

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2007-201932
(P2007-201932A)

(43) 公開日 平成19年8月9日(2007.8.9)

(51) Int. Cl. F I テーマコード (参考)
 HO 4 L 12/28 (2006.01) HO 4 L 12/28 2 0 0 Z 5 K O 3 3
 HO 4 L 12/44 (2006.01) HO 4 L 12/44 3 0 0

審査請求 未請求 請求項の数 5 O L (全 14 頁)

(21) 出願番号 特願2006-19494 (P2006-19494)
 (22) 出願日 平成18年1月27日 (2006.1.27)

(71) 出願人 000005223
 富士通株式会社
 神奈川県川崎市中原区上小田中4丁目1番
 1号
 (74) 代理人 100089118
 弁理士 酒井 宏明
 (72) 発明者 谷口 清
 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
 (72) 発明者 高安 昭男
 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
 (72) 発明者 遠藤 充昭
 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

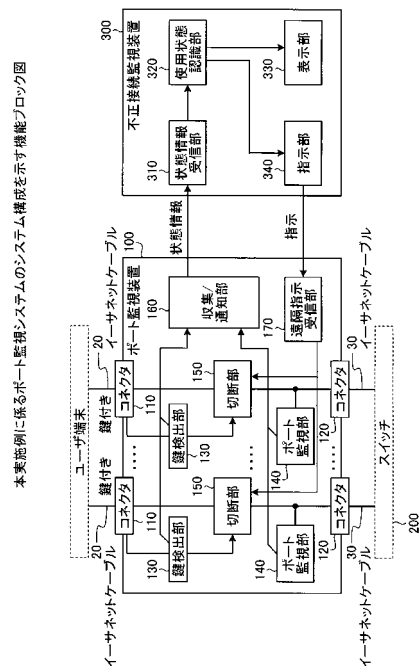
最終頁に続く

(54) 【発明の名称】 ポート監視装置およびポート監視方法

(57) 【要約】

【課題】スイッチのポートの不正使用を防止すること。
 【解決手段】ポート監視装置100の各コネクタ120をイーサネット(登録商標)ケーブル30でスイッチ200のポートにそれぞれ接続し、ユーザ端末との接続に使用しないコネクタ110にはダミーコネクタ10を挿入し、各鍵検出部130が対応するコネクタ110の鍵の状態を検出し、各ポート監視部140が対応するポートの状態を検出し、収集/通知部160が、各鍵の状態および各ポートの状態に関する情報を定期的に収集して不正接続監視装置300に送信し、不正接続監視装置300が受信した情報に基づいてスイッチ200のポートの不正使用を認識する。

【選択図】 図2



【特許請求の範囲】**【請求項 1】**

ネットワークの構築に使用するスイッチに他端が接続するケーブルの接続に使用される第 1 のコネクタ手段と、

前記第 1 のコネクタ手段のスイッチとの接続状態を検出する接続状態検出手段と、

前記スイッチを介してネットワークを利用する利用装置に他端が接続するケーブルの接続に使用され、施錠が可能な第 2 のコネクタ手段と、

前記第 2 のコネクタ手段の施錠状態を検出する施錠状態検出手段と、

前記接続状態検出手段により検出された接続状態および前記施錠状態検出手段により検出された施錠状態を所定の通知先に通知する状態通知手段と、

を備えたことを特徴とするポート監視装置。

10

【請求項 2】

前記第 2 のコネクタ手段には、施錠により該第 2 のコネクタ手段に固定されることによって、前記利用装置に他端が接続するケーブルのコネクタの挿入を不可能とするダミーコネクタが挿入され、

前記施錠状態検出手段は、前記ダミーコネクタが挿入されているか否かを検出することによって前記施錠状態を検出することを特徴とする請求項 1 に記載のポート監視装置。

【請求項 3】

前記第 1 のコネクタ手段と第 2 のコネクタ手段との接続を開閉する開閉手段と、

前記所定の通知先からの操作指示を受信し、該受信した操作指示に基づいて前記開閉手段に開閉を指示する遠隔指示受信手段と、

をさらに備えたことを特徴とする請求項 1 または 2 に記載のポート監視装置。

20

【請求項 4】

前記第 1 のコネクタ手段には、スイッチへの接続に使用されるケーブルが常時接続されていることを特徴とする請求項 1、2 または 3 に記載のポート監視装置。

【請求項 5】

ネットワークの構築に使用するスイッチに他端が接続するケーブルの接続に使用される第 1 のコネクタ、および、前記スイッチを介してネットワークを利用する利用装置に他端が接続するケーブルの接続に使用され、施錠が可能な第 2 のコネクタを備えたポート監視装置の該第 1 のコネクタのスイッチとの接続状態を検出する接続状態検出工程と、

30

前記ポート監視装置の第 2 のコネクタの施錠状態を検出する施錠状態検出工程と、

前記接続状態検出工程により検出された接続状態および前記施錠状態検出工程により検出された施錠状態を所定の通知先に通知する状態通知工程と、

を含んだことを特徴とするポート監視方法。

【発明の詳細な説明】**【技術分野】****【0001】**

この発明は、ネットワークの構築に使用するスイッチ（ハブ）のポートを監視するポート監視装置およびポート監視方法に関し、特に、既存のスイッチを用いてポートの不正使用を防止することができるポート監視装置およびポート監視方法に関するものである。

40

【背景技術】**【0002】**

従来、スイッチの接続ポートへの不正接続を防止する方法として、コンフィグレーションの設定によりソフト的にポートの機能を閉塞する方法が用いられてきた。しかし、この方法の場合、接続端末数を増加させるためにコンフィグレーションの設定変更によって閉塞中であるポートを使用可能としたときに、スイッチの再起動が必要となることが多く、ネットワーク機能が一時的に中断され、業務に影響を及ぼす場合がある。また、社内にネットワーク技術者がいない場合には、設定変更の度にメーカーへ依頼することになり、緊急時の対応が難しく、ユーザー側のランニングコスト増の一因となっていた。

【0003】

50

そこで、コンフィグレーションの設定変更をすることなくポートの不正使用の防止を可能とするスイッチとして、ポートの口にピン・スイッチを備え、このピン・スイッチを施錠により固定することで物理的に接続不可能とするスイッチなどが開発されている（例えば、特許文献1および2参照。）。

【0004】

【特許文献1】特開2001-352334号公報

【特許文献2】特開平11-154566号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

しかしながら、施錠によりポートの不正使用を防止するためには、既存のスイッチを施錠機構を備えたスイッチに置き換える必要があり、スイッチの数が多い場合には、置き換えに時間やコストがかかるという問題がある。

【0006】

この発明は、上述した従来技術による問題点を解消するためになされたものであり、既存のスイッチを用いてポートの不正使用を防止することができるポート監視装置およびポート監視方法を提供することを目的とする。

【課題を解決するための手段】

【0007】

上述した課題を解決し、目的を達成するため、請求項1の発明に係るポート監視装置は、ネットワークの構築に使用するスイッチに他端が接続するケーブルの接続に使用される第1のコネクタ手段と、前記第1のコネクタ手段のスイッチとの接続状態を検出する接続状態検出手段と、前記スイッチを介してネットワークを利用する利用装置に他端が接続するケーブルの接続に使用され、施錠が可能な第2のコネクタ手段と、前記第2のコネクタ手段の施錠状態を検出する施錠状態検出手段と、前記接続状態検出手段により検出された接続状態および前記施錠状態検出手段により検出された施錠状態を所定の通知先に通知する状態通知手段と、を備えたことを特徴とする。

【0008】

この請求項1の発明によれば、第1のコネクタ手段のスイッチとの接続状態を検出し、第2のコネクタ手段の施錠状態を検出し、検出した接続状態および施錠状態を所定の通知先に通知するよう構成したので、所定の通知先がポートの使用状態を監視することができる。

【0009】

また、請求項2の発明に係るポート監視装置は、請求項1の発明において、前記第2のコネクタ手段には、施錠により該第2のコネクタ手段に固定されることによって、前記利用装置に他端が接続するケーブルのコネクタの挿入を不可能とするダミーコネクタが挿入され、前記施錠状態検出手段は、前記ダミーコネクタが挿入されているか否かを検出することによって前記施錠状態を検出することを特徴とする。

【0010】

この請求項2の発明によれば、ダミーコネクタが挿入されているか否かを検出することによって施錠状態を検出するよう構成したので、確実に施錠状態を検出することができる。

【0011】

また、請求項3の発明に係るポート監視装置は、請求項1または2の発明において、前記第1のコネクタ手段と第2のコネクタ手段との接続を開閉する開閉手段と、前記所定の通知先からの操作指示を受信し、該受信した操作指示に基づいて前記開閉手段に開閉を指示する遠隔指示受信手段と、をさらに備えたことを特徴とする。

【0012】

この請求項3の発明によれば、所定の通知先からの指示に基づいて第1のコネクタ手段と第2のコネクタ手段との接続を開閉するよう構成したので、所定の通知先がポート監視

10

20

30

40

50

装置を遠隔操作することができる。

【0013】

また、請求項4の発明に係るポート監視装置は、請求項1、2または3の発明において、前記第1のコネクタ手段には、スイッチへの接続に使用されるケーブルが常時接続されていることを特徴とする。

【0014】

この請求項4の発明によれば、第1のコネクタ手段には、スイッチへの接続に使用されるケーブルが常時接続されているよう構成したので、スイッチとの接続を容易に行うことができる。

【0015】

また、請求項5の発明に係るポート監視方法は、ネットワークの構築に使用するスイッチに他端が接続するケーブルの接続に使用される第1のコネクタ、および、前記スイッチを介してネットワークを利用する利用装置に他端が接続するケーブルの接続に使用され、施錠が可能な第2のコネクタを備えたポート監視装置の該第1のコネクタのスイッチとの接続状態を検出する接続状態検出工程と、前記ポート監視装置の第2のコネクタの施錠状態を検出する施錠状態検出工程と、前記接続状態検出工程により検出された接続状態および前記施錠状態検出工程により検出された施錠状態を所定の通知先に通知する状態通知工程と、を含んだことを特徴とする。

10

【0016】

この請求項5の発明によれば、第1のコネクタのスイッチとの接続状態を検出し、第2のコネクタの施錠状態を検出し、検出した接続状態および施錠状態を所定の通知先に通知するよう構成したので、所定の通知先がポートの使用状態を監視することができる。

20

【発明の効果】

【0017】

請求項1および5の発明によれば、所定の通知先がポートの使用状態を監視することができるので、ポートの不正使用を防止することができるという効果を奏する。

【0018】

また、請求項2の発明によれば、確実に施錠状態を検出するので、所定の通知先に正確な情報を通知することができるという効果を奏する。

【0019】

また、請求項3の発明によれば、所定の通知先がポート監視装置を遠隔操作することができるので、所定の通知先からポートの不正使用を防止する操作を行うことができるという効果を奏する。

30

【0020】

また、請求項4の発明によれば、スイッチとの接続を容易に行うことができるので、既存スイッチを用いたポートの不正使用の防止を簡単に行うことができるという効果を奏する。

【発明を実施するための最良の形態】

【0021】

以下に添付図面を参照して、この発明に係るポート監視装置およびポート監視方法の好適な実施例を詳細に説明する。なお、本実施例では、本発明をイーサネット（登録商標）のポートに適用した場合を中心に説明する。

40

【実施例】

【0022】

まず、本実施例に係るポート監視装置のポートロック機構について説明する。図1は、本実施例に係るポート監視装置のポートロック機構を説明するための説明図である。同図(a)は本実施例に係るポート監視装置の正面図を示し、同図(b)は本実施例に係るポート監視装置の背面図を示している。

【0023】

同図(a)に示すように、このポート監視装置100では、未使用ポートについては施

50

錠機構を備えたダミーコネクタ10が挿入され、専用鍵によるロック機能が働いてダミーコネクタ10がポートに物理的にロックされる。したがって、専用鍵を有しない不正使用者は、ダミーコネクタ10を抜き取ることができず、未使用ポートを使用することができない。

【0024】

また、同図(b)に示すように、このポート監視装置100は、背面でポートごとにイーサネット(登録商標)ケーブル30でスイッチ200に接続されており、スイッチ200は、ポート監視装置100に接続されている全てのポートが使用可能な状態に設定されている。したがって、専用鍵を有するユーザーは、ポート監視装置100の未使用ポートに挿入されたダミーコネクタ10を取り除き、イーサネット(登録商標)ケーブルを接続するだけでスイッチ200を利用することができる。

10

【0025】

このように、本実施例に係るポート監視装置100は、背面の各ポートがスイッチ200のそれぞれのポートに接続された状態で使用され、施錠機構を備えたダミーコネクタ10を用いて正面の未使用ポートの不正使用を防ぐとともに、専用鍵を用いてダミーコネクタ10を取り除くだけでスイッチ200を利用することを可能としている。

【0026】

次に、本実施例に係るポート監視システムの構成について説明する。図2は、本実施例に係るポート監視システムの構成を示す機能ブロック図である。同図に示すように、このポート監視システムは、ポート監視装置100と、スイッチ200と、スイッチ200への不正接続を監視する不正接続監視装置300とから構成され、スイッチ200のポートの不正使用を監視する。

20

【0027】

ポート監視装置100は、ユーザ端末(利用装置)との接続に用いる正面のコネクタ110と、スイッチとの接続に用いる背面のコネクタ120と、鍵検出部130と、ポート監視部140と、コネクタ110とコネクタ120間の内部接続を電氣的に開閉する切断部150との組み合わせを複数個有し、また、収集/通知部160および遠隔指示受信部170を有する。

【0028】

コネクタ110は、ユーザ端末と接続されたイーサネット(登録商標)ケーブル20を接続するコネクタであり、使用されていない場合には、図1に示したダミーコネクタ10が挿入される。すなわち、コネクタ110は、ダミーコネクタ10とともに用いられて鍵付きポートとして機能する。

30

【0029】

コネクタ120はスイッチ200と接続されたイーサネット(登録商標)ケーブル30が接続されるコネクタであり、このコネクタ120には、イーサネット(登録商標)ケーブル30が常時接続され、イーサネット(登録商標)ケーブル30の反対側がスイッチ200に接続される。

【0030】

鍵検出部130は、コネクタ110にダミーコネクタ10が挿入されているか否かを検出することによって、コネクタ110の状態を検出する検出部である。具体的には、この鍵検出部130は、コネクタ110にダミーコネクタ10が挿入されている場合には、コネクタ110の状態を「鍵閉」として検出し、イーサネット(登録商標)ケーブル20が接続されている場合には、コネクタ110の状態を「鍵開」として検出する。

40

【0031】

また、この鍵検出部130は、コネクタ110の状態を「鍵閉」として検出した場合には、切断部150に対してコネクタ110とコネクタ120との間の接続を切断するように指示し、コネクタ110の状態を「鍵開」として検出した場合には、切断部150に対してコネクタ110とコネクタ120とを接続するように指示する。

【0032】

50

ポート監視部 140 は、コネクタ 120 にパケットが流れているか否かを検出することによって、コネクタ 120 に対応するポートの状態を検出する検出部である。具体的には、このポート監視部 140 は、コネクタ 120 にパケットが流れている場合には、コネクタ 120 に対応するポートの状態を「ポート生」あるいは「ポート開」として検出し、パケットが流れていない場合には、コネクタ 120 に対応するポートの状態を「ポート死」あるいは「ポート閉」として検出する。

【0033】

切断部 150 は、鍵検出部 130 または遠隔指示受信部 170 からの指示に基づいてコネクタ 110 とコネクタ 120 との間の電氣的接続を開閉するスイッチである。

【0034】

収集/通知部 160 は、各鍵検出部 130 が検出した各コネクタ 110 の状態に関する情報および各ポート監視部 140 が検出した各コネクタ 120 に対応するポートの状態に関する情報を定期的に収集し、収集した情報無線 LAN を用いてメールで不正接続監視装置 300 に送信する処理部である。

【0035】

この収集/通知部 160 が、各コネクタ 110 の状態に関する情報および各ポートの状態に関する情報を定期的に収集し、収集した情報を不正接続監視装置 300 に送信することによって、不正接続監視装置 300 は、スイッチ 200 の不正使用を監視することができる。

【0036】

なお、ここでは、無線 LAN を用いることとしたが、イーサネット（登録商標）や携帯電話など他の通信手段を用いて情報を送信することもできる。また、メール以外の方法で情報を送信することもできる。

【0037】

遠隔指示受信部 170 は、不正接続監視装置 300 からコネクタ 110 とコネクタ 120 との間の電氣的接続の開閉指示および開閉箇所の情報を無線 LAN を用いて受け取り、開閉箇所に対応する切断部 150 に開閉指示を伝える処理部である。

【0038】

この遠隔指示受信部 170 が、不正接続監視装置 300 からコネクタ 110 とコネクタ 120 との間の電氣的接続の開閉指示および開閉箇所の情報を受け取り、開閉箇所に対応する切断部 150 に開閉指示を伝えることによって、不正接続監視装置 300 はポート監視装置 100 を遠隔操作することができる。

【0039】

不正接続監視装置 300 は、ポート監視装置 100 から受信した情報などに基づいてスイッチ 200 の不正使用を監視する装置であり、状態情報受信部 310 と、使用状態認識部 320 と、表示部 330 と、指示部 340 とを有する。

【0040】

状態情報受信部 310 は、ポート監視装置 100 から各コネクタ 110 の状態に関する情報および各ポートの状態に関する情報を定期的に受信する処理部であり、受信した情報を使用状態認識部 320 に渡す。

【0041】

使用状態認識部 320 は、状態情報受信部 310 からポート監視装置 100 の各コネクタ 110 の状態に関する情報および各ポートの状態に関する情報を受け取ってスイッチ 200 のポートの使用状態を認識する処理部である。

【0042】

図 3 は、この使用状態認識部 320 によるスイッチ 200 の各ポートの使用状態認識方法を示す図である。同図に示すように、この使用状態認識部 320 は、ポート監視装置 100 のポートが「ポート生」（「ポート開」）でコネクタ 100 の状態が「鍵開」である場合には、ポート監視装置 100 のポートが生きていて鍵が空いている状態なので、スイッチ 200 の対応するポートが正常運用であると認識する。

10

20

30

40

50

【0043】

また、この使用状態認識部320は、ポート監視装置100のポートが「ポート生」（「ポート開」）でコネクタ100の状態が「鍵閉」である場合には、ポート監視装置100のポートが生きていて鍵が閉まっている状態なので、鍵を開けることによってスイッチ200の対応するポートが使用可能であると認識する。

【0044】

また、この使用状態認識部320は、ポート監視装置100のポートが「ポート死」（「ポート閉」）でコネクタ100の状態が「鍵開」である場合には、ポート監視装置100のポートが死んでいて鍵が空いている状態なので、スイッチ200の対応するポートが空いていると認識する。

10

【0045】

また、この使用状態認識部320は、ポート監視装置100のポートが「ポート死」（「ポート閉」）でコネクタ100の状態が「鍵閉」である場合には、ポート監視装置100のポートが死んでいて鍵が閉まっている状態なので、鍵が閉まっているということは不正使用を防ぐためでありポート監視装置100のポートは生きた状態であるべきであるのに死んでいるということは、ポート監視装置100とスイッチ200の間のイーサネット（登録商標）ケーブル30がスイッチ200から不正に取り外された状態であると認識し、スイッチ200の対応するポートが不正使用されていると認識する。

【0046】

このように、この使用状態認識部320が、ポート監視装置100のポートが「ポート死」でコネクタ100の状態が「鍵閉」である場合に、ポート監視装置100とスイッチ200の間のイーサネット（登録商標）ケーブル30がスイッチ200から不正に取り外された状態であると認識し、スイッチ200の対応するポートが不正使用されていると認識することによって、不正接続監視装置300は、スイッチ200のポートの不正使用を監視することができる。

20

【0047】

また、この使用状態認識部320は、ポート監視装置100からの情報に基づいて正常運用の状態にあると認識したポートについて、ユーザ端末からの情報に基づいて、ポート監視装置100からの不正接続があるか否かを認識し、ポート監視装置100からの不正接続があると認識した場合には、指示部340に対して、そのポートに対応するコネクタ

30

【0048】

すなわち、この使用状態認識部320は、ユーザ端末が通信不可の状態にあり、そのユーザ端末が使用しているはずのポート監視装置100のポートが正常運用の状態にある場合には、そのポートが不正使用されていると認識する。

【0049】

この使用状態認識部320が、ポート監視装置100からの情報に基づいて正常運用の状態にあると認識したポートについて、ユーザ端末からの情報に基づいて、ポート監視装置100からの不正接続があるか否かを認識し、ポート監視装置100からの不正接続があると認識した場合には、指示部340に対して、そのポートに対応するコネクタ110

40

- コネクタ120間の接続を切断するように指示することによって、ポート監視装置100のポートからの不正接続をポート監視装置100を遠隔操作して防止することができる。

【0050】

表示部330は、使用状態認識部320による認識結果を表示する処理部である。すなわち、この表示部330は、スイッチ200の各ポートが正常に使用されている状態か、使用可能で未使用の状態か、空きの状態か、不正使用されている状態のいずれの状態にあるかを表示する。

【0051】

指示部340は、使用状態認識部320の指示に基づいて、ポート監視装置100に対

50

して切断箇所を指定してコネクタ 1 1 0 - コネクタ 1 2 0 間の接続を切断するように指示する処理部である。

【 0 0 5 2 】

次に、本実施例に係るポート監視システムによるポート状態監視処理の処理手順について説明する。図 4 は、本実施例に係るポート監視システムによるポート状態監視処理の処理手順を示すフローチャートである。

【 0 0 5 3 】

同図に示すように、このポート状態監視処理では、ポート監視装置 1 0 0 の収集 / 通知部 1 6 0 が鍵およびポートの状態を収集し (ステップ S 1 0 1)、収集した状態に関する情報を不正接続監視装置 3 0 0 に通知する (ステップ S 1 0 2)。

10

【 0 0 5 4 】

そして、不正接続監視装置 3 0 0 の状態情報受信部 3 1 0 が状態情報を受信し、使用状態認識部 3 2 0 が状態情報に基づいてスイッチ 2 0 0 の各ポートの使用状態を判定する。すなわち、使用状態認識部 3 2 0 は、ポート状態を判定し (ステップ S 1 0 3)、ポート状態が「ポート開」である場合には、鍵の状態すなわちコネクタ 1 1 0 の状態を判定する (ステップ S 1 0 4)。

【 0 0 5 5 】

その結果、鍵の状態が「鍵閉」である場合には、使用可能で未使用の状態にあると認識し (ステップ S 1 0 5)、鍵の状態が「鍵開」である場合には、正常運用の状態にあると認識する (ステップ S 1 0 6)。

20

【 0 0 5 6 】

一方、ポート状態が「ポート閉」である場合にも、鍵の状態を判定し (ステップ S 1 0 7)、鍵の状態が「鍵開」である場合には、空きの状態にあると認識し (ステップ S 1 0 8)、鍵の状態が「鍵閉」である場合には、不正使用の状態にあると認識する (ステップ S 1 0 9)。

【 0 0 5 7 】

そして、使用状態認識部 3 2 0 は、全てのポートについて状態を認識したか否かを判定し (ステップ S 1 1 0)、状態認識を行っていないポートがある場合には、ステップ S 1 0 3 に戻って次のポートの状態を認識し、全ポートの認識が済んだ場合には、表示部 3 3 0 が認識結果を表示する (ステップ S 1 1 1)。

30

【 0 0 5 8 】

このように、ポート監視装置 1 0 0 が鍵およびポートの状態に関する情報を収集して不正接続監視装置 3 0 0 に通知し、不正接続監視装置 3 0 0 がポート監視装置 1 0 0 から通知された情報に基づいてスイッチ 2 0 0 のポートの状態を認識することによって、スイッチ 2 0 0 への不正接続を監視することができる。

【 0 0 5 9 】

上述してきたように、本実施例では、ポート監視装置 1 0 0 の各コネクタ 1 2 0 をイーサネット (登録商標) ケーブル 3 0 でスイッチ 2 0 0 のポートにそれぞれ接続し、ユーザ端末との接続に使用しないコネクタ 1 1 0 にはダミーコネクタ 1 0 を挿入し、各鍵検出部 1 3 0 が対応するコネクタ 1 1 0 の鍵の状態を検出し、各ポート監視部 1 4 0 が対応するポートの状態を検出し、収集 / 通知部 1 6 0 が、各鍵の状態および各ポートの状態に関する情報を定期的に収集して不正接続監視装置 3 0 0 に送信することとしたので、不正接続監視装置 3 0 0 がスイッチ 2 0 0 のポートの不正使用を認識することができる。

40

【 0 0 6 0 】

また、本実施例では、不正接続監視装置 3 0 0 の使用状態認識部 3 2 0 がポート監視装置 1 0 0 からの情報に基づいて正常運用の状態にあると判定したポートについて、ユーザ端末の通信状態に基づいてポート監視装置 1 0 0 からの不正接続の有無を判定し、ポート監視装置 1 0 0 からの不正接続があると判定した場合には、指示部 3 4 0 を介してポート監視装置 1 0 0 の遠隔指示受信部 1 7 0 に不正接続に対応するポートのコネクタ 1 1 0 - コネクタ 1 2 0 間の接続切断を指示し、遠隔指示受信部 1 7 0 が対応する切断部 1 5 0 に

50

切断させることとしたので、ポート監視装置 100 を遠隔操作してポートの不正使用を防止することができる。

【0061】

なお、本実施例では、不正接続監視装置について説明したが、不正接続監視装置が有する構成をソフトウェアによって実現することで、同様の機能を有する不正接続監視プログラムを得ることができる。そこで、この不正接続監視プログラムを実行するコンピュータについて説明する。

【0062】

図5は、本実施例に係る不正接続監視プログラムを実行するコンピュータの構成を示す機能ブロック図である。同図に示すように、このコンピュータ400は、RAM410と、CPU420と、HDD430と、LANインタフェース440と、入出力インタフェース450と、DVDドライブ460とを有する。

10

【0063】

RAM410は、プログラムやプログラムの実行途中結果などを記憶するメモリであり、CPU420は、RAM410からプログラムを読み出して実行する中央処理装置である。

【0064】

HDD430は、プログラムやデータを格納するディスク装置であり、LANインタフェース440は、コンピュータ400をLAN経由で他のコンピュータに接続するためのインタフェースである。

20

【0065】

入出力インタフェース450は、マウスやキーボードなどの入力装置および表示装置を接続するためのインタフェースであり、DVDドライブ460は、DVDの読み書きを行う装置である。

【0066】

そして、このコンピュータ400において実行される不正接続監視プログラム411は、DVDに記憶され、DVDドライブ460によってDVDから読み出されてコンピュータ400にインストールされる。

【0067】

あるいは、この不正接続監視プログラム411は、LANインタフェース440を介して接続された他のコンピュータシステムのデータベースなどに記憶され、これらのデータベースから読み出されてコンピュータ400にインストールされる。

30

【0068】

そして、インストールされた不正接続監視プログラム411は、HDD430に記憶され、RAM410に読み出されてCPU420によって不正接続監視プロセス421として実行される。

【0069】

なお、本実施例では、イーサネット（登録商標）のスイッチ200のポートの不正使用を防止する場合について説明したが、本発明はこれに限定されるものではなく、他のネットワーク装置のポートの不正使用を防止する場合にも同様に適用することができる。

40

【0070】

（付記1）ネットワークの構築に使用するスイッチに他端が接続するケーブルの接続に使用される第1のコネクト手段と、

前記第1のコネクト手段のスイッチとの接続状態を検出する接続状態検出手段と、

前記スイッチを介してネットワークを利用する利用装置に他端が接続するケーブルの接続に使用され、施錠が可能な第2のコネクト手段と、

前記第2のコネクト手段の施錠状態を検出する施錠状態検出手段と、

前記接続状態検出手段により検出された接続状態および前記施錠状態検出手段により検出された施錠状態を所定の通知先に通知する状態通知手段と、

を備えたことを特徴とするポート監視装置。

50

【0071】

(付記2) 前記第2のコネクタ手段には、施錠により該第2のコネクタ手段に固定されることによって、前記利用装置に他端が接続するケーブルのコネクタの挿入を不可能とするダミーコネクタが挿入され、

前記施錠状態検出手段は、前記ダミーコネクタが挿入されているか否かを検出することによって前記施錠状態を検出することを特徴とする付記1に記載のポート監視装置。

【0072】

(付記3) 前記第1のコネクタ手段と第2のコネクタ手段との接続を開閉する開閉手段と、

前記所定の通知先からの操作指示を受信し、該受信した操作指示に基づいて前記開閉手段に開閉を指示する遠隔指示受信手段と、

をさらに備えたことを特徴とする付記1または2に記載のポート監視装置。

【0073】

(付記4) 前記第1のコネクタ手段には、スイッチへの接続に使用されるケーブルが常時接続されていることを特徴とする付記1、2または3に記載のポート監視装置。

【0074】

(付記5) ネットワークの構築に使用するスイッチに他端が接続するケーブルの接続に使用される第1のコネクタ、および、前記スイッチを介してネットワークを利用する利用装置に他端が接続するケーブルの接続に使用され、施錠が可能な第2のコネクタを備えたポート監視装置の該第1のコネクタのスイッチとの接続状態を検出する接続状態検出工程と

前記ポート監視装置の第2のコネクタの施錠状態を検出する施錠状態検出工程と、

前記接続状態検出工程により検出された接続状態および前記施錠状態検出工程により検出された施錠状態を所定の通知先に通知する状態通知工程と、

を含んだことを特徴とするポート監視方法。

【0075】

(付記6) 前記第2のコネクタには、施錠により該第2のコネクタに固定されることによって、前記利用装置に他端が接続するケーブルのコネクタの挿入を不可能とするダミーコネクタが挿入され、

前記施錠状態検出工程は、前記ダミーコネクタが挿入されているか否かを検出することによって前記施錠状態を検出することを特徴とする付記5に記載のポート監視方法。

【0076】

(付記7) 前記所定の通知先からの操作指示を受信し、該受信した操作指示に基づいて前記第1のコネクタと第2のコネクタとの接続を開閉する工程をさらに含んだことを特徴とする付記5または6に記載のポート監視方法。

【0077】

(付記8) 前記第1のコネクタには、スイッチへの接続に使用されるケーブルが常時接続されていることを特徴とする付記5、6または7に記載のポート監視方法。

【0078】

(付記9) ネットワークの構築に使用するスイッチに他端が接続するケーブルの接続に使用される第1のコネクタおよび該スイッチを介してネットワークを利用する利用装置に他端が接続するケーブルの接続に使用される施錠可能な第2のコネクタを有するポート監視装置から該第1のコネクタのスイッチとの接続状態および第2のコネクタの施錠状態に関する情報を受信する状態情報受信手順と、

前記状態情報受信手順により受信した状態情報が、前記接続状態が閉であり、かつ施錠状態が閉であることを示している場合に、前記スイッチが不正使用されていると判定する不正使用判定手順と、

をコンピュータに実行させることを特徴とする不正接続監視プログラム。

【0079】

(付記10) ネットワークの構築に使用するスイッチに他端が接続するケーブルの接続に

使用される第1のコネクタおよび該スイッチを介してネットワークを利用する利用装置に他端が接続するケーブルの接続に使用される施錠可能な第2のコネクタを有するポート監視装置から該第1のコネクタのスイッチとの接続状態および第2のコネクタの施錠状態に関する情報を受信する状態情報受信手段と、

前記状態情報受信手段により受信した状態情報が、前記接続状態が閉であり、かつ施錠状態が閉であることを示している場合に、前記スイッチが不正使用されていると判定する不正使用判定手段と、

を備えたことを特徴とする不正接続監視装置。

【産業上の利用可能性】

【0080】

以上のように、本発明に係るポート監視装置およびポート監視方法は、ネットワーク装置に有用であり、特に、高度なセキュリティ管理を必要とし、ユーザ端末の接続変更が頻繁に発生するネットワークで使用されるネットワーク装置に適している。

【図面の簡単な説明】

【0081】

【図1】本実施例に係るポート監視装置のポートロック機構を説明するための説明図である。

【図2】本実施例に係るポート監視システムのシステム構成を示す機能ブロック図である。

【図3】使用状態認識部によるスイッチの各ポートの使用状態認識方法を示す図である。

【図4】本実施例に係るポート監視システムのポート状態監視処理の処理手順を示すフローチャートである。

【図5】本実施例に係る不正接続監視プログラムを実行するコンピュータの構成を示す機能ブロック図である。

【符号の説明】

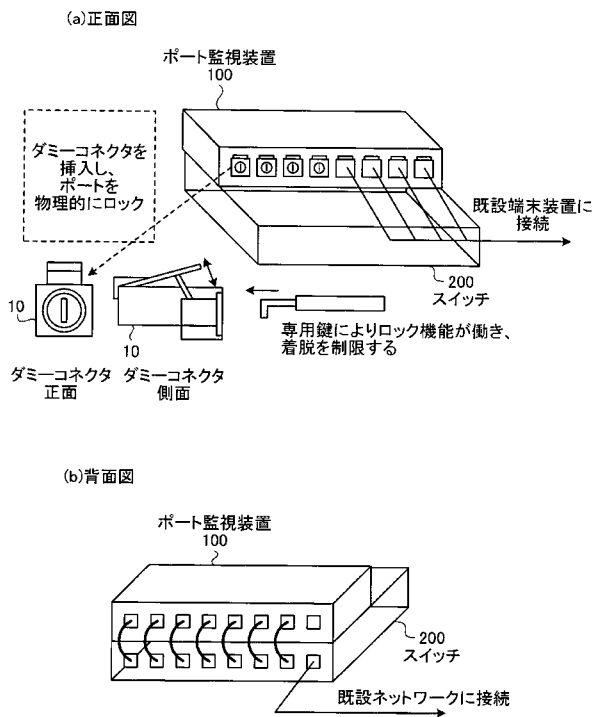
【0082】

10	ダミーコネクタ	
20	イーサネット(登録商標)ケーブル	
30	イーサネット(登録商標)ケーブル	
100	ポート監視装置	30
110	コネクタ	
120	コネクタ	
130	鍵検出部	
140	ポート監視部	
150	切断部	
160	収集/通知部	
170	遠隔指示受信部	
200	スイッチ	
300	不正接続監視装置	
310	状態情報受信部	40
320	使用状態認識部	
330	表示部	
340	指示部	
400	コンピュータ	
410	RAM	
411	不正接続監視プログラム	
420	CPU	
421	不正接続監視プロセス	
430	HDD	
440	LANインタフェース	50

- 450 入出インタフェース
- 460 DVDドライブ

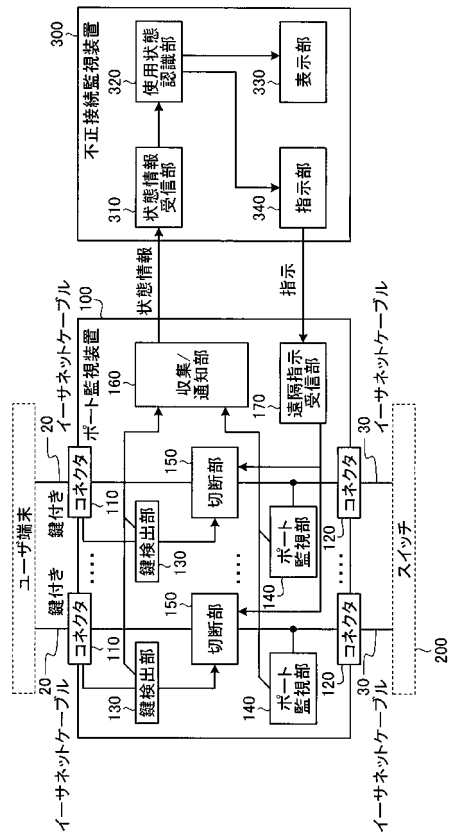
【 図 1 】

本実施例に係るポート監視装置のポートロック機構を説明するための説明図



【 図 2 】

本実施例に係るポート監視システムのシステム構成を示す機能ブロック図



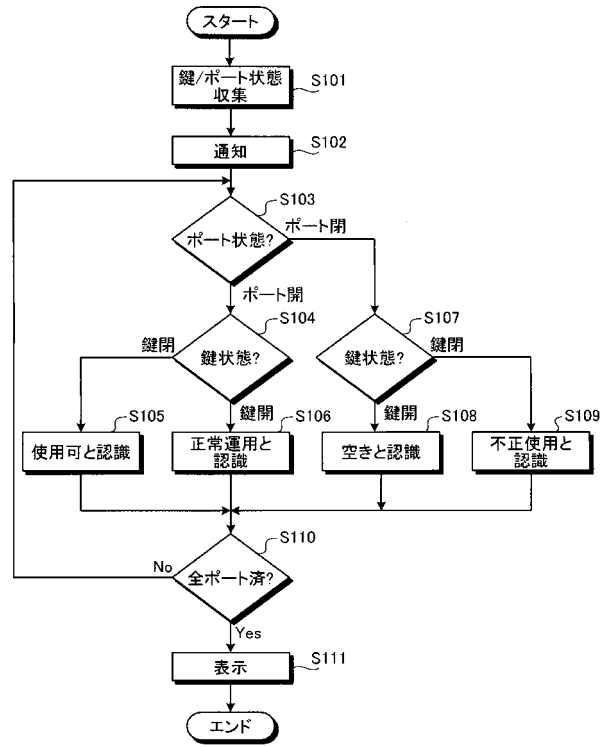
【 図 3 】

使用状態認識部によるスイッチの各ポートの使用状態認識方法を示す図

	鍵閉	鍵閉
ポート生	正常運用	使用可
ポート死	空き	不正使用

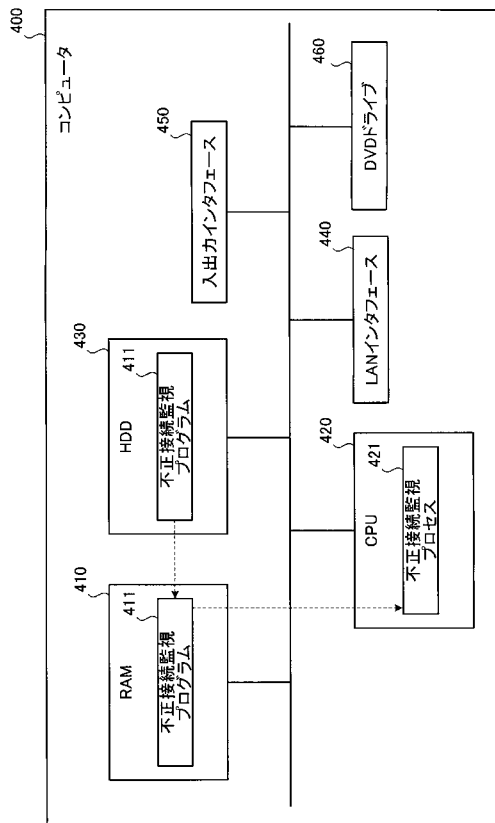
【 図 4 】

本実施例に係るポート監視システムのポート状態監視処理の処理手順を示すフローチャート



【 図 5 】

本実施例に係る不正接続監視プログラムを実行するコンピュータの構成を示す機能ブロック図



フロントページの続き

(72)発明者 三輪 稔則

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

Fターム(参考) 5K033 AA05 BA08 CC01 DA01 DA05 DB03 DB20 EA07