

(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2006-92378
(P2006-92378A)

(43) 公開日 平成18年4月6日(2006.4.6)

(51) Int. Cl.	F I	テーマコード (参考)
G06F 13/00 (2006.01)	G06F 13/00 351N	2C061
B41J 29/38 (2006.01)	B41J 29/38 Z	5B021
G06F 3/12 (2006.01)	G06F 3/12 K	5B089
H04N 1/00 (2006.01)	H04N 1/00 106C	5C062

審査請求 未請求 請求項の数 10 O L (全 14 頁)

(21) 出願番号	特願2004-278555 (P2004-278555)	(71) 出願人	000005496 富士ゼロックス株式会社
(22) 出願日	平成16年9月24日 (2004.9.24)		東京都港区赤坂二丁目17番22号
		(74) 代理人	100087343 弁理士 中村 智廣
		(74) 代理人	100082739 弁理士 成瀬 勝夫
		(74) 代理人	100085040 弁理士 小泉 雅裕
		(74) 代理人	100108925 弁理士 青谷 一雄
		(74) 代理人	100110733 弁理士 鳥野 正司

最終頁に続く

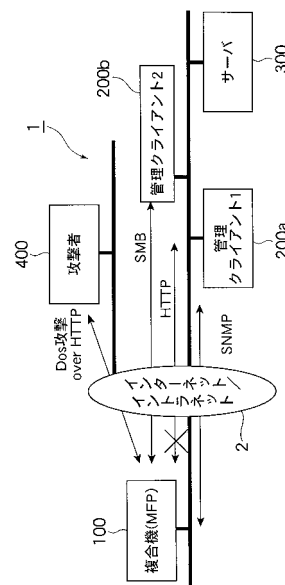
(54) 【発明の名称】 情報処理装置

(57) 【要約】

【課題】 ネットワークを介して管理装置と通信することができ、他の管理装置でリモート管理することが可能な情報処理装置であって、当該情報処理装置がネットワークを介して攻撃を受けて障害などが発生した場合でも、情報処理装置の状態を外部から把握することができ、リモート管理を確実に確保することが可能な情報処理装置を提供する。

【解決手段】 前記管理装置と複数のプロトコルで通信を行うことができ、当該管理装置によってリモート管理するための管理手段と、前記情報処理装置に少なくとも重要な障害が発生したか又は高負荷状態となったか否かを判定する判定手段と、前記管理装置と通信を行う複数のプロトコルの起動順又は起動タイミングの少なくとも一方を変更する変更手段と、前記判定手段の判定結果に基づいて、前記変更手段を制御することにより、前記管理装置と情報処理装置との通信状態を制御する制御手段とを備えるように構成した。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

管理装置とネットワークを介して通信可能であり、前記管理装置によってネットワークを介してリモート管理することが可能な情報処理装置において、

前記管理装置と複数のプロトコルで通信を行うことができ、当該管理装置によってリモート管理するための管理手段と、

前記情報処理装置に少なくとも重要な障害が発生したか又は高負荷状態となったか否かを判定する判定手段と、

前記管理装置と通信を行う複数のプロトコルの起動順又は起動タイミングの少なくとも一方を変更する変更手段と、

前記判定手段の判定結果に基づいて、前記変更手段を制御することにより、前記管理装置と情報処理装置との通信状態を制御する制御手段とを備えたことを特徴とする情報処理装置。

10

【請求項 2】

前記管理装置を特定する特定手段を備えたことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

前記制御手段は、通常使用するプロトコルを起動した後、所定時間、他のプロトコルを起動することを抑制する抑制手段を備えたことを特徴とする請求項 1 又は 2 に記載の情報処理装置。

20

【請求項 4】

前記抑制手段が他のプロトコルを起動することを抑制する時間を変更する変更手段を備えたことを特徴とする請求項 3 に記載の情報処理装置。

【請求項 5】

前記変更手段は、外部の管理装置に設けられており、当該管理装置から前記抑制手段の抑制時間を変更することを特徴とする請求項 4 に記載の情報処理装置。

【請求項 6】

前記抑制手段の抑制時間内に通信されたパケットを記憶する記憶手段を備えたことを特徴とする請求項 3 乃至 5 のいずれかに記載の情報処理装置。

【請求項 7】

前記制御手段は、障害が発生した時、または、高負荷状態になった場合に、リモート管理優先起動モードで起動することを特徴とする請求項 1 乃至 6 のいずれかに記載の情報処理装置。

30

【請求項 8】

前記制御手段は、障害が発生した時、または、高負荷状態になった場合、可能なプロトコルすべてで管理装置に通知することを特徴とする請求項 1 乃至 6 のいずれかに記載の情報処理装置。

【請求項 9】

情報処理装置をネットワークを介してリモート管理するためのリモート管理方法であって、

40

前記管理装置と複数のプロトコルで通信を行い、当該管理装置によってリモート管理するためのステップと、

前記情報処理装置に少なくとも重要な障害が発生したか又は高負荷状態となったか否かを判定するステップと、

前記管理装置と通信を行う複数のプロトコルの起動順又は起動タイミングの少なくとも一方を変更するステップと、

前記判定ステップの判定結果に基づいて、前記変更ステップを制御することにより、前記管理装置と情報処理装置との通信状態を制御するステップとを備えたことを特徴とするリモート管理方法。

【請求項 10】

50

情報処理装置としてコンピュータを動作させるプログラムであって、

管理装置と複数のプロトコルで通信を行うことができ、当該管理装置によってリモート管理するための管理手段、

前記情報処理装置に少なくとも重要な障害が発生したか又は高負荷状態となったか否かを判定する判定手段、

前記管理装置と通信を行う複数のプロトコルの起動順又は起動タイミングの少なくとも一方を変更する変更手段、

前記判定手段の判定結果に基づいて、前記変更手段を制御することにより、前記管理装置と情報処理装置との通信状態を制御する制御手段

としてコンピュータを機能させるプログラム。

10

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、プリンタや複写機、あるいはこれらの機能を兼ね備えた複合機などの情報処理装置に関し、特にネットワークを介して他の管理装置と通信することができ、他の管理装置でリモート管理することが可能な情報処理装置であって、当該情報処理装置がネットワークを介して攻撃を受けて障害などが発生した場合でも、情報処理装置の状態を外部から把握することができ、リモート管理を確実に確保することが可能な情報処理装置に関するものである。

【背景技術】

20

【0002】

【特許文献1】特開平10-301800号公報

【0003】

従来、この種のプリンタや複写機、あるいはこれらの機能を兼ね備えた複合機などの情報処理装置では、オフィス等において、イントラネットを介してパーソナルコンピュータ（PC）等と個別に接続された状態で使用されるのは勿論のこと、インターネット等のネットワークを介してパーソナルコンピュータ（PC）やサーバ等の他の装置と通信可能に構成されてきており、必要に応じて、パーソナルコンピュータ（PC）等からプリンタや複写機、あるいはこれらの機能を兼ね備えた複合機などの情報処理装置の状態をリモート管理したり、所望のソフトウェアをダウンロードしたりすることが可能となってきた

30

【0004】

このようなリモート管理が可能なプリンタや複写機などの情報処理装置において、リモート管理を可能とする技術としては、例えば、特開平10-301800号公報等に開示されたものが、既に提案されている。

【0005】

この特開平10-301800号公報に係る多機能画像処理周辺機器のメンテナンスシステムは、コンピュータと、各種情報が書換え自在に格納されるメモリを備えて前記コンピュータに接続された多機能画像処理周辺機器と、サービス拠点に設けられて、1つ或いは限られた機種に限定された前記多機能画像処理周辺機器に対する複数のメンテナンス内容を記述したスクリプトファイルを作成するファイル作成手段と、このファイル作成手段により作成されたスクリプトファイルを前記サービス拠点から前記コンピュータに提供するファイル提供手段とを備えたシステムであって、前記コンピュータは、前記ファイル提供手段により提供された前記スクリプトファイル中の任意のファイルをダウンロードするダウンロード手段と、メンテナンス用アプリケーションを実行してダウンロードしたスクリプトファイルを前記多機能画像処理周辺機器に転送するメンテナンス用アプリケーション実行手段とを備え、前記多機能画像処理周辺機器は、前記メンテナンス用アプリケーションの実行に伴い転送されたスクリプトファイル中のメンテナンス内容に応じて内部処理を実行するメンテナンス実行手段と、このメンテナンス実行手段による実行結果の良否を前記コンピュータに返送する結果返送手段とを備えるように構成したものである。

40

50

【0006】

かかる特開平10-301800号公報に開示された技術は、コンピュータによって、サービス拠点に設けられたファイル提供手段からスクリプトファイルの提供を受け、当該スクリプトファイルを多機能画像処理周辺機器に転送して、コンピュータに接続されて使用される多機能画像処理周辺機器を、ユーザが離れた場所から簡単にリモートメンテナンスを行うことができるようにしたものである。

【発明の開示】

【発明が解決しようとする課題】

【0007】

しかし、上記従来技術の場合には、次のような問題点を有している。すなわち、上記特開平10-301800号公報に係る多機能画像処理周辺機器のメンテナンスシステムの場合には、多機能画像処理周辺機器が通常の状態であれば問題はないが、当該多機能画像処理周辺機器がネットワークを介してDOS攻撃をされた場合など、多機能画像処理周辺機器に障害が発生すると、多機能画像処理周辺機器とコンピュータとの間で通信自体が困難となり、コンピュータによって多機能画像処理周辺機器の状態を把握することができなくなるといった問題点を有していた。

10

【0008】

そこで、この発明は、上記従来技術の問題点を解決するためになされたものであり、その目的とするところは、ネットワークを介して管理装置と通信することができ、他の管理装置でリモート管理することが可能な情報処理装置であって、当該情報処理装置がネットワークを介して攻撃を受けて障害などが発生した場合でも、情報処理装置の状態を外部から把握することができ、リモート管理を確実に確保することが可能な情報処理装置を提供することにある。

20

【課題を解決するための手段】

【0009】

上記目的を達成するため、請求項1に記載された発明は、管理装置とネットワークを介して通信可能であり、前記管理装置によってネットワークを介してリモート管理することが可能な情報処理装置において、

前記管理装置と複数のプロトコルで通信を行うことができ、当該管理装置によってリモート管理するための管理手段と、

30

前記情報処理装置に少なくとも重要な障害が発生したか又は高負荷状態となったか否かを判定する判定手段と、

前記管理装置と通信を行う複数のプロトコルの起動順又は起動タイミングの少なくとも一方を変更する変更手段と、

前記判定手段の判定結果に基づいて、前記変更手段を制御することにより、前記管理装置と情報処理装置との通信状態を制御する制御手段とを備えたことを特徴とする情報処理装置である。

【0010】

また、請求項2に記載された発明は、前記管理装置を特定する特定手段を備えたことを特徴とする請求項1に記載の情報処理装置である。

40

【0011】

さらに、請求項3に記載された発明は、前記制御手段は、通常使用するプロトコルを起動した後、所定時間、他のプロトコルを起動することを抑制する抑制手段を備えたことを特徴とする請求項1又は2に記載の情報処理装置である。

【0012】

又、請求項4に記載された発明は、前記抑制手段が他のプロトコルを起動することを抑制する時間を変更する変更手段を備えたことを特徴とする請求項3に記載の情報処理装置である。

【0013】

更に、請求項5に記載された発明は、前記変更手段は、外部の管理装置に設けられてお

50

り、当該管理装置から前記抑制手段の抑制時間を変更することを特徴とする請求項 4 に記載の情報処理装置である。

【0014】

また、請求項 6 に記載された発明は、前記抑制手段の抑制時間内に通信されたパケットを記憶する記憶手段を備えたことを特徴とする請求項 3 乃至 5 のいずれかに記載の情報処理装置である。

【0015】

さらに、請求項 7 に記載された発明は、前記制御手段は、障害が発生した時、または、高負荷状態になった場合に、リモート管理優先起動モードで起動することを特徴とする請求項 1 乃至 6 のいずれかに記載の情報処理装置である。

10

【0016】

又、請求項 8 に記載された発明は、前記制御手段は、障害が発生した時、または、高負荷状態になった場合、可能なプロトコルすべてで管理装置に通知することを特徴とする請求項 1 乃至 6 のいずれかに記載の情報処理装置である。

【0017】

更に、請求項 9 に記載された発明は、情報処理装置をネットワークを介してリモート管理するためのリモート管理方法であって、

前記管理装置と複数のプロトコルで通信を行い、当該管理装置によってリモート管理するためのステップと、

前記情報処理装置に少なくとも重要な障害が発生したか又は高負荷状態となったか否かを判定するステップと、

20

前記管理装置と通信を行う複数のプロトコルの起動順又は起動タイミングの少なくとも一方を変更するステップと、

前記判定ステップの判定結果に基づいて、前記変更ステップを制御することにより、前記管理装置と情報処理装置との通信状態を制御するステップとを備えたことを特徴とするリモート管理方法である。

【0018】

また、請求項 10 に記載された発明は、情報処理装置としてコンピュータを動作させるプログラムであって、

管理装置と複数のプロトコルで通信を行うことができ、当該管理装置によってリモート管理するための管理手段、

30

前記情報処理装置に少なくとも重要な障害が発生したか又は高負荷状態となったか否かを判定する判定手段、

前記管理装置と通信を行う複数のプロトコルの起動順又は起動タイミングの少なくとも一方を変更する変更手段、

前記判定手段の判定結果に基づいて、前記変更手段を制御することにより、前記管理装置と情報処理装置との通信状態を制御する制御手段としてコンピュータを機能させるプログラムである。

【発明の効果】

【0019】

40

この発明によれば、ネットワークを介して管理装置と通信することができ、他の管理装置でリモート管理することが可能な情報処理装置であって、当該情報処理装置がネットワークを介して攻撃を受けて障害などが発生した場合でも、情報処理装置の状態を外部から把握することができ、リモート管理を確実に確保することが可能な情報処理装置を提供することができる。

【発明を実施するための最良の形態】

【0020】

以下に、この発明の実施の形態について図面を参照して説明する。

【0021】

実施の形態 1

50

図1はこの発明の実施の形態1に係る情報処理装置としての複合機を適用した情報処理システム1を示すものである。上記複合機100は、図1に示すように、プリンタや複写機等の機能を兼ね備えたものであり、インターネットやイントラネット等のネットワーク2を介して管理装置としての管理クライアント200と通信可能に構成されている。

【0022】

この情報処理システム1は、図1に示すように、複合機100及び管理クライアントとしてのパーソナルコンピュータ(PC)200a、パーソナルコンピュータ(PC)200a、並びにサーバ300が接続されたオフィス等のイントラネットやインターネット等からなるネットワーク2とを備えている。

【0023】

上記サーバ300は、複合機100に提供するソフトウェアを格納したものであり、複合機100は、必要に応じて当該ソフトウェアをダウンロードすることが可能となっている。パーソナルコンピュータ(PC)200a、200bは、複合機100をリモート管理するものであって、ネットワーク2に接続されており、複合機100に対して印刷指示を行ったり、オフィス内の管理者が複合機100を管理することに使用される。

【0024】

ところで、この実施の形態では、管理装置とネットワークを介して通信可能であり、前記管理装置によってネットワークを介してリモート管理することが可能な情報処理装置において、前記管理装置と複数のプロトコルで通信を行うことができ、当該管理装置によってリモート管理するための管理手段と、前記情報処理装置に少なくとも重要な傷害が発生したか又は高負荷状態となったか否かを判定する判定手段と、前記管理装置と通信を行う複数のプロトコルの起動順又は起動タイミングの少なくとも一方を変更する変更手段と、前記判定手段の判定結果に基づいて、前記変更手段を制御することにより、前記管理装置と情報処理装置との通信状態を制御する制御手段とを備えるように構成されている。

【0025】

また、この実施の形態では、前記管理装置を特定する特定手段を備えるように構成されている。

【0026】

さらに、この実施の形態では、前記制御手段は、通常使用するプロトコルを起動した後、所定時間、他のプロトコルを起動することを抑制する抑制手段を備えるように構成されている。

【0027】

又、この実施の形態では、前記抑制手段が他のプロトコルを起動することを抑制する時間を変更する変更手段を備えるように構成されている。

【0028】

更に、この実施の形態では、前記変更手段は、外部の管理装置に設けられており、当該管理装置から前記抑制手段の抑制時間を変更するように構成されている。

【0029】

また、この実施の形態では、前記抑制手段の抑制時間内に通信されたパケットを記憶する記憶手段を備えるように構成されている。

【0030】

さらに、この実施の形態では、前記制御手段は、障害が発生した時、または、高負荷状態になった場合に、リモート管理優先起動モードで起動するか、あるいは可能なプロトコルすべてで管理装置に通知するように構成されている。

【0031】

本実施の形態に係る情報処理装置としての複合機100は、図2に示すように、CPU101と、ROM102と、RAM103と、ページメモリ104と、NVRAM105と、印刷部106と、U/I(ユーザインタフェース)107と、I/F(外部インタフェース)108と、ハードディスク109とを備えている。

【0032】

10

20

30

40

50

上記CPU101は、当該CPU101を制御するソフトウェアによって、上述した管理手段、判定手段、変更手段、制御手段、特定手段としての機能をも実現するものである。

【0033】

CPU101は、複合機100のROM102と、RAM103と、ページメモリ104と、NVRAM105と、印刷部106と、U/I(ユーザインタフェース)107と、I/F(外部インタフェース)108と、ハードディスク109を司る中央演算処理装置である。本複合機100の各種処理は、このCPU101の制御のもとで行われる。

【0034】

ROM102は、読み取り専用メモリであり、複合機100を制御するソフトウェアのうち、基本的な動作を行うためのソフトウェアが格納されている。このROM102に格納されているソフトウェアは、例えば、電源投入直後の複合機100の各ハードウェアを診断したり、NVRAM105に記憶された制御ソフトウェアを起動するといったソフトウェアなどである。

【0035】

RAM103は、読み書き可能メモリであり、複合機100で動作する各ソフトウェアが作業用として使用するデータ記憶領域である。また、このRAM103は、抑制手段の抑制時間内に通信されたパケットを記憶する記憶手段としても機能するものである。

【0036】

ページメモリ104は、文書データを用紙に印刷可能なデータに変換した結果を記憶する領域である。

【0037】

NVRAM105は、不揮発性RAMであり、複合機100を制御するソフトウェアのほとんどが格納されている。サーバ300からダウンロードした新規のソフトウェアは、当該NVRAM105の所定の領域に格納される。このNVRAM105の記憶領域に記憶されたデータは、複合機の電源を切った後も保持される。

【0038】

印刷部106は、ページメモリ104に格納された印刷可能なデータに基づいて、用紙に印刷する手段である。印刷については公知の技術であるため説明は省略する。

【0039】

U/I107は、ユーザに情報を通知したり、ユーザからの情報を取得するといった手段である。本複合機のU/I107は、液晶モニターとタッチパネルで構成されており、サーバ300にアクセスし、新規ソフトウェアの購入、ダウンロード、サポート情報の閲覧といったさまざまなサービスを、ユーザに簡単に提供することができるものである。

【0040】

I/F108は、外部インタフェースであり、本実施の形態では、イントラネットやインターネット等からなるネットワーク2に接続するためのネットワークインタフェース、赤外線やBluetoothによる無線通信を行うための無線通信インタフェース、ICカード、PCカード、コンパクトフラッシュ(登録商標)、スマートメディア、光磁気ディスクなどといった可搬性媒体とのデータ通信を行うインタフェースなどを備えている。それぞれのインタフェースに関しては既知技術のため、詳細は省略する。

【0041】

また、上記I/F108は、HTTP(Hypertext Transfer Protocol)、SNMP(Simple Network Management Protocol)、SMB(Server Message Block)、NetWare等の複数のプロトコルによって、管理装置としてのパーソナルコンピュータ(PC)200a、200bと通信を行うことができるように構成されている。

【0042】

ハードディスク109は、外部よりI/F108を介して受信した印刷(指示)情報、サーバ300から取得した文書データや、文書データを印刷可能なデータに変換するためのフォントや、複合機100の設定情報、状態情報等を格納しておく記憶媒体である。一

10

20

30

40

50

般に単位当たりのコストがRAMやページメモリに比べて安価なため、RAMやページメモリの補助記憶域としても使用される。

【0043】

上記NVRAM105には、図3に示すように、管理サーバソフト110と、プリントサーバソフト111と、IPP(Internet Printing Protocol)112とが記憶されている。また、上記I/F108は、HTTP、SNMP、SMB、NetWare等の複数のプロトコル113a~113dによって、管理装置としてのパーソナルコンピュータ(PC)200a、200bと通信を行うことができるように構成されている。また、このI/F108は、TCP/IP、NetBEUI、IPX/SPXを使用して、ネットドライバを介して、パーソナルコンピュータ(PC)200と通信を行うように構成されている。

10

【0044】

また、サーバ300は、大容量の記憶装置(図示せず)を備え、各種情報が格納されている。本実施の形態では、特に複合機100のためのソフトウェアが格納されている。また、このサーバ300は、イントラネット又はインターネットのいずれのネットワーク2内のサーバであっても構わない。

【0045】

一方、パーソナルコンピュータ(PC)200は、いわゆるパソコンであり、複合機100に対してプリント要求を行ったり、当該複合機100を管理するための管理装置である。また、パーソナルコンピュータ(PC)200は、オフィス内の管理者が操作し、サーバ300から情報を収集し、複合機100の機能拡張ソフトウェアや、新規ソフトウェア、または、パッチ(不具合修正ソフトウェア)などの情報を得たりすることも可能となるように構成されている。

20

【0046】

以上の構成において、この実施の形態に係る情報処理装置としての複合機では、次のようにして、ネットワークを介して管理装置と通信することができ、他の管理装置でリモート管理することが可能な情報処理装置であって、当該情報処理装置がネットワークを介して攻撃を受けて障害などが発生した場合でも、情報処理装置の状態を外部から把握することができ、リモート管理を確実に確保することが可能となっている。

【0047】

図4は上記複合機における動作を示すフローチャートである。

30

【0048】

本複合機100では、まず、電源が投入されると、CPU101によって、当該CPU101の負荷状態を検知するようになっている(ステップ101)。このCPU101の負荷状態は、当該CPU101に割当てられたタスクの状態等を調べることによって検知される。

【0049】

次に、CPU101は、ネットワーク2を経由した負荷の障害があるか否かを判別し(ステップ102)、ネットワーク2を経由した負荷の障害が発生するまで当該処理を待機する。なお、障害は発生しなければ、通常の処理を実行することは勿論である。そして、ネットワーク2を経由した負荷の障害が発生したことが判別されると、障害が発生しているプロトコルが検知された後(ステップ103)、重要障害か否かが判別される(ステップ104)。ここでは、通常、ネットワーク2を経由した通信がHTTP形式で行われるため、障害が発生しているプロトコルとして、HTTPが検知される。また、重要障害か否かは、例えば、CPU101の負荷の割合を判別し、当該負荷の割合が90~100%と非常に高い場合か否かによって判別したり、障害の発生回数をカウントすることによって、所定回数以上発生した場合には、重要障害と判定される。

40

【0050】

いま、図1及び図5に示すように、ネットワーク2に接続された攻撃者400から、DOS攻撃等によるHTTP形式の攻撃を受けた場合には、従来の複合機100は、CPU

50

101に動作障害が発生したり、当該CPU101の負荷が異常に上昇して、クライアントとしてのパーソナルコンピュータ(PC)200からのHTTP形式による管理要求コマンドや、SNMP形式による管理要求コマンドを受け付けず、パーソナルコンピュータ(PC)200からの管理要求コマンドに対して応答することができなくなる。

【0051】

そこで、CPU101は、重要障害が発生していると判別すると、プロトコル設定をOFFに変更した後(ステップ105)、又重要障害でないと判別した場合は、直ちに、通信プロトコルの起動順を変更するとともに(ステップ106)、起動するまでの所定の時間間隔を決定する(ステップ107)。なお、ここで、通信プロトコルの起動順の変更、又は起動するまでの所定時間の変更のいずれかのみを行っても良い。

10

【0052】

ここで、通信プロトコルの起動順の変更としては、最初に、HTTPが起動されるように設定されていたものを、例えば、図7に示すように、NetWareを1番に起動し、次に、SNMPを起動し、所定時間として30秒待った後、HTTPを起動するように変更する場合が挙げられる。なお、図7の例では、SMBを起動しないように設定されているが、SMBを所定の順番で起動するように構成しても勿論良い。

【0053】

なお、上記の如く通信プロトコルの起動順を変更する場合における起動順の設定は、デフォルトで設定されているが、その後U/I107等によって任意に変更できるように構成されている。

20

【0054】

その後、CPU101は、他のプロトコルが動作可能か否かを判別し(ステップ108)、他のプロトコルが動作可能である場合には、他のプロトコルで障害をパーソナルコンピュータ(PC)200に通知した後(ステップ109)、又他のプロトコルが動作可能でない場合には、直ちに、再起動して動作を終了する(ステップ110)。

【0055】

上記他のプロトコルとしては、図5に示すように、例えば、NetWareが挙げられる。

【0056】

また、CPU101は、障害が発生した時、または、高負荷状態になった場合に、リモート管理優先起動モードで起動するように構成される。

30

【0057】

さらに、CPU101は、障害が発生した時、または、高負荷状態になった場合、可能なプロトコルすべてで管理装置としてのパーソナルコンピュータ(PC)200に通知するように構成されている。

【0058】

このように、HTTP攻撃等を受けて、CPU101がパーソナルコンピュータ(PC)200からの管理要求コマンドに対して応答することができなくなった場合には、図6及び図8に示すように、プロトコルの起動順を変えて、HTTP以外のプロトコルを起動したり、所定時間(例えば、30秒)経過してからHTTPを起動するように構成することにより、HTTP攻撃等を受けた場合でも、他のSNMP等のプロトコルを起動して、パーソナルコンピュータ(PC)200に対して、障害発生してHTTPによる管理要求コマンドに対して応答できない旨を、SNMP等のプロトコルによってパーソナルコンピュータ(PC)200に送信することができ、ネットワークを介して管理装置と通信することができ、他の管理装置でリモート管理することが可能な情報処理装置であって、当該情報処理装置がネットワークを介して攻撃を受けて障害などが発生した場合でも、情報処理装置の状態を外部から把握することができ、リモート管理を確実に確保することが可能となっている。

40

【0059】

その際、上記複合機100は、CPU101(特定手段)によって、パーソナルコンピ

50

ユーザ（PC）200a又は200bを特定し、特定されたパーソナルコンピュータ（PC）200a又は200bに対して、障害発生している旨を送信するように構成するのが望ましい。

【0060】

図9は複合機の起動時の動作を示すフローチャートである。

【0061】

複合機100が起動されると、CPU101は、通常行われる初期化処理を実行する（ステップ201）。次に、CPU101は、図7に示すようなプロトコル設定テーブルを読み込んだ後（ステップ202）、初期化（起動）するか否かを判別する（ステップ203）。初期化（起動）しない場合は、全てのプロトコルが完了したか否かを判別し（ステップ209）、全てのプロトコルが完了した場合は、当該動作を終了し、全てのプロトコルが完了していない場合は、ステップ203に戻る。

10

【0062】

また、初期化（起動）する場合は、時間待ちがあるか否かを判別し（ステップ204）、時間待ちがない場合は、プロトコルを初期化（起動）した後（ステップ208）、全てのプロトコルが完了したか否かを判別する（ステップ209）。また、時間待ちがある場合は、所定時間だけ待機した後（ステップ205）、パケット受信するか否かを判別し（ステップ206）、パケット受信する場合は、パケット受信をした後（ステップ207）、又パケット受信しない場合は、直ちに、プロトコルを初期化（起動）して（ステップ208）、全てのプロトコルが完了したか否かを判別する（ステップ209）。なお、パケット受信した内容は、NVRAM105に記憶されるようになっている。

20

【0063】

図10はクライアントとしてのパーソナルコンピュータ（PC）200の動作を示すフローチャートである。

【0064】

まず、ユーザから管理指示があるか否かを判別し（ステップ301）、管理指示がある場合は、管理要求コマンドを複合機100に送信する（ステップ302）。なお、管理指示がない場合は、管理指示がくるまで待機する。

【0065】

パーソナルコンピュータ（PC）200は、所定時間内に応答があるか否かを判別し（ステップ303）、所定時間内に応答があった場合は、応答の内容を表示し（ステップ306）、動作を終了するか否かを判別し（ステップ307）、終了する場合は、当該動作を終了し、終了しない場合は、ステップ301に戻る。

30

【0066】

また、所定時間内に応答がなかった場合は、他のプロトコルで通信が可能か否かを判別し（ステップ304）、他のプロトコルで通信可能な場合は、プロトコルを変更して（ステップ305）、ステップ302に戻る。また、他のプロトコルで通信が不可能な場合は、ステップ307に進み、動作を終了するか否かを判別する（ステップ307）。

【0067】

このように、上記実施の形態では、複合機100に障害が発生し、または、Dos攻撃を受けて通信不可能になることを防止することができる。あるプロトコルを起動すると、障害が発生し、CPUの負荷が高くなると、リモート専用モード時に起動プロトコルを選んだり、設定値を変更したり、セキュリティポリシーを変更したりすることができる。そして、リモート管理を変更できることで、通信性能を維持向上させることが可能となる。

40

【図面の簡単な説明】

【0068】

【図1】図1はこの発明の実施の形態1に係る情報処理装置を適用した情報処理システムを示す構成図である。

【図2】図2はこの発明の実施の形態1に係る情報処理装置としての複合機を示すブロック図である。

50

【図3】図3はこの発明の実施の形態1に係る情報処理装置としての複合機で使用されるソフトウェアやプロトコル等を示す階層図である。

【図4】図4はこの発明の実施の形態1に係る情報処理装置としての複合機の動作を示すフローチャートである。

【図5】図5はこの発明の実施の形態1に係る情報処理装置としての複合機の通信状態を示す説明図である。

【図6】図6はこの発明の実施の形態1に係る情報処理装置としての複合機の通信状態を示す説明図である。

【図7】図7はプロトコル管理テーブルを示す図表である。

【図8】図8はこの発明の実施の形態1に係る情報処理装置としての複合機の通信状態を示す説明図である。

10

【図9】図9はこの発明の実施の形態1に係る情報処理装置としての複合機の動作を示すフローチャートである。

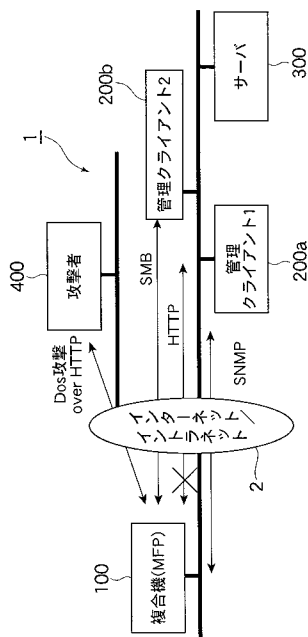
【図10】図10はクライアントの動作を示すフローチャートである。

【符号の説明】

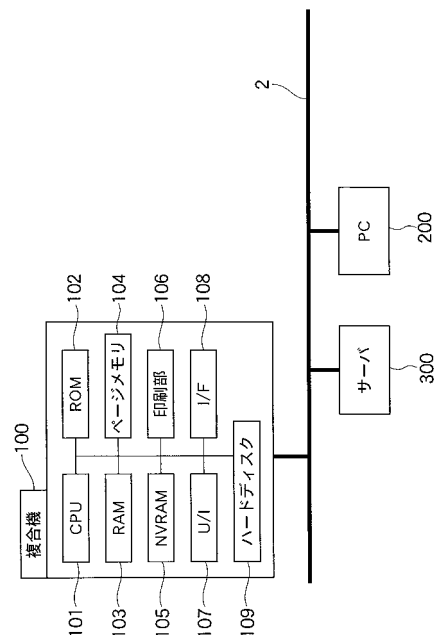
【0069】

100：複合機（情報処理装置）、2：ネットワーク、200：パーソナルコンピュータ（管理装置）。

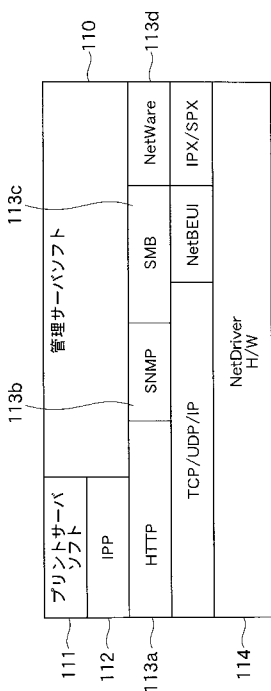
【図1】



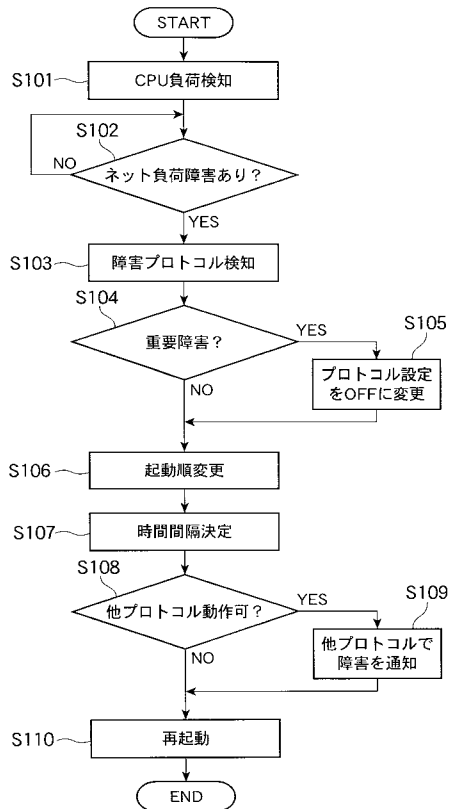
【図2】



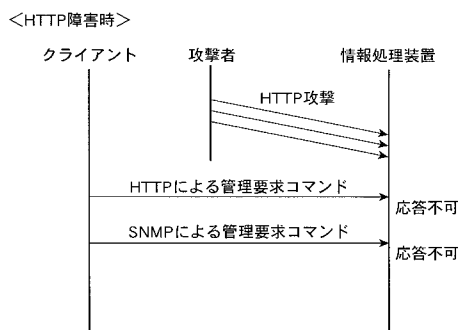
【 図 3 】



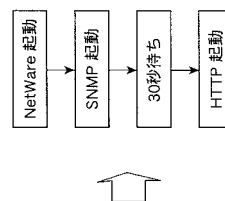
【 図 4 】



【 図 5 】

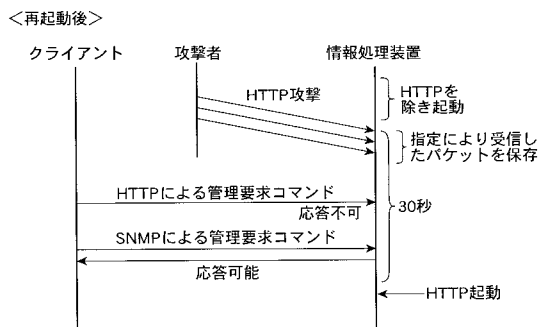


【 図 7 】

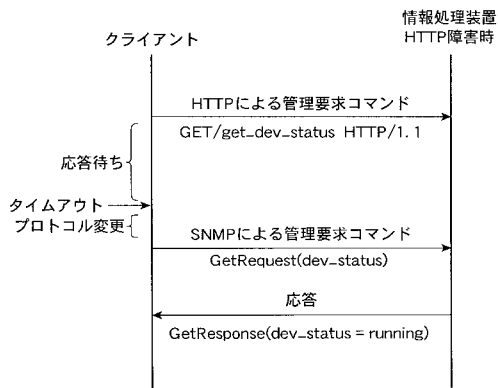


起動順	起動	起動時間	wait	プロトコル名
2	する	0	0	SNMP
1	する	0	0	NetWare
しない	しない	0	0	SMB
3	する	30秒	30秒	HTTP

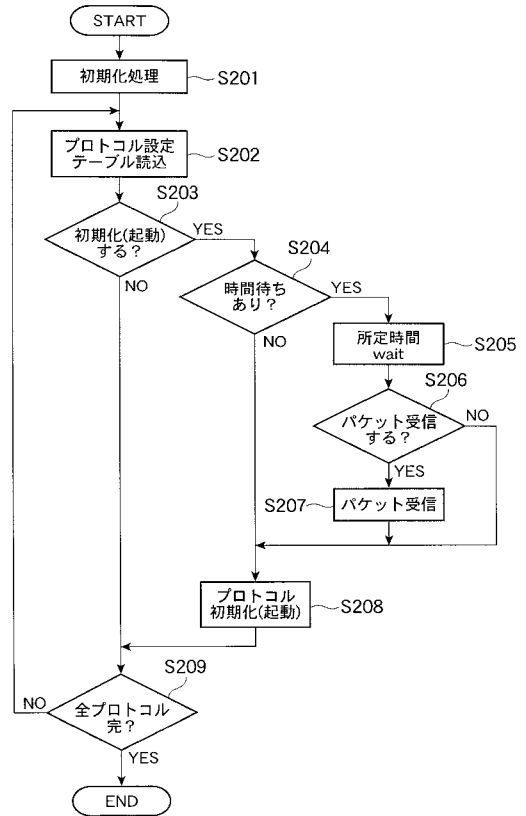
【 図 6 】



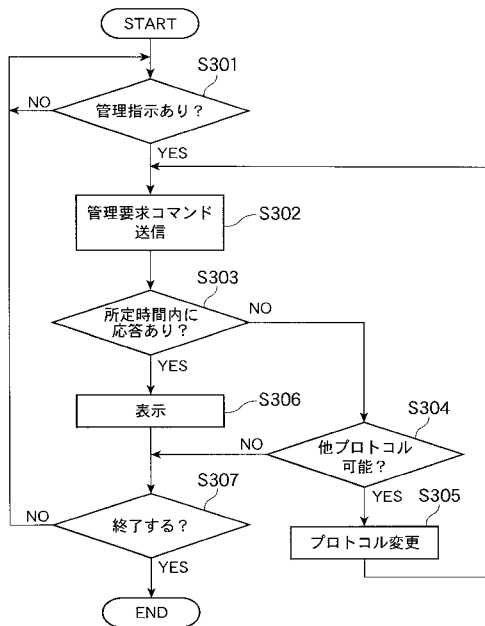
【 図 8 】



【 図 9 】



【 図 10 】



フロントページの続き

(72)発明者 榎本 尚之

神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株式会社内

Fターム(参考) 2C061 AP07 HJ08 HK11 HN15 HQ17 HV02 HV31

5B021 AA01 BB01 BB10 CC04 CC05 EE01 NN19

5B089 JA35 JB14 KA12 KB04 KB11 KC28

5C062 AA02 AA05 AA29 AB38 AC39 AC56 AC58 BA04