(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7433294号
(P7433294)

(45)発行日　令和6年2月19日(2024.2.19)

(24)登録日　令和6年2月8日(2024.2.8)

(51)国際特許分類
Ｇ０６Ｆ　21/62　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/62　３１８

請求項の数　21　（全28頁）

(21)出願番号　特願2021-509188(P2021-509188)
(86)(22)出願日　令和1年8月21日(2019.8.21)
(65)公表番号　特表2021-535475(P2021-535475A)
(43)公表日　令和3年12月16日(2021.12.16)
(86)国際出願番号　PCT/CN2019/101760
(87)国際公開番号　WO2020/038400
(87)国際公開日　令和2年2月27日(2020.2.27)
審査請求日　令和4年8月17日(2022.8.17)
(31)優先権主張番号　201810962847.6
(32)優先日　平成30年8月22日(2018.8.22)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　510280589
京東方科技集團股▲ふん▼有限公司
ＢＯＥ　ＴＥＣＨＮＯＬＯＧＹ　ＧＲＯＵＰ　ＣＯ．，ＬＴＤ．
中華人民共和国１００００１５北京市朝陽區酒仙橋路１０號
Ｎｏ．１０　Ｊｉｕｘｉａｎｑｉａｏ　Ｒｄ．，Ｃｈａｏｙａｎｇ　Ｄｉｓｔｒｉｃｔ，Ｂｅｉｊｉｎｇ　１００００１５，ＣＨＩＮＡ
(74)代理人　100108453
弁理士　村山 靖彦
(74)代理人　100110364
弁理士　実広 信哉
(72)発明者　▲張▼ 乾

最終頁に続く

(54)【発明の名称】　アクセスコントロールポリシーの配置方法、装置、システム及び記憶媒体

(57)【特許請求の範囲】
【請求項１】
ターゲットリソースを作成する要求を受信することと、
当該要求に基づいて、前記ターゲットリソースに対して、当該ターゲットリソースとその親リソースのアクセスコントロールポリシーの間の継承関係を示すアクセスコントロールポリシーの継承属性が設定されているか否かを確定することと、
確定結果に基づいて、前記ターゲットリソースのアクセスコントロールポリシーを配置することと、を含み、
確定結果に基づいて前記ターゲットリソースのアクセスコントロールポリシーを配置することは、
前記ターゲットリソースに対して前記アクセスコントロールポリシーの継承属性が設定された場合、前記アクセスコントロールポリシーの継承属性の属性値に基づいて、前記ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承するか否かを判断することと、
判断結果に基づいて前記ターゲットリソースのアクセスコントロールポリシーを配置することと、を含むアクセスコントロールポリシーを配置するための装置が実行する方法。
【請求項２】
前記ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承するか否かを判断することは、
前記アクセスコントロールポリシーの継承属性の属性値が第１設定値である場合、前記

ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承すると確定することと、
前記アクセスコントロールポリシーの継承属性の属性値が第２設定値である場合、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承しないと確定することと、
前記アクセスコントロールポリシーの継承属性の属性値が第３設定値である場合、プリセットされた設定規則に基づき、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承するか否かを確定することと、を含む請求項１に記載の方法。
【請求項３】
前記ターゲットリソースのアクセスコントロールポリシーを配置することは、
前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承すると確定する場合、前記親リソースのアクセスコントロールポリシーのアイデンティティー属性に基づいて、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を設定することと、
前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承しないと確定する場合、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を確定することと、を含み、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を確定することは、前記ターゲットリソースに対して、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を作成すること、または、前記ターゲットリソースに対して、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を作成することを、ほかのエンティティに要求することと、を含み、
前記プリセットされた設定規則は、前記ターゲットリソースとその親リソースとのアクセスコントロールポリシーの間のデフォルト継承関係を示し、前記デフォルト継承関係は、継承すること、または、継承しないこと、を含む請求項２に記載の方法。
【請求項４】
前記要求に基づいて、前記ターゲットリソースに対して、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されているか否かを確定することと、
前記ターゲットリソースに対して前記パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されている場合、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性に、前記パーソナライズドアクセスコントロールポリシーのアイデンティティー属性を追加することと、をさらに含む請求項１～３の何れか１項に記載の方法。
【請求項５】
前記ターゲットリソースが既に作成され、且つそのアクセスコントロールポリシーの継承属性の属性値が、親リソースのアクセスコントロールポリシーを継承することを示す場合、前記親リソースのアクセスコントロールポリシーのアイデンティティー属性が変化したことを検出したことに応答して、変化した前記親リソースのアクセスコントロールポリシーのアイデンティティー属性に応じて、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を更新することをさらに含むことを特徴とする請求項１～４の何れか１項に記載の方法。
【請求項６】
前記要求は、リソース作成メッセージの形式を採用し、当該方法は、前記リソース作成メッセージから前記アクセスコントロールポリシーの継承属性の属性値を抽出すること、または、前記リソース作成メッセージから前記アクセスコントロールポリシーの継承属性の属性値と前記パーソナライズドアクセスコントロールポリシーの属性値を抽出すること、を含む請求項４に記載の方法。
【請求項７】
前記ターゲットリソースに対して前記アクセスコントロールポリシーの継承属性が設定

されない場合、デフォルトのポリシーの配置規則に基づいて、前記ターゲットリソースのアクセスコントロールポリシーを配置することをさらに含む請求項１に記載の方法。
【請求項８】
ターゲットリソースとその親リソースのアクセスコントロールポリシーの間の継承関係を確定することと、
前記ターゲットリソースを作成するための要求を送信することと、
前記要求に対するリソース作成応答を受信することを含み、
前記要求に、前記ターゲットリソースのアクセスコントロールポリシーの配置に用いられる、前記継承関係を示すアクセスコントロールポリシーの継承属性が設定され、
前記ターゲットリソースのアクセスコントロールポリシーの配置は、
前記アクセスコントロールポリシーの継承属性の属性値に基づいて、前記ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承するか否かを判断することと、
判断結果に基づいて前記ターゲットリソースのアクセスコントロールポリシーを配置することと、を含むアクセスコントロールポリシーを配置するための装置が実行する方法。
【請求項９】
ターゲットリソースを作成する要求を受信する受信モジュールと、
当該要求に基づいて、前記ターゲットリソースに対して、アクセスコントロールポリシーの継承属性が設定されているか否かを確定する属性確定モジュールと、
確定結果に基づいて、前記ターゲットリソースのアクセスコントロールポリシーを配置するポリシー配置モジュールを含み、
前記アクセスコントロールポリシーの継承属性が、当該ターゲットリソースとその親リソースとのアクセスコントロールポリシーの間の継承関係を示し、
前記ポリシー配置モジュールは、
前記ターゲットリソースに対して前記アクセスコントロールポリシーの継承属性が設定されていることに応答して、前記アクセスコントロールポリシーの継承属性の属性値に基づき、前記ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承するか否かを判断するための継承判断手段と、
判断結果に基づいて前記ターゲットリソースのアクセスコントロールポリシーを設定するためのポリシー設定手段を含む、アクセスコントロールポリシーを配置するための装置。
【請求項１０】
前記継承判断手段は、前記アクセスコントロールポリシーの継承属性の属性値が第１設定値である場合、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承すると確定し、前記アクセスコントロールポリシーの継承属性の属性値が第２設定値である場合、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承しないと確定し、前記アクセスコントロールポリシーの継承属性の属性値が第３設定値である場合、プリセットされた設定規則に基づいて、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承するか否かを確定する、請求項９に記載の装置。
【請求項１１】
前記ポリシー設定手段は、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承すると確定する場合、前記親リソースのアクセスコントロールポリシーのアイデンティティー属性に基づいて、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を設定し、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承しないと確定する場合、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を決定確定し、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を確定することは、前記ターゲットリソースに対して、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を作成すること、または、前記ターゲットリソースに対して、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を作成することを、ほかのエ

ンティティに要求することを含み、前記プリセットされた設定規則は、前記ターゲットリソースとその親リソースとのアクセスコントロールポリシーの間のデフォルト継承関係を示し、前記デフォルト継承関係は、継承すること、または、継承しないことを含む、請求項１０に記載の装置。

【請求項１２】

前記属性確定モジュールは、前記要求に基づいて、前記ターゲットリソースに対して、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されているか否かを確定するように構成され、ポリシー設定手段は、前記ターゲットリソースに対して前記パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されていることに応答して、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性に、前記パーソナライズドアクセスコントロールポリシーのアイデンティティー属性を追加するように構成された、請求項９～１１の何れか１項に記載の装置。

【請求項１３】

前記ポリシー配置モジュールは、前記ターゲットリソースが既に作成され、そのアクセスコントロールポリシーの継承属性の属性値が親リソースのアクセスコントロールポリシーを継承することを示す場合、前記親リソースのアクセスコントロールポリシーのアイデンティティー属性が変化したことを検出したことに応じて、変化した前記親リソースのアクセスコントロールポリシーのアイデンティティー属性に応じて、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を更新するためのポリシー更新手段をさらに含む、請求項９～１２の何れか１項に記載の装置。

【請求項１４】

前記要求は、リソース作成メッセージの形式を採用し、前記属性確定モジュールは、前記リソース作成メッセージから前記アクセスコントロールポリシーの継承属性の属性値を抽出し、または、前記リソース作成メッセージから前記アクセスコントロールポリシーの継承属性の属性値と前記パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値を抽出するように構成されている、請求項１２に記載の装置。

【請求項１５】

ポリシー設定手段は、前記ターゲットリソースに対して前記アクセスコントロールポリシーの継承属性が設定されていないことに応答して、デフォルトのポリシーの配置規則に基づいて前記ターゲットリソースのアクセスコントロールポリシーを配置するように構成されていることを特徴とする請求項９～１４の何れか１項に記載の装置。

【請求項１６】

ターゲットリソースとその親リソースのアクセスコントロールポリシーの間の継承関係を決定する確定モジュールと、

前記ターゲットリソースを作成する要求を送信する送信モジュールと、

前記要求に対するリソース作成応答を受信する受信モジュールを含み、

前記要求には、前記ターゲットリソースのアクセスコントロールポリシーの配置に用いられる、前記継承関係を示すアクセスコントロールポリシーの継承属性が設定され、

前記ターゲットリソースのアクセスコントロールポリシーの配置は、

前記アクセスコントロールポリシーの継承属性の属性値に基づいて、前記ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承するか否かを判断することと、

判断結果に基づいて前記ターゲットリソースのアクセスコントロールポリシーを配置することと、を含むアクセスコントロールポリシーを配置する装置。

【請求項１７】

実行可能な指令を記憶するメモリと、

前記メモリに結合され、且つ、請求項１～８の何れか１項に記載の方法を実現するように、前記実行可能な指令を実行するプロセッサと、を備える、アクセスコントロールポリシーを配置するためのコンピューティングデバイス。

【請求項１８】
１つ以上のプロセッサによって実行される際に前記プロセッサによって請求項１～８の何れか１項に記載の方法を実現させるようにするコンピュータプログラム指令が記憶されている、コンピュータ読取可能な記憶媒体。
【請求項１９】
ターゲットリソースを作成する要求を送信するための第１エンティティと、
請求項９～１５のいずれか１項に記載の装置を含む第２エンティティと、を含む、アクセスコントロールポリシーを配置するシステム。
【請求項２０】
前記第１エンティティは、アプリケーションエンティティを含み、前記第２エンティティは、共通サービスエンティティを含む、請求項１９に記載のシステム。
【請求項２１】
前記第１エンティティは、請求項１６に記載の装置を含む、請求項１９に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願
本願は、２０１８年８月２２日に提出された中国特許出願Ｎｏ．２０１８１０９６２８４７．６の権利を要求し、ここで、全文にて上述の中国特許出願公開の内容を本願の一部として引用する。
【０００２】
本開示は、モノのネットワーク技術の分野に関し、特に、アクセスコントロールポリシーの配置方法、装置、システム及び記憶媒体に関する。
【背景技術】
【０００３】
モノのネットワークにおいて、リソースに対するアクセスコントロールは、通常は属性に基づくものであり、即ち、リソース属性を設定することにより、リソースに対するアクセスをコントロールする。アクセスコントロールポリシー（ａｃｃｅｓｓＣｏｎｔｒｏｌＰｏｌｉｃｙ）リソースに記憶されているのは、アクセスコントロールポリシーのコンテンツであり、即ち、ある要求に対して授権可能であるか否かを評価する根拠となるコンテンツである。ターゲットリソースとアクセスコントロールポリシーリソースは、ターゲットリソースにおけるアクセスコントロールポリシーのアイデンティティー（ａｃｃｅｓｓＣｏｎｔｒｏｌＰｏｌｉｃｙＩＤｓ）属性によって接続されている。ターゲットリソースにアクセスする要求は、アクセスコントロールポリシーのアイデンティティー属性によって示される１つ以上のアクセスコントロールポリシーリソースの授権認証によって、要求に対して授権する動作を完了することができる。
【０００４】
関連する技術において、セキュリティポリシーは、様々な方式でデプロイすることができる。しかし、アクティブセキュリティポリシーのデプロイにおいて、あるリソースを作成する際に、アクセスコントロールポリシーのアイデンティティー属性値が受信者に送信されると、アプリケーション層が干渉しない場合、これは、当該リソースの親リソースのポリシー権限を放棄することを意味する。または、あるリソースに元々アクセスコントロールポリシーのアイデンティティー属性値がない場合、それに対して1つの、アクセスコントロールポリシーのアイデンティティー属性値を単独で追加すると、それがアクセスコントロールポリシーのアイデンティティー属性値を有したので、当該リソースの親リソースのポリシー権限を放棄することを意味する。このように、上下グレードのリソース及び親子リソースの間に、アクセスコントロールポリシーは互いに独立している。現在のＭ２Ｍ（マシン・ツー・マシン）システムにおいて、デバイスの種類が多く、且つ各デバイスの種類ごとにそれぞれのパーソナライズアクセスコントロールポリシーのニーズがあるの

で、独立したアクセスコントロールポリシーしか実現できない。
【発明の概要】
【課題を解決するための手段】
【０００５】
本開示の実施例の第１の局面によれば、アクセスコントロールポリシーを配置する方法が提供される。当該方法は、ターゲットリソースを作成する要求を受信することと、当該要求に基づいて、前記ターゲットリソースに対して、当該ターゲットリソースとその親リソースのアクセスコントロールポリシーの間の継承関係を示すアクセスコントロールポリシーの継承属性が設定されているか否かを確定することと、確定結果に基づいて、前記ターゲットリソースのアクセスコントロールポリシーを配置することと、を含む。
【０００６】
ある実施例において、確定結果に基づいて前記ターゲットリソースのアクセスコントロールポリシーを配置することは、前記ターゲットリソースに対して前記アクセスコントロールポリシーの継承属性が設定された場合、前記アクセスコントロールポリシーの継承属性の属性値に基づいて、前記ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承するか否かを判断することと、判断結果に基づいて前記ターゲットリソースのアクセスコントロールポリシーを配置することと、を含む。
【０００７】
ある実施例において、前記ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承するか否かを判断することは、前記アクセスコントロールポリシーの継承属性の属性値が第１設定値である場合、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承すると確定することと、前記アクセスコントロールポリシーの継承属性の属性値が第２設定値である場合、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承しないと確定することと、前記アクセスコントロールポリシーの継承属性の属性値が第３設定値である場合、プリセットされた設定規則に基づき、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承するか否かを確定することと、を含む。
【０００８】
ある実施例において、前記ターゲットリソースのアクセスコントロールポリシーを配置することは、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承すると確定する場合、前記親リソースのアクセスコントロールポリシーのアイデンティティー属性に基づいて、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を設定することと、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承しないと確定する場合、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を確定することと、を含み、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を確定することは、前記ターゲットリソースに対して、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を作成すること、または、前記ターゲットリソースに対して、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を作成することを、ほかのエンティティに要求することと、を含み、前記プリセットされた設定規則は、前記ターゲットリソースとその親リソースとのアクセスコントロールポリシーの間のデフォルト継承関係を示し、前記デフォルト継承関係は、継承すること、または、継承しないことを含む。
【０００９】
ある実施例において、前記方法は、前記要求に基づいて、前記ターゲットリソースに対して、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されているか否かを確定することと、前記ターゲットリソースに対して前記パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されている場合、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性に、前記パーソナライズドアクセスコントロールポリシーのアイデンティティー属性を追加

することと、をさらに含む。
【００１０】
ある実施例において、前記方法は、前記ターゲットリソースが既に作成され、且つそのアクセスコントロールポリシーの継承属性の属性値が、親リソースのアクセスコントロールポリシーを継承することを示す場合、前記親リソースのアクセスコントロールポリシーのアイデンティティー属性が変化したことを検出したことに応答して、変化した前記親リソースのアクセスコントロールポリシーのアイデンティティー属性に応じて、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を更新することをさらに含む。
【００１１】
ある実施例において、前記要求は、リソース作成メッセージの形式を採用する。当該方法は、前記リソース作成メッセージから前記アクセスコントロールポリシーの継承属性の属性値を抽出すること、または、前記リソース作成メッセージから前記アクセスコントロールポリシーの継承属性の属性値と前記パーソナライズドアクセスコントロールポリシーの属性値を抽出すること、を含む。
【００１２】
ある実施例において、前記方法は、前記ターゲットリソースに対して前記アクセスコントロールポリシーの継承属性が設定されない場合、デフォルトのポリシーの配置規則に基づいて、前記ターゲットリソースのアクセスコントロールポリシーを配置することをさらに含む。
【００１３】
本開示の実施例の第２の局面によれば、アクセスコントロールポリシーを配置する方法が提供される。当該方法は、ターゲットリソースとその親リソースのアクセスコントロールポリシーの間の継承関係を確定することと、前記ターゲットリソースを作成するための要求を送信することと、前記要求に対するリソース作成応答を受信することを含み、前記要求には、前記ターゲットリソースのアクセスコントロールポリシーの配置に用いられる、前記継承関係を示すアクセスコントロールポリシーの継承属性が設定されている。
【００１４】
本開示の実施例の第３の局面によれば、アクセスコントロールポリシーを配置するための装置が提供される。当該デバイスは、ターゲットリソースを作成する要求を受信する受信モジュールと、当該要求に基づいて、前記ターゲットリソースに対してアクセスコントロールポリシーの継承属性が設定されているか否かを確定する属性確定モジュールと、確定結果に基づいて、前記ターゲットリソースのアクセスコントロールポリシーを配置するポリシー配置モジュールを含み、前記アクセスコントロールポリシーの継承属性が、当該ターゲットリソースとその親リソースとのアクセスコントロールポリシーの間の継承関係を示す。
【００１５】
ある実施例において、前記ポリシー配置モジュールは、前記ターゲットリソースに対して前記アクセスコントロールポリシーの継承属性が設定されていることに応答して、前記アクセスコントロールポリシーの継承属性の属性値に基づき、前記ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承するか否かを判断するための継承判断手段と、判断結果に基づいて前記ターゲットリソースのアクセスコントロールポリシーを設定するためのポリシー設定手段とを含む。
【００１６】
ある実施例において、前記継承判断手段は、前記アクセスコントロールポリシーの継承属性の属性値が第１設定値である場合、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承すると確定し、前記アクセスコントロールポリシーの継承属性の属性値が第２設定値である場合、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承しないと確定し、前記アクセスコントロールポリシーの継承属性の属性値が第３設定値である場合、プリセットされた設定規則に基づいて、前

記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承するか否かを確定する。

【００１７】

ある実施例において、前記ポリシー設定手段は、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承すると確定する場合、前記親リソースのアクセスコントロールポリシーのアイデンティティー属性に基づいて、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を設定し、前記ターゲットリソースが前記親リソースのアクセスコントロールポリシーを継承しないと確定する場合、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を確定し、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を確定することは、前記ターゲットリソースに対して、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を作成すること、または、前記ターゲットリソースに対して、それに使用されるアクセスコントロールポリシーのアイデンティティー属性を作成することを、ほかのエンティティに要求することを含み、前記プリセットされた設定規則は、前記ターゲットリソースとその親リソースとのアクセスコントロールポリシーの間のデフォルト継承関係を示し、前記デフォルト継承関係は、継承すること、または、継承しないことを含む。

【００１８】

ある実施例において、前記属性確定モジュールは、前記要求に基づいて、前記ターゲットリソースに対して、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されているか否かを確定するように構成され、前記ポリシー設定手段は、前記ターゲットリソースに対して前記パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されていることに応答して、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性に、前記パーソナライズドアクセスコントロールポリシーのアイデンティティー属性を追加するように構成される。

【００１９】

ある実施例において、前記ポリシー配置モジュールは、前記ターゲットリソースが既に作成され、そのアクセスコントロールポリシーの継承属性の属性値が親リソースのアクセスコントロールポリシーを継承することを示す場合、前記親リソースのアクセスコントロールポリシーのアイデンティティー属性が変化したことを検出したことに応じて、変化した前記親リソースのアクセスコントロールポリシーのアイデンティティー属性に応じて、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を更新するためのポリシー更新手段をさらに含む。

【００２０】

ある実施例において、前記要求は、リソース作成メッセージの形式を採用する。前記属性確定モジュールは、前記リソース作成メッセージから前記アクセスコントロールポリシーの継承属性の属性値を抽出し、または、前記リソース作成メッセージから前記アクセスコントロールポリシーの継承属性の属性値と前記パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値を抽出するように構成されている。

【００２１】

ある実施例において、前記ポリシー設定手段は、前記ターゲットリソースに対して前記アクセスコントロールポリシーの継承属性が設定されていないことに応答して、デフォルトのポリシーの配置規則に基づいて前記ターゲットリソースのアクセスコントロールポリシーを配置するように構成されている。

【００２２】

本開示の実施例の第４の局面によれば、アクセスコントロールポリシーを配置する装置が提供される。当該装置は、ターゲットリソースとその親リソースのアクセスコントロールポリシーの間の継承関係を決定する確定モジュールと、前記ターゲットリソースを作成する要求を送信する送信モジュールと、前記要求に対するリソース作成応答を受信する受信モジュールを含み、前記要求には、前記ターゲットリソースのアクセスコントロールポ

リシーの配置に用いられる、前記継承関係を示すアクセスコントロールポリシーの継承属性が設定されている。

【００２３】

本開示の実施例の第５の局面によれば、アクセスコントロールポリシーを配置するコンピューティングデバイスが提供される。当該コンピューティングデバイスは、実行可能な指令を記憶するメモリと、前記メモリに結合され、且つ、前述の本開示の実施例による方法を実現するように、前記実行可能な指令を実行するプロセッサと、を備える。

【００２４】

本開示の実施例の第６の局面によれば、コンピュータ読取可能な記憶媒体が提供される。当該コンピュータの読取り可能な記憶媒体に、１つ以上のプロセッサによって実行される際に、前記プロセッサによって上述の本開示の実施例による方法を実現させるコンピュータプログラム指令が記憶されている。

【００２５】

本開示の実施例の第７の局面によれば、アクセスコントロールポリシーを配置するシステムが提供される。当該システムは、ターゲットリソースを作成する要求を送信するための第１エンティティと、請求項１０～１８のいずれか１項に記載の装置を含む第２エンティティと、を含む。

【００２６】

ある実施例において、前記第１エンティティは、アプリケーションエンティティを含み、前記第２エンティティは、共通サービスエンティティを含む。

【００２７】

ある実施例において、前記第１エンティティは、本開示の実施例の第４の局面に記載の装置を含む。

【図面の簡単な説明】

【００２８】

図面を参照して具体的な実施例を詳細に説明すると、本開示の上記及びほかの特徴及び利点はより顕著になる。

【００２９】

【図１】図１は、本開示の実施例を適用可能な環境の概略図である。

【図２】図２は、本開示の方法の一実施例のフロー模式図である。

【図３】図３は、本開示の方法の別の実施例のフロー模式図である。

【図４】図４は、本開示の方法の別の実施例のフロー模式図である。

【図５】図５は、本開示の方法の別の実施例のフロー模式図である。

【図６】図６は、親リソースと子リソースのツリー構造を示す模式図である。

【図７】図７は、本開示の装置の一実施例の構造ブロック図である。

【図８】図８は、本開示の装置のほかの実施例の構造ブロック図である。

【図９】図９は、本開示の装置のほかの実施例の構造ブロック図である。

【発明を実施するための形態】

【００３０】

以下の説明では、限定ではなく、説明するためのことであり、本開示を明確に且つ徹底的に理解するために、システム構造、インタフェース及び技術のような開示される実施例の特定の詳細が述べられる。しかしながら、当業者は、本開示の精神及び範囲から大きく逸脱しない場合、本開示が、本明細書に記載された詳細に精確に合致するほかの実施例によって実施できることを容易に理解できる。また、本明細書において、簡単で明瞭化させるために、熟知されているデバイス、回路及び方法の詳細な説明は省略され、余分な詳細及び可能な混乱を回避する。

【００３１】

また、別に指定しない限り、「第一」及び／または「第二」などは、時間、空間、順序などを暗示するつもりはない。逆に、このような用語は、特徴、手段、アイテム等に対するアイデンティファイア、名称等としてのみ使用される。例えば、第１オブジェクトと第

２オブジェクトは、一般的に、オブジェクトＡとオブジェクトＢ、または、２つの異なるオブジェクト、または、２つの同じオブジェクト、または、同一のオブジェクトに対応している。

【００３２】

モノのネットワークは、検知層、ネットワーク層及びアプリケーション層を含む。検知層は、赤外線センサ、電子ラベル、カードリーダー、センサなどの検知端末を含む様々なセンサで構成されている。検知層は、モノのインターネットが物体を認識し、情報を収集するソースである。ネットワーク層は、インターネット、テレビネットワーク、ネットワーク管理システム、クラウドコンピューティングプラットフォームなどの様々なネットワークからなり、検知層によって取得された情報の伝達と処理を行う。アプリケーション層は、モノのネットワークとユーザのインタフェースであり、業界のニーズと組み合わせて、モノのインターネットの知能的な応用を実現する。Ｍ２Ｍアーキテクチャに対応するアプリケーション層において、それぞれのデバイスとセンサにおけるアプリケーションエンティティ（Ａｐｌｉｃａｔｉｏｎ　Ｅｎｔｉｔｙ，ＡＥ）は、応用に対する管理、及び、応用との交互を行う、標準化されたインタフェースを提供する。アプリケーション層とネットワーク層との間のサービス層において、共通サービスエンティティ（Ｃｏｍｍｏｎ　Ｓｅｒｖｉｃｅｓ　Ｅｎｔｉｔｙ、ＣＳＥ）は、リソース共有と相互操作性をサポートする。モノのネットワークにおいては、セキュリティ層の面において、アクセスコントロールポリシーのデプロイがある。アクセスコントロールポリシーは、例えば、既知のブラックリストユーザに対する制限、内部ビッグデータ分析ホストに対する許容／制限、特殊な機構組織に対する一部権限の許容／制限、エリア防衛に対する権限デプロイなどを含む。従来のアクセスコントロールポリシーの配置案において、アクセスコントロールポリシー（ａｃｃｅｓｓＣｏｎｔｒｏｌ　Ｐｏｌｉｃｙ）リソースにおいて記憶されているのは、アクセスコントロールポリシーのコンテンツである。アクセスコントロールポリシーは、一つのグループのアクセスコントロール規則を表す属性権限を含む。アクセスコントロールポリシーリソースが複数設定されることができる。それぞれのアクセスコントロールポリシーリソースに対して、対応するアイデンティファイアが設定されている。

【００３３】

アクセスコントロールポリシーリソースは、ルートリソースの下で配置されてもよい。ルートリソース下のターゲットリソースには、アクセスコントロールポリシーのアイデンティティー（ａｃｃｅｓｓＣｏｎｔｒｏｌ　ＰｏｌｉｃｙＩＤｓ）属性が設定されてもよい。アクセスコントロールポリシーのアイデンティティー属性の属性値は、アクセスコントロールポリシーのアイデンティファイアリストを含むことができる。リストには、少なくとも１つのアクセスコントロールポリシーアイデンティファイアが含まれている。ターゲットリソースとアクセスコントロールポリシーリソースは、アクセスコントロールポリシーのアイデンティティー属性値により接続されている。

【００３４】

ターゲットリソースにアクセスする要求に対する授権は、アクセスコントロールポリシーのアイデンティティー属性におけるアクセスコントロールポリシーのアイデンティファイアリストのうちの１つ以上のアイデンティファイアに対応するアクセスコントロールポリシーリソースの授権認証を必要とする。ターゲットリソースには、アクセスコントロールポリシーのアイデンティティー属性がない場合、授権評価は、その親リソースのアクセスコントロールポリシーのアイデンティティー属性値に対応するアクセスコントロールポリシーのアイデンティティー属性により行われ、または、ローカルポリシーにおける要求者の関連コンテンツに基づいて評価する。

【００３５】

従来のアクセスコントロールポリシーの配置案には、比較的に重大な欠陥がある。一、発起者が、アクティブセキュリティポリシーのデプロイを行うと、例えば、リソースを作成する時にアクセスコントロールポリシーのアイデンティティー属性値を属性値の１つとして受信者に送信すると、アプリケーション層が干渉しない場合には、親リソースのポリ

シー権限を放棄することを意味する。二、リソースは、初期にアクセスコントロールポリシーのアイデンティティー属性値がない時に、親リソースのアクセスコントロールポリシーに従うが、それにアクセスコントロールポリシーの属性値を単独で追加すると、親リソースのポリシー権限を放棄することを意味する。

【００３６】

以下、大規模なモノのネットワークのデバイス管理のシーンを例として説明する。大規模なモノのネットワークのデバイス管理プラットフォームは、大量の登録デバイスと多くのアクセスインタラクティブデータを持っている。このシーンにおいて、従来のアクセスコントロールポリシーの配置方法は、リソースのコントロールアクセスポリシーに対して、独立したデプロイ配置を行い、即ち、各ユーザに対して自体のアクセスコントロールポリシーを、独立して配置することである。言い換えれば、関連技術において採用しているのは、独立したアクセスコントロールポリシーであり、即ち、上下グレードの間と親子の間に互いに独立している。

【００３７】

しかし、当該シーンにおいて、プラットフォームは、ユーザのレベルを区分し、且つ包含関係があるかもしれない。例えば、高級機密組織において、デバイス情報の管理について、使用するユーザが、異なる機密レベルに分けられ、機密レベルが高いほど、見られる情報が多い。この時、独立したアクセスコントロールポリシーを採用すると、問題を引き起こすかもしれない。例えば、大規模なモノのネットワークのデバイス管理プラットフォームのグローバルアクセスコントロールポリシー情報は、当該プラットフォームの下の任意のリソースも使用できるアクセスコントロールポリシー情報として、機密情報に属するものであり、一般のユーザに知られるべきではない。また、グローバルアクセスコントロールポリシー情報の数が多く、ユーザにとってそれらを取得する可能性がない。グローバルアクセスコントロールポリシー情報を取得して再構築することで新しいアクセスコントロールポリシーのセットを生成することは、大部分の、演算力が低いモノのネットワークのデバイスにとっては実行可能性がない。従って、従来の独立したアクセスコントロールポリシーの配置方法は、アクセスのセキュリティコントロールに関するユーザの意思の具現化を制限する。

【００３８】

図１は、本開示の実施例を適用可能な環境を示す概略図である。図１に示すように、当該環境は、発起者１１０と共通サービスエンティティ（ＣＳＥ）１２０とを含むことができる。発起者１１０は、アプリケーションエンティティ（ＡＥ）であってもよい。

【００３９】

発起者１１０は、ターゲットリソースとその親リソースのアクセスコントロールポリシーの間の継承関係１０１を先に確定してもよい。ターゲットリソースは、発起者１１０が作成しようとするリソースである。その後、発起者１１０は、前記ターゲットリソースを作成する要求１０２を共通サービスエンティティ１２０に送信する。前記要求には、前記ターゲットリソースのアクセスコントロールポリシーの配置に用いられる、前記継承関係を示すアクセスコントロールポリシーの継承属性が設けられている。リソースは、ＣＳＥ、それぞれのデバイスとセンサにおけるアプリケーションエンティティ（Ａｐｐｌｉｃａｔｉｏｎ　Ｅｎｔｉｔｙ，ＡＥ）、コンテナ、ソフトウェアなどに用いるリソースを含むことができる。当該リソース作成要求１０１には、作成しようリソースの属性に関する属性値が含まれてもよい。前記属性値は、アクセスコントロールポリシーの継承属性値を含むことができる。

【００４０】

共通サービスエンティティ１２０は、受信したリソース作成要求に対して処理１０３を行う。共通サービスエンティティ１２０は、当該リソース作成要求を分析し、且つ、当該要求から属性値を抽出することにより、それに応じて当該リソースを作成することができる。ある実施例において、当該要求からアクセスコントロールポリシーの継承属性値が抽出されると、共通サービスエンティティ１２０は、リソースの作成中に、抽出されたアク

セスコントロールポリシーの継承属性値に応じて、当該リソースのアクセスコントロールポリシーのアイデンティティー属性を設定することができる。

【００４１】

共通サービスエンティティ１２０は、リソースの作成が完了した後、リソース作成応答１０４を発起者１１０に送信する。選択可能に、当該リソース作成応答１０４は、リソースの作成の詳細を含む。発起者１１０は、前記要求に対するリソース作成応答１０４を受信する。選択可能に、発起者１１０は、当該リソース作成応答１０４に含まれる詳細をローカルに記憶することができる。

【００４２】

本開示の実施例によれば、アクセスコントロールポリシーの継承属性は、ターゲットリソースを作成しようとするエンティティによって提供することができる。共通サービスエンティティＣＳＥは、現在の要求におけるアクセスコントロールポリシーの継承属性に基づき、前記ターゲットリソースのアクセスコントロールポリシーを配置することができる。これにより、異なる要求に応じて、異なるアクセスコントロールポリシー、または、発起者の意思を満足するアクセスコントロールポリシーを柔軟に配置することができる。

【００４３】

図２は、本開示のアクセスコントロールポリシーの配置方法の一実施例のフロー模式図を示す。当該アクセスコントロールポリシーの配置方法は、共通サービスエンティティによって実行することができる。

【００４４】

ステップ２０１において、ターゲットリソースを作成する要求を受信する。前記要求は、ＡＥから受信できる。

【００４５】

ステップ２０２において、当該要求に基づいて、ターゲットリソースに対してアクセスコントロールポリシーの継承属性が設定されているか否かを確定する。アクセスコントロールポリシーの継承属性は、当該ターゲットリソースとその親リソースのアクセスコントロールポリシーの間の継承関係を示す。このような継承関係は、継承することであってもよいし、継承しないことであってもよい。一般的には、継承は、オブジェクトを別のオブジェクトに基づくものとし、且つ、類似した実現メカニズムを保持することであることが理解できる。本明細書において使用される場合、リソースＡがリソースＢのアクセスコントロールポリシーを「継承」することは、リソースＡがリソースＢの子リソースであり、リソースＢがリソースＡの親リソースであり、また、「継承」により、子リソースＡが親リソースＢの各種のアクセスコントロールポリシーを有することができることを意味する。

【００４６】

具体的な実現においては、リソースが示すエンティティが異なるので、リソース間の親子関係の形式は様々である。一例において、親リソースは、車に取り付けられたブラックボックスであってもよく、その子リソースは、ブラックボックスに取り付けられた故障コード記録装置、燃費記録装置などであってもよい。別の例において、親リソースは、室内に取り付けられたエアコンであってもよく、その子リソースは、エアコンに取り付けられた温度センサ、湿度センサなどであってもよい。ツリー型のデバイスまたはリソーストポロジ構造図において、親リソースは、親ノードに対応し、子リソースは、親ノードの子ノードに対応する。

【００４７】

ある実施例において、当該確定は、当該要求において、継承関係に対する関連ユーザの指示を検索することによって行われる。当該要求が継承関係に対する指示を含む場合、ターゲットリソースに対してアクセスコントロールポリシーの継承属性が設定されていると確定する。前記指示は、ユーザによって指定された、アクセスコントロールポリシーの継承属性のための属性値であってもよい。

【００４８】

ステップ２０３において、確定結果に基づいて、ターゲットリソースのアクセスコント

ロールポリシーを配置する。配置されたアクセスコントロールポリシーは、その後の、ターゲットリソースへのアクセスをコントロールするためのものである。ある実施例において、確定結果は、ターゲットリソースに対してアクセスコントロールポリシーの継承属性が設定されていることを示すことができ、これは、当該ターゲットリソースが親リソース（もしあれば）のアクセスコントロールポリシーを継承することを示す。これにより、親リソースのアクセスコントロールポリシーに基づき、ターゲットリソースのアクセスコントロールポリシーを配置することができる。確定結果は、ターゲットリソースに対してアクセスコントロールポリシーの継承属性が設定されていないことを示すこともできる。ある実施例において、これは、発起者がまだアクセスコントロールポリシーの継承属性に対する設定をサポートしていないことを示すかもしれない。この時、関連技術におけるデフォルトのポリシーの配置規則に従って、ターゲットリソースのアクセスコントロールポリシーを配置することにより、このような従来の発起者と互換性を有することができる。

【００４９】

本開示の実施例の方法によれば、アクセスコントロールポリシーの継承属性に基づき、親リソースのアクセスポリシー権限を継承するか否かを確定することにより、子リソースのアクセスコントロールポリシーを効率的に設定・変更することができる。また、継承関係に対するユーザの指示に基づいて、アクセスコントロールポリシーの配置と変更を行うことができるので、ユーザの意思に応じて、アクセスコントロールポリシーを柔軟に配置することができ、ユーザの使用体験を改善することができる。

【００５０】

図３は、本開示の一実施例における配置アクセスコントロールポリシーのフロー模式図を示す。

【００５１】

ステップ３０１において、ターゲットリソースに対してアクセスコントロールポリシーの継承属性が設定されていると確定する場合、アクセスコントロールポリシーの継承属性の属性値に基づいて、ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承するか否かを判断する。例示的に、アクセスコントロールポリシーの継承属性の属性値は、「継承」を示す第１設定値と、「継承しない」を示す第２設定値とを有することができる。選択可能に、アクセスコントロールポリシーの継承属性の属性値は、任意の継承関係を受け入れることができることを示す第３設定値をさらに有することができる。

【００５２】

ステップ３０２において、判断結果に基づいて、ターゲットリソースのアクセスコントロールポリシーを配置する。アクセスコントロールポリシーの継承属性の属性値は、要求の発起者の、ターゲットリソースのアクセスコントロールに対する意思と、ターゲットリソースとその親リソースとの間のアクセスコントロールポリシーの継承関係に対する意思を示すことができる。当該属性値によって、その親リソースのアクセスコントロールポリシー権限を継承するか、または、ほかの（デフォルトのものを含む）アクセスコントロールポリシーを採用しようかを確定することができる。

【００５３】

一実施例において、アクセスコントロールポリシーの継承属性の属性値が第１設定値である場合、ターゲットリソースが親リソースのアクセスコントロールポリシーを継承すると確定し、アクセスコントロールポリシーの継承属性の属性値が第２設定値である場合、ターゲットリソースが親リソースのアクセスコントロールポリシーを継承しないと確定する。アクセスコントロールポリシーの継承属性の属性値が第３設定値である場合、プリセットされた配置規則に従ってアクセスコントロールポリシーを配置することができると確定する。プリセットされた配置規則は、前記ターゲットリソースとその親リソースのアクセスコントロールポリシーの間のデフォルトの継承関係を示すことができる。前記デフォルトの継承関係は、継承すること、または、継承しないことを含む。

【００５４】

第１設定値、第２設定値及び第３設定値には、値を適切に割り当てることができる。例

えば、第１設定値は１、第２設定値は０、第３設定値は空の値などとすることができる。これにより、属性値が１の場合、ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承することを示すので、親リソースのアクセスコントロールポリシーのアイデンティティー属性に基づき、ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を設定する。属性値が０の場合、ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承しないことを示す。この時、当該ターゲットリソースに対してアクセスコントロールポリシーのアイデンティティー属性を作成することを要求することができる。例示的に、要求の発起者に位置する第１エンティティを作成するよう要求することができる。代替的に、共通サービスエンティティ自体によって作成することもできる。アクセスコントロールポリシーのアイデンティティー属性の作成は、エンティティのアプリケーション層によって行われてもよい。属性値が空の値である場合、プリセットされた配置規則によって示されたデフォルトの継承関係、または、親リソースのアクセスコントロールポリシーのアイデンティティー属性、に基づいて、ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を設定したり、ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を設定するようにアプリケーション層に要求することができる。

【００５５】

本開示の実施例によれば、要求に携帯されているアクセスコントロールポリシーの継承属性の設定は簡単である（例えば、０、１、空の値であってもよい）ので、本開示の実施例の技術案は、非軽量化装置（例えば、携帯電話）だけでなく、論理が単一で、コンピューティング能力がなく、または、低いコンピューティング能力のみを有する軽量化装置にも適用できる。例えば、温度計デバイスは、論理が単一であるデバイスであり、本開示の実施例によるアクセスコントロールポリシーの継承属性の設定値は、温度計デバイスにとって簡単で固定的なものである。

【００５６】

アクセスコントロールポリシーのアイデンティティー属性値は、アクセスコントロールポリシーのアイデンティファイアリストを含むことができる。各アイデンティファイアリストは、少なくとも１つのアクセスコントロールポリシーのアイデンティファイアを含む。ある実施例において、親リソースのアクセスコントロールポリシーのアイデンティティー属性値に基づき、ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を設定することは、親リソースのアクセスコントロールポリシーのアイデンティファイアリストを、ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性にコピーすることを含む。

【００５７】

図４は、本開示の別の実施例における配置アクセスコントロールポリシーのフロー模式図を示す。

【００５８】

ステップ４０１において、ターゲットリソースを作成する際に、ターゲットリソースに対してパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されているか否かを確定する。パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値は、ユーザが所望するパーソナライズドアクセスコントロールポリシーのアイデンティファイアリストを含むことができる。ある実施例において、ターゲットリソースを作成するメッセージ要求にアクセスコントロールポリシーのアイデンティティー属性値が含まれている場合、それをパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値と見なすことができる。

【００５９】

ステップ４０２において、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されている場合、ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性には、当該パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値を追加する。

【００６０】
一実施例において、ターゲットリソースを作成する際に、ターゲットリソースに対して設定されたアクセスコントロールポリシーの継承属性の属性値は１であり、ターゲットリソースに対してパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されていない場合、共通サービスエンティティＣＳＥは、親リソースのアクセスコントロールポリシーのアイデンティティー属性の属性値をターゲットリソースにコピーし、ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性とする。親リソースのアクセスコントロールポリシーのアイデンティティー属性の属性値は、親リソースによって採用されるアクセスコントロールポリシーのアイデンティファイアリストを含む。
【００６１】
ターゲットリソースに対して設定されたアクセスコントロールポリシーの継承属性の属性値が１であり、ターゲットリソースに対してパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が設定されている場合、共通サービスエンティティは、親リソースのアクセスコントロールポリシーのアイデンティティー属性値をターゲットリソースにコピーするとともに、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性の属性値をターゲットリソースに追加してターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性とする。このように、ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性は、親リソースのアクセスコントロールポリシーのアイデンティティー属性値とパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値を含む。
【００６２】
別の実施例において、ターゲットリソースを作成する際に、ターゲットリソースに対して設定されたアクセスコントロールポリシーの継承属性の属性値は０であり、ターゲットリソースに対してパーソナライズドアクセスコントロールポリシーの属性値が設定されていなく、共通サービスエンティティは、アプリケーション層から、ターゲットリソースに用いるアクセスコントロールポリシーのアイデンティティーを要求する。共通サービスエンティティは、アプリケーション層によって作成されたアクセスコントロールポリシーのアイデンティファイアリストをターゲットリソースに追加し、ターゲットリソースのアクセスコントロールポリシーの属性値とする。
【００６３】
ターゲットリソースに対して設定されたアクセスコントロールポリシーの継承属性の属性値が０であり、ターゲットリソースに対してパーソナライズドアクセスコントロールポリシーの属性値が設定されている場合、共通サービスエンティティは、アプリケーション層によって作成されたアクセスコントロールポリシーのアイデンティティーをターゲットリソースにコピーするとともに、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値をターゲットリソースに追加してターゲットリソースのアクセスコントロールポリシーの属性とする。このように、ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性は、アプリケーション層によって作成されたアクセスコントロールポリシーのアイデンティファイアリストと、ユーザが所望するパーソナライズドアクセスコントロールポリシーのアイデンティファイアリストとを含む。
【００６４】
一実施例において、前記要求は、リソース作成メッセージの形式が採用されている。そのうち、リソース作成メッセージは、アクセスコントロールポリシーの継承属性の属性値を携帯する。代替的に、リソース作成要求は、アクセスコントロールポリシーの継承属性の属性値とパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値を同時に携帯することができる。共通サービスエンティティは、リソース作成メッセージにおける、リソースのアクセスコントロールポリシーの継承属性に関する情報により、当該リソースのアクセスコントロールポリシーを配置することができる。
【００６５】

付加的に、共通サービスエンティティは、リソースを操作するためのほかの要求、例えば、リソース更新要求に含まれるアクセスコントロールポリシーの継承属性の属性値に基づき、ターゲットリソースのアクセスコントロールポリシーの継承属性を更新し、且つ、その属性値によって示される継承関係により、ターゲットリソースのアクセスコントロールポリシーを更新することができる。

【００６６】

図５は、本開示のアクセスコントロールポリシーの配置方法の別の実施例のフロー模式図を示す。

【００６７】

ステップ５０１において、ターゲットリソースを作成するためのリソース作成メッセージを受信する。

【００６８】

ステップ５０２において、リソース作成メッセージにアクセスコントロールポリシーの継承属性の属性情報が携帯されているか否かを判断する。もしそうであれば、ステップ５０４に進み、そうでなければ、ステップ５０３に進む。例示的に、リソース作成メッセージには、アクセスコントロールポリシーの継承属性の属性情報を含むように、フィールドのｉｎｈｅｒｉｔａｎｃｅを設定することができる。フィールドのｉｎｈｅｒｉｔａｎｃｅの値は、アクセスコントロールポリシーの継承属性の属性値である。

【００６９】

ステップ５０３において、リソース作成メッセージにアクセスコントロールポリシーの継承属性の属性情報が携帯されなければ（例えば、当該リソース作成メッセージにフィールドのｉｎｈｅｒｉｔａｎｃｅが含まれていない場合）、デフォルトのポリシーの配置規則に基づいて、ターゲットリソースのアクセスコントロールポリシーを配置する。デフォルトのポリシーの配置規則は、関連技術における現在採用されているアクセスコントロールポリシーの配置規則、例えば、独立したアクセスコントロールポリシーの規則でもよい。代替的に、デフォルトのポリシーの配置規則は、当該ターゲットリソースのホスティングＣＳＥ（Ｈｏｓｔｉｎｇ　ＣＳＥ）自体が設定したほかのポリシーの配置規則であってもよい。例えば、デフォルトのポリシーの配置規則は、ターゲットリソースの親リソースのアクセスコントロールポリシーのアイデンティティー属性値をターゲットリソースにコピーして、ターゲットリソースのアクセスコントロールポリシーのアイデンティティーとすることであってもよい。

【００７０】

ステップ５０４において、リソース作成メッセージにアクセスコントロールポリシーの継承属性の属性情報が携帯されれば、アクセスコントロールポリシーの継承属性の属性値（例えば、ｉｎｈｅｒｉｔａｎｃｅの値）は１であるか否かを判断する。もしそうであれば、ステップ５０５に進み、そうではなければ、ステップ５０８に進む。

【００７１】

発起者は、新たなリソースを作成する際に、当該リソースがその親リソースのアクセスコントロールポリシーを継承することを望む場合、アクセスコントロールポリシーの継承属性の属性値を１に設定することができる。例示的に、アクティブ防御がない場合には、アクセスコントロールポリシーの継承属性の属性値は１に設定されてもよく、また、リソース作成メッセージには、ターゲットリソースに対して設定されるパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が携帯されない。アクティブ防御がある場合、アクセスコントロールポリシーの継承属性の属性値が１に設定されているほか、リソース作成メッセージのコンテンツには、ターゲットリソースに対して設定されたパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値がさらに携帯されている。

【００７２】

ステップ５０５において、アクセスコントロールポリシーの継承属性の属性値が１である場合、当該リソース作成メッセージには、パーソナライズドアクセスコントロールポリ

シーのアイデンティティー属性値が携帯されているか否かをさらに判断する。
【００７３】
ステップ５０６において、当該リソース作成メッセージにパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が携帯されていない場合、親リソースのアクセスコントロールポリシーのアイデンティティー属性値を、新たに作成されたターゲットリソースにコピーする。
【００７４】
ステップ５０７において、当該リソース作成メッセージにパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が携帯されている場合、親リソースのアクセスコントロールポリシーのアイデンティティー属性値を、新たに作成されたターゲットリソースの内にコピーするほか、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値を新たに作成されたターゲットリソースにコピーする。
【００７５】
ステップ５０８において、アクセスコントロールポリシーの継承属性の属性値が０であるか否かを判断する。もしそうであれば、ステップ５０９に進み、そうではなければ、ステップ５１２に進む。
【００７６】
発起者は、新たなリソースを作成する際に、当該リソースがその親リソースのアクセスコントロールポリシーを継承しないことを望むなら、アクセスコントロールポリシーの継承属性の属性値を０に設定することができる。アクティブ防御がない場合、アクセスコントロールポリシーの継承属性の属性値は０に設定され、また、リソース作成メッセージのコンテンツには、ターゲットリソースに対して設定されたパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が携帯されていない。アクティブ防御がある場合、アクセスコントロールポリシーの継承属性の属性値は０に設定され、また、リソース作成メッセージのコンテンツには、ターゲットリソースに対し設定されたパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が携帯されている。
【００７７】
ステップ５０９において、作成メッセージには、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が携帯されているか否かを判断する。もしそうであれば、ステップ５１０に進み、そうではなければ、ステップ５１１に進む。
【００７８】
ステップ５１０において、当該リソース作成メッセージにパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が携帯されていない場合、アプリケーション層によって作成されたアクセスコントロールポリシーのアイデンティティー属性値を新たに作成されたターゲットリソースにコピーする。
【００７９】
アクセスコントロールポリシーの継承属性の属性値が０に設定され、且つ、リソースの作成が許可された場合、Ｈｏｓｔｉｎｇ　ＣＳＥは、ターゲットリソースのために関連するアクセスコントロールポリシーを作成するようにアプリケーション層に要求する。
【００８０】
ステップ５１１において、当該リソース作成メッセージにパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が携帯されている場合、アプリケーション層によって作成されたアクセスコントロールポリシーのアイデンティティー属性値を新たに作成されたターゲットリソースにコピーするほか、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値を新たに作成されたターゲットリソースにコピーする。即ち、作成メッセージにおけるパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値もターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性値に追加される。アクセスコントロールポリシーのアイデンティティー属性値は、アクセスコントロールポリシーのアイデンティファイアリストであってもよい。

【００８１】
ステップ５１２において、アクセスコントロールポリシーの継承属性の属性値が１または０に設定されていない場合には、即ち、アクセスコントロールポリシーの継承属性の属性値が空の値に設定されている場合には、作成メッセージにはパーソナライズドアクセスコントロールポリシーのアイデンティティー属性値が携帯されているか否かを判断する。もしそうでなければ、ステップ５１３に進み、もしそうであれば、ステップ５１４に進む。
【００８２】
ある実施例において、アクセスコントロールポリシーの継承属性の属性値が空に設定されている場合には、以下のことを意味する：１、発起者は、軽量化されたモノのインターネットデバイスであるかもしれない；２、発起者は、親リソースのアクセスコントロールポリシーを継承すべきか否か分からない。この時、Ｈｏｓｔｉｎｇ　ＣＳＥは、プリセットされた設定規則に従って、作成されたリソースに対して継承関係を設定し、即ち、デフォルトの継承関係に従って、アクセスコントロールポリシーの継承属性の属性値（１，０，空）を指定し、指定された属性値に基づき、対応するアクセスコントロールポリシーを配置する。
【００８３】
ステップ５１３において、Ｈｏｓｔｉｎｇ　ＣＳＥは、親リソースのアクセスコントロールポリシーのアイデンティティー属性値またはアプリケーション層によって作成されたアクセスコントロールポリシーのアイデンティティー属性値を、新たに作成されたターゲットリソースにコピーする。
【００８４】
ステップ５１４において、Ｈｏｓｔｉｎｇ　ＣＳＥは、親リソースのアクセスコントロールポリシーのアイデンティティー属性値またはアプリケーション層によって作成されたアクセスコントロールポリシーのアイデンティティー属性値を新たに作成されたターゲットリソースにコピーするとともに、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値を新たに作成されたターゲットリソースにコピーする。
【００８５】
一実施例において、アクセスコントロールポリシーの継承属性の属性値が第１設定値であってその親リソースのアクセスコントロールポリシーを継承するいずれかの子リソースについて、そのアクセスコントロールポリシーは、親リソースのアクセスコントロールポリシーの変化に従って変化する。例えば、その親リソースのアクセスコントロールポリシーのアイデンティティー属性において、アクセスコントロールポリシーのアイデンティティー、例えばアクセスコントロールポリシーアイデンティファイアが新たに追加され、修正され、または削除された場合、これに応じて、当該子リソースのアクセスコントロールポリシーのアイデンティティー属性においても、当該アクセスコントロールポリシーのアイデンティティーが追加され、修正され、または削除される。アクセスコントロールポリシーのアイデンティティーの追加、修正、削除は、反復的な反応であってもよく、即ち、その親アクセスコントロールポリシーのアイデンティティー属性の変化は、常にサブアクセスコントロールポリシーのアイデンティティー属性の変化をもたらすことが理解できる。例示的には、３つのリソースＲ１、Ｒ２、Ｒ３が存在し、且つ、リソースＲ１とＲ２の間に第１の対の親子関係が存在し、リソースＲ２とＲ３の間に第２の対の親子関係が存在すると仮定する。リソースＲ１（第１の対の親子関係における親リソース）のアクセスコントロールポリシーのアイデンティティー属性に含まれるアクセスコントロールポリシーのアイデンティティーが変化すると、それに応じて、リソースＲ２（第１の対の親子関係における子リソース）のアクセスコントロールポリシーのアイデンティティー属性に含まれるアクセスコントロールポリシーのアイデンティティーも変化する。リソースＲ２は、第２の対の親子関係において親リソースとして機能するので、リソースＲ２のアクセスコントロールポリシーのアイデンティティー属性に含まれるアクセスコントロールポリシーのアイデンティティーの変化は、リソースＲ３（第２の対の親子関係における子リソース）のアクセスコントロールポリシーのアイデンティティー属性に含まれるアクセスコント

ロールポリシーのアイデンティティーの変化をも引き起こす。

【００８６】

図６は、親リソースと子リソースのツリー構造、及び、親リソースと子リソースに設定された属性を示す模式図である。図６に示すように、リソースツリーには、共通サービスエンティティ１がルートノードであり、アクセスコントロールポリシーのアイデンティティー属性１が設定されている。アクセスコントロールポリシーのアイデンティティー属性１の属性値は、アクセスコントロールポリシーのアイデンティファイアリスト１である。リスト１は、｛ＡＣＰ＿１、ＡＣＰ＿２、ＡＣＰ＿３｝として例示することができる。共通サービスエンティティ１は、アプリケーションエンティティ２、アプリケーションエンティティ３及びアプリケーションエンティティ５のような複数の子ノードを有してもよい。

【００８７】

アプリケーションエンティティ２には、アクセスコントロールポリシーの継承属性２とアクセスコントロールポリシーのアイデンティティー属性２とが設定されている。アクセスコントロールポリシーの継承属性２の値は、１として例示されており、アプリケーションエンティティ２がその親リソース（即ち、共通サービスエンティティ１）のアクセスコントロールポリシーを継承することを示す。アクセスコントロールポリシーのアイデンティティー属性２の属性値は、アプリケーションエンティティ２に関連するアクセスコントロールポリシーのアイデンティファイアリスト２である。リスト２は、｛ＡＣＰ＿１、ＡＣＰ＿２、ＡＣＰ＿３｝として例示されており、共通サービスエンティティ１のアクセスコントロールポリシーのアイデンティファイアリスト１と一致する。

【００８８】

アプリケーションエンティティ３には、アクセスコントロールポリシーの継承属性３とアクセスコントロールポリシーのアイデンティティー属性３が設定されている。アクセスコントロールポリシーの継承属性３の値は、１として例示されており、アプリケーションエンティティ３がその親リソース（即ち、共通サービスエンティティ１）のアクセスコントロールポリシーを継承することを示す。アクセスコントロールポリシーのアイデンティティー属性３の属性値は、アプリケーションエンティティ３に関連するアクセスコントロールポリシーのアイデンティファイアリスト３である。リスト３は、｛ＡＣＰ＿１、ＡＣＰ＿２、ＡＣＰ＿３｝として例示されてもよい。

【００８９】

アプリケーションエンティティ５には、アクセスコントロールポリシーの継承属性５とアクセスコントロールポリシーのアイデンティティー属性５が設定されている。アクセスコントロールポリシーの継承属性５の値は、０として例示されており、アプリケーションエンティティ５が親リソース（即ち、共通サービスエンティティ１）のアクセスコントロールポリシーを継承しないことを示す。アクセスコントロールポリシーのアイデンティティー属性５の属性値は、アプリケーションエンティティ５に関連するアクセスコントロールポリシーのアイデンティファイアリスト５である。リスト５は、｛ＡＣＰ＿１、ＡＣＰ＿５｝として例示されており、共通サービスエンティティ１のアクセスコントロールポリシーのアイデンティファイアリスト１とは異なる。

【００９０】

アプリケーションエンティティ３は、一つの子ノードであるアプリケーションエンティティ４を有する。アプリケーションエンティティ４には、アクセスコントロールポリシーの継承属性４とアクセスコントロールポリシーのアイデンティティー属性４が設定されている。アクセスコントロールポリシーの継承属性４の値は、１として例示され、アプリケーションエンティティ４がその親リソース（即ち、アプリケーションエンティティ３）のアクセスコントロールポリシーを継承することを示す。アクセスコントロールポリシーのアイデンティティー属性４の属性値は、アプリケーションエンティティ４に関連するアクセスコントロールポリシーのアイデンティファイアリスト４である。リスト４は、｛ＡＣＰ＿１、ＡＣＰ＿２、ＡＣＰ＿３、ＡＣＰ＿６｝として例示されている。そのうち、ＡＣＰ＿１、ＡＣＰ＿２、ＡＣＰ＿３は、アプリケーションエンティティ３のアクセスコント

ロールポリシーのアイデンティファイアリスト３と一致し、さらに、共通サービスエンティティ１のアクセスコントロールポリシーのアイデンティファイアリスト１と一致し、ＡＣＰ＿６は、アプリケーションエンティティ４自体のパーソナライズドアクセスコントロールポリシーアイデンティファイアとすることができる。

【００９１】

以下、図６を合わせて、本開示の実施例の例示的な応用シーンを例示する。当該応用シーンにおいて、疑似攻撃者Ａがクローラー方式によってモノのネットワークデータ（例えばアプリケーションエンティティ２－５のデータ）を取得していると仮定し、データセキュリティを保護するために、すべてのアプリケーションエンティティのリソースを一時的に保護する必要がある。この時、ユーザＡに対するアクセスコントロールポリシーＢを作成することができる。アクセスコントロールポリシーＢのコンテンツは、以下の通りであり：ユーザＡによって行われたリソース取得要求は、すべてブロックされる。このため、共通サービスエンティティ１のアクセスコントロールポリシーのアイデンティティー属性１に、アクセスコントロールポリシーＢに関するアイデンティファイアＡＣＰ＿４を追加することができる。これにより、リスト１は｛ＡＣＰ＿１、ＡＣＰ＿２、ＡＣＰ＿３、ＡＣＰ＿４｝として修正される。

【００９２】

アプリケーションエンティティ２、アプリケーションエンティティ３及びそのディセンダントであるアプリケーションエンティティ４のアクセスコントロールポリシーの継承属性の属性値はいずれも１であり、親リソースのアクセスコントロールポリシーを継承することを示すので、これらのアプリケーションエンティティのアクセスコントロールポリシーのアイデンティティー属性は、共通サービスエンティティ１の更新に従って相応して更新され、即ち、そのアクセスコントロールポリシーのアイデンティティー属性の属性値に、ユーザＡに関するアクセスコントロールポリシーＢのアイデンティファイアＡＣＰ＿４を追加する。これにより、リスト２とリスト３も、｛ＡＣＰ＿１、ＡＣＰ＿２、ＡＣＰ＿３、ＡＣＰ＿４｝に自動的に更新され、リスト４は、｛ＡＣＰ＿１、ＡＣＰ＿２、ＡＣＰ＿３、ＡＣＰ＿４、ＡＣＰ＿６｝に自動的に更新される。

【００９３】

アプリケーションエンティティ５のアクセスコントロールポリシーの継承属性値は０であり、親リソースのアクセスコントロールポリシーを継承しないことを示すので、アクセスコントロールポリシーのアイデンティティー属性５は更新されず、リスト５が変更されなく、依然として｛ＡＣＰ＿１、ＡＣＰ＿５｝である。ある実施例において、アプリケーションエンティティ５のデータを保護するために、ＡＣＰ＿４をリスト５に手動で追加することができる。

【００９４】

ある実施例において、共通サービスエンティティ１がそのアクセスコントロールポリシーのアイデンティティー属性１の属性値からアクセスコントロールポリシーアイデンティファイアＡＣＰ＿３を削除すれば、リスト１は｛ＡＣＰ＿１、ＡＣＰ＿２｝に修正される。この時、アクセスコントロールポリシーの継承属性を持つ属性値が１であるアプリケーションエンティティ２、アプリケーションエンティティ３及びそのディセンダントであるアプリケーションエンティティ４のアクセスコントロールポリシーのアイデンティティー属性は、それに応じて更新され、即ち、アクセスコントロールポリシーアイデンティファイアＡＣＰ＿３がその属性値から削除される。これにより、リスト２、リスト３、リスト４は、｛ＡＣＰ＿１、ＡＣＰ＿２｝、｛ＡＣＰ＿１、ＡＣＰ＿２｝及び｛ＡＣＰ＿１、ＡＣＰ＿２、ＡＣＰ＿６｝に自動的に修正される。

【００９５】

アプリケーションエンティティ５のアクセスコントロールポリシーの継承属性の属性値が０であり、その親リソースのアクセスコントロールポリシーを継承しないことを示すので、アクセスコントロールポリシーのアイデンティティー属性５は更新されず、リスト５は変更されなく、依然として｛ＡＣＰ＿１、ＡＣＰ＿５｝である。

【００９６】
本開示の実施例によれば、リソースがどのように多様化されたとしても、継承属性を有している限り、アクセスコントロールポリシーの修正は非常に効率的である。特に、緊急時にはリソース全体のアクセスコントロールポリシーを修正する必要がある場合、リソースツリーのルートノードのアクセスコントロールポリシーを簡単に配置し、継承属性を持たないリソースのアクセスコントロールポリシーを修正すればよい。これは、ユーザの修正作業量を大幅に削減し、作業効率と緊急反応速度を提供している。
【００９７】
図７は、本開示のアクセスコントロールポリシーの配置装置の一実施例の構造ブロック図を示す。図７に示すように、アクセスコントロールポリシー配置装置７０が見られる。当該アクセスコントロールポリシー配置装置７０は、受信モジュール７１と、属性確定モジュール７２と、ポリシー配置モジュール７３とを含む。アクセスコントロールポリシー配置装置７０は、共通サービスエンティティとして実現されてもよい。
【００９８】
受信モジュール７１は、ターゲットリソースを作成する要求を受信するように配置されている。受信モジュール７１は、アプリケーションエンティティから当該要求を受信することができる。前記受信は、有線または無線の方式にて行うことができる。当該要求は、リソース作成メッセージの形式であってもよい。リソース作成メッセージは、アクセスコントロールポリシーの継承属性の属性値を携帯することができる。付加的に、リソース作成メッセージは、アクセスコントロールポリシーのアイデンティティー属性を設定するための属性値を携帯してもよい。
【００９９】
属性確定モジュール７２は、前記要求に基づいて、ターゲットリソースに対してアクセスコントロールポリシーの継承属性が設定されているか否かを確定するように配置されている。属性確定モジュール７２は、前記要求を分析して、アクセスコントロールポリシーの継承属性に関する属性情報を含むか否かを確定することができる。一実施例において、属性確定モジュール７２は、前記要求にフィールドのｉｎｈｅｒｉｔａｎｃｅが含まれた場合には、ターゲットリソースに対してアクセスコントロールポリシーの継承属性が設定されていると確定することができる。ある実施例において、属性確定モジュール７２は、前記要求に含まれる、アクセスコントロールポリシーの継承属性に関する属性情報を、ポリシー配置モジュール７３に送信することができる。例示的には、属性情報は、アクセスコントロールポリシーの継承属性を設定するための属性値、即ち、アクセスコントロールポリシーの継承属性値を、フィールドのｉｎｈｅｒｉｔａｎｃｅに含めることができる。
【０１００】
ポリシー配置モジュール７３は、確定結果に基づいて、ターゲットリソースのアクセスコントロールポリシーを配置するように配置されている。ポリシー配置モジュール７３は、属性確定モジュール７２からのアクセスコントロールポリシーの継承属性値に基づいて、アクセスコントロールポリシーを配置することができる。
【０１０１】
ある実施例において、ポリシー配置モジュール７３は、継承判断手段７３１とポリシー設定手段７３２とを含むことができる。継承判断手段７３１は、アクセスコントロールポリシーの継承属性に関する属性値に基づいて、ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承するか否かを判断するように配置されている。ポリシー設定手段７３２は、継承判断手段７３１の判断結果に基づいて、ターゲットリソースのアクセスコントロールポリシー属性を設定するように配置されている。
【０１０２】
一実施例において、アクセスコントロールポリシーの継承属性の属性値が第１設定値である場合、継承判断手段７３１は、ターゲットリソースがその親リソースアクセスコントロールポリシーを継承すると確定する。アクセスコントロールポリシーの継承属性の属性値が第２設定値である場合、継承判断手段７３１は、ターゲットリソースが親リソースの

アクセスコントロールポリシーを継承しないと確定する。アクセスコントロールポリシーの継承属性の属性値が第３設定値である場合、継承判断手段７３１は、プリセットされた設定規則に基づいて、前記ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承するか否かを確定する。プリセットされた設定規則は、前記ターゲットリソースとその親リソースのアクセスコントロールポリシーの間のデフォルト継承関係を示し、前記デフォルト継承関係は、継承すること、または、継承しないことを含む。

【０１０３】

継承判断手段７３１は、ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承すると確定する場合、ポリシー設定手段７３２は、親リソースのアクセスコントロールポリシーのアイデンティティー属性に基づき、ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を設定する。継承判断手段７３１が、ターゲットリソースが親リソースのアクセスコントロールポリシーを継承しないと確定した場合、ポリシー設定手段７３２は、ターゲットリソースに対してアクセスコントロールポリシーのアイデンティティー属性を作成するようにアプリケーション層に要求する。

【０１０４】

ある実施例において、属性確定モジュール７２は、当該要求を分析して、ターゲットリソースに対してパーソナライズドアクセスコントロールポリシーのアイデンティティー属性が設定されているか否かを確定するように配置されている。属性確定モジュール７２が、ターゲットリソースに対してパーソナライズドアクセスコントロールポリシーのアイデンティティー属性が設定されていると確定した場合には、ポリシー設定手段７３２は、ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性に、パーソナライズドアクセスコントロールポリシーのアイデンティティー属性値を追加する。

【０１０５】

ある実施例において、ポリシー配置モジュール７３は、ポリシー更新手段７３３をさらに含むことができる。ポリシー更新手段７３３は、継承判断手段７３１が、ターゲットリソースがその親リソースのアクセスコントロールポリシーを継承し、且つ、ターゲットリソースの親リソースのアクセスコントロールポリシーが変化すると確定した場合、例えば、その親リソースのアクセスコントロールポリシーのアイデンティティー属性に、アクセスコントロールポリシーのアイデンティティー情報を、新らに追加し、修正し、削除する場合、ポリシー更新手段７３３が、変化した前記親リソースのアクセスコントロールポリシーのアイデンティティー属性に応じて、前記ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性を更新するように配置され、即ち、当該ターゲットリソースのアクセスコントロールポリシーのアイデンティティー属性に、アクセスコントロールポリシーのアイデンティティー情報を、新たに追加し、修正し、削除する。

【０１０６】

図８は、本開示の装置の別の実施例の構造ブロック図を示す。図８に示すように、装置８０は、確定モジュール８１と、送信モジュール８２と、受信モジュール８３とを含む。アクセスコントロールポリシー配置装置８０は、アプリケーションエンティティとして実現されてもよい。

【０１０７】

確定モジュール８１は、ターゲットリソースとその親リソースのアクセスコントロールポリシーの間の継承関係を確定するように配置されている。送信モジュール８２は、前記ターゲットリソースを作成する要求を送信するように配置されている。前記要求には、前記ターゲットリソースのアクセスコントロールポリシーの配置に用いられる、前記継承関係を示すアクセスコントロールポリシー継承属性が設けられている。受信モジュール８３は、前記要求に対するリソース作成応答を受信するように配置されている。

【０１０８】

一実施例において、本開示は、アクセスコントロールポリシー配置システムを提供する。アクセスコントロールポリシー配置システムは、第１エンティティと第２エンティティとを含む。第１エンティティは、ターゲットリソースを作成する要求を送信するためのも

のである。ある実施例において、第１エンティティは、図８を参照して述べたような装置８０を含むことができる。第２エンティティは、図７を参照して述べたようなアクセスコントロールポリシー配置装置７０を含む。第１エンティティは、アプリケーションエンティティＡＥなどであってもよく、第２エンティティは、共通サービスエンティティＣＳＥなどであってもよい。

【０１０９】

図９は、本開示の装置の別の実施例の構造ブロック図である。図９に示すように、コンピューティングデバイスによって実現されるアクセスコントロールポリシー配置装置が提供される。コンピューティングデバイスは、例えば、サービスプロバイダのサーバ、クライアントに関連するデバイス（例えば、クライアントデバイス）、システムオンチップ及び／またはいずれのほかの適当なコンピューティングデバイスまたはコンピューティングシステムであってもよい。

【０１１０】

当該装置は、メモリ９０１とプロセッサ９０２とを含むことができる。メモリ９０１は、指令を記憶するためのものであり、プロセッサ９０２は、メモリ９０１に結合される。プロセッサ９０２は、上記のいずれかの実施例のアクセスコントロールポリシー配置方法を実現するように、当該指令を実行する。

【０１１１】

当該装置は、ほかのデバイスと情報交換を行うための通信インタフェース９０３をさらに含む。同時に、当該装置は、バス９０４をさらに含む。プロセッサ９０２、通信インタフェース９０３及びメモリ９０１は、バス９０４を介して相互間の通信を完了することができる。

【０１１２】

メモリ９０１は、１つ以上のコンピュータ読取可能な媒体に関連するメモリ／記憶装置容量を表する。メモリ９０１は、リードオンリーメモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、ダイナミックＲＡＭ（ＤＲＡＭ）、デュアルデータレートＤＲＡＭ（ＤＤＲＡＭ）、シンクロナイズＤＲＡＭ（ＳＤＲＡＭ）、スタティックＲＡＭ（ＳＲＡＭ）、プログラマブルＲＯＭ（ＰＲＯＭ）、消去可能プログラマブルＲＯＭ（ＥＰＲＯＭ）、電気的消去可能プログラマブルＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリ、ポリマーメモリ（例えば、強誘電体プラズマメモリ、双方向（ｏｖｏｎｉｃ）メモリ、位相変化または強誘電体メモリ、シリコン－酸素－窒素－酸素－シリコン（ＳＯＮＯＳ）メモリ）、磁気カードまたは光カード、情報の記憶に適したほかのタイプの媒体など、各タイプのメモリを含むことができる。

【０１１３】

プロセッサ９０２は、中央処理装置ＣＰＵであってもよい。プロセッサ９０２は、ハードウェアで実現された特定用途向け集積回路または、１つ以上の半導体により形成されるほかの論理デバイス、を含むこともできる。このようなハードウェア手段は、その構成材料や、その中で採用される処理メカニズムによって制限されない。例えば、プロセッサ９０２は、（１つ以上の）半導体及び／またはトランジスタ（例えば、電子集積回路（ＩＣ））を含むことができる。

【０１１４】

一実施例において、本開示は、コンピュータ読取可能な記憶媒体を提供する。コンピュータ読取可能な記憶媒体の例は、揮発性メモリまたは不揮発性メモリ、取り外し可能なメモリまたは取り外し不可能なメモリ、消去可能メモリまたは消去不可能なメモリ、書き込み可能なメモリまたは書き換え可能メモリなど、電子データを記憶可能な１つ以上のタイプの記憶媒体を含むことができる。コンピュータ読取可能な記憶媒体には、プロセッサによって実行されると、プロセッサが上記のいずれかの実施例におけるアクセスコントロールポリシーの配置方法を実現するようにさせるコンピュータ指令が記憶されている。

【０１１５】

上記の実施例によって提供されるアクセスコントロールポリシーの配置方法、装置、シ

ステム及び記憶媒体は、アクセスコントロールポリシーの継承属性に基づいて、親リソースのアクセスポリシー権限を継承するか否かを確定し、子リソースのアクセスコントロールポリシーを効率的に設定し、変更することができる。これは、ユーザが継承関係を指示することでアクセスコントロールポリシーを配置し修正することができるため、アクセスコントロールポリシーの配置と修正の効率を向上させ、従来のアクセスコントロールポリシーの関連基準を改善する。

【０１１６】

一般的に、本明細書において記載された何れかの機能は、ソフトウェア、ファームウェア、ハードウェア（例えば、固定論理回路システム）、人工的な処理、またはこれらの実現形態の組み合わせにより実現されてもよい。本明細書で使用される用語の「モジュール」、「機能」及び「論理」は、一般に、ソフトウェア、ファームウェア、ハードウェア、または、それらの組み合わせを示す。ソフトウェアによる実現形態の場合、モジュール、機能または論理は、プロセッサ（例えば、１つ以上のＣＰＵ）において、または、プロセッサによって実行される場合に、タスクを指定するプログラムコードを実行することを示す。当該プログラムコードは、１つ以上のコンピュータ読取可能な記憶デバイスに記憶されてもよい。上述したアクセスコントロールポリシーの配置の特徴は、プラットフォームに依存しないものであり、これは、これらの技術が、様々なプロセッサを有する様々な商業コンピューティングプラットフォーム上で実現できることを意味する。

【０１１７】

本開示は、様々な例示的な実施例に合わせて説明されているが、当業者は、添付された特許請求の範囲内で多くの修正が可能であることを理解することができる。従って、本開示の範囲は、いかなる方式で上記の説明に限定されることが意図されているのではなく、添付される特許請求の範囲を完全に参照して決定すべきである。

【符号の説明】

【０１１８】

71 受信モジュール
72 属性確定モジュール
73 ポリシー配置モジュール
81 確定モジュール
82 送信モジュール
83 受信モジュール
731 継承判断手段
732 ポリシー設定手段
733 ポリシー更新手段
901 メモリ
902 プロセッサ
903 通信インタフェース
904 バス

【図面】

【図１】

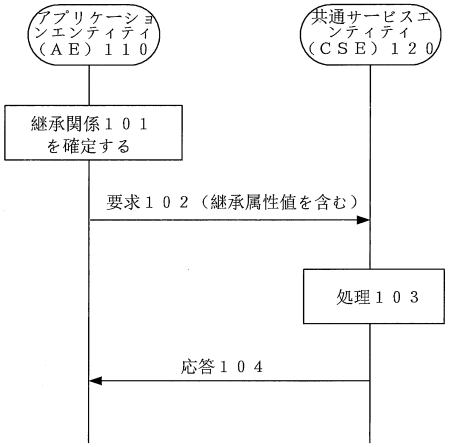

図１

【図２】

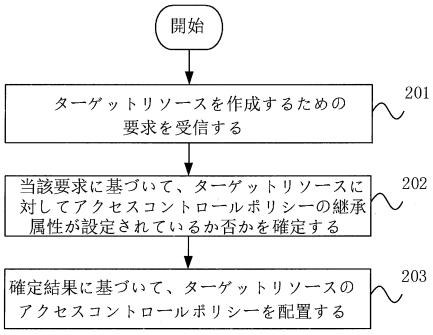

図２

【図３】

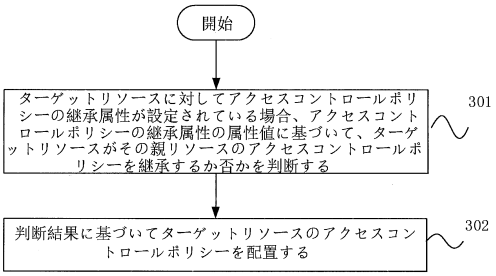

図３

【図４】

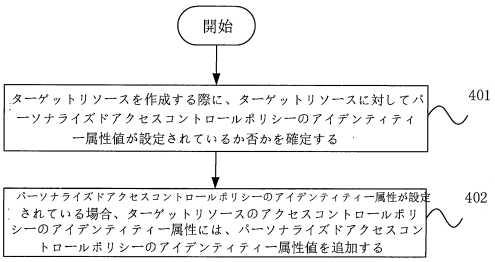

図４

【図５】

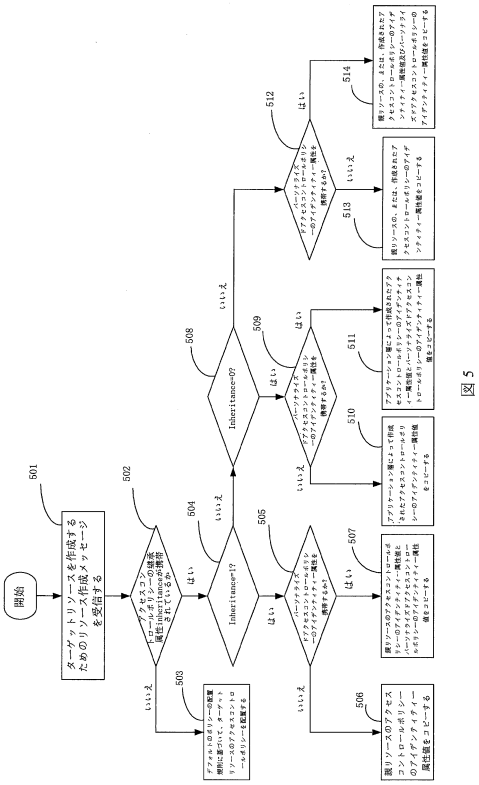

図５

【図６】

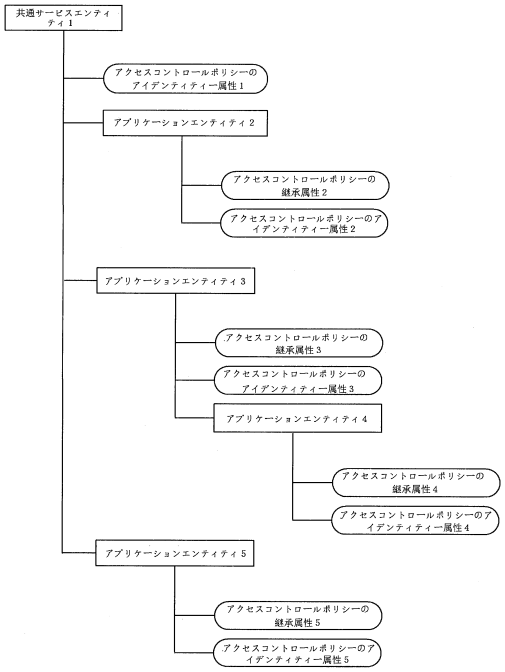

図６

【図７】

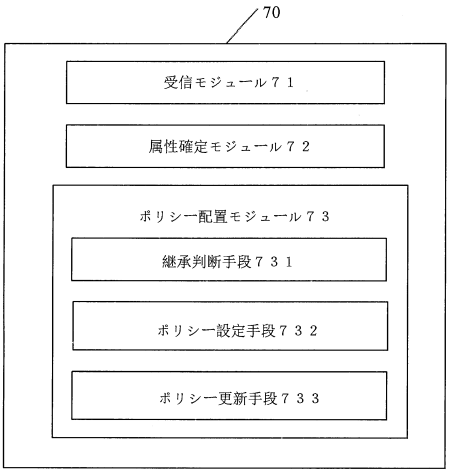

図７

【図８】

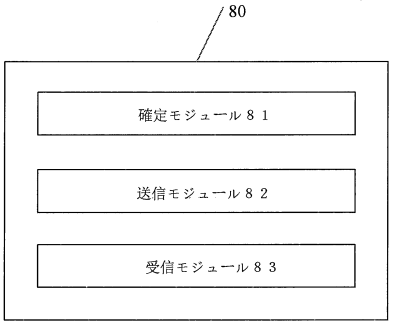

図８

【図９】

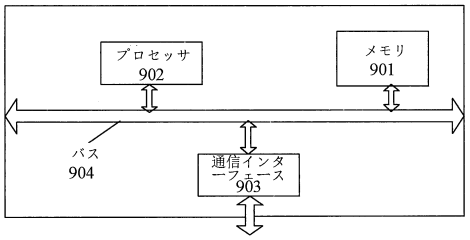

図9

フロントページの続き

中華人民共和国１００１７６北京市▲経▼▲済▼技▲術▼▲開▼▲発▼区地▲澤▼路９号
(72)発明者　▲趙▼ 君杰
中華人民共和国１００１７６北京市▲経▼▲済▼技▲術▼▲開▼▲発▼区地▲澤▼路９号
(72)発明者　▲蘇▼ 京
中華人民共和国１００１７６北京市▲経▼▲済▼技▲術▼▲開▼▲発▼区地▲澤▼路９号

審査官　宮司 卓佳

(56)参考文献
米国特許出願公開第２０１８／０２２５３５４（ＵＳ，Ａ１）
米国特許出願公開第２０１８／０１６７３９７（ＵＳ，Ａ１）
特表２０１８－５１２６７４（ＪＰ，Ａ）
中国特許出願公開第１０５６３５９３１（ＣＮ，Ａ）
特表２０１６－５２６３２２（ＪＰ，Ａ）
oneM2M Functional Architecture Baseline Draft，2014年08月01日，oneM2M-TS-0001-V-2014-08，p.89，https://www.onem2m.org/images/files/deliverables/TS-0001-oneM2M-Functional-Architecture-V-2014-08.pdf

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２