(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-213421
(P2007-213421A)
(43)公開日　平成19年8月23日(2007.8.23)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	550A	5B017
G06F 12/00	(2006.01)	G06F	12/00	537A	5B082

審査請求 未請求　請求項の数 9　ＯＬ　（全 18 頁）

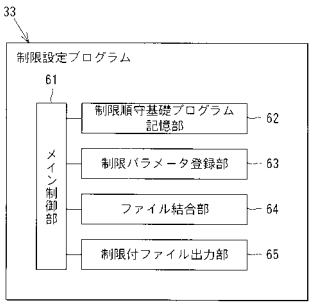
(21)出願番号　特願2006-34111 (P2006-34111)
(22)出願日　平成18年2月10日 (2006.2.10)

(71)出願人　502439201
株式会社弘染塾
京都府相楽郡精華町光台７丁目２５番地１０
(74)代理人　100067747
弁理士　永田　良昭
(74)代理人　100121603
弁理士　永田　元昭
(72)発明者　星野　洋一郎
京都府相楽郡精華町光台７丁目２５番地１０　株式会社弘染塾内
(72)発明者　黒川　ひとみ
京都府相楽郡精華町光台７丁目２５番地１０　株式会社弘染塾内

Ｆターム(参考)　5B017 AA01　AA06　BA06　CA16
5B082 GA11

(54)【発明の名称】ファイル操作制限システム、制限順守プログラム、および制限設定プログラム

(57)【要約】
【課題】ファイルに対して種々の制限をかけることのできるファイル操作制限システム１、制限順守プログラム７０、および制限設定プログラム３３を提供し、重要なファイルを管理することの利便性を向上させる。
【解決手段】制限対象ファイル８０に対する操作制限の設定入力を受け付ける入力装置１３と、入力された操作制限を順守する制限順守プログラム７０を前記制限対象ファイル８０に結合して制限付ファイル２３を作成するファイル結合部６４と、作成した制限付ファイル２３を出力する記憶装置１１とを備えた。
【選択図】図３



【特許請求の範囲】
【請求項１】
制限対象ファイルに対する操作制限の設定入力を受け付ける入力手段と、
入力された操作制限を順守する制限順守プログラムを前記制限対象ファイルに結合して制限付ファイルを作成する制限付ファイル作成手段と、
作成した制限付ファイルを出力する出力手段とを備えた
ファイル操作制限システム。
【請求項２】
前記制限順守プログラムは、アプリケーションプログラムに組み込まれて機能拡張する機能拡張プログラムで構成した
請求項１記載のファイル操作制限システム。
【請求項３】
前記アプリケーションプログラムと異なるプログラムによって前記制限付きファイルが複製されることを防止する複製防止プログラムを備えた
請求項１または2記載のファイル操作制限システム。
【請求項４】
前記入力手段は、デフォルト設定で前記制限対象ファイルに対して全ての操作を拒否しておき、許容する操作を設定入力させる構成とした
請求項１、２または３記載のファイル操作制限システム。
【請求項５】
前記入力手段と制限付ファイル作成手段と出力手段とを有するクライアント端末と、
該クライアント端末と通信回線を通じて通信可能に接続したサーバとを備え、
前記サーバに、
前記入力手段で設定入力された制限対象ファイルについての操作制限を記憶する操作制限データベースと、
制限対象ファイルとして操作制限がなされているか否かを問合せる問合せ情報を受け付ける問合せ受付手段と、
問い合わされたファイルが制限対象ファイルであれば操作制限の内容を応答する応答手段とを備え、
前記制限順守プログラムを、制限付ファイルが操作された際に前記サーバに前記問合わせ情報を送信し、該サーバから受信した操作制限の内容に従って操作制限する構成にした
請求項１から４のいずれか１つに記載のファイル操作制限システム。
【請求項６】
サーバとクライアント端末とを通信回線を通じて通信可能に接続したファイル操作制限システムであって、
前記サーバに、
制限対象ファイルについての操作制限を記憶する操作制限データベースと、
制限対象ファイルとして操作制限がなされているか否かを問合せる問合せ情報を受け付ける問合せ受付手段と、
問い合わされたファイルが制限対象ファイルであれば操作制限の内容を応答する応答手段とを備え、
前記クライアント端末に、
該クライアント端末に設けられた記憶手段に記憶されているファイルに対する操作を検知する操作検知手段と、
操作を検知したファイルについて操作制限がなされているか前記サーバに問合せる操作制限問合せ手段と、
サーバから応答を受け付ける応答受付手段と、
受け付けた応答に基づいて前記ファイルの操作を許容または拒否する制限順守手段とを備えた
ファイル操作制限システム。

【請求項７】
サーバとクライアント端末とを通信回線を通じて通信可能に接続したファイル操作制限システムであって、
前記サーバに、
制限対象ファイルについての操作制限を記憶する操作制限データベースと、
前記通信回線を通過するファイルに前記制限対象ファイルが存在するか検知する検知手段と、
制限対象ファイルを検知した場合に該ファイルに対する操作が制限されている操作か否か判定する判定手段とを備え、
前記クライアント端末に、
前記制限順守手段から操作制限についての応答を受け付けるまで操作を実行しない待機手段と、
制限されていない操作であった場合に操作を許容し、制限されている操作であった場合に操作を拒否する制限順守手段とを備えた
ファイル操作制限システム。
【請求項８】
コンピュータの記憶手段に制限対象ファイルと結合して記憶され、
コンピュータの入力手段で自身が操作された際に当該操作が制限されている操作であるか否か判定する判定処理と、
制限されていると判定した場合に操作制限を順守する操作制限順守処理と、
制限されていないと判定した場合に前記制限対象ファイルを該当するアプリケーションプログラムに渡す操作許容処理とをコンピュータの制御手段に実行させる
制限順守プログラム。
【請求項９】
制限対象ファイルに対する操作制限の内容入力をコンピュータの入力手段で受け付ける入力受付処理と、
受け付けた操作制限の内容を登録した制限順守プログラムを作成するプログラム作成処理と、
作成した制限順守プログラムを前記制限対象ファイルと結合する結合処理と、
結合したファイルを出力する出力処理とをコンピュータの制御手段に実行させる
制限設定プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、例えばコピー禁止や印刷禁止といったように管理する対象の制限対象ファイルを確実に管理するようなファイル操作制限システム、制限順守プログラム、および制限設定プログラムに関する。
【背景技術】
【０００２】
従来、コンピュータでは守秘性の低いファイルから守秘性の高い重要なファイルまで様々なファイルが利用されている。このような種々のファイルは、ファイルを作成した本人が使用する分には問題がなくとも、ファイルを他人に開示する際に問題が生じる場合がある。特に重要なファイルについては、例えば他人に閲覧許容して感想を聞きたいが、複写されて第三者に渡されることや、その後はいつでも閲覧可能になることや、プリントされてそのプリントが第三者に見られるといったことを防止したいことがある。このような場合、ファイルを情報発信する本人ができる対応としては、ファイルの受け取り側に厳重注意を呼びかけ、後はファイルの受け取り側を信用するしかなかった。このため、仮にファイルの受け取り側に悪気がなくとも、コンピュータ内に重要なファイルが残り続け、後々に問題を生じさせる原因になることが考えられた。
【０００３】

一方、ファイルについて制限するものとして、所定時間が経過するとファイルを削除するファイルデータ削除プログラムが知られている（特許文献１参照）。このファイルデータ削除プログラムは、ファイルのヘッダ部に埋め込まれたファイルデータに基づいて、制限時間が経過していたらファイルデータを削除するものである。

【０００４】

しかし、このファイルデータ削除プログラムは、制限時間が経過したらファイルを削除することしかできなかった。

【０００５】

【特許文献１】特開２００５－３１６９０３号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

この発明は、上述の問題に鑑み、ファイルに対して種々の制限をかけることのできるファイル操作制限システム、制限順守プログラム、および制限設定プログラムを提供し、重要なファイルを管理することの利便性を向上させることを目的とする。

【課題を解決するための手段】

【０００７】

この発明は、制限対象ファイルに対する操作制限の設定入力を受け付ける入力手段と、入力された操作制限を順守する制限順守プログラムを前記制限対象ファイルに結合して制限付ファイルを作成する制限付ファイル作成手段と、作成した制限付ファイルを出力する出力手段とを備え、ファイル操作に対して制限をかけることを特徴とする。

【発明の効果】

【０００８】

この発明により、ファイルに対して種々の制限をかけることができ、重要なファイルを管理することの利便性を向上させることができる。

【発明を実施するための最良の形態】

【０００９】

この発明の一実施形態を以下図面と共に説明する。

【実施例１】

【００１０】

図１は、ファイル操作制限システム１のブロック図を示す。

ファイル操作制限システム１は、ハードディスク等で構成される記憶装置１１、ＣＰＵ等で構成される制御装置１２、マウスおよびキーボード等で構成される入力装置１３、液晶ディスプレイまたはＣＲＴディスプレイ等で構成される表示装置１４、ＬＡＮボードまたは無線ＬＡＮカード等で構成される通信装置１５、および、フレキシブルディスクやＣＤ等の記憶媒体に対してデータの読み書き処理を実行するフレキシブルディスクドライブやＣＤドライブ等で構成される媒体処理装置１６等を有するコンピュータで構成されている。

【００１１】

記憶装置１１には、各種のアプリケーション（アプリケーションプログラムの略、以下同じ）で使用するデータ等の通常ファイル２１と、通常ファイルに制限がかけられた制限付ファイル２３とが記憶されている。

【００１２】

制御装置１２には、オペレーションシステムであるＯＳ３１、ＯＳ３１上で動作する各種のアプリケーション３２，３５、およびアプリケーション３２のアドイン（Ａｄｄ－ｉｎ）機能（別名Ａｄｄ－ｏｎ、Ｐｌｕｇ－ｉｎとも言う）として動作する制限設定プログラム（ＰＧ）３３が搭載されている。また、アプリケーション３２のアドイン機能として動作する制限順守プログラム（ＰＧ）７０も搭載されている。なお、アドイン機能とは、ソフトウェアの機能を拡張する機能拡張プログラムの一種であり、ソフトウェアに組み込まれて該ソフトウェアの機能を拡張する。

【００１３】
図２は、アプリケーション３２のブロック図を示す。
アプリケーション３２は、メイン制御部４１と、ファイル新規作成部４２、ファイルオープン部４３、ファイル保存部４４、ファイルクローズ部４５、印刷部４６、メール添付部４７、およびアドイン対応部４８が設けられている。
【００１４】
メイン制御部４１は、アプリケーション全体を制御するメインプログラムである。
ファイル新規作成部４２は、新規の通常ファイル２１を作成するモジュールである。
ファイルオープン部４３は、通常ファイル２１や制限付ファイル２３を開くモジュールである。
【００１５】
ファイル保存部４４は、新規作成あるいはオープンしたファイルを記憶装置１１に保存する、あるいは媒体処理装置１６によって記憶媒体に保存するモジュールである。
【００１６】
ファイルクローズ部４５は、新規作成あるいはオープンしたファイルを保存しないで閉じるモジュールである。
【００１７】
印刷部４６は、新規作成あるいはオープンしたファイルをファイル操作制限システム１としてのコンピュータに接続された適宜の印刷装置（プリンタ）に印刷出力するモジュールである。
【００１８】
メール添付部４７は、新規作成あるいはオープンしたファイルを、通信装置１５を解して送信するメールに添付するモジュールである。
【００１９】
アドイン対応部４８は、アドインプログラムを読み込んで使用可能にするモジュールであり、アプリケーション３２の機能を拡張可能にするものである。
【００２０】
図３は、制限設定プログラム３３のブロック図を示す。
制限設定プログラム３３は、メイン制御部６１、制限順守基礎プログラム記憶部６２、制限パラメータ登録部６３、ファイル結合部６４、および制限付ファイル出力部６５で構成される。
【００２１】
メイン制御部６１は、プログラム全体を制御するメインプログラムである。
制限順守基礎プログラム記憶部６２は、制限内容が指定される前の制限順守プログラムであり、制限順守プログラムの基礎となるプログラムである。
【００２２】
制限パラメータ登録部６３は、利用者による制限パラメータの入力を受け付けて制限内容の登録処理を実行する部分である。
ファイル結合部６４は、制限対象ファイルに制限順守プログラムを結合して制限付きファイルを作成する処理を実行する部分である。
【００２３】
制限付ファイル出力部６５は、ファイル結合部６４で作成した制限付きファイルを、記憶装置１１の任意の場所に記憶させる、または通信装置１５を介して他のコンピュータの記憶装置の任意の場所に記憶させる、あるいは媒体処理装置１６を介して記憶媒体に記憶させるなど、制限付きファイルを出力する処理を実行する部分である。
【００２４】
図４は、制限付ファイル２３のブロック図を示す。
制限付ファイル２３は、制限順守プログラム７０と、制限対象ファイル８０とで構成される。従って、コンピュータ上では通常のファイル（制限対象ファイル８０）として見え、見かけ上は制限順守プログラム７０が裏に隠れているようになる。

【００２５】
制限順守プログラム７０は、メイン制御部７１、アドイン組込部７２、オープン制御部７３、保存制御部７４、印刷制御部７５、メール添付制御部７６、パラメータ記憶部７７、およびファイル複製防止部７８で構成されている。
【００２６】
メイン制御部７１は、プログラム全体を制御するメインプログラムである。
アドイン組込部７２は、アプリケーション３２にアドインプログラムとして組み込む処理を実行する部分である。
【００２７】
オープン制御部７３は、ファイルオープンについての制限がかかっているか否かパラメータ記憶部７７を参照して判定し、オープン可否を制御する処理を実行する部分である。
【００２８】
保存制御部７４は、ファイル保存についての制限がかかっているか否かパラメータ記憶部７７を参照して判定し、保存可否を制御する処理を実行する部分である。この保存可否の制限は、保存場所にかかわらず保存を制限する、フレキシブルディスクやＣＤ－Ｒなどの携帯可能な記憶媒体への保存を制限する、あるいはコンピュータ自身以外に設けられた記憶手段（前記記憶媒体や通信接続された他のコンピュータ等）への保存を制限するなど、適宜の制限とすることができる。
【００２９】
印刷制御部７５は、印刷についての制限がかかっているか否かパラメータ記憶部７７を参照して判定し、印刷可否を制御する処理を実行する部分である。
メール添付制御部７６は、ファイルのメール添付についての制限がかかっているか否かパラメータ記憶部７７を参照して判定し、メール添付可否を制御する処理を実行する部分である。
【００３０】
パラメータ記憶部７７は、各種操作に対しての制限をパラメータとして記憶している部分である。
ファイル複製防止部７８は、制限付ファイル２３自身がＯＳ３１レベルの操作によって複製（コピー）されることを防止する処理を実行する部分である。なお、複製防止だけでなく、移動防止や削除防止を兼ねても良い。
【００３１】
図５は、制限パラメータを登録する際に表示装置１４に表示する制限設定画面９０の画面イメージ図を示す。
制限設定画面９０は、閲覧制限、保存制限、印刷制限、およびメール添付制限といった制限項目毎に、拒否ラジオボタン９１、許可ラジオボタン９２、許可回数入力ボックス９３、および削除チェックボックス９４が設けられており、さらに設定ボタン９５とキャンセルボタン９６が設けられている。ここで、最初に制限設定画面９０を表示したデフォルト状態では、全ての拒否ラジオボタン９１がチェックされており、そのまま設定登録した場合にファイルに対する操作が全くできないようにしている。
【００３２】
拒否ラジオボタン９１は、その制限項目についての操作を拒否するためのボタンである。
許可ラジオボタン９２は、その制限項目についての操作を許可するためのボタンである。この許可ラジオボタン９２と前記拒否ラジオボタン９１とは、択一的にいずれか一方が必ず選択される。
【００３３】
許可回数入力ボックス９３は、その制限項目についての操作を許可する回数を選択あるいは入力許容するコンボボックスであり、図中の矢印Ａに示すように、所定の整数回、あるいは無制限を選択できる。
【００３４】

削除チェックボックス９４は、前記許可回数入力ボックス９３で規定された回数の操作が行われた際に当該ファイルを削除するか否かチェックにより選択許容するボックスである。なお、許可回数入力ボックス９３で数回が入力されると削除チェックボックス９４を自動的にチェックし、利用者の操作によってチェックが外されない限り、ファイル操作が整数回行われるとファイルを削除することが好ましい。

【００３５】

設定ボタン９５は、拒否ラジオボタン９１、許可ラジオボタン９２、許可回数入力ボックス９３、および削除チェックボックス９４で設定指示された内容を記憶するためのボタンであり、押下されることで前記内容を記憶装置１１等に書き込むボタンである。

キャンセルボタン９６は、ファイルに対する操作制限の指定をキャンセルするボタンである。

【００３６】

以上の構成により、通常ファイル２１から制限付ファイル２３を作成して出力し、制限付ファイル２３に対して任意の操作制限をかけることができる。

【００３７】

図６は、制限設定プログラム３３に基づいて制御装置１２が実行する動作のフローチャートを示す。

制限設定プログラム３３は、操作制限を設定する対象ファイルとして通常ファイル２１を受け取るまで待機する（ステップＳ１：ＮＯ）。

【００３８】

通常ファイル２１を受け取ると（ステップＳ１：ＹＥＳ）、制限設定プログラム３３は、図５に示した制限設定画面９０を表示装置１４に表示し、制限設定画面９０への利用者の入力（拒否ラジオボタン９１、許可ラジオボタン９２、許可回数入力ボックス９３、および削除チェックボックス９４）を許容し、制限設定を受け付ける（ステップＳ２）。

【００３９】

設定ボタン９５が押下されると（ステップＳ３：ＹＥＳ）、制限設定プログラム３３は、制限順守基礎プログラム記憶部６２から制限順守基礎プログラムを読み出し（ステップＳ４）、制限順守基礎プログラムのパラメータ記憶部に制限パラメータを制限パラメータ登録部６３で登録し（ステップＳ５）、カスタマイズされた制限順守プログラム７０を作成する。

【００４０】

そして、制限設定プログラム３３は、作成した制限順守プログラム７０をステップＳ１でインプット許容した通常ファイル２１とファイル結合部６４で結合し（ステップＳ６）、この結合によって作成した制限付ファイル２３を制限付ファイル出力部６５で出力して（ステップＳ７）、処理を終了する。

【００４１】

前記ステップＳ３でキャンセルボタン９６が押下された場合には（ステップＳ３：ＮＯ）、制限付ファイル２３を作成することなく終了する。

【００４２】

以上の動作により、通常ファイル２１に対してかけたい操作制限の入力を許容し、入力された操作制限をかけた制限付ファイル２３を作成して出力することができる。

【００４３】

制限設定の際には、全ての制限項目についてデフォルト設定で拒否する設定となっているため、利用者は操作許可する項目だけ設定入力すればよく、操作が容易であると共に、操作拒否すべき項目を拒否設定し忘れることを防止できる。

【００４４】

図７は、制限順守プログラム７０に基づいて制御装置１２が実行する動作のフローチャートを示す。

制限順守プログラム７０は、ＯＳ３１上で自分自身が複製（コピー）されたか否か検知しており、複製されたことを検知すると（ステップＳ１１：ＹＥＳ）、複製を防止し（ス

テップＳ１２）、表示装置１４にエラーメッセージを表示してステップＳ１に処理を戻す。なお、この実施例では制限順守プログラム７０自身が複製防止する構成としているが、ＯＳ３１に常駐ソフトウェアを別途インストールし、この常駐ソフトウェアが制限付ファイル２３のＯＳ３１上での複製を防止するように構成してもよい。

【００４５】

複製が行われなかった場合（ステップＳ１１：ＮＯ）、制限付ファイル２３がダブルクリックされる等によってオープン操作されるまで待機する（ステップＳ１４：ＮＯ）。このオープン操作は、例えばアプリケーション３２のファイルオープン部４３によってオープンされる、あるいはダブルクリックによりオープンされるといった方法がある。ダブルクリックによるオープンでは、ダブルクリックされた際に拡張子等の識別子からどのアプリケーションで用いられるファイルであるかＯＳ３１が判別し、該当するアプリケーションにファイルが渡されることによってファイルオープンが適切に実行される。

【００４６】

オープン操作されると（ステップＳ１４：ＹＥＳ）、制限付ファイル２３内に隠れている制限順守プログラム７０は、アドイン組込部７２によってアプリケーション３２にアドインプログラムとして読み込まれる（ステップＳ１５）。このアドインプログラムとしての読み込みは、アプリケーション３２のアドイン対応部４８がアドイン機能に対応していることにより実現される。

【００４７】

アプリケーション３２に読み込まれた制限順守プログラム７０は、アドインプログラムとして機能し、制限付ファイル２３のパラメータ記憶部７７を参照して、閲覧が許可されているか否か判定する（ステップＳ１６）。

【００４８】

閲覧が拒否されていればステップＳ３１に処理を進め（ステップＳ１６：ＮＯ）、閲覧が許可されていれば（ステップＳ１６：ＹＥＳ）、制限付ファイル２３内の制限対象ファイル８０をアプリケーション３２に渡して表示許容する（ステップＳ１７）。

【００４９】

制限順守プログラム７０は、閲覧許可の回数が決まっていれば閲覧許可回数を１減算し、この減算後の値をパラメータ記憶部７７に更新登録する（ステップＳ１８）。

【００５０】

制限順守プログラム７０は、パラメータ記憶部７７を参照し、保存が許可されていれば（ステップＳ１９：ＹＥＳ）、アプリケーション３２がオープンしている制限対象ファイル８０を保存許容するようにアプリケーション３２を制御する（ステップＳ２１）。

【００５１】

利用者によるアプリケーション３２のファイル保存部４４の操作で制限対象ファイル８０が保存操作されると（ステップＳ２２）、制限順守プログラム７０は、制限付ファイル２３を保存する（ステップＳ２３）。このとき、保存許容回数を１減算して制限付ファイル２３を上書き保存または複製保存する、あるいは１回の閲覧のみ許容するようにパラメータ記憶部７７を更新した制限付ファイル２３を上書き保存または複製保存するなど、適宜の制限をかけた上で保存することが望ましい。

【００５２】

制限順守プログラム７０は、現在オープンしている状態の制限対象ファイル８０について、パラメータ記憶部７７に保存許容回数が規定されていればこの保存許容回数を１減算し、この減算後の値をパラメータ記憶部７７に更新登録する（ステップＳ２４）。

【００５３】

前記ステップＳ１９で保存拒否と判定した場合は（ステップＳ１９：ＮＯ）、制限順守プログラム７０は、オープンしている制限対象ファイル８０を保存できないようにアプリケーション３２を制御し（ステップＳ２０）、ステップＳ２５に処理を進める。

【００５４】

制限順守プログラム７０は、パラメータ記憶部７７を参照してメール添付が許容されて

いるか拒否されているか判定し、許容されていれば（ステップＳ２５：ＹＥＳ）、アプリケーション３２をメール添付可能に制御する（ステップＳ２７）。

【００５５】

利用者によるアプリケーション３２のメール添付部４７の操作でメール添付が選択されると（ステップＳ２８：ＹＥＳ）、制限順守プログラム７０は、制限付ファイル２３をメールソフトであるアプリケーション３５に渡してメールに添付する（ステップＳ２９）。

【００５６】

制限順守プログラム７０は、現在オープンしている状態の制限対象ファイル８０について、パラメータ記憶部７７にメール添付許容回数が規定されていればこのメール添付許容回数を１減算し、この減算後の値をパラメータ記憶部７７に更新登録する（ステップＳ３０）。

【００５７】

前記ステップＳ２５でメール添付が拒否されていると判定した場合は（ステップＳ２５：ＮＯ）、メールソフトであるアプリケーション３５に制限付ファイル２３を渡せないようにして、メールへの添付操作を制限し（ステップＳ２６）、ステップＳ３１に処理を進める。

【００５８】

前記ステップＳ１６で、制限付ファイル２３が閲覧不可であると判定した場合は（ステップＳ１６：ＮＯ）、制限対象ファイル８０を表示装置１４の画面上にオープンせず、ステップＳ３１に処理を進める。

【００５９】

制限順守プログラム７０は、パラメータ記憶部７７を参照して印刷が許容されているか拒否されているか判定し、許容されていれば（ステップＳ３１：ＹＥＳ）、アプリケーション３２を印刷可能に制御する（ステップＳ３３）。

【００６０】

利用者によるアプリケーション３２の印刷部４６の操作で印刷が選択されると（ステップＳ３４：ＹＥＳ）、制限順守プログラム７０は、制限対象ファイル８０をコンピュータに接続された適宜の印刷装置に送信し、制限対象ファイル８０を印刷出力する（ステップＳ３５）。

【００６１】

制限順守プログラム７０は、現在オープンしている状態の制限対象ファイル８０について、パラメータ記憶部７７に印刷許容回数が規定されていればこの印刷許容回数を１減算し、この減算後の値をパラメータ記憶部７７に更新登録する（ステップＳ３６）。

【００６２】

前記ステップＳ３１で印刷拒否されていると判定した場合には（ステップＳ３１：ＮＯ）、アプリケーション３２を印刷できないように制御する（ステップＳ３２）。

【００６３】

制限順守プログラム７０は、削除条件に該当すれば（ステップＳ３７：ＹＥＳ）、自分自身となる制限付ファイル２３を削除する（ステップＳ３８）。ここで削除条件は、制限設定画面９０で削除チェックボックス９４にチェックされた制限項目について許可回数に到達したことを条件とする。従って、許可回数に到達するまでは削除せず、許可回数に到達した場合に削除する。

【００６４】

以上の動作により、制限付ファイル２３に対して閲覧操作、保存操作、メール添付操作、および印刷操作といった操作を行う際に、制限設定プログラム３３で設定された制限の範囲内で操作許容することができる。

ＯＳ３１レベルでの制限付ファイル２３の複写も拒否するため、複写によって操作制限の意味がなくなることもなく、確実な操作制限を実現できる。

【００６５】

制限順守プログラム７０は、アプリケーション３２のアドインプログラムとして機能す

るため、アドインプログラムを許容するアプリケーションであれば容易に操作制限をかけることができる。

【００６６】

また、保存制御部７４による保存操作の制限として、携帯可能な記憶媒体への保存を制限可能にしているため、重要なファイルが携帯可能な記憶媒体に保存されて外部へ持ち出されることを防止できる。

【００６７】

また、印刷制御部７５により印刷可否を制御できるため、重要なファイルが印刷されることを防止でき、印刷された情報が他人に見られて情報漏洩に繋がるといったことを防止できる。

【００６８】

なお、上述した実施例１では、制限順守プログラム７０をアドインプログラムで構成したが、この制限順守プログラム７０をアプリケーション３２に組み込んで組み込み型のアプリケーションとして提供してもよい。この場合、制限付ファイル２３内の制限順守プログラム７０は、メイン制御部７１とパラメータ記憶部７７とファイル複製防止部７８とが存在すればよい。この場合でも、上述した実施例１と同様の効果が得られる。

【００６９】

また、制限付ファイル２３内に設けられた制限順守プログラム７０を無効にされることを防止する制限無効化防止プログラムを制限付ファイル２３内に設けてもよい。この場合、制限順守プログラム７０による制限が無効化されることを防止できる。

【００７０】

また、操作制限するためのインタフェースとして、入力装置１３を用いた操作によってファイルのオープン（閲覧）、保存、印刷、メール添付する操作を設定したが、これに限らず適宜のインタフェースに対して操作制限してもよい。

【実施例２】

【００７１】

図８は、実施例２のファイル操作制限システム１００のシステム構成図を示し、図９は、管理サーバ１０１のブロック図を示し、図１０は、制限一覧データの構成図を示す。

ファイル操作制限システム１００は、図８に示すように、インターネットやイントラネットなどで利用される通信回線１０２に接続された１つの管理サーバ１０１と複数のクライアント端末１０３とで構成されている。このクライアント端末１０３には、実施例１で説明したものと同様の制限順守プログラム７０を有する制限付ファイル２３が記憶されている。

【００７２】

管理サーバ１０１は、ハードディスク等で構成される記憶装置、ＣＰＵ等で構成される制御装置、マウスおよびキーボード等で構成される入力装置、液晶ディスプレイまたはＣＲＴディスプレイ等で構成される表示装置、および、ＬＡＮボードまたは無線ＬＡＮカード等で構成される通信装置等を有するコンピュータである。

【００７３】

この管理サーバ１０１は、図９に示すように、記憶装置に制限一覧データ１１１を記憶しており、制御装置で実行する管理プログラム１１０内に制限管理部１１２、問合せ受信部１１３、制限指示生成部１１４、および制限指示送信部１１５が設けられている。

【００７４】

制限管理部１１２は、制限一覧データ１１１に記憶している制限対象ファイルの登録、更新、削除といった管理処理を管理サーバ１０１で実行する部分である。この管理処理は、実施例１で説明した制限設定画面９０を表示装置に表示し、ファイルについての操作制限の内容を登録すること、および、クライアント端末１０３の制限順守プログラム７０からのアクセスに対して制限設定画面９０をクライアント端末１０３の表示装置に表示させ、ファイルについての操作制限の内容をクライアント端末１０３の制限順守プログラム７０から登録許容することで実行する。

【００７５】
問合せ受信部１１３は、クライアント端末１０３の制限順守プログラム７０から制限対象か否かの問合せを受信する処理を実行する部分である。この問合せ受信部１１３は、問い合わせを受信した際に、問い合わせを行った制限順守プログラム７０が記憶されているクライアント端末１０３のＩＰアドレスや問い合わされたファイル名、問い合わせ日時、およびログインユーザー名といった情報を問い合わせ履歴として記憶する処理も実行する。これにより、不正操作があった場合に後に履歴を参照して調査できるようにしている。
【００７６】
制限指示生成部１１４は、制限一覧データ１１１に記憶されている制限内容に従って制限指示情報を生成する処理を実行する部分である。なお、制限指示情報は、クライアント端末１０３の制限順守プログラム７０に対して指示通りに操作制限を実行させる制御命令情報で構成する、あるいは単純に制限内容で構成することができる。制限指示情報を単に制限内容で構成した場合、クライアント端末１０３の記憶装置（若しくは制限順守プログラム７０内）に制御命令一覧情報を記憶しておき、受信した制限内容に対応する制御命令をクライアント端末１０３が制限順守プログラム７０により自分で参照して実行する構成にするとよい。
制限指示送信部１１５は、生成した制限指示情報を問合せのあったクライアント端末１０３に送信する処理を実行する部分である。
【００７７】
図１０は、制限一覧データ１１１のデータ構成を示す。
制限一覧データ１１１は、制限対象ファイルを特定する制限対象ファイル特定情報としての制限対象ファイル名と、制限内容とを複数記憶している。これにより、どのファイルにどのような制限がかけられているかを一元管理している。
【００７８】
図８に示したクライアント端末１０３は、上述した実施例１のファイル操作制限システム１を構成するコンピュータと殆ど同一の構成を有するが、制限順守プログラム７０にパラメータ記憶部７７が設けられないこと、および図６、図７で説明した動作の一部が異なる。
すなわち、パラメータ記憶部７７は設けられず、その代わりに、前述した制限一覧データ１１１が管理サーバ１０１に記憶されている。
【００７９】
また、図６に示した実施例１のフローチャートで、クライアント端末１０３の制限順守プログラム７０は、ステップＳ５の制限パラメータの登録を行う場合に、管理サーバ１０１の制限一覧データ１１１に登録する。そして、次のステップＳ６で、制限パラメータのない制限順守プログラム７０と通常ファイル２１とを結合する。これ以外の処理は実施例１と同一である。
【００８０】
また、図７に示した実施例１のフローチャートで、クライアント端末１０３の制限順守プログラム７０は、ステップＳ１４とＳ１５の間に、管理サーバ１０１に対して制限内容を問い合わせる処理を実行する。詳述すると、制限順守プログラム７０は、自己の記憶されているクライアント端末１０３のＩＰアドレス、および制限付ファイル２３のファイル名（若しくは通常ファイル２１のファイル名）といった操作情報を含めて、制限対象か否か問い合わせる問い合わせ情報を管理サーバ１０１に送信する。クライアント端末１０３の制限順守プログラム７０は、この問い合わせ情報を受けた管理サーバ１０１から制限指示情報を受信し、制限内容を把握する。そして、ステップＳ１５以下の処理を実行する。これ以外の処理は、実施例１と同一であるので、その詳細な説明を省略する。
【００８１】
以上の構成により、操作制限を行いたい制限対象ファイルについて、どのような操作を制限するか管理サーバ１０１に登録することができる。クライアント端末１０３の制限順守プログラム７０は、操作制限されているファイル、つまり制限対象ファイルについて閲

覧、保存、印刷、およびメール添付といった操作を、制限一覧データ１１１に記憶された操作制限内容に従って制限することができる。

【００８２】

クライアント端末１０３の制限順守プログラム７０は、管理サーバ１０１から応答の無い場合や通信回線１０２から切り離された場合にファイル操作を拒否するため、制限対象ファイルが不正に操作されることを確実に防止できる。

【実施例３】

【００８３】

図１１は、ファイル操作制限システム１２０のブロック図を示す。

ファイル操作制限システム１２０は、インターネットやイントラネットなどで利用される通信回線に接続された１つの管理サーバ１０１と複数のクライアント端末１２３とで構成されている。

【００８４】

管理サーバ１０１は、実施例２で説明した管理サーバ１０１と同一構成であるため、同一要素に同一符号を付してその詳細な説明を省略する。

【００８５】

クライアント端末１２３は、ハードディスク等で構成される記憶装置、ＣＰＵ等で構成される制御装置、マウスおよびキーボード等で構成される入力装置、液晶ディスプレイまたはＣＲＴディスプレイ等で構成される表示装置、および、ＬＡＮボードまたは無線ＬＡＮカード等で構成される通信装置等を有するコンピュータである。

【００８６】

このクライアント端末１２３は、制御装置で実行する監視プログラム１４０内に、問合せ送信部１４１、ファイル監視部１４２、制限指示受信部１４３、制限指示解読部１４４、および制限順守部１４５が設けられている。

【００８７】

問合せ送信部１４１は、利用者によって操作されたファイルが制限対象ファイルでないか管理サーバ１０１に問合せ情報を送信して問合せる処理を実行する部分である。

【００８８】

ファイル監視部１４２は、クライアント端末１２３内で操作されるファイルを監視しており、ファイルに対する操作を検知すると問合せ送信部１４１により管理サーバ１０１へ問合せ情報を送信する処理を実行する部分である。

【００８９】

制限指示受信部１４３は、管理サーバ１０１から制限指示情報を受信する受信処理を実行する部分である。

【００９０】

制限指示解読部１４４は、制限指示受信部１４３で受信した制限指示情報を解読する処理を実行する部分である。この解読処理では、閲覧操作、保存操作、印刷操作、およびメール添付操作の可否と、これらの操作項目について実行可能な回数とを取得する。

【００９１】

制限順守部１４５は、取得した制限内容に従ってファイルの閲覧、保存、印刷、およびメール添付を制限する処理を実行する部分である。この制限は、実施例１の図７で説明した処理により実行する。なお、制限順守部１４５は、管理サーバ１０１からの応答を受信するまでファイルに対して行われた操作に対応する処理を実行せずに待機し、管理サーバ１０１からの応答を受信して操作許容されているファイルであった場合に初めて操作に対応する処理を実行する。これにより、クライアント端末１２３が通信回線から切り離された場合や、管理サーバ１０１がダウンした場合であっても、操作制限されているファイルに対する操作を許容してしまうことを防止している。

【００９２】

以上の構成により、実施例２と同様、操作制限を行いたい制限対象ファイルについて、どのような操作を制限するか管理サーバ１０１に登録することができる。クライアント端

末１２３は、操作制限されているファイル、つまり制限対象ファイルについて閲覧、保存、印刷、およびメール添付といった操作を、制限一覧データ１１１に記憶された操作制限内容に従って制限することができる。

【００９３】

クライアント端末１２３は、管理サーバ１０１から応答の無い場合や通信回線から切り離された場合にファイル操作を拒否するため、制限対象ファイルが不正に操作されることを確実に防止できる。

【実施例４】

【００９４】

図１２は、実施例４のファイル操作制限システム１５０のブロック図を示す。

このファイル操作制限システム１５０は、イントラネットなどの閉空間で利用される通信回線に接続された１つの管理サーバ１５１と複数のクライアント端末１５３とで構成されている。

【００９５】

管理サーバ１５１は、ハードディスク等で構成される記憶装置、ＣＰＵ等で構成される制御装置、マウスおよびキーボード等で構成される入力装置、液晶ディスプレイまたはＣＲＴディスプレイ等で構成される表示装置、および、ＬＡＮボードまたは無線ＬＡＮカード等で構成される通信装置等を有するコンピュータである。

【００９６】

この管理サーバ１５１は、記憶装置に制限一覧データ１６２を記憶しており、制御装置で実行する管理プログラム１６０内に監視部１６１、制限指示生成部１６３、制限管理部１６４、および制限指示送信部１６５が設けられている。

【００９７】

監視部１６１は、通信回線に接続されている全てのクライアント端末１５３を巡回し、通信回線を流れているファイルを常時監視する処理を実行する部分である。通信回線を流れているファイルを検知すると、そのファイルが制限一覧データ１６２に登録された制限対象ファイルでないか、制限対象ファイルであればどのような操作制限がなされているかを確認している。そして、制限対象ファイルを検知した場合には、制限一覧データ１６２に登録されている操作制限の内容を参照し、この操作制限内容を制限指示生成部１６３に渡す。

【００９８】

制限一覧データ１６２は、実施例２の制限一覧データ１１１と同一であり、制限指示生成部１６３は実施例２の制限指示生成部１１４と同一であり、制限管理部１６４は実施例２の制限管理部１１２と同一であり、制限指示送信部１６５は実施例２の制限指示送信部１１５と同一であるため、詳細な説明を省略する。

【００９９】

クライアント端末１５３は、ハードディスク等で構成される記憶装置、ＣＰＵ等で構成される制御装置、マウスおよびキーボード等で構成される入力装置、液晶ディスプレイまたはＣＲＴディスプレイ等で構成される表示装置、および、ＬＡＮボードまたは無線ＬＡＮカード等で構成される通信装置等を有するコンピュータである。

【０１００】

このクライアント端末１５３は、制限指示受信部１７１、制限指示解読部１７２、および制限順守部１７３が設けられている。制限指示受信部１７１は実施例２の制限指示受信部１２３と同一であり、制限指示解読部１７２は実施例２の制限指示解読部１２４と同一であり、制限順守部１７３は実施例２の制限順守部１２５と同一であるため、詳細な説明を省略する。

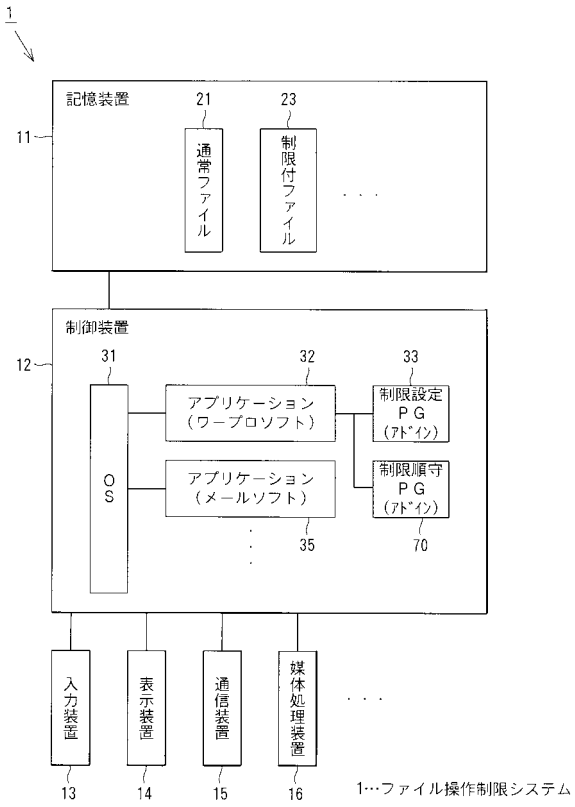
【０１０１】

また、クライアント端末１５３には、操作されるファイルを一時的に記憶するファイルバッファを設けることが好ましい。操作されるファイルをファイルバッファに一時的に記憶することにより、多数のクライアント端末１５３を監視する管理サーバ１５１がファイ

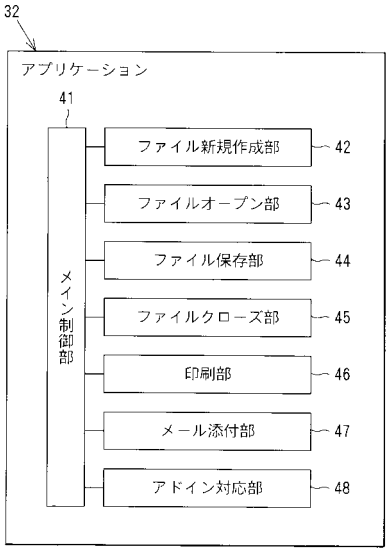
ルを見失ったりせず確実に操作制限することができる。
【０１０２】
以上の構成により、実施例３と同様、操作制限を行いたい制限対象ファイルについて、どのような操作を制限するか管理サーバ１５１に登録することができる。クライアント端末１５３は、操作制限されているファイル、つまり制限対象ファイルについて閲覧、保存、印刷、およびメール添付といった操作を、制限一覧データ１６２に記憶された操作制限内容に基づいて管理サーバ１５１から指示された内容に従って制限することができる。
【０１０３】
クライアント端末１５３は、管理サーバ１５１から応答の無い場合や通信回線から切り離された場合にファイル操作を拒否するため、制限対象ファイルが不正に操作されることを確実に防止できる。
【０１０４】
この発明の構成と、上述の実施形態との対応において、
この発明の出力手段および記憶手段は、実施形態の記憶装置１１に対応し、
以下同様に、
制御手段は、制御装置１２に対応し、
入力手段は、入力装置１３、表示装置１４、および制限設定画面９０に対応し、
異なるプログラムは、ＯＳ３１に対応し、
アプリケーションプログラムは、アプリケーション３２に対応し、
制限付ファイル作成手段は、ファイル結合部６４に対応し、
機能拡張プログラムは、アドインプログラムとなる制限順守プログラム７０に対応し、
複製防止プログラムは、ファイル複製防止部７８に対応し、
サーバは、管理サーバ１０１，１５１に対応し、
操作制限データベースは、制限一覧データ１１１，１６２に対応し、
問合せ受付手段は、問合せ受信部１１３に対応し、
応答手段は、制限指示送信部１１５に対応し、
操作検知手段は、監視プログラム１４０に対応し、
操作制限問合せ手段は、問合せ送信部１４１に対応し、
応答受付手段は、制限指示受信部１４３に対応し、
制限順守手段および待機手段は、制限順守部１４５に対応し、
検知手段および判定手段は、監視部１６１に対応し、
制限順守手段は、制限順守部１７３に対応し、
入力受付処理は、ステップＳ２に対応し、
プログラム作成処理は、ステップＳ４～Ｓ５に対応し、
結合処理は、ステップＳ６に対応し、
出力処理は、ステップＳ７に対応し、
判定処理は、ステップＳ１６，Ｓ１９，Ｓ２２，Ｓ２５，Ｓ３１に対応し、
操作制限順守処理は、ステップＳ１６（ＮＯ），Ｓ２０，Ｓ２６，Ｓ３２に対応し、
操作許容処理は、ステップＳ１７，Ｓ２１，Ｓ２３，Ｓ２７，Ｓ２９，Ｓ３３，Ｓ３５に対応し、
操作制限は、閲覧、保存、印刷、およびメール添付に対応し、
記憶手段は、記憶装置に対応するも、
この発明は、上述の実施形態の構成のみに限定されるものではなく、多くの実施の形態を得ることができる。
【図面の簡単な説明】
【０１０５】
【図１】ファイル操作制限システムのブロック図。
【図２】アプリケーションのブロック図。
【図３】制限設定プログラムのブロック図。
【図４】制限付ファイルのブロック図。

【図５】制限設定画面の画面イメージ図。
【図６】制限設定プログラムによる動作のフローチャート。
【図７】制限順守プログラムによる動作のフローチャート。
【図８】実施例２のファイル操作制限システムのシステム構成図。
【図９】実施例２のファイル操作制限システムのブロック図。
【図１０】実施例２の制限一覧データの構成図。
【図１１】実施例３のファイル操作制限システムのブロック図。
【図１２】実施例４のファイル操作制限システムのブロック図。
【符号の説明】
【０１０６】
１，１００，１２０，１５０…ファイル操作制限システム
１１…記憶装置
１２…制御装置
１３…入力装置
１４…表示装置
２３…制限付ファイル
３１…ＯＳ
３２…アプリケーション
３３…制限設定プログラム
６４…ファイル結合部
７０…制限順守プログラム
７８…ファイル複製防止部
８０…制限対象ファイル
９０…制限設定画面
１０１，１５１…管理サーバ
１０２…通信回線
１０３，１２３，１５３…クライアント端末
１１１，１６２…制限一覧データ
１１３…問合せ受信部
１１５…制限指示送信部
１４０…監視プログラム
１４１…問合せ送信部
１４３…制限指示受信部
１４５，１７３…制限順守部
１６１…監視部

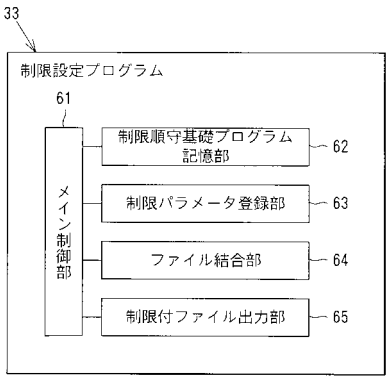
【図１】


1
記憶装置
11
21
通常ファイル
23
制限付ファイル
制御装置
12
31
OS
32
アプリケーション（ワープロソフト）
アプリケーション（メールソフト）
33
制限設定PG（アドイン）
制限順守PG（アドイン）
35
70
入力装置
表示装置
通信装置
媒体処理装置
13
14
15
16
1…ファイル操作制限システム

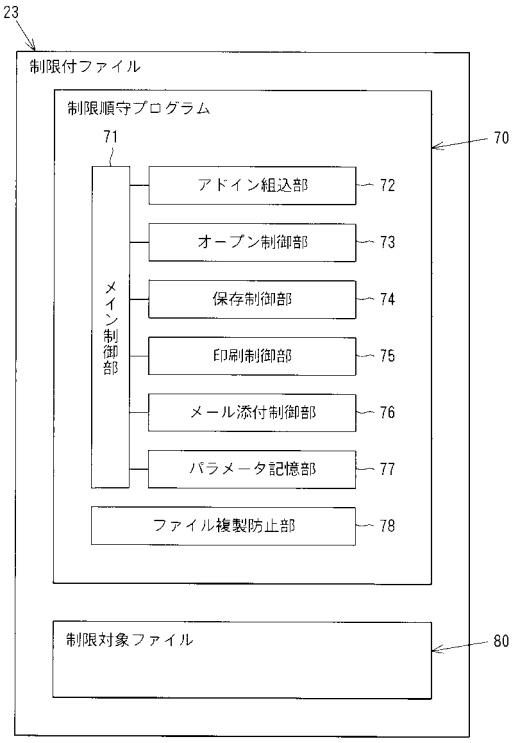
【図２】


32
アプリケーション
41
メイン制御部
ファイル新規作成部 42
ファイルオープン部 43
ファイル保存部 44
ファイルクローズ部 45
印刷部 46
メール添付部 47
アドイン対応部 48

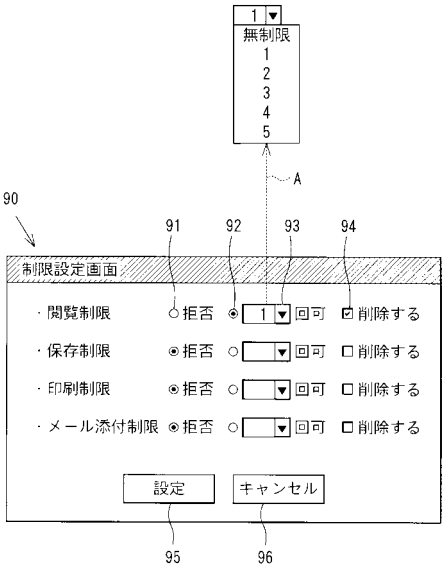
【図３】


33
制限設定プログラム
61
メイン制御部
制限順守基礎プログラム記憶部 62
制限パラメータ登録部 63
ファイル結合部 64
制限付ファイル出力部 65

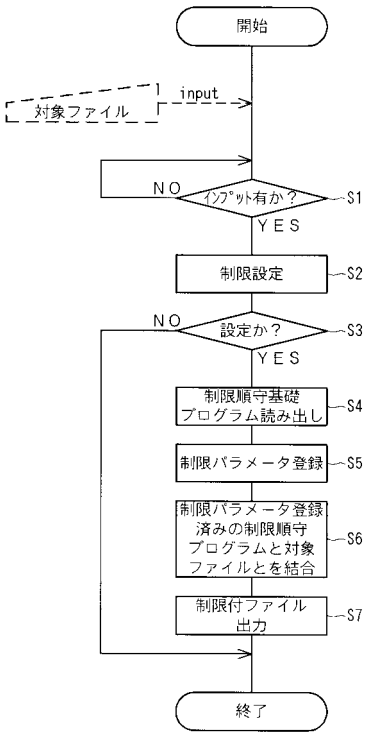
【図４】


23
制限付ファイル
制限順守プログラム
70
71
メイン制御部
アドイン組込部 72
オープン制御部 73
保存制御部 74
印刷制御部 75
メール添付制御部 76
パラメータ記憶部 77
ファイル複製防止部 78
制限対象ファイル
80

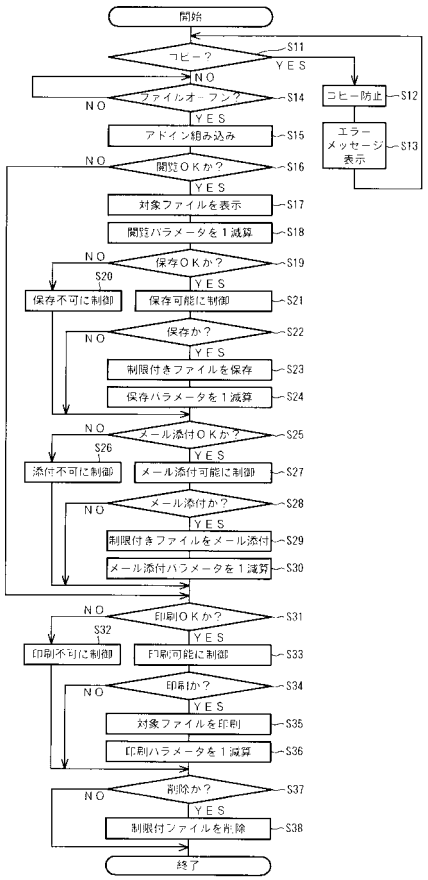
【図５】



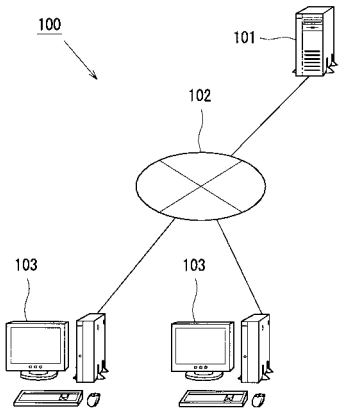
【図６】



【図７】

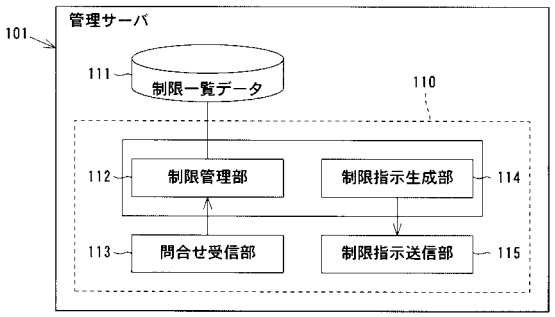


【図８】



100…ファイル操作制限システム
101…管理サーバ
102…通信回線
103…クライアント端末

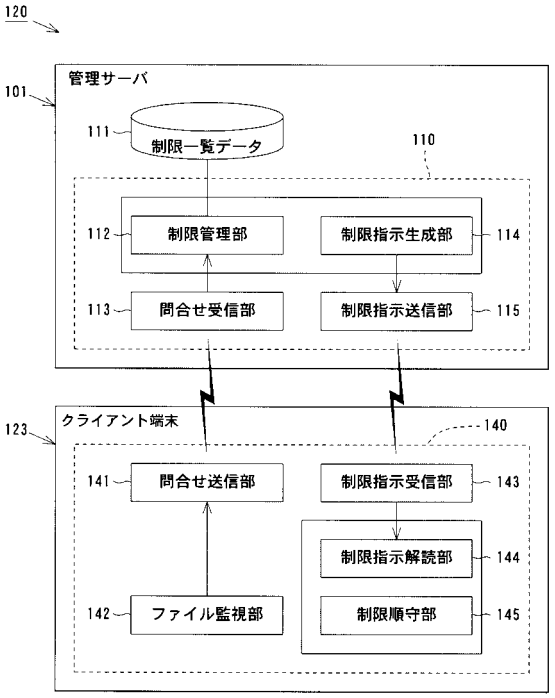
【図９】



【図１０】

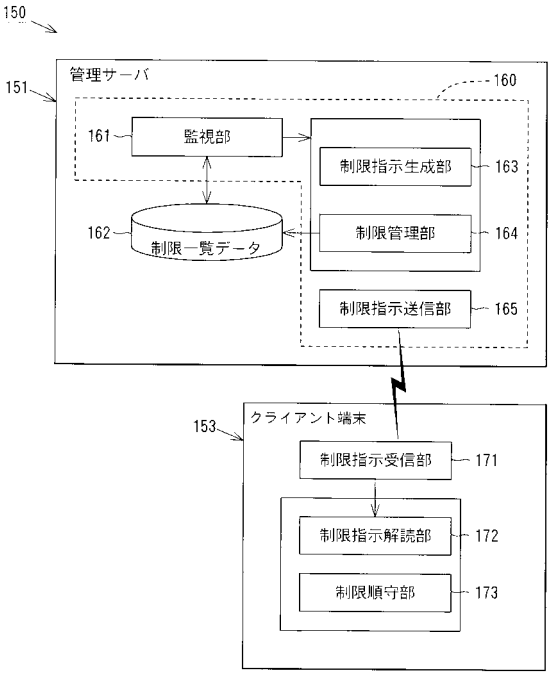
制限対象ファイル名	制限内容
顧客情報.doc	BBB
朝礼訓話.doc	AAA
社員情報.xls	BBB
⋮	

【図１１】



120…ファイル操作制限システム

【図１２】



150…ファイル操作制限システム