【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22年10月21日(2010.10.21)

【公表番号】特表2010-503123(P2010-503123A)
【公表日】平成22年1月28日(2010.1.28)
【年通号数】公開・登録公報2010-004
【出願番号】特願2009-527540(P2009-527540)
【国際特許分類】
*Ｇ０６Ｆ　21/20　　(2006.01)*
【ＦＩ】
Ｇ０６Ｆ　15/00　　３３０Ａ

【手続補正書】
【提出日】平成22年9月6日(2010.9.6)
【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】
リソースに対するアクセス要求を、メモリに格納された許可照会テーブルを使用して評価するシステムであって、
リソースにアクセスする要求を受け取り、当該要求をリソース特有のオペレーションに変換するリソース・ガード・モジュールと、
前記許可照会テーブルを使用して、前記リソース特有のオペレーションに関連する許可照会を確認するセキュリティ・ポリシー・モジュールであって、各許可照会は、要求を評価するための基準を、事実および論理演算子を組み合わせて定義する論理的表現であり、事実は、ある主体があるリソースに対してあるアクションを実行する権利を有することを表現する、セキュリティ・ポリシー・モジュールと、
前記確認された許可照会を評価する許可エンジンと
を含むことを特徴とするシステム。
【請求項２】
前記関連する許可照会は、１つまたは複数の所定の空のスロットを有する関連する許可照会テンプレートを含むことを特徴とする請求項１に記載のシステム。
【請求項３】
前記システムは、前記リソース特有のオペレーションの主体およびオペレーション対象のリソースを前記１つまたは複数の所定の空のスロットに代入することによって、前記許可照会テンプレートを許可照会に変換することを特徴とする請求項２に記載のシステム。
【請求項４】
前記事実は、さらに、第１の主体が、第２の主体によってアサートされる事実を信じる、信頼関係を表現し、
前記許可エンジンは、前記リソース特有のオペレーションから導き出されたアサーション・コンテクストであって、前記アサーション・コンテクストは、前記アクセスを要求する主体の認証に使用されるセキュリティ・トークン、および、ある主体を信頼してアクションを許可することを対象とするポリシーから収集したアサーションにより形成される、アサーション・コンテクストを用いて前記確認された許可照会を評価する
ことを特徴とする請求項１に記載のシステム。
【請求項５】

否定表現を有するアサーションを許可しないシンタックス・バリデータをさらに含むことを特徴とする請求項４に記載のシステム。
【請求項６】
前記許可照会テーブルは、否定演算子を含む許可照会を有する少なくとも１つのフィールドを含むことを特徴とする請求項５に記載のシステム。
【請求項７】
前記関連する許可照会は、複数のアサートされる事実を含み、
前記許可エンジンは、前記アサーション・コンテクストから推定された有効なアサーションを、前記関連する許可照会の前記アサートされる事実とマッチングする
ことを特徴とする請求項４に記載のシステム。
【請求項８】
前記関連する許可照会の個々のアサートされる事実は、マッチングする有効なアサーションが、前記アサーション・コンテクストから推定されることが可能である場合、「ＴＲＵＥ」ブール・ステータスで置き換えられ、マッチングする有効なアサーションが、前記アサーション・コンテクストから推定されることが可能でない場合、「ＦＡＬＳＥ」ブール・ステータスで置き換えられることを特徴とする請求項７に記載のシステム。
【請求項９】
個別のアサートされる事実が、「ＴＲＵＥ」ブール・ステータスで置き換えられる場合、前記許可エンジンは、前記個別のアサートされる事実をＴＲＵＥにするよう構成される変数置換のセットを生成することを特徴とする請求項８に記載のシステム。
【請求項１０】
リソースに対するアクセス要求を、メモリに格納された許可照会テーブルを使用して評価する方法であって、
リソース・ガード・モジュールが、リソースにアクセスする要求を受け取るステップと、
前記リソース・ガード・モジュールが、前記要求をリソース特有のオペレーションに変換するステップと、
セキュリティ・ポリシー・モジュールが、前記許可照会テーブルを使用して、前記リソース特有のオペレーションに関連する許可照会を確認するステップであって、各許可照会は、要求を評価するための基準を、事実および論理演算子を組み合わせて定義する論理的表現であり、事実は、ある主体があるリソースに対してあるアクションを実行する権利を有することを表現する、ステップと、
許可エンジンが、前記確認された許可照会を評価するステップと
を含むことを特徴とする方法。
【請求項１１】
前記確認された許可照会は、１つまたは複数の所定の空のスロットを有する許可照会テンプレートであり、
前記リソース・ガード・モジュールが、前記リソース特有のオペレーションの主体およびオペレーション対象のリソースを前記１つまたは複数の所定の空のスロットに代入することによって、前記許可照会テンプレートを許可照会に変換するステップと
をさらに含むことを特徴とする請求項１０に記載の方法。
【請求項１２】
前記事実は、さらに、第１の主体が、第２の主体によってアサートされる事実を信じる、信頼関係を表現し、
前記許可エンジンが、（ｉ）前記リソース特有のオペレーションから導き出されたアサーション・コンテクストと、（ｉｉ）前記確認された許可照会と、を評価アルゴリズムに適用するステップであって、前記アサーション・コンテクストは、前記アクセスを要求する主体の認証に使用されるセキュリティ・トークン、および、ある主体を信頼してアクションを許可することを対象とするポリシーから収集したアサーションにより形成される、ステップと、

前記許可エンジンが、前記アサーション・コンテクストの有効なアサーションを、前記確認された許可照会のアサートされる事実とマッチングするステップと、
前記マッチングすることに応答して、前記許可エンジンが、前記確認された許可照会に対してＴＲＵＥ／ＦＡＬＳＥ置き換えプロセスを実行するステップと
をさらに含み、
置き換えプロセスを実行した後、前記評価するステップは、
前記確認された許可照会が論理的にＴＲＵＥに評価された場合、前記リソース特有のオペレーションを許可し、
前記確認された許可照会が論理的にＦＡＬＳＥに評価された場合、前記リソース特有のオペレーションを拒否することを特徴とする請求項１０に記載の方法。
【請求項１３】
リソースに対するアクセス要求を、メモリに格納された許可照会テーブルを使用して評価する方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記方法は、
リソース・ガード・モジュールが、リソースにアクセスする要求を受け取るステップと、
前記リソース・ガード・モジュールが、前記要求をリソース特有のオペレーションに変換するステップと、
セキュリティ・ポリシー・モジュールが、前記許可照会テーブルを使用して、前記リソース特有のオペレーションに関連する許可照会を確認するステップであって、各許可照会は、要求を評価するための基準を、事実および論理演算子を組み合わせて定義する論理的表現であり、事実は、ある主体があるリソースに対してあるアクションを実行する権利を有することを表現する、ステップと、
許可エンジンが、前記確認された許可照会を評価するステップと
を含むことを特徴とするコンピュータ読み取り可能な記録媒体。
【請求項１４】
前記確認された許可照会は、１つまたは複数の所定の空のスロットを有する許可照会テンプレートであり、
前記方法は、前記リソース・ガード・モジュールが、前記リソース特有のオペレーションの主体およびオペレーション対象のリソースを前記１つまたは複数の所定の空のスロットに代入することによって、前記許可照会テンプレートを許可照会に変換するステップをさらに含むことを特徴とする請求項１３に記載のコンピュータ読み取り可能な記録媒体。
【請求項１５】
前記事実は、さらに、第１の主体が、第２の主体によってアサートされる事実を信じる、信頼関係を表現し、
前記方法は、
前記許可エンジンが、（ｉ）前記リソース特有のオペレーションから導き出されたアサーション・コンテクストと、（ｉｉ）前記確認された許可照会と、を評価アルゴリズムに適用するステップであって、前記アサーション・コンテクストは、前記アクセスを要求する主体の認証に使用されるセキュリティ・トークン、および、ある主体を信頼してアクションを許可することを対象とするポリシーから収集したアサーションにより形成される、ステップと、
前記許可エンジンが、前記アサーション・コンテクストの有効なアサーションを、前記確認された許可照会のアサートされる事実とマッチングするステップと、
前記マッチングすることに応答して、前記許可エンジンが、前記確認された許可照会に対してＴＲＵＥ／ＦＡＬＳＥ置き換えプロセスを実行するステップと
をさらに含み、
置き換えプロセスを実行した後、前記評価するステップは、
前記確認された許可照会が論理的にＴＲＵＥに評価された場合、前記リソース特有のオペレーションを許可し、

前記確認された許可照会が論理的にＦＡＬＳＥに評価された場合、前記リソース特有のオペレーションを拒否することを特徴とする請求項１３に記載のコンピュータ読み取り可能な記録媒体。