(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年12 月14 日 (14.12.2006)

PCT

(10) 国際公開番号
WO 2006/132178 A1

(51) 国際特許分類:
G06F 3/12 (2006.01) *B41J 29/38* (2006.01)

(21) 国際出願番号: PCT/JP2006/311217

(22) 国際出願日: 2006 年6 月5 日 (05.06.2006)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2005-167086 2005 年6 月7 日 (07.06.2005) JP

(71) 出願人 (米国を除く全ての指定国について): 大日本印刷株式会社 (DAI NIPPON PRINTING CO., LTD.) [JP/JP]; 〒1628001 東京都新宿区市谷加賀町一丁目１番１号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 深野 宣哉 (FUKANO, Nobuya) [JP/JP]; 〒1628001 東京都新宿区市谷加賀町一丁目１番１号 大日本印刷株式会社内 Tokyo (JP). 矢野 義博 (YANO, Yoshihiro) [JP/JP]; 〒1628001 東京都新宿区市谷加賀町一丁目１番１号 大日本印刷株式会社内 Tokyo (JP). 近田 恭之 (CHIKADA, Takayuki) [JP/JP]; 〒1628001 東京都新宿区市谷加賀町一丁目１番１号 大日本印刷株式会社内 Tokyo (JP).

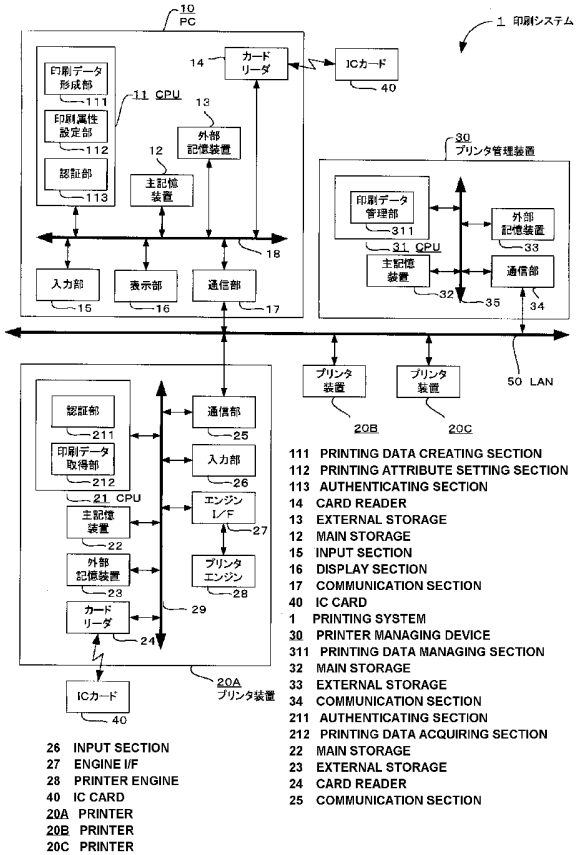
(74) 代理人: 鎌田 久男 (KAMATA, Hisao); 〒1710022 東京都豊島区南池袋２－４１－８ 池袋睦ビル３階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU,

[続葉有]

(54) Title: PRINTING SYSTEM AND PROGRAM

(54) 発明の名称: 印刷システム及びプログラム



(57) **Abstract:** A printing system and a program ensuring an improved security. A printing system (1) comprising printers (20A, 20B, 20C) for printing according to printing data further comprises a printer managing device (30) having a printing data managing section (311) for limiting the printing data supplied to the printers (20A, 20B, 20C) to printing data having a security level matching the security level based on the installation environment of the printer (20A) and a communication section (34) for providing the limited printing data to the printer (20A).

(57) 要約: セキュリティ性を向上する印刷システム及びプログラムを提供する。印刷データに基づいて印刷を行うプリンタ装置２０Ａ，２０Ｂ，２０Ｃを備える印刷システム１において、プリンタ装置２０Ａ，２０Ｂ，２０Ｃに提供する印刷データを、プリンタ装置２０Ａの設置環境に基づくセキュリティレベルに見合ったセキュリティレベルを有する印刷データに制限する印刷データ管理部３１１と、印刷データ管理部３１１によって制限された印刷データをプリンタ装置２０Ａに提供する通信部３４とを有するプリンタ管理装置３０を備える。

WO 2006/132178 A1

SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

印刷システム及びプログラム

技術分野

[0001] 本発明は、印刷データに基づいて印刷を行う印刷手段を備える印刷システム、及び、印刷データに基づいて印刷を行う印刷手段に提供する印刷データを管理するコンピュータに実行させるプログラムである。

背景技術

[0002] プリンタ装置による印刷内容の機密性を保持するため、受信した印刷情報中の出力制限データに従って生成されるイメージデータの出力先を制御することにより、ホストから転送された印刷情報の出力開始指示を印刷装置側での正規のユーザのみの指示に委ねることができる印刷装置がある(例えば、特許文献1参照。)。

特許文献1:特開平7－152520号公報

発明の開示

発明が解決しようとする課題

[0003] しかし、印刷装置が設置されている環境は、様々であって、各印刷装置の設置環境に応じてセキュリティレベルなどのセキュリティ属性は、大きく異なっている。例えば、常時ビデオカメラで監視されている場所や、複数の社員など複数の監視者がいる場所などに設置されている印刷装置のセキュリティレベルは高いが、会議室などの監視者がほとんどいない場所、外部の者が頻繁に出入りする場所などに設置されている印刷装置のセキュリティレベルは低い。また、各ユーザが印刷する印刷データのセキュリティレベルについても、極秘、部外秘、社外秘、試し刷り用などの秘匿性のないデータなど、各印刷データによって大きく異なっている。

従って、セキュリティレベルの低い印刷装置は、不正利用される可能性、不正利用に気が付かない可能性が高く、機密性の高い印刷データをこの印刷装置へ送信し、印刷した場合には、印刷データの漏洩や改竄などの可能性が高く、セキュリティに欠けるという問題があった。

[0004] 本発明の課題は、セキュリティ性を向上する印刷システム及びプログラムを提供す

ることである。

課題を解決するための手段

[0005] 本発明は、以下のような解決手段により、前記課題を解決する。なお、理解を容易にするために、本発明の実施例に対応する符号を付して説明するが、これに限定されるものではない。第1の発明は、印刷データに基づいて印刷を行う印刷手段(28)を備える印刷システムにおいて、前記印刷手段に提供する印刷データを、前記印刷手段の設置環境に基づくセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限する印刷データ制限手段(311、213)を備えること、を特徴とする印刷システム(1、1－2、1－3)を提供する。

[0006] 第2の発明は、第1の発明の印刷システムにおいて、前記印刷データ制限手段は、前記印刷手段に提供する印刷データを前記印刷手段の時間帯別のセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限すること、を特徴とする印刷システム(1、1－2、1－3)を提供する。

[0007] 第3の発明は、第1の発明の印刷システムにおいて、前記印刷データ制限手段は、印刷データのセキュリティ属性と、前記印刷手段のセキュリティ属性とに基づいて、前記印刷手段への前記印刷データの提供の可否を判定する判定手段(311, S420、213, S520)を有すること、を特徴とする印刷システム(1、1－2、1－3)を提供する。

[0008] 第4の発明は、第1の発明の印刷システムにおいて、印刷指示を行うユーザの印刷指示権限を認証するための認証情報を入力する認証情報入力手段(24)と、前記認証情報入力手段によって入力される認証情報に基づいてユーザの印刷指示権限を認証する認証手段(211)とを備え、前記印刷データ制限手段は、前記認証手段によって認証された印刷指示権限の範囲内で前記印刷手段に提供する印刷データを制限すること、を特徴とする印刷システム(1、1－3)を提供する。

[0009] 第5の発明は、第4の発明の印刷システムにおいて、ユーザが携帯し、このユーザを識別するためのユーザ識別情報を記憶する携帯型情報記憶媒体(40)を備え、前記認証情報入力手段は、ユーザの印刷指示権限を認証するための認証情報をこのユーザの前記携帯型情報記憶媒体から入力すること、を特徴とする印刷システム(1、1－3)を提供する。

[0010] 第6の発明は、第1の発明の印刷システムにおいて、複数の印刷装置(20A, 20B, 20C)と、前記複数の印刷装置に印刷データを提供する印刷データ提供装置(30)とを備え、前記印刷データ提供装置は、前記複数の各印刷装置のセキュリティ属性を記憶する印刷装置属性記憶手段(33)を有し、前記印刷データ制限手段は、前記印刷データ提供装置に設けられ、前記各印刷装置へ提供する印刷データを、前記印刷装置属性記憶手段に記憶されている前記各印刷装置のセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限し(311, S420)、前記印刷データ提供装置は、前記印刷データ制限手段によって制限された印刷データを前記各印刷装置へ提供し、前記印刷手段は、前記複数の各印刷装置に設けられ、前記印刷データ提供装置から提供される印刷データに基づいて印刷を行うこと、を特徴とする印刷システム(1、1－3)を提供する。

[0011] 第7の発明は、第6の発明の印刷システムにおいて、前記印刷装置は、ユーザの印刷指示を入力する印刷指示入力手段(26)と、前記印刷指示入力手段によって入力される印刷指示の対象となる印刷データを識別するための対象印刷データ識別情報を入力する対象印刷データ識別情報入力手段(24)と、前記対象印刷データ識別情報入力手段によって入力された対象印刷データ識別情報を前記印刷データ提供装置へ送信する対象印刷データ識別情報送信手段(25)とを有し、前記印刷データ提供装置は、前記印刷装置から対象印刷データ識別情報を受信する対象印刷データ識別情報受信手段(34)を有し、前記印刷データ制限手段は、前記対象印刷データ識別情報受信手段によって受信された対象印刷データ識別情報によって識別される印刷データのセキュリティ属性と、前記対象印刷データ識別情報の送信元の印刷装置のセキュリティ属性とに基づいて、前記印刷データの前記印刷装置への提供の可否を判定する判定手段(311, S420)を有し、前記印刷データ提供装置は、前記判定手段によって肯と判定された場合に前記印刷データを前記印刷装置へ提供すること(S430)、を特徴とする印刷システム(1、1－3)を提供する。

[0012] 第8の発明は、第6の発明の印刷システムにおいて、前記印刷データ提供装置は、印刷データのセキュリティ属性の設定、及び／又は、印刷を行う印刷装置の選択を含む印刷属性の設定を、ユーザの指示に従って行う印刷属性設定手段(112、112

－2)を有し、前記印刷データ制限手段は、印刷データのセキュリティ属性と、前記印刷装置属性記憶手段に記憶されている印刷装置のセキュリティ属性との相関関係に基づいて、前記印刷属性設定手段によって設定可能な印刷属性の範囲を制限すること、を特徴とする印刷システム(1、1－2、1－3)を提供する。

[0013] 第9の発明は、印刷データに基づいて印刷を行う印刷手段(28)に提供する印刷データを管理するコンピュータ(31、21－2)に実行させるプログラムであって、前記印刷装置に提供する印刷データを、前記印刷手段の設置環境に基づくセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限する印刷データ制限手順(S420、S520)と、前記印刷データ制限手順において制限した印刷データを前記印刷手段へ提供する印刷データ提供手順(S360, S430、S530)とを備えること、を特徴とするプログラムを提供する。

[0014] 第10の発明は、第9の発明のプログラムにおいて、前記印刷データ制限手順は、前記印刷手段に提供する印刷データを前記印刷手段の時間帯別のセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限すること、を特徴とするプログラムを提供する。

[0015] 第11の発明は、第9の発明のプログラムにおいて、前記印刷データ制限手順は、印刷データのセキュリティ属性と、前記印刷手段のセキュリティ属性とに基づいて、前記印刷手段への前記印刷データの提供の可否を判定する判定手順(S420、S520)を有すること、を特徴とするプログラムを提供する。

発明の効果

[0016] 本発明による印刷システム及びプログラムによれば、以下の効果を得ることが可能となる。

(1)印刷手段の設置環境に基づくセキュリティ属性と、印刷データのセキュリティ属性とに基づいて、印刷手段への印刷データの提供の可否を判定するなど、印刷手段に提供する印刷データを、印刷手段の設置環境に基づくセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限することによって、印刷データの漏洩や改竄などを防止し、セキュリティ性を向上する。

特に、PCやサーバなどの印刷装置に印刷データを提供する印刷データ提供装置

において、印刷データの提供を制限する場合には、セキュリティレベルの低い印刷装置に機密性の高い印刷データを提供しないなど、印刷装置に提供する印刷データをセキュリティ属性に応じて制限することができ、印刷データの漏洩や改竄などを防止し、セキュリティ性を向上することが可能となる。

また、印刷装置において印刷手段への印刷データの提供を制限する場合には、社員が外部から持ち込んだノートPCなど、ドメインに参加していない印刷データ提供装置を印刷装置へ接続して印刷を行う場合にも、印刷装置のセキュリティレベルに見合ったセキュリティレベルの印刷データのみを印刷できることとなり、セキュリティ性を向上することが可能となる。

(2)印刷手段に提供する印刷データを、印刷手段の時間帯別のセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限することによって、より一層セキュリティ性を向上することが可能となる。

(3)認証したユーザの印刷指示権限の範囲内で印刷手段に提供する印刷データを制限することによって、セキュリティ性を向上する。

(4)携帯型情報記憶媒体から認証情報を入力することによって、ユーザが容易に認証情報を入力することができ、ユーザの利便性を向上する。

(5)複数の各印刷装置のセキュリティ属性に見合ったセキュリティ属性を有する印刷データを、各印刷装置へ提供することによって、ユーザは、印刷データのセキュリティ属性に見合った印刷装置で印刷を行うこととなり、セキュリティ性を向上することが可能となる。

(6)印刷装置が印刷指示を入力し、印刷指示の対象となる対象印刷データを印刷データ提供装置から取得して印刷することによって、印刷データを予め印刷装置に記憶していなくても、印刷を行うことができ、セキュリティ性を向上することが可能となる。また、印刷装置が印刷データを取得することによって、ユーザがPCなどの印刷データ提供装置において、印刷装置を指定する必要がなく、利便性を向上することが可能となる。更に、ユーザは、複数の印刷装置のうち、任意の印刷装置の所へ行って、使用できる状態かを確認した上で、印刷を行うことができ、ユーザの利便性を向上するとともに、印刷物の回収忘れ及び印刷内容の他のユーザへの漏洩を防止し、セキ

ュリティ性を向上することが可能となる。更にまた、一の印刷装置が使用できない状態の場合には、印刷データ提供装置へ戻らずに、他の印刷装置の所へ行って、同様に状態を確認した上で印刷を行うことができ、ユーザの利便性を向上することが可能となる。一方、印刷データ提供装置が、印刷指示の対象となる印刷データのセキュリティ属性が印刷装置のセキュリティ属性に見合った場合にこの印刷データを提供することによって、セキュリティ性を向上することが可能となる。

(7)印刷データ提供装置が設定可能な印刷属性の範囲を制限することによって、印刷データ及び印刷装置のセキュリティ属性の相関関係に見合った印刷属性を設定することができ、エラーの発生を防止するなど、ユーザの利便性を向上することが可能となる。

図面の簡単な説明

[0017] [図1]本発明による印刷システムの構成を示すブロック図である。(実施例1)

[図2]外部記憶装置33に記憶されている印刷データ管理情報、プリンタ装置管理情報を説明するための図である。(実施例1)

[図3]本発明による印刷システムの動作及びプログラムを示すフローチャートである。(実施例1)

[図4]本発明による印刷システムの動作及びプログラムを示すフローチャートである。(実施例1)

[図5]本発明による印刷システムの構成を示すブロック図である。(実施例2)

[図6]本発明による印刷システムの動作及びプログラムを示すフローチャートである。(実施例2)

[図7]LAN50を介した印刷データの授受を説明するための図である。(変形例)

[図8]本発明による印刷システムの構成を示すブロック図である。(変形例)

符号の説明

[0018] 1, 1－2, 1－3 印刷システム

10, 10－2, 10－3 PC

11, 11－2 CPU

14 カードリーダ

15 入力部

17 通信部

20A, 20B, 20C, 20A－2, 20B－2, 20C－2, 20A－3, 20B－3, 20C－3 プリンタ装置

21, 21－2 CPU

23, 23－2 外部記憶装置

24 カードリーダ

25 通信部

26 入力部

28 プリンタエンジン

30 プリンタ管理装置

31 CPU

34 通信部

40 ICカード

50 LAN

111 印刷データ形成部

112, 112－2 印刷属性設定部

113 認証部

211 認証部

212 印刷データ取得部

213 印刷管理部

311 印刷データ管理部

発明を実施するための最良の形態

[0019] 本発明は、セキュリティ性を向上するという目的を、印刷データに基づいて印刷を行う印刷部を備える印刷システムにおいて、印刷部に提供する印刷データを、この印刷部の設置環境に基づくセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限する印刷データ制限部と、印刷データ制限部によって制限された印刷データを印刷部に提供する印刷データ提供部とを備えることによって実現する。

実施例 1

[0020] 以下、図面などを参照して、本発明の実施例をあげて、さらに詳しく説明する。

図1は、本発明による印刷システムの構成を示すブロック図である。

図1に示すように、印刷システム1は、LAN50を介して接続されているPC10、複数のプリンタ装置20A, 20B, 20C及びプリンタ管理装置30と、ユーザが携帯し、PC10、プリンタ装置20A, 20B, 20Cに接続可能なICカード40などとを備え、PC10によって形成された印刷データに基づいてプリンタ装置20A, 20B, 20Cが印刷を行う、企業内ネットワークなどのネットワークシステムである。

LAN50は、企業の部内、課内などの所定の範囲で設けられているローカルエリアネットワークであって、イーサネット(登録商標)などで構築することが可能である。

[0021] PC10は、CPU11と、CPU11とシステムバス18などを介して接続されている主記憶装置12、外部記憶装置13、カードリーダ14、入力部15、表示部16、通信部17などを備えるコンピュータである。

CPU11は、主記憶装置12、外部記憶装置13に記憶されているオペレーティングシステム(以下、「OS」という。)、アプリケーションプログラム、プリンタドライバなどのプログラムを実行し、PC10全体の動作を制御し、印刷データ形成部111、印刷属性設定部112、認証部113などを実現する。

印刷データ形成部111は、ユーザの入力部15の操作に従って、文書作成ソフトウェアなどを実行して、データを編集、作成し、印刷対象となるデータの範囲を決定し、印刷データを形成する。

[0022] 印刷属性設定部112は、ユーザの入力部15の操作に従って、印刷データ形成部111によって形成された印刷データの印刷属性を設定し、印刷属性を示す印刷データ属性情報を生成する。印刷データ属性情報は、この印刷データを識別するための印刷データ識別情報、印刷データの形成を指示したユーザを識別するためのユーザ識別情報、セキュリティレベル、印刷設定情報などを含み、印刷データの属性を示す情報である。印刷データ識別情報は、印刷データ形成部111によって形成された印刷データの元となったファイル名、ファイル内でのデータの範囲を示す頁番号などを含み、この印刷データを識別するための情報である。ユーザ識別情報は、ユーザ

名、社員番号などを含み、印刷データの形成を指示したユーザを識別するための情報である。印刷設定情報は、印刷の色、品質、印刷枚数など、ユーザによって設定された印刷仕様を示す情報である。セキュリティレベルは、印刷データの機密性のレベルを示す情報であって、例えば、デジタルサインが施されている文書、極秘、部外秘、社外秘の文書の印刷データなど、各印刷データの機密性に応じて設定される(後述する図2参照。)。

[0023] 認証部113は、カードリーダ14に装着されたICカード40から入力する認証情報に基づいて、ICカード40を所持するユーザがPC10を使用する権限を有する正当ユーザか否か、つまり、ユーザを認証するか否かを判定する認証判定処理を行う。例えば、認証部113は、先ず、ICカード40と相互認証を行い、ICカード40が正当なものか否かを判定する。認証部113は、ICカード40の正当性を確認後、ICカード40からユーザ識別情報、ユーザ属性識別情報などを読み出し、認証部113は、ユーザがPC10を使用する権限を有するか否かを判定する。つまり、認証部113は、PC10の外部記憶装置13又はLAN50に接続されているシステム管理サーバ(図示しない。)に記憶されている正当ユーザの識別情報又はユーザ属性情報のリストに、ICカード40から読み出したユーザ識別情報、ユーザ属性識別情報が含まれているか否かに基づいて判定を行う。肯と判定した場合には、認証部113は、ICカード40の所持者が正当ユーザであると認証する。なお、認証部113によってユーザが未認証の場合には、PC10は、スクリーンロック状態など、ユーザが使用できない閉塞状態を維持し、ユーザが認証されることによって、PC10は、閉塞状態を解除し、ユーザが使用可能な状態となる。

[0024] 主記憶装置12は、CPU11が直接利用可能な記憶装置であって、CPU11の作業領域として使用されるRAM、起動プログラムなどのプログラム、データを記憶するROMなどを備えている(図示しない。)。

外部記憶装置13は、ハードディスクなどであって、ユーザ認証を行うプログラム、印刷データを作成、形成するプログラムなどの種々のプログラム、データを記憶している。

カードリーダ14は、挿入されたICカード40と通信を行うための通信インターフェイス

である。

入力部15は、ユーザからPC10へ情報を伝達させるためのキーボード、マウスなどの入力装置であり、表示部16は、PC10からユーザへ情報を伝達させるためのディスプレイなどの表示装置である。

通信部17は、PC10をLAN50に接続し、プリンタ装置20A～20－Nへ印刷データを送信するための通信インターフェイスであって、LAN50などのネットワークを介した他の通信装置との通信を実現する。

[0025] 各プリンタ装置20A, 20B, 20Cは、異なる環境に設置されている。各プリンタ装置20A, 20B, 20Cの構成には様々なものがあり得るが、細部にこだわらなければ、本発明の構成については、各プリンタ装置20A, 20B, 20Cの構成が実質的に同じであるとみなすことができるため、プリンタ装置20Aの構成を説明し、他のプリンタ装置20B, 20Cの構成についての説明を省略する。なお、印刷システム1が備えるプリンタ装置20A, 20B, 20Cの数は、3台に限定されず、複数であればよい。実施例2において同様である。

プリンタ装置20Aは、CPU21と、CPU21とシステムバス29を介して接続されている主記憶装置22、外部記憶装置23、カードリーダ24、通信部25、入力部26及びエンジンI／F27と、エンジンI／F27に接続されているプリンタエンジン28などとを備える印刷装置である。

[0026] CPU21は、主記憶装置22、外部記憶装置23に記憶されているプログラムを実行することによってプリンタ装置20A全体の動作を制御し、認証部211、印刷データ管理部212などを実現する。認証部211は、カードリーダ24に装着されたICカード40から入力する認証情報に基づいて、ICカード40を所持するユーザがプリンタ装置20Aを使用する権限を有する正当ユーザか否かを判定する認証判定処理をPC10の認証部113と同様に行う。印刷データ取得部212は、プリンタ管理装置30に対して、印刷指示を行うユーザを識別するためのユーザ識別情報を送信して印刷データの提供を要求し、ユーザ識別情報に対応する印刷データをプリンタ管理装置30から取得する（後述する図4参照。）。

主記憶装置22及び外部記憶装置23は、PC10の主記憶装置12及び外部記憶装

置13と同様の機能を備え、主記憶装置22のROMは、プリンタエンジン28で出力する文字コードなどのデータを記憶している。

[0027] カードリーダ24は、挿入されたICカード40と通信を行うための通信インターフェイスである。

通信部25は、プリンタ装置20AをLAN50に接続し、PC10～10－Nから印刷データを受信するための通信インターフェイスであって、LAN50などのネットワークを介した他の通信装置との通信を実現する。

入力部26は、ユーザからプリンタ装置20Aへ情報を伝達させるためのキーパネルなどの入力装置である。

エンジンI／F27は、システムバス29及びプリンタエンジン28間の情報のやりとりを仲介し、印刷データをプリンタエンジン28に出力するためのインターフェイスである。プリンタエンジン28は、エンジンI／F27を介して提供される印刷データに基づいて印刷を実行する。

[0028] プリンタ管理装置30は、CPU31と、CPU31とシステムバス35を介して接続されている主記憶装置32、外部記憶装置33及び通信部34などとを備える情報処理装置である。プリンタ管理装置30は、PC10によって形成された印刷データを記憶し、必要に応じてプリンタ装置20A，20B，20Cへ提供するなど、印刷データの管理を行う。

主記憶装置32及び外部記憶装置33は、プリンタ装置20Aの主記憶装置22及び外部記憶装置23と同様の機能を備え、外部記憶装置33は、印刷データ管理情報、プリンタ装置管理情報、印刷履歴などを記憶している。

[0029] 図2は、外部記憶装置33に記憶されている印刷データ管理情報、プリンタ装置管理情報を説明するための図である。

図2(a)に示すように、印刷データ管理情報は、PC10から受信した印刷データ属性情報に、プリンタ管理装置30が印刷データを識別するための印刷データ通し番号、この印刷データを受信した日時、この印刷データを形成したPC10の識別情報(PC ID)、印刷データサイズ、格納場所(アドレスなど)などの印刷データ識別情報を関連づけたものである。

[0030] 図2(b)に示すように、プリンタ装置管理情報は、プリンタ管理装置30の管理下にある各プリンタ装置20A, 20B, 20Cの属性を示す情報であって、プリンタ装置20A, 20B, 20Cの識別情報であるプリンタ装置識別情報に、そのセキュリティレベルなどを関連づけた情報である。セキュリティレベルは、各プリンタ装置20A, 20B, 20Cのセキュリティレベルを示し、各プリンタ装置20A, 20B, 20Cの設置環境におけるセキュリティ(安全性)のレベルであって、監視者や、監視装置などの有無、監視者の信頼性の高低、部外者の立ち入りの有無などに応じて設定されている。例えば、プリンタ装置20Aは、複数の社員などの複数の監視者がいる場所、プリンタ装置20Bは、ビデオカメラで常時監視されている場所、プリンタ装置20Cは、会議室などの監視者がほとんどいない場所に設置され、各セキュリティレベルは、「2」、「1」、「3」と設定されている。本実施例において、セキュリティレベルは、「1」が一番高く(安全性が高く)、低くなるとともに数値が増える設定となっている。

プリンタ装置管理情報は、新たにプリンタ装置が設置され、LAN50に接続された場合に、プリンタ管理装置30の外部記憶装置33に登録される。

[0031] CPU31は、主記憶装置32、外部記憶装置33に記憶されているプログラムを実行することによってプリンタ管理装置30全体の動作を制御し、印刷データ管理部311などを実現する。印刷データ管理部312は、印刷データ管理情報の外部記憶装置33への書き込み、読み出し、印刷履歴の登録、印刷データの読み出し、消去などの処理を実行し、印刷データの管理を行う。また、印刷データ管理部312は、各プリンタ装置20A, 20B, 20Cのセキュリティレベルに見合ったセキュリティレベルを有する印刷データを各プリンタ装置20A, 20B, 20Cへ提供する。例えば、印刷データのセキュリティレベルよりも低いセキュリティレベルのプリンタ装置へは、この印刷データを提供せず、プリンタ装置のセキュリティレベル以下のセキュリティレベルの印刷データを提供する(後述する図4参照。)。

[0032] ICカード40は、ユーザが印刷システム1を利用するために携帯している携帯型情報記憶媒体である。携帯型情報記憶媒体とは、SIMカード、UIMカードなどの他のICカード、ICタグ、ICカード機能を備える携帯電話機、バーコードを備えるカードなど、所定の装置が読み出し可能なように情報を秘匿して記憶する携帯型の情報記憶媒

体である。

ICカード40は、ユーザ名、社員番号などのユーザを識別するためのユーザ識別情報、所属部署、役職などのユーザの属性を識別するためのユーザ属性識別情報、秘密鍵などの正当性証明情報などを記憶している。正当性証明情報は、このICカード40に記憶されている情報の正当性をPC10、プリンタ装置20A, 20B, 20Cなどの外部装置に証明するための情報である。

[0033] 図3は、本発明による印刷システムの動作及びプログラムを示すフローチャートであって、印刷データをPC10からプリンタ管理装置30へ提供する印刷データ提供処理を示している。以下、PC10のCPU11及びプリンタ管理装置30のCPU31の処理を中心に説明する。

ユーザは、PC10を使用するため、自分のICカード40をカードリーダ14へ挿入する。図3に示すように、ステップ110(以下、「ステップ」を「S」という。)において、PC10の認証部113は、ICカード40から入力したユーザ識別情報などの認証情報に基づいて認証判定処理を行う。ユーザを正当ユーザと認証した場合には、PC10は、閉塞状態を解除し、ユーザが使用可能な状態となる(S120, S130)。

[0034] ユーザは、入力部15を操作して、アプリケーションを起動し、文書、画像などのデータの編集、作成を行い、印刷するデータの範囲を指定し、印刷データ形成部111は、印刷データを形成する(S140)。また、ユーザは、入力部15を操作し、印刷の色、品質などを指示して印刷属性を設定し、印刷属性設定部112は、印刷データの形成の指示を行ったユーザのユーザ識別情報、印刷データ識別情報、印刷設定情報、セキュリティレベルなどを含む印刷データ属性情報を生成する(S150)。印刷データ送信部113は、印刷データ及び印刷データ属性情報を、LAN50を介してプリンタ管理装置30へ送信し(S160)、処理を終了する(S170)。

[0035] プリンタ管理装置30は、この印刷データ及び印刷データ属性情報を受信し(S210)、印刷データ管理部311は、印刷データ、印刷データ属性情報から生成した印刷データ管理情報を外部記憶装置33へ記憶し(S220)、処理を終了する(S230)。

[0036] 図4は、本発明による印刷システムの動作及びプログラムを示すフローチャートであって、印刷データ提供処理(図3参照。)においてPC10からプリンタ管理装置30へ

提供された印刷データに基づいて、ユーザの指示に応じて印刷を行う印刷処理を示している。以下、プリンタ装置20AのCPU21及びプリンタ管理装置30のCPU31の処理を中心に説明する。

PC10で印刷データの形成を指示したユーザは、印刷を行うため、PC10のカードリーダ14からICカード40を抜き取り、PC10から近くに設置してあり、使用中でないプリンタ装置など、印刷を行いたい任意のプリンタ装置20Aへ行き、そのカードリーダ24へICカード40を装着し、入力部26を操作し、印刷指示を行う。

[0037] 図4に示すように、S310において、プリンタ装置20Aは、印刷指示を入力し、印刷指示を行うユーザを識別するためのユーザ識別情報などを含む認証情報をICカード40から入力する。認証部211は、認証情報に基づいて、認証判定処理を行う(S320)。ユーザを正当ユーザと認証した場合には、印刷データ取得部213は、ICカード40から入力したユーザ識別情報、プリンタ装置20Aを識別するためのプリンタ装置識別情報を含み、対応する印刷データの提供を要求する印刷データ提供要求を通信部25からプリンタ管理装置30へ送信する(S330, S340)。

[0038] プリンタ管理装置30は、この要求を受信し、処理を開始する(S410)。

印刷データ管理部311は、外部記憶装置33に記憶されているプリンタ装置管理情報と、印刷データ管理情報とを参照し、印刷指示を行ったユーザ「甲」の印刷指示権限範囲内であって、セキュリティ条件を満たす印刷データを外部記憶装置33から読み出す(S420)。具体的には、印刷データ管理部311は、受信したユーザ識別情報(「甲」)に関連づけられ、また、要求元のプリンタ装置20Aのセキュリティレベル(「2」)以下である印刷データ(No. 474の印刷データ)を読み出す。No. 472, 475の印刷データは、セキュリティレベルが「1」であるため、セキュリティレベルが「2」のプリンタ装置20Aへは、提供されない。プリンタ管理装置30は、読み出した印刷データを要求の送信元であるプリンタ装置20Aへ送信する(S430)。

[0039] プリンタ装置20Aは、印刷データを受信し(S350)、この印刷データをプリンタエンジン28へ出力して印刷を行い(S360)、印刷の終了後にその旨の通知をプリンタ管理装置30へ送信し(S370)、処理を終了する(S380)。

プリンタ管理装置30は、印刷終了の通知をプリンタ装置20Aから受け(S440)、外

部記憶装置33に印刷履歴を書き込み、印刷の対象となった印刷データを外部記憶装置33から消去し(S450)、処理を終了する(S460)。

なお、ユーザが他のプリンタ装置20B, 20Cで印刷を行う場合にも、他のプリンタ20B, 20Cは、プリンタ20Aと同様に印刷処理を行う。

また、プリンタ管理装置30の印刷データ管理部311は、PC10から受信してから(図3のS210)、所定の期間以上、印刷指示(図4のS310)の対象とならず、放置されている印刷データを外部記憶装置33から消去し、その旨を印刷履歴として外部記憶装置33へ記憶する。

[0040] このように、本実施例によれば、印刷システム1は、プリンタ管理装置30が、プリンタ装置20A, 20B, 20Cの設置環境に基づくセキュリティレベルに見合ったセキュリティレベルを有する印刷データをプリンタ装置20A, 20B, 20Cへ提供するため、不正利用される可能性があるセキュリティレベルの低いプリンタ装置20A, 20B, 20Cに機密性の高い印刷データを提供しないなど、印刷データの漏洩や改竄などを防止し、セキュリティ性を向上することが可能となった。

また、印刷システム1は、印刷指示を行ったユーザを、印刷データを形成したユーザと認証した場合に、この印刷データに基づいて印刷を行い、認証したユーザの印刷指示権限の範囲内でプリンタ装置20A, 20B, 20Cに提供する印刷データを制限するため、セキュリティ性を向上することが可能となった。

[0041] 更に、印刷システム1は、ICカード40から、対象印刷データ識別情報となるユーザ識別情報、印刷指示を行ったユーザを認証するための認証情報を入力することによって、ユーザが容易に対象印刷データ識別情報、認証情報を入力することができ、ユーザの利便性を向上することが可能となった。

更にまた、印刷システム1は、複数の各プリンタ装置20A, 20B, 20Cのセキュリティレベルに見合ったセキュリティレベルを有する印刷データを、各プリンタ装置20A, 20B, 20Cへ提供するため、ユーザは、印刷データのセキュリティレベルに見合ったプリンタ装置で印刷を行うこととなり、セキュリティ性を向上することが可能となった。

また、印刷システム1は、プリンタ装置20A, 20B, 20Cが印刷指示を入力し、印刷指示の対象となる対象印刷データをプリンタ管理装置30から取得して印刷するため

、印刷データを予めプリンタ装置20A，20B，20Cに記憶していなくても、印刷を行うことができ、セキュリティ性を向上することが可能となった。

[0042] 更に、印刷システム1は、プリンタ装置20A，20B，20Cが印刷データを取得するため、ユーザがPC10において、印刷を行うプリンタ装置20A，20B，20Cを指定する必要がなく、利便性を向上することが可能となった。

更にまた、ユーザは、複数のプリンタ装置20A，20B，20Cのうち、任意のプリンタ装置20Aの所へ行って、使用できる状態かを確認した上で、印刷を行うことができ、ユーザの利便性を向上するとともに、印刷物の回収忘れ及び印刷内容の他のユーザへの漏洩を防止し、セキュリティ性を向上することが可能となった。

また、ユーザは、プリンタ装置20Aが使用できない状態の場合には、PC10へ戻らずに、他のプリンタ装置20B，20Cの所へ行って、同様に状態を確認した上で印刷を行うことができ、ユーザの利便性を向上することが可能となった。

実施例 2

[0043] 図5は、本発明による印刷システムの構成を示すブロック図である。

なお、前述した実施例と同様な機能を果たす部分には、同一の符号又は末尾に統一した符号を付して、重複する説明や図面を適宜省略する。

図5に示すように、印刷システム1－2は、LAN50を介して接続されているPC10－2及び複数のプリンタ装置20A－2，20B－2，20C－2と、PC10－2に接続可能なICカード40などとを備え、PC10－2によって形成された印刷データに基づいてプリンタ装置20A－2，20B－2，20C－2が印刷を行うネットワークシステムである。

PC10－2は、実施例1におけるPC10と略同様の構成を有し、CPU11－2などを備えている。CPU11－2は、印刷属性設定部112－2などを実現する。印刷属性設定部112－2は、ユーザの入力部15の操作に従って、印刷を行うプリンタ装置をプリンタ装置20A，20B，20Cから選択、設定し、PC10－2は、印刷データ、印刷データ属性情報などを、そのプリンタ装置へ送信し、印刷指示を行う。

[0044] プリンタ装置20A－2，20B－2，20C－2は、実施例1におけるプリンタ装置20A，20B，20Cと略同様の構成を有し、外部記憶装置23－2、CPU21－2が主記憶装置22、外部記憶装置23－2に記憶されているプログラムを実行することによって実現

される印刷管理部213などを備えている。

外部記憶装置23－2は、PC10－2から受信する印刷データ、印刷データ属性情報を記憶する。また、外部装置23－2は、設けられているプリンタ装置20A－2のセキュリティレベル、印刷履歴を記憶している。

[0045] 印刷管理部213は、印刷データ、印刷データ属性情報の外部記憶装置23への書き込み、読み出し、プリンタエンジン28への出力、消去、印刷履歴の登録などの処理を実行し、印刷データを管理し、プリンタエンジン28の印刷を制御する。また印刷管理部213は、自身が設けられているプリンタ装置20A－2のセキュリティレベルに見合ったセキュリティレベルを有する印刷データ、つまり、プリンタ装置20A－2のセキュリティレベルに基づいたセキュリティ条件を満たすセキュリティレベルの印刷データをプリンタエンジン28へ出力する。従って、印刷管理部213は、プリンタ装置20A－2のセキュリティレベルよりも高いセキュリティレベルの印刷データについて印刷指示をPC10－2から受けた場合であっても、プリンタエンジン28へ出力せず、印刷を行わない（後述する図6参照。）。

[0046] 図6は、本発明による印刷システムの動作及びプログラムを示すフローチャートである。以下、プリンタ装置20A－2のCPU21－2の処理を中心に説明する。

図6に示すように、PC10－2は、印刷データ、印刷データ属性情報などを、ユーザによって選択されたプリンタ装置20A－2へ送信して印刷指示を行い、プリンタ装置20A－2は、この印刷指示を受信し、処理を開始する（S510）。

印刷管理部213は、受信した印刷データ属性情報に含まれる印刷データのセキュリティレベルが、セキュリティ条件を満たすか否かに基づいて、この印刷データのプリンタエンジン28への提供の可否を判定する（S520）。

肯と判定した場合に、印刷管理部213は、この印刷データをプリンタエンジン28へ出力し、印刷を行う（S530）。

[0047] 印刷管理部213は、印刷日時、印刷拒否日時などの印刷履歴を外部記憶装置23へ登録し、印刷（又は印刷拒否）の対象となった印刷データを外部記憶装置23から消去し（S540）、正常終了（又はエラー）の印刷結果を印刷指示の送信元のPC10－2へ送信し（S550）、処理を終了する（S560）。

なお、PC10－2から印刷指示を他のプリンタ装置20B－2，20C－2へ送信した場合には、他のプリンタ20B－2，20C－2は、プリンタ20A－2と同様に処理を行う。

[0048] このように、本実施例によれば、実施例1と同様の効果に加え、社員が外部から持ち込んだノートPCなど、ドメインに参加していない印刷データ提供装置をプリンタ装置20A－2，20B－2，20C－2へ接続して印刷を行う場合にも、プリンタ装置20A－2，20B－2，20C－2のセキュリティレベルに見合ったセキュリティレベルの印刷データのみが印刷できることとなり、セキュリティ性を向上することが可能となった。

[0049] （変形例）

以上説明した実施例に限定されることなく、種々の変形や変更が可能であって、それらも本発明の均等の範囲内である。例えば、各実施例において、プリンタ管理装置30、プリンタ装置20A－2，20B－2，20C－2は、プリンタ装置20A，20B，20C、20A－2，20B－2，20C－2のセキュリティレベルをそれぞれ記憶しているが、就業時間外には低いセキュリティレベルとなるなど、時間帯によって異なる時間帯別のプリンタ装置20A，20B，20C、20A－2，20B－2，20C－2（以下、まとめて「20A～20C－2」と表記する。）のセキュリティレベルを記憶していてもよい。プリンタ装置20A～20C－2の設置環境により適合したセキュリティレベルに合わせて印刷データをプリンタエンジン28へ提供することができ、より一層セキュリティ性を向上することが可能となる。

[0050] 図7に示すように、実施例1又は実施例2において、印刷システム1，1－2は、プリンタ管理装置30又はプリンタ装置20A－2が、プリンタエンジン28に提供する印刷データを制限しているが（＃20，＃30）、PC10，10－2（＃10）でプリンタ装置管理情報を記憶し、印刷手段に提供する印刷データの制限を行ってもよい。例えば、PC10，10－2でプリンタエンジン28へ提供する印刷データを制限する場合には、印刷属性を設定する印刷属性設定部112，112－2が、印刷データ及びプリンタ装置20A，20B，20Cのセキュリティ属性の相関関係に基づいて、ユーザが入力部15を操作して設定できる印刷データのセキュリティレベル、選択可能なプリンタ装置20A～20C－2を制限し、設定可能な印刷属性の範囲を制限してもよい。印刷データ及びプリンタ装置20A～20C－2のセキュリティレベルの相関関係の条件にあった印刷属

性を設定することができ、セキュリティレベルが見合わない場合のエラー発生を防止し、速やかな印刷が可能となる。

[0051] また、実施例2において、印刷システム1－2が、実施例1のように、PC10－2及びプリンタ装置20A－2，20B－2，20C－2間で印刷データの授受を管理し、プリンタ装置20A－2，20B－2，20C－2への印刷データの提供を制限するプリンタ管理装置30を備えていてもよい。印刷データを形成してからプリンタエンジン28へ提供するまでの印刷データの提供経路のいずれかにおいて印刷データの制限を行えば、いずれで行うかは限定されない。

[0052] 各実施例において、携帯型情報記憶媒体としてICカード40を例示したが、これに限定されず、所持者であるユーザを認証するための認証情報をPC10，10－2、プリンタ装置20A，20B，20Cへ提供できれば他の携帯型情報記憶媒体であってもよい。従って、携帯型情報記憶媒体及びカードリーダ14，24間の通信方式は、接触式、非接触式、接触／非接触式などのいずれであってもよく、限定されない。

[0053] 各実施例において、印刷システム1，1－2が備えるプリンタ装置20A～20C，20A－2～20C－2が、FAXデータを受信し、このFAXデータについて印刷を行う印刷装置であってもよい。

図8に示すように、印刷システム1－3は、PC10－3と、PC10－3にLAN50などを介して接続されているFAX送信装置60、FAX送信装置30－3に電話回線などの通信回線70を介して接続されているプリンタ装置20A－3，20B－3，20C－3などを備えている。PC10－3、プリンタ装置20A－3，20B－3，20C－3は、PC10，10－2、プリンタ装置20A～20C、20A－2～20C－2とそれぞれ略同様の構成を備えている。PC10－3は、印刷データとなるFAXデータを形成し、FAX送信装置60へFAX指示とともにFAXデータを送信する。FAX送信装置60は、FAX指示に応じてFAXデータを所定のプリンタ装置20A－3，20B－3，20C－3へ送信する。プリンタ装置20A－3～20C－3は、このFAXデータを出力し、印刷を行う。この印刷システム1－3において、プリンタ装置20A－3，20B－3，20C－3のプリンタエンジン28に提供する印刷データを、その設置環境に基づくセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限する印刷データ管理部は、実施例1のようにFAX送

信装置60に設けられていてもよいし、実施例2のようにプリンタ装置20A－2～20C－2に設けられていてもよい。また、PC10－3が印刷データ管理部を備えていてもよい。

[0054] 各実施例において、印刷システム1，1－2は、印刷データ及びプリンタ装置20A～20C－2のセキュリティレベルに基づいて、セキュリティ条件を満たす印刷データを提供する（図4のS420，S430）、セキュリティ条件を満たすか否かを判定する（図6のS520）ことによって、プリンタエンジン28へ提供する印刷データを制限しているが、制限方法はこれらに限定されない。例えば、実施例2において、プリンタ装置20A－2，20B－2，20C－2が印刷データ属性情報を受信した場合に、この印刷データ属性情報に含まれるセキュリティレベルに基づいて、印刷データの受信を行うか否かを判定し、判定結果によって印刷データの受信を拒否してもよい。

[0055] 各実施例において、印刷システム1，1－2は、プリンタ装置20A～20C－2に提供する印刷データを、プリンタ装置20A～20C－2のセキュリティレベル以下の印刷データに制限しているが、所定のセキュリティレベル以下の印刷データを提供しないなど、プリンタ装置20A～20C－2のセキュリティレベルに対して相対的に適当なセキュリティレベルの印刷データに制限してもよい。プリンタ装置20A～20C－2及び印刷データの印刷レベルの相対的な条件は、任意に設定することが可能である。

セキュリティレベルの高い印刷装置におけるセキュリティレベルの低い印刷データについての印刷を防止することによって、セキュリティレベルの高い印刷データの印刷を速やかに行うことができ、印刷の効率を向上することが可能となる。

[0056] 各実施例において、PC10，10－2は、PCLなどのページ記述言語（PDL）で記述した印刷データを形成し、プリンタ装置20A，20B，20C、20A－2，20B－2，20C－2へ提供してもよく、PDLの印刷データをビットマップデータなどの画像データに変換して提供してもよい。PC10，10－2及びプリンタ装置20A，20B，20C、20A－2，20B－2，20C－2間において授受される印刷データのデータ形式は、限定されない。

[0057] 実施例1において、PC10の印刷属性設定部112は、印刷データについて印刷指示を行うことができるユーザを、印刷データを形成したユーザに設定しているが、印

刷データを形成したユーザの指示に従って設定し、このユーザを識別するための指示可能ユーザ識別情報を含む印刷データ属性情報を生成してもよい。例えば、甲は、形成した印刷データについて、印刷指示を行うことができる指示可能ユーザを「乙」、「営業部員」などとPC10で設定し、この指示可能ユーザを識別するための指示可能ユーザ識別情報を印刷データ属性情報としてプリンタ管理装置30に記憶する。プリンタ管理装置30は、プリンタ装置20Aから入力した印刷指示を行ったユーザのユーザ識別情報と、印刷データ属性情報に含まれる指示可能ユーザ識別情報とに基づいて、印刷指示を行ったユーザの印刷指示権限範囲内の印刷データをプリンタ装置20Aへ提供する。印刷データの形成を指示したユーザが、印刷指示を行うことができるユーザを選択することができ、利便性及びセキュリティ性を向上することが可能となる。

[0058] また、プリンタ管理装置30は、各ユーザについて印刷を行うことができる時間帯を記憶していてもよい。例えば、プリンタ管理装置30は、アルバイトのユーザであれば就業時間内を印刷可能時間帯として記憶し、プリンタ装置20A, 20B, 20Cが、このユーザのユーザ識別情報をこの印刷可能時間帯に入力した場合にのみ印刷データをプリンタ装置20A, 20B, 20Cへ提供してもよい。各ユーザの属性に合わせた設定を行うことができ、セキュリティ性を向上することが可能となる。

[0059] 実施例1において、PC10、プリンタ装置20A, 20B, 20Cは、ICカード40のカードリーダ14、24への挿入を検出するなど、ICカード40が所定の位置に置かれたこと、又は、ICカード40が所定の範囲内に持ち込まれたことなど、ICカード40が、このICカード40に記憶されている情報を読み取ることができる所定の場所へ移動してきたことを検出するICカード検出部を備えていてもよい。処理開始のきっかけとすることができ、利用者の利便性を向上することが可能となる。また、プリンタ装置20A, 20B, 20Cは、ICカード40の検出を、印刷指示として入力してもよい。

[0060] 実施例1において、プリンタ装置20A, 20B, 20Cは、印刷指示の対象となる印刷データを識別するための対象印刷データ識別情報としてユーザ識別情報をICカード40から入力しているが、プリンタ装置20A, 20B, 20Cが表示部(図示しない。)に印刷データの識別情報を表示し、ユーザが入力部26を操作し、印刷指示の対象となる

印刷データを選択し、対象印刷データ識別情報を入力するなど、印刷データ識別情報を入力してもよい。

また、プリンタ装置20A，20B，20Cは、印刷データ識別情報として、PC10の識別情報、ユーザの所属部署などの属性などを入力してもよく、印刷指示の対象となる印刷データを識別することができれば、プリンタ装置20A，20B，20Cが入力する印刷データ識別情報は限定されない。

請求の範囲

[1] 印刷データに基づいて印刷を行う印刷手段を備える印刷システムにおいて、

前記印刷手段に提供する印刷データを、前記印刷手段の設置環境に基づくセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限する印刷データ制限手段を備えること、

を特徴とする印刷システム。

[2] 請求項1に記載の印刷システムにおいて、

前記印刷データ制限手段は、前記印刷手段に提供する印刷データを前記印刷手段の時間帯別のセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限すること、

を特徴とする印刷システム。

[3] 請求項1に記載の印刷システムにおいて、

前記印刷データ制限手段は、印刷データのセキュリティ属性と、前記印刷手段のセキュリティ属性とに基づいて、前記印刷手段への前記印刷データの提供の可否を判定する判定手段を有すること、

を特徴とする印刷システム。

[4] 請求項1に記載の印刷システムにおいて、

印刷指示を行うユーザの印刷指示権限を認証するための認証情報を入力する認証情報入力手段と、

前記認証情報入力手段によって入力される認証情報に基づいてユーザの印刷指示権限を認証する認証手段とを備え、

前記印刷データ制限手段は、前記認証手段によって認証された印刷指示権限の範囲内で前記印刷手段に提供する印刷データを制限すること、

を特徴とする印刷システム。

[5] 請求項4に記載の印刷システムにおいて、

ユーザが携帯し、このユーザを識別するためのユーザ識別情報を記憶する携帯型情報記憶媒体を備え、

前記認証情報入力手段は、ユーザの印刷指示権限を認証するための認証情報を

このユーザの前記携帯型情報記憶媒体から入力すること、

を特徴とする印刷システム。

[6] 請求項1に記載の印刷システムにおいて、

複数の印刷装置と、

前記複数の印刷装置に印刷データを提供する印刷データ提供装置とを備え、

前記印刷データ提供装置は、前記複数の各印刷装置のセキュリティ属性を記憶する印刷装置属性記憶手段を有し、

前記印刷データ制限手段は、前記印刷データ提供装置に設けられ、前記各印刷装置へ提供する印刷データを、前記印刷装置属性記憶手段に記憶されている前記各印刷装置のセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限し、

前記印刷データ提供装置は、前記印刷データ制限手段によって制限された印刷データを前記各印刷装置へ提供し、

前記印刷手段は、前記複数の各印刷装置に設けられ、前記印刷データ提供装置から提供される印刷データに基づいて印刷を行うこと、

を特徴とする印刷システム。

[7] 請求項6に記載の印刷システムにおいて、

前記印刷装置は、ユーザの印刷指示を入力する印刷指示入力手段と、前記印刷指示入力手段によって入力される印刷指示の対象となる印刷データを識別するための対象印刷データ識別情報を入力する対象印刷データ識別情報入力手段と、前記対象印刷データ識別情報入力手段によって入力された対象印刷データ識別情報を前記印刷データ提供装置へ送信する対象印刷データ識別情報送信手段とを有し、

前記印刷データ提供装置は、前記印刷装置から対象印刷データ識別情報を受信する対象印刷データ識別情報受信手段を有し、

前記印刷データ制限手段は、前記対象印刷データ識別情報受信手段によって受信された対象印刷データ識別情報によって識別される印刷データのセキュリティ属性と、前記対象印刷データ識別情報の送信元の印刷装置のセキュリティ属性とに基づいて、前記印刷データの前記印刷装置への提供の可否を判定する判定手段を有

し、

前記印刷データ提供装置は、前記判定手段によって肯と判定された場合に前記印刷データを前記印刷装置へ提供すること、

を特徴とする印刷システム。

[8] 請求項6に記載の印刷システムにおいて、

前記印刷データ提供装置は、印刷データのセキュリティ属性の設定、及び／又は、印刷を行う印刷装置の選択を含む印刷属性の設定を、ユーザの指示に従って行う印刷属性設定手段を有し、

前記印刷データ制限手段は、印刷データのセキュリティ属性と、前記印刷装置属性記憶手段に記憶されている印刷装置のセキュリティ属性との相関関係に基づいて、前記印刷属性設定手段によって設定可能な印刷属性の範囲を制限すること、

を特徴とする印刷システム。

[9] 印刷データに基づいて印刷を行う印刷手段に提供する印刷データを管理するコンピュータに実行させるプログラムであって、

前記印刷装置に提供する印刷データを、前記印刷手段の設置環境に基づくセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限する印刷データ制限手順と、

前記印刷データ制限手順において制限した印刷データを前記印刷手段へ提供する印刷データ提供手順とを備えること、

を特徴とするプログラム。

[10] 請求項9に記載の印刷システムにおいて、

前記印刷データ制限手順は、前記印刷手段に提供する印刷データを前記印刷手段の時間帯別のセキュリティ属性に見合ったセキュリティ属性を有する印刷データに制限すること、

を特徴とするプログラム。

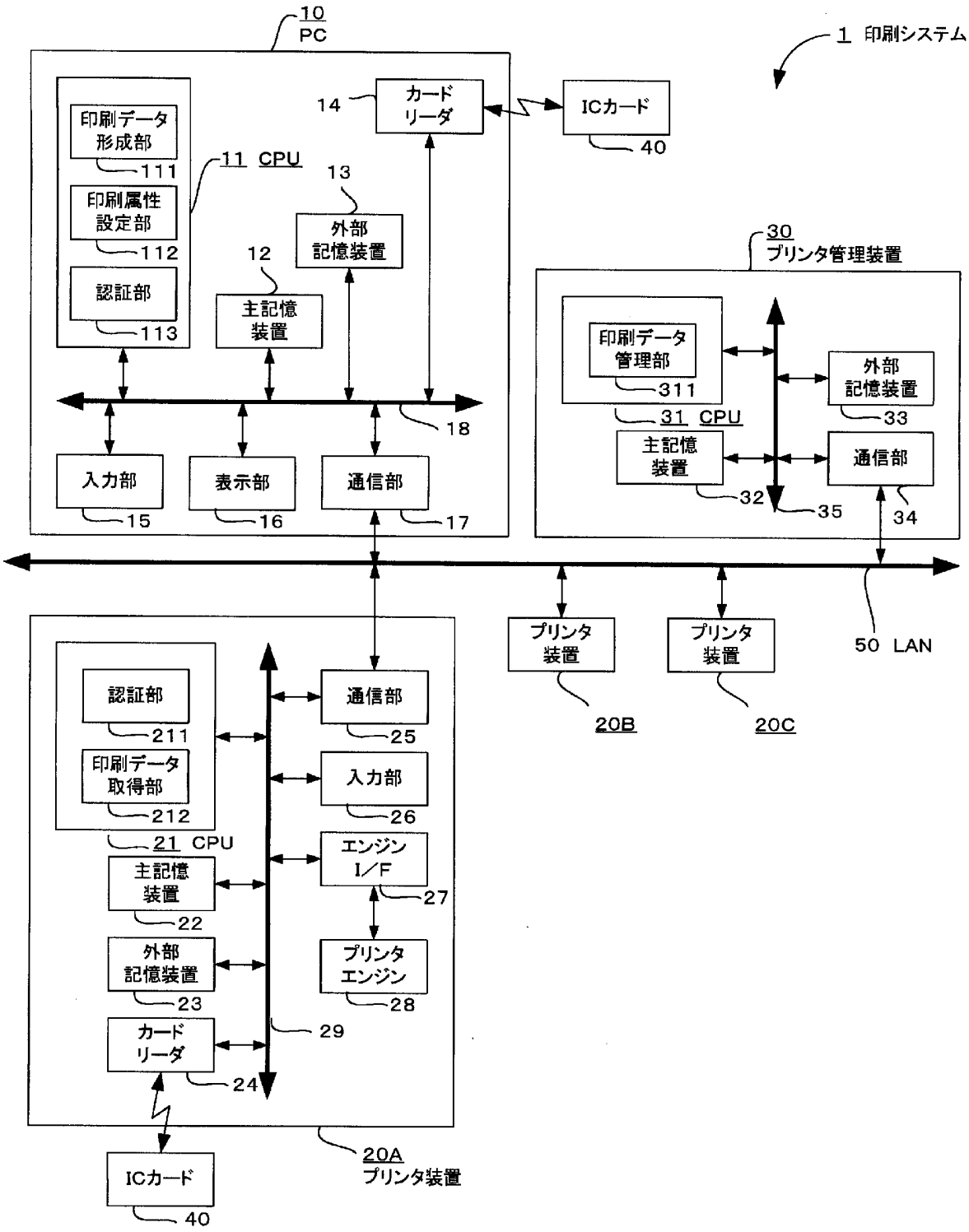
[11] 請求項9に記載のプログラムにおいて、

前記印刷データ制限手順は、印刷データのセキュリティ属性と、前記印刷手段のセキュリティ属性とに基づいて、前記印刷手段への前記印刷データの提供の可否を判

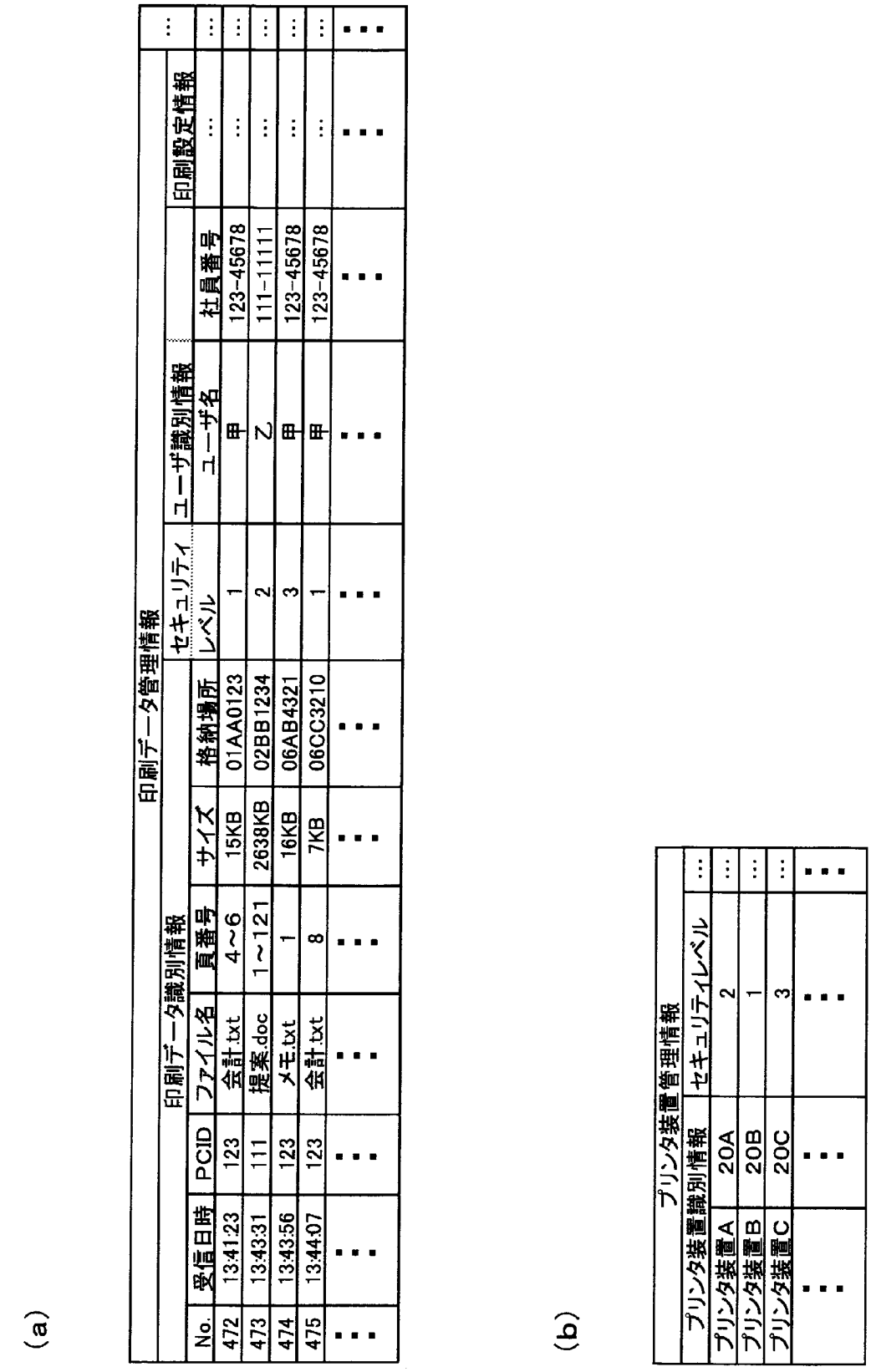
定する判定手順を有すること、

を特徴とするプログラム。

[図1]


10
PC
1 印刷システム
印刷データ
形成部
111
印刷属性
設定部
112
認証部
113
11 CPU
14
カード
リーダ
ICカード
40
13
外部
記憶装置
12
主記憶
装置
18
入力部
15
表示部
16
通信部
17
30
プリンタ管理装置
印刷データ
管理部
311
31 CPU
主記憶
装置
32
外部
記憶装置
33
通信部
34
35
50 LAN
プリンタ
装置
20B
プリンタ
装置
20C
認証部
211
印刷データ
取得部
212
21 CPU
主記憶
装置
22
外部
記憶装置
23
カード
リーダ
24
通信部
25
入力部
26
エンジン
I/F
27
プリンタ
エンジン
28
29
20A
プリンタ装置
ICカード
40

[図2]



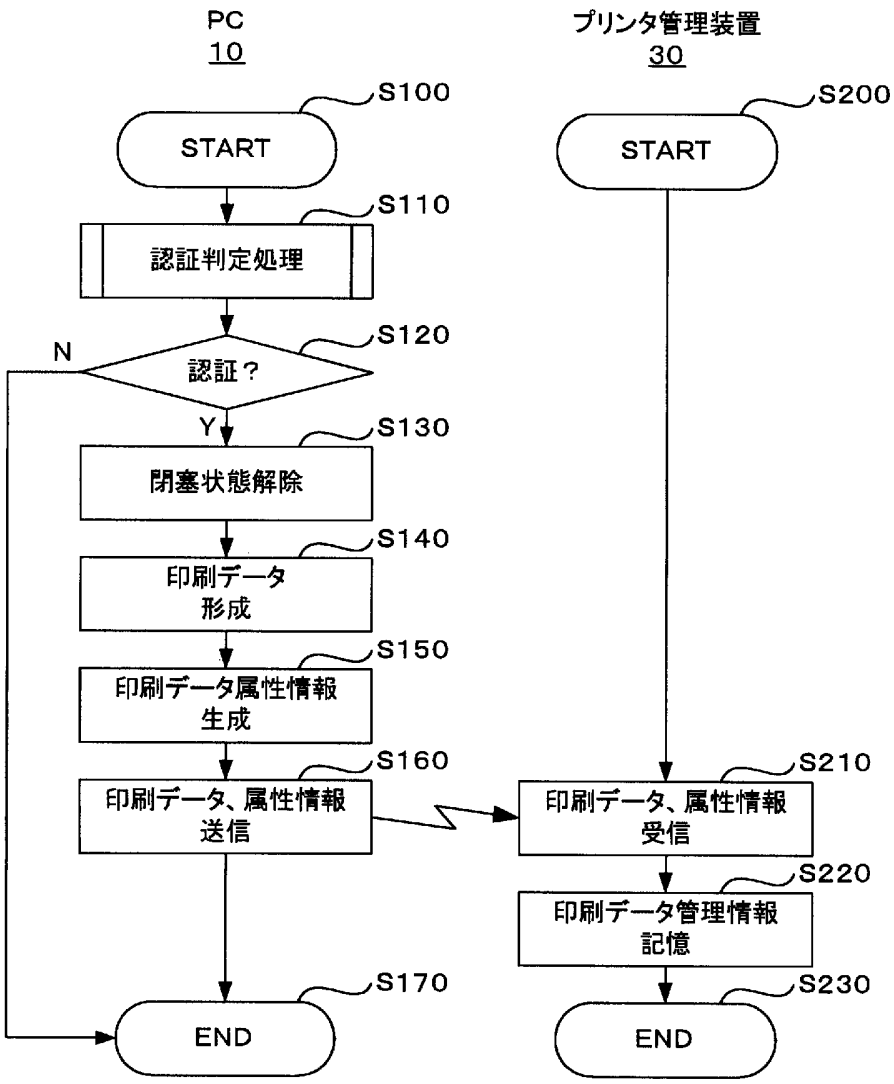
(a)

印刷データ管理情報										
印刷データ識別情報							セキュリティ	ユーザ識別情報		印刷設定情報
No.	受信日時	PCID	ファイル名	頁番号	サイズ	格納場所	レベル	ユーザ名	社員番号	…
472	13:41:23	123	会計.txt	4～6	15KB	01AA0123	1	甲	123-45678	…
473	13:43:31	111	提案.doc	1～121	2638KB	02BB1234	2	乙	111-11111	…
474	13:43:56	123	メモ.txt	1	16KB	06AB4321	3	甲	123-45678	…
475	13:44:07	123	会計.txt	8	7KB	06CC3210	1	甲	123-45678	…
▪ ▪ ▪	▪ ▪ ▪	▪ ▪ ▪	▪ ▪ ▪	▪ ▪ ▪	▪ ▪ ▪	▪ ▪ ▪	▪ ▪ ▪	▪ ▪ ▪	▪ ▪ ▪	▪ ▪ ▪

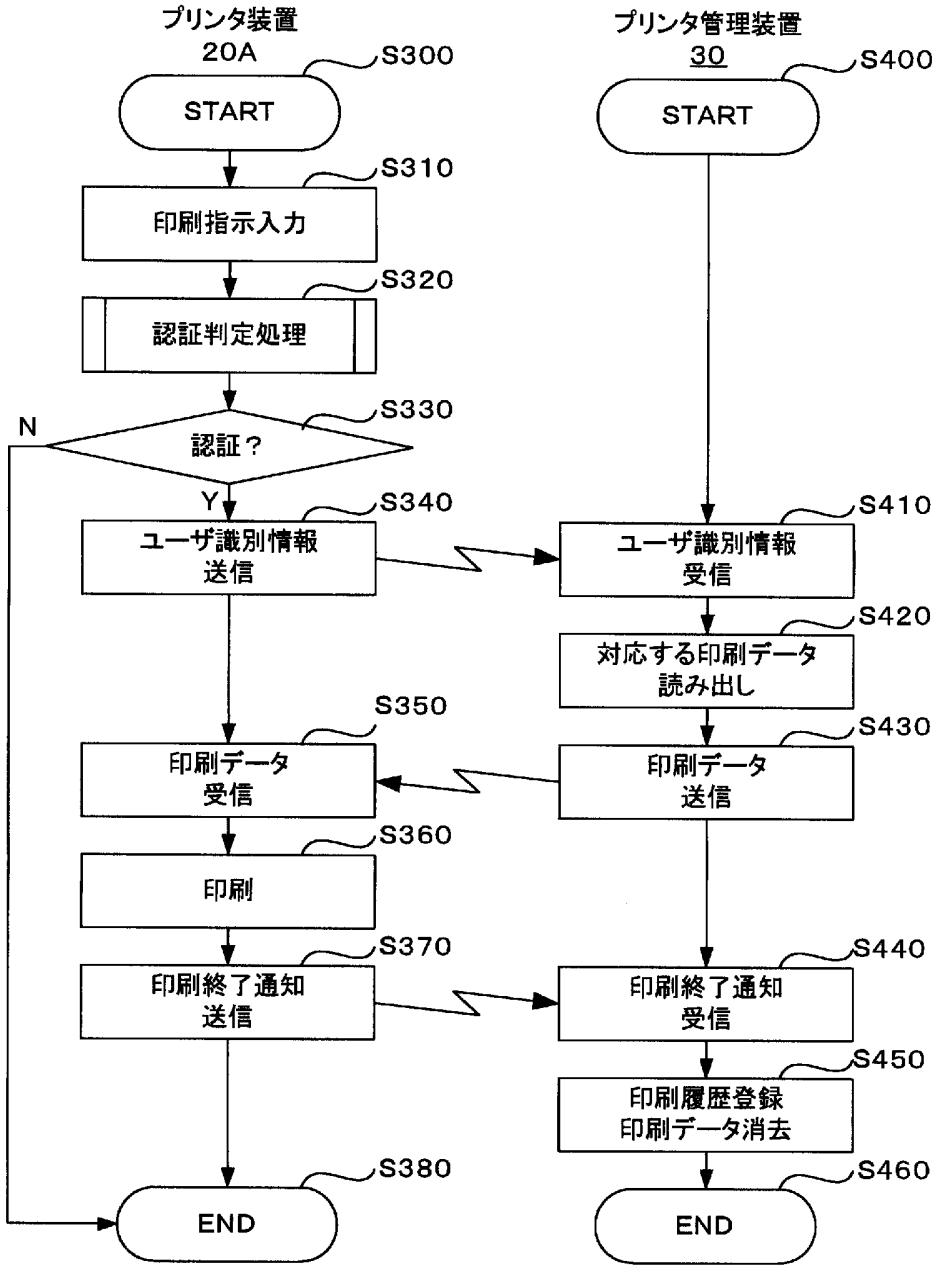
(b)

プリンタ装置管理情報		
プリンタ装置識別情報	セキュリティレベル	…
プリンタ装置A	2	…
プリンタ装置B	1	…
プリンタ装置C	3	…
▪ ▪ ▪	▪ ▪ ▪	▪ ▪ ▪

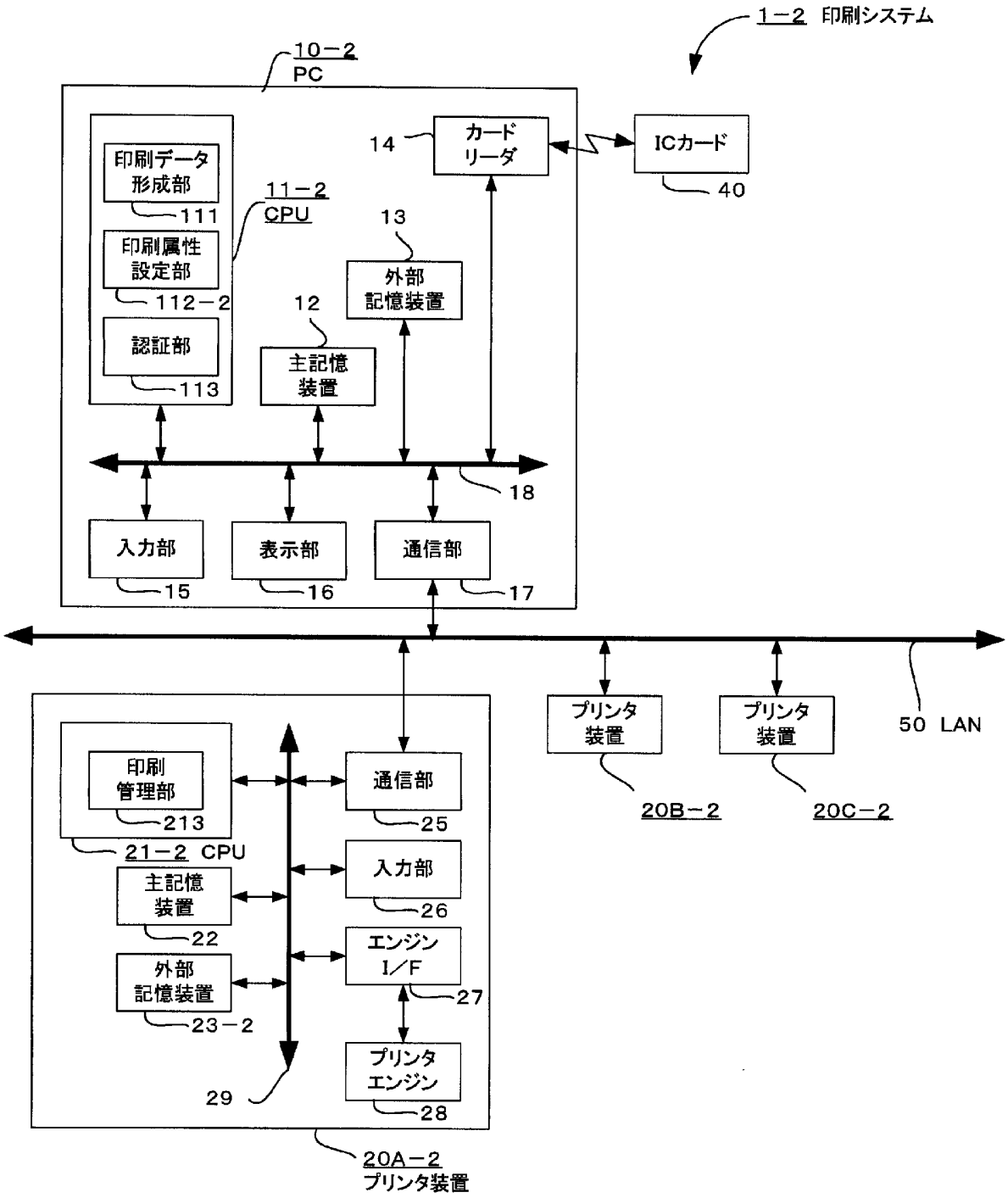
[図3]


PC
10
プリンタ管理装置
30
S100
START
S200
START
S110
認証判定処理
S120
認証？
N
Y
S130
閉塞状態解除
S140
印刷データ
形成
S150
印刷データ属性情報
生成
S160
印刷データ、属性情報
送信
S210
印刷データ、属性情報
受信
S220
印刷データ管理情報
記憶
S170
END
S230
END

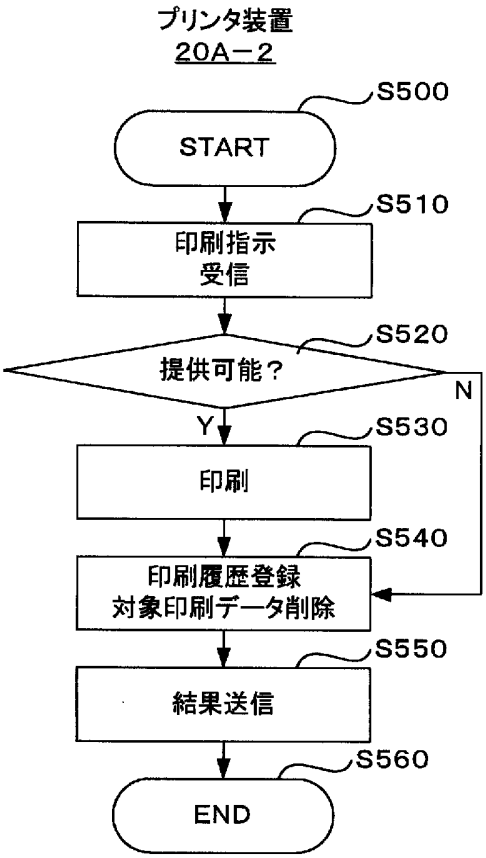
[図4]


プリンタ装置
20A
プリンタ管理装置
30
S300
START
S400
START
S310
印刷指示入力
S320
認証判定処理
S330
認証？
N
Y
S340
ユーザ識別情報
送信
S410
ユーザ識別情報
受信
S420
対応する印刷データ
読み出し
S350
印刷データ
受信
S430
印刷データ
送信
S360
印刷
S370
印刷終了通知
送信
S440
印刷終了通知
受信
S450
印刷履歴登録
印刷データ消去
S380
END
S460
END

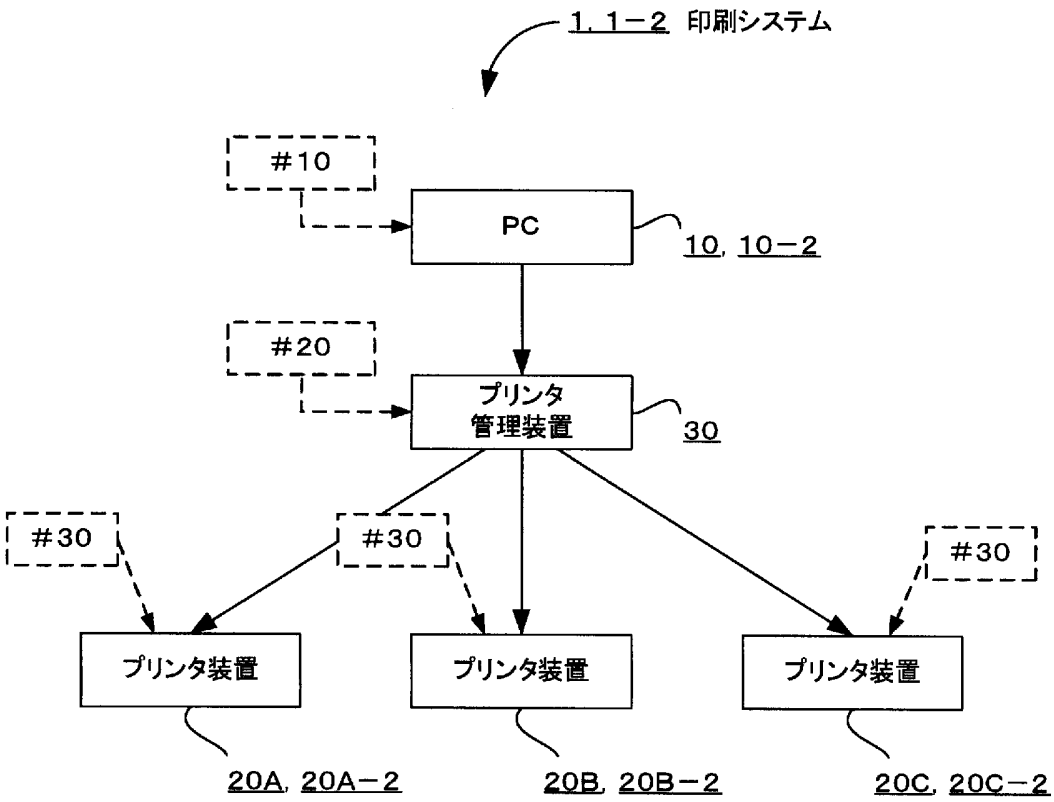
[図5]


1－2 印刷システム
10－2
PC
印刷データ
形成部
111
印刷属性
設定部
112－2
認証部
113
11－2
CPU
14
カード
リーダ
ICカード
40
13
外部
記憶装置
12
主記憶
装置
18
入力部
15
表示部
16
通信部
17
50 LAN
プリンタ
装置
20B－2
プリンタ
装置
20C－2
印刷
管理部
213
21－2 CPU
主記憶
装置
22
外部
記憶装置
23－2
通信部
25
入力部
26
エンジン
I／F
27
プリンタ
エンジン
28
29
20A－2
プリンタ装置

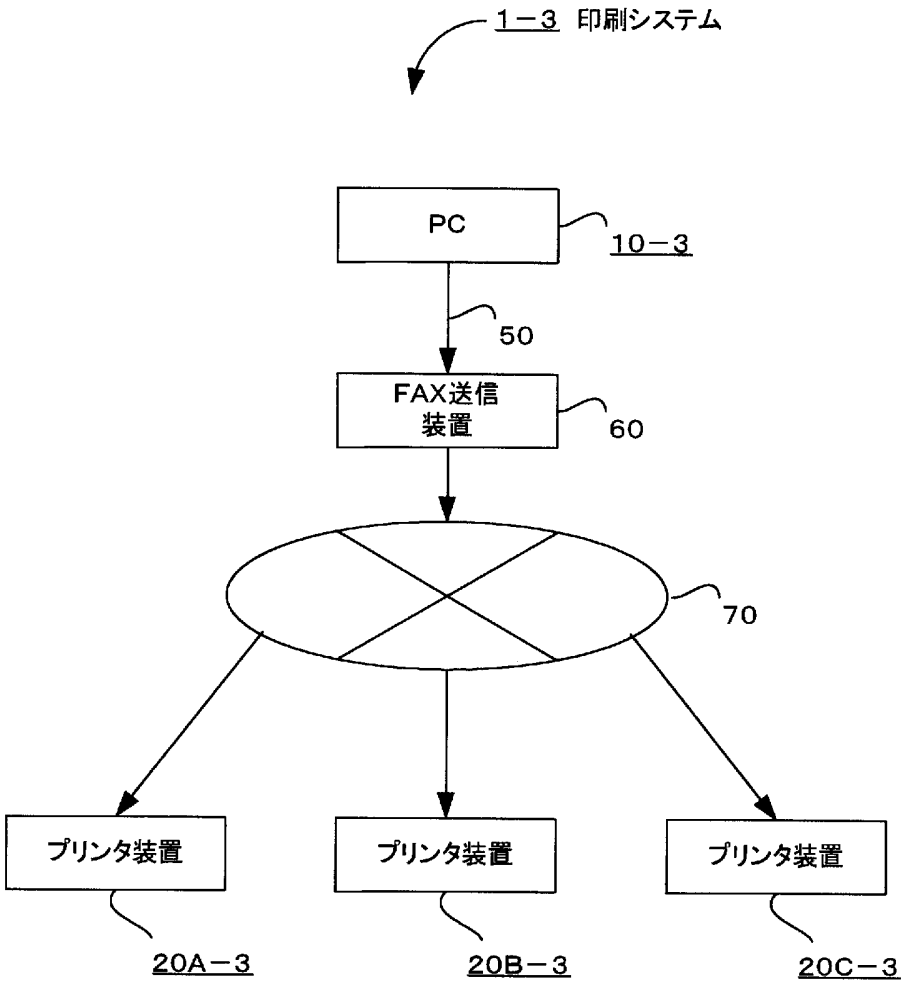
[図6]


プリンタ装置
20A－2
S500
START
S510
印刷指示
受信
S520
提供可能？
N
Y
S530
印刷
S540
印刷履歴登録
対象印刷データ削除
S550
結果送信
S560
END

[図7]


1, 1－2 印刷システム
#10
PC
10, 10－2
#20
プリンタ
管理装置
30
#30
#30
#30
プリンタ装置
プリンタ装置
プリンタ装置
20A, 20A－2
20B, 20B－2
20C, 20C－2

[図8]


1－3 印刷システム
PC
10－3
50
FAX送信
装置
60
70
プリンタ装置
プリンタ装置
プリンタ装置
20A－3
20B－3
20C－3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/311217

A. CLASSIFICATION OF SUBJECT MATTER
G06F3/12(2006.01)i, *B41J29/38*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F3/12, B41J29/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 6-103008 A (Ricoh Co., Ltd.), 15 April, 1994 (15.04.94), Abstract (Family: none)	1-11
Y	JP 2005-11131 A (Dainippon Printing Co., Ltd.), 13 January, 2005 (13.01.05), Par. No. [0036] (Family: none)	1-11
Y	JP 2005-115519 A (Canon Inc.), 28 April, 2005 (28.04.05), Par. Nos. [0015] to [0037] (Family: none)	1-11

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 July, 2006 (24.07.06)	01 August, 2006 (01.08.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/311217

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2004-102708 A (Sharp Corp.), 02 April, 2004 (02.04.04), Full text; all drawings & US 2004/0049684 A1	2,10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３１１２１７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F3/12(2006.01)i，B41J29/38(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F3/12，B41J29/38

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 6-103008 A（株式会社リコー）1994.04.15，要約　（ファミリーなし）	1-11
Y	JP 2005-11131 A（大日本印刷株式会社）2005.01.13，段落【0036】（ファミリーなし）	1-11
Y	JP 2005-115519 A（キヤノン株式会社）2005.04.28，段落【0015】-【0037】　（ファミリーなし）	1-11

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ２４．０７．２００６	国際調査報告の発送日 ０１．０８．２００６
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｅ　９０６５ 内田　正和 電話番号　０３－３５８１－１１０１　内線　３５２１

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３１１２１７

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2004-102708 A (シャープ株式会社) 2004.04.02, 全文、全図 & US 2004/0049684 A1	2,10