

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4396377号  
(P4396377)

(45) 発行日 平成22年1月13日(2010. 1. 13)

(24) 登録日 平成21年10月30日(2009. 10. 30)

(51) Int.Cl.

F I

**G 0 6 F 3/12 (2006.01)**

G O 6 F 3/12 K

**B 4 1 J 29/00 (2006.01)**

G O 6 F 3/12 D

**B 4 1 J 29/38 (2006.01)**

B 4 1 J 29/00 Z

B 4 1 J 29/38 Z

請求項の数 20 (全 18 頁)

(21) 出願番号 特願2004-127550 (P2004-127550)  
 (22) 出願日 平成16年4月23日(2004. 4. 23)  
 (65) 公開番号 特開2005-309881 (P2005-309881A)  
 (43) 公開日 平成17年11月4日(2005. 11. 4)  
 審査請求日 平成19年3月22日(2007. 3. 22)

(73) 特許権者 000005496  
 富士ゼロックス株式会社  
 東京都港区赤坂九丁目7番3号  
 (74) 代理人 100075258  
 弁理士 吉田 研二  
 (74) 代理人 100096976  
 弁理士 石田 純  
 (72) 発明者 寺尾 尚恭  
 神奈川県川崎市高津区坂戸3丁目2番1号  
 K S P R & D ビジネスパークビル  
 富士ゼロックス株式会社内

審査官 緑川 隆

最終頁に続く

(54) 【発明の名称】 印刷制御システム、サーバ装置

(57) 【特許請求の範囲】

【請求項 1】

通信ネットワークを介して互いにデータ送受可能に接続された端末、プリンタ及び管理サーバを備える印刷制御システムであって、

前記端末は、

暗号化された文書データ、及び前記文書データを一意に識別するための文書識別データを前記プリンタに送信して印刷要求を出力する手段

を有し、

前記プリンタは、

前記文書識別データ、及び前記プリンタを識別するためのプリンタ識別データを前記管理サーバに送信する手段

を有し、

前記管理サーバは、

前記文書識別データに対応した、前記文書データを印刷可能なプリンタを指定する制御属性を記憶する手段と、

前記プリンタから送信された文書識別データ及び前記プリンタ識別データが、前記制御属性の文書識別データ及び印刷可能プリンタに一致するか否かを判定する手段と、

前記判定する手段で一致すると判定された場合に、前記暗号化された文書データを復号化するための復号鍵データを前記プリンタに送信する手段

を有し、

10

20

前記プリンタは、前記復号鍵データを用いて前記暗号化された文書データを復号化して前記文書データを印刷することを特徴とする印刷制御システム。

【請求項 2】

請求項 1 記載のシステムにおいて、

前記プリンタの前記送信する手段は、さらに、前記端末から前記印刷要求を出力する文書利用者の識別データを前記管理サーバに送信し、

前記管理サーバの前記記憶する手段は、前記制御属性として前記文書識別データに対応した、前記文書データを印刷可能なプリンタ及びユーザを指定する制御属性を記憶し、

前記管理サーバの前記判定する手段は、前記プリンタから送信された文書識別データ及び前記プリンタ識別データ並びに文書利用者識別データが、前記制御属性の文書識別データ及び印刷可能プリンタ並びにユーザ識別データに一致するか否かを判定する

ことを特徴とする印刷制御システム。

【請求項 3】

請求項 1、2 のいずれかに記載のシステムにおいて、さらに、

通信ネットワークを介して前記管理サーバとデータ送受可能に接続された文書作成者端末を備え、

前記文書作成者端末は、

前記管理サーバに文書要録要求を送信する手段と、

前記管理サーバからの前記文書識別データ及び暗号鍵データを受信する手段と、

前記暗号鍵データで前記文書データを暗号化する手段と、

を有し、

前記管理サーバは、

前記文書登録要求に応じて前記文書識別データを作成する手段と、

前記文書識別データ及び前記暗号鍵データを前記文書作成者端末に送信する手段と、

を有することを特徴とする印刷制御システム。

【請求項 4】

請求項 1、2 のいずれかに記載のシステムにおいて、

前記端末は、前記文書データに付随するサムネイルデータを画面上に表示する手段

を有することを特徴とする印刷制御システム。

【請求項 5】

請求項 3 記載のシステムにおいて、

前記文書作成者端末の前記送信する手段は、前記文書データに付随するサムネイルデータ及び暗号化された文書のハッシュ値を前記管理サーバに送信し、

前記文書作成者端末の前記受信する手段は、前記管理サーバからの前記管理サーバの所定の秘密鍵データで署名された前記サムネイルデータ及びハッシュ値を受信し、

前記管理サーバは、前記文書作成者端末から送信された前記サムネイルデータ及びハッシュ値に対して前記所定の秘密鍵データで署名する手段を有し、

前記端末は、署名された前記サムネイルデータ及びハッシュ値を前記秘密鍵データに対応する所定の公開鍵データで検証して画面上に表示する手段を有する

ことを特徴とする印刷制御システム。

【請求項 6】

通信ネットワークを介して互いにデータ送受可能に接続された端末、プリンタ及び管理サーバを備える印刷制御システムであって、

前記端末は、

暗号化された文書データ、及び前記文書データを一意に識別するための文書識別データを前記プリンタに送信して印刷要求を出力する手段

を有し、

前記プリンタは、

前記文書識別データ、及び前記暗号化された文書データ、並びに前記プリンタを識別するためのプリンタ識別データを前記管理サーバに送信する手段

を有し、  
前記管理サーバは、  
前記文書識別データに対応した、前記文書データを印刷可能なプリンタを指定する制御属性を記憶する手段と、  
前記プリンタから送信された文書識別データ及び前記プリンタ識別データが、前記制御属性の文書識別データ及び印刷可能プリンタに一致するか否かを判定する手段と、  
前記判定する手段で一致すると判定された場合に、前記暗号化された文書データを復号化して文書データを前記プリンタに送信する手段  
を有し、  
前記プリンタは、前記管理サーバからの前記文書データを印刷することを特徴とする印刷制御システム。 10

【請求項 7】

請求項 6 記載のシステムにおいて、  
前記プリンタの前記送信する手段は、さらに、前記端末から前記印刷要求を出力する文書利用者の識別データを前記管理サーバに送信し、  
前記管理サーバの前記記憶する手段は、前記制御属性として前記文書識別データに対応した、前記文書データを印刷可能なプリンタ及びユーザを指定する制御属性を記憶し、  
前記管理サーバの前記判定する手段は、前記プリンタから送信された文書識別データ及び前記プリンタ識別データ並びに文書利用者識別データが、前記制御属性の文書識別データ及び印刷可能プリンタ並びにユーザ識別データに一致するか否かを判定する  
ことを特徴とする印刷制御システム。 20

【請求項 8】

請求項 6、7 のいずれかに記載のシステムにおいて、さらに、  
通信ネットワークを介して前記管理サーバとデータ送受可能に接続された文書作成者端末を備え、  
前記文書作成者端末は、  
前記管理サーバに文書データ及び文書要録要求を送信する手段と、  
前記管理サーバからの暗号化された文書データ及び前記文書識別データを受信する手段と、 30

を有し、  
前記管理サーバは、  
前記文書登録要求に応じて前記文書識別データを作成する手段と、  
前記文書登録要求に応じて前記文書データを暗号化する手段と、  
前記文書識別データ及び前記暗号化された文書データを前記文書作成者端末に送信する手段と、  
を有することを特徴とする印刷制御システム。

【請求項 9】

請求項 6、7 のいずれかに記載のシステムにおいて、  
前記端末は、前記文書データに付随するサムネイルデータを画面上に表示する手段  
を有することを特徴とする印刷制御システム。 40

【請求項 10】

請求項 8 記載のシステムにおいて、  
前記管理サーバは、  
前記文書作成者端末から送信された文書データに基づいてサムネイルデータ及びハッシュ値を生成する手段と、  
前記サムネイルデータ及びハッシュ値に所定の秘密鍵データを用いて署名して前記文書作成者端末に送信する手段  
を有し、  
前記端末は、署名された前記サムネイルデータ及びハッシュ値を前記秘密鍵データに対応する所定の公開鍵データで検証して画面上に表示する手段を有する 50

ことを特徴とする印刷制御システム。

【請求項 1 1】

請求項 1 ~ 1 0 のいずれかに記載のシステムにおいて、

前記管理サーバの前記制御属性は、前記プリンタでの印刷態様を指定する条件データを含み、

前記管理サーバは、前記条件データを前記プリンタに送信する手段を有し、

前記プリンタは、前記条件データに従い前記文書データを印刷することを特徴とする印刷制御システム。

【請求項 1 2】

請求項 1 1 記載のシステムにおいて、

前記条件データには、印刷回数制限データが含まれ、

前記管理サーバは、

前記プリンタに前記復号鍵データあるいは前記文書データを送信する場合に印刷されたとして印刷回数を記憶する手段と、

前記印刷回数が前記印刷回数制限を超える場合に前記復号鍵データあるいは前記文書データの送信を禁止する手段と、

を有することを特徴とする印刷制御システム。

【請求項 1 3】

請求項 1 1 記載のシステムにおいて、

前記条件データには、印刷期間制限データが含まれ、

前記管理サーバは、

前記プリンタに前記文書データを送信する日時が前記印刷期間制限を超える場合に前記復号鍵データあるいは前記文書データの送信を禁止する手段と、

を有することを特徴とする印刷制御システム。

【請求項 1 4】

請求項 1 1 記載のシステムにおいて、

前記条件データには、二次配布禁止印刷データが含まれ、

前記プリンタは、前記管理サーバから送信された前記二次配布禁止印刷データに従い所定の二次配布禁止印刷を施すことを特徴とする印刷制御システム。

【請求項 1 5】

請求項 1 1 記載のシステムにおいて、

前記条件データには、オーバーレイ印刷データが含まれ、

前記プリンタは、前記管理サーバから送信された前記オーバーレイ印刷データに従い所定のオーバーレイ印刷を施すことを特徴とする印刷制御システム。

【請求項 1 6】

通信ネットワークを介して互いにデータ送受可能に接続された端末、プリンタ及びサーバ装置を備えるシステムにおける前記サーバ装置であって、

前記プリンタから送信される、文書データを一意に識別するための文書識別データ、前記プリンタを識別するためのプリンタ識別データ、及び前記端末から前記プリンタに対して印刷要求を出力する文書利用者の識別データを受信する手段と、

前記文書識別データに対応した、前記文書データを印刷可能なユーザ及び印刷可能なプリンタを指定する制御属性を記憶する手段と、

前記プリンタから送信された、前記文書識別データ及び前記プリンタ識別データ並びに文書利用者識別データが、前記制御属性の文書識別データ及び印刷可能プリンタ並びに印刷可能ユーザに一致するか否かを判定する手段と、

前記判定する手段で一致すると判定した場合に、暗号化された文書データの復号鍵データを前記プリンタに送信することで前記プリンタでの前記文書データの復号化を可能とする手段と、

を有することを特徴とするサーバ装置。

【請求項 1 7】

請求項 16 記載の装置において、

通信ネットワークを介してデータ送受可能な文書作成者端末から送信された要求に応じて、前記文書識別データ及び暗号鍵データを前記文書作成者端末に送信する手段と、

を有し、前記暗号化された文書データは前記暗号鍵データにより暗号化されたものであり、前記復号鍵データは前記暗号鍵データに対応するものであることを特徴とするサーバ装置。

【請求項 18】

通信ネットワークを介して互いにデータ送受可能に接続された端末、プリンタ及びサーバ装置を備えるシステムにおける前記サーバ装置であって、

前記プリンタから送信される、文書データを一意に識別するための文書識別データ、暗号化された文書データ、前記プリンタを識別するためのプリンタ識別データ、及び前記端末から前記プリンタに対して印刷要求を出力する文書利用者の識別データを受信する手段と、

前記文書識別データに対応した、前記文書データを印刷可能なユーザ及び印刷可能なプリンタを指定する制御属性を記憶する手段と、

前記プリンタから送信された、前記文書識別データ及び前記プリンタ識別データ並びに文書利用者識別データが、前記制御属性の文書識別データ及び印刷可能プリンタ並びに印刷可能ユーザに一致するか否かを判定する手段と、

前記判定する手段で一致すると判定した場合に、前記暗号化された文書データを復号化して前記プリンタに送信することで前記プリンタでの前記文書データの印刷を可能とする手段と、

を有することを特徴とするサーバ装置。

【請求項 19】

請求項 18 記載の装置において、

通信ネットワークを介してデータ送受可能な文書作成者端末から送信された文書データ及び要求に応じて、前記文書データを暗号化するとともに前記文書識別データを作成して前記文書作成者端末に送信する手段と、

を有することを特徴とするサーバ装置。

【請求項 20】

請求項 1 ~ 10 のいずれかに記載のシステムにおいて、さらに、

前記管理サーバにアクセスし前記管理サーバが前記制御属性を記憶した後の任意のタイミングで前記制御属性を変更する手段

を有することを特徴とする印刷制御システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は印刷制御システム及び方法、サーバ装置並びにプリンタに関し、特に配布された文書データ毎の印刷主体や印刷媒体等の制御に関する。

【背景技術】

【0002】

従来より、プリンタで電子的な文書データを印刷する場合において、プリンタに送信される印刷ジョブに制御命令を付加する、あるいは印刷ジョブを発行するスプールに制限を設ける等により印刷制御する技術が知られており、これにより文書作成者以外のユーザに対して文書データの印刷を禁止することが可能である。

【0003】

例えば、下記に示す特許文献 1 には、文書データを作成する際に当該文書データの操作を制限するための制限情報を付加することが記載されている。文書データを受信した端末では、ユーザが文書データに対して操作指示すると、指示された操作が制限情報により制限されたものであるかを判断し、制限された操作である場合には指示された操作を制限する。これにより、電子文書作成者以外のユーザに対し、印刷、複製、編集等の文書操作を

10

20

30

40

50

禁止することができる。

【0004】

また、この特許文献1には、個人データを記憶する手段を有し、操作指示した個人データにとって当該制限情報が有効であるか否かを判断し、有効である場合に操作指示を制限することが記載されている。これにより、例えば企業内イントラネットにおいてレベルの高い部長クラスでは制限情報が無効となって操作指示が許容され、それ以外のクラスでは制限情報が有効となって操作指示が禁止される等の制御も可能となる。

【0005】

【特許文献1】特開2002-229939号公報

【発明の開示】

10

【発明が解決しようとする課題】

【0006】

しかしながら、最近、文書データは一層多様化しており、従来以上に細かい印刷制御が要求される場合が多くなっている。

【0007】

例えば、文書作成者が特定のユーザに文書データを配布した場合に、その文書データの性質上、その文書データが印刷されるべきプリンタを特定したい、すなわちそのユーザが任意のプリンタで印刷することを禁止したいと欲する場合があるが、上記従来技術では文書作成者が印刷プリンタを特定することができない。

20

【0008】

また、文書作成者が特定のユーザに文書データを配布した場合に、その文書データの性質上、その文書データが印刷される期間あるいは回数を限定したい、すなわちそのユーザが印刷できる期間あるいは回数を制限したいと欲する場合もあるが、上記従来技術では文書作成者が印刷期間や印刷回数を制限することはできない。

【0009】

さらに、文書作成者が一旦、ある制限を付加したとしても、その後に制限を変更したいと欲する場合も少なくないが、上記従来技術では制限情報の変更が困難であり、フレキシビリティに欠ける問題もある。

【0010】

本発明の目的は、文書データ毎に印刷制御を行うこと、例えば印刷されるべきプリンタを特定することができるシステム及び方法並びに装置を提供することにある。

30

【0011】

また、本発明の目的は、文書データ毎に、かつ、ユーザー一人一人に対して、印刷されるべきプリンタや印刷期間、印刷回数等の印刷条件を設定することができるシステム及び方法並びに装置を提供することにある。

【0012】

さらに、本発明の目的は、文書データ毎に、ユーザー一人一人に対して設定した印刷条件を容易に、そして任意のタイミングで変更することができるシステム及び方法並びに装置を提供することにある。

【課題を解決するための手段】

40

【0013】

本発明は、通信ネットワークを介して互いにデータ送受可能に接続された端末、プリンタ及び管理サーバを備える印刷制御システムであって、前記端末は、暗号化された文書データ、及び前記文書データを一意に識別するための文書識別データを前記プリンタに送信して印刷要求を出力する手段を有し、前記プリンタは、前記文書識別データ、及び前記プリンタを識別するためのプリンタ識別データを前記管理サーバに送信する手段を有し、前記管理サーバは、前記文書識別データに対応した、前記文書データを印刷可能なプリンタを指定する制御属性を記憶する手段と、前記プリンタから送信された文書識別データ及び前記プリンタ識別データが、前記制御属性の文書識別データ及び印刷可能プリンタに一致するか否かを判定する手段と、前記判定する手段で一致すると判定された場合に、前記暗

50

号化された文書データを復号化するための復号鍵データを前記プリンタに送信する手段を有し、前記プリンタは、前記復号鍵データを用いて前記暗号化された文書データを復号化して前記文書データを印刷する。ここで、制御属性は、プリンタでの印刷態様を指定する条件データを含み、管理サーバは前記条件データをプリンタに送信し、プリンタは前記条件データに従い文書データを印刷することができる。ここで言う印刷態様とは、n - u p 指定、両面指定、カラー/白黒指定、出力部数指定、出力可能な部数指定などの印刷に関する設定や、ステーブル指定、パンチ指定などの出力物に対する後処理設定が含まれる。出力部数指定とは「文書データを出力する部数」の指定であり、例えば出力指定部数が「5」なら5部出力される。出力可能な部数指定とは「そのプリンタでその文書データを出力可能な部数」の指定であり、例えば出力可能な部数指定が「3」ならプリンタ側で5部出力を設定しても3部に出力を制限する。制御属性には、印刷主体であるユーザや印刷媒体であるプリンタの種類も含まれる。

#### 【0014】

また、本発明は、通信ネットワークを介して互いにデータ送受可能に接続された端末、プリンタ及び管理サーバを備える印刷制御システムであって、前記端末は、暗号化された文書データ、及び前記文書データを一意に識別するための文書識別データを前記プリンタに送信して印刷要求を出力する手段を有し、前記プリンタは、前記文書識別データ、及び前記暗号化された文書データ、並びに前記プリンタを識別するためのプリンタ識別データを前記管理サーバに送信する手段を有し、前記管理サーバは、前記文書識別データに対応した、前記文書データを印刷可能なプリンタを指定する制御属性を記憶する手段と、前記プリンタから送信された文書識別データ及び前記プリンタ識別データが、前記制御属性の文書識別データ及び印刷可能プリンタに一致するか否かを判定する手段と、前記判定する手段で一致すると判定された場合に、前記暗号化された文書データを復号化して文書データを前記プリンタに送信する手段を有し、前記プリンタは、前記管理サーバからの前記文書データを印刷する。

#### 【0015】

また、本発明は、通信ネットワークを介して互いにデータ送受可能に接続された端末、プリンタ及び管理サーバを備えるシステムにおいて文書データの印刷を制御する方法であって、前記端末から暗号化された文書データ、及び前記文書データを一意に識別するための文書識別データを前記プリンタに送信して印刷要求を出力し、前記プリンタから前記文書識別データ、前記プリンタを識別するためのプリンタ識別データ、及び前記端末から前記印刷要求を出力する文書利用者の識別データを前記管理サーバに送信し、前記管理サーバは、前記文書識別データに対応した、前記文書データを印刷可能なユーザ及び印刷可能なプリンタを指定する制御属性を記憶する記憶装置にアクセスすることにより、前記プリンタから送信された文書識別データ及び前記プリンタ識別データ並びに文書利用者識別データが、前記制御属性の文書識別データ及び印刷可能プリンタ並びに印刷可能ユーザに一致するか否かを判定し、一致すると判定した場合に前記暗号化された文書データを復号化するための復号鍵データを前記プリンタに送信し、前記プリンタは、前記復号鍵データを用いて前記暗号化された文書データを復号化して前記文書データを印刷する。

#### 【0016】

また、本発明は、通信ネットワークを介して互いにデータ送受可能に接続された端末、プリンタ及び管理サーバを備えるシステムにおいて文書データの印刷を制御する方法であって、前記端末から暗号化された文書データ、及び前記文書データを一意に識別するための文書識別データを前記プリンタに送信して印刷要求を出力し、前記プリンタから前記文書識別データ、前記暗号化された文書データ、前記プリンタを識別するためのプリンタ識別データ、及び前記端末から前記印刷要求を出力する文書利用者の識別データを前記管理サーバに送信し、前記管理サーバは、前記文書識別データに対応した、前記文書データを印刷可能なユーザ及び印刷可能なプリンタを指定する制御属性を記憶する記憶装置にアクセスすることにより、前記プリンタから送信された文書識別データ及び前記プリンタ識別データ並びに文書利用者識別データが、前記制御属性の文書識別データ及び印刷可能プリ

ンタ並びに印刷可能ユーザに一致するか否かを判定し、一致すると判定した場合に前記暗号化された文書データを復号化して元の文書データを前記プリンタに送信し、前記プリンタは、前記文書データを印刷する。

【 0 0 1 7 】

また、本発明は、通信ネットワークを介して互いにデータ送受可能に接続された端末、プリンタ及びサーバ装置を備えるシステムにおける前記サーバ装置であって、前記プリンタから送信される、文書データを一意に識別するための文書識別データ、前記プリンタを識別するためのプリンタ識別データ、及び前記端末から前記プリンタに対して印刷要求を出力する文書利用者の識別データを受信する手段と、前記文書識別データに対応した、前記文書データを印刷可能なユーザ及び印刷可能なプリンタを指定する制御属性を記憶する手段と、前記プリンタから送信された、前記文書識別データ及び前記プリンタ識別データ並びに文書利用者識別データが、前記制御属性の文書識別データ及び印刷可能プリンタ並びに印刷可能ユーザに一致するか否かを判定する手段と、前記判定する手段で一致すると判定した場合に、暗号化された文書データの復号鍵データを前記プリンタに送信することで前記プリンタでの前記文書データの復号化を可能とする手段とを有する。

10

【 0 0 1 8 】

また、本発明は、通信ネットワークを介して互いにデータ送受可能に接続された端末、プリンタ及びサーバ装置を備えるシステムにおける前記サーバ装置であって、前記プリンタから送信される、文書データを一意に識別するための文書識別データ、暗号化された文書データ、前記プリンタを識別するためのプリンタ識別データ、及び前記端末から前記プリンタに対して印刷要求を出力する文書利用者の識別データを受信する手段と、前記文書識別データに対応した、前記文書データを印刷可能なユーザ及び印刷可能なプリンタを指定する制御属性を記憶する手段と、前記プリンタから送信された、前記文書識別データ及び前記プリンタ識別データ並びに文書利用者識別データが、前記制御属性の文書識別データ及び印刷可能プリンタ並びに印刷可能ユーザに一致するか否かを判定する手段と、前記判定する手段で一致すると判定した場合に、前記暗号化された文書データを復号化して前記プリンタに送信することで前記プリンタでの前記文書データの印刷を可能とする手段とを有する。

20

【 発明の効果 】

【 0 0 2 1 】

本発明によれば、ある文書データ毎に印刷制御を実行でき、例えば特定のプリンタでの印刷制御等を行うことができる。また、ある文書データに対して、特定のユーザによる特定のプリンタでの印刷制御を行うことができる。さらに、文書が配布された後であっても任意のタイミングで印刷制御を変更できる。

30

【 発明を実施するための最良の形態 】

【 0 0 2 2 】

以下、図面に基づき本発明の実施形態について説明する。

【 0 0 2 3 】

< 第 1 実施形態 >

図 1 には、本実施形態に係る印刷制御システムのシステム構成図が示されている。本システムは、端末 1、端末 2、文書管理サーバ 12、ユーザデータベース ( D / B ) 13 及びプリンタ 24 を含んで構成される。

40

【 0 0 2 4 】

端末 1 は、文書データを作成する文書作成者が操作する端末であり、文書管理サーバ 12 と有線あるいは無線の通信ネットワーク 50 によりデータ送受可能に接続されている。端末 2 は、文書データを受け取った ( 文書データの配布を受けた ) ユーザが操作する端末であり、プリンタ 24 と有線あるいは無線の通信ネットワーク 52 によりデータ送受可能に接続されている。端末 1 と端末 2 は非接続でもよく、図示のように通信ネットワーク 54 により接続されていてもよい。前者の場合にはユーザは例えばフレキシブルディスクや C D、D V D、フラッシュメモリ等の可搬記録媒体を介して文書作成者から文書データの

50



配布を受けることができ、後者の場合には端末 1 から所定のメールサーバを介して送信された電子メールの添付ファイル等として文書データの配布を受けることができる。ユーザが受け取る文書データは、そのまま印刷できるデータではなく、管理サーバ 1 2 が管理する秘密鍵で暗号化された文書データである。文書データを暗号化することで、任意のプリンタでの印刷が防止される。ユーザは、端末 2 からプリンタ 2 4 に対して暗号化された文書データを送信し印刷命令（印刷ジョブ）を出力する。

#### 【 0 0 2 5 】

文書管理サーバ 1 2 は、文書作成者が作成した文書データの印刷ジョブを管理するサーバであり、端末 2 から印刷命令を受け付けたプリンタ 2 4 からの要求に応じ、当該プリンタ 2 4 の認証を行う。文書管理サーバ 1 2 におけるプリンタ 2 4 の認証とは、そのユーザに対してその文書データが印刷されるべきプリンタとして予め文書作成者により設定されたプリンタに一致することを意味する。文書管理サーバ 1 2 は、プリンタ 2 4 とともに文書利用者の認証を行ってもよい。認証できた場合、プリンタ 2 4 に対してプリンタ 2 4 が暗号化された文書データを印刷するために必要なデータを返信する。暗号化された文書データを印刷するために必要なデータとは、暗号化された文書データを復号化するための復号鍵データであり、あるいは復号済みのオリジナル文書データである。

#### 【 0 0 2 6 】

プリンタ 2 4 は、端末 2 からの文書データを印刷するプリンタであり、文書管理サーバ 1 2 と通信ネットワーク 5 6 で接続される。プリンタ 2 4 は、端末 2 から印刷命令を受け付けた場合、文書管理サーバ 1 2 に対して認証を要求する。文書管理サーバ 1 2 が認証に成功すると、文書管理サーバ 1 2 から返信されるデータを用いてオリジナル文書データの印刷を実行する。

#### 【 0 0 2 7 】

このように、本実施形態のシステムでは、文書管理サーバ 1 2 においてプリンタ 2 4 の認証を実行し、認証の結果、文書作成者が指定したプリンタではないと判定された場合には、文書データは暗号化されたまま維持されるため印刷されることがなく、認証された特定のプリンタ 2 4 のみで印刷されることになる。また、プリンタ 2 4 の認証時において、ユーザの認証も同時に実行することで、特定のユーザによる特定のプリンタ 2 4 での印刷を許容することができる。さらに、印刷条件を文書管理サーバ 1 2 からプリンタ 2 4 に供給することで、文書作成者は文書管理サーバ 1 2 に記憶されている印刷条件を任意のタイミングで変更することができる。通信ネットワーク 5 0 ~ 5 6 は LAN でもよく、あるいは WAN でもよい。印刷条件を任意のタイミングで変更できるだけでなく、印刷可能となるユーザや印刷可能なプリンタも任意のタイミングで変更可能である。

#### 【 0 0 2 8 】

以下、本実施形態の印刷制御システムをより詳細に説明する。

#### 【 0 0 2 9 】

図 2 には、本実施形態の印刷制御システムにおける処理の流れが模式的に示されている。文書作成者 1 0 0 は、端末 1 を用いて文書データを作成する。この文書データはオリジナル文書 1 0 であり、文書作成者 1 0 0 が文書利用者（ユーザ）2 0 0 に配布する文書である。文書作成者 1 0 0 は、文書利用者 2 0 0 に文書データを配布するに際し、まず、文書管理サーバ 1 2 に対して文書登録の要求を行う。具体的には、端末 1 から文書管理サーバ 1 2 に対して通信ネットワーク 5 0 を介して、文書作成者 1 0 0 は文書管理サーバ 1 2 の認証を受ける。文書管理サーバ 1 2 の認可後、文書作成者 1 0 0 は、文書制御属性（印刷制御情報）とともに文書登録要求コマンドを出力する。本実施形態における文書制御属性は、印刷の条件を設定するものであり、カラー印刷を許容する、あるいは白黒のみを許容する等の他、オリジナル文書 1 0 を印刷できるユーザ及び印刷できるプリンタを制限するデータも含む。文書制御属性は、文書管理サーバ 1 2 の記憶装置に記憶される。

#### 【 0 0 3 0 】

文書管理サーバ 1 2 は、認証手段、文書識別子生成手段、暗号/復号鍵記憶手段、文書制御属性記憶手段及び文書利用ログ（文書利用履歴記憶手段）を有する。文書管理サーバ

10

20

30

40

50

12は、文書登録要求コマンドを受け付けると、文書作成者100の認証を行う。すなわち、ユーザD/B13に予め記憶された、本システムの利用者データと文書作成者100とを照合し、文書作成者100が本システムの利用者の一人であることを確認する。

#### 【0031】

文書登録要求完了後、文書管理サーバ12は、文書を一意（ユニーク）に識別するための文書識別子14を作成し、文書暗号化用の暗号鍵16とともに端末1に返信する。文書識別子は一意であるかぎり文書作成者が文書識別子を作成（例えば文書のハッシュ値）してもよい。暗号鍵16は文書識別子毎に復号鍵16'とともに作成される。共通鍵暗号を使用する場合は暗号鍵16と復号鍵16'は同一のものとなる。文書識別子14及び暗号鍵16の返信をもって、文書管理サーバ12は文書作成者100に対して文書登録完了の通知とする。また、文書管理サーバ12は、文書が登録されたことを文書利用ログ20に登録する。文書利用ログ20への登録は、具体的には文書識別子14及び文書制御属性18、暗号鍵16および復号鍵16'を1つのセットとして登録する。したがって、文書識別子14が与えられた場合、このログにアクセスすることで当該文書識別子14に対応する文書制御属性18が特定され、文書の印刷条件が決定されることになる。文書登録日付をログ20に登録してもよい。

10

#### 【0032】

文書管理サーバ12から文書識別子14及び暗号鍵16を受け取った文書作成者100は、端末1を用いてオリジナル文書10を暗号鍵16で暗号化して暗号化文書22を作成する。文書識別子14は、暗号化された文書データのヘッダ等に付加される。暗号化が完了した時点で、文書作成者100は暗号鍵16を廃棄する。オリジナル文書10を暗号化することで、以後、オリジナル文書10は文書管理サーバ12から復号鍵16'を取得しない限り復号できず、印刷できないことになる。

20

#### 【0033】

文書作成者100は、暗号化文書22を任意の方法で文書利用者200に配布する。一つの方法は、上述したように端末1から文書利用者200が使用する端末2に対して通信ネットワーク54を介して送信する方法である。暗号化文書22を受け取った文書利用者200は、暗号化文書22を印刷すべく、端末2を用いてプリンタ24に対して印刷コマンドとともに暗号化文書22を送信する。この際、文書利用者200はプリンタ24により認証を受ける。

30

#### 【0034】

暗号化文書22を受け取ったプリンタ24は、文書利用者200の認証を行う。すなわち、文書利用者200は正規のユーザであるか否かを確認する。認証完了後、プリンタ24は、暗号化文書22から文書識別子14を抽出し、ユーザ認証情報26とともに文書管理サーバ12に送信して文書制御属性を要求する。この際、プリンタ24は文書管理サーバ12により認証を受ける。

#### 【0035】

文書制御属性要求を受け取った文書管理サーバ12は、文書識別子14で特定される文書制御属性をログ20から読み出す。なお、文書識別子14が暗号化されている場合には、復号鍵16'で復号して対応する文書制御属性を読み出す。そして、文書を印刷しようとするプリンタ24及び文書利用者200が、当該文書識別子14で特定される文書制御属性で指定された印刷可能プリンタ及び印刷可能ユーザに一致するか否かを確認する。プリンタ24及び文書利用者200が、文書制御属性で指定された印刷可能プリンタ及び印刷可能ユーザに一致する場合、文書管理サーバ12は復号鍵16'及び文書制御属性18を文書属性完了としてプリンタ24に返信する。復号鍵16'をプリンタ24に返信することで、プリンタ24では暗号化文書22の復号化が可能となり、すなわちオリジナル文書10の印刷が可能になる。なお、文書管理サーバ12は、復号鍵16'をプリンタ24に返信した場合、オリジナル文書10が印刷されたものとしてログ20にその旨（印刷完了及び印刷日時）を登録する。

40

#### 【0036】

50

文書管理サーバ 12 から復号鍵 16' 及び文書制御属性 18 を受け取ったプリンタ 24 は、復号鍵 16' を用いて暗号化文書 22 を復号してオリジナル文書 10 を取得し、文書制御属性に従ってオリジナル文書 10 を印刷して印刷文書 30 を出力する。以上により、特定の文書利用者 200 による特定のプリンタ 24 での印刷が実行される。

【0037】

文書識別子 14、暗号鍵 16、及び暗号化文書 22 の流れをまとめると以下のようになる。

【0038】

<文書識別子 14>

- (1) 文書作成者 100 (端末 1) からの要求に応じ、管理サーバ 12 にて文書識別子 14 が作成される。 10
- (2) 作成された文書識別子 14 は文書作成者 100 (端末 1) に返信される。
- (3) 暗号化文書 22 とともに文書利用者 200 (端末 2) に配布される。
- (4) 文書利用者 200 (端末 2) からプリンタ 24 に送信される。
- (5) プリンタ 24 にて文書識別子 14 が抽出され、管理サーバ 12 に送信される。
- (6) 管理サーバにて文書識別子 14 に基づき、文書制御属性が読み出される。文書識別子 14 が暗号化されている場合には、管理サーバ 12 の暗号鍵 16 で復号される。

【0039】

<暗号鍵 16>

- (1) 文書作成者 100 (端末 1) からの要求に応じ、予め管理サーバ 12 に記憶され、あるいは文書毎に作成された暗号鍵 16 は文書作成者 100 (端末 1) に返信される。 20
- (2) 文書作成者 100 (端末 1) により、暗号鍵 16 を用いてオリジナル文書 10 が暗号化される。
- (3) プリンタ 24 からの要求に応じ、管理サーバ 12 で認証が成功した場合に暗号鍵 16 に対応する復号鍵 16' がプリンタ 24 に返信される。

【0040】

<暗号化文書 22>

- (1) 文書作成者 100 (端末 1) により暗号鍵 16 を用いてオリジナル文書 10 が暗号化され、暗号化文書 22 が作成される。
- (2) 暗号化文書 22 は文書作成者 100 (端末 1) から文書利用者 200 (端末 2) に配布される。 30
- (3) 文書利用者 200 (端末 2) からプリンタ 24 に送信される。
- (4) プリンタ 24 で暗号化文書 22 は復号され、オリジナル文書 10 が印刷される。

【0041】

このように、オリジナル文書 10 は特定のプリンタ 24 でのみ印刷されるが、文書制御属性 18 によりオリジナル文書 10 の印刷の態様を種々制御することができる。以下、文書制御属性 18 について説明する。

【0042】

文書制御属性 18 が、例えば「印刷可能ユーザ = 文書利用者 200、印刷可能プリンタ = プリンタ 24、印刷条件 = カラー」である場合、プリンタ 24 では印刷条件 = カラーに従い、オリジナル文書 10 をカラー印刷し、印刷文書 30 として出力する。 40

【0043】

また、文書制御属性 18 が、「印刷可能ユーザ = 文書利用者 200、印刷可能プリンタ = プリンタ 24、印刷条件 = 白黒」である場合、白黒のオリジナル文書 10 が印刷文書 30 として出力される。

【0044】

また、文書制御属性 18 が、「印刷可能ユーザ = 文書利用者 200、印刷可能プリンタ = プリンタ 24、印刷条件 = 最大印刷回数 1 回」である場合、文書管理サーバ 12 はユーザ及びプリンタを認証した後、ログ 20 にアクセスして当該文書識別子 14 で特定される文書の印刷回数を確認し、未だ印刷されていない場合には印刷可能と判定して暗号鍵 16 50

を返信する。プリンタ 24 は復号鍵 16' を用いてオリジナル文書 10 を復号し印刷文書 30 を出力する。ログ 20 にアクセスした結果、既に過去に印刷されている場合には印刷不能と判定して復号鍵 16' をプリンタ 24 に返信しない。この場合、プリンタ 24 は暗号化文書 22 を復号できないため印刷できず、印刷回数を 1 回に制限した印刷条件が満たされることになる。

【0045】

また、文書制御属性 18 が、「印刷可能ユーザ = 文書利用者 200、印刷可能プリンタ = プリンタ 24、印刷条件 = 印刷期間登録後 3 ヶ月」である場合、文書管理サーバ 12 はユーザ及びプリンタを認証した後、現在の日時が登録後 3 ヶ月以内か否かを確認する。そして、3 ヶ月以内である場合には印刷可能と判定して復号鍵 16' を返信する。プリンタ 24 は復号鍵 16' を用いてオリジナル文書 10 を復号し印刷文書 30 を出力する。現在の日時が 3 ヶ月を超える場合には印刷不能と判定して復号鍵 16' をプリンタ 24 に返信しない。この場合、プリンタ 24 は暗号化文書 22 を復号できないため印刷できず、印刷期間を制限した印刷条件が満たされることになる。

10

【0046】

また、文書制御属性 18 が、「印刷可能ユーザ = 文書利用者 200、印刷可能プリンタ = プリンタ 24、印刷条件 = 二次配布禁止 (TrustMarking)」である場合、文書管理サーバ 12 はユーザ及びプリンタを認証した後、復号鍵 16' をプリンタ 24 に返信する。プリンタ 24 では、二次配布禁止の印刷条件に従って所定のマーキング処理を施し、印刷文書 30 を出力する。なお、プリンタ 24 は二次配布禁止印刷が可能なプリンタであることが前提であり、ここにプリンタを特定する意義があるということもできる。すなわち、二次配布を禁止する場合には、二次配布禁止印刷を可能とするプリンタで印刷されるべきところ、本実施形態では特定のプリンタを指定した印刷が可能となるため二次配布禁止が可能となる。

20

【0047】

また、文書制御属性 18 が、「印刷可能ユーザ = 文書利用者 200、印刷可能プリンタ = プリンタ 24、印刷条件 = オーバレイ印刷」である場合も二次配布禁止印刷の場合と同様である。すなわち、文書管理サーバ 12 はユーザ及びプリンタを認証した後、暗号鍵 16 をプリンタ 24 に返信する。プリンタ 24 では、オーバレイ印刷の印刷条件に従って所定の背景印刷、例えば confidential の文字を背景印刷する等して印刷文書 30 を出力する。プリンタ 24 はオーバレイ印刷可能なプリンタであることが前提であり、ここにプリンタを特定する意義がある。

30

【0048】

また、文書制御属性 18 が、「印刷可能ユーザ = 文書利用者 200、印刷可能プリンタ = プリンタ 24、印刷条件 = 文書利用者 200 が課長以上の場合にはカラー印刷、そうでない場合には白黒印刷」である場合、文書管理サーバ 12 はユーザ及びプリンタを認証した後、さらにユーザ D/B 13 にアクセスして文書利用者 200 が課長以上であるかそうでないかを判定する。文書利用者 200 が課長以上である場合には復号鍵 16' とともに「印刷条件 = カラー印刷」なる制御属性をプリンタ 24 に返信する。プリンタ 24 はこの制御属性に従い暗号化文書 22 を復号して得られるオリジナル文書 10 をカラー印刷し、印刷文書 30 を出力する。文書利用者 200 が課長以上でない場合、文書管理サーバ 12 は復号鍵 16' とともに「印刷条件 = 白黒印刷」なる制御属性をプリンタ 24 に返信する。プリンタ 24 はこの制御属性に従いオリジナル文書 10 を白黒印刷し、印刷文書 30 を出力する。

40

【0049】

一方、文書制御属性 18 が、「印刷可能ユーザ = 文書利用者 201 (不図示)、印刷可能プリンタ = 25 (不図示)、印刷条件 = 白黒」である場合、プリンタ 24 から送信されたユーザ認証情報が文書利用者 201 と一致せず、プリンタ 24 はプリンタ 25 と一致しないため暗号鍵 16 はプリンタ 24 に返信されず、したがってプリンタ 24 では暗号化文書 22 を印刷できず印刷文書 30 もない。

50

## 【 0 0 5 0 】

本実施形態では、文書制御属性 1 8 は文書管理サーバ 1 2 に記憶され管理されているので、文書管理サーバ 1 2 にアクセスすることにより任意のタイミングで文書制御属性 1 8 を追加、削除、あるいは変更することが可能である。したがって、例えばオーバーレイ印刷として confidential の文字を背景印刷するとの制御属性を設定していたが、文書配布後にその文字を変更することも可能である。また、課長以上ではない場合は白黒印刷との制御属性を設定していたが、文書配布後に課長以上ではない場合もカラー印刷に変更することも容易である。具体的には、文書管理サーバ 1 2 にアクセスできる権限を有する文書管理者 3 0 0 が端末を用いて文書管理サーバ 1 2 にアクセスし、文書制御属性を変更すればよい。印刷可能ユーザあるいは印刷可能プリンタを変更する場合も同様である。

10

## 【 0 0 5 1 】

## &lt; 第 2 実施形態 &gt;

上記の実施形態では、文書作成者 1 0 0 が文書管理サーバ 1 2 から取得した暗号鍵 1 6 を用いてオリジナル文書 1 0 を暗号化して暗号化文書 2 2 を作成し、文書利用者 2 0 0 に配布しているが、オリジナル文書 1 0 の暗号化を文書管理サーバ 1 2 で実行することもできる。本実施形態ではこの場合について説明する。

## 【 0 0 5 2 】

図 3 には、本実施形態の処理が模式的に示されている。文書作成者 1 0 0 は、端末 1 を用いてオリジナル文書 1 0 を文書管理サーバ 1 2 に送信し、文書登録要求を出力する。文書管理サーバ 1 2 は、文書作成者 1 0 0 が本サービスを利用できるユーザであるか否かを認証した後、オリジナル文書 1 0 を暗号鍵 1 6 を用いて暗号化し、暗号化文書 2 2 及び文書識別子 1 4 として返信する。文書識別子 1 4 は文書データとともに暗号化してもよく、暗号化しなくてもよい。

20

## 【 0 0 5 3 】

暗号化文書 2 2 を受け取った文書作成者 1 0 0 は、記憶媒体に格納して文書利用者 2 0 0 に手渡す、あるいは端末 1 から端末 2 に対して暗号化文書 2 2 を送信することで文書利用者 2 0 0 に配布する。文書利用者 2 0 0 は、プリンタ 2 4 に対して暗号化文書 2 2 とともに印刷コマンドを出力する。

## 【 0 0 5 4 】

プリンタ 2 4 は、暗号化文書 2 2 及び文書利用者 2 0 0 のユーザ認証情報 2 6 を文書管理サーバ 1 2 に送信して文書属性を要求する。文書管理サーバ 1 2 は、プリンタ 2 4 を認証し、暗号化文書 2 2 に含まれる文書識別子 1 4 を復号し、当該文書識別子 1 4 で特定される文書制御属性に含まれる印刷可能ユーザ及び印刷可能プリンタがユーザ認証情報 2 6 及びプリンタに一致するか否かを判定する。一致する場合には、文書管理サーバ 1 2 は暗号化文書 2 2 を暗号鍵で復号し、得られたオリジナル文書 1 0 をプリンタ 2 4 に返信する。プリンタ 2 4 は、返信されたオリジナル文書 1 0 を印刷し、印刷文書 3 0 として出力する。文書制御属性として印刷可能枚数や印刷期間、カラー / 白黒等がある場合には第 1 実施形態と同様に処理される。

30

## 【 0 0 5 5 】

本実施形態では、オリジナル文書 1 0 の暗号化及び復号が文書管理サーバ 1 2 で実行されるため、端末 1 での処理及びプリンタ 2 4 での処理が簡易化される。

40

## 【 0 0 5 6 】

## &lt; 第 3 実施形態 &gt;

上記の第 2 実施形態では、文書管理サーバ 1 2 でオリジナル文書 1 0 を暗号化して文書作成者 1 0 0 に返信するとともに、暗号化文書 2 2 を復号化してプリンタ 2 4 に返信しているが、文書管理サーバ 1 2 でオリジナル文書 1 0 のフォーマットを変換してもよい。すなわち、文書作成者 1 0 0 はプリンタ 2 4 での印刷が不可能なフォーマットのオリジナル文書 1 0 を文書管理サーバ 1 2 に送信して文書登録要求を出力する。文書管理サーバ 1 2 は、この要求を受け付け、印刷不可能なフォーマットを印刷可能なフォーマットに変換し、さらに秘密鍵で暗号化して文書作成者 1 0 0 に返信する。以後は第 2 実施形態の同様の

50

処理が実行され、プリンタ 2 4 から印刷文書 3 0 が出力される。

【 0 0 5 7 】

文書管理サーバ 1 2 でのフォーマット変換は、例えば以下に行われる。文書作成者 1 0 0 からオリジナル文書 1 0 及び文書制御属性 1 8 を含む文書登録要求がなされると、文書制御属性 1 8 に含まれる印刷可能プリンタを抽出し、そのプリンタのプロパティをデータベースから検索し、印刷可能なフォーマットを取得する。そして、オリジナル文書のフォーマットがプリンタの印刷可能フォーマットと一致するか否かを判定し、一致しない場合には印刷可能フォーマットのいずれかに変換する。

【 0 0 5 8 】

本実施形態では、文書作成者 1 0 0 はオリジナル文書 1 0 のフォーマットを特に気にすることなく文書利用者 2 0 0 に文書を配布することが可能である。

【 0 0 5 9 】

< 第 4 実施形態 >

上記の第 1 ~ 第 3 実施形態では、オリジナル文書 1 0 は暗号化されて文書利用者 2 0 0 に配布されるため、文書利用者 2 0 0 はプリンタ 2 4 で印刷されるまでその文書の内容を知ることにはできない。これにより、印刷物の流出が防止されることになるが、その一方で文書利用者 2 0 0 は印刷前にどのような内容の文書を印刷しようとしているのか確認したいと欲する場合も少なくない。ある文書を印刷する場合、まず端末 2 のモニタ画面に文書データを表示してその内容を確認し、その後プリンタで印刷するのが通常のルーチンと考えられる。

【 0 0 6 0 】

そこで、本実施形態では、文書データの不正流出を防止しつつ、文書利用者 2 0 0 が印刷しようとする文書の内容をある程度事前に知ることができる構成について説明する。

【 0 0 6 1 】

図 4 には、本実施形態における処理が模式的に示されている。文書作成者 1 0 0 は、印刷可能なフォーマットのオリジナル文書 1 0 を暗号化するために端末 1 から文書管理サーバ 1 2 に対して文書登録要求を出力する。

【 0 0 6 2 】

文書管理サーバ 1 2 は、文書作成者 1 0 0 の認証を行い、認証完了後、文書を一意（ユニーク）に識別するための文書識別子 1 4 を生成し、暗号鍵 1 6 とともに文書作成者 1 0 0 に返信する。また、文書管理サーバ 1 2 は、文書が登録されたことを文書利用ログ 2 0 に登録する。

【 0 0 6 3 】

文書作成者 1 0 0 は、端末 1 を用いてオリジナル文書 1 0 を暗号鍵 1 6 で暗号化し、暗号化文書 2 2 を作成する。暗号化に用いられた暗号鍵 1 6 は、暗号作成後に廃棄される。また、文書作成者 1 0 0 は端末 1 にインストールされたハッシュ関数プログラムを用いて暗号化文書 2 2 のハッシュ値 1 7 を作成し、かつ、端末 1 にインストールされたサムネイル生成プログラムを用いてオリジナル文書 1 0 から文書内容を把握できるが内容の詳細は把握できないような縮小イメージ、すなわちサムネイル（SN）1 9 を作成する。ハッシュ値 1 7 及びサムネイル 1 9 作成後、文書作成者 1 0 0 は端末 1 から文書管理サーバ 1 2 に対して文書識別子 1 4、ハッシュ値 1 7 及びサムネイル 1 9 を送信し、文書管理サーバ 1 2 での署名を要求する。文書管理サーバ 1 2 は、サービス秘密鍵 1 5 を用いてこれらのデータにタイムスタンプを追加して署名を行い、その署名データ 2 1 を文書署名完了として文書作成者 1 0 0 に返信する。なお、公開鍵方式において、公開鍵とペアをなす秘密鍵を用いて暗号化することにより署名する技術は公知であるためその詳細は省略する。文書作成者 1 0 0 は、端末 1 を用いて暗号化文書 2 2 に署名データ 2 1 を付加した暗号化署名文書 2 3 を作成する。その後、端末 1 から端末 2 に対して暗号化署名文書 2 3 を送信する等により文書利用者 2 0 0 に配布される。

【 0 0 6 4 】

暗号化署名文書 2 3 の配布を受けた文書利用者 2 0 0 は、端末 2 のモニタ画面に暗号化

10

20

30

40

50

署名文書 23 に含まれるサムネイル 19 を表示し、内容を確認する。この際、サムネイル 19 が改竄されていないことを確認するために文書管理サーバ 12 の証明書 25 を用いてサムネイル 19 の署名の検証を行う。周知の如く、証明書 25 の実体は秘密鍵 15 に対応する公開鍵であり、検証は実質的に秘密鍵で暗号化されたサムネイルを公開鍵で復号化することに等しい。検証できた場合、文書利用者 200 はサムネイル 19 の内容が改竄されておらず正しいものであると確認することができる。検証後、文書利用者 200 は任意のタイミングで印刷すべく、端末 2 を操作して端末 2 からプリンタ 24 に対して暗号化署名文書 23 とともに印刷コマンドを送信する。

【0065】

プリンタ 24 は、まずユーザの認証を行い、認証完了後に送られてきた文書が正しい文書であるか否かを証明書 25 を用いて署名検証を行う。署名検証が正しく行なわれなかった場合、プリンタ 24 は印刷を拒否する。

【0066】

以後の処理は第 1 実施形態と同様であり、プリンタ 24 は文書管理サーバ 12 に対して文書識別子 14、ユーザ認証情報 26、を送信して文書属性を要求する。文書管理サーバ 12 は、プリンタを認証し、文書利用者 200 及びプリンタ 24 が文書制御属性 18 で指定される印刷可能ユーザ及び印刷可能プリンタに一致するか否かを判定し、一致する場合には暗号鍵 16 及び文書制御属性 18 (印刷条件を指定する属性) をプリンタ 24 に返信する。プリンタ 24 は、返信された暗号鍵 16 を用いて暗号化文書 22 を復号してオリジナル文書 10 を取得し、印刷文書 30 として出力する。

【0067】

本実施形態では、文書利用者 200 は端末 2 を用いて暗号化文書 22 の概要をサムネイル 19 で事前に知ることができる。また、サムネイル 19 は文書管理サーバ 12 の秘密鍵 15 で暗号化されることで署名されているため、その改竄も検知できる。

【0068】

< 第 5 実施形態 >

上記の第 4 実施形態では、オリジナル文書 10 の暗号化、ハッシュ値生成、サムネイル生成を文書作成者 100 側の端末 1 で実行したが、第 2 実施形態と同様にこれらを文書管理サーバ 12 側で実行してもよい。

【0069】

文書作成者 100 は端末 1 から文書管理サーバ 12 に対してオリジナル文書 10 を送信して文書登録要求を出力する。文書管理サーバ 12 は、オリジナル文書 10 から文書識別子 14 及びサムネイル 19 を生成し、またオリジナル文書 10 を暗号鍵 16 で暗号化して暗号化文書 22 を作成する。そして、暗号化文書 22 のハッシュ値 17 を生成し、文書識別子 14、ハッシュ値 17、サムネイル 19 に対してタイムスタンプを付加して秘密鍵 15 により署名し、暗号化署名文書 23 を作成する。暗号化署名文書 23 は文書作成者 100 に返信される。

【0070】

暗号化署名文書 23 の配布を受けた文書利用者 200 がプリンタ 24 に対して印刷コマンドを出力すると、プリンタ 24 は証明書 25 を用いて暗号化署名文書 23 に含まれる署名付きの文書識別子 14、ハッシュ値を検証し、改竄がなされていないことを確認した後、暗号化文書 22 を文書管理サーバ 12 に送信する。文書管理サーバ 12 は、文書利用者 200 及びプリンタ 24 が文書制御属性 18 で指定される印刷可能ユーザ及び印刷可能プリンタであるか否かを判定した後、暗号鍵 16 を用いて暗号化文書 22 を復号化し、オリジナル文書 10 をプリンタ 24 に返信する。

【0071】

以上説明したように、本実施形態では、特定のユーザによる特定のプリンタでの印刷が可能となる。また、文書制御属性を種々指定することで、特定のユーザによる特定のプリンタによる特定の印刷条件による印刷が可能となる。さらに、文書制御属性は文書管理サーバに記憶され管理されているため、任意のタイミング、具体的には文書配布後であって

10

20

30

40

50

も印刷条件を付加、削除、あるいは変更することができる。

【 0 0 7 2 】

本発明は上記の各実施形態に限定されるものではなく、種々の変形例が可能である。例えば、第1実施形態では文書作成者100が端末1を用いてオリジナル文書10を暗号化し、管理サーバ12から返信された暗号鍵16を用いてプリンタ24で復号化しているが、この場合でもプリンタ24は暗号化文書22を管理サーバ12に送信し、管理サーバ12で復号化してオリジナル文書10をプリンタ24に返信してもよい。また、第2実施形態では管理サーバ12でオリジナル文書10の暗号化及び復号化を実行しているが、オリジナル文書10の暗号化のみを実行し、プリンタ24に対して暗号鍵16を返信してプリンタ24で復号してもよい。

10

【図面の簡単な説明】

【 0 0 7 3 】

【図1】実施形態に係るシステムの概念構成図である。

【図2】実施形態の処理の流れを示す模式的説明図である。

【図3】他の実施形態の処理の流れを示す模式的説明図である。

【図4】さらに他の実施形態の処理の流れを示す模式的説明図である。

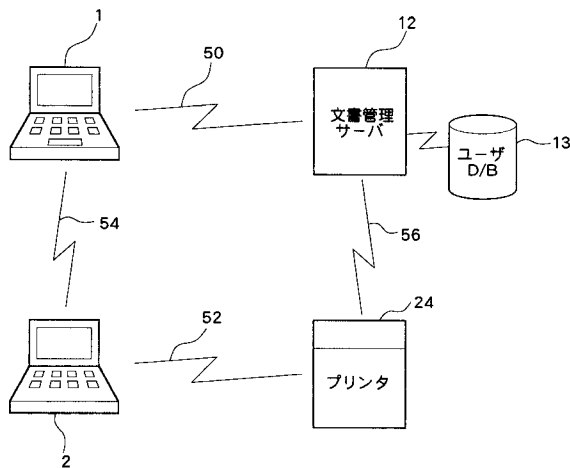
【符号の説明】

【 0 0 7 4 】

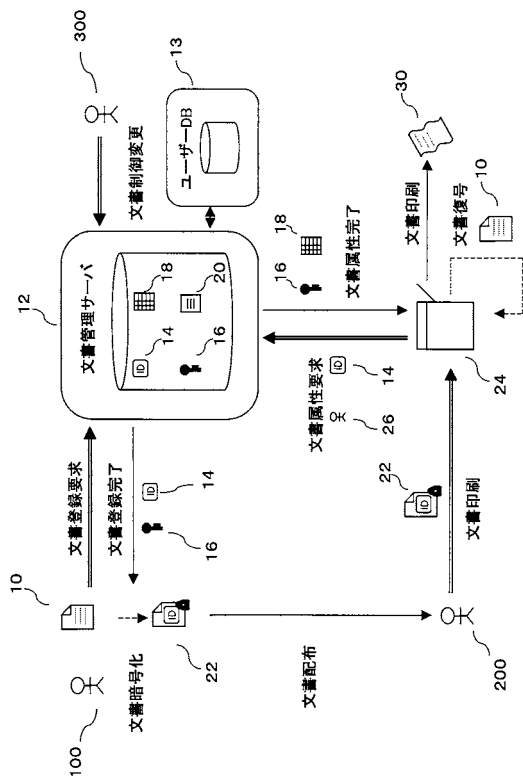
1 端末（文書作成者端末）、2 端末（文書利用者端末）、10 オリジナル文書、  
12 文書管理サーバ、13 ユーザデータベース（D/B）、14 文書識別子、16 暗号鍵、18 文書制御属性、20 文書利用ログ、22 暗号化文書、24 プリンタ、30 印刷文書、100 文書作成者、200 文書利用者、300 文書管理者。

20

【図1】

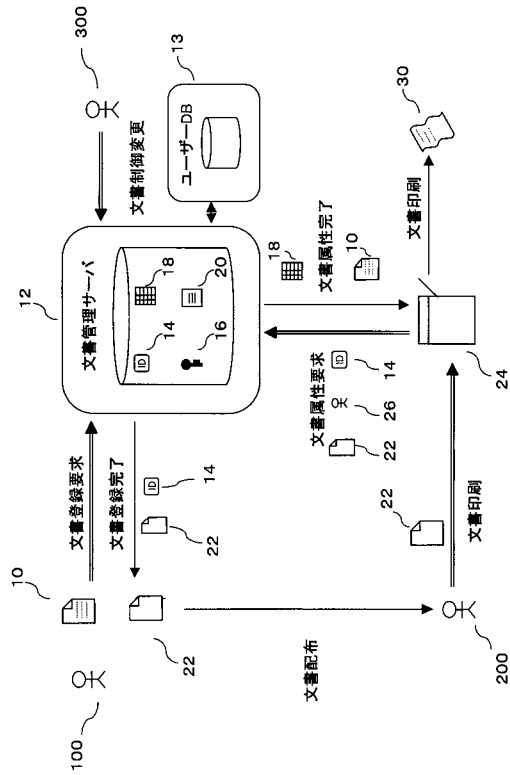


【図2】

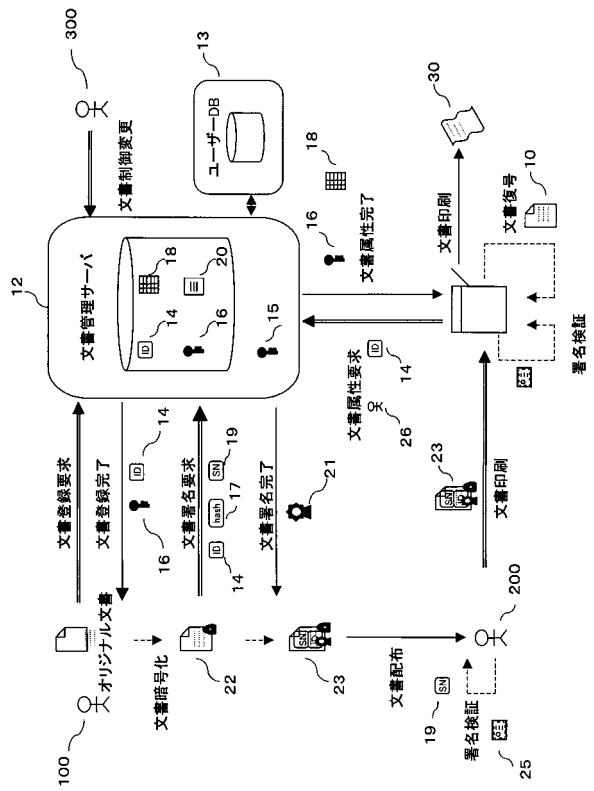




【 図 3 】



【 図 4 】



---

フロントページの続き

(56)参考文献 特開平 11 - 283003 (JP, A)  
特開 2004 - 110679 (JP, A)  
特開 2002 - 232685 (JP, A)  
特開 2004 - 152108 (JP, A)  
特開 2001 - 188664 (JP, A)  
特開 2001 - 175570 (JP, A)  
特開 2004 - 046809 (JP, A)  
特開 2003 - 036364 (JP, A)  
特開 2002 - 351743 (JP, A)  
特開 2003 - 016057 (JP, A)  
特開平 09 - 114616 (JP, A)

(58)調査した分野(Int.Cl., DB名)  
G 0 6 F        3 / 1 2  
B 4 1 J       2 9 / 0 0  
B 4 1 J       2 9 / 3 8