」が掲載される。

【０１６８】

送信先識別子は、通信拒否の送信先の端末装置１００の識別子が掲載される。通信拒否Ｓ５４の場合、送信先識別子は、端末装置１００－２の識別子「ｄｅｆ」が掲載される。

【０１６９】

署名は、署名データが掲載される。通信拒否Ｓ５４の場合、署名は、端末装置１００－１の秘密鍵Ｓｋａで生成された署名データが掲載される。

【０１７０】

図２１のシーケンスに戻り、中継装置２００は、通信拒否Ｓ５４を受信すると、通信拒否受信処理を行う（Ｓ２００）。

【０１７１】

図２４は、通信拒否受信処理Ｓ２００の処理フローチャートの例を示す図である。中継装置２００は、通信拒否受信処理Ｓ２００において、署名認証処理Ｓ１００を行う。中継装置２００は、署名認証処理Ｓ１００の結果、受信したメッセージの署名の認証が成功した場合（Ｓ２００－１のＹｅｓ）、通信用情報管理テーブルを更新し（Ｓ２００－２）、通信拒否を送信先の端末装置１００に送信し（Ｓ２００－３）、処理を終了する。

【０１７２】

中継装置２００は、処理Ｓ２００－３において、通信拒否の送信元の端末装置１００の識別子が記憶された受信側識別子に対応する送信側識別子を、なしの状態（「－」）に更新する。通信用情報管理テーブルを上述のように更新することで、通信拒否を送信した端末装置１００は、送信先の端末装置１００からの通信用メッセージの受信を許可しない状態となる。

【０１７３】

一方、中継装置２００は、認証が失敗した場合（Ｓ２００－１のＮｏ）、通信拒否を破

棄し、処理を終了する。
【０１７４】
図２１のシーケンスに戻り、中継装置２００は、通信拒否信処理Ｓ２００において、署名認証処理Ｓ１００を行い、ノード３００－３に署名検証要求を送信し（Ｓ５５、図１２のＳ１００－１）、ノード３００－３から署名検証応答を受信し（Ｓ５６、図１２のＳ１００－２）、受信した通信拒否Ｓ５４の署名の認証を行う。中継装置２００は、端末装置１００－１は正当な端末装置１００であると認証し（図１２のＳ１００－４）、認証成功と判定する（図２４のＳ２００－１のＹｅｓ）。そして、中継装置２００は、通信用情報管理テーブルを更新し（図２４のＳ２００－２）、送信先の端末装置１００－２に通信拒否を送信する（Ｓ５７、図２４のＳ２００－３）。
【０１７５】
図２５は、通信用情報管理テーブルの例を示す図である。図２５（Ａ）は、通信要求Ｓ２１受信時の通信用情報管理テーブルの例を示す図である。中継装置２００は、通信用情報管理テーブルを、図２５（Ａ）に示す状態（受信側識別子「ａｂｃ」に対応する送信側識別子「ｄｅｆ」）を、図２５（Ｂ）に示す状態のように、受信側識別子「ａｂｃ」に対応する送信側識別子を、通信拒否の送信先識別子である「ｄｅｆ」を削除した状態「－」に更新する。これにより、端末装置１００－１は、端末装置１００－２からの通信メッセージを受信しない状態となり、互いにメッセージの送受信を許可しない状態となる。
【０１７６】
＜２．通信中の通信拒否受信時の処理＞
図２６は、通信中に端末装置１００－１が通信拒否を送信する場合のシーケンスの例を示す図である。端末装置１００は、例えば、通信を終了するとき、通信拒否を送信する場合がある。
【０１７７】
端末装置１００－１は、通信拒否を中継装置２００に送信する（Ｓ６１）。中継装置２００は、通信拒否を受信すると、通信拒否受信処理Ｓ２００を行う。
【０１７８】
中継装置２００は、通信拒否信処理Ｓ２００において、署名認証処理Ｓ１００を行い、ノード３００－３に署名検証要求を送信し（Ｓ６２、図１２のＳ１００－１）、ノード３００－３から署名検証応答を受信し（Ｓ６３、図１２のＳ１００－２）、受信した通信拒否Ｓ６１の署名の認証を行う。中継装置２００は、端末装置１００－１は正当な端末装置１００であると認証し（図１２のＳ１００－４）、認証成功と判定する（図２４のＳ２００－１のＹｅｓ）。そして、中継装置２００は、通信用情報管理テーブルを更新し（図２４のＳ２００－２）、送信先の端末装置１００－２に通信拒否を送信する（Ｓ６４、図２４のＳ２００－３）。
【０１７９】
図２７は、通信用情報管理テーブルの例を示す図である。図２７（Ａ）は、通信中の通信用情報管理テーブルの例を示す図である。中継装置２００は、通信用情報管理テーブルを、図２７（Ａ）に示す状態（受信側識別子「ａｂｃ」に対応する送信側識別子「ｄｅｆ」）を、図２７（Ｂ）に示す状態のように、受信側識別子「ａｂｃ」に対応する送信側識別子を、通信拒否の送信先識別子である「ｄｅｆ」を削除した状態「－」に更新する。これにより、端末装置１００－１は、端末装置１００－２からの通信メッセージを受信しない状態となる。
【０１８０】
図２６のシーケンスに戻り、端末装置１００－２は、端末装置１００－１からの通信拒否Ｓ６４を受信すると、端末装置１００－１が以降の通信メッセージの受信を拒否したことを認識する。そして、端末装置１００－２は、自装置も端末装置１００－１からの通信メッセージの受信を拒否することを通知するため、端末装置１００－１宛ての通信拒否を中継装置２００に送信する（Ｓ６５）。
【０１８１】

中継装置２００は、通信拒否Ｓ６５を受信すると、通信拒否受信処理Ｓ２００を行う。中継装置２００は、通信拒否信処理Ｓ２００において、署名認証処理Ｓ１００を行い、ノード３００－３に署名検証要求を送信し（Ｓ６６、図１２のＳ１００－１）、ノード３００－３から署名検証応答を受信し（Ｓ６７、図１２のＳ１００－２）、受信した通信拒否Ｓ６５の署名の認証を行う。中継装置２００は、端末装置１００－２は正当な端末装置１００であると認証し（図１２のＳ１００－４）、認証成功と判定する（図２４のＳ２００－１のＹｅｓ）。そして、中継装置２００は、通信用情報管理テーブルを更新し（図２４のＳ２００－２）、送信先の端末装置１００－１に通信拒否を送信する（Ｓ６８、図２４のＳ２００－３）。

【０１８２】

中継装置２００は、通信用情報管理テーブルを、図２７（Ｂ）に示す状態（受信側識別子「ｄｅｆ」に対応する送信側識別子「ａｂｃ」）を、図２７（Ｃ）に示す状態のように、受信側識別子「ｄｅｆ」に対応する送信側識別子を、通信拒否の送信先識別子である「ａｂｃ」を削除した状態「－」に更新する。これにより、端末装置１００－２は、端末装置１００－１からの通信メッセージを受信しない状態となる。すなわち、端末装置１００－１及び２は、互いの通信メッセージを受信しない、通信拒否の状態となる。

【０１８３】

第２の実施の形態において、中継装置２００は、通信拒否を受信することで、通信用情報管理テーブルを更新し、通信メッセージの送受信を拒否する。中継装置２００は、端末装置１００－１から通信拒否を受信した場合は端末装置１００－１に対する通信メッセージの送信を拒否する状態とするが、逆方向の端末装置１００－２に対する通信メッセージの送信は許可した状態のままとする。そして、中継装置２００は、端末装置１００－２から通信拒否を受信し、端末装置１００－２に対する通信メッセージの送信を拒否する状態とすることで、互いに通信できない状態とする。また、第１の実施の形態では、通信応答受信時に、送信元の装置の受信許可をしている。中継装置２００は、署名の認証で正当性が確保されるのは送信元装置のみであり、送信先装置は正当化否かわからないため、送信元の端末装置の受信許可か否かの状態だけを更新することで、他の端末装置（例えば、悪意ある第三者）からの通信拒否メッセージによりテーブルを更新されることを抑制する。

【０１８４】

［その他の実施の形態］

端末装置１００は、互いの通信においてのみ共通鍵を使用する場合がある。通信要求メッセージは、共通鍵を含んでもよい。例えば、端末装置１００－１が生成した共通鍵を、端末装置１００－１が端末装置１００－２と通信を開始するときに送信する通信要求メッセージに含め、端末装置１００－２に送信する。これにより、端末装置１００－１，２は、中継装置２００で署名認証されたメッセージを使用して、共通鍵を共有することができる。

【０１８５】

また、第２の実施の形態において、端末装置１００は、通信拒否メッセージを受信すると、自装置も通信拒否メッセージを相手装置に送信する。しかし、例えば、一方向の通信を許容する場合、端末装置１００は、受信した通信拒否メッセージに対応した通信拒否メッセージを返信しなくてもよい。

【０１８６】

さらに、端末装置１００が３台以上存在する場合、三者間以上での通信についても同様の処理で実現可能である。

【０１８７】

以上まとめると、付記のようになる。

【０１８８】

（付記１）

通信装置の識別子と、前記通信装置が通信に使用する公開鍵を分散台帳に記憶し、前記分散台帳を共有する分散台帳機能を有する複数のノードと、前記ノードのいずれかに接続

する前記通信装置と、前記ノードのいずれかに接続する中継装置とを有する通信システムにおける前記中継装置のコンピュータに実行させる通信中継プログラムであって、
前記通信装置とメッセージを送受信する送受信処理と、
前記ノードから前記メッセージの送信元の通信装置の公開鍵を取得し、前記取得した公開鍵で前記メッセージに含まれる署名を認証する認証処理と、
第１通信装置が第２通信装置に送信する通信データを含む通信メッセージを受信したとき、前記通信メッセージに対して前記認証処理を実行し、前記認証が成功した場合、前記通信メッセージを前記第２通信装置に送信する中継処理と、
を実行させる通信中継プログラム。
【０１８９】
（付記２）
さらに、前記第１通信装置が前記第２通信装置と通信を開始するとき送信されるメッセージであって、前記第２通信装置に通信の許可を要求する通信要求メッセージを受信したとき、前記認証処理を実行し、前記認証が成功したとき、前記第２通信装置に前記通信要求メッセージを送信する要求受信処理と、
前記通信要求メッセージに対する応答である通信応答メッセージを前記第２通信装置から受信したとき、前記認証を行い、前記認証が成功したとき、前記第１通信装置に前記通信応答メッセージを送信する応答受信処理と、
を実行させる付記１記載の通信中継プログラム。
【０１９０】
（付記３）
前記中継装置は、前記通信装置が前記通信メッセージの受信を許可するか否かの受信許可状態を管理する通信管理テーブルを有し、
前記要求受信処理において、前記認証が成功したとき、前記第１通信装置が前記第２通信装置から送信される前記通信メッセージの受信を許可する状態に前記通信管理テーブルを更新する
付記２記載の通信中継プログラム。
【０１９１】
（付記４）
前記通信応答メッセージは、前記通信を許可するか否かを示す許可情報を含み、
前記応答受信処理において、前記認証が成功し、前記許可情報が前記通信を許可することを示す場合、前記第２通信装置が前記第１通信装置から送信される前記通信メッセージの受信を許可する状態に前記通信管理テーブルを更新する
付記３記載の通信中継プログラム。
【０１９２】
（付記５）
前記中継装置は、前記通信装置の識別子を登録する制御管理テーブルを有し、
さらに、前記通信装置が前記通信システムに参加したときに送信するメッセージであって、前記通信装置の識別子を含む登録要求メッセージを受信したとき、前記認証処理を実行し、前記認証が成功したとき、前記通信装置の識別子を前記制御管理テーブルに登録する登録処理と、
を実行させる付記１記載の通信中継プログラム。
【０１９３】
（付記６）
前記制御管理テーブルは、さらに、前記通信装置が前記通信メッセージ以外の制御メッセージを送受信するネットワークアドレス又は通信ポート又はその両方を記憶し、
前記登録要求メッセージは、前記ネットワークアドレス又は通信ポート又はその両方を含み、
前記登録処理において、前記通信装置の識別子を前記制御管理テーブルに登録する場合、前記ネットワークアドレス又は通信ポート又はその両方を前記制御管理テーブルに登録

する
付記５記載の通信中継プログラム。
【０１９４】
（付記７）
さらに、前記第１通信装置から前記第２通信装置に送信されるメッセージであって、前記第２通信装置から送信される前記通信メッセージの受信を拒否することを通知する拒否メッセージを受信したとき、前記認証処理を実行し、前記認証が成功した場合、前記第１通信装置が前記第２通信装置から送信される前記通信メッセージの受信を許可しない状態に前記通信管理テーブルを更新し、前記拒否メッセージを前記第２通信装置に送信する拒否受信処理と、
を実行させる付記４記載の通信中継プログラム。
【０１９５】
（付記８）
前記通信要求メッセージは、前記第１通信装置と前記第２通信装置間の通信で使用し、前記第１通信装置と前記第２通信装置間の通信以外の通信で使用しない共通鍵を含む、
付記２記載の通信中継プログラム。
【０１９６】
（付記９）
さらに、前記認証処理において、認証に失敗した場合、受信したメッセージを破棄する破棄処理と、
を実行させる付記１乃至８記載のいずれか１項記載の通信中継プログラム。
【０１９７】
（付記１０）
通信装置の識別子と、前記通信装置が通信に使用する公開鍵を分散台帳に記憶し、前記分散台帳を共有する分散台帳機能を有する複数のノードと、前記ノードのいずれかに接続する前記通信装置と、前記ノードのいずれかに接続する中継装置とを有する通信システムにおける前記中継装置であって、
前記通信装置とメッセージを送受信する送受信部と、
前記ノードから前記メッセージの送信元の通信装置の公開鍵を取得し、前記取得した公開鍵で前記メッセージに含まれる署名を認証する認証部と、
第１通信装置が第２通信装置に送信する通信データを含む通信メッセージを受信したとき、前記通信メッセージに対する認証を前記認証部に実行させ、前記認証が成功した場合、前記通信メッセージを前記第２通信装置に送信する中継部と、
を有する中継装置。
【０１９８】
（付記１１）
通信装置の識別子と、前記通信装置が通信に使用する公開鍵を分散台帳に記憶し、前記分散台帳を共有する分散台帳機能を有する複数のノードと、前記ノードのいずれかに接続する前記通信装置と、前記ノードのいずれかに接続する中継装置とを有する通信システムにおける前記中継装置における中継方法であって、
前記通信装置とメッセージを送受信する送受信工程と、
前記ノードから前記メッセージの送信元の通信装置の公開鍵を取得し、前記取得した公開鍵で前記メッセージに含まれる署名を認証する認証工程と、
第１通信装置が第２通信装置に送信する通信データを含む通信メッセージを受信したとき、前記通信メッセージに対して前記認証工程を実行し、前記認証が成功した場合、前記通信メッセージを前記第２通信装置に送信する中継工程と、
を有する通信中継方法。
【０１９９】
（付記１２）
通信装置の識別子と、前記通信装置が通信に使用する公開鍵を分散台帳に記憶し、前記

分散台帳を共有する分散台帳機能を有する複数のノードと、前記ノードのいずれかに接続する通信装置と、前記ノードのいずれかに接続する中継装置とを有する通信システムであって、

前記通信装置は、他の通信装置と通信するとき、前記他の通信装置宛ての通信データを含む通信メッセージを、前記中継装置に送信し、

前記中継装置は、前記通信装置から前記通信メッセージを受信したとき、前記ノードから前記通信装置の公開鍵を取得し、前記取得した公開鍵で前記受信した通信メッセージに含まれる署名を認証し、前記認証に成功した場合、前記通信メッセージを前記他の通信装置に送信する

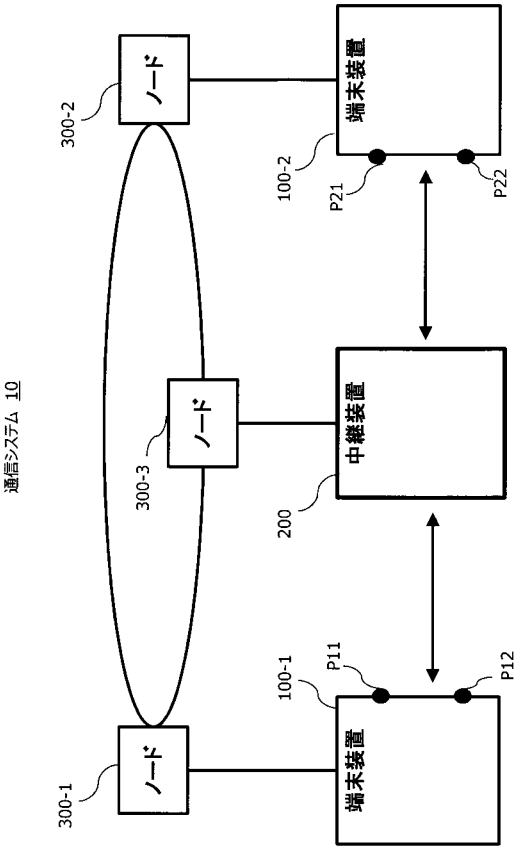
通信システム。

【符号の説明】

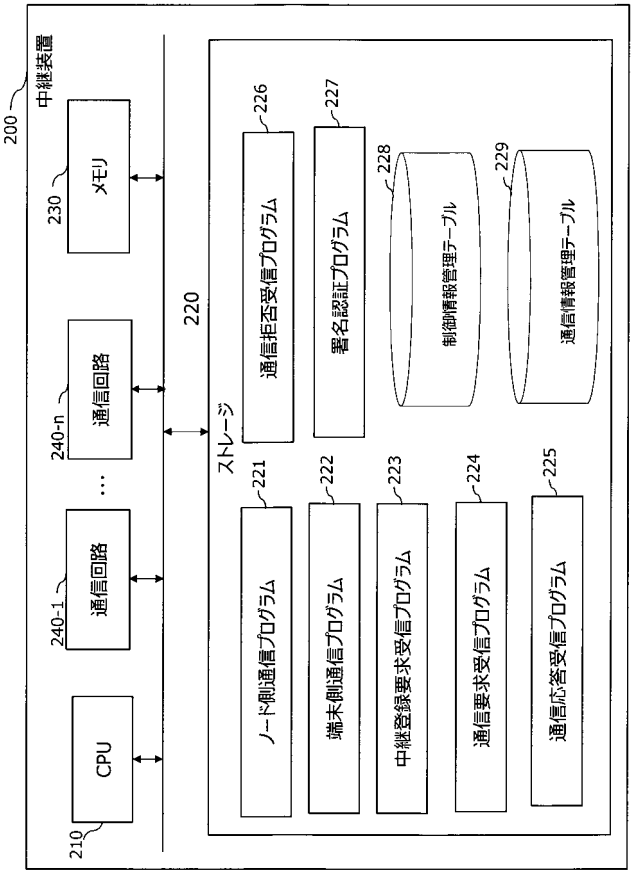
【０２００】

１０　：通信システム
１００　：端末装置
１１０　：ＣＰＵ
１２０　：ストレージ
１２１　：ノード側通信プログラム
１２２　：分散台帳登録プログラム
１２３　：通信開始プログラム
１２４　：通信プログラム
１２５　：通信拒否プログラム
１３０　：メモリ
１４０　：通信回路
２００　：中継装置
２１０　：ＣＰＵ
２２０　：ストレージ
２２１　：ノード側通信プログラム
２２２　：端末側通信プログラム
２２３　：中継登録要求受信プログラム
２２４　：通信要求受信プログラム
２２５　：通信応答受信プログラム
２２６　：通信拒否受信プログラム
２２７　：署名認証プログラム
２２８　：制御情報管理テーブル
２２９　：通信情報管理テーブル
２３０　：メモリ
２４０　：通信回路
３００　：ノード
３１０　：ＣＰＵ
３２０　：ストレージ
３２１　：分散台帳プログラム
３２２　：中継装置側通信プログラム
３２３　：分散台帳
３３０　：メモリ
３４０　：通信回路

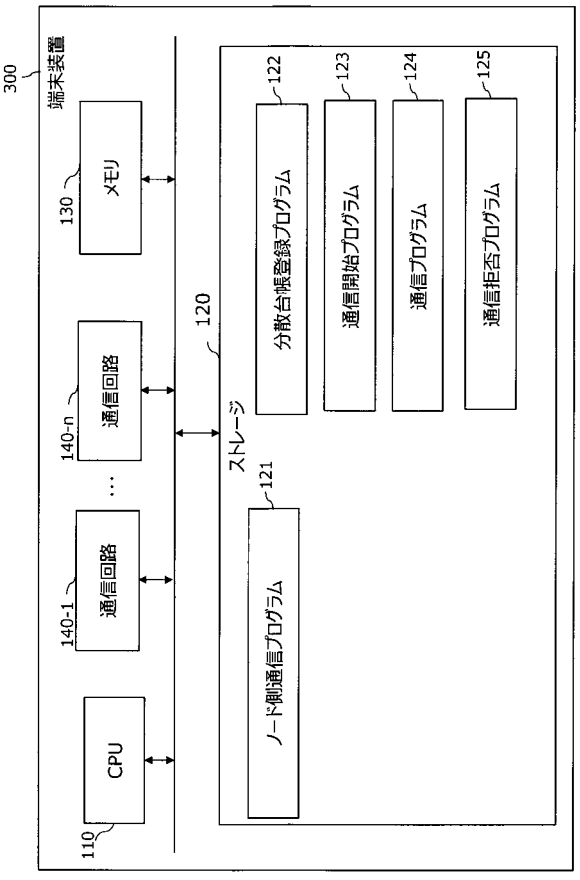
【図１】


通信システム 10
ノード
300-1
300-2
300-3
端末装置
中継装置
100-1
100-2
200
P11
P12
P21
P22

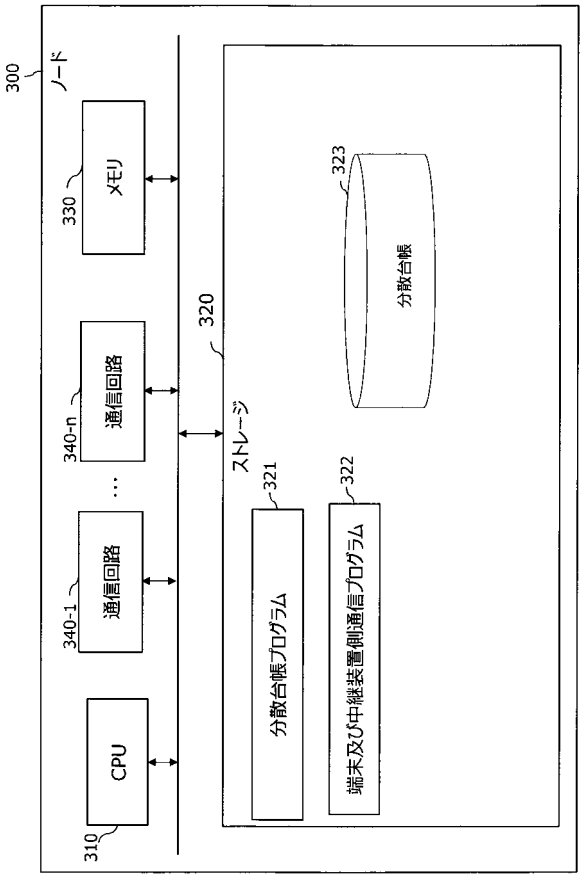
【図２】


中継装置
200
CPU
210
メモリ
230
通信回路
240-1
240-n
220
ストレージ
ノード側通信プログラム
221
端末側通信プログラム
222
中継登録要求受信プログラム
223
通信要求受信プログラム
224
通信応答受信プログラム
225
通信拒否受信プログラム
226
署名認証プログラム
227
制御情報管理テーブル
228
通信情報管理テーブル
229

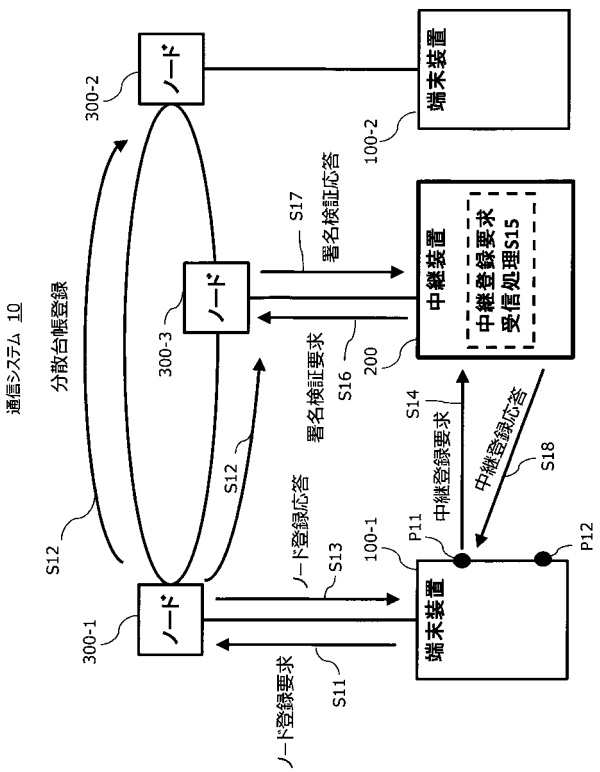
【図３】


端末装置
300
CPU
110
メモリ
130
通信回路
140-1
140-n
120
ストレージ
ノード側通信プログラム
121
分散台帳登録プログラム
122
通信開始プログラム
123
通信プログラム
124
通信拒否プログラム
125

【図４】


ノード
300
CPU
310
メモリ
330
通信回路
340-1
340-n
320
ストレージ
分散台帳プログラム
321
端末及び中継装置側通信プログラム
322
分散台帳
323

【図５】



【図６】

各装置の情報

装置	アドレス	識別子	公開鍵	秘密鍵
中継装置200	IP3	xyz	–	–
端末装置100－1	IP1	abc	Pka	Ska
端末装置100－2	IP2	def	Pkd	Skd
ノード300－1	IPN1	–	–	–
ノード300－2	IPN2	–	–	–
ノード300－3	IPN3	–	–	–

【図７】

ノード登録要求 S11

(A)

送信元アドレス	送信先アドレス	メッセージ種別	送信元識別子	公開鍵
IP1	IPN1	ノード登録要求	abc	Pka

ノード登録応答 S13

(B)

送信元アドレス	送信先アドレス	メッセージ種別	中継装置識別子	中継装置アドレス
IPN1	IP1	ノード登録応答	xyz	IP3

署名検証要求 S16

(C)

送信元アドレス	送信先アドレス	メッセージ種別	識別子
IP3	IPN3	署名検証要求	abc

署名検証応答 S17

(D)

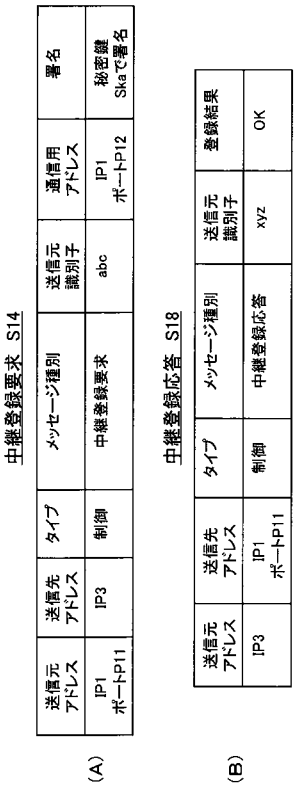
送信元アドレス	送信先アドレス	メッセージ種別	識別子検索結果	公開鍵
IPN3	IP3	署名検証応答	OK	Pka

【図８】

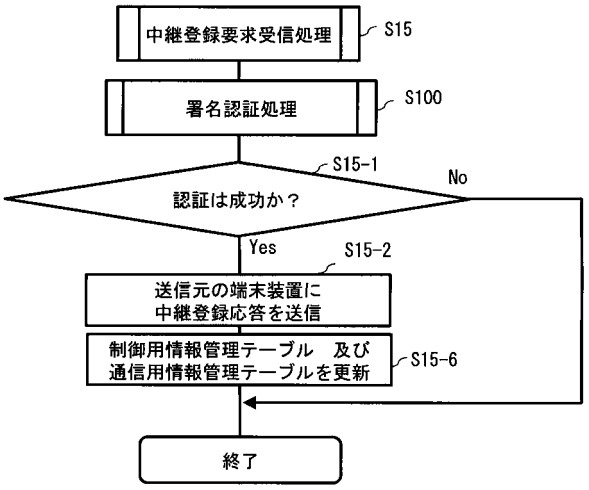
分散台帳テーブル

装置	アドレス	識別子	公開鍵
中継装置200	IP3	xyz	–
端末装置100－1	–	abc	Pka
端末装置100－2	–	def	Pkd

【図９】



【図１０】



【図１１】

制御用情報管理テーブル

(A)

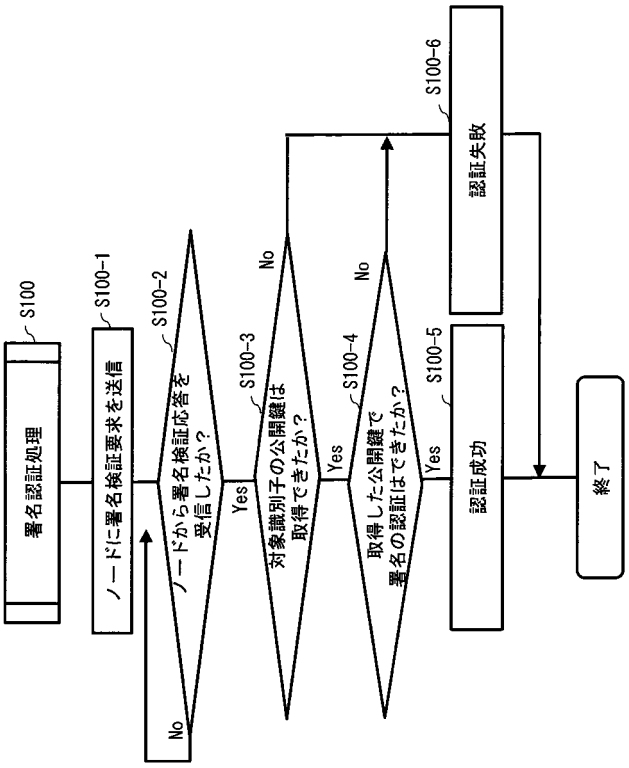
識別子	制御用アドレス
abc	IP1 ポートP11
def	IP2 ポートP21

通信用情報管理テーブル

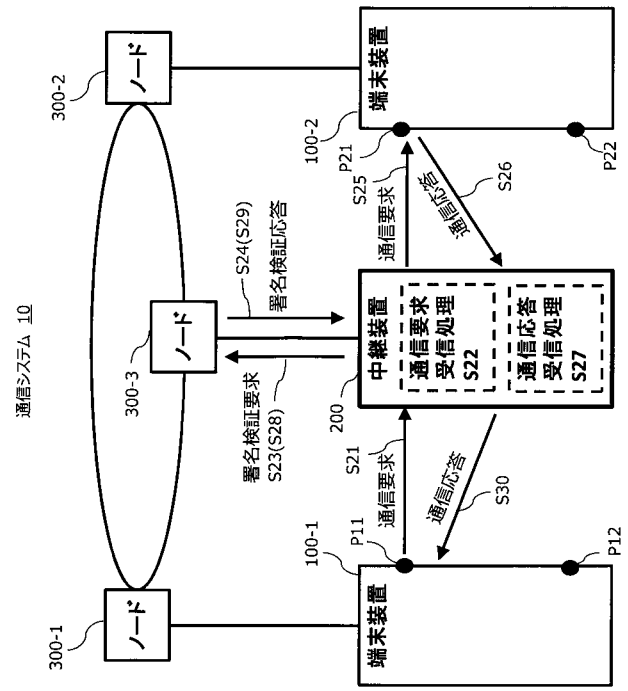
(B)

受信側識別子	送信側識別子	受信側通信用アドレス
abc	-	IP1 ポート12
def	-	IP2 ポート22

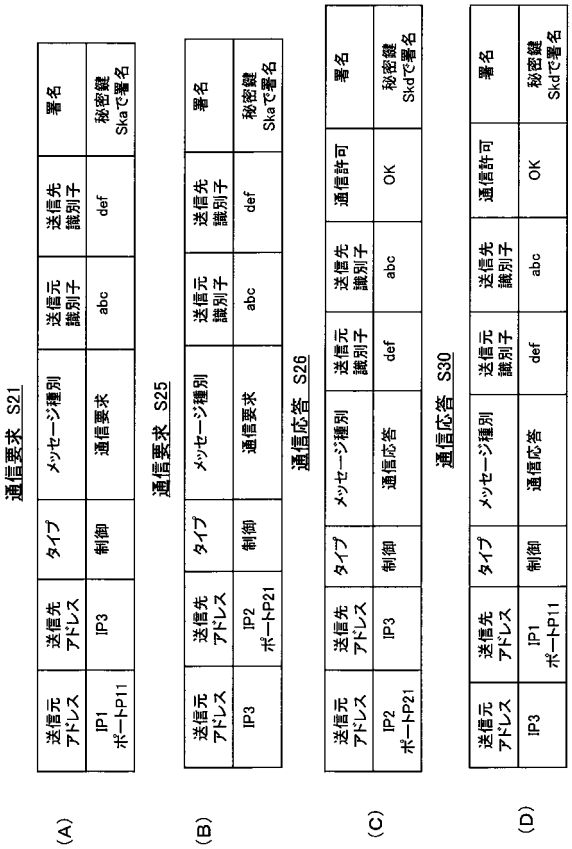
【図１２】



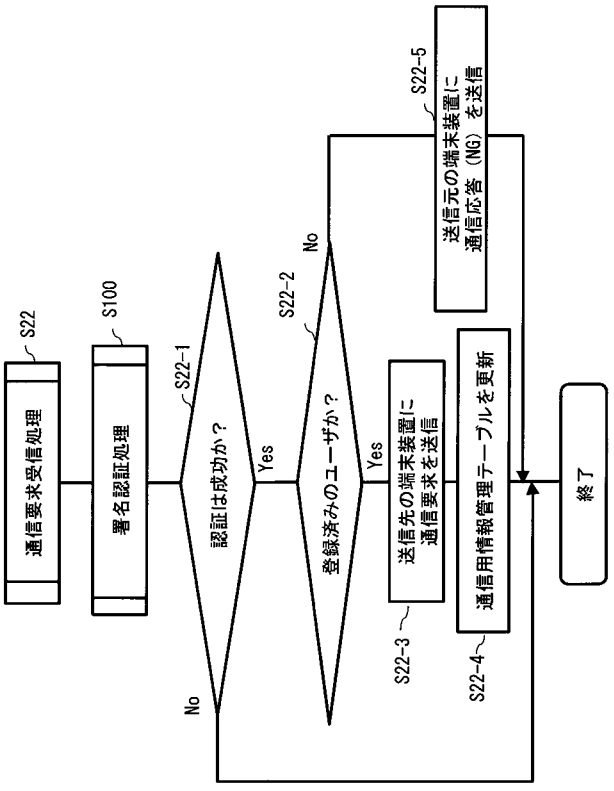
【図１３】



【図１４】



【図１５】



【図１６】

(A)

通信用情報管理テーブル

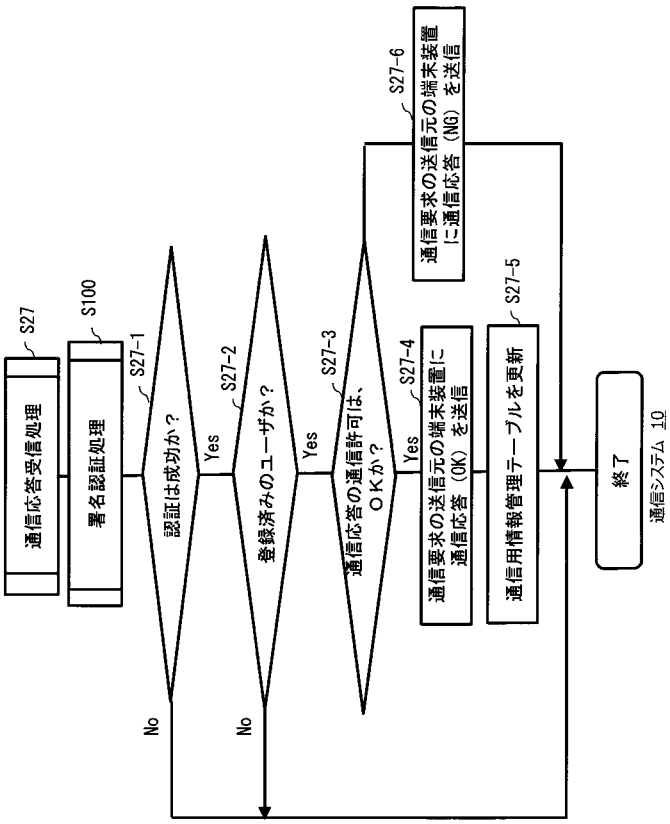
受信側識別子	送信側識別子	受信側通信用アドレス
abc	def	IP1 ポート12
def	-	IP2 ポート22

(B)

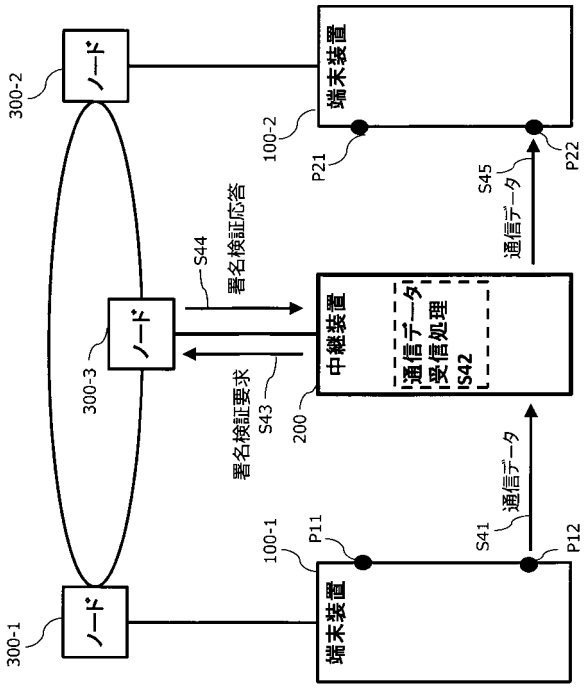
通信用情報管理テーブル

受信側識別子	送信側識別子	受信側通信用アドレス
abc	def	IP1 ポート12
def	abc	IP2 ポート22

【図１７】



【図１８】



【図１９】

(A)

通信データ S41

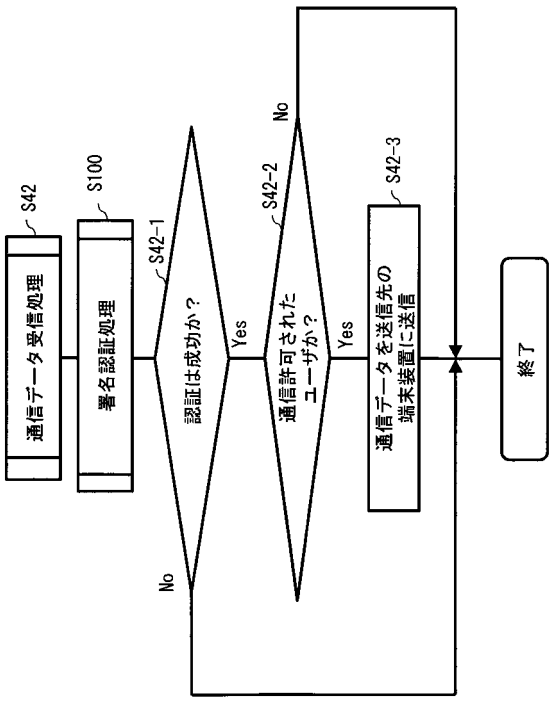
送信元アドレス	送信先アドレス	タイプ	メッセージ種別	送信元識別子	送信先識別子	ペイロード	署名
IP1 ポート-P12	IP3	通信	通信データ	abc	def	データ	秘密鍵 Skaで署名

(B)

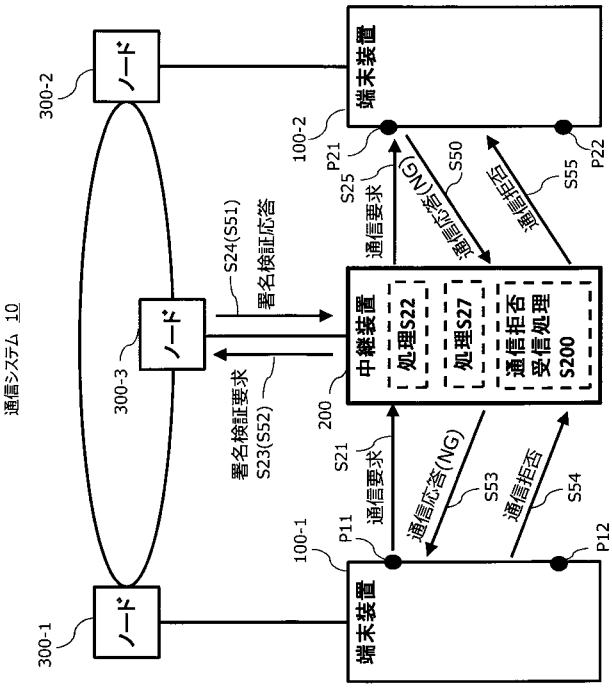
通信データ S45

送信元アドレス	送信先アドレス	タイプ	メッセージ種別	送信元識別子	送信先識別子	ペイロード	署名
IP3	IP2 ポート-22	通信	通信データ	abc	def	データ	秘密鍵 Skaで署名

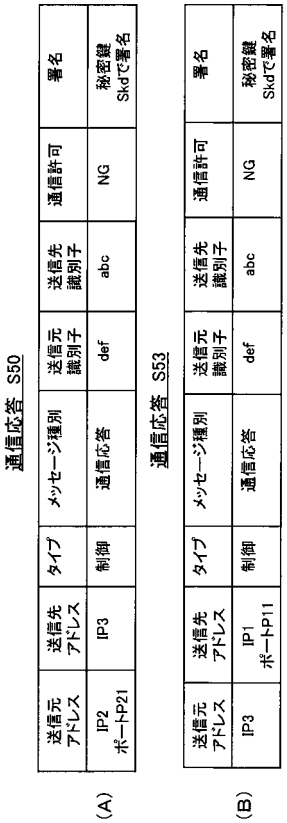
【図２０】



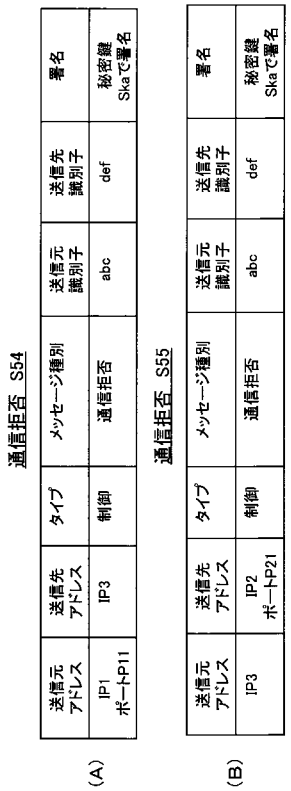
【図２１】



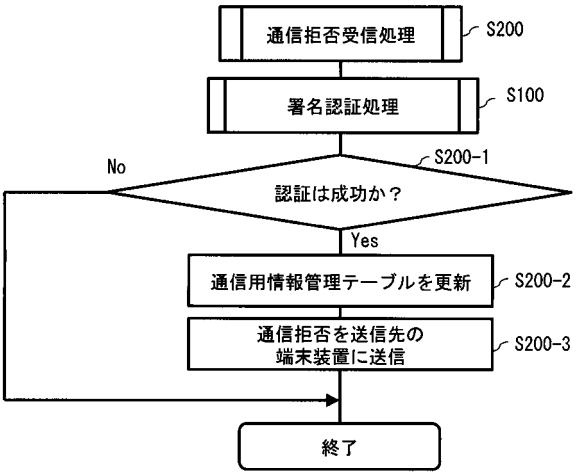
【図２２】



【図２３】



【図２４】



【図２５】

通信用情報管理テーブル

(A)

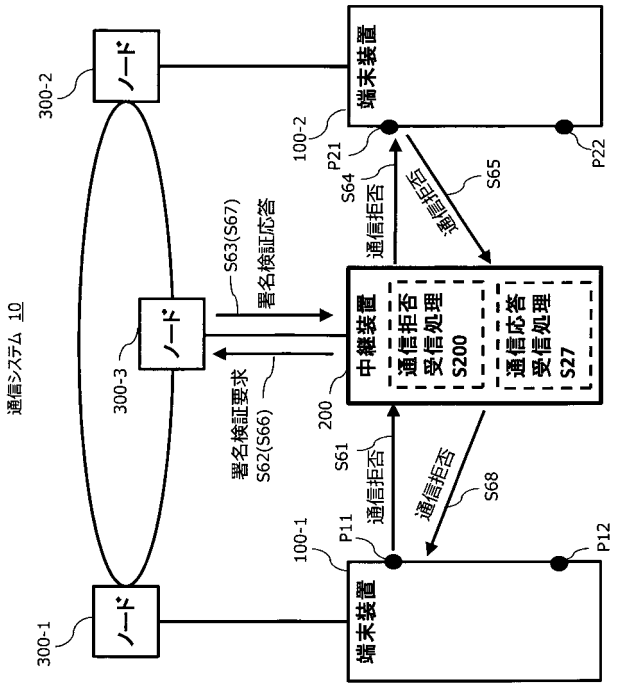
受信側識別子	送信側識別子	受信側通信用アドレス
abc	def	IP1 ポート12
def	-	IP2 ポート22

通信用情報管理テーブル

(B)

受信側識別子	送信側識別子	受信側通信用アドレス
abc	-	IP1 ポート12
def	-	IP2 ポート22

【図２６】



【図２７】

通信用情報管理テーブル

(A)

受信側識別子	送信側識別子	受信側通信用アドレス
abc	def	IP1 ポート12
def	abc	IP2 ポート22

通信用情報管理テーブル

(B)

受信側識別子	送信側識別子	受信側通信用アドレス
abc	-	IP1 ポート12
def	abc	IP2 ポート22

通信用情報管理テーブル

(C)

受信側識別子	送信側識別子	受信側通信用アドレス
abc	-	IP1 ポート12
def	-	IP2 ポート22