(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-197385
(P2014-197385A)
(43)公開日　平成26年10月16日(2014.10.16)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/31	(2013.01)	G06F	21/20	131A	5B084
G06F 13/00	(2006.01)	G06F	13/00	510C	

審査請求 有　請求項の数 47　ＯＬ　外国語出願　（全 32 頁）

(21)出願番号　特願2014-23704(P2014-23704)
(22)出願日　平成26年2月10日(2014.2.10)
(31)優先権主張番号　13154974.3
(32)優先日　平成25年2月12日(2013.2.12)
(33)優先権主張国　欧州特許庁(EP)

特許法第６４条第２項第４号の規定により明細書の一部または全部を不掲載とする。
特許法第６４条第２項第４号の規定により図面の一部または全部を不掲載とする。

(71)出願人　599041075
キヤノン　オイローパ　エヌ．ヴェー．
オランダ国　アムステルヴェーン　１１８５　エックスビー，　ボフェンケルケンヴェグ　５９
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】周辺装置ユーザの認証方法、周辺装置、および周辺装置のユーザを認証するためのシステム

(57)【要約】　（修正有）
【課題】ユーザを周辺装置で認証するための方法を提供する。
【解決手段】周辺装置ＭＦＰが、ログイン要求をユーザから受信する工程S810と、ユーザのソーシャルネットワーキングサービスアカウントの認証要求をソーシャルネットワーキングサービスに送信する工程S820と、ユーザのソーシャルネットワーキングサービスアカウント情報をソーシャルネットワーキングサービスから受信する工程S830と、ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、ユーザが周辺装置へのアクセスを認可されているかどうかを判定する工程S840と、判定する工程がユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、ユーザが周辺装置へのアクセスを認可されていると判定した場合に、ユーザに周辺装置へのアクセスを許可する工程S850,S860とを有する。
【選択図】図８

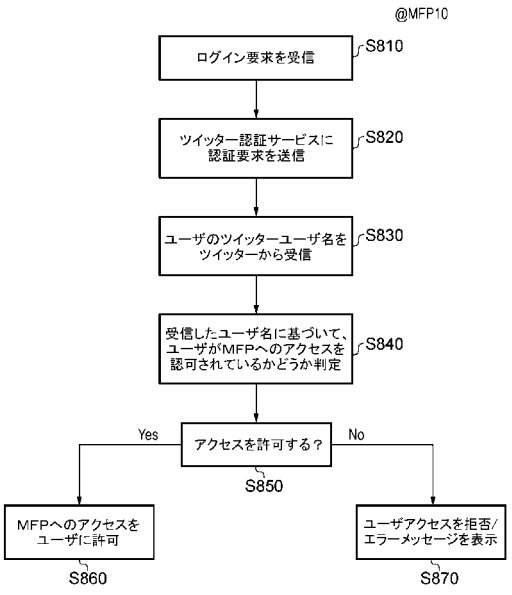

FIG. 8

【特許請求の範囲】
【請求項１】
周辺装置(10)でユーザを認証する方法であって、
前記周辺装置(10)が、
ログイン要求をユーザから受信する工程(S810)と、
ソーシャルネットワーキングサービスに前記ユーザのソーシャルネットワーキングサービスアカウントの認証要求を送信する工程(S820)と、
前記ユーザのソーシャルネットワーキングサービスアカウント情報を前記ソーシャルネットワーキングサービスから受信する工程(S830)と、
前記ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、前記ユーザが前記周辺装置へのアクセスを認可されているかどうかを判定する工程(S840)と、
を有し、
前記判定する工程が、前記ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、前記ユーザが前記周辺装置へのアクセスを認可されていると判定した場合、前記ユーザに前記周辺装置(10)へのアクセスを許可する(S850，S860)ことを特徴とする方法。
【請求項２】
前記判定する工程が、前記ユーザのソーシャルネットワーキングサービスアカウント情報が前記ソーシャルネットワーキングサービス上のリストと関連付けられているかどうかを判定するため、管理者のソーシャルネットワーキングサービスアカウントに接続する工程(S1116，S1117，S1409，S1410)を有することを特徴とする請求項１記載の方法。
【請求項３】
前記周辺装置(10)が、前記ソーシャルネットワーキングサービス上の前記ソーシャルネットワーキングサービスのメンバの１以上のリストと関連付けられて、前記ソーシャルネットワーキングサービス上で記述されることを特徴とする請求項２記載の方法。
【請求項４】
前記周辺装置(10)の前記ソーシャルネットワーキングサービス上での記述を、前記ソーシャルネットワーキングサービスのメンバの１以上のリストに関連付ける工程が、前記ソーシャルネットワーキングサービスのメンバの前記１以上のリストについて、前記周辺装置(10)の機能へのアクセスレベルを規定する工程を有することを特徴とする請求項３記載の方法。
【請求項５】
前記要求を前記ソーシャルネットワーキングサービスに送信する前記工程が、前記ソーシャルネットワーキングサービスにアクセストークンを要求する工程(S1111，S1112，S1407，S1408)を有することを特徴とする請求項１から請求項４のいずれか１項に記載の方法。
【請求項６】
前記判定する工程が、前記ユーザのソーシャルネットワーキングサービスユーザ名を取得するために前記アクセストークンを用いる工程と、前記ユーザ名が前記ソーシャルネットワーキングサービス上の前記周辺装置の記述に関連付けられているかどうかを判定する工程とを有することを特徴とする、請求項２から請求項４のいずれか１項を引用する請求項５に記載の方法。
【請求項７】
さらに、前記周辺装置(10)上に前記アクセストークンを前記ユーザを特定する情報に関連付けて保存する工程(S1113，S1406)を有することを特徴とする請求項５または請求項６に記載の方法。
【請求項８】
前記保存する工程が、前記アクセストークンを前記ユーザのＲＦＩＤと関連付けて保存する工程を有することを特徴とする請求項７記載の方法。
【請求項９】

前記保存されたアクセストークンは、繰り返されるログイン要求を前記ユーザに代わって行うために用いられることを特徴とする請求項７または請求項８に記載の方法。
【請求項１０】
前記ソーシャルネットワーキングサービスに前記アクセストークンを要求する前記工程は、OAuthまたはxAuth認証プロセスを用いる工程を有することを特徴とする請求項５から請求項９のいずれか１項に記載の方法。
【請求項１１】
前記周辺装置(10)は、プリンタ、ファクシミリ、またはスキャナの少なくとも１つとして機能する周辺機器を有することを特徴とする請求項１から請求項１０のいずれか１項に記載の方法。
【請求項１２】
前記ソーシャルネットワーキングサービスに前記要求を送信する前記工程に先行して、前記周辺装置(10)によって提供される第１の情報をモバイル機器(11)が決定する(S1905)工程を有することを特徴とする請求項１から請求項１１のいずれか１項に記載の方法。
【請求項１３】
前記第１の情報がＵＲＬであり、
前記周辺装置(10)が前記ＵＲＬを前記ユーザに提供し、
前記モバイル機器(11)が前記ユーザによって前記モバイル機器(11)に入力された前記ＵＲＬによって前記ＵＲＬを決定する、ことを特徴とする請求項１２記載の方法。
【請求項１４】
前記モバイル機器(11)によって受信された前記ＵＲＬが、前記ソーシャルネットワーキングサービスにユーザがログインすることを可能にすることを特徴とする請求項１３記載の方法。
【請求項１５】
前記モバイル機器(11)が受信した前記ＵＲＬは、ユーザが前記ソーシャルネットワーキングサービスにログインし(S1909)、前記周辺装置(10)へのアクセストークンの発行を認可することを可能にすることを特徴とする請求項１３記載の方法。
【請求項１６】
前記周辺装置(10)が、前記第１の情報を符号化した、装置が読み取り可能なコードを提供し、
前記モバイル機器(11)が、前記周辺装置(10)が提供する、前記装置が読み取り可能なコードを読んで復号することにより、前記第１の情報を決定する(S1905)ことを特徴とする請求項１２記載の方法。
【請求項１７】
前記ユーザを認証するために前記ソーシャルネットワーキングサービスに前記要求を送信する前記工程の後に、前記モバイル機器(11)が、前記ソーシャルネットワーキングサービスによって提供される第２の情報を判定する(S1910)工程を有することを特徴とする請求項１２から請求項１６に記載の方法。
【請求項１８】
前記第２の情報はコードであり、前記方法が、前記周辺装置(10)が前記コードを前記ユーザから、前記周辺装置(10)のユーザインタフェース(25)を通じて受信する工程(S1911)をさらに有することを特徴とする請求項１７記載の方法。
【請求項１９】
前記装置が読み取り可能なコードが、バーコードまたはＱＲコードであることを特徴とする、請求項１６、または請求項１６を引用する請求項１７または請求項１８に記載の方法。
【請求項２０】
周辺装置(10)で実行された際に、前記周辺装置(10)に請求項１から請求項１９のいずれか１項に記載の方法を実行させるプログラム。
【請求項２１】

モバイル機器(11)で実行された際に、前記モバイル機器(11)に請求項１２から請求項１９のいずれか１項に記載の方法を実行させるプログラム。
【請求項２２】
請求項２０または請求項２１に記載の前記プログラムを格納した記憶媒体。
【請求項２３】
周辺装置(10)であって、
ログイン要求をユーザから受信し、
ソーシャルネットワーキングサービスに前記ユーザのソーシャルネットワーキングサービスアカウントの認証要求を送信し、
前記ユーザのソーシャルネットワーキングサービスアカウント情報を前記ソーシャルネットワーキングサービスから受信し、
前記ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、前記ユーザが前記周辺装置へのアクセスを認可されているかどうかを判定し、
前記周辺装置(10)が、前記ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、前記ユーザが前記周辺装置(10)へのアクセスを認可されていると判定した場合、前記ユーザに前記周辺装置(10)へのアクセスを許可する、
ように構成されたことを特徴とする周辺装置(10)。
【請求項２４】
周辺装置(10)でユーザを認証する機能を有するモバイル機器(11)であって、
前記機能が、
識別情報を判定するために、装置が読み取り可能なコードを読み取って復号する手段と、
前記周辺装置(10)へのアクセストークンの発行を認可するために、前記判定された識別情報を用いてユーザがソーシャルネットワーキングサービスにログインすることを可能にする手段と、
を有することを特徴とするモバイル機器(11)。
【請求項２５】
周辺装置(10)のユーザを認証するためのシステムであって、
ログイン要求をユーザから受信し、ソーシャルネットワーキングサービスに前記ユーザのソーシャルネットワーキングサービスアカウントの認証要求を送信するように構成された周辺装置(10)と、
前記要求を受信し、前記ユーザのソーシャルネットワーキングサービスアカウント情報を前記周辺装置(10)に送信するように構成されたソーシャルネットワーキングサービスと、を有し
前記周辺装置(10)が、
前記ユーザのソーシャルネットワーキングサービスアカウント情報を前記ソーシャルネットワーキングサービスから受信し、
前記ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、前記ユーザが前記周辺装置へのアクセスを認可されているかどうかを判定し、
前記周辺装置(10)が、前記ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、前記ユーザが前記周辺装置(10)へのアクセスを認可されていると判定した場合、前記ユーザに前記周辺装置(10)へのアクセスを許可する、ように構成されたことを特徴とするシステム。
【請求項２６】
周辺装置(10)でユーザを認証するための方法であって、
モバイル機器(11)が、第１の識別情報を決定し(S2202)、ソーシャルネットワーキングサービスを通じて前記周辺装置(10)に、前記判定された第１の識別情報および前記ユーザのソーシャルネットワーキングサービスアカウントを特定する第２の識別情報を含む、アクセス要求を送信する(S2205)工程と、
前記周辺装置(10)が、前記アクセス要求を前記ソーシャルネットワーキングサービスを

通じて受信し、前記アクセス要求情報に基づいて、前記ユーザが前記周辺装置(10)へのアクセスを認可されているかどうか判定する工程(S2302)と、
前記周辺装置(10)が前記アクセス要求に基づいて、前記ユーザが前記周辺装置(10)へのアクセスを認可されていると判定した場合、前記周辺装置(10)が前記ユーザに前記周辺装置(10)へのアクセスを許可する工程(S2303)と、を有することを特徴とする方法。
【請求項２７】
前記周辺装置(10)によって判定する前記工程に先立って、前記周辺装置(10)が管理者のソーシャルネットワーキングサービスアカウントに接続し(S2103)、前記第１の識別情報を前記周辺装置(10)の記述と関連付けて前記ソーシャルネットワーキングサービスに登録する(S2104)工程をさらに有し、
前記周辺装置(10)によって判定する前記工程(S2302)が、前記管理者のソーシャルネットワーキングサービスアカウントに接続する工程と、前記アクセス要求にアクセスする工程と、前記アクセス要求内の情報が前記周辺装置(10)の登録された詳細と対応するかどうか判定する工程と、を有することを特徴とする請求項２６記載の方法。
【請求項２８】
前記アクセス要求は、前記ユーザのソーシャルネットワーキングサービスアカウントから前記管理者のソーシャルネットワーキングサービスアカウントに送信される直接メッセージであることを特徴とする請求項２７記載の方法。
【請求項２９】
前記周辺装置(10)は、前記ユーザのソーシャルネットワーキングサービスアカウントを特定する前記第２の情報に基づいて、前記周辺装置へのアクセスレベルを判定することを特徴とする請求項２６から請求項２８のいずれか１項に記載の方法。
【請求項３０】
前記第１の識別情報がコードを有し、
前記周辺装置(10)が前記コードを前記ユーザに提供し、
前記モバイル機器(11)は、前記モバイル機器(11)にユーザが入力した前記コードにより、前記第１の識別情報を決定する(S2202)ことを特徴とする、請求項２６から請求項２９のいずれか１項に記載の方法。
【請求項３１】
前記周辺装置(10)が、前記第１の識別情報を符号化した、装置が読み取り可能なコードを提供し、
前記モバイル機器(11)が、前記周辺装置(10)が提供する、前記装置が読み取り可能なコードを読んで復号することにより、前記第１の識別情報を決定する(S2202)ことを特徴とする、請求項２６から請求項２９のいずれか１項に記載の方法。
【請求項３２】
前記第１の識別情報が乱数を有することを特徴とする請求項２６から請求項３１のいずれか１項に記載の方法。
【請求項３３】
前記第１の識別情報は、管理者のソーシャルネットワーキングサービスアカウントを特定する情報を有することを特徴とする請求項２６から請求項３２のいずれか１項に記載の方法。
【請求項３４】
前記周辺装置(10)が前記第１の識別情報を生成するように構成されていることを特徴とする請求項２６から請求項３３のいずれか１項に記載の方法。
【請求項３５】
前記第１の識別情報が前記周辺装置の位置から導出可能であり、
前記モバイル機器(11)が、前記第１の識別情報を、前記周辺装置(10)の位置を検出することによって決定する(S2202)ことを特徴とする請求項２６から請求項２９のいずれか１項に記載の方法。
【請求項３６】

周辺装置(10)で実行された際に、前記周辺装置(10)に請求項２６から請求項３５のいずれか１項に記載の方法を実行させるプログラム。
【請求項３７】
モバイル機器(11)で実行された際に、前記モバイル機器(11)に請求項２６から請求項３５のいずれか１項に記載の方法を実行させるプログラム。
【請求項３８】
請求項３６または請求項３７に記載の前記プログラムを格納した記憶媒体。
【請求項３９】
周辺装置(10)でユーザを認証するためのシステムであって、
第１の識別情報を決定し(S2202)、ソーシャルネットワーキングサービスを通じて前記周辺装置(10)に、前記決定された第１の識別情報および前記ユーザのソーシャルネットワーキングサービスアカウントを特定する第２の識別情報を含む、アクセス要求を送信するように構成されたモバイル機器(11)と、
前記アクセス要求を受信し、前記アクセス要求情報に基づいて、前記ユーザが前記周辺装置(10)へのアクセスを認可されているかどうか判定するように構成された周辺装置(10)と、を有し、
前記周辺装置(10)は、前記周辺装置(10)が前記アクセス要求に基づいて前記ユーザが前記周辺装置(10)へのアクセスを認可されていると判定した場合、前記ユーザに前記周辺装置(10)へのアクセスを許可するように構成されていることを特徴とするシステム。
【請求項４０】
周辺装置(10)でユーザを認証する機能を有するモバイル機器(11)であって、前記機能が、
識別情報を決定するために、装置が読み取り可能なコードを読み取って復号する手段と、
ソーシャルネットワーキングサービスを通じて前記周辺装置(10)に、前記決定された第１の識別情報および前記ユーザのソーシャルネットワーキングサービスアカウントを特定する第２の識別情報を含む、アクセス要求を送信する手段と、を有することを特徴とするモバイル機器。
【請求項４１】
周辺装置(10)であって、
ユーザに、装置が読み取り可能なコードの形式で、第１の識別情報を提供するように構成された手段と、
ソーシャルネットワーキングサービスアカウントにアクセスし、前記第１の識別情報に基づいて、前記ユーザが前記周辺装置(10)へのアクセスを認可されているかどうかを判定するように構成された手段と、を有することを特徴とする周辺装置(10)。
【請求項４２】
前記第１の識別情報を提供するように構成された手段は、前記識別情報を前記周辺装置(10)のディスプレイに表示するか、前記識別情報を印刷するかの少なくとも一方によって前記識別情報をユーザに提供するように構成されていることを特徴とする請求項４１記載の周辺装置(10)。
【請求項４３】
前記識別情報が乱数を有することを特徴とする請求項４１または請求項４２に記載の周辺装置(10)。
【請求項４４】
前記識別情報は、管理者のソーシャルネットワーキングサービスアカウントを特定する情報を有することを特徴とする請求項４１から請求項４３のいずれか１項に記載の周辺装置(10)。
【請求項４５】
前記識別情報を生成する手段をさらに有することを特徴とする請求項４１から請求項４４のいずれか１項に記載の周辺装置(10)。

【請求項４６】
前記周辺装置(10)は前記識別情報をバーコードまたはＱＲコードの形式で提供するように構成されていることを特徴とする請求項４５記載の周辺装置(10)。
【請求項４７】
プリンタ、ファクシミリ、またはスキャナの少なくとも１つとして機能する周辺機器を有することを特徴とする請求項２３、請求項２５、請求項３９、請求項４１から請求項４６のいずれか１項に記載の周辺装置(10)。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は認証方法、認証装置、および認証システムに関する。特に、本発明は周辺装置でユーザを認証するための方法、周辺装置のユーザを認証するための周辺装置、および周辺装置のユーザを認証するためのシステムに関する。
【背景技術】
【０００２】
OAuthは、アプリケーションが、ユーザのクレデンシャル、例えばパスワードを共有することなくユーザに代わって振る舞うことを、ユーザが承認できるようにする認証プロトコルである。従前のクライアント－サーバ認証モデルでは、クライアントは自身のクレデンシャルを用いて、サーバが提供するリソースにアクセスする。OAuthは、リソースオーナという第３の役割をこのモデルに導入する。OAuthモデルにおいて、クライアント（リソースオーナではないが、その代理として振る舞う）はリソースオーナによってコントロールされているが提供はサーバが行うリソースに、アクセスを要求する。
【０００３】
クライアントがリソースにアクセスするためには、クライアントはまずリソースオーナから承認(permission)を得なければならない。この承認は、トークンおよび共有鍵(matching shared-secret)の形式で記述される。トークンの目的は、リソースオーナが自身のクレデンシャルをクライアントと共有する必要性をなくすことである。リソースオーナクレデンシャルとは異なり、トークンは権限および有効期限を制限して発行が可能であり、また、独立して無効化できる。OAuthに関する他の情報については、http://oauth.net/を参照されたい。
【０００４】
ソーシャルネットワーキングサービスは、興味および／または行動を共有する人々のソーシャルネットワークやソーシャルリレーションの構築および反映にフォーカスしたオンラインサービス、プラットフォーム、あるいはサイトであり、同じ、または似た興味、背景および／または行動を持つ人々がコミュニティを作る。ソーシャルネットワーキングサービスは各ユーザの記述（多くはプロファイル）、ユーザのソーシャルリンク、および様々な付加サービスからなる。ほとんどのソーシャルネットワーキングサービスはウェブベースであり、電子メールやインスタントメッセージングのような、ユーザがインターネット上で相互にやりとりするための手段を提供する。ソーシャルネットワーキングサイトは、ユーザがアイデア、行動、イベント、および興味を個々のネットワーク内で共有することを可能にする。
【０００５】
ソーシャルネットワーキングサービスの主なタイプは、カテゴリプレイス（以前の学年や同級生など）、友人を関連付けるための手段（通常は自己紹介ページを有する）、および信用度に関連する推奨システムを有するものである。人気のある方法はこれらの多くを組み合わせたものであり、フェイスブック（登録商標）、Google+（登録商標）、およびツイッター（登録商標）は世界中で広く使われている。ツイッターは、「ツイート」と呼ばれる１４０文字までのテキストベースのポストをユーザが送信したり読んだりすることを可能にする、オンラインソーシャルネットワーキングサービスかつマイクロブロギングサービスである。未登録ユーザはツイートを読むことができ、登録ユーザはウェブサイト

インターフェース、ＳＭＳ、またはモバイル機器用の様々なアプリケーションを通じてツイートをポストすることができる。

【０００６】

大規模なＭＦＰ設置の際、マイクロソフト（登録商標）社によるディレクトリサービスであるアクティブディレクトリをログオンユーザの制御のためにインストールすることができる。しかし、小規模な設置では、アクティブディレクトリのインストールは高価で不便である。従って、小規模なＭＰＦ群の設定に適した、代替的なログオンの仕組みの提供が望まれている。

【発明の概要】

【０００７】

本発明の一目的は、周辺装置に専用の認証リソースを必要とせずに、周辺装置でユーザを認証することを可能にする周辺装置および周辺装置の方法の提供にある。換言すれば、本発明の一目的は、周辺装置でユーザを認証するための、簡潔かつ低コストな仕組みを提供することにある。

【０００８】

本発明の第１の見地によれば、周辺装置でユーザを認証する方法であって、ログイン要求をユーザから受信する工程と、ソーシャルネットワーキングサービスにユーザのソーシャルネットワーキングサービスアカウントの認証要求を送信する工程と、ユーザのソーシャルネットワーキングサービスアカウント情報をソーシャルネットワーキングサービスから受信する工程と、ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、ユーザが周辺装置へのアクセスを認可されているかどうかを判定する工程と、判定する工程において、ユーザのソーシャルネットワーキングサービスアカウント情報に基づいてユーザが周辺装置へのアクセスを認可されていると判定された場合、ユーザが周辺装置にアクセスすることを許可する工程と、を周辺装置が実行する方法が提供される。

【０００９】

一部の実施形態において、判定する工程は、ユーザのソーシャルネットワーキングサービスアカウント情報がソーシャルネットワーキングサービス上の周辺装置の記述と関連付けられているかどうかを判定するため、管理者のソーシャルネットワーキングサービスアカウントに接続する工程を有する。

【００１０】

一部の実施形態において、ソーシャルネットワーキングサービス上の周辺装置の記述は、ソーシャルネットワーキングサービス上のソーシャルネットワーキングサービスのメンバのリストに関連付けられ、および／またはソーシャルネットワーキングサービス上の周辺装置の記述はソーシャルネットワーキングサービス上のソーシャルネットワーキングサービスのメンバのリストグループに関連付けられる。

【００１１】

一部の実施形態において、ソーシャルネットワーキングサービス上の周辺装置の記述をソーシャルネットワーキングサービスのメンバのリストに関連付ける工程は、ソーシャルネットワーキングサービスのメンバのリストに対し、周辺装置の機能へのアクセスレベルを規定する工程を有し、ソーシャルネットワーキングサービス上の周辺装置の記述をソーシャルネットワーキングサービスのメンバのリストグループに関連付ける工程は、ソーシャルネットワーキングサービスのメンバのリストグループに対し、周辺装置の機能へのアクセスレベルを規定する工程を有する。

【００１２】

一部の実施形態において、ソーシャルネットワーキングサービスに要求を送信する工程は、ソーシャルネットワーキングサービスにアクセストークンを要求する工程を有する。一部の実施形態において、判定する工程は、ユーザのソーシャルネットワーキングサービスユーザ名を取得するためにアクセストークンを用いる工程と、ユーザ名がソーシャルネットワーキングサービス上の周辺装置の記述に関連付けられているかどうかを判定する工程とを有する。一部の実施形態において、方法はさらに、ユーザを特定する情報と関連付

けてアクセストークンを周辺装置に保存する工程を有する。一部の実施形態において、保存する工程は、アクセストークンをユーザのＲＦＩＤに関連付ける工程を有する。好ましくは、保存されたアクセストークンは、繰り返されるログイン要求をユーザに代わって行うためのものである。

【００１３】

一部の実施形態において、ソーシャルネットワーキングサービスにアクセストークンを要求する工程は、OAuthまたはxAuth認証プロセスを用いる工程を有する。

【００１４】

一部の実施形態において、ソーシャルネットワーキングサービスに要求を送信する工程に先行して、周辺装置によって提供される第１の情報をモバイル機器が決定する。

【００１５】

一部の実施形態において、第１の情報はＵＲＬであり、周辺装置はＵＲＬをユーザに提供し、モバイル機器は、ユーザがモバイル機器に入力したＵＲＬによってＵＲＬを決定する。一部の実施形態において、モバイル機器が受信したＵＲＬはユーザがソーシャルネットワーキングサービスにログインすることを可能にする。一部の実施形態において、モバイル機器が受信したＵＲＬはユーザがソーシャルネットワーキングサービスにログインし、周辺装置へのアクセストークンの発行を認可することを可能にする。

【００１６】

別の実施形態において、周辺装置は第１の情報を符号化する、装置が読み取り可能なコードを提供し、モバイル機器は周辺装置によって提供される、装置が読み取り可能なコードを読み取って復号することによって第１の情報を決定する。

【００１７】

一部の実施形態において、ユーザを認証するためにソーシャルネットワーキングサービスに要求を送信する工程の後に、モバイル機器は、ソーシャルネットワーキングサービスによって提供される第２の情報を決定する。一部の実施形態において、第２の情報はコードであり、方法は、周辺装置が周辺装置のユーザインタフェースを通じてユーザからコードを受信する工程を有する。一部の実施形態において、コードは番号である。

【００１８】

別の実施形態において、装置が読み取り可能なコードは、識別情報を符号化している、バーコードや装置が読み取り可能な他のコードであり、モバイル機器は周辺装置が提供するバーコードまたは装置が読み取り可能な他のコードを読み取って復号することによって識別情報を決定するように構成される。

【００１９】

本発明の別の見地によれば、周辺装置であって、ログイン要求をユーザから受信し、ソーシャルネットワーキングサービスにユーザのソーシャルネットワーキングサービスアカウントの認証要求を送信し、ユーザのソーシャルネットワーキングサービスアカウント情報をソーシャルネットワーキングサービスから受信し、ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、ユーザが周辺装置へのアクセスを認可されているかどうかを判定し、ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、周辺装置が、ユーザが周辺装置へのアクセスを認可されていると判定した場合、ユーザが周辺装置にアクセスすることを許可する、ように構成された周辺装置が提供される。

【００２０】

一部の実施形態において、周辺装置は、プリンタ、ファクシミリ、またはスキャナの少なくとも１つとして機能する周辺機器からなる。

【００２１】

本発明のさらに別の見地によれば、周辺装置でユーザを認証するための機能を有するモバイル機器であって、機能は、識別情報を決定するために装置が読み取り可能なコードを読み取って復号するための手段と、周辺装置へのアクセストークンの発行を認可するためにユーザがソーシャルネットワーキングサービスにログインできるよう、決定された識別

情報を用いる手段とを含む、モバイル機器が提供される。
【００２２】
一部の実施形態において、モバイル機器は携帯電話機、ＰＤＡ、デジタルカメラ、ラップトップコンピュータ、または他のモバイル機器である。
【００２３】
本発明の別の見地によれば、周辺装置のユーザを認証するためのシステムであって、ログイン要求をユーザから受信し、ソーシャルネットワーキングサービスにユーザのソーシャルネットワーキングサービスアカウントの認証要求を送信するように構成された周辺装置と、要求を受信し、ユーザのソーシャルネットワーキングサービスアカウント情報を周辺機器に送信するように構成されたソーシャルネットワーキングサービスとを有し、周辺装置は、ユーザのソーシャルネットワーキングサービスアカウント情報をソーシャルネットワーキングサービスから受信し、ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、ユーザが周辺装置へのアクセスを認可されているかどうかを判定し、ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、周辺装置が、ユーザが周辺装置へのアクセスを認可されていると判定した場合、ユーザが周辺装置にアクセスすることを許可する、ように構成されるシステムが提供される。
【００２４】
本発明の別の見地によれば、周辺装置でユーザを認証する方法であって、モバイル機器が第１の識別情報を決定し、ソーシャルネットワーキングサービスを通じて周辺装置に、決定された第１の識別情報とユーザのソーシャルネットワーキングサービスアカウントを特定する第２の情報とを有するアクセス要求を送信する工程と、周辺装置がソーシャルネットワーキングサービスを通じてアクセス要求を受信し、ユーザが周辺装置にアクセスすることを認可するかどうかをアクセス要求情報に基づいて判定する工程と、周辺装置がアクセス要求情報に基づいて、ユーザが周辺装置へのアクセスを認可されていると判定した場合に、周辺装置がユーザに周辺装置へのアクセスを許可する工程と、を有する方法が提供される。
【００２５】
一部の実施形態において、周辺装置による判定工程に先立って、周辺装置は管理者のソーシャルネットワーキングサービスアカウントに接続し、ソーシャルネットワーキングサービス上の周辺機器の記述と関連付けて第１の識別情報を登録し、周辺機器による判定工程が、管理者のソーシャルネットワーキングサービスアカウントに接続する工程と、アクセス要求にアクセスする工程と、アクセス要求内の情報が周辺装置の登録された詳細と対応するかどうかを判定する工程と、を有する。
【００２６】
一部の実施形態において、アクセス要求は、ユーザのソーシャルネットワーキングサービスアカウントから管理者のソーシャルネットワーキングサービスアカウントに送信される直接（プライベート）メッセージである。
【００２７】
一部の実施形態において、周辺装置はユーザのソーシャルネットワーキングサービスアカウントを特定する第２の情報に基づいて、周辺装置へのアクセスレベルを決定する。
【００２８】
一部の実施形態において、第１の識別情報はコードを含み、周辺装置はコードをユーザに提供し、モバイル機器はユーザによってモバイル機器へ入力されたコードによって第１の識別情報を決定する。
【００２９】
別の実施形態において、周辺機器は第１の識別情報を符号化した、装置が読み取り可能なコードを提供し、モバイル機器は周辺機器によって提供される装置が読み取り可能なコードを読み取って復号することによって第１の識別情報を決定する。
【００３０】
一部の実施形態において、第１の識別情報は乱数を有する。

【００３１】
一部の実施形態において、第１の識別情報は管理者のソーシャルネットワーキングサービスアカウントを特定する情報（例えばユーザ名）を有する。
【００３２】
一部の実施形態において、周辺装置は第１の識別情報を生成するように構成される。
【００３３】
一部の実施形態において、第１の識別情報は周辺装置の位置から導出することができ、モバイル機器は周辺装置の位置を検出することによって第１の識別情報を決定する。好ましくは、周辺装置の位置はモバイル機器の位置検出手段を用いて測定される。一部の実施形態において、位置検出手段は地球測位センサである。好ましくは第１の識別情報は周辺装置の位置座標の所定桁数である。
【００３４】
本発明の別の見地によれば、周辺装置でユーザを認証するシステムであって、第１の識別情報を決定し、ソーシャルネットワーキングサービスを通じて周辺装置に、決定された第１の識別情報とユーザのソーシャルネットワーキングサービスアカウントを特定する第２の情報とを有するアクセス要求を送信するように構成されたモバイル機器と、ソーシャルネットワーキングサービスを通じてアクセス要求を受信し、ユーザが周辺装置にアクセスすることを認可するかどうかをアクセス要求情報に基づいて判定するように構成された周辺装置とを有し、周辺装置は、アクセス要求情報に基づいて、ユーザが周辺装置へのアクセスを認可されると判定した場合に、ユーザに周辺装置へのアクセスを許可するように構成されるシステムが提供される。
【００３５】
本発明の別の見地によれば、周辺装置でユーザを認証するための機能を有するモバイル機器であって、機能は、第１の識別情報を決定するために装置が読み取り可能なコードを読み取って復号するための手段と、ソーシャルネットワーキングサービスを通じて周辺装置に、決定された第１の識別情報とユーザのソーシャルネットワーキングサービスアカウントを特定する第２の情報とを有するアクセス要求を送信する手段とを含む、モバイル機器が提供される。
【００３６】
本発明の別の見地によれば、周辺装置であって、ユーザに第１の識別情報を装置が読み取り可能なコード手段の形式で提供するように構成された手段と、ソーシャルネットワーキングサービスアカウントにアクセスし、ユーザが周辺装置へのアクセスを認可されているかどうかを第１の識別情報に基づいて判定するように構成された手段とを有する周辺装置が提供される。
【００３７】
一部の実施形態において、第１の識別情報を提供するように構成された手段は、識別情報を周辺装置のディスプレイに表示するか、識別情報を印刷するかの少なくとも一方によって識別情報をユーザに提供するように構成される。
【００３８】
一部の実施形態において、識別情報は乱数を有する。
【００３９】
一部の実施形態において、識別情報は管理者のソーシャルネットワーキングサービスアカウントを特定する情報を有する。
【００４０】
一部の実施形態において、周辺装置は識別情報を生成する手段を有する。
【００４１】
一部の実施形態において、周辺装置は識別情報をバーコードまたはＱＲコード（登録商標）の形式で提供するように構成される。
【００４２】
本発明の別の見地によれば、周辺装置が実行する、周辺装置に関する情報を通信する方

法であって、周辺装置を表すソーシャルネットワーキングサービスアカウントに接続する工程と、周辺装置に関する情報をソーシャルネットワーキングサービスの１以上のユーザに送信する工程とを有する方法が提供される。

【００４３】

一部の実施形態において、周辺装置によって送信される情報は、周辺装置の状態に関する情報、周辺装置の利用に関する情報、周辺装置の位置に関する情報、周辺装置のユーザを特定する情報、周辺装置に関する全体的もしくは個別のユーザ活動に関する情報、周辺装置を用いて行われたユーザ動作に関する情報、ユーザが周辺装置を使用したことに対する費用を詳述する情報、ユーザ動作を処理するために周辺装置が用いた材料を詳述する情報、周辺装置の修理に関する情報の１つ以上に関する情報である。

【００４４】

本発明の別の見地によれば、周辺装置に関する情報を通信するための周辺装置であって、周辺装置を表すソーシャルネットワーキングサービスアカウントに接続するための手段と、周辺装置に関する情報をソーシャルネットワーキングサービスの１以上のユーザに送信するための手段とを有する周辺装置が提供される。

【００４５】

一部の実施形態において、周辺装置は、プリンタ、ファクシミリ、またはスキャナの少なくとも１つとして機能する周辺機器からなる。

【００４６】

一部の実施形態において、モバイル機器は携帯電話機、ＰＤＡ、デジタルカメラ、ラップトップコンピュータ、または他のモバイル機器である。

【図面の簡単な説明】

【００４７】

【図１】第１の実施形態の構成を示す図
【図２】ＭＦＰのハードウェアを示す図
【図３】管理者のツイッターアカウントを示す図
【図４】ツイッター内のＭＦＰリストを示す図
【図５】ツイッター内のＭＦＰリストの生成を示す図
【図６】ＭＦＰリストに追加するツイッターユーザの選択を示す図
【図７】図５で生成されたＭＦＰリストへのツイッターユーザの追加を示す図
【図８】ＭＦＰにおける汎用ログイン手順の工程を示す図
【図９】ＭＦＰの表示を示す図
【図１０】ＭＦＰの別の表示を示す図
【図１１】第１の実施形態に係るＭＦＰで実行される工程を示す図
【図１２】ＭＦＰの別の表示を示す図
【図１３】ＭＦＰの別の表示を示す図
【図１４】第２の実施形態に係るＭＦＰで実行される工程を示す図
【図１５】第３の実施形態の構成を示す図
【図１６】携帯電話機のハードウェアを示す図
【図１７】ＭＦＰの別の表示を示す図
【図１８】携帯電話機の表示を示す図
【図１９】第３の実施形態に従って実行される工程を示す図
【図２０Ａ】ユーザＲＦＩＤをアクセストークンと関連付けて保存するための登録リストを示す図
【図２０Ｂ】は第４の実施形態に係るＭＦＰで実行される工程を示す図
【図２１】第４の実施形態に係るＭＦＰで実行される工程を示す図
【図２２】第５の実施形態に係る携帯電話機で実行される工程を示す図
【図２３】第５の実施形態に係るＭＦＰで実行される工程を示す図
【図２４】第６の実施形態に係るＭＦＰで実行される工程を示す図

【発明を実施するための形態】

【００４８】
以下、単なる例示として、添付図面を参照して本発明の実施形態を説明する。
●第１の実施形態
図１は第１の実施形態の画像処理システムのアーキテクチャを示している。画像処理システムはＭＦＰ（多機能周辺装置）１０および認証サーバ１２を有している。ＭＦＰ１０は認証サーバ１２によって提供されるツイッターＡＰＩにアクセスするために、ＷｉＦｉネットワーク１４のようなローカルエリアネットワークを介してインターネットに接続可能である。
【００４９】
図２はＭＦＰ１０のハードウェア構成を示している。ＭＦＰはＣＰＵ２０、ＲＯＭ２１、ハードディスクドライブ２２、およびＲＡＭ２３を有している。これらの部品はコンピュータや他の機器に関して一般的なハードウェア部品であり、通常の機能を実行する。ＭＦＰ１０はさらに、表示部２４、操作部２５、通信制御部２６、画像リーダ２７、記録部２８、画像メモリ２９、画像処理部２１０、認証部２１１、カードリーダ２１２、およびＩ／Ｏ制御部２１３を有する。表示部２４はＭＦＰ１０に設けられたタッチスクリーンＬＣＤディスプレイであり、ユーザがＭＦＰ１０の情報を選択したり見たりすることを可能にする。操作部２５はユーザが認証クレデンシャル、設定および他の情報をＭＦＰ１０に入力することを可能にするキーパッドおよび他のボタン群である。通信制御部２６は、ＭＦＰ１０がＬＡＮを通じてウェブサーバ１２と通信することを可能にする。画像リーダ２７はドキュメントのスキャンを可能にするスキャナである。図２に示す記録部２８は、ＭＦＰ１０の印刷専用部分を示している。記録部２８は、画像データを記録媒体に印刷し、記録媒体をユーザによる回収のために出力するように機能する。画像メモリ２９は、画像リーダ２７によるスキャンや記録部２８による印刷の間、画像データを保存するために設けられているメモリである。画像処理部２１０は、スキャンされたＲＧＢデータのＣＭＹＫデータへの変換など、複写動作の間の所定の画像処理のスピードを向上させるためにＭＦＰ１０に設けられている様々な特定用途向け集積回路(ASIC)を表している。認証処理部２１１はカードリーダ２１２から受信したユーザ詳細を認証するために設けられている。カードリーダ２１２からのデータは、Ｉ／Ｏ制御部２１３を通じて認証部２１１で受信される。認証部は別個のハードウェアとしてではなく、ＣＰＵ２０およびＲＡＭ２３を用いて稼動するソフトウェアによって実現されてもよい。上述した構成要素はバス２１４を通じて相互接続されている。
【００５０】
ＭＦＰ１０はオペレーティングシステムを実行する。この特定の実施形態において、オペレーティングシステムは、キヤノン（登録商標）社が販売するＭＦＰで提供されているランタイム環境であるＭＥＡＰ（多機能組み込みアプリケーションプラットフォーム）アプリケーション（ログインアプリケーション）を実行する。オペレーティングシステムはJAVA（登録商標）アプリケーションの稼働を許し、さらに後述するようにウェブインタフェースを含んでもよい。これらのアプリケーションは周辺機器の動作を制御することが可能であり、情報の表示が可能であり、また操作部２５および接触感知式表示部２４を通じてユーザからの入力命令を受信することができる。
【００５１】
画像処理システムの動作について、図３から図７を参照して説明する。以下でより詳細に説明するように、本発明の実施形態では、管理者が、ＭＦＰ１０のような周辺機器へのアクセスを管理するために、サービスプロバイダ（例えばツイッターのような、特定のソーシャルネットワーキングサービス）を用いる。
【００５２】
サービスプロバイダでのリスト設定
例えば、管理者は、所定の登録ツイッターユーザによる特定のＭＦＰへのアクセスを制御するためのＭＦＰリストをツイッター内に生成するために管理者ツイッターアカウントを用いる。各ＭＦＰはツイッターリストによって表すことができる。例えば、ＭＦＰ１０

にアクセス可能なユーザは、ＭＦＰ１０を表すツイッターリストに含まれるであろう。あるいは、個々のＭＦＰへのアクセスをより柔軟に制御できるようにするため、管理者は（アクティブディレクトリ(AD)で管理者が行うような）論理グループ、例えばツイッター内に生成することができるグループ内のユーザリストを作成できるかもしれない。上述した制御手法は、グループ（またはツイッターリスト）に対するパーミッションをＭＦＰ１０で局所的に維持することによって実現されてもよい。すなわち、ＭＰＦ１０（ＭＥＡＰアプリケーション）は、管理者により、特定のグループをチェックするように構成されてよい。どのグループのチェックが必要かに関する情報は管理者ツイッターアカウントに保存される必要はないが、代わりにＭＦＰ１０にローカル保存することができる。そしてアクセス管理システム（ＡＭＳ）は、異なるユーザグループに対し、個々のＭＦＰの個々の機能への異なるアクセス種類／レベルを与えるために用いることができる。例えば、グループ１はコピーとファックスが可能であるが、グループ２はコピーのみ可能とする。

【００５３】

管理者はＭＦＰ１０に関するツイッターリストに対してユーザを追加／除去することにより、ＭＰＦ１０へのユーザアクセスを許可／拒否することができる。

【００５４】

管理者（例えばツイッターユーザＩＤ@BenTesting 2を有する）が管理者ツイッターアカウントにログインすると、図３に示すホームページが表示される。プリンタリストを生成するため、管理者は「リスト」をプロファイルメニュー（最上段左）から選択すると、図４に示すページが表示されるようになる。図４に示すように、１つのプリンタリスト（（公序良俗違反につき、不掲載））が既に作成されている。図５に示すように、新規リストを生成するため、管理者は「リスト生成」をクリックし、プリンタの名称(（公序良俗違反につき、不掲載））と説明（例えば、「向こうの窓際の隅(over in the corner by the window)」）を入力し、「リストを保存」をクリックする。図６および図７に示すように、新規ユーザをツイッターで検索して特定のプリンタリストに追加することもできる。図６は、ユーザアカウント名の隣の「リストに対する追加または削除」を選択することにより、RobertTestingにプリンタへのアクセス権を与えている状態を示している。図７は、ユーザにどのプリンタへのアクセスを許可するかの選択を示している。図７に示す特定の例において、ユーザは（公序良俗違反につき、不掲載）へのアクセスを許可されている。

【００５５】

汎用ログイン手順

図８を参照すると、ＭＦＰ１０でユーザはログイン画面を通じて自身のログイン詳細を入力する（図８、Ｓ８１０）。以下でより詳細に説明するように、第１の実施形態では、ユーザが自身のユーザ名およびパスワードを秘密に保ち、それらをＭＥＡＰアプリケーションや他のサイトと共有しないようにすることを可能にするため、サービスプロバイダのサーバに直接アクセスするためにウェブブラウザが用いられる。これに対し後述する第２の実施形態では、ユーザはＭＥＡＰアプリケーションに自身のクレデンシャルを直接入力し、ＭＥＡＰアプリケーションがこれらクレデンシャルをサービスプロバイダに渡す。図８のステップＳ８２０において、ＭＥＡＰアプリケーションはサービスプロバイダにアクセストークンを要求する。図８のステップＳ８３０において、ＭＥＡＰアプリケーションはサービスプロバイダからアクセストークンを受信する。図８のステップＳ８４０において、（図３から図７に関して上述したように）管理者によってサービスプロバイダ（例えばツイッター）に規定された、ＭＦＰ１０に対するＭＦＰリストがアクセスされ、ユーザのサービスプロバイダＩＤ（ツイッターＩＤ／ユーザ名）が、ユーザがアクセスを希望するＭＦＰ１０を表すＭＦＰリストに存在するか否かが判定される（ステップＳ８５０）。ユーザのツイッターＩＤがリスト上に存在する場合、ユーザはそのＭＦＰへのアクセスを許可される（図８、Ｓ８６０）。ユーザのツイッターＩＤがリスト上に存在しない場合、ＭＦＰ１０にエラーメッセージが表示されてよい（図８、Ｓ８７０）。

【００５６】

詳細なログイン手順

図９から図１１に関し、説明を目的として、ユーザがＭＦＰ１０へ歩いて行き、ＭＦＰ１０にアクセスしたいという状況を仮定する。ユーザはＭＦＰ１０の表示部２４を見ると、図９に対応する表示が見える。ユーザは、「ツイッターを用いてサインイン」アイコン６０を選択するため、表示部２４のタッチ画面を用いる。タッチ画面上でアイコン６０がタッチされると、ログインアプリケーションであるＭＥＡＰアプリケーションは、ログイン画面を表示するために状態を変更する（図１１のステップＳ１１０１）。

【００５７】

ＭＥＡＰアプリケーションは、１つ以上のソーシャルネットワーキングサービス（例えばツイッター）を用いてログインすることができるように構成される。そのようにするため、ＭＥＡＰアプリケーションはツイッターのOAuth対応ＡＰＩとともに用いるためのクライアントクレデンシャル群（クライアントＩＤおよびシークレット）を、事前にツイッターから取得している。

【００５８】

図１１のステップＳ１１０２で、ＭＥＡＰアプリケーションはそのユーザに対して保存されているOAuthアクセストークンをＭＥＡＰアプリケーションが有しているか否かを判定する。ＭＥＡＰアプリケーションがアクセストークンを有していれば、ＭＥＡＰアプリケーションはステップＳ１１０４に進む。ＭＥＡＰアプリケーションがアクセストークンを有していなければ、ＭＥＡＰアプリケーションはステップＳ１１０３に進む。

【００５９】

図１１のステップＳ１１０３でＭＥＡＰアプリケーションは、未認可要求トークンをツイッターのOAuth認証サービスから取得するために、署名された要求を送信する。この時点で、未認可要求トークンはリソースオーナー固有のものではなく、ユーザのツイッターアカウントにアクセスするためのリソースオーナー認可をユーザから得るためにＭＥＡＰアプリケーションによって用いられてよい。

【００６０】

図１１のステップＳ１１０４において、ツイッターのOAuth認証サービスはＭＥＡＰ要求に対して未認可要求トークンで応答する。図１１のステップＳ１１０５において、ＭＥＡＰアプリケーションが未認可要求トークンを受信すると、ＭＥＡＰアプリケーションはユーザにログインおよびトークンの認可を促すため、未認可要求トークンを用いてユーザをツイッターのOAuthユーザ認証ＵＲＬ（図１０）にリダイレクトする。リダイレクトＵＲＬは、未認可要求トークンと、ＭＥＡＰアプリケーションに認可が与えられたらＭＥＡＰアプリケーションにユーザをリダイレクトするようにツイッターに要求するコールバックＵＲＬとを特定する。

【００６１】

図１１のステップＳ１１０６において、ＭＦＰ１０上のブラウザは、ツイッターのOAuthログインページに要求を送信することにより、リダイレクトを管理する。図１１のステップＳ１１０７において、ユーザは特定のツイッターＵＲＬ（図１０）にリダイレクトされ、そのサイトにサインインするように要求される。OAuthは、まずツイッターがリソースオーナーを認証してから、ユーザ（リソースオーナー）に（例えばアクセス要求ページを通じて）ＭＦＰへのアクセス許可を要求することを義務づけている。

【００６２】

ユーザはブラウザＵＲＬ（図１０）を見ることで、自身が今ツイッターのウェブページにいることを確認することができ、自身のツイッターユーザ名とパスワードを図１１のステップＳ１１０７およびＳ１１０８で入力することができる。

【００６３】

ツイッターサーバに直接アクセスするためにウェブブラウザを用いることにより、ユーザは自身のユーザ名およびパスワードを秘密に保つことができ、それらをＭＥＡＰアプリケーションや他のサイトと共有しなくてすむ。ユーザが自身のクレデンシャルをＭＥＡＰアプリケーションに入力することは決してない。

【００６４】
ツイッターへのログイン時またはツイッターに無事にログインした後、ユーザはクライアントであるＭＥＡＰアプリケーションにアクセスを許可するように要求される。ツイッターはユーザに、誰がアクセスを要求しているか（この場合はＭＥＡＰアプリケーション）と、許可されているアクセスタイプとをユーザに知らせる。図１１のステップＳ１１０８でユーザはアクセスを許可あるいは拒否することができる。
【００６５】
ユーザが要求を認可し、入力されたクレデンシャルが有効であれば、図１１のステップＳ１１０８で、ツイッターは要求トークン（仮のクレデンシャル）を、ユーザによる、リソースオーナーが認可したものとして特定（マーク）する。ユーザがアクセスを許可した場合、ツイッターのOAuth認証サービスは、ステップＳ１１０６でＭＥＡＰアプリケーションがＵＲＬに含めたコールバックＵＲＬにユーザをリダイレクトする（図１１のステップＳ１１０９）。ユーザはアカウントアクセスを拒否することもでき、その場合、OAuth認証サービスはＭＥＡＰアプリケーションに戻るためのリンクを有するページを表示するであろう。図１１のステップＳ１１１０で、ユーザのブラウザはリダイレクトを管理し、コールバックＵＲＬに要求を送信する。リダイレクトＵＲＬは認可された要求トークンの値を含んでいる。従ってブラウザは、仮のクレデンシャルＩＤ（認可済み要求トークン）とともにＭＥＡＰアプリケーションにリダイレクトされる。
【００６６】
ステップＳ１１１１でＭＥＡＰアプリケーションは、要求トークンをアクセストークンと交換するため、ツイッターのOAuth認証サービスに、署名された要求を送信する。ステップＳ１１１２で、ツイッターのOAuth認証サービスはＭＥＡＰアプリケーションからのこの要求に、アクセストークンとともに応答する。要求トークンはユーザ認可を得るためだけに有効であるが、アクセストークンは保護されたリソース、この場合はユーザのツイッターＩＤ（例えばツイッターアカウントユーザ名）へのアクセスに用いられる。最初の要求において、ＭＥＡＰアプリケーションは、署名された要求をツイッターの認証サービスへ提出することにより、要求トークンをアクセストークンと交換する（Ｓ１１１１，Ｓ１１１２）。得られた、特定のユーザに関連づけられたアクセストークンは、将来、ＭＥＡＰアプリケーションが同じユーザについての認証済み要求を行うために同じアクセストークンを使用できるよう、保存されてもよい（図１１のステップＳ１１１３）（例えば、第４の実施形態でより詳細に説明するように、ユーザに関するＲＦＩＤが、以前取得したアクセストークンと関連づけされてＭＦＰ１０に保存されてよい）。ステップＳ１１１４において、ＭＥＡＰアプリケーションは要求を認証するためにアクセストークンを用いてＡＰＩ要求を提出する。具体的には、２番目（複数の要求であってよい）の署名済み要求において、ＭＥＡＰアプリケーションはツイッターＡＰＩからユーザのツイッターＩＤを取得する（図１１、ステップＳ１１１５）。同時に、（図３から図７に関して上述したように）管理者によってツイッターに規定された、ＭＦＰ１０に対するＭＦＰリストがアクセスされ、ユーザのツイッターＩＤが、ユーザがアクセスを希望するＭＦＰ１０を表すＭＦＰリストに存在するか否かが判定される（図１１、ステップＳ１１１６およびＳ１１１７）。ＭＥＡＰアプリケーションが管理者のユーザ名およびパスワードを保存して入力するので、ＭＦＰ１０は管理者ツイッターアカウントに直接アクセスすることができる。あるいは、管理者のユーザ名／パスワードは保存されなくてもよい。この場合、管理者は、設定時にサーブレット（ウェブユーザインタフェース）を介してOAuthを用いてログインする。そして、このアカウントについてのアクセスおよびリフレッシュトークンはローカル保存される。アクセストークンが失効した場合（ツイッター起こる可能性は低いが）、再認証のためにリフレッシュトークンを用いることができる。そして、管理者のアクセストークンは管理者のツイッターアカウントにアクセスするために用いられ、次いでツイッターで管理者によってＭＦＰリストが定義される。ユーザのツイッターＩＤがリスト上に存在する場合、ユーザはそのＭＦＰへのアクセスを許可される。ユーザのツイッターＩＤがリスト上に存在しない場合、ＭＦＰ１０にエラーメッセージが表示されてよい。

【００６７】
●第２の実施形態
図３～図７に関して上述した「サービスプロバイダ上でのリスト設定」および図８に関して上述した「汎用ログイン手順」の内容は、本実施形態にも適用可能であるため、第２の実施形態に関してこれらの内容は省略する。
【００６８】
xAuthベースのログイン
図９～図１１に示した構成の代替構成を、図１２～図１４を参照して説明する。OAuth仕様1.0は、ユーザにクレデンシャルの開示を要求することなく、ウェブサイトまたはアプリケーションが、保護されたウェブリソースにアクセスすることを可能にするプロトコルである。図１２～図１４は、ＭＦＰ１０上で稼働するＭＥＡＰアプリケーションがウェブブラウザを起動する仕組みを持っていない場合など、ブラウザへのHTTPリダイレクションが利用できないか、好ましくない場合に、ユーザが自身のクレデンシャルを提供することを可能にする技術を示している。この実施形態は、（それが用いるヘッダx_authによる）xAuthと呼ばれる、OAuthの１バージョンを実施する。OAuthのこのバージョンは、図９～図１１に関して説明したようなブラウザへの往復を必要とする従前のOAuth体験とは異なるフローを用いる。
【００６９】
OAuthへのxAuth拡張は、クライアント（例えばＭＥＡＰアプリケーション）がブラウザを経由することなくユーザのクレデンシャルを取得してそれらをOAuthアクセストークンと交換することを可能にする。xAuthは（そうでないウェブアプリケーションとは対照的に）信頼できるコンテクストで動作するデスクトップおよびモバイルアプリケーションに適している。
【００７０】
xAuthは依然としてOAuthプロトコルの一部である。特定のサービスプロバイダ（例えばツイッター）に署名された要求を送信する必要があることは変わらない。
【００７１】
xAuth処理は読みとり専用または読み書きアクセストークンだけを生成するであろう。直接メッセージ読み出しアクセスはxAuthに備わらない。
【００７２】
xAuthはデスクトップおよびモバイルアプリケーションがユーザ名およびパスワードをOAuthアクセストークンと交換する方法を提供する。アクセストークンが読み出されると、ユーザに対応するパスワードはモバイル／デスクトップアプリケーションによって破棄される。ユーザ名もまた、モバイル／デスクトップアプリケーションによって破棄されてよい。しかし、図１４のステップ１４０３に関して後で詳述するように、ユーザ名はモバイル／デスクトップアプリケーションによって保存されてもよい。
【００７３】
xAuthはデスクトップおよびモバイルアプリケーションがトークン要求ならびに認証ステップをスキップし、アクセストークンステップへすぐジャンプすることを可能にする。
【００７４】
クライアントはアクセストークンの取得を要求する。
【００７５】
図１２から図１４に関し、説明を目的として、ユーザがＭＦＰ１０へ歩いて行き、ＭＦＰ１０にアクセスしたいという状況を想定する。ユーザがＭＦＰ１０の表示部２４を見ると、図１２に対応する表示が見える。ユーザは、「ツイッターを用いてサインイン」アイコン７０を選択するため、表示部２４のタッチ画面を用いる。タッチ画面上でアイコン７０がタッチされると、ログインアプリケーションであるＭＥＡＰアプリケーションは、ログイン画面を表示するために状態を変更する（図１４のステップＳ１４０１）。ＭＥＡＰアプリケーションは、１つ以上のサービスプロバイダ、例えばツイッター、フェイスブック、およびGoogle+のようなソーシャルネットワーキングサービスを用いるログインをサ

ポートするように構成されている。ＭＥＡＰアプリケーションはユーザに、図１３の操作部２５を用いて自身の認証クレデンシャルをＭＥＡＰアプリケーションに入力するように促す（図１４、ステップＳ１４０２）。本実施形態において、ユーザが自身のユーザ名をＭＥＡＰアプリケーションに入力する（図１３）ので、ＭＥＡＰアプリケーションは、その特定のユーザに対して、入力されたユーザ名をアクセストークンと関連づけて既に保存しているかもしれない。図１４のステップＳ１４０３で、ＭＥＡＰアプリケーションは、その特定のユーザについてアクセストークンが既に保存されているかどうかをチェックする。アクセストークンが既に保存されていれば、図１４のフローはステップＳ１４０７にスキップする。アクセストークンが保存されていなければ、図１４のフローはステップＳ１４０４に進む。図１４のステップＳ１４０４において、ブラウザを持たないＭＥＡＰアプリケーションにアクセストークンを要求するため、ＭＥＡＰアプリケーションは、ＭＥＡＰアプリケーションのコンシューマキーを用いて、サービスプロバイダのアクセストークンＵＲＬ（例えばツイッターアクセストークンＵＲＬ https://api.twitter.com/oauth/access_token）へのＳＳＬ（ＨＴＴＰＳ）要求を行う。従前のoauth_*シグナリングパラメータに加え、以下のポストパラメータを提示しなければならない。

x_auth_username：クライアントが代わりにトークンを取得しているユーザのログインクレデンシャル

x_auth_password：クライアントが代わりにトークンを取得しているユーザのパスワードクレデンシャル

x_auth_mode：この値は”client_auth”でなければならない（ここで説明する処理を参照）

【００７６】

応答

アクセストークンを許可するために、サービスプロバイダ（例えばツイッターのようなソーシャルネットワークプロバイダ）は、以下の点をチェックする。

・要求の署名がOAuth仕様で規定されているように正しく検証されていること
・供給されたタイムスタンプとノンスを有する要求がこれまで受信されていないこと
・供給されたユーザ名およびパスワードがユーザのクレデンシャルと合致すること

もしこれらが確認できれば、サービスプロバイダ（例えばツイッターＡＰＩ）はアクセストークンおよびトークンシークレットを生成し、それらをＨＴＴＰ応答本文で戻す（図１４、ステップＳ１４０５）。応答は以下のパラメータを含んでいる。

・oauth_token：アクセストークン
・oauth_token_secret：トークンシークレット
・x_auth_expires：アクセストークンが失効する、1970-01-01T00:00からの秒単位のタイムスタンプ、失効が指定されていない場合には０となる
・他のパラメータ：サービスプロバイダが規定した他の追加パラメータ

【００７７】

保護されたリソースへのアクセス

アクセストークンおよびトークンシークレットを無事に受信した後、ＭＥＡＰアプリケーションは、OAuth仕様の第７章のように、保護されたリソースにユーザに代わってアクセスすることができる。換言すれば、ここで取得されるアクセストークンは、OAuth仕様で定義されたアクセストークンと同一である。得られた、特定のユーザに関連付けられたアクセストークンは、その特定のユーザが次にＭＥＰ１０にアクセスする際に図１４のフローをステップＳ１４０３からステップＳ１４０７にスキップできるよう、ＭＥＡＰアプリケーションによって保存されてもよい（図１４、ステップＳ１４０６）。上述のプロセスを用いて認証されると、ＭＥＡＰアプリケーションは、そのユーザの保護リソース（ユーザのツイッターＩＤ）に対するその後の全ての要求に、返されたトークンシークレットを用いて署名する（図１４のステップＳ１４０７およびＳ１４０８）。これはOAuthを用いる場合にも当てはまる。特に、ＭＥＡＰアプリケーションは、取得されたアクセストークンを、サービスプロバイダＡＰＩ（例えばツイッターＡＰＩ）にユーザのツイッターＩ

Ｄ（ユーザ名）の提供を要求するために用いる。ＭＥＡＰアプリケーションがユーザのツイッターＩＤを取得すると（図１４、ステップＳ１４０８）、バックグラウンドで、（図３から図７を参照して上述したように）管理者によってツイッターに規定された、ＭＦＰ１０に対するＭＦＰリストがアクセスされ、ユーザのツイッターＩＤが、ユーザがアクセスを希望するＭＦＰ１０を表すＭＦＰリストに存在するか否かが判定される（図１４、ステップＳ１４０９およびＳ１４１０）。ユーザのツイッターＩＤがリスト上に存在する場合、ユーザはＭＦＰ１０へのアクセスを許可される。ユーザのツイッターＩＤがリスト上に存在しない場合、ＭＦＰ１０にエラーメッセージが表示されてよい。

【００７８】

●第３の実施形態

図１５は第３の実施形態の画像処理システムのアーキテクチャを示している。画像処理システムは第１および第２の実施形態のＭＰＦ（多機能周辺機器）１０および認証サーバ１２と、携帯電話機１１のようなモバイル機器を有している。ＭＰＦ１０、携帯電話機１１、および認証サーバ１２はＷｉＦｉネットワーク１４およびインターネットのようなネットワークを通じて互いに通信可能である。

【００７９】

図１６は携帯電話機１１のハードウェア構成を示している。携帯電話機１１はデジタル信号処理部３１に接続された制御部３０を有する。制御部３０は表示部３２、操作部３３、カメラ部３４、外部Ｉ／Ｆ３５、無線通信部３６、および電源部３７の動作を制御する。表示部３２は携帯電話機１１のユーザに情報を表示するためのＬＣＤディスプレイを有している。操作部３３はユーザが携帯電話機１１に入力することを可能にするキーパッドおよび他の操作ボタンを有している。カメラ部３４は携帯電話機１１に組み込まれたカメラであり、ユーザが写真を撮ったり視覚的な情報を収集することを可能にする。外部Ｉ／Ｆ３５は携帯電話機１１が他の機器と通信することを可能にするポートを携帯電話機１１に提供する。特に外部Ｉ／Ｆ３５は携帯電話機１１が携帯電話機１１に保存されているデータ（詳細な連絡先やカレンダーに入力されたデータなど）をコンピュータに保存されているデータと同期するためにコンピュータと接続することを可能にする。無線通信部３６は様々な無線サービスに関するサポートを提供する。特に無線通信部３６は、Ｗｉ－Ｆｉ接続に関するサポートを提供する。無線通信部３６はアンテナ３８に接続されている。電源部３７は電池と、外部電源から電池を充電するための機構を含んでいる。

【００８０】

デジタル信号処理部３１は音声入力部３９、音声出力部４０、およびＲＦ入力／出力部４１に接続されている。音声入力部３９はマイク４２からの音声信号を受信し、変換するアナログデジタルプロセッサである。音声出力部４０はデジタル信号を受信し、スピーカ４３で出力するアナログ出力に変換するデジタルアナログプロセッサである。ＲＦ入力／出力部４１はアンテナ４４に接続され、携帯電話機１１がローカル携帯電話局と通信することを可能にする。音声入力部３９、音声出力部４０、デジタル信号処理部３１およびＲＦ入力／出力部４１は、携帯電話機１１がポータブルな電話機として動作することを可能にする。

【００８１】

携帯電話機１１はいわゆる「スマートフォン」であり、Google（登録商標）Android（登録商標）オペレーティングシステムが動作している。他の実施形態では、異なる携帯電話機用のオペレーティングシステムが動作するものを含む、他のタイプの電話機を用いることができる。

【００８２】

図３～図７に関して上述した「サービスプロバイダ上でのリスト設定」および図８に関して上述した「汎用ログイン手順」の内容は、本実施形態にも適用可能であるため、第３の実施形態に関してこれらの内容は省略する。なお、図８に関し、第３の実施形態では、受信するログイン詳細がＰＩＮコードであることに留意されたい。

【００８３】

携帯電話機を用いたアクセス

図９～図１１および図１２～図１４に示した構成の代替構成を、図１７～図１９を参照して説明する。図１７～図１９は、ＭＦＰ１０上で稼働するＭＥＡＰアプリケーションがウェブブラウザを起動する仕組みを持っていない場合に、ユーザが自身のクレデンシャルをOAuthの仕組みを用いて提供することを可能にする技術を示している。

【００８４】

説明を目的として、携帯電話機１１を手に持っているユーザがＭＦＰ１０まで歩いて行き、ＭＦＰ１０を用いてスキャンまたはプリントを行いたいシナリオを想定する。ユーザはＭＦＰ１０の表示部２４を見ると、図１７に対応する表示が見える。ユーザは、「ツイッターを用いてサインイン」アイコン５０を選択するため、表示部２４のタッチ画面を用いる。タッチ画面上でアイコンがタッチされると、ログインアプリケーションであるＭＥＡＰアプリケーションは、ログイン画面を表示するために状態を変更する（図１９のステップＳ１９０１）。

【００８５】

ＭＥＡＰアプリケーションは、１つ以上のソーシャルネットワーキングサービス（例えばツイッター）を用いてログインすることができるように構成される。そのようにするため、ＭＥＡＰアプリケーションはツイッターのOAuth対応ＡＰＩとともに用いるためのクライアントクレデンシャル群（クライアントＩＤおよびシークレット）を、事前にツイッターから取得している。

【００８６】

ＭＥＡＰアプリケーションは、ツイッターのOAuth認証サービスから要求トークンを取得するため、要求パラメータの１つとしてoauth_callback=oobを含んだ署名済み要求を送信して仮クレデンシャル群をツイッターに要求する。この時点で、仮クレデンシャルはリソースオーナー固有のものではなく、ユーザのツイッターアカウントにアクセスするためのリソースオーナー認可をユーザから得るためにＭＥＡＰアプリケーションによって用いられてよい。

【００８７】

図１９のステップＳ１９０３でＭＥＡＰアプリケーションが仮クレデンシャル（要求トークン）を受信すると、ＭＥＡＰアプリケーションは、（要求トークンに対応する）oauth_tokenパラメータを含んだ、ツイッターのOAuthユーザ認証ＵＲＬへのリンクを生成する。そして図１９のステップＳ１９０４で、ＭＥＡＰアプリケーションは、生成したツイッターのOAuthユーザ認証ＵＲＬへのリンクを、装置が読み取り可能なコードまたはバーコード（例えばＱＲコード）に埋め込み、そのバーコードをＭＦＰ１０の表示部２４に表示する。

【００８８】

携帯電話機１１を持っているユーザは次に、携帯電話機上の適切なアプリケーションを用いて、ＭＦＰ１０に表示されている装置が読み取り可能なコードをスキャンする（図１９、ステップＳ１９０５）と、携帯電話機１１のウェブブラウザをツイッターがOAuthユーザ認証ＵＲＬにリダイレクトされ（図１９、ステップＳ１９０６およびＳ１９０７）、ユーザはツイッターにログインするように要求される（図１８および、図１９のステップＳ１９０８およびＳ１９０９）。上述の通り、OAuthは、まずリソースオーナ（ユーザ）を認証してから、ユーザにクライアント（例えばＭＥＡＰアプリケーション）へのアクセス許可を要求することをサーバに義務づけている。

【００８９】

ユーザはブラウザＵＲＬ（図１８）を見ることで、自身が今ツイッターのウェブページにいることを確認することができ、自身のツイッターユーザ名とパスワードを図１８および、図１９のステップＳ１９０９で入力する。

【００９０】

OAuthはユーザが自身のユーザ名およびパスワードを秘密に保ち、それらをＭＥＡＰアプリケーションや他のサイトと共有しなくてすむようにできる。ユーザが自身のクレデン

シャルをＭＥＡＰアプリケーションに入力することは決してない。
【００９１】
ツイッターへのログイン時またはツイッターに無事にログインした後、ユーザはクライアントであるＭＥＡＰアプリケーションにアクセスを許可するように要求される。ツイッターはユーザに、誰がアクセスを要求しているか（この場合はＭＥＡＰアプリケーション）と、許可されているアクセスタイプとをユーザに知らせる。図１９のステップＳ１９０９でユーザは、アクセスを許可あるいは拒否することができる。
【００９２】
ユーザが要求を認可し、入力されたクレデンシャルが有効であれば、ツイッターは仮クレデンシャルを、ユーザによる、リソースオーナーが認可したものとして特定（マーク）する。そして、携帯電話機１１上のブラウザはoauth_verifier（例えばＰＩＮコード）を表示するページにリダイレクトされる（図１９、Ｓ１９１０）。
【００９３】
図１９のステップＳ１９１１でユーザは、ＭＦＰ１０の操作部を用い、ＭＥＡＰアプリケーションの画面にＰＩＮコードを入力する。ＭＥＡＰアプリケーションは入力されたＰＩＮコードを収集ならびに保存してもよい（図１９、Ｓ１９１２）。
【００９４】
ユーザが待機している間、バックグラウンドで、ＭＥＡＰアプリケーションが、ユーザがoauth_verifierの値として入力したＰＩＮコードを含んだ認証済み要求トークンを用い、それをアクセストークンと交換している（図１９、ステップＳ１９１３およびＳ１９１４）。要求トークンはユーザ認可を得るためだけに有効であるが、アクセストークンは保護されたリソース、この場合はユーザのツイッターＩＤへのアクセスに用いられる。最初の要求において、ＭＥＡＰアプリケーションは、署名された要求をツイッターの認証サービスへ提出することにより、要求トークンをアクセストークンと交換する（図１９のＳ１９１３，Ｓ１９１４）。得られた、特定のユーザに関連づけられたアクセストークンは、将来、ＭＥＡＰアプリケーションが同じユーザについての認証済み要求を行うために同じアクセストークンを使用できるよう、保存されてもよい（図１９のステップＳ１９１５）。２番目（複数の要求であってよい）の要求において、ＭＥＡＰアプリケーションはユーザのツイッターＩＤを取得する（図１９、ステップＳ１９１６およびＳ１９１７）。同時に、（図３から図７に関して上述したように）管理者によってツイッターに規定された、ＭＦＰ１０に対するＭＦＰリストがアクセスされ、ユーザのツイッターＩＤが、ユーザがアクセスを希望するＭＦＰ１０を表すＭＦＰリストに存在するか否かが判定される（図１９、ステップＳ１９１８およびＳ１９１９）。ユーザのツイッターＩＤがリスト上に存在する場合、ユーザはＭＦＰ１０へのアクセスを許可される。ユーザのツイッターＩＤがリスト上に存在しない場合、ＭＦＰ１０にエラーメッセージが表示されてよい。
【００９５】
oauth_callbackは図９～図１１に関してはオプションパラメータであり、ＭＥＡＰアプリケーションがユーザのツイッターＩＤへのアクセスを許可された後、ユーザがリダイレクトされるＵＲＬを指定するものである。図１７～図１９に関し、oauth_callbackはoauth_callback=oobに設定され、これによってＭＦＰ１０にＰＩＮコードが表示されるようになる。しかし、oauth_callbackパラメータを設定しないことにより、ＰＩＮコードの表示ステップ（図１９のステップＳ１９１０）をスキップすることも可能である。従って、ユーザがログインプロセスを成功裏に完了（図１９のステップＳ１９０９）した後、フローは、要求トークンがアクセストークンと交換されるステップＳ１９１３に直接スキップしてもよい。
【００９６】
●第４の実施形態
図３～図７に関して上述した「サービスプロバイダ上でのリスト設定」および図８に関して上述した「汎用ログイン手順」の内容は、本実施形態にも適用可能であるため、第４の実施形態に関してこれらの内容は省略する。

【００９７】
図２０Ａおよび図２０Ｂに関し、説明を目的として、ユーザがＭＦＰ１０へ歩いて行き、ＭＦＰ１０にアクセスしたいという状況を想定する。本実施形態において、ユーザはＭＦＰ１０にアクセスするために、（例えば携帯電話機１１に取り付けられている）ＲＦＩＤカードまたはＲＦＩＤタグを用いる。ユーザが自身のＲＦＩＤカードまたはＲＦＩＤタグをカードリーダ２１２に接触させると、ログインアプリケーションであるＭＥＡＰアプリケーションは、ＭＦＰ１０にログイン画面を表示するために状態を変更する。ＭＥＡＰアプリケーションはＭＦＰ１０に以前アクセスしたユーザの登録リストを維持しており、受信したＲＦＩＤ ＩＤに基づいて、その特定のユーザに対するアクセストークンが既に保存されているかどうかを判定する（図２０Ａ参照）。

【００９８】
図２０ＢのステップＳ２００１において、ＭＥＡＰアプリケーションはカードリーダ２１２からＲＦＩＤを受信する。図２０ＢのステップＳ２００２において、ＭＥＡＰアプリケーションは受信したＲＦＩＤに対応するアクセストークンがＭＥＡＰアプリケーションによって維持されている登録リストに存在するかどうか判断する。

【００９９】
受信したＲＦＩＤに関するアクセストークンが存在する場合、図２０Ｂのフローはステップ Ｓ２００３に進む。ステップＳ２００３で、（図３から図７に関して上述したように）管理者によってツイッターに規定された、ＭＦＰ１０に対するＭＦＰリストがアクセスされ、ユーザのツイッターＩＤが、ユーザがアクセスを希望するＭＦＰ１０を表すＭＦＰリストに存在するか否かが判定される。

【０１００】
ユーザのツイッターＩＤがリスト上に存在する場合、ユーザはそのＭＦＰへのアクセスを許可される（図２０Ｂ、ステップＳ２００４）。ユーザのツイッターＩＤがリスト上に存在しない場合、ＭＦＰ１０にエラーメッセージが表示されてよい（ステップＳ２００５）。ステップＳ２００３，Ｓ２００４，Ｓ２００５は図１１のステップＳ１１１４～Ｓ１１１７、図１４のステップＳ１４０７～Ｓ１４１０、および図１９のステップＳ１９１６～Ｓ１９１９に対応する。

【０１０１】
図２０ＢのステップＳ２００２において、受信したＲＦＩＤに対するアクセストークンが存在しないと判定された場合、図２０Ｂのフローはステップ Ｓ２００６に進む。ステップＳ２００６において、図８，１１，１４および１９で上述したフローチャートのいずれかを実行することにより、アクセストークンを取得することができる。ＭＥＡＰアプリケーションによってアクセストークンが受信されると、ＭＥＡＰアプリケーションは特定のユーザのＲＦＩＤと、対応するアクセストークンとを登録リストに保存する（図２０Ａ）。

【０１０２】
●第５の実施形態
第３の実施形態で説明した、画像処理装置のアーキテクチャ（図１５）および、携帯電話機のハードウェア構成（図１６）は、本実施形態にも適用可能であるため、本実施形態においてこれら図面の説明は省略する。図３～図７に関して上述した「サービスプロバイダ上でのリスト設定」の内容は、本実施形態にも適用可能であるため、本実施形態に関してこれらの内容は省略する。第５の実施形態において、「携帯電話機を用いたアクセス」は以下の様に実施される。

【０１０３】
説明を目的として、携帯電話機１１を手に持っているユーザがＭＦＰ１０まで歩いて行き、ＭＦＰ１０を用いてスキャンまたはプリントを行いたいシナリオを想定する。ユーザがＭＦＰ１０の表示部２４を見ると、図１７に対応する表示が見える。ユーザは、「ツイッターを用いてサインイン」アイコン５０を選択するため、表示部２４のタッチ画面を用いる。タッチ画面上でアイコンがタッチされると、ログインアプリケーションであるＭＥ

ＡＰアプリケーションは、ログイン画面を表示するために状態を変更する（図２１のステップＳ２１０１）。

【０１０４】

ＭＥＡＰアプリケーションは、１つ以上のソーシャルネットワーキングサービス（例えばツイッター）を用いてログインすることができるように構成される。そのようにするため、管理者は事前に、ＭＦＰ１０についてのソーシャルネットワーキングサービスアカウント（例えばツイッターアカウント）を作成しておく。ＭＰＦ１０で稼動するＭＥＡＰアプリケーションは、乱数または疑似乱数生成器を用いて乱数を生成するように構成される（図２１のステップＳ２１０２）。ＭＥＡＰアプリケーションはＭＦＰのツイッターアカウントに接続（図２１のステップＳ２１０３）し、乱数を、ソーシャルネットワーキングサービスの１以上のユーザに関連付けて登録する（図２１のステップＳ２１０４）。例えば、乱数は、図３～図７に関して上述したユーザのリストに関連付けられて（リンクされて）よい。ＭＥＡＰアプリケーションは乱数およびＭＦＰのツイッターアカウントを特定する情報（ユーザ名）を、装置が読み取り可能なコードまたはバーコード（例えばＱＲコード）に埋め込み（図２１、ステップＳ２１０５）、その、装置が読み取り可能なコードを、ＭＦＰ１０の表示部２４に表示する（図２１、ステップＳ２１０６）ように構成されている。

【０１０５】

携帯電話機１１を持っているユーザは次に、周辺装置でユーザを認証するためのアプリケーションを携帯電話機１１で起動する（図２２のステップＳ２２０１）。携帯電話機１１上のアプリケーションは、ＭＦＰ１０に表示されている、装置が読み取り可能なコードまたはバーコードをスキャンする（図２２、ステップＳ２２０２）ために用いられ、そのアプリケーションはユーザを自身のツイッターアカウントに自動ログインさせる（図２２、ステップＳ２２０３）ように構成されている。そしてそのアプリケーションは、周辺装置に表示された識別コードと、ユーザのソーシャルネットワーキングアカウントを特定する情報とを有するメッセージを生成する（図２２、ステップＳ２２０４）ように構成される。そしてアプリケーションは、ＭＥＡＰアプリケーションがＭＦＰのツイッターアカウントを用いて見ることのできる直接メッセージまたはツイートを送信する（図２２、ステップＳ２２０５）。このメッセージはＭＦＰのツイッターアカウント（インボックス）に直接（ダイレクトメッセージ、すなわちプライベートに）送信されてもよいし、ツイッターの複数のユーザがアクセス可能な場所にポストされてもよい。例えば、ツイートはそのユーザのフォロワーに送信（ポスト）されてよい。もちろん、ツイッターへのログインステップ、メッセージの生成ステップ、およびメッセージの送信ステップは、ユーザが手動で実行してもよい。ＭＦＰ１０で稼動するＭＥＡＰアプリケーションは、ＭＦＰのツイッターアカウントにログインしてメッセージをツイッターから読み出す（図２３、ステップＳ２３０１）ように構成されている。ＭＥＡＰアプリケーションは、メッセージに含まれる詳細が、ＭＦＰのソーシャルネットワーキングアカウントに登録されている（図２１のステップＳ２１０４を参照）詳細に対応するかどうかを判定する（図２３のステップＳ２３０２）ように構成されている。例えば、ＭＥＡＰアプリケーションは、メッセージに含まれるユーザＩＤと乱数が、ＭＦＰのツイッターアカウントに登録されている数字およびユーザＩＤと対応するかどうかを判定する。詳細が対応する場合、ＭＦＰ１０はユーザにアクセスを許可する（図２３のステップＳ２３０３）。ＭＥＡＰアプリケーションは、ユーザのソーシャルネットワーキングサービスアカウント情報に基づいて、ユーザによって異なるアクセスレベルを許可することができる。例えば、ユーザ名１にはコピーとスキャンの許可を割り当てることができ、ユーザ名２にはコピーの許可のみを割り当てることができる。メッセージ内の詳細がツイッターアカウントに登録されている詳細と対応しない場合に、ＭＦＰ１０がユーザにアクセスを許可しないことは言うまでもない（図２３、ステップＳ２３０４）。

【０１０６】

代替実施形態において、識別情報はＭＦＰ１０のＧＰＳ座標に基づいて生成される。Ｍ

ＦＰ１０は、ＭＦＰのＧＰＳ座標を、第１の識別情報の一部としてソーシャルネットワーキングサービス（例えばツイッター）に所定数登録する。ユーザがＭＦＰ１０にアクセスを希望する場合、ユーザは携帯電話機１１をＭＦＰ１０の上に置き、携帯電話機１１上で予め定められたアプリケーションを開く。この、予め定められたアプリケーションは携帯電話機１１のＧＰＳ部にアクセスし、携帯電話機の位置を特定するＧＰＳ座標を特定する（あるいは、携帯電話機はＭＦＰのディスプレイからＧＰＳ座標を読み取ってもよい）。携帯電話機１１上のアプリケーションは、所定数のＧＰＳ座標を選択し、ＭＦＰ１０に送信されるメッセージでこれらの座標を識別情報として用いる。（携帯電話機１１がＭＦＰ１０の上に置かれているため）携帯電話機１１およびＭＦＰ１０は同じ場所にある。そのためＭＦＰ１０について登録されている第１の識別情報は携帯電話機１１が生成した識別情報と合致し、ユーザのツイッターＩＤ（これは携帯電話機１１からＭＦＰ１０に送信されるメッセージにも含まれている）がツイッター上でＭＰＦ１０について登録されているＧＰＳ座標に関連付けられていれば、ユーザはＭＦＰ１０へのアクセスを許可される。

【０１０７】

●第６の実施形態

本実施形態では、管理者がＭＰＦ１０についてのソーシャルネットワーキングサービスアカウント（例えばツイッター）を設定する。ＭＦＰ１０で稼動するＭＥＡＰアプリケーションは、ＭＦＰのソーシャルネットワーキングサービスアカウントに接続（図２４、ステップＳ２４０１）し、ＭＦＰ１０の動作に関する情報をソーシャルネットワーキングサービスのユーザに送信するように構成されている（図２４、ステップＳ２４０２）。例えば、ＭＦＰ１０はツイッターアカウントを有している。興味のあるユーザ（一般には管理者ユーザであろう）は、ＭＦＰ１０を「フォロー」するであろう。そして、ＭＰＦ１０は、自身の状態に関する情報（例えば媒体切れ、紙詰まりおよび他のエラー）や、利用に関する情報（例えばＭＦＰ１０のユーザを特定する情報、ユーザに対するＭＦＰ１０の使用料明細、周辺装置の位置に関する情報、周辺装置の全体または個別ユーザアクティビティに関する情報、ユーザ動作を処理巣ツタ目に周辺装置が用いている素材（例えば紙のタイプ）に関する情報、およびサービス情報（例えばサービス要求））をツイートするように構成されてよい。

【０１０８】

●第７の実施形態

本実施形態は第６の実施形態を変形したものである。本実施形態において、ＭＰＦ１０は、ソーシャルネットワーキングサービスのフォローユーザに、ユーザのアクティビティに関する情報を送信するために自身のソーシャルネットワーキングサービスアカウントを用いるように構成されている。例えば、ＭＦＰ１０がツイッターアカウントを有するものとした場合、ＭＥＡＰアプリケーションは、恐らくは販売促進情報をブロードキャストするマーケティングツールとして、ユーザのアクティビティに関するツイートを行うように構成されてよい。例えば、「@JoeBloggsがすばらしく美しいCanonカラーで１５ページコピーしました！Canonを選ぼう！」といった具合である。この場合、ＭＦＰ１０内のＭＥＡＰアプリケーションは、ユーザのツイッターアカウントを用いてツイートするであろう。そのため、ユーザはこれを可能にするためにアクセスを許可する必要があるだろう。これは以前説明したOAuth/xAuthログインプロセスの間に起こりうる。あるいは、ＭＦＰ１０は自身のアカウントを用いてツイートし、そのツイート内でユーザのツイッターアカウントを記述する。

【０１０９】

本発明の実施形態を説明してきた。本発明のさらなる実施形態は、上述した実施形態の１つ以上の機能を実行するために、記憶装置に記録されたプログラムを読み出して実行するシステムや、上述した実施形態の１つ以上の機能を実行するために、例えば記憶装置に記録されたプログラムを読み出して実行することによってステップが実行される方法によっても実現することができる。この目的のため、１つ以上のプログラムが、ネットワークを通じて、あるいは記憶装置として機能する様々なタイプの記録媒体（例えばコンピュー

タ読み取り可能な媒体）から、周辺装置、モバイル機器および画像処理システムに提供されてよい。

【図１】

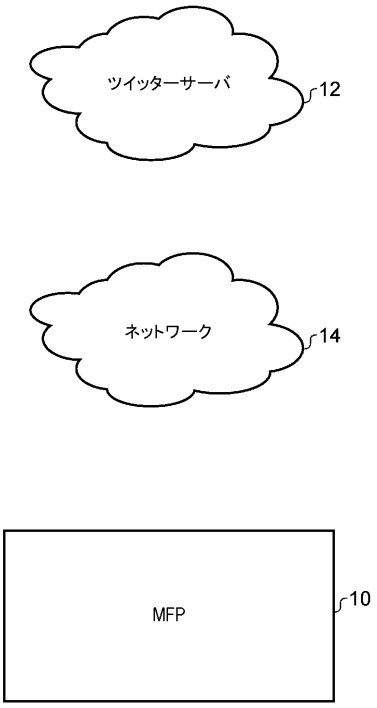

FIG. 1

【図２】

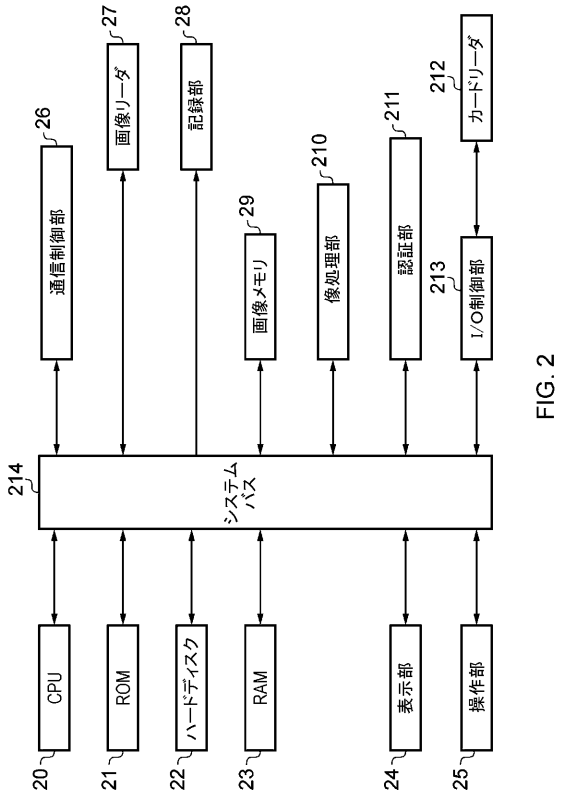

FIG. 2

【図３】

この図は公序良俗違反のため不掲載とする

【図４】

この図は公序良俗違反のため不掲載とする

【図５】

この図は公序良俗違反のため不掲載とする

【図６】

この図は公序良俗違反のため不掲載とする

【図７】

この図は公序良俗違反のため不掲載とする

【図８】

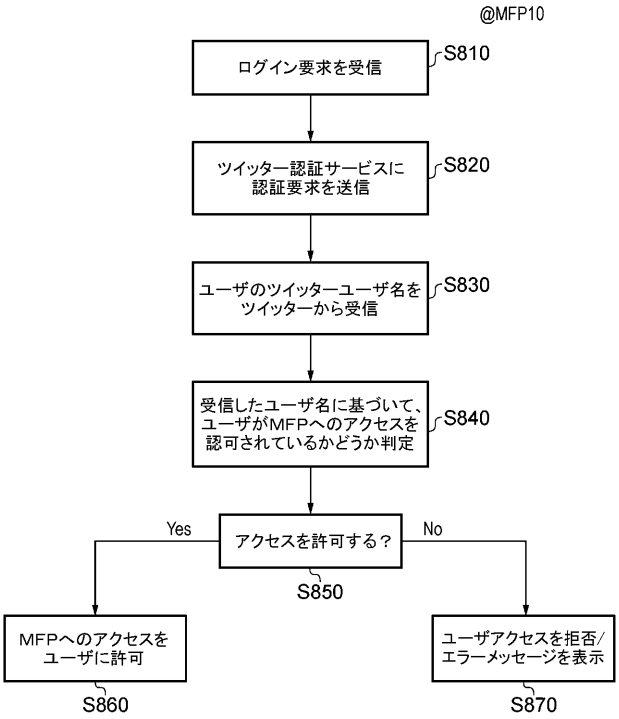

FIG. 8

【図９】

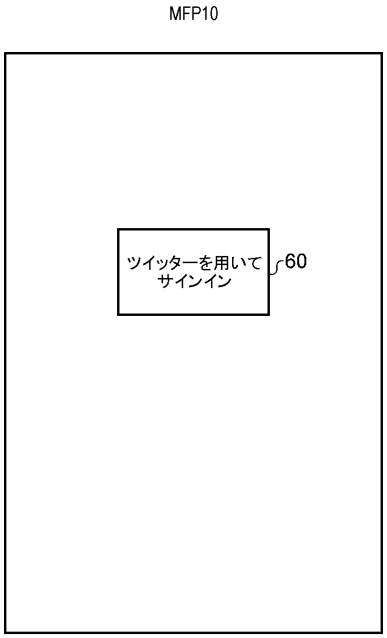

FIG. 9

【図１０】

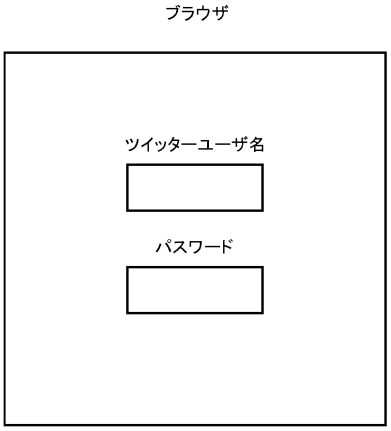

FIG. 10

【図１１】

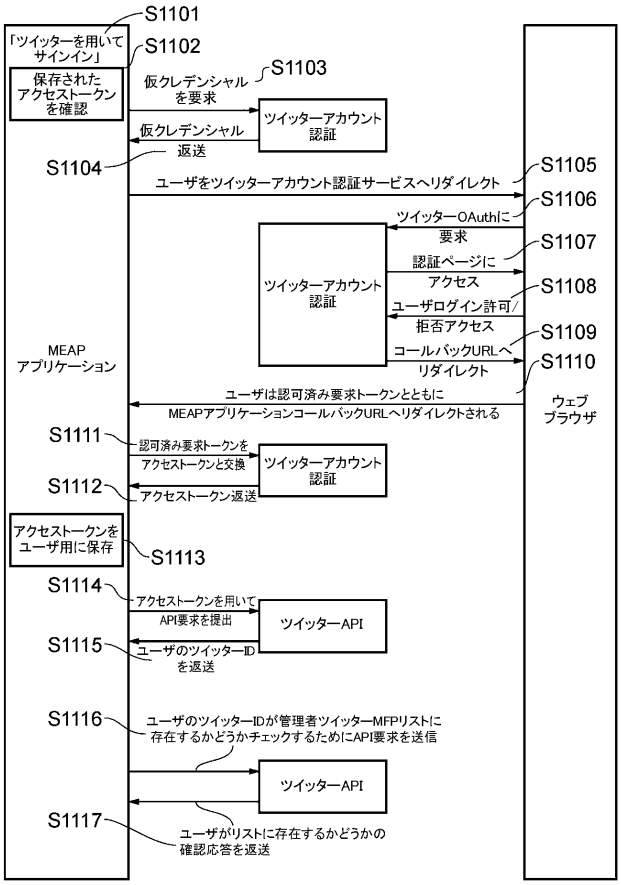

FIG. 11

【図１２】

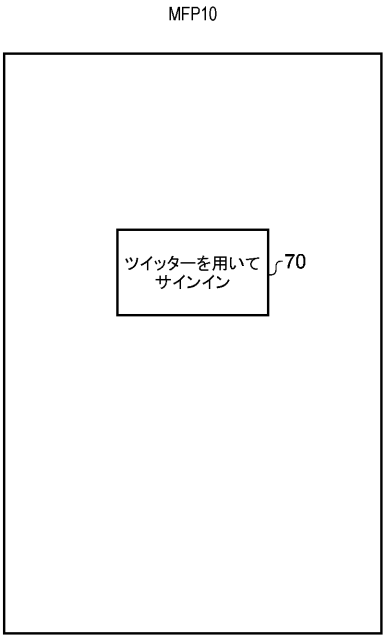

FIG. 12

【図１３】

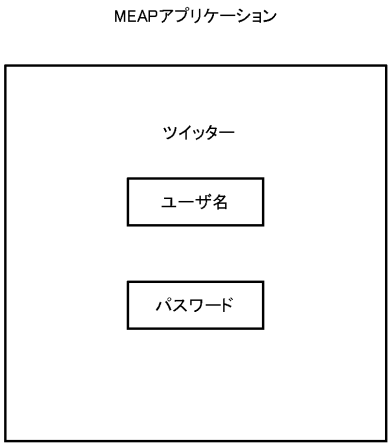

FIG. 13

【図１４】

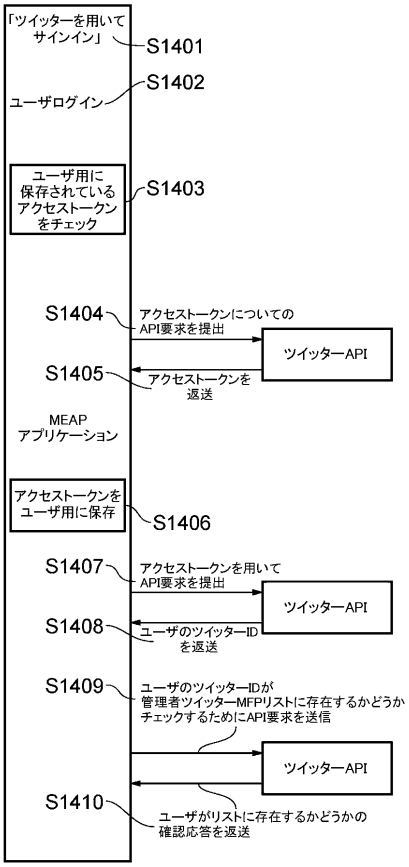

FIG. 14

【図１５】

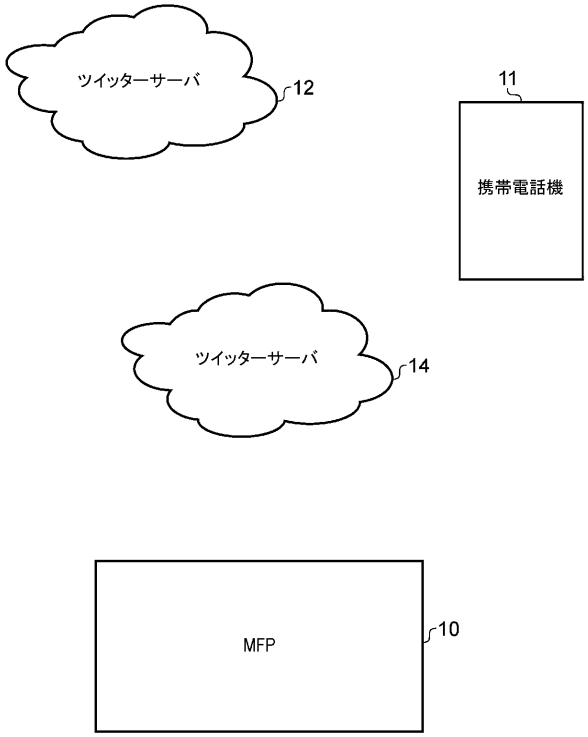

FIG. 15

【図１６】

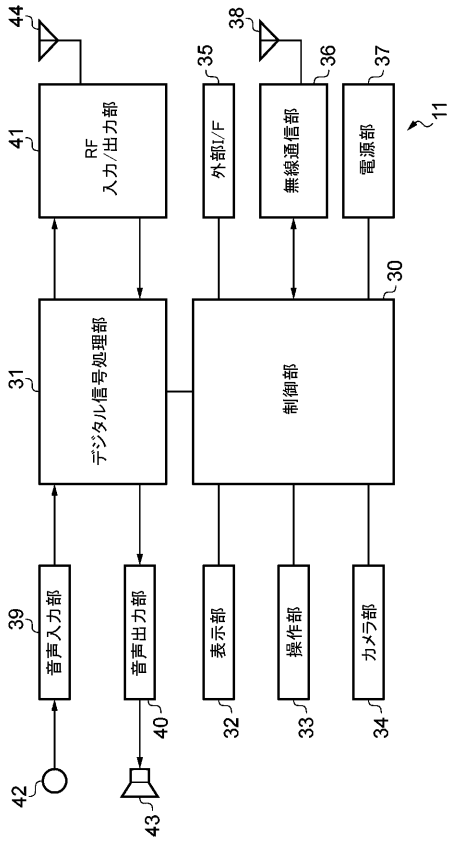

FIG. 16

【図１７】

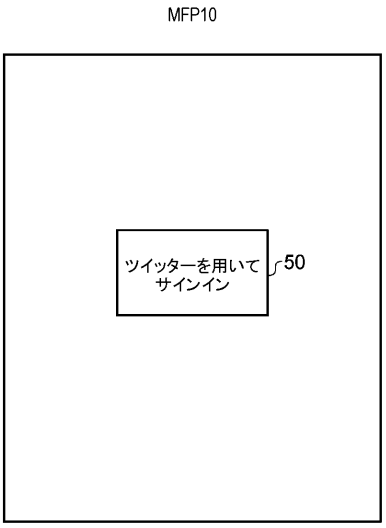

FIG. 17

【図１８】

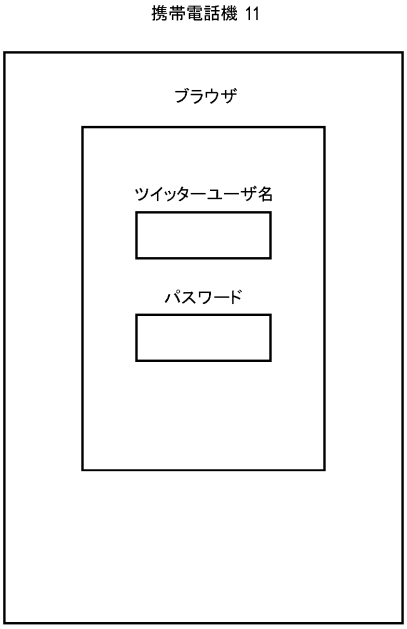

FIG. 18

【図１９】

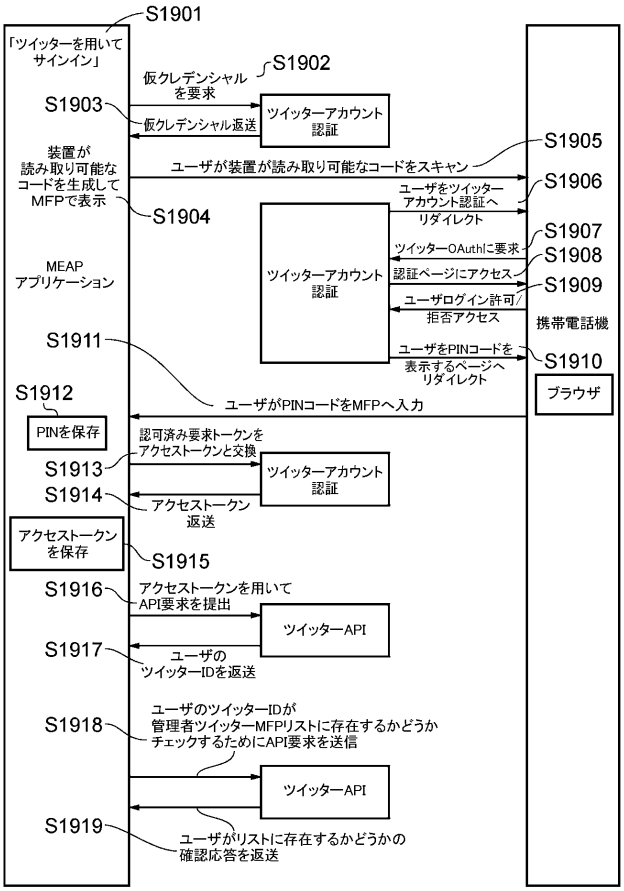

FIG. 19

【図２０Ａ】

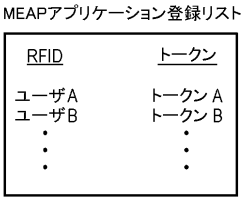

FIG. 20A

【図２０Ｂ】

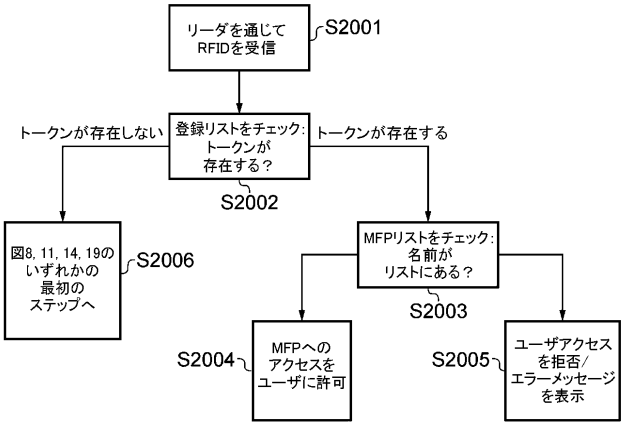

FIG. 20B

【図２１】

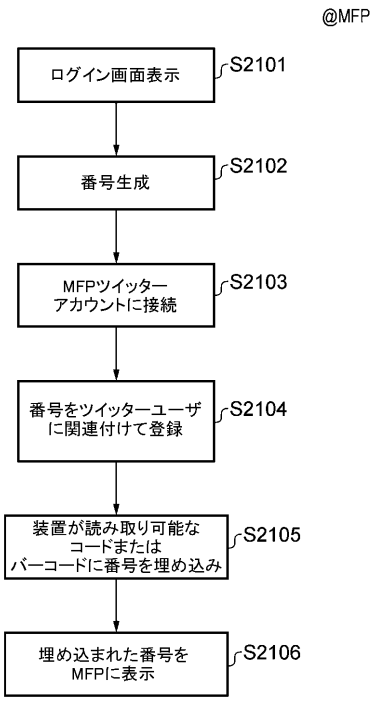

FIG. 21

【図２２】

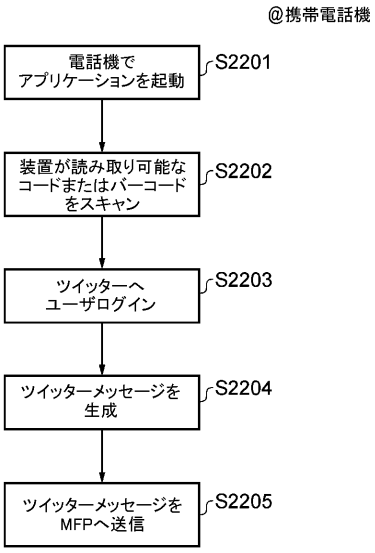

FIG. 22

【図２３】

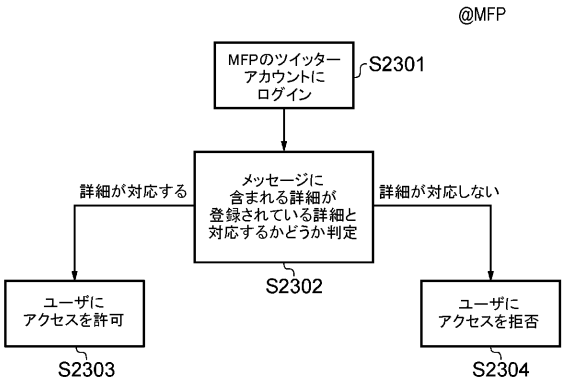

FIG. 23

【図２４】

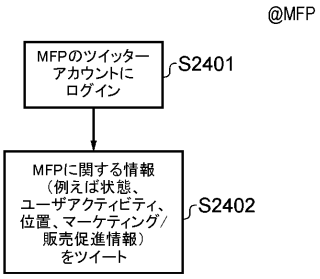

FIG. 24

フロントページの続き

(74)代理人 100134175
弁理士 永川 行光
(72)発明者 ベンジャミン ジョン, パークス
イギリス国 バークシャー州 アールジー６ ４エイチエヌ, リーディング, ロウワー アーリー, ヒルマントン ２５

Ｆターム(参考) 5B084 AA02 AA06 AA30 AB30 AB36 AB39 BA09 BB12 DA16 DB08
DC02 DC03

【外国語明細書】
2014197385000001.pdf