(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2018-521399
(P2018-521399A)
(43)公表日　平成30年8月2日(2018.8.2)

(51)Int.Cl.			F I			テーマコード（参考）
G06F	9/451	(2018.01)	G06F	9/451		5B376
G06F	9/455	(2006.01)	G06F	9/455	150	
G06F	9/50	(2006.01)	G06F	9/50	150Z	

審査請求 有　予備審査請求 未請求　（全 34 頁）

(21)出願番号　特願2017-563099 (P2017-563099)
(86)(22)出願日　平成28年6月23日 (2016.6.23)
(85)翻訳文提出日　平成29年12月4日 (2017.12.4)
(86)国際出願番号　PCT/US2016/039018
(87)国際公開番号　WO2016/210131
(87)国際公開日　平成28年12月29日 (2016.12.29)
(31)優先権主張番号　14/750,868
(32)優先日　平成27年6月25日 (2015.6.25)
(33)優先権主張国　米国 (US)

(71)出願人　506329306
アマゾン　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　９８１０８－１２２６
ワシントン州　シアトル　ピーオー　ボックス　８１２２６
(74)代理人　100106541
弁理士　伊藤　信和
(72)発明者　ハシミ　オマール
アメリカ合衆国　９８１０９－５２１０
ワシントン州　シアトル　テリー　アヴェニュー　ノース　４１０

最終頁に続く

(54)【発明の名称】コマンド実行に対するユーザアクセスの制御

(57)【要約】
ネットワークアクセス可能コンピューティングリソース上でコマンドを行うために、ユーザにアクセスを提供するための技術が説明される。いくつか状況では、許可は、オンラインサービスによって提供されるコンピューティングノード（複数可）上でコマンド（複数可）を実行するユーザ（複数可）に対して確立され、これは、当該提供されたコンピューティングノードにアクセスし、それを使用する、及び／または修正するユーザの能力を制御する際に使用されるそれらの提供されたコンピューティングノードへの種々の許可情報を外部で保持すること等によって行われる。インターフェースコンポーネントは、そのような外部許可情報を使用して、特定のユーザが、１つ以上の特定のコンピューティングノード上で１つ以上の特定のコマンドを実行することが承認されたかどうかを判定し、承認時、当該コンピューティングノード（複数可）上で当該コマンド（複数可）の同時実行及び独立実行を開始してもよい。当該インターフェースコンポーネントはさらに、当該ユーザに結果を提供する前に、当該コマンド（複数可）を実行した各コンピューテ

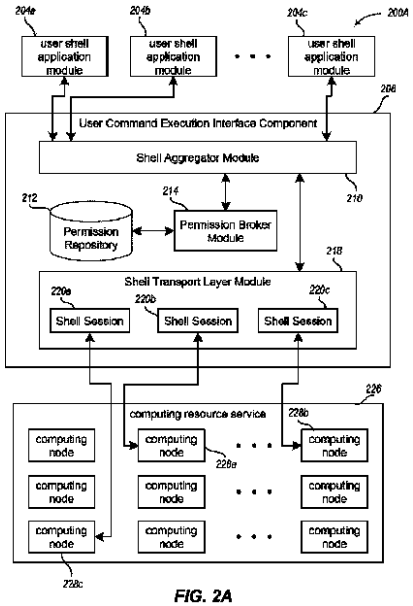


FIG. 2A

【特許請求の範囲】
【請求項１】
コンピュータ実施方法であって、
１つ以上のコンピューティングシステム上で実行するシェルアグリゲータ（ｓｈｅｌｌ　ａｇｇｒｅｇａｔｏｒ）によって、第１のユーザによる使用のためにネットワークアクセス可能サービスによって提供される１つ以上のコンピューティングノードによって実行されるコマンドを指示する前記第１のユーザから要求を受信することと、
前記シェルアグリゲータによって及び記憶済み許可情報に少なくとも部分的に基づいて、前記第１のユーザが前記コマンドを前記１つ以上のコンピューティングノードによって実行させることを承認されたことを判定することと、
前記シェルアグリゲータによって及び前記判定することに応答して、前記１つ以上のコンピューティングノードによって前記コマンドの実行を開始することと、
を含む、前記コンピュータ実施方法。
【請求項２】
前記１つ以上のコンピューティングシステムによって、前記１つ以上のコンピューティングノードによって実行される第２のコマンドを指示する前記第１のユーザから第２の要求を受信することと、
前記シェルアグリゲータによって及び前記記憶済み許可情報に少なくとも部分的に基づいて、前記第１のユーザが前記第２のコマンドを前記１つ以上のコンピューティングノードによって実行させることを承認されていないことを判定することと、
前記判定することに応答して、前記１つ以上のコンピューティングノードによる前記第２のコマンドの実行を拒否することと、
をさらに含む、請求項１に記載のコンピュータ実施方法。
【請求項３】
前記第１のユーザが承認されたことを前記判定することは、前記１つ以上のコンピューティングノードの外部の許可ブローカー（Ｐｅｒｍｉｓｓｉｏｎ　Ｂｒｏｋｅｒ）にクエリを行い、前記第１のユーザに特有の記憶済み許可情報を取得し、ならびに前記取得された記憶済み許可情報を前記コマンド及び前記１つ以上のコンピューティングノードと比較し、マッチを識別することを含む、請求項１に記載のコンピュータ実施方法。
【請求項４】
前記取得された記憶済み許可情報を前記コマンド及び前記１つ以上のコンピューティングノードと前記比較することは、前記コマンドを、前記取得された記憶済み許可情報に記憶された１つ以上の正規表現にマッチさせることを含む、請求項３に記載のコンピュータ実施方法。
【請求項５】
前記取得された記憶済み許可情報を前記コマンド及び前記１つ以上のコンピューティングノードと前記比較することは、前記コマンドを、前記取得された記憶済み許可情報に記憶された１つ以上のアクセス制御表現にマッチさせることを含む、請求項３に記載のコンピュータ実施方法。
【請求項６】
前記要求を前記受信することは、複数のコンピューティングノードのグループの指示を受信することを含み、前記コマンドの前記実行を前記開始することは、前記グループの各コンピューティングノードによって前記コマンドの前記実行を開始することを含む、
請求項１に記載のコンピュータ実施方法。
【請求項７】
前記シェルアグリゲータによって、前記グループの前記複数のコンピューティングノードによる前記コマンドの実行から得られた複数の結果を受信することと、
前記シェルアグリゲータによって、前記受信された複数の結果を集約し、前記集約された結果を前記第１のユーザに返すことと、
をさらに含む、請求項６に記載のコンピュータ実施方法。

【請求項８】
前記コマンドの前記実行を前記開始する前に、前記シェルアグリゲータによって、前記１つ以上のコンピューティングノードへのシェルトランスポート層を介した１つ以上の安全な接続を確立することを含み、前記１つ以上のコンピューティングノードによる前記コマンドの前記実行を前記開始することは、前記シェルアグリゲータによって及び前記１つ以上のコンピューティングノードに、前記確立された安全な接続を介して前記コマンドを提供することをさらに含む、請求項１に記載のコンピュータ実施方法。
【請求項９】
１つ以上のコンピュータシステムを備えるシステムであって、前記１つ以上のコンピュータシステムは、１つ以上のメモリに連結される１つ以上のプロセッサを含み、前記１つ以上のメモリは、実行時に、コンピューティングシステムに、少なくとも、
前記システムによって、ネットワークアクセス可能サービスから提供された１つ以上の仮想マシン内で起動する１つ以上のオペレーティングシステム上で実行するためのコマンドを指示する第１のユーザから情報を受信させ、
前記システムによって及び前記１つ以上のオペレーティングシステムに外部で記憶された前記第１のユーザに関する許可情報に少なくとも部分的に基づいて、前記第１のユーザが前記コマンドを実行することを承認されたことを判定させ、
前記システムによって、前記１つ以上のオペレーティングシステム上で前記コマンドの実行を開始させる、
命令を含む、前記システム。
【請求項１０】
前記１つ以上のメモリは、実行時に、さらに、前記システムに、少なくとも、
現在のステータス情報を前記１つ以上のオペレーティングシステムから受信させ、
前記現在のステータス情報を集約させ、
前記集約された現在のステータス情報を前記第１のユーザに提供させる、
命令をさらに含む、請求項９に記載のシステム。
【請求項１１】
実行時に、前記システムに、少なくとも、前記第１のユーザが前記コマンドを実行することを承認されたことを判定させる前記命令は、実行時に、前記システムに、
前記第１のユーザの第１の記憶済み許可情報と異なる第２の記憶済み許可情報を伴う定義済み役割を有する異なる第２のユーザの指示を受信させ、
前記定義済み役割に関する前記第２の記憶済み許可を使用し、前記第１のユーザが前記コマンドを実行することを承認されたことを判定させる、
命令をさらに含む、請求項９に記載のシステム。
【請求項１２】
前記命令は、実行時に、さらに、前記システムに、少なくとも、
前記システムによって、許可を一時的にロックしコマンドの実行を禁止する命令を受信させ、
前記システムによって、実行するための第２のコマンドを指示する前記第１のユーザからさらなる情報を受信させ、
前記システムによって及び前記一時的にロックされた許可に基づいて、前記第２のコマンドを実行するための承認を拒否させる、
請求項９に記載のシステム。
【請求項１３】
実行時に、さらに、前記システムに、少なくとも、前記１つ以上のオペレーティングシステム上の前記コマンドの実行を開始させる前記命令は、
前記システムに、シェルトランスポート層を介して、前記１つ以上のオペレーティングシステムへの１つ以上の安全な接続を確立させ、前記確立された安全な接続を介して前記コマンドを提供させる、命令をさらに含む、請求項９に記載のシステム。
【請求項１４】

実行時に、さらに、前記システムに、前記第１のユーザが前記コマンドを実行することを承認されたことを判定させる前記命令は、

実行時に、さらに、前記システムに、前記コマンドを前記許可情報に記憶された１つ以上のアクセス制御表現にマッチさせることによって、前記第１のユーザが前記コマンドを実行することを承認されたことを判定させる、命令をさらに含む、請求項９に記載のシステム。

【請求項１５】

実行時に、さらに、前記システムに、情報を前記第１のユーザから受信させる前記命令は、実行時に、前記システムに、仮想マシンのグループの指示を受信させる命令をさらに含み、

前記コマンドの前記実行を前記開始することは、前記グループの各仮想マシンによって前記コマンドの前記実行を開始することを含む、請求項９に記載のシステム。

【発明の詳細な説明】

【背景技術】

【０００１】

多くの企業及びその他の組織は、業務をサポートする数々のコンピューティングシステムを相互接続するコンピュータネットワークを操作する。そのコンピューティングシステムは、代替的に、共同設置される（例えば、プライベートローカルエリアネットワークまたは「ＬＡＮ」の一部として）、または、その代わりに、複数の異なった地理的位置にある（例えば、他の１つ以上のプライベートまたは共有中間ネットワークを介して接続される）。例えば、単体の組織及びその代わりのものによって運用されるプライベートデータセンター、ならびにコンピューティングリソースを顧客に提供するビジネスとして組織によって運用されるパブリックデータセンター等の、相互接続され共同設置されたかなりの数のコンピューティングシステムを収容するデータセンターハウジングは、一般的になりつつある。いくつかのパブリックデータセンターのオペレータは、様々な顧客が所有するハードウェアのためのネットワークアクセス、電力、安全な設置施設を提供する一方、その他のパブリックデータセンターのオペレータは、その顧客による使用のために利用可能にされたハードウェアリソースも含む「フルサービス」施設を提供する。しかしながら、典型的なデータセンター及びコンピュータネットワークの規模及び範囲が拡大するにつれて、関連する物理コンピュータリソースをセットアップする、運営する、管理するためのタスクは、ますます複雑になりつつある。

【０００２】

汎用ハードウェアに関する仮想化技術の出現は、多様なニーズがある多くの顧客のための大規模のコンピューティングリソースの管理に関して何らかの利益をもたらしており、種々のコンピューティングリソースが、複数の顧客間で効率的及び安全に共有されることを可能にする。例えば、ＶＭＷａｒｅ、ＸＥＮ、Ｌｉｎｕｘ（登録商標）のＫＶＭ（「Ｋｅｒｎｅｌベースの仮想マシン」）、またはＵｓｅｒ－Ｍｏｄｅ　Ｌｉｎｕｘ（登録商標）によって提供されるもの等の仮想化技術は、単一の物理コンピューティングマシンが、その単一の物理コンピューティングマシンによってホストされた１つ以上の仮想マシンを各ユーザに提供することによって、複数のユーザ間で共有されることを可能にし得る。そのような仮想マシンはそれぞれ、ユーザに、所定のハードウェアコンピューティングリソースの唯一のオペレータ及びアドミニストレータであるという錯覚をもたらす、特徴のある論理コンピューティングシステムとしての機能を果たすソフトウェアシミュレーションであり、また、種々の仮想マシンにおけるアプリケーション隔離及び安全も提供しながら動作する。

【０００３】

サービスによって制御される仮想マシン及び他のコンピューティング関連リソースへのユーザのアクセスを提供するネットワークアクセス可能サービスが存在する一方で、そのようなアクセスに関する種々の問題が存在する。

【図面の簡単な説明】

【０００４】
【図１】ネットワークアクセス可能コンピューティングリソース上でコマンドを行うために、ユーザにアクセスを提供するための技術が使用され得る例示的環境を例示する、ネットワーク図である。
【図２Ａ】ネットワークアクセス可能コンピューティングリソース上でコマンドを行うために、ユーザにアクセスを提供する例を例示する。
【図２Ｂ】ネットワークアクセス可能コンピューティングリソース上でコマンドを行うために、ユーザにアクセスを提供する例を例示する。
【図３】ネットワークアクセス可能コンピューティングリソース上でコマンドを行うために、ユーザにアクセスを提供するためのシステムの実施形態を実行するために適した例示的コンピューティングシステムを例示するブロック図である。
【図４】コンピューティングリソースサービスルーチンの例示的実施形態のフロー図を例示する。
【図５】シェルアグリゲータ（Ｓｈｅｌｌ　Ａｇｇｒｅｇａｔｏｒ）ルーチンの例示的実施形態のフロー図を例示する。
【図６】許可ブローカー（Ｐｅｒｍｉｓｓｉｏｎ　Ｂｒｏｋｅｒ）ルーチンの例示的実施形態のフロー図を例示する。
【発明を実施するための形態】
【０００５】
顧客及び他のユーザに対してサービスプロバイダ環境によって提供されるコンピューティングノード、及び他のコンピューティング関連リソース等の、ネットワークアクセス可能コンピューティングリソースを制御するための技術が説明される。少なくともいくつかの実施形態では、サービスプロバイダ環境は、類似点があるインターフェースをシェルツールに提供するためなど、そのようなユーザによる使用のためのユーザコマンド実行インターフェースコンポーネントを提供してもよい。ユーザコマンド実行インターフェースコンポーネントは、それらの提供されたコンピューティングノード及びその他のコンピューティング関連リソースに外部で記憶される情報等の、提供されたコンピューティングノード及びその他のコンピューティング関連リソースにアクセスし、それらを使用及び／または修正するためのユーザの能力を制御する際に使用する種々の許可情報をさらに保持してもよい。
【０００６】
ユーザコマンド実行インターフェースコンポーネントは、少なくともいくつかの実施形態では、ユーザが１つ以上のコンピューティングノードまたはその他のコンピューティング関連リソース上で１つ以上の指示されたコマンドを実行することが承認されたかどうかを判定してもよい。ユーザが承認されたことが判定される場合、ユーザコマンド実行インターフェースコンポーネントは、コンピューティング関連リソース（複数可）上でコマンド（複数可）の実行を行い、またはそうでなければ、それを開始してもよい。例えば、コンピューティング関連リソース（複数可）がプログラムを実行するコンピューティングノードを含むとき、コマンド（複数可）は、それらのコンピューティングノードに提供され及びそれらによって実行されてもよい。代替として、コンピューティング関連リソースがストレージ関連リソースを含む場合、ユーザコマンド実行インターフェースコンポーネントは、データを記憶させるまたは読み出させるなどして、それらのストレージ関連リソース上でコマンド（複数可）を実行してもよい。ユーザコマンド実行インターフェースコンポーネントの動作は、例えば、コマンド（複数可）を実行するための１つ以上のコンピューティング関連リソースに関する情報上で実行するために１つ以上のコマンドをユーザコマンド実行インターフェースコンポーネントのシェルアグリゲータモジュールに提供する、クライアントデバイスのユーザによって開始されても
よい。シェルアグリゲータモジュールは、ユーザがコンピューティング関連リソース（複数可）上でコマンド（複数可）を実行することが承認されたかどうかを判定し、これは、ユーザコマンド実行インターフェースコンポーネントの許可ブローカーモジュールにクエ

リを行い、ユーザがそのようなアクションに対して承認されたかどうかを判定することによって、またはそうでなければ、コンピューティング関連リソース（複数可）の外部の記憶済み許可情報を使用すること等によって行われる。そのような許可情報は、下記にさらに詳細に説明されるように、種々の形態を有し、種々の様式で使用されてもよい。ユーザが承認された場合、シェルアグリゲータモジュールは、コンピューティングリソース（複数可）のそれぞれとやり取りし、そのコンピューティングリソースにコマンド（複数可）を実行させ、またはそうでなければ、そのコンピューティングリソースに関するコマンド（複数可）を実施させる。いくつかの実施形態では、シェルアグリゲータモジュールは、シェルトランスポート層モジュールを採用し、特定のコンピューティング関連リソースとの安全な接続を確立し及びコマンド（複数可）をそれらのコンピューティング関連リソースに提供し、ならびに要求を行うユーザに提供するそのようなコマンド実行から結果を随意に取得してもよい。

【０００７】

ユーザコマンド実行インターフェースコンポーネントは、少なくともいくつかの実施形態では、要求を行うユーザに集約結果を提供する前に、複数のコンピューティングノードまたはその他のコンピューティング関連リソースから受信された集約結果をさらに集約してもよい。このように、ユーザコマンド実行インターフェースコンポーネントは、複数のコンピューティングノード上で１つ以上のコマンドの同時実行及び独立実行を容易にすること等によって、多数の関連コンピューティング関連リソースのユーザによって効率的な管理を提供してもよい。例えば、シェルアグリゲータモジュールは、関連コンピューティングノードのグループ（例えば、サービスプロバイダ環境によってユーザに提供される仮想コンピュータネットワーク内の複数のコンピューティングノード、そのような仮想コンピュータネットワークの複数の論理サブネットのうちの１つの複数のコンピューティングノード、要求を行うユーザ及び／または他のユーザであるかに関わらず、共通タグを共有するために、ユーザにタグ付けされている複数のコンピューティングノード、サービスプロバイダ環境によってサポートされ及び地理的位置と関連する１つ以上のデータセンターに対応する、複数の地理的位置のうちの１つなどの、共通地理的位置における複数のコンピューティングノード等）を含む、複数のコンピューティング関連リソース上で実行される１つ以上のコマンドを管理してもよい。種々の実施形態では、シェルアグリゲータモジュールは、結果をユーザに提供する前に、それらのコンピューティング関連リソースのそれぞれから得られた結果を管理し、これは、シェルアグリゲータモジュールが集約結果をユーザに提供する前に、（同じコマンド（複数可）を実行した）複数の異なるコンピューティングノードから結果を集約することによって行われるものを含む。さらに、ユーザからの要求は、例えば、特有のコンピューティングノードで行われる特有のコマンドを指示することなど、種々の形式を有してもよい。代替として、要求は、シェルアグリゲータモジュールが複数の対応するコマンドを識別するために使用するハイレベル指図もしくは他の情報を含んでよく、及び／または定義済みグループの複数のコンピューティングノードもしくは他のコンピューティング関連リソースの指示を含んでもよく、またはそうでなければ、シェルアグリゲータモジュールがそれらのような複数のコンピューティング関連リソースを識別するために使用する情報を含んでもよい。

【０００８】

下記に説明される少なくともものいくつかの実施形態では、説明された技術は、１つ以上のサービスプロバイダ環境によって提供されるコンピューティング関連リソースに関するコマンドと併用されてもよい。他の実施形態では、説明された技術は、他の種類のコンピューティング関連リソースと併用されてもよい。下記に議論される実施形態は、例示目的のために提供され、簡潔にするために簡略化され、本発明の技術は、多種多様な他の状況で使用されてもよく、いくつかの状況が下記に議論される。

【０００９】

図１は、ユーザ構成可能管理コンピューティングノード及び／または仮想コンピュータネットワークをユーザに提供する、コンピューティングリソースサービスの例を例示する

ネットワーク図である。それらのような１つ以上の管理コンピューティングノード及び／または仮想コンピュータネットワークが、コンピューティングリソースサービスのユーザに対してコンピューティングリソースサービスによって構成及び提供された後、ユーザは、１つ以上の遠隔地から、提供されたコンピューティングノード（複数可）及び／または仮想コンピュータネットワーク（複数可）とやり取りしてもよく、これは、コンピューティングノード上でプログラムを実行し、使用中に仮想コンピュータネットワーク（複数可）及び／または提供されたコンピューティングノード（複数可）を動的に修正するなどのために行われる。ネットワークアクセス可能コンピューティングリソース上のコマンド及び関連機能を行うためにユーザにアクセスを提供するために説明された技術は、図２Ａ～２Ｂの例及び図４～６と併せて例示及び説明されるフローチャートに関するものを含む、本明細書の他の箇所でさらに詳細に議論されるような、そのようなコンピューティングリソースサービスがあるいくつかの実施形態で使用されてもよい。

【００１０】

具体的には、図１の例示的システム１００は、１つ以上のコンピュータネットワーク１０２を通して（例えば、インターネットを通して）、ユーザコンピューティングデバイス１３２を使用するユーザ（図示されない）に機能を提供するために、１つ以上の構成されたコンピューティングシステム（図示されない）を使用して実施されるコンピューティングリソースサービス１０７を含む。コンピューティングリソースサービス１０７は、例えば、インターネットまたは他のネットワークを通して利用可能であるネットワークサービス等のサービスプロバイダ組織によって提供される環境の一部であってもよい。コンピューティングリソースサービス１０７は、ユーザが、コンピューティングリソースサービス１０７によってユーザに提供されるコンピューティングノード、仮想コンピュータネットワーク、及び／または他のコンピューティングリソースにアクセスし及びそれらを使用することを可能にするが、他の実施形態及び状況では、特定のコンピューティングリソースサービスは、そのような種類のコンピューティング関連リソースのサブセット（例えば、コンピューティングノード、仮想コンピュータネットワーク、及び他のコンピューティングリソースの１つのみ）を提供してもよい。例えば、複数のユーザは、コンピュータネットワーク１０２を通して、コンピューティングリソースサービス１０７のコンピューティングリソースシステムモジュール（複数可）１１２とやり取りし、コンピューティングリソースサービス１０７によって提供される種々の提供されるコンピューティングノード１２７及び／または仮想コンピュータネットワーク１２２を作り及び構成する。本例示的実施形態では、コンピューティングリソースシステムモジュール（複数可）１１２は、コンピューティングリソースサービス１０７の機能を遠隔ユーザに提供することを補助する。また、コンピューティングリソースサービス１０７は、ユーザコマンド実行インターフェースコンポーネント１１４を含み、コンピューティングリソースサービス１０７の機能を遠隔ユーザに提供することをさらに補助し、これは、例えば、説明された技術の一部または全てを行い、提供されたコンピューティングノード１２７、提供された仮想コンピュータネットワーク１１２、及び／または他の提供されたコンピューティングリソース１９７（例えば、データベース、ストレージボリューム、または他のストレージ構造）へのユーザのアクセスを制御するために行われる。他の実施形態では、ユーザコマンド実行インターフェースコンポーネントは、（例えば、それらの１つ以上のコンピューティングリソースサービスを提供する１つ以上の他の第２オペレータ組織とは異なった第１オペレータ組織によって提供される）それらのような１つ以上のコンピューティングリソースサービスとは別々に動作してもよい。その動作は、例えば、そのようなコンピューティングリソースサービスのそのようなユーザコマンド実行インターフェースコンポーネント１１４のいずれかの代わりに、または、それに加えてかに関わらず、コンピューティングリソースサービスが別個のユーザコマンド実行インターフェースコンポーネント（例えば、ユーザコマンド実行インターフェースコンポーネントの顧客、またはそうでなければ、クライアント）と連携される場合、そのようなコンピューティングリソースサービスへのユーザアクセスを制御する随意の別個のユーザコマンド実行インターフェースコンポーネント１４５

等のために行われてもよい。

【００１１】

少なくともいくつかの実施の形態では、コンピューティングリソースシステムモジュール（複数可）１１２及びユーザコマンド実行インターフェースコンポーネント１１４は、コンピューティングリソースサービス１０７の１つ以上のコンピューティングシステム（図示されない）上で実行してもよく、コンピューティングリソースサービス１０７のユーザによる使用のために１つ以上のインターフェース１１９を提供してもよい。例えば、そのインターフェースとして、（例えば、提供されたコンピューティングノード１２７及び／または管理された仮想コンピュータネットワーク１２２を作る、構成する、及び／またはそれらの使用を開始するために）、ユーザの代わりに、遠隔コンピューティングシステムが、コンピューティングリソースサービスとプログラムでやり取りし、コンピューティングリソースサービス１０７の一部または全ての機能にアクセスすることを可能にする１つ以上のＡＰＩ（アプリケーションプログラミングインターフェース）等が挙げられる。また、少なくともいくつかの実施形態では、インターフェース（複数可）１１９は、ユーザがコンピューティングリソースサービス１０７と手動でやり取りし、いくつかまたは全てのそのようなアクションを行う、１つ以上のＧＵＩ（グラフィカルユーザインターフェース）を含んでもよい。

【００１２】

例示された実施形態では、コンピューティングデバイス１３２のユーザがインターフェース（複数可）１１９を使用し、提供されたコンピューティング関連リソース１２７、１２２、及び１９７を対象とするコマンドまたは関連要求を送信するとき、そのような少なくともいくつかのコマンドまたは関連要求は、そのようなコマンドまたは関連要求を行うかどうか、及びそれをどのように行うかを判定するために、ユーザコマンド実行インターフェースコンポーネント１１４を対象とするものであり、このとき、ユーザコマンド実行インターフェースコンポーネント１１４は、必要に応じて、ユーザの代わりに、提供されたコンピューティング関連リソース１２７、１２２、及び１９７と連続してやり取りする。他の箇所でさらに詳細に説明されるように、そのようなやり取りは、例えば、以下に示すもののうちの、１つ以上のものを含んでもよい。すなわち、リソース１２７、１２２、及び１９７上の１つ以上のコマンドを行うことによって、それらのような１つ以上のコンピューティング関連リソース１２７、１２２、及び１９７の動作を修正する、またはそうでなければ改変することと（例えば、提供されたコンピューティングノード１２７によってコマンドを実行すること、コマンドを提供された仮想コンピュータネットワーク１１２及び／または他のコンピューティングリソース１９７に提供すること等）；リソース１２７、１２２、及び１９７上の１つ以上の上のコマンドを行うことによって、ステータス情報をそれらのような１つ以上のコンピューティング関連リソース１２７、１２２、及び１９７から集めること、ならびに随意に、（集約または個別化されるかに関わらず）コマンドの結果を、要求を行うユーザに提供することと；ユーザに事前に割り当てられ及び提供された特定のコンピューティング関連リソースの使用を終了または停止することによって、ならびに／またはユーザのために提供された追加のコンピューティング関連リソース１２７、１２２、及び１９７を追加し、もしくはそうでなければ、それらの使用を開始すること等によって、コンピューティング関連リソース１２７、１２２、及び１９７のどれが要求を行うユーザのために使用されているかを修正すること、等である。いくつかの実施形態及び状況では、提供されたコンピューティング関連リソース１２７、１２２、及び１９７を対象とするいくつかのコマンドまたはその他の関連要求は、ユーザコマンド実行インターフェースコンポーネントによって制御されることなく、それらの提供されたコンピューティング関連リソースに直接送信されてもよい。

【００１３】

コンピュータネットワーク１０２は、例えば、インターネット等の、別の関係者によって動作される可能性があるリンクされたネットワークの公衆にアクセス可能なネットワークであってもよい。同様に、コンピューティングリソースサービス１０７は、コンピュー

タネットワーク１０２から離れた及びそれとは異なった内部ネットワーク等の、コンピューティングリソースサービス１０７のコンピューティングシステムを互いに接続するための１つ以上の内部ネットワーク（図示されない）を含んでもよい。

【００１４】

提供された仮想コンピュータネットワーク１２２のそれぞれは、そのネットワークが提供されたユーザよって、種々の方法で構成されてもよい。いくつかの状況では、そのような少なくともいくつかの仮想コンピュータネットワークは、既存のユーザの遠隔プライベートコンピュータネットワークへのネットワーク拡張として作られてよく及び構成されてもよいが、例示された実施形態では、提供された仮想コンピュータネットワーク１２２は、そのような他の既存のコンピュータネットワークに接続されることが示されていない。また、そのような少なくともいくつかの仮想コンピュータネットワークは、それぞれ、そのネットワークを作るユーザだけによってアクセス可能であるプライベートコンピュータネットワークであり得るが、他の実施形態では、ユーザのためにコンピューティングリソースサービス１０７によって提供される少なくともいくつかのコンピュータネットワークは、公衆にアクセス可能であってもよい。例示された例では、提供されたコンピュータネットワーク１２２のそれぞれは、複数のコンピューティングノード（図示されない）を含み、それらの少なくとも一部は、コンピューティングリソースサービス１０７によって、またそうでなければ、その制御の下、提供される複数のコンピューティングノード１２７からのものである。一方、他の実施形態では、少なくともいくつかの他のコンピューティングシステム１３７は、提供された仮想コンピュータネットワーク１２２の１つ以上のものに、いくつかのまたは全てのコンピューティングノードを提供するために使用されてもよい。そのような他のコンピューティングシステム１３７は、例えば、それらの他のコンピューティングシステム１３７を使用する仮想コンピュータネットワーク１２２が提供されたユーザによって、もしくはそのユーザの制御の下、提供されてもよく、または、（例えば、有料で）第３者によって提供されるコンピューティングシステムであってもよい。例えば、少なくともいくつかの実施形態では、提供された仮想コンピュータネットワーク１２２のそれぞれは、提供されたコンピュータネットワークの一部としての使用のために専用で用いられる、顧客が構成する量のそれらのような複数のコンピューティングノードを含んでもよい。具体的に、ユーザは、コンピューティングリソースシステムモジュール１１２とやり取りしてもよく、ユーザのために提供されたコンピュータネットワークに最初に含まれるある量のコンピューティングノードを構成し（例えば、コンピューティングリソースサービス１０７によって提供されるＡＰＩとの１つ以上のプログラムのやり取りによって）、提供された仮想コンピュータネットワーク（例えば、１つ以上の論理サブネットであって、それぞれが、提供されたコンピューティングノード１２７、仮想ルートデバイス及び他の仮想ネットワークデバイス、ＶＰＮ（仮想プライベートネットワーク）接続のためのエンドポイントまたは他の外部の組織への接続等の１つ以上を含むもの）のネットワークトポロジをさらに構成してもよい。

【００１５】

また、コンピューティングリソースサービス１０７は、少なくともいくつかの実施形態では、例えば、種々の性能特性（例えば、プロセッサ速度、利用可能メモリ、利用可能ストレージ等）、または他の能力を伴うコンピューティングノード等の、複数の異なる種類のコンピューティングノードを提供してもよい。そのような場合、そのような少なくともいくつかの実施形態では、ユーザは、顧客のために提供されたコンピュータネットワークに含まれるコンピューティングノードの種類を指定してもよい。また、少なくともいくつかの実施形態では、コンピューティングノードは、物理コンピューティングシステムであってもよく、または１つ以上の物理コンピューティングシステムもしくは物理コンピューティングマシン上でそれぞれがホストされる仮想マシンであってもよく、管理された仮想コンピュータネットワークのために対処される通信は、種々の形態のデータ（例えば、メッセージ、パケット、フレーム、ストリーム等）の伝送を含んでもよい。さらに、少なくともいくつかの状況では、コンピューティングリソースサービスの実施形態は、サービス

の複数のユーザの代わりに複数のプログラムを実行するプログラム実行サービス（または、「ＰＥＳ」）の一部、またはそうでなければ、そのプログラム実行サービスと連携されてもよい。例えば、そのプログラム実行サービスとして、複数の物理ネットワーク（例えば、１つ以上のデータセンター内の複数の物理コンピューティングシステム及びネットワーク）上で、随意に、複数の地理的位置で、複数のコンピューティングシステムを使用するもの等が挙げられる。このように、コンピューティング関連リソース１２７、１９７、及び／または１２２は、種々の実施形態において種々の様式でユーザに提供されてもよく、種々の実施形態において各種の機能を有するように構成されてもよい。

【００１６】

図２Ａ～２Ｂは、図１のコンピューティングリソースサービスによって提供され得るなど、ネットワークアクセス可能コンピューティングリソース上でコマンドを行うために、ユーザアクセスを提供する例を例示する。本明細書に説明されるように、コンピューティングリソースサービスは、コンピューティングリソースサービスのユーザによる使用のためにコンピューティングノードを提供する。

【００１７】

図２Ａは、ユーザシェルアプリケーションモジュール２０４、ユーザコマンド実行インターフェースコンポーネント２０６、及びコンピューティングリソースサービス２２６を含む、例示的システム２００Ａを例示する。ユーザシェルアプリケーションモジュール２０４ａ～ｃは、例えば、ユーザのクライアントデバイス（図示されない）上で実行し、ユーザが、コマンド及びその他の関連要求をコンピューティングリソースサービス２２６のコンピューティングノード２２８に提供することを可能にし得る。

【００１８】

ユーザコマンド実行インターフェースコンポーネント２０６は、フロントエンドインターフェースを、ユーザのためにユーザシェルアプリケーションモジュール２０４によって提供されるコマンド及びその他の関連要求を受信するコンピューティングリソースサービス２２６に提供する。ユーザコマンド実行インターフェースコンポーネント２０６は、ユーザがコンピューティングノード２２８の１つ以上で、１つ以上のコマンドを実行することが承認されたかどうかを判定する機能を提供する。ユーザが承認された場合、ユーザコマンド実行インターフェースコンポーネント２０６は、それらのコンピューティングノード２２８の少なくとも１つとやり取りし、それらのコンピューティングノードにコマンド（複数可）を実行させる。ユーザコマンド実行インターフェースコンポーネント２０６はまた、コンピューティングノード２２８から、コマンド（複数可）の実行から得られた結果を受信し、適切な場合及びそのような場合、ユーザのためにその結果を対応するユーザシェルアプリケーションモジュール２０４に提供する前に、いくつかの状況においてそれらの結果を集約してもよい。

【００１９】

例示された実施形態では、ユーザコマンド実行インターフェースコンポーネント２０６は、シェルアグリゲータモジュール２１０、許可ブローカーモジュール２１４、及びシェルトランスポート層モジュール２１８を含む。シェルアグリゲータモジュール２１０は、ユーザによって使用中に、コマンド及びその他の関連要求をユーザシェルアプリケーションモジュール２０４から受信し、許可ブローカーモジュール２１４にクエリを行い、ユーザが１つ以上のコンピューティングノード２２８（例えば、ユーザが活動し得る権限または指図の下、それらのコンピューティングノードが、ユーザによる使用のために、またはその代わりに別のユーザのために、事前に割り当てられ及び提供される場合は、コンピューティングノード２２８ａ～ｃ）上で１つ以上の対応するコマンドを実行することが承認されるかどうかを判定する。ユーザがコンピューティングノード２２８ａ～ｃ上でコマンドを実行することが承認された場合、シェルアグリゲータモジュール２１０は、シェルトランスポート層モジュール２１８に命令し、コンピューティングノード２２８ａ～ｃと対応するやり取りを行い、コンピューティングノード２２８ａ～ｃにコマンドを実行させ、適切な場合、結果を受信させる。モジュール２１８によって受信された場合、シェルアグ

リゲータモジュール２０６は、コンピューティングノード２２８ａ～ｃ上でのコマンドの実行から得られた結果を、シェルトランスポート層モジュール２１８から受信し、随意に、結果をユーザシェルアプリケーションモジュール２０４に提供する前に、その結果を集約する。

【００２０】

許可ブローカーモジュール２１４は、許可リポジトリ２１２にアクセスしユーザの許可を取得し、取得された許可を、ユーザＩＤ、実行されたコマンド、及びコマンドを実行するためのコンピューティングノードを比較する。許可リポジトリ２１２は、１人以上のユーザに関する許可を保持し、ユーザ毎の許可は、どのコマンドでユーザが実行することを承認されたのか（または、承認されないのか）及びどのコンピューティングノード上で実行されたのかを識別する。このように、ユーザコマンド実行インターフェースコンポーネントは、そのコンピューティングノードとやり取りすることなく、１つ以上のコマンドが１つ以上の特定のコンピューティングノードのために承認されたかどうかを判定することを含む、コンピューティングノード２２８の外部の許可情報を保持及び使用することができ、ユーザがそのコンピューティングノード上でそのコマンド（または、いずれかのコマンド）を行うことが承認されない場合、そのコンピューティングノードとのユーザによるやり取りをブロックすることができる。許可情報は、下記にさらに詳細に議論されるように、種々の実施形態において種々の様式で、指定及び使用されてもよい。

【００２１】

シェルトランスポート層２１８は、１つ以上のコマンドを実行するためのものである各コンピューティングノード２２８との接続（例えば、安全な接続）を確立させる。いくつかの実施形態では、シェルトランスポート層モジュール２１８は、コンピューティングノード２２８ａ～ｃとの安全な接続またはチャネル（例えば、セキュアシェルまたはｓｓｈ等）を確立するために別個のシェルセッション２２０ａ～ｃを初期化してもよい。いったん安全な接続が確立されると、シェルトランスポート層モジュール２１８は、実行のためにコマンドをコンピューティングノード２２８ａ～ｃに提供する（例えば、コンピューティングノード２２８ａ～ｃ上で実行するシェルプログラム（図示されない）等に提供する）。コンピューティングノード２２８ａ～ｃ上でのコマンドの実行から得られた結果がある場合、安全な接続及びシェルセッション２２０ａ～ｃを介して、シェルトランスポート層モジュール２１８に返される。その次に、シェルトランスポート層モジュール２１８は、結果をシェルアグリゲータモジュール２１０に転送する。シェルトランスポート層モジュール２１８は、例えば、Ｗｉｎｄｏｗｓ　ＰｏｗｅｒＳｈｅｌｌ、ＭｙＳＱＬ等のコンピューティングノードまたは他のコンピューティング関連リソース上でコマンドを実行するために他の機構を採用してもよいことを認識されたい。

【００２２】

システム２００Ａは、例示されるものよりも多いまたは少ない数の、ユーザシェルアプリケーションモジュール２０４、シェルセッション２２０、及びコンピューティングノード２２８を含み、ユーザコマンド実行インターフェースコンポーネントの他の実施形態は、示されるものよりも多いまたは少ない数のモジュールを有してもよいことを理解されたい。

【００２３】

図２Ｂは、図２Ａの例示的システム２００Ａに従った、ネットワークアクセス可能コンピューティングリソース上でコマンドを行うために、ユーザアクセスを提供するための例示的シーケンス２００Ｂを例示する。例示された例は、コンピューティングリソースサービスによって提供される３つのコンピューティングノード（例えば、一般的に、この例では、ノード１、ノード２、及びノード３と称される、コンピューティングノード２２８ａ～ｃ）を含む。ユーザは、ユーザシェルアプリケーションモジュールを介して、要求をシェルアグリゲータモジュールに提供する。例示された例では、コマンド要求は、特有のコマンド及びコンピューティングノード（例えば、ノード１、ノード２、及びノード３）を識別しコマンドを実行するが、他の状況では、他の形態を有してもよい。シェルアグリゲ

ータモジュールは、許可ブローカーモジュールにクエリを行い、ユーザが３つのコンピューティングノードのそれぞれでコマンドを実行することが承認されるかどうかを判定する。許可ブローカーモジュールは、シェルアグリゲータモジュールに、ユーザが承認される（例示されるような）または承認されない（図示されない）かどうかを示す結果を返す。ユーザが承認された場合、シェルアグリゲータモジュールは、３つのコンピューティングノードの指示と一緒に、コマンドをシェルトランスポート層モジュールに提供する。その次に、シェルトランスポート層モジュールは、各コンピューティングノードとの接続を確立し、実行のために、コマンドを各コンピューティングノードに提供する。各コンピューティングノード（互いに別々であり及び独立している）は、コマンドを実行し、その実行から得られた結果を、シェルトランスポート層モジュールに戻すように提供する。コマンドが３つのノードのそれぞれに送信される順番またはシェルトランスポート層モジュールに結果を戻すように提供される順番は、いくつかの異なる要因（例えば、コマンドを実行するためにコンピューティングノードに利用可能であるコンピューティングリソース、ネットワークトラフィック等）に起因して例示されるものと異なる場合があることを認識されたい。シェルトランスポート層モジュールは、結果をシェルアグリゲータモジュールに転送する。その次に、シェルアグリゲータモジュールは、ユーザシェルアプリケーションモジュールを介して、ユーザに結果を戻すように提供する。いくつかの実施形態では、シェルアグリゲータモジュールは、結果が受信されるとき（図示されない）、その結果をユーザシェルアプリケーションモジュールに伝えてもよく、またはシェルアグリゲータモジュールは、他の実施形態で、結果をユーザシェルアプリケーションモジュールに返す前に、１つ以上の種々の様式で、一緒に結果を集約してもよい（例えば、種々の様式として、全ての結果を連続的にリスト化することによるもの；結果の複数の値のそれぞれのカウントもしくは蓄積、または結果の種類等の、複数のコンピューティングノードから結果を集計しまたは組み合わせ、及び結果として生じる概要を提供することによるもの；結果とその結果を提供したコンピューティングノードとを比較し及び結果として生じる発見を提供するもの；等が挙げられる）。

【００２４】

上記に説明されるように、コマンド要求は、１つ以上のコンピューティングノード上で実行されるコマンドであり、またはそのコマンドを含んでもよい。しかしながら、他の実施形態では、コマンド要求は、複数のコマンド、グループのコマンド、またはそれらの複数のコマンドのいずれかを特別に含むことがない複数のコマンドに対応するハイレベルの命令または指示等を含んでもよい。例えば、いくつかの実施形態では、命令は、情報を１つ以上のコンピューティングノードから取得するための要求であってもよい。
その要求として、ステータス要求、複数のコンピューティングノードにおける分散タスクを行うまたは修正するための要求、複数のコンピューティングノードにおける事前に初期化された分散タスクまたは現在実行中の分散タスクに関する情報を取得するための要求等が挙げられる。この命令から、シェルアグリゲータモジュール２１０は、コマンド要求と関連する命令を満足するために、１つ以上のコンピューティングノード上で実行する１つ以上のコマンドを判定する。いくつかの実施形態では、シェルアグリゲータモジュールは、命令及び各命令と関連するコマンドのリストを記憶してもよい。このように、シェルアグリゲータモジュールは、受信された命令に基づいて、コマンドを調べてコンピューティングノードに提供することができる。

【００２５】

また、コマンド要求は、１つ以上のコンピューティングノードを（例えば、コンピューティングノード名、ネットワークアドレス等によって）個別に識別し、またはコマンドを実行するためのコンピューティングノードの１つ以上のグループを個別に識別してもよい。例えば、コマンド要求は、仮想コンピュータネットワークＭの全てのコンピューティングノード上でコマンドＡを実行するためのものであってもよい。この例では、シェルアグリゲータモジュールは、同じ仮想コンピュータネットワークの他のノードのリストに関する仮想コンピュータネットワークにおけるコンピューティングノードの１つにクエリを行

うこと等によって、どのコンピューティングノードが仮想コンピュータネットワークＭ内にあるのかを判定し、その次に、実行のために、コマンドをそのコンピューティングノードに提供する。他の実施形態では、コマンド要求は、個別のコンピューティングノードのそれぞれを識別することなく、特定のコンピューティングリソースサービス、コンピューティングリソース等を識別してもよい。例えば、コマンド要求は、「どれくらいの追加ストレージがユーザＺによる使用のために利用可能であるか」であり得る。その次に、シェルアグリゲータモジュールは、どのコンピューティングノードがストレージをユーザＺに提供しているかを判定し、ユーザＺは、コマンド要求を提供したユーザと同じまたは異なるユーザであり得る。このように、複数のコンピューティングノードのそれぞれに対してユーザからコマンドを別々に把握することなく、または直接提供することなく、ユーザは複数のコンピューティングノード上でコマンドを実行することができる。

【００２６】

上記に説明されるように、許可ブローカーモジュール２１４は、ユーザが１つ以上のコンピューティングノード上で１つ以上のコマンドを実行することが承認されたかどうかを判定する。ユーザが各コンピューティングノード上で各コマンドを実行することが承認された場合、許可ブローカーモジュールは、コマンド毎及びコンピューティングノード毎（例えば、各コマンド／コンピューティングノードの組み合わせ）に基づいて、判定してもよい。いくつかの実施形態では、承認は全体的な判定であってもよく、これにより、ユーザが１つのコマンド／コンピューティングノードの組み合わせに関して承認されない場合、ユーザがシェルアグリゲータモジュールに提供されるコマンド要求全部に関して承認されない。他の実施形態では、承認は個別の判定であってもよく、これにより、ユーザが承認されたコマンド／コンピューティングノードの組み合わせに関して（ただし、ユーザが承認されないコマンド／コンピューティングノードの組み合わせに関してではなく）、コマンドがコンピューティングノードに提供され及びそこで実行される。このように、要求コマンドの一部は、いくつかのコンピューティングノード上で実行され得るが、その他のもので実行されない場合がある一方、他のコマンドは、他のコンピュータノード上で実行され得る、または全くそうではない場合がある。種々の実施形態では、許可を確立するアドミニストレータはまた、許可ブローカーモジュールがユーザごとに全部の承認または個別の承認を判定するかどうかを指示してもよい。他の種々の実施形態では、ユーザは、コンピューティングリソースサービスに内部に存在してもよく、または、コンピューティングリソースサービスの顧客等のコンピューティングリソースサービスの外部に存在してもよい。

【００２７】

本明細書に説明されるいくつかの実施形態がコンピューティングノード上でコマンドを実行することに言及するが、コマンドは、例えば、アプリケーション、仮想化コンテナ（例えば、アプリケーションの配置を自動化するオペレーティングシステムレベル仮想化）等の、他のアドレス可能なアイテムに提供され、またはそこで実行されてもよい。いくつかの実施形態では、各コンピューティングノードは、１つ以上のコンテナを含んでもよく、本明細書に説明される実施形態は、コンピューティングノードの１つ以上のコンテナ上で、１つ以上のコマンドを実行するために採用されてもよい。

【００２８】

シェルアグリゲータモジュール２１０、許可ブローカーモジュール２１４、及びシェルトランスポート層モジュール２１８の機能は、例示されるように、別個のモジュールとして提供されてもよく、または、１つ以上の他のモジュールによって提供されてもよく、随意に、許可ブローカーモジュール及び／またはシェルトランスポート層モジュールの機能は、シェルアグリゲータモジュールの一部として含まれることを理解されたい。同様に、ユーザシェルアプリケーションモジュール２０４は、随意であってもよく、ユーザは、ブラウザ、ＡＰＩコール、または他のインターフェースを経由して、コマンド要求を提供してもよい。種々の実施形態では、ユーザコマンド実行コンポーネント２０６の機能またはそのモジュールのいずれかは、コンピューティングリソースサービスの別のモジュール（

例えば、図１のコンピューティングリソースシステムモジュール１１２）のサブモジュールまたはサブコンポーネントであってもよい。いくつかの実施形態では、ユーザコマンド実行インターフェースコンポーネントは、コンピューティングリソースサービスのコンピューティングリソースシステムモジュールのフロントエンドとして、動作してもよい。他の実施形態では、ユーザコマンド実行コンポーネントは、別個のモジュール（例えば、図１に例示されるような）であってもよく、これにより、ユーザ（複数可）がコンピューティングノード（複数可）上でコマンド（複数可）を実行する要求を提供することを可能にするユーザコマンド実行インターフェースコンポーネントとは別に、コンピューティングリソースサービスのコンピューティングリソースシステムモジュールは、ユーザが、コンピューティングノード（複数可）を構成すること、または他のユーザ（複数可）の許可を確立することを可能にする。

【００２９】

また、許可を受信しコンピューティングノード上でコマンドを実行する要求を提供するユーザは、コンピューティングノードが提供されたコンピューティングリソースサービスのユーザ（例えば、提供されたコンピューティングノードを受信したユーザ）と同じまたは異なるユーザであってもよいことを理解されたい。例えば、コンピューティングノードのグループは、コンピューティングリソースサービスに関するウェブサイトを開発するウェブ開発者のグループに提供されてもよい。ユーザは、コンピューティングノードのアドミニストレータとして役割を果たすように指定されてもよく、許可を他のユーザ（例えば、ＩＴサポート技術者ユーザ）に提供し、ウェブ開発者に提供されるコンピューティングノードのグループ内の１つ以上の特有のコンピューティングノード上で特有のコマンドを実行してもよい。このように、ユーザコマンド実行インターフェースコンポーネント２０６は、コンピューティングノードにアクセスする他のユーザのためにコンピューティングリソースサービスによって保持される許可から独立して、特有のユーザに関する許可を保持し、特定のコンピューティングノード上の特定のコマンドを実行する。また、許可は、いくつかの実施形態及び状況では、ユーザが、他のユーザの役割を想定しコンピューティングノード上でコマンドを実行することを可能にし得る。さらなる他の実施形態では、許可は、テンプレート許可（例えば、読取専用ポリシー、ユーザの役割等）に基づき、１人以上のユーザのために選択されてもよい。したがって、許可情報は、種々の実施形態において種々の様式で、指定及び使用されてもよい。例えば、いくつかの実施形態では、ユーザコマンド実行インターフェースコンポーネント及び／またはコンピューティングリソースサービスは、連合ＩＤモデルを使用してもよく、及び／または、関連のアクセス許可を有する種々の役割を定義してもよく、各ユーザはゼロ以上のそのような役割と関連付けられる。いくつかの実施形態では、特定のユーザは、その特定のユーザまたはそのグループに提供された１つ以上のコンピューティングノードまたは他のコンピューティング関連リソースの一部または全てへの共用アクセスを受信する複数のユーザのグループを管理または指図してもよく、これにより、全てのグループユーザは、同じアクセス許可を有し、または、その代わりに、異なるグループメンバーは、特定のコマンドもしくはコマンド種類に関して及び／または特定のコンピューティングノードもしくはコンピューティング関連リソースの種類に関して、異なる許可が割り当てられる。指定され得るアクセス許可の非排他的例は、以下を含む。すなわち、認められる、または認められないユーザ、コマンド、及び／またはコンピューティング関連リソースの組み合わせ；例えば、アクセス許可を指定し、読み出し、書き込み、及び／または実行するための、特定のコンピューティング関連リソース及び／またはコマンド及び／またはユーザ；認証される、または認証されないコマンド及び／またはユーザ及び／またはコンピューティング関連リソースにマッチする正規表現；ユーザグループもしくは種類、または、全てもしくは特有のコマンド及び／もしくはコンピューティング関連リソースに関する認証を指定している他の集約された複数のユーザの識別；コマンドグループもしくは種類、または、全てもしくは特有のユーザ及び／もしくはコンピューティング関連リソースに関する認証を指定している他の集約された複数のコマンドの識別；コンピューティングリソースグループもしくは種類、または

、全てもしくは特有のユーザ及び／もしくはコマンドに関する認証を指定している他の集約された複数のコンピューティングリソースの識別；関連の許可情報及びユーザにどのユーザの役割が割り当てられたかに関する情報を用いた、ユーザの役割の識別；実行時に、１人（１つ）以上のユーザ、コマンド、及び／またはコンピューティング関連リソースの組み合わせに関する認証の指示を、提供するまたは提供しない、１つ以上のスクリプトまたは他のプログラム；等である。複数のアクセス許可が指定されると、優先順位または順序付けは、いくつかの実施形態において、特定の状況で、どの指定されたアクセス許可情報を使用するかを判定するために、さらに使用されてもよい。種々の実施形態では、許可リポジトリ２１２は、どのコマンドでユーザが実行することを承認されたのか（または、承認されないのか）及びどのコンピューティングノード上で実行されたのかを示す、コマンド／コンピューティングノードの組み合わせの「許可する／拒否する」リストを含んでもよい。

【００３０】

以下の説明は、ユーザ許可を定義するための及びユーザがコマンドを実行することが承認された場合を判定するための正規表現を使用する一例であるが、そのような情報が他の実施形態において他の様式で指定されてもよいこと及び／または他の種類のアクセス許可が他の実施形態で使用されてもよいことが理解されるだろう。この例では、ユーザごとのテーブルは、許可リポジトリに記憶されてもよく、そのテーブルは、ユーザが、ユーザと関連するいずれかのコンピューティングノード上でコマンドをマッチさせることを実行することを承認されるか否かを指定する正規表現のリストを含む。この例の情報は、特定のコンピューティングノードに特有ではない一方、そのような情報は、他の実施形態において、特定のコンピューティングノード、またはコンピューティングノードのグループもしくは種類（または、他の種類のコンピューティングリソース）に適用するように、さらに指定されてもよいことが理解されるだろう。ユーザがコマンドをシェルアグリゲータモジュールに提供すると、許可ブローカーは、コマンド及び記憶された正規表現のマッチを探しているそのユーザに関するテーブルによって検索してもよい（例えば、複数のマッチング表現がある場合、最初のマッチまたは最優先マッチに関して行われる）。いったんマッチが識別されると、マッチした正規表現に関して対応する「許可する／拒否する」の許可またはアクションが、ユーザがコマンドを実行することが承認されるか否かを指示する。そのような記憶されたテーブルの一非限定例は、次のようなものであってもよい。

【表１】

ユーザＡ	
マッチ	アクション
／ｌｓ／	許可する
／ｃａｔ／	拒否する
／．＊／	拒否する

【００３１】

上記テーブルでは、「マッチ」カラムは、実行するコマンドに対して比較する正規表現を含んでもよく、「アクション」カラムは、ユーザが対応する正規表現にマッチするコマンドを実行することが承認されるか（例えば、許可する）、または承認されないか（例えば

、拒否する）どうかを指示する。この例では、「ｌｓ」は、いくつかのオペレーティングシステムに関するディレクトリのコンテンツをリスト化するためのコマンドであり、「ｃａｔ」は、いくつかのオペレーティングシステムに関するファイルのコンテンツを見るためのコマンドであり、「．＊」は、ゼロ以上の文字のいずれかの組み合わせにマッチさせるためのワイルドカード表現である。いくつかの実施形態及び状況では、他のより複雑な正規表現もまた、採用されることができる。例えば、正規表現「ｌｓ／ｈｏｍｅ／ｕｓｅｒ－ａ／＊」及びアクション「許可する」は、ユーザが特有のディレクトリ「／ｈｏｍｅ／ｕｓｅｒ－ａ／＊」のコンテンツをリスト化することを承認してもよいが、より後のまたはより低い優先度の正規表現「ｌｓ．＊」及びアクション「拒否する」は、ユーザがいずれかの他のディレクトリのコンテンツをリスト化することを禁止する場合がある。上記の例示的テーブルでは、２つのフォワードスラッシュ（「／／」）は、スラッシュ間のコンテンツが正規表現であることを指示するシンタックスであるが、他のシンタックスもまた、採用されてもよい。また、テーブルのエントリは、例証目的のためのものであり、示されたものに限定されない。

【００３２】

いくつかの実施形態では、ユーザは、複数の異なる許可レベルにおいて、１つ以上のコンピューティングノード上で１つ以上のコマンドを実行することが許可されてもよい。例えば、ユーザの標準ログインＩＤ（例えば、ユーザ名）は、いくつかのコマンドの実行を承認するが他のコマンドを承認しない１つ以上の関連の第１の許可レベルを有してもよい。そのような場合、いくつかの実施形態及び状況では、説明された技術は、１回毎に、一時的などに、対応する指定された構成情報に基づいて１つ以上の関連の第１の許可レベルよりも高い第２の許可レベル（例えば、アドミニストレータ特権）を必要とする、ユーザが要求している１つ以上のコマンドを実行することを判定してもよく、これは、ユーザが、より高い第２の許可レベルと関連する役割または他のユーザＩＤを引き継ぐことを承認されるなどの場合に行われる。一例として、ユーザは、複数の許可レベルと関連して実行される複数のコマンドを有する要求を提供してもよい。そのような場合、シェルアグリゲータモジュールは、許可ブローカーモジュールにクエリを行い、ユーザの１つ以上の関連の第１の許可レベル等に基づき、ユーザが１つ以上の関連のコンピューティングノード上でコマンドのそれぞれを実行することが承認されたかどうかを判定する。そのような場合、シェルアグリゲータモジュールは、ユーザのログインＩＤ及びその１つ以上の関連の第１の許可レベルを使用して、コマンドのそれぞれの実行を開始してもよい。

【００３３】

逆に、許可ブローカーモジュールは、ユーザの１つ以上の関連の第１の許可レベルにおいて要求コマンドの１つ以上の第１のコマンドを実行することをユーザが承認されたことを示す場合（ただし、このとき、ユーザの１つ以上の関連の第１の許可レベルにおいて要求コマンドの１つ以上の他の第２のコマンドを実行することが承認されない）、シェルアグリゲータモジュールは、種々の実施形態及び状況において種々の様式で、処理を継続してもよい。いくつかのそのような実施形態及び状況では、シェルアグリゲータモジュールは、ユーザに関する１つ以上の第１のコマンドの実行を開始してもよいが、ユーザに提供される対応するエラー情報を用いる等、ユーザに関する１つ以上の第２のコマンドの実行を開始しない場合がある。他の実施形態及び状況では、少なくとも１つの要求コマンドが承認されない場合、シェルアグリゲータモジュールは、いずれの要求コマンドの実行も開始しない場合がある。さらなる他の実施形態では、シェルアグリゲータモジュールは、ユーザのログインＩＤ及び１つ以上の関連の第１の許可レベルを使用して、ユーザに関する１つ以上の第１のコマンドの実行を開始してもよいが、ユーザの代わりに第２のコマンドの実行を開始するようにさらに措置を取り（ただし、１つ以上の他のより高い第２の許可レベルを使用することによって）、これは、ユーザがより高い第２の許可レベルを有する別のユーザの役割もしくはログインＩＤを引き受けることが承認される、またはユーザと関連する構成情報は、特有の環境で、より高い第２の許可レベルのそのような使用を許可するなどの場合に行われる。それぞれ、そのような機能は、技術者が、最初にエンドユー

ザの許可を使用してコマンドを実行し及び続けてアドミニストレータの許可を使用して同じコマンドを実行することによって、エンドユーザの問題のトラブルシューティングを行うことを可能にすることができる。この機能は、エンドユーザの許可、ノード関連問題等についての問題があるかどうかを判定するために使用されることができる。複数のコマンドが１つ以上のコンピューティングノード上で実行する他の状況のように、異なる許可レベルにおいて別々の実行から得られた結果は、いくつかの状況では、ユーザに個別に伝えられてもよく、一方、他の状況では、ユーザに送信する前に、集約されてもよい。また、ユーザは、いくつかの状況では、単一の要求であるかまたは長期にわたる複数の要求であるかに関わらず、複数の異なる許可レベルにおいて１つ以上のコマンドを実行する要求をしてもよいことを認識されたい。

【００３４】

また、いくつかの実施形態及び状況では、１人以上のユーザに関して指定された許可は、（一時的または永久的に関わらず）アドミニストレータまたはサービスオーナーによって無効にされてもよく、これにより、シェルアグリゲータモジュール及び／または許可ブローカーモジュールは、そのユーザの許可に関わらず全てのコマンド実行要求を拒否する場合がある。例えば、アドミニストレータユーザは、命令をユーザコマンド実行インターフェースコンポーネントに提供し、一時的に全てのコマンド実行をロックアウトしてもよい。本一非限定例は、ピーク時間中に発生する場合があり、これにより、ユーザは、他のユーザへのコンピューティングノードのアクセスに影響を与え得るコマンド（例えば、システム再起動、ノードアップグレード、計算集約コマンド等）を実行しない。いくつかの実施形態では、このロックアウトは、所定期間に基づき、一時的であってもよく、またはアドミニストレータが無効を解除するまで行われてもよい。

【００３５】

他のストレージ機構及びデータ構造は、他の実施形態で利用され、ユーザ許可を記憶し、ならびにどのコマンドでユーザが実行することが承認されたのか、または承認されなかったのか及びどのコンピューティングノード上で実行されたのかを記憶してもよいことを理解されたい。

【００３６】

図３は、ネットワークアクセス可能コンピューティングリソース上でコマンドを行うために、ユーザにアクセスを提供するための例示的コンピューティングシステムを例示するブロック図である。具体的には、図３は、サーバコンピュータシステム３０５、ユーザコンピュータシステム３５０、提供するコンピューティングノード３７０、及び他のコンピューティングシステム３８０を含む、例示的システム３００を例示する。

【００３７】

サーバコンピューティングシステム３０５は、説明された技術の少なくとも一部を提供するために自動化動作を行うことに適している。その説明された技術は、その少なくとも一部を使用することができるコンピューティングリソースサービスの実施形態を提供する、ユーザコマンド実行インターフェースコンポーネント３４２及びコンピューティングリソースシステムモジュール（複数可）３４０を動作させることを含む。しかし、他の実施形態では、説明された技術は、コンピューティングリソースサービスを含まない他の環境で使用されてもよく、またはコンピューティングリソースサービスは、ユーザコマンド実行インターフェースコンポーネントを提供するものと異なるサーバコンピューティングシステムによって提供されてもよい。

【００３８】

例示された実施形態では、サーバコンピューティングシステム３０５は、１つ以上のハードウェアＣＰＵ（「中央処理装置」）コンピュータプロセッサ３０７、種々のＩ／Ｏ（「入力／出力」）コンポーネント３１０、ストレージ３２０、及びメモリ３３０を含む、コンポーネントを有する。例示されたＩ／Ｏコンポーネントは、ディスプレイ３１１、ネットワーク接続３１２、コンピュータ可読媒体ドライバ３１３、及び他のＩ／Ｏデバイス３１５（例えば、キーボード、マウス、スピーカ等）を含む。また、ユーザコンピュータ

システム３５０（１つ以上のＣＰＵ３５１、Ｉ／Ｏコンポーネント３５２、ストレージ３５４、及びメモリ３５７を含む）は、それぞれ、サーバコンピューティングシステム３０５のコンポーネントに類似するものを有してもよい。ただし、いくつかの詳細は、簡潔にするために、コンピューティングシステム３５０に例示されない。他のコンピューティングシステム３８０（複数のホストされた仮想マシンにおいて提供されたハードウェアリソースを分割することを含む）はまた、それぞれ、サーバコンピューティングシステム３０５に関して例示されたコンポーネントの一部または全てに類似するコンポーネントを含んでもよいが、そのようなコンポーネントは、簡潔にするために本例に例示されない。

【００３９】

ユーザコマンド実行インターフェースコンポーネント３４２の１つ以上のモジュール（例えば、図１のユーザコマンド実行インターフェースコンポーネント１１４または図２のユーザコマンド実行インターフェースコンポーネント２０６）は、メモリ３３０内に記憶され、本明細書に説明されるネットワークアクセス可能コンピューティングリソース上でコマンドを行うためのユーザアクセスを制御する。いくつかの実施形態では、各モジュールは、実行時に、ＣＰＵプロセッサ３０７の１つ以上のものをプログラムし説明された機能を提供する、種々のソフトウェア命令を含む。ユーザコマンド実行インターフェースコンポーネント３４２は、シェルアグリゲータモジュール３４４（例えば、図２のシェルアグリゲータモジュール２１０）を含み、随意に、許可ブローカーモジュール３４６（例えば、図２の許可ブローカーモジュール２１４）、及び／またはシェルトランスポート層モジュール３４８（例えば、図２のシェルトランスポート層モジュール２１８）を含んでもよい。

【００４０】

１つ以上のコンピューティングリソースシステムモジュール３４０（例えば、図１のコンピューティングリソースシステムモジュール１１２）は、メモリ３３０内に記憶され、コンピューティングリソースサービスの実施形態を提供し、いくつかの実施形態では、各モジュールは、実行時に、ＣＰＵプロセッサ３０７の１つ以上のものをプログラムし説明された機能を提供する、種々のソフトウェア命令を含む。コンピューティングリソースシステムモジュール３４０のモジュール（複数可）は、ネットワーク３９０を通して（例えば、コンピューティングリソースサービス内のローカルもしくはプライベートネットワーク、インターネット、またはワールドワイドウェブを介して、プライベートセルラーネットワーク等を介して）、ユーザコンピューティングシステム３５０及び他のコンピューティングシステム３８０とやり取りする。

【００４１】

コンピューティングリソースシステムモジュール３４０の機能に関連する種々の情報は、ストレージ３２０内に記憶され、動作中にコンピューティングリソースシステムモジュール３４０によって使用されてもよい。種々の情報は、例えば以下のものである。すなわち、特定のユーザに関連するユーザデータ３２１（例えば、ユーザのアカウント情報、ユーザに提供されたコンピューティングリソースに関する指定された構成情報等）；ユーザに提供される特定の仮想コンピュータネットワークに関連するユーザ仮想ネットワークデータ３２５（例えば、提供されたコンピューティングノード３７０等に関する仮想コンピュータネットワークによって使用される特定のコンピューティングリソース；仮想コンピュータネットワークに関する指定されたネットワークトポロジ及び他の指定された構成情報等）；特定のコンピューティングリソースに関連するコンピューティングリソースデータ３２３（例えば、提供されたコンピューティングノード３７０等に関する、ユーザに提供される他のコンピューティングリソースに関する情報、追加のコンピューティングリソースに関する情報（そのような提供されたコンピューティングリソースとして使用され利用可能であるもの）等；ユーザ許可情報に関連する許可リポジトリ３２７（例えば、ユーザ（複数可）がコンピューティングノード（複数可）を実行することが承認され、または承認されない特定のコマンド（複数可））が挙げられる。

【００４２】

他のコンピューティングシステム３８０は、１つ以上のデータセンター（図示されない）等で仮想コンピュータネットワーク及び他のコンピューティングリソースを提供するために、または、ユーザコマンド実行インターフェースコンポーネント３４２とは別に、１つ以上のコンピューティングリソースサービスの他の機能もしくはサービスを提供するために、コンピューティングリソースサービスによって使用されるコンピューティングシステムであってもよい。

【００４３】

ユーザコンピューティングシステム３５０及び他のコンピューティングシステム３８０は、コンピューティングリソースシステムモジュール（複数可）３４０とのやり取りの一部として種々のソフトウェアを実行してもよい。例えば、ユーザコンピュータシステム３５０は、それぞれ、メモリ３５７（ウェブブラウザ３５８または選択ユーザシェルアプリケーションモジュール３５９等）内のソフトウェアを実行し、コンピューティングリソースシステムモジュール（複数可）３４０及び／またはユーザコマンド実行インターフェースコンポーネント３４２とやり取りしてもよい。コンピューティングリソースシステムモジュール（複数可）３４０及び／またはユーザコマンド実行インターフェースコンポーネント３４２は、コマンド要求を提供し、少なくとも１つのコンピューティングノード上で少なくとも１つのコマンドを実行し、コンピューティングリソースをコンピューティングリソースサービスから要求することと、そのようなコンピューティングリソースとやり取りし、またはそうでなければ、そのようなコンピューティングリソースを使用することとを含む。

【００４４】

コンピューティングシステム３０５、３５０、３７０及び３８０は、単なる例証であり、本発明の範囲を限定することが意図されないことを理解されたい。コンピューティングシステムは、それぞれ、代わりに、複数のやり取りするコンピューティングシステムまたはデバイスを含んでもよく、コンピューティングシステムは、例示されない他のデバイスに接続されてもよく、これは、インターネット等の１つ以上のネットワークを経由する、ウェブを介する、またはプライベートネットワーク（例えば、モバイル通信ネットワーク等）を介することを含む。より一般的には、コンピューティングシステムまたは他のコンピューティングノードは、説明された種類の機能とやり取りし及びそれを行う場合があるハードウェアまたはソフトウェアのいずれかの組み合わせを含んでもよい。これは、限定ではないが、デスクトップまたは他のコンピュータ、データベースサーバー、ネットワークストレージデバイス及び他のネットワークデバイス、ＰＤＡ、携帯電話、無線電話、ポケットベル、電子手帳、インターネット家電、テレビベースシステム（例えば、セットトップボックス及び／またはパーソナル／デジタルビデオレコーダー）、ならびに適切な通信能力を含む他の種々の消費者製品を含む。また、コンピューティングリソースシステムモジュール（複数可）３４０及び／またはユーザコマンド実行インターフェースコンポーネント３４２によって提供される機能は、いくつかの実施形態では、本明細書の他の箇所で説明されるように、１つ以上のモジュールに分散されてもよい。

【００４５】

また、種々のアイテムが、使用中に、メモリ内にまたはストレージ上に記憶されるように例示される一方、これらのアイテムまたはそれらの一部は、メモリ管理及びデータ整合のために、メモリと他のストレージデバイスとの間で移送されてもよいことを理解されたい。代替として、他の実施形態では、ソフトウェアモジュール及び／またはシステムの一部または全ては、別のデバイス上のメモリ内で実行し、コンピュータ間通信を介して、例示されたコンピューティングシステムと通信してもよい。したがって、いくつかの実施形態では、説明された技術の一部または全ては、ハードウェア手段によって行われてもよい。ハードウェア手段は、１つ以上のプロセッサ及び／もしくはメモリ及び／もしくはストレージ（１つ以上のソフトウェアプログラムによって（例えば、コンピューティングリソースシステムモジュール（複数可）３４０及び／またはユーザコマンド実行インターフェースコンポーネント３４２によって）構成されるときのもの）、またはデータ構造を含む

。これは、１つ以上のソフトウェアプログラムのソフトウェア命令の実行により、ならびに／または、そのようなソフトウェア命令及び／もしくはデータ構造の記憶等によるものによって行われてもよい。さらに、いくつかの実施形態では、本システムまたはモジュールの一部または全ては、限定ではないが、１つ以上の特定用途向け集積回路（ＡＳＩＣ）、標準的集積回路、コントローラ（例えば、適切な命令を実行することによって使用されるもの、ならびにマイクロコントローラ及び／または組込コントローラを含むもの）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、結合プログラム可能論理回路（ＣＰＬＤ）等を含む、ファームウェア及び／またはハードウェアで少なくとも部分的または完全に実施される手段等を使用することによって、他の様式で、実施または提供されてもよい。モジュール、システム、及びデータ構造の一部または全ては、また、非一過性コンピュータ可読ストレージ媒体（ハードディスクもしくはフラッシュドライブ、または他の不揮発性ストレージデバイス等）、揮発性もしくは不揮発性メモリ（例えば、ＲＡＭ）、ネットワークストレージデバイス、または適切なドライブによってもしくは適切な接続を介して読み出されるポータブルメディア用品（例えば、ＤＶＤディスク、ＣＤディスク、光ディスク等）で、（例えば、ソフトウェア命令または構造化データとして）記憶されてもよい。本システム、モジュール、及びデータ構造はまた、いくつかの実施形態では、無線ベース及び有線／ケーブルベースの媒体を含む、様々なコンピュータ可読伝送媒体上で、生成されたデータ信号（例えば、搬送波、または他のアナログもしくはデジタル伝搬信号の一部となるのもの）として伝達されてもよく、（例えば、単一もしくは多重アナログ信号の一部として、または複数の別々のデジタルパケットもしくはフレームとして）様々な形態をとってもよい。そのようなコンピュータプログラム製品はまた、他の実施形態では、他の形態をとってもよい。したがって、本発明は、他のコンピュータシステム構成で行われてもよい。

【００４６】

図４は、コンピューティングリソースサービスルーチン４００の例示的実施形態のフロー図を例示する。ルーチン４００は、例えば、図３のコンピューティングリソースシステムモジュール（複数可）３４０、図１のコンピューティングリソースシステムモジュール（複数可）１１２の実行によって、またはそうなければ、本明細書に議論されるようなコンピューティングリソースサービスによって、提供されてもよい。これによって、ユーザ構成可能管理コンピューティングノードまたは他のコンピューティング関連リソースをユーザに提供するための及びユーザアクセスを構成しそのようなコンピューティング関連リソース（例えば、１つ以上の管理コンピューティングノード等）上でコマンドを行うための説明された技術等を行う。ネットワークアクセス可能コンピューティングリソース上でコマンドを行うための及び関連の機能を行うためにユーザにアクセスを提供するための説明された技術は、コンピューティングリソースサービスによって少なくともサポートされるように本例で議論され、そのような機能は、他の実施形態では、コンピューティングリソースサービスと別々のシステムによって提供されてもよいことが理解されるだろう。

【００４７】

例示された実施形態では、ルーチン４００は、ブロック４０５で始まり、そこで、命令または他の情報が受信される。いくつかの実施形態では、命令または他の情報は、ユーザ、サービスオーナー等（例えば、図１のコンピューティングリソースサービス１０７の管理者、アドミニストレータ等）から得られたものであってもよい。いくつかの実施形態では、命令は、１人以上のユーザに提供または配分されるコンピューティングリソース、１つ以上のコンピューティングノード上で１つ以上のコマンドを実行するための１人以上のユーザに関する許可等をカスタマイズする構成情報であってもよい。

【００４８】

ルーチン４００は、決定ブロック４１０に進み、ブロック４０５で受信された命令または他の情報が１つ以上のコンピューティングノードを１人以上のユーザに提供する要求であるかどうかを判定し、そのような場合、ルーチン４００は、ブロック４１５に進む。

【００４９】

ブロック４１５では、ルーチン４００は、ユーザから構成情報を受信し、（例えば、必要料金を提供することに基づいて、該当する場合、コンピューティングリソースサービスでのユーザの以前の登録活動等に基づいて）ユーザが要求に対して承認されかどうかを判定する。ユーザが要求に対して承認されない場合、その要求は断られ、ルーチン４００は、随意に、対応するエラーメッセージが生成されユーザに提供された後、決定ブロック４２０に進む。ユーザが承認された場合、ルーチン４００は、コンピューティングマシン及びコンピューティングリソースサービスによって提供される他のコンピューティングリソースを使用して、（コンピューティングリソースを要求しているユーザを含み得る）１人以上のユーザに関する１つ以上のコンピューティングノードを選択し、選択されたコンピューティングノード（複数可）をユーザ（複数可）に利用可能にさせる。いくつかの実施形態では、１つ以上のコンピューティングノードを含む仮想コンピュータネットワークは、ユーザ（複数可）のために作られてもよい。他の実施形態では、１つ以上のサブネットは、各サブネットがユーザ（複数可）に提供される少なくとも１つのコンピューティングノードを含むように、仮想コンピュータネットワーク内で作られてもよい。

【００５０】

ブロック４１５の次に、またはその代わりに、コンピューティングノード（複数可）を１人以上のユーザに提供する情報がブロック４０５で受信されないことが決定ブロック４１０で判定される場合、ルーチン４００は、決定ブロック４２０に進み、情報がブロック４０５で受信されかどうかを判定し、１人以上のユーザに関する許可を作り、またはそうでなければ、それを修正し、選択された１つ以上のコンピューティングノード上で１つ以上のコマンドを実行し、ブロック４１５でユーザ（複数可）に利用可能にさせる。許可が提供される場合、ルーチン４００はブロック４２５に進む。

【００５１】

ブロック４２５では、ルーチン４００は、コンピューティングリソースサービスに関する許可リポジトリ（例えば、図３の許可リポジトリ３２７、図２Ａの許可リポジトリ２１２等）内に、どのユーザ（複数可）がどのコンピューティングノード（複数可）上でどのコマンド（複数可）を実行することができるのかを示す受信された許可を記憶する。記憶済み許可及びその使用に関連するさらなる詳細は、本明細書の他の箇所で説明される。

【００５２】

ブロック４２５の次に、またはその代わりに、１つ以上のコンピューティングノード（複数可）上でコマンド（複数可）を実行するための許可を保存する情報がブロック４０５で受信されないことが決定ブロック４２０で判定される場合、ルーチン４００は、決定ブロック４４０に進む。ブロック４４０では、ルーチン４００は、該当する場合、必要に応じて、１つ以上の他の指示された動作を行う。例えば、いくつかの実施形態では、ルーチンは、コンピューティングリソースサービスの顧客に提供される１つ以上のコンピューティングノードの提供されたコンピューティングリソースを操作する要求を受信してもよく、そのような場合、要求が承認されたとき、そのような要求を満たす活動を行ってもよい。ブロック４４０に関連して行われる他の種類の動作は、例えば、提供されたコンピューティングノード（複数可）を使用することができる新しいユーザを登録する動作を行うような、コンピューティングリソースサービスに関する種々の管理動作を含んでもよい。

【００５３】

ブロック４４０の次に、ルーチン４００は、決定ブロック４４５に進み、例えば、終了するための明確な指示が受信されるまで、ルーチンを継続し付加情報を処理するかどうかを判定する。継続すると判定された場合、ルーチン４００は、ブロック４０５に戻り、そうでなければ、ルーチン４００は終了する。

【００５４】

図５は、シェルアグリゲータルーチン５００の例示的実施形態のフロー図を例示する。ルーチン５００は、例えば、図２のユーザコマンド実行インターフェースコンポーネント２０６及び／もしくはシェルアグリゲータモジュール２１０、図３のユーザコマンド実行インターフェースコンポーネント３４２及び／もしくはシェルアグリゲータモジュール３

４４、ならびに／または図１のユーザコマンド実行インターフェースコンポーネント１１４もしくは１４５の実行によって提供されてもよい。これによって、ユーザアクセスを提供しユーザアクセス可能コンピューティングリソース上でコマンドを行うための説明された技術等の一部または全てを行う。ネットワークアクセス可能コンピューティングリソース上でコマンドを行うための、及び関連の機能を行うために、ユーザアクセスを提供するための説明された技術は、コンピューティングリソースサービスによって提供されるように本例で議論される一方、そのような機能は、他の実施形態では、コンピューティングリソースサービス（例えば、ＣＮＳコンピューティングリソースサービス）と別々のシステムによって提供されてもよいことが理解されるだろう。

【００５５】

ルーチン５００は、ブロック５０５で始まり、そこで、コマンドまたは他の情報を実行する要求がユーザから受信される。本明細書の他の箇所で説明されるように、コマンド要求は、１つ以上のコマンド、複数のコマンド、グループのコマンド、またはハイレベル命令もしくは指図（特有のコマンドを含まない）等を含んでもよい。

【００５６】

ブロック５０５の次に、ルーチン５００は、決定ブロック５１０に進み、ブロック４０５で受信された情報が１つ以上のコンピューティングノード上でコマンドを実行する要求であるかどうかを判定する。コマンド要求がブロック５０５で受信された場合、ルーチン５００は決定ブロック５１０からブロック５２０に進み、そうでなければ、ルーチン５００は決定ブロック５１０からブロック５１５に進む。

【００５７】

ブロック５１５では、ルーチン５００は、必要に応じて、１つ以上の他の指示された動作を行う。ブロック５１５０の次に、ルーチン５００は決定ブロック５６０に進む。

【００５８】

ブロック５０５で受信された情報がコマンド要求である場合、ルーチン５００は、決定ブロック５１０からブロック５２０に進み、受信されたコマンド要求と関連する１つ以上のコマンドを識別し、識別されたコマンドを実行するための１つ以上のコンピューティングノードを識別する。いくつかの実施形態では、コマンド要求は、実行するためのコマンドを含んでもよく、またはコマンドは、要求で提供された他の情報に基づいて判定されてもよい（例えば、ルックアップテーブルを使用して、ハイレベル命令と関連する１つ以上のコマンドを判定するなど）。同様に、コマンド要求は、識別されたコマンドを実行するためのコンピューティングノードのそれぞれの識別子を含んでもよく、または、コンピューティングノードは、要求で提供された他の情報（例えば、コンピューティングノード、仮想コンピュータネットワーク、コンピューティングリソースサービス等のグループの識別子）に基づいて判定されてもよい。種々の実施形態では、コマンド要求は、全ての識別されたコンピューティングノード上で識別された全てのコマンドを実行するためのものであってもよいが、他の実施形態では、識別されたコマンドの第１サブセットは、識別されたコンピューティングノードの第１サブセット上で実行されてもよく、識別されたコマンドの第２のサブセットは、識別されたコンピューティングノードの第２のサブセット上で実行されてもよい。しかしながら、実施形態は、そのように限定されるものではなく、コマンド及び／またはコンピューティングノードの他の数のサブセットは、コマンド要求において提供されてもよい。

【００５９】

ブロック５２０の次に、ルーチン５００はブロック５２５に進み、下記により詳細に説明される、図６の許可ブローカールーチン６００を行う。しかしながら、簡潔に説明すると、許可ブローカールーチン６００は、ユーザ（ブロック５０５でコマンド要求を提供した）がいずれかの識別されたコンピューティングノード（複数可）上のいずれかの識別されたコマンド（複数可）を実行することが承認されたどうかの指示を返す。

【００６０】

ブロック５２５の次に、ルーチンは、決定ブロック５３０に進み、ブロック５２５で受

信された情報に基づいて、識別されたコンピューティングノード（複数可）上で識別されたコマンド（複数可）を実行することが承認されたかどうかを判定する。ユーザが承認された場合、ルーチン５００は決定ブロック５３０からブロック５３５に進み、そうでなければ、ルーチン５００は、決定ブロック５３０からブロック５５５に進む。

【００６１】

ブロック５５５では、ユーザがブロック５２０で識別されたコンピューティングノードの１つ以上のコマンド要求に関する１つ以上のコマンドを行うことが承認されないことのレポートが、ユーザに提供される。ブロック５５５の次に、ルーチン５００は決定ブロック５６０に進む。

【００６２】

ユーザが決定ブロック５３０で承認された場合、ルーチン５００は決定ブロック５３０からブロック５３５に進み、承認されたコンピューティングノード（複数可）とやり取りし、その承認されたコンピューティングノード（複数可）に承認されたコマンドを実行させる。

【００６３】

ブロック５３５の次に、ルーチン５００は決定ブロック３４０に進み、承認されたコンピューティングノード（複数可）とやり取りし、該当する場合、承認されたコマンド（複数可）の実行時に承認されたコンピューティングノード（複数可）から結果を取得する。

【００６４】

ブロック３４０の次に、ルーチン５００は選択ブロック５４５に進み、承認されたコンピューティングノード（複数可）から結果を集約する。選択ブロック５４５の次に、ルーチン５００はブロック５５０に進み、（例えば、ユーザシェルアプリケーションを介して）結果をユーザに返す。

【００６５】

ブロック５１５、５５０、または５５５の次に、ルーチン５００は、決定ブロック５６０に進み、例えば、終了するための明確な指示が受信されるまで、またはユーザによって提供された指示と関連する各コマンドが行われた後及びユーザの許可が判定された後などに、ルーチンを継続し付加情報を処理するかどうかを判定する。継続すると判定された場合、ルーチン５００は、ブロック５０５に戻り、そうでなければ、ルーチン５００は終了する。

【００６６】

図６は、許可ブローカールーチン６００の例示的実施形態のフロー図を例示する。ルーチン６００は、例えば、図２のユーザコマンド実行インターフェースコンポーネント２０６及び／もしくは許可ブローカーモジュール２１４、図３のユーザコマンド実行インターフェースコンポーネント３４２及び／もしくは許可ブローカーモジュール３４６、ならびに／または図１のユーザコマンド実行インターフェースコンポーネント１１４もしくは１４５の実行によって提供されてもよい。これによって、ユーザアクセスを提供しユーザアクセス可能コンピューティングリソース上でコマンド及び関連機能を行うための説明された技術等の一部を行う。

【００６７】

ルーチン６００は、ブロック６０５で始まり、そこで、１つ以上のコマンド、ユーザＩＤ、及び１つ以上のコマンドを実行するための１つ以上のコンピューティングノードのＩＤが受信される。コマンド及びコンピューティングノードは、図５のルーチン５００のブロック５２０に識別されてもよい。そして、ユーザＩＤ（例えば、ユーザ名、ユーザ識別番号等）は、コマンドの指示とともに、図５のルーチン５００のブロック５０５に受信されてもよい。そうでなければ、ルーチンは、ユーザ名、パスワード、または他の識別／承認情報に関して、ユーザにクエリを行ってもよい。

【００６８】

ブロック６０５の次に、ルーチン６００は、決定ブロック６１０に進み、１つ以上のコ

ンピューティングノード上で１つ以上のコマンドを実行するためのユーザの許可を取得する。種々の実施形態では、ルーチンは、コンピューティングリソースサービスの許可リポジトリにアクセスし、ユーザの許可を取得してもよい。

【００６９】

ブロック６１０の次に、ルーチン６００は、決定ブロック６１５に進み、取得されたユーザの許可に基づいて識別されたコンピューティングノード（複数可）上で受信されたコマンド（複数可）を実行することが承認されたかどうかを判定する。ルーチン６００は、取得された許可を各コマンド／コンピューティングノードの組み合わせと比較する。ユーザが１つの識別されたコンピューティングノード（複数可）上の１つの受信されたコマンド（複数可）を実行することが承認されない場合、ルーチン６００は決定ブロック６１５からブロック６２０に進み、そうでなければ、ルーチン６００は決定ブロック６１５からブロック６２５に進む。

【００７０】

ブロック６２０では、ルーチン６００は、少なくとも１つのコンピューティングノード（複数可）上の少なくとも１つの受信されたコマンド（複数可）を実行することが承認されないことの指示を返す。この指示は、そのようなコマンド（複数可）が行われることを禁止、ブロックし、またはそうでなければ、防ぐために行われる。ブロック６２５では、ルーチン６００は、ユーザが識別されたコンピューティングノード（複数可）上で受信されたコマンド（複数可）を実行することが承認されたことの指示を返す。ブロック６２０または６２５の次に、ルーチンは終了する。

【００７１】

本開示の実施形態は、以下の条項を考慮して、説明されることができる。

１．コンピュータ実施方法であって、

１つ以上のコンピューティングシステム上で実行するシェルアグリゲータ（ｓｈｅｌｌ　ａｇｇｒｅｇａｔｏｒ）によって、第１のユーザによる使用のためにネットワークアクセス可能サービスによって提供される１つ以上のコンピューティングノードによって実行されるコマンドを指示する前記第１のユーザから要求を受信することと、

前記シェルアグリゲータによって及び記憶済み許可情報に少なくとも部分的に基づいて、前記第１のユーザが前記コマンドを前記１つ以上のコンピューティングノードによって実行させることを承認されたことを判定することと、

前記シェルアグリゲータによって及び前記判定することに応答して、前記１つ以上のコンピューティングノードによって前記コマンドの実行を開始することと、

を含む、前記コンピュータ実施方法。

【００７２】

２．前記１つ以上のコンピューティングシステムによって、前記１つ以上のコンピューティングノードによって実行される第２のコマンドを指示する前記第１のユーザから第２の要求を受信することと、

前記シェルアグリゲータによって及び前記記憶済み許可情報に少なくとも部分的に基づいて、前記第１のユーザが前記第２のコマンドを前記１つ以上のコンピューティングノードによって実行させることを承認されていないことを判定することと、

前記判定することに応答して、前記１つ以上のコンピューティングノードによる前記第２のコマンドの実行を拒否すること、

をさらに含む、条項１に記載のコンピュータ実施方法。

【００７３】

３．前記第１のユーザが承認されたことを前記判定することは、前記１つ以上のコンピューティングノードの外部の許可ブローカー（Ｐｅｒｍｉｓｓｉｏｎ　Ｂｒｏｋｅｒ）にクエリを行い、前記第１のユーザに特有の記憶済み許可情報を取得し、ならびに前記取得された記憶済み許可情報を前記コマンド及び前記１つ以上のコンピューティングノードと比較し、マッチを識別することを含む、条項１に記載のコンピュータ実施方法。

【００７４】

４.前記取得された記憶済み許可情報を前記コマンド及び前記１つ以上のコンピューティングノードと前記比較することは、前記コマンドを、前記取得された記憶済み許可情報に記憶された１つ以上の正規表現にマッチさせることを含む、条項３に記載のコンピュータ実施方法。

【００７５】

５.前記取得された記憶済み許可情報を前記コマンド及び前記１つ以上のコンピューティングノードと前記比較することは、前記コマンドを、前記取得された記憶済み許可情報に記憶された１つ以上のアクセス制御表現にマッチさせることを含む、条項３に記載のコンピュータ実施方法。

【００７６】

６.前記要求を前記受信することは、複数のコンピューティングノードのグループの指示を受信することを含み、前記コマンドの前記実行を前記開始することは、前記グループの各コンピューティングノードによって前記コマンドの前記実行を開始することを含む、条項１に記載のコンピュータ実施方法。

【００７７】

７．前記シェルアグリゲータによって、前記グループの前記複数のコンピューティングノードによる前記コマンドの実行から得られた複数の結果を受信することと、

前記シェルアグリゲータによって、前記受信された複数の結果を集約し、前記集約された結果を前記第１のユーザに返すことと、

をさらに含む、条項６に記載のコンピュータ実施方法。

【００７８】

８．前記コマンドの前記実行を前記開始する前に、前記シェルアグリゲータによって、前記１つ以上のコンピューティングノードへのシェルトランスポート層を介した１つ以上の安全な接続を確立することを含み、前記１つ以上のコンピューティングノードによる前記コマンドの前記実行を前記開始することは、前記シェルアグリゲータによって及び前記１つ以上のコンピューティングノードに、前記確立された安全な接続を介して前記コマンドを提供することをさらに含む、条項１に記載のコンピュータ実施方法。

【００７９】

９．前記１つ以上のコンピューティングノードは、複数のコンピューティングノードを含み、前記コマンドの前記実行は、現在のステータス情報を前記複数のコンピューティングノードから取得させ、及び第１のユーザに提供させる、条項１に記載のコンピュータ実施方法。

【００８０】

１０．前記１つ以上のコンピューティングノードは、複数のコンピューティングノードを含み、前記コマンドの前記実行は、前記複数のコンピューティングノード上で進行中の動作を修正する、条項１に記載のコンピュータ実施方法。

【００８１】

１１．前記要求を前記受信することは、複数のコマンドに対応するハイレベル指図を受信することを含み、前記実行を前記開始することは、前記複数のコマンドを識別することと、前記１つ以上のコンピューティングノードのそれぞれによって前記複数のコマンドのそれぞれの実行を開始することと、をさらに含む、条項１に記載のコンピュータ実施方法。

【００８２】

１２．記憶済みコンテンツを有する非一過性コンピュータ可読媒体であって、コンピューティングシステムに、少なくとも、

前記コンピューティングシステムによって、ネットワークアクセス可能サービスから提供された１つ以上のコンピューティング関連リソースのために実行するコマンドを指示する第１のユーザから情報を受信させ、

前記コンピューティングシステムによって、及び前記１つ以上のコンピューティング関連リソースに外部で記憶された前記第１のユーザに関する許可情報に少なくとも部分的に

基づいて、前記第１のユーザが前記１つ以上のコンピューティング関連リソースに関する前記コマンドを実行することが承認されたことを判定させ、
前記コンピューティングシステムによって、前記１つ以上のコンピューティング関連リソースに関する前記コマンドの実行を開始させる、
前記非一過性コンピュータ可読媒体。
【００８３】
１３．前記１つ以上のコンピューティング関連リソースは、複数のコンピューティングノードを含み、前記記憶済みコンテンツは、実行時、前記コンピューティングシステムに、

複数のコンピューティングノードのそれぞれに、前記コマンドを実行させ、現在のステータス情報を、前記複数のコンピューティングノードから前記コンピューティングシステム上で実行するシェルアグリゲータに提供させることと、
前記シェルアグリゲータによって、前記現在のステータス情報を前記複数のコンピューティングノードから集約することと、
前記集約された現在のステータス情報を前記第１のユーザに提供することと、
によって、前記コマンドの前記実行を前記開始することを行わせるソフトウェア命令をさらに含む、条項１２に記載の非一過性コンピュータ可読媒体。
【００８４】
１４．前記１つ以上のコンピューティング関連リソースは、複数のコンピューティングノードを含み、前記コマンドの前記実行を前記開始することは、前記複数のコンピューティングノードそれぞれに前記コマンドを実行させることによって、前記複数のコンピューティングノードの動作を改変することを含む、条項１２に記載の非一過性コンピュータ可読媒体。
【００８５】
１５．前記情報を前記受信することは、前記第１のユーザの第１の記憶済みの許可情報と異なる第２の記憶済みの許可情報を伴う、定義された役割を有する異なる第２のユーザの指示を受信することを含み、前記第１のユーザが承認されたことを前記判定することは、前記異なる第２のユーザの前記定義された役割を想定することを前記第１のユーザに許可することを判定することに基づいて、及び前記１つ以上のコンピューティング関連リソースに関する前記コマンドを実行することが前記定義された役割の前記第２の記憶済み許可情報によって許可されることに基づいて行われる、条項１２に記載の非一過性コンピュータ可読媒体。
【００８６】
１６．前記１つ以上のコンピューティング関連リソースに関する前記コマンドの前記実行は、前記第１のユーザと関連する第１の許可レベルで行われ、前記受信された情報は、前記１つ以上のコンピューティング関連リソースに対して実行するための第２のコマンドをさらに指示し、前記記憶済みコンテンツは、さらに、前記コンピューティングシステムに、

前記記憶済み許可情報に少なくとも部分的に基づいて、前記第１のユーザが前記第１の許可レベルで前記１つ以上のコンピューティング関連リソースに関する前記第２のコマンドを実行することが承認されないことを判定させ、
前記コンピューティングシステムによって、前記第１の許可レベルよりも高く及び前記１つ以上のコンピューティング関連リソースに関する前記第２のコマンドを実行することが承認される、第２の許可レベルを識別させ、
前記第２の許可レベルで、前記１つ以上のコンピューティング関連リソースに関する前記第２のコマンドの前記実行を開始させる、
条項１２に記載の非一過性コンピュータ可読媒体。
【００８７】
１７．前記記憶済みコンテンツは、さらに、前記コンピューティングシステムに、
前記コンピューティングシステムによって、許可を一時的にロックし前記１つ以上のコ

ンピューティング関連リソースに関するコマンドの実行を禁止する命令を受信させ、
前記コンピューティングシステムによって、前記１つ以上のコンピューティング関連リソースに対して実行するための第２のコマンドを指示する前記第１のユーザからさらなる情報を受信させ、
前記コンピューティングシステムによって及び前記一時的にロックされた許可に基づいて、前記１つ以上のコンピューティング関連リソースに関する前記第２のコマンドを実行するための承認を拒否させる、
条項１２に記載の非一過性コンピュータ可読媒体。
【００８８】
１８．前記１つ以上のコンピューティング関連リソースのノードは、第１及び第２のコンピューティングノードを含み、前記コマンドの前記実行を前記開始することは、
前記第１コンピューティングノードによって、及び追加の安全検証をすることなく、第１のユーザに関する前記コマンドを行うことと、
前記第２のコンピューティングノードによって、前記第２のコンピューティングノード上で記憶された追加のセキュリティ情報は、前記第２のコンピューティングノードによって、前記第１のユーザに関する前記コマンドを行うことを許可しないことを識別することと、
前記第２のコンピューティングノート及び前記識別することに基づいて、前記第２のコンピューティングノードによって前記第１のユーザに関する前記コマンドの遂行を拒否することと、
を含む、条項１２に記載の非一過性コンピュータ可読媒体。
【００８９】
１９．前記記憶済みコンテンツは、前記コンピューティングシステムに、前記第１のユーザが承認されたことを前記判定する前に、前記第１のユーザを含む複数のユーザのグループのアクセスを制御する第２のユーザから、前記１つ以上のコンピューティング関連リソースを含むコンピューティング関連リソースのグループへの、前記許可情報を受信させ、前記許可情報は、前記第１のユーザに特有の１つ以上の許可を含む、条項１２に記載の非一過性コンピュータ可読媒体。
【００９０】
２０．前記コンピューティング関連リソースのグループは、前記ネットワークアクセス可能サービスによって、前記第１のユーザに提供される仮想コンピュータネットワークと関連する複数のコンピューティング関連リソースを含み、１人以上のユーザによって指定される共通タグを共有する複数のコンピューティング関連リソースを含み、または共通地理的位置に複数のコンピューティング関連リソースを含む、条項１９に記載の非一過性コンピュータ可読媒体。
【００９１】
２１．システムであって、
１つ以上のコンピューティングシステムの１つ以上のプロセッサと、
実行時に、前記１つ以上のプロセッサの少なくとも１つによって、ソフトウェア命令を記憶する１つ以上のメモリと、を備え、前記ソフトウェア命令は、前記少なくとも１つのプロセッサに、
第１のユーザによる使用のために提供される１つ以上のコンピューティングノードによって実行されるコマンドを指示する前記第１のユーザから要求を受信することと、
前記１つ以上のコンピューティングノードとやり取りすることなく、前記第１のユーザが前記コマンドを前記１つ以上のコンピューティングノードによって実行させることを承認されたことを判定することと、
前記判定することに基づいて、前記１つ以上のコンピューティングノードによる前記コマンドの実行を開始することと、
によってコマンドの実行を管理させる、前記システム。
【００９２】

２２．前記１つ以上のコンピューティングシステムは、前記第１のユーザに関する許可情報を記憶し、及び前記判定することに関する前記記憶済みの許可情報を使用する、ネットワークアクセス可能サービスの一部であり、

前記１つ以上のコンピューティングノードは、前記第１のユーザによる一時使用のために前記ネットワークアクセス可能サービスによって提供される、条項２１に記載のシステム。

【００９３】

本明細書の他の箇所で説明されるように、承認は、個別のコマンド／コンピューティングノードの組み合わせに対してされてもよく、または、全部のコマンド要求に対してされてもよい。図５及び図６の例示されたルーチン５００及び６００は、それぞれ、承認が全部のコマンド要求に対して判定され、これにより、ユーザが１つのコンピューティングノード上で１つのコマンドを実行することが承認されない場合、ルーチン６００はルーチン５００に戻る（つまり、ユーザがコマンド要求に対してコンピューティングノード（複数可）上でコマンド（複数可）を実行することが承認されない）、シナリオを説明する。他の種々の実施形態では、承認は、個別のコマンド／コンピューティングの組み合わせに対してされてもよく、このため、ルーチン６００はルーチン５００に戻り、ルーチンは、ユーザが承認された各コマンド／コンピューティングノードの組み合わせ、及び／またはユーザが承認されない各コマンド／コンピューティングノードの組み合わせに対して行われる。このように、ルーチン５００のブロック５３５、５４０、５４５、及び５５０は、承認されたコマンド／コンピューティングノードの組み合わせごとに採用されてもよく、ブロック５５５は、承認されないコマンド／コンピューティングノードの組み合わせごとに採用されてもよい。

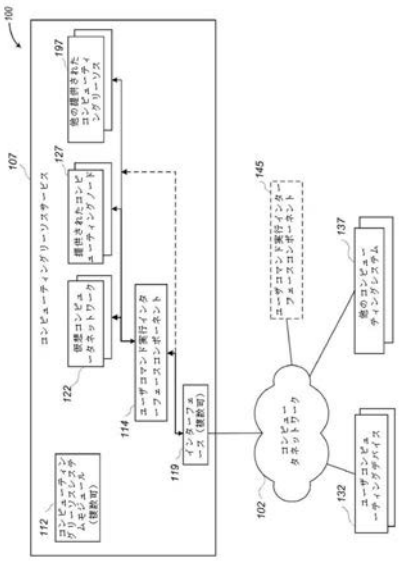
【００９４】

また、いくつかの実施形態では、上記で議論されたルーチンによって提供される機能は、より多くのルーチンにおいて分割され、またはより少ないルーチンに統合されるような、代替的方法で提供されてもよいことを理解されたい。同様に、いくつかの実施形態では、例示されたルーチンは、他の例示されるルーチンがそれぞれ、そのような機能がむしろ不足し、もしくはそれを含むとき、または提供された機能数が改変されるなどのときに、説明されるものよりも多いまたは少ない数の機能を提供してもよい。また、種々の動作は、特定の様式（例えば、連続して、または同時に）及び／または特定の順番で行われるように例示され得る一方で、当業者は、他の実施形態で、動作が他の順番及び他の様式で行われる場合があることを理解するはずである。当業者は、また、上記で議論されたデータ構造は、単一のデータ構造を複数のデータ構造に分割させることによって、または複数のデータ構造を単一のデータ構造に統合させることによって、異なる様式で構造化されてもよいことを理解するはずである。同様に、いくつかの実施形態では、例示されたデータ構造は、他の例示されるデータ構造がそれぞれ、そのような情報がむしろ不足し、もしくはそれを含むとき、または記憶された情報の量もしくは種類が改変されるなどのときに、説明されるものよりも多いまたは少ない量の情報を記憶しもよい。

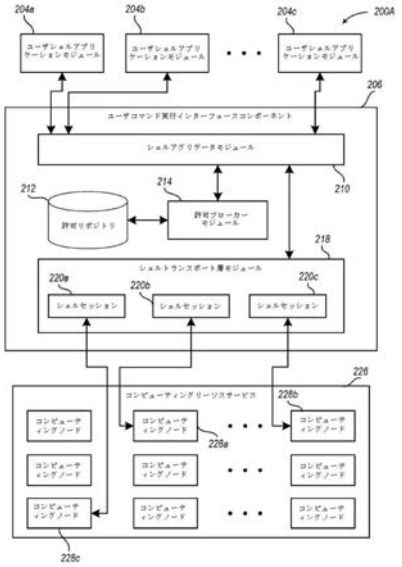
【００９５】

前述から、特有の実施形態が例証目的のために本明細書に説明されているが、本発明の趣旨及び範囲から逸脱することなく、種々の修正がされてもよいことを理解されたい。したがって、本発明は、添付の請求項及びそこに列挙される要素によるものを除いて、限定されない。また、本発明の一定の態様は、一定の請求様式で下記に提示される一方、本発明者は、いずれかの利用可能である請求様式で、本発明の種々の態様を熟考している。例えば、本発明の一部の態様だけが、現時点で、コンピュータ可読媒体に具体化されるように列挙され得る一方、同様に、他の態様もそのように具体化される場合がある。

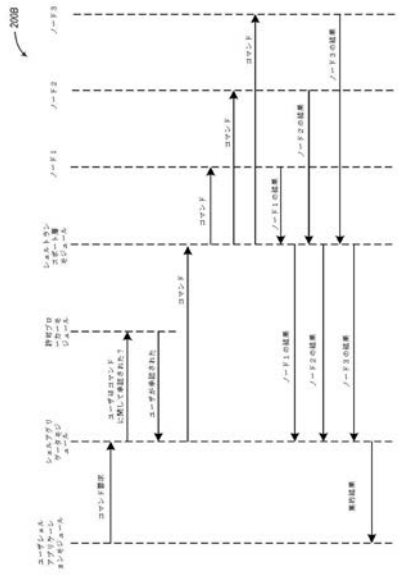
【図１】



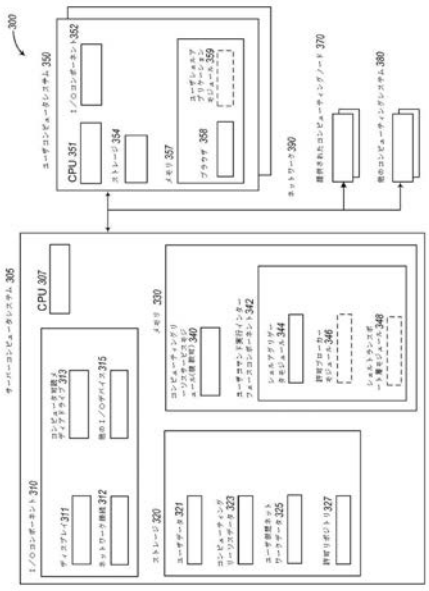
【図２Ａ】



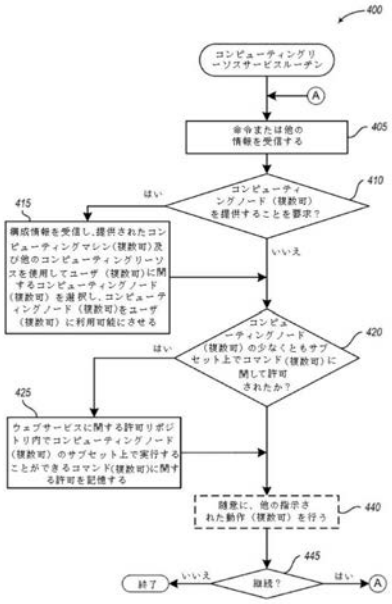
【図２Ｂ】



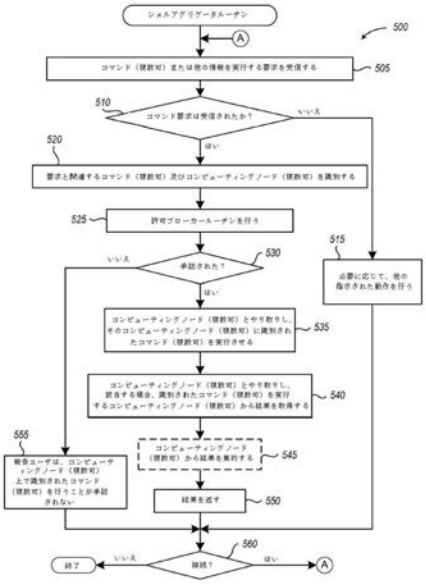
【図３】



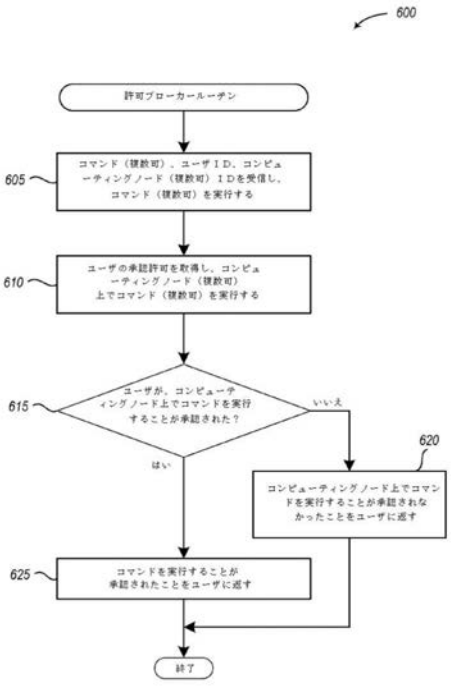
【図４】


400
コンピューティングリソースサービスルーチン
A
命令または他の情報を受信する
405
コンピューティングノード（複数可）を提供することを要求？
410
はい
いいえ
415
構成情報を受信し、提供されたコンピューティングマシン（複数可）及び他のコンピューティングリソースを使用してユーザ（複数可）に関するコンピューティングノード（複数可）を選択し、コンピューティングノード（複数可）をユーザ（複数可）に利用可能にさせる
コンピューティングノード（複数可）の少なくともサブセット上でコマンド（複数可）に関して許可されたか？
420
はい
425
ウェブサービスに関する許可リポジトリ内でコンピューティングノード（複数可）のサブセット上で実行することができるコマンド（複数可）に関する許可を記憶する
随意に、他の指示された動作（複数可）を行う
440
445
終了
いいえ
継続？
はい
A

【図５】


シェルアグリゲータールーチン
A
500
コマンド（複数可）または他の情報を実行する要求を受信する
505
510
コマンド要求は受信されたか？
いいえ
はい
520
要求と関連するコマンド（複数可）及びコンピューティングノード（複数可）を識別する
525
許可ブローカールーチンを行う
515
必要に応じて、他の指示された動作を行う
承認された？
530
いいえ
はい
コンピューティングノード（複数可）とやり取りし、そのコンピューティングノード（複数可）に識別されたコマンド（複数可）を実行させる
535
コンピューティングノード（複数可）とやり取りし、該当する場合、識別されたコマンド（複数可）を実行するコンピューティングノード（複数可）から結果を取得する
540
555
要求ユーザは、コンピューティングノード（複数可）上で識別されたコマンド（複数可）を行うことが承認されない
コンピューティングノード（複数可）から結果を実行する
545
結果を返す
550
560
終了
いいえ
継続？
はい
A

【図６】


600
許可ブローカールーチン
605
コマンド（複数可）、ユーザＩＤ、コンピューティングノード（複数可）ＩＤを受信し、コマンド（複数可）を実行する
610
ユーザの承認許可を取得し、コンピューティングノード（複数可）上でコマンド（複数可）を実行する
615
ユーザが、コンピューティングノード上でコマンドを実行することが承認された？
いいえ
はい
620
コンピューティングノード上でコマンドを実行することが承認されなかったことをユーザに返す
625
コマンドを実行することが承認されたことをユーザに返す
終了

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/039018

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/08 G06F9/455 G06F9/50 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 9 009 217 B1 (NAGARGADDE APARNA [US] ET AL) 14 April 2015 (2015-04-14) column 1, lines 5-30 column 2, lines 25-35 column 18, lines 5-65 column 19, lines 10-30 column 19, lines 40-65 column 20, lines 20-40 figures 9-10 ----- -/--	1-15

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 September 2016	21/09/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Erdene-Ochir, O

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/039018

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7 475 419 B1 (BASU SUJOY [US] ET AL) 6 January 2009 (2009-01-06) column 1, lines 10-65 column 6, lines 10-20 column 7, lines 30-65 column 8, lines 1-65 column 9, lines 1-35 columns 10-11, lines 1-65 claims 1,6,8 figures 2-5, 6A, 7	1-15
A	US 2005/027863 A1 (TALWAR VANISH [US] ET AL) 3 February 2005 (2005-02-03) paragraph [0014] paragraphs [0016] - [0017] paragraphs [0019] - [0020] paragraph [0023] claims 1, 11 figure 1	1-15
A	US 2014/075029 A1 (LIPCHUK MAOR [IL] ET AL) 13 March 2014 (2014-03-13) paragraph [0002] paragraph [0019] paragraph [0023] paragraph [0026] paragraph [0055] claim 1 figure 2	1-15

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/039018

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 9009217 B1	14-04-2015	US 9009217 B1	14-04-2015
		US 2015288750 A1	08-10-2015
US 7475419 B1	06-01-2009	NONE	
US 2005027863 A1	03-02-2005	NONE	
US 2014075029 A1	13-03-2014	NONE	

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

（特許庁注：以下のものは登録商標）
１．ＷＩＮＤＯＷＳ

(72)発明者 チャン キャサリン イチェン
アメリカ合衆国 ９８１０９－５２１０ ワシントン州 シアトル テリー アヴェニュー ノース ４１０
Ｆターム(参考) 5B376 AE20 AE44 AE67

【要約の続き】
ィングノードから結果を集約してもよい。
【選択図】図２Ａ