【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成30年3月8日(2018.3.8)

【公表番号】特表2017-526048(P2017-526048A)
【公表日】平成29年9月7日(2017.9.7)
【年通号数】公開・登録公報2017-034
【出願番号】特願2016-575001(P2016-575001)
【国際特許分類】
Ｇ０６Ｆ　21/62　　(2013.01)
Ｇ０６Ｆ　21/53　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/62　　３１８
Ｇ０６Ｆ　21/53

【手続補正書】
【提出日】平成30年1月26日(2018.1.26)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
複数のパーティションと、複数のパーティションリソースと、複数のグローバルリソースとを含むマルチテナントアプリケーションサーバ環境におけるセキュリティを提供するための方法であって、前記方法は、
管理セキュリティレルムと第１のセキュリティレルムと第２のセキュリティレルムとを含む複数のセキュリティレルムを規定するステップと、
前記複数のパーティションのうちの第１のパーティションを、前記複数のパーティションリソースのうちの第１の複数のパーティションリソースを有するように構成するステップと、
前記複数のパーティションのうちの第２のパーティションを、前記複数のパーティションリソースのうちの第２の複数のパーティションリソースを有するように構成するステップと、
前記第１のパーティションを前記第１のセキュリティレルムに関連付ける第１のセキュリティ構成を与えるステップと、
前記第２のパーティションを前記第２のセキュリティレルムに関連付ける第２のセキュリティ構成を与えるステップと、
第１のプライマリアイデンティティドメインを前記第１のパーティションに関連付けるステップとを含み、前記第１のプライマリアイデンティティドメインは、第１のテナントに関連付けられた第１の複数のユーザを表わし、
第２のプライマリアイデンティティドメインを前記第２のパーティションに関連付けるステップを含み、前記第２のプライマリアイデンティティドメインは、第２のテナントに関連付けられた第２の複数のユーザを表わし、
前記管理セキュリティレルム、前記第１のセキュリティレルム、および前記第２のセキュリティレルム各々を実行時に同時に動作させることにより、前記複数のパーティションリソースおよび前記複数のグローバルリソースへのアクセスの認証および認可を制御するステップを含み、
前記第１のテナントに関連付けられた前記第１の複数のユーザは、前記第１のパーティ

ションの前記第１の複数のパーティションリソースにアクセスできるが、前記第２のパーティションの前記第２の複数のパーティションリソースにはアクセスできず、
前記第２のテナントに関連付けられた前記第２の複数のユーザは、前記第２のパーティションの前記第２の複数のパーティションリソースにアクセスできるが、前記第１のパーティションの前記第１の複数のパーティションリソースにはアクセスできない、方法。
【請求項２】
前記第１のプライマリアイデンティティドメインを、前記第１のテナントに関連付けられた前記第１の複数のユーザの第１の表現を格納するための第１のアイデンティティ記憶域を参照するように構成するステップと、
前記第２のプライマリアイデンティティドメインを、前記第２のテナントに関連付けられた前記第２の複数のユーザの第２の表現を格納するための、前記第１のアイデンティティ記憶域と異なる第２のアイデンティティ記憶域を参照するように構成するステップとをさらに含む、請求項１に記載の方法。
【請求項３】
前記第１のプライマリアイデンティティドメインを、前記第１のテナントに関連付けられた前記第１の複数のユーザの第１の表現を格納するためのアイデンティティ記憶域の第１の部分を参照するように構成するステップと、
前記第２のプライマリアイデンティティドメインを、前記第２のテナントに関連付けられた前記第２の複数のユーザの第２の表現を格納するための前記アイデンティティ記憶域の第２の部分を参照するように構成するステップとをさらに含む、請求項１に記載の方法。
【請求項４】
管理アイデンティティドメインを前記マルチテナントアプリケーションサーバ環境に関連付けるステップをさらに含み、前記管理アイデンティティドメインは、前記マルチテナントアプリケーションサーバ環境の複数のシステムアドミニストレータを表わし、
前記マルチテナントアプリケーションサーバ環境に関連付けられた前記複数のシステムアドミニストレータは、前記複数のグローバルリソースにアクセス可能である、請求項１～３のいずれかに記載の方法。
【請求項５】
第１の認証サービスを提供するステップをさらに含み、前記第１の認証サービスは、前記第１のテナントに関連付けられた前記第１の複数のユーザを認証するように構成されるとともに、前記第１の複数のユーザのうちの１人以上のユーザと組合わせて前記第１のプライマリアイデンティティドメインを識別する第１の署名付きプリンシパルを生成するように構成される、請求項１～４のいずれかに記載の方法。
【請求項６】
前記第１の複数のパーティションリソース各々を前記第１のプライマリアイデンティティドメインに関連付けるステップと、
前記第２の複数のパーティションリソースを各々前記第２のプライマリアイデンティティドメインに関連付けるステップと、
認可サービスを提供するステップとをさらに含み、前記認可サービスは、リソースへのアクセスのためのコールをユーザから受けたことに応じて、前記ユーザに関連付けられたプライマリアイデンティティドメインと前記リソースに関連付けられたプライマリアイデンティティドメインとを比較し、前記ユーザに関連付けられた前記プライマリアイデンティティドメインと前記リソースに関連付けられた前記プライマリアイデンティティドメインとが一致する場合に限り、前記リソースへのアクセスを認可する、請求項１～５のいずれかに記載の方法。
【請求項７】
前記方法はさらに、
第１の認証サービスを提供するステップを含み、前記第１の認証サービスは、前記第１のテナントに関連付けられた前記第１の複数のユーザを認証するように構成されるととも

に、前記第１の複数のユーザのうちの１人以上のユーザと組合わせて前記第１のプライマリアイデンティティドメインを識別する第１の署名付きプリンシパルを生成するように構成され、
第２の認証サービスを提供するステップを含み、前記第２の認証サービスは、前記第２のテナントに関連付けられた前記第２の複数のユーザを認証するように構成されるとともに、前記第２の複数のユーザのうちの１人以上のユーザと組合わせて前記第２のプライマリアイデンティティドメインを識別する第２の署名付きプリンシパルを生成するように構成され、
前記第１の複数のパーティションリソース各々を前記第１のプライマリアイデンティティドメインに関連付けるステップと、
前記第２の複数のパーティションリソース各々を前記第２のプライマリアイデンティティドメインに関連付けるステップと、
認可サービスを提供するステップとを含み、前記認可サービスは、プリンシパルに関連付けられた、リソースへのアクセスのためのコールを受けたことに応じて、前記プリンシパルにおいて識別されたプライマリアイデンティティドメインを、前記リソースに関連付けられたプライマリアイデンティティドメインと比較し、前記プリンシパルに関連付けられたプライマリアイデンティティドメインが前記リソースに関連付けられた前記プライマリアイデンティティドメインと一致する場合に限り、前記リソースへのアクセスを認可するように構成される、請求項１～４のいずれかに記載の方法。
【請求項８】
コンピュータシステムによって実行されると前記コンピュータシステムに請求項１～７のいずれかに記載の方法を実行させる機械読取可能なフォーマットのプログラム命令を含むコンピュータプログラム。
【請求項９】
マルチテナントアプリケーションサーバ環境システムであって、
複数のマイクロプロセッサとメモリとを含むアプリケーションサーバ環境と、
前記アプリケーションサーバ環境に構成された複数のパーティションと、
前記アプリケーションサーバ環境に設けられた複数のパーティションリソースと複数のグローバルリソースと、
前記アプリケーションサーバ環境に構成された管理セキュリティレルムと第１のセキュリティレルムと第２のセキュリティレルムとを含む複数のセキュリティレルムと、
前記複数のパーティションリソースのうちの第１の複数のパーティションリソースを有するように構成された前記複数のパーティションのうちの第１のパーティションと、
前記複数のパーティションリソースのうちの第２の複数のパーティションリソースを有するように構成された前記複数のパーティションのうちの第２のパーティションと、
前記第１のパーティションを前記第１のパーティションレルムに関連付ける第１のセキュリティ構成と、
前記第２のパーティションを前記第２のパーティションレルムに関連付ける第２のセキュリティ構成と、
前記第１のパーティションに関連付けられた第１のプライマリアイデンティティドメインとを備え、前記第１のプライマリアイデンティティドメインは、第１のテナントに関連付けられた第１の複数のユーザを表わし、前記マルチテナントアプリケーションサーバ環境システムはさらに、
前記第２のパーティションに関連付けられた第２のプライマリアイデンティティドメインを備え、前記第２のプライマリアイデンティティドメインは、第２のテナントに関連付けられた第２の複数のユーザを表わし、
前記管理セキュリティレルム、前記第１のセキュリティレルム、および前記第２のセキュリティレルムは、実行時に同時に動作することにより、前記複数のパーティションリソースおよび前記複数のグローバルリソースへのアクセスの認証および認可を制御するように構成され、

前記第１のテナントに関連付けられた前記第１の複数のユーザは、前記第１のパーティションの前記第１の複数のパーティションリソースにアクセスできるが、前記第２のパーティションの前記第２の複数のパーティションリソースにはアクセスできず、

前記第２のテナントに関連付けられた前記第２の複数のユーザは、前記第２のパーティションの前記第２の複数のパーティションリソースにアクセスできるが、前記第１のパーティションの前記第１の複数のパーティションリソースにはアクセスできない、マルチテナントアプリケーションサーバ環境システム。