(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7月4日(04.07.2024)

WIPO | PCT

(10) 国際公開番号
WO 2024/142136 A1

(51) 国際特許分類:
H04L 41/28 (2022.01)

(21) 国際出願番号： PCT/JP2022/047830

(22) 国際出願日： 2022年12月26日(26.12.2022)

(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: 吉野 學(**YOSHINO Manabu**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 原 一貴(**HARA Kazutaka**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 金子 慎(**KANEKO Shin**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 可児 淳一(**KANI Junichi**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

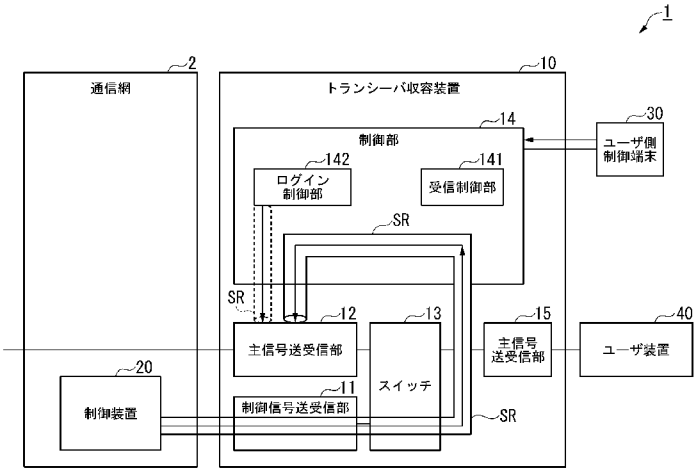
(74) 代理人: 弁理士法人志賀国際特許事務所 (**SHIGA INTERNATIONAL PATENT OFFICE**); 〒1006620 東京都千代田区丸の内一丁目９番２号 Tokyo (JP).

(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, 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,

(54) **Title:** COMMUNICATION SYSTEM, SETTING METHOD, AND PROGRAM

(54) 発明の名称： 通信システム、設定方法及びプログラム

[図1]



2... COMMUNICATION NETWORK
10... TRANSCEIVER STORAGE DEVICE
11... CONTROL SIGNAL TRANSMISSION/RECEPTION UNIT
12,15... MAIN SIGNAL TRANSMISSION/RECEPTION UNIT
13... SWITCH
14... CONTROL UNIT
20... CONTROLLER
30... USER-SIDE CONTROL TERMINAL
40... USER DEVICE
141... RECEPTION CONTROL UNIT
142... LOGIN CONTROL UNIT

(57) **Abstract:** This communication system comprises a reception control unit that constructs a path for a control signal from a controller disposed in a communication network before a main signal between the communication network and a main signal transmission/reception unit is interrupted to permit communication continuity, and a login control unit that enables login from the controller, disables login from a user-side control terminal where a relevant setting of the main signal transmission/reception unit can be changed, cancels interruption and permits communication continuity when login from the user-side control terminal is continuously disabled, and disables login again or causes an interruption again when login from the user-side control terminal is not continuously disabled.

WO 2024/142136 A1

［続葉有］

SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能):ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告(条約第21条(3))

(57) 要約:通信システムは、通信網と主信号送受信部との間の主信号を遮断して通信導通を許可する前に、通信網に配置された制御装置からの制御信号の経路を構築する受信制御部と、制御装置からのログインを有効化し、主信号送受信部の関連設定の変更が可能なユーザ側制御端末からのログインを無効化し、ユーザ側制御端末からのログインの無効化が維持されている場合に遮断を解除し、通信導通を許可し、ユーザ側制御端末からのログインの無効化が維持されていない場合にログインを再び無効化する、又は、再び遮断するログイン制御部とを備える。

明　細　書

発明の名称 ： 通信システム、設定方法及びプログラム

技術分野

[0001] 本発明は、通信システム、設定方法及びプログラムに関する。

背景技術

[0002] ユーザ宅に設置される事業用電気通信設備の一つとして、デジタルコヒーレント通信に用いられるトランシーバを収容した通信装置（トランシーバ収容装置）がある。トランシーバ収容装置は、例えば、ホワイトボックススイッチ（ＷＢＳ：White Box Switch）及びトランスポンダを含むホワイトボックストランスポンダ（White box transponder）である。オープントランスポンダ（Open transponder）とも呼ばれる（例えば、非特許文献１参照）。ホワイトボックススイッチの具体例として、例えば、ガリレオ又はカッシーニがある。

[0003] ホワイトボックススイッチのハードウェアには、装置用ソフトウェア（例えば、ゴールドストーン（Goldstone））が実装される。大容量のコヒーレント光トランシーバとホワイトボックススイッチとが組み合わされることによって、大容量のサービスを提供する通信システム（光伝送システム）が構築される。

先行技術文献

非特許文献

[0004] 非特許文献1：Nishizawa et al., “Open whitebox architecture for smart integration of optical networking and data center technology”,Jocn-13-1-A78.

発明の概要

発明が解決しようとする課題

[0005] トランシーバ収容装置のマネージメントポートを介してログインしたユーザによるトランシーバ収容装置への制御により、電気通信事業者の意図に反

する動作が実行されるおそれがある。電気通信事業者の意図に反する動作とは、例えば、ユーザ宅等に設置されたトランシーバ収容装置や収容されたトランシーバのサービス上変更されては困る予め定められた設定（関連設定）の変更及び読出や、サービス上変更されては困るソフトウェアの書き換え（入替及び追加）である。

[0006] このように、電気通信事業者の意図に反する動作がされてはサービス提供に与える影響を抑制できない問題がある。

[0007] 上記事情に鑑み、本発明は、電気通信事業者の意図に反する動作がサービス提供に与える影響を抑制可能な通信システム、設定方法及びプログラムを提供することを目的としている。

課題を解決するための手段

[0008] 本発明の一態様は、通信網と主信号送受信部との間の主信号の通信導通が許可される前に、前記通信網に配置された制御装置からの制御信号の経路を構築する受信制御部と、前記制御装置からのログインを有効化し、前記主信号送受信部の関連設定の変更が可能なユーザ側制御端末からのログインを無効化し、前記ユーザ側制御端末からのログインの無効化が維持されている場合に前記通信導通を許可し、前記ユーザ側制御端末からのログインの無効化が維持されていない場合に前記ユーザ側制御端末からのログインを再び無効化するログイン制御部とを備える通信システムである。

[0009] 本発明の一態様は、通信システムが実行する設定方法であって、通信網と主信号送受信部との間の主信号の通信導通が許可される前に、前記通信網に配置された制御装置からの制御信号の経路を構築するステップと、前記制御装置からのログインを有効化し、前記主信号送受信部の関連設定の変更が可能なユーザ側制御端末からのログインを無効化し、前記ユーザ側制御端末からのログインの無効化が維持されている場合に前記通信導通を許可し、前記ユーザ側制御端末からのログインの無効化が維持されていない場合に前記ユーザ側制御端末からのログインを再び無効化するステップとを含む設定方法である。

[0010] 本発明の一態様は、コンピュータに、通信網と主信号送受信部との間の主信号の通信導通が許可される前に、前記通信網に配置された制御装置からの制御信号の経路を構築する手順と、前記制御装置からのログインを有効化し、前記主信号送受信部の関連設定の変更が可能なユーザ側制御端末からのログインを無効化し、前記ユーザ側制御端末からのログインの無効化が維持されている場合に前記通信導通を許可し、前記ユーザ側制御端末からのログインの無効化が維持されていない場合に前記ユーザ側制御端末からのログインを再び無効化する手順とを実行させるためのプログラムである。

発明の効果

[0011] 本発明により、電気通信事業者の意図に反する動作がサービス提供に与える影響を抑制可能である。

図面の簡単な説明

[0012] [図1]第１実施形態における、通信システムの構成例を示す図である。

[図2]第１実施形態における、通信システムの動作例を示すフローチャートである。

[図3]第２実施形態における、通信システムの構成例を示す図である。

[図4]第２実施形態における、通信システムの動作例を示すフローチャートである。

[図5]第３実施形態における、通信システムの構成例を示す図である。

[図6]第３実施形態における、通信システムの動作例を示すシーケンス図である。

[図7]各実施形態における、通信システム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

[0013] 本発明の実施形態について、図面を参照して詳細に説明する。

（第１実施形態）

図１は、第１実施形態における、通信システム１の構成例を示す図である。通信システム１は、トランシーバ収容装置１０と、制御装置２０とを備え

る。通信システム１は、例えば、オールフォトニックネットワーク(APN: All-Photonics Network)における光伝送システムである。トランシーバ収容装置１０は、例えば、ユーザ宅に配置される。トランシーバ収容装置１０は、例えば、ホワイトボックストランスポンダである。制御装置２０は、例えば、通信網２に配置される。

[0014] トランシーバ収容装置１０には、ユーザ装置４０が接続される。更に、トランシーバ収容装置１０を制御するために、シリアルバス等のマネージメントポートに、ユーザ側制御端末３０が接続されるおそれがある。接続される恐れがあるのは、シリアルバスに限られない。トランシーバ収容装置１０は、制御信号送受信部１１（制御信号トランシーバ）と、主信号送受信部１２（主信号トランシーバ）と、スイッチ１３と、制御部１４と、主信号送受信部１５とを備える。制御部１４は、受信制御部１４１と、ログイン制御部１４２（検出部）とを備える。

[0015] 受信制御部１４１は、制御装置２０と制御部１４との間、制御部１４と主信号送受信部１２との間、制御部１４内のログイン制御部１４２と主信号送受信部１２との間に、制御信号経路ＳＲを構築する。

[0016] なお、受信制御部１４１は、制御部１４と主信号送受信部１２との間がセキュアな環境である場合、図１に示す主信号送受信部１２と制御部１４内のログイン制御部１４２との間の破線で示す経路においては、制御信号経路ＳＲを構築しなくてもよい。ここで、制御部１４と主信号送受信部１２との間がセキュアな環境とは、少なくとも制御部１４と主信号送受信部１２との間のやり取りがインターセプトされたり、データが改ざんされたりしない環境である。

[0017] なお、受信制御部１４１とログイン制御部１４２とは、制御信号送受信部１１又は主信号送受信部１２に配置されてもよい。この場合、トランシーバ収容装置１０のソフトウェアを介さずに、制御信号送受信部１１又は主信号送受信部１２で閉じて処理できるので、電気通信事業者の意図に反する動作への対応の抜け穴が少なく、電気通信事業者（例えば、認証された制御装置

）の意図に反する動作への対応を早くすることが可能である。

[0018] [認証された制御装置からの制御]

ここで、認証された制御装置からの制御とは、例えば以下に示す認証された制御装置からのいずれかの制御を含む。

・主信号遮断解除（主信号導通）

・主信号遮断（主信号非導通）

・主信号に係る機能部又は装置の給電停止（給電遮断）又は給電（給電許可）

・主信号の波長(光周波数)、波長幅（周波数幅）、偏波、多値度又は伝送方式等の主信号や主信号の品質に関する設定値

・制御対象の主信号自体又はそれとチャネル等を共用するか又は隣接するチャネルを用いる他の主信号や他の主信号の品質に影響を与える設定値、例えば主信号の波長(光周波数)、波長幅(周波数幅)、偏波、多値度又は伝送方式等の主信号や主信号の品質に関する設定値等の設定や設定変更に関する制御を表す。

[0019] ログイン制御部１４２がトランシーバ収容装置１０内にあれば、ローカルユーザのログインの有効無効に関するトランシーバ収容装置１０での対応が早くなる。

受信制御部１４１がトランシーバ収容装置１０内にあれば、通信網２側の制御装置２０との通信の有効無効に関するトランシーバ収容装置１０での対応が早くなる。

ログイン制御部１４２がトランシーバ収容装置１０内にあれば、通信網２側のローカルユーザのログインの有効無効に関する通信網２での対応が早くなる。

[0020] トランシーバ収容装置１０は、例えばホワイトボックススイッチにソフトウェア（アプリケーション）がインストール（実装）されることによって機能する。トランシーバ収容装置１０は、通信網２（例えば、制御装置２０）との間で、光通信を実行する。制御部１４上で実行されるソフトウェアには

、例えば、通常のホワイトボックススイッチのＮＯＳ（Network Operating System）及び装置用ソフトウェア（例えば、ゴールドストーン）等と、ログイン制限機能等のソフトウェアとが含まれる。

[0021] 以下の説明において、第１の実施形態、第２実施形態及び第３の実施形態では、ホワイトボックススイッチのＮＯＳと及び装置用ソフトウェア等がホワイトボックススイッチにインストールされている構成を例に説明する。第４の実施形態では、さらに、ゴールドストーンが、ホワイトボックススイッチにインストールされている構成を例に説明する。

[0022] 制御装置２０は、例えば、フォトニックゲートウェイである。制御装置２０は、例えば、フォトニックゲートウェイのコントローラでもよい。制御装置２０は、トランシーバ収容装置１０に備えられた主信号送受信部１２のサービス上変更されては困る予め定められた設定（関連設定）（例えば、主信号の光信号の波長の設定）を制御する。例えば、制御装置２０は、トランシーバ収容装置１０宛に制御信号を送信することによって、主信号送受信部１２の設定等を制御する。さらに、その応答を受信することにより、制御された設定等を確認してもよい。主信号送受信部１２の設定等の制御内容として、例えば、主信号送受信部１２の起動、停止もしくは再起動と、所定のパラメータの設定、変更及び削除と、主信号の送信開始もしくは停止ととが挙げられる。

[0023] ユーザ側制御端末３０は、例えば、情報処理装置（例えば、パーソナルコンピュータ）である。ユーザ側制御端末３０は、例えば、トランシーバ収容装置１０が設置されたユーザ宅のユーザによって操作される。トランシーバ収容装置１０に例えばトランシーバ収容装置１０のローカルアカウントでログインしたユーザ側制御端末３０からログインしたユーザは、ローカルアカウントが有効である場合には、トランシーバ収容装置１０に備えられた主信号送受信部１２の所定の関連設定を変更することが可能である。ユーザ側制御端末３０は、ユーザが利用するトランシーバ収容装置１０のアカウント例えばローカルアカウントが無効である場合には、トランシーバ収容装置１０

及びそれに備えられた主信号送受信部１２の所定の関連設定を変更することができない。

[0024] ユーザによって操作されたユーザ側制御端末３０が主信号送受信部１２の設定を変更する動作には、電気通信事業者の意図に反する動作（例えば、主信号送受信部１２（トランシーバ）の関連設定の変更及び読出、及び、関連するソフトウェアの書き換え（入替及び追加））が含まれることがある。

[0025] ユーザ装置４０は、対向装置（不図示）との間で、通信網２及びトランシーバ収容装置１０を介して、主信号の通信（送受信）を実行する。ユーザ装置４０は、例えば、顧客構内設備(CPE : Customer Premises Equipment)である。ユーザ装置４０は、トランシーバ収容装置１０においてユーザ側と主信号を通信（送受信）する主信号送受信部１５に接続される。

[0026] 次に、トランシーバ収容装置１０の具体的な構成について説明する。

制御信号送受信部１１は、制御信号用のトランシーバである。制御信号送受信部１１は、通信網２内の制御装置２０との間で、光信号を用いて、制御信号を通信（送受信）してもよい。信号は光信号に限られない。通信網２を介さずに、別の通信網（不図示）を介してもよい。通信網２と制御信号送受信部１１とスイッチ１３とを介した接続に限られない。制御信号送受信部１１は、別の通信網（不図示）につながるドングル等を介して、トランシーバ収容装置１０のマネージメントポートから接続してもよい。制御装置２０から送信される制御信号には、トランシーバ収容装置１０の設定の変更を指示するための情報が含まれる。

[0027] なお、制御信号送受信部１１と、通信網内の制御装置２０との間で送受信される制御信号は、電気信号であってもよいし、光信号であってもよい。制御信号が、主信号と波長分割多重される場合には、制御信号は光信号である。

[0028] 制御装置２０から送信される制御信号には、トランシーバ収容装置１０の主信号送受信部１２の所定のパラメータを指示する情報が含まれる。主信号送受信部１２の所定のパラメータとは、例えば（発光又は消光、（例えば、tx

-dis false/true)、光強度、波長(例えば、波長グリッド(100-ghz|50-ghz|33-ghz|25-ghz|12-5-ghz|6-25-ghz 等）、光周波数、チャネル番号）等である。主信号送受信部１２の所定のパラメータには、伝送フォーマット(例えば、bpsk|dp-bpsk|qpsk|dp-qpsk|8-qam|dp-8-qam|16-qam|dp-16-qam|32-qam|dp-32-qam|64-qam|dp-64-qam等)、ラインレート(例えば、100g|200g|300g|400g等)、前方誤り訂正(FEC : forward error correction)タイプ(例えば、ｓｃ(Staircase)－ｆｅｃ｜ｃ(Concatenated)ｆｅｃ｜ｏ(Open)ｆｅｃ等)等の情報が含まれてもよい。

[0029] 制御信号送受信部１１は、制御信号が光信号である場合には、受信された制御信号を電気信号に変換して、電気信号をスイッチ１３に出力する。通信網２内の制御装置２０との間で信号（例えば、光信号）をやり取りし、スイッチ１３を介して受信制御部１４１に接続する制御信号送受信部１１が、図１に例示されている。トランシーバ収容装置１０のマネージメントポートが、シリアルポート、ＵＳＢ（Universal Serial Bus）、又は、Ethernet（登録商標）インタフェースである場合、制御信号送受信部１１は、シリアルポート、ＵＳＢ、又は、Ethernet（登録商標）インタフェースに接続し、通信網２側の制御装置２０と通信しうる、取替可能なトランシーバ又はドングルでもよい。

[0030] 主信号送受信部１２は、主信号用のトランシーバである。主信号送受信部１２は、通常、取替可能なトランシーバである。主信号送受信部１２は、通信網２との間で、光信号等を用いて、主信号を通信（送受信）する。主信号送受信部１２は、通信網２内の制御装置２０との間で、光信号を用いて、主信号又は制御信号を通信（送受信）してもよい。

[0031] 主信号送受信部１２がアナログコヒーレント光学系（ACO :Analogue Coherent Optics)トランシーバである場合、制御信号送受信部１１とスイッチ１３との間、及び、主信号送受信部１２とスイッチ１３との間には、デジタル信号処理部（不図示）が備えられてもよい。このデジタル信号処理部（不図示）は、例えば、制御信号送受信部１１又は主信号送受信部１２から出力され

た電気信号に対して、例えば、ＯＴＮ(Optical Transport Network) フレーミング及びFEC処理等の誤り訂正等の信号処理を実行する。

[0032] 主信号送受信部１２がデジタルコヒーレント光学系（DCO : Digital Coherent Optics)トランシーバである場合、主信号送受信部１２は、デジタル信号処理部を備えてもよい。主信号送受信部１２のデジタル信号処理部は、例えば、ＯＴＮフレーミング、FEC処理、変復調処理及び光学劣化補正等を実行する。

[0033] 以下の説明では、制御信号送受信部１１の信号と主信号送受信部１２の信号とは、例えば、波長分割多重等で多重される。多重された信号は、例えば、同一芯線（例えば、光ファイバ等の伝送路）で伝送される。

[0034] 主信号送受信部１５は、ユーザ装置４０との間で主信号を通信（送受信）する。主信号送受信部１５は、トランシーバ、又は、ＮＩＣ(Network Interface Card)である。

[0035] スイッチ１３は、制御信号送受信部１１と制御部１４とを接続する。また、スイッチ１３は、主信号かそれを伝送するフレームやＡＭＣＣで制御信号を通信する場合、主信号送受信部１２と制御部１４とを接続する。例えば、スイッチ１３は、主信号送受信部１２と主信号送受信部１５とを接続することで、主信号を導通させる。例えば、スイッチ１３は、制御信号送受信部１１と制御部１４とを接続することで、制御装置２０から送信された制御信号を制御部１４に転送する。このように、スイッチ１３は、制御装置２０から送信された制御信号を制御部１４に渡すためのアダプタとしても機能する。

[0036] 制御部１４は、トランシーバ収容装置１０の各機能部を制御する。制御部１４は、少なくとも主信号送受信部１２に関する制御を実行する。制御部１４は、ＣＰＵ（Central Processing Unit）等の１以上のプロセッサと１以上のメモリとを用いて構成される。制御部１４は、１以上のプロセッサがプログラムを実行することによって、受信制御部１４１とログイン制御部１４２との機能を実現する。ここで、制御部１４の機能の全て又は一部は、ＡＳＩＣ（Application Specific Integrated Circuit）やＰＬＤ（Programmable L

ogic Device）やＦＰＧＡ（Field Programmable Gate Array）等のハードウェアを用いて実現されても良い。上記のプログラムは、コンピュータ読み取り可能な記録媒体に記録されても良い。コンピュータ読み取り可能な記録媒体とは、例えばフレキシブルディスク、光磁気ディスク、ＲＯＭ（Read Only Memory）、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、半導体記憶装置（例えばＳＳＤ：Solid State Drive）等の可搬媒体、コンピュータシステムに内蔵されるハードディスクや半導体記憶装置等の記憶装置である。上記のプログラムは、電気通信回線を介して送信されてもよい。

[0037] 制御部１４は、ユーザ装置４０と主信号送受信部１２と通信網２との間の主信号の通信導通が許可される前に、制御信号送受信部１１及びスイッチ１３を介して、制御装置２０との間に制御信号経路ＳＲを構築することが望ましい。更に、制御信号経路ＳＲを構築するだけでなく、所定の設定に関し、受信制御部１４１からの制御のみを受ける制御部１４とされた後に許可することが、より望ましい。いずれかが未了で許可すると、意図しない主信号が導通するおそれがあるからである。このように、制御部１４は、ログインが制限されてから、主信号の通信導通を許可する。但し、後述の遮断部で予め遮断している場合には、その限りでない。制御信号経路ＳＲは、主信号送受信部１２に関する設定の変更、又は、読み出しを制限すべき所定の関連設定へのアクセスを可能とする。ここで、制御信号経路ＳＲは、セキュリティが高い通信経路であることが望ましいが、関連設定へのアクセスを可能とする制御信号経路であればよい。制御信号経路ＳＲのセキュリティは、必ずしも高くなくてよい。セキュリティが高い通信経路とは、例えば、仮想プライベートネットワーク（VPN：Virtual Private Network）である。これによって、制御の通信内容をユーザに対して秘匿することが可能である。

[0038] 制御信号経路ＳＲとは、ＶＰＮ等のセキュリティが高い通信経路であることが望ましいが、関連設定へのアクセスを可能とする制御信号経路であって、認証されていない装置（例えば、ユーザ側制御端末３０）からトランシーバ収容装置１０が備える機能部（例えば、受信制御部１４１及びログイン制

御部１４２）へのアクセスができないようになっていればよく、必ずしもセキュリティが高い通信経路である必要はない。このような制御信号経路ＳＲを用いることで、悪意のあるユーザによって機能部間のやり取りがインターセプトされたり、改ざんされたりしてしまうことを防ぐことができる。

[0039] また、受信制御部１４１は、設定状態(設定実行完了又は設定値)を、制御装置２０に通知又は応答する。

[0040] 受信制御部１４１は、所定のクライアント信号、制御信号用ＧＣＣチャネル、又は、ＡＭＣＣ（Auxiliary Management and Control Channel）等を用いて、主信号送受信部１２との間で関連設定を通信してもよい。この場合、受信制御部１４１は、主信号送受信部１２と制御装置２０との間に、制御信号経路ＳＲを構築してもよい。主信号送受信部１２と制御装置２０との間に制御信号経路ＳＲが構築される場合、受信制御部１４１は、トランシーバ収容装置１０と対向装置（不図示）との間の通信導通が許可された後に、制御信号経路ＳＲを構築する。なお、例えば制御信号がユーザ信号にフレーム多重される形式で、又は、例えばユーザ信号を運ぶフレーム（例えば、ＧＣＣ（Generic Communications Channel））等の形式で、制御信号が時分割多重されていない場合には、スイッチ１３によって、又は、スイッチ１３以外の所定の機能部によって、ユーザ信号は廃棄されてもよい。

[0041] ログイン制御部１４２は、ログインを制御するが、必ずしもパラメータを設定しなくてよい。ログイン制御部１４２は、制御装置２０からのログイン（管理者権限等）を、ユーザ側制御端末３０を介したユーザ（ローカル）に対して隠ぺいされた条件下で有効化する。また、ログイン制御部１４２は、ローカルアカウント等を用いて主信号送受信部１２の関連設定を変更及び読出することが可能なユーザ側制御端末３０からのログインを、ユーザ側制御端末３０に対して隠ぺいされた条件下で無効化する。

[0042] 受信制御部１４１は、ユーザ側制御端末３０以外からの制御信号（指示）に従って、主信号送受信部１２のパラメータを設定する。例えば、受信制御部１４１は、制御装置２０からの制御信号（指示）のみに従って、主信号送

受信部１２の設定を実行する。ここで、ログイン制御部１４２は、主信号送受信部１２のログインに係る設定以外の所定の関連設定の変更及び読出を、制御装置２０からの制御信号のみに基づいて実行する。

[0043] 第１実施形態では、制御部１４のログイン制御部１４２は、ユーザ側制御端末３０からのログインの無効化が維持されているか否か（ログインの制限が維持されているか否か）を、例えば、標準出力への出力及びログ等に基づいて検出（判定）してもよい。

[0044] 上記では、アカウントのＩＤ及びパスワード等の無効を中心に説明されているが、ユーザがログインし難くするアクセス制限では、例えば、主信号送受信部１２の所定状態を制御し得る信号経路が不通となる。ログイン制御部１４２は、このような信号経路を同定するためのアドレスを、ユーザ側制御端末３０に与えないようにしてもよい。ログイン制御部１４２は、ユーザにアドレスを与えないようにすると共に、アドレスを同定するユーザからの問い合わせ（例えば、「ping」）に対して応答しないようにしてもよい。ログイン制御部１４２は、辞書攻撃があった場合には、その辞書攻撃があったことを検出してもよい。ログイン制御部１４２は、トランシーバ収容装置１０のマネージメントポートで受信制御部１４１が制御情報をやりとりしない場合、トランシーバ収容装置１０のマネージメントポート等の特定のポート（例えば、シリアルポート）等からのアクセスを許容しないようにしてもよい。ログイン制御部１４２は、制御信号としてテレタイプ(tty）等を使わない場合、tty等からのユーザセッション（アクセス）を許容しないようにしてもよい。

[0045] 次に、通信システム１の動作例を説明する。通信システム１は、まず、ユーザ側制御端末３０からのログイン無効化と、通信網からの遠隔有効化を行う。次に、行った無効化又は有効化ができなくなった場合に無効化と有効化を再び行う例を示す。

図２は、第１実施形態における、通信システム１の動作例を示すフローチャートである。受信制御部１４１は、主信号送受信部１２と通信網２との間

の主信号の通信導通が許可される前に、制御装置２０からの制御信号の制御信号経路ＳＲを構築する（ステップＳ００１）。

[0046] ログイン制御部１４２は、制御装置２０からのログインを有効化する。ログイン制御部１４２は、主信号送受信部１２の関連設定を変更及び読出することが可能なユーザ側制御端末３０からのログインを無効化する（ステップＳ００２）。無効化として、ＩＤの情報の無効化及び削除と、パスワードの変更とがある。無効化に際し、特に無効化対象としたログインのセッションが残っていれば、通信断にしたほうがよい。

[0047] ログイン制御部１４２は、主信号送受信部１２の所定の関連設定の変更及び読出を、制御信号のみに基づいて実行する（ステップＳ００３）。ログイン制御部１４２は、ユーザ側制御端末３０からのログインの無効化が維持されているか否かを判定する（ステップＳ００４）。ユーザ側制御端末３０からのログインの無効化が維持されている場合（ステップＳ００４：ＹＥＳ）、ログイン制御部１４２は、主信号送受信部１２と通信網２との間の通信導通を許可、又は許可し続ける（ステップＳ００５）。ログイン制御部１４２は、ステップＳ００４に処理を戻す。

[0048] トランシーバ収容装置１０から異常のアラームをあげるが、通信網側の制御装置２０でトランシーバ収容装置１０とのやり取りが正常にできないことや、通信網への異常なトラフィック流入を契機に有効無効を判定してもよい。異常なトラフィックとは、所定の関連設定の値に不適合なトラフィックである。例えば、関連設定の値が波長であれば、不適切な波長の信号、強度であれば、不適切に高強度や低強度の信号である。さらに、制御装置２０から送信された設定の指示を含む制御信号を受信、又は、スヌーピング等で得た設定の情報を保持し、その保持した設定の情報を、設定、設定確認等ができないこと、設定異常の通知や検出、通信網の経路（例えば、制御信号経路ＳＲ以外の経路）以外から設定を書き換えられたこと、書き換えようとする現象が発生したことを契機に有効無効を判定してもよい。

[0049] ユーザ側制御端末３０からのログインの無効化が維持されていない場合（

ステップＳ００４：ＮＯ）、ログイン制御部１４２は、ユーザ側制御端末３０からのログインを再び無効化する（ステップＳ００６）。ログイン制御部１４２は、ステップＳ００４に処理を戻す。

[0050] なお、ログインを変更するステップが、ユーザ側制御端末３０の機器認証処理の前又は後に追加されてもよい。また、その機器認証処理の一部として、ログインを変更するステップが追加されてもよい。

[0051] 以上のように、受信制御部１４１は、主信号送受信部１２と通信網２との間の主信号を遮断して通信導通を許可する前に、通信網２に配置された制御装置２０からの制御信号の制御信号経路ＳＲを構築する。制御信号経路ＳＲは、例えば、制御装置２０と受信制御部１４１との間に構築される。

[0052] ログイン制御部１４２は、制御装置２０からのログインを有効化する。ログイン制御部１４２は、主信号送受信部１２の関連設定を変更及び読出することが可能なユーザ側制御端末３０からのログインを無効化する。ログイン制御部１４２は、ユーザ側制御端末３０からのログインの無効化が維持されている場合に、通信網２と主信号送受信部１２との間の遮断を解除して、主信号の通信導通を許可する。ログイン制御部１４２は、ユーザ側制御端末３０からのログインの無効化が維持されていない場合に、主信号送受信部１２の関連設定を変更及び読出することが可能なユーザ側制御端末３０からのログインを再び無効化する、又は、再び遮断する。

[0053] これによって、電気通信事業者の意図に反する動作（ユーザが操作すべきでない変更）がサービス提供に与える影響を抑制可能である。ここで、トランシーバ収容装置１０の改造の規模は小さい。

[0054] 電気通信事業者の意図に反する動作以外については、ユーザによる制御が可能でもよい。ログイン制御部１４２等が制御信号送受信部１１又は主信号送受信部１２にソフトウェア等で実装された場合と比較して、制御部１４への実装では演算リソースがより豊富であることから、高度な制御が可能である。また、制御の入替も容易であり、第３実施形態（後述）と比較して早く応答することが可能である。さらに、通信網２とのやりとりを頻繁に実行す

ることなく対応が可能である。

[0055] （第１実施形態の変形例）

ログイン制御部１４２は、トランシーバ収容装置１０における既存のセッションを消去してから、ユーザ側制御端末３０からのログインを、ユーザ側制御端末３０にとって未知の値に変更してもよい。ここで、受信制御部１４１及びログイン制御部１４２は、セキュリティが高い制御信号経路ＳＲと制御信号経路ＳＲとを経由したセッションのうちで、セキュリティが高い制御信号経路ＳＲを経由したセッションを残す。これよって、変更後のログイン（ユーザ側制御端末３０にとって未知の値）をユーザ側制御端末３０が入手することを回避することが可能である。

[0056] （第２実施形態）

第２実施形態では、制御部が遮断部を備える点が、第１実施形態との差分である。

[0057] 図３は、第２実施形態における、通信システム１ａの構成例を示す図である。通信システム１ａは、トランシーバ収容装置１０ａと、制御装置２０ａとを備える。通信システム１ａは、例えば、オールフォトニックネットワーク(APN)における光伝送システムである。トランシーバ収容装置１０ａは、例えば、ユーザ宅に配置される。トランシーバ収容装置１０ａは、例えば、ホワイトボックストランスポンダである。制御装置２０ａは、例えば、通信網２に配置される。

[0058] トランシーバ収容装置１０ａには、ユーザ装置４０が接続される。更に、トランシーバ収容装置１０を制御するために、シリアルバス等のマネージメントポートに、ユーザ側制御端末３０が接続されおそれがある。接続される恐れがあるのは、シリアルバスに限られない。トランシーバ収容装置１０ａは、制御信号送受信部１１（制御信号トランシーバ）と、主信号送受信部１２（主信号トランシーバ）と、スイッチ１３と、制御部１４ａと、主信号送受信部１５とを備える。制御部１４ａは、受信制御部１４１と、ログイン制御部１４２（検出部）と、遮断部１４３（遮断部）とを備える。

[0059] 受信制御部１４１は、制御装置２０ａと制御部１４ａとの間、制御部１４ａと主信号送受信部１２との間、制御部１４ａ内のログイン制御部１４２と遮断部１４３との間、制御部１４ａ内の遮断部１４３と主信号送受信部１２との間に制御信号経路ＳＲを構築する。なお、受信制御部１４１は、制御部１４ａ内がセキュアな環境である場合、制御部１４ａ内のログイン制御部１４２と遮断部１４３との間の破線で示す経路においては、制御信号経路ＳＲを構築しなくてもよい。

[0060] なお、受信制御部１４１は、制御部１４ａと主信号送受信部１２との間がセキュアな環境である場合、図３に示す主信号送受信部１２と制御部１４ａ内の遮断部１４３との間の破線で示す経路においては、制御信号経路ＳＲを構築しなくてもよい。ここで、制御部１４ａと主信号送受信部１２との間がセキュアな環境とは、少なくとも制御部１４ａと主信号送受信部１２との間のやり取りがインターセプトされたり、データが改ざんされたりしない環境である。

[0061] なお、受信制御部１４１とログイン制御部１４２と遮断部１４３とは、制御信号送受信部１１又は主信号送受信部１２に配置されてもよい。この場合、トランシーバ収容装置１０のソフトウェアを介さずに、制御信号送受信部１１又は主信号送受信部１２で閉じて処理できるので、電気通信事業者の意図に反する動作への対応の抜け穴が少なく、電気通信事業者の意図に反する動作への対応を早くすることが可能である。

[0062] ログイン制御部１４２がトランシーバ収容装置１０ａ内にあれば、ローカルユーザのログインの有効無効に関するトランシーバ収容装置１０ａでの対応が早くなる。

受信制御部１４１がトランシーバ収容装置１０ａ内にあれば、通信網２側の制御装置２０との通信の有効無効に関するトランシーバ収容装置１０ａでの対応が早くなる。

遮断部１４３とログイン制御部１４２がトランシーバ収容装置１０ａ内にあれば、ローカルユーザのログインの有効無効に関するトランシーバ収容装

置１０ａでの対応が早くなる。

遮断部１４３と受信制御部１４１がトランシーバ収容装置１０内にあれば、通信網２側の制御装置２０との通信の有効無効に関するトランシーバ収容装置１０ａでの対応が早くなる。

ログイン制御部１４２がトランシーバ収容装置１０ａ内にあれば、通信網２側のローカルユーザのログインの有効無効に関する通信網２での対応が早くなる。

遮断部１４３とログイン制御部１４２がトランシーバ収容装置１０ａ内にあれば、通信網２側のローカルユーザのログインの有効無効に関する通信網２での対応が早くなる。

[0063] トランシーバ収容装置１０ａは、例えばホワイトボックススイッチにソフトウェア（アプリケーション）がインストール（実装）されることによって機能する。トランシーバ収容装置１０ａは、通信網２（例えば、制御装置２０ａ）との間で、光通信を実行する。制御部１４ａ上で実行されるソフトウェアには、例えば、通常のホワイトボックススイッチのＮＯＳ及び装置用ソフトウェア（例えば、ゴールドストーン）等と、ログイン制限機能等のソフトウェアとが含まれる。

[0064] 制御装置２０ａは、例えば、フォトニックゲートウェイである。制御装置２０ａは、例えば、フォトニックゲートウェイのコントローラでもよい。制御装置２０ａは、トランシーバ収容装置１０ａに備えられた主信号送受信部１２のサービス上変更されては困る予め定められた設定（関連設定）（例えば、主信号の光信号の波長）を制御する。例えば、制御装置２０ａは、トランシーバ収容装置１０ａ宛に制御信号を送信することによって、主信号送受信部１２の設定等を制御する。さらに、その応答を受信することにより、制御された設定等を確認してもよい。主信号送受信部１２の設定等の制御内容として、例えば、主信号送受信部１２の起動、停止もしくは再起動と、所定のパラメータの設定、変更及び削除と、主信号の送信開始もしくは停止と、遮断とが挙げられる。ユーザ信号（主信号）の遮断とは、例えば、主信号送

受信部１２の送信停止、出力強度低減、主信号送受信部１２の停止、再起動又は電源断と、スイッチ１３等の内部の主信号導通の遮断と、トランシーバ収容装置１０ａの電源断と、通信網側での遮断とである。

[0065] ユーザ側制御端末３０は、例えば、情報処理装置（例えば、パーソナルコンピュータ）である。ユーザ側制御端末３０は、例えば、トランシーバ収容装置１０ａが設置されたユーザ宅のユーザによって操作される。トランシーバ収容装置１０ａに例えばトランシーバ収容装置１０ａのローカルアカウントでログインしたユーザ側制御端末３０からログインしたユーザは、ローカルアカウントが有効である場合には、トランシーバ収容装置１０ａに備えられた主信号送受信部１２の所定の関連設定を変更することが可能である。ユーザ側制御端末３０は、ユーザが利用するトランシーバ収容装置１０ａのアカウント例えばローカルアカウントが無効である場合には、トランシーバ収容装置１０ａ及びそれに備えられた主信号送受信部１２の所定の関連設定を変更することができない。

[0066] ユーザによって操作されたユーザ側制御端末３０が主信号送受信部１２の設定を変更する動作には、電気通信事業者の意図に反する動作（例えば、主信号送受信部１２（トランシーバ）の関連設定の変更及び読出、及び、関連するソフトウェアの書き換え（入替及び追加））が含まれることがある。

[0067] ユーザ装置４０は、対向装置（不図示）との間で、通信網２及びトランシーバ収容装置１０ａを介して、主信号の通信（送受信）を実行する。ユーザ装置４０は、例えば、顧客構内設備(CPE)である。ユーザ装置４０は、トランシーバ収容装置１０ａにおいてユーザ側と主信号を通信（送受信）する主信号送受信部１５に接続される。

[0068] 次に、トランシーバ収容装置１０ａの具体的な構成について説明する。

制御信号送受信部１１は、制御信号用のトランシーバである。制御信号送受信部１１は、通信網２内の制御装置２０ａとの間で、光信号を用いて、制御信号を通信（送受信）してもよい。信号は光信号に限られない。通信網２を介さずに、別の通信網（不図示）を介してもよい。通信網２と制御信号送

受信部１１とスイッチ１３とを介した接続に限られない。制御信号送受信部１１は、別の通信網（不図示）につながるドングル等を介して、トランシーバ収容装置１０ａのマネージメントポートから接続してもよい。制御装置２０ａから送信される制御信号には、トランシーバ収容装置１０ａの設定の変更を指示するための情報が含まれる。

[0069] なお、制御信号送受信部１１と、通信網内の制御装置２０ａとの間で送受信される制御信号は、電気信号であってもよいし、光信号であってもよい。制御信号が、主信号と波長分割多重される場合には、制御信号は光信号である。

[0070] 制御装置２０ａから送信される制御信号には、トランシーバ収容装置１０ａの主信号送受信部１２の所定のパラメータを指示する情報が含まれる。主信号送受信部１２の所定のパラメータとは、例えば（発光又は消光、光強度、波長）等である。主信号送受信部１２の所定のパラメータには、伝送フォーマット、ラインレート等の情報が含まれてもよい。

[0071] 制御信号送受信部１１は、制御信号が光信号である場合には、受信された制御信号を電気信号に変換して、電気信号をスイッチ１３に出力する。通信網２内の制御装置２０ａとの間で信号（例えば、光信号）をやり取りし、スイッチ１３を介して受信制御部１４１に接続する制御信号送受信部１１が、図３に例示されている。トランシーバ収容装置１０ａのマネージメントポートが、シリアルポート、ＵＳＢ、又は、Ethernet（登録商標）インタフェースである場合、制御信号送受信部１１は、シリアルポート、ＵＳＢ、又は、Ethernet（登録商標）インタフェースに接続し、通信網２側の制御装置２０ａと通信しうる、取替可能なトランシーバ又はドングルでもよい。

[0072] 主信号送受信部１２は、主信号用のトランシーバである。主信号送受信部１２は、通常、取替可能なトランシーバである。主信号送受信部１２は、通信網２との間で、光信号等を用いて、主信号を通信（送受信）する。主信号送受信部１２は、通信網２内の制御装置２０ａとの間で、光信号を用いて、主信号又は制御信号を通信（送受信）してもよい。

[0073] 主信号送受信部１２がアナログコヒーレント光学系（ACO)トランシーバである場合、制御信号送受信部１１とスイッチ１３との間、及び、主信号送受信部１２とスイッチ１３との間には、デジタル信号処理部（不図示）が備えられてもよい。このデジタル信号処理部（不図示）は、例えば、制御信号送受信部１１又は主信号送受信部１２から出力された電気信号に対して、例えば、ＯＴＮフレーミング及びFEC処理等の誤り訂正等の信号処理を実行する。

[0074] 主信号送受信部１２がデジタルコヒーレント光学系（DCO)トランシーバである場合、主信号送受信部１２は、デジタル信号処理部を備えてもよい。主信号送受信部１２のデジタル信号処理部は、例えば、光伝送網フレーミング、前方誤り訂正処理、変復調処理及び光学劣化補正等を実行する。

[0075] 主信号送受信部１５は、ユーザ装置４０との間で主信号を通信（送受信）する。主信号送受信部１５は、トランシーバ、又は、ＮＩＣである。

[0076] スイッチ１３は、制御信号送受信部１１と制御部１４ａとを接続する。また、スイッチ１３は、主信号かそれを伝送するフレームやＡＭＣＣで制御信号を通信する場合、主信号送受信部１２と制御部１４ａとを接続する。例えば、スイッチ１３は、主信号送受信部１２と主信号送受信部１５とを接続することで、主信号を導通させる。例えば、スイッチ１３は、制御信号送受信部１１と制御部１４ａとを接続することで、制御装置２０ａから送信された制御信号を制御部１４ａに転送する。このように、スイッチ１３は、制御装置２０ａから送信された制御信号を制御部１４ａに渡すためのアダプタとしても機能する。

[0077] 制御部１４ａは、トランシーバ収容装置１０ａの各機能部を制御する。制御部１４ａは、少なくとも主信号送受信部１２に関する制御を実行する。制御部１４ａは、ＣＰＵ等の１以上のプロセッサと１以上のメモリとを用いて構成される。制御部１４ａは、１以上のプロセッサがプログラムを実行することによって、受信制御部１４１とログイン制御部１４２と遮断部１４３との機能を実現する。ここで、制御部１４ａの機能の全て又は一部は、ＡＳＩＣやＰＬＤやＦＰＧＡ等のハードウェアを用いて実現されても良い。上記の

プログラムは、コンピュータ読み取り可能な記録媒体に記録されても良い。コンピュータ読み取り可能な記録媒体とは、例えばフレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ、半導体記憶装置（例えば、ＳＳＤ）等の可搬媒体、コンピュータシステムに内蔵されるハードディスクや半導体記憶装置等の記憶装置である。上記のプログラムは、電気通信回線を介して送信されてもよい。

[0078] 制御部１４ａは、ユーザ装置４０と主信号送受信部１２と通信網２との間の主信号の通信導通が許可される前に、制御信号送受信部１１及びスイッチ１３を介して、制御装置２０ａとの間に制御信号経路ＳＲを構築することが望ましい。更に、制御信号経路ＳＲを構築するだけでなく、所定の設定に関し、受信制御部１４１からの制御のみを受ける制御部１４ａとされた後に許可することが、より望ましい。いずれかが未了で許可すると、意図しない主信号が導通するおそれがあるからである。このように、制御部１４ａは、ログインが制限されてから、主信号の通信導通を許可する。但し、後述の遮断部で予め遮断している場合には、その限りでない。制御信号経路ＳＲは、主信号送受信部１２に関する設定の変更、又は、読み出しを制限すべき所定の関連設定へのアクセスを可能とする。ここで、制御信号経路ＳＲは、セキュリティが高い通信経路であることが望ましいが、関連設定へのアクセスを可能とする制御信号経路であればよい。制御信号経路ＳＲのセキュリティは、必ずしも高くなくてよい。セキュリティが高い通信経路とは、例えば、仮想プライベートネットワーク（VPN）である。これによって、制御の通信内容をユーザに対して秘匿することが可能である。

[0079] また、受信制御部１４１は、設定状態(設定実行完了又は設定値)を、制御装置２０ａに通知又は応答する。

[0080] 受信制御部１４１は、所定のクライアント信号、制御信号用ＧＣＣチャネル、又は、ＡＭＣＣ等を用いて、主信号送受信部１２との間で関連設定を通信してもよい。この場合、受信制御部１４１は、主信号送受信部１２と制御装置２０ａとの間に、制御信号経路ＳＲを構築してもよい。主信号送受信部

１２と制御装置２０ａとの間に制御信号経路ＳＲが構築される場合、受信制御部１４１は、トランシーバ収容装置１０ａと対向装置（不図示）との間の通信導通が許可された後に、制御信号経路ＳＲを構築する。なお、例えば制御信号がユーザ信号にフレーム多重される形式で、又は、例えばユーザ信号を運ぶフレーム（例えば、ＧＣＣ）等の形式で、制御信号が時分割多重されていない場合には、スイッチ１３によって、又は、スイッチ１３以外の所定の機能部によって、ユーザ信号は廃棄されてもよい。

[0081] ログイン制御部１４２は、ログインを制御するが、必ずしもパラメータを設定しなくてよい。ログイン制御部１４２は、制御装置２０ａからのログイン（管理者権限等）を、ユーザ側制御端末３０を介したユーザ（ローカル）に対して隠ぺいされた条件下で有効化する。また、ログイン制御部１４２は、ローカルアカウント等を用いて主信号送受信部１２の関連設定を変更及び読出することが可能なユーザ側制御端末３０からのログインを、ユーザ側制御端末３０に対して隠ぺいされた条件下で無効化する。

[0082] ユーザ側制御端末３０以外からの制御信号（指示）に従って、受信制御部１４１又は制御装置２０ａが、主信号送受信部１２のパラメータを設定する。例えば、ログイン制御部１４２は、制御装置２０ａからの制御信号（指示）のみに従って、主信号送受信部１２の設定を実行する。ここで、ログイン制御部１４２は、主信号送受信部１２のログインに係る設定以外の所定の関連設定の変更及び読出を、制御装置２０ａからの制御信号のみに基づいて実行する。

[0083] 第２実施形態では、制御部１４ａのログイン制御部１４２は、ユーザ側制御端末３０からのログインの無効化が維持されているか否か（ログインの制限が維持されているか否か）を、例えば、標準出力への出力及びログ等に基づいて検出（判定）する。

[0084] ログイン制御部１４２又は遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されている場合、主信号送受信部１２と通信網２との間の通信導通を許可する。遮断部１４３は、ユーザ側制御端末３０からの

ログインの無効化が維持されている場合、主信号送受信部１２と通信網２との間の通信導通の遮断を解除する。

[0085] 遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されていない場合、主信号送受信部１２と通信網２との間の通信導通を遮断する。ログイン制御部１４２又は遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されていない場合、主信号送受信部１２と通信網２との間の通信導通の許可を取り消してもよい。

[0086] 遮断部１４３は、主信号送受信部１２と通信網２内の制御装置２０ａとの間の導通を遮断する。遮断部１４３は、トランシーバ収容装置１０ａから異常のアラームをあげるが、通信網側の制御装置２０ａでトランシーバ収容装置１０ａとのやり取りが正常にできないことや、通信網への異常なトラフィック流入を契機に遮断してもよい。異常なトラフィックとは、所定の関連設定の値に不適合なトラフィックである。例えば、関連設定の値が波長であれば、不適切な波長の信号、強度であれば、不適切に高強度や低強度の信号である。さらに、遮断部１４３は、制御装置２０ａから送信された設定の指示を含む制御信号を受信、又は、スヌーピング等で得た設定の情報を保持し、その保持した設定の情報を、設定、設定確認等ができないこと、設定異常の通知や検出、通信網の経路（例えば、制御信号経路ＳＲ以外の経路）以外から設定を書き換えられたこと、書き換えようとする現象が発生したことを契機に遮断してもよい。さらに、遮断部１４３は、設定の通知や応答がない場合に遮断してもよいし、設定の失敗や異常の場合に遮断してもよい。

[0087] 例えば、遮断部１４３は、主信号送受信部１２のレジスタ等への書込みによって、主信号送受信部１２（トランシーバ）の光出力を、無視できるレベルまで落してもよい。遮断部１４３は、ハードウェアのピンへの入力に関して、光信号の送信をオフにしてもよい。遮断部１４３は、主信号送受信部１２（トランシーバ）への給電を落としてもよい。遮断部１４３は、トランシーバ収容装置１０ａの電源を落としてもよい。通信網２側で、信号が遮断されてもよい。遮断部１４３は、「Keep Alive」信号又は「Health check」信

号のような信号を通信網２（フォトニック・ゲートウェイ）との間でやり取りした結果に基づいて、主信号送受信部１２の連絡不能及び状態変化を検出してもよい。通信導通を許可する条件を満たさない状態が検出された場合には、遮断部１４３は、フォトニックゲートウェイの遮断機能と、フォトニックゲートウェイの光振分部の振分設定の変更とのうちの少なくとも一方を用いて、通信導通の遮断を実行してもよい。遮断部１４３は、通信網２における制御装置２０ａに、遮断の指示を送信してもよい。

[0088] 上記では、アカウントのＩＤ及びパスワード等の無効を中心に説明されているが、ユーザがログインし難くするアクセス制限では、例えば、主信号送受信部１２の所定状態を制御し得る信号経路が不通となる。ログイン制御部１４２又は遮断部１４３は、このような信号経路を同定するためのアドレスを、ユーザ側制御端末３０に与えないようにしてもよい。ログイン制御部１４２又は遮断部１４３は、アドレスをユーザに与えないようにすると共に、アドレスを同定するユーザからの問い合わせ（例えば、「ping」）に対して応答しないようにしてもよい。ログイン制御部１４２又は遮断部１４３は、辞書攻撃があった場合には、その辞書攻撃があったことを検出してもよい。ログイン制御部１４２又は遮断部１４３は、トランシーバ収容装置１０ａのマネージメントポートで受信制御部１４１が制御情報をやりとりしない場合、トランシーバ収容装置１０のマネージメントポート等の特定のポート（例えば、シリアルポート）等からのアクセスを許容しないようにしてもよい。ログイン制御部１４２又は遮断部１４３は、制御信号としてテレタイプ(tty）等を使わない場合、tty等からのユーザセッション（アクセス）を許容しないようにしてもよい。

[0089] 次に、通信システム１ａの動作例を説明する。

図４は、第２実施形態における、通信システム１ａの動作例を示すフローチャートである。受信制御部１４１は、主信号送受信部１２と通信網２との間の主信号の通信導通が許可される前に、制御装置２０ａからの制御信号の制御信号経路ＳＲを構築する（ステップＳ１０１）。

[0090] ログイン制御部１４２は、制御装置２０ａからのログインを有効化する。ログイン制御部１４２は、主信号送受信部１２の関連設定を変更及び読出することが可能なユーザ側制御端末３０からのログインを無効化する（ステップＳ１０２）。

[0091] ログイン制御部１４２は、主信号送受信部１２の所定の関連設定の変更及び読出を、制御信号のみに基づいて実行する（ステップＳ１０３）。ログイン制御部１４２は、ユーザ側制御端末３０からのログインの無効化が維持されているか否かを判定する（ステップＳ１０４）。ユーザ側制御端末３０からのログインの無効化が維持されている場合（ステップＳ１０４：ＹＥＳ）、ログイン制御部１４２又は遮断部１４３は、主信号送受信部１２と通信網２との間の通信導通を許可する。遮断部１４３は、主信号送受信部１２と通信網２との間の通信導通の遮断を解除してもよい（ステップＳ１０５）。ログイン制御部１４２及び遮断部１４３は、ステップＳ１０４に処理を戻す。

[0092] ここで、トランシーバ収容装置１０ａの導通を遮断する方法として、主信号送受信部１２の光出力を無視できるレベルまで落す(レジスタ等書込み)、光送信をＯＦＦにする（ハードピンへの入力や対応するレジスタ等の書込み）、主信号送受信部１２の停止、主信号送受信部１２の再起動、主信号送受信部１２の電源断、ユーザ装置４０と制御装置２０との間の主信号送受信部１２の間の主信号導通の遮断、主信号送受信部１２の給電を落とす、トランシーバ収容装置１０ａの電源を落とす、通信網側での信号の遮断等の少なくともいずれかの方法が挙げられる。

[0093] ユーザ側制御端末３０からのログインの無効化が維持されていない場合（ステップＳ１０４：ＮＯ）、遮断部１４３は、通信導通を遮断する。ログイン制御部１４２又は遮断部１４３は、通信導通の許可を取り消してもよい。ログイン制御部１４２は、ユーザ側制御端末３０からのログインを再び無効化してもよい（ステップＳ１０６）。ログイン制御部１４２及び遮断部１４３は、ステップＳ１０４に処理を戻す。

[0094] なお、ログインを変更するステップが、ユーザ側制御端末３０の機器認証

処理の前又は後に追加されてもよい。また、その機器認証処理の一部として、ログインを変更するステップが追加されてもよい。

[0095] 以上のように、受信制御部１４１は、主信号送受信部１２と通信網２との間の主信号を遮断して通信導通を許可する前に、通信網２に配置された制御装置２０ａからの制御信号の制御信号経路ＳＲを構築する。制御信号経路ＳＲは、例えば、制御装置２０ａと受信制御部１４１との間に構築される。

[0096] ログイン制御部１４２は、制御装置２０ａからのログインを有効化する。ログイン制御部１４２は、ローカルアカウントを用いて主信号送受信部１２の関連設定を変更及び読出することが可能なユーザ側制御端末３０からのログインを無効化する。ログイン制御部１４２又は遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されている場合に、通信網２と主信号送受信部１２との間の遮断を解除して、主信号の通信導通を許可する。遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されている場合に、通信網２と主信号送受信部１２との間の主信号の通信導通の遮断を解除してもよい。遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されていない場合に、通信網２と主信号送受信部１２との間の主信号の通信導通を遮断する。

[0097] これによって、電気通信事業者の意図に反する動作（ユーザが操作すべきでない変更）がサービス提供に与える影響を抑制可能である。ここで、トランシーバ収容装置１０ａの改造の規模は小さい。

[0098] 電気通信事業者の意図に反する動作以外については、ユーザによる制御が可能でもよい。遮断部１４３等が制御信号送受信部１１又は主信号送受信部１２にソフトウェア実装された場合と比較して、演算リソースがより豊富であることから、高度な制御が可能である。また、制御の入替が容易であり、第３実施形態（後述）と比較して早く応答することが可能である。さらに、通信網２とのやりとりを頻繁に実行することなく対応が可能である。

[0099] （第２実施形態の変形例）

ログイン制御部１４２は、トランシーバ収容装置１０ａにおける既存のセ

ッションを消去してから、ユーザ側制御端末３０からのログインを、ユーザ側制御端末３０にとって未知の値に変更してもよい。ここで、受信制御部１４１及びログイン制御部１４２は、セキュリティが高い制御信号経路ＳＲと制御信号経路ＳＲを経由したセッションとのうちで、セキュリティが高い制御信号経路ＳＲを残す。これよって、変更後のログイン（ユーザ側制御端末３０にとって未知の値）をユーザ側制御端末３０が入手することを回避することが可能である。

[0100] （第３実施形態）

第３実施形態では、通信網２に配置された制御装置にログイン制御部及び遮断部が備えられる点が、第２実施形態との主な差分である。第３実施形態では、第２実施形態との差分を中心に説明する。

[0101] 図５は、第３実施形態における、通信システム１ｂの構成例を示す図である。通信システム１ｂは、トランシーバ収容装置１０ｂと、制御装置２０ｂとを備える。トランシーバ収容装置１０ｂは、例えば、ユーザ宅に配置される。制御装置２０ｂは、例えば、通信網２に配置される。

[0102] トランシーバ収容装置１０ｂには、例えばシリアルバスを介して、ユーザ側制御端末３０が接続されてもよい。トランシーバ収容装置１０ｂは、制御信号送受信部１１（制御信号トランシーバ）と、主信号送受信部１２（主信号トランシーバ）と、スイッチ１３と、制御部１４ｂとを備える。制御部１４ｂは、受信制御部１４１を備える。通信網２に配置された制御装置２０ｂは、ログイン制御部１４２（検出部）と、遮断部１４３とを備える。制御装置２０ｂに備えられる遮断部１４３と、トランシーバ収容装置１０ｂとは制御信号経路ＳＲを介して通信してもよい。

[0103] 第３実施形態では、制御装置２０ｂのログイン制御部１４２は、ユーザ側制御端末３０からのログインの無効化が維持されているか否かを、例えば、ユーザ側制御端末３０の状態を確認するための通信結果、及び、制御装置２０ｂによって検出された通信状態等に基づいて検出（判定）する。検出された通信状態とは、例えば、光信号の波長及び強度が設定した通りの所定の波

長及び強度等であるか否かを表す状態、又は、ドリフト修正等の変更指示に主信号送受信部１２が従うか否かを表す状態である。

[0104] 遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されている場合、主信号送受信部１２と通信網２との間の通信導通を許可する。

[0105] 遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されていない場合、主信号送受信部１２と通信網２との間の通信導通を禁止する。遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されていない場合、主信号送受信部１２と通信網２との間の通信導通の許可を取り消してもよい。

[0106] 例えば、遮断部１４３は、主信号送受信部１２のレジスタ等への書込みによって、主信号送受信部１２（トランシーバ）の光出力を、無視できるレベルまで落してもよい。遮断部１４３は、ハードウェアのピンへの入力に関して、光信号の送信をオフにしてもよい。遮断部１４３は、主信号送受信部１２（トランシーバ）への給電を落としてもよい。遮断部１４３は、トランシーバ収容装置１０ｂの電源を落としてもよい。通信網２側で、信号が遮断されてもよい。遮断部１４３は、「Keep Alive」信号又は「Health check」信号のような信号をトランシーバ収容装置１０ｂとの間でやり取りした結果に基づいて、主信号送受信部１２の連絡不能及び状態変化を検出してもよい。通信導通を許可する条件を満たさない状態が検出された場合には、遮断部１４３は、フォトニックゲートウェイの遮断機能と、フォトニックゲートウェイの光振分部の振分設定の変更とのうちの少なくとも一方を用いて、通信導通の遮断を実行してもよい。遮断部１４３は、遮断の指示をトランシーバ収容装置１０ｂに送信してもよい。

[0107] トランシーバ収容装置１０ｂと制御装置２０ｂとの両方において、遮断処理がそれぞれ実行されてもよい。

[0108] 受信制御部１４１は、制御装置２０ｂと制御部１４ｂとの間、制御部１４ｂと主信号送受信部１２との間に、制御信号経路ＳＲを構築する。

[0109] ログイン制御部１４２は、ログイン制御部１４２と遮断部１４３との間に制御信号経路ＳＲを構築する。なお、ログイン制御部１４２は、制御装置２０ｂ内がセキュアな環境である場合、図５に示すログイン制御部１４２と遮断部１４３との間の破線で示す経路においては、制御信号経路ＳＲを構築しなくてもよい。

[0110] なお、遮断部１４３及びログイン制御部１４２は制御装置２０ｂ内に限らず、通信網内のどこに備えられていてもよい。この場合、制御装置２０ｂの近傍又は通信網を制御するオペレーションシステム内やその近傍がよい。ただし、遮断部１４３が制御装置２０ｂ以外に備えられる場合には、通信網内がクラッキングを受けづらいように構成されていることが前提となる。遮断部１４３がトランシーバ収容装置１０ｂの主信号送受信部１２から出力される主信号を通信網内で遮断する場合、遮断部１４３は主信号の動線上に配置されることが望ましい。遮断部１４３が、主信号送受信部１２に停止や電源断を指示する、トランシーバ収容装置１０ｂに対して主信号送受信部１２の電源を断させる、スイッチ１３で通信網側の主信号送受信部１２とユーザ装置４０側の主信号送受信部１５との間の信号導通を断させる、又は、トランシーバ収容装置１０ｂ自体の電源を断させる場合には、遮断部１４３は制御装置２０ｂに備えられることが望ましい。

[0111] 次に、通信システム１ｂの動作例を説明する。

図６は、第３実施形態における、通信システム１ｂの動作例を示すシーケンス図である。受信制御部１４１は、主信号送受信部１２と通信網２との間の主信号の通信導通が許可される前に、制御装置２０ｂからの制御信号の制御信号経路ＳＲを構築する（ステップＳ２０１）。

[0112] 制御装置２０ｂのログイン制御部１４２は、制御装置２０ｂからのログインを有効化する。制御装置２０ｂのログイン制御部１４２は、ローカルアカウントを用いて主信号送受信部１２の関連設定を変更及び読出することが可能なユーザ側制御端末３０からのログインを無効化する（ステップＳ２０２）。

[0113] 制御装置２０ｂのログイン制御部１４２は、制御信号を用いて、ログインを制限する。制御装置２０ｂのログイン制御部１４２は、制御信号を用いて、主信号送受信部１２の所定の関連設定の変更及び読出を、受信制御部１４１に指示する（ステップＳ２０３）。受信制御部１４１は、主信号送受信部１２の所定の関連設定の変更及び読出を、制御信号のみに基づいて実行する（ステップＳ２０４）。

[0114] 制御装置２０ｂのログイン制御部１４２は、ユーザ側制御端末３０からのログインの無効化の状態を判定する（ステップＳ２０５）。受信制御部１４１は、ユーザ側制御端末３０からのログインの無効化が維持されている場合に、制御装置２０ｂの遮断部１４３による制御に応じて、主信号送受信部１２と通信網２との間の通信導通を許可する（ステップＳ２０６）。

[0115] 例えば、ユーザ側制御端末３０からのログインの有効化を、ユーザ側制御端末３０が実行することがある。例えば、ユーザ側制御端末３０がコンピュータウイルスの侵入を試みることがある。例えば、ユーザ側制御端末３０がソフトウェアのアップデートを試みることがある（ステップＳ２０７）。制御装置２０ｂのログイン制御部１４２は、ユーザ側制御端末３０からのログインの無効化の状態等を判定する。例えば、ユーザ側制御端末３０からのログインの有効化をユーザ側制御端末３０が実行することがあるので、ログイン制御部１４２は、ログインの有効化を検出する。例えば、ログイン制御部１４２は、コンピュータウイルスの侵入を検出してもよい。例えば、ログイン制御部１４２は、ソフトウェアのアップデートを検出してもよい（ステップＳ２０８）。受信制御部１４１は、ユーザ側制御端末３０からのログインの無効化が維持されていない場合に、制御装置２０ｂの遮断部１４３による制御に応じて、通信導通を禁止する。受信制御部１４１は、ユーザ側制御端末３０からのログインの無効化が維持されていない場合に、制御装置２０ｂの遮断部１４３による制御に応じて、通信導通の許可を取り消してもよい（ステップＳ２０９）。

[0116] 以上のように、受信制御部１４１は、主信号送受信部１２と通信網２との

間の主信号を遮断して通信導通を許可する前に、通信網２に配置された制御装置２０ｂからの制御信号の制御信号経路ＳＲを構築する。制御信号経路ＳＲは、制御装置２０ｂと受信制御部１４１との間に構築される。

[0117] 制御装置２０ｂのログイン制御部１４２は、制御装置２０ｂからのログインを有効化する。制御装置２０ｂのログイン制御部１４２は、ローカルアカウントを用いて主信号送受信部１２の関連設定を変更及び読出することが可能なユーザ側制御端末３０からのログインを無効化する。制御装置２０ｂの遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されている場合に、通信網２と主信号送受信部１２との間の遮断を解除して、主信号の通信導通を許可する。制御装置２０ｂの遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されている場合に、通信網２と主信号送受信部１２との間の主信号の通信導通の遮断を解除してもよい。制御装置２０ｂの遮断部１４３は、ユーザ側制御端末３０からのログインの無効化が維持されていない場合に、通信網２と主信号送受信部１２との間の主信号の通信導通を遮断する。

[0118] これによって、電気通信事業者の意図に反する動作がサービス提供に与える影響を抑制可能である。ここで、トランシーバ収容装置１０ｂの改造の規模は小さい。また、第１実施形態及び第２実施形態と比較して攻撃されにくく、通信網（ゲートウェイ）側で主信号を迅速に遮断することが可能である。

[0119] （第４実施形態）

第４実施形態では、制御部に実装された装置用ソフトウェアが、一例としてゴールドストーン（Goldstone）である。第４実施形態では、第１実施形態から第３実施形態までとの差分を中心に説明する。

[0120] 第４実施形態では、コンテナ・オーケストレーション・ツールのクーベネティス（Kubernetes）を用いた例で一般的に示し、その後、特定のゴールドストーン（Goldstone）を用いた構成について示す。

[0121] コンテナは、実行プロセスがグループ化されて分離された空間の中だけで

実行する名前空間「namespace」と、実行プロセスに対してハードウェアリソースを制限するコントロールグループ「cgroups」との実装等により、実行プロセスをカーネル（Kernel）の機能で隔離し、読み込み専用の「Read Only Layer」のコンテナイメージと実行プロセスによって書込可能なレイヤの「Thin R/W layer」のファイルとからなるCOW(Copy-On-Write)の仕組みで、ファイルシステム等でコンテナイメージを共有する。

[0122] コンテナ削除では書込可能なレイヤだけが削除されるので、起動後の内容を保存するためにはコンテナイメージとして再度新しいレイヤとともにイメージ化するか、別途外部ファイルに書き出す仕組みを構成する。

[0123] コンテナイメージは、rootファイルシステム含むTAR（Tape ARchive）ファイルで、アプリケーションを動作させるファイルシステムと、起動コマンドやポートなどの設定が記載されたJSON（JavaScript Object Notation）のメタデータとの組み合わせである。

[0124] コンテナ実行エンジンはKernelの機能をAPI(Application Programming Interface)として実装するライブラリであり、コンテナを生成及び実行するコンテナランタイムを内部動作として呼び出し、コンテナ実行を実現する。コンテナを実行する際にはコンテナイメージを展開(Filesystem Bundle)しコンテナランタイムに受け渡す。ランタイムは、コンテナの隔離環境作成や直接操作するrunC等のLow-level Container Runtimeとコンテナイメージを展開しLow-level Container Runtimeにコンテナ実行作業を受け渡すcontainerd等のHigh-level Container Runtimeとからなる。

[0125] クーベネティスはHigh-level Container RuntimeをCRI(Container Runtime Interface)のAPI規格で呼び出す。

[0126] クーベネティスは、ビジネスのワークロードに応じ、アプリケーションの実行形式であるコンテナの配置、あるべき状態を宣言することで適切なリソースを配置するスケジューリング、セルフヒーリング、インフラの抽象化を行い、コンテナ化されたワークロードとサービスを管理するコンテナ・オーケストレーション・ツールである。クーベネティスは「k8s」と記載され、そ

の軽量版は「k3s」とも記載される。

[0127] クーベネティスクラスタを構成する２要素は、クーベネティスクラスタ上で稼働するコンテナ、ネットワーク、ストレージ等のリソース、コンテナの展開内容、再起動、アップグレード、接続等のポリシのあるべき姿を定義した抽象的な構成管理ファイルであるObjectと、その要求を実現するための実装やプロセスであるクラスタ基盤であるControl Planeである。

[0128] YAML(YAML Ain't Markup Language)形式でオブジェクトを定義したものは、マニフェストと呼ばれる。

[0129] コントロールプレーンに関連する基本オブジェクトとして、Pod、Service、ReplicaSet及びDeploymentの４つが挙げられる。Podは、クラスタ上でコンテナをデプロイする単位を管理するオブジェクトであり、Volumeやネットワークグループを共有するコンテナをまとめた単位である。Podは、クラスタ上でコンテナをデプロイする単位を管理するオブジェクトで内部に複数のコンテナを起動できる。Serviceは、Podに対するアクセスルーティングの設定を行うオブジェクトである。ReplicaSetは、Podを作成するテンプレートPodTemplateを利用して、クラスタ内に必要なPod数(レプリカ数)を管理するオブジェクトである。Deploymentは、新しいバージョンのリリースを管理するオブジェクトである。なお、クーベネティスはコンテナ単位ではリソースを取り扱わない。

[0130] コントロールプレーンにはMaster NodeとWorker Nodeの二つのグループがある。Master Nodeはマニフェストから要求を受け付け、稼働しているコンテナやインフラリソースに対しタスクをスケジューリングする。Worker NodeはMaster Nodeからの指示に従ってコンテナの起動や削除を行うとともに自身のサーバ上で起動しているコンテナの状態を監視しMaser Nodeに通知する。

[0131] マスタノード（Master Node）は、分散ストレージのetcd状態を定義したマニフェストをリソース要求として受け渡すインタフェースであるkube-apiserver(クーベネティス API)、それらから処理を受け取るkube-shedulerやkube-controller-manager等がある。あるべき姿はetcdに保存されたリソースの状

態を指す。

[0132] クーベネティス APIでは、特定の権限を持ち合わせたユーザアカウントやサービス(サービスアカウント)のみがetcdに保存されているオブジェクト情報への参照や変更を許すフィルタを備える。フィルタプロセスは接続アカウントの認証を行い、どのリソースに何の権限を与えるかの認可を判定し、ユーザ特有のリソース制限を判断する。認証(Authentication)の接続元は、クラスタ外部からの操作者またはプロセスの接続を対象とした認証アカウントのユーザアカウントとクラスタのnamespace内のPodで実行されているプロセスを対象とした認証アカウントのサービスアカウントに大別される。ユーザアカウントはクラスタのグローバルに定義されるためnamespaceに関係なくクラスタ内で一意となり、サービスアカウントはnamespace別に管理がわかれ、それぞれで一意となる。サービスアカウントトークンはSecretとしてPodにマウントされる。クーベネティスクラスタでは登録したアカウントのSecretを作成することでコンテナレジストリの認証が行える。ただしSecretは暗号化されているわけではないので安全なオブジェクトでは通常ないのでRBAC等の利用と合わせた対策が必要となる

[0133] 認証が許可されたアクセスのうち、authorization-modeオプションの順序に従う認可(Authorization)モジュールで接続元に応じて許可される操作を制御する。指定した全モジュールが拒否すると禁止応答「403」を応答し、どれかの認可モジュールが承認するとAdmission Controllerの評価に移る。評価モジュールは利用権限を定義したRoleというオブジェクトと、ユーザアカウントやグループを関連させるRoleBindingを定義しアクセス規制する役割ベースのアクセス制御のRBAC(Role-based access)等がある。RBACでは、ユーザアカウントやプロセスの認証対象のsubject、クラスタで利用可能なAPIリソースセットであるPodやDeployments、Services、Node等のresource、リソースに対して実行できるget, watch, create, delete等の一連のCRUD (Create/Read/Update/Delete) 操作のverbsの３つのうちのresourceとverbsを合わせたものがRoleというオブジェクトで、RoleとsubjectをRoleBindingで関連付け

る。例えば、クラスタ全体制限ならClusterRoleとClusterRoleBindingを利用し、namespace単位で制限ならRoleとRoleBindingの組み合わせで定義すればよい。

[0134] Admission ControlはAPIへのリクエスト内容を確認しリクエストの変更や制御をおこなう。Admission Controlは、各フィルタ作業するプラグイン型の実装コンポーネントであるAdmission Controllerの総称である。これらのコンポーネントのうち、イメージ取得ポリシを強制することによってPod起動時にイメージ利用の認証を行うAlwaysPullImagesにより、本実施形態で利用する機能部（例えば、受信制御部１４１、ログイン制御部１４２、及び、遮断部１４３のいずれか）を備えたPodとなるように強制してもよいし、クーベネティス APIにアクセスするためのServiceAccoutTokenをマウントするService Accountにより、所定のポリシのTokenをマウントさせてもよい。MutatingAdmissionWebhookやValidatingAdmissionWebhookを用いて柔軟に制限してもよい。

[0135] ＜改変防止＞

従って、本実施形態において、改変防止の機能を主にトランシーバ収容装置に配置すれば、トランシーバ収容装置をクラスタとして、クラスタ全体制限のClusterRoleとClusterRoleBindingまたはClusterRoleとRoleBindingとが利用されてもよい。

[0136] ユーザアカウントを利用する場合、通信網２側の制御装置からの制御するユーザよりも権限の劣るユーザを設定し、当該ユーザには本実施形態の機能部を配置したPodのNamespaceとそれ以外のPodのNamespaceとを分け、または、当該ユーザが制御すべきでない設定を制御可能なPodのNamespaceとそれ以外のPodのNamespaceとを分け、ユーザから制御できないようにする。

[0137] サービスアカウントを利用する場合で、ユーザからのアクセスがtty(teletypewriter)入力のみやシリアル接続に対応するCOM入力のみに限定できる場合は、namespace単位で制限となるので、そのRoleまたはRoleとRoleBindingの組み合わせで定義してもよい。(監視では、監視機能自体をドライバ収容装置

上に配置しなければ、制限せずともよい。トランシーバ上に機能を配置する場合は、機能の一部をトランシーバ収容装置上に配置しない限りは制限せずとも良い）

[0138] 例えば、Subjectとして顧客(Login ID)やTTY等(CUI経由)やManagement Port(IPアドレス)で対象とすればよい。ネットワーク接続できないように、ResourceでServiceの操作の情報を授受させないか、制御させない設定関連の制御を集めたPodアクセス禁止、ログイン停止の場合、Node＝ハードウェア＝ドライバ収容装置自体である。）

[0139] なお、本実施形態の機能部またはユーザにアクセスを制限する設定に関するnamespaceのSecretは見えないようにすべきであるが、機能部の削除変更やアクセスを制限すべき設定へのアクセスを、認可やAccess Controlにより抑止してもよい。

[0140] ただし、変更等を、Secretがみえたら、IDを偽ってアクセスしうるので、網の制御装置との接続確認を行い、制御信号送受信部１１を通信網２との接続を解除したりして接続が断となる場合や、通信網２の制御装置から設定値等の確認を行い、通信網２からの接続以外の接続や変更が検出した場合、主信号を断とし、設定や認証情報等の検査を行い正常であることを確認してから再度導通を行うとしたほうが望ましい。

[0141] 制御信号送受信部１１を通信網２との接続を解除したりして、ユーザがアクセスすべきでない設定等を変更したりすることを抑制する観点からは、これ以前の実施形態においても、通信網２の制御装置との接続確認を行い、制御信号送受信部１１を通信網２との接続を解除したりして接続が断となる場合や、通信網２の制御装置から設定値等の確認を行い、通信網２からの接続以外の接続や変更が検出した場合、主信号を断とし、設定や認証情報等の検査を行い正常であることを確認してから再度導通を行うとしたほうが望ましいことは同様である。

[0142] ＜本実施形態の機能部の削除防止＞

本実施形態の機能部（例えば、受信制御部１４１、ログイン制御部１４２

、及び、遮断部１４３のいずれか）を備えるPodは、本実施形態の機能が停止されないように優先度が高くなるようにするのが望ましい。

[0143] 具体的には、Pod新規作成や再作成時、Podの定義における実行されるべきノードのフィールドであるNodeNameが未指定で、Worker Nodeが未指定の場合、指定されていないPodを常に監視するkube-schedulerにより、適したWorker Nodeが選択され、NodeNameを更新し、対象のWorker Nodeで稼働しているkubeletに新規Pod追加の依頼が通知され、当該Worker Node Podを起動する。逆に特定ノード上にPodが収まらないときは、不適切なNodeを除去するフィルタリングのPredicateで不適切とされたPodが除去される。

[0144] そのため、本実施形態の機能部を備えるPodは、その機能部が動作する十分なPodがないときは新規Podの追加の依頼が通知され、削除されるとその機能部が動作するに不十分なPodとなる時は削除されないようなノードの優先順位のPriorityとなるよう重み付けをすることが望ましい。

[0145] 同様に、Podのオートスケールを設定する場合、Horizontal Pod Autoscaler(HPA)でのスケールアウト又はスケールインでのPodの台数の増減で削減されないようにする。増加する場合は、セキュリティが劣化しないようにする。Vertical Pod Autoscaler (VPA)でのスケールアップ又はスケールダウンでのPod自体の処理能力の増減で本実施形態に必要な処理の処理能力(通信網２側の機能との通信速度や頻度、また、監視の場合では、監視や遮断の速度や頻度等)を担保する。なお、稼働中のPodに対する動的なリソース変更を許容せず、Eviction APIを介した操作等でPodを削除し、ReplicaSetのセルフヒーリング機能等でのPod再作成により適切なリソースのPodとするVPAでは、本実施形態の処理に係るPodに関しては一つ未満になる場合に削除しないようにする。または、一連の流れでの本実施形態の処理が妨げられる時間が所定の時間以下となるようにするか、所定の時間以下にならない場合はその処理を抑止することが望ましい。Pod Disruption Budgetが設定されている場合、本実施形態の処理に係るPodに関しては、その値をサービス上で許容される異常状態の継続時間よりも十分小さくしておくことが望ましい。

[0146] ＜アクセスすべきでない設定、通信網２側の制御装置との証明書として利用するTLSタイプや、Dockerイメージの認証情報の秘密確保＞

マニフェスト等により、ユーザアカウント毎に異なる暗号化したKey-Value形式の値等のSecretやConfigMapオブジェクトを起動時に登録し、Pod上で読み込まれるように、Podの環境変数として読み込ませるか、volumeをマウントして読み込ませてもよい。ここで、SecretやConfigMapは環境変数やアプリケーションの設定ファイルをコンテナ内に含めず、Podとは別のオブジェクトとして管理するためのボリュームである。Secretはクレデンシャル情報を取り扱うオブジェクトであり適切に暗号化してetcdに保存され、利用の際にワーカーノード上のメモリ領域に確保された一時的なファイルシステムであるtmpfsに展開されワーカーノードに永続的なデータが残らない。ConfigMapは平文形式のコンテンツをボリュームとして管理するものである。

[0147] これらを用いる場合で、すでに起動しているPodに反映するにはDeploymentを更新し、Podを切替するか、コンテナのプロセスに反映するためにプロセス側の再読込設定や再起動を行ってもよい。環境変数としてPodに反映するためのフィールドとして「valueFrom.configMapkeyRef」や「envFrom[].configMapRef」等を利用してもよい。

[0148] Podマニフェストではなく、ラベルセレクタをもとにPod作成時に特定の情報を追加するフック機能であるPodPresetを利用し、Pod起動のタイミングで特定の環境変数を動的に指定してもよい。PodPresetを利用した場合、Pod毎に全ての情報を毎回指定することなく共通の情報が利用でき、デプロイ環境によらずに動的に必要な情報や機密情報を付与することが可能である。

[0149] ＜本実施形態で用いられているアプリケーションであるかの確認方法＞

アプリケーションやサービスに対する様々な業務要求を定義し、構成情報だけでなく、デプロイメントプロセスやその運用またはその品質を保証できる設計も加味されうる、機能のテンプレートセットであるITIL（Information Technology Infrastructure Library）等で定義されるサービスカタログによるカタログ化を活用してもよい。

[0150] ここで、サービスカタログは、Kubernetesクラスタ上で実行されているアプリケーションが、クラウドプロバイダ等によって提供されるマネージドデータベースやオブジェクトストレージなどのコンテナ化されていないリソースの接続に利用するようなクラスタ外部にあるソフトウェアやサービスを使用するための拡張APIでありOpen Service Broker API規格を用いたKubernetesのService Catalogは意味しない。

[0151] アプリケーションの要求定義として、Deployment、Service、ConfigMapといったオブジェクトをラベルとセレクタによって個別に関連付けた例で示したが、ワークロードに応じたマニフェストをパッケージ化して管理を容易にするように、特定のアプリケーションやサービスに必要な要素をあらかじめ決めておき、それに対応できるオブジェクトをテンプレート化するパッケージ化を行い、このパーケージを応用しアプリケーションのロールバックやバージョン管理を行うパッケージマネージメントを行ってもよい。例えば、アプリケーションのワークロード毎にDeploymentやServiceの管理、ConfigMapを利用した変数やボリュームの取り扱いし処理の作業を軽減可能なKubernetesにおけるパッケージマネージメントツールのHelmを用いてもよい。Helmは、Kubernetesのマニフェストをテンプレート化してまとめたパッケージでありYAMLのセットであるChartを管理するクライアントツールである。Helmバージョン「２」であれば、そのパッケージマネージメント機能全体は、コンソールやCI/CDのパイプライン上からChartを呼び出すクライアントツールのHelm(Client)とKubernetesクラスタ上で動作しChartのデプロイや管理を行うサービスであるTiller(Server)のコンポーネントからなり、Helmクライアントはg RPCを介しTillerと対話し、デプロイ対象となるChartの情報を送信したり、アップグレードやアンインストールの要求を指示したりする。TillerはHelmクライアントから要求されたChartの構成をKubernetesに指示し、リソースの展開を管理する。Helmバージョン「３」であれば、Kubernetes上で展開されているバージョンとChartのリリースバージョンを比較してリソースを管理するTillerを活用せずに、これらのリリース情報をCRD(Custom Resource Defin

ition)に格納し、クライアント側から操作することで代替する。

[0152] この仕組みを用い、本実施形態で用いるアプリケーションが適正なバージョンか簡易に確認してもよい。例えば、Chartの定義済変数であり、リリースが最後に更新された時刻であるRelease.Timeや、更新のたびに１から増加するリビジョン番号であるRelease.RevisionやChart.yamlのversionフィールド等を利用してもよい。不適切なバージョンを検出したら、差分のあるPodまたは全てのPodをロールバックにより適切なバージョンに戻すとし、戻せない場合に、遮断としてもよい。

[0153] もちろん、Kubernetesにより管理されるPodやDeploymentなどのコアリソースを、Kubernetesがもつリソースとコントローラによって実現する仕組みであり、現在の稼働状態であるCurrent Stateの監視を行う「Observe」、Current StateとDesired Stateの差分を比較する「Diff」、適切な状態に調整する「Act」の３つの状態からなるControl Loopを用いて、監視、検出、調整を行い、適切な状態に調整し、調整できない場合に、遮断としてもよい。ここで、Control loopはDeploymentであれば、Deploymentコントローラによって管理される。

[0154] 本実施形態で独自のリソースとして追加したカスタムリソースであるアプリケーション（例えば、受信制御部１４１、ログイン制御部１４２、及び、遮断部１４３のいずれか）の運用実装を「カスタムリソース」と「カスタムコントローラ」を利用してKubernetesから監視、検出、調整を行ってもよい。

[0155] ここでカスタムリソースは既存のKubernetes APIを拡張した独自のデータ構造であり、etcd内に保存されるオブジェクトのDesired StateとCurrent Stateを管理するための拡張リソースの箱を作り、アプリケーション独自のステート情報やミドルウェアのクラスト管理に必要なフラグを格納し、今までアプリケーション側だけで管理していたステートをKubernetesのリソースとして保存しておくことで、Control Loopを用い、コントローラにてオブジェクトの状態を調整する。この場合も適切に調整できない場合に、遮断としても

よい。

[0156] なお、カスタムリソースとして、API拡張は、API Aggregationで、Kubernetes APIにAggregated APIとしてオブジェクトを新たに実装し、Aggregation LayerにAPI登録することで、詳細に定義して拡張してもよいし、Customer Resource Definition(CRD)で、独自のAPIを作らずに、リソースを新たに定義することで拡張してもよいが、Operatorでは後者のCRDによるAPI拡張を用いる。

[0157] カスタムコントローラはカスタムリソースやコアリソースの状態を確認（Diff）し、リソースのDesired Stateに更新対象をなるEventがあった場合に管理されるオブジェクトを調整(Act）する。

[0158] 次に、トランシーバ収容装置１０に組み込まれるソフトウェアとして、ゴールドストーンを用いた構成について説明する。上述した各実施形態では、遮断部を備えないトランシーバ収容装置１０（例えば、第１実施形態）と、遮断部を備えるトランシーバ収容装置１０（例えば、第２実施形態や第３実施形態）について説明した。第４実施形態の説明においても、遮断部を備える場合と遮断部を備えない場合について分けて説明する。

[0159] （遮断部を備えない場合）

遮断部を備えない場合の構成として、第１実施形態におけるトランシーバ収容装置１０を例に説明する。第１実施形態におけるトランシーバ収容装置１０の制御部１４上で動作するソフトウェアとして、ホワイトボックススイッチのネットワークＯＳ、ゴールドストーン及び設定機能等のセットがホワイトボックススイッチにインストールされる。設定機能である受信制御部１４１、ログイン制御部１４２及び遮断部１４３は、ゴールドストーンとは別のＯＳ上のアプリケーションでもよいし、ゴールドストーン上のアプリケーションでもよい。

[0160] 受信制御部１４１、ログイン制御部１４２及び遮断部１４３が、ゴールドストーン上のアプリケーションである場合、受信制御部１４１、ログイン制御部１４２及び遮断部１４３は、通常のゴールドストーンに含まれないアプ

リケーションであって、それぞれ異なるＰｏｄ上のコンテナ上のアプリケーションでもよいし、同一のＰｏｄ上の別コンテナ上のアプリケーションでもよいし、同一Ｐｏｄ上の同一コンテナ上のアプリケーションでもよいし、一体のアプリケーションでもよい。既存のゴールドストーンの一部のアプリケーションを改造したものであってもよい。

[0161] 例えば、トランシーバ収容装置１０の変更が少ない構成として、受信制御部１４１は、ＣＬＩ（Command Line Interface）、ｎｅｔｆｏｎｆ、ＳＮＭＰ（Simple Network Management Protocol）、ｒｅｓｔｃｏｎｆ等を予め備えるNorth Management Interface、又は、それらが値を書き込むＳｙｓｒｅｐｏである。ログイン制御部１４２及び遮断部１４３は、ＴＡＩやｔａｉシェルである。なお、非特許文献１のＦｉｇ．９に示す構成では、South Management LayerのSouth TAIに該当する。通信網から所定の経路を経由したログインする機能をNorth Management InterfaceやＳｙｓｒｅｐｏやSouth TAIを改造して備えてもよいし、North Management InterfaceやSouth TAIと並列に別途備えてもよい。

[0162] ・Ｓｙｓｒｅｐｏ(ＳｙｓｒｅｐｏはUNIX（登録商標）/Linux（登録商標）システム用のＹＡＮＧベースのデータストアで、ＹＡＮＧ形式で記述されたアプリケーション構成を格納する)を使用するアプリケーションをＮＥＴＣＯＮＦで制限してもよい(ＳｙｓｒｅｐｏはNetopeer2 NETCONFサーバと統合されているＳｙｓｒｅｐｏを使用するアプリケーションをＮＥＴＣＯＮＦで管理可能)

・Ｓｙｓｒｅｐｏには、複雑なアクセス制御を強制できるマスタープロセスがないため、標準のファイルシステムパーミッションに依存し、以下を留意して使用する。許可されていないプロセスから機密データにアクセスできないようにするため、インストールするすべてのＹＡＮＧモジュールに常に正しい権限と所有者を設定する。ユーティリティＳｙｓｒｅｐｏｃｔｌは、ＡＰＩで使用できるこの機能に加えて、すべての権限の表示(--list)と変更(--change<module>)の両方に用いる。Ｓｙｓｒｅｐｏにリンクされているすべて

のプロセスからアクセスできる必要がある共有ファイルに書き込むことで、Ｓｙｓｒｅｐｏを完全に中断する。リバースエンジニアリングによっては、これらの共有ファイルでデータが通信されているときに、非正規化プロセスによってデータにアクセスされないように、２つのｃｍａｋｅ変数Ｓｙｓｒｅｐｏ_ｕｍａｓｋとＳｙｓｒｅｐｏｇｒｏｕｐを調整する。一般に、新しいシステムグループを作成してＳｙｓｒｅｐｏ_ｇｒｏｕｐに設定し、次にＳｙｓｒｅｐｏｊｍａｓｋを００００７に設定して、すべての外部アクセスをｆｒｏｖｉｄｅｄにする。Ｓｙｓｒｅｐｏプロセスを実行しているすべてのユーザアカウントがこのグループに属している場合は、Ｓｙｓｒｅｐｏファイルや機密情報に他のユーザアカウントがアクセスできないようにする。

[0163]（遮断部を備える場合）

遮断部を備える場合の構成として、第２実施形態におけるトランシーバ収容装置１０ａを例に説明する。なお、第３実施形態におけるトランシーバ収容装置１０ｂにおいても基本的な処理は同様である。第２実施形態におけるトランシーバ収容装置１０ａの制御部１４上で動作するソフトウェアとして、ホワイトボックススイッチのＮＯＳ、ゴールドストーン、設定機能及び遮断機能等がホワイトボックススイッチにインストールされる。設定機能である受信制御部１４１、ログイン制御部１４２及び遮断部１４３は、ゴールドストーンとは別のアプリケーションでもよいし、ゴールドストーン上のアプリケーションでもよい。

[0164] 受信制御部１４１、ログイン制御部１４２及び遮断部１４３が、ゴールドストーン上のアプリケーションである場合、受信制御部１４１、ログイン制御部１４２及び遮断部１４３は、通常のゴールドストーンに含まれないアプリケーションであって、それぞれ異なるＰｏｄ上のコンテナ上のアプリケーションでもよいし、同一のＰｏｄ上の別コンテナ上のアプリケーションでもよいし、同一Ｐｏｄ上の同一コンテナ上のアプリケーションでもよいし、一体のアプリケーションでもよい。既存のゴールドストーンの一部のアプリケーションを改造したものであってもよい。

[0165] 例えば、トランシーバ収容装置１０ａの変更が少ない構成として、受信制御部１４１は、ＣＬＩ、ｎｅｔｆｏｎｆ、ＳＮＭＰ、ｒｅｓｔｃｏｎｆ等を予め備えるNorth Management Interface、又は、それらが値を書き込むＳｙｓｒｅｐｏである。ログイン制御部１４２及び遮断部１４３は、ＴＡＩやｔａｉシェルである。なお、非特許文献１のＦｉｇ．９に示す構成では、South Management LayerのSouth TAIに該当する。通信網から所定の経路を経由したログインする機能をNorth Management InterfaceやＳｙｓｒｅｐｏやSouth TAIを改造して備えてもよいし、North Management InterfaceやSouth TAIと並列に別途備えてもよい。

[0166] 制御装置２０側にDying GASP相当を送信することが望ましいが、Keep aliveやHealth check相当の断を見て制御装置２０側で推定してもよい。

[0167] ・Ｓｙｓｒｅｐｏ(ＳｙｓｒｅｐｏはUNIX（登録商標）/Linux（登録商標）システム用のＹＡＮＧベースのデータストアで、ＹＡＮＧ形式で記述されたアプリケーション構成を格納する)を使用するアプリケーションをＮＥＴＣＯＮＦで制限してもよい(ＳｙｓｒｅｐｏはNetopeer2 NETCONFサーバと統合されているＳｙｓｒｅｐｏを使用するアプリケーションをＮＥＴＣＯＮＦで管理可能)

・Ｓｙｓｒｅｐｏには、複雑なアクセス制御を強制できるマスタープロセスがないため、標準のファイルシステムパーミッションに依存し、以下を留意して使用する。許可されていないプロセスから機密データにアクセスできないようにするため、インストールするすべてのＹＡＮＧモジュールに常に正しい権限と所有者を設定する。ユーティリティＳｙｓｒｅｐｏｃｔｌは、ＡＰＩで使用できるこの機能に加えて、すべての権限の表示(--list)と変更(--change<module>)の両方に用いる。Ｓｙｓｒｅｐｏにリンクされているすべてのプロセスからアクセスできる必要がある共有ファイルに書き込むことで、Ｓｙｓｒｅｐｏを完全に中断する。リバースエンジニアリングによっては、これらの共有ファイルでデータが通信されているときに、非正規化プロセスによってデータにアクセスされないように、２つのｃｍａｋｅ変数Ｓｙｓｒ

ｅｐｏ_ｕｍａｓｋとＳｙｓｒｅｐｏｇｒｏｕｐを調整する。一般に、新しいシステムグループを作成してＳｙｓｒｅｐｏ_ｇｒｏｕｐに設定し、次にＳｙｓｒｅｐｏｊｍａｓｋを００００７に設定して、すべての外部アクセスをｆｒｏｖｉｄｅｄにする。Ｓｙｓｒｅｐｏプロセスを実行しているすべてのユーザアカウントがこのグループに属している場合は、Ｓｙｓｒｅｐｏファイルや機密情報に他のユーザアカウントがアクセスできないようにする。

[0168]（変形例１）

第４実施形態においてトランシーバ収容装置１０，１０ａ，１０ｂは、各実施形態で追加した機能部の削除改変に係るような、また各実施形態で追加した機能部の処理をバイパスするような新たなＮａｍｅｓｐａｃｅやＮｏｄｅやコンテナの追加や複製をＫｕｂａｎｅｔｅｓ等で制限するように構成されてもよい。この場合、トランシーバ収容装置１０ａ，１０ｂ上の遮断部１４３が配置されたコンテナやコンテナに対応するＮｏｄｅ等が制御装置２０，２０ｂからアクセスできない状態や、遮断部１４３が遮断する場合には遮断できない状態とならなければよい。

[0169]（変形例２）

第４実施形態においてトランシーバ収容装置１０，１０ａ，１０ｂは、以下のように起動するように構成されてもよい。（起動時、又は、停止時の遮断、起動時からのログイン制御、ＡＰＮＣへの接続)再起動時にトランシーバ収容装置１０，１０ａ，１０ｂにユーザがログインして起動し直さず、制御装置２０，２０ｂ側からの制御のみ受け付ける形でのみ起動するようにしてもよい(起動時又は停止時の遮断、起動時からのログイン制御、ＡＰＮＣへの接続)。

[0170]（変形例３）

第４実施形態においてトランシーバ収容装置１０，１０ａ，１０ｂは、以下のように自動立ち上げするように構成されてもよい。自動立ち上げは、例えば、通常の起動シーケンスで、ゴールドストーン起動画面→起動後即Ｋｕｂａｎｅｔｅｓ内→ｔａｉシェル停止(tai.sh stop) →ｔａｉシェル起動(ta

i.sh start）→ｓｏｕｔｈ－ｔａｉ再起動(k rollout restart ds/south-tai）→ｔａｉシェル起動(k exec -it deploy/tai -- taish) →ｔａｉシェルから各ＰＩＵ（プラグインユニット）に入る(module /dev/piu1,ここではｐｉｕ１の例）→主信号送受信部１２をアクティブにする(set admin-status up)であれば、それも自動立ち上げする。

[0171]（変形例４）

第４実施形態においてトランシーバ収容装置１０，１０ａ，１０ｂにおいて、管理者権限より下位の権限のＩＤをつくり、下位の権限のＩＤのみユーザにアクセス可能としてもよい。その上で、下位の権限のＩＤでは各実施形態で追加した機能部の削除改変に係るようなソフトウェア又は設定のファイルに関し、読込不可、書込不可、実行不可、又は読込のみ可とする。ファイルの場合そのモードは---(0)又はr--(4)(read/write/execute)とする。

[0172]（変形例５）

第４実施形態においてトランシーバ収容装置１０，１０ａ，１０ｂは、各実施形態で追加した機能部の削除改変に係るような以下のようなアクセス制限を行うように構成されてもよい。

・ＩＰアドレスを検索できないようにしてもよい。

ＫｕｂａｎｅｔｅｓやＯＳのルーティングテーブルで、機能部自体や、設定値やそれらを配置したコンテナ等のIPアドレスのアドレス解決や広告を抑止し、かつIPアドレスを推測困難な値とすることで、アクセスを抑止する。

・ネットワークアクセス制御リストによって、ＡＰＩ Ｓｅｒｖｅｒ(Kubernetesコントロールプレーン)へのアクセスは、クラスタ管理に必要なＩＰアドレスを制限してもよいし、関連Ｎｏｄｅへのアクセスを制限してもよい。・ｍＴＬＳ等を用い、ＴＡＩに係るサービス間のネットワークトラフィックは暗号化。

・ＫｕｂｅｒｎｅｔｅｓでＰｏｄやコンテナの権限を強制するセキュリティポリシーやＯＰＡ Ｇａｔｅｋｅｅｐｅｒを用いてもよい。

・ｋｕｂｅｒｎｅｔｅｓのデフォルトではアクセス制限ないが、Network Pol

icyを使うことでＰｏｄに対してingress ruleを記述し、ingress ruleによってＰｏｄ単位(ＩＰアドレス単位)、またはＴＣＰ/ＵＤＰポート単位でのアクセス制御をかけてもよい。

[0173] 次に、トランシーバ収容装置（制御部）又は制御装置は、所定の機能部の処理をバイパスするような新たなネームスペース、ノード、コンテナの追加及び複製を制限するシーケンスを、クーベネティス（Kubernetes）を用いて実行する。トランシーバ収容装置（制御部）又は制御装置は、ONL（Open Network Linux）、K3s（軽量クーベネティス）、「South management layer」（例えば、ゴールドストーンにおける、South-TAI、South-ONLP)、及び、「North management layer」(例えば、ゴールドストーンにおける、north-CLI、north-netconf)へのログインを制限する。トランシーバ収容装置（制御部）又は制御装置は、例えば、むき出しのオペレーティングシステム（Bare OS）へのログインを制限する。トランシーバ収容装置（制御部）又は制御装置は、クーベネティスへのログインを制限する。トランシーバ収容装置（制御部）又は制御装置は、クーベネティスのゴールドストーンのアドレスへの接続が制御装置からのみ可能となるように、接続を制限する。

[0174] トランシーバ収容装置の再起動時、トランシーバ収容装置（制御部）又は制御装置は、本シーケンスを繰り返す。起動時に、ユーザ側制御端末３０がトランシーバ収容装置に再度ログインして、トランシーバ収容装置が再起動するという設定である場合、制御装置は、トランシーバ収容装置の再起動時に、主信号送受信部１２の遮断を実行する。

[0175] 「Dying GASP」に相当する信号をトランシーバ収容装置が通信網２（ゲートウェイ）側に送信することが望ましいが、制御装置（ゲートウェイ）が「Keep alive」や「Health check」に基づいて通信断を推定（判定）してもよい。

[0176] 起動時又は停止時の遮断、起動時の初期ＩＤ（識別情報）及びパスワードの確認、又は、オールフォトニックネットワークの制御装置（APNC）への接続など、再起動時にユーザ側制御端末３０がトランシーバ収容装置にログイ

ンしても、トランシーバ収容装置が再起動せず、制御装置（ゲートウェイ）側からの制御のみをトランシーバ収容装置が受け付ける形式でのみ、トランシーバ収容装置が起動されるようにしてもよい(起動時又は停止時の遮断、起動時のソフトウェア構成の確認、起動時の自動的な立ち上げ、及び、オールフォトニックネットワークの制御装置への接続)。

[0177] トランシーバ収容装置の自動的な立ち上げでは、例えば、データセンタ間の光伝送ネットワークにおいてハードウェアとソフトウェアの分離を可能にするオープンソースソフトウェア（TAI：Transponder Abstraction Interface)を用いて、通常の起動シーケンスが、「Goldstone起動画面」→「起動後、即、クーベネティス内」→「tai.シェル停止(tai.sh stop)」→「tai.シェル起動(tai.sh start)」→「south-tai再起動(k rollout restart ds/south-tai)」→「taiシェル起動(k exec -it deploy/tai -- taish)」→「taiシェルから、各PIU（プラグインユニット）に入る(module /dev/piu1,ここではpiu1の例)」→「トランシーバをアクティブにする(set admin-status up)」というシーケンスである場合、それらも自動的に立ち上げする。

[0178] パスワード変更時の既存セッションの断では、例えば、パスワード変更時に、テレタイプ(tty）等からのユーザセッションは、一旦、既存セッションを断にする。これにより、ログインを続けるユーザによる操作が排除される。また、制御用のシリアル等のポートが「Disable」にされる。

[0179] アクセスできないように、Cni0(Container Network Interface 0)等を用いたブリッジ方式(ホスト側のネットワーク・ネームスペースに仮想ブリッジが作成され、各Pod（Dockerコンテナを管理するための最小単位）用に作成された仮想ネットワーク（veth)のホスト側がブリッジに接続されることで、Podとホストが通信できるようにされる。例えば、CNIプラグイン（Flannel）が用いられる。主に、同一ノード上のPodは、各Podが同一セグメントに属するのであれば、ブリッジでフィルタリングされる。

[0180] クーベネティスの「Calico」等を用いてホストとコンテナの疎通が実行される「Point to Point」方式(主に、Podごとに独立したネットワークセグメ

ントが払い出される方式)では、一度、仮想ブリッジにルーティングされて、ARP（Address Resolution Protocol）で繋がっているネットワークインターフェースカード（NIC）のMACアドレス（Media Access Control address）を解決して通信するのではなく、それぞれのPodに直接対応する仮想ネットワーク（veth)にルーティングされるので、仮想ブリッジにはルーティングされないようになる。

[0181] ログイン状態の管理には、クーベネティスのPOD状態の監視(k get pods等)が用いられてもよい。少なくとも以下に例示された切断対象、又は、切断対象に相当するPodへのユーザからの接続は、ログイン制限時において切断される。

[0182] 切断対象：シリアル接続の「/dev/ttyS*」、「SSH」又は「telnet」のネットワーク経由で接続している仮想端末（ターミナル)の「/dev/pts/*」で示される対象を切断(念のため、モデム用の「/dev/modem」と、マウス用の「/dev/mouse」と、シリアルの古い名称の「/dev/cua」とは、切断対象である）。

[0183] 接続抑制対象は、ゴールドストーン（Goldstone）における、例えば、「GS_SOUTH_AGENTSのsouth-sonic south-tai south-onlp south-system south-gearbox south-dpll」と、「GS_NORTH_AGENTSのnorth-cli north-snmp north-netconf north-notif」と、「GS_XLATE_AGENTSのxlate-ocn (tai, usonic-cli、gs-mgmt-np2,snmpの関連(gs-mgmt-snmp, svclb-gs-mgmt-snmp,svclb-netopeer2等)」とである。

[0184] ＜アクセス制限＞

・ＩＰ(Internet Protocol)アドレスが検索できないようにされてもよい。クーベネティス及びオペレーティングシステムのルーティングテーブルにおける、設定値等が配置されたコンテナと機能部自体等とのＩＰアドレスのアドレス解決又は広告が抑止される。また、ＩＰアドレスが推測困難な値に定められることで、アクセスが抑止される。

・ネットワークアクセス制御リストによって、APIサーバ(クーベネティス・コントロールプレーン)へのアクセスは、クラスタ管理に必要なIPアドレス

が制限されてもよいし、関連ノードへのアクセスが制限されてもよい。

[0185] ・ＴＬＳ相互認証（mTLS：mutual Transport Layer Security）等が用いられて、ＴＡＩに係るサービス間のネットワークトラフィックは、暗号化されてもよい。

・クーベネティスにおいて、Podやコンテナの権限を強制するセキュリティポリシーや、OPAゲートキーパ（Open Policy Agent Gatekeeper）が用いられてもよい。

[0186] ・クーベネティスのデフォルトではアクセス制限が無いが、ネットワーク・ポリシーが用いられることで、Podに対して「ingress rule」が記述され、「ingress rule」が用いられて、「Pod単位(IPアドレス単位)」または「TCP/UDPポート」単位でのアクセス制御が実行されてもよい。

[0187] ・システムリポジトリ構成「Sysrepo」を使用するアプリケーションが、「NETCONF」で制限されてもよい。「Sysrepo」は、「UNIX（登録商標）/Linux（登録商標）システム」用のYANG（Yet Another Next Generation）ベースのデータストアで、YANG形式で記述されたアプリケーション構成を格納する。「Sysrepo」は、「Netopeer2 NETCONFサーバ」に統合された「Sysrepo」を使用するアプリケーションを、「NETCONF」で管理可能である。

[0188] ・「Sysrepo」には、複雑なアクセス制御を強制できるマスタープロセスが無いので、標準のファイルシステムパーミッションに依存し、以下に留意して使用される。

[0189] 許可されていないプロセスからは機密データにアクセスできないようにするために、インストールされる全てのYANGモジュールには、正しい権限と所有者が常に設定される。ユーティリティ「sysrepoctl」（システムリポジトリ構成の制御）には、アプリケーション・プログラミング・インターフェース（API）で使用できるこの機能に加えて、全ての権限の表示(--list)と変更(--change<module>)との両方が用いられる。

[0190] 「Sysrepo」にリンクされている全てのプロセスからアクセスできる必要がある共有ファイルに書き込まれることで、「Sysrepo」が完全に中断される。

リバースエンジニアリングによっては、これらの共有ファイルでデータが通信されているときに、非正規化プロセスによってデータにアクセスされないように、２個のcmake変数（sysrepo_umaskとsysrepo_group）が調整される。

[0191] 一般に、新しいシステムグループが作成されて、「sysrepo_group」に設定され、「sysrepo_jmask」が00007に設定されることで、外部アクセスがすべて禁止にされる。「sysrepo_umask」が「00007」に設定されることで、外部からのアクセスがすべて禁止されてもよい。「Sysrepo」プロセスを実行しているすべてのユーザアカウントがこのグループに属している場合には、「Sysrepo」ファイル及び機密情報に他のユーザアカウントがアクセスできないようにされてもよい。

[0192] ログインの情報が交換されることなく、トランシーバ収容装置で保持又は生成され値が、通信網２に送信されてもよい。

[0193] 以上のように、制御部１４ｂに予めソフトウェア実装された装置用ソフトウェア（ゴールドストーン）を用いて、電気通信事業者の意図に反する動作がサービス提供に与える影響を抑制可能である。

[0194] （ハードウェア構成）

図７は、各実施形態における、通信システム１のハードウェア構成例を示す図である。図７に例示された通信システム１は、第１実施形態の通信システム１と、第２実施形態の通信システム１ａと、第３実施形態の通信システム１ｂと、第４実施形態の通信システム１とのそれぞれに相当する。図７に例示された通信システム１は、ＣＰＵ等のプロセッサ２０１が、不揮発性の記録媒体（非一時的な記録媒体）を有する記憶装置２０３とメモリ２０２とに記憶されたプログラムを実行することにより、ソフトウェアとして実現される。プログラムは、コンピュータ読み取り可能な記録媒体に記録されてもよい。コンピュータ読み取り可能な記録媒体とは、例えばフレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置などの非一時的な記録媒体である。通信部２０４は、通信処理を実行する。

[0195] 図７に例示された通信システム１は、例えば、ＬＳＩ（Large Scale Integrated circuit）、ＡＳＩＣ（Application Specific Integrated Circuit）、ＰＬＤ（Programmable Logic Device）又はＦＰＧＡ（Field Programmable Gate Array）等を用いた電子回路（electronic circuit又はcircuitry）を含むハードウェアを用いて実現されてもよい。

[0196] 以上、この発明の実施形態について図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

産業上の利用可能性

[0197] 本発明は、APN等の光通信システム（光伝送システム）に適用可能である。

符号の説明

[0198] １，１ａ，１ｂ…通信システム、２…通信網、１０，１０ａ，１０ｂ…トランシーバ収容装置、１１…制御信号送受信部、１２…主信号送受信部、１３…スイッチ、１４，１４ａ，１４ｂ…制御部、１５…主信号送受信部、２０，２０ａ，２０ｂ…制御装置、３０…ユーザ側制御端末、４０…ユーザ装置、１４１…受信制御部、１４２…ログイン制御部、１４３…遮断部、ＳＲ…制御信号経路

請求の範囲

[請求項1] 通信網と主信号送受信部との間の主信号を遮断して通信導通を許可する前に、前記通信網に配置された制御装置からの制御信号の経路を構築する受信制御部と、

前記制御装置からのログインを有効化し、前記主信号送受信部の関連設定の変更が可能なユーザ側制御端末からのログインを無効化し、前記ユーザ側制御端末からのログインの無効化が維持されている場合に前記遮断を解除して前記通信導通を許可し、前記ユーザ側制御端末からのログインの無効化が維持されていない場合に前記ユーザ側制御端末からのログインを再び無効化する、又は、再び遮断するログイン制御部と

を備える通信システム。

[請求項2] 前記ログイン制御部は、前記ユーザ側制御端末からのログインの無効化が維持されている場合に前記遮断を解除して前記通信導通を許可し、前記ユーザ側制御端末からのログインの無効化が維持されていない場合に前記ユーザ側制御端末からのログインを再び無効化する、請求項１に記載の通信システム。

[請求項3] 前記ユーザ側制御端末からのログインの無効化が維持されていない場合に前記通信導通を遮断し、前記ユーザ側制御端末からのログインの無効化が維持されている場合に前記通信導通の遮断を解除する遮断部を更に備える、請求項１又は請求項２に記載の通信システム。

[請求項4] 通信システムが実行する設定方法であって、

通信網と主信号送受信部との間の主信号を遮断して通信導通を許可する前に、前記通信網に配置された制御装置からの制御信号の経路を構築するステップと、

前記制御装置からのログインを有効化し、前記主信号送受信部の関連設定の変更が可能なユーザ側制御端末からのログインを無効化し、前記ユーザ側制御端末からのログインの無効化が維持されている場合

に前記遮断を解除して前記通信導通を許可し、前記ユーザ側制御端末からのログインの無効化が維持されていない場合に前記ユーザ側制御端末からのログインを再び無効化する、又は、再び遮断するステップと

を含む設定方法。

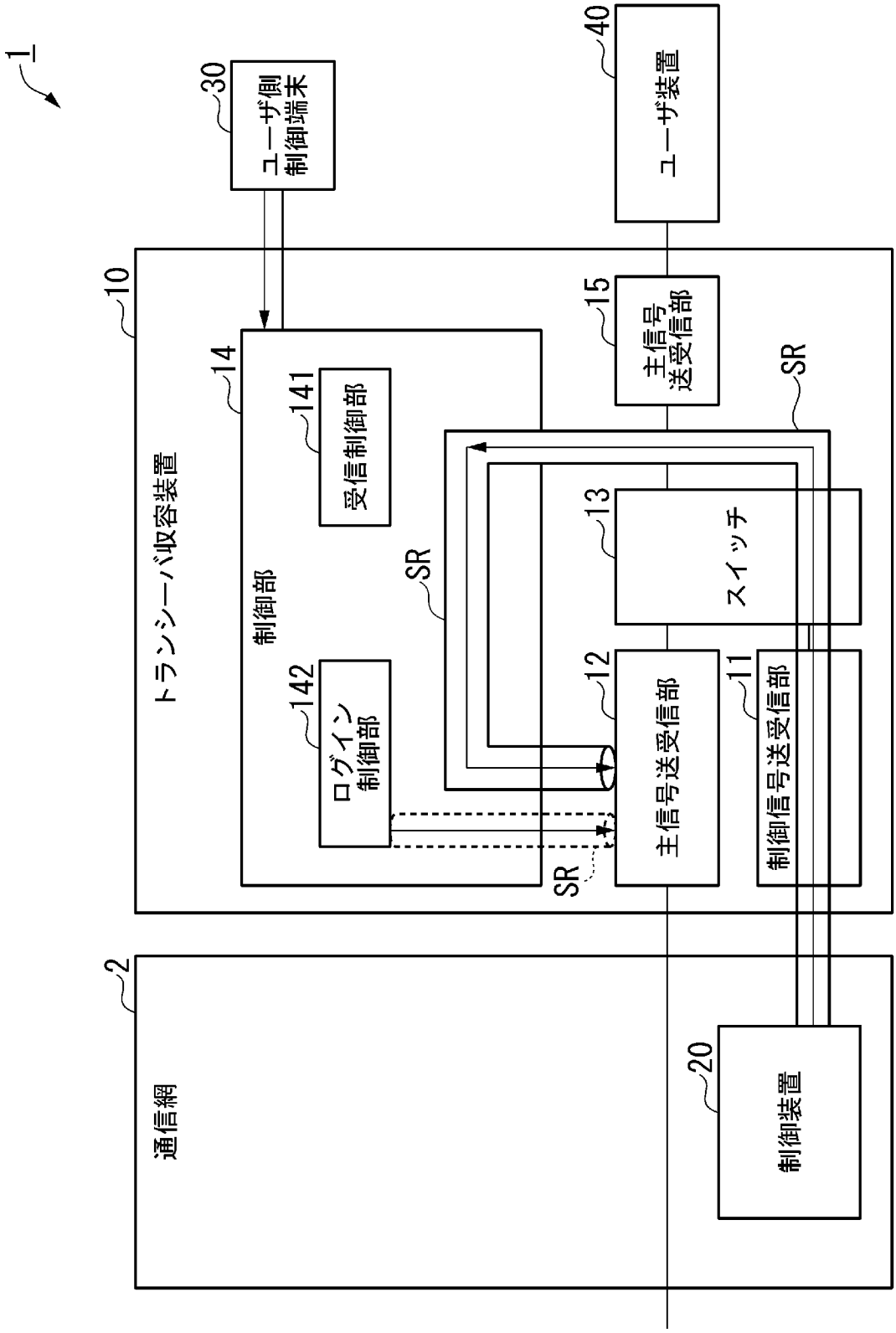
[請求項5] コンピュータに、

通信網と主信号送受信部との間の主信号を遮断して通信導通を許可する前に、前記通信網に配置された制御装置からの制御信号の経路を構築する手順と、

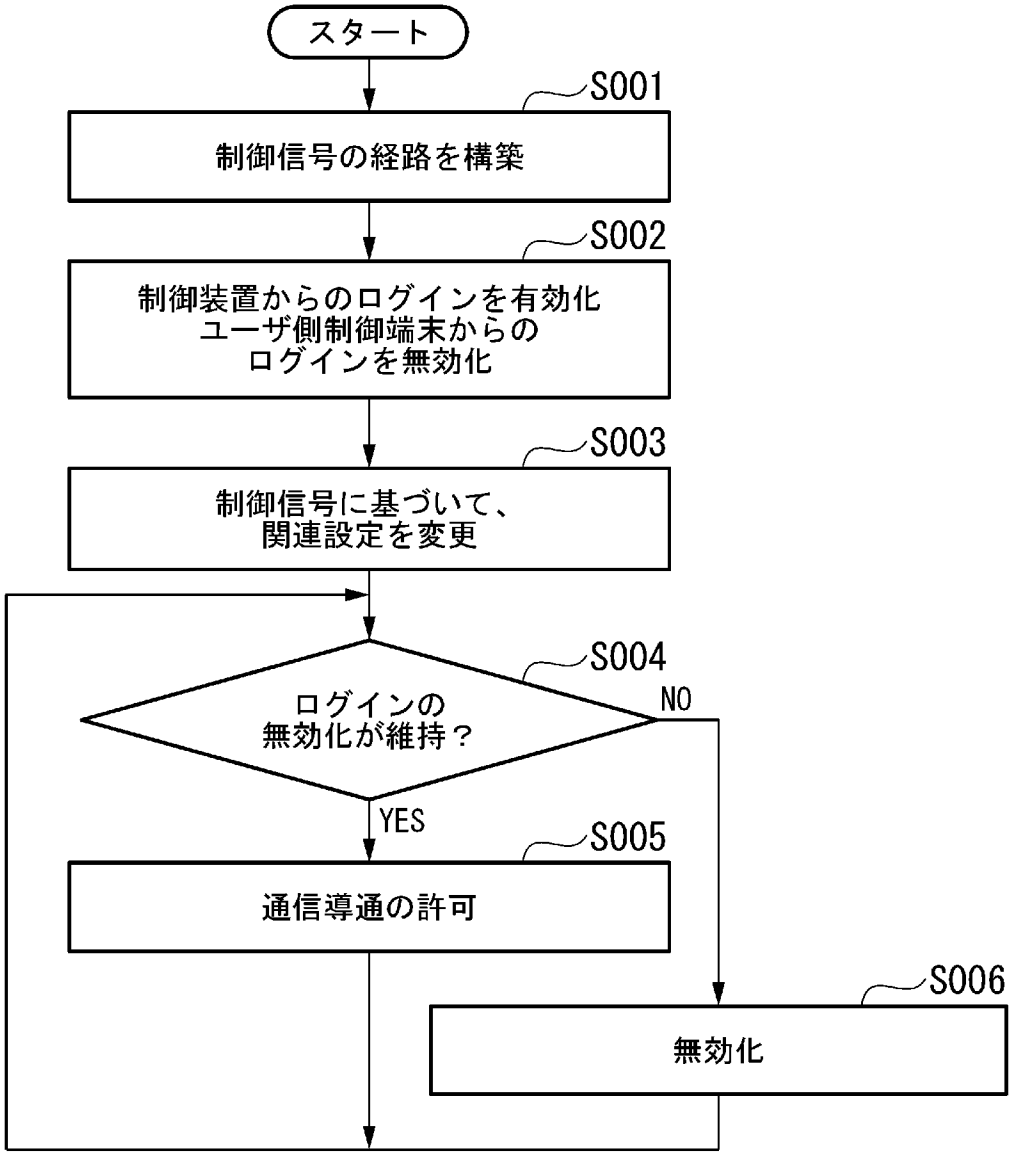
前記制御装置からのログインを有効化し、前記主信号送受信部の関連設定の変更が可能なユーザ側制御端末からのログインを無効化し、前記ユーザ側制御端末からのログインの無効化が維持されている場合に前記遮断を解除して前記通信導通を許可し、前記ユーザ側制御端末からのログインの無効化が維持されていない場合に前記ユーザ側制御端末からのログインを再び無効化する、又は、再び遮断する手順と

を実行させるためのプログラム。

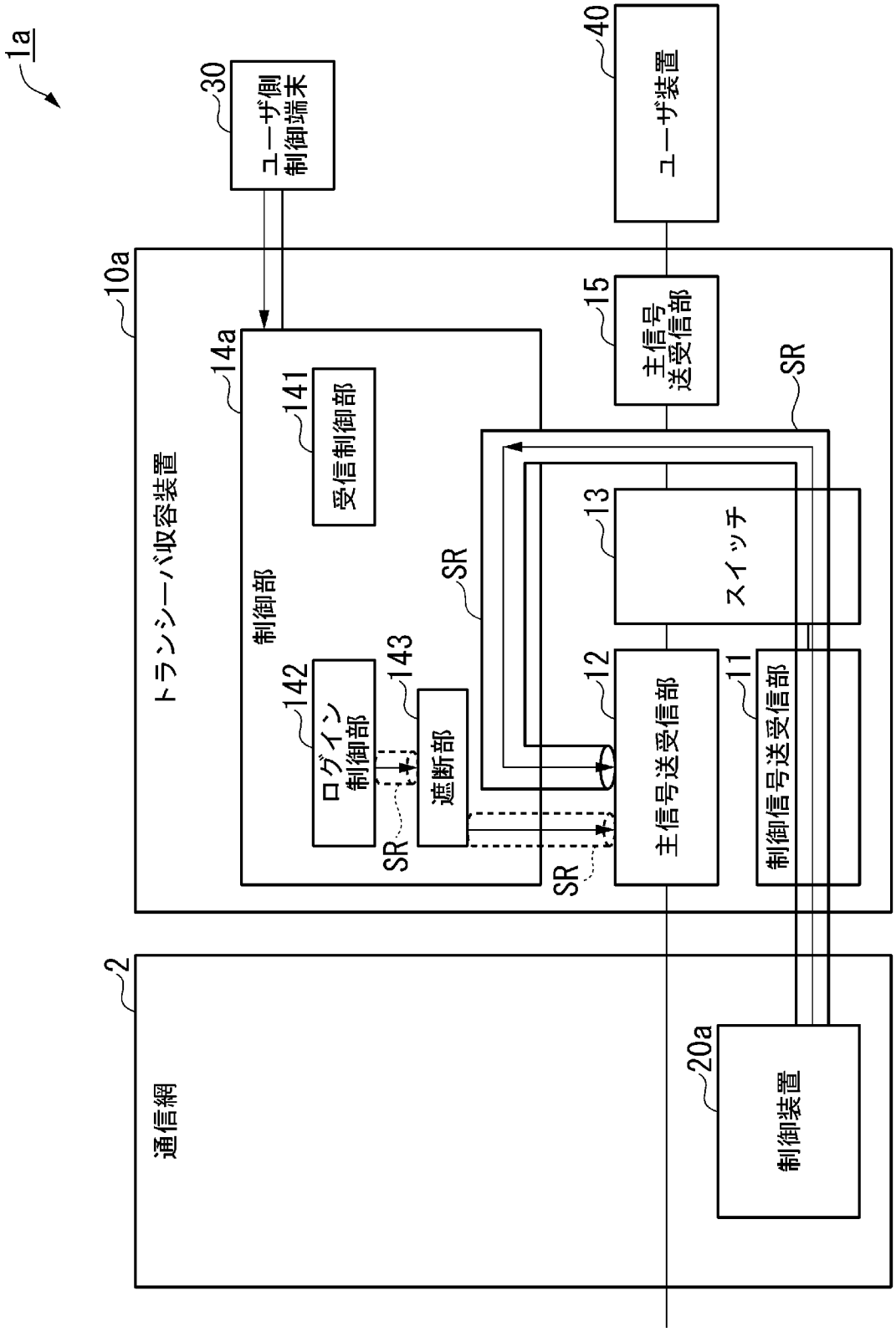
[図1]


1
30
ユーザ側制御端末
40
ユーザ装置
10
トランシーバ収容装置
14
制御部
141
受信制御部
142
ログイン制御部
15
主信号送受信部
SR
13
スイッチ
12
主信号送受信部
11
制御信号送受信部
2
通信網
20
制御装置

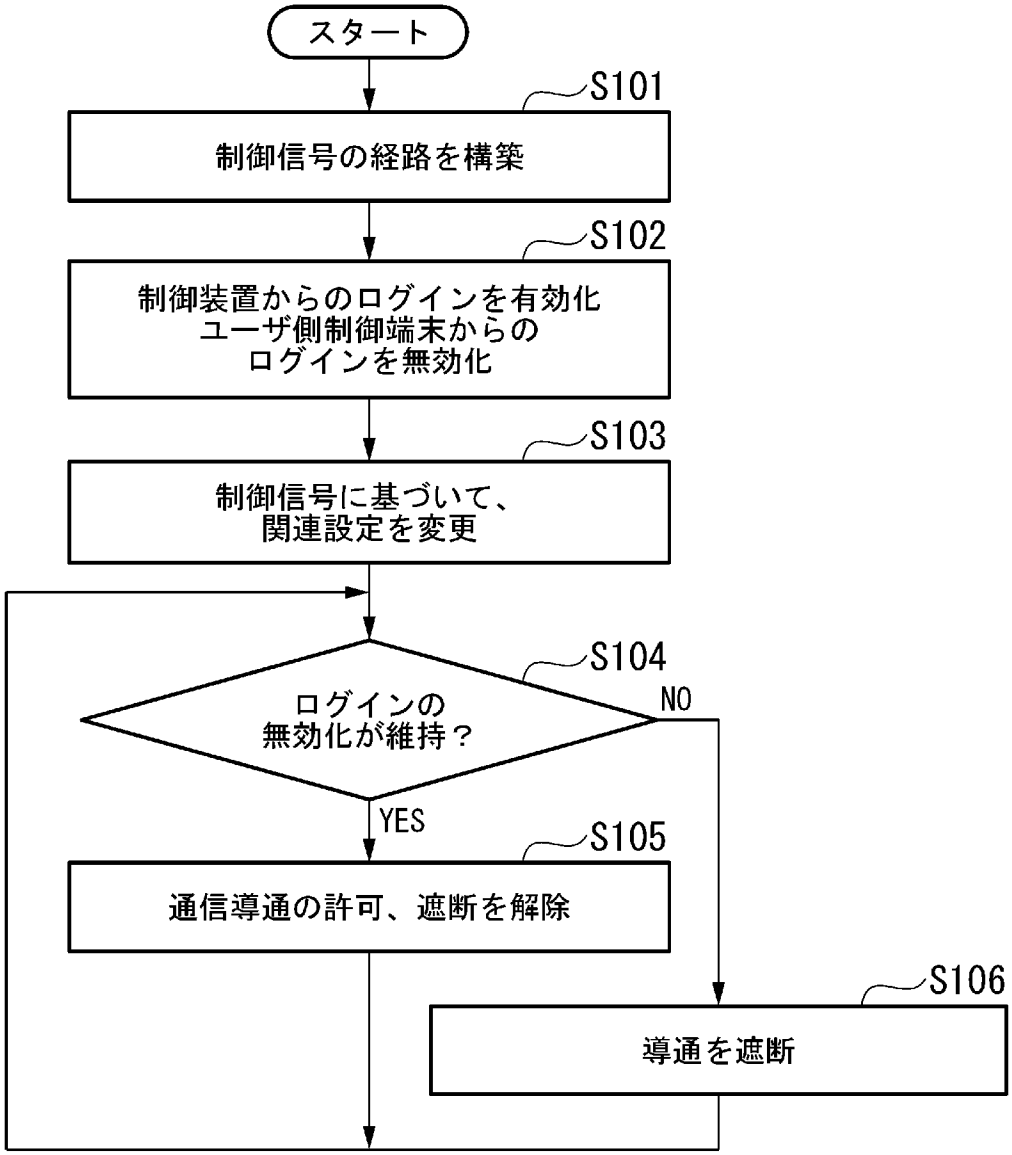
[図2]


スタート
S001
制御信号の経路を構築
S002
制御装置からのログインを有効化
ユーザ側制御端末からの
ログインを無効化
S003
制御信号に基づいて、
関連設定を変更
S004
ログインの
無効化が維持？
NO
YES
S005
通信導通の許可
S006
無効化

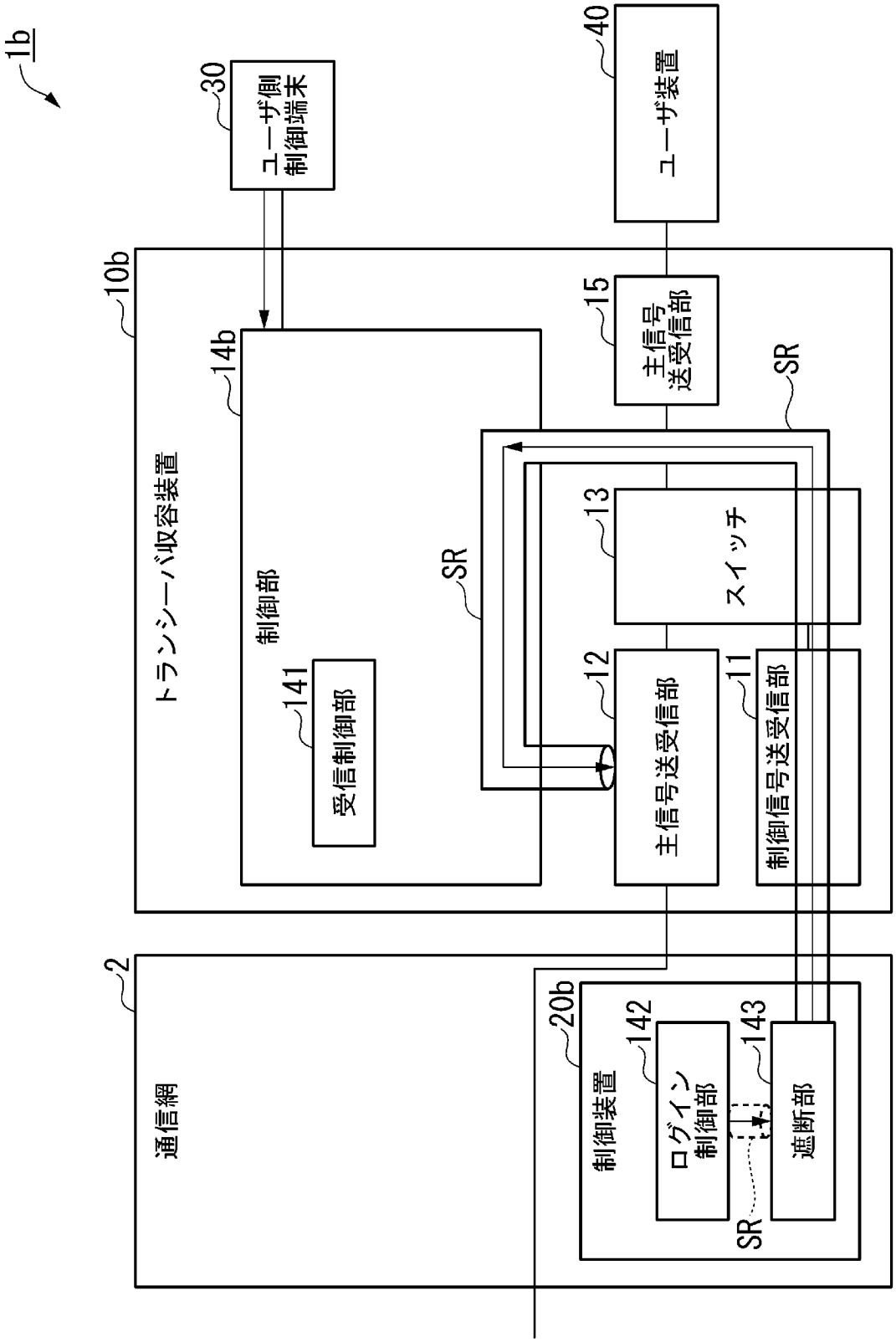
[図3]


1a
30
ユーザ側制御端末
40
ユーザ装置
10a
トランシーバ収容装置
14a
制御部
141
受信制御部
142
ログイン制御部
143
遮断部
15
主信号送受信部
SR
13
スイッチ
12
主信号送受信部
11
制御信号送受信部
2
通信網
20a
制御装置

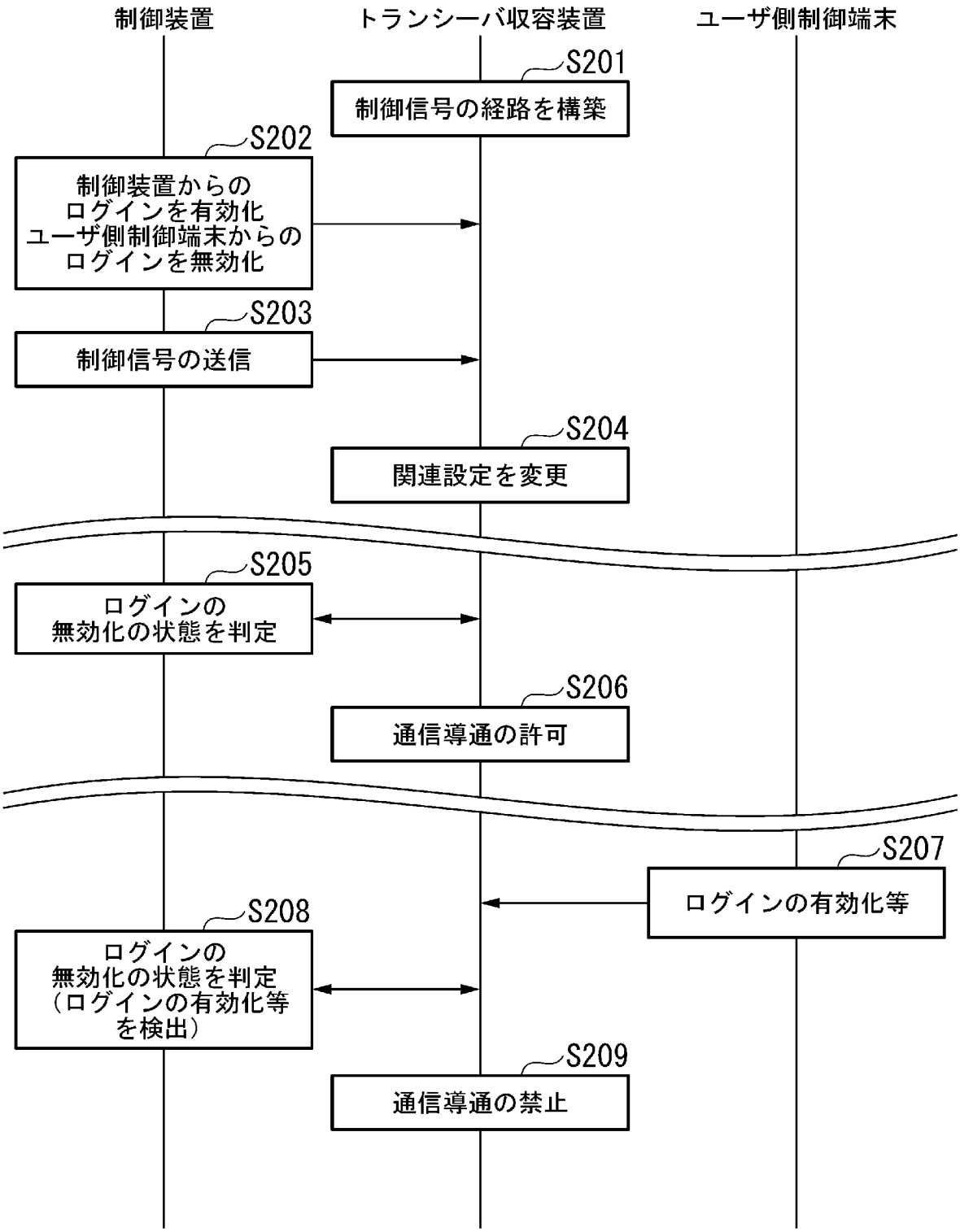
[図4]


スタート
S101
制御信号の経路を構築
S102
制御装置からのログインを有効化
ユーザ側制御端末からの
ログインを無効化
S103
制御信号に基づいて、
関連設定を変更
S104
ログインの
無効化が維持？
NO
YES
S105
通信導通の許可、遮断を解除
S106
導通を遮断

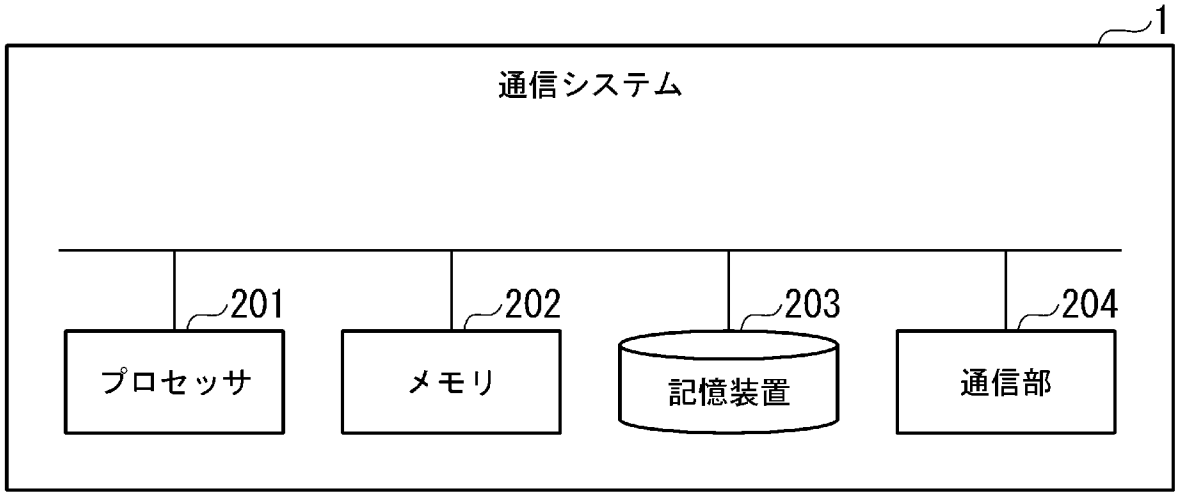
[図5]


1b
30
ユーザ側制御端末
40
ユーザ装置
10b
トランシーバ収容装置
14b
制御部
141
受信制御部
15
主信号送受信部
SR
13
スイッチ
12
主信号送受信部
11
制御信号送受信部
2
通信網
20b
制御装置
142
ログイン制御部
143
遮断部
SR

[図6]


制御装置
トランシーバ収容装置
ユーザ側制御端末
S201
制御信号の経路を構築
S202
制御装置からの
ログインを有効化
ユーザ側制御端末からの
ログインを無効化
S203
制御信号の送信
S204
関連設定を変更
S205
ログインの
無効化の状態を判定
S206
通信導通の許可
S207
ログインの有効化等
S208
ログインの
無効化の状態を判定
（ログインの有効化等
を検出）
S209
通信導通の禁止

[図7]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2022/047830

A. CLASSIFICATION OF SUBJECT MATTER

H04L 41/28(2022.01)i
FI: H04L41/28

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)

H04L41/28

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.
A	JP 2013-201521 A (MITSUBISHI ELECTRIC CORPORATION) 03 October 2013 (2013-10-03) entire text, all drawings (Family: none)	1-5
A	JP 2013-17026 A (NEC CORP.) 24 January 2013 (2013-01-24) entire text, all drawings (Family: none)	1-5
A	JP 2006-318383 A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 24 November 2006 (2006-11-24) entire text, all drawings (Family: none)	1-5

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 March 2023	**20 March 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.

国際調査報告

国際出願番号
PCT/JP2022/047830

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 41/28(2022.01)i
FI: H04L41/28

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））

H04L41/28

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２３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
A	JP 2013-201521 A (三菱電機株式会社) 03.10.2013 (2013-10-03) 全文、全図 (ファミリーなし)	1-5
A	JP 2013-17026 A (日本電気株式会社) 24.01.2013 (2013-01-24) 全文、全図 (ファミリーなし)	1-5
A	JP 2006-318383 A (日本電信電話株式会社) 24.11.2006 (2006-11-24) 全文、全図 (ファミリーなし)	1-5

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 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	国際調査報告の発送日
07.03.2023	20.03.2023

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）
宮島　郁美 5X 8523

電話番号 03-3581-1101 内線 3596