(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
2016 年 9 月 15 日(15.09.2016)

WIPO | PCT

(10) 国際公開番号
WO 2016/143003 A1

(51) 国際特許分類:
G06F 13/00 (2006.01)

(21) 国際出願番号: PCT/JP2015/056686

(22) 国際出願日: 2015 年 3 月 6 日(06.03.2015)

(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: 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者: ▲高▼宮　淳一 (TAKAMIYA, Junichi); 〒2118588 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 Kanagawa (JP).

(74) 代理人: 原田　一男 (HARADA, Kazuo); 〒1440052 東京都大田区蒲田五丁目４９番１２号蒲田M＆M１ビル６階 Tokyo (JP).

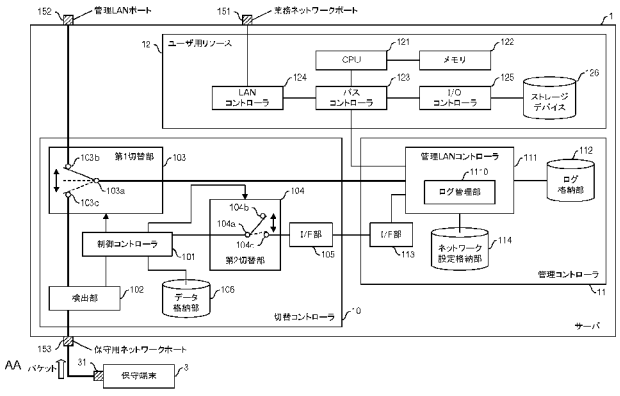
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, 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, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) **Title**: INFORMATION PROCESSING APPARATUS AND MAINTENANCE SYSTEM

(54) 発明の名称 : 情報処理装置及び保守システム



1 Server
3 Maintenance terminal
10 Switching controller
11 Management controller
12 User resources
101 Control controller
102 Detection section
103 First switching section
104 Second switching section
105, 113 I/F section
106 Data storage section
111 Management LAN controller
112 Log storage section
114 Network setting storage section
122 Memory
123 Bus controller
124 LAN controller
125 Input/output controller
126 Storage device
151 Business network port
152 Management LAN port
153 Maintenance network port
1110 Log management section
AA Packets

(57) **Abstract**: This information processing apparatus has: a detection section that detects connection of a first device to a first network port; a control section that changes the network setting of the information processing apparatus to a network setting for the first network port, when the detection section has detected the connection of the first device to the first network port; and a switching section that performs switching a transmission line in the information processing apparatus to enable the first device to perform communication via the first network port, when the detection section has detected the connection of the first device to the first network port.

(57) 要約:　本情報処理装置は、第１のネットワークポートに第１の装置が接続されたことを検出する検出部と、第１のネットワークポートに第１の装置が接続されたことが検出部により検出された場合、情報処理装置のネットワーク設定を、第１のネットワークポート用のネットワーク設定に変更する制御部と、第１のネットワークポートに第１の装置が接続されたことが検出部により検出された場合、第１の装置が第１のネットワークポートを介した通信を行えるように情報処理装置内の伝送路の切替を行う切替部とを有する。

WO 2016/143003 A1

明　細　書

発明の名称 ： 情報処理装置及び保守システム

技術分野

[0001] 情報処理装置の保守技術に関する。

背景技術

[0002] サーバは、サーバ上で動作するユーザ用ＯＳ（Operating System）が使用するネットワーク（以下、業務ネットワークと呼ぶ）とは別に、管理用のネットワーク（以下、管理ネットワークと呼ぶ）に接続されることがある。管理ネットワークは、サーバ内の管理コントローラにアクセスするための専用のネットワークである。業務ネットワークと管理ネットワークとは物理的に分けられているため、ＯＳ上にあるユーザデータに管理ネットワークからアクセスすることはできない。

[0003] このようなサーバに対して保守員がメンテナンス作業を行う際、保守員は、サーバの動作をチェックするため、サーバに保存されたログの閲覧等を行う。但し、セキュリティの問題によりサーバを直接操作できない場合には、保守用の端末を管理ネットワークを介してサーバに接続することで、サーバに保存されているログにアクセスする。

[0004] ＴＣＰ／ＩＰｖ４（Transmission Control Protocol/Internet Protocol version 4）によれば、保守用の端末を管理ネットワーク経由でサーバに接続する場合、サーバと端末が同じネットワークに属していなければならない。両者を同じネットワークに属させるためには、例えば図１に示すように、端末のネットワーク設定をサーバのネットワーク設定に合わせて変更すればよい。図１の例においては、端末のＩＰアドレスが「１２８．１０．２０．３０」から「１９２．１６８．１．１１」に変更され、端末のサブネットマスクが「２５５．２５５．０．０」から「２５５．２５５．２５５．０」に変更されている。また、例えば図２に示すように、サーバのネットワーク設定を端末のネットワーク設定に合わせて変更してもよい。図２の例においては

、サーバのＩＰアドレスが「１９２．１６８．１．１０」から「１２８．１０．２０．３１」に変更され、サーバのサブネットマスクが「２５５．２５５．２５５．０」から「２５５．２５５．０．０」に変更されている。

[0005] 但し、保守員がサーバのネットワーク設定を取得できない（例えば、ユーザがネットワーク設定の公開を望まない）場合がある。この場合、保守員はネットワーク設定を合致させることができないので、端末をサーバ内のログにアクセスさせることができず、メンテナンス作業を行うことができない。サーバと端末との接続に関する従来技術においては、このような問題には着目されていない。

先行技術文献

特許文献

[0006] 特許文献1：特開平０８－１１０８７９号公報

発明の概要

発明が解決しようとする課題

[0007] 従って、１つの側面では、本発明の目的は、サーバに端末を接続した場合に、サーバのネットワーク設定を接続した端末用のネットワーク設定に変更するための技術を提供することである。

課題を解決するための手段

[0008] 本発明に係る情報処理装置は、第１のネットワークポートに第１の装置が接続されたことを検出する検出部と、第１のネットワークポートに第１の装置が接続されたことが検出部により検出された場合、情報処理装置のネットワーク設定を、第１のネットワークポート用のネットワーク設定に変更する制御部と、第１のネットワークポートに第１の装置が接続されたことが検出部により検出された場合、第１の装置が第１のネットワークポートを介した通信を行えるように情報処理装置内の伝送路の切替を行う切替部とを有する。

発明の効果

[0009] １つの側面では、サーバに端末を接続した場合に、サーバのネットワーク設定を接続した端末用のネットワーク設定に変更できるようになる。

図面の簡単な説明

[0010] [図1]図１は、ネットワーク設定の変更について説明するための図である。

[図2]図２は、ネットワーク設定の変更について説明するための図である。

[図3]図３は、第１の実施の形態のシステム概要を示す図である。

[図4]図４は、データ格納部に格納されるデータの一例を示す図である。

[図5]図５は、保守端末の機能ブロック図である。

[図6]図６は、第１の実施の形態の概要を説明するための図である。

[図7]図７は、第１の実施の形態のサーバが実行する処理の処理フローを示す図である。

[図8]図８は、退避処理の処理フローを示す図である。

[図9]図９は、第１の実施の形態における設定切替処理の処理フローを示す図である。

[図10]図１０は、第１の実施の形態のサーバが実行する処理の処理フローを示す図である。

[図11]図１１は、第１の実施の形態のサーバが実行する処理の処理フローを示す図である。

[図12]図１２は、第２の実施の形態のシステム概要を示す図である。

[図13]図１３は、第２の実施の形態のサーバが実行する処理の処理フローを示す図である。

[図14]図１４は、第２の実施の形態のサーバが実行する処理の処理フローを示す図である。

[図15]図１５は、第２の実施の形態のサーバが実行する処理の処理フローを示す図である。

[図16]図１６は、第３の実施の形態のサーバが実行する処理の処理フローを示す図である。

[図17]図１７は、第３の実施の形態の保守端末が実行する処理の処理フロー

を示す図である。

[図18]図１８は、第４の実施の形態のシステム概要を示す図である。

[図19]図１９は、第４の実施の形態のサーバが実行する処理の処理フローを示す図である。

[図20]図２０は、第４の実施の形態のサーバが実行する処理の処理フローを示す図である。

[図21]図２１は、第５の実施の形態の概要を説明するための図である。

[図22]図２２は、第５の実施の形態のサーバが実行する処理の処理フローを示す図である。

[図23]図２３は、第５の実施の形態における設定切替処理の処理フローを示す図である。

[図24]図２４は、第５の実施の形態のサーバが実行する処理の処理フローを示す図である。

[図25]図２５は、コンピュータの機能ブロック図である。

発明を実施するための形態

[0011] ［実施の形態１］

図３に、本実施の形態におけるシステム概要を示す。サーバ１は、業務ネットワークに接続されるネットワークポートである業務ネットワークポート１５１と、管理ＬＡＮ（Local Area Network）に接続されるネットワークポートである管理ＬＡＮポート１５２と、保守端末３をサーバ１に接続させるためのネットワークポートである保守用ネットワークポート１５３とを有する。保守用ネットワークポート１５３には、ＬＡＮケーブル等を介して保守端末３が接続される。

[0012] サーバ１は、例えばＮＩＣ（Network Interface Card）である切替コントローラ１０と、管理コントローラ１１と、サーバ１のユーザ用のリソースであるユーザ用リソース１２とを有する。

[0013] 切替コントローラ１０は、制御コントローラ１０１と、検出部１０２と、第１切替部１０３と、第２切替部１０４と、Ｉ／Ｆ（InterFace）部１０５と

、データ格納部１０６とを有する。

[0014] 制御コントローラ１０１は、第１切替部１０３及び第２切替部１０４を制御する処理等を実行する。検出部１０２は、保守用ネットワークポート１５３に保守端末３が接続されたことを検出する処理等を実行する。

[0015] 第１切替部１０３は、伝送路の切替を行うスイッチである。具体的には、第１切替部１０３は、管理ＬＡＮポート１５２と管理コントローラ１１とをつなぐ伝送路（以下、第１の伝送路と呼ぶ）と、保守用ネットワークポート１５３と管理コントローラ１１とをつなぐ伝送路（以下、第２の伝送路と呼ぶ）と、いずれの伝送路も切断された状態とを切り替える。第１の伝送路を生成する場合、第１切替部１０３は、接点１０３ａと接点１０３ｂとを接続する。第２の伝送路を生成する場合、第１切替部１０３は、接点１０３ａと接点１０３ｃとを接続する。両方の伝送路を切断する場合、第１切替部１０３は、接点１０３ａを接点１０３ｂ及び１０３ｃのいずれにも接続しない。

[0016] 第２切替部１０４は、制御コントローラ１０１とＩ／Ｆ部１０５との間の伝送路を生成及び切断するスイッチである。具体的には、第２切替部１０４は、制御コントローラ１０１とＩ／Ｆ部１０５とを伝送路でつなぐ場合、接点１０４ａと接点１０４ｃとを接続する。制御コントローラ１０１とＩ／Ｆ部１０５とを伝送路でつながない場合、第２切替部１０４は、接点１０４ａと接点１０４ｂとを接続する。Ｉ／Ｆ部１０５は、管理コントローラ１１と接続するためのインタフェースである。

[0017] 図４に、データ格納部１０６に格納されるデータの一例を示す。データ格納部１０６は、識別データ格納領域と、管理ＬＡＮ設定格納領域と、保守用設定格納領域とを含む。識別データ格納領域には、識別データが予め格納される。管理ＬＡＮ設定格納領域は、管理ＬＡＮ設定を退避するための領域である。保守用設定格納領域には、保守用設定が予め格納される。識別データとは、保守端末３がサーバ１にアクセスする際に使用されるデータである。管理ＬＡＮ設定とはサーバ１の元々のネットワーク設定であり、本実施の形態においては、ネットワーク設定はＩＰアドレス及びサブネットマスクを含

む。保守用設定とはサーバ１に保守端末３が接続された際に使用されるネットワーク設定であり、管理ＬＡＮ設定と同様、保守用設定はＩＰアドレス及びサブネットマスクを含む。このように、保守用設定を予め用意しておくことで、サーバ１の元々のネットワーク設定の取得に制限がある場合であっても、保守端末３がサーバ１内のデータにアクセスすることができるようになる。

[0018] 図３の説明に戻り、管理コントローラ１１は、ログ管理部１１１０を有する管理ＬＡＮコントローラ１１１と、ログ格納部１１２と、Ｉ／Ｆ部１１３と、ネットワーク設定格納部１１４とを有する。

[0019] ログ管理部１１１０は、ログ格納部１１２に格納されたログを管理する処理等を実行する。ログ格納部１１２には、サーバ１に関するログ（例えば、動作ログ）が格納される。Ｉ／Ｆ部１１３は、切替コントローラ１０と接続するためのインタフェースである。ネットワーク設定格納部１１４には、サーバ１のネットワーク設定が格納される。

[0020] ユーザ用リソース１２は、ＣＰＵ１２１と、メモリ１２２と、バスコントローラ１２３と、ＬＡＮコントローラ１２４と、Ｉ／Ｏ（Input/Output）コントローラ１２５と、ストレージデバイス１２６とを有する。サーバ１のＯＳのプログラム及びアプリケーションプログラムはストレージデバイス１２６に格納されており、メモリ１２２にロードされＣＰＵ１２１により実行される。なお、ユーザ用リソース１２は通常のコンピュータに用いられるリソースと同じであるので、ここでは詳細な説明を省略する。

[0021] 図５に、保守端末３の機能ブロック図を示す。保守端末３は、通信部３０１と、ネットワーク設定格納部３０２と、識別データ格納部３０３と、ポート３１とを有する。通信部３０１は、サーバ１にデータを送信する処理及びサーバ１からデータを受信する処理を実行する。ネットワーク設定格納部３０２には、保守用設定（本実施の形態においては、ＩＰアドレス及びサブネットマスク）が予め格納される。保守端末３のネットワーク設定格納部３０２に格納されるネットワーク設定が表すネットワークは、保守用設定格納領

域に格納されるネットワーク設定が表すネットワークと同じである。識別データ格納部３０３には、保守端末３がサーバ１にアクセスする際に使用される識別データが予め格納される。

[0022] 次に、図６を用いて、本実施の形態の概要について説明する。

[0023] まず、サーバ１の保守用ネットワークポート１５３に接続された保守端末３が、ネットワーク識別データ（００－００－５Ｅ－００－０１－０１）とネットワーク設定（１９２．１６８．１．１０／２５５．２５５．２５５．０）とを含むパケットをサーバ１に送信する。サーバ１における切替コントローラ１０は、パケットに含まれるネットワーク識別データと、切替コントローラ１０に予め登録されたネットワーク識別データ（００－００－５Ｅ－００－０１－０１）とが一致する場合、保守用ネットワークポート１５３と管理コントローラ１１とを伝送路でつなげる。

[0024] 但し、切替コントローラ１０は、保守端末３のアクセスが開始される前に、管理コントローラ１１のネットワーク設定格納部１１４に格納されたネットワーク設定（１９２．１６８．２．１０／２５５．２５５．２５５．０）を、保守端末３がアクセスできない領域に退避しておく。また、切替コントローラ１０は、管理コントローラ１１のネットワーク設定格納部１１４に格納されているネットワーク設定を、管理ＬＡＮ設定（１９２．１６８．２．１０／２５５．２５５．２５５．０）から保守用設定（１９２．１６８．１．１０／２５５．２５５．２５５．０）に変更しておく。

[0025] すると、管理コントローラ１１のネットワーク設定格納部１１４に格納されたネットワーク設定（１９２．１６８．１．１０／２５５．２５５．２５５．０）と、保守端末３が送信したパケットに含まれるネットワーク設定（１９２．１６８．１．１０／２５５．２５５．２５５．０）とが一致するようになる。これにより、保守端末３は、ログ格納部１１２に格納されたログを管理コントローラ１１から取得できるようになる。また、保守端末３の接続が終了した場合には、退避されたネットワーク設定を、管理コントローラ１１のネットワーク設定格納部１１４に再び格納することで、通常の運用を

再開できるようになる。

[0026] 次に、図７乃至図１１を用いて、本実施の形態についてより詳細に説明する。はじめに、保守端末３がサーバ１に接続される際の処理について説明する。

[0027] まず、検出部１０２は、保守用ネットワークポート１５３の状態を確認し（図７：ステップＳ１）、保守用ネットワークポート１５３にＬＡＮケーブルが接続された（すなわち、リンクアップした）か判断する（ステップＳ３）。

[0028] 保守用ネットワークポート１５３にＬＡＮケーブルが接続されていない場合（ステップＳ３：Ｎｏルート）、検出部１０２は所定時間待機し、ステップＳ１の処理に戻る。一方、保守用ネットワークポート１５３にＬＡＮケーブルが接続された場合（ステップＳ３：Ｙｅｓルート）、検出部１０２は、ＬＡＮケーブルを介して受信したパケットから、ネットワーク識別データを取り出す（ステップＳ５）。本実施の形態においては、ネットワーク識別データは仮想ＭＡＣ（Media Access Control）アドレスであり、パケットにおける送信元ＭＡＣアドレスのフィールドに格納される。

[0029] 検出部１０２は、ネットワーク識別データを取得することを要求する第１取得要求を制御コントローラ１０１に出力する。これに応じ、制御コントローラ１０１は、ネットワーク識別データをデータ格納部１０６における識別データ格納領域から読み出し（ステップＳ７）、検出部１０２に通知する。

[0030] 検出部１０２は、ステップＳ５においてパケットから取り出したネットワーク識別データと、ステップＳ７において識別データ格納領域から読み出したネットワーク識別データとが一致するか判断する（ステップＳ９）。

[0031] ステップＳ５においてパケットから取り出したネットワーク識別データと、ステップＳ７において識別データ格納領域から読み出したネットワーク識別データとが一致しない場合（ステップＳ９：Ｎｏルート）、受信したパケットを廃棄し、ステップＳ１の処理に戻る。

[0032] 一方、ステップＳ５においてパケットから取り出したネットワーク識別デ

ータと、ステップＳ７において識別データ格納領域から読み出したネットワーク識別データとが一致する場合（ステップＳ９：Ｙｅｓルート）、検出部１０２は、ネットワーク識別データが一致したことを制御コントローラ１０１に通知する。

[0033] 制御コントローラ１０１は、第１の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第１切替部１０３は、管理ＬＡＮコントローラ１１１と管理ＬＡＮポート１５２とをつなぐ伝送路を切断し、いずれの伝送路も切断された状態に切り替える。また、第２切替部１０４は、接点１０４ａと接点１０４ｃとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とを伝送路でつなぐ（ステップＳ１１）。

[0034] 制御コントローラ１０１は、退避処理を実行する（ステップＳ１３）。退避処理については、図８を用いて説明する。

[0035] まず、切替コントローラ１０における制御コントローラ１０１は、管理ＬＡＮ設定の取得を要求する第２取得要求を管理コントローラ１１における管理ＬＡＮコントローラ１１１に送信する（図８：ステップＳ３１）。ここでは、制御コントローラ１０１と管理ＬＡＮコントローラ１１１とをつなぐ伝送路を介して第２取得要求が送信される。

[0036] 管理コントローラ１０における管理ＬＡＮコントローラ１１１は、制御コントローラ１０１から第２取得要求を受信する（ステップＳ３３）。そして、管理ＬＡＮコントローラ１１１は、管理ＬＡＮ設定をネットワーク設定格納部１１４から読み出し（ステップＳ３５）、読み出した管理ＬＡＮ設定を含む応答を、制御コントローラ１０１に送信する（ステップＳ３７）。ここでは、制御コントローラ１０１と管理ＬＡＮコントローラ１１１とをつなぐ伝送路を介して応答が送信される。

[0037] 制御コントローラ１０１は、管理ＬＡＮコントローラ１１１から応答を受信し（ステップＳ３９）、データ格納部１０６における管理ＬＡＮ設定格納領域に、応答に含まれる管理ＬＡＮ設定を格納する（ステップＳ４１）。そして呼び出し元の処理に戻る。

[0038] 以上のような処理を実行すれば、ネットワーク設定の変更によって管理ＬＡＮ設定が失われることを防げるようになる。また、データ格納部１０６は保守端末３がアクセスできない場所にあるので、管理コントローラ１１へのアクセスを許可したとしても管理ＬＡＮ設定が漏洩してしまうことは無い。

[0039] 図７の説明に戻り、制御コントローラ１０１は、第１の実施の形態における設定切替処理を実行する（ステップＳ１５）。設定切替処理については、図９を用いて説明する。

[0040] まず、切替コントローラ１０における制御コントローラ１０１は、データ格納部１０６における保守用設定格納領域に格納された保守用設定を読み出す（図９：ステップＳ５１）。そして、制御コントローラ１０１は、ステップＳ５１において読み出した保守用設定を、管理ＬＡＮコントローラ１１１に送信する（ステップＳ５３）。ここでは、制御コントローラ１０１と管理ＬＡＮコントローラ１１１とをつなぐ伝送路を介して保守用設定が送信される。

[0041] 管理コントローラ１１における管理ＬＡＮコントローラ１１１は、制御コントローラ１０１から保守用設定を受信する（ステップＳ５５）。そして、管理ＬＡＮコントローラ１１１は、ネットワーク設定格納部１１４に格納されているネットワーク設定（ここでは、管理ＬＡＮ設定）を、ステップＳ５５において受信した保守用設定に変更する（ステップＳ５７）。そして呼び出し元の処理に戻り、処理は端子Ａを介して図１０のステップＳ１７の処理に移行する。

[0042] 以上のような処理を実行すれば、保守端末３が管理コントローラ１１にアクセスすることが許可されるようになる。

[0043] 図１０の説明に移行し、制御コントローラ１０１は、第２の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第２切替部１０４は、接点１０４ａと接点１０４ｂとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とをつなぐ伝送路を切断する。また、第１切替部１０３は、接点１０３ａと接点１０３ｃとを接続すること

で、管理ＬＡＮコントローラ１１１と保守用ネットワークポート１５３とを伝送路でつなぐ（ステップＳ１７）。

[0044] ここで、保守端末３は管理コントローラ１１にアクセスし、ログ管理部１１１０を介してログ格納部１１２からログを取得する。ここでの処理については、後で説明する。

[0045] 検出部１０２は、保守用ネットワークポート１５３の状態を確認し（ステップＳ１９）、保守用ネットワークポート１５３にＬＡＮケーブルが接続されているか判断する（ステップＳ２１）。

[0046] 保守用ネットワークポート１５３にＬＡＮケーブルが接続されている場合（ステップＳ２１：Ｙｅｓルート）、ステップＳ１９の処理に戻る。一方、保守用ネットワークポート１５３にＬＡＮケーブルが接続されていない場合（ステップＳ２１：Ｎｏルート）、検出部１０２は、保守用ネットワークポート１５３にＬＡＮケーブルが接続されていないことを制御コントローラ１０１に通知する。

[0047] 制御コントローラ１０１は、第３の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第１切替部１０３は、管理ＬＡＮコントローラ１１１と保守用ネットワークポート１５３とをつなぐ伝送路を切断し、いずれの伝送路も切断された状態に切り替える。また、第２切替部１０４は、接点１０４ａと接点１０４ｃとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とを伝送路でつなぐ（ステップＳ２３）。

[0048] 制御コントローラ１０１は、ネットワーク設定格納部１１４に格納されたネットワーク設定（ここでは、保守用設定）を、データ格納部１０６における管理ＬＡＮ設定格納領域に退避した管理ＬＡＮ設定に変更する（ステップＳ２５）。具体的には、制御コントローラ１０１は、データ格納部１０６における管理ＬＡＮ設定格納領域に退避した管理ＬＡＮ設定を管理コントローラ１１に送信する。管理コントローラ１１における管理ＬＡＮコントローラ１１１は、ネットワーク設定格納部１１４に格納されているネットワーク設

定を、受信した管理ＬＡＮ設定に変更する。なお、ステップＳ２５においては、制御コントローラ１０１と管理ＬＡＮコントローラ１１１とをつなぐ伝送路を介して管理ＬＡＮ設定が送信される。

[0049] 制御コントローラ１０１は、第４の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第２切替部１０４は、接点１０４ａと接点１０４ｂとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とをつなぐ伝送路を切断する。また、第１切替部１０３は、接点１０３ａと接点１０３ｂとを接続することで、管理ＬＡＮコントローラ１１１と管理ＬＡＮポート１５２とを伝送路でつなぐ（ステップＳ２７）。そして処理を終了する。

[0050] 以上のような処理を実行すれば、元々のネットワーク設定（ここでは、管理ＬＡＮ設定）を保守員が事前に取得することができなくても、サーバ１のログを閲覧してメンテナンス作業を行えるようになる。また、ネットワーク設定の変更は自動で行われるので、保守員は特に意識することなくメンテナンス作業を開始できるようになる。また、メンテナンス作業の終了後は自動的にネットワーク設定が元に戻るので、保守員が誤ったネットワーク設定に戻してしまうことを防止できる。

[0051] 次に、図１１を用いて、保守端末３からのパケットを受信した管理コントローラ１１が実行する処理について説明する。

[0052] まず、切替コントローラ１０における検出部１０２は、パケットを受信する（図１１：ステップＳ６１）。検出部１０２は、ステップＳ２７において生成された伝送路を介して、受信したパケットを管理コントローラ１１に出力する。

[0053] 管理コントローラ１１は、受信したパケットに含まれるネットワーク設定と、ネットワーク設定格納部１１４に格納されているネットワーク設定とが一致するか判断する（ステップＳ６３）。

[0054] 受信したパケットに含まれるネットワーク設定と、ネットワーク設定格納部１１４に格納されているネットワーク設定とが一致する場合（ステップＳ

６３：Ｙｅｓルート）、管理ＬＡＮコントローラ１１１は、受信したパケットに含まれるデータに応じた処理を実行する（ステップＳ６５）。そして処理を終了する。例えば、パケットがログの取得を要求するログ要求パケットである場合、ログ管理部１１１０は、ログ格納部１１２から該当するログを読み出し、応答として保守端末３に送信する。

[0055] 一方、受信したパケットに含まれるネットワーク設定と、ネットワーク設定格納部１１４に格納されているネットワーク設定とが一致しない場合（ステップＳ６３：Ｎｏルート）、管理ＬＡＮコントローラ１１１は、受信したパケットを廃棄する（ステップＳ６７）。そして処理を終了する。

[0056] 以上のような処理を実行すれば、管理コントローラ１１にアクセスする資格が無い保守端末３からのアクセスを排除できるようになる。

[0057] ［実施の形態２］

第２の実施の形態においては、ハードウエアキーに基づく認証を利用することでセキュリティを高める方法について説明する。

[0058] 図１２に、第２の実施の形態のシステム概要を示す。サーバ１は、ハードウエアキー読み取り装置１３を有する。なお、サーバ１におけるハードウエアキー読み取り装置１３以外の部分は第１の実施の形態と同じであるので、説明に使用する部分以外を省略する。

[0059] ハードウエアキー読み取り装置１３は、ハードウエアキー読み取り装置１３に近付いたハードウエアキー５（例えば、ＩＣ（Integrated Circuit）チップを搭載したカード）から情報を取得し、ハードウエアキー読み取り装置１３に予め登録された情報と比較することで認証を行う。認証が成功した場合、ハードウエアキー読み取り装置１３は、認証が成功したことを切替コントローラ１０における制御コントローラ１０１に通知する。

[0060] 次に、図１３乃至図１５を用いて、第２の実施の形態におけるサーバ１が実行する処理について説明する。はじめに、ハードウエアキー５による認証が成功し且つネットワーク識別データが一致した場合に端子Ｂ以降の処理を実行する例について説明する。

[0061] まず、検出部１０２は、ハードウエアキー５による認証が成功したか判断する（図１３：ステップＳ７１）。ハードウエアキー５による認証が成功したか否かは、ハードウエアキー読み取り装置１３から認証が成功したことを通知された制御コントローラ１０１から、認証が成功したことを通知されたか否かによって判断される。

[0062] ハードウエアキー５による認証が成功していない場合（ステップＳ７１：Ｎｏルート）検出部１０２は所定時間待機し、ステップＳ７１の処理に戻る。一方、ハードウエアキー５による認証が成功した場合（ステップＳ７１：Ｙｅｓルート）、検出部１０２は、保守用ネットワークポート１５３の状態を確認し（ステップＳ７３）、保守用ネットワークポート１５３にＬＡＮケーブルが接続された（すなわち、リンクアップした）か判断する（ステップＳ７５）。

[0063] 保守用ネットワークポート１５３にＬＡＮケーブルが接続されていない場合（ステップＳ７５：Ｎｏルート）、ステップＳ７１の処理に戻る。一方、保守用ネットワークポート１５３にＬＡＮケーブルが接続された場合（ステップＳ７５：Ｙｅｓルート）、検出部１０２は、ＬＡＮケーブルを介して受信したパケットから、ネットワーク識別データを取り出す（ステップＳ７７）。本実施の形態においては、ネットワーク識別データは仮想ＭＡＣアドレスであり、パケットにおける送信元ＭＡＣアドレスのフィールドに格納される。

[0064] 検出部１０２は、ネットワーク識別データを取得することを要求する第１取得要求を制御コントローラ１０１に出力する。これに応じ、制御コントローラ１０１は、ネットワーク識別データをデータ格納部１０６における識別データ格納領域から読み出し（ステップＳ７９）、検出部１０２に通知する。

[0065] 検出部１０２は、ステップＳ７７においてパケットから取り出したネットワーク識別データと、ステップＳ７９において識別データ格納領域から読み出したネットワーク識別データとが一致するか判断する（ステップＳ８１）

。

[0066] ステップＳ７７においてパケットから取り出したネットワーク識別データと、ステップＳ７９において識別データ格納領域から読み出したネットワーク識別データとが一致しない場合（ステップＳ８１：Ｎｏルート）、受信したパケットを廃棄し、ステップＳ７１の処理に戻る。

[0067] 一方、ステップＳ７７においてパケットから取り出したネットワーク識別データと、ステップＳ７９において識別データ格納領域から読み出したネットワーク識別データとが一致する場合（ステップＳ８１：Ｙｅｓルート）、処理は端子Ｂを介して図７のステップＳ１１に移行する。

[0068] 以上のような処理を実行すれば、二重保護方式を実現できるので、セキュリティを高めることができるようになる。

[0069] 次に、図１４を用いて、ハードウエアキー５による認証が成功するか又はネットワーク識別データが一致した場合に端子Ｂ以降の処理を実行する例について説明する。

[0070] まず、検出部１０２は、ハードウエアキー５による認証が成功したか判断する（図１４：ステップＳ９１）。ハードウエアキー５による認証が成功したか否かは、ハードウエアキー読み取り装置１３から認証が成功したことを通知された制御コントローラ１０１から、認証が成功したことを通知されたか否かによって判断される。

[0071] ハードウエアキー５による認証が成功した場合（ステップＳ９１：Ｙｅｓルート）、処理は端子Ｂを介して図７のステップＳ１１に移行する。一方、ハードウエアキー５による認証が成功していない場合（ステップＳ９１：Ｎｏルート）、検出部１０２は、保守用ネットワークポート１５３の状態を確認し（ステップＳ９３）、保守用ネットワークポート１５３にＬＡＮケーブルが接続された（すなわち、リンクアップした）か判断する（ステップＳ９５）。

[0072] 保守用ネットワークポート１５３にＬＡＮケーブルが接続されていない場合（ステップＳ９５：Ｎｏルート）、ステップＳ９１の処理に戻る。一方、

保守用ネットワークポート１５３にＬＡＮケーブルが接続された場合（ステップＳ９５：Ｙｅｓルート）、検出部１０２は、ＬＡＮケーブルを介して受信したパケットから、ネットワーク識別データを取り出す（ステップＳ９７）。

[0073] 検出部１０２は、ネットワーク識別データを取得することを要求する第１取得要求を制御コントローラ１０１に出力する。これに応じ、制御コントローラ１０１は、ネットワーク識別データをデータ格納部１０６における識別データ格納領域から読み出し（ステップＳ９９）、検出部１０２に通知する。

[0074] 検出部１０２は、ステップＳ９７においてパケットから取り出したネットワーク識別データと、ステップＳ９９において識別データ格納領域から読み出したネットワーク識別データとが一致するか判断する（ステップＳ１０１）。

[0075] ステップＳ９７においてパケットから取り出したネットワーク識別データと、ステップＳ９９において識別データ格納領域から読み出したネットワーク識別データとが一致しない場合（ステップＳ１０１：Ｎｏルート）、受信したパケットを廃棄し、ステップＳ９１の処理に戻る。

[0076] 一方、ステップＳ９７においてパケットから取り出したネットワーク識別データと、ステップＳ９９において識別データ格納領域から読み出したネットワーク識別データとが一致する場合（ステップＳ１０１：Ｙｅｓルート）、処理は端子Ｂを介して図７のステップＳ１１に移行する。

[0077] 以上のような処理を実行すれば、ハードウエアキー５による認証が成功するか又はネットワーク識別データが一致すればよいので、保守員の利便性を高めることができるようになる。

[0078] 次に、図１５を用いて、ハードウエアキー５による認証が一旦成功した場合には以降ネットワーク識別データが一致さえすれば端子Ｂ以降の処理を実行する例について説明する。

[0079] まず、検出部１０２は、ハードウエアキー５による認証を既に行い成功し

たか判断する（図１５：ステップＳ１１１）。

[0080] ハードウエアキー５による認証が未だ成功していない場合（ステップＳ１１１：Ｎｏルート）、検出部１０２は、以下の処理を実行する。具体的には、検出部１０２は、ハードウエアキー５による認証が成功するまで待機する。そして、ハードウエアキー５による認証が成功した場合、検出部１０２は、受信したパケットの送信元ＭＡＣアドレスを取り出し、ネットワーク識別データとしてデータ格納部１０６における識別データ格納領域に保存する（ステップＳ１１３）。処理は端子Ｂを介して図７のステップＳ１１に移行する。

[0081] 一方、ハードウエアキー５による認証を既に行い成功した場合（ステップＳ１１１：Ｙｅｓルート）、検出部１０２は、保守用ネットワークポート１５３の状態を確認し（ステップＳ１１５）、保守用ネットワークポート１５３にＬＡＮケーブルが接続された（すなわち、リンクアップした）か判断する（ステップＳ１１７）。

[0082] 保守用ネットワークポート１５３にＬＡＮケーブルが接続されていない場合（ステップＳ１１７：Ｎｏルート）、ステップＳ１１１の処理に戻る。一方、保守用ネットワークポート１５３にＬＡＮケーブルが接続された場合（ステップＳ１１７：Ｙｅｓルート）、検出部１０２は、ＬＡＮケーブルを介して受信したパケットから、ネットワーク識別データを取り出す（ステップＳ１１９）。本実施の形態においては、ネットワーク識別データは仮想ＭＡＣアドレスであり、パケットにおける送信元ＭＡＣアドレスのフィールドに格納される。

[0083] 検出部１０２は、ネットワーク識別データを取得することを要求する第１取得要求を制御コントローラ１０１に出力する。これに応じ、制御コントローラ１０１は、ネットワーク識別データをデータ格納部１０６における識別データ格納領域から読み出し（ステップＳ１２１）、検出部１０２に通知する。

[0084] 検出部１０２は、ステップＳ１１９においてパケットから取り出したネッ

トワーク識別データと、ステップＳ１２１において識別データ格納領域から読み出したネットワーク識別データとが一致するか判断する（ステップＳ１２３）。

[0085] ステップＳ１１９においてパケットから取り出したネットワーク識別データと、ステップＳ１２１において識別データ格納領域から読み出したネットワーク識別データとが一致しない場合（ステップＳ１２３：Ｎｏルート）、受信したパケットを廃棄し、ステップＳ１１１の処理に戻る。

[0086] 一方、ステップＳ１１９においてパケットから取り出したネットワーク識別データと、ステップＳ１２１において識別データ格納領域から読み出したネットワーク識別データとが一致する場合（ステップＳ１２３：Ｙｅｓルート）、処理は端子Ｂを介して図７のステップＳ１１に移行する。

[0087] 以上のような処理を実行すれば、セキュリティを高めつつ、保守員の利便性を向上させることができるようになる。

[0088] ［実施の形態３］

第３の実施の形態においては、同じネットワーク識別データを使い続けないようにすることでセキュリティを高める方法について説明する。

[0089] 図１６を用いて、第３の実施の形態におけるサーバ１が実行する処理について説明する。まず、検出部１０２は、保守用ネットワークポート１５３の状態を確認し（図１６：ステップＳ１３１）、保守用ネットワークポート１５３にＬＡＮケーブルが接続された（すなわち、リンクアップした）か判断する（ステップＳ１３３）。

[0090] 保守用ネットワークポート１５３にＬＡＮケーブルが接続されていない場合（ステップＳ１３３：Ｎｏルート）、ステップＳ１３１の処理に戻る。一方、保守用ネットワークポート１５３にＬＡＮケーブルが接続された場合（ステップＳ１３３：Ｙｅｓルート）、検出部１０２は、ＬＡＮケーブルを介して受信したパケットから、ネットワーク識別データを取り出す（ステップＳ１３５）。本実施の形態においては、ネットワーク識別データは仮想ＭＡＣアドレスであり、パケットにおける送信元ＭＡＣアドレスのフィールドに

格納される。

[0091] 検出部１０２は、ネットワーク識別データを取得することを要求する第１取得要求を制御コントローラ１０１に出力する。これに応じ、制御コントローラ１０１は、ネットワーク識別データをデータ格納部１０６における識別データ格納領域から読み出し（ステップＳ１３７）、検出部１０２に通知する。

[0092] 検出部１０２は、ステップＳ１３５においてパケットから取り出したネットワーク識別データと、ステップＳ１３７において識別データ格納領域から読み出したネットワーク識別データとが一致するか判断する（ステップＳ１３９）。

[0093] ステップＳ１３５においてパケットから取り出したネットワーク識別データと、ステップＳ１３７において識別データ格納領域から読み出したネットワーク識別データとが一致しない場合（ステップＳ１３９：Ｎｏルート）、受信したパケットを廃棄し、ステップＳ１３１の処理に戻る。

[0094] 一方、ステップＳ１３５においてパケットから取り出したネットワーク識別データと、ステップＳ１３７において識別データ格納領域から読み出したネットワーク識別データとが一致する場合（ステップＳ１３９：Ｙｅｓルート）、検出部１０２は、以下の処理を実行する。具体的には、検出部１０２は、ステップＳ１３５において取り出されたネットワーク識別データとは異なる新たなネットワーク識別データを含むパケットを、保守端末３から受信したか判断する（ステップＳ１４１）。

[0095] 新たなネットワーク識別データを含むパケットを保守端末３から受信していない場合（ステップＳ１４１：Ｎｏルート）、検出部１０２は所定時間待機し、ステップＳ１４１の処理に戻る。一方、新たなネットワーク識別データを含むパケットを保守端末３から受信した場合（ステップＳ１４１：Ｙｅｓルート）、検出部１０２は、新たなネットワーク識別データを制御コントローラ１０１に出力する。これに応じ、制御コントローラ１０１は、データ格納部１０６における識別データ格納領域に格納されているネットワーク識

別データを、新たなネットワーク識別データに変更する（ステップＳ１４３）。制御コントローラ１０１は、ネットワーク識別データの変更が完了したことを検出部１０２に通知する。

[0096] 検出部１０２は、ネットワーク識別データを変更したことを示す完了通知を、保守端末３に送信する（ステップＳ１４５）。そして処理は端子Ｂを介して図７のステップＳ１１に移行する。

[0097] 以上のような処理を実行すれば、ＬＡＮケーブルが接続される度にネットワーク識別データを変更できるので、同じネットワーク識別データを使い続けることを防止し、セキュリティを高めることができるようになる。

[0098] 図１７を用いて、第３の実施の形態における保守端末３が実行する処理について説明する。本処理は、ネットワーク識別データを含むパケットの初回の送信が行われた後に実行される。まず、保守端末３の通信部３０１は、ネットワーク識別データを含むパケットの初回の送信によってサーバ１との接続が確立されたか判断する（図１７：ステップＳ１５１）。

[0099] サーバ１との接続が確立されていない場合（ステップＳ１５１：Ｎｏルート）、通信部３０１は所定時間待機し、ステップＳ１５１の処理に戻る。一方、サーバ１との接続が確立された場合（ステップＳ１５１：Ｙｅｓルート）、通信部３０１は、ネットワーク識別データをランダムに生成する（ステップＳ１５３）。

[0100] 通信部３０１は、識別データ格納部３０３に格納されているネットワーク識別データを、ステップＳ１５３において生成したネットワーク識別データに変更する（ステップＳ１５５）。そして、通信部３０１は、ステップＳ１５３において生成したネットワーク識別データとネットワーク設定格納部３０２に格納されたネットワーク設定とを含むパケットを、サーバ１に送信する（ステップＳ１５７）。

[0101] 通信部３０１は、サーバ１から完了通知を受信したか判断する（ステップＳ１５９）。完了通知を受信していない場合（ステップＳ１５９：Ｎｏルート）、通信部３０１は所定時間待機し、ステップＳ１５９の処理に戻る。一

方、完了通知を受信した場合（ステップＳ１５９：Ｙｅｓルート）、処理は終了する。

[0102] 以上のようにすれば、特定困難な新たなネットワーク識別データをＬＡＮケーブルを介した接続の度に生成できるので、セキュリティを高めることができるようになる。なお、何らかの理由で保守端末３を変更する場合には、新しい保守端末３ネットワーク識別データを引き継ぐか、又は、サーバ１に登録されたネットワーク識別データを初回のネットワーク識別データに戻すことで、保守作業を継続できるようになる。

[0103] ［実施の形態４］

第４の実施の形態においては、切替コントローラ１０と管理コントローラ１１とを別々の装置に設ける例について説明する。

[0104] 図１８を用いて、本実施の形態のシステム概要について説明する。第４の実施の形態におけるサーバ１は、第１の実施の形態と同様に管理コントローラ１１を有するが、切替コントローラ１０を有しない。切替コントローラ１０は、切替装置７に設けられる。切替装置７は、切替コントローラ１０と、保守用ネットワークポート１５３と、管理ＬＡＮポート１５５及び１５７とを有する。

[0105] 切替コントローラ１０は、第１の実施の形態と同様、伝送路の切替を行うことができる。具体的には、接点１０３ａと接点１０３ｃとを接続することで、保守用ネットワークポート１５３と管理ＬＡＮコントローラ１１１とを伝送路でつなぐ。また、接点１０３ａと接点１０３ｂとを接続することで、管理ＬＡＮポート１５５と管理ＬＡＮコントローラ１１１とを伝送路でつなぐ。なお、第１の実施の形態と同様、切替コントローラ１０における制御コントローラ１０１と管理ＬＡＮコントローラ１１１との間には第２切替部１０４が設けられ、第２切替部１０４が制御コントローラ１０１と管理ＬＡＮコントローラ１１１との間の伝送路の生成及び切断を行う。但し、図を見やすくするため、図１８においては省略されている。

[0106] なお、サーバ１、保守端末３、及び切替コントローラ１０について上で述

べた点以外の点については第１の実施の形態と同じであるので、ここでは説明を省略する。

[0107] 次に、図１９及び図２０を用いて、第４の実施の形態における切替装置７が実行する処理について説明する。

[0108] まず、検出部１０２は、保守用ネットワークポート１５３の状態を確認し（図１９：ステップＳ１６１）、保守用ネットワークポート１５３にＬＡＮケーブルが接続された（すなわち、リンクアップした）か判断する（ステップＳ１６３）。

[0109] 保守用ネットワークポート１５３にＬＡＮケーブルが接続されていない場合（ステップＳ１６３：Ｎｏルート）、検出部１０２は所定時間待機し、ステップＳ１６１の処理に戻る。一方、保守用ネットワークポート１５３にＬＡＮケーブルが接続された場合（ステップＳ１６３：Ｙｅｓルート）、検出部１０２は、ＬＡＮケーブルを介して受信したパケットから、ネットワーク識別データを取り出す（ステップＳ１６５）。本実施の形態においては、ネットワーク識別データは仮想ＭＡＣアドレスであり、パケットにおける送信元ＭＡＣアドレスのフィールドに格納される。

[0110] 検出部１０２は、ネットワーク識別データを取得することを要求する第１取得要求を制御コントローラ１０１に出力する。これに応じ、制御コントローラ１０１は、ネットワーク識別データをデータ格納部１０６における識別データ格納領域から読み出し（ステップＳ１６７）、検出部１０２に通知する。

[0111] 検出部１０２は、ステップＳ１６５においてパケットから取り出したネットワーク識別データと、ステップＳ１６７において識別データ格納領域から読み出したネットワーク識別データとが一致するか判断する（ステップＳ１６９）。

[0112] ステップＳ１６５においてパケットから取り出したネットワーク識別データと、ステップＳ１６７において識別データ格納領域から読み出したネットワーク識別データとが一致しない場合（ステップＳ１６９：Ｎｏルート）、

受信したパケットを廃棄し、ステップＳ１６１の処理に戻る。

[0113] 一方、ステップＳ１６５においてパケットから取り出したネットワーク識別データと、ステップＳ１６７において識別データ格納領域から読み出したネットワーク識別データとが一致する場合（ステップＳ１６９：Ｙｅｓルート）、検出部１０２は、ネットワーク識別データが一致したことを制御コントローラ１０１に通知する。

[0114] 制御コントローラ１０１は、第１の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第１切替部１０３は、管理ＬＡＮコントローラ１１１と管理ＬＡＮポート１５５とをつなぐ伝送路を切断し、いずれの伝送路も切断された状態に切り替える。また、第２切替部１０４は、接点１０４ａと接点１０４ｃとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とを伝送路でつなぐ（ステップＳ１７１）。

[0115] 制御コントローラ１０１は、データ格納部１０６における管理ＬＡＮ設定格納領域に格納された管理ＬＡＮ設定に基づき、サーバ１の管理ＬＡＮコントローラ１１１との接続を確立する（ステップＳ１７３）。なお、管理ＬＡＮ設定は予めサーバ１から取得されているものとする。

[0116] 制御コントローラ１０１は、データ格納部１０６における保守用設定格納領域に格納された保守用設定をサーバ１に送信する（ステップＳ１７５）。処理は端子Ｃを介して図２０のステップＳ１７７の処理に移行する。なお、ステップＳ１７５の処理に応じ、サーバ１における管理ＬＡＮコントローラ１１１は、ネットワーク設定格納部１１４に格納されているネットワーク設定（ここでは、管理ＬＡＮ設定）を保守用設定に変更する。

[0117] 図２０の説明に移行し、制御コントローラ１０１は、第２の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第２切替部１０４は、接点１０４ａと接点１０４ｂとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とをつなぐ伝送路を切断する。また、第１切替部１０３は、接点１０３ａと接点１０３ｃとを接続すること

で、管理ＬＡＮコントローラ１１１と保守用ネットワークポート１５３とを伝送路でつなぐ（ステップＳ１７７）。

[0118] ここで、保守端末３は管理コントローラ１１にアクセスし、ログ管理部１１１０を介してログ格納部１１２からログを取得する。

[0119] 検出部１０２は、保守用ネットワークポート１５３の状態を確認し（ステップＳ１７９）、保守用ネットワークポート１５３にＬＡＮケーブルが接続されているか判断する（ステップＳ１８１）。

[0120] 保守用ネットワークポート１５３にＬＡＮケーブルが接続されている場合（ステップＳ１８１：Ｙｅｓルート）、ステップＳ１７９の処理に戻る。一方、保守用ネットワークポート１５３にＬＡＮケーブルが接続されていない場合（ステップＳ１８１：Ｎｏルート）、検出部１０２は、保守用ネットワークポート１５３にＬＡＮケーブルが接続されていないことを制御コントローラ１０１に通知する。

[0121] 制御コントローラ１０１は、第３の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第１切替部１０３は、管理ＬＡＮコントローラ１１１と保守用ネットワークポート１５３とをつなぐ伝送路を切断し、いずれの伝送路も切断された状態に切り替える。また、第２切替部１０４は、接点１０４ａと接点１０４ｃとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とを伝送路でつなぐ（ステップＳ１８３）。

[0122] 制御コントローラ１０１は、データ格納部１０６における保守用設定格納領域に格納された保守用設定に基づき、サーバ１の管理ＬＡＮコントローラ１１１との接続を確立する（ステップＳ１８５）。

[0123] 制御コントローラ１０１は、データ格納部１０６における管理ＬＡＮ設定格納領域に格納された管理ＬＡＮ設定をサーバ１に送信する（ステップＳ１８７）。なお、ステップＳ１８７の処理に応じ、サーバ１における管理ＬＡＮコントローラ１１１は、ネットワーク設定格納部１１４に格納されているネットワーク設定（ここでは、保守用設定）を管理ＬＡＮ設定に変更する。

[0124] 制御コントローラ１０１は、第４の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第２切替部１０４は、接点１０４ａと接点１０４ｂとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とをつなぐ伝送路を切断する。また、第１切替部１０３は、接点１０３ａと接点１０３ｂとを接続することで、管理ＬＡＮコントローラ１１１と管理ＬＡＮポート１５５とを伝送路でつなぐ（ステップＳ１８９）。そして処理を終了する。

[0125] 以上のように、切替コントローラ１０と管理コントローラ１１とを別々の装置に設けるようなシステム構成を実現可能にすることで、サーバの配置状況や処理性能などの実情に合ったシステムを柔軟に構築することができるようになる。

[0126] ［実施の形態５］

第５の実施の形態においては、退避させるネットワーク設定に、ＩＰアドレス及びサブネットマスクだけでなくＭＡＣアドレスを含ませる例について説明する。

[0127] 図２１を用いて、第５の実施の形態の概要について説明する。

[0128] まず、サーバ１の保守用ネットワークポート１５３に接続された保守端末３が、ネットワーク識別データ（００－００－５Ｅ－００－０１－０１）とネットワーク設定（１９２．１６８．１．１０／２５５．２５５．２５５．０）とを含むパケットをサーバ１に送信する。本実施の形態においては、初回にはＡＲＰ（Address Resolution Protocol）パケットを送信（ここではブロードキャスト）するものとし、ＡＲＰパケットにネットワーク識別データとネットワーク設定とを含ませる。

[0129] サーバ１における切替コントローラ１０は、ＡＲＰパケットに含まれるネットワーク識別データと、切替コントローラ１０に予め登録されたネットワーク識別データ（００－００－５Ｅ－００－０１－０１）とが一致する場合、保守用ネットワークポート１５３と管理コントローラ１１とを伝送路でつなげる。

[0130] 但し、切替コントローラ１０は、保守端末３のアクセスが開始される前に、管理コントローラ１１のネットワーク設定格納部１１４に格納されたネットワーク設定（１９２．１６８．２．１０／２５５．２５５．２５５．０／００－００－５Ｅ－００－０１－０２）を、保守端末３がアクセスできない領域に退避しておく。また、切替コントローラ１０は、管理コントローラ１１のネットワーク設定格納部１１４に格納されているネットワーク設定を、管理ＬＡＮ設定（１９２．１６８．２．１０／２５５．２５５．２５５．０／００－００－５Ｅ－００－０１－０２）から保守用設定（１９２．１６８．１．１０／２５５．２５５．２５５．０／１１－２２－３３－４４－５５－６６）に変更しておく。保守用設定は、ＩＰアドレス及びサブネットマスクと、切替コントローラ１０がランダムに生成したＭＡＣアドレスとを含む。

[0131] そして、サーバ１は、ＡＲＰ要求を生成したＭＡＣアドレスを含むＡＲＰ応答を保守端末３に送信する。これに応じ、保守端末３は、ＡＲＰ応答に含まれるＭＡＣアドレスを宛先ＭＡＣアドレスに設定してパケットを送信するようにする。すると、管理コントローラ１１のネットワーク設定格納部１１４に格納されたネットワーク設定（１９２．１６８．１．１０／２５５．２５５．２５５．０／１１－２２－３３－４４－５５－６６）と、保守端末３が送信したパケットに含まれるネットワーク設定（１９２．１６８．１．１０／２５５．２５５．２５５．０／１１－２２－３３－４４－５５－６６）とが一致するようになる。これにより、保守端末３は、ログ格納部１１２に格納されたログを管理コントローラ１１から取得できるようになる。また、保守端末３の接続が終了した場合には、退避されたネットワーク設定を、管理コントローラ１１のネットワーク設定格納部１１４に再び格納することで、通常の運用を再開できるようになる。

[0132] 次に、図２２乃至図２４を用いて、第５の実施の形態におけるサーバ１が実行する処理について説明する。

[0133] まず、検出部１０２は、保守用ネットワークポート１５３の状態を確認し

（図２２：ステップＳ１９１）、保守用ネットワークポート１５３にＬＡＮケーブルが接続された（すなわち、リンクアップした）か判断する（ステップＳ１９３）。

[0134] 保守用ネットワークポート１５３にＬＡＮケーブルが接続されていない場合（ステップＳ１９３：Ｎｏルート）、検出部１０２は所定時間待機し、ステップＳ１９１の処理に戻る。一方、保守用ネットワークポート１５３にＬＡＮケーブルが接続された場合（ステップＳ１９３：Ｙｅｓルート）、検出部１０２は、ＬＡＮケーブルを介して受信したＡＲＰパケットから、ネットワーク識別データを取り出す（ステップＳ１９５）。本実施の形態においては、ネットワーク識別データは仮想ＭＡＣアドレスであり、ＡＲＰパケットにおける送信元ＭＡＣアドレスのフィールドに格納される。

[0135] 検出部１０２は、ネットワーク識別データを取得することを要求する第１取得要求を制御コントローラ１０１に出力する。これに応じ、制御コントローラ１０１は、ネットワーク識別データをデータ格納部１０６における識別データ格納領域から読み出し（ステップＳ１９７）、検出部１０２に通知する。

[0136] 検出部１０２は、ステップＳ１９５においてＡＲＰパケットから取り出したネットワーク識別データと、ステップＳ１９７において識別データ格納領域から読み出したネットワーク識別データとが一致するか判断する（ステップＳ１９９）。

[0137] ステップＳ１９５においてＡＲＰパケットから取り出したネットワーク識別データと、ステップＳ１９７において識別データ格納領域から読み出したネットワーク識別データとが一致しない場合（ステップＳ１９９：Ｎｏルート）、受信したＡＲＰパケットを廃棄し、ステップＳ１９１の処理に戻る。

[0138] 一方、ステップＳ１９５においてＡＲＰパケットから取り出したネットワーク識別データと、ステップＳ１９７において識別データ格納領域から読み出したネットワーク識別データとが一致する場合（ステップＳ１９９：Ｙｅｓルート）、検出部１０２は、ネットワーク識別データが一致したことを制

御コントローラ１０１に通知する。

[0139] 制御コントローラ１０１は、第１の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第１切替部１０３は、管理ＬＡＮコントローラ１１１と管理ＬＡＮポート１５２とをつなぐ伝送路を切断し、いずれの伝送路も切断された状態に切り替える。また、第２切替部１０４は、接点１０４ａと接点１０４ｃとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とを伝送路でつなぐ（ステップＳ２０１）。

[0140] 制御コントローラ１０１は、退避処理を実行する（ステップＳ２０３）。退避処理については図８を用いて説明したとおりであるので、ここでは説明を省略する。但し、第５の実施の形態においては、ステップＳ３５において読み出される管理ＬＡＮ設定にＭＡＣアドレスが含まれる。従って、ステップＳ４１において格納される管理ＬＡＮ設定にもＭＡＣアドレスが含まれる。

[0141] 制御コントローラ１０１は、第５の実施の形態における設定切替処理を実行する（ステップＳ２０５）。設定切替処理については、図２３を用いて説明する。

[0142] まず、切替コントローラ１０における制御コントローラ１０１は、ＭＡＣアドレスをランダムに生成し、データ格納部１０６における保守用設定格納領域に格納する（図２３：ステップＳ２３１）。なお、既に保守用設定格納領域にＭＡＣアドレスが格納されている場合には、既に格納されているＭＡＣアドレスを上書きする。

[0143] 制御コントローラ１０１は、データ格納部１０６における保守用設定格納領域に格納された保守用設定を読み出す（ステップＳ２３３）。読み出される保守用設定は、ＩＰアドレス、サブネットマスク、及びステップＳ２３１において生成したＭＡＣアドレスを含む。

[0144] そして、制御コントローラ１０１は、ステップＳ２３３において読み出した保守用設定を、管理ＬＡＮコントローラ１１１に送信する（ステップＳ２

３５）。ここでは、制御コントローラ１０１と管理ＬＡＮコントローラ１１１とをつなぐ伝送路を介して保守用設定が送信される。

[0145] 管理コントローラ１１における管理ＬＡＮコントローラ１１１は、制御コントローラ１０１から保守用設定を受信する（ステップＳ２３７）。そして、管理ＬＡＮコントローラ１１１は、ネットワーク設定格納部１１４に格納されているネットワーク設定（ここでは、管理ＬＡＮ設定）を、ステップＳ２３７において受信した保守用設定に変更する（ステップＳ２３９）。そして呼び出し元の処理に戻り、処理は端子Ｄを介して図２４のステップＳ２０７の処理に移行する。

[0146] 以上のような処理を実行すれば、保守端末３が管理コントローラ１１にアクセスすることが許可されるようになる。

[0147] 図２４の説明に移行し、制御コントローラ１０１は、第２の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第２切替部１０４は、接点１０４ａと接点１０４ｂとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とをつなぐ伝送路を切断する。また、第１切替部１０３は、接点１０３ａと接点１０３ｃとを接続することで、管理ＬＡＮコントローラ１１１と保守用ネットワークポート１５３とを伝送路でつなぐ（ステップＳ２０７）。

[0148] 制御コントローラ１０１は、ＡＲＰ要求を管理ＬＡＮコントローラ１１１に送信する（ステップＳ２０９）。これに応じ、管理ＬＡＮコントローラ１１１は、ネットワーク設定格納部１１４に格納されているＭＡＣアドレスを含むＡＲＰ応答を、制御コントローラ１０１に送信する。そして、制御コントローラ１０１は、管理ＬＡＮコントローラ１１１から受信したＡＲＰ応答を、保守端末３に送信する（ステップＳ２１１）。

[0149] これに応じ、保守端末３は、サーバ１に送信するパケットの宛先アドレスとして、ＡＲＰ応答に含まれるＭＡＣアドレスを使用するようにする。

[0150] そして、保守端末３は管理コントローラ１１にアクセスし、ログ管理部１１１０を介してログ格納部１１２からログを取得する。

[0151] 検出部１０２は、保守用ネットワークポート１５３の状態を確認し（ステップＳ２１３）、保守用ネットワークポート１５３にＬＡＮケーブルが接続されているか判断する（ステップＳ２１５）。

[0152] 保守用ネットワークポート１５３にＬＡＮケーブルが接続されている場合（ステップＳ２１５：Ｙｅｓルート）、ステップＳ２１３の処理に戻る。一方、保守用ネットワークポート１５３にＬＡＮケーブルが接続されていない場合（ステップＳ２１５：Ｎｏルート）、検出部１０２は、保守用ネットワークポート１５３にＬＡＮケーブルが接続されていないことを制御コントローラ１０１に通知する。

[0153] 制御コントローラ１０１は、第３の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第１切替部１０３は、管理ＬＡＮコントローラ１１１と保守用ネットワークポート１５３とをつなぐ伝送路を切断し、いずれの伝送路も切断された状態に切り替える。また、第２切替部１０４は、接点１０４ａと接点１０４ｃとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とを伝送路でつなぐ（ステップＳ２１７）。

[0154] 制御コントローラ１０１は、ネットワーク設定格納部１１４に格納されたネットワーク設定（ここでは、保守用設定）を、データ格納部１０６における管理ＬＡＮ設定格納領域に退避した管理ＬＡＮ設定に変更する（ステップＳ２１９）。具体的には、制御コントローラ１０１は、データ格納部１０６における管理ＬＡＮ設定格納領域に退避した管理ＬＡＮ設定を管理コントローラ１１に送信する。管理コントローラ１１における管理ＬＡＮコントローラ１１１は、ネットワーク設定格納部１１４に格納されているネットワーク設定を、受信した管理ＬＡＮ設定に変更する。なお、ステップＳ２１９においては、制御コントローラ１０１と管理ＬＡＮコントローラ１１１とをつなぐ伝送路を介して管理ＬＡＮ設定が送信される。

[0155] 制御コントローラ１０１は、第４の切替指示を第１切替部１０３及び第２切替部１０４に出力する。これに応じ、第２切替部１０４は、接点１０４ａ

と接点１０４ｂとを接続することで、管理ＬＡＮコントローラ１１１と制御コントローラ１０１とをつなぐ伝送路を切断する。また、第１切替部１０３は、接点１０３ａと接点１０３ｂとを接続することで、管理ＬＡＮコントローラ１１１と管理ＬＡＮポート１５２とを伝送路でつなぐ（ステップＳ２２１）。そして処理を終了する。

[0156] 以上のような処理を実行すれば、ＩＰアドレス及びサブネットマスクだけでなくＭＡＣアドレスをも退避の対象となるので、秘匿性をより高めることができるようになる。

[0157] ［実施の形態６］

第１乃至第５の実施の形態においてはＴＣＰ／ＩＰプロトコルを利用しているが、ファイバーチャネル或いはインフィニバンドを利用してもよい。この場合、ＩＰアドレス、サブネットマスク、及びＭＡＣアドレスの代わりに、動的ポートのアドレス、ＧＵＩＤ（Globally Unique IDentifier）、及びＷＷＮ（World Wide Name）を使用すればよい。

[0158] 以上本発明の一実施の形態を説明したが、本発明はこれに限定されるものではない。例えば、上で説明したサーバ１及び保守端末３の機能ブロック構成は実際のプログラムモジュール構成に一致しない場合もある。

[0159] また、上で説明したデータ保持構成は一例であって、上記のような構成でなければならないわけではない。さらに、処理フローにおいても、処理結果が変わらなければ処理の順番を入れ替えることも可能である。さらに、並列に実行させるようにしても良い。

[0160] なお、上で述べた保守端末３は、コンピュータ装置であって、図２５に示すように、メモリ２５０１とＣＰＵ（Central Processing Unit）２５０３とハードディスク・ドライブ（ＨＤＤ：Hard Disk Drive）２５０５と表示装置２５０９に接続される表示制御部２５０７とリムーバブル・ディスク２５１１用のドライブ装置２５１３と入力装置２５１５とネットワークに接続するための通信制御部２５１７とがバス２５１９で接続されている。オペレーティング・システム（ＯＳ：Operating System）及び本実施例における処理を

実施するためのアプリケーション・プログラムは、ＨＤＤ２５０５に格納されており、ＣＰＵ２５０３により実行される際にはＨＤＤ２５０５からメモリ２５０１に読み出される。ＣＰＵ２５０３は、アプリケーション・プログラムの処理内容に応じて表示制御部２５０７、通信制御部２５１７、ドライブ装置２５１３を制御して、所定の動作を行わせる。また、処理途中のデータについては、主としてメモリ２５０１に格納されるが、ＨＤＤ２５０５に格納されるようにしてもよい。本発明の実施例では、上で述べた処理を実施するためのアプリケーション・プログラムはコンピュータ読み取り可能なリムーバブル・ディスク２５１１に格納されて頒布され、ドライブ装置２５１３からＨＤＤ２５０５にインストールされる。インターネットなどのネットワーク及び通信制御部２５１７を経由して、ＨＤＤ２５０５にインストールされる場合もある。このようなコンピュータ装置は、上で述べたＣＰＵ２５０３、メモリ２５０１などのハードウエアとＯＳ及びアプリケーション・プログラムなどのプログラムとが有機的に協働することにより、上で述べたような各種機能を実現する。

[0161] 以上述べた本発明の実施の形態をまとめると、以下のようになる。

[0162] 本実施の形態の第１の態様に係る情報処理装置は、（Ａ）第１のネットワークポートに第１の装置が接続されたことを検出する検出部と、（Ｂ）第１のネットワークポートに第１の装置が接続されたことが検出部により検出された場合、情報処理装置のネットワーク設定を、第１のネットワークポート用のネットワーク設定に変更する制御部と、（Ｃ）第１のネットワークポートに第１の装置が接続されたことが検出部により検出された場合、第１の装置が第１のネットワークポートを介した通信を行えるように情報処理装置内の伝送路の切替を行う切替部とを有する。

[0163] このようにすれば、第１のネットワークポート用のネットワーク設定を使用して第１の装置との通信を行えるので、元のネットワーク設定の取得に制限がある場合であっても作業者が保守作業を行えるようになる。

[0164] また、上で述べた制御部は、（ｂ１）変更前のネットワーク設定を、第１

の装置がアクセスできない記憶領域に移動してもよい。このようにすれば、変更前のネットワーク設定の秘匿性を高めることができるようになる。

[0165] また、上で述べた検出部は、（ａ１）第１のネットワークポートに第１の装置が接続されていないことを検出し、上で述べた制御部は、（ｂ２）第１のネットワークポートに第１の装置が接続されていないことが検出部により検出された場合、情報処理装置のネットワーク設定を、第１のネットワークポート用のネットワーク設定から、元のネットワーク設定である第２のネットワーク設定に変更し、（ｃ１）上で述べた切替部は、第１のネットワークポートに第１の装置が接続されていないことが検出部により検出された場合、元のネットワークポートである第２のネットワークポートを介した通信を行えるように情報処理装置内の伝送路の切替を行ってもよい。このようにすれば、保守作業が終了した場合には元の状態に戻すことができるようになる。

[0166] また、本情報処理装置は、（Ｄ）上で述べた第１の識別データを格納するデータ格納部をさらに有してもよい。そして、上で述べた検出部は、（ａ２）第１の装置から受信した第２の識別データと、データ格納部に格納された第１の識別データとが一致する場合、第１の装置が第１のネットワークポートに接続されたと判定してもよい。このようにすれば、情報処理装置に接続する資格が無い装置が情報処理装置に接続することを防止できるようになる。

[0167] また、上で述べた検出部は、（ａ３）第１の装置が第１のネットワークポートに接続された後、第２の識別データとは異なる第３の識別データを第１の装置から受信した場合、データ格納部に格納された第１の識別データを第３の識別データで更新してもよい。このようにすれば、同じ識別データを使い続けなくてよいので、セキュリティを向上させることができるようになる。

[0168] また、本情報処理装置は、（Ｅ）外部のハードウエアから取得した情報に基づき認証を行う認証部をさらに有してもよい。そして、上で述べた制御部

は、（ｂ３）第１のネットワークポートに第１の装置が接続されたことが検出部により検出され且つ認証部による認証の結果が所定の条件を満たす場合、情報処理装置のネットワーク設定を、第１のネットワークポート用のネットワーク設定に変更し、上で述べた切替部は、（ｃ２）第１のネットワークポートに第１の装置が接続されたことが検出部により検出され且つ認証部による認証の結果が所定の条件を満たす場合、第１の装置が第１のネットワークポートを介した通信を行えるように情報処理装置内の伝送路の切替を行ってもよい。このようにすれば、セキュリティを向上させることができるようになる。

[0169] また、上で述べたネットワーク設定は、ＩＰ（Internet Protocol）アドレス、サブネットマスク、及びＭＡＣ（Media Access Control）アドレスの少なくともいずれかを含んでもよい。

[0170] また、上で述べたネットワーク設定は、ＷＷＮ（World Wide Name）、動的ポートのアドレス、及びＧＵＩＤ（Globally Unique Identifier）の少なくともいずれかを含んでもよい。

[0171] 本実施の形態の第２の態様に係る保守システムは、（Ｆ）情報処理装置と、（Ｇ）第１の装置とを有してもよい。そして、上で述べた情報処理装置は、（ｆ１）情報処理装置の第１のネットワークポートに第１の装置が接続されたことを検出する検出部と、（ｆ２）第１のネットワークポートに第１の装置が接続されたことが検出部により検出された場合、情報処理装置のネットワーク設定を、第１のネットワークポート用のネットワーク設定に変更する制御部と、（ｆ３）第１のネットワークポートに第１の装置が接続されたことが検出部により検出された場合、第１の装置が第１のネットワークポートを介した通信を行えるように前記情報処理装置内の伝送路の切替を行う切替部とを有する。そして、上で述べた第１の装置は、（ｇ１）第１のネットワークポート用のネットワーク設定に基づき情報処理装置との通信を行う通信部を有する。

請求の範囲

[請求項1] 情報処理装置であって、

第１のネットワークポートに第１の装置が接続されたことを検出する検出部と、

前記第１のネットワークポートに前記第１の装置が接続されたことが前記検出部により検出された場合、前記情報処理装置のネットワーク設定を、前記第１のネットワークポート用のネットワーク設定に変更する制御部と、

前記第１のネットワークポートに前記第１の装置が接続されたことが前記検出部により検出された場合、前記第１の装置が前記第１のネットワークポートを介した通信を行えるように前記情報処理装置内の伝送路の切替を行う切替部と、

を有する情報処理装置。

[請求項2] 前記制御部は、

変更前の前記ネットワーク設定を、前記第１の装置がアクセスできない記憶領域に移動する、

請求項１記載の情報処理装置。

[請求項3] 前記検出部は、

前記第１のネットワークポートに前記第１の装置が接続されていないことを検出し、

前記制御部は、

前記第１のネットワークポートに前記第１の装置が接続されていないことが前記検出部により検出された場合、前記情報処理装置のネットワーク設定を、前記第１のネットワークポート用のネットワーク設定から、元のネットワーク設定である第２のネットワーク設定に変更し、

前記切替部は、

前記第１のネットワークポートに前記第１の装置が接続されていな

いことが前記検出部により検出された場合、元のネットワークポートである第２のネットワークポートを介した通信を行えるように前記情報処理装置内の伝送路の切替を行う、

請求項１又は２記載の情報処理装置。

[請求項4] 第１の識別データを格納するデータ格納部

をさらに有し、

前記検出部は、

前記第１の装置から受信した第２の識別データと、前記データ格納部に格納された第１の識別データとが一致する場合、前記第１の装置が前記第１のネットワークポートに接続されたと判定する、

請求項１乃至３のいずれか１つ記載の情報処理装置。

[請求項5] 前記検出部は、

前記第１の装置が前記第１のネットワークポートに接続された後、前記第２の識別データとは異なる第３の識別データを前記第１の装置から受信した場合、前記データ格納部に格納された前記第１の識別データを前記第３の識別データで更新する、

請求項４記載の情報処理装置。

[請求項6] 外部のハードウエアから取得した情報に基づき認証を行う認証部

をさらに有し、

前記制御部は、

前記第１のネットワークポートに前記第１の装置が接続されたことが前記検出部により検出され且つ前記認証部による認証の結果が所定の条件を満たす場合、前記情報処理装置のネットワーク設定を、前記第１のネットワークポート用のネットワーク設定に変更し、

前記切替部は、

前記第１のネットワークポートに前記第１の装置が接続されたことが前記検出部により検出され且つ前記認証部による認証の結果が前記所定の条件を満たす場合、前記第１の装置が前記第１のネットワーク

ポートを介した通信を行えるように前記情報処理装置内の伝送路の切替を行う、

請求項１乃至５のいずれか１つ記載の情報処理装置。

[請求項7] 前記ネットワーク設定は、ＩＰ（Internet Protocol）アドレス、サブネットマスク、及びＭＡＣ（Media Access Control）アドレスの少なくともいずれかを含む

請求項１乃至６のいずれか１つ記載の情報処理装置。

[請求項8] 前記ネットワーク設定は、ＷＷＮ（World Wide Name）、動的ポートのアドレス、及びＧＵＩＤ（Globally Unique Identifier）の少なくともいずれかを含む

請求項１乃至６記載の情報処理装置。

[請求項9] 第１のネットワークポートに第１の装置が接続されたことを検出する検出部と、

前記第１のネットワークポートに前記第１の装置が接続されたことが前記検出部により検出された場合、情報処理装置のネットワーク設定を、前記第１のネットワークポート用のネットワーク設定に変更する制御部と、

前記第１のネットワークポートに前記第１の装置が接続されたことが前記検出部により検出された場合、前記第１の装置が前記第１のネットワークポートを介した通信を行えるように前記情報処理装置内の伝送路の切替を行う切替部と、

を有するネットワークインタフェースカード。

[請求項10] 情報処理装置と、

第１の装置と、

を有し、

前記情報処理装置は、

前記情報処理装置の第１のネットワークポートに前記第１の装置が接続されたことを検出する検出部と、

前記第１のネットワークポートに前記第１の装置が接続されたことが前記検出部により検出された場合、情報処理装置のネットワーク設定を、前記第１のネットワークポート用のネットワーク設定に変更する制御部と、

前記第１のネットワークポートに前記第１の装置が接続されたことが前記検出部により検出された場合、前記第１の装置が前記第１のネットワークポートを介した通信を行えるように前記情報処理装置内の伝送路の切替を行う切替部と、

を有し、

前記第１の装置は、

前記第１のネットワークポート用のネットワーク設定に基づき前記情報処理装置との通信を行う通信部

を有する、保守システム。

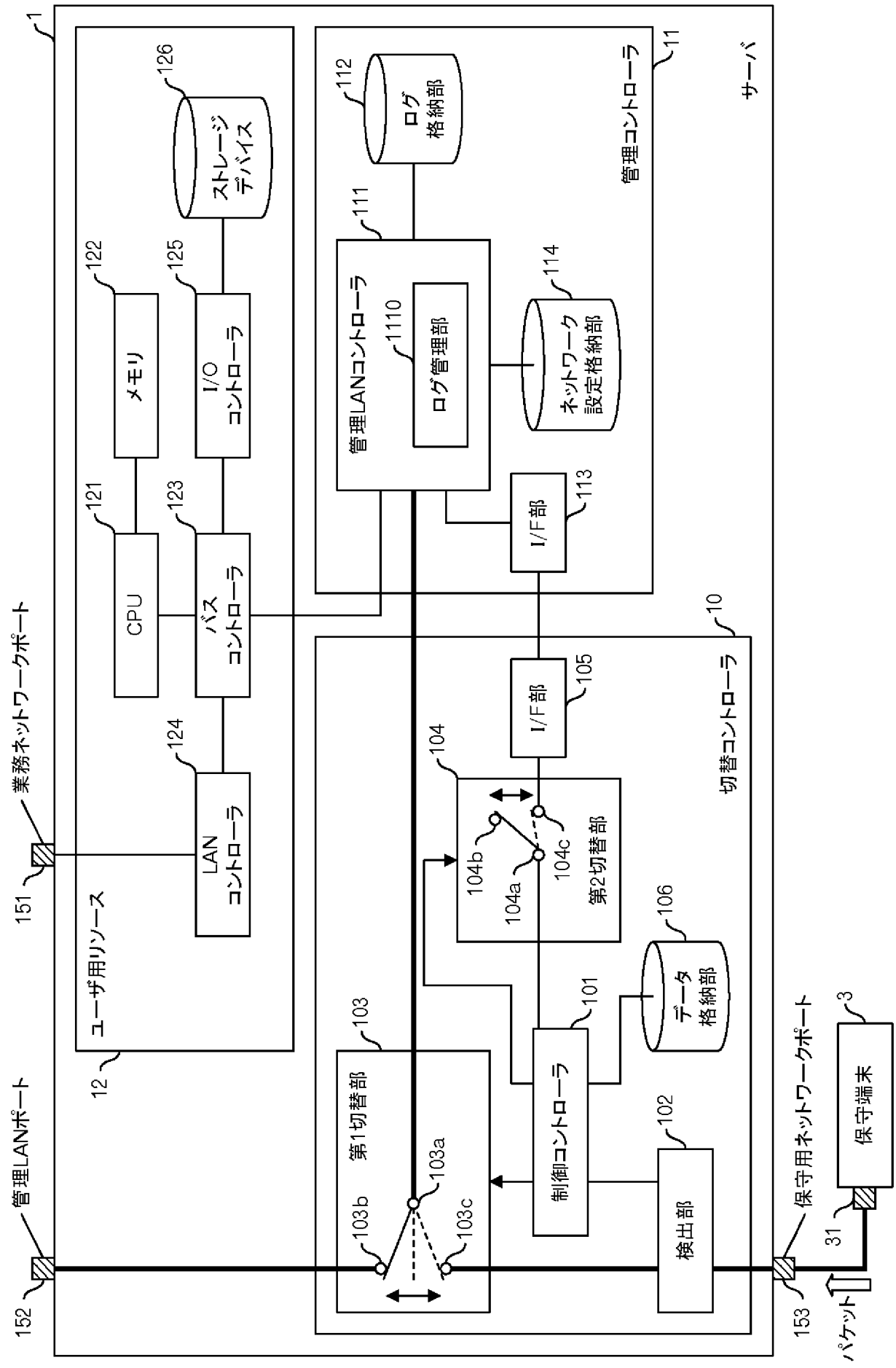
[図1]

	IPアドレス	サブネットマスク
サーバ	192.168.1.10	255.255.255.0
端末	128.10.20.30 ⇒192.168.1.11	255.255.0.0 ⇒255.255.255.0

[図2]

	IPアドレス	サブネットマスク
サーバ	192.168.1.10 ⇒128.10.20.31	255.255.255.0 ⇒255.255.0.0
端末	128.10.20.30	255.255.0.0

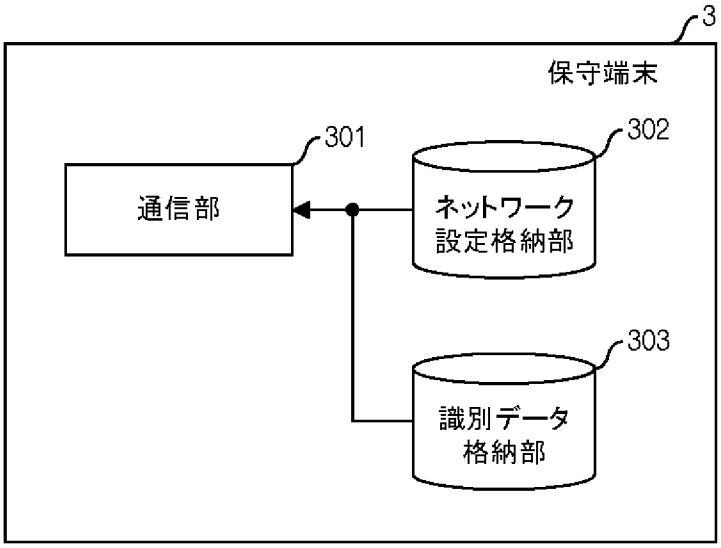
[図3]


1
サーバ
管理コントローラ
11
ユーザ用リソース
12
切替コントローラ
10
ストレージデバイス
126
メモリ
122
CPU
121
I/Oコントローラ
125
バスコントローラ
123
LANコントローラ
124
ログ格納部
112
管理LANコントローラ
111
ログ管理部
1110
ネットワーク設定格納部
114
I/F部
113
I/F部
105
第2切替部
104
104a
104b
104c
データ格納部
106
制御コントローラ
101
第1切替部
103
103a
103b
103c
検出部
102
業務ネットワークポート
151
管理LANポート
152
保守用ネットワークポート
153
保守端末
3
31
パケット

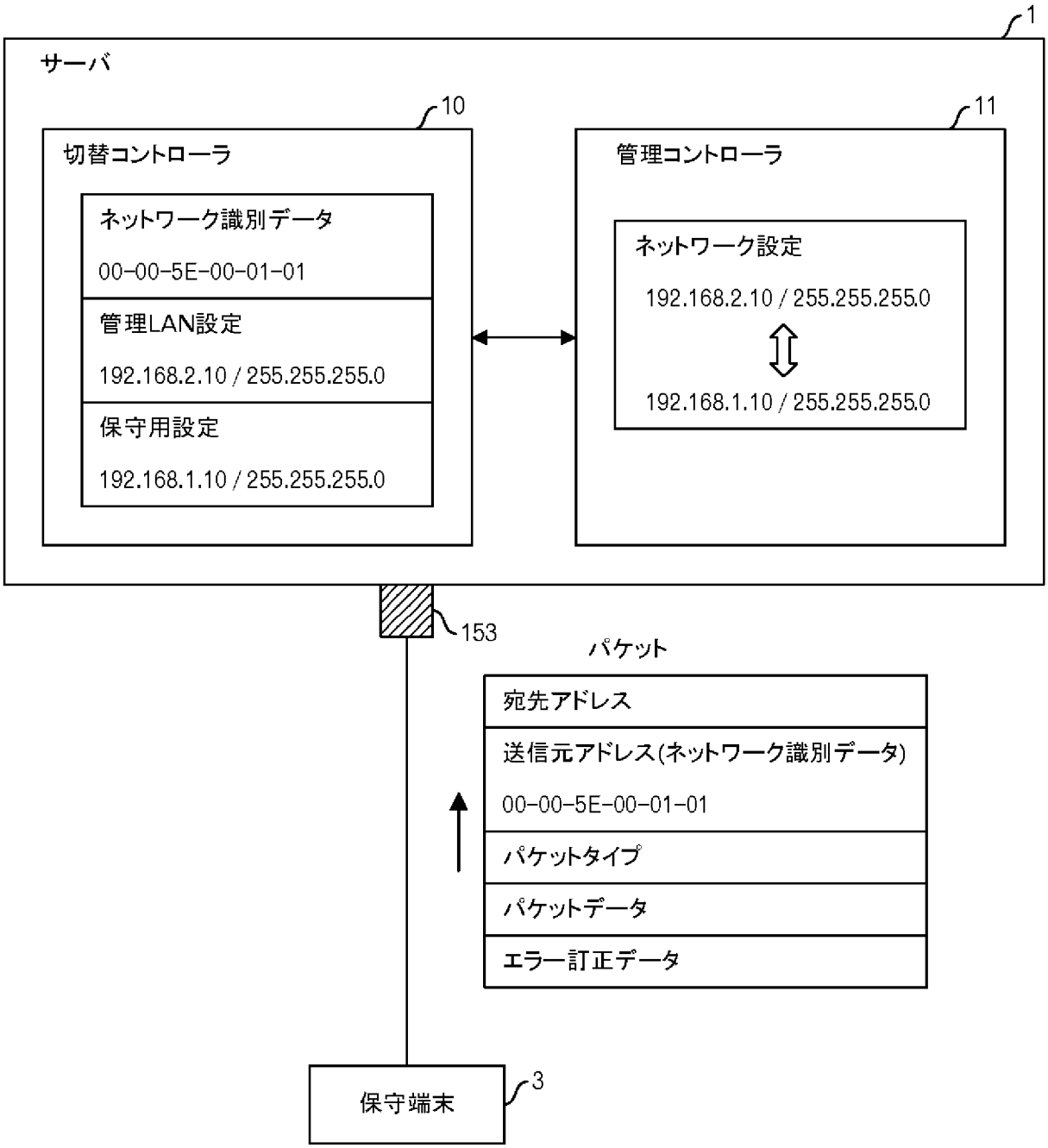
[図4]

識別データ格納領域 00-00-5E-00-01-01
管理LAN設定格納領域 192.168.2.10 / 255.255.255.0
保守用設定格納領域 192.168.1.10 / 255.255.255.0

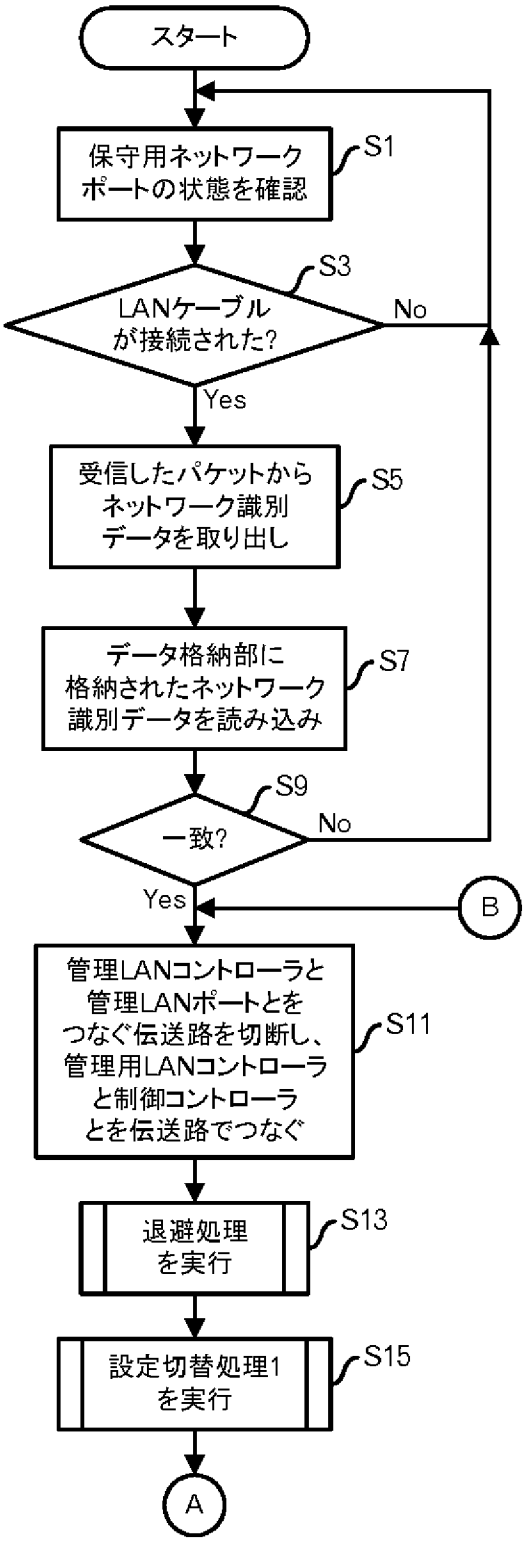
[図5]



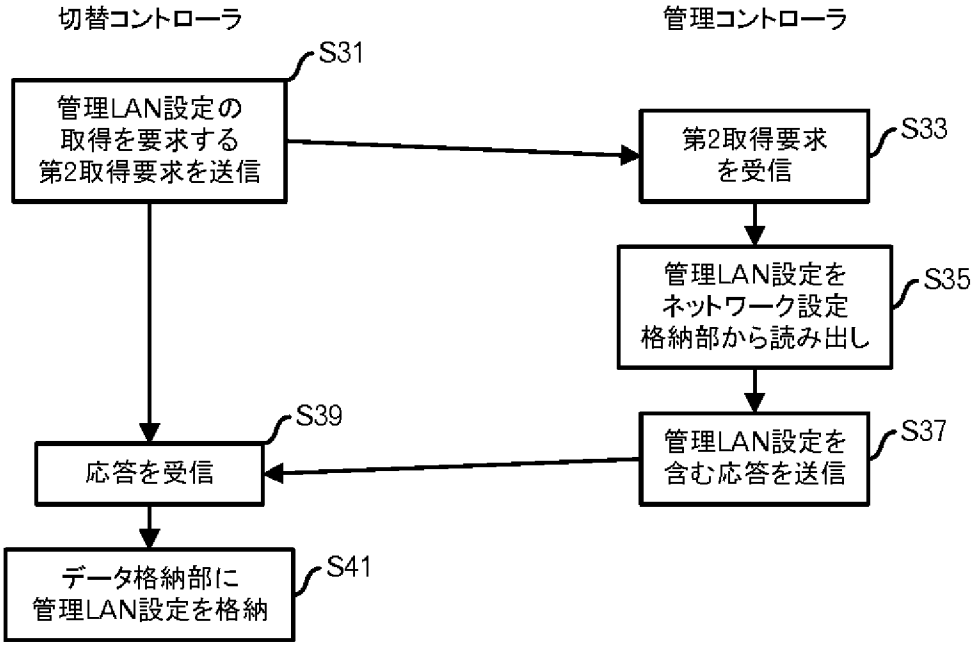
[図6]


1
サーバ
10
切替コントローラ
ネットワーク識別データ
00-00-5E-00-01-01
管理LAN設定
192.168.2.10 / 255.255.255.0
保守用設定
192.168.1.10 / 255.255.255.0
11
管理コントローラ
ネットワーク設定
192.168.2.10 / 255.255.255.0
192.168.1.10 / 255.255.255.0
153
パケット
宛先アドレス
送信元アドレス(ネットワーク識別データ)
00-00-5E-00-01-01
パケットタイプ
パケットデータ
エラー訂正データ
保守端末
3

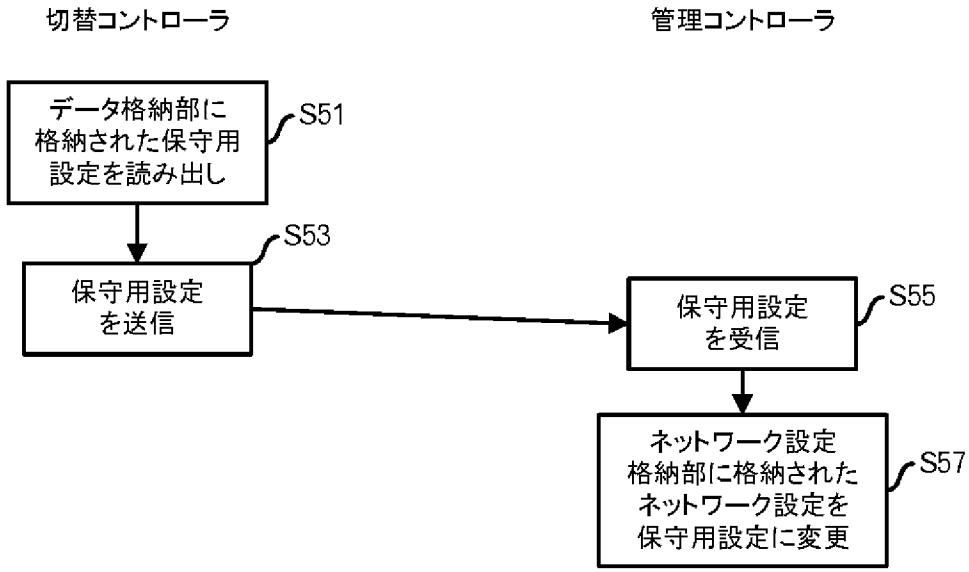
[図7]


スタート
保守用ネットワーク
ポートの状態を確認
S1
S3
LANケーブル
が接続された?
No
Yes
受信したパケットから
ネットワーク識別
データを取り出し
S5
データ格納部に
格納されたネットワーク
識別データを読み込み
S7
S9
一致?
No
Yes
B
管理LANコントローラと
管理LANポートとを
つなぐ伝送路を切断し、
管理用LANコントローラ
と制御コントローラ
とを伝送路でつなぐ
S11
退避処理
を実行
S13
設定切替処理1
を実行
S15
A

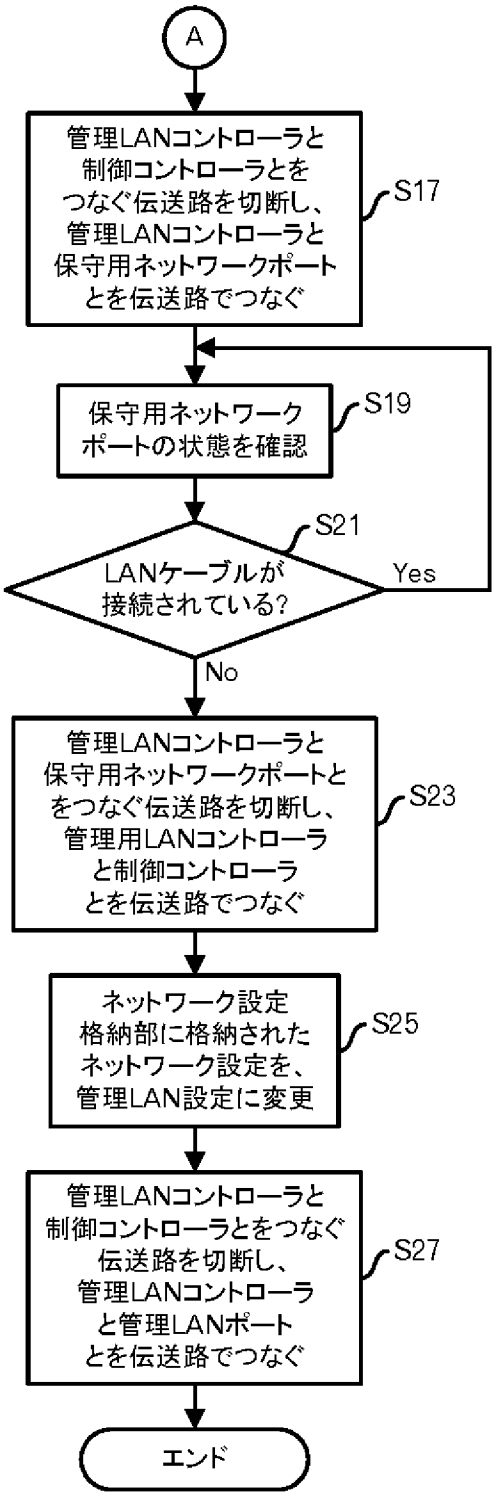
[図8]


切替コントローラ
管理コントローラ
S31
管理LAN設定の
取得を要求する
第2取得要求を送信
第2取得要求
を受信
S33
管理LAN設定を
ネットワーク設定
格納部から読み出し
S35
S39
応答を受信
管理LAN設定を
含む応答を送信
S37
データ格納部に
管理LAN設定を格納
S41

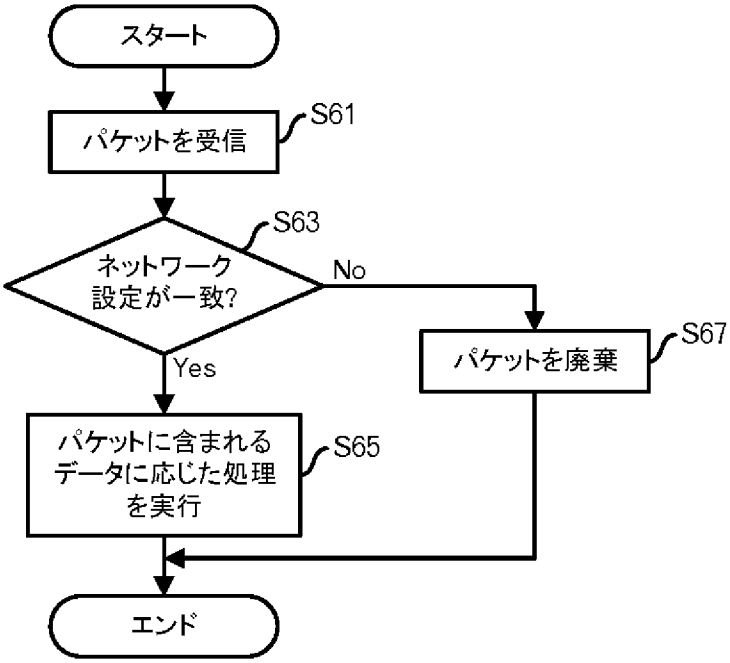
[図9]


切替コントローラ
管理コントローラ
データ格納部に
格納された保守用
設定を読み出し
S51
S53
保守用設定
を送信
保守用設定
を受信
S55
ネットワーク設定
格納部に格納された
ネットワーク設定を
保守用設定に変更
S57

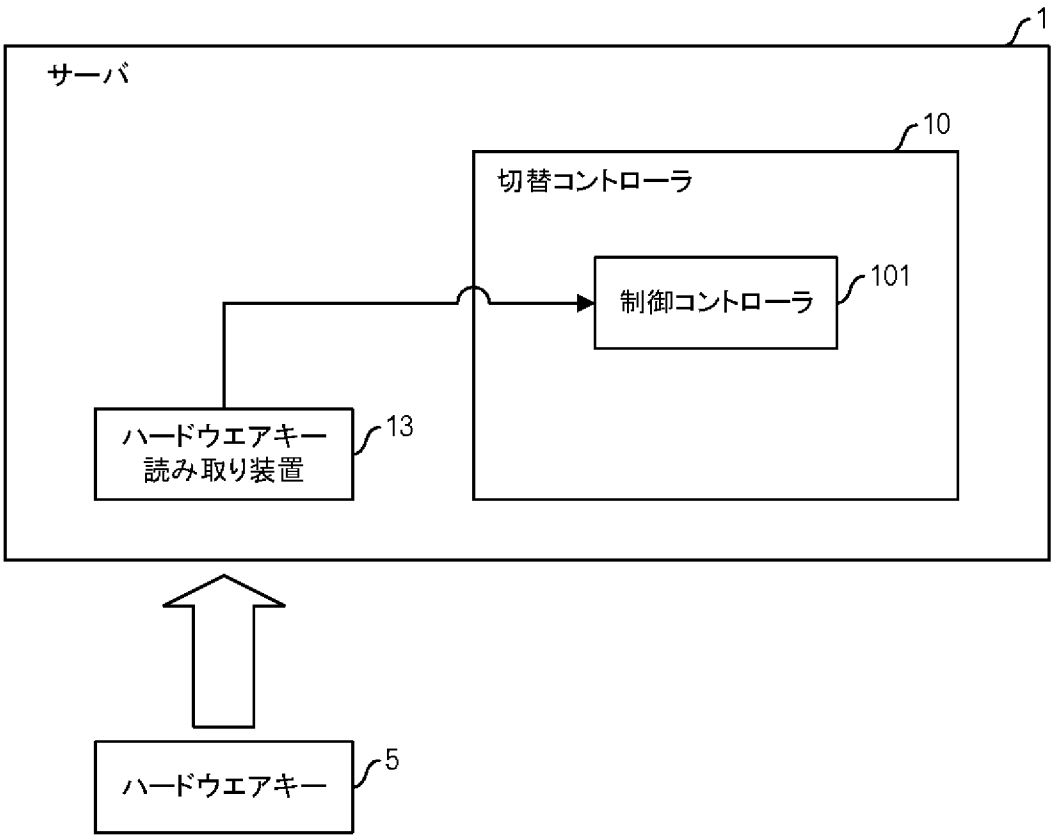
[図10]


A
管理LANコントローラと制御コントローラとをつなぐ伝送路を切断し、管理LANコントローラと保守用ネットワークポートとを伝送路でつなぐ
S17
保守用ネットワークポートの状態を確認
S19
S21
LANケーブルが接続されている?
Yes
No
管理LANコントローラと保守用ネットワークポートとをつなぐ伝送路を切断し、管理用LANコントローラと制御コントローラとを伝送路でつなぐ
S23
ネットワーク設定格納部に格納されたネットワーク設定を、管理LAN設定に変更
S25
管理LANコントローラと制御コントローラとをつなぐ伝送路を切断し、管理LANコントローラと管理LANポートとを伝送路でつなぐ
S27
エンド

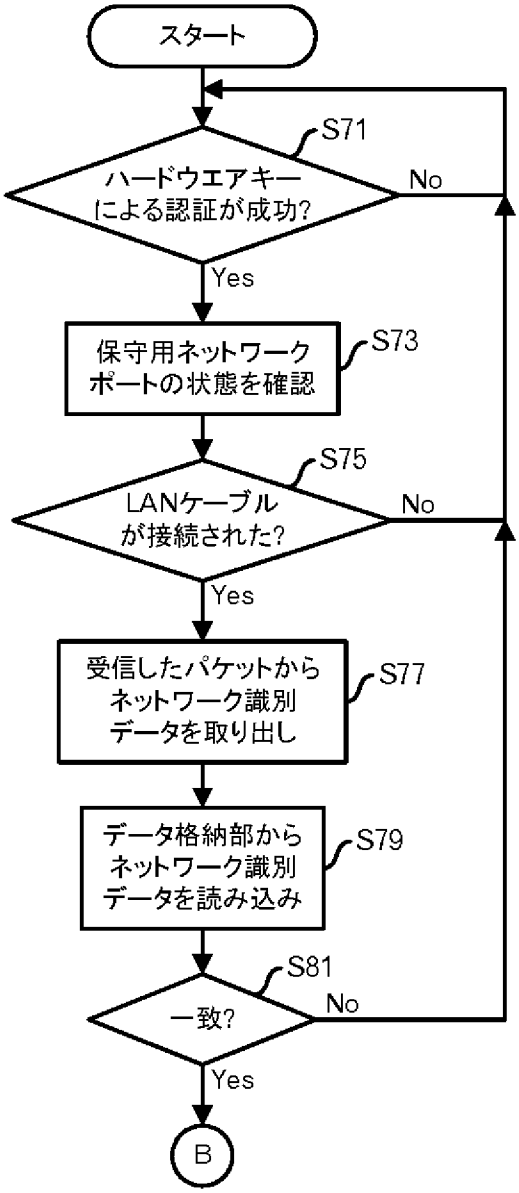
[図11]


スタート
パケットを受信
S61
S63
ネットワーク
設定が一致?
No
Yes
パケットを廃棄
S67
パケットに含まれる
データに応じた処理
を実行
S65
エンド

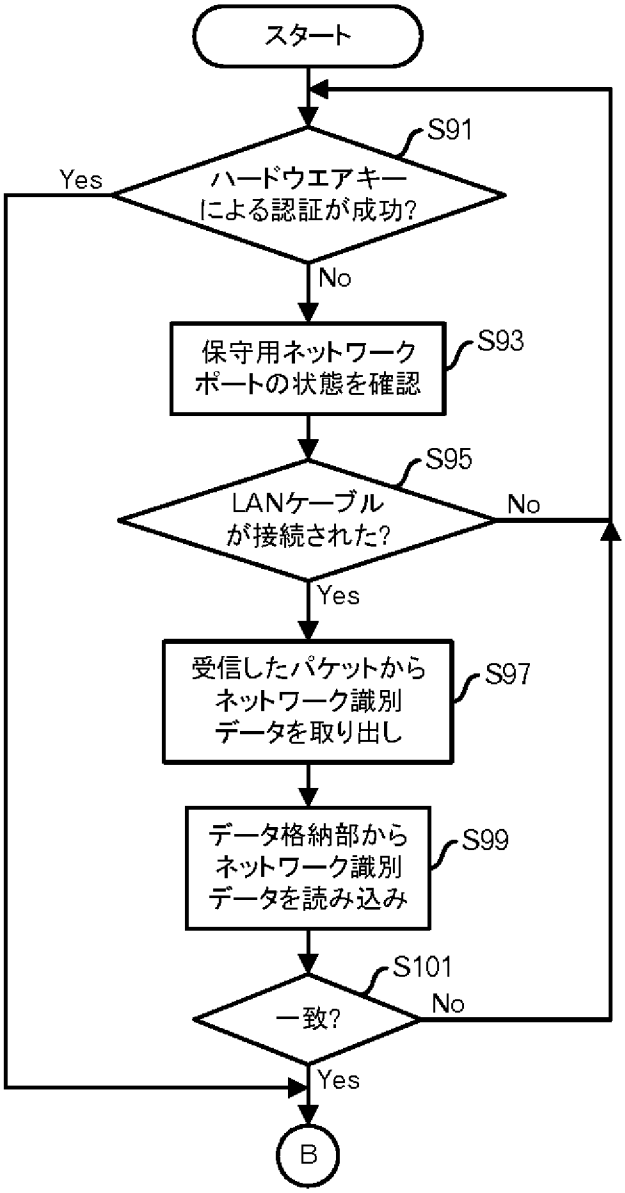
[図12]


1
サーバ
10
切替コントローラ
制御コントローラ
101
ハードウエアキー
読み取り装置
13
ハードウエアキー
5

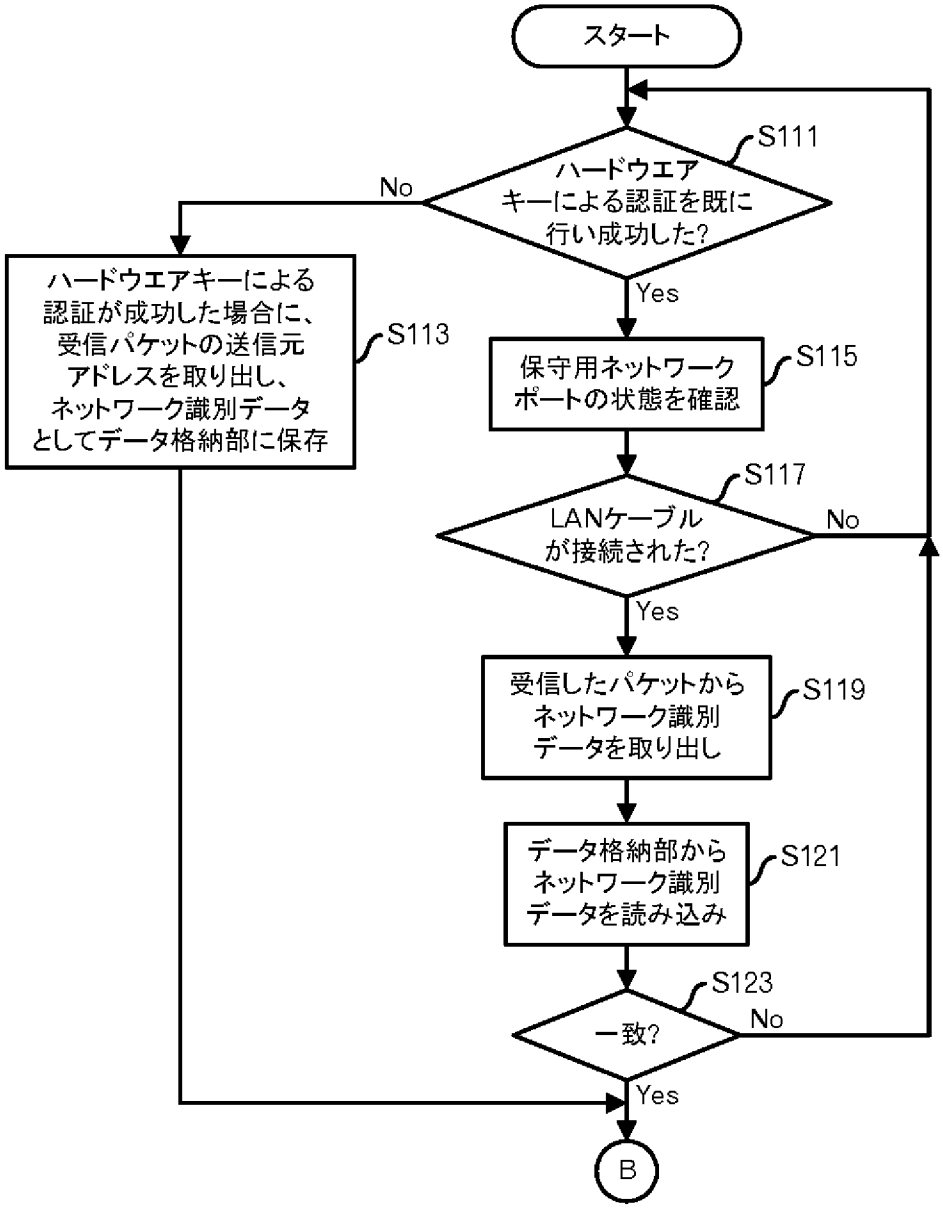
[図13]


スタート
S71
ハードウエアキー
による認証が成功?
No
Yes
保守用ネットワーク
ポートの状態を確認
S73
S75
LANケーブル
が接続された?
No
Yes
受信したパケットから
ネットワーク識別
データを取り出し
S77
データ格納部から
ネットワーク識別
データを読み込み
S79
S81
一致?
No
Yes
B

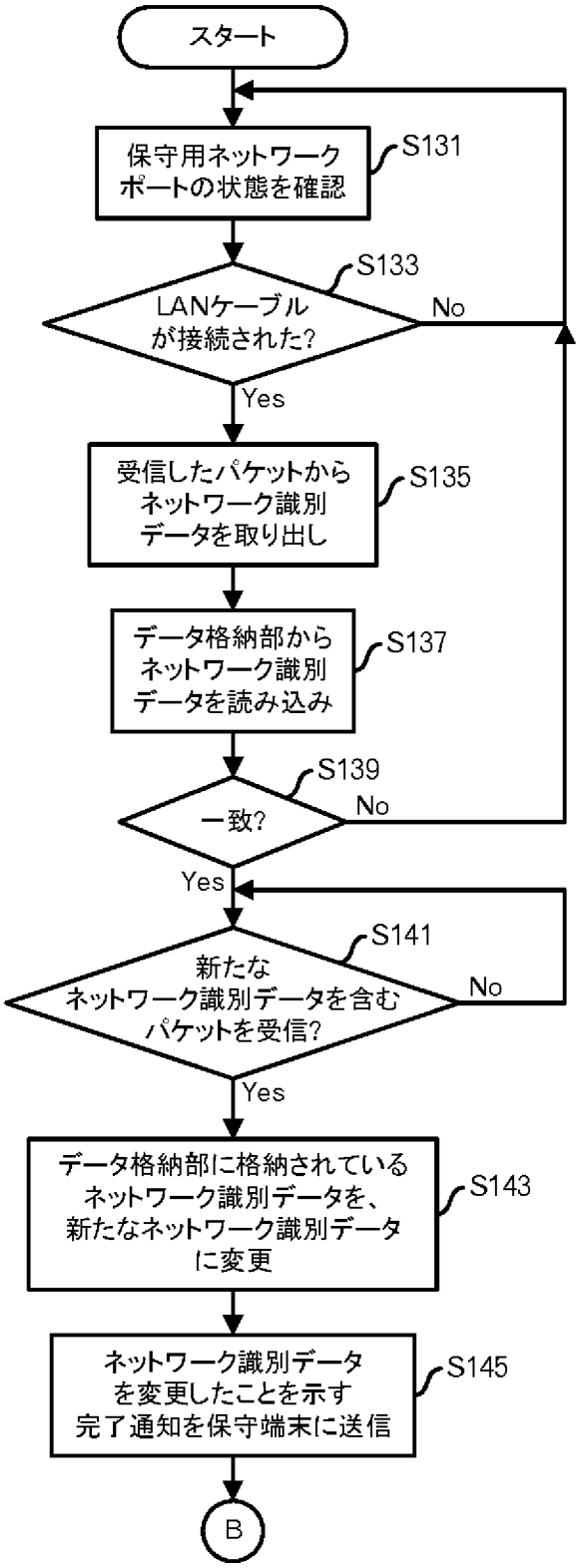
[図14]


スタート
S91
ハードウエアキー
による認証が成功?
Yes
No
保守用ネットワーク
ポートの状態を確認
S93
S95
LANケーブル
が接続された?
No
Yes
受信したパケットから
ネットワーク識別
データを取り出し
S97
データ格納部から
ネットワーク識別
データを読み込み
S99
S101
一致?
No
Yes
B

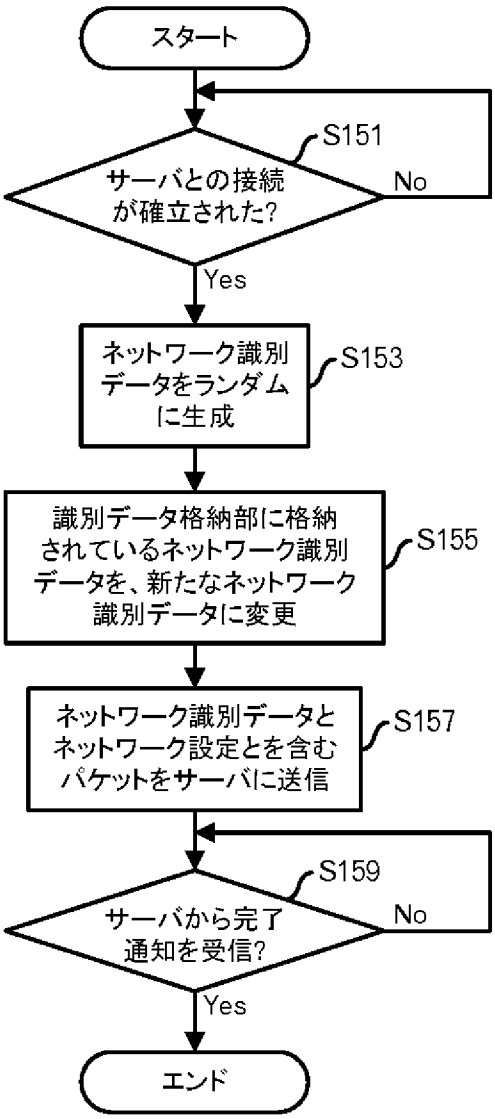
[図15]


スタート
S111
ハードウエア
キーによる認証を既に
行い成功した?
No
Yes
ハードウエアキーによる
認証が成功した場合に、
受信パケットの送信元
アドレスを取り出し、
ネットワーク識別データ
としてデータ格納部に保存
S113
保守用ネットワーク
ポートの状態を確認
S115
S117
LANケーブル
が接続された?
No
Yes
受信したパケットから
ネットワーク識別
データを取り出し
S119
データ格納部から
ネットワーク識別
データを読み込み
S121
S123
一致?
No
Yes
B

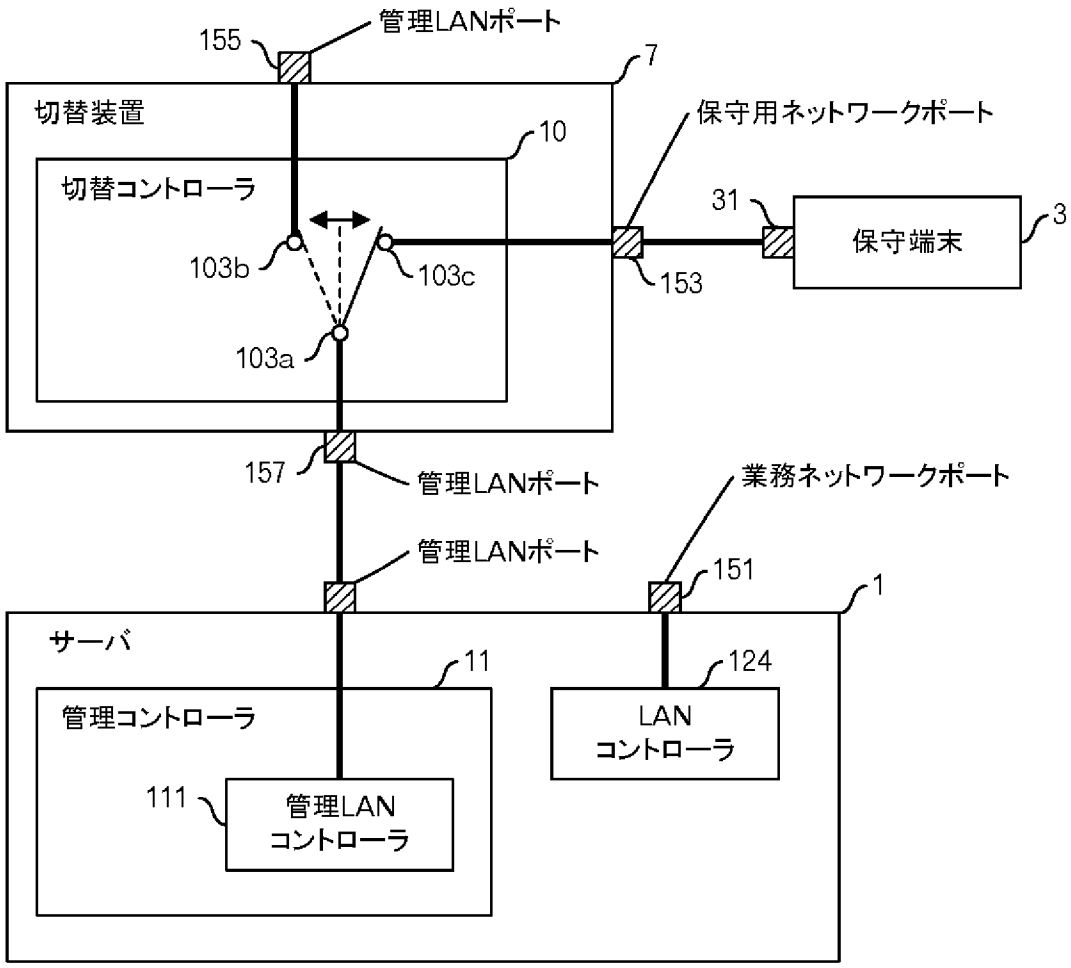
[図16]


スタート
保守用ネットワーク
ポートの状態を確認
S131
LANケーブル
が接続された?
S133
No
Yes
受信したパケットから
ネットワーク識別
データを取り出し
S135
データ格納部から
ネットワーク識別
データを読み込み
S137
一致?
S139
No
Yes
新たな
ネットワーク識別データを含む
パケットを受信?
S141
No
Yes
データ格納部に格納されている
ネットワーク識別データを、
新たなネットワーク識別データ
に変更
S143
ネットワーク識別データ
を変更したことを示す
完了通知を保守端末に送信
S145
B

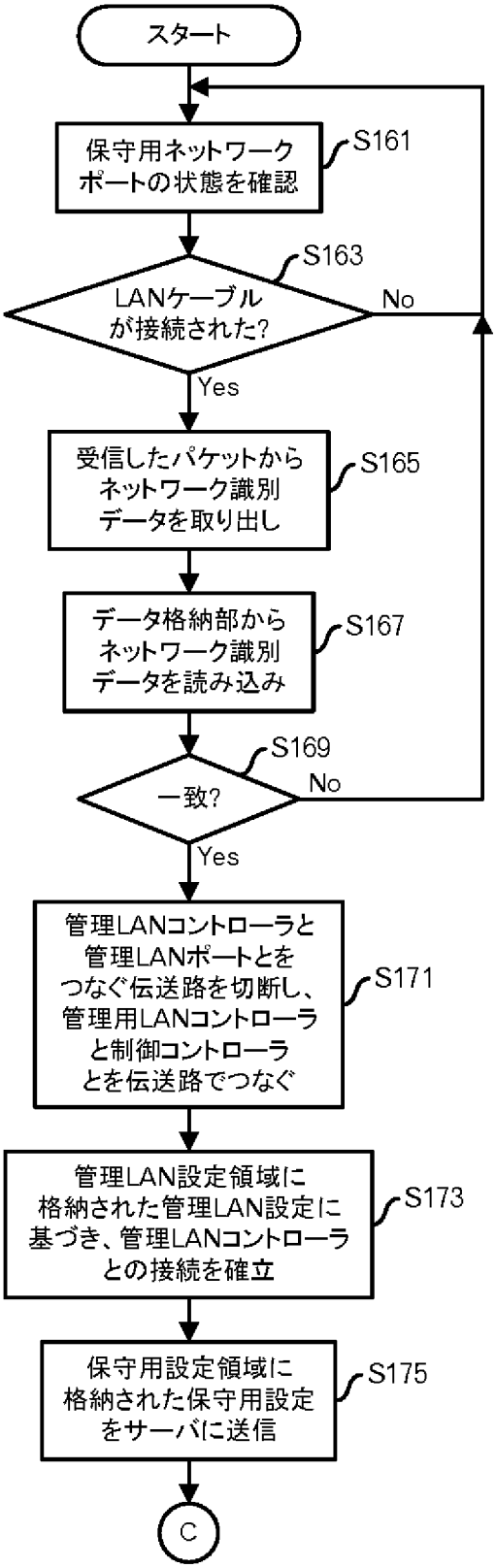
[図17]


スタート
S151
サーバとの接続が確立された?
No
Yes
ネットワーク識別データをランダムに生成
S153
識別データ格納部に格納されているネットワーク識別データを、新たなネットワーク識別データに変更
S155
ネットワーク識別データとネットワーク設定とを含むパケットをサーバに送信
S157
S159
サーバから完了通知を受信?
No
Yes
エンド

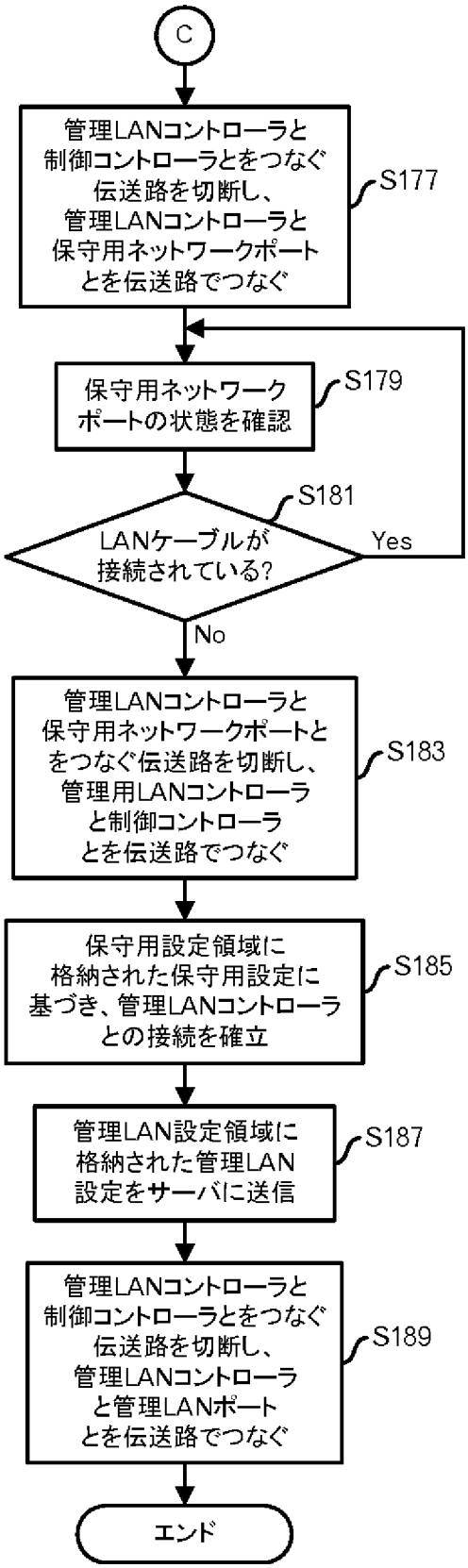
[図18]


155
管理LANポート
7
切替装置
10
切替コントローラ
保守用ネットワークポート
31
保守端末
3
103b
103c
153
103a
157
管理LANポート
業務ネットワークポート
管理LANポート
151
1
サーバ
11
124
管理コントローラ
LAN
コントローラ
111
管理LAN
コントローラ

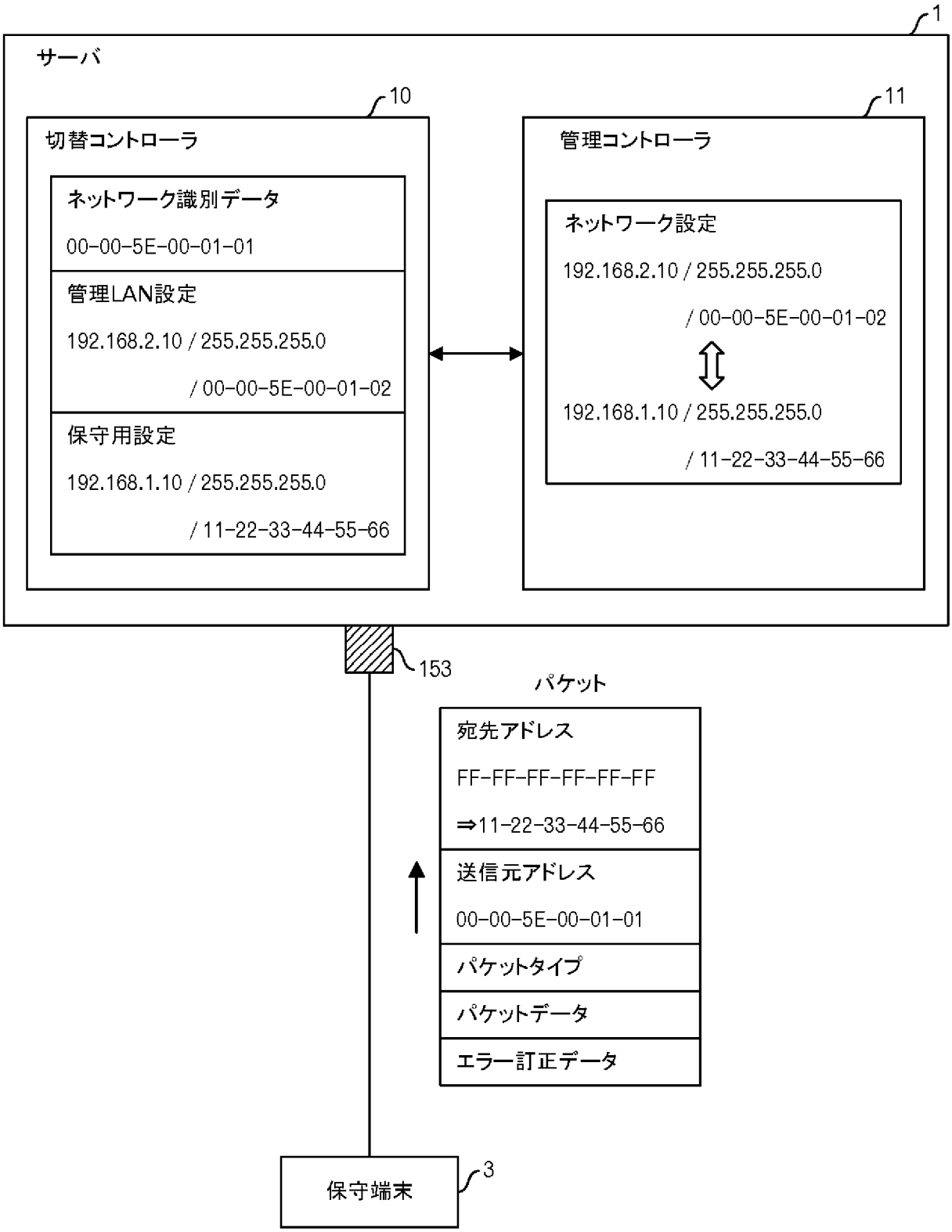
[図19]


スタート
保守用ネットワーク
ポートの状態を確認
S161
S163
LANケーブル
が接続された?
No
Yes
受信したパケットから
ネットワーク識別
データを取り出し
S165
データ格納部から
ネットワーク識別
データを読み込み
S167
S169
一致?
No
Yes
管理LANコントローラと
管理LANポートとを
つなぐ伝送路を切断し、
管理用LANコントローラ
と制御コントローラ
とを伝送路でつなぐ
S171
管理LAN設定領域に
格納された管理LAN設定に
基づき、管理LANコントローラ
との接続を確立
S173
保守用設定領域に
格納された保守用設定
をサーバに送信
S175
C

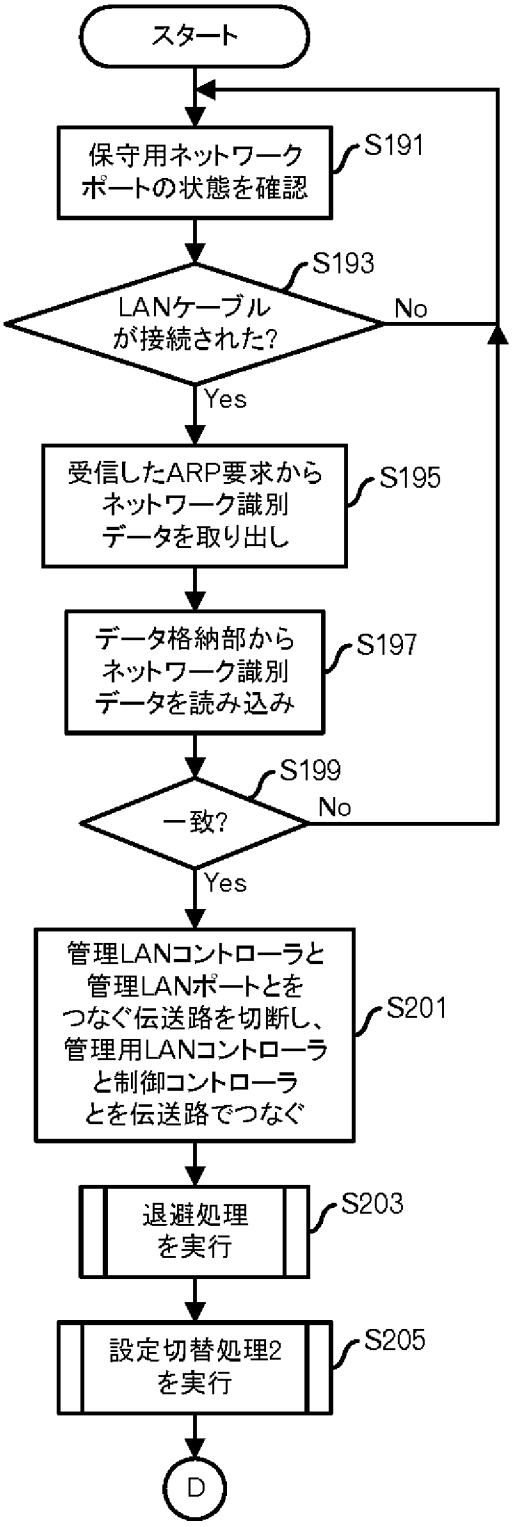
[図20]


C
管理LANコントローラと制御コントローラとをつなぐ伝送路を切断し、管理LANコントローラと保守用ネットワークポートとを伝送路でつなぐ
S177
保守用ネットワークポートの状態を確認
S179
S181
LANケーブルが接続されている?
Yes
No
管理LANコントローラと保守用ネットワークポートとをつなぐ伝送路を切断し、管理用LANコントローラと制御コントローラとを伝送路でつなぐ
S183
保守用設定領域に格納された保守用設定に基づき、管理LANコントローラとの接続を確立
S185
管理LAN設定領域に格納された管理LAN設定をサーバに送信
S187
管理LANコントローラと制御コントローラとをつなぐ伝送路を切断し、管理LANコントローラと管理LANポートとを伝送路でつなぐ
S189
エンド

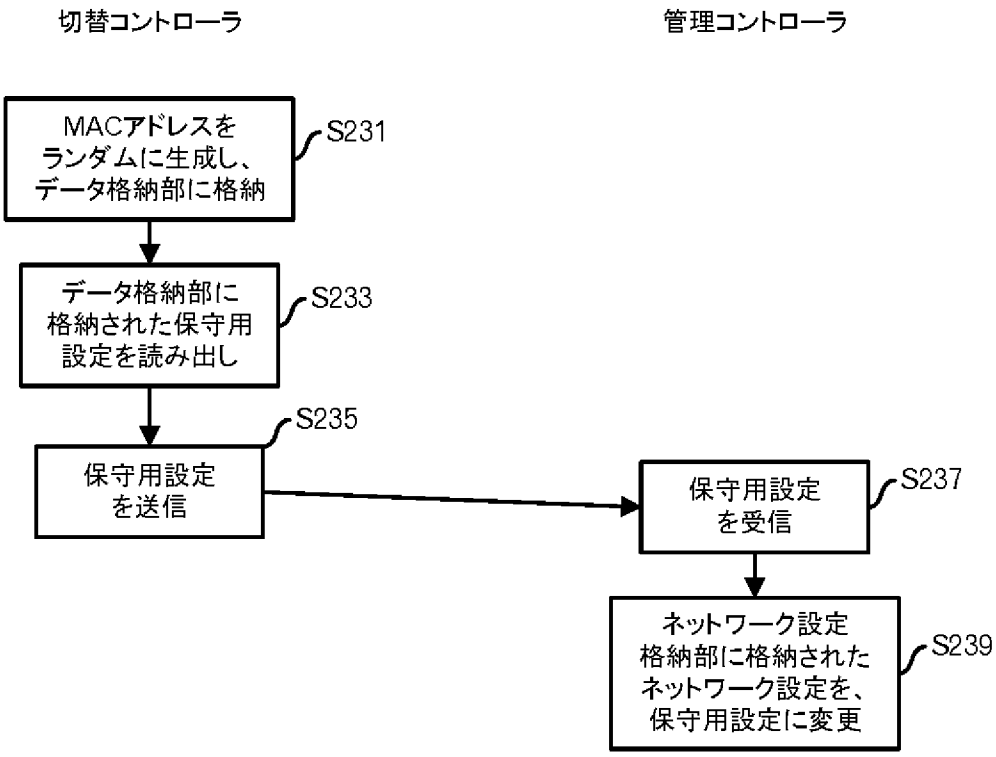
[図21]


1
サーバ
10
切替コントローラ
ネットワーク識別データ
00-00-5E-00-01-01
管理LAN設定
192.168.2.10 / 255.255.255.0
/ 00-00-5E-00-01-02
保守用設定
192.168.1.10 / 255.255.255.0
/ 11-22-33-44-55-66
11
管理コントローラ
ネットワーク設定
192.168.2.10 / 255.255.255.0
/ 00-00-5E-00-01-02
192.168.1.10 / 255.255.255.0
/ 11-22-33-44-55-66
153
パケット
宛先アドレス
FF-FF-FF-FF-FF-FF
⇒11-22-33-44-55-66
送信元アドレス
00-00-5E-00-01-01
パケットタイプ
パケットデータ
エラー訂正データ
保守端末
3

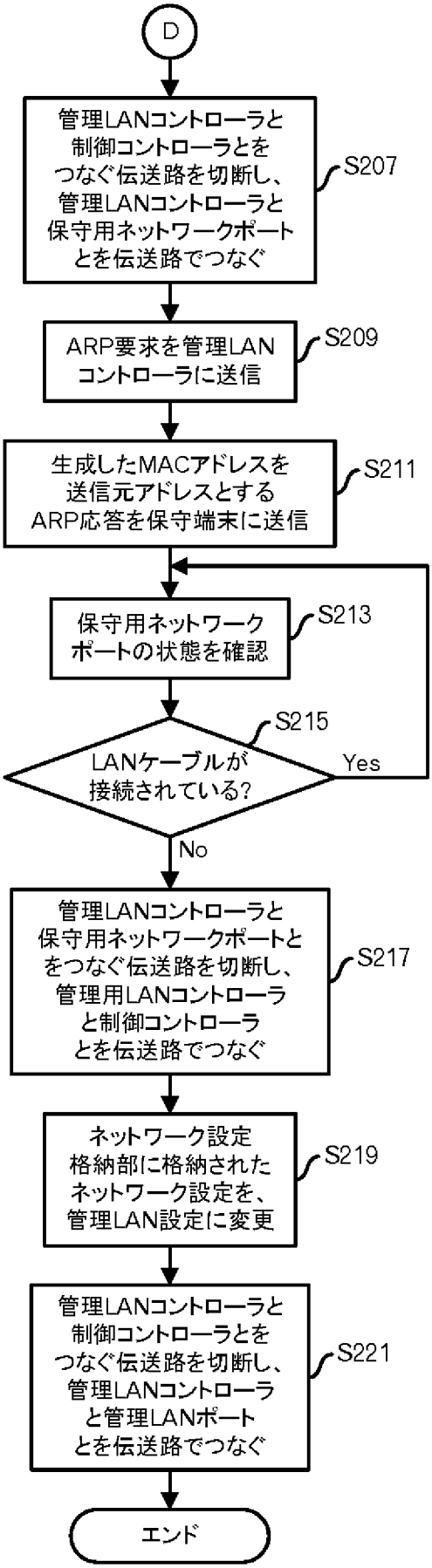
[図22]


スタート
保守用ネットワーク
ポートの状態を確認
S191
S193
LANケーブル
が接続された?
No
Yes
受信したARP要求から
ネットワーク識別
データを取り出し
S195
データ格納部から
ネットワーク識別
データを読み込み
S197
S199
一致?
No
Yes
管理LANコントローラと
管理LANポートとを
つなぐ伝送路を切断し、
管理用LANコントローラ
と制御コントローラ
とを伝送路でつなぐ
S201
退避処理
を実行
S203
設定切替処理2
を実行
S205
D

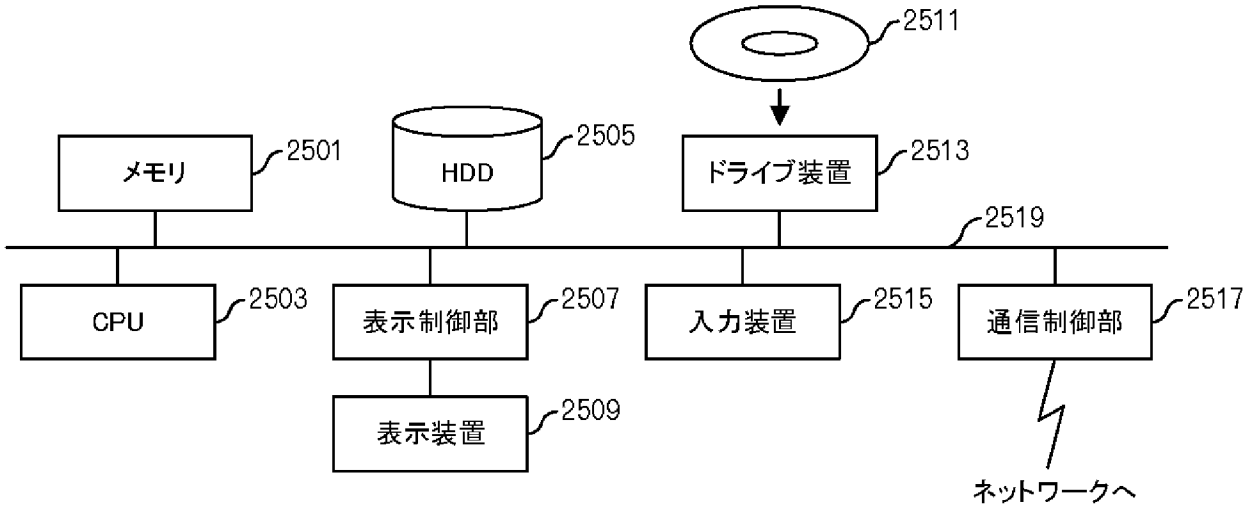
[図23]


切替コントローラ
管理コントローラ
MACアドレスを
ランダムに生成し、
データ格納部に格納
S231
データ格納部に
格納された保守用
設定を読み出し
S233
S235
保守用設定
を送信
保守用設定
を受信
S237
ネットワーク設定
格納部に格納された
ネットワーク設定を、
保守用設定に変更
S239

[図24]


D
管理LANコントローラと制御コントローラとをつなぐ伝送路を切断し、管理LANコントローラと保守用ネットワークポートとを伝送路でつなぐ
S207
ARP要求を管理LANコントローラに送信
S209
生成したMACアドレスを送信元アドレスとするARP応答を保守端末に送信
S211
保守用ネットワークポートの状態を確認
S213
S215
LANケーブルが接続されている?
Yes
No
管理LANコントローラと保守用ネットワークポートとをつなぐ伝送路を切断し、管理用LANコントローラと制御コントローラとを伝送路でつなぐ
S217
ネットワーク設定格納部に格納されたネットワーク設定を、管理LAN設定に変更
S219
管理LANコントローラと制御コントローラとをつなぐ伝送路を切断し、管理LANコントローラと管理LANポートとを伝送路でつなぐ
S221
エンド

[図25]


2511
メモリ
2501
HDD
2505
ドライブ装置
2513
2519
CPU
2503
表示制御部
2507
入力装置
2515
通信制御部
2517
表示装置
2509
ネットワークへ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/056686

A. CLASSIFICATION OF SUBJECT MATTER
G06F13/00(2006.01)i

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)
G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2015
Kokai Jitsuyo Shinan Koho 1971-2015 Toroku Jitsuyo Shinan Koho 1994-2015

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 2003-152806 A (Ionos Co., Ltd.), 23 May 2003 (23.05.2003), paragraphs [0042] to [0070]; fig. 7 (Family: none)	1-10
A	JP 2011-010080 A (Ricoh Co., Ltd.), 13 January 2011 (13.01.2011), paragraphs [0043] to [0079]; fig. 1 (Family: none)	1-10
A	JP 2013-048399 A (Panasonic Corp.), 07 March 2013 (07.03.2013), paragraphs [0133] to [0191]; fig. 12 & US 2012/0213125 A1	1-10

☐ 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
19 May 2015 (19.05.15)	26 May 2015 (26.05.15)
Name and mailing address of the ISA/ Japan Patent Office 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／ＪＰ２０１５／０５６６８６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F13/00(2006.01)i

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））

Int.Cl.　G06F13/00

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	１９７１－２０１５年
日本国実用新案登録公報	１９９６－２０１５年
日本国登録実用新案公報	１９９４－２０１５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 2003-152806 A（株式会社イオノス）2003.05.23, 段落【００４２】－【００７０】,図７ （ファミリーなし）	1-10
Ａ	JP 2011-010080 A（株式会社リコー）2011.01.13, 段落【００４３】－【００７９】,図１ （ファミリーなし）	1-10
Ａ	JP 2013-048399 A（パナソニック株式会社）2013.03.07, 段落【０１３３】－【０１９１】,図１２ & US 2012/0213125 A1	1-10

☐　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矛盾するものではなく、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
１９．０５．２０１５	２６．０５．２０１５

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｔ　４１７６
田上　隆一
電話番号　０３－３５８１－１１０１　内線　３５６８