【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７部門第３区分
【発行日】平成25年3月14日(2013.3.14)

【公表番号】特表2012-518330(P2012-518330A)
【公表日】平成24年8月9日(2012.8.9)
【年通号数】公開・登録公報2012-031
【出願番号】特願2011-550170(P2011-550170)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/62　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｇ０６Ｆ　21/24　１６６Ｅ

【手続補正書】
【提出日】平成25年1月28日(2013.1.28)
【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】
信頼性を複数のエンティティに分散させて一点でのデータ暴露を回避する、データをサブスクライブするための方法であって、
少なくとも１つのサブスクライバ装置が、データ・ストレージ・プロバイダから検索可能な暗号化データのサブセットを要求するステップであって、前記検索可能な暗号化データにより、前記暗号化データのサブセットを越えてアクセスすることなく、検索機能または問合せ機能に基づく前記暗号化データのサブセットへの選択的なアクセスを提供する、ステップと、
前記少なくとも１つのサブスクライバ装置に関連付けられた識別情報に基づいて、暗号化鍵情報を生成する鍵生成コンポーネントから、暗号化鍵情報を受信するステップであって、前記鍵生成コンポーネントは、前記データ・ストレージ・サーバから独立して分離している、ステップと、
前記要求した検索可能な暗号化データのサブセットを受信するステップと、
前記暗号化鍵情報において定義されたケイパビリティによって許可されるように、前記暗号化鍵情報を用いて前記暗号化データのサブセットを復号化するステップと、
前記要求と一致する暗号化データの正しいサブセットを前記少なくとも１つのサブスクライバ装置が受信したことを、妥当性確認するステップと
を含むことを特徴とする方法。
【請求項２】
前記妥当性確認するステップは、前記正しいサブセットを前記少なくとも１つのサブスクライバが受信したことを証明するための、データ所有証明を実施するステップを含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記受信するステップは、暗号化鍵情報を、前記識別情報から決定する少なくとも１つの役割に基づいて前記暗号化鍵情報を生成する、独立した制御領域で実行される鍵生成コンポーネントから受け取るステップを含むことを特徴とする請求項１に記載の方法。
【請求項４】

前記暗号化データのサブセットを受け取る前に、前記暗号化データのサブセットの内容が削除も修正もされていなかったことを検証するステップをさらに含むことを特徴とする請求項１に記載の方法。
【請求項５】
前記検証するステップは、前記コンテンツに干渉しないことを証明するための、再取り出し可能性証明を実施するステップを含むことを特徴とする請求項４に記載の方法。
【請求項６】
信頼性を複数のエンティティに分散させることによりデータへの選択的なアクセスを提供して、一点でのデータ暴露を回避するためのシステムであって、
選択的にアクセス可能な暗号化データレコードを格納する少なくとも１つのデータ・ストアであって、少なくとも１つのサブスクライバがデータレコードのサブセットに対するサブスクリプションを要求する、データ・ストアと、
前記少なくとも１つのサブスクライバに関連付けられた識別情報に基づいて、暗号化鍵情報を生成する第１の独立エンティティと、
前記第１の独立エンティティによって生成された前記暗号化鍵情報に基づいて、前記サブセットの復号化を実行する第２の独立エンティティであって、前選択的にアクセス可能な暗号化データにより、前記暗号化データのサブセットを越えてアクセスすることなく、検索機能または問合せ機能に基づく前記暗号化データのサブセットへの選択的なアクセスを提供する、第２の独立エンティティと、
ネットワークサービスを実行するよう構成され、前記少なくとも１つのサブスクライバによる少なくとも１つの要求を取り扱う少なくとも１つのプロセッサであって、前記データレコードのサブセットへの選択的なアクセスを提供し、前記サブセットが、前記サブスクリプションと一致する正しいサブセットであることを妥当性確認する、少なくとも１つのプロセッサと
を備えたことを特徴とするシステム。
【請求項７】
信頼性を複数のエンティティに分散させて一点でのデータ暴露を回避する、データをサブスクライブするための方法であって、
少なくとも１つのサブスクライバ装置が、データ・ストレージ・プロバイダから検索可能な暗号化データのサブセットを要求するステップであって、前記検索可能な暗号化データにより、前記暗号化データのサブセットを越えてアクセスすることなく、検索機能または問合せ機能に基づく前記暗号化データのサブセットへの選択的なアクセスを提供する、ステップと、
前記少なくとも１つのサブスクライバ装置に関連付けられた識別情報に基づいて、前記暗号化鍵情報を生成する鍵生成コンポーネントから、暗号化鍵情報を受信するステップであって、前記鍵生成コンポーネントは、前記データ・ストレージ・サーバから独立して分離している、ステップと、
前記要求した検索可能な暗号化データのサブセットを受信するステップと、
前記暗号化鍵情報において定義されたケイパビリティによって許可されるように、前記暗号化鍵情報を用いて前記暗号化データのサブセットを復号化するステップと、
前記少なくとも１つのサブスクライバ装置によって受け取られる前に、前記暗号化データのサブセットの内容が削除も修正もされていなかったことを検証するステップと
を含むことを特徴とする方法。
【請求項８】
前記検証するステップは、前記コンテンツに干渉しないことを証明するための、再取り出し可能性証明を実施するステップを含むことを特徴とする請求項７に記載の方法。
【請求項９】
前記受信するステップは、暗号化鍵情報を、前記識別情報から決定する少なくとも１つの役割に基づいて前記暗号化鍵情報を生成する鍵生成コンポーネントから受け取るステップを含むことを特徴とする請求項７に記載の方法。

【請求項１０】
前記要求と一致する暗号化データの正しいサブセットを前記少なくとも１つのサブスクライバ装置が受信したことを、妥当性確認するステップをさらに含むことを特徴とする請求項７に記載の方法。
【請求項１１】
前記妥当性確認するステップは、前記正しいサブセットを前記少なくとも１つのサブスクライバが受信したことを証明するための、データ所有証明を実施するステップを含むことを特徴とする請求項１０に記載の方法。
【請求項１２】
信頼性を複数のエンティティに分散させることによりデータへの選択的なアクセスを提供して、一点でのデータ暴露を回避するためのシステムであって、
選択的にアクセス可能な暗号化データレコードを格納する少なくとも１つのデータ・ストアであって、少なくとも１つのサブスクライバ装置がデータレコードのサブセットに対するサブスクリプションを要求する、データ・ストアと、
前記少なくとも１つのサブスクライバ装置に関連付けられた識別情報に基づいて、暗号化鍵情報を生成する第１の独立エンティティと、
前記第１の独立エンティティによって生成された前記暗号化鍵情報に基づいて、前記サブセットの復号化を実行する第２の独立エンティティであって、前選択的にアクセス可能な暗号化データにより、前記暗号化データのサブセットを越えてアクセスすることなく、検索機能または問合せ機能に基づく前記暗号化データのサブセットへの選択的なアクセスを提供する、第２の独立エンティティと、
前記少なくとも１つのサブスクライバ装置による要求について、ネットワークサービスを実行するよう構成される少なくとも１つのプロセッサであって、前記データレコードのサブセットへの選択的なアクセスを提供し、前記サブセットの前記データレコードの内容が許可なく修正されていないことを検証する、少なくとも１つのプロセッサと
を備えたことを特徴とするシステム。