(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2020-25278
(P2020-25278A)
(43)公開日　令和2年2月13日(2020.2.13)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 9/32	(2006.01)	H04L 9/00	675D	
G06F 21/44	(2013.01)	G06F 21/44		
G06F 21/64	(2013.01)	G06F 21/64		

審査請求 有　請求項の数 16　ＯＬ　外国語出願　（全 65 頁）

(21)出願番号　特願2019-175521 (P2019-175521)
(22)出願日　令和1年9月26日 (2019.9.26)
(62)分割の表示　特願2017-568211 (P2017-568211)の分割
原出願日　平成28年6月30日 (2016.6.30)
(31)優先権主張番号　62/188,141
(32)優先日　平成27年7月2日 (2015.7.2)
(33)優先権主張国・地域又は機関　米国 (US)
(31)優先権主張番号　62/248,808
(32)優先日　平成27年10月30日 (2015.10.30)
(33)優先権主張国・地域又は機関　米国 (US)

(71)出願人　515222713
コンヴィーダ　ワイヤレス，　エルエルシー
アメリカ合衆国　デラウェア　１９８０９－３７２７，　ウィルミントン，　ベルビュー　パークウェイ　２００，　スイート　３００
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　チョイ，　ビノッド　クマー
アメリカ合衆国　ペンシルベニア　１９４０３，　ノリスタウン，　ミニットメン　レーン　１２０１

最終頁に続く

(54)【発明の名称】サービス層におけるコンテンツセキュリティ

(57)【要約】　（修正有）
【課題】エンティティ間の通信では、ＴＬＳによってセキュアにされるが、エンティティにおいて保護されないこともあることから、保護できる装置を提供する。
【解決手段】プロセッサと、メモリと、通信回路とを備えている装置であって、装置は、その通信回路を介してネットワークに接続される。装置は、装置のメモリ内に記憶されたコンピュータ実行可能命令をさらに備える。命令は、装置のプロセッサによって実行されると、コンテンツの保護を提供する１つ以上の証明書に対する要求を送信する。要求は、コンテンツに関連付けられた１つ以上のセキュリティパラメータに基づくことと、１つ以上の証明書を取得することと、１つ以上の証明書を使用して、コンテンツをセキュアにすることと、を含む。
【選択図】なし

【特許請求の範囲】
【請求項１】
プロセッサと、メモリと、通信回路とを備えている装置であって、前記装置は、その通信回路を介してネットワークに接続され、前記装置は、前記装置の前記メモリ内に記憶されたコンピュータ実行可能命令をさらに備え、前記命令は、前記装置の前記プロセッサによって実行されると、
第１のアプリケーションからリソースを作成するための第１の要求を受信することであって、前記リソースは、前記第１のアプリケーションに関連付けられたセキュアにされたコンテンツをホストする、ことと、
前記第１のアプリケーションが前記装置において前記リソースを作成するために承認されているかどうかを決定することと、
前記第１のアプリケーションが承認されている場合、前記セキュアにされたコンテンツをホストすることと
を含む動作を前記装置に行わせる、装置。
【請求項２】
前記第１のアプリケーションは、前記装置とは別個の共通サービスエンティティによって、前記リソースを作成するために承認されている、請求項１に記載の装置。
【請求項３】
前記要求は、前記共通サービスエンティティによって生成された証明書識別を含む、請求項２に記載の装置。
【請求項４】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
第２のアプリケーションから前記セキュアにされたコンテンツにアクセスするための第２の要求を受信することと、
前記第２のアプリケーションが前記セキュアにされたコンテンツにアクセスするために承認されているかどうかを決定することと、
前記第２のアプリケーションが前記セキュアにされたコンテンツにアクセスするために承認されている場合、前記セキュアにされたコンテンツを前記第２のアプリケーションに送信することと
を含むさらなる動作を前記装置に行わせる、請求項１に記載の装置。
【請求項５】
前記セキュアにされたコンテンツは、前記共通サービスエンティティが前記セキュアにされたコンテンツに関連付けられた１つ以上の証明書を前記第２のアプリケーションに送信した場合、解読されることができる、請求項４に記載の装置。
【請求項６】
前記第２のアプリケーションは、前記第１のアプリケーションのアクセス制御ポリシによって前記セキュアにされたコンテンツにアクセスするために承認されている、請求項４に記載の装置。
【請求項７】
プロセッサと、メモリと、通信回路とを備えている装置であって、前記装置は、その通信回路を介してネットワークに接続され、前記装置は、前記装置の前記メモリ内に記憶されたコンピュータ実行可能命令をさらに備え、前記命令は、前記装置の前記プロセッサによって実行されると、
コンテンツの保護を提供する１つ以上の証明書に対する要求を送信することであって、前記要求は、前記コンテンツに関連付けられた１つ以上のセキュリティパラメータに基づく、ことと、
前記１つ以上の証明書を取得することと、
前記１つ以上の証明書を使用して、前記コンテンツをセキュアにすることと
を含む動作を前記装置に行わせる、装置。
【請求項８】

前記１つ以上の証明書は、対称キー機密性保護のためのマスタキーを備えている、請求項７に記載の装置。
【請求項９】
前記１つ以上の証明書は、完全性保護および機密性保護のためのものである、請求項７に記載の装置。
【請求項１０】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記コンテンツを暗号化し、暗号化されたコンテンツを作成することを含むさらなる動作を前記装置に行わせる、請求項７に記載の装置。
【請求項１１】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記コンテンツに関連付けられる認証タグを生成することであって、前記認証タグは、ホスティング共通サービスエンティティにおいてホストするための前記コンテンツの完全性および真正性を示す、ことを含むさらなる動作を前記装置に行わせる、請求項１０に記載の装置。
【請求項１２】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記暗号化されたコンテンツおよび前記セキュリティパラメータを含むリソースを作成するための要求をホスティング共通サービスエンティティに送信することを含むさらなる動作を前記装置に行わせる、請求項１０に記載の装置。
【請求項１３】
前記装置は、アプリケーションエンティティであり、前記証明書は、信頼有効化機能から取得される、請求項７に記載の装置。
【請求項１４】
前記コンテンツを取得するために承認されている第２のアプリケーションエンティティは、前記信頼有効化機能から前記１つ以上の証明書を取得することができる、請求項１３に記載の装置。
【請求項１５】
プロセッサと、メモリと、通信回路とを備えている装置であって、前記装置は、その通信回路を介してネットワークに接続され、前記装置は、前記装置の前記メモリ内に記憶されたコンピュータ実行可能命令をさらに備え、前記命令は、前記装置の前記プロセッサによって実行されると、
コンテンツに関連付けられたセキュリティ要件に基づいて、１つ以上の証明書を生成することと、
前記１つ以上の証明書を使用して前記コンテンツをセキュアにすることと、
承認されたクライアントのみがホスティングノードから前記コンテンツを読み出すことができるように、前記ホスティングノードが前記セキュアにされたコンテンツを記憶するという要求を送信することと
を含む動作を前記装置に行わせる、装置。
【請求項１６】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記１つ以上の証明書を信頼有効化機能に登録することを含むさらなる動作を前記装置に行わせる、請求項１５に記載の装置。
【請求項１７】
前記１つ以上の証明書は、前記装置と信頼有効化機能との間のアソシエーションをブートストラップすることによって生成される、請求項１６に記載の装置。
【請求項１８】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記要求に応答して、前記信頼有効化機能から証明書識別を受信することであって、前記要求は、前記証明書識別に関連付けられた証明書を備え、前記要求は、前記証明書の登

録を得ようとする、ことを含むさらなる動作を前記装置に行わせる、請求項１６に記載の装置。
【請求項１９】
前記証明書識別は、前記共通サービスエンティティに一意である、請求項１８に記載の装置。
【請求項２０】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記装置が前記ホスティングノードにおいてリソースを作成するために承認されていることを前記ホスティングノードが決定した場合、成功メッセージを受信することを含むさらなる動作を前記装置に行わせる、請求項１５に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願の引用）
本願は、米国仮特許出願第６２／１８８，１４１号（２０１５年７月２日出願）および米国仮特許出願第６２／２４８，８０８号（２０１５年１０月３０日出願）の利益を主張し、両出願の内容は、それらの全体が参照により本明細書に引用される。
【背景技術】
【０００２】
典型的通信セッションは、概して、ノードとも称され得る、２つ以上の通信エンティティ（例えば、デバイス、アプリケーション等）間の情報の持続的双方向交換を伴う。現在のＲＥＳＴｆｕｌアプローチでは、実際の持続的接続はない。代わりに、通信は、オンデマンドの要求および応答メッセージを介して行われる。例えば、通信セッションは、ある時点で確立され、種々の状況に基づいて（例えば、セッションがタイムアウトした後、またはエンティティのうちの１つがセッションを終了することを決定するときに）、後の時点で解除され得る。通信セッションは、多くの場合、エンティティ間の複数のメッセージの交換を伴い、典型的には、ステートフル（通信エンティティのうちの少なくとも１つが、通信セッションを維持することができるためにセッション履歴についての情報を保存する必要があることを意味する）である。保存され得る例示的情報は、証明書、識別子等のセキュリティコンテキストを含む。通信セッションは、ネットワークプロトコルスタック内の種々の層においてプロトコルおよびサービスの一部として実装され得る。例として、図１は、トランスポートプロトコル層、アプリケーションプロトコル層、アプリケーションサービス層においてネットワークノード間で、およびアプリケーション間で確立された通信セッションを示す。
【０００３】
マシンツーマシン（Ｍ２Ｍ）サービス層は、具体的には、Ｍ２Ｍタイプデバイスおよびアプリケーションのための付加価値サービスを提供することを標的にした、１つのタイプのアプリケーションサービス層の例である。例えば、Ｍ２Ｍサービス層は、サービス層によってサポートされるＭ２Ｍ中心能力の集合へのアクセスをアプリケーションおよびデバイスに提供するアプリケーションプログラミングインターフェース（ＡＰＩ）をサポートすることができる。例示的能力は、限定ではないが、セキュリティ、課金、データ管理、デバイス管理、発見、プロビジョニング、およびコネクティビティ管理を含む。図２は、ｏｎｅＭ２Ｍ仕様によって規定される共通サービス機能（ＣＳＦ）を描写する。
【０００４】
図２を参照すると、図示される機能（能力）は、Ｍ２Ｍサービス層によって定義されるメッセージフォーマット、リソース構造、およびリソース表現を利用するＡＰＩを介して、アプリケーションに利用可能にされる。Ｍ２Ｍネットワーク技術の標準化の高まりつつある傾向が、Ｍ２Ｍサービス層の標準化であった。Ｍ２Ｍサービス層の標準化の例は、種々のｏｎｅＭ２Ｍ仕様を含む。
【０００５】

ＭＭサービス層セッションは、ＭＭサービス層インスタンスとＭＭアプリケーションまたは別のＭＭサービス層インスタンスとの間で確立される通信セッションを指す。ＭＭサービス層セッションは、コネクティビティ、セキュリティ、スケジューリング、データ、コンテキスト等に関連するＭＭサービス層状態から成ることができる。この状態は、ＭＭサービス層、ＭＭアプリケーション、またはその組み合わせによって維持されることができる。ＭＭサービス層セッションは、１つ以上の下にある下層通信セッションの上に重ねられることができる。そうすることで、セッション状態（例えば、セキュリティ証明書、輻輳情報等）は、異なるセッション間で共有され、活用されることができる。加えて、ＭＭサービス層セッションは、ＭＭサービス層セッションが持続し、下層セッションが設定および解除されることから独立して維持されることができるように、下層セッションに対して持続性をサポートすることができる。ＭＭサービス層セッションがその上に重ねられることができる下層セッションの例は、例えば、トランスポート層セキュリティ（ＴＣＰのためのＴＬＳ）またはデータグラムトランスポート層セキュリティ（ＵＤＰのためのＤＴＬＳ）等のプロトコルを使用してセキュアにされ得る、アプリケーションプロトコル層セッション（例えば、ＨＴＴＰまたはＣｏＡＰ）およびトランスポートプロトコル層セッション（例えば、ＴＣＰならびに／もしくはＵＤＰ）を含むが、それらに限定されない。

【０００６】

ｏｎｅＭ２Ｍサービス層セキュリティへの現在のアプローチに関して、ｏｎｅＭ２Ｍエンドポイントがセキュアな様式で互いに通信するとき、ノードおよび中間ノードは、ホップ毎の様式で互いにセキュリティアソシエーションを確立する。各ホップは、他のホップから独立した別個のセキュリティアソシエーションを有し得る。ホップ毎のセキュリティアソシエーションは、対称キーを用いて、認証書／未加工公開キーを使用することによって、または直接プロセスによって、または、デバイス製造業者またはサービスプロバイダのサービスを使用することによって遠隔で行われ得るブートストラッピングプロセスによって、確立され得る。さらに、ｏｎｅＭ２Ｍ　Ｓｅｃｕｒｉｔｙ　Ｓｏｌｕｔｉｏｎの現在のバージョンである、ｏｎｅＭ２Ｍ－ＴＳ－０００３　Ｓｅｃｕｒｉｔｙ　Ｓｏｌｕｔｉｏｎに関連して、「サービス層レベルで、セキュリティアソシエーション確立は、隣接するＡＥ／ＣＳＥ間で、すなわち、ホップ毎に交換されているメッセージを保護するＴＬＳまたはＤＴＬＳセッションをもたらす」。

【０００７】

図３は、関与する２つの通信エンティティに一意、かつ機密である証明書を使用する（Ｄ）ＴＬＳセキュア関連付けを用いた、エンティティ間のホップ毎（ＨｂＨ）のセキュリティアソシエーションの例を示す。示されるように、第１のアプリケーションエンティティ（ＡＥ１）および第１のホスティング共通サービスエンティティ（ＨＣＳＥ１）は、２つのエンティティ（ＡＥ１、ＨＣＳＥ１）によって共有されるＨｂＨ証明書（Ｈ１）に基づいて、セキュアな（Ｄ）ＴＬＳ接続を作成する。同様に、ＨＣＳＥ１および中間ノード（ＩＮ－ＣＳＥ１）は、Ｈ２証明書を使用して、セキュアな（Ｄ）ＴＬＳ接続を設定している。示されるように、証明書Ｈ３は、ＩＮ－ＣＳＥと第２のＨＣＳＥ（ＨＣＳＥ２）との間で（Ｄ）ＴＬＳ接続を作成するために使用され、証明書Ｈ４は、第２のＡＥ（ＡＥ２）とＨＣＳＥ２との間でセキュアな接続を作成するために使用される。

【０００８】

依然として図３を参照して、ＨＣＳＥ１が情報をＡＥ２に通信することを欲した場合、情報は、最初に、ＨＣＳＥ１とＩＮ－ＣＳＥとの間の（Ｄ）ＴＬＳ接続を通して送信される。情報は、次いで、（Ｄ）ＴＬＳアプリケーションによって解読された後に抽出され、次いで、サービス層において処理され、ＩＮ－ＣＳＥとＨＣＳＥ２との間の別個の（Ｄ）ＴＬＳトンネルを通して再パッケージ化されて送信される。ＨＣＳＥ２は、メッセージを処理し、次いで、ＨＣＳＥ２とＡＥ２との間の異なるセキュアなトンネルにメッセージを再び通す。図示される例に示されるように、いずれか２つのＨｂＨエンティティ間の通信は、（Ｄ）ＴＬＳによってセキュアにされ、したがって、エンティティ間で移動中である

メッセージの機密性または完全性の侵害は、それらが（Ｄ）ＴＬＳ接続によって保護されているので、困難であり得るが、しかしながら、メッセージは、次のホップに転送される前にそれがサービス層（ＳＬ）で処理されているエンティティにおいて保護されないこともある。

【０００９】

ここでオブジェクトセキュリティイニシアチブを参照すると、オブジェクトセキュリティイニシアチブは、ＩＥＴＦ内で研究され、標準化され、種々の単一サインオンソリューション（例えば、ＯｐｅｎＩＤ）のために実装されている。ＩＥＴＦ　ＲＦＣ　７１６５、ＪＳＯＮオブジェクト署名および暗号化のための使用事例ならびに要件で記述されるように、「多くのインターネットアプリケーションは、ネットワーク層またはトランスポート層におけるセキュリティ機構に加えて、オブジェクトベースのセキュリティ機構の必要性を有する。長年、暗号メッセージ構文（ＣＭＳ）は、ＡＳＮ．１に基づくバイナリセキュアオブジェクトフォーマットを提供してきた。経時的に、ＡＳＮ．１等のバイナリオブジェクト符号化は、Ｊａｖａ（登録商標）Ｓｃｒｉｐｔ　Ｏｂｊｅｃｔ　Ｎｏｔａｔｉｏｎ（ＪＳＯＮ）等のテキストベースの符号化ほど一般的ではなくなっている」。ＪＳＯＮに基づく異なるセキュリティ側面は、１）完全性／真正性のために、ＪＳＯＮウェブ署名、ＩＥＴＦ－ＲＦＣ　７５１５、２）機密性のために、ＪＳＯＮウェブ暗号化、ＩＥＴＦ－ＲＦＣ　７５１６、３）証明書表現のために、ＪＳＯＮウェブキー、ＩＥＴＦ－ＲＦＣ　７５１６、および４）アルゴリズムのために、ＪＳＯＮウェブアルゴリズム、ＩＥＴＦ－ＲＦＣ　７５１８で規定されている。

【００１０】

上で説明されるように、ｏｎｅＭ２Ｍネットワーク内のセキュリティへの既存のアプローチは、例えば、限定されている。例えば、コンテンツは、コンテンツが互いを信頼するエンティティ間で移動中である（静止していない）間のみ保護され得る。

【発明の概要】

【課題を解決するための手段】

【００１１】

本概要は、発明を実施するための形態において以下でさらに説明される、簡略化形態の一連の概念を導入するように提供される。本概要は、請求される主題の主要な特徴または不可欠な特徴を識別することを意図せず、請求される主題の範囲を限定するために使用されることも意図していない。さらに、請求される主題は、本開示の任意の部分で記述されるいずれかまたは全ての不利点を解決する制限に限定されない。

【００１２】

上で説明される問題等の種々の欠点が、本明細書で対処される。一実施形態では、Ｍ２Ｍネットワーク内のコンテンツの完全性および機密性が保護される。そのようなコンテンツは、コンテンツがノードまたは装置に記憶されるように「静止」し得る。

【００１３】

一実施形態では、装置、例えば、アプリケーションエンティティは、コンテンツの保護を提供する１つ以上の証明書に対する要求を送信する。要求は、コンテンツに関連付けられた１つ以上のセキュリティパラメータに基づき得る。装置は、１つ以上の証明書を取得し、コンテンツをセキュアにするために１つ以上の証明書を使用し得る。証明書は、対称キー機密性保護のためのマスタキーを備え得る。証明書は、完全性保護および機密性保護のための証明書を備え得る。装置は、暗号化されたコンテンツを作成するためにコンテンツを暗号化し得る。装置は、コンテンツに関連付けられる認証タグを生成し得る。さらに、装置は、セキュアにされたコンテンツおよびセキュリティパラメータを含むリソースを作成するための要求をホスティング共通サービスエンティティに送信し得る。証明書は、一例によると、信頼有効化機能、例えば、Ｍ２Ｍ登録機能から取得され得る。ホスティング共通サービスエンティティは、承認されたアプリケーションのみがリソースを作成することを可能にし得、ホスティング共通サービスエンティティは、承認されたアプリケーションのみが暗号化されたコンテンツを読み出すことを可能にし得る。

【００１４】
別の実施形態では、１つ以上のセキュリティ要件に基づいて、装置は、１つ以上の暗号パラメータを決定する。装置はさらに、セキュアホスティング要求メッセージをコンテンツホスティング機能に送信し得、セキュアホスティング要求メッセージは、コンテンツホスティング機能が１つ以上の暗号パラメータを使用してコンテンツをセキュアに記憶することができるように、１つ以上の暗号パラメータおよびそれに関連付けられるコンテンツを含み得る。１つ以上の暗号パラメータに基づいて、装置は、コンテンツが機密であるようにコンテンツを暗号化し得る。例では、コンテンツは、サブコンポーネントから成り得、ノードは、１つ以上の暗号パラメータに基づいて、各サブコンポーネントが機密であるように、サブコンポーネントの各々を暗号化する。別の例では、コンテンツは、属性および値のペアから成り得、ノードは、１つ以上の暗号パラメータに基づいて、各値が機密であるように、値の各々を暗号化し得る。ノードはまた、コンテンツが完全性保護されるように、コンテンツに関連付けられる認証タグを計算し得る。

【図面の簡単な説明】

【００１５】
本願のより堅調な理解を促進するために、ここで、同様の要素が同様の数字で参照される、付随の図面を参照する。これらの図面は、本願を限定するものと解釈されるべきではなく、例証にすぎないものであることを意図している。
【図１】図１は、ネットワークノード間で確立される種々の通信セッションの例を示す略図である。
【図２】図２は、ｏｎｅＭ２Ｍによって規定される共通サービス機能を示す、略図である。
【図３】図３は、ホップ毎の様式で互いにのセキュリティアソシエーションを確立するｏｎｅＭ２Ｍノードの例を示すコールフローである。
【図４】図４は、アプリケーションエンティティ（ＡＥ）、ホスティング共通サービスエンティティ（ＨＣＳＥ）、および中間ノード共通サービスエンティティ（ＩＮ－ＣＳＥ）を含むネットワークの脆弱性を悪用する悪意のあるエンティティの例を示す、例示的使用事例を図示するコールフローである。
【図５】図５は、攻撃者がＩＮ－ＣＳＥまたはＨＣＳＥにおける脆弱性を悪用し得る別の例示的使用事例を図示するコールフローである。
【図６】図６は、例示的実施形態による、例示的機能およびその間の相互作用を描写するコールフローである。
【図７】図７は、コンポーネントおよびサブコンポーネントで構成されるコンテンツを含む例示的コンテンツを描写する。
【図８】図８は、例示的コンテンツに関連付けられる例示的暗号パラメータを描写する。
【図９】図９は、例示的コンテンツに関連付けられる例示的なクライアント特定の暗号パラメータを描写する。
【図１０】図１０は、例示的実施形態による、コンテンツ作成およびセキュリティ決定機能（ＣＣＳＤＦ）と低信頼性コンテンツホスティング機能（ＣＨＦ）との間の例示的メッセージングを示すコールフローである。
【図１１】図１１は、例示的実施形態による、ＣＣＳＤＦとセキュアコンテンツホスティング機能（ＳＣＨＦ）との間の例示的メッセージングを示すコールフローである。
【図１２】図１２は、任意の例示的実施形態による、コンテンツをホストするための場所を決定するための例示的フロー図である。
【図１３】図１３は、例示的実施形態による、保護コンテンツ記憶部（ＰＣＳ）内に記憶された例示的保護コンテンツ構造を示す。
【図１４】図１４は、コンテンツに関連付けられる例示的暗号パラメータを描写する。
【図１５】図１５は、例示的実施形態による、コンテンツ特定の証明書請求を描写するコールフローである。
【図１６】図１６は、例示的実施形態による、クライアント特定の証明書請求を描写する

コールフローである。
【図１７】図１７は、例示的実施形態による、コンテンツ特定の証明書登録を描写するコールフローである。
【図１８】図１８は、別の例示的実施形態による、クライアント証明書登録を描写するコールフローである。
【図１９】図１９は、例示的実施形態による、第三者証明書請求を描写するコールフローである。
【図２０】図２０は、例示的実施形態による、コンテンツ読み出しのためのコールフローである。
【図２１】図２１は、例示的実施形態による、クライアントによって行われることができる例示的セキュリティチェックを図示するフロー図である。
【図２２】図２２は、本明細書に説明される例示的セキュリティ機能性とともに示される図２からの略図である。
【図２３】図２３は、本明細書に説明される例示的セキュリティ機能性が描写された共通サービス機能（ＣＳＦ）の略図である。
【図２４】図２４は、コンテンツがｏｎｅＭ２Ｍリソースとして表される例示的実施形態を図示するコールフローである。
【図２５】図２５は、例示的実施形態による、ＣＳＥにおいて作成されたＣｒｅｄｅｎｔｉａｌ－Ｉｄリソースの例示的構造を図示する。
【図２６】図２６は、サービス有効化機能（ＳＥＦ）がＣＳＥに常駐する別の例示的実施形態を図示するコールフローである。
【図２７】図２７は、例示的実施形態による、特にマシンツーマシン（Ｍ２Ｍ）登録機能（ＭＥＦ）の中で、信頼有効化機能において作成されたＣｒｅｄｅｎｔｉａｌ－Ｉｄリソースの例示的構造を図示する。
【図２８】図２８は、例示的実施形態による、例示的アクセス制御ポリシの例示的構造を描写する。
【図２９】図２９は、例示的実施形態による、保護されたコンテンツのための例示的リソース構造を図示する。
【図３０】図３０は、例示的実施形態による、例示的暗号パラメータリソースを図示する。
【図３１】図３１は、完全性保護される管理オブジェクトの例を図示する。
【図３２】図３２は、例示的セキュリティポリシリソースを図示する。
【図３３】図３３は、例示的実施形態による、ＣＣＳＤＦにおいて提供され得る例示的グラフィカルユーザインターフェース（ＧＵＩ）を図示する。
【図３４】図３４は、例示的実施形態による、ＳＣＨＦにおいて提供され得る例示的ＧＵＩを図示する。
【図３５】図３５は、例示的実施形態による、ＳＥＦにおいて提供され得る例示的ＧＵＩを図示する。
【図３６Ａ】図３６Ａは、１つ以上の開示される実施形態が実装され得る例示的マシンツーマシン（Ｍ２Ｍ）もしくはモノのインターネット（ＩｏＴ）通信システムの系統図である。
【図３６Ｂ】図３６Ｂは、図３６Ａに図示されるＭ２Ｍ／ＩｏＴ通信システム内で使用され得る例示的アーキテクチャの系統図である。
【図３６Ｃ】図３６Ｃは、図３６Ａに図示される通信システム内で使用され得る例示的Ｍ２Ｍ／ＩｏＴ端末またはゲートウェイデバイスの系統図である。
【図３６Ｄ】図３６Ｄは、図３６Ａの通信システムの側面が具現化され得る例示的コンピューティングシステムのブロック図である。
【図３７】図３７は、リソース特定のコンテンツ保護のための例示的実施形態を図示するコールフローである。
【図３８】図３８は、クライアント特定のコンテンツ保護のための例示的実施形態を図示

するコールフローである。
【発明を実施するための形態】
【００１６】
上で説明されるように、Ｍ２Ｍネットワーク内のセキュリティへの既存のアプローチは、限定されている。例えば、ｏｎｅＭ２Ｍでは、コンテンツは、それがトランスポート層プロトコル（例えば、ＴＬＳ／ＤＴＬＳ）を用いて２つの「信頼される」エンティティ間で「移動中」である間のみ保護され得る。したがって、コンテンツは、それがエンティティにおいてホストされている（静止している）間には保護されない。コンテンツ（オブジェクト）保護は、行われるとすれば、アプリケーション層において行われなければならないようである。本明細書では、アプリケーションコンテンツ保護アプローチに関連付けられる問題があることが認識される。例えば、アプリケーションは、アプリケーションコンテンツ保護のための一様な機構を提供しない。さらに、サービス層リソースは、それ自体が保護されない。また、アプリケーション層保護があったとしても、それらは実際のアプリケーションデータのためにのみ保護を提供し、サービス層（ＳＬ）に関連付けられるリソースのための保護を提供しないであろう。本明細書では、コンテンツをセキュアにするための別個のアプリケーション層プロトコルが、アプリケーションコンテンツ保護アプローチのために行われなければならず、それが煩雑であり得ることが、さらに認識される。あるシナリオでは、サービス層が付加価値サービスを提供することができるために、コンテンツは、その非暗号化形態である必要があり得る。本明細書では、ｏｎｅＭ２Ｍリソースに関連付けられるセキュリティ証明書およびセキュリティ保護のライフサイクル管理が、現在、行われていないことも認識される。解除されたエンティティ上でホストされるデータのセキュリティをハンドリングするための機構は、現在、対処されていない。
【００１７】
本明細書で使用される場合、「サービス層」という用語は、ネットワークサービスアーキテクチャ内の機能層を指す。サービス層は、典型的には、ＨＴＴＰ、ＣｏＡＰ、またはＭＱＴＴ等のアプリケーションプロトコル層の上方に位置し、付加価値サービスをクライアントアプリケーションに提供する。サービス層はまた、例えば、制御層およびトランスポート／アクセス層等のより下のリソース層におけるコアネットワークへのインターフェースも提供する。サービス層は、サービス定義、サービス実行時間有効化、ポリシ管理、アクセス制御、およびサービスクラスタ化を含む、（サービス）能力または機能性の複数のカテゴリをサポートする。近年、いくつかの業界規格団体（例えば、ｏｎｅＭ２Ｍ）が、インターネット／ウェブ、セルラー、企業、およびホームネットワーク等の展開の中へのＭ２Ｍタイプのデバイスならびにアプリケーションの統合に関連付けられる課題に対処するように、Ｍ２Ｍサービス層を開発している。Ｍ２Ｍサービス層は、ＣＳＥまたはＳＣＬと称され得る、サービス層によってサポートされる上記の能力もしくは機能性の集合または組へのアクセスをアプリケーションおよび／もしくは種々のデバイスに提供することができる。いくつかの例は、種々のアプリケーションによって一般的に使用されることができる、セキュリティ、課金、データ管理、デバイス管理、発見、プロビジョニング、およびコネクティビティ管理を含むが、それらに限定されない。これらの能力または機能性は、Ｍ２Ｍサービス層によって定義されるメッセージフォーマット、リソース構造、およびリソース表現を利用するＡＰＩを介して、そのような種々のアプリケーションに利用可能にされる。ＣＳＥまたはＳＣＬは、ハードウェアおよび／もしくはソフトウェアによって実装され得る機能的エンティティであり、種々のアプリケーションならびに／もしくはデバイスが（サービス）能力または機能性（例えば、そのような機能的エンティティ間の機能的インターフェース）を使用することができるために、それらにエクスポーズされるそのような能力もしくは機能性を提供する。
【００１８】
例の目的で、現在のｏｎｅＭ２Ｍソリューションに関する問題をさらに例証するために、図４および５は、それぞれの使用事例を図示する。図４では、データ／コンテンツプライバシーへの影響が示され、図５は、データ／コンテンツの完全性保護および認証の不足

に関連付けられる問題を例証する。

【００１９】

図４を特に参照すると、ネットワーク４００は、４つの例示的エンティティ、すなわち、第１のアプリケーションエンティティ（ＡＥ１）と、ホスティング共通サービスエンティティ（ＨＣＥＳ１）と、中間ノードＣＳＥ（ＩＮ－ＣＳＥ）と、ハッカーアプリケーションまたは悪意のない機能であり得る、悪意のあるエンティティとを含む。４０２では、ＡＥ１は、サービス層において、ＨＣＳＥ１内でリソースを作成し、リソースは、属性およびコンテンツ／コンテンツインスタンスを記憶する。この使用事例では、２つの属性が、すなわち、属性１および属性２が、例として提供される。例によると、ＡＥ１およびＨＣＳＥ１は、互いに相互認証しており、４０２において「リソースを作成する」動作を行うことに先立って、セキュアな通信チャネルを使用している。ある時点で、４０４では、悪意のあるエンティティ（例えば、ハッキングアプリケーション）は、ＩＮ－ＣＳＥを通してＨＣＳＥ１内の脆弱性を悪用する。ある場合、ハッキングアプリケーションは、ＩＮ－ＣＳＥを通過する必要なく、ＨＣＳＥ１に到達することが可能であり得る。他の場合、ＩＮ－ＣＳＥ上のプロトコルサポート（例えば、起動する開放ポートおよびサービス）の多様性により、おそらくＩＮ－ＣＳＥにおける脆弱性も悪用することによって、ＩＮ－ＣＳＥは、ハッキングアプリケーションのための良好な進入点になり得る。ハッカーがＨＣＳＥ１にアクセスすることができると、４０６においてＡＥ１リソース内に記憶されたコンテンツを盗む。これは、巧妙さをあまり必要としない古典的な攻撃であり得る。そのような攻撃を軽減する１つの方法は、ディスク全体を暗号化すること、またはファイル毎の基準で暗号化を使用することである。しかしながら、コンテンツは、ＳＬにおいて処理され、通信パス上の通過ノードにおいて解読される必要があり得、その結果、コンテンツは、攻撃の影響を受けやすくなる。別の軽減技法は、ＪＳＯＮベースのオブジェクト署名および暗号化機構を使用して、コンテンツを保護することである。しかし、現在、ＳＬリソースを保護するためのそのような機構の使用を可能にする枠組みがない。追加の問題は、ＨＣＳＥ１のプラットフォームが信頼できず、したがって、セキュアなプロセスが実施されないこともあることである。さらに、ルートキーが破られた場合、それは、ＨＣＳＥ１上に記憶された全てのＡＥからのデータを露出させる。手短に言えば、アプリケーションデータまたはユーザの機密データのセキュリティは、ユーザもしくはアプリケーションがあまり制御を有していないエンティティにオフロードされ、プラットフォームの信頼性は、ユーザが有するＳＰの信頼に基づく。加えて、ＨＣＳＥ１が解除された場合、データは、ＨＣＳＥ１内に留まり、ファイルベースの暗号化のみによって保護され得、それは、リソースを保護する旧来のオペレーティングシステムによって容易に破られ得る。

【００２０】

したがって、要約すると、図４の使用事例は、例えば、限定ではないが、コンテンツが静止しているときのホスティングエンティティ（例えば、ＨＣＳＥ）における機密性保護機構の欠如と、ＨＣＳＥ（例えば、低信頼性ＨＣＳＥ）からさえもコンテンツを隠す機構の欠如と（コンテンツをクライアントに転送するときに、データがＴＬＳ／ＤＴＬＳトンネルを通り抜けると各ホップ（例えば、通過ＣＳＥ）がコンテンツへの非暗号化アクセスを有する）、コンテンツのライフサイクルのために規則的にコンテンツのセキュリティを再生利用する能力の欠如とを示す。

【００２１】

ここで図５に図示される使用事例を参照すると、ネットワーク５００は、コンテンツを生成する第１のアプリケーションエンティティ（ＡＥ１）と、第２のＡＥ（ＡＥ２）と、ＡＥ１によって生成されるコンテンツを消費するクライアントアプリケーションである第３のＡＥ（ＡＥ３）とを含む。ネットワークはさらに、ホスティングＣＳＥ（ＨＣＳＥ１）と、中間ノード－ＣＳＥ（ＩＮ－ＣＳＥ）とを含む。例では、コンテンツは、いかなる完全性保護も伴わずにＨＣＳＥ１上でホストされる。図４に図示される例示的使用事例と同様に、攻撃者は、ＩＮ－ＣＳＥまたはＨＣＳＥ１における脆弱性を悪用し得る。１では、ＡＥ１は、ＨＣＳＥ１においてリソースを作成する。例えば、攻撃者は、２および３に

おいて、リソースおよび／またはリソース構造（例えば、属性ならびに／もしくはコンテンツ）を修正し得る。示されるように、図５は、攻撃者が、属性１と称されるＡＥ１の属性の無承認修正を行うことができるシナリオを図示する。ＡＥ１のリソースにサブスクライブするＡＥ２は、４および５において、リソースの修正されたコピーを取得する。ある場合、例えば、ＡＥ１から取得されるリソースがＡＥ２によって重要な決定または動作を行うために使用されるとき、修正は、多大な影響を及ぼし得る。６および７では、図示される例によると、攻撃者は、属性２を削除し、新しい属性（属性３および属性４）を追加する。したがって、例では、攻撃者は、リソースだけではなく、リソースの構造も変更している。リソースにサブスクライブするＡＥ３は、次いで、ＡＥ１によって作成されたものと完全に異なるリソースツリーを有する。したがって、図５の例示的使用事例によって示されるように、現在のセキュリティアプローチは、完全性保護をリソースに提供しないこと、完全性保護をリソースの構造に提供しないこと、および／または完全性保護をシステム重要リソースに提供しないこともある。

【００２２】

上で説明される問題等の種々の欠点が、本明細書で対処される。一実施形態では、コンテンツの完全性および機密性が保護される。本明細書で使用される場合、他に規定されない限り、コンテンツという用語は、機械制御型または人間制御型クライアントアプリケーションもしくはサービス機能によって生成または消費される任意のデータ（例えば、ファームウェア、構成パラメータ、ポリシ、コンテキスト、文書等）を指す。したがって、コンテンツおよびデータという用語は、限定ではないが、本明細書では同義的に使用され得る。コンテンツは、その最も未加工の形態（例えば、温度読み取り値、他のセンサ読み取り値等）であり得る。ある場合、コンテンツは、それに関連付けられる追加のメタデータを伴う未加工データであり得るか、または未加工データおよびメタデータを伴う未加工データの組み合わせであり得る。コンテンツは、例えば、機械実行可能コンテンツ（例えば、コンピュータプログラム、バイナリコード、コンパイルまたは翻訳されていることもある実行可能機械コード、コンピュータプログラムスクリプト等）、コンピュータ関連構成パラメータ、動作ポリシ（例えば、セキュリティまたはサービスポリシ）、マルチメディアコンテンツ（例えば、ビデオ、オーディオ等）、文書、またはある通貨、方略、もしくは知的価値を有し得るあらゆるもの等の種々の情報も指し得る。コンテンツは、オブジェクトも指し得る。

【００２３】

本明細書で使用される場合、別様に規定されない限り、認証は、エンティティに関連付けられる識別における信頼を確立するプロセスを指す。機密性は、概して、承認エンティティのみがデータを閲覧できることを確実にするプロセスを指す。本明細書で使用される場合、別様に規定されない限り、エンティティまたはノードは、アプリケーション、複数のアプリケーションの一部、サービス有効化機能、もしくはデバイス（例えば、センサデバイス）を指し得る。本明細書に説明される種々の技法は、ハードウェア、ファームウェア、ソフトウェア、または適切である場合、それらの組み合わせに関連して、実装され得る。そのようなハードウェア、ファームウェア、およびソフトウェアは、通信ネットワークの種々のノードに位置する装置の中に常駐し得る。装置は、本明細書に説明される方法を達成するように、単独で、または互いに組み合わせて動作し得る。本明細書で使用される場合、「装置」、「ネットワーク装置」、「ノード」、「デバイス」、「エンティティ」、および「ネットワークノード」という用語は、同義的に使用され得る。「完全性」という用語は、メッセージまたはシステムが無承認エンティティによって改変されていないという信頼を確立するプロセスを指し得る。モノのインターネット（ＩｏＴ）は、概して、インターネットに接続されることができる、一意に識別可能なオブジェクトおよびそれらの仮想表現を指す。本明細書で使用される場合、ライフサイクル管理という用語は、データおよびそれに関連付けられる証明書が、プロビジョニング、保守、および解除段階を通して管理される機構を指す。

【００２４】

種々のＭ２Ｍ用語が、本明細書で使用される。Ｍ２Ｍサービス層は、概して、アプリケーションプログラミングインターフェース（ＡＰＩ）および下層ネットワーキングインターフェースの組を通して、Ｍ２Ｍアプリケーションならびにデバイスのための付加価値サービスをサポートするソフトウェアミドルウェア層を指す。Ｍ２Ｍサービス層ホップは、２つのＭ２Ｍサービス層間、またはＭ２Ｍサービス層とＭ２Ｍアプリケーションとの間のＭ２Ｍサービス層通信セッションを指す。Ｍ２Ｍサービス層セッションは、典型的には、本質的にステートフルである、２つ以上の通信エンティティ間のメッセージの確立された交換を指す。本明細書で使用される場合、別様に規定されない限り、Ｍ２Ｍサービス層セッションエンドポイントは、Ｍ２Ｍサービス層セッション通信のソースまたは宛先であることができる論理エンティティを指す。さらに、本明細書で使用される場合、別様に規定されない限り、Ｍ２Ｍサービス層セッションマネージャは、Ｍ２Ｍサービス層セッション管理のためのサービスを提供する論理エンティティを指す。ノンスは、セッションに関連付けられ得、その有効性がセッション／時間成分に関連付けられ得る乱数値を指す。

【００２５】

前置きとして、種々の機能およびプロセス機構が、コンテンツのセキュリティ保護を可能にするために本明細書で定義される。種々の機能性は、例の目的のために名前を付けられ、機能は、代替として、所望に応じて名前を付けられ得ることが理解されるであろう。コンテンツ作成およびセキュリティ決定機能（ＣＣＳＤＦ）が、以下で説明される。ＣＣＳＤＦは、複数の機能から成り、同一のエンティティ（ノード）上でホストされ得るか、または異なる管理ドメイン上にも常駐し得る複数のエンティティ（ノード）を横断して分散され得る。コンテンツ作成機能（ＣＣＦ）は、収集されるデータに基づいてコンテンツを作成し得る。ある場合、コンテンツは、未加工データまたは情報であり得、コンテンツは、未加工データから作成されるセンサデータまたは情報を含み得る。ＣＣＦは、コンテンツに対する構造、およびコンテンツのサブコンポーネントに基づくコンテンツに対する構造のある形態を作成し得る。セキュリティ決定機能（ＳＤＦ）は、コンテンツに関連付けられたセキュリティ要件を決定する責任があり得る。ＳＤＦは、コンテンツを保護するために要求されるセキュリティのレベルを決定し得る。例えば、ＳＤＦは、確立されたポリシに基づいて、コンテンツ保護のための一般的セキュリティ要件を決定し得る。

【００２６】

セキュアコンテンツホスティング機能（ＳＣＨＦ）が、本明細書に説明される。例示的実施形態では、ＳＣＨＦは、コンテンツをセキュアにホストする機能である。ＳＣＨＦは、セキュリティポリシ有効化エンティティとしても機能し、アクセス制御チェックを行い得る。ＳＣＨＦは、コンテンツをセキュアにすることができるために、必要な暗号プロシージャを処理し、識別し、行い得る。ＳＣＨＦは、適切な証明書を要求して登録するために、セキュリティ有効化機能（ＳＥＦ）と相互作用し得る。一実施形態では、ＳＥＦは、コンテンツを保護すること、および／またはコンテンツにアクセスすることを行うための証明書を提供する有効化機能である。ＳＥＦは、例えば、コンテンツへのアクセスをクライアントに提供するために、信頼される第三者（ＴＴＰ）等の信頼される仲介者として動作し得る。ＳＥＦは、適切なコンテンツ特定の証明書をプロビジョニングし、登録し得る。ＳＥＦは、適切なクライアント特定の証明書をプロビジョニングし、登録し得る。

【００２７】

セキュリティパラメータ決定プロセス（ＳＰＤＰ）が、例示的実施形態に従って以下で説明される。例示的ＳＰＤＰの一部として、セキュリティパラメータの正しい組が、「静止している」特定のコンテンツのために決定される。加えて、コンテンツのライフサイクル管理も、決定され得る。例えば、静止しているコンテンツセキュリティに関するセキュリティポリシが、クエリを行われ得る。ポリシは、適切なセキュリティパラメータが導出されるように処理され得る。ライフサイクル管理パラメータも、決定され、導出され得る。

【００２８】

例示的実施形態では、セキュアホスティング請求プロセス（ＳＨＲＰ）が、ＣＣＳＤＦ

によって開始され得る。ある事例では、ＳＨＲＰは、ＳＣＨＦによっても開始され得る。請求の一部として、ＣＣＳＤＦは、ＳＣＨＦを用いたコンテンツのセキュアなホスティングに対して要求し得る。ＳＣＨＦは、ゼロホップ（同一のプラットフォーム上でホストされる）であり得るか、ＣＣＳＤＦから１つのホップで離れ得るか（概して、好ましいアプローチ）、またはＣＣＳＤＦから複数のホップで離れ得る（２つ以上のホップで離れて）。ＳＨＲＰは、あるレベルの信頼性に基づいて、ＳＣＨＦが発見されることを可能にする。例示的実施形態では、コンテンツのホスティングは、セキュリティ要件に基づいて要求され得る。ＳＣＨＦは、一実施形態に従ってセキュアなコンテンツをホストし得る。

【００２９】

証明書請求プロセス（ＣＱＰ）と、証明書登録プロセス（ＣＧＰ）とを含み得る、証明書請求および登録プロセス（ＣＲＲＰ）が、以下で説明される。ＣＱＰ中、ＳＣＨＦは、コンテンツのセキュアな記憶のための適切な証明書のプロビジョニングを要求し得る。このプロセスは、例えば、ある場合、ＳＣＨＦがコンテンツのための適切な証明書を生成するために十分であり得るので、随意であり得る。クライアント特定のコンテンツが保護されるべきである例では、次いで、ＳＤＰは、クライアントの証明書を要求し得る。例えば、特定のコンテンツに関連付けられる証明書が、要求され得る。さらなる一例として、証明書は、アルゴリズムおよび証明書タイプに基づいて要求され得る。クライアントに特定である証明書も、要求され得る。例示的ＣＧＰの一部として、コンテンツを保護するために使用される証明書の組が、ＳＥＦを用いて発行され得る。拡張性の理由により、例えば、証明書は、複数のＳＥＦにおいて発行され得る。ＣＧＰは、コンテンツに関連付けられる生成された証明書の登録を要求する能力；使用されるべきアルゴリズム、証明書タイプ、どのようにして証明書が使用され得るかについての機構、および証明書に関連付けられるアクセス制御ポリシ（ＡＣＰ）を規定する能力；および、クライアントによる使用のために意図される証明書を登録する能力を提供し得る。

【００３０】

例示的セキュアホスティングプロセス（ＳＨＰ）が、本明細書に説明される。このプロセスの一部として、ＳＣＨＦは、ＣＣＳＤＦからのＳＨＲＰメッセージに基づいてコンテンツをホストし得る。コンテンツは、コンテンツを保持するためのコンテナ／属性の正しい組を含むことによって、ＣＣＳＤＦによって要求される適切なフォーマットでホストされ得る。代替として、または加えて、ＳＣＨＦは、コンテンツをセキュアにホストするために、適切な暗号動作を行う必要があり得る。実施され得る暗号動作のタイプは、コンテンツに関連付けられるセキュリティパラメータに基づき得る。ＳＣＨＰは、コンテンツを保護するために適切な暗号プロセスを取得して実施し得る。さらに、ＳＨＲＰメッセージに基づいて、ＳＣＨＦは、コンテンツに関連付けられるセキュリティプロパティを更新するためにトリガされる適切なライフサイクル管理プロセスを作成し得る。例えば、コンテンツは、削除され得るか、またはアクセス不可能にされ得る。

【００３１】

例示的第三者証明書請求プロセス（ＴＰＣＲＰ）が、本明細書に説明される。ある場合、ＳＥＦは、クライアントを認証し、クライアント（第三者）がリソースにアクセスし、その真正性を検証することができるように、クライアントに必要な証明書を提供する必要があり得る。ＴＰＣＲＰは、コンテンツに関連付けられる識別（ｃｏｎｔｅｎｔ－Ｉｄ）に基づいて、任意のエンティティ（例えば、クライアント）がＳＥＦまたはＳＣＨＦに証明書を要求することを可能にし得る。例示的コンテンツ読み出しプロセス（ＣＲＰ）中、クライアントは、コンテンツへのアクセスを要求する機構を開始する。クライアントは、事前構成された情報からＳＣＨＦに関する情報を取得し得るか、または、情報は、ＤＮＳ－ＳＤもしくはＲＤを使用して動的に発見され得るための。必要な暗号パラメータを含むセキュアなコンテンツ（暗号化および／または完全性保護された）が、読み出され得る。コンテンツ処理（ＣＰ）も、本明細書に説明される。ＣＰ中、コンテンツにアクセスすることを希望するクライアントは、コンテンツの真正性および／または完全性を検証することを所望し得る。加えて、クライアントは、コンテンツ構造およびコンテンツに関連付け

られる属性を検証することも所望し得る。一例では、クライアントは、コンテンツの真正性／完全性、コンテンツのサブコンポーネント、およびコンテンツの構造を検証することができる。コンテンツは、プロビジョニングされた暗号パラメータに基づいて解読され得る。

【００３２】

例示的コンテンツライフサイクル管理プロセス（ＣＬＭＰ）では、ＣＣＳＤＦは、随意に、特定のコンテンツのためのライフサイクル管理を更新するために明示的ＣＬＭＰメッセージを送信し得る。このプロセス／メッセージングは、ＣＣＳＤＦがＳＨＲＰの一部として明示的ライフサイクル管理要件を通信した場合、省略され得る。証明書は、リフレッシュされ得、暗号動作は、周期的に行われ得る。コンテンツは、解除期間に基づいて消去され得る。コンテンツに関連付けられる証明書は、証明書が、一時的または恒久的に、再プロビジョニング、再保護、もしくは除去されるように管理され得る。

【００３３】

概して、図６を参照すると、上で説明される種々の欠点に対抗するために、コンテンツ／データの保護が、本明細書に説明されるように可能にされる。本明細書に説明されるように、データの保護は、データへのアクセスを要求するエンティティが、データにアクセスするために承認されていることを確実にすることを含み得る（認証も含み得る）。データの保護は、データが無承認エンティティから隠され（例えば、暗号化され）、無承認エンティティに対して不透明に見えることを含み得る。データの保護は、データの無承認修正を検出することを含み得る。コンテンツの保護は、規則的または恒久的にコンテンツのライフサイクルを管理することを含み得る。

【００３４】

一実施形態では、コンテンツは、（要求される場合）サブコンポーネントから作成され、コンテンツに対する構造は、サブコンポーネントに基づいて作成され得る。これは、ＣＣＰによって行われ得る。ＳＤＦは、そのサブコンポーネントのセキュリティ要件を査定することによって、コンテンツ保護のためのセキュリティ要件のリスクベースの査定を行い得る。実施形態では、静止しているコンテンツを保護するために要求される適切なセキュリティパラメータが、識別される。これは、ＳＰＤＰを使用することによって達成され得る。ＣＲＲＰは、証明書を取得または生成し、コンテンツ保護のために証明書を登録し得る。例示的実施形態では、コンテンツは、ＳＨＰを使用してセキュアな様式でホストされる。本明細書に説明されるようなＴＰＣＲＰは、承認された第三者にコンテンツにアクセスするための証明書をプロビジョニングするための能力を提供し得る。

【００３５】

以下の説明は、主にコンテンツの保護に焦点を当てているが、本明細書に説明される証明書は、種々のサービス有効化機能によって作成され、更新され、削除され、読み出されるシステムリソースを保護するために適切に調整され得ることが理解されるであろう。

【００３６】

図６－３５、３７、および３８（本明細書の以降で説明される）は、コンテンツを保護する方法ならびに装置の種々の実施形態を図示する。これらの図では、種々のステップまたは動作が、１つ以上のノードもしくは装置によって行われるように示されている。これらの図に図示されるノードおよび装置は、通信ネットワーク内の論理エンティティを表し得、以下で説明される図３６Ａまたは３６Ｂに図示される一般的アーキテクチャのうちの１つを備え得る、そのようなネットワークのノードまたは装置のメモリ内に記憶され、そのプロセッサ上で実行するソフトウェア（例えば、コンピュータ実行可能命令）の形態で実装され得ることが理解される。すなわち、図６－３５、３７、および３８に図示される方法は、例えば、図３６Ｃまたは３６Ｄに図示されるノードもしくはコンピュータシステム等のネットワークノードまたは装置のメモリ内に記憶されたソフトウェア（例えば、コンピュータ実行可能命令）の形態で実装され得、そのコンピュータ実行可能命令は、ノードまたは装置のプロセッサによって実行されると、図に図示されるステップを行う。これらの図に図示される任意の伝送および受信ステップがノードまたは装置のプロセッサなら

びにそれが実行するコンピュータ実行可能命令（例えば、ソフトウェア）の制御下で、ノードまたは装置の通信回路（例えば、それぞれ、図３６Ｃおよび３６Ｄの回路３４または９７）によって行われ得ることも理解される。

【００３７】

ソフトウェアで実装され、例えば、ユーザ機器（ＵＥ）上またはサーバ上にホストされる他のアプリケーションとともに、エンティティ上に常駐し得る、例示的機能が、以下で説明される。これらの機能は、専用ハードウェアエンティティ上に常駐し得、したがって、本書の全体を通して、機能、エンティティ、装置、およびノードという用語は、限定ではないが、同義的に使用され得る。例えば、クライアントは、ユーザのデバイス上に常駐するアプリケーションまたはサービスであり得る。クライアントは、マシン上に常駐するアプリケーションまたはサービス、専用ハードウェア、もしくはクラウドベースのアプリケーションまたはサービスも指し得る。クライアントは、プラットフォーム内で、または異なるプラットフォーム上で分散様式において一緒に動作するアプリケーションもしくはサービスのグループの一部でもあり得る。クライアントは、概して、コンテンツにアクセスするために要求を開始する。コンテンツにアクセスするためにクライアントが要求を送信するためのトリガが、ユーザ、マシン、アプリケーション、またはサービスによって開始され得る。

【００３８】

図６を参照すると、コンテンツ作成およびセキュリティ決定機能（ＣＣＳＤＦ）は、複数の機能から成り、同一のエンティティ（ノード）上でホストされ得るか、または異なる管理ドメイン上にも常駐し得るエンティティ（複数のノード）を横断して分散され得る。機能が異なる管理ドメイン内に常駐する場合、機能がトランザクションを行うために常駐する種々のエンティティ間に信頼関係が存在し得る。ＣＣＳＤＦは、コンテンツを生成するエンティティ、またはコンテンツを作成するためにデータソース（例えば、センサ）を使用するエンティティであり得る。ある場合、ＣＣＳＤＦおよびＳＣＨＦは、同一の物理的エンティティ（例えば、サーバ、ゲートウェイ）上で共同ホストされ得る。一実施形態では、コンテンツ作成機能（ＣＣＦ）は、種々のソース（例えば、センサ、アプリケーション、データベース等）からデータを収集し、コンテンツを作成することに関与する。データは、センサおよびアプリケーションによって先を見越して収集または発行され得る。ＣＣＦは、コンテンツ作成に関与するプロセスを管理する。セキュリティ決定機能（ＳＤＦ）は、コンテンツに関連付けられたセキュリティ要件を決定する責任があり得る。ＳＤＦは、コンテンツを保護するために要求されるセキュリティのレベルを決定し得る。本開示では、コンテンツが「静止している」ときのコンテンツに関連付けられたセキュリティ要件が、決定される。すなわち、記憶に関するセキュリティ要件およびコンテンツセキュリティの管理が、本明細書に説明される。上記のように、ＣＣＦおよびＳＤＦは、同一のノード／エンティティ上で実施され得るか、または機能は、異なるノード／エンティティ上に常駐し得る。

【００３９】

セキュアコンテンツホスティング機能（ＳＣＨＦ）は、コンテンツをホストし得る。ＳＣＨＦは、セキュリティポリシ施行エンティティとしても機能し、アクセス制御チェックを行い得る。ある場合、ＳＣＨＦは、コンテンツに関連付けられるセキュリティ動作（例えば、セキュリティポリシ施行）を行うために必要な能力（例えば、機能性、計算リソース）を有していなければならず、セキュアな様式でコンテンツをホストするリソースを有していなければならない。セキュリティ有効化機能（ＳＥＦ）は、コンテンツを保護するため、および／またはコンテンツにアクセスするための証明書を提供し得る。ＳＥＦは、コンテンツへのアクセスをクライアントに提供するために、信頼される第三者（ＴＴＰ）等の信頼される仲介者として動作し得る。ＳＥＦは、対称証明書ならびに公開キー証明書をプロビジョニングすることが可能であり得る。それは、外部証明機関（ＣＡ）に対して機能し得るか、またはそれにインターフェースをとり得る。

【００４０】

図６に示されるように、コンテンツセキュリティを提供することに関与するプロセスは、以下で識別される種々のプロセスに分類され得る。例えば、例示的コンテンツ作成プロセス（ＣＣＰ）の一部として、コンテンツのサブコンポーネントが、ある関係および構造を有する複合コンテンツを作成するために使用される。例示的コンテンツは、１つ以上の属性／値ペアで構成され得、属性／値ペアの各々は、サブコンポーネントである。例示的セキュリティパラメータ決定プロセス（ＳＰＤＰ）の一部として、セキュリティパラメータの正しい組が、「静止している」特定のコンテンツのために決定される。加えて、コンテンツのライフサイクル管理も決定される。セキュアホスティング請求プロセス（ＳＨＲＰ）が、ＣＣＳＤＦによって、またはＳＣＨＦによって開始され得る。一例では、請求の一部として、ＣＣＳＤＦは、ＳＣＨＦ上のコンテンツのセキュアなホスティングを要求する。ＳＣＨＦは、ゼロホップ（同一のプラットフォーム上でホストされる）であり得るか、ＣＣＳＤＦから１ホップ離れ得るか（概して、好ましいアプローチ）、またはＣＣＳＤＦから複数のホップで離れ得る（２またはそれを上回るホップ離れて）。ＣＣＦ、ＳＤＦ、およびＳＣＨＦが、同一のノード／エンティティ上で実装される例では、ステップ０、１、および２は、ノード／エンティティ内で内部に実施され得、したがって、機能間の通信は、プロセス内通信を使用して実施され得る。

【００４１】

例示的実施形態では、証明書請求および登録プロセス（ＣＲＲＰ）は、証明書請求プロセス（ＣＱＰ）と、証明書登録プロセス（ＣＧＰ）とを含み得る。ＣＲＰ中、ＳＣＨＦは、コンテンツのセキュアな記憶のための適切な証明書のプロビジョニングを要求し得る。このプロセスは、多くの場合、ＳＣＨＦがそのコンテンツのための適切な証明書を生成するために十分であり得るので、随意であり得る。クライアント特定のコンテンツが保護されるべき場合において、次いで、ＣＣＳＤＦ／ＳＤＰは、クライアントの証明書を要求し得る。ＣＧＰの一部として、コンテンツを保護するために使用される証明書の組が、ＳＥＦを用いて発行され得る。拡張性の理由により、証明書は、複数のＳＥＦにおいて発行され得る。ある場合、ＣＣＳＤＦがそれ自身で証明書を生成することができる場合、ＣＣＳＤＦは、ＣＧＰのみを行い得る。しかしながら、他の場合、ＣＣＳＤＦが適切な証明書を生成することができない場合、完全ＣＲＲＰプロセスを行う必要があろう。例示的セキュアホスティングプロセス（ＳＨＰ）の一部として、ＳＣＨＦは、ＣＣＳＤＦからのＳＨＲＰメッセージに基づいて、コンテンツのホスティングを行い得る。ここでの仮定は、コンテンツが保護されるようにＣＣＳＤＦが必要な暗号動作を行い得ることであり、ＣＣＳＤＦからの命令に基づいて、ＳＣＨＦは、コンテンツを適切にホストする。代替として、ＳＣＨＦは、コンテンツをセキュアにホストするために、適切な暗号動作を行う必要があり得る。実施される暗号動作のタイプは、コンテンツに関連付けられるセキュリティパラメータに基づき得る。ＳＨＲＰメッセージに基づいて、ＳＣＨＦは、コンテンツに関連付けられるセキュリティプロパティを更新し、随意に、コンテンツを削除するために、またはそれをアクセス不可能にするためにトリガされる必要があろう適切なライフサイクル管理プロセスを作成し得る。

【００４２】

ここで第三者証明書請求プロセス（ＴＰＣＲＰ）を参照すると、第三者（例えば、クライアント）がリソースにアクセスするために、ＳＥＦは、クライアントが、コンテンツを解読すること、および／またはコンテンツの完全性／真正性を検証することができるように、クライアントを承認し、クライアントに必要な証明書を提供する必要があり得る。ＴＰＣＲＰは、認証および承認、ならびに第三者（例えば、クライアント）への証明書配布を伴い得る。例示的コンテンツ読み出しプロセス（ＣＲＰ）中、クライアントは、コンテンツにアクセスするための要求を開始する。クライアントは、事前構成された情報からＳＣＨＦに関する情報を取得し得るか、または、情報は、ＤＮＳ－ＳＤもしくはＲＤを使用して動的に発見され得る。コンテンツ処理（ＣＰ）の例中、コンテンツにアクセスすることを希望するクライアントは、コンテンツの真正性および／または完全性を検証することを所望し得る。加えて、クライアントは、コンテンツ構造およびコンテンツに関連付けら

れる属性を検証することも所望し得る。コンテンツが機密性のために保護される場合において、コンテンツは、暗号化されたコンテンツとして送信され得、コンテンツは、ＳＣＨＦによってコンテンツをクライアントに送信する前に解読され得る。コンテンツがＳＣＨＦによって解読される必要があるかどうかの決定は、コンテンツに関連付けられるポリシおよびセキュリティ要件に基づき得る。

【００４３】

例示的コンテンツライフサイクル管理プロセス（ＣＬＭＰ）の一部として、ＣＣＳＤＦは、随意に、特定のコンテンツのためのライフサイクル管理を更新するために明示的ＣＬＭＰメッセージを送信し得る。このプロセス／メッセージングは、ＣＣＳＤＦがＳＨＲＰの一部として明示的ライフサイクル管理要件を通信した場合、省略され得る。それは、ＳＣＨＦにおけるローカルポリシがコンテンツのライフサイクル管理を扱うように事前構成されている場合にも省略され得る。ＳＣＨＦにおけるポリシは、コンテンツを削除するか、または任意のエンティティに利用不可能にする等、コンテンツに関連付けられるセキュリティプロパティを更新するために実施される必要があろう必要な動作を決定し得る。

【００４４】

コンテンツ作成プロセス（ＣＣＰ）が、ここで詳細に議論されるであろう。このプロセスの一部として、データコレクタ（例えば、センサデータ）によって収集される未加工データが、ある構造において記憶されるコンテンツを作成するために、ＣＣＦによって使用され得る。ＣＣＰの一部として、例示的実施形態によると、コンテンツのサブコンポーネントが、ある関係および構造を有する複合コンテンツを作成するために使用される。例示的コンテンツは、１つ以上の属性／値ペアで構成され得、属性／値ペアの各々は、サブコンポーネントである。上記のように、便宜上、データまたは情報もしくはコンテンツは、概して、限定ではないが、コンテンツと称され得る。コンテンツは、大域的に一意のリソース識別子によって識別され得るか、またはローカルで識別可能であり得る。コンテンツは、サブコンポーネント間にある関係構造（例えば、階層またはフラットウェブ）を有する１つ以上のサブコンテンツ（コンポーネント）で構成され得る。そのサブコンポーネントまたは属性を伴う例示的コンテンツが、図７で描写されている。図７は、コンテンツ識別子「ＡＢＣ」を有し、３つのコンポーネント、すなわち、コンポーネント－Ａ、コンポーネント－Ｂ、およびコンポーネント－Ｃで構成されるコンテンツを描写する。コンポーネント－Ｃは、再度、２つのサブコンポーネント、すなわち、サブコンポーネント－Ｘ、サブコンポーネント－Ｙで構成される。

【００４５】

ここで、例示的実施形態による、セキュリティパラメータ決定プロセス（ＳＰＤＰ）を参照すると、ＳＤＰＤ中、ＣＳＳＤＦの一部であり得るＳＤＦが、「静止している」コンテンツを保護するために要求される適切なセキュリティ要件およびパラメータを決定する。前述のように、ＣＣＳＤＦがそれ自身で証明書を生成することができるいくつかの場合、次いで、ＣＣＳＤＦは、ＣＧＰのみを行い得る。代替として、ＣＣＳＤＦが適切な証明書を生成することができない場合、それは、完全ＣＲＲＰプロセスの両方を行う必要があり得る。決定プロセスの一部として、ＣＣＳＤＦは、例えば、限定ではないが、以下を決定し得る。

- コンテンツが盗聴者から保護される必要があるかどうか（機密性／プライバシ保護）
  - 保護のレベル：アルゴリズム強度、証明書タイプ／サイズ
- コンテンツの無承認修正からの保護－完全性保護
  - 保護のレベル：アルゴリズム強度、ダイジェスト／署名の長さ
- 保護機構を更新する能力
- 証明書のセキュアな記憶／セキュアな動作環境の要件
- コンテンツに関連付けられる存続期間セキュリティ管理

【００４６】

【表１】

コンテンツId／サブ	機密性保護		完全性保護		セキュアな環境	ライフサイクル／セキュリティ保護の更新
	アルゴリズム強度	証明書強度	アルゴリズム強度	認証コード／署名の長さ		
XYZ／いいえ	高	＞200ビット	中	MAC＞＝256	いいえ	10年／3年
ABC／はい	高	＞200ビット	高	DS＞＝4096	はい	5年／1年
MNO／いいえ	低	＞120ビット	中	MAC＞＝256	いいえ	15年／いいえ

【００４７】

上記の表１において、コンテンツＸＹＺ（ＸＹＺ－Ｉｄによって識別される）、ＡＢＣ、およびＭＮＯに関連付けられる高レベルセキュリティパラメータの例が図示されている。コンテンツの各々は、それらの対応するセキュリティパラメータに関連付けられる。例として、示されるように、コンテンツＸＹＺは、「高」の機密性要件を有し、使用されるキーサイズが少なくとも２００ビットであることを要求する。証明書強度は、暗号化のタイプ（例えば、対称キー）に基づき得、したがって、他の暗号化タイプ（例えば、公開キー）のための同等キーサイズが、適切に使用され得る。ある場合、コンテンツが制約されたエンティティ上でホストされ得ることを考慮して、証明書強度のための最大サイズ限界があり得る。示されるように、例示的完全性保護アルゴリズムは、「中」であり、＞＝２５６ビットのＭＡＣ長を有する。コンテンツは、セキュアな環境を利用する必要がない。ライフサイクル管理に関して、図示される例によると、コンテンツは、１０年の期間後にパージされ得るか、またはアクセス不可能にされ得、セキュリティ保護は、３年毎に更新され得る。表は、コンテンツ保護のための可能な高レベルセキュリティ要件の例を実証するにすぎない。追加の要件は、特定の実装に適するために追加または除去され得ることが理解されるであろう。例えば、ライフサイクル管理に関連付けられる要件は、あるタイプに対してないこともある。

【００４８】

ＳＰＤＰは、例えば、ＣＣＦ上のローカルポリシまたはコンテンツ所有者／サービスプロバイダによってプロビジョニングされるポリシに基づいて、ＳＤＦにおけるプロセスによってトリガされ得る。ＳＰＤＰをトリガするために使用される機構は、あるコンテンツにたいする要求に基づいて、先手型または後手型であり得る。ＳＰＤＰは、国家安全関連事項または商業的価値を有する極秘データ／コンテンツを保護するための最良実践に基づいてプロビジョニングもしくは実装されているセキュリティ特定のポリシを使用して行われ得る。ＳＰＤＰによって使用されるポリシの簡略化された例が、表２において以下で挙げられるが、ポリシは、所望に応じて変動し得ることが理解されるであろう。

【００４９】

【表２】

セキュリティ値	機密性	完全性	セキュアな環境	ライフサイクル管理
低	低	中	いいえ	いいえ
中	中	高	いいえ	はい
高	高	高	はい	はい

【００５０】
ある場合、コンテンツは、各々がそれ自身の識別を有するサブコンポーネントから成り得るか、または、コンテンツに関連付けられる属性／値があり得る。各サブコンポーネントまたは属性／値は、それ自身の対応するセキュリティ要件を有し得る。全てのサブコンポーネント（例えば、属性／値）が個々に保護されるので、コンテンツ全体が、保護（例えば、完全性保護）され得る。
【００５１】
例示的実施形態では、ＳＤＦは、要件に基づいて、適切な暗号パラメータ（ＣｒｙｐｔｏＰａｒａｍｓ）を決定する。ＣＳＳＤＦがコンテンツをホストする場合、ＣＣＳＤＦは、コンテンツのための要求されるセキュリティ値を導出し得る。コンテンツＸＹＺに関連付けられるＣｒｙｐｔｏＰａｒａｍｓの例が、図８で描写されている。図８は、暗号化／暗号解読アルゴリズム、すなわち、２５６ビットキーを使用するＡＥＳを説明する。このキーは、キー導出関数（ＫＤＦ）を使用して生成され得る。例示的ＫＤＦは、Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ　Ｋｅｙ（ＣＫ）＝ＫＤＦ（ＫｅｙＧｅｎＫｅｙ，　”ＣｏｎｔｅｎｔＩｄ”｜｜”ＲａｎｄｏｍＶａｌｕｅ”｜｜”ＣｏｎｆｉｄｅｎｔｉａｌｉｔｙＫｅｙＧｅｎ”）という形態であり得る。
【００５２】
例えば、Ｋｅｙｅｄ－Ｈａｓｈ－Ｍｅｓｓａｇｅ－Ａｕｔｈｅｎｔｉｃａｔｉｏｎ－Ｃｏｄｅ（ＨＭＡＣ－ＳＨＡ）等のＫＤＦが、ＣＫを導出するために使用され得る。入力パラメータは、本明細書ではＫｅｙＧｅｎＫｅｙと称され得る、他のキーを生成するためにＣＳＳＤＦによって使用されるキーを伴い得る。加えて、入力パラメータは、ＣＣＳＤＦのコンテキスト内で一意であることが仮定され得るＣｏｎｔｅｎｔＩｄと、ＳＤＦによって生成される乱数値と、文字列「ＣｏｎｆｉｄｅｎｔｉａｌｉｔｙＫｅｙＧｅｎ」とを含み得る。上記のように、ＣＫの生成は、例証目的のために例として使用されるにすぎず、入力パラメータは、衝突の可能な低減のために所望に応じて変動させられ得ることが理解されるであろう。
【００５３】
依然として図８を参照すると、選択される完全性／認証アルゴリズムは、関連付けられるＩｎｔｅｇｒｉｔｙＫｅｙ（ＩＫ）を用いたＨＭＡＣ－ＳＨＡ－２５６アルゴリズムである。ＩＫは、ＣＫに類似する手段を使用するが、入力パラメータ上の変動を伴って導出され得る。例として、新しいＲａｎｄｏｍＶａｌｕｅが、生成され、「ＣｏｎｆｉｄｅｎｔｉａｌｔｉｙＫｅｙＧｅｎ」が、「ＩｎｔｅｇｒｉｔｙＫｅｙＧｅｎ」文字列によって置換され得る。
【００５４】
例示的実施形態では、コンテンツは、特定のクライアントのみがコンテンツにアクセスすることができるように保護される。加えて、クライアントは、特定のＳＤＦがコンテンツを作成したことと、非常に高い確実度で、それがいかなる他のエンティティによっても修正されなかったこととを検証することが可能であり得る。例えば、クライアント特定のコンテンツ保護機構が使用される場合、クライアントの公開キーを取得するためにクライアントのデジタル証明を使用し、コンテンツを暗号化するためにその公開キーを使用することが好ましくあり得る。クライアント特定のＣｒｙｐｔｏＰａｒａｍｓの例が、図９で

描写されている。示されるように、機密性アルゴリズムは、Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｄｌｅｍａｎ（ＲＳＡ）公開キーアルゴリズムであることが決定され、Ｋｅｙは、クライアント１に関連付けられるデジタル証明から取得され得るクライアント１の公開キーであることが決定される。クライアント１のデジタル証明を取得するために、例えば、ＳＤＦがまだデジタル証明を処理していない場合、以下で説明される証明書請求プロセスが実施され得る。例によると、完全性（デジタル署名）アルゴリズムは、ＳＨＡ－２５６ダイジェストを使用するＲＳＡであることが決定され、使用されるべき署名キー（ＩＫ）は、ＳＤＦのデジタル証明に関連付けられるＳＤＦの秘密キーであり、それは、好ましくは、セキュアな記憶装置の中に記憶される。ＣｒｙｐｔｏＰａｒａｍｓが作成されたときの時間／日付、ＣｏｎｔｅｎｔＩｄ、および／またはコンテンツに関連付けられるメタデータ等のノンスが、ノンスとして使用され得る。

【００５５】

例示的シナリオでは、クライアントは、証明書の組を共有するクライアントのグループであり得る。機密性のために公開キーイング機構を使用することは、各エンティティが秘密キーを共有する必要があり得、それは、セキュリティを低下させるので、そのようなシナリオではうまく機能しないこともある。このシナリオでは、代わりに、対称キー機構が、好ましくは、機密性のために使用され得る。代替として、完全性／認証のために、公開キーイング機構が、好ましいアプローチであり得る。したがって、拡張性のために、および最適性能を維持するために、機密性アルゴリズムが、対称キーイング機構に基づき得、公開キーイング機構が、一実施形態によると、コンテンツ／コンテンツジェネレータの完全性／真正性を提供するために使用され得る。ある場合、コンテンツの機密性が、無視され得る一方で、コンテンツ／コンテンツジェネレータの完全性／真正性は、検証される。

【００５６】

例えば、コンテンツがサブコンポーネントで構成される場合、サブコンポーネントの各々は、それ自身のセキュリティパラメータと、それに関連付けられる対応するＣｒｙｐｔｏＰａｒａｍｓとを有し得る。例えば、属性／値ペアで構成され得るコンテンツおよびサブコンポーネントは、それら自身の一意のＣｒｙｐｔｏＰａｒａｍｓを有し得る。各特定の属性／値ペアを保護するために要求される計算リソースの金額は、高価であり得、多くの場合、別個に保護されたその個々のコンポーネントを有するのではなく、コンポーネントが全体として保護され得る。本明細書に説明される機構は、グローバルコンテンツの観点から、またはより粒度の細かい属性／値ペアの観点から、コンテンツの保護を行うために使用され得、コンテンツに関連付けられるサブコンポーネントの各々は、様々なセキュリティ要件を有し得る。ｃｒｙｐｔｏＰａｒａｍｓが、アルゴリズムおよびキーのためのＪＷＡならびにＪＷＫを用いて、ＪＳＯＮ表記法を使用して表され得ることが理解されるであろう。

【００５７】

ここで、例示的セキュアホスティング請求プロセス（ＳＨＲＰ）を参照すると、ＳＣＨＦは、ＣＣＳＤＦと同一のエンティティ（ノード）上に位置し得、したがって、ＳＨＲＰメッセージングは、そのような場合、内部で行われ得る。ＣＣＳＤＦおよびＳＣＨＦが異なるエンティティ上に位置するある場合、ＣＣＳＤＦは、１つ以上のＳＣＨＦと共にＳＨＲＰを開始し得る。単一のＳＣＨＦを用いたコンテンツのホスティングが、本明細書に説明されるが、しかしながら、類似機構が、複数のＳＣＨＦを用いたホスティングに使用され得る。ＳＨＲＰは、以下のサブプロセス、例えば、限定ではないが、セキュリティ値の計算、適切なＳＣＨＦの発見、およびメッセージングプロセスから成り得る。

【００５８】

セキュリティ値を計算することに関して、必要なセキュリティ値が、ＳＤＦにおけるローカルポリシ、および／または、上で説明されるＳＰＤＰの一部として決定されたＣｒｙｐｔｏＰａｒａｍｓに基づいて、計算され得る。ある場合、セキュリティ値の計算は、信頼される第三者（ＴＴＰ）またはＳＣＨＦにオフロードされ得る。ＳＤＦをホストするエンティティにおけるローカルポリシは、サービスプロバイダポリシ、ＳＤＦをホストする

エンティティの能力（例えば、制約されたデバイス、正しいファームウェア／ソフトウェアの利用可能性等）、およびコンテンツタイプの組み合わせに基づき得る。保護された値（ＰＶ）という用語は、計算されたセキュリティ値を表すために本明細書で使用される。例示的な計算されたＰＶは、暗号化されたコンテンツ（ＥＣ）および認証タグ（ＡＴ）を含む。ＥＣに関して、コンテンツ全体が、暗号化され得るか、またはサブコンポーネントもしくは属性／値ペアが、サブコンポーネントの各々に関連付けられるＣｒｙｐｔｏＰａｒａｍｓに基づいて暗号化され得る。ある場合、属性／値ペアの「値」コンポーネントのみが暗号化される。ＡＴは、完全性値であり、それは、その特定のコンテンツのためのＣｒｙｐｔｏＰａｒａｍｓの中で規定される完全性パラメータを使用して、コンテンツに対して計算される。前述のように、コンテンツの各サブコンポーネントは、それ自身の一意の計算されたＡＴを有し得る。

【００５９】

例示的実施形態では、ＥＣおよびＡＴが両方とも、例えば、ＡＥＳ－Ｇａｌｏｉｓモード（ＡＥＳ－ＧＣＭ）等の認証付き暗号（ＡＥＡＤ）機構を使用することによって達成される。ＡＥＡＤの使用は、ＣｒｙｐｔｏＰａｒａｍｓ内で明示的に規定され得るか、またはＳＣＨＦによって推測され得る。ＥＣおよびＡＴは、別個のＣＫ、ＩＫを使用して、または機密性ならびに完全性の両方のための単一のキーを有して生成され得る。また、ＡＥＳ－ＧＣＭの場合、ＡＴは、「追加の認証されたデータ」であり得る。ＥＣおよびＡＴは、ＪＷＥおよびＪＷＳをそれぞれ用いて、ＪＳＯＮ表記法を使用して表され得る。

【００６０】

例示的実施形態では、ＣＣＳＤＦは、そのコンテンツをホストするための正しいＳＣＨＦを決定するために、発見プロセスを行い得る。発見プロセスは、信頼されるエンティティにクエリを行うこと、または利用可能なサービス（例えば、ＤＮＳ－ＳＤ、ＲＤ）のアクティブなリスティングを行う他のエンティティにクエリを行うことを伴い得る。ある場合、ＣＣＳＤＦは、ローカルホスティングエンティティに発見プロセスをオフロードし得、ローカルホスティングエンティティは、次いで、適切なＳＣＨＦを決定する。クエリへの応答として、ＣＣＳＤＦは、ＳＣＨＦ、またはセキュリティパラメータに最良に適合するある基準に基づいて順序付けられるＳＣＨＦのリストに関する場所情報（例えば、ＵＲＩ）を提供され得る。高度に信頼できるＳＣＨＦが利用可能ではない場合において、ＰＶの計算を伴う暗号動作は、ＣＣＳＤＦによって行われ得る。高度に信頼できるＳＣＨＦが発見される場合、ＰＶの計算は、ＳＣＨＦにオフロードされ得る。

【００６１】

ここで図１０を参照すると、ネットワーク１０００は、例によると、ＣＣＳＤＦ１００２と、ＣＣＳＤＦ１００２と共にセキュアホスティング請求（ＳＨＲ）メッセージングを行うＳＣＨＦ１００４とを含む。例示的ネットワーク１０００は、開示される主題の説明を促進するように簡略化され、本開示の範囲を限定することを意図していないことが理解されるであろう。他のデバイス、システム、および構成が、ネットワーク１０００等のネットワークに加えて、またはその代わりに、本明細書に開示される実施形態を実装するために使用され得、全てのそのような実施形態は、本開示の範囲内として考慮される。ＣＣＳＤＦ１００２によって受信される応答のタイプに基づいて、ＣＣＳＤＦ１００２は、適切なメッセージと、コンテンツがＳＣＨＦ１００４上でホストされるために要求され得るパラメータの正しい組の生成とを作成し得る。ＳＣＨＦが低信頼性エンティティである場合、図１０で描写されるメッセージが行われ得る。

【００６２】

０では、図示される実施形態によると、ＣＣＳＤＦ１００２は、コンテンツの適切なＰＶ、すなわち、ＥＣおよび関連付けられるＡＴを生成する。１では、ＣＣＳＤＦ１００２と選択されたＳＣＨＦ１００４とは、互いに相互認証し、セキュアな通信チャネルを確立し得る。２では、ＣＣＳＤＦ１００２は、ＥＣ、関連付けられるＡＴ、およびＣｒｙｐｔｏＰａｒａｍｓを含むセキュアホスティング（ＳＨ）要求メッセージをＳＣＨＦ１００４に送信する。３では、図示される例によると、ＳＣＨＦ１００４は、ＥＣ、ＡＴ、および

ＣｒｙｐｔｏＰａｒａｍｓをホストし、それらを保護コンテンツ記憶部（ＰＣＳ）内に記憶する。ＳＣＨＦ１００４は、随意に、以下でさらに説明される、ＳＥＦを用いてＣｏｎｔｅｎｔＩｄとともにＣｒｙｐｔｏＰａｒａｍｓをポストし得る。４では、ＥＣおよびＰＶがホストされると、一意のｈｏｓｔｅｄ－ｉｄ（Ｈ－Ｉｄ）を随意に含む成功メッセージがＣＣＳＤＦ１００２に送信され、Ｈ－Ｉｄは、ＥＣならびにＡＴおよびＣｒｙｐｔｏＰａｒａｍｓの場所へのＵＲＩであり得る。ＥＣは、１つの物理エンティティ上でホストされ得、ＣｒｙｐｔｏＰａｒａｍｓおよびＡＴは、異なる信頼されるエンティティ上に位置し得る。

【００６３】

ここで図１１を参照すると、ネットワーク１１００は、示されるように、ＣＣＳＤＦ１１０２と、信頼されるエンティティであるＳＣＨＦ１００４とを含み、ＣＣＳＤＦ１１０２は、ＣＳＤＦ１１０２の代わりに暗号動作を行うために信頼されるＳＣＨＦ１１０４に依存し得る。例によると、ＣＣＳＤＦ１１０２は、コンテンツおよび関連付けられるＣｒｙｐｔｏＰａｒａｍｓをＳＣＨＦ１１０４に提供するのみである。０では、図示される例によると、ＣＣＳＤＦ１１０２とＳＣＨＦ１１０４とは、互いに相互認証し、互いにセキュアな通信チャネルを確立し得る。１では、ＣＣＳＤＦ１００２は、関連付けられるＣｒｙｐｔｏＰａｒａｍｓとともに（保護されていない）コンテンツを含むＳＨ要求メッセージを送信する。加えて、サブコンポーネントが個々に完全性保護されなければならないことを示す、Ｓｕｂ＿Ｉ－ｆｌａｇも送信される。ＳＣＨＦ１１０４が信頼されるので、さらに、メッセージがセキュアな通信チャネルを通して送信されるので、コンテンツおよびパラメータは、「移動中」、保護される。ＳＣＨＦ１１０４がＣＣＳＤＦ１１０２からいくつかのホップ離れて位置する場合、およびメッセージングペイロードが信頼できないエンティティを通してトラバースする場合、コンテンツおよびＣｒｙｐｔｏＰａｒａｍｓは、エンドツーエンドセキュリティ機構を使用して保護されなければならない。２では、ＳＣＨＦ１１０４は、ＥＣおよび関連付けられるＡＴを導出するために、コンテンツに対してＣｒｙｐｔｏＰａｒａｍｓを使用する。Ｓｕｂ＿Ｉ－ｆｌａｇ＝１であるので、各コンテンツの個々のサブコンポーネントも、完全性保護され、適切なＡＴ値が、計算される。ＳＣＨＦ１１０４は、使用される必要がある証明書の正しい組を取得するために、ＳＥＦのサービスを使用し得る。これは、保護されるべきコンテンツがクライアント特定のコンテンツである場合、特に必要であり得る。ＳＣＨＦ１１０４は、その上にＥＣおよびＡＴを記憶し得る。例示的セキュアホスティングプロセスの詳細が、以下で説明される。３では、ＳＣＨＦ１１０４は、「成功」を含むＳＨ応答をＣＣＳＤＦ１１０２に送信する。ＳＣＨＦ１１０４は、随意に、ホスティング識別子も送信し得る。

【００６４】

したがって、図１０および１１を参照すると、ノード（例えば、ＣＣＳＤＦ）は、プロセッサと、メモリと、通信回路とを含むことができる。ノードは、その通信回路を介してネットワークに接続され得、ノードはさらに、ノードのプロセッサによって実行されると、ノードに、１つ以上のセキュリティ要件に基づいて１つ以上の暗号パラメータを決定させる、ノードのメモリ内に記憶されたコンピュータ実行可能命令を備えている。ノードはまた、セキュアホスティング要求メッセージをコンテンツホスティング機能（ＣＨＦ）に送信し得る。セキュアホスティング要求メッセージは、コンテンツホスティング機能が１つ以上の暗号パラメータを使用してコンテンツをセキュアに記憶することができるように、１つ以上の暗号パラメータと、それに関連付けられるコンテンツとを含み得る。１つ以上の暗号パラメータに基づいて、ノードは、コンテンツが機密であるようにコンテンツを暗号化し得る。代替として、コンテンツは、サブコンポーネントから成り得、ノードは、１つ以上の暗号パラメータに基づいて、各サブコンポーネントが機密であるように、サブコンポーネントの各々を暗号化し得る。なおも代替として、コンテンツは、属性および値のペアから成り得、ノードは、１つ以上の暗号パラメータに基づいて、各値が機密であるように、値の各々を暗号化し得る。ノードはまた、コンテンツが完全性保護されるように、コンテンツに関連付けられる認証タグ（ＡＴ）を計算し得る。代替として、または加え

て、コンテンツは、サブコンポーネントから成り得、ノードは、サブコンポーネントの各々が完全性保護されるように、サブコンポーネントの各々に関連付けられるそれぞれの認証タグを計算し得る。

【００６５】

コンテンツがローカルで、またはプロキシ上でホストされることができるかどうかを決定するために、ＣＣＳＤＦによって行われ得る例示的機構が、図１２に図示されている。図１２を参照して、図示される例によると、１では、ＣＣＳＤＦは、コンテンツに関連付けられたセキュリティ要件の査定を行う。セキュリティ要件は、コンテンツが、コンテンツを生成したエンティティまたはドメインの外に取り出されることを許されないことを要求し得る（例えば、異なる郡、州、国内等のコンテンツの記憶の制約）。それは、コンテンツがホストされ得る地理的場所に対する制約を有し得る。あるセキュリティ機能を果たす効率および能力等の他のセキュリティ査定も、実施され得る。２では、ＣＣＳＤＦは、コンテンツがプロキシ上でホストされることができるかどうかの査定を行う。３では、コンテンツがプロキシ上でホストされることができる場合、ＣＣＳＤＦは、コンテンツをホストすることが可能であり得る潜在的な１つ以上のＳＣＨＦのリストを取得し得る。ＣＣＳＤＦは、ある優先順位で順序付けられた潜在的ＳＣＨＦのリストで構成されているか、またはＴＴＰからリストを取得し得る。ある場合、ＣＣＳＤＦは、発見サービス（例えば、ＤＮＳ－ＳＤまたはｏｎｅＭ２Ｍ発見サービス）の手段を使用することによって、より動的な様式でＳＣＨＦを発見し得る。４では、ＣＣＳＤＦは、ＳＣＦＨがコンテンツの要件を少なくとも満たすかどうかを決定する。５では、図示される例によると、ＳＣＦＨがコンテンツの要件を満たさない場合、ＳＤＦは、コンテンツがＣＣＳＤＦ上でローカルにホストされることができるかどうかを決定する。６では、コンテンツがローカルにホストされることができる場合、それは、ＳＨＰプロセスをトリガする。そうでなければ、ＣＣＳＤＦが必要なセキュリティ能力（アプリケーション、ソフトウェア、ファームウェア、ハードウェア等）を保有しない場合、セキュアホスティングプロセスが中断され得る。代替として、新しい発見プロセスが行われ得るか、またはより低いセキュリティ要件を有する修正されたコンテンツが、更新された発見プロセスに基づいてホストされ得る。

【００６６】

ここでセキュアホスティングプロセス（ＳＨＰ）を参照して、例示的実施形態によると、コンテンツは、セキュリティ要件またはコンテンツに関連付けられるセキュリティプロファイルを満たす様式でハンドリングされる。セキュアホスティングは、データにアクセスするための強力な認証機構を提供すること、ロバストな承認機構を提供すること、完全性をデータに提供すること、および／またはデータの機密性を提供することを含み得る。セキュアな様式でデータをホストする能力は、セキュア要素（ＳＥ）または信頼される実行環境（ＴＥＥ）の使用を伴い得る。ある場合、関与するオーバーヘッド（計算、メモリ、バッテリ）は、制約されたデバイスのために大きすぎることもある。暗号証明書（例えば、キー／証明／識別子）および／または極秘暗号機能が、ＳＥもしくはＴＥＥを伴わずに実施され得る。エンティティがセキュアな様式でデータをホストすることができない場合、そのデータを記憶するためにプロキシを使用し得る。Ｒｏｏｔｓ－ｏｆ－Ｔｒｕｓｔ（ＲｏＴ）の使用が、概して、役立つが、本開示は、ハードウェアまたはソフトウェアベースのＲｏＴの存在に関して、いかなる仮定も行わない。

【００６７】

上で説明されるように、ＳＣＨＦは、ＣＣＳＤＦから１ホップ離れて常駐し得るか、またはＣＣＳＤＦから複数のホップ離れ得る。ホップの数は、サービス層ホップの数を指す。ＣＣＳＤＦは、ＳＣＨＦとの直接信頼関係を有することも、有しないこともあるが、確立された信頼階層を基礎とすること、または共通の信頼のルートを使用して新しい信頼関係を作成することが可能であり得る。ＣＣＳＤＦとＳＣＨＦとの間の接続をセキュアにするためのエンドツーエンドアプローチが好ましくあり得るが、エンドツーエンドセキュリティ機構は、利用可能ではなく、ホップ毎のセキュリティが使用され得る。

【００６８】

例示的実施形態では、エンティティは、データに関連付けられる要件に基づいて、エンティティがホストされるデバイス内でローカルにデータを記憶することを決定し得る。例えば、エンティティが、ホストエンティティがセキュアな様式でデータをホストできることを決定した場合、それは、データが完全性保護されるように、および／または機密性のために保護されるように、データに対して必要な暗号動作を行う。適切な暗号アルゴリズムおよび証明書が、データを保護するために使用され得る。機密性保護のための暗号値の例が、以下の表３で提供されている。

【００６９】

【表３】

セキュリティレベル－機密性	アルゴリズム	キー長	記憶要件
低	3－DES	168ビット	なし
中	AES	192ビット	FDE
高	AES	25ビット	ファイルベース
臨界	RSA	4096	TEE／SE*

【００７０】

ＰＣＳ内に記憶された保護コンテンツの例が、図１３で描写されている。図１３は、Ａ、Ｂ、およびＣを有する、識別子ＡＢＣを伴うコンテンツを描写し、コンポーネントＣは、サブコンポーネントＸおよびＹで構成される。ＣｒｙｐｔｏＰａｒａｍｓおよび保護される必要があるコンポーネントの指示に基づいて、ＣＣＳＤＦは、コンテンツに関連付けられるＥＣおよびＡＴを計算する。コンポーネントＡおよびＢは、一意であり得る証明書を使用して暗号化される。しかしながら、コンポーネントＣ自体が、いかなるデータも含まないこともあり、保護されないこともある一方で、サブコンポーネントＸ、Ｙは、暗号化される。コンポーネントＡおよびＢのため完全性データ（ＡＴ）、ならび構造およびコンポーネントＣ全体のための完全性データ（ＡＴ）は、（Ｃｏｍｐｏｎｅｎｔ－Ｃ－ＡＴを使用して）保護され、個々のサブコンポーネントＸおよびＹは、保護される。ＡＢＣ－ＡＴは、コンテンツ、「ＡＢＣ」、およびサブコンポーネント、ならびにコンテンツ内のそれらの関係／構造を完全性保護するために計算される。

【００７１】

ある場合、保護機構は、煩雑で計算的に高価であり、したがって、制約されたＣＣＳＤＦのために好適ではないこともある。したがって、動作のうちのいくつかは、信頼されるＳＣＨＦ上にオフロードされ得る。ここで説明される、粒度の細いレベルでコンテンツを保護するための機構は、ロバストなセキュリティ機構を提供しながら、コンテンツ消費のために多くの融通性を提供する。コンテンツのサブコンポーネント（例えば、サブコンポーネント－Ｘ）にアクセスすることのみ承認されているクライアントは、その全体としてコンテンツについていかなる情報も有することなく、（例えば、Ｃｏｍｐｏｎｅｎｔ－Ｘ－ＡＴを使用して）その特定のサブコンポーネントの完全性を検証することが可能であり得る。ＣｒｙｐｔｏＰａｒａｍｓおよびコンテンツ保護の粒度の選択は、実装されている（例えば、サービスプロバイダによって決定される）ソリューションのタイプならびにプラットフォームによって決定されるＣＣＳＤＦ上のローカルポリシに基づき得る。

【００７２】

別の例示的実施形態では、ＣＣＤＳＦは、ＳＣＨＦが常駐するプロキシ上にコンテンツをホストすることを決定し得る。上で説明される発見機構は、セキュアなプロキシを発見するために使用され得る。あるシナリオでは、ＣＣＳＤＦが信頼できるプロキシに到達することが可能ではないこともあるので、制約されたＣＣＳＤＦは、完全に信頼できるプロキシ上にコンテンツをホストすることが可能ではないこともある。そのようなシナリオでは、ＣＣＳＤＦは、ＣｒｙｐｔｏＰａｒａｍｓをＳＣＨＦ（プロキシ）に提供しないこと

もあるが、代わりに、ＴＴＰ（例えば、ＳＥＦ）上に記憶されたＣｒｙｐｔｏＰａｒａｍｓへのリンクを提供し得る。例では、ＳＥＦは、適切な承認を有するエンティティにのみＣｒｙｐｔｏＰａｒａｍｓを提供する。しかしながら、プロキシがセキュアなＳＣＨＦである場合、ＣｒｙｐｔｏＰａｒａｍｓは、ＳＣＨＦにおけるセキュアな記憶装置の中に位置し得る。セキュアな様式でコンテンツを記憶するための機構は、上で説明されるプロシージャに従い得る。

【００７３】

ＣＣＳＤＦによって低信頼性ＳＣＨＦに提供され得る例示的ＣｒｙｐｔｏＰａｒａｍｓが、図１４に図示されている。証明書は、提供されないこともあるが、ＳＥＦに登録されたＣｒｅｄｅｎｔｉａｌ－Ｉｄが、提供され得る。エンティティは、エンティティが承認された後のみＳＥＦから証明書を取得することが可能であり得る。したがって、ＥＣをホストするＳＣＨＦさえも、それが証明書を保有しないのでコンテンツを暗号化することができず、それは、ＳＥＦを用いて承認されているエンティティではないこともある。

【００７４】

ここで証明書請求および登録プロセス（ＣＲＲＰ）を参照すると、ＣＲＲＰプロセスは、ＳＨＲＰとＳＨＰとの間にインターリーブされ得、ＣＣＳＤＦとＳＥＦとの間の信頼関係、またはＣＣＳＤＦもしくはＳＣＨＦにおけるクライアント証明書の利用可能性に基づいて、コンテンツをホストするために使用される機構に依存し得る。ＣＲＲＰプロセスは、セキュリティ保護プロセスを行っているエンティティに基づいて、ＣＣＳＤＦとＳＥＦとの間、またはＳＣＨＦとＳＥＦとの間で実施され得る。ＣＲＲＰは、証明書請求プロセス（ＣＲＰ）と証明書再生プロセス（ＣＧＰ）とから成る。

【００７５】

例示的ＣＲＰに関して、ＳＤＦが、それがホストされるエンティティ内でローカルに証明書（例えば、証明、キー）を生成または取得することができない場合、ＳＤＦは、ＳＥＦを用いてＣＲＰを開始し得る。あるシナリオでは、ＳＤＦは、物理的にそれにより近くあり得るＴＴＰエンティティから証明書を取得することが可能であり得る。一般的シナリオとして、ＳＤＦが、中央証明書レポジトリとしても機能し得るＳＥＦと信頼関係を有することが仮定される。図１５は、信頼されるＳＥＦと共にＣＣＳＤＦによって開始されるＣＲＰを図示するが、同一のコールフローはまた、ＣＨＦとＳＥＦとの間のＣＲＰにも適用可能であり得る。

【００７６】

１では、図示される例によると、（０における）成功した認証およびＣＣＳＤＦとＳＥＦとの間のセキュアな通信チャネルの確立後、ＳＥＦは、証明書要求（ＣＲ）メッセージを送信する。メッセージは、限定ではないが、一例として提示される、以下のパラメータを含み得る。

● Ｃｏｎｔｅｎｔ－Ｉｄ［］：コンテンツ識別子のリスト。エントリの数は、１つ以上であり得る。

● Ａｌｇｏｒｉｔｈｍ＿Ｓｔｒｅｎｇｔｈ［］：各コンテンツのために、対応するＡｌｇｏｒｉｔｈｍ＿Ｓｔｒｅｎｇｔｈ。これは、随意であり得、ＣＣＳＤＦは、それ自身における強度に基づいて適切なアルゴリズムを選択し得る。

● Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅ＿Ｌｅｎｇｔｈ＿Ｌｉｆｅｔｉｍｅ［］：各コンテンツのために、対応する証明書タイプ、長さ、および証明書の有効性の持続時間が、提供される。コンテンツのＣｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅが、「証明」であり得る一方で、別のタイプに対して、それは、「対称キー」を要求し得る。「対称キー」のための証明書の長さが、（例えば、６４／１２８／２５６ビット）であり得る一方で、Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅ＝「証明」に対して、供給される証明書の長さは、使用されるアルゴリズムに依存する（例えば、ＲＳＡ公開キーが、２０４８／４０９６ビットであり得る一方で、ＥＣＣに対して、それは、２２４／２５６ビットであり得る）。存続期間値は、証明書が有効である持続時間であり、類似ＣＲプロセスまたは更新プロセスが、実施される必要があり得る。証明書の存続期間は、表１に説明される「セキュリティ保護を更新する」

値に基づき得る。
● Ｐｕｂｌｉｃ＿Ｋｅｙ［］：コンテンツに関連付けられる公開キーのリスト。そのＣｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅ＝「対称キー」であるコンテンツのためのＰｕｂｌｉｃ＿Ｋｅｙエントリは、空であり得ることに留意されたい。Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅが「証明」である、それらのコンテンツのみ、例によると、対応する公開キーエントリが存在するであろう。
● Ｒ－ｆｌａｇ：このフラグは、これらの証明書をＳＥＦに登録することを所望することを示すために、ＣＣＳＤＦによって使用され得る。例えば、Ｒ－ｆｌａｇ＝１である場合、ＣＣＳＤＦは、ＣＲＰ、また、ＣＧＰの両方を行うことを要求している。フラグが「０」に設定される場合、証明書請求のみが行われる。
● Ｃｌｉｅｎｔ－ｓｐｅｃｉｆｉｃ：このフラグは、メッセージがクライアント特定の証明書要求であるかどうかを示す。ここでは、それは、コンテンツ特定のＣＲにすぎないことを示すために「０」に設定されている。

【００７７】
依然として図１５を参照して、図示される例によると、ＳＥＦは、要求に基づいて、証明書の正しい組を生成する。Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅ＝「対称キー」である場合において、ＫＤＦを用いた上で説明されるような類似機構が、使用され得る。ＳＥＦは、要求された「存続期間」値に対して有効であるＫｅｙＧｅｎＫｅｙを生成し得、それをＣＣＳＤＦに提供する。ＫｅｙＧｅｎＫｅｙは、次いで、ＣＤＢにおいて、その特定のコンテンツのためにＳＥＦに登録される。代替として、ＳＥＦは、ＩＫおよびＣＫの両方を生成し得、それらをコンテンツに対して登録し、証明書データベース（ＣＤＢ）の中に記憶する。Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅ＝「証明書」である場合、ＳＥＦは、ＳＥＦによって署名される証明を生成するために公開キーを使用し、証明をＣｏｎｔｅｎｔ－Ｉｄに関連付け、証明の使用を要求の一部として提供された存続期間値に限定する。コンテンツのための証明は、ＣＤＢの中にも記憶される。３では、ＳＥＦは、証明書リストを送信する。対応するアルゴリズムが選択された場合において、次いで、アルゴリズムのリストも、登録が成功したかどうかの指示を提供するフラグとともに、提供され得る。証明書リストの一部として、証明書がＫｅｙＧｅｎＫｅｙであるかどうか、ならびに証明書の有効性を示す、フラグが提供され得る。各証明書に関連付けられる一意のＣｒｅｄｅｎｔｉａｌ－Ｉｄのリストも、例によると、ＣＣＳＤＦに提供される。４では、ＣＣＳＤＦは、証明書、Ｃｒｅｄｅｎｔｉａｌ－Ｉｄ、および関連付けられる存続期間をＣＤＢの中に記憶する。証明書がＫｅｙＧｅｎＫｅｙである場合、ＣＣＳＤＦは、随意にＣＫ、ＩＫを生成し得るか、または、それは、それらを導出するようにクライアントに委ねられ得る。

【００７８】
ここで図１６を参照すると、例示的なクライアント特定のＣＲプロセスが描写されている。ＣＣＳＤＦは、例えば、これらのクライアントのみがコンテンツにアクセスできることを要求するであろう場合、クライアント特定の証明書を要求し得る。０では、セキュアな通信チャネルが、ＣＣＳＤＦおよびＳＥＦが互いに相互認証した後、ＣＣＳＤＦとＳＥＦとの間に確立される。チャネルが確立された後、１では、ＣＣＳＤＦは、それらの証明書が要求されているクライアントのリストを含むＣＲメッセージを送信する。Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅは、要求されている証明書のタイプである。Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅは、「証明」または公開キー、もしくは「対称キー」であり得る。「対称キー」ではなく、クライアントに関連付けられる「証明」または「公開キー」を要求することが好ましくあり得る。Ｃｌｉｅｎｔ－ｉｄが、複数のクライアントに関連付けられ、クライアントのグループが同一のＣｌｉｅｎｔ－ｉｄを共有することが可能であり得る。

【００７９】
２では、ＳＥＦは、要求を処理し、ＣＤＢにクエリを行い、特定のクライアントのための証明書の正しい組を取得する。Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅ＝「証明」または「公開キー」である場合、そのクライアントに関連付けられるそれらの証明書は、図示される例で描写されるように、ＣＤＢからフェッチされる。Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅ＝

「対称キー」である場合、ＳＥＦは、ＣＤＢからＣＫをフェッチするのみであり得る。ある事例では、それは、代替として、クライアントに関連付けられる、ＫｅｙＧｅｎＫｅｙをフェッチし得、ＫｅｙＧｅｎＫｅｙは、次いで、ＣＫを生成するためにＣＣＳＤＦによって使用される。３では、図示される例によると、クライアントに関連付けられる証明のみが送信される。ＳＥＦは、各々がクライアントに関連付けられる証明書のリストを送信し得る。証明書の各々は、あるタイプ（公開キー、証明、または対称キー）であり得る。クライアントのグループが同一の証明書を共有することも可能であり得る。４では、送信された証明書がＫｅｙＧｅｎＫｅｙであった場合、ＣＣＳＤＦは、それから各クライアントのためのＣＫを生成し得、ローカルＣＤＢ内に証明書を記憶する。証明書が、各クライアントに関連付けられる「公開キー」または「証明」である場合、それらは、そのままで記憶され得る。

【００８０】

簡単のために、クライアント証明書ならびにコンテンツ特定の証明書は、例によると、一般的ＣＤＢ内に記憶され得るが、それらが別個のＤＢの中に記憶され得、それらが異なる管理ドメイン内でホストされ得ることも理解されるであろう。コンテンツ特定のＣＲのために使用されるＳＥＦとクライアント特定のＣＲのために使用されるＳＥＦとは、異なり得、したがって、ＣＣＳＤＦとＳＥＦとの間の信頼関係は、異なり得る。

【００８１】

ここで図１７を参照すると、ＣＣＤＳＦは、図１７で描写されるような証明書登録プロセス（ＣＧＰ）を使用して、コンテンツに関連付けられる証明書をＳＥＦ上に登録し得る。ここで説明される類似機構は、証明書をＳＣＨＦに登録するためにＣＣＤＳＦによって使用され、または、コンテンツのプロキシに基づくホスティングが使用されるとき、証明書をＳＥＦに登録するためにＳＣＨＦによって使用され得る。例示的実施形態では、ＣＧＰは、コンテンツ特定の証明書がＳＥＦによって生成されていないときのみ要求される。証明書がＣＣＳＤＦによって、またはＳＣＨＦによって生成される場合において、証明書は、ＳＥＦに登録され得る。

【００８２】

依然として図１７を参照して、図示される例によると、１において、ＣＣＤＳＦは、セキュアな通信チャネルを使用して、ＣＧ要求メッセージをＳＥＦに送信する。上記のように、ＣＧ要求メッセージのエンドポイントは、他のＳＥＦまたはＳＣＨＦであり得る。メッセージの一部として、限定ではないが、一例として提示される、以下のパラメータが、含まれ得る。

● Ｃｏｎｔｅｎｔ－Ｉｄ［］：大域的に、またはＳＥＦおよびＣＣＳＤＦのドメイン内で一意であることが仮定されるコンテンツ識別子のリスト。追加のメッセージングが、コンテンツが登録されているドメイン内のＣｏｎｔｅｎｔ－Ｉｄの唯一性を確実にするために使用され得る。

● Ａｌｇｏｒｉｔｈｍ［］：コンテンツの各々のために、ならびに実施され得る動作のタイプに対して使用されるべきアルゴリズムのリスト。例えば、各コンテンツは、１つ以上の関連付けられるアルゴリズム（例えば、完全性保護：ＨＭＡＣ－ＳＨＡおよび機密性保護：ＡＥＳ）を有し得る。

● Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅ［］：前述のように、これは、対称キー、公開キー、または証明であり得る。

● Ｕｓａｇｅ［］：どのようにしてアルゴリズムおよび証明書が使用されるべきかについての一般的ガイドラインであり得る。殆どの場合、これは、最良の実践に基づき、ポリシによって決定付けられ得、したがって、省略され得る。

● ＡＣＰ［］：可能にされ得るか、阻止され得るか、または証明書を提供されることを制約され得るエンティティ（クライアント）のリスト。このリストは、さらに、クライアントのクラスを含み得るか、またはクライアントドメイン情報（例えば、ＦＱＤＮ）等に基づき得る。

【００８３】

２では、図示される例によると、ＳＥＦは、Ｃｏｎｔｅｎｔ－Ｉｄが一意であること、および（例えば、公開キー／証明の場合に）証明書が正しいＣｏｎｔｅｎｔ－Ｉｄに関連付けられることを検証する。正しい秘密キーの保有のサイドチャネル検証が、行われ得る。チェックが行われ、正常に検証されると、証明書は、ＣＤＢ内に記憶される。３では、ＳＥＦは、登録成功メッセージで応答し、ＳＥＦに登録された各証明書に関連付けられる一意の識別子であるＣｒｅｄｅｎｔｉａｌ－Ｉｄのリストも含む。

【００８４】

クライアントは、同一のＳＥＦまたは異なるＳＥＦと信頼関係を有し得る。クライアント証明書に関連付けられるＣＧプロセスの例示的説明図が、図１８で描写されている。１では、図示される例によると、その証明書をＳＥＦに登録することを所望するクライアントは、限定ではないが、一例として提示される、以下のパラメータを送信し得る。

● Ｃｌｉｅｎｔ－Ｉｄ
● Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅ：これは、登録されている証明書のタイプの指示である。クライアントのための好ましいＣｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅは、「公開キー」またはその「証明」であり得る。クライアントが、機密性保護を提供するためのみに使用される、「対称キー」を登録することも可能であり得る。
● Ｃｒｅｄｅｎｔｉａｌ：クライアントは、複数の証明書を有し得、種々の証明書をＳＥＦに登録し得る。
● Ａｌｇｏｒｉｔｈｍ：証明書のタイプのために使用されるべきアルゴリズム。
● Ｕｓａｇｅ：どのようにして証明書が使用され得るかについてのポリシ。このパラメータは、一例によると、随意であると見なされる。
● ＡＣＰ：誰／何が証明書を使用することができるかについての制限のリスト。これも、随意であり得る。

【００８５】

２では、図示される例によると、ＳＥＦは、ＣＧ要求を検証し、ＣＤＢ内に証明書を記憶する。３では、ＳＥＦは、証明書を正常に登録することに応じて、「成功」メッセージをクライアントに送信する。それは、クライアントのために登録された証明書の各々に関連付けられる一意のＣｒｅｄｅｎｔｉａｌ－Ｉｄも送信する。

【００８６】

ここで例示的第三者証明書請求プロセス（ＴＰＣＲＰ）を参照すると、コンテンツの真正性を検証することを望むクライアントは、クライアントが暗号化されたコンテンツを解読できる能力を要求する場合、ＳＥＦから証明書を要求し得る。代替として、コンテンツに関連付けられる証明書がＳＣＨＦに登録され、クライアントがＳＣＨＦを発見することができる場合、クライアントは、ＳＣＨＦを用いてＣＲ要求を発行し得る。証明書が決して外部から登録されず、コンテンツジェネレータ（例えば、ＣＣＳＤＦ）においてローカルに記憶されることも可能である。そのような場合、クライアントは、ＣＣＳＤＦを用いてＣＲを発行し得る。ＳＥＦ、ＳＣＨＦ、またはＣＣＳＤＦに関連付けられるＵＲＩは、共通サービス発見／リソース発見機構（例えば、ＤＮＳ－ＳＤ、ＲＤメッセージング）を使用することによって、発見され得る。証明書が登録されている場所にかかわらず、エンティティ（例えば、ＳＥＦ、ＳＣＨＦ、またはＣＣＳＤＦ）は、それ自身で認証および承認を行う必要があり得るか、または証明書が公開されるために、エンティティの代わりに行い得るＴＴＰサービスを使用し得る。ＡＣＰは、ＣＲプロセスの一部として提供されていることもある。認証および承認機構の強度は、要求されているコンテンツのタイプに基づき得る。例示的ＴＰＣＲＰは、証明書がＳＥＦに登録されている図１９に図示されている。前述のように、要求がＣＣＳＤＦまたはＳＣＨＦに標的化されている場合、類似機構が使用され得る。

【００８７】

図１９を参照して、図示される例によると、１では、クライアントは、ＴＰＣＲＰ要求をＳＥＦに送信する。要求は、限定ではないが、一例として提示される、以下のパラメータを含み得る。

● Ｃｏｎｔｅｎｔ－Ｉｄ：クライアントが要求することを望むコンテンツの識別。
● Ｃｒｅｄｅｎｔｉａｌ－Ｉｄ（随意）：クライアントがコンテンツに関連付けられる特定の証明書を受信することを望む場合、このパラメータを使用し得る。殆どの場合、Ｃｒｅｄｅｎｔｉａｌ－Ｉｄが存在する場合、Ｃｏｎｔｅｎｔ－Ｉｄは省略され得る。しかしながら、Ｃｒｅｄｅｎｔｉａｌ－Ｉｄが複数のコンテンツを保護するために使用され得る場合において、Ｃｏｎｔｅｎｔ－ＩｄならびにＣｒｅｄｅｎｔｉａｌ－Ｉｄの組み合わせを使用することが、使用され得る。
● Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅ（随意）：クライアントがＣｒｅｄｅｎｔｉａｌ－Ｉｄへのアクセスを有していない場合において、クライアントは、あるタイプ（例えば、公開キーまたは対称キー）の証明書を要求し得る。
● Ａｌｇｏｒｉｔｈｍ（随意）：クライアントが特定の暗号化アルゴリズム（例えば、ＡＥＳ）のみを行うことができる場合、クライアントは、例えば、それを規定し得る。

【００８８】

２では、ＳＥＦは、クライアントが、コンテンツに関連付けられるＡＣＰ（例えば、証明書へのアクセスのために要求される認証／承認レベル）を満たすことを検証し、証明書がＣＤＢの中に存在する場合、ＳＥＦは、Ｃｏｎｔｅｎｔ－Ｉｄに基づいて証明書を読み出す。ＳＥＦがＣｏｎｔｅｎｔ－Ｉｄに関連付けられる複数の証明書を有する場合、およびＣｒｅｄｅｎｔｉａｌ－Ｉｄもクライアントによって提示されている場合、ＳＥＦは、その特定の証明書を読み出す。Ｃｒｅｄｅｎｔｉａｌ－Ｉｄがない場合、ＳＥＦは、クライアントがその要求内で好ましいＣｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅを送信したかどうかを確認するためにチェックし、該当する場合、Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅに一致するＣｏｎｔｅｎｔ－Ｉｄに関連付けられる証明書を選ぶ。Ｃｒｅｄｅｎｔｉａｌ＿Ｔｙｐｅがないが、好ましいアルゴリズムが要求されている場合、ＳＥＦは、その特定のアルゴリズムによって使用されることができる証明書を選択し得る。代替実施形態では、ＳＥＦは、ＡＣＰがそのようなトランザクションを可能にするならば、Ｃｏｎｔｅｎｔ－Ｉｄに関連付けられる全ての証明書を送信し得る。３では、示されるように、ＳＥＦは、証明書を含む応答を送信する。

【００８９】

図２０は、例示的コンテンツ読み出しプロセス（ＣＲＰ）を示す。１では、図示される例によると、クライアントは、ＣＲＰ要求を開始し、ＳＣＨＦへのメッセージの一部としてＣｏｎｔｅｎｔ－Ｉｄを提示する。２では、ＳＣＨＦは、クライアントがコンテンツにアクセスするために承認されているかどうかを決定するために、承認チェックを開始し得る。クライアントは、承認トークンがＳＥＦから取得された場合、それを提示し得る。そうでなければ、新たな承認が、クライアントとＳＣＨＦとの間で実施される必要があり得る。３では、図示される例によると、要求を検証した後、ＳＣＨＦは、ＰＣＳからＥＣおよび関連付けられるＡＴを読み出す。４では、ＳＣＨＦは、ＥＣ、ＡＴ、およびＣｒｙｐｔｏＰａｒａｍｓを含むＣＲＰ応答メッセージを送信する。ＣｒｙｐｔｏＰａｒａｍｓは、随意に、ＳＣＨＦによって送信され得る。ある場合、ＳＣＨＦは、ＣｒｙｐｔｏＰａｒａｍｓを処理しないこともある。そのような場合、クライアントは、上で説明されるＴＰＣＲＰを使用して、いずれの事前にフェッチされたＣｒｙｐｔｏＰａｒａｍｓも有し得る。コンテンツのタイプおよびＣｒｙｐｔｏＰａｒａｍｓに基づいて、いくつかのコンテンツは、暗号化されないこともあり、したがって、コンテンツは、非暗号化形態で送信され得る。殆どの場合、コンテンツは、完全性保護され得、したがって、対応するＡＴが、ＳＤＦによって導出されていることもあることが仮定される。

【００９０】

例示的実施形態では、クライアントがＥＣおよび関連付けられるＡＴを読み出した後、クライアントは、コンテンツが無承認エンティティによって修正されておらず、合法または信頼できるエンティティ（例えば、ＣＣＳＤＦもしくは高信頼性ＳＣＨＦ）によって生成されたことを検証することによって、かつクライアントがコンテンツを消費することができるように、暗号化されたコンテンツを解読することによって、コンテンツを処理する

。図２１を参照すると、完全性／真正性チェックならびにクライアントによって実施される暗号解読プロセスの高レベル図を描写するフローチャートが図示されている。図２１の説明は、コンテンツがクライアントの公開キーを使用して暗号化され、ＳＤＰの秘密キーを使用して完全性保護される、図９に図示されるクライアント特定のＣｒｙｐｔｏＰａｒａｍｓに基づく。１では、図示される例によると、クライアントは、ＳＣＨＦから読み出されたＥＣを使用し、ＥＣのハッシュを計算するために、ハッシングアルゴリズム（例えば、ＳＨＡ－２５６）とＣｒｙｐｔｏＰａｒａｍｓ内で規定されるノンスとを使用する。２では、クライアントは、ＡＴを使用し、ＳＤＦによって計算されたハッシュを取得するために、公開キーアルゴリズム（例えば、ＲＳＡ）とＳＤＦの公開キーとを使用してそれを解読する。３では、図示される例によると、クライアントによって計算されたハッシュが、ＳＤＦによって生成された解読されたハッシュと比較される。ハッシュが一致しない場合、このプロセスは、停止される。４では、ハッシュが一致した場合、クライアントは、公開キーアルゴリズム（例えば、ＲＳＡ）を用いて、クライアントの秘密キーを使用してＥＣを解読する。ある形態のパッディングが、暗号化されたコンテンツを生成することにおける無作為性のために使用されることが仮定される。本明細書で提示される例がＲＳＡに基づく暗号化であるとしても、実施形態は、そのように限定されないことが理解されるであろう。例えば、公開キーベースの機構ではなく、対称キーベースの暗号化アルゴリズムが、暗号化のために好ましくあり得る。５では、クライアントは、コンテンツを消費する。

【００９１】

ここで例示的コンテンツライフサイクル管理プロセス（ＣＬＭＰ）を参照すると、ＣＣＳＤＦおよび／またはＳＤＦは、特定のコンテンツのコンテンツライフサイクル管理に関与し得る。ＣＬＭプロセスは、表１で提供されるようなセキュリティパラメータ内で提供される（例えば、年単位の）「ライフサイクル」値に基づいて、ＣＣＳＤＦによって開始され得る。ライフサイクル期間がポリシに基づいて達成されたとき、コンテンツは、（例えば、乱数値とコンテンツを混合してパッディングし、ワンタイムキーおよび強力な暗号化アルゴリズムを使用して、それを暗号化することによって）削除され得るか、またはアクセス不可能にされ得る。（例えば、年単位の）「セキュリティ保護を更新する」値が、コンテンツに関連付けられるセキュリティ保護を更新するために使用され得る。セキュリティ保護を更新することは、随意であり得、ある場合、コンテンツをセキュリティ攻撃にさらし得、したがって、信頼されるエンティティ（例えば、ＴＥＥを有し、ＲｏＴに基づくプラットフォーム）のみが、ＣＬＭプロセスを実施することを可能にされ得る。新しいＣＲＰ、ＣＧＰ、再ホスティングプロセス、およびＴＰＣＲＰが、証明書を生成して登録し、コンテンツを保護するために行われ得る。要約すると、新しい証明書が生成されて登録され、コンテンツが、次いで、新しい証明書を使用して保護され、次いで、保護されたコンテンツは、好ましくは、消費のための別個のチャネルを使用して、新たに生成された証明書とともに、承認されたクライアントに提供される。

【００９２】

本明細書に説明される実施形態は、主に、便宜上、ｏｎｅＭ２Ｍアーキテクチャに焦点を当てているが、実施形態はｏｎｅＭ２Ｍに限定されないことが理解されるであろう。以前に説明された一般的機能（例えば、ＳＥＦ）は、図２２に示されるように、Ｍｃａインターフェースを経由して「セキュリティ」の一部としてｏｎｅＭ２Ｍアーキテクチャに組み込まれ得る。例では、ＡＥは、ＣＣＳＤＦを組み込み得、ＣＳＥは、ＳＣＨＦを実装し得る。ＳＥＦは、例示的実施形態では、Ｍ２Ｍ登録機能（ＭＥＦ）に組み込まれる。ＡＥとＭＥＦとの間、また、ＣＳＥとＭＥＦとの間に、基礎的信頼関係があることが理解されるであろう。以前に説明された機能性の概要マッピングおよびｏｎｅＭ２Ｍエンティティが、限定ではないが、一例として、以下の表４で提供されている。

【００９３】

【表４】

oneM2Mエンティティ	機能性
AE	SCHF
	SDF／CCSDF
CSE	SCHF
	SEF
	SDF
	CLMP
MEF	SEF
	CLMP

【００９４】

図２３は、Ｍｃｃインターフェースにおいて、コンテンツセキュリティを提供するためのセキュリティ機能性を組み込むための一例を描写する。以前に説明された機能性の概要マッピングおよびｏｎｅＭ２Ｍエンティティが、限定ではないが、一例として表５で提供されている。

【００９５】

【表５】

oneM2Mエンティティ	機能性
CSE1	SCHF
	SDF
CSE2	SEF
	SCHF
	CLMP

【００９６】

示されるように、ＣＳＥ１は、ＳＤＦおよびＳＣＨＦを実装し得る。ＳＣＨＦ機能性は、セキュアな様式でアプリケーションコンテンツまたはｏｎｅＭ２Ｍシステムリソースに関連し得るｏｎｅＭ２Ｍリソースを記憶するために使用される。ＳＣＨＦは、常駐し得、データ管理およびレポジトリＣＳＦの一部として管理され得る。ＳＤＦは、常駐し、セキュリティＣＳＦ内で管理され得る。ＣＳＥ２では、例によると、ＳＥＦおよびＣＬＭＰ機能性が、セキュリティＣＳＦの一部として組み込まれ得る一方で、セキュアな様式で証明書リソースをセキュアに記憶することに主に関与するＳＣＨＦは、データ管理およびレポジトリの一部として組み込まれ得る。上記で描写されるｃｒｅｄｅｎｔｉａｌ－ＩｄリソースおよびｃｒｙｐｔｏＰａｒａｍｓは、ＳＣＨＦによって記憶されて管理され得る、適切なリソースであり得る。

【００９７】

ここで図２４を参照すると、例示的実施形態が、ｏｎｅＭ２Ｍに従って描写されている。示されるように、コンテンツが、ｏｎｅＭ２Ｍリソースとして表され得る一方で、サブコンポーネントは、属性およびｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ内で表され得る。ここでは、サービス層接続（ホップ）がＴＬＳ／ＤＴＬＳベースのセキュアな接続を使用して保

護され得ることが仮定される。１では、図示される例によると、保護をそれによって作成されるリソースに提供することを意図するＡＥ１は、Ｍ２Ｍ登録機能ＭＥＦを用いて適切な証明書を要求し得る。ＡＥ１とＭＥＦとは、それらの間で相互認証を行っており、（Ｄ）ＴＬＳを使用するセキュアな通信チャネルを確立していることもあることが仮定される。ＭＥＦが、ＡＥ１がそのような要求を行うために承認されていることを決定したことも仮定される。ＡＥ１が完全性ならびに機密性保護を提供することを望む場合、それは、これらの証明書を明示的に要求し得る。代替として、ＡＥ１は、対称キー機構を使用する場合、マスタキー（例えば、ＫｅｙＧｅｎＫｅｙ）のみを要求し得る。ＡＥ１は、リソース作成要求を送信し、要求とともにそのセキュリティ要件（ＳｅｃＲｅｑｕｉｒｅｍｅｎｔｓ）を提供し得る。承認エンティティのリスト（例えば、ＡＥ２の識別）を含み得るアクセス制御ポリシ（ＡＣＰ）リストも提供され得る。２では、ＭＥＦは、ＡＥ１がＭＥＦにおいてリソースを作成するために承認されていることを確実にするためにチェックする。ＡＥ１が承認されている場合、ＭＥＦは、適切な証明書および関連付けられるｃｒｅｄｅｎｔｉａｌ－Ｉｄを生成する。それは、図２５で描写されるようなリソース構造を作成し得る。３では、図示される例によると、ＭＥＦは、ＡＥ１に戻す応答として、証明書およびｃｒｅｄｅｎｔｉａｌ－Ｉｄを送信する。代替として、ＡＥ１は、証明書を取得するために、読み出し動作を行うことが可能であり得る。証明書は、例えば、ＪＳＯＮウェブキー（ＪＷＫ）フォーマットの形態で表され、送信され得る。

【００９８】

依然として図２４を参照して、図示される例によると、４では、ＣｒｙｐｔｏＰａｒａｍｓならびにＡＥ１によって読み出された証明書に基づいて、ＡＥ１は、ＥＣ－Ｒ１を作成するためにリソースを暗号化し、Ｒ１－ＡＴと称されるリソースのＡＴ（ＭＡＣまたはデジタル署名）を生成する。アルゴリズムならびにノンスおよびＩｄの選択は、ＣｒｙｐｔｏＰａｒａｍｓ内の値に基づき得る。作成されるＥＣ－Ｒ１は、ＪＳＯＮウェブ暗号化（ＪＷＥ）に基づき得、作成されるＲ１－ＡＴは、ＪＳＯＮウェブ署名に基づき得る。適切なアルゴリズムは、例えば、ＪＳＯＮウェブアルゴリズム（ＪＷＡ）規格で規定されるような形態で表され得る。５では、ＡＥ１は、暗号化されたコンテンツ（ＥＣ－Ｒ１）ならびにＲ１－ＡＴおよびＣｒｙｐｔｏＰａｒａｍｓを含むリソースを作成するための要求をホスティング－ＣＳＥ（Ｈ－ＣＳＥ）に送信する。５における要求は、登録プロセスの一部であり得るか、またはＡＥ１は、要求を送信することに先立って、前もってＨ－ＣＳＥに登録していることもある。Ｈ－ＣＳＥが、ある場合、完全には信頼できないこともあるので、ＣＫ、ＩＫ、およびＫｅｙＧｅｎＫｅｙがＣｒｙｐｔｏＰａｒａｍｓの一部としてＨ－ＣＳＥに提供または露出されないことを確実にするように、注意を払うべきである。しかしながら、公開キー機構が使用される場合、例えば、公開キー値、または証明もしくは公開キーへのリンクが、ＣｒｙｐｔｏＰａｒａｍｓの一部として提供され得る。６では、例えば、ＡＥ１がＨ－ＣＳＥにおいてリソースを作成するために承認されている場合、Ｈ－ＣＳＥは、保護されたコンテンツをホストする。保護されたコンテンツのために作成される例示的リソース構造が、図２９に図示されている。７では、図示される例によると、クライアント（ＡＥ２）は、保護されたリソースＥＣ－Ｒ１を取得することを望み、したがって、Ｒ１を読み出すために、要求メッセージをＨ－ＣＳＥに送信する。８では、Ｈ－ＣＳＥは、ＥＣ－Ｒ１に関連付けられるＡＣＰを使用することによって、ＡＥ２の承認を検証する。ＡＣＰは、ＡＥ（ＣＣＳＤＦ）によって提供されるポリシ、ＳＰがプロビジョニングしたポリシ、またはＨ－ＣＳＥにおけるローカルポリシに基づいて、作成されていることもある。９では、ＡＥ２が承認チェックをパスする場合、Ｈ－ＣＳＥが、ＥＣ－Ｒ１、Ｒ１－ＡＴ、およびＣｒｙｐｔｏＰａｒａｍｓを含む応答をＡＥ２に送信する。上記のように、ＣｒｙｐｔｏＰａｒａｍｓは、Ｈ－ＣＳＥが、ある場合、信頼できないこともあるので、ＣＫ、ＩＫ、またはＫｅｙＧｅｎＫｅｙを含まないこともある。ＣｒｙｐｔｏＰａｒａｍｓは、公開キーまたは証明、もしくは公開キーまたは証明へのリンクを含み得る。１０では、ＡＥ２は、ＣｒｙｐｔｏＰａｒａｍｓからＣｒｅｄｅｎｔｉａｌ－Ｉｄを抽出する。１２では、ＡＥ２は、要求メッセージをＭＥＦに送信する。要求メッセー

ジは、証明書のための読み出し動作を行うために、Ｒ１に関連付けられるＣｒｅｄｅｎｔｉａｌ－Ｉｄを含み得る。１２では、図示される例によると、ＭＥＦは、ＡＥ１によって作成されたＡＣＰに基づいて、ＡＥ２が証明書をプロビジョニングされるために承認されていることを決定する。１３では、ＡＥ２が承認されている場合、ＭＥＦは、証明書をＡＥ２に送信する。１４では、ＡＥ２は、Ｒ１の真正性／完全性を検証するため、およびそれを解読するために、証明書を使用する。

【００９９】

図２４を参照して上で説明される実施形態は、（例えば、２つのＣＳＥ、すなわち、ＣＳＥ１、ＣＳＥ２間の）Ｍｃｃインターフェースに適用可能であり得ることが理解されるであろう。そのようなシナリオでは、例えば、ＡＥ１は、ＣＳＥ１と置換され得、ＡＥ２は、ＣＳＥ２によって置換され得る。

【０１００】

したがって、図２４を参照すると、装置（例えば、ＡＥ１）は、プロセッサと、メモリと、通信回路とを含み得る。装置は、その通信回路を介してネットワークに接続され得、装置はさらに、装置のプロセッサによって実行されると、装置に、コンテンツの保護を提供する１つ以上の証明書に対する要求を送信させるノードのメモリ内に記憶されたコンピュータ実行可能命令を備え得る。要求は、コンテンツに関連付けられた１つ以上のセキュリティパラメータに基づき得る。装置は、１つ以上の証明書を取得し、コンテンツをセキュアにするために１つ以上の証明書を使用し得る。証明書は、対称キー機密性保護のためのマスタキーを備え得る。証明書は、完全性保護および機密性保護の両方のための証明書を備え得る。装置は、暗号化されたコンテンツを作成するためにコンテンツを暗号化し得る。装置は、コンテンツに関連付けられる認証タグを生成し得る。さらに、示されるように、装置は、暗号化されたコンテンツおよびセキュリティパラメータを含むリソースを作成するための要求をホスティング共通サービスエンティティに送信し得る。示されるように、証明書は、一例によると、Ｍ２Ｍ登録機能から取得され得る。

【０１０１】

ＳＥＦがＣＳＥに常駐する代替実施形態が、図２６に図示されている。図２６を参照して、図示される実施形態によると、１では、リソースＲ１をセキュアにホストすることを望むＡＥ１が、セキュリティ要件に基づいて適切な証明書を生成する。証明書を使用して、ＡＥ１は、ＥＣ－Ｒ１を作成するためにコンテンツを暗号化し得、（使用されている証明書のタイプに基づいてＤＳまたはＭＡＣであり得る）Ｒ１－ＡＴを作成するためにそれを完全性保護する。暗号化されたＥＣ－Ｒ１の例は、ＪＳＯＮウェブ暗号化として表され得る。２では、ＡＥ１は、証明書ホスティングサービスを行うＣＳＥにおいてＣｒｅｄｅｎｔｉａｌ－Ｉｄリソースを作成するための要求を行う。例では、ＡＥおよびＣＳＥが相互信頼関係を共有することが仮定される。例では、ＡＥ１とＣＳＥとの間の通信がセキュアな通信チャネル（例えば、ＤＴＬＳ、ＴＬＳ）を経由して搬送されることも仮定される。セキュアな通信チャネルを使用して、ＡＥ１は、ＡＥ１が生成し、コンテンツを暗号化し、および／または完全性保護するために使用した１つ以上の証明書をＣＳＥに送信し得る。３では、ＣＳＥは、ＡＥ１がリソースを作成するために承認されているかどうかを決定し得る。例えば、ＣＳＥは、（Ｄ）ＴＬＳを使用するセキュアな通信チャネル確立プロセス中、認証プロシージャを実施していることもある。代替として、または加えて、ＡＣＰポリシが、サービスプロバイダによってＣＳＥにおいて事前プロビジョニングされていることもある。ＣＳＥは、随意に、ＡＥ１の公開キーを使用してＡＴを検証し得る。ＣＳＥは、随意に、ＣＳＥに関連付けられる一意のＣｒｅｄｅｎｔｉａｌ－Ｉｄを生成し得る。これは、随意であり、ＡＥ１によって提供されていることもある。ある場合、ドメイン内の唯一性ならびに大域的到達可能性を提供するために、ＣＳＥは、ＡＥ１の代わりにＣｒｅｄｅｎｔｉａｌ－Ｉｄを生成し得る。ＣＳＥにおいて作成されるＣｒｅｄｅｎｔｉａｌ－Ｉｄリソースは、図２７の例によって図示される形態であり得る。

【０１０２】

依然として図２６を参照して、図示される実施形態によると、ＣＳＥは、４においてＣ

ｒｅｄｅｎｔｉａｌ－ＩｄをＡＥ１に送信する。５では、ＡＥ１は、暗号化されたＥＣ－Ｒ１であり、Ｒ１－ＡＴを使用して完全性保護されたセキュアなリソースＲ１を作成することを要求する。したがって、図示される例によると、Ｈ－ＣＳＥは、第１のアプリケーションに関連付けられたセキュアにされたコンテンツをホストするためのリソースを作成するための第１の要求を第１のアプリケーション（ＡＥ１）から受信する。ＡＥ１は、必要なＣｒｙｐｔｏＰａｒａｍｓおよびＣｒｅｄｅｎｔｉａｌ－Ｉｄを提供し得る。したがって、要求は、Ｈ－ＣＳＥとは別個であるＣＳＥによって生成される証明書識別を含み得る。Ｃｒｅｄｅｎｔｉａｌ－Ｉｄは、ＣｒｙｐｔｏＰａｒａｍｓの一部であり得るか、またはＲ１に関連付けられる別個の子リソースとして送信され得る。例では、ＡＥ１とＨ－ＣＳＥとが、互いに相互認証しており、ＴＬＳまたはＤＴＬＳを使用してセキュアな通信チャネルを確立していることが仮定される。それは、例えば、図２８で描写されるように、関連付けられるアクセス制御ポリシリソースを含み得る。このＡＣＰは、完全性保護され得、ＡＴは、ＡＥ１の秘密キーを使用して生成されたＤＳに基づいて作成され得る。作成されるＥＣ－Ｒ１は、ＪＳＯＮウェブ暗号化（ＪＷＥ）に基づき得、作成されるＲ１－ＡＴは、ＪＳＯＮウェブ署名に基づき得る。適切なアルゴリズムは、ＪＳＯＮウェブアルゴリズム（ＪＷＡ）規格で規定されるような形態で表され得る。６では、Ｈ－ＣＳＥは、要求を検証し、ＡＥ１がＨ－ＣＳＥにおいてリソースを作成するために承認されていることを確実にする（そうであるかどうかを決定する）ためにチェックする。７では、図示される例によると、Ｈ－ＣＳＥは、成功で応答する。したがって、例示的アプリケーションが承認される場合、Ｈ－ＣＳＥは、セキュアにされたコンテンツをホストし得る。ある場合、アプリケーションは、Ｈ－ＣＳＥと別個であるＣＳＥによって、リソースを作成するために承認され得る。

【０１０３】

８では、クライアント（ＡＥ２）は、Ｒ１を読み出すことを望み、したがって、Ｒ１を読み出すための要求、例えば、第２の要求をＨ－ＣＳＥに送信する。したがって、Ｈ－ＣＳＥは、ＡＥ１に関連付けられるセキュアにされたコンテンツにアクセスするための第２の要求を第２のアプリケーション（ＡＥ２）から受信し得る。Ｒ１を発見することに関与する機構は、例の範囲外であり、ＡＥ２は、Ｒ１のセキュアなバージョンの場所を発見できることが仮定される。ＡＥ２が、完全性の観点から、より劣った確実性を有するＲ１のあまりセキュアではないバージョンを発見することが可能であり得る。要求は、相互認証がＤＴＬＳまたはＴＬＳに基づいて行われた後、セキュアなチャネルを経由して送信されることが仮定される。９では、図示される実施形態によると、Ｈ－ＣＳＥは、ＡＥ１によって作成されたＡＣＰ内の情報を使用して、ＡＥ２が読み出し動作を行うことを許可されているかどうかの承認を検証する。したがって、Ｈ－ＣＳＥは、ＡＥ２がセキュアにされたコンテンツにアクセスするために承認されているかどうかを決定することができる。１０では、Ｈ－ＣＳＥは、ＥＣ－Ｒ１、ＥＣ－ＡＴ、ならびにＲ１－ＣｒｙｐｔｏＰａｒａｍｓを含む応答を送信する。したがって、第２のアプリケーションがセキュアにされたコンテンツにアクセスするために承認されている場合、Ｈ－ＣＳＥは、セキュアにされたコンテンツを第２のアプリケーションに送信することができる。ＥＣ－Ｒ１が、例えば、ＪＳＯＮベースの表記法ＪＷＥを使用して表され得る一方で、ＥＣ－ＡＴは、ＪＷＳを使用して表され得、Ｒ１－ＣｒｙｐｔｏＰａｒａｍｓは、ＪＷＡを使用して表され得る。１１では、Ｃｒｅｄｅｎｔｉａｌ－ＩｄがＣｒｙｐｔｏＰａｒａｍｓの一部として含まれた場合、ＡＥ２は、それからＣｒｅｄｅｎｔｉａｌ－Ｉｄを抽出する。１２では、ＡＥ２は、メッセージ内にｒｅｓｏｕｒｃｅ－ｉｄとしてＣｒｅｄｅｎｔｉａｌ－Ｉｄを含むことによって、読み出し動作を行うための要求メッセージをＣＳＥに送信する（例えば、ＣＳＥのＵＲＩは、Ｃｒｅｄｅｎｔｉａｌ－Ｉｄ内に含まれるドメイン情報に基づいて決定され得、Ｃｒｅｄｅｎｔｉａｌ－Ｉｄは、Ｒ１ｘｙｒｔａｂｓｆｆａｓ@ＣＳＥ．ｃｏｍという形態であり得る）。例では、ＡＥ２およびＣＳＥは、互いに相互認証し、ＴＬＳまたはＤＴＬＳを使用してセキュアな通信チャネルを確立していることが仮定される。Ｃｒｅｄｅｎｔｉａｌ－Ｉｄは、例えば、ＪＷＫ等のＪＳＯＮベースの表記法を使用して送信され

得る。１３では、ＣＳＥは、２において証明書登録プロセス中にＡＥによって作成されたＡＣＰに基づいて、ＡＥ２の承認を検証する。１４では、ＡＥ２が読み出すために承認されている場合、ＣＳＥは、セキュアなチャネルを経由して証明書をＡＥ２に送信する。１５では、証明書を使用して、ＡＥ２は、Ｒ１－ＡＴを使用して完全性を検証し、Ｒ１を解読する。したがって、セキュアにされたコンテンツは、ＣＳＥがセキュアにされたコンテンツに関連付けられた１つ以上の証明書を第２のアプリケーション（ＡＥ２）に送信した場合、解読されることができる。ある場合、上で説明されるように、ＡＥ２は、ＡＥ１のアクセス制御ポリシによって、セキュアにされたコンテンツにアクセスするために承認されている。

【０１０４】

図２６に関して上で説明される実施形態は、（例えば、２つのＣＳＥ、すなわち、ＣＳＥ１、ＣＳＥ２間の）Ｍｃｃインターフェースにも適用可能であり得ることが理解されるであろう。そのようなシナリオでは、エンティティＡＥ１は、ＣＳＥ１と置換され得、ＡＥ２は、ＣＳＥ２によって置換され得る。

【０１０５】

したがって、図２６を参照すると、装置（例えば、ＡＥ１）は、プロセッサと、メモリと、通信回路とを備え得る。装置は、その通信回路を介してネットワークに接続され得、装置はさらに、装置のプロセッサによって実行されると、装置に、コンテンツに関連付けられたセキュリティ要件に基づいて、１つ以上の証明書を生成させる、装置のメモリ内に記憶されたコンピュータ実行可能命令を備え得る。以下で詳細に説明されるように（例えば、図３７参照）、１つ以上の証明書は、装置と信頼有効化機能との間のアソシエーションをブートストラップすることによって生成され得る。装置は、１つ以上の証明書を使用してコンテンツをセキュアにし（例えば、暗号化）、承認されたクライアントのみがホスティングノードからコンテンツを読み出すことができるように、ホスティングノードがセキュアにされたコンテンツを記憶することを要求し得る。装置は、１つ以上の証明書を使用して、認証タグを生成し得る。認証タグは、ホスティング共通サービスエンティティにおいてホストするためのコンテンツの完全性および真正性を示し得る。要求に応答して、装置は、共通サービスエンティティから証明書識別を受信し得る。要求は、証明書識別に関連付けられる証明書を含み得、要求は、証明書の登録を得ようとする。例示的実施形態では、証明書識別は、共通サービスエンティティに一意である。示されるように、装置は、ノードがホスティングノードにおいてリソースを作成するために承認されていることをホスティングノードが決定した場合、成功メッセージをさらに受信し得る。

【０１０６】

別の実施形態によると、データセキュリティ証明書が、ブートストラップを使用して生成される。例えば、ＡＥは、ＡＥと、Ｍ２Ｍ登録機能（ＭＥＦ）、信頼有効化機能（ＴＥＦ）、またはＭ２Ｍ認証機能（ＭＡＦ）等の信頼される第３のエンティティとの間の既存のアソシエーションを使用するブートストラッピングプロセスを活用することによって、データセキュリティ証明書を生成し得る。この文脈で使用される場合、「データセキュリティ」という用語は、コンテンツセキュリティまたはリソースセキュリティを指し得ることが理解されるであろう。データは、コンテンツのインスタンスを指し得る。したがって、コンテンツインスタンスセキュリティは、概して、本明細書ではデータセキュリティとも称され得る。ある場合、ＴＥＦは、特定のセキュリティ証明書のデータ（例えば、コンテンツまたはリソース）の遠隔プロビジョニングのために主に使用されるＭＥＦの特別な実装である。したがって、別様に規定されない限り、ＴＥＦおよびＭＥＦという用語は、限定ではないが、同義的に使用され得る。

【０１０７】

ここで図３７を参照して、図示される実施形態によると、データ／コンテンツセキュリティ証明書が、ＡＥとＴＥＦとの間のブートストラッピングプロセスの結果として生成される。０では、ｏｎｅＭ２Ｍ仕様書（ＴＳ－０００３、リリース１）内で現在説明されているブートストラッピングプロセスは、データセキュリティ証明書を導出するためにブー

トストラッピングを使用することによって、強化され得る。ＡＥとＭＥＦ／ＴＥＦとの間で共有される証明書ＫｐｍＩｄ／Ｋｐｍは、ＴＳ－０００３（リリース１）で説明されるように、セッション証明書ＫｅＩｄ／Ｋｅを生成するために使用される。証明書Ｋｅは、ＡＥとＴＥＦとの間でデータセキュリティ特定の証明書を生成するために使用され得る。同様に、ＡＥとＣＳＥとの間のブートストラッピングプロセスは、ＡＥとＣＳＥとの間の既存のセキュリティアソシエーションを活用し得る。セキュリティアソシエーションは、ｏｎｅＭ２Ｍ　ＴＳ－０００３で説明されるように、ＫｐｓａＩｄ／Ｋｐｓａによって識別され得る。Ｋｐｓａが、次いで、Ｋｅの代わりに使用される。同様に、ＡＥとＭＥＦとの間にセキュリティアソシエーションを確立するために使用されるＫｍＩｄ／Ｋｍは、ＡＥとＭＥＦとの間でデータセキュリティ証明書を生成するために使用され得る。ある場合、より好ましいアプローチは、ＡＥおよびＴＥＦのためにデータセキュリティ証明書を生成することである。

【０１０８】

依然として図３７を参照して、１では、図示される例によると、マスタキーがＡＥ（ＡＥ１）によって生成される。キー生成の一部として使用される乱数値であるソルトが、ブートストラッピングプロセス中に共有され得るか、またはブートストラッピング中にＡＥとＴＥＦとの間の初期通信のハッシュ値として計算され得る。ソルトは、ＡＥ１とＴＥＦとの間で結合されるチャネルの暗号表現であり得る。チャネルは、ＴＬＳまたはＤＴＬＳを使用して確立されるセキュアな接続であり得る。エンローリと称され得るＡＥ１、および登録標的と称され得るＴＥＦは、Ｋｅを使用してデータセキュリティ証明書を生成し得る。示されるように、Ｋｅ＿ＡＥ１－ＴＥＦは、ＡＥ１とＴＥＦとの間で関連付けられるＫｅを指す。Ｋｅは、データセキュリティマスタキー、すなわち、Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒを生成するために使用されるマスタキーであり得る。代替として、例えば、標的がＭＥＦである場合、Ｋｍが、データセキュリティマスタキーを生成するためのマスタキーとして使用され得る。エンローリがＡＥであり、登録標的がＴＥＦである、ＲＦＣ　５８０９を使用するデータセキュリティキー生成の例が、以下に提供される。

● Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒ＝ＨＭＡＣ－Ｈａｓｈ（Ｓａｌｔ，Ｋｅ＿ＡＥ１＿ＴＥＦ）

● Ｔ（０）＝空の文字列（ゼロ長）

● Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒが生成されると、それは、一意のデータ真正性およびデータ機密性キーを生成するために、キー拡張に使用され得る。ある場合、データ真正性および機密性がＡＥＡＤ（例えば、ＡＥＳ－ＣＣＭまたはＡＥＳ－ＧＣＭ）等のアルゴリズムによって提供される場合、単一のキーのみが生成される。

● Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ａｕｔｈ＝Ｔ（１）＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒ，Ｔ（０）｜”Ｄａｔａ　Ａｕｔｈｅｎｔｉｃｉｔｙ　ａｎｄ　Ｉｎｔｅｇｒｉｔｙ”｜０ｘ０１）

● Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ａｕｔｈキーは、データ真正性およびデータ完全性を提供するために使用され、したがって、データ真正性またはデータ完全性キーと称され得る。

● Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｃｏｎｆ＝Ｔ（２）＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒ，Ｔ（１）｜”Ｄａｔａ　Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ　Ｋｅｙ”｜０ｘ０２）

【０１０９】

ある場合、（ＡＥ１とＣＳＥ１との間のＫｐｓａである）Ｋｐｓａ＿ＡＥ１＿ＣＳＥ１が、Ｋｅ＿ＡＥ１＿ＴＥＦの代わりに使用され得、上で説明されるプロセスが、データセキュリティ保護（例えば、データ認証、完全性、およびデータ機密性）のための一意のキーを生成するために使用され得る。Ｋｐｓａは、ＣＳＥがデータセキュリティ証明書レジストリとしてＡＥによって使用される場合に使用され得る。ある場合、Ｋｐｓａ＿ＡＥ１＿ＣＳＥ、Ｋｅ＿ＡＥ＿ＴＥＦ、またはＫｍ＿ＡＥ１＿ＭＡＦが、Ｋ＿ＡＥ１＿ＴＥＦ＿

ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒ ｋｅｙとして使用され得、上で説明されるプロセスが、データセキュリティ保護（例えば、データ認証、完全性、およびデータ機密性）のための一意のキーを生成するために使用され得る。ある他の場合、セッションキーが、次いで、データ真正性およびデータ機密性のための一意のキーを生成するためのマスタキーとして使用される、Ｋｅ＿ＡＥ１＿ＣＳＥ１、Ｋｐｓａ＿ＡＥ１＿ＴＥＦ、Ｋｍ＿ＡＥ１＿ＭＡＦから生成される。ある他の場合、Ｋｅ、Ｋｐｓａ、またはＫｐｍから生成される単一のセッションキー（Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ａｕｔｈ＿ｃｏｎｆ）のみが、ＡＥＡＤクラスのアルゴリズムとともに使用されるときに、データ真正性およびデータ機密性の両方を提供するために使用される。

【０１１０】

２では、図示される例によると、キー生成の類似プロセスが、ＴＥＦによって実施される。アルゴリズム、キー生成機構、キーのタイプ、生成されるキーの数等のネゴシエーションは、ブートストラッピングプロセスがＡＥ１とＴＥＦとの間で実施されたときのステップ０中に行われ得る。

【０１１１】

３では、ＡＥ１は、コンテンツ／データを生成する。コンテンツ／データの各インスタンスは、データ真正性およびデータ機密性キーの一意の組によって保護され得る。別の例では、コンテンツのインスタンス、例えば、コンテンツの全てのインスタンスが、単一のデータ真正性キーによって、および単一のデータ機密性キーによって、保護され得る。単一のデータ真正性および単一のデータ機密性キーのみが、複数のコンテンツインスタンスを含み得るコンテナのために生成される例示的キー生成が、以下に示される。

● Ｋ＿ＡＥ１＿Ｃｏｎｔａｉｎｅｒ－ｘ＿ｄａｔａ＿ａｕｔｈ＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ａｕｔｈ，”Ｄａｔａ Ａｕｔｈｅｎｔｉｃｉｔｙ ａｎｄ Ｉｎｔｅｇｒｉｔｙ”｜”Ｃｏｎｔａｉｎｅｒ－ｘ”｜Ｎｏｎｃｅ ｏｒ ｃｒｅａｔｉｏｎＴｉｍｅ）および

● Ｋ＿ＡＥ１＿Ｃｏｎｔａｉｎｅｒ－ｘ＿ｄａｔａ＿ｃｏｎｆ＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｃｏｎｆ，”Ｄａｔａ Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ”｜”Ｃｏｎｔａｉｎｅｒ－ｘ”｜Ｎｏｎｃｅ ｏｒ ｃｒｅａｔｉｏｎＴｉｍｅ）

【０１１２】

代替として、コンテナ内のコンテンツの各インスタンスのために、キーの一意の組が生成され得る。そのような実施形態の例が、以下に示される。

● Ｋ＿ＡＥ１＿ＣｏｎｔｅｎｔＩｎｓｔａｎｃｅ－ｘ＿ｄａｔａ＿ａｕｔｈ＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ａｕｔｈ，”Ｄａｔａ Ａｕｔｈｅｎｔｉｃｉｔｙ ａｎｄ Ｉｎｔｅｇｒｉｔｙ”｜”Ｃｏｎｔａｉｎｅｒ－ｘ”｜Ｎｏｎｃｅ ｏｒ ｃｒｅａｔｉｏｎＴｉｍｅ）および

● Ｋ＿ＡＥ１＿ＣｏｎｔｅｎｔＩｎｓｔａｎｃｅ－ｘ＿ｄａｔａ＿ｃｏｎｆ＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｃｏｎｆ，”Ｄａｔａ Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ”｜”Ｃｏｎｔｅｎｔ Ｉｎｓｔａｎｃｅ”｜Ｎｏｎｃｅ ｏｒ ｃｒｅａｔｉｏｎＴｉｍｅ）

【０１１３】

コンテンツは、上記の生成されたキーを使用して、暗号化および／または完全性保護され得る。コンテンツを暗号化するために、ランダムＩＶが、ＡＥ１によって生成され得る。ランダムＩＶは、暗号化されたコンテンツ（ＥＣ－Ｒ１、暗号化されたリソース）を生成するために、暗号化アルゴリズムおよびコンテンツ（データ）とともに使用され得る。

【０１１４】

コンテンツインスタンスが別個に暗号化されているある場合、各コンテンツインスタンスは、一意の機密性キーを有し得、暗号化プロセスが実行される度に新しいＩＶが生成され得、それによって、暗号化されたコンテンツインスタンスを生成する。したがって、各コンテンツインスタンスは、関連付けられる別個の暗号化されたコンテンツインスタンス

を有し得る。
【０１１５】
完全性保護のために、または真正性をコンテンツ／データに追加するために、関連付けられる時間成分を伴うランダムノンスが、コンテンツに関連付けられる認証タグ（ＡＴ）を生成するために使用され得る。各コンテンツインスタンスが別個に保護されている場合において、各コンテンツインスタンスは、関連付けられるＡＴを有し得る。データ真正性を提供するために、ある場合、各個々のＡＴを生成するために単一のキーを使用することが好ましくあり得る。
【０１１６】
暗号化されたコンテンツは、図２９で描写されるように、修正されたｏｎｅＭ２Ｍコンテナまたは＜ｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ＞リソースとして表され得る。代替として、作成されるＥＣ－Ｒ１は、ＲＦＣ　７５１６に規定されるＪＳＯＮウェブ暗号化（ＪＷＥ）に基づき得る。作成されるＥＣ－Ｒ１は、ＲＦＣ　７５１５に規定されるＪＳＯＮウェブ署名に基づき得る。適切なアルゴリズムは、ＪＳＯＮウェブアルゴリズム（ＪＷＡ）規格、ＲＦＣ　７５１８に規定されるような形態で表され得る。
【０１１７】
概して、生成されて使用される各キーは、一意のＣｒｅｄｅｎｔｉａｌ－Ｉｄに関連付けられ得る。Ｃｒｅｄｅｎｔｉａｌ－Ｉｄは、ＡＥ１によって生成され得るか、またはＴＥＦによってＡＥ１に提供され得る。ある場合、Ｃｒｅｄｅｎｔｉａｌ－Ｉｄは、コンテンツｉｄまたはコンテンツインスタンスｉｄの特性および証明書のタイプを保持し得る。Ｃｒｅｄｅｎｔｉａｌ－ｉｄの例は、キーＫ＿ＡＥ１＿Ｃｏｎｔａｉｎｅｒ－ｘ＿ｄａｔａ＿ｃｏｎｆに関連付けられる、Ｋ＿ＡＥ１＿Ｃｏｎｔａｉｎｅｒ－ｘ＿ｄａｔａ＿ｃｏｎｆ－Ｉｄ@ＴＥＦ．ｃｏｍという形態であり得る。
【０１１８】
図３７を続けて参照して、４では、図示される実施形態によると、ＡＥ１は、Ｃｒｅｄｅｎｔｉａｌ－ＩｄをＴＥＦに登録し得る。図示されるように、ＡＥ１は、Ｃｒｅｄｅｎｔｉａｌ－Ｉｄおよび関連付けられるアクセス制御ポリシによって識別される証明書リソースを作成することを要求する。Ｃｒｅｄｅｎｔｉａｌ－Ｉｄは、代替として、例えば、ＴＥＦに関連付けられるＣｒｅｄｅｎｔｉａｌ－Ｉｄの衝突を回避するために、ＴＥＦによって提供され得る。Ｃｒｅｄｅｎｔｉａｌ－Ｉｄの衝突は、ハッシュがＡＥ１による生成ｉｄの範囲外に保持される場合、回避され得る。例示的ハッシュが、以下に示される。
● Ｈ１＝Ｈａｓｈ（Ｋ＿ＡＥ１＿Ｃｏｎｔａｉｎｅｒ－ｘ＿ｄａｔａ＿ｃｏｎｆ－Ｉｄ）
● Ｃｒｅｄｅｎｔｉａｌ－Ｉｄ＝Ｈ１@ＴＥＦ．ｃｏｍ
【０１１９】
５では、示されるように、ＴＥＦは、ＡＥ１が証明書をＴＥＦに登録するために承認されていることを確実にするためにチェックする。ＴＥＦは、Ｃｒｅｄｅｎｔｉａｌ－Ｉｄおよび含まれていることもある随意のＣｒｙｐｔｏＰａｒａｍｓも検証し得る。ＴＥＦは、次いで、＜ｃｒｅｄｅｎｔｉａｌ－Ｉｄ＞リソースタイプを作成し得、例えば、＜ａｃｃｅｓｓＣｏｎｔｒｏｌＰｏｌｉｃｙ＞値等の属性でそれにデータ投入する。
【０１２０】
６では、図示される例によると、ＴＥＦは、証明書リソースの成功した作成を示す応答をＡＥ１に送信する。７では、ＡＥ１は、暗号化されたＥＣ－Ｒ１であり、Ｒ１－ＡＴを使用して完全性保護されたセキュアなリソースＲ１を作成することを要求する。ＡＥ１は、ＣｒｙｐｔｏＰａｒａｍｓおよびＣｒｅｄｅｎｔｉａｌ－Ｉｄも提供し得る。Ｃｒｅｄｅｎｔｉａｌ－Ｉｄは、ＣｒｙｐｔｏＰａｒａｍｓの一部であり得るか、またはＲ１に関連付けられる別個の子リソースとして送信され得る。ある場合、ＡＥ１とＨＣＳＥとは、互いに相互認証し、ＴＬＳまたはＤＴＬＳを使用してセキュアな通信チャネルを確立している。要求は、関連付けられるアクセス制御ポリシ（ＡＣＰ）リソースも含み得る。このＡＣＰは、完全性保護され得る。

【０１２１】
８では、Ｈ－ＣＳＥは、要求を検証し、ＡＥ１がＨ－ＣＳＥにおいてリソースを作成するために承認されていることを確実にするためにチェックする。９では、Ｈ－ＣＳＥは、成功メッセージで対応する。１０を参照すると、ある時点で、クライアント（ＡＥ２）は、Ｒ１を読み出すことを望み得る。クライアントは、Ｒ１を読み出す要求をＨＣＳＥに送信し得る。ある場合、ＡＥ２は、Ｒ１のセキュアなバージョンの場所を発見することができる。ある場合、ＡＥ２は、完全性の観点から、より劣った確実性を有するＲ１のあまりセキュアではないバージョンを発見し得る。要求は、相互認証がＤＴＬＳまたはＴＬＳに基づいて行われた後、セキュアなチャネルを経由して送信され得る。ＡＥ２は、リソースＲ１に「読み出し」動作を行うための要求を送信し得る。１１では、図示される例によると、ＨＣＳＥは、ＡＥ１によって作成されたＡＣＰ内の情報を使用して、ＡＥ２が読み出し動作を行うことを可能にされているかどうかの承認を検証する。１２では、ＨＣＳＥは、ＥＣ－Ｒ１、ＥＣ－ＡＴ、およびＲ１－ＣｒｙｐｔｏＰａｒａｍｓを含む応答を送信する。ＥＣ－Ｒ１は、ＪＳＯＮベースの表記法（例えば、ＪＷＥ）を使用して表され得、例えば、ＥＣ－ＡＴは、ＪＷＳを使用して表され得、Ｒ１－ＣｒｙｐｔｏＰａｒａｍｓは、ＪＷＡを使用して表され得る。代替として、特に、例えば、暗号化および完全性保護に使用されるアルゴリズムが、ＡＥＡＤアルゴリズム（例えば、ＡＥＳ－ＧＣＭまたはＡＥＳ－ＣＣＭ）に基づく場合、ＥＣ－ＡＴおよびＥＣ－Ｒ１は両方とも、ＪＷＥとして表され得る。なおも代替として、暗号化されたコンテンツＥＣ－Ｒ１およびＲ１－ＡＴは、適切なＣｒｙｐｔｏＰａｒａｍｓとともにｏｎｅＭ２Ｍリソースとして表され得る。

【０１２２】
１３では、図示される例によると、Ｃｒｅｄｅｎｔｉａｌ－ＩｄがＣｒｙｐｔｏＰａｒａｍｓの一部として含まれた場合、ＡＥ２は、それからＣｒｅｄｅｎｔｉａｌ－Ｉｄを抽出する。１４では、ＡＥ２は、例えば、メッセージ内にｒｅｓｏｕｒｃｅ－ｉｄとしてＣｒｅｄｅｎｔｉａｌ－Ｉｄを含むことによって、読み出し動作を行うための要求メッセージをＴＥＦに送信する。ＡＥ２とＴＥＦとは、互いに相互認証し、ＴＬＳまたはＤＴＬＳを使用してセキュアな通信チャネルを確立していることもある。Ｃｒｅｄｅｎｔｉａｌ－Ｉｄは、例えば、ＪＳＯＮベースの表記（例えば、ＪＷＫ）を使用して、またはｏｎｅＭ２Ｍリソース構造を使用して、送信され得る。ＡＥ２は、リソースＲ１（データ）に関連付けられるＣｒｙｐｔｏＰａｒａｍｓからソルトまたはノンスも抽出し得る。ＡＥ２は、Ｃｒｅｄｅｎｔｉａｌ－Ｉｄとともに、リソース特定の証明書を読み出すためのソルトまたはノンスを送信し得る。

【０１２３】
１５では、ＴＥＦは、２における証明書登録プロセス中にＡＥ１によって作成されたＡＣＰに基づいて、ＡＥ２の承認を検証する。１６では、ＡＥ２が読み出すために承認されている場合、ＴＥＦは、リソース特定の証明書を計算し、セキュアなチャネルを経由して証明書をＡＥ２に送信する。ＴＥＦは、どのようにして証明書が使用され得るか、および使用されることができる関連付けられるアルゴリズムを示す使用情報も送信し得る。ある場合、ＡＥ２は、使用情報をすでに入手していることもあり。ＡＥ２は、それをＣｒｙｐｔｏＰａｒａｍｓの一部としてＨＣＳＥから取得していることもある。しかしながら、コンテナが、いくつかのｃｏｎｔｅｎｔＩｎｓｔａｎｃｅリソースを含み得る（かつ各リソースが、それ自身の暗号化されたｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ、認証タグ、証明書に関連付けられ得る）、他の場合、ＴＥＦは、ｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ完全性を検証するために、かつｃｏｎｔｅｎｔＩｎｓｔａｎｃｅを解読するために、どのようにして証明書が使用され得るかについて追加のガイダンスを提供することが可能であり得る。ソルトが送信される例では、ＴＥＦは、Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒを生成し得、それは、ＡＥ２にプロビジョニングされ得る。例では、ＡＥ２は、コンテナ特定またはｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ特定の証明書を生成するために、Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒを使用する。Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ａｕｔｈおよびＫ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｃｏｎｆ（ならびに関連付けられ

るコンテナまたはｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ特定の証明書）を生成する機構は、上で説明される機構に従って実装され得る。Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒをプロビジョニングすることの利点は、より新しいコンテンツインスタンスがＡＥ１によって生成されるかどうかにかかわらず、Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒに関連付けられる証明書存続期間が満了していない限り、ＡＥ２がＴＥＦにコンタクトする必要がないことであることが、本明細書で認識される。ＡＥ２は、ステップ１２で行われるリソース読み出しプロセスの一部としてＡＥ２が取得するＣｒｙｐｔｏＰａｒａｍｓを使用して、Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒからコンテナまたはｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ特定の証明書を生成することが可能であり得る。ある場合、Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒのプロビジョニングは、コンテンツおよびインスタンス、例えば、ＡＥ１によって生成される全てのコンテンツおよびインスタンスへのＡＥ２暗号アクセスを与え得る。したがって、このプロビジョニングは、ある場合、好ましいアプローチではないことが、本明細書で認識される。

【０１２４】

別の例示的実施形態では、ＴＥＦは、ＡＥ２に、Ｋ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ａｕｔｈおよび／またはＫ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｃｏｎｆをプロビジョニングし得、それは、次いで、コンテナ特定もしくはｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ特定の証明書を生成する。他の場合、ＴＥＦは、コンテナ特定もしくはｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ特定の証明書のみをＡＥ２にプロビジョニングすることもある。ある場合、ＡＥ２は、キーをプロビジョニングされるので、いかなるキー生成も行わない場合があり、それによって、ＡＥ２が特定のコンテナまたはｃｏｎｔｅｎｔＩｎｓｔａｎｃｅへの暗号アクセスを有することを制限する。ある場合、各キーのために、関連付けられるノンス、コンテナに関連付けられる作成時間、またはコンテンツインスタンスは、ＴＥＦに提供される必要があり得る。ある場合、ＡＥ１が４において証明書プロセスの登録を行うとき、ＡＥ１は、ＴＥＦへのＣｒｅｄｅｎｔｉａｌ－Ｉｄに関連付けられるＣｒｙｐｔＰａｒａｍｓを含み得る。

【０１２５】

性能およびセキュリティの観点から、アプローチは、ＴＥＦがＫ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ａｕｔｈおよび／またはＫ＿ＡＥ１＿ＴＥＦ＿ｄａｔａ＿ｃｏｎｆのみをＡＥ２にプロビジョンすべきであり得ることが本明細書で認識される。証明書は、それらの各々に関連付けられる、関連付けられる存続期間を有し得る。存続期間の満了後、新しい証明書が生成される必要があり得る。

【０１２６】

１７では、図示される例によると、証明書を使用して、ＡＥ２は、Ｒ１－ＡＴを使用して完全性を検証し、プロビジョニングまたは生成されたコンテナもしくはｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ証明書を使用して、Ｒ１を解読する。

【０１２７】

代替実施形態では、ノード（例えば、ＡＥ１）は、特定のクライアント（例えば、ＡＥ２）による消費のために保護され得るクライアント特定の「保護された」コンテンツを生成する。ｏｎｅＭ２Ｍでは、ＡＥが互いを認証するように直接通信しないので、ＣＳＥは、クライアント特定の（例えば、ＡＥ２）保護されたコンテンツが生成され、ＣＳＥにおいてホストされるように、ＡＥ１の代わりにクライアント特定の保護を行い得る。代替として、ＣＳＥがＡＥ１の代わりにセキュリティ機能を果たす、本明細書に説明される類似機構は、ＣＳＥ１に依拠する必要なく、ＡＥ１自体によって行われ得る。クライアント特定の保護されたコンテンツの実施形態が、ここで議論されるであろう、図３８に図示されている。

【０１２８】

上記のように、図３８は、クライアント特定のコンテンツ保護の実施形態を図示する。図３８を参照して、図示される実施形態によると、０では、ＡＥ１は、（Ｄ）ＴＬＳを使

用してＨＣＳＥと相互認証している。同様に、ＡＥ２は、（Ｄ）ＴＬＳを使用してＨＣＳＥと相互認証している。

【０１２９】

１では、図示される例によると、ＡＥ１は、コンテンツ（データ）および／またはｃｏｎｔｅｎｔＩｎｓｔａｎｃｅを生成する。さらに、ＡＥ１は、コンテンツがホスティングＣＳＥによって完全性および／または機密性のために保護されることを確実にすることを望む。２では、ＡＥ１は、コンテンツが、一意のクライアント特定の証明書を使用して、各特定のクライアントのための完全性および／または機密性のために保護されることを要求する。３では、ＨＣＳＥは、ＡＥ１によって提供されるＡＣＰを処理し、セキュアにされたコンテンツにＣＲＵＤ動作を行うことができるために承認されているクライアント（例えば、ＡＥ２）を決定する。ＨＣＳＥはまた、一意のクライアント特定の（例えば、ＡＥ２特定の）証明書が生成される必要があろうことも決定する。代替として、ＣＳＥ１は、ＡＣＰ、したがって、承認されたクライアントを決定し得る。または、ある場合、ＡＥ１によって提供されるＡＣＰは、コンテンツに対するＣＲＵＤ動作、特に、「読み出し」動作を行うことを許可されている承認されたクライアントを決定するために、サービスプロバイダによって提供されているＡＣＰと組み合わせられる。例によると、ＡＥ２が承認されたクライアントであり、ＡＥ１によって承認されていることを仮定して、ＨＣＳＥは、Ｋｐｓａ＿ＨＣＳＥ＿ＡＥ２である、ｏｎｅＭ２Ｍ　ＴＳ－０００３仕様書（リリース１）に従った遠隔プロビジョニングまたはブートストラッピングの結果としてプロビジョニングもしくは生成された事前共有キーを活用することによって、Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒを生成する。データセキュリティに使用されるマスタキー、すなわち、Ｋ＿ＨＳＣＥ＿ＡＥ２＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒは、例えば、ＲＦＣ　５８６９に基づいて、キー拡張機構を使用して生成され得る。

● Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒ＝ＨＭＡＣ－Ｈａｓｈ（Ｓａｌｔ，Ｋｐｓａ＿ＨＣＳＥ＿ＡＥ２）

● Ｔ（０）＝空の文字列（ゼロ長）

【０１３０】

４では、Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒが生成されると、これは、一意のデータ真正性およびデータ機密性キーを生成するためのキー拡張のために使用され得る。ある場合、データ真正性および機密性が、例えば、ＡＥＡＤ（例えば、ＡＥＳ－ＣＣＭまたはＡＥＳ－ＧＣＭ）等のアルゴリズムによって提供される場合、単一のキーのみが生成される。例えば、キーは、以下のように生成され得る。

● Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ａｕｔｈ＝Ｔ（１）＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒ，Ｔ（０）｜”Ｄａｔａ　Ａｕｔｈｅｎｔｉｃｉｔｙ　ａｎｄ　Ｉｎｔｅｇｒｉｔｙ”｜０ｘ０１）

● Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ａｕｔｈキーは、データ真正性およびデータ完全性を提供するために使用され、データ真正性またはデータ完全性キーと称され得る。

● Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｃｏｎｆ＝Ｔ（２）＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒ，Ｔ（１）｜”Ｄａｔａ　Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ　Ｋｅｙ”｜０ｘ０２）

【０１３１】

複数のコンテンツインスタンスを含み得るコンテンツのための単一のデータ真正性およびデータ機密性キーのみにおける、キー生成が、例の目的のために以下に示される。

● Ｋ＿ＨＣＳＥ＿ＡＥ２＿Ｃｏｎｔａｉｎｅｒ－ｘ＿ｄａｔａ＿ａｕｔｈ＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ａｕｔｈ，”Ｄａｔａ　Ａｕｔｈｅｎｔｉｃｉｔｙ　ａｎｄ　Ｉｎｔｅｇｒｉｔｙ”｜”Ｃｏｎｔａｉｎｅｒ－ｘ”｜Ｎｏｎｃｅ　ｏｒ　ｃｒｅａｔｉｏｎＴｉｍｅ）および

● Ｋ＿ＨＣＳＥ＿ＡＥ２＿Ｃｏｎｔａｉｎｅｒ－ｘ＿ｄａｔａ＿ｃｏｎｆ＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ｃｏｎｆ，”Ｄａｔａ　Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ”｜”Ｃｏｎｔａｉｎｅｒ－ｘ”｜Ｎｏｎｃｅ　ｏｒ　ｃｒｅａｔｉｏｎ

Ｔｉｍｅ）
【０１３２】
代替として、コンテナ内の各コンテンツのインスタンスのために、例えば、以下に示されるように、キーの一意の組が生成され得る。
● Ｋ＿ＨＣＳＥ＿ＡＥ２＿ＣｏｎｔｅｎｔＩｎｓｔａｎｃｅ－ｘ＿ｄａｔａ＿ａｕｔｈ＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ａｕｔｈ，”Ｄａｔａ Ａｕｔｈｅｎｔｉｃｉｔｙ ａｎｄ Ｉｎｔｅｇｒｉｔｙ”｜”Ｃｏｎｔａｉｎｅｒ－ｘ”｜Ｎｏｎｃｅ ｏｒ ｃｒｅａｔｉｏｎＴｉｍｅ）および
● Ｋ＿ＨＣＳＥ＿ＡＥ２＿ＣｏｎｔｅｎｔＩｎｓｔａｎｃｅ－ｘ＿ｄａｔａ＿ｃｏｎｆ＝ＨＭＡＣ－Ｈａｓｈ（Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ｃｏｎｆ，”Ｄａｔａ Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ”｜”ＣｏｎｔｅｎｔＩｎｓｔａｎｃｅ”｜Ｎｏｎｃｅ ｏｒ ｃｒｅａｔｉｏｎＴｉｍｅ）
【０１３３】
なおも代替として、公開キーイング機構が使用される、ある場合、クライアント特定の証明書は、識別ベースの暗号化（ＩＢＥ）機構に基づき得る。
【０１３４】
依然として図３８を参照して、５では、図示される例によると、ＡＥ２は、ＨＣＳＥからリソースＲ１（コンテナまたはｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ）を「読み出す」ことを（ある時点で）要求する。６では、ＨＣＳＥは、ＡＥ２の承認を検証する。７では、ＨＣＳＥは、暗号化されたコンテンツＥＣ－Ｒ１、認証タグ、Ｒ１－ＡＴ、および関連付けられるＣｒｙｐｔｏＰａｒａｍｓで応答する。８では、ＡＥ２は、ＣｒｙｐｔｏＰａｒａｍｓを使用し、Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ｓｅｃ＿ｍａｓｔｅｒを生成するために、ＵｓａｇｅＩｎｆｏおよび「ソルト」を抽出する。さらに、ＡＥ２は、Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ｃｏｎｆ、Ｋ＿ＨＣＳＥ＿ＡＥ２＿ｄａｔａ＿ａｕｔｈ等を生成するために要求される、ノンスおよび他のパラメータを抽出する。ＡＥ２は、次いで、コンテナ／ｃｏｎｔｅｎｔＩｎｓｔａｎｃｅ内のデータの真正性および完全性を検証し、各ｃｏｎｔａｉｎｅｒＩｎｓｔａｎｃｅ内に含まれるコンテナまたはデータ内のデータを解読するために、コンテナ特定ならびにｃｏｎｔｅｎｔＩｎｓｔａｎｃｅキーを生成し得る。
【０１３５】
したがって、図３７および３８を参照すると、図示されるノードは、プロセッサと、メモリと、通信回路とを備え得る。ノードは、その通信回路を介してネットワークに接続され得、ノードはさらに、ノードのプロセッサによって実行されると、ノードに図示および説明されるステップを行わせる、ノードのメモリ内に記憶されたコンピュータ実行可能命令を備え得る。
【０１３６】
図２７は、例示的ｃｒｅｄｅｎｔｉａｌ－Ｉｄリソースを図示する。示されるように、例示的ｃｒｅｄｅｎｔｉａｌ－Ｉｄリソースは、ｃｒｅｄｅｎｔｉａｌｓ－ＡＴを使用して、それ自体が完全性保護され、ｃｒｅｄｅｎｔｉａｌｓ－ＡＴは、作成者の証明書（例えば、ＡＥ１の秘密キー）を用いてｃｒｅｄｅｎｔｉａｌ－Ｉｄリソースの作成者によって作成され得るか、またはＳＣＨＦ（例えば、Ｈ－ＣＳＥ）によって作成され得る。例示的属性の詳細が、ここで説明され、限定ではないが、一例として提示される。
● ｃｒｅｄｅｎｔｉａｌ－Ｉｄ：これは、ドメイン内の証明書を一意に識別する。それは、大域的に一意またはローカルに一意であり、概して、証明書のスコープに基づき得る。それは、接頭辞としてランダムであるが一意の値、および接尾辞としてＦＱＤＮを使用する形態（例えば、ｘｙｚ@ｃｒｅｄｅｎｔｉａｌｓ．ｅｘａｍｐｌｅ．ｃｏｍ）、またはＵＲＩの形態（例えば、／／ｅｘａｍｐｌｅ．ｃｏｍ／ｃｒｅｄｅｎｔｉａｌｓ／ｘｙｚ）であり得る。
● ｃｒｅｄｅｎｔｉａｌ：それは、証明書に特定である子リソース属性で構成される。属性は、以下である。
○ ｃｒｅｄｅｔｉａｌＴｙｐｅ：証明書のタイプ、すなわち、対称キーまたは公開キ

ーを説明する。それは、公開キーのタイプ（例えば、ＲＳＡまたはＥＣＣ）も規定し得る。

○　ｃｒｅｄｅｎｔｉａｌ：属性は、実際の証明書値（例えば、対称キーまたは公開キー）を記憶する。注：証明書のサイズは、証明書のタイプに依存し得る。キーが公開キーである場合、関連付けられる以下を有し得る。

・　ｐｕｂｌｉｃＫｅｙＰａｒａｍｓ：パラメータは、（例えば、使用される曲線のタイプ、キーサイズ）であり得、および／または、ＪＷＫパラメータに基づき得る。これは、随意であり得る。

● ａｃｃｅｓｓＣｏｎｔｒｏｌＰｏｌｉｃｙ：ｏｎｅＭ２Ｍ定義ＡＣＰに基づく例示的ＡＣＰは、３つの属性、すなわち、ａｃｃｅｓｓＣｏｎｔｒｏｌＯｒｉｇｉｎａｔｏｒｓ、ａｃｃｅｓｓＣｏｎｔｒｏｌＯｐｅｒａｔｉｏｎｓ、およびａｃｃｅｓＣｏｎｔｒｏｌＣｏｎｔｅｘｔｓを有する。

● ｓｃｏｐｅＵｓａｇｅ：この属性は、スコープ（例えば、署名または暗号化、キー生成プロセス）を定義する。それは、どのようにして証明書が使用され得るかについての使用法を提供することも可能であり得る。証明書を使用することについての規則。

● ｖａｌｉｄｉｔｙ：ｖａｌｉｄｉｔｙ属性は、証明書に関連付けられる存続期間を示すために使用され得る。証明書は、更新される必要があり得、ＣＬＭＰは、ポリシに基づいて開始され得る。

● ｉｓｓｕｅｒ：証明書を生成して発行したエンティティ（例えば、ＦＱＤＮ）の識別。

● ｃｒｅｄｅｎｔｉａｌ－ＡＴ：この属性は、図３０に説明される、関連付けられるｃｒｙｐｔｏＰａｒａｍｓサブリソースを使用して、（ｃｒｅｄｅｎｔｉａｌ－ＡＴ属性を除く全ての属性を含む）証明書リソースに対して計算されるＡＴ値を記憶し得る。

【０１３７】

完全性保護される一般的ＡＣＰの例示的実施形態が、図２８に図示されている。図示されるＡＣＰは、関連ＡＴを有し、それは、ｃｒｙｐｔｏＰａｒａｍｓが公開キー機構の使用を規定する場合、ＡＥの秘密キーを使用して生成されていることもある。ＡＣＰを作成する任意のエンティティが、認証／完全性保護されたＡＣＰを生成できることも可能である。したがって、ＡＣＰがＣＳＥによって作成された場合、生成されるＡＴは、ＣｒｙｐｔｏＰａｒａｍｓが公開キー機構の使用を要求したならば、ＣＳＥの秘密キーに基づく。

【０１３８】

図２９は、ｃｒｙｐｔｏＰａｒａｍｓリソース内で説明される暗号化アルゴリズムおよび特定の証明書（例えば、対称キー）を使用して機密性保護される（ＥＣ－ｃｏｎｔｅｎｔＩｎｆｏ）、ｃｏｎｔｅｎｔＩｎｓｔａｎｃｅの例を図示する。それは、ＤＳもしくはＭＡＣ（例えば、ｃｏｎｔｅｎｔ－ＡＴ属性に記憶される）を用いることによっても完全性保護され得、ＤＳもしくはＭＡＣは、公開キーイング機構（例えば、コンテンツジェネレータの秘密キー）を用いて、またはマスタキー（例えば、ＫｅｙＧｅｎＫｅｙ）から生成された対称キーを用いて生成される。

【０１３９】

例示的な関連付けられるｃｒｙｐｔｏＰａｒａｍｓリソースが、図３０で描写されている。ｃｒｙｐｔｏＰａｒａｍｓリソースに関連付けられる例示的属性に関する詳細が、以下に提供され、限定ではないが、一例として提示される。

● ｃｒｙｐｔｏＰａｒａｍｓＩｄ：それは、保護されているコンテンツ／データに関連付けられる暗号パラメータを一意に識別するために使用され得る随意の属性である。

● ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ：これは、暗号化プロセスに関連付けられるパラメータを説明するサブリソースタイプである。例示的属性は、以下である。

○　ａｌｇｏｒｉｔｈｍ：使用される暗号化アルゴリズムを説明する（例えば、ＡＥＳ－１２８）。

○　ｃｒｅｄｅｎｔｉａｌ－Ｉｄ：コンテンツ（例えば、遠心分離機温度）を暗号化するために使用される証明書（例えば、キー）を読み出すために使用されるべきｃｒｅｄｅ

ｎｔｉａｌ－Ｉｄを説明する。
○　ｉｎｉｔｉａｌｉｚａｔｉｏｎＶｅｃｔｏｒ：それは、その特定のアルゴリズムのためのコンテンツを暗号化／解読するために使用される必要があるＩＶを説明する。
○　ｓｃｏｐｅＵｓａｇｅ：これは、コンテンツ／リソースを暗号化または解読するための、証明書、ＩＶ、アルゴリズムの使用法ならびにスコープを説明し得る随意の属性である。
●　ｉｎｔｅｇｒｉｔｙ：それは、コンテンツ／リソースを完全性保護することに関連付けられるパラメータを説明する、サブリソースである。属性は、以下である。
○　ｄｉｇｅｓｔＡｌｇｏｒｉｔｈｍ：ダイジェストを作成するために使用されるアルゴリズム（例えば、ＳＨＡ－１）。
○　ｓｉｇｎｉｎｇＡｌｇｏｒｉｔｈｍ：公開キーの場合にダイジェストをデジタル署名するために使用されるアルゴリズムであり、適切なアルゴリズムが、使用され得る（例えば、ＲＳＡ）一方で、対称キーの場合、適切なアルゴリズムが使用され得る（例えば、ＨＭＡＣ－ＳＨＡ－１）。対称キーの場合、ｄｉｇｅｓｔＡｌｇｏｒｉｔｈｍがＫｅｙｅｄ－Ｈａｓｈ－ＭＡＣアルゴリズム（例えば、ＨＭＡＣ－ＳＨＡ－２５６）によって置換されることが可能であり得る。ここで説明される例は、公開キー機構を使用するが、しかしながら、類似機構が、対称キーに使用され得る。
○　ｃｒｅｄｅｎｔｉａｌ－Ｉｄ：コンテンツ／リソースに関連付けられるＡＴを作成するための証明書（例えば、キー）を読み出すために使用されるべきｃｒｅｄｅｎｔｉａｌ－Ｉｄ（例えば、ｃｒｅｄ２@ｖｅｒｉｓｉｇｎ．ｃｏｍ）を説明する。
○　ｎｏｎｃｅ：この値は、リプレイ保護のために使用され、コンテンツ／リソースの作成に関連付けられるランダムに生成された値または時間／日付を含み得る。
○　ｓｃｏｐｅＵｓａｇｅ：これは、コンテンツ／リソースのＡＴを作成するために、証明書、ノンス、およびアルゴリズムの使用法を説明し得る随意の属性である。
●　ｃｒｔｙｐｏｔｏＰａｒａｍｓ－ＡＴ：これは、関連付けられるｃｒｙｐｔｏＰａｒａｍｓサブリソースを使用して、ｃｒｙｐｔｏＰａｒａｍｓＩｄ：ｃｐ＿ｔｅｍ＿ｃｅｎｔ＿３０＿２０／１０／１５）によって識別されるｃｒｙｐｔｏＰａｒａｍｓリソースに関連付けられるＡＴである。

【０１４０】

完全性および真正性のために保護される＜ｍｇｍｔＯｂｊ＞リソースの例が、図３１に図示されている。例示的セキュリティポリシリソースが、図３２に図示されている。

【０１４１】

例示的実施形態によると、コンテンツセキュリティに関連付けられるポリシおよびセキュリティパラメータの構成が、グラフィカルユーザインターフェース（ＧＵＩ）を使用して、ユーザによって行われ得る。代替として、ウェブインターフェースが、ＧＵＩの代わりに、またはそれに加えて、使用され得る。例示的ユーザインターフェース（ＵＩ）が、図３３に示されている。例えば、ＵＩが、限定ではないが、以下のために使用され得る。
●　コンテンツセキュリティに関するセキュリティポリシの構成。
●　以下を行う能力をユーザに提供する。
○　コンテンツを構成するものを定義する。
○　コンテンツの構造を定義する。
●　コンテンツ／コンテンツタイプに基づいてセキュリティ要件を定義する。
●　ユーザがセキュリティ要件を構成する／関連付けられるセキュリティパラメータにマップすることができるように、ユーザによって使用され得るテーブルを表示する。
●　コンテンツライフサイクルパラメータ（より具体的にはセキュリティパラメータ）の構成。
●　信頼できるＳＣＨＦを識別するために使用されるパラメータを定義する。

【０１４２】

種々のＵＩが、ＳＣＨＦにおいて提供され得る。図３４は、限定ではないが、一例として提示される、以下を含む、ＳＣＨＦにおいて提供され得る例示的ＵＩを示す。

● コンテンツセキュリティに関するセキュリティポリシの構成のためのＵＩ。
● コンテンツライフサイクルパラメータ（より具体的にはセキュリティパラメータ）の構成のためのＵＩ。
● その（ＳＣＨＦの）信頼性を定義するために使用されるパラメータを定義するためのＵＩ。

【０１４３】

図３５は、限定ではないが、一例として提示される、ＳＥＦにおいて提供され得る例示的ＵＩを図示する。

● コンテンツセキュリティ関連証明書請求および登録に関するセキュリティポリシの構成のためのＵＩ。
● 証明書関連パラメータの構成のためのＵＩ。

【０１４４】

例示的ユーザインターフェースが、所望に応じて代替的パラメータを監視して制御するために使用され得ることが理解されるであろう。ＧＵＩが、種々のチャートまたは代替的視覚描写を介して、ユーザが関心を持つ種々の情報をユーザに提供できることがさらに理解されるであろう。

【０１４５】

図３６Ａは、１つ以上の開示される実施形態が実装され得る、例示的マシンツーマシン（Ｍ２Ｍ）、モノのインターネット（ＩｏＴ）、もしくはモノのウェブ（ＷｏＴ）通信システム１０の略図である。概して、Ｍ２Ｍ技術は、ＩｏＴ／ＷｏＴのための基礎的要素を提供し、任意のＭ２Ｍデバイス、Ｍ２Ｍゲートウェイ、またはＭ２Ｍサービスプラットフォームは、ＩｏＴ／ＷｏＴのコンポーネントならびにＩｏＴ／ＷｏＴサービス層等であり得る。図６－３５、３７、および３８のうちのいずれかに図示されるクライアントまたはエンティティのうちのいずれかは、図３６Ａ－Ｄに図示されるもの等の通信システムのノードを備え得る。

【０１４６】

図３６Ａに示されるように、Ｍ２Ｍ／ＩｏＴ／ＷｏＴ通信システム１０は、通信ネットワーク１２を含む。通信ネットワーク１２は、固定ネットワーク（例えば、Ｅｔｈｅｒｎｅｔ（登録商標）、Ｆｉｂｅｒ、ＩＳＤＮ、ＰＬＣ等）、または無線ネットワーク（例えば、ＷＬＡＮ、セルラー等）、もしくは異種ネットワークのネットワークであり得る。例えば、通信ネットワーク１２は、音声、データ、ビデオ、メッセージング、ブロードキャスト等のコンテンツを複数のユーザに提供する複数のアクセスネットワークを備え得る。例えば、通信ネットワーク１２は、符号分割多重アクセス（ＣＤＭＡ）、時分割多重アクセス（ＴＤＭＡ）、周波数分割多重アクセス（ＦＤＭＡ）、直交ＦＤＭＡ（ＯＦＤＭＡ）、単一キャリアＦＤＭＡ（ＳＣ－ＦＤＭＡ）等の１つ以上のチャネルアクセス方法を採用し得る。さらに、通信ネットワーク１２は、例えば、コアネットワーク、インターネット、センサネットワーク、工業制御ネットワーク、パーソナルエリアネットワーク、融合個人ネットワーク、衛星ネットワーク、ホームネットワーク、または企業ネットワーク等の他のネットワークを備え得る。

【０１４７】

図３６Ａに示されるように、Ｍ２Ｍ／ＩｏＴ／ＷｏＴ通信システム１０は、インフラストラクチャドメインと、フィールドドメインとを含み得る。インフラストラクチャドメインは、エンドツーエンドＭ２Ｍ展開のネットワーク側を指し、フィールドドメインは、通常、Ｍ２Ｍゲートウェイの背後にあるエリアネットワークを指す。フィールドドメインおよびインフラストラクチャドメインは両方とも、ネットワークの種々の異なるノード（例えば、サーバ、ゲートウェイ、デバイス）を備え得る。例えば、フィールドドメインは、Ｍ２Ｍゲートウェイ１４と、端末デバイス１８とを含み得る。任意の数のＭ２Ｍゲートウェイデバイス１４およびＭ２Ｍ端末デバイス１８が、所望に応じてＭ２Ｍ／ＩｏＴ／ＷｏＴ通信システム１０に含まれ得ることが理解されるであろう。Ｍ２Ｍゲートウェイデバイス１４およびＭ２Ｍ端末デバイス１８の各々は、通信ネットワーク１２または直接無線リ

ンクを介して、信号を伝送ならびに受信するように構成される。Ｍ２Ｍゲートウェイデバイス１４は、無線Ｍ２Ｍデバイス（例えば、セルラーおよび非セルラー）ならびに固定ネットワークＭ２Ｍデバイス（例えば、ＰＬＣ）が、通信ネットワーク１２等のオペレータネットワークを通して、または直接無線リンクを通してのいずれかで、通信することを可能にする。例えば、Ｍ２Ｍデバイス１８は、データを収集し、通信ネットワーク１２または直接無線リンクを介して、データをＭ２Ｍアプリケーション２０もしくはＭ２Ｍデバイス１８に送信し得る。Ｍ２Ｍデバイス１８はまた、Ｍ２Ｍアプリケーション２０またはＭ２Ｍデバイス１８からデータを受信し得る。さらに、データおよび信号は、以下で説明されるように、Ｍ２Ｍサービス層２２を介して、Ｍ２Ｍアプリケーション２０に送信され、そこから受信され得る。Ｍ２Ｍデバイス１８およびゲートウェイ１４は、例えば、セルラー、ＷＬＡＮ、ＷＰＡＮ（例えば、Ｚｉｇｂｅｅ（登録商標）、６ＬｏＷＰＡＮ、Ｂｌｕｅｔｏｏｔｈ（登録商標））、直接無線リンク、および有線を含む種々のネットワークを介して通信し得る。例示的Ｍ２Ｍデバイスは、タブレット、スマートフォン、医療デバイス、温度および気象モニタ、コネクテッドカー、スマートメータ、ゲームコンソール、携帯情報端末、保健および健康モニタ、照明、サーモスタット、電化製品、ガレージドア、および他のアクチュエータベースのデバイス、セキュリティデバイス、ならびにスマートコンセントを含むが、それらに限定されない。

【０１４８】

図３６Ｂを参照すると、フィールドドメイン内の図示されるＭ２Ｍサービス層２２は、Ｍ２Ｍアプリケーション２０、Ｍ２Ｍゲートウェイデバイス１４、およびＭ２Ｍ端末デバイス１８ならびに通信ネットワーク１２のためのサービスを提供する。Ｍ２Ｍサービス層２２は、所望に応じて、任意の数のＭ２Ｍアプリケーション、Ｍ２Ｍゲートウェイデバイス１４、Ｍ２Ｍ端末デバイス１８、および通信ネットワーク１２と通信し得ることが理解されるであろう。Ｍ２Ｍサービス層２２は、１つ以上のサーバ、コンピュータ等によって実装され得る。Ｍ２Ｍサービス層２２は、Ｍ２Ｍ端末デバイス１８、Ｍ２Ｍゲートウェイデバイス１４、およびＭ２Ｍアプリケーション２０に適用されるサービス能力を提供する。Ｍ２Ｍサービス層２２の機能は、例えば、ウェブサーバとして、セルラーコアネットワークで、クラウドで等の種々の方法で実装され得る。

【０１４９】

図示されるＭ２Ｍサービス層２２と同様に、インフラストラクチャドメイン内にＭ２Ｍサービス層２２’がある。Ｍ２Ｍサービス層２２’は、インフラストラクチャドメイン内のＭ２Ｍアプリケーション２０’および下層通信ネットワーク１２’のためのサービスを提供する。Ｍ２Ｍサービス層２２’は、フィールドドメイン内のＭ２Ｍゲートウェイデバイス１４およびＭ２Ｍ端末デバイス１８のためのサービスも提供する。Ｍ２Ｍサービス層２２’は、任意の数のＭ２Ｍアプリケーション、Ｍ２Ｍゲートウェイデバイス、およびＭ２Ｍ端末デバイスと通信し得ることが理解されるであろう。Ｍ２Ｍサービス層２２’は、異なるサービスプロバイダによってサービス層と相互作用し得る。Ｍ２Ｍサービス層２２’は、１つ以上のサーバ、コンピュータ、仮想マシン（例えば、クラウド／計算／記憶ファーム等）等によって実装され得る。

【０１５０】

依然として図３６Ｂを参照すると、Ｍ２Ｍサービス層２２および２２’は、多様なアプリケーションならびにバーティカルが活用することができるサービス配信能力のコアの組を提供する。これらのサービス能力は、Ｍ２Ｍアプリケーション２０および２０’がデバイスと相互作用し、データ収集、データ分析、デバイス管理、セキュリティ、課金、サービス／デバイス発見等の機能を果たすことを可能にする。本質的に、これらのサービス能力は、これらの機能性を実装する負担をアプリケーションから取り除き、したがって、アプリケーション開発を単純化し、市場に出すコストおよび時間を削減する。サービス層２２および２２’は、Ｍ２Ｍアプリケーション２０および２０’が、サービス層２２および２２’が提供するサービスと関連して、種々のネットワーク１２および１２’を通して通信することも可能にする。

【０１５１】
Ｍ２Ｍアプリケーション２０および２０’は、限定ではないが、輸送、保健および健康、コネクテッドホーム、エネルギー管理、アセット追跡、ならびにセキュリティおよび監視等の種々の産業での用途を含み得る。上記のように、システムのデバイス、ゲートウェイ、および他のサーバを横断して起動するＭ２Ｍサービス層は、例えば、データ収集、デバイス管理、セキュリティ、課金、場所追跡／ジオフェンシング、デバイス／サービス発見、およびレガシーシステム統合等の機能をサポートし、サービスとしてこれらの機能をＭ２Ｍアプリケーション２０および２０’に提供する。
【０１５２】
概して、図３６Ａならびに３６Ｂに図示されるサービス層２２および２２’等のサービス層（ＳＬ）は、アプリケーションプログラミングインターフェース（ＡＰＩ）および下層ネットワーキングインターフェースの組を通して付加価値サービス能力をサポートするソフトウェアミドルウェア層を定義する。ＥＴＳＩ　Ｍ２Ｍおよびｏｎｅ Ｍ２Ｍアーキテクチャは両方とも、サービス層を定義する。ＥＴＳＩ　Ｍ２Ｍのサービス層は、サービス能力層（ＳＣＬ）と称される。ＳＣＬは、ＥＴＳＩ　Ｍ２Ｍアーキテクチャの種々の異なるノードで実装され得る。例えば、サービス層のインスタンスは、Ｍ２Ｍデバイス（デバイスＳＣＬ（ＤＳＣＬ）と称される）、ゲートウェイ（ゲートウェイＳＣＬ（ＧＳＣＬ）と称される）、および／またはネットワークノード（ネットワークＳＣＬ（ＮＳＣＬ）と称される）内で実装され得る。ｏｎｅＭ２Ｍサービス層は、共通サービス機能（ＣＳＦ）（すなわち、サービス能力）の組をサポートする。１つ以上の特定のタイプのＣＳＦの組のインスタンス化は、異なるタイプのネットワークノード（例えば、インフラストラクチャノード、中間ノード、特定用途向けノード）上でホストされ得る共通サービスエンティティ（ＣＳＥ）と称される。第３世代パートナーシッププロジェクト（３ＧＰＰ）は、マシンタイプ通信（ＭＴＣ）のためのアーキテクチャも定義している。そのアーキテクチャでは、サービス層およびそれが提供するサービス能力は、サービス能力サーバ（ＳＣＳ）の一部として実装される。ＥＴＳＩ　Ｍ２ＭアーキテクチャのＤＳＣＬ、ＧＳＣＬ、もしくはＮＳＣＬで、３ＧＰＰ　ＭＴＣアーキテクチャのサービス能力サーバ（ＳＣＳ）で、ｏｎｅＭ２ＭアーキテクチャのＣＳＦもしくはＣＳＥで、またはネットワークのある他のノードで具現化されるかどうかにかかわらず、サービス層のインスタンスが、サーバ、コンピュータ、および他のコンピューティングデバイスもしくはノードを含む、ネットワーク内の１つ以上の独立型ノード上で、もしくは１つ以上の既存のノードの一部としてのいずれかで実行する論理エンティティ（例えば、ソフトウェア、コンピュータ実行可能命令等）で実装され得る。例として、サービス層またはそのコンポーネントのインスタンスは、以下で説明される図３６Ｃまたは３６Ｄに図示される一般的アーキテクチャを有する、ネットワークノード（例えば、サーバ、コンピュータ、ゲートウェイ、デバイス等）上で起動するソフトウェアの形態で実装され得る。
【０１５３】
さらに、本明細書に説明される方法および機能性は、例えば、上記のネットワークおよびアプリケーション管理サービス等のサービスにアクセスするために、サービス指向アーキテクチャ（ＳＯＡ）および／またはリソース指向アーキテクチャ（ＲＯＡ）を使用するＭ２Ｍネットワークの一部として実装され得る。
【０１５４】
図３６Ｃは、図３６Ａおよび３６Ｂに図示されるもの等のＭ２Ｍネットワーク内のＭ２Ｍサーバ、ゲートウェイ、デバイス、または他のノードとして動作し得る、図６－３５、３７、および３８に図示されるクライアントまたはエンティティのうちの１つ等のネットワークのノードの例示的ハードウェア／ソフトウェアアーキテクチャのブロック図である。図３６Ｃに示されるように、ノード３０は、プロセッサ３２と、送受信機３４と、伝送／受信要素３６と、スピーカ／マイクロホン３８と、キーパッド４０と、ディスプレイ／タッチパッド４２と、非取り外し可能メモリ４４と、取り外し可能メモリ４６と、電源４８と、全地球測位システム（ＧＰＳ）チップセット５０と、他の周辺機器５２とを含み得

る。ノード３０はまた、送受信機３４および伝送／受信要素３６等の通信回路を含み得る。ノード３０は、実施形態と一致したままで、先述の要素の任意の副次的組み合わせを含み得ることが理解されるであろう。このノードは、本明細書に説明されるセキュリティ保護およびそれに関連する方法を実装するノードであり得る。

【０１５５】

プロセッサ３２は、汎用プロセッサ、特殊目的プロセッサ、従来のプロセッサ、デジタル信号プロセッサ（ＤＳＰ）、複数のマイクロプロセッサ、ＤＳＰコアに関連付けられた１つ以上のマイクロプロセッサ、コントローラ、マイクロコントローラ、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）回路、任意の他のタイプの集積回路（ＩＣ）、状態マシン等であり得る。プロセッサ３２は、信号符号化、データ処理、電力制御、入出力処理、および／またはノード３０が無線環境で動作することを可能にする任意の他の機能性を果たし得る。プロセッサ３２は、伝送／受信要素３６に結合され得る送受信機３４に結合され得る。図３６Ｃは、プロセッサ３２および送受信機３４を別個のコンポーネントとして描写するが、プロセッサ３２および送受信機３４は、電子パッケージまたはチップに一緒に統合され得ることが理解されるであろう。プロセッサ３２は、アプリケーション層プログラム（例えば、ブラウザ）および／または無線アクセス層（ＲＡＮ）プログラムならびに／もしくは通信を行い得る。プロセッサ３２は、例えば、アクセス層および／またはアプリケーション層等で、認証、セキュリティキー一致、ならびに／もしくは暗号化動作等のセキュリティ動作を行い得る。

【０１５６】

図３６Ｃに示されるように、プロセッサ３２は、その通信回路（例えば、送受信機３４および伝送／受信要素３６）に結合される。プロセッサ３２は、コンピュータ実行可能命令の実行を通して、それが接続されるネットワークを介してノード３０を他のノードと通信させるために、通信回路を制御し得る。具体的には、プロセッサ３２は、（例えば、図６－３５、３７、および３８で）本明細書ならびに請求項に説明される、伝送および受信するステップを行うために、通信回路を制御し得る。図３６Ｃは、プロセッサ３２および送受信機３４を別個のコンポーネントとして描写するが、プロセッサ３２および送受信機３４は、電子パッケージまたはチップに一緒に統合され得ることが理解されるであろう。

【０１５７】

伝送／受信要素３６は、Ｍ２Ｍサーバ、ゲートウェイ、デバイス等を含む他のノードに信号を伝送するように、またはそこから信号を受信するように構成され得る。例えば、実施形態では、伝送／受信要素３６は、ＲＦ信号を伝送および／または受信するように構成されるアンテナであり得る。伝送／受信要素３６は、ＷＬＡＮ、ＷＰＡＮ、セルラー等の種々のネットワークならびにエアインターフェースをサポートし得る。実施形態では、伝送／受信要素３６は、例えば、ＩＲ、ＵＶ、もしくは可視光信号を伝送および／または受信するように構成されるエミッタ／検出器であり得る。さらに別の実施形態では、伝送／受信要素３６は、ＲＦおよび光信号の両方を伝送ならびに受信するように構成され得る。伝送／受信要素３６は、無線もしくは有線信号の任意の組み合わせを伝送および／または受信するように構成され得ることが理解されるであろう。

【０１５８】

加えて、伝送／受信要素３６は、単一の要素として図３６Ｃで描写されているが、ノード３０は、任意の数の伝送／受信要素３６を含み得る。より具体的には、ノード３０は、ＭＩＭＯ技術を採用し得る。したがって、実施形態では、ノード３０は、無線信号を伝送および受信するための２つ以上の伝送／受信要素３６（例えば、複数のアンテナ）を含み得る。

【０１５９】

送受信機３４は、伝送／受信要素３６によって伝送される信号を変調するように、および伝送／受信要素３６によって受信される信号を復調するように構成され得る。上記のように、ノード３０は、マルチモード能力を有し得る。したがって、送受信機３４は、ノード３０が、例えば、ＵＴＲＡおよびＩＥＥＥ　８０２．１１等の複数のＲＡＴを介して通

信することを可能にするための複数の送受信機を含み得る。

【０１６０】

プロセッサ３２は、非取り外し可能メモリ４４および／または取り外し可能メモリ４６等の任意のタイプの好適なメモリから情報にアクセスし、その中にデータを記憶し得る。非取り外し可能メモリ４４は、ランダムアクセスメモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、ハードディスク、または任意の他のタイプのメモリ記憶デバイスを含み得る。取り外し可能メモリ４６は、加入者識別モジュール（ＳＩＭ）カード、メモリスティック、セキュアデジタル（ＳＤ）メモリカード等を含み得る。他の実施形態では、プロセッサ３２は、サーバまたはホームコンピュータ上等のノード３０上に物理的に位置しないメモリから情報にアクセスし、その中にデータを記憶し得る。プロセッサ３２は、ＵＥ（例えば、ＧＵＩ１４００参照）、具体的には、ＵＥと通信する下層ネットワーク、アプリケーション、または他のサービスのステータスを反映するために、ディスプレイもしくはインジケータ４２上の照明パターン、画像、もしくは色を制御するように構成され得る。プロセッサ３２は、電源４８から電力を受け取り得、ノード３０内の他のコンポーネントへの電力を分配および／または制御するように構成され得る。電源４８は、ノード３０に給電するための任意の好適なデバイスであり得る。例えば、電源４８は、１つ以上の乾電池バッテリ（例えば、ニッケルカドミウム（ＮｉＣｄ）、ニッケル亜鉛（ＮｉＺｎ）、ニッケル水素（ＮｉＭＨ）、リチウムイオン（Ｌｉ－ｉｏｎ）等）、太陽電池、燃料電池等を含み得る。

【０１６１】

プロセッサ３２はまた、ノード３０の現在の場所に関する場所情報（例えば、経度および緯度）を提供するように構成されるＧＰＳチップセット５０に結合され得る。ノード３０は、実施形態と一致したままで、任意の好適な場所決定方法を介して場所情報を獲得し得ることが理解されるであろう。

【０１６２】

プロセッサ３２はさらに、追加の特徴、機能性、および／または有線もしくは無線コネクティビティを提供する、１つ以上のソフトウェアならびに／もしくはハードウェアモジュールを含み得る他の周辺機器５２に結合され得る。例えば、周辺機器５２は、加速度計、ｅ－コンパス、衛星送受信機、センサ、デジタルカメラ（写真またはビデオ用）、ユニバーサルシリアルバス（ＵＳＢ）ポートまたは他の相互接続インターフェース、振動デバイス、テレビ送受信機、ハンズフリーヘッドセット、Ｂｌｕｅｔｏｏｔｈ（登録商標）モジュール、周波数変調（ＦＭ）ラジオユニット、デジタル音楽プレーヤ、メディアプレーヤ、ビデオゲームプレーヤモジュール、インターネットブラウザ等を含み得る。

【０１６３】

図３６Ｄは、図３６Ａおよび３６Ｂに図示されるもの等のＭ２Ｍネットワーク内のＭ２Ｍサーバ、ゲートウェイ、デバイス、または他のノードとして動作し得る、図６－３５、３７、および３８に図示されるクライアントもしくはエンティティ等のネットワークの１つ以上のノードを実装するためにも使用され得る例示的コンピューティングシステム９０のブロック図である。コンピューティングシステム９０は、コンピュータまたはサーバを備え得、主に、そのようなソフトウェアが記憶またはアクセスされる場所もしくは手段にかかわらず、ソフトウェアの形態であり得るコンピュータ読み取り可能な命令によって制御され得る。そのようなコンピュータ読み取り可能な命令は、コンピューティングシステム９０を稼働させるように、中央処理装置（ＣＰＵ）９１内で実行され得る。多くの既知のワークステーション、サーバ、およびパーソナルコンピュータでは、中央処理装置９１は、マイクロプロセッサと呼ばれる単一チップＣＰＵによって実装される。他のマシンでは、中央処理装置９１は、複数のプロセッサを備え得る。コプロセッサ８１は、追加の機能を果たす、またはＣＰＵ９１を支援する、主要ＣＰＵ９１とは異なる随意のプロセッサである。ＣＰＵ９１および／またはコプロセッサ８１は、セキュリティ保護のための開示されるシステムおよび方法に関連するデータを受信、生成、ならびに処理し得る。

【０１６４】

動作時、ＣＰＵ９１は、命令をフェッチ、復号、および実行し、コンピュータの主要データ転送パスであるシステムバス８０を介して、情報を他のリソースへ、ならびにそこから転送する。そのようなシステムバスは、コンピューティングシステム９０内のコンポーネントを接続し、データ交換のための媒体を定義する。システムバス８０は、典型的には、データを送信するためのデータラインと、アドレスを送信するためのアドレスラインと、インタラプトを送信するため、およびシステムバスを動作させるための制御ラインとを含む。そのようなシステムバス８０の例は、ＰＣＩ（周辺コンポーネント相互接続）バスである。

【０１６５】

システムバス８０に結合されるメモリデバイスは、ランダムアクセスメモリ（ＲＡＭ）８２と、読み取り専用メモリ（ＲＯＭ）９３とを含む。そのようなメモリは、情報が記憶され、読み出されることを可能にする回路を含む。ＲＯＭ９３は、概して、容易に修正されることができない記憶されたデータを含む。ＲＡＭ８２に記憶されたデータは、ＣＰＵ９１または他のハードウェアデバイスによって読み取られること、または変更されることができる。ＲＡＭ８２および／またはＲＯＭ９３へのアクセスは、メモリコントローラ９２によって制御され得る。メモリコントローラ９２は、命令が実行されると、仮想アドレスを物理的アドレスに変換するアドレス変換機能を提供し得る。メモリコントローラ９２はまた、システム内のプロセスを隔離し、ユーザプロセスからシステムプロセスを隔離するメモリ保護機能を提供し得る。したがって、第１のモードで起動するプログラムは、それ自身のプロセス仮想アドレス空間によってマップされるメモリのみにアクセスすることができ、プロセス間のメモリ共有が設定されていない限り、別のプロセスの仮想アドレス空間内のメモリにアクセスすることができない。

【０１６６】

加えて、コンピューティングシステム９０は、ＣＰＵ９１からプリンタ９４、キーボード８４、マウス９５、およびディスクドライブ８５等の周辺機器に命令を通信する責任がある周辺機器コントローラ８３を含み得る。

【０１６７】

ディスプレイコントローラ９６によって制御されるディスプレイ８６は、コンピューティングシステム９０によって生成される視覚出力を表示するために使用される。そのような視覚出力は、テキスト、グラフィックス、動画グラフィックス、およびビデオを含み得る。ディスプレイ８６は、ＣＲＴベースのビデオディスプレイ、ＬＣＤベースのフラットパネルディスプレイ、ガスプラズマベースのフラットパネルディスプレイ、またはタッチパネルを伴って実装され得る。ディスプレイコントローラ９６は、ディスプレイ８６に送信されるビデオ信号を生成するために要求される電子コンポーネントを含む。

【０１６８】

さらに、コンピューティングシステム９０は、コンピューティングシステム９０がネットワークの他のノードと通信することを可能にするように、図３６Ａおよび図３６Ｂのネットワーク１２等の外部通信ネットワークにコンピューティングシステム９０を接続するために使用され得る通信回路（例えば、ネットワークアダプタ９７等）を含み得る。通信回路は、単独で、またはＣＰＵ９１と組み合わせて、（例えば、図６－３５、３７、および３８で）本明細書ならびに請求項に説明される伝送および受信するステップを行うために使用され得る。

【０１６９】

本明細書に説明される方法およびプロセスのうちのいずれかは、コンピュータ読み取り可能な記憶媒体上に記憶されたコンピュータ実行可能命令（すなわち、プログラムコード）の形態で具現化され得、その命令は、コンピュータ、サーバ、Ｍ２Ｍ端末デバイス、Ｍ２Ｍゲートウェイデバイス等のマシンによって実行されると、本明細書に説明されるシステム、方法、およびプロセスを実施ならびに／または実装することが理解されるであろう。具体的には、上で説明されるステップ、動作、または機能のうちのいずれかは、そのようなコンピュータ実行可能命令の形態で実装され得る。コンピュータ読み取り可能な記憶

媒体は、情報の記憶のための任意の方法または技術で実装される揮発性および不揮発性媒体、取り外し可能および非取り外し可能媒体の両方を含むが、そのようなコンピュータ読み取り可能な記憶媒体は、信号を含まない。コンピュータ読み取り可能な記憶媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリもしくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）もしくは他の光学ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置もしくは他の磁気記憶デバイス、または所望の情報を記憶するために使用されることができ、かつコンピュータによってアクセスされることができる任意の他の物理的媒体を含むが、それらに限定されない。

【０１７０】

図で図示されるような本開示の主題の好ましい実施形態を説明する上で、具体的用語が、明確にするために採用される。しかしながら、請求される主題は、そのように選択された具体的用語に限定されることを意図せず、各具体的要素は、類似目的を達成するように同様に動作する全ての技術的均等物を含むことを理解されたい。

【０１７１】

以下は、上記の説明の中で出現し得る、サービスレベル技術に関する頭字語のリストである。別様に規定されない限り、本明細書で使用される頭字語は、以下に列挙される対応する用語を指す。

【０１７２】

【表６－１】

ACP	アクセス制御ポリシ
AE	アプリケーションエンティティ
AEAD	関連付けられるデータを用いた認証された暗号化
AES	高度暗号化規格
AES－GCM	AES－Galoisモード
Cert	デジタル証明
CCF	コンテンツ作成機能
CCP	コンテンツ作成プロセス
CCSDF	コンテンツ作成およびセキュリティ決定機能
CDB	証明書データベース
CHF	コンテンツホスティング機能
CLMP	コンテンツライフサイクル管理プロセス
CR	証明書レジストリ
CGP	証明書登録プロセス
CQP	証明書請求プロセス
CP	コンテンツ処理
CRP	コンテンツ読み出しプロセス
CRRP	証明書請求および登録プロセス
DES	デジタル暗号化規格
DS	デジタル署名
DTLS	データグラムトランスポート層セキュリティ
ECC	楕円曲線暗号化
E2E	エンドツーエンド
IoT	モノのインターネット
IPSec	インターネットプロトコルセキュリティ
JWA	JSONウェブアルゴリズム
JWE	JSONウェブ暗号化
JWK	JSONウェブキー
JWS	JSONウェブ署名
JWT	JSONウェブトークン
KDF	キー導出関数
M2M	マシンツーマシン

【０１７３】

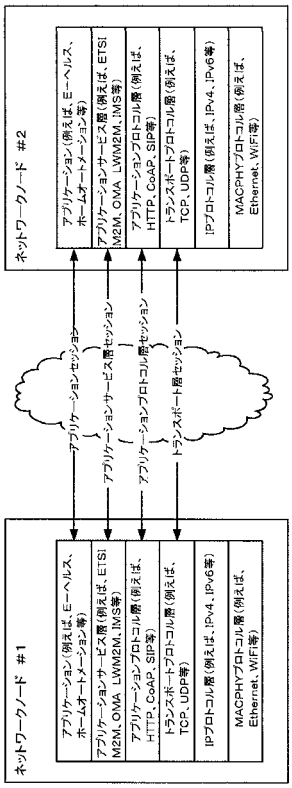
【表６－２】

MAC	メッセージ認証コード
MEF	M2M登録機能
NTP	ネットワークタイムプロトコル
PCS	保護コンテンツ記憶部
PKI	公開キーインフラストラクチャ
PSK	事前共有キー
RoT	信頼のルート
RSA	Rivest－Shamir－Addlemanアルゴリズム
SCHF	セキュアコンテンツホスティング機能
SDF	セキュリティ決定機能
SE	セキュア要素
SEF	サービス有効化機能
SESC	サービス有効化およびセキュリティ構成
SHRP	セキュアホスティング請求プロセス
SL	サービス層
SP	サービスプロバイダ
SPDP	セキュリティパラメータ決定機能
TEE	信頼される実行環境
TLS	トランスポート層セキュリティ
TTP	信頼される第三者

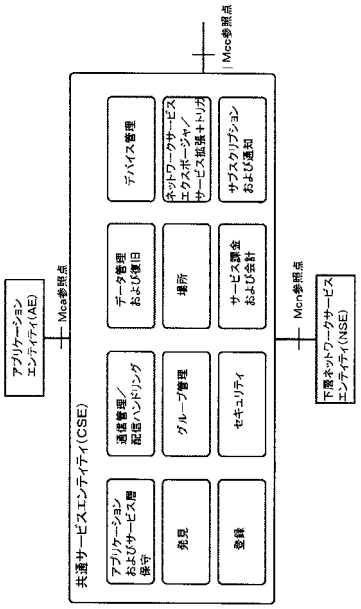
【０１７４】

本明細書は、最良の様態を含む、本発明を開示するために、また、当業者が、任意のデバイスまたはシステムを作製して使用することと、任意の組み込まれた方法を行うこととを含む、本発明を実践することを可能にするために、例を使用する。本発明の特許性のある範囲は、請求項によって定義され、当業者に想起される他の例を含み得る。そのような他の例は、請求項の文字通りの用語と異ならない構造要素を有する場合、または請求項の文字通りの用語からごくわずかな差異を伴う同等の構造要素を含む場合、請求項の範囲内であることを意図している。

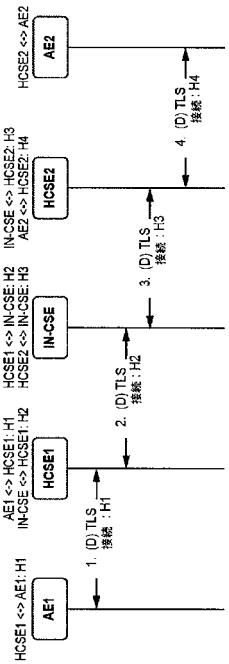
【図１】


ネットワークノード #2
アプリケーション（例えば、E-ヘルス、ホームオートメーション等）
アプリケーションサービス層（例えば、ETSI M2M、OMA LWM2M、IMS等）
アプリケーションプロトコル層（例えば、HTTP、CoAP、SIP等）
トランスポートプロトコル層（例えば、TCP、UDP等）
IPプロトコル層（例えば、IPv4、IPv6等）
MAC/PHYプロトコル層（例えば、Ethernet、WiFi等）
アプリケーションセッション
アプリケーションサービス層セッション
アプリケーションプロトコル層セッション
トランスポート層セッション
ネットワークノード #1
アプリケーション（例えば、E-ヘルス、ホームオートメーション等）
アプリケーションサービス層（例えば、ETSI M2M、OMA LWM2M、IMS等）
アプリケーションプロトコル層（例えば、HTTP、CoAP、SIP等）
トランスポートプロトコル層（例えば、TCP、UDP等）
IPプロトコル層（例えば、IPv4、IPv6等）
MAC/PHYプロトコル層（例えば、Ethernet、WiFi等）

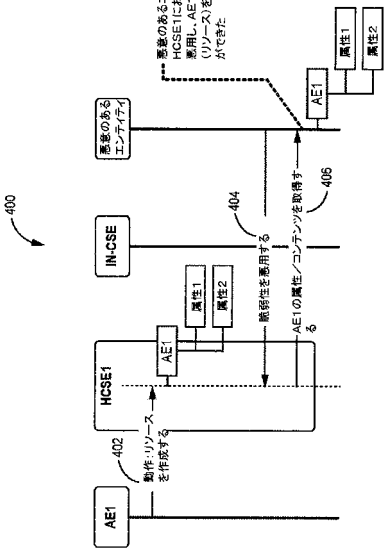
【図２】


アプリケーションエンティティ(AE)
Mca参照点
共通サービスエンティティ(CSE)
アプリケーションおよびサービス層保守
通信管理／配信ハンドリング
データ管理および蓄積
デバイス管理
発見
グループ管理
場所
ネットワークサービスエクスポージャ／サービス拡張＋トリガ
登録
セキュリティ
サービス課金および会計
サブスクリプションおよび通知
Mcn参照点
Mcc参照点
下層ネットワークサービスエンティティ(NSE)

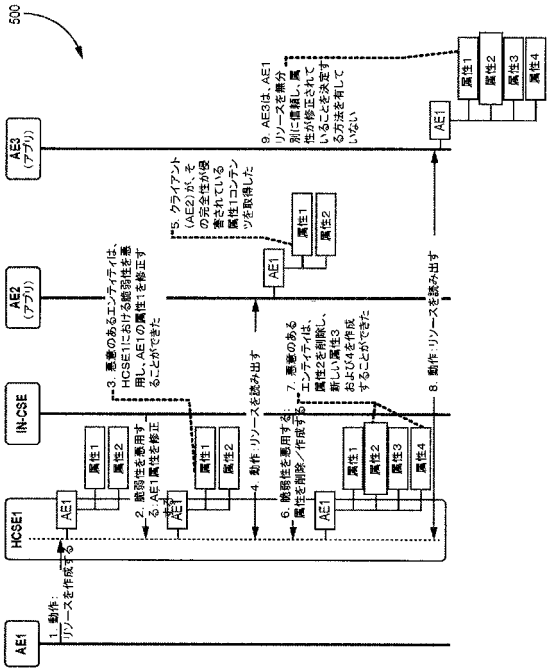
【図３】


HCSE1 <-> AE1: H1
AE1 <-> HCSE1: H1
IN-CSE <-> HCSE1: H2
HCSE1 <-> IN-CSE: H2
HCSE2 <-> IN-CSE: H3
IN-CSE <-> HCSE2: H3
AE2 <-> HCSE2: H4
HCSE2 <-> AE2
AE1
HCSE1
IN-CSE
HCSE2
AE2
1. (D) TLS 接続：H1
2. (D) TLS 接続：H2
3. (D) TLS 接続：H3
4. (D) TLS 接続：H4

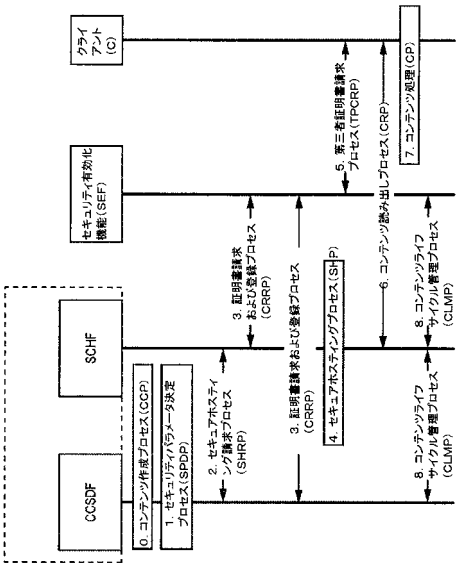
【図４】


400
悪意のあるエンティティは、HCSE1における脆弱性を悪用し、AE1のコンテンツ（リソース）を取得することができた
悪意のあるエンティティ
AE1
IN-CSE
HCSE1
AE1'
属性1
属性2
402
動作：リソースを作成する
脆弱性を悪用する
404
AE1の属性／コンテンツを取得する
406

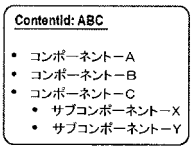
【図５】



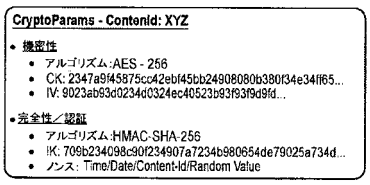
【図６】



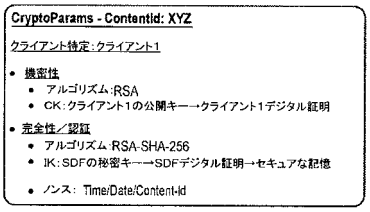
【図７】



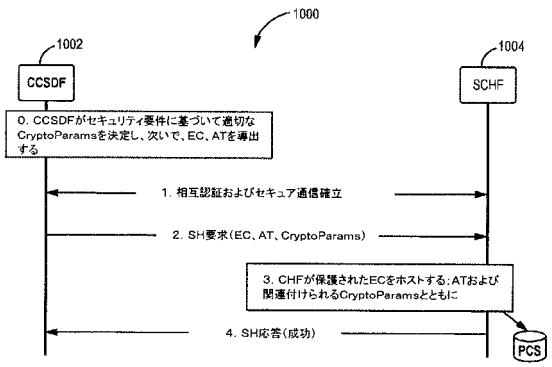
【図８】



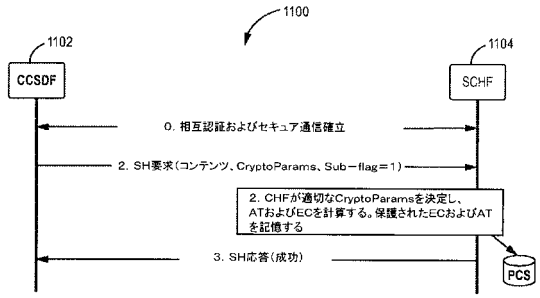
【図９】



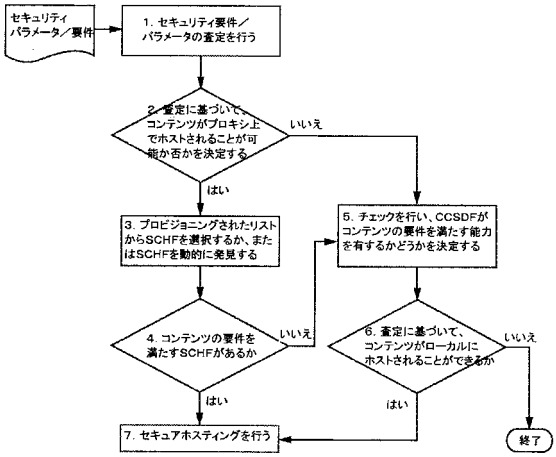
【図１０】



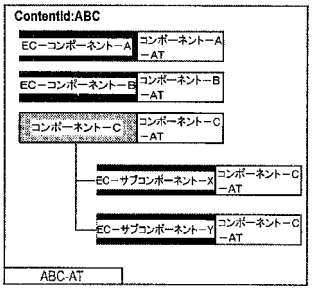
【図１１】



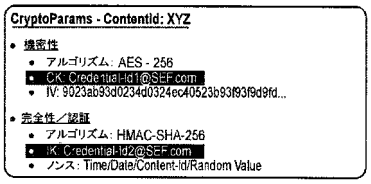
【図１２】



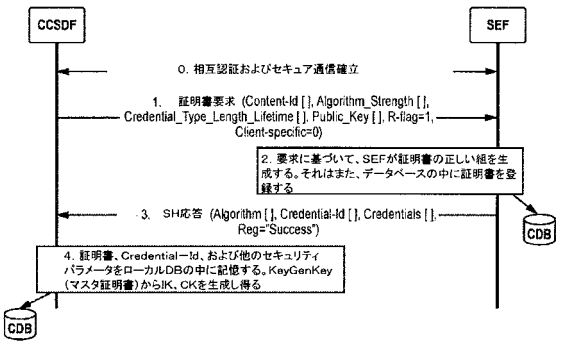
【図１３】



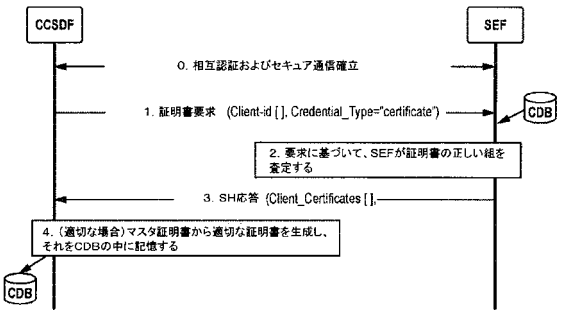
【図１４】



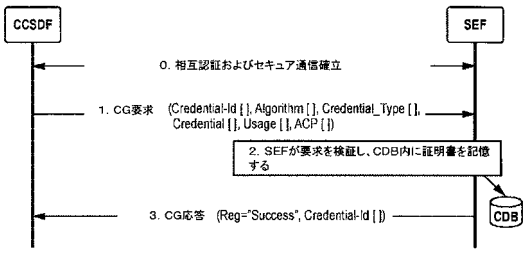
【図１５】



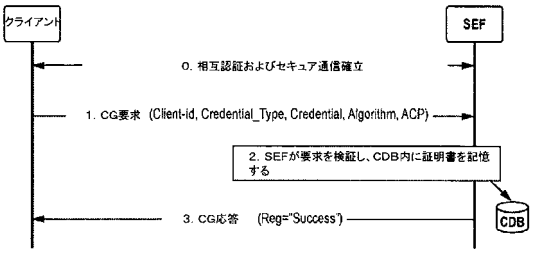
【図１６】



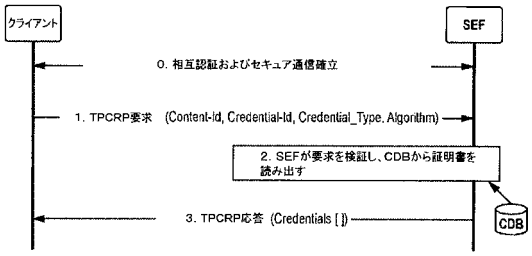
【図１７】



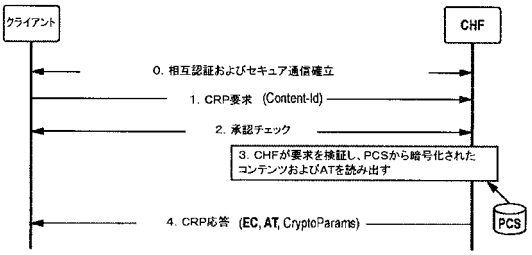
【図１８】



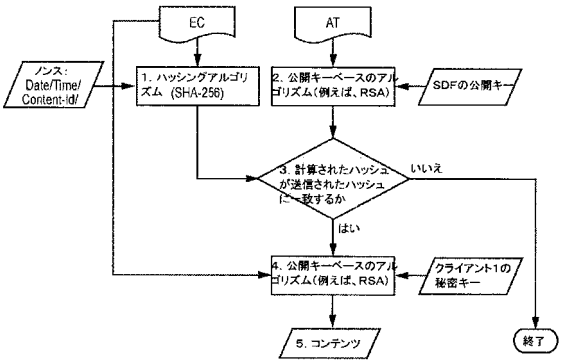
【図１９】



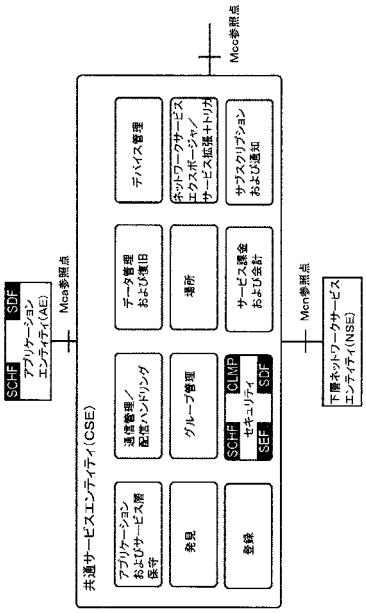
【図２０】



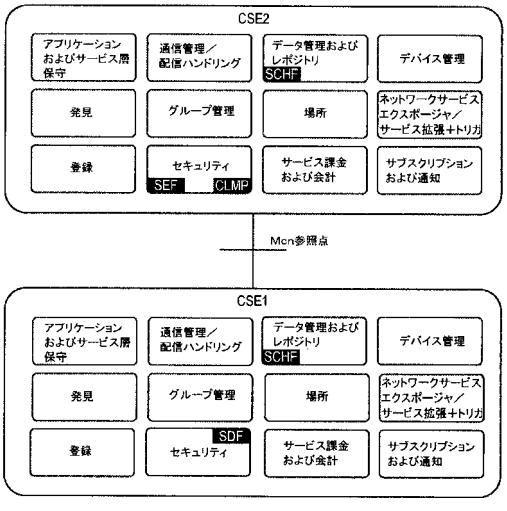
【図２１】



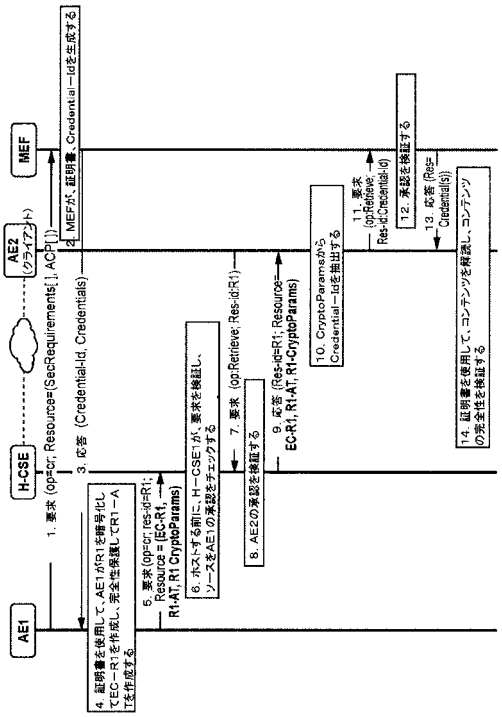
【図２２】



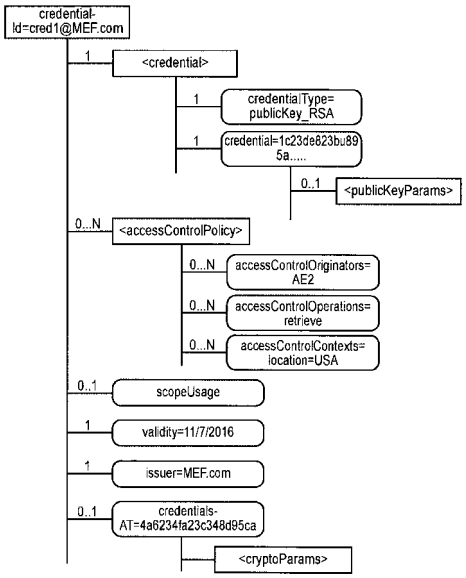
【図２３】



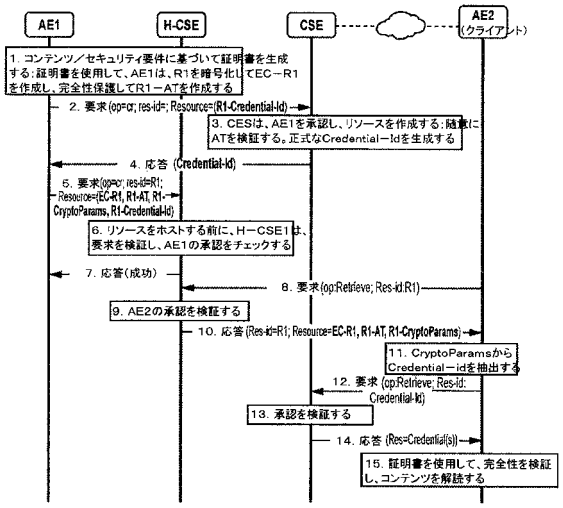
【図２４】



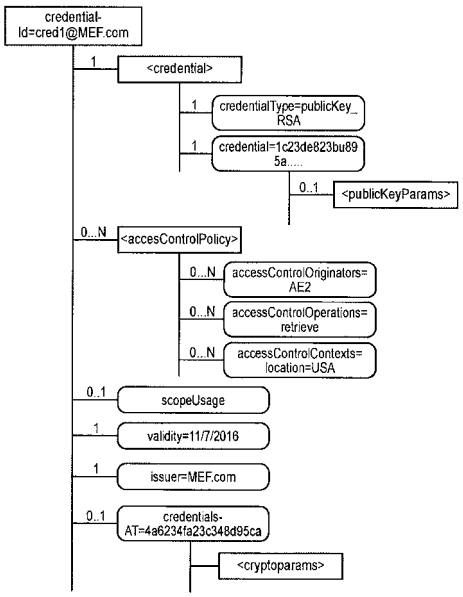
【図２５】



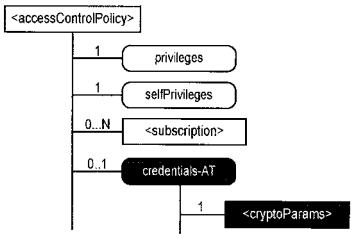
【図２６】



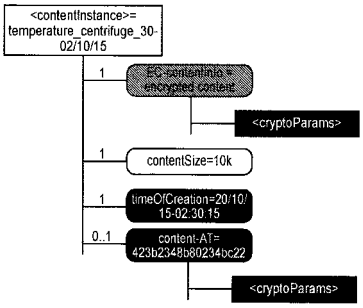
【図２７】



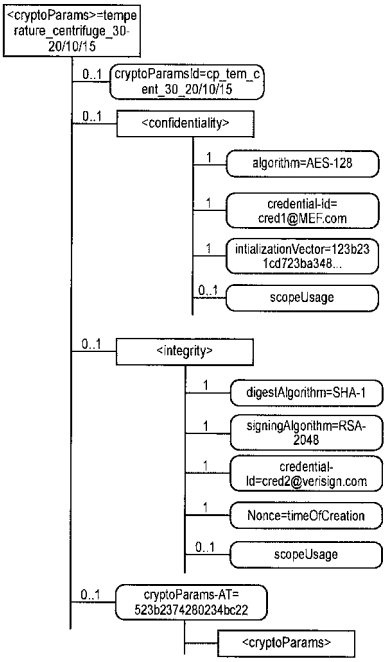
【図２８】



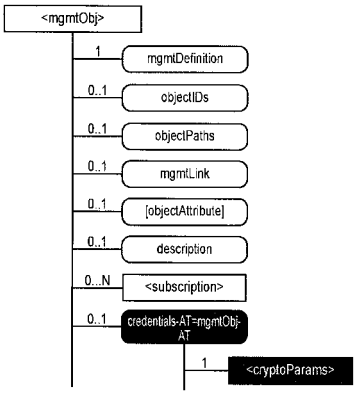
【図２９】



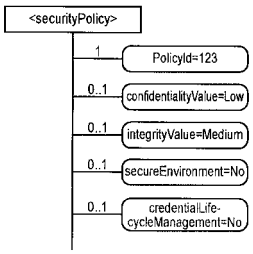
【図３０】



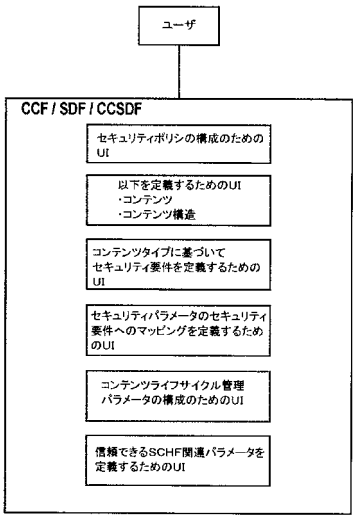
【図３１】



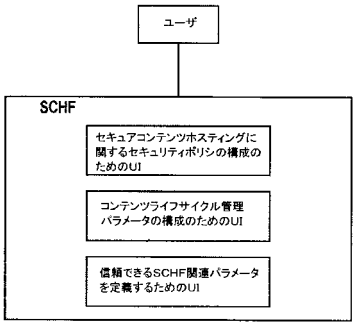
【図３２】



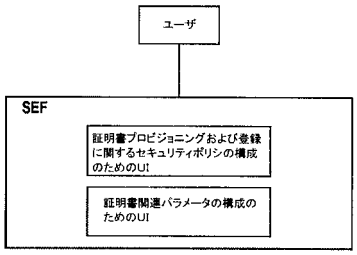
【図３３】



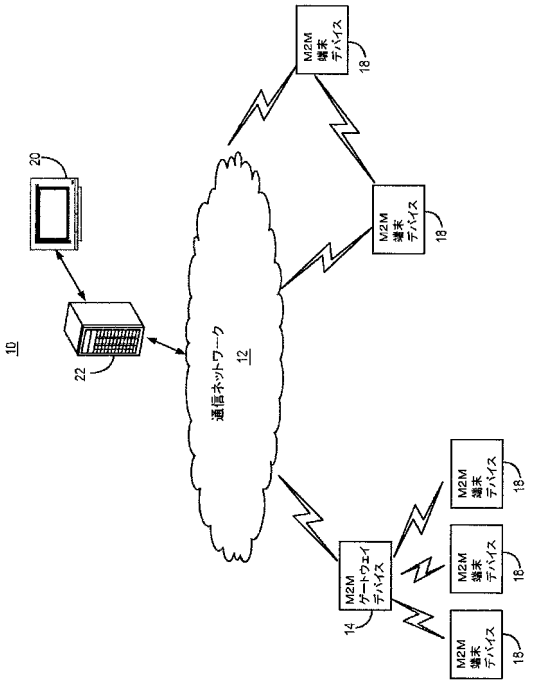
【図３４】



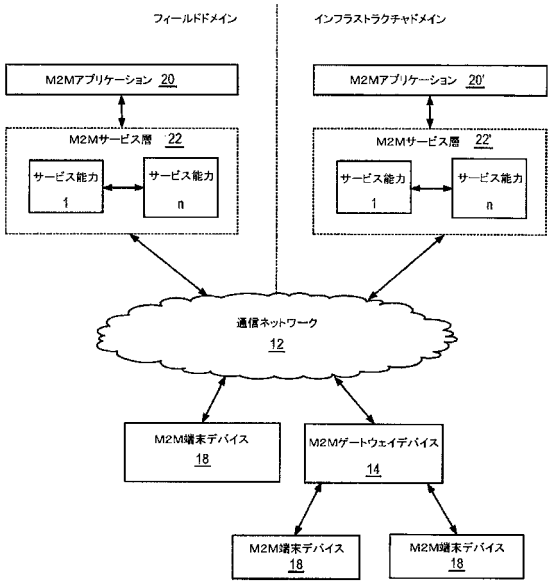
【図３５】



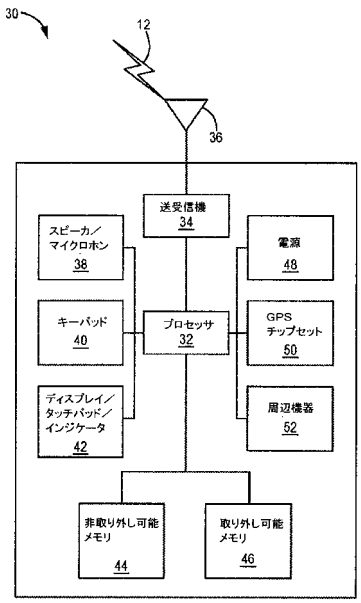
【図３６Ａ】



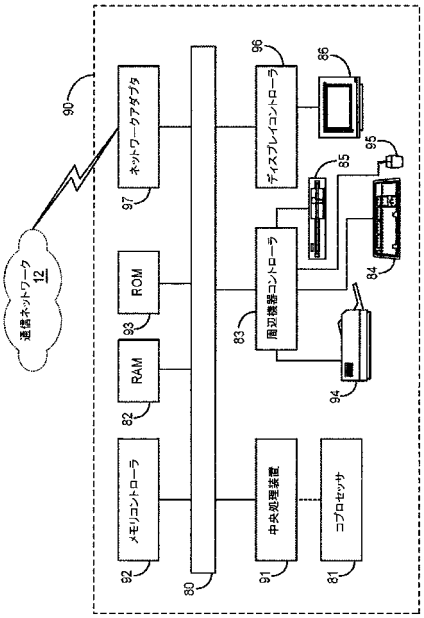
【図３６Ｂ】



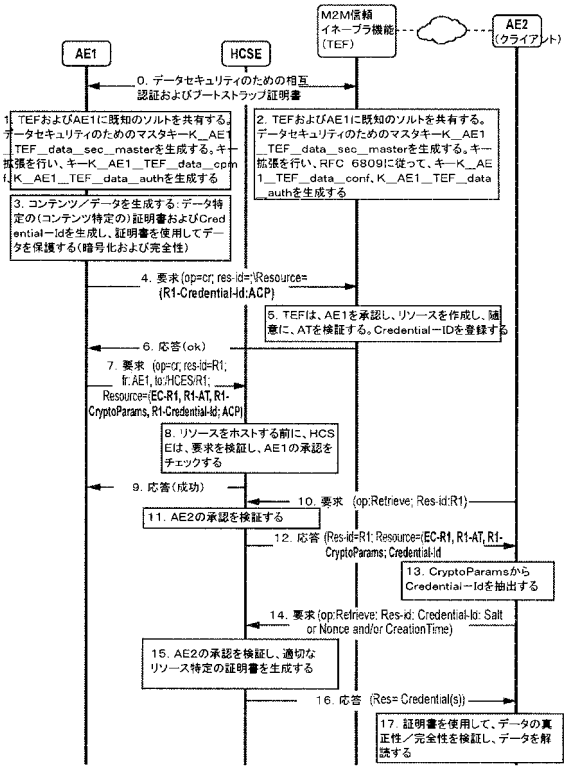
【図３６Ｃ】



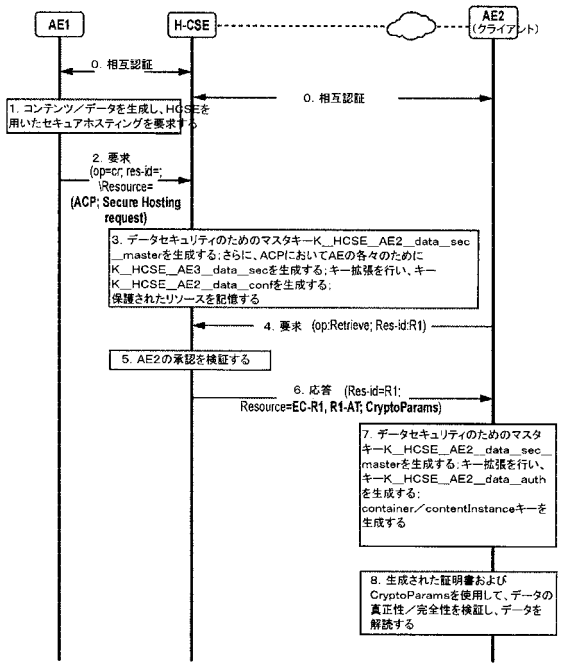
【図３６Ｄ】


通信ネットワーク 12
90
ネットワークアダプタ 97
ROM 93
RAM 82
メモリコントローラ 92
80
ディスプレイコントローラ 96
周辺機器コントローラ 83
中央処理装置 91
コプロセッサ 81
86
85
95
84
94

【図３７】


M2M信頼イネーブラ機能 (TEF)
AE2 (クライアント)
AE1
HCSE
0. データセキュリティのための相互認証およびブートストラップ証明書
1. TEFおよびAE1に既知のソルトを共有する。データセキュリティのためのマスタキーK_AE1_TEF_data_sec_masterを生成する。キー拡張を行い、キーK_AE1_TEF_data_confおよびK_AE1_TEF_data_authを生成する
2. TEFおよびAE1に既知のソルトを共有する。データセキュリティのためのマスタキーK_AE1_TEF_data_sec_masterを生成する。キー拡張を行い、RFC 6809に従って、キーK_AE1_TEF_data_conf、K_AE1_TEF_data_authを生成する
3. コンテンツ／データを生成する：データ特定の（コンテンツ特定の）証明書およびCredential－Idを生成し、証明書を使用してデータを保護する（暗号化および完全性）
4. 要求 (op=cr; res-id=\Resource= (R1-Credential-Id:ACP)
5. TEFは、AE1を承認し、リソースを作成し、随意に、ATを検証する。Credential－IDを登録する
6. 応答（ok）
7. 要求 (op=cr; res-id=R1; fr:AE1, to:HCES/R1; Resource=(EC-R1, R1-AT, R1-CryptoParams, R1-Credential-Id; ACP)
8. リソースをホストする前に、HCSEは、要求を検証し、AE1の承認をチェックする
9. 応答（成功）
10. 要求 (op:Retrieve; Res-id:R1)
11. AE2の承認を検証する
12. 応答 (Res-id=R1; Resource=(EC-R1, R1-AT, R1-CryptoParams; Credential-Id
13. CryptoParamsからCredential－Idを抽出する
14. 要求 (op:Retrieve; Res-id: Credential-Id: Salt or Nonce and/or CreationTime)
15. AE2の承認を検証し、適切なリソース特定の証明書を生成する
16. 応答 (Res= Credential(s))
17. 証明書を使用して、データの真正性／完全性を検証し、データを解読する

【図３８】


AE1
H-CSE
AE2 (クライアント)
0. 相互認証
0. 相互認証
1. コンテンツ／データを生成し、HCSEを用いたセキュアホスティングを要求する
2. 要求 (op=cr; res-id=; \Resource= (ACP; Secure Hosting request)
3. データセキュリティのためのマスタキーK_HCSE_AE2_data_sec_masterを生成する；さらに、ACPにおいてAEの各々のために K_HCSE_AE3_data_secを生成する；キー拡張を行い、キーK_HCSE_AE2_data_confを生成する；保護されたリソースを記憶する
4. 要求 (op:Retrieve; Res-id:R1)
5. AE2の承認を検証する
6. 応答 (Res-id=R1; Resource=EC-R1, R1-AT; CryptoParams)
7. データセキュリティのためのマスタキーK_HCSE_AE2_data_sec_masterを生成する；キー拡張を行い、キーK_HCSE_AE2_data_authを生成する；container／contentInstanceキーを生成する
8. 生成された証明書およびCryptoParamsを使用して、データの真正性／完全性を検証し、データを解読する

【手続補正書】
【提出日】令和1年9月26日(2019.9.26)
【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】
プロセッサと、メモリと、通信回路とを備えている装置であって、前記装置は、その通信回路を介してネットワークに接続され、前記装置は、前記装置の前記メモリ内に記憶されたコンピュータ実行可能命令をさらに備え、前記命令は、前記装置の前記プロセッサによって実行されると、
コンテンツの保護を提供する１つ以上の証明書に対する要求を送信することであって、前記要求は、前記コンテンツに関連付けられた１つ以上のセキュリティパラメータに基づく、ことと、
前記１つ以上の証明書を取得することと、
前記１つ以上の証明書を使用して、前記コンテンツをセキュアにすることと
を含む動作を前記装置に行わせる、装置。
【請求項２】
前記１つ以上の証明書は、対称キー機密性保護のためのマスタキーを備えている、請求項１に記載の装置。
【請求項３】
前記１つ以上の証明書は、完全性保護および機密性保護のためのものである、請求項１に記載の装置。
【請求項４】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記コンテンツを暗号化し、暗号化されたコンテンツを作成することを含むさらなる動作を前記装置に行わせる、請求項１に記載の装置。
【請求項５】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記コンテンツに関連付けられる認証タグを生成することであって、前記認証タグは、ホスティング共通サービスエンティティにおいてホストするための前記コンテンツの完全性および真正性を示す、ことを含むさらなる動作を前記装置に行わせる、請求項４に記載の装置。
【請求項６】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記暗号化されたコンテンツおよび前記セキュリティパラメータを含むリソースを作成するための要求をホスティング共通サービスエンティティに送信することを含むさらなる動作を前記装置に行わせる、請求項４に記載の装置。
【請求項７】
前記装置は、アプリケーションエンティティであり、前記証明書は、信頼有効化機能から取得される、請求項１に記載の装置。
【請求項８】
前記コンテンツを取得するために承認されている第２のアプリケーションエンティティは、前記信頼有効化機能から前記１つ以上の証明書を取得することができる、請求項７に記載の装置。
【請求項９】
前記要求は、クライアント毎のアルゴリズムおよび証明書タイプに基づき、
前記１つ以上の証明書は、クライアント固有のセキュリティプロファイルに関連する、

請求項１に記載の装置。
【請求項１０】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記セキュリティプロファイルに従って、前記コンテンツをセキュアにする、請求項９に記載の装置。
【請求項１１】
プロセッサと、メモリと、通信回路とを備えている装置であって、前記装置は、その通信回路を介してネットワークに接続され、前記装置は、前記装置の前記メモリ内に記憶されたコンピュータ実行可能命令をさらに備え、前記命令は、前記装置の前記プロセッサによって実行されると、
コンテンツに関連付けられたセキュリティ要件に基づいて、１つ以上の証明書を生成することと、
前記１つ以上の証明書を使用して前記コンテンツをセキュアにすることと、
承認されたクライアントのみがホスティングノードから前記コンテンツを読み出すことができるように、前記ホスティングノードが前記セキュアにされたコンテンツを記憶するという要求を送信することと
を含む動作を前記装置に行わせる、装置。
【請求項１２】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記１つ以上の証明書を信頼有効化機能に登録することを含むさらなる動作を前記装置に行わせる、請求項１１に記載の装置。
【請求項１３】
前記１つ以上の証明書は、前記装置と信頼有効化機能との間のアソシエーションをブートストラップすることによって生成される、請求項１２に記載の装置。
【請求項１４】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記要求に応答して、前記信頼有効化機能から証明書識別を受信することであって、前記要求は、前記証明書識別に関連付けられた証明書を備え、前記要求は、前記証明書の登録を得ようとする、ことを含むさらなる動作を前記装置に行わせる、請求項１２に記載の装置。
【請求項１５】
前記証明書識別は、共通サービスエンティティに一意である、請求項１４に記載の装置。
【請求項１６】
前記装置は、コンピュータ実行可能命令をさらに備え、前記命令は、
前記装置が前記ホスティングノードにおいてリソースを作成するために承認されていることを前記ホスティングノードが決定した場合、成功メッセージを受信することを含むさらなる動作を前記装置に行わせる、請求項１１に記載の装置。

フロントページの続き

(72)発明者 シャ, ヨゲンドラ シー.
アメリカ合衆国 ペンシルベニア １９３４１, エクストン, リージェンシー コート １０
(72)発明者 シード, デール エヌ.
アメリカ合衆国 ペンシルベニア １８１０４, アレンタウン, エヌ. ３６ティーエイチ ストリート ２２９
(72)発明者 スターシニック, マイケル エフ.
アメリカ合衆国 ペンシルベニア １８９４０, ニュータウン, アンドリュー ドライブ １９０
(72)発明者 ラフマン, シャミム アクバル
カナダ国 エイチ４ブイ １ビー８ ケベック, コート サン リュック, コンクリン ロード ６７０４
(72)発明者 リー, チュアン
アメリカ合衆国 ペンシルベニア １９４５４, ノース ウェールズ, スターリング ドライブ １１５
(72)発明者 チェン, ズオ
アメリカ合衆国 デラウェア １９７０３, クレーモント, パリシュ アベニュー １３９７
(72)発明者 フリン, ウィリアム ロバード ザ フォース
アメリカ合衆国 ペンシルベニア １９４７３, シュウェンクスビル, メイベリー ロード ４５１

【外国語明細書】
2020025278000001.pdf