(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5800389号
(P5800389)
(45)発行日　平成27年10月28日(2015.10.28)　(24)登録日　平成27年9月4日(2015.9.4)

(51)Int.Cl.　　F I
G06F 21/62 (2013.01)　　G06F 21/62　318
G06F 12/00 (2006.01)　　G06F 12/00　537A

請求項の数 25　(全 26 頁)

(21)出願番号　特願2011-257055(P2011-257055)
(22)出願日　平成23年11月25日(2011.11.25)
(65)公開番号　特開2012-138078(P2012-138078A)
(43)公開日　平成24年7月19日(2012.7.19)
審査請求日　平成26年6月11日(2014.6.11)
(31)優先権主張番号　12/979117
(32)優先日　平成22年12月27日(2010.12.27)
(33)優先権主張国　米国(US)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】クラウド・コンピューティング環境に保管されたデータに関するきめ細かい任意アクセス制御の有効化のための方法、システム、およびコンピュータ・プログラム

(57)【特許請求の範囲】
【請求項１】
電子データ・ファイルを表す複数のデータ・アーティファクトと、
クラウド・コンピューティング・モデルに応じて動作するように構成された複数のクラウド・サービス・プロバイダと、
前記複数のデータ・アーティファクトの保管およびアクセスを管理するように構成されたデータ・ストレージと、
前記データ・ストレージによって管理される前記複数のデータ・アーティファクトに対する任意アクセス制御を提供するように構成されたアクセス・マネージャであって、前記任意アクセス制御が前記データ・ストレージによって実行されるアクセス制御操作に加えて実行され、前記アクセス・マネージャの前記任意アクセス制御が前記データ・ストレージによって行われたアクセス許可およびアクセス拒否を撤回することができる、前記アクセス・マネージャと
を含む、システム。
【請求項２】
前記データ・ストレージが、
前記複数のデータ・アーティファクトのアクセスに関する制限を定義する複数のデータ処理規則であって、前記データ・ストレージが前記複数のデータ処理規則を使用して、データ・アーティファクトへのアクセスを要求するデータ・コンシューマに関するアクセス許可およびアクセス拒否のうちの少なくとも一方を決定する、前記複数のデータ処理規則

をさらに含む、請求項１記載のシステム。
【請求項３】
前記アクセス・マネージャが、
データ・アーティファクトへのアクセスを制限する少なくとも１つのパラメータ値を定義する複数の所有者指定のアクセス規則と、
前記データ・アーティファクトへのアクセスを許可する条件を定義する複数の所有者指定のアクセス例外であって、前記アクセスが前記データ・ストレージおよび少なくとも１つの所有者指定のアクセス規則のうちの少なくとも一方によって拒否される、前記複数の所有者指定のアクセス例外と
をさらに含む、請求項１又は２に記載のシステム。
【請求項４】
所有者指定のアクセス例外に関連する認証情報を妥当性検査するように構成された認証部であって、前記アクセス・マネージャによって有効な認証データを受信することを条件に、前記データ・アーティファクトへのアクセスが可能になる、前記認証部
をさらに含む、請求項１乃至３のいずれか一項に記載のシステム。
【請求項５】
前記認証部が、前記認証情報を自動的に生成するようにさらに構成される、請求項４記載のシステム。
【請求項６】
前記認証部が、厳密認証プロセスを使用するように構成される、請求項４又は５に記載のシステム。
【請求項７】
前記複数の所有者指定のアクセス規則および前記複数の所有者指定のアクセス例外の定義を可能にするように構成されたアクセス・マネージャ・サービス・ユーザ・インターフェースをさらに含む、請求項３に記載のシステム。
【請求項８】
コンピュータが、
データ要求および前記データ要求に関する応答メッセージを入手することであって、前記応答メッセージが前記データ要求に応答してデータ・ストレージによって生成され、前記応答メッセージが前記データ・ストレージによって保管されたデータ・アーティファクトへのアクセスの許可および拒否のうちの少なくとも一方を示す、前記入手することと、
前記データ要求に対して適用可能な少なくとも１つの所有者指定のアクセス規則および少なくとも１つの所有者指定のアクセス例外のうちの少なくとも一方の存在を識別することと、
前記識別された少なくとも１つの所有者指定のアクセス規則および少なくとも１つの所有者指定のアクセス例外に基づいて前記データ要求に対するアクセス応答を決定することであって、前記アクセス応答が前記データ要求で要求された前記データ・アーティファクトへのアクセスの前記許可および前記拒否のうちの少なくとも一方を示し、所有者指定のアクセス規則が前記データ・アーティファクトへのアクセスを制限する少なくとも１つのパラメータ値を定義し、所有者指定のアクセス例外が前記データ・アーティファクトへのアクセスを許可する条件を定義し、前記データ・ストレージおよび少なくとも１つの所有者指定のアクセス規則のうちの少なくとも一方によって前記アクセスが拒否される、前記決定することと、
前記決定されたアクセス応答を前記応答メッセージと比較することと、
前記決定されたアクセス応答が前記応答メッセージと一致しない場合に、前記決定されたアクセス応答を表すために前記応答メッセージをオーバライドすることと、
前記決定されたアクセス応答が前記応答メッセージと一致する場合に、前記データ要求の発信エンティティに前記応答メッセージを伝達することと
を実行することを含む、方法。
【請求項９】

前記データ要求および応答メッセージを入手することが、
前記データ・ストレージによる前記データ要求の受信を検出することと、
前記データ・ストレージから前記データ要求のコピーを要求することと
をさらに含む、請求項８記載の方法。
【請求項１０】
前記データ要求および応答メッセージを入手することが、
前記データ・ストレージによる前記応答メッセージの送信を検出することと、
前記応答メッセージの前記送信をインターセプトすることと
をさらに含む、請求項８記載の方法。
【請求項１１】
前記識別の結果、所有者指定のアクセス例外の前記存在が判明した場合に、前記コンピュータが、
前記データ要求の前記発信エンティティから認証データを要求することと、
前記認証データの受信次第、前記認証データを妥当性検査することと、
前記認証データが有効と判断された場合に、前記所有者指定のアクセス例外を表すために前記応答メッセージを直ちにオーバライドすることと
をさらに実行することを含む、請求項８乃至１０のいずれか一項に記載の方法。
【請求項１２】
前記コンピュータが、
前記所有者指定のアクセス例外が、アクセス・マネージャ・サービスによる使用のためにアクティブのままであるべきかどうかを査定することと、
前記所有者指定のアクセス例外がアクティブのままであるべきではないと査定された場合に、前記所有者指定のアクセス例外を自動的に非活動化することであって、前記所有者指定のアクセス例外が前記アクセス・マネージャ・サービスによる使用のために使用不能である、前記非活動化ことと
をさらに実行することを含む、請求項８乃至１１のいずれか一項に記載の方法。
【請求項１３】
前記コンピュータが、
前記認証データが無効と判断された場合に、前記データ要求の前記発信エンティティに前記無効認証データを通知することと、
前記発信エンティティからの認証データの前記要求および妥当性検査を繰り返すことと
をさらに実行することを含む、請求項１１に記載の方法。
【請求項１４】
前記アクセス応答を決定することが、
前記少なくとも１つの識別された所有者指定のアクセス規則を集約することと、
所有者指定のアクセス規則の前記集約内の矛盾の存在を識別することであって、少なくとも２つの所有者指定のアクセス規則のパラメータ値が相互に排他的である場合に前記少なくとも２つの所有者指定のアクセス規則が矛盾していると見なされる、前記識別することと、
前記矛盾が存在する場合に、矛盾しているものとして識別されたそれぞれの所有者指定のアクセス規則に関連する優先順位の値を使用して前記矛盾を解決することであって、最も高い優先順位の値を有する所有者指定のアクセス規則がより低い優先順位の値を有する所有者指定のアクセス規則より優先的に使用され、前記より低い優先順位の値を有する前記所有者指定のアクセス規則が所有者指定のアクセス規則の前記集約から除去される、前記解決することと、
所有者指定のアクセス規則の前記集約によって表されたパラメータ値に対応する前記データ要求からのデータ値を比較することと、
前記データ値が前記パラメータ値を満足することを前記比較が示す場合に、前記データ・アーティファクトへのアクセスの前記拒否として前記アクセス応答を設定することと、
前記パラメータ値が前記データ値によって満足されないことを前記比較が示す場合に、

前記データ・アーティファクトへのアクセスの前記許可として前記アクセス応答を設定することと
をさらに含む、請求項８乃至１３のいずれか一項に記載の方法。
【請求項１５】
前記応答メッセージの前記オーバライドが、
前記データ要求について前記データ・ストレージによって作成されたセッションの少なくとも１つのパラメータに対する変更を遂行することであって、前記少なくとも１つのパラメータが前記セッションに許可されたアクセスを制御する、前記遂行することと、
前記決定されたアクセス応答を反映するように前記応答メッセージを変更することと、
前記データ要求の前記発信エンティティに前記応答メッセージを伝達することと
をさらに含む、請求項８乃至１４のいずれか一項に記載の方法。
【請求項１６】
コンピュータ・プログラムであって、コンピュータにより実行されることにより、前記コンピュータに、
データ要求および前記データ要求に関する応答メッセージを入手することであって、前記応答メッセージが前記データ要求に応答してデータ・ストレージによって生成され、前記応答メッセージが前記データ・ストレージによって保管されたデータ・アーティファクトへのアクセスの許可および拒否のうちの少なくとも一方を示す、前記入手することと、
前記データ要求に対して適用可能な少なくとも１つの所有者指定のアクセス規則および少なくとも１つの所有者指定のアクセス例外のうちの少なくとも一方の存在を識別することと、
前記識別された少なくとも１つの所有者指定のアクセス規則および少なくとも１つの所有者指定のアクセス例外に基づいて前記データ要求に対するアクセス応答を決定することであって、前記アクセス応答が前記データ要求で要求された前記データ・アーティファクトへのアクセスの前記許可および前記拒否のうちの少なくとも一方を示し、所有者指定のアクセス規則が前記データ・アーティファクトへのアクセスを制限する少なくとも１つのパラメータ値を定義し、所有者指定のアクセス例外が前記データ・アーティファクトへのアクセスを許可する条件を定義し、前記データ・ストレージおよび少なくとも１つの所有者指定のアクセス規則のうちの少なくとも一方によって前記アクセスが拒否される、前記決定することと、
前記決定されたアクセス応答を前記応答メッセージと比較することと、
前記決定されたアクセス応答が前記応答メッセージと一致しない場合に、前記決定されたアクセス応答を表すために前記応答メッセージをオーバライドすることと、
前記決定されたアクセス応答が前記応答メッセージと一致する場合に、前記データ要求の発信エンティティに前記応答メッセージを伝達することと
を実行させる、前記コンピュータ・プログラム。
【請求項１７】
前記識別の結果、所有者指定のアクセス例外の前記存在が判明した場合に、前記コンピュータに、
前記データ要求の前記発信エンティティから認証データを要求することと、
前記認証データの受信次第、前記認証データを妥当性検査することと、
前記認証データが有効と判断された場合に、前記所有者指定のアクセス例外を表すために前記応答メッセージを直ちにオーバライドすることと
をさらに実行させる、請求項１６記載のコンピュータ・プログラム。
【請求項１８】
前記コンピュータに、
前記認証データが無効と判断された場合に、前記データ要求の前記発信エンティティに前記無効認証データを通知することと、
前記発信エンティティからの認証データの前記要求および妥当性検査を繰り返すことと
をさらに実行させる、請求項１７記載のコンピュータ・プログラム。

【請求項１９】
前記アクセス応答を決定することが、
前記少なくとも１つの識別された所有者指定のアクセス規則を集約することと、
所有者指定のアクセス規則の前記集約内の矛盾の存在を識別することであって、少なくとも２つの所有者指定のアクセス規則のパラメータが相互に排他的である場合に前記少なくとも２つの所有者指定のアクセス規則が矛盾していると見なされる、前記識別することと、
前記矛盾が存在する場合に、矛盾しているものとして識別されたそれぞれの所有者指定のアクセス規則に関連する優先順位の値を使用して前記矛盾を解決することであって、最も高い優先順位の値を有する所有者指定のアクセス規則がより低い優先順位の値を有する所有者指定のアクセス規則より優先的に使用され、前記より低い優先順位の値を有する前記所有者指定のアクセス規則が所有者指定のアクセス規則の前記集約から除去される、前記解決することと、
所有者指定のアクセス規則の前記集約によって表されたパラメータ値に対応する前記データ要求からのデータ値を比較することと、
前記データ値が前記パラメータ値を満足することを前記比較が示す場合に、前記データ・アーティファクトへのアクセスの前記拒否として前記アクセス応答を設定することと、
前記パラメータ値が前記データ値によって満足されないことを前記比較が示す場合に、前記データ・アーティファクトへのアクセスの前記許可として前記アクセス応答を設定することと
をさらに含む、請求項１６乃至１８のいずれか一項に記載のコンピュータ・プログラム。
【請求項２０】
アクセス・マネージャを含むコンピュータが、
データ・ストレージによりデータ要求を受信することであって、前記データ要求がクラウド・ストレージによって保管されたデータ・アーティファクトへのアクセスを要求する、前記受信することと、
前記データ・ストレージにより前記データ要求に対する応答を決定することであって、前記決定が前記データ・アーティファクトへのアクセスを許可することおよびアクセスを拒否することのうちの少なくとも一方を示すことと、
前記アクセス・マネージャにより前記データ・ストレージによる前記データ要求の受信を検出する、前記決定することと、
前記アクセス・マネージャにより、前記決定された応答の実行前に前記データ・ストレージによる前記データ要求の処理に割り込むことと、
前記アクセス・マネージャにより、前記データ要求のコピーおよび前記データ・ストレージの応答を入手することと、
前記データ・アーティファクトについて定義された任意アクセス制御に関して、前記アクセス・マネージャにより前記データ要求の前記コピーの内容を評価することであって、前記任意アクセス制御が前記データ・アーティファクトに関連するエンティティによって構成される、前記評価することと、
前記アクセス・マネージャにより前記データ要求コピーの前記評価からの応答を決定することであって、前記決定が前記データ・アーティファクトへのアクセスを許可することおよびアクセスを拒否することのうちの少なくとも一方を示す、前記決定することと、
前記データ・ストレージによって決定された前記応答を前記アクセス・マネージャによって内部で決定された前記応答と比較することと、
前記比較が前記データ・ストレージと前記アクセス・マネージャの前記応答間の不一致を示す場合に、前記アクセス・マネージャにより前記データ・ストレージの応答をオーバライドすることであって、前記アクセス・マネージャによって決定された前記応答が前記データ・ストレージによって決定された前記応答より優先される、前記オーバライドすることと、
前記比較が前記データ・ストレージと前記アクセス・マネージャの前記応答間の一致を

示す場合に、前記アクセス・マネージャにより前記データ・ストレージによる前記データ要求の処理に対する前記割り込みをリリースすることであって、前記データ・ストレージが前記データ要求の履行を完了できるようになる、前記リリースすることと
を実行することを含む、方法。
【請求項２１】
前記データ・ストレージによる前記データ要求の処理に対する割り込みが、
前記アクセス・マネージャにより、前記データ・ストレージから前記データ要求の発信エンティティへの前記応答の送信を検出することと、
前記アクセス・マネージャにより前記送信をインターセプトすることと
をさらに含む、請求項２０記載の方法。
【請求項２２】
前記データ要求コピーの前記内容を評価することが、
前記アクセス・マネージャにより前記データ要求に対して適用可能な少なくとも１つの所有者指定のアクセス例外の存在を識別することであって、所有者指定のアクセス例外が前記任意アクセス制御によって使用され、前記所有者指定のアクセス例外が、そうでなければ前記データ・ストレージおよび前記任意アクセス制御のうちの少なくとも一方によって拒否される前記データ・アーティファクトへのアクセスを許可する条件を定義する、前記識別することと、
前記少なくとも１つの適用可能な所有者指定のアクセス例外が存在する場合に、前記アクセス・マネージャにより前記データ要求コピーの前記発信エンティティから認証データを要求することと、
前記認証データの受信次第、前記アクセス・マネージャにより前記認証データを妥当性検査することと、
前記認証データが有効と判断された場合に、前記アクセス・マネージャにより前記データ・ストレージの応答を直ちにオーバライドすることであって、前記アクセス・マネージャによって決定された前記応答が前記データ・ストレージによって決定された前記応答より優先される、前記オーバライドすることと
をさらに含む、請求項２１に記載の方法。
【請求項２３】
前記少なくとも１つの所有者指定のアクセス例外が存在しない場合に、前記コンピュータが、
前記アクセス・マネージャにより前記データ要求コピーに対して適用可能な少なくとも１つの所有者指定のアクセス規則の存在を識別することであって、所有者指定のアクセス規則が前記任意アクセス制御によって使用され、前記所有者指定のアクセス規則が前記データ・アーティファクトへのアクセスを制限する少なくとも１つのパラメータ値を定義する、前記識別することと、
前記少なくとも１つの適用可能な所有者指定のアクセス規則が存在する場合に、前記アクセス・マネージャにより前記少なくとも１つの適用可能な所有者指定のアクセス規則を集約することと、
前記アクセス・マネージャにより適用可能な所有者指定のアクセス規則の前記集約内の矛盾の存在を識別することであって、少なくとも２つの適用可能な所有者指定のアクセス規則のパラメータ値が相互に排他的である場合に前記少なくとも２つの所有者指定のアクセス規則が矛盾していると見なされることと、
前記矛盾が存在する場合に、前記アクセス・マネージャにより矛盾しているものとして識別されたそれぞれの所有者指定のアクセス規則に関連する優先順位の値を使用して前記矛盾を解決することであって、最も高い優先順位の値を有する前記所有者指定のアクセス規則がより低い優先順位の値を有する所有者指定のアクセス規則より優先的に使用され、前記より低い優先順位の値を有する前記所有者指定のアクセス規則が適用可能な所有者指定のアクセス規則の前記集約から除去される、前記識別することと、
前記アクセス・マネージャにより適用可能な所有者指定のアクセス規則の前記集約によ

って表されたパラメータ値に対応する前記データ要求からのデータ値を比較することであって、前記データ値が前記パラメータ値を満足することが前記データ・アーティファクトへのアクセスの拒否を示す、前記比較することと
をさらに実行することを含む、請求項２２記載の方法。
【請求項２４】
前記データ・ストレージの応答をオーバライドすることが、
前記アクセス・マネージャにより、前記データ要求についてデータ・ストレージ・サービスによって作成されたセッションの少なくとも１つのパラメータに対する変更を遂行することであって、前記少なくとも１つのパラメータが前記セッションに許可されたアクセスを制御する、前記遂行することと、
前記アクセス・マネージャにより、前記データ・ストレージによる前記データ要求の処理を再開することであって、前記データ・ストレージによる前記データ要求の処理が前記セッションの前記少なくとも１つのパラメータに対する前記変更を反映する、前記再開することと
をさらに含む、請求項２０乃至２３のいずれか一項に記載の方法。
【請求項２５】
コンピュータ・プログラムであり、アクセス・マネージャを含むコンピュータにより実行されることにより、前記コンピュータに、
クラウド・ストレージ・システムのデータ・ストレージによりデータ要求を受信することであって、前記データ要求が前記クラウド・ストレージ・システムによって保管されたデータ・アーティファクトへのアクセスを要求すること、前記受信することと、
前記データ・ストレージにより前記データ要求に対する応答を決定することであって、前記決定が前記データ・アーティファクトへのアクセスを許可することおよびアクセスを拒否することのうちの少なくとも一方を示す、前記決定することと、
前記アクセス・マネージャにより前記データ・ストレージによる前記データ要求の受信を検出することと、
前記アクセス・マネージャにより、前記決定された応答の実行前に前記データ・ストレージによる前記データ要求の処理に割り込むことと、
前記アクセス・マネージャにより、前記データ要求のコピーおよび前記データ・ストレージの応答を入手することと、
前記データ・アーティファクトについて定義された任意アクセス制御に関して、前記アクセス・マネージャにより前記データ要求の前記コピーの内容を評価することであって、前記任意アクセス制御が前記データ・アーティファクトに関連するエンティティによって構成される、前記評価すること、
前記アクセス・マネージャにより前記データ要求コピーの前記評価からの応答を決定することであって、前記決定が前記データ・アーティファクトへのアクセスを許可することおよびアクセスを拒否することのうちの少なくとも一方を示す、前記決定することと、
前記データ・ストレージによって決定された前記応答を前記アクセス・マネージャによって内部で決定された前記応答と比較することと、
前記比較が前記データ・ストレージと前記アクセス・マネージャの前記応答間の不一致を示す場合に、前記アクセス・マネージャにより前記データ・ストレージの応答をオーバライドすることであって、前記アクセス・マネージャによって決定された前記応答が前記データ・ストレージによって決定された前記応答より優先される、前記オーバライドすることと、
前記比較が前記データ・ストレージと前記アクセス・マネージャの前記応答間の一致を示す場合に、前記アクセス・マネージャにより前記データ・ストレージによる前記データ要求の処理に対する前記割り込みをリリースすることであって、前記データ・ストレージが前記データ要求の履行を完了できる、前記リリースすることと
を実行させる、前記コンピュータ・プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、クラウド・コンピューティング・データ・ストレージの分野に関し、詳細には、クラウド・コンピューティング環境（cloud computing environment）に保管されたデータに関するきめ細かい（granular）データ所有者構成可能アクセス制御の有効化に関する。
【背景技術】
【０００２】
特にデータの保管あるいは管理またはその両方のためのクラウド・サービスであるクラウドベースのストレージ・サービスにより、組織はデータ管理オーバヘッドの負担を軽減し、地理的に分離されているグループ間のデータ・アクセシビリティを高めることができる。クラウド・ストレージに保管されたデータは任意のコンピューティング・デバイスからアクセス可能であり、許可ユーザはクラウド・ストレージ・サービスに接続することができる。
【０００３】
たとえば、修理専門技術者は、インターネット接続が使用可能であれば、どのような現場からでもクラウド・ストレージ内のサービス・マニュアルおよび修理報告書にアクセスすることができる。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
クラウド・コンピューティング環境における任意データ・アクセス制御の有効化を提供する。
【課題を解決するための手段】
【０００５】
本発明の一態様は、クラウド・コンピューティング環境において任意データ・アクセス制御（discretionary data access control）を有効化するための方法を含むことができる。このような方法は、クラウド・コンピューティング環境で動作するアクセス・マネージャ・サービスによりデータ要求およびデータ要求に関する応答メッセージを入手することから始めることができる。応答メッセージは、データ要求に応答してクラウド・コンピューティング環境のデータ・ストレージ・サービスによって生成することができる。応答メッセージは、データ・ストレージ・サービスによって保管されたデータ・アーティファクト（data artifact）へのアクセスの許可または拒否を示すことができる。データ要求に対して適用可能な所有者指定のアクセス規則あるいは所有者指定のアクセス例外またはその両方を識別することができる。データ要求に対するアクセス応答は、適用可能な所有者指定のアクセス規則あるいは所有者指定のアクセス例外またはその両方に基づいて決定することができる。アクセス応答は、要求されたデータ・アーティファクトへのアクセスの許可または拒否を示すことができる。所有者指定のアクセス規則は、データ・アーティファクトへのアクセスを制限するパラメータ値を定義することができる。所有者指定のアクセス例外は、そうでなければ拒否されるはずのデータ・アーティファクトへのアクセスを許可する条件を定義することができる。次に、決定されたアクセス応答は応答メッセージと比較することができる。決定されたアクセス応答が応答メッセージと一致しない場合、応答メッセージは、決定されたアクセス応答を表すためにオーバライドすることができる。決定されたアクセス応答が応答メッセージと一致する場合、応答メッセージはデータ要求の発信エンティティに伝達することができる。
【０００６】
本発明の他の態様は、クラウド・ストレージ・サービスに関する任意データ・アクセス制御を有効化するシステムを含むことができる。このようなシステムは、電子データ・ファイルを表すデータ・アーティファクト、クラウド・コンピューティング環境、データ・

ストレージ・クラウド・サービス、およびアクセス・マネージャ・クラウド・サービスを含むことができる。クラウド・コンピューティング環境は、クラウド・コンピューティング・モデルに応じて動作するように構成されたクラウド・サービス・プロバイダを含むことができる。データ・ストレージ・クラウド・サービスは、クラウド・コンピューティング環境内のデータ・アーティファクトの保管およびアクセスを管理するように構成することができる。アクセス・マネージャ・クラウド・サービスは、データ・ストレージ・クラウド・サービスによって管理されるデータ・アーティファクトに関する任意アクセス制御を提供するように構成することができる。任意アクセス制御は、データ・ストレージ・クラウド・サービスによって実行されるアクセス制御操作に加えて実行することができる。任意アクセス制御は、データ・ストレージ・クラウド・サービスによって行われたアクセス許可およびアクセス拒否を撤回することができる。

【０００７】

本発明のさらに他の態様は、埋め込まれたコンピュータ使用可能プログラム・コードを有するコンピュータ・プログラム（computer program product）及びそれを記憶するコンピュータ可読媒体を含むことができる。このコンピュータ使用可能プログラム・コードは、データ要求およびデータ要求に関する応答メッセージを入手するように構成することができる。応答メッセージは、データ要求に応答してクラウド・コンピューティング環境で動作するデータ・ストレージ・サービスによって生成することができる。応答メッセージは、データ・ストレージ・サービスによって保管されたデータ・アーティファクトへのアクセスの許可または拒否を示すことができる。コンピュータ使用可能プログラム・コードは、データ要求に対して適用可能な所有者指定のアクセス規則あるいは所有者指定のアクセス例外またはその両方を識別するように構成することができる。次に、コンピュータ使用可能プログラム・コードは、識別された所有者指定のアクセス規則あるいは所有者指定のアクセス例外またはその両方に基づいてデータ要求に対するアクセス応答を決定するように構成することができる。アクセス応答は、要求されたデータ・アーティファクトへのアクセスの許可または拒否を示すことができる。所有者指定のアクセス規則は、データ・アーティファクトへのアクセスを制限するパラメータ値を定義することができる。所有者指定のアクセス例外は、そうでなければ拒否されるはずのデータ・アーティファクトへのアクセスを許可する条件を定義することができる。コンピュータ使用可能プログラム・コードは、決定されたアクセス応答を応答メッセージと比較するように構成することができる。決定されたアクセス応答が応答メッセージと一致しない場合、コンピュータ使用可能プログラム・コードは、決定されたアクセス応答を表すために応答メッセージをオーバライドするように構成することができる。コンピュータ使用可能プログラム・コードは、決定されたアクセス応答が応答メッセージと一致する場合、データ要求の発信エンティティに応答メッセージを伝達するように構成することができる。

【０００８】

本発明のさらに他の態様は、クラウド・ストレージ・システムにおいて任意データ・アクセス制御を有効化するための方法を含むことができる。このような方法は、クラウド・ストレージ・システムのデータ・ストレージ・クラウド・サービスがクラウド・コンピューティング環境内のクラウド・ストレージ・システムによって保管されたデータ・アーティファクトへのアクセスに関するデータ要求を受信したときに始めることができる。データ要求に対する応答はデータ・ストレージ・クラウド・サービスによって決定することができ、データ・アーティファクトへのアクセスの許可または拒否を示す。アクセス・マネージャ・クラウド・サービスは、データ・ストレージ・クラウド・サービスによるデータ要求の受信を検出することができる。次にアクセス・マネージャ・クラウド・サービスは、決定された応答の実行前にデータ・ストレージ・クラウド・サービスによるデータ要求の処理に割り込むことができる。データ要求のコピーおよびデータ・ストレージ・クラウド・サービスの応答はアクセス・マネージャ・クラウド・サービスによって入手することができる。アクセス・マネージャ・クラウド・サービスは、データ・アーティファクトについて定義された任意アクセス制御に関して、データ要求コピーの内容を評価することが

できる。任意アクセス制御は、データ・アーティファクトに関連するエンティティによって構成することができる。データ要求コピーの内容の前記評価からの応答はアクセス・マネージャ・クラウド・サービスによって決定することができ、データ・アーティファクトへのアクセスの許可または拒否を示す。次にアクセス・マネージャ・クラウド・サービスは、データ・ストレージ・クラウド・サービスによって決定された応答を内部で決定された応答と比較することができる。この比較がデータ・ストレージ・クラウド・サービスとアクセス・マネージャ・クラウド・サービスの応答間の不一致を示す場合、アクセス・マネージャ・クラウド・サービスはデータ・ストレージ・クラウド・サービスの応答をオーバライドすることができる。この比較がデータ・ストレージ・クラウド・サービスとアクセス・マネージャ・クラウド・サービスの応答間の一致を示す場合、アクセス・マネージャ・クラウド・サービスは、データ・ストレージ・クラウド・サービスによるデータ要求の処理に対する割り込みをリリースして、データ・ストレージ・クラウド・サービスがデータ要求の履行を完了できるようにすることができる。

【図面の簡単な説明】

【０００９】

【図１】本明細書に開示されている本発明の配置の諸実施形態によりクラウド・コンピューティング環境内のデータ・ストレージ・サービスを使用するためにそれに対するアクセスが提供されるデータ・アーティファクトに関するきめ細かい任意アクセス制御の有効化を描写する概念プロセス流れ図である。

【図２】本明細書に開示されている本発明の配置の一実施形態によりクラウド・コンピューティング環境内で動作するデータ・ストレージ・サービスのためにきめ細かい任意アクセス制御を提供するシステムを示す概略図である。

【図３】本明細書に開示されている本発明の配置の一実施形態により任意アクセス制御を有効化するためのデータ・ストレージ・サービスに関するアクセス・マネージャ・サービスの機能を全般的に詳述する方法の流れ図である。

【図４】本明細書に開示されている本発明の配置の諸実施形態によりアクセス・マネージャ・サービスの動作を記述する方法の流れ図である。

【図５】本明細書に開示されている本発明の配置の諸実施形態によりデータ所有者によるアクセス・マネージャ・サービスの使用を詳述する方法に関する流れ図の集合である。

【発明を実施するための形態】

【００１０】

データ・セキュリティは常にデータの保管およびデータ伝送に関する関心事であるが、他のユーザあるいは組織またはその両方による保管データへのアクセスまたは保管データの可視性の制御はデータ所有者（すなわち、オーサリング・ユーザ（authoring user）、組織）に限られている場合が多い。クラウド・サービスは典型的に広範囲のユーザ・タイプおよび必要性に対応するように設計されているので、クラウド・サービスの特徴あるいは機能またはその両方は本質的に基本的または一般的なものである場合が多い。このため、クラウド・ストレージ・サービスで使用可能なアクセス制御のタイプ（すなわち、アクセス制御リスト、ユーザ・グループ、役割ベースのアクセスなど）は、多くの組織が慣れているエンタープライズレベルのデータ管理システムに比べて、比較的簡単すぎるものである。

【００１１】

クラウド・ストレージ・サービスを使用するすべての組織は同じアクセス制御に限定される。役割ベースのアクセス制御手法は大きい組織には役に立つ可能性があるが、小さい組織には過剰に複雑になる可能性がある。同様に、中小組織に適しているユーザ・グループベースの手法は大企業には役に立たない可能性がある。

【００１２】

さらに、クラウド・ストレージ・サービスによって保管された組織のデータはサービス・プロバイダの可視性あるいはアクセスまたはその両方の規則の対象になる。クラウド・ストレージ・サービス・プロバイダがその可視性／アクセス規則を変更した場合、組織の

データへのアクセスが損なわれる可能性がある。

【００１３】

本発明は、クラウド・コンピューティング環境内のデータ・ストレージ・クラウド・サービスによって処理されたデータ・アーティファクトに関する任意データ・アクセス制御を有効化するための解決策を開示するものである。データ・ストレージ・クラウド・サービスは、データ・アーティファクトの保管およびアクセスを管理することができる。アクセス・マネージャ・クラウド・サービスは、データ・ストレージ・クラウド・サービスによって決定されたデータ・アーティファクトへのアクセスの許可または拒否を動的に調整するために１組の任意アクセス制御を適用することができる。任意アクセス制御は、所有者指定のアクセス規則および所有者指定のアクセス例外によって表すことができる。所有者指定のアクセス規則は、データ・アーティファクトへのアクセスを制限するパラメータ値を定義することができる。所有者指定のアクセス例外は、そうでなければ拒否されるはずのデータ・アーティファクトへのアクセスを許可する条件を定義することができる。

【００１４】

当業者であれば認識するように、本発明の諸態様は、システム、方法、またはコンピュータ・プログラムとして実施することができる。したがって、本発明の諸態様は、完全にハードウェアの実施形態、完全にソフトウェアの実施形態（ファームウェア、常駐ソフトウェア、マイクロコードなどを含む）、またはソフトウェア態様とハードウェア態様を結合した一実施形態を採ることができ、このような実施形態は一般に本明細書ではいずれも「回路」、「モジュール」、または「システム」と呼ぶことがある。さらに、本発明の諸態様は、コンピュータ可読プログラム・コードがそこに実現されているコンピュータ・プログラム又はそれが記憶されるコンピュータ可読媒体の態様を採ることもできる。

【００１５】

１つまたは複数のコンピュータ可読媒体の任意の組み合わせを使用することができる。コンピュータ可読媒体は、コンピュータ可読信号媒体またはコンピュータ可読記憶媒体にすることができる。コンピュータ可読記憶媒体は、たとえば、電子、磁気、光、電磁、赤外線、または半導体システム、装置、あるいはデバイス、もしくはこれらの任意の適切な組み合わせにすることができるが、これらに限定されないものである。コンピュータ可読記憶媒体のより具体的な例（非網羅的リスト）としては、１つまたは複数のワイヤを有する電気接続、ポータブル・コンピュータ・ディスケット、ハード・ディスク、ランダム・アクセス・メモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、消去可能プログラム可能読み取り専用メモリ（ＥＰＲＯＭまたはフラッシュ・メモリ）、光ファイバ、ポータブル・コンパクト・ディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、光記憶装置、磁気記憶装置、またはこれらの任意の適切な組み合わせを含むであろう。本書に関連して、コンピュータ可読記憶媒体は、命令実行システム、装置、またはデバイスによりあるいはそれに関連して使用するためのプログラムを収容または保管可能な任意の有形媒体にすることができる。

【００１６】

コンピュータ可読信号媒体は、たとえば、ベースバンド内にまたは搬送波の一部として、コンピュータ可読プログラム・コードがそこに実施されている伝搬データ信号を含むことができる。このような伝搬信号は、電磁、光、またはこれらの任意の適切な組み合わせを含むがこれらに限定されない様々な形のいずれかを取ることができる。コンピュータ可読信号媒体は、コンピュータ可読記憶媒体ではなく、命令実行システム、装置、またはデバイスによりあるいはそれに関連して使用するためのプログラムを伝達、伝搬、または移送可能な任意のコンピュータ可読媒体にすることができる。

【００１７】

コンピュータ可読媒体上に実施されたプログラム・コードは、無線、有線、光ファイバ・ケーブル、ＲＦなど、またはこれらの任意の適切な組み合わせを含むがこれらに限定されない任意の適切な媒体を使用して伝送することができる。本発明の諸態様に関する動作を実行するためのコンピュータ・プログラム・コードは、Ｊａｖａ（Ｒ）、Ｓｍａｌｌｔ

ａｌｋ（Ｒ）、Ｃ＋＋などのオブジェクト指向プログラミング言語ならびに「Ｃ」プログラミング言語または同様のプログラミング言語などの従来の手続き型プログラミング言語を含む、１つまたは複数のプログラミング言語の任意の組み合わせで作成することができる。このプログラム・コードは、スタンドアロン・ソフトウェア・パッケージとして、完全にユーザのコンピュータ上で、一部分はユーザのコンピュータ上で、一部分はユーザのコンピュータ上でしかも一部分はリモート・コンピュータ上で、あるいは完全にリモート・コンピュータまたはサーバ上で実行することができる。後者のシナリオでは、リモート・コンピュータは、ローカル・エリア・ネットワーク（ＬＡＮ）または広域ネットワーク（ＷＡＮ）を含む任意のタイプのネットワークを介してユーザのコンピュータに接続される場合もあれば、（たとえば、インターネット・サービス・プロバイダを使用してインターネットを介して）外部コンピュータに対して接続が行われる場合もある。

【００１８】

本発明の諸実施形態による方法、装置（システム）、およびコンピュータ・プログラムの流れ図あるいはブロック図またはその両方に関連して、本発明の諸態様について以下に説明する。流れ図あるいはブロック図またはその両方の各ブロックならびに流れ図あるいはブロック図またはその両方の複数ブロックの組み合わせは、コンピュータ・プログラム命令によって実装可能であることが理解されるであろう。これらのコンピュータ・プログラム命令は、マシンを生産するために汎用コンピュータ、特殊目的コンピュータ、またはその他のプログラマブル・データ処理装置のプロセッサに提供することができ、それにより、コンピュータまたはその他のプログラマブル・データ処理装置のプロセッサを介して実行される命令は流れ図あるいはブロック図またはその両方の１つまたは複数のブロックに指定された機能／動作を実装するための手段を作成することになる。

【００１９】

また、これらのコンピュータ・プログラム命令は、コンピュータ、その他のプログラマブル・データ処理装置、またはその他のデバイスに対して特定の方法で機能するよう指示することができるコンピュータ可読媒体に保管することもでき、それにより、コンピュータ可読媒体に保管された命令は流れ図あるいはブロック図またはその両方の１つまたは複数のブロックに指定された機能／動作を実装する命令を含む装置（article of manufacture）を生産することになる。

【００２０】

また、これらのコンピュータ・プログラム命令は、コンピュータ、その他のプログラマブル・データ処理装置、またはその他のデバイス上にロードして、コンピュータによって実装されるプロセスを生成するためにコンピュータ、その他のプログラマブル装置、またはその他のデバイス上で一連の動作ステップを実行させることができ、それにより、コンピュータまたはその他のプログラマブル装置上で実行される命令は流れ図あるいはブロック図またはその両方の１つまたは複数のブロックに指定された機能／動作を実装するためのプロセスを提供することになる。

【００２１】

図１は、本明細書に開示されている本発明の配置の諸実施形態によりクラウド・コンピューティング環境１１０内のデータ・ストレージ・サービス１１５を使用するためにそれに対するアクセスが提供されるデータ・アーティファクト１４５に関するきめ細かい任意アクセス制御１３０の有効化を描写する概念プロセス・フロー１００である。

【００２２】

プロセス・フロー１００では、データ・コンシューマ１０５は、クラウド・コンピューティング環境１１０内で動作しているデータ・ストレージ・サービス１１５に対してデータ・アーティファクト１４５に関するデータ要求１０７を送信することができる。データ・コンシューマ１０５は、指定のデータ・アーティファクト１４５へのアクセスを要求するヒューマン・ユーザあるいはコンピューティング・エンティティまたはその両方に相当する可能性がある。データ・アーティファクト１４５は、電子フォーマット（すなわち、テキスト・ファイル、イメージ・ファイル、オーディオ・ファイル、マルチメディア・フ

ァイルなど）で保管された様々なデータを表すことができる。

【００２３】

データ要求１０７は、要求側データ・コンシューマ１０５およびアクセスすべきデータ・アーティファクト１４５を識別する電子メッセージにすることができる。また、データ要求１０７は、メッセージ・フォーマットあるいはデータ・ストレージ・サービス１１５またはその両方に応じて、要求側データ・コンシューマ１０５のインターネット・プロトコル（ＩＰ）アドレス、データ・コンシューマ１０５によって実行されるアクション、データ要求１０７のタイムスタンプなどの様々なその他のメッセージング情報も含むことができる。

【００２４】

クラウド・コンピューティング環境１１０は、クラウド・コンピューティング・モデルにより構成されたハードウェア／ソフトウェア・コンピューティング環境を表すことができる。クラウド・コンピューティング環境１１０は、リポジトリ１２５のような構成可能なコンピューティング・リソースの共用プールへのオンデマンド・アクセスを有効化することができる。クラウド・コンピューティング環境１１０は、プライベート・クラウド（private cloud）（すなわち、唯一の組織によって所有される）、コミュニティ・クラウド（community cloud）（すなわち、複数の共感組織によって共用される）、パブリック・クラウド（public cloud）（すなわち、公衆または大きいグループにとって使用可能である）、またはハイブリッド・クラウド（hybrid cloud）（すなわち、複数のクラウド・タイプからなる構成）として実現することができる。

【００２５】

データ・ストレージ・サービス１１５は、その関連クラウド・リポジトリ１２５内のデータ・アーティファクト１４５の保管およびアクセスを管理するために特に構成されたクラウド・サービスを表すことができる。データ・ストレージ・サービス１１５およびリポジトリ１２５は、一般にクラウド・ストレージ・システムまたはクラウド・ストレージ・サービスと呼ばれるものを表すことができる。データ・アーティファクト１４５の単純な保管に加えて、データ・ストレージ・サービス１１５は、ファイル共用、バージョン管理、およびオンライン・コラボレーションのような様々なデータ管理機能も含むことができる。

【００２６】

データ・ストレージ・サービス１１５は、データ要求１０７を許可するかまたは拒否するかを決定することができる。しかし、典型的なデータ・ストレージ・サービス１１５の実装例とは異なり、アクセス・マネージャ・サービス１２０は、データ・ストレージ・サービス１１５によるデータ・アーティファクト１４５の提供に割り込み、本明細書で任意アクセス制御１３０と呼ぶきめ細かい任意アクセス制御１３０に基づいてデータ・アーティファクト１４５の提供が許可されているかどうかをチェックすることができる。

【００２７】

アクセス・マネージャ・サービス１２０は、データ・ストレージ・サービス１１５によって提供されたデータ・アーティファクト１４５に対する任意アクセス制御１３０の実行を有効化する独立メカニズムとして動作するように構成されたクラウド・サービスを表すことができる。すなわち、アクセス・マネージャ・サービス１２０は、任意アクセス制御１３０に定義されたパラメータに基づいて、データ・ストレージ・サービス１１５によるデータ・コンシューマ１０５へのデータ・アーティファクト１４５の提供を調整することができる。

【００２８】

たとえば、任意アクセス制御１３０は、データ・ストレージ・サービス１１５が一般には任意のユーザ（群）１０５にデータ・アーティファクト１４５を提供する場合でも、特定のデータ・アーティファクト１４５へのアクセスを３人のユーザ１０５のみに制限するために使用することができる。

【００２９】

任意アクセス制御１３０は、データ・アーティファクト１４５のデータ所有者１５０の裁量でデータ・アーティファクト１４５へのアクセスを許可するかあるいは拒否するかまたはその両方を行うように設定することができる構成可能パラメータを表すことができる。データ所有者１５０は、データ・アーティファクト１４５のオーサリング・ユーザまたは組織あるいはオーサリング・ユーザ／組織に代わって動作するための許可を有するユーザを表すことができる。

【００３０】

たとえば、オーサリング組織のデータ管理者は、データ・アーティファクト１４５のオーサリング・ユーザではないにもかかわらず、すべてのデータ・アーティファクト１４５に関する任意アクセス制御１３０を管理するための仕事が与えられる可能性がある。

【００３１】

任意アクセス制御１３０は所有者指定のアクセス規則１３５と所有者指定のアクセス例外１４０とを含むことができる。本明細書でアクセス規則１３５と呼ばれる所有者指定のアクセス規則１３５は、データ・アーティファクト１４５へのアクセスを制限する条件を表すことができる。本明細書でアクセス例外１４０と呼ばれる所有者指定のアクセス例外１４０は、アクセス規則１３５に対する許可例外を表すことができる。アクセス規則１３５は標準ポリシーとしての意味を持つ可能性があるが、アクセス例外１４０は標準ポリシーとは反対に臨時あるいは一時的またはその両方の許可を表すことができる。

【００３２】

アクセス規則１３５およびアクセス例外１４０の両方に関するパラメータは、データ要求１０７内に含まれるデータ・フィールド、データ・アーティファクト１４５について定義されたメタデータ、あるいはデータ・ストレージ・サービス１１５によって使用されるデータ要素（たとえば、ユーザ名、ユーザ役割、アクセス・レベルなど）、またはこれらの組み合わせを使用することができる。

【００３３】

データ要求１０７を許可／拒否しなければならないかどうかをアクセス・マネージャ・サービス１２０が確認すると、アクセス・マネージャ・サービス１２０は、データ・ストレージ・サービス１１５によるデータ・アーティファクト１４５の提供をオーバライドまたは続行しなければならないかどうかを判断することができる。この判断に応じて、アクセス・マネージャ・サービス１２０は、適切なアクセス応答１４７（すなわち、アクセス許可／拒否）をデータ・コンシューマ１０５に送信することができる。

【００３４】

従来の手法と任意アクセス制御１３０によって提供されるものとの違いを例示するために、典型的に内部ユーザ１０５に制限されているデータ・アーティファクト１４５を表示するためのワンタイム・アクセスを要求する外部エンティティ１０５の例を使用する。

【００３５】

従来のクラウド・データ・ストレージ・サービス１１５を使用すると、データ・ストレージ・サービス１１５の使用可能なアクセス制御メカニズムを使用して、データ・アーティファクト１４５に関する適切なアクセス・レベルを外部エンティティ１０５に割り当てる（すなわち、適切な役割を外部エンティティ１０５に割り当てる）ことができる。しかし、このようにすると、そのアクセス・レベルにとって使用可能なすべてのデータ・アーティファクト１４５への無制限のアクセス権を外部エンティティ１０５に提供することになり、その他の機密の内部データ・アーティファクト１４５がそのアクセス・レベルを共用する場合には望ましくない状況になる。

【００３６】

その代わりに、特定のデータ・アーティファクト１４５のみにアクセスできるデータ・ストレージ・サービス１１５のアクセス制御メカニズムを使用する新しい役割／グループを定義しようと試みることができるであろう。より良いオプションであるが、最も可能性のあるアクセス制御メカニズムは、幅広い観点から定義され、外部エンティティ１０５がデータ・アーティファクト１４５に対して実行できるアクションのタイプに対する制限を

サポートしない。したがって、この手法は、外部エンティティ１０５によるアクセスを特定のデータ・アーティファクト１４５に限定するが、外部エンティティ１０５がそのデータ・アーティファクト１４５を表示できるだけになることを保証することはできない。

【００３７】

これらのオプションのいずれでも、データ所有者１５０は、アクセス・セッションが完全であると判断されると、データ・ストレージ・サービス１１５のアクセス制御メカニズムによる外部エンティティ１０５に関するアクセスを除去または非活動化することを忘れないようにしなければならない。

【００３８】

このタイプの状況を処理するためのもう１つの一般的な手段は、データ・アーティファクト１４５のコピーを外部エンティティ１５０に電子的に提供すること（すなわち、電子メール、ファイル転送）にすることができる。この事例では、データ所有者１５０はデータ・アーティファクト１４５に対する制御を放棄し、外部エンティティ１０５は制限なしにデータ・アーティファクト１４５を配布するかあるいは変更するかまたはその両方を行うことができる。外部エンティティ１０５がデータ・アーティファクト１４５の取り扱いを誤る場合には、このオプションは組織にとって有害なものになる可能性がある。

【００３９】

代わって、ＵＮＩＸ（The Open Groupの商標）またはＵＮＩＸ系のオペレーティング・システムの固有のファイル・セキュリティの特徴をデータ・ストレージ・サービス１１５に使用することができる。ＵＮＩＸまたはＵＮＩＸ系のオペレーティング・システムは、ファイル所有者、その所有者が属すグループ、およびその他のすべてのユーザに関する読み取り／書き込み／実行許可を定義する保護ビットを保管されたデータ・アーティファクト１４５に関連付けることができる。この特徴は外部エンティティ１０５がデータ・アーティファクト１４５に関して実行できるアクションを可能にすると思われるが、このオプションはその他のアクセス関連問題を引き起こす可能性がある。

【００４０】

第一に、ほとんどの組織はＩＮＴＥＬ(Intel Corporationの商標)ベースのオペレーティング・システムを使用し、これにより、異なるオペレーティング・システムでデータ・アーティファクト１４５を保管しようと試みる場合に相互運用性の問題を引き起こす可能性がある。第二に、保護ビットを変更して許可を変更することは、実際の作成者（データ・アーティファクト１４５を作成したユーザ）またはシステム管理者しか実行することができない。これがクラウドベースのデータ・ストレージ・サービス１１５である場合、データ所有者１５０には、オペレーティング・システムベースのコマンドを実行する能力がまったく与えられない可能性がある。

【００４１】

これらの問題が克服された場合でも、この手法は他にもパフォーマンス関連の短所がある可能性がある。保護ビットは、データ・コンシューマ１０５あるいはデータ所有者１５０またはその両方が複数のグループのメンバになり得るアクセス制御メカニズムをサポートするために使用することができない。さらに、データ・コンシューマ１０５が属すグループは、グループ許可が割り当てられるはずのデータ所有者１５０のグループとは異なることはできない。許可変更を行うためにシステム管理者以外のプロキシを使用することはできない。最後に、保護ビットが変更されると、その変更は、分け隔てなくそのグループのすべてのメンバのアクセスに影響する可能性がある。

【００４２】

アクセス・マネージャ・サービス１２０を使用すると、このデータ・アーティファクト１４５あるいはその他のデータ・アーティファクト１４５またはその両方に関する標準アクセス・ポリシーであるので、内部ユーザに対するデータ・アーティファクト１４５の制限はアクセス規則１３５として表すことができる。外部エンティティ１０５によりデータ・アーティファクト１４５にアクセスする必要性は、アクセス例外１４０として定義することができる。アクセス例外１４０は、外部エンティティ１０５のＩＤに固有のものにな

るように作成し、許容アクションを表示のみに限定し、単一アクセス・セッションのみを許可することができる。

【００４３】

さらに、この手法では、データ・アーティファクト１４５はリポジトリ１２５内に安全に保管されたままになる可能性があり、外部エンティティ１０５はローカル・コピーを保管することができない。アクセス規則１３５によって表されたデータ・アーティファクト１４５に関する標準アクセス・ポリシーはそのまま残る可能性がある。アクセス・マネージャ・サービス１２０がアクセス例外１４０を実行すると、外部エンティティ１０５によるデータ・アーティファクト１４５の追加アクセスを防止するためにアクセス例外１４０を非活動化することができる。

【００４４】

この手法では、クラウド・コンピューティング環境１１０内に以下の機能を提供することができる。

・リポジトリ１２５がどの国に常駐するかにかかわらず、組織の操業国のデータ・アクセス規制／制限に基づく組織固有の「拒否パーティ・リスト（Denied Party Lists）」

・データ・ストレージ・サービス１１５が損なわれた状態になるかまたはその内部アクセス／可視性規則を変更する場合にデータ漏洩の最小化

・クラウド・データ・ストレージ・サービス１１５が組織のイントラネットを処理する能力

【００４５】

クラウド・コンピューティング環境１１０は、搬送波内でエンコードされたデータを伝達するために必要な任意のハードウェア／ソフトウェア／ファームウェアを含むことができる。データは、アナログまたはデジタル信号内に含め、データまたは音声チャネルを介して伝達することができる。クラウド・コンピューティング環境１１０は、コンピューティング・デバイスのコンポーネント間ならびに統合デバイスのコンポーネントと周辺装置との間で交換すべき通信に必要なローカル・コンポーネントおよびデータ・パスを含むことができる。また、クラウド・コンピューティング環境１１０は、まとめてインターネットなどのデータ・ネットワークを形成する、ルータ、データ回線、ハブ、および中間サーバなどのネットワーク装置も含むことができる。クラウド・コンピューティング環境１１０は、電話交換機、モデム、セルラー通信タワーなど、回線ベースの通信コンポーネントおよび移動通信コンポーネントも含むことができる。クラウド・コンピューティング環境１１０は、回線ベースあるいはワイヤレスまたはその両方の通信パスを含むことができる。

【００４６】

本明細書で使用するように、提示されたリポジトリ１２５は、デジタル情報を保管するように構成された物理または仮想記憶空間にすることができる。リポジトリ１２５は、磁気ディスク、光ディスク、半導体メモリ、デジタルでエンコードされたプラスチック・メモリ、ホログラム・メモリ、または任意のその他の記録媒体を含むがこれらに限定されない任意のタイプのハードウェア内に物理的に実装することができる。リポジトリ１２５は、独立型ストレージ・ユニットならびに複数の物理装置から形成されたストレージ・ユニットにすることができる。さらに、情報はリポジトリ１２５内に様々な方法で保管することができる。たとえば、情報は、データベース構造内に保管するかあるいはファイル・ストレージ・システムの１つまたは複数のファイル内に保管することができ、その場合、各ファイルには情報検索のためにインデックスが付けられる場合もあれば、付けられない場合もある。さらに、リポジトリ１２５は、保管情報を無許可アクセスから保護するために１つまたは複数の暗号化メカニズムを使用することができる。

【００４７】

図２は、本明細書に開示されている本発明の配置の諸実施形態によりクラウド・コンピューティング環境２０５内で動作するデータ・ストレージ・サービス２２５のためにきめ細かい任意アクセス制御を提供するシステム２００を示す概略図である。システム２００

は、プロセス・フロー１００のコンテキスト内で使用することができる。

【００４８】

システム２００では、データ・アーティファクト２１５は、クラウド・コンピューティング環境２０５のリポジトリ２１０内にデータ・ストレージ・サービス２２５によって保管することができる。データ・アーティファクト２１５のデータ所有者２８０は、アクセス・マネージャ・サービス２４５の、本明細書でアクセス規則２５５と呼ばれる所有者指定のアクセス規則２５５あるいは本明細書でアクセス例外２６０と呼ばれる所有者指定のアクセス例外２６０またはその両方を使用して、データ・アーティファクト２１５へのアクセスを得ようとしているデータ・コンシューマ２６５に関する任意アクセス制御を定義することができる。

【００４９】

データ所有者２８０は、データ・アーティファクト２１５のオーサリング・ユーザまたは発信組織あるいはオーサリング・ユーザ／組織に代わって動作するための許可を有するユーザを表すことができる。データ・コンシューマ２６５は、指定のデータ・アーティファクト２１５へのアクセスを要求するヒューマン・ユーザあるいはコンピューティング・エンティティ（すなわち、他のクラウド・サービス）またはその両方に相当する可能性がある。データ・アーティファクト２１５は、電子フォーマット（すなわち、テキスト・ファイル、イメージ・ファイル、オーディオ・ファイル、マルチメディア・ファイルなど）で保管された様々なデータを表すことができる。

【００５０】

クラウド・コンピューティング環境２０５は、クラウド・コンピューティング・モデルを実装するハードウェア／ソフトウェア・コンポーネントの構成を表すことができる。一般に、クラウド・コンピューティング環境２０５は、サーバ、データ・ストア、およびソフトウェア・アプリケーションなど、インターネットによるクラウド・サービスの提供をサポートするハードウェア／ソフトウェア・コンポーネントを含むことができる。

【００５１】

この例では、クラウド・コンピューティング環境２０５は、データ・アーティファクト２１５の保管用のリポジトリ２１０と、データ・ストレージ・サービス２２５用のサービス・プロバイダ２２０と、アクセス・マネージャ・サービス２４５用のサービス・プロバイダ２４０とを含むことができる。

【００５２】

本発明のこの実施形態の精神を逸脱せずに、追加のリポジトリ２１０あるいはサービス・プロバイダ２２０／２４０またはその両方ならびにサービス・プロバイダ２２０／２４０によって提供されるその他のクラウド・サービスをクラウド・コンピューティング環境２０５内に含めることができることに留意されたい。

【００５３】

また、クラウド・コンピューティング環境２０５はインターネットベースであるので、システム２００の様々なコンポーネント間の通信に必要な任意のコンピュータ・ネットワーク（たとえば、公衆網、私設網、ＷＡＮ、ＬＡＮなど）はクラウド・コンピューティング環境２０５の一部として含めることができ、個別のエンティティとして例示されていないことに留意することも重要である。

【００５４】

サービス・プロバイダ２２０および２４０は、それぞれのサービス２２５および２４５の動作をサポートするために必要なハードウェアあるいはソフトウェアまたはその両方のコンポーネントを表すことができる。他の企図された実施形態では、データ・ストレージ・サービス２２５およびアクセス・マネージャ・サービス２４５は同じサービス・プロバイダ２２０または２４０によって提供することができる。

【００５５】

システム２００では、各サービス・プロバイダ２２０および２４０は、それぞれ、個別のデータ・ストア２３０および２５０を有するものとして示すことができる。データ・ス

トア２３０および２５０の使用は、各クラウド・サービス２２５および２５５に固有のデータ要素の論理的分離を例示するためのものであって、必要な実装例の表現として意図されているわけではないことに留意されたい。システム２００の実装例では、データ・ストア２３０あるいは２５０またはその両方の内容をリポジトリ２１０あるいは対応するサービス・プロバイダ２２０または２４０によってアクセス可能な他のこのようなリポジトリ２１０またはその両方に保管することができる。すなわち、データ・ストア２３０および２５０の内容は、クラウド・コンピューティング環境２０５内に含まれるリポジトリ２１０のうち、サービス・プロバイダ２２０または２４０によってアクセス可能なものに保管することができる。

【００５６】

データ・ストレージ・サービス２２５は、クラウド・リポジトリ２１０内のデータ・アーティファクト２１５の保管およびアクセスを管理するように構成されたクラウド・サービスを表すことができる。データ・アーティファクト２１５の保管に加えて、データ・ストレージ・サービス２２５は、ファイル共用、バージョン管理、およびオンライン・コラボレーションのような様々なデータ管理機能も含むことができる。

【００５７】

データ・ストレージ・サービス２２５は、データ・ストレージ・サービス２２５に固有の１組のデータ処理規則２３５に基づいて、データ・アーティファクト２１５へのアクセスを許可するかまたは拒否するかを決定することができる。データ処理規則２３５は、サービス・プロバイダ２２０、リポジトリ２１０、データ所有者２８０、あるいはデータ・コンシューマ２６５、またはこれらの組み合わせの位置に適用可能な行政機関または組織によって課せられたデータ・アクセス要件あるいは規制またはその両方を表すことができる。

【００５８】

たとえば、米国内をベースとする医療データ用のデータ・ストレージ・サービス２２５は、データ・ストレージ・サービス２２５によって処理されるデータ・アーティファクト２１５が医療保険の相互運用性と説明責任に関する法律（ＨＩＰＡＡ：Health Insurance Portability and Accountability Act）を遵守していることを保証するデータ処理規則２３５を有する可能性がある。

【００５９】

アクセス・マネージャ・サービス２４５は、データ所有者２８０の裁量でデータ・ストレージ・サービス２２５によって提供されたデータ・アーティファクト２１５に対して、さらにアクセス規則２５５によりアクセスを制御するかまたはアクセス例外２６０により分配を許可することができる独立メカニズムとして動作するように構成されたクラウド・サービスを表すことができる。したがって、アクセス・マネージャ・サービス２４５は、アクセス規則２５５あるいはアクセス例外２６０またはその両方の対象になるデータ・アーティファクト２１５へのアクセスを可能にするときにデータ・ストレージ・サービス２２５の決定をオーバライドすることができる。

【００６０】

前述の通り、アクセス規則２５５は標準ポリシーの表現としての意味を持つ可能性があるが、アクセス例外２６０はデータ・ストレージ・サービス２２５のデータ処理規則２３５あるいはアクセス・マネージャ・サービス２４５のアクセス規則２５５またはその両方によって実施されるポリシーに対する臨時あるいは一時的またはその両方の免除を表すことができる。

【００６１】

アクセス規則２５５およびアクセス例外２６０の管理および実行はデータ・ストレージ・サービス２２５の動作とは無関係に行われることを強調しておかなければならない。すなわち、データ・ストレージ・サービス２２５がその動作を完了した後で、アクセス・マネージャ・サービス２５５がその動作を実行することができる。データ・ストレージ・サービス２２５は、アクセス・マネージャ・サービス２５５のアクションを意識せずに動作

することができる。したがって、クラウド・コンピューティング環境２０５内のアーキテクチャあるいはシステムまたはその両方の変更を必要とせずに、アクセス・マネージャ・サービス２５５の機能を現行のデータ・ストレージ・サービス２２５に適用することができる。

【００６２】

他の実施形態では、アクセス・マネージャ・サービス２５５は、要求されたデータ・アーティファクト２１５へのアクセスを可能にする前に、アクセス制御の最終段階としてデータ・ストレージ・サービス２２５によって呼び出すことができる。

【００６３】

アクセス規則２５５およびアクセス例外２６０を表すために使用されるパラメータは、データ・コンシューマ２６５からデータ・ストレージ・サービス２２５が受信したデータ要求内に含まれるデータ・フィールド、データ・アーティファクト２１５について定義されたメタデータ、あるいはデータ・ストレージ・サービス２２５によって使用されるデータ要素、またはこれらの組み合わせを使用することができる。

【００６４】

これらのパラメータの例としては、ユーザ名、電子メール・アドレス、電子メール・ドメイン、ＩＰアドレス、データ・アーティファクト２１５のタイプ、ユーザ役割、実行されるアクションのタイプ、データ・アーティファクト２１５の機密性レベル、要求が受信された時刻、要求ルーティングなどを含むことができるが、これらに限定されない。

【００６５】

データ所有者２８０は、クライアント・デバイス２７０上で実行されるアクセス・マネージャ・ユーザ・インターフェース２７５を使用してアクセス規則２５５あるいはアクセス例外２６０またはその両方を定義することができる。クライアント・デバイス２７０は、アクセス・マネージャ・ユーザ・インターフェース２７５を実行し、クラウド・コンピューティング環境２０５と通信することができる様々なコンピューティング・デバイスを表すことができる。

【００６６】

アクセス・マネージャ・ユーザ・インターフェース２７５は、アクセス規則２５５あるいはアクセス例外２６０またはその両方を定義するための構成可能なメカニズムをデータ所有者２８０に提示することができるグラフィカル・ユーザ・インターフェース（ＧＵＩ）を表すことができる。アクセス・マネージャ・ユーザ・インターフェース２７５は、データ項目あるいは特徴またはその両方へのアクセスまたはそれらの使用を制限するためのセキュリティ手段を使用するようにさらに構成することができる。

【００６７】

たとえば、アクセス例外２６０の作成を、「管理者」の役割を有するデータ所有者２８０に限定するために、役割ベースの手法を使用することができる。さらに、データ所有者２８０が作成するかあるいは変更するかまたはその両方を行うことができるアクセス規則２５５のタイプを制限するために、種々の役割を使用することができる。

【００６８】

アクセス・マネージャ・ユーザ・インターフェース２７５はデータ・ストレージ・サービス２２５と対話するために使用されないことに留意されたい。データ・ストレージ・サービス２２５との対話では、データ・ストレージ・サービス２２５に関連するユーザ・インターフェース（図示せず）を使用することになるであろう。

【００６９】

クラウド・コンピューティング環境２０５は、搬送波内でエンコードされたデータを伝達するために必要な任意のハードウェア／ソフトウェア／ファームウェアを含むことができる。データは、アナログまたはデジタル信号内に含め、データまたは音声チャネルを介して伝達することができる。クラウド・コンピューティング環境２０５は、コンピューティング・デバイスのコンポーネント間ならびに統合デバイスのコンポーネントと周辺装置との間で交換すべき通信に必要なローカル・コンポーネントおよびデータ・パスを含むこ

とができる。また、クラウド・コンピューティング環境２０５は、まとめてインターネットなどのデータ・ネットワークを形成する、ルータ、データ回線、ハブ、および中間サーバなどのネットワーク装置も含むことができる。クラウド・コンピューティング環境２０５は、電話交換機、モデム、セルラー通信タワーなど、回線ベースの通信コンポーネントおよび移動通信コンポーネントも含むことができる。クラウド・コンピューティング環境２０５は、回線ベースあるいはワイヤレスまたはその両方の通信パスを含むことができる。

【００７０】

本明細書で使用するように、提示されたリポジトリ２１０ならびにデータ・ストア２３０および２５０は、デジタル情報を保管するように構成された物理または仮想記憶空間にすることができる。リポジトリ２１０ならびにデータ・ストア２３０および２５０は、磁気ディスク、光ディスク、半導体メモリ、デジタルでエンコードされたプラスチック・メモリ、ホログラム・メモリ、または任意のその他の記録媒体を含むがこれらに限定されない任意のタイプのハードウェア内に物理的に実装することができる。リポジトリ２１０ならびにデータ・ストア２３０および２５０は、独立型ストレージ・ユニットならびに複数の物理装置から形成されたストレージ・ユニットにすることができる。さらに、情報はリポジトリ２１０ならびにデータ・ストア２３０および２５０内に様々な方法で保管することができる。たとえば、情報は、データベース構造内に保管するかあるいはファイル・ストレージ・システムの１つまたは複数のファイル内に保管することができ、その場合、各ファイルには情報検索のためにインデックスが付けられる場合もあれば、付けられない場合もある。さらに、リポジトリ２１０あるいはデータ・ストア２３０／２５０またはこれらの組み合わせは、保管情報を無許可アクセスから保護するために１つまたは複数の暗号化メカニズムを使用することができる。

【００７１】

図３は、本明細書に開示されている本発明の配置の諸実施形態により任意アクセス制御を有効化するためのデータ・ストレージ・サービスに関するアクセス・マネージャ・サービスの機能を全般的に詳述する方法３００の流れ図である。方法３００は、プロセス・フロー１００あるいはシステム２００またはその両方のコンテキスト内で実行することができる。

【００７２】

方法３００は、データ・ストレージ・サービスによって実行される一連のステップ３０５～３２５と、データ・ストレージ・サービスによって実行されるステップ３０５および３２５に応答してトリガされるようにアクセス・マネージャ・サービスによって実行される第２の１組のステップ３５０～３９５を例示することができる。簡単にするため、方法３００のうち、データ・ストレージ・サービスに関連する部分について最初に述べ、続いてアクセス・マネージャ・サービスの諸ステップについて述べることにする。

【００７３】

方法３００のステップ３０５～３２５は、データ・ストレージ・サービスによるデータ要求の典型的な処理を表すことができる。ステップ３０５では、データ・ストレージ・サービスはデータ・コンシューマからデータ要求を受信することができる。必要であれば、ステップ３１０でデータ・ストレージ・サービスによってデータ・コンシューマに関するユーザ・セッションを開始することができる。

【００７４】

ステップ３１５では、データ・ストレージ・サービスは、その内部処理規則に基づいて、データ要求に対するプロバイダ応答（すなわち、許可、拒否）を決定することができる。「プロバイダ応答」という用語は、データ・ストレージ・サービスによって決定される応答と、「アクセス応答」という用語で呼ばれるアクセス・マネージャ・サービスによって決定される応答とを区別するために使用されることに留意されたい。

【００７５】

次にデータ・ストレージ・サービスはステップ３２０でデータ要求に関する応答メッセ

ージを作成することができる。ステップ３２５では、データ・ストレージ・サービスによって要求側（データ・コンシューマ）に応答メッセージを送信することができる。

【００７６】

データ・ストレージ・サービスによるステップ３０５の実行は、点線３０７によって示されるように、アクセス・マネージャ・サービスによるステップ３５０の実行をトリガすることができる。ステップ３５０では、アクセス・マネージャ・サービスは、リスナ・コンポーネント（listener component）の使用によるかまたはデータ・ストレージ・サービスのメッセージ待ち行列に照会することなどにより、データ・ストレージ・サービスがデータ要求を受信したことを検出することができる。

【００７７】

ステップ３５５では、アクセス・マネージャ・サービスによってデータ要求のコピーを入手することができる。ステップ３６０では、データ要求に適用可能なものとして所有者指定のアクセス規則あるいはアクセス例外またはその両方をアクセス・マネージャ・サービスによって識別することができる。次に、ステップ３６５では、識別されたアクセス規則あるいはアクセス例外またはその両方に基づいて、データ要求に関するアクセス応答をアクセス・マネージャ・サービスによって決定することができる。

【００７８】

データ・ストレージ・サービスによるステップ３２５の実行に応答して、アクセス・マネージャ・サービスによってステップ３７０を実行することができる。ステップ３７０では、アクセス・マネージャ・サービスは、データ・ストレージ・サービスによって送信された応答メッセージをインターセプトすることができる。アクセス・マネージャ・サービスはステップ３７５で、それが決定したアクセス応答がインターセプトされた応答メッセージのプロバイダ応答と一致するかどうかを判断することができる。

【００７９】

応答が一致する（すなわち、要求側がアクセスできる必要があるかまたはないかについて両方のサービスが合意する）場合、ステップ３８０を実行することができ、そのステップでアクセス・マネージャ・サービスは要求側に応答メッセージを送信する（すなわち、インターセプトされた応答メッセージをリリースする）。

【００８０】

応答が一致しない場合、アクセス・マネージャ・サービスはステップ３８５で、データ・ストレージ・サービスの応答メッセージをオーバライドすることができる。ステップ３８５が実行される時点では、起こりうる２通りの状況が存在する可能性があり、すなわち、アクセス・マネージャ・サービスは、データ・ストレージ・サービスによって許可されているアクセスを拒否することまたはデータ・ストレージ・サービスによって拒否されているアクセスを許可することを希望している。

【００８１】

いずれの状況でも、ステップ３９０を実行することができ、そのステップでアクセス・マネージャ・サービスは要求側のセッション許可に関する必要なオーバライド変更をデータ・ストレージ・サービスに提供することができる。次に、アクセス・マネージャ・サービスはステップ３９５で、応答メッセージの応答を変更し、応答メッセージを要求側に送信することができる。

【００８２】

図４は、本明細書に開示されている本発明の配置の諸実施形態によりアクセス・マネージャ・サービスの動作を記述する方法４００の流れ図である。方法４００は、プロセス・フロー１００、システム２００のコンテキスト内で、あるいは方法３００に併せて、またはその両方で実行することができる。

【００８３】

方法４００はステップ４０５から始めることができ、そのステップでアクセス・マネージャ・サービスはデータ・ストレージ・サービスによって決定されたデータ要求および応答メッセージを入手することができる。ステップ４１０では、データ要求について所有者

指定のアクセス規則あるいはアクセス例外またはその両方を識別することができる。
【００８４】
ステップ４１５では、データ要求についてアクセス例外が存在するかどうかを判断することができる。アクセス例外が存在しない場合、識別されたアクセス規則はステップ４２０で集約することができる。
【００８５】
アクセス規則は個別のユーザが作成するか、可変レベルの細分性で存在するか、あるいは種々のパラメータに適用されるか、またはこれらの組み合わせが行われる可能性があるので、アクセス規則が相互に矛盾する潜在性が存在する可能性がある。アクセス・マネージャ・サービスは、優先順位の値を使用して、どのアクセス規則を優先しなければならないかを確立することができる。ステップ４２５では、必要であれば、この優先順位の値を使用して、識別されたアクセス規則間の矛盾を解決することができる。
【００８６】
ステップ４３０では、識別されたアクセス規則に基づいて、アクセス応答を決定することができる。ステップ４３５では、決定されたアクセス応答がデータ・ストレージ・サービスからの応答メッセージのものと一致するかどうかを判断することができる。
【００８７】
決定されたアクセス応答が応答メッセージと一致する場合、ステップ４４０を実行することができ、そのステップで応答メッセージが要求側（データ・コンシューマ）に伝達される。決定されたアクセス応答が応答メッセージと一致しない場合、ステップ４６５では決定されたアクセス応答によりアクセスを許可または拒否するように要求側のセッションを変更することができる。ステップ４７０では、決定されたアクセス応答を反映する応答メッセージを要求側に送信することができる。
【００８８】
ステップ４１５でアクセス例外が存在すると判断された場合、方法４００のフローはステップ４４５に移行することができ、そのステップでアクセス・マネージャ・サービスは要求側から認証を要求することができる。アクセス例外に関する認証は追加のセキュリティ段階にすることができ、機密または占有データ・アーティファクトについて推奨することができる。
【００８９】
認証は、ユーザ確認の質問／応答フォーマット、使い捨てパスワード、デジタル・トークン、スマート・カード上に保管された認証パラメータ、管理者によるセッションの手動許可、生体情報の読み取り、認証形式の組み合わせなどを含むがこれらに限定されない様々な形を取ることができる。
【００９０】
ステップ４５０では認証の妥当性を判断することができる。要求側が有効な認証を供給する場合、ステップ４５５を実行することができ、そのステップでアクセス・マネージャ・サービスはアクセス例外に応じて要求側のセッションを変更することができる。
【００９１】
要求側によって無効な認証が供給される場合、要求側はステップ４６０で無効な認証の通知を受けることができる。ステップ４６０からフローはステップ４４５に戻ることができ、そのステップでもう一度認証が要求される。
【００９２】
図５は、本明細書に開示されている本発明の配置の諸実施形態によりデータ所有者によるアクセス・マネージャ・サービスの使用を詳述する方法５００および５２０に関する流れ図の集合である。方法５００あるいは方法５２０またはその両方は、プロセス・フロー１００、システム２００のコンテキスト内で、あるいは方法３００あるいは方法４００またはその両方に併せて、またはその両方で実行することができる。
【００９３】
方法５００では、ユーザはステップ５０５でアクセス・マネージャ・ユーザ・インター

フェースを使用して新しいアクセス規則を定義することができる。次に、ステップ５１０では、入力されたアクセス規則に優先順位の値を割り当てることができる。

【００９４】

代わって、自動的にステップ５１０を実行し、アクセス規則を作成するユーザに基づいて優先順位の値を割り当てるようにアクセス・マネージャ・サービスを構成することができる。たとえば、管理者レベルのユーザによって作成されたアクセス規則には、チームレベルのユーザなどによって作成されたアクセス規則より高い優先順位の値を自動的に割り当てることができる。

【００９５】

ステップ５１５では、アクセス・マネージャ・サービスで使用するために新しいアクセス規則を保管することができる。

【００９６】

方法５２０はアクセス例外の作成を記述することができる。方法５２０はステップ５２５から始めることができ、そのステップで管理者はアクセス・マネージャ・ユーザ・インターフェース内のアクセス例外を定義することができる。ステップ５３０では、自動化認証（すなわち、アクセス・マネージャ・サービスによって自動的に生成された認証情報）を有効化するかどうかを判断することができる。

【００９７】

アクセス・マネージャ・サービスによって使用される自動化認証のタイプは、２つまたはそれ以上の識別手段を必要とする認証手法である厳密認証（strong authentication）を包含するように拡張することができる。たとえば、アクセス・マネージャ・サービスは一時パスワードとユーザ確認の質問／応答のセットを生成することができる。要求側は、アクセスするためにパスワードと応答の両方を正確に入力しなければならない。

【００９８】

自動化認証を有効化すると、アクセス・マネージャ・サービスはステップ５３５で管理者に認証情報を提供することができる。ステップ５４０では、管理者は、それに関するアクセスが許可される指定のユーザに認証情報を提供することができる。方法４００のステップ４４５および４５０のように、ステップ５４０からアクセス・マネージャ・サービスは指定のユーザを電子的に認証するステップに進むことができる。

【００９９】

自動化認証を有効化しない場合、ステップ５４５を実行することができ、そのステップで管理者は指定のユーザのアウト・オブ・バンド認証を待つことができる。たとえば、指定のユーザは、管理者に連絡し、識別情報（すなわち、アドレス、出生データ、社会保障番号）を口頭で提供することができる。

【０１００】

ステップ５５０では、有効な認証の受信を判断することができる。受信した認証が有効である場合、管理者はステップ５５５でアクセス・マネージャ・サービスに関するアクセス例外を手動で活動化することができる。受信した認証が無効である場合、方法５２０のフローはステップ５４５に戻ることができ、そのステップで管理者は有効な認証を待ち続けることができる。

【０１０１】

上記の図面内の流れ図およびブロック図は、本発明の様々な実施形態によるシステム、方法、およびコンピュータ・プログラムについて可能な実装例のアーキテクチャ、機能、および動作を例示している。この点に関しては、流れ図またはブロック図内の各ブロックは、指定の論理機能（複数も可）を実装するための１つまたは複数の実行可能命令を含む、コードのモジュール、セグメント、または一部分を表すことができる。また、いくつかの代替実装例では、ブロック内に示された機能は図面内に示された順序から外れて行われる可能性があることにも留意されたい。たとえば、連続して示されている２つのブロックは、関係する機能に応じて、実際にはほぼ同時に実行される場合もあれば、ときには逆の順序で実行される場合もある。また、ブロック図あるいは流れ図またはその両方の各ブロ

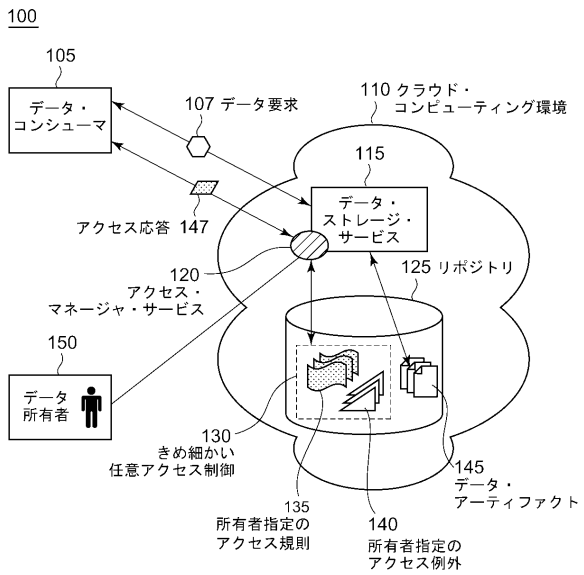
ックならびにブロック図あるいは流れ図またはその両方の複数ブロックの組み合わせは、指定の機能または動作を実行する特殊目的ハードウェアベースのシステムによって、または特殊目的ハードウェアとコンピュータ命令の組み合わせによって、実装可能であることも留意されるであろう。

【符号の説明】

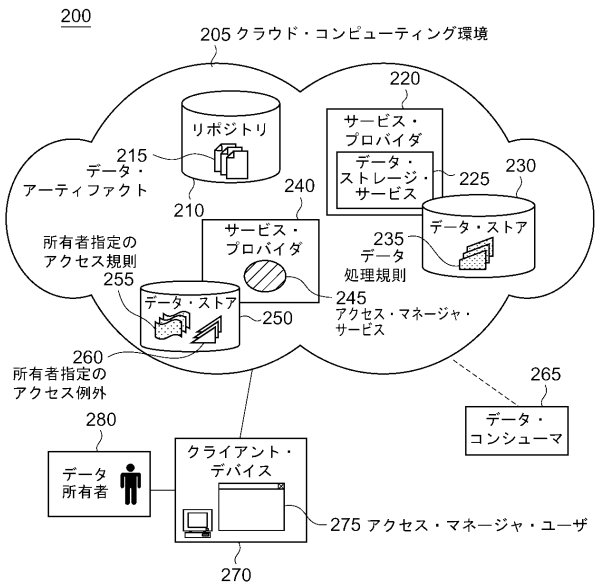
【０１０２】

２００　システム
２０５　クラウド・コンピューティング環境
２１０　リポジトリ
２１５　データ・アーティファクト
２２０　サービス・プロバイダ
２２５　データ・ストレージ・サービス
２３０　データ・ストア
２３５　データ処理規則
２４０　サービス・プロバイダ
２４５　アクセス・マネージャ・サービス
２５０　データ・ストア
２５５　所有者指定のアクセス規則
２６０　所有者指定のアクセス例外
２６５　データ・コンシューマ
２７０　クライアント・デバイス
２７５　アクセス・マネージャ・ユーザ・インターフェース
２８０　データ所有者

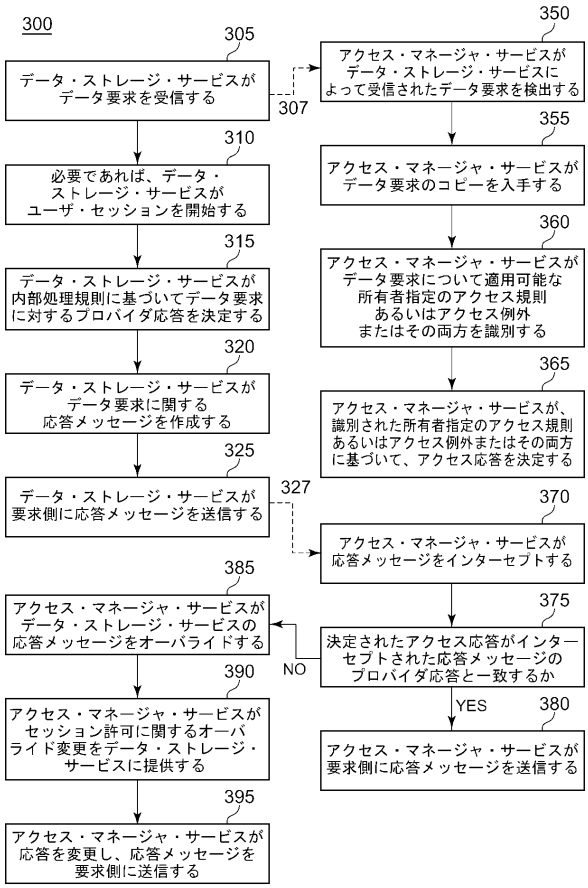
【図１】



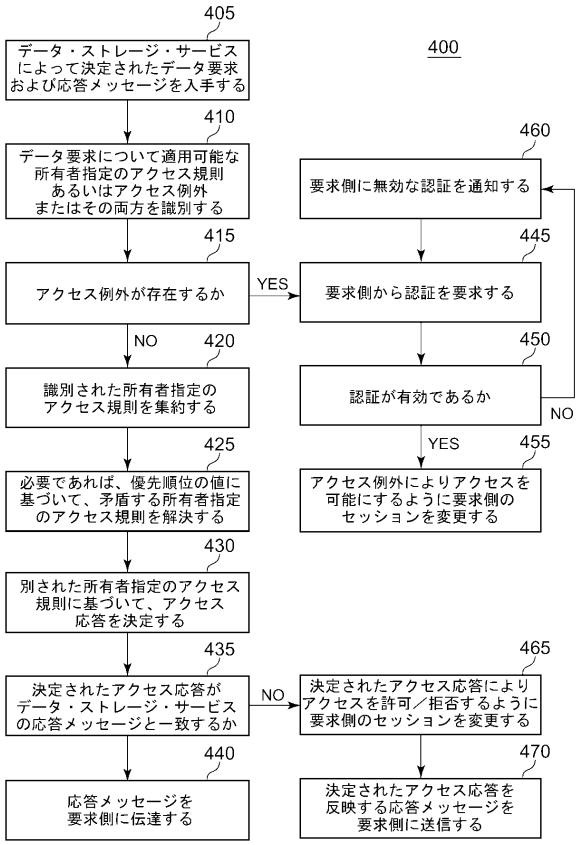
【図２】



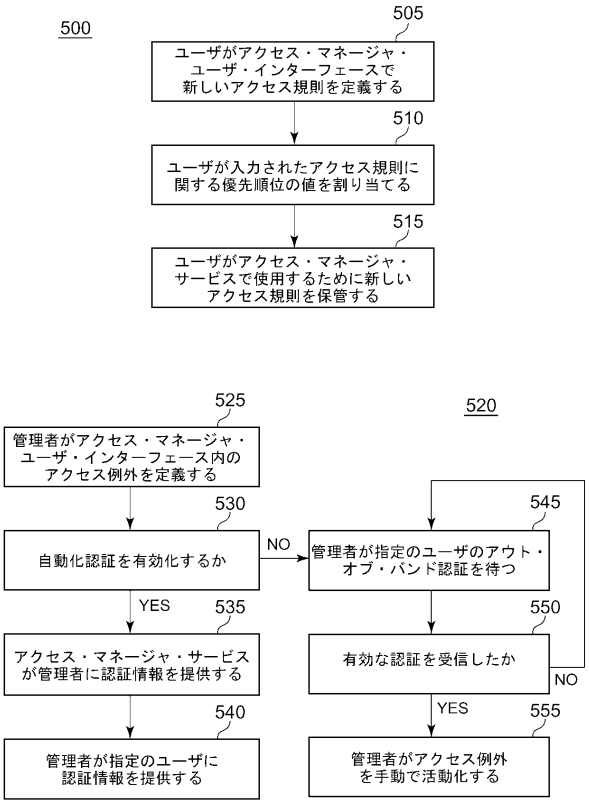
【図３】


300
305
データ・ストレージ・サービスがデータ要求を受信する
307
310
必要であれば、データ・ストレージ・サービスがユーザ・セッションを開始する
315
データ・ストレージ・サービスが内部処理規則に基づいてデータ要求に対するプロバイダ応答を決定する
320
データ・ストレージ・サービスがデータ要求に関する応答メッセージを作成する
325
データ・ストレージ・サービスが要求側に応答メッセージを送信する
327
385
アクセス・マネージャ・サービスがデータ・ストレージ・サービスの応答メッセージをオーバライドする
NO
390
アクセス・マネージャ・サービスがセッション許可に関するオーバライド変更をデータ・ストレージ・サービスに提供する
395
アクセス・マネージャ・サービスが応答を変更し、応答メッセージを要求側に送信する
350
アクセス・マネージャ・サービスがデータ・ストレージ・サービスによって受信されたデータ要求を検出する
355
アクセス・マネージャ・サービスがデータ要求のコピーを入手する
360
アクセス・マネージャ・サービスがデータ要求について適用可能な所有者指定のアクセス規則あるいはアクセス例外またはその両方を識別する
365
アクセス・マネージャ・サービスが、識別された所有者指定のアクセス規則あるいはアクセス例外またはその両方に基づいて、アクセス応答を決定する
370
アクセス・マネージャ・サービスが応答メッセージをインターセプトする
375
決定されたアクセス応答がインターセプトされた応答メッセージのプロバイダ応答と一致するか
YES
380
アクセス・マネージャ・サービスが要求側に応答メッセージを送信する

【図４】


400
405
データ・ストレージ・サービスによって決定されたデータ要求および応答メッセージを入手する
410
データ要求について適用可能な所有者指定のアクセス規則あるいはアクセス例外またはその両方を識別する
415
アクセス例外が存在するか
YES
NO
420
識別された所有者指定のアクセス規則を集約する
425
必要であれば、優先順位の値に基づいて、矛盾する所有者指定のアクセス規則を解決する
430
別された所有者指定のアクセス規則に基づいて、アクセス応答を決定する
435
決定されたアクセス応答がデータ・ストレージ・サービスの応答メッセージと一致するか
NO
440
応答メッセージを要求側に伝達する
460
要求側に無効な認証を通知する
445
要求側から認証を要求する
450
認証が有効であるか
NO
YES
455
アクセス例外によりアクセスを可能にするように要求側のセッションを変更する
465
決定されたアクセス応答によりアクセスを許可／拒否するように要求側のセッションを変更する
470
決定されたアクセス応答を反映する応答メッセージを要求側に送信する

【図５】


500
505
ユーザがアクセス・マネージャ・ユーザ・インターフェースで新しいアクセス規則を定義する
510
ユーザが入力されたアクセス規則に関する優先順位の値を割り当てる
515
ユーザがアクセス・マネージャ・サービスで使用するために新しいアクセス規則を保管する
525
管理者がアクセス・マネージャ・ユーザ・インターフェース内のアクセス例外を定義する
530
自動化認証を有効化するか
NO
YES
535
アクセス・マネージャ・サービスが管理者に認証情報を提供する
540
管理者が指定のユーザに認証情報を提供する
520
545
管理者が指定のユーザのアウト・オブ・バンド認証を待つ
550
有効な認証を受信したか
NO
YES
555
管理者がアクセス例外を手動で活動化する

フロントページの続き

(72)発明者　ステファン・ポール・クルガー
アイルランド　ダブリン１５　ムルフダルト　ダマスタウン・インダストリアル・エステート
(72)発明者　オルギエルド・スタニスラフ・ピエツル
アイルランド　ダブリン１５　ムルフダルト　ダマスタウン・インダストリアル・エステート

審査官　岸野　徹

(56)参考文献　特開２０１０－１９８１８６（ＪＰ，Ａ）
特開２００９－２１１６６８（ＪＰ，Ａ）
特開２００３－０３００６３（ＪＰ，Ａ）
特表２００９－５０７２７５（ＪＰ，Ａ）
米国特許出願公開第２００６／０１２３００５（ＵＳ，Ａ１）
特開２００８－２９９４１４（ＪＰ，Ａ）
こちら検証ラボ，日経ＳＹＳＴＥＭＳ　第２０９号，日本，日経ＢＰ社　Nikkei Business Publications,Inc.，２０１０年　８月２６日，pp.62-67

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　１２／００