

【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 06 F 21/20 (2006.01)

H 04 L 9/32 (2006.01)

【F I】

G 06 F 15/00 3 3 0 B

H 04 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・プリンシバル・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・プリンシバル・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・プリンシバル・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。