

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-18741

(P2005-18741A)

(43) 公開日 平成17年1月20日(2005.1.20)

(51) Int.Cl.⁷

G06F 3/12
B41J 29/38
G06F 15/00
G06K 17/00
G06K 19/00

F I

G06F 3/12 K
G06F 3/12 D
B41J 29/38 Z
G06F 15/00 33OG
G06K 17/00 T

テーマコード (参考)

2C061
5B021
5B035
5B058
5B085

審査請求 未請求 請求項の数 26 O L (全 45 頁) 最終頁に続く

(21) 出願番号 特願2004-123156 (P2004-123156)
(22) 出願日 平成16年4月19日 (2004.4.19)
(31) 優先権主張番号 特願2003-162352 (P2003-162352)
(32) 優先日 平成15年6月6日 (2003.6.6)
(33) 優先権主張国 日本国 (JP)

(71) 出願人 000002369
セイコーエプソン株式会社
東京都新宿区西新宿2丁目4番1号
(74) 代理人 100066980
弁理士 森 哲也
(74) 代理人 100075579
弁理士 内藤 嘉昭
(74) 代理人 100103850
弁理士 崔 秀▲てつ▼
(72) 発明者 谷口 真也
長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内
(72) 発明者 空屋 銃一
長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

最終頁に続く

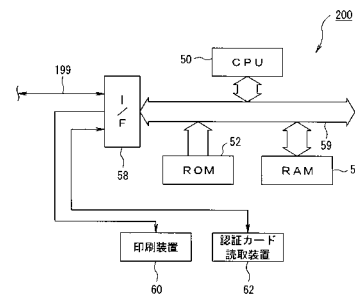
(54) 【発明の名称】 認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方

(57) 【要約】 (修正有)

【課題】 印刷データまたは印刷内容の機密を保護するのに好適な認証動作システムを提供する。

【解決手段】 ネットワークプリンタ200は、ユーザの認証カード300を読み込み、読み込んだ証明情報を印刷データ取得要求とともにユーザ端末100に送信する。ユーザ端末100は、ネットワークプリンタから取得要求と証明情報を受信すると、受信した証明情報と端末が保持している認証情報登録テーブル400の認証情報を比較して、ユーザは該印刷データの利用適格があるか否かを判定し、適格と判定したときは、端末の印刷キューから要求された印刷データをネットワークプリンタ200に送信する。ネットワークプリンタ200は受信した印刷データを印刷する。

【選択図】 図7



【特許請求の範囲】

【請求項 1】

動作データに基づいて動作を行うネットワークデバイスと、前記ネットワークデバイスを利用するデバイス利用端末とを通信可能に接続したシステムであって、

前記ネットワークデバイスは、前記動作データの利用適格を証明する証明情報を読み込み、読み込んだ証明情報を取得要求とともに前記デバイス利用端末に送信し、前記動作データを受信したときは、受信した動作データに基づいて動作を行うようになっており、

前記デバイス利用端末は、前記動作データを記憶する動作データ記憶手段と、前記動作データの利用適格を認証する認証情報を記憶する認証情報記憶手段とを有し、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記動作データの利用適格があるか否かを判定し、前記動作データの利用適格があると判定したときは、前記動作データ記憶手段の動作データを前記ネットワークデバイスに送信するようになっていることを特徴とする認証動作システム。 10

【請求項 2】

印刷データに基づいて印刷を行うネットワークプリンタと、前記ネットワークプリンタを利用するプリンタ利用端末とを通信可能に接続したシステムであって、

前記ネットワークプリンタは、前記印刷データの利用適格を証明する証明情報を読み込む証明情報読込手段と、前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷手段とを有し、 20

前記認証印刷手段は、前記証明情報読込手段で読み込んだ証明情報を取得要求とともに前記プリンタ利用端末に送信し、前記印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっており、

前記プリンタ利用端末は、前記印刷データを記憶する印刷データ記憶手段と、前記印刷データの利用適格を認証する認証情報を記憶するための認証情報記憶手段と、前記印刷データの利用適格を認証する利用適格認証手段とを有し、

前記利用適格認証手段は、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信するようになっていることを特徴とする認証印刷システム。 30

【請求項 3】

印刷データに基づいて印刷を行うネットワークプリンタと、前記ネットワークプリンタを利用するプリンタ利用端末と、プリンタ管理サーバとを通信可能に接続したシステムであって、

前記ネットワークプリンタは、前記プリンタ管理サーバから前記印刷データが記憶された前記プリンタ利用端末の位置情報を取得する位置情報取得手段と、前記印刷データの利用適格を証明する証明情報を読み込む証明情報読込手段と、前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷手段とを有し、

前記認証印刷手段は、前記証明情報読込手段で読み込んだ証明情報を取得要求とともに前記印刷データが保存されているプリンタ利用端末に送信し、当該印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっており、 40

前記プリンタ利用端末は、前記印刷データを記憶する印刷データ記憶手段と、前記印刷データの位置情報を前記プリンタ管理サーバに通知する位置情報通知手段と、前記印刷データの利用適格を認証する認証情報を記憶するための認証情報記憶手段と、前記印刷データの利用適格を認証する利用適格認証手段とを有し、

前記利用適格認証手段は、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信するようになっており、 50

前記プリンタ管理サーバは、印刷データが記憶された前記プリンタ利用端末の位置情報を登録する位置情報登録手段を有していることを特徴とする認証印刷システム。

【請求項 4】

印刷データに基づいて印刷を行うネットワークプリンタと、前記ネットワークプリンタを利用するプリンタ利用端末と、プリンタ管理サーバとを通信可能に接続したシステムであって、

前記ネットワークプリンタは、前記プリンタ管理サーバから前記印刷データが記憶された前記プリンタ利用端末の位置情報を取得する位置情報取得手段と、前記印刷データの利用適格を証明する証明情報を読み込む証明情報読込手段と、前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷手段とを有し、

10

前記認証印刷手段は、前記証明情報読込手段で読み込んだ証明情報を取得要求とともに前記プリンタ管理サーバに送信し、前記プリンタ利用端末から前記印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっており、

前記プリンタ利用端末は、前記印刷データを記憶する印刷データ記憶手段と、前記印刷データの位置情報を前記プリンタ管理サーバに通知する位置情報通知手段と、前記印刷データの利用適格を認証する認証情報を前記プリンタ管理サーバに通知する認証情報通知手段と、前記プリンタ管理サーバから送信指示があったときに前記印刷データを前記ネットワークプリンタに送信する印刷データ送信手段とを有し、

前記プリンタ管理サーバは、前記印刷データが記憶された前記プリンタ利用端末の位置情報を登録する位置情報登録手段と、前記印刷データの利用適格を認証する認証情報を記憶するための認証情報記憶手段と、前記印刷データの利用適格を認証する利用適格認証手段とを有し、

20

前記利用適格認証手段は、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記プリンタ利用端末の印刷データ送信手段に前記印刷データ記憶手段に記憶された印刷データを前記ネットワークプリンタに送信する指示を行うようになっていることを特徴とする認証印刷システム。

【請求項 5】

請求項 2～4 のいずれか 1 項に記載の認証印刷システムにおけるプリンタ利用端末と通信可能に接続するネットワークプリンタであって、

30

前記プリンタ利用端末に対して出力の制限を要求する出力制限要求手段を備え、

前記出力制限要求手段は、当該ネットワークプリンタで印刷を行うときは、前記プリンタ利用端末に出力制限要求を送信するようになっていることを特徴とするネットワークプリンタ。

【請求項 6】

印刷データの利用適格を証明するための証明情報を読み出す証明情報読込手段と、前記印刷データを取得して印刷を行う認証印刷手段とを備え、

前記認証印刷手段は、前記証明情報読込手段で読み込んだ証明情報を前記印刷データの取得要求とともに送信し、前記印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっていることを特徴とするネットワークプリンタ。

40

【請求項 7】

請求項 6 において、

プリンタ利用端末が接続されているときは、当該プリンタ利用端末に前記印刷データの出力制限を要求する送信を行う出力制限要求手段を有することを特徴とするネットワークプリンタ。

【請求項 8】

請求項 7 において、

前記出力制限要求手段は、認証用記憶媒体が与えられたときに、前記プリンタ利用端末に前記出力制限要求を送信するようになっていることを特徴とするネットワークプリンタ

50

。

【請求項 9】

請求項 7 において、

前記出力制限要求手段は、前記取得要求の送信とともに前記出力制限要求を前記プリンタ利用端末に送信するようになっていて、ことを特徴とするネットワークプリンタ。

【請求項 10】

ネットワークプリンタと通信可能に接続するプリンタ利用端末であって、

印刷データを記憶する印刷データ記憶手段と、前記印刷データの利用適格を認証する認証情報を記憶するための認証情報記憶手段と、前記印刷データの利用適格を認証する利用適格認証手段とを有し、

前記利用適格認証手段は、前記ネットワークプリンタから印刷データの取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信するようになっていて、ことを特徴とするプリンタ利用端末。

10

【請求項 11】

請求項 10 において、

前記印刷データの出力を制限する出力制限手段を備え、

前記出力制限手段は、前記ネットワークプリンタで印刷を行うときは、当該印刷以外の用途で前記印刷データの内容が出力されないように出力を制限するようになっていて、ことを特徴とするプリンタ利用端末。

20

【請求項 12】

請求項 10 において、

前記印刷データの出力を制限する出力制限手段を備え、

前記出力制限手段は、前記ネットワークプリンタから出力制限要求を受信したときは、受信した出力制限要求に係る印刷以外の用途で前記印刷データの内容が出力されないように出力を制限するようになっていて、ことを特徴とするプリンタ利用端末。

【請求項 13】

請求項 10 において、

前記印刷データの出力を制限する出力制限手段を備え、

前記出力制限手段は、印刷要求を入力したときは、表示を制限するようになっていて、ことを特徴とするプリンタ利用端末。

30

【請求項 14】

請求項 10 において、

前記印刷データの出力を制限する出力制限手段を備え、

前記出力制限手段は、前記プリンタ利用端末から前記認証用記憶媒体が取り外されたときは、表示を制限するようになっていて、ことを特徴とするプリンタ利用端末。

【請求項 15】

請求項 10～14 のいずれか 1 項において、

前記証明情報を生成する証明情報生成手段と、前記証明情報生成手段で生成した証明情報を前記認証用記憶媒体に書き込む証明情報書込手段とを有することを特徴とするプリンタ利用端末。

40

【請求項 16】

コンピュータからなるネットワークプリンタに実行させるためのプログラムであって、

与えられた認証用記憶媒体から印刷データの利用適格を証明するための証明情報を読み出す証明情報読込手段、及び前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷手段として実現される処理を実行させるためのプログラムであり、

前記認証印刷手段は、前記証明情報読込手段で読み込んだ証明情報を前記印刷データの取得要求とともに送信し、前記印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっていて、ことを特徴とするプリンタ用プログラム。

50

【請求項 17】

請求項 16 において、

プリンタ利用端末が接続されているときは、前記プリンタ利用端末に対して出力の制限を要求する出力制限要求手段として実現される処理を実行させるためのプログラムであり、

前記出力制限要求手段は、前記ネットワークプリンタで印刷を行うときは、前記プリンタ利用端末に出力制限要求を送信するようになっていることを特徴とするプリンタ用プログラム。

【請求項 18】

ネットワークプリンタと通信可能に接続するプリンタ利用端末で用いられるプログラムであって、 10

前記プリンタ利用端末のコンピュータを、

印刷データを記憶する印刷データ記憶手段と、前記印刷データの利用適格を認証する認証情報を記憶するための認証情報記憶手段と、前記印刷データの利用適格を認証する利用適格認証手段として機能させると共に、

前記利用適格認証手段は、前記ネットワークプリンタから印刷データの取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信させるようになっていることを特徴とするプリンタ利用端末用プログラム。 20

【請求項 19】

請求項 18 において、

前記印刷データの出力を制限する出力制限手段として機能させると共に、

前記出力制限手段は、前記ネットワークプリンタで印刷を行うときは、当該印刷以外の用途で前記印刷データの内容が出力されないように出力を制限するようになっていることを特徴とするプリンタ利用端末用プログラム。

【請求項 20】

コンピュータからなるネットワークプリンタに実行させるためのプログラムを記録したコンピュータ読み取り可能な記憶媒体であって、

与えられた認証用記憶媒体から印刷データの利用適格を証明するための証明情報を読み出す証明情報読込手段、及び前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷手段として実現される処理を実行させるためのプログラムであり、 30

前記認証印刷手段は、前記証明情報読込手段で読み込んだ証明情報を前記印刷データの取得要求とともに送信し、前記印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっていることを特徴とするプリンタ用プログラムを記録したコンピュータ読み取り可能な記憶媒体。

【請求項 21】

請求項 20 において、

プリンタ利用端末が接続されているときは、前記プリンタ利用端末に対して出力の制限を要求する出力制限要求手段として実現される処理を実行させるためのプログラムであり 40

、
前記出力制限要求手段は、前記ネットワークプリンタで印刷を行うときは、前記プリンタ利用端末に出力制限要求を送信するようになっていることを特徴とするプリンタ用プログラムを記録したコンピュータ読み取り可能な記憶媒体。

【請求項 22】

ネットワークプリンタと通信可能に接続するプリンタ利用端末で用いられるプログラムを記録したコンピュータ読み取り可能な記憶媒体であって、

前記プリンタ利用端末のコンピュータを、

印刷データを記憶する印刷データ記憶手段と、前記印刷データの利用適格を認証する認証情報を記憶するための認証情報記憶手段と、前記印刷データの利用適格を認証する利用 50

適格認証手段として機能させると共に、

前記利用適格認証手段は、前記ネットワークプリンタから印刷データの取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信させるようになっていることを特徴とするプリンタ利用端末用プログラムを記録したコンピュータ読み取り可能な記憶媒体。

【請求項 2 3】

請求項 2 2 において、

前記印刷データの出力を制限する出力制限手段として機能させると共に、

10

前記出力制限手段は、前記ネットワークプリンタで印刷を行うときは、当該印刷以外の用途で前記印刷データの内容が出力されないように出力を制限するようになっていることを特徴とするプリンタ利用端末用プログラムを記録したコンピュータ読み取り可能な記憶媒体。

【請求項 2 4】

印刷データに基づいて印刷を行うネットワークプリンタと、前記ネットワークプリンタを利用するプリンタ利用端末とを通信可能に接続し、前記ネットワークプリンタが前記プリンタ利用端末から前記印刷データを取得して印刷を行う方法であって、

前記ネットワークプリンタに対しては、

与えられた認証用記憶媒体から前記印刷データの利用適格を証明する証明情報を読み出す証明情報読込ステップと、前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷ステップとを含み、

20

前記認証印刷ステップは、前記証明情報読込ステップで読み込んだ証明情報を取得要求とともに前記プリンタ利用端末に送信し、前記印刷データを受信したときは、受信した印刷データに基づいて印刷を行い、

前記プリンタ利用端末に対しては、

前記印刷データを印刷データ記憶手段に記憶する印刷データ記憶ステップと、前記印刷データの利用適格を認証する認証情報を認証情報記憶手段に記憶する認証情報記憶ステップと、前記印刷データの利用適格を認証する利用適格認証ステップとを含み、

前記利用適格認証ステップは、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信することを特徴とする認証印刷方法。

30

【請求項 2 5】

印刷データに基づいて印刷を行うネットワークプリンタと通信可能に接続するプリンタ利用端末の出力を制限する方法であって、

前記プリンタ利用端末の出力を制限する出力制限ステップを含み、

前記出力制限ステップは、前記ネットワークプリンタで印刷を行うときは、当該印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限することを特徴とするプリンタ利用端末の出力制限方法。

40

【請求項 2 6】

印刷データに基づいて印刷を行うネットワークプリンタと通信可能に接続するプリンタ利用端末の出力を制限する方法であって、

前記ネットワークプリンタに対しては、

前記プリンタ利用端末に対して出力の制限を要求する出力制限要求ステップを含み、

前記出力制限要求ステップは、前記ネットワークプリンタで印刷を行うときは、前記プリンタ利用端末に出力制限要求を送信し、

前記プリンタ利用端末に対しては、

当該プリンタ利用端末の出力を制限する出力制限ステップを含み、

50

前記出力制限ステップは、前記出力制限要求を受信したときは、受信した出力制限要求に係る印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限することを特徴とするプリンタ利用端末の出力制限方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、本発明は、認証を得て印刷を行うシステム、プリンタ、端末及びプログラム、並びに方法に係り、特に、印刷データまたは印刷内容の機密を保護するのに好適な認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法に関する。に関するものである。 10

【背景技術】

【0002】

ネットワークプリンタの普及に伴い、不正アクセス等により印刷データを第三者に盗取されることがある。そのため、ネットワークプリンタには、印刷データのセキュリティ機能を設けることが要望されている。

従来、印刷データのセキュリティを向上させることを目的とした技術としては、例えば、特許文献1に開示されている画像形成システム、及び特許文献2に開示されている印刷制御装置があった。

【0003】

20

特許文献1記載の発明は、画像形成装置とネットワーク装置とをネットワークにより接続している。画像形成装置は、ネットワークを介してネットワーク装置と通信を行う通信部と、通信部により通信されるネットワーク装置が現在接続されているネットワーク環境を判定する判定部と、通信部により受信した印刷ジョブの印刷を行う印刷部と、印刷部による印刷後、判定部の判定結果に応じて印刷された印刷ジョブを削除または保持する制御部とで構成されている。ネットワーク装置は、ネットワークを介して画像形成装置に印刷ジョブを送信する通信部で構成されている。

【0004】

特許文献2記載の発明は、印刷データ及び印刷データに対応する認証情報を記憶する記憶部と、認証情報をユーザに入力させるための入力部と、記憶部に記憶されている認証情報と、入力部により入力された認証情報とを照合して、入力された認証情報に対応する印刷データの一覧を表示部に表示させる表示制御部と、表示部に表示されている一覧の中から少なくとも1つの印刷データをユーザに選択させるための選択部と、選択部により選択された印刷データに基づいて印刷を行うための印刷料金が支払われたことが確認された後に、選択された印刷データに基づく印刷を実行する制御部とで構成されている。 30

【特許文献1】特開2002-10012号公報

【特許文献2】特開2002-334150号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

40

しかしながら、特許文献1記載の発明にあっては、画像形成装置に印刷ジョブを保持する構成となっているため、ネットワーク装置でユーザが印刷要求を入力してから印刷が完了するまでの間、または印刷後も印刷ジョブを保持する場合は印刷完了後に、不正アクセス等により画像形成装置から印刷ジョブが盗取される可能性があった。ここで、特に問題となるのは、ネットワーク装置が印刷ジョブを受信してから印刷が開始されるまでの間である。この間は、印刷ジョブを保持したまま他の印刷が完了するまで待機している状態であるため、不正アクセス等により印刷ジョブが盗取されやすい。

【0006】

また、特許文献2記載の発明にあっては、印刷制御装置から印刷装置に印刷データを送信する構成となっているため、印刷データを記憶可能なメモリを有する印刷装置を利用し 50

た場合は、特許文献 1 記載の発明と同様に、不正アクセス等により印刷装置から印刷データが盗取される可能性があった。

また、ユーザが印刷を行う場合、ユーザは、ユーザ端末においてアプリケーション等から印刷要求を入力すると、ネットワークプリンタで印刷が行われる。そして、印刷物を取りにユーザ端末を離れることとなるが、ユーザ端末を離れている間に、ユーザ端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性がある。

【0007】

そこで、本発明は、このような従来の技術の有する未解決の課題に着目してなされたものであって、印刷データまたは印刷内容の機密を保護するのに好適な認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法を提供することを目的としている。 10

【課題を解決するための手段】

【0008】

〔発明 1〕前記目的を達成するために、発明 1 の認証動作システムは、動作データに基づいて動作を行うネットワークデバイスと、前記ネットワークデバイスを利用するデバイス利用端末とを通信可能に接続したシステムであって、前記ネットワークデバイスは、前記動作データの利用適格を証明する証明情報を読み込み、読み込んだ証明情報を取得要求とともに前記デバイス利用端末に送信し、前記動作データを受信したときは、受信した動作データに基づいて動作を行うようになっており、前記デバイス利用端末は、前記動作データを記憶する動作データ記憶手段と、前記動作データの利用適格を認証する認証情報を記憶する認証情報記憶手段とを有し、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記動作データの利用適格があるか否かを判定し、前記動作データの利用適格があると判定したときは、前記動作データ記憶手段の動作データを前記ネットワークデバイスに送信するようになっていることを特徴とする。 20

【0009】

このような構成であれば、ネットワークデバイスを動作させる場合、ユーザは、デバイス利用端末において動作データ記憶手段に動作データを記憶するとともに、その動作データの利用適格を証明するための証明情報を記憶した認証用記憶媒体を持ってネットワークデバイスに赴き、認証用記憶媒体をネットワークデバイスに与える。 30

ネットワークデバイスでは、認証用記憶媒体が与えられると、与えられた認証用記憶媒体から証明情報が読み出され、読み出された証明情報が取得要求とともにデバイス利用端末に送信される。

【0010】

デバイス利用端末では、取得要求とともに証明情報を受信すると、受信した証明情報及び認証情報記憶手段の認証情報に基づいて動作データの利用適格があるか否かが判定される。その結果、動作データの利用適格があると判定されると、動作データ記憶手段の動作データがネットワークデバイスに送信される。

ネットワークデバイスでは、動作データを受信すると、受信した動作データに基づいて動作が行われる。 40

【0011】

これにより、ネットワークデバイスの動作時に、デバイス利用端末の認証を得てデバイス利用端末から動作データが取得されるので、デバイス利用端末でユーザが動作要求を入力してから動作が完了するまでの間に、不正アクセス等により動作データが盗取される可能性を低減することができる。従って、従来に比して、動作データの機密を保護することができるという効果が得られる。

【0012】

また、ユーザは、ネットワークデバイスに認証用記憶媒体を与えるだけでよいので、ネットワークデバイスを動作させるための手続が比較的簡単となるという効果も得られる。 50

ここで、ネットワークデバイスは、動作データに基づいて動作を行うようになっていればどのような構成であってもよく、これには、例えば、印刷データに基づいて印刷を行うプリンタ、画像信号または画像データに基づいて表示を行うディスプレイやプロジェクタが含まれる。

【0013】

また、証明情報は、一意に識別可能な情報であって、動作データの利用適格を証明するための情報をいい、証明情報及びこれに対応する認証情報に基づいて所定の認証処理を行った場合に、動作データの利用適格があると判定されるものであればよい。

所定の認証処理としては、例えば、証明情報と認証情報とが所定関係を満たしているかを判定し、所定関係を満たしていると判定したときは、動作データの利用適格があると判定する処理が挙げられる。ここで、所定関係を満たすこととしては、例えば、証明情報と認証情報とが一致していること、証明情報を用いて所定演算式により演算を行った結果が認証情報と一致していること、または証明情報を用いて所定演算式により演算を行った結果と認証情報を用いて所定演算式により演算を行った結果が一致することが挙げられる。

【0014】

また、認証情報は、動作データの利用適格を認証するための情報をいい、認証情報及びこれに対応する証明情報に基づいて所定の認証処理を行った場合に、動作データの利用適格があると判定されるものであればよい。所定の認証処理としては、前記例と同様の処理が挙げられる。

また、動作データ記憶手段は、動作データをあらゆる手段でかつあらゆる時期に記憶するものであり、動作データをあらかじめ記憶してあるものであってもよいし、動作データをあらかじめ記憶することなく、本システムの動作時に外部からの入力等によって動作データを記憶するようになっていてもよい。このことは、認証情報記憶手段に認証情報を記憶する場合についても同様である。

【0015】

〔発明2〕一方、前記目的を達成するために、発明2の認証印刷システムは、

印刷データに基づいて印刷を行うネットワークプリンタと、前記ネットワークプリンタを利用するプリンタ利用端末とを通信可能に接続したシステムであって、前記ネットワークプリンタは、前記印刷データの利用適格を証明する証明情報を読み出す証明情報読込手段と、前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷手段とを有し、前記認証印刷手段は、前記証明情報読込手段で読み込んだ証明情報を取得要求とともに前記プリンタ利用端末に送信し、前記印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっており、前記プリンタ利用端末は、前記印刷データを記憶する印刷データ記憶手段と、前記印刷データの利用適格を認証する認証情報を記憶する認証情報記憶手段と、前記印刷データの利用適格を認証する利用適格認証手段とを有し、前記利用適格認証手段は、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信するようになっていることを特徴とする。

【0016】

このような構成であれば、ネットワークプリンタで印刷を行う場合、ユーザは、プリンタ利用端末において印刷データ記憶手段に印刷データを記憶するとともに、その印刷データの利用適格を証明するための証明情報を記憶した認証用記憶媒体を持ってネットワークプリンタに赴き、認証用記憶媒体をネットワークプリンタに与える。

ネットワークプリンタでは、認証用記憶媒体が与えられると、証明情報読込手段により、与えられた認証用記憶媒体から証明情報が読み出され、認証印刷手段により、読み出された証明情報が取得要求とともにプリンタ利用端末に送信される。

【0017】

10

20

30

40

50

プリンタ利用端末では、取得要求とともに証明情報を受信すると、利用適格認証手段により、受信した証明情報及び認証情報記憶手段の認証情報に基づいて印刷データの利用適格があるか否かが判定される。その結果、印刷データの利用適格があると判定されると、印刷データ記憶手段の印刷データがネットワークプリンタに送信される。

ネットワークプリンタでは、印刷データを受信すると、認証印刷手段により、受信した印刷データに基づいて印刷が行われる。

【0018】

これにより、ネットワークプリンタでの印刷時に、プリンタ利用端末の認証を得てプリンタ利用端末から印刷データが取得されるので、プリンタ利用端末でユーザが印刷要求を入力してから印刷が完了するまでの間に、不正アクセス等により印刷データが盗取される可能性を低減することができる。従って、従来に比して、印刷データの機密を保護することができるという効果が得られる。 10

【0019】

また、ユーザは、ネットワークプリンタに認証用記憶媒体を与えるだけでよいので、ネットワークプリンタで印刷を行うための手続が比較的簡単となるという効果も得られる。

ここで、証明情報は、印刷データの利用適格を証明するための情報をいい、証明情報及びこれに対応する認証情報に基づいて所定の認証処理を行った場合に、印刷データの利用適格があると判定されるものであればよい。所定の認証処理としては、例えば、証明情報と認証情報とが所定関係を満たしているか否かを判定し、所定関係を満たしていると判定したときは、印刷データの利用適格があると判定する処理が挙げられる。ここで、所定関係を満たすこととしては、例えば、証明情報と認証情報とが一致していること、証明情報を用いて所定演算式により演算を行った結果が認証情報と一致していること、または証明情報を用いて所定演算式により演算を行った結果と認証情報を用いて所定演算式により演算を行った結果が一致することが挙げられる。以下、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム、利用端末用プログラム、認証印刷方法において同じである。 20

【0020】

また、認証情報は、一意に識別可能な情報であって、印刷データの利用適格を認証するための情報をいい、認証情報及びこれに対応する証明情報に基づいて所定の認証処理を行った場合に、印刷データの利用適格があると判定されるものであればよい。所定の認証処理としては、前記例と同様の処理が挙げられる。以下のプリンタ利用端末、利用端末用プログラム、認証印刷方法において同じである。 30

【0021】

また、印刷データ記憶手段は、印刷データをあらゆる手段でかつあらゆる時期に記憶するものであり、印刷データをあらかじめ記憶してあるものであってもよいし、印刷データをあらかじめ記憶することなく、本システムの動作時に外部からの入力等によって印刷データを記憶するようになっていてもよい。このことは、認証情報記憶手段に認証情報を記憶する場合についても同様である。以下のプリンタ利用端末において同じである。

また、前記印刷データの利用適格を証明する証明情報は、前述したような認証用記憶媒体に限られるものでなく、他の手段、例えば、指紋や静脈パターン、虹彩等の生体情報であってもよい。 40

【0022】

〔発明3〕さらに、発明3の認証印刷システムは、

発明2の認証印刷システムにおいて、前記プリンタ利用端末は、前記証明情報を生成する証明情報生成手段と、前記証明情報生成手段で生成した証明情報を前記認証用記憶媒体に書き込む証明情報書込手段とを有することを特徴とする。

このような構成であれば、ネットワークプリンタで印刷を行う場合、ユーザは、プリンタ利用端末に認証用記憶媒体を与える。

プリンタ利用端末では、認証用記憶媒体が与えられると、証明情報生成手段により、証明情報が生成され、証明情報書込手段により、生成された証明情報が認証用記憶媒体に書 50

き込まれる。

【0023】

これにより、ユーザは、プリンタ利用端末に認証用記憶媒体を与えるだけで、印刷を行うのに必要な証明情報が認証用記憶媒体に書き込まれるので、ネットワークプリンタで印刷を行うための手続がさらに簡単となるという効果も得られる。

【0024】

〔発明4〕さらに、発明4の認証印刷システムは、

発明3の認証印刷システムにおいて、前記プリンタ利用端末は、当該プリンタ利用端末の出力を制限する出力制限手段を有し、前記出力制限手段は、前記ネットワークプリンタで印刷を行うときは、当該印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限するようになっていることを特徴とする。 10

【0025】

このような構成であれば、プリンタ利用端末では、ネットワークプリンタで印刷が行われると、出力制限手段により、その印刷以外の用途で印刷データの内容が出力されないようにプリンタ利用端末の出力が制限される。

これにより、印刷物を取りに行くためユーザがプリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができるという効果が得られる。

【0026】

ここで、出力制限手段は、ネットワークプリンタで印刷を行うときは、プリンタ利用端末の出力を制限するようになっていればどのような構成であってもよく、ネットワークプリンタで印刷を行うことの判定は、例えば、ユーザが印刷要求を入力したこと、認証用記憶媒体がプリンタ利用端末から取り外されたこと、またはネットワークプリンタからアクセスがあったことを検出することにより行うことができる。 20

【0027】

また、出力制限手段は、その印刷以外の用途で印刷データの内容が出力されないようにプリンタ利用端末の出力を制限するようになっていればどのような構成であってもよく、例えば、印刷データの内容が表示または音声出力されないようにプリンタ利用端末の表示または音声出力を制限するようになっていてもよいし、目的の印刷以外の用途で印刷データが印刷されないようにプリンタ利用端末での印刷を制限するようになっていてもよい。 30
後者の場合は、例えば、目的のネットワークプリンタ以外のネットワークプリンタに印刷データを送信することを禁止したり、目的のネットワークプリンタであっても指定部数以上の印刷となることを禁止したりする。以下の認証印刷システム、プリンタ利用端末、利用端末用プログラムにおいて同じである。

【0028】

〔発明5〕さらに、発明5の認証印刷システムは、

発明4の認証印刷システムにおいて、前記出力制限手段は、印刷要求を入力したときは、前記プリンタ利用端末の表示を制限するようになっていることを特徴とする。

このような構成であれば、プリンタ利用端末では、印刷要求を入力すると、出力制限手段により、プリンタ利用端末の表示が制限される。 40

【0029】

これにより、ユーザがプリンタ利用端末に印刷要求を入力した後は、プリンタ利用端末の表示が制限されるので、プリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性をさらに低減することができる。従って、印刷内容の機密をより確実に保護することができるという効果が得られる。

また、プリンタ利用端末に印刷要求を入力した後は、ユーザは、ネットワークプリンタに印刷物を取りに行く可能性が高く、プリンタ利用端末を継続して利用する可能性が低いので、プリンタ利用端末の表示が制限されてもユーザの利便性をさほど損なうことがない 50

という効果も得られる。

【0030】

〔発明6〕さらに、発明6の認証印刷システムは、

発明4の認証印刷システムにおいて、前記出力制限手段は、前記プリンタ利用端末から前記認証用記憶媒体が取り外されたときは、前記プリンタ利用端末の表示を制限するようになっていることを特徴とする。

【0031】

このような構成であれば、プリンタ利用端末では、プリンタ利用端末から認証用記憶媒体が取り外されると、出力制限手段により、プリンタ利用端末の表示が制限される。

これにより、ユーザがプリンタ利用端末から認証用記憶媒体を取り外した後は、プリンタ利用端末の表示が制限されるので、プリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性をさらに低減することができる。従って、印刷内容の機密をより確実に保護することができるという効果が得られる。

10

【0032】

また、プリンタ利用端末から認証用記憶媒体を取り外した後は、ユーザは、ネットワークプリンタに印刷物を取りに行く可能性が高く、プリンタ利用端末を継続して利用する可能性が低いので、プリンタ利用端末の表示が制限されてもユーザの利便性をさほど損なうことがないという効果も得られる。

20

【0033】

〔発明7〕さらに、発明7の認証印刷システムは、

発明3の認証印刷システムにおいて、前記ネットワークプリンタは、前記プリンタ利用端末に対して出力の制限を要求する出力制限要求手段を有し、前記出力制限要求手段は、前記ネットワークプリンタで印刷を行うときは、前記プリンタ利用端末に出力制限要求を送信するようになっており、前記プリンタ利用端末は、当該プリンタ利用端末の出力を制限する出力制限手段を有し、前記出力制限手段は、前記出力制限要求を受信したときは、受信した出力制限要求に係る印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限するようになっていることを特徴とする。

【0034】

このような構成であれば、ネットワークプリンタでは、ネットワークプリンタで印刷が行われると、出力制限要求手段により、プリンタ利用端末に出力制限要求が送信される。

30

プリンタ利用端末では、出力制限要求を受信すると、出力制限手段により、受信した出力制限要求に係る印刷以外の用途で印刷データの内容が出力されないようにプリンタ利用端末の出力が制限される。

【0035】

これにより、印刷物を取りに行くためユーザがプリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができるという効果が得られる。

ここで、出力制限要求手段は、ネットワークプリンタで印刷を行うときは、プリンタ利用端末に出力制限要求を送信するようになっていればどのような構成であってもよく、ネットワークプリンタで印刷を行うことの判定は、例えば、ユーザが印刷要求を入力したこと、プリンタ利用端末に取得要求を送信したこと、またはネットワークプリンタに認証用記憶媒体が与えられたことを検出することにより行うことができる。

40

【0036】

〔発明8〕さらに、発明8の認証印刷システムは、

発明7の認証印刷システムにおいて、前記出力制限要求手段は、前記ネットワークプリンタに前記認証用記憶媒体が与えられたときは、前記プリンタ利用端末に前記出力制限要求を送信するようになっており、前記出力制限手段は、前記出力制限要求を受信したときは、前記プリンタ利用端末の表示を制限するようになっていることを特徴とする。

50

【0037】

このような構成であれば、ネットワークプリンタでは、ネットワークプリンタに認証用記憶媒体が与えられると、出力制限要求手段により、プリンタ利用端末に出力制限要求が送信される。

プリンタ利用端末では、出力制限要求を受信すると、出力制限手段により、プリンタ利用端末の表示が制限される。

【0038】

これにより、ユーザがネットワークプリンタに認証用記憶媒体を与えた後は、プリンタ利用端末の表示が制限されるので、プリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性をさらに低減することができる。従って、印刷内容の機密をより確実に保護することができるという効果が得られる。 10

【0039】

また、ネットワークプリンタに認証用記憶媒体を与えた後は、ユーザは、プリンタ利用端末を離れている可能性が高いので、プリンタ利用端末の表示が制限されてもユーザの利便性をさほど損なうことがないという効果も得られる。

【0040】

〔発明9〕さらに、発明9の認証印刷システムは、

発明7の認証印刷システムにおいて、前記出力制限要求手段は、前記取得要求の送信とともに前記出力制限要求を前記プリンタ利用端末に送信するようになっており、前記出力制限手段は、前記出力制限要求を受信したときは、前記プリンタ利用端末の表示を制限するようになっていないことを特徴とする。 20

【0041】

このような構成であれば、ネットワークプリンタでは、出力制限要求手段により、取得要求の送信とともに出力制限要求がプリンタ利用端末に送信される。

プリンタ利用端末では、出力制限要求を受信すると、出力制限手段により、プリンタ利用端末の表示が制限される。

これにより、ネットワークプリンタで印刷データの取得が開始された後は、プリンタ利用端末の表示が制限されるので、プリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性をさらに低減することができる。従って、印刷内容の機密をより確実に保護することができるという効果が得られる。 30

【0042】

また、ネットワークプリンタで印刷データの取得が開始された後は、ユーザは、プリンタ利用端末を離れている可能性が高いので、プリンタ利用端末の表示が制限されてもユーザの利便性をさほど損なうことがないという効果も得られる。

【0043】

〔発明10〕また、発明10の認証印刷システムは、

印刷データに基づいて印刷を行うネットワークプリンタと、前記ネットワークプリンタを利用するプリンタ利用端末と、プリンタ管理サーバとを通信可能に接続したシステムであって、前記ネットワークプリンタは、前記プリンタ管理サーバから前記印刷データが記憶された前記プリンタ利用端末の位置情報を取得する位置情報取得手段と、前記印刷データの利用適格を証明する証明情報を読み込む証明情報読込手段と、前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷手段とを有し、前記認証印刷手段は、前記証明情報読込手段で読み込んだ証明情報を取得要求とともに前記印刷データが保存されているプリンタ利用端末に送信し、当該印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっており、前記プリンタ利用端末は、前記印刷データを記憶する印刷データ記憶手段と、前記印刷データの位置情報を前記プリンタ管理サーバに通知する位置情報通知手段と、前記印刷データの利用適格を認証する認証情報を記憶するための認証情報記憶手段と、前記印刷データの利用適格を認証する利用適格認証手段と 40 50

を有し、前記利用適格認証手段は、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信するようになっており、前記プリンタ管理サーバは、印刷データが記憶された前記プリンタ利用端末の位置情報を登録する位置情報登録手段を有していることを特徴とするものである。

【0044】

すなわち、本発明は、プリンタ管理サーバを加えたネットワークにおいて、印刷データを保存するプリンタ利用端末の位置情報（アドレス情報）をプリンタ管理サーバに通知して保存させるようにしたものである。

10

従って、ネットワークプリンタは、印刷データを取得する際には、このプリンタ管理サーバに一旦アクセスしてプリンタ利用端末の位置情報を取得してからプリンタ利用端末に前記印刷データの取得要求を前記証明情報とともに送信することになる。

【0045】

これにより、発明2と同様に、ネットワークプリンタでの印刷時に、プリンタ利用端末の認証を得てプリンタ利用端末から印刷データが取得されるので、プリンタ利用端末でユーザが印刷要求を入力してから印刷が完了するまでの間に、不正アクセス等により印刷データが盗取される可能性を低減することができる。さらに、認証用印刷媒体には、印刷データの位置情報を記録する必要がないため、認証用印刷媒体から印刷データの位置情報が盗取される可能性を低減することができる。従って、従来及び発明2のシステムに比して、印刷データの機密を保護することができるという効果が得られる。

20

【0046】

〔発明11〕また、発明11の認証印刷システムは、

印刷データに基づいて印刷を行うネットワークプリンタと、前記ネットワークプリンタを利用するプリンタ利用端末と、プリンタ管理サーバとを通信可能に接続したシステムであって、前記ネットワークプリンタは、前記プリンタ管理サーバから前記印刷データが記憶された前記プリンタ利用端末の位置情報を取得する位置情報取得手段と、前記印刷データの利用適格を証明する証明情報を読み込む証明情報読込手段と、前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷手段とを有し、前記認証印刷手段は、前記証明情報読込手段で読み込んだ証明情報を取得要求とともに前記プリンタ管理サーバに送信し、前記プリンタ利用端末から前記印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっており、前記プリンタ利用端末は、前記印刷データを記憶する印刷データ記憶手段と、前記印刷データの位置情報を前記プリンタ管理サーバに通知する位置情報通知手段と、前記印刷データの利用適格を認証する認証情報を前記プリンタ管理サーバに通知する認証情報通知手段と、前記プリンタ管理サーバから送信指示があったときに前記印刷データを前記ネットワークプリンタに送信する印刷データ送信手段とを有し、前記プリンタ管理サーバは、前記印刷データが記憶された前記プリンタ利用端末の位置情報を登録する位置情報登録手段と、前記印刷データの利用適格を認証する認証情報を記憶するための認証情報記憶手段と、前記印刷データの利用適格を認証する利用適格認証手段とを有し、前記利用適格認証手段は、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記プリンタ利用端末の印刷データ送信手段に前記印刷データ記憶手段に記憶された印刷データを前記ネットワークプリンタに送信する指示を行うようになっていることを特徴とするものである。

30

40

【0047】

すなわち、本発明は、プリンタ管理サーバを加えたネットワークにおいて、さらにそのプリンタ管理サーバに、前記印刷データの利用適格を認証する認証情報を記憶する認証情報記憶手段と、前記印刷データの利用適格を認証する利用適格認証手段とを供えたものである。

50

これにより、ネットワークプリンタでの印刷時に、プリンタ管理サーバでの認証を得てプリンタ利用端末から印刷データが取得されるので、プリンタ利用端末でユーザが印刷要求を入力してから印刷が完了するまでの間に、不正アクセス等により印刷データが盗取される可能性を低減することができる。さらに、認証用印刷媒体には、印刷データの位置情報を記録する必要がないため、認証用印刷媒体から印刷データの位置情報が盗取される可能性を低減することができる。従って、従来及び発明 2 のシステムに比して、印刷データの機密を保護することができるという効果が得られる。また、認証処理や認証情報の記憶がプリンタ管理サーバで実施されるため、プリンタ利用端末のリソースの節減にも寄与することができる。

【0048】

10

〔発明 1 2〕さらに、発明 1 2 の認証印刷システムは、

発明 1 0 又は 1 1 の認証印刷システムにおいて、前記プリンタ利用端末は、前記証明情報を生成する証明情報生成手段と、前記証明情報生成手段で生成した証明情報を前記認証用記憶媒体に書き込む証明情報書込手段とを有することを特徴とする。

これにより、発明 3 と同様に、ユーザは、プリンタ利用端末に認証用記憶媒体を与えるだけで、印刷を行うのに必要な証明情報が認証用記憶媒体に書き込まれるので、ネットワークプリンタで印刷を行うための手続がさらに簡単となるという効果も得られる。

【0049】

〔発明 1 3〕さらに、発明 1 3 の認証印刷システムは、

発明 1 0 または 1 1 の認証印刷システムにおいて、前記プリンタ利用端末は、当該プリンタ利用端末の出力を制限する出力制限手段を有し、前記出力制限手段は、前記ネットワークプリンタで印刷を行うときは、当該印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限するようになっていることを特徴とする。

20

【0050】

これにより、発明 4 と同様に、印刷物を取りに行くためユーザがプリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができるという効果が得られる。

〔発明 1 4〕さらに、発明 1 4 の認証印刷システムは、

30

発明 1 3 の認証印刷システムにおいて、前記出力制限手段は、印刷要求を入力したときは、前記プリンタ利用端末の表示を制限するようになっていることを特徴とする。

【0051】

これにより、発明 5 と同様に、ユーザがプリンタ利用端末に印刷要求を入力した後は、プリンタ利用端末の表示が制限されるので、プリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性をさらに低減することができる。従って、印刷内容の機密をより確実に保護することができるという効果が得られる。

【0052】

また、プリンタ利用端末に印刷要求を入力した後は、ユーザは、ネットワークプリンタに印刷物を取りに行く可能性が高く、プリンタ利用端末を継続して利用する可能性が低いので、プリンタ利用端末の表示が制限されてもユーザの利便性をさほど損なうことがないという効果も得られる。

40

〔発明 1 5〕さらに、発明 1 5 の認証印刷システムは、

発明 1 3 の認証印刷システムにおいて、前記出力制限手段は、前記プリンタ利用端末から前記認証用記憶媒体が取り外されたときは、前記プリンタ利用端末の表示を制限するようになっていることを特徴とする。

【0053】

これにより、発明 6 と同様に、ユーザがプリンタ利用端末から認証用記憶媒体を取り外した後は、プリンタ利用端末の表示が制限されるので、プリンタ利用端末を離れている間

50

に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性をさらに低減することができる。従って、印刷内容の機密をより確実に保護することができるという効果が得られる。

【0054】

また、プリンタ利用端末から認証用記憶媒体を取り外した後は、ユーザは、ネットワークプリンタに印刷物を取りに行く可能性が高く、プリンタ利用端末を継続して利用する可能性が低いので、プリンタ利用端末の表示が制限されてもユーザの利便性をさほど損なうことがないという効果も得られる。

【0055】

〔発明16〕さらに、発明16の認証印刷システムは、

発明10又は11の認証印刷システムにおいて、前記ネットワークプリンタは、前記プリンタ利用端末に対して出力の制限を要求する出力制限要求手段を有し、前記出力制限要求手段は、前記ネットワークプリンタで印刷を行うときは、前記プリンタ利用端末に出力制限要求を送信するようになっており、前記プリンタ利用端末は、当該プリンタ利用端末の出力を制限する出力制限手段を有し、前記出力制限手段は、前記出力制限要求を受信したときは、受信した出力制限要求に係る印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限するようになっていることを特徴とする。

10

【0056】

これにより、発明7と同様に、印刷物を取りに行くためユーザがプリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができるという効果が得られる。

20

【0057】

〔発明17〕さらに、発明17の認証印刷システムは、

発明16の認証印刷システムにおいて、前記出力制限要求手段は、前記ネットワークプリンタに前記認証用記憶媒体が与えられたときは、前記プリンタ利用端末に前記出力制限要求を送信するようになっており、前記出力制限手段は、前記出力制限要求を受信したときは、前記プリンタ利用端末の表示を制限するようになっていることを特徴とする。

【0058】

これにより、発明8と同様に、ユーザがネットワークプリンタに認証用記憶媒体を与えた後は、プリンタ利用端末の表示が制限されるので、プリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性をさらに低減することができる。従って、印刷内容の機密をより確実に保護することができるという効果が得られる。

30

【0059】

また、ネットワークプリンタに認証用記憶媒体を与えた後は、ユーザは、プリンタ利用端末を離れている可能性が高いので、プリンタ利用端末の表示が制限されてもユーザの利便性をさほど損なうことがないという効果も得られる。

【0060】

〔発明18〕さらに、発明18の認証印刷システムは、

発明16の認証印刷システムにおいて、前記出力制限要求手段は、前記取得要求の送信とともに前記出力制限要求を前記プリンタ利用端末に送信するようになっており、前記出力制限手段は、前記出力制限要求を受信したときは、前記プリンタ利用端末の表示を制限するようになっていることを特徴とする。

40

【0061】

これにより、発明9と同様に、ネットワークプリンタで印刷データの取得が開始された後は、プリンタ利用端末の表示が制限されるので、プリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性をさらに低減することができる。従って、印刷内容の機密をより確実に保護すること

50

ができるという効果が得られる。

【0062】

また、ネットワークプリンタで印刷データの取得が開始された後は、ユーザは、プリンタ利用端末を離れている可能性が高いので、プリンタ利用端末の表示が制限されてもユーザの利便性をさほど損なうことがないという効果も得られる。

【0063】

〔発明19〕一方、前記目的を達成するために、発明19のネットワークプリンタは、与えられた認証用記憶媒体から印刷データの利用適格を証明するための証明情報を読み出す証明情報読込手段と、前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷手段とを備え、前記認証印刷手段は、前記証明情報読込手段で読み込んだ証明情報を取得要求とともに前記プリンタ利用端末に送信し、前記印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっていることを特徴とする。 10

このような構成であれば、発明2の認証印刷システムにおけるネットワークプリンタと同等の作用が得られる。従って、発明2の認証印刷システムと同等の効果が得られる。

【0064】

〔発明20〕また、発明20のネットワークプリンタは、

発明19において、プリンタ利用端末が接続されているときは、当該プリンタ利用端末に前記印刷データの出力制限を要求する送信を行う出力制限要求手段を有することを特徴とするものである。

これにより、発明7と同様に、印刷物を取りに行くためユーザがプリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができるという効果が得られる。 20

【0065】

〔発明21〕また、発明21のネットワークプリンタは、

発明20において、前記出力制限要求手段は、認証用記憶媒体が与えられたときに、前記プリンタ利用端末に前記出力制限要求を送信するようになっていることを特徴とするものである。

これにより、発明8と同様に、ユーザがネットワークプリンタに認証用記憶媒体を与えた後は、プリンタ利用端末等での表示が制限されるので、プリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性をさらに低減することができる。従って、印刷内容の機密をより確実に保護することができるという効果が得られる。 30

【0066】

また、ネットワークプリンタに認証用記憶媒体を与えた後は、ユーザは、プリンタ利用端末を離れている可能性が高いので、プリンタ利用端末の表示が制限されてもユーザの利便性をさほど損なうことがないという効果も得られる。

【0067】

〔発明22〕また、発明22のネットワークプリンタは、

発明20において、前記出力制限要求手段は、前記取得要求の送信とともに前記出力制限要求を前記プリンタ利用端末に送信するようになっていることを特徴とするものである。 40

【0068】

これにより、発明9と同様に、ネットワークプリンタで印刷データの取得が開始された後は、プリンタ利用端末等での表示が制限されるので、プリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性をさらに低減することができる。従って、印刷内容の機密をより確実に保護することができるという効果が得られる。

【0069】

また、ネットワークプリンタで印刷データの取得が開始された後は、ユーザは、プリン 50

タ利用端末を離れている可能性が高いので、プリンタ利用端末の表示が制限されてもユーザの利便性をさほど損なうことがないという効果も得られる。

【0070】

〔発明23〕さらに、発明23のネットワークプリンタは、

発明7の認証印刷システムにおけるプリンタ利用端末と通信可能に接続するネットワークプリンタであって、前記プリンタ利用端末に対して出力の制限を要求する出力制限要求手段を備え、前記出力制限要求手段は、当該ネットワークプリンタで印刷を行うときは、前記プリンタ利用端末に出力制限要求を送信するようになっていることを特徴とする。

【0071】

このような構成であれば、ネットワークプリンタでは、ネットワークプリンタで印刷が行われると、出力制限要求手段により、プリンタ利用端末に出力制限要求が送信される。 10

プリンタ利用端末では、出力制限要求を受信すると、出力制限手段により、受信した出力制限要求に係る印刷以外の用途で印刷データの内容が出力されないようにプリンタ利用端末の出力が制限される。

【0072】

これにより、印刷物を取りに行くためユーザがプリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができるという効果が得られる。

ここで、出力制限要求手段は、ネットワークプリンタで印刷を行うときは、プリンタ利用端末に出力制限要求を送信するようになっていればどのような構成であってもよく、ネットワークプリンタで印刷を行うことの判定は、例えば、ユーザが印刷要求を入力したことを検出することにより行うことができる。以下、発明16のプリンタ用プログラムにおいて同じである。 20

【0073】

〔発明24〕一方、前記目的を達成するために、発明24のプリンタ利用端末は、

ネットワークプリンタと通信可能に接続するプリンタ利用端末であって、印刷データを記憶するための印刷データ記憶手段と、前記印刷データの利用適格を認証するための認証情報を記憶するための認証情報記憶手段と、前記印刷データの利用適格を認証する利用適格認証手段とを備え、前記利用適格認証手段は、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信するようになっていることを特徴とする。 30

このような構成であれば、発明2の認証印刷システムにおけるプリンタ利用端末と同等の作用が得られる。従って、発明2の認証印刷システムと同等の効果が得られる。

【0074】

〔発明25〕さらに、発明25のプリンタ利用端末は、

発明24のプリンタ利用端末において、当該プリンタ利用端末の出力を制限する出力制限手段を備え、前記出力制限手段は、前記ネットワークプリンタで印刷を行うときは、当該印刷以外の用途で前記印刷データの内容が出力されないように当該プリンタ利用端末の出力を制限するようになっていることを特徴とする。 40

【0075】

このような構成であれば、プリンタ利用端末では、ネットワークプリンタで印刷が行われると、出力制限手段により、その印刷以外の用途で印刷データの内容が出力されないようにプリンタ利用端末の出力が制限される。

これにより、印刷物を取りに行くためユーザがプリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができるという効果が得られる。 50

【0076】

ここで、出力制限手段は、ネットワークプリンタで印刷を行うときは、プリンタ利用端末の出力を制限するようになっていればどのような構成であってもよく、ネットワークプリンタで印刷を行うことの判定は、例えば、ユーザが印刷要求を入力したこと、またはネットワークプリンタからアクセスがあったことを検出することにより行うことができる。以下の利用端末用プログラム及び利用端末用プログラムを記録したコンピュータ読み取り可能な垂記憶媒体において同じである。

【0077】

〔発明26〕さらに、発明26のプリンタ利用端末は、

発明24のプリンタ利用端末において、当該プリンタ利用端末の出力を制限する出力制限手段を備え、前記出力制限手段は、前記出力制限要求を受信したときは、受信した出力制限要求に係る印刷以外の用途で前記印刷データの内容が出力されないように当該プリンタ利用端末の出力を制限するようになっていることを特徴とする。 10

【0078】

このような構成であれば、ネットワークプリンタでは、ネットワークプリンタで印刷が行われると、出力制限要求手段により、プリンタ利用端末に出力制限要求が送信される。

プリンタ利用端末では、出力制限要求を受信すると、出力制限手段により、受信した出力制限要求に係る印刷以外の用途で印刷データの内容が出力されないようにプリンタ利用端末の出力が制限される。

【0079】

これにより、印刷物を取りに行くためユーザがプリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができるという効果が得られる。 20

【0080】

〔発明27〕一方、前記目的を達成するために、発明27のプリンタ用プログラムは、

コンピュータからなるネットワークプリンタに実行させるためのプログラムであって、与えられた認証用記憶媒体から印刷データの利用適格を証明するための証明情報を読み出す証明情報読込手段、及び前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷手段として実現される処理を実行させるためのプログラムであり、前記認証印刷手段は、前記証明情報読込手段で読み込んだ証明情報を取得要求とともに前記プリンタ利用端末に送信し、前記印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっていることを特徴とする。 30

このような構成であれば、ネットワークプリンタによってプログラムが読み取られ、読み取られたプログラムに従ってネットワークプリンタが処理を実行すると、発明10のネットワークプリンタと同等の作用及び効果が得られる。

【0081】

〔発明28〕さらに、発明28のプリンタ用プログラムは、

コンピュータからなるネットワークプリンタに実行させるためのプログラムであって、前記プリンタ利用端末に対して出力の制限を要求する出力制限要求手段として実現される処理を実行させるためのプログラムであり、前記出力制限要求手段は、前記ネットワークプリンタで印刷を行うときは、前記プリンタ利用端末に出力制限要求を送信するようになっていることを特徴とする。 40

このような構成であれば、ネットワークプリンタによってプログラムが読み取られ、読み取られたプログラムに従ってネットワークプリンタが処理を実行すると、発明11のネットワークプリンタと同等の作用及び効果が得られる。

【0082】

〔発明29〕一方、前記目的を達成するために、発明29のプリンタ利用端末用プログラムは、

コンピュータからなるプリンタ利用端末に実行させるためのプログラムであって、前記 50

印刷データの利用適格を認証する利用適格認証手段として実現される処理を実行させるためのプログラムであり、前記利用適格認証手段は、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信するようになっていることを特徴とする。

このような構成であれば、プリンタ利用端末によってプログラムが読み取られ、読み取られたプログラムに従ってプリンタ利用端末が処理を実行すると、発明 14 のプリンタ利用端末と同等の作用及び効果が得られる。

【0083】

10

〔発明 30〕さらに、発明 30 のプリンタ利用端末用プログラムは、

コンピュータからなるプリンタ利用端末に実行させるためのプログラムであって、前記プリンタ利用端末の出力を制限する出力制限手段として実現される処理を実行させるためのプログラムであり、前記出力制限手段は、前記ネットワークプリンタで印刷を行うときは、当該印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限するようになっていることを特徴とする。

このような構成であれば、プリンタ利用端末によってプログラムが読み取られ、読み取られたプログラムに従ってプリンタ利用端末が処理を実行すると、発明 15 のプリンタ利用端末と同等の作用及び効果が得られる。

【0084】

20

〔発明 31〕さらに、発明 31 のプリンタ利用端末用プログラムは、

コンピュータからなるプリンタ利用端末に実行させるためのプログラムであって、前記プリンタ利用端末の出力を制限する出力制限手段として実現される処理を実行させるためのプログラムであり、前記出力制限手段は、前記出力制限要求を受信したときは、受信した出力制限要求に係る印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限するようになっていることを特徴とする。

このような構成であれば、プリンタ利用端末によってプログラムが読み取られ、読み取られたプログラムに従ってプリンタ利用端末が処理を実行すると、発明 16 のプリンタ利用端末と同等の作用及び効果が得られる。

【0085】

30

〔発明 32〕さらに、発明 32 のプリンタ利用端末用プログラムを記録したコンピュータ読み取り可能な記憶媒体は、

コンピュータからなるプリンタ利用端末に実行させるためのプログラムであって、前記印刷データの利用適格を認証する利用適格認証手段として実現される処理を実行させるためのプログラムであり、前記利用適格認証手段は、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信するようになっていることを特徴とするものである。

このような構成であれば、プリンタ利用端末によって記録媒体に記録された利用端末用プログラムが読み取られ、読み取られたプログラムに従ってプリンタ利用端末が処理を実行すると、発明 14 のプリンタ利用端末と同等の作用及び効果が得られる。

40

【0086】

〔発明 33〕さらに、発明 33 のプリンタ利用端末用プログラムを記録したコンピュータ読み取り可能な記憶媒体は、

コンピュータからなるプリンタ利用端末に実行させるためのプログラムであって、前記プリンタ利用端末の出力を制限する出力制限手段として実現される処理を実行させるためのプログラムであり、前記出力制限手段は、前記ネットワークプリンタで印刷を行うときは、当該印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限するようになっていることを特徴とするものである。

50

このような構成であれば、プリンタ利用端末によって記録媒体に記録された利用端末用プログラムが読み取られ、読み取られたプログラムに従ってプリンタ利用端末が処理を実行すると、発明 15 のプリンタ利用端末と同等の作用及び効果が得られる。

【0087】

〔発明 34〕さらに、発明 34 のプリンタ利用端末用プログラムを記録したコンピュータ読み取り可能な記憶媒体は、

コンピュータからなるプリンタ利用端末に実行させるためのプログラムであって、前記プリンタ利用端末の出力を制限する出力制限手段として実現される処理を実行させるためのプログラムであり、前記出力制限手段は、前記出力制限要求を受信したときは、受信した出力制限要求に係る印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限するようになっていることを特徴とするものである。 10

このような構成であれば、プリンタ利用端末によって記録媒体に記録された利用端末用プログラムが読み取られ、読み取られたプログラムに従ってプリンタ利用端末が処理を実行すると、発明 16 のプリンタ利用端末と同等の作用及び効果が得られる。

【0088】

〔発明 35〕一方、前記目的を達成するために、発明 35 の認証印刷方法は、

印刷データに基づいて印刷を行うネットワークプリンタと、前記ネットワークプリンタを利用するプリンタ利用端末とを通信可能に接続し、前記ネットワークプリンタが前記プリンタ利用端末から前記印刷データを取得して印刷を行う方法であって、前記ネットワークプリンタに対しては、与えられた認証用記憶媒体から前記印刷データの利用適格を証明するための証明情報を読み出す証明情報読込ステップと、前記プリンタ利用端末から前記印刷データを取得して印刷を行う認証印刷ステップとを含み、前記認証印刷ステップは、前記証明情報読込ステップで読み込んだ証明情報を取得要求とともに前記プリンタ利用端末に送信し、前記印刷データを受信したときは、受信した印刷データに基づいて印刷を行い、前記プリンタ利用端末に対しては、前記印刷データを印刷データ記憶手段に記憶する印刷データ記憶ステップと、前記印刷データの利用適格を認証するための認証情報を認証情報記憶手段に記憶する認証情報記憶ステップと、前記印刷データの利用適格を認証する利用適格認証ステップとを含み、前記利用適格認証ステップは、前記取得要求とともに前記証明情報を受信したときは、受信した証明情報及び前記認証情報記憶手段の認証情報に基づいて前記印刷データの利用適格があるか否かを判定し、前記印刷データの利用適格があると判定したときは、前記印刷データ記憶手段の印刷データを前記ネットワークプリンタに送信することを特徴とする。 20 30

これにより、発明 2 の認証印刷システムと同等の効果が得られる。

【0089】

〔発明 36〕一方、前記目的を達成するために、発明 36 のプリンタ利用端末の出力制限方法は、

印刷データに基づいて印刷を行うネットワークプリンタと通信可能に接続するプリンタ利用端末の出力を制限する方法であって、前記プリンタ利用端末の出力を制限する出力制限ステップを含み、前記出力制限ステップは、前記ネットワークプリンタで印刷を行うときは、当該印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限することを特徴とする。 40

【0090】

これにより、印刷物を取りに行くためユーザがプリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができるという効果が得られる。

ここで、出力制限ステップは、ネットワークプリンタで印刷を行うときは、プリンタ利用端末の出力を制限すればどのような方法であってもよく、ネットワークプリンタで印刷を行うことの判定は、例えば、ユーザが印刷要求を入力したこと、またはネットワークプリンタからアクセスがあったことを検出することにより行うことができる。 50

【0091】

〔発明37〕さらに、発明37のプリンタ利用端末の出力制限方法は、

印刷データに基づいて印刷を行うネットワークプリンタと通信可能に接続するプリンタ利用端末の出力を制限する方法であって、前記ネットワークプリンタに対しては、前記プリンタ利用端末に対して出力の制限を要求する出力制限要求ステップを含み、前記出力制限要求ステップは、前記ネットワークプリンタで印刷を行うときは、前記プリンタ利用端末に出力制限要求を送信し、前記プリンタ利用端末に対しては、当該プリンタ利用端末の出力を制限する出力制限ステップを含み、前記出力制限ステップは、前記出力制限要求を受信したときは、受信した出力制限要求に係る印刷以外の用途で前記印刷データの内容が出力されないように前記プリンタ利用端末の出力を制限することを特徴とする。

10

【0092】

これにより、印刷物を取りに行くためユーザがプリンタ利用端末を離れている間に、プリンタ利用端末のディスプレイ等で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができるという効果が得られる。

ここで、出力制限要求ステップは、ネットワークプリンタで印刷を行うときは、プリンタ利用端末に出力制限要求を送信すればどのような方法であってもよく、ネットワークプリンタで印刷を行うことの判定は、例えば、ユーザが印刷要求を入力したことを検出することにより行うことができる。

【発明を実施するための最良の形態】

20

【0093】

以下、本発明の第1の実施の形態を図面を参照しながら説明する。

図1ないし図9は、本発明に係る認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法の実施の第1の形態を示す図である。

本実施の形態は、本発明に係る認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法を、図1に示すように、認証カード300を利用してネットワークプリンタ200で印刷を行う場合について適用したものである。

30

【0094】

まず、本発明を適用するネットワークシステムの構成を図1を参照しながら説明する。

図1は、本発明を適用するネットワークシステムの構成を示すブロック図である。

インターネット199には、図1に示すように、複数のユーザ端末100と、複数のネットワークプリンタ200とが接続されている。

ネットワークプリンタ200で印刷を行う場合、ユーザは、ユーザ端末100において認証カード300に必要な情報を書き込み、認証カード300をネットワークプリンタ200に挿入する。そして、認証カード300の情報が正当なものである場合は、ネットワークプリンタ200で印刷が行われる。ここで、認証カード300は、例えば、書換可能な不揮発性メモリやRFID(Radio Frequency Identification)非接触型ICタグとして構成されている。

40

【0095】

次に、ユーザ端末100の構成を図2を参照しながら詳細に説明する。

図2は、ユーザ端末100の構成を示すブロック図である。

ユーザ端末100は、図2に示すように、制御プログラムに基づいて演算及びシステム全体を制御するCPU30と、所定領域にあらかじめCPU30の制御プログラム等を格納しているROM32と、ROM32等から読み込んだデータやCPU30の演算過程に必要な演算結果を格納するためのRAM34と、外部装置に対してデータの入出力を媒介するI/F38とで構成されており、これらは、データを転送するための信号線であるバス39で相互にかつデータ授受可能に接続されている。

50

【0096】

I / F 3 8 には、外部装置として、ヒューマンインターフェースとしてデータの入力可能なキーボードやマウス等からなる入力装置 4 0 と、印刷データやテーブル等をファイルとして格納する記憶装置 4 2 と、画像信号に基づいて画面を表示する表示装置 4 4 と、認証カード 3 0 0 に対して情報の読込及び書込を行う認証カード読取装置 4 6 と、インターネット 1 9 9 に接続するための信号線とが接続されている。

【0097】

記憶装置 4 2 には、印刷データの利用適格を認証するための認証情報を登録する認証情報登録テーブルが格納されている。

図 3 は、認証情報登録テーブル 4 0 0 のデータ構造を示す図である。

10

認証情報登録テーブル 4 0 0 には、図 3 に示すように、各印刷ジョブごとに 1 つのレコードが登録される。各レコードは、ユーザ名を登録するフィールド 4 0 2 と、パスワードを登録するフィールド 4 0 4 と、印刷データのファイル名を登録するフィールド 4 0 6 とを含んで構成されている。

【0098】

図 3 の例では、第 1 段目のレコードには、ユーザ名として「t a r o」が、パスワードとして「1 2 3 4 a b c」が、印刷データのファイル名として「P r i n t d a t a 1 . d a t」がそれぞれ登録されている。これは、ユーザ名「t a r o」というユーザが行った印刷要求に係る印刷データのファイル名が「P r i n t d a t a 1 . d a t」であり、ネットワークプリンタ 2 0 0 がその印刷データを取得するために必要なパスワードが「1 2 3 4 a b c」であることを示している。

20

【0099】

C P U 3 0 は、マイクロプロセッシングユニット (M P U) 等からなり、R O M 3 2 の所定領域に格納されている所定のプログラムを起動させ、そのプログラムに従って、図 4 及び図 6 のフローチャートに示す印刷開始処理及び利用適格認証処理をそれぞれ時分割で実行するようになっている。

初めに、印刷開始処理を図 4 を参照しながら詳細に説明する。

【0100】

図 4 は、印刷開始処理を示すフローチャートである。

印刷開始処理は、ユーザからの印刷要求に応じて印刷を開始する処理であって、C P U 3 0 において実行されると、図 4 に示すように、まず、ステップ S 1 0 0 に移行するようになっている。

30

ステップ S 1 0 0 では、印刷要求を入力装置 4 0 から入力したか否かを判定し、印刷要求を入力したと判定したとき (Y e s) は、ステップ S 1 0 2 に移行するが、そうでないと判定したとき (N o) は、印刷要求を入力するまでステップ S 1 0 0 で待機する。

【0101】

ステップ S 1 0 2 では、印刷データを生成し、ステップ S 1 0 4 に移行して、生成した印刷データを記憶装置 4 2 に登録する。記憶装置 4 2 への登録は、生成した印刷データをそのファイル名と対応付けて記憶装置 4 2 のキュー方式の記憶領域 (以下、印刷キューという。) の末尾に登録することにより行う。印刷キューは、印刷要求のあった順に印刷データを末尾に登録し、先頭から順に印刷データを処理するものである。

40

【0102】

次いで、ステップ S 1 0 6 に移行して、認証カード読取装置 4 6 に認証カード 3 0 0 が挿入されているか否かを判定し、認証カード 3 0 0 が挿入されていると判定したとき (Y e s) は、ステップ S 1 0 8 に移行する。

ステップ S 1 0 8 では、ステップ S 1 0 4 で登録した印刷データについてその利用適格を認証するための認証情報及びその利用適格を証明するための証明情報をそれぞれ生成し、ステップ S 1 1 0 に移行して、生成した認証情報を認証情報登録テーブル 4 0 0 に登録し、ステップ S 1 1 2 に移行する。

【0103】

50

ステップS112では、生成した証明情報及び印刷データを保存した印刷キューへのアクセス情報（印刷データの位置情報）を認証カード読取装置46により認証カード300に書き込む。

図5は、認証カード300に書き込む証明情報及びアクセス情報のデータ構造を示す図である。

【0104】

認証カード300には、図5に示すように、認証情報登録テーブル400のフィールド402～406と同一の内容が証明情報420～424として登録され、ユーザ端末100の印刷キューのネットワーク上のアドレスがアクセス情報426として登録される。

図5の例では、ユーザ名として「t a r o」が、パスワードとして「1 2 3 4 a b c」が、印刷データのファイル名として「P r i n t d a t a 1 . d a t」が、アクセス情報として「h t t p : / / t a r o - p c . j p / q u e u e /」がそれぞれ登録されている。これは、ユーザ名「t a r o」というユーザが行った印刷要求に係る印刷データのファイル名が「P r i n t d a t a 1 . d a t」であり、ネットワークプリンタ200がその印刷データを取得するために必要なパスワードが「1 2 3 4 a b c」であり、その印刷データがアドレス「h t t p : / / t a r o - p c . j p / q u e u e /」から取得可能であることを示している。 10

【0105】

次いで、ステップS114に移行して、ユーザ端末100を低消費電力モードに設定し、ステップS116に移行して、ユーザ端末100の表示画面をロックし、一連の処理を終了して元の処理に復帰させる。 20

低消費電力モードでは、電力の低消費化を図るため記憶装置42の駆動や表示装置44の表示を抑制する。また、表示画面のロック状態では、少なくとも印刷内容が表示されないように表示装置44の表示を制限する。低消費電力モード及び画面ロックは、例えば、ユーザが所定のパスワードを入力することにより解除することができる。

【0106】

一方、ステップS106で、認証カード読取装置46に認証カード300が挿入されていないと判定したとき（N o）は、ステップS118に移行して、認証カード300の挿入をユーザに対して要求し、ステップS106に移行する。

次に、利用適格認証処理を図6を参照しながら詳細に説明する。 30

図6は、利用適格認証処理を示すフローチャートである。

【0107】

利用適格認証処理は、ネットワークプリンタ200からの取得要求に応じて印刷データの利用適格を認証する処理であって、CPU30において実行されると、図6に示すように、まず、ステップS150に移行するようになっている。

ステップS150では、印刷データの取得要求を受信したか否かを判定し、取得要求を受信したと判定したとき（Y e s）は、ステップS152に移行するが、そうでないと判定したとき（N o）は、取得要求を受信するまでステップS150で待機する。

【0108】

ステップS152では、証明情報を受信し、ステップS154に移行して、受信した証明情報及び認証情報登録テーブル400の認証情報に基づいて印刷データの利用適格があるか否かを判定する。まず、証明情報に含まれるファイル名と同一のファイル名が登録されているレコードを認証情報登録テーブル400から検索し、検索により該当レコードを索出したときは、証明情報に含まれるユーザ名及びパスワードと、該当レコードのユーザ名及びパスワードとが一致しているか否かを判定し、一致していると判定したときは、印刷データの利用適格があると判定する。これに対し、該当レコードを索出できないとき、または該当レコードを索出したがユーザ名またはパスワードが一致しないと判定したときは、印刷データの利用適格がないと判定する。 40

【0109】

次いで、ステップS156に移行して、印刷データの利用適格があるとの認証が得られ 50

たか否かを判定し、認証が得られたと判定したとき（Ｙｅｓ）は、ステップＳ１５８に移行して、取得要求のあったネットワークプリンタ２００（以下、要求元ネットワークプリンタ２００という。）に認証通知を送信し、ステップＳ１６０に移行する。

ステップＳ１６０では、要求元ネットワークプリンタ２００から接続要求を受信したか否かを判定し、接続要求を受信したと判定したとき（Ｙｅｓ）は、ステップＳ１６２に移行するが、そうでないと判定したとき（Ｎｏ）は、接続要求を受信するまで所定時間を限度として待機する。

【０１１０】

ステップＳ１６２では、受信した証明情報に含まれるファイル名の印刷データを印刷キューから読み込み、読み込んだ印刷データを要求元ネットワークプリンタ２００に送信し、ステップＳ１６３に移行して、受信した証明情報に含まれるファイル名の印刷データを印刷キューから削除し、一連の処理を終了して元の処理に復帰させる。 10

一方、ステップＳ１５６で、印刷データの利用適格があるとの認証が得られないと判定したとき（Ｎｏ）は、ステップＳ１６４に移行して、要求元ネットワークプリンタ２００に否認通知を送信し、一連の処理を終了して元の処理に復帰させる。

【０１１１】

次に、ネットワークプリンタ２００の構成を図７を参照しながら詳細に説明する。

図７は、ネットワークプリンタ２００の構成を示すブロック図である。

ネットワークプリンタ２００は、図７に示すように、制御プログラムに基づいて演算及びシステム全体を制御するＣＰＵ５０と、所定領域にあらかじめＣＰＵ５０の制御プログラム等を格納しているＲＯＭ５２と、ＲＯＭ５２等から読み込んだデータやＣＰＵ５０の演算過程で必要な演算結果を格納するためのＲＡＭ５４と、外部装置に対してデータの入出力を媒介するＩ／Ｆ５８とで構成されており、これらは、データを転送するための信号線であるバス５９で相互にかつデータ授受可能に接続されている。 20

【０１１２】

Ｉ／Ｆ５８には、外部装置として、印刷データに基づいて印刷を行う印刷装置６０と、認証カード３００に対して情報の読込及び書込を行う認証カード読取装置６２と、インターネット１９９に接続するための信号線とが接続されている。

ＣＰＵ５０は、マイクロプロセッシングユニット（ＭＰＵ）等からなり、ＲＯＭ５２の所定領域に格納されている所定のプログラムを起動させ、そのプログラムに従って、図８のフローチャートに示す認証印刷処理を実行するようになっている。 30

【０１１３】

図８は、認証印刷処理を示すフローチャートである。

認証印刷処理は、認証カード読取装置６２に認証カード３００が挿入されたときは、ユーザ端末１００から印刷データを取得して印刷を行う処理であって、ＣＰＵ５０において実行されると、図８に示すように、まず、ステップＳ２００に移行するようになっている。

【０１１４】

ステップＳ２００では、認証カード読取装置６２に認証カード３００が挿入されたか否かを判定し、認証カード３００が挿入されたと判定したとき（Ｙｅｓ）は、ステップＳ２０６に移行するが、そうでないと判定したとき（Ｎｏ）は、認証カード３００が挿入されるまでステップＳ２００で待機する。 40

ステップＳ２０６では、ネットワークプリンタ２００が現在印刷中であるか否かを判定し、印刷中でないと判定したとき（Ｎｏ）は、ステップＳ２０８に移行するが、そうでないと判定したとき（Ｙｅｓ）は、ステップＳ２００に移行する。

【０１１５】

ステップＳ２０８では、認証カード読取装置６２により証明情報及びアクセス情報を認証カード３００から読み込み、ステップＳ２１０に移行して、読み込んだアクセス情報に基づいてユーザ端末１００に取得要求を送信し、ステップＳ２１２に移行して、読み込んだアクセス情報に基づいてユーザ端末１００に証明情報を送信し、ステップＳ２１４に移 50

行する。

【0116】

ステップS214では、認証通知を受信したか否かを判定し、認証通知を受信したと判定したとき（Yes）は、ステップS216に移行して、読み込んだアクセス情報に基づいてユーザ端末100に接続要求を送信し、ステップS218に移行して、印刷データを受信し、ステップS220に移行する。

ステップS220では、受信した印刷データに基づいて印刷装置60により印刷を行い、ステップS222に移行して、認証カード読取装置62により証明情報及びアクセス情報を認証カード300から消去し、一連の処理を終了して元の処理に復帰させる。

【0117】

一方、ステップS214で、認証通知を受信しないと判定したとき（No）は、ステップS224に移行して、否認通知を受信したか否かを判定し、否認通知を受信したと判定したとき（Yes）は、一連の処理を終了して元の処理に復帰させるが、そうでないと判定したとき（No）は、ステップS214に移行する。

次に、本実施の形態の動作を図9を参照しながら説明する。

【0118】

図9は、実施の形態の動作を説明するための図である。

ネットワークプリンタ200で印刷を行う場合、ユーザは、ユーザ端末100において、図9（1）に示すように、まず、認証カード読取装置46に認証カード300を挿入するとともに印刷要求を入力装置40から入力する。

ユーザ端末100では、認証カード300が挿入された状態で印刷要求が入力されると、図9（2）に示すように、ステップS102、S104を経て、印刷データが生成され、生成された印刷データが印刷キューに登録される。次いで、ステップS108～S112を経て、登録された印刷データについて認証情報及び証明情報がそれぞれ生成され、生成された認証情報が認証情報登録テーブル400に登録され、生成された証明情報及びアクセス情報が認証カード読取装置46により認証カード300に書き込まれる。そして、ステップS114、S116を経て、ユーザ端末100が低消費電力モードに設定され、ユーザ端末100の表示画面がロックされる。

【0119】

次に、ユーザは、認証カード300を持ってネットワークプリンタ200に赴き、図9（3）に示すように、認証カード読取装置62に認証カード300を挿入する。

ネットワークプリンタ200では、認証カード300が挿入されると、印刷可能となるまで待機した後、ステップS208～S212を経て、認証カード読取装置62により証明情報及びアクセス情報が認証カード300から読み出され、読み出されたアクセス情報に基づいて証明情報が取得要求とともにユーザ端末100に送信される。

【0120】

ユーザ端末100では、取得要求とともに証明情報を受信すると、ステップS154を経て、受信した証明情報及び認証情報登録テーブル400の認証情報に基づいて印刷データの利用適格があるか否かが判定される。その結果、印刷データの利用適格があると判定されると、ステップS158を経て、要求元ネットワークプリンタ200に認証通知が送信される。

【0121】

ネットワークプリンタ200では、認証通知を受信すると、図9（4）に示すように、ステップS216を経て、アクセス情報に基づいてユーザ端末100に接続要求が送信される。

ユーザ端末100では、要求元ネットワークプリンタ200から接続要求を受信すると、ステップS162を経て、受信した証明情報に含まれるファイル名の印刷データが印刷キューから読み出され、読み出された印刷データが要求元ネットワークプリンタ200に送信される。また、ステップS163を経て、受信した証明情報に含まれるファイル名の印刷データが印刷キューから削除される。

10

20

30

40

50

【0122】

ネットワークプリンタ200では、印刷データを受信すると、図9(5)に示すように、ステップS220を経て、受信した印刷データに基づいて印刷装置60により印刷が行われる。また、ステップS222を経て、認証カード読取装置62により証明情報及びアクセス情報が認証カード300から消去される。

なお、例えば、不正な証明情報を記憶した認証カード300や、証明情報またはアクセス情報が記憶されていない認証カード300をネットワークプリンタ200に与えた場合は、ユーザ端末100では、印刷データの利用適格がないと判定されるので、ステップS164を経て、要求元ネットワークプリンタ200に否認通知が送信される。

【0123】

ネットワークプリンタ200では、否認通知を受信すると、ステップS224を経て、印刷データの取得及び印刷が行われることなく処理が終了する。

このようにして、本実施の形態では、ネットワークプリンタ200は、与えられた認証カード300から証明情報を読み込み、読み込んだ証明情報を取得要求とともにユーザ端末100に送信し、印刷データを受信したときは、受信した印刷データに基づいて印刷を行うようになっており、ユーザ端末100は、取得要求とともに証明情報を受信したときは、受信した証明情報及び認証情報登録テーブル400の認証情報に基づいて印刷データの利用適格があるか否かを判定し、印刷データの利用適格があると判定したときは、印刷キューの印刷データをネットワークプリンタ200に送信するようになっている。

【0124】

これにより、ネットワークプリンタ200での印刷時に、ユーザ端末100の認証を得てユーザ端末100から印刷データが取得されるので、ユーザ端末100でユーザが印刷要求を入力してから印刷が完了するまでの間に、不正アクセス等により印刷データが盗取される可能性を低減することができる。従って、従来に比して、印刷データの機密を保護することができる。

【0125】

また、ユーザは、ネットワークプリンタ200に認証カード300を与えるだけでよいので、ネットワークプリンタ200で印刷を行うための手続が比較的簡単となる。

また、ネットワークプリンタ200が障害等により印刷不能である場合、従来の一般的な方式では、ユーザ端末100が印刷データの送信を所定周期で試行する。そのため、ネットワークのトラフィックが増大する可能性がある。これに対して、本実施の形態では、ネットワークプリンタ200が確実に印刷可能となっているときに印刷データの送受信を行うようになっているので、ネットワークのトラフィックが増大するのを抑制することができる。

【0126】

さらに、本実施の形態では、ユーザ端末100は、証明情報を生成し、生成した証明情報を認証カード300に書き込むようになっている。

これにより、ユーザは、ユーザ端末100に認証カード300を与えるだけで、印刷を行うのに必要な証明情報が認証カード300に書き込まれるので、ネットワークプリンタ200で印刷を行うための手続がさらに簡単となる。

【0127】

さらに、本実施の形態では、ユーザ端末100は、印刷要求を入力したときは、ユーザ端末100の表示画面をロックするようになっている。

これにより、ユーザがユーザ端末100に印刷要求を入力した後は、ユーザ端末100の表示が制限されるので、ユーザ端末100を離れている間に、ユーザ端末100の表示装置44で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができる。

【0128】

また、ユーザ端末100に印刷要求を入力した後は、ユーザは、ネットワークプリンタ200に印刷物を取りに行く可能性が高く、ユーザ端末100を継続して利用する可能性

10

20

30

40

50

が低いので、ユーザ端末１００の表示が制限されてもユーザの利便性をさほど損なうことがない。

さらに、本実施の形態では、ユーザ端末１００は、印刷要求を入力したときは、ユーザ端末１００を低消費電力モードに設定するようになっている。

【０１２９】

これにより、ユーザがユーザ端末１００に印刷要求を入力した後は、ユーザ端末１００が低消費電力モードに設定されるので、ユーザ端末１００を離れている間に、ユーザ端末１００の電力が無駄に消費されるのを抑えることができる。従って、ユーザ端末１００の消費電力を低減することができる。

また、ユーザ端末１００に印刷要求を入力した後は、ユーザは、ネットワークプリンタ２００に印刷物を取りに行く可能性が高く、ユーザ端末１００を継続して利用する可能性が低いので、ユーザ端末１００が低消費電力モードに設定されてもユーザの利便性をさほど損なうことがない。

【０１３０】

前記第１の実施の形態において、印刷データは、発明１の動作データに対応し、ユーザ端末１００は、発明１のデバイス利用端末、または発明２等のプリンタ利用端末に対応し、記憶装置４２は、発明１の動作データ記憶手段、発明２等の印刷データ記憶手段、または発明１、２等の認証情報記憶手段に対応している。また、ステップＳ１０８は、発明３の証明情報生成手段に対応し、ステップＳ１１２は、発明３の証明情報書込手段に対応し、ステップＳ１１６は、発明４等の出力制限手段、及び出力制限ステップに対応している。

【０１３１】

また、前記第１の実施の形態において、ステップＳ１５０～Ｓ１６２は、発明２等の利用適格認証手段、及び利用適格認証ステップに対応し、ネットワークプリンタ２００は、発明１等のネットワークデバイスに対応し、ステップＳ２０８は、発明２等の証明情報読込手段、及び証明情報読込ステップに対応している。また、ステップＳ２１０～Ｓ２２０は、発明２等の認証印刷手段、及び認証印刷ステップに対応し、認証カード３００は、発明１等の認証用記憶媒体に対応している。

【０１３２】

次に、本発明の実施の第２の形態を図面を参照しながら説明する。

図１０は、本発明に係る認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法の実施の第２の形態を示す図である。

本実施の形態は、本発明に係る認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法を、図１に示すように、認証カード３００を利用してネットワークプリンタ２００で印刷を行う場合について適用したものであり、前記第１の実施の形態と異なるのは、ユーザ端末１００から認証カード３００を取り外したときに低消費電力モードの設定及び画面ロックを行う点にある。なお、以下、前記第１の実施の形態と異なる部分についてのみ説明し、重複する部分については同一の符号を付して説明を省略する。

【０１３３】

まず、ユーザ端末１００の構成を図１０を参照しながら説明する。

ユーザ端末１００は、図４及び図６のフローチャートに示す印刷開始処理及び利用適格認証処理に加えて、図１０のフローチャートに示す表示禁止処理を実行するようになっている。なお、図４の印刷開始処理については、ステップＳ１１４、Ｓ１１６の処理は実行しない。

【０１３４】

図１０は、表示禁止処理を示すフローチャートである。

表示禁止処理は、認証カード読取装置４６から認証カード３００が取り外されたときは

、表示装置 44 の表示を禁止する処理であって、CPU 30 において実行されると、図 10 に示すように、まず、ステップ S 300 に移行するようになっている。

ステップ S 300 では、認証カード読取装置 46 に認証カード 300 が挿入されているか否かを判定し、認証カード 300 が挿入されていないと判定したとき (Yes) は、ステップ S 302 に移行して、ユーザ端末 100 を低消費電力モードに設定し、ステップ S 304 に移行して、ユーザ端末 100 の表示画面をロックし、一連の処理を終了して元の処理に復帰させる。

【0135】

一方、ステップ S 300 で、認証カード読取装置 46 に認証カード 300 が挿入されていると判定したとき (Yes) は、ステップ S 306 に移行して、認証カード読取装置 46 により証明情報を認証カード 300 から読み込み、ステップ S 308 に移行して、読み込んだ証明情報及び認証情報登録テーブル 400 の認証情報に基づいて印刷データの利用適格があるか否かを判定し、ステップ S 310 に移行する。

10

【0136】

ステップ S 310 では、印刷データの利用適格があるとの認証が得られたか否かを判定し、認証が得られたと判定したとき (Yes) は、ステップ S 312 に移行して、ユーザ端末 100 が低消費電力モードに設定されている場合は低消費電力モードを解除し、ステップ S 314 に移行して、ユーザ端末 100 の表示画面がロックされている場合は画面ロックを解除し、一連の処理を終了して元の処理に復帰させる。

【0137】

20

一方、ステップ S 310 で、印刷データの利用適格があるとの認証が得られないと判定したとき (No) は、一連の処理を終了して元の処理に復帰させる。

次に、本実施の形態の動作を説明する。

ネットワークプリンタ 200 で印刷を行う場合、ユーザは、ユーザ端末 100 において、印刷要求を入力した後、認証カード読取装置 46 から認証カード 300 を取り外し、認証カード 300 を持ってネットワークプリンタ 200 に赴く。

【0138】

ユーザ端末 100 では、認証カード 300 が取り外されると、ステップ S 302, S 304 を経て、ユーザ端末 100 が低消費電力モードに設定され、ユーザ端末 100 の表示画面がロックされる。

30

また、ユーザは、ネットワークプリンタ 200 から印刷物を取り、ユーザ端末 100 に戻ったときは、認証カード読取装置 46 に認証カード 300 を再び挿入する。

【0139】

ユーザ端末 100 では、認証カード 300 が挿入されると、ステップ S 306, S 308 を経て、認証カード読取装置 46 により証明情報が認証カード 300 から読み出され、読み出された証明情報及び認証情報登録テーブル 400 の認証情報に基づいて印刷データの利用適格があるか否かが判定される。その結果、印刷データの利用適格があると判定されると、ステップ S 312, S 314 を経て、低消費電力モード及び画面ロックが解除される。

【0140】

40

なお、例えば、不正な証明情報を記憶した認証カード 300 や、証明情報が記憶されていない認証カード 300 を挿入した場合は、ユーザ端末 100 では、印刷データの利用適格がないと判定されるので、ステップ S 310 を経て、低消費電力モード及び画面ロックが解除されることなく処理が終了する。

このようにして、本実施の形態では、ユーザ端末 100 は、認証カード読取装置 46 から認証カード 300 が取り外されたときは、ユーザ端末 100 の表示画面をロックするようになっている。

【0141】

これにより、ユーザがユーザ端末 100 から認証カード 300 を取り外した後は、ユーザ端末 100 の表示が制限されるので、ユーザ端末 100 を離れている間に、ユーザ端末

50

100の表示装置44で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができる。

また、ユーザ端末100から認証カード300を取り外した後は、ユーザは、ネットワークプリンタ200に印刷物を取りに行く可能性が高く、ユーザ端末100を継続して利用する可能性が低いので、ユーザ端末100の表示が制限されてもユーザの利便性をさほど損なうことがない。

【0142】

さらに、本実施の形態では、ユーザ端末100は、認証カード読取装置46から認証カード300が取り外されたときは、ユーザ端末100を低消費電力モードに設定するようになっている。

これにより、ユーザがユーザ端末100から認証カード300を取り外した後は、ユーザ端末100が低消費電力モードに設定されるので、ユーザ端末100を離れている間に、ユーザ端末100の電力が無駄に消費されるのを抑えることができる。従って、ユーザ端末100の消費電力を低減することができる。

【0143】

また、ユーザ端末100から認証カード300を取り外した後は、ユーザは、ネットワークプリンタ200に印刷物を取りに行く可能性が高く、ユーザ端末100を継続して利用する可能性が低いので、ユーザ端末100が低消費電力モードに設定されてもユーザの利便性をさほど損なうことがない。

前記第2の実施の形態において、印刷データは、発明1の動作データに対応し、ユーザ端末100は、発明1のデバイス利用端末、または発明2ないし4、6、10、12、13、15、17、18、20若しくは21のプリンタ利用端末に対応し、ステップS304は、発明4、6、13若しくは18の出力制限手段、または発明21の出力制限ステップに対応している。また、ネットワークプリンタ200は、発明1のネットワークデバイスに対応し、認証カード300は、発明1ないし3、6、10、15または20の認証用記憶媒体に対応している。

【0144】

次に、本発明の実施の第3の形態を図面を参照しながら説明する。

図11及び図12は、本発明に係る認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法の実施の第3の形態を示す図である。

【0145】

本実施の形態は、本発明に係る認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法を、図1に示すように、認証カード300を利用してネットワークプリンタ200で印刷を行う場合について適用したものであり、前記第1の実施の形態と異なるのは、ネットワークプリンタ200に認証カード300を挿入したときに低消費電力モードの設定及び画面ロックを行う点にある。なお、以下、前記第1の実施の形態と異なる部分についてのみ説明し、重複する部分については同一の符号を付して説明を省略する。

【0146】

まず、ユーザ端末100の構成を図11を参照しながら説明する。

ユーザ端末100は、図4及び図6のフローチャートに示す印刷開始処理及び利用適格認証処理に加えて、図11のフローチャートに示す表示禁止処理を実行するようになっている。なお、図4の印刷開始処理については、ステップS114、S116の処理は実行しない。

【0147】

図11は、表示禁止処理を示すフローチャートである。

表示禁止処理は、ネットワークプリンタ200からの表示禁止要求に応じて表示装置4

10

20

30

40

50

4の表示を禁止する処理であって、CPU30において実行されると、図11に示すように、まず、ステップS400に移行するようになっている。

ステップS400では、ユーザ端末100の表示を禁止する表示禁止要求を受信したか否かを判定し、表示禁止要求を受信したと判定したとき(Yes)は、ステップS402に移行するが、そうでないと判定したとき(No)は、表示禁止要求を受信するまでステップS400で待機する。

【0148】

ステップS402では、ユーザ端末100を低消費電力モードに設定し、ステップS404に移行して、ユーザ端末100の表示画面をロックし、一連の処理を終了して元の処理に復帰させる。

10

次に、ネットワークプリンタ200の構成を図12を参照しながら説明する。

ネットワークプリンタ200は、図8のフローチャートに示す認証印刷処理に代えて、図12のフローチャートに示す認証印刷処理を実行するようになっている。

【0149】

図12は、認証印刷処理を示すフローチャートである。

認証印刷処理は、認証カード読取装置62に認証カード300が挿入されたときは、ユーザ端末100から印刷データを取得して印刷を行う処理であって、CPU50において実行されると、図12に示すように、まず、ステップS500に移行するようになっている。

【0150】

20

ステップS500では、認証カード読取装置62に認証カード300が挿入されたか否かを判定し、認証カード300が挿入されたと判定したとき(Yes)は、ステップS502に移行するが、そうでないと判定したとき(No)は、認証カード300が挿入されるまでステップS500で待機する。

ステップS502では、認証カード読取装置62によりアクセス情報を認証カード300から読み込み、ステップS504に移行して、読み込んだアクセス情報に基づいて表示禁止要求をユーザ端末100に送信し、ステップS506に移行する。

【0151】

ステップS506では、ネットワークプリンタ200が現在印刷中であるか否かを判定し、印刷中でないと判定したとき(No)は、ステップS508に移行するが、そうでないと判定したとき(Yes)は、ステップS500に移行する。

30

ステップS508では、認証カード読取装置62により証明情報及びアクセス情報を認証カード300から読み込み、ステップS510に移行して、読み込んだアクセス情報に基づいてユーザ端末100に取得要求を送信し、ステップS512に移行して、読み込んだアクセス情報に基づいてユーザ端末100に証明情報を送信し、ステップS514に移行する。

【0152】

ステップS514では、認証通知を受信したか否かを判定し、認証通知を受信したと判定したとき(Yes)は、ステップS516に移行して、読み込んだアクセス情報に基づいてユーザ端末100に接続要求を送信し、ステップS518に移行して、印刷データを受信し、ステップS520に移行する。

40

ステップS520では、受信した印刷データに基づいて印刷装置60により印刷を行い、ステップS522に移行して、認証カード読取装置62により証明情報及びアクセス情報を認証カード300から消去し、一連の処理を終了して元の処理に復帰させる。

【0153】

一方、ステップS514で、認証通知を受信しないと判定したとき(No)は、ステップS524に移行して、否認通知を受信したか否かを判定し、否認通知を受信したと判定したとき(Yes)は、一連の処理を終了して元の処理に復帰させるが、そうでないと判定したとき(No)は、ステップS514に移行する。

次に、本実施の形態の動作を説明する。

50

【0154】

ネットワークプリンタ200で印刷を行う場合、ユーザは、認証カード300を持ってネットワークプリンタ200に赴き、認証カード読取装置62に認証カード300を挿入する。

ネットワークプリンタ200では、認証カード300が挿入されると、ステップS502、S504を経て、認証カード読取装置62によりアクセス情報が認証カード300から読み出され、読み出されたアクセス情報に基づいて表示禁止要求がユーザ端末100に送信される。

【0155】

ユーザ端末100では、表示禁止要求を受信すると、ステップS402、S404を経て、ユーザ端末100が低消費電力モードに設定され、ユーザ端末100の表示画面がロックされる。

このようにして、本実施の形態では、ネットワークプリンタ200は、認証カード読取装置62に認証カード300が挿入されたときは、ユーザ端末100に表示禁止要求を送信するようになっており、ユーザ端末100は、表示禁止要求を受信したときは、ユーザ端末100の表示画面をロックするようになっている。

【0156】

これにより、ユーザがネットワークプリンタ200に認証カード300を与えた後は、ユーザ端末100の表示が制限されるので、ユーザ端末100を離れている間に、ユーザ端末100の表示装置44で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができる。

また、ネットワークプリンタ200に認証カード300を与えた後は、ユーザは、ユーザ端末100を離れている可能性が高いので、ユーザ端末100の表示が制限されてもユーザの利便性をさほど損なうことがない。

【0157】

さらに、本実施の形態では、ネットワークプリンタ200は、認証カード読取装置62に認証カード300が挿入されたときは、ユーザ端末100に表示禁止要求を送信するようになっており、ユーザ端末100は、表示禁止要求を受信したときは、ユーザ端末100を低消費電力モードに設定するようになっている。

これにより、ユーザがネットワークプリンタ200に認証カード300を与えた後は、ユーザ端末100が低消費電力モードに設定されるので、ユーザ端末100を離れている間に、ユーザ端末100の電力が無駄に消費されるのを抑えることができる。従って、ユーザ端末100の消費電力を低減することができる。

【0158】

また、ネットワークプリンタ200に認証カード300を与えた後は、ユーザは、ユーザ端末100を離れている可能性が高いので、ユーザ端末100が低消費電力モードに設定されてもユーザの利便性をさほど損なうことがない。

前記第3の実施の形態において、印刷データは、発明1の動作データに対応し、表示禁止要求は、発明7、8等の出力制限要求に対応し、ユーザ端末100は、発明1のデバイス利用端末、または発明2等のプリンタ利用端末に対応している。また、ステップS404は、発明7、8等の出力制限手段、及び出力制限ステップに対応し、ネットワークプリンタ200は、発明1のネットワークデバイスに対応し、ステップS504は、発明7、8等の出力制限要求手段、及び出力制限要求ステップに対応している。

【0159】

また、前記第3の実施の形態において、ステップS508は、発明2等の証明情報読込手段、及び証明情報読込ステップに対応し、ステップS510～S520は、発明2等の認証印刷手段、及び認証印刷ステップに対応している。また、認証カード300は、発明1等の認証用記憶媒体に対応している。

次に、本発明の実施の第4の形態を図面を参照しながら説明する。

【0160】

図 1 3 は、本発明に係る認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法の実施の第 4 の形態を示す図である。

本実施の形態は、本発明に係る認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法を、図 1 に示すように、認証カード 3 0 0 を利用してネットワークプリンタ 2 0 0 で印刷を行う場合について適用したものであり、前記第 3 の実施の形態と異なるのは、ネットワークプリンタ 2 0 0 での印刷時に低消費電力モードの設定及び画面ロックを行う点にある。なお、以下、前記第 3 の実施の形態と異なる部分についてのみ説明し、重複する部分については同一の符号を付して説明を省略する。 10

【0 1 6 1】

まず、ネットワークプリンタ 2 0 0 の構成を図 1 3 を参照しながら説明する。

ネットワークプリンタ 2 0 0 は、図 8 のフローチャートに示す認証印刷処理に代えて、図 1 3 のフローチャートに示す認証印刷処理を実行するようになっている。

図 1 3 は、認証印刷処理を示すフローチャートである。

認証印刷処理は、認証カード読取装置 6 2 に認証カード 3 0 0 が挿入されたときは、ユーザ端末 1 0 0 から印刷データを取得して印刷を行う処理であって、C P U 5 0 において実行されると、図 1 3 に示すように、まず、ステップ S 6 0 0 に移行するようになっている。 20

【0 1 6 2】

ステップ S 6 0 0 では、認証カード読取装置 6 2 に認証カード 3 0 0 が挿入されたか否かを判定し、認証カード 3 0 0 が挿入されたと判定したとき (Y e s) は、ステップ S 6 0 6 に移行するが、そうでないと判定したとき (N o) は、認証カード 3 0 0 が挿入されるまでステップ S 6 0 0 で待機する。

ステップ S 6 0 6 では、ネットワークプリンタ 2 0 0 が現在印刷中であるか否かを判定し、印刷中でないと判定したとき (N o) は、ステップ S 6 0 8 に移行するが、そうでないと判定したとき (Y e s) は、ステップ S 6 0 0 に移行する。

【0 1 6 3】

ステップ S 6 0 8 では、認証カード読取装置 6 2 により証明情報及びアクセス情報を認証カード 3 0 0 から読み込み、ステップ S 6 1 0 に移行して、読み込んだアクセス情報に基づいて取得要求及び表示禁止要求をユーザ端末 1 0 0 に送信し、ステップ S 6 1 2 に移行して、読み込んだアクセス情報に基づいてユーザ端末 1 0 0 に証明情報を送信し、ステップ S 6 1 4 に移行する。 30

【0 1 6 4】

ステップ S 6 1 4 では、認証通知を受信したか否かを判定し、認証通知を受信したと判定したとき (Y e s) は、ステップ S 6 1 6 に移行して、読み込んだアクセス情報に基づいてユーザ端末 1 0 0 に接続要求を送信し、ステップ S 6 1 8 に移行して、印刷データを受信し、ステップ S 6 2 0 に移行する。

ステップ S 6 2 0 では、受信した印刷データに基づいて印刷装置 6 0 により印刷を行い、ステップ S 6 2 2 に移行して、認証カード読取装置 6 2 により証明情報及びアクセス情報を認証カード 3 0 0 から消去し、一連の処理を終了して元の処理に復帰させる。 40

【0 1 6 5】

一方、ステップ S 6 1 4 で、認証通知を受信しないと判定したとき (N o) は、ステップ S 6 2 4 に移行して、否認通知を受信したか否かを判定し、否認通知を受信したと判定したとき (Y e s) は、一連の処理を終了して元の処理に復帰させるが、そうでないと判定したとき (N o) は、ステップ S 6 1 4 に移行する。

次に、本実施の形態の動作を説明する。

【0 1 6 6】

ネットワークプリンタ 2 0 0 で印刷を行う場合、ユーザは、認証カード 3 0 0 を持って 50

ネットワークプリンタ 200 に赴き、認証カード読取装置 62 に認証カード 300 を挿入する。

ネットワークプリンタ 200 では、認証カード 300 が挿入されると、印刷可能となるまで待機した後、ステップ S 608 ～ S 612 を経て、認証カード読取装置 62 により証明情報及びアクセス情報が認証カード 300 から読み出され、読み出されたアクセス情報に基づいて取得要求及び表示禁止要求とともに証明情報がユーザ端末 100 に送信される。

【0167】

ユーザ端末 100 では、表示禁止要求を受信すると、ステップ S 402, S 404 を経て、ユーザ端末 100 が低消費電力モードに設定され、ユーザ端末 100 の表示画面がロックされる。 10

このようにして、本実施の形態では、ネットワークプリンタ 200 は、取得要求の送信とともに表示禁止要求をユーザ端末 100 に送信するようになっており、ユーザ端末 100 は、表示禁止要求を受信したときは、ユーザ端末 100 の表示画面をロックするようになっている。

【0168】

これにより、ネットワークプリンタ 200 で印刷データの取得が開始された後は、ユーザ端末 100 の表示が制限されるので、ユーザ端末 100 を離れている間に、ユーザ端末 100 の表示装置 44 で表示されている印刷内容が第三者に盗み見られる可能性を低減することができる。従って、従来に比して、印刷内容の機密を保護することができる。 20

また、ネットワークプリンタ 200 で印刷データの取得が開始された後は、ユーザは、ユーザ端末 100 を離れている可能性が高いので、ユーザ端末 100 の表示が制限されてもユーザの利便性をさほど損なうことがない。

【0169】

さらに、本実施の形態では、ネットワークプリンタ 200 は、取得要求の送信とともに表示禁止要求をユーザ端末 100 に送信するようになっており、ユーザ端末 100 は、表示禁止要求を受信したときは、ユーザ端末 100 を低消費電力モードに設定するようになっている。

これにより、ネットワークプリンタ 200 で印刷データの取得が開始された後は、ユーザ端末 100 が低消費電力モードに設定されるので、ユーザ端末 100 を離れている間に、ユーザ端末 100 の電力が無駄に消費されるのを抑えることができる。従って、ユーザ端末 100 の消費電力を低減することができる。 30

【0170】

また、ネットワークプリンタ 200 で印刷データの取得が開始された後は、ユーザは、ユーザ端末 100 を離れている可能性が高いので、ユーザ端末 100 が低消費電力モードに設定されてもユーザの利便性をさほど損なうことがない。

前記第 4 の実施の形態において、印刷データは、発明 1 の動作データに対応し、表示禁止要求は、発明 7 等の出力制限要求に対応し、ユーザ端末 100 は、発明 1 のデバイス利用端末、または発明 2 等のプリンタ利用端末に対応している。また、ステップ S 404 は、発明 7 等の出力制限手段、及び出力制限ステップに対応し、ネットワークプリンタ 200 は、発明 1 のネットワークデバイスに対応し、ステップ S 608 は、発明 2 等の証明情報読込手段、及び証明情報読込ステップに対応している。 40

【0171】

また、前記第 4 の実施の形態において、ステップ S 610 は、発明 7 等の出力制限要求手段、及び出力制限要求ステップに対応し、ステップ S 610 ～ S 220 は、発明 2 等の認証印刷手段、及び認証印刷ステップに対応している。また、認証カード 300 は、発明 1 等の認証用記憶媒体に対応している。

次に、本発明の第 5 の実施の形態を図面を参照しながら説明する。

【0172】

図 14 ないし図 20 は、本発明に係る認証動作システム、認証印刷システム、ネットワ 50

ークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法の第5の実施の形態を示す図である。

本実施の形態は、本発明に係る認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法を、図14に示すように、認証カード300を利用してネットワークプリンタ200で印刷を行う場合について適用したものであり、前記第1の実施の形態と異なるのは、ネットワーク199に、ユーザ端末100とネットワークプリンタ200の他にサーバ250を設け、このサーバ250に印刷データのアクセス情報を登録するようにした点にある。なお、以下、前記第1の実施の形態と異なる部分についてのみ説明し、重複する部分については同一の符号を付して説明を省略する。

10

【0173】

先ず、図15は、このサーバ250のハードウェア構成を示すブロック図である。

図示するようにこのサーバ250は、制御プログラムに基づいて演算及びシステム全体を制御するCPU70と、所定領域にあらかじめCPU70の制御プログラム等を格納しているROM72と、ROM72等から読み込んだデータやCPU70の演算過程で必要な演算結果を格納するためのRAM74と、外部装置に対してデータの入出力を媒介するI/F78とで構成されており、これらは、データを転送するための信号線であるバス79で相互にかつデータ授受可能に接続されている。

20

【0174】

I/F78には、外部装置として、ヒューマンインターフェースとしてデータの入力可能なキーボードやマウス等からなる入力装置80と、前述した証明情報やアクセス情報を保存しておくための記憶装置82と、画像信号に基づいて画面を表示する表示装置84と、インターネット199に接続するための信号線とが接続されている。

図16は、本実施の形態に係るユーザ端末100における印刷開始処理を示すフローチャートである。

【0175】

この印刷開始処理は、基本的には、前記第1の実施の形態で説明した図4のユーザ端末における処理とほぼ同様であるが、ステップS110において、生成した認証情報を認証情報登録テーブル400に登録したならば、ステップS111に移行して所定の処理を実行するようになっている。

30

ステップS111では、ステップS108で生成した図5に示すような証明情報と、印刷データへのアクセス情報、すなわち、自己の印刷キューのネットワーク上のアドレスであるアクセス情報とをサーバ250に送信してからステップS113に移行するようになっている。

【0176】

そして、ステップS113では、その証明情報と、そのサーバ250のネットワーク上のアドレスであるサーバ250へのアクセス情報を認証カード300へ書き込むことになる。すなわち、前記第1の実施の形態では、認証カード300へ書き込むアクセス情報は自己の印刷キューへのアクセス情報であったが、本実施の形態では認証カード300へ書き込むアクセス情報はサーバ250へのアクセス情報となっている点が前記第1の実施の形態と大きく異なる点である。

40

【0177】

図17は、本実施の形態に係るネットワークプリンタ200における認証印刷処理を示すフローチャートである。

この認証印刷処理も、基本的には、前記第1の実施の形態で説明した図8のネットワークプリンタ200における処理とほぼ同様であるが、ステップS208において、認証カード300から証明情報及びサーバへのアクセス情報を読み込んだならば、次のステップS209に移行して所定の処理を実行するようになっている。

50

【0178】

ステップS209では、読み込んだアクセス情報に基づいて所定のサーバ205にアクセスして、目的とする印刷データが保存されている印刷キュー（ユーザ端末100）へのアクセス情報を取得してから、ステップS212に移行してこのアクセス情報に基づいてユーザ端末100に証明情報を送信するようになっている。

図18及び図19は、本実施の形態に係るサーバ250における情報登録処理及び情報送信処理を示すフローチャート図である。

【0179】

先ず、図18に示す情報登録処理は、ユーザ端末100からサーバ250に対する証明情報及びアクセス情報の登録を行う処理であって、図15に示すCPU70において実行されると、まず、ステップS700に移行するようになっている。 10

ステップS700では、ユーザ端末100から情報の登録要求があったか否かを判定し、登録要求がないと判定したとき（No）は、そのまま登録要求があるまで待機することになるが、登録要求があったと判定したとき（Yes）は、次のステップS702に移行して情報登録の権利の有無を確認する。例えば、インターネット199には、多種多様なユーザ端末が接続されていることから、登録要求があった端末が、本発明システムを構築（利用）するためのユーザ端末100であるか否かをその端末のIPアドレスやパスワード等に基づいて判断する。

【0180】

そして、次の判断ステップS704において、情報の登録権がないと判断したとき（No）は、ステップS708側に移行して情報の登録を拒否して処理を終了することになるが、情報の登録権がないと判断したとき（No）は、次のステップS708に移行して前記証明情報及びそのユーザ端末100へのアクセス情報をその取得して図15に示すRAM74や記憶装置82等に登録して処理を終了する。 20

【0181】

一方、図19に示す情報送信処理は、ネットワークプリンタ200からサーバ250に対する印刷データへのアクセス情報の問い合わせに対する応答を行う処理であって、図15に示すCPU70において実行されると、まず、ステップS750に移行するようになっている。

ステップS750では、ネットワークプリンタ200からアクセス情報の読み込み要求があったか否かを判定し、読み込み要求がないと判定したとき（No）は、そのまま読み込み要求があるまで待機することになるが、読み込み要求があったと判定したとき（Yes）は、次のステップS752に移行して情報の読み込みに関する権利の有無を確認する。このステップS752における読込権の確認は、例えば、ユーザ端末100の認証カード読取装置46によって認証カード300に直接書き込まれた証明情報と、ユーザ端末100からインターネット199を介して送られてきた証明情報とを照合し、両情報が完全に一致している場合は、正規の読込権を有すると判断し、両情報の一部でも相違している場合は正規の読込権を有していないと判断することになる。 30

【0182】

そして、次の判断ステップS754において、情報の読込権がないと判断したとき（No）は、ステップS758側に移行してその情報の読み込み（提供）を拒否して処理を終了することになるが、情報の読込権があると判断したとき（Yes）は、次のステップS756に移行して対象となる印刷データが保存されているユーザ端末100（印刷キュー）へのアクセス情報（例えば、「http://taropco.jp/queue/」）をネットワークプリンタ200へ送信して処理を終了することになる。 40

【0183】

次に、本実施の形態の動作を図20を参照しながら説明する。

ネットワークプリンタ200で印刷を行う場合、ユーザは、ユーザ端末100において、図20（1）に示すように、まず、認証カード読取装置46に認証カード300を挿入するとともに印刷要求を入力装置40から入力する。 50

ユーザ端末100では、認証カード300が挿入された状態で印刷要求が入力されると、図20(2)に示すように、ステップS102、S104を経て、印刷データが生成され、生成された印刷データが印刷キューに登録される。次いで、ステップS108～S112を経て、登録された印刷データについて認証情報及び証明情報がそれぞれ生成され、生成された認証情報が認証情報登録テーブル400に登録され、生成された証明情報及びサーバ250へのアクセス情報が認証カード読取装置46により認証カード300に書き込まれる。また、図20(3)に示すように、これと同時に、生成された証明情報及び自己の印刷キューへのアクセス情報がステップS111を経て、インターネット199を介して所定のサーバ250に保存される。そして、ステップS114、S116を経て、ユーザ端末100が低消費電力モードに設定され、ユーザ端末100の表示画面がロックされる。 10

【0184】

次に、ユーザは、認証カード300を持ってネットワークプリンタ200に赴き、図20(4)に示すように、認証カード読取装置62に認証カード300を挿入する。

ネットワークプリンタ200では、認証カード300が挿入されると、印刷可能となるまで待機した後、ステップS209を経て、認証カード読取装置62により証明情報及びサーバのアクセス情報が認証カード300から読み出され、読み出されたアクセス情報に基づいて所定のサーバ250にアクセスして印刷データへのアクセス情報を取得することになる。そして、ネットワークプリンタ200は、ステップS212を経て、取得したアクセス情報に基づいて所定のユーザ端末100にインターネット199を介してアクセスして認証カード300から取得した証明情報をユーザ端末100に送信することになる。 20

【0185】

その後は、前記第1の形態と同様に、ユーザ端末100では、取得要求とともに証明情報を受信すると、ステップS154を経て、受信した証明情報及び認証情報登録テーブル400の認証情報に基づいて印刷データの利用適格があるか否かが判定される。その結果、印刷データの利用適格があると判定されると、ステップS158を経て、要求元ネットワークプリンタ200に認証通知が送信され、ネットワークプリンタ200では、認証通知を受信すると、ステップS216を経て、アクセス情報に基づいてユーザ端末100に接続要求が送信される。

【0186】

ユーザ端末100では、要求元ネットワークプリンタ200から接続要求を受信すると、ステップS162を経て、受信した証明情報に含まれるファイル名の印刷データが印刷キューから読み出され、図20(6)に示すように、読み出された印刷データが要求元ネットワークプリンタ200に送信される。また、ステップS163を経て、受信した証明情報に含まれるファイル名の印刷データが印刷キューから削除される。

【0187】

ネットワークプリンタ200では、印刷データを受信すると、図20(7)に示すようステップS220を経て、受信した印刷データに基づいて印刷装置60により印刷が行われる。また、ステップS222を経て、認証カード読取装置62により証明情報及びアクセス情報が認証カード300から消去される。 40

このようにして、本実施の形態では、新たに、あるいは既に接続されているサーバ250に、印刷データへのアクセス情報を保存しておき、ネットワークプリンタ200がそのアクセス情報に基づいて所定の印刷データをユーザ端末100から取得するようになって

【0188】

これにより、前記第1の実施の形態と同様な効果に加え、サーバ250を介してネットワークプリンタ200からユーザ端末100にアクセスされるようになるため、サーバ250における印刷管理を容易に行うことができる。さらに、認証用印刷媒体には、印刷データの位置情報を記録する必要がないため、認証用印刷媒体から印刷データの位置情報が盗取される可能性を低減することができる。従って、従来のシステムに比して、印刷デー 50

タの機密を保護することができるという効果が得られる。

【0189】

なお、前記第1ないし第5の実施の形態においては、印刷先のネットワークプリンタ200を特に指定しなかったが、これに限らず、印刷先のネットワークプリンタ200を指定して印刷を行うように構成することもできる。

これにより、指定のネットワークプリンタ200以外のネットワークプリンタ200に認証カード300を与えても、印刷データの取得及び印刷が行われることがないので、印刷データの機密をより確実に保護することができる。

【0190】

また、前記第1ないし第5の実施の形態においては、ネットワークプリンタ200がユーザ端末100から印刷データを取得して印刷を行うように構成したが、これに限らず、ユーザ端末100及びネットワークプリンタ200のほか、図4、図6、図10及び図11のフローチャートに示す処理を前記プリンタ管理サーバ250で実行させることにより、ネットワークプリンタ200がプリンタ管理サーバ250から印刷データを取得して印刷を行うように構成することもできる。この場合、認証カード読取装置46はユーザ端末100に設けたままとし、ユーザ端末100は、プリンタ管理サーバから証明情報を受信し、受信した証明情報を認証カード300に書き込むようにしてもよい。

【0191】

また、前記第1ないし第5の実施の形態においては、証明情報のパスワードと認証情報のパスワードとを同一のものとして設定するように構成したが、これに限らず、認証情報または証明情報のうち一方のパスワードを暗号鍵として所定の情報を暗号化し、暗号化したものを認証情報または証明情報のうち他方のパスワードとして設定するように構成してもよいし、公開鍵暗号化方式を利用して、公開鍵または秘密鍵のうち一方を認証情報のパスワードとして設定し、公開鍵または秘密鍵のうち他方を証明情報のパスワードとして設定するように構成してもよい。

【0192】

また、前記第1ないし第5の実施の形態においては、1つの印刷データに対応する証明情報を認証カード300に書き込むように構成したが、これに限らず、複数の印刷データに対応するそれぞれの証明情報を認証カード300に書き込むように構成することもできる。

これにより、複数の印刷ジョブを1回の認証カード300の挿入により実行することができる。

【0193】

また、前記第1ないし第5の実施の形態においては、1つの印刷データに対して1つの証明情報及び認証情報を対応付けるように構成したが、これに限らず、複数の印刷データに対して1つの証明情報及び認証情報を対応付けるように構成することもできる。

これにより、複数の印刷ジョブを1回の認証カード300の挿入により実行することができる。

【0194】

また、前記第2の実施の形態において、ステップS306～S316では、認証カード300から証明情報を読み込み、読み込んだ証明情報及び認証情報登録テーブル400の認証情報に基づいて印刷データの利用適格があるか否かを判定し、印刷データの利用適格があると判定したときは、低消費電力モード及び画面ロックを解除するように構成したが、ユーザがネットワークプリンタ200で印刷を終えて戻ってきたときには、認証カード300の証明情報が消去（ステップS222）されているので、認証カード300を挿入しても低消費電力モード及び画面ロックを解除することができない。

【0195】

そこで、前記第2の実施の形態においては、ステップS222の処理を実行しないように構成するか、ステップS306～S310の処理に代えて、ユーザが所定のパスワードを入力することにより低消費電力モード及び画面ロックを解除するように構成することが

考えられる。

また、前記第1ないし第5の実施の形態において、図4、図6、図10、図11、図16、図17、図18、図19のフローチャートに示す処理を実行するにあたってはいずれも、ROM32にあらかじめ格納されている制御プログラムを実行する場合について説明したが、これに限らず、これらの手順を示したプログラムが記憶された記憶媒体から、そのプログラムをRAM34に読み込んで実行するようにしてもよい。

【0196】

ここで、記憶媒体とは、RAM、ROM等の半導体記憶媒体、FD、HD等の磁気記憶型記憶媒体、CD、CDV、LD、DVD等の光学的読取方式記憶媒体、MO、MD等の磁気記憶型／光学的読取方式記憶媒体であって、電子的、磁氣的、光学的等の読み取り方法のいかににかかわらず、コンピュータで読み取り可能な記憶媒体であれば、あらゆる記憶媒体を含むものである。

【0197】

また、前記第1ないし第5の実施の形態においては、本発明に係る認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法を、インターネット199からなるネットワークシステムに適用した場合について説明したが、これに限らず、例えば、インターネット199と同一方式により通信を行ういわゆるイントラネットに適用してもよい。もちろん、インターネット199と同一方式により通信を行うネットワークに限らず、通常のネットワークに適用することもできる。

【0198】

また、前記第1ないし第5の実施の形態においては、本発明に係る認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法を、図1に示すように、認証カード300を利用してネットワークプリンタ200で印刷を行う場合について適用したが、これに限らず、本発明の主旨を逸脱しない範囲で他の場合にも適用可能である。

【0199】

また、前記第1ないし第5の実施の形態においては、認証カード300という認証記憶媒体を介して証明情報及びアクセス情報をネットワークプリンタ200に与えるようにしたが、これは、そのユーザが正規のユーザであることを証明することを目的とするものであることから、この目的を達成できれば、他の手段、例えば、指紋や静脈パターン、虹彩等の生体情報であってもよい。この場合、ネットワークプリンタ200のハードウェア構成は、図2に示す認証カード読取装置46に代えて、それら生体情報を認識するための装置（パターン認識装置等）が用いられることはもちろんである。

【0200】

また、前記第1ないし第5の実施の形態においては、ユーザ端末100によって送信された証明情報に基づいて認証を行っていたが、認証情報登録テーブル400をプリンタ管理サーバ250側におき、図6に示すような利用適格認証処理をプリンタ管理サーバ250で実施するようにしてもよい。すなわち、プリンタ管理サーバ250は、ネットワークプリンタ200からユーザ端末（印刷データ）100のアドレス情報の問い合わせがあったときは、そのアドレス情報の回答と共に、証明情報と認証情報登録テーブル400とに基づいてそのネットワークプリンタ200に正当な利用適格があるか否かの認証処理を実施し、利用適格が「ない」と判断したときはアドレス情報の回答を拒否し、利用適格が「ある」と判断したときは、そのアドレス情報をネットワークプリンタ200に回答することで認証処理を同時に実行することが可能となる。

【0201】

また、前記第1ないし第5の実施の形態においては、ユーザ名とパスワードの両方が完全に一致した場合に、利用適格を証明する「証明情報」が正当であると判断したが、ユーザ名のみ、あるいはパスワードのみ、または生体情報のみが一致した場合でも正当である

と判断してもよい。

また、前記第1ないし第5の実施の形態においては、印刷データの場所を示す位置情報を表すものとして、「http://…」を用いた例で示したが、「https://…」や「ftp://…」も利用できることはもちろんである。

【図面の簡単な説明】

【0202】

【図1】本発明を適用するネットワークシステムの構成を示すブロック図である。

【図2】ユーザ端末100の構成を示すブロック図である。

【図3】認証情報登録テーブル400のデータ構造を示す図である。

【図4】印刷開始処理を示すフローチャートである。

10

【図5】認証カード300に書き込む証明情報及びアクセス情報のデータ構造を示す図である。

【図6】利用適格認証処理を示すフローチャートである。

【図7】ネットワークプリンタ200の構成を示すブロック図である。

【図8】認証印刷処理を示すフローチャートである。

【図9】第1の実施の形態の動作を説明するための図である。

【図10】表示禁止処理を示すフローチャートである。

【図11】表示禁止処理を示すフローチャートである。

【図12】認証印刷処理を示すフローチャートである。

【図13】認証印刷処理を示すフローチャートである。

20

【図14】第5の実施の形態を示すブロック図である。

【図15】プリンタ管理サーバ250の構成を示すブロック図である。

【図16】印刷開始処理を示すフローチャートである。

【図17】認証印刷処理を示すフローチャートである。

【図18】情報登録処理を示すフローチャートである。

【図19】情報読込処理を示すフローチャートである。

【図20】第5の実施の形態の動作を説明するための図である。

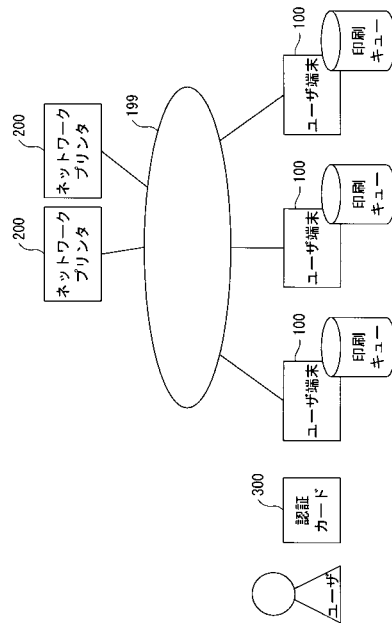
【符号の説明】

【0203】

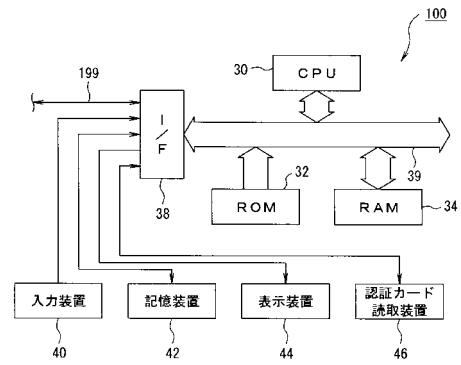
100…ユーザ端末，30…CPU，32…ROM，34…RAM，38…I/F，40…入力装置，42…記憶装置，44…表示装置，46…認証カード読取装置，200…ネットワークプリンタ，50…CPU，52…ROM，54…RAM，58…I/F，60…印刷装置，62…認証カード読取装置，300…認証カード，400…認証情報登録テーブル。

30

【図 1】



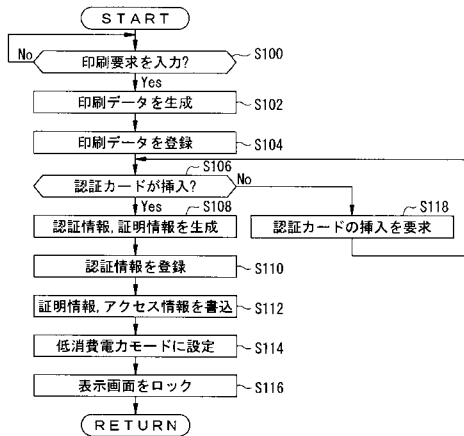
【図 2】



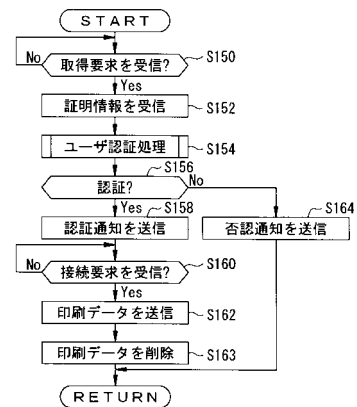
【図 3】

ユーザ名	パスワード	印刷データ ファイル名
taro	1234abc	Printdata1.dat

【図 4】



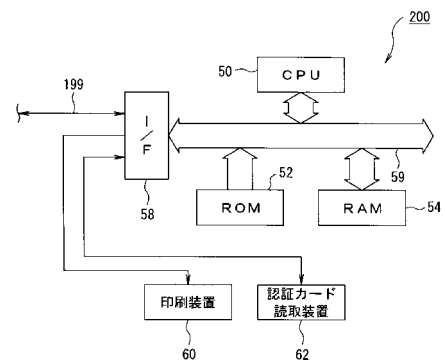
【図 6】



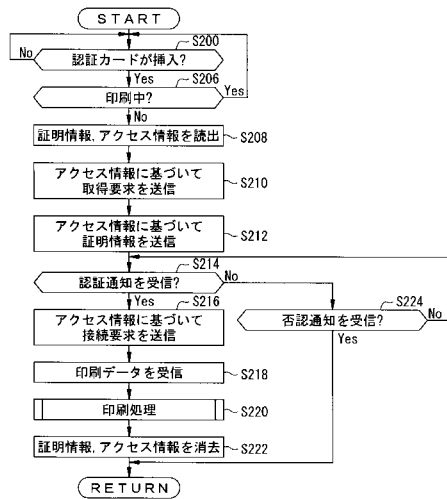
【図 5】

ユーザ名	taro	420
パスワード	1234abc	422
印刷データファイル名	Printdata1.dat	424
アクセス情報	http://taro-pc.jp/queue/	426

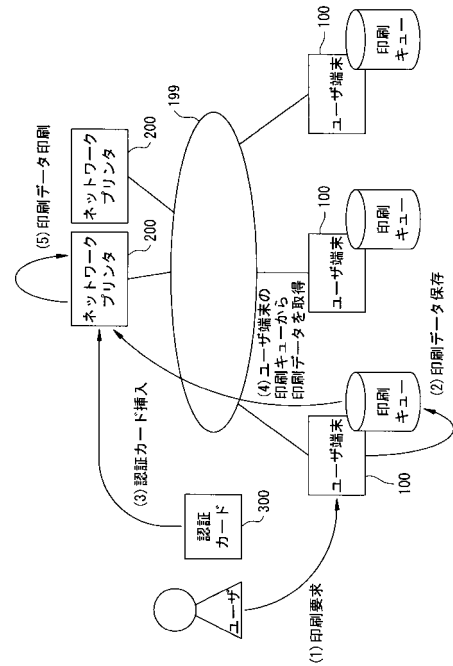
【図 7】



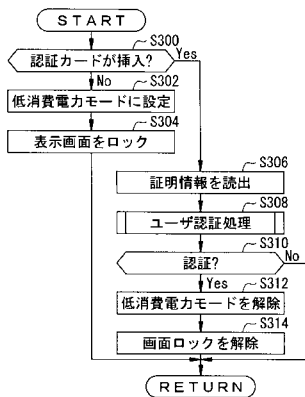
【図 8】



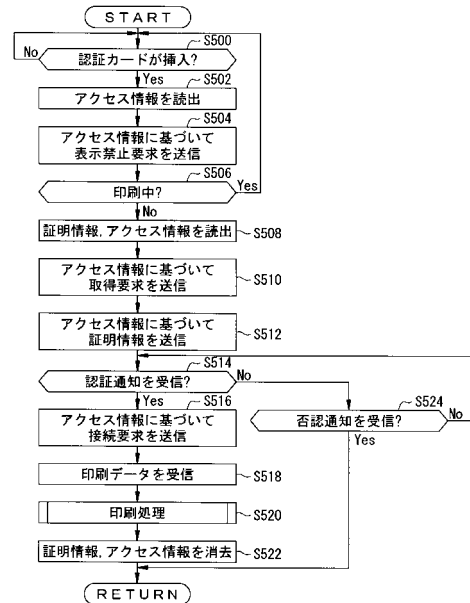
【図 9】



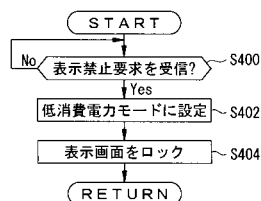
【図 10】



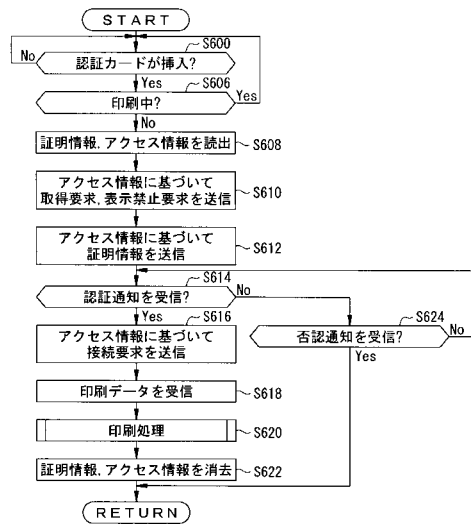
【図 12】



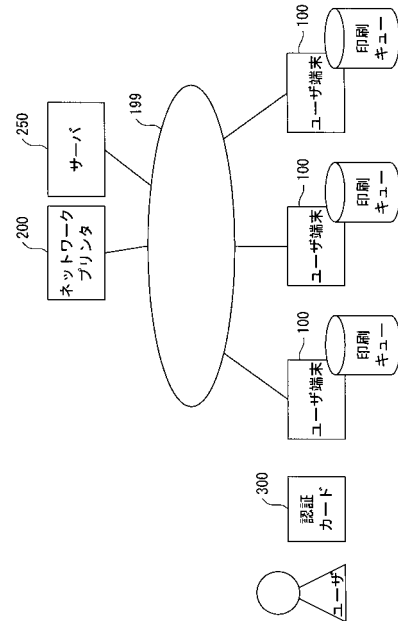
【図 11】



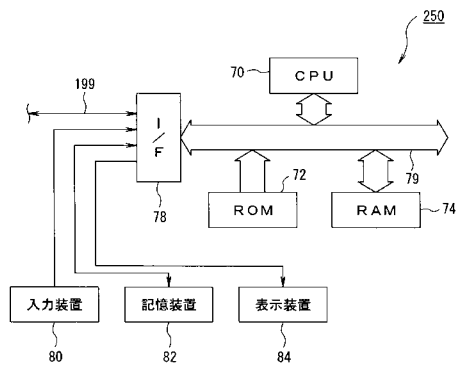
【図 13】



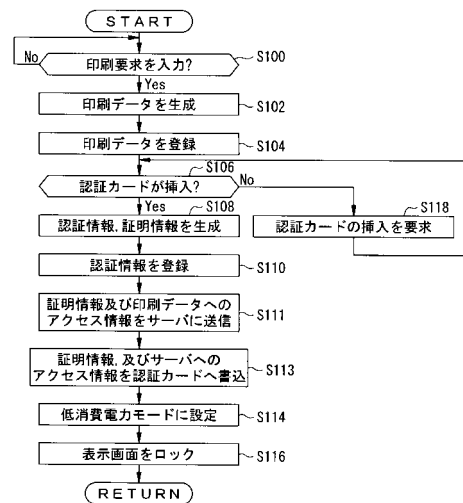
【図 14】



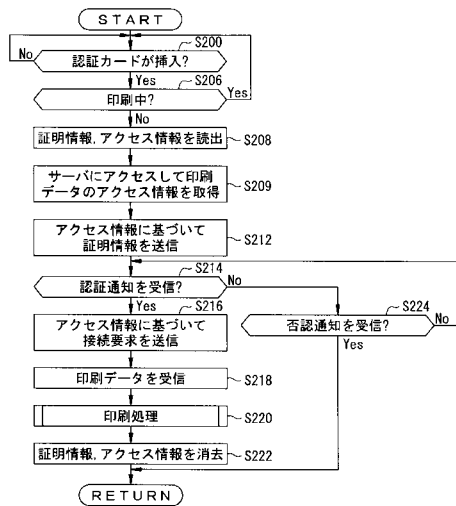
【図 15】



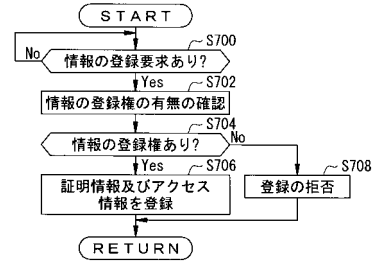
【図 16】



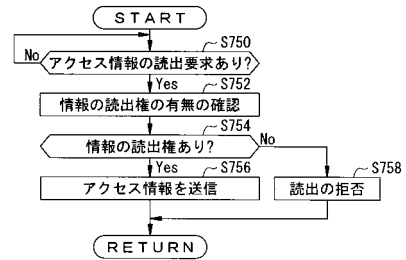
【図 17】



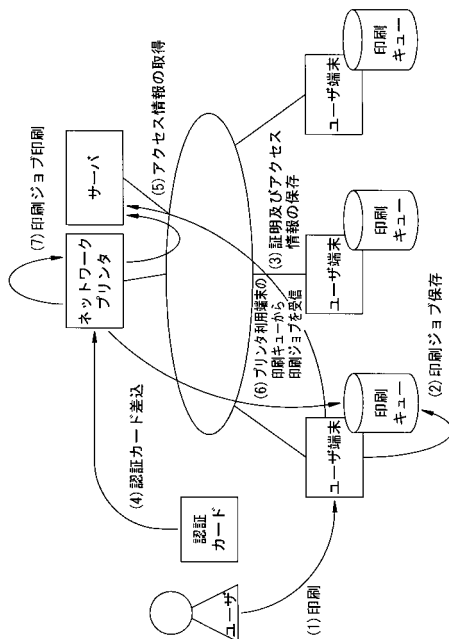
【図 18】



【図 19】



【図 20】



フロントページの続き

(51)Int.Cl.⁷ F I テーマコード (参考)
G O 6 K 19/00 T

(72)発明者 北田 成秀

長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

Fターム(参考) 2C061 AP01 HJ08 HK11 HP00

5B021 AA01 CC05 EE01 EE04 NN18

5B035 AA13 BC03 CA23 CA29

5B058 CA01 KA31 KA33 YA20

5B085 AE12 BE07

(54)【発明の名称】 認証動作システム、認証印刷システム、ネットワークプリンタ、プリンタ利用端末、プリンタ用プログラム及び利用端末用プログラム、並びに認証印刷方法及びプリンタ利用端末の出力制限方法