(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2021-36645
(P2021-36645A)
(43)公開日　令和3年3月4日(2021.3.4)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 12/08	(2021.01)	H04W	12/08		5E555
H04W 84/18	(2009.01)	H04W	84/18		5K067
G06F 21/44	(2013.01)	G06F	21/44		
G06F 3/01	(2006.01)	G06F	3/01	570	

審査請求 未請求　請求項の数 10　ＯＬ　（全 18 頁）

(21)出願番号　特願2019-158004 (P2019-158004)
(22)出願日　令和1年8月30日 (2019.8.30)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100080816
弁理士　加藤　朝道
(74)代理人　100098648
弁理士　内田　潔人
(72)発明者　中石　浩志
東京都港区芝五丁目７番１号　日本電気株式会社内

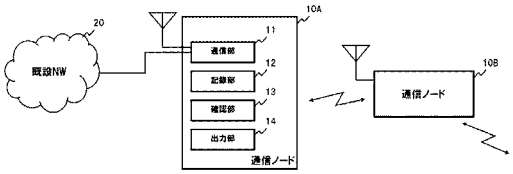
Ｆターム(参考)　5E555 AA53 BA01 BA04 BA45 BB04 BC03 BC16 BE17 CA42 CB66 CB74 DA08 DA09 DA23 DB41 DB57 DC09 EA03 EA05 EA08 EA14 EA25 FA00

最終頁に続く

(54)【発明の名称】通信ノード、マルチホップネットワーク、機器の正当性確認方法及びプログラム

(57)【要約】

【課題】マルチホップネットワークを利用する情報システムのセキュリティの向上。
【解決手段】通信ノードは、マルチホップネットワークを介して通信する機器間のデータをマルチホップ方式で中継する通信部と、前記中継したデータのうち、所定の種類のデータを記録する記録部と、前記所定の種類のデータと、前記記録部に記録された過去のデータとを照合し、前記機器の正当性を確認する確認部と、所定の出力先に対し、前記機器の正当性の確認結果を出力する出力部と、を備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
マルチホップネットワークを介して通信する機器間のデータをマルチホップ方式で中継する通信部と、
前記中継したデータのうち、所定の種類のデータを記録する記録部と、
前記所定の種類のデータと、前記記録部に記録された過去のデータとを照合し、前記機器の正当性を確認する確認部と、
所定の出力先に対し、前記機器の正当性の確認結果を出力する出力部と、
を備えた通信ノード。
【請求項２】
前記所定の種類のデータは、一方の機器から他方の機器に送信する機器操作用のジェスチャーデータである請求項１の通信ノード。
【請求項３】
前記確認部は、前記機器操作用のジェスチャーデータに表れたジェスチャの特徴に有意な差異がある場合に、なりすましが行われていると判定する請求項２の通信ノード。
【請求項４】
前記所定の種類のデータは、一方の機器から他方の機器に送信する作業指示用のデータである請求項１から３いずれか一の通信ノード。
【請求項５】
前記確認部は、前記作業指示用のデータに表れた作業指示に有意な差異がある場合に、なりすましが行われていると判定する請求項４の通信ノード。
【請求項６】
前記記録部は、さらに、前記所定の種類のデータの転送経路情報を記録し、
前記確認部は、さらに、前記データの転送経路を確認することにより、前記データの送信元の機器の正当性を確認する、
請求項１から５いずれか一の通信ノード。
【請求項７】
他の通信ノードから前記機器の正当性の確認結果を受け取り、
前記確認部は、前記他の通信ノードにおける前記機器の正当性の確認結果も用いて、前記機器の正当性を確認する
請求項１から６いずれか一の通信ノード。
【請求項８】
請求項１から６いずれか一の通信ノードを含んで構成されたマルチホップネットワーク。
【請求項９】
前記通信ノードの位置に応じて、前記確認部における前記機器の正当性の確認方法を変更可能である請求項８のマルチホップネットワーク。
【請求項１０】
マルチホップネットワークを介して通信する機器間のデータをマルチホップ方式で中継する通信ノードが、
前記中継したデータのうち、所定の種類のデータを記録し、
前記所定の種類のデータと、記録した過去のデータとを照合し、前記機器の正当性を確認し、
所定の出力先に対し、前記機器の正当性の確認結果を出力する、
機器の正当性確認方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信ノード、マルチホップネットワーク、機器の正当性確認方法及びプログラムに関する。

【背景技術】
【０００２】
無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）のアクセスポイントの電波が届かず、また、無線通信網のサービスを受けられない場所においても、ネットワークを利用したいという需要がある。こうしたケースでは、マルチホップ機能を備えた無線ＬＡＮアクセスポイント（いわゆる「親機」）を用いることで、既存ＬＡＮに接続可能な範囲を拡張できる。
【０００３】
特許文献１に、ＭＡＣ（Media Access Control）アドレスまたは識別アドレスを偽装した不正な通信端末によるなりすましを防止する事ができるという無線中継システムが開示されている。同文献には、マルチホップ式に中継する複数の無線中継装置３と、無線中継装置３に接続された通信端末２と、通信端末２が指定する通信先である買い物サーバ７との間で通信データを中継するゲートウェイ装置１とからなる無線中継システムが開示されている。そして、無線中継装置３は、通信端末２から送信した代行認証要求コマンドを受信すると、ゲートウェイ装置１が受信するまでに経由した経路情報と、予めゲートウェイ装置１に格納されている経路情報とを照合することで通信端末２の認証を行う。
【０００４】
特許文献２に、認証のセキュリティ、認証の精度を向上させることに寄与する認証装置が開示されている。具体的には、この認証装置は、互いに異なる認証方式による識別情報を取得する複数の情報取得部と、前記情報取得部による認証方式と照合情報の組を１つの認証要素とし、前記認証要素の組み合わせと順序からなる、認証シーケンス情報を記憶する記憶部と、を備える。そして、この認証装置は、前記認証要素の組み合わせと順序に基づいて、被認証者を認証する。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１３－２０１４８１号公報
【特許文献２】特開２０１７－１５１７５９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
以下の分析は、本発明者によって与えられたものである。マルチホップ機能を備えた無線ＬＡＮアクセスポイントを用いてマルチホップネットワークを構築した環境では、ある機器から通信先の機器に送信されたデータは、複数のノードを中継して返信される。このため、データの偽造、いわゆるなりすましが行われる可能性がある。
【０００７】
また、マルチホップネットワークにおけるセキュリティの脆弱性は、親機よりも上流側のネットワークに対しても脅威となりうる。
【０００８】
本発明は、マルチホップネットワークを利用する情報システムのセキュリティの向上に貢献できる通信ノード、マルチホップネットワーク、機器の正当性確認方法及びプログラムを提供することを目的とする。
【課題を解決するための手段】
【０００９】
第１の視点によれば、マルチホップネットワークを介して通信する機器間のデータをマルチホップ方式で中継する通信部と、前記中継したデータのうち、所定の種類のデータを記録する記録部と、前記所定の種類のデータと、前記記録部に記録された過去のデータとを照合し、前記機器の正当性を確認する確認部と、所定の出力先に対し、前記機器の正当性の確認結果を出力する出力部と、を備えた通信ノードが提供される。
【００１０】

第２の視点によれば、上記した通信ノードを含んで構成されたマルチホップネットワークが提供される。

【００１１】

第３の視点によれば、マルチホップネットワークを介して通信する機器間のデータをマルチホップ方式で中継する通信ノードが、前記中継したデータのうち、所定の種類のデータを記録し、前記所定の種類のデータと、前記記録部に記録された過去のデータとを照合し、前記機器の正当性を確認し、所定の出力先に対し、前記機器の正当性の確認結果を出力する、機器の正当性確認方法が提供される。本方法は、マルチホップネットワークを介して通信する機器間のデータをマルチホップ方式で中継する通信ノードという、特定の機械に結びつけられている。

【００１２】

第４の視点によれば、マルチホップネットワークを介して通信する機器間のデータをマルチホップ方式で中継する通信ノードに搭載されたコンピュータに、前記中継したデータのうち、所定の種類のデータを記録する処理と、前記所定の種類のデータと、前記記録部に記録された過去のデータとを照合し、前記機器の正当性を確認する処理と、所定の出力先に対し、前記機器の正当性の確認結果を出力する処理と、を実行させるプログラムが提供される。このプログラムは、コンピュータ装置に入力装置又は外部から通信インターフェースを介して入力され、記憶装置に記憶されて、プロセッサを所定のステップないし処理に従って駆動させる。また、このプログラムは、必要に応じ中間状態を含めその処理結果を段階毎に表示装置を介して表示することができ、あるいは通信インターフェースを介して、外部と通信することができる。そのためのコンピュータ装置は、一例として、典型的には互いにバスによって接続可能なプロセッサ、記憶装置、入力装置、通信インターフェース、及び必要に応じ表示装置を備える。

【発明の効果】

【００１３】

本発明によれば、マルチホップネットワークを利用する情報システムのセキュリティの向上に貢献することが可能となる。

【図面の簡単な説明】

【００１４】

【図１】本発明の一実施形態の構成を示す図である。

【図２】本発明の一実施形態の動作を説明するための図である。

【図３】本発明の一実施形態の動作を説明するための別の図である。

【図４】本発明の第１の実施形態の構成を示す図である。

【図５】本発明の第１の実施形態のマルチホップネットワークを構成する通信ゲートウェイ（親機）及び通信ノードの構成を示す機能ブロック図である。

【図６】本発明の第１の実施形態のロギングデータの一例を示す図である。

【図７】本発明の第１の実施形態の動作（データ学習）を示す図である。

【図８】本発明の第１の実施形態の動作（運用時－操作ジェスチャー検証）を示す図である。

【図９】本発明の第１の実施形態の動作（運用時－作業活用データ検証）を示す図である。

【図１０】本発明の第１の実施形態の動作（運用時－作業成果データ検証）を示す図である。

【図１１】本発明の第２の実施形態の構成と動作を説明するための図である。

【図１２】本発明の通信ノードに搭載されたコンピュータの構成を示す図である。

【発明を実施するための形態】

【００１５】

はじめに本発明の一実施形態の概要について図面を参照して説明する。なお、この概要に付記した図面参照符号は、理解を助けるための一例として各要素に便宜上付記したものであり、本発明を図示の態様に限定することを意図するものではない。また、以降の説明

で参照する図面等のブロック間の接続線は、双方向及び単方向の双方を含む。一方向矢印については、主たる信号（データ）の流れを模式的に示すものであり、双方向性を排除するものではない。このプログラムはコンピュータ装置を介して実行され、コンピュータ装置は、例えば、プロセッサ、記憶装置、入力装置、通信インターフェース、及び必要に応じ表示装置を備える。また、このコンピュータ装置は、通信インターフェースを介して装置内又は外部の機器（コンピュータを含む）と、有線、無線を問わず、通信可能に構成される。また、図中の各ブロックの入出力の接続点には、ポート乃至インターフェースがあるが図示省略する。また、以下の説明において、「Ａ及び／又はＢ」は、Ａ又はＢ、又はＡ及びＢという意味で用いる。

【００１６】

本発明は、その一実施形態において、図１に示すように、通信部１１と、記録部１２と、確認部１３と、出力部１４と、を備えた通信ノード１０Ａにて実現できる。以下の説明では、通信ノード１０Ａは、既設ネットワーク（既設ＮＷ）２０に配置されたマルチホップネットワークの親機に対し、子機として動作する機器であるものとして説明する。通信ノード１０Ａは、他の通信ノード１０Ｂと連携して、既設ネットワーク（既設ＮＷ）２０に接続された機器（図示省略）と、通信ノード１０Ｂに接続された機器（端末３０）間のデータを中継する。

【００１７】

より具体的には、通信部１１は、マルチホップネットワークを介して通信する機器間のデータをマルチホップ方式で中継する。記録部１２は、前記中継したデータのうち、所定の種類のデータを記録する。所定の種類のデータとしては、ユーザの癖や挙動、あるいは、攻撃の対象となりやすいデータ等のうち、なりすまし等を検出可能な種類のデータが選択される。

【００１８】

確認部１３は、前記所定の種類のデータと、前記記録部に記録された過去のデータとを照合し、前記機器の正当性を確認する。出力部１４は、所定の出力先に対し、前記機器の正当性の確認結果を出力する。ここで、「機器の正当性の確認」とは、機器そのものの正当性に加えて、適切な権限を持ったユーザ（作業員等）が当該機器を使用している状態を確認するものである。

【００１９】

図２は、前記所定の種類のデータとして、端末３０にて撮影されたジェスチャーデータを用いた場合の動作を表した図である。端末３０のユーザーが、ジェスチャーを撮影し、ジェスチャーデータＧ１として通信ノード１０Ｂに送ると、通信ノード１０Ｂは、通信ノード１０Ａにジェスチャーデータ Ｇ１を転送する。

【００２０】

前記ジェスチャーデータＧ１を受信した通信ノード１０Ａは、ジェスチャーデータＧ１を既設ＮＷ２０側に中継するとともに、記録部１２にてジェスチャーデータＧ１を記録（ロギング）する。

【００２１】

さらに、確認部１３は、記録部１２に記録された直近のジェスチャーデータＧ１と、前回、端末３０から送られたジェスチャーデータＧ０とを照合し、端末３０の正当性を確認する。例えば、ここで、ユーザーの親指を立てるジェスチャーが前回記録したものと異なる場合、確認部１３は、端末３０の正当性を確認できないものと判定する。この場合、出力部１４は、所定の出力先に対し、端末３０の正当性の確認結果（なりすましの可能性あり）を出力する。

【００２２】

もちろん、確認部１３が、端末３０の正当性を確認できた場合も、出力部１４は、所定の出力先に対し、前記機器の正当性の確認結果（なりすましの可能性なし）を出力するようにしてもよい。

【００２３】

図３は、前記所定の種類のデータとして、既設ＮＷ２０側からスマートグラス４０に宛てて送信されたＡＲ（Ａｕｇｍｅｎｔｅｄ　Ｒｅａｌｉｔｙ）データを用いた場合の動作を表した図である。既設ＮＷ２０側の機器（例えば、ＡＲを用いた作業指示サーバ）が、ＡＲデータＡＲ１として通信ノード１０Ａに送ると、通信ノード１０Ａ、通信ノード１０ＢにＡＲデータＡＲ１を転送する。

【００２４】

前記ＡＲデータＡＲ１を受信した通信ノード１０Ｂは、ＡＲデータＡＲ１をスマートグラス４０側に送信する。

【００２５】

上記の過程において、通信ノード１０Ａの記録部１２は、ＡＲデータＡＲ１を記録（ロギング）する。通信ノード１０Ａの確認部１３は、記録部１２に記録された直近のＡＲデータＡＲ１と、前回、既設ＮＷ２０から送られたＡＲデータＡＲ０とを照合し、既設ＮＷ２０側の機器（例えば、ＶＲを用いた作業指示サーバ）の正当性を確認する。例えば、ここで、ＡＲデータＡＲ１に含まれる特定の情報（例えば、ＡＲ中の図形）が前回記録したものと異なる場合、確認部１３は、既設ＮＷ２０側の機器の正当性を確認できないものと判定する。この場合、出力部１４は、所定の出力先に対し、既設ＮＷ２０側の機器の正当性の確認結果（なりすましの可能性あり）を出力する。

【００２６】

もちろん、確認部１３が、既設ＮＷ２０側の機器の正当性を確認できた場合も、出力部１４は、所定の出力先に対し、既設ＮＷ２０側の機器の正当性の確認結果（なりすましの可能性なし）を出力するようにしてもよい。

【００２７】

以上のように、本実施形態によれば、通常の機器間で行われる認証処理に加え、マルチホップネットワーク側で記録したデータを用いた認証を追加し、マルチホップネットワークのセキュリティを向上させることが可能となる。

【００２８】

［第１の実施形態］

続いて、本発明の第１の実施形態について図面を参照して詳細に説明する。図４は、本発明の第１の実施形態の構成を示す図である。図４を参照すると、上位サーバ６１０及び表示装置６２０が設置された事務所と、基地局５００と、通信ゲートウェイ（親機）１１０を用いて構成されたマルチホップネットワークと、が接続された構成が示されている。

【００２９】

マルチホップネットワークは、通信ゲートウェイ（親機）１１０及び複数の通信ノード（子機）１２０によって構成され、基地局５００の電波の届かない場所にあるデバイス８００に対し上位サーバ６１０への接続環境を提供する。このようなマルチホップネットワークの構成機器としては、マルチホップ中継機能を備えた無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）アクセスポイントを用いることもできる。いずれの場合も、プラント、建屋内、導水路、導管、下水道管等の基地局や無線ＬＡＮアクセスポイントの電波が届かないエリアでネットワークへの接続環境を提供することが可能となる。

【００３０】

基地局５００は、３Ｇ、ＬＴＥ（Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ）、５Ｇ等に対応する移動体通信事業者の基地局である。

【００３１】

上位サーバ６１０は、インターネット等を介して、基地局５００及びマルチホップネットワーク経由で、デバイス８００に「作業活用データ」と呼ばれる作業支援情報（「作業指示用のデータ」に相当）を送信する機器である。表示装置６２０は、前記デバイスのなりすまし検出時に、メッセージの表示先として使用される機器の一つである。本実施形態では、作業活用データは、作業員７００の作業を支援するＶＲ（Ｖｉｒｔｕａｌ　Ｒｅａｌｉｔｙ）、ＡＲ、ＭＲ（Ｍｉｘｅｄ　Ｒｅａｌｉｔｙ）を用いて作成された情報であるものとして説明する。

【００３２】
デバイス８００は、スマートグラスに代表されるウェアラブル端末やスマートフォン等の端末である。デバイス８００は、マルチホップネットワークを介して、上位サーバ６１０にログインし、ジェスチャーで操作を行うことで、上位サーバ６１０から作業活用データを取得し、表示可能となっている。なお、本実施形態では、作業活用データは、ＶＲ、ＡＲ、ＭＲといった方法で表示されるものとする。もちろん、ＶＲ、ＡＲ、ＭＲを用いずに、デバイスの表示装置やスピーカーから「作業活用データ」をテキストや音声で出力する態様も採用可能である。
【００３３】
図５は、マルチホップネットワークを構成する通信ゲートウェイ（親機）及び通信ノードの構成を示す機能ブロック図である。図５を参照すると、通信ゲートウェイ（親機）１１０は、通信部１１１、記録部１１２、確認部１１３及び出力部１１４を備えている。
【００３４】
通信部１１１は、上位サーバ６１０とデバイス８００間のデータをマルチホップ方式で中継する。
【００３５】
記録部１１２は、前記中継したデータのうち、所定の種類のデータを記録する。以下、この記録したデータをロギングデータという。本実施形態では、デバイス８００で撮影され、上位サーバ６１０側に送信される操作ジェスチャー（「機器操作用のジェスチャーデータ」に相当）と、上位サーバ６１０からデバイス８００側に送信される作業活用データを記録の対象とする。また、記録部１１２は、上記データの記録に加えて、所定の種類のデータについて、その経路データを「ルートタグデータ」（転送経路情報）として記録する。本実施形態では、記録部１１２は、作業員７００が作業完了後に上位サーバ６１０に送る作業成果データの経路データを記録する。
【００３６】
図６は、記録部１１２に保持されているロギングデータの一例を示す図である。図６の上段は、利用者ＩＤと、上位サーバ６１０を特定するためのシステムＩＤと、利用年月日時と、ロギングデータ（操作ジェスチャーデータ）とを対応付けて格納するテーブルが示されている。図６の下段は、システムＩＤと、利用者ＩＤと、利用年月日時と、ロギングデータ（作業活用データ）とを対応付けて格納するテーブルが示されている。利用者ＩＤは、デバイス８００を特定するための情報として使用される作業員（利用者）のＩＤである。システムＩＤは、上位サーバ６１０を特定するための情報として使用されるサーバのＩＤである。利用年月日時は、ロギングを行った日時であり、ロギングデータとしては、操作ジェスチャーや作業活用データの特徴データが格納される。
【００３７】
確認部１１３は、直近のロギングデータと、過去のロギングデータとを照合し、有意な差異が認められるか否かにより、機器の正当性を確認する。例えば、デバイス８００が上位サーバ６１０に送った操作ジェスチャーに表れた手指の動き、手指の色や形、背景等が、過去の操作ジェスチャーと有意な差異がある場合、なりすましの可能性ありと判定することができる。ここで、操作ジェスチャーにおける有意な差異とは、手指の動きの速さや傾き等に表れる作業者の癖に起因するものや、手指の色や形、背景の違いなどから、本人が行った操作ジェスチャーでない可能性があると判断される差異を設定すればよい。
【００３８】
同様に、上位サーバ６１０がデバイス８００に送った作業活用データも、ＶＲ、ＡＲ、ＭＲに表れた画像の動きや、図形要素の形、色等が過去の作業活用データと有意な差異がある場合、なりすましの可能性ありと判定することができる。ここで、作業活用データにおける有意な差異とは、ＡＲで作業者の視野範囲に合成されるデジタル映像そのものの差異や、デジタル映像と併せて出力されるテキストや音声の違いなどから、上位サーバ６１０が送信した作業活用データでない可能性があると判断される差異を設定すればよい。
【００３９】

また、確認部１１３は、作業成果データのルートタグデータと、該当するデバイス８００の過去の作業成果データのルートタグデータとが一致するか否かにより機器の正当性を確認する。例えば、デバイス８００が、本来の作業位置と異なる経路で作業成果データを送信してきた場合、なりすましの可能性ありと判定する。

【００４０】

出力部１１４は、上記確認部１１３による正当性確認の結果、異常が認められた場合に、所定の出力先装置に対し、メッセージを送信する（上記出力部１４に相当）。本実施形態では、出力部１１４は、機器の正当性の確認結果を上位サーバ６１０に接続された表示装置６２０のほか、作業者の上司や監督者であるシステム管理者１、２が保持する端末に、メッセージを送信する。メッセージの具体的な内容については、後の動作の説明と併せて説明する。

【００４１】

通信ノード（子機）１２０は、通信部１２１、記録部１２２、確認部１２３及び出力部１２４を備えている。通信ノード（子機）１２０の通信部１２１、記録部１２２、確認部１２３及び出力部１２４は、それぞれ通信ゲートウェイ（親機）１１０の通信部１１１、記録部１１２、確認部１１３及び出力部１１４と同等であるので、説明を省略する。従って、通信ゲートウェイ（親機）１１０及び複数の通信ノード（子機）１２０が、上記した通信ノードに相当する。

【００４２】

続いて、本実施形態の動作について図面を参照して詳細に説明する。図７は、本実施形態のマルチホップネットワークの運用開始前に行われるデータ学習処理の流れを表したシーケンス図である。以下の説明では、デバイス８００がｎ台目の子機（子機ｎ）に接続し、上位サーバ６１０にアクセスする例を挙げて説明する。

【００４３】

図７を参照すると、まず、デバイス８００においてシステム利用入力が行われる（ステップＳ００１）。ここでは、利用者ＩＤ、システムＩＤ、システムデータＩＤ、利用年月日時及び操作ジェスチャーデータの入力が行われるものとする。ここで、システムデータＩＤとは、上位サーバ６１０から提供を受けるデータを特定するためのＩＤであり、例えば、地下鉄ＸＸ駅（仮称）構内工事　第１期基礎工３日目、ＹＹ発電所建屋工事　外構（東側）工事２日目といったデータ（コンテンツ）を特定するためのＩＤが設定される。

【００４４】

システム利用入力で入力を受け付けたデバイス８００は、利用者ＩＤ、システムＩＤ、システムデータＩＤ、利用年月日時、操作ジェスチャーデータを上位サーバ６１０に送信する（ステップＳ００２）。

【００４５】

上位サーバ６１０は、利用者ＩＤで利用者を特定した上で、操作ジェスチャーデータによる認証を行う（ステップＳ００３）。ここでの認証は、予め登録された作業員７００の操作ジェスチャーと、操作ジェスチャーデータとの類似率を計算し、所定のスコア以上である場合に、認証成功とするといった認証方法を用いることができる。

【００４６】

上記システム利用入力で入力を受け付けたデータの中継を行った通信ゲートウェイ（以下、通信ＧＷ）１１０及び通信ノードは、それぞれ中継したデータをロギングする（ステップＳ００４、図６参照）。なお、図７において、通信ノード（子機１）におけるロギング処理は省略されている。すべての通信ノードが、ロギングする必要はなく、一部の通信ノードにおけるロギング処理を省略することができる。

【００４７】

一方、本実施形態の上位サーバ６１０は、操作ジェスチャーデータの過去データを保持している場合、過去データとの一致不一致を確認する（ステップＳ００５）。

【００４８】

前記確認の結果、操作ジェスチャーデータが過去データと不一致であった場合、上位サ

ーバ６１０は、デバイス８００に対し、暗号付き操作ジェスチャー変更指示を送信する（ステップＳ００７）。暗号付き操作ジェスチャー変更指示とは、事前に定めた暗号（パスワード）の入力を条件に操作ジェスチャーの変更指示を閲覧できるようにしたメッセージである。従って、学習段階において、デバイス８００のなりすましが行われている場合、操作ジェスチャーの変更内容を閲覧することができないため、不正なユーザーの登録を抑止することが可能となっている。

【００４９】

暗号（パスワード）の入力に成功するとデバイス８００において、操作ジェスチャーの変更指示の表示が行われる（ステップＳ００８）。前記操作ジェスチャーの変更指示を閲覧した作業員７００は、ステップＳ００１に戻って再度、システム利用入力を行なう（ステップＳ００１）。

【００５０】

ステップＳ００６で、操作ジェスチャーデータが過去データと一致した場合、上位サーバ６１０は、デバイス８００に対し、システムへのログインが完了したことを示すシステムログインメッセージを送信する（ステップＳ００９）。

【００５１】

上記システムログインメッセージの中継を行った通信ＧＷ１１０及び通信ノード１２０は、それぞれデバイス８００がログインに成功したことを認識する（ステップＳ０１０、ログイン認識）。次に、通信ＧＷ１１０及び通信ノード１２０は、ステップＳ００４でロギングしたデータを学習する（ステップＳ０１１）。さらに、通信ＧＷ１１０及び通信ノード１２０は、操作ジェスチャーデータの認識を行い、必要があれば、操作ジェスチャーデータに対応する処理を行う（ステップＳ０１２）。

【００５２】

前記システムログインメッセージを受信したデバイス８００は、上位サーバ６１０に対し、作業活用データのダウンロードを要求する（ステップＳ０１３）。前記作業活用データのダウンロード要求を受けた上位サーバ６１０は、デバイス８００に対し、作業活用データを送信する（ステップＳ０１４；作業活用データダウンロード）。

【００５３】

上記作業活用データの中継を行った通信ＧＷ１１０及び通信ノード１２０は、それぞれ作業活用データのロギングを行う（ステップＳ０１５）。

【００５４】

以上により、デバイス８００の正当性確認に必要な学習データ（過去データ）の蓄積が行われる。

【００５５】

図８は、上記データ学習処理の後に、実運用が始まった際の、各装置による操作ジェスチャーの検証動作の一例を示す図である。図８を参照すると、まず、デバイス８００においてシステム利用入力が行われる（ステップＳ１０１）。ここでのシステム利用入力は、図７で説明したステップＳ００１と同様である。

【００５６】

システム利用入力で入力を受け付けたデバイス８００は、利用者ＩＤ、システムＩＤ、システムデータＩＤ、利用年月日時、操作ジェスチャーデータを上位サーバ６１０に宛てて送信する（ステップＳ１０２）。

【００５７】

上記システム利用入力で入力を受け付けたデータの中継を行った通信ＧＷ１１０及び通信ノードは、操作ジェスチャーデータを含むデータを受信した場合、それぞれ中継したデータをロギングする（ステップＳ１０３、図６参照）。

【００５８】

次に、通信ＧＷ１１０及び通信ノード１２０は、それぞれ過去にロギングしたデータと、ステップＳ１０２で受信したデータとを比較し、一致不一致を確認する（ステップＳ１０４）。通信ノード１２０は、確認の結果を、通信ＧＷ１１０に送信する。

【００５９】
通信ＧＷ１１０は、通信ＧＷ１１０と通信ノード１２０の少なくとも一方で操作ジェスチャーデータが過去データと不一致であった場合、システム管理者１、２の端末に対し、システム利用不正アラームを送信する（ステップＳ１０７、Ｓ１０８）。ここで、システム管理者１としては、上位サーバ６１０が設置されている事務所の管理者が想定される。また、システム管理者２としては、作業員７００の管理者が想定される。システム利用不正アラームは、デバイス８００において「なりすまし」が行われている可能性を伝えるものであればよく、ＳＭＳ（Ｓｈｏｒｔ　Ｍｅｓｓａｇｅ　Ｓｅｒｖｉｃｅ）、メール、音声通話等、適当な形態を採ることができる。

【００６０】
通信ＧＷ１１０は、システム管理者１、２の端末に対するシステム利用不正アラームの送信後、デバイス８００に対して、操作ジェスチャーメッセージを送信する（ステップＳ１０９、Ｓ１１０）。この操作ジェスチャーメッセージは、操作ジェスチャーに問題があったことを伝える内容であればよく、詳しい判定結果を伝える必要はない。操作ジェスチャーメッセージを受信したデバイス８００は、操作ジェスチャーメッセージを表示する。ここで、作業員７００が真正の作業員であれば、いつもと異なるジェスチャーをしたことに気づき、再度、システム利用入力を行なうことになる。一方、作業員７００が非真正の作業員である場合、いつもと異なるジェスチャーをしたことに気づいても、ジェスチャーのどの部分に問題があったのかわからないため、再度、システム利用入力を行っても、ログインに成功することはない。

【００６１】
一方、ステップＳ１０６で、操作ジェスチャーデータが過去データと一致した場合、通信ＧＷ１１０は、上位サーバ６１０に対し、システム利用入力データを転送する（ステップＳ１１２）。以降、システム利用入力データを用いたシステムログイン手順が行われる（ステップＳ１１３；システム利用開始）。具体的には、ステップＳ００３と同様に、上位サーバ６１０が、利用者ＩＤで利用者を特定した上で、操作ジェスチャーデータによる認証を行う。

【００６２】
以上のように、本実施形態によれば、システム利用開始時にデバイス８００から上位サーバに送られる操作ジェスチャーデータを用いてなりすましの検出を行うことが可能となる。また、この判定は、上位サーバ６１０における操作ジェスチャーデータと異なる観点で行われ、問題があれば、上位サーバ６１０に対するシステム利用入力データの送信も抑止されるため、上位サーバ６１０に対するＤｏＳ（Ｄｅｎｙ　ｏｆ　Ｓｅｒｖｉｃｅ）攻撃対策としても有効である。また、通信ＧＷ１１０と通信ノード１２０において異なる観点で操作ジェスチャーデータ等の判定が行われてもよい。例えば、通信ノード１２０は、通信ＧＷ１１０との比較において、メモリやプロセッサの処理能力が落ちるため、通信ＧＷ１１０よりも簡略化した内容の判定を行うようにしてもよい。なお、図７の例では、通信ＧＷ１１０と通信ノード１２０の双方で、操作ジェスチャーデータの過去データとの一致不一致を判定しているが、これらの双方で一致不一致を判定しなくてもよい。例えば、通信ＧＷ１１０と通信ノード１２０のいずれか一方で操作ジェスチャーデータの過去データとの一致不一致を判定する構成も採用可能である。

【００６３】
さらに本実施形態では、上位サーバ６１０側からデバイス８００側に送られる作業活用データの検証を行う。図９は、上記システムログイン後の、各装置による作業活用データの検証動作の一例を示す図である。図９を参照すると、まず、デバイス８００が、上位サーバ６１０に対し、作業活用データのダウンロード要求を行う（ステップＳ２０１）。前記ダウンロード要求を受けた上位サーバ６１０は、作業活用データのダウンロードに応じ、作業活用データを通信ＧＷ１１０に送信する（ステップＳ２０２）。

【００６４】
前記作業活用データの中継を行った通信ＧＷ１１０及び通信ノードは、作業活用データ

を受信した場合、それぞれ中継した作業活用データをロギングする（ステップＳ２０３、図６参照）。

【００６５】

次に、通信ＧＷ１１０及び通信ノード１２０は、それぞれ過去にロギングしたデータと、ステップＳ２０２で受信したデータとを比較し、一致不一致を確認する（ステップＳ２０４）。なお、ステップＳ２０４の確認において、それぞれのデータに付されているシーケンス番号があれば、その整合性を検証してもよい。例えば、過去にロギングしたデータに対し、ステップＳ２０２で受信したデータの方が、若い（時間的に古い）シーケンス番号が付されている場合、作業活用データの不正が疑われる。通信ノード１２０は、確認の結果を、通信ＧＷ１１０に送信する。

【００６６】

通信ＧＷ１１０は、通信ＧＷ１１０と通信ノード１２０の少なくとも一方で作業活用データが過去データと不一致であった場合、システム管理者１、２の端末に対し、作業活用データ不正アラームを送信する（ステップＳ２０７、Ｓ２０８）。ここで、システム管理者１としては、上位サーバ６１０が設置されている事務所の管理者が想定される。また、システム管理者２としては、作業員７００の管理者が想定される。作業活用データ不正アラームは、作業活用データの送信元が上位サーバ６１０でない可能性を伝えるものであればよく、ＳＭＳ（Ｓｈｏｒｔ　Ｍｅｓｓａｇｅ　Ｓｅｒｖｉｃｅ）、メール、音声通話等、適当な形態を採ることができる。

【００６７】

通信ＧＷ１１０は、システム管理者１、２の端末に対する作業活用データ不正アラームの送信後、デバイス８００に対して、作業中止指示アラームを送信する（ステップＳ２０９、Ｓ２１０）。この作業中止指示アラームは、作業活用データが上位サーバ６１０から送信されたものではない可能性があることを伝える内容であればよい。作業中止指示アラームを受信したデバイス８００は、作業中止指示アラームを表示する。前記アラームを受け取った作業員７００は、作業活用データによる作業を中止する。なお、すでに受け取った作業活用データにより、作業を開始していた場合において、ある時点から、この作業中止指示アラームを受け取った場合も、途中でなりすましが行われた可能性を示しているので、作業活用データによる作業を中止することが好ましい。

【００６８】

一方、ステップＳ２０６で、作業活用データが過去データと一致した場合、通信ＧＷ１１０は、デバイス８００に対し、作業活用データを転送する（ステップＳ２１２）。デバイス８００は、作業活用データを受信するとデータ受信メッセージを表示し（ステップＳ２１３）、作業員７００による作業活用データの操作を待つ。以降、同様の手順で、作業活用データのダウンロード要求と、過去データとの照合によるなりすましの有無の判定が行われた後、デバイスに作業活用データが送られる（ステップＳ２１４；システム通常運用手順）。

【００６９】

以上のように、本実施形態によれば、上位サーバ６１０からデバイス８００に送られる作業活用データを用いてなりすましの検出を行うことが可能となる。例えば、悪意を持って作業員７００に、間違った作業をさせようとして偽の作業活用データが送られた場合であっても、通信ＧＷ１１０と通信ノード１２０によって検出することが可能となる。とりわけ、デバイス８００によっては、メモリや計算処理能力に制限がある場合が多い。また、デバイス８００にそのリソースがあったとしても、なりすまし検出にリソースを割くことが適切でない場合は、多いと考えられる。本実施形態は、そのようなケースにおいてより有効にその効果を発揮することができる。

【００７０】

さらに本実施形態では、作業終了後に、デバイス８００側から上位サーバ６１０側に送られる作業成果データの検証を行う。図１０は、作業成果データの検証動作の一例を示す図である。図１０を参照すると、まず、デバイス８００が、上位サーバ６１０に対し、作

業成果データのアップロード要求を行う（ステップＳ３０１）。前記アップロード要求を受けた上位サーバ６１０は、作業成果データのアップロードを許可するメッセージをデバイス８００に送信する（ステップＳ３０２）。

【００７１】

前記作業成果データのアップロードを許可するメッセージの中継を行った通信ＧＷ１１０及び通信ノード１２０は、これらの上位サーバ６１０とデバイス８００間のやり取りをロギングする（ステップＳ３０３）。

【００７２】

作業成果データのアップロードを許可するメッセージを受け取ったデバイス８００は、作業成果データのアップロードを許可するメッセージを表示する（ステップＳ３０４）。前記メッセージを確認した作業員７００が、作業成果データのアップロード操作を行うと、作業成果データのアップロードが開始される（ステップＳ３０５）。

【００７３】

作業成果データの中継を行った通信ＧＷ１１０及び通信ノード１２０は、それぞれ中継の際に、作業成果データにルートタグを付与し、記録する（ステップＳ３０６、Ｓ３０７）。このルートタグは、作業成果データの転送経路上の通信ＧＷ１１０及び通信ノード１２０がそれぞれ自身のＩＤをタグとして付加することで構成することができる。

【００７４】

次に、通信ＧＷ１１０は、それぞれ過去の作業成果データのルートタグと、今回の作業成果データのルートタグとを比較し、一致不一致を確認する（ステップＳ３０８）。

【００７５】

通信ＧＷ１１０は、前記確認の結果、作業成果データのルートタグが過去のルートタグと不一致であった場合、システム管理者１、２の端末に対し、作業成果データのルートタグ不一致アラートを送信する（ステップＳ３０９、Ｓ３１０）。ルートタグ不一致アラートの送信先は、作業活用データ不正アラームと同一でよい。ルートタグ不一致アラートは、作業成果データが適正でない位置から送信されていることを伝えるものであればよく、ＳＭＳ（Ｓｈｏｒｔ　Ｍｅｓｓａｇｅ　Ｓｅｒｖｉｃｅ）、メール、音声通話等、適当な形態を採ることができる。

【００７６】

一方、ステップＳ３０８で、作業成果データのルートタグが過去データと一致した場合、通信ＧＷ１１０は、上位サーバ６１０に対し、作業成果データを転送する（ステップＳ３１１）。作業成果データを受け取った上位サーバ６１０は、デバイス８００に対して、作業成果データのアップロードが完了したことを伝えるメッセージを送信する（ステップＳ３１２；作業成果データアップロード完了通知）。

【００７７】

前記作業成果データのアップロードが完了したことを伝えるメッセージの中継を行った通信ＧＷ１１０及び通信ノード１２０は、作業成果データその他の、上位サーバ６１０とデバイス８００間のやり取りをロギングする（ステップＳ３１３）。

【００７８】

その後、上位サーバ６１０とデバイス８００間で、システムログアウト完了手順が行われる（ステップＳ３１４）。

【００７９】

以上のように、本実施形態によれば、デバイス８００から上位サーバ６１０に送られる作業成果データの不正な送信を検出することが可能となる。例えば、悪意を持って、通常と異なる位置から、作業成果データの送信が行われた場合、作業成果データが上位サーバ６１０に転送される前に、これを検知し、アラートを上げることが可能となる。

【００８０】

なお、上記した実施形態では、操作ジェスチャーデータ、作業活用データ、作業成果データをなりすまし検出の対象としているが、その他データについてもロギングし、過去のデータと比較することで、なりすまし等を検出することができる。

【００８１】
［第２の実施形態］
上記した第１の実施形態では、操作ジェスチャーデータと作業活用データについては、ロギングデータとの照合により、なりすましの検出（正当性確認）を行ったが、操作ジェスチャーデータと作業活用データについてもルートタグデータをその都度記録してもよい。このようにすることで、操作ジェスチャーデータと作業活用データについても。ロギングデータとルートタグデータとの双方を用いた、なりすまし検出（正当性確認）を行うことができる。
【００８２】
図１１は、第２の実施形態の構成と動作を説明するための図である。第２の実施形態は、第１の実施形態と基本的な構成は同一であるので、以下、その相違点を中心に説明する。
【００８３】
図１１の例では、通信ＧＷ１１０、通信ノード１２０ａの２ヶ所でロギングデータとルートタグデータとの双方を用いた、なりすまし検出（正当性確認）を行っている。ここでのなりすましの検出（正当性確認）は、第１の実施形態における作業成果データの検証と同様に、デバイス８００の位置（経路の始点）が適正でない位置から送信されているか否かの観点で行うことができる。また、図１１の例では、通信ノード１２０ｂでは、なりすまし検出（正当性確認）が省略されている。即ち、通信ノード１２０ｂは、ロギングデータの記録もルートタグデータの記録も行わない。通信ノードの計算リソースが少ない場合、通信ノード１２０ｂのように、なりすまし検出（正当性確認）を省略してもよい。
【００８４】
また、図１１の例では、通信ノード１２０ｃでは、ロギングデータを用いたなりすまし検出（正当性確認）を行っている。その理由は、通信ノード１２０ｃはマルチホップネットワークの端部（親機から離れた方向）に配置され、上り方向のデータについて、一定の長さを持つルートタグデータが取れない可能性が高いためである。
【００８５】
以上のように、通信ＧＷ１１０、通信ノード１２０の位置や性能に応じて、ルートタグデータを併用するか否かを変更（設定）できるようにすることもできる。
【００８６】
また、ルートタグデータを併用するか否かはマルチホップネットワークに求められるセキュリティの高低に応じて設定してもよい。例えば、マルチホップネットワークが、ゲストユーザの利用を認めている場合、高度なセキュリティ管理が必要でない場合もある。そのようなケースでは、通信ＧＷ１１０におけるなりすまし検出（正当性確認）を行い、通信ノード１２０のなりすまし検出（正当性確認）を省略することもできる。
【００８７】
以上、本発明の各実施形態を説明したが、本発明は、上記した実施形態に限定されるものではなく、本発明の基本的技術的思想を逸脱しない範囲で、更なる変形・置換・調整を加えることができる。例えば、各図面に示したネットワーク構成、各要素の構成、メッセージの表現形態は、本発明の理解を助けるための一例であり、これらの図面に示した構成に限定されるものではない。
【００８８】
また、上記した第１、第２の実施形態に示した手順は、通信ＧＷ１１０や通信ノード１２０に搭載されたコンピュータ（図１２の９０００）に、これらの装置としての機能を実現させるプログラムにより実現可能である。このようなコンピュータは、図１２のＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）９０１０、通信インターフェース９０２０、メモリ９０３０、補助記憶装置９０４０を備える構成に例示される。すなわち、図１２のＣＰＵ９０１０にて、領域分割プログラムや位置推定プログラムを実行し、その補助記憶装置９０４０等に保持された各計算パラメーターの更新処理を実施させればよい。

【００８９】
即ち、上記した実施形態に示した通信ＧＷ１１０や通信ノード１２０の各部（処理手段、機能）は、これらの装置に搭載されたプロセッサに、そのハードウェアを用いて、上記した各処理を実行させるコンピュータプログラムにより実現することができる。
【００９０】
最後に、本発明の好ましい形態を要約する。
［第１の形態］
（上記第１の視点による通信ノード参照）
［第２の形態］
上記した通信ノードにおいて、
一方の機器から他方の機器に送信する機器操作用のジェスチャーデータを、前記所定の種類のデータとして記録する構成を採ることができる。
［第３の形態］
上記した通信ノードにおいて、
前記確認部は、前記機器操作用のジェスチャーデータに表れたジェスチャーの特徴に有意な差異がある場合に、なりすましが行われていると判定する構成を採ることができる。
［第４の形態］
上記した通信ノードにおいて、
一方の機器から他方の機器に送信する作業指示用のデータを、前記所定の種類のデータとして記録する構成を採ることができる。
［第５の形態］
上記した通信ノードにおいて、
前記確認部は、前記作業指示用のデータに表れた作業指示に有意な差異がある場合に、なりすましが行われていると判定する構成を採ることができる。
［第６の形態］
上記した通信ノードにおいて、
前記記録部は、さらに、前記所定の種類のデータの転送経路情報（ルートタグデータ）を記録し、
前記確認部は、さらに、前記データの転送経路を確認することにより、前記機器の正当性を確認する構成を採ることができる。
［第７の形態］
上記した通信ノードにおいて、
他の通信ノードから前記機器の正当性の確認結果を受け取り、
前記確認部は、前記他の通信ノードにおける前記機器の正当性の確認結果も用いて、前記機器の正当性を確認する構成を採ることができる。
［第８の形態］
（上記第２の視点によるマルチホップネットワーク参照）
［第９の形態］
（上記第３の視点による機器の正当性確認方法参照）
［第１０の形態］
（上記第４の視点によるプログラム参照）
なお、上記第８～第１０の形態は、第１の形態と同様に、第２～第７の形態に展開することが可能である。
【００９１】
なお、上記の特許文献の各開示は、本書に引用をもって繰り込み記載されているものとし、必要に応じて本発明の基礎ないし一部として用いることが出来るものとする。本発明の全開示（請求の範囲を含む）の枠内において、さらにその基本的技術思想に基づいて、実施形態ないし実施例の変更・調整が可能である。また、本発明の開示の枠内において種々の開示要素（各請求項の各要素、各実施形態ないし実施例の各要素、各図面の各要素等を含む）の多様な組み合わせ、ないし選択（部分的削除を含む）が可能である。すなわち

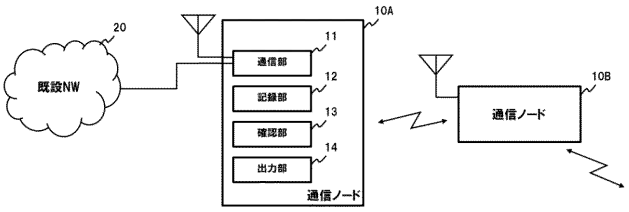
、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし得るであろう各種変形、修正を含むことは勿論である。特に、本書に記載した数値範囲については、当該範囲内に含まれる任意の数値ないし小範囲が、別段の記載のない場合でも具体的に記載されているものと解釈されるべきである。さらに、上記引用した文献の各開示事項は、必要に応じ、本発明の趣旨に則り、本発明の開示の一部として、その一部又は全部を、本書の記載事項と組み合わせて用いることも、本願の開示事項に含まれるものと、みなされる。

【符号の説明】

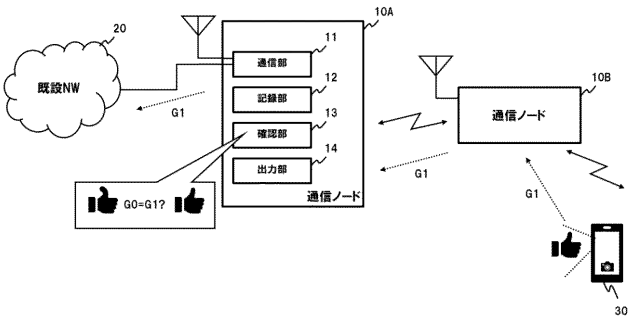
【００９２】

１０Ａ、１０Ｂ　通信ノード
１１、１１１、１２１　通信部
１２、１１２、１２２　記録部
１３、１１３、１２３　確認部
１４、１１４、１２４　出力部
２０　既設ネットワーク（既設ＮＷ）
３０　端末
４０　スマートグラス
１１０　通信ゲートウェイ（親機）
１２０、１２０ａ～１２０ｃ　通信ノード
６１０　上位サーバ
６２０　表示装置
５００　基地局
７００　作業員
８００　デバイス
９０００　コンピュータ
９０１０　ＣＰＵ
９０２０　通信インターフェース
９０３０　メモリ
９０４０　補助記憶装置
Ｇ０、Ｇ１　ジェスチャーデータ
ＡＲ１、ＡＲ１　ＡＲデータ

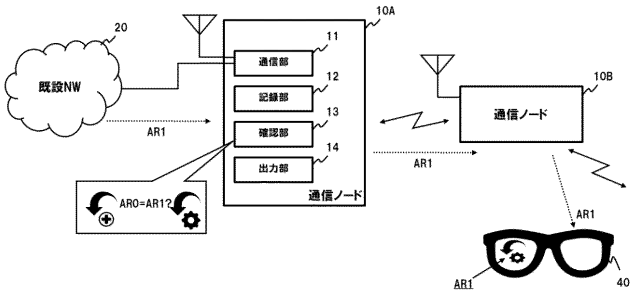
【図１】



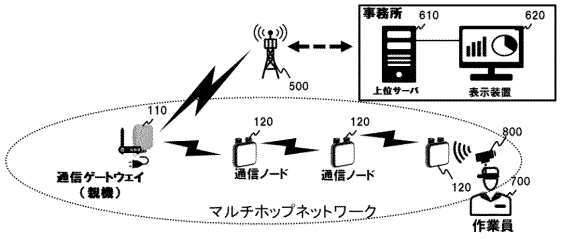
【図２】



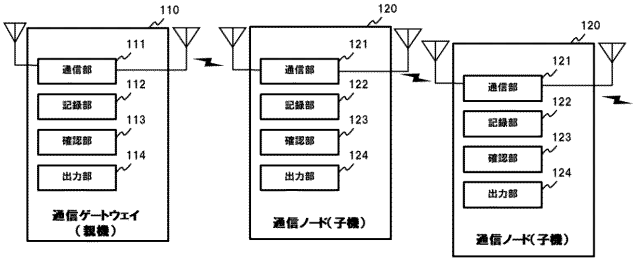
【図３】



【図４】



【図５】

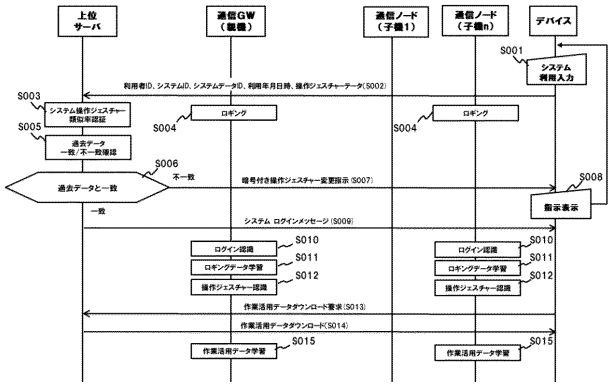


【図６】

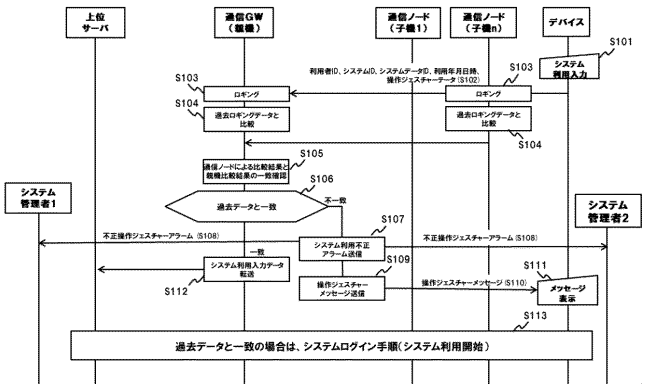
利用者ID	システムID	利用年月日時	ロギングデータ
T001	S001	2019/8/1 12:00:00	操作ジェスチャー
:	:	:	:
:	:	:	:
:	:	:	:

システムID	利用者ID	利用年月日時	ロギングデータ
:	:	:	:
S001	T001	2019/8/1 12:01:00	作業活用データ1
S001	T001	2019/8/1 12:02:00	作業活用データ2
:	:	:	:

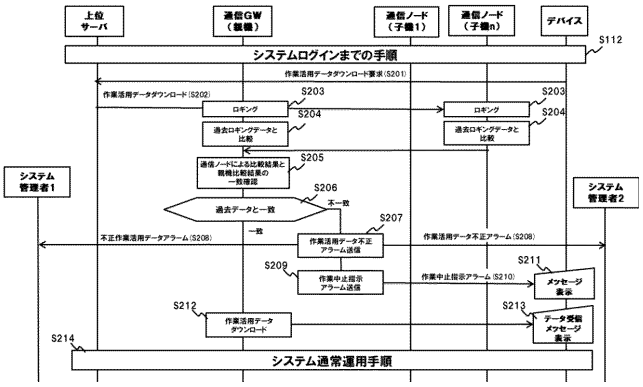
【図７】



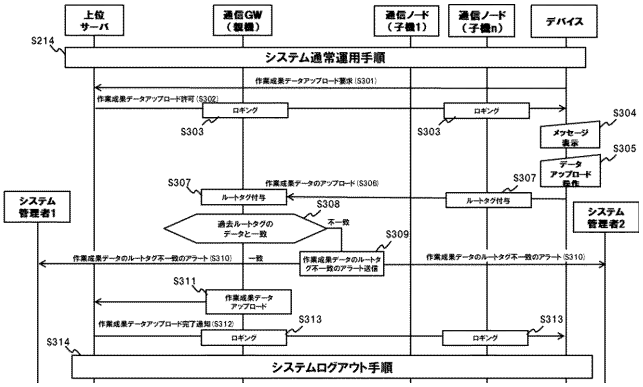
【図８】



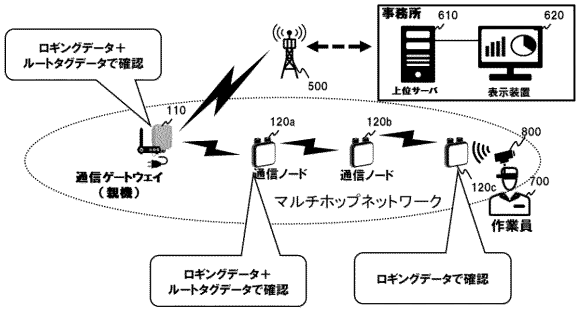
【図９】



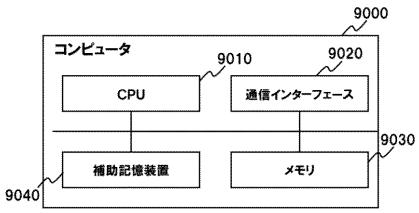
【図１０】



【図１１】



【図１２】



フロントページの続き

Ｆターム(参考) 5K067 AA30 BB21 EE02 EE10 EE16 FF01 HH22 HH23