(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4855194号
(P4855194)
(45)発行日　平成24年1月18日(2012.1.18)　(24)登録日　平成23年11月4日(2011.11.4)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330A
G06F 21/22 (2006.01)　　G06F 9/06 660N

請求項の数 8　(全 20 頁)

(21)出願番号　特願2006-250204 (P2006-250204)
(22)出願日　平成18年9月15日 (2006.9.15)
(65)公開番号　特開2008-71210 (P2008-71210A)
(43)公開日　平成20年3月27日 (2008.3.27)
審査請求日　平成21年4月14日 (2009.4.14)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(72)発明者　坂倉　隆史
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　小野　良司
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　撫中　達司
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

最終頁に続く

(54)【発明の名称】検疫装置、検疫プログラム及び検疫方法

(57)【特許請求の範囲】
【請求項１】
端末からネットワークへの接続要求を通信装置を介して受信する接続要求受信部と、
検疫処理済の端末及び外部記憶装置を示す検疫処理済情報と、端末及び外部記憶装置を検疫処理した時を示す検疫処理時情報とを記憶装置に記憶する検疫情報記憶部と、
外部記憶装置に接続した記録を示す外部記憶装置接続記録を、上記接続要求受信部が受信した接続要求の送信元端末から通信装置を介して受信する外部記憶装置接続記録受信部と、
上記外部記憶装置接続記録受信部が受信した外部記憶装置接続記録に基づき、上記検疫処理時情報が示す上記送信元端末を検疫処理した時の後、上記送信元端末が外部記憶装置に接続したか否かを処理装置により判定する外部記憶装置接続判定部と、
上記検疫情報記憶部が記憶した検疫処理済情報に基づき、上記送信元端末が外部記憶装置に接続したと上記外部記憶装置接続判定部が判定した場合、上記検疫情報記憶部が記憶した検疫処理済情報に基づき上記送信元端末が接続した外部記憶装置が検疫処理済であるか否かを処理装置により判定する検疫済状況判定部と、
上記送信元端末が外部記憶装置へ接続していないと上記外部記憶装置接続判定部が判定した場合、又は、上記送信元端末が接続した外部記憶装置が検疫処理済であると上記検疫済状況判定部が判定した場合、上記接続要求に対して接続許可の応答をする接続要求応答部と
を備えることを特徴とする検疫装置。

【請求項２】
上記検疫装置は、さらに、
ネットワーク接続した記録を示すネットワーク接続記録を端末から通信装置を介して受信するネットワーク接続記録受信部と、
上記ネットワーク接続記録受信部が受信したネットワーク接続記録に基づき、上記検疫処理時情報が示す上記送信元端末を検疫処理した時の後、上記送信元端末がネットワーク接続したか否かを処理装置により判定するネットワーク接続判定部と
を備え、
上記接続要求応答部は、上記送信元端末が外部記憶装置へ接続していないと上記外部記憶装置接続判定部が判定した場合、又は、上記送信元端末が接続した外部記憶装置が検疫処理済であると上記検疫済状況判定部が判定した場合であって、かつ上記送信元端末がネットワーク接続していないと上記ネットワーク接続判定部が判定した場合、上記接続要求に対して接続許可の応答をする
ことを特徴とする請求項１に記載の検疫装置。
【請求項３】
上記検疫装置は、さらに、
上記送信元端末が外部記憶装置へ接続していたと上記外部記憶装置接続判定部が判定した場合、又は、上記送信元端末が接続した外部記憶装置が検疫処理済でないと上記検疫済状況判定部が判定した場合、上記接続要求受信部が受信した接続要求の送信元端末へ健全性チェック処理の実行指示を通信装置を介して送信する健全性チェック指示部と、
上記健全性チェック指示部が送信した実行指示により上記送信元端末が健全性チェックを実行した結果である健全性チェック結果を通信装置を介して受信する健全性チェック結果受信部とを備え、
上記接続要求応答部は、上記健全性チェック結果受信部が受信した健全性チェック結果に基づき検疫処理を実行し、検疫処理ができた場合上記接続要求に対して接続許可の応答する
ことを特徴とする請求項１記載の検疫装置。
【請求項４】
上記検疫装置は、さらに、
上記送信元端末が接続した外部記憶装置への上記送信元端末以外の端末の接続した記録を示す他端末接続記録を上記送信元端末から通信装置を介して受信する他端末接続記録受信部と、
上記他端末接続記録受信部が受信した他端末接続記録に基づき、上記検疫処理時情報が示す上記外部記憶装置を検疫処理した時の後、上記外部記憶装置への上記送信元端末以外の端末が接続したか否かを処理装置により判定する他端末接続判定部とを備え、
上記接続要求応答部は、上記送信元端末が外部記憶装置へ接続していないと上記外部記憶装置接続判定部が判定した場合、又は、上記送信元端末が接続した外部記憶装置が検疫処理済であると上記検疫済状況判定部が判定し、かつ上記外部記憶装置へ上記送信元端末以外の端末が接続していないと上記他端末接続判定部が判定した場合、上記接続要求に対して接続許可の応答をする
ことを特徴とする請求項１記載の検疫装置。
【請求項５】
上記検疫装置は、さらに、
端末がネットワーク接続中に外部記憶装置に接続した場合に、上記外部記憶装置が検疫処理済でないと上記検疫済状況判定部が判定した場合には、上記端末をネットワークから切断するネットワーク切断部
を備えることを特徴とする請求項４記載の検疫装置。
【請求項６】
上記検疫装置は、さらに、
上記ネットワーク切断部が上記端末をネットワークから切断した場合、上記端末へ健全

性チェック処理の実行指示を通信装置を介して送信する健全性チェック指示部と、
上記健全性チェック指示部が送信した実行指示により上記端末が健全性チェックを実行した結果である健全性チェック結果を通信装置を介して受信する健全性チェック結果受信部とを備え、
上記接続要求応答部は、上記健全性チェック結果受信部が受信した健全性チェック結果に基づき検疫処理を実行し、検疫処理ができた場合上記接続要求に対して接続許可の応答をする
ことを特徴とする請求項５記載の検疫装置。
【請求項７】
端末からネットワークへの接続要求を通信装置を介して受信する接続要求受信処理と、
検疫処理済の端末及び外部記憶装置を示す検疫処理済情報と、端末及び外部記憶装置を検疫処理した時を示す検疫処理時情報とを記憶装置に記憶する検疫情報記憶処理と、
外部記憶装置に接続した記録を示す外部記憶装置接続記録を、上記接続要求受信処理で受信した接続要求の送信元端末から通信装置を介して受信する外部記憶装置接続記録受信処理と、
上記外部記憶装置接続記録受信処理で受信した外部記憶装置接続記録に基づき、上記検疫処理時情報が示す上記送信元端末を検疫処理した時の後、上記送信元端末が外部記憶装置に接続したか否かを処理装置により判定する外部記憶装置接続判定処理と、
上記検疫情報記憶処理で記憶した検疫処理済情報に基づき、上記送信元端末が外部記憶装置に接続したと上記外部記憶装置接続判定処理で判定した場合、上記検疫情報記憶処理で記憶した検疫処理済情報に基づき上記送信元端末が接続した外部記憶装置が検疫処理済であるか否かを処理装置により判定する検疫済状況判定処理と、
上記送信元端末が外部記憶装置へ接続していないと上記外部記憶装置接続判定処理で判定した場合、又は、上記送信元端末が接続した外部記憶装置が検疫処理済であると上記検疫済状況判定処理で判定した場合、上記接続要求に対して接続許可の応答をする接続要求応答処理と
をコンピュータに実行させることを特徴とする検疫プログラム。
【請求項８】
通信装置が、端末からネットワークへの接続要求を受信する接続要求受信ステップと、
記憶装置が、検疫処理済の端末及び外部記憶装置を示す検疫処理済情報と、端末及び外部記憶装置を検疫処理した時を示す検疫処理時情報とを記憶する検疫情報記憶ステップと、
通信装置が、外部記憶装置に接続した記録を示す外部記憶装置接続記録を、上記接続要求受信ステップで受信した接続要求の送信元端末から受信する外部記憶装置接続記録受信ステップと、
処理装置が、上記外部記憶装置接続記録受信ステップで受信した外部記憶装置接続記録に基づき、上記検疫処理時情報が示す上記送信元端末を検疫処理した時の後、上記送信元端末が外部記憶装置に接続したか否かを判定する外部記憶装置接続判定ステップと、
処理装置が、上記検疫情報記憶ステップで記憶した検疫処理済情報に基づき、上記送信元端末が外部記憶装置に接続したと上記外部記憶装置接続判定ステップで判定した場合、上記検疫情報記憶ステップで記憶した検疫処理済情報に基づき上記送信元端末が接続した外部記憶装置が検疫処理済であるか否かを判定する検疫済状況判定ステップと、
処理装置が、上記送信元端末が外部記憶装置へ接続していないと上記外部記憶装置接続判定ステップで判定した場合、又は、上記送信元端末が接続した外部記憶装置が検疫処理済であると上記検疫済状況判定ステップで判定した場合、上記接続要求に対して接続許可の応答をする接続要求応答ステップと
を備えることを特徴とする検疫方法。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、例えば、端末をネットワークへ接続する際等に、端末の健全性を確認する技術に関する。

【背景技術】

【０００２】

インターネットの普及により、その利便性とは裏腹に、いわゆるコンピュータウイルスによる被害が顕在化している。コンピュータウイルスによる被害を防ぐために、端末のコンピュータウイルスを駆除するアンチウイルスソフトが使用されている。アンチウイルスソフトは端末にインストールされる。そして、アンチウイルスソフトは、ウイルスを発見するため、端末のファイルシステムのファイルを全検索したり、電子メールの添付ファイルをチェックしたりする。

また、最近はコンピュータウイルスのみならず、ファイル交換ソフトウェア、ＶＰＮソフトウェア、およびＩＰ電話ソフトウェアによる情報漏えいの課題も顕在化している。これらの課題に対しては、所定の使用禁止ソフトウェアを端末から発見除去している。

また、特許文献１には、無線ネットワークを含めたネットワークのパケットを精査し、コンピュータウイルスの伝播をブロックしコンピュータウイルスの感染を防ぐ技術が開示されている。

【特許文献１】特開平９－２６９９３０号公報

【発明の開示】

【発明が解決しようとする課題】

【０００３】

アンチウイルスソフトの実行や使用禁止ソフトウェアの検索には時間を要する。そこで、ユーザの利便性から、これらの時間の短縮、もしくは排除が望まれている。

本発明は、例えば、アンチウイルスソフトの実行や使用禁止ソフトウェアの検索等の健全性チェックにかかる時間を短縮又は排除することを目的とする。

【課題を解決するための手段】

【０００４】

本発明に係る検疫装置は、例えば、端末からネットワークへの接続要求を通信装置を介して受信する接続要求受信部と、

上記接続要求受信部が受信した接続要求の送信元端末の検疫処理ができた場合に、上記接続要求に対して接続許可の応答をする接続要求応答部と、

検疫処理済の端末を示す検疫処理済情報と端末を検疫処理した時を示す検疫処理時情報とを記憶装置に記憶する検疫情報記憶部と、

上記検疫情報記憶部が記憶した検疫処理済情報に基づき、上記送信元端末が検疫処理済の端末であるか否かを処理装置により判定する検疫済状況判定部と、

上記検疫情報記憶部が記憶した検疫処理時情報が示す上記送信元端末を検疫処理した時の後、上記送信元端末が外部の機器へ接続したか否かを処理装置により判定する外部接続判定部と、

上記送信元端末を検疫処理済の端末であると上記検疫済状況判定部が判定し、かつ上記送信元端末が外部の機器へ接続していないと上記外部接続判定部が判定した場合、接続許可の応答をするように上記接続要求応答部を制御する検疫処理制御部と

を備えることを特徴とする。

【発明の効果】

【０００５】

本発明の係る検疫装置によれば、既に検疫処理済の端末が検疫処理後外部接続していないと外部接続判定部が判定した場合、端末が健全性チェック処理を実行することなくネットワーク接続することが許可される。したがって、本発明に係る検疫装置によれば、アンチウイルスソフトの実行や使用禁止ソフトウェアの検索等の健全性チェックにかかる時間を短縮又は排除することができる。

【発明を実施するための最良の形態】

【０００６】

図１は、実施の形態における検疫システム１０００の外観の一例を示す図である。
図１において、検疫システム１０００は、サーバ９１０、ＰＣ（パーソナルコンピュータ）９０９、ＬＣＤ（液晶）９０１、キーボード９０２（Ｋｅｙ・Ｂｏａｒｄ：Ｋ／Ｂ）、マウス９０３、ＦＤＤ９０４（Ｆｌｅｘｉｂｌｅ・Ｄｉｓｃ・　Ｄｒｉｖｅ）、外部サーバ９１６などのハードウェア資源を備え、これらはケーブルや信号線で接続されている。
サーバ９１０、ＰＣ９０９は、コンピュータであり、ローカルエリアネットワーク９４２（ＬＡＮ）、ゲートウェイ９４１を介してインターネット９４０に接続されている。
ここで、サーバ９１０は、検疫装置１００の一例である。また、ＰＣ９０９は、端末２００（健全性チェック端末）の一例である。

【０００７】
図２は、実施の形態における検疫装置１００、端末２００のハードウェア資源の一例を示す図である。
図２において、検疫装置１００、端末２００は、プログラムを実行するＣＰＵ９１１（Ｃｅｎｔｒａｌ・Ｐｒｏｃｅｓｓｉｎｇ・Ｕｎｉｔ、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう）を備えている。ＣＰＵ９１１は、バス９１２を介してＲＯＭ９１３、ＲＡＭ９１４、通信ボード９１５、ＬＣＤ９０１、キーボード９０２、マウス９０３、ＦＤＤ９０４、磁気ディスク装置９２０と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装置９２０の代わりに、光ディスク装置、メモリカード読み書き装置などの記憶装置９８４でもよい。

【０００８】
ＬＣＤ９０１は、表示装置９８６の一例である。
ＲＡＭ９１４は、揮発性メモリの一例である。ＲＯＭ９１３、ＦＤＤ９０４、ＣＤＤ９０５、磁気ディスク装置９２０の記憶媒体は、不揮発性メモリの一例である。これらは、記憶装置９８４の一例である。
通信ボード９１５、キーボード９０２、ＦＤＤ９０４などは、入力装置９８２の一例である。

【０００９】
通信ボード９１５は、ＬＡＮ９４２等に接続されている。通信ボード９１５は、ＬＡＮ９４２に限らず、インターネット９４０、ＩＳＤＮ等のＷＡＮ（ワイドエリアネットワーク）などに接続されていても構わない。インターネット９４０或いはＩＳＤＮ等のＷＡＮに接続されている場合、ゲートウェイ９４１は不用となる。
磁気ディスク装置９２０又はＲＯＭ９１３などには、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、プログラム群９２３、ファイル群９２４が記憶されている。プログラム群９２３のプログラムは、ＣＰＵ９１１、オペレーティングシステム９２１、ウィンドウシステム９２２により実行される。

【００１０】
上記プログラム群９２３には、以下に述べる実施の形態の説明において「検疫処理部１１０」、「端末処理部２１０」として説明する機能を実行するプログラムが記憶されている。プログラムは、ＣＰＵ９１１により読み出され実行される。
ファイル群９２４には、以下に述べる実施の形態の説明において、「～判定」として説明する情報やデータや信号値や変数値やパラメータが、「ファイル」や「データベース」の各項目として記憶されている。「ファイル」や「データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリになどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してＣＰＵ９１１によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのＣＰＵ９１１の動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示のＣＰＵ９１１の動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。

また、以下に述べる実施の形態の説明において説明するフローチャートの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、ＲＡＭ９１４のメモリ、ＦＤＤ９０４のフレキシブルディスク、コンパクトディスク、磁気ディスク装置９２０の磁気ディスク、その他光ディスク、ミニディスク、ＤＶＤ（Ｄｉｇｉｔａｌ・Ｖｅｒｓａｔｉｌｅ・Ｄｉｓｃ）等の記録媒体に記録される。また、データや信号は、バス９１２や信号線やケーブルその他の伝送媒体によりオンライン伝送される。

【００１１】

また、以下に述べる実施の形態の説明において「～部」として説明するものは、「～回路」、「～装置」、「～機器」、「～手段」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。すなわち、「～部」として説明するものは、ＲＯＭ９１３に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ミニディスク、ＤＶＤ等の記録媒体に記憶される。プログラムはＣＰＵ９１１により読み出され、ＣＰＵ９１１により実行される。すなわち、プログラムは、以下に述べる「～部」としてコンピュータを機能させるものである。あるいは、以下に述べる「～部」の手順や方法をコンピュータに実行させるものである。

【００１２】

実施の形態１.

実施の形態１では、検疫処理済の端末が、検疫処理後外部接続していない場合、改めて健全性チェックを実行することなくネットワーク接続を許可する検疫システム１０００について説明する。

【００１３】

まず、図３に基づき実施の形態１に係る検疫システム１０００の概要について説明する。図３は、実施の形態１に係る検疫システム１０００の構成を示す図である。

検疫システム１０００は、端末２００に対して検疫処理を実行する検疫装置１００と、検疫ネットワークに接続しようとする端末２００（健全性チェック端末）と、ネットワーク接続を制御するスイッチ、ゲートウェイ、無線ＬＡＮ等のアクセスポイント等のオーセンティケータ３０（ネットワーク機器）と、検疫処理で端末２００に異常があった場合に治療を行うリソースを管理する治療サービス３１とを備える。

【００１４】

検疫装置１００は、接続許可判断部１０、インテグリティチェック情報受信部１１、複数の検疫プログラム１２とを備える。接続許可判断部１０は、認証情報のオーセンティケーションサーバとしても動作し、端末２００のネットワークへの接続許可を判断する。インテグリティチェック情報受信部１１は、インテグリティチェック情報を端末２００から受信する。検疫プログラム１２は、端末２００の健全性チェックプログラム２１のチェック結果を検証する。

端末２００は、複数のアプリケーション２０、複数の健全性チェックプログラム２１、インテグリティチェック情報送信部２２、サプリカント２３、耐タンパストレージ使用インターフェース２４、耐タンパストレージライブラリ２５、耐タンパストレージ２６、ディスク領域２７とを備える。アプリケーション２０は、各種ソフトウェアであり、治療サービス３１の治療対象である。健全性チェックプログラム２１は、使用禁止ソフトウェアを検索するチェッカや、ウイルスチェックソフト、ＯＳのパッチバージョンチェッカ等である。インテグリティチェック情報送信部２２は、健全性チェックプログラム２１とインターフェースし、健全性を示す情報であるインテグリティチェック情報を検疫装置１００へ送信する。サプリカント２３は、認証情報を検疫装置１００へ送信する。また、インテグリティチェック情報送信部２２だけでなく、健全性チェックプログラム２１やサプリカント２３によっても検疫装置１００へインテグリティチェック情報の送信は行われる。

耐タンパストレージ使用インターフェース２４、耐タンパストレージライブラリ２５、耐タンパストレージ２６、ディスク領域２７については後述する。

【００１５】

端末２００は、検疫ネットワークへ接続しようとする。端末２００がネットワーク接続する場合の検疫システム１０００の動作は以下のようになる。

（１）端末２００のサプリカント２３は、オーセンティケータ３０へ接続要求を出す。

（２）オーセンティケータ３０は、サプリカント２３から接続要求を受信し、接続決定要求を接続許可判断部１０へ出す。

（３）検疫装置１００の接続許可判断部１０は、オーセンティケータ３０から接続決定要求を受信し、併せてユーザ認証情報、機器認証情報を、オーセンティケータ３０を介してサプリカント２３から受信する。

（４）検疫装置１００の接続許可判断部１０は、端末２００へ健全性チェックの実行を指示する。また、接続許可判断部１０は、インテグリティチェック情報受信部１１へインテグリティチェック情報送信部２２からチェック結果を取得するように指示をする。また、接続許可判断部１０は、検疫プログラム１２へインテグリティチェック情報受信部１１が取得したチェック結果の検証（ｉ）、ユーザ認証（ｉｉ）、機器認証（ｉｉｉ）を行うように指示をする。ここで、ｉ～ｉｉｉの処理が検疫処理である。

（５）端末２００の健全性チェックプログラム２１は、使用禁止ソフトウェアチェック、ウイルスチェック、ＯＳのパッチバージョンチェックを行う。

（６）検疫装置１００のインテグリティチェック情報受信部１１は、インテグリティチェック情報送信部２２からチェックの結果を取得する。

（７）検疫装置１００の検疫プログラム１２は、接続許可判断部１０からユーザ認証情報、機器認証情報を受信し、インテグリティチェック情報受信部１１からチェックの結果を受信する。そして、検疫プログラム１２は、検疫処理を実行する。

（８）

（７）における検証が全てＯＫの場合

検疫装置１００の検疫プログラム１２は、検証が全てＯＫである旨を接続許可判断部１０へ通知する。そして、接続許可判断部１０は、オーセンティケータ３０へ端末２００のネットワークへの接続を許可する。

（７）における検証にＮＧがある場合

検疫装置１００の検疫プログラム１２は、検証にＮＧがある旨を接続許可判断部１０へ通知する。そして、接続許可判断部１０は、オーセンティケータ３０へ検証にＮＧがある旨を通知する。この通知を受けるとオーセンティケータ３０は、端末２００を治療サービス３１に接続する。そして、端末２００は、使用禁止ソフトウェア、ウイルスチェックのパターンファイル、ＯＳのパッチ等の情報を取得し、取得した情報に基づき治療を行う。

治療を行った後、端末２００、オーセンティケータ３０及び検疫装置１００は、上記（５）から再度実行する。

【００１６】

ここで、上記（５）で、端末２００が行う処理は時間を要する。そこで、いかに上記（５）の処理を省略するかが実施の形態１に係る検疫システム１０００の特徴点である。

実施の形態１に係る検疫システム１０００では、端末２００が以前に検疫処理済であり、かつ検疫処理実施後ネットワーク接続及び外部記憶装置への接続がされていない場合、改めて上記（５）の処理を行う必要はないと判断し上記（５）の処理を省略する。ここで、改めて上記（５）の処理を行う必要があるか否かを判定するのは端末２００ではなく検疫装置１００である。つまり、検疫装置１００が改めて上記（５）の処理を行う必要があると判定した場合のみ、上記（５）の処理を実行して新たなチェック結果に基づき接続許可判断部１０の判断を受ける。

【００１７】

次に、図４から図６に基づき上記（５）の処理を省略する機能を備えた検疫システム１０００について説明する。図４は、実施の形態１に係る検疫システム１０００が備える検

疫装置１００の機能を示す機能ブロック図である。図５は、実施の形態１に係る検疫システム１０００が備える端末２００（健全性チェック端末）の機能を示す機能ブロック図である。図６は、実施の形態１に係る検疫システム１０００の動作を示すフローチャートである。

【００１８】

まず、図４に基づき検疫装置１００が備える機能について説明する。

検疫装置１００は、検疫処理部１１０、処理装置９８０、入力装置９８２、記憶装置９８４、表示装置９８６、通信装置９８８を備える。検疫処理部１１０は、例えば、ソフトウェア、プログラム等であり、この場合記憶装置９８４に記憶され処理装置９８０により実行される。検疫処理部１１０は、これに限られず回路等であっても構わない。検疫処理部１１０は、接続許可判断部１０、インテグリティチェック情報受信部１１（健全性チェック結果受信部）、検疫プログラム１２、健全性チェック制御部１３を備える。また、接続許可判断部１０は、接続要求受信部１１２、接続要求応答部１１４、健全性チェック指示部１１６を備える。健全性チェック制御部１３は、検疫情報記憶部１１８、検疫済状況判定部１２０、検疫処理制御部１２２、外部接続判定部１２４を備える。また、外部接続判定部１２４は、ネットワーク接続記録受信部１２６、ネットワーク接続判定部１２８、外部記憶装置接続記録受信部１３０、外部記憶装置接続判定部１３２を備える。

次に、図５に基づき端末２００が備える機能について説明する。

端末２００は、端末処理部２１０、処理装置９８０、入力装置９８２、記憶装置９８４、表示装置９８６、通信装置９８８を備える。端末処理部２１０は、例えば、ソフトウェア、プログラム等であり、この場合記憶装置９８４に記憶され処理装置９８０により実行される。端末処理部２１０は、これに限られず回路等であっても構わない。端末処理部２１０は、アプリケーション２０、健全性チェックプログラム２１（健全性チェック処理実行部）、インテグリティチェック情報送信部２２（健全性チェック結果送信部）、サプリカント２３（接続要求送信部）、指示受信部２１２を備える。

【００１９】

次に、図４から図６に基づき検疫システム１０００の動作について説明する。

以下に説明する処理の前提として、検疫装置１００の検疫情報記憶部１１８は、検疫装置１００が検疫処理を既に行っている検疫処理済の端末２００を示す検疫処理済情報と、端末２００を検疫処理した時を示す検疫処理時情報とを記憶装置９８４に記憶する。また、端末２００は、ネットワークに接続した記録をネットワーク接続記録として、外部記憶装置に接続した記録を外部記憶装置接続記録として記憶装置９８４に記憶する。

【００２０】

まず、接続要求送信処理（Ｓ１０１）では、端末２００のサプリカント２３はネットワークへの接続要求を検疫装置１００へ通信装置９８８を介して送信する。つまり、（Ｓ１０１）は上記（１）（２）の処理に相当する。

次に、接続要求受信処理（Ｓ１０２）では、検疫装置１００の接続要求受信部１１２は、サプリカント２３が送信した接続要求を通信装置９８８を介して受信する。つまり、（Ｓ１０２）は上記（３）の処理に相当する。

【００２１】

次に、端末検疫状況判定処理（Ｓ１０３）では、検疫情報記憶部１１８が記憶装置９８４に記憶した検疫処理済情報に基づき、検疫済状況判定部１２０は接続要求を送信した送信元端末が検疫処理済の端末２００であるか否かを処理装置９８０により判定する。送信元端末が検疫処理済の端末２００であると検疫済状況判定部１２０が判定した場合（Ｓ１０３でＹｅｓ）、ネットワーク接続判定処理（Ｓ１０４）へ進む。一方、送信元端末が検疫処理済の端末２００でないと検疫済状況判定部１２０が判定した場合（Ｓ１０３でＮｏ）、健全性チェック指示処理（Ｓ１０７）へ進む。

次に、ネットワーク接続判定処理（Ｓ１０４）では、ネットワーク接続記録受信部１２６はネットワーク接続記録を送信元端末から通信装置９８８を介して受信する。そして、ネットワーク接続判定部１２８は、ネットワーク接続記録受信部１２６が受信したネット

ワーク接続記録に基づき、検疫情報記憶部１１８が記憶装置９８４に記憶した検疫処理時情報が示す送信元端末を検疫処理した時の後、送信元端末がネットワーク接続したか否かを処理装置９８０により判定する。送信元端末がネットワーク接続したとネットワーク接続判定部１２８が判定した場合（Ｓ１０４でＹｅｓ）、健全性チェック指示処理（Ｓ１０７）へ進む。一方、送信元端末がネットワーク接続していないとネットワーク接続判定部１２８が判定した場合（Ｓ１０４でＮｏ）、外部記憶装置接続判定処理（Ｓ１０５）へ進む。

次に、外部記憶装置接続判定処理（Ｓ１０５）では、外部記憶装置接続記録受信部１３０は、外部記憶装置接続記録を送信元端末から通信装置９８８を介して受信する。そして、外部記憶装置接続判定部１３２は、外部記憶装置接続記録受信部１３０が受信した外部記憶装置接続記録に基づき、検疫情報記憶部１１８が記憶装置９８４に記憶した検疫処理時情報が示す送信元端末を検疫処理した時の後、送信元端末が外部記憶装置に接続したか否かを処理装置９８０により判定する。送信元端末が外部記憶装置に接続したと外部記憶装置接続判定部１３２が判定した場合（Ｓ１０５でＹｅｓ）、健全性チェック指示処理（Ｓ１０７）へ進む。一方、送信元端末が外部記憶装置に接続していないと外部記憶装置接続判定部１３２が判定した場合（Ｓ１０５でＮｏ）、検疫制御処理（Ｓ１０６）へ進む。

ここで、ネットワーク接続判定処理（Ｓ１０４）と外部記憶装置接続判定処理（Ｓ１０５）とは、外部接続判定処理である。

次に、検疫制御処理（Ｓ１０６）では、検疫処理制御部１２２は接続許可の応答をするように接続要求応答部１１４を制御する。そして、接続要求応答処理（Ｓ１１２）へ進む。

【００２２】

一方、健全性チェック指示処理（Ｓ１０７）では、健全性チェック指示部１１６は、送信元端末へ健全性チェック処理の実行指示を通信装置９８８を介して送信する。つまり、（Ｓ１０７）は上記（４）の処理に相当する。

次に、指示受信処理（Ｓ１０８）では、端末２００の指示受信部２１２は、健全性チェック指示部１１６が送信した指示を通信装置９８８を介して受信する。

次に、健全性チェック処理（Ｓ１０９）では、健全性チェックプログラム２１は、送信元端末の記憶装置９８４やアプリケーション２０の健全性チェック処理を処理装置９８０により実行する。つまり、（Ｓ１０９）は上記（５）の処理に相当する。

次に、健全性チェック結果送信処理（Ｓ１１０）では、インテグリティチェック情報送信部２２は、健全性チェックプログラム２１のチェック結果である健全性チェック結果を検疫装置１００へ通信装置９８８を介して送信する。

次に、健全性チェック結果受信処理（Ｓ１１１）では、検疫装置１００のインテグリティチェック情報受信部１１は、インテグリティチェック情報送信部２２が送信した健全性チェック結果を通信装置９８８を介して受信する。つまり、（Ｓ１１０）と（Ｓ１１１）とは上記（６）の処理に相当する。

【００２３】

そして、接続要求応答処理（Ｓ１１２）では、接続要求応答部１１４は、原則として接続要求受信部１１２が受信した接続要求の送信元端末の検疫処理ができた場合、接続要求に対して接続許可の応答をし、検疫処理ができない場合、接続要求に対して接続不許可の応答をする。しかし、検疫制御処理（Ｓ１０６）で、検疫処理制御部１２２に接続許可の応答をするように制御された場合、検疫処理の成否にかかわらず接続要求に対して接続許可の応答をする。つまり、（Ｓ１１２）は上記（７）と（８）との処理に相当する。

【００２４】

つまり、実施の形態１に係る検疫システム１０００は、端末検疫状況判定処理（Ｓ１０３）でＹｅｓと判定され、ネットワーク接続判定処理（Ｓ１０４）と外部記憶装置接続判定処理（Ｓ１０５）とでＮｏと判定された場合、健全性チェック指示処理（Ｓ１０７）から健全性チェック結果受信処理（Ｓ１１１）までの処理を実行しない。すなわち、実施の形態１に係る検疫システム１０００は、端末２００が以前に検疫処理済であり、かつ検疫

処理実施後ネットワーク接続及び外部記憶装置への接続がされていない場合、健全性チェック指示処理（Ｓ１０７）から健全性チェック結果受信処理（Ｓ１１１）までの処理を実行しない。

【００２５】

上記検疫制御処理（Ｓ１０６）で、検疫処理制御部１２２の動作は、健全性チェック処理の実行指示を送信しないように上記健全性チェック指示部を制御するとともに、接続許可の応答をするように接続要求応答部１１４を制御すると言い換えることができる。

【００２６】

また、上記では、端末２００が以前に検疫処理済であり、かつ検疫処理実施後ネットワーク接続及び外部記憶装置への接続がされていない場合、接続要求応答部１１４は接続許可の応答をするとした。しかし、これに限らず、端末２００が以前に検疫処理済であり、かつ検疫処理実施後ネットワーク接続及び外部記憶装置への接続がされていない場合には、以前に実行した健全性チェックのチェック結果により検疫処理を行い、検疫処理ができた場合に接続許可の応答をするとしても構わない。

【００２７】

さらに、端末２００は図３に示す耐タンパストレージ使用インターフェース２４、耐タンパストレージライブラリ２５、耐タンパストレージ２６を備えているものとし、以前に実行した健全性チェックのチェック結果、ネットワーク接続記録、外部記憶装置接続記録等の改ざんを防止する必要がある情報を耐タンパストレージに記憶するとしても構わない。この場合、耐タンパストレージ使用インターフェース２４と耐タンパストレージライブラリ２５と耐タンパストレージ２６とは、アプリケーション２０、健全性チェックプログラム２１、インテグリティチェック情報送信部２２が管理する情報の耐タンパ性を保証するものである。

また、さらに、端末２００は図３に示すディスク領域２７を備えているものとし、資源の限られた耐タンパストレージ２６は暗号キーのみを記憶するとしても構わない。そして、健全性チェックプログラム２１のチェック結果等の耐タンパ性を保証すべき情報はディスク領域２７に記憶し、耐タンパストレージ２６に記憶した暗号キーで暗号化することで改ざんを防止するとしても構わない。

【００２８】

実施の形態１に係る検疫システム１０００によれば、ネットワーク接続や外部記憶装置への接続を行っていない場合には、ウイルスに感染することや使用禁止ソフトウェアのインストールもされていないと判断して、冗長なアンチウイルスソフトや使用禁止ソフトウェアの検査を排除することができる。

【００２９】

実施の形態１をまとめると、検疫済みのネットワークへの接続履歴を取り、該ネットワークに、検疫接続後、再接続する間に外部記憶層の接続、乃至ネットワークに接続していなければ、使用禁止ソフトウェアおよびウイルスチェック実行なしに端末２００からの問い合わせに許可応答することを特徴とするコンピュータ検疫システムである。

【００３０】

実施の形態２.

実施の形態２では、実施の形態１に係る検疫システム１０００の処理に加え、アンチウイルスソフトのパターンファイル等の健全性チェックに使用するリソースに更新があったか否かを判定する検疫システム１０００について説明する。

【００３１】

まず、図７、図８に基づき実施の形態２に係る検疫システム１０００について説明する。

図７は、実施の形態２に係る検疫システム１０００が備える検疫装置１００を示す機能ブロック図である。

実施の形態２に係る検疫システム１０００は、実施の形態１に係る検疫システム１０００と比較して、検疫装置１００の健全性チェック制御部１３がリソース更新判定部１３４

を備える部分のみ異なる。
端末２００は、実施の形態１の端末２００と同様である。
【００３２】
図８は、実施の形態２に係る検疫システム１０００の動作を示すフローチャートである。
（Ｓ２０１）から（Ｓ２０５）までは、実施の形態１に係る（Ｓ１０１）から（Ｓ１０５）までと同様である。但し、外部記憶装置接続判定処理（Ｓ２０５）で送信元端末が外部記憶装置に接続していないと外部記憶装置接続判定部１３２が判定した場合（Ｓ２０５でＮｏ）、リソース更新判定処理（Ｓ２０６）へ進む。
リソース更新判定処理（Ｓ２０６）では、リソース更新判定部１３４は、健全性チェック処理に使用されるリソースが更新されたか否かを処理装置９８０により判定する。リソースが更新されたとリソース更新判定部１３４が判定した場合（Ｓ２０６でＹｅｓ）、健全性チェック指示処理（Ｓ２０８）へ進む。一方、リソースが更新されていないとリソース更新判定部１３４が判定した場合（Ｓ２０６でＮｏ）、検疫制御処理（Ｓ２０７）へ進む。
（Ｓ２０７）から（Ｓ２１３）までは、実施の形態１に係る（Ｓ１０６）から（Ｓ１１２）までと同様である。
【００３３】
つまり、実施の形態２に係る検疫システム１０００では、端末２００が以前に検疫処理済であり、かつ検疫処理実施後ネットワーク接続及び外部記憶装置への接続がされていないことに加え、健全性チェック処理に使用されるリソースが更新されていない場合に、健全性チェック指示処理（Ｓ２０８）から健全性チェック結果受信処理（Ｓ２１２）までの処理を実行しない。
【００３４】
ここで、健全性チェック処理に使用されるリソースとは、例えば、アンチウイルスソフトのパターンファイルや、使用禁止ソフトウェアのリストファイル等である。
つまり、実施の形態２に係る検疫システム１０００は、健全性チェック処理に使用されるリソースが更新されている場合には、以前の健全性チェックで発見できなかったウイルスが発見可能となっている場合や、以前使用禁止でなかったソフトウェアが使用禁止ソフトウェアになっている可能性があると判断し、改めて健全性チェックを行う。このため、実施の形態２に係る検疫システム１０００は、冗長なアンチウイルスソフトや使用禁止ソフトウェアの検査を排除しつつも、実施の形態１に係る検疫システム１０００と比べ安全性を高めている。
【００３５】
実施の形態３.
実施の形態３では、実施の形態２に係る検疫システム１０００の処理に加え、外部記憶装置に接続があった場合に、その外部記憶装置が検疫処理済であるか否かを判定する検疫システム１０００について説明する。
【００３６】
図７、図９に基づき実施の形態３に係る検疫システム１０００について説明する。
実施の形態３に係る検疫システム１０００が備える検疫装置１００と端末２００との機能構成は、実施の形態２に係る検疫システム１０００の機能構成と同様である。
【００３７】
図９は、実施の形態３に係る検疫システム１０００の動作を示すフローチャートである。
以下に説明する処理の前提として、検疫装置１００の検疫情報記憶部１１８は、検疫装置１００が検疫処理を既に行っている検疫処理済の外部記憶装置を示す検疫処理済情報を記憶装置９８４に記憶する。
【００３８】
（Ｓ３０１）から（Ｓ３０５）までは、実施の形態２に係る（Ｓ２０１）から（Ｓ２０

５）までと同様である。但し、外部記憶装置接続判定処理（Ｓ３０５）で送信元端末が外部記憶装置に接続したと外部記憶装置接続判定部１３２が判定した場合（Ｓ３０５でＹｅｓ）、外部記憶装置検疫状況判定処理（Ｓ３０６）へ進む。

外部記憶装置検疫状況判定処理（Ｓ３０６）では、検疫済状況判定部１２０は、検疫情報記憶部１１８が記憶した検疫処理済情報に基づき送信元端末が接続した外部記憶装置が検疫処理済であるか否かを判定する。外部記憶装置が検疫処理済であると検疫済状況判定部１２０が判定した場合（Ｓ３０６でＹｅｓ）、リソース更新判定処理（Ｓ３０７）へ進む。一方、外部記憶装置が検疫処理済でないと検疫済状況判定部１２０が判定した場合（Ｓ３０６でＮｏ）、健全性チェック指示処理（Ｓ３０７）へ進む。

（Ｓ３０７）から（Ｓ３１４）までは、実施の形態２に係る（Ｓ２０６）から（Ｓ２１３）までと同様である。

【００３９】

つまり、実施の形態３に係る検疫システム１０００では、検疫処理実施後に端末２００が外部記憶装置への接続がされている場合であっても、接続先の外部記憶装置が検疫処理済であれば、外部記憶装置に接続されていない場合と同様の扱いをする。すなわち、接続した外部記憶装置が検疫処理済であれば、端末２００が接続した場合であってもウイルスに感染することもなく、使用禁止ソフトウェアがインストールされることもないと判断して、冗長なアンチウイルスソフトや使用禁止ソフトウェアの検査を排除することができる。

【００４０】

実施の形態３をまとめると、外部記憶装置内に、使用禁止ソフトウェアおよびウイルスチェック済み証明が確認される場合は使用禁止ソフトウェアおよびウイルスチェック実行なしに検疫装置１００からのウイルスチェック実行問い合わせに許可応答することを特徴とするコンピュータ検疫システムである。

【００４１】

実施の形態４.

実施の形態４では、実施の形態３に係る検疫システム１０００の処理に加え、接続した外部記憶装置が検疫処理済であった場合に、検疫処理後その外部記憶装置に他の端末２００が接続したか否かを判定する検疫システム１０００について説明する。

【００４２】

まず、図１０、図１１に基づき実施の形態４に係る検疫システム１０００について説明する。

図１０は、実施の形態４に係る検疫システム１０００が備える検疫装置１００を示す機能ブロック図である。

実施の形態４に係る検疫システム１０００は、実施の形態３に係る検疫システム１０００と比較して、検疫装置１００の健全性チェック制御部１３が他端末接続記録受信部１３６、他端末接続判定部１３８を備える部分のみ異なる。

端末２００は、実施の形態３の端末２００と同様である。

【００４３】

図１１は、実施の形態４に係る検疫システム１０００の動作を示すフローチャートである。

以下に説明する処理の前提として、検疫装置１００の検疫情報記憶部１１８は、検疫装置１００が外部記憶装置を検疫処理した時を示す検疫処理時情報を記憶装置９８４に記憶する。

【００４４】

（Ｓ４０１）から（Ｓ４０６）までは、実施の形態３に係る（Ｓ３０１）から（Ｓ３０６）までと同様である。但し、外部記憶装置検疫状況判定処理（Ｓ４０６）で外部記憶装置が検疫処理済であると検疫済状況判定部１２０が判定した場合（Ｓ４０６でＹｅｓ）、他端末接続記録受信処理（Ｓ４０７）へ進む。

他端末接続記録受信処理（Ｓ４０７）では、他端末接続記録受信部１３６は、送信元端

末が接続した外部記憶装置への送信元端末以外の端末２００の接続した記録を示す他端末接続記録を送信元端末から受信する。ここで、他端末接続記録受信部１３６は、直接外部記憶装置から他端末接続記録を受信しても、端末２００を介して取得しても構わない。

次に、他端末接続判定処理（Ｓ４０８）では、他端末接続判定部１３８は、他端末接続記録受信部１３６が受信した他端末接続記録に基づき、検疫処理時情報が示す外部記憶装置を検疫処理した時の後、外部記憶装置への送信元端末以外の端末２００が接続したか否かを判定する。外部記憶装置への送信元端末以外の端末２００が接続したと他端末接続判定部１３８が判定した場合（Ｓ４０８でＹｅｓ）、健全性チェック指示処理（Ｓ４１１）へ進む。一方、外部記憶装置への送信元端末以外の端末２００が接続していないと他端末接続判定部１３８が判定した場合（Ｓ４０８でＮｏ）、リソース更新判定処理（Ｓ４０９）へ進む。

（Ｓ４０９）から（Ｓ４１６）までは、実施の形態３に係る（Ｓ３０７）から（Ｓ３１４）までと同様である。

【００４５】

つまり、実施の形態４に係る検疫システム１０００では、接続先の外部記憶装置が検疫処理済であっても、検疫処理実施後に他の端末２００がその外部記憶装置に接続した場合、その外部記憶装置はウイルスに感染している場合や使用禁止ソフトウェアを記憶している可能性があると判断する。このため、実施の形態４に係る検疫システム１０００は、冗長なアンチウイルスソフトや使用禁止ソフトウェアの検査を排除しつつも、実施の形態３に係る検疫システム１０００と比べ安全性を高めている。

【００４６】

ここで、外部記憶装置から取得する他端末接続記録等が改ざんされている場合、上記処理を行ったとしても安全性を確保できない。そこで、他端末接続記録等の改ざんを防止するため、外部記憶装置に、ＩＣチップ内蔵の耐タンパデバイスに他端末接続記録等を記憶させるとしても構わない。

また、他端末接続記録等の改ざんを防止するため、外部記憶装置に、暗号機能付きＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）に他端末接続記録等を記憶させるとしても構わない。

さらに、他端末接続記録等の改ざんを防止するため、使用禁止ソフトウェアの検索、アンチウイルスソフトの実行プログラム等の各健全性チェックプログラム２１の秘密鍵でインテグリティチェック情報を暗号化して記憶するとしても構わない。つまりこの場合、各健全性チェックプログラム２１が発行する使用禁止ソフトウェアおよびウイルスチェック後のインテグリティを証明する証明書を使用して他端末接続記録等の改ざんを防止する。

【００４７】

実施の形態５.

実施の形態５では、端末２００がネットワーク接続中に外部記憶装置に接続した場合の検疫システム１０００の動作について説明する。

【００４８】

図１２に基づき実施の形態５に係る検疫システム１０００について説明する。図１２は、実施の形態５に係る検疫システム１０００が備える検疫装置１００を示す機能ブロック図である。ここで、端末２００は、実施の形態４の端末２００と同様である。

実施の形態５に係る検疫システム１０００は、実施の形態４に係る検疫システム１０００と比較して、検疫装置１００の健全性チェック制御部１３がネットワーク切断部１４０を備える部分のみ異なる。

ネットワーク切断部１４０は、端末２００がネットワーク接続中に外部記憶装置に接続した場合に、その端末２００をネットワークから切断する。ネットワーク切断部１４０は、端末２００が接続した外部記憶装置が検疫処理済でないと検疫済状況判定部１２０が判定した場合には、端末２００をネットワークから切断し、端末２００が接続した外部記憶装置が検疫処理済であると判定した場合には、ネットワーク接続を維持するとしても構わない。

【００４９】
　また、ネットワーク切断部１４０が端末２００をネットワークから切断した場合、端末２００に改めて健全性チェックをさせ、検疫処理を行い、ネットワークに再接続させるとしても構わない。つまり、ネットワーク切断部１４０が端末２００をネットワークから切断した場合、健全性チェック指示部１１６は、端末２００へ健全性チェック処理の実行指示を通信装置９８８を介して送信する。端末２００は指示を受けると健全性チェックを実行し、インテグリティチェック情報受信部１１は、健全性チェック結果を端末２００から受信する。そして、接続要求応答部１１４は、受信した健全性チェック結果に基づき検疫処理を実行し、検疫処理ができた場合上記接続要求に対して接続許可の応答をし、端末２００はネットワークに再接続するとしても構わない。
【００５０】
　実施の形態５に係る検疫システム１０００は、端末２００がネットワーク接続中に外部記憶装置に接続した場合に、その端末２００をネットワークから切断するため、ネットワーク接続中に端末２００がウイルスに感染し、そのウイルスがネットワーク内に広がることを防止できる。
【００５１】
　実施の形態５をまとめると、検疫完了後コンピュータ使用中に外部記憶装置が接続された場合、上記実施の形態で説明した方法により外部記憶装置の使用禁止ソフトウェアおよびウイルスチェック済み状態が保証されれば、何もせず、該コンピュータの使用継続を許可することを特徴とするコンピュータ検疫システムである。
　また、検疫完了後コンピュータ使用中に外部記憶装置が接続された場合、上記実施の形態で説明した方法により外部記憶装置の使用禁止ソフトウェアおよびウイルスチェック済み状態が保証されなければネットワークから該コンピュータを切断することを特徴とするコンピュータ検疫システムである。
　さらに、検疫完了後コンピュータ使用中に外部記憶装置が接続された場合、上記実施の形態で説明した方法により外部記憶装置の使用禁止ソフトウェアおよびウイルスチェック済み状態が保証されなければ、使用禁止ソフトウェアおよびウイルスチェックを再実行し、該コンピュータの使用継続を許可することを特徴とするコンピュータ検疫システムである。
【００５２】
　実施の形態６．
　実施の形態６では、健全性チェック処理を実行する場合に、その実行範囲を最小限に抑える端末２００を備える検疫システム１０００について説明する。
【００５３】
　図１３に基づき実施の形態６に係る検疫システム１０００について説明する。図１３は、実施の形態５に係る検疫システム１０００が備える端末２００を示す機能ブロック図である。
　実施の形態６に係る検疫システム１０００は、実施の形態４に係る検疫システム１０００と比較して、端末２００の端末処理部２１０が最終チェック地点記憶部２１４を備える部分が異なる。
　最終チェック地点記憶部２１４は、健全性チェックプログラム２１がチェックした記憶領域の最終地点を記憶する。
　また、実施の形態６に係る端末２００は、ファイルシステムとしてログストラクチャードファイルシステム等を採用している。ログストラクチャードファイルシステムでは、更新差分や、新規追加のデータはすべてディスク後方の空き領域へアペンド追加される。つまり、端末２００が備える記憶装置９８４は、データの追加を記憶領域の後方に行う。
【００５４】
　実施の形態６に係る端末２００では、データの追加は記憶領域の後方にのみ行われるため、健全性チェック済の記憶領域については、改めて健全性チェックを行う必要はない。そのため、健全性チェックプログラム２１は、最終チェック地点記憶部２１４が記憶した

最終地点の後方に記憶されたデータについてのみ健全性チェックを行う。このため、実施の形態６に係る検疫システム１０００によれば、健全性チェックを行う範囲を最小限にとどめることが可能である。

【００５５】

実施の形態６をまとめると、ログストラクチャードファイルシステムが適用されたコンピュータについては、ファイルシステム上の新規差分についてのみ健全性チェック処理を行うことを特徴とするコンピュータ検疫システムである。

【図面の簡単な説明】

【００５６】

【図１】実施の形態における検疫システム１０００の外観の一例を示す図。

【図２】実施の形態における検疫装置１００、端末２００のハードウェア資源の一例を示す図。

【図３】実施の形態１に係る検疫システム１０００の構成を示す図。

【図４】実施の形態１に係る検疫システム１０００が備える検疫装置１００の機能を示す機能ブロック図。

【図５】実施の形態１に係る検疫システム１０００が備える端末２００（健全性チェック端末）の機能を示す機能ブロック図。

【図６】実施の形態１に係る検疫システム１０００の動作を示すフローチャート。

【図７】実施の形態２に係る検疫システム１０００が備える検疫装置１００を示す機能ブロック図。

【図８】実施の形態２に係る検疫システム１０００の動作を示すフローチャート。

【図９】実施の形態３に係る検疫システム１０００の動作を示すフローチャート。

【図１０】実施の形態４に係る検疫システム１０００が備える検疫装置１００を示す機能ブロック図。

【図１１】実施の形態４に係る検疫システム１０００の動作を示すフローチャート。

【図１２】実施の形態５に係る検疫システム１０００が備える検疫装置１００を示す機能ブロック図。

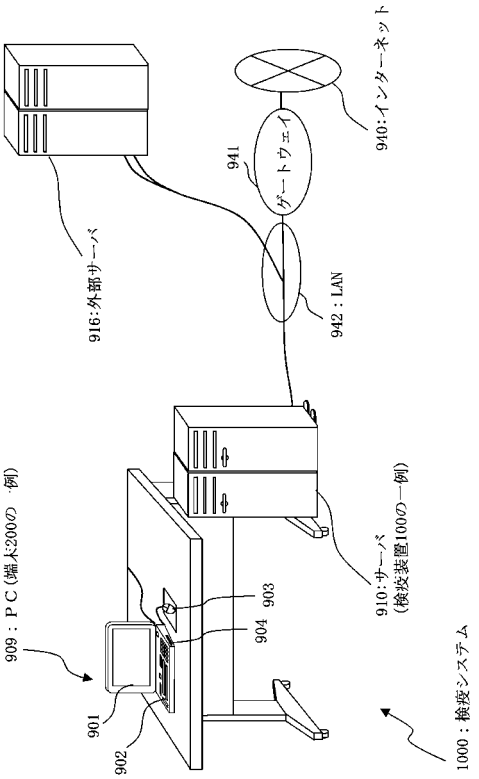
【図１３】実施の形態６に係る検疫システム１０００が備える端末２００を示す機能ブロック図。

【符号の説明】

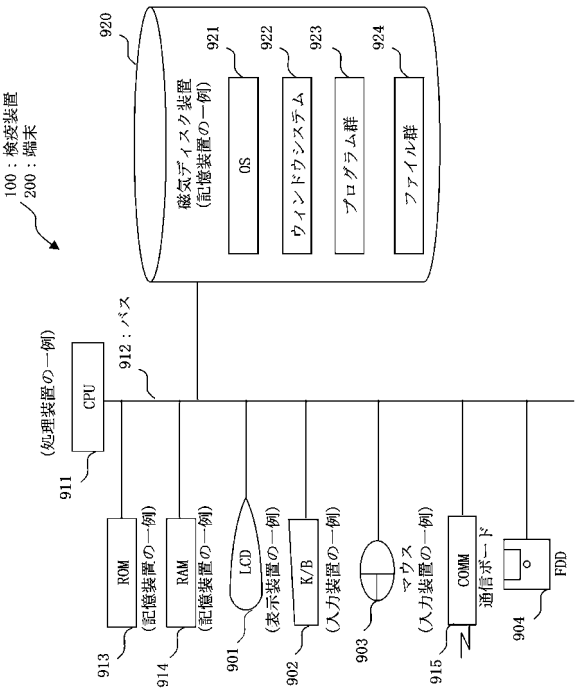
【００５７】

１０　接続許可判断部、１１　インテグリティチェック情報受信部、１２　検疫プログラム、１３　健全性チェック制御部、２０　アプリケーション、２１　健全性チェックプログラム、２２　インテグリティチェック情報送信部、２３　サプリカント、２４　耐タンパストレージ使用インターフェース、２５　耐タンパストレージライブラリ、２６　耐タンパストレージ、２７　ディスク領域、３０　オーセンティケータ、３１　治療サービス、１００　検疫装置、１１０　検疫処理部、１１２　接続要求受信部、１１４　接続要求応答部、１１６　健全性チェック指示部、１１８　検疫情報記憶部、１２０　検疫済状況、１２２　検疫処理制御部、１２４　外部接続判定部、１２６　ネットワーク接続記録受信部、１２８　ネットワーク接続判定部、１３０　外部記憶装置接続記録受信部、１３２　外部記憶装置接続判定部、１３４　リソース更新判定部、１３６　他端末接続記録受信部、１３８　他端末接続判定部、１４０　ネットワーク切断部、２００　端末、２１０　端末処理部、２１２　指示受信部、２１４　最終チェック地点記憶部、９０１　ＬＣＤ、９０２　Ｋ／Ｂ、９０３　マウス、９０４　ＦＤＤ、９０９　ＰＣ、９１０　サーバ、９１１　ＣＰＵ、９１２　バス、９１３　ＲＯＭ、９１４　ＲＡＭ、９１５　通信ボード、９１６　外部サーバ、９２０　磁気ディスク装置、９２１　ＯＳ、９２２　ウィンドウシステム、９２３　プログラム群、９２４　ファイル群、９４０　インターネット、９４１　ゲートウェイ、９４２　ＬＡＮ、９８０　処理装置、９８２　入力装置、９８４　記憶装置、９８６　表示装置、９８８　通信装置、１０００　検疫システム。

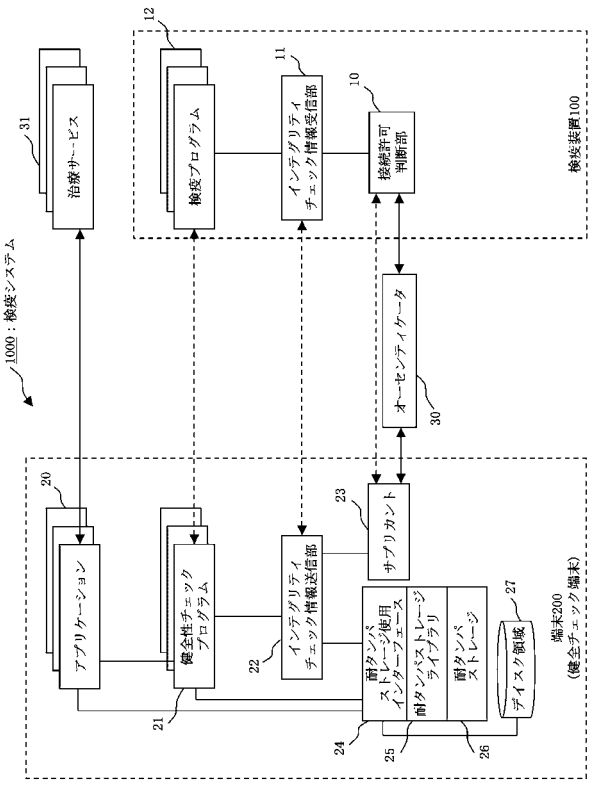
【図１】


940:インターネット
941
ゲートウェイ
942：LAN
916:外部サーバ
910:サーバ
(検疫装置100の一例)
909：ＰＣ(端末200の一例)
901
902
903
904
1000：検疫システム

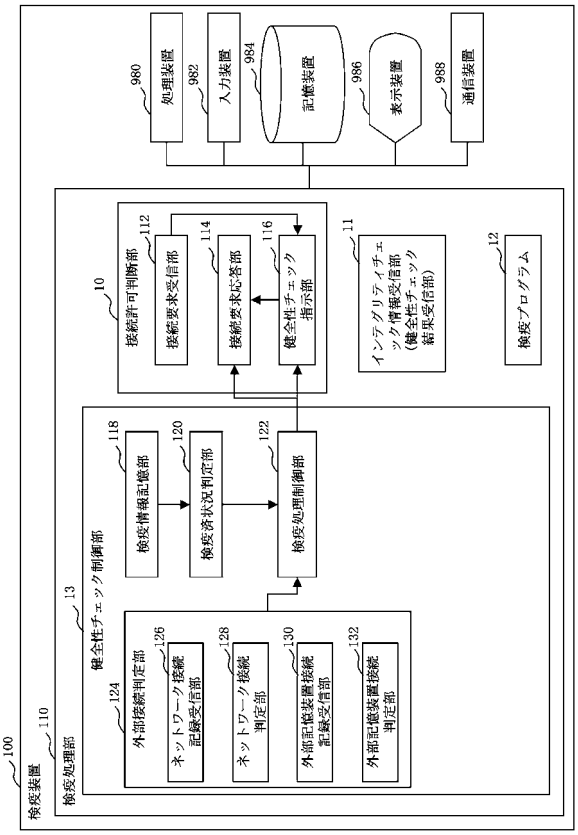
【図２】


100：検疫装置
200：端末
(処理装置の一例)
CPU
911
912：バス
920
磁気ディスク装置
(記憶装置の一例)
921
OS
922
ウィンドウシステム
923
プログラム群
924
ファイル群
ROM
(記憶装置の一例)
913
RAM
(記憶装置の一例)
914
LCD
(表示装置の一例)
901
K/B
(入力装置の一例)
902
マウス
(入力装置の一例)
903
COMM
通信ボード
915
FDD
904

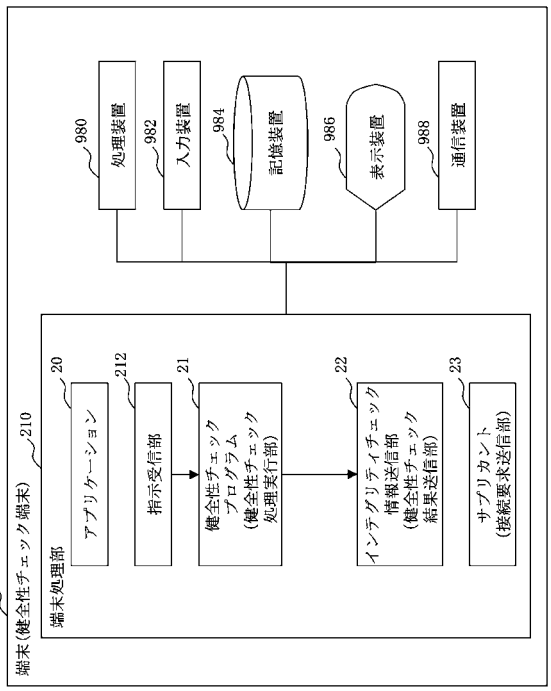
【図３】


1000：検疫システム
検疫装置100
検疫プログラム
12
インテグリティ
チェック情報受信部
11
接続許可
判断部
10
治療サーバ
31
オーセンティケータ
30
アプリケーション
20
健全性チェック
プログラム
21
インテグリティ
チェック情報送信部
22
サプリカント
23
耐タンパ
ストレージ使用
インターフェース
24
耐タンパストレージ
ライブラリ
25
耐タンパ
ストレージ
26
ディスク領域
27
端末200
(健全チェック端末)

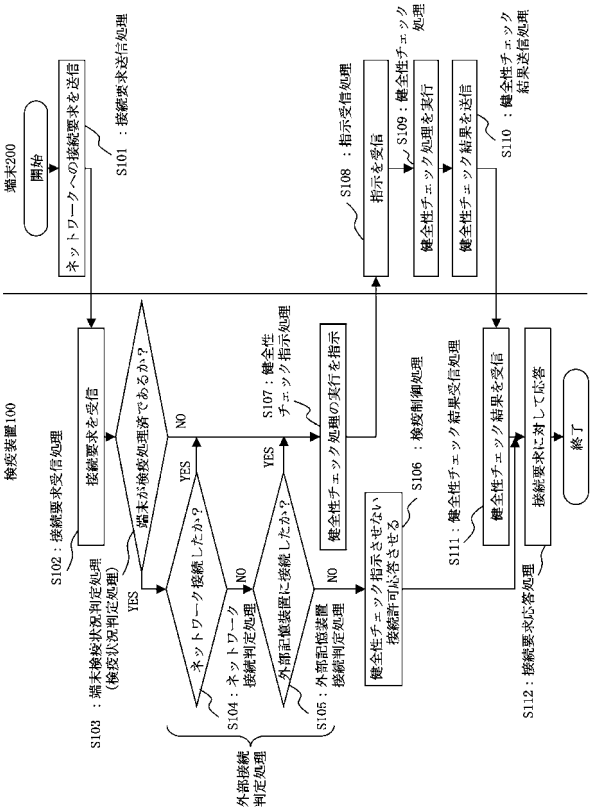
【図４】


100
検疫装置
110
検疫処理部
健全性チェック制御部
13
外部接続判定部
124
ネットワーク接続
記録受信部
126
ネットワーク接続
判定部
128
外部記憶装置接続
記録受信部
130
外部記憶装置接続
判定部
132
検疫情報記憶部
118
検疫済状況判定部
120
検疫処理制御部
122
接続許可判断部
10
接続要求受信部
112
接続要求応答部
114
健全性チェック
指示部
116
インテグリティチェック情報受信部
(健全性チェック結果受信部)
11
検疫プログラム
12
処理装置
980
入力装置
982
記憶装置
984
表示装置
986
通信装置
988

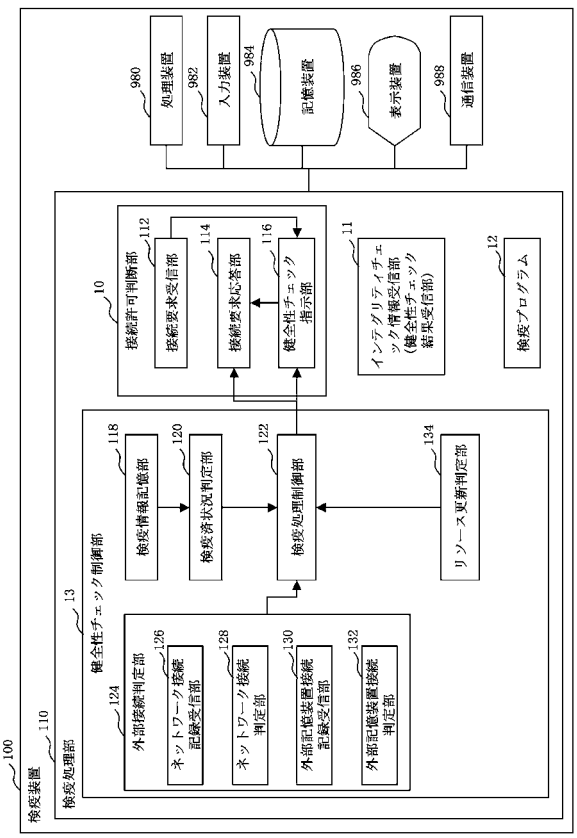
【図５】


200
端末(健全性チェック端末)
210
端末処理部
20
アプリケーション
212
指示受信部
21
健全性チェック
プログラム
(健全性チェック
処理実行部)
22
インテグリティチェック
情報送信部
(健全性チェック
結果送信部)
23
サプリカント
(接続要求送信部)
980
処理装置
982
入力装置
984
記憶装置
986
表示装置
988
通信装置

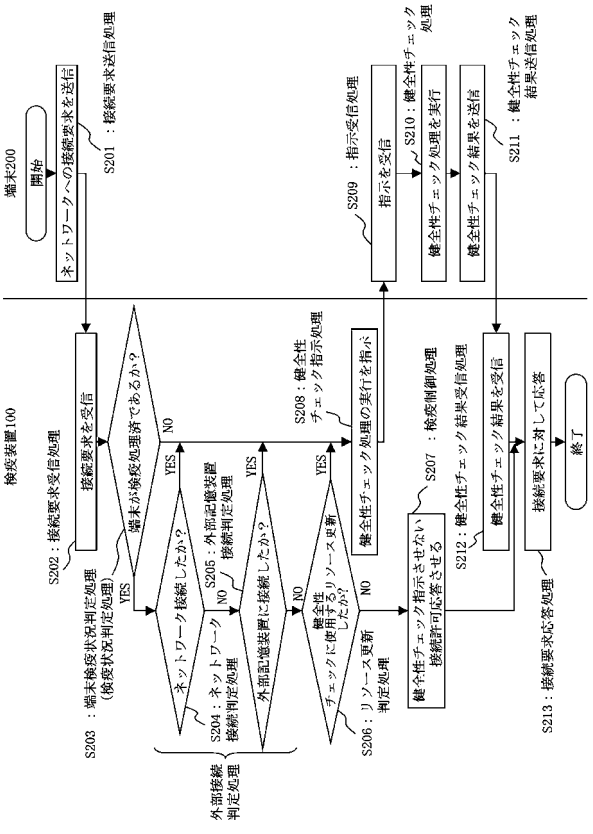
【図６】


端末200
開始
ネットワークへの接続要求を送信
S101 ：接続要求送信処理
検疫装置100
接続要求を受信
S102：接続要求受信処理
S103 ：端末検疫状況判定処理
(検疫状況判定処理)
端末が検疫処理済であるか?
NO
YES
ネットワーク接続したか?
NO
YES
S104：ネットワーク
接続判定処理
外部記憶装置に接続したか?
NO
YES
S105：外部記憶装置
接続判定処理
外部接続
判定処理
S107：健全性
チェック指示処理
健全性チェック処理の実行を指示
S106 ：検疫制御処理
健全性チェック指示させない
接続許可応答させる
S111：健全性チェック結果を受信
S112：接続要求応答処理
S108 ：指示受信処理
指示を受信
S109：健全性チェック
処理
健全性チェック処理を実行
健全性チェック結果を送信
S110 ：健全性チェック
結果送信処理
接続要求に対して応答
終了

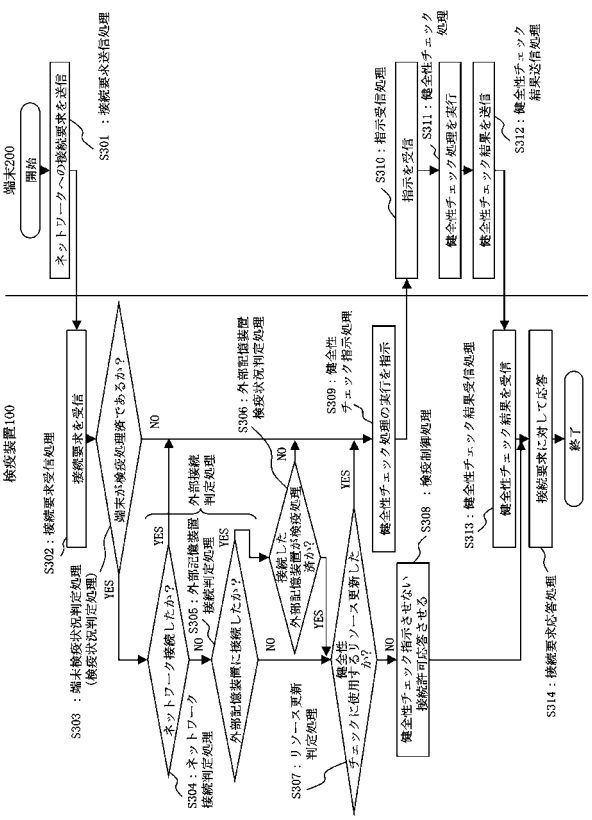
【図７】


100
検疫装置
110
検疫処理部
13
健全性チェック制御部
124
外部接続判定部
126
ネットワーク接続
記録受信部
128
ネットワーク接続
判定部
130
外部記憶装置接続
記録受信部
132
外部記憶装置接続
判定部
118
検疫情報記憶部
120
検疫済状況判定部
122
検疫処理制御部
134
リソース更新判定部
10
接続許可判断部
112
接続要求受信部
114
接続要求応答部
116
健全性チェック
指示部
11
インテグリティチェック情報受信部
(健全性チェック
結果受信部)
12
検疫プログラム
980
処理装置
982
入力装置
984
記憶装置
986
表示装置
988
通信装置

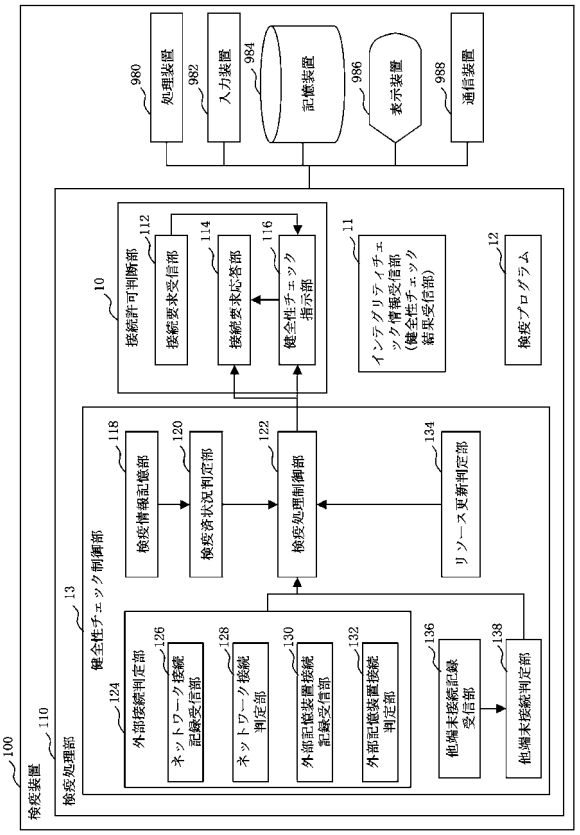
【図８】


端末200
開始
ネットワークへの接続要求を送信
S201 ：接続要求送信処理
検疫装置100
接続要求を受信
S202：接続要求受信処理
S203 ：端末検疫状況判定処理
(検疫状況判定処理)
端末が検疫処理済であるか?
NO
YES
ネットワーク接続したか?
NO
YES
S204：ネットワーク
接続判定処理
S205：外部記憶装置
接続判定処理
外部記憶装置に接続したか?
NO
YES
外部接続
判定処理
S208：健全性
チェック指示処理
健全性チェック処理の実行を指示
S209 ：指示受信処理
指示を受信
S210：健全性チェック
処理
健全性チェック処理を実行
健全性チェック結果を送信
S211 ：健全性チェック
結果送信処理
S207 ：検疫制御処理
健全性チェック指示させない
接続許可応答させる
S212：健全性チェック結果を受信
S213：接続要求応答処理
健全性
チェックに使用するリソース更新
したか?
NO
YES
S206：リソース更新
判定処理
接続要求に対して応答
終了

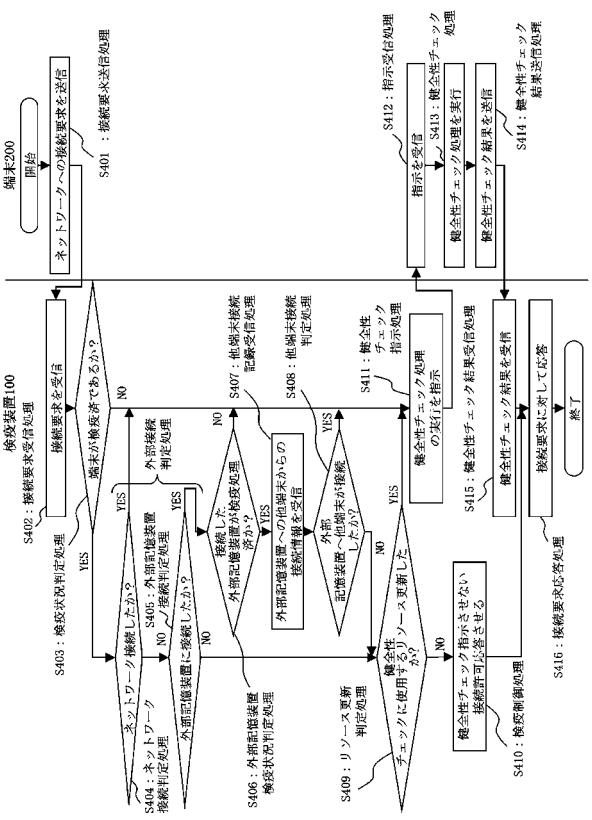
【図９】



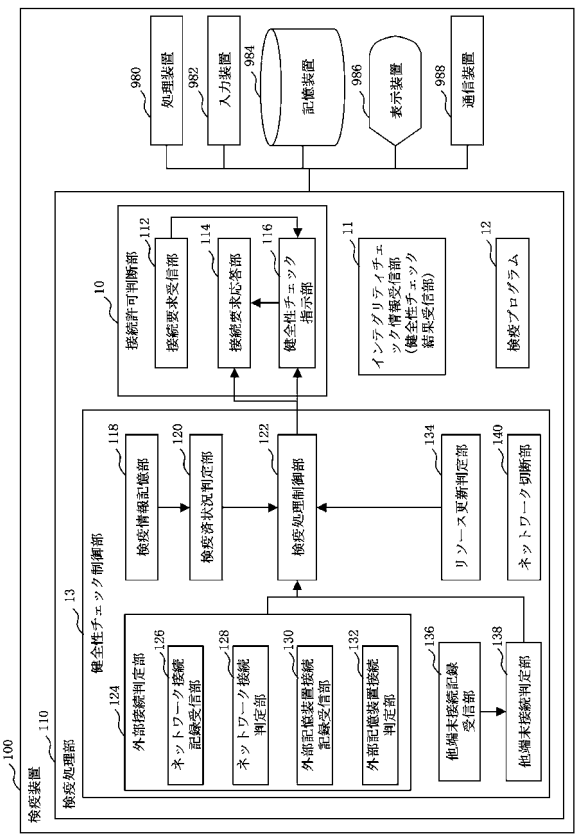
【図１０】



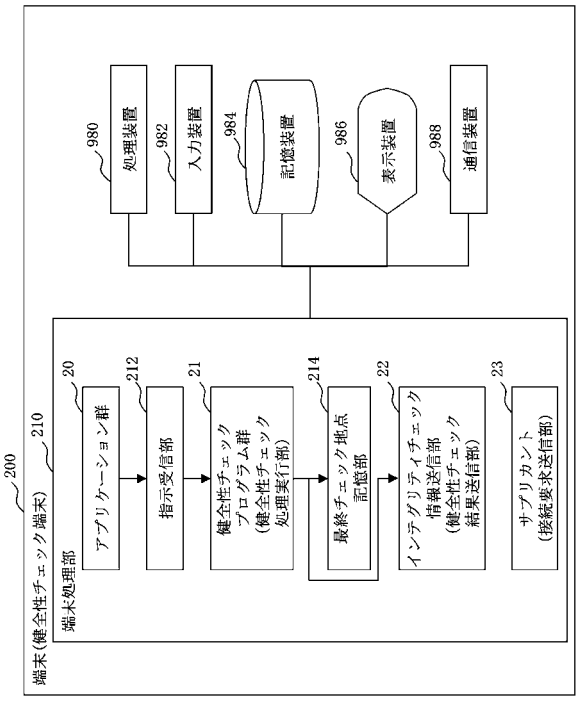
【図１１】



【図１２】



【図１３】


200
端末(健全性チェック端末)
210
端末処理部
20
アプリケーション群
212
指示受信部
21
健全性チェック
プログラム群
(健全性チェック
処理実行部)
214
最終チェック地点
記憶部
22
インテグリティチェック
情報送信部
(健全性チェック
結果送信部)
23
サブリカント
(接続要求送信部)
980
処理装置
982
入力装置
984
記憶装置
986
表示装置
988
通信装置

フロントページの続き

審査官　田中　慎太郎

(56)参考文献　再公表特許第２００６／０９２９３１（ＪＰ，Ａ１）
特開２００６－１９５７０２（ＪＰ，Ａ）
佐藤隆哉，検疫ネットワーク，Ｎ＋Ｉ　ＮＥＴＷＯＲＫ，日本，ソフトバンクパブリッシング株式会社，２００４年　９月　１日，第４巻第９号，p.36-45

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０６Ｆ　２１／２２