(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-257292
(P2012-257292A)
(43)公開日　平成24年12月27日(2012.12.27)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5J104
G09C 1/00	(2006.01)	G09C	1/00	640D	
G06F 21/22	(2006.01)	G06F	21/22	110A	
G06F 21/00	(2006.01)	G06F	21/00	157A	

審査請求 有　請求項の数 27　ＯＬ　（全 68 頁）

(21)出願番号　特願2012-168650 (P2012-168650)
(22)出願日　平成24年7月30日 (2012.7.30)
(62)分割の表示　特願2009-509765 (P2009-509765)の分割
原出願日　平成19年5月4日 (2007.5.4)
(31)優先権主張番号　60/798,152
(32)優先日　平成18年5月5日 (2006.5.5)
(33)優先権主張国　米国(US)

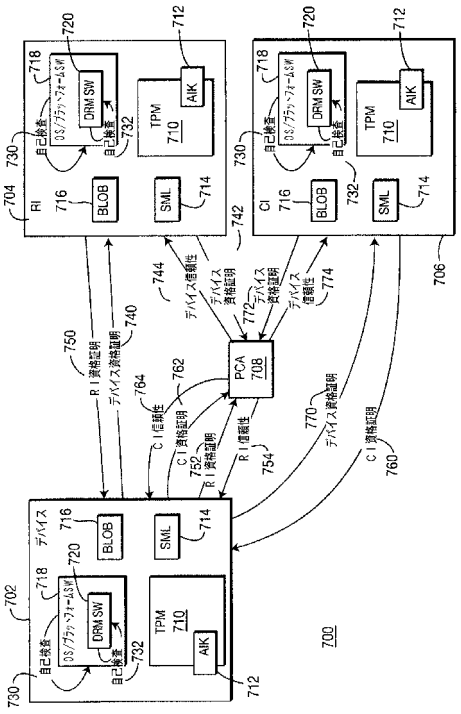
（特許庁注：以下のものは登録商標）
１．ＢＬＵＥＴＯＯＴＨ

(71)出願人　596008622
インターデイジタル　テクノロジー　コーポレーション
アメリカ合衆国　１９８１０　デラウェア州　ウィルミントン　シルバーサイド　ロード　３４１１　コンコルド　プラザ　ヘイグリー　ビルディング　スイート　１０５
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　インヒョク　チャ
アメリカ合衆国　１９０６７　ペンシルベニア州　ヤードリー　サウスリッジ　サークル　５１０

最終頁に続く

(54)【発明の名称】信頼される処理技術を使用したデジタル権利管理

(57)【要約】
【課題】本発明は、ＯＭＡ　ＤＲＭによって規定されるコンテンツ配布と関係するエンティティ、メッセージ、および処理の完全性を強化するいくつかの方法を開示する。
【解決手段】これらの方法は、ＴＣＧ仕様と関係する技術を使用する。第１の実施形態は、ＤＲＭ　ＲＯＡＰ仕様およびＤＲＭコンテンツフォーマット仕様の変更を伴う場合と、伴わない場合の両方で、ＴＣＧ技術を使用して、プラットフォームおよびＤＲＭソフトウェアの完全性または信頼性を検証する。第２の実施形態は、既存のＲＯＡＰプロトコルを変更することなしに、ＴＣＧ技術を使用して、ＲＯＡＰメッセージ、ＲＯＡＰメッセージを構成する情報、およびＲＯＡＰ処理の完全性を強化する。第３の実施形態は、既存のＲＯＡＰプロトコルのいくつかの変更を伴って、ＴＣＧ技術を使用して、ＲＯＡＰメッセージ、ＲＯＡＰ情報、およびＲＯＡＰ処理の完全性を強化する。
【選択図】図７



【特許請求の範囲】
【請求項１】
要求するエンティティ（ＲＥ）装置と、ターゲットエンティティ（ＴＥ）装置との間でプラットフォーム完全性検査を実行するための方法であって、
前記ＴＥ装置に、そのＴＥ装置の信頼される資格証明を報告することを求める要求を送信するステップと、
前記ＴＥ装置の信頼される資格証明を受信するステップと、
前記ＴＥ装置の信頼される資格証明を、完全性検証のために、レスポンダに転送するステップと、
前記レスポンダから前記ＴＥ装置の信頼される資格証明の完全性検証ステータスを受信するステップと、
前記ＴＥ装置に、そのＴＥ装置自身のプラットフォーム完全性ステータスを報告することを求める要求を送信するステップと、
前記ＴＥ装置からプラットフォーム完全性ステータス標識を受信するステップと、
前記レスポンダからの前記ＴＥ装置の信頼される資格証明の完全性検証ステータスと前記ＴＥ装置からの前記プラットフォーム完全性ステータス標識とに基づいて、前記ＴＥ装置のプラットフォーム完全性ステータスに十分な信頼を与えて、権利オブジェクト獲得プロトコル（ＲＯＡＰ）登録プロトコルにおいて前記ＴＥ装置を進めるか、または、デバイスが権利発行者（ＲＩ）からの権利オブジェクト（ＲＯ）を獲得することを可能にする別のプロトコルにおいて前記ＴＥ装置を進めるのかを決定するステップと
を含み、
前記ＴＥ装置が、前記方法を開始するトリガを前記ＲＥ装置に送信することによって、前記方法が、前記ＴＥ装置が前記ＲＥ装置を相手に前記登録プロトコルを開始するのに先立って実行されることを特徴とする方法。
【請求項２】
前記ＲＥ装置は、前記ＲＩであり、前記ＴＥ装置は、前記デバイスであることを特徴とする請求項１に記載の方法。
【請求項３】
前記デバイスが前記ＲＩ装置に最も新しく登録してから経過した時間に基づいて、前記方法が定期的に実行されることを特徴とする請求項２に記載の方法。
【請求項４】
前記デバイスが該デバイスのプラットフォーム完全性ステータスを前記ＲＩ装置に最も新しく検証してから経過した時間に基づいて、前記方法が定期的に実行されることを特徴とする請求項２に記載の方法。
【請求項５】
前記ＲＥ装置は、コンテンツ発行者（ＣＩ）であり、前記ＴＥ装置は、前記デバイスであることを特徴とする請求項１に記載の方法。
【請求項６】
前記デバイスが該デバイスのプラットフォーム完全性ステータスを前記ＣＩに最も新しく検証してから経過した時間に基づいて、前記方法が定期的に実行されることを特徴とする請求項５に記載の方法。
【請求項７】
前記デバイスが、前記ＣＩからコンテンツを購入すると、前記方法が実行されることを特徴とする請求項５に記載の方法。
【請求項８】
要求するエンティティ（ＲＥ）装置と、ターゲットエンティティ（ＴＥ）装置との間でデジタル権利管理（ＤＲＭ）ソフトウェア完全性検査を実行するための方法であって、
前記ＴＥ装置がＤＲＭソフトウェア完全性検査を実行するための要求を、前記ＲＥ装置から受信するステップと、
前記ＴＥ装置において前記ＤＲＭソフトウェア完全性検査を実行するステップと、

権利発行者（ＲＩ）にデバイスから権利オブジェクト要求メッセージが送信されることに先立って、前記ＲＥ装置にＤＲＭソフトウェア完全性ステータス標識を送信するステップであって、前記ＤＲＭソフトウェア完全性ステータス標識は、前記ＴＥ装置の完全性ステータスに十分な信頼を与えて、権利オブジェクト獲得プロトコル（ＲＯＡＰ）登録プロトコルにおいて前記ＴＥ装置を進めるか、または、デバイスが前記ＲＩからの権利オブジェクト（ＲＯ）を獲得することを可能にする別のプロトコルにおいて前記ＴＥ装置を進めるのかを示すように構成される、ステップと
を含み、
前記ＴＥ装置は、前記ＴＥ装置が前記ＲＯＡＰプロセスを開始するのに先立って、前記方法を開始するトリガを前記ＲＥ装置に送信することを特徴とする方法。

【請求項９】
前記ＲＥ装置は、前記ＲＩであり、前記ＴＥ装置は、前記デバイスであることを特徴とする請求項８に記載の方法。

【請求項１０】
前記ＲＯＡＰプロセスは、２パス登録、２パスドメイン参加、または２パスドメイン退去のうちの少なくとも１つから選択されることを特徴とする請求項８に記載の方法。

【請求項１１】
前記デバイスが前記ＲＩを相手に権利オブジェクト獲得プロトコル（ＲＯＡＰ）プロセスを完了した後、前記方法が定期的に実行されることを特徴とする請求項９に記載の方法。

【請求項１２】
前記ＲＯＡＰプロセスは、２パス登録、２パスドメイン参加、または２パスドメイン退去のうちの少なくとも１つから選択されることを特徴とする請求項１１に記載の方法。

【請求項１３】
前記デバイスが該デバイスのＤＲＭソフトウェア完全性ステータスを前記ＲＩに検証し、報告した後、前記方法が定期的に実行されることを特徴とする請求項９に記載の方法。

【請求項１４】
前記デバイスが該デバイスのＤＲＭソフトウェアを更新した後、前記方法が実行されることを特徴とする請求項９に記載の方法。

【請求項１５】
前記ＲＩは、前記デバイス上のメディアプレーヤに対して前記ＤＲＭソフトウェア完全性検査を実行するよう、前記デバイスに要求することを特徴とする請求項９に記載の方法。

【請求項１６】
前記ＲＥ装置は、コンテンツ発行者（ＣＩ）であり、前記ＴＥ装置は、デバイスであることを特徴とする請求項８に記載の方法。

【請求項１７】
前記デバイスは、前記デバイスが権利オブジェクト獲得プロトコル（ＲＯＡＰ）プロセスを開始するのに先立って、前記方法を開始するトリガを前記ＣＩに送信することを特徴とする請求項１６に記載の方法。

【請求項１８】
前記デバイスが、前記ＣＩを相手に権利オブジェクト獲得プロトコル（ＲＯＡＰ）プロセスを完了した後、前記方法が定期的に実行されることを特徴とする請求項１６に記載の方法。

【請求項１９】
前記デバイスが該デバイスのＤＲＭソフトウェア完全性ステータスを前記ＣＩに検証し、報告した後、前記方法が定期的に実行されることを特徴とする請求項１６に記載の方法。

【請求項２０】
前記デバイスが該デバイスのＤＲＭソフトウェアを更新した後、前記方法が実行される

ことを特徴とする請求項１６に記載の方法。
【請求項２１】
前記ＣＩは、前記デバイス上のメディアプレーヤに対してＤＲＭソフトウェア完全性検査を実行するよう、前記デバイスに要求することを特徴とする請求項１６に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、無線通信ネットワークにおけるＤＲＭ（デジタル権利管理）方法に関する。より詳細には、本発明は、ＯＭＡ（Ｏｐｅｎ　Ｍｏｂｉｌｅ　Ａｌｌｉａｎｃｅ）ＤＲＭ仕様に準拠して動作するシステムにおいてセキュリティ、完全性、および信頼性を強化するための方法を提供する。
【背景技術】
【０００２】
ＯＭＡ　ＤＲＭは、移動電話機および移動デバイスの製造業者、ならびにモバイルサービスプロバイダのコンソーシアムであるＯＭＡによって指定されるＤＲＭシステムである。このスキームは、多くの移動電話機上で実施され、モバイルコンテンツプロバイダによって、プロバイダの製品およびサービスにＤＲＭを追加するのに使用されることが意図される。ＯＭＡ　ＤＲＭの２つのバージョン、すなわち、ＯＭＡ　ＤＲＭ１．０およびＯＭＡ　ＤＲＭ２．０が、公開されている。
【０００３】
ＯＭＡ　ＤＲＭ１．０は、コンテンツオブジェクトに関するデジタル権利の基本的管理に関するスキームを扱う。このため、ＯＭＡ　ＤＲＭ１．０は、コンテンツオブジェクトに関しても、権利オブジェクトに関しても強力な保護は提供しなかった。ＯＭＡ　ＤＲＭ１．０は、３つの配信方法、すなわち、転送ロック（ユーザが、コンテンツを他のユーザ、または他のデバイスに転送するのを防止する）、組み合わされた配信（組み合わされた権利オブジェクトとメディアオブジェクト）、および分離した配信（分離した権利オブジェクトとメディアオブジェクト）を規定する。ＯＭＡ　ＤＲＭ１．０は、電話機に関する呼び出し音または壁紙などの小さいサイズのメディアオブジェクトを扱うように設計された。
【０００４】
ＯＭＡ　ＤＲＭ２．０は、ＯＭＡ　ＤＲＭ１．０配信機構を改良し、拡張する。ＯＭＡ　ＤＲＭ２．０に準拠するデバイスは、ＤＲＭ　ＰＫＩ（公開鍵インフラストラクチャ）に基づく個別の証明書を有し、すなわち、各デバイスは、公開鍵、対応する秘密鍵を有するとともに、この事実を検証する証明書を有する。各ＲＯ（権利オブジェクト）は、機密性（暗号化によって）と完全性（デジタル署名によって）の両方に関して保護される。ＰＫＩ、暗号化、および完全性検査の使用が、ＯＭＡ　ＤＲＭ１．０システムのセキュリティと比べて、ＯＭＡ　ＤＲＭ２．０システムのセキュリティを強化する。
【０００５】
また、ＯＭＡ　ＤＲＭ２．０は、デバイスとＲＩ（権利発行者）との間の相互認証および相互登録、ＲＯを要求すること、ＲＯの配信に対する応答、またはＲＯを配信することの拒否、ならびにデバイスがドメインに参加すること、およびドメインを退去することと関係する様々なサブプロトコルを含むＲＯＡＰ（権利オブジェクト獲得プロトコル）とまとめて呼ばれるプロトコルのセットも規定する。
【０００６】
以下は、ＯＭＡ　ＤＲＭにおいて定義される主なエンティティのいくつかである。すなわち、
【０００７】
アクタ　アクタは、使用事例を実行する外部エンティティである。
【０００８】
バックアップ／リモートストレージ　ＲＯおよびＣＯ（コンテンツオブジェクト）を、

元のデバイスに送り返すことを意図して、別のロケーションに転送すること。
【０００９】
組み合わされた配信　保護されたコンテンツおよびＲＯを配信するためのＯＭＡ　ＤＲＭ１．０メソッド。ＲＯおよび保護されたコンテンツは、ＤＲＭメッセージという単一のエンティティの中で一緒に配信される。
【００１０】
機密性　情報が、許可のない個人、エンティティ、またはプロセスに提供されない、または開示されないという特性。
【００１１】
合成オブジェクト　包含によって１つまたは複数のメディアオブジェクトを含むＣＯ。
【００１２】
接続されたデバイス　適切なワイドエリアトランスポート／ネットワーク層インタフェースを介して、適切なプロトコルを使用してＲＩに直接に接続することができるデバイス。
【００１３】
コンテンツ　１つまたは複数のメディアオブジェクト
【００１４】
ＣＩ（コンテンツ発行者）　ＤＲＭエージェントにコンテンツを提供するエンティティ。
【００１５】
コンテンツプロバイダ　ＣＩまたはＲＩであるエンティティ。
【００１６】
デバイス　ＤＲＭエージェントを有するユーザ機器。デバイスは、接続されたデバイスであることも、接続されていないデバイスであることも可能であるが、この区別は、接続されたデバイスが、ＲＩに直接に接続する能力を失うと、接続されていないデバイスになる可能性があるので、コンテキスト依存であり、性質が不定である。
【００１７】
デバイス取り消し　或るデバイスがＲＯを獲得することが、もはや信頼されないことをＲＩが示すプロセス。
【００１８】
デバイスＲＯ　或る特定のデバイスに、そのデバイスの公開鍵によって専用とされるＲＯ。
【００１９】
ドメイン　ドメインＲＯを共有することができるデバイスのセット。ドメイン内のデバイスは、ドメイン鍵を共有する。ドメインは、ＲＩによって定義され、管理される。
【００２０】
ドメイン識別子　ドメイン鍵の一意ストリング識別子。
【００２１】
ドメイン鍵　１２８ビットの対称暗号鍵
【００２２】
ＤＲＭエージェント　デバイス上のメディアオブジェクトに関する許可を管理するデバイス内のエンティティ。
【００２３】
ＤＲＭコンテンツ　ＲＯの中の許可セットに従って消費されるメディアオブジェクト。
【００２４】
ＤＲＭ時間　セキュリティで保護された、ユーザが変更できない時間源。ＤＲＭ時間は、ＵＴＣ時間フォーマットになっている。
【００２５】
完全性　データが、許可のない仕方で変更、または破壊されていないという特性。
【００２６】

ドメインに参加する　ＲＩが、デバイスをドメインに含めるプロセス。
【００２７】
ドメインを退去する（参加解消する）ＲＩが、取り消されていないデバイスをドメインから除外するプロセス。
【００２８】
メディアオブジェクト　デジタル作品または合成オブジェクト。
【００２９】
ネットワークサービスプロバイダ　移動デバイスにネットワーク接続を提供するエンティティ。
【００３０】
許可　ＤＲＭコンテンツに対してＲＩによって許される実際の使用または活動。
【００３１】
再生する　リソースの一過性の知覚可能な表現を作成すること。
【００３２】
保護されたコンテンツ　ＲＯの中の許可セットに従って消費されるメディアオブジェクト。
【００３３】
復元する　保護されたコンテンツおよび／またはＲＯを外部ロケーションから、保護されたコンテンツおよび／またはＲＯのバックアップの源とされたデバイスに送り返すこと。
【００３４】
取り消す　デバイスまたはＲＩ証明書を無効と宣言するプロセス。
【００３５】
ＲＩ（権利発行者）　ＯＭＡ　ＤＲＭに準拠するデバイスにＲＯを発行するエンティティ。
【００３６】
ＲＩコンテキスト　ＲＩ　ＩＤ、ＲＩ証明書チェーン、バージョン、アルゴリズム、およびその他の情報などの、４パス登録プロトコル中に所与のＲＩを相手にネゴシエートされた情報。ＲＩコンテキストは、デバイスが、登録プロトコルを除いて、ＲＯＡＰスイートのすべてのプロトコルに参加することに成功するのに必要である。
【００３７】
ＲＯ（権利オブジェクト）　保護されたコンテンツにリンクされた許可およびその他の属性の集合。
【００３８】
ＲＯＡＰ（権利オブジェクト獲得プロトコル）　デバイスが、ＲＩからＲＯを要求し、獲得することを可能にするプロトコル。
【００３９】
ＲＯＡＰトリガ　デバイスによって受信されると、ＲＯＡＰを開始するＵＲＬを含むＸＭＬ（拡張マークアップ言語）ドキュメント。
【００４０】
状態のない権利　デバイスが状態情報を保持しなくてもよいＲＯ。
【００４１】
状態のある権利　デバイスが、状態情報を明示的に保持して、ＲＯの中で表現される制約および許可が、正しく実施されることが可能であるようにしなければならないＲＯ。以下の制約または許可のいずれかを含むＲＯが、状態のある権利である。すなわち、＜ｉｎｔｅｒｖａｌ＞、＜ｃｏｕｎｔ＞、＜ｔｉｍｅｄ－ｃｏｕｎｔ＞、＜ｄａｔｅｔｉｍｅ＞、＜ａｃｃｕｍｕｌａｔｅｄ＞、または＜ｅｘｐｏｒｔ＞である。
【００４２】
スーパ配布　（１）セキュリティで保護されていない可能性があるチャネルを介して、ユーザが保護されたコンテンツを他のデバイスに配布することを許し、さらに、そのデバ

イスのユーザが、スーパ配布された保護されたコンテンツに関するＲＯを獲得することを可能にする機構。

【００４３】

接続されていないデバイス　ローカル接続技術を介する適切なプロトコル、例えば、ＯＢＥＸ　ｏｖｅｒ　ＩｒＤＡ（ｏｂｊｅｃｔ　ｅｘｃｈａｎｇｅ　ｏｖｅｒ　ｉｎｆｒａｒｅｄ）、Ｂｌｕｅｔｏｏｔｈ、またはＵＳＢ（ユニバーサルシリアルバス）を使用して、接続されたデバイス経由でＲＩに接続することができるデバイス。

【００４４】

ユーザ　デバイスの人間ユーザ。ユーザは、デバイスを必ずしも所有しない。

【００４５】

図１は、既存のＯＭＡ　ＤＲＭ２．０機能アーキテクチャ１００の概略図である。アーキテクチャ１００は、ＤＲＭシステム１０２、コンテンツプロバイダ１０４、およびユーザ１０６から成る。ＤＲＭシステム１０２は、ＣＩ１１０、ＲＩ１１２、ＤＲＭエージェント１１４、ネットワークストア１１６、およびリムーバブルメディア１１８を含む。ＣＩ１１０は、保護されたコンテンツ１２２を配布し、ＲＩ１１２は、ＲＯ１２４を配布する。ＤＲＭエージェント１１４は、保護されたコンテンツ１２２を再配布する。

【００４６】

ＣＩ１１０は、ＤＲＭコンテンツ１２２を配信するエンティティである。ＯＭＡ　ＤＲＭは、ＤＲＭエージェント１１４に配信されるべきＤＲＭコンテンツ１２２のフォーマット、ならびにＤＲＭコンテンツ１２２が、様々なトランスポート機構を使用してＣＩ１１０からＤＲＭエージェント１１４にトランスポートされることが可能な仕方を定義する。ＣＩ１１０は、ＤＲＭコンテンツ１２２の実際のパッケージ化を自ら行っても、他の何らかの源からあらかじめパッケージ化されたコンテンツを受信してもよい。

【００４７】

ＲＩ１１２は、ＤＲＭコンテンツ１２２に許可および制約を割り当て、ＲＯ１２４を生成するエンティティである。ＲＯ１２４は、ＤＲＭコンテンツ１２２に関連する許可および制約を表現するＸＭＬドキュメントである。ＲＯ１２４は、ＤＲＭコンテンツ１２２がどのように使用されることが可能であるかを支配し、つまり、ＤＲＭコンテンツ１２２は、関連付けられたＲＯ１２４なしに使用されることが可能でなく、関連付けられたＲＯによって指定されるとおりにしか使用されることが可能でない。ＤＲＭコンテンツは、例えば、ＲＯが、時間有効期限（例えば、１０日）を有し、この時間有効期限の後、このコンテンツにアクセスするのに新たなＲＯが必要とされる場合、複数のＲＯに関連付けられることも可能である。

【００４８】

ＤＲＭエージェント１１４は、ＤＲＭコンテンツ１２２の消費時点の執行を管理することを担う論理的エンティティである。ＤＲＭエージェント１１４は、デバイスの信頼される構成要素を実体化し、デバイス上のＤＲＭコンテンツ１２２に関する許可および制約を執行すること、デバイス上のＤＲＭコンテンツ（ＤＲＭエージェントを介してしかアクセスすることができない）へのアクセスを制御することなどを担う。

【００４９】

ＤＲＭコンテンツ１２２は、配信される前に、許可のないアクセスからコンテンツ１２２を保護するようにパッケージ化される。ＣＩ１１０が、ＤＲＭコンテンツ１２２を配信し、ＲＩ１２２が、ＲＯ１２４を生成する。ＣＩ１１０およびＲＩ１１２は、システム１０２において、物理的エンティティではなく、論理的役割を実体化する。例えば、１つの展開において、コンテンツ所有者が、ＤＲＭコンテンツをあらかじめパッケージ化し、その後、このコンテンツが、ＣＩとＲＩの両方の役割をするコンテンツ配給元によって配布される。

【００５０】

ＲＯ１２４が、ＤＲＭコンテンツ１２２がどのように使用されることが可能であるかを支配する。ＤＲＭコンテンツ１２２は、関連付けられたＲＯ１２４なしに使用されること

が可能でなく、ＲＯ１２４の中で指定される許可および制約に従ってしか使用されることが可能でない。ＯＭＡ　ＤＲＭは、ＲＯからのＤＲＭコンテンツの論理的分離を行う。ＤＲＭコンテンツとＲＯは、別々に要求されても、一緒に要求されてもよく、別々に配信されても、同時に配信されてもよい。ＤＲＭコンテンツとＲＯは、同時に配信される場合、通常、ともに、ＣＩ１１０によって提供され、ＲＯおよびコンテンツは、ＤＣＦ（ＤＲＭコンテンツフォーマット）に埋め込まれる。

【００５１】

ＲＯ１２４は、鍵のセットによって、或る特定のＤＲＭエージェント１１４に暗号上、結び付けられて、その特定のＤＲＭエージェント１１４だけが、ＲＯ１２４にアクセスすることができるようにされる。ＤＲＭコンテンツ１２２は、有効なＲＯ１２４を使用してしかアクセスすることができず、したがって、コンテンツ１２２は、自由に配布される、またはスーパ配布されることが可能である。

【００５２】

ＯＭＡ　ＤＲＭ２．０は、１つのＲＯが、ＤＲＭエージェントのグループに結び付けられることを許す。そのようなグループは、ドメインと呼ばれる。或るドメインに配布されたＤＲＭコンテンツおよびＲＯは、そのドメインに属するすべてのＤＲＭエージェントによってオフラインで共有され、アクセスされることが可能である。例えば、ユーザは、ユーザの電話機とユーザのＰＤＡの両方で使用するためにＤＲＭコンテンツを購入することができる。

【００５３】

ＯＭＡ　ＤＲＭ仕様は、ＤＲＭコンテンツのためのフォーマットおよび保護機構（つまり、ＤＣＦ）、ＲＯのためのフォーマット（ＲＥＬ（権利表現言語））および保護機構、暗号鍵の管理のためのセキュリティモデルを定義する。また、ＯＭＡ　ＤＲＭ仕様は、ＤＲＭコンテンツおよびＲＯが、プル（ＨＴＴＰプル、ＯＭＡダウンロード）、プッシュ（ＷＡＰプッシュ、ＭＭＳ）、およびストリーミングを含む一連のトランスポート機構を使用して、どのようにデバイスにトランスポートされることが可能であるかも定義する。しかし、ＯＭＡ　ＤＲＭ仕様は、ネットワークエンティティ間、例えば、ＣＩ１１０とＲＩ１１２の間の対話を全く扱わない。

【００５４】

以下は、ＯＭＡ　ＤＲＭ２．０仕様が範囲に含む使用事例の網羅的ではないリストである。

【００５５】

１．基本プルモデル

【００５６】

ユーザは、Ｗｅｂサイトにブラウズして行くことによって、ダウンロードすべきコンテンツを選択し、購入の条件を確認する。ＣＩ１１０は、コンテンツ１２２を識別し、保護する、すなわち、コンテンツ１２２をパッケージ化する。コンテンツ１２２は、ＣＥＫ（コンテンツ暗号化鍵）を使用して暗号化される。デバイス能力が、公示されたＭＩＭＥタイプサポートなどを使用して検出されることが可能である。ＲＩ１１２が、コンテンツ１２２およびターゲットＤＲＭエージェント１１４に関するＲＯ１２４を生成する。ＲＯ１２４は、コンテンツトランザクションに関する許可、およびＣＥＫを含む。最期に、ＲＯ１２４は、暗号化（ＲＯ暗号化鍵、つまり、ＲＥＫを使用する）およびデジタル署名によって暗号で保護され、ターゲットＤＲＭエージェント１１４だけに結び付けられる。次に、ＤＲＭコンテンツ１２２および保護されたＲＯ１２４が、ＤＲＭエージェント１１４に配信される。

【００５７】

２．ＤＲＭコンテンツのプッシュ

【００５８】

代替の配布モデルは、先行する発見プロセスなしに、ＭＭＳ（マルチメディアメッセージングサービス）、ＷＡＰプッシュ、または類似した方法を使用して、デバイスにコンテ

ンツを直接にプッシュすることである。この使用事例の２つの変種が存在する。
【００５９】
２Ａ．コンテンツプッシュ
【００６０】
ＣＩ１１０および／またはＲＩ１１２は、或るユーザ、および或る特定のＤＲＭエージェント１１４のいくらかの事前の知識を有することが可能であり、したがって、コンテンツ１２２およびＲＯ１２４は、配信のためにフォーマットされ、パッケージ化されることが可能である。
【００６１】
２Ｂ．プッシュによって開始されるプル
【００６２】
この場合、ＣＩ１１０および／またはＲＩ１１２は、ユーザ、またはユーザのＤＲＭエージェント１１４についての事前の知識を全く有さないことが可能であるが、それでも、例えば、ユーザが、コンテンツを購入するようにユーザの気を引くコンテンツ１２２をプレビューすることを可能にするように、コンテンツを配信することを望む可能性がある。ＤＲＭコンテンツ１２２をユーザに直接にプッシュする代わりに、このコンテンツへのリンク、またはこのコンテンツのプレビューへのリンクが、送信されることが可能である。このリンクをたどることにより、ユーザは、或る特定のロケーションに連れて行かれ、その後、手続きは、基本プルモデルにおけるとおりに進む。
【００６３】
３．ＤＲＭコンテンツのストリーミング
【００６４】
基本プル使用事例とプッシュ使用事例はともに、コンテンツの全体がパッケージ化され、配信されるものと想定する。代替として、コンテンツは、ストリームとしてパケット化されて、配信されてもよい。この場合、ストリーム自体が保護される（暗号化される）。暗号化の厳密なフォーマットは、ＯＭＡ　ＤＲＭの範囲外とされており、既存の暗号化標準から選択されることが可能である。これらのストリームは、可能なパケット損失などに対処するように、ダウンロードに関してＯＭＡによって規定される暗号化スキームとは異なる暗号化スキームを使用して保護されてもよい。しかし、ストリームが暗号化された後、ストリームへのアクセスは、離散的コンテンツに関して前段で説明したのと同一の手続きを介して制御されることが可能である。ＲＯが生成され、ストリーム暗号化鍵が、ＣＥＫと同様にＲＯの中に入れられ、次に、このＲＯが、ＤＲＭエージェントと暗号上、結び付けられる。
【００６５】
４．ドメイン
【００６６】
ドメインは、オプションのフィーチャであり、すべてのＲＩによってサポートされるわけではない可能性がある。ドメインは、ＲＯとＣＥＫが或る特定のＤＲＭエージェント１１４に結び付けられるＯＭＡ　ＤＲＭ２．０の基本モデルを拡張し、ＲＩ１１２が、権利およびＣＥＫを、単一のＤＲＭエージェントだけにではなく、ＤＲＭエージェントのグループに結び付けることを許す。すると、ユーザは、同一のドメインに属するすべてのＤＲＭエージェントの間で、ＤＲＭコンテンツ１２２をオフラインで共有することができる。ＲＩ１１２は、ドメイン概念を使用して、ユーザが所有するいくつかのデバイスから、ユーザがＤＲＭコンテンツ１２２にアクセスすることができるようにすることなどの、新たなサービスを提供する、あるいはユーザが、１つのデバイス（例えば、ＰＣ）を介して、別のデバイス（例えば、ポータブルプレーヤ）上で後に使用するために、ＤＲＭコンテンツおよび権利を購入する場合、接続されていないデバイスのサポートを提供することができる。
【００６７】
５．バックアップ

【００６８】
ＤＲＭコンテンツ１２２は、リムーバブルメディア１１８上に、ネットワークストア１１６の中に、または他の何らかの形態のストレージの中に格納されることが可能である。ＤＲＭコンテンツ１２２は、暗号化された形態で格納され、関連付けられたＲＯ１２４を使用する或る特定のターゲットＤＲＭエージェント１１４によってしかアクセスされることが可能でない。ＲＯ１２４は、ＲＯが、状態のない許可だけしか含まない場合、バックアップの目的で格納されることが可能である。セキュリティモデルが、ＲＯ１２４がオフデバイスで格納される場合でさえ、ＲＯ１２４が保護されて、意図されるＤＲＭエージェント１１４によってしかアクセスされることが可能でないことを確実にする。一部の許可は、ＤＲＭエージェント１１４による状態、例えば、限られた回数の再生の保持を要求する。そのようなＲＯは、オフデバイスで格納されることが、そうすることにより、状態情報が失われることになる可能性があるので、可能でない。

【００６９】
６．スーパ配布

【００７０】
ＤＲＭコンテンツ１２２は、コピーされて、他のＤＲＭエージェント１１４に転送されること、例えば、ユーザが、ＤＲＭコンテンツ１２２を友人に送信することが可能である。友人は、コンテンツ１２２にアクセスするために、ＤＲＭコンテンツパッケージの中のリンクを介してＲＩ１１２に連れて行かれて、ＲＯ１２４を獲得する。

【００７１】
７．エクスポート（非ＯＭＡ　ＤＲＭシステムへの）

【００７２】
ＤＲＭコンテンツ１２２は、ＯＭＡ　ＤＲＭ準拠ではないが、他の何らかのＤＲＭ機構をサポートするデバイス上で使用されるように、他のＤＲＭシステムにエクスポートされることが可能である。ＯＭＡ　ＤＲＭアーキテクチャは、ＲＩ１１２が、所望する場合、別の特定ＤＲＭシステムへの変換を、ＤＲＭエージェント１１４が、場合により、その別のＤＲＭシステムによって指定されるとおり実行する、許可を表明することを許す。ＲＩ１１２は、特定の外部ＤＲＭシステムだけに、このエクスポートを制限することができる。

【００７３】
８．接続されていないデバイスのサポート

【００７４】
ＯＭＡ　ＤＲＭは、接続されていないデバイスがコンテンツ１２２およびＲＯ１２４を購入して、ダウンロードするのを助ける仲介役の働きを、接続されたデバイスがすることを可能にする。ユーザが、例えば、ネットワーク接続を全く有さないＯＭＡ　ＤＲＭに準拠するポータブルデバイス（接続されていないデバイス）と、ネットワーク接続を有するＯＭＡ　ＤＲＭに準拠する移動デバイス（接続されたデバイス）とを有することが可能である。接続されたデバイスを使用して、ＤＲＭコンテンツ１２２をブラウズして、購入し、ＤＲＭコンテンツ１２２を、接続されたデバイスにダウンロードした後、ユーザは、次に、接続されていないデバイス上でＤＲＭコンテンツ１２２を再生することを所望することが可能である。この場合、接続されたデバイス上のＤＲＭエージェント１１４は、ＲＩ１１２からドメインＲＯ１２４を要求して、ダウンロードする。

次に、接続されたデバイス上のＤＲＭエージェント１１４は、ＤＣＦの中にドメインＲＯ１２４を埋め込む。次に、このＤＣＦが、ローカル接続技術を介する適切なプロトコル、例えば、ＢｌｕｅｔｏｏｔｈまたはＵＳＢを使用して、接続されていないデバイスに転送されることが可能である。接続されたデバイスと接続されていないデバイスの両方が、ＯＭＡ　ＤＲＭ準拠であって、この機能をサポートしなければならない。また、接続されていないデバイスは、接続されたデバイスと同一のドメインに属さなければならない。

【００７５】
セキュリティおよび信頼

【００７６】
以下は、ＯＭＡ　ＤＲＭ２．０のセキュリティ方策および信頼方策の概要である。一般に、いずれのＤＲＭソリューションも、以下の２つのセキュリティ要件を満たす必要がある。すなわち、（１）保護されたコンテンツは、適切に認証され、許可されたＤＲＭエージェントによってだけアクセスされなければならず、さらに（２）保護されたコンテンツ上の許可は、すべてのＤＲＭエージェントによって遵守されなければならない。ＤＲＭコンテンツに関連する許可および制約の執行は、任意のＤＲＭスキームのセキュリティ方策および信頼方策の主要な関心事である。関連付けられたＲＯによって規定されるものを超えたＤＲＭコンテンツへの許可のないアクセス、不正なコピーの作成、およびＤＲＭコンテンツの再配布が、いずれのＤＲＭシステムにも主な脅威を成す。

【００７７】
ＯＭＡ　ＤＲＭシステムは、ＯＭＡ環境における保護されたコンテンツのセキュリティで保護された配布および管理のための手段を提供し、前段で規定された要件を満たす。ＯＭＡ　ＤＲＭは、ＲＯの制約下におけるコンテンツの保護された使用を確実にするＤＲＭエージェントを使用することによって、消費時点でコンテンツおよびＲＯの使用および保護を執行する。

【００７８】
ＤＲＭコンテンツを配布するための基本ステップは、以下のとおり要約されることが可能である。すなわち、

【００７９】
１．コンテンツパッケージ化。コンテンツは、セキュリティで保護されたコンテンツコンテナ（ＤＣＦ）の中にパッケージ化される。ＤＲＭコンテンツは、対称ＣＥＫ（コンテンツ暗号化鍵）を使用して暗号化される。コンテンツは、あらかじめパッケージ化されることが可能であり、すなわち、コンテンツパッケージ化は、オンザフライで行われなくてもよい。同一のＣＥＫが、コンテンツのすべてのインスタンスに関して使用されるわけではなく、ただし、このことは、ＯＭＡ　ＤＲＭにおける要件ではない。

【００８０】
２．ＤＲＭエージェント認証。すべてのＤＲＭエージェントが、一意の秘密鍵／公開鍵ペアと、証明書とを有する。証明書は、デバイス製造業者、デバイスタイプ、ソフトウェアバージョン、通し番号などのさらなる情報を含む。このことは、ＣＩおよびＲＩが、ＤＲＭエージェントをセキュリティで保護された仕方で認証することを可能にする。

【００８１】
３．ＲＯ生成。ＲＯは、ＤＲＭコンテンツが、関連付けられたＲＯなしに使用されることが可能でないことを確実にするＣＥＫを含む。ＲＯは、許可（例えば、再生、表示、および実行）および制約（例えば、１ヶ月間、再生する、１０分間、表示する）から成る。また、ＲＯは、コンテンツにアクセスが行われる際に、或るユーザが居合わせること（例えば、ユーザの身元によって判定される）を要求する制約を含むことも可能である。これらの許可および制約、ならびにＲＯに実体化される他の情報（例えば、著作権情報）は、ユーザに提示されることが可能である。

【００８２】
４．ＲＯ保護。ＲＯを配信する前に、ＲＯのセンシティブな部分（ＣＥＫなどの）が、ＲＥＫ（権利暗号化鍵）を使用して暗号化され、次に、このＲＯが、ターゲットＤＲＭエージェントに暗号上、結び付けられる。このことにより、ターゲットＤＲＭエージェントだけが、ＲＯ、ＣＥＫ、およびＤＲＭコンテンツにアクセスすることができることが確実にされる。さらに、ＲＩが、ＲＯにデジタルで署名する。また、ＲＯは、ＣＥＫを含めることによって、ＤＲＭへのアクセスを支配する。ＯＭＡ　ＤＲＭ　ＲＥＬ（権利表現言語）が、ＤＲＭコンテンツの使用を支配する許可および制約のシンタックス（ＸＭＬ）およびセセマンティックスを規定する。ＲＯは、ＲＯ独自のＭＩＭＥコンテンツタイプを有する。

【００８３】

５．配信。次に、ＲＯおよびＤＣＦは、ターゲットＤＲＭエージェントに配信されることが可能である。両方のアイテムは、本来的にセキュリティで保護されているので、任意のトランスポート機構（例えば、ＨＴＴＰ／ＷＳＰ、ＷＡＰプッシュ、ＭＭＳ）を使用して配信されることが可能である。ＲＯとＤＣＦは、例えば、ＭＩＭＥ複数パートメッセージの中で、一緒に配信されることも、別々に配信されることも可能である。

【００８４】

ＲＯに関するＯＭＡ　ＤＲＭ信頼モデルは、双方によって認識され、信頼される主役のグループ、検証者、および１つまたは複数の認証機関が存在する、ＰＫＩ（公開鍵インフラストラクチャ）に基づく。単一のエンティティが、選択されたコンテキストおよびソリューションのニーズに応じて、主役の役割をすることも、検証者の役割をすることもできる。ＰＫＩは、検証者と主役が、開かれた、セキュリティで保護されていないネットワークを介して通信する際に、検証者が、主役の身元、およびその他の属性を認証することを可能にする。そのようなシステムにおいて、通常、検証者は、認証の目的で、検証者が対話する相手の主役についてのセンシティブな情報を全く保持する必要はない。さらに、ＣＡ（証明機関）は、主役と検証者の間のトランザクションに直接に関与していない。ＲＩは、ＤＲＭエージェントの証明書が、ＲＩによって検証可能であり、取り消されていない場合、ＤＲＭエージェントが正しく振る舞うことを信頼する。同様に、ＤＲＭエージェントは、ＲＩの証明書が、ＤＲＭエージェントによって検証可能であり、取り消されていない場合、ＲＩが正しく振る舞うことを信頼する。

【００８５】

ＯＭＡ　ＤＲＭに適用されるＰＫＩの主なエンティティは、ＣＡ、デバイス、およびＲＩである。ＯＭＡ　ＤＲＭの認証プロトコルおよび鍵転送プロトコルは、ＲＩが、デバイスを認証することができ、デバイスが、ＲＩを認証することができることを要求する。そのような相互認証は、ＲＯＡＰによって達せられる。

【００８６】

さらに、デバイスは、デバイス公開鍵およびデバイス秘密鍵、ならびに適切なＣＡによって署名された関連する証明書を備えさせられる（製造時に、または後に）ものと想定される。ＲＩによって表明される証明書選好に基づき、デバイスは、適切な証明書を提供しなければならない。デバイスは、完全性および機密性の保護を有するローカルストレージの中に秘密鍵を格納することを要求される。

【００８７】

また、ＲＩも、公開鍵、秘密鍵、およびＣＡによって署名された証明書を与えられる。証明書チェーン（１つのＣＡによって署名された公開鍵所有者の証明書と、他のＣＡによって署名されたＣＡの０、または１つ以上のさらなる証明書とを含む複数の証明書のチェーン）は、信頼の証明書チェーンの検証のための認証プロトコルの時点で、デバイスに提示される。

【００８８】

複数のＣＡが、ＤＲＭシステム内に存在することが可能であることに留意されたい。ＲＯＡＰプロトコルは、ＲＩ証明書に署名するＣＡが、プロトコルの実行中に使用するために、ＯＣＳＰ（オンライン証明書ステータスプロトコル）レスポンダを実行することを要求する。また、ＣＡは、発行された証明書の使用を支配する適切な証明書ポリシーを定義することも要求される。

【００８９】

以下は、ＯＭＡ　ＤＲＭセキュリティの主な態様を説明する。

【００９０】

１．データが、許可のないパーティによってアクセスされることが可能でないことを確実にする機密性。前述したとおり、保護されたコンテンツは、適切に認証され、許可されたＤＲＭエージェントによってだけアクセス可能でなければならない。この目標を達するのに、保護されたコンテンツは、暗号化される。暗号化鍵は、各メディアオブジェクトに一意であり、ＲＯが、意図される受信者によってしかアクセス可能でない鍵の中にラップ

された暗号化鍵を担持する。

【００９１】

２．或るパーティが、別のパーティに自らの身元を明かすプロセスである認証。ＯＭＡ ＤＲＭにおいて、相互ＤＲＭエージェント－ＲＩ認証が、４パス登録プロトコル、２パスＲＯ獲得プロトコル、および２パスドメイン参加プロトコルにおいて達せられる。使用されるプロトコル、および送信されるメッセージに依存して、認証は、ナンス上、またはタイムスタンプ上のデジタル署名を介して達せられる。１パスＲＯ獲得プロトコルは、タイムスタンプ上のデジタル署名を介してＲＩ認証を実現する。１パスＲＯ獲得プロトコルは、ＲＩに対してＤＲＭエージェントを認証しないが、保護されたコンテンツが、受信者の公開鍵でラップされることにより、認証は、鍵結び付けを介して間接的に行われる。２パスドメイン退去プロトコルは、タイムスタンプ上のデジタル署名を介して、ＲＩに対してＤＲＭエージェントを認証する。２パスドメイン退去プロトコルは、ＤＲＭエージェントに対してＲＩを認証しない。ＲＩは、ＲＯの配信中にＤＲＭエージェントに対して自らを認証することを要求される。このことにより、ＲＩの真正性について或る程度の保証が提供される。

【００９２】

３．データ完全性保護は、データの許可のない変更を検出する能力を確実にする。ＯＭＡ ＤＲＭにおいて、データ完全性保護は、適宜、ＲＯＡＰメッセージ上、およびＲＯ上のデジタル署名を介して達せられる。

【００９３】

４．鍵確認は、保護された鍵を含むメッセージの受信者に、メッセージ送信者が鍵値を知っていることを保証する。ＤＲＭコンテキストにおいて、この特性は、或るＲＩからのＲＯを、別のＲＩが許可なく再発行することを防止する。ＯＭＡ ＤＲＭシステムにおいて、鍵確認は、保護された鍵の諸部分をＭＡＣ鍵として使用することによる、保護された鍵、および送信するパーティの身元に対するＭＡＣ（メディアアクセス制御）を介して達せられる。

【００９４】

ＤＲＭエージェントは、正しい振舞いと、セキュリティで保護された実施の両方の点で、ＲＩによって信頼されなければならない。ＯＭＡ ＤＲＭにおいて、各ＤＲＭエージェントは、そのＤＲＭエージェントを識別し、そのエージェントと鍵ペアとの間の結び付きを証明する、一意の鍵ペア、および関連する証明書を備えさせられる。このことにより、ＲＩは、標準のＰＫＩ手続きを使用してＤＲＭエージェントをセキュリティで保護された仕方で認証することが可能になる。

【００９５】

証明書の中の情報は、ＲＩが、ビジネス規則、コンテンツの価値などに基づいて、ポリシーを適用することを可能にする。例えば、ＲＩは、或る製造業者を信頼することが可能であり、あるいはＲＩによって定義されたいくつかの基準に従って信頼されるべき、または信頼されるべきでないことが知られているＤＲＭエージェントの更新されたリストを保持することが可能である。

【００９６】

ＤＣＦ（ＤＲＭコンテンツフォーマット）は、独自のＭＩＭＥコンテンツタイプを有する、暗号化されたコンテンツに関するセキュリティで保護されたコンテンツパッケージである。暗号化されたコンテンツに加え、ＤＣＦは、コンテンツ記述（元のコンテンツタイプ、ベンダ、バージョンなど）、ＲＩ ＵＲＩ（ユニフォームリソース識別子）（ＲＯが獲得されることが可能なロケーション）などのさらなる情報を含む。このさらなる情報は、暗号化されず、ＲＯが取得される前にユーザに提示されることが可能である。ＤＣＦ内のＤＲＭコンテンツをアンロックするのに必要とされるＣＥＫは、ＲＯ内に含まれる。このため、ＲＯなしにＤＲＭコンテンツにアクセスすることは可能でなく、ＤＲＭコンテンツは、ＲＯの中で規定されたとりにしか使用されることが可能でない。ＯＭＡ ＤＲＭは、ＤＲＭエージェントが、ＤＣＦの完全性を検証することを可能にして、許可のないエン

ティティによるコンテンツの変更を防止する機構を含む。

【００９７】

ＯＭＡ　ＤＲＭシステムは、ＤＲＭエージェントの中にＤＲＭ時間が存在することを想定する。ユーザは、ＤＲＭ時間を変更することができないので、ＤＲＭ時間が、ＯＣＳＰレスポンダによって保持される時間と同期されることが可能な機構が、定義される。いくつかの制約（例えば、絶対時間制約）、ならびにＲＯに関する配信プロトコルのいくつかの態様は、セキュリティで保護された時間源を有するＤＲＭエージェントに依拠する。ＯＭＡ　ＤＲＭ仕様のコンテキストにおけるＤＲＭ時間は、正確な時間、ならびにユーザが変更することが可能でない時間値を意味する。ＯＭＡ　ＤＲＭ仕様は、ＤＲＭ時間が、必要な際、例えば、ＤＲＭ時間が、長い停電の後に失われた場合、同期される機構を提供する。一部の限られた能力の接続されていないデバイスは、リアルタイムのクロックをサポートしないことが可能であり、このため、ＤＲＭ時間をサポートしない可能性がある。しかし、接続されたデバイスは、ＤＲＭ時間をサポートしなければならない。

【００９８】

ＯＭＡ　ＤＲＭは、ＲＯリプレー保護攻撃を防止する。ＲＯリプレー攻撃の例は、中間者が、ＤＲＭエージェントへの配信中に、限られた回数の実行でＲＯを傍受する場合である。ＤＲＭエージェント上で権利が失効した際、この傍受されたＲＯが、中間者から再び配信される（リプレーされる）可能性がある。ＯＭＡ　ＤＲＭは、このこと、および類似した攻撃が行われることを防ぐ。

【００９９】

ＯＭＡ　ＤＲＭシステムは、前段で列挙したセキュリティ機構の使用を介してアプリケーション層セキュリティを提供する。このため、ＯＭＡ　ＤＲＭシステムは、トランスポート層セキュリティに依拠しない、またはトランスポート層セキュリティを前提としない。

【０１００】

ＲＯＡＰは、ＯＭＡ　ＤＲＭ２．０において、ＲＯに関する情報のセキュリティで保護された認証ベースの交換を可能にすることに中心的な役割を果たす。ＲＯＡＰは、ＲＩと、デバイス内のＤＲＭエージェントとの間のＤＲＭセキュリティプロトコルスイートを表す一般的な名前である。このプロトコルスイートは、以下のいくつかのサブプロトコルを含む。すなわち、

【０１０１】

１．図２に示される、ＲＩにデバイスを登録するための４パスプロトコル。

【０１０２】

２．図３に示される、ＲＯの要求および配信を含む２パスＲＯ獲得プロトコル。

【０１０３】

３．１パスＲＯ獲得プロトコルは、図４に示されるとおり、ＲＩからデバイスへのＲＯの配信（例えば、メッセージング／プッシュ）と関係する。

【０１０４】

４．図５に示される、デバイスがドメインに参加する２パスドメイン参加プロトコル。

【０１０５】

５．図６に示される、デバイスがドメインを退去する２パスドメイン退去プロトコル。

【０１０６】

図２は、４パス登録プロトコル２００の流れ図である。プロトコル２００は、デバイス２０２、ＲＩ２０４、およびＯＣＳＰレスポンダ２０６を利用する。デバイス２０２は、デバイスＩＤ（ＲＩ２０４が、ＯＣＳＰレスポンダ２０６に後に確認をとることができるデバイスの証明書のハッシュ）、およびその他の情報などの情報を含む、デバイスハローメッセージを送信すること（ステップ２１０）によって、ＲＩ２０４との連絡を開始する（場合により、ＲＯＡＰトリガを受信した後）。テーブル１は、デバイスハローメッセージの主な構成要素を示す。デバイスハローメッセージの中の情報のいずれも、完全性保護されておらず、すなわち、このメッセージに関する署名は、存在しない。

【０１０７】
【表１】
表1 デバイスハローメッセージのフォーマット

パラメータ	必須またはオプション	メモ
バージョン	必須	ROAPによってサポートされる最高のROAPバージョン番号の<major.minor>表現。この値は、OMA DRM v2.0の場合、1.0である。デバイスは、指定されるバージョンを含む以前のすべてのバージョンをサポートしなければならない。
デバイスID	必須	現在、定義されている唯一のIDは、証明書の中に現れる、デバイスの公開鍵情報のSHA-1ハッシュ(すなわち、デバイス証明書の中の完全なDER(Distinguished Encoding Rules)によって符号化されたSubjectPublicKeyInfo構成要素)である。デバイスが、複数の鍵を保持する場合、デバイスは、これらの公開鍵の1つまたは複数を選択し、対応するデバイスIDを送信することができる。
サポートされるアルゴリズム	オプション	一般的なURIによって識別される暗号アルゴリズム(ハッシュ、MAC、署名、鍵トランスポート、鍵ラップ)を識別する。すべてのデバイスおよびRIが、OMA DRM 2.0において指定されるアルゴリズムをサポートしなければならない。
拡張子	オプション	デバイスが、RIが、デバイス証明書情報を格納したか否かという情報をRIコンテキストの中に格納する能力をデバイスが有することを、RIに示す証明書キャッシング。実際のストレージ標識は、デバイスの公開鍵指示に関するピア鍵識別子によって行われる。

【０１０８】
ＲＩ２０４は、デバイスハローメッセージに応答して（ステップ２１０）、ＲＩの証明書資格情報（ＲＩ　ＩＤの形態の）、いくつかのセッション関連の（リプライ防止目的の）ナンスおよびセッション番号、ならびにＲＩ２０４が認識するデバイスについての信頼チェーンに関する情報などの他のオプションの情報などの情報を含む、ＲＩハローメッセージをデバイス２０２に送信する（ステップ２１２）。テーブル２は、ＲＩハローメッセージのフォーマットを示す。ＲＩハローメッセージの中の情報のいずれも、完全性保護されていないことに留意されたい。
【０１０９】

【表２】

表2 RIハローメッセージのフォーマット

パラメータ	ROAP-RIハロー		メモ
	ステータス=「成功」	ステータス「成功」でない	
ステータス	必須	必須	デバイスハローメッセージ処理が成功したか否かを示す。
セッションID	必須	-	RIによって設定されたプロトコルセッションID。
選択されたバージョン	必須	-	(デバイスによって示唆されるROAPバージョン、RIによってサポートされる最高のROAPバージョン)の最低。
RI ID	必須	-	現在、定義される唯一のIDは、RIの証明書の中に現れる、RIの公開鍵情報のハッシュである。RIが、複数の鍵を保持する場合、RIは、1つの鍵だけを選択しなければならない。
選択されたアルゴリズム	オプション	-	後続のROAP対話において使用されるべき暗号アルゴリズム。
RIナンス	必須	-	RIによって送信されるランダムなナンス。
信頼されるデバイス権限	オプション	-	RIによって認識されるデバイス信頼アンカのリスト。このリストは、RIが、デバイス証明書を既に有する場合、またはそれ以外でデバイスを信頼することができる場合、送信されない。
サーバ情報	オプション	-	デバイスが、登録要求メッセージの中で、後に変更なしに戻さなければならない<=512バイトのサーバ特有の情報。デバイスは、この情報を解釈しようと試みてはならない。
拡張子	オプション	-	ピア鍵識別子、証明書キャッシング、デバイス詳細:これを含めることによって、RIは、後の登録要求メッセージの中でデバイス特有の情報(製造業者、モデルなど)を戻すよう、デバイスに要求する。

【０１１０】

ＲＩハローメッセージの中に含まれる情報の検証が成功すると、デバイス２０２は、要求時間、セッションＩＤ、および署名などの必須の情報と、証明書チェーン、信頼されるＲＩ権限アンカ、拡張子などのオプションの情報とを含む登録要求メッセージを送信する

（ステップ２１４）。テーブル３は、登録要求メッセージのフォーマットを示す。登録要求メッセージは、末尾において、登録要求メッセージの中の署名フィールドまでの、デバイス２０２とＲＩ２０４の間で交換されるすべてのメッセージの、すなわち、デバイスハローメッセージ全体、ＲＩハローメッセージ全体、および署名フィールドまでの（このフィールドを除く）登録要求メッセージのフィールドのデジタル署名を含む。このデジタル署名は、デバイスの秘密鍵を使用して作成される。このデジタル署名を含めることにより、関連するＲＯＡＰメッセージのいくらかの完全性保護がもたらされる。

【０１１１】

【表３】

表3 登録要求メッセージのフォーマット

パラメータ	登録要求	メモ
セッションID	必須	RIハローメッセージの中のセッションIDと同一。同一でない場合、RIは、登録プロトコルを終了させる。
デバイスナンス	必須	デバイスによって選択されたナンス。
要求時間	必須	デバイスによって測定される現在のDRM時間。
証明書チェーン	オプション	証明書チェーンは、デバイスの証明書を含むが、ルート証明書は含まない。証明書チェーンは、RIハローメッセージが、ピア鍵識別子拡張子を含んでおり、その拡張子の値が、デバイスの現在の証明書の中の鍵を識別しているのでない限り、存在する。RIが、RIハローメッセージの中で信頼アンカ選好を示した場合、デバイスは、デバイス証明書、ならびにRIによって示される信頼アンカの1つまで戻るように連鎖するチェーンを選択しなければならない。
信頼されるRI権限	オプション	デバイスによって認識されるRI信頼アンカのリスト。空である場合、このリストは、RIが、任意の証明書を自由に選択できることを示す。
サーバ情報	オプション	サーバ情報パラメータが、RIハローメッセージの中に存在していた場合に限り、存在(しなければならない)。存在する場合、このフィールドは、RIハローメッセージの場合と同一でなければならない。
拡張子	オプション	ピア鍵識別子、OCSP応答なし、OCSP応答鍵識別子、デバイス詳細(製造業者、モデル、バージョン)。
署名	必須	この署名要素を除き、プロトコルにおいてそれまでに送信されたデータのSHA-1ハッシュ。デバイスの秘密鍵を使用して行われる。

【０１１２】

デバイス２０２が、拡張子の中の情報を介して、ＯＣＳＰ検証が必要ない、またはサポートされないことを示すのでない限り、ＲＩ２０４は、デバイス２０２によってＲＩ２０４に供給される情報の検証を要求するＯＣＳＰ要求メッセージをＯＣＳＰレスポンダ２０６に送信する（ステップ２１６）。ＯＣＳＰレスポンダ２０６は、要求メッセージの中でこの情報を探して、この情報を検証し、要求の結果を含むＯＣＳＰ応答メッセージを戻そ

うと試みる（ステップ２１８）。

【０１１３】

ＲＩ２０４は、登録が成功したか、失敗したかという指示、ならびに他の情報を含む登録応答メッセージをデバイス２０２に送信する。テーブル４は、登録応答メッセージのフォーマットを示す。登録応答メッセージは、末尾に、登録要求メッセージおよび登録応答メッセージのＳＨＡ－１ハッシュ（署名フィールドまでの、署名フィールドを除く）を含む。このデジタル署名は、ＲＩの秘密鍵を使用して行われる。デジタル署名を含めることにより、関連するＲＯＡＰメッセージのいくらかの完全性保護がもたらされる。ＳＨＡ－１ハッシュが、このデジタル署名に関して使用されるが、デジタル署名を適用するための任意の適切なアルゴリズムが使用されることが可能であることに留意されたい。

【０１１４】

【表４】

表4 登録応答メッセージのフォーマット

パラメータ	登録応答		メモ
	ステータス=「成功」	ステータス「成功」でない	
ステータス	必須	必須	デバイスハローメッセージ処理が成功したか否かを示す。
セッションID	必須	-	RIによって設定されたプロトコルセッションID。
選択されたバージョン	必須	-	(デバイスによって示唆されるROAPバージョン、RIによってサポートされる最高のROAPバージョン)の最低。
RI ID	必須	-	現在、定義される唯一のIDは、RIの証明書の中に現れる、RIの公開鍵情報のハッシュである。RIが、複数の鍵を保持する場合、RIは、1つの鍵だけを選択しなければならない。
選択されたアルゴリズム	必須	-	後続のROAP対話において使用されるべき暗号アルゴリズム。
RIナンス	必須	-	RIによって送信されるランダムなナンス。
信頼されるデバイス権限	オプション	-	RIによって認識されるデバイス信頼アンカのリスト。このリストは、RIが、デバイス証明書を既に有する場合、またはそれ以外でデバイスを信頼することができる場合、送信されない。
サーバ情報	オプション	-	デバイスが、登録要求メッセージの中で、後に変更なしに戻さなければならない<=512バイトのサーバ特有の情報。デバイスは、この情報を解釈しようと試みてはならない。
拡張子	オプション	-	ピア鍵識別子、証明書キャッシング、デバイス詳細:これを含めることによって、RIは、後の登録要求メッセージの中でデバイス特有の情報(製造業者、モデルなど)を戻すよう、デバイスに要求する。
署名	必須	-	SHA-1が、RIの秘密鍵を使用して、登録要求メッセージおよび登録応答メッセージ(署名フィールドを除く)について有する。

【０１１５】

図３は、２パスＲＯ獲得プロトコル３００の流れ図である。プロトコル３００は、デバイス２０２およびＲＩ２０４を利用し、４パス登録プロトコル２００が完了して、デバイス２０２が、ＲＩ２０４についての有効な証明書チェーンを受信した後に機能する。プロトコル３００は、デバイス２０２によって、ＲＩ２０４からＲＯを要求するのに使用される。デバイス２０２は、ＲＯ要求メッセージをＲＩ２０４に送信して、ＲＯを要求する（ステップ３１０）。テーブル５は、ＲＯ要求メッセージのフォーマットを示す。ＲＯ要求メッセージは、メッセージのデジタル署名（署名フィールドを除く）を含む。

【０１１６】

【表５】

表5 RO要求メッセージのフォーマット

パラメータ	ROAP-RO要求 必須/ オプション	メモ
デバイスID	M	要求するデバイスを識別する。
ドメインID	O	存在する場合、ドメインを識別する。
RI ID	M	許可するRI ID。登録応答メッセージの場合と同一の値。
デバイスナンス	M	デバイスによって選択されたナンス。
要求時間	M	デバイスに見える現在のDRM時間。
RO情報	M	要求されるROのIDとともに、デバイスがDCFを保有する場合、DCFのオプションのハッシュ。
証明書チェーン	O	デバイスが必要な証明書情報を有することを、RIコンテキストが示すのでない限り、送信される。デバイスの証明書を含まなければならない。
拡張子	O	ピア鍵識別子、OCSP応答なし、OCSPレスポンダ鍵識別子、トランザクションID。
署名	M	署名要素なしのRO要求メッセージのSHA-1ハッシュ。

【０１１７】

ＲＩ２０４は、要求メッセージに応答して、デバイス２０２にＲＯ応答メッセージを送信する（ステップ３１２）。ＲＯ応答メッセージは、ＲＯを含む、またはＲＯが送信されないという指示を含む。

【０１１８】

テーブル６は、ＲＯ応答メッセージのフォーマットを示す。ＲＯ応答メッセージは、成功した状態の場合、署名フィールドを除くＲＯ要求メッセージおよびＲＯ応答メッセージのＳＨＡ－１ハッシュであるデジタル署名を含む。

【０１１９】

【表６】

表6 RO応答メッセージのフォーマット

パラメータ	2パス成功	2パス成功ではない	メモ
ステータス	M	M	要求が処理されることが成功したか否かを示す。
デバイスID	M	-	デバイスハローメッセージの場合と同一の仕方で、要求するデバイスを識別する。この値は、RO要求メッセージの場合と同一でなければならない。同一でない場合、終了しなければならない。
RI ID	M	-	RIを識別し、RO要求メッセージの中のRI IDと等しくなければならない。
デバイスナンス	M	-	RO要求メッセージの場合と同一の値を有さなければならない。
保護されたRO	M	-	センシティブな情報(CEKなどの)が暗号化されたRO。
証明書チェーン	O	-	登録応答メッセージの場合と同一。
OCSP応答	O	-	RIの証明書チェーンに関するOCSP応答の完全なセット。
拡張子	O	-	RIが、トランザクションを追跡するための情報をデバイスに提供することを可能にするトランザクション識別子。
署名	M	-	RI秘密鍵を使用する、RO要求メッセージおよびRO応答メッセージ(この署名フィールドなしの)のSHA-1ハッシュ。

【０１２０】

図４は、１パスＲＯ獲得プロトコル４００の流れ図である。プロトコル４００は、デバイス２０２およびＲＩ２０４を利用する。プロトコル４００において、ＲＩ２０４は、デバイス２０２による要求なしに、ＲＯを含むＲＯ応答メッセージをデバイス２０２に一方的に送信する（ステップ４１０）。プロトコル４００は、例えば、プッシュ使用事例を適用する。テーブル７は、ＲＯ応答メッセージのフォーマットを示す。

【０１２１】

【表７】

表7 RO応答メッセージのフォーマット

パラメータ	1パス	メモ
ステータス	M	要求が処理されることが成功したか否かを示す。
デバイスID	M	デバイスハローメッセージの場合と同一の仕方で、要求するデバイスを識別する。この値は、RO要求メッセージの場合と同一でなければならない。同一でない場合、終了しなければならない。
RI ID	M	RIを識別し、格納されたRI IDと等しくなければならない。
デバイスナンス	-	RO要求メッセージの場合と同一の値を有さなければならない。
保護されたRO	M	センシティブな情報(CEKなどの)が暗号化されたRO。
証明書チェーン	O	登録応答メッセージの場合と同一。
OCSP応答	M	RIの証明書チェーンに関するOCSP応答の完全なセット。
拡張子	O	RIが、トランザクションを追跡するための情報をデバイスに提供することを可能にするトランザクション識別子。
署名	M	この署名フィールドなしのRO応答メッセージのSHA-1ハッシュ。RIの秘密鍵を使用して、この署名が生成される。

【０１２２】

図５は、２パスドメイン参加プロトコル５００の流れ図である。プロトコル５００は、デバイス２０２およびＲＩ２０４を利用する。デバイス２０２が、ドメインに参加することを望む場合、デバイス２０２は、ＲＩ２０４にドメイン参加要求メッセージを送信する（ステップ５１０）。ＲＩ２０４は、この要求を評価し、ドメイン参加応答メッセージをデバイス２０２に送信する（ステップ５１２）。テーブル８は、ドメイン参加要求メッセージのフォーマットを示し、テーブル９は、ドメイン参加応答メッセージのフォーマットを示す。

【０１２３】

【表８】

表8 ドメイン参加要求メッセージのフォーマット

パラメータ	必須またはオプション	メモ
デバイスID	M	要求するデバイスを識別する。この値は、登録応答メッセージからの格納された値と同一でなければならない。
RI ID	M	RIを識別し、登録応答メッセージからのRI IDと等しくなければならない。
デバイスナンス	M	デバイスによって選択されたナンス。
要求時間	M	デバイスに見える現在のDRM時間。DRM時間をサポートしない非接続のデバイスはここで「非定義」値を使用しなければならない。
ドメイン識別子	M	デバイスが参加することを望むドメインを識別する。
証明書チェーン	O	このパラメータは、証明書キャッシングが、このRIを使用してRIコンテキストの中で示されない限り、送信される。存在する場合、このパラメータ値は、登録応答メッセージの中の証明書チェーンパラメータに関して説明されたとおりでなければならない。
拡張子	O	ピア鍵識別子、OCSP応答なし、OCSPレスポンダ鍵識別子、およびハッシュチェーンサポートという拡張子を含む。
署名	M	デバイスの秘密鍵を使用する、ドメイン参加要求メッセージ(この署名フィールドなしの)のSHA-1ハッシュ。

【０１２４】

【表９】

表9 ドメイン参加応答メッセージのフォーマット

パラメータ	ステータス=成功	ステータスは、成功ではない	メモ
ステータス	M	M	要求が処理されることが成功したか否かを示す。
デバイスID	M	-	要求するデバイスを識別する。この場合に戻される値は、この応答をトリガしたドメイン参加要求メッセージの場合と同一でなければならない。
RI ID	M	-	この場合に戻される値は、先立つドメイン参加要求メッセージの中でデバイスによって送信されたRI IDと等しくなければならない。
デバイスナンス	M	-	先立つドメイン参加要求メッセージの場合と同一の値を有さなければならない。
ドメイン情報	M	-	このパラメータは、ドメイン鍵(デバイスの公開鍵を使用して暗号化された)、ならびにドメインの最大寿命についての情報を担持する。デバイスは、RIによって示唆されるよりも短い寿命を使用することが可能である。
証明書チェーン	O	-	このパラメータは、先立つROAPドメイン参加要求メッセージが、ピア鍵識別子拡張子を含んでおり、この拡張子が、RIによって無視されておらず、この拡張子の値が、RIの現在の鍵を識別しているのでない限り、存在しなければならない。存在する場合、証明書チェーンのパラメータの値は、登録応答メッセージの証明書チェーンパラメータに関して説明されたとおりでなければならない。
OCSP応答	O	-	RIの証明書チェーンに関する有効なOCSP応答の完全なセット。
拡張子	O	-	現在、1つだけの拡張子が、ドメイン参加応答メッセージに関して定義されている。この拡張子は、ハッシュチェーンサポートである。この拡張子は、存在する場合、RIが、ドメインセクションにおいて説明されるハッシュチェーンを介する生成の技術、ドメイン鍵を使用していることを示す。RIは、同一の拡張子が、先立つドメイン参加要求の中で受信されているのでない限り、ドメイン参加応答の中にこの拡張子を含めてはならない。
署名	M	-	署名フィールド自体を除いたドメイン参加応答メッセージのSHA-1ハッシュ。

【０１２５】

図６は、２パスドメイン退去プロトコル６００の流れ図である。プロトコル６００は、デバイス２０２およびＲＩ２０４を利用する。デバイス２０２が、ドメインを退去するこ

とを望む場合、デバイス２０２は、ＲＩ２０４にドメイン退去要求メッセージを送信する（ステップ６１０）。ＲＩ２０４は、この要求を評価して、デバイス２０２にドメイン退去応答メッセージを送信する（ステップ６１２）。テーブル１０は、ドメイン退去要求メッセージのフォーマットを示し、テーブル１１は、ドメイン退去応答メッセージのフォーマットを示す。

【０１２６】

【表１０】

表10 ドメイン退去要求メッセージのフォーマット

パラメータ	必須またはオプション	メモ
デバイスID	M	要求するデバイスを識別する。この値は、登録応答メッセージからの格納された値と同一でなければならない。
RI ID	M	RIを識別し、登録応答メッセージからのRI IDと等しくなければならない。
デバイスナンス	M	デバイスによって選択されたナンス。
要求時間	M	デバイスに見える現在のDRM時間。DRM時間をサポートしない、接続されていないデバイスは、この場合、「未定義」である、この値を使用しなければならない。
ドメイン識別子	M	ドメインが退去することを望むドメインを識別する。
証明書チェーン	O	このパラメータは、証明書キャッシングが、このRIを使用してRIコンテキストの中で示されない限り、送信される。存在する場合、このパラメータ値は、登録応答メッセージの中の証明書チェーンパラメータに関して説明されたとおりでなければならない。
拡張子	O	「ドメインメンバではない」拡張子が、ドメイン退去要求メッセージに関して、現在、定義されている。この拡張子の存在は、デバイスが自らを、このドメインのメンバであると見なさないことをRIに示す(デバイスは、このドメインからデバイスを除外するようRIへの要求を送信しているものの)。このことは、例えば、デバイスが、このドメインを既に退去しているが、このドメインを退去する新たなトリガを受信した(おそらく、RIが、前のROAPドメイン退去要求メッセージを受信していないために)場合、生じることが可能である。この拡張子は、デバイスが、識別されたドメインのメンバではない場合、要求の中に含められなければならない。
署名	M	デバイスの秘密鍵を使用する、ドメイン退去要求メッセージ(この署名フィールドなしの)のSHA-1ハッシュ。

【０１２７】
【表１１】
表11 ドメイン退去応答メッセージのフォーマット

パラメータ	ステータス=成功	ステータスは、成功ではない	メモ
ステータス	M	M	要求が処理されることが成功したか否かを示す。
デバイスナンス	M	–	先立つドメイン退去要求メッセージの場合と同一の値を有さなければならない。
ドメイン識別子	M	–	RIがデバイスを除外したドメイン。
拡張子	0	–	拡張子は、ドメイン退去応答メッセージに関して、現在、全く定義されていない。

【０１２８】
１パスＲＯ獲得プロトコルを除いて、ＲＯＡＰスイートに含まれるプロトコルのすべては、ＲＯＡＰトリガを使用して開始されることが可能である。また、デバイス２０２は、ユーザ対話の結果、一方的にプロトコルを開始することもできる。ＲＩ２０４は、ＲＯＡＰトリガを生成して、デバイス２０２に送信して、ＲＯＡＰプロトコル交換をトリガする。代替として、ＲＩ２０４は、必要な情報（ＲＯ識別子やドメイン識別子などの）を他のシステムに供給することによって、ＲＯＡＰトリガ生成をこれらのシステムに委任してもよい。また、ＲＯＡＰトリガ（ＲＩ２０４によって直接に生成されたか、間接的に生成されたかにかかわらず）は、他のシステム（例えば、ＣＩ）によってデバイス２０２に送信されることも可能である。
【０１２９】
デバイス２０２が、ＲＯＡＰトリガを受信すると、デバイス２０２は、可能な限り早くＲＯＡＰプロトコル交換を開始する。ＲＯＡＰトリガを受信した結果、ＲＯＡＰプロトコルを開始するのに先立って、適切なユーザ同意が、得られていなければならない。ＲＯＡＰは、いくつかのプロトコルを含むので、ＲＯＡＰトリガは、デバイス２０２によって開始されるべき実際のプロトコル（例えば、登録、ＲＯ獲得、ドメイン参加、またはドメイン退去）の指示を含む。
【０１３０】
ＲＯＡＰメッセージ、およびこれらのメッセージが、プロトコルによって、どのように扱われるかは、ＲＯ，および関連する処理を提供するだけでなく、ＯＭＡ　ＤＲＭ２．０におけるＲＯを取り巻くセキュリティ機能も提供する。より具体的には、以下のセキュリティ態様および信頼態様が、ＲＯＡＰプロトコルによって扱われる。すなわち、
【０１３１】
１．ＲＩとデバイスの間の相互認証、
【０１３２】
２．様々なメッセージにおいてナンスを使用することによって、リプレー攻撃に対処すること、
【０１３３】
３．ＲＯＡＰメッセージ、およびＲＯＡＰメッセージの諸部分の完全性を保護すること、および
【０１３４】

４．ＲＯＡＰメッセージ、またはＲＯＡＰメッセージの諸部分におけるセキュリティで保護されたＤＲＭ時間の検証である。

【０１３５】

（信頼されるコンピューティング技術）

【０１３６】

最近、信頼されるコンピューティング技術が、おおむね、ＴＣＧ（Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ）の技術的傘下において文献および製品に出現している。ＴＣＧ技術は、コンピューティングエンティティが、信頼チェーンを使用することによって、エンティティ、および他のデバイスの信頼性を確立することができ、したがって、そのようなデバイス上の処理またはコンピューティングは、以下のとおりであることが可能である。すなわち、

【０１３７】

１．プラットフォーム、ならびに様々なＨＷ（ハードウェア）構成要素およびＳＷ（ソフトウェア）構成要素の信頼性に関して評価され、

【０１３８】

２．適切な信頼レベルが確立された場合にだけ、検証され、外部要求があると、エンティティまたはデバイス自らに対して、ならびに他のエンティティまたはデバイスに対して検証されることが可能であり、さらに

【０１３９】

３．外部パーティは、他のデバイスとの情報および処理の交換に関する評価および決定を実行することができ、そのようなターゲットデバイスの表明された信頼レベルに基づく。

【０１４０】

ＴＣＧは、以下のフィーチャを有する、ＴＰＭ（信頼される処理モジュール）と呼ばれるコア処理モジュールを定義する。すなわち、

【０１４１】

１．モジュール、およびモジュールのインタフェースの物理的保護、

【０１４２】

２．保護された揮発性のストレージスペース、および保護された不揮発性のストレージスペース、

【０１４３】

３．暗号化、およびデジタル署名を実行することができるモジュール内部の保護された暗号化機能、

【０１４４】

４．ハッシュ拡張によるプラットフォーム、およびプラットフォームのＳＷ構成要素の「状態」を連続的にキャプチャするＰＣＲ（プラットフォーム構成レジスタ）の使用、

【０１４５】

５．デバイスの認証のルートの役割をするが、ただし、直接的な仕方でそのような役割をするのではないＰＫＩに基づく、デバイス特有のセキュリティで保護されたＥＫ（承認鍵）の存在。ＥＫは、決して外部に開示されないが、ＡＩＫ（構成証明アイデンティティ鍵）と呼ばれるＥＫのエイリアスが、プラットフォームの完全性測定値に署名するのに使用され、さらに

【０１４６】

６．データの「密封」を、ＡＩＫによって署名されたＰＣＲ値と併せて、メモリ「ＢＬＯＢ」の中で使用して、プラットフォーム完全性またはＳＷ完全性（ＴＰＭからの、または密封メモリＢＬＯＢからの合致するＰＣＲ値によって測定され、検証された）が検証された場合に限って、データがアクセスされる、または抽出されることが可能であるようにすること。

【０１４７】

信頼されるコンピューティング技術が、特に移動電話デバイスのコンテキストにおいて

、そのような移動デバイス上のＤＲＭアプリケーションをセキュリティで保護することへの可能な応用のために、検査される。ＴＣＧ技術の使用によってＤＲＭアプリケーションをセキュリティで保護するようにこれまでに提案された方法は、ＴＰＭ密封の手続き、およびメモリＢＬＯＢを使用して、ＴＣＧ鍵を使用するＲＯＡＰプロトコル処理の後、ＴＰＭ、および鍵保護を有するストレージエリアの中にＤＲＭ関連のデータをセキュリティで保護された仕方で格納することを含んでいた。

【０１４８】

しかし、既存の従来技術は、プラットフォーム、および／またはＤＲＭソフトウェアに対してどのように「信頼」を確立し、使用すべきかを明示的に扱う、または秩序立った仕方で扱うことはしない。また、従来技術は、ＲＯＡＰメッセージの中の完全性をセキュリティで保護して、ＯＭＡ　ＤＲＭ２．０システムにおける完全性処理を強化することもしない。本発明は、そのような目的で新たな技術を含む。

【０１４９】

現在のＯＭＡ　ＤＲＭ２．０仕様は、ＣＡ、ＲＩ、およびデバイスが関与するＰＫＩに基づく、強いセキュリティ方法を提供する。しかし、ＯＭＡ　ＤＲＭ２．０仕様の範囲内でも、ＯＭＡ　ＤＲＭ２．０準拠であるデバイスおよびＲＩの不特定の実施に関連しても、プラットフォーム、ＳＷ、エージェント、およびメッセージのセキュリティおよび完全性と関係する脆弱性が、存在する。

【０１５０】

ＯＭＡ　ＤＲＭ仕様は、デバイスまたはＲＩが、ＯＭＡ　ＤＲＭ２．０仕様を遵守している場合でも、いずれのデバイスまたはＲＩも直面する可能性がある様々な脅威および脆弱性を認識している。これらの脆弱性には、以下が含まれる。すなわち、

【０１５１】

１．攻撃者が、ＤＲＭシステムのエンティティを物理的に、またはそれ以外で侵害しようと試みることが可能な、エンティティ侵害。エンティティ侵害攻撃のタイプには、デバイス上のＤＲＭエージェント、およびＲＩにおけるＤＲＭ　ＳＷを侵害することが含まれる。エンティティ侵害の結果には、秘密鍵、ドメイン鍵、ＲＯ暗号化鍵、コンテンツ暗号化鍵、および保護されたコンテンツの開示、ならびに、例えば、ＤＲＭエージェントのリプレーキャッシュの完全性保護が失われること、および／またはＤＲＭエージェントの内部に格納された権利の保護が失われることが含まれる。さらに、ＤＲＭ時間が失われることが、生じる可能性もある。侵害されたＣＡまたはＯＣＳＰレスポンダのＰＫＩに対する影響は、例えば、非特許文献１において説明される。

【０１５２】

ＯＭＡ　ＤＲＭシステムは、侵害されたエンティティによって生じる損害を最小限に抑えるのに、証明書取り消しに依拠する。ＤＲＭエージェントおよびＲＩは、エンティティの証明書ステータスを調べることによって、ＤＲＭエージェントおよびＲＩが通信している相手のエンティティが、侵害されていないことを常に検証しなければならない。エンティティ侵害攻撃は、「順方向」でも、「逆方向」でも行われる可能性がある。順方向侵害攻撃は、ＤＲＭエンティティ（ＲＩ、ＤＲＭエージェント、ＣＩ、ＣＡ、またはＯＣＳＰレスポンダ）に対してであり、許可のない振舞いにつながる。逆方向侵害攻撃は、ＤＲＭエージェントのセキュリティ、完全性設定、および構成を無力化する、または脆弱にする。

【０１５３】

２．攻撃者が、ＤＲＭエージェントとＲＩの間で送信されるメッセージを削除することができ、通常、ＤｏＳ（サービス拒否）攻撃をもたらすメッセージ削除。メッセージ削除攻撃には、登録プロトコル中、またはＲＯ獲得プロトコル中のメッセージ削除、リプレーナンス削除、ＲＯＡＰトリガの削除などが含まれることが可能である。

【０１５４】

３．攻撃者が、ＤＲＭエージェントとＲＩの間で送信される任意のメッセージを変更することができ、通常、ＤｏＳ攻撃をもたらすメッセージ変更。メッセージ変更攻撃には、

登録プロトコル中の変更、ドメイン参加プロトコル中の変更、およびドメイン退去プロトコル中の変更、ならびに様々なＲＯＡＰトリガに対する変更が含まれることが可能である。

【０１５５】

４．攻撃者が、ＲＩとＤＲＭエージェントの間の任意のポイントで通信チャネルにメッセージを挿入することができるメッセージ挿入。また、攻撃者は、メッセージを記録して、これらのメッセージを後の時点でリプレーしようと試みることもできる。メッセージ挿入攻撃は、登録プロトコルの最中に挿入されたメッセージ、２パスＲＯ獲得プロトコルの最中に挿入されたメッセージ、１パスＲＯ獲得プロトコルの最中に挿入されたメッセージ、および様々なＲＯＡＰトリガに挿入されたメッセージを含むことが可能である。

【０１５６】

５．一般的なＤｏＳ攻撃、トラフィック解析などの受動的攻撃、およびプライバシー開示などのその他の攻撃。

【０１５７】

現在のＯＭＡ　ＤＲＭ仕様およびＯＭＡ　ＤＲＭ実施形態の以下の問題が、特定される。ＯＭＡ　ＤＲＭスキームに適用された「完全性」の拡大された概念が、定義される。従来の意味で、ＯＭＡ　ＤＲＭ仕様は、ＲＯＡＰメッセージ完全性の小さい範囲だけしか扱わない。本発明において定義される完全性の拡大された概念において、以下において、どこで、どのような種類の完全性が考慮されることが可能であるか留意されたい。

【０１５８】

１．ＤＲＭプラットフォーム完全性。ＤＲＭプラットフォーム完全性は、プラットフォームエンティティにおける、またはプラットフォームエンティティ内の、すなわち、デバイス、ＲＩ、およびコンテンツ機能を含む物理的エンティティにおける完全性と関係する。異なるエンティティには、ＯＳ（オペレーティングシステム）、起動コード（例えば、ＰＣの事例におけるＢＩＯＳ）、メモリアクセスのためのＨＷ／ＦＷ（ファームウェア）／ＳＷ、セキュリティ関連の機能（暗号法および鍵管理、ならびにポリシー、証明書などの秘密データの特権的格納）を処理する様々なＨＷ／ＦＷ／ＳＷエンティティ、ならびにネットワーク接続ＨＷ／ＦＷ／ＳＷおよびローカル接続ＨＷ／ＦＷ／ＳＷが含まれる。プラットフォーム完全性は、プラットフォームが、有効であり、真性であり、正当なプロセスによる他は、変更されておらず、意図されるとおりにしか動作しないかどうかを判定する。

【０１５９】

２．ＤＲＭ　ＳＷ完全性。ＤＲＭ　ＳＷとは、ＯＭＡ　ＤＲＭ仕様、およびＯＭＡ　ＤＲＭ仕様の手続きに特有の機能を実行するデバイス内、ＲＩ内、またはＣＩ内に存在するソフトウェアエンティティおよびソフトウェア構成要素を指す。デバイスにおいて、ＤＲＭエージェントは、ＤＲＭ　ＳＷから成る。ＲＩおよびＣＩにおいて、ＤＲＭ　ＳＷとは、ＲＯパッケージ化、ＤＣＦフォーマット、コンテンツ暗号化、コンテンツ配信もしくはＲＯ配信、検証、ＲＯＡＰ処理などのＤＲＭ特有の機能を実行するＳＷのセットをまとめて指す。ＤＲＭ　ＳＷ完全性は、ＤＲＭ　ＳＷが、有効であり、真性であり、正当なプロセスによる他は、変更されておらず、意図されるとおりにしか動作しない場合に、維持される。

【０１６０】

３．ＲＯＡＰメッセージおよびＲＯＡＰ情報の完全性。ＲＯＡＰメッセージ、およびこれらのメッセージを構成する情報の完全性は、そのような情報が、有効であり、真性であり、正当なプロセスによる他は、変更されていない場合、維持される。ＯＭＡ　ＤＲＭ２．０仕様において、ＲＯＡＰメッセージのいくつかのサブセット、およびこれらのサブセットを構成する情報は、デジタル署名の使用によって完全性保護される。

【０１６１】

４．メディアオブジェクトおよびＤＲＭコンテンツの完全性。メディアオブジェクトおよびＤＲＭコンテンツも、完全性保護されなければならず、すなわち、メディアオブジェ

クトおよびＤＲＭコンテンツが、デバイスにおいて格納されているか、ＲＩにおいて格納されているか、ＣＩにおいて格納されているか、あるいはいずれかの２つのパーティ間で伝送中または配信中であるかにかかわらず、変更される、削除される、または不正に挿入されることがあってはならない。特に関心を引くのが、ＤＲＭコンテンツが、基本的に開かれたチャネルを使用して配信される場合の、移動デバイスへのコンテンツの転送に適用可能な、コンテンツのＯＴＡ（無線）配信である。

【０１６２】

５．ＤＲＭ関連の情報の完全性。エンティティＩＤ（デバイスＩＤ、ＲＩ　ＩＤなど）、暗号化鍵（ＣＥＫ、ＲＥＫ）および署名鍵、ＲＯ自体、コンテキスト情報、証明書、およびその他の信頼チェーン関連の情報などのＤＲＭ関連の情報は、セキュリティで保護されなければならず、このことは、これらの情報が、機密性を保護されるだけでなく、完全性も保護されなければならないことを意味する。

【０１６３】

現在のＯＭＡ　ＤＲＭ２．０仕様も、既存の従来技術も、エンティティ侵害または完全性問題に対するソリューションを提供したように思われないことに留意されたい。ソリューションのこの欠如は、以下の問題をもたらす。すなわち、例えば、すべてのＲＯＡＰ手続きが、ＯＭＡ　ＤＲＭ２．０仕様に準拠して正しく実施された場合でも、ＲＩのプラットフォームが信頼できるかどうか、デバイスはどのようにして本当に知ることができるか。つまり、ＲＩのプラットフォームが、ＲＯＡＰプロトコルの一環としてデバイスが送信するデータを乱用しないかどうか、またはＤＲＭ処理自体を乱用しないかどうかを、デバイスは、どのようにして知ることができるか。例えば、デバイスは、ＲＩのプラットフォームＳＷが、侵害されており、デバイスのさもなければ有効な使用権利を制限するため、ＲＩが、デバイスの使用権利を恣意的に、誤って制限するかどうかを知らない。ＤＲＭソフトウェアの完全性の問題に関して、同様の問題が生じる。より具体的には、前述した完全性の拡大された概念から見た現在のＯＭＡ　ＤＲＭ２．０システムの問題のいくつかは、以下のとおりである。

【０１６４】

１．プラットフォームおよびＤＲＭ　ＳＷの完全性を検査して、報告する方法の欠如。前段で特定されたエンティティ侵害脅威と関係して、ＯＭＡ　ＤＲＭ２．０仕様によって指定される、またはＴＣＧ１．２使用事例の一環としての、デバイスとＲＩとの間の明確な、構造化されたプラットフォーム完全性検証、およびＳＷエージェント完全性検証のための方法は、従来技術において、全く存在しない。このことは、ＤＲＭエージェントに関してだけでなく、プラットフォーム完全性検証に関して特に当てはまる。

【０１６５】

２．プラットフォーム（デバイスと関係して、ＰＣもしくはＰＤＡ，あるいはＲＩに関して、サーバなどの）が、悪意のある仕方で侵害されることが可能であり、これにより、ＤＲＭエージェントおよびＲＩエージェントＳＷが、正しい、機密性保護され、完全性保護された情報を与えられても、正しく動作することが妨げられることになる可能性がある。例えば、さもなければよく保護されたＤＲＭエージェントＳＷが、処理に先立って、処理中に、または処理後に、いくらかの情報を共有メモリの中に平文で格納する可能性がある。侵害されたプラットフォームは、そのような事例において、共有メモリにひどくアクセスして、情報を削除する、情報を変更する、または新たな偽の情報を挿入して、この情報が、そのような偽の情報を真性と認識する可能性があるＤＲＭエージェントＳＷによって後に処理される得る可能性がある。このことは、ＤｏＳ攻撃、プライベート情報の許可のない開示、またはＤＲＭ　ＲＯもしくはＤＲＭコンテンツの許可のない配信、配布、または消費をもたらす可能性がある。

【０１６６】

３．ＤＲＭ関連の情報を処理するＳＷの部分であるＤＲＭエージェントＳＷおよびＲＩＳＷが、様々な理由で侵害される可能性がある。そのようなＳＷが、例えば、ウイルス、または他の悪意のあるＳＷエンティティによって変更されることが可能である。プラッ

トフォームまたはＤＲＭ　ＳＷのそのような侵害の１つの結果は、ＯＭＡ　ＤＲＭ２．０が考慮するメッセージおよび情報、特にＲＯＡＰプロトコルメッセージの完全性が後に侵害されることである。１つには、ＲＯＡＰメッセージのすべてではなく、一部だけが完全性保護されるため、ＲＯＡＰメッセージは、理論上、侵害されたデバイスと、不正な、つまり、侵害されたＲＩとの間で同期された仕方で操作されることが可能である。メッセージは、デバイスとＲＩの両方において同期した仕方で変更されることが可能であり、メッセージは、同一の仕方で変更されたため、それでも、「完全性検証」されているように見える可能性がある。

【０１６７】

４．ＲＯＡＰメッセージの不十分な完全性保護。メッセージ完全性と関係して、ＲＯＡＰメッセージ、および様々なメッセージフィールドによって担持される情報は、ＯＭＡ　ＤＲＭ２．０仕様によっては解決されない脆弱性を被る。例えば、ＯＭＡ　ＤＲＭ２．０仕様の中で現在、指定されているＲＯＡＰメッセージ完全性保護は、以下のような穴を残す。すなわち、

【０１６８】

４Ａ．すべてのＲＯＡＰメッセージが、完全性保護されるわけではない。すべてのメッセージの中にデジタル署名を含めるわけではないことにより、一部の場合において脆弱性がもたらされる可能性がある。

【０１６９】

４Ｂ．ＲＯＡＰメッセージ、または情報の一部のフィールドが、デジタル署名によって完全性保護されている場合でさえ、一旦、そのような情報が解読され、完全性検査され、その後、平文で使用されると、悪意のあるエンティティが、この平文情報にアクセスして、それまでに完全性検査された情報を削除する、改変する、または再配布する可能性がある。このため、強化された完全性保護が、要求される。

【０１７０】

５．ＤＲＭコンテンツ、およびＤＲＭコンテンツの配信の完全性に関する脆弱性。より具体的には、以下の問題が存在する。すなわち、

【０１７１】

５Ａ．コンテンツ完全性検査機構が、不完全である。例えば、コンテンツが伝送されている、または配信されている（例えば、ＯＴＡダウンロード）最中のコンテンツの完全性が、規定されていない。例えば、ＤＦＣに関する署名は、ＲＯＡＰ手続きにおいて使用するためにだけ生成される。ＲＯＡＰ手続きが行われるまで、この手続きより前に、例えば、ＣＩにおける格納中に、コンテンツ完全性を管理する完全性検査機構は、全く存在しない。

【０１７２】

５Ｂ．コンテンツ暗号化は、ＲＯＡＰプロトコルにおいて使用するためにさえ、必須であるが、完全性検査は、単にオプションである。

【０１７３】

５Ｃ．特に、ストリーミングサービスに関するパケット化されたコンテンツに関して、ＰＤＣＦフォーマットは、タイミング問題を有する。不正に変更されているパケットが、ダウンロードされる可能性があり、ストリーム全体の完全性が検査されることが可能である前に、消費される（すなわち、メディアプレーヤ上で再生される）可能性さえある。

【先行技術文献】

【非特許文献】

【０１７４】

【非特許文献１】ＩＥＴＦ　ＲＦＣ３２８０

【発明の概要】

【発明が解決しようとする課題】

【０１７５】

中心的問題は、以下のとおりとなる。すなわち、様々なパーティ（デバイス、ＲＩ、お

よびＣＩ）はどのようにして、プラットフォーム完全性、およびＤＲＭ　ＳＷ完全性を確信することができるか。このため、ＤＲＭエージェントＳＷまたはＲＩ　ＳＷが依拠するプラットフォーム（例えば、ＯＳ、ＢＩＯＳ，ドライバ、メディアプレーヤ、通信ソフトウェア、共有メモリなど）の完全性を強化し、検証する方法が、必要とされる。本発明は、従来技術の欠点に対処する。

【課題を解決するための手段】

【０１７６】

本発明は、ＯＭＡ　ＤＲＭ仕様　ｖ２．０と関係するエンティティ、メッセージ、および処理の完全性を強化するいくつかの方法を開示する。これらの方法は、業界フォーラム、ＴＣＧ（Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ）によって規定される、信頼されるコンピューティング（Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ）技術として一般に知られる技術を使用する。本発明の第１の実施形態において、ＤＲＭ　ＲＯＡＰ仕様およびＤＣＦ仕様の変更を伴う場合と、伴わない場合の両方の、プラットフォームおよびＤＲＭ　ＳＷの完全性または信頼性を検証する技術が、開示される。第２の実施形態において、既存のＲＯＡＰプロトコルを変更することなしに、ＯＭＡ　ＤＲＭ　ＲＯＡＰメッセージ、ＲＯＡＰメッセージを構成する情報、およびＲＯＡＰ処理の完全性を強化する技術が、開示される。第３の実施形態において、既存のＲＯＡＰプロトコルのいくつかの変更を伴って、ＲＯＡＰメッセージ、情報、および処理の完全性を強化する技術が、開示される。

【０１７７】

本発明のより詳細な理解は、例として与えられ、添付の図面と併せて理解されるべき、好ましい実施形態の以下の説明から得ることができる。

【図面の簡単な説明】

【０１７８】

【図１】既存のＯＭＡ　ＤＲＭ２．０機能アーキテクチャを示すブロック図である。

【図２】既存のＯＭＡ　ＤＲＭ２．０　ＲＯＡＰ　４パス登録プロトコルを示す流れ図である。

【図３】既存のＯＭＡ　ＤＲＭ２．０　ＲＯＡＰ　２パスＲＯ獲得プロトコルを示す流れ図である。

【図４】既存のＯＭＡ　ＤＲＭ２．０　ＲＯＡＰ　１パスＲＯ獲得プロトコルを示す流れ図である。

【図５】既存のＯＭＡ　ＤＲＭ２．０　ＲＯＡＰ　２パスドメイン参加プロトコルを示す流れ図である。

【図６】既存のＯＭＡ　ＤＲＭ２．０　ＲＯＡＰ　１パスドメイン退去プロトコルを示す流れ図である。

【図７】ＯＭＡ　ＤＲＭ２．０エンティティ間のマルチパーティプラットフォーム完全性検査を示すブロック図である。

【図８】２つのエンティティが、デバイスとＲＩ、またはデバイスとＣＩであることが可能である場合の２つのエンティティ間でプラットフォーム完全性検証を実行するための方法を示す流れ図である。

【図９】従来の信頼検査を使用してデバイスとＲＩの間で相互プラットフォーム完全性検査を実行するための４パスＲＯＡＰ登録プロトコルを示す流れ図である。

【図１０】変更されたデバイスハローメッセージ、および変更されたＲＩハローメッセージを使用して、デバイスとＲＩの間で相互プラットフォーム完全性検査を実行するための４パスＲＯＡＰ登録プロトコルを示す流れ図である。

【図１１】２つのエンティティが、デバイスとＲＩ、またはデバイスとＣＩであることが可能である場合の２つのエンティティ間でＤＲＭソフトウェア完全性検査を実行するための方法を示す流れ図である。

【図１２】デバイスとＲＩの間で相互ＤＲＭソフトウェア完全性検査を実行するための２パスＲＯＡＰ　ＲＯ獲得プロトコルを示す流れ図である。

【図１３】密封結び付け、およびメモリＢＬＯＢ生成を含むＴＣＧ技術を使用したＲＯＡＰメッセージおよびＲＯＡＰ処理の完全性を向上させるための方法を示す流れ図である。
【発明を実施するための形態】
【０１７９】
以降、「無線送信／受信ユニット」（ＷＴＲＵ）という用語には、ユーザ機器、移動局、固定加入者ユニットもしくは移動加入者ユニット、ポケットベル、または有線環境または無線環境において動作することが可能な他の任意のタイプのデバイスが含まれるが、以上には限定されない。以降、言及される場合、「基地局」という用語には、ノードＢ、サイトコントローラ、アクセスポイント、または無線環境における他の任意のタイプのインタフェースデバイスが含まれるが、以上には限定されない。
【０１８０】
本発明は、ＤＲＭエンティティ（例えば、デバイス、ＲＩ、またはＣＩ）の信頼状態または完全性に関する情報が、ＯＭＡ　ＤＲＭ手続きの前提条件として、いずれの２つのＤＲＭエンティティの間でも明示的に、相互に要求され、交換される方法を開示する。
【０１８１】
この方法の一般的なアーキテクチャ７００が、図７に示される。このアーキテクチャは、４つのＤＲＭエンティティ、すなわち、デバイス７０２、ＲＩ７０４、ＣＩ７０６、およびＰＣＡ（プライベート証明機関）７０８を含む。プラットフォーム完全性検査は、ＰＣＡ７０８が、その他のＤＲＭエンティティ（例えば、デバイス７０２、ＲＩ７０４、およびＣＩ７０６）に関する信頼されるコンピューティング（例えば、ＴＣＧ）資格証明のレコードを有し、それらのＴＣＧ資格証明の証明に関する信頼のルートを提供するものと想定する。
【０１８２】
互いの間で相互プラットフォーム完全性検査を望む任意のエンティティペア（例えば、デバイス７０２とＲＩ７０４、デバイス７０２とＣＩ７０６、またはＲＩ７０４とＣＩ７０６）が、信頼されるコンピューティング対応である（例えば、ＴＣＧ　ＴＰＭ（信頼される処理モジュール）７１０を備えている）。このことは、信頼されるコンピューティング対応のＤＲＭエンティティが、ＴＰＭ７１０（または均等物）を有するだけでなく、ＡＩＫ７１２、ＳＭＬ７１４、およびＢＬＯＢを使用する保護されたメモリ７１６などの、関連するＴＣＧリソースも有することを暗示する。やはり存在するのが、ＯＳまたはプラットフォームソフトウェア７１８およびＤＲＭソフトウェア７２０である。
【０１８３】
以上の要件が満たされる場合、様々なＤＲＭエンティティの任意のペアが、ＰＣＡ７０８、および信頼されるコンピューティング能力を使用して、プラットフォーム完全性またはプラットフォーム信頼状態を互いに検査することができる。例として、デバイス７０２とＲＩ７０４の間の相互完全性検査のための手続きは、以下のとおりである。
【０１８４】
デバイス７０２、ＲＩ７０４、およびＣＩ７０６がすべて、ＯＳ構成要素、または他のプラットフォームソフトウェア構成要素の自己検査（ステップ７３０）、およびＤＲＭソフトウェアの自己検査（ステップ７３２）を実行することができる。自己検査は、より大きい検証プロセス（後段でより詳細に説明される）の一環として要求されることも、スタンドアロンのプロセスであることも可能である。これらの自己検査のいずれかが不合格であった場合、そのことは、そのエンティティが、侵害されており、信頼されるべきでないことの表れである可能性がある。
【０１８５】
デバイス７０２は、デバイス７０２のプラットフォームＴＣＧ資格証明をＲＩ７０４に送信する（ステップ７４０）。プラットフォームＴＣＧ資格証明の例には、署名されたＴＣＧプラットフォーム証明書、または署名されたＴＰＭ証明書が含まれるが、以上には限定されない。資格証明の一部として、デバイス７０２は、自己証明された信頼状態フラグ、または自己証明されたプラットフォーム完全性検査済みフラグを補足的な情報として、

ＲＩ７０４に送信することもできる。デバイス７０２が、ＲＩ７０４のプラットフォーム完全性を検証する場合、ステップ７４０で送信される資格証明情報は、ＲＩ７０４が、デバイス７０２のプラットフォーム完全性を検証する手続きを開始することをデバイス７０２が望むという、デバイス７０２による指示も含む。デバイス７０２は、ＲＩのプラットフォーム完全性ステータスの検証がオプションのフィーチャである場合に限って、ＲＩ７０４のプラットフォーム完全性を検証すべきかどうかに関する決定を行うことができ、一実施形態では、ＲＩのプラットフォーム完全性を検証することは、必須のフィーチャであることに留意されたい。

【０１８６】

デバイス７０２から資格証明情報を受信すると、ＲＩ７０４は、この資格証明情報をＰＣＡ７０８に中継し（ステップ７４２）、デバイス７０２についての資格証明、特に、デバイスの最新の信頼性を検証するよう、ＰＣＡ７０８に要求も行う。すると、ＰＣＡ７０８は、デバイス７０２に関する最新の信頼性情報（例えば、プラットフォーム信頼レベルなど）をＲＩ７０４に送信する（ステップ７４４）。ＰＣＡ７０８からデバイスプラットフォーム信頼性情報を受信し、オプションとして、デバイス７０２から補足的な情報も受信すると、ＲＩ７０４は、デバイス７０２の信頼レベルを評価する。ＲＩ７０４は、デバイスプラットフォームの完全性に十分な信頼を与えて、登録プロトコルまたはＲＯ獲得プロトコルなどのＤＲＭ手続きをさらに進めるかどうかを決定する。

【０１８７】

デバイス７０２は、必須の手続きとして、またはオプションの手続きとして、ステップ７４０～７４４の場合と同様な、相互の仕方でＲＩ７０４のプラットフォーム完全性を評価することができる。より具体的には、ＲＩ７０４が、ＲＩ７０４のプラットフォームＴＣＧ資格証明についての情報を、デバイス７０２に送信する（ステップ７５０）。資格証明の一部として、ＲＩ７０４は、自己証明された信頼状態フラグ、または自己証明されたプラットフォーム完全性検査済みフラグを補足的情報として、デバイス７０２に送信することもできる。

【０１８８】

ＲＩ７０４からＴＣＧ関連の情報を受信すると、デバイス７０２は、この情報をＰＣＡに中継し（ステップ７５２）、ＲＩ７０４についての資格証明、特に、ＲＩの最新の信頼性を検証するよう、ＰＣＡ７０８に要求も行う。すると、ＰＣＡ７０８は、ＲＩ７０４に関する最新の信頼性情報をデバイス７０２に送信する（ステップ７５４）。ＲＩ７０４に関してＰＣＡ７０８からＲＩプラットフォーム信頼性情報を受信し、オプションとして、ＲＩ自体から補足的な情報も受信すると、デバイス７０２は、ＲＩ７０４の信頼レベルを評価する。デバイス７０２は、ＲＩプラットフォームの完全性に十分な信頼を与えて、登録プロトコルまたはＲＯ獲得プロトコルなどのＤＲＭ手続きをさらに進めるかどうかを決定する。

【０１８９】

デバイス７０２は、必須の手続きとして、またはオプションの手続きとして、ＣＩ７０６のプラットフォーム完全性を評価することができる。ＣＩ７０６が、ＣＩ７０６のプラットフォームＴＣＧ資格証明についての情報を、デバイス７０２に送信する（ステップ７６０）。資格証明の一部として、ＣＩ７０６は、自己証明された信頼状態フラグ、または自己証明されたプラットフォーム完全性検査済みフラグを補足的な情報として、デバイス７０２に送信することもできる。

【０１９０】

ＣＩ７０６からＴＣＧ関連の情報を受信すると、デバイス７０２は、この情報をＰＣＡに中継し（ステップ７０６）、ＣＩ７０６についての資格証明、特に、ＣＩの最新の信頼性を検証するよう、ＰＣＡ７０８に要求も行う。すると、ＰＣＡ７０８は、ＣＩ７０６に関する最新の信頼性情報をデバイス７０２に送信する（ステップ７６４）。ＣＩ７０６に関してＰＣＡ７０８からＣＩプラットフォーム信頼性情報を受信し、オプションとして、ＣＩ自体から補足的な情報も受信すると、デバイス７０２は、ＣＩ７０６の信頼レベルを

評価する。デバイス７０２は、ＣＩプラットフォームの完全性に十分な信頼を与えて、ＤＲＭ手続きをさらに進めるかどうかを決定する。

【０１９１】

デバイス７０２のプラットフォーム完全性が、以下のとおり、ＣＩ７０６によって検証されることが可能である。デバイス７０２は、デバイス７０２のプラットフォームＴＣＧ資格証明についての情報をＣＩ７０６に送信する（ステップ７７０）。資格証明の一環として、デバイス７０２は自己構成証明信頼状態検査フラグまたはプラットフォーム完全性検査フラグを補足情報としてＣＩ７０６に送信することも可能である。デバイス７０２が、ＣＩ７０６のプラットフォーム完全性を検証する場合、ステップ７７０で送信される資格証明情報は、ＣＩ７０６が、デバイス７０２のプラットフォーム完全性を検証する手続きを開始することをデバイス７０２が望むという、デバイス７０２による指示も含む。デバイス７０２は、ＣＩのプラットフォーム完全性ステータスの検証がオプションのフィーチャである場合に限って、ＣＩ７０６のプラットフォーム完全性を検証すべきかどうかに関する決定を行うことができ、一実施形態では、ＣＩのプラットフォーム完全性を検証することは、必須のフィーチャであることに留意されたい。

【０１９２】

デバイス７０２から資格証明情報を受信すると、ＣＩ７０６は、この資格証明情報をＰＣＡ７０８に中継し（ステップ７２２）、デバイス７０２についての資格証明、特に、デバイスの最新の信頼性を検証するよう、ＰＣＡ７０８に要求も行う。すると、ＰＣＡ７０８は、デバイス７０２に関する最新の信頼性情報をＣＩ７０６に送信する（ステップ７７４）。ＰＣＡ７０８からデバイスプラットフォーム信頼性情報を受信し、オプションとして、デバイス７０２から補足的な情報も受信すると、ＣＩ７０６は、デバイス７０２の信頼レベルを評価する。ＣＩ７０６は、デバイスプラットフォームの完全性に十分な信頼を与えて、ＤＲＭ手続きをさらに進めるかどうかを決定する。

【０１９３】

前述の例では、ステップ７４０～７４４は、デバイス７０２が、ＲＩ７０４に対してデバイス７０２の完全性ステータスを検証するのに、本発明の必須のフィーチャであることに留意されたい。しかし、デバイス７０２に対してＲＩ７０４のプラットフォーム完全性を検証すること（ステップ７５０～７５４）、デバイス７０２に対してＣＩ７０６のプラットフォーム完全性を検証すること（ステップ７６０～７６４）、およびＣＩ７０６に対してデバイスプラットフォーム完全性を検証すること（ステップ７７０～７７４）は、ＤＲＭシステムにおける、オプションであるが、それでも強く推奨されるフィーチャである。

【０１９４】

これらの手続きは、検証される必要があるエンティティによる能動的な開始によって開始される必要はないことにも留意されたい。これらの完全性検証手続きは、その他のパーティの完全性を検証することを所望するエンティティによる要求で始まることが可能である。そのような場合において、ステップ７４０、７５０、７６０、または７７０のそれぞれには、その他のパーティのプラットフォーム完全性の検証を要望するエンティティが、関係のある信頼関連の情報を送信するよう、その他のパーティを呼び出す、またはその他のパーティに要求する別のステップが先行する。

【０１９５】

代替の実施形態では、実際的なＯＭＡ　ＤＲＭシステム実施に関して、前述した、提案されるプラットフォーム完全性検証手続きに関する条件またはトリガ機構には、以下が含まれることが可能である。

【０１９６】

１．デバイスプラットフォーム完全性検証手続き（すなわち、ステップ７４０～７４４）が、以下の１つまたは複数によって実行されることが可能である。

【０１９７】

１Ａ．デバイスが、新たな４パスＲＯＡＰ登録プロトコルを開始することを要望する前

。

【０１９８】

１Ｂ．各ＲＩにつき１回、その特定のＲＩへの最初の登録が行われる前。この場合、ＲＩは、最初の登録より前に１回、デバイスのＴＣＧ資格証明を受信し、次に、ＲＩは、デバイスの資格証明情報をＴＰＭ鍵に結び付けることによって、ＲＩ自らのＴＰＭの下で、この資格証明情報を保護する。ＲＩは、後に、この格納されたＴＣＧ資格証明の結び付きを解除して、定期的に、またはいくつかのイベント時に、例えば、ＯＣＳＰ　ＣＡを調べることによって、ＲＩが受信したデバイスのＴＣＧ資格証明が依然として有効であるかどうかを検証する。

【０１９９】

１Ｃ．定期的に、指定された時間、例えば、デバイスが、同一のＲＩに対して前回の登録プロトコルを完了して以来、$T_{DEV-PLATFORM-LAST-REG}$が経過するたびに。

【０２００】

１Ｄ．定期的に、指定された時間、例えば、デバイスが、同一のＲＩに対してデバイスの完全性ステータスを前回に検証して以来、$T_{DEV-PLATFORM-LAST-REPORT}$が経過するたびに。

【０２０１】

２．ＲＩプラットフォーム完全性検証手続き（すなわち、ステップ７５０～７５４）が実施される場合、実施される際に、実施されるプラットフォーム完全性検証手続きは、以下の１つまたは複数によって実行されることが可能である。

【０２０２】

２Ａ．各デバイスにつき１回、その特定のデバイスへの最初の登録が行われる前。この場合、デバイスは、最初の登録より前に１回、ＲＩのＴＣＧ資格証明を受信し、次に、デバイスは、ＲＩの資格証明情報をＴＰＭ鍵に結び付けることによって、デバイス自らのＴＰＭの下で、この資格証明情報を保護する。デバイスは、後に、この格納されたＴＣＧ資格証明の結び付きを解除して、定期的に、またはいくつかのイベント時に、例えば、ＯＣＳＰ　ＣＡを調べることによって、デバイスが受信したＲＩのＴＣＧ資格証明が依然として有効であるかどうかを検証する。

【０２０３】

２Ｂ．ＲＩがデバイスに対してＲＩの完全性ステータスを検証することをデバイスが望むというデバイスからの指示を、スタンドアロンのメッセージとして、または変更されたＲＯＡＰプロトコルメッセージの一部として、ＲＩが受信するといつでも。

【０２０４】

２Ｃ．定期的に、指定されたセキュリティで保護された時間、例えば、ＲＩが、デバイスに対してＲＩの完全性ステータスを前回に検証して以来、$T_{RI-PLATFORM-LAST-REPORT}$が経過するたびに。

【０２０５】

３．デバイスとＣＩの間のプラットフォーム完全性検証に関して、前述した機構と同様の機構が、完全性検証プロセスの定期的発生および／またはイベント駆動の発生に関して考慮されることが可能である。また、ＣＩのプラットフォーム完全性のデバイスによる検証の場合、検証は、コンテンツが購入される、またはダウンロードされることが必要とされるのに先立って毎回、実行されることも可能であり、場合により、その逆（すなわち、デバイスのプラットフォーム完全性が、ＣＩに対して検証されなければならない）も同様である。

【０２０６】

従来技術は、堅牢なＤＲＭのアプリケーションに結合されたＴＣＧ技術を使用する「セキュリティで保護された起動」の使用を考慮してきた。そのようなスキームにおいて、プラットフォームのＯＳ、および他の起動関連のコードは、デバイスが起動されるといつでも、完全性検査され、プラットフォーム完全性検査を暗黙に実行してからでないと、いずれのＤＲＭアプリケーションも実行されることが可能でない。本発明は、起動時プラット

フォーム完全性検査のより系統立った、明示的な使用とともに、所定の期間に基づく他の時点におけるプラットフォーム完全性検査、ならびにいくつかのイベントの発生時のプラットフォーム完全性検査を提供する。また、本発明は、プラットフォーム完全性検査をデバイスからＲＩおよびＣＩにまで一般化する。継続的なプラットフォーム完全性検査は、デバイスが、或る特定の有効なＣＯを正しく受信しただけで、ＲＩまたはＣＩが、その時点から将来にわたって無期限に信頼できると見なされるべきことにはならないということのために、有益である。信頼性の定期的な、さらに／またはイベント駆動の継続的検証は、良好な保護機構を提供する。

【０２０７】

また、デバイスとＣＩの間の完全性検査の必要性に関して、コンテンツが、ＲＯより前に着信した場合でも、コンテンツは、ＣＩのプラットフォームまたはＣＩのＤＲＭ　ＳＷが侵害されると、侵害される可能性がある。例えば、ユーザが、或るファイルをダウンロードしたものと想定されたい。ＲＯが、まだ獲得されていない場合でも、ユーザは、コンテンツを誤ってクリックする可能性があり、あるいはコンテンツに対して有効性検査を実行する可能性がある。コンテンツが、侵害されたている（例えば、コンテンツにウイルスが添付されている）場合、コンテンツは、ＲＯなしでも、デバイスに損害を与える可能性がある。また、デバイスとＣＩの間のダウンロード前の対話において（例えば、発見段階中に）、侵害されたデバイスが、例えば、コンテンツに添付されたウイルスを、ＣＩを宛先とするメッセージに追加することによって、ＣＩに害を与える可能性がある。さらに、ビジネスの点から、ＣＩは、侵害されたデバイスにコンテンツを送信することを望まず、つまり、例えば、侵害されたデバイスは、許可のない受信者にコンテンツを無料で再配布する可能性がある。このため、デバイスとＣＩの間の相互プラットフォーム（およびＳＷ）完全性検証は、システム全体を保護することにメリットがある。

【０２０８】

また、前段のアーキテクチャの説明において概要を述べた中心的な考えを実現する、いくつかの異なる仕方が存在することが可能であることに留意されたい。２つのそのような例が、後段で説明されるが、これらは、前段で説明されるアーキテクチャに基づくより広い概念の説明的な例に過ぎないことに留意されたい。

【０２０９】

（プラットフォーム完全性検証）

【０２１０】

図８は、２つのエンティティ間のプラットフォーム完全性検証を実行するための方法８００の流れ図である。この２つのエンティティは、デバイスとＲＩ、デバイスとＣＩ、またはＲＩとＣＩであることが可能である。方法８００は、ＲＥ（要求するエンティティ）とＴＥ（ターゲットエンティティ）とを利用し、つまり、ペアのいずれのエンティティ（デバイス、ＲＩ、またはＣＩ）が、ＲＥであることも可能であることに留意されたい。方法８００は、いずれのエンティティがＲＥであり、いずれのエンティティがＴＥであるかにかかわらず、同一の仕方で動作する。

【０２１１】

方法８００は、ＲＥが、ＴＥのプラットフォーム完全性ステータスを報告するよう、ＴＥに要求を送信することから始まる（ステップ８０２）。この要求に応答して、ＴＥは、ＴＥのＴＣＧ資格証明をＲＥに送信する（ステップ８０４）。これらのＴＣＧ資格証明には、例えば、プラットフォーム資格証明、ＴＰＭ資格証明、または準拠資格証明が含まれることが可能である。次に、ＲＥが、ＴＥのＴＣＧ資格証明を、これらの資格証明の検証のためにＯＣＳＰレスポンダに送信する（ステップ８０６）。ＯＣＳＰレスポンダは、ＴＥのＴＣＧ資格証明を精査して、検証ステータスをＲＥに報告する（ステップ８０８）。

【０２１２】

ＲＥが、ＴＥ自らのプラットフォーム完全性ステータスを報告するよう、ＴＥに要求を送信する（ステップ８１０）。ＴＥは、ＴＥのプラットフォーム完全性ステータスを検査し（ステップ８１２）、プラットフォーム完全性ステータスフラグをＲＥに送信し（ステ

ップ８１４）、方法は、終了する（ステップ８１６）。
【０２１３】
方法８００は、ＲＯＡＰプロトコルの変更が行われなくても（図９に関連して後段で説明される）、ＲＯＡＰプロトコルの変更が行われても（図１０に関連して後段で説明される）、適用されることが可能である。
【０２１４】
（ＲＯＡＰプロトコルの変更なしの完全性検証）
【０２１５】
図９は、ＲＯＡＰプロトコルとは別個にＴＣＧ技術を使用して（すなわち、ＯＣＳＰレスポンダ／ＰＣＡ９０６を利用して）、デバイス９０２とＲＩ９０４の間で完全性関連の情報を交換する方法９００の流れ図である。方法９００では、同一のエンティティ９０６が、ＤＲＭ処理のためのＰＣＡとしても、ＴＣＧ処理のためのＯＣＳＰレスポンダとしても示されていることに留意されたい。方法９００では、プラットフォーム完全性検証（破線の長方形で示される）は、ＲＯＡＰ４パス登録プロトコルに先立って実行される。登録プロトコルより前にプラットフォーム完全性検証を実行することは、登録プロトコルが、頻繁には実行されず、プラットフォーム完全性検証プロセスが、完了するのにいくらかの時間を要するため、有用であり、つまり、プラットフォーム完全性検証が、各メッセージで実行されたとした場合、システムの全体的な動作は、不必要に減速させられる可能性がある。当業者は、プラットフォーム完全性検証が実行された後、１つだけのデバイスハローメッセージが、信頼されるデバイスを示すので、ＲＩによって受信されるものと想定することができる。複数のデバイスハローメッセージが、同一のデバイスからＲＩによって受信されたとした場合、このことは、ＤｏＳ攻撃の表れである可能性がある。また、プラットフォーム完全性検証は、認証プロトコルおよびオブジェクト獲得プロトコルに関連して実行されることも可能である。
【０２１６】
デバイス９０２は、ＲＩ９０４を相手に４パス登録プロトコルを開始することに先立って、ＲＩ９０４を相手に、プラットフォーム完全性の相互検証を実行する別の手続きセットを開始する。デバイス９０２はまず、デバイス９０２自らのＴＣＧ資格証明（例えば、プラットフォーム資格証明、ＴＰＭ資格証明、準拠資格証明など）、あるいはＴＣＧ資格証明を含む、またはＴＣＧ資格証明と関係する他の情報を、ＲＩ９０４に送信する（ステップ９１０）。オプションとして、デバイス９０２は、ＲＩ９０４自らのプラットフォーム完全性ステータスを検査して、デバイス９０２に報告するよう、ＲＩ９０４に要求を送信することも行い、この要求には、デバイス資格証明が含められる。
【０２１７】
ＲＩ９０４は、デバイスのＴＣＧ資格証明を検証するようＰＣＡ９０６に要求する（ステップ９１２）。ＰＣＡ９０６は、ＲＩの要求に応答して、デバイスのＴＣＧ資格証明に関する情報を送信する（ステップ９１４）。
【０２１８】
ＲＩ９０４は、デバイス９０２のプラットフォーム完全性ステータスフラグを報告するよう、デバイス９０２に要求する（ステップ９１６）。また、デバイス９０２が、ステップ９１０で、ＲＩ９０４が、ＲＩ９０４のプラットフォーム完全性ステータスを検証して、報告することを要求し、かつＲＩ９０４が、この要求に応じることを望み、応じることができる場合、ＲＩ９０４は、ＲＩ９０４自らのＴＣＧ資格証明、あるいはＴＣＧ資格証明を含む、またはＴＣＧ資格証明と関係する他の情報を、ステップ９１６で、デバイス９０２に送信する。ＲＩ９０４が、この要求に応じることができない、または応じることを望まない場合、ＲＩ９０４は、「応じない」メッセージをデバイスに送信する。ＲＩ９０４は、リソースが限られたＲＩ（すなわち、ＲＩが、この要求に応答するのに利用可能なリソースを十分に有さない）、またはデバイス信頼性検査が不合格であることを含め、いくつかの理由で、この要求に応答しない可能性がある。デバイスは、デバイスがＲＩに対して有する信用レベルに依存して、このプロトコルを中止することができ、つまり、デバ

イスが、ＲＩを信頼する場合、デバイスは、ＲＩが、この要求に応答することを拒否した場合でも、このプロトコルを続ける可能性が高い。ＲＩ９０４から、プラットフォームステータスを検査する要求を受信すると、デバイス９０２は、デバイス９０２自らのプラットフォーム完全性ステータスを検査する（ステップ９１８）。

【０２１９】

デバイス９０２は、ＲＩのＴＣＧ資格証明を検証するよう、ＰＣＡ９０６に要求する（ステップ９２０）。ＰＣＡ９０６は、デバイス９０２からこの要求を受信すると、ＲＩのＴＣＧ資格証明に関する情報を戻す（ステップ９２２）。デバイス９０２は、デバイス９０２のプラットフォーム完全性ステータスフラグをＲＩ９０４に送信する（ステップ９２４）。ＲＩ９０４が、ＲＩ９０４の完全性ステータスを検査するよう、デバイス９０２から要求を受信し、ＲＩ９０４が、この要求に応じることを望み、応じることができる場合、ＲＩ９０４は、ＲＩ９０４自らのプラットフォーム完全性を検査する（ステップ９２６）。次に、ＲＩは、ＲＩのプラットフォーム完全性ステータスフラグをデバイス９０２に戻す（ステップ９２８）。ＲＩ完全性検査に関するオプションのステップは、任意の順序で実行されることが可能であり、つまり、それらのステップは、図９に示されるとおりにデバイス完全性検査と絡み合わされなくてもよい。さらに、ＲＩは、ＲＩ自らの完全性検査を開始することができる。また、ＲＩが、可能な理由のいずれかで、ＲＩ自らのＴＣＧ資格証明情報で要求に完全には応答することを拒否する場合、ＲＩは、例えば、ステップ９２２で、適切な仕方で、そのような事実をデバイスに示すことができる。

【０２２０】

方法９００は、デバイス９０２およびＲＩ９０４が、相互プラットフォーム完全性検証を実現することを可能にする。そのような検証後、デバイスは、ＲＯＡＰ登録プロトコルを開始することができる。図９に示される登録プロトコルのステップ（ステップ９３０～９４０）は、前述した方法２００のステップ２１０～２２０と同一である。また、これらの手続きは、周期的な間隔でトリガされる、または繰り返されることが可能であることにも留意されたい。

【０２２１】

（ＲＯＡＰ登録プロトコルの変更を伴う完全性検証）

【０２２２】

図１０は、別の例示的な実施形態において、デバイス１００２とＲＩ１００４が、ＯＣＳＰレスポンダ／ＰＣＡ１００６のサービスをやはり利用して、完全性関連の情報を交換する方法１０００を示す。方法１０００では、ＲＯＡＰ登録プロトコルの既存のデバイスハローメッセージおよびＲＩハローメッセージは、ＴＣＧ資格証明と、プラットフォーム完全性検証を求める、相手への要求をともに伝えるように変更される。

【０２２３】

デバイス１００２は、変更されたデバイスハローメッセージをＲＩ１００４に送信し（ステップ１０１０）、このメッセージは、デバイスＴＣＧ資格証明と、ＲＩ１００４のプラットフォーム完全性を報告するようにという、ＲＩ１００４へのオプションの要求とを含む。ＲＩ１００４は、これらのデバイス資格証明を、検証ためにＰＣＡ１００６に転送する（ステップ１０１２）。次に、ＰＣＡ１００６は、デバイスＴＣＧ資格証明をＲＩ１００４に戻す（ステップ１０１４）。ＲＩ１００４は、変更されたＲＩハローメッセージでデバイス１００２に応答し（ステップ１０１６）、このメッセージは、ＲＩのＴＣＧ資格証明をオプションとして含む。

【０２２４】

次に、デバイス１００２は、オプションとして、ＲＩのＴＣＧ資格証明を検査するようＰＣＡ１００６に要求を送信する（ステップ１０１８）。ＰＣＡ１００６はＲＩの資格証明を検査し、結果をデバイス１００２に報告する（ステップ１０２０）。デバイス１００２は、デバイス１００２自らの完全性ステータスを検査し（ステップ１０２２）、完全性ステータスをＲＩ１００４に報告する（ステップ１０２４）。

【０２２５】

デバイス１００２が、ＲＩ１００４が、ＲＩ１００４の完全性ステータスを報告することを要求した場合、ＲＩ１００４は、プラットフォーム完全性検査を実行し（ステップ１０２６）、完全性ステータス、例えば、ＲＩ１００４の信頼状態フラグを、デバイス１００２に送り返す（ステップ１０２８）。ステップ１０３０～１０３６は、ＲＯＡＰ登録プロトコルの図２に示されるステップ２１４～２２０と同一である。

【０２２６】

（ＤＲＭソフトウェアの完全性を検査すること）

【０２２７】

図１１は、ＤＲＭエンティティの任意のペアの間でＤＲＭ　ＳＷ（例えば、デバイスに常駐するＤＲＭユーザエージェントＳＷ、あるいはＲＩまたはＣＩに常駐するＤＲＭ　ＳＷ）の完全性を検査するための方法１１００の流れ図である。ＲＥ（要求するエンティティ）が、ＤＲＭ　ＳＷ完全性検査を実行するよう、ＴＥ（ターゲットエンティティ）に要求を送信する（ステップ１１０２）。ＴＥは、ＴＥのＤＲＭ　ＳＷ完全性を検査し（ステップ１１０４）、ＤＲＭ　ＳＷ完全性ステータスフラグをＲＥに送信し（ステップ１１０６）、方法は、終了する（ステップ１１０８）。ＴＥが、デバイスである場合、デバイスドライバおよびメディアプレーヤＳＷの完全性が、ＤＲＭ　ＳＷの完全性とは別個に検査されることが、これら２つの構成要素が、デバイス上に別々に存在する場合、可能であることに留意されたい。

【０２２８】

方法１１００は、ＲＥが、ＴＥからＤＲＭ　ＳＷ完全性検査を獲得することだけに関する。相互ＤＲＭ　ＳＷ完全性検査を実行するのに、方法１１００は、ＲＥからＴＥに１回、次に、ＴＥからＲＥに１回（ＲＥとＴＥが役割を交替して）の、２回、実行される必要がある。相互ＤＲＭ　ＳＷ完全性検査中、これらの要求は、絡み合わされる（図１２に示されるとおり）ことも、図１１に示されるとおり、分離されることも可能である。この方法の動作は、相互ＤＲＭ　ＳＷ完全性検査が実行されている場合、変化しない。

【０２２９】

ＯＭＡ　ＤＲＭ２．０仕様は、そのような想定が、どのようにして有効に実施されることが可能であるかを示唆することなしに、ＤＲＭユーザエージェントＳＷ（または本発明において使用される用語では、デバイスＤＲＭ　ＳＷ）、およびＲＩ（またはＲＩのＤＲＭ　ＳＷ）が、暗黙に信頼されることが可能であるものと想定する。このため、ＯＭＡ　ＤＲＭ２．０仕様における認証プロトコルは、既に信用できると考えられるエンティティ間の実際の認証手続きだけしか規定しない。明白な理由で、この暗黙のＳＷ信頼想定は、実際には、それらの想定を実施し、検証する実際のステップなしに、自動的に想定されることは可能でない。このセクションで説明される方法は、そのような具体的なステップにかかわる。

【０２３０】

図１２は、ＲＯＡＰ　ＲＯ獲得プロトコルに関連してＤＲＭ　ＳＷ検査を適用するための方法１２００の流れ図である。この方法１２００は、デバイス１２０２、ＲＩ１２０４、およびＯＣＳＰレスポンダ／ＰＣＡ１２０６を利用する。第１に、ＰＣＡ１２０６は、デバイス１２０２およびＲＩ１２０４と通信して、プラットフォーム完全性検査およびＲＯＡＰ登録プロトコルを実行する（ステップ１２１０）。デバイス１２０２とＲＩ１２０４が、相互プラットフォーム完全性検査、単方向ＤＲＭ　ＳＷ完全性検査、または相互ＤＲＭ　ＳＷ完全性検査を実行する（ステップ１２１２）。

【０２３１】

ＲＩ１２０４が、デバイスのＤＲＭ　ＵＡ（ユーザエージェント）ＳＷ完全性を検査して、報告するよう、デバイス１２０２に要求を送信する（ステップ１２１４）。デバイス１２０２が、デバイス１２０２の最新のＤＲＭ　ＵＡ　ＳＷ完全性を検査する（ステップ１２１６）。デバイス１２０２は、オプションとして、ＲＩのＤＲＭ　ＳＷ完全性を検査して、報告するよう、ＲＩ１２０４に要求を送信する（ステップ１２１８）。要求された場合、ＲＩ１２０４は、ＲＩ１２０４の最新のＤＲＭ　ＳＷ完全性を検査する（ステップ

１２２０）。デバイス１２０２が、デバイスＤＲＭ　ＳＷ完全性ステータスフラグをＲＩ１２０４に送信する（ステップ１２２２）。前に要求されている場合、ＲＩ１２０４が、ＲＩ　ＤＲＭ　ＳＷ完全性ステータスフラグをデバイス１２０２に送信する（ステップ１２２４）。オプションのＲＩ完全性検査のステップは、任意の順序で実行されることが可能であり、図１２に示されるとおりにデバイス完全性検査と絡み合わされる必要はないことに留意されたい。

【０２３２】

方法１２００は、例示されるデバイス／ＲＩ対話の代わりに、デバイスとＣＩの間の相互ＤＲＭ　ＳＷ完全性検証に関して一般化されることが可能であることに留意されたい。ステップ１２１０～１２２４が完了すると、デバイス１２０２は、例えば、図３に関連して前述したステップ３１０および３１２と同一であるステップ１２２６および１２２８における２パスＲＯ獲得プロトコルを開始することができる。方法１２００は、ＲＯ獲得プロトコルに関連して図示されるものの、方法１２００は、他の任意のＲＯＡＰプロトコルに関連して使用されることが可能であり、ただし、方法１２００に関連するオーバヘッドを最小限に抑えるのに、方法１２００は、任意の所与の時点で、ＲＯＡＰプロトコルの適切に選択されたサブセットだけしか伴わずに実行されることが可能であることにさらに留意されたい。実際的なＯＭＡ　ＤＲＭシステム実施形態に関して、前述した、提案されるプラットフォーム完全性検証手続きおよび／またはＤＲＭ　ＳＷ完全性検証手続きのための条件またはトリガ機構のいくつかには、以下が含まれることが可能である。すなわち、

【０２３３】

１．デバイスＤＲＭ　ＳＷ完全性検証手続きは、以下の１つまたは複数によってトリガされることが可能である。

【０２３４】

１Ａ．デバイスが、新たな２パスＲＯＡＰ登録プロトコル、２パスドメイン参加プロトコル、または２パスドメイン退去プロトコルを開始することを要望する前。

【０２３５】

１Ｂ．定期的に、指定された時間、例えば、デバイスが、同一のＲＩに対して２パスＲＯＡＰ登録プロトコル、２パスドメイン参加プロトコル、または２パスドメイン退去プロトコルを前回に完了して以来、$T_{DEV\text{-}DRM\text{-}LAST\text{-}ROAP}$が経過するたびに。

【０２３６】

１Ｃ．定期的に、指定された時間、例えば、デバイスが、前回に、デバイスのＤＲＭ　ＳＷ完全性ステータスを検証して、同一のＲＩに報告して以来、$T_{DEV\text{-}DRM\text{-}LAST\text{-}REPORT}$が経過するたびに。

【０２３７】

１Ｄ．デバイスが、デバイスのＤＲＭ　ＳＷを更新するといつでも。

【０２３８】

１Ｅ．プラットフォームＳＷが、更新される、または変更されるといつでも。

【０２３９】

２．ＲＩ　ＤＲＭ完全性検証手続きは、以下の１つまたは複数によって実行されることが可能である。

【０２４０】

２Ａ．ＲＩがデバイスに対してＲＩのＤＲＭ　ＳＷ完全性ステータスを検証することをデバイスが望むというデバイスからの指示を、スタンドアロンのメッセージとして、または変更されたＲＯＡＰプロトコルメッセージの一部として、ＲＩが受信するといつでも。

【０２４１】

２Ｂ．定期的に、指定された時間、例えば、ＲＩが、前回に、ＲＩのＤＲＭ　ＳＷ完全性ステータスを検証して、デバイスに報告して以来、$T_{RI\text{-}DRM\text{-}LAST\text{-}REPORT}$が経過するたびに。

【０２４２】

２Ｃ．ＲＩが、ＲＩのＤＲＭ　ＳＷを更新するといつでも。

【０２４３】
２Ｄ．ユーザが、ストリーミングコンテンツの場合のように、コンテンツを頻繁に獲得している場合において、デバイスがＲＯ要求を送信するのに先立って毎回。
【０２４４】
デバイスとＣＩの間のプラットフォーム完全性検証に関して、前述した機構と同様の機構が、ＤＲＭ　ＳＷ完全性検証プロセスの定期的発生および／またはイベント駆動の発生に関して考慮されることが可能である。
【０２４５】
ＤＲＭプラットフォーム検証およびＤＲＭ　ＳＷ検証のための提案される方法は、互いに無関係に実行されることが可能であるが、これらの検証手続きが、手続きのグループの一部として組み合わされることが可能であることも企図される。そのような実施形態では、ＤＲＭプラットフォーム検証ステップは、ＤＲＭ　ＳＷ検証ステップの前提条件と考えられる。例えば、デバイスとＲＩの間の完全性検証のために、デバイスとＲＩはまず、前述したとおり、ＤＲＭプラットフォーム検証手続きを実行することによって、互いのプラットフォーム全体に対する信頼を確立する。トリガ機構は、一般的なプラットフォーム検証トリガ条件を含む。次に、ＤＲＭ　ＳＷ検証トリガに関する条件が生じると、ＤＲＭ　ＳＷ検証手続きが、その後に続く。両方のタイプの検証手続きは、それぞれのトリガ条件が満たされると、実行されることに留意されたい。しかし、ＤＲＭ　ＳＷ検証ステップは、ＤＲＭプラットフォーム検証ステップが成功して完了することに追従させられ、すなわち、デバイスとＲＩの間でＤＲＭプラットフォーム検証が不合格である場合、ＤＲＭ　ＳＷ検証におけるさらなる処理、ならびに実際のＤＲＭ　ＲＯＡＰ処理および使用関連の処理は、失敗する。
【０２４６】
（密封署名および結び付け）
【０２４７】
ＲＯＡＰプロトコルの完全性を保護するＯＭＡ　ＤＲＭ２．０仕様の既存の機構は、ＲＯＡＰメッセージのいくつかに、ただし、すべてにではなく、デジタル署名（またはメッセージ完全性検査）を含めることに限られる。ＲＯＡＰプロトコルが、セキュリティで保護されたＤＲＭ処理実施に中心的な重要性を有することから、ＲＯＡＰプロトコルにおいて使用され、交換される情報の完全性を保護し、絶えず検証することが重要である。
【０２４８】
したがって、本発明の代替の実施形態では、ＤＲＭデバイスとＲＩの間の信頼できる認証および完全性検証に中心的な情報が、（１）ＴＣＧ技術を使用して安全に格納され、さらに（２）他方の側に伝送されるのに先立って、または情報が格納される側において処理のために使用されるのに先立って、事前検証されることが可能である、ＲＯＡＰプロトコルの完全性を強化する方法が、開示される。
【０２４９】
この方法には、密封署名（すなわち、ターゲット情報を対称的に暗号化し、次に、対称鍵に加え、プラットフォームまたは特定のＳＷ構成要素のその時点で最新の完全性ステータスを示すＰＣＲ値のセットに非対称的に署名する）、および結び付け（秘密解読鍵がＴＰＭなどの、保護されたモジュールの中に保持された鍵を使用して、ターゲット情報を非対称的に暗号化する）というＴＣＧ技術を使用する２つの基本的な手続きがかかわる。密封署名は、保護されたＰＣＲ値によって示される、デバイスＤＲＭユーザエージェントＳＷの信頼状態に、非対称暗号化、デジタル署名、および結び付けによってもたらされる最高レベルの情報セキュリティを与える。結び付けは、解読鍵がＴＰＭ内部で保護される場合に、非対称暗号化を使用する高いレベルの保護を与える。
【０２５０】
以下の体系的な原理は、密封署名、および結び付けを使用して、ＲＯＡＰメッセージの中で使用される情報の機密性と完全性をともに保護して、ＲＯＡＰプロトコル自体の完全性の強度を間接的に高める。以下の説明において、デバイスとＲＩ（またはこの特定のデ

バイスを扱うＲＩの部分）はともに、ＴＰＭを備えており、完全なＴＰＭ機能をサポートするものと想定される。

【０２５１】

デバイスとＲＩはそれぞれ、デバイスまたはＲＩが存在する信頼されるプラットフォームに、ＲＯＡＰ処理と関係する或る情報を暗号上、結び付け、セキュリティで保護された仕方で格納する２つのストレージ鍵のセットを取っておき、使用することができる。デバイスに関して、これらの鍵は、Ｋ＿ＤＥＶ＿ＢＩＮＤ＿ＡおよびＫ＿ＤＥＶ＿ＢＩＮＤ＿Ｂである。ＲＩに関して、これらの鍵は、Ｋ＿ＲＩ＿ＢＩＮＤ＿ＡおよびＫ＿ＲＩ＿ＢＩＮＤ＿Ｂである。これらの鍵は、ＴＰＭによって保持される非対称鍵（すなわち、暗号化は、公開鍵を使用して行われ、解読は、ＴＰＭ内で保護された秘密鍵を使用して行われる）である。

【０２５２】

デバイスとＲＩはそれぞれ、ＤＲＭ処理のために単一のＰＣＲ、またはＰＣＲのセットを使用する。また、デバイスとＲＩは、ＡＩＫ（構成証明アイデンティティ鍵）を取っておき、信頼されるプラットフォーム、およびそのプラットフォームの特定のＰＣＲ値に、ＲＯＡＰ処理と関係する或る情報を密封署名するのに使用する。ＴＣＧ　ＡＩＫ鍵は、ＰＣＲ値に署名するためだけに使用されることに留意されたい。デバイスに関して、デバイスのＡＩＫは、Ｋ＿ＤＥＶ＿ＡＩＫであり、ＲＩに関して、ＲＩのＡＩＫは、Ｋ＿ＲＩ＿ＡＩＫである。また、密封署名は、ターゲットデータの暗号化操作のための非対称ストレージ鍵を要求する。このため、デバイスとＲＩはそれぞれ、この目的でストレージ鍵を取っておき、使用する。デバイスに関するストレージ鍵は、Ｋ＿ＤＥＶ＿ＳＴＯ＿ＳＥＡＬであり、ＲＩに関するストレージ鍵は、Ｋ＿ＲＩ＿ＳＴＯ＿ＳＥＡＬである。

【０２５３】

この方法は、ＲＯＡＰ処理にかかわる様々な情報要素を格納することの強度を高めるように、密封署名および結び付けと、機密性および完全性を保護する追加の対策との組合せを使用する。例えば、図１３は、ＴＰＭ密封署名操作およびＴＰＭ結び付け操作を使用して、４パスＲＯＡＰ登録プロトコルを含む様々なメッセージの中の情報の機密性および完全性が保護される方法１３００の流れ図である。方法１３００では、デバイス１３０２とＲＩ１３０４がそれぞれ、４パス登録プロトコルの過程においてそれぞれが送信する（他方の側に）または受信する（他方の側から）ストレージ鍵の２つのセットを使用して、ＲＯＡＰ関連の情報の選択的なセットに密封署名し、情報を結び付ける。

【０２５４】

デバイス１３０２がまず、暗号化鍵Ｋ＿ＤＥＶ＿ＳＴＯ＿ＳＥＡＬおよびデバイス特有のＡＩＫ、Ｋ＿ＤＥＶ＿ＡＩＫを使用して、デバイスＩＤ情報要素（ＯＭＡ　ＤＲＭの場合、ＯＭＡ　ＤＲＭ公開鍵のＳＨＡ－１ハッシュである）に密封署名する。この情報は、ストレージ鍵Ｋ＿ＤＥＶ＿ＢＩＮＤ＿Ａを使用して、デバイスハローメッセージ向けの他の情報に結び付けられる（非対称暗号化を使用して）（ステップ１３１０）。次に、このデバイスハローメッセージが、デバイス１３０２からＲＩ１３０４に送信される（ステップ１３１２）。

【０２５５】

デバイスＩＤなどの情報に密封署名すること、およびデバイスハローメッセージを含む他の情報を結び付けることにより、デバイス１３０２は、デバイス１３０２が、デバイス１３０２の保護されたストレージから以前に密封署名され、結び付けられた情報を回復し（すなわち、密封署名解除して、結び付け解除し）、それらの情報を、ＤＲＭ　ＳＷが使用している可能性があるような情報要素の現在の値と比較し、これらの現在の値の真正性および完全性を検証すると、その場合に限って、デバイスハローメッセージが伝送されるというポリシーを定めることもできる。このシナリオにおける、密封署名されるべき情報要素対結び付けられるべき情報要素の選択は、例として与えられているに過ぎないことに留意されたい。他の情報要素は、本発明の動作を実行することなしに、様々な組合せで密封署名され、結び付けられることが可能である。他の組合せは、システム時間、メッセー

ジの中の任意の情報要素、アルゴリズム、およびナンスなどのアイテムから導き出されることが可能である。ナンスをセキュリティで保護する１つの理由は、一部の乱数発生器、特に有害な侵害を受けている可能性がある乱数発生器は、同一のパターンを繰り返して、同一の数を乱数発生器の出力として、容認できない短い周期で生成する可能性があるので、ナンスが本当にランダムであるかどうかを判定するためである。

【０２５６】

ＲＩ１３０４は、デバイスハローメッセージの受信後、ＲＩ１３０４の結び付け鍵、ＫＩ＿ＲＩ＿ＢＩＮＤ＿Ａを使用して、デバイスハローメッセージの中に含まれる情報を結び付ける（ステップ１３１４）。このステップは、ＲＩ１３０４がデバイス１３０２から受信した鍵情報の、セキュリティで保護された、完全性保護された格納を可能にする。代替として、ＲＩ１３０４は、デバイスハローメッセージからデバイスＩＤ（または他の任意の情報要素）を抽出し、ＡＩＫ、Ｋ＿ＲＩ＿ＡＩＫ、および暗号化鍵Ｋ＿ＲＩ＿ＳＴＯ＿ＳＥＡＬを別々に使用して、その情報要素に密封署名することもできる。

【０２５７】

ＲＩ１３０４が、暗号化鍵Ｋ＿ＲＩ＿ＳＴＯ＿ＳＥＡＬおよびＡＩＫ、Ｋ＿ＲＩ＿ＡＩＫを使用して、ＲＩ　ＩＤおよびＲＩ　ＵＲＬ情報要素に密封署名する（ステップ１３１６）。また、ＲＩ１３０４は、ストレージ鍵Ｋ＿ＲＩ＿ＢＩＮＤ＿Ａを使用して、ＲＩ１３０４のＲＩハローメッセージの中に含まれるその他の情報を結び付けることも行う（ステップ１３１６）。次に、ＲＩ１３０４は、ＲＩハローメッセージをデバイス１３０２に送信する（ステップ１３１８）。

【０２５８】

ＲＩ１３０４は、ＲＩ１３０４がまず、保護されたストレージから以前に密封署名され、結び付けられた情報を回復し（すなわち、密封署名解除して、結び付け解除し）、それらの情報を、ＲＩ　ＤＲＭ　ＳＷが使用している可能性があるような情報要素の現在の値と比較し、これらの現在の値の真正性および完全性を検証すると、その場合に限って、デバイス１３０２にＲＩハローメッセージを送信する。

【０２５９】

デバイス１３０２は、ＲＩハローメッセージを受信すると、第２の結び付け鍵、すなわち、Ｋ＿ＤＥＶ＿ＢＩＮＤ＿Ｂを使用して、ＲＩハローメッセージの中に含まれる情報を結び付ける（ステップ１３２０）。このステップは、デバイスがＲＩ１３０４から受信した鍵情報のセキュリティで保護された、完全性保護された格納を可能にする。代替として、デバイス１３０２は、受信されたＲＩハローメッセージから、選択された情報要素（ＲＩ　ＩＤおよび／またはＲＩ　ＵＲＬなどの）を抽出し、ＡＩＫ、Ｋ＿ＤＥＶ＿ＡＩＫおよび暗号鍵Ｋ＿ＤＥＶ＿ＳＴＯ＿ＳＥＡＬを使用して、これらの情報要素に密封署名する一方で、Ｋ＿ＤＥＶ＿ＢＩＮＤ＿Ｂを使用して、ＲＩハローメッセージの中で受信された残りの情報を単に結び付けることも可能である。

【０２６０】

デバイス１３０２が、Ｋ＿ＤＥＶ＿ＡＩＫおよびＫ＿ＤＥＶ＿ＳＴＯ＿ＳＥＡＬを使用して、証明書チェーン、ＤＣＦハッシュ、および要求時間に密封署名する（ステップ１３２２）。次に、デバイス１３０２は、Ｋ＿ＤＥＶ＿ＢＩＮＤ＿Ａを使用して、登録要求メッセージ向けのその他の情報を結び付ける（ステップ１３２２）。次に、デバイス１３０２は、この登録要求メッセージをＲＩ１３０４に送信する（ステップ１３２４）。デバイス１３０２は、デバイス１３０２が、以前に密封署名され、結び付けられた情報を回復し（すなわち、密封署名解除して、結び付け解除し）、回復された値を、ＤＲＭ　ＳＷメモリの中で使用される現在の一時的な値と比較し、これらの現在の値の真正性および完全性を検証すると、その場合に限って、この登録要求メッセージを送信する。この登録要求メッセージを受信すると、ＲＩ１３０４は、結び付け鍵、Ｋ＿ＲＩ＿ＢＩＮＤ＿Ｂを使用して、登録要求メッセージからの情報を結び付ける（ステップ１３２６）。

【０２６１】

ＲＩ１３０４が、ＫＩ＿ＲＩ＿ＡＩＫおよびＫ＿ＲＩ＿ＳＴＯ＿ＳＥＡＬを使用して、

鍵、証明書チェーン、およびＲＯに密封署名する（ステップ１３２８）。次に、ＲＩ１３０４は、密封署名された鍵、証明書チェーン、およびＲＯを、結び付け鍵Ｋ＿ＲＩ＿ＢＩＮＤ＿Ａを使用して、登録応答メッセージに含められるべき他の情報に結び付ける（ステップ１３２８）。次に、ＲＩ１３０４は、この登録応答メッセージをデバイス１３０２に送信する（ステップ１３３０）。ＲＩ１３０４は、ＲＩが、以前に密封署名され、結び付けられた情報を回復し（すなわち、密封署名解除して、結び付け解除し）、これらの回復された値を、ＤＲＭ　ＳＷメモリの中で使用される現在の一時的な値と比較し、これらの現在の値の真正性および完全性を検証した場合に限って、この登録応答メッセージを送信する。登録応答メッセージを受信すると、デバイス１３０２は、登録応答メッセージからのＲＩによって生成された情報を、結び付け鍵Ｋ＿ＤＥＶ＿ＢＩＮＤ＿Ｂを使用して結び付ける（ステップ１３３２）。

【０２６２】

この密封署名および結び付けは、他の任意のＲＯＡＰプロトコルで使用されることが可能であることに留意されたい。前述した方法１３００は、例示的であり、方法１３００の原理は、他の任意のＲＯＡＰプロトコルにも等しく適用されることが可能である。

【０２６３】

ＯＭＡ　ＤＲＭ　ＲＯＡＰメッセージ交換中に獲得されたデータは、このデータを密封した、またはこのデータに密封署名したエンティティが、そのエンティティのＯＳまたはＤＲＭ　ＳＷを更新した場合、密封解除され、新たな構成ＰＣＲ値に再密封される必要がある。そのような事態が生じると、或る特定の状態（または、均等なこととして、或る特定のＰＣＲ値セット）に密封されていた、または密封署名されていたＤＲＭ　ＲＯＡＰ関連のデータが、最初に、密封解除され、次に、更新されたプラットフォームＯＳの最新の状態に再密封されなければならない。この手続き要件に対処する既存の技術が、従来技術に存在し、そのような手続きは、本明細書で提案される密封または密封署名を使用して格納された任意のＤＲＭ　ＲＯＡＰ関連のデータの適切な密封解除および再密封を確実にするように行われるものと想定される。

【０２６４】

１つのさらなる機能強化は、送信するデバイスのＴＣＧ能力を示すフィールドを、既存のＲＯＡＰメッセージフォーマットに追加することである。このＴＣＧ能力フィールドは、受信するエンティティが、ＴＣＧ関連の情報および手続きをサポートすることができるかどうかの早期判定を行うことによって、レガシーデバイスとの相互運用性を高めることに役立つことが可能である。

【０２６５】

（デバイスハローメッセージの変更、およびこの変更の導出）

【０２６６】

第１の変更は、デバイスのＴＰＣ能力の標識である、新たなＤＴＣＩ（デバイスＴＰＭ能力指示）を、デバイスハローメッセージの既存の拡張子パラメータの新たな要素の中に追加すること、または代替として、好ましくは、このＤＣＴＩを、デバイスハローメッセージのヘッダの中の新たな第１のパラメータとして追加することである。ＤＴＣＩは、１ビット（デバイスＴＰＭの欠如、または存在を示す）、または数ビット（デバイスのＴＰＭ能力に関して、より細分性の高い情報を示す）であることが可能である。ＤＴＣＩは、新たなパラメータとして挿入される場合、好ましくは、デバイスＩＤパラメータより前に、最初のパラメータとして挿入されて、他のパラメータに先立って、デバイスがいくつかのＴＰＣ能力を有することをＲＩが知り、ＤＴＣＩを利用して、後のパラメータ（例えば、デバイスＩＤ）からの情報を処理することができるようにされなければならない。ＤＴＣＩ情報の利点は、この情報により、ＲＩが、ＲＯＡＰプロトコルの残りの部分におけるデバイスとのさらなる対話において、デバイスの信頼性を評価することが可能になることである。

【０２６７】

第２の変更は、デバイス特有のＴＣＧ　ＥＫ資格証明またはＴＣＧ　ＡＩＫ資格証明を

使用して、ＤＲＭデバイスＩＤをハッシングし、導き出すことである。この変更の利点は、ＥＫ資格証明および／またはＡＩＫ資格証明が、デバイス内のＴＰＭによって強固に保護されており、このため、これらの資格証明のいずれかからＤＲＭデバイスＩＤを導き出すことにより、ＤＲＭデバイスＩＤ情報の完全性が強化されることである。

【０２６８】

第３の変更は、署名までの、署名を除くデバイスハローメッセージに、ＲＩによって検証されることが意図される、デバイスのＡＩＫ秘密鍵を使用して署名が行われる場合に、新たな署名パラメータを追加することである。この変更の利点は、デバイスとＲＩの間の最初の対話から、デバイスＴＰＭ能力の完全性を保護することである。ＴＰＭによって強固に保護される、デバイスのＡＩＫ秘密鍵の使用により、署名動作の完全性が強化される。

【０２６９】

テーブル１２および１３は、変更されたデバイスハローメッセージに関する可能な２つのフォーマットを示す。テーブル１２は、最初のパラメータとしてＤＴＣＩビットを有するメッセージのフォーマットを示す。テーブル１３は、ＤＴＣＩが、既存の拡張子パラメータの新たな要素である、デバイスハローメッセージのフォーマットを示す。

【０２７０】

【表１２】

表12 別個のDTCIパラメータを有する変更されたデバイスハローメッセージフォーマット

パラメータ	必須またはオプション	メモ(OMA DRM2.0 ROAPデバイスハローメッセージからの変更)
DTCI(デバイスTPM能力標識)	オプション	新たなパラメータ:1ビット(デバイスTPMの欠如、または存在を示すための)、またはデバイスのTPM能力について、より細分性の高い情報を示す、より多くのビット。
バージョン	必須	変更なし。
デバイスID	必須	フォーマットに変更はないが、デバイスTPMのEK資格証明、またはデバイスTPMのAIK資格証明の1つの資格証明のデバイスTPMによって計算されたSHA-1ハッシュを使用する。
サポートされるアルゴリズム	オプション	変更なし。
拡張子	オプション	変更なし。
署名	必須	新たなパラメータ:RIが公開鍵をあらかじめ獲得しているデバイスのAIK秘密鍵の1つによって署名された、署名パラメータまでの、署名パラメータを除くデバイスハローメッセージに対して、RSA-PSSアルゴリズムを使用した署名。

【０２７１】

【表１３】
表13 拡張子の中にDTCIを有する変更されたデバイスハローメッセージフォーマット

パラメータ	必須またはオプション	メモ(OMA DRM2.0 ROAPデバイスハローメッセージからの変更)
バージョン	必須	変更なし。
デバイスID	必須	フォーマットに変更はないが、デバイスTPMのEK資格証明、またはデバイスTPMのAIK資格証明の1つの資格証明のデバイスTPMによって計算されたSHA-1ハッシュを使用する。
サポートされるアルゴリズム	オプション	変更なし。
拡張子	オプション	OMA DRM2.0 ROAPデバイスハロー拡張子要素のすべてに加えて、デバイスのTPM能力を示す1つまたは複数のビットから成るDTCI要素。
署名	必須	新たなパラメータ:RIが公開鍵をあらかじめ獲得しているデバイスのAIK秘密鍵の1つによって署名された、署名パラメータまでの、署名パラメータを除くデバイスハローメッセージに対して、RSA-PSSアルゴリズムを使用した署名。

【０２７２】
（ＲＩハローメッセージの変更、およびこの変更の導出）
【０２７３】
第１の変更は、ＲＩのＴＰＭ能力の標識である新たなＲＴＣＩ（ＲＩ　ＴＰＭ能力指示）を、ＲＩハローメッセージの既存の拡張子パラメータの新たな要素として追加すること、または代替として、好ましくは、このＲＴＣＩを、ＲＩハローメッセージのヘッダの中の新たな第１のパラメータとして追加することである。この変更の利点は、この変更により、デバイスが、ＲＴＣＩ情報を使用して、ＲＩの信頼性を評価し、さらに、ＲＯＡＰプロトコル手続きの残りの部分におけるＲＩとのさらなる対話において、そのような情報を利用することが可能になることである。
【０２７４】
第２の変更は、ＲＩ　ＴＰＭを使用して、セッションＩＤを表す擬似乱数を提供することである。この変更の利点は、ＴＰＭが、セキュリティで強固に保護されたハードウェアベースの擬似乱数発生器を提供することである。ＴＰＭを使用して、セッションＩＤとして使用される擬似乱数を生成することにより、プロトコルのセキュリティが強化される。
【０２７５】
第３の変更は、ＲＩ　ＴＣＧ　ＥＫ資格証明、またはＲＩのＴＰＭに属するＴＣＧ　ＡＩＫ資格証明を使用して、ＲＩ　ＩＤを導き出すことである。この変更の利点は、ＥＫ資格証明および／またはＡＩＫ資格証明が、デバイス内のＴＰＭによって強固に保護され、これらの資格証明のいずれかからＤＲＭデバイスＩＤを導き出すことにより、ＤＲＭデバイスＩＤ情報の完全性が強化されることである。
【０２７６】
第４の変更は、ＲＩ　ＴＰＭを使用して、ＲＩナンスを提供することである。この変更の利点は、ＴＰＭが、セキュリティで強固に保護されたハードウェアベースの擬似乱数発生器を提供することである。ＴＰＭを使用して、ＲＩナンスを生成することにより、ＲＩハローメッセージの中で使用されるナンスの完全性が強化される。
【０２７７】

第５の変更は、デバイスによって信頼されるＲＩアンカの中にデバイスＴＣＧ資格証明を含めることである。デバイスのＴＣＧ資格証明には、ＥＫ資格証明、ＡＩＫ資格証明、プラットフォーム資格証明、ならびにＲＩが、信頼されるＴＣＧ　ＣＡから事前獲得した準拠資格証明が含まれる。この変更の利点は、デバイスがＲＩハローメッセージに対して有することが可能な信頼を強化することである。

【０２７８】

第６の変更は、ＲＩのＡＩＫ公開鍵が、ＲＩハローメッセージの一部としてデバイスにあらかじめ配布されている場合に、ＲＩのＡＩＫ秘密鍵を使用して署名された、署名までの、署名を除くＲＩハローメッセージの署名を追加することである。この変更の利点は、ＲＩとデバイスの間の最初の対話から、ＲＴＣＩの完全性を保護することである。ＲＩのＴＰＭによって強固なセキュリティで保護されたＲＩのＡＩＫ秘密鍵を使用することにより、署名動作の完全性が強化される。

【０２７９】

テーブル１４および１５は、変更されたＲＩハローメッセージに関する可能な２つのフォーマットを示す。テーブル１４は、最初のパラメータとしてＲＴＣＩビットを有するＲＩハローメッセージのフォーマットを示す。テーブル１５は、ＲＴＣＩが、既存の拡張子パラメータの新たな要素である場合の、ＲＩハローメッセージのフォーマットを示す。

【０２８０】

【表１４】

表14 変更されたRIハローメッセージフォーマット

パラメータ	ROAP-RIハロー		メモ(OMA DRM2.0 RIハローメッセージからの変更)
	ステータス=「成功」	ステータスは、「成功」でない	
RTCI(RI TPM能力標識)	オプション	オプション	新たなパラメータ:1ビット(RI TPMの欠如、または存在を示すための)、またはRI TPM能力について、より細分性の高い情報を示す、より多くのビット。
ステータス	必須	必須	変更なし。
セッションID	必須	-	フォーマットに変更はないが、RIのTPMによって生成された。
選択されたバージョン	必須	-	変更なし。
RI ID	必須	-	フォーマットに変更はないが、OMA DRM 2.0 ROAPによってサポートされるRSA-PSS法を使用して、RI TPM EK資格証明、またはRI TPM AIK資格証明の1つの資格証明の、RIのTPMによって生成されたSHA-1ハッシュを使用する。
選択されたアルゴリズム	オプション	-	変更なし。
RIナンス	必須	-	フォーマットに変更はないが、RIのTPMが存在する場合、RI TPMによって生成されるべき。
信頼されるデバイス権限	オプション	-	RIによって認識されたデバイス信頼アンカのリスト。提案される変更は、信頼アンカのリストの一部として、デバイスのTCG資格証明を含む。
サーバ情報	オプション	-	変更なし。
拡張子	オプション	-	変更なし。
署名	必須	必須	新たなパラメータ:デバイスが公開鍵をあらかじめ獲得しているRI AIK秘密鍵の1つによって署名された、署名パラメータまでの、署名パラメータを除くRIハローメッセージに対して、RSA-PSSアルゴリズムを使用して計算される。この署名は、デバイスハローメッセージの成功または失敗にかかわらず、必須である。

【０２８１】

【表１５】

表15 変更されたRIハローメッセージフォーマット

パラメータ	ROAP-RIハロー		メモ(OMA DRM2.0 RIハローからの変更)
	ステータス=「成功」	ステータスは、「成功」でない	
ステータス	必須	必須	変更なし。
セッションID	必須	-	フォーマットに変更はないが、RIのTPMによって生成された。
選択されたバージョン	必須	-	変更なし。
RI ID	必須	-	フォーマットに変更はないが、OMA DRM2.0 ROAPによってサポートされるRSA-PSS法を使用して、RI TPM EK資格証明、またはRI TPM AIK資格証明の1つの資格証明の、RIのTPMによって計算されたSHA-1ハッシュを使用する。
選択されたアルゴリズム	オプション	-	変更なし。
RIナンス	必須	-	フォーマットに変更はないが、RIのTPMが存在する場合、RI TPMによって生成されるべき。
信頼されるデバイス権限	オプション	-	RIによって認識されたデバイス信頼アンカのリスト。提案される変更は、信頼アンカのリストの一部として、デバイスのTCG資格証明をさらに含めることを備える。
サーバ情報	オプション	-	変更なし。
拡張子	オプション	-	OMA DRM2.0 ROAP RIハロー拡張子要素のすべてに加えて、RIのTPM能力を示す1つまたは複数のビットから成る新たなRTCI(RI TPM能力標識)要素。
署名	必須	必須	新たなパラメータ:デバイスが公開鍵をあらかじめ獲得しているRI AIK秘密鍵の1つによって署名された、署名パラメータまでの、署名パラメータを除くRIハローメッセージに対して、RSA-PSSアルゴリズムを使用して計算される。やはり、デバイスハローメッセージの成功または失敗にかかわらず、この署名を必須にする。

【０２８２】

（登録要求メッセージの変更、およびこの変更の導出）

【０２８３】

第１の変更は、デバイスＴＰＭを使用して、デバイスナンスを提供することである。この変更の利点は、ＴＰＭが、ナンスに使用するのに適したセキュリティで保護された、信

頼できる擬似乱数を提供することである。

【０２８４】

第２の変更は、デバイスＴＣＧ資格証明を証明書チェーンの中に含めることである。デバイスＴＣＧ資格証明を含めることは、既存のＯＭＡ　ＤＲＭ２．０デバイス資格証明の代わりであること、または既存のＯＭＡ　ＤＲＭ２．０デバイス資格証明に加えてであることが可能である。ＴＣＧ資格証明（ＥＫ資格証明、ＡＩＫ資格証明、プラットフォーム資格証明、または準拠資格証明）を含めることの利点は、デバイスの信頼性を高めることである。

【０２８５】

第３の変更は、ＲＩによって信頼されるＴＣＧ　ＣＡのリストを、信頼ＲＩアンカ要素の中に含めることである。ＲＩによって信頼されるＴＣＧ　ＣＡを含めることは、既存のＯＭＡ　ＤＲＭ２．０　ＲＩ信頼アンカ要素リストの代わりであること、または既存のＯＭＡ　ＤＲＭ２．０　ＲＩ信頼アンカ要素リストに加えてであることが可能である。ＲＩによって信頼されるＴＣＧ　ＣＡのリストを含めることの利点は、デバイスの信頼性を高めることである。

【０２８６】

第４の変更は、デバイスＴＰＭについての情報を、拡張子パラメータのデバイス詳細要素の中に含めることである。この情報を含めることの利点は、ＲＩに対するデバイスについての信頼性を高めることである。

【０２８７】

第５の変更は、変更されたデバイスハローメッセージに署名するのに使用されたデバイスＡＩＫを使用して署名に署名することである。この変更の利点は、デバイスＡＩＫの強固に保護された性質のため、デバイス、および登録要求メッセージの信頼性を高めることである。

【０２８８】

テーブル１６は、変更された登録要求メッセージに関するフォーマットを示す。

【０２８９】

【表１６】
表16 変更された登録要求メッセージフォーマット

パラメータ	登録要求	メモ(OMA DRM2.0 ROAP登録要求メッセージからの変更)
セッションID	必須	変更なし。
デバイスナンス	必須	フォーマットに変更はないが、デバイスTPMによって生成された。
要求時間	必須	変更なし。
証明書チェーン	オプション	フォーマットに変更はないが、TCG証明書だけをリストアップする、またはフォーマットが変更されて、OMA DRM証明書とTCG証明書をともにリストアップする。
信頼されるRI権限	オプション	フォーマットに変更はないが、RI信頼アンカとしてTCG CA権限に関する情報だけをリストアップする、またはフォーマットが変更されて、OMA DRM RI信頼アンカとTCG CA権限をともに、さらなるRI信頼アンカとしてリストアップする。
サーバ情報	オプション	変更なし。
拡張子	オプション	既存のすべてのOMA DRM2.0登録要求拡張子要素。しかし、デバイスが、TPMを有する場合、デバイスのTPMに関する情報(製造業者名、バージョンなどの)が、デバイス詳細要素の中に含められなければならない。
署名	必須	フォーマットに変更はないが、変更されたデバイスハローメッセージに署名するのに使用されたデバイスTPMのAIKを使用する。

【０２９０】
（登録応答メッセージの変更、およびこの変更の導出）
【０２９１】
第１の変更は、ＲＩ　ＴＰＭを使用して、セッションＩＤを表す擬似乱数を提供することである。この変更の利点は、ＴＰＭが、セキュリティで強固に保護されたハードウェアベースの擬似乱数発生器を提供することである。ＴＰＭを使用して、セッションＩＤとして使用される擬似乱数を生成することにより、プロトコルのセキュリティが強化される。
【０２９２】
第２の変更は、ＲＩ　ＴＣＧ　ＥＫ資格証明、またはＲＩのＴＰＭに属するＴＣＧ　ＡＩＫ資格証明を使用して、ＲＩ　ＩＤを導き出すことである。この変更の利点は、ＥＫ資格証明および／またはＡＩＫ資格証明が、デバイス内のＴＰＭによって強固に保護され、これらの資格証明のいずれかからＤＲＭデバイスＩＤを導き出すことにより、ＤＲＭデバイスＩＤ情報の完全性が強化されることである。
【０２９３】
第３の変更は、ＲＩ　ＴＰＭを使用して、ＲＩナンスを提供することである。この変更の利点は、ＲＩ　ＴＰＭが、ナンスとして使用するのに適したセキュリティで保護された、信頼できる擬似乱数を提供することである。
【０２９４】
第４の変更は、デバイスによって信頼されるＴＣＧ　ＣＡのリストを、信頼されるデバイスアンカ要素の中に含めることである。デバイスによって信頼されるＴＣＧ　ＣＡを含

めることは、既存のＯＭＡ　ＤＲＭ２．０信頼デバイスアンカ要素リストの代わりであること、または既存のＯＭＡ　ＤＲＭ２．０信頼デバイスアンカ要素リストに加えてであることが可能である。デバイスによって信頼されるＴＣＧ　ＣＡのリストを含めることの利点は、ＲＩの信頼性を高めることである。

【０２９５】

第５の変更は、変更されたＲＩハローメッセージに署名するのに使用されたＲＩ　ＡＩＫを使用して署名に署名することである。この変更の利点は、ＲＩ　ＡＩＫの強固に保護された性質のため、ＲＩ、および登録応答メッセージの信頼性を高めることである。

【０２９６】

テーブル１７は、変更された登録応答メッセージに関するフォーマットを示す。

【０２９７】

【表１７】

表17 変更された登録応答メッセージフォーマット

パラメータ	登録応答		メモ(OMA DRM2.0 ROAP登録応答メッセージからの変更)
	ステータス=「成功」	ステータスは、「成功」でない	
ステータス	必須	必須	変更なし。
セッションID	必須	-	フォーマットに変更はないが、RIのTPMによって生成された擬似乱数を使用する。
選択されたバージョン	必須	-	変更なし。
RI ID	必須	-	フォーマットに変更はないが、RI TPM EK資格証明、またはAIK資格証明の1つの資格証明の、RIのTPMによって計算されたSHA-1ハッシュを使用する。
選択されたアルゴリズム	必須	-	変更なし。
RIナンス	必須	-	フォーマットに変更はないが、RI TPMによって生成されたナンスを使用する。
信頼されるデバイス権限	オプション	-	フォーマットに変更はないが、デバイスが信頼アンカとして信頼するTCG CAに関する情報だけをリストアップする、またはフォーマットが変更されて、OMA DRMデバイス信頼アンカと、デバイスによって信頼されるTCG CA権限をともに、さらなるデバイス信頼アンカとしてリストアップする。
サーバ情報	オプション	-	変更なし。
拡張子	オプション	-	変更なし。
署名	必須	必須	フォーマットに変更はないが、変更されたRIハローメッセージに署名する際に使用されたのと同一のRI TPM AIKを使用して署名する。この署名は、登録要求メッセージの成功または失敗にかかわらず、必須である。

【０２９８】

（ＲＯ要求メッセージの変更、およびこの変更の導出）

【０２９９】

第１の変更は、ＴＰＭを使用して、デバイスＩＤとして使用すべき、選択されたＴＣＧ資格証明（ＥＫ資格証明、ＡＩＫ資格証明、プラットフォーム資格証明、または準拠資格

証明）のＳＨＡ－１ハッシュを作成する。この変更の利点は、資格証明が、ＴＰＭによって強固に保護され、このため、これらの資格証明のいずれかからデバイスＩＤを導き出すことにより、デバイスＩＤ情報の完全性が強化されることである。

【０３００】

第２の変更は、デバイスＴＰＭを使用して、デバイスナンスを生成することである。この変更の利点は、ＴＰＭによって生成されるナンスが、ＴＰＭの保護された擬似乱数発生能力のために、セキュリティで保護されていることである。

【０３０１】

第３の変更は、ＴＣＧ資格証明を証明書チェーンの中に含めることである。ＴＣＧ資格証明を含めることは、既存のＯＭＡ　ＤＲＭ２．０デバイス資格証明の代わりであること、または既存のＯＭＡ　ＤＲＭ２．０デバイス資格証明に加えてであることが可能である。ＴＣＧ資格証明を含めることの利点は、デバイスの信頼性を高めることである。

【０３０２】

第４の変更は、拡張子パラメータの中のデバイスＡＩＫを使用して、オプションのＤＣＦハッシュに署名することである。この変更の利点は、デバイスＡＩＫが強固に保護されており、ＤＣＦ署名が、より強固なセキュリティで保護されるようにすることである。

【０３０３】

第５の変更は、正常に応答があった最新の登録要求メッセージに署名するのに使用されたデバイスＡＩＫを使用して、ＲＯ要求メッセージに署名することである。この変更の利点は、ＲＩ　ＡＩＫの強固に保護された性質のため、ＲＩ、およびＲＯ要求メッセージの信頼性を高めることである。

【０３０４】

テーブル１８は、変更されたＲＯ要求メッセージのフォーマットを示す。

【０３０５】

【表１８】

表18 変更されたRO要求メッセージフォーマット

パラメータ	ROAP-RO要求 必須/ オプション	メモ
デバイスID	M	フォーマットに変更はないが、TPMを使用して、デバイスIDとして使用すべきTCG資格証明のSHA-1ハッシュを計算する。
ドメインID	O	変更なし。
RI ID	M	変更なし。
デバイスナンス	M	フォーマットに変更はないが、デバイスTPMによって生成されたナンスを使用する。
要求時間	M	変更なし。
RO情報	M	変更なし。
証明書チェーン	O	デバイスTCG証明書チェーンを使用する、またはOMA DRM2.0証明書チェーンとデバイスTCG証明書チェーンの両方を使用する。
拡張子	O	フォーマットに変更はないが、DCF署名が含められる場合、RI AIKを使用してDCFに署名する。
署名	M	フォーマットに変更はないが、TPMを使用して、正常に応答があった最新の登録要求メッセージに署名するのに使用されたデバイスAIKを使用する署名を計算する。

【０３０６】

（ＲＯ応答メッセージの変更、およびこの変更の導出）

【０３０７】

１つの変更は、ＲＩのＴＰＭを使用して、成功した最新の登録応答メッセージに署名する際に使用されたのと同一のＲＩ　ＴＰＭ　ＡＩＫを使用して、ＲＯ応答メッセージに署名することである。この変更の利点は、ＲＩ　ＡＩＫの強固に保護された性質のため、ＲＩ、およびＲＯ応答メッセージの信頼性を高めることである。

【０３０８】

テーブル１９は、変更されたＲＯ要求メッセージのフォーマットを示す。

【０３０９】

【表１９】
表19 変更されたRO応答メッセージフォーマット

パラメータ	2パス成功	2パス成功ではない	メモ
ステータス	M	M	変更なし。
デバイスID	M	-	変更なし。
RI ID	M	-	変更なし。
デバイスナンス	M	-	変更なし。
保護されたRO	M	-	変更なし。
証明書チェーン	O	-	変更なし。
OCSP応答	O	-	変更なし。
拡張子	O	-	変更なし。
署名	M	M	フォーマットに変更はないが、RI TPMを使用して、成功した最新の登録応答メッセージの中で使用されたRI AIKで署名する。この署名は、RO要求メッセージの成功または失敗にかかわらず、必須である。

【０３１０】
本発明の特徴および要素は、特定の組合せで、好ましい実施形態において説明されるものの、各フィーチャ、または各要素は、単独で（好ましい実施形態のその他のフィーチャ、およびその他の要素なしに）、あるいは本発明の他のフィーチャ、および他の要素を伴って、または伴わずに様々な組合せで使用されることが可能である。
【０３１１】
（実施形態）
【０３１２】
１．ＲＥ（要求するエンティティ）と、ＴＥ（ターゲットエンティティ）との間でプラットフォーム完全性検査を実行するための方法であって、ＴＥのＴＣＧ（Ｔｒｕｓｔｅｄ Ｃｏｍｐｕｔｉｎｇ Ｇｒｏｕｐ）資格証明を報告するようＴＥに要求する要求を、ＲＥからＴＥに送信するステップと、ＴＥからＲＥにＴＥのＴＣＧ資格証明を送信するステップと、ＴＥのＴＣＧ資格証明を、検証のために、ＲＥからＯＣＳＰ（オンライン証明書ステータスプロトコル）レスポンダに転送するステップと、ＴＥのＴＣＧ資格証明の検証ステータスを、ＯＣＳＰレスポンダからＲＥに報告するステップと、ＴＥ自らのプラットフォーム完全性ステータスを報告するようＴＥに要求する要求を、ＲＥからＴＥに送信するステップと、ＴＥのプラットフォーム完全性ステータスを検査するステップと、ＴＥからＲＥにプラットフォーム完全性ステータス標識を送信するステップとを含む方法。
【０３１３】
２．ＲＥは、ＲＩ（権利発行者）であり、ＴＥは、デバイスである実施形態１による方法。
【０３１４】
３．デバイスが、方法を開始するトリガをＲＩに送信することによって、デバイスが、ＲＩを相手にＲＯＡＰ（権利オブジェクト獲得プロトコル）登録プロトコルを開始するのに先立って実行される実施形態２による方法。
【０３１５】
４．デバイスが、ＲＩに最も新しく登録してから経過した時間に基づいて、定期的に実

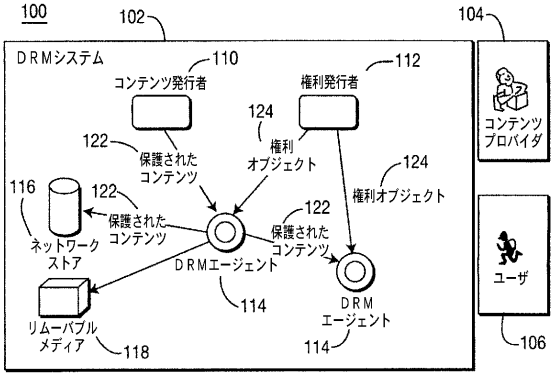
行される実施形態２または３による方法。
【０３１６】
５．デバイスが、デバイスのプラットフォーム完全性ステータスをＲＩに最も新しく検証してから経過した時間に基づいて、定期的に実行される実施形態２から４のいずれかによる方法。
【０３１７】
６．ＲＥは、デバイスであり、ＴＥは、ＲＩ（権利発行者）である実施形態１による方法。
【０３１８】
７．ＲＩが、ＲＩのプラットフォーム完全性ステータスをデバイスに最も新しく検証してから経過した時間に基づいて、定期的に実行される実施形態６による方法。
【０３１９】
８．ＲＥは、ＣＩ（コンテンツ発行者）であり、ＴＥは、デバイスである実施形態１による方法。
【０３２０】
９．デバイスが、デバイスのプラットフォーム完全性ステータスをＣＩに最も新しく検証してから経過した時間に基づいて、定期的に実行される実施形態８による方法。
【０３２１】
１０．デバイスが、ＣＩからコンテンツを購入すると、実行される実施形態８または９による方法。
【０３２２】
１１．ＲＥは、デバイスであり、ＴＥは、ＣＩ（コンテンツ発行者）である実施形態１による方法。
【０３２３】
１２．ＣＩが、ＣＩのプラットフォーム完全性ステータスをデバイスに最も新しく検証してから経過した時間に基づいて、定期的に実行される実施形態１１による方法。
【０３２４】
１３．デバイスが、ＣＩからコンテンツを購入すると、実行される実施形態１１または１２による方法。
【０３２５】
１４．ＲＯＡＰ（権利オブジェクト獲得プロトコル）プロセスの一環として実行される実施形態１による方法。
【０３２６】
１５．ＲＯＡＰプロセスに先立って実行される実施形態１４による方法。
【０３２７】
１６．ＲＯＡＰプロセスは、ＲＯＡＰプロセスの一環として方法を組み込むように変更される実施形態１４または１５による方法。
【０３２８】
１７．ＲＥ（要求するエンティティ）と、ＴＥ（ターゲットエンティティ）との間でＤＲＭ（デジタル権利管理）ソフトウェア完全性検査を実行するための方法であって、ＴＥがＤＲＭソフトウェア完全性検査を実行することを要求する要求を、ＲＥからＴＥに送信するステップと、ＴＥによってＤＲＭソフトウェア完全性を検査するステップと、ＴＥからＲＥにＤＲＭソフトウェア完全性ステータス標識を送信するステップとを含む方法。
【０３２９】
１８．ＲＥは、ＲＩ（権利発行者）であり、ＴＥは、デバイスである実施形態１７による方法。
【０３３０】
１９．デバイスは、デバイスが、ＲＯＡＰ（権利オブジェクト獲得プロトコル）プロセスを開始するのに先立って、方法を開始するトリガをＲＩに送信する実施形態１８による方法。

【０３３１】
２０．ＲＯＡＰプロセスは、２パス登録、２パスドメイン参加、および２パスドメイン退去から成るグループから選択される実施形態１９による方法。
【０３３２】
２１．デバイスが、ＲＩを相手にＲＯＡＰ（権利オブジェクト獲得プロトコル）プロセスを完了した後、定期的に実行される実施形態１９または２０による方法。
【０３３３】
２２．ＲＯＡＰプロセスは、２パス登録、２パスドメイン参加、および２パスドメイン退去から成るグループから選択される実施形態１９から２１のいずれかによる方法。
【０３３４】
２３．デバイスが、デバイスのＤＲＭソフトウェア完全性ステータスをＲＩに検証し、報告した後、定期的に実行される実施形態１８から２２のいずれかによる方法。
【０３３５】
２４．デバイスが、デバイスのＤＲＭソフトウェアを更新した後、実行される実施形態１８から２３のいずれかによる方法。
【０３３６】
２５．ＲＩは、デバイス上のメディアプレーヤに対してＤＲＭソフトウェア完全性検査を実行するよう、デバイスに要求する実施形態１８から２４のいずれかによる方法。
【０３３７】
２６．ＲＥは、デバイスであり、ＴＥは、ＲＩ（権利発行者）である実施形態１７による方法。
【０３３８】
２７．デバイスによって開始されると、実行される実施形態２６による方法。
【０３３９】
２８．スタンドアロンのプロセスである実施形態２６または２７による方法。
【０３４０】
２９．変更された権利オブジェクト獲得プロトコルプロセスの一環である実施形態２６から２８のいずれかによる方法。
【０３４１】
３０．ＲＩが、ＲＩのＤＲＭソフトウェア完全性ステータスをデバイスに検証し、報告した後、定期的に実行される実施形態２６から２９のいずれかによる方法。
【０３４２】
３１．ＲＩが、ＲＩのＤＲＭソフトウェアを更新した後、実行される実施形態２６から３０のいずれかによる方法。
【０３４３】
３２．デバイスが、ＲＩに権利オブジェクト要求を送信するのに先立って実行される実施形態２６から３１のいずれかによる方法。
【０３４４】
３３．ストリーミングコンテンツを求めるデバイスからＲＩへの要求中に、定期的に実行される実施形態２６から３２のいずれかによる方法。
【０３４５】
３４．ＲＥは、ＣＩ（コンテンツ発行者）であり、ＴＥは、デバイスである実施形態１７による方法。
【０３４６】
３５．デバイスは、デバイスが、ＲＯＡＰ（権利オブジェクト獲得プロトコル）プロセスを開始するのに先立って、方法を開始するトリガをＣＩに送信する実施形態３４による方法。
【０３４７】
３６．デバイスが、ＣＩを相手にＲＯＡＰ（権利オブジェクト獲得プロトコル）プロセスを完了した後、定期的に実行される実施形態３４または３５による方法。

【０３４８】
３７．デバイスが、デバイスのＤＲＭソフトウェア完全性ステータスをＣＩに検証し、報告した後、定期的に実行される実施形態３４から３６のいずれかによる方法。
【０３４９】
３８．デバイスが、デバイスのＤＲＭソフトウェアを更新した後、実行される実施形態３４から３７のいずれかによる方法。
【０３５０】
３９．ＣＩは、デバイス上のメディアプレーヤに対してＤＲＭソフトウェア完全性検査を実行するよう、デバイスに要求する実施形態３４から３８のいずれかによる方法。
【０３５１】
４０．ＲＥは、デバイスであり、ＴＥは、ＣＩ（コンテンツ発行者）である実施形態１７による方法。
【０３５２】
４１．デバイスによって開始されると、実行される実施形態４０による方法。
【０３５３】
４２．スタンドアロンのプロセスである実施形態４０または４１による方法。
【０３５４】
４３．変更された権利オブジェクト獲得プロトコルプロセスの一環である実施形態４０から４２のいずれかによる方法。
【０３５５】
４４．ＣＩが、ＣＩのＤＲＭソフトウェア完全性ステータスをデバイスに検証し、報告した後、定期的に実行される実施形態４０から４３のいずれかによる方法。
【０３５６】
４５．ＣＩが、ＣＩのＤＲＭソフトウェアを更新した後、実行される実施形態４０から４４のいずれかによる方法。
【０３５７】
４６．デバイスが、権利オブジェクト要求をＣＩに送信するのに先立って実行される実施形態４０から４５のいずれかによる方法。
【０３５８】
４７．ストリーミングコンテンツを求めるデバイスからＣＩへの要求中に、定期的に実行される実施形態４０から４６のいずれかによる方法。
【０３５９】
４８．２つのエンティティ間で交換されるＲＯＡＰ（権利オブジェクト獲得プロトコル）メッセージの完全性を強化するための方法であって、信頼されるコンピューティング技術を使用して各エンティティにおいて、ＲＯＡＰメッセージの中で使用されるべき情報を安全に格納するステップと、ＲＯＡＰメッセージに関連して使用されるのに先立って、ＲＯＡＰメッセージの中で使用されるべき情報を事前検証するステップとを含む方法。
【０３６０】
４９．格納するステップは、情報に密封署名すること、および情報を結び付けることを含む実施形態４８による方法。
【０３６１】
５０．密封署名するステップは、対称暗号化鍵を使用して情報を対称的に暗号化すること、およびこの対称暗号化鍵、およびオブジェクトの現在の完全性ステータスを示す値のセットに非対称的に署名することを含む実施形態４９による方法。
【０３６２】
５１．署名するステップは、エンティティが動作するプラットフォームの完全性ステータスを使用することを含む実施形態５０による方法。
【０３６３】
５２．署名するステップは、エンティティのソフトウェア構成要素の完全性ステータスを使用することを含む実施形態５０または５１による方法。

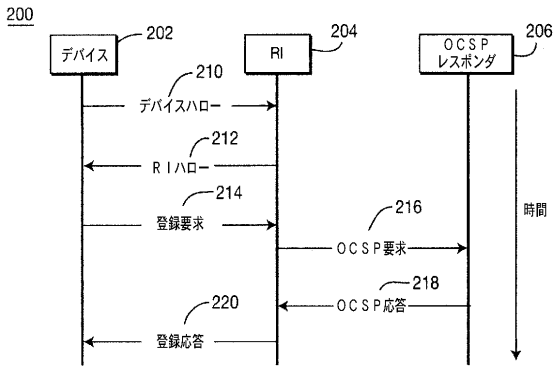
【０３６４】
５３．結び付けるステップは、秘密解読鍵がエンティティ内の保護されたモジュールの中に格納された鍵を使用して、情報を非対称的に暗号化することを含む実施形態４９から５２のいずれかによる方法。
【０３６５】
５４．保護されたモジュールは、ＴＰＭ（信頼される処理モジュール）である実施形態５３による方法。
【０３６６】
５５．ＴＰＭは、ＲＯＡＰメッセージの中で使用すべきパラメータを導き出すのに使用される実施形態５４による方法。
【０３６７】
５６．情報は、デバイスＩＤ、権利発行者ＩＤ、証明書、証明書チェーン、デジタル権利管理関連の時間値、権利オブジェクト、アルゴリズム、およびナンスから成るグループから選択される実施形態４８から５５のいずれかによる方法。
【０３６８】
５７．すべてのＲＯＡＰメッセージに適用される実施形態４８から５６のいずれかによる方法。
【０３６９】
５８．ＲＯＡＰメッセージとは別個に適用される実施形態４８から５６のいずれかによる方法。
【０３７０】
５９．ＲＯＡＰメッセージの生成および伝送に組み込まれる実施形態４８から５６のいずれかによる方法。
【０３７１】
６０．送信するエンティティの信頼されるコンピューティング能力を示すフィールドを、既存のＲＯＡＰメッセージに追加するステップをさらに含む実施形態４８から５６のいずれかによる方法。
【０３７２】
６１．実施形態１から６０のいずれかによる方法を実行するように構成されたシステム。
【０３７３】
６２．実施形態１から６０のいずれかによる方法を実行するように構成された集積回路。

【図１】



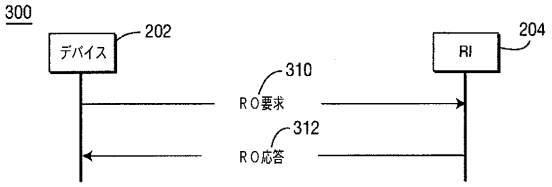
従来技術

【図２】



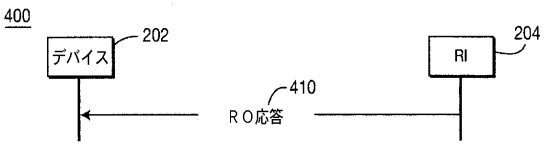
従来技術

【図３】



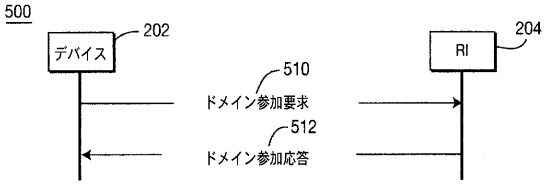
従来技術

【図４】



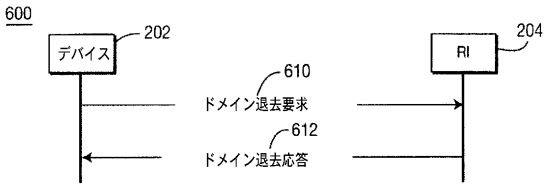
従来技術

【図５】



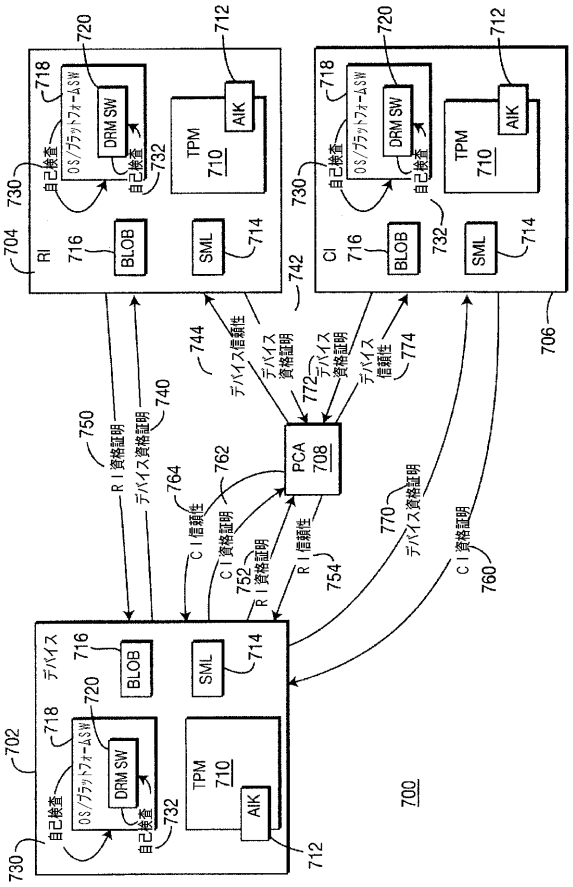
従来技術

【図６】

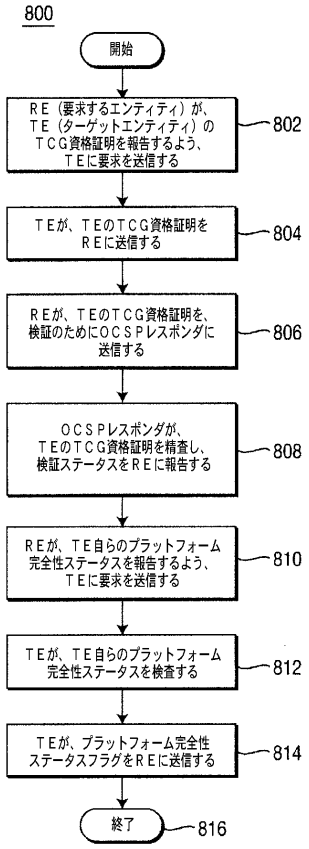


従来技術

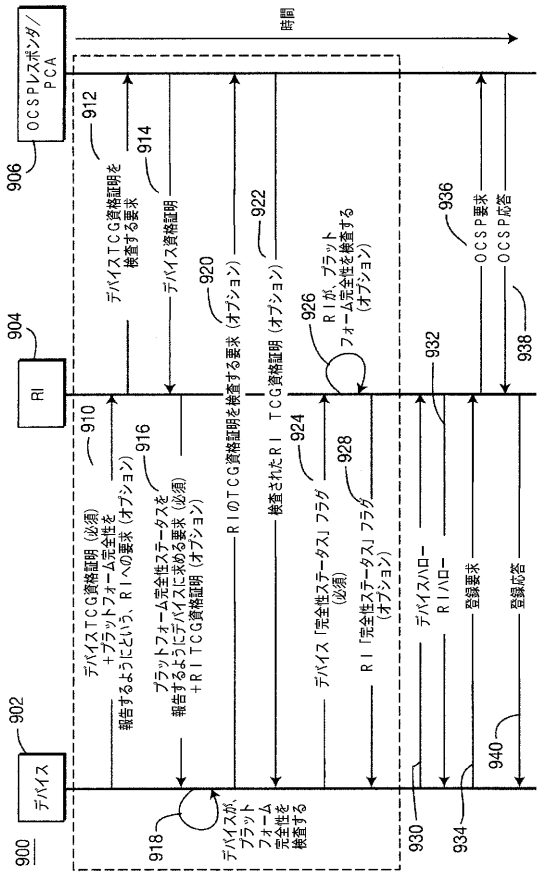
【図７】



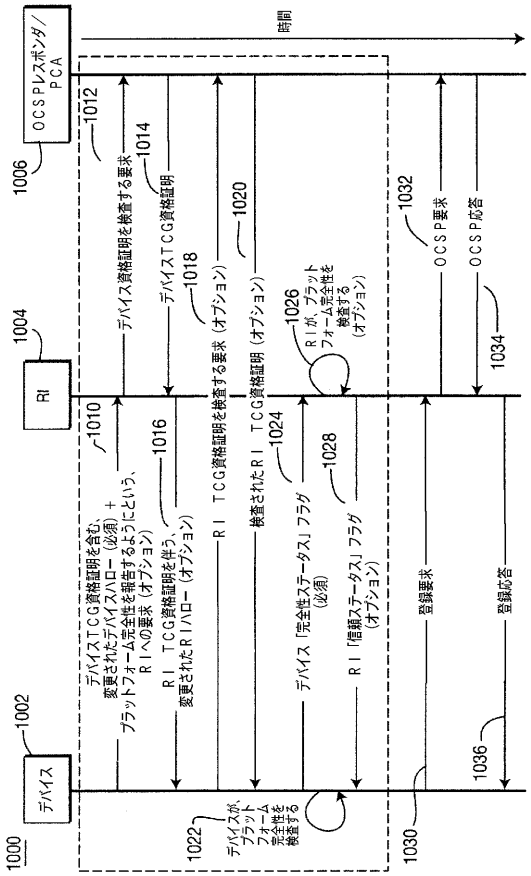
【図８】


800
開始
RE（要求するエンティティ）が、TE（ターゲットエンティティ）のTCG資格証明を報告するよう、TEに要求を送信する
802
TEが、TEのTCG資格証明をREに送信する
804
REが、TEのTCG資格証明を、検証のためにOCSPレスポンダに送信する
806
OCSPレスポンダが、TEのTCG資格証明を精査し、検証ステータスをREに報告する
808
REが、TE自らのプラットフォーム完全性ステータスを報告するよう、TEに要求を送信する
810
TEが、TE自らのプラットフォーム完全性ステータスを検査する
812
TEが、プラットフォーム完全性ステータスフラグをREに送信する
814
終了
816

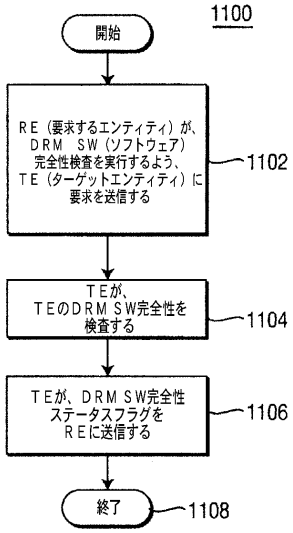
【図９】


OCSPレスポンダ/PCA
906
RI
904
デバイス
902
900
時間
912
914
920
922
926
936
932
938
910
916
924
928
940
930
934
918
デバイスTCG資格証明を検査する要求
デバイス資格証明
RIのTCG資格証明を検査する要求（オプション）
RI TCG資格証明（オプション）
RIが、プラットフォーム完全性を検査する（オプション）
OCSP要求
OCSP応答
デバイスTCG資格証明（必須）＋プラットフォーム完全性を報告するようにという、RIへの要求（オプション）
プラットフォーム完全性ステータスを報告するようにデバイスに求める要求（必須）＋RI TCG資格証明（オプション）
検査されたRI TCG資格証明
デバイス「完全性ステータス」フラグ（必須）
RI「完全性ステータス」フラグ（オプション）
デバイスハロー
RIハロー
登録要求
登録応答
デバイスが、プラットフォーム完全性を検査する

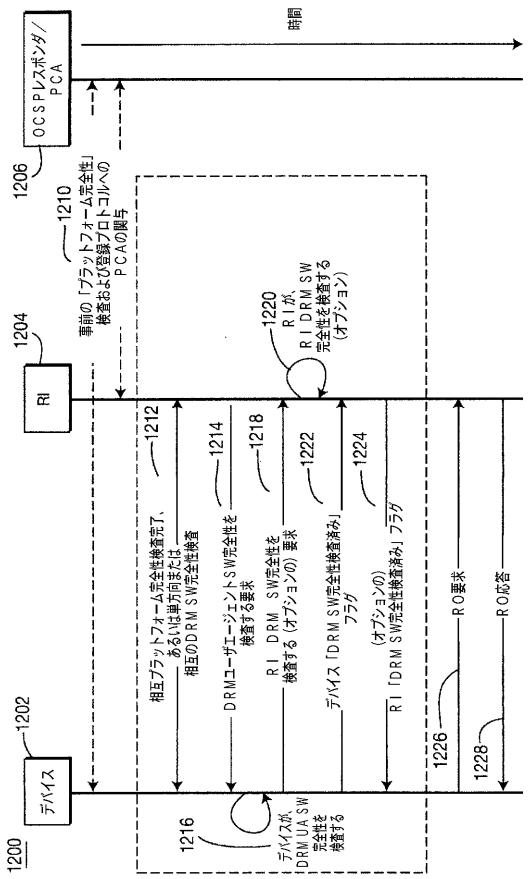
【図１０】


OCSPレスポンダ/PCA
1006
RI
1004
デバイス
1002
1000
時間
1012
1014
1018
1020
1032
1034
1010
1016
1024
1028
1036
1022
1030
デバイス資格証明を検査する要求
デバイスTCG資格証明
RI TCG資格証明を検査する要求（オプション）
RIが、プラットフォーム完全性を検査する（オプション）
OCSP要求
OCSP応答
デバイスTCG資格証明を含む、変更されたデバイスハロー（必須）＋プラットフォーム完全性を報告するようにという、RIへの要求（オプション）
RI TCG資格証明を伴う、変更されたRIハロー（オプション）
検査されたRI TCG資格証明
デバイス「完全性ステータス」フラグ（必須）
RI「信頼ステータス」フラグ（オプション）
登録要求
登録応答
デバイスが、プラットフォーム完全性を検査する

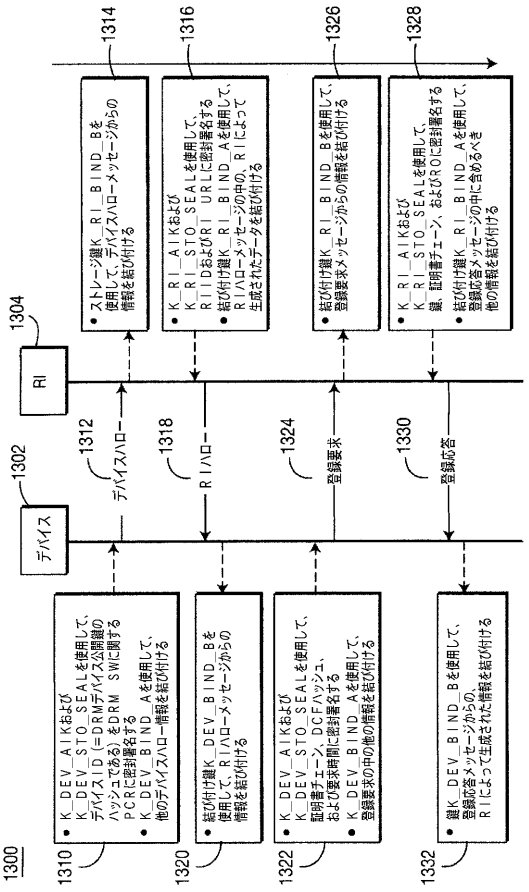
【図１１】


1100
開始
RE（要求するエンティティ）が、DRM SW（ソフトウェア）完全性検査を実行するよう、TE（ターゲットエンティティ）に要求を送信する
1102
TEが、TEのDRM SW完全性を検査する
1104
TEが、DRM SW完全性ステータスフラグをREに送信する
1106
終了
1108

【図１２】



【図１３】



【手続補正書】
【提出日】平成24年8月29日(2012.8.29)
【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】
要求するエンティティ（ＲＥ）装置と、ターゲットエンティティ（ＴＥ）装置との間でプラットフォーム完全性検査を実行するための方法であって、
前記ＲＥ装置によって、
（ａ）前記ＴＥ装置に、そのＴＥ装置の信頼される資格証明と、そのＴＥ装置自身のプラットフォーム完全性ステータスとを報告するよう要求するステップと、
（ｂ）前記ＴＥ装置の信頼される資格証明と、そのＴＥ装置のプラットフォーム完全性ステータスについての情報とを受信するステップと、
（ｃ）前記ＴＥ装置の信頼される資格証明と、そのＴＥ装置のプラットフォーム完全性ステータスについての情報とを、完全性検証のために、レスポンダに転送するステップと、
（ｄ）前記レスポンダから前記ＴＥ装置の信頼される資格証明の完全性検証と、前記ＴＥ装置のプラットフォーム完全性ステータスとの指示を受信するステップと、
（ｅ）前記レスポンダからの、前記ＴＥ装置の信頼される資格証明の完全性検証と前記ＴＥ装置のプラットフォーム完全性ステータスとの指示に基づいて、前記ＴＥ装置において十分な信頼を与えて、前記ＴＥ装置を進めるか、または、デバイスが保護されたコンテンツを獲得することを可能にする別のプロトコルにおいて前記ＴＥ装置を進めるのかを決

定するステップと
が実行されることを特徴とする方法。
【請求項２】
前記ＲＥ装置は、権利発行者（ＲＩ）であり、前記ＴＥ装置は、前記デバイスであることを特徴とする請求項１に記載の方法。
【請求項３】
前記デバイスが、前記方法を開始するトリガを前記ＲＩ装置に送信することによって、前記方法が、前記デバイスが前記ＲＩ装置を相手に前記登録プロトコルを開始するのに先立って実行されることを特徴とする請求項２に記載の方法。
【請求項４】
前記デバイスが前記ＲＩ装置に最も新しく登録してから経過した時間に基づいて、前記方法が定期的に実行されることを特徴とする請求項２に記載の方法。
【請求項５】
前記デバイスが該デバイスのプラットフォーム完全性ステータスを前記ＲＩ装置に最も新しく検証してから経過した時間に基づいて、前記方法が定期的に実行されることを特徴とする請求項２に記載の方法。
【請求項６】
前記ＲＥ装置は、コンテンツ発行者（ＣＩ）であり、前記ＴＥ装置は、前記デバイスであることを特徴とする請求項１に記載の方法。
【請求項７】
前記デバイスが該デバイスのプラットフォーム完全性ステータスを前記ＣＩに最も新しく検証してから経過した時間に基づいて、前記方法が定期的に実行されることを特徴とする請求項６に記載の方法。
【請求項８】
前記デバイスが、前記ＣＩからコンテンツを購入すると、前記方法が実行されることを特徴とする請求項６に記載の方法。
【請求項９】
前記ＴＥ装置を進める、前記デバイスが保護されたコンテンツを獲得することを可能にする別のプロトコルは、権利オブジェクト獲得プロトコル（ＲＯＡＰ）を含むことを特徴とする請求項１に記載の方法。
【請求項１０】
要求するエンティティ（ＲＥ）装置と、ターゲットエンティティ（ＴＥ）装置との間でデジタル権利管理（ＤＲＭ）ソフトウェア完全性検査を実行するための方法であって、
前記ＴＥ装置によって、
前記ＴＥ装置がＤＲＭソフトウェア完全性検査を実行するための要求を、前記ＲＥ装置から受信するステップと、
前記ＴＥ装置において前記ＤＲＭソフトウェア完全性検査を実行するステップと、
前記ＲＥ装置にＤＲＭソフトウェア完全性ステータス標識を送信するステップであって、前記ＤＲＭソフトウェア完全性ステータス標識は、前記ＴＥ装置の完全性ステータスに十分な信頼を与えて、前記ＴＥ装置を進めるか、または、デバイスが保護されるコンテンツを獲得することを可能にする別のプロトコルにおいて前記ＴＥ装置を進めるのかを示すように構成される、ステップと
が実行されることを特徴とする方法。
【請求項１１】
前記ＲＥ装置は、権利発行者（ＲＩ）であり、前記ＴＥ装置は、前記デバイスであることを特徴とする請求項１０に記載の方法。
【請求項１２】
前記デバイスは、前記デバイスが権利オブジェクト獲得プロトコル（ＲＯＡＰ）プロセスを開始するのに先立って、前記方法を開始するトリガを前記ＲＩに送信することを特徴とする請求項１１に記載の方法。

【請求項１３】
前記ＲＯＡＰプロセスは、２パス登録、２パスドメイン参加、または２パスドメイン退去のうちの少なくとも１つから選択されることを特徴とする請求項１２に記載の方法。
【請求項１４】
前記デバイスが前記ＲＩを相手に権利オブジェクト獲得プロトコル（ＲＯＡＰ）プロセスを完了した後、前記方法が定期的に実行されることを特徴とする請求項１１に記載の方法。
【請求項１５】
前記ＲＯＡＰプロセスは、２パス登録、２パスドメイン参加、または２パスドメイン退去のうちの少なくとも１つから選択されることを特徴とする請求項１４に記載の方法。
【請求項１６】
前記デバイスが該デバイスのＤＲＭソフトウェア完全性ステータスを前記ＲＩに検証し、報告した後、前記方法が定期的に実行されることを特徴とする請求項１１に記載の方法。
【請求項１７】
前記デバイスが該デバイスのＤＲＭソフトウェアを更新した後、前記方法が実行されることを特徴とする請求項１１に記載の方法。
【請求項１８】
前記ＲＩは、前記デバイス上のメディアプレーヤに対して前記ＤＲＭソフトウェア完全性検査を実行するよう、前記デバイスに要求することを特徴とする請求項１１に記載の方法。
【請求項１９】
前記ＲＥ装置は、コンテンツ発行者（ＣＩ）であり、前記ＴＥ装置は、デバイスであることを特徴とする請求項１０に記載の方法。
【請求項２０】
前記デバイスは、前記デバイスが権利オブジェクト獲得プロトコル（ＲＯＡＰ）プロセスを開始するのに先立って、前記方法を開始するトリガを前記ＣＩに送信することを特徴とする請求項１９に記載の方法。
【請求項２１】
前記デバイスが、前記ＣＩを相手に権利オブジェクト獲得プロトコル（ＲＯＡＰ）プロセスを完了した後、前記方法が定期的に実行されることを特徴とする請求項１９に記載の方法。
【請求項２２】
前記デバイスが該デバイスのＤＲＭソフトウェア完全性ステータスを前記ＣＩに検証し、報告した後、前記方法が定期的に実行されることを特徴とする請求項１９に記載の方法。
【請求項２３】
前記デバイスが該デバイスのＤＲＭソフトウェアを更新した後、前記方法が実行されることを特徴とする請求項１９に記載の方法。
【請求項２４】
前記ＣＩは、前記デバイス上のメディアプレーヤに対してＤＲＭソフトウェア完全性検査を実行するよう、前記デバイスに要求することを特徴とする請求項１９に記載の方法。
【請求項２５】
前記ＴＥ装置を進める、前記デバイスが保護されたコンテンツを獲得することを可能にする別のプロトコルは、権利オブジェクト獲得プロトコル（ＲＯＡＰ）を含むことを特徴とする請求項１０に記載の方法。
【請求項２６】
（ａ）から（ｄ）は、前記ＣＩからのトリガに基づく最も少ない第２の時間において実行されることを特徴とする請求項６に記載の方法。
【請求項２７】

前記ＲＥ装置にＤＲＭソフトウェア完全性ステータス標識を送信するステップは、前記デバイスから権利発行者（ＲＩ）に権利オブジェクト要求メッセージが送信されるのに先立って実行されることを特徴とする請求項１０に記載の方法。

フロントページの続き

(72)発明者　アミット　エックス．シンガル
アメリカ合衆国　１９４０３　ペンシルベニア州　キング　オブ　プロシア　ウエスト　デカルプ　パイク　２５１
(72)発明者　ヨゲンドラ　シー．シャー
アメリカ合衆国　１９３４１　ペンシルベニア州　エクストン　リージェンシー　コート　１０

Ｆターム(参考) 5J104 AA09 LA03 NA38