(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4464309号
(P4464309)
(45)発行日　平成22年5月19日(2010.5.19)　(24)登録日　平成22年2月26日(2010.2.26)

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

請求項の数 22　(全 30 頁)

(21)出願番号　特願2005-114469(P2005-114469)
(22)出願日　平成17年4月12日(2005.4.12)
(65)公開番号　特開2006-293742(P2006-293742A)
(43)公開日　平成18年10月26日(2006.10.26)
審査請求日　平成20年4月8日(2008.4.8)

(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　100145827
弁理士　水垣　親房
(72)発明者　横山　英彦
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】画像形成システムおよび画像形成装置およびサービス連携処理方法およびコンピュータが読み取り可能なプログラムを格納した記憶媒体およびプログラム

(57)【特許請求の範囲】
【請求項１】
画像処理要求を行う情報端末と、複数の画像形成装置に対するユーザまたは各画像形成装置が提供するサービスの権限の認証を行う認証情報端末と該情報端末に接続可能な画像形成装置とが互いに通信可能な画像形成システムであって、
情報端末は、
ログインする各ユーザに対するユーザ認証情報を前記認証情報端末から取得して、いずれかの画像形成装置に対して、該取得されるユーザ認証情報とともに画像形成装置が提供する画像処理サービス要求を出力するサービス要求手段とを備え、
認証情報端末は、
前記情報端末からのユーザ接続認証または各画像形成装置からのユーザ権限認証を行うユーザ認証手段と、
いずれかの画像形成装置からのサービス権限認証を行うサービス認証手段とを備え、
いずれかの画像形成装置は、
前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求手段と、
前記第１のサービス要求手段に対する他の画像形成装置からの特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される自機のサービス認証情報を伴って前記特定画像処理サービス要求を画像形成装置に再出力する第２のサービス要求手段と、

前記第２のサービス要求手段による要求に対して他の画像形成装置により生成される出力情報を取得する取得手段と、
前記取得手段により取得される出力情報を画像出力する出力手段とを備え、
いずれか他の画像形成装置は、
画像形成装置から取得するユーザ認証情報に対して前記認証情報端末での認証を要求するユーザ認証要求手段と、
画像形成装置から取得するサービス認証情報に対して前記認証情報端末での認証を要求するサービス認証要求手段と、
前記ユーザ認証要求手段または前記サービス認証要求手段による前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行手段と、
前記サービス実行手段により生成される出力情報をサービス要求元の画像形成装置に返信する返信手段とを備えることを特徴とする画像形成システム。
【請求項２】
前記ユーザ認証要求手段によるユーザ認証結果に基づいて前記特定画像処理サービスを実行できないユーザであると認証された場合に、他の画像形成装置から返信されるユーザ認証情報を保存するデータ保存手段を備え、
前記第２のサービス要求手段は、第１のサービス要求手段に代えて、前記他の画像形成装置に対して前記サービス認証情報を伴う特定画像処理サービスを要求することを特徴とする請求項１記載の画像形成システム。
【請求項３】
前記画像形成装置は、特定画像処理サービスの実行要求を所定のメッセージ形式で情報端末より受信することを特徴とする請求項１記載の画像形成システム。
【請求項４】
前記所定のメッセージ形式は、ＳＯＡＰメッセージ形式であることを特徴とする請求項３記載の画像形成システム。
【請求項５】
前記サービス要求手段は、所定のアプリケーションを実行時に、ログインする各ユーザに対するユーザ認証情報を前記認証情報端末から取得して、いずれかの画像形成装置に対して、該取得されるユーザ認証情報とともに画像形成装置が提供する画像処理サービス要求を出力することを特徴とする請求項１記載の画像形成システム。
【請求項６】
情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置であって、
前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求手段と、
前記第１のサービス要求手段に対する他の画像形成装置からの特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される記憶されている自機のサービス認証情報を伴って前記特定画像処理サービス要求を画像形成装置に再出力する第２のサービス要求手段と、
前記第２のサービス要求手段による要求に対して他の画像形成装置により生成される出力情報を取得する取得手段と、
前記取得手段により取得される出力情報を画像出力する出力手段と、
を有することを特徴とする画像形成装置。
【請求項７】
情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置であって、
画像形成装置から取得するユーザ認証情報に対して前記認証情報端末での認証を要求す

るユーザ認証要求手段と、
画像形成装置から取得するサービス認証情報に対して前記認証情報端末での認証を要求するサービス認証要求手段と、
前記ユーザ認証要求手段または前記サービス認証要求手段による前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行手段と、
前記サービス実行手段により生成される出力情報をサービス要求元の画像形成装置に返信する返信手段と、
を有することを特徴とする画像形成装置。
【請求項８】
前記ユーザ認証要求手段によるユーザ認証結果に基づいて前記特定画像処理サービスを実行できないユーザであると認証された場合に、他の画像形成装置から返信されるユーザ認証情報を保存するデータ保存手段を備え、
前記第２のサービス要求手段は、第１のサービス要求手段に代えて、前記他の画像形成装置に対して前記サービス認証情報を伴う特定画像処理サービスを要求することを特徴とする請求項６記載の画像形成装置。
【請求項９】
前記画像形成装置は、特定画像処理サービスの実行要求を所定のメッセージ形式で情報端末より受信することを特徴とする請求項７または８記載の画像形成装置。
【請求項１０】
前記所定のメッセージ形式は、ＳＯＡＰメッセージ形式であることを特徴とする請求項９記載の画像形成装置。
【請求項１１】
画像処理要求を行う情報端末と、複数の画像形成装置に対するユーザまたは各画像形成装置が提供するサービスの権限の認証を行う認証情報端末と該情報端末に接続可能な画像形成装置とが互いに通信可能な画像形成システムにおけるサービス連携処理方法であって、
情報端末は、
ログインする各ユーザに対するユーザ認証情報を前記認証情報端末から取得して、いずれかの画像形成装置に対して、該取得されるユーザ認証情報とともに画像形成装置が提供する画像処理サービス要求を出力するサービス要求ステップを備え、
認証情報端末は、
前記情報端末からのユーザ接続認証または各画像形成装置からのユーザ権限認証を行うユーザ認証ステップと、
いずれかの画像形成装置からのサービス権限認証を行うサービス認証ステップとを備え、
いずれかの画像形成装置は、
前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求ステップと、
前記第１のサービス要求ステップに対する他の画像形成装置からの特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される自機のサービス認証情報を伴って前記特定画像処理サービス要求を画像形成装置に再出力する第２のサービス要求ステップと、
前記第２のサービス要求ステップによる要求に対して他の画像形成装置により生成される出力情報を取得する取得ステップと、
前記取得ステップにより取得される出力情報を画像出力する出力ステップとを備え、
いずれか他の画像形成装置は、
画像形成装置から取得するユーザ認証情報に対して前記認証情報端末での認証を要求するユーザ認証要求ステップと、
画像形成装置から取得するサービス認証情報に対して前記認証情報端末での認証を要求

するサービス認証要求ステップと、
前記ユーザ認証要求ステップまたは前記サービス認証要求ステップによる前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行ステップと、
前記サービス実行ステップにより生成される出力情報をサービス要求元の画像形成装置に返信する返信ステップとを備えることを特徴とするサービス連携処理方法。
【請求項１２】
前記ユーザ認証要求ステップによるユーザ認証結果に基づいて前記特定画像処理サービスを実行できないユーザであると認証された場合に、他の画像形成装置から返信されるユーザ認証情報をデータ保存手段に保存する保存ステップを備え、
前記第２のサービス要求ステップは、第１のサービス要求手段に代えて、前記他の画像形成装置に対して前記サービス認証情報を伴う特定画像処理サービスを要求することを特徴とする請求項１１記載のサービス連携処理方法。
【請求項１３】
前記画像形成装置は、特定画像処理サービスの実行要求を所定のメッセージ形式で情報端末より受信することを特徴とする請求項１１記載のサービス連携処理方法。
【請求項１４】
前記所定のメッセージ形式は、ＳＯＡＰメッセージ形式であることを特徴とする請求項１３記載のサービス連携処理方法。
【請求項１５】
前記サービス要求ステップは、所定のアプリケーションを実行時に、ログインする各ユーザに対するユーザ認証情報を前記認証情報端末から取得して、いずれかの画像形成装置に対して、該取得されるユーザ認証情報とともに画像形成装置が提供する画像処理サービス要求を出力することを特徴とする請求項１１記載のサービス連携処理方法。
【請求項１６】
情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置におけるサービス連携処理方法であって、
前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求ステップと、
前記第１のサービス要求ステップに対する他の画像形成装置からの特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される記憶されている自機のサービス認証情報を伴って前記特定画像処理サービス要求を画像形成装置に再出力する第２のサービス要求ステップと、
前記第２のサービス要求ステップによる要求に対して他の画像形成装置により生成される出力情報を取得する取得ステップと、
前記取得ステップにより取得される出力情報を画像出力する出力ステップと、
を有することを特徴とするサービス連携処理方法。
【請求項１７】
情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置におけるサービス連携処理方法であって、
画像形成装置から取得するユーザ認証情報に対して前記認証情報端末での認証を要求するユーザ認証要求ステップと、
画像形成装置から取得するサービス認証情報に対して前記認証情報端末での認証を要求するサービス認証要求ステップと、
前記ユーザ認証要求ステップまたは前記サービス認証要求ステップによる前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行ステップと、
前記サービス実行ステップにより生成される出力情報をサービス要求元の画像形成装置に返信する返信ステップと、

を有することを特徴とするサービス連携処理方法。
【請求項１８】
前記ユーザ認証要求ステップによるユーザ認証結果に基づいて前記特定画像処理サービスを実行できないユーザであると認証された場合に、他の画像形成装置から返信されるユーザ認証情報をデータ保存手段に保存するデータ保存ステップを備え、
前記第２のサービス要求ステップは、第１のサービス要求ステップに代えて、前記他の画像形成装置に対して前記サービス認証情報を伴う特定画像処理サービスを要求することを特徴とする請求項１６記載のサービス連携処理方法。
【請求項１９】
前記画像形成装置は、特定画像処理サービスの実行要求を所定のメッセージ形式で情報端末より受信することを特徴とする請求項１７または１８記載のサービス連携処理方法。
【請求項２０】
前記所定のメッセージ形式は、ＳＯＡＰメッセージ形式であることを特徴とする請求項１９記載のサービス連携処理方法。
【請求項２１】
請求項１１～２０のいずれかに記載のサービス連携処理方法を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２２】
請求項１１～２０のいずれかに記載のサービス連携処理方法を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、ネットワーク上の複数の情報処理装置とサービスが異なる複数の画像形成装置とが通信してそれぞれの画像形成装置が提供するサービスを連携して複合画像処理を行う画像形成システムに関するものである。
【背景技術】
【０００２】
近年、ＳＯＡＰ（Ｓｉｍｐｌｅ Ｏｂｊｅｃｔ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）／ＸＭＬを利用したＷｅｂサービスと呼ばれるプログラムを情報処理装置上で動作させ、異なるアーキテクチャにより構成される情報処理装置間でデータ交換やデータ処理が行われている。
【０００３】
従来、情報処理装置間のデータ交換やデータ処理は、Ｍｉｃｒｏｓｏｆｔ（登録商標）のＤＣＯＭ（Ｄｉｓｔｒｉｂｕｔｅｄ Ｃｏｍｐｏｎｅｎｔ Ｏｂｊｅｃｔ Ｍｏｄｅｌ）、ＯＭＧ（Ｏｂｊｅｃｔ Ｍａｎａｇｅｍｅｎｔ Ｇｒｏｕｐ）のＣＯＲＢＡ（Ｃｏｍｍｏｎ Ｏｂｊｅｃｔ Ｒｅｑｕｅｓｔ Ｂｒｏｋｅｒ Ａｒｃｈｉｔｅｃｔｕｒｅ）、Ｓｕｎ ＭｉｃｒｏｓｙｓｔｅｍｓのＪａｖａ（登録商標）ＲＭＩ（Ｊａｖａ（登録商標） Ｒｅｍｏｔｅ Ｍｅｔｈｏｄ Ｉｎｖｏｃａｔｉｏｎ）といった固有のプロトコルを認識する装置間でのみ行われていた。一方、Ｗｅｂサービスは、ＸＭＬ及びＳＯＡＰと呼ばれるテキストベースのデータ構造を解釈可能な装置であれば処理が可能であり、ＯＳ等の情報処理装置のアーキテクチャに関わらず、異機種間でのデータ交換を可能にすることから、急速に普及してきている。
【０００４】
また、印刷装置や複合機能装置（ＭＦＰ）等の画像形成装置は、情報処理装置と同等のデータ処理能力を持つようになってきており、Ｗｅｂサービスを動作させることにより、情報処理装置あるいは他の画像形成装置との間でデータ交換やデータ処理が行われるようになってきた。
【０００５】
例えばサービス連携ジョブを処理する際に、連携サーバにより、処理途中のデータに対

して発行元（ユーザ）の署名を要求するかどうかを設定可能にする技術が下記特許文献１に記載されている。
【特許文献１】特開２００４－１９２２７３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
Ｗｅｂサービスは、単に２台の情報処理装置のうちの一方から他方で動作するＷｅｂサービスを呼び出して、データ処理を行わせるだけでなく、複数の情報処理装置で動作するＷｅｂサービスを連携させて処理させることが可能であるところに大きな特徴がある。
【０００７】
しかしながら、あるサービスで処理が許可されているユーザであっても、他のサービスでは処理が許可されないことが有り、一連の処理に対して実行されるすべてのサービスにおいて処理が許可されていなければ、処理全体を不許可とすることが一般的であった。
【０００８】
また、上記特許文献１では、複数のサービスを連携させる場合に、署名の添付を必要とするかどうかを選択可能とし、署名を添付することで、経路途中における改竄を防止すると共に、データ生成元の識別が可能になっているが、経路途中でアクセスが許可されていないサービスが存在した場合の処置に関しては触れられていない。
【０００９】
本発明は、上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、ユーザが画像形成装置に要求する特定画像処理サービスが他の画像形成装置と連携が必要な場合に、ユーザとして他の画像形成装置に認証否定される場合であっても、要求元の画像形成装置の特定画像処理サービスの認証情報を伴い、他の画像形成装置に特定画像処理サービスの実行を要求することで、他の画像形成装置が要求元の画像形成装置におけるサービス認証が確認できる場合には、要求された特定画像処理サービスを実行できるようにアクセス権を制御することにより、複数の装置あるいは単一の装置で動作する、複数のサービスから構成される複合画像処理サービスにおいて、サービス利用者に対して、各サービスにおけるアクセス制限が異なり、一連の処理の一部において実行する権限が無いユーザからの処理要求があった場合でも、各画像形成装置におけるサービス間の信頼関係に基づき、呼び出し側サービスの権限を用いることにより、一定のアクセス制限を担保したシステム環境の下で、一連の特定画像処理サービスを複数の画像形成装置で適正に連携し合いながら実行することができる画像形成システムおよび画像形成装置およびサービス連携処理方法およびコンピュータが読み取り可能なプログラムを格納した記憶媒体およびプログラムを提供することである。
【課題を解決するための手段】
【００１０】
上記目的を達成する本発明の画像形成システムは以下に示す構成を備える。
【００１１】
画像処理要求を行う情報端末と、複数の画像形成装置に対するユーザまたは各画像形成装置が提供するサービスの権限の認証を行う認証情報端末と該情報端末に接続可能な画像形成装置とが互いに通信可能な画像形成システムであって、情報端末は、ログインする各ユーザに対するユーザ認証情報を前記認証情報端末から取得して、いずれかの画像形成装置に対して、該取得されるユーザ認証情報とともに画像形成装置が提供する画像処理サービス要求を出力するサービス要求手段とを備え、認証情報端末は、前記情報端末からのユーザ接続認証または各画像形成装置からのユーザ権限認証を行うユーザ認証手段と、いずれかの画像形成装置からのサービス権限認証を行うサービス認証手段とを備え、いずれかの画像形成装置は、前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求手段と、前記第１のサービス要求手段に対する他の画像形成装置からの特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される自機の

サービス認証情報を伴って前記特定画像処理サービス要求を画像形成装置に再出力する第２のサービス要求手段と、前記第２のサービス要求手段による要求に対して他の画像形成装置により生成される出力情報を取得する取得手段と、前記取得手段により取得される出力情報を画像出力する出力手段とを備え、いずれか他の画像形成装置は、画像形成装置から取得するユーザ認証情報に対して前記認証情報端末での認証を要求するユーザ認証要求手段と、画像形成装置から取得するサービス認証情報に対して前記認証情報端末での認証を要求するサービス認証要求手段と、前記ユーザ認証要求手段または前記サービス認証要求手段による前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行手段と、前記サービス実行手段により生成される出力情報をサービス要求元の画像形成装置に返信する返信手段とを備えることを特徴とする。

【００１２】

上記目的を達成する本発明の画像形成装置は以下に示す構成を備える。

【００１３】

情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置であって、前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求手段と、前記第１のサービス要求手段に対する他の画像形成装置からの特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される記憶されている自機のサービス認証情報を伴って前記特定画像処理サービス要求を画像形成装置に再出力する第２のサービス要求手段と、前記第２のサービス要求手段による要求に対して他の画像形成装置により生成される出力情報を取得する取得手段と、前記取得手段により取得される出力情報を画像出力する出力手段とを有することを特徴とする。

【００１４】

情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置であって、画像形成装置から取得するユーザ認証情報に対して前記認証情報端末での認証を要求するユーザ認証要求手段と、画像形成装置から取得するサービス認証情報に対して前記認証情報端末での認証を要求するサービス認証要求手段と、前記ユーザ認証要求手段または前記サービス認証要求手段による前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行手段と、前記サービス実行手段により生成される出力情報をサービス要求元の画像形成装置に返信する返信手段とを有することを特徴とする。

【００１５】

上記目的を達成する本発明の画像形成システムにおけるサービス連携処理方法は以下に示す構成を備える。

【００１６】

画像処理要求を行う情報端末と、複数の画像形成装置に対するユーザまたは各画像形成装置が提供するサービスの権限の認証を行う認証情報端末と該情報端末に接続可能な画像形成装置とが互いに通信可能な画像形成システムにおけるサービス連携処理方法であって、情報端末は、ログインする各ユーザに対するユーザ認証情報を前記認証情報端末から取得して、いずれかの画像形成装置に対して、該取得されるユーザ認証情報とともに画像形成装置が提供する画像処理サービス要求を出力するサービス要求ステップとを備え、認証情報端末は、前記情報端末からのユーザ接続認証または各画像形成装置からのユーザ権限認証を行うユーザ認証ステップと、いずれかの画像形成装置からのサービス権限認証を行うサービス認証ステップとを備え、いずれかの画像形成装置は、前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求ステップと、前記第１のサービス要求ステップに対する他の画像形成装置からの特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される自機のサービス認証情報を伴って前記特定

画像処理サービス要求を画像形成装置に再出力する第２のサービス要求ステップと、前記第２のサービス要求ステップによる要求に対して他の画像形成装置により生成される出力情報を取得する取得ステップと、前記取得ステップにより取得される出力情報を画像出力する出力ステップとを備え、いずれか他の画像形成装置は、画像形成装置から取得するユーザ認証情報を前記認証情報端末での認証を要求するユーザ認証要求ステップと、画像形成装置から取得するサービス認証情報を前記認証情報端末での認証を要求するサービス認証要求ステップと、前記ユーザ認証要求ステップまたは前記サービス認証要求ステップによる前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行ステップと、前記サービス実行ステップにより生成される出力情報をサービス要求元の画像形成装置に返信する返信ステップとを備えることを特徴とする。

【００１７】

上記目的を達成する本発明の画像形成装置におけるサービス連携処理方法は以下に示す構成を備える。

【００１８】

情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置におけるサービス連携処理方法であって、前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求ステップと、前記第１のサービス要求ステップに対する他の画像形成装置からの特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される記憶されている自機のサービス認証情報を伴って前記特定画像処理サービス要求を画像形成装置に再出力する第２のサービス要求ステップと、前記第２のサービス要求ステップによる要求に対して他の画像形成装置により生成される出力情報を取得する取得ステップと、前記取得ステップにより取得される出力情報を画像出力する出力ステップとを有することを特徴とする。

【００１９】

また、情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置におけるサービス連携処理方法であって、画像形成装置から取得するユーザ認証情報を前記認証情報端末での認証を要求するユーザ認証要求ステップと、画像形成装置から取得するサービス認証情報を前記認証情報端末での認証を要求するサービス認証要求ステップと、前記ユーザ認証要求ステップまたは前記サービス認証要求ステップによる前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行ステップと、前記サービス実行ステップにより生成される出力情報をサービス要求元の画像形成装置に返信する返信ステップとを有することを特徴とする。

【発明の効果】

【００２０】

本発明によれば、複数の装置あるいは単一の装置で動作する、複数のサービスから構成される複合画像処理サービスにおいて、サービス利用者に対して、各サービスにおけるアクセス制限が異なり、一連の処理の一部において実行する権限が無いユーザからの処理要求があった場合でも、各画像形成装置におけるサービス間の信頼関係に基づき、呼び出し側サービスの権限を用いることにより、一定のアクセス制限を担保したシステム環境の下で、一連の特定画像処理サービスを複数の画像形成装置で適正に連携し合いながら実行することができる。

【発明を実施するための最良の形態】

【００２１】

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。

【００２２】

＜システム構成の説明＞

〔第１実施形態〕

以下、図面を参照して本発明の実施の形態を説明する。

【００２３】

図１は、本発明の第１実施形態に係る画像形成装置を適用可能な画像処理システムのネットワーク構成を示す図であり、画像形成装置例として、プリンタ１０３、１０４がネットワーク接続されてそれぞれの所定のプロトコルで相互に通信可能なシステム例を示すが、画像形成装置は、スキャナ機能やプリンタ機能などを連携して複合画像処理を行う複合機であっても本発明を適用可能である。

【００２４】

図１において、情報処理装置１０１、１０２及び画像形成装置１０３、１０４は、Ｅｔｈｅｒｎｅｔ（登録商標）等のＬＡＮ（ローカルエリアネットワーク）１０５に接続されており相互に直接通信することが可能である。

【００２５】

なお、図１で各画像形成装置は同一のＬＡＮ１０５に接続されているが、ＬＡＮはＬＡＮ同士を複数接続することによりＷＡＮ（ワイドエリアネットワーク）を構成することが可能であり、ＷＡＮを構成する何れかのＬＡＮに接続されていれば、本実施形態を実現可能であり、必ずしも同一ＬＡＮに接続する必要がある訳ではないことは言うまでもない。また、情報処理装置１０２は、後述するような画像形成装置１０３、１０４、あるいは情報処理装置１０１からの特定のユーザあるいはサービスに対するトークン認証処理を行うサーバ装置として構成してもよい。なお、本実施形態において、トークンという用語は、ネットワーク上におけるある種の権限情報であって、情報処理装置１０２等にユーザ別、あるいは画像形成装置１０３、１０４に設定された権限情報として登録されたものと、各画像形成装置１０３、１０４からのトークン認証要求時にそれぞれが照合されることで認証処理が実行される構成としている。

【００２６】

図２は、本発明の第１実施形態を示す画像形成装置の構成を説明するブロック図であり、図１に示した画像処理システムにおける画像形成装置１０３、１０４の内部構成例である。

【００２７】

図２において、ネットワークインタフェース２０１は、図１に示したＬＡＮ１０５と接続され、同様にＬＡＮ１０５に接続された装置、あるいはＬＡＮ１０５を介して接続可能な他のＬＡＮに接続された装置と通信を行う。ネットワークインタフェース２０１によりＬＡＮ１０５から受信したデータは、プロトコルスタック２０２により各プロトコルに対して処理が行われた後、機器制御部２０８の調停の下で、コマンド解析部２０３に送られて内容が解析される。

【００２８】

コマンド解析部２０３の解析により、受信データが印刷ジョブと呼ばれる印刷要求であった場合は、データ管理部２０９の制御により、データ保存部２１０のうち一定領域を占める印刷キューに該印刷ジョブを保存する。

【００２９】

ここで、印刷キューは、ＦＩＦＯ（Ｆｉｒｓｔ　Ｉｎ　Ｆｉｒｓｔ　Ｏｕｔ）形式の待ち行列であり、一般に印刷キューに保存された順番で印刷が行われるが、ジョブ制御命令により印刷順番を変更することも可能である。

【００３０】

ジョブ制御部２１１は、データ保存部２１０の印刷キューを監視し、印刷ジョブが溜まっている場合には、印刷制御部２１４に問い合わせて、印刷処理が可能かどうかを確認し、印刷可能であれば、データ保存部２１０の印刷キューの先頭におかれた印刷ジョブに含まれる印刷データを画像処理部２１２に転送する。

【００３１】

画像処理部２１２は、各種画像処理を行い、印刷データを印刷イメージに変換する。そして、生成された１ページ分の印刷イメージは、ページメモリ２１３に転送される。

【００３２】
ページメモリ２１３に印刷イメージが置かれたことを検知した印刷制御部２１４は、プリンタエンジン２１５に指示を出して、ページメモリ２１３の内容を印刷媒体に印刷する。
【００３３】
このように印刷ジョブ中の印刷データの全ページに対して、画像処理部２１２における画像処理とページメモリ２１３への展開及びプリンタエンジン２１５による印刷処理を繰り返すことで、印刷要求が処理される。
【００３４】
画像形成装置１０３、１０４は、ネットワークインタフェース２０１以外に、ＩＥＥＥ１２８４やＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）等のローカルインタフェース２０７を持ち、情報処理装置等からの処理要求を受け付けることが可能である。
【００３５】
入出力制御部２０６は機器制御部２０８から画像形成装置の状態を取得し、それをもとに画面生成部２０４により表示画面を生成後、表示画面を操作パネル２０５に表示したり、利用者の指による操作パネル２０５への接触検出を通知されると、接触位置に対応するボタン等の画面要素に対応付けられた処理を行う。
【００３６】
２１６はスキャナ制御部で、スキャナ２１７を制御して原稿の画像データを取得し、データ管理部２０９の制御によりデータ保存部２１０に保存する。
【００３７】
図３は、図１に示した情報処理装置１０１、１０２の内部構成の一例を示すブロック図である。
【００３８】
図３において、ＣＰＵ３０１はＲＡＭ３０２などに記憶されたプログラムを実行したり、フロッピー（登録商標）ディスクドライブ３１０に挿入されたフロッピー（登録商標）ディスク３１０やハードディスク（ＨＤ）３１２に保存されているプログラムやデータをＲＡＭ３０２にロードしたり、逆にＲＡＭ３０２の内容をＦＤ３１０やＨＤ３１２に保存する。
【００３９】
３０３はビデオコントローラで、接続されたディスプレイ３０４に処理情報などを投影する。３０６はキーボード及びマウス等の入力装置で、これらの装置からの入力はコントローラ３０５を経由してＣＰＵで動作しているプログラムによって処理される。ネットワークコントローラ３０７は、ＨＵＢ３０８を経由して図１のＬＡＮ１０５と接続され、ネットワーク上の装置と通信を行う。ＣＰＵ３０１、ＲＡＭ３０２及び各コントローラは内部バス３１３に接続されており、制御情報やデータの交換を行う。
【００４０】
図４は、図１に示した情報処理装置１０１、１０２と画像形成装置１０３，１０４から構成されるシステムのモジュールを説明するブロック図である。
【００４１】
図４において、ユーザ（Ｕｓｅｒ－Ａ）はクライアントと呼ばれる情報処理装置１０１上で動作しているログインサービス４０１に対して、ログイン名とパスワードからなる認証情報を渡してログインを要求する。
【００４２】
情報処理装置１０１のログインサービス４０１は、認証サーバと呼ばれる情報処理装置１０２で動作している認証・認可サービス（ＡＡＳ）４０６に認証情報を転送して、認証情報が予め登録されている登録情報（例えば図３に示すハードディスク３１２等に記憶されている）と一致するかどうかの認証処理を行う。
【００４３】
そして、情報処理装置１０２の認証・認可サービス（ＡＡＳ）４０６は認証情報が登録

情報と一致したと判断した場合に、ＡＡＳ４０６は肯定応答を、一致しなければ否定応答を情報処理装置１０１のログインサービス４０１に返却する。

【００４４】

これを受けてログインサービス４０１は、ＡＡＳ４０６から肯定応答が返った場合に、認証情報を提供したユーザに対して、当該情報処理装置１０１に対するアクセスを許可し、否定応答が返った場合は、ユーザに対して再度認証情報の入力を促し、情報処理装置１０１へのアクセスは許可しない。

【００４５】

そして、情報処理装置１０１のログインサービス４０１により情報処理装置１０１へのアクセスが許可されたＵｓｅｒ－Ａは、ＰＤＦアプリケーション４０２の様なプログラムを実行し所望の操作を行うことが可能になる。

【００４６】

ここで、ＰＤＦアプリケーションは、Ａｄｏｂｅ　Ｓｙｓｔｅｍ　Ｉｎｃ．が開発し、仕様を公開しているＰＤＦ（Ｐｏｒｔａｂｌｅ　Ｄｏｃｕｍｅｎｔ　Ｆｉｌｅ）形式の文書ファイルの表示、編集、印刷等が行えるプログラムである。

【００４７】

そして、Ｕｓｅｒ－ＡがＰＤＦアプリケーション４０２に対し、現在ディスプレイ３０４に表示中のＰＤＦ文書ファイルの内容を画像形成装置（ＭＦＰ）１０３から印刷させる指示を出すと、ＰＤＦアプリケーション４０２は、Ｕｓｅｒ－Ａのトークンと共に画像形成装置１０３のＰＤＦプリントサービス（以下ＰＤＦＰ－Ｓと呼ぶ）４０４をＳＯＡＰハンドラ４０３を介して呼び出す。ＳＯＡＰハンドラは、ＸＭＬ形式のデータ構造であるＳＯＡＰメッセージを解析し、ＳＯＡＰメッセージに対応するＷｅｂサービスを実行すると共に、該Ｗｅｂサービスの実行結果をＳＯＡＰメッセージに変換するモジュールである。

【００４８】

なお、ＰＤＦＰ－Ｓ４０４はＳＯＡＰメッセージにより実行されるＷｅｂサービスである。

【００４９】

ここで、ＰＤＦＰ－Ｓ４０４は、管理者によって画像形成装置１０３にインストールされる前に、情報処理装置１０２のＡＡＳ４０６に対して、ＰＤＦＰ－Ｓ４０４の登録を行う。

【００５０】

ここで、登録処理は、情報処理装置１０２上で起動させた管理プログラムから行うのが一般的である。そして、この登録処理により、ＡＡＳ４０６はＰＤＦＰ－Ｓ４０４のユーザ名とパスワードから構成される認証情報を管理データベース（図３のＨＤ３１２に保存されるデータに相当）に登録すると同時に、ＰＤＦＰ－Ｓ４０４をインストールする画像形成装置１０３を、信頼できる装置として登録する。

【００５１】

また、管理者がＰＤＦＰ－Ｓ４０４を画像形成装置１０３にインストールする際には、受信したＰＤＦデータをプリントエンジン４０５が解釈可能なＰＣＬ（Ｐｒｉｎｔｅｒ　Ｃｏｎｔｒｏｌ　Ｌａｎｇｕａｇｅ）に変換する必要があるが、画像形成装置１０３は、当該変換処理を行うモジュールを搭載してないため、変換処理が可能な画像形成装置１０４で動作するＰＤＦ－ＰＣＬ変換サービス（以下、ＰＤＦｔｏＰＣＬ－Ｓと呼ぶ）４０８を利用する必要があり、先にＡＡＳ４０６に登録したユーザ名とパスワードを入力して、ＡＡＳ４０６から認証トークンを取得する。

【００５２】

同時にユーザ名とパスワードは画像形成装置１０３のデータ保存部２１０に暗号化して保存する。

【００５３】

次に、ＰＤＦＰ－Ｓ４０４は、呼び出し先である画像形成装置１０４に対して先に取得したトークンと共にＰＤＦｔｏＰＣＬ－Ｓ４０８の呼び出し許可要求をＳＯＡＰハンドラ

４０３を介して画像形成装置１０４のＳＯＡＰハンドラ４０７へ送信する。
【００５４】
そして、サービス呼び出し要求を受信した画像形成装置１０４のＳＯＡＰハンドラ４０７は、ＡＡＳ４０６に対して、認証トークンと画像形成装置１０３にＩＰアドレスを渡してトークン認証と信頼性チェックを依頼し、応答として双方がＯＫだった場合に、画像形成装置１０３の識別情報（ＩＰアドレス）とＰＤＦＰ－Ｓ４０４の識別情報の対をデータ保存部２１０に保存される、図７の様な呼び出し許可サービスリストに登録し、呼び出し許可応答を画像形成装置１０３のＰＤＦＰ－Ｓ４０４にＳＯＡＰハンドラ４０３を介して返却する。
【００５５】
以上の処理により、呼び出し許可応答を受信した画像形成装置１０３は、以降のＰＤＦＰ－Ｓ４０４の呼び出しに対して、画像形成装置１０４のＰＤＦｔｏＰＣＬ－Ｓ４０８を呼び出す様に構成される。
【００５６】
つまり、前述のＵｓｅｒ－ＡによるＰＤＦアプリケーション４０２に対する画像形成装置１０３からの印刷要求に対して、ＰＤＦアプリケーション４０２から呼び出された、画像形成装置１０３のＰＤＦＰ－Ｓ４０４は、ＰＤＦデータからＰＣＬデータへの変換処理のため、画像形成装置１０４のＰＤＦｔｏＰＣＬ－Ｓ４０８を呼び出し、呼び出しに対する応答として受信したＰＣＬデータをプリントエンジン４０５に渡すことで印刷処理を行う。
【００５７】
上記のように構成された画像処理システムにおいて、本実施形態では、画像形成装置１０４の管理者が情報処理装置１０２の認証認可サービス（以下、ＡＡＳ）４０６に、信頼するデバイスとして画像形成装置１０３を登録する。そして、画像形成装置１０３の管理者は、ＰＤＦプリントサービス（以下、ＰＤＦＰ－Ｓ）４０４のユーザ情報をＡＡＳ４０６に登録する。そして、画像形成装置１０３にＰＤＦＰ－Ｓ４０４をインストールする際に、ＰＤＦＰ－Ｓ４０４から呼び出す、ＰＤＦからＰＣＬへのデータ変換サービス（以下、ＰＤＦｔｏＰＣＬ－Ｓ）４０８を指定する。
【００５８】
例えば、画像形成装置１０４のＰＤＦｔｏＰＣＬ－Ｓ４０８を指定する時には、画像形成装置１０３のＰＤＦＰ－Ｓ４０４の認証トークンを情報処理装置１０２から取得し（この際に管理者はパスワード等の入力が求められ、入力したパスワードはＨＤＤ等にセキュアに保存される）、画像形成装置１０４のＰＤＦｔｏＰＣＬ－Ｓ４０８に対して、認証トークンを含むサービス呼び出し許可要求を送信する。
【００５９】
すると、この要求に対して画像形成装置１０４のＰＤＦｔｏＰＣＬ－Ｓ４０８は、ＡＡＳ４０６に問い合わせ、要求送信元の画像形成装置１０３が信頼できるかどうかを判定する。ここで、信頼できる（信頼するデバイスに登録されている）と判定すると、ＰＤＦＰ－Ｓ４０４の識別情報と画像形成装置１０３の識別情報の対を呼び出し許可サービスリストとしてデータ保存部２１０に記憶する。
【００６０】
以下、Ｕｓｅｒ－Ａが情報処理処理装置１０１上で動作したＰＤＦアプリケーション（Ａｄｏｂｅ　Ａｃｒｏｂａｔ　Ｒｅａｄｅｒ等）４０２より、画像形成装置１０３のＰＤＦプリントサービス４０４を呼び出して印刷を行う場合を例に説明する。
【００６１】
（１）Ｕｓｅｒ－Ａは情報処理装置１０１にログイン要求を出すと、ログインサービス４０１が情報処理装置１０２のＡＡＳ４０６にユーザ名／パスワード等の認証情報を渡し（２）、認証に成功すると、情報処理装置１０１の資源が利用可能になる。
【００６２】
そして、情報処理装置１０１のＰＤＦアプリケーション４０２の操作により画像形成装

置１０３にＰＤＦ印刷を要求する際に、まずログインサービス４０１を介してＵｓｅｒ－Ａの認証トークンを情報処理装置１０２から取得する（３）。

【００６３】

次に、情報処理装置１０２から取得した認証トークンと共に画像形成装置１０３のＰＤＦＰ－Ｓ４０４を呼び出す（４）。これを受けて、ＰＤＦＰ－Ｓ４０４は、受信したＵｓｅｒ－Ａの認証トークンを情報処理装置１０２のＡＡＳ４０６に送り、アクセス許可されているかどうかを判定する（５）。

【００６４】

ここで、アクセス許可がされていると、Ｕｓｅｒ－Ａのトークンを印刷するＰＤＦデータ共に画像形成装置１０４のＰＤＦｔｏＰＣＬ－Ｓ４０８を呼び出す（６）。

【００６５】

ここで、ＰＤＦｔｏＰＣＬ－Ｓ４０８は、Ｕｓｅｒ－ＡのトークンをＡＡＳ４０６に送り、アクセス権があるかどうかを判定する（７）。ここで、アクセス権があれば、画像形成装置１０４は、ＰＤＦｔｏＰＣＬ変換を行い、処理結果を画像形成装置１０３のＰＤＦＰ－Ｓ４０４に返却する。

【００６６】

一方、アクセス権が無ければ、アクセス権なし応答を画像形成装置１０３に返却する（８）。

【００６７】

そして、アクセス権なし応答を受信した画像形成装置１０３はＨＤＤに保存されたＰＤＦＰ－Ｓ４０４に対するパスワードを用いて、ＡＡＳ４０６からＰＤＦＰ－Ｓ４０４の認証トークンを取得し（９）、取得したトークンと共にＰＤＦｔｏＰＣＬ－Ｓ４０８を呼び出す（１０）。

【００６８】

そして、ＰＤＦｔｏＰＣＬ－Ｓ４０８は、受信した認証トークンをＡＡＳ４０６に送り該トークンが認証されると、認証トークンに関連付けられたサービス及び呼び出しデバイスが、ＨＤＤに保存している信頼するサービス及びデバイスの対と等しいかどうかをＰＤＦｔｏＰＣＬ－Ｓ４０８が判定し（１１）、等しければＰＤＦｔｏＰＣＬ処理を行い結果（ＰＣＬデータ）を画像形成装置１０３のＰＤＦＰ－Ｓ４０４に返却する（１２）。そして、処理結果を受信したＰＤＦＰ－Ｓ４０４は他の処理を行い最終的に、プリントエンジン４０５にＰＣＬデータを送って印刷を行う（１３）。

【００６９】

このように、サービス要求を行うデバイスとサービスが、登録されているサービス及びデバイスと一致するかどうかにより、要求サービスのトークンが渡された場合の処理の可否を画像形成装置１０４が決定することから、万が一要求サービスのパスワードが盗まれた場合であっても、異なるデバイスから要求を出すと要求が拒絶されるため、セキュリティレベルの高いサービス委譲処理が可能になる。以下、本実施形態におけるサービス委譲処理の詳細について説明する。

【００７０】

図５は、図１に示した情報処理装置１０１から画像形成装置１０３のサービス、画像形成装置１０３のサービスから画像形成装置１０４のサービス間で送受信される、ＳＯＡＰメッセージの一例を示す図である。

【００７１】

図５に示すように、ＳＯＡＰメッセージはヘッダとボディー部に分けられ、ヘッダ部には、サービスの実行を所望するユーザやサービスを識別する認証トークン７０１が設定され、ボディー部には、実行するサービスの識別子や処理データ７０２から構成される。

【００７２】

図６は、図１に示した情報処理装置１０２により管理されるアクセス制御情報の一例を示す図であり、図１に示した情報処理装置１０２が認証認可サーバとして機能し、サービスごとに設定されるアクセス制御情報の管理例である。

【００７３】
図６において、８０１は前記画像形成装置１０３で実行されるＰＤＦプリントサービス（ＰＤＦＰ－Ｓ４０４）のアクセス制御情報で、Ｕｓｅｒ－ＡとＵｓｅｒ－Ｂに対してアクセスがともに許可されていることを示している。
【００７４】
８０２は、前記画像形成装置１０４で実行されるＰＤＦ－ＰＣＬ変換サービス（ＰＣＬｔｏＰＤＦ－Ｓ４０８）のアクセス制御情報で、Ｕｓｅｒ－Ａにはアクセスが許可されず、Ｕｓｅｒ－ＢとＰＤＦＰ－Ｓに対してアクセスが許可されていることを示している。
【００７５】
図７は、図１に示した画像形成装置１０４が管理する呼び出し許可サービスリストの一例を示す図である。
【００７６】
図７に示すように、サービスがデバイスに登録する際には、認証認可サーバとして機能する情報処理装置１０２に対して、サービスの識別情報を渡してサービスの登録を行うが、この際に、サービスの識別情報とサービスを実行する画像形成装置の識別情報（ＩＰアドレス）とを関連付けて設定する。これにより、認証トークンをネットワーク上で盗聴して、別の画像形成装置で動作するサービスから不正にアクセスすることを回避することが出来る。
【００７７】
９０１は前記画像形成装置１０３（ＩＰアドレス：１９２．１６８．１．１）で実行されるＰＤＦＰ－Ｓ４０４に関する登録情報を示している。
【００７８】
以下、図８、図９のフローチャートを用いて、図４の様な情報処理装置と画像形成装置から構成されるシステムにおいて、ユーザＡ（Ｕｓｅｒ－Ａ）が情報処理装置１０１上で動作するアプリケーションプログラムの操作により、画像形成装置１０３に対して印刷出力を行わせる場合の、画像形成装置１０３及び画像形成装置１０４における各サービスのユーザ認証に関して説明する。
【００７９】
図８は、本発明に係る画像処理システムにおける第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、画像形成装置１０３に権限を有する情報処理装置１０１のユーザが、情報処理装置１０２における認証処理を経て、ＰＤＦファイルの印刷を画像形成装置１０３に指示した場合に、該画像形成装置１０３が保持していないＰＤＦｔｏＰＣＬ変換処理を、情報処理装置１０２のサービス認証を経て、画像形成装置１０４に依頼して、変換されたＰＣＬデータを取得して画像形成装置１０３が印刷処理する一連の処理手順に対応する。なお、Ｓ６０１～Ｓ６０９は各ステップを示し、また、各ステップは、画像形成装置１０３の機器制御部２０８、または情報処理装置１０１、１０２のＣＰＵ３０１が対応するメモリから制御プログラムを読み出して実行することで実現される。
【００８０】
なお、Ｕｓｅｒ－Ａから画像形成装置１０３への印刷を指示されたＰＤＦアプリケーション４０２は、情報処理装置１０１のログインサービス４０１を介して、認証サーバとして機能する情報処理装置１０２の認証認可サービス（ＡＡＳ）４０６からＵｓｅｒ－Ａの認証トークンを取得し、これをＰＤＦデータに添付して、画像形成装置１０３のＰＤＦプリントサービス（ＰＤＦＰ－Ｓ）４０４を呼び出す。
【００８１】
この呼び出しは、図５に一例を示した様に、Ｗ３Ｃ勧告のＳＯＡＰ１．２仕様に基づき、ＰＤＦデータをＢａｓｅ６４形式でエンコードしてＢｏｄｙに挿入すると共に、認証トークンをＯＡＳＩＳ Ｗｅｂ Ｓｅｒｖｉｃｅｓ Ｓｅｃｕｒｉｔｙ １．０仕様に基づいて、ＳＯＡＰ Ｈｅａｄｅｒに挿入したＳＯＡＰメッセージとして、画像形成装置１０３に送信される。
【００８２】

この呼び出しに対して、画像形成装置１０３のＳＯＡＰハンドラ４０３は、図８に示すステップＳ６０１で、情報処理装置１０２のＡＡＳ４０６に対してＳＯＡＰメッセージに添付された認証トークンを送信することで、当該トークンがＡＡＳ４０６により発行された正当なものかどうかをチェックすると共に、ＰＤＦＰ－Ｓ４０４に対する呼び出し許可が与えられているかどうかを図６に示したアクセス制御情報８０２等を参照してチェックする。

【００８３】

なお、呼び出し許可は、後述する図９に示すステップＳ５０１～Ｓ５０４、Ｓ５１０で判定される。

【００８４】

そして、ステップＳ６０２で、ＡＡＳ４０６から返答される内容が認証トークンが正当で、且つＰＤＦＰ－Ｓ４０４の呼び出し許可が与えられていることを示すかどうかを判断して、認証トークンが正当で、且つＰＤＦＰ－Ｓ４０４の呼び出し許可が与えられていると判断した場合は、ステップＳ６０３に進み、認証トークンが不正か、またはＰＤＦＰ－Ｓ４０４の呼び出し許可が与えられていないと判断した場合には、本処理を終了する。

【００８５】

そして、ステップＳ６０３で、前述の通り、予め呼び出すように構成されている、画像形成装置１０４に対して、受信したＰＤＦデータと認証トークンからなるＰＤＦｔｏＰＣＬ変換サービス（ＰＤＦｔｏＰＣＬ－Ｓ）４０８を呼び出すＳＯＡＰメッセージを送信する。

【００８６】

次に、ステップＳ６０４で、呼び出しが正常終了しているかどうかを判断して、正常終了していると判断した場合は、ステップＳ６０９へ進み、正常終了していないと判断した場合は、ステップＳ６０５に進む。

【００８７】

ここで、図９を参照して、情報処理装置１０１、１０２と画像形成装置１０４による処理について説明する。

【００８８】

図９は、本発明に係る画像処理システムにおける第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４に示した画像形成装置１０３からの呼び出し許可要求に対する画像形成装置１０４による応答処理手順、並びに、ＰＤＦｔｏＰＣＬ変換処理に対応する。なお、Ｓ５０１～Ｓ５１０は各ステップを示す。また、各ステップは、画像形成装置１０４の機器制御部２０８が対応するメモリから制御プログラムを読み出して実行することで実現される。

【００８９】

先ず、ステップＳ５０１で、画像形成装置１０３から呼び出し許可要求を受信しているかどうかを判断し、呼び出し許可要求を受信している場合は、ステップＳ５０２で、認証サーバとして機能する情報処理装置１０２のＡＡＳ４０６に対して、呼び出し許可要求に含まれる認証トークンと画像形成装置１０３のＩＰアドレスを送信する。認証トークンとＩＰアドレスを受信したＡＡＳ４０６は、認証トークンが示すサービスが正当かどうかをチェックすると共に、ＩＰアドレスが信頼デバイスリストに登録されているかどうかをチェックする。

【００９０】

そして、そのチェック結果として受信した認証トークンが正当なもので且つＩＰアドレスが信頼するデバイスのものであった場合は認証ＯＫを、正当なものでなければ認証ＮＧを返却する。ステップＳ５０３で認証がＯＫであるかどうかを判断して、ＯＫと判定された場合は、ステップＳ５０４で、呼び出し許可応答を画像形成装置１０３に返却して、本処理を終了する。

【００９１】

一方、ステップＳ５０３で認証ＮＧ（エラー）となった場合には、サービスを呼び出す

権限がないものと判定して、ステップＳ５１０で、エラー応答を画像形成装置１０３に返却して、本処理を終了する。

【００９２】

以上のステップＳ５０１～Ｓ５０４及びＳ５１０の処理により、画像形成装置１０３、画像形成装置１０４で動作するＰＤＦｔｏＰＣＬ－Ｓ４０８に対する呼び出し要求があった場合に、呼び出し要求に伴う認証トークンを情報処理装置１０２で動作するＡＡＳ４０６に送信し、この認証トークンを受信したＡＡＳ４０６は、認証トークンが正当なものかどうかを判定し、判定結果を画像形成装置１０４に返却し、判定が該認証トークンは正当なものであった場合に画像形成装置１０４は、呼び出し許可サービスリストを参照して、呼び出し要求が、要求を許可する様に登録されているサービスから送信されたかどうかに基づいて、サービス呼び出し要求に対しする許可あるいは拒否のいずれかの応答を、呼び出し元の画像形成装置１０３に対して返却することになる。なお、ＰＤＦｔｏＰＣＬ－Ｓ４０８の呼び出し元は、画像形成装置１０３に限定されるものでは無く、任意の画像形成装置あるいは情報処理装置で実行されるサービスからの呼び出しが可能であることは言うまでも無い。ただし、サービス呼び出し要求が許可されるのは、画像形成装置１０４のデータ保存部２１０で管理された呼び出し許可サービスリストに登録されたサービスに限定される。

【００９３】

一方、ステップＳ５０１で、呼び出し許可要求でないと判断した場合は、ステップＳ５０５以降へ進み、例えばＰＤＦｔｏＰＣＬ－Ｓ４０８の呼び出しを受信しているかどうかを判断して、ＰＤＦｔｏＰＣＬ－Ｓ４０８の呼び出しを受信したと判断した場合、すなわち、図９に示すステップＳ５０５で呼び出しを受信した画像形成装置１０４のＳＯＡＰハンドラ４０７は、図９に示すフローチャートのステップＳ５０６に進み、まず、図７の呼び出し許可サービスリストを参照して、呼び出し元の装置及びサービスが登録されているかどうかを判定し、登録されていない場合は、呼び出し拒否エラーを返却して処理を終了する。呼び出し許可サービスリストに登録されていた場合は、認証サーバとして機能する情報処理装置１０２のＡＡＳ４０６に受信した認証トークンを送信して、認証トークンの正当性とＰＤＦｔｏＰＣＬ－Ｓ４０８の呼び出しが許可されているかをチェックする。チェックは、図６の８０２に示したアクセス制御情報を参照して為され、認証トークンに対応するユーザあるいはサービスに対するアクセスが許可されていれば（図６の８０２でＯＫと記載されている項目に相当）認証ＯＫを、アクセスが禁止されていれば（図６の８０２でＮＧと記載されている項目に相当）認証ＮＧを、画像形成装置１０４のＳＯＡＰハンドラ４０７に返却する。

【００９４】

そして、そのチェック結果としてステップＳ５０７で認証がＯＫであるかどうかを判断して、ＯＫと判定された場合は、ステップＳ５０８で、ＰＤＦｔｏＰＣＬ－Ｓ４０８によるＰＤＦｔｏＰＣＬ変換処理を実行後、生成されたＰＣＬデータを画像形成装置１０３に返却して、本処理を終了する。

【００９５】

一方、ステップＳ５０７で認証に失敗したと判定した場合は、ステップＳ５０９で権限無しエラーを画像形成装置１０３に返却して、画像形成装置１０４のＰＤＦｔｏＰＣＬ－Ｓ４０８の呼び出しに関する処理を終了する。

【００９６】

図８に戻り、ステップＳ６０４で、画像形成装置１０３がＰＤＦｔｏＰＣＬ－Ｓ４０８の呼び出し結果が正常終了であると判断した場合は、ステップＳ６０９に進み、画像形成装置１０４から返却されたＰＤＦデータをプリントエンジン４０５に渡して印刷を行い、本処理を終了する。

【００９７】

一方、ステップＳ６０４で、正常終了以外の値が返ったと判定された場合は、ステップＳ６０５で、権限なしエラーが返ったかどうかを判定し、権限なしエラー以外の値が返っ

ている場合（ＮＯの場合）は、本処理を終了する。

【００９８】

また、ステップＳ６０５で、権限なしエラーが返ったと判定した場合（ＹＥＳの場合）は、ステップＳ６０６で、前記ＰＤＦＰ－Ｓ４０４を画像形成装置１０３にインストールする際に、画像形成装置１０３のデータ保存部２１０に保存したＰＤＦＰ－Ｓ４０４のユーザ名とパスワードを取り出し、認証サーバとしての情報処理装置１０２のＡＡＳ４０６に送信することで、ＰＤＦＰ－Ｓ４０４の認証トークンを取得する。

【００９９】

そして、ステップＳ６０７で、情報処理装置１０２から取得したＰＤＦＰ－Ｓ４０４の認証トークンとＰＤＦデータを添付した、画像形成装置１０４のＰＤＦｔｏＰＣＬ－Ｓ４０８を呼び出すＳＯＡＰメッセージをＳＯＡＰハンドラ４０３を介して画像形成装置１０４に送信する。

【０１００】

これを受けて、ＰＤＦｔｏＰＣＬ－Ｓ４０８の呼び出しＳＯＡＰメッセージを受信した画像形成装置１０４のＳＯＡＰハンドラ４０７は、図９に示すフローチャートのステップＳ５０６以降の処理を実行するが、ＰＤＦＰ－Ｓ４０４を画像形成装置１０３にインストールする際に、ＰＤＦＰ－Ｓ４０４に対して画像形成装置１０４のＰＤＦｔｏＰＣＬ－Ｓ４０８の呼び出しが許可されている（図６に示すアクセス制御情報８０２参照）ことから、ステップＳ５０７で認証ＯＫと判定され、ステップＳ５０８でサービス呼び出しと共に受信したＰＤＦデータはＰＣＬデータに変換されて、正常終了として、呼び出し処理が完了する。

【０１０１】

そして、図８に示すステップＳ６０８に戻り、ＰＤＦｔｏＰＣＬ－Ｓ４０８の呼び出しが正常終了した場合は、ステップＳ６０９で、画像形成装置１０４で変換処理されたＰＣＬデータの印刷処理を行い、エラー終了した場合は、ＰＤＦＰ４０４の呼び出し処理を終了する。

【０１０２】

なお、ＰＤＦＰ－Ｓ４０４から画像形成装置１０４のＰＤＦｔｏＰＣＬ－Ｓ４０８を呼び出す際に、ユーザの認証トークンを使わずに、常にＰＤＦＰ－Ｓ４０４の認証トークンを添付することも可能であるが、この場合、画像形成装置１０４から更に別の装置で動作するサービスを実行するように構成が変更された場合に、そのサービスの実行権限はＰＤＦＰ－Ｓ４０４の認証トークンに対しては与えられておらず、Ｕｓｅｒ－Ａの認証トークンに対して実行権限が付与されている可能性があるため、まずユーザの認証トークンによるサービス実行を試行し、権限がなかった場合に、サービスの認証トークンを設定してサービス実行するものである。

【０１０３】

以上、説明したように本実施形態によれば、複数台の情報処理装置及び画像形成装置から構成される画像処理システムにおいて、あるサービスが別のサービスを呼び出す様に構成されており、最初に呼び出されるサービスに対する実行権限を持つユーザが、その先に呼び出される別のサービス（本実施形態では、情報処理装置１０１のユーザが情報処理装置１０２で認証サービスを受け、画像形成装置１０３のＰＤＦプリントサービスを実行する権限を持つが、画像形成装置１０４のＰＤＦｔｏＰＣＬ変換サービスを実行する権限を持たない場合を例とする）を実行する権限を持たない場合でも、ユーザの認証トークンの代わりに、呼び出し元サービスの認証トークンを用いることにより、一連のサービス実行を可能にするものである。

【０１０４】

なお、本実施形態では、異なる画像形成装置にＰＤＦプリントサービス４０４とＰＤＦｔｏＰＣＬ変換サービス４０８が配置された場合に関して述べてきたが、同一の画像形成装置に配置されている場合や、両方あるいは何れか一方が情報処理装置上に配置された場合であっても本実施形態を実現可能であることは言うまでも無い。

【０１０５】
〔第２実施形態〕
第１実施形態では、Ｕｓｅｒ－Ａが画像形成装置１０４で動作するＰＤＦｔｏＰＣＬ－Ｓ４０８へのアクセス権を所有しない場合に、画像形成装置１０３で動作し、Ｕｓｅｒ－Ａに対するアクセス権を許可するように構成されたＰＤＦＰＳ４０４の認証トークンを添付することにより、ＰＤＦｔｏＰＣＬ－Ｓ４０８へのアクセスを可能にする場合について説明したが、この場合には、Ｕｓｅｒ－Ａに対してＰＤＦｔｏＰＣＬ－Ｓ４０８へのアクセス権が与えられない限りは、ＰＤＦＰ－Ｓ４０４からＰＤＦｔｏＰＣＬ－Ｓ４０８の一度目の呼び出しは必ず権限なしエラーで失敗する（図８に示したステップＳ６０５で、権限なしとなる）ことになる。
【０１０６】
そこで、本実施形態では、ＰＤＦＰ－Ｓ４０４がＰＤＦｔｏＰＣＬ－Ｓ４０８の呼び出しに失敗したことを検出すると、該呼び出しに用いられた認証トークンに対応するユーザ名を画像形成装置１０３のデータ保存部２１０に保存し、以降でＰＤＦｔｏＰＣＬ－Ｓ４０８を呼び出す際に、情報処理装置１０１から受信した認証トークンに対応するユーザが、先に、画像形成装置１０３のデータ保存部２１０に保存したユーザ名と一致する場合には、図８に示したフローチャートのステップＳ６０２で認証トークンが正当で且つ認証トークンが示すユーザにアクセス権限が無いと判定すると、ステップＳ６０６に進み、ＰＤＦＰＳ４０４の認証トークンを情報処理装置１０２のＡＡＳ４０６から取得して、これを添付して画像形成装置１０４のＰＤＦｔｏＰＣＬ－Ｓ４０８を呼び出しても良い。
【０１０７】
このように、本発明の第２の実施形態によれば、呼び出し先サービスの実行権限を所有しないユーザを予め検出し、該ユーザからの呼び出しを受信した場合に、呼び出し元サービスのトークンを取得し、これを添付したサービス呼び出しを行うことにより、呼び出し先のサービスの実行権限が無いユーザからの要求が、権限なしエラーで失敗することを回避し、処理の高速化を計ることが可能となる。
【０１０８】
このように権限なしエラーとなるユーザを画像形成装置１０３において検出し、このユーザのトークンが含まれるサービ呼び出しを受信した場合には、はじめからＰＤＦＰ－Ｓ４０４のトークンを取得して、これを画像形成装置１０４のＰＤＦｔｏＰＣＬサービス１０４呼び出しに添付することで、権限無し時の検証オーバヘッドを解消することも可能になる。
【０１０９】
〔第３実施形態〕
なお、上記実施形態では、Ｕｓｅｒ－ＡがＰＤＦｔｏＰＣＬ－Ｓ４０８へのアクセス権を所有しない場合に、ＰＤＦＰＳ４０４の認証トークンを添付することにより、ＰＤＦｔｏＰＣＬ－Ｓ４０８へのアクセスを可能にする場合について説明したが、ユーザレベルに代えて、複数のユーザに割当てられているグループを単位としてグループ認証を行う場合にも本発明を適用可能である。
【０１１０】
〔第４実施形態〕
なお、上記実施形態では、Ｕｓｅｒ－ＡがＰＤＦｔｏＰＣＬ－Ｓ４０８へのアクセス権を所有しない場合に、ＰＤＦＰ－Ｓ４０４の認証トークンを添付することにより、ＰＤＦｔｏＰＣＬ－Ｓ４０８へのアクセスを可能にする場合について説明したが、最初のユーザ認証情報で特定画像処理サービス要求を画像形成装置１０４が否定した際に、上記ＰＤＦＰ－Ｓ４０４の認証トークンの代わりに、デバイスとしての認証情報（あらかじめ情報処理装置１０２に登録されているものとする）を添付して画像形成装置１０４に同様の画像処理サービスを要求させ、そのデバイスとしての認証情報を情報処理装置１０２で記憶される信頼性デバイステーブルに登録されたデバイス情報と照合することで、その特定画像処理サービスの要求の可否を決定することで、同様の認証結果を得るように構成してもよ

い。
【０１１１】
これにより、特定画像処理サービス要求に限らず、デバイスとしての認証情報を利用したネットワーク上の各画像形成装置に対するアクセス権管理も可能となる。
【０１１２】
〔第５実施形態〕
以下、図１０に示すメモリマップを参照して本発明に係る印刷装置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。
【０１１３】
図１０は、本発明に係る印刷装置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。
【０１１４】
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。
【０１１５】
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。
【０１１６】
本実施形態における図８，図９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。
【０１１７】
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。
【０１１８】
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。
【０１１９】
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。
【０１２０】
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。
【０１２１】
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。
【０１２２】
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。

【０１２３】

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。

【０１２４】

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。

【０１２５】

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。

【０１２６】

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。

【０１２７】

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のではなく、以下の実施態様も含まれることはいうまでもない。

【０１２８】

上記第１実施形態における画像形成システムは、画像処理要求を行う情報端末と、複数の画像形成装置に対するユーザまたは各画像形成装置が提供するサービスの権限の認証を行う認証情報端末と該情報端末に接続可能な画像形成装置とが互いに通信可能な画像形成システムであって、情報端末（例えば図１に示す情報処理装置１０１）は、ログインする各ユーザに対するユーザ認証情報を前記認証情報端末から取得して、いずれかの画像形成装置に対して、該取得されるユーザ認証情報とともに画像形成装置が提供する画像処理サービス要求を出力するサービス要求手段（ログインサービス４０１）とを備え、認証情報端末（例えば図１に示す情報処理装置１０２）は、前記情報端末からのユーザ接続認証または各画像形成装置からのユーザ権限認証を行うユーザ認証手段（例えば図４に示すＡＡＳ４０６）と、いずれかの画像形成装置からのサービス権限認証を行うサービス認証手段（例えば図４に示すＡＡＳ４０６）とを備え、いずれかの画像形成装置（例えば図１に示す画像形成装置１０３）は、前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求手段（例えば図４に示すＳＯＡＰハンドラ４０３）と、前記第１のサービス要求手段に対する他の画像形成装置からの特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される自機のサービス認証情報を伴って前記特定画像処理サービス要求を画像形成装置に再出力する第２のサービス要求手段（例えば図

４に示すＳＯＡＰハンドラ４０３）と、前記第２のサービス要求手段による要求に対して他の画像形成装置により生成される出力情報を取得する取得手段（例えば図４に示すＳＯＡＰハンドラ４０３）と、前記取得手段により取得される出力情報を画像出力する出力手段（例えば図４に示すプリンタエンジン４０５）とを備え、いずれか他の画像形成装置（例えば図４に示す画像形成装置１０４）画像形成装置から取得するユーザ認証情報に対して前記認証情報端末での認証を要求するユーザ認証要求手段（例えば図４に示すＳＯＡＰハンドラ４０７）と、画像形成装置から取得するサービス認証情報に対して前記認証情報端末での認証を要求するサービス認証要求手段（例えば図４に示すＳＯＡＰハンドラ４０７）と、前記ユーザ認証要求手段または前記サービス認証要求手段による前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行手段（例えば図４に示すＰＤＦｔｏＰＣＬ－Ｓ）と、前記サービス実行手段により生成される出力情報をサービス要求元の画像形成装置に返信する返信手段（例えば図４に示すＳＯＡＰハンドラ４０７）とを備えることを特徴としてもよい。

【０１２９】

これにより、情報処理装置から特定画像処理サービスを伴う要求を画像形成装置が受け付けた場合に、ユーザ認証により、特定画像処理サービスに対するユーザ権限がないために、他の画像形成装置に特定画像処理サービスを委譲できない場合でも、要求元の画像形成装置に登録されている特定画像処理サービスに設定されているサービス認証情報に基づいて、他の画像形成装置が認証された場合には、要求される特定画像処理サービスを実行して、各画像形成装置が連携して複合画像処理を継続することできる。したがって、ネットワーク上の画像形成装置に対するユーザ権限では利用できない画像形成装置であっても、一方の画像形成装置でユーザ認証されている場合には、それに一定の信頼性を認めて、該画像形成装置におけるサービス認証情報を利用して利用権限を連携する画像形成装置で認証することで、ネットワークの資源を有効に活用した画像処理を行える。

【０１３０】

また、上記第１実施形態における画像形成システムにおいて、前記ユーザ認証要求手段によるユーザ認証結果に基づいて前記特定画像処理サービスを実行できないユーザであると認証された場合に、他の画像形成装置から返信されるユーザ認証情報を保存するデータ保存手段（例えば図２に示したデータ保存部２１０）を備え、前記第２のサービス要求手段は、第１のサービス要求手段に代えて、前記他の画像形成装置に対して前記サービス認証情報を伴う特定画像処理サービスを要求することを特徴とする構成としてもよい。

【０１３１】

これにより、ユーザ認証では利用できないユーザから同様の特定画像処理サービスを受け付けた場合に、他の画像形成装置から同様なユーザ認証では利用できないという認証処理を行うことなく、最初からサービス認証情報を伴う特定画像処理サービス要求を他の画像形成装置に行うことが可能となり、無駄なトラフィックを行うことなく、速やかに意図する特定画像処理サービスを他の画像処理装置に要求して、他の画像形成装置と連携した複合画像処理を効率よく行うことができる。

【０１３２】

また、上記第１実施形態における画像形成システムにおいて、前記画像形成装置は、特定画像処理サービスの実行要求を所定のメッセージ形式で情報端末より受信することを特徴とする構成としても良い。

【０１３３】

これにより、ネットワーク上の各機器相互の通信規約との制限に左右されずに、画像処理サービスを連携するシステムを構築することができる。

【０１３４】

また、上記第１実施形態における画像形成システムにおいて、前記所定のメッセージ形式は、ＳＯＡＰメッセージ形式であることを特徴とする構成としてもよい。

【０１３５】

これにより、ネットワーク上の各機器相互の通信規約との制限に左右されずに、画像処

理サービスを連携する汎用性の高いシステムを自在に構築することができる。

【０１３６】

また、上記第１実施形態における画像形成システムにおいて、前記サービス要求手段は、所定のアプリケーション（例えば図４に示すＰＤＦアプリ４０２）を実行時に、ログインする各ユーザに対するユーザ認証情報を前記認証情報端末から取得して、いずれかの画像形成装置に対して、該取得されるユーザ認証情報とともに画像形成装置が提供する画像処理サービス要求を出力することを特徴とする構成としても良い。

【０１３７】

これにより、ログイン時に取得されるユーザ認証情報を伴う所定のアプリ実行時に、画像処理サービス要求を確実に画像形成装置に出力することができる。

【０１３８】

また、上記第１実施形態における画像形成システムの画像形成装置は、情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置であって、前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求手段（例えば図４に示すＳＯＡＰハンドラ４０３）と、前記第１のサービス要求手段に対する他の画像形成装置からの特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される記憶されている自機のサービス認証情報を伴って前記特定画像処理サービス要求を画像形成装置に再出力する第２のサービス要求手段（例えば図４に示すＳＯＡＰハンドラ４０３）と、前記第２のサービス要求手段による要求に対して他の画像形成装置により生成される出力情報を取得する取得手段（例えば図４に示すＳＯＡＰハンドラ４０３）と、前記取得手段により取得される出力情報を画像出力する出力手段（例えば図４に示すプリンタエンジン４０５）とを有することを特徴とする構成としても良い。

【０１３９】

これにより、情報処理装置から特定画像処理サービスを伴う要求を画像形成装置が受け付けた場合に、ユーザ認証により、特定画像処理サービスに対するユーザ権限がないために、他の画像形成装置に特定画像処理サービスを委譲できない場合でも、要求元の画像形成装置に登録されている特定画像処理サービスに設定されているサービス認証情報に基づいて、他の画像形成装置が認証された場合には、要求される特定画像処理サービスを実行して、各画像形成装置が連携して複合画像処理を継続することできる。したがって、ネットワーク上の画像形成装置に対するユーザ権限では利用できない画像形成装置であっても、一方の画像形成装置でユーザ認証されている場合には、それに一定の信頼性を認めて、該画像形成装置におけるサービス認証情報を利用して利用権限を連携する画像形成装置で認証することで、ネットワークの資源を有効に活用した画像処理を行える。

【０１４０】

また、上記第１実施形態における画像形成システムの画像形成装置は、情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置であって、画像形成装置から取得するユーザ認証情報に対して前記認証情報端末での認証を要求するユーザ認証要求手段（例えば図４に示すＳＯＡＰハンドラ４０７）と、画像形成装置から取得するサービス認証情報に対して前記認証情報端末での認証を要求するサービス認証要求手段（例えば図４に示すＳＯＡＰハンドラ４０７）と、前記ユーザ認証要求手段または前記サービス認証要求手段による前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行手段（例えば図４に示すＰＤＦｔｏＰＣＬ－Ｓ４０８）と、前記サービス実行手段により生成される出力情報をサービス要求元の画像形成装置に返信する返信手段（例えば図４に示すＳＯＡＰハンドラ４０７）とを有することを特徴とする構成としてもよい。

【０１４１】

これにより、情報処理装置から特定画像処理サービスを伴う要求を画像形成装置が受け

付けた場合に、ユーザ認証により、特定画像処理サービスに対するユーザ権限がないために、他の画像形成装置に特定画像処理サービスを委譲できない場合でも、要求元の画像形成装置に登録されている特定画像処理サービスに設定されているサービス認証情報に基づいて、他の画像形成装置が認証された場合には、要求される特定画像処理サービスを実行して、各画像形成装置が連携して複合画像処理を継続することできる。したがって、ネットワーク上の画像形成装置に対するユーザ権限では利用できない画像形成装置であっても、一方の画像形成装置でユーザ認証されている場合には、それに一定の信頼性を認めて、該画像形成装置におけるサービス認証情報を利用して利用権限を連携する画像形成装置で認証することで、ネットワークの資源を有効に活用した画像処理を行える。

【０１４２】

また、上記第１実施形態における画像形成システムの画像形成装置は、前記ユーザ認証要求手段によるユーザ認証結果に基づいて前記特定画像処理サービスを実行できないユーザであると認証された場合に、他の画像形成装置から返信されるユーザ認証情報を保存するデータ保存手段（例えば図２に示すデータ保存部２１０）を備え、前記第２のサービス要求手段は、第１のサービス要求手段に代えて、前記他の画像形成装置に対して前記サービス認証情報を伴う特定画像処理サービスを要求することを特徴とする構成としても良い。

【０１４３】

これにより、ユーザ認証では利用できないユーザから同様の特定画像処理サービスを受け付けた場合に、他の画像形成装置から同様なユーザ認証では利用できないという認証処理を行うことなく、最初からサービス認証情報を伴う特定画像処理サービス要求を他の画像形成装置に行うことが可能となり、無駄なトラフィックを行うことなく、速やかに意図する特定画像処理サービスを他の画像処理装置に要求して、他の画像形成装置と連携した複合画像処理を効率よく行うことができる。

【０１４４】

また、上記第１実施形態における画像形成システムの画像形成装置は、前記画像形成装置は、特定画像処理サービスの実行要求を所定のメッセージ形式で情報端末より受信することを特徴とする構成としてもよい

これにより、ネットワーク上の各機器相互の通信規約との制限に左右されずに、画像処理サービスを連携するシステムを構築することができる。

【０１４５】

また、上記第１実施形態における画像形成システムの画像形成装置は、前記所定のメッセージ形式は、ＳＯＡＰメッセージ形式であることを特徴とする構成としてもよい。

【０１４６】

これにより、ネットワーク上の各機器相互の通信規約との制限に左右されずに、画像処理サービスを連携する汎用性の高いシステムを自在に構築することができる。

【０１４７】

また、上記第１実施形態における画像形成システムにおけるサービス連携処理方法は、画像処理要求を行う情報端末と、複数の画像形成装置に対するユーザまたは各画像形成装置が提供するサービスの権限の認証を行う認証情報端末と該情報端末に接続可能な画像形成装置とが互いに通信可能な画像形成システムにおけるサービス連携処理方法であって、情報端末は、ログインする各ユーザに対するユーザ認証情報を前記認証情報端末から取得して、いずれかの画像形成装置に対して、該取得されるユーザ認証情報とともに画像形成装置が提供する画像処理サービス要求を出力するサービス要求ステップを備え、認証情報端末は、前記情報端末からのユーザ接続認証または各画像形成装置からのユーザ権限認証を行うユーザ認証ステップと、いずれかの画像形成装置からのサービス権限認証を行うサービス認証ステップとを備え、いずれかの画像形成装置は、前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求ステップ（図８に示すステップＳ６０３）と、前記第１のサービス要求ステップに対する他の画像形成装置からの

特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される自機のサービス認証情報を伴って前記特定画像処理サービス要求を画像形成装置に再出力する第２のサービス要求ステップ（図８に示すステップＳ６０７）と、前記第２のサービス要求ステップによる要求に対して他の画像形成装置により生成される出力情報を取得する取得ステップ（図８に示すステップＳ６０９）と、前記取得ステップにより取得される出力情報を画像出力する出力ステップ（図８に示すステップＳ６０７）とを備え、いずれか他の画像形成装置は、画像形成装置から取得するユーザ認証情報に対して前記認証情報端末での認証を要求するユーザ認証要求ステップ（図９に示すステップＳ５０６）と、画像形成装置から取得するサービス認証情報に対して前記認証情報端末での認証を要求するサービス認証要求ステップ（図９に示すステップＳ５０６）と、前記ユーザ認証要求ステップまたは前記サービス認証要求ステップによる前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行ステップ（図９に示すステップＳ５０８）と、前記サービス実行ステップにより生成される出力情報をサービス要求元の画像形成装置に返信する返信ステップとを備えることを特徴とする構成としても良い。

【０１４８】

これにより、情報処理装置から特定画像処理サービスを伴う要求を画像形成装置が受け付けた場合に、ユーザ認証により、特定画像処理サービスに対するユーザ権限がないために、他の画像形成装置に特定画像処理サービスを委譲できない場合でも、要求元の画像形成装置に登録されている特定画像処理サービスに設定されているサービス認証情報に基づいて、他の画像形成装置が認証された場合には、要求される特定画像処理サービスを実行して、各画像形成装置が連携して複合画像処理を継続することできる。したがって、ネットワーク上の画像形成装置に対するユーザ権限では利用できない画像形成装置であっても、一方の画像形成装置でユーザ認証されている場合には、それに一定の信頼性を認めて、該画像形成装置におけるサービス認証情報を利用して利用権限を連携する画像形成装置で認証することで、ネットワークの資源を有効に活用した画像処理を行える。

【０１４９】

また、上記画像形成システムにおけるサービス連携処理方法において、前記ユーザ認証要求ステップによるユーザ認証結果に基づいて前記特定画像処理サービスを実行できないユーザであると認証された場合に、他の画像形成装置から返信されるユーザ認証情報をデータ保存手段（例えば図２に示すデータ保存部２１０）に保存する保存ステップを備え、前記第２のサービス要求ステップは、第１のサービス要求手段に代えて、前記他の画像形成装置に対して前記サービス認証情報を伴う特定画像処理サービスを要求することを特徴とする構成としてもよい。

【０１５０】

これにより、ユーザ認証では利用できないユーザから同様の特定画像処理サービスを受け付けた場合に、他の画像形成装置から同様なユーザ認証では利用できないという認証処理を行うことなく、最初からサービス認証情報を伴う特定画像処理サービス要求を他の画像形成装置に行うことが可能となり、無駄なトラフィックを行うことなく、速やかに意図する特定画像処理サービスを他の画像処理装置に要求して、他の画像形成装置と連携した複合画像処理を効率よく行うことができる。

【０１５１】

さらに、上記画像形成システムにおけるサービス連携処理方法において、前記画像形成装置は、特定画像処理サービスの実行要求を所定のメッセージ形式で情報端末より受信することを特徴とする構成としてもよい。

【０１５２】

これにより、ネットワーク上の各機器相互の通信規約との制限に左右されずに、画像処理サービスを連携するシステムを構築することができる。

【０１５３】

さらに、上記画像形成システムにおけるサービス連携処理方法において、前記所定のメッセージ形式は、ＳＯＡＰメッセージ形式であることを特徴とする構成としてもよい。

【０１５４】
これにより、ネットワーク上の各機器相互の通信規約との制限に左右されずに、画像処理サービスを連携する汎用性の高いシステムを自在に構築することができる。
【０１５５】
また、上記画像形成システムにおけるサービス連携処理方法において、前記サービス要求ステップは、所定のアプリケーションを実行時に、ログインする各ユーザに対するユーザ認証情報を前記認証情報端末から取得して、いずれかの画像形成装置に対して、該取得されるユーザ認証情報とともに画像形成装置が提供する画像処理サービス要求を出力することを特徴とする構成としてもよい。
【０１５６】
これにより、ログイン時に取得されるユーザ認証情報を伴う所定のアプリ実行時に、画像処理サービス要求を確実に画像形成装置に出力することができる。
【０１５７】
さらに、上記第１実施形態における画像形成装置におけるサービス連携処理方法は、情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置におけるサービス連携処理方法であって、前記情報端末から取得する前記ユーザ認証情報に対して前記認証情報端末で認証されるユーザ権限認証を伴う特定画像処理サービス要求を他の画像形成装置に行う第１のサービス要求ステップ（図８に示すステップＳ６０３）と、前記第１のサービス要求ステップに対する他の画像形成装置からの特定画像処理サービス要求応答に基づいて、前記認証情報端末で認証される記憶されている自機のサービス認証情報を伴って前記特定画像処理サービス要求を画像形成装置に再出力する第２のサービス要求ステップ（図８に示すステップＳ６０７）と、前記第２のサービス要求ステップによる要求に対して他の画像形成装置により生成される出力情報を取得する取得ステップ（図８に示すステップＳ６０７）と、前記取得ステップにより取得される出力情報を画像出力する出力ステップ（図８に示すステップＳ６０９）とを有することを特徴とする構成としてもよい。
【０１５８】
これにより、情報処理装置から特定画像処理サービスを伴う要求を画像形成装置が受け付けた場合に、ユーザ認証により、特定画像処理サービスに対するユーザ権限がないために、他の画像形成装置に特定画像処理サービスを委譲できない場合でも、要求元の画像形成装置に登録されている特定画像処理サービスに設定されているサービス認証情報に基づいて、他の画像形成装置が認証された場合には、要求される特定画像処理サービスを実行して、各画像形成装置が連携して複合画像処理を継続することできる。したがって、ネットワーク上の画像形成装置に対するユーザ権限では利用できない画像形成装置であっても、一方の画像形成装置でユーザ認証されている場合には、それに一定の信頼性を認めて、該画像形成装置におけるサービス認証情報を利用して利用権限を連携する画像形成装置で認証することで、ネットワークの資源を有効に活用した画像処理を行える。
【０１５９】
上記画像形成装置におけるサービス連携処理方法において、情報端末から画像処理要求を受け、認証情報端末でユーザ認証されるユーザからの特定画像処理サービスを他の画像形成装置によるサービスと連携して処理可能な画像形成装置におけるサービス連携処理方法であって、画像形成装置から取得するユーザ認証情報に対して前記認証情報端末での認証を要求するユーザ認証要求ステップ（図９に示すステップＳ５０６）と、画像形成装置から取得するサービス認証情報に対して前記認証情報端末での認証を要求するサービス認証要求ステップ（図９に示すステップＳ５０６）と、前記ユーザ認証要求ステップまたは前記サービス認証要求ステップによる前記認証情報端末での認証結果に基づいて特定画像処理サービスを実行するサービス実行ステップ（図９に示すステップＳ５０８）と、前記サービス実行ステップにより生成される出力情報をサービス要求元の画像形成装置に返信する返信ステップ（図９に示すステップＳ５０８）とを有することを特徴とする構成とし

てもよい。

【０１６０】

これにより、情報処理装置から特定画像処理サービスを伴う要求を画像形成装置が受け付けた場合に、ユーザ認証により、特定画像処理サービスに対するユーザ権限がないために、他の画像形成装置に特定画像処理サービスを委譲できない場合でも、要求元の画像形成装置に登録されている特定画像処理サービスに設定されているサービス認証情報に基づいて、他の画像形成装置が認証された場合には、要求される特定画像処理サービスを実行して、各画像形成装置が連携して複合画像処理を継続することできる。

【０１６１】

したがって、ネットワーク上の画像形成装置に対するユーザ権限では利用できない画像形成装置であっても、一方の画像形成装置でユーザ認証されている場合には、それに一定の信頼性を認めて、該画像形成装置におけるサービス認証情報を利用して利用権限を連携する画像形成装置で認証することで、ネットワークの資源を有効に活用した画像処理を行える。

【０１６２】

また、画像形成装置におけるサービス連携処理方法において、前記ユーザ認証要求ステップによるユーザ認証結果に基づいて前記特定画像処理サービスを実行できないユーザであると認証された場合に、他の画像形成装置から返信されるユーザ認証情報をデータ保存手段に保存するデータ保存ステップを備え、前記第２のサービス要求ステップは、第１のサービス要求ステップに代えて、前記他の画像形成装置に対して前記サービス認証情報を伴う特定画像処理サービスを要求することを特徴とする構成としてもよい。

【０１６３】

これにより、ユーザ認証では利用できないユーザから同様の特定画像処理サービスを受け付けた場合に、他の画像形成装置から同様なユーザ認証では利用できないという認証処理を行うことなく、最初からサービス認証情報を伴う特定画像処理サービス要求を他の画像形成装置に行うことが可能となり、無駄なトラフィックを行うことなく、速やかに意図する特定画像処理サービスを他の画像処理装置に要求して、他の画像形成装置と連携した複合画像処理を効率よく行うことができる。

【０１６４】

さらに、画像形成装置におけるサービス連携処理方法において、前記画像形成装置は、特定画像処理サービスの実行要求を所定のメッセージ形式で情報端末より受信することを特徴とする構成としてもよい。

【０１６５】

これにより、ネットワーク上の各機器相互の通信規約との制限に左右されずに、画像処理サービスを連携するシステムを構築することができる。

【０１６６】

また、画像形成装置におけるサービス連携処理方法において、前記所定のメッセージ形式は、ＳＯＡＰメッセージ形式であることを特徴とする構成としてもよい。

【０１６７】

これにより、ネットワーク上の各機器相互の通信規約との制限に左右されずに、画像処理サービスを連携する汎用性の高いシステムを自在に構築することができる。

【０１６８】

さらに、画像形成装置におけるサービス連携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としてコンピュータが読み取り可能な記憶媒体に格納したことを特徴とする構成としてもよい。

【０１６９】

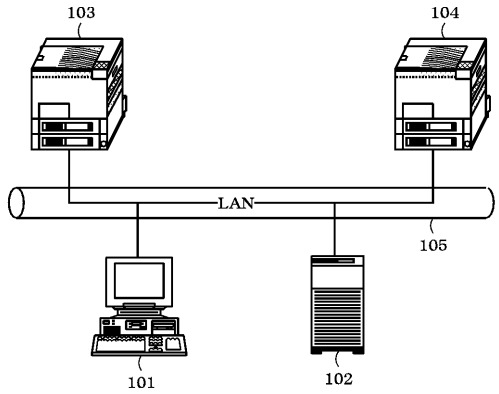
これにより、上述した効果を奏する。

【０１７０】

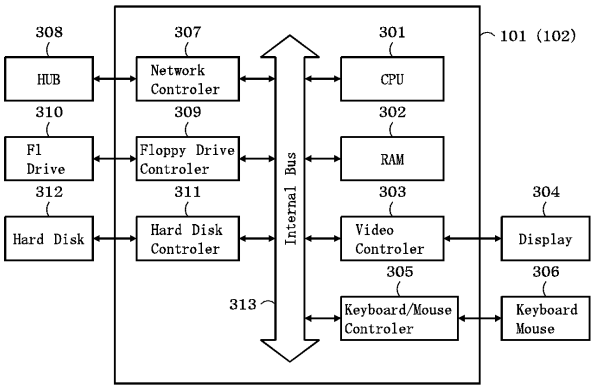
さらに、画像形成装置におけるサービス連携処理方法をコンピュータに実行させるためのプログラムとしたことを特徴とする構成としてもよい。

【０１７１】
　これにより、上述した効果を奏する。
【図面の簡単な説明】
【０１７２】
【図１】本発明の第１実施形態に係る画像形成装置を適用可能な画像処理システムのネットワーク構成を示す図である。
【図２】本発明の第１実施形態を示す画像形成装置の構成を説明するブロック図である。
【図３】図１に示した情報処理装置の内部構成の一例を示すブロック図である。
【図４】図１に示した情報処理装置と画像形成装置から構成されるシステムのモジュールを説明するブロック図である。
【図５】図１に示した情報処理装置から画像形成装置のサービス、画像形成装置間のサービスで送受信されるＳＯＡＰメッセージの一例を示す図である。
【図６】図１に示した情報処理装置により管理されるアクセス制御情報の一例を示す図である。
【図７】図１に示した画像形成装置が管理する呼び出し許可サービスリストの一例を示す図である。
【図８】本発明に係る画像処理システムにける第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９】本発明に係る画像処理システムにける第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１０】本発明に係る画像処理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】
【０１７３】
１０１、１０２　情報処理装置
１０３、１０４　画像形成装置
４０３、４０７　ＳＯＡＰハンドラ
４０４　ＰＤＦＰ－Ｓ
４０６　ＡＡＳ
４０８　ＰＤＦｔｏＰＣＬ－Ｓ

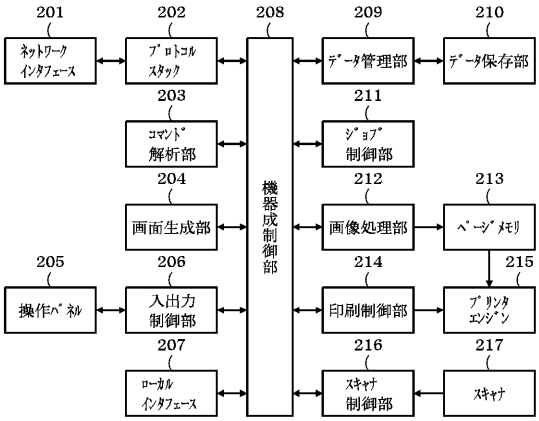
【図１】


103
104
LAN
105
101
102

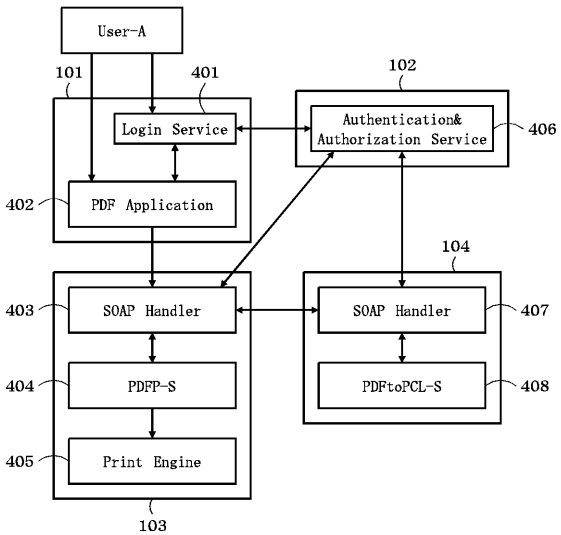
【図３】


308
HUB
307
Network Controler
301
CPU
101 (102)
310
Fl Drive
309
Floppy Drive Controler
302
RAM
312
Hard Disk
311
Hard Disk Controler
Internal Bus
303
Video Controler
304
Display
305
313
Keyboard/Mouse Controler
306
Keyboard Mouse

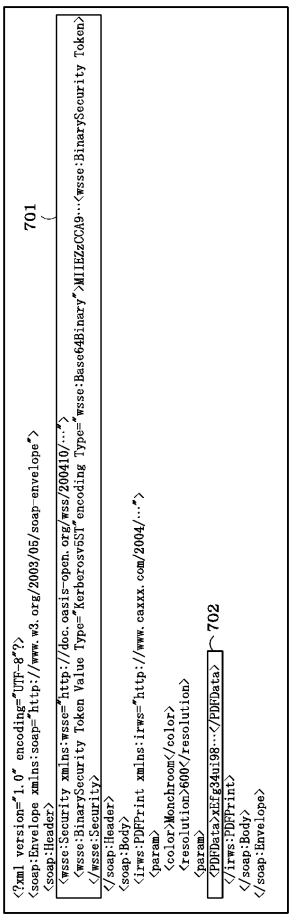
【図２】


201
ネットワーク インタフェース
202
プロトコル スタック
208
209
データ管理部
210
データ保存部
203
コマンド 解析部
211
ジョブ 制御部
204
画面生成部
212
画像処理部
213
ページメモリ
205
操作パネル
206
入出力 制御部
機器成制御部
214
印刷制御部
215
プリンタ エンジン
207
ローカル インタフェース
216
スキャナ 制御部
217
スキャナ

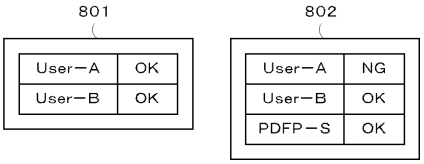
【図４】


User-A
101
401
102
Login Service
Authentication& Authorization Service
406
402
PDF Application
104
403
SOAP Handler
SOAP Handler
407
404
PDFP-S
PDFtoPCL-S
408
405
Print Engine
103

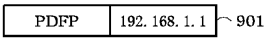
【図５】


701
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
<soap:Header>
<wsse:Security xmlns:wsse="http://doc.oasis-open.org/wss/200410/…">
<wsse:BinarySecurity Token Value Type="wsse:Base64Binary">MIIEZzCCA9…</wsse:BinarySecurity Token>
</wsse:Security>
</soap:Header>
<soap:Body>
<irws:PDFPrint xmlns:irws="http://www.caxxx.com/2004/…">
<param>
<color>Monchrome</color>
<resolution>600</resolution>
<param>
<PDFData>xEfg34u198…</PDFData>
702
</irws:PDFPrint>
</soap:Body>
</soap:Envelope>

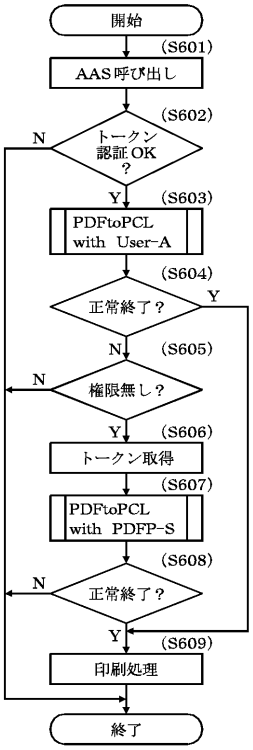
【図６】



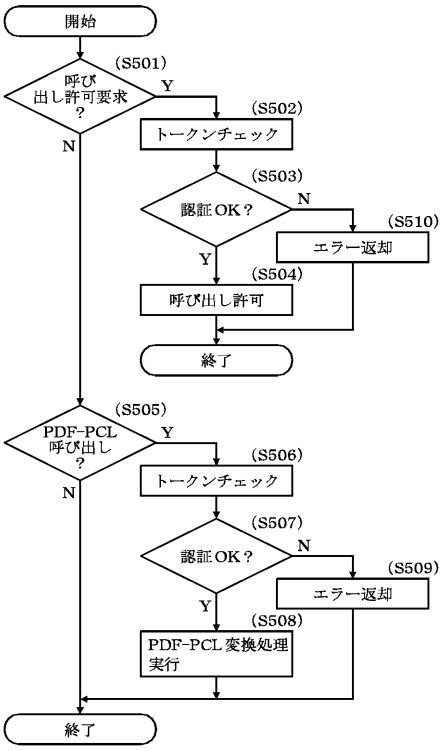
【図７】



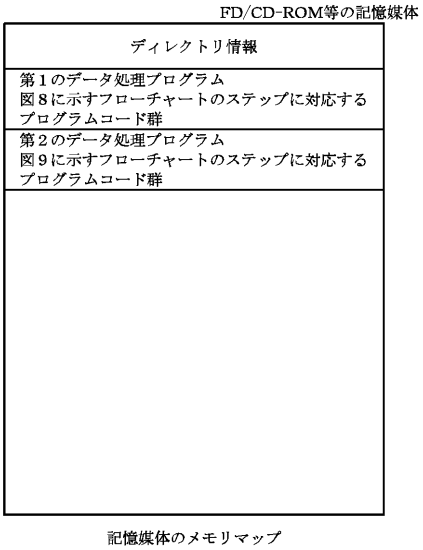
【図８】



【図９】



【図１０】



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２００４－２８９５００（ＪＰ，Ａ）
特開２００４－１９９２７３（ＪＰ，Ａ）
特開２００２－２５９１００（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　３／１２