

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6444855号  
(P6444855)

(45) 発行日 平成30年12月26日 (2018.12.26)

(24) 登録日 平成30年12月7日 (2018.12.7)

(51) Int. Cl.	F I
<b>G06F 21/62 (2013.01)</b>	G06F 21/62 318
<b>G06F 21/60 (2013.01)</b>	G06F 21/60 340
<b>G06Q 50/10 (2012.01)</b>	G06Q 50/10

請求項の数 31 (全 25 頁)

(21) 出願番号	特願2015-501830 (P2015-501830)	(73) 特許権者	391030332
(86) (22) 出願日	平成25年3月18日 (2013.3.18)		アルカテルルーセント
(65) 公表番号	特表2015-518201 (P2015-518201A)		フランス国、92100・ブローニュービ
(43) 公表日	平成27年6月25日 (2015.6.25)		ヤンクール、ルート・ドゥ・ラ・レーヌ・
(86) 国際出願番号	PCT/US2013/032751		148/152
(87) 国際公開番号	W02013/142399	(74) 代理人	100094112
(87) 国際公開日	平成25年9月26日 (2013.9.26)		弁理士 岡部 譲
審査請求日	平成26年10月27日 (2014.10.27)	(74) 代理人	100106183
審判番号	不服2017-2771 (P2017-2771/J1)		弁理士 吉澤 弘司
審判請求日	平成29年2月27日 (2017.2.27)	(72) 発明者	メンテン, ローレンス, イー.
(31) 優先権主張番号	13/423,795		アメリカ合衆国 07974-0636
(32) 優先日	平成24年3月19日 (2012.3.19)		ニュージャージー, マレイ ヒル, マウ
(33) 優先権主張国	米国 (US)		ンテン アヴェニュー 600-700
(31) 優先権主張番号	13/423,697		
(32) 優先日	平成24年3月19日 (2012.3.19)		
(33) 優先権主張国	米国 (US)		

最終頁に続く

(54) 【発明の名称】 クエリ言語を使用してウェブ・サービスに対するアクセス制御を修正する方法

## (57) 【特許請求の範囲】

## 【請求項 1】

サービスが呼び出されることに応答して1つまたは複数のノードにアクセス制御クエリを構成するための情報を受信するステップであって、前記サービスは、第1のユーザに関連するソーシャル・グラフのリソースへのアクセスを要求するためにアクセス制御クエリを使用するように構成され、前記リソースのサブセットは前記ソーシャル・グラフの一部分内のノードに関連する、ステップと、

前記アクセス制御クエリが前記ノードに関連する前記ソーシャル・グラフの前記リソースの前記サブセットで動作するように前記ノードに前記アクセス制御クエリをアタッチするステップであって、前記アクセス制御クエリは、第2のユーザと前記リソースとの関係を表す履歴情報、および、前記第2のユーザと前記リソースの所有者である前記第1のユーザとの関係を表す履歴情報の少なくとも1つに応じて、前記リソースの前記サブセットにアクセスするための要求が許可されるか、それとも拒否されるかを示す情報を返す、ステップと

を含む、プロセッサによって実行される方法。

## 【請求項 2】

第2のユーザから、前記ノードに関連する前記リソースの前記サブセットにアクセスするための要求を受信し、前記要求を受信することに応答して前記アクセス制御クエリを呼び出すステップを含む請求項1に記載の方法。

## 【請求項 3】

10

20

前記アクセス制御クエリを呼び出すステップは、前記第1のユーザとの前記第2のユーザの関係を表す履歴情報または前記リソースの前記サブセットとの前記第2のユーザの関係を表す履歴情報の少なくとも1つに基づいて、要求を許可するか、それとも拒否するかを決定するステップを含み、前記関係は、前記ソーシャル・グラフのエッジによって表される請求項2に記載の方法。

【請求項4】

前記アクセス制御クエリを呼び出すステップは、前記リソースの前記サブセットにアクセスするための要求が許可されるか、それとも拒否されるかを示すブール値を返すステップを含む請求項3に記載の方法。

【請求項5】

前記ノードに前記アクセス制御クエリをアタッチするステップは、前記第1のユーザが、前記ノードに関連する前記リソースの前記サブセットへのアクセスを要求するサービスを呼び出すことに応答して、前記ノードに前記アクセス制御クエリをアタッチするステップを含む請求項1に記載の方法。

【請求項6】

前記第1のユーザが前記サービスを呼び出すことに応答して、前記第1のユーザに関連する前記ソーシャル・グラフの前記一部分に前記ノードを追加し、次に前記新しく追加されたノードに前記アクセス制御クエリをアタッチするステップをさらに含む請求項5に記載の方法。

【請求項7】

前記第1のユーザが前記サービスを終了することに応答して前記アクセス制御クエリを削除するステップをさらに含む請求項5に記載の方法。

【請求項8】

前記ノードに前記アクセス制御クエリをアタッチするステップは、前記第1のユーザが、前記第1のユーザによって所有される前記ノードに前記アクセス制御クエリをアタッチすることを承認したと決定したことに応答して前記ノードに前記アクセス制御クエリをアタッチするステップを含む請求項1に記載の方法。

【請求項9】

前記ノードに前記アクセス制御クエリをアタッチするステップは、前記ソーシャル・グラフを所有するサービス・プロバイダが、前記第1のユーザによって所有される前記ノードに前記アクセス制御クエリをアタッチすることを承認したと決定したことに応答して前記ノードに前記アクセス制御クエリをアタッチするステップを含む請求項1に記載の方法。

【請求項10】

第1のユーザによって所有されるソーシャル・グラフのリソースに対してアクセス制御クエリを実行するように構成されたサービスを呼び出すステップであって、前記リソースのサブセットは前記ソーシャル・グラフの一部分内のノードに関連する、ステップと、

前記アクセス制御クエリが、第2のユーザと前記リソースとの関係を表す履歴情報、および、前記第2のユーザと前記リソースの所有者である前記第1のユーザとの関係を表す履歴情報の少なくとも1つに応じて、前記ノードと関連する前記リソースの前記サブセットにアクセスするための要求が許可されるか、それとも拒否されるかを決定するように、サービスを呼び出すことに応答して前記ノードに前記アクセス制御クエリをアタッチするステップと

を含む、プロセッサによって実行される方法。

【請求項11】

前記ノードに前記アクセス制御クエリをアタッチするステップは、前記第1のユーザが、前記ノードに関連する前記リソースの前記サブセットへのアクセスを要求するサービスを呼び出すことに応答して、前記ノードに前記アクセス制御クエリをアタッチするステップを含む請求項10に記載の方法。

【請求項12】

前記第 1 のユーザが前記サービス呼び出すことに応答して、前記第 1 のユーザに関連する前記ソーシャル・グラフの前記一部分に前記ノードを追加し、次に前記新しく追加されたノードに前記アクセス制御クエリをアタッチするステップをさらに含む請求項 11 に記載の方法。

【請求項 13】

前記第 1 のユーザが前記サービスを終了することに応答して前記アクセス制御クエリを削除するステップをさらに含む請求項 11 に記載の方法。

【請求項 14】

前記ノードに前記アクセス制御クエリをアタッチするステップは、前記第 1 のユーザが、前記第 1 のユーザによって所有される前記ノードに前記アクセス制御クエリをアタッチすることを承認したと決定したことに応答して前記ノードに前記アクセス制御クエリをアタッチするステップを含む請求項 10 に記載の方法。

10

【請求項 15】

前記ノードに前記アクセス制御クエリをアタッチするステップは、前記ソーシャル・グラフを所有するサービス・プロバイダが、前記第 1 のユーザによって所有される前記ノードに前記アクセス制御クエリをアタッチすることを承認したと決定したことに応答して前記ノードに前記アクセス制御クエリをアタッチするステップを含む請求項 10 に記載の方法。

【請求項 16】

第 2 のユーザから、前記ノードに関連する前記リソースの前記サブセットにアクセスするための前記サービスを使用する要求を受信し、前記要求を受信することに応答して前記アクセス制御クエリを呼び出すステップを含む請求項 10 に記載の方法。

20

【請求項 17】

前記アクセス制御クエリを呼び出すステップは、前記第 1 のユーザとの前記第 2 のユーザの関係を表す履歴情報または前記リソースの前記サブセットとの前記第 2 のユーザの関係を表す履歴情報の少なくとも 1 つに基づいて、要求を許可するか、それとも拒否するかを決定するステップを含み、前記関係は、前記ソーシャル・グラフのエッジによって表される請求項 16 に記載の方法。

【請求項 18】

前記アクセス制御クエリを呼び出すステップは、前記リソースの前記サブセットにアクセスするための要求が許可されるか、それとも拒否されるかを示すブール値を返すステップを含む請求項 16 に記載の方法。

30

【請求項 19】

前記要求が許可されることを示す前記ブール値を返す前記アクセス制御クエリに応答して前記リソースへのアクセスを有する前記サービスを提供するステップをさらに含む請求項 18 に記載の方法。

【請求項 20】

ソーシャル・グラフの一部分へのアクセス制御を提供する装置であって、  
データ記憶装置と、  
前記データ記憶装置と通信可能に結合されるプロセッサと  
を含み、前記プロセッサは、

40

サービスが呼び出されることに応答して 1 つまたは複数のノードにアクセス制御クエリを構成するための情報を受信するステップであって、前記サービスは、第 1 のユーザに関連するソーシャル・グラフのリソースへのアクセスを要求するためにアクセス制御クエリを使用するように構成され、前記リソースのサブセットは前記ソーシャル・グラフの前記一部分内のノードに関連する、ステップと、

前記アクセス制御クエリが前記ノードに関連する前記ソーシャル・グラフの前記リソースの前記サブセットで動作するように前記ノードに前記アクセス制御クエリをアタッチするステップであって、前記アクセス制御クエリは、第 2 のユーザと前記リソースとの関係を表す履歴情報、および、前記第 2 のユーザと前記リソースの所有者である前記第 1 の

50

ユーザとの関係を表す履歴情報の少なくとも1つに応じて、前記リソースの前記サブセットにアクセスするための要求が許可されるか、それとも拒否されるかを示す情報を返す、ステップとを含むプログラムを実行するように構成された装置。

【請求項 2 1】

前記プロセッサが実行する前記プログラムは、第2のユーザから、前記ノードに関連する前記リソースの前記サブセットにアクセスするための要求を受信し、前記要求を受信することに応じて前記アクセス制御クエリを呼び出すステップをさらに含む請求項20に記載の装置。

【請求項 2 2】

前記プロセッサが実行する前記プログラムは、前記第1のユーザが前記ノードに関連する前記リソースの前記サブセットへのアクセスを要求するサービスを呼び出すことに応答して、前記ノードに前記アクセス制御クエリをアタッチすることにより、前記ノードに前記アクセス制御クエリをアタッチするステップをさらに含む請求項20に記載の装置。

【請求項 2 3】

前記プロセッサが実行する前記プログラムは、前記第1のユーザが前記サービスを呼び出すことに応答して、前記第1のユーザに関連するソーシャル・グラフの前記一部分に前記ノードを追加し、次に前記新しく追加されたノードに前記アクセス制御クエリをアタッチするステップをさらに含む請求項22に記載の装置。

【請求項 2 4】

前記プロセッサが実行する前記プログラムは、前記第1のユーザが前記サービスを終了することに応答して前記アクセス制御クエリを削除するステップをさらに含む請求項22に記載の装置。

【請求項 2 5】

前記プロセッサが実行する前記プログラムは、前記第1のユーザが、前記第1のユーザによって所有される前記ノードに前記アクセス制御クエリをアタッチすることを承認したと決定したことに応答して前記ノードに前記アクセス制御クエリをアタッチすることにより前記ノードに前記アクセス制御クエリをアタッチするステップをさらに含む請求項20に記載の装置。

【請求項 2 6】

前記プロセッサが実行する前記プログラムは、前記ソーシャル・グラフを所有するサービス・プロバイダが、前記第1のユーザによって所有される前記ノードに前記アクセス制御クエリをアタッチすることを承認したと決定したことに応答して前記ノードに前記アクセス制御クエリをアタッチすることにより、前記ノードに前記アクセス制御クエリをアタッチするステップをさらに含む請求項20に記載の装置。

【請求項 2 7】

ソーシャル・グラフの一部分へのアクセス制御提供する装置であって、  
データ記憶装置と、  
前記データ記憶装置と通信可能に結合されるプロセッサと  
を含み、前記プロセッサは、

第1のユーザによって所有されるソーシャル・グラフのリソースに対してアクセス制御クエリを実行するように構成されたサービスを呼び出すステップであって、前記リソースのサブセットは前記ソーシャル・グラフの前記一部分内のノードに関連するステップと、

前記アクセス制御クエリが、第2のユーザと前記リソースとの関係を表す履歴情報、および、前記第2のユーザと前記リソースの所有者である第1のユーザとの関係を表す履歴情報の少なくとも1つに応じて、前記ノードと関連する前記リソースの前記サブセットにアクセスするための要求が許可されるか、それとも拒否されるかを決定するように、サービスを呼び出すことに応答して前記ノードに前記アクセス制御クエリをアタッチする、ステップとを含むプログラムを実行するように構成された装置。

【請求項 2 8】

前記プロセッサが実行する前記プログラムは、前記第1のユーザが前記サービスを呼び出すことに応答して、前記第1のユーザに関連する前記ソーシャル・グラフの前記一部分に前記ノードを追加し、次に前記新しく追加されたノードに前記アクセス制御クエリをアタッチするステップをさらに含む請求項27に記載の装置。

【請求項29】

前記プロセッサが実行する前記プログラムは、前記第1のユーザが前記サービスを終了することに応答して前記アクセス制御クエリを削除するステップをさらに含む請求項27に記載の装置。

【請求項30】

前記プロセッサが実行する前記プログラムは、前記第1のユーザが、前記第1のユーザによって所有される前記ノードに前記アクセス制御クエリをアタッチすることを承認したと決定したことに応答して前記ノードに前記アクセス制御クエリをアタッチすることにより前記ノードに前記アクセス制御クエリをアタッチするステップをさらに含む請求項27に記載の装置。

10

【請求項31】

前記プロセッサが実行する前記プログラムは、前記ソーシャル・グラフを所有するサービス・プロバイダが、前記第1のユーザによって所有される前記ノードに前記アクセス制御クエリをアタッチすることを承認したと決定したことに応答して前記ノードに前記アクセス制御クエリをアタッチすることにより、前記ノードに前記アクセス制御クエリをアタッチするステップをさらに含む請求項27に記載の装置。

20

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

本出願は、2012年3月19日に出願した、Lawrence E. Mentenによる米国特許出願第13/423,697号「Method of Extending Web Service Application Programming Interfaces using Query Languages」の一部継続出願である。

【0002】

30

本出願は、一般的に、プロセッサベースのシステムに関し、より具体的には、プロセッサベースのシステムのためのアクセス制御に関する。

【背景技術】

【0003】

本項では、請求される主題についてより深い理解を容易にするのに役に立つ可能性がある態様を紹介する。したがって、本項の記述は、この観点から読むべきであり、何が従来技術であるか、または何が従来技術でないかについて自ら認めるものと理解するべきではない。

【0004】

一部の知られている通信方式では、ユーザは、ソーシャル・ネットワークを使用して、互いに通信する。ソーシャル・ネットワーキング・サービスは、共通の背景、関心事、または活動を共有できる人々の間の社会的関係の表現に基づいて加入者にサービスを提供するオンライン・サービス、プラットフォーム、またはサイトとして規定することができる。ソーシャル・ネットワークは、典型的には、各ユーザの表現（多くの場合プロフィール）、彼/彼女のソーシャル・リンク、および写真、状況報告、ウェブ・リンクなど様々な追加的な要素から構成される。ほとんどのソーシャル・ネットワーク・サービスはウェブベースであり、電子メールおよびインスタント・メッセージングなど、インターネットを通じてユーザが対話することを可能にするツール/サービスを提供する。ソーシャル・ネットワーキング・サイトは、ユーザが個々のネットワーク内で考え、活動、イベント、および関心事を共有することを可能にする。代表的なソーシャル・ネットワークには、F a

40

50

cebook、Google+、Twitter、LinkedIn、VKontakte、Orkut、およびRenRenが含まれる。

【0005】

ソーシャル・ネットワークは、ソーシャル・グラフを使用して、個人および彼らの関係を表す。一般的に、ソーシャル・グラフは、(ユーザのアバタとも呼ぶことができる)加入者のオンライン・ペルソナ(persona)と、他の加入者のオンライン・ペルソナとの関係を記述するものである。したがって、ソーシャル・グラフは、一般的にはソーシャル・ネットワークと呼ばれる、加入者間の現実世界の関係を反映している。たとえば、ソーシャル・ネットワークのソーシャル・グラフは、ノード間の関係によって規定された(リンクまたは接続とも呼ぶことができる)エッジを使用して互いに関連する一連のノード(たとえば、「Subscriber(加入者)」、「FriendsLists(友達リスト)」、「CloseFriends(親しい友達)」など)として構造化することができる。葉ノードは、親ノードに関連しているが、それらは子ノードを持たない。たとえば、「CloseFriends」ノードに関連する葉ノードはそれぞれ、加入者の友達の1人に対する情報を含むデータ構造を含むことができる。ソーシャル・グラフは、また、特定の関心事に関連するグループなど異なるタイプの関係のためのノードだけでなく、写真、音楽、およびウェブ・リンクなど異なるタイプの情報のためのノードも含むことができる。ソーシャル・グラフを構築するノード、エッジ、情報、および関係は、ソーシャル・グラフのリソースと呼ぶことができる。

【0006】

ソーシャル・グラフのリソースは、関係を表すエッジによってソーシャル・グラフで明示的に接続されていないユーザまたは加入者に関連する場合がある。たとえば、加入者は、親睦会のピクニックですべての卒業生のグループ写真を投稿することができる。グループ写真は、加入者のFriendsListsまたはCloseFriendsのグループに記載されている人々およびソーシャル・グラフの加入者にリンクされていない他の人々の画像を含むことができる。加入者または加入者の友達は、加入者にリンクされていないグループ写真の人々を識別または「タグ付け」することができる。他の例では、加入者は、グループを規定したが、ソーシャル・グラフで互いにリンクされていない可能性がある加入者にすべてリンクされている他の加入者を含む、「Business\_\_Lunch\_\_Group」などのグループを規定することができる。ともにリンクされている加入者は、ビジネス・ランチをスケジュールリングするための計画メッセージなど、ソーシャル・ネットワークを通じて情報を交換することができない場合がある。

【0007】

ソーシャル・ネットワークのプロバイダは、サービスまたはアプリケーション(アプリ)を実装するためにソーシャル・グラフの情報を使用する。開発者は、ソーシャル・ネットワーク・プロバイダによって開発およびサポートされるアプリケーション・プログラミング・インターフェース(API)を使用して、サービスまたはアプリケーションを作成することができる。ソーシャル・ネットワークのためのAPIは通常、クライアントおよびサーバから構成されるRepresentational State Transfer(REST)構造を実装する。クライアントは、サーバへの要求を開始し、サーバは要求を処理し、適切な応答をクライアントに返す。要求および応答は、リソースの表現の転送について構築される。リソースは、実質的に、アドレス指定することができる任意の一貫性および意味のある概念でもよい。リソースの表現は、典型的には、リソースの現在の、または意図する状態を収めるドキュメントである。一般的に、REST-full構造は、クライアントサーバ・ベース、ステートレス、キャッシュ可能、レイヤ構造であり、一様なインターフェースを使用する必要があり、要求に応じてコードを提供することができる。たとえば、Facebookなどソーシャル・ネットワークのためのAPIは、ハイパーテキスト転送プロトコル(HTTP)要求メッセージの規定された組とともに、たとえば、拡張マークアップ言語(XML)またはJavaScript Object Notation(JSON)形式の応答メッセージの構造の定義を含む。

## 【発明の概要】

## 【課題を解決するための手段】

## 【0008】

以下は、開示された内容の一部の態様について基本的な理解を得るために、開示された内容を単純化して概要を示すものである。この概要は、開示された内容の完全な概要ではない。これは、開示された内容の重要または不可欠な要素を特定することも、開示された内容の範囲を示すことも意図するものではない。その唯一の目的は、後で記述するより詳細な記述の準備として、単純化した形で一部の概念を示すことである。

## 【0009】

一実施形態では、ソーシャル・グラフのリソースへのアクセスを制御するための方法が提供される。方法の一実施形態は、サービスが呼び出されることに応答してクエリを構成するための情報を受信するステップを含む。サービスは、第1のユーザに関連するソーシャル・グラフの一部分内のノードに関連するリソースへのアクセスを要求ためにクエリを使用するように構成される。方法は、また、ノードにクエリに関連させるステップを含む。クエリは、ノードに関連するリソースに対して動作し、ソーシャル・グラフの現在の状態に応じて、リソースにアクセスするための要求が許可されるか、それとも拒否されるかを示す情報を返す。

10

## 【0010】

他の実施形態では、ソーシャル・グラフのリソースへのアクセスを制御するための方法が提供される。方法の一実施形態は、第1のユーザによって所有されるソーシャル・グラフの一部分内のノードに関連するリソースに対してクエリを実行するように構成されたサービスを呼び出すステップを含む。方法のこの実施形態は、また、サービスを呼び出すことに応答してノードにクエリに関連させるステップを含む。クエリは、ソーシャル・グラフの現在の状態に応じて、ノードに関連するリソースにアクセスするための要求を許可するか、それとも拒否するかを決定する。

20

## 【0011】

開示された内容は、同じ参照番号は同じ要素を示している添付の図面とともに以下の記述を参照することによって理解されるだろう。

## 【図面の簡単な説明】

## 【0012】

30

【図1】通信システムの代表的な一実施形態を概念的に示す図である。

【図2】ソーシャル・グラフの一部分の第1の代表的な実施形態を概念的に示す図である。

【図3】ソーシャル・グラフに対するアクセス制御を修正するための方法の第1の代表的な実施形態を概念的に示す図である。

【図4】ソーシャル・グラフへの修正されたアプリケーション・プログラミング・インターフェースにクエリする方法の代表的な一実施形態を概念的に示す図である。

【図5】ソーシャル・グラフへのアプリケーション・プログラミング・インターフェースへの修正を取り除くまたは逆転させる方法の代表的な一実施形態を概念的に示す図である。

40

【図6】ソーシャル・グラフの一部分の第2の代表的な実施形態を概念的に示す図である。

【図7】ソーシャル・グラフに対するアクセス制御を修正するための方法の第2の代表的な実施形態を概念的に示す図である。

## 【発明を実施するための形態】

## 【0013】

例示的实施形態について以下に記述する。分かりやすくするために、実際の実装のすべての機能が本明細書に記述されているとは限らない。もちろん、そのような実際の実施形態を開発する際に、実装によって異なる、システム関連およびビジネス関連の制約への遵守など、開発者の特定の目標を達成するために多数の実装特有の決定が下されるべきであ

50

ることを理解されたい。さらに、そのような開発努力は、複雑かつ時間がかかる可能性があるが、本開示の利益を受ける当業者にとっては日常的な仕事であろうことを理解されたい。記述および図は、単に特許請求される主題の原理を示すものである。したがって、本明細書に明示的に記述または図示していないが、本明細書に記述した原理を具体化し、特許請求された主題の範囲内に含まれ得る様々な構成を当業者であれば考案できることを理解されたい。さらに、本明細書に詳述したすべての例は、原則として、読者が特許請求された主題の原則およびその技術を推進する発明者（ら）によって提供された概念を理解するのを支援するために、教育のみを目的とすることを明確に意図するものであり、そのような具体的に詳述された例および条件に限定しないものとして解釈するべきである。

#### 【0014】

ここで、開示された内容について、添付の図面に関して記述する。様々な構造、システム、およびデバイスは、説明のみを目的として、かつ当業者に周知の詳細によって記述を不明瞭にしないように、図面に概略的に示している。しかし、添付の図は、開示された内容の実例となる例を記述し説明するために含まれている。本明細書に使用される単語および句は、当業者によるそれらの単語および句の理解に一致する意味を持つものと理解および解釈するべきである。本明細書において用語または句を一貫して使用することによって、用語または句の特別な定義、つまり、当業者によって理解されている通常および慣習的な意味とは異なる定義を意味することを意図するものではない。用語または句が特別な意味、つまり当業者によって理解されるものと異なる意味を持つことを意図する場合は、そのような特別な定義は、用語または句の特別な定義を直接的かつ明白に提供する定義方法で明細書に特に記述することになる。さらに、本明細書に使用する「または（or）」という用語は、そうでないことが明記されていない限り（たとえば、「さもなければ（otherwise）」または「別の方法では（in the alternative）」など）、非排他的な「または（or）」を示している。また、本明細書に記述した様々な実施形態は、必ずしも相互排他的ではなく、一部の実施形態は、新しい実施形態を形成するために、1つまたは複数の他の実施形態と組み合わせることができる。

#### 【0015】

ソーシャル・ネットワーク・サービスの加入者（またはその他のユーザ）は、加入者の個人情報の安全および秘密を維持するために、ソーシャル・ネットワーク・サービスのプロバイダに依拠している。しかし、加入者は、また、たとえば「Friends Lists」に示される加入者など、選択された加入者に個人情報をブロードキャスト、送信、または表示するためにソーシャル・ネットワーク・サービスを使用する。ソーシャル・ネットワーク・サービスのプロバイダは、ソーシャル・グラフの特定部分に関連するリソースにユーザがアクセスできるかどうかを決定するアクセス制御ポリシーを規定することによって、情報を公開し、かつそれを秘密に維持するという競合する要望のバランスをとることを試みる。たとえば、Joe Subscriberの「Friends Lists」で指定されたユーザは、典型的には、Joe Subscriberによって投稿された状態の更新、写真、または他の情報を見ることができる。ネットワークにおけるJoeの友達は、また、たとえば、彼の「ウォール」に書き込むか、または彼が投稿した情報に関してコメントすることによって、Joe Subscriberに情報を送信または投稿できる場合がある。他のユーザは、典型的には、Joe Subscriberによって投稿された情報を見ることができないか、または彼が投稿した情報に関してコメントすることができない。加入者は、たとえば、一部のカテゴリの情報を公開する、または他の情報カテゴリへのアクセスを友達または友達の友達に制限することによって、情報へのアクセスを制御する能力が制限されている。

#### 【0016】

ソーシャル・グラフの情報に誰がアクセスできるかを決定するアクセス制御ポリシーは、一般的に静的である。たとえば、現在のRESTfulウェブ・サービスAPIは、ソーシャル・グラフのリソースおよびそれらのリソースへのアクセスをゲート制御するアクセス制御方式の両方を静的に規定する。アクセス制御方式は、エンド・ユーザ/加入者に

10

20

30

40

50

よって、またはアプリケーション開発者もしくは他のサード・パーティによって拡張可能ではない。したがって、加入者は、事前規定されたセキュリティ設定を使用して、個人情報へのアクセスを制限することができるが、加入者もサード・パーティも、事前規定されたセキュリティ設定を変更することはできない。結果として、アプリケーションの操作に必要なアクセスを許可するには、エンド・ユーザより広範なリソースへのアクセスを許可することを必要とするか、またはサービス・プロバイダは、たとえば、いつでもすべてのユーザに対してグローバルに許可する意思があるため、潜在的に価値のある多数のアプリケーションを作成することができない。

#### 【 0 0 1 7 】

本出願に記述した技術の実施形態は、開発者またはサード・パーティが、ソーシャル・グラフの現在の状態に基づいて、関連するリソースへのアクセスを許可する、（既存または新しい）リソースにクエリをアタッチすることを可能にすることができる。たとえば、クエリは、リソースを所有するユーザとの要求元ユーザの関係、リソースとの要求元ユーザの関係、または両方の基準の組み合わせに基づいて、リソースへのアクセスを許可することができる。リソースへのアクセスは、また、リソース所有者とリソース要求元との間の過去の対話に基づいて、許可することも、または拒否することもできる。たとえば、写真に頻繁に現れた、またはリソース所有者によって所有されるリソースに頻繁にコメントした要求元にアクセスを許可することができる。アクセスを許可するクエリは、リソースへのアクセスが許可されたかどうかを示すブール値を返す。ユーザまたはソーシャル・ネットワーク・サービスのプロバイダは、アクセス制御クエリをソーシャル・グラフに追加することができる前に、リソースにクエリをアタッチすることを承認することができる。開発者または他のサード・パーティは、ユーザのリソースに条件付きアクセスを提供できるクエリを作成し、次にユーザのリソースの拡大されたアクセス可能性を利用するアプリケーションまたはサービスを作成するためにこれらのクエリを使用することができる。たとえば、開発者は、第1のユーザによって投稿された写真などのリソースへのアクセスを許可するアプリケーションを作成できるため、第1のユーザによって所有されるリソースの読み込みまたは書き込みが通常は承認されていなくても、写真でタグを付けられたユーザまたは加入者は、写真に関してコメントすることができる。アクセス制御クエリは、動的または一時的な場合がある。たとえば、承認されたアクセス制御クエリは、ユーザが、アクセス制御クエリを使用するサービスを開始することに応答して、ユーザのリソースにアタッチすることができ、次に、サービスが終了するときに、アクセス制御クエリを除去することができる。

#### 【 0 0 1 8 】

図1は、通信システム100の代表的な一実施形態を概念的に示す図である。図示する実施形態では、通信システム100は、複数の加入者またはユーザ105を含む。本明細書で使用する場合、「加入者」という用語は、ソーシャル・グラフをサポートするソーシャル・ネットワーク・サービスに申し込んだユーザを表すものと理解される。「ユーザ」という用語は、ソーシャル・グラフで参照できるか、またはソーシャル・グラフに関連している可能性があるが、必ずしもソーシャル・ネットワーク・サービスの加入者ではない人々またはエンティティを表している。したがって、加入者は、ソーシャル・ネットワーク・サービスに関連するユーザのサブセットの場合がある。たとえば、加入者は、ソーシャル・ネットワーク・サービスの登録されたユーザと呼ぶことができる。ユーザ105は、スマート・フォンなどの移動通信装置として示されている。しかし、本開示の恩恵を受ける当業者は、「ユーザ」という用語は、通信システム100にアクセスするために使用される電子デバイス、またはデバイスを所有または運用する人を表すことができることを理解されたい。さらに、当業者は、電子デバイスは移動通信装置に限定されず、一部の実施形態では、タブレット型コンピュータ、ラップトップ型コンピュータ、デスクトップ型コンピュータなどのデバイスも、通信システム100にアクセスするために使用することができることを理解されたい。様々な実施形態において、ユーザ105は、有線接続、無線接続、またはそれらの任意の組み合わせを使用して、通信システム100にアクセスす

10

20

30

40

50

ることができる。

#### 【0019】

ユーザ105は、1つまたは複数のソーシャル・ネットワーク・サービス110、115に加入することができる。代表的なソーシャル・ネットワーク・サービスには、Facebookによって提供されるソーシャル・ネットワーク・サービス110、およびGoogle+によって提供されるソーシャル・ネットワーク・サービス115が含まれる。しかし、本開示の恩恵を受ける当業者は、通信システム100の代替実施形態は、Twitter、LinkedIn、VKontakte、Orkut、RenRenなど、他のソーシャル・ネットワーク・サービスを含むことができることを理解されたい。図示する実施形態では、ユーザ105(1~4)は、ソーシャル・ネットワーク・サービス110に加入しており、ユーザ105(4~5)は、ソーシャル・ネットワーク・サービス115に加入している。したがって、ユーザ105はプロフィールを作成し、ソーシャル・ネットワーク・サービス110、115のソーシャル・グラフの他の加入者との関係を築いておくことができる。ユーザ105、ユーザ105に関する情報、およびユーザ105間の関係は、ソーシャル・グラフの構造によって表すことができる。たとえば、ソーシャル・ネットワーク110のソーシャル・グラフは、ノード間の関係によって規定されたエッジを使用して互いに関連されたノード(たとえば、「Subscriber」、「FriendsLists」、「CloseFriends」など)を含むことができる。

#### 【0020】

アプリケーション開発者120は、ユーザ105、またはユーザ105に狙いを定めた広告を提供することを試みる広告主など他のサード・パーティのために有益な情報を生成および提供するために、ソーシャル・ネットワーク110、115のソーシャル・グラフの情報を使用するアプリケーション(アプリ)またはサービスを開発することができる。アプリケーション開発者120は、ソーシャル・ネットワーク・サービス110、115に対してアプリケーション・プログラミング・インターフェース(API)125、130を使用するアプリケーションまたはサービスをそれぞれ作成または規定する。API125、130は、ソーシャル・ネットワーク・サービス110、115のプロバイダまたは所有者によって最初に規定され、同じAPI125、130は、ユーザ105のすべてに対してサポートされる。一実施形態では、API125、130は、Representational State Transfer(REST)構造によって課された制約に準拠する。ソーシャル・ネットワーキング・サイト110、115へのREST-fulウェブ・サービスAPI125、130は、(サービスAPIによって規定された)リソース階層を提供し、各ユーザ105に関連するソーシャル・ネットワーク情報の様々な要素への読み込みまたは書き込みアクセスをサポートすることができる。たとえば、リソース階層は、情報のカテゴリまたはサブセットを規定する非葉ノードを含むツリーを規定することができる。ツリーは、また、ウェブ・サービスAPI125、130を通じて読み込みまたは書き込みできるデータのインスタンスを表すノードまたは葉を規定することができる。この構成は、多くのウェブ・サービスにおいて一般的である。従来のウェブ・サービスで、リソース指定方式は、サービス・プロバイダによって規定されており拡張可能ではない。

#### 【0021】

本明細書に記述したように、ソーシャル・ネットワーキング・サイト110、115へのREST-fulウェブ・サービスAPI125、130は、リソース、およびリソースへのアクセスを制御またはゲート制御するアクセス制御方式を静的に規定する。本明細書に記述した技術の実施形態は、たとえば、ユーザごとまたはサービスごとまたはアプリケーションごとにアクセス制御権を拡大することによって、より柔軟なアクセス制御をサポートするために、API125、130の拡大または拡張を可能にする。拡大されたアクセス制御権は、ソーシャル・グラフの現在の状態に応じてアクセスを許可するために使用することができる。たとえば、選択されたリソースへのアクセスは、選択されたリソースとの関係またはリソースの所有者との関係に応じて、ユーザまたは加入者に条件付きで

許可することができる。一実施形態では、新しいサービスまたはアプリケーションによって必要な可能性がある R E S T f u l ウェブ・サービスに対するアクセス制御の粒度を予想する試みの代わりに、アプリケーション開発者は、適切に規定されたクエリ表現を使用して、アクセス制御をカスタマイズすることができる場合がある。

#### 【0022】

アクセス制御クエリの様々な実施形態は、論理式を使用して規定することができ、異なる値を返すことができる。一実施形態では、開発者は、ユーザがウェブ・サービス・リソースにアクセスできるかどうかを決定するために、ウェブ・サービス・リソースに対して適用できるブール値（真／偽）のクエリ表現を選択または指定することができる。開発者は、ユーザのアクセス制御状態を示すために使用できる他のパラメータを返すクエリ表現を代わりに選択または指定することができる。たとえば、関係するリソースにユーザが以前にアクセスした回数を示すカウンタ値を返すクエリ表現が、ウェブ・サービス・リソースへのアクセスがユーザに与えられるかどうかを決定するために使用される。より複雑なクエリを規定することもできる。たとえば、アクセス制御を許可するクエリ表現は、ブール（真または偽）結果を提供するために、論理演算子（たとえば「AND」、「OR」、または「NOT」）または数学的な比較演算子（<、<=、>+、==、!=）を用いてクエリの結果を組み合わせる論理式を返すクエリの場合がある。他の例では、真／偽結果を提供するために、1つまたは複数のクエリの「結果の組」の行および列で動作する、たとえば J a v a S c r i p t で表現された、動的な言語の機能を提供することができる。したがって、たとえば、2つのクエリを含むアクセス制御クエリ表現は、以下の形式の場合がある。

```
" ( 0 < ( S E L E C T   c o u n t   f r o m   f r i e n d s _ t a b l e   w h e r e . . . ) ) A N D ( 6 <
      ( S E L E C T   c o u n t   f r o m   p h o t o s _ t a b l e   w h e r e . . . ) ) "
```

あるいは、J a v a S c r i p t 機能を用いて、クエリ表現は、以下の形式の場合がある。

```
" f u n c t i o n   h a s R e q u e s t e d A c c e s s ( R e q u e s t _ U R I ) {
    v a r   r s = d b . e x e c u t e ( ' s e l e c t   f r i e n d   f r o m
    f r i e n d s _ t a b l e   w h e r e . . . ' ) ;
    w h i l e ( r s . i s V a l i d R o w ( ) ) {
        . . .
    }
    r e t u r n   i s A c c e s s G r a n t e d ;
} "
```

本開示の恩恵を受ける当業者は、前述の代表的なクエリは、説明を意図していることを理解されたい。アクセス制御クエリの代替実施形態は、これらの形式、他のクエリ形式、またはその組み合わせを使用することができる。

#### 【0023】

クエリ表現は、R E S T f u l 動作（G E T、P U T / P O S T、D E L E T E）に関連する場合があり、ウェブ・サービス要求に対するアクセスが許可されるかどうかを決定することができる。クエリ表現は、S Q L、S P A R Q L、またはX P a t hを含む任意のクエリ言語で実装することができる。クエリ表現は、ターゲット・リソースに直接的に関連している場合があり、または多数のリソースに対して適用し、単一の操作でその一部またはすべてを無効化または修正できる追加のリソースとして、ウェブ・サービスに代わりに追加することができる。クエリ表現によって許可された権限の性質を提案または記述する名前または記述は、クエリ表現に関連する場合がある。クエリ表現がウェブ・サービスに拡張として追加される場合、R E S T f u l P U T / P O S T、G E T、およびD E L E T E 操作を通じてクエリ表現を確立、読み込み、削除するために使用されるU R I

でリソース名の要素として名前を使用することができる。

#### 【0024】

図示する実施形態では、ユーザ105は、ソーシャル・ネットワーク・サービス110、115の1つまたは複数にリソースを投稿することができる。投稿されたリソースに条件付きアクセスを提供することができるサービス呼び出すことができる。たとえば、ユーザ105(4)は、Facebookにグループ写真を投稿し、次に写真に載っているユーザ105(4)に対してユーザが持つことができる他の関係に関係なく、写真でタグが付けられたユーザへのアクセスを条件付きで許可するためにグループ写真に関連するノードにクエリをアタッチするサービス呼び出す。ユーザ105(1)がユーザ105(4)のFacebook友達の場合、ユーザ105(1)は、写真に関してコメントすることができ、ユーザ105(2)は、ユーザ105(4)のFacebook友達ではないかもしれないが、サービスは、ユーザ105(2)への条件付きアクセスを許可するためにクエリを使用できるため、ユーザ105(2)が写真でタグを付けられていれば、ユーザ105(2)は写真に関してコメントすることができる。ユーザ105(3)は、ユーザ105(4)のFacebook友達でない場合があり、写真でタグを付けられていない場合がある。したがって、クエリは、ユーザ105(3)へのアクセスを許可しない。

10

#### 【0025】

通信システム100の実施形態は、新しい葉ノードがアタッチされたノードによって表されるデータの新しい「ビュー」を表す葉ノードを追加することによって、適切な権限を持つ開発者120がリソース・ツリーを拡張することを可能にすることができる。これらのノードは、開発者120によって指定し、新しい葉ノードが挿入されるツリーの枝によって識別されるデータ・サブセット(またはサブツリー)で動作する1つまたは複数のアクセス制御クエリに関連する場合がある。ノードまたはクエリは、オフラインのウェブ・インターフェースを通じて追加するか、またはHTTP POST要求を通じて挿入することができる。クエリ/ビューは、開発者120によって指定または規定することも、またはクエリ/ビューは、ソーシャル・ネットワーク・サービス110、115のプロバイダから利用可能な事前規定された「クエリ/ビュー」のメニューから選択することもできる。様々な代替の実施形態において、クエリ・パラメータは開発者によって規定する、コンテキスト/ノードによって決定する、またはサービスもしくはアプリケーションによって動的に決定することができる。

20

30

network.com/Joe.Subscriber/Photographs

#### 【0026】

図2は、ソーシャル・グラフ200の一部分の第1の代表的な実施形態を概念的に示す図である。図示する実施形態では、部分200は、完全なソーシャル・グラフのサブツリーであり、サブツリー200は、特定の加入者「Joe Subscriber(加入者ジョー)」に関連するノードを含む。部分200は、入り口ノードまたは親ノードの205を介してアクセスすることができる。部分200は、1つまたは複数のサーバに格納することができ、クライアントは適切なユニフォーム・リソース・インジケータ(URI)または他のアドレスをサーバに送信することによって、入り口ノード205にアクセスすることができる。たとえば、入り口ノード205は、URIアドレスhttp://www.fakesocialnetwork.com/Joe.Subscriberを送信することによってアクセスすることができる。部分200は、また、入り口ノード205または部分200内の他のノードに接続された子ノード210を含む。子ノード210は、情報、カテゴリ、他の加入者などに関連する場合がある。たとえば、子ノード210は、「友達」「写真」「プロフィール」「音楽」などに関連する場合がある。ノード200は、また、家族、親しい友達、知人、職業上の連絡先などユーザ/加入者の間の関係の性質を示す関心事またはグループを共有する加入者またはユーザのグループと関連する場合がある。ノード210は、以下のような対応するアドレスを使用してアクセスすることができる。

40

50

`http://www.fakesocialnetwork.com/Joe.Subscriber/FriendsLists/CloseFriends`、および  
`http://www.fakesocialnetwork.com/Joe.Subscriber/Photographs`  
【0027】

図示する実施形態では、開発者または他のサード・パーティは、加入者に対応するソーシャル・グラフの部分200のノード210に1つまたは複数のアクセス制御クエリ215をアタッチすることができる。アクセス制御クエリ215は、写真または他のリソースなど、ノード210(1)に関連するリソース220に対して動作することができる。一実施形態では、開発者は、クエリ215を規定するためにメッセージまたはコマンドを使用し、ソーシャル・グラフ200へのアプリケーション・プログラミング・インターフェース(API)を修正するために1つまたは複数のノードにクエリ215をアタッチすることができる。たとえば、クエリ215は、ノード210(1)に関連するリソース220に対するアクセス制御を修正するために、Joe Subscriberがクエリ215を利用するサービスを呼び出すことに応答して、ノード210(1)(たとえばPhotographsノード)にアタッチすることができる。クエリを呼び出すアドレスの一例は以下のとおりである。

`http://www.fakesocialnetwork.com/Joe.Subscriber/Photographs/Photo1/Tagged_User`  
これにより、Photographsノード210(1)にアタッチされたクエリ215を呼び出す。クエリ215に示されたユーザがPhoto1でタグを付けられている場合、クエリ215はブール値真を返すことができるため、それによって、たとえば、写真に関してコメントするためにリソースへのアクセスをユーザに許可する。そうでない場合、クエリ215は、アクセスに対する要求が拒否されたことを示すためにブール値偽を返すことができる。たとえば、写真Photo1は、Frank FriendlyおよびBob Whatsisnameに対するタグを含むことができる。タグは、タグ・リスト225に、または他の指標を使用して示すことができる。タグ・リスト225の「Y」によって示すように、Frank FriendlyはJoe Subscriberの友達であり、タグ・リスト225の「N」によって示すように、Bob WhatsisnameはJoe Subscriberの友達ではない。しかし、Bob Whatsisnameは写真Photo1でタグを付けられているため、クエリ215は、写真Photo1への条件付きアクセス権をBob Whatsisnameに許可することができる。

【0028】

従来のクエリ言語の実施形態は、典型的には、ソーシャル・グラフ200内の異なる位置またはノードで適用できる単一のクエリを設計できるように十分に柔軟な場合がある。ノードは、開発者によって各クエリ215に対して選択することができるか、またはノードは、自動化された手順またはアルゴリズムを使用して選択することができる。たとえば、ソーシャル・ネットワーキング・サイトは、クエリ215を検査し、クエリ215を適用するべき適切なノードを選択し、ツリーにおいて選択されたノードにクエリ215を反復的に(または同時に)適用し、結果を組み合わせることができる。一部の実施形態では、開発者またはサード・パーティは、ソーシャル・グラフ200にクエリ215をアタッチする権限または承認を取得する必要がある場合がある。たとえば、開発者またはサード・パーティは、Joe Subscriberまたはソーシャル・グラフのサービス・プロバイダもしくは所有者から権限または承認を取得する必要がある場合がある。承認は、たとえば、加入者がクエリ215を利用するアプリケーションまたはサービスを呼び出したか、または開始した後、加入者がアプリケーションまたはサービスを終了するまでなど、制限された時間のみ有効な場合がある。したがって、クエリ215は、一時的または動的なクエリの場合がある。

【0029】

10

20

30

40

50

図3は、ソーシャル・グラフに対するアクセス制御を修正するための方法300の第1の代表的な実施形態を概念的に示している。図示する実施形態では、アクセス制御クエリは、開発者またはサード・パーティによって生成される(305)。アクセス制御クエリは、開発者またはサード・パーティによって作成されたサービスまたはアプリケーションの一部として使用することができる。アクセス制御クエリは、開発者またはサード・パーティによって規定されたノードのサブツリーで動作することができ、たとえば、クエリを利用するサービスを呼び出した加入者など、1人または複数のユーザに関連するソーシャル・グラフの一部分に挿入されることが意図される。次に、開発者またはサード・パーティは、1つまたは複数の指定されたノードにクエリをアタッチするために、要求を送信することができる(310)。たとえば、クエリ表現は、ソーシャル・グラフのリソースに対するアクセス制御の修正を要求するREST - full POST要求として書き込むことができる。

#### 【0030】

従来のアクセス制御方式では、REST - fullサービスのユーザは、サービスにアクセス・トークンを提示し(または、アプリケーションがエンド・ユーザに代わってアクセス・トークンを提示する)、アクセス・トークンは、ユーザ/アプリケーションに許可されたアクセスを識別する。サービスの事前に定められたリソースは、どのアクセス権が特定のユーザに許可されるかを指定することができる。たとえば、Googleカレンダーでは、ユーザは、そのユーザに対するアクセス権を決定する役割を割り当てることができる。所与のリソースについて(たとえば、Google: "/calendar/v3/calendars/KidsEvents")、役割は、(HTTP GET要求を通じて)ユーザがリソースへのアクセス権を持っているかどうか、(HTTP PUT要求を通じて)カレンダーを更新することができるかどうか、または(HTTP DELETE要求を通じて)カレンダーを削除することができるかどうかを決定する。役割は、役割に対して事前規定されたアクセス権の集合を許可する。事前に定めた役割は、サービス・プロバイダによって固定され、ユーザ、開発者、またはサード・パーティによって拡張することはできない。

#### 【0031】

図示する実施形態では、要求された(305)アクセス制御クエリは、リソースへの個々のアクセス権を許可するために使用することができるため、それによって役割ベースのアクセス制御を回避することができる。あるいは、ユーザは、アクセス・トークンを通じてユーザに許可されたアクセスを無効(または強化)できる、要求された(305)アクセス制御クエリの結果に基づいて、特定の役割に関連する場合がある。アクセス制御クエリは、リソース・ツリーのノードにアタッチされ、クエリ・ノードの配置により、役割の範囲を決定することができる。たとえば、クエリ範囲は、クエリがアタッチされているサブツリーのリソースに制限することができる。クエリ・ノードには、意味のある名前を付けることができる。たとえば、子どものイベントを記載する加入者のカレンダーに養護者(caregiver)アクセス権を与えるべきかどうかを決定するクエリのためのクエリ・ノードは、「GrantCaregiversAccess」という名前を付けることができ、関連するURIを使用して交換または削除することができる。

http://www.fakesocialnetwork.com/Joe.Subscriber/Calendar/Calendars/KidsEvents/GrantCaregiversAccess

適切な承認を用いて、Googleのカレンダーのようなサービスに対するクエリを作成するために使用されるPOST要求は、(JSON)形式を使用することができる。

POST/calendar/calendars HTTP/1.1

Content-Type: application/json

Content-length: 200

...

{

10

20

30

40

50

```

    "kind": "calendar#calendarAccessControl
    Query",
    "id": "GrantCaregiversAccess",
    "accessRole": "reader".
    "query": "SELECT..."
  }

```

あるいは、POST要求は、GETコマンドを介して特定の権利を許可するために以下の形式を使用することができる。

```

POST/calendar/calendars/HTTP/1.1
Content-Type: application/json
Content-Length: 203
...
{
  "kind": "calendar#calendarAccessControl
  Query",
  "id": "GrantCaregiversAccess",
  "accessRights": "GET".
  "query": "SELECT..."
}

```

アクセス制御クエリを削除するために、アプリケーションまたはエンド・ユーザは、以下のようなHTTP要求を発行することができる。

```

DELETE/calendar/calendars/GrantCaregive
rsAccess HTTP/1.1

```

様々な代替の実施形態において、1つまたは複数のアクセス制御クエリは、所与のノードに[アタッチ](#)することができるが、実際には、ユーザは、そのユーザに対して少数の高い値(high value)を用いることを選択することができる。一部の実施形態では、シャドー・ノードまたはパターン一致は、クエリを作ったユーザに制御されないノードにクエリを関連させるために使用することができる。

#### 【0032】

他の例では、Facebookのようなサービスのコンテキストでは、クエリは、アルバム、またはクエリの設計に基づいてアルバムの個々の写真へのアクセスを許可または拒否するために使用することができる。サービスは、クエリへのパラメータに基づいて、アルバムもしくはそれが[アタッチ](#)されているアルバムのリスト、またはアルバム内の個々の写真またはそれが[アタッチ](#)されているアルバムのリストへのクエリがアクセスを許可するかどうかを決定することができる。

```

POST/Joe.Subscriber/ElizabethHighSchool
Graduation/photos HTTP/1.1
Content-Type: application/json
Content-Length: 203
...
{

```

```

  "kind": "AccessControlQuery",
  "id": "GrantElizabethFriendsAccess",
  "accessRights": "GET".
  "query": "SELECT..."
}

```

Facebookの写真はそれぞれ多数の「プロパティ」を持つことができ、これらはアクセスをさらに制限するためにクエリに現れる場合がある。たとえば、「タグ」プロパティは、写真に描写された個人を記載し、特定のユーザが描写されているこれらの写真のみへのアクセスを制限するために使用することができる。

## 【 0 0 3 3 】

図示する実施形態では、アクセス制御クエリをアタッチする要求は、ユーザ/加入者から承認を必要とする場合がある。ユーザ承認プロセスは、ユーザのソーシャル・グラフの1つまたは複数のノードにアクセス制御クエリをアタッチすることをユーザが承認したことを検証するために実行することができる(315)。ユーザ承認は、様々な技術を使用して実行することができる。たとえば、クエリを挿入する要求は、新しいクエリの実装を承認または許可するかをユーザが示すことを許可(315)する認証/承認プロセスを開始する要求を含むことができる。ユーザが確認または認証を提供しなければ、要求は拒否される(320)。加入者が要求を確認または認証すれば、要求を続行することができる。

10

## 【 0 0 3 4 】

図示する実施形態では、要求は、また、ソーシャル・ネットワーク(SN)サービスのプロバイダまたは所有者から承認を必要とする場合がある。プロバイダ承認プロセスは、ユーザのソーシャル・グラフに新しいクエリを挿入することをプロバイダ/所有者が承認したことを検証するために実行することができる(325)。プロバイダ承認は、様々な技術を使用して実行することができる。たとえば、アクセス制御クエリをアタッチする要求は、新しいクエリの実装を承認または許可するかをプロバイダが示すことを許可(315)する認証/承認プロセスを開始する要求を含むことができる。一実施形態では、プロバイダは、要求を調査し、プロバイダによって確立されたセキュリティ、プライバシー、または他のポリシーに要求が準拠しているかどうかを決定する自動化されたシステムを使用して、認証/承認プロセスを実行することができる。ウェブ・サービスに設置する前に、クエリは、ウェブ・サービスのセキュリティ/使用法のポリシーにそれが準拠していることを保証するために機械的に検証することができる。たとえば、ウェブ・サービスは、ブール結果を返すクエリのみを許可することができ、アクセス制御クエリが関連付けられ得るノードのタイプを限定することができる(たとえば「Photographs」ノードのみ)。プロバイダが確認または認証を提供しなければ、要求は拒否される(320)。プロバイダが要求を確認または認証すれば、要求を続行することができる。本開示の恩恵を受ける当業者は、図3に示した特定の認証シーケンスは、説明を意図したものであることを理解されたい。代替実施形態は、同時または図3に示したものと異なる順序で、ユーザおよびプロバイダの認証プロセスを実行することができる。さらに、他の代替実施形態は、両方ではなく、ユーザ認証またはプロバイダ認証のみを実行することができるか、または認証をまったく実行しない場合がある。

20

30

## 【 0 0 3 5 】

要求が承認されたら、要求されたクエリは、ソーシャル・グラフ内の選択された位置にアタッチすることができる(330)。次に、開発者もしくはサード・パーティ、または他のエンティティは、新しいクエリを利用するアプリケーションまたはサービスを可能にするために、修正されたインターフェースを使用することができる場合がある。たとえば、上に記述したPOST要求の結果として、加入者(Joe Subscriber)に対するAPIを拡張することになる場合があるため、ここで、URIに対してGET要求を行うことができる。

40

`http://www.fakesocialnetwork.com/Joe.Subscriber/Photographs/Photo1`  
要求されたりソース(つまり写真Photo1)へのアクセス制御は、以下のようなクエリを使用して決定することができる。

`http://www.fakesocialnetwork.com/Joe.Subscriber/Photographs/AllowAccessforTaggedUser`

アクセス制御クエリは、Bob What'sisnameが写真Photo1に対するタグ・リストにあるかどうかに応じてブール値を返す。一実施形態では、アクセス制御クエリを開発者は見ることができ、アクセス制御クエリを使用するアプリケーションに利用可

50

能であるが、アクセス制御クエリはユーザには見えない場合があるため、リソースへのアクセスを得ることを試みるユーザは、アクセス制御が実行されていることに気づかない場合がある。

#### 【0036】

したがって、方法300の実施形態は、ソーシャル・グラフを表す基礎をなすデータベースへの過度または完全なアクセスを提供するリスクを減らしながら、より広くより様々な組のアクセス制御権を提供する、修正されたインターフェースをサポートすることができる。POST要求によって行われた修正は、要求を承認したユーザのみに影響することができ(Joe Subscriber)、対応するHTTP DELETE要求または他の操作によって逆転することができる。一実施形態では、クエリを挿入するためのメカニズムは、エンド・ユーザに関連するレコードを作成することの場合がある。挿入されたレコードは、GET要求で使用されるクエリおよび関連する経路を含むことができる。様々な実施形態において、ウェブ・サービスは、1つまたは複数のクエリ言語をサポートし、クエリ言語に伴うスキーマを公開する。

#### 【0037】

図4は、ソーシャル・グラフへの修正されたアプリケーション・プログラミング・インターフェースにクエリする方法400の代表的な一実施形態を概念的に示している。図示する実施形態では、方法400は、ユーザごとおよびアプリケーションごとにアプリケーション・プログラミング・インターフェースを修正するため、インターフェースによって使用されるアクセス制御権は、いつでも全体的に変更されるのではなく、修正されたインターフェースを使用するサービスを特定のユーザが呼び出した場合のみ変更され、一部の実施形態では、関係するサービスを呼び出し、ソーシャル・グラフの関連する部分へのインターフェースの修正を承認したユーザに対してのみである。1人または複数のユーザは、サービスまたはアプリケーションを開始することができる(405)。開始されたアプリケーションは、プロバイダによって規定されたAPIによってサポートされないアクセス制御クエリを利用することができる。次に、1つまたは複数の新しいアクセス制御クエリを作成することができ、また、アクセス制御クエリを関連するノードにアタッチすることができる(410)。クエリをアタッチするための技術の実施形態については図3に示している。

#### 【0038】

次に、(たとえば、サービス・プロバイダによって所有または運用される1つまたは複数のサーバで実装されたソフトウェア、ファームウェア、またはハードウェアを使用する)サービス・プロバイダは、サービスに関連するクエリを監視することができる(410)。サービス・プロバイダがクエリを検出しないうり、監視を継続することができる(410)。サービス・プロバイダが、アクセス制御クエリ、たとえば、加入者によって要求または呼び出されたサービスの一部としてソーシャル・グラフへのアクセスを要求するために実行されるクエリを検出すると(415)、クエリに関連するノードのサブツリーに含まれる情報に対してクエリを実行することができる(420)。たとえば、クエリは、ノードのサブツリーに含まれる情報に少なくとも部分的に基づいて、アクセス要求が許可されたか拒否されたかを示すブール値を返すことができる(420)。

#### 【0039】

図5は、ソーシャル・グラフへのアプリケーション・プログラミング・インターフェースへの修正を取り除くか、または逆転する方法500の代表的な一実施形態を概念的に示している。図示する実施形態では、アプリケーション・プログラミング・インターフェースは、1人または複数のユーザが、修正されたインターフェースを使用するサービスを呼び出すことに応答して、ユーザごとまたはアプリケーションごとに(たとえば図3~図4に関して本明細書に記述したように)以前に修正されており、一部の実施形態では、関係するサービスを呼び出し、ソーシャル・グラフの関連する部分へのインターフェースの修正を承認したユーザに対してのみである。ソーシャル・グラフへのインターフェースを修正する結果となった、サービスを以前に開始した1人または複数のユーザは、アプリケー

ションを終了すると決定することができる。したがって、サービス・プロバイダは、アプリケーションを終了する要求を受信することができる(505)。サービス・プロバイダは、修正されたインターフェースをサポートするために、ソーシャル・グラフにアタッチされた一時的アクセス制御クエリを識別することができる(510)。一時的クエリの識別(510)は、サービス・プロバイダによって格納された情報またはユーザによって提供された情報を使用して実行することができる。次に、一時的クエリは削除することができる(515)、アプリケーションを終了することができる(520)。一実施形態では、一時的クエリの削除(515)は、ノード、葉ノード、サブツリー、または一時的クエリに関連する他の情報を取り除くことを含むことができる。

#### 【0040】

図6は、ソーシャル・グラフ600の一部分の第2の代表的な実施形態を概念的に示している。図2に示す第1の実施形態と同様に、部分600は、特定の加入者「Joe Subscriber」に関連するノードを含む完全なソーシャル・グラフのサブツリーである。部分600は、入り口ノードまたは親ノード605を介してアクセスすることができる。部分600は、1つまたは複数のサーバに格納することができ、クライアントは、適切なユニフォーム・リソース・インジケータ(URI)または他のアドレスを使用して、入り口ノード605にアクセスすることができる。部分600は、また、入り口ノード605または部分600内の他のノードに接続されている子ノード610を含む。本明細書に記述したように、子ノード610は、情報、カテゴリ、他の加入者などに関連する場合があります。ノード610は、以下のような対応するアドレスを使用してアクセスすることができる。

`http://www.fakesocialnetwork.com/Joe.Subscriber/Calendar`

#### 【0041】

図示する実施形態では、開発者または他のサード・パーティは、加入者に対応するソーシャル・グラフの部分600に1つまたは複数のノード615を追加することができる。たとえば、開発者は、サブツリー600のノード610(4)に関連する、またはアタッチされたノード615を挿入するためにHTTP POSTコマンドを使用することができる。次に、ノード615は、適切なURIまたは他のアドレスを使用してアクセスすることができる。たとえば、ノード610(3)は、Joe Subscriberの「Calendar(カレンダー)」に関連する場合があります、ノード610(4)は、Joe Subscriberの「Calendars(カレンダー)」に関連する場合があります、ノード615は、「KidEvents(子どものイベント)」などJoeの子どもが参加するイベントを含むカテゴリに関連する場合があります。ノード615は、また、バレエ・レッスン、サッカーの練習、ピアノ・リサイタルなど、複数の葉ノード625を含む、他のサブツリー620に関連付ける、または接続することができる。しかし、本開示の恩恵を受ける当業者は、サブツリー620は、ノードまたは葉ノードの異なる組み合わせを含むことができることを理解されたい。サブツリー620または葉ノード625は、開発者、サード・パーティ、加入者、またはサービス・プロバイダによって自動的にポピュレートすることができる。ノード615は、以下のようなアドレスを使用してアクセスすることができる。

`http://www.fakesocialnetwork.com/Joe.Subscriber/Calendar/Calendars/KidEvents`

一部の実施形態では、開発者またはサード・パーティは、ソーシャル・グラフにノード615を追加する権限または承認を取得する必要がある場合がある。たとえば、開発者またはサード・パーティは、Joe Subscriberまたはソーシャル・グラフのサービス・プロバイダもしくは所有者から権限または承認を取得する必要がある場合がある。承認は、たとえば、加入者がノード615を利用するアプリケーションまたはサービスを呼び出したか、または開始した後、加入者がアプリケーションまたはサービスを終了するまでなど、制限された時間のみ有効な場合がある。したがって、ノード615は、一時的

10

20

30

40

50

または動的なノードの場合がある。

#### 【0042】

ソーシャル・グラフ600へのインターフェースは、ソーシャル・グラフ600に追加されたノード615で動作するアクセス制御クエリ630をサポートするように修正することができる。一実施形態では、開発者は、アクセス制御クエリ630を規定するためにメッセージまたはコマンドを使用し、ソーシャル・グラフ200へのアプリケーション・プログラミング・インターフェース（API）を修正するために1つまたは複数のノードにクエリ630をアタッチすることができる。たとえば、子どものイベント「Kids Events」のためのノード615を作成し、子どものイベントを記載する加入者のカレンダーへのアクセス権を養護者に与えるべきかどうかを決定するクエリにアタッチすることができ、これは「GrantCaregiversAccess」という名前を付けることができ、関連するURIを使用して交換または削除することができる。

10

```
http://www.fakesocialnetwork.com/Joe.Subscriber/Calendar/Calendars/KidsEvents/GrantCaregiversAccess
```

適切な承認を用いて、Googleのカレンダーのようなサービスに対するクエリを作成するために使用されるPOST要求は、（JSON）形式を使用することができる。

```
POST/calendar/calendars HTTP/1.1
```

```
Content-Type: application/json
```

```
Content-length: 200
```

20

```
...
{
  "kind": "calendar#calendarAccessControlQuery",
  "id": "GrantCaregiversAccess",
  "accessRole": "reader",
  "query": "SELECT..."
}
```

しかし、代替実施形態では、他の形式の他のアドレスまたは要求メッセージは、ノード615またはアクセス制御クエリ630を作成するために使用することができる。

30

#### 【0043】

図7は、ソーシャル・グラフに対するアクセス制御を修正するための方法700の第2の代表的な実施形態を概念的に示している。図示する実施形態では、本明細書に記述するように、アクセス制御クエリは、開発者またはサード・パーティによって生成される（705）。アクセス制御クエリは、開発者またはサード・パーティによって作成されたサービスまたはアプリケーションの一部として使用することができる。アクセス制御クエリは、開発者またはサード・パーティによって規定されたノードのサブツリーで動作することができ、たとえば、クエリを利用するサービスを呼び出した加入者など、1人または複数のユーザに関連するソーシャル・グラフの一部分に挿入されることが意図される。次に、開発者またはサード・パーティは、ノードを作成し、新しく作成されたノードにアクセス制御クエリをアタッチするために、要求を送信することができる（710）。たとえば、クエリ表現は、ソーシャル・グラフへのAPIのプログラマのビューの修正を要求するREST-full POST要求として書き込むことができる。適切な承認を用いて、APIを拡張するためのURI

40

```
http://www.fakesocialnetwork.com/Joe.Subscriber/Calendar/Calendars/
```

へのPOST要求は、以下のように書くことができる。

```
POST/Joe.Subscriber/Calendar/Calendars/ HTTP/1.0
```

```
Content-Type: text/xml
```

50

```

< extend >
  < node > KidEvents < / node >
  < query > SELECT . . . < / query >
< / extend >

```

しかし、本開示の恩恵を受ける当業者は、他のクエリ表現または形式を要求に使用することができることを理解されたい。

#### 【0044】

図示する実施形態では、要求は、ユーザ/加入者からの承認を必要とする場合がある。ユーザ承認プロセスは、ユーザのソーシャル・グラフに新しいノードを挿入することをユーザが承認したことを検証するために実行することができる(715)。ユーザ承認は、様々な技術を使用して実行することができる。たとえば、ノードを作成し、クエリをアタッチする要求は、新しいノードの作成および新しいクエリの実装を承認または許可するかをユーザが示すことを許可(715)する認証/承認プロセスを開始する要求を含むことができる。ユーザが確認または認証を提供しなければ、要求は拒否される(720)。加入者が要求を確認または認証すれば、要求を続行することができる。

#### 【0045】

図示する実施形態では、要求は、また、ソーシャル・ネットワーク(SN)サービスのプロバイダまたは所有者から承認を必要とする場合がある。プロバイダ承認プロセスは、ユーザのソーシャル・グラフに新しいノードを挿入することをプロバイダ/所有者が承認したことを検証するために実行することができる(725)。プロバイダ承認は、様々な技術を使用して実行することができる。たとえば、ノードを作成し、クエリをアタッチする要求は、新しいノードの作成または新しいアクセス制御クエリの実装を承認または許可するかをプロバイダが示すことを許可(715)する認証/承認プロセスを開始する要求を含むことができる。一実施形態では、プロバイダは、要求を調査する自動化されたシステムを使用して、認証/承認プロセスを実行することができ、プロバイダによって確立されたセキュリティ、プライバシー、または他のポリシーに要求が準拠しているかどうかを決定する。ウェブ・サービスにインストールする前に、アクセス制御クエリは、ウェブ・サービスのセキュリティ/使用法のポリシーにそれが準拠していることを保証するために機械的に検証することができる。プロバイダが確認または認証を提供しなければ、要求は拒否される(720)。プロバイダが要求を確認または認証すれば、要求を続行することができる。本開示の恩恵を受ける当業者は、図7に示した特定の認証シーケンスは、説明を意図したものであることを理解されたい。代替実施形態は、同時または図7に示したものと異なる順序で、ユーザおよびプロバイダの認証プロセスを実行することができる。さらに、他の代替実施形態は、両方ではなく、ユーザ認証またはプロバイダ認証のみを実行することができるか、または認証をまったく実行しない場合がある。

#### 【0046】

要求が承認されたら、要求されたノードは、ソーシャル・グラフ内の選択された位置に挿入することができる(730)。次に、ソーシャル・グラフへのインターフェースは、新しいノードまたはツリー内のより低いノードにアクセス制御クエリをアタッチする(735)ことによって修正することができる。開発者もしくはサード・パーティ、または他のエンティティは、次に、新しいアクセス制御クエリを利用するアプリケーションまたはサービスを開発できる場合がある。たとえば、カレンダーKidEventsに関連するアクセス制御クエリは、以下のURIを使用して呼び出すことができる。

```

http://www.fakesocialnetwork.com/Joe.Subscriber/Calendar/Calendars/KidEvents/GrantCaregiversAccess

```

図示する実施形態では、承認された養護者から要求が来る場合、要求はブール値真を返し、承認された養護者から要求が来ない場合、ブール値偽を返す。したがって、方法700の実施形態は、ソーシャル・グラフを表す基礎をなすデータベースへの過度または完全なアクセスを提供するリスクを減らしながら、より広くより様々な組のアクセス制御権を提

10

20

30

40

50

供することができる。POST 要求によって行われた修正は、ユーザのリソース、または要求を承認したユーザ (Joe Subscriber) にアクセス可能なそれらのリソースへのアクセスのみに影響する場合があります、対応する HTTP DELETE 要求または他の操作によって逆転することができる。一実施形態では、クエリを挿入するためのメカニズムは、エンド・ユーザに関連するレコードを作成することの場合がある。挿入されたレコードは、GET 要求で使用するクエリおよび関連する経路を含むことができる。様々な実施形態において、ウェブ・サービスは、1 つまたはクエリ言語をサポートし、クエリ言語に伴うスキーマを公開する。一実施形態では、新しいノードまたは アタッチ されるクエリは、一時的な場合がある。たとえば、ノードまたはクエリは、ユーザが、ノードまたはクエリを利用するサービスを呼び出すことに応答して追加することができる。ノードまたはクエリは、たとえば、ノードまたはクエリを使用するサービスの終了に応答して、除去または削除することができる。

#### 【0047】

図 8 は、ソーシャル・グラフの部分を格納する、ソーシャル・グラフへのアプリケーション・プログラミング・インターフェースを実装する、またはソーシャル・ネットワーク・サービスを実装するために使用できる、サーバ 800 の代表的な一実施形態を概念的に示している。図示する実施形態では、サーバ 800 は、プロセッサ 805、データ記憶装置 810、および入力/出力 (I/O) インターフェース 815 を含む。プロセッサ 805 は、たとえば、データ記憶装置 810 または他の場所に格納されたデータまたは命令を使用するなど、サーバ 800 の動作を制御するように構成される。サーバ 800 によって実行できる動作の実施形態は、図 1 ~ 図 7 に関連して本明細書に記述している。一実施形態では、データ記憶装置 810 は、ソーシャル・グラフへの 1 つまたは複数のアプリケーション・プログラミング・インターフェースを表す情報 820、ソーシャル・グラフの部分を表す情報 825、またはソーシャル・グラフに格納された情報を使用できるソーシャル・ネットワーク・サービスを表す情報 830 を格納する。

#### 【0048】

図 8 は単一のサーバ 800 を示しているが、本開示の恩恵を受ける当業者は、代替実施形態は、複数のサーバを使用し、複数のサーバの全体にわたり図 8 に示した機能の部分を分散することができることを理解されたい。一部の実施形態では、サーバ 800 はバーチャル・マシンの場合がある。これらの実施形態の一部では、バーチャル・マシンは、異なるマシンからのコンポーネントを含む場合も、または地理的に分散している場合もある。たとえば、データ記憶装置 810 およびプロセッサ 805 は、2 台の異なる物理的なマシンにある場合がある。ソーシャル・ネットワーク・サービス 830 など、プロセッサで実行可能なプログラムがプロセッサ 805 で実装される場合、特定の論理回路と同様に動作する一意のデバイスを提供するために、プログラム・コード・セグメントはプロセッサ 805 と組み合わせられる。

#### 【0049】

開示した内容および対応する詳細な記述の部分は、ソフトウェア、またはアルゴリズムおよびコンピュータ・メモリ内のデータ・ビットの動作を記号で表現したものに関して示したものである。これらの記述および表現は、当業者が他の当業者に仕事の本質を効果的に伝達するものである。本明細書で使用し、一般的に使用されるアルゴリズムという用語は、望ましい結果につながる首尾一貫した連続したステップであると考えられる。ステップは、物理量の物理的な操作を必要とするものである。通常、必須ではないが、これらの量は、格納、転送、組み合わせ、比較、または操作可能な光学的、電気的、または磁気的な信号の形をとる。これらの信号は、主に一般的に使用する理由から、ビット、値、要素、記号、文字、用語、数値などと呼ぶことが便利であると分かっている。

#### 【0050】

しかし、これらおよび同様の用語はすべて、適切な物理量に関連しており、これらの量に適用される便利なラベルにすぎないことを覚えておくべきである。特に別記しない限り、または記述から明白でない限り、「処理」または「コンピューティング」または「計算

10

20

30

40

50

」または「決定」または「表示」などの用語は、コンピュータ・システムのレジスタおよびメモリ内の物理的な電子量として表されたデータを操作し、コンピュータ・システムのメモリもしくはレジスタ、または他のそのような情報記憶装置、伝送デバイスもしくは表示デバイス内の物理量として同様に表される他のデータへと変形するコンピュータ・システム、または同様の電子計算デバイスの動作およびプロセスを指すものである。

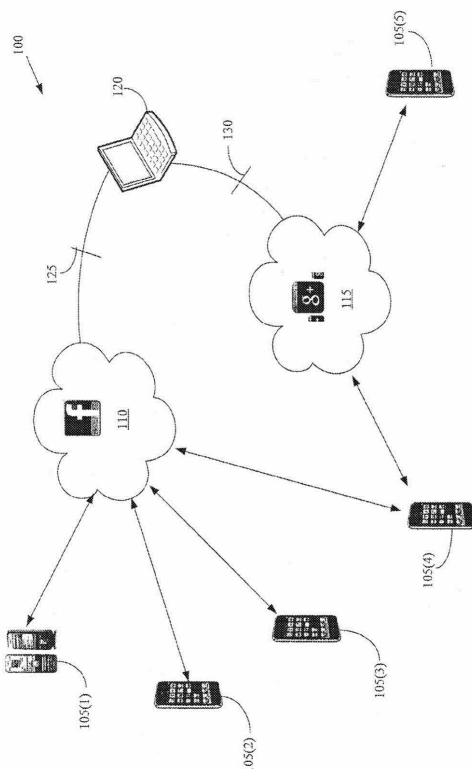
#### 【 0 0 5 1 】

また、開示された内容のソフトウェアに実装された態様は、典型的に、プログラム記憶媒体の一形式で符号化されるか、または何らかの伝送媒体を通じて実装されることに注意すること。プログラム記憶媒体は、磁氣的（たとえば、フロッピー・ディスクまたはハードドライブ）、または光学的（たとえば、コンパクト・ディスクを使った読み出し専用メモリ、または「CD ROM」）でもよく、読み出し専用またはランダム・アクセスでもよい。同様に、伝送媒体は、ツイストペア線、同軸ケーブル、光ファイバ、または当技術分野で知られている他の何らかの適切な伝送媒体でもよい。開示された内容は、特定の実装のこれらの態様によって限定されるものではない。

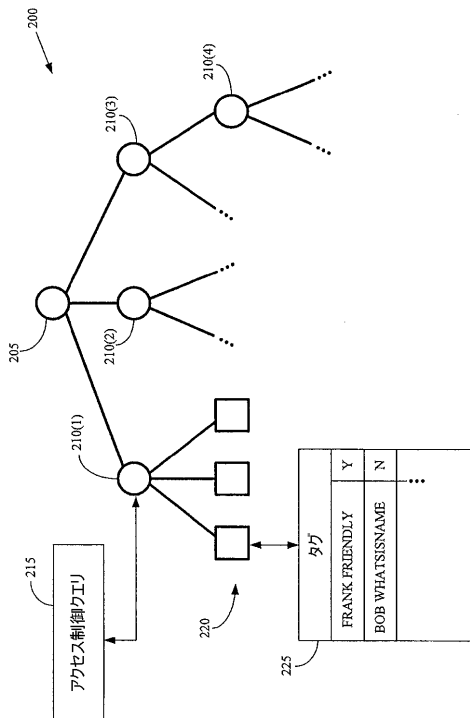
#### 【 0 0 5 2 】

上に開示した特定の実施形態は例を示しているにすぎず、開示した内容は、本明細書の教示の利益を受ける当業者に明白な、異なるが同等の方法で修正および実施することができる。さらに、以下の特許請求の範囲に記述した以外、本明細書に示した構造または設計の詳細に限定することを意図するものではない。したがって、上に開示した特定の実施形態は変更または修正することができ、そのような変形形態はすべて、開示された内容の範囲内にあると考えられることは明白である。したがって、本明細書に求められる保護は、以下の特許請求の範囲に記述するとおりである。

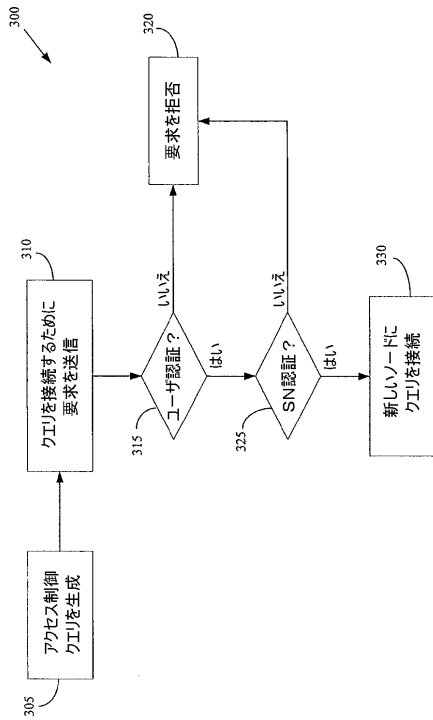
【 図 1 】



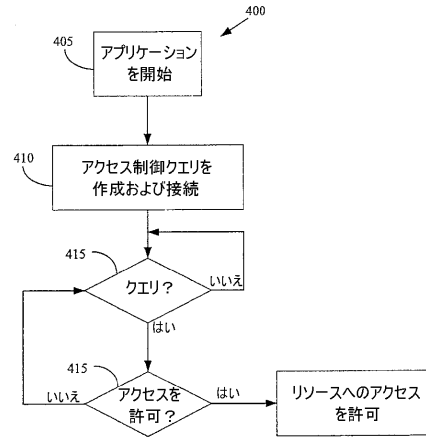
【 図 2 】



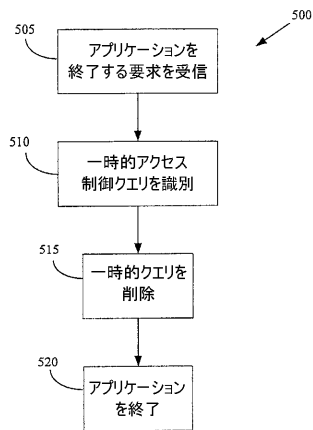
【 図 3 】



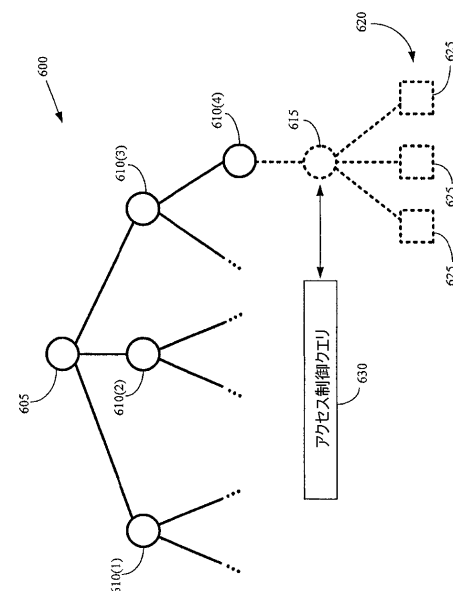
【 図 4 】



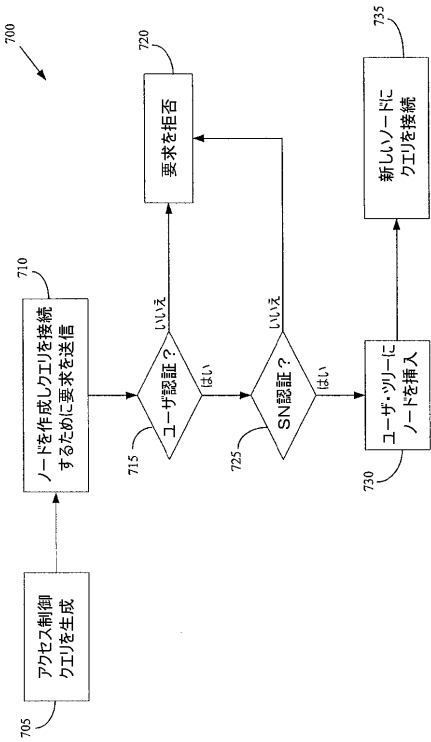
【 図 5 】



【 図 6 】



【図 7】



【図 8】

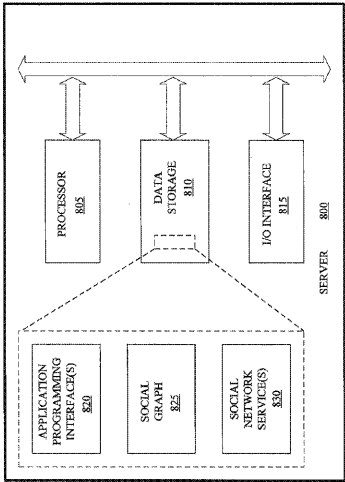


Figure 8

---

フロントページの続き

合議体

審判長 仲間 晃

審判官 辻本 泰隆

審判官 山崎 慎一

(56)参考文献 国際公開第2011/116528(WO, A1)

Bernie Hogan、A comparison of on and offline  
networks through the Facebook API、SSRN、その他  
、2008.12.01発行

(58)調査した分野(Int.Cl. , DB名)

G06F21/00-21/88