

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4978571号
(P4978571)

(45) 発行日 平成24年7月18日(2012.7.18)

(24) 登録日 平成24年4月27日(2012.4.27)

(51) Int.Cl.	F I		
G06F 3/12 (2006.01)	G06F 3/12		K
G03G 21/04 (2006.01)	G03G 21/00	390	
B41J 29/38 (2006.01)	B41J 29/38		Z
B41J 29/00 (2006.01)	B41J 29/00		Z
H04N 1/00 (2006.01)	H04N 1/00	107A	
請求項の数 9 (全 20 頁) 最終頁に続く			

(21) 出願番号 特願2008-156925 (P2008-156925)
 (22) 出願日 平成20年6月16日(2008.6.16)
 (65) 公開番号 特開2009-301421 (P2009-301421A)
 (43) 公開日 平成21年12月24日(2009.12.24)
 審査請求日 平成22年12月17日(2010.12.17)

(73) 特許権者 303000372
 コニカミノルタビジネステクノロジーズ株式会社
 東京都千代田区丸の内一丁目6番1号
 (74) 代理人 100064746
 弁理士 深見 久郎
 (74) 代理人 100085132
 弁理士 森田 俊雄
 (74) 代理人 100083703
 弁理士 仲村 義平
 (74) 代理人 100096781
 弁理士 堀井 豊
 (74) 代理人 100098316
 弁理士 野田 久登

最終頁に続く

(54) 【発明の名称】 情報処理装置、情報処理システム、情報処理方法、情報処理プログラムおよび記録媒体

(57) 【特許請求の範囲】

【請求項1】

認証コードが付加された印刷データを受信する受信手段と、
 記憶手段と、
 前記受信手段で受信した印刷データを前記記憶手段に記憶するための制御手段とを備え

、
 前記制御手段は、
 前記受信手段により受信した印刷データが前記認証コードが付加された印刷データであるか否かを判別する判別手段と、

前記判別手段により、前記認証コードが付加された印刷データが受信されたと判別された場合には、前記認証コードに対応付けて前記記憶手段の一定の記憶領域を確保する記憶領域確保手段と、

前記記憶手段の記憶領域に対応付けられている認証コードと前記受信手段により受信された印刷データに付加された認証コードとを比較する認証コード比較手段と、

前記認証コード比較手段の比較結果に基づいて、認証コードが一致した場合には、受信した印刷データに含まれる送信元を示す送信元情報と前記記憶手段の記憶領域に記憶されている、一致した認証コードに対応する印刷データに含まれる送信元情報とを比較する送信元情報比較手段と、

前記送信元情報比較手段の比較結果に基づいて、送信元情報が一致した場合には、当該一致した認証コードに対応して設けられた前記記憶手段の記憶領域に前記受信手段により

受信された印刷データを記憶する保存手段とを含み、

前記記憶領域確保手段は、前記送信元情報比較手段の比較結果に基づいて、前記送信元情報が不一致の場合には、前記送信元情報を前記認証コードに関連付けて、前記記憶手段の別の記憶領域を確保し、

前記保存手段は、前記送信元情報比較手段の比較結果に基づいて、前記送信元情報が不一致の場合には、前記記憶手段の前記別の記憶領域に前記受信手段により受信された印刷データを記憶する、情報処理装置。

【請求項 2】

前記記憶領域確保手段は、別の認証コードが付加された印刷データを受信した場合には、前記別の認証コードに対応付けて前記記憶手段の一定の記憶領域を確保する、請求項 1 記載の情報処理装置。

10

【請求項 3】

前記送信元情報は、ユーザ名、前記印刷データの送信先のアドレスを示す IP アドレス、コンピュータ名の少なくとも 1 つに相当する、請求項 1 記載の情報処理装置。

【請求項 4】

前記記憶手段に記憶された認証コードが付加された印刷データに対するアクセス処理の入力指示を受け付ける操作入力受付手段と、

前記操作入力受付手段の入力指示に従って前記認証コードが付加された印刷データに対するアクセス処理を実行する印刷制御手段とを備え、

前記印刷制御手段は、

20

前記認証コードが付加された印刷データに対するアクセス処理の入力指示があった場合に、認証コードの入力を受け付ける認証コード入力受付手段と、

前記認証コード入力受付手段により入力された認証コードと、印刷処理の入力指示された印刷データに付加された認証コードとが一致するか否かを判断する認証手段と、

前記認証手段における認証が成功した場合に、前記記憶手段の認証が成功した前記認証コードに対応付けられて確保された記憶領域が複数存在するか否かを判断する判断手段と、

前記判断手段において、前記認証コードに対応付けられて確保された記憶領域が複数存在する場合には、送信元情報の入力を受け付ける送信元入力受付手段と、

前記送信元入力受付手段により入力された送信元情報と、前記認証コードに対応付けられて確保された前記複数の記憶領域にそれぞれ記憶される印刷データに含まれる送信元情報とが一致する記憶領域を検索する送信元情報検索手段と、

30

前記送信元情報検索手段により検索された一致した記憶領域に記憶された印刷データに対して所定の処理を実行する実行手段とを含む、請求項 1 記載の情報処理装置。

【請求項 5】

前記所定の処理は、前記記憶領域に記憶された印刷データに対する印刷処理および / または削除処理に相当する、請求項 4 記載の情報処理装置。

【請求項 6】

認証コードを付加した印刷データを送信する端末と、

前記ネットワークを介して前記端末と接続され、前記端末から送信された前記認証コードが付加された印刷データを受信する情報処理装置とを備え、

40

前記情報処理装置は、

前記認証コードが付加された印刷データを受信する受信手段と、

記憶手段と、

前記受信手段で受信した印刷データを前記記憶手段に記憶するための制御手段とを備え、

、

前記制御手段は、

前記受信手段により受信した印刷データが前記認証コードが付加された印刷データであるか否かを判別する判別手段と、

前記判別手段により、前記認証コードが付加された印刷データが受信されたと判別され

50

た場合には、前記認証コードに対応付けて前記記憶手段の一定の記憶領域を確保する記憶領域確保手段と、

前記記憶手段の記憶領域に対応付けられている認証コードと前記受信手段により受信された印刷データに付加された認証コードとを比較する認証コード比較手段と、

前記認証コード比較手段の比較結果に基づいて、認証コードが一致した場合には、受信した印刷データに含まれる送信元を示す送信元情報と前記記憶手段の記憶領域に記憶されている、一致した認証コードに対応する印刷データに含まれる送信元情報とを比較する送信元情報比較手段と、

前記送信元情報比較手段の比較結果に基づいて、送信元情報が一致した場合には、当該一致した認証コードに対応して設けられた前記記憶手段の記憶領域に前記受信手段により受信された印刷データを記憶する保存手段とを有し、

10

前記記憶領域確保手段は、前記送信元情報が不一致の場合には、前記送信元情報を前記認証コードに関連付けて、前記記憶手段の別の記憶領域を確保し、

前記保存手段は、前記送信元情報比較手段の比較結果に基づいて、前記送信元情報が不一致の場合には、前記記憶手段の前記別の記憶領域に前記受信手段により受信された印刷データを記憶する、情報処理システム。

【請求項7】

認証コードが付加された印刷データを受信するステップと、

受信した印刷データを記憶手段に記憶するステップとを備え、

前記記憶手段に記憶するステップは、

20

受信した印刷データが前記認証コードが付加された印刷データであるか否かを判別するステップと、

前記認証コードが付加された印刷データが受信されたと判別された場合には、前記認証コードに対応付けて前記記憶手段の一定の記憶領域を確保するステップと、

前記記憶手段の記憶領域に対応付けられている認証コードと前記受信手段により受信された印刷データに付加された認証コードとを比較するステップと、

前記認証コードの比較結果に基づいて、認証コードが一致した場合には、受信した印刷データに含まれる送信元を示す送信元情報と前記記憶手段の記憶領域に記憶されている、一致した認証コードに対応する印刷データに含まれる送信元情報とを比較するステップと

30

、前記送信元情報の比較結果に基づいて、送信元情報が一致した場合には、当該一致した認証コードに対応して設けられた前記記憶手段の記憶領域に受信された印刷データを記憶するステップとを含み、

前記一定の記憶領域を確保するステップは、前記送信元情報の比較結果に基づいて、前記送信元情報が不一致の場合には、前記送信元情報を前記認証コードに関連付けて、前記記憶手段の別の記憶領域を確保し、

前記印刷データを記憶するステップは、前記送信元情報の比較結果に基づいて、前記送信元情報が不一致の場合には、前記記憶手段の前記別の記憶領域に受信された印刷データを記憶する、情報処理方法。

【請求項8】

40

記憶手段を備えたコンピュータに実行させるための情報処理プログラムであって、

前記認証コードが付加された印刷データを受信するステップと、

受信した印刷データを前記記憶手段に記憶するステップとを備え、

前記記憶手段に記憶するステップは、

受信した印刷データが前記認証コードが付加された印刷データであるか否かを判別するステップと、

前記認証コードが付加された印刷データが受信されたと判別された場合には、前記認証コードに対応付けて前記記憶手段の一定の記憶領域を確保するステップと、

前記記憶手段の記憶領域に対応付けられている認証コードと前記受信手段により受信された印刷データに付加された認証コードとを比較するステップと、

50

前記認証コードの比較結果に基づいて、認証コードが一致した場合には、受信した印刷データに含まれる送信元を示す送信元情報と前記記憶手段の記憶領域に記憶されている、一致した認証コードに対応する印刷データに含まれる送信元情報とを比較するステップと、

前記送信元情報の比較結果に基づいて、送信元情報が一致した場合には、当該一致した認証コードに対応して設けられた前記記憶手段の記憶領域に受信された印刷データを記憶するステップとを含み、

前記一定の記憶領域を確保するステップは、前記送信元情報の比較結果に基づいて、前記送信元情報が不一致の場合には、前記送信元情報を前記認証コードに関連付けて、前記記憶手段の別の記憶領域を確保し、

前記印刷データを記憶するステップは、前記送信元情報の比較結果に基づいて、前記送信元情報が不一致の場合には、前記記憶手段の前記別の記憶領域に受信された印刷データを記憶する、情報処理プログラム。

【請求項 9】

請求項 8 に記載の情報処理プログラムを記録した、記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、認証コードすなわち認証情報が付加されている印刷データを情報処理装置から出力する技術であって、特に印刷データを情報処理装置の記憶部に一旦記憶させ、印刷指示がなされた場合に情報処理装置の操作部を介した認証処理後に、記憶部に記憶されている印刷データを出力する技術に関する。

【背景技術】

【0002】

従来より、たとえば、端末装置等で作成された印刷データをプリンタ等の情報処理装置によりプリント出力し、配布資料を作成したりすることが広く行なわれている。

【0003】

プリンタは、一般的に複数のユーザで共有されている場合が多く、その排紙部には複数のユーザがそれぞれ作成し、印刷指示された印刷物がそのユーザが取りに来るまで残されることになる。

【0004】

ユーザが印刷指示した印刷物には極めて機密性が高いものがある。

したがって、そのような場合には、ユーザは印刷指示した後に、直ちにプリンタの所に行き、印刷物を他人に見られないように回収する必要がある。

【0005】

このような問題に対処するために機密性の高い文書（機密文書）を印刷する場合に、印刷物の取り忘れ、および第三者に閲覧あるいは印刷されることを防止するために機密文書の印刷データに対して認証コードを付加して、情報処理装置の記憶部へ保存し、情報処理装置の操作パネルを介して認証処理を実行した後、認証処理が成功した場合に当該ユーザの印刷指示を受けて印刷を実行する機能（いわゆるセキュアプリント）が知られている（特許文献 1）。

【0006】

当該セキュアプリントでは、管理者による認証コードに対する取決めがなく、ユーザがフレキシブルに認証コードを設定できる利便性がある。

【特許文献 1】特開 2007 - 251279 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、このようなセキュアプリントでは、簡易的に認証コードが設定され易く、これにより第三者と認証コードが重複する可能性がある。

10

20

30

40

50

【 0 0 0 8 】

したがって、認証コードが付加されている印刷データについて、第三者と認証コードが重複している場合には、機密文書であっても第三者に閲覧あるいは印刷されてしまう可能性があった。

【 0 0 0 9 】

本発明は、上記のような問題を解決するためになされたものであって、簡易な方式でセキュアプリントの機密性を向上させることが可能な情報処理装置、情報処理システム、情報処理方法、情報処理プログラムおよび記録媒体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】

【 0 0 1 0 】

本発明に係る情報処理装置は、認証コードが付加された印刷データを受信する受信手段と、記憶手段と、受信手段で受信した印刷データを記憶手段に記憶するための制御手段とを備える。制御手段は、受信手段により受信した印刷データが認証コードが付加された印刷データであるか否かを判別する判別手段と、判別手段により、認証コードが付加された印刷データが受信されたと判別された場合には、認証コードに対応付けて記憶手段の一定の記憶領域を確保する記憶領域確保手段と、記憶手段の記憶領域に対応付けられている認証コードと受信手段により受信された印刷データに付加された認証コードとを比較する認証コード比較手段と、認証コード比較手段の比較結果に基づいて、認証コードが一致した場合には、受信した印刷データに含まれる送信元を示す送信元情報と記憶手段の記憶領域に記憶されている、一致した認証コードに対応する印刷データに含まれる送信元情報とを比較する送信元情報比較手段と、送信元情報比較手段の比較結果に基づいて、送信元情報が一致した場合には、当該一致した認証コードに対応して設けられた記憶手段の記憶領域に受信手段により受信された印刷データを記憶する保存手段とを含む。記憶領域確保手段は、送信元情報比較手段の比較結果に基づいて、送信元情報が不一致の場合には、送信元情報を認証コードに関連付けて、記憶手段の別の記憶領域を確保する。保存手段は、送信元情報比較手段の比較結果に基づいて、送信元情報が不一致の場合には、記憶手段の別の記憶領域に受信手段により受信された印刷データを記憶する。

【 0 0 1 1 】

好ましくは、記憶領域確保手段は、別の認証コードが付加された印刷データを受信した場合には、別の認証コードに対応付けて記憶手段の一定の記憶領域を確保する。

【 0 0 1 2 】

好ましくは、送信元情報は、ユーザ名、印刷データの送信先のアドレスを示すIPアドレス、コンピュータ名の少なくとも1つに相当する。

【 0 0 1 3 】

好ましくは、記憶手段に記憶された認証コードが付加された印刷データに対するアクセス処理の入力指示を受け付ける操作入力受付手段と、操作入力受付手段の入力指示に従って認証コードが付加された印刷データに対するアクセス処理を実行する印刷制御手段とを備える。印刷制御手段は、認証コードが付加された印刷データに対するアクセス処理の入力指示があった場合に、認証コードの入力を受け付ける認証コード入力受付手段と、認証コード入力受付手段により入力された認証コードと、印刷処理の入力指示された印刷データに付加された認証コードとが一致するか否かを判断する認証手段と、認証手段における認証が成功した場合に、記憶手段の認証が成功した認証コードに対応付けられて確保された記憶領域が複数存在するか否かを判断する判断手段と、判断手段において、認証コードに対応付けられて確保された記憶領域が複数存在する場合には、送信元情報の入力を受け付ける送信元入力受付手段と、送信元入力受付手段により入力された送信元情報と、認証コードに対応付けられて確保された複数の記憶領域にそれぞれ記憶される印刷データに含まれる送信元情報とが一致する記憶領域を検索する送信元情報検索手段と、送信元情報検索手段により検索された一致した記憶領域に記憶された印刷データに対して所定の処理を実行する実行手段とを含む。

【 0 0 1 4 】

特に、所定の処理は、記憶領域に記憶された印刷データに対する印刷処理および/または削除処理に相当する。

【0015】

本発明に係る情報処理システムは、認証コードを付加した印刷データを送信する端末と、ネットワークを介して端末と接続され、端末から送信された認証コードが付加された印刷データを受信する情報処理装置とを備える。情報処理装置は、認証コードが付加された印刷データを受信する受信手段と、記憶手段と、受信手段で受信した印刷データを記憶手段に記憶するための制御手段とを備える。制御手段は、受信手段により受信した印刷データが認証コードが付加された印刷データであるか否かを判別する判別手段と、判別手段により、認証コードが付加された印刷データが受信されたと判別された場合には、認証コード
10
に対応付けて記憶手段の一定の記憶領域を確保する記憶領域確保手段と、記憶手段の記憶領域に対応付けられている認証コードと受信手段により受信された印刷データに付加された認証コードとを比較する認証コード比較手段と、認証コード比較手段の比較結果に基づいて、認証コードが一致した場合には、受信した印刷データに含まれる送信元を示す送信元情報と記憶手段の記憶領域に記憶されている、一致した認証コードに対応する印刷データに含まれる送信元情報とを比較する送信元情報比較手段と、送信元情報比較手段の比較結果に基づいて、送信元情報が一致した場合には、当該一致した認証コードに対応して設けられた記憶手段の記憶領域に受信手段により受信された印刷データを記憶する保存手段とを有する。記憶領域確保手段は、送信元情報が不一致の場合には、送信元情報を認証
20
コードに関連付けて、記憶手段の別の記憶領域を確保する。保存手段は、送信元情報比較手段の比較結果に基づいて、送信元情報が不一致の場合には、記憶手段の別の記憶領域に受信手段により受信された印刷データを記憶する。

【0016】

本発明に係る情報処理方法は、認証コードが付加された印刷データを受信するステップと、受信した印刷データを記憶手段に記憶するステップとを備える。記憶手段に記憶するステップは、受信した印刷データが認証コードが付加された印刷データであるか否かを判別するステップと、認証コードが付加された印刷データが受信されたと判別された場合には、認証コードに対応付けて記憶手段の一定の記憶領域を確保するステップと、記憶手段の記憶領域に対応付けられている認証コードと受信手段により受信された印刷データに付加された認証コードとを比較するステップと、認証コードの比較結果に基づいて、認証
30
コードが一致した場合には、受信した印刷データに含まれる送信元を示す送信元情報と記憶手段の記憶領域に記憶されている、一致した認証コードに対応する印刷データに含まれる送信元情報とを比較するステップと、送信元情報の比較結果に基づいて、送信元情報が一致した場合には、当該一致した認証コードに対応して設けられた記憶手段の記憶領域に受信された印刷データを記憶するステップとを含む。一定の記憶領域を確保するステップは、送信元情報の比較結果に基づいて、送信元情報が不一致の場合には、送信元情報を認証コードに関連付けて、記憶手段の別の記憶領域を確保する。印刷データを記憶するステップは、送信元情報の比較結果に基づいて、送信元情報が不一致の場合には、記憶手段の別の記憶領域に受信された印刷データを記憶する。

【0017】

本発明に係る情報処理プログラムは、記憶手段を備えたコンピュータに実行させるための情報処理プログラムであって、認証コードが付加された印刷データを受信するステップと、受信した印刷データを記憶手段に記憶するステップとを備える。記憶手段に記憶するステップは、受信した印刷データが認証コードが付加された印刷データであるか否かを判別するステップと、認証コードが付加された印刷データが受信されたと判別された場合には、認証コードに対応付けて記憶手段の一定の記憶領域を確保するステップと、記憶手段の記憶領域に対応付けられている認証コードと受信手段により受信された印刷データに付加された認証コードとを比較するステップと、認証コードの比較結果に基づいて、認証
40
コードが一致した場合には、受信した印刷データに含まれる送信元を示す送信元情報と記憶手段の記憶領域に記憶されている、一致した認証コードに対応する印刷データに含まれる
50

送信元情報とを比較するステップと、送信元情報の比較結果に基づいて、送信元情報が一致した場合には、当該一致した認証コードに対応して設けられた記憶手段の記憶領域に受信された印刷データを記憶するステップとを含む。一定の記憶領域を確保するステップは、送信元情報の比較結果に基づいて、送信元情報が不一致の場合には、送信元情報を認証コードに関連付けて、記憶手段の別の記憶領域を確保する。印刷データを記憶するステップは、送信元情報の比較結果に基づいて、送信元情報が不一致の場合には、記憶手段の別の記憶領域に受信された印刷データを記憶する。

【0018】

本発明に係る記録媒体は、上記情報処理プログラムを記録する。

【発明の効果】

10

【0019】

本発明に係る情報処理装置、情報処理システムおよび情報処理方法は、認証コードが付加された印刷データを受信し、受信した印刷データを記憶手段に記憶する。受信した印刷データが認証コードが付加された印刷データであるか否かを判別し、認証コードが付加された印刷データが受信されたと判別された場合には、認証コードに対応付けて記憶手段の一定の記憶領域を確保する。記憶手段の記憶領域に対応付けられている認証コードと受信された印刷データに付加された認証コードとを比較し、認証コードの比較結果に基づいて、認証コードが一致した場合には、受信した印刷データに含まれる送信元を示す送信元情報と記憶手段の記憶領域に記憶されている、一致した認証コードに対応する印刷データに含まれる送信元情報とを比較する。送信元情報の比較結果に基づいて、送信元情報が一致した場合には、当該一致した認証コードに対応して設けられた記憶手段の記憶領域に受信された印刷データを記憶する。送信元情報の比較結果に基づいて、送信元情報が不一致の場合には、送信元情報を認証コードに関連付けて、記憶手段の別の記憶領域を確保する。送信元情報の比較結果に基づいて、送信元情報が不一致の場合には、記憶手段の別の記憶領域に受信された印刷データを記憶する。

20

【0020】

当該方式により、認証コードに対応付けられて記憶領域が確保されて印刷データが記憶され、認証コードが同一である印刷データを受信した場合に、送信元を確認し、一致すれば、確保されている記憶領域に記憶し、送信元が別であれば、送信元情報をさらに関連付けて別の記憶領域に確保される。

30

【0021】

したがって、認証コードが第三者と重複した場合であっても、送信元を確認して、送信元情報に関連付けて別の記憶領域に印刷データが記憶されるため、印刷の際に第三者に自由に閲覧あるいは印刷されてしまう問題を防止し、簡易な方式でセキュアプリントの機密性を向上させることができる。

【発明を実施するための最良の形態】

【0022】

以下、図面を参照しつつ本発明の実施の形態について説明する。以下の説明において同一の部品および構成要素には同一の符号を付してある。それらの名称および機能も同一であるものとする。

40

【0023】

図1は、本発明の実施の形態に従う情報処理システムについて説明する概略図である。

図1を参照して、本発明の実施の形態に従う情報処理システムは、情報処理装置の一種であるMFP(Multi Function Peripheral)100と、MFP100とネットワーク800で結合されたパーソナルコンピュータ(単にパソコンとも称する)200, 250, 300とを備える。

【0024】

MFP100は、ユーザ端末であるパソコン200, 250, 300から受信した印刷データを印刷する印刷機能やコピー機能、ファクシミリ機能等を備えている。

【0025】

50

また、MFP100は、スキャナで読込んだ画像データをもとに指定されたフォーマットのデータを作成し、指定されたユーザ端末に対して送信するファイル転送機能等も備えている。

【0026】

さらに、MFP100は、後述するがユーザ端末であるパソコン200、250、300から受信した印刷データを記憶部に一旦記憶し、MFP100のタッチパネルやテンキー等の操作部を介して、印刷指示がなされた場合に操作部を介した認証処理後に、記憶部に記憶してある印刷データの印刷処理を行なうセキュアプリント機能もさらに備えている。

【0027】

なお、本実施の形態においてはMFP100としての複合機を図示しているが、単機能のプリンタであってもよい。

【0028】

ユーザ端末であるパソコン200、250、300は、MFP100に対して印刷データを送信し、印刷処理を行なわせる。なお、本例においては、一例として3つのパソコン200、250、300を示しているが、3つに限られず、いくつであってもよい。

【0029】

ネットワーク800は、LAN(Local Area Network)であってもよいし、公衆回線等を用いたWAN(Wide Area Network)であってもよい。なお、MFP100が行なうネットワーク800を介する通信は有線であってもよいし、無線であってもよい。

【0030】

図2は、本発明の実施の形態に従うMFP100の機能ブロック図である。

図2を参照して、本発明の実施の形態に従うMFP100は、紙媒体等の資料を電子データに変換する画像読取部103と、たとえばハードディスク(HDD)で構成される記憶部102と、印刷処理を実行する印刷部106と、ネットワーク800を介して外部機器であるパソコン200、250、300との間でデータの送受信を実行するためのネットワークインターフェイス107と、入力画像データに対して補正、加工、編集を行ったり、印刷部106等への出力画像データに対して補正、解像度変換等を行なう画像処理部104と、ディスプレイ画面、タッチパネルやテンキー等が設けられた操作パネル部105と、MFP100全体を制御する制御部101とを備える。なお、各部は、内部バス111で接続されており、各部との間でデータの授受を実行することが可能である。

【0031】

図3は、本発明の実施の形態に従うパソコン200の概略構成を説明するブロック図である。

【0032】

図3を参照して、本発明の実施の形態に従うパソコン200は、オペレーティングシステム(OS: Operating System)を含む各種プログラムを実行するCPU(Central Processing Unit)201と、CPU201のプログラム部分の実行に必要なデータを一時的に記憶するメモリ部213と、CPU201で実行されるプログラムを不揮発的に記憶するハードディスク部(HDD: Hard Disk Drive)211とを含む。

【0033】

また、ハードディスク部211には、MFP100に対して印刷データを送信するためのソフトウェアプログラムであるプリンタドライバが記憶されており、当該プリンタドライバをCPU201が読み込むことにより、後述する機能が実現される。このようなプログラムは、FDドライブ217あるいはCD-ROM(Compact Disc-Read Only Memory)ドライブ215によってそれぞれフレキシブルディスク217aまたはCD-ROM215aなどから読取られる。

【0034】

CPU201は、キーボードやマウス等からなる入力部209を介してユーザからの指示を受け取るとともに、プログラム実行によって生成される画面出力をディスプレイ部2

10

20

30

40

50

05へ出力する。

【0035】

また、CPU201は、LANカード等からなる通信インターフェイス部207を介してLANやWANに接続されたMFP100に対して印刷データを送信する。また、上述の各部は、内部バス203を介して相互にデータを授受する。なお、パソコン250, 300についても同様の構成であるのでその説明は繰り返さない。

【0036】

図4は、本発明の実施の形態に従うプリンタドライバの機能ブロックを説明する図である。

【0037】

図4を参照して、プリンタドライバ400は、CPU201に読み込まれることにより大きく分けて2つの機能を実現することが可能である。

【0038】

具体的には、各種の印刷設定を実行するための各種印刷設定処理部410と、それら各種の印刷設定に基づいて画像生成を行なうための画像生成部405とに分けられる。

【0039】

各種印刷設定処理部410は、セキュアプリントの設定をするためのセキュアプリント設定処理部420を含む。また、画像生成部405は、認証コード付加処理部415を含む。

【0040】

セキュアプリント設定処理部420で設定した認証コード等に基づいて、画像生成部405の認証コード付加処理部415は、認証コードを画像データに付加した印刷データを生成する。

【0041】

そして、CPU201は、生成された印刷データを通信インターフェイス部207を介してMFP100に対して送信する。

【0042】

図5は、本発明の実施の形態に従うパソコン200のディスプレイ部205に表示される各種印刷設定処理部410の機能に基づく印刷設定画面を説明する図である。

【0043】

図5を参照して、本発明の実施の形態に従う印刷設定画面500において、ここでは、「基本設定画面」が一例として示されている。ユーザは、一例として、「原稿の向き」、「原稿サイズ」、「用紙サイズ」、「出力方法」および「部数」等を入力部209に含まれる図示しないマウス等のポインティングデバイス等を用いて設定することが可能である。

【0044】

また、ここでは、「出力方法」の設定として、「通常印刷」、「セキュリティ印刷」、「ボックス保存」、「確認印刷」を選択可能な場合が示されており、本例においては、出力方法として「セキュリティ印刷」にカーソル505が指定されている場合が示されている。

【0045】

この「セキュリティ印刷」にカーソル505が指定されている状態において、「OK」ボタン510を押下することによりセキュアプリントを実行するための認証コードを付加した印刷データを送信することが可能である。なお、「Cancel」ボタン515を押下することにより、印刷設定画面500を終了することが可能である。

【0046】

図6は、図5の印刷画面500において、セキュリティ印刷を指定した場合のセキュアプリント設定処理部420の機能に基づく認証コード設定画面520を説明する図である。

【0047】

10

20

30

40

50

図6を参照して、本発明の実施の形態に従う認証コード設定画面520において、セキュリティ印刷を実行する場合の認証コードを入力する画面が示されている。

【0048】

具体的には、ユーザのID (Identification) およびパスワード (Password) をそれぞれ入力欄530, 535が設けられている。

【0049】

ユーザは、キーボードやマウス等からなる入力部209を用いて任意に自己のIDおよびパスワードを入力することが可能である。

【0050】

そして、「OK」ボタン540を押下することにより、認証コードを設定することが可能である。一方、「Cancel」ボタン515を押下することにより、印刷設定画面500に戻るものとする。

10

【0051】

そして、認証コードが設定された場合には、上述したように認証コード付加処理部415により、設定された認証コードを画像データに付加した印刷データが生成される。

【0052】

本例においては、IDの入力欄530に「1234」が入力され、パスワードの入力欄535に「abcd」が入力されているものとする。なお、パスワードの入力欄535に表示される文字としては、機密性を高めるために「*」の記号が表示されている。

【0053】

20

図7は、印刷データ600を説明する図である。

図7を参照して、ここでは、一例として各種の必要なデータがいわゆるPGL (Printer Job Language) 形式のファイルデータとして示されている。具体的には、画像データの前にPGL形式のコマンドで記述された認証コードを含む印刷ジョブデータが示されている。

【0054】

具体的には、印刷ジョブデータとして、一例として、ジョブID (JOBID) や、送信時刻 (SEND_DATETIME) や、ジョブ名 (JOBNAME)、ユーザ名 (USERNAME)、コンピュータ名 (COMPUTERNAME)、IP (Internet Protocol) アドレス (IP_ADDRESS) とともに、セキュアプリントを実行するために必要な認証コード等が記述されている。

30

【0055】

この点で、セキュアプリントを実行する指示コマンドである「SECUREPRINT」=「ON」が記述されており、認証コードであるIDおよびパスワードである「SECUREPRINT_ID」=「1234」、「SECUREPRINT_PASSWORD」=「abcd」が記述されている。

【0056】

この「SECUREPRINT」=「ON」の指示コマンドが設定されることにより、MFP100において受信された印刷データに対してセキュアプリントが実行される。

【0057】

図8は、本発明の実施の形態に従うセキュアプリントの印刷データを受信した場合のMFP100の制御部101の処理を説明するフロー図である。

40

【0058】

図8を参照して、制御部101は、ネットワークインターフェース107を介して印刷ジョブを受信したかどうかを判断する (ステップS1)。本例において印刷ジョブとは印刷の際の所定のコマンドが記述された印刷ジョブデータを含む印刷データを指すものとする。印刷ジョブを受信するまで待機し、印刷ジョブを受信した場合には、次のステップに進む。

【0059】

ステップS1において、印刷ジョブを受信した場合には、次に印刷ジョブがセキュアプリントジョブであるかどうかを判断する (ステップS2)。具体的には、印刷データの印刷ジョブデータにセキュアプリントの実行指示であるコマンドが含まれているかどうかを

50

判断する。すなわち、「SECUREPRINT」=「ON」か否かを判断する。「OFF」である場合には、セキュアプリントジョブでは無いとして、印刷部106において印刷処理を実行する(ステップS9)。そして、終了する(エンド)。

【0060】

ステップS2において、印刷ジョブがセキュアプリントジョブであると判断される場合、具体的には、「SECUREPRINT」=「ON」である場合には、次のステップS3に進む。

【0061】

そして、次に、認証コードが同一の記憶領域が存在するかどうかを判断する(ステップS3)。

【0062】

具体的には、印刷データの印刷ジョブデータに含まれる認証コードと、後述する記憶テーブルを参照して、当該認証コードに対応付けられた記憶領域が記憶部102に存在するか否かを判断する。本例においては、認証コードであるIDおよびパスワードに記憶部102の一定の記憶領域が対応付けられて印刷ジョブが格納されるものとする。

【0063】

図9は、記憶テーブルを説明する図である。

図9を参照して、ここでは、記憶部102の記憶領域のアドレスA0~A2と、認証コード(IDおよびパスワード)との対応付けが成されている場合が示されている。ここでは、一例として、設定されたIDとパスワードとを組み合わせたデータ列が示されている。データ列のうち上4桁がIDに対応し、下4桁がパスワードに対応している。

【0064】

再び図8を参照して、ステップS3において、記憶テーブルを参照して、認証コードが同一の記憶領域が存在しないと判断された場合には、ステップS7に進む。

【0065】

そして、ステップS7において、新規に認証コードに対応付けられた記憶領域を確保する(ステップS7)。なお、その際に、記憶テーブルに確保された記憶領域のアドレスと認証コードとの対応付けが成された情報が格納されるものとする。

【0066】

そして、次に、当該確保された記憶領域に印刷ジョブを保存する(ステップS7)。

そして、保存された印刷ジョブの印刷指示があるまで待機する(ステップS8)。そして、終了する(エンド)。

【0067】

一方、ステップS3において、認証コードが同一の記憶領域がある場合には、次に記憶領域に保存された印刷ジョブは同一の送信元ユーザであるかどうかを判断する(ステップS4)。

【0068】

具体的には、受信した印刷データの印刷ジョブデータに含まれる送信元を示す情報と、認証コードが同一の記憶領域に格納されている印刷データの印刷ジョブデータに含まれる送信元を示す情報とを比較する。本例においては、一例として、印刷ジョブデータに含まれる送信元情報として、IPアドレスを用いるものとする。受信した印刷データの印刷ジョブデータに含まれるIPアドレスと、認証コードが同一の記憶領域に格納されている印刷データの印刷ジョブデータに含まれるIPアドレスとを比較し、一致した場合には、同一の送信元ユーザであると判断する。一方、不一致であれば異なる送信元ユーザであると判断する。

【0069】

ステップS4において、記憶領域に保存された印刷ジョブが同一の送信元ユーザであると判断された場合には、次に、既に予め設けられている認証コードに対応する記憶領域に印刷ジョブを保存する(ステップS6)。そして、ステップS8に進む。

【0070】

一方、ステップS4において、記憶領域に保存された印刷ジョブが同一の送信元ユーザ

10

20

30

40

50

ではない場合すなわち異なる送信元ユーザであると判断された場合には、新規に認証コードに送信元ユーザ情報を関連付けた記憶領域を確保する（ステップ S 5）。本例においては、認証コードにさらに IP アドレスを関連付けた新規の記憶領域を確保する。

【 0 0 7 1 】

なお、その際に、記憶テーブルに確保された記憶領域のアドレスと認証コードおよび IP アドレスとの対応付けが成された情報が格納されるものとする。

【 0 0 7 2 】

そして、次に、新規の記憶領域に印刷ジョブを保存する（ステップ S 5）。そして、ステップ S 8 に進む。

【 0 0 7 3 】

なお、本例においては、ステップ S 4 において、送信元ユーザであるか否かの判断に、IP アドレスを用いた例について説明したが、特にこれに限られず、例えば、ユーザ名（USERNAME）、あるいは、コンピュータ名（COMPUTERNAME）等を用いることも可能である。また、これらを組み合わせて判断することも可能である。

【 0 0 7 4 】

また、本例においては、認証コードにさらに IP アドレスを関連付けた新規の記憶領域を確保する場合について説明したが、特に IP アドレスに限られず、別の送信元ユーザであることが識別可能であれば、どんなものを用いても良い。

【 0 0 7 5 】

再び、図 9 を参照して、具体例として、ここでは、「1 2 3 4 a b c d」、「1 2 3 4 a b c d」、「2 3 4 5 e f g h」の認証コードにそれぞれ対応付けられた記憶領域のアドレス A 0 ~ A 2 が示されている。

【 0 0 7 6 】

例えば、まず、最初に、認証コード = 「1 2 3 4 a b c d」が付加されている印刷ジョブを受信した場合には、図 8 のフロー図に従って、アドレス A 0 の記憶領域が確保されて、当該印刷ジョブが保存される。

【 0 0 7 7 】

そして、次に、認証コード = 「1 2 3 4 a b c d」が付加されている印刷ジョブを受信した場合には、図 8 のフロー図に従って、認証コードが同一の記憶領域があると判定される。そして、ステップ S 4 において、同一の送信元ユーザか否かの判断がされる。仮に、同一の送信元ユーザでない、すなわち別の送信元ユーザからの印刷ジョブの受信であると判断された場合には、ステップ S 5 に進み、認証コード = 「1 2 3 4 a b c d」にさらに、例えば IP アドレス = 「1 0 . 1 2 8 . 3 2 . 1 0 0」を関連付けたアドレス A 1 の新規の記憶領域が確保されて、当該印刷ジョブが保存される。

【 0 0 7 8 】

また、次に、認証コード = 「2 3 4 5 e f g h」が付加されている印刷ジョブを受信した場合には、図 8 のフロー図に従って、認証コードが同一の記憶領域がないと判定される。そして、ステップ S 7 において、アドレス A 2 の新規の記憶領域が確保されて、当該印刷ジョブが保存される。

【 0 0 7 9 】

なお、上記においては、認証コードに含まれる ID およびパスワードに対応付けて記憶領域に記憶させる方式について説明したが、ID のみあるいはパスワードのみに基づいて同様の方式に従って対応付けることも可能であるし、送信元ユーザを認証可能な他の情報等と組み合わせて用いることも可能である。

【 0 0 8 0 】

図 1 0 は、本発明の実施の形態に従うセキュアプリントの印刷ジョブに対する印刷指示を実行する場合のフロー図である。

【 0 0 8 1 】

図 1 0 を参照して、まず、ステップ S 1 0 において、セキュアプリントの印刷指示があったかどうかを判断する。具体的には、図示しないが、制御部 1 0 1 は、操作パネル部 1

10

20

30

40

50

05のタッチパネル等の操作に従って、セキュアプリントの印刷指示が実行されたかどうかを判断するものとする。

【0082】

ステップS10において、セキュアプリントの印刷指示があった場合には、次に、印刷ジョブ認証コードの入力画面をポップアップする(ステップS11)。

【0083】

図11は、印刷ジョブ認証コードの入力画面700を説明する図である。

図11を参照して、ここでは、図示しない操作パネル部105に含まれるディスプレイ画面に印刷ジョブ認証コード入力画面700が表示されている場合が示されている。

【0084】

そして、操作パネル部105に含まれるタッチパネルあるいはテンキー等を利用して、印刷ジョブ認証コードとして、IDおよびパスワード(Password)を入力可能な入力欄705,710が示されている。

【0085】

そして、「OK」ボタン715を押下することにより、入力されたIDおよびパスワード(Password)の認証が実行される。「Cancel」ボタン720を押下することにより、セキュアプリントの印刷指示が終了するものとする。

【0086】

再び図10を参照して、印刷ジョブ認証コードの入力があったかどうかを判断する(ステップS12)。具体的には、印刷ジョブ認証コードの入力欄に入力が有り、「OK」ボタン715の押下があった場合は、次に、認証OKかどうかを判断する(ステップS13)。一方、「Cancel」ボタン720の押下があった場合には、ステップS12において、入力がなかったとして終了する(エンド)。

【0087】

認証が「OK」であるか否かは、印刷ジョブ認証コード入力画面700における入力欄705,710に入力されたIDおよびパスワードに基づいて、認証処理を行い該当する印刷ジョブが有るか否かを判断する。

【0088】

具体的には、図9で説明した記憶テーブルの認証コードが一致するか否かに基づいて、認証がOKか否かを判断する。入力されたIDおよびパスワードのデータ列と一致するデータ列が認証コードとして記憶テーブルに格納されている場合には認証OKとなり、一致するデータ列が認証コードとして記憶テーブルに格納されていない場合には認証失敗となる。

【0089】

ステップS13において、認証が「OK」である場合には、次に、印刷ジョブ認証コードに対応する送信元ユーザが異なる印刷ジョブが複数あるかどうかを判断する(ステップS14)。

【0090】

具体的には、入力されたIDおよびパスワードのデータ列と一致するデータ列が認証コードとして図9で説明した記憶テーブルに複数格納されているか否かを判断する。複数格納されている場合には、印刷ジョブ認証コードに対応する送信元ユーザが異なる印刷ジョブが複数あると判断される。

【0091】

ステップS14において、印刷ジョブ認証コードに対応する送信元ユーザが異なる印刷ジョブが複数あると判断された場合には、送信元ユーザ確認画面をポップアップする(ステップS15)。

【0092】

図12は、送信元ユーザ確認画面をポップアップした場合を説明する図である。

図12を参照して、ここでは、図示しない操作パネル部105に含まれるディスプレイ画面に送信元ユーザ確認画面730が示されている。

10

20

30

40

50

【 0 0 9 3 】

そして、操作パネル部 1 0 5 に含まれるタッチパネルあるいはテンキー等を利用して、送信元のユーザを確認するための IP アドレスを入力可能な入力欄 7 3 5 が示されている。

【 0 0 9 4 】

ユーザは、操作パネル部 1 0 5 を用いてタッチパネルあるいはテンキー等を利用して、入力欄 7 3 5 に IP アドレスを入力して「OK」ボタン 7 4 0 を押下することにより、送信元ユーザの認証を実行することができる。

【 0 0 9 5 】

再び図 1 0 を参照して、次に、送信元ユーザ確認が OK かどうかを判断する（ステップ S 1 6 ）。

【 0 0 9 6 】

送信元ユーザ確認が OK かどうかは、送信元ユーザ確認画面 7 3 0 における入力欄 7 3 5 に入力された IP アドレスに基づいて、認証処理を行い該当する印刷ジョブが有るか否かを判断する。

【 0 0 9 7 】

具体的には、図 9 で説明した記憶テーブルの認証コードが一致するアドレスに記憶されている印刷ジョブに含まれている印刷ジョブデータの IP アドレスが一致するか否かに基づいて、確認が OK か否かを判断する。確認が OK である場合には、次に、ステップ S 1 7 に進む。

【 0 0 9 8 】

一方、一致しない場合には、確認が失敗となり、セキュアプリントの印刷指示が終了するものとする。（エンド）。なお、送信元ユーザ確認画面 7 3 0 において、「Cancel」ボタン 7 4 5 の押下があった場合にも、確認が失敗となり、セキュアプリントの印刷指示が終了するものとする（エンド）。

【 0 0 9 9 】

次に、ステップ S 1 6 において送信元ユーザ確認が「OK」である場合には送信元ユーザの印刷ジョブのみについてセキュアプリントジョブボックス画面へ表示する（ステップ S 1 7 ）。

【 0 1 0 0 】

具体的には、図 9 で説明した記憶テーブルに基づいて、送信元ユーザ確認が OK であった印刷ジョブを読み出して、印刷ジョブに含まれている印刷ジョブデータに従って、印刷ジョブのリストを作成する。

【 0 1 0 1 】

図 1 3 は、セキュアプリントジョブボックス画面 7 5 0 を説明する図である。

図 1 3 を参照して、ここでは、セキュアプリントジョブボックス画面 7 5 0 が示されており、送信元ユーザの印刷ジョブリスト 7 6 0 が示されている。当該印刷ジョブリストは、印刷ジョブデータに含まれている送信時刻（SEND_DATETIME）や、ジョブ名（JOBNAME）およびユーザ名（USERNAME）等に基づいてリスト表示されている場合が示されている。なお、印刷ジョブデータに含まれている他の情報を表示することも当然に可能である。

【 0 1 0 2 】

そして、当該画面においては、印刷を実行指示する印刷ボタン 7 6 2、印刷を実行指示した後、記憶部に格納されている印刷ジョブを削除指示する印刷後削除ボタン 7 6 4、印刷ジョブを削除する削除ボタン 7 6 5 が示されており、当該ボタンを押下することにより所定の処理が実行される。

【 0 1 0 3 】

再び、図 1 0 を参照して、ステップ S 1 4 において、印刷ジョブ認証コードに対応する送信元ユーザが異なる印刷ジョブが複数存在しない、すなわち 1 つだけと判断された場合には、記憶領域に格納されている対応する印刷ジョブを読み出して、上述したのと同様のセキュアプリントジョブボックス画面 7 5 0 をポップアップする（ステップ S 2 1 ）。そ

10

20

30

40

50

して、ステップ S 1 8 に進む。

【 0 1 0 4 】

次に、セキュアプリントジョブボックス画面の表示後、次に、印刷ジョブに対する指示（印刷、印刷後削除、削除）があるまで待機する（ステップ S 1 8 ）。

【 0 1 0 5 】

そして、次に、印刷ジョブに対する指示（印刷、印刷後削除、削除）があるかどうかを判断する（ステップ S 1 9 ）。指示が無い場合には、ステップ S 1 8 に戻る。

【 0 1 0 6 】

ステップ S 1 9 において、印刷ジョブに対する指示がある場合には、印刷ジョブに対する指示（印刷、印刷後削除、削除）を実行する（ステップ S 2 0 ）。そして、終了する（

10

エンド）。

【 0 1 0 7 】

印刷ジョブに対する指示に関して、具体的には、印刷ボタン 7 6 2 を押下することにより、指定されたセキュアプリントジョブボックスに表示されている印刷ジョブに含まれる画像データの印刷処理を実行する。

【 0 1 0 8 】

また、印刷後削除ボタン 7 6 4 を押下することにより、指定されたセキュアプリントジョブボックスに表示されている印刷ジョブに含まれる画像データの印刷処理後、記憶部 1 0 2 に格納されている印刷ジョブを削除する処理を実行する。

【 0 1 0 9 】

20

また、削除ボタン 7 6 5 を押下することにより、記憶部 1 0 2 に記憶されている指定されたセキュアプリントジョブボックスに表示されている印刷ジョブを削除する処理を実行する。

【 0 1 1 0 】

当該方式により、本発明の実施の形態に従うセキュアプリントにおいては、ユーザがフレキシブルに認証コードを設定した場合に、第三者と認証コードが重なった場合には、記憶領域に送信元ユーザを識別可能な情報をさらに関連付けて印刷ジョブを格納する。

【 0 1 1 1 】

そして、認証コードが第三者と重なる場合には、同一の送信元ユーザであるかの認証を行なって、認証が成功した場合に、印刷ジョブに対するアクセスが可能となるため、機密性の高い文書について、簡易な方式でさらに機密性を高めることが可能であり、セキュアプリントにおいて第三者に自由に閲覧および印刷されるという問題を防止することができる。

30

【 0 1 1 2 】

なお、上記においては、送信元ユーザ確認画面 7 3 0 において、入力欄 7 3 5 に入力された IP アドレスに基づいて、認証処理を行い該当する印刷ジョブが有るか否かを判断する場合について説明したが、特に IP アドレスに限られず、印刷ジョブデータに含まれている第三者と識別可能なデータであればどんなものを用いても良い。例えば、ユーザ名を入力して、ユーザ名に基づいて、認証処理を行うようにすることも可能である。

【 0 1 1 3 】

40

なお、本発明にかかる情報処理装置は M F P に限定されず、プリンタやファクシミリ装置等であってもよい。なお、情報処理装置を制御するコントローラについて、コンピュータを機能させて、上述のフローで説明したような制御を実行させるプログラムを提供することもできる。このようなプログラムは、コンピュータに付属するフレキシブルディスク、C D - R O M (Compact Disk-Read Only Memory)、R O M (Read Only Memory)、R A M (Random Access Memory) およびメモ리카ードなどのコンピュータ読取り可能な記録媒体にて記録させて、プログラム製品として提供することもできる。あるいは、コンピュータに内蔵するハードディスクなどの記録媒体にて記録させて、プログラムを提供することもできる。また、ネットワークを介したダウンロードによって、プログラムを提供することもできる。

50

【 0 1 1 4 】

なお、本発明にかかるプログラムは、コンピュータのオペレーションシステム（OS）の一部として提供されるプログラムモジュールのうち、必要なモジュールを所定の配列で所定のタイミングで呼出して処理を実行させるものであってよい。その場合、プログラム自体には上記モジュールが含まれずOSと協働して処理が実行される。このようなモジュールを含まないプログラムも、本発明にかかるプログラムに含まれ得る。

【 0 1 1 5 】

また、本発明にかかるプログラムは他のプログラムの一部に組込まれて提供されるものであってよい。その場合にも、プログラム自体には上記他のプログラムに含まれるモジュールが含まれず、他のプログラムと協働して処理が実行される。このような他のプログラムに組込まれたプログラムも、本発明にかかるプログラムに含まれ得る。

10

【 0 1 1 6 】

提供されるプログラム製品は、ハードディスクなどのプログラム格納部にインストールされて実行される。なお、プログラム製品は、プログラム自体と、プログラムが記録された記録媒体とを含む。

【 0 1 1 7 】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

20

【 図面の簡単な説明 】

【 0 1 1 8 】

【 図 1 】 本発明の実施の形態に従う情報処理システムについて説明する概略図である。

【 図 2 】 本発明の実施の形態に従うMFP 100の機能ブロック図である。

【 図 3 】 本発明の実施の形態に従うパソコン 200の概略構成を説明するブロック図である。

【 図 4 】 本発明の実施の形態に従うプリンタドライバの機能ブロックを説明する図である。

【 図 5 】 本発明の実施の形態に従うパソコン 200のディスプレイ部 205に表示される各種印刷設定処理部 410の機能に基づく印刷設定画面を説明する図である。

30

【 図 6 】 図 5 の印刷画面 500において、セキュリティ印刷を指定した場合のセキュアプリント設定処理部 420の機能に基づく認証コード設定画面 520を説明する図である。

【 図 7 】 印刷データ 600を説明する図である。

【 図 8 】 本発明の実施の形態に従うセキュアプリントの印刷データを受信した場合のMFP 100の制御部 101の処理を説明するフロー図である。

【 図 9 】 記憶テーブルを説明する図である。

【 図 10 】 本発明の実施の形態に従うセキュアプリントの印刷ジョブに対する印刷指示を実行する場合のフロー図である。

【 図 11 】 印刷ジョブ認証コードの入力画面 700を説明する図である。

【 図 12 】 送信元ユーザ確認画面をポップアップした場合を説明する図である。

40

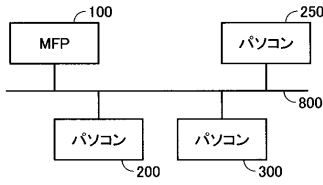
【 図 13 】 セキュアプリントジョブボックス画面 750を説明する図である。

【 符号の説明 】

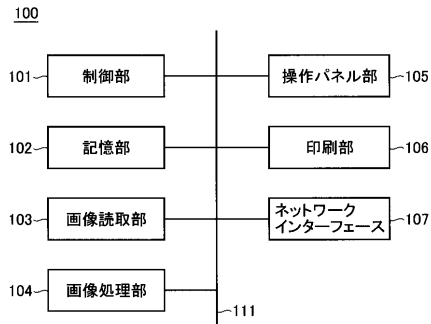
【 0 1 1 9 】

100 MFP、101 制御部、102 記憶部、103 画像読取部、104 画像処理部、105 操作パネル部、106 印刷部、107 ネットワークインターフェース、200、250、300 パソコン、201 CPU、205 ディスプレイ部、207 通信インターフェース部、209 入力部、211 HDD、213 メモリ部、215 CD-ROMドライブ、217 FDDドライブ。

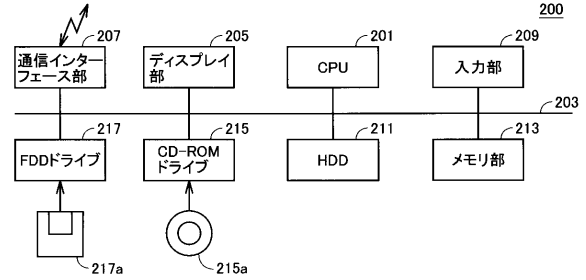
【図1】



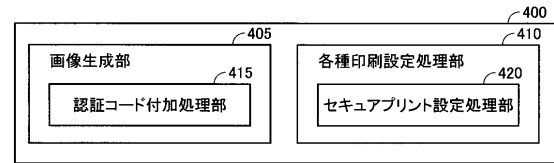
【図2】



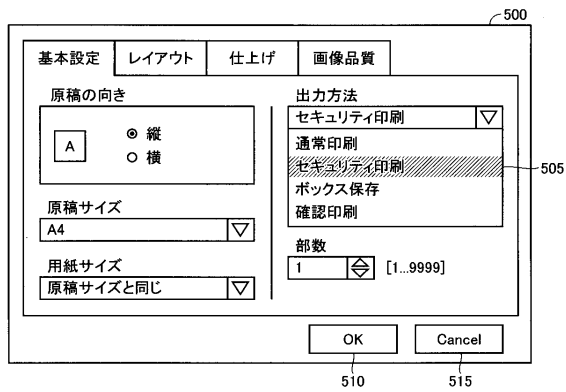
【図3】



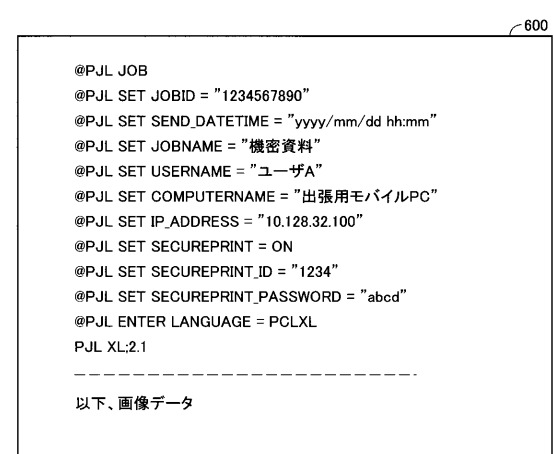
【図4】



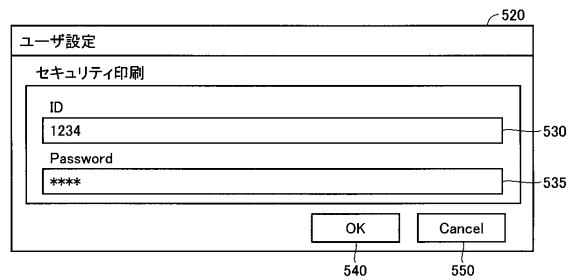
【図5】



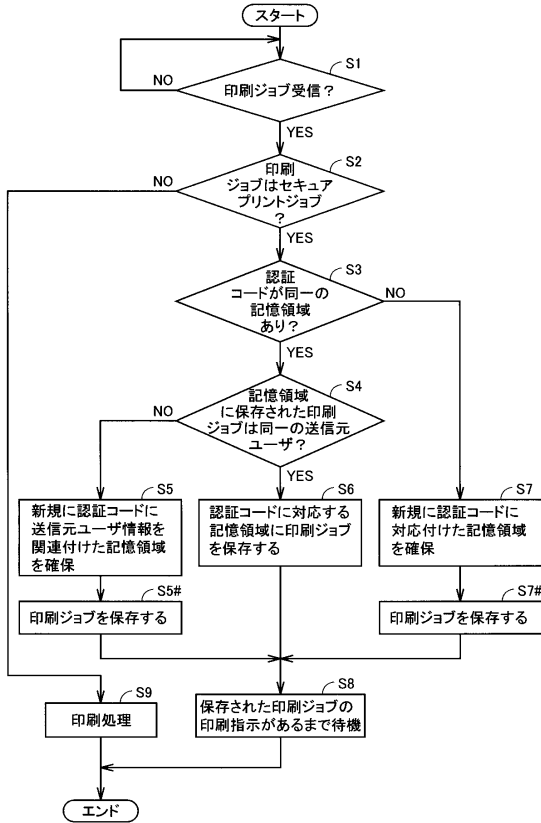
【図7】



【図6】



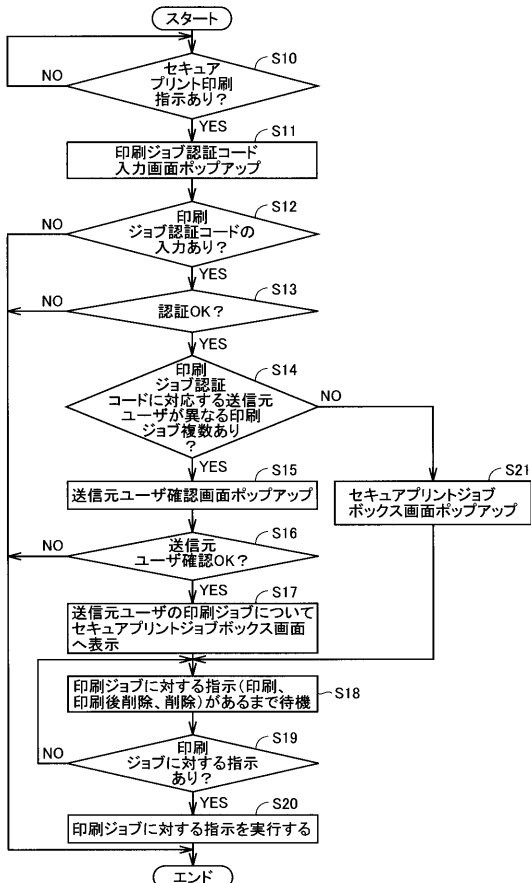
【図8】



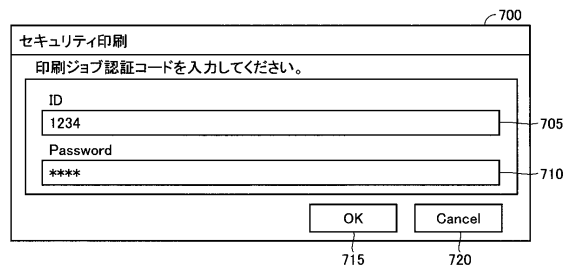
【図9】

アドレス	認証コード	IPアドレス
A0	1234abcd	—
A1	1234abcd	10.128.32.100
A2	2345efgh	—

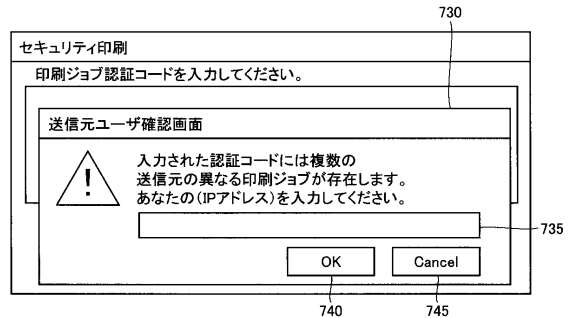
【図10】



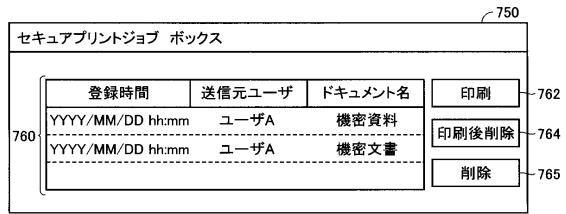
【図11】



【図12】



【図13】



フロントページの続き

(51) Int.Cl. F I
H 0 4 N 1/21 (2006.01) H 0 4 N 1/21

(74)代理人 100109162

弁理士 酒井 将行

(74)代理人 100111246

弁理士 荒川 伸夫

(72)発明者 京尾 俊作

東京都千代田区丸の内一丁目6番1号 コニカミノルタビジネステクノロジーズ株式会社内

審査官 内田 正和

(56)参考文献 特開平09-248951(JP,A)
特開2001-312388(JP,A)
特開2005-115485(JP,A)
特開2003-271342(JP,A)
特開2005-128733(JP,A)

(58)調査した分野(Int.Cl., DB名)

G 0 6 F 3 / 1 2
B 4 1 J 2 9 / 0 0
B 4 1 J 2 9 / 3 8
G 0 3 G 2 1 / 0 4
H 0 4 N 1 / 0 0
H 0 4 N 1 / 2 1