(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6844364号
(P6844364)

(45)発行日　令和3年3月17日(2021.3.17)　(24)登録日　令和3年3月1日(2021.3.1)

(51)Int.Cl.		F I		
H04N 1/00	(2006.01)	H04N	1/00	C
G06F 21/44	(2013.01)	G06F	21/44	
B41J 29/38	(2006.01)	B41J	29/38	

請求項の数 5　(全 17 頁)

(21)出願番号　特願2017-58777(P2017-58777)
(22)出願日　平成29年3月24日(2017.3.24)
(65)公開番号　特開2018-164131(P2018-164131A)
(43)公開日　平成30年10月18日(2018.10.18)
審査請求日　令和2年2月18日(2020.2.18)

(73)特許権者　000005496
富士ゼロックス株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　100104880
弁理士　古部　次郎
(74)代理人　100125346
弁理士　尾形　文雄
(74)代理人　100166981
弁理士　砂田　岳彦
(72)発明者　西　栄治
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックス株式会社内
(72)発明者　坂倉　啓太
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックス株式会社内
最終頁に続く

(54)【発明の名称】端末管理装置、端末管理システムおよびプログラム

(57)【特許請求の範囲】
【請求項１】
ネットワークを介して管理対象である端末装置と接続する接続部と、
予め定められた認証情報を用いて前記端末装置の認証を行う認証部と、
前記端末装置との間で、正常な接続が行われない予め定められた特定状態があった場合に、当該端末装置との間のデータ通信を制御する接続制御部と、を備え、
前記接続制御部は、特定の前記端末装置に関して、当該端末装置の動作電圧が低下した一定期間の後に前記特定状態となった場合は、当該端末装置との間のデータ通信を制限せず、当該端末装置の動作電圧が低下した期間を経ることなく当該特定状態となった場合は、当該端末装置との間のデータ通信を制限する
ことを特徴とする、端末管理装置。
【請求項２】
ネットワークを介して管理対象である端末装置と接続する接続部と、
予め定められた認証情報を用いて前記端末装置の認証を行う認証部と、
前記端末装置との間で、正常な接続が行われない予め定められた特定状態があった場合に、当該端末装置との間のデータ通信を制御する接続制御部と、を備え、
前記接続制御部は、特定の前記端末装置に関して、一定期間、当該端末装置から送信される電波の強度が弱くなった後に前記特定状態となった場合は、当該端末装置との間のデータ通信を制限せず、当該端末装置から送信される電波が弱くなった期間を経ることなく当該特定状態となった場合は、当該端末装置との間のデータ通信を制限する

ことを特徴とする、端末管理装置。
【請求項３】
ネットワークを介して管理対象である端末装置と接続するコンピュータを制御するプログラムであって、
前記コンピュータを、
予め定められた認証情報を用いて前記端末装置の認証を行う認証手段と、
前記端末装置との間で、正常な接続が行われない予め定められた特定状態があった場合に、当該端末装置との間のデータ通信を制御する接続制御手段として機能させ、
前記接続制御手段は、特定の前記端末装置に関して、当該端末装置の動作電圧が低下した一定時間の後に前記特定状態となった場合は、当該端末装置との間のデータ通信を制限せず、当該端末装置の動作電圧が低下した期間を経ることなく当該特定状態となった場合は、当該端末装置との間のデータ通信を制限する
ことを特徴とする、プログラム。
【請求項４】
ネットワークを介して管理対象である端末装置と接続するコンピュータを制御するプログラムであって、
前記コンピュータを、
予め定められた認証情報を用いて前記端末装置の認証を行う認証手段と、
前記端末装置との間で、正常な接続が行われない予め定められた特定状態があった場合に、当該端末装置との間のデータ通信を制御する接続制御手段として機能させ、
前記接続制御手段は、特定の前記端末装置に関して、一定期間、当該端末装置から送信される電波の強度が弱くなった後に前記特定状態となった場合は、当該端末装置との間のデータ通信を制限せず、当該端末装置から送信される電波が弱くなった期間を経ることなく当該特定状態となった場合は、当該端末装置との間のデータ通信を制限する
ことを特徴とする、プログラム。
【請求項５】
端末装置と、
ネットワークを介して前記端末装置と接続し、当該端末装置を管理する端末管理装置と、
インターネット上に設けられた接続記録サーバと、を備え、
前記端末装置は、前記ネットワークを介して前記端末管理装置に通信要求を行って、接続が許可されたならばデータ通信を行い、前記ネットワークを介さずにインターネットに接続された場合は、前記接続記録サーバに接続して自装置を特定する情報を送信し、
前記接続記録サーバは、前記端末装置から受信した前記情報と共に当該端末装置との接続履歴を保持し、
前記端末管理装置は、前記ネットワークを介して前記端末装置から通信要求を受け付けると、前記接続記録サーバに当該端末装置との接続履歴の有無を問い合わせ、当該接続履歴がある場合は、当該端末装置とのデータ通信を制限する
ことを特徴とする、端末管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、端末管理装置、端末管理システムおよびプログラムに関する。
【背景技術】
【０００２】
ネットワークを介して複数の装置を接続し、装置間でデータ交換を行う場合、不正な接続を防止するため、装置間で認証が行われる。特許文献１には、盗まれた正規の認証情報を用いて不正な接続を行う、いわゆる「なりすまし」を防止する技術が開示されている。同文献に記載された従来技術では、認証要求に応答して、ユーザＩＤおよびパスワードが入力されたとき、認証が行われるとともに、入力されたユーザＩＤおよびパスワードが、

ユーザパソコンから与えられたか否かの判別がされる。判別の結果、ユーザパソコン以外からユーザＩＤおよびパスワードが与えられたときには、認証用記憶手段に記憶されているメールアドレスに対して、認証を行った旨および受け付けたジョブを報知する。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特開２００６－２７０４１４号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

ネットワークに正規に接続された装置が不正に持ち出された後、改めてネットワークに接続された場合、装置自体は正規の装置であるので、いわゆる「なりすまし」による不正に接続された装置のように検出することができない。

【０００５】

本発明は、ネットワークに正規に接続された装置であって、不正に持ち出された後に改めてネットワークに接続された装置を検出することを目的とする。

【課題を解決するための手段】

【０００６】

本発明の請求項１に係る端末管理装置は、

ネットワークを介して管理対象である端末装置と接続する接続部と、

予め定められた認証情報を用いて前記端末装置の認証を行う認証部と、

前記端末装置との間で、正常な接続が行われない予め定められた特定状態があった場合に、当該端末装置との間のデータ通信を制御する接続制御部と、を備え、

前記接続制御部は、特定の前記端末装置に関して、当該端末装置の動作電圧が低下した一定期間の後に前記特定状態となった場合は、当該端末装置との間のデータ通信を制限せず、当該端末装置の動作電圧が低下した期間を経ることなく当該特定状態となった場合は、当該端末装置との間のデータ通信を制限する

ことを特徴とする、端末管理装置である。

本発明の請求項２に係る端末管理装置は、

ネットワークを介して管理対象である端末装置と接続する接続部と、

予め定められた認証情報を用いて前記端末装置の認証を行う認証部と、

前記端末装置との間で、正常な接続が行われない予め定められた特定状態があった場合に、当該端末装置との間のデータ通信を制御する接続制御部と、を備え、

前記接続制御部は、特定の前記端末装置に関して、一定期間、当該端末装置から送信される電波の強度が弱くなった後に前記特定状態となった場合は、当該端末装置との間のデータ通信を制限せず、当該端末装置から送信される電波が弱くなった期間を経ることなく当該特定状態となった場合は、当該端末装置との間のデータ通信を制限する

ことを特徴とする、端末管理装置である。

本発明の請求項３に係るプログラムは、

ネットワークを介して管理対象である端末装置と接続するコンピュータを制御するプログラムであって、

前記コンピュータを、

予め定められた認証情報を用いて前記端末装置の認証を行う認証手段と、

前記端末装置との間で、正常な接続が行われない予め定められた特定状態があった場合に、当該端末装置との間のデータ通信を制御する接続制御手段として機能させ、

前記接続制御手段は、特定の前記端末装置に関して、当該端末装置の動作電圧が低下した一定時間の後に前記特定状態となった場合は、当該端末装置との間のデータ通信を制限せず、当該端末装置の動作電圧が低下した期間を経ることなく当該特定状態となった場合は、当該端末装置との間のデータ通信を制限する

ことを特徴とする、プログラムである。

本発明の請求項４に係るプログラムは、
ネットワークを介して管理対象である端末装置と接続するコンピュータを制御するプログラムであって、
前記コンピュータを、
予め定められた認証情報を用いて前記端末装置の認証を行う認証手段と、
前記端末装置との間で、正常な接続が行われない予め定められた特定状態があった場合に、当該端末装置との間のデータ通信を制御する接続制御手段として機能させ、
前記接続制御手段は、特定の前記端末装置に関して、一定期間、当該端末装置から送信される電波の強度が弱くなった後に前記特定状態となった場合は、当該端末装置との間のデータ通信を制限せず、当該端末装置から送信される電波が弱くなった期間を経ることなく当該特定状態となった場合は、当該端末装置との間のデータ通信を制限する
ことを特徴とする、プログラムである。
本発明の請求項５に係る端末管理システムは、
端末装置と、
ネットワークを介して前記端末装置と接続し、当該端末装置を管理する端末管理装置と、
インターネット上に設けられた接続記録サーバと、を備え、
前記端末装置は、前記ネットワークを介して前記端末管理装置に通信要求を行って、接続が許可されたならばデータ通信を行い、前記ネットワークを介さずにインターネットに接続された場合は、前記接続記録サーバに接続して自装置を特定する情報を送信し、
前記接続記録サーバは、前記端末装置から受信した前記情報と共に当該端末装置との接続履歴を保持し、
前記端末管理装置は、前記ネットワークを介して前記端末装置から通信要求を受け付けると、前記接続記録サーバに当該端末装置との接続履歴の有無を問い合わせ、当該接続履歴がある場合は、当該端末装置とのデータ通信を制限する
ことを特徴とする、端末管理システムである。
【発明の効果】
【０００７】
請求項１の発明によれば、正常な接続が行われない予め定められた特定状態があった端末装置による接続を単に制限する構成と比較して、正常な接続が行われない原因が電池の消耗であると推定される場合に、かかる端末装置の接続制限を緩和することができる。
請求項２の発明によれば、正常な接続が行われない予め定められた特定状態があった端末装置による接続を単に制限する構成と比較して、正常な接続が行われない原因が電池の消耗であると推定される場合に、かかる端末装置の接続制限を緩和することができる。
請求項３の発明によれば、正常な接続が行われない予め定められた特定状態があった端末装置による接続を単に制限する構成と比較して、正常な接続が行われない原因が電池の消耗であると推定される場合に、かかる端末装置の接続制限を緩和することができる。
請求項４の発明によれば、正常な接続が行われない予め定められた特定状態があった端末装置による接続を単に制限する構成と比較して、正常な接続が行われない原因が電池の消耗であると推定される場合に、かかる端末装置の接続制限を緩和することができる。
請求項５の発明によれば、予め定められた認証情報による認証のみに基づいて接続を許可する構成と比較して、端末管理装置の管理下から切り離されてインターネットに接続された後に、端末管理装置に対して再接続しようとする端末装置による接続を制限することができる。
【図面の簡単な説明】
【０００８】
【図１】本実施形態の端末管理システムの全体構成を示す図である。
【図２】管理サーバの一例としての複合機の機能構成を示す図である。
【図３】制御部の機能構成を示す図である。
【図４】端末装置の機能構成を示す図である。

【図５】端末装置と接続する際の管理サーバの動作を示すフローチャートである。
【図６】他の実施形態による端末管理システムの全体構成を示す図である。
【図７】不正接続記録サーバの機能構成を示す図である。
【図８】端末装置の機能構成を示す図である。
【図９】端末装置のネットワーク接続時の動作を示すフローチャートである。
【図１０】端末管理システムにおける管理サーバの動作を示すフローチャートである。
【発明を実施するための形態】
【０００９】
以下、添付図面を参照して、本発明の実施の形態について詳細に説明する。
＜本実施形態が適用されるシステム＞
図１は、本実施形態の端末管理システムの全体構成を示す図である。図１に示す端末管理システム１０は、管理サーバ１００と、管理対象である端末装置２００とを備える。管理サーバ１００と端末装置２００とは、ネットワーク３００を介して接続されている。また、図１では省略しているが、管理サーバ１００自体もネットワーク３００を介して他のサーバ（外部サーバ）に接続するようにしても良い。この場合、管理サーバ１００は、ネットワーク上の他のサーバも含む情報システムにおける、いわゆるエッジサーバとして機能する。
【００１０】
管理サーバ１００は、端末装置２００を管理する端末管理装置の一例であり、例えば、パーソナルコンピュータやサーバマシンの他、通信機能を備えた種々の情報処理装置により実現される。本実施形態では、一例として、複写機能、画像読み取り機能、印刷機能、ＦＡＸ通信機能などを有するとともに、ネットワーク３００に接続するための通信機能を備えた複合機である画像処理装置を管理サーバ１００として用いた場合について説明する。
【００１１】
管理サーバ１００は、端末装置２００を管理し、端末装置２００から情報を受信したり、端末装置２００へ制御命令を送信したりする。管理サーバ１００は、複数の種類のネットワーク回線に接続するために複数のネットワーク・インターフェイスを備える。図１に示す例では、有線通信によりＬＡＮ（Local Area Network）に接続するためのネットワークアダプタ、無線通信によりＬＡＮに接続するためのアクセスポイントとしてのＷｉ－Ｆｉ（登録商標）モジュール、ＦＡＸ通信回線（電話回線）で接続するためのＦＡＸモジュールが設けられている。
【００１２】
端末装置２００は、ネットワーク３００を介して通信を行う通信機能を備えた電子機器である。具体例としては、いわゆるＩｏＴデバイスが挙げられる。端末装置２００は、例えば、情報取得手段としてのセンサを有しており、センサにより得られた情報を、通信機能を用い、ネットワーク３００を介して管理サーバ１００に送信する。また、端末装置２００は、アクチュエータや発光装置等の動作手段を有しており、ネットワーク３００を介して管理サーバ１００から受信する制御命令に従って動作手段を動作させる。
【００１３】
本実施形態では、複数の端末装置２００が管理サーバ１００に管理される構成を想定するが、各端末装置２００の情報取得手段や動作手段は同じ種類のものに限定されず、端末装置２００ごとに種々の情報取得手段や動作手段を有していて良い。また、一つの端末装置２００は、必ずしも情報取得手段と動作手段の両方を有している必要はなく、一方のみを有していても良い。また、一つの端末装置２００は、複数の種類の情報取得手段を有していても良いし、複数の種類の動作手段を有していても良い。また、本実施形態において、端末装置２００は、取得しようとする情報や実施する動作の内容に応じて種々の場所に設置される。そのため、管理サーバ１００と端末装置２００との物理的な位置関係も様々である。
【００１４】

ネットワーク３００は、管理サーバ１００と端末装置２００との間のデータ通信に用いられる通信ネットワークであれば特に限定されず、例えばＬＡＮ、ＷＡＮ（Wide Area Network）、インターネット等として良い。データ通信に用いられる通信回線は、上述したように、有線と無線とを問わず、種々の回線を対象として良い。また、複数のネットワークや通信回線を介して各装置を接続するように構成しても良い。

【００１５】

＜管理サーバの構成＞

図２は、管理サーバ１００の一例としての複合機の機能構成を示す図である。図２に示す構成において、管理サーバ１００は、制御部６０を構成するＣＰＵ（Central Processing Unit）１０２と、ＲＯＭ（Read Only Memory）１０３と、ＲＡＭ（Random Access Memory）１０４とを備える。また、管理サーバ１００は、記憶部１０５と、操作部１０６と、表示部１０７と、画像読み取り部１０８と、画像形成部１０９と、通信部１１０と、画像処理部１１１とを備える。これらの各機能部は、バス１０１に接続され、このバス１０１を介してデータの授受を行う。

【００１６】

操作部１０６は、ユーザ（使用者）の操作を受け付ける。操作部１０６は、例えば、ハードウェアキーにより構成される。また、例えば、押圧された位置に応じた制御信号を出力するタッチセンサにより構成される。タッチセンサと後述の表示部１０７を構成する液晶ディスプレイとを組み合わせたタッチパネルとして構成しても良い。

【００１７】

表示部１０７は、表示手段の一例であり、例えば液晶ディスプレイにより構成される。この表示部１０７は、ＣＰＵ１０２の制御の下、管理サーバ１００に関する情報を表示する。また、表示部１０７は、ユーザが管理サーバ１００を操作する際にユーザが参照するメニュー画面を表示する。すなわち、上記の操作部１０６と表示部１０７とを組み合わせて、管理サーバ１００のユーザインタフェース部として機能する。

【００１８】

画像読み取り部１０８は、いわゆるスキャナ装置により構成され、セットされた原稿上の画像を光学的に読み取り、読み取り画像（画像データ）を生成する。画像の読み取り方式としては、例えば、光源から原稿に照射した光に対する反射光をレンズで縮小してＣＣＤ（Charge Coupled Devices）で受光するＣＣＤ方式や、ＬＥＤ（Light Emitting Diode）光源から原稿に順に照射した光に対する反射光をＣＩＳ（Contact Image Sensor）で受光するＣＩＳ方式が用いられる。

【００１９】

画像形成部１０９は、画像形成手段の一例であり、記録材の一例である用紙に対して、画像形成材を用いて画像データに基づく画像を形成する。記録材に画像を形成する方式としては、例えば、感光体に付着させたトナーを記録材に転写して像を形成する電子写真方式や、インクを記録材上に吐出して像を形成するインクジェット方式等が用いられる。

【００２０】

通信部１１０は、ネットワーク３００を介して端末装置２００に接続するための接続部であり、通信手段に応じたネットワーク・インターフェイスを有している。図示は省略しているが、通信部１１０は、ネットワーク・インターフェイスの例として、ネットワークアダプタ、Ｗｉ－Ｆｉモジュール、ＦＡＸモジュール等が設けられている。また、通信部１１０としては、ＮＦＣ（Near field radio communication）やＢｌｕｅｔｏｏｔｈ（登録商標）等の近距離無線通信により端末装置２００に接続するためのモジュール（図示せず）を設けても良い。

【００２１】

画像処理部１１１は、演算手段であるプロセッサと作業用メモリとを備え、画像データが表す画像に色補正や階調補正等の画像処理を施す。なお、プロセッサとして制御部６０のＣＰＵ１０２を、作業用メモリとして制御部６０のＲＡＭ１０４を、それぞれ兼用しても良い。

【００２２】
記憶部１０５は、記憶手段の一例であり、例えば、ハードディスク装置などの記憶装置により構成される。記憶部１０５は、画像読み取り部１０８にて生成された読み取り画像等の画像データを記憶する。さらに、本実施形態の記憶部１０５は、端末装置２００と接続するための端末情報を記憶する端末情報保持部として機能する。
【００２３】
制御部６０を構成するＣＰＵ１０２、ＲＯＭ１０３およびＲＡＭ１０４において、ＲＯＭ１０３は、ＣＰＵ１０２により実行されるプログラムを記憶する。ＣＰＵ１０２は、ＲＯＭ１０３に記憶されているプログラムを読み出し、ＲＡＭ１０４を作業エリアにして、プログラムを実行する。また、記憶部１０５に格納されたプログラムをＲＡＭ１０４に読み込んで、ＲＡＭ１０４に読み込んだプログラムをＣＰＵ１０２が実行するようにしても良い。ＣＰＵ１０２によりプログラムが実行されることで、上述した管理サーバ１００の各機能部を制御するとともに、以下の各機能を実現する。
【００２４】
ここで、ＣＰＵ１０２によって実行されるプログラムは、磁気記録媒体（磁気ディスクなど）、光記録媒体（光ディスクなど）、半導体メモリなどのコンピュータが読取可能な記録媒体に記憶した状態で、画像形成装置へ提供し得る。また、ＣＰＵ１０２によって実行されるプログラムは、インターネットなどのネットワークを介して画像形成装置に提供するようにしても良い。
【００２５】
＜制御部の機能構成＞
図３は、制御部６０の機能構成を示す図である。制御部６０において、ソフトウェアとハードウェア資源とが協働することにより、図３に示すように、通信処理部６１、認証部６２、特定状態判断部６３、接続制御部６４の各機能を実現する。
【００２６】
通信処理部６１は、後述する認証部６２および接続制御部６４の処理により端末装置２００との間の接続が成立した場合に、その端末装置２００との間でデータの送受信を行う。また、この接続に関する情報（接続対象の端末装置２００の識別情報、接続時間など）を含む接続履歴を記憶部１０５に保存する。
【００２７】
認証部６２は、ネットワーク３００を介して管理サーバ１００に接続された端末装置２００の認証処理を行う。認証処理は、予め定められた認証情報を用いて行われる。認証情報は、例えば記憶部１０５に保持される。認証情報としては、例えば、端末装置２００やそのユーザのＩＤ（識別情報）およびパスワードが用いられる。ＩＤとしては、例えばユーザ名を用いても良い。また、パスワードとしては、ＰＩＮ（Personal Identification Number）コードを用いても良い。また、デジタル証明書を利用した認証を行っても良い。また、２回目以降の接続に対しては、前回の認証成功時に管理サーバ１００から端末装置２００に対して認証トークンを発行し、次回の接続の際にこの認証トークンを用いることで認証処理を代替しても良い。なお、本実施形態は、認証情報の種類や認証方法を限定するものではなく、既存の種々の認証技術を適用して良い。
【００２８】
特定状態判断部６３は、端末装置２００との間の接続履歴に基づき、端末装置２００との間で、正常な接続が行われない予め定められた特定状態があったか否かを判断する。ここで、正常な接続が行われない特定状態の例としては、予め定められた期間、管理サーバ１００とその端末装置２００との間の接続が行われず、その後、接続が再開されるようになった場合とすることができる。例えば、端末装置２００からの通信要求に基づいて接続が成立する通信形態の場合は、端末装置２００から通信要求が一定期間送信されず、その後、再び通信要求が送信されるようになった場合となる。また、管理サーバ１００からの通信要求に端末装置２００が応答することにより接続が成立する通信形態の場合は、管理サーバ１００の通信要求に対して端末装置２００からの応答がない期間が一定期間以上あ

り、その後、再び通信要求に対する応答が返されるようになった場合となる。このような特定状態があった場合の対応措置の詳細については後述する。

【００２９】

接続制御部６４は、特定状態判断部６３により上記の特定状態があったと判断された端末装置２００に対し、接続制御を行う。具体的には、接続制御部６４は、予め定められた条件を満足するまで、その端末装置２００による管理サーバ１００への再度の接続を拒絶する。接続制御の内容は、具体的な端末管理システム１０の仕様等に応じて個別に定め得る。例えば、一度接続を拒否した端末装置２００に対しては、管理サーバ１００への再度の接続を許可しないとしても良い。また、予め定められた期間を経過した後に、管理サーバ１００への再度の接続を許可するようにしても良い。また、認証処理に加えて、予め定められた特定の手続きを行って問題がなかった場合に、管理サーバ１００への再度の接続を許可するようにしても良い。また、改めて認証情報の設定を行った後に、管理サーバ１００への再度の接続を許可するようにしても良い。

【００３０】

本実施形態では、上記のような特定状態があった場合に、該当する端末装置２００が、端末管理システム１０から一時的に取り外されたものとして扱う。また、本実施形態では、端末装置２００としてＩｏＴデバイスを想定しているため、端末管理システム１０から外された端末装置２００は、原則として、不正に取り外されたものとみなす。そして、上述した接続制御部６４の制御により、その端末装置２００の端末管理システム１０（管理サーバ１００）への接続を制限する。ただし、保守等の理由により端末装置２００や管理サーバ１００の電源が切断されたり、ネットワーク３００への接続が断たれたりする場合がある。例えば、端末装置２００の電池が切れて通信を行うことができなくなった場合、正当な保守の目的等により端末装置２００の電源が切断された場合、正当な保守の目的等により管理サーバ１００の電源が切断された場合などである。そこで、特定の条件を定め、この条件を満たす場合には、その端末装置２００を不正に取り外されたのではないものとみなし、接続制御部６４による接続制限の対象から外す。以下、特定の条件について説明する。

【００３１】

＜接続制御部による接続制限を抑制する特定の条件の例＞

まず、端末装置２００の電池が切れたことを原因として上記の特定状態が起こる場合に対する対応について説明する。この場合、電池の消耗度合いは、電圧を計測する等の手段により知ることができる。そこで、例えば、端末装置２００に動作電圧を計測する計測手段を設け、計測した電圧のデータを定期的に管理サーバ１００へ送信する。管理サーバ１００は、受信した電圧のデータに基づき、電圧が低下した一定期間の後に、上述した正常な接続が行われない特定状態があった場合は、端末装置２００における電池の消耗により接続ができなくなったものとして、接続制御部６４による接続制限を行わないこととする。また、端末装置２００に電圧の計測手段を設けず、端末装置２００から送信される電波の強度を管理サーバ１００において計測し、電波が弱くなったり、瞬間的に途切れたりすることが一定期間あった後に、上述した正常な接続が行われない特定状態があった場合は、端末装置２００における電池の消耗により接続ができなくなったものとして、接続制御部６４による接続制限を行わないこととしても良い。

【００３２】

次に、正当な保守等の目的で端末装置２００の電源が切断されたことを原因として上記の特定状態が起こる場合に対する対応について説明する。この場合、端末装置２００の電源を切断する際の作業手順として、特定の操作を行うことを義務づける。そして、この特定の操作が行われた場合に、例えば、特別のコードを端末装置２００から管理サーバ１００へ送信する等の手段により、特定の操作が行われたことを管理サーバ１００に通知するようにする。これにより、管理サーバ１００は、その端末装置２００が正当な目的で意図的に電源を切断されたことを認識する。そして、この場合は、上述した正常な接続が行われない特定状態があっても、接続制御部６４による接続制限を行わないこととする。

【００３３】
次に、正当な保守等の目的で管理サーバ１００の電源が切断されたことを原因として上記の特定状態が起こる場合に対する対応について説明する。この場合、管理サーバ１００側で電源が切断されることにより端末装置２００との接続が行われなくなるだけなので、単に、管理サーバ１００の電源が切断されている間に上述した正常な接続が行われない特定状態があっても、接続制御部６４による接続制限を行わないとしても良い。また、管理サーバ１００の代替装置（図示せず）を用意できる場合は、管理サーバ１００の電源が切断されている間、端末装置２００との通信をこの代替装置で行い、管理サーバ１００が復帰した際に、代替装置による通信履歴を管理サーバ１００が引き継ぐようにしても良い。このようにすれば、上述した正常な接続が行われない特定状態が発生しないため、接続制御部６４による接続制限は行われない。
【００３４】
＜接続制御部による接続制限を解除する特定の手続きの例＞
また、上記において、接続制御部６４による接続制限が行われた後、認証処理に加えて、予め定められた特定の手続きを行って問題がなかった場合に、管理サーバ１００への再度の接続を許可することについて述べた。この場合における特定の手続きの例について説明する。
【００３５】
この特定の手続きの一例として、認証情報とは別に、個々の端末装置２００に固有な複数の情報を用いて端末装置２００の検証を行う。端末装置２００に固有な情報（以下、固有情報）としては、例えば、ＭＡＣ（Media Access Control）アドレス、製品のシリアル番号、各種の設定情報等を用いることができる。また、個体の検証用の特定データをメモリに格納しておき、これを端末装置２００の固有情報として用いても良い。さらに、端末装置２００を動作させるためのファームウェアのデータ（プログラム）自体やファームウェアのチェックサムを端末装置２００の固有情報として用いても良い。具体的な手続きとしては、これらの情報を管理サーバ１００の記憶部１０５に保持しておき、接続制御部６４は、特定状態判断部６３により特定状態があったと判断された端末装置２００から取得したこれらの情報を照合する。
【００３６】
本実施形態において、接続制御部６４は、上記のような端末装置２００に固有な複数の情報を用いて検証を行うことにより、認証情報による認証を経た端末装置２００であっても、特定状態が発生する前の状態と比較して全く変更されていない同一の個体か否かを判断する。また、正当な目的で設定情報の初期化やファームウェアの更新などの操作が行われると、その端末装置２００は、特定状態が発生する前の状態と異なることになる。この場合は、例えば、ＭＡＣアドレス等のように初期化や更新される可能性のない情報の優先度を高くしたり、予め初期化や更新による変更内容の情報を管理サーバ１００に報知したりすることにより、接続制御部６４が、同一の個体が維持されていることを確認することができる。
【００３７】
＜端末装置の構成＞
図４は、端末装置２００の機能構成を示す図である。図４に示すように、端末装置２００は、接続部２０１と、認証情報保持部２０２と、制御部２０３とを備える。接続部２０１は、ネットワーク３００を介して管理サーバ１００と接続するためのネットワーク・インターフェイスを備える。認証情報保持部２０２は、例えば半導体メモリや磁気ディスク等の記憶装置により実現され、管理サーバ１００と接続するための認証処理に用いられる認証情報を保持する。制御部２０３は、端末装置２００が有する各機能の制御を行う。例えば、制御部２０３は、センサにより情報を取得して管理サーバ１００へ送信したり、管理サーバ１００から受信した命令に基づいてアクチュエータ等の動作手段の動作を制御したりする。また、制御部２０３は、端末装置２００と管理サーバ１００との間で通信を行う際に、認証処理に必要となる認証情報を認証情報保持部２０２から読み出して管理サー

バ１００へ送る。さらに、制御部２０３は、管理サーバ１００において上述した特定の手続きとして、端末装置２００の固有情報を用いた検証が行われる場合は、検証に用いられる情報を管理サーバ１００へ送る。

【００３８】

＜管理サーバの動作＞

図５は、端末装置２００と接続する際の管理サーバ１００の動作を示すフローチャートである。ここでは、端末装置２００から通信要求を行って接続する方式とする。図５に示すように、初期的に、管理サーバ１００は、端末装置２００からの通信要求の受信を待っている（Ｓ５０１）。管理サーバ１００が一の端末装置２００（以下、この一の端末装置２００を端末装置Ａと記載する）から通信要求を受信すると（Ｓ５０２）、管理サーバ１００の認証部６２が、端末装置Ａの認証情報を受け付けて認証処理を行う（Ｓ５０３）。認証部６２による認証を通過できない場合（Ｓ５０３でＮＧ）、管理サーバ１００は、処理を終了し、再び端末装置２００からの通信要求を待つ状態へ移行する（Ｓ５０１）。

【００３９】

認証部６２による認証を通過した場合（Ｓ５０３でＯＫ）、次に管理サーバ１００の接続制御部６４が、端末装置Ａが正当な目的で端末管理システム１０から取り外された後に再接続されたことを示す特定の条件を満たすか否かを判定する（Ｓ５０４）。端末装置Ａがこの特定の条件を満たす場合（Ｓ５０４でＹｅｓ）、接続制御部６４は、端末装置Ａの接続を許可し（Ｓ５０９）、通信処理部６１が、端末装置Ａとの通信を実行する（Ｓ５１０）。そして、この通信処理におけるデータの送受信が終了した後、通信処理部６１は、端末装置Ａとの通信を切断する（Ｓ５１１）。また、通信処理部６１は、今回の通信に関する接続履歴を記憶部１０５に保存し、端末装置２００からの通信要求を待つ状態へ移行する（Ｓ５０１）。

【００４０】

一方、端末装置Ａが上記の特定の条件を満たさない場合（Ｓ５０４でＮｏ）、接続制御部６４は、記憶部１０５に保持されている各端末装置２００との接続履歴から、端末装置Ａとの接続履歴を検索する（Ｓ５０５）。そして、端末装置Ａとの接続履歴が検出されない場合（Ｓ５０６でＮｏ）、端末装置Ａは管理サーバ１００に対する最初の接続であるので、接続制御部６４は、端末装置Ａの接続を許可する（Ｓ５０９）。これは、管理サーバ１００に対する最初の接続であるために、端末装置Ａは、端末管理システム１０から取り外された後に再接続されたという事態が起こり得ないためである。接続制御部６４により端末装置Ａの接続が認証された後は、通信処理部６１が、端末装置Ａとの通信を実行する（Ｓ５１０）。そして、この通信処理におけるデータの送受信が終了した後、通信処理部６１は、端末装置Ａとの通信を切断する（Ｓ５１１）。また、通信処理部６１は、今回の通信に関する接続履歴を記憶部１０５に保存し、端末装置２００からの通信要求を待つ状態へ移行する（Ｓ５０１）。

【００４１】

これに対し、端末装置Ａの接続履歴が検出された場合（Ｓ５０６でＹｅｓ）、次に接続制御部６４は、検証に用いる端末装置Ａの固有情報を端末装置Ａから取得する（Ｓ５０７）。取得した情報が接続履歴に記録されている端末装置Ａの固有情報と一致していれば（Ｓ５０８でＹｅｓ）、接続制御部６４は、端末装置Ａの接続を許可し（Ｓ５０９）、通信処理部６１が、端末装置Ａとの通信を実行する（Ｓ５１０）。そして、この通信処理におけるデータの送受信が終了した後、通信処理部６１は、端末装置Ａとの通信を切断する（Ｓ５１１）。また、通信処理部６１は、今回の通信に関する接続履歴を記憶部１０５に保存し、端末装置２００からの通信要求を待つ状態へ移行する（Ｓ５０１）。

【００４２】

また、端末装置Ａから取得した情報が接続履歴に記録されている端末装置Ａの固有情報と一致していない場合（Ｓ５０８でＮｏ）、接続制御部６４は、端末装置Ａの接続を認証せず、管理サーバ１００は、処理を終了し、再び端末装置２００からの通信要求を待つ状態へ移行する（Ｓ５０１）。

【００４３】
なお、上記の動作例では、認証部６２による認証の後に、直ちに、端末装置Ａが正当な目的で端末管理システム１０から取り外された後に再接続されたことを示す特定の条件を満たすか否かを判定することとした（Ｓ５０４参照）。これに対し、まず、特定状態判断部６３により、端末装置Ａが端末管理システム１０から一時的に取り外された後に再接続されたという事態が発生しているか否かを判定し、かかる事態が発生している場合に、それが正当な目的で行われたことを示す特定の条件を満たすか否かを判定しても良い。同様に、上記の動作において、発明の技術思想を逸脱しない範囲で処理手順の変更、追加、削除を行って良く、本実施形態の管理サーバ１００の動作は、図５に示した手順に限定されるものではない。

【００４４】
＜他の実施形態＞
上記の実施形態では、管理サーバ１００に保存された端末装置２００との接続履歴等の情報に基づいて、端末装置２００が端末管理システム１０から一時的に取り外された後に再接続されたか否か、かかる事態が正当な目的で行われたか否かを判定した。一方、端末装置２００が端末管理システム１０から取り外されて別のネットワークに接続された場合に、かかる不正な接続情報を残すようにしても良い。以下、この場合の端末装置２００の構成および動作と、管理サーバ１００の動作とを説明する。

【００４５】
図６は、本実施形態における端末管理システムの全体構成を示す図である。図６に示す端末管理システム２０は、管理サーバ１００と、端末装置２１０と、不正接続記録サーバ４００とを備える。管理サーバ１００と端末装置２１０とは、ネットワーク３００を介して接続されている。図１に示した構成と同様に、管理サーバ１００は、ネットワーク上の他のサーバ（外部サーバ）に接続し、いわゆるエッジサーバとして機能するようにしても良い。図６に示す構成において、管理サーバ１００は、インターネット５００を介して不正接続記録サーバ４００と接続されている。

【００４６】
不正接続記録サーバ４００は、ネットワーク３００ではなくインターネット５００に接続されている。ここで、図１を参照して説明した端末管理システム１０において、ネットワーク３００としてインターネットを用いても良いとしたが、不正接続記録サーバ４００への接続に用いられるネットワークは、管理サーバ１００の管理下にないため、ネットワーク３００とは分けて記載している。不正接続記録サーバ４００は、端末装置２００が管理サーバ１００の管理下から切り離されてインターネット５００に接続された場合に、端末装置２００の接続先となる。

【００４７】
図７は、不正接続記録サーバ４００の機能構成を示す図である。図７に示すように、不正接続記録サーバ４００は、インターネット５００に接続するためのネットワーク・インターフェイスを有する接続部４０１と、インターネット５００を介して管理サーバ１００や端末装置２００と通信を行うための通信制御部４０２と、端末装置２００と通信を行った際の通信履歴を保存する通信履歴記憶部４０３とを備える。

【００４８】
図８は、端末装置２１０の機能構成を示す図である。図８に示す端末装置２１０において、接続部２０１、認証情報保持部２０２および制御部２０３は、図４に示した端末装置２００の各構成と同様であるので、同一の符号を付して説明を省略する。接続先制御部２１１は、接続部２０１がネットワーク（ネットワーク３００またはインターネット５００）に接続されると、接続先のサーバを探索する。具体的には、接続先制御部２１１は、まず管理サーバ１００を探索し、管理サーバ１００に接続できなければ、次に不正接続記録サーバ４００を探索し、接続する。管理サーバ１００および不正接続記録サーバ４００の探索は、例えば、ＩＰ（Internet Protocol）通信において接続先のアドレス（ＩＰアドレス）を変更することにより行われる。

【００４９】
ここで、接続先制御部２１１による接続先の切り替えについて、さらに説明する。端末装置２１０がネットワーク３００ではなくインターネット５００に接続された場合、接続先制御部２１１は、管理サーバ１００に接続できないことを認識して、接続先を管理サーバ１００から不正接続記録サーバ４００へ切り替えることが必要となる。これを実現するため、接続先制御部２１１は、端末装置２１０が管理サーバ１００の管理下における本来の接続環境とは異なる環境でインターネット５００に接続されたことを認識する。
【００５０】
接続環境が本来の環境とは異なることを認識する手法の一例としては、管理サーバ１００に対する通信要求の失敗を利用しても良い。すなわち、管理サーバ１００は、ネットワーク３００を経由しない端末装置２１０からの通信要求は受け付けないので、端末装置２１０から管理サーバ１００への通信要求は、時間切れとなって失敗する。そこで、接続先制御部２１１は、例えば、一定回数連続して通信要求が失敗したならば、接続環境が本来の環境とは異なることを認識し、接続先を不正接続記録サーバ４００に切り替える。
【００５１】
接続環境が本来の環境とは異なることを認識する手法の他の一例としては、ｐｉｎｇコードの送信等により端末装置２１０が接続されたネットワーク上で管理サーバ１００を探索し、管理サーバ１００を検出できない場合に、接続先制御部２１１は、接続環境が本来の環境とは異なることを認識し、接続先を不正接続記録サーバ４００に切り替えるようにしても良い。
【００５２】
接続環境が本来の環境とは異なることを認識する手法のさらに他の一例としては、ネットワーク３００がＤＨＣＰ（Dynamic Host Configuration Protocol）サーバを利用するＩＰネットワーク環境である場合に、ＤＨＣＰサーバから取得するネットワークアドレスに基づいて接続環境を認識しても良い。すなわち、管理サーバ１００と接続できていたときのネットワークアドレスを記憶装置に保持しておき、今回の接続においてＤＨＣＰサーバ（ＩＰｖ４）から取得したネットワークアドレス（ＩＰｖ６（ＤＨＣＰｖ６）の場合はネットワークプレフィックス）が記憶装置に保持しているネットワークアドレスとは異なる場合に、接続先制御部２１１は、接続環境が本来の環境とは異なることを認識し、接続先を不正接続記録サーバ４００に切り替えるようにしても良い。
【００５３】
上記の例では、接続環境が異なることを認識して接続先を切り替えることとしたが、端末装置２１０の物理的な位置（設置場所）が変わったことを認識して（すなわち、本来の設置場所から移動されたことを認識して）、接続先を切り替えるようにしても良い。この場合、例えば端末装置２１０に、ＧＰＳ（Global Positioning System）による測位機能を設け、この情報に基づき端末装置２１０が物理的に移動されたことを認識するようにしても良い。
【００５４】
図９は、端末装置２１０のネットワーク接続時の動作を示すフローチャートである。図９に示すように、端末装置２１０の接続部２０１がネットワークに接続されると（Ｓ９０１）、接続先制御部２１１が、上記のような認識手法を用いて、接続環境が管理サーバ１００の管理下のネットワーク３００か否かを判断する（Ｓ９０２）。そして、接続環境が管理サーバ１００の管理下のネットワーク３００である場合は（Ｓ９０２でＹｅｓ）、接続環境が変更されていないので、制御部２０３が管理サーバ１００に通信要求を行い、認証処理を経て、通信を開始する（Ｓ９０３）。
【００５５】
一方、接続環境が管理サーバ１００の管理下のネットワーク３００でない場合（Ｓ９０２でＮｏ）、接続先制御部２１１は、接続先を管理サーバ１００から不正接続記録サーバ４００に切り替える（Ｓ９０４）。そして、接続先制御部２１１が、不正接続記録サーバ４００に送信要求を行って接続し（Ｓ９０５）、自装置を特定する情報を送信する（Ｓ９

０６）。ここで、自装置を特定する情報としては、例えば、管理サーバ１００に接続する際に用いる認証情報や接続元ＩＰアドレス等が挙げられる。これらの情報は、接続時刻等の接続に関する情報と共に不正接続記録サーバ４００に保存される。

【００５６】

図１０は、端末管理システム２０における管理サーバ１００の動作を示すフローチャートである。図１０には、図５のＳ５０３で認証部６２による認証が行われた後の動作を示している。また、ここでは図５に示す動作の説明において記載した端末装置Ａから通信要求が行われたものとする。

【００５７】

図１０に示すように、認証部６２により認証されると、次に接続制御部６４は、インターネット５００を介して不正接続記録サーバ４００に接続する（Ｓ１００１）。そして、認証部６２による認証に用いられた認証情報を用いて、端末装置Ａの接続履歴を検索する（Ｓ１００２）。端末装置Ａの接続履歴が検出された場合（Ｓ１００３でＹｅｓ）、端末装置Ａが端末管理システム２０から切り離され、インターネット５００に接続されたことを意味するので、接続制御部６４は、端末装置Ａの接続を認証せず、管理サーバ１００は、処理を終了し、再び端末装置２００からの通信要求を待つ状態（図５のＳ５０１）へ移行する。

【００５８】

一方、端末装置Ａの接続履歴が検出されない場合（Ｓ１００３でＮｏ）、接続制御部６４は、図５のＳ５０４に示した、端末装置Ａが正当な目的で端末管理システム１０から取り外された後に再接続されたことを示す特定の条件を満たすか否かの判定に移行する。

【００５９】

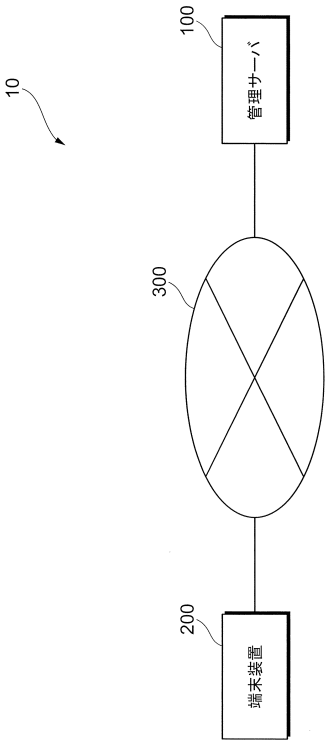
以上のようにして、本実施形態によれば、端末装置２１０が端末管理システム２０から切り離されて他のネットワークに接続された場合に、その不正な接続の情報を取得することができるため、端末装置２１０に対して不正な操作が行われたことを、より直接的に検知することができる。

【符号の説明】

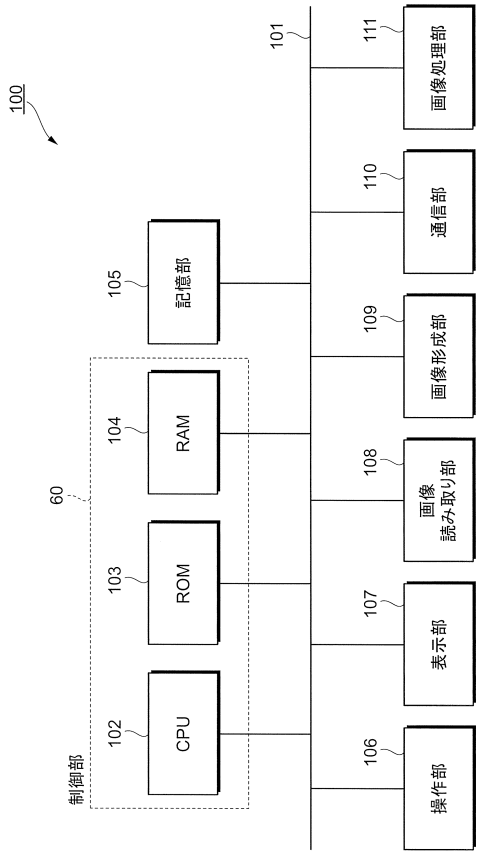
【００６０】

１０、２０…端末管理システム、６０…制御部、６１…通信処理部、６２…認証部、６３…特定状態判断部、６４…接続制御部、１００…管理サーバ、１０１…バス、１０２…ＣＰＵ、１０３…ＲＯＭ、１０４…ＲＡＭ、１０５…記憶部、１０６…操作部、１０７…表示部、１１０…通信部、２００、２１０…端末装置、２０１…接続部、２０２…認証情報保持部、２０３…制御部、２１１…接続先制御部、３００…ネットワーク、４００…不正接続記録サーバ、５００…インターネット

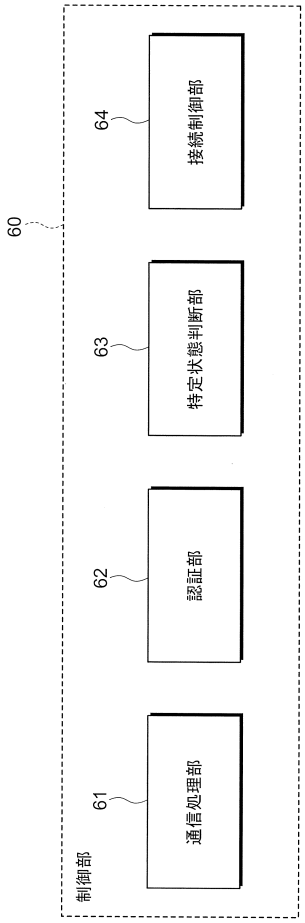
【図１】


10
100
管理サーバ
300
200
端末装置

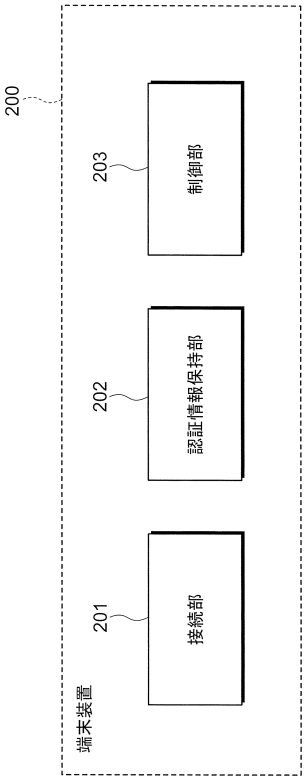
【図２】


100
101
111
画像処理部
110
通信部
109
画像形成部
108
画像
読み取り部
107
表示部
106
操作部
105
記憶部
60
104
RAM
103
ROM
102
CPU
制御部

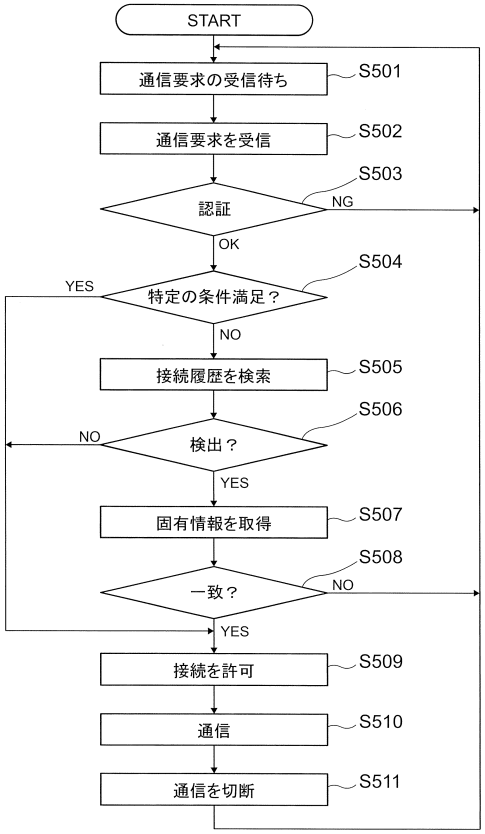
【図３】


60
64
接続制御部
63
特定状態判断部
62
認証部
61
通信処理部
制御部

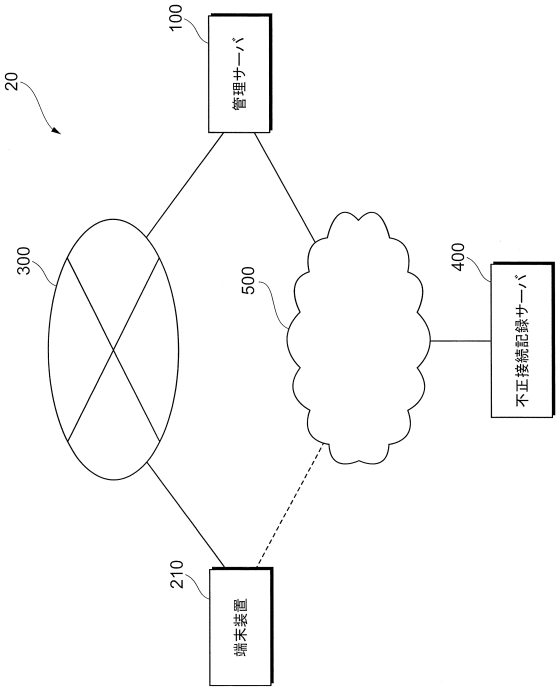
【図４】


200
203
制御部
202
認証情報保持部
201
接続部
端末装置

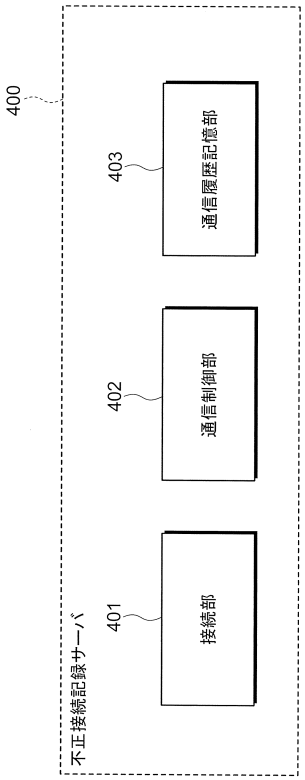
【図５】


START
通信要求の受信待ち
S501
通信要求を受信
S502
認証
S503
NG
OK
特定の条件満足？
S504
YES
NO
接続履歴を検索
S505
検出？
S506
NO
YES
固有情報を取得
S507
一致？
S508
NO
YES
接続を許可
S509
通信
S510
通信を切断
S511

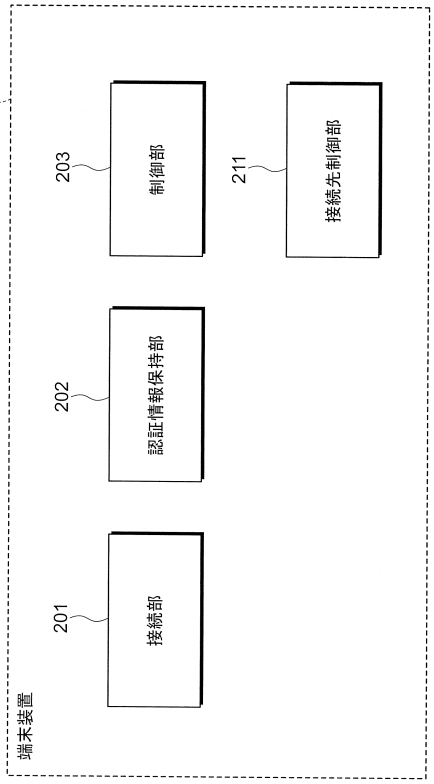
【図６】


20
100
管理サーバ
300
500
400
不正接続記録サーバ
210
端末装置

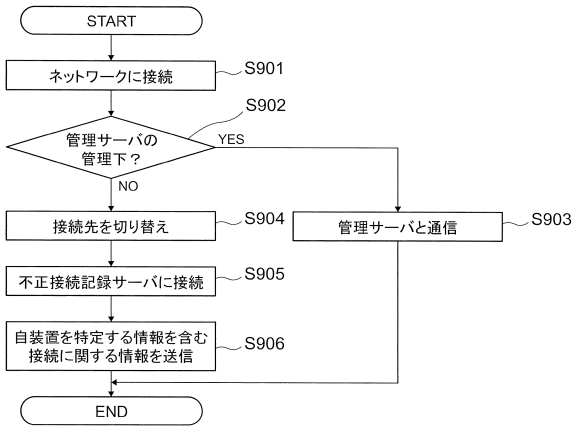
【図７】


400
403
通信履歴記憶部
402
通信制御部
401
接続部
不正接続記録サーバ

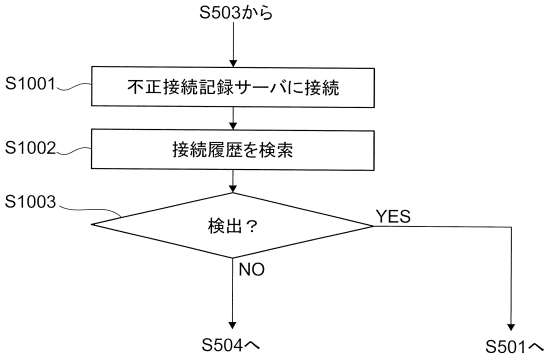
【図８】


210
203
制御部
211
接続先制御部
202
認証情報保持部
201
接続部
端末装置

【図９】


START
ネットワークに接続
S901
S902
管理サーバの
管理下？
YES
NO
接続先を切り替え
S904
管理サーバと通信
S903
不正接続記録サーバに接続
S905
自装置を特定する情報を含む
接続に関する情報を送信
S906
END

【図１０】


S503から
S1001
不正接続記録サーバに接続
S1002
接続履歴を検索
S1003
検出？
YES
NO
S504へ
S501へ

フロントページの続き

(72)発明者　石塚　隆一
東京都港区赤坂九丁目７番３号　富士ゼロックス株式会社内
(72)発明者　関根　義寛
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックス株式会社内
(72)発明者　黒石　健児
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックス株式会社内
(72)発明者　古谷　健
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックス株式会社内
(72)発明者　御厨　洋
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックスアドバンストテクノロジー株式会社内

審査官　野口　俊明

(56)参考文献　特開２００６－３３１００７（ＪＰ，Ａ）
特開平１１－０７５２６２（ＪＰ，Ａ）
特開２０１６－０３１６９３（ＪＰ，Ａ）
特開２００５－１９６５６８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｎ　　１／００
Ｂ４１Ｊ　２９／３８
Ｇ０６Ｆ　２１／４４