

【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 8 月 9 日 (2012.8.9)

【公表番号】特表 2011-527482 (P2011-527482A)
 【公表日】平成 23 年 10 月 27 日 (2011.10.27)
 【年通号数】公開・登録公報 2011-043
 【出願番号】特願 2011-517472 (P2011-517472)
 【国際特許分類】

G 0 6 F 21/20 (2006.01)

H 0 4 L 9/32 (2006.01)

【 F I 】

G 0 6 F 15/00 3 3 0 B

H 0 4 L 9/00 6 7 3 A

【手続補正書】
 【提出日】平成 24 年 6 月 20 日 (2012.6.20)
 【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】

セキュリティアイデンティティを表すためのデータモデルのデータ構造であって、
 エンティティのアイデンティティを少なくとも 1 つの他のエンティティに対する複数の
 属性として表す少なくとも 1 つのアイデンティティコンポーネントのための記憶領域、
 前記エンティティのアイデンティティに関連付けられたセキュリティ情報を表す少なく
 とも 1 つのアイデンティティ・プリンシパル・コンポーネントのための記録領域、
 前記エンティティによって少なくとも 1 つの他のエンティティに対して作成された宣言
 を表す少なくとも 1 つのクレームコンポーネントのための記録領域、および
 前記宣言に関連付けられたメタデータを表す少なくとも 1 つのクレーム・プロパティ・
 コンポーネントのための記録領域を備え、
少なくとも 1 つのクレームを表すために、前記アイデンティティコンポーネント、アイ
 デンティティ・プリンシパル・コンポーネント、クレームコンポーネント、クレーム・プ
 ロパティ・コンポーネントが組み合わされて、前記データモデルが前記エンティティのコン
 ピュータまたは前記データモデルを作成したコンピュータから他のエンティティのコン
 ピュータに送られ、前記他のエンティティのコンピュータは、前記エンティティのコンピ
 ュータまたは前記データモデルを作成したコンピュータから受け取ったデータモデルを使
 用することにより前記エンティティのアイデンティティを認証することを特徴とするデー
 タモデルのデータ構造。

【請求項 2】

前記アイデンティティコンポーネントは、前記クレームのコレクション、ラベル、およ
 び委任アイデンティティのフィールドを含むことを特徴とする請求項 1 に記載のデータモ
 デルのデータ構造。

【請求項 3】

前記アイデンティティ・プリンシパル・コンポーネントは、アイデンティティコレクシ
 ョンのフィールドを含むことを特徴とする請求項 1 に記載のデータモデルのデータ構造。

【請求項 4】

前記クレームコンポーネントは、前記クレームのタイプ、クレーム値、クレーム値タイ

ブ、プロパティコレクション、発行者、および対象者のフィールドを含むことを特徴とする請求項 1 に記載のデータモデルのデータ構造。

【請求項 5】

前記少なくとも 1 つのクレーム・プロパティ・コンポーネントは、前記各々の少なくとも 1 つのクレームコンポーネントに関連付けられ、前記少なくとも 1 つのクレームコンポーネントは、前記少なくとも 1 つのアイデンティティ・プリンシパル・コンポーネントに関連付けられ、前記少なくとも 1 つのクレーム・プロパティ・コンポーネントは、前記少なくとも 1 つのクレームコンポーネントに関連付けられることを特徴とする請求項 1 に記載のデータモデルのデータ構造。

【請求項 6】

前記少なくとも 1 つのクレーム・アイデンティティ・コンポーネントは、1 つのクレームコンポーネントに関連付けられることを特徴とする請求項 1 に記載のデータモデルのデータ構造。

【請求項 7】

前記データモデルを作成したコンピュータにより前記クレームがセキュリティトークンに変換されることをさらに含むことを特徴とする請求項 1 に記載のデータモデルのデータ構造。

【請求項 8】

エンティティのアイデンティティを少なくとも 1 つの他のエンティティに対する複数の属性として表す第 1 のパラメータ、

前記エンティティのアイデンティティに関連付けられたセキュリティ情報を表す第 2 のパラメータ、

前記エンティティによって前記少なくとも 1 つの他のエンティティに対して作成された宣言を表す第 3 のパラメータ、

前記宣言に関連付けられたメタデータを表す第 4 のパラメータ、および

前記第 1 ～ 第 4 のパラメータを受信して格納し、当該格納された第 1 ～ 第 4 のパラメータを使用することにより前記エンティティのアイデンティティを認証する処理をコンピュータに実行させるプログラム

を記憶していることを特徴とするコンピュータ可読記憶媒体。

【請求項 9】

前記第 1 のパラメータは、クレーム・アイデンティティ・パラメータであることを特徴とする請求項 8 に記載のコンピュータ可読記憶媒体。

【請求項 10】

前記第 2 のパラメータは、アイデンティティ・プリンシパル・パラメータであることを特徴とする請求項 8 に記載のコンピュータ可読記憶媒体。

【請求項 11】

前記第 3 のパラメータは、クレームパラメータであることを特徴とする請求項 8 に記載のコンピュータ可読記憶媒体。

【請求項 12】

前記第 4 のパラメータは、クレーム・プロパティ・パラメータであることを特徴とする請求項 8 に記載のコンピュータ可読記憶媒体。

【請求項 13】

前記アイデンティティコンポーネントは、前記クレームのコレクション、ラベル、および委任アイデンティティのフィールドを含むことを特徴とする請求項 9 に記載のコンピュータ可読記憶媒体。

【請求項 14】

前記アイデンティティ・プリンシパル・コンポーネントは、前記アイデンティティのコレクションのフィールドを含むことを特徴とする請求項 10 に記載のコンピュータ可読記憶媒体。

【請求項 15】

前記クレームコンポーネントは、前記クレームのタイプ、クレーム値、クレーム値タイプ、プロパティコレクション、発行者、および対象者のフィールドを含むことを特徴とする請求項 11 に記載のコンピュータ可読記憶媒体。

【請求項 16】

第 1 のエンティティに関連付けられている第 1 のセキュリティ識別子を第 1 のコンピュータで発行するステップ、

前記第 1 のセキュリティ識別子を少なくとも 1 つの処理サーバに送信するステップ、

第 2 のエンティティに関連付けられている第 2 のセキュリティ識別子を第 2 のコンピュータで発行するステップであって、前記第 2 のセキュリティ識別子には前記第 1 のセキュリティ識別子が組み込まれている、第 2 のセキュリティ識別子を発行するステップ、および

前記第 1 のエンティティのアイデンティティに関して、前記第 2 のセキュリティ識別子に基づいて第 3 のコンピュータで認証決定を行うことを特徴とする方法。

【請求項 17】

前記第 1 のセキュリティ識別子は少なくとも 1 つのクレームを含み、前記第 2 のセキュリティ識別子は少なくとも 1 つのクレームを含むことを特徴とする請求項 16 に記載の方法。

【請求項 18】

前記少なくとも 1 つのクレームは、エンティティに関する宣言を含むことを特徴とする請求項 17 に記載の方法。

【請求項 19】

前記第 1 のコンピュータで、前記第 1 のセキュリティ識別子を第 1 のセキュリティトークンにパッケージ化して前記第 2 のコンピュータに送信するステップおよび前記第 2 のコンピュータで前記第 2 の識別子を前記第 2 のセキュリティトークンにパッケージ化して前記第 3 のコンピュータに送信するステップをさらに含むことを特徴とする請求項 16 に記載の方法。

【請求項 20】

前記第 3 のコンピュータは、前記第 1 のエンティティのアイデンティティに関して、前記第 2 のセキュリティ識別子の中に組み込まれた第 1 のセキュリティ識別子に基づいて認証決定を行うことを特徴とする請求項 16 に記載の方法。