(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4687722号
(P4687722)

(45)発行日　平成23年5月25日(2011.5.25)　(24)登録日　平成23年2月25日(2011.2.25)

(51)Int.Cl.　F I
H04N 1/00 (2006.01)　H04N 1/00 107A
G06F 13/00 (2006.01)　H04N 1/00 C
G06F 13/00 510A
G06F 13/00 560A

請求項の数 9　(全 26 頁)

(21)出願番号　特願2008-23633(P2008-23633)
(22)出願日　平成20年2月4日(2008.2.4)
(65)公開番号　特開2009-188493(P2009-188493A)
(43)公開日　平成21年8月20日(2009.8.20)
審査請求日　平成22年2月2日(2010.2.2)

(73)特許権者　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町１５番１号
(74)代理人　110000110
特許業務法人快友国際特許事務所
(72)発明者　古川　顕寛
愛知県名古屋市瑞穂区苗代町１５番１号
ブラザー工業株式会社内
(72)発明者　安藤　智子
愛知県名古屋市瑞穂区苗代町１５番１号
ブラザー工業株式会社内

審査官　松尾　淳一

最終頁に続く

(54)【発明の名称】スキャナ

(57)【特許請求の範囲】
【請求項１】
スキャナであって、
スキャン対象物をスキャンしてスキャンデータを作成するスキャンデータ作成手段と、
スキャンデータ作成手段によって作成された前記スキャンデータを記憶するスキャンデータ記憶手段と、
前記スキャナによって生成される認証情報を表示する認証情報出力手段と、
スキャンデータ作成手段によって作成された前記スキャンデータが送信されるべきデバイスに向けて、認証情報出力手段によって表示される前記認証情報を送信せずに、前記スキャンデータが記憶されているロケーションを特定するロケーション特定情報を送信するロケーション特定情報送信手段と、
スキャンデータ作成手段によって作成された前記スキャンデータが送信されるべき前記デバイスのＩＰアドレスと、前記スキャンデータが記憶されているロケーションを特定する前記ロケーション特定情報と、認証情報出力手段によって表示される前記認証情報と、が対応づけられている情報を記憶するデバイス－ロケーション記憶手段と、
前記デバイスから、前記ロケーション特定情報と、前記ユーザによって前記デバイスに入力される前記認証情報と、の組合せを受信する受信手段と、
受信手段によって受信された組合せに含まれる前記ロケーション特定情報と、当該組合せに含まれる前記認証情報と、当該組合せの送信元である前記デバイスの前記ＩＰアドレスと、が対応づけられている情報がデバイス－ロケーション記憶手段に記憶されているこ

とを条件として、前記ＩＰアドレスによって特定される前記デバイスに向けて、前記ロケーション特定情報によって特定されるロケーションに記憶されている前記スキャンデータを送信するスキャンデータ送信手段と
を備えるスキャナ。
【請求項２】
前記スキャンデータ作成手段によって作成された前記スキャンデータを、前記認証情報出力手段によって出力された前記認証情報をキーとして暗号化する暗号化手段をさらに備え、
前記スキャンデータ送信手段は、暗号化手段によって暗号化された前記スキャンデータを送信する
ことを特徴とする請求項１に記載のスキャナ。
【請求項３】
自身が暗号化通信プロトコルを利用して前記スキャンデータを送信することが可能であるのか否かを判断する判断手段をさらに備え、
判断手段によって肯定的に判断された場合に、（１）前記暗号化手段は、前記スキャンデータ作成手段によって作成された前記スキャンデータを暗号化せず、（２）前記スキャンデータ送信手段は、暗号化されていない前記スキャンデータを送信し、
判断手段によって否定的に判断された場合に、（１）前記暗号化手段は、前記スキャンデータ作成手段によって作成された前記スキャンデータを暗号化し、（２）前記スキャンデータ送信手段は、前記暗号化手段によって暗号化された前記スキャンデータを送信する
ことを特徴とする請求項２に記載のスキャナ。
【請求項４】
前記判断手段によって肯定的に判断された場合に、前記ロケーション特定情報送信手段は、暗号化通信プロトコルのスキーム文字列を含む前記ロケーション特定情報を送信し、
前記判断手段によって否定的に判断された場合に、前記ロケーション特定情報送信手段は、非暗号化通信プロトコルのスキーム文字列を含む前記ロケーション特定情報を送信する
ことを特徴とする請求項３に記載のスキャナ。
【請求項５】
スキャンデータのデータ形式を入力するデータ形式入力手段をさらに備え、
前記スキャンデータ作成手段は、データ形式入力手段に入力されたデータ形式に基づいて前記スキャンデータを作成し、
前記ロケーション特定情報送信手段は、前記スキャンデータ作成手段によって作成された前記スキャンデータが記憶されているロケーションを特定する前記ロケーション特定情報と、当該スキャンデータのデータ形式を特定するデータ形式特定情報とを送信する
ことを特徴とする請求項１から４のいずれかに記載のスキャナ。
【請求項６】
前記データ形式入力手段に複数パターンのデータ形式が入力された場合に、前記スキャンデータ作成手段は、前記データ形式入力手段に入力された前記複数パターンのデータ形式に基づいて前記スキャンデータを作成し、
前記ロケーション特定情報送信手段は、前記データ形式入力手段に入力された前記複数パターンのデータ形式のそれぞれについて、前記ロケーション特定情報と、当該パターンのデータ形式を特定する前記データ形式特定情報とを送信し、
前記受信手段は、前記ロケーション特定情報と前記認証情報と少なくとも１つの前記データ形式特定情報との組合せを受信し、
前記スキャンデータ送信手段は、前記受信手段によって受信された組合せに含まれる前記ロケーション特定情報と、当該組合せに含まれる前記認証情報と、当該組合せの送信元である前記デバイスの前記ＩＰアドレスと、が対応づけられている情報が前記デバイスーロケーション記憶手段に記憶されていることを条件として、当該組合せに含まれる前記データ形式特定情報によって特定されるデータ形式の前記スキャンデータを送信する

ことを特徴とする請求項５に記載のスキャナ。
【請求項７】
前記ロケーション特定情報送信手段は、前記スキャンデータ作成手段によって作成された前記スキャンデータが複数のファイルによって構成される場合に、前記複数のファイルを格納しているフォルダのロケーションを特定する前記ロケーション特定情報を送信する
ことを特徴とする請求項１から６のいずれかに記載のスキャナ。
【請求項８】
前記ロケーション特定情報送信手段は、前記スキャンデータ作成手段によって作成された前記スキャンデータが記憶されているロケーションを特定する前記ロケーション特定情報と、前記スキャンデータのサムネイル画像データとを送信する
ことを特徴とする請求項１から７のいずれかに記載のスキャナ。
【請求項９】
スキャナに搭載されるコンピュータに、以下の各処理、即ち、
スキャン対象物をスキャンしてスキャンデータを作成するスキャンデータ作成処理と、
スキャンデータ作成処理で作成された前記スキャンデータを記憶するスキャンデータ記憶処理と、
前記スキャナによって生成される認証情報を表示する認証情報出力処理と、
スキャンデータ作成処理で作成された前記スキャンデータが送信されるべきデバイスに向けて、認証情報出力処理で表示される前記認証情報を送信せずに、前記スキャンデータが記憶されているロケーションを特定するロケーション特定情報を送信するロケーション特定情報送信処理と、
スキャンデータ作成処理で作成された前記スキャンデータが送信されるべき前記デバイスのＩＰアドレスと、前記スキャンデータが記憶されているロケーションを特定する前記ロケーション特定情報と、認証情報出力処理で表示される前記認証情報と、が対応づけられている情報を記憶するデバイス－ロケーション記憶処理と、
前記デバイスから、前記ロケーション特定情報と、前記ユーザによって前記デバイスに入力される前記認証情報と、の組合せを受信する受信処理と、
受信処理で受信された組合せに含まれる前記ロケーション特定情報と、当該組合せに含まれる前記認証情報と、当該組合せの送信元である前記デバイスの前記ＩＰアドレスと、が対応づけられている情報がデバイス－ロケーション記憶処理で記憶されたことを条件として、前記ＩＰアドレスによって特定される前記デバイスに向けて、前記ロケーション特定情報によって特定されるロケーションに記憶されている前記スキャンデータを送信するスキャンデータ送信処理と
を実行させることを特徴とするコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、スキャンデータを外部に送信することができるスキャナに関する。
【背景技術】
【０００２】
下記の特許文献１には、スキャンデータを外部に送信することができるスキャナが開示されている。このスキャナは、スキャンデータを作成して記憶することができる。スキャナは、スキャンデータが記憶されているＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）を電子メールに記述し、その電子メールを他のデバイスに送信する。このデバイスは、電子メールに記述されているＵＲＬにアクセスすることによって、スキャンデータをダウンロードする。
【０００３】
【特許文献１】特開２００６－３１１３４４号公報
【発明の開示】
【発明が解決しようとする課題】

【０００４】
上述したように、特許文献１に開示されているスキャナは、スキャンデータが記憶されているロケーションを特定するロケーション特定情報（上記の例ではＵＲＬ）を他のデバイスに送信することができる。スキャナからデバイスにロケーション特定情報が送信される過程において、ロケーション特定情報が第三者によって盗み見られる可能性がある。この場合、このロケーション特定情報によって特定されるロケーションに記憶されているスキャンデータが第三者によって盗み取られる可能性がある。本明細書では、スキャンデータが第三者によって盗み取られる事象が発生することを抑制することができる技術を開示する。

【課題を解決するための手段】

【０００５】
本発明のスキャナは、スキャン対象物をスキャンしてスキャンデータを作成するスキャンデータ作成手段と、スキャンデータ作成手段によって作成された前記スキャンデータを記憶するスキャンデータ記憶手段と、前記スキャナによって生成される認証情報を表示する認証情報出力手段と、スキャンデータ作成手段によって作成された前記スキャンデータが送信されるべきデバイスに向けて、認証情報出力手段によって表示される前記認証情報を送信せずに、前記スキャンデータが記憶されているロケーションを特定するロケーション特定情報を送信するロケーション特定情報送信手段と、スキャンデータ作成手段によって作成された前記スキャンデータが送信されるべきデバイスのＩＰアドレスと、前記スキャンデータが記憶されているロケーションを特定する前記ロケーション特定情報と、認証情報出力手段によって表示される前記認証情報と、が対応づけられている情報を記憶するデバイス－ロケーション記憶手段と、前記デバイスから、前記ロケーション特定情報と、前記ユーザによって前記デバイスに入力される前記認証情報と、の組合せを受信する受信手段と、受信手段によって受信された組合せに含まれる前記ロケーション特定情報と、当該組合せに含まれる前記認証情報と、当該組合せの送信元である前記デバイスの前記ＩＰアドレスと、が対応づけられている情報がデバイス－ロケーション記憶手段に記憶されていることを条件として、前記ＩＰアドレスによって特定される前記デバイスに向けて、前記ロケーション特定情報によって特定されるロケーションに記憶されている前記スキャンデータを送信するスキャンデータ送信手段とを備える。
本明細書によって開示される一つの形態のスキャナは、スキャンデータ作成手段とスキャンデータ記憶手段とロケーション特定情報送信手段とデバイス－ロケーション記憶手段と受信手段とスキャンデータ送信手段とを備える。スキャンデータ作成手段は、スキャン対象物をスキャンしてスキャンデータを作成する。スキャンデータ記憶手段は、スキャンデータ作成手段によって作成されたスキャンデータを記憶する。ロケーション特定情報送信手段は、スキャンデータ作成手段によって作成されたスキャンデータが送信されるべきデバイスに向けて、当該スキャンデータが記憶されているロケーションを特定するロケーション特定情報を送信する。上記の「スキャンデータが送信されるべきデバイス」は、スキャン毎にユーザによって設定されてもよいし、ユーザによって予め設定されていてもよいし、他の手法によって決められてもよい。このデバイスの例として、パーソナルコンピュータ、サーバ、プリンタ、携帯端末（携帯電話、パーソナルデジタルアシスタント（ＰＤＡ））等を挙げることができる。また、上記の「ロケーション特定情報」という用語は、最も広義に解釈されるべきものであり、スキャンデータが記憶されているロケーションを特定することができるあらゆる情報を含む概念である。「ロケーション特定情報」の例として、ＵＲＩ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｉｄｅｎｔｉｆｉｅｒｓ）、ＵＲＬ、フォルダ名、ファイル名等を挙げることができる。

【０００６】
デバイス－ロケーション記憶手段は、スキャンデータ作成手段によって作成されたスキャンデータが送信されるべきデバイスを特定するデバイス特定情報と、当該スキャンデータが記憶されているロケーションを特定するロケーション特定情報とが対応づけられている情報を記憶する。上記の「デバイス特定情報」という用語は、最も広義に解釈されるべ

きものであり、デバイスを特定することができるあらゆる情報を含む概念である。「デバイス特定情報」の例として、ＵＲＩ、ＵＲＬ、ＩＰアドレス、ＭＡＣアドレス等を挙げることができる。受信手段は、デバイス特定情報とロケーション特定情報との組合せを受信する。なお、「組合せを受信する」という用語は、「組合せを同時に受信すること」に限られない。一方の情報を受信するタイミングと他方の情報を受信するタイミングとの間に時間差があってもよい。スキャンデータ送信手段は、受信手段によって受信された組合せに含まれるデバイス特定情報とロケーション特定情報とが対応づけられている情報がデバイス－ロケーション記憶手段に記憶されていることを条件として、当該デバイス特定情報によって特定されるデバイスに向けて、当該ロケーション特定情報によって特定されるロケーションに記憶されているスキャンデータを送信する。

【０００７】

上記のスキャナは、スキャンデータが送信されるべきデバイス（以下ではデバイス特定情報を「Ｘ」とする）に向けて、そのスキャンデータのロケーション特定情報（以下では「Ｙ」とする）を送信する。この結果、このデバイスのユーザは、スキャンデータのロケーション特定情報Ｙを知ることができる。スキャナは、デバイス特定情報Ｘとロケーション特定情報Ｙとを対応づけて記憶しておく（デバイス－ロケーション記憶手段に記憶される）。ロケーション特定情報Ｙの送信先のデバイスのユーザは、このデバイスを利用してロケーション特定情報Ｙにアクセスすることができる。この場合、デバイス特定情報Ｘとロケーション特定情報Ｙとの組合せがデバイスから送信され、スキャナによって受信される。このＸとＹの組合せは、デバイス－ロケーション記憶手段に記憶されている。この結果、スキャナは、ロケーション特定情報Ｙに対応するスキャンデータをデバイスに送信する。デバイスは、スキャンデータを取得することができる。一方において、第三者がロケーション特定情報Ｙを盗み見て、上記のデバイス以外のデバイス（以下ではデバイス特定情報を「Ｚ」とする）を利用してロケーション特定情報Ｙにアクセスした場合、デバイス特定情報Ｚとロケーション特定情報Ｙとの組合せがスキャナによって受信される。このＺとＹの組合せは、デバイス－ロケーション記憶手段に記憶されていない。ロケーション特定情報Ｙに対応するスキャンデータが送信されない。これにより、スキャンデータが第三者によって盗み取られる事象が発生することを抑制することができる。

【０００８】

第三者がロケーション特定情報Ｙを盗み見て、このロケーション特定情報Ｙの送信先のデバイス（デバイス特定情報Ｘ）を利用してロケーション特定情報Ｙにアクセスする可能性も否定できない。このような状況においてスキャンデータが第三者によって盗み取られないように、以下の構成を採用してもよい。即ち、上記のスキャナは、認証情報を出力する認証情報出力手段をさらに備えていてもよい。この「出力」という用語は、最も広義に解釈されるべきものであり、例えば、表示すること、音声出力すること、印刷すること、他のデバイスに送信すること等を含む概念である。デバイス－ロケーション記憶手段は、デバイス特定情報と、ロケーション特定情報と、認証情報出力手段によって出力された認証情報とが対応づけられている情報を記憶してもよい。受信手段は、デバイス特定情報とロケーション特定情報と認証情報との組合せを受信してもよい。スキャンデータ送信手段は、受信手段によって受信された組合せに含まれるデバイス特定情報とロケーション特定情報と認証情報とが対応づけられている情報がデバイス－ロケーション記憶手段に記憶されていることを条件として、当該デバイス特定情報によって特定されるデバイスに向けて、当該ロケーション特定情報によって特定されるロケーションに記憶されているスキャンデータを送信してもよい。

【０００９】

上記の構成によると、第三者は、認証情報を知り得ないために、スキャンデータを取得することができない。スキャンデータが第三者によって盗み取られることを効果的に抑制することができる。

【００１０】

上記のスキャナは、スキャンデータ作成手段によって作成されたスキャンデータを、認

証情報出力手段によって出力された認証情報をキーとして暗号化する暗号化手段をさらに備えていてもよい。この場合、スキャンデータ送信手段は、暗号化手段によって暗号化されたスキャンデータを送信してもよい。この構成によると、スキャンデータが第三者によって盗み取られることを効果的に抑制することができる。

【００１１】

上記のスキャナは、自身が暗号化通信プロトコルを利用してスキャンデータを送信することが可能であるのか否かを判断する判断手段をさらに備えていてもよい。上記の「暗号化通信プロトコル」という用語は、最も広義に解釈されるべきものであり、暗号化通信を行なうあらゆるプロトコルを含む概念である。「暗号化通信プロトコル」の例として、ＨＴＴＰＳ（Ｈｙｐｅｒｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ Ｓｅｃｕｒｉｔｙ）、ＦＴＰＳ（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ ｏｖｅｒ ＳＳＬ／ＴＬＳ）、ＳＦＴＰ（Ｓｅｃｕｒｅ Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）等を挙げることができる。上記の判断手段によって肯定的に判断された場合に、暗号化手段は、スキャンデータ作成手段によって作成されたスキャンデータを暗号化しなくてもよい。この場合、スキャンデータ送信手段は、暗号化されていないスキャンデータを送信してもよい。一方において、上記の判断手段によって否定的に判断された場合に、暗号化手段は、スキャンデータ作成手段によって作成されたスキャンデータを暗号化してもよい。この場合、スキャンデータ送信手段は、暗号化手段によって暗号化されたスキャンデータを送信してもよい。この構成では、暗号化通信によってスキャンデータを送信することができる場合に、スキャンデータ自身を暗号化しない。これにより、スキャンデータの暗号化処理を省略することができ、スキャナの処理負担を軽減させることができる。

【００１２】

上記の判断手段によって肯定的に判断された場合に、ロケーション特定情報送信手段は、暗号化通信プロトコルのスキーム文字列を含むロケーション特定情報を送信してもよい。この場合、デバイスが上記のロケーション特定情報にアクセスする際に、暗号化通信プロトコルが利用される。この結果、デバイスからのアクセスに対してスキャナがスキャンデータを送信する際にも、暗号化通信プロトコルが利用されることになる。スキャナは、暗号化通信プロトコルを利用してスキャンデータを送信することができる。一方において、上記の判断手段によって否定的に判断された場合に、ロケーション特定情報送信手段は、非暗号化通信プロトコルのスキーム文字列を含むロケーション特定情報を送信してもよい。上記の「非暗号化通信プロトコル」という用語は、最も広義に解釈されるべきものであり、暗号化通信を行なわないあらゆるプロトコルを含む概念である。「非暗号化通信プロトコル」の例として、ＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）、ＦＴＰ（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）、ＣＩＦＳ（Ｃｏｍｍｏｎ Ｉｎｔｅｒｎｅｔ Ｆｉｌｅ Ｓｙｓｔｅｍ）、ＳＭＢ（Ｓｅｒｖｅｒ Ｍｅｓｓａｇｅ Ｂｌｏｃｋ）等を挙げることができる。

【００１３】

上記のスキャナは、スキャンデータのデータ形式を入力するデータ形式入力手段をさらに備えていてもよい。上記の「スキャンデータのデータ形式」という用語は、最も広義に解釈されるべきものであり、スキャンデータのデータ形式を特定するためのあらゆる項目を含む概念である。「スキャンデータのデータ形式」の例として、解像度、色彩情報（カラー、グレースケール、モノクロ、色数等）、ファイル形式（ＰＤＦ、ＴＩＦＦ、ＪＰＥＧ等）、それらの組合せ等を挙げることができる。なお、ユーザは、スキャナの操作部を操作することによってスキャンデータのデータ形式を入力してもよい。この場合、上記の操作部がデータ形式入力手段に相当することになる。一方において、スキャンデータのデータ形式は、他のデバイスからスキャナに送信されてもよい。この場合、他のデバイスから送信されたデータ形式を受信する手段がデータ形式入力手段に相当することになる。スキャンデータ作成手段は、データ形式入力手段に入力されたデータ形式に基づいてスキャンデータを作成してもよい。ロケーション特定情報送信手段は、スキャンデータ作成手段によって作成されたスキャンデータが記憶されているロケーションを特定するロケーショ

ン特定情報と、当該スキャンデータのデータ形式を特定するデータ形式特定情報とを送信してもよい。この構成によると、データ形式特定情報をデバイスに提供することができる。デバイスのユーザは、データ形式特定情報を見ることによって、スキャンデータのデータ形式を知ることができる。

【００１４】

データ形式入力手段に複数パターンのデータ形式が入力された場合に、スキャンデータ作成手段は、データ形式入力手段に入力された上記の複数パターンのデータ形式に基づいてスキャンデータを作成してもよい。なお、スキャンデータ作成手段は、上記の複数パターンのデータ形式のそれぞれについてスキャンデータを作成してもよい。また、スキャンデータ作成手段は、上記の複数パターンのデータ形式のそれぞれのスキャンデータを作成するためのベースとなるスキャンデータを作成してもよい。例えば、カラーと白黒の２つのデータ形式がデータ形式入力手段に入力された場合、スキャンデータ作成手段は、カラーのスキャンデータのみを作成してもよい。この場合、白黒のスキャンデータが必要になると、カラーのスキャンデータから白黒のスキャンデータを作成することができる。ロケーション特定情報送信手段は、データ形式入力手段に入力された上記の複数パターンのデータ形式のそれぞれについて、ロケーション特定情報と、当該パターンのデータ形式を特定するデータ形式特定情報とを送信してもよい。これにより、デバイスのユーザは、複数パターンのデータ形式を知ることができ、少なくとも１つのパターンのデータ形式を選択することができる。この場合、デバイス特定情報とロケーション特定情報と少なくとも１つのデータ形式特定情報との組合せがデバイスから送信され、この組合せがスキャナの受信手段によって受信される。スキャンデータ送信手段は、受信手段によって受信された組合せに含まれるデバイス特定情報とロケーション特定情報とが対応づけられている情報がデバイス－ロケーション記憶手段に記憶されていることを条件として、当該組合せに含まれるデータ形式特定情報によって特定されるデータ形式のスキャンデータを送信してもよい。この構成によると、デバイスのユーザによって選択されたデータ形式のスキャンデータをデバイスに提供することができる。

【００１５】

ロケーション特定情報送信手段は、スキャンデータ作成手段によって作成されたスキャンデータが複数のファイルによって構成される場合に、それらのファイルを格納しているフォルダのロケーションを特定するロケーション特定情報を送信してもよい。一方において、ロケーション特定情報送信手段は、スキャンデータ作成手段によって作成されたスキャンデータが複数のファイルによって構成される場合に、それらのファイルのそれぞれのロケーションを特定するロケーション特定情報を送信してもよい。

【００１６】

また、ロケーション特定情報送信手段は、スキャンデータ作成手段によって作成されたスキャンデータが記憶されているロケーションを特定するロケーション特定情報と、当該スキャンデータのサムネイル画像データとを送信してもよい。この構成によると、デバイスのユーザは、スキャンデータの内容を知ることができる。

【００１７】

本発明のコンピュータプログラムは、スキャナに搭載されるコンピュータに、以下の各処理、即ち、スキャン対象物をスキャンしてスキャンデータを作成するスキャンデータ作成処理と、スキャンデータ作成処理で作成された前記スキャンデータを記憶するスキャンデータ記憶処理と、前記スキャナによって生成される認証情報を表示する認証情報出力処理と、スキャンデータ作成処理で作成された前記スキャンデータが送信されるべきデバイスに向けて、認証情報出力処理で表示される前記認証情報を送信せずに、前記スキャンデータが記憶されているロケーションを特定するロケーション特定情報を送信するロケーション特定情報送信処理と、スキャンデータ作成処理で作成された前記スキャンデータが送信されるべき前記デバイスのＩＰアドレスと、前記スキャンデータが記憶されているロケーションを特定する前記ロケーション特定情報と、認証情報出力処理で表示される前記認証情報と、が対応づけられている情報を記憶するデバイス－ロケーション記憶処理と、前

記デバイスから、前記ロケーション特定情報と、前記ユーザによって前記デバイスに入力される前記認証情報と、の組合せを受信する受信処理と、受信処理で受信された組合せに含まれる前記ロケーション特定情報と、当該組合せに含まれる前記認証情報と、当該組合せの送信元である前記デバイスの前記ＩＰアドレスと、が対応づけられている情報がデバイス－ロケーション記憶処理で記憶されたことを条件として、前記ＩＰアドレスによって特定される前記デバイスに向けて、前記ロケーション特定情報によって特定されるロケーションに記憶されている前記スキャンデータを送信するスキャンデータ送信処理とを実行させる。

また、本明細書によって開示される一つの形態のコンピュータプログラムは、スキャナに搭載されるコンピュータに以下の各処理を実行させる。

・スキャン対象物をスキャンしてスキャンデータを作成するスキャンデータ作成処理。
・スキャンデータ作成処理で作成されたスキャンデータを記憶するスキャンデータ記憶処理。
・スキャンデータ作成処理で作成されたスキャンデータが送信されるべきデバイスに向けて、当該スキャンデータが記憶されているロケーションを特定するロケーション特定情報を送信するロケーション特定情報送信処理。
・スキャンデータ作成処理で作成されたスキャンデータが送信されるべきデバイスを特定するデバイス特定情報と、当該スキャンデータが記憶されているロケーションを特定するロケーション特定情報とが対応づけられている情報を記憶するデバイス－ロケーション記憶処理。
・デバイス特定情報とロケーション特定情報との組合せを受信する受信処理。
・受信処理で受信された組合せに含まれるデバイス特定情報とロケーション特定情報とが対応づけられている情報がデバイス－ロケーション記憶処理で記憶されたことを条件として、当該デバイス特定情報によって特定されるデバイスに向けて、当該ロケーション特定情報によって特定されるロケーションに記憶されているスキャンデータを送信するスキャンデータ送信処理。

このコンピュータプログラムを利用すると、スキャンデータが第三者によって盗み取られることを抑制することができるスキャナを実現することができる。

【発明を実施するための最良の形態】

【００１８】

ここでは、以下の実施例に記載の技術の特徴の一部をまとめておく。

（形態１）スキャナは、複数のデバイス特定情報が記述されたリストを記憶することが可能であってもよい。ユーザは、このリストから少なくとも１つのデバイス特定情報を選択することが可能であってもよい。スキャナは、ユーザによって選択されたデバイス特定情報に向けて、ロケーション特定情報を送信してもよい。

（形態２）上記のリストでは、複数のデバイス特定情報のそれぞれについて、所定の情報が付加されてもよい。スキャナは、ユーザによって選択されたデバイス特定情報に付加されている上記の所定情報が第１タイプの情報である場合、認証情報を出力してもよい。スキャナは、ユーザによって選択されたデバイス特定情報に付加されている上記の所定情報が第２タイプの情報である場合、認証情報を出力しなくてもよい。

（形態３）スキャナは、複数枚のスキャン対象物が存在する場合、複数のスキャンデータファイルを作成してもよい。スキャナは、複数枚のスキャン対象物のそれぞれについて１つのスキャンデータファイルを作成してもよいし、別の手法を利用して複数のスキャンデータファイルを作成してもよい。後者の場合、スキャナは、所定の用紙がスキャンされると、それ以降のスキャン対象物のスキャンデータについて別のスキャンデータファイルを作成してもよい。

【実施例】

【００１９】

図面を参照して実施例を説明する。図１は、本実施例のスキャナシステム２を示す。ス

キャナシステム２は、スキャナ１０とＰＣ４０等を備える。図１では１つのＰＣ４０のみが示されているが、実際は複数のＰＣが存在している。各デバイス１０，４０は、ＬＡＮやインターネット回線等の通信回線３６を介して相互に通信可能に接続されている。

【００２０】

（スキャナの構成）

スキャナ１０は、操作装置１２と表示装置１４とスキャン装置１６と原稿トレイ１８と制御装置２０と記憶装置２２とネットワークインターフェイス３２等を有する。操作装置１２は、複数のキーによって構成される。ユーザは、操作装置１２を操作することによって、様々な情報や指示をスキャナ１０に入力することができる。表示装置１４は、様々な情報を表示することができる。スキャン装置１６は、原稿トレイ１８に載置された原稿をスキャンすることによってスキャンデータを作成する。制御装置２０は、記憶装置２２に記憶されているプログラム（図示省略）に従って、様々な処理を実行する。制御装置２０が実行する処理の内容については、後で詳しく説明する。

【００２１】

記憶装置２２は、ＲＯＭ、ＥＥＰＲＯＭ、ＲＡＭ等によって構成されている。記憶装置２２は、送信先デバイスＵＲＬ記憶領域２４とスキャンデータ記憶領域２６と対応情報記憶領域２８とその他の記憶領域３０とを有する。各記憶領域２４，２６，２８等に記憶されるべき情報について順に説明する。

【００２２】

送信先デバイスＵＲＬ記憶領域２４は、スキャンデータが送信されるべきデバイスを特定する情報を記憶することができる。図２は、送信先デバイスＵＲＬ記憶領域２４の記憶内容の一例を示す。送信先デバイスＵＲＬ記憶領域２４は、複数の組合せデータ７０，７２を記憶することができる。各組合せデータ７０，７２は、名称６０と共有フォルダＵＲＬ６２と暗号化の有無に関する情報（以下では「暗号化情報」と呼ぶ）６６とが対応づけられたデータである。名称６０は、デバイスのユーザを特定する名称を示す。共有フォルダＵＲＬ６２は、デバイスに設定されている共有フォルダのＵＲＬを示す。なお、上記の「共有フォルダ」は、外部からアクセス可能なフォルダを意味している。即ち、共有フォルダが存在する場合、その共有フォルダに格納されているファイルに外部からアクセスしたり、その共有フォルダに新たなファイルを外部から格納させたりすることができる。共有フォルダのＵＲＬは、その共有フォルダを有するデバイスのＩＰアドレスを含んでいる。例えば、組合せデータ７０の共有フォルダＵＲＬ６２である「１９２．１６８．０．２／ｃｏｍｍｏｎ」は、「１９２．１６８．０．２」というＩＰアドレスを含んでいる。なお、ここでは、ＵＲＬに含まれるべきスキーム文字列（例えばｆｉｌｅ：／／）を図示省略している。以下でも、スキーム文字列を省略してＵＲＬを記載することがある。暗号化情報６６は、後述するパスワードを生成するのか否かを示す情報である。暗号化情報６６は、「ＹＥＳ」と「ＮＯ」のいずれかである。

【００２３】

ユーザは、送信先デバイスＵＲＬ記憶領域２４に各組合せデータ７０，７２を記憶させることができる。例えば、ユーザは、操作装置１２を操作することによって、各組合せデータ７０，７２を送信先デバイスＵＲＬ記憶領域２４に記憶させることができる。また、例えば、ユーザは、外部装置（スキャナ１０以外のデバイス）に各組合せデータ７０，７２を入力し、その外部装置からスキャナ１０に向けて各組合せデータ７０，７２を送信させることができる。この場合、スキャナ１０は、上記の外部装置から送信された各組合せデータ７０，７２を送信先デバイスＵＲＬ記憶領域２４に記憶することができる。

【００２４】

スキャンデータ記憶領域２６は、スキャン装置１６によって作成されたスキャンデータを記憶することができる。図３は、スキャンデータ記憶領域２６の記憶内容の一例を示す。なお、図３に示される符号２６ａは、スキャナ１０のホスト名を示す。スキャンデータ記憶領域２６は、フォルダとファイルの階層構造を利用してスキャンデータ（スキャンデータファイル）を記憶することができる。スキャンデータ記憶領域２６は、複数のスキャ

ンデータファイルを記憶することができる。図３の例では、スキャンデータ記憶領域２６は、２つのフォルダ８０，９０を記憶している。フォルダ８０は、「ｓｃａｎ０００１」というフォルダ名８０ａを有する。フォルダ８０は、スキャンデータファイル８２を格納している。即ち、フォルダ８０の下位ファイルとして、スキャンデータファイル８２が存在する。スキャンデータファイル８２は、ファイル名８２ａとスキャンデータ８２ｄとが対応づけられたものである。ファイル名８２ａは、スキャンデータファイル８２が作成された日時を示す文字列８２ｂを含んでいる。この文字列８２ｂの場合、２００８年１月１日１時１分００秒にスキャンデータファイル８２が作成されたことを意味している。また、ファイル名８２ａは、拡張子を示す文字列８２ｃを含んでいる。本実施例では、「．ｂｉｎ」という拡張子が利用されている。フォルダ８０やスキャンデータファイル８２がどのようにして作成されるのかについては、後で詳しく説明する。

【００２５】

フォルダ９０は、「ｓｃａｎ０００２」というフォルダ名９０ａを有する。フォルダ９０は、複数のファイル９２，９４，９６を格納している。より具体的に言うと、フォルダ９０は、１つのデータ形式ファイル９２と複数のスキャンデータファイル９４，９６とを格納している。データ形式ファイル９２は、ファイル名９２ａとドキュメントデータ９２ｄとが対応づけられたものである。ドキュメントデータ９２ｄは、スキャンデータのデータ形式が記述されたデータである。ドキュメントデータ９２ｄの具体的な内容については、後で詳しく説明する。上記のスキャンデータファイル８２と同様に、スキャンデータファイル９４は、ファイル名９４ａとスキャンデータ９４ｄとが対応づけられたものである。ファイル名９４ａは、スキャンデータファイル９４が作成された日時を示す文字列９４ｂと拡張子を示す文字列９４ｃを含んでいる。スキャンデータファイル９６は、ファイル名９６ａとスキャンデータ９６ｄとが対応づけられたものである。ファイル名９６ａは、スキャンデータファイル９６が作成された日時を示す文字列９６ｂと拡張子を示す文字列９６ｃを含んでいる。フォルダ９０や各ファイル９２，９４，９６がどのようにして作成されるのかについては、後で詳しく説明する。

【００２６】

図４は、対応情報記憶領域２８の記憶内容の一例を示す。対応情報記憶領域２８は、複数の対応情報１１０，１１２を記憶することができる。各対応情報１１０，１１２は、ＩＤ１００とＵＲＬ１０２と送信先１０４とパスワード１０６とが対応づけられたデータである。ＩＤ１００は、各対応情報を識別する情報を示す。ＵＲＬ１０２は、スキャンデータが格納されているフォルダのＵＲＬを示す。送信先１０４は、スキャンデータの送信先の共有フォルダのＵＲＬ及び送信先のデバイスのＩＰアドレスを示す。パスワード１０６は、スキャンデータが作成される際に出力されるパスワードを示す。なお、対応情報は、パスワードを含まないことがある（対応情報１１２参照）。各対応情報１１０，１１２がどのように作成されるのかについては、後で詳しく説明する。

【００２７】

記憶領域３０は、上記の各記憶領域２４，２６，２８に記憶されるべき情報以外の情報を記憶することができる。記憶領域３０に記憶される情報の内容については、必要に応じて後で説明する。

【００２８】

ネットワークインターフェイス３２は、通信回線３６に接続されている。スキャナ１０は、ネットワークインターフェイス３２及び通信回線３６を介して、ＰＣ４０と通信可能である。

【００２９】

（ＰＣの構成）

ＰＣ４０は、操作装置４２と表示装置４４と制御装置４６と記憶装置４８とネットワークインターフェイス５４等を有する。操作装置４２は、キーボードやマウスによって構成される。ユーザは、操作装置４２を操作することによって、様々な情報や指示をＰＣ４０に入力することができる。表示装置４４は、様々な情報を表示することができる。制御装

置４６は、記憶装置４８に記憶されているプログラム（図示省略）に従って、様々な処理を実行する。

【００３０】

記憶装置４８は、ＲＯＭ、ＥＥＰＲＯＭ、ＲＡＭ、ハードディスク装置等によって構成されている。記憶装置４８は、共有フォルダ５０とその他の記憶領域５２とを有する。ユーザは、操作装置４２を操作することによって、ＰＣ４０内に共有フォルダ５０を作成することができる。共有フォルダ５０は、他のデバイスからアクセス可能なフォルダである。逆に言うと、共有フォルダとして設定されていないフォルダは、他のデバイスからアクセス不能である。本実施例では、上記の図２の組合せデータ７０に含まれる共有フォルダＵＲＬ６２（１９２．１６８．０．２／ｃｏｍｍｏｎ）は、ＰＣ４０の共有フォルダ５０に対応する。記憶領域５２は、様々な情報を記憶することができる。

【００３１】

ネットワークインターフェイス５４は、通信回線３６に接続されている。ＰＣ４０は、ネットワークインターフェイス５４及び通信回線３６を介して、スキャナ１０と通信可能である。

【００３２】

（ＳＣＡＮ　ＴＯ処理）

続いて、スキャナ１０が実行する処理の内容について説明する。以下の各処理は、スキャナ１０の制御装置２０によって実行される。図５～図８は、スキャナ１０のＳＣＡＮ　ＴＯ処理のフローチャートを示す。ユーザは、スキャナ１０の操作装置１２を操作することによって、ＳＣＡＮ　ＴＯをスタートすることを指示することができる。制御装置２０は、ＳＣＡＮ　ＴＯをスタートすることが指示されることを監視している（Ｓ１０）。ここでＹＥＳの場合、制御装置２０は、スキャンの対象となる原稿が原稿トレイ１８に載置されているのか否かを判断する（Ｓ１２）。制御装置２０は、原稿トレイ１８に原稿が載置されるまで待機する。

【００３３】

Ｓ１２でＹＥＳの場合、制御装置２０は、スキャンデータのデータ形式及び送信先が指定されるまで待機する（Ｓ１４）。ユーザは、操作装置１２を操作することによって、スキャンデータのデータ形式を指定することができる。具体的には、ユーザは、以下の３つの項目のそれぞれについて具体的な形式を指定することができる。まず、ユーザは、スキャンデータの解像度を指定することができる。ユーザは、１つの解像度のみを指定することもできるし、複数の解像度を指定することもできる。また、ユーザは、スキャンデータの色彩情報（カラー、グレースケール、白黒）を指定することができる。ユーザは、１つの色彩情報のみを指定することもできるし、複数の色彩情報を指定することもできる。また、ユーザは、ＰＤＦ、ＴＩＦＦ、ＪＰＥＧ等の中からファイル形式を指定することができる。ユーザは、１つのファイル形式のみを指定することもできるし、複数のファイル形式を指定することもできる。上記の３つの項目のそれぞれがユーザによって指定された場合、制御装置２０は、ユーザによって指定されたデータ形式を記憶領域３０に記憶する。

【００３４】

また、ユーザは、操作装置１２を操作することによって、送信先デバイスＵＲＬ記憶領域２４（図２参照）に記憶されている複数の組合せデータ７０，７２の中から少なくとも１つの組合せデータを指定することができる。これにより、スキャンデータの送信先が指定されることになる。制御装置２０は、ユーザによって指定された組合せデータ（即ち送信先に関する情報）を記憶領域３０に記憶する。スキャンデータのデータ形式及び送信先が指定されると、Ｓ１６に進む。

【００３５】

ユーザは、操作装置１２を操作することによって、スキャンをスタートすることを指示することができる。Ｓ１６では、制御装置２０は、スキャンをスタートすることが指示されることを監視している。ここでＹＥＳの場合、制御装置２０は、Ｓ１４で指定された組合せデータに含まれる暗号化情報６６が「ＹＥＳ」であるのか否かを判断する（Ｓ１８）

。例えば、図２の例では、組合せデータ７０の暗号化情報６６は「ＹＥＳ」である。従って、Ｓ１４で指定された組合せデータが組合せデータ７０である場合、Ｓ１８でＹＥＳと判断される。この場合、Ｓ２０に進む。一方において、図２の例では、組合せデータ７２の暗号化情報６６は「ＮＯ」である。従って、Ｓ１４で指定された組合せデータが組合せデータ７２である場合、Ｓ１８でＮＯと判断される。この場合、Ｓ２０をスキップする。

【００３６】

Ｓ２０では、制御装置２０は、パスワードを生成して表示する。例えば、制御装置２０は、複数の数字の中からランダムに１つの数字を選択し、選択された数字を含むパスワードを生成してもよい。また、例えば、制御装置２０は、前回のＳ２０の処理においてパスワードとして作成された数字をインクリメントすることによって新たなパスワードを生成してもよい。制御装置２０は、生成されたパスワードを表示装置１４に表示する。これにより、ユーザは、パスワードを知ることができる。なお、パスワードは、別の手法によって出力されてもよい。例えば、音声出力されてもよいし、印刷されてもよいし、他のデバイス（例えばユーザの携帯電話等）に送信されてもよい。制御装置２０は、Ｓ２０で作成されたパスワードを記憶領域３０に記憶する。

【００３７】

次いで、制御装置２０は、スキャンデータ記憶領域２６にフォルダを作成する（Ｓ２２）。具体的に言うと、制御装置２０は、フォルダ名を作成する。本実施例では、制御装置２０は、前回のＳ２２の処理において作成されたフォルダ名（ｓｃａｎ＋４桁の数字）に含まれる数字に「１」をインクリメントすることによって、フォルダ名を作成する。例えば、前回のＳ２２の処理において作成されたフォルダ名が図３のフォルダ名９０ａである場合、制御装置２０は、「ｓｃａｎ０００３」というフォルダ名を作成する。Ｓ２２を終えると、Ｓ２４に進む。

【００３８】

Ｓ２４では、制御装置２０は、Ｓ２２で作成されたフォルダの下位ファイルを作成する。具体的に言うと、制御装置２０は、ファイル名を作成する。このファイル名は、スキャンデータファイルのファイル名として使用される。制御装置２０は、現在の日時を示す文字列と、拡張子を示す文字列（．ｂｉｎ）とを含むファイル名（図３のファイル名８２ａ，９４ａ，９６ａ参照）を作成する。なお、Ｓ２４の段階では、スキャンデータはまだ作成されていない。

【００３９】

次いで、制御装置２０は、原稿トレイ１８に原稿が載置されているのか否かを判断する（Ｓ２６）。ここでＹＥＳの場合、制御装置２０は、スキャン装置１６を駆動し、１枚の原稿をスキャンする（Ｓ２８）。制御装置２０は、Ｓ１４で指定されたデータ形式に基づいて、具体的なスキャンの手法を決定する。例えば、Ｓ１４で指定されたデータ形式において、解像度が「１５０ｄｐｉ」であり、色彩情報が「カラー」であり、ファイル形式が「ＰＤＦ」である場合、制御装置２０は、１５０ｄｐｉの解像度でカラースキャンを実行させる。しかも、制御装置２０は、後述するＳ３２の処理において、ＰＤＦのファイル形式を利用してスキャンデータファイルを作成する（ただしＳ２４で作成されるファイル名の拡張子は「．ｂｉｎ」を採用する）。また、例えば、Ｓ１４において、複数の解像度、及び／又は、複数の色彩情報、及び／又は、複数のファイル形式が指定された場合、制御装置２０は、全ての組合せのデータ形式のスキャンデータを作成するためのベースとなるスキャンデータを作成する。即ち、制御装置２０は、全ての組合せのいずれにでも変換可能であるデータ形式を有するスキャンデータを作成する。例えば、Ｓ１４において、Ｌ個の解像度が指定され、Ｍ個の色彩情報が指定され、Ｎ個のファイル形式が指定された場合、制御装置２０は、Ｌ×Ｍ×Ｎ個の全ての組合せのデータ形式のスキャンデータを作成するためのベースとなるスキャンデータを作成する。例えば、複数の解像度が指定されている場合、制御装置２０は、大きい解像度を利用してスキャンデータを作成する。また、例えば、複数の色彩情報が指定された場合、制御装置２０は、大きい色数を利用してスキャンデータを作成する。例えば、カラーとグレースケールと白黒が指定されている場合、制

御装置２０は、カラースキャンを実行する。また、例えば、複数のファイル形式が指定されている場合、制御装置２０は、それらの各ファイル形式に変換可能な１つのファイル形式を利用してスキャンデータファイルを作成する。

【００４０】

ユーザは、スキャン対象の複数枚の原稿の中にセパレータ用紙を挿入することができる。セパレータ用紙は、スキャン対象と区別することができる用紙であれば、どのようなタイプの用紙であってもよい。本実施例では、全面が黒色の用紙をセパレータ用紙として採用している。制御装置２０は、Ｓ２８で得られたスキャンデータに基づいて、スキャン対象がセパレータ用紙であるのか否かを判断する（Ｓ３０）。ここでＮＯの場合、制御装置２０は、Ｓ２８で得られたスキャンデータをスキャンデータ記憶領域２６に記憶する（Ｓ３２）。制御装置２０は、Ｓ２４で作成されたファイル名にスキャンデータを対応づける。Ｓ３２を終えると、制御装置２０は、Ｓ２６に戻って、次の原稿が存在するのか否かを判断する。次の原稿が存在する場合、制御装置２０は、当該原稿をスキャンする（Ｓ２８）。当該原稿がセパレータ用紙でない場合（Ｓ３０でＮＯの場合）、制御装置２０は、Ｓ２８で得られたスキャンデータを記憶する（Ｓ３２）。このスキャンデータは、前回のＳ３２の処理で記憶されたスキャンデータに続く形式で記憶される。即ち、本実施例では、１つのスキャンデータファイルが、複数枚の原稿のスキャンデータを含むことができる。

【００４１】

一方において、Ｓ３０でＹＥＳの場合、制御装置２０は、Ｓ２４で作成されたスキャンデータファイルをクローズする（Ｓ３４）。この場合、制御装置２０は、Ｓ２４に戻って、Ｓ２２で作成されたフォルダの下位ファイルを新たに作成する。即ち、Ｓ３４を経てＳ２４が実行されると、１つのフォルダの下位ファイルとして複数のスキャンデータファイルが作成されることになる。例えば、図３の例において、フォルダ９０は、複数のスキャンデータファイル９４，９６を格納している。これは、Ｓ３４を経てＳ２４が実行されたことを意味している。逆に言うと、Ｓ３４を経てＳ２４が実行されなければ、１つのフォルダの下位ファイルとして１つのスキャンデータファイルのみが作成される。例えば、図３の例において、フォルダ８０は、１つのスキャンデータファイル８２のみを格納している。これは、Ｓ３４を経てＳ２４が実行されなかったことを意味している。

【００４２】

原稿トレイ１８に載置されていた全ての原稿がスキャンされると、制御装置２０は、Ｓ２６でＮＯと判断する。この場合、制御装置２０は、Ｓ２４で作成されたスキャンデータファイルをクローズする（Ｓ３６）。次いで、図６のＳ５０に進む。Ｓ５０では、制御装置２０は、ＨＴＴＰＳを使用可能であるのか否かを判断する。ユーザは、ＨＴＴＰＳを使用する場合、そのための設定をスキャナ１０に予め登録しておく。この場合、Ｓ５０でＹＥＳと判断され、Ｓ５２に進む。一方において、ＨＴＴＰＳの設定が登録されていない場合、Ｓ５０でＮＯと判断される。この場合、図７のＳ８０に進む。

【００４３】

Ｓ５２では、制御装置２０は、図５のＳ２２で作成されたフォルダ内に複数のスキャンデータファイルが格納されているのか否かを判断する。例えば、図５のＳ２２で作成されたフォルダが図３のフォルダ８０である場合、制御装置２０は、Ｓ５２でＮＯと判断する。フォルダ８０は、１つのスキャンデータファイル８２のみを格納しているからである。Ｓ５２でＮＯの場合、制御装置２０は、ＵＲＬとサムネイル画像を含むＨＴＭＬファイルを作成する（Ｓ５４）。図６のフローチャートには、Ｓ５４で作成されるＵＲＬ１２０の一例が示されている。ＵＲＬ１２０は、ＨＴＴＰＳの通信プロトコルを示すスキーム文字列１２０ａと、スキャナ１０のホスト名１２０ｂと、図５のＳ２２で作成されたフォルダ名１２０ｃと、図５のＳ２４で作成されたファイル名１２０ｄと、データ形式を示すデータ形式文字列１２０ｅとを含んでいる。データ形式文字列１２０ｅは、図５のＳ１４においてユーザによって指定されたデータ形式を特定する文字列である。例えば、図５のＳ１４で指定されたデータ形式において、解像度が「１５０ｄｐｉ」であり、色彩情報が「カラー」であり、ファイル形式が「ＰＤＦ」である場合、制御装置２０は、「ｃ１５０．ｐ

ｄｆ」というデータ形式文字列１２０ｅを作成する。

【００４４】

なお、上述したように、図５のＳ１４において、ユーザは、複数の解像度、及び／又は、複数の色彩情報、及び／又は、複数のファイル形式を指定することができる。この場合、制御装置２０は、全ての組合せのそれぞれについて、当該組合せのデータ形式を特定する文字列１２０ｅを含むＵＲＬ１２０を作成する。例えば、図５のＳ１４において、Ｌ個の解像度が指定され、Ｍ個の色彩情報が指定され、Ｎ個のファイル形式が指定された場合、制御装置２０は、Ｌ×Ｍ×Ｎ個のＵＲＬ１２０を作成する。例えば、図５のＳ１４で指定されたデータ形式において、解像度が「１５０ｄｐｉ」と「３００ｄｐｉ」であり、色彩情報が「カラー」と「グレースケール」であり、ファイル形式が「ＰＤＦ」である場合、制御装置２０は、「ｃ１５０．ｐｄｆ」を含むＵＲＬと、「ｃ３００．ｐｄｆ」を含むＵＲＬと、「ｇ１５０．ｐｄｆ」を含むＵＲＬと、「ｇ３００．ｐｄｆ」を含むＵＲＬとを作成する。なお、これらの各ＵＲＬでは、他の文字列１２０ａ～１２０ｄは共通している。

【００４５】

また、制御装置２０は、図５のＳ２４で作成されたスキャンデータファイルに含まれる１ページ目のスキャンデータに基づいてサムネイル画像を作成する。サムネイル画像は、スキャンデータより解像度が低い画像データである。制御装置２０は、ＵＲＬ１２０に含まれるデータ形式（データ形式文字列１２０ｅ）が反映されたサムネイル画像を作成する。例えば、制御装置２０は、データ形式文字列１２０ｅに含まれる解像度の大きさに応じて、サムネイル画像の大きさを変える。また、例えば、制御装置２０は、データ形式文字列１２０ｅに含まれる色彩情報（カラー、グレースケール、白黒）に応じて、サムネイル画像の色彩を決定する。なお、上述したように、複数のＵＲＬ１２０が作成されることがある。この場合、制御装置２０は、複数のＵＲＬ１２０のそれぞれについて、当該ＵＲＬ１２０のデータ形式文字列１２０ｅが反映されたサムネイル画像を作成する。即ち、制御装置２０は、複数のサムネイル画像を作成する。制御装置２０は、上記のようにして作成されたＵＲＬ１２０とサムネイル画像とを含むＨＴＭＬファイルを作成する。上述したように、ＨＴＭＬファイルは、複数のＵＲＬ１２０と複数のサムネイル画像を含む場合もある。制御装置２０は、ＨＴＭＬファイルを記憶領域３０に記憶する。なお、実際には、ＨＴＭＬファイルは、サムネイル画像自体は含まず、サムネイル画像のリンク先のＵＲＬを含んでいる。本実施例では、このような構成であっても、「ＨＴＭＬファイルがサムネイル画像を含んでいる」と表現する。Ｓ５４を終えると、Ｓ６０に進む。

【００４６】

例えば、図５のＳ２２で作成されたフォルダが図３のフォルダ９０である場合、制御装置２０は、Ｓ５２でＹＥＳと判断する。フォルダ９０は、複数のスキャンデータファイル９４，９６を格納しているからである。Ｓ５２でＹＥＳの場合、制御装置２０は、ＵＲＬを含む（サムネイル画像は含まない）ＨＴＭＬファイルを作成する（Ｓ５６）。図６のフローチャートには、Ｓ５６で作成されるＵＲＬ１３０の一例が示されている。ＵＲＬ１３０は、ＨＴＴＰＳの通信プロトコルを示すスキーム文字列１３０ａと、スキャナ１０のホスト名１３０ｂと、図５のＳ２２で作成されたフォルダ名１３０ｃとを含んでいる。Ｓ５６で作成されるＵＲＬ１３０は、Ｓ５４で作成されるＵＲＬ１２０と異なり、ファイル名とデータ形式文字列を含んでいない。制御装置２０は、上記のようにして作成されたＵＲＬ１３０を含むＨＴＭＬファイルを作成する。制御装置２０は、ＨＴＭＬファイルを記憶領域３０に記憶する。Ｓ５６を終えると、Ｓ５８に進む。

【００４７】

Ｓ５８では、制御装置２０は、データ形式ファイルを作成する。このデータ形式ファイルは、図５のＳ２２で作成されたフォルダの下位ファイルとして作成される。図３には、データ形式ファイルの一例が示されている（符号９２参照）。制御装置２０は、ファイル名「ｄａｔａｆｏｒｍａｔ．ｄｏｃ」を作成する（図３の例の符号９２ａ参照）。また、制御装置２０は、図５のＳ１４において指定されたデータ形式が記述されたドキュメント

データを作成する（図３の例の符号９２ｄ参照）。図５のＳ１４において指定されたデータ形式が１つの組合せである場合、ドキュメントデータは、当該組合せのデータ形式を示す文字列を含んでいる。一方において、図５のＳ１４において指定されたデータ形式が複数の組合せを有する場合、ドキュメントデータは、各組合せのデータ形式を示す文字列を含んでいる。データ形式ファイルがどのようにして利用されるのかについては、後で詳しく説明する。Ｓ５８を終えると、Ｓ６０に進む。

【００４８】

Ｓ６０では、制御装置２０は、図５のＳ１４において指定された送信先に向けて、Ｓ５４又はＳ５６で作成されたＨＴＭＬファイルを送信する。上述したように、図２の組合せデータ７０に含まれる共有フォルダＵＲＬ６２（１９２．１６８．０．２／ｃｏｍｍｏｎ）は、ＰＣ４０の共有フォルダ５０に対応する。従って、例えば、図５のＳ１４において図２の組合せデータ７０が指定された場合、制御装置２０は、Ｓ５４又はＳ５６において作成されたＨＴＭＬファイルと、そのＨＴＭＬファイルを共有フォルダ５０内に格納することを指示するコマンドとをＰＣ４０（即ちＩＰアドレス「１９２．１６８．０．２」）に向けて送信する。これにより、ＰＣ４０の共有フォルダ５０内にＨＴＭＬファイルが格納される。この結果、ＰＣ４０のユーザは、共有フォルダ５０内に格納されているＨＴＭＬファイルを見ることができる。Ｓ５４で作成されたＨＴＭＬファイルの場合、ユーザは、ＵＲＬ１２０とサムネイル画像とを見ることができる。Ｓ５６で作成されたＨＴＭＬファイルの場合、ユーザは、ＵＲＬ１３０を見ることができる。

【００４９】

次いで、制御装置２０は、対応情報記憶領域２８の記憶内容を更新する（Ｓ６２）。具体的に言うと、制御装置２０は、１つの対応情報を対応情報記憶領域２８に記憶する。即ち、制御装置２０は、ＩＤ１００と、図５のＳ２２で作成されたフォルダ名を含むＵＲＬ１０２と、図５のＳ１４で指定された送信先１０４（ＨＴＭＬファイルの送信先のＩＰアドレス）と、Ｓ２０で生成されたパスワード１０６とが対応づけられている対応情報を対応情報記憶領域２８に記憶する。なお、制御装置２０は、前回のＳ６２の処理で作成されたＩＤに「１」をインクリメントすることによって、ＩＤ１００を作成する。上述したように、図５のＳ１８でＮＯと判断された場合、パスワードが作成されない。この場合、Ｓ６２においてパスワードは記憶されない。Ｓ６２を終えると、ＳＣＡＮ　ＴＯ処理が終了する。

【００５０】

続いて、図６のＳ５０でＮＯと判断された後のフローチャートについて説明する。即ち、ＨＴＴＰＳを使用不可能であってＨＴＴＰを使用する場合のフローチャートについて説明する。Ｓ５０でＮＯの場合、図７のＳ８０に進む。Ｓ８０では、制御装置２０は、図５のＳ２２で作成されたフォルダ内に複数のスキャンデータファイルが格納されているのか否かを判断する。この処理は、図６のＳ５２と同様である。例えば、図５のＳ２２で作成されたフォルダが図３のフォルダ８０である場合、制御装置２０は、Ｓ８０でＮＯと判断する。この場合、制御装置２０は、図５のＳ２０でパスワードが生成されたのか否かを判断する（Ｓ８２）。図５のＳ１８でＮＯと判断された場合、図５のＳ２０がスキップされてパスワードが生成されない。この場合、Ｓ８２でＮＯと判断され、Ｓ８４に進む。一方において、図５のＳ１８でＹＥＳと判断された場合、図５のＳ２０が実行されてパスワードが生成される。この場合、Ｓ８２でＹＥＳと判断され、Ｓ８６に進む。

【００５１】

Ｓ８４では、制御装置２０は、ＵＲＬとサムネイル画像を含むＨＴＭＬファイルを作成する。図７のフローチャートには、Ｓ８４で作成されるＵＲＬ１４０の一例が示されている。ＵＲＬ１４０は、ＨＴＴＰの通信プロトコルを示すスキーム文字列１４０ａと、スキャナ１０のホスト名１４０ｂと、図５のＳ２２で作成されたフォルダ名１４０ｃと、図５のＳ２４で作成されたファイル名１４０ｄと、データ形式を示すデータ形式文字列１４０ｅとを含んでいる。データ形式文字列１４０ｅは、図５のＳ１４においてユーザにおいて指定されたデータ形式を特定する文字列であり、図６のＳ５４の場合と同様の手法によっ

て作成される。制御装置２０は、ＨＴＭＬファイルを記憶領域３０に記憶する。Ｓ８４を終えると、図６のＳ６０に進む。即ち、制御装置２０は、図５のＳ１４で指定された送信先に向けて、Ｓ８４で作成されたＨＴＭＬファイルを送信する。さらに、制御装置２０は、対応情報記憶領域２８の記憶内容を更新する（Ｓ６２）。

【００５２】

Ｓ８６では、制御装置２０は、図５のＳ２４で作成されたスキャンデータファイルに基づいてＺＩＰファイルを作成する。制御装置２０は、図５のＳ２０で生成されたパスワードを暗号化キーとしてＺＩＰファイルを作成する。例えば、図５のＳ１４で指定されたデータ形式が１つの組合せである場合、制御装置２０は、図５のＳ２４で作成されたスキャンデータファイルをＺＩＰファイルに変換する。また、例えば、図５のＳ１４で指定されたデータ形式が複数の組合せである場合、制御装置２０は、各組合せについてＺＩＰファイルを作成する。例えば、図５のＳ１４で指定されたデータ形式において、解像度が「１５０ｄｐｉ」と「３００ｄｐｉ」であり、色彩情報が「カラー」と「グレースケール」であり、ファイル形式が「ＰＤＦ」である場合、制御装置２０は、図５のＳ２４で作成されたスキャンデータファイルに含まれるスキャンデータを変換することによって、カラーの１５０ｄｐｉのＰＤＦファイルと、カラーの３００ｄｐｉのＰＤＦファイルと、グレースケールの１５０ｄｐｉのＰＤＦファイルと、グレースケールの３００ｄｐｉのＰＤＦファイルとを作成する。次いで、制御装置２０は、各ＰＤＦファイルからＺＩＰファイルを作成する。この例の場合、４つのＺＩＰファイルが作成されることになる。これらのＺＩＰファイルのファイル名は、例えば、「．ｐｄｆ．ｚｉｐ」のように、図５のＳ１４で指定されたファイル形式のＺＩＰファイルであることを示す文字列を含んでいる。制御装置２０は、Ｓ８６で作成されたＺＩＰファイルを、図５のＳ２２で作成されたフォルダの下位ファイルとして記憶する。

【００５３】

次いで、制御装置２０は、ＵＲＬとサムネイル画像を含むＨＴＭＬファイルを作成する（Ｓ８８）。図７のフローチャートには、Ｓ８８で作成されるＵＲＬ１５０の一例が示されている。ＵＲＬ１５０は、ＨＴＴＰの通信プロトコルを示すスキーム文字列１５０ａと、スキャナ１０のホスト名１５０ｂと、図５のＳ２２で作成されたフォルダ名１５０ｃと、図５のＳ２４で作成されたファイル名１５０ｄと、データ形式を示すデータ形式文字列１５０ｅとを含んでいる。データ形式文字列１５０ｅは、図５のＳ１４においてユーザにおいて指定されたデータ形式を特定する文字列であり、図６のＳ５４の場合と同様の手法によって作成される。但し、Ｓ８８で作成されるデータ形式文字列１５０ｅは、ＺＩＰファイルの拡張子を示す文字列１５０ｆを含んでいる。この点は、図６のＳ５４の場合と異なる。また、制御装置２０は、図６のＳ５４の場合と同じ手法を利用してサムネイル画像を作成する。制御装置２０は、ＨＴＭＬファイルを記憶領域３０に記憶する。Ｓ８８を終えると、図６のＳ６０に進む。即ち、制御装置２０は、図５のＳ１４で指定された送信先に向けて、Ｓ８８で作成されたＨＴＭＬファイルを送信する。さらに、制御装置２０は、対応情報記憶領域２８の記憶内容を更新する（Ｓ６２）。

【００５４】

例えば、図５のＳ２２で作成されたフォルダが図３のフォルダ９０である場合、制御装置２０は、Ｓ８０でＹＥＳと判断する。この場合、図８のＳ１００に進む。Ｓ１００では、制御装置２０は、図５のＳ２０でパスワードが生成されたのか否かを判断する。Ｓ１００でＮＯの場合はＳ１０２に進み、Ｓ１００でＹＥＳの場合はＳ１０６に進む。

【００５５】

Ｓ１０２では、制御装置２０は、ＵＲＬを含む（サムネイル画像は含まない）ＨＴＭＬファイルを作成する。図８のフローチャートには、Ｓ１０２で作成されるＵＲＬ１６０の一例が示されている。ＵＲＬ１６０は、ＨＴＴＰの通信プロトコルを示すスキーム文字列１６０ａと、スキャナ１０のホスト名１６０ｂと、図５のＳ２２で作成されたフォルダ名１６０ｃとを含んでいる。Ｓ１０２で作成されるＵＲＬ１６０は、ファイル名とデータ形式文字列を含んでいない。制御装置２０は、上記のようにして作成されたＵＲＬ１６０を

含むＨＴＭＬファイルを作成する。制御装置２０は、ＨＴＭＬファイルを記憶領域３０に記憶する。Ｓ１０２を終えると、制御装置２０は、データ形式ファイルを作成する（Ｓ１０４）。この処理は、図６のＳ５８と同様である。Ｓ１０４を終えると、図６のＳ６０に進む。即ち、制御装置２０は、図５のＳ１４で指定された送信先に向けて、Ｓ１０２で作成されたＨＴＭＬファイルを送信する。さらに、制御装置２０は、対応情報記憶領域２８の記憶内容を更新する（Ｓ６２）。

【００５６】

Ｓ１０６では、制御装置２０は、図５のＳ２４で作成された複数のスキャンデータファイルに基づいてＺＩＰファイルを作成する。制御装置２０は、図５のＳ２０で生成されたパスワードを暗号化キーとしてＺＩＰファイルを作成する。例えば、図５のＳ１４で指定されたデータ形式が１つの組合せであり、図３のスキャンデータファイル９４，９６が作成された場合、スキャンデータファイル９４，９６のそれぞれをＺＩＰファイルに変換する。この場合、２つのＺＩＰファイルが作成される。また、例えば、図５のＳ１４で指定されたデータ形式が複数の組合せである場合、各組合せについてＺＩＰファイルを作成する。例えば、図５のＳ１４で指定されたデータ形式が４つの組合せであり、図３のスキャンデータファイル９４，９６が作成された場合、８つのＺＩＰファイルが作成される。これらのＺＩＰファイルの各ファイル名は、例えば、「．ｔｉｆｆ．ｚｉｐ」のように、図５のＳ１４で指定されたファイル形式のＺＩＰファイルであることを示す文字列を含んでいる。制御装置２０は、Ｓ１０６で作成されたＺＩＰファイルを、図５のＳ２２で作成されたフォルダの下位ファイルとして記憶する。

【００５７】

次いで、制御装置２０は、ＵＲＬを含む（サムネイル画像は含まない）ＨＴＭＬファイルを作成する（Ｓ１０８）。図８のフローチャートには、Ｓ１０８で作成されるＵＲＬ１７０の一例が示されている。ＵＲＬ１７０は、ＨＴＴＰの通信プロトコルを示すスキーム文字列１７０ａと、スキャナ１０のホスト名１７０ｂと、図５のＳ２２で作成されたフォルダ名１７０ｃとを含んでいる。制御装置２０は、上記のようにして作成されたＵＲＬ１７０を含むＨＴＭＬファイルを作成する。制御装置２０は、ＨＴＭＬファイルを記憶領域３０に記憶する。Ｓ１０８を終えると、制御装置２０は、データ形式ファイルを作成する（Ｓ１１０）。この処理は、図６のＳ５８と同様である。Ｓ１１０を終えると、図６のＳ６０に進む。即ち、制御装置２０は、図５のＳ１４で指定された送信先に向けて、Ｓ１０８で作成されたＨＴＭＬファイルを送信する。さらに、制御装置２０は、対応情報記憶領域２８の記憶内容を更新する（Ｓ６２）。

【００５８】

（スキャンデータ提供処理）

続いて、スキャナ１０のスキャンデータ提供処理について説明する。図９及び図１０は、スキャナ１０のスキャンデータ提供処理のフローチャートを示す。上述したように、図６のＳ６０では、図５のＳ１４で指定された送信先に向けてＨＴＭＬファイルが送信される。ここでは、ＰＣ４０の共有フォルダ５０に向けてＨＴＭＬファイルが送信されたものとする。これにより、共有フォルダ５０内にＨＴＭＬファイルが格納される。ＰＣ４０のユーザは、操作装置４２を操作することによって、共有フォルダ５０内に格納されているＨＴＭＬファイルをオープンすることができる。この場合、ＨＴＭＬファイルに記述されているＵＲＬ（図６のＳ５４、図６のＳ５６、図７のＳ８４、図７のＳ８８、図８のＳ１０２、又は、図８のＳ１０８で作成されたＵＲＬ）が表示装置４４に表示される。ユーザは、操作装置４２を操作することによって、ＵＲＬを指定することができる。この場合、アクセスリクエストがスキャナ１０に送信される。このアクセスリクエストは、ユーザによって指定されたＵＲＬと、ＰＣ４０のＩＰアドレス（１９２．１６８．０．２（図２参照））とを含んでいる。このアクセスリクエストは、ユーザによって指定されたＵＲＬに含まれるスキーム文字列（図６のＳ５４の符号１２０ａ等）によって特定される通信プロトコルを利用して送信される。例えば、ユーザによって指定されたＵＲＬが図６のＳ５４のＵＲＬ１２０であった場合、ＨＴＴＰＳを利用してアクセスリクエストが送信される。

また、例えば、ユーザによって指定されたＵＲＬが図７のＳ８４のＵＲＬ１４０であった場合、ＨＴＴＰを利用してアクセスリクエストが送信される。スキャナ１０の制御装置２０は、ＰＣ４０から送信されたアクセスリクエストを受信することを監視している（Ｓ１３０）。ここでＹＥＳの場合、Ｓ１３２に進む。

【００５９】

Ｓ１３２では、制御装置２０は、アクセスリクエストに含まれるＵＲＬ（即ちアクセス先）が対応情報記憶領域２８に記憶されているのか否かを判断する。なお、Ｓ１３２でＹＥＳと判断された対応情報のことを、以下では「特定対応情報」と呼ぶ。ここでＹＥＳの場合、制御装置２０は、特定対応情報のＵＲＬ１０２（図４参照）に含まれるスキーム文字列（ｈｔｔｐ又はｈｔｔｐｓ）と、アクセスリクエストの通信プロトコルとが一致しているのか否かを判断する（Ｓ１３４）。ここでＹＥＳの場合、制御装置２０は、特定対応情報の送信先１０４（図４参照）と、アクセスリクエストに含まれるＩＰアドレスとが一致するのか否かを判断する（Ｓ１３６）。ここでＹＥＳの場合、Ｓ１４０に進む。一方において、Ｓ１３２、Ｓ１３４、又は、Ｓ１３６でＮＯの場合、制御装置２０は、エラーレスポンスをＰＣ４０に送信する（Ｓ１３８）。

【００６０】

Ｓ１４０では、制御装置２０は、アクセスリクエストの通信プロトコルがＨＴＴＰＳであるのか否かを判断する。アクセスリクエストの通信プロトコルがＨＴＴＰである場合、Ｓ１４０でＮＯと判断される。この場合、図１０のＳ１６０に進む。一方において、Ｓ１４０でＹＥＳの場合、Ｓ１４２に進む。Ｓ１４２では、制御装置２０は、特定対応情報にパスワード１０６（図４参照）が含まれるのか否かを判断する（Ｓ１４２）。ここでＹＥＳの場合、制御装置２０は、特定対応情報に含まれるパスワードと、アクセスリクエストに含まれるパスワードパラメータとが一致するのか否かを判断する（Ｓ１４４）。パスワードパラメータにパスワードが記述されていない場合は、Ｓ１４４でＮＯと判断される。この場合、制御装置２０は、パスワード入力画面データをＰＣ４０に送信する。ＰＣ４０は、パスワード入力画面を表示する。ユーザは、ＰＣ４０の操作装置４２を操作することによって、パスワードを入力することができる。これにより、ユーザによって入力されたパスワードを含むアクセスリクエストがスキャナ１０に送信される。このアクセスリクエストにも、ユーザによって指定されたＵＲＬと、ＰＣ４０のＩＰアドレス（１９２．１６８．０．２（図２参照））とが含まれる。この結果、Ｓ１３０～Ｓ１４２を経てＳ１４４が再び実行される。このＳ１４４において、特定対応情報に含まれるパスワードと、アクセスリクエストに含まれるパスワードパラメータとが一致すると（Ｓ１４４でＹＥＳ）、図１０のＳ１６０に進む。なお、Ｓ１４２でＮＯと判断された場合も、図１０のＳ１６０に進む。

【００６１】

Ｓ１６０では、制御装置２０は、アクセスリクエストに含まれるＵＲＬが、フォルダのＵＲＬであるのか、あるいは、ファイルのＵＲＬであるのかを判断する。例えば、図６のＳ５４で作成されたＵＲＬ１２０がＰＣ４０のユーザによって指定された場合、アクセスリクエストにファイルのＵＲＬ１２０が含まれる。この場合、図１０のＳ１６０でＮＯと判断され、Ｓ１６４に進む。また、例えば、図６のＳ５６で作成されたＵＲＬ１３０がＰＣ４０のユーザによって指定された場合、アクセスリクエストにフォルダのＵＲＬ１３０が含まれる。この場合、図１０のＳ１６０でＹＥＳと判断され、Ｓ１６２に進む。

【００６２】

Ｓ１６２では、制御装置２０は、アクセスリクエストに含まれるＵＲＬ（フォルダのＵＲＬ）の下位ファイルとして存在するファイル群を特定する。例えば、アクセスリクエストに含まれるＵＲＬが図３のフォルダ９０のＵＲＬである場合、制御装置２０は、データ形式ファイル９２と各スキャンデータファイル９４，９６を特定する。なお、以下では、ここで特定されたデータ形式ファイルのことを「特定データ形式ファイル」と呼ぶ。また、ここで特定されたスキャンデータファイルのことを「特定スキャンデータファイル」と呼ぶ。制御装置２０は、特定データ形式ファイルと特定スキャンデータファイルとに基づ

いてＵＲＬを作成する。

【００６３】

図１０のフローチャートには、Ｓ１６２で作成されるＵＲＬ１８０の一例が示されている。ＵＲＬ１８０は、特定対応情報のＵＲＬ１０２（図４参照）に含まれるスキーム文字列１８０ａと、特定対応情報のＵＲＬ１０２に含まれるスキャナ１０のホスト名１８０ｂと、特定対応情報のＵＲＬ１０２に含まれるフォルダ名１８０ｃと、特定スキャンデータファイルのファイル名１８０ｄと、データ形式文字列とを含んでいる。データ形式文字列は、特定データ形式ファイルのドキュメントデータ（例えば図３の符号９２）に記述されているデータ形式に基づいて作成される。例えば、データ形式ファイルのドキュメントデータに複数のデータ形式の組合せが記述されている場合、その組合せ数のＵＲＬが１つの特定スキャンデータファイルについて作成される。例えば、図３のスキャンデータファイル９４，９６が特定スキャンデータファイルであり、図３のデータ形式ファイル９２のドキュメントデータ９２ｄに３つのデータ形式の組合せが記述されている場合、制御装置２０は、６つのＵＲＬを作成する。即ち、制御装置２０は、スキャンデータファイル９４のファイル名９４ｂ（２００８０１０１－０１０２００）を含む３つのＵＲＬを作成するとともに、スキャンデータファイル９６のファイル名９６ｂ（２００８０１０１－０１０３００）を含む３つのＵＲＬを作成する。前者の３つのＵＲＬは、異なるデータ形式文字列を含んでいる。また、後者の３つのＵＲＬは、異なるデータ形式文字列を含んでいる。なお、図８のＳ１０６では、複数のＺＩＰファイルが作成され、それらのＺＩＰファイルのＵＲＬが作成されている。このために、図８のＳ１０８で作成されたＵＲＬ１７０がＰＣ４０のユーザによって選択された場合、制御装置２０は、Ｓ１６２の処理においてＵＲＬを作成する必要がなく、各ＺＩＰファイルのＵＲＬを引用する。なお、アクセスリクエストに含まれるＵＲＬが、図８のＳ１０８で作成されたフォルダのＵＲＬ１７０であるのか、あるいは、それ以外のフォルダのＵＲＬ１３０，１６０（図６のＳ５６、図８のＳ１０２参照）であるのかは、アクセスリクエストに含まれるＵＲＬ（即ちフォルダ）の下位ファイルとしてＺＩＰファイル（図８のＳ１０６で作成されたＺＩＰファイル）が存在するのか否かに基づいて判断することができる。

【００６４】

制御装置２０は、上記の作成された各ＵＲＬについて、サムネイル画像を作成する。サムネイル画像を作成するための手法は、図６のＳ５４と同様である。次いで、制御装置２０は、上記の作成された各ＵＲＬと各サムネイル画像とをＰＣ４０に送信する。ＰＣ４０は、各ＵＲＬと各サムネイル画像を表示する。ユーザは、ＰＣ４０の操作装置４２を操作することによって、ＵＲＬを選択することができる。これにより、ユーザによって選択されたＵＲＬを含むアクセスリクエストがスキャナ１０に送信される。

【００６５】

Ｓ１６４では、制御装置２０は、アクセスリクエストに含まれるＵＲＬがＺＩＰファイルのＵＲＬであるのか否かを判断する。この処理は、アクセスリクエストに含まれるＵＲＬに「．ｚｉｐ」の文字列が含まれるのか否かを判断することによって行なわれる。ここでＹＥＳの場合、制御装置２０は、アクセスリクエストに含まれるＵＲＬに対応するＺＩＰファイル（即ちスキャンデータ）と、そのＺＩＰファイルを共有フォルダ５０内に格納することを指示するコマンドとをＰＣ４０に送信する。なお、このコマンドで指示される共有フォルダ５０のＵＲＬは、アクセスリクエストに含まれるＩＰアドレスに対応づけて送信先デバイスＵＲＬ記憶領域２４に記憶されている。このために、制御装置２０は、共有フォルダのＵＲＬを特定することができる。

【００６６】

Ｓ１６６が実行されると、ＰＣ４０の共有フォルダ５０にＺＩＰファイルが格納される。ユーザは、ＰＣ４０の操作装置４２を操作することによって、ＺＩＰファイルを選択することができる。この場合、ＺＩＰファイルをオープンするためのパスワード入力画面が表示される。ユーザは、パスワードを入力することによってＺＩＰファイルをオープンすることができる。これにより、ユーザは、スキャンデータを取得することができる。

【００６７】
例えば、図６のＳ５４又は図７のＳ８４で作成されたＵＲＬがＰＣ４０のユーザによって選択され、このＵＲＬがアクセスリクエストに含まれる場合、Ｓ１６４でＮＯと判断される。このＵＲＬは、ＺＩＰファイルを示すものではないからである。また、上述したように、Ｓ１６２では、「．ｚｉｐ」を含まないＵＲＬが作成されることがある。このＵＲＬ
がＰＣ４０のユーザによって選択され、このＵＲＬがアクセスリクエストに含まれる場合も、Ｓ１６４でＮＯと判断される。Ｓ１６４でＮＯの場合、制御装置２０は、アクセスリクエストに含まれるＵＲＬに対応するファイルが作成済であるのか否かを判断する（Ｓ１６８）。ここでＮＯの場合、Ｓ１７０に進む。
【００６８】
Ｓ１７０では、制御装置２０は、アクセスリクエストに含まれるＵＲＬからデータ形式を特定する。例えば、アクセスリクエストに含まれるＵＲＬがＳ１６２に例示されているＵＲＬ１８０である場合（「ｃ１５０．ｐｄｆ」が含まれる場合）、制御装置２０は、カラー、解像度１５０ｄｐｉ、及び、ＰＤＦファイルというデータ形式を特定する。この場合、制御装置２０は、ＵＲＬ１８０に含まれるフォルダ名１８０ｃ及びファイル名１８０ｄを有するスキャンデータファイル８２（図３参照）のスキャンデータ８２ｄを、上記の特定されたデータ形式に変換する。これにより、ＰＣ４０のユーザによって選択されたデータ形式を有するスキャンデータ（以下では「変換スキャンデータ」と呼ぶ）が作成される。制御装置２０は、ＵＲＬ１８０のファイル名１８０ｄ及び文字列１８０ｅを有するファイル名と変換スキャンデータとが対応づけられているファイルを、フォルダ名１８０ｃを有するフォルダ８０（図３参照）の下位ファイルとしてスキャンデータ記憶領域２６に記憶させる。
【００６９】
制御装置２０は、アクセスリクエストに含まれるＵＲＬに対応するファイル（即ちＳ１７０で作成されたファイル）と、そのファイルを共有フォルダ５０内に格納することを指示するコマンドとをＰＣ４０に送信する（Ｓ１７２）。これにより、ＰＣ４０の共有フォルダ５０にファイルが格納される。ユーザは、このファイルをオープンすることによって、スキャンデータを取得することができる。なお、図５のＳ１４で複数の送信先が指定された場合、一方の送信先がＵＲＬにアクセスすると、そのＵＲＬのファイルがＳ１７０で作成される。この後に他方の送信先が同じＵＲＬにアクセスする際には、そのＵＲＬのファイルが既に作成されている。この場合、Ｓ１６８でＹＥＳと判断され、Ｓ１７０がスキップされる。
【００７０】
（キャンセル処理）
続いて、スキャナ１０のキャンセル処理について説明する。図１１は、スキャナ１０のキャンセル処理のフローチャートを示す。ユーザは、スキャナ１０の操作装置１２を操作することによって、スキャンデータのキャンセルを指示することができる。制御装置２０は、このキャンセルが指示されることを監視している（Ｓ１９０）。ここでＹＥＳの場合、制御装置２０は、対応情報記憶領域２８に記憶されている対応情報１１０，１１２（図４参照）のリストを表示装置１４に表示する（Ｓ１９２）。なお、パスワード１０６は表示されない。
【００７１】
ユーザは、操作装置１２を操作することによって、表示装置１４に表示されたリストの中から１つの対応情報を指定することができる。制御装置２０は、対応情報が指定されることを監視している（Ｓ１９４）。ここでＹＥＳの場合、制御装置２０は、指定された対応情報にパスワードが含まれるのか否かを判断する（Ｓ１９６）。ここでＮＯの場合、後述のＳ１９８～Ｓ２０２をスキップする。一方において、Ｓ１９６でＹＥＳの場合、制御装置２０は、パスワード入力画面を表示装置１４に表示する（Ｓ１９８）。ユーザは、操作装置１２を操作することによって、パスワードを入力することができる。制御装置２０

は、パスワードが入力されることを監視している（Ｓ２００）。ここでＹＥＳの場合、制御装置２０は、Ｓ１９４で指定された対応情報のパスワードと、Ｓ２００で入力されたパスワードとが一致するのか否かを判断する（Ｓ２０２）。ここでＮＯの場合、制御装置２０は、Ｓ１９８に戻ってパスワード入力画面を表示装置１４に再び表示する。一方において、Ｓ２０２でＹＥＳの場合、Ｓ２０４に進む。

【００７２】

Ｓ２０４では、制御装置２０は、Ｓ１９４で指定された対応情報の送信先１０４（図４参照）の共有フォルダ内から、Ｓ１９４で指定された対応情報のＵＲＬ１０２（図４参照）を含むＨＴＭＬファイルを削除する。次いで、制御装置２０は、Ｓ１９４で指定された対応情報のＵＲＬ１０２に対応するフォルダと全ての下位ファイルとをスキャンデータ記憶領域２６から削除する（Ｓ２０６）。続いて、制御装置２０は、Ｓ１９４で指定された対応情報を対応情報記憶領域２８から削除する（Ｓ２０８）。これにより、キャンセル処理が終了する。

【００７３】

本実施例のスキャナシステム２について詳しく説明した。スキャナ１０は、スキャンデータが送信されるべきデバイス（ここでは「ＰＣ４０」とする）に向けて、そのスキャンデータを格納しているＵＲＬ（図６の符号１２０ｃ、図６の符号１３０ｃ、図７の符号１４０ｃ、図７の符号１５０ｃ、図８の符号１６０ｃ、又は、図８の符号１７０ｃ）を送信する。この結果、ＰＣ４０のユーザは、スキャンデータのロケーションを知ることができる。ＰＣ４０のユーザは、ＵＲＬにアクセスすることができる。この場合、上記のＵＲＬとＰＣ４０のＩＰアドレスとの組合せがＰＣ４０から送信され、スキャナ１０によって受信される。スキャナ１０は、上記の組合せが対応情報記憶領域２８に記憶されていることを条件として、上記のＵＲＬに格納されているスキャンデータをＰＣ４０に送信する。スキャナ１０からＰＣ４０に上記のＵＲＬが送信される過程において、第三者がＵＲＬを盗み見る可能性がある。第三者がＰＣ４０以外のデバイスを利用して上記のＵＲＬにアクセスしても、ＵＲＬとデバイスのＩＰアドレスとの組合せが対応情報記憶領域２８に記憶されていないために、スキャナ１０は、スキャンデータを送信しない。本実施例によると、スキャンデータが第三者によって盗み取られる事象が発生することを抑制することができる。

【００７４】

また、本実施例では、ＳＣＡＮ　ＴＯ処理を実行する際にパスワードを発行することができる。第三者は、パスワードを知り得ないために、スキャンデータを取得することができない。本実施例によると、スキャンデータが第三者によって盗み取られることを効果的に抑制することができる。

【００７５】

また、スキャナ１０は、ＨＴＴＰを使用する場合、パスワードを暗号化キーとしてＺＩＰファイルを作成することができる。このＺＩＰファイルが送信される。このために、スキャンデータが第三者によって盗み取られることを効果的に抑制することができる。一方において、スキャナ１０は、ＨＴＴＰＳを使用する場合、ＺＩＰファイルを作成しない。ＨＴＴＰＳを使用する場合、通信データの全てが暗号化されるからである。ＺＩＰファイルを作成する処理を省略することによって、効率的に処理を実行することができる。

【００７６】

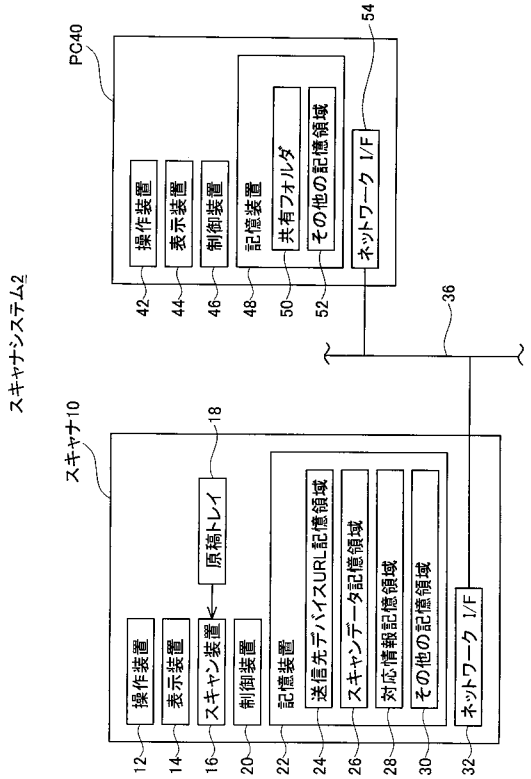
以上、本発明の具体例を詳細に説明したが、これらは例示にすぎず、特許請求の範囲を限定するものではない。特許請求の範囲に記載の技術には、以上に例示した具体例を様々に変形、変更したものが含まれる。上記の実施例の変形例を以下に列挙する。

【００７７】

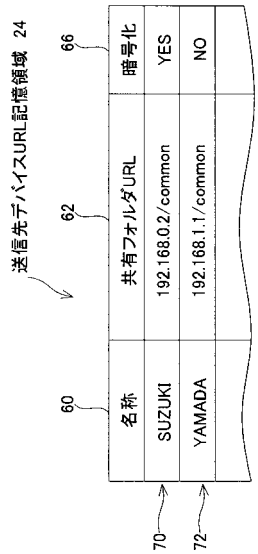
（１）スキャンデータ記憶領域２６に記憶されているフォルダと下位ファイルは、スキャンデータが送信された際に削除されてもよい。なお、図５のＳ１４において複数の送信先が指定された場合、全ての送信先にスキャンデータが送信された際に、フォルダと下位ファイルが削除されてもよい。

（２）スキャンデータ記憶領域２６に記憶されているフォルダと下位ファイルは、所定時間が経過すると削除されてもよい。
（３）スキャンデータ記憶領域２６に記憶されているフォルダと下位ファイルは、古いものから順に削除されてもよい。この場合、スキャナ１０のデータ記憶量が所定値を超えたことを契機として削除されてもよい。
（４）スキャンデータ記憶領域２６に記憶されているフォルダと下位ファイルは、スキャンデータが送信されたものから優先的に削除されてもよい。
【００７８】
（５）図６のＳ５６、及び／又は、図８のＳ１０２、及び／又は、図８のＳ１０８の処理において、図１０のＳ１６２の処理を実行して各ファイルのＵＲＬ及びサムネイル画像データが作成されてもよい。この場合、図１０のフローチャートにおいて、Ｓ１６２の処理を省略してもよい。
【００７９】
また、本明細書または図面に説明した技術要素は、単独であるいは各種の組合せによって技術的有用性を発揮するものであり、出願時請求項記載の組合せに限定されるものではない。また、本明細書または図面に例示した技術は複数目的を同時に達成するものであり、そのうちの一つの目的を達成すること自体で技術的有用性を持つものである。
【図面の簡単な説明】
【００８０】
【図１】スキャナシステムの構成を示す。
【図２】送信先デバイスＵＲＬ記憶領域の記憶内容の一例を示す。
【図３】スキャンデータ記憶領域の記憶内容の一例を示す。
【図４】対応情報記憶領域の記憶内容の一例を示す。
【図５】ＳＣＡＮ　ＴＯ処理のフローチャートを示す。
【図６】図５の続きのフローチャートを示す。
【図７】図６の続きのフローチャートを示す。
【図８】図７の続きのフローチャートを示す。
【図９】スキャンデータ提供処理のフローチャートを示す。
【図１０】図９の続きのフローチャートを示す。
【図１１】キャンセル処理のフローチャートを示す。
【符号の説明】
【００８１】
２：スキャナシステム
１０：スキャナ
１６：スキャン装置
２０：制御装置
２２：記憶装置
２６：スキャンデータ記憶領域
２８：対応情報記憶領域
４０：ＰＣ
４６：制御装置
４８：記憶装置
５０：共有フォルダ

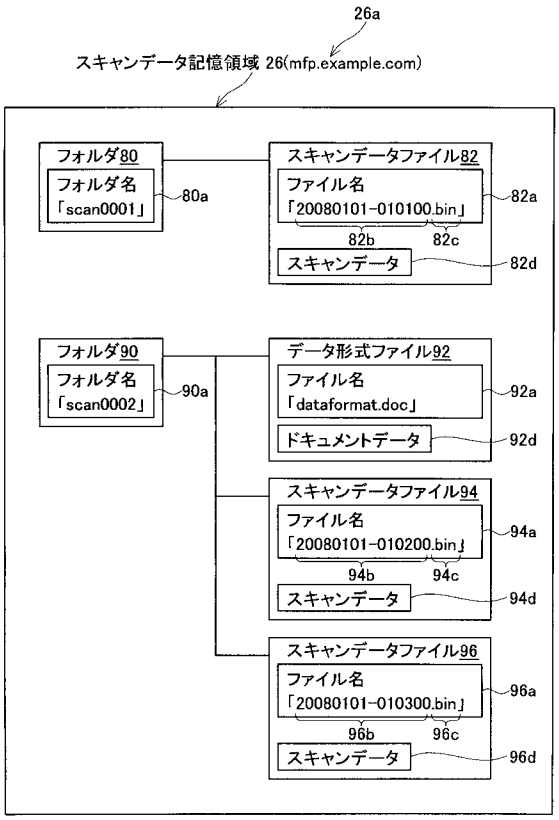
【図１】


スキャナシステム2
PC40
54
操作装置
表示装置
制御装置
記憶装置
共有フォルダ
その他の記憶領域
ネットワーク I/F
42
44
46
48
50
52
36
スキャナ10
18
原稿トレイ
操作装置
表示装置
スキャン装置
制御装置
記憶装置
送信先デバイスURL記憶領域
スキャンデータ記憶領域
対応情報記憶領域
その他の記憶領域
ネットワーク I/F
12
14
16
20
22
24
26
28
30
32

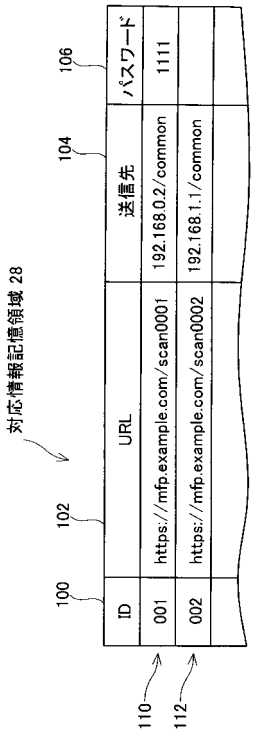
【図２】


送信先デバイスURL記憶領域 24
66
62
60
名称
共有フォルダURL
暗号化
SUZUKI
192.168.0.2/common
YES
YAMADA
192.168.1.1/common
NO
70
72

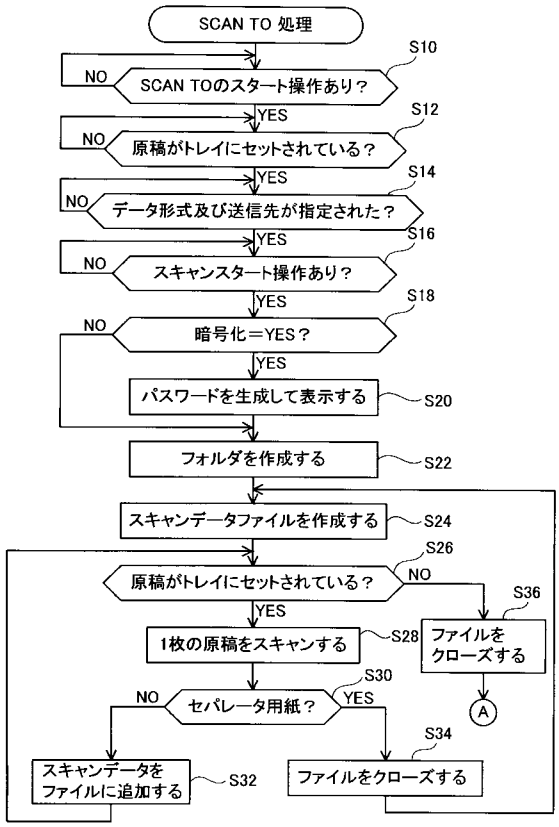
【図３】


26a
スキャンデータ記憶領域 26(mfp.example.com)
フォルダ80
フォルダ名
「scan0001」
80a
スキャンデータファイル82
ファイル名
「20080101-010100.bin」
82a
82b
82c
スキャンデータ
82d
フォルダ90
フォルダ名
「scan0002」
90a
データ形式ファイル92
ファイル名
「dataformat.doc」
92a
ドキュメントデータ
92d
スキャンデータファイル94
ファイル名
「20080101-010200.bin」
94a
94b
94c
スキャンデータ
94d
スキャンデータファイル96
ファイル名
「20080101-010300.bin」
96a
96b
96c
スキャンデータ
96d

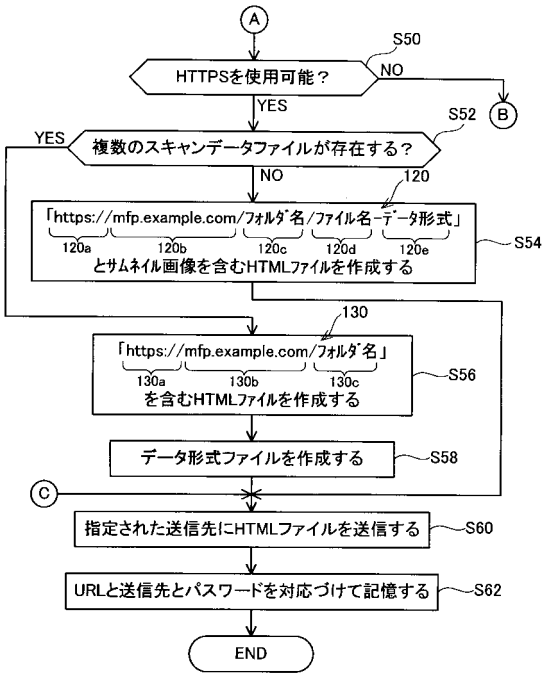
【図４】


対応情報記憶領域 28
106
104
102
100
ID
URL
送信先
パスワード
001
https://mfp.example.com/scan0001
192.168.0.2/common
1111
002
https://mfp.example.com/scan0002
192.168.1.1/common
110
112

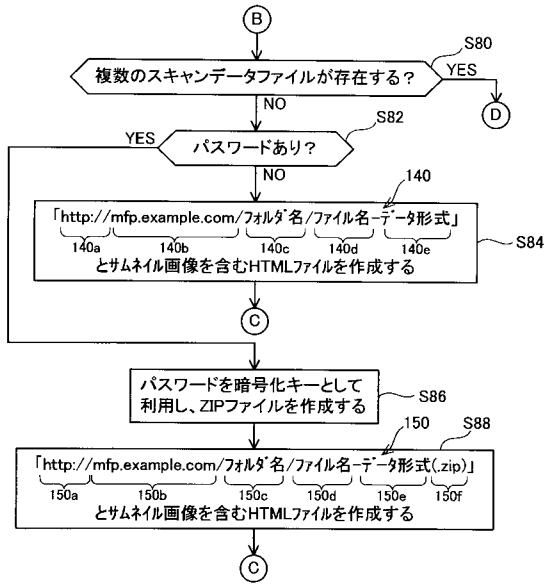
【図５】


SCAN TO 処理
S10
NO
SCAN TOのスタート操作あり？
YES
S12
NO
原稿がトレイにセットされている？
YES
S14
NO
データ形式及び送信先が指定された？
YES
S16
NO
スキャンスタート操作あり？
YES
S18
NO
暗号化＝YES？
YES
パスワードを生成して表示する
S20
フォルダを作成する
S22
スキャンデータファイルを作成する
S24
S26
原稿がトレイにセットされている？
NO
S36
YES
1枚の原稿をスキャンする
S28
ファイルをクローズする
A
S30
NO
セパレータ用紙？
YES
S34
スキャンデータをファイルに追加する
S32
ファイルをクローズする

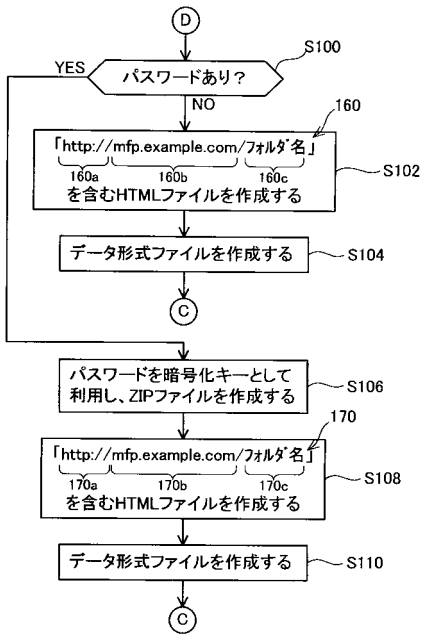
【図６】


A
S50
HTTPSを使用可能？
NO
B
YES
S52
YES
複数のスキャンデータファイルが存在する？
NO
120
「https://mfp.example.com/フォルダ名/ファイル名-データ形式」
120a 120b 120c 120d 120e
とサムネイル画像を含むHTMLファイルを作成する
S54
130
「https://mfp.example.com/フォルダ名」
130a 130b 130c
を含むHTMLファイルを作成する
S56
データ形式ファイルを作成する
S58
C
指定された送信先にHTMLファイルを送信する
S60
URLと送信先とパスワードを対応づけて記憶する
S62
END

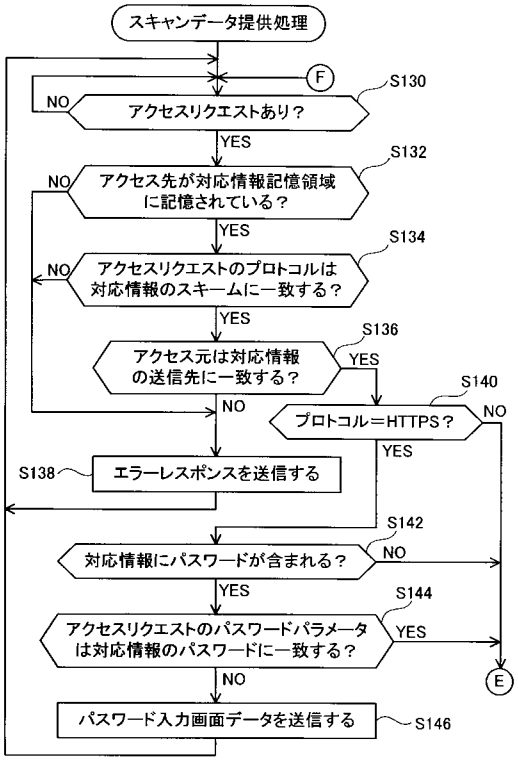
【図７】


B
S80
複数のスキャンデータファイルが存在する？
YES
D
NO
S82
YES
パスワードあり？
NO
140
「http://mfp.example.com/フォルダ名/ファイル名-データ形式」
140a 140b 140c 140d 140e
とサムネイル画像を含むHTMLファイルを作成する
S84
C
パスワードを暗号化キーとして利用し、ZIPファイルを作成する
S86
150
S88
「http://mfp.example.com/フォルダ名/ファイル名-データ形式(.zip)」
150a 150b 150c 150d 150e 150f
とサムネイル画像を含むHTMLファイルを作成する
C

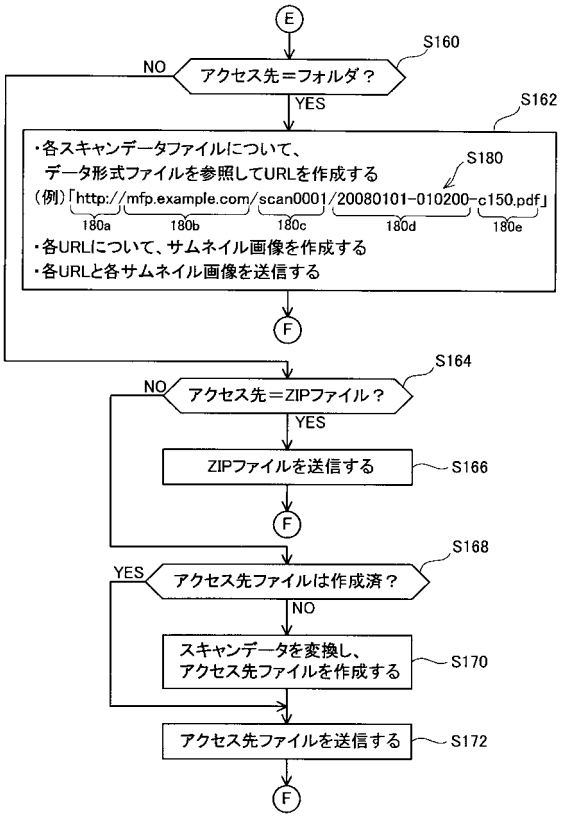
【図８】


D
S100
YES
パスワードあり？
NO
160
「http://mfp.example.com/フォルダ名」
160a 160b 160c
を含むHTMLファイルを作成する
S102
データ形式ファイルを作成する
S104
C
パスワードを暗号化キーとして利用し、ZIPファイルを作成する
S106
170
「http://mfp.example.com/フォルダ名」
170a 170b 170c
を含むHTMLファイルを作成する
S108
データ形式ファイルを作成する
S110
C

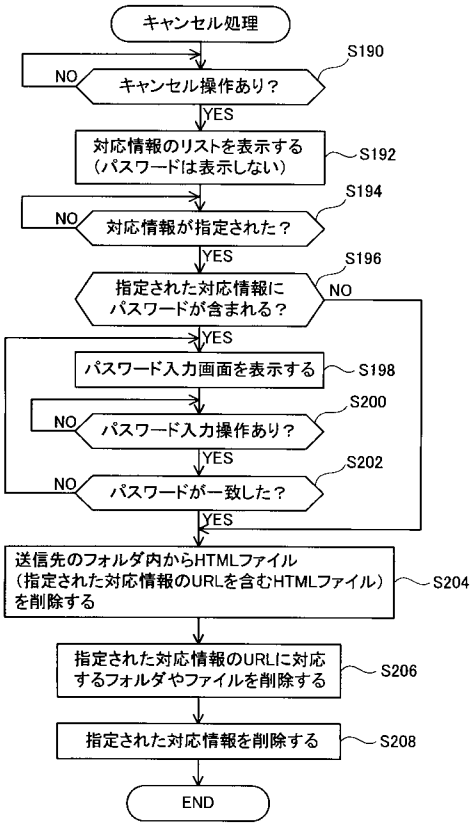
【図９】


スキャンデータ提供処理
F
S130
NO
アクセスリクエストあり？
YES
S132
NO
アクセス先が対応情報記憶領域に記憶されている？
YES
S134
NO
アクセスリクエストのプロトコルは対応情報のスキームに一致する？
YES
S136
アクセス元は対応情報の送信先に一致する？
YES
S140
NO
プロトコル＝HTTPS？
NO
YES
S138
エラーレスポンスを送信する
S142
対応情報にパスワードが含まれる？
NO
YES
S144
アクセスリクエストのパスワードパラメータは対応情報のパスワードに一致する？
YES
NO
E
パスワード入力画面データを送信する
S146

【図１０】


E
S160
NO
アクセス先＝フォルダ？
YES
S162
・各スキャンデータファイルについて、
データ形式ファイルを参照してURLを作成する
S180
（例）「http://mfp.example.com/scan0001/20080101-010200-c150.pdf」
180a
180b
180c
180d
180e
・各URLについて、サムネイル画像を作成する
・各URLと各サムネイル画像を送信する
F
S164
NO
アクセス先＝ZIPファイル？
YES
ZIPファイルを送信する
S166
F
S168
YES
アクセス先ファイルは作成済？
NO
スキャンデータを変換し、
アクセス先ファイルを作成する
S170
アクセス先ファイルを送信する
S172
F

【図１１】


キャンセル処理
S190
NO
キャンセル操作あり？
YES
対応情報のリストを表示する
（パスワードは表示しない）
S192
S194
NO
対応情報が指定された？
YES
S196
指定された対応情報にパスワードが含まれる？
NO
YES
パスワード入力画面を表示する
S198
S200
NO
パスワード入力操作あり？
YES
S202
NO
パスワードが一致した？
YES
送信先のフォルダ内からHTMLファイル
（指定された対応情報のURLを含むHTMLファイル）
を削除する
S204
指定された対応情報のURLに対応するフォルダやファイルを削除する
S206
指定された対応情報を削除する
S208
END

フロントページの続き

(56)参考文献 特開２０００－０９２１２１（ＪＰ，Ａ）
特開２００２－０７７４７３（ＪＰ，Ａ）
特開２００３－１１５９６９（ＪＰ，Ａ）
特開２００４－０８６７３１（ＪＰ，Ａ）
特開２００４－１７２９０３（ＪＰ，Ａ）
特開２００４－３６３９３４（ＪＰ，Ａ）
特開２００５－１９１７７７（ＪＰ，Ａ）
特開２００６－１３６０１４（ＪＰ，Ａ）
特開２００６－３１１３４４（ＪＰ，Ａ）
特許第３４６１７５０（ＪＰ，Ｂ２）
国際公開第０１／０９１４５２（WO，Ａ１）
ハーマン エリック，ＣＧＩ入門－原理、技法、Ｐｅｒｌスクリプト，日本，プレンティスホール出版，１９９７年 6月１０日， 初版，p.385-413

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １２／００
Ｇ０６Ｆ １３／００
Ｈ０４Ｎ １／００
コンピュータソフトウェアデータベース（ＣＳＤＢ）