【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24年6月28日(2012.6.28)

【公表番号】特表2011-526387(P2011-526387A)
【公表日】平成23年10月6日(2011.10.6)
【年通号数】公開・登録公報2011-040
【出願番号】特願2011-516585(P2011-516585)
【国際特許分類】
Ｇ０６Ｆ　21/24　　(2006.01)
Ｇ０６Ｆ　21/20　　(2006.01)
Ｇ０６Ｆ　21/22　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　　５２０Ｃ
Ｇ０６Ｆ　15/00　　３３０Ａ
Ｇ０６Ｆ　 9/06　　６６０Ｚ

【手続補正書】
【提出日】平成24年5月10日(2012.5.10)
【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】
実行可能命令を含むコンピューター記憶媒体であって、該実行可能命令は、プロセッサーによって実行されると、
前記プロセッサー上で動作するオペレーティングシステムを用意するステップであって、前記プロセッサーは前記オペレーティングシステムを介してアプリケーションを実行する、ステップと、
前記プロセッサーが、前記アプリケーションによりアクセスされるリソース及び前記アプリケーションがなすことができるコールを制御するために前記オペレーティングシステムを介してセキュリティ構造を実施するステップであって、前記プロセッサーは、
前記プロセッサーがランタイムオブジェクトを作成する場合、前記プロセッサーが、関連付けられるサブジェクトのための一意の識別子を定義し、該関連付けられるサブジェクトに関連付けられるアカウントを指定するためのセキュリティ識別子（１００）を設けるステップ、
前記一意の識別子をメモリーに保持されるアカウントデータベース内のエントリにマッピングするステップであって、前記セキュリティ識別子（１００）に割り当てられた基本特権（２１４）及び拡張特権（２１６）を求める、マッピングするステップ、
前記プロセッサーが、前記関連付けられるサブジェクトのマイグレーションに沿って関連付けられるサブジェクトの識別子（２１０、２１２）を蓄積するステップ、
前記プロセッサーが、前記セキュリティ識別子（１００）に割り当てられた前記基本特権（２１４）及び前記拡張特権（２１６）を求めることに基づいて、識別情報（２１０、２１２）のセット及び該識別情報のセットに割り当てられた特権の集合を定義するためのセキュリティトークン（２００）を作成するステップ、並びに
前記プロセッサーが、前記関連付けられるサブジェクトの前記蓄積された識別子（２１０、２１２）のすべて及び前記特権（２１４、２１６）の集合をインターセクトすることによって前記関連付けられるサブジェクトのアクセス特権を求めるステップ

によって、前記セキュリティ構造を実施する、ステップと
によって、関連付けられるサブジェクトによるリソースへのアクセスを制御するためのセキュリティインフラストラクチャーを提供する、実行可能命令を含むコンピューター記憶媒体。
【請求項２】
前記関連付けられるサブジェクトは、プロセス又はプロセスのスレッドを含む、請求項１に記載のコンピューター記憶媒体。
【請求項３】
前記関連付けられるサブジェクトのアクセス特権（２１４、２１６）を求める前記ステップは、前記リソースへのアクセスを付与する前に、前記現在の関連付けられるサブジェクトのコールチェーンコンテキストをキャプチャするステップと、前記現在の関連付けられるサブジェクトを分析して、前記コールチェーンにおける蓄積された各前記識別情報（２１０、２１２）及び各前記関連付けられるサブジェクトが、前記要求されたリソースにアクセスすることができることを検証するステップとをさらに含み、それによって、デフォルトにより最小特権を可能にする、請求項１に記載のコンピューター記憶媒体。
【請求項４】
前記セキュリティトークン（２００）とセキュリティ記述子（３００）との間の関係が、要求されたリソースへの関連付けられるサブジェクトによるアクセス権の制御を決定する、請求項１に記載のコンピューター記憶媒体。
【請求項５】
アクセス特権（２１４、２１６）を求める前記ステップは、セキュリティトークン（２００）における各前記セキュリティ識別子（１００）を使用して、セキュリティトークンが、セキュリティ記述子（３００）によって指定されたリソースへのアクセスを要求したか否かを判断し、前記コンタクトチェーン内のあらゆるコーラーが、要求されたリソースへのアクセスを付与する特権を有するときにのみ、前記要求されたリソースへのアクセスが付与される、請求項１に記載のコンピューター記憶媒体。
【請求項６】
前記リソースへのアクセス権を定義するセキュリティ記述子（３００）を構築するステップと、
前記セキュリティトークン（２００）に従って前記関連付けられるサブジェクトを識別するステップと、
前記セキュリティ記述子（３００）において定義された前記識別情報（３２０、３３０）が前記セキュリティ記述子におけるアクセス制御エントリ（５００）に含まれるか否かを判断するステップと、
前記アクセス制御エントリに基づいて前記識別情報にとって利用可能なアクセス権を求めるステップと、
前記求めたアクセス権に従って前記識別情報（３２０、３３０）にアクセス権を付与するステップと
をさらに含む、請求項１に記載のコンピューター記憶媒体。
【請求項７】
関連付けられるサブジェクトに関係するすべてのトークンのリスト（２００）をセキュリティトークンリスト（７００）内に保持するステップをさらに含み、現在のアクティブトークン（７１０）は、常に前記セキュリティトークンリストの先頭にあり、現在の関連付けられるサブジェクトに対するすべてのアクセスチェック及び特権チェックは、関連付けられるサブジェクトがアクセスを要求するリソースを前記セキュリティトークンリスト（７００）の先頭の前記現在のアクティブセキュリティトークンと比較することにより、前記現在のアクティブセキュリティトークン（７１０）及び前記関連付けられるサブジェクトの現在のコンテキストを使用してハンドリングされる、請求項１に記載のコンピューター記憶媒体。
【請求項８】

クライアント側（１０２０）において、関連付けられるサブジェクトのセキュリティコンテキストをメッセージキューに書き込むステップと、前記サーバー側（１０３０）において、前記メッセージキューから前記関連付けられるサブジェクトの前記セキュリティコンテキストを非同期にリトリーブするステップと、及び偽装される前記関連付けられるサブジェクトの前記リトリーブしたセキュリティコンテキストをコピーすることによって前記関連付けられるサブジェクトを偽装するステップとをさらに含む、請求項１に記載のコンピューター記憶媒体。

【請求項９】

関連付けられるサブジェクトの現在のセキュリティトークン（７１０）に関連付けられるすべての識別情報（２１０、２１２）が要求リソースにアクセスすることができるときに、前記要求されたリソースへのアクセスを付与するステップをさらに含み、現在の関連付けられるサブジェクトのコールスタック（８００）におけるすべてのチャンバーに関連付けられるすべての識別情報は、前記要求リソースにアクセスすることができ、前記関連付けられるサブジェクトのための保存されたコンテキストに関連付けられるすべての識別情報は、前記要求されたリソースにアクセスすることができる、請求項１に記載のコンピューター記憶媒体。

【請求項１０】

オフライン処理用に、オフラインデータベース内にセキュリティコンタクトを記憶するステップをさらに含む、請求項１に記載のコンピューター記憶媒体。

【請求項１１】

プロセッサーによってオペレーティングシステムを介して実施されるセキュリティインフラストラクチャーであって、

関連付けられるサブジェクトのための一意の識別子を定義し、該関連付けられるサブジェクトに関連付けられるアカウントを指定するための、前記プロセッサーによって作成されるセキュリティ識別子（１００）と、

前記セキュリティ識別子（１００）に割り当てられた基本特権（２１４）及び拡張特権（２１６）を求めることに基づいて、識別情報のセット及び該識別情報のセットに割り当てられた特権の集合を定義するための、前記プロセッサーによって作成されるセキュリティトークン（２００）と、

要求されたリソースにアクセスすることができるアカウント及び前記プロセスに関するルールを定義するための、前記プロセッサーによって作成されるセキュリティ記述子と、

前記プロセッサーによって作成されるアクセス制御リスト（４００）であって、該アクセス制御リストは、セキュリティ識別子（１００）のアクセス権を識別するための少なくとも１つのアクセス制御エントリ（５００）を含む、アクセス制御リスト（４００）と

を備える、セキュリティインフラストラクチャー。

【請求項１２】

前記セキュリティトークン（２００）は、構造体のバージョン（２０２）、フラグ（２０４）、オフセット（２０６）、直接グループの個数（２０７）、及びグループ識別子の総数（２０８）を識別するためのフィールドを含む、請求項１１に記載のセキュリティインフラストラクチャー。

【請求項１３】

前記セキュリティトークン（２００）は、プライマリオーナーセキュリティ識別子（２１０）、グループセキュリティ識別子（２１２）、基本特権（２１４）、及び拡張特権（２１６）をさらに含む、請求項１２に記載のセキュリティインフラストラクチャー。

【請求項１４】

前記プライマリセキュリティ識別子（２１０）及び前記グループセキュリティ識別子（２１２）は、前記セキュリティトークン（２００）の関連付けられるサブジェクトの識別情報を定義する、請求項１３に記載のセキュリティインフラストラクチャー。

【請求項１５】

前記基本特権（２１４）は、前記セキュリティトークン（２００）において指定された

前記識別情報に有効な特権のセットを含む、請求項１３に記載のセキュリティインフラストラクチャー。
【請求項１６】
前記拡張特権（２１６）は、前記セキュリティトークン（２００）においてセキュリティ識別子（１００）について定義されたカスタム特権を含む、請求項１３に記載のセキュリティインフラストラクチャー。
【請求項１７】
関連付けられるサブジェクトに最小特権アクセスを付与するための、プロセッサーによって実行される方法であって、
プロセッサー上で動作するオペレーティングシステムを用意するステップであって、前記プロセッサーは前記オペレーティングシステムを介してアプリケーションを実行する、ステップと、
前記プロセッサーが、前記アプリケーションによりアクセスされるリソース及び前記アプリケーションがなすことができるコールを制御するために前記オペレーティングシステムを介してセキュリティ構造を実施するステップであって、前記プロセッサーは、
前記プロセッサーがランタイムオブジェクトを作成する場合、前記プロセッサーが、関連付けられるサブジェクトのための一意の識別子を定義し、該関連付けられるサブジェクトに関連付けられるアカウントを指定するためのセキュリティ識別子（１００）を設けるステップ、
前記一意の識別子をメモリーに保持されるアカウントデータベース内のエントリにマッピングするステップであって、前記セキュリティ識別子（１００）に割り当てられた基本特権（２１４）及び拡張特権（２１６）を求める、マッピングするステップ、
前記プロセッサーが、前記関連付けられるサブジェクトのマイグレーションに沿って関連付けられるサブジェクトの識別子（２１０、２１２）を蓄積するステップ、
前記プロセッサーが、前記セキュリティ識別子（１００）に割り当てられた前記基本特権（２１４）及び前記拡張特権（２１６）を求めることに基づいて、識別情報（２１０、２１２）のセット及び該識別情報のセットに割り当てられた特権の集合を定義するためのセキュリティトークン（２００）を作成するステップ、並びに
前記プロセッサーが、前記関連付けられるサブジェクトの前記蓄積された識別子（２１０、２１２）のすべて及び前記特権（２１４、２１６）の集合をインターセクトすることによって前記関連付けられるサブジェクトのアクセス特権を求めるステップ
によって前記セキュリティ構造を実施する、ステップと
を含む方法。
【請求項１８】
前記関連付けられるサブジェクトのアクセス特権（２１４、２１６）を求める前記ステップは、前記リソースへのアクセスを付与する前に、現在の関連付けられるサブジェクトのコールチェーンコンテキストをキャプチャするステップと、前記現在の関連付けられるサブジェクトを分析して、前記コールチェーンにおける蓄積された各識別情報（２１０、２１２）及び各関連付けられるサブジェクトが、前記要求されたリソースにアクセスすることができることを検証するステップとをさらに含み、それによって、デフォルトにより最小特権を可能にする、請求項１７に記載の方法。
【請求項１９】
クライアント側（１０２０）において、関連付けられるサブジェクトのセキュリティコンテキストをメッセージキューに書き込むステップと、
前記サーバー側（１０３０）において、前記メッセージキューから前記関連付けられるサブジェクトの前記セキュリティコンテキストを非同期にリトリーブするステップと、
偽装される前記関連付けられるサブジェクトの前記リトリーブしたセキュリティコンテキストをコピーすることによって前記関連付けられるサブジェクトを偽装するステップと、
前記コピーしたセキュリティコンテキスト（７５０）を分析するステップであって、前

記要求リソースへのアクセス権を定義するセキュリティ記述子（３００）を構築する、分析するステップと、
前記セキュリティトークン（２００）に従って前記関連付けられるサブジェクトを識別するステップと、
前記セキュリティ記述子（３００）に定義された前記識別情報（３２０、３３０）が該セキュリティ記述子のアクセス制御エントリ（５００）に含まれるか否かを判断するステップと、
前記アクセス制御エントリ（５００）に基づいて前記識別情報（３２０、３３０）に利用可能なアクセス権を求めるステップと
をさらに含む、請求項１７に記載の方法。
【請求項２０】
関連付けられるサブジェクトの現在のセキュリティトークン（７１０）に関連付けられるすべての識別情報（２１０、２１２）が要求リソースにアクセスすることができるときに、前記要求されたリソースへのアクセスを付与するステップをさらに含み、現在の関連付けられるサブジェクトのコールスタック（８００）のすべてのチャンバーに関連付けられるすべての識別情報は、前記要求リソースにアクセスすることができ、前記関連付けられるサブジェクトの保存されたコンテキストに関連付けられるすべての識別情報は、前記要求されたリソースにアクセスすることができる、請求項１７に記載の方法。