

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6148042号
(P6148042)

(45) 発行日 平成29年6月14日 (2017. 6. 14)

(24) 登録日 平成29年5月26日 (2017. 5. 26)

(51) Int. Cl.

F I

G 0 6 F 3 / 1 2 (2006.01)

G 0 6 F 3 / 1 2 3 7 3

G 0 6 F 3 / 1 2 3 3 8

G 0 6 F 3 / 1 2 3 3 9

G 0 6 F 3 / 1 2 3 8 5

G 0 6 F 3 / 1 2 3 0 3

請求項の数 8 (全 14 頁) 最終頁に続く

(21) 出願番号 特願2013-52390 (P2013-52390)
 (22) 出願日 平成25年3月14日 (2013. 3. 14)
 (65) 公開番号 特開2014-178881 (P2014-178881A)
 (43) 公開日 平成26年9月25日 (2014. 9. 25)
 審査請求日 平成28年3月14日 (2016. 3. 14)

(73) 特許権者 000104652
 キヤノン電子株式会社
 埼玉県秩父市下影森 1 2 4 8 番地
 (74) 代理人 100076428
 弁理士 大塚 康德
 (74) 代理人 100112508
 弁理士 高柳 司郎
 (74) 代理人 100115071
 弁理士 大塚 康弘
 (74) 代理人 100116894
 弁理士 木村 秀二
 (74) 代理人 100130409
 弁理士 下山 治
 (74) 代理人 100134175
 弁理士 永川 行光

最終頁に続く

(54) 【発明の名称】 情報処理装置、情報処理方法

(57) 【特許請求の範囲】

【請求項 1】

ネットワークを介して複数の端末装置からリモートログインしているリモートユーザが同時に使用可能であり、かつ該複数の端末装置のそれぞれから受信した印刷要求に応じた印刷を印刷装置に実行させる情報処理装置であって、

前記情報処理装置内に備わっており且つ前記印刷を管理するための管理部、の動作を監視する監視手段と、

前記監視手段にて監視された、前記印刷を実行させたことに応じて生成された印刷情報が、リストに登録されている登録印刷情報と重複しているか否かを判断する判断手段と、

前記印刷情報が、前記リストに登録されている登録印刷情報のいずれとも異なる場合には、該印刷情報を登録印刷情報として前記リストに登録する手段と、

前記リストに登録されている登録印刷情報から、ユーザの印刷ログを生成する生成手段と

を備えることを特徴とする情報処理装置。

【請求項 2】

複数の端末装置から同時に使用可能であり、かつ該複数の端末装置のそれぞれから受信した印刷要求に応じた印刷を印刷装置に実行させる情報処理装置であって、

前記印刷を実行させたことに応じて生成された印刷情報が、リストに登録されている登録印刷情報と重複しているか否かを判断する判断手段と、

前記印刷情報が、前記リストに登録されている登録印刷情報のいずれとも異なる場合に

10

20

は、該印刷情報を登録印刷情報として前記リストに登録する手段と、

前記リストに登録されている登録印刷情報から、ユーザの印刷ログを生成する生成手段と、

前記端末装置のユーザ情報を管理する管理手段と、

前記印刷を実行させたことに応じて生成された印刷情報が、前記管理手段が管理しているユーザ情報に対応するユーザの情報を含むか否かを判断する手段と

を備え、

前記生成手段は、前記管理手段が管理しているユーザ情報に対応するユーザの情報を含む印刷情報から、前記ユーザの印刷ログを生成することを特徴とする情報処理装置。

【請求項 3】

更に、

前記リストに登録されている登録印刷情報を規定時間ごとに消去する手段を備えることを特徴とする請求項 1 または 2 に記載の情報処理装置。

【請求項 4】

更に、

前記印刷の可否制御を行う制御手段を備え、

前記制御手段は、前記印刷装置を識別する情報と、前記ユーザ情報またはドキュメントを識別する情報とを関連付けたテーブルを参照して、該印刷の可否制御を行うことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 5】

ネットワークを介して複数の端末装置からリモートログインしているリモートユーザが同時に使用可能であり、かつ該複数の端末装置のそれぞれから受信した印刷要求に応じた印刷を印刷装置に実行させる情報処理装置が行う情報処理方法であって、

前記情報処理装置の監視手段が、前記情報処理装置内に備わっており且つ前記印刷を管理するための管理部、の動作を監視する監視工程と、

前記情報処理装置の判断手段が、前記監視工程にて監視された、前記印刷を実行させたことに応じて生成された印刷情報が、リストに登録されている登録印刷情報と重複しているか否かを判断する判断工程と、

前記情報処理装置の登録手段が、前記印刷情報が、前記リストに登録されている登録印刷情報のいずれとも異なる場合には、該印刷情報を登録印刷情報として前記リストに登録する工程と、

前記情報処理装置の生成手段が、前記リストに登録されている登録印刷情報から、ユーザの印刷ログを生成する生成工程と

を備えることを特徴とする情報処理方法。

【請求項 6】

コンピュータを、請求項 1 乃至 4 の何れか 1 項に記載の情報処理装置の各手段として機能させるためのコンピュータプログラム。

【請求項 7】

複数の端末装置と、

請求項 1 又は 2 に記載の情報処理装置と、

を有するシステム。

【請求項 8】

複数の端末装置から同時に使用可能であり、かつ該複数の端末装置のそれぞれから受信した印刷要求に応じた印刷を印刷装置に実行させる情報処理装置が行う情報処理方法であって、

前記情報処理装置の第 1 の判断手段が、前記印刷を実行させたことに応じて生成された印刷情報が、リストに登録されている登録印刷情報と重複しているか否かを判断する判断工程と、

前記情報処理装置の登録手段が、前記印刷情報が、前記リストに登録されている登録印刷情報のいずれとも異なる場合には、該印刷情報を登録印刷情報として前記リストに登録

10

20

30

40

50

する工程と、

前記情報処理装置の生成手段が、前記リストに登録されている登録印刷情報から、ユーザの印刷ログを生成する生成工程と、

前記情報処理装置の管理手段が、前記端末装置のユーザ情報を管理する管理工程と、

前記情報処理装置の第2の判断手段が、前記印刷を実行させたことに応じて生成された印刷情報が、前記管理工程で管理しているユーザ情報に対応するユーザの情報を含むか否かを判断する工程と

を備え、

前記生成工程では、前記管理工程で管理しているユーザ情報に対応するユーザの情報を含む印刷情報から、前記ユーザの印刷ログを生成することを特徴とする情報処理方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、印刷ログの収集技術に関するものである。

【背景技術】

【0002】

機密情報が漏洩した場合に漏洩経路の追跡を可能にする方法に関する従来技術として、印刷の履歴から印刷されたファイルを特定・追跡したり、印刷情報のみを印刷ログとして残し、印刷ログから印刷されたファイルを特定・追跡する方法が知られている。

【0003】

特許文献1によれば、Windows（登録商標）が提供する印刷監視用のWin32 APIを利用して、監視対象の装置での印刷の実行を監視する。そして、印刷が実行された場合に、Win32 APIを通して、印刷実行通知とともに、実行された印刷の情報を取得し、印刷ログを取得する。

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特開2010-211620号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかし、従来技術では、次のような問題がある。印刷ログに書き出すログインユーザ名は、印刷が実行された時点で監視対象装置にログインしていたユーザの名前である。然るに、複数のユーザが同時に使用可能な情報処理装置において、あるユーザが印刷を実行した場合、監視対象装置にログインしているすべてのユーザの印刷ログとして出力されてしまうため、実際に印刷を実行していないユーザの印刷ログが出力されてしまう。

【0006】

本発明はこのような問題に鑑みてなされたものであり、複数ユーザからの印刷要求に応じた印刷を印刷装置に行わせる場合であっても、ユーザごとの印刷ログを記録可能な技術を提供することを目的とする。

【課題を解決するための手段】

【0007】

本発明の第1の様態によれば、ネットワークを介して複数の端末装置からリモートログインしているリモートユーザが同時に使用可能であり、かつ該複数の端末装置のそれぞれから受信した印刷要求に応じた印刷を印刷装置に実行させる情報処理装置であって、

前記情報処理装置内に備わっており且つ前記印刷を管理するための管理部、の動作を監視する監視手段と、

前記監視手段にて監視された、前記印刷を実行させたことに応じて生成された印刷情報が、リストに登録されている登録印刷情報と重複しているか否かを判断する判断手段と、

前記印刷情報が、前記リストに登録されている登録印刷情報のいずれとも異なる場合に

10

20

30

40

50

は、該印刷情報を登録印刷情報として前記リストに登録する手段と、

前記リストに登録されている登録印刷情報から、ユーザの印刷ログを生成する生成手段と

を備えることを特徴とする。

【発明の効果】

【0008】

本発明の構成によれば、複数ユーザからの印刷要求に応じた印刷を印刷装置に行わせる場合であっても、ユーザごとの印刷ログを記録することができる。

【図面の簡単な説明】

【0009】

【図1】システムの機能構成例を示すブロック図。

【図2】ログインしたユーザのユーザ情報を収集して管理するための処理のフローチャート。

【図3】印刷ログを生成するための処理のフローチャート。

【図4】サーバ装置100のハードウェア構成例を示すブロック図。

【図5】印刷情報リストの更新例を示す図。

【図6】印刷情報の例を示す図。

【図7】システム構成の模式図。

【発明を実施するための形態】

【0010】

以下、添付図面を参照し、本発明の好適な実施形態について説明する。

【0011】

〔第1の実施形態〕

まず、本実施形態に係るシステムの機能構成例について、図1のブロック図を用いて説明する。本実施形態に係るシステムは、ターミナルサービスを実施するためのものである。ターミナルサービスとは周知の通り、クライアント端末装置側で行われた入力に応じてサーバ装置がアプリケーションプログラムを実行するサービスである。すなわち、アプリケーションプログラムを有していないクライアント端末装置であっても、このアプリケーションプログラムの恩恵を享受できるようにするサービスである。

【0012】

本実施形態に係るシステムは図1に示す如く、ターミナルサービスを提供するサーバ装置100、ターミナルサービスを楽しむクライアント端末装置170a、b、サーバ装置100からの印刷データに基づいて印刷を行う印刷装置150a、bを有する。サーバ装置100、印刷装置150a、150b、クライアント端末装置170a、170bはいずれもLANやインターネットなどにより構成されているネットワーク160に接続されており、互いにデータ通信を行うことができる。

【0013】

なお、図1に示した構成はあくまでも一例であり、以下に説明するシステムの動作と同等以上の動作を実現できるのであれば、他の構成を採用しても良い。例えば図1ではクライアント端末装置や印刷装置は2台としているが、これに限るものではなく、例えば、3台以上としても良い。また、サーバ装置100が有する機能として説明する全機能のうち一部を外部装置に割り当て、この外部装置をネットワーク160に接続させて、この一部の機能をこの外部装置に実行させるようにしても良い。

【0014】

まず、サーバ装置100について説明する。セキュリティソフトウェア103は、クライアント端末装置170a(170b)ごと(クライアント端末装置のユーザごと)にスプーラ104の動作を監視する。また、セキュリティソフトウェア103は、スプーラ104が印刷データを印刷装置150a(150b)に対して送出して印刷装置150a(150b)に印刷を実行させると、この印刷に係る情報(印刷情報)から印刷ログを生成する。

【 0 0 1 5 】

スプーラ 1 0 4 は、クライアント端末装置 1 7 0 a (1 7 0 b) から送信された印刷データを管理し、この印刷データを順次ネットワーク 1 6 0 を介して、印刷装置 1 5 0 a、1 5 0 b のうち印刷データ中に指定されている一方に送出する。スプーラ 1 0 4 の機能については周知であるので、これ以上の詳細な説明は省略する。また、スプーラ 1 0 4 に限定されず、印刷の実行を管理するソフトウェアなら何でもよい。

【 0 0 1 6 】

ターミナルサービス提供部 1 0 2 は、クライアント端末装置 1 7 0 a、1 7 0 b に対してターミナルサービスを提供するための処理を実行する。

【 0 0 1 7 】

記憶部 1 0 1 には、クライアント端末装置 1 7 0 a やクライアント端末装置 1 7 0 b を利用可能な各ユーザの情報（ユーザ情報）が予め登録されている。また、記憶部 1 0 1 には、クライアント端末装置 1 7 0 a やクライアント端末装置 1 7 0 b を利用可能なユーザごとに、該ユーザが使用可能な印刷装置を特定する情報（アドレスや名称）も保存されている。

【 0 0 1 8 】

次に、クライアント端末装置 1 7 0 a、1 7 0 b について説明する。クライアント端末装置 1 7 0 a とクライアント端末装置 1 7 0 b とは同じ構成、同じ動作を実行する装置である。然るに、以下では、クライアント端末装置 1 7 0 a とクライアント端末装置 1 7 0 b とに共通する説明の場合には、クライアント端末装置 1 7 0 a とクライアント端末装置 1 7 0 b とをまとめてクライアント端末装置 1 7 0 と呼称する。

【 0 0 1 9 】

クライアント端末装置 1 7 0 は、サーバ装置 1 0 0 が提供するターミナルサービスを享受したい場合にはまず、サーバ装置 1 0 0 に対してログインする必要がある。然るに、クライアント端末装置 1 7 0 はログインに必要な情報（クライアント端末装置 1 7 0 を操作するユーザのユーザ情報（ユーザ名、パスワードなど））をサーバ装置 1 0 0 に対して送信する必要がある。このユーザ情報がサーバ装置 1 0 0 側で認証されると（記憶部 1 0 1 に予め登録されているユーザ情報の何れかと合致すると）、クライアント端末装置 1 7 0 はサーバ装置 1 0 0 が提供するターミナルサービスを享受することができるようになる。このように、ターミナルサービスを享受するためには、リモートデスクトップ接続（R D C ）と呼ばれるプログラムや、ターミナル・サービス・クライアント（T S C ）と呼ばれるプログラムを実行する必要がある。然るにクライアント端末装置 1 7 0 にはこのようなプログラムがインストールされている必要がある。ターミナルサービスとは、Windows（登録商標）、Mac OS および Linux（登録商標）などの一般的なオペレーションシステム（OS）であれば一般に備えているサービスであるから、その名称は OS によって異なっている。

【 0 0 2 0 】

リモートサービスは、第 1 のパーソナルコンピュータ（P C ）に対して第 2 の P C からリモートログインして、第 1 の P C を遠隔操作するサービスである。例えば、第 1 の P C から情報を取得したり、第 1 の P C に情報を書き込んだり、第 1 の P C にインストールされているソフトウェアを第 1 の P C 上で実行したりする。なお、第 1 の P C の入力部を通じて直接ログインしているユーザをローカルユーザと呼び、第 2 の P C から第 1 の P C へリモートログインしているユーザをリモートユーザと呼んで区別することにする。

【 0 0 2 1 】

例えば、ターミナルサービス提供部 1 0 2 はクライアント端末装置 1 7 0 から実行要求のあったアプリケーションプログラムを実行して表示画面を生成し、該生成した表示画面のデータをクライアント端末装置 1 7 0 に対して返信する。クライアント端末装置 1 7 0 はこのデータに基づいて表示画面を生成し、該生成した表示画面を表示装置に表示する。クライアント端末装置 1 7 0 のユーザがこの表示画面を見て何らの操作（例えば印刷指示操作（印刷データ送信））を入力すると、この操作内容（例えば印刷データ）はサーバ装

10

20

30

40

50

置 1 0 0 に対して送信される。ターミナルサービス提供部 1 0 2（更に他の機能部が動作しても良い）はこの操作内容に基づいた処理を実行し、該実行の結果をクライアント端末装置 1 7 0 に返信したりする。クライアント端末装置 1 7 0 は、この実行の結果を表示画面上に反映させる。サーバ装置 1 0 0 は、リモートユーザによって使用される一方で、同時並行的にローカルユーザによっても使用可能である。

【 0 0 2 2 】

このように、リモートユーザとローカルユーザとを含む複数のユーザが同時に使用可能なシステム（ターミナルサービス）においては、アプリケーションプログラムが、サーバ装置 1 0 0 で実行される。クライアント端末装置 1 7 0 からサーバ装置 1 0 0 に同時に接続してアプリケーションプログラムを実行することも可能である。この場合、リモートユーザ毎にセッションが分けられ、各ユーザは別々の仮想デスクトップ環境を利用してアプリケーションプログラムを実行することができる。ターミナルサービス提供部 1 0 2 は、各セッションを区別するためにセッション ID を発行する。なお、同時に使用可能とは、同じ時間に複数のユーザがログインしている状態を含む。このようなターミナルサービスは一般的な技術であるため、これ以上の説明は省略する。

10

【 0 0 2 3 】

次に、印刷装置 1 5 0 a、1 5 0 b について説明する。印刷装置 1 5 0 a、1 5 0 b はネットワーク 1 6 0 を介して受信した印刷データに基づいて、紙などの記録媒体上に文字や画像などを印刷する装置である。なお、図 1 では印刷装置 1 5 0 a、1 5 0 b はネットワーク 1 6 0 上に接続されているが、サーバ装置 1 0 0 に直接接続するようにしても構わない。

20

【 0 0 2 4 】

次に、サーバ装置 1 0 0 のハードウェア構成例について、図 4 のブロック図を用いて説明する。

【 0 0 2 5 】

C P U 4 0 1 は、R A M 4 0 2 や R O M 4 0 3 に格納されているコンピュータプログラムやデータを用いて処理を実行することで、サーバ装置 1 0 0 全体の動作制御を行うと共に、サーバ装置 1 0 0 が行うものとして後述する各処理を実行する。

【 0 0 2 6 】

R A M 4 0 2 は、外部記憶装置 4 0 5 からロードされたコンピュータプログラムやデータを一時的に記憶するためのエリア、C P U 4 0 1 が各種の処理を実行する際に用いるワークエリア、を有する。更に、R A M 4 0 2 は、ネットワーク I / F（インターフェース）4 0 7 を介してクライアント端末装置 1 7 0 から受信した各種のデータを一時的に記憶するためのエリアも有する。このように、R A M 4 0 2 は、各種のエリアを適宜提供することができる。

30

【 0 0 2 7 】

R O M 4 0 3 には、サーバ装置 1 0 0 の設定データやブートプログラムなどが格納されている。

【 0 0 2 8 】

操作部 4 0 4 はマウスやキーボードなどにより構成されており、サーバ装置 1 0 0 の操作者が操作することで各種の指示を C P U 4 0 1 に対して入力することができる。

40

【 0 0 2 9 】

外部記憶装置 4 0 5 は、ハードディスクドライブ装置に代表される大容量情報記憶装置である。外部記憶装置 4 0 5 には、O S（オペレーティングシステム）や、上記のセキュリティソフトウェア 1 0 3、スプーラ 1 0 4、ターミナルサービス提供部 1 0 2 に相当するコンピュータプログラムが保存されている。また、外部記憶装置 4 0 5 には、印刷装置 1 5 0 a、1 5 0 b のそれぞれのドライバソフトウェアも保存されている。また、外部記憶装置 4 0 5 は、スプーラ 1 0 4 によって複数の印刷データをバッファリングする為に使用される。また、外部記憶装置 4 0 5 は、図 1 の記憶部 1 0 1 としても機能するので、外部記憶装置 4 0 5 には、記憶部 1 0 1 が保持しているものとして上述したデータも保存

50

されていることになる。

【0030】

外部記憶装置405に保存されているコンピュータプログラムやデータは、CPU401による制御に従って適宜RAM402にロードされ、CPU401による処理対象となる。

【0031】

表示部406は、CRTや液晶画面などにより構成されており、CPU401による処理結果を画像や文字などでもって表示する。

【0032】

ネットワークI/F407は、サーバ装置100を上記のネットワーク160に接続するためのものであり、サーバ装置100はこのネットワークI/F407を介して、ネットワーク160に接続されている各機器とのデータ通信を行うことができる。

10

【0033】

上記の各部はいずれも、バス408に接続されている。

【0034】

なお、図4に示したハードウェア構成はあくまでも一例であり、サーバ装置100が行うものとして後述する各処理を実行可能な構成であれば、如何なる構成を採用しても構わない。また、図4に示した構成は、クライアント端末装置170に適用しても構わない。

【0035】

次に、サーバ装置100が行う処理について、同処理のフローチャートを示す図2, 3を用いて説明する。図2は、サーバ装置100にログインしたユーザのユーザ情報を収集して管理するための処理のフローチャート、図3は、印刷ログを生成するための処理のフローチャートである。

20

【0036】

なお、図2, 3のフローチャートに従った処理をCPU401に実行させるためのコンピュータプログラムやデータは外部記憶装置405に保存されている。CPU401はこのコンピュータプログラムやデータをRAM402にロードして実行することで、CPU401は図2, 3のフローチャートに従った処理を実行することができる。

【0037】

ステップS201では、CPU401は、外部記憶装置405に保存されているセキュリティソフトウェア103をRAM402にロードして、このセキュリティソフトウェア103を起動する。ステップS201における処理は、サーバ装置100の起動時に行われても良いし、ユーザが操作部404を操作して起動指示を入力し、CPU401がこの入力を検知したことに応じて行われても良いし、別のプログラムによって起動されても良い。もちろん、図1に示した他の機能部についても起動しておく。

30

【0038】

ステップS202では、CPU401はセキュリティソフトウェア103を実行する。これによりCPU401は、サーバ装置100に対するログインのためにクライアント端末装置170から送信されたユーザ情報を受信すると、該ユーザ情報と、外部記憶装置405(記憶部101)に予め登録されている各ユーザのユーザ情報と、を比較する。

40

【0039】

ユーザ情報は上記の通り、サーバ装置100にログインするためのものである。例えばクライアント端末装置170のユーザは不図示の操作部を操作して自身のユーザ名及びパスワードをユーザ情報として入力する。そしてユーザは不図示の操作部を操作してユーザ情報の送信指示を入力すると、クライアント端末装置170はこのユーザ情報をサーバ装置100に対して送信する。なお、ユーザ情報には、アカウント名、ドメイン名、ユーザ名など、ユーザを一意に識別することが可能な値を用いることができる。

【0040】

そしてこの比較の結果、クライアント端末装置170から受信したユーザ情報と一致するユーザ情報が外部記憶装置405に保存されていた場合には、認証成功と判断し、処理

50

はステップS 2 0 3に進む。一方、この比較の結果、クライアント端末装置1 7 0から受信したユーザ情報と一致するユーザ情報が外部記憶装置4 0 5に保存されていなかった場合には、認証失敗と判断し、その旨をクライアント端末装置1 7 0に送信して図2の処理は終了する。

【0 0 4 1】

ステップS 2 0 3では、CPU 4 0 1は、セキュリティソフトウェア1 0 3を実行する。これによりCPU 4 0 1は、ステップS 2 0 2でクライアント端末装置1 7 0から受信したユーザ情報を、ログイン中のユーザのユーザ情報を登録するためのリスト(ユーザ情報リスト)に登録する。このときユーザ情報のかわりにセッションIDを使用してもよい。そして処理は、図3のステップS 2 0 5に進む。

10

【0 0 4 2】

CPU 4 0 1は、ネットワークI / F 4 0 7を介してクライアント端末装置1 7 0(認証が成功したクライアント端末装置)から受信した印刷データをスプーラ1 0 4に転送する。そしてCPU 4 0 1はスプーラ1 0 4を実行することで、この転送された印刷データを外部記憶装置4 0 5内で管理し、該印刷データを適当なタイミングで印刷装置1 5 0 a若しくは印刷装置1 5 0 bに対して送出する。印刷データはそのフォーマットによっては適宜変換してから印刷装置1 5 0 a若しくは印刷装置1 5 0 bに対して送信する。

【0 0 4 3】

このとき、ステップS 2 0 5では、CPU 4 0 1は、セキュリティソフトウェア1 0 3を実行し、Windows(登録商標)が提供する印刷操作監視用Win 3 2 API等を利用してスプーラ1 0 4を監視している。そしてCPU 4 0 1は、ある印刷データを印刷装置1 5 0 a若しくは印刷装置1 5 0 bに対して送出すると(タイミングは送出後に限らない)、監視用Win 3 2 API等を介して、この印刷に係る印刷情報を取得する。印刷情報には、例えば、ユーザ名、プリンタ名、ジョブID、ドキュメント名、PC名、印刷枚数、印刷(開始、終了)時刻、印刷状態(印刷開始、印刷終了)、印刷装置のIPアドレスなどが含まれる。

20

【0 0 4 4】

以下では、具体例を挙げて説明を行うために、サーバ装置1 0 0にはユーザA、ユーザB、ユーザC、ユーザDがログイン中であるとする(然るにユーザ情報リストには、ユーザA、ユーザB、ユーザC、ユーザDのそれぞれのユーザ情報が登録されている)。そして、ユーザ名=ユーザAが、プリンタ名=印刷装置1 5 0 aのプリンタ名を利用して印刷を実行し、CPU 4 0 1が監視用Win 3 2 API等を介して、「ユーザ名=ユーザA、プリンタ名=印刷装置1 5 0 aのプリンタ名」を含む印刷情報を取得したとする。

30

【0 0 4 5】

このときステップS 2 0 5ではCPU 4 0 1は、同ステップで取得した印刷情報中のプリンタ名(ここでは印刷装置1 5 0 aのプリンタ名)の印刷装置が使用可能なユーザごとの印刷情報を取得する。ここでは印刷装置1 5 0 aを使用可能なユーザがユーザA、ユーザC、ユーザDであるとするので、ユーザA、ユーザC、ユーザDから、(「ユーザ名=ユーザA、プリンタ名=印刷装置1 5 0 aのプリンタ名」を含む)印刷情報を取得することになる。

40

【0 0 4 6】

セキュリティソフトウェア1 0 3は、サーバ装置1 0 0が受け付けた印刷情報を保持するリスト(印刷情報リスト)を作成する。次に、ステップS 3 0 1では、CPU 4 0 1はセキュリティソフトウェア1 0 3を実行し、サーバ装置1 0 0が過去に受け付けた印刷情報を登録するためのリスト(印刷情報リスト)内の各印刷情報と、ステップS 2 0 5で取得した印刷情報と、を比較する。この比較は、印刷情報に含まれている全ての要素を比較しても良いし、一部を比較しても良い。即ち、ステップS 2 0 5で取得した印刷情報と同じ印刷内容を示す印刷情報がすでに印刷情報リストに登録されているか否かを判断することができるのであれば、どのような比較であっても構わない。

【0 0 4 7】

50

そして、ステップ S 2 0 5 で取得した印刷情報と同じ印刷情報が印刷情報リストにすでに登録されている場合には、処理はステップ S 3 0 8 に進む。一方、ステップ S 2 0 5 で取得した印刷情報と同じ印刷情報が印刷情報リストに登録されていない場合には、処理はステップ S 3 0 2 に進む。

【 0 0 4 8 】

ステップ S 3 0 8 では、CPU 4 0 1 は、ステップ S 2 0 5 で取得した印刷情報を破棄して処理を終了する。一方、ステップ S 3 0 2 では、CPU 4 0 1 は、ステップ S 2 0 5 で取得した印刷情報を印刷情報リストに登録する。

【 0 0 4 9 】

ここで、印刷情報リストの更新例を図 5 を用いて説明する。初期状態では印刷情報リストにはまだ何も登録されていないので、図 5 (a) に示す如く、印刷情報リストは空の状態となっている。そしてその後、印刷情報 A を取得した場合、印刷情報リストにはまだ何も登録されていないので、この印刷情報 A は図 5 (b) に示すごとく印刷情報リストに登録される。そしてその後、印刷情報 B を取得したとする。この場合、印刷情報リストには印刷情報 A は登録されているものの、印刷情報 B はまだ登録されていないので、印刷情報 B は図 5 (c) に示すごとく印刷情報リストに登録される。そしてその後、印刷情報 A を取得したとする。この場合、印刷情報リストにはすでに印刷情報 A は登録されているので、この取得した印刷情報 A は印刷情報リストには登録されずに、破棄される。このようにして、印刷情報リストには、印刷情報が重複することなく登録される。

【 0 0 5 0 】

図 6 は、アカウント名(ユーザ名)=hoge1 が、プリンタ名=Micro XPS Document Writer を利用して印刷を実行した場合に取得される印刷情報(、 、)を示す。サーバ装置 1 0 0 にログイン中であるユーザのユーザ名が hoge1、hoge2、hoge3、hoge4 であるとする。このとき、このユーザ名の中で、プリンタ名=Micro XPS Document Writer を利用できるユーザ(例えば hoge1、hoge2、hoge3) 分、同一の印刷情報(、 、)が取得される。しかし、印刷情報リストに登録されるのは印刷情報 のみとなる。

【 0 0 5 1 】

ステップ S 3 0 3 では、CPU 4 0 1 は、ステップ S 2 0 5 で取得した印刷情報中に含まれているユーザ名(アカウント名でも良い)と、ユーザ情報リストから読み出したユーザ情報中のユーザ名(アカウント名でも良い)と、を比較する。この比較の結果、ステップ S 2 0 5 で取得した印刷情報中に含まれているユーザ名が、ユーザ情報リスト内のいずれかのユーザ情報中のユーザ名と一致した場合、処理はステップ S 3 0 4 に進む。一方、ステップ S 2 0 5 で取得した印刷情報中に含まれているユーザ名が、ユーザ情報内のユーザ名のいずれでもない場合は、処理はステップ S 3 0 5 に進む。

【 0 0 5 2 】

ここで、「ステップ S 2 0 5 で取得した印刷情報中に含まれているユーザ名が、ユーザ情報リストのユーザ名のいずれでもない場合」とは、例えば次のようなケースが考え得る。例えば、クライアント端末装置 1 7 0 から管理者権限で印刷データを送信したケースである。また、印刷装置を使用する際に認証処理が必要な場合では、次のようなケースも考え得る。即ち、印刷装置を使用する為にクライアント端末装置からサーバ装置 1 0 0 に送信したユーザ情報と、サーバ装置 1 0 0 にログインする為にクライアント端末装置からサーバ装置 1 0 0 に送信したユーザ情報とが異なる場合である。

【 0 0 5 3 】

ステップ S 3 0 4 で CPU 4 0 1 はセキュリティソフトウェア 1 0 3 を実行し、ステップ S 2 0 5 で取得した印刷情報を、ユーザ情報リストにおいて該印刷情報とユーザ名が一致するユーザ情報に対応するユーザの印刷ログとして外部記憶装置 4 0 5 に記録する。例えば上記の例の場合、ステップ S 2 0 5 で取得した印刷情報中に含まれているユーザ名は「ユーザ A」であるので、この印刷情報をユーザ A の印刷ログとして外部記憶装置 4 0 5 に記録する。

【 0 0 5 4 】

10

20

30

40

50

また、複数のクライアント端末装置 170 から印刷が実行される環境においては、印刷情報に含まれる PC 名で、まずフィルタをかけたのち、ユーザ情報と印刷情報とを印刷ログとして出力してもよい。

【0055】

一方、ステップ S305 では、CPU401 は、セキュリティソフトウェア 103 を実行し、サーバ装置 100 に現在ログイン中のユーザが 1 名であるか否かを判断する。これは、ユーザ情報リストに登録されているユーザ情報が 1 名分であるか否かを判断すればよい。この判断の結果、サーバ装置 100 に現在ログイン中のユーザが 1 名である（ユーザ情報リストに登録されているユーザ情報が 1 名分である）場合には、処理はステップ S306 に進む。一方、サーバ装置 100 に現在ログイン中のユーザが 2 名以上である（ユーザ情報リストに登録されているユーザ情報が 2 名分以上である）場合には、処理はステップ S307 に進む。

10

【0056】

ステップ S306 では、CPU401 は、セキュリティソフトウェア 103 を実行し、ステップ S205 で取得した印刷情報を、ユーザ情報リストに登録されている 1 名分のユーザ情報に対応するユーザの印刷ログとして外部記憶装置 405 に記録する。

【0057】

一方、ステップ S307 で CPU401 は、セキュリティソフトウェア 103 を実行し、ステップ S205 で取得した印刷情報を印刷ログとして記録する若しくは破棄する。前者の場合、ユーザ情報リストに登録されている全て若しくは一部のユーザ情報に対応するユーザの印刷ログとして外部記憶装置 405 に記録しても良いし、不明者の印刷ログとして外部記憶装置 405 に記録しても良い。どのユーザに対する印刷ログとして記録するのかについては予め設定しておいても良いし、その都度サーバ装置 100 の操作者が操作部 404 を用いて指定しても良い。

20

【0058】

なお、CPU401 は、規定時間ごとに、印刷情報リストに登録されている印刷情報を消去する。この規定時間については特定の時間に限るものではないが、例えば、あるクライアント端末装置から印刷情報を受信してから次のクライアント端末装置から印刷情報を受信するまでの平均的な時間間隔（数秒）をこの「規定時間」としても良い。

【0059】

30

また、ログインユーザが一人ではなかった場合、印刷が実行された時間帯のログインユーザ毎の操作履歴を取得し、特定の操作をした（例えば、印刷する際の印刷設定ウィンドウを表示、印刷されたドキュメント名と同じドキュメント名を閲覧していた等）ユーザを、印刷を実行したユーザであると特定してもよい。

【0060】

以上説明したシステムの動作について、図 7 の模式図を用いて説明する。図 7 では、ユーザ A が使用するクライアント端末装置 701、ユーザ B が使用するクライアント端末装置 702、ユーザ C が使用するクライアント端末装置 703 がサーバ装置 100 に接続されている。103a ~ 103c はそれぞれ、セキュリティソフトウェア 103 において、クライアント端末装置 701 ~ 703 のそれぞれを担当する部分である。

40

【0061】

セキュリティソフトウェア 103a ~ 103c のそれぞれは、対応するクライアント端末装置からユーザ情報を受けると上記認証処理を行うと共に、ユーザ情報リストへのユーザ情報登録を行う。また、セキュリティソフトウェア 103a ~ 103c のそれぞれは、スプーラ 104 の動作を監視しており、印刷に係る印刷情報を取得すると、該取得した印刷情報をセキュリティソフトウェア 103 に対して送出する。そしてセキュリティソフトウェア 103 は、それぞれの印刷情報を取得すると、上記のようにして、この印刷情報を用いてユーザの印刷ログを作成する。

【0062】

このように、本実施形態によれば、複数のユーザが同時使用可能な情報処理装置におい

50

て、複数名のユーザがログインして印刷を実行した場合であっても、一人のユーザに印刷ログを割り当てることも可能となる。

【 0 0 6 3 】

〔 第 2 の実施形態 〕

また、ポーリングのため、印刷した際に書き出される複数の印刷情報が、印刷情報毎に異なる（例えば、印刷枚数、印刷時刻）場合がある。そこで、まず、印刷を行ったユーザを特定し、次に、所定の条件（例えば、印刷枚数が一番多い、印刷時刻が一番新しい）に一致しているか判断し、一致している印刷情報を特定されたユーザに関連付け、印刷を行ったユーザの印刷ログとして出力してもよい。以上から、複数ユーザが同時に使用可能な情報処理装置の使用において、印刷情報とユーザを関連付けることができ、印刷を行ったユーザの印刷ログとして出力できる。

10

【 0 0 6 4 】

複数のユーザが同時に使用可能な情報処理装置の使用において、印刷情報と印刷を行ったユーザを関連付けることができれば、以下の処理も行うことができる。印刷情報には、印刷装置のIPアドレスを含むため、IPアドレスとユーザを関連付ければユーザ毎の印刷の使用を制御することができる。例えば、複数の部門が複数の印刷装置を使用できる環境である場合、ユーザの属する部門に関係のない他部門の印刷を閲覧、または盗用することができてしまう。そこで、セキュリティソフトウェア 1 0 3 は、印刷が開始された時（印刷状態が印刷開始）の印刷情報を取得し、予め記憶されているユーザと印刷を許可する印刷装置のIPアドレスを関連付けたテーブルを参照して、印刷の制御（許可/不許可）を行う。印刷装置のIPアドレスとユーザを関連付けたテーブルを参照することにより、より情報漏洩の抑制を行うことが可能となる。

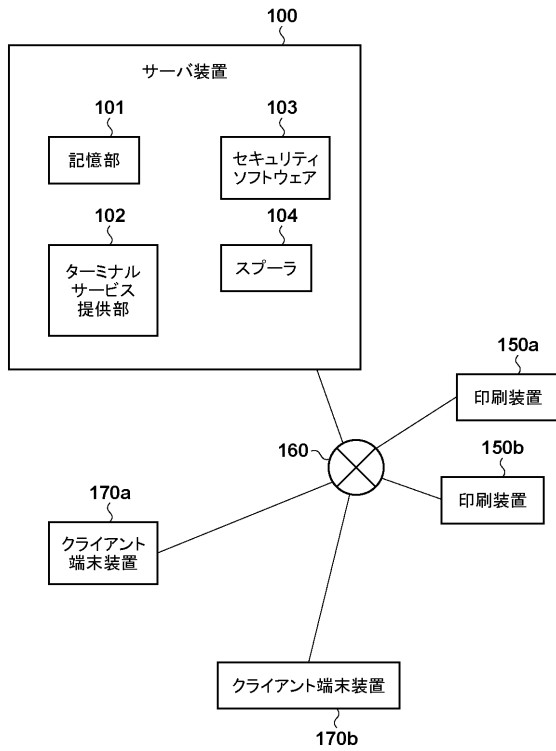
20

【 0 0 6 5 】

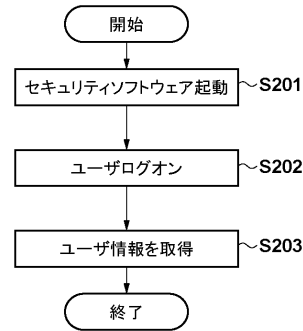
また、印刷装置は、白黒印刷可能な印刷装置（カラー印刷不可能）と、カラー印刷可能な印刷装置が存在する。事務業務のユーザには白黒印刷、営業業務のユーザにはカラー印刷、社内処理のために使用されるドキュメントは白黒印刷、社外で使用されるドキュメントはカラー印刷など、ユーザやドキュメント名にあわせた印刷の制御を行うことも可能である。具体的には、セキュリティソフトウェア 1 0 3 は、印刷が開始された時（印刷状態が印刷開始）の印刷情報を取得し、予め記憶されているユーザ/ドキュメント名とプリンタ名（色設定を含む）を関連付けたテーブルを参照して、印刷の制御（許可/不許可）を行う。ユーザ/ドキュメント名とプリンタ名を関連付けたテーブルを参照することにより、ユーザの利便性がよい印刷コストの削減を行うことが可能となる。

30

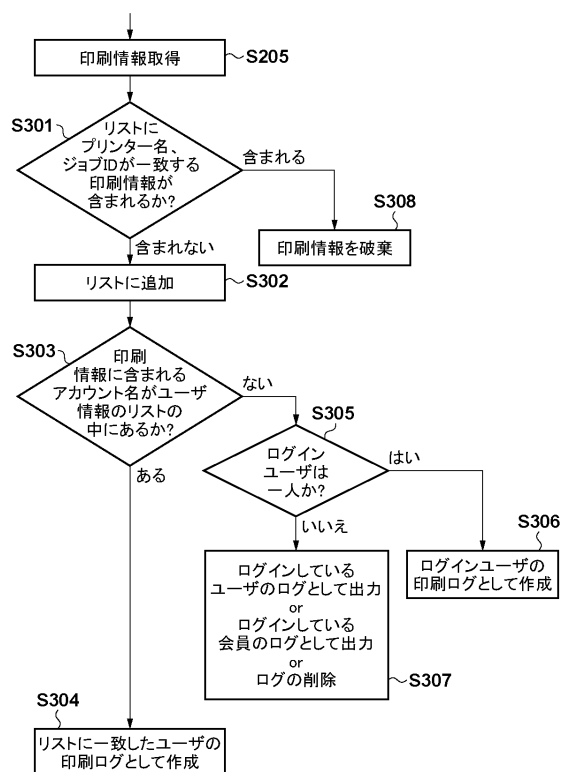
【図 1】



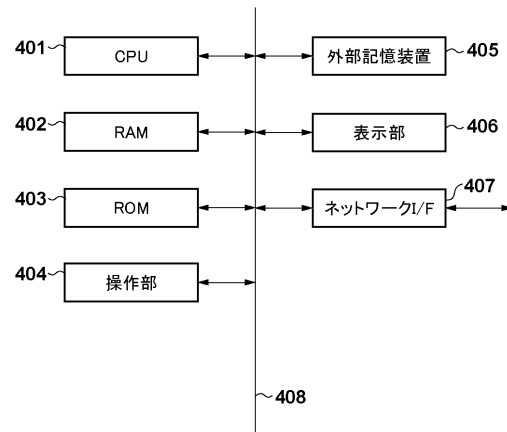
【図 2】



【図 3】



【図 4】



フロントページの続き

(51)Int.Cl. F I
G 0 6 F 3/12 3 0 7

(72)発明者 関口 あずさ
埼玉県秩父市下影森 1 2 4 8 番地 キヤノン電子株式会社内

審査官 佐賀野 秀一

(56)参考文献 特開 2 0 0 4 - 1 7 8 2 4 9 (J P , A)
特開 2 0 0 2 - 1 6 3 0 9 7 (J P , A)
特開 2 0 0 8 - 0 5 2 6 7 9 (J P , A)
特開 2 0 0 3 - 3 0 8 1 8 5 (J P , A)
特開 2 0 0 7 - 2 9 3 6 7 3 (J P , A)
特開 2 0 0 2 - 0 1 4 7 9 1 (J P , A)
特開 2 0 0 3 - 3 0 8 1 9 2 (J P , A)
特開 2 0 0 5 - 1 4 1 5 5 6 (J P , A)

(58)調査した分野(Int.Cl. , D B 名)
G 0 6 F 3 / 0 9 - 3 / 1 2
B 4 1 J 2 9 / 0 0 - 2 9 / 7 0
H 0 4 N 1 / 0 0