(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4018645号
(P4018645)
(45)発行日　平成19年12月5日(2007.12.5)　(24)登録日　平成19年9月28日(2007.9.28)

(51)Int.Cl.　F I
G06F 3/12 (2006.01)　G06F 3/12 K

請求項の数 10 (全 21 頁)

(21)出願番号　特願2004-22494(P2004-22494)
(22)出願日　平成16年1月30日(2004.1.30)
(65)公開番号　特開2005-216029(P2005-216029A)
(43)公開日　平成17年8月11日(2005.8.11)
審査請求日　平成17年6月13日(2005.6.13)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100071711
弁理士　小林　将高
(72)発明者　土樋　直基
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　中田　剛史

最終頁に続く

(54)【発明の名称】印刷装置、データ処理方法、記憶媒体、プログラム

(57)【特許請求の範囲】
【請求項１】
情報処理装置のプリンタドライバにより生成される印刷ジョブを受信処理可能な印刷装置であって、
受信する印刷ジョブの個々の属性情報を管理する属性データベース手段と、
前記印刷ジョブのＰＤＬデータ部分を一時的に記憶するＰＤＬ記憶手段と、
前記印刷ジョブを受信し、当該印刷ジョブに含まれる属性部分を第１の復号鍵情報に基づいて復号し、当該復号により取り出された属性部分を前記属性データベース手段に登録し、さらに、当該印刷ジョブに含まれる前記ＰＤＬデータ部分を暗号化したまま前記ＰＤＬ記憶手段に記憶する印刷ジョブ解釈手段と、
ユーザ操作によって前記ＰＤＬ記憶手段に記憶された印刷ジョブから選択された印刷ジョブの印刷指示を行う印刷指示手段と、
前記印刷指示手段によって印刷指示された印刷ジョブの暗号化されているＰＤＬデータを第２の復号鍵情報に基づいて復号化するＰＤＬデータ復号化手段と、
を有することを特徴とする印刷装置。
【請求項２】
印刷装置が所有する秘密鍵情報と公開鍵情報とを鍵ペア情報として管理する公開鍵管理手段と、
前記公開鍵管理手段によって管理された鍵ペア情報のうち、前記公開鍵情報を前記情報処理装置に通知する公開鍵通知手段とを有することを特徴とする請求項１記載の印刷装置

。
【請求項３】
前記印刷ジョブ解釈手段は、属性部分の復号化の際に、復号化対象となるデータに対して復号化の後段で、可逆圧縮方式による伸張処理を行うことを特徴とする請求項１又は２に記載の印刷装置。
【請求項４】
前記ＰＤＬデータ復号化手段は、ＰＤＬデータ部分の復号化の際に、復号化対象となるデータに対して復号化の後段で、可逆圧縮方式による伸張処理を行うことを特徴とする請求項１乃至３のいずれか１項に記載の印刷装置。
【請求項５】
受信する印刷ジョブの個々の属性情報を管理する属性データベース手段を備え、情報処理装置のプリンタドライバにより生成される印刷ジョブを受信処理可能な印刷装置におけるデータ処理方法であって、
前記印刷ジョブのＰＤＬデータ部分を一時的にＰＤＬ記憶手段に記憶するＰＤＬ記憶ステップと、
前記印刷ジョブを受信し、当該印刷ジョブに含まれる属性部分を第１の復号鍵情報に基づいて復号し、当該復号により取り出された属性部分を前記属性データベース手段に登録し、さらに、当該印刷ジョブに含まれる前記ＰＤＬデータ部分を暗号化したまま前記ＰＤＬ記憶手段に記憶する印刷ジョブ解釈ステップと、
ユーザ操作によって前記ＰＤＬ記憶手段に記憶された印刷ジョブから選択された印刷ジョブの印刷指示を行う印刷指示ステップと、
前記印刷指示ステップによって印刷指示された印刷ジョブの暗号化されているＰＤＬデータを第２の復号鍵情報に基づいて復号化するＰＤＬデータ復号化ステップと、
を有することを特徴とするデータ処理方法。
【請求項６】
印刷装置が所有する秘密鍵情報と公開鍵情報とを鍵ペア情報として管理する公開鍵管理ステップと、
前記公開鍵管理ステップによって管理された鍵ペア情報のうち、前記公開鍵情報を前記情報処理装置に通知する公開鍵通知ステップとを有することを特徴とする請求項５記載のデータ処理方法。
【請求項７】
前記印刷ジョブ解釈ステップは、属性部分の復号化の際に、復号化対象となるデータに対して復号化の後段で、可逆圧縮方式による伸張処理を行うことを特徴とする請求項５又は６に記載のデータ処理方法。
【請求項８】
前記ＰＤＬデータ復号化ステップは、ＰＤＬデータ部分の復号化の際に、復号化対象となるデータに対して復号化の後段で、可逆圧縮方式による伸張処理を行うことを特徴とする請求項５乃至７のいずれか１項に記載のデータ処理方法。
【請求項９】
請求項５乃至８のいずれか１項に記載のデータ処理方法をコンピュータに実行させるためのプログラムを格納したことを特徴とするコンピュータが読み取り可能な記憶媒体。
【請求項１０】
請求項５乃至８のいずれか１項に記載のデータ処理方法をコンピュータに実行させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置のプリンタドライバにより生成される印刷ジョブを受信処理可能な印刷装置のデータ処理に関するものである。
【背景技術】

【０００２】
従来、この種の印刷システムにおいては、プライバシ情報の印刷結果を他の人に見られないようにするために、印刷ジョブの生成時に特定な指示を行うことによって、ユーザがホストコンピュータから印刷指示を行っても印刷装置では直ちに印刷を行わず、ホールド状態となり、ユーザが印刷装置に赴き印刷装置の操作パネルを操作することによって当該印刷ジョブを認識、選択し、解除するＰＩＮコード(数字によるパスワード)を操作パネルから与えることによってホールド状態が解除されて実際の印刷処理を開始する方式が多数実装されている。
【０００３】
このような印刷方法は一般的に、セキュア印刷、セキュリティ印刷、あるいは機密印刷などと呼ばれる。以下、本提案において、当該印刷方法をセキュア印刷として用語を統一する。また、セキュア印刷される印刷ジョブを特別にセキュアジョブと呼ぶことにする。
【０００４】
セキュア印刷が使われるユースケースとしては、病院の診断情報や給料明細、住民情報など当事者以外に参照されてはいけないプライバシデータの印刷が想定される。
【０００５】
そして、セキュア印刷においては、ホールド(解除待ち)状態になった場合にも、他のジョブの印刷制御を妨げないことが望まれるために、一時的にＨＤＤのような２次記憶装置に格納される。また、セキュア印刷時の印刷ジョブへの特殊な指示とは、セキュア印刷指示属性と解除を行うＰＩＮコード属性である。
【０００６】
さらに、一般的にセキュア印刷の機能と、通常の印刷ジョブを送ったらすぐに印刷を開始する通常ジョブ印刷の機能は並存している。
【０００７】
また、従来のセキュア印刷においては、ホストコンピュータで作成される印刷ジョブは平文（暗号化されない、の意味）で生成され、解除に使用されるＰＩＮコードも同様に平文で印刷ジョブに添付される。
【０００８】
ＬＡＮなどのネットワークを介して印刷ジョブをホストコンピュータから印刷装置に送る場合、専用の機器あるいはソフトウエアによって、経路の盗聴、改ざんは比較的容易であり、ネットワーク上に脅威を与える悪意をもった攻撃者がいると想定した場合には、機密情報を印刷するシステムとしては脆弱であるといえる。あるいはIEEE802.11bに代表される無線ＬＡＮをネットワークインフラとして使用する場合、十分なセキュリティ対策を行わなければ、屋外でも盗聴を行うことが技術的にはより容易である。
【０００９】
さらに、セキュアジョブは印刷装置に蓄えられ、ホールド解除されるまでＨＤＤなどに代表される２次記憶装置に格納されるが、悪意を持った攻撃者が印刷装置に物理的に作用できると想定した場合、印刷装置の電源を切られて、２次記憶装置を抜き取られ持ち出されて内部を解析することにより、技術的に印刷ジョブに含まれる機密情報を取得可能であり、印刷システムとして脆弱であるといえる。
【００１０】
これらの問題に対処するために、印刷ジョブを暗号化し、経路を盗聴したり２次記憶装置を抜き取られて格納された印刷ジョブを解析されたとしても、復号鍵を持っていないために実質的に機密情報が漏洩しないようにする、という対応が考えられる。周辺機器とクライアントＰＣ間でデータを暗号化するシステムとして、特許文献１のシステムが開示されている。
【特許文献１】特開２００３－１６９０５３号公報
【発明の開示】
【発明が解決しようとする課題】
【００１１】

そして、上記セキュアジョブを暗号化する場合に、論点としてどこで復号化するか、という問題と誰の鍵で復号化を行うか、という２つの観点から発生する問題が存在する。

【００１２】

例えば復号に使う鍵を、セキュアジョブを発行したユーザが個別に所有するスマートカードのような物理的な媒体に含まれる電気情報として格納された鍵によって提供される第１の方式を想定する。

【００１３】

その場合、印刷装置に入ったセキュアジョブは暗号化されており、鍵の提供がされない場合はまったく中身を解釈することができない。

【００１４】

一方、解除したいセキュアジョブの解除には、印刷ジョブのオーナ名やジョブ名称といった付加情報によって解除対象となるセキュアジョブを選択させるヒントが必要となる。

【００１５】

しかし、セキュアジョブのすべてのデータが暗号化されているとすると、上記のスマートカードが挿入されて復号処理が行われるまで付加情報の読み出しができず、セキュアジョブを選択することができない、という第１の問題点があった。

【００１６】

あるいは、暗号に使う鍵をユーザが所有するスマートカードのような物理的な鍵ではなく、印刷装置が自身の２次記憶装置、あるいは不揮発性メモリ上に静的に電気情報として保有する鍵、例えば公開鍵方式の鍵ペアを想定し、この方式を第２の方式とする。

【００１７】

この場合、予め鍵ペアの一方である公開鍵はホストコンピュータに提供され、公開鍵を元にセキュアジョブは暗号化され、印刷装置に送られることが考えられる。印刷装置に送られたセキュアジョブは印刷装置内部で直ちに印刷装置に含まれた公開鍵方式の鍵ペアのもう一方の秘密鍵（これは印刷装置によって外部に漏れないように管理される）を元に復号され、復号結果がＨＤＤなどの２次記憶装置に保存される。この場合は、予めホストコンピュータがセキュアジョブの生成を行う際に、付加情報として解除用のＰＩＮコードが属性として割り当てられ、操作パネルを通して入力されたＰＩＮコードが一致した場合に印刷処理を行う、といった動作が想定される。

【００１８】

この方式の場合、セキュアジョブは印刷装置に投入されるとただちに復号化され、２次記憶装置には平文でセキュアジョブのデータが保管されることとなり、攻撃者が印刷装置に物理的に作用できると想定した場合に、印刷装置の電源を切られて、２次記憶装置を抜き取られて内部を解析され、機密情報が暴露されるという脅威に対抗できない、という第２の問題点があった。

【００１９】

本発明は、前記の課題を解決するためになされたもので、本発明の目的は、情報処理装置から受信する印刷ジョブの属性部分を復号鍵で復号し、ＰＤＬデータについては暗号化した状態で印刷ジョブを記憶し、ＰＤＬデータについては印刷指示されるまで暗号化した状態で記憶できる仕組みを提供することである。

【課題を解決するための手段】

【００２１】

本発明に係る印刷装置は、以下の特徴的構成を備える。

情報処理装置のプリンタドライバにより生成される印刷ジョブを受信処理可能な印刷装置であって、受信する印刷ジョブの個々の属性情報を管理する属性データベース手段と、前記印刷ジョブのＰＤＬデータ部分を一時的に記憶するＰＤＬ記憶手段と前記印刷ジョブを受信し、当該印刷ジョブに含まれる属性部分を第１の復号鍵情報に基づいて復号し、当該復号により取り出された属性部分を前記属性データベース手段に登録し、さらに、当該印刷ジョブに含まれる前記ＰＤＬデータ部分を暗号化したまま前記ＰＤＬ記憶手段に記憶する印刷ジョブ解釈手段と、ユーザ操作によって前記ＰＤＬ記憶手段に記憶された印刷ジ

ョブから選択された印刷ジョブの印刷指示を行う印刷指示手段と、前記印刷指示手段によって印刷指示された印刷ジョブの暗号化されているＰＤＬデータを第２の復号鍵情報に基づいて復号化するＰＤＬデータ復号化手段とを有することを特徴とする。

【発明の効果】

【００４４】

本発明によれば、情報処理装置から受信する印刷ジョブの属性部分を復号鍵で復号し、ＰＤＬデータについては暗号化した状態で印刷ジョブを記憶し、ＰＤＬデータについては印刷指示されるまで暗号化した状態で記憶できる。

【発明を実施するための最良の形態】

【００４５】

次に本発明を実施するための最良の形態について図面を参照して説明する。

【００４６】

〔第１実施形態〕

図１は、本発明の第１実施形態を示すデータ処理装置（ホストコンピュータ）および印刷装置を含む印刷システムの構成を示すブロック図である。

【００４７】

図１において、本印刷システムは印刷ジョブを生成し、印刷装置におくるホストコンピュータ１００と、前記印刷ジョブを受信し、電子写真やインクジェットなどの既知の印刷技術により実際の用紙に印刷を行う印刷装置（プリンタ）１５０と、ホストコンピュータ１００と印刷装置１５０を接続するための既知のインタフェース技術を利用したインタフェース手段１７０から構成される。

【００４８】

インタフェース手段１７０はＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）やＩＥＥＥ１２８４準拠のローカルインタフェースやＥｔｈｅｒｎｅｔ（登録商標）やＴｏｋｅｎ－Ｒｉｎｇのような有線ＬＡＮのインタフェース、あるいはＩＥＥＥ８０２．１１ｂ，Ｂｌｕｅｔｏｏｔｈ（登録商標）のような無線ＬＡＮのインタフェースであっても構わず、途中経路にルータやスイッチングハブ、あるいはインターネットを介していてもよい。

【００４９】

ホストコンピュータ１００は、アプリケーション部１０１によってＧＵＩを介してユーザが所望する画像データの生成を行う。ドライバ部１０２は、ホストコンピュータ独自の画像形式から印刷装置１５０で解釈可能な印刷ジョブへの変換作業を行う。

【００５０】

セキュアジョブ生成部１０３は、ドライバ部１０２で生成された印刷ジョブを受け取り、所有者しか解析できないセキュアジョブ（印刷ジョブをセキュリティ対応したもの）への変換作業を行う。この際、前記印刷ジョブを属性部分とＰＤＬデータ部分とに分割して、属性部分を印刷装置が持つ公開鍵を元に暗号化し、ＰＤＬデータ部分はユーザが持つ公開鍵を元に暗号化する。

【００５１】

そして、セキュアジョブ生成部１０３により生成されたセキュアジョブは既存のスプール部１０４に格納され、Ｉ／Ｆ１０５を介して印刷装置１５０に送られる。

【００５２】

なお、上記セキュアジョブ生成時に必要となるユーザが持つ公開鍵は、印刷処理の前段階でスマートカードなどの公開鍵を電気的に保持し、提供するメディアに保持され、既存のカードリーダ部１０８によって読み取られ、ユーザ公開鍵記憶部１０９によって保管され、セキュアジョブ生成部１０３に提供される。

【００５３】

一方、セキュアジョブ生成時に必要となる印刷装置が持つ公開鍵はインタフェース手段１７０を介して印刷装置１５０から供給され、デバイス公開鍵受信部１０６を介してデバイス公開鍵記憶部１０７に保管され、セキュアジョブ生成部１０３に提供される。

【００５４】
セキュアジョブはＩ／Ｆ１５１を介して印刷装置１５０に投入される。パケット判断部１５３は、セキュアジョブの各パケットを監視し、属性部分なら属性復号部１５５へ、ＰＤＬデータ部分ならＰＤＬスプール部１５４へ転送する。
【００５５】
また、セキュアジョブの送信に先立って、ホストコンピュータ１００のデバイス公開鍵受信部１０６は印刷装置１５０に対して印刷装置の公開鍵の要求を行うと、その要求に応じて印刷装置１５０の内部にあるデバイス公開鍵管理部１６１から印刷装置１５０に固有の公開鍵をデバイス公開鍵送信部１６２，インタフェース手段１７０を介してホストコンピュータ１００へ提供を行っている。
【００５６】
属性復号部１５５において、デバイス公開鍵管理部１６１よりセキュアジョブの属性部分が送られると、デバイス公開鍵管理部１６１が保持している公開鍵ペアのもう一方である秘密鍵を使って公開鍵方式によって属性部分を復号化し、属性データを属性ＤＢ１５６に書き込む。
【００５７】
属性ＤＢ１５６は、例えば揮発性メモリであるＲＡＭで構成され、描画処理に関するコピー数や、カラー情報などの印刷情報やジョブ名称やオーナ名などのモニタリング情報を一時的に保持し、描画部１５９に提供する一方、不図示の操作パネルからの表示要求に合わせてＵＩ部１６３へセキュアジョブのモニタリングに必要な属性情報の提供を行う。
【００５８】
さて、セキュアジョブは印刷装置１５０内に入るとホールド（解除待ち）状態となり、データ処理が停止する。ユーザは、カードリーダ部１５８に、ＰＤＬデータ暗号化に使用したものと同じスマートカードなどの公開鍵を提供するメディアが挿入されると、後述の手順によってＰＤＬデータ部分を復号化する復号鍵が提供され、その復号鍵を使って復号化されたＰＤＬデータ部分が描画部１５９に渡され、印刷データの描画処理が行われ、描画されたイメージデータは電子写真やインクジェット技術などの既知の印刷技術を使うプリンタエンジン部１６０において実際の用紙に印刷される。
【００５９】
より詳細に説明するために、セキュアジョブの内部情報について説明する。
【００６０】
１つのセキュアジョブは複数のジョブパケットから構成される。セキュアジョブを構成する一連のジョブパケットの集まりをジョブスクリプトと呼ぶ。
【００６１】
ジョブパケットはＯＳＩ７階層で言うところのアプリケーション層のプロトコルに相当し、ヘッダ部、パラメータ部から構成されるパケット構造になっている。
【００６２】
図２は、図１に示したホストコンピュータ１００から印刷装置１５０に転送されるジョブパケットの構造を示す説明図である。
【００６３】
図２において、縦軸はバイトを示し、横軸は各バイトのビットを示している。図中において０～１バイト目のオペレーションコードは、パケットの機能を示す長さ２バイトのＩＤである。ジョブパケットにおいては以下の値を取ることができる。０ｘ０２０１はジョブ開始命令を示し、０ｘ０２０２はジョブ属性設定命令（属性部分）を示し、０ｘ０２０４はＰＤＬデータ送信命令（ＰＤＬデータ部分）を示し、０ｘ０２０５はジョブ終了命令を示す。
【００６４】
２～３バイト目のブロック番号は、ジョブパケットを送信した側が、返答を要求する場合に、受信側からの返答が送信側のどの返答要求に対するものであるか、その対応を取るために使用する番号である。

【００６５】
例えばそれぞれブロック番号＝１，２，３というジョブパケットを立て続けに送信した時にブロック番号＝２というエラーパケットが帰ってきた場合、返答が帰ってきたとき、送信側は、２番目に送ったジョブパケットにエラーが発生したことを特定することが可能である。
【００６６】
４～５バイト目のパラメータ長はデータ部のバイト長さを示す領域で、０～６４Ｋバイトまでを示すことが可能である。
【００６７】
６～７バイト目はジョブパケットの各種フラグを示す領域でそれぞれ以下の値を示す。
【００６８】
エラーフラグの値が「１」の場合、印刷装置で何らかのエラーが発生したことを示す。このフラグは印刷装置からホストコンピュータに送られる返信パケットに付加される。
【００６９】
また、通知フラグの値が「１」の時は、ホストコンピュータからの要求パケットに対する返答ではなく、印刷装置がなんらかの通知事項があることをホストコンピュータに通知することを示している。
【００７０】
さらに、継続フラグの値が「１」の場合は、データ部にすべてのデータが入らなかったため、次のジョブパケットで残りのデータが送られることを示す。次のジョブパケットは前のパケットと同じオペレーションコード、ブロック番号を設定しなくてはならない。
【００７１】
返答要求は、ホストコンピュータから印刷装置に対して返答パケットが必要な場合に１をセットする。０のときは要求パケットは正常に処理された場合には返答は返さない。印刷装置でエラーが発生した場合には返答要求の０／１に関わらす、つねにエラーフラグを１にした返答パケットを送出する。
【００７２】
８～９バイト目のユーザＩＤおよび１０～１１バイト目のパスワードは、要求パケットでできる操作にセキュリティ的制限を設ける際に認証に使われる領域である。本実施形態には影響しない。
【００７３】
１２バイト目以降はオペレーションコードに対応した追加データが格納される。
【００７４】
なお、ジョブ開始オペレーションの場合、追加データとして、ジョブの実行モードが記述される。指定可能な実行モードを以下にあげる。
【００７５】
０ｘ０１はジョブの通常実行モードで、当該ジョブは通常ジョブとして印刷装置のキューの最後に追加され、スケジューリングが回ってきたら印刷処理を行う。
【００７６】
０ｘ０４はジョブのセキュリティ印刷実行モードで、当該ジョブはセキュアジョブとして扱い、印刷を行わずに鍵が与えられるまでホールド（解除待ち）状態として扱う。
【００７７】
ホストコンピュータ１００内部のドライバ部１０２は暗号化される前の通常と同じ形式のジョブスクリプトを生成する。これはドライバ部１０２とセキュアジョブ生成部１０３の処理を分離することによってドライバ部１０２に負担を与えないようにするためである。
【００７８】
図３は、本発明に係る印刷システムにおける第１のジョブスクリプトが暗号化される仕組みを説明するための模式図である。
【００７９】

図３の（ａ）は、はドライバ部１０２が生成したジョブスクリプトで、上部から下部へ順番にジョブパケットが生成される。中の四角いマス一つがジョブパケットである。図３の（ａ）によれば、ジョブスクリプトは印刷ジョブの開始を告げるジョブ開始命令と、複数個の属性設定命令、複数個のＰＤＬデータ送信命令、ジョブ終了命令によって構成される。セキュアジョブ生成部１０３は図３の（ａ）のジョブスクリプトを解析し、図３の（ｂ）のセキュアジョブを生成する。このとき、ジョブパケットのオペレーションコードを判定し、属性設定命令の場合は印刷装置１５０から提供されたデバイスの公開鍵を用いてジョブパケットのデータ部の暗号化を行い（図３の濃い網掛け部分）、ＰＤＬデータ送信命令の場合は、スマートカードなどの公開鍵を提供するメディアから提供されたユーザの公開鍵を用いて暗号化を行う（図３の薄い網掛け部分）。ここでいう暗号化とは、共通鍵方式と公開鍵方式を組み合わせた方法で行われる。

【００８０】

図４は、図１に示したセキュアジョブ生成部１０３により生成される印刷ジョブを属性設定部分の暗号化属性の構造を示すデータ構造図である。

【００８１】

図４に示すデータ構造は、図２に示したジョブパケットのうち、１２バイト目からのデータ部を示しており、オペレーションコードなどの説明は割愛している。

【００８２】

まず、セキュアジョブ生成部１０３は発生周期が長く、信用できる十分な大きさの乱数を２つ（乱数Ａ，乱数Ｂ）生成する。この乱数はそれぞれ属性部分、およびＰＤＬデータ部分の共通鍵暗号方式による暗号鍵として使用される。さらに、属性部分の暗号鍵となる乱数Ａはプリンタ１５０がデバイス公開鍵記憶部１０７に所有しているプリンタ１５０の公開鍵によって公開鍵暗号方式による暗号化がなされ、図４に示すデバイス公開鍵で暗号化された属性復号鍵４０１として添付される。

【００８３】

さらに、乱数Ａは後に暗号鍵の正当性を確認するためにハッシュ処理されたハッシュ値である属性復号鍵のハッシュ値４０２として添付される。

【００８４】

ハッシュ処理は後に鍵の同一性を比較するために使用されるものであり、ＳＨＡ－１（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ　１）などの公開技術を使用することを想定している。

【００８５】

さらに、ＰＤＬデータ部分の暗号鍵となる乱数Ｂは、ユーザがスマートカードに保持しカードリーダ１０８を介して一時的にユーザ公開鍵記憶部１０９に所有しているユーザの公開鍵によって公開鍵方式による暗号化がなされ、図４に示すデバイス公開鍵で暗号化されたＰＤＬデータ復号鍵４０３として添付される。

【００８６】

さらに乱数Ｂは後に暗号鍵の正当性を確認するためにハッシュ処理されたハッシュ値であるＰＤＬデータ復号鍵のハッシュ値４０４として添付される。

【００８７】

同様にハッシュ処理は後に鍵の同一性を比較するために使用されるものであり、ＳＨＡ－１（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ　１）などの公開技術を使用することを想定している。

【００８８】

ＰＤＬデータ送信命令は、ＰＤＬデータ部分をジョブパケットに分割して送信する命令であり、通常の印刷ジョブの場合はＰＤＬデータ部分は平文で格納されるが、セキュアジョブの場合は、ＰＤＬデータ部分は乱数Ｂによって共通鍵暗号方式による暗号化を行った結果が添付される。これは後にホールド解除されたときにユーザ公開鍵で暗号化されたＰＤＬデータ復号鍵４０３の公開鍵方式を用いた復号化によって乱数Ｂが取り出され、ＰＤＬデータが復号可能となる。

【００８９】
ここでいう共通鍵方式の暗号化とは、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）や３ＤＥＳ（Ｔｒｉｐｌｅ－ＤＥＳ），あるいはＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）暗号化方式に代表される共通鍵暗号方式を用いており、ここで与えられる共通鍵は暗号と復号で共通に使用される鍵であり、秘密に保持されなくてはならない。

【００９０】
ホストコンピュータ１００はセキュアジョブを生成する毎に異なる乱数を生成してこれを共通鍵として利用し、送信した後は破棄されるため、共通鍵はホストコンピュータには保持されない。

【００９１】
共通鍵はセキュアジョブに添付されるが、共通鍵は後述の公開鍵暗号方式によって暗号化されるため、共通鍵のセキュリティ強度は公開鍵暗号方式に拠っている。

【００９２】
さらに、ここでいう公開鍵の暗号化とは、ＲＳＡ（Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ，Ａｄｅｌｍａｎ）暗号化方式に代表される公開鍵方式を用いており、ここで与えられる公開鍵は広く公開できるものである。

【００９３】
公開鍵方式においては対照となる秘密鍵なしに復号化するのは、数学的に素因数分解レベルの難易度があり、十分な鍵長を用いれば高速なコンピュータ環境でも実時間で復号化することが難しいことが証明されている。デバイスの秘密鍵、ユーザの秘密鍵ともセキュアジョブには添付されないために、悪意を持った攻撃者がセキュアジョブの属性、及びＰＤＬデータの中身を解釈するためには、ＲＳＡ公開鍵暗号を解読しなくてはならず、非常に多くのモチベーションが必要となる。

【００９４】
なお、暗号化属性は属性部分の一部であるが、暗号化そのものに関わる属性であるので、属性そのものは平文（暗号化されない、の意味）で添付されるものである。

【００９５】
次にセキュアジョブがプリンタ１５０に投入されたときの処理を説明する。

【００９６】
図５は、本発明に係る印刷装置における第１のデータ処理手順の一例を示すフローチャートであり、図１に示したパケット判断部１５３のデータ処理手順に対応する。なお、（５０１）～（５１２）は各ステップを示す。

【００９７】
パケット判断部１５３は、プリンタ１５０の起動とともに動作を開始し、プリンタ１５０の電源遮断まで処理を継続する。

【００９８】
先ず、ステップ（５０１）において、初期処理としてＳｅｃｕｒｅＦｌａｇをＮｏに初期化する。そして、ステップ（５０２）において、ジョブパケットの受信を行う。ジョブパケットを受信すると、ジョブパケットのオペレーションコードを取得し、オペレーションによって処理を分ける。

【００９９】
次に、ステップ（５０３）において、オペレーションコードがジョブ開始命令かどうか判定し、ジョブ開始命令であると判断した場合は、ステップ（５０４）において、ジョブ開始命令の実行モードを調査し、そのコードによって通常ジョブかセキュアジョブかを判断して、セキュアジョブであると判断された場合は、ステップ（５０５）で、ＳｅｃｕｒｅＦｌａｇをＹｅｓに設定する。

【０１００】
そして、ステップ（５０６）において、属性ＤＢに新規印刷ジョブをエントリして、ステップ（５０２）へ戻る。

【０１０１】
一方、ステップ（５０３）で、オペレーションコードがジョブ開始命令でないと判断された場合、ステップ（５０７）において、オペレーションコードが属性設定命令であるか否かを判断して、属性設定命令であると判断された場合、ステップ（５０８）において属性復号部１５５に処理が渡され、ステップ（５０２）へ戻る。
【０１０２】
一方、ステップ（５０７）で、オペレーションコードが属性設定命令でないと判断した場合は、ステップ（５０９）で、オペレーションコードがＰＤＬデータ送信命令であるか否かを判断して、ＰＤＬデータ送信命令であると判断された場合、ステップ（５１０）において、ＰＤＬスプール部１５４にＰＤＬデータ部分が書き込まれた後、ステップ（５０２）へ戻る。この場合のＰＤＬデータ部分はユーザの秘密鍵によって暗号化された共通鍵すなわち乱数Ｂによって共通暗号化されたＰＤＬデータ部分であり、この段階ではまだ復号化はされていない。
【０１０３】
一方、ステップ（５０９）で、ＰＤＬデータ送信命令でないと判断した場合は、ステップ（５１１）で、オペレーションコードがジョブの終了命令であるか否かを判断して、ジョブの終了命令でないと判断された場合は、そのままステップ（５０２）へ戻り、ジョブの終了命令であると判断された場合、ステップ（５１２）においてＳｅｃｕｒｅＦｌａｇをＮｏにして初期化され、ステップ（５０２）に戻る。
【０１０４】
次に、図１に示した属性復号部１５５のデータ処理について説明する。
【０１０５】
属性復号部１５５はパケット判断部１５３に対する図５に示すステップ（５０８）で呼ばれて、属性の解釈処理を行う。
【０１０６】
図６は、本発明に係る印刷装置における第２のデータ処理手順の一例を示すフローチャートであり、図１に示した属性復号部１５５のデータ処理手順に対応する。なお、（６０１）～（６１０）は各ステップを示す。
【０１０７】
先ず、ステップ（６０９）において、ＳｅｃｕｒｅＦｌａｇがＹｅｓに設定されているか否かをチェックする。なお、ＳｅｃｕｒｅＦｌａｇがＹｅｓに設定されていると判断した場合は、当該ジョブがセキュアジョブであることを示す。
【０１０８】
ここで、セキュアジョブでないと判断した場合は、ステップ（６１０）で属性値を属性ＤＢに記録して処理を終了する。
【０１０９】
一方、ステップ（６０９）で、ＳｅｃｕｒｅＦｌａｇがＹｅｓに設定されていると判断した場合は、ステップ（６０１）で属性ＩＤを調査し、暗号化属性の属性ＩＤと一致するかどうかを判断して、暗号化属性の属性ＩＤであると判断した場合は、当該属性は平文で送信されるため特殊パスに入り、ステップ（６０２）において属性復号鍵をデバイス公開鍵管理部１６１に保存されているデバイス公開鍵で公開鍵暗号方式で復号化する。
【０１１０】
さらに、デバイス公開鍵が一致していないと正しい復号化処理が行えないため、ステップ（６０３）で、そのチェックのためにハッシュ処理を行う。これはホストコンピュータ１００で行われるハッシュ処理と同じアルゴリズムによって行われる。
【０１１１】
次に、ステップ（６０４）において、ハッシュ結果と暗号化属性に添付された属性復号鍵（乱数Ａ）のハッシュ値４０２と一致するかどうかを判断して、ハッシュが一致すると判断した場合には、ステップ（６０５）において、属性復号鍵が属性ＤＢに登録され、本処理を終了する。これにより、属性復号化の鍵として利用可能である。

【０１１２】
一方、ステップ（６０４）で、ハッシュが一致しないと判断した場合には、ステップ（６０６）において、当該セキュアジョブは本機で受信可能ではないとして、キャンセルを行って、本処理を終了する。
【０１１３】
このことからセキュアジョブはターゲットとなる印刷装置が一致しないと印刷できないことになる。
【０１１４】
一方、ステップ（６０１）において、暗号化属性でないと判断した場合には、ステップ（６０７）において、属性データを属性復号鍵で共通鍵方式で復号化する。なお、属性復号鍵はステップ（６０５）で設定されるため、属性の設定順番としては、最初に暗号化属性であることが求められる。復号処理が完了したら、ステップ（６０８）において、共通鍵方式で復号化した属性値を属性ＤＢに記録する。この情報は後にセキュアジョブのモニタリングやトランスレート処理に使用されることになる。
【０１１５】
次に、ホールド解除処理について説明する。
【０１１６】
プリンタ１５０において、セキュアジョブがＰＤＬスプール部１５４に格納された時点で、ユーザからのホールド解除待ちを行う。
【０１１７】
図７は、本発明に係る印刷装置における第３のデータ処理手順の一例を示すフローチャートであり、図１に示したＰＤＬデータ復号部１５７のデータ復号処理手順に対応する。なお、（７０１）～（７０８）は各ステップを示す。
【０１１８】
また、本処理は、ＰＤＬデータ復号部は印刷装置１５０の起動とともに起動し、以降電源遮断まで処理を継続するものとする。
【０１１９】
先ず、ステップ（７０１）において、操作パネル上に表示されるＵＩを介して、ユーザに印刷したいセキュアジョブの選択を行わせる。ここで、いずれかのジョブが選択されると、ステップ（７０２）において、例えばスマートカードをカードリーダ部１５８に挿入することを操作パネル上の表示によりユーザに催促指示する。
【０１２０】
次に、ステップ（７０３）において、上記スマートカードがプリンタ１５０に挿入されたとプリンタＣＰＵにより判断されると、ステップ（７０４）において、スマートカードに復号鍵の公開鍵方式による復号を依頼する。スマートカードから復号鍵、すなわち乱数Ｂの候補を取得すると、ステップ（７０５）においてハッシュ処理を行う。これはホストコンピュータ１００で行われるハッシュ処理と同じアルゴリズムによって行われる。
【０１２１】
次に、ステップ（７０６）において、ハッシュ結果を暗号化属性の中のＰＤＬデータ復号鍵（乱数Ｂ）のハッシュ値４０４と比較し、両値が一致したかどうかを判断して、乱数Ｂの候補と暗号化属性の中のＰＤＬデータ復号鍵に対応する乱数Ｂと一致したと判断した場合は、ステップ（７０７）において、復号鍵（＝乱数Ｂ）を用いてＰＤＬデータ部分の復号処理を行い、結果を描画部１５９に渡して描画、描画結果をプリンタエンジン１６０に渡し、既知の電子写真技術やインクジェット技術によって実際の用紙に印刷を行い、ステップ（７０１）に戻る。
【０１２２】
一方、ステップ（７０６）で、一致しないと判断した場合は、ステップ（７０８）で、復号不可の表示を操作パネル部に行い、ステップ（７０１）に戻る。
【０１２３】
これにより、セキュアジョブはユーザからホールド解除されるまで保管される印刷ジョ

ブである。あるいは一定時間経過後に不図示の従来技術である破棄処理によって破棄が行われる。

【０１２４】

本実施形態によれば、セキュアジョブは暗号化属性以外の属性情報、ＰＤＬデータ部分ともに配送経路では２種類の鍵を使って暗号化されるため、ＰＤＬデータ部分に含まれる機密情報もセキュアジョブに付加された属性も暗号化されるため、通信経路の盗聴に対してセキュアジョブの情報を漏らさず送信可能である。

【０１２５】

また、保管されて状態においては、属性ＤＢに属性情報を保持し、よって属性情報は印刷装置に入ってからは平文で格納され、必要な属性値を公開することによりセキュアジョブのモニタリングや追跡が可能である。一方、ＰＤＬデータ部分は乱数Ｂによって共通鍵方式で暗号化され、共通鍵を復号するための公開鍵方式の秘密鍵はユーザ毎に配布されるスマートカードに保持され、印刷装置には復号を行う手がかりは存在しない。喩え印刷装置から２次記憶装置を抜き出したとしても、属性情報は揮発性のＲＡＭから構成される属性ＤＢに格納されており、２次記憶装置に入っていないので解析および改竄することは非常に困難である。

【０１２６】

さらに、ＰＤＬデータ部分は共通鍵方式で暗号化されており、共通鍵を公開鍵方式によって復号する鍵が印刷装置に保持されていないため、セキュアジョブの解析は非常に困難であり、攻撃者からの高度な攻撃に対してもセキュアジョブ含まれている機密情報の保護が可能である。

【０１２７】

〔第２実施形態〕

上記第１実施形態によれば、ジョブスクリプトのＰＤＬデータ部分と属性部分はそれぞれ暗号化されるが、オペレーションコードを解釈するためにジョブパケットの構造は暗号化処理によって隠蔽化されていない。

【０１２８】

言い換えると、いくつかのジョブパケットがあり、それぞれいくつの属性設定命令やＰＤＬデータ送信命令があるか特定可能な状態でパケットがネットワーク上を転送されることとなる。

【０１２９】

この場合、ある程度ジョブパケットの平文を想定して暗号化した情報を類推することが可能であり、比較的機能強度が弱くなる恐れがある。

【０１３０】

そこで、第２実施形態として平文の属性部分と、暗号化されたＰＤＬデータ部分をまとめて印刷装置の共通暗号方式の鍵によって暗号化する方式について説明する。説明は上述した第１実施形態の構成を踏襲するものとし、差分部分についてのみ詳細を述べる。

【０１３１】

図８は、本発明に係る印刷システムにおける第２のジョブスクリプトが暗号化される仕組みを説明するための模式図であり、図３に示したジョブスクリプトの構造を改良したセキュアプリントのジョブスクリプトの構造に対応する。

【０１３２】

図８の（ａ）はドライバ部１０２が生成した通常の印刷ジョブのジョブスクリプトを示しており、図３の（ａ）と同等である。図８の（ｂ）はセキュアジョブ生成部１０３がＰＤＬデータ部分だけを暗号化し、ユーザの暗号化属性を添付したジョブスクリプトの中間イメージである。

【０１３３】

ここでのＰＤＬデータ部分は、第１実施形態と同等で、乱数Ｂを用いた共通鍵暗号方式による暗号化を行った結果が添付される（網掛け部分）。一方、属性部分は平文のまま添付される。

【０１３４】
図８の（ｃ）はセキュアジョブ生成部１０３が生成するジョブスクリプトであり、網掛けの部分すなわちデバイス暗号データは、図８の（ｂ）のジョブスクリプト全てを乱数Ａで共通鍵暗号化されたものである。ここではジョブパケットのデータ部だけではなく、パケットヘッダも含めてすべてを暗号化される。
【０１３５】
言い換えると、図８の（ｂ）に示すジョブスクリプトを１つのデータストリームと見なし、その全てを暗号化しているということができる。ＰＤＬデータ部分はすでに暗号鍵Ｂによって一度暗号化されており、ここでは２重に暗号化さることになる。また、ジョブスクリプトには、暗号化の方法を識別するために先頭にデバイス暗号命令と、暗号化の情報を示すデバイス鍵暗号化属性設定の２つのジョブパケットが付加されている。この二つは平文で添付される。
【０１３６】
図９は、図８に示したユーザ鍵暗号化属性のうち、ジョブパケットのヘッダ部分を省略したデータ部を記述を説明する図である。
【０１３７】
図９において、９０１は属性の役割を示す属性ＩＤで、指定属性がユーザ鍵暗号化属性であることを示す。９０２はユーザがスマートカードなどの鍵メディアに所有する公開鍵で暗号化されたＰＤＬデータ復号鍵（乱数Ｂ）を示し、これは図４に示したＰＤＬデータ復号鍵４０３に相当する。
【０１３８】
９０３はＰＤＬデータ復号鍵（乱数Ｂ）のハッシュ値を示し、これは図４に示したＰＤＬデータ復号鍵のハッシュ４０４に相当する。ＰＤＬデータ部分は乱数Ｂを用いて共通鍵暗号方式によって暗号化され、ジョブパケットとして添付される（図の網掛け部分）。一方、属性部分はこの段階では平文のままである。
【０１３９】
なお、図８の（ｂ）に示したジョブスクリプトは内部的に一時的に生成されるジョブスクリプトであり、実際に通信経路上には流れることはない。
【０１４０】
図１０は、図８に示したデバイス鍵暗号化属性のうち、ジョブパケットのヘッダ部分を省略したデータ部分を記述を説明する図である。
【０１４１】
図１０において、１００１は属性の役割を示す属性ＩＤで、指定属性がデバイス鍵暗号化属性であることを示す。１００２はデバイス公開鍵で暗号化されたジョブスクリプト復号鍵（乱数Ａ）を示し、これは図４に示すデバイス公開鍵で暗号化された属性復号鍵４０１に相当する。１００３はジョブスクリプト復号鍵（乱数Ａ）のハッシュ値を示し、これは図４に示したＰＤＬデータ復号鍵のハッシュ値４０４に相当する。
【０１４２】
そして、本実施形態では、上記のジョブスクリプトを処理するために、印刷システムの構成を変更する。
【０１４３】
図１１は、本発明の第２実施形態を示すデータ処理装置（ホストコンピュータ）および印刷装置を含む印刷システムの構成を示すブロック図である。
【０１４４】
図１１において、印刷システムは印刷ジョブを生成し、印刷装置におくるホストコンピュータ１１００と、前記印刷ジョブを受信し、電子写真やインクジェットなどの既知の印刷技術により実際の用紙に印刷を行う印刷装置１１５０と、ホストコンピュータ１１００と印刷装置１１５０を接続するための既知のインタフェース技術を利用したインタフェース手段１１７０から構成される。インタフェース手段１１７０はＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）やＩＥＥＥ１２８４準拠のローカルインタフェースやＥｔ

ｈｅｒ－Ｎｅｔ（登録商標）やＴｏｋｅｎ－Ｒｉｎｇのような有線ＬＡＮのインタフェース、あるいはＩＥＥＥ８０２．１１ｂ，Ｂｌｕｅｔｏｏｔｈ（登録商標）のような無線ＬＡＮのインタフェースであっても構わず、途中経路にルータやスイッチングハブ、あるいはインターネットを介していてもよい。

【０１４５】

ホストコンピュータ１１００はアプリケーション部１１０１によってＧＵＩを駆使してユーザが所望する画像データの生成を行う。ドライバ部１１０２は、ホストコンピュータ独自の画像形式から印刷装置１１５０で解釈可能な印刷ジョブへの変換作業を行う。セキュアジョブ生成部１１０３はドライバ部１１０２で生成された印刷ジョブを受け取り、所有者しか解析できないセキュアジョブ（印刷ジョブをセキュリティ対応したもの）への変換作業を行う。この作業は、図８の（ａ）～（ｃ）を生成する作業である。

【０１４６】

そして、生成されたセキュアジョブは既存のスプール部１１０４に格納され、Ｉ／Ｆ１１０５を介して印刷装置１１５０に送られる。セキュアジョブ生成時に必要となるユーザが持つ公開鍵は、印刷処理の前段階でスマートカードなどの公開鍵を電気的に保持し、提供するメディアに保持され、既存のカードリーダ部１１０８によって読み取られ、ユーザ公開鍵記憶部１１０９によって保管され、セキュアジョブ生成部１１０３に提供される。

【０１４７】

一方、セキュアジョブ生成時に必要となる印刷装置が持つ公開鍵はインタフェース手段１１７０を介して印刷装置１１５０から供給され、デバイス公開鍵受信部１１０６を介してデバイス公開鍵記憶部１１０７に保管され、セキュアジョブ生成部１１０３に提供される。セキュアジョブはＩ／Ｆ１１５１を介して印刷装置１１５０に投入される。

【０１４８】

１１５５はジョブスクリプト復号部で、Ｉ／Ｆ１１５１に投入されたセキュアジョブを印刷装置の持つ秘密鍵情報を使って公開鍵方式で復号化する。この段階ではジョブスクリプトは図８の（ｃ）から図８の（ｂ）に変換され後段に渡す。このとき属性部分は平文になる。

【０１４９】

パケット判断部１１５３は受信したジョブスクリプトの個々のジョブパケットを調査し、属性設定命令に関してはデータ部に含まれている属性部分を属性ＤＢ１１５６、ＰＤＬデータ送信命令に関してはＰＤＬスプール部１１５４に送る。この時、ＰＤＬデータ部分は図８の（ｂ）の状態で示してあるように乱数Ｂで暗号化されている状態である。

【０１５０】

また、セキュアジョブの送信に先立って、ホストコンピュータ１１００はデバイス公開鍵受信部１１０６は印刷装置１１５０に対して印刷装置の公開鍵の要求を行うと、その要求に応じて印刷装置１１５０の内部にあるデバイス公開鍵管理部から印刷装置１１５０に固有の公開鍵をデバイス公開鍵送信部１１６２，インタフェース部１７１０を介してホストコンピュータ１１００へ提供を行っている。

【０１５１】

属性ＤＢ１１５６は揮発性メモリであるＲＡＭで構成され、描画処理に関するコピー数や、カラー情報などの情報を一時的に保持し、描画部１１５９に提供する一方、不図示の操作パネルからの表示要求に合わせてＵＩ部１１６３へセキュアジョブの属性情報の提供を行う。

【０１５２】

さて、セキュアジョブは印刷装置１１５０内に入るとホールド（解除待ち）状態となり、処理が停止する。ユーザはカードリーダ部１１５８に、ＰＤＬデータ暗号化に使用したものと同じスマートカードなどの公開鍵を提供するメディア（所定のデバイスとして機能する）が挿入されると、後述の手順によってＰＤＬデータ部分を復号化する復号鍵情報が提供され、その鍵情報を使ってＰＤＬデータ復号部１１５７は暗号化されたＰＤＬデータ部分の公開鍵方式による復号化を行い、ＰＤＬデータ部分が描画部１１５９に渡され、印

刷データの描画処理が行われ、描画されたイメージデータは電子写真やインクジェット技術などの既知の印刷技術を使うプリンタエンジン部１６０において実際の用紙に印刷される。

【０１５３】

これにより、セキュアジョブはユーザからホールド解除されるまで保管される印刷ジョブとなる。なお、保管される印刷ジョブは、一定時間経過後に不図示の従来技術である破棄処理によって破棄処理が行われる。

【０１５４】

上記第２実施形態によれば、セキュアジョブは暗号化属性以外の属性情報、ＰＤＬデータ部分ともに配送経路では２種類の鍵情報を使って暗号化されるため、ＰＤＬデータ部分に含まれる機密情報もセキュアジョブに付加された属性も暗号化されるため、通信経路の盗聴に対してセキュアジョブの情報を漏らさず送信可能である。

【０１５５】

さらに、第１実施形態と比較して、セキュアジョブのジョブスクリプトそのものが完全に暗号化されることによって、通信経路上ではジョブスクリプトの構成さえも判断できないため、さらにセキュリティ強度が向上されている。

【０１５６】

また、保管されて状態においては、属性ＤＢに属性情報を保持し、よって属性情報は印刷装置に入ってからは平文で格納され、必要な属性値を公開することによりセキュアジョブのモニタリングや追跡が可能である。

【０１５７】

一方、ＰＤＬデータ部分は乱数Ｂによって共通鍵方式で暗号化され、共通鍵を復号するための公開鍵方式の秘密鍵はユーザ毎に配布されるスマートカードに保持され、印刷装置には復号を行う手がかりは存在しない。喩え印刷装置から２次記憶装置を抜き出したとしても、属性情報はＲＡＭから構成される属性ＤＢに格納されており、２次記憶装置に入っていないので解析および改ざんすることは非常に困難である。

【０１５８】

さらに、ＰＤＬデータ部分は共通鍵方式で暗号化されており、共通鍵を復号する鍵が印刷装置に保持されていないため、セキュアジョブの解析は非常に困難であり、攻撃者からの高度な攻撃に対してもセキュアジョブに含まれている機密情報の保護が可能である。

【０１５９】

〔第３実施形態〕

上記第１或いは第２実施形態に示した構成において、暗号化の前段にＬＺＷ方式に代表される可逆圧縮方式による圧縮処理と、復号処理の後段による伸張処理を適応することが可能である。

【０１６０】

これにより、圧縮処理によって暗号化対象となるデータサイズが小さくなる可能性が高いため、暗号化処理の負荷を軽くする効果がある。

【０１６１】

また、セキュアジョブのサイズが小さくなるため、比較的遅い通信経路においてはパフォーマンスを向上させることができる。

【０１６２】

さらに、圧縮処理によって暗号化前のデータの冗長性を取り除くことができるため、暗号の解読がより困難になるという効果もある。

【０１６３】

以下、図１２に示すメモリマップを参照して本発明に係る印刷システムで読み取り可能なデータ処理プログラムの構成について説明する。

【０１６４】

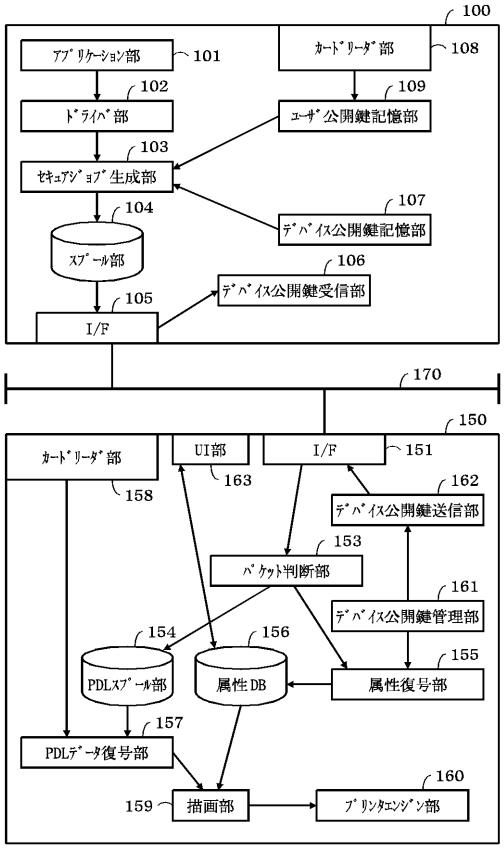
図１２は、本発明に係る印刷システムで読み取り可能な各種データ処理プログラムを格納する記憶媒体のメモリマップを説明する図である。

【０１６５】
なお、特に図示しないが、記憶媒体に記憶されるプログラム群を管理する情報、例えばバージョン情報，作成者等も記憶され、かつ、プログラム読み出し側のＯＳ等に依存する情報、例えばプログラムを識別表示するアイコン等も記憶される場合もある。
【０１６６】
さらに、各種プログラムに従属するデータも上記ディレクトリに管理されている。また、各種プログラムをコンピュータにインストールするためのプログラムや、インストールするプログラムが圧縮されている場合に、解凍するプログラム等も記憶される場合もある。
【０１６７】
本実施形態における図５～図７に示す機能が外部からインストールされるプログラムによって、ホストコンピュータにより遂行されていてもよい。そして、その場合、ＣＤ－ＲＯＭやフラッシュメモリやＦＤ等の記憶媒体により、あるいはネットワークを介して外部の記憶媒体から、プログラムを含む情報群を出力装置に供給される場合でも本発明は適用されるものである。
【０１６８】
以上のように、前述した実施形態の機能を実現するソフトウエアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、本発明の目的が達成されることは言うまでもない。
【０１６９】
この場合、記憶媒体から読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。
【０１７０】
従って、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給するスクリプトデータ等、プログラムの形態を問わない。
【０１７１】
プログラムを供給するための記憶媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＭＯ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＤＶＤなどを用いることができる。
【０１７２】
この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。
【０１７３】
その他、プログラムの供給方法としては、クライアントコンピュータのブラウザを用いてインターネットのホームページに接続し、該ホームページから本発明のコンピュータプログラムそのもの、もしくは、圧縮され自動インストール機能を含むファイルをハードディスク等の記録媒体にダウンロードすることによっても供給できる。また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるＷＷＷサーバやｆｔｐサーバ等も本発明の請求項に含まれるものである。
【０１７４】
また、本発明のプログラムを暗号化してＣＤ－ＲＯＭ等の記憶媒体に格納してユーザに配布し、所定の条件をクリアしたユーザに対し、インターネットを介してホームページから暗号化を解く鍵情報をダウンロードさせ、その鍵情報を使用することにより暗号化され

たプログラムを実行してコンピュータにインストールさせて実現することも可能である。
【０１７５】
また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。
【０１７６】
さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。
【０１７７】
本発明は上記実施形態に限定されるものではなく、本発明の趣旨に基づき種々の変形（各実施形態の有機的な組合せを含む）が可能であり、それらを本発明の範囲から排除するものではない。
【０１７８】
本発明の様々な例と実施形態を示して説明したが、当業者であれば、本発明の趣旨と範囲は、本明細書内の特定の説明に限定されるものではない。
【０１７９】
なお、本発明は、上記した実施形態に限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。
【図面の簡単な説明】
【０１８０】
【図１】本発明の第１実施形態を示すデータ処理装置（ホストコンピュータ）および印刷装置を含む印刷システムの構成を示すブロック図である。
【図２】図１に示したホストコンピュータからプリンタに転送されるジョブパケットの構造を示す説明図である。
【図３】本発明に係る印刷システムにおける第１のジョブスクリプトが暗号化される仕組みを説明するための模式図である。
【図４】図１に示したセキュアジョブ生成部により生成される印刷ジョブの属性部分の暗号化属性の構造を示すデータ構造図である。
【図５】本発明に係る印刷装置における第１のデータ処理手順の一例を示すフローチャートである。
【図６】本発明に係る印刷装置における第２のデータ処理手順の一例を示すフローチャートである。
【図７】本発明に係る印刷装置における第３のデータ処理手順の一例を示すフローチャートである。
【図８】本発明に係る印刷システムにおける第２のジョブスクリプトが暗号化される仕組みを説明するための模式図である。
【図９】図８に示したユーザ鍵暗号化属性のうち、ジョブパケットのヘッダ部分を省略したデータ部の記述を説明する図である。
【図１０】図８に示したデバイス鍵暗号化属性のうち、ジョブパケットのヘッダ部分を省略したデータ部の記述を説明する図である。
【図１１】本発明の第２実施形態を示すデータ処理装置（ホストコンピュータ）および印刷装置を含む印刷システムの構成を示すブロック図である。
【図１２】本発明に係る印刷システムで読み取り可能な各種データ処理プログラムを格納する記憶媒体のメモリマップを説明する図である。
【符号の説明】

【０１８１】
１００　ホストコンピュータ
１０１　アプリケーション部
１０２　ドライバ部
１０３　セキュアジョブ生成部
１０４　スプール部
１０６　デバイス公開鍵受信部
１０７　デバイス公開鍵記憶部
１０８　カードリーダ部
１０９　ユーザ公開鍵記憶部
１５０　プリンタ
１５３　パケット判断部
１５４　ＰＤＬスプール部
１５５　属性復号部
１５６　属性ＤＢ
１５７　ＰＤＬデータ復号部
１６１　デバイス公開鍵管理部
１６２　デバイス公開鍵送信部

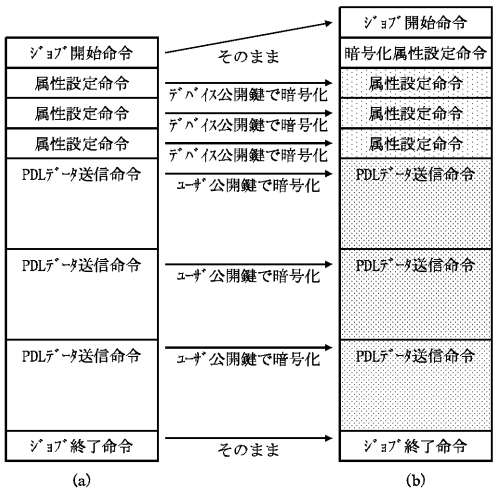
【図１】



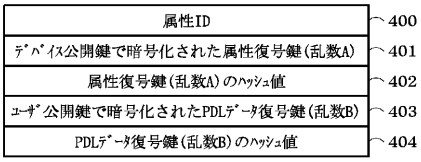
【図２】

byte \ bit	7	6	5	4	3	2	1	0
0	ｵﾍﾟﾚｰｼｮﾝｺｰﾄﾞ							
1								
2	ﾌﾞﾛｯｸ番号							
3								
4	ﾊﾟﾗﾒｰﾀ長							
5								
6	ｴﾗｰﾌﾗｸﾞ	通知ﾌﾗｸﾞ						
7						返答要求	継続ﾌﾗｸﾞ	返答送信
8	ﾕｰｻﾞID							
9								
10	ﾊﾟｽﾜｰﾄﾞ							
11								
12～	ﾃﾞｰﾀ部							

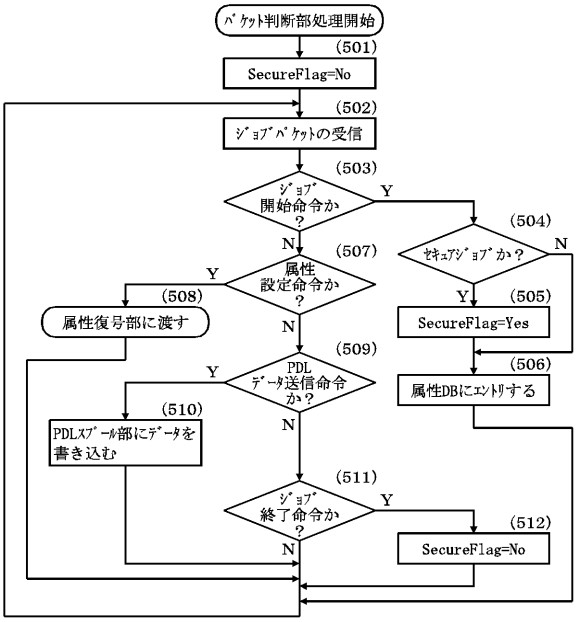
【図３】



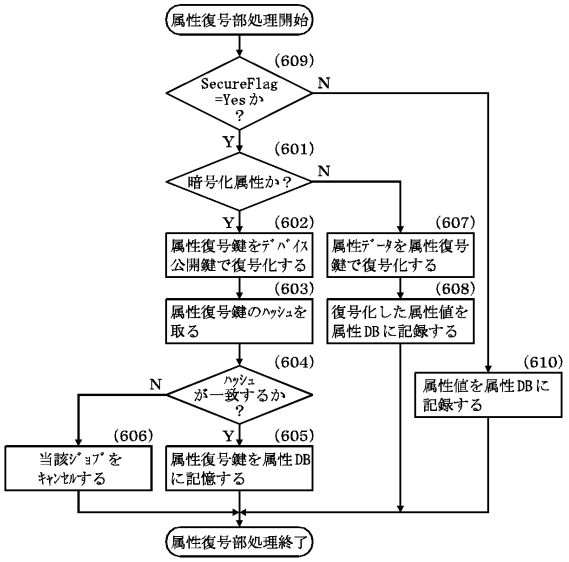
【図４】



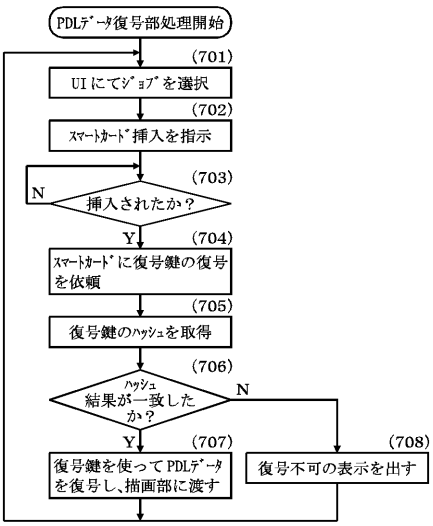
【図５】



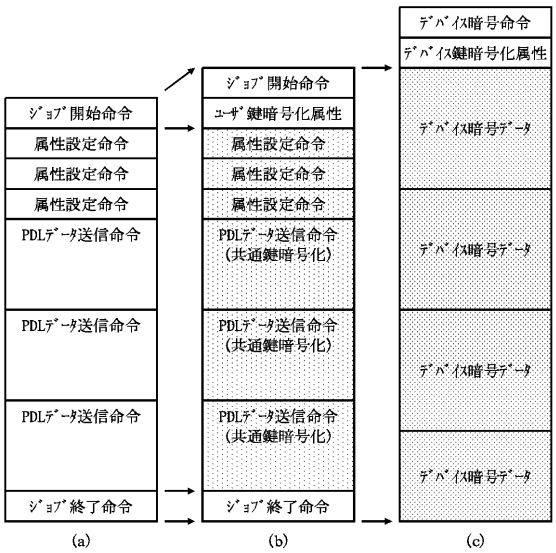
【図６】



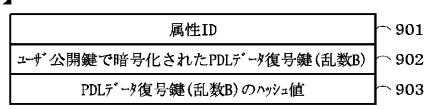
【図７】



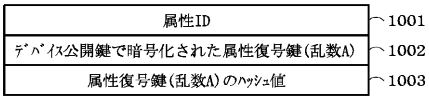
【図８】



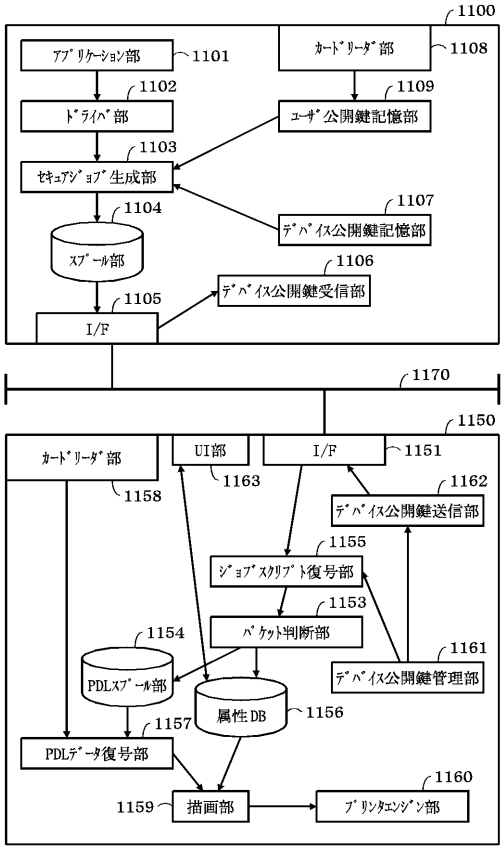
【図９】



【図１０】



【図１１】



【図１２】

FD/CD-ROM等の記憶媒体

ディレクトリ情報
第１のデータ処理プログラム 図５に示すフローチャートのステップに対応する プログラムコード群
第２のデータ処理プログラム 図６に示すフローチャートのステップに対応する プログラムコード群
第３のデータ処理プログラム 図７に示すフローチャートのステップに対応する プログラムコード群

記憶媒体のメモリマップ

フロントページの続き

(56)参考文献 特開２００２－３１８５３５（ＪＰ，Ａ）
特開２００２－０９１７４４（ＪＰ，Ａ）
特開２００１－３０６２７３（ＪＰ，Ａ）
特開平０６－１２４１７８（ＪＰ，Ａ）
特開２００４－０３２３１５（ＪＰ，Ａ）
特開２００３－３０８１９６（ＪＰ，Ａ）
特開２００３－１６９０４６（ＪＰ，Ａ）
特開２００１－１８８６６４（ＪＰ，Ａ）
特開２００１－１８６３５８（ＪＰ，Ａ）
特開２００１－１１７７４４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　３／１２