【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2012-518329(P2012-518329A)
【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2011-550169(P2011-550169)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/31　(2013.01)
Ｇ０６Ｆ　21/62　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｇ０６Ｆ　21/20　１３１Ｅ
Ｇ０６Ｆ　21/24　１６６Ａ

【手続補正書】
【提出日】平成25年1月25日(2013.1.25)
【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】
少なくとも部分的に暗号化技術プロバイダにより分散される少なくとも１つの暗号化コンポーネントであって、データの発行またはデータのサブスクライブの少なくとも一方のための鍵情報を生成する鍵ジェネレータから独立して実装され、前記少なくとも１つの暗号化コンポーネントは、前記鍵ジェネレータにより生成される前記鍵情報に基づき、少なくとも１つの検索可能な暗号化アルゴリズムまたは検索可能な復号アルゴリズムを実行するように構成される少なくとも１つのプロセッサを含み、前記鍵情報は、前記少なくとも１つの暗号化コンポーネントにより暗号化される前記データに対するアクセス特権を定義する機能情報を含み、前記機能情報は、最新のアクセス特権を所与のサブスクライバに与えることができるように遅延バインドされ、前記所与のサブスクライバに対してアクセス可能にするデータは、サブスクライバの機能が前記鍵情報内に符号化されるので、発行者による前記アクセス特権に対する変更と一致して動的に変化する、暗号化コンポーネントと、
ネットワークサービスプロバイダであって、前記鍵ジェネレータおよび前記少なくとも１つの暗号化コンポーネントから独立して実装され、前記少なくとも１つの暗号化コンポーネントにより暗号化されるデータに対してネットワークサービスを実装するように構成される少なくとも１つのプロセッサを含む、ネットワークサービスプロバイダと
を備えたことを特徴とするシステム。
【請求項２】
前記ネットワークサービスプロバイダから、サブスクライバにより取り出されるデータ項目を検証して、前記ネットワークサービスから正しい項目を取り出したことを、サブスクライバに証明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３】
前記ネットワークサービスプロバイダから、サブスクライバにより取り出される前記データ項目の内容を照合して、前記データ項目の内容に障害が無いことを、サブスクライバ

に証明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４】
データサブスクライバ、またはデータの発行者は、匿名の認証情報に基づき、それぞれコンテンツをサブスクライブして、または発行して、個人情報を露出することなく特権が与えられるサブスクライバまたは発行者のロールを判定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】
前記ネットワークサービスプロバイダは、選択的にアクセス可能な暗号化されたデータを記憶する少なくとも１つのデータストアをさらに含み、少なくとも１つのサブスクライバは、前記暗号化されたデータの特定のサブセットをサブスクライブして、第１の独立エンティティは、少なくとも１つのサブスクライバに関連する識別情報に基づき暗号化鍵情報を生成して、第２の独立エンティティは、前記第１の独立エンティティにより生成される暗号化鍵情報に基づき、前記特定のサブセットの復号を実行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６】
前記少なくとも１つのサブスクライバは、前記暗号化されたデータのサブセットを監査する少なくとも１つの監査者であることを特徴とする請求項５に記載のシステム。
【請求項７】
前記少なくとも１つのサブスクライバは、前記暗号化されたデータに影響を与える処理を管理または監視する少なくとも１つの管理者であることを特徴とする請求項５に記載のシステム。
【請求項８】
データをサブスクライブする方法であって、前記方法は、
少なくとも１つのサブスクライバデバイスからの検索可能に暗号化されたデータのサブセットの要求に応答して、前記少なくとも１つのサブスクライバデバイスに関連する識別情報に基づき暗号化鍵情報を生成する鍵生成コンポーネントから、前記暗号化鍵情報を受信することと、
前記暗号化鍵情報において定義される少なくとも１つサブスクライバデバイスに与えられる特権の機能として、前記暗号化されたデータのサブセットを復号することと、
前記少なくとも１つのサブスクライバデバイスからの暗号化されたデータの前記サブセットのデータ項目に対する取得可能性の証明の要求を受信することと、
前記少なくとも１つのサブスクライバデバイスによる前記要求に関連する暗号化されたデータの前記サブセットにおける前記データ項目が正しいことを、前記サブスクライバデバイスに対し証明するための情報を生成することと
を含む方法。
【請求項９】
前記受信することは、前記少なくとも１つのサブスクライバデバイスのロールに基づいて前記暗号化鍵情報を生成する制御の別個の領域において操作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ことを備えたことを特徴とする請求項８に記載の方法。
【請求項１０】
前記受信することは、前記少なくとも１つのサブスクライバデバイスのロールを監査する機能として、暗号化鍵情報を受信することを備えたことを特徴とする請求項９に記載の方法。
【請求項１１】
前記受信することは、前記少なくとも１つのサブスクライバデバイスの管理者のロールの機能として暗号化鍵情報を受信することを備えたことを特徴とする請求項９に記載の方法。
【請求項１２】
前記少なくとも１つのサブスクライバデバイスによる要求より前に、前記暗号化されたデータのサブセットは干渉されなかったという証明を求める要求を受信することと、

前記少なくとも１つのサブスクライバデバイスによる要求より前に、前記暗号化されたデータのサブセットが干渉されなかったということをサブスクライバデバイスに証明する情報を生成することと

をさらに備えたことを特徴とする請求項８に記載の方法。