

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5127520号
(P5127520)

(45) 発行日 平成25年1月23日 (2013. 1. 23)

(24) 登録日 平成24年11月9日 (2012. 11. 9)

(51) Int. Cl.		F I		
H04N	1/00	(2006.01)	H04N	1/00 107Z
G03G	21/00	(2006.01)	G03G	21/00 388
B41J	29/38	(2006.01)	B41J	29/38 Z
G06F	3/12	(2006.01)	G06F	3/12 K

請求項の数 5 (全 16 頁)

(21) 出願番号	特願2008-67880 (P2008-67880)	(73) 特許権者	000001007 キヤノン株式会社 東京都大田区下丸子3丁目30番2号
(22) 出願日	平成20年3月17日 (2008. 3. 17)	(74) 代理人	100125254 弁理士 別役 重尚
(65) 公開番号	特開2009-225152 (P2009-225152A)	(72) 発明者	伊藤 千恵 東京都大田区下丸子3丁目30番2号 キ ヤノン株式会社内
(43) 公開日	平成21年10月1日 (2009. 10. 1)		
審査請求日	平成23年3月16日 (2011. 3. 16)	審査官	橋爪 正樹
		(56) 参考文献	特開2007-304861 (JP, A)

最終頁に続く

(54) 【発明の名称】 画像形成装置及び画像形成装置の制御方法

(57) 【特許請求の範囲】

【請求項 1】

画像形成装置であって、前記画像形成装置は前記画像形成装置のユーザ毎の権限情報を発行するアクセスコントロール装置と、前記画像形成装置のジョブ履歴を管理するジョブ履歴管理装置のそれぞれと通信可能であり、前記画像形成装置にログインしたユーザの権限情報を前記アクセスコントロール装置から取得する取得手段と、前記ユーザによるジョブの実行指示により前記取得手段が取得した前記権限情報を参照して前記ジョブの実行が可能かを判定する第1の判定手段と、前記第1の判定手段が前記ジョブの実行が可能であると判定しなかった場合、前記ジョブの履歴を前記ジョブ履歴管理装置へ送信することを条件に前記ジョブを実行することが可能かを、ジョブの履歴を前記ジョブ履歴管理装置へ送信することを前記権限情報が制限するジョブの実行を許可する条件として示す、前記権限情報に含まれる許可情報に基づいて判定する第2の判定手段と、前記第1、第2の判定手段のいずれかが前記ジョブの実行が可能と判定した場合に前記ジョブを実行する実行手段と、前記第2の判定手段が前記ジョブの実行が可能と判定したことに基づいて前記実行手段により実行されたジョブの履歴を取得して前記ジョブ履歴管理装置へ送信する送信手段と

、

10

20

を備えることを特徴とする画像形成装置。

【請求項 2】

前記第 2 の判定手段により前記ジョブの実行が可能と判定された場合及び可能と判定されなかった場合にその旨表示する表示手段を備えることを特徴とする請求項 1 記載の画像形成装置。

【請求項 3】

前記ジョブの履歴は複数種類の情報を含み、前記許可情報は、前記実行手段が実行したジョブの履歴のうち、前記ジョブ履歴管理装置へ送信する情報の種類を特定する情報を含むことを特徴とする、請求項 1 または 2 に記載の画像形成装置。

【請求項 4】

前記第 1 の判定手段が前記ジョブを実行可能でないと判定し、前記第 2 の判定手段が、前記許可情報が示す条件に従えば前記ジョブを実行可能であると判定した場合に、前記ジョブの実行指示の操作を行ったユーザに対して前記許可情報が示す条件に従って前記ジョブを実行するか否かを問い合わせる問い合わせ手段と、

前記実行手段は、前記問い合わせ手段による問い合わせに応答して前記ユーザから前記ジョブを実行する旨の指示を受け付けたことに基づいて前記ジョブを実行し、前記問い合わせ手段による問い合わせに応答して前記ユーザから前記ジョブを実行する旨の指示を受け付けなかったことに基づいて前記ジョブを実行しないことを特徴とする、請求項 1 乃至請求項 3 のいずれか 1 項に記載の画像形成装置。

【請求項 5】

画像形成装置の制御方法であって、

前記画像形成装置は前記画像形成装置のユーザ毎の権限情報を発行するアクセスコントロール装置と、前記画像形成装置のジョブ履歴を管理するジョブ履歴管理装置のそれぞれと通信可能であり、

前記画像形成装置にログインしたユーザの権限情報を前記アクセスコントロール装置から取得する取得工程と、

前記ユーザによるジョブの実行指示により前記取得工程で取得された前記権限情報を参照して前記ジョブの実行が可能か判定する第 1 の判定工程と、

前記第 1 の判定工程が前記ジョブの実行が可能であると判定しなかった場合、前記ジョブの履歴を前記ジョブ履歴管理装置へ送信することを条件に前記ジョブの実行が可能かを、
ジョブの履歴を前記ジョブ履歴管理装置へ送信することを前記権限情報が制限するジョブの実行を許可する条件として示す、前記権限情報に含まれる許可情報に基づいて判定する第 2 の判定工程と、

前記第 1、第 2 の判定工程のいずれかで前記ジョブの実行が可能と判定した場合に前記ジョブを実行する実行工程と、

前記第 2 の判定工程で前記ジョブの実行が可能と判定したことに基づいて前記実行工程で実行したジョブの履歴を取得して前記ジョブ履歴管理装置へ送信する送信工程と、
を備えることを特徴とする制御方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、アクセスコントロール技術に特徴のある画像形成装置及び画像形成装置の制御方法に関する。

【背景技術】

【0002】

近年、画像形成装置の高機能化、デジタル化に伴い、画像形成装置が扱う情報が多様化し、また、簡単な操作での出力が可能となっている。その一方、セキュリティ意識の高まりから、機密漏洩の防止、また、漏洩が発生した場合には、漏洩源、漏洩ルートの特定が要求される。

【0003】

機密漏洩防止の一環として、紙出力、電子データ送信等のジョブの履歴を、ジョブを実行したユーザの情報とともに記録しておくジョブ履歴管理システムがある。

【0004】

また、画像形成装置の利用に際し、アクセスコントロールを行い、機能が必要なユーザにのみ利用可能とすることで、機密漏洩の抑止を図るシステム（アクセスコントロールシステム）がある。

【0005】

特許文献1には、ジョブ履歴管理システムにおいて、履歴を取得する旨をユーザに通知することで、不正使用の抑止と無断で個人情報を履歴に残すことによる諸問題を回避することが記載されている。

10

【0006】

また、特許文献2には、認証機能により、利用権限を持たないユーザに対し、利用権限を保持するユーザが一時的に利用権限を付与することで、権限を有していないユーザも利用可能となる技術が記載されている。

【特許文献1】特開2006-295529号公報

【特許文献2】特開2006-235757号公報

【発明の開示】

【発明が解決しようとする課題】

【0007】

しかしながら、特許文献1記載の技術では、履歴の取得の通知は、監視文書に対して設定が可能であるが、ジョブ種での設定はなされていない。また、ジョブの履歴を取得する場合、ユーザ問わず画一的に設定に従った履歴を取得することになる。

20

【0008】

また、特許文献2記載の技術では、権限を持つユーザの存在が必須であり、権限を持つユーザが不在の場合、権限を保持しないユーザは機能を実行することができない。

【0009】

このように、ジョブ履歴管理システムもアクセスコントロールシステムも、機密漏洩抑止という同じ目的を持ちながら、それぞれが独立に機能していたため、効率的な連携ができていないという現状があった。

【0010】

本発明の目的は、機密漏洩抑止の信頼性を高めることができる画像形成装置及び画像形成装置の制御方法を提供することにある。

30

【課題を解決するための手段】

【0011】

上記目的を達成するために、本発明の画像形成装置は、画像形成装置であって、前記画像形成装置は前記画像形成装置のユーザ毎の権限情報を発行するアクセスコントロール装置と、前記画像形成装置のジョブ履歴を管理するジョブ履歴管理装置のそれぞれと通信可能であり、前記画像形成装置にログインしたユーザの権限情報を前記アクセスコントロール装置から取得する取得手段と、前記ユーザによるジョブの実行指示により前記取得手段が取得した前記権限情報を参照して前記ジョブの実行が可能かを判定する第1の判定手段と、前記第1の判定手段が前記ジョブの実行が可能であると判定しなかった場合、前記ジョブの履歴を前記ジョブ履歴管理装置へ送信することを条件に前記ジョブを実行することが可能かを、ジョブの履歴を前記ジョブ履歴管理装置へ送信することを前記権限情報が制限するジョブの実行を許可する条件として示す、前記権限情報に含まれる許可情報に基づいて判定する第2の判定手段と、前記第1、第2の判定手段のいずれかが前記ジョブの実行が可能と判定した場合に前記ジョブを実行する実行手段と、前記第2の判定手段が前記ジョブの実行が可能と判定したことに基づいて前記実行手段により実行されたジョブの履歴を取得して前記ジョブ履歴管理装置へ送信する送信手段と、を備えることを特徴とする。

40

【発明の効果】

50

【0012】

本発明の画像形成装置及び画像形成装置の制御方法によれば、機密漏洩抑止の信頼性を高めることができる。

【発明を実施するための最良の形態】

【0013】

以下、本発明の実施の形態を図面を参照しながら詳細に説明する。

【0014】

図1は、本発明の実施の形態に係る画像形成システムの構成図である。

【0015】

本画像形成システムは、画像形成装置100、サービスプロバイダ101、データサーバ102、セキュリティエージェント103及びディレクトリサーバ104がLAN105により接続されることで構築されている。

10

【0016】

サービスプロバイダ101は、ジョブ履歴管理システム（ジョブ履歴管理装置）の主要構成要素である。セキュリティエージェント103は、アクセスコントロールシステム（アクセスコントロール装置）の主要構成要素である。

【0017】

画像形成装置100は、コピー、FAX、スキャン、プリント等のジョブ及びジョブを実行したユーザに関する履歴情報107をサービスプロバイダ101に送信し、サービスプロバイダ101は、履歴情報107をデータサーバ102に格納する。

20

【0018】

セキュリティエージェント103は、ユーザ別の権限情報をアクセス制限情報106として発行するサーバである。ディレクトリサーバ104は、ユーザやプリンタ情報を一元管理するデータベースである。

【0019】

セキュリティエージェント103は、ユーザ毎の情報をディレクトリサーバ104から獲得する。画像形成装置100は、セキュリティエージェント103から生成されるアクセス制限情報106に従って利用できる機能の制限を行う。

【0020】

図2は、本発明の実施の形態に係る画像形成装置のコントローラユニットのブロック図である。

30

【0021】

図2において、コントローラユニット200は、画像入力装置であるスキャナ216及び画像出力装置であるプリンタ217に接続され、また、LAN105や公衆回線219と接続されている。そして、コントローラユニット200は、画像情報やデバイス情報の入出力の制御を行う。

【0022】

コントローラユニット200において、主にCPU203が画像形成装置全体を制御する。操作部I/F204は、操作部218とのインタフェース部で、操作部218に表示する画像データを操作部218に対して出力する。また、操作部218からユーザが入力した情報をCPU203に伝える役割も担っている。

40

【0023】

ネットワークI/F205は、LAN105に接続され、情報の入出力を行う。モデム206は、公衆回線219に接続され、データ送受信を行うための変調復調処理を行う。

【0024】

RAM207は、CPU203が動作するためのシステムワークメモリであり、画像データを一時記憶するための画像メモリとしても利用される。ROM208は、ブートROMとして利用され、画像形成装置のブートプログラムが格納されている。

【0025】

HDD（ハードディスクドライブ）209は、システムソフトウェア、画像データ等を

50

格納する。このHDD 209には、ネットワーク（LAN 105）に接続されているノードに関する画像出力速度、設置位置等の情報がアドレスごとに保存される場合もある。これらのデバイスがシステムバス 201 上に配置される。

【0026】

イメージバス I / F 210 には、システムバス 201 と画像データを高速で転送するイメージバス 202 が接続されており、イメージバス I / F 210 は、データ構造を変換するバスブリッジとして機能する。

【0027】

イメージバス 202 は、PCI バスまたは IEEE 1394 等の高速バスで構成される。イメージバス 202 上には以下のデバイスが配置される。

10

【0028】

ラストイメージプロセッサ（RIP）211 は、PDL コードをラスト画像に展開する。デバイス I / F 212 は、画像入出力デバイスであるスキャナ 216 やプリンタ 217 とコントローラユニット 200 を接続する。

【0029】

スキャナ画像処理部 213 は、入力画像データに対し補正、加工、編集を行う。プリンタ画像処理部 214 は、プリント出力画像データに対して、プリンタに合わせた補正、解像度変換等を行う。画像圧縮部 215 は、多値画像データは JPEG、2 値画像データは JBIG、MMR、MH の圧縮伸張処理を行う。

【0030】

20

図 3 は、図 1 におけるサービスプロバイダ、データサーバ、セキュリティエージェント及びディレクトリサーバのハード構成例を示す図である。いずれも汎用 PC なので同じブロック図としている。

【0031】

図 3 において、各装置では、バス 300 上に、以下に説明する各種デバイスが接続されている。

【0032】

CPU 301 は、各種制御や演算を行う。RAM 302 は、揮発性メモリであり、CPU 301 の演算結果等が格納される。また、本発明を実現するためのプログラムをロードするための一時記憶として利用される。

30

【0033】

ROM 303 は、不揮発性メモリであり、CPU 301 を動作させるためのプログラムやフォントデータ等が格納されている。尚、ROM 303 は、書き換え可能なものであってもよい。また、CPU 301 を動作させるプログラムは、RAM 302 上に存在しているてもよい。

【0034】

CPU 301 は、入力部 304、出力部 305、ネットワークインタフェース 306、ディスクインタフェース 307、及びユニット制御部 309 に対して指示等を与える。また、CPU 301 は、処理結果や入力結果等の一時的に必要な情報を RAM 302 に格納する。

40

【0035】

入力部 304 は、各装置間の入力データ等を受け取る。出力部 305 は、必要に応じて情報表示を行う。ネットワークインタフェース 306 は、LAN 等の外部ネットワークとの接続を行う。ディスクインタフェース 307 は、ハードディスク 308 に接続されている。

【0036】

ハードディスク 308 には、各データ、プログラム等を保管すべきデータが格納されている。ハードディスク 308 に格納されているデータは、必要に応じて、CPU 301 からの指示により、RAM 302 に読み出されて利用される。また、ハードディスク 308 は、複数存在しているてもよい。

50

【0037】

図4は、本発明の実施の形態に係る画像形成システムの機能ブロック図である。

【0038】

図4において、認証情報保持手段401、ユーザ認証手段402、実行可能判定手段403及び条件付実行可能判定手段404はアクセスコントロールシステム（アクセスコントロール装置）の構成要素である。

【0039】

認証情報保持手段401は、ディレクトリサーバ104のハードディスク308等に相当し、例えば、Windows（登録商標）ドメインのユーザ及びユーザグループ情報を管理するディレクトリサーバ等でユーザ名、パスワード、所属、権限情報等を保持する。

10

【0040】

ユーザ認証手段402は、セキュリティエージェント103のCPU301に相当し、認証情報保持手段401のデータとログインユーザを照合し、アクセス制限情報106を生成する。

【0041】

実行可能判定手段403は、同様にセキュリティエージェント103のCPU301に相当し、アクセス制限情報106をもとに、ユーザが実行しようとする機能が実行可能かどうかを判定する。

【0042】

条件付実行可能判定手段404も同様に、セキュリティエージェント103のCPU301に相当し、実行可能判定手段403で実行不可能と判定された場合、さらにアクセス制限情報106から条件付で実行可能か否かを判定する。

20

【0043】

表示手段405、入力手段406及び実行手段407は画像形成装置の構成要素である。

【0044】

表示手段405は、操作部218に相当し、ユーザに対し入力画面や機能実行不可メッセージを表示する。入力手段406も同様に操作部218に相当し、入力手段406を介し、ユーザの操作指示や条件の承諾／拒否の入力を受け付ける。

【0045】

入力手段406より受け取った指示に基づき、実行手段407は指定の処理を実行する。実行手段407は、スキャナ216やプリンタ217に相当する。

30

【0046】

履歴取得レベル判定手段408、履歴取得レベル保持手段409及び履歴格納手段410は、ジョブ履歴管理システム（ジョブ履歴管理装置）の構成要素である。

【0047】

履歴取得レベル判定手段408は、サービスプロバイダ101のCPU301に相当する。履歴取得レベル判定手段408は、実行手段407で実行されようとする処理について、実行処理の履歴を取得するか否か、取得する場合はどのレベルまでの履歴を取得するかを、履歴取得レベル保持手段409に問い合わせ、その応答を待つ。

40

【0048】

履歴取得レベル保持手段409は、サービスプロバイダ101のRAM302やハードディスク308に相当する。実行手段407は、履歴取得レベル判定手段408により判定された履歴を履歴格納手段410に記録する。履歴格納手段410は、データサーバ102のハードディスク308に相当する。

【0049】

本実施の形態では、履歴取得レベル判定手段408や履歴取得レベル保持手段409は、サービスプロバイダ101が保持するとしたが、アクセス制限情報106に記載されていてもよいし、画像形成装置100のRAM207やHDD209が保持してもよい。

【0050】

50

図5は、図4における画像形成装置、アクセスコントロールシステム、ジョブ履歴管理システムそれぞれの、通常のジョブ処理の手順を示すフローチャートである。

【0051】

図5(a)において、画像形成装置100にユーザがログインすると(ステップS501)、画像形成装置100はセキュリティエージェント103に、ログインユーザのアクセス制限情報106を要求し(ステップS502)、これを取得する(ステップS503)。

【0052】

ユーザからのジョブ実行指示があると(ステップS504)、取得したアクセス制限情報106に従い機能の制限を行い(ステップS505)、ジョブを実行する(ステップS506)。実行ジョブの履歴を取得し(ステップS507)、取得した履歴をサービスプロバイダ101に送信して(ステップS508)、処理を終了する。

10

【0053】

図5(b)において、アクセスコントロールシステムを構成するセキュリティエージェント103は、画像形成装置100よりアクセス制限情報の発行要求を取得する(ステップS511)。そして、ディレクトリサーバ104よりユーザの権限情報(許可情報)を取得し、アクセス制限情報106を生成する(ステップS512)。生成したアクセス制限情報106を画像形成装置100に送信して(ステップS513)、処理を終了する。

【0054】

図5(c)において、ジョブ履歴管理システムを構成するサービスプロバイダ101は、画像形成装置100よりジョブ履歴情報を受信する(ステップS521)。自身のHDD308、RAM302もしくは画像形成装置100よりどのレベルまでの履歴を取得するかの情報取得し(ステップS522)、取得した情報に従い必要な履歴情報を抽出(フィルタリング処理)する(ステップS523)。

20

【0055】

抽出した情報を自身のHDD308もしくはデータサーバ102へ転送して履歴を保存し(ステップS524)、処理を終了する。

【0056】

ここでは、サービスプロバイダ101が履歴情報のレベルを取得し、必要な履歴情報を抽出するとしたが、画像形成装置100が既に必要な情報だけを送信してもよいし、データサーバ102が必要な情報だけ保存してもよい。

30

【0057】

図6は、図4の画像形成システムによって実行される制限ジョブ処理の第1の例の手順を示すフローチャートである。

【0058】

ユーザは前述の通り、画像形成装置100にログインし(ステップS601)、アクセス制限情報106を取得する(ステップS602)。ステップS602は、画像形成装置へのログインによりアクセス制限情報106を取得する取得手段として機能する。ユーザが入力手段406を介し、ジョブの実行を指示する(ステップS603)。

【0059】

40

実行可能判定手段403は、ユーザ認証手段402が生成したアクセス制限情報106を参照し、ユーザが実行しようとするジョブが実行可能か判定する(ステップS604)。ステップS604は、ジョブの実行指示により取得手段で取得されたアクセス制限情報106を参照してジョブの実行が可能か判定する第1の判定手段として機能する。

【0060】

実行可能な場合(ステップS604-YES)、ジョブを実行し(ステップS609)、制限ジョブでない場合も履歴取得の必要がある場合は(ステップS610-YES)、履歴を取得する(ステップS611)。履歴取得の必要がない場合は(ステップS610-NO)そのまま終了する。

【0061】

50

ジョブ実行が不可能な場合（ステップS604-NO）、条件付実行可能判定手段404は、ジョブ履歴を取得することを条件に実行可能なジョブであるかを判定する（ステップS605）。ステップS605は、第1の判定手段によりジョブの実行が不可能と判定された場合にジョブ履歴を取得する第2の取得手段として、また、第2の取得手段で取得されたジョブ履歴を参照してジョブが実行可能か判定する第2の判定手段として機能する。

【0062】

ジョブ履歴取得が実行可能条件でない場合（実行可能なジョブでない場合）（ステップS605-NO）、表示手段405に実行不可能な旨を通知（表示）し（ステップS606）、終了する。

10

【0063】

ジョブ履歴取得により実行が可能な場合（ステップS605-YES）、表示手段405はユーザに対し、ジョブ履歴取得によりジョブ実行が可能な旨を通知（表示）する（ステップS607）。

【0064】

ステップS606、ステップS607は、第2の判定手段によりジョブの実行が可能と判定された場合及び不可能と判定された場合にその旨表示する表示手段として機能する。

【0065】

ユーザが入力手段406を介し、ジョブ履歴取得による実行を選択した場合（ステップS608-YES）、ジョブを実行し（ステップS609）、履歴を取得する（ステップS610-YES、ステップS611）。取得した履歴をサービスプロバイダ101に送信して（ステップS612）、終了する。

20

【0066】

ステップS609は、第1、第2の判定手段によりジョブの実行が可能と判定された場合にジョブを実行する実行手段として機能する。また、ステップS611は、実行手段により実行されたジョブの履歴を取得する第3の取得手段として機能する。

【0067】

図6では、取得する履歴のレベルはジョブ履歴管理システムに設定されているものとしている。図6のフローチャートによれば、アクセスコントロールシステムによって実行が制限されるジョブに対して、ジョブの実行履歴をジョブ履歴管理システムに保存することを条件に制限されたジョブの実行を許可することができる。これにより、ジョブ履歴管理システムとアクセスコントロールシステムが連携しながらセキュリティのレベルを落とすことなくユーザに対してフレキシビリティの高い機能提供を実現することが可能になる。

30

【0068】

図7は、図4の画像形成システムによって実行される制限ジョブ処理の第2の例の手順を示すフローチャートである。

【0069】

具体的には、図7は、アクセス制限情報106に制限ジョブ実行時に取得するジョブ履歴のレベルが記載されている場合のフローチャートである。

【0070】

図7において、画像形成装置100にログインし（ステップS701）、アクセス制限情報106を取得する（ステップS702）。ユーザが入力手段406を介し、ジョブの実行を指示する（ステップS703）。

40

【0071】

実行可能判定手段403は、ユーザ認証手段402が生成したアクセス制限情報106を参照し、ユーザが実行しようとするジョブが実行可能か判定する（ステップS704）。

【0072】

実行可能な場合（ステップS704-YES）、ジョブを実行し（ステップS709）、制限ジョブでない場合もアクセス制限情報106に履歴取得レベルの記載がない場合は

50

(ステップS710-NO)、デフォルト設定を取得する(ステップS711)。そして、履歴を取得し(ステップS713)、取得した履歴をサービスプロバイダ101に送信して(ステップS714)、処理を終了する。

【0073】

アクセス制限情報106に履歴取得レベルの記載がある場合は(ステップS710-YES)、その履歴取得レベルを取得する(ステップS712)。ジョブ履歴には複数種類の情報が含まれている。取得レベルとは、アクセス制限を解除する条件として、最低限取得すべきジョブ履歴の種類を示す情報である。例えば、「ジョブを実行したユーザのID」と「ジョブを実行した日時」と「ジョブで用いられた画像データ」といった情報である。

【0074】

ステップS710は、実行手段によるジョブの実行後にアクセス制限情報106にジョブ履歴の取得レベルの設定があるか判定する第3の判定手段として機能する。ステップS711は、第3の判定手段によりジョブ履歴の取得レベルの設定がないと判定された場合にデフォルト設定を取得する第4の取得手段として機能する。ステップS712は、第3の判定手段によりジョブ履歴の取得レベルの設定があると判定された場合に取得レベルを取得する第5の取得手段として機能する。

【0075】

取得したレベルに従い履歴を取得し(ステップS713)、取得した履歴をサービスプロバイダ101に送信して(ステップS714)、終了する。

【0076】

ジョブ実行が不可能な場合(ステップS704-NO)、条件付実行可能判定手段404は、ジョブ履歴取得により、実行可能なジョブでないか判定する(ステップS705)。ジョブ履歴取得が実行可能条件でない場合(実行可能なジョブでない場合)(ステップS705-NO)、表示手段405に実行不可能な旨を通知(表示)し(ステップS706)、終了する。

【0077】

ジョブ履歴取得により実行が可能な場合(ステップS705-YES)、表示手段405はユーザに対し、ジョブ履歴取得によりジョブ実行が可能な旨を通知(表示)する(ステップS707)。ユーザが入力手段406を介し、ジョブ履歴取得による実行を選択した場合(ステップS708-YES)、ジョブを実行する(ステップS709)。以下、上述したステップS710以降の処理が実行される。

【0078】

デフォルト設定は不図示の設定手段(画像形成装置101、サービスプロバイダ102どちらでもよい)により設定される。

【0079】

図8は、図4の画像形成システムによって実行される制限ジョブ処理の第3の例の手順を示すフローチャートである。

【0080】

具体的には、図8は、アクセス制限情報106もしくはジョブ履歴管理システムに、制限ジョブ実行時に取得するジョブ履歴のレベルが記載されている場合のフローチャートである。

【0081】

図8において、画像形成装置100にログインし(ステップS801)、アクセス制限情報106を取得する(ステップS802)。ユーザが入力手段406を介し、ジョブの実行を指示する(ステップS803)。

【0082】

実行可能判定手段403は、ユーザ認証手段402が生成したアクセス制限情報106を参照し、ユーザが実行しようとするジョブが実行可能か判定する(ステップS804)。

【0083】

10

20

30

40

50

実行可能な場合（ステップS804－YES）、ジョブを実行し（ステップS809）、制限ジョブでない場合もアクセス制限情報106に履歴取得レベルの記載がある場合は（ステップS810－YES）、履歴取得レベルを取得する（ステップS811）。

【0084】

履歴取得レベルの記載がない場合は（ステップS810－NO）、ジョブ履歴管理システムにレベルの指定がないか判定し（ステップS812）、指定がある場合は（ステップS812－YES）、履歴取得レベルを取得する（ステップS813）。

【0085】

ステップS812は、第3の判定手段によりジョブ履歴の取得レベルの設定がないと判定された場合にジョブ履歴管理システムにジョブ履歴の取得レベルの設定があるか判定する第4の判定手段として機能する。

10

【0086】

指定がない場合は（ステップS812－NO）、デフォルト設定を取得する（ステップS814）。アクセス制限情報106または履歴管理システムから取得したレベルに従い、履歴を取得し（ステップS815）、サービスプロバイダ101に送信して（ステップS816）、終了する。

【0087】

ジョブ実行が不可能な場合（ステップS804－NO）、条件付実行可能判定手段404は、ジョブ履歴取得により、実行可能なジョブでないか判定する（ステップS805）。ジョブ履歴取得が実行可能条件でない場合（実行可能なジョブでない場合）（ステップS805－NO）、表示手段405に実行不可能な旨を通知（表示）し（ステップS806）、終了する。

20

【0088】

ジョブ履歴取得により実行が可能な場合（ステップS805－YES）、表示手段405はユーザに対し、ジョブ履歴取得によりジョブ実行が可能な旨を通知（表示）する（ステップS807）。

【0089】

ユーザが入力手段406を介し、ジョブ履歴取得による実行を選択した場合（ステップS808－YES）、ジョブを実行する（ステップS809）。そして、上述のステップS810以降の処理を実行する。

30

【0090】

ユーザが入力手段406を介し、ジョブ履歴取得による実行を選択しない場合（ステップS808－NO）、ジョブ実行が不可能である旨、表示手段405に表示する（ステップS806）。

【0091】

本実施の形態ではアクセス制限情報のレベルを優先するフローとなっているが、不図示の優先設定手段により、ジョブ履歴管理システムの設定を優先させてもよい。

【0092】

図7、図8の履歴取得レベルの設定により、全てのログを取得せず、必要に応じたログの取得が可能となる。また全てのログを取得しサービスプロバイダ101に転送し、履歴管理システム側で必要なログを抽出することも、転送する前に、必要なログを抽出することも可能となるため、より柔軟なシステムの構築が実現する。

40

【0093】

図9は、図4におけるユーザ認証手段により生成されたアクセス制限情報の第1の例を示す図である。

【0094】

XML形式で記述されているが形式は問わない。要素Attribute、属性ApplicationCategoryでジョブの実行許可、不許可、条件付許可について記載してある。図9では、Print、Copyカテゴリは許可、Sendカテゴリは不許可となっている。

50

【0095】

図10は、図4におけるユーザ認証手段により生成されたアクセス制限情報の第2の例を示す図である。

【0096】

XML形式で記述されているが形式は問わない。要素Attribute、属性ApplicationCategoryでジョブの実行許可、不許可、条件付許可について記載してある。図10では、Printカテゴリは許可、Copyカテゴリは条件付許可、Sendカテゴリは不許可となっている。また、要素Attribute、属性LimitedConditionで条件付許可のカテゴリに対する要求条件が記載されており、条件付許可カテゴリを実行するにはGetLog、即ち、ジョブ履歴の取得が要求されている。つまり、ジョブの履歴を取得することが不許可の種類のジョブを実行可能にするための許可条件として設定されていることになる。

10

【0097】

図10では、アクセス制限情報106には履歴取得レベルについては記載されていないため、ジョブ履歴を取得する際はデフォルト設定、もしくはジョブ履歴管理システム側で設定されたレベルに従い履歴を取得する。

【0098】

図11は、図4におけるユーザ認証手段により生成されたアクセス制限情報の第3の例を示す図である。

【0099】

20

XML形式で記述されているが形式は問わない。図10で記載されていた情報に加えて、Loginfo要素で、デフォルトで取得する履歴の項目、条件付カテゴリジョブ実行時に取得する履歴の項目の情報が記載されている。

【0100】

条件付カテゴリジョブを実行する際にはdefault要素の子要素、item要素で記載された項目に加えて、セクションID、ジョブ開始時間、ジョブ終了時間、デバイスID、ページ数の履歴も取得することが要求されている。

【0101】

図12は、図4の画像形成システムにおいて、取得された履歴の第1の例を示す図である。

30

【0102】

XMLで記載されているが形式は問わない。ジョブ種はコピー、LogID、UserID、ホストマシンIDが記録されている。

【0103】

図13は、図4の画像形成システムにおいて、取得された履歴の第2の例を示す図である。

【0104】

図11のアクセス制限情報106を持つユーザが条件付カテゴリジョブを実行した際の履歴に相当する。図12のログに加えてセクションID、ジョブ開始時間、ジョブ終了時間、デバイスID、ページ数が記録されている。

40

【図面の簡単な説明】

【0105】

【図1】本発明の実施の形態に係る画像形成システムの構成図である。

【図2】本発明の実施の形態に係る画像形成装置のコントローラユニットのブロック図である。

【図3】図1におけるサービスプロバイダ、データサーバ、セキュリティエージェント及びディレクトリサーバのハード構成例を示す図である。

【図4】本発明の実施の形態に係る画像形成システムの機能ブロック図である。

【図5】図4における画像形成装置、アクセスコントロールシステム、ジョブ履歴管理システムそれぞれの、通常のジョブ処理の手順を示すフローチャートである。

50

【図 6】図 4 の画像形成システムによって実行される制限ジョブ処理の第 1 の例の手順を示すフローチャートである。

【図 7】図 4 の画像形成システムによって実行される制限ジョブ処理の第 2 の例の手順を示すフローチャートである。

【図 8】図 4 の画像形成システムによって実行される制限ジョブ処理の第 3 の例の手順を示すフローチャートである。

【図 9】図 4 におけるユーザ認証手段により生成されたアクセス制限情報の第 1 の例を示す図である。

【図 10】図 4 におけるユーザ認証手段により生成されたアクセス制限情報の第 2 の例を示す図である。

10

【図 11】図 4 におけるユーザ認証手段により生成されたアクセス制限情報の第 3 の例を示す図である。

【図 12】図 4 の画像形成システムにおいて、取得された履歴の第 1 の例を示す図である。

【図 13】図 4 の画像形成システムにおいて、取得された履歴の第 2 の例を示す図である。

【符号の説明】

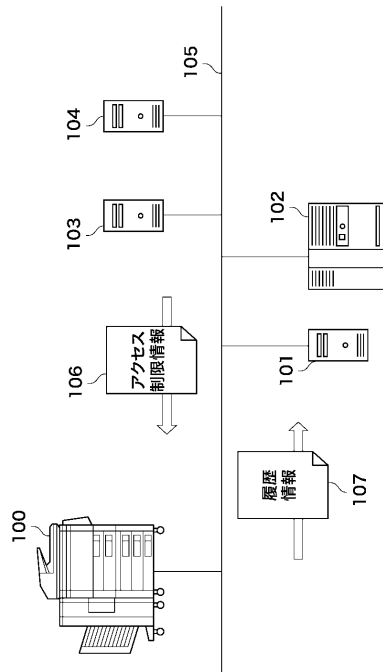
【0106】

- 100 画像形成装置
- 101 サービスプロバイダ
- 102 データサーバ
- 103 サービスエージェント
- 104 ディレクトリサーバ
- 106 アクセス制限情報
- 107 履歴情報
- 401 認証情報保持手段
- 402 ユーザ認証手段
- 403 実行可能判断手段
- 404 条件付実行可能判定手段
- 405 表示手段
- 406 入力手段
- 407 実行手段
- 408 履歴取得レベル判定手段
- 409 履歴取得レベル保持手段
- 410 履歴格納手段

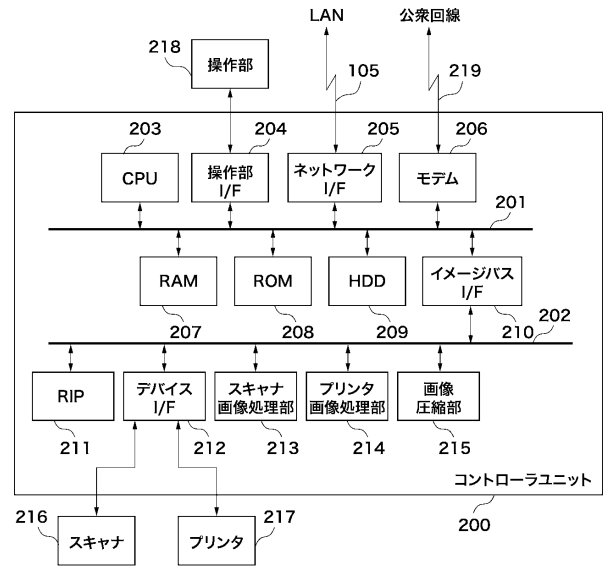
20

30

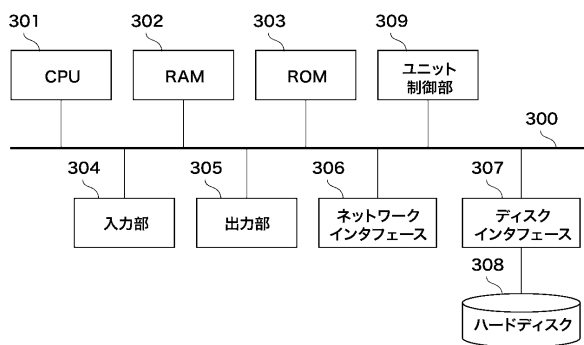
【図 1】



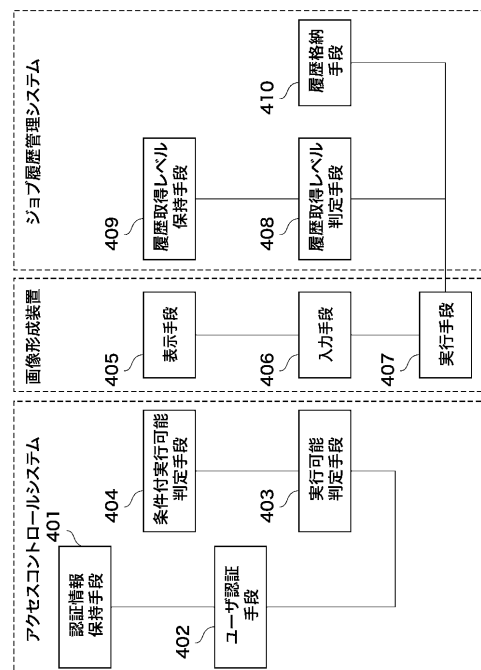
【図 2】



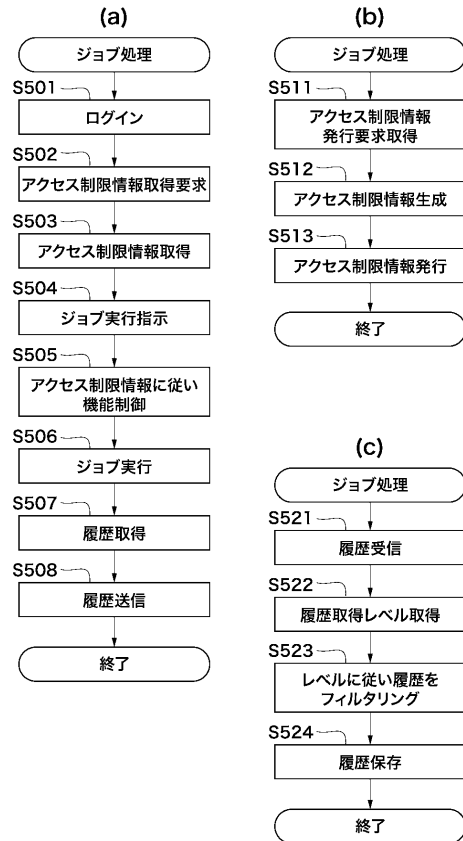
【図 3】



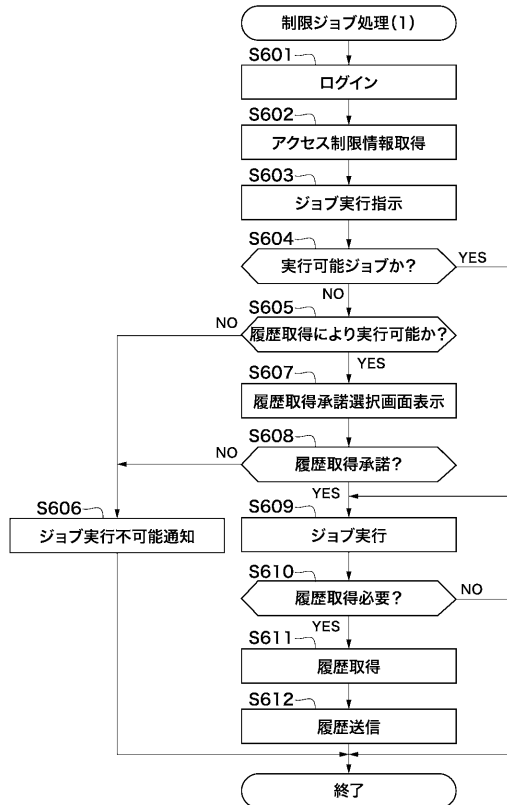
【図 4】



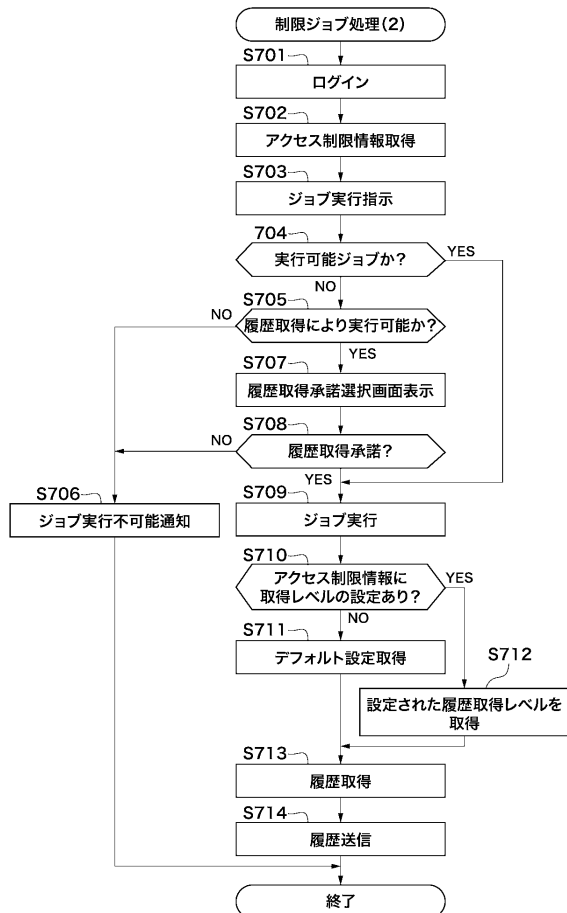
【図 5】



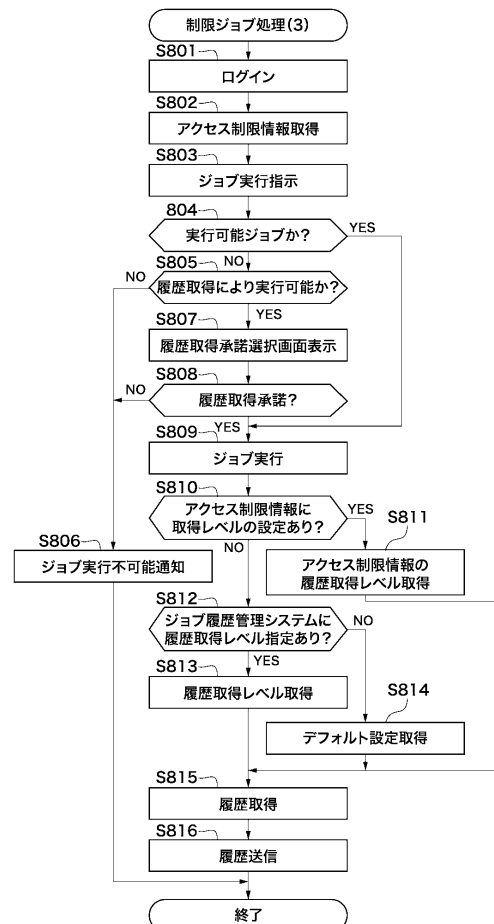
【図 6】



【図 7】



【図 8】



【図 9】

```

<AccessControllInfo>
  <UserInfo>
    <UserName>xxx</UserName>
    <ExtralInfo>
      <UserGroupList>
        <UserGroup>AAA</UserGroup>
        <UserGroup>CCC</UserGroup>
      </UserGroupList>
    </ExtralInfo>
    <DeviceInfo>
      <Attribute Name="ApplicationId">
        <AttributeValue Name="UsePossible">aaa</AttributeValue>
        <AttributeValue Name="UseImpossible">bbb</AttributeValue>
      </Attribute>
      <Attribute Name="ApplicationCategory">
        <AttributeValue Name="PrintCategory">Permit</AttributeValue>
        <AttributeValue Name="CopyCategory">Permit</AttributeValue>
        <AttributeValue Name="SendCategory">Deny</AttributeValue>
      </Attribute>
    </DeviceInfo>
  </UserInfo>
</AccessControllInfo>

```

【図 10】

```

<AccessControllInfo>
  <UserInfo>
    <UserName>xxx</UserName>
    <ExtralInfo>
      <UserGroupList>
        <UserGroup>AAA</UserGroup>
        <UserGroup>CCC</UserGroup>
      </UserGroupList>
    </ExtralInfo>
    <DeviceInfo>
      <Attribute Name="ApplicationId">
        <AttributeValue Name="UsePossible">aaa</AttributeValue>
        <AttributeValue Name="UseImpossible">bbb</AttributeValue>
      </Attribute>
      <Attribute Name="ApplicationCategory">
        <AttributeValue Name="PrintCategory">Permit</AttributeValue>
        <AttributeValue Name="CopyCategory">LimitedPermit</AttributeValue>
        <AttributeValue Name="SendCategory">Deny</AttributeValue>
      </Attribute>
      <Attribute Name="LimitedCondition">
        <AttributeValue Name="Requirement">GetLog</AttributeValue>
      </Attribute>
    </DeviceInfo>
  </UserInfo>
</AccessControllInfo>

```

【図 11】

```

<AccessControllInfo>
  <UserInfo>
    <UserName>xxx</UserName>
    <ExtralInfo>
      <UserGroupList>
        <UserGroup>AAA</UserGroup>
        <UserGroup>CCC</UserGroup>
      </UserGroupList>
      <LogInfo>
        <defaultitem>
          <item>JobType</item>
          <item>LogID</item>
          <item>UserID</item>
          <item>HostID</item>
        </defaultitem>
        <LimitedConditionSubsequent>
          <item>SectionID</item>
          <item>JobStartTime</item>
          <item>JobEndTime</item>
          <item>DeviceID</item>
          <item>PageCount</item>
        </LimitedConditionSubsequent>
      </LogInfo>
    </ExtralInfo>
    <DeviceInfo>
      <Attribute Name="ApplicationId">
        <AttributeValue Name="UsePossible">aaa</AttributeValue>
        <AttributeValue Name="UseImpossible">bbb</AttributeValue>
      </Attribute>
      <Attribute Name="ApplicationCategory">
        <AttributeValue Name="PrintCategory">Permit</AttributeValue>
        <AttributeValue Name="CopyCategory">LimitedPermit</AttributeValue>
        <AttributeValue Name="SendCategory">Deny</AttributeValue>
      </Attribute>
      <Attribute Name="LimitedCondition">
        <AttributeValue Name="Requirement">GetLog</AttributeValue>
      </Attribute>
    </DeviceInfo>
  </UserInfo>
</AccessControllInfo>

```

【図 12】

```

<?xml versions="1.0"?>
<jdd:LogData xmlns:jdd=http://xxx/xxx/xx>
  <jdd:parameter>
    <jdd:JobData JobType="Print"
      LogID="0001"
      UserID="1111"
      HostID="0011"
    </jdd:JobData>
  </jdd:parameter>
</jdd:LogData>

```

【図 13】

```

<?xml versions="1.0"?>
<jdd:LogData xmlns:jdd=http://xxx/xxx/xx>
  <jdd:parameter>
    <jdd:JobData JobType="Copy"
      LogID="0001"
      UserID="1111"
      HostID="0011"
      SectionID="2365"
      JobStartTime="2007/08/01 15:00"
      JobEndTime="2007/08/01 15:05"
      DeviceID="000888111"
      PageCount="5"
    </jdd:JobData>
  </jdd:parameter>
</jdd:LogData>

```

フロントページの続き

(58)調査した分野(Int.Cl., DB名)

H04N 1/00

B41J 29/38

G03G 21/00

G06F 3/12