【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２区分
【発行日】平成20年8月7日(2008.8.7)

【公表番号】特表2008-500589(P2008-500589A)
【公表日】平成20年1月10日(2008.1.10)
【年通号数】公開・登録公報2008-001
【出願番号】特願2007-515538(P2007-515538)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
Ｇ０６Ｑ　50/00　(2006.01)
Ｇ０６Ｑ　30/00　(2006.01)
Ｇ０９Ｃ　5/00　(2006.01)
Ｈ０４Ｎ　7/167　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６６０Ｄ
Ｇ０６Ｆ　17/60　１４２
Ｇ０６Ｆ　17/60　３０２Ｅ
Ｇ０９Ｃ　5/00
Ｈ０４Ｎ　7/167　Ｚ
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｇ０６Ｆ　15/00　３３０Ｚ

【手続補正書】
【提出日】平成20年6月23日(2008.6.23)
【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】
コンテンツ・アイテムを配信する方法であって、
第１のエンティティで、暗号化済みコンテンツを得るステップであって、前記暗号化済みコンテンツは、第１の暗号化鍵で暗号化されたコンテンツ・アイテムを含む、ステップと、
前記第１のエンティティで、認証手段に、第１部分と第１鍵とを有する第１の変化識別子を要求するステップと、
前記第１のエンティティで、透かしを、前記第１の変化識別子からの前記第１鍵で暗号化して、第１の暗号化済みラベルを生成するステップと、
前記第１のエンティティで、前記第１の変化識別子の前記第１部分を、前記第１の暗号化済みラベルとグループ化して、第１の暗号化済み透かしを生成するステップと、
前記第１のエンティティで、通信リンクを介して、アイデンティティおよび第２の変化識別子を有する第２のエンティティからコンテンツ・アイテムを求める要求を受信するステップと、
前記第１のエンティティで、暗号化解除鍵を求める要求を生成するステップと、
前記暗号化解除鍵を求める要求を、通信リンクを介して、前記第１のエンティティから前記認証手段へ送るステップと、

前記第１のエンティティで、通信リンクを介して、第１の前記暗号化解除鍵と第２の暗号化鍵とを前記認証手段から受信するステップと、
前記第１のエンティティで、前記第１の暗号化解除鍵を用いて、前記暗号化済みコンテンツの暗号化解除を行い、前記コンテンツ・アイテムを得るステップと、
前記第１のエンティティで、前記コンテンツ・アイテムへ前記透かしを適用して、透かし付きコンテンツを得るステップと、
前記第１のエンティティで、前記第２の暗号化鍵を用いて前記透かし付きコンテンツを暗号化して、暗号化済み透かし付きコンテンツを生成するステップと、
前記第１の暗号化済み透かしを、通信リンクを介して、前記第１のエンティティから前記第２のエンティティへ送るステップと、
前記認証手段で、前記第２のエンティティの前記アイデンティティを検証するステップと、
前記第２のエンティティの前記アイデンティティの検証に基づいて、前記暗号化済み透かし付きコンテンツを、通信リンクを介して、前記第１のエンティティから前記第２のエンティティへ送るステップと、
前記第２のエンティティの前記アイデンティティの検証に基づいて、第２の暗号化解除鍵を、通信リンクを介して、前記認証手段から前記第２のエンティティへ送るステップと
を備える方法。
【請求項２】
請求項１に記載の方法であって、前記透かしを含む複数の透かしを生成するステップを更に備え、それぞれの透かしは独特のものである、方法。
【請求項３】
請求項１に記載の方法であって、前記第１の暗号化鍵は、前記コンテンツ・アイテムと関連する既知の識別子と関連する、方法。
【請求項４】
請求項１に記載の方法であって、前記第２の暗号化解除鍵は、前記透かし付きコンテンツを暗号化するために用いられる前記第２の暗号化鍵である、方法。
【請求項５】
請求項１に記載の方法であって、前記第１の暗号化済み透かしは、前記第２のエンティティへのみへ送られる、方法。
【請求項６】
請求項１に記載の方法であって、
前記第２のエンティティの前記アイデンティティを検証する前記ステップは、
前記第２のエンティティで、前記第２のエンティティの前記第２の変化識別子に含まれる鍵を用いて前記第１の暗号化済み透かしを暗号化して、二重に暗号化した透かしを作成するステップと、
前記二重に暗号化した透かしを、前記第２のエンティティから前記認証手段へ送るステップと、
前記認証手段で、前記二重に暗号化した透かしの暗号化解除を行い、前記第１の暗号化済み透かしを取り出すステップと、
前記認証手段で、前記第１の暗号化済み透かしの暗号化解除を行い、前記透かしを取り出すステップと、
前記認証手段で、前記第１のエンティティに対しての受領証を生成するステップと
を備える、
方法。
【請求項７】
請求項６に記載の方法であって、前記第１のエンティティに対する前記受領証が、前記第２のエンティティのアイデンティティと前記第１の暗号化済み透かしとを連結したものを含む、方法。
【請求項８】

請求項６に記載の方法であって、前記認証手段で、前記第１のエンティティに知られている変化識別子で、前記第１のエンティティに対する前記受領証を暗号化するステップを更に備える方法。
【請求項９】
請求項６に記載の方法であって、前記認証手段から第３の変化識別子を前記第２のエンティティへ送るステップを更に備える方法。
【請求項１０】
請求項９に記載の方法であって、前記認証手段で、前記第２の変化識別子を使用済みとマーク付けするステップを更に備える方法。
【請求項１１】
請求項１に記載の方法であって、前記認証手段で、第３のエンティティに対しての受領証を生成するステップを更に備える方法。
【請求項１２】
請求項１１に記載の方法であって、前記第３のエンティティに対する前記受領証が、前記第２のエンティティのアイデンティティと、前記透かしの関数とを連結したものを含む、方法。
【請求項１３】
請求項１１に記載の方法であって、前記第３のエンティティに知られている変化識別子を用いて、前記第３のエンティティに対する前記受領証を暗号化するステップを更に備える方法。
【請求項１４】
請求項１に記載の方法であって、前記認証手段で、前記第１の変化識別子を使用済みとマーク付けするステップを更に備える方法。
【請求項１５】
請求項１に記載の方法であって、前記第２の暗号化解除鍵を前記第２のエンティティへ送る前に、前記第２の暗号化解除鍵と関連する既知の識別子に基づいて、前記第２のエンティティへ前記第２の暗号化解除鍵の許可を要求するステップを更に備える方法。
【請求項１６】
請求項１に記載の方法であって、第３のエンティティで、前記コンテンツ・アイテムにラベルを割り当てるステップを更に備える方法。
【請求項１７】
請求項１６に記載の方法であって、前記第３のエンティティで、前記第１の暗号化鍵についての、鍵を求める要求を生成するステップを更に備え、前記鍵を求める要求は前記ラベルを含む、方法。
【請求項１８】
請求項１７に記載の方法であって、前記鍵を求める要求を、前記第３のエンティティから前記認証手段へ送るステップを更に備える方法。
【請求項１９】
請求項１８に記載の方法であって、前記第３のエンティティで、前記認証手段から前記第１の暗号化鍵を受信するステップを更に備える方法。
【請求項２０】
請求項１９に記載の方法であって、前記第３のエンティティで、前記第１の暗号化鍵を用いて前記コンテンツ・アイテムを暗号化して、前記暗号化済みコンテンツを生成するステップを更に備える方法。
【請求項２１】
請求項２０に記載の方法であって、前記暗号化済みコンテンツを、通信リンクを介して、前記第１のエンティティへ送るステップを更に備える方法。
【請求項２２】
コンテンツを配信する方法であって、
第１のエンティティで、暗号化済みコンテンツを得るステップであって、前記暗号化済

みコンテンツは、第１の暗号化鍵で暗号化されたコンテンツ・アイテムを含む、ステップと、
前記第１のエンティティで、第１の暗号化済み透かしを得るステップであって、前記第１の暗号化済み透かしは、第１の変化識別子の第１鍵で暗号化された透かしを含む、ステップと、
前記第１のエンティティで、認証手段に、第２部分と第２鍵とを有する第２の変化識別子を要求するステップと、
前記第１のエンティティで、前記第１の暗号化済み透かしを、前記第２の変化識別子からの前記第２鍵で暗号化して、第２の暗号化済み透かしを生成するステップと、
前記第１のエンティティで、前記第２の変化識別子の前記第２部分を、前記第２の暗号化済み透かしとグループ化して、第１の二重暗号化済み透かしを生成するステップと、
前記第１のエンティティで、通信リンクを介して、アイデンティティおよび第３の変化識別子を有する第２のエンティティからコンテンツ・アイテムを求める要求を受信するステップと、
前記第１のエンティティで、暗号化解除鍵を求める要求を生成するステップと、
前記暗号化解除鍵を求める要求を、通信リンクを介して、前記第１のエンティティから前記認証手段へ送るステップと、
前記第１のエンティティで、通信リンクを介して、前記透かしと、第１の暗号化解除鍵と第２の暗号化鍵とを前記認証手段から受信するステップと、
前記第１のエンティティで、前記第１の暗号化解除鍵を用いて、前記暗号化済みコンテンツの暗号化解除を行い、前記コンテンツ・アイテムを得るステップと、
前記第１のエンティティで、前記コンテンツ・アイテムへ前記透かしを適用して、透かし付きコンテンツを得るステップと、
前記第１のエンティティで、前記第２の暗号化鍵を用いて前記透かし付きコンテンツを暗号化して、暗号化済み透かし付きコンテンツを生成するステップと、
前記第１の二重暗号化済み透かしを、通信リンクを介して、前記第１のエンティティから前記第２のエンティティへ送るステップと、
前記認証手段で、前記第２のエンティティの前記アイデンティティを検証するステップと、
前記第２のエンティティの前記アイデンティティの検証に基づいて、前記暗号化済み透かし付きコンテンツを、通信リンクを介して、前記第１のエンティティから前記第２のエンティティへ送るステップと、
前記第２のエンティティの前記アイデンティティの検証に基づいて、第２の暗号化解除鍵を、通信リンクを介して、前記認証手段から前記第２のエンティティへ送るステップと
を備える方法。
【請求項２３】
請求項２２に記載の方法であって、前記透かしを含む複数の透かしを生成するステップを更に備え、それぞれの透かしは独特のものである、方法。
【請求項２４】
請求項２２に記載の方法であって、前記第１の暗号化鍵は既知の識別子と関連し、前記既知の識別子は前記要求に含まれる、方法。
【請求項２５】
請求項２２に記載の方法であって、前記第２の暗号化解除鍵は、前記透かし付きコンテンツを暗号化するために用いられる前記第２の暗号化鍵である、方法。
【請求項２６】
請求項２２に記載の方法であって、前記第１の二重暗号化済み透かしは、前記第２のエンティティへのみへ送られる、方法。
【請求項２７】
請求項２２に記載の方法であって、
前記第２のエンティティの前記アイデンティティを検証する前記ステップは、

前記第２のエンティティで、前記第２のエンティティの前記第３の変化識別子に含まれる鍵を用いて前記第１の二重暗号化済み透かしを暗号化して、三重に暗号化した透かしを作成するステップと、

前記三重に暗号化した透かしを、前記第２のエンティティから前記認証手段へ送るステップと、

前記認証手段で、前記三重に暗号化した透かしの暗号化解除を行い、前記第１の二重暗号化済み透かしを取り出すステップと、

前記認証手段で、前記第１の二重暗号化済み透かしの暗号化解除を行い、前記暗号化済み透かしを取り出すステップと、

前記認証手段で、前記暗号化済み透かしの暗号化解除を行い、前記透かしを取り出すステップと、

前記認証手段で、前記第１のエンティティに対しての受領証を生成するステップとを備える、

方法。

【請求項２８】

請求項２７に記載の方法であって、前記第１のエンティティに対する前記受領証が、前記第２のエンティティのアイデンティティと前記暗号化済み透かしとを連結したものを含む、方法。

【請求項２９】

請求項２７に記載の方法であって、前記認証手段で、前記第１のエンティティに知られている変化識別子で、前記受領証を暗号化するステップを更に備える方法。

【請求項３０】

請求項２２に記載の方法であって、前記認証手段から第４の変化識別子を前記第２のエンティティへ送るステップを更に備える方法。

【請求項３１】

請求項３０に記載の方法であって、前記認証手段で、前記第３の変化識別子を使用済みとマーク付けするステップを更に備える方法。

【請求項３２】

請求項２２に記載の方法であって、前記認証手段で、前記第１の変化識別子および前記第２の変化識別子を使用済みとマーク付けするステップを更に備える方法。

【請求項３３】

請求項２２に記載の方法であって、前記認証手段で、第３のエンティティに対しての受領証を生成するステップを更に備える方法。

【請求項３４】

請求項３３に記載の方法であって、前記第３のエンティティに対する前記受領証が、前記第２のエンティティのアイデンティティと、前記透かしの関数とを連結したものを含む、方法。

【請求項３５】

請求項３３に記載の方法であって、前記認証手段で、前記第３のエンティティに知られている変化識別子を用いて、前記第３のエンティティに対する前記受領証を暗号化するステップを更に備える方法。

【請求項３６】

請求項２２に記載の方法であって、前記認証手段で、前記第２の暗号化解除鍵を前記第２のエンティティへ送る前に、前記第２の暗号化解除鍵と関連する既知の識別子に基づいて、前記第２のエンティティへ前記第２の暗号化解除鍵の許可を要求するステップを更に備える方法。

【請求項３７】

請求項２２に記載の方法であって、第３のエンティティで、前記コンテンツ・アイテムにラベルを割り当てるステップを更に備える方法。

【請求項３８】

請求項３７に記載の方法であって、前記第３のエンティティで、前記第１の暗号化鍵についての、鍵を求める要求を生成するステップを更に備え、前記鍵を求める要求は前記ラベルを含む、方法。

【請求項３９】

請求項３８に記載の方法であって、前記鍵を求める要求を、前記第３のエンティティから前記認証手段へ送るステップを更に備える方法。

【請求項４０】

請求項３９に記載の方法であって、前記第３のエンティティで、前記認証手段から前記第１の暗号化鍵を受信するステップを更に備える方法。

【請求項４１】

請求項４０に記載の方法であって、前記第１の暗号化鍵を用いて前記コンテンツ・アイテムを暗号化して、前記暗号化済みコンテンツを生成するステップを更に備える方法。

【請求項４２】

請求項４１に記載の方法であって、前記暗号化済みコンテンツを、通信リンクを介して、前記第１のエンティティへ送るステップを更に備える方法。

【請求項４３】

請求項４２に記載の方法であって、前記第３のエンティティで透かしを生成するステップを更に備える方法。

【請求項４４】

請求項４３に記載の方法であって、前記第３のエンティティで、前記認証手段に、前記第１の変化識別子を要求するステップであって、前記第１の変化識別子は第１部分および第１鍵を含む、ステップを更に備える方法。

【請求項４５】

請求項４４に記載の方法であって、前記第３のエンティティで、前記認証手段から前記第１の変化識別子を受信するステップを更に備える方法。

【請求項４６】

請求項４５に記載の方法であって、前記第３のエンティティで、前記第１の変化識別子の前記第１鍵を用いて前記ラベルおよび前記透かしを暗号化して、第１の暗号化済み透かしを生成するステップを更に備える方法。

【請求項４７】

請求項４６に記載の方法であって、前記第１の変化識別子の前記第１部分を、第１の前記暗号化済みラベルとグループ化して、第１の暗号化済み透かしを生成するステップを更に備える方法。

【請求項４８】

請求項４７に記載の方法であって、前記第１の暗号化済み透かしを、通信リンクを介して、前記第１のエンティティへ送るステップを更に備える方法。