(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4868724号
(P4868724)
(45)発行日　平成24年2月1日(2012.2.1)　(24)登録日　平成23年11月25日(2011.11.25)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330A
G09C 1/00 (2006.01)　　G09C 1/00 640E

請求項の数 12　(全 31 頁)

(21)出願番号　特願2004-253198(P2004-253198)
(22)出願日　平成16年8月31日(2004.8.31)
(65)公開番号　特開2006-72548(P2006-72548A)
(43)公開日　平成18年3月16日(2006.3.16)
審査請求日　平成19年8月31日(2007.8.31)
審判番号　不服2010-20247(P2010-20247/J1)
審判請求日　平成22年9月8日(2010.9.8)

(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　100090273
弁理士　國分　孝悦
(72)発明者　西尾　雅裕
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

合議体
審判長　赤川　誠一
審判官　殿川　雅也
審判官　石井　茂和

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理方法及びそのプログラム

(57)【特許請求の範囲】
【請求項１】
外部端末からのサービスを識別するための識別情報を含むヘッダ部と、サービスの内容を示す属性情報を記述したボディ部とから構成される要求を受信した場合に、該要求に応じたサービスを実行するサービス手段を備えた情報処理装置であって、
前記サービスを実行する前に認証処理を実施する複数種類のセキュリティ手段と、
前記サービスに対応した認証処理の呼び出し手続きが記述された情報である第１の情報を格納する第１の格納手段と、
前記第１の格納手段から前記第１の情報を参照して、前記外部端末から受信した要求のヘッダ部を解析して得られる前記識別情報により識別されるサービスに対応した認証処理を前記複数種類のセキュリティ手段の少なくとも何れかに実施させる機能及び、当該セキュリティ手段から認証処理の結果を受け取り出力する機能を備える調停処理手段と、
前記調停処理手段が出力する前記認証処理の結果に応じて、前記外部端末から受信した要求のボディ部を解析して得られる前記属性情報を用いたサービスを行うために、前記サービス手段に対してサービスを呼び出す呼び出し手段とを具備し、
前記第１の格納手段に格納される第１の情報は、登録、更新、削除および有効化の設定の少なくとも何れかが可能であることを特徴とする情報処理装置。
【請求項２】
前記外部端末の利用者別又は前記利用者の属性別に前記サービス別の利用制限を定める利用制限情報を含む第２の情報を格納する第２の格納手段を更に具備し、

前記セキュリティ手段は、前記第２の格納手段から前記第２の情報を参照することで、前記利用者又は前記利用者の属性に応じた制限処理を更に行うことを特徴とする請求項１に記載の情報処理装置。

【請求項３】

前記セキュリティ手段は、前記外部端末からの要求において、前記第２の格納手段から参照する前記第２の情報に含まれる前記利用制限情報で定まる前記利用制限を超える要求があれば、前記利用制限内の要求となるよう改編する機能を更に有し、

前記調停処理手段は、前記セキュリティ手段が改編後の改編要求を前記認証処理の結果と合わせて出力し、

前記呼び出し手段は、前記調停処理手段が出力する前記認証処理の結果に応じて、前記サービス手段に対して前記改編要求に応じたサービスを呼び出すことを特徴とする請求項２に記載の情報処理装置。

【請求項４】

前記第２の格納手段に格納される前記第２の情報は、外部より登録、更新、削除および有効化の設定が少なくとも可能な情報であることを特徴とする請求項２または３に記載の情報処理装置。

【請求項５】

前記第２の格納手段に格納される前記第２の情報は、構造化言語で記述されていることを特徴とする請求項２～４のいずれか１項に記載の情報処理装置。

【請求項６】

前記第２の格納手段に格納される前記第２の情報は、構造化言語で記述されていると共に、前記外部端末からの前記要求は、構造化言語で記述されており、

前記セキュリティ手段は、前記外部端末からの前記要求において、前記第２の格納手段から参照する前記第２の情報に含まれる前記利用制限情報で定まる前記利用制限を超える要求があれば、構造化言語で記述された前記利用制限内の要求となるよう、前記外部端末からの前記要求のボディ部を解析して得られる前記属性情報を改編することを特徴とする請求項３に記載の情報処理装置。

【請求項７】

前記調停処理手段は、前記第１の格納手段に格納されている前記第１の情報に記述された前記認証処理の呼び出し手続きに従って、１つ又は複数のセキュリティ手段を呼び出し、当該呼び出された１つ又は複数のセキュリティ手段による認証処理の結果を受け取り、当該結果を前記呼び出し手段へ出力することを特徴とする請求項１～６のいずれか１項に記載の情報処理装置。

【請求項８】

前記第１の格納手段に格納される前記第１の情報は、前記サービスを特定する情報と、前記サービスに対応するセキュリティ手段を特定する情報とを関連付けた情報であることを特徴とする請求項１～７のいずれか１項に記載の情報処理装置。

【請求項９】

前記第１の格納手段に格納される前記第１の情報は、外部端末から登録、更新、削除および有効化の設定が少なくとも可能な情報であることを特徴とする請求項１～８のいずれか１項に記載の情報処理装置。

【請求項１０】

前記第１の格納手段に格納される前記第１の情報は、構造化言語で記述されていることを特徴とする請求項１～９のいずれか１項に記載の情報処理装置。

【請求項１１】

外部端末からのサービスを識別するための識別情報を含むヘッダ部と、サービスの内容を示す属性情報を記述したボディ部とから構成される要求を受信した場合に、該要求に応じたサービスを実行するサービス手段と、前記サービスを実行する前に認証処理を実施する複数種類のセキュリティ手段とを備えた情報処理装置における情報処理方法であって、

前記外部端末からの前記サービスの要求を受信する受信ステップと、

前記サービスに対応した認証処理の呼び出し手続きが記述された情報である第１の情報を格納する第１の格納手段から、前記第１の情報を参照して、前記外部端末から受信した要求のヘッダ部を解析して得られる前記識別情報により識別されるサービスに対応した認証処理を前記複数種類のセキュリティ手段の少なくとも何れかに実施させる実施ステップと、

当該セキュリティ手段から認証処理の結果を受け取り出力する出力ステップと、

前記出力ステップで出力する前記認証処理の結果に応じて、前記外部端末から受信した要求のボディ部を解析して得られる前記属性情報を用いたサービスを行うために、前記サービス手段に対してサービスを呼び出す呼び出しステップとを有し、

前記第１の格納手段に格納される第１の情報は、登録、更新、削除および有効化の設定の少なくとも何れかが可能であることを特徴とする情報処理方法。

【請求項１２】

外部端末からのサービスを識別するための識別情報を含むヘッダ部と、サービスの内容を示す属性情報を記述したボディ部とから構成される要求を受信した場合に、該要求に応じたサービスを実行するサービス手段を備えたコンピュータを、

前記サービスを実行する前に認証処理を実施する複数種類のセキュリティ手段と、

前記サービスに対応した認証処理の呼び出し手続きが記述された情報である第１の情報を格納する第１の格納手段から前記第１の情報を参照して、前記外部端末から受信した要求のヘッダ部を解析して得られる前記識別情報により識別されるサービスに対応した認証処理を前記複数種類のセキュリティ手段の少なくとも何れかに実施させる機能及び、当該セキュリティ手段から認証処理の結果を受け取り出力する機能を備える調停処理手段と、

前記調停処理手段が出力する前記認証処理の結果に応じて、前記外部端末から受信した要求のボディ部を解析して得られる前記属性情報を用いたサービスを行うために、前記サービス手段に対してサービスを呼び出す呼び出し手段として機能させ、

前記第１の格納手段に格納される第１の情報は、登録、更新、削除および有効化の設定の少なくとも何れかが可能であ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、ネットワークに対応した周辺装置、および該周辺装置を制御する情報処理装置、情報処理方法及びそのプログラムに関するものである。

【背景技術】

【０００２】

近年、構造化言語であるＸＭＬ（ｅＸｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）がビジネス文書管理、メッセージング、データベースなど多岐に渡り利用され、その応用範囲は、ますます広がっている。

その顕著な例が、ＸＭＬ－ＳＯＡＰ（Ｓｉｍｐｌｅ Ｏｂｊｅｃｔ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）を利用した分散オブジェクトモデルであるＷｅｂサービスへの応用である。さらに、このＷｅｂサービスの出現により、従来のオブジェクト指向モデルからサービス指向アーキテクチャ（ＳＯＡ：Ｓｅｒｖｉｃｅ Ｏｒｉｅｎｔｅｄ Ａｒｃｈｉｔｅｃｔｕｒｅ）への転換が徐々に進められてきている。

【０００３】

ここで、サービス指向アーキテクチャとは、プロセスをサービスを単位として分割し、既存サービスの再利用、再編成することで高信頼性、低コストを維持しながら、迅速にビジネスソリューションを構築・提供するためのアーキテクチャである。

【０００４】

一方、ビジネスソリューションに対して、強固なセキュリティがその要求案件として求められつつある。特にネットワーク上に構築されるビジネスソリューションにおいては、ユーザ情報、ユーザデータの保護、さらには本人性の識別、認証が重要な課題となっている。その一方で、ネットワークソリューションの利便性、簡易性を高めるために、シング

ルサインオン、Ｆｅｄｅｒａｔｅｄ　Ｉｄｅｎｔｉｔｙ（統合認証）等の要求が高まってきている。

【０００５】

Ｗｅｂサービスを基盤とするサービス指向アーキテクチャにおいても、その例外ではなく、同一のサービスであっても、そのサービスが使用される環境、セキュリティレベル、システム構成によって、それぞれ異なる認証、権限付与処理といった柔軟な対応が必要である。例えば、ユーザ認証ひとつとっても、簡便なパスワード認証、ＰＩＮコードによる認証、ＩＣカードによる認証、生体認証等、その方法は多岐に渡る。また、複数のサービスを統合して、新規サービスを構築、提供する場合において、それぞれ異なる認証、権限付与手段を統合し、シングルサインオン等の環境を提供する手法の確立が要求されている（例えば、特許文献１を参照）。

【０００６】

すなわち、サービス指向アーキテクチャの効率の良さ、柔軟性を損なわずに、強固なセキュリティを実現するという背反する要求を満たす解決策が必要となってきている。

【０００７】

【特許文献１】特開２００３－２２８５０９公報

【発明の開示】

【発明が解決しようとする課題】

【０００８】

ここで、従来のサービスにおける認証モデルを考察すると、第一に、図１８－１に示すように、個々のサービス（サービスＡやサービスＢ）が各々認証処理、権限付与処理、およびユーザ認証情報を保持するデータベースが組み込まれた形態が考えられる。この形態においては、適用するサービスのユースケースに応じて要求される認証、権限処理が異なる場合、その要求に応じて、これら認証のためのデータベース変更、アクセス制限条件の変更処理を実施するにあたり、サービス全体を改造する必要があり、その開発コスト、管理コストの負荷は大きい。また、認証・権限付与のデータベースを個々のサービスが個別に抱えるため、開発済みのサービスを組み合わせ、新規のサービスを提供するような場合において、シングルサインオン、統合認証等の機能提供を実現することが極めて困難である。

【０００９】

また、図１８－２に示すようにサービスを提供する複数の装置（サービスＡ、Ｂ）の外部に認証、権限処理を行う外部装置（認証処理装置）を備える場合について説明する。この場合には、外部装置において複数のサービスにおける認証、権限付与のデータベースの共有を実現することは可能であるが、各サービスを提供する装置は各々、認証、権限処理を実施する外部装置とのインタフェイス、プロトコル処理を実装しなければならない。そのため、適用するサービスのユースケースに応じて要求される認証、権限処理が異なる場合、その要求に応じてインタフェイス、プロトコルの改造、あるいは個々のサービスが複数のインタフェイス、プロトコルを実装する必要があり、そのため前者の例と同様にその開発コスト、管理コストの負荷は大きく、またユーザ要求に応じて迅速に対応サービスを提供することは極めて困難であった。

【００１０】

また、図１８－２においてサービスの利用制限、アクセス制限の実現手段に注目した場合、例えば、従来は外部装置の認証データベースに登録されたユーザ情報に対応づけて、サービスの利用、アクセス制限を記述した既成、あるいは動的に生成されたトークン（ネットワークを巡回するパケット）がサービスに通知される方法がある。これにより、サービスが該トークンを解釈することで提供するサービスを一部、あるいは全部制限することでサービスの利用制限、アクセス制限を実現してきた。そのため、複数のサービスを組み合わせて新規サービスを構築する場合、新規サービスに応じたトークンを定義、生成する手段、さらに新規サービスは新規トークンを解釈、処理する機能を新たに実装する必要があり、その開発コスト、管理コストは極めて高いものであった。

【００１１】
上述した諸問題は、最適なセキュリティシステムを最適なタイミングで導入することへの妨げとなり、ひいては不正利用による被害をもたらすことの原因となっている。
【００１２】
この発明は、上述した事情を考慮してなされたもので、サービス指向アーキテクチャによるネットワークサービスの提供処理において、その効率の良さ、柔軟性を損うことなく、そのネットワークサービスに最適なセキュリティを簡便に実現することができる情報処理装置、情報処理方法及びそのプログラムを提供することを目的とする。
【課題を解決するための手段】
【００１３】
この発明は、上述した課題を解決すべくなされたもので、本発明による情報処理装置においては、外部端末からのサービスを識別するための識別情報を含むヘッダ部と、サービスの内容を示す属性情報を記述したボディ部とから構成される要求を受信した場合に、該要求に応じたサービスを実行するサービス手段を備えた情報処理装置であって、前記サービスを実行する前に認証処理を実施する複数種類のセキュリティ手段と、前記サービスに対応した認証処理の呼び出し手続きが記述された情報である第１の情報を格納する第１の格納手段と、前記第１の格納手段から前記第１の情報を参照して、前記外部端末から受信した要求のヘッダ部を解析して得られる前記識別情報により識別されるサービスに対応した認証処理を前記複数種類のセキュリティ手段の少なくとも何れかに実施させる機能及び、当該セキュリティ手段から認証処理の結果を受け取り出力する機能を備える調停処理手段と、前記調停処理手段が出力する前記認証処理の結果に応じて、前記外部端末から受信した要求のボディ部を解析して得られる前記属性情報を用いたサービスを行うために、前記サービス手段に対してサービスを呼び出す呼び出し手段とを具備し、前記第１の格納手段に格納される第１の情報は、登録、更新、削除および有効化の設定の少なくとも何れかが可能であることを特徴とする。
【００１４】
これにより、本発明による情報処理装置においては、第１の格納手段に格納する第１の情報の記述内容を変更することで、同一のサービスに対し、他の認証・権限サービスへの対応付けを実施することを簡便に行うことができる。更に、情報処理装置が複数の独立したサービスの組み合わせにより機能するサービスを実行する機能を更に備えるサービス指向アーキテクチャに対応した装置であれば、複数のサービスを組み合わせにより機能する新規サービスに対し、新たに認証、権限サービスを対応付ける処理を簡便に行うことができる。
【００１５】
また、本発明による情報処理装置の一態様例においては、前記外部端末の利用者別又は前記利用者の属性別に前記サービス別の利用制限を定める利用制限情報を含む第２の情報を格納する第２の格納手段を更に具備し、前記セキュリティ手段は、前記第２の格納手段から前記第２の情報を参照することで、前記利用者又は前記利用者の属性に応じた制限処理を更に行うことを特徴とする。
【００１６】
これにより、第２の格納手段に格納される第２の情報の記述内容を変更することで、同一のサービスに対して複数の要求を行った同一の利用者（又は同一の利用者の属性）に対して、様々なケースに応じて異なる権限付与、アクセス制限を実施することができる。
【００１７】
また、本発明による情報処理装置の一態様例においては、前記セキュリティ手段は、前記外部端末からの要求において、前記第２の格納手段から参照する前記第２の情報に含まれる前記利用制限情報で定まる前記利用制限を超える要求があれば、前記利用制限内の要求となるよう改編する機能を更に有し、前記調停処理手段は、前記セキュリティ手段が改編後の改編要求を前記認証処理の結果と合わせて出力し、前記呼び出し手段は、前記調停処理手段が出力する前記認証処理の結果に応じて、前記サービス手段に対して前記改編要

求に応じたサービスを呼び出すことを特徴とする。

【００１８】

これにより、情報処理装置は、あくまで受信した要求を実行するだけで、適切な権限付与、アクセス制限が施されたサービスを提供することが可能となり、また利用者にとっては、適切な要求を再度設定し直す手間を省くことができる。

【００１９】

また、本発明による情報処理方法においては、外部端末からのサービスを識別するための識別情報を含むヘッダ部と、サービスの内容を示す属性情報を記述したボディ部とから構成される要求を受信した場合に、該要求に応じたサービスを実行するサービス手段と、前記サービスを実行する前に認証処理を実施する複数種類のセキュリティ手段とを備えた情報処理装置における情報処理方法であって、前記外部端末からの前記サービスの要求を受信する受信ステップと、前記サービスに対応した認証処理の呼び出し手続きが記述された情報である第１の情報を格納する第１の格納手段から、前記第１の情報を参照して、前記外部端末から受信した要求のヘッダ部を解析して得られる前記識別情報により識別されるサービスに対応した認証処理を前記複数種類のセキュリティ手段の少なくとも何れかに実施させる実施ステップと、当該セキュリティ手段から認証処理の結果を受け取り出力する出力ステップと、前記出力ステップで出力する前記認証処理の結果に応じて、前記外部端末から受信した要求のボディ部を解析して得られる前記属性情報を用いたサービスを行うために、前記サービス手段に対してサービスを呼び出す呼び出しステップとを有し、前記第１の格納手段に格納される第１の情報は、登録、更新、削除および有効化の設定の少なくとも何れかが可能であることを特徴とする。

【００２０】

また、本発明によるプログラムは、外部端末からのサービスを識別するための識別情報を含むヘッダ部と、サービスの内容を示す属性情報を記述したボディ部とから構成される要求を受信した場合に、該要求に応じたサービスを実行するサービス手段を備えたコンピュータを、前記サービスを実行する前に認証処理を実施する複数種類のセキュリティ手段と、前記サービスに対応した認証処理の呼び出し手続きが記述された情報である第１の情報を格納する第１の格納手段から前記第１の情報を参照して、前記外部端末から受信した要求のヘッダ部を解析して得られる前記識別情報により識別されるサービスに対応した認証処理を前記複数種類のセキュリティ手段の少なくとも何れかに実施させる機能及び、当該セキュリティ手段から認証処理の結果を受け取り出力する機能を備える調停処理手段と、前記調停処理手段が出力する前記認証処理の結果に応じて、前記外部端末から受信した要求のボディ部を解析して得られる前記属性情報を用いたサービスを行うために、前記サービス手段に対してサービスを呼び出す呼び出し手段として機能させ、前記第１の格納手段に格納される第１の情報は、登録、更新、削除および有効化の設定の少なくとも何れかが可能であることを特徴とする。

【発明の効果】

【００２１】

本発明による情報処理装置、情報処理方法及びそのプログラムは、サービス指向アーキテクチャによるネットワークサービスの提供処理において、その効率の良さ、柔軟性を損うことなく、そのネットワークサービスに最適なセキュリティを簡便に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】

【００２２】

以下に、図面を参照して、本発明の好適な実施の形態について説明する。

［第１の実施形態］

まず、本発明の第１の実施形態における情報処理装置として、ＳＯＡ（サービス指向アーキテクチャ）モデルを実現するＷｅｂサービスを実装するコンピュータの機能モデルについて説明する。図１６は、第１の実施形態における情報処理装置１７０の機能モデル例を示すモデル図である。

【００２３】
図１６において、エントランス部１７１は、情報処理装置１７０が提供するサービスに対するリクエストを例えばクライアント（端末）から受信する。エントランス部１７１は、受信したリクエスト先のサービス名称、認証関連情報を、調停処理部１７２に対し通知する。調停処理部１７２は、マッピングテーブル１７３を参照して、リクエストされたサービスに対する認証、権限処理サービスに関する情報（以下、サービス対応認証情報とする）を取得する。調停処理部１７２は、取得したサービス対応認証情報に基づき、エントランス部１７１より受信した認証情報を対応する認証・権限処理サービス部１７４に通知する。

【００２４】
認証・権限処理サービス部１７４は、調停処理部１７２から通知された認証情報を基に認証処理を実施する。また、さらに認証・権限処理サービス部１７４は、権限情報テーブル１７５を参照し、必要に応じて、その権限情報テーブル１７５に記述された権限付与・アクセス制限情報に基づき、リクエストの内容を改編する。認証・権限処理サービス部１７４における認証、権限処理の結果は、調停処理部１７２に返信される。

【００２５】
調停処理部１７２は、その処理結果に基づきサービス実行の可否、あるいはアクセス制限情報をエントランス部１７１に通知する。エントランス部１７１は、調停処理部１７２から返信された結果に基づき、リクエストされたサービスをサービス部１７６に対してコールするか、あるいはリクエスト発行元であるクライアントに対し、サービス実行が拒否された旨を通知する。

【００２６】
以上に説明したように、本実施形態の情報処理装置１７０は、認証・権限処理のための制御の流れをサービス提供処理の流れと独立して設けることにより、サービスと、そのサービスに対する認証、権限処理サービスの疎結合を実現するものである。また、サービスをコールする際、そのリクエストの内容は予め認証・権限処理サービス部１７４によって、そのリクエストの発行元に付与された権限、アクセス制限に基づき改編されており、あくまで受信したリクエストを実行するだけで、権限付与、アクセス制限が施された処理を実施することが可能となり、サービスの実施に対する、権限付与、アクセス制限サービスの疎結合を実現する。

【００２７】
上述した情報処理装置１７０は、調停処理部１７２と、サービス部１７６と、そのサービス部１７６が提供するサービスに対する認証、権限処理を実施するために、サービスに対応する認証・権限処理サービスに関する情報の情報テーブル（マッピングテーブル１７３）を導入した点が特徴である。また、情報処理装置１７０において、権限付与、アクセス制限の処理に関しては、該処理を実施する認証・権限処理サービス部１７４が、権限付与、アクセス制限に関する情報テーブル（権限情報テーブル１７５）を参照して、該情報テーブルに記述された権限付与・アクセス制限情報に従ってクライアントからのリクエストを改編する機能を導入した点が特徴である。

【００２８】
従って、上述した特徴を有する情報処理装置１７０においては、マッピングテーブル１７３の記述内容を変更することで、同一のサービスに対し、他の種類の認証・権限サービスへの対応付けを実施することが可能である。また、情報処理装置１７０においては、複数のサービスを組み合わせにより機能する新規サービスがサービス部１７６に追加されたとしても、マッピングテーブル１７３において、この新規サービスに対し、新たに認証・権限サービスを対応付けることなどが可能とである。また、情報処理装置１７０においては、権限情報テーブル１７５の記述内容を変更することで、同一のサービスに対しリクエストを実施した同一のリクエスタに対し、ユースケースに応じて異なる権限付与、アクセス制限を実施することが可能となり、柔軟にサービス指向アーキテクチャにおけるセキュリティ要件に対応することが可能である。

【００２９】
［第２の実施形態］
次に、上述した第１の実施形態における情報処理装置１７０の特徴的な処理を、複合機において実現した場合の第２の実施形態について説明する。すなわち、本発明の第２の実施形態における情報処理装置として印刷機能や複写機能を有する複合機を例に説明する。具体的には、ネットワークに接続された複合機（ネットワーク対応型複合機）を含むネットワーク画像処理システムについて説明する。
【００３０】
図１７は、本発明の第２の実施形態であるネットワーク対応型複合機Ｍ１を含むネットワーク画像処理システムの概略構成を示す図である。図１７において、Ｍ１は、複合機（ＭＦＰ）であり、ネットワークＮ１を介して接続可能なコンピュータ端末（端末Ｃ１及び端末Ｃ２）へ印刷サービス、スキャンサービス、ストレージサービス、ＦＡＸサービスなどを提供するネットワーク対応型複合機である。Ｃ１、Ｃ２、…は、コンピュータ端末であり、ネットワークＮ１を介して複合機Ｍ１の提供する上記サービスを利用することができる。
【００３１】
本実施形態における複合機Ｍ１は、構造化言語であるＸＭＬ（ｅＸｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）を用いてユーザ認証、アクセス制限等のセキュリティ処理を行う機能を有する。また、複合機Ｍ１は、サービス指向アーキテクチャによりＷｅｂサービスを実現している。また、複合機Ｍ１のハードウェア構成は、例えば通信装置１００、ＣＰＵ（中央処理装置）１０１、メモリ１０２、ＨＤＤ（ハード ディスク ドライブ）１０３、プリンタ１０４、スキャナ１０５、及び画像処理装置１０６などから構成されている。通信装置１００は、ネットワークＮ１を介して端末Ｃ１、Ｃ２、…などと通信を行う。ＣＰＵ１０１は、複合機Ｍ１における種々の機能を実現するためのプログラムを実行するコンピュータである。具体的には、ＣＰＵ１０１は、ＨＤＤ１０３から種々の機能を実現するためのプログラム（アプリケーションプログラム等）を読み出し、メモリ１０２をワーク領域として、読み出したプログラムを実行する。
【００３２】
次に、本実施形態における複合機Ｍ１が有する機能構成について説明する。
図１は、本実施形態における複合機Ｍ１が有する機能構成を示すブロック図である。
複合機Ｍ１は、通信機能としてＴＣＰ／ＩＰ／ＵＤＰプロトコルをスタックするプロトコルスタック処理部１を備え、その上位層にＳＯＡＰ（Ｓｉｍｐｌｅ Ｏｂｊｅｃｔ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）処理部２を備え、その上位層に調停サービス部３、マッピングスクリプト処理部４、認証・権限サービスＡ・７、認証サービスＢ・８、権限サービスＢ・９、権限スクリプト処理部１５、プリントサービス１０、スキャンサービス１１、ストレージサービス１２、及びＦＡＸサービス１３を備え、ネットワークＮ１を介して、クライアントＰＣ・１７に対し、これらサービスを提供する。
【００３３】
また、１４は、認証・権限サービスＣであり、認証・権限サービス機能を実現する論理ユニットを、ネットワークＮ１を介して独立させた形態であり、例えばＰＣによるサーバ上に独立して実装される論理ユニットである。尚、本実施形態では、認証・権限サービスＣ・１４を複合機Ｍ１の外部に設けたが、認証・権限サービスＡなどと同様に、認証・権限サービスＣ・１４を、ＳＯＡＰ処理部２の上位層に設けてもよい。１７は、複合機Ｍ１のサービスを利用するクライアントＰＣであり、１８は、複合機Ｍ１の設定等を行う管理端末ＰＣである。ネットワークＮ１は、例えばＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）などの通信網である。
【００３４】
複合機Ｍ１に対しては、外部デバイス（例えば、管理端末ＰＣ・１８）から、上記サービスの一部又は全ての機能の停止、サービスの削除、サービスの再インストール、新規サービスのインストールが可能である。この場合、新規サービスとは、例えば既にインスト

ール済みの複数のサービスを組みあわせにより、新規機能を提供するサービスを含む。

【００３５】

ＳＯＡＰ処理部２は、受信したＳＯＡＰエンベロープを調停サービス部３に対し送信し、調停サービス部３から返信される処理結果に基づき、ＳＯＡＰレスポンスを生成し、リクエストを発行したクライアントＰＣ・１７に対し返信する機能を有する。また、ＳＯＡＰ処理部２は、調停サービス部３から返信される処理結果に基づき、該当するサービスに対しＳＯＡＰボディの記述内容を送信し、該当サービスから通知される処理結果に基づきＳＯＡＰレスポンスを生成し、リクエストを発行したクライアントＰＣ・１７に対し返信する機能を有する。

【００３６】

調停サービス部３は、ＳＯＡＰ処理部２より送信されたＳＯＡＰヘッダ部の記述内容を解析し、実行要求されたサービスに関する情報を取得する機能を有する。また、調停サービス部３は、マッピングスクリプト処理部４を介して、メモリ装置制御部５が管理するメモリ上に登録されたマッピングスクリプト６より、要求されたサービスに対応する認証・権限サービスに関する情報（サービス対応認証情報）を取得する機能を有する。また、調停サービス部３は、マッピングスクリプト６より取得したサービス対応認証情報に基づき特定される認証・権限サービスに対して、ＳＯＡＰヘッダに記述された認証情報を送信する機能を有する。また、調停サービス部３は、認証・権限サービスから通知される処理結果に基づきレスポンスを生成し、ＳＯＡＰ処理部２に対し通知する機能を有する。

【００３７】

図１に示すように、複合機Ｍ１は、認証、権限付与機能を実現するサービスである認証・権限サービスとして、認証・権限サービスＡ・７、認証サービスＢ・８、権限サービスＢ・９が組み込まれている。これらの各認証・権限サービスは、調停サービス部３より送信された認証情報を処理し、その処理結果を調停サービス部３に対し返信する機能を有する。また、これらの各認証・権限サービスのうち、権限付与機能を備えた認証・権限サービスＡ・７、権限サービスＢ・９は、権限スクリプト処理部１５を介して、メモリ装置制御部５が管理するメモリ上に登録された権限スクリプト１６より、要求されたサービスに対するアクセス権限に関する情報を取得する機能を有する。

【００３８】

また、権限スクリプト処理部１５は、権限スクリプト１６の登録、削除、および権限スクリプト１６の有効化指定機能を有する。また、権限スクリプト処理部１５は、認証・権限サービスＡ・７、および権限サービスＢ・９からＳＯＡＰボディに記述されたサービス実行要求情報を受け取り、権限スクリプト１６より取得したアクセス制限情報に基づきレスポンス（実行要求情報）を改編する機能を有する。権限スクリプト処理部１５が改編したレスポンスは、認証・権限サービスＡ・７、および権限サービスＢ・９が受け取り、調停サービス部３に対し通知する。尚、本実施形態においては、権限スクリプト処理部１５がレスポンス（実行要求情報）を改編する処理を行うが、この限りではなく、認証・権限サービスＡ・７、および権限サービスＢ・９などの認証・権限サービスがレスポンス（実行要求情報）を改編する処理を行ってもよい。

【００３９】

図１に示すように、複合機Ｍ１は、サービスを提供する機能としてプリントサービス１０、スキャンサービス１１、ストレージサービス１２、ＦＡＸサービス１３を実装する。これらサービスは、ＸＭＬ－ＳＯＡＰに対応したＷｅｂサービスであり、これらサービスは管理者により管理された外部デバイス（管理端末ＰＣ・１８）よりネットワークＮ１を介してアクセスすることで、サービスの一部又は全ての機能の停止、再開、削除、再インストールが可能であり、また、同様に新規サービスの追加、開始、停止、削除が可能である。

【００４０】

調停サービス部３の下位層となるマッピングスクリプト処理部４は、メモリ装置制御部５を介してメモリへアクセスする機能を有する。メモリ装置制御部５は、マッピングスク

リプト処理部４からの制御に応じて、サービス及びそのサービスに対する認証・権限サービスに関する情報（サービス対応認証情報）や、処理手順が記述されたマッピングスクリプト６を格納するメモリへのデータの書込み及び読み出しを制御する。

【００４１】

また、上記マッピングスクリプト６は、管理者により管理された外部デバイス（管理端末ＰＣ・１８）より削除、再インストール、更新処理が可能である。これにより、該マッピングスクリプト６の記述内容に従って、同一のサービスに対し、他の認証・権限サービスへの対応付けを実施することができる。また、複数のサービスを組み合わせにより機能する新規サービスに対し、新たに認証・権限サービスを対応付けるなど、柔軟にセキュリティ要件に対応することが可能である。

【００４２】

認証・権限サービスＡ・７、および権限サービスＢ・９の下位層となる権限スクリプト処理部１５は、メモリ装置制御部５を介してメモリへアクセスする機能を有する。メモリ装置制御部５は、認証・権限サービスＡ・７、および権限サービスＢ・９からの制御に応じて、権限付与、アクセス制限に関する情報（権限付与・アクセス制限情報）、および処理手順が記述された権限スクリプト１６を格納するメモリへのデータの書込み及び読み出しを制御する。

【００４３】

本実施形態では、複合機Ｍ１上で稼動状態にあるサービスに対応づけられた認証・権限サービスに関する情報（サービス対応認証情報）が記載されたマッピングスクリプト６、および権限付与・アクセス制限情報が記載された権限スクリプト１６を、複合機Ｍ１のメモリに対して予め登録しておく。

【００４４】

尚、この登録処理を実行せずに、複合機Ｍ１のメモリ上に該マッピングスクリプト６が存在しない場合、本実施例の場合、複合機Ｍ１上で稼動中のサービスのいずれも実行することはできない。同様に、複合機Ｍ１のメモリ上に該権限スクリプト１６が存在しない場合、この権限スクリプト１６を参照する権限付与サービスに対応付けられたサービスを実行することはできない。

【００４５】

マッピングスクリプト６は、システムの管理者が複合機Ｍ１に対し、ネットワークを介して登録処理を実施することで、メモリ装置制御部５が制御するメモリ上に格納される。システム管理者は、システム管理者により管理された管理端末ＰＣ・１８から、複合機Ｍ１に実装された各サービスに対応づけられた認証・権限サービスを記述したマッピングスクリプト６を複合機Ｍ１に対して送信する。

【００４６】

本実施形態においては、マッピングスクリプト６の登録、削除に関して以下に示すＸＭＬ－ＳＯＡＰ　ＲＰＣ（Ｒｅｍｏｔｅ　Ｐｒｏｃｅｄｕｒｅ　Ｃａｌｌ）を備える。これにより、マッピングスクリプト処理部４は、マッピングスクリプト６の登録、削除、およびマッピングスクリプト６の有効化指定機能を実現する。以下に、登録や削除を行うＳＯＡＰ関数について説明する。

【００４７】

ＵｐｌｏａｄＳｃｒｉｐｔ（ｓｃｒｉｐｔＮａｍｅ、ａｃｃｏｕｎｔ、ｐａｓｓｗｏｒｄ）とは、マッピングスクリプト６を複合機Ｍ１に対し送信、登録するためのＳＯＡＰ関数である。本実施形態の複合機Ｍ１においてマッピングスクリプト６は複数登録することが可能であるため、ｓｃｒｉｐｔＮａｍｅはその識別情報として使用する。本実施形態の複合機Ｍ１においては、３２文字までのＡＳＣＩＩ文字列が使用可能である。尚、ａｃｃｏｕｎｔ（アカウント）とｐａｓｓｗｏｒｄ（パスワード）は、いずれも３２文字までのＡＳＣＩＩ文字列が使用されている。これら情報は、本実施形態においては予め複合機Ｍ１に対し登録済みであり、その情報はメモリ装置制御部５が管理するメモリ上に記録されており、システム管理者のみが知りうる情報である。ＸＭＬデータであるマッピングスク

リプト６は、該ＳＯＡＰ関数を記述するＳＯＡＰエンベロープの添付ファイルの形式で送信される。

【００４８】

ＤｅｌｅｔｅＳｃｒｉｐｔ（ｓｃｒｉｐｔＮａｍｅ、ａｃｃｏｕｎｔ、ｐａｓｓｗｏｒｄ）とは、複合機Ｍ１に登録済みのマッピングスクリプト６を削除するためのＳＯＡＰ関数である。ａｃｃｏｕｎｔ，ｐａｓｓｗｏｒｄ情報を知りうるシステム管理者のみが、複合機Ｍ１のメモリ上に登録されたマッピングスクリプト６を削除することができる。本実施形態においては、複数のマッピングスクリプト６が登録可能であるためｓｃｒｉｐｔＮａｍｅにより、削除対象となるマッピングスクリプト６を指定する。

【００４９】

ＥｎａｂｌｅＳｃｒｉｐｔ（ｓｃｒｉｐｔＮａｍｅ、ａｃｃｏｕｎｔ、ｐａｓｓｗｏｒｄ）とは、複合機Ｍ１に登録された複数のマッピングスクリプト６に対し、ｓｃｒｉｐｔＮａｍｅで指定したマッピングスクリプト６を有効とするためのＳＯＡＰ関数である。この関数も、ａｃｃｏｕｎｔ，ｐａｓｓｗｏｒｄ情報を知りうるシステム管理者のみが、複合機Ｍ１のメモリ上に登録されたマッピングスクリプト６を指定し、有効とすることができる。

【００５０】

次に、図面を用いてマッピングスクリプト６の登録処理について説明する。

図２は、本実施形態の複合機Ｍ１におけるマッピングスクリプト６の登録処理を示すフローチャートである。尚、図２の処理の前提として、外部デバイスである管理端末ＰＣ・１８は、ＳＯＡＰリクエストおよびマッピングスクリプト６を、マッピングスクリプト処理部４を備えた複合機Ｍ１に対し送信する。

【００５１】

図２に示すように、まず、調停サービス部３を構成するマッピングスクリプト処理部４は、ＳＯＡＰ処理部２を介してＳＯＡＰリクエストであるＵｐｌｏａｄＳｃｒｉｐｔを受信したか否かを判断する（ｓｔｅｐ１）。ここで、ＳＯＡＰリクエストであるＵｐｌｏａｄＳｃｒｉｐｔを受信したと判断した場合には、マッピングスクリプト処理部４は、引数であるａｃｃｏｕｎｔとｐａｓｓｗｏｒｄの内容を確認するため、メモリ装置制御部５を介してメモリ上に記録されている情報（以下、アカウント情報とする）と一致するか否かを判断する（ｓｔｅｐ２）。

【００５２】

アカウント情報が一致しないと判断した場合には（ｓｔｅｐ３）、マッピングスクリプト処理部４は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信する（ｓｔｅｐ４）。アカウント情報が一致すると判断した場合には、マッピングスクリプト処理部４は、既に同一ｓｃｒｉｐｔＮａｍｅを持つマッピングスクリプト６が登録済みであるか否かを判断する（ｓｔｅｐ５）。

【００５３】

ｓｔｅｐ５において既に登録済みであると判断した場合には（ｓｔｅｐ６）、マッピングスクリプト処理部４は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信し（ｓｔｅｐ４）、図２のｓｔｅｐ１に戻る。尚、この場合には、管理者は既に登録済みとなっているマッピングスクリプト６に対してＤｅｌｅｔｅＳｃｒｉｐｔリクエストを使ってそれを削除しない限り、同一のｓｃｒｉｐｔＮａｍｅを持つマッピングスクリプトを登録する事はできない。

【００５４】

登録済みのマッピングスクリプトが存在しないと判断した場合には、マッピングスクリプト処理部４は、該リクエストの添付ファイルの形式で送信されたマッピングスクリプトを、メモリ装置制御部５を介してメモリ上に記録する（ｓｔｅｐ７）。

【００５５】

また、ｓｔｅｐ１においてＳＯＡＰリクエストであるＵｐｌｏａｄＳｃｒｉｐｔを受信していないと判断した場合には、マッピングスクリプト処理部４は、ＳＯＡＰ処理部２を

介してＳＯＡＰリクエストであるＤｅｌｅｔｅＳｃｒｉｐｔを受信したか否かを判断するｓｔｅｐ８。ここで、ＳＯＡＰリクエストであるＤｅｌｅｔｅＳｃｒｉｐｔを受信したと判断した場合には、マッピングスクリプト処理部４は、引数であるａｃｃｏｕｎｔとｐａｓｓｗｏｒｄの内容を確認するため、メモリ装置制御部５を介してメモリ上に記録されている情報（アカウント情報）と一致するか否かを判断する（ｓｔｅｐ９）。

【００５６】

ステップＳ２８において、アカウント情報が一致しないと判断した場合には（ｓｔｅｐ１０）、マッピングスクリプト処理部４は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信する（ｓｔｅｐ１１）。また、アカウント情報が一致すると判断した場合には、マッピングスクリプト処理部４は、既に同一ｓｃｒｉｐｔＮａｍｅを持つマッピングスクリプトが登録済みか否か判断する（ｓｔｅｐ１２）。

【００５７】

Ｓｔｅｐ１２において、指定されたｓｃｒｉｐｔＮａｍｅをもつマッピングスクリプト６がメモリ上に記録されていない場合（登録済みでない場合）には（ｓｔｅｐ１３）、マッピングスクリプト処理部４は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信する（ｓｔｅｐ１１）。また、指定されたｓｃｒｉｐｔＮａｍｅをもつマッピングスクリプト６がメモリ上に記録されている場合（登録済みである場合）には、マッピングスクリプト処理部４は、メモリ装置制御部５を介してメモリ上に記録されたマッピングスクリプトを削除する（ｓｔｅｐ１４）。

【００５８】

また、ｓｔｅｐ８においてＳＯＡＰリクエストであるＤｅｌｅｔｅＳｃｒｉｐｔを受信していないと判断した場合には、マッピングスクリプト処理部４は、ＳＯＡＰ処理部２を介してＳＯＡＰリクエストであるＥｎａｂｌｅＳｃｒｉｐｔを受信したか否かを判断する（ｓｔｅｐ１５）。ここで、ＳＯＡＰリクエストであるＥｎａｂｌｅＳｃｒｉｐｔを受信したと判断した場合には、マッピングスクリプト処理部４は、引数であるａｃｃｏｕｎｔとｐａｓｓｗｏｒｄの内容を確認するため、メモリ装置制御部５を介してメモリ上に記録されている情報（アカウント情報）と一致するか否かを判断する（ｓｔｅｐ１６）。

【００５９】

ｓｔｅｐ１６において、アカウント情報が一致しないと判断した場合（ｓｔｅｐ１７）には、マッピングスクリプト処理部４は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信する（ｓｔｅｐ１８）。また、アカウント情報が一致すると判断した場合には、マッピングスクリプト処理部４は、指定されたｓｃｒｉｐｔＮａｍｅを持つマッピングスクリプトが登録済みか否か判断する（ｓｔｅｐ１９）。

【００６０】

ｓｔｅｐ１９において、指定されたｓｃｒｉｐｔＮａｍｅをもつマッピングスクリプトがメモリ上に記録されていない場合（登録済みでない場合）には（ｓｔｅｐ２０）、マッピングスクリプト処理部４は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信する（ｓｔｅｐ１８）。また、指定されたｓｃｒｉｐｔＮａｍｅをもつマッピングスクリプトがメモリ上に記録されている場合（登録済みである場合）には、マッピングスクリプト処理部４は、指定されたｓｃｒｉｐｔＮａｍｅを持つマッピングスクリプト６を有効とし（ｓｔｅｐ２１）、以降、調停サービス部３が該マッピングスクリプト６を参照する。

【００６１】

以上に示した処理により、外部デバイス（管理端末ＰＣ・１８）から、複合機Ｍ１へのアプリケーション（サービス）に応じたマッピングスクリプトの登録処理、および有効化処理が完了する。システム管理者は必要、用途に応じて該当するアプリケーション（サービス）のマッピングスクリプトを登録、削除、有効化処理を繰り返し実行することが可能である。

【００６２】

同様に、権限スクリプト１６は、システムの管理者が複合機Ｍ１に対し、ネットワーク

Ｎ１を介して登録処理を実施することで、メモリ装置制御部５が制御するメモリ上に格納される。システム管理者は、システム管理者により管理された管理端末ＰＣ・１８から、複合機Ｍ１に実装された各権限付与サービスに対応づけられ、権限付与・アクセス制限情報が記述された権限スクリプト１６を複合機Ｍ１に対し送信する。

【００６３】

本実施形態においては、権限スクリプト１６の登録、削除に関して以下に示すＸＭＬ－ＳＯＡＰ　ＲＰＣ（Ｒｅｍｏｔｅ　Ｐｒｏｃｅｄｕｒｅ　Ｃａｌｌ）を備える。これにより、権限スクリプト処理部１５は、権限スクリプト１６の登録、削除、および権限スクリプト１６の有効化指定機能を実現する。以下、ＳＯＡＰ関数について説明する。

【００６４】

ＵｐｌｏａｄＡｕｔｈＳｃｒｉｐｔ（ｓｃｒｉｐｔＮａｍｅ、ａｕｔｈＮａｍｅ、ａｃｃｏｕｎｔ、ｐａｓｓｗｏｒｄ）とは、権限スクリプト１６を複合機Ｍ１に対し送信、登録するためのＳＯＡＰ関数である。本実施形態において権限スクリプト１６は複数登録することが可能であるため、ｓｃｒｉｐｔＮａｍｅはその識別情報として使用する。本実施形態においては、３２文字までのＡＳＣＩＩ文字列が使用可能である。また、ａｕｔｈＮａｍｅにより、該権限スクリプト１６を参照する権限付与サービスを指定する。なお、ａｃｃｏｕｎｔとｐａｓｓｗｏｒｄは、いずれも３２文字までのＡＳＣＩＩ文字列が使用されている。これら情報は、本実施形態においては予め複合機Ｍ１に対し登録済みであり、その情報はメモリ装置制御部が管理するメモリ上に記録されており、システム管理者のみが知りうる情報である。ＸＭＬデータである権限スクリプト１６は、該ＳＯＡＰ関数を記述するＳＯＡＰエンベロープの添付ファイルの形式で送信される。

【００６５】

ＤｅｌｅｔｅＡｕｔｈＳｃｒｉｐｔ（ｓｃｒｉｐｔＮａｍｅ、ａｕｔｈＮａｍｅ、ａｃｃｏｕｎｔ、ｐａｓｓｗｏｒｄ）とは、複合機Ｍ１に登録済みの権限スクリプト１６を削除するためのＳＯＡＰ関数である。ａｃｃｏｕｎｔ，ｐａｓｓｗｏｒｄ情報を知りうるシステム管理者のみが、複合機Ｍ１のメモリ上に登録された権限スクリプト１６を削除する。本実施形態においては、複数の権限スクリプト１６が登録可能であるためｓｃｒｉｐｔＮａｍｅ、およびａｕｔｈＮａｍｅにより、削除対象となる権限スクリプト１６を指定する。

【００６６】

ＥｎａｂｌｅＡｕｔｈＳｃｒｉｐｔ（ｓｃｒｉｐｔＮａｍｅ、ａｕｔｈＮａｍｅ，ａｃｃｏｕｎｔ、ｐａｓｓｗｏｒｄ）とは、複合機Ｍ１に登録された複数の権限スクリプト１６に対し、ｓｃｒｉｐｔＮａｍｅ、およびａｕｔｈＮａｍｅで指定した権限スクリプト１６を有効とするためのＳＯＡＰ関数である。ａｃｃｏｕｎｔ，ｐａｓｓｗｏｒｄ情報を知りうるシステム管理者のみが、複合機Ｍ１のメモリ上に登録された権限スクリプト１６を指定し、有効とすることができる。

【００６７】

次に、図面を用いて権限スクリプト１６の登録処理について説明する。

図３は、本実施形態の複合機Ｍ１における権限スクリプト１６の登録処理を示すフローチャートである。尚、図３の処理の前提として、外部デバイスである管理端末ＰＣ１８は、ＳＯＡＰリクエスト、および権限スクリプト１６を、権限スクリプト処理部１５を備えた複合機Ｍ１に対し送信する。

【００６８】

図３に示すように、まず、調停サービス部３を構成する権限スクリプト処理部１５は、ＳＯＡＰ処理部２を介してＳＯＡＰリクエストであるＵｐｌｏａｄＡｕｔｈＳｃｒｉｐｔを受信したか否かを判断する（ｓｔｅｐ１）。ここで、ＳＯＡＰリクエストであるＵｐｌｏａｄＡｕｔｈＳｃｒｉｐｔを受信したと判断した場合には、権限スクリプト処理部１５は、引数であるａｃｃｏｕｎｔとｐａｓｓｗｏｒｄの内容を確認するため、メモリ装置制御部５を介してメモリ上に記録されている情報（以下、アカウント情報とする）と一致するか否かを判断する（ｓｔｅｐ２）。

【００６９】
アカウント情報が一致しないと判断した場合には（ｓｔｅｐ３）、権限スクリプト処理部１５は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信する（ｓｔｅｐ４）。アカウント情報が一致すると判断した場合には、権限スクリプト処理部１５は、既に同一ｓｃｒｉｐｔＮａｍｅ、ａｕｔｈＮａｍｅを持つ権限スクリプト１６が登録済みであるか否かを判断する（ｓｔｅｐ５）。
【００７０】
既に登録済みであると判断した場合には（ｓｔｅｐ６）、権限スクリプト処理部１５は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信し（ｓｔｅｐ４）、図３のｓｔｅｐ１に戻る。尚、この場合には、管理者は既に登録済みとなっている権限スクリプト１６をＤｅｌｅｔｅＡｕｔｈＳｃｒｉｐｔリクエストを使って削除しない限り、同一のｓｃｒｉｐｔＮａｍｅ、およびａｕｔｈＮａｍｅを持つ権限スクリプト１６を登録する事はできない。
【００７１】
登録済みの権限スクリプトが存在しないと判断した場合には、権限スクリプト処理部１５はＡｕｔｈＮａｍｅで指定された権限付与サービスが複合機Ｍ１上で稼動状態にあるか否かを判断する（ｓｔｅｐ７）。ここで、指定された権限付与サービスが複合機Ｍ１上で稼動状態にない場合（ｓｔｅｐ８）、権限スクリプト処理部１５は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信し（ｓｔｅｐ４）、図３のｓｔｅｐ１に戻る。
【００７２】
また、指定された権限付与サービスがＭ１上で稼動状態にある場合、権限スクリプト処理部１５は、該リクエストの添付ファイルの形式で送信された権限スクリプト１６を、メモリ装置制御部５を介してメモリ上に記録する（ｓｔｅｐ９）。
【００７３】
また、ｓｔｅｐ１においてＳＯＡＰリクエストであるＵｐｌｏａｄＡｕｔｈＳｃｒｉｐｔを受信していない判断した場合には、権限スクリプト処理部１５は、ＳＯＡＰ処理部２を介してＳＯＡＰリクエストであるＤｅｌｅｔｅＡｕｔｈＳｃｒｉｐｔを受信したか否かを判断する（ｓｔｅｐ１０）。ここで、ＳＯＡＰリクエストであるＤｅｌｅｔｅＡｕｔｈＳｃｒｉｐｔを受信したと判断した場合には、権限スクリプト処理部１５は、引数であるａｃｃｏｕｎｔとｐａｓｓｗｏｒｄの内容を確認するため、メモリ装置制御部５を介してメモリ上に記録されている情報（アカウント情報）と一致するか否かを判断する（ｓｔｅｐ１１）。
【００７４】
アカウント情報が一致しないと判断した場合には（ｓｔｅｐ１２）、権限スクリプト処理部１５は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信する（ｓｔｅｐ１３）。また、アカウント情報が一致すると判断した場合には、権限スクリプト処理部１５は、既に同一ｓｃｒｉｐｔＮａｍｅ、ａｕｔｈＮａｍｅを持つ権限スクリプト１６が登録済みか否か判断する（ｓｔｅｐ１４）。
【００７５】
ｓｔｅｐ１４において、指定されたｓｃｒｉｐｔＮａｍｅを持ち、さらに指定されたＡｕｔｈＮａｍｅに対応する権限スクリプト１６がメモリ上に記録されていない場合（登録済みでない場合）には（ｓｔｅｐ１５）、権限スクリプト処理部１５は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信する（ｓｔｅｐ１３）。また、指定されたｓｃｒｉｐｔＮａｍｅを持ち、さらに指定されたＡｕｔｈＮａｍｅに対応する権限スクリプト１６がメモリ上に記録されている場合（登録済みである場合）には、権限スクリプト処理部１５は、メモリ装置制御部５を介してメモリ上に記録された権限スクリプト１６を削除する（ｓｔｅｐ１６）。
【００７６】
また、ｓｔｅｐ８においてＳＯＡＰリクエストであるＤｅｌｅｔｅＡｕｔｈＳｃｒｉｐｔを受信していないと判断した場合には、権限スクリプト処理部１５は、ＳＯＡＰ処理部

２を介してＳＯＡＰリクエストであるＥｎａｂｌｅＡｕｔｈＳｃｒｉｐｔを受信したか否かを判断する（ｓｔｅｐ１７）。ここで、ＳＯＡＰリクエストであるＥｎａｂｌｅＡｕｔｈＳｃｒｉｐｔを受信したと判断した場合には、権限スクリプト処理部１５は、引数であるａｃｃｏｕｎｔとｐａｓｓｗｏｒｄの内容を確認するため、メモリ装置制御部５を介してメモリ上に記録されている情報（アカウント情報）と一致するか否かを判断する（ｓｔｅｐ１８）。

【００７７】

ここで、アカウント情報が一致しないと判断した場合（ｓｔｅｐ１９）には、権限スクリプト処理部１５は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信する（ｓｔｅｐ２０）。また、アカウント情報が一致すると判断した場合には、権限スクリプト処理部１５は、指定されたｓｃｒｉｐｔＮａｍｅ、およびＡｕｔｈＮａｍｅを持つ権限スクリプト１６が登録済みか否か判断する（ｓｔｅｐ２１）。

【００７８】

ここで、指定されたｓｃｒｉｐｔＮａｍｅ、およびＡｕｔｈＮａｍｅをもつ権限スクリプト１６がメモリ上に記録されていない場合（登録済みでない場合）には（ｓｔｅｐ２２）、権限スクリプト処理部１５は、ＳＯＡＰ処理部２を介してエラーレスポンスメッセージを返信する（ｓｔｅｐ２０）。

【００７９】

また、指定されたｓｃｒｉｐｔＮａｍｅ、およびＡｕｔｈＮａｍｅをもつ権限スクリプト１６がメモリ上に記録されている場合（登録済みである場合）には、権限スクリプト処理部１５は、指定されたｓｃｒｉｐｔＮａｍｅを持つ権限スクリプト１６を有効とし（ｓｔｅｐ２３）、以降、各権限付与サービス（本実施形態では認証・権限サービスＡ・７及び権限サービスＢ・９）が該権限スクリプト１６を参照する。

【００８０】

以上に示した処理により、外部デバイス（管理端末ＰＣ１８）から、複合機Ｍ１へのアプリケーションに応じた権限スクリプト１６の登録処理、および有効化処理が完了する。システム管理者は必要、用途に応じて該当するアプリケーションの権限スクリプト１６を登録、削除、有効化処理を繰り返し実行することが可能である。

【００８１】

マッピングスクリプト６、および権限スクリプト１６の登録処理が完了すると、本実施形態の複合機Ｍ１における各サービスが稼動可能となる。

【００８２】

次に、本実施形態の複合機Ｍ１の特徴となる処理を行う認証、権限処理の制御フローの詳細を説明する。尚、ここで、図１６に示した第１の実施形態における情報処理装置１７０と、図１に示す本実施形態の複合機Ｍ１との機能ブロックの対応について示す。図１６における受信部１７１は、本実施形態においては図１におけるＳＯＡＰ処理部２に相当し、図４－１はその制御フローを示すフローチャートである。また、図１６における調停処理部１７２は、本実施形態においては図１における調停サービス部３に相当し、図４－２はその制御フローを示すフローチャートである。

【００８３】

また、図１６におけるマッピングテーブル１７３は、本実施形態においては図１におけるマッピングスクリプト６に相当する。また、図１６における認証・権限処理サービス部１７４は、本実施形態においては図１における認証・権限サービスＡ・７、認証サービスＢ・８、及び権限サービスＢ・９（まとめて認証・権限サービスとする）に相当し、図４－３はその制御フローを示すフローチャートである。また、図１６における権限情報テーブル１７５は図１における権限スクリプト１６に相当する。また、図１６におけるサービス部１７６は、本実施形態においては図１に示す各サービスであるプリントサービス１０、スキャンサービス１１、ストレージサービス１２、ＦＡＸサービス１３に相当し、図４－４はその制御フローを示すフローチャートである。

【００８４】

以下、図４－１～図４－４に示すフローチャートに従い、制御の流れを説明する。
まず、図４－１に示すとおり、複合機Ｍ１が稼動中、ＳＯＡＰ処理部２はクライアントＰＣ・１７から送信されるＳＯＡＰリクエストの受信を、ＴＣＰ／ＩＰ／ＵＤＰプロトコルスタックを介して常時監視し（ｓｔｅｐ１）、ＳＯＡＰリクエストの受信を確認すると（ｓｔｅｐ２）、受信したＳＯＡＰエンベロープを、調停サービス部３に対し送信する（ｓｔｅｐ３）。続いて、調停サービス部３の処理について図４－２を用いて説明し、図４－１におけるＳＯＡＰ処理部２の他の処理についての説明は、後述する。

【００８５】
図４－２に示すとおり、調停サービス部３は、ＳＯＡＰ処理部２からのＳＯＡＰエンベロープの受信を常時監視し（ｓｔｅｐ４）、ＳＯＡＰ処理部２から、ＳＯＡＰエンベロープを受信した場合（ｓｔｅｐ５）、調停サービス部３は、ＳＯＡＰヘッダの記述内容をパース（解析）する（ｓｔｅｐ６）。

【００８６】
図５は、ＳＯＡＰエンベロープのフォーマット例を示した図である。図５のＳＯＡＰエンベロープは、ＳＯＡＰヘッダ部とＳＯＡＰボディ部に大きく分かれる。図５に示すように、該ＳＯＡＰヘッダにはＷＳ－Ａｄｄｒｅｓｓｉｎｇ仕様に基づき、リクエスト対象とするサービス名称が＜ＡＣＴＩＯＮ＞タグ５１のコンテンツとして記述される。また、標準化団体ＯＡＳＩＳにより策定されたＷＳ－Ｓｅｃｕｒｉｔｙ　ＵｓｅｒｎａｍｅＴｏｋｅｎ　Ｐｒｏｆｉｌｅ　１．０仕様に基づき＜ＵｓｅｒｎａｍｅＴｏｋｅｎ＞タグ５２のコンテンツとして認証情報が記述されている。
（参考ＵＲＬ：http://schemas.xmlsoap.org/ws/2003/03/addressing/）

【００８７】
ｓｔｅｐ６において調停サービス部３は図５に示すようなＳＯＡＰヘッダをパースし、まず、＜ＡＣＴＩＯＮ＞タグ５１の有無、およびそのコンテンツ内容をチェックする。＜ＡＣＴＩＯＮ＞タグ５１が記述されていない場合、あるいは＜ＡＣＴＩＯＮ＞タグ５１が存在しても、そのコンテンツが無い、すなわち空タグであった場合は不正要求として、調停サービス部３はＳＯＡＰ処理部２に対しエラーを通知する（ｓｔｅｐ７）。また、＜ＡＣＴＩＯＮ＞タグ５１のコンテンツが存在すると判断した場合、調停サービス部３は、あらかじめＥｎａｂｌｅＳｃｒｉｐｔにより有効化していされたマッピングスクリプト６の内容をメモリ装置制御部５を介して読み出し（ｓｔｅｐ８）、＜ＡＣＴＩＯＮ＞タグ５１のコンテンツとして記述されたサービスが、該マッピングスクリプト６に記述されているか否かを検索する（ｓｔｅｐ９）。

【００８８】
検索した結果、＜ＡＣＴＩＯＮ＞タグ５１に記述されたサービスに該当する登録が見つからなかった場合、調停サービス部３はＳＯＡＰ処理部２に対し不正要求としてエラーを通知する（ｓｔｅｐ１０）。検索した結果、＜ＡＣＴＩＯＮ＞タグ５１に記述されたサービスに該当する登録が見つかった場合、続けて、指定されたサービスに対応づけられた認証サービス、権限サービスの記述情報の有無を検索する（ｓｔｅｐ１１）。

【００８９】
ｓｔｅｐ１１において検索した結果、マッピングスクリプト６に指定されたサービスに対応づけられた認証サービス、権限サービスの記述が見つからなかった場合、該サービスに対する認証、権限処理は不要と判断し、調停サービス部３は、実行許可をＳＯＡＰ処理部２へ通知する（ｓｔｅｐ１２）。この場合、調停サービス部３からＳＯＡＰ処理部２に対しＳＯＡＰエンベロープが返信される。

【００９０】
ｓｔｅｐ１１において検索した結果、マッピングスクリプト６に指定されたサービスに対応づけられた認証サービス、権限サービスの記述が見つかった場合、調停サービス部３は、マッピングスクリプト６に記述されたＵＲＬに対し、ＳＯＡＰエンベロープを送信する（ｓｔｅｐ１３）。ここでマッピングスクリプト６に記述されたＵＲＬとは、認証・権限サービスのＵＲＬである。すなわち、調停サービス部３は、ＳＯＡＰエンベロープを認

証・権限サービスへ送信する。以下、図４－２に示す調停サービス部３の説明を保留し、図４－３に示す認証・権限サービスの処理について説明する。

【００９１】

図４－３に示すとおり、調停サービス部３から、ＳＯＡＰエンベロープを受信（ｓｔｅｐ１４）した認証・権限サービスは、ＳＯＡＰエンベロープの記述内容をパースして、図５に示す＜ＵｓｅｒｎａｍｅＴｏｋｅｎ＞タグ５２よりＵｓｅｒｎａｍｅＴｏｋｅｎ情報を取得する（ｓｔｅｐ１５）。次に、認証・権限サービスは、取得したＵｓｅｒｎａｍｅＴｏｋｅｎ情報を元に認証処理を実行する（ｓｔｅｐ１６）。その結果、指定されたＵｓｅｒｎａｍｅＴｏｋｅｎに相当するユーザ情報が認証・権限サービスに登録されていないと判断した場合（ｓｔｅｐ１７）、認証・権限サービスは調停サービス部３に対し不正要求としてＮＧを通知する（ｓｔｅｐ１８）。

【００９２】

ｓｔｅｐ１６における認証処理の結果、指定されたＵｓｅｒｎａｍｅＴｏｋｅｎに相当するユーザ情報が認証・権限サービスに登録されている（＝認証ＯＫ）と判断した場合（ｓｔｅｐ１９）、認証・権限サービスは、あらかじめＥｎａｂｌｅＡｕｔｈＳｃｒｉｐｔにより有効化していされた権限スクリプト１６の内容をメモリ装置制御部５を介して読み出し、図５に示す＜Ｕｓｅｒｎａｍｅ＞タグ５３のコンテンツとして記述されたユーザ名が、該権限スクリプト１６に記述されているか否かを検索する（ｓｔｅｐ２０）。

【００９３】

検索した結果、＜Ｕｓｅｒｎａｍｅ＞タグ５３に記述されたユーザ名に該当する登録が見つからなかった場合（ｓｔｅｐ２１）、調停サービス部３から認証・権限サービスに対して送信されたＳＯＡＰエンベロープに記述されるリクエストに対して、実行制限、アクセス制限無しと認証・権限サービスは処理する。この場合、認証・権限サービスは例えばＳＡＭＬ（Ｓｅｃｕｒｉｔｙ Ａｓｓｅｒｔｉｏｎ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）１．１に従ったＳＯＡＰエンベロープを生成し（ｓｔｅｐ２２）、該ＳＯＡＰエンベロープを調停サービス部３に対し返信する（ｓｔｅｐ２３）。返信処理完了後、認証・権限サービスは、ｓｔｅｐ１４に戻り調停サービス部３からのＳＯＡＰエンベロープの受信待ちに移行する。

【００９４】

検索した結果、＜Ｕｓｅｒｎａｍｅ＞タグ５３に記述されたユーザ名に該当する登録が見つかった場合（ｓｔｅｐ２４）、認証・権限サービスは、続けて、指定されたユーザに対応づけられた実行権限、アクセス制限に関する記述情報の有無を検索する（ｓｔｅｐ２５）。ｓｔｅｐ２５において検索した結果、権限スクリプト１６に、指定されたユーザに対応づけられた実行権限、アクセス制限の記述が見つからなかった場合（ｓｔｅｐ２６）、認証・権限サービスは、調停サービス部３から認証・権限サービスに対して送信されたＳＯＡＰエンベロープに記述されるリクエストに対して、実行制限、アクセス制限無しと処理する。この場合、認証・権限サービスは、ＳＡＭＬ１．１に従ったＳＯＡＰエンベロープを生成し（ｓｔｅｐ２２）、該ＳＯＡＰエンベロープを調停サービス部３に対し返信する（ｓｔｅｐ２３）。返信処理完了後、認証・権限サービスは、ｓｔｅｐ１４に戻り調停サービス部３からのＳＯＡＰエンベロープの受信待ちに移行する。

【００９５】

ｓｔｅｐ２５において検索した結果、権限スクリプト１６に、指定されたユーザに対応づけられた実行権限、アクセス制限の記述が見つかった場合（ｓｔｅｐ２７）、権限スクリプト処理部１５は、調停モジュール部３より送信されたＳＯＡＰエンベロープのｂｏｄｙ部の内容をパースする（ｓｔｅｐ２８）。図５のＳＯＡＰボディ部にプリントサービスに対するリクエスト内容が記述されたＳＯＡＰエンベロープを示している。この例においては、＜ＪｏｂＮａｍｅ＞タグ５４において、そのジョブ名称をＭｙＪｏｂと設定し、＜Ｃｏｌｏｒ＞タグ５５においてＦＵＬＬＣＯＬＯＲ、即ちフルカラー印刷を指定し、＜Ｃｏｐｙ＞タグ５６において１００、即ち１００部の印刷を指定し、＜Ｓｉｄｅｓ＞タグ５７においてＯＮＥＳＩＤＥ、即ち片面印刷を指定し、＜ＭｅｄｉａＳｉｚｅ＞タグ５８に

おいて出力用紙サイズをＡ４と指定し、＜ＭｅｄｉａＴｙｐｅ＞タグ５９において出力用紙のタイプをＰＨＯＴＯＱＵＡＬＩＴＹ、即ち写真品質の上質紙を指定し、＜ＰｒｉｎｔＱｕａｌｉｔｙ＞タグ５Ａにおいて印刷クオリティをＨＩＧＨ、即ち高品位印刷を指定している。

【００９６】

権限スクリプト処理部１５は、権限スクリプト１６に記述された実行権限、アクセス制限に関する記述を参照し、該権限スクリプト１６に記述された内容とＳＯＡＰエンベロープのｂｏｄｙ部の内容とを比較する。図６は、権限スクリプト１６の記述例を示す図である。図６の例ではリクエスタＸＸＸに対する記述を抜粋したものであり、権限スクリプト１６には登録されたリクエスタの数だけ同様の記述が記録されている。図６においては、ユーザ名（ｕｓｅｒｎａｍｅ）がＸＸＸのリクエスタに対し、＜Ｃｏｌｏｒ＞タグ６１においてＢＬＡＣＫＡＮＤＷＨＩＴＥ、即ち白黒印刷のみを許可し、＜Ｃｏｐｙ＞タグ６２において１０、即ち１０部までの印刷を許可し、＜Ｓｉｄｅｓ＞タグ６３においてＴＷＯ－ＳＩＤＥ、即ち両面印刷のみを許可し、＜ＭｅｄｉａＳｉｚｅ＞タグ６４において出力用紙のサイズをＡ４のみ許可し、＜ＭｅｄｉａＴｙｐｅ＞タグ６５において出力用紙のタイプをＰＬＡＩＮＰＡＰＥＲ、即ち普通紙のみを許可し、＜ＰｒｉｎｔＱｕａｌｉｔｙ＞タグ６６において印刷クオリティをＨＩＧＨ、即ち高品位印刷を許可している。

【００９７】

ｓｔｅｐ２８のパースの結果、ＳＯＡＰエンベロープに記述された要求内容に、アクセス制限を越える要求が検出された場合（ｓｔｅｐ２９）、権限スクリプト処理部１５は、ＳＯＡＰエンベロープボディに記述された要求内容を、権限スクリプト６の内容に応じて書換えを実行する（ｓｔｅｐ３０）。具体的には、図５に示すＳＯＡＰエンベロープボディに対して、図６に示す権限スクリプト例を用いて書換えを行う場合、リクエスタＸＸＸからのリクエスト内容は、＜Ｃｏｌｏｒ＞，＜Ｃｏｐｙ＞，＜Ｓｉｄｅｓ＞，＜ＭｅｄｉａＴｙｐｅ＞の項目に関して、アクセス制限を越える要求がなされており、権限スクリプト処理部１５は、各項目に対し、その記述内容を変更する。

【００９８】

また、権限スクリプト処理部１５は、さらにＳＯＡＰヘッダ部に対しその変更履歴を記述する（ｓｔｅｐ３１）。図７は、図５のＳＯＡＰエンベロープに対する改編の一例を示す図である。図７に示すように、ＳＯＡＰヘッダ部に対し改編対象となったタグに関して、改編する前の要求内容を＜ＭｏｄｉｆｉｅｄＲｅｑｕｅｓｔ＞タグ７１の子タグとして各々記述する。改編したＳＯＡＰエンベロープは、メモリ装置制御部５を介してメモリ上に記録される。また、図７に示すように、ＳＯＡＰボディ部は、＜Ｃｏｌｏｒ＞タグ５５がＢＬＡＣＫＡＮＤＷＨＩＴＥに書き換えられ、＜Ｃｏｐｙ＞タグ５６が１０に書き換えられるなど、図６に示した権限スクリプト１６に応じた改編が行われている。

【００９９】

ＳＯＡＰエンベロープボディに対し記述された全タグに対して以上の処理が完了すると（ｓｔｅｐ３２）、認証・権限サービスはＳＡＭＬ１．１に従った処理結果に基づいてＳＯＡＰエンベロープに対して追記し（ｓｔｅｐ２２）、該ＳＯＡＰエンベロープを調停サービス部３に対し返信する（ｓｔｅｐ２３）。返信処理完了後、認証・権限サービスは、ｓｔｅｐ１４に戻り調停サービス部３からのＳＯＡＰエンベロープの受信待ちに移行する。以下、図４－２に示す、調停サービス部３の処理の説明に戻る。

【０１００】

図４－２に示すとおり、認証・権限サービスから認証結果を受信（ｓｔｅｐ２４）した調停サービス部３は、マッピングスクリプト６に引き続き認証・権限サービスの呼び出し手続きの記述の有無を確認し（ｓｔｅｐ２５）、記述がある場合はｓｔｅｐ１３からｓｔｅｐ２５までのプロセスを繰り返す。マッピングスクリプト６において認証・権限サービスの呼び出し手続きの記述が完了している場合、調停サービス部３は、認証・権限サービスから受信した認証結果をＳＯＡＰ処理部２に対して返信する（ｓｔｅｐ２６）。返信処理完了後、調停サービス部３は、ｓｔｅｐ４に戻りＳＯＡＰ処理部２からのＳＯＡＰヘッ

ダ受信待ち状態に移行する。

【０１０１】

以上説明したように、調停サービス部３は、マッピングスクリプト６の記述に従い、クライアントＰＣ・１７から実行指定されたサービスに対する認証・権限サービスの呼び出しを実行する。これにより、調停サービス部３は、マッピングスクリプト６の記述内容によって、それぞれ異なる認証・権限サービスを実施することが可能となる。

【０１０２】

本実施形態におけるマッピングスクリプト６においては、＜ｘｍｌｓｃｒｉｐｔ＞タグの属性ｎａｍｅに、マッピングスクリプト６を識別するファイル名が記述されている。該ファイル名は、先に説明したＵｐｌｏａｄＳｃｒｉｐｔ関数で指定したｓｃｒｉｐｔＮａｍｅにより設定される。＜ｍａｐｐｉｎｇ＞タグの子タグとして、対象となるサービス情報をＵＲＬ形式で記述する＜Ｓｅｒｖｉｃｅ＞タグと、そのサービスに対応づけられた認証、権限処理サービス情報をＵＲＬ形式で記述する＜ＡｕｔｈＳｅｒｖｉｃｅ＞タグが定義されている。

【０１０３】

図８は、マッピングスクリプト６の例１を示す図である。図８に示すマッピングスクリプト６のファイル名は"Ｓａｍｐｌｅ１"である。図８の＜ｍａｐｐｉｎｇ＞タグ内のコンテンツ（＜Ｓｅｒｖｉｃｅ＞タグと＜ＡｕｔｈＳｅｒｖｉｃｅ＞タグ）に示すように、上から順に以下のようなサービスと認証・権限サービスを対応させている。

・プリントサービスに対して、認証・権限サービスＡを関連付け。
・スキャンサービスに対して、認証サービスＢを関連付け。
・ストレージサービスに対して、権限サービスＢを関連付け。
・ＦＡＸサービスに対して、認証・権限サービスＣを関連付け。

【０１０４】

調停サービス部３は、図８に示すマッピングスクリプト６を基に、それぞれのサービスに対し、それぞれ異なる認証・権限サービスを実施する。従って、調停サービス部３は、例えばプリントサービスにはパスワード認証、スキャンサービスにはＰＩＮコード認証、ＦＡＸサービスにはＩＣカード認証と、異なる認証処理を実施することが可能となる。これにより、複合機Ｍ１は、サービス指向アーキテクチャによる種々のサービス提供時に、その効率の良さ、柔軟性を損うことなく、最適なセキュリティを簡便に実現することができる。

【０１０５】

次に、図８に示したマッピングスクリプト６の例１と異なるケースを幾つか示す。

図９は、マッピングスクリプト６の例２を示す図である。この図９に示すマッピングスクリプト６は、同じプリントサービスに対し、異なる認証、権限処理を実施するケースである。図９の行９１で定義するアドホックプリントサービスは、ネットワークＮ１に接続したクライアントＰＣ・１７に対し簡易プリント機能を提供するサービスである。このアドホックプリントサービスは、複合機Ｍ１に実装された認証・権限サービスＡ・７により、認証、権限処理を実施するサービスである。しかし、行９２で定義する課金プリントサービスは、ネットワークＮ１を介して複合機Ｍ１の外部において稼動状態にある認証・権限サービスＣ・１４において認証・権限処理を実施するサービスとして処理される。

【０１０６】

このような記述により、例えば、認証・権限サービスＡ・７が部門コードによる簡易な認証・権限サービスであるのに対し、認証・権限サービスＣ・１４はクレジットカード番号、暗証番号、およびランタイムパスワードによるセキュアレベルの高い認証・権限処理を実施することが可能となる。

【０１０７】

図１０は、マッピングスクリプト６の例３を示す図である。この図１０に示すマッピングスクリプト６は、それぞれ単独で機能するスキャンサービスとストレージサービスを組み合わせて、新規のサービスであるスキャン－ストレージサービスを提供するケースを示

している。図１０の記載１１１、記載１１２に示すように、スキャンサービス、ストレージサービスに対しては、それぞれ認証・権限サービスＡ・７、認証サービスＢ・８を関連付ける。また、図１０の記載１１３、１１４に示すように、新規サービスであるスキャンーストレージサービスに対しては認証・権限サービスＣ・１４を関連付けている。

【０１０８】

図１１は、マッピングスクリプト６の例４を示す図である。この図１１に示すマッピングスクリプト６は、記載１２１、１２２に示すように、プリントサービス、スキャンサービス共に認証・権限サービスＡ・７を関連づけるものである。これにより、両サービスは認証・権限サービスＣ・１４で管理されるデータベースに基づいて処理されるため、両サービスを利用するユーザクライアントは同一のクレデンシャル（証明書）情報に基づき認証、権限付与が実施される、即ちシングルサインオンをプリント、スキャンサービスに対し実施することが可能となる。

【０１０９】

図１２は、マッピングスクリプト６の例５を示す図である。この図１２に示すマッピングスクリプト６は、プリントサービスに対し、認証サービスＢ・８、および権限サービスＢ・９を記述して、対応づけている。しかし、この場合、調停サービス部３は該スクリプトに記述された順番に、各人証、権限サービスを呼び出す。そのため、認証サービスＢ・８により認証処理が実施され、該認証サービスにより付与されたアサーションを、次の処理である権限サービスＢ・９に対し通知することで権限情報の付与を受けることが可能となる。即ち、認証処理を多重に実施する必要がある場合、あるいは、認証処理と権限処理とを切り分け、ユースケースによってその組み合わせを変更する必要がある場合に、この図１２に示すようなマッピングスクリプト６を記述して、メモリに登録する。

【０１１０】

本実施例においては、これら例１～５に示した複数のマッピングスクリプト６をメモリに登録することが可能であり、ＥｎａｂｌｅＳｃｒｐｔで指定されたスクリプトの記述に従い、サービスと認証・権限サービスとの対応付け処理が実施される。従って、本実施形態における複合機Ｍ１においては、マッピングスクリプト６の記述を変更するのみで、実施する認証・権限付与処理をユースケースに応じて変更、更新するこが可能となっている。すなわち、複合機Ｍ１は、サービス指向アーキテクチャによる種々のサービス提供時に、その効率の良さ、柔軟性を損うことなく、最適なセキュリティを簡便に実現することができる。

【０１１１】

次に、上述した図４－２におけるｓｔｅｐ７、１０、１２、及び２６において調停サービス部３がなんらかの処理結果をＳＯＡＰ処理部２に返信した後の、ＳＯＡＰ処理部２における処理について図４－１を用いて説明する。

図４－１に示すとおり、調停サービス部３から処理結果を受信（ｓｔｅｐ２６）したＳＯＡＰ処理部２は、その処理結果を解析する（ｓｔｅｐ２７）。ここで、調停サービス部３から通知された処理結果がＮＧ（エラー返信）であった場合には、要求クライアントであるクライアントＰＣ・１７に対し不正要求としてＳＯＡＰ　Ｆａｕｌｔを返信する（ｓｔｅｐ２８）。

【０１１２】

また、調停サービス部３から通知された処理結果がＯＫであった場合、即ち調停サービス部３からＳＯＡＰエンベロープが送信された場合には、ＳＯＡＰ処理部２は、ＳＯＡＰボディ部に記述されたサービス属性情報をパースする（ｓｔｅｐ２９）。次に、ＳＯＡＰ処理部２は、該当するサービスに対する属性情報を読み取り、該属性情報をサービスに対して通知し、サービスの実行を要求する（ｓｔｅｐ３０）。これにより、図４－４に示す、サービスの処理フローに以降する。

【０１１３】

図４－４に示すとおり、ＳＯＡＰ処理部２からサービス実行要求を受信したサービスは、通知されたジョブ属性に基づき、サービス処理を実行する（ｓｔｅｐ３１）、その処理

結果をＳＯＡＰ処理部２に対して返信する（ｓｔｅｐ３２）。次に、サービスは、処理結果返信後、ＳＯＡＰ処理部２からのサービス実行要求受信待ちに移行する。これにより、図４－１に示すＳＯＡＰ処理部２の処理に移行する。

【０１１４】

図４－１において、サービスから処理結果を受信したＳＯＡＰ処理部２は、その処理結果に基づきＳＯＡＰボディ部にＳＯＡＰレスポンスを生成する（ｓｔｅｐ３３）。次に、ＳＯＡＰ処理部２は、調停サービス部３を介して、認証・権限サービスよりクライアントＰＣ・１７に返信すべくアサーション情報、およびアクセス制限に基づき記録された変更履歴が挿入されたＳＯＡＰヘッダと、該ＳＯＡＰボディ部とを連結し、返信用のＳＯＡＰエンベロープを生成する（ｓｔｅｐ３４）。

【０１１５】

次に、ＳＯＡＰ処理部２は、ＳＯＡＰエンベロープ生成が完了した時点で、該エンベロープをクライアントＰＣ・１７に対して返信する（ｓｔｅｐ３５）。ＳＯＡＰレスポンス返信後、ＳＯＡＰ処理部２は、ｓｔｅｐ１に戻り、クライアントＰＣ・１７からのＳＯＡＰエンベロープ受信待ちに移行する。

【０１１６】

リクエストに対する処理結果を受信したクライアントＰＣ・１７は、必要に応じて返信されたＳＯＡＰエンベロープのヘッダ部を解析し、要求したジョブ内容に対し制限処理が付与されたか否か、およびその詳細内容を判断することが可能である。

以上説明した一連のプロセスを繰り返すことにより、指定されたサービスに対する認証、権限処理を実施することが可能となる。

【０１１７】

［他の実施形態］

以下に、上述した実施形態の種々の応用例や変形例を示す。

上述した実施形態において、サービスと、認証、権限付与サービスの対応づけを記述したマッピングスクリプト６、および権限付与、アクセス制限情報を記述した権限スクリプト１６を登録する手段として、外部デバイス、即ちシステム管理者によって管理された管理端末ＰＣ・１８からネットワークＮ１を介して、マッピングスクリプト処理部４、および権限スクリプト処理部１５に対して送信、登録する手段を説明したが、この限りではなく、システム管理者によって管理された管理端末ＰＣ・１８からネットワークＮ１を介して、マッピングスクリプト処理部４、および権限スクリプト１５に対して、それぞれマッピングスクリプト６、権限スクリプト１６が登録されているサーバのＵＲＬを登録してもよい。これにより、マッピングスクリプト処理部４、および権限スクリプト処理部１５が、該ＵＲＬを保有するサーバからマッピングスクリプトや権限スクリプトをダウンロードし、自身が管理するメモリ上に登録するという構成を実現できる。

【０１１８】

また、コンピュータと、上述した実施形態の複合機Ｍ１とをＵＳＢ、ＩＥＥＥ１３９４などのローカルインタフェイスとで接続し、該インタフェイスを介してマッピングスクリプト処理部４、権限スクリプト処理部１５に対しマッピングスクリプトや権限スクリプトを登録する手段でも実現可能である。

【０１１９】

また、上述したスクリプトはＣＤ－ＲＯＭ、コンパクトフラッシュ（登録商標）、メモリスティック等の記録媒体に記録し、複合機Ｍ１に対して読取可能に設置されたその記録媒体から、マッピングスクリプト処理部４がマッピングスクリプトを、権限スクリプト処理部１５が権限スクリプトを読み取る機能を備えることでも実現可能である。また、本スクリプトは権限を与えられた管理者が、複合機Ｍ１が備える操作部を介して、入力する手段でも実現可能である。

【０１２０】

また、上述した実施形態の複合機Ｍ１においては、サービスと、そのサービスに対応付けた認証、権限付与サービスの情報をＸＭＬの書式で記述したが、他のスクリプト記述言

語、あるいは単純なテキストデータであっても記述可能である。同様に本実施形態の複合機Ｍ１においては、サービスを利用するリクエスタに対し、権限付与、アクセス制限に関する情報をＸＭＬの書式で記述したが、他のスクリプト記述言語、あるいは単純なテキストデータであっても記述可能である。

【０１２１】

また、上述した実施形態においては、複数のマッピングスクリプト６をマッピングスクリプト処理部４が管理し、指定されたマッピングスクリプト６の記述を有効とする例を記述したが、一つのマッピングスクリプト６に対し、複数のパタンを記述し、いずれのパタンを採用するかを指定することで同様の効果を実現することが可能である。

【０１２２】

図１３は、プリントサービスに対し、その認証、権限サービスへの関連づけを、セキュリティレベルに応じて記述した図ある。例えば、このセキュリティレベルの権限を与えられた管理者が、複合機１Ｍが備える操作部を介して切り替えることで、セキュリティレベル１において認証処理が不要であったプリントサービスが、セキュリティレベル２に切り替えられることで、ＩＣカードによる認証と、ユーザごとに異なる利用制限が付与されるプリントサービスへと変更される。

【０１２３】

また、上述した実施形態の調停サービス部３は、複合機Ｍ１のノード内に実装された形態を説明したが、図１４に示すように、調停サービス機能を実現する論理ユニットを、ネットワークＮ１を介して外部に独立させた形態であってもよい。この場合、調停サービス機能を実現する論理ユニットは、例えばコンピュータによるサーバ上に独立して実装されることで実現可能である。なお、この場合、調停サービス機能を実現する論理ユニットと、複合機Ｍ１との間の通信はＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）などの手段を用いて、認証、権限サービスによる処理結果が、第三者によって改竄されないように保護する必要がある。

【０１２４】

同様に、上述した実施形態においては認証・権限サービスＡ・７、権限サービスＢ・８は複合機Ｍ１のノード内に実装された形態であったが、この限りではなく、図１における認証・権限サービスＣ・１４に示すとおり、認証・権限サービス機能を実現する論理ユニットを、ネットワークＮ１を介して外部に独立させた形態であってもよい。尚、認証・権限サービス機能を実現する論理ユニットは、例えばコンピュータによるサーバ上に独立して実装されることで実現可能である。

【０１２５】

図１５は、認証・権限サービスＣ・１４の機能構成例を示す図である。図１５に示すように、認証・権限サービスＣ・１４は、ＴＣＰ／ＩＰ／ＵＤＰプロトコルスタック１、ＳＯＡＰ処理部２、認証・権限サービスＣ処理部１５０、権限スクリプト処理部１５、メモリ装置制御部４、および権限スクリプト１６から構成される。尚、図１と同じ符号を付与している構成部分は、図１と同様の機能を有するものである。

【０１２６】

なお、上述した実施形態においては調停サービス部３と、認証、権限サービスはＳＡＭＬプロトコルを使用して通信しているが、該プロトコルは各認証、権限サービス固有のプロトコルである場合においても実施可能であり、調停サービスが各認証、権限サービスに対応したプロトコルに基づき通信する。そのため、この場合においても、サービスは認証、権限サービスの存在を意識することなく、各ユースケースにおいて最適な認証、権限処理を実施することが可能である。

【０１２７】

また、上述した実施形態においては、リクエスト対象とするサービス名称の記述をＷＳ－Ａｄｄｒｅｓｓｉｎｇ仕様に基づき記述した例を示したが、調停サービスにおいて（Ａｃｔｉｏｎ）タグが検出できなかった場合には、ＳＯＡＰボディ部をパースし、そこに記述されるサービス名称を取得する手段によっても実施可能である。

【０１２８】
また、上述した実施形態においては認証情報に関してはＯＡＳＩＳ　ＷＳ－ｓｅｃｕｒｉｔｙ　ＵｓｅｒｎａｍｅＴｏｋｅｎ　Ｐｒｏｆｉｌｅの規定に基づき記述された例を示したが、これら標準仕様において定義されていない認証クレデンシャルにも対応可能であり、この場合、マッピングスクリプトにいずれのタグがクレデンシャル情報に該当するか記述することで対応、実施することが可能である。
【０１２９】
また、上述した実施形態においてはリクエスタからのリクエスト内容が、付与された権限、アクセス制限を越える場合、そのリクエスト内容を書き換えた結果を実行し、その結果をリクエスタに対し通知結果を受信したリクエスタがそのヘッダ部に記述された内容を解析することで、リクエスト内容に対し制限処理が実施されたことを知るフローを示した。しかし、他の実施形態として、図４－１のｓｔｅｐ２６において、調停サービス部からＳＯＡＰエンベロープが返信され、かつ、そのヘッダ部に＜ＭｏｄｉｆｉｅｄＲｅｑｕｅｓｔ＞タグがある場合、リクエスタに対しリクエストが改編された旨を通知し、リクエスタから許諾通知を受け取った場合のみサービスの実行要求を発行する（図４－１のｓｔｅｐ３０）制御フローを実施することも可能であり、この場合、権限付与サーバにより改編されたジョブ内容をサービス実行前にリクエスタが知ることが可能となり、より利便性が向上する。
【０１３０】
また、上述した実施形態において図１に示した複合機Ｍ１内の各処理部は、各処理部の機能を実現する為のプログラムをメモリ（例えば図１７のＨＤＤ１０３）から読み出してＣＰＵ１０１が実行することによりその機能を実現させるものであったが、これに限定されるものではなく、各処理の全部または一部の機能を専用のハードウェアにより実現してもよい。また、上述したメモリは、ＨＤＤ１０３に限定されるものではなく、光磁気ディスク装置、フラッシュメモリ等の不揮発性のメモリや、ＣＤ－ＲＯＭ等の読み出しのみが可能な記録媒体、ＲＡＭ以外の揮発性のメモリ、あるいはこれらの組合せによるコンピュータ読み取り、書き込み可能な記録媒体より構成されてもよい。
【０１３１】
また、図１に示した複合機Ｍ１内の各機能を実現する為のプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより各処理を行っても良い。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。具体的には、記憶媒体から読み出されたプログラムが、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こまれた後、そのプログラムの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなど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む。
【０１３２】
また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。
【０１３３】
また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

また、上記プログラムは、前述した機能の一部を実現する為のものであっても良い。さらに、前述した機能をコンピュータシステムに既に記録されているプログラムとの組合せで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【０１３４】

また、上記のプログラムを記録したコンピュータ読み取り可能な記録媒体等のプログラムプロダクトも本発明の実施形態として適用することができる。上記のプログラム、記録媒体、伝送媒体およびプログラムプロダクトは、本発明の範疇に含まれる。

以上、この発明の実施形態について図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【図面の簡単な説明】

【０１３５】

【図１】本実施形態における複合機Ｍ１が有する機能構成を示すブロック図である。

【図２】本実施形態の複合機Ｍ１におけるマッピングスクリプト６の登録処理を示すフローチャートである。

【図３】本実施形態の複合機Ｍ１における権限スクリプト１６の登録処理を示すフローチャートである。

【図４－１】図１におけるＳＯＡＰ処理部２の制御フローを示すフローチャートである。

【図４－２】図１における調停サービス部３の制御フローを示すフローチャートである。

【図４－３】図１における認証・権限サービスの制御フローを示すフローチャートである。

【図４－４】図１に示す各サービスの制御フローを示すフローチャートである。

【図５】ＳＯＡＰエンベロープのフォーマット例を示した図である。

【図６】権限スクリプト１６の記述例を示す図である。

【図７】図５のＳＯＡＰエンベロープに対する改編の一例を示す図である。

【図８】マッピングスクリプト６の例１を示す図である。

【図９】マッピングスクリプト６の例２を示す図である。

【図１０】マッピングスクリプト６の例３を示す図である。

【図１１】マッピングスクリプト６の例４を示す図である。

【図１２】マッピングスクリプト６の例５を示す図である。

【図１３】プリントサービスに対し、その認証、権限サービスへの関連づけを、セキュリティレベルに応じて記述した図である。

【図１４】他の実施形態における情報処理装置を含むネットワーク画像処理システム例を示す図である。

【図１５】認証・権限サービスＣ・１４の機能構成例を示す図である。

【図１６】第１の実施形態における情報処理装置１７０の機能モデル例を示すモデル図である。

【図１７】本発明の第２の実施形態であるネットワーク対応型複合機Ｍ１を含むネットワーク画像処理システムの概略構成を示す図である。

【図１８－１】従来の個々のサービス（サービスＡやサービスＢ）において、各々認証処理、権限付与処理、およびユーザ認証情報を保持するデータベースが組み込まれた形態例を示す図である。

【図１８－２】従来のサービスを提供する複数の装置（サービスＡ、Ｂ）の外部に認証、権限処理を行う外部装置（認証処理装置）を備える形態例を示す図である。

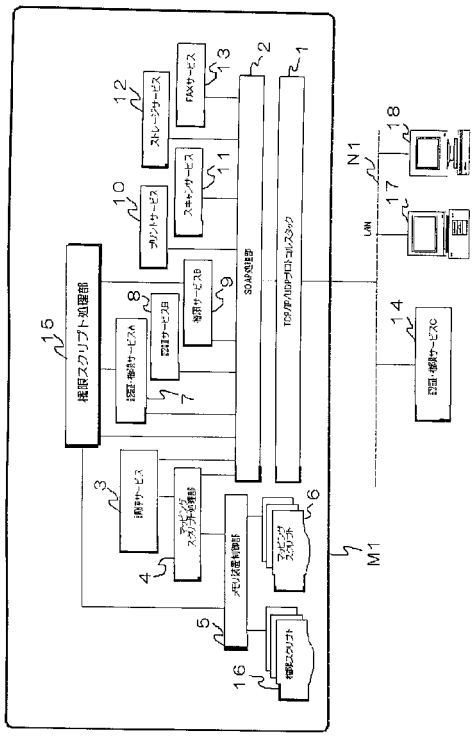
【符号の説明】

【０１３６】

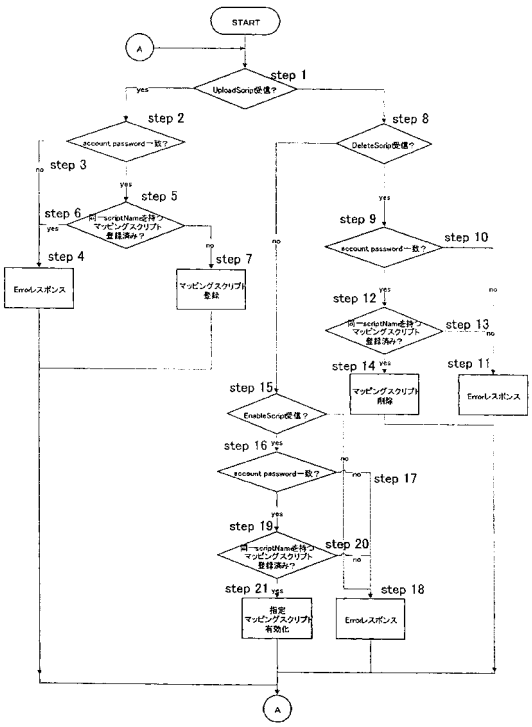
Ｃ１、Ｃ２	コンピュータ端末
Ｎ１	ネットワーク
Ｍ１	複合機（ネットワーク対応型ＭＦＰ）
１	ＴＣＰ／ＩＰ／ＵＤＰプロトコルスタック処理部

2	ＳＯＡＰ処理部
3	調停サービス部
4	マッピングスクリプト処理部
5	メモリ装置制御部
6	マッピングスクリプト
7	認証・権限サービスＡ
8	認証サービスＢ
9	権限サービスＢ
１０	プリントサービス
１１	スキャンサービス
１２	ストレージサービス
１３	ＦＡＸサービス
１４	認証・権限サービスＣ
１５	権限スクリプト処理部
１６	権限スクリプト
１００	通信装置
１０１	ＣＰＵ
１０２	メモリ
１０３	ＨＤＤ
１０４	プリンタ
１０５	スキャナ
１０６	画像処理装置

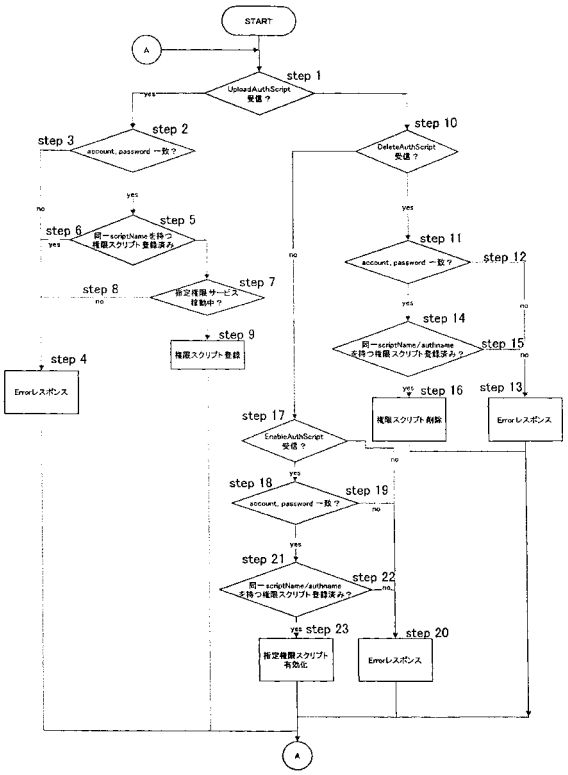
【図１】



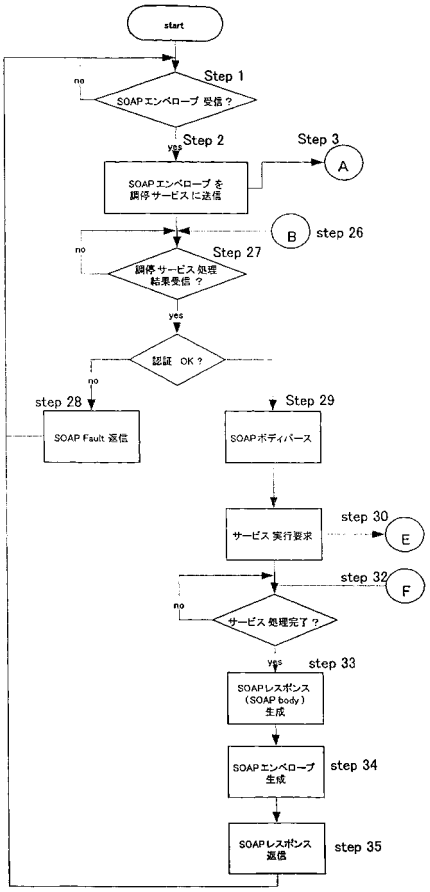
【図２】



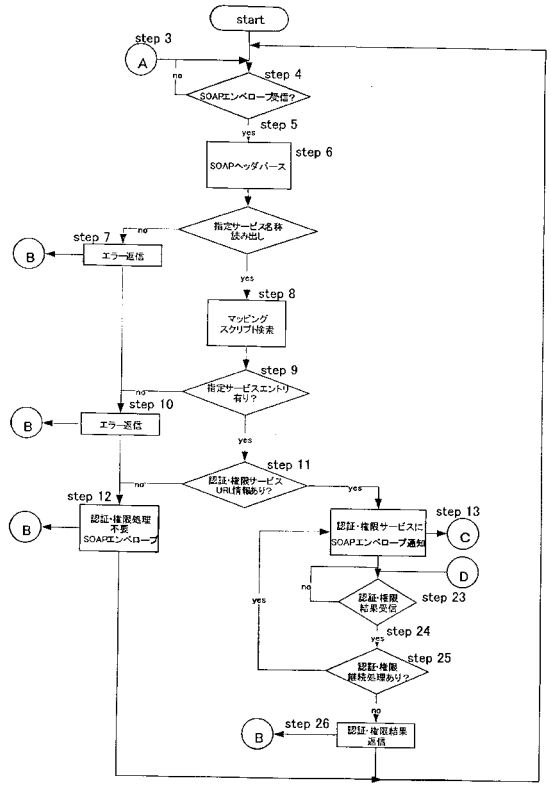
【図３】



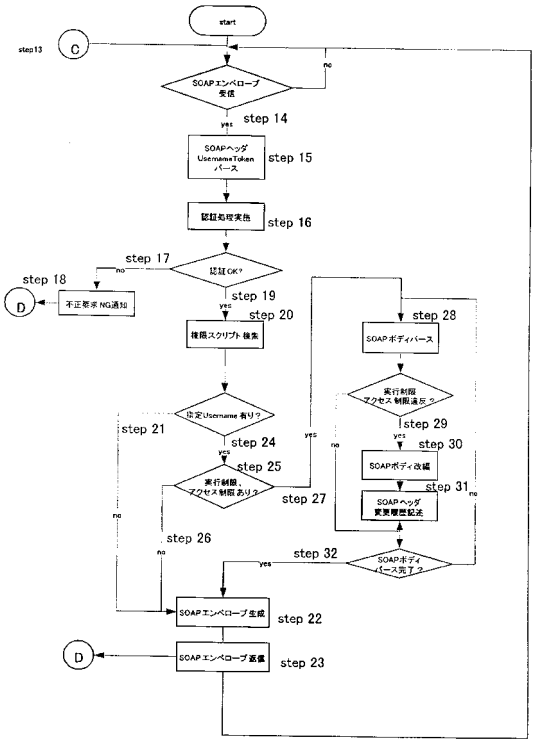
【図４－１】



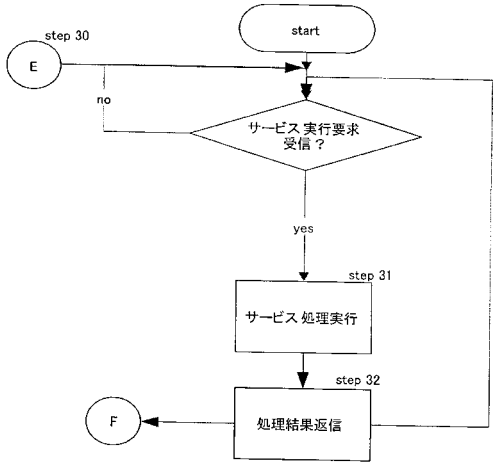
【図４－２】



【図４－３】



【図４－４】



【図５】

```
<Envelope>
<Header>
        <Action>http//abc.org/mfp/PrintService</Action>  51
        <MessageID> uuid0a6dc791-2be6-4991-9af1-454778a1917a</MessageID>
        <To> http//abc.org/mfp</To>
        <Security>
                <UsernameToken>  52
                        <Username>ABCDEF</Username>  53
                        <Password Type="...#PasswordDigest">
                        lEdZep5nTBtlerlisTo60wRbc==
                        </Password>
                        <Nonce>PsCAjo08nyQiaTlo== </Nonce>
                        <Created>2004-06-30T012345Z</Created>
                </UsernameToken>
        </Security>
</Header>

<Body>
        <CreateJob>
                <JobName>MyJob</JobName>  54
                <Color>FULLCOLOR</Color>  55
                <Copy>100</Copy>  56
                <Sides>ONESIDE</Sides>  57
                <MediaSize>A4</A4>  58
                <MediaType>PHOTOQUALITY</MediaType>  59
                <PrintQuality>HIGH</PrintQuality>  5A
        </CreateJob>
</Body>
</Envelope>
```

【図６】

```
<AccessControlScript>
        <scriptName>SCRIPTType1</scriptName>
        <authName>AUTHORIZATION B</authName>
        <RequestorInfo username="XXX">
                <Color>BLACKANDWHITE</Color>  61
                <Copy>10</Copy>  62
                <Sides>TWO-SIDE</Sides>  63
                <MediaSize>A4</A4>  64
                <MediaType>PLAINPAPAER</MediaType>  65
                <PrintQuality>HIGH</PrintQuality>  66
        </RequestorInfo>
        <RequestorInfo username="YYY">
                **************************
                **************************
                **************************
        </RequestorInfo>

        <RequestorInfo username="ZZZ">
                **************************
                **************************
                **************************
        </RequestorInfo>
</AccessControlScript>
```

【図７】

```
<Envelope>
<Header>
        <Action>http//abc.org/mfp/PrintService</Action>  51
        <MessageID> uuid0a6dc791-2be6-4991-9af1-454778a1917a</MessageID>
        <To> http//abc.org/mfp</To>
        <Assertion>
                <AuthenticationStatement
                        Decision="Permit"
                            Resource="http://abc.org/mfp/AuthorizationB>
                        <Subject>http://www.abc.org/PrintService</Subject>
                </AuthenticationStatement>
        </Assertion>
        <ModifiedRequest>  71
                <Color>FULLCOLOR</Color>
                <Copy>100</Copy>
                <Sides>ONESIDE</Sides>
                <MediaType>PHOTOQUALITY</MediaType>
        </ModifiedRequest>
</Header>

<Body>
        <CreateJob>
                <JobName>MyJob</JobName>  54
                <Color>BLACKANDWHITE</Color>  55
                <Copy>10</Copy>  56
                <Sides>TWO-SIDE</Sides>  57
                <MediaSize>A4</A4>  58
                <MediaType>PLAINPAPAER</MediaType>  59
                <PrintQuality>HIGH</PrintQuality>  5A
        </CreateJob>
</Body>
</Envelope>
```

【図８】

```
<?xml version="1.0" ?>
<xmlscript name="Sample1">
        <mapping>
                <Service>http://abc.org/mfp/PrintService</Service>
                <AuthService>http://abc.org/mfp/AuthenticationA</AuthService>
        </mapping>
        <mapping>
                <Service> http://abc.org/mfp/ScanService</Service>
                <AuthService> http://abc.org/mfp/AuthenticationB</AuthService>
        </mapping>
        <mapping>
                <Service> http://abc.org/mfp/StorageService</Service>
                <AuthService> http://abc.org/mfp/AuthorizationB</AuthService>
        </mapping>
        <mapping>
                <Service> http://abc.org/mfp/FaxService</Service>
                <AuthService> https://zzz.org/server/AuthenticationC</AuthService>
        </mapping>
</xmlscript>
```

【図９】

```
<?xml version="1.0" ?>
<xmlscript name="Sample2">
        <mapping>                                                    91
                <Service>http://abc.org/mfp/adhocPrinting/PrintService</Service>
                <AuthService>http://abc.org/mfp/AuthenticationA</AuthService>
        </mapping>
        <mapping>                                                    92
                <Service> http://abc.org/mfp/ChargedPrint/PrintService</Service>
                <AuthService> https://zzz.org/server/AuthenticationC</AuthService>
        </mapping>
</xmlscript>
```

【図１０】

```
<?xml version="1.0" ?>
<xmlscript name="Sample3">
        <mapping>
                <Service>http://abc.org/mfp/ScanService</Service>                    111
                <AuthService>http://abc.org/mfp/AuthenticationA</AuthService>
        </mapping>
        <mapping>
                <Service> http://abc.org/mfp/StorageService</Service>                112
                <AuthService> http://abc.org/mfp/AuthenticationB</AuthService>
        </mapping>
        <mapping>
                <Service> http://abc.org/mfp/ScanToStorage/ScanService</Service>     113
                <AuthService> http://zzz.org/server/AuthenticationC</AuthService>
        </mapping>
        <mapping>
                <Service> http://abc.org/mfp/ScanToStorage/StorageService</Service>  114
                <AuthService> https://zzz.org/server/AuthenticationC</AuthService>
        </mapping>
</xmlscript>
```

【図１１】

```
<?xml version="1.0" ?>
<xmlscript name="Sample4">
        <mapping>
                <Service>http://abc.org/mfp/PrintService</Service>                   121
                <AuthService>http://abc.org/mfp/AuthenticationA</AuthService>
        </mapping>
        <mapping>
                <Service> http://abc.org/mfp/ScanService</Service>                   122
                <AuthService> http://abc.org/mfp/AuthenticationA</AuthService>
        </mapping>
</xmlscript>
```

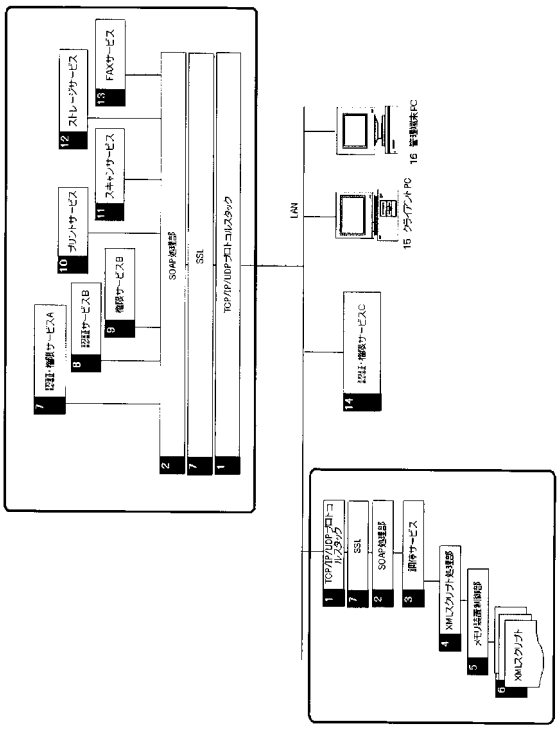
【図１２】

```
<?xml version="1.0" ?>
<xmlscript name="Sample5">
        <mapping>
                <Service>http://abc.org/mfp/PrintService</Service>
                <AuthService>http://abc.org/mfp/AuthenticationB</AuthService>
                <AuthService>http://abc.org/mfp/AuthorizationB</AuthService>
        </mapping>
</xmlscript>
```

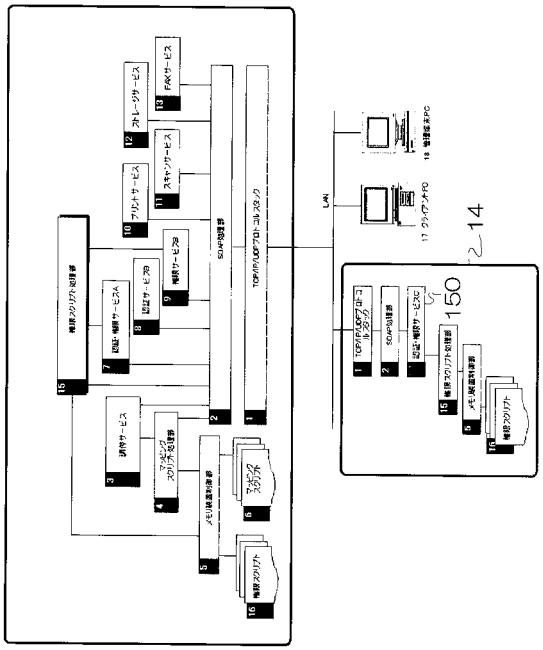
【図１３】

```
<?xml version="1.0" ?>
<xmlscript name="Sample6">
        <SecurityPolicy level="1">
                <mapping>
                    <Service>http://abc.org/mfp/PrintService</Service>
                    <AuthService></AuthService>
                </mapping>
        </SecurityPolicy>
        <SecurityPolicy level="2">
                <mapping>
                    <Service>http://abc.org/mfp/PrintService</Service>
                    <AuthService> http://abc.org/mfp/AuthenticationA</AuthService>
                </mapping>
        </SecurityPolicy>
        <SecurityPolicy level="3">
                <mapping>
                    <Service>http://abc.org/mfp/PrintService</Service>
                    <AuthService> http://abc.org/mfp/AuthenticationB</AuthService>
                </mapping>
        </SecurityPolicy>
        <SecurityPolicy level="4">
                <mapping>
                    <Service>http://abc.org/mfp/PrintService</Service>
                    <AuthService>https://zzz.org/server/AuthenticationC</AuthService>
                </mapping>
        </SecurityPolicy>
</xmlscript>
```

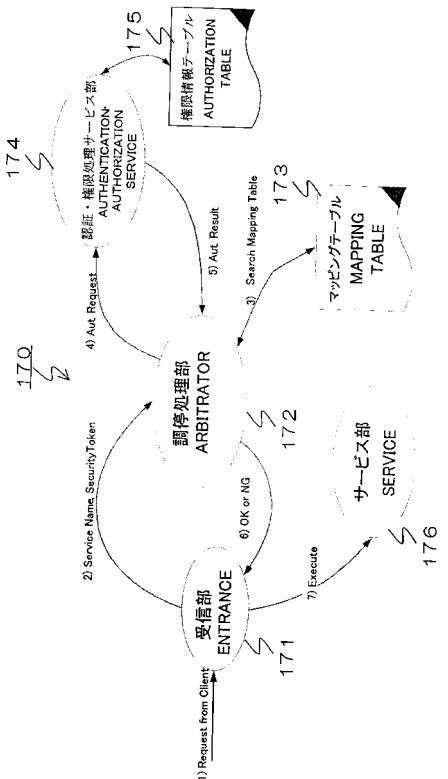
【図１４】



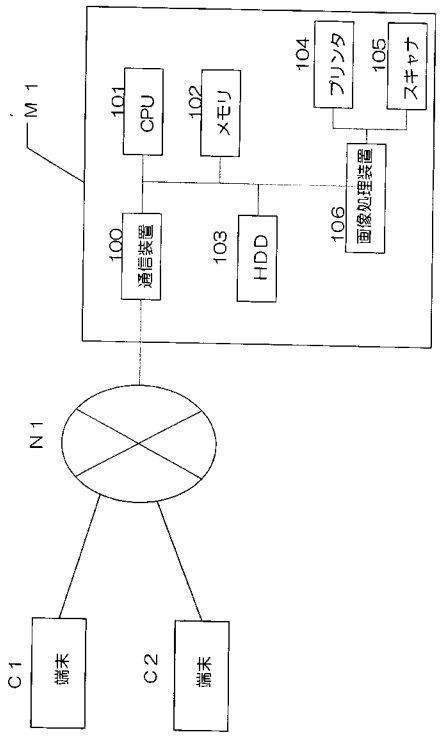
【図１５】



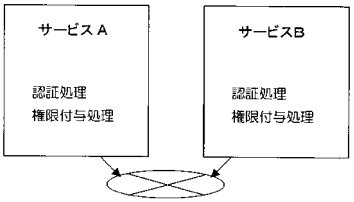
【図１６】



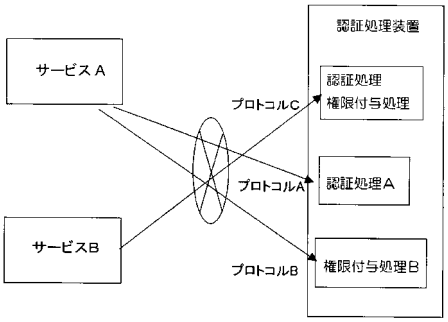
【図１７】



【図１８－１】



【図１８－２】



フロントページの続き

(56)参考文献 特開２００３－１６７８５４号公報
特開２００４－２１３６００号公報
特開２００４－１６６２４１号公報
特開２００４－１５２２６１号公報
特開２００３－００６１６２号公報
特開２００４－００５４０９号公報
末安泰三，「ねらわれるフリーＵＮＩＸ　第４部　一歩進んだ対策　段階的にセキュリティを強化，人材不足なら委託を考慮する」，日経インターネットテクノロジー，第１６号，第７６－８１頁，日経ＢＰ社，１９９８年１０月２２日

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F21/00
G09C1/00