

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5491499号
(P5491499)

(45) 発行日 平成26年5月14日 (2014.5.14)

(24) 登録日 平成26年3月7日 (2014.3.7)

(51) Int.Cl.

F I

G 0 6 F 21/33 (2013.01)

G 0 6 F 21/20 1 3 3

H 0 4 L 9/32 (2006.01)

H 0 4 L 9/00 6 7 5 B

H 0 4 L 9/08 (2006.01)

H 0 4 L 9/00 6 0 1 F

請求項の数 20 (全 25 頁)

(21) 出願番号 特願2011-512565 (P2011-512565)
 (86) (22) 出願日 平成21年6月1日 (2009.6.1)
 (65) 公表番号 特表2011-525014 (P2011-525014A)
 (43) 公表日 平成23年9月8日 (2011.9.8)
 (86) 国際出願番号 PCT/US2009/045857
 (87) 国際公開番号 W02009/149019
 (87) 国際公開日 平成21年12月10日 (2009.12.10)
 審査請求日 平成24年5月31日 (2012.5.31)
 (31) 優先権主張番号 12/134, 360
 (32) 優先日 平成20年6月6日 (2008.6.6)
 (33) 優先権主張国 米国 (US)

(73) 特許権者 500046438
 マイクロソフト コーポレーション
 アメリカ合衆国 ワシントン州 9805
 2-6399 レッドモンド ワン マイ
 クロソフト ウェイ
 (74) 代理人 100140109
 弁理士 小野 新次郎
 (74) 代理人 100075270
 弁理士 小林 泰
 (74) 代理人 100080137
 弁理士 千葉 昭男
 (74) 代理人 100096013
 弁理士 富田 博行
 (74) 代理人 100120112
 弁理士 中西 基晴

最終頁に続く

(54) 【発明の名称】 コンテンツ共有のための一時的ドメイン会員資格付与

(57) 【特許請求の範囲】

【請求項 1】

一時的ドメイン会員資格を許可する方法であって、

計算機が、ドメインの会員でない第1デバイスが一時的に前記ドメインに加入する要求を受け取るステップであって、前記要求が、前記ドメインの会員である第2デバイスによってデジタル署名されており、前記ドメインの会員でないデバイスは、デジタル権利管理 (DRM) により保護された前記ドメインに拘束されたコンテンツを一時的ドメイン証明書なしで消費することが許可されず、DRMにより保護された前記ドメインに拘束されたコンテンツを一時的ドメイン証明書により消費することが許可される、ステップと、

前記計算機が、前記要求が有効であるか否かチェックするステップと、

前記計算機が、前記要求が有効でない場合、前記要求を拒否するステップと、

前記要求が有効である場合、

前記計算機が、前記第1デバイスに前記一時的ドメイン証明書を発生するステップであって、前記一時的ドメイン証明書が、前記第1デバイスが前記ドメインに一時的に加入することを許可する、ステップと、

前記計算機が、前記一時的ドメイン証明書を前記第1デバイスに送るステップと、を含む、方法。

【請求項 2】

請求項1記載の方法において、前記要求が有効であるか否かチェックするステップは、

前記計算機が、前記第1デバイスの証明書が破棄されているか否かチェックするステッ

10

20

プと、

前記計算機が、前記要求にデジタル署名した前記第2デバイスからのデジタル署名を検証するステップと、

前記計算機が、前記第1デバイスの証明書が破棄されておらず、かつ前記デジタル署名が検証された場合、前記要求が有効であると判定するステップと、

前記計算機が、前記第1デバイスの証明書が破棄されていること、および前記デジタル署名が検証されていないこと的一方または双方である場合、前記要求は有効でないと判定するステップと、

を含む、方法。

【請求項3】

請求項1または2に記載の方法において、前記一時的ドメイン証明書は、前記第1デバイスが会員になっている第2ドメインに拘束される、方法。

【請求項4】

請求項1から3のいずれかに記載の方法において、前記一時的ドメイン証明書は、前記第1デバイスに拘束される、方法。

【請求項5】

請求項1から4のいずれかに記載の方法において、前記要求は、前記第1デバイスの公開／秘密鍵対のうち公開鍵を含み、前記方法は、更に、前記計算機が、前記第1デバイスに、該第1デバイスの公開鍵によって暗号化された、前記ドメインの公開／秘密鍵対のうちドメイン秘密鍵を送るステップを含む、方法。

【請求項6】

請求項5記載の方法において、前記第1デバイスの公開／秘密鍵対のうち前記公開鍵は、前記要求に含まれたデジタル証明書に含まれており、前記デジタル証明書は、前記第1デバイスから前記第2デバイスによって受け取られている、方法。

【請求項7】

請求項1から6のいずれかに記載の方法において、前記一時的ドメイン証明書は、前記第1デバイスが前記ドメインに拘束されているコンテンツを消費することができる期間を定めた期限を含む、方法。

【請求項8】

請求項1から7のいずれかに記載の方法において、前記要求を受け取るステップは、前記第1デバイスから前記要求を受け取るステップを含む、方法。

【請求項9】

請求項1から8のいずれかに記載の方法において、前記要求を受け取るステップは、前記第2デバイスから前記要求を受け取るステップを含む、方法。

【請求項10】

請求項1から9のいずれかに記載の方法であって、更に、

前記計算機が、一時的デバイスを前記ドメインに追加することについて、1つ以上の規準をチェックするステップと、

前記計算機が、前記1つ以上の規準が満たされた場合にのみ、前記一時的ドメイン証明書を発生し送るステップと、

を含む、方法。

【請求項11】

請求項10記載の方法において、前記1つ以上の規準は、任意の一時にどれくらい多くの期限切れでない一時的ドメイン証明書を発行することができるのかについての制約を含む、方法。

【請求項12】

複数の命令が格納された1つ以上のコンピューター記憶媒体であって、前記命令は、第1デバイスの1つ以上のプロセッサによって実行されると、該1つ以上のプロセッサに、ドメインの会員でない第2デバイスから、該第2デバイスのデジタル証明書と、デジタル署名付き一時的ドメイン加入要求に対する要求を受け取らせ、

10

20

30

40

50

前記デジタル証明書が破棄されているか否かチェックさせ、

前記第 1 デバイスのユーザーが、前記第 1 デバイスが会員となっている前記ドメインに、前記第 2 デバイスが一時的に加入することを許可することを承認したか否かチェックさせ、前記ドメインの会員でないデバイスは、前記ドメインに加入することなくデジタル権利管理 (D R M) により保護されたドメインに拘束されたコンテンツを消費することが許可されず、前記ドメインに一時的に加入したことに応答して D R M により保護された前記ドメインに拘束されたコンテンツを消費することが許可され、

前記デジタル証明書が破棄されておらず、前記第 1 デバイスのユーザーが、前記第 2 デバイスが前記ドメインに一時的に加入することを許可することを承認した場合、

前記第 2 デバイスの公開鍵を含む一時的ドメイン加入要求を作成させ、デジタル署名させ、 D R M により保護された前記ドメインに拘束された前記コンテンツを一時的に消費することを前記第 2 デバイスに許可させ、

前記デジタル署名した一時的ドメイン加入要求を受け取り側に送らせ、

前記デジタル証明書が破棄されている場合、または前記第 1 デバイスのユーザーが、前記第 2 デバイスが前記ドメインに一時的に加入することを許可することを承認していない場合、前記デジタル署名付き一時的ドメイン加入要求に対する要求を拒否させる、1 つ以上のコンピューター記憶媒体。

【請求項 1 3】

請求項 1 2 記載の 1 つ以上のコンピューター記憶媒体において、前記第 2 デバイスのデジタル証明書は、前記第 2 デバイスが会員となっている第 2 ドメインに特定のデジタル証明書である、1 つ以上のコンピューター記憶媒体。

【請求項 1 4】

請求項 1 2 または 1 3 に記載の 1 つ以上のコンピューター記憶媒体において、前記第 2 デバイスのデジタル証明書は、前記第 2 デバイスに特定のデジタル証明書である、1 つ以上のコンピューター記憶媒体。

【請求項 1 5】

請求項 1 2 から 1 4 のいずれかに記載の 1 つ以上のコンピューター記憶媒体において、前記受け取り側は前記第 2 デバイスを含む、1 つ以上のコンピューター記憶媒体。

【請求項 1 6】

請求項 1 2 から 1 5 のいずれかに記載の 1 つ以上のコンピューター記憶媒体において、前記受け取り側は、前記ドメインを管理するドメイン・コントローラーを含む、1 つ以上のコンピューター記憶媒体。

【請求項 1 7】

複数の命令が格納された 1 つ以上のコンピューター記憶媒体であって、前記命令は、第 1 デバイスの 1 つ以上のプロセッサによって実行されると、該 1 つ以上のプロセッサに、ドメインの会員である第 2 デバイスに対し、前記第 1 デバイスの代わりにデジタル署名した一時的ドメイン加入要求を前記第 2 デバイスが発生するために、前記ドメインの会員でない前記第 1 デバイスのデジタル証明書を送らせ、

前記ドメインを管理するドメイン・コントローラーから、前記第 1 デバイスが一時的に前記ドメインに加入することを許可する一時的ドメイン証明書を受け取らせ、前記ドメインの会員でないデバイスは、デジタル権利管理 (D R M) により保護されたドメインに拘束されたコンテンツを一時的ドメイン証明書なしで消費することが許可されず、 D R M により保護された前記ドメインに拘束されたコンテンツを一時的ドメイン証明書により消費することが許可される、

1 つ以上のコンピューター記憶媒体。

【請求項 1 8】

請求項 1 7 記載の 1 つ以上のコンピューター記憶媒体において、前記命令は、更に、前記 1 つ以上のプロセッサに、

前記第 2 デバイスに前記デジタル証明書を送ったことに応答して、前記第 2 デバイスから、前記デジタル署名付き一時的ドメイン加入要求を受け取らせ、前記デジタル署

10

20

30

40

50

名付き一時的ドメイン加入要求が、前記第 2 デバイスによってデジタル署名されており、

前記デジタル署名付き一時的ドメイン加入要求を前記ドメイン・コントローラーに送らせ、

前記一時的ドメイン証明書は、前記デジタル署名付き一時的ドメイン加入要求に応答して、前記ドメイン・コントローラーから受け取られる、1 つ以上のコンピューター記憶媒体。

【請求項 19】

請求項 18 記載の 1 つ以上のコンピューター記憶媒体において、前記第 1 デバイスのデジタル証明書および前記デジタル署名付き一時的ドメイン加入要求の双方は、前記第 1 デバイスの公開 / 秘密鍵対のうち公開鍵を含み、前記命令は、更に、前記 1 つ以上のプロセッサに、前記ドメインの公開 / 秘密鍵対のうちドメイン秘密鍵を受け取らせ、前記ドメイン秘密鍵は、前記第 1 デバイスの公開 / 秘密鍵対のうち前記公開鍵によって暗号化された、1 つ以上のコンピューター記憶媒体。

【請求項 20】

請求項 17 から 19 のいずれかに記載の 1 つ以上のコンピューター記憶媒体において、前記第 1 デバイスのデジタル証明書は、前記第 1 デバイスが会員になっている第 2 ドメインのデジタル証明書を含み、前記ドメインおよび前記第 2 ドメインは 2 つの異なるドメインである、1 つ以上のコンピューター記憶媒体。

【発明の詳細な説明】

【従来技術】

【0001】

[0001] 携帯用音楽プレーヤーのようなデジタル・メディア再生デバイス、デスクトップおよびラップトップ・コンピューター、ハンドヘルド・コンピューターまたはパーソナル・デジタル・アシスタント (PDA)、セル・フォン等は、増々普及している。これらのデバイスは、アーティストの権利および / またはデジタル・コンテンツの著作権所有者の権利をこれらのデバイス上で保護するために、デジタル権利管理 (DRM) 技法を頻繁に用いている。

【発明の概要】

【発明が解決しようとする課題】

【0002】

しかしながら、これらの DRM 技法を用いると、他のユーザーのデバイスにおいてデジタル・コンテンツを再生するユーザーにできること (ability) が制限されるのが通例である。これが問題であるのは、ユーザーは彼らの書籍、CD、および DVD を彼らの友人に貸与できることに慣れており、これらの DRM 技法が、通例、彼らが購入したデジタル・メディアを彼らの友人に貸与する行為 (ability) を制限するからである。

【課題を解決するための手段】

【0003】

[0002] この摘要は、詳細な説明において以下で更に説明する概念から選択したものを、簡略化した形態で紹介するために設けられている。この摘要は、特許請求する主題の主要な特徴や必須の特徴を特定することを意図するのではなく、特許請求する主題の範囲を限定するために用いられることを意図するのでもない。

【0004】

[0003] コンテンツ共有のための一時的ドメイン会員資格付与の 1 つ以上の形態によれば、第 1 デバイスが一時的にドメインに加入する要求が受け取られ、この要求は、当該ドメインの会員である第 2 デバイスによってデジタル署名されている。この要求が有効であるか否かについてチェックが行われる。この要求が有効でない場合、要求は拒否される。しかしながら、この要求が有効である場合、第 1 デバイスに一時的ドメイン証明書が発生される。この一時的ドメイン証明書は、第 1 デバイスがドメインに一時的に加入することを許可する。一時的ドメイン証明書は、第 1 デバイスに送られる。

【 0 0 0 5 】

【0004】 コンテンツ共有のための一時的ドメイン会員資格付与の1つ以上の形態によれば、第1デバイスにおいて、第2デバイスのデジタル証明書と、デジタル署名付き一時的ドメイン加入要求の要求が、第2デバイスから受信される。デジタル証明書が取り消されたか否かについてチェックが行われ、更に第1デバイスのユーザーが、第2デバイスが、第1デバイスが会員であるドメインに一時的に加入することを許可することを承認したか否かについてチェックが行われる。デジタル証明書が取り消されておらず、第1デバイスのユーザーが、第2デバイスがそのドメインに一時的に加入することを許可することを承認した場合、第2デバイスの公開鍵を含む一時的ドメイン加入要求が作成され、デジタル署名され、このデジタル署名付き一時的ドメイン加入要求が受け取り側に送られる。しかしながら、デジタル署名が取り消されていない場合、または第1デバイスが、第2デバイスがそのドメインに一時的に加入することを許可することを承認していない場合、デジタル署名付き一時的ドメイン加入要求の要求は拒否される。

10

【 0 0 0 6 】

【0005】 コンテンツ共有のための一時的ドメイン会員資格付与の1つ以上の形態によれば、第1デバイスが、第2デバイスが第1デバイスの代わりにデジタル署名付き一時的ドメイン加入要求を発生するために、第1デバイスのデジタル証明書を、第2デバイスに送る。第1デバイスは、第2デバイスが会員であるドメインを管理するドメイン・コントローラーから、第1デバイスがそのドメインに一時的に加入することを許可する一時的ドメイン証明書を受け取る。

20

【図面の簡単な説明】

【 0 0 0 7 】

【0006】 図面全体を通じて、同様の機構を引用する際には同じ番号を用いることとする。

【図1】図1は、1つ以上の実施形態にしたがってコンテンツ共有のための一時的ドメイン会員資格付与を用いることができるシステム例を示す。

【図2】図2は、1つ以上の実施形態にしたがってコンテンツ共有のための一時的ドメイン会員資格付与を実現するシステム例を更に詳細に示す。

【図3】図3は、1つ以上の実施形態による一時的ドメイン証明書の一例を示す。

【図4】図4は、1つ以上の実施形態による、コンテンツ共有のための一時的ドメイン会員資格付与のプロセス例を示すフロー・チャートである。

30

【図5】図5は、1つ以上の実施形態による、コンテンツ共有のための一時的ドメイン会員資格付与の別のプロセス例を示すフロー・チャートである。

【図6】図6は、1つ以上の実施形態による、コンテンツ共有のための一時的ドメイン会員資格付与の別のプロセス例を示すフロー・チャートである。

【図7】図7は、1つ以上の実施形態によるコンテンツ共有のための一時的ドメイン会員資格付与を実現するように構成することができる計算機例を示す。

【発明を実施するための形態】

【 0 0 0 8 】

【0014】 コンテンツ共有のための一時的ドメイン会員資格付与について、以下に論ずる。特定のドメインの会員ではない第1デバイスのために、一時的ドメイン会員資格を要求することができる。その特定のドメインの会員である第2デバイスが、第1デバイスの代わりに、一時的ドメイン加入要求にデジタル署名し、この要求を特定のドメインのドメイン・コントローラーに送る。ドメイン・コントローラーは、第1デバイスに、第1デバイスがその特定のドメインに一時的に加入することを許可する一時的ドメイン証明書を発行する。

40

【 0 0 0 9 】

【0015】 図1は、1つ以上の実施形態にしたがってコンテンツ共有のための一時的ドメイン会員資格付与を用いることができるシステム例100を示す。システム100は、ドメイン・コントローラー102、コンテンツ・プロバイダー104、ライセンス・サーバ

50

ー 1 0 6、1 つ以上 (x) のドメイン 1 0 8 (1)、. . .、1 0 8 (x)、1 つ以上 (y) のデバイス 1 1 0 (1)、. . .、1 1 0 (y)、およびトラスト・オーソリティ (trust authority) 1 2 0 を含む。ドメイン・コントローラー 1 0 2、コンテンツ・プロバイダー 1 0 4、ライセンス・サーバー 1 0 6、およびトラスト・オーソリティ 1 2 0 は 1 つしか示されていないが、複数のコンポーネント 1 0 2、1 0 4、1 0 6、および 1 2 0 をシステム 1 0 0 に含めることができることは認められてしかるべきである。

【 0 0 1 0 】

[0016] ドメイン・コントローラー 1 0 2、コンテンツ・プロバイダー 1 0 4、ライセンス・サーバー 1 0 6、およびトラスト・オーソリティ 1 2 0 の各々は、1 つ以上の計算機において実現することができるサービスを表す。オプションとして、これらのサービスの 2 つ以上を、同じ計算機において実現することができる。加えて、ドメイン・コントローラー 1 0 2、コンテンツ・プロバイダー 1 0 4、ライセンス・サーバー 1 0 6、およびトラスト・オーソリティ 1 2 0 の 1 つ以上を組み合わせることで 1 つのデバイスにすることもでき、または代わりに各々が別個のサービスになることもできる。

【 0 0 1 1 】

[0017] これらのコンポーネント 1 0 2、1 0 4、1 0 6、1 0 8、1 1 0、1 1 6、および 1 2 0 の各々は、ネットワーク 1 1 0 を通じて互いに通信する。ネットワーク 1 1 0 は、インターネット、ローカル・エリア・ネットワーク、セルラまたはその他のワイヤレス電話ネットワーク、その他の公衆および / または企業所有ネットワーク、その組み合わせ等のような種々のネットワークの 1 つ以上を含むことができる。

【 0 0 1 2 】

[0018] 各ドメイン 1 0 8 は、デバイス 1 1 2 (1)、. . .、1 1 2 (a) および 1 1 4 (1)、. . .、1 1 4 (b) として示されている、1 つ以上のデバイスを含む。これらのデバイス 1 1 2、1 1 4 の各々は、1 つのドメインに含まれており、そのドメインの会員であるとも言われる。加えて、1 つ以上のデジタル・メディア・デバイス 1 1 6 (1)、. . .、1 1 6 (y) は、任意のドメイン 1 0 8 の一部でなくてもよい。デバイス 1 1 2、1 1 4、および 1 1 6 は、各々、デスクトップ・コンピューター、ラップトップ・コンピューター、ハンドヘルド・コンピューターまたはパーソナル・デジタル・アシスタント (P D A)、自動車用コンピューター、携帯用音楽プレーヤー、携帯用ムービー・プレーヤー、セルラまたはその他のワイヤレス電話機などのような、種々の異なるタイプのデジタル・メディア・デバイスとすることができる。異なるデバイス 1 1 2、1 1 4、および 1 1 6 は、同じタイプ、または異なるタイプのデジタル・メディア・デバイスであることも可能である。

【 0 0 1 3 】

[0019] デバイス 1 1 2、1 1 4、および 1 1 6 の各々は、デジタル・コンテンツを消費することが可能なデジタル・メディア・デバイスである。本明細書で用いる場合、デジタル・コンテンツとは、オーディオ・コンテンツ (例えば、ソング)、オーディオ / ビデオ・コンテンツ (例えば、テレビジョン・ショー、ムービー、ドキュメンタリー、漫画等)、画像コンテンツ (例えば、デジタル写真)、グラフィクス・コンテンツ、テキスト・コンテンツ (例えば、電子書籍)、コンパイルされたコンピューター・プログラムまたはコンパイルされていないコンピューター・プログラムあるいはその一部、J a v a ゲーム、P K Z I P 圧縮またはその他の圧縮ファイル、電子メール・メッセージおよび添付書類等、ならびにその組み合わせというような、種々の異なるデジタルまたは電子コンテンツのことを言う。デジタル・コンテンツの消費は、デジタル・コンテンツの再生、デジタル・コンテンツの他のデバイスへの転送、デジタル・コンテンツの C D (コンパクト・ディスク) またはその他の光ディスクへの焼き付け、デジタル・コンテンツのハード・コピーの印刷、デジタル・コンテンツの電子メール送信等というような、異なる形態を取ることができる。

【 0 0 1 4 】

[0020] 各ドメイン 1 0 8 は、特定のユーザーまたはユーザーのグループと関連付け

られている。デジタル・コンテンツは、ユーザーのドメインに関連付けられており（拘束されている(bound)とも言う）、そのユーザーのドメインの一部であるデバイス 1 1 2、1 1 4 のうち任意のものが、彼または彼女のドメインに拘束されているデジタル・コンテンツを消費することを許可する。特定のドメイン 1 0 8 における異なるデバイス 1 1 2、1 1 4 は、異なるタイプのデジタル・メディア・デバイスであることができ、または代わりにデバイス 1 1 2、1 1 4 の 1 つ以上が同じタイプのデバイスであることもできる。例えば、ユーザーは、彼または彼女のデスクトップ・コンピューター、携帯用音楽プレーヤー、セル・フォン、および自動車用コンピューターを彼または彼女のドメインの全ての部分に有することができ、これらのデバイスの全ては、彼または彼女のドメインに拘束されているデジタル・コンテンツを消費することができる。個々のデバイス 1 1 2、1 1 4 は、1 つ以上のドメイン 1 0 8 の会員となることができる。更に、ドメイン 1 0 8 内にあるデバイス 1 1 2、1 1 4 は、その同じドメイン内にある他のデバイス 1 1 2、1 1 4 を意識する必要はないことは、記してしかるべきである。

10

【 0 0 1 5 】

[0021] ドメインの一部ではないデバイス 1 1 6 では、デジタル・コンテンツがその特定のデバイス 1 1 6 と関連付けられている（または拘束されている）。また、デバイス 1 1 6 は、デバイス 1 1 6 に拘束されているデジタル・コンテンツも消費することができる。

【 0 0 1 6 】

[0022] ドメイン・コントローラー 1 0 2 は、ドメイン 1 0 8 を管理する。ドメインの管理とは、当該ドメインにおける会員資格を制御し、ドメインの会員に対して制約を賦課することを指し、デバイスをドメインに追加し、デバイスをドメインから除外し、ドメイン会員資格証明書を発生および配布し、一時的ドメイン証明書を発生および配布する等を含む。デバイス 1 1 2、1 1 4 がドメインに加入すると、デバイス 1 1 2、1 1 4 には、ドメイン・コントローラー 1 0 2 から、そのドメインに対するドメイン会員資格証明書が与えられる。このドメイン会員資格証明書は、コンテンツ・ライセンスと共に、そのドメインに拘束されている保護対象コンテンツを消費することを、そのデバイスに許可する。これについては、以下で更に詳しく説明する。また、デバイス 1 1 2、1 1 4、および/または 1 1 6 は、一時的にドメインに加入することもでき、その場合、デバイス 1 1 2、1 1 4、1 1 6 には、ドメイン・コントローラー 1 0 2 から、そのドメインに対する一時的ドメイン証明書が与えられる。この一時的ドメイン証明書は、コンテンツ・ライセンスと共に、そのドメインに拘束されているコンテンツを一時的に消費することを、そのデバイスに許可する。これについては、以下で更に詳しく説明する。

20

30

【 0 0 1 7 】

[0023] コンテンツ・プロバイダー 1 0 4 は、コンテンツをデバイス 1 1 2、1 1 4、および 1 1 6 に供給する。デバイス 1 1 2、1 1 4、および 1 1 6 に供給されるコンテンツは、通例、保護対象コンテンツである。保護対象コンテンツは、暗号化によって保護されており、その保護対象コンテンツと関連付けられたコンテンツ・ライセンスの中に解読鍵が含まれている。各コンテンツ・ライセンスは、特定のドメイン 1 0 8 または特定のデバイス 1 1 6 に拘束されているので、コンテンツ・ライセンスが拘束されている特定のドメイン 1 0 8 の一部であるデバイスのみ、またはコンテンツ・ライセンスが拘束されている特定のデバイスが、コンテンツを消費することができる。これについては、以下で更に詳しく論ずる。

40

【 0 0 1 8 】

[0024] ライセンス・サーバー 1 0 6 は、コンテンツ・ライセンスをデバイス 1 1 2、1 1 4、および 1 1 6 に提供する。デバイス 1 1 2、1 1 4、および 1 1 6 がコンテンツ・プロバイダー 1 0 4 から入手するコンテンツは、保護されている。デバイス 1 1 2、1 1 4、および 1 1 6 は、保護対象コンテンツのコンテンツ・ライセンスを得るために、ライセンス・サーバー 1 0 6 にアクセスする。コンテンツ・ライセンスは、特定のドメインまたはデバイスに拘束することができる。

50

【 0 0 1 9 】

[0025] トラスト・オーソリティ 1 2 0 は、デジタル署名を行い、デジタル証明書を発行する。トラスト・オーソリティ 1 2 0 は、ドメイン・コントローラー 1 0 2、コンテンツ・プロバイダー 1 0 4、およびライセンス・サーバー 1 0 6 によって信頼されているエンティティであり、通例、1 つ以上の計算機において実現されるサービスである。トラスト・オーソリティ 1 2 0 は、信頼のおける第三者として行動し、デバイス 1 1 2、1 1 4、1 1 6 が真正であることを認証するデジタル証明書をデバイス 1 1 2、1 1 4、1 1 6 に発行することができる。また、トラスト・オーソリティ 1 2 0 は、別のエンティティ（デバイス製造業者のような）がこのようなデジタル証明書をデバイス 1 1 2、1 1 4、1 1 6 に発行することを許可する証明書も発行することができ、これによってデジタル証明書の発行をこの他のエンティティに委任する。

10

【 0 0 2 0 】

[0026] ここで、対称鍵暗号、公開鍵暗号、および公開 / 秘密鍵対について説明する。このような鍵暗号は、当業者には周知であるが、本明細書では読者を補助するために、このような暗号の端的な全体像が含まれる。公開鍵暗号では、エンティティ（ハードウェアまたはソフトウェア・コンポーネント、デバイス、ドメイン等）には、公開 / 秘密鍵対が関連付けられている。公開鍵は公に入手可能にすることができるが、エンティティは秘密鍵を秘密にしておく。秘密鍵がないと、公開鍵を用いて暗号化されているデータを解読するのは、計算的に非常に困難である。したがって、データは、公開鍵を用いてあらゆるエンティティによって暗号化することができるが、対応する秘密鍵を有するエンティティでなければ解読することはできない。加えて、データおよび秘密鍵を用いることによって、そのデータのデジタル署名を発生することができる。秘密鍵がないと、公開鍵を用いて検証することができる署名を作成するのは、計算的に非常に困難である。公開鍵を有する任意のエンティティは、公開鍵を用いて得られた検証値を元のデータと比較することによって、公開鍵を用いてデジタル署名を検証することができ、これら 2 つが同一である場合、デジタル署名されたデータを改竄したり、あるいは変更した者がいないことが保証される。

20

【 0 0 2 1 】

[0027] 一方、対称鍵暗号では、2 つのエンティティによって共有鍵が知られており、秘密に保たれている。この共有鍵を有する任意のエンティティは、通例、その共有鍵によって暗号化されたデータを解読することができる。共有鍵がないと、この共有鍵を用いて暗号化されたデータを解読するのは計算的に非常に困難である。したがって、2 つのエンティティ双方が共有鍵を知っている場合、各々はデータを暗号化することができ、このデータは他方によって解読することができるが、他のエンティティは、共有鍵を知らない場合、これら他のエンティティはデータを解読することはできない。

30

【 0 0 2 2 】

[0028] また、デジタル証明書についてもここで説明する。デジタル証明書は、当業者には周知である。しかしながら、本明細書では読者を補助するために、デジタル証明書の端的な全体像が含まれる。デジタル証明書は、特定のエンティティが信頼できることを証明するトラスト・オーソリティによって発生することができる。デジタル証明書は、通例、当該デジタル証明書を発生しようとしている特定のエンティティの公開鍵を含み、デジタル証明書はトラスト・オーソリティによって、当該トラスト・オーソリティの秘密鍵を用いてデジタル署名される。エンティティ A がエンティティ B の信頼性を検証することを望む場合、エンティティ A は、トラスト・オーソリティ（実施形態によっては、エンティティ A であることができる）の公開鍵を入手し、エンティティ B のデジタル証明書のデジタル署名を検証することができる。トラスト・オーソリティがエンティティ A によって信頼されているので、エンティティ B のデジタル証明書のデジタル署名が正しいと検証されれば、エンティティ B を信頼されたものとして検証することができる。

40

【 0 0 2 3 】

50

[0029] 一般に、システム 100 の動作中、デバイスは、ドメイン・コントローラー 102 と通信して、特定のドメイン 108 に加入することができる。特定のドメイン 108 に加入するとき、ドメイン・コントローラー 102 はそのデバイスに、そのドメイン 108 に拘束されたコンテンツを消費できる機能(ability)を与える。このドメイン 108 の中にあるデバイスは、暗号化されたコンテンツをコンテンツ・プロバイダー 104 またはそのドメイン 108 内部にある他のデバイス 112 (または 114) から入手することができる。このコンテンツに対応するライセンスをライセンス・サーバー 106 から入手することができる。このライセンスは、特定のドメイン 108 に拘束され、通例、暗号化されたコンテンツを解読するためのコンテンツ鍵を含む。この特定のドメイン 108 の会員であるデバイスは、その特定のドメイン 108 に拘束されたライセンスからコンテンツ鍵を解読し、次いでこのコンテンツ鍵を用いて、暗号化されたコンテンツを解読することができる。次に、このようなデバイスは、ライセンスに含まれる方針にしたがって、コンテンツを消費することができる。この特定のドメイン 108 に拘束されていないデバイスは、その特定のドメイン 108 に拘束されたライセンスからコンテンツ鍵を解読することができず、したがって暗号化されたコンテンツを解読することができない。

【0024】

[0030] しかしながら、ある種の実施形態の下では、その特定のドメイン 108 の会員ではないデバイスが、その特定のドメイン 108 に対する一時的なドメイン会員資格を得ることができる。特定のドメイン 108 に対する一時的なドメイン会員資格を得るためには、その特定のドメイン 108 の会員が、当該デバイスの代わりに一時的ドメイン加入要求にデジタル署名する。この一時的ドメイン加入要求は、当該デバイスのデジタル証明書を含む。ドメイン・コントローラー 102 は、この一時的ドメイン加入要求を受け取り、一時的ドメイン会員資格を発行するか否かを判定する。ドメイン・コントローラー 102 が一時的ドメイン会員資格を発行すると決定した状況では、ドメイン・コントローラー 102 は一時的ドメイン証明書をそのデバイスのために発行する。この一時的ドメイン証明書は、そのデバイスが一時的に特定のドメイン 108 に加入することを許可し、このデバイスは、当該ドメインの会員であるかのように、特定のドメイン 108 に拘束されたコンテンツを一時的に消費することが許可される。しかしながら、このコンテンツの消費は、コンテンツおよび/またはその他の制約(例えば、一時的ドメイン証明書に含まれる制約)に対応するライセンスに基づいて制限される可能性がある。このような制約には、通例、一時的ドメイン会員資格が有効な時間量が含まれ、この時間量は、正規の(non-temporary)ドメイン会員よりも短いのが通例である。

【0025】

[0031] 図 2 は、1 つ以上の実施形態にしたがって、コンテンツ共有のための一時的ドメイン会員資格付与を実現する、更に詳細なシステム例 200 を示す。図 2 は、ドメイン・コントローラー 202、デバイス 204、およびドメイン 206 を示す。これらは、それぞれ、図 1 のドメイン・コントローラー 102、デバイス 116、およびドメイン 108 とすることができる。これらのコンポーネント 202、204、および 206 間の通信は、図 1 のネットワーク 110 のようなネットワークを通じて行うことができる。

【0026】

[0032] ドメイン 206 は、会員デバイス 208 を有するように示されている。説明を容易にするために、1 つのデバイス 208 がドメイン 206 の会員であるように示されているが、ドメイン 206 は 2 つ以上のデバイス 208 を含むことができることは認められてしかるべきである。デバイス 208 は、デジタル権利管理(DRM)モジュール 210、コンテンツ・消費モジュール 212、コンテンツ・ライセンス・ストア 214、ドメイン証明書ストア 216、およびデバイス・コンテンツ・ストア 218 を含む。別個に示されているが、代わりに、モジュール 210、モジュール 212、ストア 214、ストア 216、およびストア 218 の 1 つ以上を組み合わせることもできる。

【0027】

[0033] DRM モジュール 210 は、デバイス 208 のためにデジタル権利管理技法

を実施する。デジタル権利管理とは、アーティスト、出版社、および/またはデジタル・コンテンツの著作権所有者の権利保護のことを指す。コンテンツ・ライセンスおよび/またはドメインまたはデバイスの証明書に含まれるコンテンツ使用に対する制限は、DRMモジュール210によって執行(enforce)される。一般に、DRMは、コンテンツの消費を制限するために、条件付きアクセス、コピー保護、コンテンツ保護等のような、種々の技法を用いることができる。これらの技法を実施する具体的な形態は、DRMシステムによって様々に変更することができる。

【0028】

[0034] デジタル・コンテンツは、通例、暗号化されることによって保護されており、適正な解読鍵(1つまたは複数)を知っている場合にのみコンテンツを明瞭に(intelligible)再生できるようにしている。DRMモジュール210は、コンテンツを解読することが許されるときを判定するために、種々のDRM技法を用いることができ、これらのDRM技法は種々の異なる形態で実施することができる。例えば、DRM技法は、デバイス208において実行しているオペレーティング・システムおよび/またはその他のソフトウェアが信頼できることの検証、コンテンツの著作権の所有者および/またはコンテンツの配信業者によって指図された制約が満たされていることの検証、ドメイン会員証明書が有効である(例えば、期限切れでない)ことの検証等を含むことができる。種々の異なるDRM技法が当業者には知られており、このような技法のうち任意のものをDRMモジュール210によって用いることができる。

【0029】

[0035] デバイス・コンテンツ・ストア218は、図1のコンテンツ・プロバイダー104のような、コンテンツ・プロバイダーから得られるコンテンツを格納する。コンテンツ・プロバイダーは、通例、リモート・デバイスまたはサービスであり、ここから保護(例えば、暗号化された)対象コンテンツを入手することができる。あるいは、コンテンツ・プロバイダーは、他のローカル・デバイス(例えば、図1の他のデバイス112、114、または116)、ローカル・メディア・デバイス(例えば、コンパクト・ディスク(CD)またはデジタル・バーサタイル・ディスク(DVD))等とすることができる。デバイス・コンテンツ・ストア218は、通例、デバイス208の一部として実装されるが、デバイス・コンテンツ・ストア218の全部または一部を、代わりに、別個のデバイスに実装することもできる。加えて、デバイス・コンテンツ・ストア218は、少なくとも部分的に、フラッシュ・メモリー・カード、携帯用ハード・ドライブ等のような、リムーバブル媒体上に実装することができる。

【0030】

[0036] コンテンツ・ライセンス・ストア214は、コンテンツ・ストア214の中にある保護対象コンテンツに対応するコンテンツ・ライセンスを格納する。ライセンスは、図1のライセンス・サーバー106のようなライセンス・サーバーから、あるいは代わりに別のサーバーまたはデバイス(例えば、図1のデバイス112、114、または116)から入手することができる。コンテンツ・ライセンスは、ドメイン206の会員のみがコンテンツを解読することを許可することによって、特定のコンテンツをドメイン206に拘束する。1つ以上の実施形態では、この拘束を遂行するには、コンテンツのコンテンツ鍵(例えば、対称鍵)をドメイン206の公開鍵を用いて暗号化し、この暗号化したコンテンツ鍵をライセンスに含ませる。ドメイン206の会員はドメイン206の秘密鍵の知識を有するので、これらの会員はコンテンツ鍵を解読することができ、したがってコンテンツも解読することができる。あるいは、この拘束は、ドメイン206の対称鍵を用いてコンテンツ鍵を暗号化する、デバイス208の公開鍵を用いてコンテンツ鍵を暗号化する等のように、別の形態で遂行することもできる。

【0031】

[0037] ドメイン証明書ストア216は、デバイス208にこれまでに発行されたドメイン証明書を格納する。ドメイン証明書によって、デバイス208はコンテンツ・ライセンスの中にある情報にアクセスし、コンテンツ・ライセンスからしかるべき情報を引き出

10

20

30

40

50

して、デバイス 208 が関連するコンテンツを消費することを可能にすることができる。ストア 216 におけるドメイン証明書は、例えば、デバイス 208 の公開鍵を用いて暗号化されたドメイン 206 の秘密鍵、またはデバイス 208 の公開鍵を用いて暗号化された別のドメイン（デバイス 208 が一時的会員となっている）の秘密鍵を含む。デバイス 208 はデバイス 208 の秘密鍵の知識を有するので、デバイス 208 は証明書においてドメイン 206 の秘密鍵を解読することができる。あるいは、このドメイン鍵は対称鍵であることも可能である。

【0032】

[0038] また、デバイス 208 はコンテンツ消費モジュール 212 も含む。コンテンツ消費モジュール 212 は、DRMモジュール 210 にしたがって、デバイス 208 にあるデジタル・コンテンツにアクセスしてこれを消費する。コンテンツ消費モジュール 212 は、デジタル・コンテンツの再生、デジタル・コンテンツの他のデバイスへの転送、デジタル・コンテンツのCDまたは他の光ディスクへの焼き付け、デジタル・コンテンツのハード・コピーの印刷、デジタル・コンテンツの電子メール送信等というような、種々の異なる種類のデジタル・コンテンツ消費に備えることができる。コンテンツ消費モジュール 212 は、図示のように別個のモジュールとすることができ、または代わりに別のモジュール（DRMモジュール 210 のような）に組み込むこともできる。

【0033】

[0039] 尚、デバイス 208 によって入手されたコンテンツの一部は保護対称コンテンツでなくてもよいことは記してしかるべきである。例えば、無料配信コンテンツをデバイス 208 によって入手することができ、コンテンツをデバイス 208 からCDに全く保護なくコピーすることもできる等である。このような非保護対称コンテンツをどのように扱うかは、コンテンツ消費モジュール 212 によって決定されるのであり、DRMモジュール 210 が関与する必要はない。

【0034】

[0040] デバイス 204 は、ドメイン 206 の会員ではないものとして示されている。デバイス 204 は、いずれのドメインの会員でもない別個のデバイスとすることができ、または代わりに1つ以上のドメイン（ドメイン 206 以外）の会員とすることもできる。デバイス 204 は、デバイス 208 のDRMモジュール 210 と同様に動作するDRMモジュール 220 と、デバイス 208 のコンテンツ消費モジュール 212 と同様に動作するコンテンツ消費モジュール 222 とを含む。同様に、デバイス 204 は、デバイス 208 のコンテンツ・ライセンス・ストア 214 と同様に動作するコンテンツ・ライセンス・ストア 224 と、デバイス 208 のドメイン証明書ストア 216 と同様に動作するドメイン証明書ストア 226 と、デバイス 208 のデバイス・コンテンツ・ストア 218 と同様に動作するデバイス・コンテンツ・ストア 228 とを含む。

【0035】

[0041] ドメイン・コントローラー 102 は、ドメイン要求モジュール 232、デバイス拘束暗号化モジュール 234、およびドメイン情報ストア 236 を含む。モジュール 232、モジュール 234、およびストア 236 は、同じデバイスに実装することができ、または代わりに複数のデバイスに実装することもできる。

【0036】

[0042] ドメイン要求モジュール 232 は、ドメイン 206 を管理し、どのデバイスがドメイン 206 に加入することを許可されるか制御する。この管理は、デバイスが一時的にドメイン 206 に加入できるか否かを制御することを含む。ドメイン要求モジュール 232 は、種々の異なる規準に基づいてデバイスがドメイン 206 に加入することを許可すること、またはデバイスがドメイン 206 に加入するのを禁止することができる。このような規準の例には、どれくらいのデバイスがドメイン 206 に加入することができるかについての制約、どのタイプのデバイス（例えば、デバイスにおけるDRMモジュール 210）がドメイン 206 に加入することができるかについての制約、ドメイン 206 に加入するためにデバイスのユーザーによって供給されるはずのユーザー信任状(user credenti

10

20

30

40

50

al)等が含まれる。ドメイン要求モジュール232は、どれくらいのデバイスがドメイン206に加入することができるかについての制約、どのタイプのデバイス(例えば、デバイスにおけるDRMモジュール210)がドメイン206に加入することができるかについての制約、デバイスのデジタル証明書がドメイン206の会員によってデジタル署名されているか否か等というような、1つ以上の同じまたは異なる規準に基づいて、デバイスがドメイン206に一時的に加入することを許可することができる。

【0037】

[0043] ドメイン情報ストア236は、ドメイン・コントローラ202によって管理されている種々のドメインに関する情報を格納する。このドメイン情報は、どれくらいのデバイスがドメインの一部となることができるかについての限度を記述する情報、どれくらい頻繁にユーザーはデバイスをドメインに追加することができるかについての限度を記述する情報等のような、デバイスがドメイン206に加入することを許可するか否か判定する(一時的または永続的に関係なく)際に、ドメイン要求モジュール232によって用いられる情報を含むことができる。また、このドメイン情報は、ドメイン206の会員であるデバイス毎のデバイスID、ドメイン206と関連のある権利、ドメイン206の公開/秘密鍵対、ドメイン206の会員であるデバイスの公開鍵等も含むことができる。

【0038】

[0044] デバイス拘束暗号化モジュール234は、ライセンスを拘束するドメイン証明書(つまり、先に論じたように、コンテンツ)をドメイン206に対して発生する。ドメイン証明書は、異なる形態で、ライセンスをドメイン206に拘束することができる。1つ以上の実施形態では、この拘束を遂行するには、デバイス208の公開鍵を用いて暗号化された少なくとも一部(例えば、ドメイン206の秘密鍵)を含むドメイン証明書を発生する。あるいは、この拘束は、鍵を用いて暗号化された少なくとも一部(例えば、ドメイン206の秘密鍵)を含むドメイン証明書を発生し、ドメインの中にあるデバイスにこの鍵を安全に発行することによって、安全鍵交換プロトコルを用いてドメイン・コントローラ202とドメイン206の中にあるデバイスとの間で対称鍵を確立し、この対称鍵を用いて暗号化された少なくとも一部(例えば、ドメイン206の秘密鍵)を含むドメイン証明書を発行することによって等というように、他の形態でも遂行することができる。

【0039】

[0045] 一時的ドメイン会員は、ユーザーが一時的に彼または彼女のドメインにデバイスを加入させたい多くの異なる場面において有用である。例えば、ユーザーが友人の家を訪問しており、彼らがこのユーザーの携帯用デバイスにおいてムービーを見ることを望んでいると判定する場合があり得る。友人は、ムービー再生デバイスを有するが、このデバイスは、ユーザーの携帯用デバイスと同じドメインの会員ではない。したがって、本明細書において論じているコンテンツ共有のために一時的ドメイン会員を用いて、友人のデバイスに一時的ドメイン証明書を与えることができ、ユーザーのドメインにおいてユーザーの友人のデバイスに一時的会員資格を与えることができる。ユーザーの携帯用デバイスからのコンテンツは、友人のデバイスによって再生することができ、これによってユーザーはコンテンツを彼または彼女の友人と共有することが可能になる。

【0040】

[0046] システム200において、デバイス204はドメイン206の会員ではないが、デバイス204に一時的ドメイン証明書を与えて、デバイス204がドメイン206に一時的に加入することを許可することができる。この一時的ドメイン証明書を入手するために、デバイス204はデバイス204のデジタル証明書250を、デバイス208のような、ドメイン206の中にあるデバイスに送る。デバイス204のデジタル証明書250は、デバイス204に特定のデジタル証明書、またはデバイス204が会員となっている他のドメイン(ドメイン206以外)に特定のデジタル証明書とすることができる。

【0041】

[0047] デジタル証明書250の送付は、デバイス204によって、または代わりに

10

20

30

40

50

デバイス 208 によって開始することができる。例えば、デバイス 204 は、一時的にドメイン 206 に加入することをデバイス 204 に許可することを要求することができ、またはデバイス 208 が、一時的にドメイン 206 に加入することをデバイス 204 に許可することを要求することもできる。このような要求は、デバイス 204 またはデバイス 208 の一方のユーザーによって開始することができ、あるいは代わりにデバイス 204 または 208 の一方のモジュールまたはコンポーネントによって自動的に発生することもできる。

【0042】

[0048] デジタル証明書 250 を受け取ると、DRM モジュール 210 は、デバイス 204 の代わりに一時的ドメイン加入要求を発生するか否か判定する。この一時的ドメイン加入要求を発生するか否か判定する際には、種々の異なる規準を用いることができる。1 つ以上の実施形態では、DRM モジュール 210 は、デジタル証明書 250 が有効であるか否かチェックする。このような実施形態では、デバイス 208 は、破棄されたデジタル証明書のリストまたはその他の記録を維持するか、またはアクセスすることができる。DRM モジュール 210 は、デジタル証明書 250 がこのリスト上にあり、つまり破棄されているか否かチェックする。デジタル証明書 250 が破棄されている場合、DRM モジュール 210 は一時的ドメイン要求を発行しない。それ以外の場合、DRM モジュール 210 は一時的ドメイン要求を発行することができる（オプションとして、満たされている他の規準に従う）。

【0043】

[0049] 1 つ以上の他の実施形態では、DRM モジュール 210 は、デバイス 208 のユーザーがデバイス 204 が一時的にドメイン 206 に加入することを承認したか否かチェックする。このチェックは、デジタル証明書 250 が有効であるか否かのチェックに加えて、またはその代わりに行うことができる。このデバイス 208 のユーザーがデバイス 204 が一時的にドメイン 206 に加入することを承認したか否かのチェックは、デバイス 208 のユーザー・インターフェース（UI）上にプロンプトを表示して、ユーザーにデバイス 204 が一時的にドメイン 206 に加入することの承認または拒否を入力するように要求するというような、異なる形態で行うこともできる。あるいは、このチェックは、ユーザーが予めデバイス 208 について 1 つ以上の好みまたは選択肢を設定しておく、ドメイン 206 に一時的に加入することを承認する 1 つ以上の他のデバイス（またはユーザー）を特定しておくというような、別の形態でも行うことができる。他の代案では、デバイス 208 のユーザーが、デバイス 204 にデジタル証明書 250 を要求することによって、デバイス 204 が一時的にドメイン 206 に加入することを元々から承認しておく。

【0044】

[0050] DRM モジュール 210 が、デバイス 204 の代わりに一時的ドメイン加入要求を発生しないと決定した場合、一時的ドメイン加入要求は発生されず、オプションとしてデバイス 204 にはこの決定が通知される。しかしながら、DRM モジュール 210 が、デバイス 204 の代わりに一時的ドメイン加入要求を発生すると決定した場合、DRM モジュール 210 は、デジタル証明書 250 を含む一時的ドメイン加入要求を発生する。また、DRM モジュール 210 は、この一時的ドメイン加入要求にデジタル署名して、ドメイン・コントローラー 202 が、ドメイン 206 の会員によって要求が発生されたことを検証することを可能にする。これについては、以下で更に詳しく論ずる。DRM モジュール 210 は、一時的ドメイン加入要求全体にデジタル署名することができ、または代わりにこの要求の一部のみ（例えば、少なくともデジタル証明書 250）にデジタル署名することもできる。DRM モジュール 210 は、デバイス 208 の秘密鍵、DRM モジュール 210 の秘密鍵、ドメイン 206 の秘密鍵等というような、秘密鍵を用いて、一時的ドメイン加入要求（またはその一部）にデジタル署名することができる。

【0045】

[0051] あるいは、デジタル署名付き一時的ドメイン加入要求には、デジタル証明

書 250 の一部だけが含まれる。例えば、デバイス 204 の公開鍵（デバイス 204 に特定の公開鍵、またはデバイス 204 が会員となっているドメインに特定の公開鍵というような公開鍵）をデジタル証明書 250 から抽出して、デジタル署名付き一時的ドメイン加入要求に含ませ、デジタル証明書 250 の残りの部分を用いないことも可能である。あるいは、他の鍵またはメカニズムをデバイス 204（またはデバイス 204 が会員となっているドメイン）と関連付け、証明書をデバイス 204（またはデバイス 204 が会員となっているドメイン）に拘束するために用いることができる。これらの鍵またはメカニズムは、デジタル証明書 250 の代わりに、デジタル署名付き一時的ドメイン加入要求に含めることができる。

【0046】

10

【0052】 1つ以上の実施形態では、デジタル署名付き一時的ドメイン加入要求は、一時的ドメイン加入要求 252 となる。要求 252 はデバイス 204 に返送され、次いで、デバイス 204 はこの要求をドメイン・コントローラー 202 に一時的ドメイン加入要求 254 として送る。1つ以上の他の実施形態では、デジタル署名付き一時的ドメイン加入要求は、一時的ドメイン加入要求 260 となり、DRMモジュール 210 はこの要求をドメイン・コントローラー 202 に送る。つまり、デジタル署名付き一時的ドメイン加入要求は、デバイス 204 を経由して、デバイス 208 から直接等というように、異なる形態でドメイン・コントローラー 202 に伝達することができる。

【0047】

【0053】 ドメイン・コントローラー 202 は、要求 254 または要求 260 のような、一時的ドメイン加入要求を受け取り、ドメイン要求モジュール 232 は、この要求にตอบสนองして、一時的ドメイン証明書 256 を発行するか否かを判定する。ドメイン要求モジュール 232 は、どれくらい多くのデバイスが一時的にドメイン 206 に加入することができるかに対する制約、どのタイプのデバイス（例えば、デバイスにおける DRMモジュール 220）が一時的にドメイン 206 に加入することができるか等というような、1つ以上の異なる規準に基づいて、一時的ドメイン証明書 256 を発行するか否かを判定することができる。これらの制約は、例えば、ドメイン・コントローラー 202 の監督者(administrator)またはその他のユーザーによって確立され、ドメイン情報ストア 236 に維持することができる。

20

【0048】

30

【0054】 1つ以上の実施形態では、ドメイン・コントローラー 202 は、いつでも一度にしきい値数以下の有効な(non-expired)一時的ドメイン証明書を発行することを許可することに制限される。これに応じて、しきい値数の有効一時的ドメイン証明書が発行された後に受け取られた一時的ドメイン加入要求は、ドメイン要求モジュール 232 によって拒否される。一旦発行されている一時的ドメイン証明書の1つ以上が期限切れとなったなら、一時的ドメイン加入要求は、その規準ではもはや拒否されなくなる。

【0049】

【0055】 1つ以上の実施形態では、一時的ドメイン会員が要求されているドメインは、一時的ドメイン加入要求にデジタル署名したデバイスが会員となっているドメインである。このドメインの会員は、例えば、一時的ドメイン加入要求に含まれるデータによって、ドメイン情報ストア 236 の中にあるデータによって等で、特定することができる。

40

【0050】

【0056】 一時的ドメイン加入要求が、一時的ドメイン会員が要求されているドメインを特定する実施形態では、ドメイン要求モジュール 232 は、一時的ドメイン加入要求、または一時的ドメイン加入要求に含まれる少なくともデジタル証明書 250 が、要求されたドメインの会員によってデジタル署名されているか否かをチェックする。デジタル署名には、通例、デジタル証明書またはデジタル署名を発生したエンティティを特定する他のデータが関連する。ドメイン 206 の会員の識別子がドメイン情報ストア 236 に維持されているので、ドメイン 206 の会員によってデジタル署名されている要求は、容易に確認することができる。

50

【 0 0 5 1 】

[0057] デジタル署名を検証することができない場合（またはドメイン 2 0 6 の会員でないデバイスによってデジタル署名が発生された場合）、ドメイン要求モジュール 2 3 2 は一時的ドメイン加入要求を拒否し、一時的ドメイン証明書 2 5 6 を発生しない。この拒否の指示は、オプションとして、一時的ドメイン加入要求の発生源に戻ることができる。しかしながら、デジタル署名が検証され、ドメイン 2 0 6 の会員であるデバイスによって発生されたものである場合、ドメイン要求モジュール 2 3 2 は一時的ドメイン証明書 2 5 6（オプションとして、満たされている他の規準に従う）を発生する。

【 0 0 5 2 】

[0058] 加えて、1つ以上の実施形態では、ドメイン要求モジュール 2 3 2 は、受け取られた一時的ドメイン加入要求に含まれているデジタル署名 2 5 0 が有効であるか否かチェックする。このチェックは、先に論じたような、DRMモジュール 2 1 0 によって行われるチェックに加えて、またはその代わりに行うことができる。このような実施形態では、ドメイン・コントローラ 2 0 2 は、破棄されたデジタル証明書のリストまたはその他の記録を維持するか、あるいはそれにアクセスすることができる。ドメイン要求モジュール 2 3 2 は、デジタル証明書 2 5 0 がこのリスト上にあり、したがって破棄されているか否かチェックする。デジタル証明書 2 5 0 が破棄されている場合、ドメイン要求モジュール 2 3 2 は一時的ドメイン加入要求を拒否する。それ以外の場合、ドメイン要求モジュール 2 3 2 は（オプションとして、満たされている他の規準にしたがって）一時的ドメイン証明書 2 5 6 を発生する。

【 0 0 5 3 】

[0059] ドメイン要求モジュール 2 3 2 が、一時的ドメイン加入要求に応答して、一時的ドメイン証明書 2 5 6 を発行すると決定した場合、デバイス拘束暗号化モジュール 2 3 4 は一時的ドメイン証明書 2 5 6 を発生する。デバイス拘束暗号化モジュール 2 3 4 は、一時的ドメイン証明書 2 5 6 をデバイス 2 0 4 に拘束するか、または代わりに、デバイス 2 0 4 が会員となっているドメインに拘束する。先に論じたように、デバイス 2 0 8 によって発生されデジタル署名付き一時的ドメイン加入要求は、デバイス 2 0 4 の公開鍵、あるいはデバイス 2 0 4（またはデバイス 2 0 4 が会員となっているドメイン）と関連のあるその他の鍵またはメカニズムを含む。デジタル署名付き一時的ドメイン加入要求に含まれる鍵またはその他のメカニズムは、一時的ドメイン証明書 2 5 6 をデバイス 2 0 4（またはデバイス 2 0 4 が会員となっているドメイン）に拘束するために、デバイス拘束暗号化モジュール 2 3 4 によって用いられる。

【 0 0 5 4 】

[0060] 1つ以上の実施形態では、暗号化モジュール 2 3 4 が、ドメイン・コントローラ 2 0 2 によって受け取られた一時的ドメイン加入要求に含まれているデジタル証明書 2 5 0 を用いて、一時的ドメイン証明書 2 5 6 をデバイスおよび/またはドメインに拘束する。ドメイン・コントローラ 2 0 2 によって受け取られた一時的ドメイン加入要求に含まれているデジタル証明書 2 5 0 は、デバイス 2 0 4 の公開鍵（デバイス 2 0 4 またはデバイス 2 0 4 が会員となっているドメインに特定の公開鍵）を含む。一時的ドメイン証明書 2 5 6 は、ドメイン 2 0 6 の秘密鍵を含み、少なくともドメイン 2 0 6 のこの秘密鍵は、デバイス 2 0 4 の公開鍵を用いて暗号化されている。また、一時的ドメイン証明書 2 5 6 の追加部分も、デバイス 2 0 4 の公開鍵を用いて、暗号化することができる。

【 0 0 5 5 】

[0061] デバイス 2 0 4 は、一時的ドメイン証明書 2 5 6 を受け取り、一時的ドメイン証明書 2 5 6 をドメイン証明書ストア 2 2 6 に格納する。一時的ドメイン証明書 2 5 6 はデバイス 2 0 4（または、デバイス 2 0 4 が会員となっているドメイン）に拘束されており、これによって、デバイス 2 0 4 がデバイス 2 0 4 の秘密鍵（例えば、デバイス 2 0 4 に特定の秘密鍵、またはデバイス 2 0 4 が会員となっているドメインに特定の秘密鍵）を用いて、ドメイン 2 0 6 の秘密鍵を解読すること、つまりドメイン 2 0 6 に拘束されたコンテンツを消費することを許可する。

【 0 0 5 6 】

[0062] あるいは、ドメイン・コントローラー 202 は、秘密鍵を一時的ドメイン証明書 256 に含ませる以外の他の形態で、デバイス 206 の秘密鍵をデバイス 204 に伝達することができる。一例として、ドメイン 206 の秘密鍵をデバイス 204 (またはデバイス 204 が会員となっているドメイン) に拘束し、一時的ドメイン証明書 256 とは別個にデバイス 204 に送ることができる。この拘束は、種々の異なる形態で、デバイス 204 (またはデバイス 204 が会員となっているドメイン) の公開鍵を用いてドメイン 206 の秘密鍵を暗号化する、安全鍵交換プロトコルを用いてコントローラー 202 とデバイス 204 との間で対称鍵を確立し、この対称鍵を用いてドメイン 206 の秘密鍵を暗号化する等によって、行うことができる。

10

【 0 0 5 7 】

[0063] 1つ以上の実施形態では、本明細書において論じているコンテンツ共有のための一時的ドメイン会員は、デバイス 204 とデバイス 208 との間における近接度に何の制約も付けない。例えば、デバイス 204 および 208 は、同じ部屋、異なる都市、異なる国等に位置付けることができる。あるいは、1つ以上の実施形態では、近接度の制約を執行することができる。例えば、証明書 250 にデジタル署名すべきか否か判定する際に DRM モジュール 210 によって用いられる 1つの規準は、デバイス 204 がデバイス 208 からしきい値近接度以内にあることである。別の一例として、一時的ドメイン証明書 256 を発行すべきか否か判定する際にドメイン要求モジュール 232 によって用いられる 1つの規準は、デバイス 204 がデバイス 208 からしきい値近接度以内にあること

20

【 0 0 5 8 】

[0064] デバイス 204 および 208 の互いに対する近接度は、異なる形態で識別することができる。1つ以上の実施形態では、デバイス 204 および 208 の地理的位置を特定し、近接度を判定するために用いられる。これらの地理的位置は、デバイス 204 および 208 が位置する場所のジップ・コード (例えば、デバイスのユーザーによって特定される) に基づいて、デバイス 204 および 208 の電話番号に基づいて (例えば、デバイスのユーザーによって特定される)、デバイス 204 および 208 の汎地球測位システム (GPS) 座標に基づいて (例えば、GPS モジュールあるいはこれらのデバイス内に含まれるまたはこれらに結合されているコンポーネントによって特定される)、デバイス 204 および 208 が通信しているセル・サイトまたは基地局に基づいて (例えば、これらのデバイスに含まれるまたはこれらに結合されているモジュールまたはコンポーネントによって特定される) 等というように、異なる形態で特定することができる。これらの地理的位置を特定し、これらのデバイスの地理的位置間の距離を計算し、この距離がしきい値数よりも下か否かチェックすることができる。

30

【 0 0 5 9 】

[0065] あるいは、デバイス 204 および 208 の近接度は、異なる形態で特定することができる。例えば、デバイス 204 および 208 が特定のプロトコルまたは技法を用いて通信している場合、これらが互いのしきい値近接度以内にあると想定することができる。このようなプロトコルおよび技法の例として、デバイス 204 および 208 が赤外線 (IR) 接続を用いて、専用有線接続を用いて、ワイヤレス・ユニバーサル・シリアル・バス (ワイヤレス USB) 接続を用いて、何らかのその他のパーソナル・エリア・ネットワーク (PAN) 通信プロトコル等を通じて互いに通信している場合、これらは互いからしきい値近接度以内にあると想定することができる。

40

【 0 0 6 0 】

[0066] 図 3 は、1つ以上の実施形態による一時的ドメイン証明書の一例 300 を示す。一時的ドメイン証明書 300 は、例えば、図 2 の一時的ドメイン証明書 256 とすることができる。一時的ドメイン証明書 300 は、デバイス ID 302、ドメイン ID 304、ドメイン秘密鍵 306、ドメイン証明書 308、完全性検証値 310、権利リスト 312、および期限 314 といった、複数のフィールドまたは部分を含む。一時的ドメイン証

50

明書 300 は、特定のデバイスおよび / または特定のドメイン（例えば、図 2 のデバイス 204、および / またはデバイス 204 が会員となっているドメイン）に拘束されている。

【0061】

[0067] デバイス ID 302 は、一時的ドメイン証明書 300 が拘束されるデバイス（例えば、図 2 のデバイス 204）の識別子、または代わりに一時的ドメイン証明書 300 が拘束されるドメイン（例えば、図 2 のデバイス 204 が会員となっているドメイン）の識別子である。この識別子は、受け取った一時的ドメイン加入要求に応答して一時的ドメイン証明書 300 を発生したモジュールまたはコンポーネントが受け取ることができる。ドメイン ID 304 は、一時的会員資格が与えられようとしている一時的ドメイン証明書 300 のドメイン（例えば、図 2 のドメイン 206）の識別子である。

10

【0062】

[0068] ドメイン秘密鍵 306 は、ドメイン ID 304 によって特定されるドメインの公開 / 秘密鍵対の秘密鍵である。各ドメインは、それ自体の公開 / 秘密鍵対を有しており、これらは、例えば、図 2 のドメイン情報ストア 236 に格納することができる。ドメイン秘密鍵 306 は、一時的ドメイン証明書 300 において暗号化されている。一時的ドメイン証明書の 1 つ以上の他の部分も、オプションとして、暗号化することができる。

【0063】

[0069] ドメイン証明書 308 は、ドメイン ID 304 によって特定されたドメインと関連付けられているデジタル証明書である。このデジタル証明書は、ドメインの公開 / 秘密鍵対の公開鍵のような、ドメインを記述する種々の情報を含むことができ、ドメイン・コントローラー 202 の秘密鍵を用いてデジタル署名されている（例えば、図 2 のデバイス拘束暗号化モジュール 234 によって）。このデジタル署名によって、他のモジュールまたはコンポーネントは、望ましければ、証明書が実際にドメイン・コントローラー 202 によって発生され、改竄されていないことを検証することができる。

20

【0064】

[0070] 完全性検証値 310 は、一時的ドメイン証明書 300 の完全性を検証するために用いることができる値である。この値は、一時的ドメイン証明書 300 の前述の部分（オプションとして、値 310 を除く）全体のチェックサム、一時的ドメイン証明書 300 の 1 つ以上の部分（オプションとして、値 310 を除く）に跨るデジタル署名等のように、種々の異なる検証技法にしたがって発生することができる。

30

【0065】

[0071] 権利リスト 312 は、一時的ドメイン証明書 300 によって付与される一時的ドメイン会員資格に対する 1 組の権利および / または制約である。先に論じたように、コンテンツの消費について種々の制約を、ドメインの会員に賦課することができ、これらの制約は権利リスト 312 において識別することができる。オプションとして、一時的ドメイン会員資格が与えられた会員には、再生は許可するが CD へのコピーまたは焼き付けは許可しない、一度だけコンテンツの再生または電子メール送信を許可する、ドメインにおける一時的会員資格のために他のデバイスに代わってデジタル署名付き一時的ドメイン会員要求をデバイスが発生することを許可しない等のような、追加の制約を賦課することができる。

40

【0066】

[0072] あるいは、または権利リスト 312 に加えて、一時的ドメイン証明書 300 によって付与される一時的ドメイン会員資格に権利および / または制約を確立するためには、他のメカニズムも用いることができる。例えば、このような権利および / または制約は、オプションとして、デバイスの DRM モジュール（例えば、図 2 の DRM モジュール 220）に含ませることができる。

【0067】

[0073] 期限 314 は、一時的ドメイン証明書 300 を用いることができる時間量を示す。通例、期限 314 は、一時的ドメイン証明書 300 が期限切れとなり関連するコンテ

50

ンツを消費するためにコンテンツ・ライセンスから情報を抽出するためにもはや用いることができなくなる日および／または時刻を含む。あるいは、一時的ドメイン証明書300は、関連する発行日および／または時刻（一時的ドメイン証明書300の一部として含まれるか、または代わりに別個に維持される）を有することができ、期限314は、その発行日および／または時刻後の時間量を示す期間とすることもでき、この期間中一時的ドメイン証明書300を用いて、関連するコンテンツを消費するためにコンテンツ・ライセンスから情報を抽出することができる。期限切れでない間、一時的ドメイン証明書300は、先に論じたように、コンテンツ鍵を解読するためにデバイス（例えば、図2のデバイス204）によって用いることができる。期限切れの後、一時的ドメイン証明書は、コンテンツ鍵を解読するためにデバイスによって用いることはできない（例えば、デバイスのDRMモジュールは、一時的ドメイン証明書300が期限切れになっていることを認識し、コンテンツ鍵を解読するために証明書300を用いることはない）。

10

【0068】

[0074] 図4は、1つ以上の実施形態による、コンテンツ共有のための一時的ドメイン会員資格付与のプロセス例400を示すフローチャートである。プロセス400は、図2のデバイス204のような、ドメインの中にあり一時的会員を求めているデバイスによって実行され、ソフトウェア、ファームウェア、ハードウェア、またはその組み合わせによって実現することができる。プロセス400は、コンテンツ共有のための一時的ドメイン会員資格付与のプロセス例であり、本明細書では、コンテンツ共有のための一時的ドメイン会員資格付与についての、異なる図面を参照した更に別の論述が含まれる。

20

【0069】

[0075] 最初に、ドメインにおいて一時的会員を求めているデバイスのデジタル証明書が、一時的会員が求められているドメインの会員に送られる（動作402）。先に論じたように、この証明書は、デバイスに特定の証明書とすることができ、あるいは代わりに、プロセス400を実行するデバイスが会員となっているドメインに特定の証明書とすることもできる。

【0070】

[0076] 動作402における証明書の送付は、プロセス400を実行するデバイスによって開始することができ、あるいは代わりに証明書が送られる先のドメインの会員からの要求に応答して開始することもできる。一例として、プロセス400を実行するデバイスのユーザーにUIを表示することができ、このユーザーが一時的ドメイン会員の要求を入力することができ、これによってユーザーは、当該ドメイン内にあるデバイスにおいて特定のコンテンツの要求を入力すること等ができる。別の一例として、証明書が送られる先のデバイスのユーザーにUIを表示することができ、ユーザーは、プロセス400を実行するデバイスに一時的ドメイン会員資格を与える要求、プロセス400を実行するデバイスに特定のコンテンツを転送する要求等を入力することができる。

30

【0071】

[0077] 1つ以上の実施形態では、動作402の後、デジタル署名付き一時的ドメイン加入要求がドメイン会員から受け取られ（動作404）、先に論じたように、ドメイン・コントローラーに送られる（動作406）。あるいは、ドメインの会員が、プロセス400を実行するデバイスの代わりにデジタル署名付き一時的ドメイン加入要求を発生しないと決定した場合、または先に論じたように、デジタル署名付き一時的ドメイン加入要求が、ドメイン会員によってドメイン・コントローラーに送られる場合、このような要求を受け取らないこともある。

40

【0072】

[0078] デジタル署名付き一時的ドメイン加入要求がドメイン・コントローラーに送られる形態には関係なく、要求を送った後、ドメイン会員が会員であるドメインに対する一時的ドメイン証明書が受け取られる（動作408）。このドメインのドメイン鍵は、一時的ドメイン証明書に含まれており、このドメイン会員のドメインに拘束されているコンテンツを消費するために用いられる（動作410）。先に論じたように、1つ以上の実施

50

形態では、このドメイン鍵は、コンテンツを解読するために、コンテンツ鍵を解読する際に用いることができる。この消費は、一時的ドメイン証明書が期限切れになるまで、コンテンツと関連付けられた1つ以上のライセンスにしたがって継続することができる。

【0073】

[0079] 尚、ドメイン・コントローラーが、一時的ドメイン加入要求に応答して一時的ドメイン証明書を発行することを決定した場合、一時的ドメイン証明書ドメイン(temporary domain certificate domain)は、プロセス400を実行するデバイスによって受け取られることは記してしかるべきである。ドメイン・コントローラーが、一時的ドメイン加入要求に応答して一時的ドメイン証明書を発行しないことを決定した場合、このような証明書は動作408において受け取られ、動作410において用いられる。

10

【0074】

[0080] 図5は、1つ以上の実施形態による、コンテンツ共有のための一時的ドメイン会員資格付与のプロセス例500を示すフローチャートである。プロセス500は、図2のデバイス208のような、ドメインの会員であるデバイスによって実行され、ソフトウェア、ファームウェア、ハードウェア、またはその組み合わせによって実現することができる。プロセス500は、コンテンツ共有のための一時的ドメイン会員資格付与のプロセス例であり、本明細書では、コンテンツ共有のための一時的ドメイン会員資格付与について、異なる図面を参照した更に別の論述が含まれる。

【0075】

[0081] 最初に、デバイスのデジタル証明書が、デジタル署名付き一時的ドメイン加入要求と共に、要求元デバイスから受け取られる(動作502)。この証明書および要求は別個にすることができ、または代わりに要求が内在(inherent)することもできる。例えば、証明書は、当該証明書の要求に応答して、プロセス500を実行するデバイスによって受け取ることができ、この場合、デジタル署名付き一時的ドメイン加入要求の要求は、正にこの証明書の受け取りに内在することができる。加えて、先に論じたように、要求元デバイスの証明書は、当該要求元デバイスに特定のであること、または当該要求元デバイスが会員となっているドメインに特定のであることも可能である。

20

【0076】

[0082] 次いで、動作502において受け取られた要求元デバイスのデジタル証明書が有効か否かについてチェックを行う(動作504)。この有効性についてのチェックは、先に論じたように、破棄リストまたは記録をチェックするというように、異なる形態で行うことができる。動作502において受け取った証明書にデジタル署名されている場合、この有効性についてのチェックは、証明書のデジタル署名を検証することも含むことができる。あるいは、動作504を実行しなくてもよい。先に論じたように、デバイスのデジタル証明書は、当該デバイスに特定のであることも、または当該デバイスが会員となっているドメインに特定のであることも可能である。

30

【0077】

[0083] 要求元デバイスのデジタル証明書が有効でない場合、動作502において受け取った要求を拒否する(動作506)。この拒否の指示を、オプションとして、要求元デバイスに戻すことができる。

40

【0078】

[0084] しかしながら、このデバイスのデジタル証明書が有効である場合、プロセス500を実行するデバイスのユーザーが、要求元デバイスが一時的にドメインに加入することを承認するか否かについてチェックを行う(動作508)。先に論じたように、このユーザー承認の判定は、種々の異なる形態で行うことができる。あるいは、動作508を実行しなくてもよい。

【0079】

[0085] ユーザーが、要求元デバイスがドメインに一時的に加入する許可を承認しない場合、動作502において受け取った要求を拒否する(動作506)。この拒否の指示を、オプションとして、要求元デバイスに戻すことができる。

50

【 0 0 8 0 】

[0086] しかしながら、ユーザーが、要求元デバイスが一時的にドメインに加入することを承認した場合、要求元デバイスの鍵を含むデジタル署名付き一時的ドメイン加入要求を作成する（動作 5 1 0）。1 つ以上の実施形態では、このデジタル署名付き一時的ドメイン加入要求は、要求元デバイスの公開鍵を含む（動作 5 0 2 において受け取ったデジタル証明書から）。デジタル署名付き一時的ドメイン加入要求は、動作 5 0 2 において受け取った要求元デバイスの証明書（要求元デバイスの公開鍵を含む）を含むことができ、あるいは代わりに、一時的ドメイン証明書を要求元デバイスに拘束することを可能にする何らかの他の鍵またはメカニズムを含むことができる。

【 0 0 8 1 】

[0087] デジタル署名付き一時的ドメイン加入要求は、要求元デバイスまたはドメイン・コントローラーのような、受け取り側に送られる。1 つ以上の実施形態では、デジタル署名付き一時的ドメイン加入要求は要求元デバイスに戻される（動作 5 1 2）。デジタル署名付き一時的ドメイン加入要求を要求元デバイスに送る代わりに、または代わりに、デジタル署名付き一時的ドメイン加入要求を要求元デバイスに送ることに加えて、デジタル署名付き一時的ドメイン加入要求をドメイン・コントローラーに送る（動作 5 1 4）。

【 0 0 8 2 】

[0088] 図 6 は、1 つ以上の実施形態による、コンテンツ共有のための一時的ドメイン会員資格付与のプロセス例 6 0 0 を示すフローチャートである。プロセス 6 0 0 は、図 2 のドメイン・コントローラー 2 0 2 のような、ドメイン・コントローラーによって実行され、ソフトウェア、ファームウェア、ハードウェア、またはその組み合わせによって実現することができる。プロセス 6 0 0 は、コンテンツ共有のための一時的ドメイン会員資格付与のプロセス例であり、本明細書では、コンテンツ共有のための一時的ドメイン会員資格付与について、異なる図面を参照した更に別の論述が含まれる。

【 0 0 8 3 】

[0089] 最初に、デジタル署名付き一時的ドメイン加入要求を受け取る（動作 6 0 2）。次いで、この一時的ドメイン加入要求にあるデジタル署名が有効か否かについてチェックする（動作 6 0 4）。一時的ドメイン加入要求にあるデジタル署名を検証することができれば、これは有効である。一時的ドメイン加入要求にあるデジタル署名が有効でない場合、一時的ドメイン加入要求を拒否する（動作 6 0 6）。この拒否の指示を、オプションとして、動作 6 0 2 において受け取られた要求を送ったデバイスに戻すことができる。

【 0 0 8 4 】

[0090] しかしながら、一時的ドメイン加入要求にあるデジタル署名が検証された場合、次に、一時的ドメイン加入要求に含まれる証明書（または鍵あるいは他のメカニズム）が有効か否かについてチェックを行う（動作 6 0 8）。この有効性についてのチェックは、先に論じたように、破棄リストまたはその他の記録をチェックするというように、異なる形態で行うことができる。代わりに、動作 6 0 8 を実行しなくてもよい（例えば、先に論じたように、一時的ドメイン加入要求にデジタル署名したデバイスによって、有効性についてのチェックが既に行われている場合）。

【 0 0 8 5 】

[0091] 一時的ドメイン加入要求に含まれる証明書（または鍵あるいは他のメカニズム）が有効でない場合、一時的ドメイン加入要求を拒否する（動作 6 0 6）。この拒否の指示を、オプションとして、動作 6 0 2 において受け取られた要求を送ったデバイスに戻すことができる。

【 0 0 8 6 】

[0092] しかしながら、一時的ドメイン加入要求に含まれる証明書（または鍵あるいは他のメカニズム）が有効である場合、一時的ドメイン加入要求に含まれている証明書に含まれている公開鍵に拘束された一時的ドメイン証明書を発生する（動作 6 1 0）。オプシ

10

20

30

40

50

ョンとして、先に論じたように、一時的ドメイン証明書を発生するためには、1つ以上の他の規準も満たす必要がある場合もある。先に論じたように、この一時的ドメイン証明書は特定のデバイスまたは特定のドメインに拘束することができる。次いで、発生した一時的ドメイン証明書を、一時的ドメイン会員を要求しているデバイスに送る（動作612）。この一時的ドメイン証明書は、一時的ドメイン加入要求にデジタル署名したデバイスが会員であるドメインのためのものである。

【0087】

[0093] 図7は、1つ以上の実施形態にしたがって、コンテンツ共有のための一時的ドメイン会員資格付与を実現するように構成することができる計算機例700を示す。計算機700は、例えば、図1のデバイス112、114、または116、図2のデバイス204または208とすることができ、あるいは図1のドメイン・コントローラー102、または図2のドメイン・コントローラー202、図1のコンテンツ・プロバイダー104、図1のライセンス・サーバー106、あるいは図1のトラスト・オーソリティ120の少なくとも一部を実現することができる。

10

【0088】

[0094] 計算機700は、1つ以上のプロセッサまたは処理ユニット702、1つ以上のメモリーおよび/または記憶コンポーネント706を含むことができる1つ以上のコンピューター読み取り可能媒体704、1つ以上の入出力（I/O）デバイス708、ならびに種々のコンポーネントおよびデバイスが互いに通信できるようにするバス710を含む。コンピューター読み取り可能媒体704および/または1つ以上のI/Oデバイス708は、計算機700の一部として含むことができ、または代わりに計算機700に結合することもできる。バス710は、メモリー・バスまたはメモリー・コントローラー、周辺バス、加速グラフィックス・ポート、プロセッサまたはローカル・バス等を含み、種々の異なるバス・アーキテクチャを用いる、様々なタイプのバス構造のうち1つ以上を表す。バス710は、有線バスおよび/またはワイヤレス・バスを含むことができる。

20

【0089】

[0095] メモリー/記憶コンポーネント706は、1つ以上のコンピューター記憶媒体を表す。コンポーネント706は、揮発性媒体（ランダム・アクセス・メモリー（RAM）のような媒体）および/または不揮発性媒体（リード・オンリ・メモリー（ROM）、フラッシュ・メモリー、光ディスク、磁気ディスク等のような媒体）を含むことができる。コンポーネント706は、固定媒体（例えば、RAM、ROM、固定ハード・ドライブ等）、およびリムーバブル媒体（例えば、フラッシュ・メモリー・ドライブ、リムーバブル・ハード・ドライブ、光ディスク等）を含むことができる。

30

【0090】

[0096] 本明細書において論じた技法は、ソフトウェアで実現することができ、1つ以上の処理ユニット702が命令を実行する。尚、異なる命令は、処理ユニット702の中、処理ユニット702の種々のキャッシュ・メモリーの中、デバイス700の他のキャッシュ・メモリー（図示せず）の中、他のコンピューター読み取り可能媒体上等のように、計算機700の異なるコンポーネントに格納できることは認められてしかるべきである。加えて、計算機700内において命令を格納する位置は、ときと共に変化する可能性があることも認められてしかるべきである。

40

【0091】

[0097] 1つ以上の入出力デバイス708は、ユーザーがコマンドおよび情報を計算機700に入力することを可能にし、更に情報をユーザーおよび/または他のコンポーネントまたはデバイスに提示することも可能にする。入力デバイスの例には、キーボード、カーソル制御デバイス（例えば、マウス）、マイクロフォン、スキャナ等が含まれる。出力デバイスの例には、ディスプレイ・デバイス（例えば、モニタまたはプロジェクタ）、スピーカ、プリンタ、ネットワーク・カード等が含まれる。

【0092】

[0098] 本明細書では、種々の技法をソフトウェアまたはプログラム・モジュールとい

50

う一般的なコンテキストにおいて記載することができる。一般に、ソフトウェアは、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造等を含み、特定のタスクを実行するかまたは特定の抽象データ・タイプを実現する。これらのモジュールおよび技法の実現例は、何らかの形態のコンピューター読み取り媒体を通じて格納または送信することができる。コンピューター読み取り可能媒体は、計算機がアクセスすることができる任意の入手可能な1つまたは複数の媒体とすることができる。一例として、そして限定ではなく、コンピューター読み取り可能媒体は「コンピューター記憶媒体」および「通信媒体」を含むことができる。

【0093】

[0099] 「コンピューター記憶媒体」は、揮発性および不揮発性、リムーバブルおよび非リムーバブル媒体を含み、これらは、コンピューター読み取り可能命令、データ構造、プログラム・モジュール、またはその他のデータというような、情報の記憶のための任意の方法または技術によって実現される。コンピューター記憶媒体は、限定ではなく、RAM、ROM、EEPROM、フラッシュ・メモリーまたはその他のメモリー技術、CD-ROM、デジタル・バーサタイル・ディスク(DVD)またはその他の光ストレージ、磁気カセット、磁気テープ、磁気ディスク・ストレージまたはその他の磁気記憶デバイス、あるいは所望の情報を格納するために用いることができ、しかもコンピューターがアクセスすることができる任意の他の媒体を含む。

【0094】

[0100] 「通信媒体」は、通例、コンピューター読み取り可能命令、データ構造、プログラム・モジュール、またはその他のデータを、搬送波またはその他の伝送メカニズムのような、変調データ信号において具体化する。また、通信媒体は、任意の情報配信媒体も含む。「変調データ信号」という用語は、情報を信号内にエンコードするような様式で、その特性1つ以上を設定または変化させた信号を意味する。限定ではなく、一例として、通信媒体は、有線ネットワークまたは直接有線接続というような有線媒体、ならびに音響、RF、赤外線、およびその他のワイヤレス媒体というようなワイヤレス媒体を含む。前述のうち任意のものの組み合わせも、コンピューター読み取り可能媒体の範囲に当然含まれるものとする。

【0095】

[0101] 一般に、本明細書において記載した機能または技法のうち任意のものが、ソフトウェア、ファームウェア、ハードウェア(例えば、固定論理回路)、手動処理、またはこれらの実現例の組み合わせを用いて実現することができる。「モジュール」という用語は、本明細書において用いる場合、一般にソフトウェア、ファームウェア、ハードウェア、またはその組み合わせを表す。ソフトウェア実現例の場合、モジュール、機能、またはロジックは、プロセッサ(例えば、1つまたは複数のCPU)において実行されると、指定されたタスクを実行するプログラム・コードを表す。プログラム・コードは、1つ以上のコンピューター読み取り可能メモリー・デバイスに格納することができる。これらの更に詳しい説明は、図7を参照すれば見出すことができる。本明細書に記載したコンテンツ共有のための一時的ドメイン会員資格付与の特徴は、プラットフォームに依存しないということであり、種々のプロセッサを有する種々の商用計算プラットフォームにおいて、本技術を実現できることを意味する。

【0096】

[0102] 以上、構造的特徴および/または方法論的動作に特定の文言で主題について説明したが、添付した特許請求の範囲において定められている主題は、以上に記載した特定の特徴または動作には必ずしも限定されないことは言うまでもない。逆に、以上に記載した特定の特徴および動作は、特許請求の範囲を実現する形態例として開示したのである。

。

【図 1】

100

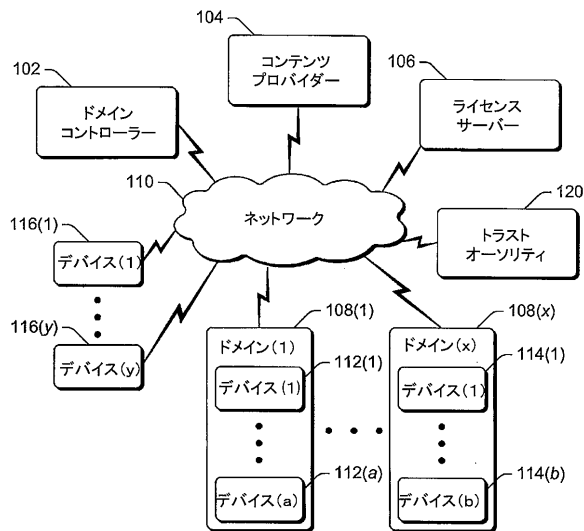


Fig. 1

【図 2】

200

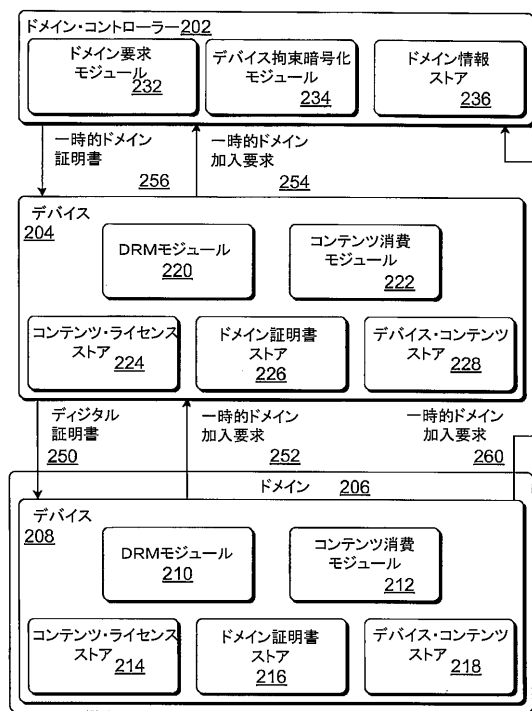


Fig. 2

【図 3】

300

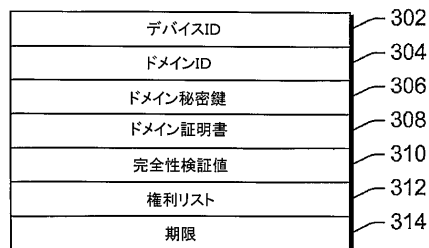


Fig. 3

【図 4】

400

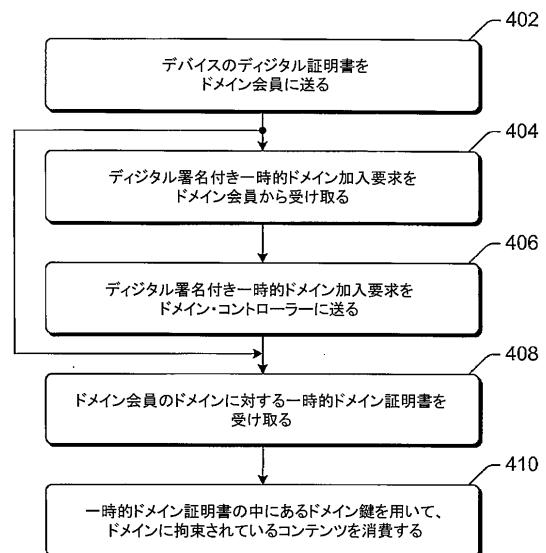


Fig. 4

【図 5】

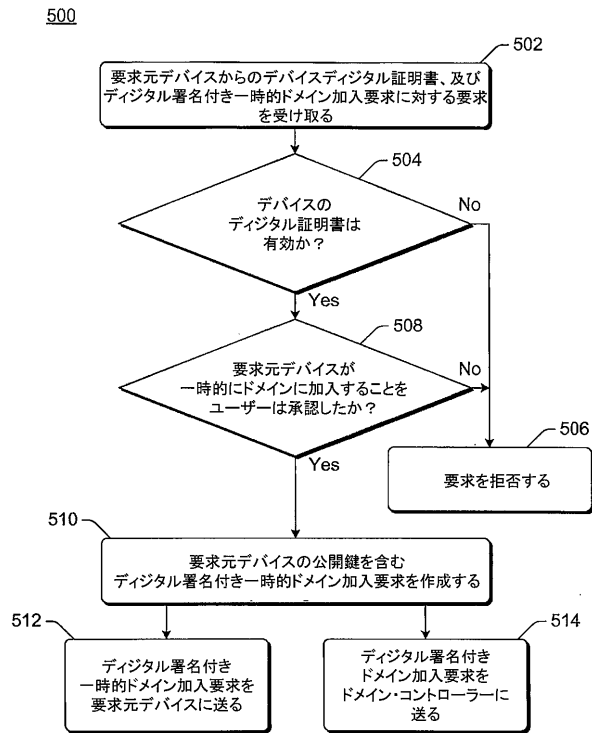


Fig. 5

【図 6】

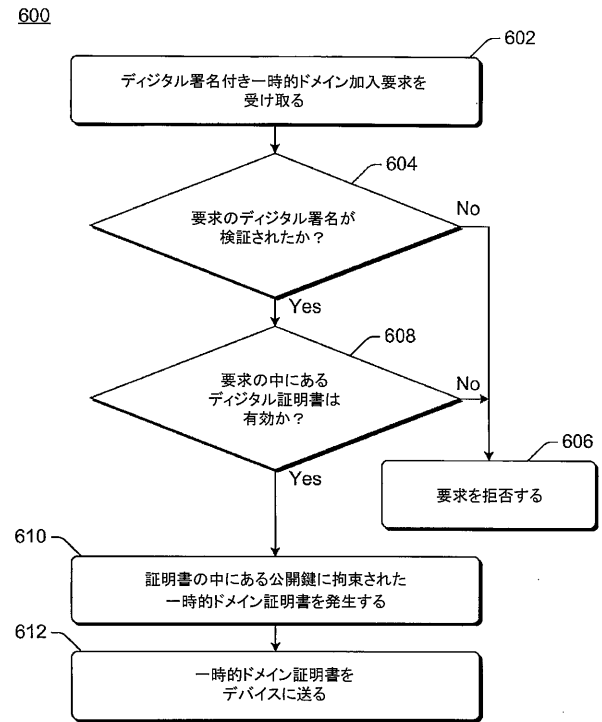


Fig. 6

【図 7】

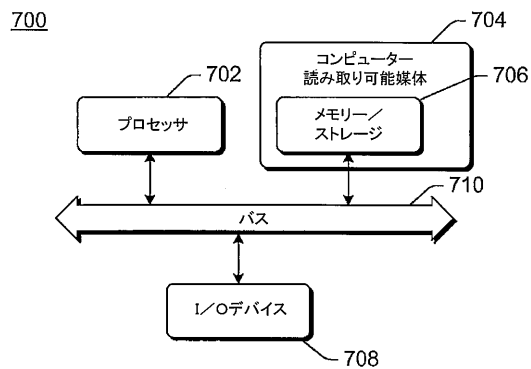


Fig. 7

フロントページの続き

(72)発明者 シュネル, パトリック

アメリカ合衆国ワシントン州 9 8 0 5 2 - 6 3 9 9 , レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, エルシーエイ・インターナショナル・パテンツ

(72)発明者 アルコーヴ, ジェームズ・エム

アメリカ合衆国ワシントン州 9 8 0 5 2 - 6 3 9 9 , レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, エルシーエイ・インターナショナル・パテンツ

審査官 岸野 徹

(56)参考文献 特開 2 0 0 6 - 1 9 0 2 0 0 (J P , A)

特開 2 0 0 7 - 0 1 8 3 0 1 (J P , A)

特表 2 0 0 6 - 5 0 4 1 7 6 (J P , A)

特開 2 0 0 5 - 2 4 3 0 1 6 (J P , A)

特開平 0 7 - 1 6 0 1 9 8 (J P , A)

特開 2 0 0 1 - 1 8 8 7 5 7 (J P , A)

特開 2 0 0 5 - 0 0 2 5 6 6 (J P , A)

特開 2 0 0 2 - 3 7 3 2 9 5 (J P , A)

特表 2 0 0 8 - 5 1 8 3 4 9 (J P , A)

(58)調査した分野(Int.Cl. , D B 名)

G 0 6 F 2 1 / 3 3

H 0 4 L 9 / 0 8

H 0 4 L 9 / 3 2