(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7028065号
(P7028065)

(45)発行日　令和4年3月2日(2022.3.2)

(24)登録日　令和4年2月21日(2022.2.21)

(51)国際特許分類

H04L	*12/66*	*(2006.01)*	H04L	12/66
H04L	*12/22*	*(2006.01)*	H04L	12/22

FI

請求項の数　15　（全20頁）

(21)出願番号　特願2018-103753(P2018-103753)
(22)出願日　平成30年5月30日(2018.5.30)
(65)公開番号　特開2019-208173(P2019-208173A)
(43)公開日　令和1年12月5日(2019.12.5)
審査請求日　令和3年4月16日(2021.4.16)

(73)特許権者　000001270
コニカミノルタ株式会社
東京都千代田区丸の内二丁目７番２号
(74)代理人　110001195
特許業務法人深見特許事務所
(72)発明者　川口 俊和
東京都千代田区丸の内二丁目７番２号
コニカミノルタ株式会社内
(72)発明者　橋本 晋弥
東京都千代田区丸の内二丁目７番２号
コニカミノルタ株式会社内
(72)発明者　浅井 佑樹
東京都千代田区丸の内二丁目７番２号
コニカミノルタ株式会社内
審査官　宮島 郁美

最終頁に続く

(54)【発明の名称】　画像処理装置、その制御方法、およびプログラム

(57)【特許請求の範囲】
【請求項１】
ファイルを格納する記憶部と、
ファイルに関する２以上の機能のそれぞれを実現する機能実現部と、
前記記憶部に格納されたファイルのウィルスチェックを実行する制御部とを備え、
前記記憶部は、
ウィルスの種別と前記２以上の機能の中の１以上の機能とを関連付けるウィルス種別情報と、
ファイル種別と前記２以上の機能の中の１以上の機能とを関連付けるファイル種別情報と、の少なくとも一方を格納し、
前記制御部は、
前記２以上の機能のうち、前記ウィルスチェックにおいて検出されたウィルスの種別に関連付けられた機能、および、前記記憶部に格納されたファイルの中の前記ウィルスチェックによって検出されたウィルスに感染している可能性があるファイルの種別に関連付けられた機能、の少なくとも一方を制限する、画像処理装置。
【請求項２】
前記制御部は、ウィルス種別情報に基づいて前記機能の一部を制限する、請求項１に記載の画像処理装置。
【請求項３】
前記制御部は、ファイル種別情報に基づいて前記機能の一部を制限する、請求項１または

２に記載の画像処理装置。
【請求項４】
前記制御部は、ウィルス種別情報およびファイル種別情報に基づいて前記機能の一部を制限する、請求項１～請求項３のいずれか１項に記載の画像処理装置。
【請求項５】
前記制御部は、前記ウィルスチェックにおいて検出されたファイルが実行されておらず、かつ、前記ウィルスチェックにおいて検出されたウィルスの種別が前記記憶部内のファイルを改ざんしない種別である場合には、前記ウィルスが除去された後、前記２以上の機能の制限を解除する、請求項１～請求項４のいずれか１項に記載の画像処理装置。
【請求項６】
前記制御部は、前記ファイルが実行されたか否かを、ファイルへのアクセスログ、または、前記記憶部に格納されたファイルの履歴に基づいて判断する、請求項５に記載の画像処理装置。
【請求項７】
前記制御部は、前記ウィルスチェックにおいて検出されたウィルスの種別が前記記憶部内のファイルを改ざんする種別である場合に、前記記憶部内のファイルに対して前記ウィルスチェックにおいて検出されたウィルスに感染している可能性があるか否かを検査する、請求項１～請求項６のいずれか１項に記載の画像処理装置。
【請求項８】
前記２以上の機能は、外部機器と通信する機能を含み、
前記制御部は、前記ウィルスチェックにおいてウィルスが検出された場合に、前記外部機器と通信する機能を制限した後、当該ウィルス除去を実行する、請求項１～請求項７のいずれか１項に記載の画像処理装置。
【請求項９】
前記制御部は、前記ウィルスに感染している可能性があるファイルを報知する、請求項１～請求項８のいずれか１項に記載の画像処理装置。
【請求項１０】
前記制御部は、前記記憶部内の各ファイルに対して、当該ファイルが前記記憶部内に格納されたときの当該ファイルの情報、前回のウィルスチェックのときの当該ファイルの情報、最新の利用時の当該ファイルの情報、および、今回のウィルスチェックのときの当該ファイルの情報の中の少なくとも一つを利用して、各ファイルが前記ウィルスに感染している可能性があるか否かを検査する、請求項１～請求項９のいずれか１項に記載の画像処理装置。
【請求項１１】
最新の利用時の当該ファイルの情報は、
最新の利用時の日時を特定する情報を含み、
前回のウィルスチェックのときの当該ファイルの情報は、
前回のウィルスチェックの日時を特定する情報と、前回のウィルスチェックのときの当該ファイルのチェックサム値とを含み、
今回のウィルスチェックのときの当該ファイルの情報は、
今回のウィルスチェックのときの当該ファイルのチェックサム値を含む、
請求項１０に記載の画像処理装置。
【請求項１２】
前記２以上の機能は、通信機能、プリント機能、スキャン機能、ファイル送信機能、ブラウザー機能のうち２以上の機能を含む、請求項１～請求項１１のいずれか１項に記載の画像処理装置。
【請求項１３】
前記画像処理装置は、プリンター装置およびスキャナー装置の少なくとも一方を含む、請求項１～請求項１２のいずれか１項に記載の画像処理装置。
【請求項１４】

ファイルを格納する記憶部と、２以上の機能のそれぞれを実現する機能実現部とを備えた画像処理装置の制御方法であって、
前記記憶部に格納されたファイルのウィルスチェックを実行するステップと、
前記２以上の機能のうち、前記ウィルスチェックにおいて検出されたウィルスの種別に関連付けられた機能、および、前記記憶部に格納されたファイルの中の前記ウィルスチェックによって検出されたウィルスに感染している可能性があるファイルの種別に関連付けられた機能、の少なくとも一方を制限するステップとを備えた、画像処理装置の制御方法。
【請求項１５】
ファイルを格納する記憶部と、２以上の機能のそれぞれを実現する機能実現部とを備えた画像処理装置のコンピューターによって実行されるプログラムであって、
前記プログラムは、前記コンピューターに、
前記記憶部に格納されたファイルのウィルスチェックを実行するステップと、
前記２以上の機能のうち、前記ウィルスチェックにおいて検出されたウィルスの種別に関連付けられた機能、および、前記記憶部に格納されたファイルの中の前記ウィルスチェックによって検出されたウィルスに感染している可能性があるファイルの種別に関連付けられた機能、の少なくとも一方を制限するステップとを実行させる、プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、画像処理装置、その制御方法、およびプログラムに関し、特に、画像処理装置におけるウィルスチェックの結果に従った当該画像処理装置の制御に関する。
【背景技術】
【０００２】
従来、ＭＦＰ（Multi-Functional Peripheral）等の画像処理装置におけるウィルスチェックについて種々検討がなされてきた。たとえば、特開２０１１－６５４８３号公報（特許文献１）は、ＭＦＰ等の複合機において、ウィルスチェックによってウィルス感染の無いことが確認されている制御モジュールのみを使用するジョブの実行を許可する技術が開示している。特開２０１０－１４１７０５号公報（特許文献２）は、外部端末から複合機へのアクセスに関し、アクセス時の安全性の指標となるセキュリティ情報を取得し、セキュリティ情報がセキュリティ基準を満たすことを条件として外部端末からのアクセス要求を許可する技術を開示している。特開２００６－２５６１０４号公報（特許文献３）は、クライアントＰＣから受信したデータにウィルスが混入していることが検知された場合に、ウィルスの混入をパネルで通知し、データに混入しているウィルスの二次感染を防止する構成を備える複合機を開示している。二次感染の防止としては、ユーザへの通知、全ての機能制限および電源遮断、ウィルス駆除、ウィルス駆除が不可能なファイルの削除、ならびに、ネットワークの遮断が挙げられている。
【先行技術文献】
【特許文献】
【０００３】
【文献】特開２０１１－６５４８３号公報
特開２０１０－１４１７０５号公報
特開２００６－２５６１０４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、二次感染の危険性を考慮すると、ウィルスに感染したファイルの利用は回避されるべきではある。一方で、全ての機能が制限されれば、ウィルス感染に無関係の機能まで制限される可能性があるため、作業効率が不当に低下するおそれがある。
【０００５】
本開示は、係る実情に鑑み考え出されたものであり、その目的は、画像処理装置において

、ウィルスに感染したファイルが検知された場合に制限される機能を適切に決定することである。

【課題を解決するための手段】

【０００６】

本開示のある局面に従うと、ファイルを格納する記憶部と、ファイルに関する２以上の機能のそれぞれを実現する機能実現部と、記憶部に格納されたファイルのウィルスチェックを実行する制御部とを備える画像処理装置が提供される。記憶部は、ウィルスの種別と２以上の機能の中の１以上の機能とを関連付けるウィルス種別情報と、ファイル種別と２以上の機能の中の１以上の機能とを関連付けるファイル種別情報と、の少なくとも一方を格納し、制御部は、２以上の機能のうち、ウィルスチェックにおいて検出されたウィルスの種別に関連付けられた機能、および、記憶部に格納されたファイルの中のウィルスチェックによって検出されたウィルスに感染している可能性があるファイルの種別に関連付けられた機能、の少なくとも一方を制限する。

制御部は、ウィルス種別情報に基づいて機能の一部を制限してもよい。

制御部は、ファイル種別情報に基づいて機能の一部を制限してもよい。

制御部は、ウィルス種別情報およびファイル種別情報に基づいて機能の一部を制限してもよい。

【０００７】

制御部は、ウィルスチェックにおいて検出されたファイルが実行されておらず、かつ、ウィルスチェックにおいて検出されたウィルスの種別が記憶部内のファイルを改ざんしない種別である場合には、ウィルスが除去された後、２以上の機能の制限を解除してもよい。

【０００８】

制御部は、ファイルが実行されたか否かを、ファイルへのアクセスログ、または、記憶部に格納されたファイルの履歴に基づいて判断してもよい。

【０００９】

制御部は、ウィルスチェックにおいて検出されたウィルスの種別が記憶部内のファイルを改ざんする種別である場合に、記憶部内のファイルに対してウィルスチェックにおいて検出されたウィルスに感染している可能性があるか否かを検査してもよい。

【００１０】

２以上の機能は、外部機器と通信する機能を含んでもよい。制御部は、ウィルスチェックにおいてウィルスが検出された場合に、外部機器と通信する機能を制限した後、当該ウィルス除去を実行してもよい。

【００１１】

制御部は、ウィルスに感染している可能性があるファイルを報知してもよい。

制御部は、記憶部内の各ファイルに対して、当該ファイルが記憶部内に格納されたときの当該ファイルの情報、前回のウィルスチェックのときの当該ファイルの情報、最新の利用時の当該ファイルの情報、および、今回のウィルスチェックのときの当該ファイルの情報の中の少なくとも一つを利用して、各ファイルがウィルスに感染している可能性があるか否かを検査してもよい。

【００１２】

最新の利用時の当該ファイルの情報は、最新の利用時の日時を特定する情報を含んでもよい。前回のウィルスチェックのときの当該ファイルの情報は、前回のウィルスチェックの日時を特定する情報と、前回のウィルスチェックのときの当該ファイルのチェックサム値とを含んでもよい。今回のウィルスチェックのときの当該ファイルの情報は、今回のウィルスチェックのときの当該ファイルのチェックサム値を含んでもよい。

２以上の機能は、通信機能、プリント機能、スキャン機能、ファイル送信機能、ブラウザー機能のうち２以上の機能を含んでいてもよい。

画像処理装置は、プリンター装置およびスキャナー装置の少なくとも一方を含んでいてもよい。

【００１３】

本開示の他の局面に従うと、ファイルを格納する記憶部と、２以上の機能のそれぞれを実現する機能実現部とを備えた画像処理装置の制御方法が提供される。制御方法は、記憶部に格納されたファイルのウィルスチェックを実行するステップと、２以上の機能のうち、ウィルスチェックにおいて検出されたウィルスの種別に関連付けられた機能、および、記憶部に格納されたファイルの中のウィルスチェックによって検出されたウィルスに感染している可能性があるファイルの種別に関連付けられた機能、の少なくとも一方を制限するステップとを備える。

【００１４】

本開示のさらに他の局面に従うと、ファイルを格納する記憶部と、２以上の機能のそれぞれを実現する機能実現部とを備えた画像処理装置のコンピューターによって実行されるプログラムが提供される。プログラムは、コンピューターに、記憶部に格納されたファイルのウィルスチェックを実行するステップと、２以上の機能のうち、ウィルスチェックにおいて検出されたウィルスの種別に関連付けられた機能、および、記憶部に格納されたファイルの中のウィルスチェックによって検出されたウィルスに感染している可能性があるファイルの種別に関連付けられた機能、の少なくとも一方を制限するステップとを実行させる。

【発明の効果】

【００１５】

本開示によれば、ウィルスの種別だけでなく、ウィルスに感染した可能性があるファイルの種別に基づいて、制限される機能が決定され得る。これにより、画像処理装置内のファイルがウィルスに感染した場合に、必要最小限の機能が制限される。

【図面の簡単な説明】

【００１６】

【図１】本開示に係る画像処理装置の外観を示す図である。

【図２】図１の画像処理装置のハードウェア構成を示す図である。

【図３】ファイル管理情報の内容の一例を示す図である。

【図４】更新後のファイル管理情報の内容の一例を示す図である。

【図５】更新後のファイル管理情報の内容の他の例を示す図である。

【図６】ウィルス種別情報の一例を示す図である。

【図７】ファイル種別情報の内容の一例を示す図である。

【図８】画像処理装置１においてウィルスチェックに関連して実行される処理のフローチャートである。

【図９】図８のステップＳ３２のサブルーチンのフローチャートである。

【図１０】ステップＳ３２４のサブルーチンのフローチャートである。

【図１１】ステップＳ３２６のサブルーチンのフローチャートである。

【図１２】ステップＳ３２８のサブルーチンのフローチャートである。

【発明を実施するための形態】

【００１７】

以下に、図面を参照しつつ、画像処理装置の実施の形態について説明する。以下の説明では、同一の部品および構成要素には同一の符号を付してある。それらの名称および機能も同じである。したがって、これらの説明は繰り返さない。

【００１８】

［１．画像処理装置の構成］

図１は、本開示に係る画像処理装置の外観を示す図である。図２は、図１の画像処理装置のハードウェア構成を示す図である。

【００１９】

画像処理装置１の一例は、ＭＦＰ、すなわち、コピー、ネットワークプリンティング、スキャナー、ＦＡＸ、またはドキュメントサーバーなどの機能を集約した装置である。画像処理装置１は、操作パネル１１、スキャナー装置１３、プリンター装置１４、ステープル、パンチ等の処理を行うフィニッシャー装置１５、通信インターフェース１６、ドキュメ

ントフィーダー１７、給紙装置１８、ＣＰＵ（Central Processing Unit）２０、ＲＯＭ（Read Only Memory）２１、ＲＡＭ（Random Access Memory）２２、記憶部２３、および、ＵＳＢ（Universal Serial Bus）インターフェース２３Ａを含む。

【００２０】

操作パネル１１は、操作装置１１ａとディスプレイ１１ｂとを含む。操作装置１１ａは、数字、文字、および記号などを入力するための複数のキー、投稿文を作成したいときに押下されるコメントキー、押下された各種のキーを認識するセンサ、および認識したキーを示す信号をＣＰＵ２０に送信する送信用回路を含む。

【００２１】

ディスプレイ１１ｂは、メッセージまたは指示を与えるための画面、ユーザーが設定内容および処理内容を入力するための画面、および、画像処理装置１で形成された画像および処理の結果を示す画面などを表示する。ディスプレイ１１ｂは、タッチパネルであってもよい。すなわち、ディスプレイ１１ｂと操作装置１１ａの少なくとも一部とが一体的に構成されていてもよい。ディスプレイ１１ｂはユーザーが指で触れたタッチパネル上の位置を検知し、検知結果を示す信号をＣＰＵ２０に送信する機能を備えている。

【００２２】

画像処理装置１は、通信インターフェース１６を介して、外部機器（たとえば、パーソナルコンピューター）と通信可能である。外部機器には、画像処理装置１に対して指令を与えるためのアプリケーションプログラムおよびドライバがインストールされていてもよい。これにより、ユーザーは、外部機器を使用して、画像処理装置１を遠隔的に操作できる。

【００２３】

スキャナー装置１３は、写真、文字、絵などの画像情報を原稿から光電的に読取って画像データを取得する。取得された画像データ（濃度データ）は、図示しない画像処理部においてデジタルデータに変換され、周知の各種画像処理を施された後、プリンター装置１４や通信インターフェース１６に送られ、画像の印刷やデータの送信に供されるか、または、後の利用のために記憶部２３に格納される。

【００２４】

プリンター装置１４は、スキャナー装置１３により取得された画像データ、通信インターフェース１６により外部機器から受信した画像データ、または記憶部２３に格納されている画像を、用紙またはフィルムなどの記録シートに印刷する。給紙装置１８は、画像処理装置１本体の下部に設けられており、印刷対象の画像に適した記録シートをプリンター装置１４に供給するために用いられている。プリンター装置１４によって画像が印刷された記録シートつまり印刷物は、フィニッシャー装置１５を通って、モード設定に応じてステープル、パンチなどの処理を行い、トレイ２４に排出される。

【００２５】

通信インターフェース１６は、送信部および受信部を含み、ＰＣおよびＦＡＸ端末とデータのやりとりを行うための装置である。通信インターフェース１６の一例は、ＮＩＣ（Network Interface Card）、モデム、または、ＴＡ（Terminal Adapter）などが用いられる。

【００２６】

ＣＰＵ２０は、画像処理装置１の全体を統括的に制御し、通信機能、プリント機能、スキャン機能、ファイル送信機能、およびブラウザー機能等の基本機能を使用可能に制御する。より具体的には、ＣＰＵ２０は、通信機能等の、ＣＰＵ２０以外の要素を用いた機能を実現するための機能制御部２０Ａ、ファイル送信機能を実現するためのプログラムモジュールによって構成されるファイル送信部２０Ｂ、および、ブラウザー機能を実現するためのブラウザーモジュールによって構成されるブラウザー処理部２０Ｃを含む。

【００２７】

ＲＯＭ２１は、ＣＰＵ２０の動作プログラム等を格納するメモリーである。

ＲＡＭ２２は、ＣＰＵ２０が動作プログラムに基づいて動作する際の作業領域を提供するメモリーであり、ＣＰＵ２０は、ＲＯＭ２１等から動作プログラムをロードするとともに

種々のデータをロードして、作業を行う。
【００２８】
記憶部２３は、例えばハードディスクドライブ（ＨＤＤ）などの不揮発性の記憶デバイスにより構成されており、各種のアプリケーション、スキャナー装置１３で読み取られた原稿の画像データ等が記憶されている。
【００２９】
ＵＳＢインターフェース２３Ａは、画像処理装置１に対して着脱可能なＵＳＢメモリー２３Ｘのインターフェースである。ＣＰＵ２０は、ＵＳＢインターフェース２３Ａを介して、ＵＳＢメモリー２３Ｘに格納された情報を読出す。ＣＰＵ２０は、また、ＵＳＢインターフェース２３Ａを介して、ＵＳＢメモリー２３Ｘに情報を書き込む。
【００３０】
［２．ファイル管理情報］
記憶部２３は、各種のファイルとともに、各ファイルを管理する情報（ファイル管理情報）を格納する。図３は、ファイル管理情報の内容の一例を示す図である。図３を参照して、ファイル管理情報は、各ファイルのファイル名に、格納時情報と、ウィルスチェック情報と、最新利用情報とを関連付ける。
【００３１】
格納時情報は、各ファイルが記憶部２３に格納されたときの情報であり、格納日時（ＴＳ）と、作成日時（ＴＰ）と、ファイル容量（ＶＳ）と、チェックサム値（ＣＳ）とを含む。格納日時（ＴＳ）は、ファイルが記憶部２３に格納された日時を表わす。作成日時（ＴＰ）は、当該ファイルが作成された日時を表わす。ファイル容量（ＶＳ）は、当該ファイルが記憶部２３に格納されたときのファイルの容量を表わす。チェックサム値（ＣＳ）は、当該ファイルが記憶部２３に格納されたときの、当該ファイルのチェックサム値を表わす。
【００３２】
ＣＰＵ２０は、たとえば外部からファイルをダウンロードした場合、当該ファイルに付随する作成日時および容量を、作成日時（ＴＰ）およびファイル容量（ＶＳ）として格納時情報に登録する。また、ＣＰＵ２０は、ダウンロードした日時を、格納日時（ＴＳ）として登録する。さらに、ＣＰＵ２０は、その時点でのファイルのチェックサム値を算出し、チェックサム値（ＣＳ）として格納時情報に登録する。なお、チェックサム値の算出にはいかなるアルゴリズムが利用されてもよい。
【００３３】
ウィルスチェック情報は、画像処理装置１において最新のウィルスチェックが実行されたときの情報であり、前回チェック日時（ＴＣ）と、ファイル容量（ＶＣ）と、チェックサム値（ＣＣ）とを含む。前回チェック日時（ＴＣ）とは、前回のウィルスチェックの日時を表わす。ファイル容量（ＶＣ）は、前回ウィルスチェックが実行されたときの各ファイルの容量を表わす。チェックサム値（ＣＣ）は、前回ウィルスチェックが実行されたときの各ファイルのチェックサム値を表わす。
【００３４】
ＣＰＵ２０は、たとえば定期的にウィルスチェックを実行し、ウィルスチェックを実行するたびに前回チェック日時（ＴＣ）を更新する。また、ＣＰＵ２０は、各ウィルスチェックにおいて各ファイルの容量とチェックサム値とを取得（または、算出）し、ファイル容量（ＶＣ）およびチェックサム値（ＣＣ）としてウィルスチェック情報に登録する。
【００３５】
最新利用情報は、ウィルスチェック後にファイルがアクセスされたときの情報であり、利用日時（ＴＵ）と、ファイル容量（ＶＵ）と、チェックサム値（ＣＵ）とを含む。
【００３６】
利用日時（ＴＵ）は、ファイルがアクセスされた最新の日時を表わす。ファイル容量（ＶＵ）は、当該アクセスの終了後のファイルの容量を表わす。チェックサム値（ＣＵ）は、当該アクセスの終了後のファイルのチェックサム値を表わす。

【００３７】
ＣＰＵ２０は、たとえばファイルが編集された後で保存されると、保存された日時を利用日時（ＴＵ）として登録する。さらに、ＣＰＵ２０は、保存されたファイルの容量およびチェックサム値を取得（または、算出）し、ファイル容量（ＶＵ）およびチェックサム値（ＣＵ）として登録する。チェックサム値（ＣＳ）とチェックサム値（ＣＣ）とチェックサム値（ＣＵ）とは、同じ種類のアルゴリズムに従って算出されることが好ましい。これにより、ファイルに変更が加えられていないことがチェックサムの値を比較することによって判定され得る。
【００３８】
図３の例では、２つのファイル（それぞれのファイル名は、「ＮＭ１」と「ＮＭ２」）についての情報が格納されている。説明のため、各ファイルのファイル名の末尾に数字が付されている。各ファイルの格納日時等の値には、「ＴＳ１」等のように、ファイル名の末尾に付されたものと同じ数字が付されている。
【００３９】
図３は、記憶部２３にファイルＮＭ１が格納された後、時刻ＴＣ１（ファイルＮＭ１の前回チェック日時（ＴＣ））にウィルスチェックが実行されたことを表わす。図３は、また、時刻ＴＣ１のウィルスチェックの後、ファイルＮＭ２が記憶部２３に格納されたことを表わす。ファイルＮＭ２が記憶部２３に格納された後、まだウィルスチェックは実行されていない。したがって、ファイルＮＭ２はウィルスチェック情報の値を有していない。図３は、さらに、ファイルＮＭ２が記憶部２３に格納されてから、まだファイルＮＭ２にアクセスされていないことを表わす。したがって、ファイルＮＭ２は、最新利用情報を有していない。
【００４０】
図４は、更新後のファイル管理情報の内容の一例を示す図である。図４は、図３に示された状態の後、時刻ＴＵ２（図４のファイルＮＭ２の利用日時ＴＵ））に、ファイルＮＭ２にアクセスがあったことを表わす。
【００４１】
このアクセスにより、ファイルＮＭ２の容量は、ＶＳ２からＶＵ２に変化している。なお、ＶＳ２とＶＵ２とは同じ値であってもよい。また、このアクセスにより、ファイルＮＭ２のチェックサム値は、ＣＳ２からＣＵ２に変化している。なお、ＣＳ２とＣＵ２とは同じ値であってもよい。
【００４２】
図５は、更新後のファイル管理情報の内容の他の例を示す図である。図５は、図４に示された状態の後、時刻ＴＣ２（図５のファイルＮＭ１およびファイルＮＭ２の前回チェック日時（ＴＣ））にウィルスチェックが実行されたことを表わす。
【００４３】
本実施の形態において、ウィルスチェックとは、後述する図８のステップＳ１０のみを指してもよいし、ステップＳ１０およびこれに付随するステップ（図８～図１２に示されたステップ）を指してもよい。
【００４４】
［３．ウィルス種別情報］
図６は、ウィルス種別情報の一例を示す図である。ウィルス種別情報は、コンピューターウィルスの種別と、画像処理装置１の各機能の実行の可否とを関連付ける。ＣＰＵ２０は、ウィルスチェックにおいてウィルスを検出した場合、ウィルス種別情報において、当該ウィルスの種別に所与の態様（たとえば、「不可」）で関連付けられている機能を制限する。「制限」とは、たとえば、当該機能の実行が指示されても、当該機能を実現しないように画像処理装置１を制御することを意味する。
【００４５】
ウィルス種別情報は、たとえば、記憶部２３に格納されている。画像処理装置１の管理者は、たとえば操作装置１１ａを操作することによって、ウィルス種別情報を更新し得る。

管理者は、たとえばウィルス定義ファイルに従って、各種別のウィルスが検出されたときに制限するべき機能を特定し、当該機能が制限されるようにウィルス種別情報を更新する。

【００４６】

図６の例では、画像処理装置１の機能として、通信機能、プリント機能、スキャン機能、ファイル送信機能、および、ブラウザー機能が例示されている。

【００４７】

通信機能は、たとえば、通信インターフェース１６を利用して、他の機器とデータの送受信する機能である。プリント機能は、たとえば、プリンター装置１４を利用して、記録用紙に画像を印刷する機能である。スキャン機能は、たとえば、スキャナー装置１３を利用して、原稿の画像データを生成する機能である。ファイル送信機能は、たとえば、記憶部２３に格納されたデータおよび／またはスキャナー装置１３が生成した画像データを、通信インターフェース１６を利用して外部の装置に送信する機能である。ブラウザー機能は、たとえば、通信インターフェース１６を利用してネットワークにアクセスし、ウェブページを閲覧する機能である。

【００４８】

各機能は、機能制御部２０Ａとして動作するＣＰＵ２０によって制御される。ファイル送信機能は、ファイル送信部２０Ｂとして動作するＣＰＵ２０によって実現され得る。ブラウザー機能は、ブラウザー処理部２０Ｃとして動作するＣＰＵ２０によって実現され得る。機能制御部２０Ａ、ファイル送信部２０Ｂ、ブラウザー処理部２０Ｃのそれぞれは、プログラムモジュールとして実現され得る。

【００４９】

図６の例では、ウィルスＡ～Ｄで表される４種類のウィルスについての情報を含む。図６では、それぞれのウィルスの特性が括弧内に示され、また、制限される機能には「不可」を付し、制限されない機能には「許可」を付す。

【００５０】

ウィルスＡは、画像処理装置１の内部データ（記憶部２３等の画像処理装置１内の記憶装置に格納されたデータ）を画像処理装置１の外部へ流出させる特性を有する。ウィルス種別情報では、たとえば、ウィルスＡについて、通信機能、ファイル送信機能、および、ブラウザー機能に「不可」が付され、プリント機能およびスキャン機能には「許可」が付されている。これにより、ＣＰＵ２０は、画像処理装置１においてウィルスＡが検出されると、通信機能、ファイル送信機能、および、ブラウザー機能の実行を制限し、プリント機能およびスキャン機能の実行は制限しない。

【００５１】

ウィルスＢは、内部装置（画像処理装置１内の要素。たとえば、プリンター装置１４、スキャナー装置１３、ドキュメントフィーダー１７、および／または、給紙装置１８。）を無効化させる特性を有する。図６に従うと、ＣＰＵ２０は、ウィルスＢが検出されると、画像処理装置１のプリント機能、スキャン機能、および、ファイル送信機能の実行を制限し、通信機能およびブラウザー機能の実行を制限しない。

【００５２】

ウィルスＣは、コンピューターに強制的に特定サイトを閲覧させる特性を有する。図６に従うと、ＣＰＵ２０は、ウィルスＣが検出されると、画像処理装置１の通信機能およびブラウザー機能の実行を制限し、プリント機能、スキャン機能、およびファイル送信機能の実行を制限しない。

【００５３】

ウィルスＤは、画像処理装置１の内部データを改ざんする特性を有する。図６に従うと、ＣＰＵ２０は、ウィルスＤが検出されると、画像処理装置１のプリント機能、スキャン機能、および、ファイル送信機能の実行を制限し、通信機能およびブラウザー機能の実行を制限しない。

【００５４】

［４．ファイル種別情報］

図７は、ファイル種別情報の内容の一例を示す図である。ファイル種別情報は、ファイルの種別と画像処理装置１の機能とを関連付ける。ＣＰＵ２０は、ウィルスチェックにおいて或る種別のファイルがウィルスに感染している可能性があると判断すると、画像処理装置１において、当該種別に所与の態様（たとえば、「不可」）で関連付けられている機能の実行を制限する。

【００５５】

図７の例では、ファイル種別として「画像ファイル」と「通信設定ファイル」の２つが例示されている。「画像ファイル」は、画像を表わすファイルであり、「.img」「.png」等の予め定められた拡張子を有するファイルに対応する。「通信設定ファイル」は、通信インターフェース１６の設定情報を記述するファイルであり、一例では独特の拡張子を有するファイルに対応する。設定情報は、たとえば、画像処理装置１のＩＰ（Internet Protocol）を含む。

【００５６】

図７の「画像ファイル」では、通信機能およびブラウザー機能には「許可」が付され、プリント機能、スキャン機能、およびファイル送信機能には「不可」が付されている。これにより、ＣＰＵ２０は、ウィルスチェックにおいてウィルスに感染している可能性があると判断したファイルが画像ファイルを含む場合、プリント機能、スキャン機能、およびファイル送信機能の実行を制限し、通信機能およびブラウザー機能の実行は制限しない。

【００５７】

また、図７に従うと、ＣＰＵ２０は、ウィルスチェックにおいてウィルスに感染している可能性があると判断したファイルが通信設定ファイルを含む場合、通信機能、ファイル送信機能、およびブラウザー機能の実行を制限し、プリント機能およびスキャン機能の実行を制限しない。

【００５８】

［５．処理の流れ］

図８は、画像処理装置１においてウィルスチェックに関連して実行される処理のフローチャートである。一例では、図８の処理はＣＰＵ２０が所与のプログラムを実行することによって実現される。図８を参照して、当該処理の流れを説明する。図８の処理が開始されるタイミングの一例は、予め設定された時刻が到来したときである。他の例は、ＵＳＢインターフェース２３ＡにＵＳＢメモリー２３Ｘが装着されたときである。さらに他の例は、ユーザーが操作装置１１ａに対してウィルスチェックの実行を指示したときである。

【００５９】

ステップＳ１０にて、ＣＰＵ２０は、記憶部２３に格納された各ファイルのウィルスチェックを実行する。このとき、ＣＰＵ２０は、ウィルスチェックを実行した各ファイルについて、ファイル管理情報の「ウィルスチェック情報」を更新してもよい。

【００６０】

ステップＳ１２にて、ＣＰＵ２０は、ステップＳ１０におけるウィルスチェックにおいてウィルスが検出されたか否かを判断する。ＣＰＵ２０は、ウィルスが検出されなかったと判断すると（ステップＳ１２にてＮＯ）、図８の処理を終了する。ＣＰＵ２０は、ウィルスが検出されたと判断すると（ステップＳ１２にてＹＥＳ）、ステップＳ１４へ制御を進める。

【００６１】

ステップＳ１４にて、ＣＰＵ２０は、通信機能を中断（一時的に制限）する。これにより、通信インターフェース１６を利用した外部の装置との通信が遮断される。

【００６２】

ステップＳ１６にて、ＣＰＵ２０は、ステップＳ１０のウィルスチェックにおいて検出されたウィルスを除去するための制御を実行する。一例では、ＣＰＵ２０は、ウィルス定義ファイルにアクセスし、当該ウィルス定義ファイルを参照して、検出されたウィルスを除去する方法を取得し、当該方法を実行することによってウィルスを除去する。

【００６３】

ステップＳ１８にて、ＣＰＵ２０は、検出されたウィルスが実行された形跡があるか否かを判断する。ウィルスの実行の一例は、ウィルスに感染した実行ファイルが実行されたことである。他の例は、ウィルスに感染したドキュメントファイルが開かれたことである。実行の形跡があるか否かは、一例では、ＣＰＵ２０の動作ログが当該ファイルを実行したことを含むか否かに基づいて判断され、他の例では、当該ファイルの利用日時（ＴＵ）が前回チェック日時（ＴＣ）より遅い日時を表わすか否かに基づいて判断される。利用日時（ＴＵ）は、ファイルの履歴の一例である。ＣＰＵ２０は、ウィルスが実行された形跡があると判断すると（ステップＳ１８にてＹＥＳ）、ステップＳ２８へ制御を進め、そうでなければ（ステップＳ１８にてＮＯ）、ステップＳ２０へ制御を進める。

【００６４】

ステップＳ２０にて、ＣＰＵ２０は、検出されたウィルスが内蔵ＨＤＤ（記憶部２３）内のデータを改ざんする可能性があるか否かを判断する。一例では、ＣＰＵ２０は、検出されたウィルスの種別が特定の種別（図６のウィルスＤ、等）であるか否かを判断することによってステップＳ２０の判断を実現する。ＣＰＵ２０は、検出されたウィルスが内蔵ＨＤＤ内のデータを改ざんする可能性があると判断すると（ステップＳ２０にてＹＥＳ）、ステップＳ２８へ制御を進め、そうでなければ（ステップＳ２０にてＮＯ）、ステップＳ２２へ制御を進める。

【００６５】

ステップＳ２２にて、ＣＰＵ２０は、ステップＳ１６にて開始されたウィルスの除去が完了したか否かを判断する。ＣＰＵ２０は、ウィルスの除去が完了したと判断すると（ステップＳ２２にてＹＥＳ）、ステップＳ２４へ制御を進め、そうでなければ（ステップＳ２２にてＮＯ）、図８の処理を終了させる。

【００６６】

ステップＳ２４にて、ＣＰＵ２０は、ステップＳ１４で中断した通信機能を再開させる。これにより、画像処理装置１は、外部の装置との通信を再開する。

【００６７】

画像処理装置１では、検出されたウィルスがＣＰＵ２０によって除去されないものである場合、ステップＳ２２にてＮＯの判断がなされて、図８の処理が終了する。終了前に、ＣＰＵ２０は、画像処理装置１が当該ＣＰＵ２０によって除去されないウィルスに感染していることを報知（表示、音声、および／またはレポートの印刷）してもよい。

【００６８】

ステップＳ２６にて、ＣＰＵ２０は、画像処理装置１において通信機能の他に中断された機能があれば再開させた後、図８の処理を終了する。これにより、画像処理装置１においてウィルスが検出されたときに通信機能を一時的に中断するが、当該ウィルスが内蔵ＨＤＤ内のデータを改ざんする可能性がない場合には、当該ウィルスの除去が完了した後、通信機能を含む全ての機能を再開させる。

【００６９】

ステップＳ２８にて、ＣＰＵ２０は、ステップＳ２２と同様に、ステップＳ１６にて開始されたウィルスの除去が完了したか否かを判断する。ＣＰＵ２０は、ウィルスの除去が完了したと判断すると（ステップＳ２８にてＹＥＳ）、ステップＳ３０へ制御を進め、そうでなければ（ステップＳ２８にてＮＯ）、図８の処理を終了させる。

【００７０】

ステップＳ３０にて、ＣＰＵ２０は、ステップＳ１４で中断した通信機能を再開させる。これにより、画像処理装置１は、外部の装置との通信を再開する。

【００７１】

ステップＳ３２にて、ＣＰＵ２０は、内蔵ＨＤＤ（記憶部２３）内に格納された全てのファイルについて、ウィルスの二次感染により改ざんされた可能性があるか否かを判断する。

【００７２】

図９は、図８のステップＳ３２のサブルーチンのフローチャートである。図９を参照してステップＳ３２におけるファイル検査について説明する。

【００７３】
ステップＳ３２０にて、ＣＰＵ２０は、処理対象のファイルについて、ファイル管理情報に、前回チェック日時（ＴＣ）、利用日時（ＴＵ）、およびチェックサム値（ＣＵ）が登録されているか否かを判断する。ＣＰＵ２０は、処理対象のファイルについて、これらの３種類の情報のすべてが登録されていると判断すると（ステップＳ３２０にてＹＥＳ）、ステップＳ３２４へ制御を進め、３種類のうち少なくとも１種類が登録あれていないと判断すると（ステップＳ３２０にてＮＯ）、ステップＳ３２２へ制御を進める。
【００７４】
ステップＳ３２２にて、ＣＰＵ２０は、処理対象のファイルについて、ファイル管理情報に、前回チェック日時（ＴＣ）および利用日時（ＴＵ）が登録されているか否かを判断する。ＣＰＵ２０は、処理対象のファイルについて、これら２種類の双方が登録されていると判断すると（ステップＳ３２２にてＹＥＳ）、ステップＳ３２６へ制御を進め、少なくとも一方が登録されていないと判断すると（ステップＳ３２２にてＮＯ）、ステップＳ３２８へ制御を進める。
【００７５】
ステップＳ３２４，Ｓ３２６，Ｓ３２８のそれぞれにて、ＣＰＵ２０は、処理対象の検査方法として検査方法Ａ，Ｂ，Ｃのそれぞれを設定する。図１０は、検査方法Ａを表し、ステップＳ３２４のサブルーチンのフローチャートである。図１１は、検査方法Ｂを表し、ステップＳ３２６のサブルーチンのフローチャートである。図１２は、検査方法Ｃを表し、ステップＳ３２８のサブルーチンのフローチャートである。
【００７６】
図１０を参照して、検査方法Ａについて説明する。ステップＳＡ１０にて、ＣＰＵ２０は、前回チェック日時（ＴＣ）と利用日時（ＴＵ）とが一致しているか否かを判断する。前回チェック日時（ＴＣ）は、実行中のウィルスチェックより前に実行されたウィルスチェックの日時を意味する。一例では、前回チェック日時（ＴＣ）と利用日時（ＴＵ）とが一致することは、前回のウィルスチェック以降、処理対象のファイルに変更が加えられていないことを意味する。ＣＰＵ２０は、これらが一致していると判断すると（ステップＳＡ１０にてＹＥＳ）、ステップＳＡ１４へ制御を進め、そうでなければ（ステップＳＡ１０にてＮＯ）、ステップＳＡ１２へ制御を進める。
【００７７】
ステップＳＡ１２にて、ＣＰＵ２０は、処理対象のファイルのチェックサム値（現在のチェックサム値）を算出し、現在のチェックサム値とチェックサム値（ＣＵ）とが一致するか否かを判断する。一例では、現在のチェックサム値とチェックサム値（ＣＵ）とが一致することは、処理対象のファイルが最後に更新された後、当該ファイルに変更が加えられていないことを意味する。ＣＰＵ２０は、これらの値が一致すると判断すると（ステップＳＡ１２にてＹＥＳ）、ステップＳＡ１４へ制御を進め、そうでなければ（ステップＳＡ１２にてＮＯ）、ステップＳＡ１６へ制御を進める。
【００７８】
ステップＳＡ１４にて、ＣＰＵ２０は、処理対象のファイルが改ざんされた可能性が無い（ウィルスに感染している可能性が無い）との検査結果を生成した後、図９を介して、図８へ制御を戻す。
【００７９】
ステップＳＡ１６にて、ＣＰＵ２０は、処理対象のファイルが改ざんされた可能性が有る（ウィルスに感染している可能性が有る）との検査結果を生成した後、図９を介して、図８へ制御を戻す。
【００８０】
図１１を参照して、検査方法Ｂについて説明する。ステップＳＢ１０にて、ＣＰＵ２０は、前回チェック日時（ＴＣ）と利用日時（ＴＵ）が一致するか否かを判断する。一例では、前回チェック日時（ＴＣ）と利用日時（ＴＵ）が一致することは、処理対象のファイルが、前回ウィルスチェックが実行された後、変更を加えられていないことを意味する。Ｃ

ＰＵ２０は、これらの値が一致すると判断すると（ステップＳＢ１０にてＹＥＳ）、ステップＳＢ１４へ制御を進め、そうでなければ（ステップＳＢ１０にてＮＯ）、ステップＳＢ１６へ制御を進める。

【００８１】

ステップＳＢ１４にて、ＣＰＵ２０は、処理対象のファイルが改ざんされた可能性が無い（ウィルスに感染している可能性が無い）との検査結果を生成した後、図９を介して、図８へ制御を戻す。

【００８２】

ステップＳＢ１６にて、ＣＰＵ２０は、処理対象のファイルが改ざんされた可能性が有る（ウィルスに感染している可能性が有る）との検査結果を生成した後、図９を介して、図８へ制御を戻す。

【００８３】

図１２を参照して、検査方法Ｃについて説明する。ステップＳＣ１０にて、ＣＰＵ２０は、ファイル管理情報が、処理対象のファイルの格納時情報を含むか否かを判断する。ＣＰＵ２０は、ファイル管理情報が、処理対象のファイルの格納時情報を含むと判断すると（ステップＳＣ１０にてＹＥＳ）、ステップＳＣ１２へ制御を進め、そうでなければ（ステップＳＣ１０にてＮＯ）、ステップＳ１６へ制御を進める。

【００８４】

ステップＳＣ１２にて、ＣＰＵ２０は、ウィルスチェック情報のファイル容量（ＶＣ）と最新利用情報のファイル容量（ＶＵ）が一致するか否かを判断する。一例では、これらの値が一致する場合、処理対象のファイルに対して前回ウィルスチェックから変更が加えられていないことが推測される。ＣＰＵ２０は、これらの値が一致すると判断すると（ステップＳＣ１２にてＹＥＳ）、ステップＳＣ１４へ制御を進め、そうでなければ（ステップＳＣ１２にてＮＯ）、ステップＳＣ１６へ制御を進める。

【００８５】

ステップＳＣ１４にて、ＣＰＵ２０は、処理対象のファイルが改ざんされた可能性が無い（ウィルスに感染している可能性が無い）との検査結果を生成した後、図９を介して、図８へ制御を戻す。

【００８６】

ステップＳＣ１６にて、ＣＰＵ２０は、処理対象のファイルが改ざんされた可能性が有る（ウィルスに感染している可能性が有る）との検査結果を生成した後、図９を介して、図８へ制御を戻す。

【００８７】

図１２に示された処理では、処理対象のファイルについて格納時情報が登録されていなければ、当該ファイルはウィルスに感染している可能性があると判断される（ステップＳＣ１０にてＮＯ→ステップＳＣ１６）。一例では、格納時情報はすべてのファイルについて登録されているべき情報である。このため、所与のファイルについて格納時情報が登録されていないことは、当該ファイルの情報が改ざんされることによって格納時情報が削除された可能性が高い。図１２に示された処理は、そのようなファイルを、ウィルスに感染している可能性が有ると判定し得る。

【００８８】

上記の図９～図１２を参照した説明では、各ファイルについて、検査方法Ａ～Ｃのいずれか１つが実行されたが、検査方法Ａ～Ｃの中の２つまたはすべての方法が実行されてもよい。これにより、各ファイルについて、より精度が高く、ウィルスに感染したか否かが検査され得る。

【００８９】

図８に戻って、ステップＳ３２において、記憶部２３内の全ファイルのそれぞれについてファイル検査を実行した後、ＣＰＵ２０は、ステップＳ３４にて、ファイル検査において改ざんの可能性が有るという検査結果を生成されたファイルのリストを作成する。なお、ステップＳ３２では、記憶部２３内のファイルのうち、予め設定された条件に適合するフ

ファイルについてのみ検査が実行されてもよい。
【００９０】
ステップＳ３６にて、ＣＰＵ２０は、ステップＳ３４において作成されたリストに少なくとも１つのファイルが含まれるか否かを判断する。ＣＰＵ２０は、少なくとも１つのファイルがリストに含まれると判断すると（ステップＳ３４にてＹＥＳ）、ステップＳ３８へ制御を進め、そうでなければ、ステップＳ４２へ制御を進める。すなわち、検査されたすべてのファイルがウィルスに感染している可能性が無い場合には、ステップＳ４２へ制御が進められる。
【００９１】
ステップＳ４２にて、ＣＰＵ２０は、ステップＳ２４と同様に、画像処理装置１において通信機能の他に中断された機能があれば再開させた後、図８の処理を終了する。
【００９２】
ステップＳ３８にて、ＣＰＵ２０は、ステップＳ１０にて検出されたウィルスの種別、および、ステップＳ３６にて作成されたリスト中のファイルの種別に従って、制限される機能を設定する。当該設定の一例は、たとえば各機能の実行を制限する制限フラグをセットすることである。ＣＰＵ２０は、制限フラグがセットされている機能は、たとえ実行を要求されても、実行しない。なお、ＣＰＵ２０は、ステップＳ２４，Ｓ３０において、すべての機能についての制限フラグをリセットしてもよい。
【００９３】
たとえば、検出されたウィルスの種別が「ウィルスＣ」であり、上記リストが種別「通信設定ファイル」のファイルのみを含む場合には、通信機能、ファイル送信機能、およびブラウザー機能が制限される機能として設定され、プリント機能およびスキャン機能は制限される機能としては設定されない。このことは、ウィルスの種別が「ウィルスＣ」であることによって制限される機能が通信機能およびブラウザー機能であり（図６）、かつ、ファイルの種別が「通信設定ファイル」であることによって制限される機能は通信機能、ファイル送信機能、およびブラウザー機能である（図７）、ことに対応する。
【００９４】
この場合、コピージョブは実行可能である。コピージョブは、スキャン機能とプリント機能を利用し、通信機能、ファイル送信機能、およびブラウザー機能を利用しないからである。
【００９５】
また、Ｓｃａｎ＿ｔｏ＿Ｂｏｘジョブ（スキャンによって生成された画像データを記憶部２３内の所与のボックスに格納するジョブ）は実行可能である。Ｓｃａｎ＿ｔｏ＿Ｂｏｘジョブは、スキャン機能を利用し、通信機能、ファイル送信機能、およびブラウザー機能を利用しないからである。
【００９６】
一方、Ｓｃａｎ＿ｔｏ＿ＰＣジョブ（スキャンによって生成された画像データを外部のＰＣに送信するジョブ）は実行不能である。Ｓｃａｎ＿ｔｏ＿ＰＣジョブは、スキャン機能とファイル送信機能を利用する。ファイル送信機能が制限されているため、Ｓｃａｎ＿ｔｏ＿ＰＣジョブは実行不能である。
【００９７】
ＣＰＵ２０は、一部の機能が制限されているときに当該機能を利用するジョブの実行を指示された場合には、一部の機能が制限されているため当該ジョブが実行不能であることを報知してもよい。
【００９８】
ステップＳ４０にて、ＣＰＵ２０は、ステップＳ３４において作成されたリストを出力（たとえば、印刷）した後、図８の処理を終了する。リストが出力されることにより、ユーザーは、どのファイルがウィルスに感染した可能性があるかを認識できる。
【００９９】
［６．開示の要約］

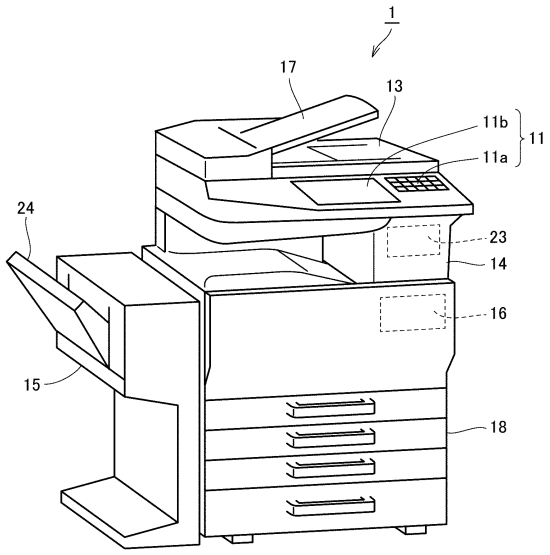
本開示は、以下のように要約され得る。
【０１００】
＜１＞画像処理装置１は、ファイルを格納する記憶部２３と、ファイルに関する２以上の機能のそれぞれを実現する機能実現部（スキャナー装置１３、プリンター装置１４、ファイル送信部２０Ｂ、ブラウザー処理部２０Ｃ、等）と、記憶部に格納されたファイルのウィルスチェックを実行する制御部（機能制御部２０Ａ）とを備える。記憶部は、ウィルスの種別と２以上の機能の中の１以上の機能とを関連付けるウィルス種別情報（図６）と、ファイル種別と２以上の機能の中の１以上の機能とを関連付けるファイル種別情報（図７）とを格納する。制御部は、２以上の機能のうち、ウィルスチェックにおいて検出されたウィルスの種別に関連付けられた機能（たとえば、種別「ウィルスＣ」について「不可」を付与された、通信機能とブラウザー機能）、および、記憶部に格納されたファイルの中のウィルスチェックによって検出されたウィルスに感染している可能性があるファイルの種別に関連付けられた機能（たとえば、種別「通信設定ファイル」について「不可」を付与された、通信機能とファイル送信機能とブラウザー機能）を制限する（ステップＳ３８）。
【０１０１】
＜２＞制御部は、ウィルスチェックにおいて検出されたファイルが実行されておらず、かつ、ウィルスチェックにおいて検出されたウィルスの種別が記憶部内のファイルを改ざんしない種別である場合には、ウィルスが除去された後、２以上の機能の制限を解除してもよい（ステップＳ２４）。
【０１０２】
＜３＞制御部は、ファイルが実行されたか否かを、ファイルへのアクセスログ、または、記憶部に格納されたファイルの履歴に基づいて判断してもよい（ステップＳ１８）。
【０１０３】
＜４＞制御部は、ウィルスチェックにおいて検出されたウィルスの種別が記憶部内のファイルを改ざんする種別である場合に（ステップＳ２０にてＹＥＳ）、記憶部内のファイルに対してウィルスチェックにおいて検出されたウィルスに感染している可能性があるか否かを検査してもよい（ステップＳ３２）。
【０１０４】
＜５＞２以上の機能は、外部機器と通信する機能（通信機能）を含んでいてもよい。制御部は、ウィルスチェックにおいてウィルスが検出された場合に、外部機器と通信する機能を制限した後、当該ウィルス除去を実行してもよい（ステップＳ１４，Ｓ１６）。
【０１０５】
＜６＞制御部は、ウィルスに感染している可能性があるファイルを報知してもよい（ステップＳ４０）。
【０１０６】
＜７＞制御部は、記憶部内の各ファイルに対して、当該ファイルが記憶部内に格納されたときの当該ファイルの情報（図３等の「格納時情報」）、前回のウィルスチェックのときの当該ファイルの情報（図３等の「ウィルスチェック情報」）、最新の利用時の当該ファイルの情報（図３等の「最新利用情報」）、および、今回のウィルスチェックのときの当該ファイルの情報（図１０のステップＳＡ１２の「現在のチェックサム値」）の中の少なくとも一つを利用して、各ファイルがウィルスに感染している可能性があるか否かを検査する（図１０～図１２）。
【０１０７】
＜８＞最新の利用時の当該ファイルの情報は、最新の利用時の日時を特定する情報（利用日時（ＴＵ））を含んでいてもよい。前回のウィルスチェックのときの当該ファイルの情報は、前回のウィルスチェックの日時を特定する情報（図３等の「前回チェック日時（ＴＣ）」）と、前回のウィルスチェックのときの当該ファイルのチェックサム値（図３等の「チェックサム値（ＣＣ）」）とを含んでいてもよい。今回のウィルスチェックのときの当該ファイルの情報は、今回のウィルスチェックのときの当該ファイルのチェックサム値

（図１０のステップＳＡ１２の「現在のチェックサム値」）を含んでいてもよい。
【０１０８】
今回開示された各実施の形態は全ての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内での全ての変更が含まれることが意図される。また、実施の形態および各変形例において説明された発明は、可能な限り、単独でも、組合わせても、実施することが意図される。
【符号の説明】
【０１０９】
１　画像処理装置、１１　操作パネル、１１ａ　操作装置、１１ｂ　ディスプレイ、１３　スキャナー装置、１４　プリンター装置、１５　フィニッシャー装置、１６　通信インターフェース、１７　ドキュメントフィーダー、１８　給紙装置、２０　ＣＰＵ、２０Ａ　機能制御部、２０Ｂ　ファイル送信部、２０Ｃ　ブラウザー処理部。

【図面】

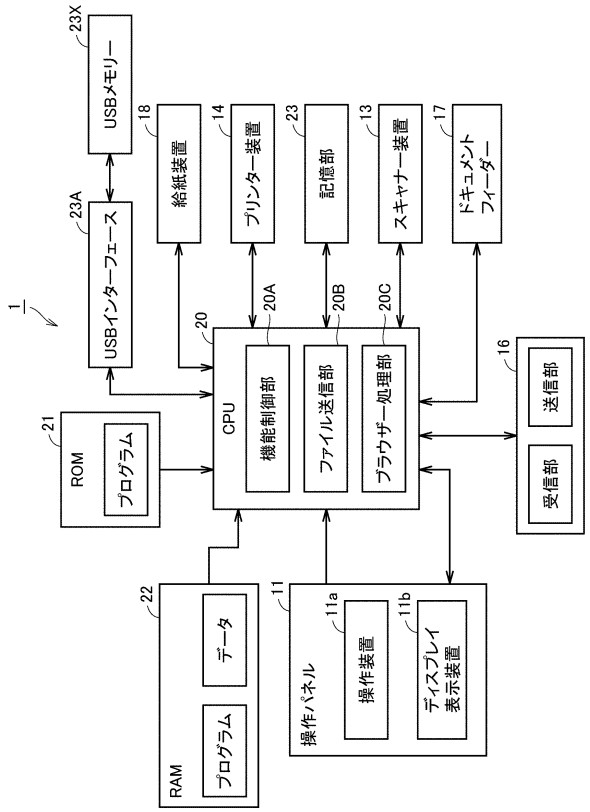
【図１】

図1



【図２】

図2



【図３】

図3

ファイル管理情報

ファイル名	格納時情報				ウィルスチェック情報			最新利用情報		
	格納日時(TS)	作成日時(TP)	ファイル容量(VS)	チェックサム値(CS)	前回チェック日時(TC)	ファイル容量(VC)	チェックサム値(CC)	利用日時(TU)	ファイル容量(VU)	チェックサム値(CU)
NM1	TS1	TP1	VS1	CS1	TC1	VC1	CC1	TU1	VU1	CU1
NM2	TS2	TP2	VS2	CS2	–	–	–	–	–	–
:	:	:	:	:	:	:	:	:	:	:

【図４】

図4

ファイル管理情報

ファイル名	格納時情報				ウィルスチェック情報			最新利用情報		
	格納日時(TS)	作成日時(TP)	ファイル容量(VS)	チェックサム値(CS)	前回チェック日時(TC)	ファイル容量(VC)	チェックサム値(CC)	利用日時(TU)	ファイル容量(VU)	チェックサム値(CU)
NM1	TS1	TP1	VS1	CS1	TC1	VC1	CC1	TU1	VU1	CU1
NM2	TS2	TP2	VS2	CS2	–	–	–	TU2	VU2	CU2
:	:	:	:	:	:	:	:	:	:	:

【図５】

図5

ファイル管理情報

ファイル名	格納時情報				ウィルスチェック情報			最新利用情報		
	格納日時(TS)	作成日時(TP)	ファイル容量(VS)	チェックサム値(CS)	前回チェック日時(TC)	ファイル容量(VC)	チェックサム値(CC)	利用日時(TU)	ファイル容量(VU)	チェックサム値(CU)
NM1	TS1	TP1	VS1	CS1	TC2	VC1	CC1	TU1	VU1	CU1
NM2	TS2	TP2	VS2	CS2	TC2	VC2	CC2	TU2	VU2	CU2
：	：	：	：	：	：	：	：	：	：	：

【図６】

図6

ウィルス種別情報

	通信機能	プリント機能	スキャン機能	ファイル送信機能	ブラウザー機能
ウィルスA（内部データを流出）	不可	許可	許可	不可	不可
ウィルスB（内部装置を無効化）	許可	不可	不可	不可	許可
ウィルスC（特定サイトの閲覧）	不可	許可	許可	許可	不可
ウィルスD（内部データを改ざん）	許可	不可	不可	不可	許可
：	：	：	：	：	：

【図７】

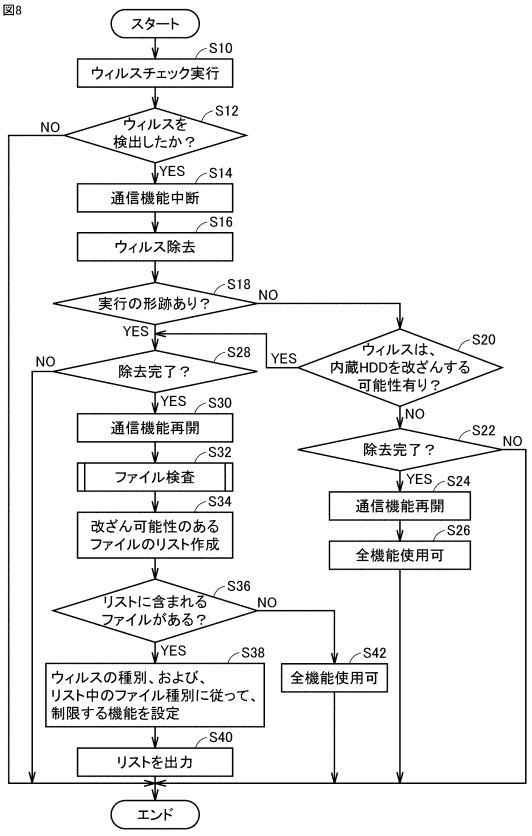
図7

ファイル種別情報

	通信機能	プリント機能	スキャン機能	ファイル送信機能	ブラウザー機能
画像ファイル	許可	不可	不可	不可	許可
通信設定ファイル	不可	許可	許可	不可	不可
：	：	：	：	：	：

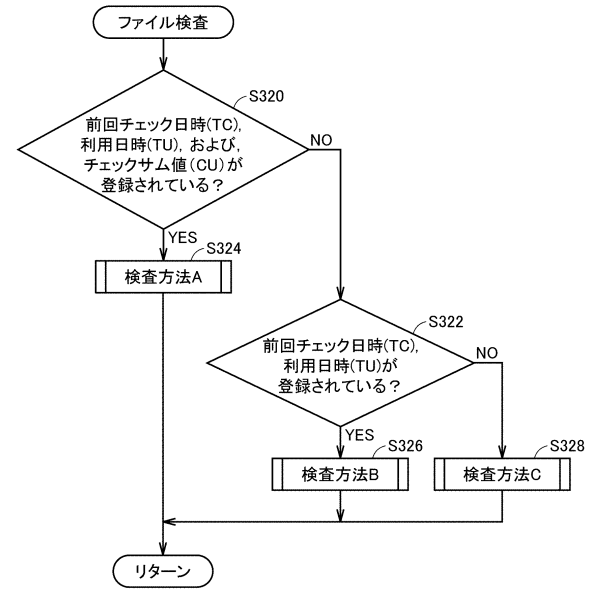
【図８】

図8



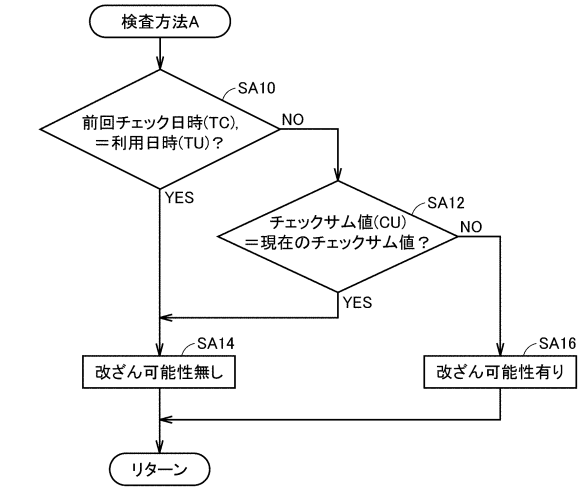
【図９】

図9



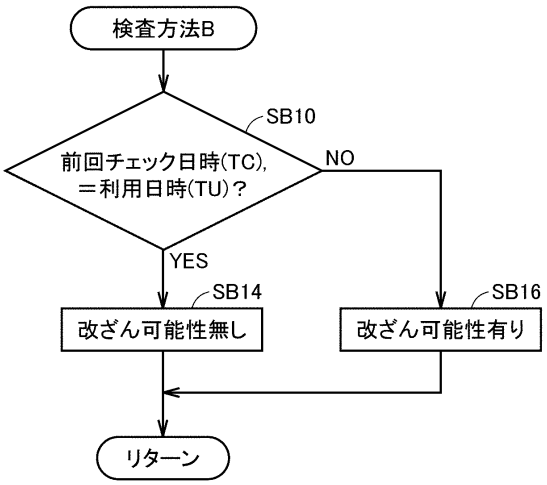
【図１０】

図10



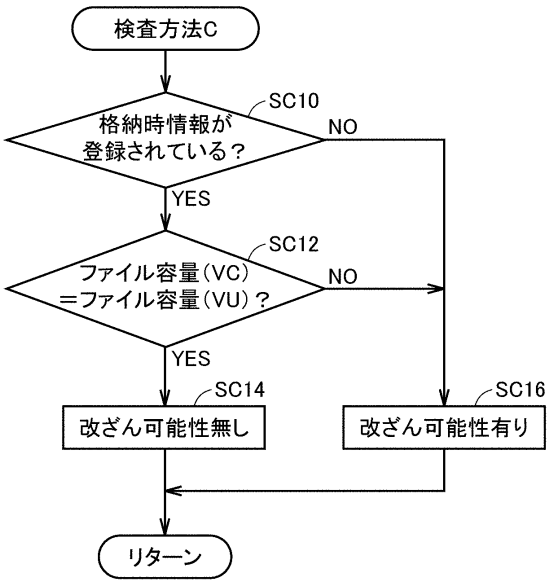
【図１１】

図11



【図１２】

図12



フロントページの続き

(56)参考文献 特開２０１１－０６５４８３（ＪＰ，Ａ）
米国特許出願公開第２０１１／００６７１００（ＵＳ，Ａ１）
中国特許出願公開第１０２０２５８６９（ＣＮ，Ａ）
特開２０１１－０８２８１４（ＪＰ，Ａ）
特開２０１８－０７３０３５（ＪＰ，Ａ）
特開２０１０－１４１７０５（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ１２／００－１２／２２，１２／５０－１２／６６，４５／００－４９／９０５７