

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4944140号
(P4944140)

(45) 発行日 平成24年5月30日(2012.5.30)

(24) 登録日 平成24年3月9日(2012.3.9)

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

請求項の数 17 (全 42 頁)

(21) 出願番号	特願2009-11722 (P2009-11722)	(73) 特許権者	390002761 キヤノンマーケティングジャパン株式会社 東京都港区港南2丁目16番6号
(22) 出願日	平成21年1月22日(2009.1.22)	(73) 特許権者	301015956 キヤノンソフトウェア株式会社 東京都品川区東品川二丁目4番11号
(65) 公開番号	特開2010-15537 (P2010-15537A)	(74) 代理人	100096091 弁理士 井上 誠一
(43) 公開日	平成22年1月21日(2010.1.21)	(72) 発明者	橋本 紘 東京都港区三田3丁目11番28号 キヤノンITソリューションズ株式会社内
審査請求日	平成22年11月22日(2010.11.22)	審査官	衣川 裕史
(31) 優先権主張番号	特願2008-148848 (P2008-148848)		
(32) 優先日	平成20年6月6日(2008.6.6)		
(33) 優先権主張国	日本国(JP)		

最終頁に続く

(54) 【発明の名称】 ネットワークインタフェース装置、制御方法、プログラム、および画像形成装置

(57) 【特許請求の範囲】

【請求項1】

画像形成装置に接続され、ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続されるネットワークインタフェース装置であって、

前記画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付手段と

、前記印刷データ記憶手段で記憶されている印刷データを識別する印刷データ識別情報を記憶する印刷データ識別情報記憶手段と、

前記ユーザ識別情報受付手段で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定手段と、

前記受付判定手段で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶手段で記憶されている前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除手段と、

を備えることを特徴とするネットワークインタフェース装置。

【請求項2】

前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段に記憶されている印刷データを前記画像形成装置に送信する第1の印刷データ送信手段を更に備え、

10

20

前第1の記印刷手段は、同一ユーザの読取対象物を再度受け付けない場合に、前記印刷データ識別情報記憶手段で記憶されている前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを取得して送信することを特徴とする請求項1に記載のネットワークインタフェース装置。

【請求項3】

前記ユーザ識別情報の受け付けに応じて、前記印刷データ識別情報記憶手段で記憶されている当該ユーザ識別情報に対応する印刷データを所定時間ユーザに通知するように、前記画像形成装置に前記印刷データ識別情報を送信する印刷データ識別情報送信手段を更に備え、

前記印刷データ削除は、前記受付判定手段で、前記印刷データ識別情報送信手段によって送信した前記印刷データ識別情報を前記画像形成装置で所定時間通知する間に、同一ユーザの読取対象物を再度受け付けたと判定される場合に、通知されている前記印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除することを特徴とする請求項1又は2に記載のネットワークインタフェース装置。

10

【請求項4】

前記受付判定手段で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記読取手段に読取対象物がかざされている間隔の値を取得する値取得手段と、

前記値取得手段で取得された値が所定の値となるか否かを判定する値判定手段とを更に備え、

前記印刷データ削除手段は、前記値判定手段で所定の値となると判定された場合に、前記ユーザ識別情報に対応する印刷データを前記印刷データ記憶手段から全て削除することを特徴とする請求項2又は3に記載のネットワークインタフェース装置。

20

【請求項5】

前記印刷データ識別情報送信手段は、前記値判定手段で所定の値とならないと判定された場合に、前記印刷データ記憶手段で記憶されている次の印刷データを識別する印刷データ識別情報を所定時間ユーザに通知すべく前記画像形成装置に印刷データ識別情報を送信することを特徴とする請求項4に記載のネットワークインタフェース装置。

【請求項6】

前記ネットワークインタフェース装置は、ユーザの認証を行う認証サーバと通信し、

前記ユーザ識別情報受付手段によって前記ユーザ識別情報を受け付けた場合、前記ユーザ識別情報を含む認証要求を前記認証サーバに送信する認証要求送信手段と、

前記認証要求送信手段で認証要求を前記認証サーバに送信することで、前記ユーザ識別情報が認証された場合、前記ユーザ識別情報に対応する印刷データの印刷データ識別情報を取得する印刷データ識別情報取得手段とを更に備え、

前記印刷データ識別情報送信手段は、前記印刷データ識別情報取得手段で取得した印刷データ識別情報を送信することを特徴とする請求項1乃至5のいずれか1項に記載のネットワークインタフェース装置。

30

【請求項7】

前記ネットワークインタフェース装置は、印刷データを送信する情報処理装置と通信し、

前記情報処理装置から送信された印刷データを受け付ける印刷データ受付手段と、

前記印刷データ受付手段によって受け付けた印刷データを前記印刷データ記憶に保存する保存手段と

を更に備えることを特徴とする請求項1乃至6のいずれか1項に記載のネットワークインタフェース装置。

40

【請求項8】

前記認証サーバと通信可能か否かを判断する通信可否判断手段と、

前記通信可否判断手段で、前記認証サーバと通信可能でないと判断した場合、前記印刷データ受付手段によって受け付けた印刷データを、前記印刷データ記憶手段に保存するための設定を解除する解除手段と、

50

前記解除手段によって設定が解除されている場合、前記印刷データ受付手段によって受け付けた印刷データを、前記印刷データ記憶手段に保存することなく、前記画像形成装置に送信する第2の印刷データ送信手段と
を更に備えることを特徴とする請求項1乃至7のいずれか1項に記載のネットワークインタフェース装置。

【請求項9】

前記通信可否判断手段は、前記解除手段で印刷データ記憶手段に保存するための設定が解除されている場合、一定間隔で前記認証サーバと通信可能かどうかを判断することを特徴とする請求項8に記載のネットワークインタフェース装置。

【請求項10】

前記通信可否判断手段で前記認証サーバと通信可能であると判断した場合、かつ前記印刷データ記憶手段に保存するための設定が解除されている場合、前記印刷データ記憶手段に保存するための設定を設定する設定手段
を更に備えることを特徴とする請求項8又は9に記載のネットワークインタフェース装置。

【請求項11】

前記通信可否判断で前記認証サーバとの通信ができた際の時間情報を記憶する時間情報記憶手段を更に備え、

前記印刷データ識別情報送信手段は、前記時間情報と前記印刷データ記憶手段に印刷データを保存した保存時間情報に従って、前記印刷データ識別情報を送信することを特徴とする請求項8乃至10のいずれか1項に記載のネットワークインタフェース装置。

【請求項12】

前記ユーザ識別情報受付手段で受け付けたユーザ識別情報は、前記読取手段に読取対象物がかざされた場合に、当該読取対象物の所定の領域を読み取ることによって得られる情報であることを特徴とする請求項1乃至11のいずれか1項に記載のネットワークインタフェース装置。

【請求項13】

画像形成装置に接続され、ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続されるネットワークインタフェース装置の制御方法であって、

前記ネットワークインタフェース装置が、

前記画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付工程と

前記印刷データ記憶手段で記憶されている印刷データを識別する印刷データ識別情報を記憶する印刷データ識別情報記憶工程と、

前記ユーザ識別情報受付工程で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定工程と、

前記受付判定工程で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶工程で記憶した前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除工程と

を実行することを特徴とするネットワークインタフェース装置の制御方法。

【請求項14】

画像形成装置に接続され、ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続されるネットワークインタフェース装置で実行可能なプログラムであって、

前記ネットワークインタフェースを、

前記画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付手段と

10

20

30

40

50

前記印刷データ記憶手段で記憶されている印刷データを識別する印刷データ識別情報を記憶する印刷データ識別情報記憶手段と、

前記ユーザ識別情報受付手段で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定手段と、

前記受付判定手段で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶手段で記憶されている前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除手段として機能させることを特徴とするプログラム。

【請求項 15】

ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続される画像形成装置であって、

当該画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付手段と、

前記印刷データ記憶手段で記憶されている印刷データを識別する印刷データ識別情報を記憶する印刷データ識別情報記憶手段と、

前記ユーザ識別情報受付手段で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定手段と、

前記受付判定手段で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶手段で記憶されている前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除手段と

を備えることを特徴とする画像形成装置。

【請求項 16】

ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続される画像形成装置の制御方法であって、

前記画像形成装置が、

当該画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付工程と

前記印刷データ記憶手段で記憶されている印刷データを識別する印刷データ識別情報を記憶する印刷データ識別情報記憶工程と、

前記ユーザ識別情報受付工程で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定工程と、

前記受付判定工程で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶工程で記憶した前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除工程と

を備えることを特徴とする画像形成装置の制御方法。

【請求項 17】

ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続される画像形成装置で実行可能なプログラムであって、

前記画像形成装置を、

当該画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付手段と

前記印刷データ記憶手段で記憶されている印刷データを識別する印刷データ識別情報を記憶する印刷データ識別情報記憶手段と、

前記ユーザ識別情報受付手段で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定手段と、

10

20

30

40

50

前記受付判定手段で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶手段で記憶されている前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除手段

として機能させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、印刷データを生成する情報処理装置と通信可能に接続される印刷装置に設けられるネットワークインタフェース装置、制御方法、プログラム、および画像形成装置に関する。

10

【背景技術】

【0002】

従来から、ユーザが印刷装置からサーバ上に一時蓄積された印刷データに対して印刷要求を行うことで、印刷装置から印刷データの出力を可能にする所謂「プルプリント（蓄積印刷）」のプリントシステムが提案されている。

「プルプリント（蓄積印刷）」のプリントシステムの例として、特許文献1が挙げられる。特許文献1には、複合機に認証機能を備え、セキュリティを考慮した印刷制御システムが開示されている。

【0003】

20

特許文献1は以下の通りである。

特許文献1の図4に示されるように、まず、ユーザは、クライアントPC(Personal Computer)100にログインする((1)-1)。そしてクライアントPC100からプリンタへの印刷指示を行う((1)-2)。そして、クライアントPC100は、生成した印刷データをプリントサーバ200に送信して((2)-1)、プリントサーバ200の所定の格納場所に格納させる((2)-2)。この時点で印刷装置へは印刷データを送信しない。

次に、クライアントPC100は、プリントサーバ200に送信した印刷データの書誌情報データを生成し、該生成した書誌情報データを印刷管理サーバ400に送信して、印刷管理サーバ400の所定の格納場所に格納させる((3)-1)。印刷管理サーバ400は、クライアントPC100から書誌情報データファイルが格納されると、該書誌情報データファイルを解析し書誌情報を書誌情報DBに登録する((3)-2)。次に、複合機300は、カードリーダーによりICカード410を検知すると、該ICカード410内の個人認証情報を読み取り、該読み取った個人認証情報を認証要求として印刷管理サーバ400に送信する((4)-1)。印刷管理サーバ400は、複合機300より個人認証情報を受信すると、該個人認証情報の認証処理を印刷管理サーバ400の外部記憶装置上に記憶されるICカード認証用テーブルに基づいて行い、認証結果を複合機300に返信する((4)-2)。

30

【0004】

次に、複合機300は、印刷管理サーバ400から、認証に成功した旨の認証結果(クライアントPC100のログインユーザID)を受信すると、印刷管理サーバ400に印刷データ一覧要求を送信する((5)-1)。

40

なお、印刷データ一覧要求には、クライアントPC100のログインユーザIDが含まれているものとする。印刷管理サーバ400は、複合機300から印刷データ一覧要求を受信すると、該印刷データ一覧要求に含まれるログインユーザIDで書誌情報DBを検索して、該ログインユーザIDに対応する印刷データ一覧を生成し、複合機300に返信する((5)-2)。複合機300は、印刷管理サーバ400から印刷データ一覧を受信すると、該印刷データ一覧を操作部308のUI上に表示する。そして、ユーザにより、印刷データが選択され、印刷指示がなされると、複合機300は、該選択された印刷データの印刷要求(出力指示)を印刷管理サーバ400に送信する(6)。

50

【 0 0 0 5 】

印刷管理サーバ400は、複合機300から印刷データの印刷要求（出力指示）を受信すると、該出力指示がなされた印刷データの書誌情報を、クライアントPC100のログインユーザ名、印刷データのタイムスタンプをキーにして書誌情報DBから検索する。該検索した書誌情報から該当する印刷データを格納しているプリントサーバ200を特定し、該プリントサーバ200に該当する印刷データの印刷指示を送信する（7）。プリントサーバ200は、印刷管理サーバ400から印刷指示を受信すると、該印刷指示に基づいて印刷データを複合機300に送信して複合機300で印刷させる（8）。

【 0 0 0 6 】

上記の方法によれば、印刷物が出力されるのは、ユーザが印刷装置からサーバ上に印刷要求を行ったときとなるので、印刷物が長時間放置されることを防ぐことができ、セキュアなプリントシステムを実現できる。

【 先行技術文献 】

【 特許文献 】

【 0 0 0 7 】

【 特許文献 1 】 特開 2 0 0 6 - 9 9 7 1 4 号 公 報

【 発明の概要 】

【 発明が解決しようとする課題 】

【 0 0 0 8 】

しかしながら、上記の方法では、認証用サーバでユーザ情報を一元管理するため、認証サーバがダウンしたときには業務が停滞してしまうという問題がある。

【 0 0 0 9 】

また、特許文献1では、印刷データ一覧を操作部に表示することができるためユーザは削除したい印刷データを指定することができる。このプリンタは所謂マルチファンクションプリンタ（MFP：複合機）で、複数の機能进行操作したりするための操作部（表示可能な操作部）が備えられており、その操作部に印刷データの一覧を表示できるからこそ、ユーザは不要な印刷データを指定して削除させることが可能である。一方、シングルファンクションプリンタ（SFP）では、マルチファンクションプリンタのような操作部が備えられていないため、特許文献1のような蓄積印刷を実現させようとする場合、印刷データを指定することができないので、ICカードをかざしたユーザの蓄積されている印刷データを全て印刷させてしまう。つまり、印刷設定などを間違えて印刷実行してしまった不要な印刷データも印刷されてしまうといった問題がある。尚、一覧を表示できないマルチファンクションプリンタも存在する。

【 0 0 1 0 】

更に、操作部に印刷データの一覧を表示できないようなプリンタの場合、一度ジョブを投入すると、印刷データをユーザに選択させることができないため、削除することができないという問題があった。特に、誤って投入したジョブは、本来削除したいにも関わらず印刷するしかないという問題があった。

【 0 0 1 1 】

本発明の目的は、操作部で印刷データを削除できないようなプリンタからでも、印刷データを削除することができる仕組みを提供することである。また、認証サーバがダウンするなどの理由により認証できない場合にも、印刷業務を滞らせないようにすることができる仕組みを提供することである。

【 課題を解決するための手段 】

【 0 0 1 2 】

前述した目的を達成するために第1の発明は、画像形成装置に接続され、ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続されるネットワークインタフェース装置であって、前記画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付手段と、前記印刷データ記憶手段で記憶されている印刷データを識

10

20

30

40

50

別する印刷データ識別情報を記憶する印刷データ識別情報記憶手段と、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定手段と、前記受付判定手段で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶手段で記憶されている前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除手段と、を備えることを特徴とする。

【0013】

また、前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段に記憶されている印刷データを前記画像形成装置に送信する第1の印刷データ送信手段を更に備え、前第1の記印刷手段は、同一ユーザの読取対象物を再度受け付けない場合に、前記印刷データ識別情報記憶手段で記憶されている前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを取得して送信する。

10

【0014】

また、前記ユーザ識別情報の受け付けに応じて、前記印刷データ識別情報記憶手段で記憶されている当該ユーザ識別情報に対応する印刷データ識別情報を所定時間ユーザに通知するように、前記画像形成装置に前記印刷データ識別情報を送信する印刷データ識別情報送信手段を更に備え、前記印刷データ削除は、前記受付判定手段で、前記印刷データ識別情報送信手段によって送信した前記印刷データ識別情報を前記画像形成装置で所定時間通知する間に、同一ユーザの読取対象物を再度受け付けたと判定される場合に、通知されている前記印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する。

20

【0015】

また、前記受付判定手段で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記読取手段に読取対象物がかざされている間隔の値を取得する値取得手段と、前記値取得手段で取得された値が所定の値となるか否かを判定する値判定手段とを更に備え、前記印刷データ削除手段は、前記値判定手段で所定の値となると判定された場合に、前記ユーザ識別情報に対応する印刷データを前記印刷データ記憶手段から全て削除する。

【0016】

また、前記印刷データ識別情報送信手段は、前記値判定手段で所定の値とならないと判定された場合に、前記印刷データ記憶手段で記憶されている次の印刷データを識別する印刷データ識別情報を所定時間ユーザに通知すべく前記画像形成装置に印刷データ識別情報を送信する。

30

【0017】

また、前記ネットワークインタフェース装置は、ユーザの認証を行う認証サーバと通信し、前記ユーザ識別情報受付手段によって前記ユーザ識別情報を受け付けた場合、前記ユーザ識別情報を含む認証要求を前記認証サーバに送信する認証要求送信手段と、前記認証要求送信手段で認証要求を前記認証サーバに送信することで、前記ユーザ識別情報が認証された場合、前記ユーザ識別情報に対応する印刷データの印刷データ識別情報を取得する印刷データ識別情報取得手段とを更に備え、前記印刷データ識別情報送信手段は、前記印刷データ識別情報取得手段で取得した印刷データ識別情報を送信することを特徴とする。

40

【0018】

また、前記ネットワークインタフェース装置は、印刷データを送信する情報処理装置と通信し、前記情報処理装置から送信された印刷データを受け付ける印刷データ受付手段と、前記印刷データ受付手段によって受け付けた印刷データを前記印刷データ記憶に保存する保存手段とを更に備えることを特徴とする。

【0019】

また、前記認証サーバと通信可能か否かを判断する通信可否判断手段と、前記通信可否判断手段で、前記認証サーバと通信可能でないと判断した場合、前記印刷データ受付手段によって受け付けた印刷データを、前記印刷データ記憶手段に保存するための設定を解除

50

する解除手段と、前記解除手段によって設定が解除されている場合、前記印刷データ受付手段によって受け付けた印刷データを、前記印刷データ記憶手段に保存することなく、前記画像形成装置に送信する第2の印刷データ送信手段とを更に備えることを特徴とする。

【0020】

また、前記通信可否判断手段は、前記解除手段で印刷データ記憶手段に保存するための設定が解除されている場合、一定間隔で前記認証サーバと通信可能かどうかを判断することを特徴とする。

【0021】

また、前記通信可否判断手段で前記認証サーバと通信可能であると判断した場合、かつ前記印刷データ記憶手段に保存するための設定が解除されている場合、前記印刷データ記憶手段に保存するための設定を設定する設定手段を更に備えることを特徴とする。

【0022】

また、前記通信可否判断で前記認証サーバとの通信ができた際の時間情報を記憶する時間情報記憶手段を更に備え、前記印刷データ識別情報送信手段は、前記時間情報と前記印刷データ記憶手段に印刷データを保存した保存時間情報に従って、前記印刷データ識別情報を送信することを特徴とする。

また、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報は、前記読取手段に読取対象物がかざされた場合に、当該読取対象物の所定の領域を読み取ることによって得られる情報であることを特徴とする。

【0023】

第2の発明は、画像形成装置に接続され、ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続されるネットワークインタフェース装置の制御方法であって、前記ネットワークインタフェース装置が、前記画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付工程と、前記印刷データ記憶手段で記憶されている印刷データを識別する印刷データ識別情報を記憶する印刷データ識別情報記憶工程と、前記ユーザ識別情報受付工程で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定工程と、前記受付判定工程で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶工程で記憶した前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除工程とを実行することを特徴とする。

【0024】

第3の発明は、画像形成装置に接続され、ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続されるネットワークインタフェース装置で実行可能なプログラムであって、前記ネットワークインタフェースを、前記画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付手段と、前記印刷データ記憶手段で記憶されている印刷データを識別する印刷データ識別情報を記憶する印刷データ識別情報記憶手段と、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定手段と、前記受付判定手段で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶手段で記憶されている前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除手段として機能させることを特徴とする。

【0025】

第4の発明は、ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続される画像形成装置であって、当該画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付手段と、前記印刷データ記憶手段で記憶されている印刷

10

20

30

40

50

データを識別する印刷データ識別情報を記憶する印刷データ識別情報記憶手段と、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定手段と、前記受付判定手段で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶手段で記憶されている前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除手段とを備えることを特徴とする。

第5の発明は、ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続される画像形成装置の制御方法であって、前記画像形成装置が、当該画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付工程と、前記印刷データ記憶手段で記憶されている印刷データを識別する印刷データ識別情報を記憶する印刷データ識別情報記憶工程と、前記ユーザ識別情報受付工程で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定工程と、前記受付判定工程で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶工程で記憶した前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除工程とを備えることを特徴とする画像形成装置の制御方法。

第6の発明は、ユーザ識別情報と対応付けられた印刷データを記憶する印刷データ記憶手段と接続される画像形成装置で実行可能なプログラムであって、前記画像形成装置を、当該画像形成装置を利用するために用いられる読取手段で読取対象物を読み取ることによって得られるユーザを識別するユーザ識別情報を受け付けるユーザ識別情報受付手段と、前記印刷データ記憶手段で記憶されている印刷データを識別する印刷データ識別情報を記憶する印刷データ識別情報記憶手段と、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報と同一ユーザの読取対象物を前記読取手段で再度受け付けたか否かを判定する受付判定手段と、前記受付判定手段で、同一ユーザの読取対象物を再度受け付けたと判定される場合に、前記印刷データ識別情報記憶手段で記憶されている前記ユーザ識別情報に対応する印刷データ識別情報に従って、前記印刷データ記憶手段から印刷データを削除する印刷データ削除手段として機能させることを特徴とする。

【発明の効果】

【0026】

本発明によれば、操作部で印刷データを削除できないようなプリンタからでも、印刷データを削除することができる。また、認証サーバがダウンするなどの理由により認証できない場合にも、印刷業務を滞らせないようにすることができる。

【図面の簡単な説明】

【0027】

【図1】従来のセキュアプリントシステムの構成の一例を示す図

【図2】本発明に係るセキュアプリントシステム1の構成の一例を示す図

【図3】LDAPサーバ200、クライアントPC300のハードウェア構成を示す図

【図4】印刷装置1000のハードウェア構成を示す図

【図5】NIC700のハードウェア構成を示す図

【図6】本発明に係るセキュアプリントシステム1の構成を示すブロック図

【図7】セキュアプリントシステム1の印刷ジョブ投入処理手順の一例を示すフローチャート

【図8】セキュアプリントシステム1の印刷ジョブ出力処理手順の一例を示すフローチャート

【図9】セキュアプリントシステム1の印刷ジョブ出力処理手順の一例を示すフローチャート

【図10】セキュアプリントシステム1の印刷ジョブ出力処理手順の一例を示すフローチャート

10

20

30

40

50

- 【図 1 1】セキュアプリントシステム 1 の印刷ジョブ出力処理手順の一例を示すフローチャート
- 【図 1 2】セキュアプリントシステム 1 の印刷ジョブ出力処理手順の一例を示すフローチャート
- 【図 1 3】セキュアプリントシステム 1 の削除確認処理手順の一例を示すフローチャート
- 【図 1 4】セキュアプリントシステム 1 の削除処理手順の一例を示すフローチャート
- 【図 1 5】セキュアプリントシステム 1 の出力処理の詳細手順の一例を示すフローチャート
- 【図 1 6】セキュアプリントシステム 1 の L D A P サーバ監視処理手順の一例を示すフローチャート 10
- 【図 1 7】セキュアプリントシステム 1 のユーザ通知処理手順の一例を示すフローチャート
- 【図 1 8】設定情報 8 0 2 の一例を示す図
- 【図 1 9】監視ポート 9 0 7 の詳細を示す図
- 【図 2 0】印刷装置 1 0 0 0 に表示するメッセージの一例を示す図
- 【図 2 1】ジョブ 3 1 0 の詳細を示す図
- 【図 2 2】印刷情報管理ヘッダ 3 1 1 の詳細を示す図
- 【図 2 3】ジョブ情報 8 2 0 の詳細を示す図
- 【図 2 4】ジョブリスト 8 0 5 の詳細を示す図
- 【図 2 5】実行リスト 8 0 4 の詳細を示す図 20
- 【図 2 6】ファイルシステム 5 0 1 の詳細を示す図
- 【図 2 7】I C カード 4 1 0 の詳細を示す図
- 【図 2 8】ユーザ情報 2 1 0 の一例を示す図
- 【図 2 9】L D A P ディレクトリ 2 0 1 の詳細を示す図
- 【図 3 0】削除設定 8 4 0 の一例を示す図
- 【図 3 1】実行カード情報 8 5 0 の一例を示す図
- 【図 3 2】復帰時間情報 8 6 0 の一例を示す図
- 【図 3 3】セキュアプリントシステム 1 a の実施例を示す図
- 【図 3 4】セキュアプリントシステム 1 b の実施例を示す図
- 【図 3 5】セキュアプリントシステム 1 の実施形態 2 における、印刷ジョブ出力処理手順の一例を示すフローチャート 30
- 【図 3 6】セキュアプリントシステム 1 の実施形態 2 における、印刷ジョブ出力処理手順の一例を示すフローチャート
- 【図 3 7】セキュアプリントシステム 1 の実施形態 2 における、設定情報 8 0 2 の一例を示す図
- 【発明を実施するための形態】
- 【 0 0 2 8 】
- 〔実施形態 1 〕
- 本発明の目的を達成するための構成として、例えば、プリントサーバを使わない構成がある。このプリントサーバを使わない構成での印刷方法には通常印刷モードとジョブ蓄積モードを用いた方法を用いる。 40
- 通常印刷モードとは、ジョブをストレージに蓄積せずに印刷を行うモードである。また、ジョブ蓄積モードとは、ジョブをストレージに蓄積し、ユーザが I C カードをかざすことによって印刷を行うモードである。そして、認証サーバが正常なときはジョブ蓄積モードで運用し、認証サーバがダウンしたときは、ジョブ蓄積モードから通常印刷モードに切り替えるという運用が行われる。
- より具体的には、例えば、あるユーザがジョブ蓄積モードのときにジョブを投入すると、ジョブがストレージに蓄積される。続いて、ジョブを印刷しようと I C カードをかざしたときに、認証サーバがダウンしていたとする。認証サーバがダウンしている場合、I C カードに紐づくユーザ名が取得できない。よって、蓄積ジョブの中からユーザのジョブを 50

特定することができない。従って、通常印刷モードに切り替えて運用する必要がある。そして、ユーザが同じジョブをもう一度投入すると、ジョブが蓄積されずにそのまま出力される。これにより、ユーザは認証サーバがダウンしていても業務に支障をきたさず印刷をおこなうことができる。更に、認証サーバが復帰した場合、通常印刷モードからジョブ蓄積モードに切り替える。これにより、通常通りジョブを蓄積させられるのでセキュリティの高い印刷が行うことが可能となる。つまり、認証サーバが復帰すると、ユーザがICカードをかざしたときに、ストレージに蓄積されているジョブが再び印刷されることになる。

しかし、このような運用では、ユーザはすでに同じ内容のジョブを出力しているので、ストレージに蓄積されているジョブを印刷する必要がないにも関わらず、ICカードをかざしたときに無駄なジョブ（重複したジョブ）が印刷されてしまう。このような運用では、切り替え時に発生する重複したジョブを削除することができず、無駄とわかりつつ印刷しなくてはならないという課題が存在する。

本発明によれば、上記のような課題を解決することができる。

以下、添付図面を参照しながら、本発明に係るセキュアプリントシステムの好適な実施形態について詳細に説明する。

図1は、従来 of セキュアプリントシステムの構成の一例を示す図である。

【0029】

図1に示すように、例えば、階毎に設置する1又は複数の印刷装置（画像形成装置）1000、管理者に1台、ユーザ毎に1台ずつというように設置する1又は複数のクライアントPC300、拠点毎に設置する1又は複数のプリンタサーバ101、拠点毎に設置する1又は複数の認証サーバ102がLAN（Local Area Network）150を介して接続される。また、印刷装置（画像形成装置）1000には、USBケーブル160を介してカードリーダー400が接続される。

【0030】

クライアントPC300は、印刷装置（画像形成装置）1000の設定を行うPCである。クライアントPC300は、LAN150を介して、例えば、HTTP（Hyper Text Transfer Protocol）、TCP/IP（Transmission Control Protocol/Internet Protocol）などによって、印刷装置（画像形成装置）1000と通信することができる機能を搭載したPCである。

また、クライアントPC300は、ユーザから印刷ジョブを投入するためのPCである。ユーザがクライアントPC300上で動くアプリケーションからプリンタドライバを介して印刷ジョブを生成すると、プリンタドライバがLPR（Line Printer daemon protocol）等の印刷プロトコルを用いて、印刷ジョブを印刷装置（画像形成装置）1000やプリンタサーバ101に送信することができる。

【0031】

プリンタサーバ101は、クライアントPC300から印刷ジョブを受け取り、印刷ジョブを解析してジョブ情報を取得し、印刷ジョブを蓄積する。また、印刷装置（画像形成装置）1000から印刷要求を受け取り、印刷要求に含まれるユーザ名をもとにして、蓄積ジョブからユーザのジョブを検索し、見つかったユーザのジョブを印刷装置（画像形成装置）1000に対して印刷指示を行う。

【0032】

認証サーバ102は、印刷装置（画像形成装置）1000がユーザ認証を行うためのサーバである。カードID211に紐づくユーザ名、メールアドレス、利用権限等のデータを持っている。認証サーバ102は、印刷装置（画像形成装置）1000からの問い合わせに対して、ユーザの有無と、ユーザが存在する場合はそのユーザ情報を返答する機能を有する。

【0033】

カードリーダー400は、USBケーブル160を介して印刷装置（画像形成装置）10

10

20

30

40

50

00に接続される。

カードリーダー400は、ICカード410（例えば、ソニー（登録商標）社のフェリカ（Felica）（登録商標））がかざされるとカード内部の情報を読み取り、USBケーブル160を介して印刷装置（画像形成装置）1000に通知する。

【0034】

次に、図2を参照しながら、本発明に係るセキュアプリントシステム1について説明する。

図2は、本発明に係るセキュアプリントシステム1の構成の一例を示す図である。

【0035】

図2に示すセキュアプリントシステム1は、LAN150を介してクライアントPC（情報処理装置）300、LDAP（Lightweight Directory Access Protocol）サーバ（認証サーバ）200、NIC（ネットワークインタフェース装置）700が接続される。印刷装置1000には、NIC（ネットワークインタフェース装置）700が挿入される。

NIC700は、USBケーブル160、USBハブ600を介してマストレージ（記憶部）500、カードリーダー400を接続している。

マストレージ500及びUSBハブ600がNIC700を介して印刷装置1000に外付けされているが、印刷装置1000に内蔵するにしてもよい。また、NIC700が複数のUSBポート160を有する場合はUSBハブ600を介する必要はなく、NIC700にカードリーダー400及びマストレージ500が直接接続される。

【0036】

LDAPサーバ200は、図1の認証サーバ102の役割を行うもので、LDAPプロトコルにて通信を行う機能を有する。LDAPサーバ200は、内部のディレクトリにユーザ情報を一元管理することができる。LDAPサーバ200は、1つのサーバで構成しても良い。また、LDAPサーバ200は、後述するように、プライマリおよびセカンダリの2つのサーバによって構成しても良い。また、LDAPサーバ200は、3つ以上のサーバによって構成しても良い。いずれの場合であっても、LDAPサーバ200がダウンするとは、LDAPサーバ200を構成する全てのサーバがダウンしたことを意味するものとする。

図2では、LDAPサーバ200を使用しているが、認証を行うことができるサーバであればLDAPサーバに限らない。

クライアントPC300は、印刷データを生成する情報処理装置である。

【0037】

マストレージ500は、HDD（Hard Disk Drive）やフラッシュメモリのような大容量のファイルシステムを持つハードウェアで、USBケーブル160を介してUSBハブ600に接続している。

マストレージ500は、印刷装置1000からファイル書き込み、読み込み、削除等のファイルシステムの制御を行うことが可能である。

【0038】

次に、図3、4、5を参照しながら、クライアントPC300、LDAPサーバ200、印刷装置1000、NIC700について説明する。

図3は、LDAPサーバ200、クライアントPC300のハードウェア構成を示す図、図4は、印刷装置1000のハードウェア構成を示す図、図5は、NIC700のハードウェア構成を示す図である。

【0039】

図3に示すように、LDAPサーバ200、クライアントPC300は、システムバス2004を介してCPU（Central Processing Unit）2001、RAM（Random Access Memory）2002、ROM（Read Only Memory）2003、入力コントローラ2005、ビデオコントローラ2006、メモリコントローラ2007、通信I/Fコントローラ2008が接続される。

【 0 0 4 0 】

C P U 2 0 0 1 は、システムバス 2 0 0 4 に接続される各デバイスやコントローラを統括的に制御する。

R O M 2 0 0 3 あるいは外部メモリ 2 0 1 1 は、C P U 2 0 0 1 の制御プログラムである B I O S (B a s i c I n p u t / O u t p u t S y s t e m) や O S (O p e r a t i n g S y s t e m s) や、各サーバあるいは各 P C が実行する各種プログラム等を保持している。

R A M 2 0 0 2 は、C P U 2 0 0 1 の主メモリ、ワークエリア等として機能する。C P U 2 0 0 1 は、処理の実行に際して必要なプログラム等を R O M 2 0 0 3 あるいは外部メモリ 2 0 1 1 から R A M 2 0 0 2 にロードし、ロードしたプログラムを実行することで各種動作を実現する。

10

【 0 0 4 1 】

入力コントローラ 2 0 0 5 は、キーボード (K B) 2 0 0 9 やマウス (図示しない) 等のポインティングデバイス等からの入力を制御する。

ビデオコントローラ 2 0 0 6 は、C R T (C a t h o d e R a y T u b e) 2 0 1 0 等の表示器への表示を制御する。表示器は C R T に限らず、液晶ディスプレイ等の他の表示器でもよい。これらは、必要に応じて管理者が使用する。

【 0 0 4 2 】

メモリコントローラ 2 0 0 7 は、ブートプログラム、各種のアプリケーション、フォントデータ、ユーザファイル、編集ファイル、各種データ等を記憶するハードディスク (H D) や、フレキシブルディスク (F D)、あるいは、P C M C I A (P e r s o n a l C o m p u t e r M e m o r y C a r d I n t e r n a t i o n a l A s s o c i a t i o n) カードスロットにアダプタを介して接続されるコンパクトフラッシュ (登録商標) メモリ等の外部メモリ 2 0 1 1 へのアクセスを制御する。

20

通信 I / F コントローラ 2 0 0 8 は、L A N 1 5 0 のようなネットワークを介して外部機器と接続・通信し、ネットワーク上での通信制御処理を実行する。通信 I / F コントローラ 2 0 0 8 は、例えば、T C P / I P (T r a n s m i s s i o n C o n t r o l P r o t o c o l / I n t e r n e t P r o t o c o l) を用いた通信等が可能である。

【 0 0 4 3 】

C P U 2 0 0 1 は、例えば R A M 2 0 0 2 内の表示情報用領域へアウトラインフォントの展開 (ラスタライズ) 処理を実行することにより、C R T 2 0 1 0 上に表示することが可能である。また、C P U 2 0 0 1 は、C R T 2 0 1 0 上のマウスカーソル (図示しない) 等によるユーザ指示を可能とする。

30

L D A P サーバ 2 0 0、クライアント P C 3 0 0 のハードウェア上で動作する各種プログラムは、外部メモリ 2 0 1 1 に記録されており、必要に応じて R A M 2 0 0 2 にロードされ、C P U 2 0 0 1 により実行される。プログラムの実行時に用いられる定義ファイル及び各種情報テーブル等は、外部メモリ 2 0 1 1 に格納されている。

【 0 0 4 4 】

次に、印刷装置 1 0 0 0 のハードウェア構成について説明する。

40

図 4 に示すように、印刷装置 1 0 0 0 は、入力部 3 0 0 0、C P U 3 0 0 1、操作部 3 0 0 2、印刷処理部 3 0 0 3、記憶部 3 0 0 4、出力カセット 3 0 0 5、用紙カセット 3 0 0 6 等を有する。

【 0 0 4 5 】

入力部 3 0 0 0 は、本印刷装置と N I C 7 0 0 を接続するものであり、N I C 7 0 0 とのデータ通信を制御する。

C P U 3 0 0 1 は、印刷装置 1 0 0 0 全体の動作を制御する。

操作部 3 0 0 2 は、印刷装置 1 0 0 0 に直接ユーザによる操作のインタフェースを提供する。

印刷処理部 3 0 0 3 は、入力部 3 0 0 0 で受信したコマンドの解析、印刷データ (P D

50

L)の解析等を行う。

記憶部3004は、印刷装置1000を動作させるためのROM(図示しない)、RAM(図示しない)、二次記憶装置(図示しない)等からなる。RAMは使用制限のないデータ記憶領域で、入力部3000の受信バッファ、あるいは、印刷処理部3003でのデータ展開等に使用する。

出力部3005は、入力部3000で受信した印刷データを、印刷処理部3003で印刷可能なイメージ情報に展開したものを紙に転写する。

用紙カセット3006は、出力部3005の処理に合わせて適切な用紙を供給する。

【0046】

NIC700は、ネットワークインタフェースカードであり、LAN150を介して他の機器から受信したデータをNIC700が窓口となって受け取り、NIC内部のプログラム(図示しない)や、印刷装置1000の入力部3000に渡す。

【0047】

次に、NIC700のハードウェア構成について説明する。

図5に示すように、NIC700は、CPU4001、RAM4002、通信I/Fコントローラ4003、USB I/Fコントローラ4004、内部メモリ4005、メモリコントローラ4006、ROM4007、機器I/Fコントローラ4008等を有する。

【0048】

CPU4001はNIC700の制御を行うもので、内部で接続されている装置を制御する。

RAM4002は、CPU4001の主メモリ、ワークエリア等として機能する。CPU4001は、処理の実行に際して必要なプログラム等をROM4007あるいは内部メモリ4005からRAM4002にロードして、ロードしたプログラムを実行する。

通信I/Fコントローラ4003は、LAN150のようなネットワークを介して外部機器と接続・通信するものであり、ネットワークでの通信制御処理を実行する。例えば、TCP/IPやUDP(User Datagram Protocol)などの通信プロトコルを用いた通信が可能である。

【0049】

USB I/Fコントローラ4004は、カードリーダー400、マスタストレージ500及びUSBハブ600などのUSB機器とNIC700を接続、通信するもので、USBの通信制御処理を実行する。

内部メモリ4005は、NIC700を制御するOSが搭載されており、またOS上で動作するアプリケーションプログラム、その設定情報を記憶する。

メモリコントローラ4006は、各種のアプリケーション、各種データ等を記憶する内部メモリ4005へのアクセスを制御する。

ROM4007は、読み出し専用の半導体メモリであり、電源を切っても内容が消えないことからブートプログラムが格納される。

機器I/Fコントローラ4008は、NIC700と印刷装置1000を接続、通信する。

【0050】

次に、図6、図18、図19、図21、図22、図23、図24、図25、図26、図27、図28、図29、図30、図31、図32を参照しながら、セキュアプリントシステム1の全体の処理の流れについて説明する。

図6は、本発明に係るセキュアプリントシステム1の構成を示すブロック図である。図18は、設定情報802の一例を示す図、図19は、監視ポート907の詳細を示す図である。図21は、ジョブ310の詳細を示す図である。図22は、印刷情報管理ヘッダ311の詳細を示す図である。図23は、ジョブ情報820の詳細を示す図である。図24は、ジョブリスト805の詳細を示す図である。図25は、実行リスト804の詳細を示す図である。図26は、ファイルシステム501の詳細を示す図である。図27は、ICカード410の詳細を示す図である。図28は、ユーザ情報210の一例を示す図である

10

20

30

40

50

。図29は、LDAPディレクトリ201の詳細を示す図である。図30は、削除設定840の一例を示す図である。図31は、実行カード情報850の一例を示す図である。図32は、復帰時間情報860の一例を示す図である。

【0051】

セキュアプリントシステム1は、LDAPサーバ200とクライアントPC300、印刷装置1000に接続されたNIC700が、双方向通信可能なLAN150を介して接続している。NIC700には、USB通信可能なUSBケーブル160を介して、マスタストレージ500、USBハブ600及びカードリーダー400が接続している。

【0052】

LDAPサーバ200は、LDAPディレクトリ201、LDAP機能部202、I/Fドライバ部190等を有する。LDAPサーバ200、は冗長構成をとることが可能で、複数台設置してもよい。

LDAPサーバ200は、システム内でのユーザ情報の検索という役割を有するため、ユーザ情報の格納及び検索機能を持つサーバであればLDAPサーバに限らない。

【0053】

LDAPディレクトリ201は、図29に示すデータを格納している。

LDAPディレクトリ201は、データ群をまとめる最上位の単位Suffixの下に識別コードが1または複数配備されており、さらに、その識別コードの下に1または複数のユーザ情報210が格納される。

一般的に、識別コードはOU(Organization Unit)で構築される。また、Active

Directory(登録商標)では、Suffixがドメインという単位にあたる。

ユーザ情報210は、図28に示すようにカードID211、ユーザ名212、パスワード213、サブユーザ1 214、サブユーザ2 215、サブユーザ3 216、サブユーザ4 217、利用制限218等を有する。

【0054】

カードID211は、図27に示すように、ユーザのICカード410のIDを登録するもので、suffixの中で一意となる値である。

ユーザ名212は、カードID211と一致するICカード410を保持しているユーザの名前である。

パスワード213は、ユーザの認証を行う際に、本人確認を行うために格納される。

サブユーザ1~4 214~217は、ユーザが使っているメインのユーザ名212とは別の名前で、ユーザが他のユーザの代理を行う場合に使用するユーザ名である。

利用制限218は、印刷装置1000を利用する上での制限情報が格納されている。

【0055】

LDAP機能部202は、LDAPプロトコルに従って通信の接続、認証、検索、変更、追加、削除、切断等を行う。

接続では、接続要求を発行したクライアントに対して、論理的な通信経路を確保する。

認証では、認証要求を発行したユーザ名を、LDAPディレクトリ201内から検索し、パスワードの照合を行って認証結果を返答する。

検索では、検索要求を受けた値を元に、LDAPディレクトリ201から該当するユーザを検索し、一致したユーザ情報210を返答する。

【0056】

I/Fドライバ部190は、LAN150等のネットワークを介して外部機器と接続・通信を行うもので、TCP/IPやUDPなどの通信プロトコルに従って通信を制御する。

【0057】

クライアントPC300は、アプリケーション部301、プリンタドライバ部302、送信バッファ303、I/Fドライバ部190等を有する。

アプリケーション部301は、ユーザにグラフィックユーザインタフェースを提供し、

10

20

30

40

50

ユーザの目的に適った画像データを生成する。

プリンタドライバ部 302 は、アプリケーション部 301 が生成した画像データを印刷装置 1000 で印刷可能なページ記述言語 (P D L) データに変換する。さらに、 P D L データに対して、図 22 に示すようにジョブオーナー 312、ジョブ名 313 等のジョブ情報を含んだ印刷情報管理ヘッダ 311 を付与し、図 21 に示すジョブ 310 を作成する。

送信バッファ 303 は、プリンタドライバ部 302 が作成したジョブ 310 を一時的に格納し、スプールを実現する。

【 0058 】

USB ハブ 600 は、USB 通信部 195 等を有する。USB ハブ 600 は、USB データを中継し、USB ハブ 600 に接続された機器の USB データを他の各機器へ転送する。

10

USB 通信部 195 は、USB 仕様に従ってコントロール転送、インタラプト転送、バルク転送、アイソクロナス転送などのデータ通信を行う。データ転送することが必要条件であり、転送速度や USB バージョンなどは特に問わない。

【 0059 】

マストレージ 500 は、ファイルシステム 501、ファイルシステム管理部 502、USB 通信部 195 等を有する。

図 26 に示すように、ファイルシステム 501 はジョブ 310 を内部記憶装置 (図示しない) に格納する。また、ジョブ 310 の書き込み、読み込み、削除を行う。

【 0060 】

20

カードリーダー 400 は、USB 通信部 195、カード読取部 401 等を有する。

カード読取部 401 は、IC カード 410 (記憶媒体) からカード ID 211 を読み取るためのものである。IC カード 410 がカードリーダー 400 にかざされると、IC カード 410 (記憶媒体) からカード ID 211 等の情報を読み取り、USB 通信部 195 を介して接続された他機器に情報を伝達する。

尚、本実施形態では IC カードをカードリーダーにかざすことによる認証を用いた構成としたが、指紋或いは手や指の静脈の情報 (生体情報) を用いた認証を用いた構成であってもよい。この場合、カードリーダー 400 を指や手などの読取対象物を読み取るリーダー (読取部) に置き換えることで実現可能である。

【 0061 】

30

NIC 700 は、アプリケーション 800、NIC OS 900 等を有する。

アプリケーション 800 は、NIC OS 900 上で動作するプログラムである。

NIC OS 900 は、NIC 700 を制御すると同時に、NIC 700 上のアプリケーション 800 の管理、印刷装置 1000 への各種指示なども行う。

【 0062 】

NIC 700 のアプリケーション 800 は、設定情報管理部 801、設定情報 802、LPR 通信部 803、実行リスト 804、ジョブリスト 805、LDAP 通信部 806、LDAP サーバ監視部 807、印刷情報管理プロトコル解析部 808、リスト管理部 809、ユーザ通知部 810、カードリーダー管理部 811、ファイル管理部 812、印刷指示部 813、ビープ指示部 814、パネル表示指示部 815 等を有する。更に、図 6 には図示していないが、アプリケーション 800 は、削除設定 840、実行カード情報 850、復帰時間情報 860 等を有する。

40

【 0063 】

設定情報管理部 801 は、図 18 に示すアプリケーション 800 の実行に必要な設定情報 802 を管理するもので、設定情報 802 の書き込み、読み出しを行う。

クライアント PC 300 が、ブラウザを使ってアプリケーション 800 にアクセスしてアプリケーション 800 の設定情報を設定し、アプリケーション 800 がクライアント PC 300 からの指示を受け取ると、設定情報管理部 801 は、設定されたデータを設定情報 802 として保持する。

設定情報 802 は、Suffix 831、識別コード 832、プライマリサーバ 833

50

、プライマリポート 834、セカンダリサーバ 835、セカンダリポート 836、ユーザ 837、パスワード 838等を有する。

【0064】

S u f f i x 831、識別コード 832は、LDAPサーバ 200に検索要求を発行する際、検索場所を指定する条件となる。

プライマリサーバ 833、プライマリポート 834、セカンダリサーバ 835、セカンダリポート 836は、LDAPサーバ 200に接続するための情報である。LDAPサーバ 200は冗長構成をとることができるため、プライマリ・セカンダリのように複数台の設定することが可能となっている。

ユーザ 837、パスワード 838は、LDAPサーバ 200に認証要求を発行する際に必要な情報である。

10

【0065】

L P R 通信部 803は、L P R 印刷プロトコルを解析し、通信を行うもので、クライアント P C 300からジョブ 310を受け取る際のプロトコルを解析し、通信する。

ここでは、例示的に L P R と記したが、印刷プロトコルであれば特に L P R に限らない。

【0066】

実行リスト 804は、図 25で示されるもので、図 24に示すジョブリスト 805のサブセットである。印刷を実施するときは、実行リスト 804に格納されたジョブ情報 310をもとに印刷指示を行う。

20

ジョブリスト 805は、図 23に示すジョブ情報 820で構成されている。ジョブ情報 820は、ジョブ 310を管理するために必要な情報を抽出した情報で、ユーザ名 821、ファイル名 822、ジョブ名 823、タイムスタンプ 824等を有する。ジョブリスト 805は、ファイルシステム 501に格納されているジョブ 310の情報をすべて保持している。

【0067】

L D A P 通信部 806は、L D A P サーバ 200と L D A P プロトコルに従って通信を行うもので、設定情報 802のプライマリサーバ及びプライマリポートで指定される L D A P サーバ 200に接続する。

L D A P 通信部 806は、設定情報 802のユーザ 837及びパスワード 838を用いて認証を行う。また、L D A P 通信部 806は設定情報 802の S u f f i x 831、識別コード 832を検索場所として、カード I D 211に紐づくユーザ情報 210(図 28)を検索する。プライマリにもセカンダリにもアクセスできなかった場合、監視ポート 907から印刷ポートの指定を解除する。

30

【0068】

L D A P サーバ監視部 807は、L D A P サーバ 200と N I C 700が通信できる状態にあるかどうかを定期的に監視する。実際の接続処理等は、L D A P 通信部 806を通じて行われる。監視処理中に、L D A P サーバ 200と N I C 700が通信できると判断した場合で、かつ監視ポート 907に印刷ポートが設定されていない場合、監視ポート 907に印刷ポートを追加する。これにより、サーバダウン時の印刷切り替えの復帰を実現する。

40

【0069】

印刷情報管理プロトコル解析部 808は、ジョブ 310に含まれる印刷情報管理ヘッダ 311を解析する。印刷情報管理ヘッダ 311は、P D L データの先頭に付加されるバイナリデータで、様々なジョブ情報が含まれる。

印刷情報管理ヘッダ 311に含まれるジョブオーナー 312とジョブ名 313を取得し、ジョブ情報 820を作成する際、印刷情報管理プロトコル解析部 808で解析した値を利用する。

【0070】

リスト管理部 809は、実行リスト 804及びジョブリスト 805を管理する。ジョブ

50

310がファイルシステム501に書き込まれると、ジョブ情報820をファイル管理部812から受け取り、ジョブリスト804に追加して管理する。また、ジョブリスト805の中でLDAP通信部806から渡されたユーザ名に一致したジョブ情報820を抽出し、実行リスト804を作成する。リスト管理部809は、印刷完了時にファイル管理部812から通知を受け、該当するジョブ情報820をジョブリスト805から削除する。

【0071】

ユーザ通知部810は、印刷装置1000を利用しているユーザに対して、エラーなどを通知する。ユーザ通知部810は、NIC OS900に対してビープ指示し、印刷装置1000からビープ音を鳴動させてユーザの聴覚に訴えたり、パネル表示指示を行って任意の文字を印刷装置1000のパネルに表示し、ユーザの視覚に訴えたりする機能を持つ。

10

【0072】

カードリーダ管理部811は、NIC700にUSB160を介して接続されたカードリーダ400を制御するためのものである。ICカード410(記憶媒体)がカードリーダ400にかざされると、カードリーダ管理部811はカードID211を取得する。

【0073】

ファイル管理部812は、ジョブ310をアプリケーション800内で管理する。ファイル管理部812は、ジョブ310を暗号化してファイルシステム501に格納する。また、ジョブ310を復号化し、印刷指示部813にジョブ310を送ったり、あるいは、印刷指示部813へのジョブ投入が終わったタイミングで、該当するジョブ310をファイルシステム501から削除する。

20

【0074】

印刷指示部813は、ファイル管理部812から送られてきた復号化されたジョブ310をNIC OS900に対して、印刷情報管理プロトコルを用いて印刷指示する。

【0075】

ビープ指示部814は、ユーザ通知部810からのビープ指令を受け取って、NIC OS900に通知する。ビープ音に関しては、印刷情報管理プロトコル、JL、UDP等を使用したり、様々な方法でビープ鳴動を実現できるが、どの機能がサポートされているかは印刷装置1000によって異なる。ビープ指示部814は、印刷装置1000の種別

30

による違いを吸収して適切なビープ指示を行う。
パネル表示指示部815は、MIB(Management Information Base)を使って印刷装置1000のパネル(図示しない)に任意のメッセージを表示させる。一定時間表示させることができない機種の場合、印刷装置1000の場合は、数秒表示後に表示のリセットを行う。

【0076】

削除設定840は、図30に示されるもので、LDAPサーバ200がダウンした後、復帰した際のマストレージ500に蓄積されている印刷データの削除処理機能に関する設定である。「ON」の場合、NIC700は、削除処理を実行する。「AUTO」の場合、NIC700は、実行リスト804をチェックし、削除対象のジョブがある場合には削除処理を実行する。「OFF」の場合、NIC700は、削除処理を実行しない。実行カード情報850は、図31に示されるもので、削除処理を実行するユーザが持つカードの情報である。復帰時間情報860は、図32に示されるもので、LDAPサーバ200がダウンした後、復帰した時刻を示す情報である。尚、一定間隔でLDAPサーバ200と通信可能かどうかを確認するような構成の場合、復帰時間情報860は、LDAPサーバ200が実際に復帰した時間でなく、LDAPサーバ200に接続を試みて接続が確認できた時刻とすることも可能である。つまり、復帰時間情報860は、接続時間情報と言い換えることが可能である。また、時間は時刻を含むものである。

40

【0077】

次に、NIC OS900について詳細を説明する。

50

N I C O S 9 0 0 は、I / F ドライバ部 1 9 0、U S B 通信部 1 9 5、暗号/復号化部 9 0 5、印刷情報管理プロトコル解析・通信部 9 0 4、J L 通信部 9 0 3、U D P 通信部 9 0 2、M I B 通信部 9 0 1、通信制御部 9 0 6、監視ポート 9 0 7 を有する。

【 0 0 7 8 】

暗号/復号化部 9 0 5 は、データの暗号化及び復号化を行うためのものである。形式は固定のものではなく、D E S (D a t a E n c r y p t i o n S t a n d a r d) やトリプル D E S、A E S (A d v a n c e d E n c r y p t i o n S t a n d a r d) 等のブロック暗号化、及び R C 4 などのストリーム暗号化などを行うことができる。

印刷情報管理プロトコル解析・通信部 9 0 4 は、印刷情報管理プロトコルに従ってデータ通信を行うためのものである。印刷情報管理プロトコルは、印刷装置 1 0 0 0 の制御を行うための通信プロトコルであり、印刷指示やビープ音鳴動等などが行える。

J L 通信部 9 0 3 は、J L 通信を行うためのものである。J L はジョブ制御言語であり、印刷装置 1 0 0 0 の情報取得指令や、P D L データの受信指令、印刷装置 1 0 0 0 へのビープ指令などを行うことができる。

【 0 0 7 9 】

U D P 通信部 9 0 2 は、U D P 通信を行う。この U D P 通信を使って、D N S (D o m a i n N a m e S y s t e m) クエリや、ビープ指令などを行うことができる。

M I B 通信部 9 0 1 は、M I B 通信を行うためのものである。M I B は、通信機器を管理するためのプロトコルで、印刷装置 1 0 0 0 のパネル表示等を行う。

通信制御部 9 0 6 は、I / F ドライバ部 1 9 0 から受信したデータを、アプリケーション 8 0 0 に通知したり、印刷装置 1 0 0 0 に渡したりする。通信制御部 9 0 6 は、監視ポート 9 0 7 に設定されているポートに対してデータが送信されてきた場合、アプリケーション 8 0 0 に通知し、監視ポート 9 0 7 に設定されていないポートへのデータを受信した場合は、印刷装置 1 0 0 0 にデータを転送する。

監視ポート 9 0 7 は、図 1 9 に示すように、通信制御部 9 0 6 がアプリケーション 8 0 0 と印刷装置 1 0 0 0 のどちらにデータを転送するかを決定するための情報である。監視ポート 9 0 7 は、アプリケーション 8 0 0 に通知する通信ポート番号を指定する。

【 0 0 8 0 】

次に、印刷装置 1 0 0 0 について説明する。

印刷装置 1 0 0 0 は、I / F ドライバ部 1 9 0、受信バッファ 1 0 0 1、送信バッファ 1 0 0 2、M I B 通信部 9 0 1、U D P 通信部 9 0 2、J L 通信部 9 0 3、印刷情報管理プロトコル解析・通信部 9 0 4、L P R 通信部 8 0 3、パネル表示部 1 0 0 8、ビープ鳴動部 1 0 0 9、P D L トランスレータ部 1 0 1 1、機器 D B 部 1 0 1 0、描画バッファ 1 0 1 2、描画部 1 0 1 3、プリンタエンジン部 1 0 1 4 を有する。

【 0 0 8 1 】

受信バッファ 1 0 0 1 は、I / F ドライバ部 1 9 0 で受信した全データを一時的に確保し、処理遅延の緩衝材となる。

送信バッファ 1 0 0 2 は、I / F ドライバ部 1 9 0 に送信する前の全データを一時的に確保し、処理遅延の緩衝材となる。

パネル表示部 1 0 0 8 は、指定されたメッセージを印刷装置 1 0 0 0 のパネルに表示する。

ビープ鳴動部 1 0 0 9 は、印刷装置 1 0 0 0 内蔵の鳴動装置 (図示しない) を作動させ、音を鳴らす。

機器 D B 部 1 0 1 0 は、J L により設定された印刷装置 1 0 0 0 の情報を格納し、P D L トランスレータ部 1 0 1 1 に情報を提供する。ここでいう環境情報とは、例えば印刷枚数のことである。

【 0 0 8 2 】

P D L トランスレータ部 1 0 1 1 は、P D L データの翻訳処理を行い、描画に適した描画オブジェクトである中間データに変換を行う。

描画バッファ 1 0 1 2 は、P D L トランスレータ部 1 0 1 1 によって生成された描画オ

10

20

30

40

50

プロジェクトの中間データを、実際に印刷を行うまで一時的に格納しておく。

描画部 1013 は、描画バッファ 1012 に一時格納された描画オブジェクトを実際に描画してビットマップ画像であるイメージデータを生成する。

プリンタエンジン部 1014 は、描画部 1013 が生成したビットマップ画像を受け取り、既知の印刷技術により用紙等のメディアに印刷を行う。

【0083】

次に、図 7、8、9、10、11、12、13、14、15、16、17、20 を参照しながら、本発明に係るセキュアプリントシステム 1 の詳細な処理について説明する。

図 7 は、セキュアプリントシステム 1 の印刷ジョブ投入処理手順の一例を示すフローチャートである。図 8 は、セキュアプリントシステム 1 の印刷ジョブ出力処理手順の一例を示すフローチャートである。図 9 は、セキュアプリントシステム 1 の印刷ジョブ出力処理手順の一例を示すフローチャートである。図 10 は、セキュアプリントシステム 1 の印刷ジョブ出力処理手順の一例を示すフローチャートである。図 11 は、セキュアプリントシステム 1 の印刷ジョブ出力処理手順の一例を示すフローチャートである。図 12 は、セキュアプリントシステム 1 の印刷ジョブ出力処理手順の一例を示すフローチャートである。図 13 は、セキュアプリントシステム 1 の削除確認処理手順の一例を示すフローチャートである。図 14 は、セキュアプリントシステム 1 の削除処理手順の一例を示すフローチャートである。図 15 は、セキュアプリントシステム 1 の出力処理の詳細手順の一例を示すフローチャートである。図 16 は、セキュアプリントシステム 1 の LDAP サーバ監視処理手順の一例を示すフローチャートである。図 17 は、セキュアプリントシステム 1 のユーザ通知処理手順の一例を示すフローチャートである。図 20 は、印刷装置 1000 に表示するメッセージの一例を示す図である。

【0084】

以下では、NIC 700 が行う処理について、アプリケーション 800 の機能と NIC OS 900 との機能を区別して記載する。そのため、便宜上、処理の主体は、アプリケーション 800 と NIC OS 900 とする。但し、実際には、処理を行う主体は、NIC 700 である。ハードウェアである NIC 700 は、ソフトウェアであるアプリケーション 800 または NIC OS 900 と協働して、後述する処理を実行する。

【0085】

図 7 では、NIC 700 は、クライアント PC 300 から、印刷データを受付ける。また、NIC 700 は、受け付けた印刷データをマストレージ 500 に記憶する。また、NIC 700 は、印刷データを印刷装置 1000 に送信する。

【0086】

図 7 に示すように、セキュアプリントシステム 1 へのジョブ投入の処理では、クライアント PC 300 のアプリケーションが、プリンタドライバを介してジョブ 310 を生成する（ステップ S001）。

クライアント PC 300 が、生成されたジョブ 310 を NIC OS 900 に対して送信すると（ステップ S002）、NIC OS 900 はクライアント PC 300 から送信されたデータを受信し、監視ポート 907 の設定を見て分岐処理を行う（ステップ S003）。

クライアント PC 300 は、印刷方法がマストレージ 500 を使ったものか、LDAP サーバ 200 と通信できずにそのまま印刷装置 1000 から出力するのかが、意識する必要はない。印刷出力する際に、LDAP サーバ 200 と通信できているのかが否かを意識せずに、ジョブ 310 を送信することができるため、設定変更の手間が省け、よりユーザビリティの高いセキュアプリントシステムを実現している。

【0087】

監視ポート 907 に設定されていない監視対象外のポートへのデータの場合、NIC OS 900 は受信したジョブ 310 を印刷装置 1000 に転送し（ステップ S004）、印刷装置 1000 は転送されたジョブ 310 を受け付け、受信バッファ 1001 に格納し、スプール処理を行う（ステップ S005）。

10

20

30

40

50

印刷装置 1000 は、スプールされたジョブ 310 のデータの印刷情報管理ヘッダ 311 を解析する (ステップ S006)。解析したデータは、図示しない内部ログデータなどに利用される。

印刷装置 1000 は、ジョブ 310 内の PDL データを解析し、描画オブジェクトの中間データを作成し、さらにその中間データをもとにビットマップイメージを作成する (ステップ S007)。

印刷装置 1000 は、作成したビットマップイメージを既知の印刷技術により用紙等のメディアに印刷を行う (ステップ S008)。

【0088】

受信データが監視ポート 907 に設定されているポートへのデータの場合、受信データが監視対象になっているポートへのデータの場合、NIC OS900 はアプリケーション 800 にジョブ 310 を転送する (ステップ S009)。

アプリケーション 800 は、ジョブ 310 の印刷情報管理ヘッダ 311 を解析し、ジョブオーナー及びジョブ名を取得し (ステップ S010)、アプリケーション 800 はジョブ情報 820 を作成する (ステップ S011)。

取得したジョブオーナー 312 をユーザ名 821 として、取得したジョブ名 313 をジョブ名 823 として格納する。また、アプリケーション内で一意となる文字列を生成してファイル名 822 とする。タイムスタンプ 824 は、ファイル書き込み後に記憶する。

【0089】

アプリケーション 800 は、ジョブ 310 を暗号化するため、ジョブ 310 のデータを NIC OS900 に渡し、暗号化鍵や暗号化アルゴリズムなどを指定する (ステップ S012)。

NIC OS900 は、渡されたジョブデータを指定されたパラメータを用いて暗号化する (ステップ S013)。

アプリケーション 800 は、NIC OS900 が暗号化したジョブをファイルシステム 501 (記憶部) に書き込む (書込) (ステップ S014)。

ファイルシステム 501 にジョブ 310 を書き込むことにより、従来のようにプリンタサーバ 101 にジョブ 310 を書き込む必要がなくなる。これにより、プリンタサーバ 101 を不要なものとし、よりセキュリティの高いセキュアプリントシステムを実現している。また、プリンタサーバ 101 が不要なため、サーバを設置するコストや、セキュアプリントシステム導入におけるサーバ設置の設定などの手間が省ける。さらに、万が一、マストレージ 500 が印刷装置 1000 から取り外された場合も、ジョブ 310 は暗号化して書き込まれているため、ジョブ 310 内の PDL データを読み取られる心配はなく、より高いセキュリティを実現している。

【0090】

NIC OS900 が、ジョブ 310 を保存した処理をマストレージ 500 に伝達すると (ステップ S015)、マストレージ 500 は暗号化されたジョブ 310 をファイルシステム 501 に書き込む (ステップ S016)。

NIC OS900 が、暗号化されたジョブ 310 のファイルシステム 501 への書き込み処理をアプリケーション 800 に伝達する (ステップ S017)。アプリケーション 800 に伝達すると、アプリケーション 800 はファイルシステム 501 にジョブ 310 を書き込み終了した時点のタイムスタンプ (記憶時間情報) を取得し、ジョブ情報 820 のタイムスタンプ 824 に格納する (ステップ S018)。

アプリケーション 800 は、作成したジョブ情報 820 をジョブリスト 805 に格納する (ステップ S019)。

【0091】

次に、図 8、図 9、図 10、図 11、図 12、図 13、図 14、図 15 を参照しながら、セキュアプリントシステム 1 のジョブ出力の処理について説明する。

【0092】

図 8 では、NIC 700 は、ユーザ情報 210 を含む認証要求を LDAP サーバ 200

10

20

30

40

50

に送信する。また、NIC700は、LDAPサーバ200と通信できるか否かを判断する。また、LDAPサーバ200と通信できない場合、NIC700は、印刷データをマストレージ500に記憶する設定を解除する。また、認証サーバと通信可能、かつ印刷データをマストレージ500に記憶する設定が解除されている場合、NIC700は、その設定を再設定する。

【0093】

図8に示すように、カードリーダー400は、ICカード410（記憶媒体）を検知して、内部に記録されているカードID211を読み取り（ステップS100）、NIC OS900は読み取った情報をアプリケーション800に伝達する（ステップS101）。尚、この読み取りは、ICカード（記憶媒体）の特定の領域を読み取ることで、カードIDを取得するものとする。また、この特定の領域には、カードの識別情報或いは、ユーザの識別情報が記憶されていてもよい。

10

【0094】

アプリケーション800は、NIC OS900から、カードIDを取得する（ユーザ識別情報受付）。そして、監視ポート907の設定を見て印刷ポート（例えばRawであれば9100番、LPRであれば515番など）が設定されているかどうか確認する（ステップS102）。

印刷ポートが監視対象外になっており、LDAPサーバ200と通信もできない場合、アプリケーション800は図20に示すメッセージからメッセージ1である「APヒョウジュンインサツ」を選択し、図17に示すユーザ通知処理を行う（ステップS103）。

20

【0095】

印刷ポートが監視ポート907に設定されている場合、あるいは、印刷ポートが監視対象外になっていても、LDAPサーバ200に通信を行い通信が確立できる場合は監視ポートに印刷ポートを追加する。アプリケーション800は設定情報802をもとに、LDAPサーバ200に接続を試みる（ステップS104）。より詳細には、アプリケーション800は、設定情報802を参照し、プライマリであるLDAPサーバ200aのプライマリポートに対して接続を行い、仮に接続できなかった場合は、セカンダリであるLDAPサーバ200bのセカンダリポートに対して接続を行う。また、このときLDAPサーバ200に通信可能である場合は、復帰時間情報860に、現在の時刻を設定する（時間情報記憶）。実行リスト804内のジョブ情報820のタイムスタンプと復帰時間情報860に設定したタイムスタンプとを比較することによって、実行リスト804内に、削除対象のジョブがあるかどうかを自動で判定することが可能となる。

30

【0096】

NIC OS900は、接続要求をもとにLDAPサーバ200に接続を試行し（ステップS105）、アプリケーション800は、接続試行が成功したか否か（通信可否判断）で分岐処理を行う（ステップS106）。

より詳細には、プライマリであるLDAPサーバ200a、およびセカンダリであるLDAPサーバ200bの両方に接続できなかった場合、接続失敗とみなす。

そして、アプリケーション800は、監視ポート907に設定されている印刷ポートの設定を解除し（ステップS107）、図20に示すメッセージからメッセージ2の「APサーバエラー」を選択し、ユーザ通知処理を行う（ステップS108）。

40

LDAPサーバ200に接続できなかった場合、監視ポート907の設定を解除するため、次の印刷からはマストレージ500にジョブ310を保存せずに、印刷装置1000から直接印刷することになる。従って、LDAPサーバ200と通信できない状態のときも印刷物を出力することが可能となる。

【0097】

次に、図9に示すように、プライマリであるLDAPサーバ200a、あるいはセカンダリであるLDAPサーバ200bのいずれかに接続できた場合、アプリケーション800はLDAP認証を行う（ステップS109）。

設定情報802のユーザ837及びパスワード838をLDAPサーバ200に送信し

50

、認証要求を発行（認証要求送信）する。なお、この認証処理に関しては、LDAPサーバ200が認証をしなければ検索をさせないという強固なセキュリティが施されている場合の処理である。他の実施形態として、検索を行うにあたって認証が必要ない設定（非認証の設定）がなされていた場合は、認証に伴うS109からS114までの処理を省略してもよい。

【0098】

NIC OS900は、アプリケーション800から伝達されたデータをLDAPサーバ200に送信する（ステップS110）。

LDAPサーバ200は、LDAPサーバ200が送信したデータのユーザ名でLDAPディレクトリ201を検索する。ユーザが見つかった場合、送信されたデータと対応するユーザのユーザ情報210に含まれるパスワード213を照合し、認証結果を返答する（ステップS111）。

10

NIC OS900が、LDAPサーバ200から受信したデータをアプリケーション800に伝達すると（ステップS112）、アプリケーション800はLDAP認証結果を受け取る（ステップS113）。

【0099】

アプリケーション800は、前段S113での認証結果の可否により分岐処理を行い（ステップS114）、認証に失敗した場合、図20に示すメッセージからメッセージ2の「APサーバエラー」を選択し、ユーザ通知処理を行う（ステップS115）。

認証に成功した場合、アプリケーション800は設定情報802をもとにカードID211の検索をLDAPサーバ200に対して行う（ステップS116）。

20

アプリケーション800は、設定情報802のSuffix831と識別コード832を用いて検索位置を指定する。

【0100】

NIC OS900は、アプリケーション800から伝達されたデータをLDAPサーバ200へ送信する（ステップS117）。

LDAPサーバ200は、アプリケーション800から送信されたデータをもとにLDAPディレクトリ201を検索し、検索結果を返信する（ステップS118）。

指定されたSuffix831及び識別コード832以下にあるデータの中から、指定されたカードID211を探し、見つかったユーザ情報210を送信する。Suffix831や識別コード832は、LDAPディレクトリ201中のユーザの位置を特定するために指定する情報であり、一般的にLDAP検索の際にSearchBaseとして指定される値である。

30

【0101】

NIC OS900が、LDAPサーバ200から受信したデータをアプリケーション800に伝達すると（ステップS119）、アプリケーション800はLDAPサーバ200からの検索結果を取得する（ユーザ識別情報受付）（ステップS120）。

【0102】

次に、図10に示すように、アプリケーション800は、LDAPサーバ200からの検索結果を見てユーザ情報210が取得できたか、即ち、ユーザが存在したか否かにより分岐処理を行う（ステップS121）。

40

ユーザ情報210が取得できない場合、アプリケーション800は図20に示すメッセージからメッセージ3の「APユーザミトウロク」を選択し、ユーザ通知処理を行う（ステップS122）。

【0103】

ユーザ情報が取得できた場合、アプリケーション800はユーザ情報210の利用制限をもとに、ユーザに利用権があるか否かで分岐処理を行う（ステップS123）。

利用制限には様々な設定方法が考えられるが、例えば、4桁の数字で利用権限を表現し、1桁目がプリンタの利用権限、2桁目がコピーの利用権限、3桁目がスキヤンの利用権限、4桁目がファクスの利用権限とする。そして、その値が“0”は「使用不可能」、

50

“ 1 ” は「モノクロのみ使用可能」、「 2 ” は「カラーモノクロ双方利用可能」とする。そして、ユーザ情報 2 1 0 内の利用権限を参照し、プリンタの項目が “ 0 ” ならば「権限なし」、「 1 ” あるいは “ 2 ” ならば「権限あり」、とみなすという方法が考えられる。

利用権限がない場合、アプリケーション 8 0 0 は図 2 0 に示すメッセージからメッセージ 4 の「 A P ユーザエラー」を選択し、ユーザ通知処理を行う（ステップ S 1 2 4）。

【 0 1 0 4 】

図 1 1 では、 N I C 7 0 0 は、 L D A P サーバ 2 0 0 と通信できる場合、マストレージ 5 0 0 からユーザ情報 2 1 0 に応じた印刷データを取得する。

【 0 1 0 5 】

図 1 1 に示すように、利用権限がある場合、アプリケーション 8 0 0 は取得したユーザ情報 2 1 0 内のユーザ名をキーとして、ジョブリスト 8 0 5 の中からユーザ名が一致するジョブ情報 8 2 0 を抽出する（ステップ S 1 2 5）。

アプリケーション 8 0 0 は、抽出したジョブ情報 8 2 0 をリストにして実行リスト 8 0 4 を作成する（ステップ S 1 2 6）。

【 0 1 0 6 】

アプリケーション 8 0 0 は、取得したユーザ情報 2 1 0 の中からサブユーザを取得する（ステップ S 1 2 7）。

直前にサブユーザ 1 を取得していれば、次のサブユーザ 2 を取得する。サブユーザに関連する S 1 2 7 から S 1 3 0 までの一連の処理は、一人のユーザで複数ユーザの印刷物を出力させるために行う処理である。例えば、従来は I C カード一枚につき 1 ユーザまでしか登録できなかったため、秘書が上司の印刷物を出力したい場合は I C カードを借りる必要があった。また、一人で 2 台の P C を使っているユーザは 2 枚の I C カードを携帯する必要があった。この一連のサブユーザに関連する処理を行うことにより、上記問題を解決し、 1 枚の I C カードで複数ユーザの印刷物を出力することが可能となる。

【 0 1 0 7 】

アプリケーション 8 0 0 は、取得したサブユーザをチェックし（ステップ S 1 2 8）、サブユーザ 4 までのすべてのサブユーザを取得した場合、あるいは、サブユーザが取得できなかった場合、登録されていなかった場合は S 1 3 1 へ進む。

サブユーザが取得できた場合、アプリケーション 8 0 0 はサブユーザに一致するジョブ情報 8 2 0 をジョブリスト 8 0 5 の中から抽出し（ステップ S 1 2 9）、抽出したジョブ情報 8 2 0 を実行リスト 8 0 4 に加える（ステップ S 1 3 0）。

【 0 1 0 8 】

すべてのサブユーザを取得すると、アプリケーション 8 0 0 は作成した実行リスト 8 0 4 をソートする（ステップ S 1 3 1）。

ジョブ情報 8 2 0 をタイムスタンプ 8 2 4 でソートし、続いてユーザ名 8 2 1 でソートし、ユーザ名 8 2 1 のまとまりで時系列に並び替えられる。このソートにより、複数ユーザの印刷物を出力したいときにユーザ毎にまとめた出力物が得られ、分別の手間が省ける。また、各ユーザの印刷物はタイムアウト順に並んでいるため、印刷実行したユーザの指示通りの順番になりユーザにわかりやすい出力順になる。また、ソートの仕方についてはこの方法に限られず、ユーザ名でソートし、続いてタイムスタンプでソートしてもよい。

【 0 1 0 9 】

次に、図 1 2 に示すように、アプリケーション 8 0 0 は、実行リスト 8 0 4 内のジョブ情報 8 2 0 の数をチェックし（ステップ S 1 3 2）、 0 件の場合、図 2 0 に示すメッセージからメッセージ 5 の「 A P ジョブナシ」を選択し、ユーザ通知処理を行う（ステップ S 1 3 3）。

【 0 1 1 0 】

次に、図 1 3 に示す削除確認処理を行い（ステップ S 1 3 4）、実行リスト 8 0 4 内のジョブ情報 8 2 0 をすべてクリアする（ステップ S 1 3 8）。

【 0 1 1 1 】

10

20

30

40

50

次に、図13を参照しながら、セキュアプリントシステム1の削除確認処理について説明する。

【0112】

まず、アプリケーション800は削除設定840を参照する(ステップS601)。ここで、削除設定840が「OFF」であれば、ステップS602へ進む。削除設定840が、「ON」もしくは「AUTO」であれば、ステップS607に進む。ここで削除設定840を確認するのは、図14に示す削除処理は通常の印刷に比べて時間がかかるため、設定されていないければ、通常の印刷処理を行うためである。

【0113】

ステップS601での判定において削除設定840が「OFF」の場合、アプリケーション800は実行リスト804内のジョブ情報820の数で、ループ処理を行う(ステップS602)。すべてのジョブ情報820を参照すると、ループ処理を終了する。このループ処理とは、実行リストにある全てのジョブ情報820に関して、ステップS603からステップS606を行う処理である。ステップS602では、実行リストにある全てのジョブ情報820について、当該処理を終えたかを判定し、当該処理を終えた場合、削除確認処理を終了する。

アプリケーション800は、ジョブ投入可否を判定する(ステップS603)。通常、印刷機器はRAMに制限があるため、一度に投入できる印刷ジョブを制限している。ジョブ投入可否を判定するのは、投入制限を越えているにも関わらずジョブを投入してしまい、印刷が失敗してしまうことを防ぐためである。

次に、アプリケーション800はウエイト処理を行う(ステップS604)。このウエイト処理は、ジョブが投入制限を越えて投入できない場合にループ(ステップS603からステップS604)を回り続け、CPUを占有してしまう現象を防ぐ。

アプリケーション800は、図15に示す出力詳細処理を行い(ステップS605)、実行リスト804内から、ジョブ情報820を削除する(ステップS606)。

【0114】

アプリケーション800は、ステップS601での判定において削除設定840が「ON」もしくは「AUTO」の場合、削除設定840が「AUTO」かどうかの判定を行う(ステップS607)。ここで、削除設定840の確認を行うのは、図14に示す削除処理は通常の印刷に比べて時間がかかるため、設定により、削除印刷処理を毎回しなくてもいいように切り替えられるようにするためである。

【0115】

アプリケーション800は、ステップS607にて、削除設定840がONの場合、図14に示す削除処理を行う(ステップS610)。

ここで、削除設定840が「AUTO」となっていれば、実行リスト804の確認を行う(ステップS608)。詳しくは、実行リスト804内にあるジョブ情報820内のタイムスタンプ824(印刷データを記憶する際の時間(時刻を含む))と、復帰時間情報860とを比較する。これは実行リスト804内のすべてのジョブ情報820に対して比較を行う。この結果、ひとつでも復帰時間情報860前のジョブ情報820があれば、削除対象のジョブがある、とみなし、逆にひとつもなければ、削除対象のジョブがない、とみなす(ステップS609)。これにより、LDAPサーバ200が復帰したときに、無駄なジョブが出力されることを避けることができる。

【0116】

削除対象のジョブとは、認証サーバがダウンする前に投入されたものであって、その後認証サーバがダウンして印刷ができなかったものである。そして、削除対象のジョブであっても、実際に削除するかどうかは、ユーザの判断が必要となる。これは、認証サーバがダウンした後、ユーザが同一内容のジョブを印刷した場合には削除しても良いが、それ以外は削除すべきではなく、同一内容のジョブを印刷したかどうかはユーザしか分からないためである。例えば、図23に示すユーザ名821、ファイル名822、ジョブ名823の全てが同一であっても、内容が一致しているかどうかはシステムでは判断できない。

そこで、本発明の実施の形態では、投入されたジョブの内容（ファイル名 8 2 2、ジョブ名 8 2 3 等）ではなく、ジョブの投入時刻（タイムスタンプ 8 2 4 等）に基づいて判断し、ユーザの判断が必要なジョブを削除対象のジョブとしてユーザに通知する。

【 0 1 1 7 】

アプリケーション 8 0 0 は、ステップ S 6 0 9 にて、削除対象のジョブがなければ、ステップ S 6 0 2 へ進み、通常の印刷を実施する。

【 0 1 1 8 】

アプリケーション 8 0 0 は、ステップ S 6 0 9 にて、削除対象のジョブがあれば、図 1 4 に示す削除処理を行う（ステップ S 6 1 0）。

【 0 1 1 9 】

次に、図 1 4 を参照しながら、セキュアプリントシステム 1 の削除処理について説明する。なお、削除処理は 3 パターン存在する。一つ目は、実行リスト 8 0 4 内のジョブすべてをユーザに削除確認を行う方法であり、以下で説明する。二つ目は、実行リスト 8 0 4 内にあるジョブのうち、ステップ S 6 0 9 にて削除対象である、と判定されたもののみ、ユーザに削除確認を行う。残りのジョブは、ステップ S 6 0 2 ~ ステップ S 6 0 6 のフローにより、自動的に印刷を行う。三つ目は、実行リスト 8 0 4 内にあるジョブのうち、ステップ S 6 0 9 にて削除対象である、と判定されたものはユーザに削除確認をとらずに自動的に削除を行ってしまう。残りのジョブは、ステップ S 6 0 2 ~ ステップ S 6 0 6 のフローにより、自動的に印刷を行う。なお、ここでは一つ目のパターンのフローについて説明を行う。

【 0 1 2 0 】

まず、アプリケーション 8 0 0 は、ステップ S 1 0 0 で読み取ったカード I D 2 1 1 を、実行カード情報 8 5 0 に記憶する（ユーザ識別情報記憶）（ステップ S 7 0 1）。これにより、削除の際に他のユーザがカードをかざすことで、不正に削除されることを防ぐことができる。続いて、アプリケーション 8 0 0 は実行リスト 8 0 4 内のジョブ情報 8 2 0 の数で、ループ処理を行う（ステップ S 7 0 2）。すべてのジョブ情報 8 2 0 を参照すると、ループ処理を終了する。このループ処理とは、実行リストにある全てのジョブ情報 8 2 0 に関して、ステップ S 7 0 3 からステップ S 7 1 5 を行う処理である。ステップ S 7 0 2 では、実行リストにある全てのジョブ情報 8 2 0 について、当該処理を終えたかを判定し、当該処理を終えた場合には、実行カード情報 8 5 0 に設定してあるカード I D 2 1 1 を削除して（ステップ S 7 1 7）、削除処理を終了する。

【 0 1 2 1 】

アプリケーション 8 0 0 は、実行リスト 8 0 4 内からジョブ情報 8 2 0 を取得（印刷データ識別情報取得）し、その中のジョブ名 8 2 3（印刷データ識別情報）を、パネルに表示するよう N I C O S 9 0 0 に指令を出す（印刷データ識別情報送信）（ステップ S 7 0 3）。

【 0 1 2 2 】

N I C O S 9 0 0 は、アプリケーション 8 0 0 より受け取った指令を、印刷装置 1 0 0 0 に転送する（印刷データ識別情報送信）（ステップ S 7 0 4）。

【 0 1 2 3 】

印刷装置 1 0 0 0 は、N I C O S 9 0 0 より受け付けた指令を元に、パネルにジョブ名 8 2 3 を表示（識別情報通知）する（ステップ S 7 0 5）。

【 0 1 2 4 】

アプリケーション 8 0 0 は、印刷装置 1 0 0 0 に設置されているパネルのボタン（印刷指示ボタン）が押下されたかを判断する（ステップ S 7 0 6）。パネルのボタンが押下されたかの判断は、ボタンが押下されたことを検知した N I C O S 9 0 0 からボタンが押下された通知を受けることでボタンが押下されたと判断する。押下されていれば、S 7 1 2 へ処理が移る。尚、割り込み処理として、即座にパネルの表示部をリセットするため、このタイミングで S 7 0 8 ~ S 7 1 0 の処理を実行するように構成することも可能である。

10

20

30

40

50

また、押下されなければ、アプリケーション 800 は、パネルの表示部にジョブ名 823 を表示している間（ステップ S703 ~ ステップ S705 の間）にカードがかざされたかどうかを判定する（S711）。カードがかざされていれば、かざされたカードのカード ID 211 と実行カード情報 850 とを比較する（一致するか否かを判定する）（ステップ S716）。ここでカード ID 211 の比較を行うのは、最初にカードをかざしたユーザ以外の人物がカードをかざすことで、不正に他人の印刷物を削除してしまうことを防ぐためである。

カード ID 211 が、実行カード情報 850 と同じだった（一致した）場合は、後述するジョブの削除を行う（ステップ S715）。カード ID 211 が、実行カード情報 850 と異なる場合は、他人と判断し削除できない旨のエラー通知を行う（S718）。このエラー通知は、パネルの表示部に「削除できません」というメッセージを表示して通知する構成でも良いし、音声で通知する構成でも良い。

カードがかざされていない場合、パネルの表示部に一定秒数表示（所定時間通知）したかを確認し（ステップ S707）、表示していなければ、再びパネルボタンの押下確認（ステップ S706）を行う。パネルのボタンの押下を確認するのは利便性を向上させるためである。これを行わないと、ユーザが不必要だとわかっているジョブに対しても必ず数秒間待ってしまう。よって、明らかに不要なジョブに対しては、パネルボタンを押すことですぐに非表示にして、即座に印刷を行う。また、パネルの表示部にジョブ名 823 を一定秒数表示するのは、ユーザに表示されたジョブ名を認識し、カードをかざす時間を与えるためである。

【0125】

また、アプリケーション 800 は、ステップ S706 で、カードがかざされたと判定した場合は、当該ジョブの削除は行わないものとして、ジョブ投入可否を判定する（ステップ S712）。通常、印刷機器は RAM に制限があるため、一度に投入できる印刷ジョブを制限している。ジョブ投入可否を判定するのは、投入制限を越えているにも関わらずジョブを投入してしまい、印刷が失敗してしまうことを防ぐためである。

次に、ジョブの投入制限（投入可能ジョブ数）を越えている場合には（ステップ S712 で NO）、アプリケーション 800 はウエイト処理、つまり、一時的な待機処理を行う（ステップ S713）。このウエイト処理により、ジョブが投入制限を越えて投入できない場合に、ステップ S712 を待機することなく行うということを防ぐ。これにより、CPU を占有してしまう現象を防ぐ。

ステップ S712 でジョブの投入が可能と判断された場合、アプリケーション 800 は、図 15 に示す出力詳細処理を行い（ステップ S714）、実行リスト 804 内から、ジョブ情報 820 を削除する（ステップ S715）。また、ファイルシステム 501 が対応するジョブを削除する。

アプリケーション 800 は、ステップ S715 でジョブの削除後、或いはパネルにジョブ名 823 を一定秒表示した後（S707 で一定秒数表示したと判断した場合）に、パネルの表示部をリセットするよう NIC OS 900 に依頼する（ステップ S708）。

【0126】

NIC OS 900 は、アプリケーション 800 より受け取った指令を、印刷装置 1000 に転送する（ステップ S709）。

【0127】

印刷装置 1000 は、NIC OS 900 より受け付けた指令を元に、パネル表示をリセットする（ステップ S710）。尚、パネルの表示部のリセットは S715 の処理を実行した後に実行するように構成したが、これに限ることなく任意のタイミングでパネルリセット処理を行うようにすることも可能である。例えば、S707 で一定秒数表示したと判定された場合に、S712 の処理に移る前に S707 の処理を実行する。或いは、S706 でボタンが押下されたと判定された場合に、S712 の処理に移る前に S707 の処理を実行する。

【0128】

10

20

30

40

50

アプリケーション 800 は、ステップ S 708 の処理が終了すると、ステップ S 702 に戻り、実行リスト 804 内の次のジョブ情報 820 の処理へ移る。

【0129】

次に、図 15 を参照しながら、セキュアプリントシステム 1 のジョブ出力詳細処理について説明する。

図 15 では、NIC 700 は、印刷データを印刷装置 1000 に送信する。

【0130】

図 15 に示すように、アプリケーション 800 は、上位から渡されたジョブ情報 820 をもとに、ファイルシステム 501 内からジョブ 310 を取得する（ステップ S 201）。アプリケーション 800 は、ジョブ情報 820 に格納されているファイル名 822 に一致するファイルシステム 501 内のファイルの取得をマストレージ 500 に要求する。

NIC OS 900 が、アプリケーション 800 からの指令をマストレージ 500 に伝達すると（ステップ S 202）、マストレージ 500 はファイルシステム 501 から指定のファイルを読み込んで、アプリケーション 800 に返し（ステップ S 203）、NIC OS 900 がマストレージ 500 からの指令をアプリケーション 800 に伝達する（ステップ S 204）。

【0131】

アプリケーション 800 は、取得したジョブ 310 の復号化を NIC OS 900 に要求し、同時に復号化キーや復号化アルゴリズム等を指定する（ステップ S 205）。

NIC OS 900 は、データの復号化処理を行い（ステップ S 206）、アプリケーション 800 は復号化されたジョブ 310 の印刷指示を行う（ステップ S 207）。

NIC OS 900 は、アプリケーション 800 からの指令を受け取り、印刷装置 1000 に印刷情報管理プロトコル通信を用いてジョブ 310 の印刷指示を送る（ステップ S 208）。

【0132】

印刷装置 1000 は、ジョブ 310 を受け取って受信バッファに格納し、スプール処理を行う（ステップ S 209）。受信バッファへの格納が終了すると、印刷装置 1000 は印刷終了を待たずに制御を NIC OS 900 へ戻す。

印刷装置 1000 は、スプールされたジョブ 310 のデータの印刷情報管理ヘッダ 311 を解析する（ステップ S 210）。解析したデータは、図示しない内部ログデータなどに利用される。

印刷装置 1000 は、ジョブ 310 内の PDL データを解析して描画オブジェクトの中間データを作成して、中間データをもとにビットマップイメージを作成し（ステップ S 211）、作成したビットマップイメージを既知の印刷技術により用紙等のメディアに印刷を行う（ステップ S 212）。

【0133】

NIC OS 900 が、印刷装置 1000 の指令をアプリケーション 800 へ伝達すると（ステップ S 213）、アプリケーション 800 は該当するジョブ 310 をファイルシステム 501 からの削除をマストレージ 500 に要求する（ステップ S 214）。

NIC OS 900 が、アプリケーション 800 の指令をマストレージ 500 へ伝達すると（ステップ S 215）、マストレージ 500 は指定されたジョブ 310 をファイルシステム 501 から削除する（ステップ S 216）。

NIC OS 900 は、マストレージ 500 からの指令をアプリケーション 800 へ伝達する（ステップ S 217）。

【0134】

次に、図 16 を参照しながら、セキュアプリントシステム 1 の LDAP サーバ監視処理について説明する。

図 16 では、NIC 700 は、一定間隔で LDAP サーバ 200 と通信可能かどうかを確認する。また、NIC 700 は、LDAP サーバ 200 と通信可能、かつ印刷データをマストレージ 500 に記憶する設定が解除されている場合、その設定を再設定する。

10

20

30

40

50

【 0 1 3 5 】

図 1 6 に示すように、アプリケーション 8 0 0 が、LDAPサーバ監視処理をスレッドとしてNIC OS 9 0 0 に登録し、処理を開始すると(ステップ S 3 0 1)、NIC OS 9 0 0 はアプリケーション 8 0 0 が終了したかどうかをチェックする(ステップ S 3 0 2)。

【 0 1 3 6 】

アプリケーション 8 0 0 が終了していない場合、アプリケーション 8 0 0 は設定情報 8 0 2 に設定されたプライマリであるLDAPサーバ 2 0 0 a 及びセカンダリであるLDAPサーバ 2 0 0 b のポートへの接続をNIC OS 9 0 0 に要求し(ステップ S 3 0 3)、NIC OS 9 0 0 は指定された2つのLDAPサーバ 2 0 0 に接続を行う(ステップ S 3 0 4)。

10

アプリケーション 8 0 0 は、プライマリであるLDAPサーバ 2 0 0 a またはセカンダリであるLDAPサーバ 2 0 0 b のいずれかに接続できたかどうか確認(通信可否判断)を行い(ステップ S 3 0 5)、接続できた場合、監視ポート 9 0 7 の設定で印刷ポートが設定されているか否かを確認する(ステップ S 3 0 6)。

監視ポート 9 0 7 に印刷ポートが設定されていない場合、アプリケーション 8 0 0 は監視ポート 9 0 7 に印刷ポートを追加する(ステップ S 3 0 7)。

また、このときLDAPサーバ 2 0 0 に通信可能である場合は、復帰時間情報 8 6 0 に、現在の時刻を設定する。実行リスト 8 0 4 内のジョブ情報 8 2 0 のタイムスタンプと復帰時間情報 8 6 0 に設定したタイムスタンプとを比較することによって、実行リスト 8 0 4 内に、削除対象のジョブがあるかどうかを自動で判定することが可能となる。

20

アプリケーション 8 0 0 は、ウェイト処理を行い、ループによりCPUを占有してしまう可能性を回避する(ステップ S 3 0 8)。

【 0 1 3 7 】

次に、図 1 7 を参照しながら、セキュアプリントシステム 1 のユーザ通知処理について説明する。

【 0 1 3 8 】

図 1 7 に示すように、アプリケーション 8 0 0 は、上位から伝達されたメッセージ文字列を取得し(ステップ S 5 0 1)、ピーブ音鳴動、及び指定のメッセージ表示をNIC OS 9 0 0 に要求する(ステップ S 5 0 2)。

30

NIC OS 9 0 0 は、印刷装置 1 0 0 0 の種別を判定し、適切な方法を使ってピーブ音鳴動を指示する(ステップ S 5 0 3)。例えば、機種によってUDP、印刷情報管理プロトコル、JLを使用したりするため、その情報をNIC OS 9 0 0 が吸収し、印刷装置 1 0 0 0 の機種にあった方法でピーブ音鳴動指示をする。パネル表示については、MIBを用いて表示指示を印刷装置 1 0 0 0 に送る。

印刷装置 1 0 0 0 は、指令を受け取り、ピーブ音を鳴動させ(ステップ S 5 0 4)、パネルに指定されたメッセージを表示させる(ステップ S 5 0 5)。

【 0 1 3 9 】

次に、図 3 3 を参照しながら、本発明に係るセキュアプリントシステム 1 a の実施例について説明する。

40

図 3 3 は、セキュアプリントシステム 1 a の実施例を示す図である。

【 0 1 4 0 】

ユーザがクライアントPC 3 0 0 にログインし(ステップ 1 - 1)、データの印刷指示を行う(ステップ 1 - 2)。

プリンタドライバは、印刷装置 1 0 0 0 に対して、データからジョブを生成して送信する(ステップ 2 - 1)。ここで、印刷装置 1 0 0 0 上でNIC 7 0 0 がポートの監視を行っていないければ、ジョブはそのまま印刷装置 1 0 0 0 から出力される(ステップ 2 - 2 A)。一方、NIC 7 0 0 がポートの監視を行っている場合、ジョブが印刷装置 1 0 0 0 に渡る前にNIC 7 0 0 が先取りし、マスストレージ 5 0 0 に格納する(ステップ 2 - 2 B)。

50

【0141】

印刷指示をしたユーザが、カードリーダー400にICカード410をかざす(ステップ3-1)。カードリーダー400は、ICカード410からカードID211を読み取って、印刷装置1000に通知する(ステップ3-2)。

印刷装置1000は、受け取ったカードID211に一致するユーザ名をLDAPサーバ200に問い合わせる(ステップ4-1)。LDAPサーバ200は、LDAPディレクトリ201内を検索し、検索したユーザ名を印刷装置1000に送信する(ステップ4-2)。

印刷装置1000は、マストレージ500内からユーザ名に一致するジョブを検索し(ステップ5-1)、マストレージ500は、該当するジョブを印刷装置1000に渡す(ステップ5-2)。

印刷装置1000は、受け取ったジョブのひとつをディスプレイに表示する。その間にユーザがカードリーダー400に、ICカード410をかざせば、該当ジョブを削除する(ステップ6-1)。ユーザがカードリーダー400にICカード410をかざさなければ、そのまま該当ジョブを出力する(ステップ6-2)。印刷装置1000は、ステップ5-2で取得したジョブ数分だけ、ステップ6-1、ステップ6-2を繰り返す。

【0142】

次に、図34を参照しながら、本発明に係るセキュアプリントシステム1bの実施例について説明する。

図34は、セキュアプリントシステム1bの実施例を示す図である。

ユーザがクライアントPC300にログインし(ステップ1-1)、データの印刷指示を行う(ステップ1-2)。

プリンタドライバは、プリンタサーバ101に対して、データからジョブを生成して送信する(ステップ2-1)。プリンタサーバ101はジョブをファイルシステムに格納し(ステップ2-2)、ジョブから書誌データを抽出し、書誌情報に登録する(ステップ2-3)。

印刷指示をしたユーザが、カードリーダー400にICカード410をかざす(ステップ3-1)。カードリーダー400は、ICカード410からカードID211を読み取って、印刷装置1000に通知する(ステップ3-2)。

印刷装置1000は受け取ったカードID211に一致するユーザ名を、認証サーバ102に問い合わせる(ステップ4-1)。認証サーバ102は、認証テーブル内を検索し、検索したユーザ名を印刷装置1000に送信する(ステップ4-2)。

印刷装置1000は、ユーザ名に一致するジョブリストを取得するよう、プリンタサーバ101に依頼する(ステップ5-1)。プリンタサーバ101は、書誌データ内を検索し(ステップ5-2)、印刷装置1000にリストを送信する(ステップ5-3)。

印刷装置1000は、受け取ったジョブのひとつをディスプレイに表示する。その間にユーザがカードリーダー400に、ICカード410をかざせば、プリンタサーバ101に削除要求を発行する(ステップ6-2)。ユーザがカードリーダー400にICカード410をかざさなければ、ユーザのジョブを印刷するよう、プリンタサーバ101に印刷指示を発行する(ステップ6-2)。プリンタサーバ101は、該当ユーザのジョブを書誌情報内から検索し(ステップ6-3)、書誌データをもとに実際のジョブデータをファイルシステムから取得する(ステップ6-4)。プリンタサーバ101は、印刷装置1000に印刷命令を発行し(ステップ6-5)、印刷装置1000は命令に従ってデータを出力する(ステップ6-6)。

印刷装置1000は、ステップ5-3で取得したジョブ数分だけ、ステップ6-1、ステップ6-6を繰り返す。

【0143】

このように本発明の実施の形態によれば、操作部で印刷データを削除できないようなプリンタからでも、印刷データを削除する仕組みを提供することができる。また、認証サーバがダウンするなどの理由により認証できない場合にも、印刷業務を滞らせないための仕

10

20

30

40

50

組みを提供することができる。

【0144】

本発明に係るセキュアプリントシステム1a、セキュアプリントシステム1bでは、操作部で印刷データを削除できないようなプリンタからでも、印刷データを削除することができる。また、本発明に係るセキュアプリントシステム1a、セキュアプリントシステム1bでは、認証サーバが何らかの理由で動作しない場合でも、印刷を行うことが可能であるため、ユーザの業務をとめることがない可用性の高いシステムとなる。

【0145】

本発明に係るセキュアプリントシステム1aでは、プリンタサーバを使わないため、プリンタサーバに印刷データが蓄積されセキュリティホールになるという問題が解消され、より機密性の高いシステムとなる。また、プリンタサーバを使わないため、セキュアな印刷を行う際の環境構築コストを削減でき、より安価なシステムとなる。また、本発明に係るセキュアプリントシステム1aでは、プリンタサーバを使わないことにより、セキュアな印刷を行う蓄積印刷の場合も、あるいは、認証サーバが停止したときの蓄積印刷をしない場合でも、クライアントは違いを意識せずにまったく同じ操作で印刷ジョブを投入できるため、ユーザの利便性がより高いシステムとなる。また、本発明に係るセキュアプリントシステム1aでは、プリンタサーバを用いず、プリンタドライバの設定変更も不要なことから、導入設置が容易に行え、より手間のかからないシステムとなる。

【0146】

〔実施形態2〕

次に、本発明に係るセキュアプリントシステム1a(図33)の実施形態2について説明する。

実施形態1では、ユーザがジョブを削除する場合、一旦ICカードをかざし、その後パネルに表示されるジョブを見て、削除したいジョブであればICカードをかざすことで1ジョブずつ削除を決定する構成について説明したが、本実施形態では、ICカードが所定時間かざされた場合は、ユーザのジョブをすべて削除する構成について説明する。

以下、図35~37を参照しながら、本実施形態について説明する。

尚、実施形態1の図8は、図35に置き換え、実施形態1の図12は、図36に置き換え、実施形態1の図18は、図37に置き換えることで本実施形態を実現可能となる。

その他の図面に関しては、実施形態1と同等のものとし、説明は省略する。

【0147】

まず、図37を参照しながら、本実施形態の利用するデータについて説明する。

図37は、本実施形態における、設定情報802の詳細を示す図である。

設定情報802は、Su f f i x 8 3 1、識別コード832、プライマリサーバ833、プライマリポート834、セカンダリサーバ835、セカンダリポート836、ユーザ837、パスワード838、全削除待機時間839等を有する。全削除待機時間839はICカードがかざされた時間と比較するための値を格納する。この時間は任意に設定できるものとし、例えば3秒などの時間(所定時間)を設定することができる。

尚、図37で示す設定情報802は、図18で示す設定情報802と同様のものであり、図18で示す設定情報802に、全削除待機時間839を追加したものである。

【0148】

次に、図35、図36を参照しながら、本実施形態の詳細な処理について説明する。

図35は、本実施形態における、印刷ジョブ出力処理手順の一例を示すフローチャート、図36は、本実施形態における、印刷ジョブ出力処理手順の一例を示すフローチャートである。

以下では、NIC700が行う処理について、アプリケーション800の機能とNIC OS900の機能とを区別して記載する。そのため、便宜上、処理の主体は、アプリケーション800とNIC OS900とする。ただし、実際には、処理を行う主体は、NIC700である。ハードウェアであるNIC700は、ソフトウェアであるアプリケーション800またはNIC OS900と協働して、後述する処理を実行する。

【 0 1 4 9 】

まず、図 3 5 を参照しながら、本実施形態の印刷ジョブ出力の処理の詳細について説明する。

図 3 5 では、アプリケーション 8 0 0 は、IC カード 4 1 0 (記憶媒体) がかざされていた時間を記憶する。また、NIC 7 0 0 は、ユーザ情報 2 1 0 を含む認証要求を LDAP サーバ 2 0 0 に送信する。また、NIC 7 0 0 は、LDAP サーバ 2 0 0 と通信できるか否かを判断する。また、LDAP サーバ 2 0 0 と通信できない場合、NIC 7 0 0 は、印刷データをマストレージ 5 0 0 に記憶する設定を解除する。また、認証サーバと通信可能、かつ印刷データをマストレージ 5 0 0 に記憶する設定が解除されている場合、NIC 7 0 0 は、その設定を再設定する。

10

【 0 1 5 0 】

図 3 5 に示すように、カードリーダ 4 0 0 は、IC カード 4 1 0 (記憶媒体) を検知して、内部に記録されているカード ID 2 1 1 を読み取り (ステップ S 1 0 0)、NIC OS 9 0 0 は読み取った情報をアプリケーション 8 0 0 に伝達する (ステップ S 1 0 1)。尚、この読み取りは、IC カード (記憶媒体) の特定の領域を読み取ることで、カード ID を取得するものとする。また、この特定の領域には、カードの識別情報或いは、ユーザの識別情報が記憶されていてもよい。

図 3 5 のステップ S 1 0 0 でカード検知がなされた場合、カードリーダ 4 0 0 は NIC OS 9 0 0 に IC カードのカード ID を含むカードがかざされたことを示す情報を伝達 (送信) し、NIC OS 9 0 0 はアプリケーション 8 0 0 に IC カードのカード ID を含むカードがかざされたことを示す情報を通知 (送信) する。

20

尚、カード ID は LDAP サーバ 2 0 0 で一意にユーザ名と対応付いているため、カード ID をユーザを識別するためのユーザ識別情報と言い換えることも可能である。

【 0 1 5 1 】

アプリケーション 8 0 0 は、IC カードのカード ID を含むカードがかざされたことを示す情報を受け付けると、現在の時刻を秒単位で取得して、「IC カードかざしタイムスタンプ」として記憶する (ステップ S 1 0 1 - 1)。ここで現在の時刻を取得するのは、IC カード 4 1 0 (記憶媒体) がかざされた時間を後で計算するためである。

【 0 1 5 2 】

カードリーダ 4 0 0 は、前段でかざされた IC カード 4 1 0 (記憶媒体) が離されたことを検知し、NIC OS 9 0 0 に IC カード 4 1 0 のカード ID を含むカードが離されたことを示す情報を伝達 (送信) する (ステップ S 1 0 1 - 2)。また、NIC OS 9 0 0 は伝達 (送信) されたカード ID を含むカードが離されたことを示す情報をアプリケーション 8 0 0 に通知 (送信) する (ステップ S 1 0 1 - 3)。

30

【 0 1 5 3 】

アプリケーション 8 0 0 は、カード ID を含むカードが離されたことを示す情報を受け、IC カード 4 1 0 (記憶媒体) がカードリーダ 4 0 0にかざされていた時間 (「IC カードかざし時間」) を取得して RAM 4 0 0 2 に記憶する (ステップ S 1 0 1 - 4)。

具体的には、カード ID を含むカードが離されたことを示す情報を受け付けた現在の時刻を秒単位で取得して、「IC カードはずしタイムスタンプ」として記憶する。そして、ステップ S 1 0 1 - 1 で記憶した「IC カードかざしタイムスタンプ」との差を計算して RAM 4 0 0 2 に記憶する (IC カードがかざされていた時間を決定)。この計算結果を IC カード 4 1 0 がかざされていた時間とする。

40

尚、ここではかざした時間、はずされた時間、かざしていた時間を秒数として計算しているが、厳密にチェックしたい場合は、ミリ秒単位で計算してもよい。

また、IC カードがかざされてから、IC カードがはずされた間の時間の算出方法は、タイムスタンプを用いず、IC カードがかざされたことを示す情報を受け付けた場合にタイマーを開始し、次に IC カードがはずされたことを示す情報を受け付けた時の時間を取得するように構成することも可能である。

ステップ S 1 0 2 ~ S 1 0 8 の処理については、実施形態 1 と同様のため説明を割愛す

50

る。

また、本実施形態においても、ＩＣカードをカードリーダーにかざすことによる認証を用いた構成としたが、実施形態１と同様に指紋或いは手や指の静脈の情報（生体情報）を用いた認証を用いた構成であってもよい。この場合、カードリーダー４００を指や手などの読取対象物を読み取るリーダー（読取部）に置き換えることで実現可能である。

さらに、かざされていた時間は、ＩＣカード（読取対象物）がカードリーダー（読取部）にかざされていた時間以外に、指や手（読取対象物）がリーダー（読取部）におかれていた時間をかざされていた時間とし、この時間に応じて全印刷ジョブを削除するか、１つずつ印刷ジョブを削除するかを切り替えることも可能である。

【 0 1 5 4 】

次に、図３６を参照しながら、本実施形態の図１１に続く印刷ジョブ出力の処理について説明する。

図３６では、アプリケーション８００は、実行リスト８０４のジョブ数をチェックする。また、アプリケーション８００はＩＣカード４１０（記憶媒体）がかざされた時間によって、処理を分岐する。

【 0 1 5 5 】

図３６に示すように、アプリケーション８００は、実行リスト８０４内のジョブ情報８２０の数をチェックし（ステップＳ１３２）、実行リスト８０４内のジョブ情報８２０の数が０件の場合、図２０に示すメッセージからメッセージ５の「ＡＰジョブナシ」を選択し、ユーザ通知処理を行う（ステップＳ１３３）。

実行リスト８０４内のジョブ情報８２０の数が０件でない（１件以上である）場合、ステップＳ１４０へ処理を移す。

アプリケーション８００は、ＲＡＭ４００２から、ステップＳ１０１－４で記憶したＩＣカード４１０（記憶媒体）がかざされていた時間を取得し、かざされていた時間が一定時間以上か否かを判定する（ＩＣカードがかざされていた時間が所定時間であるか否かを判定する）（ステップＳ１４０）。

具体的には、ステップＳ１０１－４で計算した「ＩＣカードかざし時間」と、設定情報８０２に設定された全削除待機時間８３９とを比較する。比較の結果、「ＩＣカードかざし時間」の方が長ければ、一定時間以上かざされたと判断する（ステップＳ１４０でＹＥＳ）。また、比較の結果、全削除待機時間８３９の方が長ければ、一定時間以上かざされていないと判断する。

尚、判定基準となる全削除待機時間８３９の設定を変更できるので、通常印刷を行う場合でもＩＣカード４１０をかざす時間が長いユーザがいる環境や、全削除を早く行いたいユーザがいる環境など、ユーザの環境に応じて柔軟に対応することができる。

【 0 1 5 6 】

アプリケーション８００は、実行リスト８０４を参照して、カードＩＤに対応するユーザのジョブをマストレージ（記憶部）からすべて削除する（ステップＳ１４１）。

具体的には、実行リスト８０４からジョブ情報８２０を取り出す。次にジョブ情報８２０に保持されているファイル名８２２を取得する。次にファイル名８２２に一致するジョブ３１０を、ファイルシステム５０１内を検索して削除する。

以上の処理を、実行リスト８０４に格納されたジョブ数繰り返す。

【 0 1 5 7 】

尚、ステップＳ１３４、ステップＳ１３８については実施形態１と同様のため詳細な説明を割愛するが、ステップＳ１４０で、ＲＡＭ４００２から、ステップＳ１０１－４で記憶したＩＣカード４１０（記憶媒体）がかざされていた時間を取得し、かざされていた時間が一定時間以上でない判定された場合に（ステップＳ１４０でＮＯ）、ステップＳ１３４へ処理を移し、パネルにジョブ名８２３を表示（識別情報通知）させてＩＣカードがかざされるたびにジョブ名に対応するジョブをマストレージ（記憶部）から削除する。

【 0 1 5 8 】

以上の処理（ステップＳ１４０、ステップＳ１４１）により、ＩＣカードを通常より長

10

20

30

40

50

くかざす、という簡単な動作で、ユーザが簡単に全ジョブ削除することが可能になる。よって、ユーザが誤って大量にジョブを投入してしまったり、印刷の必要がなくなったジョブが大量に残っていたりした場合も、実施形態 1 のように、ひとつずつ削除する必要がなくなり、より使いやすい仕組みとなる。

また、IC カードをかざした時間が短ければ、実施形態 1 と同様の処理を行うことができるため、実施形態 1 と本実施形態（実施形態 2）を切り替えることができる。よってユーザは目的に応じて、全ジョブを削除するか、ジョブ毎に印刷 / 削除をするかの方法を決定し、IC カードをかざす動作（時間）に応じて、印刷装置上で削除方法を切り替えることが可能となる。

尚、本実施形態では図 3 3 の構成で説明を行ったが、図 3 4 のプリントサーバ 1 0 1 を備えるシステム（セキュアプリントシステム 1 b）においても実現可能である。

10

【 0 1 5 9 】

このように本発明の実施の形態によれば、カードをかざすことでジョブを削除する仕組みを提供することができる。また、カードを長くかざすことで、ユーザの全ジョブを削除する仕組みを提供することができる。

【 0 1 6 0 】

以上、添付図面を参照しながら本発明に係るセキュアプリントシステムおよびネットワークインタフェース装置等の好適な実施形態について説明したが、前述した実施の形態に限定されない。当業者であれば、特許請求の範囲に記載された技術的思想の範疇内において各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

20

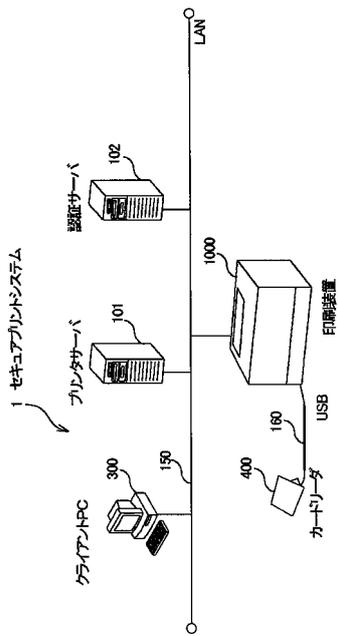
【符号の説明】

【 0 1 6 1 】

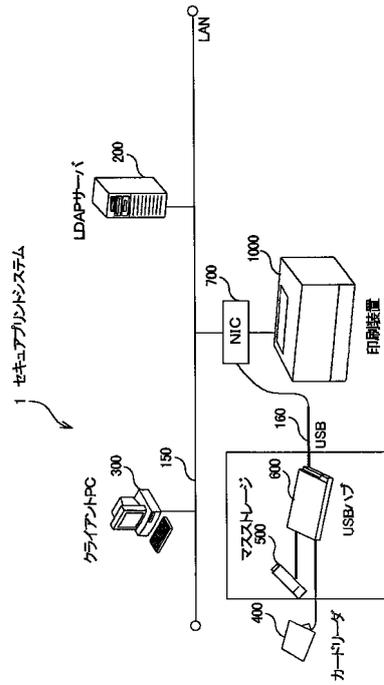
- 1 0 1 プリンタサーバ
- 1 0 2 認証サーバ
- 1 5 0 L A N
- 1 6 0 U S B ケーブル
- 2 0 0 L D A P サーバ
- 3 0 0 クライアント P C
- 4 0 0 カードリーダー
- 5 0 0 マスストレージ
- 6 0 0 U S B ハブ
- 7 0 0 N I C
- 1 0 0 0 印刷装置

30

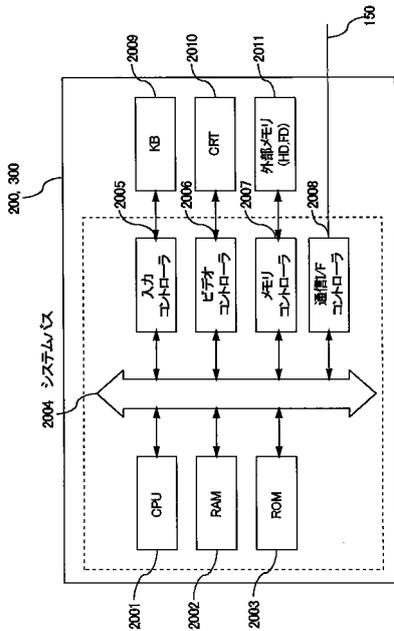
【 図 1 】



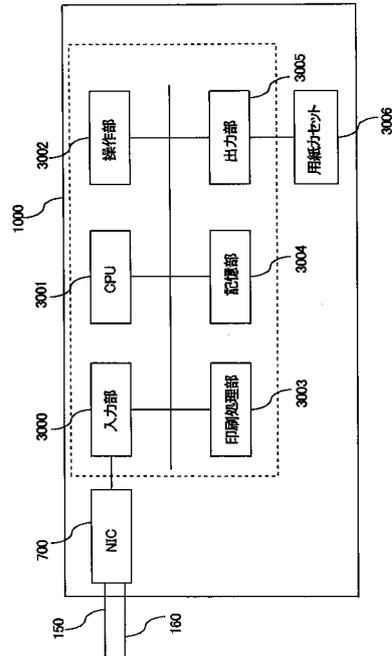
【 図 2 】



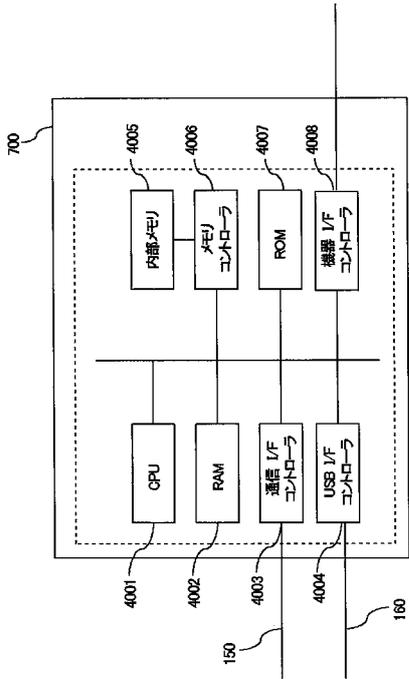
【 図 3 】



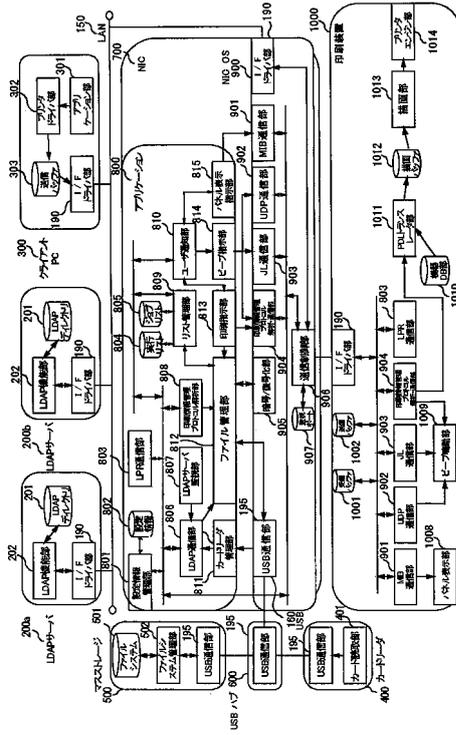
【 図 4 】



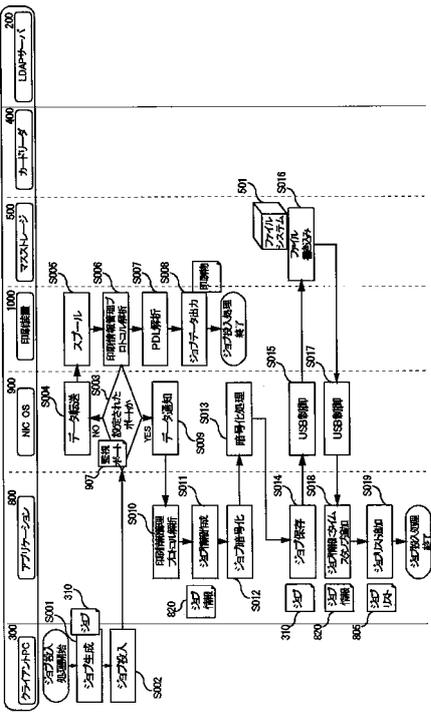
【図5】



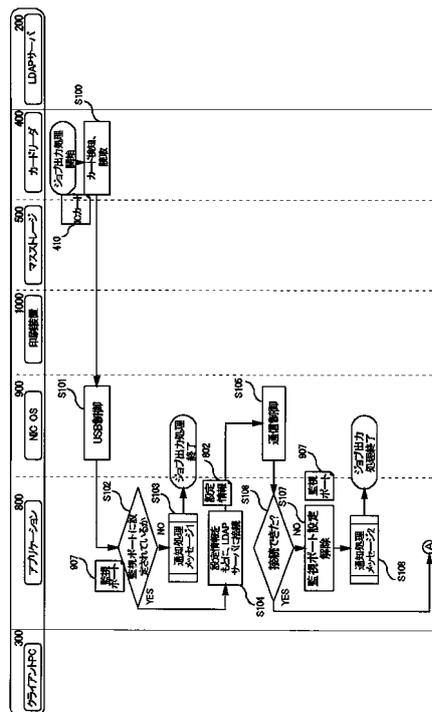
【図6】



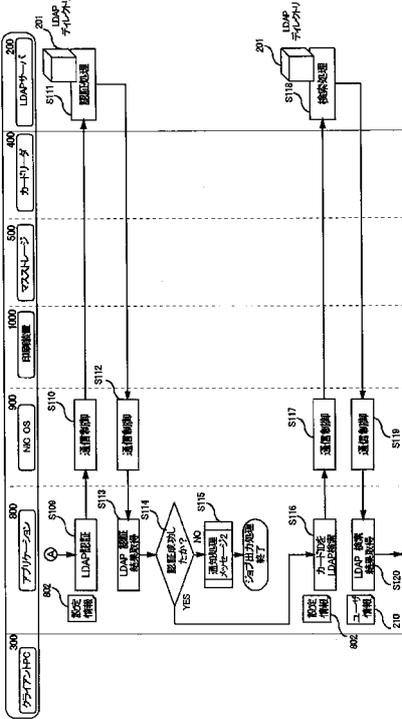
【図7】



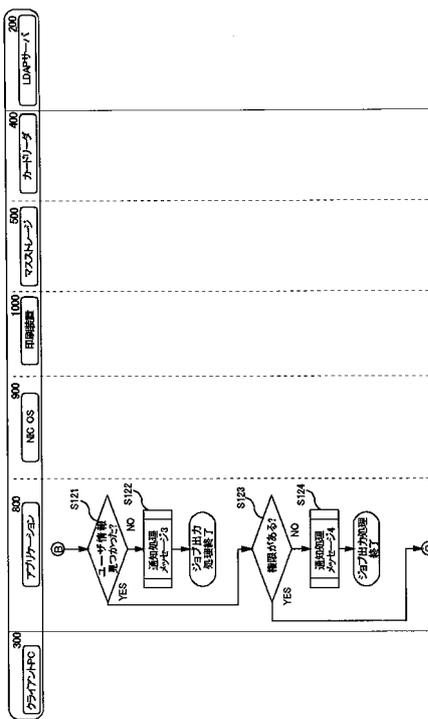
【図8】



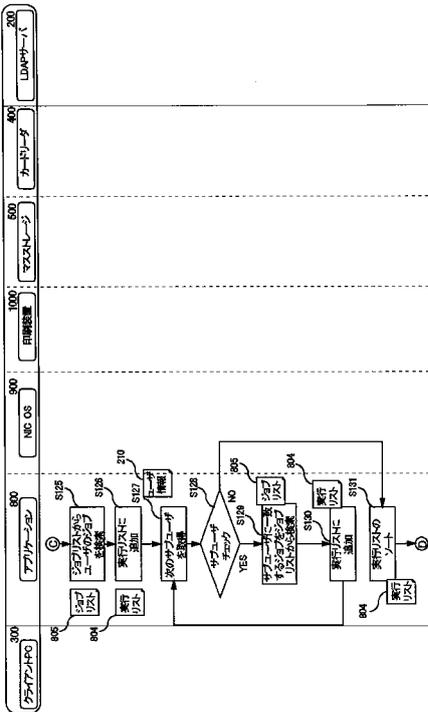
【 9 】



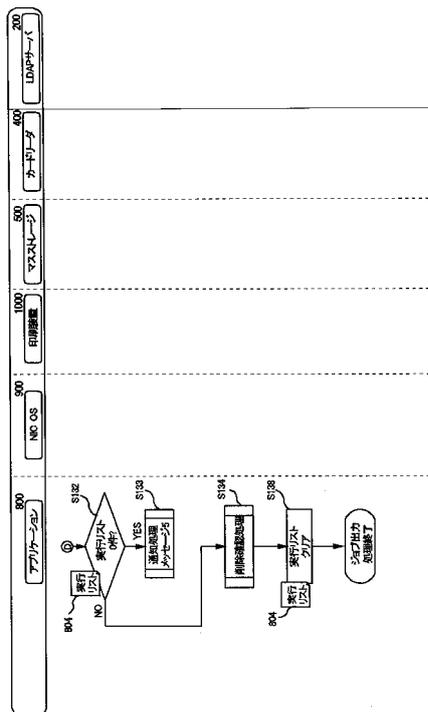
【 10 】



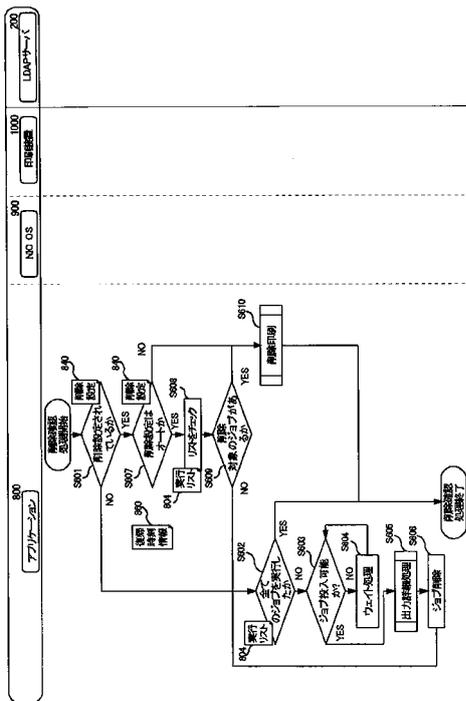
【 11 】



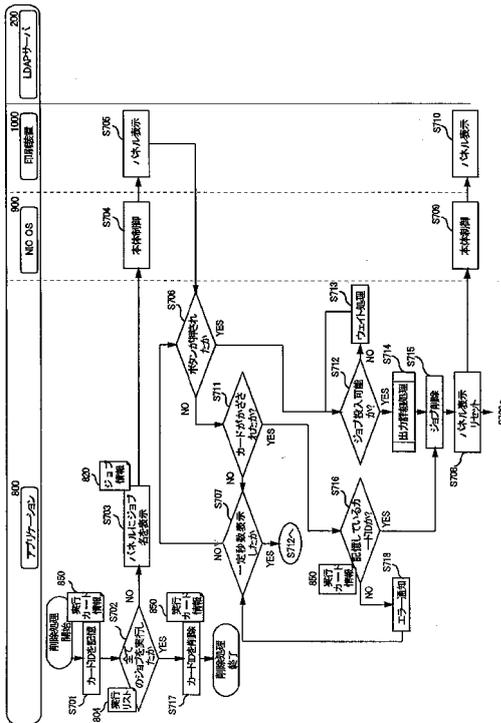
【 12 】



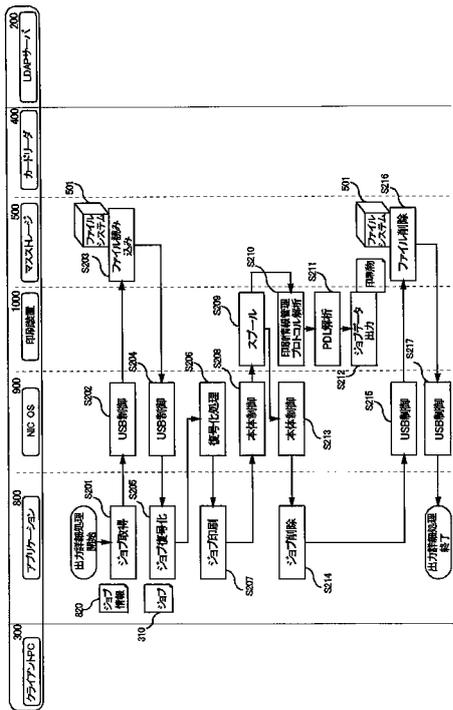
【 13 】



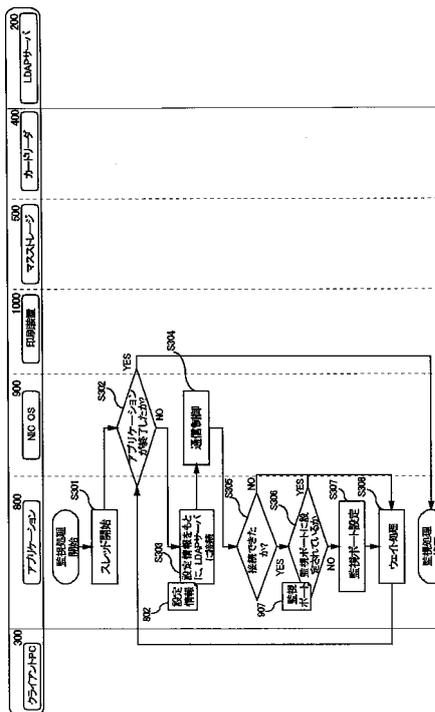
【 14 】



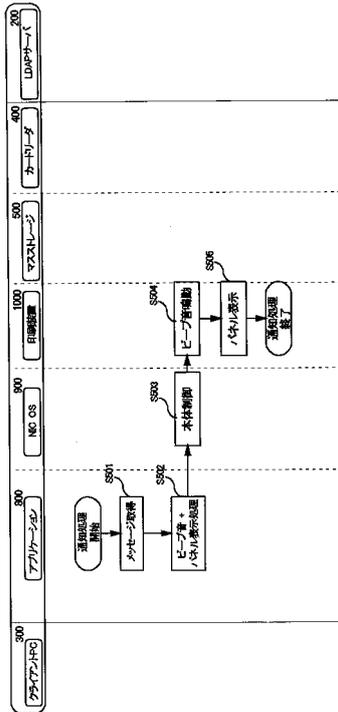
【 15 】



【 16 】



【図 17】



【図 18】

Suffix	dc=abcd, dc=local	831
識別コード	ou=meap	832
プライマリサーバ	192.168.0.1	833
プライマリポート	389	834
セカンダリサーバ	192.168.0.2	835
セカンダリポート	389	836
ユーザ	uid=abcd, ou=admin, dc=abcd, dc=local	837
パスワード	*****	838

【図 19】

監視ポート	515, 9100
-------	-----------

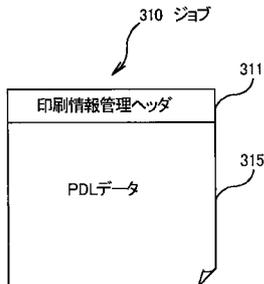
【図 20】

No	メッセージ
1	APIログイン成功
2	APサーバエラー
3	APユーザミクロク
4	APユーザエラー
5	APジョブナシ

【図 22】

ジョブオーナー	admin	311
ジョブ名	テスト.txt	312
		313

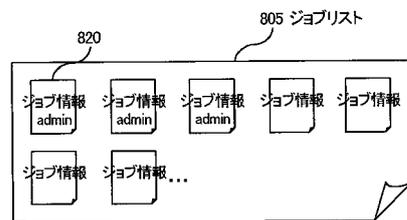
【図 21】



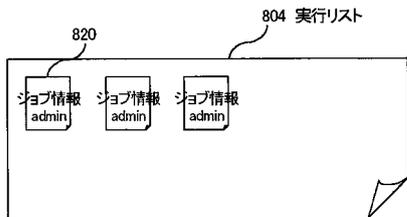
【図 23】

ユーザ名	admin	820
ファイル名	00012345.prn	821
ジョブ名	テスト.txt	822
タイムスタンプ	200804010940	823
		824

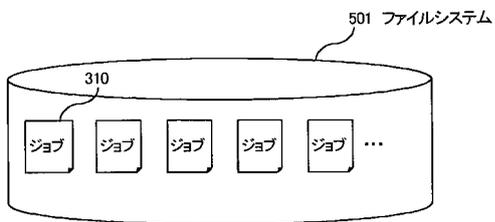
【図 24】



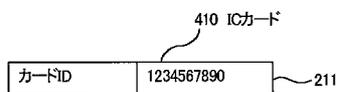
【図25】



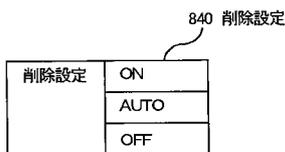
【図26】



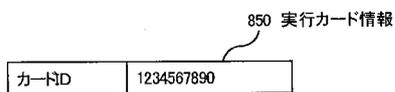
【図27】



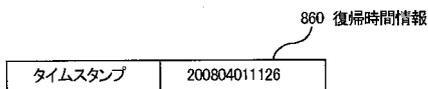
【図30】



【図31】



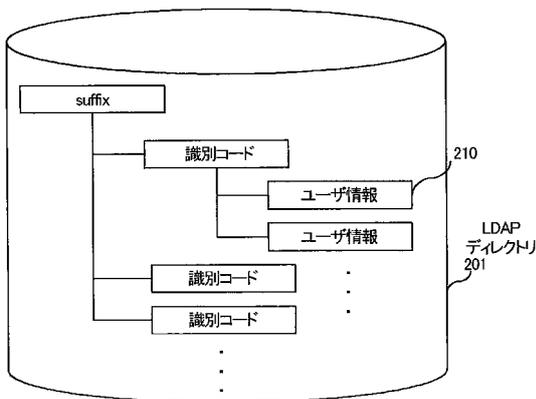
【図32】



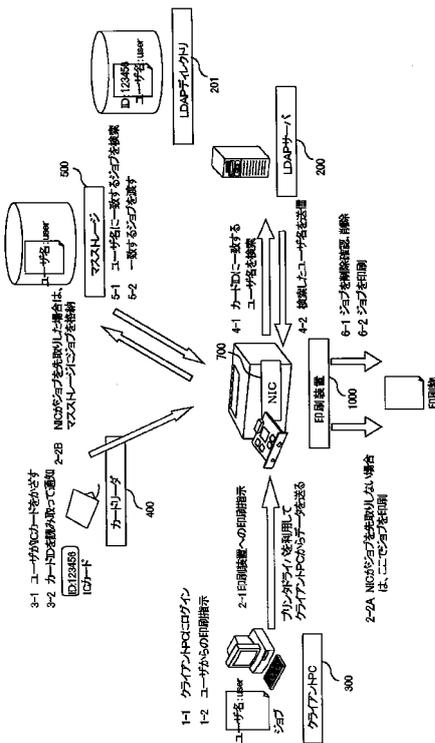
【図28】

カードID	1234567890
ユーザ名	admin
パスワード	xxxxxxxx
サブユーザ1	admin2
サブユーザ2	boss
サブユーザ3	
サブユーザ4	
利用制限	0000

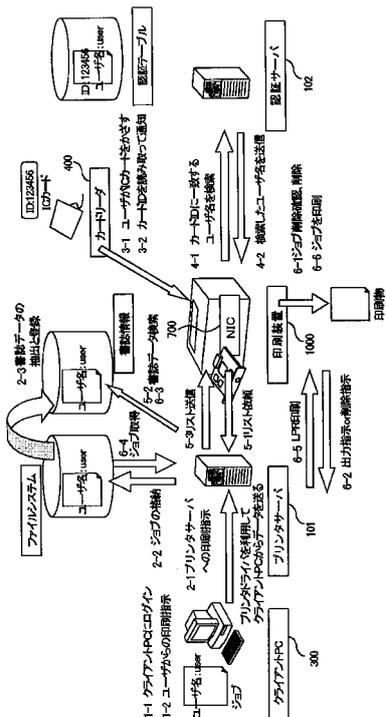
【図29】



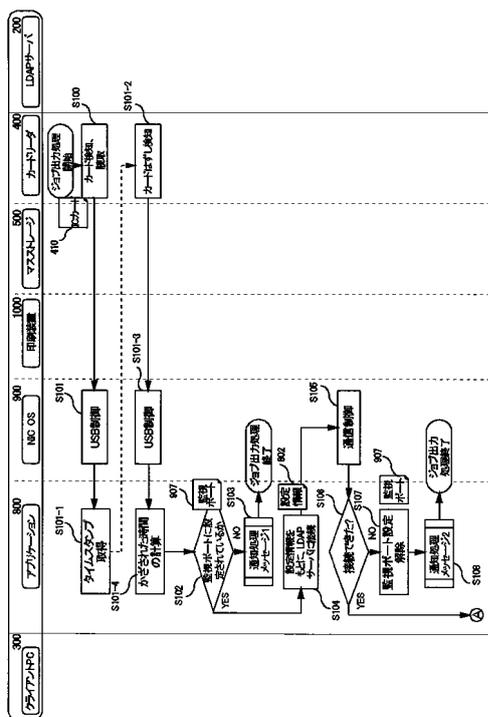
【図33】



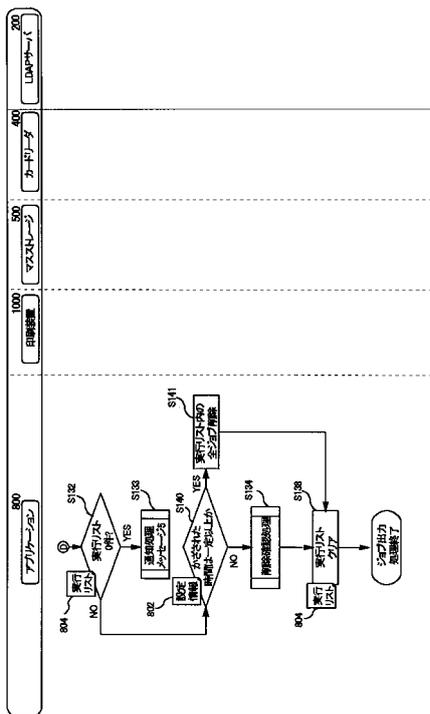
【 3 4 】



【 3 5 】



【 3 6 】



【 3 7 】

802 設定情報	
Suffix	dc=abcd, dc=local
識別コード	ou=meap
プライマリサーバ	192.168.0.1
プライマリポート	389
セカンダリサーバ	192.168.0.2
セカンダリポート	389
ユーザ	uid=abcd, ou=admin, dc=abcd, dc=local
パスワード	*****
全削除待機時間	3秒

フロントページの続き

- (56)参考文献 特開2003-182187(JP,A)
特開2005-335282(JP,A)
特開平06-095464(JP,A)
特開2003-196069(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F	3/12
B41J	29/38
H04N	1/21