

(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2008-192051
(P2008-192051A)

(43) 公開日 平成20年8月21日(2008.8.21)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 3/12 (2006.01)	G06F 3/12 C	2C061
B41J 29/00 (2006.01)	B41J 29/00 Z	5B021

審査請求 未請求 請求項の数 14 O L (全 28 頁)

(21) 出願番号 特願2007-28158 (P2007-28158)
(22) 出願日 平成19年2月7日(2007.2.7)

(71) 出願人 500112146
サイレックス・テクノロジー株式会社
京都府相楽郡精華町光台二丁目3番地1
(74) 代理人 100123504
弁理士 小倉 啓七
(72) 発明者 井村 慶崇
大阪府東大阪市小阪本町1丁目6番20号
サイレックス・テクノロジー株式会社内
Fターム(参考) 2C061 AP01 BB15 CL08 HH03 HJ08
HK03 HK04 HN02 HN05 HN15
5B021 AA01 CC00

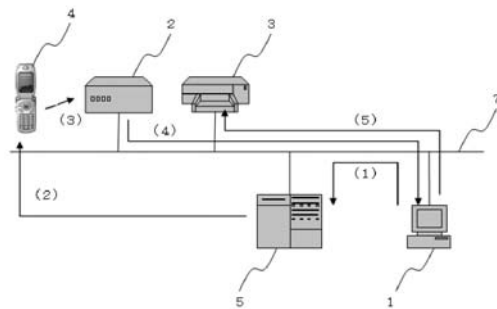
(54) 【発明の名称】 携帯端末を使用したセキュリティ印刷システム並びにセキュリティ印刷方法

(57) 【要約】

【課題】クライアント端末が印刷を実行する場合に、すぐに印刷ジョブをプリンタ端末に送信しないで、ユーザがプリンタ端末側に移動してから、クライアント端末が印刷ジョブを送信できる、機密性が高くユーザの利便性に優れた印刷システムを提供する。

【解決手段】クライアント端末から電子メールを用いて印刷ジョブ用認証データを携帯端末に取得させ、携帯端末から認証装置に非接触でデータを取得させることで、印刷ジョブの所在情報を保存した記憶媒体のやり取り、そして記憶媒体の装着作業を不要とする。携帯端末から認証装置に非接触でデータを取得させる手段としては、印刷ジョブ用認証データを2次元バーコードデータとし、携帯端末の表示画面に表示された2次元バーコードを認証装置に備えられたバーコードリーダを用いて読み込ませる。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

プリンタ端末と認証装置とクライアント端末とメールサーバと携帯端末とがネットワークで接続されるシステムであって、

前記クライアント端末は、

少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成手段と、

前記印刷ジョブ用認証データを電子メールに添付して前記メールサーバを介して前記携帯端末に送信するメール送信手段と、

前記認証装置から、少なくとも印刷ジョブ情報とプリンタ端末情報とを受信する印刷指示データ受信手段と、

前記印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、前記プリンタ端末情報に対応するプリンタ端末に送信する印刷ジョブ送信手段と、を備え、

前記認証装置は、

前記プリンタ端末情報の設定手段と、

前記携帯端末から前記印刷ジョブ用認証データを取得し解析する手段と、

前記クライアント端末に対して少なくとも印刷ジョブ情報とプリンタ端末情報とを送信する印刷指示データ送信手段と、を備え、

前記認証装置が前記携帯端末から前記印刷ジョブ用認証データを取得した場合、前記クライアント端末から前記プリンタ端末に印刷ジョブが送信され、印刷が実行されることを特徴とするセキュリティ印刷システム。

【請求項 2】

認証装置を内蔵したプリンタ端末とクライアント端末とメールサーバと携帯端末とがネットワークで接続されるシステムであって、

前記クライアント端末は、

少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成手段と、

前記印刷ジョブ用認証データを電子メールに添付して前記メールサーバを介して前記携帯端末に送信するメール送信手段と、

前記認証装置から、少なくとも印刷ジョブ情報とプリンタ端末情報とを受信する印刷指示データ受信手段と、

前記印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、前記プリンタ端末情報に対応するプリンタ端末に送信する印刷ジョブ送信手段と、を備え、

前記認証装置は、

前記携帯端末から前記印刷ジョブ用認証データを取得し解析する手段と、

前記クライアント端末に対して少なくとも印刷ジョブ情報とプリンタ端末情報とを送信する印刷指示データ送信手段と、を備え、

前記認証装置が前記携帯端末から前記印刷ジョブ用認証データを取得した場合、前記クライアント端末から前記プリンタ端末に印刷ジョブが送信され、印刷が実行されることを特徴とするセキュリティ印刷システム。

【請求項 3】

プリンタ端末とプリントサーバ機能を備えた認証装置とがローカルに接続され、当該認証装置とクライアント端末とメールサーバと携帯端末とがネットワークで接続されるシステムであって、

前記クライアント端末は、

少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成手段と、

前記印刷ジョブ用認証データを電子メールに添付して前記メールサーバを介して前記携

10

20

30

40

50

帯端末に送信するメール送信手段と、

前記認証装置から、少なくとも印刷ジョブ情報を受信する印刷指示データ受信手段と、
前記印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、
前記認証装置に送信する印刷ジョブ送信手段と、を備え、

前記認証装置は、

前記携帯端末から前記印刷ジョブ用認証データを取得し解析する手段と、

前記クライアント端末に対して少なくとも印刷ジョブ情報を送信する印刷指示データ送信手段と、を備え、

前記認証装置が前記携帯端末から前記印刷ジョブ用認証データを取得した場合、前記クライアント端末から前記認証装置に印刷ジョブが送信され、前記認証装置のプリントサーバ機能によりローカル接続されたプリンタ端末から印刷が実行されることを特徴とするセキュリティ印刷システム。

10

【請求項 4】

プリンタ端末とプリントサーバ機能を備えた認証装置とがローカルに接続され、当該認証装置とクライアント端末とメールサーバとスプールサーバと携帯端末とがネットワークで接続されるシステムであって、

前記クライアント端末は、

少なくとも印刷ジョブ情報とスプールサーバ識別情報とを含む印刷ジョブ用認証データを生成する認証データ生成手段と、

前記印刷ジョブ用認証データを電子メールに添付して前記メールサーバを介して前記携帯端末に送信するメール送信手段と、

20

前記スプールサーバに印刷ジョブを送信する印刷ジョブ送信手段と、を備え、

前記認証装置は、

前記携帯端末から前記印刷ジョブ用認証データを取得し解析する手段と、

前記スプールサーバから印刷ジョブを取得する印刷ジョブ取得手段と、を備え、

前記スプールサーバは、

前記認証装置から、少なくとも印刷ジョブ情報を受信する印刷ジョブ要求受信手段と、

前記印刷ジョブ要求受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、

前記認証装置に送信する印刷ジョブ送信手段と、を備え、

前記認証装置が前記携帯端末から前記印刷ジョブ用認証データを取得した場合、前記スプールサーバから前記認証装置に印刷ジョブが送信され、前記認証装置のプリントサーバ機能によりローカル接続されたプリンタ端末から印刷が実行されることを特徴とするセキュリティ印刷システム。

30

【請求項 5】

前記スプールサーバがメールサーバの機能を有し、前記クライアント端末がスプールサーバに対して印刷ジョブを送信する前記印刷ジョブ送信手段、および/又は、前記認証装置がスプールサーバから印刷ジョブを取得する前記印刷ジョブ取得手段において、印刷ジョブデータの通信に電子メール転送プロトコルを用いることを特徴とする請求項 4 に記載のセキュリティ印刷システム。

【請求項 6】

40

前記印刷ジョブ用認証データは 2 次元バーコードデータであり、

前記携帯端末から前記印刷ジョブ用認証データを取得し解析する手段は、携帯端末の表示画面に表示された 2 次元バーコードを前記認証装置に備えられたバーコードリーダを用いて読み込ませることであることを特徴する請求項 1 乃至 5 のいずれか 1 項に記載のセキュリティ印刷システム。

【請求項 7】

前記携帯端末は、メール受信機能を備えた携帯電話であることを特徴とする請求項 1 乃至 5 のいずれか 1 項に記載のセキュリティ印刷システム。

【請求項 8】

プリンタ端末と認証装置とクライアント端末とメールサーバと携帯端末とがネットワー

50

クで接続されるシステムを用いた印刷方法であって、

前記クライアント端末において、

少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成ステップと、

前記印刷ジョブ用認証データを電子メールに添付して前記メールサーバを介して前記携帯端末に送信するメール送信ステップと、

前記認証装置から、少なくとも印刷ジョブ情報とプリンタ端末情報とを受信する印刷ジョブ情報受信ステップと、

前記印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、前記プリンタ端末情報に対応するプリンタ端末に送信する印刷ジョブ送信ステップと、

を備え、

前記認証装置において、

前記プリンタ端末情報の設定ステップと、

前記携帯端末から前記印刷ジョブ用認証データを取得し解析するステップと、

前記クライアント端末に対して少なくとも印刷ジョブ情報とプリンタ端末情報とを送信する印刷指示データ送信ステップと、を備え、

前記認証装置が前記携帯端末から前記印刷ジョブ用認証データを取得した場合、前記クライアント端末から前記プリンタ端末に印刷ジョブが送信され、印刷が実行されることを特徴とするセキュリティ印刷方法。

【請求項 9】

認証装置を内蔵したプリンタ端末とクライアント端末とメールサーバと携帯端末とがネットワークで接続されるシステムを用いた印刷方法であって、

前記クライアント端末において、

少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成ステップと、

前記印刷ジョブ用認証データを電子メールに添付して前記メールサーバを介して前記携帯端末に送信するメール送信ステップと、

前記認証装置から、少なくとも印刷ジョブ情報とプリンタ端末情報とを受信する印刷ジョブ情報受信ステップと、

前記印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、前記プリンタ端末情報に対応するプリンタ端末に送信する印刷ジョブ送信ステップと、

を備え、

前記認証装置において、

前記携帯端末から前記印刷ジョブ用認証データを取得し解析するステップと、

前記クライアント端末に対して少なくとも印刷ジョブ情報とプリンタ端末情報とを送信する印刷指示データ送信ステップと、を備え、

前記認証装置が前記携帯端末から前記印刷ジョブ用認証データを取得した場合、前記クライアント端末から前記プリンタ端末に印刷ジョブが送信され、印刷が実行されることを特徴とするセキュリティ印刷方法。

【請求項 10】

プリンタ端末とプリントサーバ機能を備えた認証装置とがローカルに接続され、当該認証装置とクライアント端末とメールサーバと携帯端末とがネットワークで接続されるシステムを用いた印刷方法であって、

前記クライアント端末において、

少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成ステップと、

前記印刷ジョブ用認証データを電子メールに添付して前記メールサーバを介して前記携帯端末に送信するメール送信ステップと、

前記認証装置から、少なくとも印刷ジョブ情報を受信する印刷ジョブ情報受信ステップと、

10

20

30

40

50

前記印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、前記認証装置に送信する印刷ジョブ送信ステップと、を備え、

前記認証装置において、

前記携帯端末から前記印刷ジョブ用認証データを取得し解析するステップと、

前記クライアント端末に対して少なくとも印刷ジョブ情報を送信する印刷指示データ送信ステップと、を備え、

前記認証装置が前記携帯端末から前記印刷ジョブ用認証データを取得した場合、前記クライアント端末から前記認証装置に印刷ジョブが送信され、前記認証装置のプリントサーバ機能によりローカル接続されたプリンタ端末から印刷が実行されることを特徴とするセキュリティ印刷方法。

10

【請求項 11】

プリンタ端末とプリントサーバ機能を備えた認証装置とがローカルに接続され、当該認証装置とクライアント端末とメールサーバとスプールサーバと携帯端末とがネットワークで接続されるシステムを用いた印刷方法であって、

前記クライアント端末において、

少なくとも印刷ジョブ情報とスプールサーバ識別情報とを含む印刷ジョブ用認証データを生成する認証データ生成ステップと、

前記印刷ジョブ用認証データを電子メールに添付して前記メールサーバを介して前記携帯端末に送信するメール送信ステップと、

前記スプールサーバに印刷ジョブを送信する印刷ジョブ送信ステップと、を備え、

20

前記認証装置において、

前記携帯端末から前記印刷ジョブ用認証データを取得し解析するステップと、

前記スプールサーバから印刷ジョブを取得する印刷ジョブ取得ステップと、を備え、

前記スプールサーバにおいて、

前記認証装置から、少なくとも印刷ジョブ情報を受信する印刷ジョブ要求受信ステップと、

前記印刷ジョブ要求受信ステップにて取得した印刷ジョブ情報から特定された印刷ジョブを、前記認証装置に送信する印刷ジョブ送信ステップと、を備え、

前記認証装置が前記携帯端末から前記印刷ジョブ用認証データを取得した場合、前記スプールサーバから前記認証装置に印刷ジョブが送信され、前記認証装置のプリントサーバ機能によりローカル接続されたプリンタ端末から印刷が実行されることを特徴とするセキュリティ印刷方法。

30

【請求項 12】

前記スプールサーバがメールサーバの機能を有し、前記クライアント端末がスプールサーバに対して印刷ジョブを送信する前記印刷ジョブ送信手段、および/又は、前記認証装置がスプールサーバから印刷ジョブを取得する前記印刷ジョブ取得手段において、印刷ジョブデータの通信に電子メール転送プロトコルを用いることを特徴とする請求項 4 に記載のセキュリティ印刷方法。

【請求項 13】

前記印刷ジョブ用認証データは 2 次元バーコードデータであり、

40

前記携帯端末から前記印刷ジョブ用認証データを取得し解析するステップは、携帯端末の表示画面に表示された 2 次元バーコードを前記認証装置に備えられたバーコードリーダを用いて読み込ませることであることを特徴する請求項 7 乃至 10 のいずれか 1 項に記載のセキュリティ印刷方法。

【請求項 14】

前記携帯端末は、メール受信機能を備えた携帯電話であることを特徴とする請求項 7 乃至 10 のいずれか 1 項に記載のセキュリティ印刷方法。

【発明の詳細な説明】

【技術分野】

【0001】

50

本発明は、携帯端末を使用したセキュリティ印刷システム並びにセキュリティ印刷方法に関する。

【背景技術】

【0002】

従来、ネットワーク上のクライアント端末がプリンタ端末を共有するシステムにおいて、携帯端末を用いたセキュリティ印刷を行う技術が知られている（特許文献1）。これは、クライアント端末が印刷を実行する場合に、携帯端末にパスワードを送信し、プリンタ端末に電話番号とパスワードを付加した印刷ジョブを送信する。そして、ユーザがネットワーク上のプリンタ端末に移動して、携帯端末から電話番号とパスワードをプリンタ端末に送信し、プリンタ側で照合ができた場合に印刷が行われるというものである。

10

【0003】

しかし、この携帯端末から電話番号とパスワードをプリンタ端末に送信してプリンタ側で照合するシステムでは、印刷ジョブがプリンタ端末に送信されてからユーザがプリンタ端末側へ移動するまでの間について、印刷ジョブがプリンタ端末内に保持された状態となることから機密性の問題がある。

また、印刷ジョブをプリンタ端末へ送信した後で、プリンタ端末にトラブルが発生した場合、印刷ジョブを再送信しなければならないといった問題がある。

さらに、プリンタ端末側で、電話番号とパスワードの照合機能が必要となる。

【0004】

そこで、クライアント端末が印刷を実行する場合に、すぐに印刷ジョブをプリンタ端末に送信しないで、ユーザがプリンタ端末側に移動してから、クライアント端末が印刷ジョブを送信する技術が知られている（特許文献2）。

20

これは、クライアント端末が印刷を実行する場合に、その印刷ジョブの所在情報（クライアント端末のIPアドレスと印刷ジョブ番号）を携帯可能な記憶媒体に出力する。そして、ユーザがプリンタ端末側に移動して、プリンタ端末が記憶媒体から印刷ジョブの所在情報を取得すると共に、この印刷ジョブの所在情報より特定されるクライアント端末から印刷ジョブを受信するというものである。

このため、特許文献1に開示されている技術の如く、予め印刷ジョブをプリンタ端末に送信する場合と比べ、機密性を向上させることができる。

【0005】

30

しかし、上記技術では、クライアント端末に携帯可能な記憶媒体を装着し、印刷ジョブの所在情報を当該携帯可能な記憶媒体に出力する必要がある。また、ユーザがその記憶媒体を持ち運んでプリンタ端末側に装着する必要がある。この装着作業はユーザにとって利便性があまり良くない。

また、クライアント端末で印刷操作する者と、プリンタ端末で印刷物を受け取る者が異なり、クライアント端末とプリンタ端末が別フロア・別建屋等の離散された場所に設置されているといった場合に、記憶媒体でやり取りするのは利便性が低く、現実的でない。

【0006】

そこで、セキュリティを保つために、印刷を行った本人が印刷物を受け取るシステムとして、個人識別を行う非接触ICカード等を使うシステムが開発されている。

40

これは、クライアント端末から印刷を実行した後に、プリンタ端末に内蔵された認証装置（認証装置がプリンタ端末と独立にネットワークに接続されている場合も同様）に、印刷を実行した印刷ジョブの所在情報（クライアント端末のIPアドレスと印刷ジョブ番号）とICカード情報を通知する。認証装置は、認証装置内データベースに印刷ジョブの所在情報とICカード情報を保存する。ユーザが認証装置に接続されているカードリーダーに、非接触でICカードの読み込みをさせる。認証装置は認証装置内のデータベースを使用してクライアント端末を特定する。認証装置は、特定したクライアント端末に対して印刷先であるプリンタ端末と印刷ジョブの印刷開始を指示する。クライアント端末は、認証装置から指示されたプリンタ端末の情報を基づいて、プリンタ端末に対して印刷ジョブを送信するというものである。

50

【 0 0 0 7 】

しかしながら、上記の非接触 IC カード等を使うシステムの問題点は、認証装置内にデータベースがあることである。認証装置は、データベースの管理を行う必要があり、また、認証装置内にデータベースがあることで、IC カード情報などのセキュリティ情報が認証装置に集中してしまうという問題もある。

さらに、クライアント端末側でも、予めクライアント端末に IC カード情報が必要となるため、カードリーダーを使い IC カード情報を登録する必要があるなど煩雑な前準備が必要となる問題もある。

【 0 0 0 8 】

【特許文献 1】特開 2 0 0 2 - 1 6 3 0 9 4 号公報

10

【特許文献 2】特開 2 0 0 5 - 3 2 4 4 9 7 号公報

【 発明の開示 】

【発明が解決しようとする課題】

【 0 0 0 9 】

上述の問題点やニーズに対応すべく、本発明は、クライアント端末が印刷を実行する場合に、すぐに印刷ジョブをプリンタ端末に送信しないで、ユーザがプリンタ端末側に移動してから、クライアント端末が印刷ジョブを送信できるシステムを提供することを目的とする。

【 0 0 1 0 】

また、本発明は、クライアント端末側の使用者と、プリンタ端末側の印刷物受領者とが異なる場合に、利便性が向上するように、印刷ジョブの所在情報を保存した記憶媒体のやり取り、そして記憶媒体の装着作業が不要となるシステムを提供することを目的とする。

20

【 0 0 1 1 】

さらに、本発明は、プリンタ端末若しくは認証装置にデータベースを不要とし、セキュリティ情報の集中や漏洩を防ぐことができるシステムを提供することを目的とする。

【課題を解決するための手段】

【 0 0 1 2 】

上記目的を達成するため、本発明の第 1 の観点のセキュリティ印刷システムは、プリンタ端末と認証装置とクライアント端末とメールサーバと携帯端末とがネットワークで接続されるシステムであって、

30

1) クライアント端末は、

- ・少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成手段と、
- ・印刷ジョブ用認証データを電子メールに添付してメールサーバを介して携帯端末に送信するメール送信手段と、
- ・認証装置から、少なくとも印刷ジョブ情報とプリンタ端末情報とを受信する印刷指示データ受信手段と、
- ・印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、プリンタ端末情報に対応するプリンタ端末に送信する印刷ジョブ送信手段と、を備え、

40

2) 認証装置は、

- ・プリンタ端末情報の設定手段と、
 - ・携帯端末から前記印刷ジョブ用認証データを取得し解析する手段と、
 - ・クライアント端末に対して少なくとも印刷ジョブ情報とプリンタ端末情報とを送信する印刷指示データ送信手段と、を備えた構成とされ、
- 認証装置が携帯端末から印刷ジョブ用認証データを取得した場合、クライアント端末からプリンタ端末に印刷ジョブが送信され、印刷が実行されることを特徴とする。

【 0 0 1 3 】

本発明のセキュリティ印刷システムは、クライアント端末により印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成し、その印刷ジョブ用認証データを電子メールに添付してメールサーバを介して携帯端末に送信する。

50

今や電子メールは、コンピュータネットワーク社会において最も利用されるコミュニケーション手段である。LANやインターネット上のクライアント端末や携帯電話などの携帯端末の間で、電子メールを用いた情報のやり取りできる環境は容易に構築できるようになっている。

【0014】

本発明は、この電子メールを用いて印刷ジョブ用認証データを携帯端末に取得させ、さらに、携帯端末から認証装置に非接触でデータを取得させることで、印刷ジョブの所在情報を保存した記憶媒体のやり取り、そして記憶媒体の装着作業が不要とする。また、本発明はプリンタ端末若しくは認証装置にデータベースを不要とし、セキュリティ情報の集中や漏洩を防ぐ。

【0015】

クライアント端末が、認証装置から取得した印刷ジョブ情報から特定された印刷ジョブを、プリンタ端末情報に対応するプリンタ端末に送信することで、クライアント端末が印刷を実行する場合に、すぐに印刷ジョブをプリンタ端末に送信しないで、ユーザがプリンタ端末側に移動してから、クライアント端末が印刷ジョブを送信できることとなる。

【0016】

また、クライアント端末側の使用者とプリンタ端末側の印刷物受領者とが異なる場合にも、以下に述べるように利便性が向上する。

すなわち、印刷ジョブ用認証データを電子メールに添付してメールサーバを介して携帯端末に送信することで、クライアント端末の使用者とプリンタ端末側の印刷物受領者の間で、印刷ジョブ用認証データを保存した記憶媒体のやり取りが不要となり、利便性が向上する。

例えば、印刷物受領者の所有する携帯端末に対して印刷ジョブ用認証データを添付して送信することで、印刷物受領者は、自由な時間に、また任意の場所に設置されているプリンタ端末で、携帯端末からプリンタ端末に印刷ジョブ用認証データを取得させて印刷物の受け取りが可能となるのである。

【0017】

このことは、例えば、個人情報を含む印刷物（用紙は特定のものを使用）を、該個人に引き渡す際にも活用可能である。一例として、先ず情報管理会社から個人の携帯電話に対して印刷ジョブ用認証データをメールに添付して送信する。個人がコンビニエンスストアなどに設置されている認証装置に印刷ジョブ用認証データを送り、プリンタ端末から印刷物を受け取るのである。

【0018】

次に、本発明の第2の観点のセキュリティ印刷システムは、認証装置を内蔵したプリンタ端末とクライアント端末とメールサーバと携帯端末とがネットワークで接続されるシステムであって、

1) クライアント端末は、

・少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成手段と、

・印刷ジョブ用認証データを電子メールに添付してメールサーバを介して携帯端末に送信するメール送信手段と、

・認証装置から、少なくとも印刷ジョブ情報とプリンタ端末情報とを受信する印刷指示データ受信手段と、

・印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、プリンタ端末情報に対応するプリンタ端末に送信する印刷ジョブ送信手段と、を備え、

2) 認証装置は、

・携帯端末から前記印刷ジョブ用認証データを取得し解析する手段と、

・クライアント端末に対して少なくとも印刷ジョブ情報とプリンタ端末情報とを送信する印刷指示データ送信手段と、を備えた構成とされ、

認証装置が携帯端末から印刷ジョブ用認証データを取得した場合、クライアント端末か

10

20

30

40

50

らプリンタ端末に印刷ジョブが送信され、印刷が実行されることを特徴とする。

【0019】

本発明の第2の観点のセキュリティ印刷システムが第1の観点のセキュリティ印刷システムと異なる点は、認証装置がプリンタ端末に内蔵され一体化されていることである。プリンタ端末がネットワークに接続されており、認証装置が携帯端末から印刷ジョブ用認証データを取得した際、一体となっているプリンタ端末から印刷出力される。

認証装置がプリンタ端末と独立にネットワークに接続される第1の観点のセキュリティ印刷システムでは、特殊な装置である認証装置を共用化可能で、印刷出力させるプリンタ端末情報を任意に設定するのである。

【0020】

また、本発明の第3の観点のセキュリティ印刷システムは、プリンタ端末とプリントサーバ機能を備えた認証装置とがローカルに接続され、当該認証装置とクライアント端末とメールサーバとがネットワークで接続されるシステムであって、

1) クライアント端末は、

- ・少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成手段と、
- ・印刷ジョブ用認証データを電子メールに添付してメールサーバを介して携帯端末に送信するメール送信手段と、
- ・認証装置から、少なくとも印刷ジョブ情報を受信する印刷指示データ受信手段と、
- ・印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、認証装置に送信する印刷ジョブ送信手段と、を備え、

2) 認証装置は、

- ・携帯端末から前記印刷ジョブ用認証データを取得し解析する手段と、
- ・クライアント端末に対して少なくとも印刷ジョブ情報を送信する印刷指示データ送信手段と、を備えた構成とされ、

認証装置が携帯端末から前記印刷ジョブ用認証データを取得した場合、クライアント端末から認証装置に印刷ジョブが送信され、認証装置のプリントサーバ機能によりローカル接続されたプリンタ端末から印刷が実行されることを特徴とする。

【0021】

本発明の第3の観点のセキュリティ印刷システムが第1の観点や第2の観点のセキュリティ印刷システムと異なる点は、認証装置がプリンタ端末とローカルに接続されプリントサーバ機能を備えていることである。認証装置が携帯端末から印刷ジョブ用認証データを取得した場合、クライアント端末から認証装置に印刷ジョブが送信され、認証装置のプリントサーバ機能によりローカル接続されたプリンタ端末から印刷出力されることとなる。

【0022】

また、本発明の第4の観点のセキュリティ印刷システムは、プリンタ端末とプリントサーバ機能を備えた認証装置とがローカルに接続され、当該認証装置とクライアント端末とメールサーバとスプールサーバと携帯端末とがネットワークで接続されるシステムであって、

1) クライアント端末は、

- ・少なくとも印刷ジョブ情報とスプールサーバ識別情報とを含む印刷ジョブ用認証データを生成する認証データ生成手段と、
- ・印刷ジョブ用認証データを電子メールに添付してメールサーバを介して携帯端末に送信するメール送信手段と、
- ・スプールサーバに印刷ジョブを送信する印刷ジョブ送信手段と、を備え、

2) 認証装置は、

- ・携帯端末から前記印刷ジョブ用認証データを取得し解析する手段と、
- ・スプールサーバから印刷ジョブを取得する印刷ジョブ取得手段と、を備え、

3) スプールサーバは、

- ・認証装置から、少なくとも印刷ジョブ情報を受信する印刷ジョブ要求受信手段と、

・印刷ジョブ要求受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、認証装置に送信する印刷ジョブ送信手段と、を備えた構成とされ、
認証装置が携帯端末から印刷ジョブ用認証データを取得した場合、スプールサーバから認証装置に印刷ジョブが送信され、認証装置のプリントサーバ機能によりローカル接続されたプリンタ端末から印刷が実行されることを特徴とする。

【0023】

本発明の第4の観点のセキュリティ印刷システムは、本発明の第3の観点のセキュリティ印刷システムをイントラネット内のシステムから、インターネットを介したシステムに拡張するものである。スプールサーバを設け、クライアント端末から印刷ジョブをスプールサーバに送信することで、認証装置が印刷ジョブを取得することが可能となる。

10

ここで、認証装置におけるスプールサーバから印刷ジョブを取得する印刷ジョブ取得手段は、認証装置がスプールサーバに対して少なくとも印刷ジョブ情報を送信し、スプールサーバから印刷ジョブを受信することをいう。

【0024】

本発明の第5の観点のセキュリティ印刷システムは、本発明の第4の観点のセキュリティ印刷システムにおけるスプールサーバがメールサーバの機能を有し、クライアント端末がスプールサーバに対して印刷ジョブを送信する印刷ジョブ送信手段、および/又は、認証装置がスプールサーバから印刷ジョブを取得する印刷ジョブ取得手段において、印刷ジョブデータの通信に電子メール転送プロトコルを用いることを特徴とする。

20

【0025】

クライアント端末や認証装置が、スプールサーバとのデータ通信に電子メールを用いることで、クライアント端末、スプールサーバ、認証装置の間にファイアウォールが存在する場合にも印刷を行うことが可能となる。

ここで、電子メール転送プロトコルとは、具体的には、クライアント端末がスプールサーバに対して印刷ジョブを送信する場合には、印刷ジョブを添付ファイルとした電子メールがSMTP (Simple Mail Transfer Protocol) プロトコルを用いてクライアント端末からスプールサーバに送信されるものであり、また、認証装置がスプールサーバから印刷ジョブを取得する場合には、印刷ジョブを添付ファイルとした電子メールがPOP (Post Office Protocol) プロトコルを用いてスプールサーバから認証装置に送信されるものである。

30

【0026】

本発明の第6の観点のセキュリティ印刷システムは、上述の第1の観点から第5の観点のセキュリティ印刷システムにおいて、印刷ジョブ用認証データを2次元バーコードデータとし、携帯端末の表示画面に表示された2次元バーコードを認証装置に備えられたバーコードリーダを用いて読み込ませることである。印刷ジョブ用認証データを2次元バーコードデータとし、携帯端末の表示画面に表示された2次元バーコードを認証装置に備えられたバーコードリーダを用いて読み込ませることで、携帯端末から認証装置に非接触でデータを取得させることが可能となり利便性が向上する。

【0027】

次に、上述の目的を達成する本発明のセキュリティ印刷方法について説明する。

40

本発明の第8の観点のセキュリティ印刷方法は、プリンタ端末と認証装置とクライアント端末とメールサーバと携帯端末とがネットワークで接続されるシステムを用いた印刷方法であって、

1) クライアント端末において、

- ・少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成ステップと、
- ・印刷ジョブ用認証データを電子メールに添付してメールサーバを介して携帯端末に送信するメール送信ステップと、
- ・認証装置から、少なくとも印刷ジョブ情報とプリンタ端末情報とを受信する印刷ジョブ情報受信ステップと、

50

- ・印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、プリンタ端末情報に対応するプリンタ端末に送信する印刷ジョブ送信ステップと、を備え、
- 2) 認証装置において、
- ・プリンタ端末情報の設定ステップと、
- ・携帯端末から印刷ジョブ用認証データを取得し解析するステップと、
- ・クライアント端末に対して少なくとも印刷ジョブ情報とプリンタ端末情報とを送信する印刷指示データ送信ステップと、を備え、

認証装置が携帯端末から印刷ジョブ用認証データを取得した場合、クライアント端末からプリンタ端末に印刷ジョブが送信され、印刷が実行されることを特徴とする。

【0028】

また、本発明の第9の観点のセキュリティ印刷方法は、認証装置を内蔵したプリンタ端末とクライアント端末とメールサーバと携帯端末とがネットワークで接続されるシステムを用いた印刷方法であって、

- 1) クライアント端末において、
- ・少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成ステップと、
- ・印刷ジョブ用認証データを電子メールに添付してメールサーバを介して携帯端末に送信するメール送信ステップと、
- ・認証装置から、少なくとも印刷ジョブ情報とプリンタ端末情報とを受信する印刷ジョブ情報受信ステップと、

- ・印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、プリンタ端末情報に対応するプリンタ端末に送信する印刷ジョブ送信ステップと、を備え、
- 2) 認証装置において、

- ・携帯端末から印刷ジョブ用認証データを取得し解析するステップと、
- ・クライアント端末に対して少なくとも印刷ジョブ情報とプリンタ端末情報とを送信する印刷指示データ送信ステップと、を備え、

認証装置が携帯端末から印刷ジョブ用認証データを取得した場合、クライアント端末からプリンタ端末に印刷ジョブが送信され、印刷が実行されることを特徴とする。

【0029】

また、本発明の第10の観点のセキュリティ印刷方法は、プリンタ端末とプリントサーバ機能を備えた認証装置とがローカルに接続され、当該認証装置とプリントサーバ機能を備えた認証装置とクライアント端末とメールサーバと携帯端末とがネットワークで接続されるシステムを用いた印刷方法であって、

- 1) クライアント端末において、
- ・少なくとも印刷ジョブ情報とクライアント端末情報とを含む印刷ジョブ用認証データを生成する認証データ生成ステップと、
- ・印刷ジョブ用認証データを電子メールに添付してメールサーバを介して携帯端末に送信するメール送信ステップと、
- ・認証装置から、少なくとも印刷ジョブ情報を受信する印刷ジョブ情報受信ステップと、
- ・印刷指示データ受信手段にて取得した印刷ジョブ情報から特定された印刷ジョブを、認証装置に送信する印刷ジョブ送信ステップと、を備え、

- 2) 認証装置において、
- ・携帯端末から印刷ジョブ用認証データを取得し解析するステップと、
- ・クライアント端末に対して少なくとも印刷ジョブ情報を送信する印刷指示データ送信ステップと、を備え、

認証装置が携帯端末から印刷ジョブ用認証データを取得した場合、クライアント端末から認証装置に印刷ジョブが送信され、認証装置のプリントサーバ機能によりローカル接続されたプリンタ端末から印刷が実行されることを特徴とする。

【0030】

また、本発明の第11の観点のセキュリティ印刷方法は、プリンタ端末とプリンタサー

10

20

30

40

50

バ機能を備えた認証装置とがローカルに接続され、当該認証装置とクライアント端末とメールサーバとスプールサーバと携帯端末とがネットワークで接続されるシステムを用いた印刷方法であって、

1) クライアント端末において、

- ・少なくとも印刷ジョブ情報とスプールサーバ識別情報とを含む印刷ジョブ用認証データを生成する認証データ生成ステップと、
- ・印刷ジョブ用認証データを電子メールに添付してメールサーバを介して携帯端末に送信するメール送信ステップと、
- ・スプールサーバに印刷ジョブを送信する印刷ジョブ送信ステップと、を備え、

2) 認証装置において、

- ・携帯端末から印刷ジョブ用認証データを取得し解析するステップと、
- ・スプールサーバから印刷ジョブを取得する印刷ジョブ取得ステップと、を備え、

3) スプールサーバにおいて、

- ・認証装置から、少なくとも印刷ジョブ情報を受信する印刷ジョブ要求受信ステップと、
- ・印刷ジョブ要求受信ステップにて取得した印刷ジョブ情報から特定された印刷ジョブを、認証装置に送信する印刷ジョブ送信ステップと、を備え、

認証装置が携帯端末から印刷ジョブ用認証データを取得した場合、スプールサーバから認証装置に印刷ジョブが送信され、認証装置のプリントサーバ機能によりローカル接続されたプリンタ端末から印刷が実行されることを特徴とする。

【0031】

本発明の第12の観点のセキュリティ印刷方法は、本発明の第11の観点のセキュリティ印刷方法におけるスプールサーバがメールサーバの機能を有し、クライアント端末がスプールサーバに対して印刷ジョブを送信する印刷ジョブ送信手段、および/又は、認証装置がスプールサーバから印刷ジョブを取得する印刷ジョブ取得手段において、印刷ジョブデータの通信に電子メール転送プロトコルを用いることを特徴とする。

【0032】

本発明の第13の観点のセキュリティ印刷方法は、上述の第8の観点から第12の観点のセキュリティ印刷方法において、印刷ジョブ用認証データは2次元バーコードデータであり、携帯端末から印刷ジョブ用認証データを取得し解析するステップは、携帯端末の表示画面に表示された2次元バーコードを認証装置に備えられたバーコードリーダを用いて読み込ませることであることを特徴する。

【発明の効果】

【0033】

本発明のセキュリティ印刷システムによれば、クライアント端末が印刷を実行する場合に、すぐに印刷ジョブをプリンタ端末に送信しないで、ユーザがプリンタ端末側に移動してから、クライアント端末が印刷ジョブを送信できるため、機密性が高い印刷システムを提供できる。

また、クライアント端末側の使用者とプリンタ端末側の印刷物受領者とが異なる場合に、印刷ジョブの所在情報を保存した記憶媒体のやり取り、そして記憶媒体の装着作業が不要とできるため、利便性が高い印刷システムを提供できる。

さらに、プリンタ端末若しくは認証装置にデータベースを不要とし、セキュリティ情報の集中化や誤り等のヒューマンエラーのリスクを低減できるといった効果がある。

【発明を実施するための最良の形態】

【0034】

以下、本発明のセキュリティ印刷システムの実施形態について、図面を参照しながら詳細に説明していく。ただし、本発明の範囲は、図示例に限定されるものではない。

【実施例1】

【0035】

図1は、実施例1のセキュリティ印刷システムの概略システム構成図を示している。実施例1のセキュリティ印刷システムは、図1に示されるように、プリンタ端末3と認証装

10

20

30

40

50

置 2 とクライアント端末 1 とメールサーバ 5 が LAN (Local Area Network) 等のネットワークで接続された構成となっている。また、携帯端末 4 として携帯電話がシステムの構成要素になっている。

実施例 1 のセキュリティ印刷システムの処理フローについて、図 1 に示される (1) ~ (5) のフローの順に説明を行う。

【 0 0 3 6 】

(1) 処理 1

クライアント端末 1 で印刷を指示したとき、クライアント端末 1 は、携帯端末 4 のメールアドレスを宛先とした電子メールを作成し、当該電子メールに印刷ジョブ用認証データ (クライアント端末情報および印刷ジョブ情報) を添付して、メールサーバ 5 へ送信する。電子メールの送信には SMTP (Simple Mail Transfer Protocol) を使用する。

ここで、クライアント端末情報としては、ホスト名、IP アドレス、LAN I / F の MAC (Media Access Control) アドレス等、ネットワーク上に接続されたクライアント端末を識別可能な情報を 1 又は複数組み合わせる。また、印刷ジョブ情報としては、印刷ジョブ名、印刷ジョブ ID 等、印刷ジョブを一意に特定可能な情報を 1 又は複数組み合わせる。

なお、電子メールの添付データとしては、かかる印刷ジョブ用認証データを 2 次元バーコードにデータ変換したものをを用いる。

また、クライアント端末 1 で生成された印刷ジョブはクライアント端末にて保持される。

【 0 0 3 7 】

(2) 処理 2

次に、メールサーバ 5 は、上記処理 1 のメール送信先 (携帯端末 4) に対して電子メールを転送する。

【 0 0 3 8 】

(3) 処理 3

携帯端末 4 のユーザは、上記処理 2 で送られた電子メールに添付されている 2 次元バーコードを携帯端末 4 の画面に表示させ、プリンタ端末 3 近辺の認証装置 2 のバーコードリーダーを用いて、当該 2 次元バーコードを認証装置 2 に読み取らせる。

【 0 0 3 9 】

(4) 処理 4

認証装置 2 は、上記処理 3 で取得した印刷ジョブ用認証データ (クライアント端末情報および印刷ジョブ情報) を利用して、印刷開始を要求するクライアント端末 1 を特定する。そして、印刷指示データ (印刷ジョブ情報およびプリンタ端末情報) を当該特定されたクライアント端末 1 に通知する。図 1 ではプリンタ端末 3 が印刷出力するプリンタになるので、プリンタ端末 3 のプリンタ端末情報が送信される。ここでプリンタ端末情報としては、プリンタ名、IP アドレス等、ネットワーク上に接続されたプリンタ端末を識別可能な情報を 1 又は複数組み合わせる。

【 0 0 4 0 】

(5) 処理 5

印刷を行うクライアント端末 1 は、上記処理 4 で認証装置 2 から送信された印刷指示データ (印刷ジョブ情報およびプリンタ端末情報) を基にして、プリンタ端末 3 に送るべき印刷ジョブを特定し、プリンタ端末 3 に対して印刷ジョブを送信する。なお、印刷ジョブの送信には LPR (Line PRinter daemon protocol) 等の印刷プロトコルを使用する。

【 0 0 4 1 】

これにより、プリンタ端末 3 から印刷ジョブに係る印刷物が出力される。上述の (1) ~ (5) の処理動作により、プリンタ端末 3 近辺にいるユーザはプリンタ出力される印刷結果を他人に見られることなく回収することができ、機密性の向上を図ることができる。

また、ユーザ個々の情報を、ユーザ個々が持っている携帯電話に転送し、ユーザ個々が持ち歩くことで認証装置 2 内にユーザが使用するクライアント端末や印刷ジョブ情報等の

10

20

30

40

50

情報を記憶しておく必要がなくなる。これにより、従来のICカード等を用いたセキュリティ印刷システムのように、認証装置2内にデータベースを設ける必要がなくなる。

このことにより、認証装置2が盗難されることによるユーザ個人情報の流出(カード情報流出など)を防ぐことが可能となる。

【0042】

この他、操作性の面においては、クライアント端末側の事前準備もポートモニタに対応するメールアドレス入力程度となり、クライアント端末を使用するユーザの負担も軽減されることになる。

【0043】

さらに、上記処理4で出力先のプリンタ端末3の識別情報(プリンタ端末情報)を認証装置2からクライアント端末1に送る処理を入れているので、同種のプリンタ端末であれば、クライアント端末1で印刷を行った後に出力先のプリンタ端末を任意に選択することも可能になる。印刷を行いたいプリンタ端末に対応する認証装置に対して、携帯端末からバーコードデータを読み込ませることで、該プリンタ端末に印刷物を出力させることができるのである。

10

【0044】

また、異種のプリンタ端末の場合でも、クライアント端末1で印刷を行った後に出力先のプリンタ端末を任意に選択することも可能である。この場合は、印刷の対象として印刷ジョブを特定せず、クライアント端末に記憶されている印刷対象のファイル(文書ファイルや画像ファイルなど)を特定して、それをプリンタ端末で受信し印刷するものとする。

20

印刷対象のファイルを受信したプリンタ端末側で印刷ジョブ生成を行ったり、プリンタ端末により実行可能な印刷ジョブの生成をクライアント端末へ指示し、この指示に伴って生成された印刷ジョブを受信するものとする。

これにより、実行可能な印刷ジョブが異なる異種のプリンタ端末の場合でも、本セキュリティ印刷システムを利用して、クライアント端末1で印刷を行った後に出力先のプリンタ端末を任意に選択することが可能となる。

【0045】

次に、本実施例1の構成とされたセキュリティ印刷システムについて、その概要を図2~図6を参照して詳細に説明する。

【0046】

30

図2は、クライアント端末の機能ブロック図を示している。クライアント端末1は、一般的なパーソナルコンピュータであり、オペレーティングシステム(OS)として、Windows(登録商標)XPが稼動しているものとする。アプリケーション1Aは、文書処理や画像処理等のプログラムである。ユーザは、アプリケーション1Aを操作して印刷を指示する。プリンタドライバ1Bは、印刷対象となるデータをプリンタにて出力可能な形式(PDL等)へと変換するためのプログラムである。ネットワーク通信部1FはTCP/IPモジュールであり、ネットワーク送受信の基本的な処理を行う。

【0047】

ポートモニタ1Cは、印刷ジョブ制御部11C、メール送信部12C、バーコード生成部13C、設定領域部14Cで構成される。印刷ジョブ制御部11Cは、プリンタドライバ1Bから与えられた印刷ジョブを印刷ジョブ格納領域12Dに格納すると共に当該印刷ジョブの情報を管理テーブル11Dに追記する。メール送信部12Cは、SMTPクライアントの機能を有し、電子メールの作成および送信を管理する。バーコード生成部13Cは、印刷ジョブ用認証データを二次元バーコードへと変換する。設定領域部14Cには携帯端末4のメールアドレスが設定されている。

40

【0048】

印刷ジョブスプール領域1Dは、クライアント端末1で印刷ジョブを保持しておくための記憶領域である。管理テーブル11Dは、印刷ジョブ格納領域12Dに格納された印刷ジョブの情報を記憶するテーブルである。印刷ジョブ格納領域12Dは、印刷ジョブを格納するための記憶領域であり、クライアント端末1のHDD(Hard Disk Drive)、RA

50

M (Random Access Memory) 等に設けられる。

【0049】

印刷サービス1Eは、印刷指示データ受信部11Eと印刷ジョブ送信部12Eで構成される。印刷指示データ受信部11Eは、認証装置2から受信した印刷指示データに含まれる情報や指示を印刷ジョブ送信部12Eへ与える。印刷ジョブ送信部12Eは、印刷ジョブのプリンタ端末3への送信処理を管理する。

【0050】

図3は管理テーブルの一例である。印刷ジョブID(001, 002, 003)は、印刷ジョブ格納領域12Dに格納された印刷ジョブに一意に付与される識別情報である。印刷ジョブ名(test1.doc等)は、印刷ジョブの名称である。

10

【0051】

図4は認証装置2の機能ブロック図である。バーコードリーダ31は、USB I/Fを経由して認証装置と接続されている。ここで、バーコードリーダ31は二次元バーコードリーダを例とする。バーコード読出部2Eは、当該バーコードリーダ31で取得された二次元バーコードを取り込む。バーコード解析部2Dは、二次元バーコードを解析し印刷ジョブ用認証データを取得する。

【0052】

また、ネットワーク通信部2Aは、TCP/IPモジュールであり、ネットワーク送受信の基本的な処理を行う。出力先プリンタ設定領域部2Bは、クライアント端末1が印刷ジョブを送信すべきプリンタ端末情報を登録する。ユーザは、認証装置2の操作表示パネル等のユーザI/F37から、若しくはネットワーク上の管理コンピュータ(図示せず)から、出力先プリンタ設定領域部2Bのプリンタ端末情報を設定することができる。印刷指示データ送信部2Cは、印刷ジョブ情報とプリンタ端末情報とをクライアント端末1に送信する。

20

【0053】

また、出力先プリンタ設定領域部2Bにはプリンタ端末情報に加えて印刷設定情報を登録することができる。印刷設定情報とは、クライアント端末が印刷ジョブを送信するときの印刷プロトコル(LPR、RAW等)や印刷ポート(lp等)を設定するための情報である。印刷設定情報を登録するか否かは任意であり本発明が用いられる環境によって適宜判断すればよい。

30

【0054】

図6は認証装置のハードウェア構成図である。認証装置2は、その動作を制御するCPU32と、CPU32が実行時に参照するプログラムやデータが一時的に記憶されるRAM34と、CPU32が実行するための所定のプログラムを格納しているROM33と、LAN等のネットワーク7とデータを送受信するための通信I/F36と、バーコードリーダ31とデータを送受信するためのUSB I/F38と、操作表示パネル等のユーザI/F37と、これらを接続するバスライン35とを備えている。

【0055】

システム全体の処理フローを図5に示している。以下、図5の処理フローに従って順番に説明していく。まず、クライアント端末1では印刷ジョブ情報および印刷ジョブを生成する動作について図2~図3, 図5を参照して説明する。その後、メールサーバ5、携帯端末4の動作を説明し、その後、認証装置2について図4と図6を参照して説明する。そして、再びクライアント端末1の動作を説明する。

40

【0056】

(クライアント端末の動作)

まず、クライアント端末1のユーザは文書処理や画像処理等のアプリケーション1Aから印刷を指示する。クライアント端末1が印刷指示を受けると、プリンタドライバ1Bは、印刷データをプリンタ出力可能な形式(PDL等)へと変換し、印刷ジョブとしてポートモニタ1Cへ与える。

【0057】

50

ポートモニタ 1 C の印刷ジョブ制御部 1 1 C は、プリンタドライバ 1 B から与えられた印刷ジョブを印刷ジョブ格納領域 1 2 D に格納するとともに、管理テーブル 1 1 D に情報（印刷ジョブ ID と印刷ジョブ名）を追記する。

【 0 0 5 8 】

また、ポートモニタ 1 C のメール送信部 1 2 C は、印刷ジョブ用認証データを生成する。印刷ジョブ用認証データにはクライアント端末情報と印刷ジョブ情報が含まれており、クライアント端末情報としては、クライアント端末の IP アドレス、ホスト名等が該当し、印刷ジョブ情報としては、印刷ジョブ ID、印刷ジョブ名等が該当する。実際にはこれらの情報を適宜組み合わせると印刷ジョブ用認証データを生成すればよい。以下の説明では、印刷ジョブ用認証データとして、クライアント端末の IP アドレス、印刷ジョブ ID を利用するものとする。

10

【 0 0 5 9 】

ポートモニタ 1 C のバーコード生成部 1 3 C は、印刷ジョブ用認証データ（クライアント端末の IP アドレス、印刷ジョブ ID）を二次元バーコードに変換する（図 6 のステップ S 0 1）。

【 0 0 6 0 】

メール送信部 1 2 C は、設定領域部 1 4 C から携帯端末 4（図 1 に図示）のメールアドレスを取得する。そして、携帯端末 4 のメールアドレスを宛先とした電子メールに当該二次元バーコードを添付し、メールサーバ 5（図 1 に図示）に送信する。具体的には、メール送信部 1 2 C は当該電子メールをネットワーク通信部 1 F へ与え、ネットワーク通信部 1 F はメールサーバ 5 とのネットワーク接続を確立し送信処理を行う（図 6 のステップ S 0 2）。

20

ここで、バーコード生成部 1 3 C が認証データ生成手段に相当し、メール送信部 1 2 C がメール送信手段に相当する。

【 0 0 6 1 】

なお、本実施例では、セキュリティ印刷システムの運用をスムーズにするため、事前準備として、ポートモニタ 1 C の設定領域部 1 4 C に携帯端末 4 のメールアドレスを登録しておいた。ユーザの入力負担が軽減できるとともに、誤入力によるメール送信ミスを回避することができるからである。また別の方法として、印刷指示を行うごとにユーザがメールアドレスを入力するように構成してもよい。

30

【 0 0 6 2 】

（メールサーバの動作）

クライアント端末 1 から電子メールを受信したメールサーバ 5 は、送信先メールアドレスの携帯端末 4 に向けて、電子メールを送信する（図 6 のステップ S 0 3）。

【 0 0 6 3 】

（携帯端末の動作）

携帯端末 4 は二次元バーコードが添付された電子メールを受信する。携帯端末 4 のユーザは、二次元バーコードを携帯端末の画面に表示し、認証装置 2 のバーコードリーダに読み取らせる（図 6 のステップ S 0 4）。

40

【 0 0 6 4 】

（認証装置の動作）

図 4 に示される認証装置 2 のバーコード読出部 2 E は、バーコードリーダ 3 1 から、携帯端末 4 の画面上の二次元バーコードを取得し、バーコード解析部 2 D に与える。バーコード解析部 2 D は、二次元バーコードを解析し、印刷ジョブ用認証データを取り出す（図 6 のステップ S 0 5）。このバーコードリーダ 3 1 とバーコード読出部 2 E とバーコード解析部 2 D が、携帯端末から印刷ジョブ用認証データを取得し解析する手段に相当する。

【 0 0 6 5 】

そして、取り出した印刷ジョブ用認証データ（クライアント端末の IP アドレス、印刷ジョブ ID）を印刷指示データ送信部 2 C へと与える。印刷指示データ送信部 2 C は、かかる印刷ジョブ用認証データと出力先プリンタ設定領域部 2 B にある登録情報とを適宜組

50

み合わせて印刷指示データを生成する。出力先プリンタ設定領域部 2 B にある登録情報は、プリンタ端末情報（IPアドレス、プリンタ名等）および印刷設定情報（印刷プロトコル、印刷ポート等）である。印刷設定情報の登録は任意でありユーザの判断により登録しなくてもよい。以下の説明では、印刷指示データには、印刷ジョブ用認証データ（クライアント端末の IP アドレス、印刷ジョブ ID）、プリンタ端末情報（プリンタの IP アドレス）、印刷設定情報（印刷プロトコルとして LPR 設定、印刷ポートとして lp 設定）が含まれるものとする。そして、印刷ジョブ用認証データから送信先のクライアント端末を特定し、印刷指示データを、ネットワーク通信部 2 A を経由して送信する（図 6 のステップ S 0 6）。この印刷指示データ送信部 2 C が、印刷指示データ送信手段に相当する。また、出力先プリンタ設定領域部 2 B がプリンタ端末情報の設定手段に相当する。

10

【0066】

（クライアント端末の動作）

クライアント端末 1 の印刷指示データ受信部 1 1 E は、ネットワーク通信部 1 F を経由して印刷指示データを受信する。印刷指示データ受信部 1 1 E は、印刷指示データに含まれる印刷ジョブ ID、プリンタ端末情報、印刷設定情報などを印刷ジョブ送信部 1 2 E へ伝える。印刷ジョブ送信部 1 2 E は、当該印刷ジョブ ID と一致する印刷ジョブを、管理テーブル 1 1 D を用いて検索する。一致する印刷ジョブがあれば、印刷ジョブ送信部 1 2 E は、当該印刷ジョブを印刷ジョブ格納領域 1 2 D から取得する。

【0067】

印刷ジョブ送信部 1 2 E は、プリンタ端末情報から送信すべきプリンタを特定する。また、印刷指示データの中に印刷設定情報が含まれていれば、かかる指示に従い、印刷ジョブの送信を行う。

20

この場合、印刷設定情報が含まれており、印刷プロトコルで LPR、印刷ポート lp が指示されているので、印刷ジョブ送信部 1 2 E は、印刷ジョブを LPR の手順に従って lp に対して送信する。具体的には、印刷ジョブ送信部 1 2 E は印刷ジョブをネットワーク通信部 1 F へ与え、ネットワーク通信部 1 F は、送信先のプリンタ端末 3 とのネットワーク接続を確立し、当該印刷ジョブを送信する。（図 6 のステップ S 0 8）。

ここで、印刷指示データ受信部 1 1 E が印刷指示データ受信手段に相当し、印刷ジョブ送信部 1 2 E が印刷ジョブ送信手段に相当する。

【0068】

30

（プリンタ端末の動作）

プリンタ端末 3 は、クライアント端末 1 から印刷ジョブを受信し印刷出力する。

【実施例 2】

【0069】

次に、実施例 2 のセキュリティ印刷システムについて説明する。図 7 は、実施例 2 のセキュリティ印刷システムの概略システム構成図を示している。実施例 2 のセキュリティ印刷システムは、図 7 に示されるように、認証装置 2 を内蔵したプリンタ端末 3 とクライアント端末 1 とメールサーバ 5 が LAN 等のネットワーク 7 で接続された構成となっている。また、携帯端末 4 として携帯電話がシステムの構成要素になっている。次に、実施例 2 の処理について以下説明する。特に、実施例 1 と異なる処理のところに重点をおいて説明する。

40

【0070】

（1）処理 1

実施例 1 と同様、クライアント端末 1 で印刷を指示したとき、クライアント端末 1 は携帯端末 4 のメールアドレスを宛先とした電子メールを作成し、当該電子メールに印刷ジョブ用認証データ（クライアント端末情報および印刷ジョブ情報）を添付して、メールサーバ 5 へ送信する。電子メールの添付データとしては、実施例 1 と同様、かかる印刷ジョブ用認証データを 2 次元バーコードにデータ変換したものをを用いる。また、クライアント端末 1 で生成された印刷ジョブはクライアント端末にて保持される。

【0071】

50

(2) 処理 2

実施例 1 と同様、メールサーバ 5 は、上記処理 1 のメール送信先（携帯端末 4）に対して電子メールを転送する。

【0072】

(3) 処理 3

携帯端末 4 のユーザは印刷を実行させたいプリンタ端末 3 に移動し、上記処理 2 で送られた電子メールに添付されている 2 次元バーコードを携帯端末 4 の画面に表示させ、プリンタ端末 3 に内蔵された認証装置 2 のバーコードリーダを用いて、当該 2 次元バーコードを認証装置 2 に読み取らせる。

【0073】

(4) 処理 4

認証装置 2 は、上記処理 3 で取得した印刷ジョブ用認証データ（クライアント端末情報および印刷ジョブ情報）を利用して、印刷開始を要求するクライアント端末 1 を特定し、印刷指示データ（印刷ジョブ情報）を当該クライアント端末 1 に伝える。ここで、プリンタ端末情報を送信しない点が、実施例 1 と異なる。

【0074】

(5) 処理 5

実施例 1 と同様、印刷を行うクライアント端末 1 は、上記処理 4 で認証装置 2 から送信された印刷指示データ（印刷ジョブ情報）を基にして、プリンタ端末 3 に送るべき印刷ジョブを特定し、プリンタ端末 3 に対して印刷ジョブを送信する。

【実施例 3】

【0075】

次に、実施例 3 のセキュリティ印刷システムについて説明する。図 8 は、実施例 3 のセキュリティ印刷システムの概略システム構成図を示している。実施例 3 のセキュリティ印刷システムは、図 8 に示されるように、プリンタ端末 3 と周辺ケーブル 9 を介してローカルに接続されプリントサーバ機能を備えた認証装置 2 とクライアント端末 1 とメールサーバ 5 が LAN 等のネットワーク 7 で接続された構成となっている。また、携帯端末 4 として携帯電話がシステムの構成要素になっている。次に、実施例 3 の処理について以下説明する。特に、実施例 1 と異なる処理のところに重点をおいて説明する。

【0076】

(1) 処理 1

実施例 1 と同様、クライアント端末 1 で印刷を指示したとき、クライアント端末 1 は携帯端末 4 のメールアドレスを宛先とした電子メールを作成し、当該電子メールに印刷ジョブ用認証データ（クライアント端末情報および印刷ジョブ情報）を添付して、メールサーバ 5 へ送信する。電子メールの添付データとしては、実施例 1 と同様、かかる印刷ジョブ用認証データを 2 次元バーコードにデータ変換したものをを用いる。また、クライアント端末 1 で生成された印刷ジョブはクライアント端末にて保持される。

【0077】

(2) 処理 2

実施例 1 と同様、メールサーバ 5 は、上記処理 1 のメール送信先（携帯端末 4）に対して電子メールを転送する。

【0078】

(3) 処理 3

携帯端末 4 のユーザは印刷を実行させたいプリンタ端末 3 に接続されている認証装置 2 に移動し、上記処理 2 で送られた電子メールに添付されている 2 次元バーコードを携帯端末 4 の画面に表示させ、認証装置 2 のバーコードリーダを用いて、当該 2 次元バーコードを認証装置 2 に読み取らせる。

【0079】

(4) 処理 4

認証装置 2 は、上記処理 3 で取得した印刷ジョブ用認証データ（クライアント端末情報

10

20

30

40

50

および印刷ジョブ情報)を利用して、印刷開始を要求するクライアント端末1を特定し、印刷指示データ(印刷ジョブ情報)を当該クライアント端末1に伝える。

【0080】

(5) 処理5

実施例1と同様、印刷を行うクライアント端末1は、上記処理4で認証装置2から送信された印刷指示データ(印刷ジョブ情報)を基にして、認証装置2に送るべき印刷ジョブを特定し、認証装置2に対して印刷ジョブを送信する。認証装置2が印刷ジョブを受信すると、認証装置2にローカル接続されたプリンタ端末3に印刷ジョブを送る。プリンタ端末3で印刷が実行される。

【実施例4】

【0081】

図9は、実施例4のセキュリティ印刷システムの概略システム構成図を示している。実施例4のセキュリティ印刷システムは、図9に示されるように、プリンタ端末3とローカルに接続されプリントサーバ機能を備えた認証装置2が、インターネット7Cおよびファイアウォール(Firewall)10を介してクライアント端末1とメールサーバ5とスプールサーバ6とに接続された構成となっている。また、携帯端末4として携帯電話がシステムの構成要素になっている。

以下に、実施例4のセキュリティ印刷システムの処理フローについて、図9に示される(1)~(4)のフローの順に説明を行う。

【0082】

(1) 処理1

クライアント端末1で印刷を指示したとき、クライアント端末1は携帯端末4のメールアドレスを宛先とした電子メールを作成し、当該電子メールに印刷ジョブ用認証データ(スプールサーバ識別情報および印刷ジョブ情報)を添付して、メールサーバ5へ送信する。

【0083】

ここで、スプールサーバ識別情報としては、ホスト名、IPアドレス、URL(Uniform Resource Locator)、LANI/FのMACアドレス等、ネットワーク上に接続されたスプールサーバを識別可能な情報を1又は複数組み合わせる。

また、電子メールの添付データとしては、かかる印刷ジョブ用認証データを2次元バーコードにデータ変換したものを用いる。

また、クライアント端末1は、スプールサーバ6に対して、印刷ジョブを送信する。このスプールサーバ6に対して印刷ジョブを送信する処理が完了することで、クライアント端末1の電源をOFFにしても構わない。

【0084】

(2) 処理2

次に、メールサーバ5は、上記処理1のメール送信先(携帯端末4)に対して電子メールを転送する。

【0085】

(3) 処理3

携帯端末4のユーザは、上記処理2で送られた電子メールに添付されている2次元バーコードを携帯端末4の画面に表示させ、プリンタ端末3がローカルに接続されている認証装置2のバーコードリーダを用いて、2次元バーコードを認証装置2に読み取らせる。

【0086】

(4) 処理4

認証装置2は、上記処理3で取得した印刷ジョブ用認証データ(スプールサーバ識別情報、印刷ジョブ情報)を利用して、印刷開始を要求するスプールサーバ6を特定し、印刷ジョブの取得を行う。このスプールサーバ6と認証装置2の通信は、電子メールを用いることにより、スプールサーバ6と認証装置2の間にファイアウォール(Firewall)10が存在する場合においても通信を行うことが可能となる。

10

20

30

40

50

【 0 0 8 7 】

認証装置 2 は、上記処理 4 で取得した印刷ジョブを、ローカルに接続されたプリンタ端末 3 に送る。これにより、プリンタ端末 3 から印刷ジョブに係る印刷物が出力される。プリンタ端末 3 近辺にいるユーザはプリンタ出力される印刷結果を他人に見られることなく回収することができ、機密性の向上を図ることができる。

また、ユーザ個々の情報を、ユーザ個々が持っている携帯電話に転送し、ユーザ個々が持ち歩くことで認証装置 2 内にユーザが使用するクライアント端末やジョブ情報等の情報を記憶しておく必要がなくなる。これにより、従来の IC カード等を用いたセキュリティ印刷システムのように、認証装置 2 の内にデータベースを設ける必要がなくなる。

このことにより、認証装置 2 が盗難されることによるユーザ個人情報の流出(カード情報流出など)を防ぐことが可能となる。

10

【 0 0 8 8 】

この他、操作性の面においては、クライアント端末側の事前準備もポートモニタに対応するメールアドレス入力程度となり、クライアント端末を使用するユーザの負担も軽減されることになる。

【 0 0 8 9 】

次に、本実施例 4 の構成とされたセキュリティ印刷システムについて、その動作を図 1 0 ~ 図 1 4 を参照して詳細に説明する。

【 0 0 9 0 】

図 1 0 は、実施例 4 のクライアント端末の機能ブロック図を示している。ポートモニタ 1 C は、印刷ジョブ送信部 1 5 C、メール送信部 1 2 C、バーコード生成部 1 3 C、設定領域部 1 4 C で構成される。このうち、印刷ジョブ送信部 1 5 C と設定領域部 1 4 C が実施例 1 とは異なる。印刷ジョブ送信部 1 5 C は、SMTP クライアントの機能を有し、クライアント端末情報および印刷ジョブ情報を記載した電子メールを作成するとともに当該作成した電子メールに印刷ジョブを添付してスプールサーバに送信する。設定領域部 1 4 C は、携帯端末 4 のメールアドレスとスプールサーバ識別情報を記憶している。スプールサーバ識別情報は、スプールサーバの IP アドレス、ホスト名等のネットワーク上に接続されたスプールサーバを識別するための情報である。

20

【 0 0 9 1 】

なお、実施例 4 においては印刷ジョブをクライアント端末 1 にて保持しないため印刷ジョブスプール領域と印刷指示データ受信部は必要としない。上記以外の構成は実施例 1 と同様である。

30

【 0 0 9 2 】

図 1 1 は実施例 4 の認証装置の機能ブロック図である。実施例 4 の認証装置 2 は、プリントサーバ機能を有しておりプリンタ端末 3 と接続されている。印刷ジョブ取得部 4 2 は POP クライアント機能を有し、スプールサーバに格納された電子メールを取得する。プリンタコントロール部 4 1 はプリンタ端末 3 への印刷ジョブの送信処理を管理する。上記以外の構成は実施例 1 と同様である。

【 0 0 9 3 】

図 1 2 は実施例 4 のスプールサーバの機能ブロック図である。実施例 4 のスプールサーバ 6 はメールサーバの機能を有している。電子メール管理部 4 4 は電子メール格納領域 4 5 に格納される電子メールの処理(電子メールの管理、電子メールの書込み、電子メールの読出し)を行う。電子メール格納領域 4 5 は、電子メールを格納するための記憶領域であり、スプールサーバ 6 の HDD、RAM 等に設けられる。ネットワーク通信部 4 3 は TCP/IP モジュールであり、ネットワーク送受信の基本的な処理を行う。

40

【 0 0 9 4 】

システム全体の処理フローを図 1 3 に示している。以下では、図 1 3 の処理フローに従って順に説明を行う。まず、クライアント端末 1 側で印刷ジョブ情報および印刷ジョブを生成する動作について図 1 0 と図 1 3 を参照して説明する。その後、メールサーバ 5、携帯端末 4 の動作を説明し、その後、認証装置 2 について図 1 1 を参照して説明する。その

50

後、スプールサーバ6について図12を参照して説明する。

【0095】

(クライアント端末の動作)

先ず、クライアント端末1のユーザは文書処理や画像処理等のアプリケーション1Aから印刷を指示する。クライアント端末1が印刷指示を受けると、プリンタドライバ1Bは、印刷データをプリンタ出力可能な形式(PDL等)へと変換し、印刷ジョブとしてポートモニタ1Cへ与える。

【0096】

ポートモニタ1Cの印刷ジョブ送信部15Cは、設定領域部14Cからスプールサーバ6の識別情報(IPアドレス、ホスト名等)を取得し、印刷ジョブを送信すべきスプールサーバを特定する。そして、電子メールにクライアント端末情報および印刷ジョブIDを記載の上、印刷ジョブを添付し、スプールサーバ6へ送信する(図13のステップS02)。具体的には、印刷ジョブ送信部15Cは当該電子メールをネットワーク通信部1Fへ与え、ネットワーク通信部1Fはメールサーバ6とのネットワーク接続を確立し送信処理を行う。

10

【0097】

一方、バーコード生成部13Cは、印刷ジョブ用認証データ(クライアント端末情報、印刷ジョブID、スプールサーバ識別情報)を二次元バーコードに変換する(図13のステップS01)。

【0098】

メール送信部12Cは、設定領域部14Cから携帯端末4(図9に図示)のメールアドレスを取得する。そして、携帯端末4のメールアドレスを宛先とした電子メールに当該二次元バーコードを添付してメールサーバ5に送信する。具体的には、メール送信部12Cは当該電子メールをネットワーク通信部1Fへ与え、ネットワーク通信部1Fはメールサーバ5とのネットワーク接続を確立し送信処理を行う。(図13のステップS03)。

20

ここで、バーコード生成部13Cが認証データ生成手段に相当し、メール送信部12Cがメール送信手段に相当し、印刷ジョブ送信部15Cが印刷ジョブ送信手段に相当する。

【0099】

実施例4では、認証装置2からスプールサーバ6を特定することが必要になるので、メール送信部12Cから送信される印刷ジョブ用認証データにはスプールサーバ識別情報が追加されている。

30

【0100】

なお、セキュリティ印刷システムの運用をスムーズにするため、事前準備として、ポートモニタ1Cの設定領域部14Cに携帯端末4のメールアドレスを登録しておいた。ユーザの入力負担が軽減できるとともに、誤入力によるメール送信ミスを回避することができるからである。また別の方法として、印刷指示を行うごとにユーザがクライアント端末からメールアドレスを入力するように構成してもよい。

【0101】

(メールサーバの動作)

クライアント端末1から電子メールを受信したメールサーバ5は、送信先メールアドレスの携帯端末4に向けて、電子メールを送信する(図13のステップS04)。

40

【0102】

(携帯端末の動作)

携帯端末4は二次元バーコードが添付された電子メールを受信する。携帯端末4のユーザは、二次元バーコードを携帯端末4の画面に表示し、認証装置2のバーコードリーダに読み取らせる(図13のステップS05)。

【0103】

(認証装置の動作)

次に、認証装置2の動作について説明する。図11に認証装置の機能ブロック図を示す。また、図14に認証装置のハードウェア構成図を示す。

50

図 1 1 に示される認証装置 2 のバーコード読出部 2 E は、バーコードリーダ 3 1 から、携帯端末 4 の画面上の二次元バーコードを取得し、バーコード解析部 2 D に与える。バーコード解析部 2 D は、二次元バーコードを解析し、印刷ジョブ用認証データを取り出す（図 1 3 のステップ S 0 6）。このバーコードリーダ 3 1 とバーコード読出部 2 E とバーコード解析部 2 D が、携帯端末から前記印刷ジョブ用認証データを取得し解析する手段に相当する。

【 0 1 0 4 】

そして、取り出した印刷ジョブ用認証データ（クライアント端末情報、印刷ジョブ ID、スプールサーバ識別情報）を印刷ジョブ取得部 4 2 へと与える。印刷ジョブ取得部 4 2 は、スプールサーバ識別情報からスプールサーバ 6 を特定し、当該スプールサーバ 6 に対して、印刷ジョブの取得処理を行う。印刷ジョブ用認証データには、クライアント端末情報と印刷ジョブ ID が含まれているので、これらの情報が記載された電子メールをスプールサーバから取得する。具体的には、印刷ジョブ取得部 4 2 は、スプールサーバ 6 に対して、POP（Post Office Protocol）プロトコルを用いて、当該クライアント端末情報と印刷ジョブ ID が記載された電子メールの取得要求を行う（図 1 3 のステップ S 0 7）。

10

【 0 1 0 5 】

なお、印刷ジョブ取得要求は、印刷ジョブ取得部 4 2 からネットワーク通信部 2 A を経由してスプールサーバ 6 に送信される。

この印刷ジョブ取得部 4 2 が、印刷ジョブ取得手段に相当する。

20

【 0 1 0 6 】

（スプールサーバの動作）

次に、スプールサーバの動作について図 1 2 を参照して説明する。

スプールサーバ 6 の電子メール管理部 4 4 は、ネットワーク通信部 4 3 を経由して電子メールを受信し、電子メール格納領域 4 5 に格納する。

【 0 1 0 7 】

スプールサーバ 6 の電子メール管理部 4 4 は、ネットワーク通信部 4 3 経由で認証装置 2 から印刷ジョブ取得要求を受信する。印刷ジョブ取得要求にはクライアント端末情報と印刷ジョブ ID が含まれているので、これらの情報から電子メールを検索し、送信すべき電子メールを特定する（図 1 3 のステップ S 0 8）。

30

【 0 1 0 8 】

電子メール管理部 4 4 は、電子メールを認証装置 2 に送信する。具体的には印刷ジョブを添付した電子メールが電子メール管理部 4 4 からネットワーク通信部 4 3 を経由して認証装置 2 に送信される（図 1 5 のステップ S 0 9）。ここで、電子メール管理部 4 4 が印刷ジョブ要求受信手段および印刷ジョブ送信手段に相当する。

【 0 1 0 9 】

認証装置 2 の印刷ジョブ取得部 4 2 は、電子メールを受信し、添付された印刷ジョブを取り出してプリンタコントロール部 4 1 へ与える。プリンタコントロール部 4 1 は、周辺ケーブル 9 を介してローカル接続されているプリンタ端末 3 に印刷ジョブを転送する（図 1 3 のステップ S 1 0）。

40

【 0 1 1 0 】

（プリンタ端末の動作）

プリンタ端末 3 は、印刷ジョブを印刷出力する。

【 0 1 1 1 】

実施例 4 においてはインターネットを経由する場合を説明したが、本実施例の適用は必ずしもインターネットに限定されるものではない。本実施例はインターネットを経由するシステムだけでなく、インターネットを経由しないシステム（LAN）においても適用可能である。

【 0 1 1 2 】

以上、本発明を実施するための最良の形態について実施例 1 ~ 4 を用いて説明したが、本発明はこうした実施例になんら限定されるものではなく、本発明の要旨を逸脱しない範

50

圏内において、さまざまな形態で実施し得る。

【産業上の利用可能性】

【0113】

本発明のセキュリティ印刷システムは、一般公衆に安全・確実に個人情報等が記載された印刷物を渡すことができるので、コンビニエンスストアなど特定店舗に設置されている認証装置とプリンタ端末を利用することで、インターネットを経由した安全・確実な印刷サービスを提供することができる。

【図面の簡単な説明】

【0114】

【図1】実施例1のセキュリティ印刷システムの概略システム構成図

10

【図2】クライアント端末の機能ブロック図

【図3】クライアント端末が保持する管理テーブルの一例

【図4】認証装置の機能ブロック図

【図5】実施例1のセキュリティ印刷システムの処理フロー図

【図6】認証装置のハードウェア構成図

【図7】実施例2のセキュリティ印刷システムの概略システム構成図

【図8】実施例3のセキュリティ印刷システムの概略システム構成図

【図9】実施例4のセキュリティ印刷システムの概略システム構成図

【図10】実施例4のクライアント端末の機能ブロック図

【図11】実施例4の認証装置の機能ブロック図

20

【図12】実施例4のスプールサーバの機能ブロック図

【図13】実施例4のセキュリティ印刷システムの処理フロー図

【図14】実施例4の認証装置のハードウェア構成図

【符号の説明】

【0115】

1 クライアント端末

2 認証装置

3 プリンタ端末

4 携帯端末

5 メールサーバ

30

6 スプールサーバ

7 ネットワーク

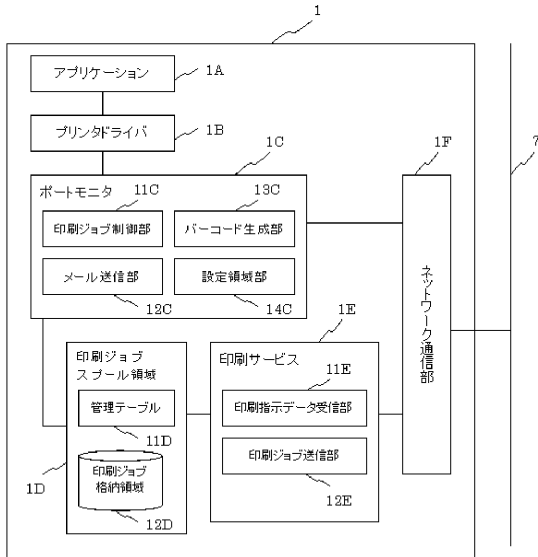
7 a , 7 b イントラネット

7 c インターネット

9 周辺ケーブル

10 ファイアウォール (F i r e W a l l)

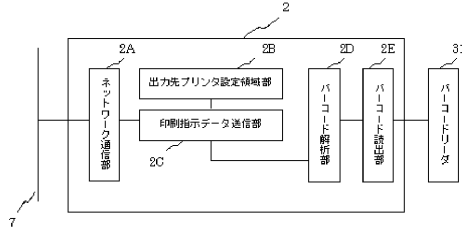
【図 2】



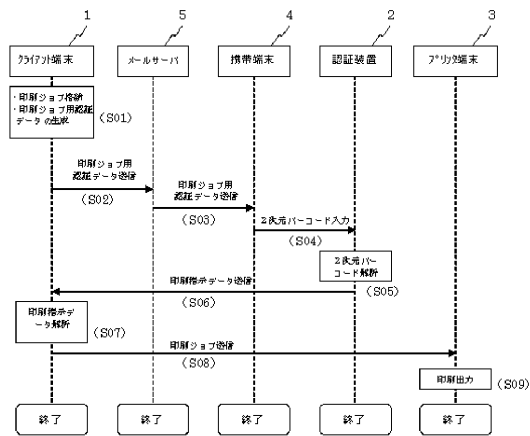
【図 3】

印刷ジョブID	印刷ジョブ名
001	test1.doc
002	test2.doc
003	test3.doc

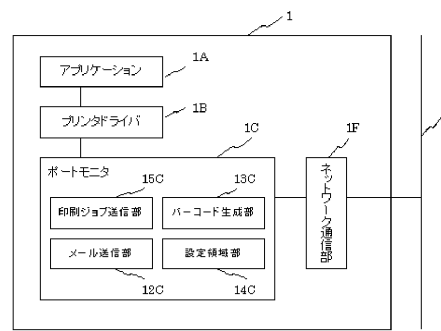
【図 4】



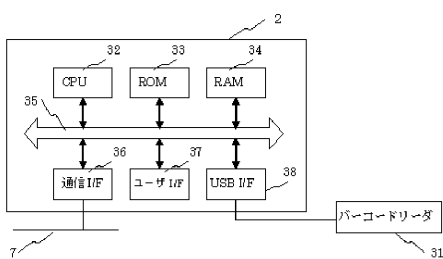
【図 5】



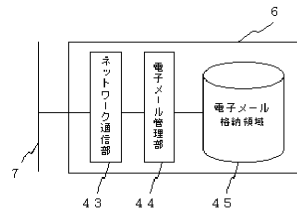
【図 10】



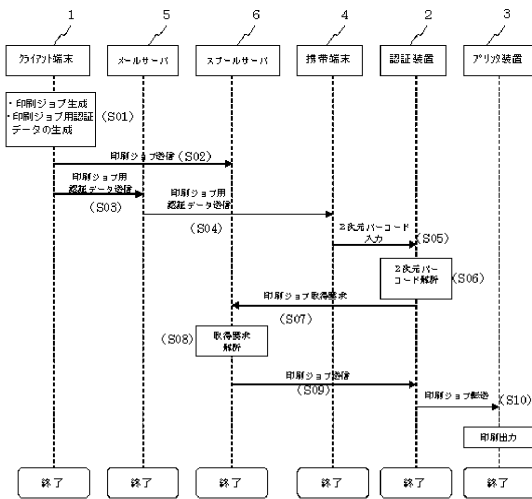
【図 6】



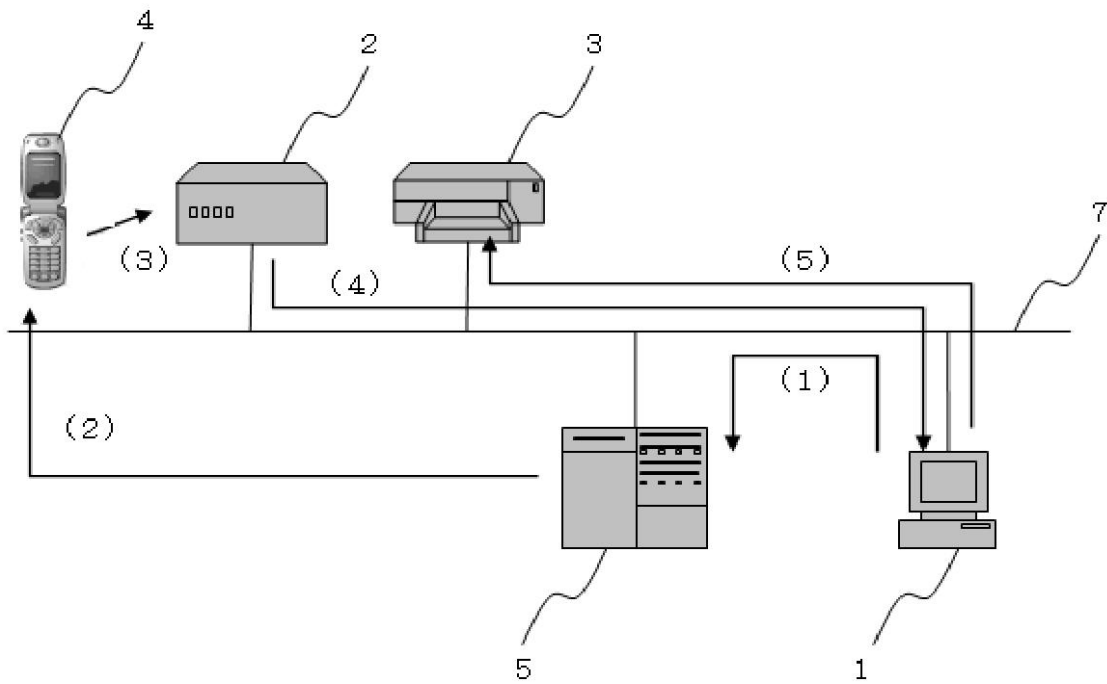
【図 12】



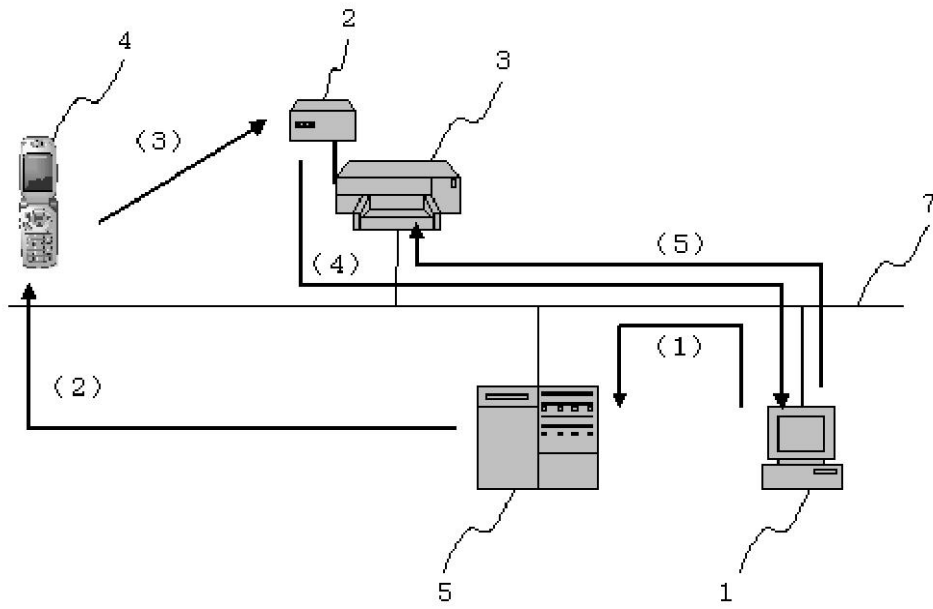
【 図 1 3 】



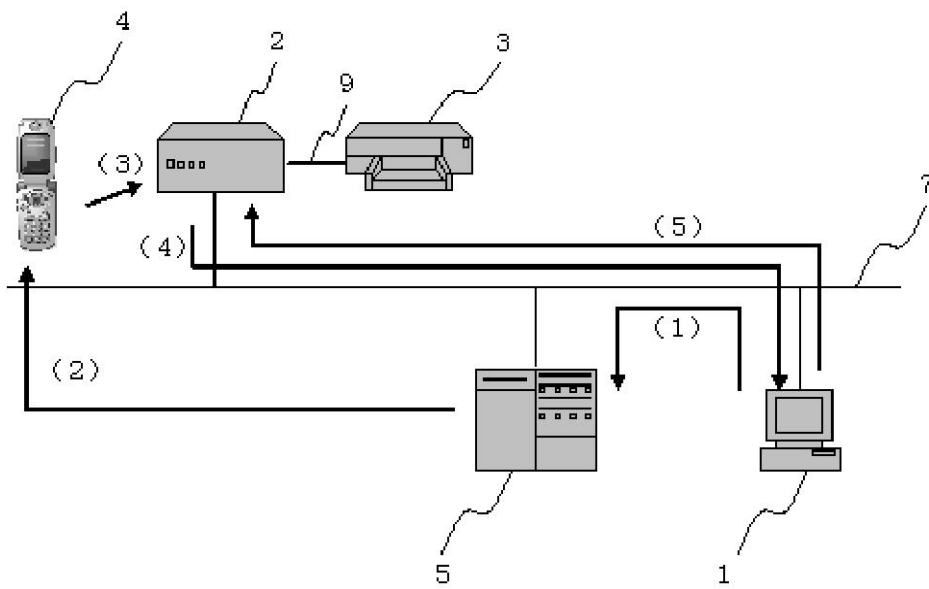
【 図 1 】



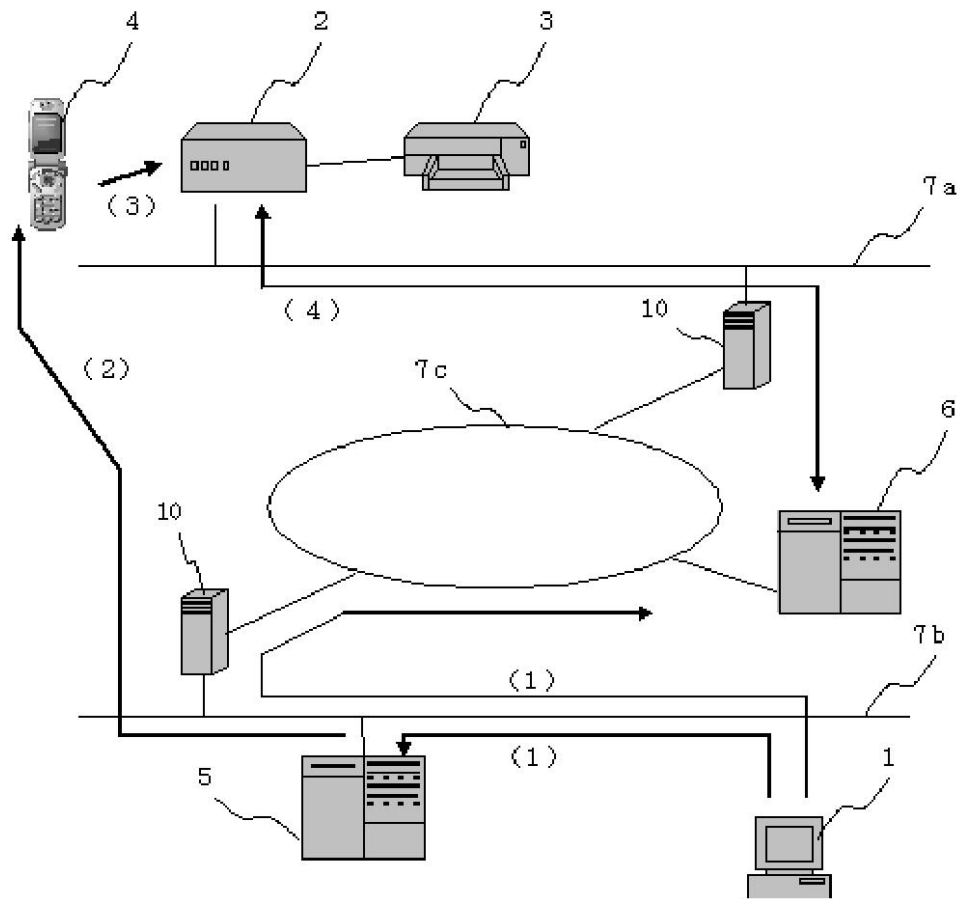
【 図 7 】



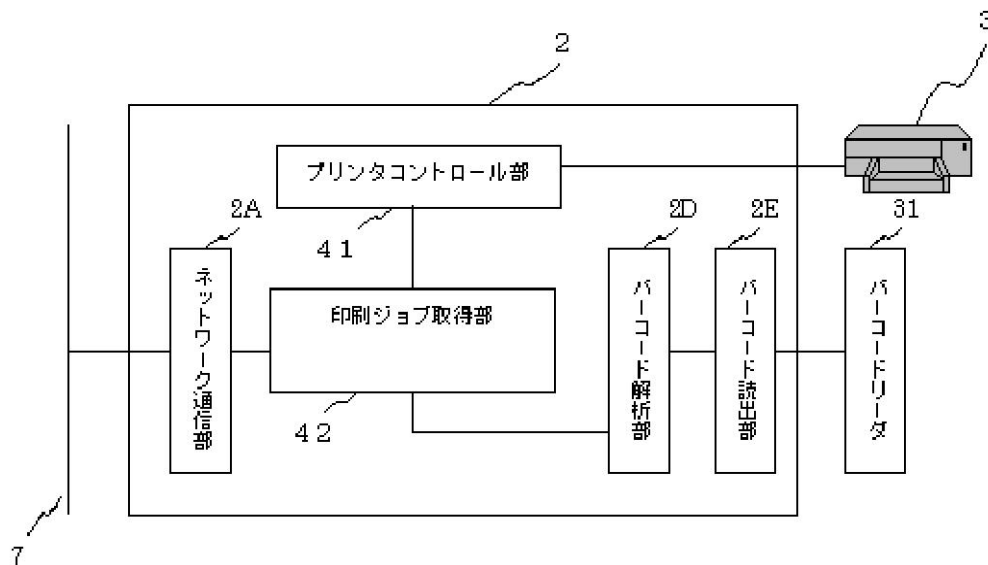
【 図 8 】



【図9】



【図11】



【図14】

