(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2009-517922
(P2009-517922A)
(43)公表日　平成21年4月30日(2009.4.30)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/14	(2006.01)	H04L	9/00	641	5J104
G06Q 30/00	(2006.01)	G06F	17/60	302E	
G06Q 50/00	(2006.01)	G06F	17/60	ZEC	
H04L 9/08	(2006.01)	H04L	9/00	601E	
G06Q 10/00	(2006.01)	H04L	9/00	601B	

審査請求 未請求　予備審査請求 未請求　（全 75 頁）　最終頁に続く

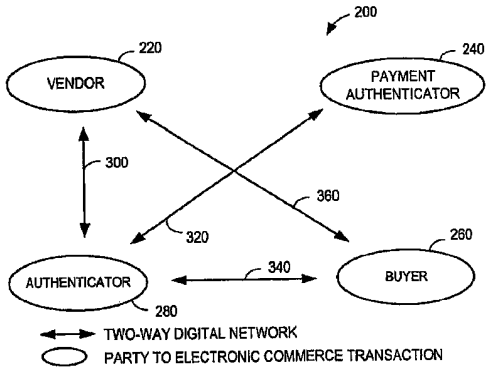
(21)出願番号　特願2008-542420 (P2008-542420)
(86)(22)出願日　平成18年11月22日 (2006.11.22)
(85)翻訳文提出日　平成20年7月23日 (2008.7.23)
(86)国際出願番号　PCT/US2006/045110
(87)国際公開番号　WO2007/120215
(87)国際公開日　平成19年10月25日 (2007.10.25)
(31)優先権主張番号　11/286,890
(32)優先日　平成17年11月23日 (2005.11.23)
(33)優先権主張国　米国 (US)

(71)出願人　505324939
イマジニア・ソフトウェア，インコーポレーテッド
アメリカ合衆国ウィスコンシン州５３２１１，ミルウォーキー，ノース・ハケット３４５２
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100089705
弁理士　社本　一夫
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男

最終頁に続く

(54)【発明の名称】変化する識別子を使用したセキュアな電子商取引

(57)【要約】
変化識別子を使用して電子商取引を行う方法およびシステム。１つの方法は、第１の変化識別子で購入者取引データを暗号化するステップと、購入者取引データを認証者デバイスへ送信するステップと、購入者取引データを解読するステップと、支払い要求を生成するステップと、第３の変化識別子で支払い要求を暗号化するステップと、支払い要求を支払い認証者デバイスへ送信するステップとを含むことができる。



【特許請求の範囲】
【請求項１】
変化識別子を使用して電子商取引を行う方法。
【請求項２】
請求項１に記載の方法であって、
第１の変化識別子で購入者取引データを暗号化するステップと、
前記購入者取引データを認証者デバイスへ送信するステップと、
前記購入者取引データを解読するステップと、
支払い要求を生成するステップと、
第３の変化識別子で前記支払い要求を暗号化するステップと、
前記支払い要求を、支払い認証者デバイスへ送信するステップと
を更に備える方法。
【請求項３】
請求項２に記載の方法であって、第２の変化識別子でベンダ取引データを暗号化し、前記ベンダ取引データを前記認証者デバイスへ送信するステップを更に備える方法。
【請求項４】
請求項３に記載の方法であって、前記ベンダ取引データを解読するステップを更に備える方法。
【請求項５】
請求項２に記載の方法であって、前記支払い要求を生成する前記ステップは、ベンダ・デバイスの識別とベンダの証明とを含む支払い要求を生成するステップを含む、方法。
【請求項６】
請求項２に記載の方法であって、第２の受領証をベンダ・デバイスへ送信するステップを更に備える方法。
【請求項７】
請求項２に記載の方法であって、第５の変化識別子をベンダ・デバイスへ送信するステップを更に備える方法。
【請求項８】
請求項２に記載の方法であって、前記支払い認証者デバイスが前記支払い要求を承認する場合、承認メッセージをベンダ・デバイスへ送信するステップを更に備える方法。
【請求項９】
請求項２に記載の方法であって、前記支払い認証者デバイスが前記支払い要求を拒絶する場合、拒絶メッセージをベンダ・デバイスへ送信するステップを更に備える方法。
【請求項１０】
請求項２に記載の方法であって、前記支払い要求を生成する前記ステップは、購入者デバイスの識別と購入者の証明とを含む支払い要求を生成するステップを含む、方法。
【請求項１１】
請求項２に記載の方法であって、第１の受領証を購入者デバイスへ送信するステップを更に備える方法。
【請求項１２】
請求項２に記載の方法であって、第４の変化識別子を購入者デバイスへ送信するステップを更に備える方法。
【請求項１３】
請求項２に記載の方法であって、前記支払い認証者デバイスが前記支払い要求を承認する場合、購入者デバイスへ承認メッセージを送信するステップを更に備える方法。
【請求項１４】
請求項２に記載の方法であって、前記支払い認証者デバイスが前記支払い要求を拒絶する場合、購入者デバイスへ拒絶メッセージを送信するステップを更に備える方法。
【請求項１５】
請求項２に記載の方法であって、第３の受領証を前記支払い認証者デバイスへ送信する

ステップを更に備える方法。
【請求項１６】
請求項２に記載の方法であって、第６の変化識別子を前記支払い認証者デバイスへ送信するステップを更に備える、方法。
【請求項１７】
請求項２に記載の方法であって、前記支払い認証者デバイスが前記支払い要求を承認する場合、第１の口座と第２の口座との間で資金を転送するステップを更に備える方法。
【請求項１８】
請求項２に記載の方法であって、前記支払い認証者デバイスが前記支払い要求を承認する場合、エスクロー・サービスを提供するステップを更に備える方法。
【請求項１９】
第１のデバイスと第２のデバイスとの間で通信を確立する方法であって、
取引鍵を求める要求を生成するステップと、
前記取引鍵の要求を、前記第１のデバイスの第１の変化識別子で暗号化するステップと、
暗号化された前記取引鍵の要求を認証者デバイスへ送信するステップと、
取引鍵を生成するステップと、
前記取引鍵を含む第１のメッセージを生成するステップと、
前記第１のメッセージを、前記第１のデバイスの前記第１の変化識別子で暗号化するステップと
を備える方法。
【請求項２０】
請求項１９に記載の方法であって、前記第１のデバイスの第３の変化識別子を生成するステップを更に備え、前記第１のメッセージは前記第３の変化識別子を含む、方法。
【請求項２１】
請求項２０に記載の方法であって、前記第１のメッセージを前記第１のデバイスへ送信するステップを更に備える方法。
【請求項２２】
請求項１９に記載の方法であって、前記取引鍵を含む第２のメッセージを生成し、前記第２のデバイスの第２の変化識別子で前記第２のメッセージを暗号化するステップを更に備える方法。
【請求項２３】
請求項２２に記載の方法であって、前記第２のデバイスの第４の変化識別子を生成するステップを更に備え、前記第２のメッセージは前記第４の変化識別子を含む、方法。
【請求項２４】
請求項２３に記載の方法であって、前記第２のデバイスへ前記第２のメッセージを送信するステップを更に備える方法。
【請求項２５】
請求項１９に記載の方法であって、前記取引鍵の要求を生成する前記ステップは、取引鍵の要求を生成するステップを含み、前記取引鍵の要求は、要求を識別するデータを含む、方法。
【請求項２６】
請求項２５に記載の方法であって、前記取引鍵を含む第１のメッセージを生成する前記ステップは、前記取引鍵と前記要求を識別するデータとを含む第１のメッセージを生成するステップを含む、方法。
【請求項２７】
変化識別子を使用して電子商取引を行う方法であって、
第１の変化識別子で購入者取引データを暗号化するステップと、
前記購入者取引データを認証者デバイスへ送信するステップと、
第１の取引鍵で購入者の証明を暗号化するステップと、

前記購入者の証明を、支払い認証者デバイスへ送信するステップと、
第２の変化識別子でベンダ取引データを暗号化するステップと、
前記ベンダ取引データを認証者デバイスへ送信するステップと、
第２の取引鍵でベンダの証明を暗号化するステップと、
前記ベンダの証明を、支払い認証者デバイスへ送信するステップと、
前記購入者取引データを解読するステップと、
前記ベンダ取引データを解読するステップと、
支払い認証者デバイスに対しての支払い要求を生成するステップと、
第３の変化識別子で前記支払い要求を暗号化するステップと、
前記支払い要求を、前記支払い認証者デバイスへ送信するステップと、
前記支払い要求を解読するステップと、
前記購入者の証明を解読するステップと、
前記ベンダの証明を解読するステップと、
前記購入者の証明、前記ベンダの証明、および前記支払い要求に基づいて、第１の応答を生成するステップと、
前記購入者の証明、前記ベンダの証明、および前記支払い要求に基づいて、第２の応答を生成するステップと、
前記第１の応答を購入者デバイスへ送信するステップと、
前記第２の応答をベンダ・デバイスへ送信するステップと
を備える方法。

【請求項２８】
請求項２７に記載の方法であって、前記ベンダ取引データを暗号化する前記ステップは、売渡証および価格を暗号化するステップを含む、方法。

【請求項２９】
請求項２７に記載の方法であって、前記支払い要求を生成する前記ステップは、前記ベンダ・デバイスの識別と前記購入者デバイスの識別とを含む支払い要求を生成するステップを含む、方法。

【請求項３０】
請求項２７に記載の方法であって、前記購入者の証明の有効性を検証するステップおよび前記ベンダの証明の有効性を検証するステップを更に備える方法。

【請求項３１】
請求項２７に記載の方法であって、前記支払い要求を生成する前記ステップは、前記購入者デバイスに対する第１の受領証を含む支払い要求を生成するステップを含む、方法。

【請求項３２】
請求項３１に記載の方法であって、前記第１の応答を生成する前記ステップは、前記第１の受領証を含む第１の応答を生成するステップを含む、方法。

【請求項３３】
請求項２７に記載の方法であって、前記支払い要求を生成する前記ステップは、前記購入者デバイスの第４の変化識別子を含む支払い要求を生成するステップを含む、方法。

【請求項３４】
請求項３３に記載の方法であって、前記第１の応答を生成する前記ステップは、前記第４の変化識別子を含む第１の応答を生成するステップを含む、方法。

【請求項３５】
請求項２７に記載の方法であって、前記第１の応答を生成する前記ステップは、前記購入者デバイスに対しての承認メッセージおよび拒絶メッセージの少なくとも一方を含む第１の応答を生成するステップを含む、方法。

【請求項３６】
請求項２７に記載の方法であって、前記購入者取引データを暗号化する前記ステップは、売渡証および価格を暗号化するステップを含む、方法。

【請求項３７】

請求項２７に記載の方法であって、前記購入者取引データを暗号化する前記ステップは、前記支払い認証者デバイスの識別を暗号化するステップを含む、方法。
【請求項３８】
請求項２７に記載の方法であって、前記支払い要求を生成する前記ステップは、前記ベンダ・デバイスに対しての第２の受領証を含む支払い要求を生成するステップを含む、方法。
【請求項３９】
請求項３８に記載の方法であって、前記第２の応答を生成する前記ステップは、前記第２の受領証を含む第２の応答を生成するステップを含む、方法。
【請求項４０】
請求項２７に記載の方法であって、前記支払い要求を生成する前記ステップは、前記ベンダ・デバイスに対しての第５の変化識別子を含む支払い要求を生成するステップを含む、方法。
【請求項４１】
請求項４０に記載の方法であって、前記第２の応答を生成する前記ステップは、前記第５の変化識別子を含む第２の応答を生成するステップを含む、方法。
【請求項４２】
請求項２７に記載の方法であって、前記第２の応答を生成する前記ステップは、前記ベンダ・デバイスへの承認メッセージおよび拒絶メッセージの少なくとも一方を含む第２の応答を生成するステップを含む、方法。
【請求項４３】
請求項２７に記載の方法であって、前記支払い要求を生成する前記ステップは、前記支払い認証者デバイスに対しての第３の受領証を含む支払い要求を生成するステップを含む、方法。
【請求項４４】
請求項２７に記載の方法であって、前記支払い要求を生成する前記ステップは、前記支払い認証者デバイスに対しての第６の変化識別子を含む支払い要求を生成するステップを含む、方法。
【請求項４５】
請求項２７に記載の方法であって、前記支払い認証者が前記支払い要求を承認する場合、第１の口座から第２の口座へ資金を転送するステップを更に供える、方法。
【請求項４６】
請求項２７に記載の方法であって、前記支払い認証者が前記支払い要求を承認する場合、エスクロー・サービスを提供するステップを更に備える、方法。
【請求項４７】
電子商取引システムであって、
ベンダ・デバイスと、
第１の変化識別子で購入者取引データを暗号化し、前記購入者取引データを認証者デバイスへ送信するように構成された購入者デバイスと、
支払い要求を承認または拒絶し、前記購入者デバイスへの第１の応答を生成し、前記ベンダ・デバイスへの第２の応答を生成し、前記第１の応答を前記購入者デバイスへ送信し、前記第２の応答を前記ベンダ・デバイスへ送信するように構成された支払い認証者デバイスと
を備え、
前記認証者デバイスは、前記購入者取引データを解読し、前記支払い認証者デバイスに対しての支払い要求を生成し、前記支払い認証者デバイスの第３の変化識別子で前記支払い要求を暗号化し、前記支払い要求を前記支払い認証者デバイスへ送信するように構成される、
システム。
【請求項４８】

請求項４７に記載のシステムであって、前記ベンダ・デバイスは更に、第２の変化識別子でベンダ取引データを暗号化し、前記ベンダ取引データを前記認証者デバイスへ送信するように構成される、システム。

【請求項４９】

請求項４８に記載のシステムであって、前記認証者デバイスは更に、前記ベンダ取引データを解読するように構成される、システム。

【請求項５０】

請求項４７に記載のシステムであって、前記ベンダ・デバイスは更に、第２の取引鍵でベンダの証明を暗号化し、前記ベンダの証明を前記支払い認証者デバイスへ送信するように構成される、システム。

【請求項５１】

請求項５０に記載のシステムであって、前記支払い認証者デバイスは更に、前記ベンダの証明を解読するように構成される、システム。

【請求項５２】

請求項５０に記載のシステムであって、前記支払い認証者デバイスは更に、前記第２の取引鍵で前記第２の応答を暗号化するように構成される、システム。

【請求項５３】

請求項４７に記載のシステムであって、前記認証者デバイスは更に、前記支払い要求にベンダの証明を含めるように、構成される、システム。

【請求項５４】

請求項５３に記載のシステムであって、前記支払い認証者デバイスは更に、前記ベンダの証明の有効性を検証するように構成される、システム。

【請求項５５】

請求項４７に記載のシステムであって、前記認証者デバイスは更に、前記ベンダ・デバイスの第５の変化識別子を前記支払い要求に含めるように、構成される、システム。

【請求項５６】

請求項５５に記載のシステムであって、前記支払い認証者デバイスは更に、前記第５の変化識別子を前記ベンダ・デバイスへ送信するように構成される、システム。

【請求項５７】

請求項４７に記載のシステムであって、前記支払い認証者デバイスは更に、承認メッセージおよび拒絶メッセージの少なくとも一方を前記第２の応答に含めるように、構成される、システム。

【請求項５８】

請求項４７に記載のシステムであって、前記購入者デバイスは更に、第１の取引鍵で購入者の証明を暗号化し、前記購入者の証明を前記支払い認証者デバイスへ送信するように構成される、システム。

【請求項５９】

請求項５８に記載のシステムであって、前記支払い認証者は更に、前記購入者の証明を解読するように構成される、システム。

【請求項６０】

請求項５８に記載のシステムであって、前記支払い認証者デバイスは更に、前記第１の取引鍵で前記第１の応答を暗号化するように構成される、システム。

【請求項６１】

請求項４７に記載のシステムであって、前記認証者デバイスは更に、前記支払い要求に購入者の証明を含めるように、構成される、システム。

【請求項６２】

請求項６１に記載のシステムであって、前記支払い認証者デバイスは更に、前記購入者の証明の有効性を検証するように構成される、システム。

【請求項６３】

請求項４７に記載のシステムであって、前記認証者デバイスは更に、前記購入者デバイ

スの第４の変化識別子を前記支払い要求に含めるように、構成される、システム。
【請求項６４】
請求項６３に記載のシステムであって、前記支払い認証者デバイスは更に、前記第４の変化識別子を前記購入者デバイスへ送信するように構成される、システム。
【請求項６５】
請求項４７に記載のシステムであって、前記支払い認証者デバイスは更に、承認メッセージおよび拒絶メッセージの少なくとも一方を前記第１の応答に含めるように、構成される、システム。
【請求項６６】
請求項４７に記載のシステムであって、前記認証者デバイスは更に、前記支払い認証者デバイスへの第３の受領証を前記支払い要求に含めるように、構成される、システム。
【請求項６７】
請求項４７に記載のシステムであって、前記認証者デバイスは更に、前記支払い認証者デバイスの第６の変化識別子を前記支払い要求に含めるように、構成される、システム。
【請求項６８】
請求項４７に記載のシステムであって、前記支払い認証者デバイスは更に、前記支払い要求を承認すると、第１の口座と第２の口座との間で資金の転送を行うように構成される、システム。
【請求項６９】
請求項４７に記載のシステムであって、前記支払い認証者デバイスは更に、前記支払い要求を承認すると、エスクロー・サービスを提供するように構成される、システム。
【請求項７０】
変化識別子を使用して電子商取引を行う方法であって、
第１の変化識別子で取引データを暗号化するステップと、
前記取引データを認証者デバイスへ送信するステップと、
支払い認証者デバイスから応答を受信するステップと
を備える方法。
【請求項７１】
変化識別子を使用して電子商取引を行う方法であって、
取引データを含む支払い要求を認証者デバイスから入手するステップであって、前記支払い要求は第１の変化識別子で暗号化されている、ステップと、
前記支払い要求を解読するステップと、
前記取引データを検証するステップと、
応答を送信するステップと
を備える方法。
【請求項７２】
変化識別子を使用して電子商取引を行う方法であって、
第１の変化識別子で暗号化する取引データを入手するステップと、
前記取引データを解読するステップと、
前記取引データの少なくとも一部を含む支払い要求を生成するステップと、
前記支払い要求を支払い認証者デバイスへ送信するステップと
を備える方法。
【請求項７３】
第１のデバイスと第２のデバイスとの間に通信を確立する方法であって、
取引鍵の要求を生成するステップと、
前記第１のデバイスの第１の変化識別子で前記取引鍵の要求を暗号化するステップと、
暗号化された前記取引鍵の要求を認証者デバイスへ送信するステップと、
前記第１の変化識別子で暗号化する取引鍵を含むメッセージを受信するステップと
を備える方法。
【請求項７４】

第１のデバイスと第２のデバイスとの間に通信を確立する方法であって、
前記第１のデバイスから取引鍵の要求を入手するステップであって、前記取引鍵の要求は第１の変化識別子において暗号化されている、ステップと、
前記取引鍵の要求を解読するステップと、
前記取引鍵を含む第１のメッセージを生成するステップと、
前記第１のデバイスの前記第１の変化識別子で前記第１のメッセージを暗号化するステップと、
前記第１のメッセージを前記第１のデバイスへ送信するステップと
を備える方法。
【請求項７５】
電子商取引を遂行する方法であって、
第１の購入者鍵で購入者取引データを暗号化するステップと、
前記購入者取引データを認証者デバイスへ送信するステップと、
第１の取引鍵で購入者の証明を暗号化するステップと、
前記購入者の証明を支払い認証者デバイスへ送信するステップと
を備える方法。
【請求項７６】
請求項７５に記載の方法であって、
ベンダ鍵でベンダ取引データを暗号化するステップと、
前記ベンダ取引データを認証者デバイスへ送信するステップと、
第２の取引鍵でベンダの証明を暗号化するステップと、
前記ベンダの証明を、支払い認証者デバイスへ送信するステップと
を更に備える方法。
【請求項７７】
請求項７６に記載の方法であって、
前記購入者取引データを解読するステップと、
前記ベンダ取引データを解読するステップと、
支払い認証者デバイスに対して支払い要求を生成するステップと、
支払い要求鍵で前記支払い要求を暗号化するステップと、
前記支払い要求を前記支払い認証者デバイスへ送信するステップと
を更に備える方法。
【請求項７８】
請求項７７に記載の方法であって、
前記支払い要求を解読するステップと、
前記購入者の証明を解読するステップと、
前記ベンダの証明を解読するステップと、
前記購入者の証明、前記ベンダの証明、および前記支払い要求に基づいて、第１の応答を生成するステップと、
前記購入者の証明、前記ベンダの証明、および前記支払い要求に基づいて、第２の応答を生成するステップと、
前記第１の応答を前記購入者デバイスへ送信するステップと、
前記第２の応答を前記購入者デバイスへ送信するステップと
を更に備える方法。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願
本願は、２００５年１１月２３に出願された米国特許出願１１／２８６８９０からの優先権を主張し、米国特許出願１１／２８６８９０は、２００４年５月２６日に出願された米国特許出願１０／８５４６０４の一部継続出願であり、米国特許出願１０／８５４６０

４は、２００２年２月２７日に出願された米国仮特許出願６０／３６００２３の優先権を主張する２００３年２月２７日に出願された米国特許出願１０／２４８８９４の一部継続出願である。上記出願の全内容はすべて参照により本願に組み込まれる。

【０００２】

本発明の実施形態は、コンテンツ（テキスト、音声、映像、マルチメディア素材など）の配布に関する。より詳細には、本発明は、コンテンツ所有者の著作権および他の同様の法的権利が守られることを保証する方式でそのようなコンテンツを配信することに関する。

【背景技術】

【０００３】

デジタル形態で配信されるコンテンツが増加しており、また、イントラネット、インターネット、ケーブルＴＶネットワーク等の私設および公衆のネットワークを通じて配信されるデジタル・コンテンツが増加している。そのようなコンテンツの消費者に対して、デジタルのバージョン（アナログ、紙コピー、および他の形態と相対する）は、忠実度の向上、再生の選択肢の改良と増加、対話性その他といった様々な利益をもたらす。オンライン配信またはネットワーク配信は、一般に、より高い利便性と適時性を提供する。オンライン配信はまた、他の配信方法よりも低コストでもあり、この事はコンテンツの発行者にとって利益となる。

【０００４】

現在のデジタル配信コンテンツおよび今後行われる可能性のあるデジタル配信コンテンツの大半は、大半の書籍と同じように、一般には発行者または所有者が、コンテンツを消費者に付与または販売するような形で配信されるが、そうしたコンテンツは、コンテンツが消費者の物理的管理下のみに置かれた後もコンテンツを使用する権利を制限し続ける。例えば、典型的には、コンテンツ所有者がコンテンツの著作権を保持し、そのため、消費者は、許可を得ずにコンテンツを合法的に再生または公開することはできない。他形態のメディアと異なり、デジタル・コンテンツでは、消費者が恒久的なコピーを作ることを許されるか、または配信時にコンテンツを視聴することのみを許されるかに応じて、コンテンツ所有者が価格設定を調整することができる。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

デジタルおよびネットワーク配信の価値のある特性にも関わらず、デジタル・コンテンツの不正な複製、海賊行為、および配布（例えばＮａｐｓｔｅｒのユーザにより行われたような配布）が非常に容易であるため、コンテンツ所有者は、なおも一般には、コンテンツ、特に高価値のコンテンツをネットワークを介して配布することに消極的である。アナログのレコーダや、複写機、他の旧来のデバイスと違って、現在の技術では、デジタル・コンテンツの劣化のない（ｐｒｉｓｔｉｎｅ）コピーを無制限に作製することができる。しかも、大半の事例では、デジタル・コンテンツのコピーは、非常に迅速に、あるいはほぼ瞬時に作製されることができる。更に、公開鍵暗号法や、デジタル多用途ディスクに使用されるコンテンツ・スクランブル・システム（「ＣＳＳ」）等の現在の保護措置さえも破られている。

【０００６】

更に、暗号化されたコンテンツを解除する鍵が一旦合法的または不法に入手または発見されると、そのコンテンツは永久に危険にさらされてしまう。そのようにコンテンツに自由にアクセスできると、鍵の所有者は、解読されたコンテンツのコピーを無限数作製し、配布することが可能になる。鍵が使用されてコンテンツ・アイテムの不法なコピーを出回らせた場合には、最初にその鍵を所有した者まで、不法に配布されたコンテンツをさかのぼることは一般には非現実的である。

【０００７】

コンテンツの配布に加えて、インターネットなどのネットワーク化されたシステムの使

用可能性と普及は、商業の地勢を変えた。電子商取引（「ｅ－ｃｏｍｍｅｒｃｅ」）は、ビジネスの大きく且つ重要な部分へと成長した。電子商取引機能を提供することは、企業が全国規模および世界規模で競争するための必須事項となっている。

【０００８】

電子商取引機能の提供に加えて、企業は、セキュアな電子商取引機能を提供することも求められる。大半の購入者は、自分のデータがセキュアに保たれることを保証されない限り、電子商取引を完了するための課金情報や機密情報を提供しない。多くの現在の電子商取引プロトコルは、公開鍵交換プロトコルの一種を用いる。このプロトコルは、買い手と売り手の間にセキュアな接続を確立する。セキュアな接続が確立されると、機密情報（例えばクレジット・カード番号や口座番号等）が買い手から売り手に通信される。そして、売り手は、その情報を使用して企業（例えばクレジット・カード会社や金融機関）から支払いを得る。

【０００９】

しかし、上記のプロトコルでは、クレジット・カード情報あるいは機密情報が一旦売り手に提供されると、売り手は、その情報を無期限に所有する。そのような情報のセキュリティの信用が落ちている事例が発生している。そのようなセキュリティの信用の下落は、消費者が電子取引に慎重になる等の幾つかの問題を呈する。

【課題を解決するための手段】

【００１０】

上記に照らして、コンテンツ所有者の権利が守られることを保証するコンテンツの配布方法およびシステムを提供する必要性がある。また、窃盗者を追跡し、コンテンツの不法な配布を思いとどまらせる機構を提供する必要性もある。更に、セキュアな電子商取引を行う方法およびシステムを提供する必要性がある。

【００１１】

本発明は、特に、コンテンツを配布するための複数パーティー（多当事者）システムを提供する。一実施形態では、消費者、コンテンツ提供者、および認証者の３つの当事者がこのシステムに関係する。コンテンツ提供者から消費者へのコンテンツの配布は、所定のプロトコル、変化するＩＤ（ｍｕｔａｔｉｎｇ　ＩＤ、変化ＩＤ）、およびライセンスを使用して実施される。認証者は、変化ＩＤの配布を管理し、両当事者のアイデンティティ（識別）を検証する。

【００１２】

別の実施形態では、コンテンツを配布するための多当事者システムには４つの当事者が関係する。このシステムは、消費者、サービス・プロバイダ（サービス提供者）、認証者、およびコンテンツ・プロバイダ（コンテンツ提供者）を含む。サービス提供者のサービスを通じてのコンテンツ提供者から消費者へのコンテンツの配布は、所定のプロトコル、変化ＩＤ、およびライセンスを使用して実施される。認証者は、変化ＩＤの配布を管理し、１または複数の当事者の識別を検証する。

【００１３】

実施形態は、コンテンツを配布する方法も提供する。コンテンツを配布する一つの方法は、コンテンツ提供者が、消費者へコンテンツを送信する要求を行うことを含む。この要求は、送信されるべきコンテンツの暗号化された識別子を含む。この要求に応答して、消費者は、その要求を暗号化して認証要求を作成し、その認証要求を認証者へ送信する。認証者は、認証要求を確認し、有効である場合には、最初の要求で識別される暗号化コンテンツを消費者へ送信するようにコンテンツ提供者に通知する。認証者は、消費者がコンテンツを解読して視聴または消費することができるように、消費者へ解読鍵を送信する。

【００１４】

別の実施形態では、この方法は、消費者が、サービス提供者へコンテンツ要求を行い、その要求をコンテンツ提供者に中継することを含む。要求に応答して、コンテンツ提供者は、サービス提供者に関する識別情報と、要求されるコンテンツを識別する暗号化情報とを含むライセンスを作成する。ライセンスは、サービス提供者へ送信される。サービス提

供者は、コンテンツ提供者からのライセンスを暗号化し、そのメッセージを消費者へ送信する。消費者は、メッセージを暗号化して認証要求を作成し、その認証要求を認証者へ送信する。認証者は、認証要求を確認し、有効である場合には、そのライセンスで指定される暗号化コンテンツを消費者へ送信するようにコンテンツ提供者に通知する。認証者は、消費者がコンテンツを解読して消費できるように、消費者へ解読鍵を送信する。

【００１５】

本発明の実施形態は更に、コンテンツを配布する方法を提供し、この方法では、コンテンツのそれぞれのコピーに一意に透かしが入れられる。この方法は、消費者が、サービス提供者にコンテンツ要求を行い、その要求をコンテンツ提供者に中継することを含む。要求に応答して、コンテンツ提供者は、サービス提供者に関する識別情報と、要求されるコンテンツを識別する暗号化情報と、一意の透かしとを含むライセンスを作成する。ライセンスは、サービス提供者へ送信される。サービス提供者は、サービス提供者からのライセンスを暗号化し、そのメッセージを消費者へ送信する。消費者は、メッセージを暗号化して認証要求を作成し、その認証要求を認証者へ送信する。認証者は、認証要求を確認し、有効である場合、受信されたライセンスで指定される透かしにより透かしが入れられた暗号化コンテンツを消費者へ送信するように、コンテンツ提供者に通知する。認証者は、消費者が透かしの入ったコンテンツを解読して視聴できるように、消費者へ解読鍵を送信する。

【００１６】

別の実施形態では、本発明は、認証者とコンテンツ提供者と消費者を含むコンテンツ配布システムを提供する。コンテンツ提供者は、コンテンツとコンテンツ識別子を有し、そのコンテンツ識別子に関連した第１の変化識別子を生成する。このシステムは消費者デバイスも含み、この消費者デバイスは、コンテンツを受信する要求をコンテンツ提供者へ送信するように、およびコンテンツ提供者からコンテンツを受信するように、動作可能である。消費者デバイスは、要求（リクエスト）の形態でコンテンツ提供者から第１の変化識別子を受信し、第１の変化識別子に関連した第２の変化識別子を生成し、その第２の変化識別子を認証者へ配布する。認証者は、要求の有効性を検証し、その後、要求の有効性について消費者に通知する。要求が有効である場合、コンテンツ提供者はその後コンテンツを暗号化し、暗号化されたコンテンツを消費者へ送信し、認証者は解読コードを消費者へ送信する。

【００１７】

別の実施形態では、本発明は、認証者とコンテンツ提供者を含むコンテンツ配布システムを提供する。コンテンツ提供者は、コンテンツとコンテンツ識別子を有し、そのコンテンツ識別子に関連した第１の変化識別子を生成する。このシステムは、コンテンツの要求を生成するように動作可能な消費者デバイスも含む。また、このシステムは、サービス提供者を含む。サービス提供者は、消費者デバイスから要求を受信し、コンテンツ提供者から第１の変化識別子を受信し、第１の変化識別子に関連した第２の変化識別子を生成し、第２の変化識別子を消費者デバイスへ配布する。消費者デバイスは、第２の変化識別子に関連した第３の変化識別子を生成し、第３の変化識別子を認証者へ配布する。認証者は、要求の有効性を検証し、その後、要求の有効性をサービス提供者に通知する。要求が有効である場合、コンテンツ提供者はその後コンテンツを暗号化し、暗号化されたコンテンツを消費者へ送信し、認証者は、消費者へ解読コードを送信する。

【００１８】

追加的な実施形態は、変化識別子を使用して電子商取引を行う方法を提供する。１つの方法は、第１の変化識別子で購入者取引データを暗号化するステップと、購入者取引データを認証者デバイスへ送信するステップと、購入者取引データを解読するステップと、支払い要求を生成するステップと、第３の変化識別子で支払い要求を暗号化するステップと、支払い要求を支払い認証者デバイスへ送信するステップとを含むことができる。

【００１９】

別の実施形態は、第１のデバイスと第２のデバイスの間に通信を確立する方法を提供す

る。１つの方法は、取引鍵を求める要求を生成するステップと、要求を第１のデバイスの第１の変化識別子で暗号化するステップと、暗号化された要求を認証者デバイスへ送信するステップと、取引鍵を生成するステップと、取引鍵を含む第１のメッセージを生成するステップと、第１のメッセージを第１のデバイスの第１の変化識別子で暗号化するステップとを含むことができる。

【００２０】

実施形態は、変化識別子を使用して電子商取引を行う方法も提供する。１つの方法は、第１の変化識別子で購入者取引データを暗号化するステップと、購入者取引データを認証者デバイスへ送信するステップと、購入者の証明（ｃｒｅｄｅｎｔｉａｌ）を第１の取引鍵で暗号化するステップと、購入者の証明を支払い認証者デバイスへ送信するステップとを含むことができる。この方法は、ベンダ取引データを第２の変化識別子で暗号化するステップと、ベンダ取引データを認証者デバイスへ送信するステップと、ベンダの証明を第２の取引鍵で暗号化するステップと、ベンダの証明を支払い認証者デバイスへ送信するステップとも含むことができる。更に、この方法は、購入者取引データを解読するステップと、ベンダ取引データを解読するステップと、支払い認証者デバイスへの支払い要求を生成するステップと、支払い要求を第３の変化識別子で暗号化するステップと、支払い要求を支払い認証者デバイスへ送信するステップとを含むことができる。また、この方法は、支払い要求を解読するステップと、購入者の証明を解読するステップと、ベンダの証明を解読するステップと、購入者の証明、ベンダの証明、および支払い要求に基づいて第１の応答を生成するステップと、購入者の証明、ベンダの証明、および支払い要求に基づいて第２の応答を生成するステップと、第１の応答を購入者デバイスへ送信するステップと、第２の応答を購入者デバイスへ送信するステップとを含むことができる。

【００２１】

更に別の実施形態は、電子商取引システムを提供する。１つのシステムは、ベンダ・デバイスと、購入者取引データを第１の変化識別子で暗号化し、購入者取引データを認証者デバイスへ送信するように構成された購入者デバイスと、支払い要求を承認または拒絶し、購入者デバイスへの第１の応答を生成し、ベンダ・デバイスへの第２の応答を生成し、第１の応答を購入者デバイスへ送信し、第２の応答をベンダ・デバイスへ送信するように構成された支払い認証者デバイスと含むことができる。認証者デバイスは、購入者取引データを解読し、支払い認証者デバイスへの支払い要求を生成し、支払い要求を支払い認証者デバイスの第３の変化識別子で暗号化し、支払い要求を支払い認証者デバイスへ送信するように構成されることができる。

【００２２】

本発明の一代替実施形態は、暗号化を伴うが、変化識別子は伴わない。一例示的方法は、第１の購入者鍵で購入者取引データを暗号化するステップと、購入者取引データを認証者デバイスへ送信するステップと、購入者の証明を第１の取引鍵で暗号化するステップと、購入者の証明を支払い認証者デバイスへ送信するステップとを含むことができる。この方法は、ベンダ鍵でベンダ取引データを暗号化するステップと、ベンダ取引データを認証者デバイスへ送信するステップと、ベンダの証明を第２の取引鍵で暗号化するステップと、ベンダの証明を支払い認証者デバイスへ送信するステップも含むことができる。更に、この方法は、購入者取引データを解読するステップと、ベンダ取引データを解読するステップと、支払い認証者デバイスへの支払い要求を生成するステップと、支払い要求鍵で支払い要求を暗号化するステップと、支払い要求を支払い認証者デバイスへ送信するステップを含むことができる。また、この方法は、支払い要求を解読するステップと、購入者の証明を解読するステップと、ベンダの証明を解読するステップと、購入者の証明、ベンダの証明、および支払い要求に基づいて、第１の応答を生成するステップと、購入者の証明、ベンダの証明、および支払い要求に基づいて、第２の応答を生成するステップと、第１の応答を購入者デバイスへ送信するステップと、第２の応答を購入者デバイスへ送信するステップとを含むことができる。

【００２３】

変化識別子は好ましいものであるが、前の段落に記載される代替形態は、例えば非対称暗号化方式で実装されることができる。また、鍵が全く変更されないか、ごく時折変更される対称システムを使用することも可能である。本明細書に記載される他の電子商取引プロトコル、システム、および方式もそのように、即ち、非対称暗号化、非変動鍵、または時折変更される鍵を使用するように変更されてよい。

【００２４】

本発明の実施形態は、詳細な説明と図面を考察することにより明らかになろう。

【発明を実施するための最良の形態】

【００２５】

本発明の実施形態を詳細に説明する前に、本発明の適用は、以下の説明に述べられる、または図面に示される構成要素の構造および配置の詳細に限定されないことを理解されたい。本発明は、更に他の実施形態が可能であり、各種の方式で実施または実行されることが可能である。また、本明細書で使用される語句および用語は、説明を目的とするものであり、制限的なものとみなすべきでないことも理解されたい。

【００２６】

特に、本発明は、パーソナル・コンピュータや家庭用コンピュータ、サーバ、および、プロセッサを備え、プログラムや命令セットを実行することが可能な、例えばセット・トップ・ボックスなどの特殊目的のデバイスを含む他のデバイス等の各種コンピュータ・デバイスを使用して実装されることを理解されたい。一般に、本発明は、既存のハードウェア、または当業者により容易に作製されることが可能なハードウェアを使用して実装されてよい。従って、例示的デバイスのアーキテクチャは、一般にはプロセッサと、メモリ（何らかの種）と、入出力デバイスとを有するということを指摘する以外には、詳細には説明しない。幾つかの事例では、デバイスは、オペレーティング・システムと、オペレーティング・システムにより管理されるアプリケーション・プログラムも有する場合がある。ハードウェア・デバイスは一般には、実装される本発明の特定の実施形態におけるそのデバイスの役割に応じて、データを圧縮や、圧縮解除（伸張）し、データを符号化したり暗号化データを復号するいくらかの能力も必要とする。多くの事例では、伸張機能は、ハードウェア実装のＭＰＥＧコーデックなどの使用可能なコーデックを使用して提供されることができる。暗号解読機能（解読機能）は、選択された暗号化アルゴリズムを使用して暗号化されたデータを解読することが可能な解読用ハードウェアやソフトウェア・モジュールを使用して提供されることができる。本発明の実施形態で使用するのに適した暗号化アルゴリズムの１つは、Ｒｉｊｎｄａｅｌアルゴリズムであり、その一例は、ｈｔｔｐ：／／ｗｗｗ．ｅｓａｔ．ｋｕｌｅｕｖｅｎ．ａｃ．ｂｅ／～ｒｉｊｍｅｎ／ｒｉｊｎｄａｅｌ／ｒｉｊｎｄａｅｌｒｅｆ．ｚｉｐで入手することができる。

【００２７】

図１は、ネットワークを通じてコンテンツを配布するように構成された例示的システム２０を示す。当業者には明らかなように、実際には、インターネット、電話システム、ワイヤレス・ネットワーク、衛星ネットワーク、ケーブルＴＶネットワーク、および各種の他の私設および公衆のネットワーク等の１または複数のネットワークや通信システムが各種の組み合わせで使用されて、本発明の実施形態または実装をなすために要求または必要とされる通信リンクを、提供することができる。従って、本発明は、特定のネットワークまたはネットワークの組み合わせに限定されない。しかし、使用されるネットワークや通信システムは、データがＲｉｊｎｄａｅｌ暗号化の１つのバージョンで暗号化された通信、セキュア・ソケット・レイヤ（「ＳＳＬ」）通信、または他の通信などのような、セキュアな通信を支援する能力を有することが好ましい。更に、データは、配線、デジタル衛星サービス（「ＤＳＳ」）、または物理的に１人の当事者から別の当事者へ物理的に運搬される物理媒体で、１人の当事者から別の当事者へ送られることができる。

【００２８】

図１に示す実施形態では、システム２０は、コンテンツ所有者またはプロバイダ（提供者）２２、ケーブル会社やインターネット・サービス・プロバイダ等のサービス提供者（

プロバイダ）２４、消費者２６、および認証者２８、の４つの参加者（関係者）を含む。１つのみのコンテンツ提供者、サービス提供者、および消費者が示されているが、本発明の大半の実装では、多数のコンテンツ提供者、サービス提供者、および消費者が関係する。更に、必須なのは１つのみであるが、複数の認証者があってもよい。実際には、次の関係、すなわち、認証者の数＜コンテンツ提供者の数＜サービス提供者の数＜消費者の数、が存在する可能性が高いが、ここでも、関係者の数の制限や、各種関係者の数の間の特定の関係の要件はない。

【００２９】

図２に示す別の実施形態では、システム２０は、コンテンツ所有者または提供者２２、消費者２６、および認証者２８、の３つの関係者を含む。図には１つのコンテンツ提供者と消費者が示されるが、本発明の大半の実装では、多数のコンテンツ提供者と消費者が関係する。更に、上で述べたように、必須なのは１つのみであるが、２つ以上の認証者があってもよい。ここでも、関係者の数の制限や、各種の関係者の数の間の特定の関係の要件はない。

【００３０】

関係者２２、２４、２６、２８は、双方向リンク３０、３２、３４、３６、３８を介して相互に接続される。これらのリンクは、上記のネットワークのすべてまたは一部から構築される。システム２０は、鍵方式の暗号化アルゴリズムを使用し、Ｒｉｊｎｄａｅｌアルゴリズムなどの現在使用可能なアルゴリズムが使用されてよい。使用されるアルゴリズムの最終的な選択は、アルゴリズムの強度（解読されるという観点から見た）と速度（選択されたアルゴリズムで必要とされる数学演算を行うプロセッサの能力から見た）とのトレードオフを含む各種の要因に応じて決まる。

【００３１】

本発明の一実施形態では、消費者は、例えば「セット・トップ・ボックス」、家庭用コンピュータ、または他のデバイスの形態をとりうる復号プロセッサまたは同様のデバイスを有するものとする。同じ実施形態において、消費者が復号プロセッサの権利管理機能を改竄または他の方法で回避しようとする可能性があると言う意味で、復号プロセッサは「敵対環境」にあるものと想定される。そのため、復号プロセッサは、その内部への侵入を検出する能力を有する容器に収容されることが好ましい。また、復号プロセッサは、電力が供給されなくなった後もデータが損なわれずに保たれる不揮発性ＲＡＭ、ＥＰＲＯＭ、または他の記憶機構などの「永続的」なメモリを有することも好ましい。永続メモリは、識別情報を記憶するために使用され、識別情報は、好ましくは時間の経過と共に変化する「変化ＩＤ（ｍｕｔａｔｉｎｇ　ＩＤ）」であってよい。

【００３２】

好ましい実施形態では、システム２０は、乱数発生器を使用して、このシステムで実装または準拠されるプロトコルで使用される何らかの数を生成する。乱数発生器は、本発明の実装に使用される特定の技術で可能な限り真にランダムな数を生成することが好ましい。一実施形態では、コンテンツを入手するための消費者からの要求などのような通信トラフィックを使用して乱数を作成する。そのような要求は、一般には、予測不能な形で発生する。そのため、そのようなトラフィックに基づいて生成される乱数は、アルゴリズム的な方法で生成される擬似乱数と異なり、真またはほぼ真にランダムになる。

【００３３】

図の例示的実施形態では、システム２０のそれぞれのパーティー（当事者）２２～２８は、異なる責任を有し、それぞれの当事者は認証者２８を信頼するものと想定される。更に、コンテンツ提供者２２、サービス提供者２４、および消費者２６には、変化または変動する識別子（「ＩＤ」）が割り当てられることが好ましい。この識別子については下記で更に説明する。

【００３４】

コンテンツ提供者（“アリス（Ａｌｉｃｅ）”）

コンテンツ提供者（コンテンツ・プロバイダ）２２は、映画製作会社や、録音会社、あ

るいは電子的にコンテンツを配信することを望む任意の他のエンティティ等のエンティティである。一般には、コンテンツ提供者２２は、コンテンツの著作権または他の知的財産権を所有するか、または、そのような権利の所有者によりコンテンツの配布を許可されているものと想定される。コンテンツ提供者２２は、システム２０を使用して配布される自身のコンテンツの各コピーについて公正に支払いを受けることを望むものと想定する。また、コンテンツ提供者２２は、そのコピーが割り当てられたサービス提供者２４と消費者２６の両方まで自身のコンテンツの提供済みの各コピーを追跡することを望むものと仮定する。従って、本発明の一実施形態では、システム２０は、コンテンツ提供者２２が変化ＩＤ（一般には必要時に作成される）のリストを使用してコンテンツのライセンスの仮想目録を生成することができるように構成され、各ライセンスは、提供されたコンテンツのコピーを視聴する、または一部の事例では維持する、という権限を付与する。仮想目録（またはライセンスのセット）は、１または複数のサービス提供者等の各種の配布エンティティに割り当てられることができる。仮想目録が消費されると、何れのサービス提供者２４がその消費者の１人にコンテンツのコピーを提供したかを記録、ログにとる、または記すために、その消費が追跡される。例えば、仮想メモリを追跡することにより、ケーブル会社と衛星放送会社に配布権を販売した映画製作会社などのコンテンツ提供者は、それらエンティティ、即ち、ケーブル会社と衛星放送会社のどちらがそのコンテンツを対象消費者に配布したかを判断することができる。好ましい実施形態では、コンテンツ提供者２２が自身のコンテンツの唯一の暗号化実施者（ｅｎｃｒｙｐｔｅｒ）であり、下記で更に説明するように、例えば要求を拒絶することにより、コンテンツの復号を制御する。

【００３５】

本発明の別の実施形態では、システム２０は、コンテンツ提供者２２が透かし（ｗａｔｅｒｍａｒｋ）のリストを生成し、自身のコンテンツの各コピーに一意の透かしを適用し、変化ＩＤ（一般には必要時に作成される）のリストを使用して、透かしが入れられたコンテンツについてのライセンスの仮想目録を生成することができるように構成される。ここで、各ライセンスは、提供された透かし入りコンテンツのコピーを視聴する権限、または事例によっては保持する権限を付与する。仮想目録（即ち、ライセンスのセット）は、１または複数のサービス提供者などの各種の配布側エンティティに割り当てられることができる。仮想目録が消費されると、何れのサービス提供者２４がその消費者の１人にコンテンツのコピーを提供したか、更にはどの消費者が特定の透かし入りコンテンツを受信したかを記録、ログにとる、または記すために、その消費が追跡される。例えば、仮想メモリを追跡することにより、ケーブル会社と衛星放送会社に配布権を販売した映画製作会社などのコンテンツ提供者は、それらエンティティ、即ち、ケーブル会社と衛星放送会社のどちらがそのコンテンツを対象消費者に配布したかを判断することができる。透かし入りのコンテンツは特定の消費者に対応付けられる（マップする）ことができるので、追跡システムは、個々の消費者の消費活動を記録またはログ記録することも可能にする。

【００３６】

サービス提供者（“ボブ（Ｂｏｂ）”）

図の実施形態では、サービス提供者（サービス・プロバイダ）２４が、コンテンツ提供者のコンテンツを配布する。しかし、サービス提供者は、変化ＩＤによる自身と対象コンテンツの識別を含む幾つかの追加的な責任を負ってもよい。ここで説明する実施形態では、適切な変化ＩＤを持たない消費者２６等のユーザは、コンテンツを復号することができない。多くのシナリオでは、サービス提供者２４は、サービス提供者２４にとってローカルな記憶デバイスから、要求されたコンテンツを提供する。しかし、本発明では、コンテンツの場所は何れの特定の場所にも限定されず、コンテンツは、コンテンツ提供者２２のストレージから取り出され、その後消費者２６に転送されてもよい。本発明の好ましい実施形態では、すべてのサービス提供者２４がシステム２０内の消費者からの各要求を見て、認証者２８から認証を受信する。一部の実施形態では、特定の実施形態におけるサービス提供者の何れか１つが、コンテンツを消費者へ発送または転送する役割を担ってよい。これにより、コンテンツ提供者は、望まれる場合には、自身のコンテンツをサービス提供

者に配信する必要性を回避することができる。即ち、サービス提供者２４は、消費者から注文されたコンテンツを（ローカルのストレージに暗号化されたコピーを保持すること等により）所有する必要がない。

【００３７】

消費者（“キャロル（Ｃａｒｏｌ）”）

少なくとも一部の消費者が代金を支払わずにコンテンツを視聴または消費することを望む、または、試みる場合があるものと想定する。そのため、不正なコンテンツの消費を防止するための措置が提供される。上述の変化ＩＤは、コンテンツの復号、および、従ってコンテンツの消費を規制するための１つの機構を提供する。複数の変化ＩＤをカプセル化することにより、下記でより詳細に説明するように、セット・トップ・ボックスは、認証者２８に対して、１）そのセット・トップ・ボックスが、認可されたコンテンツのデコーダであること、２）サービス提供者２４が認可されたコンテンツの配布者であること、および、３）コンテンツ自体が、消費者のためにコンテンツ提供者２２により使用を認可されたこと、を証明することができる。

【００３８】

認証者（“トレント（Ｔｒｅｎｔ）”）

認証者２８は、特定のコンテンツ、または適用可能な場合には透かし入りのコンテンツを復号するために必要なデータを保持するリポジトリである。ここで論じる実施形態では、認証者２８は、対象消費者２６に復号の情報を送信する前に、消費者２６、サービス提供者２４、およびコンテンツをそれらの変化ＩＤで検証する。認証者２８は、変化ＩＤの供給元でもあり、データベースあるいは同様の機構を使用してそのＩＤを追跡する。

【００３９】

変化ＩＤ

例示的な変化ＩＤ３８が図３ａに示されている。変化ＩＤ３８は、第１の部分４０と第２の部分４２の２つの部分を有する識別子である。第１の部分４０は、識別番号であり、これは乱数である。第２の部分４２は、符号化／復号化鍵であり、これも乱数であり、好ましくは対称暗号鍵である。本明細書で論じる実施形態で実装される場合、変化ＩＤは、１回のみ使用されることができ、その後再度使用できない。変化ＩＤは、認証者２８により生成され、追跡される。変化ＩＤは、使い捨て（ｏｎｅ－ｔｉｍｅ－ｕｓｅ、一回使用）の機構なので、サービス提供者または消費者または他のエンティティが自身に供給された分の変化ＩＤを使用してしまうと、認証者２８から追加的な変化ＩＤを入手しなければならない。変化ＩＤ中のデータは、すべての変化ＩＤの確率を等しくしてランダムに選択される。特定のコンテンツの要求または復号が行われると、３つの変化ＩＤ（消費者、サービス提供者、コンテンツ）が破棄され、下記でより詳細に説明する要領で、更なる取引のための新しい変化ＩＤが生成される。システム２０の当事者にどのように変化ＩＤが配布されるかに関する情報も図３ｂおよび３ｃで提供される。具体的には、このシステムのエンティティは、望まれる使用に応じて、多数の変化ＩＤまたは単一の変化ＩＤを受け取ることができる。本発明の一実施形態では、コンテンツ提供者とサービス提供者の両方の機能を行うことができる提供者４３が、認証者に複数の数／鍵の対を要求することができる。コンテンツ・アイテムの各コピーは、一意の数／鍵の対から作られる一意のライセンスを持たなければならないため、それぞれの提供者４３は、多数の数／鍵の対を必要とする。認証者は、提供者４３が要求する数だけの変化ＩＤを作成し、対のリスト２６を提供者４３に送り返す。提供者４３は、要求した数／鍵の対の数量と各対のサイズを把握しており、リストを個々の数／鍵の対に分ける。本発明の他の実施形態では、コンテンツ配布システムの各エンティティは、自身を認証者に対して識別するために変化ＩＤを必要とし、１つの変化ＩＤを使用すると、エンティティは、認証者に新しい変化ＩＤを要求する。１つの新しい変化ＩＤがそのエンティティへ送信され、その新しい変化ＩＤがエンティティの以前の変化ＩＤに取って代わる。

【００４０】

明らかなように、本発明の実施形態は、対称鍵システムである。対称鍵システムは、通

例、システムのエンティティ数が増えるにつれて、鍵管理の問題が生じる。例えば、ｎ個のエンティティからなるネットワークは、すべてのエンティティが互いと通信することを可能にするためにｎ（ｎ－１）／２個の鍵を必要とする。従って、１０００個のエンティティのシステムで、すべてのエンティティが同じコンテンツをすべての他のエンティティへ送信したい場合には、５０万個近くの鍵が必要となる。

【００４１】

しかし、ここに開示される実施形態は、システムのすべてのエンティティ対に対して別個の鍵を必要としない。下記で例示するように、各エンティティと配布されるコンテンツは、１つの鍵を受け取り、その鍵は１回使用されるごとに変更される。１０００個のエンティティからなるシステムの場合は、以前の対称鍵システムにおける５０万個近くの鍵と比べて、わずか２０００個の鍵で済む。また、認証者は、変化ＩＤのビット列全体を記憶する必要はない。認証者は、ハッシュ関数または単に位置のインデックスを使用して、変化ＩＤの各鍵パーティションを、対応する数に基づくメモリ記憶位置に対応付けることができる。

【００４２】

本発明の実施形態と以前のセキュリティ・システムとの他の違いは、速度と、特定の攻撃に対する脆弱性の低下とに関する。対称鍵の使用により高速の計算も可能になり（公開鍵システムと比べて）、選択平文攻撃の影響を低減させる。本発明の実施形態は、公開鍵ではなく対称鍵を使用するため、比較的高速である。公開鍵システムの背後にある基本的な概念は、一方向関数の使用である。一方向関数は、計算が容易であるが、逆方向に計算するのが難しい。公開鍵システムは、逆方向に一方向関数を計算するための鍵を提供するトラップドア一方向関数を使用する。公開鍵システムは、自由に使用され、メッセージに適用する一方向関数として使用される公開鍵を、各関係者に提供する。公開鍵システムは、一方向関数の計算を与えられたメッセージを計算するために、プライベート鍵（少なくとも当初の考えでは公開鍵からは導出できない）も各関係者に提供する。公開鍵システムのセキュリティは、公開鍵からプライベート鍵を導出できないことに依拠する。この要件を維持するために、公開鍵システムで使用される一方向関数は複雑である。しかし、この複雑性の増大は、計算時間が増すという代償となる。公開鍵システムは、しばしば、対称鍵システムよりも１０００倍低速である。

【００４３】

攻撃への脆弱性が低下することに関しては、選択平文攻撃は、侵入者が暗号鍵または暗号化プロセスへのアクセス権を持ち、暗号化する特定の平文を選択し、暗号化されたテキストから知識を得ることを試みる時に発生する。公開鍵システムでは、一人の個人の公開鍵は、通信システム内のすべての関係者に知られる。どの侵入者でも、個人の公開鍵を使用して無限数のメッセージを暗号化することができる。攻撃者がある個人の公開鍵で適当なメッセージを暗号化し、その後、その個人へ送信される暗号化メッセージを傍受した場合、侵入者は、傍受したメッセージを、自身が作成したメッセージと比較することができる。傍受メッセージが、侵入者により作成された暗号化メッセージと一致する場合、そのメッセージは危険にさらされたことになり、侵入者は、自分宛ではないメッセージを読むことができるようになる。この攻撃は、少数の適当なメッセージが存在する場合には容易で効果的であるが、メッセージの数が、侵入者が暗号化することが可能なメッセージの数または傍受した暗号化メッセージと比較することが可能なメッセージの数よりも多い場合でも、傍受された暗号化メッセージが特定のメッセージと対応しないということが分かることだけでも、侵入者には有用な情報が得られたこととなる。何れの状況でも、侵入者は、その個人のプライベート鍵は推測できないが、その個人へ送信されるメッセージまたはそのメッセージに関する情報は推測できる可能性がある。本発明の実施形態は対称鍵システムを使用し、暗号鍵が公に知られていないので、選択平文攻撃を適用することができない。

【００４４】

従来の対称鍵システムおよび公開鍵システムには別の問題もある。権限のないエンティ

ティが、権限のある鍵へのアクセス権を得ると、その権限のないエンティティは、その汚された鍵で暗号化されたすべてのメッセージを復号することができ、そして恐らくはより危険なことには、偽のメッセージを暗号化してそのシステムの他のエンティティをだますことができる。変化ＩＤプロトコルは、使用された後にそれぞれの対称鍵を変化させることにより、この脆弱性を低減する。鍵が汚された場合でも、汚された鍵は、認証者により使用済みとしてマークされ、メッセージの暗号化には二度と使用されないため、将来のメッセージの生成にも将来のメッセージの解読にも使用されることができない。

【００４５】

プロトコル

システム２０は、プロトコルを使用してエンティティ間の通信を制御する。各エンティティには、認証者２８により以前に変更されたＩＤにタグ付けされる使い捨て（ワンタイム・ユーズ）の数／鍵の対、即ち、変化ＩＤ（図３ａに示す識別子あるいはＩＤ３８）がランダムに割り当てられる。先に述べたように、それぞれの変化ＩＤは、乱数４０と、それに対応するランダムの符号化鍵４２を含む。使い捨ての数／鍵の対は、変更されたハッシュの形態をとることができる。ランダムであることに加えて、使い捨ての数／鍵の対またはハッシュは、一度解読されるごとに直ちに破棄される。言い換えると、このプロトコルは、ハッシュまたは使い捨ての数／鍵が必要とされる時には、それまでに使用されたことのない新しい乱数を生成する。コンテンツ配布システムに参加するエンティティを識別することに加えて、使い捨ての数／鍵は、それを使用するエンティティとは完全に無関係のハッシュでもある。即ち、このハッシュは、エンティティの識別に関する何の情報も含まない。このようにして、エンティティの識別は、認証者２８を除いてはどの関係者にも公開されない。

【００４６】

認証者２８は、システム２０を通じて配布されるコンテンツの暗号鍵も生成する。コンテンツの配布を希望するエンティティは、何れも鍵を要求する。コンテンツを送信する側のエンティティは、配布するコンテンツの関数または識別文字列を認証者に供給し、認証者は、関連した鍵で応答する。鍵は、変化ＩＤと同様に、その鍵が暗号化するコンテンツには関係しない。コンテンツの関数またはランダムの識別子のみが提供されるので、認証者も真のコンテンツについての知識を持たない。認証者は、コンテンツの鍵および関連した関数、または識別文字列を記録する。認証者は、合法な要求を行うシステム２０の許可されたエンティティに鍵を供給する。コンテンツ・アイテムに関連した鍵を求める要求は、そのコンテンツ・アイテムの関数または識別文字列への参照を含む。認証者２８は、要求に示される関数または識別文字列と一致する鍵を探し、見つかった鍵を返す。

【００４７】

システム２０の特定の実施形態は、暗号化アルゴリズムおよび乱数発生器とともに実装される。暗号化アルゴリズムは、好ましくは、対称鍵に基づく暗号化アルゴリズムである。鍵は、順列の識別、オフセット、およびスキップである。これら３つすべてがまとめられて、「鍵」と呼ばれる１つのオブジェクトにされることができる。従って、本発明の実施形態では、任意の鍵方式の暗号化アルゴリズムが使用されることができる。新しい暗号化アルゴリズムの導入は、非常に時間がかかるプロセスである可能性があるので、システム２０は、既存の試験済みの鍵方式暗号化アルゴリズムの使用を可能にするように作成された。

【００４８】

乱数の発生に関して、ここに示す実施形態では、３つの異なる手順が使用される。無論、乱数の手順の他の組み合わせを使用して乱数を発生させてもよい。第１の乱数発生手順は、標準的な合同法乱数である。第２の乱数発生手順は、ランダム・ストリームのサンプリング・レートを決定するために使用される乱数を生成する。

【００４９】

ランダム・ストリームの入手は、困難である可能性がある。従来の定義によると、ランダム・ストリームまたは数の集合は、その集合が、それらの数を表す最もコンパクトな方

式である時に限り、ランダムとみなされる。例えば、集合２、４、６、８、１０、
【数１】

を与えられた場合には、よりコンパクトな表現は、｛２ｉ｜ｉ∈Ｚ＋｝、即ち、正の整数の集合中のすべての偶数となる。これを示す別の方法は、識別可能な「パターン」が存在しない数の集合である。暗号化通信の目的は、送信される暗号化データからすべてのパターンを取り除き、それにより、知的な推測を使用して暗号化送信データを解読することができないようにすることである。システム２０の実施形態では、認証者２８が、コンテンツの配布および送信で使用されるすべての乱数を提供する。より詳細に述べるように、生成される数の数列は、乱数の数列、即ち、ランダム・ストリームであるか、または、少なくとも、ランダム・ストリームに近似したものである。
【００５０】
乱数発生器の第３のプロセスは、次の数を取り出すための決定的な方法がないことを保証することである。認証者２８に到来し、認証者２８から出て行くランダム・ストリームは、暗号化されており、それにより暗号化データを含んでいる。ランダム・ストリームを生成するために使用されるこの非決定的な機構は、乱数の数列がそれよりコンパクトな表現で表せないことを保証し、従って、ランダム・ストリームを定義することを助ける。
【００５１】
例えば、認証者２８は、コンテンツを復号する要求を受け取るように設計される。それらの要求は、ランダムな順序で認証者２８に到着する。例えば、消費者Ｘが映画Ｙの鍵を要求し、消費者Ｗが歌曲Ｚの鍵を要求する等と想定する。これらの要求は、意図的に任意とするか又は任意の鍵で暗号化されるかの何れかになるように任意に選択された数の列として、プロトコルにより形式付けられる。要求は本質的に任意であり、任意に処理されるため、必然的に乱数のストリームが生成される。このストリームを準任意の方式（即ち、合同法乱数）でサンプリングすることにより、良好な乱数の数列が生成される。
【００５２】
一実施形態では、システム２０で使用されるプロトコルは、パケット組立／分解生成器即ちＰＡＤ、鍵のペアリング、およびＲＣ４ランダム・ストリーム暗号を組み合わせる。より具体的には、あるデータ・ウィンドウ中の情報を暗号化するには、ＰＡＤ生成器が選択されるとＰＡＤの数列が生成される。そのＰＡＤの数列に基づいて次のように第２のランダム・ストリームＰが生成される。
【００５３】
【数２】

$$p_k = pad_{(k_i) \bmod n} \otimes pad_{(k_{i+1}) \bmod n} \otimes \cdots \otimes pad_{(k_{i+j}) \bmod n}$$

【００５４】
ここでp_kは、Ｐの数列のｋ番目のエレメントであり、$pad_{(kj) \bmod n}$は、ＰＡＤの数列のｊ番目のエレメントである。即ち、Ｐの数列のエレメントはすべて、ＰＡＤ生成器で生成された数列のエレメントの排他的論理和（排他的ＯＲ）の組み合わせとなっている。鍵の対は、一般に、公開鍵とプライベート鍵を含む。それらの鍵は、数学的関係は持たない。それらの鍵はランダムに、かつ互いからは独立して生成される。鍵自体は、単に、２０桁以上の数である。各エンティティは、一意の鍵の対を有する。
【００５５】
次いでプロトコルの例示的実施形態をより詳細に説明する。図１に示す実施形態では、コンテンツ提供者２２が暗号化を行う（時に「暗号者」と呼ぶ）。コンテンツ提供者２２は、特定の鍵または鍵のセットＫでコンテンツを暗号化する。コンテンツ提供者２２が鍵のセットＫを記憶または保持するか、あるいはそれに代えて認証者２８が鍵のセットを保持してもよい。認証者２８に保持される場合、認証者２８は、鍵のセットＫを秘密に保持

する。コンテンツ提供者のコンテンツには、秘密の識別ラベル（例えば一般には決して変化しない数）が割り当てられる。このラベルが認証者２８に与えられ、認証者は、ラベルを、暗号化されたコンテンツを復号するのに必要とされる鍵に関連付ける。関連付けのプロセスは実際の鍵へのエンティティのアクセスは提供しないため、この関連付けは、間接的である。コンテンツの解読に必要な実際の鍵を持っているのがコンテンツ提供者と認証者のみであるため、これで、暗号化されたコンテンツは、権限のない復号が行われる恐れなく、サービス提供者２４または別のエンティティへ与えられることができる。この時点で、コンテンツ提供者２２は、コンテンツの仮想目録を作成する。この作成には、コンテンツ提供者２２が必要とする又は持つことを望む数だけの変化ＩＤを認証者２８に要求することが、伴う。それぞれの変化ＩＤは、正確に１度のコンテンツの使用または消費を許可するライセンスに相当する。先に述べたように、変化ＩＤは、数と鍵である。コンテンツ提供者２２は、変化ＩＤ鍵で識別ラベルを暗号化し、変化ＩＤの数と暗号化された識別ラベルとを、「暗号化識別子」と称される１つのデータにまとめ、このデータは、ここでは「$E_{content}$」（Ｅコンテンツ）と表される。

【００５６】

１つのコンテンツが消費されると、認証者２８は、その特定のコンテンツの供給元であったサービス提供者２４を追跡し、そのような復号があるたびにコンテンツ提供者２２に復号を通知する。サービス提供者２４は、コンテンツを受信すると、消費者２６に配布する前に、それぞれの暗号化コンテンツを他の識別データと組み合わせる。それぞれのサービス提供者２４は、その特定のサービス提供者を識別するために使用される変化ＩＤの集合を手元に保持する。すべての他の変化ＩＤと同様に、それらの変化ＩＤは、認証者２８により作成され、追跡される。サービス提供者２４は、各コンテンツについての$E_{content}$識別子のリストも有する。要求されると、サービス提供者２４は、未使用の$E_{content}$識別子と、所有する未使用変化ＩＤの１つとを選択する。サービス提供者は、選択した変化ＩＤの鍵で$E_{content}$識別子を暗号化し、関連した数を付加して、本明細書で「配布可能コンテンツ」または「$E_{distrib}$」（Ｅ配布）と称するデータを作成する。サービス提供者２４は、$E_{distrib}$コンテンツを消費者２６へ送信し、復号を許可する認証者２８からの確認信号を待つ。

【００５７】

確認信号は、$E_{distrib}$コンテンツを作成するために使用された変化ＩＤ鍵で解読されることができる、暗号化されたデータのまとまり（ｐａｒｃｅｌ、パーセル）として受信される。確認信号は、サービス提供者２４と認証者２８により設定された、合意済みの秘密のバイトのセットである。確認信号が受信され検証されると、サービス提供者２４は、暗号化コンテンツ即ち$E_{content}$識別子を消費者２６へ送信することができる。

【００５８】

上記で述べたように、消費者２６がシステム２０に不正を働こうとしていると仮定する。この理由から、消費者２６と認証者２８間のすべての通信は、何らかの暗号化通信方法で暗号化される。消費者２６には、１度に１つのみの変化ＩＤが与えられる。消費者２６が何らかのコンテンツを視聴または受信したい時、消費者２６は、消費者２６の場所に配備されたセット・トップ・ボックスまたはハードウェアを使用して、所望のコンテンツの選択を行う。ハードウェア・デバイスは次いで、サービス提供者２４にそのコンテンツを要求し、サービス提供者２４は、特定の復号のために$E_{distrib}$コンテンツを送信する。$E_{distrib}$コンテンツが消費者２６に受信されると、$E_{distrib}$コンテンツは、消費者の変化ＩＤ鍵で暗号化され、変化ＩＤの数と結合されて、$E_{consumer}$（Ｅ消費者）識別子と称される消費者識別子とされる。$E_{consumer}$識別子は、次いで検証のために認証者２８へ送信される。検証されると、認証者２８は、消費者のセット・トップ・ボックスが対象コンテンツを消費することを認可されていることを、セキュアな通信路でサービス提供者２４に通知する。認証者２８はまた、現在のセット・トップ・ボックスの変化ＩＤを破棄し、セット・トップ・ボックスに新しい未使用の変化

ＩＤを送信する。

【００５９】

消費者２６は、同時に別々の供給元から、暗号化されたデータと、そのデータを解読するために必要な鍵を受信する。これにより、復号デバイスは、要求したコンテンツを復号することができる。

【００６０】

変化ＩＤの生成とその追跡は、認証者２８の主要な作業である。コンテンツ提供者とサービス提供者への変化ＩＤの配布は、それぞれの受信者だけに変化ＩＤが秘密に保たれる限り、両者へのどのような許容可能な手段を介して扱われてもよい。消費者が絶対に１つより多くの変化ＩＤを持たないことを確実にするために、Ｅ$_{consumer}$識別子が正確なものであると検証されると、新しい変化ＩＤは、その消費者の現在の変化ＩＤ鍵を使用して暗号化され、消費者２６へ送信される。そして、消費者は、次の取引にそのＩＤを使用することができる。認証者２８は、すべての変化ＩＤを常に把握しているので、Ｅ$_{consumer}$識別子が有効な要求であること、または有効な要求を含んでいることを検証することができる。検証するために、認証者２８は、Ｅ$_{consumer}$識別子の中の数に関連した鍵を見つけ、その鍵を解読し、Ｅ$_{consumer}$識別子を明らかにする。鍵が見つからない場合、認証者２８は、「失敗」と返す。全く同じプロセスを使用して、認証者２８は、Ｅ$_{content}$識別子を復元する。鍵が見つからない場合は、認証者２８は「失敗」を返す。再度、認証者２８は、可能であれば、Ｅ$_{content}$識別子を解読する。解読が可能であれば、認証者２８は、サービス提供者２４の確認コードを調べ、サービス提供者２４により使用される変化ＩＤ鍵でその確認コードを暗号化し、サービス提供者へ返す。次いで、新しい変化ＩＤが送信され、続いて復号用のデータが送信される。認証者２８は次いで、課金の目的で、その取引に関わるすべての関係当事者、時刻、およびコンテンツを記載または他の方法で記録する。

【００６１】

上記で述べたように、本発明の一態様は、コンテンツのコピーが、権限のないエンティティまたは認可されていないエンティティに入手されないことを保証することである。ここで論じる実施形態では、コンテンツの不正コピーを入手するには、個人またはエンティティは、メッセージを傍受し、次いで、暗号化されたコンテンツを解読することが必要となる。コンテンツが傍受された（これは些細な作業ではない）場合でもそのコンテンツを復号することは非常に難しいので、少なくとも実際的な意味では上記の事は不可能である。その理由は、一つには、ここで論じられる乱数と暗号化アルゴリズムを使用すると、解読に非常に長い時間（数年単位、本発明者の意見では数千年）を要する暗号化データを作成することが可能なためである。種々の攻撃は、一般に、Ｅ$_{consumer}$識別子を正しく推測するか、または他の形で入手することを必要とする。しかし、それぞれの変化ＩＤは、そのＩＤの管理者により一回しか使用されないため、別のＥ$_{consumer}$を調べることにより或るＥ$_{consumer}$識別子を推測する方法はない。更に、変化ＩＤは、ランダムになるように計算される（乱数発生器の限界まで）ので、別の変化ＩＤから或る変化ＩＤを計算することは不可能である。

【００６２】

高度のセキュリティを提供することに加えて、このプロトコルは、それぞれの立場の当事者が入れ替え可能であることを考慮する。即ち、複数のコンテンツ提供者が、複数のサービス提供者を使用して、すべての当事者に同意された認証者２８を使用して複数の消費者に接触することができる。更に、立場は、多くの異なる配布モデルに適合するように容易に併合または変更されることができる。しかし、一般には、仮想目録はコンテンツ提供者２２および／またはサービス提供者により保持されることが要求される。上記で述べたように、仮想目録は、秘密の変化ＩＤを含むリストであることが好ましい。仮想目録は、他の商品のように取引されてよい。そのため、個々のデータは、所望のコンテンツの実際のデジタル・コンテンツであるのではなく、個々のデータは、そのコンテンツを１回視聴させることになる特定の事象のセットにより構築されるＥ$_{consumer}$識別子になる

。Ｅｃｏｎｓｕｍｅｒ識別子は、間係する全ての当事者の協力なしには構築されることができないので、すべての当事者は、消費者２６の要求時に、交渉し、デジタル・コンテンツの消費について相互に利益をもたらす取り決めに達するための能力を有する。１人の当事者が不参加を決めた場合には、認証者２８との通信は、１または複数の当事者の同意を取り下げることにより、復号を阻止することができる。

【００６３】

上記で述べたように、システム２０は、４つの当事者のみに限定されない。より多くの配布層が導入され、同じ方式で解明プロセスを通じて検証されることができる。例えば、１つのサービス提供者２４が、別のサービス提供者に配布を行うことができる。認証者２８は、コンテンツ提供者２２を見つけるまでＥｃｏｎｓｕｍｅｒ識別子を解き続けることができる。これは、Ｅｃｏｎｓｕｍｅｒ識別子を作成するために使用される単純な再帰アルゴリズムにより達成されることができる。重要な特徴は、認証者２８のインプリメンテーションが、Ｅｃｏｎｓｕｍｅｒ識別子に基づいてコンテンツの最終的な復号を制御することである。コンテンツ提供者２２またはサービス提供者２４がダウンストリームの配布を制御したい場合、特定の状況ではコンテンツの復号を拒否することを認証者２８に伝えることにより、容易に制御することができる。

【００６４】

次いで、本発明の実施形態を数例を使用して説明する。

【００６５】

通信プロトコルの多くの説明と同様に、このプロトコルで使用される各種エンティティ（またはそれらのエンティティに関連したコンピュータ・システム）には名前が割り当てられる。一実施形態では、アリス（Ａ）、ボブ（Ｂ）、およびキャロル（Ｃ）が、プロトコルの様々な関係者を表し、トレント（Ｔ）が信頼される通信の調整者（ａｒｂｉｔｅｒ）を表す。下の表、表１は、このプロトコルの複数の実施形態を説明するために本文献で使用される他の記号の一覧である。

【００６６】

【表１】

記号	意味
A, B, B′, C, T	プロトコルを用いるエンティティ
M	コンテンツ・アイテム
Ｘｉｄ	例えばｅメール・アドレス、アカウント番号などのような、Ｘの何らかの（秘密ではない）デジタル識別子
Ｘｃｒｅｄ	Ｘを識別する秘密の情報または証明書
Ｋｘ	何らかのエンティティＸと関連する対称鍵暗号の鍵
Ｎｘ	何らかの鍵Ｋｘと関連する一回使用（使い捨て）番号
Ｈ（Ｘ）	Ｘのハッシュを作る関数
Ｅ（Ｋ, Ｘ）	ＸをＫで暗号化する暗号
Ｄ（Ｋ, Ｘ）	Ｋを用いてＸを解読する暗号
Ｗ（Ｄ, Ｘ）	透かしＤをＸに適用する透かし関数
Ｘ→Ｙ：Ｘ	ＸからＹへ送られるメッセージＺ
{(N^{i}x, K^{i}x)}	エンティティＸと関連する任意のサイズの番号と鍵の対の組

【００６７】

このプロトコルの例示的実施形態は、上記のエンティティのうちの３つに関係する。エンティティ・アリスまたはＡがコンテンツ提供者２２の役割を行い、エンティティ・キャロルまたはＣが消費者２６の役割を行い、エンティティ・トレントまたはＴが認証者２８

の役割を行う。この提案されるプロトコルは信頼される権限者に依拠するため、アリスとキャロルはトレントを信頼する。また、アリスは、数（N_A）と、何らかの対称暗号の鍵（K_A）との、２つの秘密を有する。同様に、キャロルは、秘密の数（N_C）と鍵（K_C）を有する。更に、すべての割り当てられる数と鍵は、トレントにより割り当てられ、知られる。

【００６８】

この例のみの目的で、アリスが電子メール・メッセージP_1をセキュアにキャロルへ送信したいとする。無論、アリスは、各種のコンテンツ・アイテムを配布することを必要とする任意のエンティティを表すものでもよい。テキスト・メッセージの他に、アリスは、本明細書に記載されるプロトコルを使用して、音楽、画像、映像、データ等を配布することもできる。

【００６９】

初めに、アリスがメッセージP_1をキャロルへ送信したい場合、アリスは、メッセージP_1用の鍵、すなわち、P_1を暗号化するためにアリスが使用するものであり且つP_1を解読するためにキャロルが使用する鍵を、要求する。そのために、アリスは、メッセージのハッシュを作成する関数を使用してメッセージP_1のラベルを作成し、そのラベルを彼女のK_Aで暗号化し、N_Aを先頭に付加する。

【００７０】

$A \rightarrow T : N_A E(K_A, H(P_1))$

【００７１】

トレントがアリスからの要求を受信すると、トレントは、アリスの秘密を知っているので、N_Aに関連した鍵を調べ、メッセージP_1に使用される鍵の要求を復号する。しかし、トレントは、メッセージＰは受信せず、メッセージP_1のハッシュのみを受信する。トレントは次いで、鍵K_{P1}を生成し、今後の参照のために、その鍵K_{P1}を、供給されたハッシュに関連付けることができる。このプロトコルを使用すると、メッセージはトレントからさえセキュアに保たれ、トレントにより生成された鍵は、その鍵がその後暗号化するデータに関して何の有用な情報も提供しない。トレントは、アリスにより生成されたメッセージを直接知ることを可能にする情報や、アリスにより生成されたメッセージを望まれない当事者へ送信することによりシステムを損壊させることを可能にする情報は、受信しない。各数／鍵の対は１回の使用に有効なので、アリスは、新しい変化ＩＤも要求する。トレントは、メッセージP_1のための鍵K_{P1}と、新しい秘密の数（N'_A）と、新しい秘密鍵（K'_A）をアリスに供給する。トレントは、これら３つのエレメントをアリスの元の秘密鍵で暗号化し、そのメッセージをアリスに送り返す。

【００７２】

$T \rightarrow A : E(K_A N'_A K'_A K_{P1})$

【００７３】

アリスは、トレントから受信した自身の新しい秘密の数と鍵を認識し、メッセージP_1のハッシュを新しい秘密鍵K'_Aで暗号化し、N'_Aを先頭に付加し、メッセージをキャロルへ送信する。

【００７４】

$A \rightarrow C : N'_A E(K'_A, H(P_1))$

【００７５】

キャロルは、アリスからのメッセージを受信すると、自身の秘密鍵K_Cでそのメッセージを暗号化し、自身の秘密の数N_Cを先頭に付加し、メッセージをトレントへ送信する。

【００７６】

$C \rightarrow T : N_C E(K_C, N'_A E(K'_A, H(P_1)))$

【００７７】

トレントは、N_Cがキャロルのものであることを認識し、キャロルにより行われた外側の暗号化を解読することができる。トレントは、N'_Aがアリスの秘密鍵であることを認識しているので、アリスにより行われた内側の暗号化も解読することができる。解読する

と、トレントは、H（P_1）がアリスが以前へ送信したメッセージのハッシュであり、自分が以前にそのために鍵K_{P1}を作成したことを判断する。トレントは次いで、アリスがキャロルへメッセージP_1を送信してよいことを知らせるための、アリスへの受領証を生成し、メッセージP_1のために以前に生成された鍵とメッセージP_1のハッシュとをキャロルへ送信する。トレントがアリスのために生成する受領証は、メッセージのハッシュ（キャロルがそのメッセージのハッシュのための解読鍵を要求している）、この例ではH（P_1）と、キャロルの識別C_{id}とを含む。メッセージとそのメッセージを受信するエンティティの両方を識別することにより、アリスは、正しい受信者が正しいメッセージを受信することを保証される。キャロルが意図する受信者ではないか、またはメッセージのハッシュがキャロル宛のメッセージではない場合、アリスは、トレントにより生成された受領証に含まれる情報に基づいて、メッセージP_1を送信しないことを選択してよい。アリスがメッセージP_1をキャロルへ送信しないことを選択した場合は、キャロルがトレントからそのメッセージ用の解読鍵K_{P1}を受信していても、メッセージP_1は汚されない。キャロルが受信する鍵（トレントが生成）は、それにより暗号化することになっていたメッセージに関する情報は含んでいない。そのため、アリスがメッセージP_1を送信しない場合、キャロルは、鍵K_{P1}を持っていることだけではメッセージP_1の内容を推定することはできない。アリスとキャロルはどちらも自分の現在の秘密鍵と数を使用してしまったので、トレントは、アリスとキャロルの両方に新しい数／鍵の対も生成する。トレントは、受領証（アリスの新しい秘密の数N''_Aと秘密鍵K''_A）を連結し、連結したエレメントをアリスの現在の秘密鍵K'_Aで暗号化し、メッセージをアリスへ送信する。トレントは、メッセージP（キャロルの新しい秘密の数N'_Cと秘密鍵K'_C）の解読鍵K_{P1}を連結し、連結したエレメントをキャロルの現在の秘密鍵K_Cで暗号化し、メッセージをキャロルへ送信する。

【００７８】

$T \rightarrow A : E(K'_A, N''_A K''_A H(P_1) C_{id})$

$T \rightarrow C : E(K_C, N'_C K'_C K_{P1} H(P_1))$

【００７９】

トレントからのメッセージを受信すると、アリスは、メッセージを復号し、受領証でトレントから彼女へ返されたハッシュH（P_1）が、彼女がキャロルへ送信したハッシュと同じであるかどうかを判断することができる。これは、アリスに、メッセージを送信する前に、メッセージと意図される受信者とを再確認する機会を与える。上述したように、受領証の何れかの部分が不正であるように思われる場合、例えば、メッセージのハッシュが、アリスがキャロルへ送信したかったメッセージではない場合や、キャロル以外の受信者がメッセージの解読鍵を要求している場合に、アリスは、単に、トレントが生成した鍵で暗号化されたメッセージP_1を送信しなければよい。すべてが正しく思われる場合、アリスは、トレントにより生成された鍵K_{P1}でメッセージP_1を暗号化し、暗号化したメッセージをキャロルへ送信することができる。

【００８０】

$A \rightarrow C : E(K_{P1}, P_1)$

【００８１】

アリスからの暗号化メッセージP_1とトレントからの解読鍵を受信すると、キャロルは、受信した解読鍵を受信した暗号化メッセージに適用することにより、メッセージP_1を復元することができる。

【００８２】

$P_{recovered} = D(K_{P1}, E(K_{P1}, P_1))$

【００８３】

キャロルは、メッセージのラベルを作成するためにアリスが最初に使用した関数を知っている場合には、アリスから受信したメッセージを検証することもできる。具体的には、キャロルは、$P_{recovered}$（P復元）のハッシュを、アリスから受信したメッセージP_1のハッシュと比較することができる。２つのハッシュが同一であれば、キャロル

は、アリスから受信した暗号化メッセージが、キャロルとトレントの両方へ送信された最初のメッセージ・ハッシュＨ（$Ｐ_{1}$）に関連していると結論を出すことができる。２つのハッシュが同一でない場合、キャロルは、コンテンツ配布システム内で不正行為が進行中であると確信するだけの理由を得ることになる。

【００８４】

上に挙げた電子メールの例は、より一般的な問題に拡張できる。このプロトコルは、例えば、ネットワークを介してサーバから提供される資源を使用するコンピュータを認証するために使用されることができる。ネットワーク上で接続された多くのユーザは、セキュアな通信のために仮想私設網（「ＶＰＮ」）に依存するアプリケーションを使用している。ＶＰＮのセキュリティは、オープン・システム相互接続（「ＯＳＩ」）モデルで定義される通信モデルのネットワーク層に組み込まれている。アプリケーション層で変化ＩＤを使用することにより、ＶＰＮに代えて仮想私設アプリケーション（“ＶＰＡ”）を作り出すことができる。ＶＰＡを使用すると、電子メール、ファイル・システム、および他のビジネス・レベルのエンドユーザ・アプリケーションは、複雑なネットワーキングを必要とせずに認証することができる。アプリケーション層の通信をセキュアにすることにより、ローカル・エリア・ネットワーク（「ＬＡＮ」）層でより高いセキュリティが得られる。これは、また、エンドユーザに対するワイド・エリア・ネットワーク（「ＷＡＮ」）とＬＡＮのセキュリティを簡素化する。

【００８５】

変化ＩＤの別の使用は、取引の関係者を認証する際のものである。アリスが、クライアント・コンピュータであるキャロルが使用できる資源を備えたサーバであるとする。ボブは、クライアント・コンピュータであるキャロルのユーザであり、キャロルに特定の資源を使用するように指示するものとする。トレントは、引き続きプロトコルの認証者である。アリス、キャロル、およびボブはすべて、先に述べたように秘密の数Ｎと秘密鍵Ｋを有するものとする。更に、トレントはすべての秘密を知っており、アリス、キャロル、ボブは互いの秘密を知らないものとする。

【００８６】

アリスは一度に多くのクライアントに対応する必要があるため、数／鍵の対の大きなリストを必要とする。アリスがすでに１つの数／鍵の対を持っているものと仮定すると、アリスは、認証者トレントと交渉して多くの数／鍵の対を得ることができる。アリスはまず、彼女が適格なサーバであることをトレントに証明する必要がある。そのために、アリスは、アリスに属するものとトレントが認識する何らかの識別子を、ｘ個の数／鍵の対を求める要求とともに暗号化する。

【００８７】

Ａ→Ｔ：$Ｎ_{Ａ}$Ｅ（$Ｋ_{Ａ}$，$Ａ_{ｉｄ}$，ｘ個の数／鍵の対を送信）

【００８８】

トレントは、要求の有効性を確認すると、図３ｂに示すように、数／鍵の対を生成し、それらを$Ｋ_{Ａ}$で暗号化して、対のリストをアリスへ送り返す。

【００８９】

Ｔ→Ａ：Ｅ（$Ｋ_{Ａ}$，$Ｎ^{1}{}_{Ａ}Ｋ^{1}{}_{Ａ}Ｎ^{2}{}_{Ａ}Ｋ^{2}{}_{Ａ}$．．．）

【００９０】

これで、アリスは、数／鍵の対$Ｎ_{Ａ}$／$Ｋ_{Ａ}$を破壊してよく、トレントはそれらを使用済みとマークする。このプロトコルは任意の時に実行して、サーバが、要求に対応するのに十分な数／鍵の対を有することを保証することができる。

【００９１】

ユーザであるボブが、彼を識別する証明（例えばパスワード、ユーザ識別子）を、クライアント・コンピュータであるキャロルのクライアント・ソフトウェアへ供給し、キャロルは、ボブの証明と彼女の識別とを彼女の現在の秘密鍵で暗号化し、彼女の現在の数を先頭に付加する。次いで、それが、要求されたサーバ、アリスへ送信される。

【００９２】

C→A：$N_C E(K_C, B_{cred} C_{id})$
（C→A：$N_C E(K_C$，B証明C識別））
【００９３】
次いで、アリスは、受信したメッセージを、彼女の鍵の１つで暗号化し、その鍵に関連した数を先頭に付加する。それが、次いで、認証者トレントへ送信される。
【００９４】
$A \rightarrow T : N_A E(K_A, N_C E(K_C, B_{cred} C_{id}))$
【００９５】
トレントは、メッセージの暗号化を解いて、ボブが、サーバのアリスにあるサービスの使用を希望していることを判断することができる。この時点で、トレントは、ボブとキャロルの識別（ＩＤ）を検証し、ボブとキャロルの両方がサーバ、アリスを使用する権限を持つことを確認することができる。識別と許可用の証明とが確認され、承認されると、トレントは、次いで２つのメッセージを生成することができる。第１のメッセージは、キャロル、即ちクライアント・コンピュータ宛であり、K_Cで暗号化された、新しい数／鍵の対、サーバであるアリスの識別、およびセッション鍵K_Sを含む。第２のメッセージは、アリス、即ちサーバ宛であり、ユーザであるボブの識別子、クライアント・コンピュータのキャロルの識別、およびK_Pを含む。すべてのコンポーネントは、次いでK_Aで暗号化される。
【００９６】
$T \rightarrow C : E(K_C, A_{id} N'_C K_C K_S)$
（T→C：$E(K_C$，A識別$N'_C K_C K_S)$）
$T \rightarrow A : E(K_A, B_{id} C_{id} K_S)$
（T→A：$E(K_A$，B識別C識別$K_S)$）
【００９７】
この時点で、クライアント・コンピュータのキャロルは、鍵K_Sが、サーバ・アリスとのすべての通信を暗号化するために使用するのに安全であることを知る。更に、アリスは、クライアント・コンピュータのキャロルと、ユーザのボブとのＩＤ（識別）がトレントにより確認済みであることを知る。
【００９８】
明らかなように、本発明の上記の実施形態を使用する非セキュアなシステム内のエンティティ間のセキュアな有効性確認は、最小限のステップ数を必要とする。キャロルがアリスとの通信をセキュアに開始するために、キャロルは、アリスに１つのメッセージを送信し、アリスは次いで有効性確認のための要求をトレントへ送る。要求が確認されると、トレントは、キャロルとアリスの両方に、通信に使用するための変化ＩＤを送信する。また、アリスが、要求側エンティティへ発行するために必要とされる彼女の数／鍵の対を、このプロトコルを通じていつでも入手できるようにすることにより、必要なステップ数が減る。アリスは、エンティティが認証者に数／鍵の対を求めるためのサービスを要求することを待つ必要がなく、また、エンティティも、アリスが必要時に一度に１つずつ数／鍵の対を入手することを待つ必要がない。
【００９９】
それと比較して、２つのエンティティ間に正当性が確認された通信を確立するために使用される現行のシステムは、より多くのステップ数を必要とし、そのステップ数は、多数のサービスとサービスを要求するエンティティとを伴うシステムに適用された場合には、高い率で増加する。現行のシステムの中には、サービスと直接通信することを許可される前にエンティティが複数のエンティティとの間で要求を確認しなければないものもある。ログ・オン等の単純な作業に必要とされるステップの数ですら、システムに関連するエンティティやサービス等のコンポーネントの数に対して二次的に増加し得る。多くの現行システムは、すべての関係当事者間のタイムスタンプとクロック同期にも依拠する。エンティティ間で内部クロックが異なる場合、エンティティは、自身を再度認証し、新しいセッション鍵を得ることを要求される場合があり、それが、サービスの使用の正当性を確認す

るために必要とされる通信を更に増加させる。多数のエンティティが多数のサービスについての確認を要求する際、現行のシステムで発生するオーバーヘッドは、同様の状況で上記の変化ＩＤシステムで必要とされるオーバーヘッドより大きいと考えられる。

【０１００】

このプロトコルの別の実施形態は、先に述べた４つのエンティティすべてに関係する。この実施形態では、アリス即ちＡがコンテンツ提供者２２の役割を行い、エンティティのボブ即ちＢがサービス提供者２４の役割を行い、エンティティのキャロル即ちＣが消費者２６の役割を行い、エンティティのトレント即ちＴが認証者２８の役割を行う。ここで提案されるプロトコルは、信頼される権限者に依拠するため、アリス、ボブ、およびキャロルは、トレントを信頼する。また、アリスは、数（N_A）と何らかの対象暗号のための鍵（K_A）の２つの秘密を有する。ボブも、数（N_B）と何らかの対称暗号のための鍵（K_B）の２つの秘密を有する。同様に、キャロルも秘密の数（N_C）と鍵（K_C）を有する。更に、すべての割り当てられる数と鍵は、トレントにより割り当てられ、知られている。

【０１０１】

この例のみの目的で、アリスが、映画Ｍを所有する映画製作者であるとする。アリスは、ボブのケーブル会社（例えばビデオ・オン・デマンド）を使用して映画Ｍを配布することを希望しており、ボブの消費者の１人であるキャロルは、映画Ｍを受信し、鑑賞したいと思っている。無論、アリスは、各種のコンテンツ・アイテムを配布することを必要とされる任意のエンティティを表すものとすることができる。アリスは、本明細書に記載されるプロトコルを使用して、電子メール・メッセージ、音楽、画像、データ等を配布することができる。

【０１０２】

初めに、アリスが彼女のコンテンツを配布したい場合、アリスは、トレントに多数の数／鍵の対を要求する。要求するために、アリスは、その要求を知らせるメッセージP_2を作成し、その要求を自身のK_Aで暗号化し、N_Aを先頭に付加する。要求をアリス自身の秘密鍵で暗号化することにより、トレントは、許可された者だけに数／鍵の対が付与されることを確かめることができる。次いでアリスはメッセージをトレントへ送信する。

【０１０３】

$A \rightarrow T : N_A\ E(K_A, P_2)$

【０１０４】

アリスからのメッセージを受信すると、トレントは、アリスの秘密を知っているので多数の数／鍵の対のを要求する要求を解読する。図３ｂを参照すると、トレントは、ライセンスのリストを生成し、そのリスト全体を、トレントとアリスとの両方に知られているアリスの鍵K_Aで暗号化してアリスに送り返す。

【０１０５】

$T \rightarrow A : E(K_A, \{N^i_A, K^i_A)\})$

【０１０６】

そして、アリスは、トレントと連携して、彼女の映画Ｍの各コピーを暗号化する鍵を受信する。アリスは、Ｍのラベルを生成し、現在の実施形態ではＭのハッシュが使用され、これが映画Ｍの識別子として使用される。アリスは、何れかの任意の数／鍵の対ｊを取り出し、ＭのハッシュをK^j_Aで暗号化し、N^j_Aを先頭に付加し、そのメッセージをトレントへ送信する。

【０１０７】

$A \rightarrow T : N^j_A\ E(K^j_A, H(M))$

【０１０８】

アリスは、このプロトコルの他のエンティティに知られている映画Ｍの一意の識別子M_{id}を、トレントへ送信されるメッセージに含めてもよい。識別子を加えることにより、暗号化コンテンツを要求する要求の突き合わせおよび許可のための機構が、トレントに提供される。

【０１０９】
$A \rightarrow T : N^{j}{}_{A}\, E(K^{j}{}_{A}, H(M) M_{id})$
【０１１０】
アリスからメッセージを受信すると、トレントは、映画Ｍのハッシュに関連した鍵K_Mを生成し、その鍵を$K^{j}{}_{A}$で暗号化してアリスに送り返す。トレントは、送信した鍵K_Mが映画Ｍのハッシュ（そして、提供される場合には一意の識別子M_{id}）に関連付けられていることを記録する。トレントは、暗号化コンテンツの鍵を生成しているにも関わらず、コンテンツは決して受信しない。トレントが受信するのは、映画Ｍのハッシュと、可能性としては、システムのすべてのエンティティに知られている一意の識別子のみである。トレントは、コンテンツ提供者から提供されるコンテンツに関する他の有用な情報は得ない。トレントは、コンテンツ提供者の介在と許可なしにコンテンツを直接配布することを可能にする情報は持たない。
【０１１１】
$T \rightarrow A : E(K^{j}{}_{A}, K_M)$
【０１１２】
ここでアリスは、彼女とトレントだけがK_Mを知っていることを確信して、ＭをK_Mで暗号化することができる。アリスはK_MでＭを暗号化し、ボブへ送信する。
【０１１３】
$A \rightarrow B : E(K_M, M)$
【０１１４】
アリスはまた、ボブに、暗号化されたコピーに対応する一次ライセンスを送信する。このコンテンツ提供者から送信されるライセンスは、配布される前にサービス提供者により更に認証される場合もあるため、一次ライセンスと呼ぶ。アリスは、映画Ｍのハッシュを鍵$K^{k}{}_{A}$で暗号化し、トレントにより生成されたリストから任意に選択された数／鍵の対ｋの数$N^{k}{}_{A}$を先頭に付加することにより、それぞれの一次ライセンスを作成する。アリスは、それぞれの一次ライセンスをボブへ送信する。
【０１１５】
$A \rightarrow B : N^{k}{}_{A}\, E(K^{k}{}_{A}, H(M))$
【０１１６】
ボブは、暗号化コンテンツとそれに対応する一次ライセンスの両方を受信しているが、まだ解読鍵は知らず、そのため、アリスが知らないＭのコピーを配布することができない。ボブは、暗号化されたコンテンツまたは一次ライセンスの何れかを、アリスまたはトレントからの介入なしに、彼が望むだけの数の消費者へ配布することができる。しかし、消費者は、暗号化されたコンテンツを視聴することも、一次ライセンスを使用することもできない。また、ボブは、暗号化されたコピーからも、一次ライセンスからも、アリスが提供するコンテンツに関する情報を得ない。ボブにライセンスを提供することにより、アリスは、ボブが配信できるコンテンツのコピー数を制限することができる。なぜなら、各ライセンスは消費者に対して発行されると、トレントにより使用済みとマークされるからである。アリスからの有効なライセンスを用いて、サービス提供者および消費者はコンテンツを入手することはできない。アリスには、トレントに知られた数／鍵の対が少なくとも１つ残っているはずである。アリスがより多くの数／鍵の対を必要とする場合は、残っているその１つの数／鍵の対を使用してトレントに更に対を要求することができる。
【０１１７】
ボブは、Ｍの暗号化されたコピーと、それに対応するアリスにより署名された一次ライセンスを受信すると、アリスから送信されたそれぞれの一次ライセンスを更に認証して、ライセンスが消費者へ配布される前に、そのコンテンツに彼の所有権を設定する。ボブにそれぞれの一次ライセンスを更に認証させることは必須ではないが、それによりアリスの映画Ｍについての保護が増大される。なぜなら、アリスは、コンテンツ・アイテムに対する要求が、許可された配布者を通じて適正に開始されたことを保証することができるからである。それぞれの一次ライセンスに更に高い権限を付加するために、ボブはまず、アリ

スが上記で定義した多数の数／鍵の対を入手した際と同様の方式でトレントに多数の数／鍵の対を要求する。ボブは、その要求を示すメッセージP_3を作成し、要求を彼のK_Bで暗号化し、N_Bを先頭に付加する。次いで、ボブは、メッセージをトレントへ送信する。

【０１１８】

$B \rightarrow T : N_B E(K_B, P_3)$

【０１１９】

トレントがボブからのメッセージを受信すると、トレントはボブの秘密を知っているので、N_Bに関連した鍵を調べ、要求を解読する。そして、トレントは、要求された多数の数／鍵の対を生成し、K_Bで暗号化してボブに送り返す。

【０１２０】

$T \rightarrow B : E(K_B, \{N^i_B, K^i_B)\})$

【０１２１】

明らかに、ボブは、アリスから暗号化されたコピーを受信する前に数／鍵の対を要求しても、受信した後に要求してもよい。ボブは、トレントに数／鍵の対を要求するために、アリスから受信するものは何も送信する必要がない。ボブは単に、数／鍵の対を要求および受信することが可能なエンティティとして、トレントに識別可能であればよい。

【０１２２】

ボブは、トレントから数／鍵の対を受信すると、トレントから受信したリストから任意の数／鍵の対ｍを選択し、アリスから受信した暗号化された識別子を鍵K^m_Aで暗号化し、選択された数／鍵の対ｍの数N^m_Aを先頭に付加することにより、配布可能ライセンス、即ち、要求側の消費者へ配布することができるライセンスを、作成することができる。

【０１２３】

$N^m_A E(K^m_A, N^k_A E(K^k_A, H(M)))$

【０１２４】

ボブは、彼が配布したい配布可能ライセンスの数だけ、またはアリスにより配布を許可された配布可能ライセンスの数だけこの手順を繰り返す。

【０１２５】

この時点でボブはコンテンツを有するので、このプロセスの次のステップについて説明する。キャロルは、コンテンツＭの視聴を望んでおり、映画Ｍの一意の識別子を含む、Ｍを求める要求をボブへ送信する。

【０１２６】

$C \rightarrow B : M_{id}$を送信

【０１２７】

キャロルからのコンテンツの要求は、破損から保護するために符号化されてよい。要求を符号化しないと、キャロルの要求は傍受され、変更される可能性があり、キャロルは、購入するつもりのなかったコンテンツを受け取る可能性がある。キャロルは、ボブとキャロルの間で共有される秘密鍵で要求を暗号化することにより、要求を保護することができる。キャロルは、本発明の先に開示した実施形態の１つを使用してボブに要求を送信することもできる。概して、キャロルは、任意のセキュリティ機構を使用して彼女の要求のセキュリティを保護することができる。

【０１２８】

ボブは、キャロルからの要求を受信し、キャロルの要求に含まれる一意の識別子M_{id}で識別される映画Ｍのために以前ボブが生成した配布可能ライセンスの１つを選択することにより、返答する。ボブは、配布可能ライセンスをキャロルへ送信し、そして、そのライセンスが使用され、キャロルへ送信されたことを記録する。

【０１２９】

$B \rightarrow C : N^m_B E(K^m_B, N^k_A E(K^k_A, H(M)))$

【０１３０】

キャロルは、ボブから配布可能ライセンスを受信すると、そのライセンスを彼女の鍵K_Cで暗号化し、彼女の番号N_Cを先頭に付加する。キャロルは、暗号化した配布可能ライ

センスをトレントへ送信する。

【０１３１】

$C \rightarrow T : N_C E(K_C, N^m{}_B E(K^m{}_B, N^k{}_A E(K^k{}_A, H(M))))$

【０１３２】

キャロルから暗号化された配布可能ライセンスを受信すると、トレントは、キャロル、ボブ、およびアリスの秘密を知っているので暗号化をすべて解くことができ、そして、キャロルが有効なライセンスを受信しており、コンテンツＭの解読鍵を必要としていることを、判断することができる。この情報を復元することにより、トレントは、ボブへの受領証を生成することができ、この生成は、ボブの一次ライセンスをキャロルの識別（ＩＤ）と連結して、それを最初に署名された鍵$K^m{}_B$で暗号化し、ボブがライセンスに署名した時に最初に先頭に付加された数$N^m{}_B$を先頭に付加することによりなされる。トレントは受領証をボブへ送信する。

【０１３３】

$T \rightarrow B : N^m{}_B E(K^m{}_B, N^k{}_A E(K^k{}_A, H(M)) C_{id})$

【０１３４】

ボブがトレントから受け取る受領証は、キャロルが消費者として権限を与えられていることをボブに通知するだけでなく、ハッシュＨ（Ｍ）で指定されるコンテンツの対応する暗号化コピーをキャロルへ送信することをボブに指示する。ボブは、キャロルがトレントへ送った配布可能ライセンスは、ボブが初めにキャロルへ送信した配布可能ライセンスと同じライセンスであることを、検証することもできる。キャロルは別の配布可能ライセンスに置き換えることはできず、また、キャロルがボブから受け取った配布可能ライセンスを別の消費者が使用することもできない。ボブは、トレントからの受領証を検査すると、要求される暗号化コピーをキャロルへ送信する。

【０１３５】

$B \rightarrow C : E(K_M, M)$

【０１３６】

キャロルは、受信したＭの暗号化されたコピーを解読するのに必要な解読鍵と、新しい数／鍵の対との両方を必要とし、それにより、彼女は第２のコンテンツ要求を行えるようになる。なぜなら、彼女は、古い変化ＩＤを映画Ｍの要求に消費してしまったからである。トレントは、要求されたコンテンツＭと、Ｍのコピーを暗号化するために使用される鍵とを知っており（作成したのがトレントであるため）、トレントは、その鍵を、将来の要求に使用される新しい数／鍵の対とともにキャロルへ送信する。トレントは、新しい数／鍵の対を、Ｍの暗号化されたコピーに対して必要な鍵と連結し、それらのエレメントをキャロルの現在の鍵K_Cで暗号化する。トレントは、キャロルに割り当てられた数N_Cを先頭に付加する必要はない。なぜなら、キャロルは１つしか数／鍵の対を持っておらず、アリスとボブと同様に、数／鍵の対のリストから、数を与えられた一致する鍵を探す必要がある。従って、トレントは、下記のものをキャロルへ送信する。

【０１３７】

$T \rightarrow C : E(K_C, N'_C K'_C K_M)$

【０１３８】

あるいは、アリスが、暗号化コンテンツに対しての、キャロルに知られている一意の識別子をトレントに提供した場合、トレントは、解読鍵を送信する前に、コンテンツについての最終的な誓約をキャロルに要求することができる。トレントは、新しい数／鍵の対と、トレントがキャロルから受け取った配布可能ライセンスで指定されたコンテンツに対応する一意の識別子M_{id}とを、キャロルへ送信することができる。

【０１３９】

$T \rightarrow C : E(K_C, N'_C K'_C M_{id})$

【０１４０】

この一意の識別子は関係する全エンティティに知られているので、キャロルは、トレントから受信しようとする解読鍵が、彼女が要求したコンテンツの鍵であることを検証するこ

とができる。識別子が、要求したコンテンツに対応しない場合、キャロルは、彼女の最初の要求が欠陥を含んでいたか、または損なわれたことを知り、彼女は、トレントがコンテンツの解読鍵を提供するのを止めさせることができる。解読鍵を送信する前に最終的な許可を要求することにより、キャロルは、希望しなかったコンテンツに対する課金を回避することができる。そうでなく、識別子が、要求したコンテンツと一致する場合、キャロルは、解読鍵の送信をトレントに許可することができる。

【０１４１】

$C \rightarrow T : E(K_C, \text{許可})$

$T \rightarrow C : E(K_C, K_M)$

【０１４２】

これで、キャロルは、映画Ｍを見るのに必要とするものをすべて持つ。

【０１４３】

トレントは、この時点でアリスへの受領証を生成して、アリスが特定のコンテンツまで消費者を追跡できるようにしてもよい。トレントは、Ｍのラベルとキャロルの識別Ｃとを連結し、すべてのエレメントをアリスの鍵$K^{k}{}_{A}$で暗号化し、キャロルへ送信されたライセンスで使用される数$N^{k}{}_{A}$を先頭に付加することができる。

【０１４４】

$T \rightarrow A : N^{k}{}_{A}\, E(K^{k}{}_{A}, H(M)\, C_{id})$

【０１４５】

トレントは、取引中に遭遇されるすべての数／鍵の対（$\{K^{k}{}_{A}, N^{k}{}_{A}\}$，$\{K^{m}{}_{B}, N^{m}{}_{B}\}$，$\{K_C, N_C\}$）を使用済みとマークすることもでき、それにより、将来それらの１つに遭遇した場合には何かがおかしいことが分かる。即ち、トレントは、それぞれの数／鍵の対が１度のみ使用されることを確実にすることができる。従って、対が再使用されることは、エンティティまたは個人がシステムに不正を試みていることの印となる。

【０１４６】

この時点で、アリスは、ボブが映画Ｍのコピーをキャロルへ配布したことを知る。しかし、アリスは、映画Ｍの特定のコピーをボブまたはキャロルまで追跡することはできない。映画Ｍの不法に配布されたコピーが市場に出現した場合、そのコピーを、特定のサービス提供者または消費者までたどることはできない。アリスができるのは、そのコンテンツのライセンスを付与したエンティティのリストを生成することのみである。追跡されないということは、映画Ｍのコピーを合法に購入した消費者が、その入手したコピーを不法に配布することを助長する。

【０１４７】

別の実施形態では、アリスは、作成され配布されるそれぞれのコピーに一意に透かしを入れることにより、サービス提供者および消費者までコンテンツ・アイテムの特定のコピーをたどることができる。特定の消費者まで特定のコピーを追跡する手段をアリスに提供することにより、合法にコンテンツを購入した消費者が入手したコピーを不正に複製することを思いとどまらせることができる。

【０１４８】

透かしを入れる一実施形態では、エンティティ・アリス即ちＡが再びコンテンツ提供者２２の役割を行い、エンティティ・ボブ即ちＢがサービス提供者の役割を行い、エンティティ・キャロル即ちＣが消費者２６の役割を行い、エンティティ・トレント即ちＴが認証者２８の役割を行う。

【０１４９】

４つのエンティティを伴う透かしを入れない実施形態と同様に、アリスは、暗号化されたメッセージP_4でトレントに多数の数／鍵の対を要求する。

【０１５０】

$A \rightarrow T : N_A\, E(K_A, P_4)$

【０１５１】

トレントは、アリスからのメッセージを受信すると、数／鍵の対のリストを生成し、リスト全体をアリスに送り返す。

【０１５２】

$T \rightarrow A : E(K_A, \{N^i_A, K^i_A\})$

【０１５３】

アリスが多数の数／鍵の対を受信すると、アリスは、Ｍのそれぞれのコピーに一意の透かしを適用することにより、彼女のコンテンツを更に保護することを選択することができる。アリスは、透かしのリスト$D_1, D_2, \ldots, D_n$と、彼女の映画Ｍの透かし方式Ｗを生成する。アリスは次いで、Ｍの多数の異なるハッシュ（それぞれの透かしに１つずつ）を生成することができる。次を考察されたい。

【０１５４】

$M_1 = W(D_1, M)$
$M_2 = W(D_2, M)$
$M_3 = W(D_3, M)$ ・・・

【０１５５】

透かしを入れない実施形態と異なり、アリスは、彼女の映画Ｍを暗号化するための１つの鍵を受信する代わりに、次いで、トレントと連携して、彼女の映画Ｍの透かし入りのそれぞれのコピーを暗号化する鍵を受信するようにする。アリスは、Ｍのラベルと、それぞれの透かし$D_1, D_2, \ldots, D_n$のハッシュとを生成し、何らかの任意の数／鍵の対ｊを選択する。アリスは、Ｍのハッシュと個々の透かしD_1のハッシュとの両方をK^j_Aで暗号化し、N^j_Aを先頭に付加し、メッセージをトレントへ送信する。

【０１５６】

$A \rightarrow T : N^j_A E(K^j_A, H(M) H(D_1))$

【０１５７】

前の実施形態で述べたように、アリスは、トレントへのメッセージで映画の既知の識別子M_{id}を提供することができ、それにより、トレントは後にその識別子を使用して消費者に最終的な許可を要求できる。

【０１５８】

$A \rightarrow T : N^j_A E(K^j_A, H(M) H(D_1) M_{id})$

【０１５９】

アリスからのメッセージを受信すると、トレントは、映画Ｍのハッシュに関連した鍵K_{M1}を生成し、その鍵をK^j_Aで暗号化してアリスへ送り返す。トレントは、送信した鍵K_{M1}が映画Ｍのハッシュと透かしD_1のハッシュ（および、既知の識別子M_{id}が提供される場合はそれも）に関連付けられていることを、記録する。トレントは、暗号化された透かし入りコンテンツのための鍵を生成しているにも関わらず、解読された透かし入りコンテンツは受信しない。ここでも、トレントは、アリスから提供されるコンテンツに関する何の有用な情報ももたない。

【０１６０】

$T \rightarrow A : E(K^j_A, K_{M1})$

【０１６１】

アリスは次いで、M_1、即ち、透かし入りのコンテンツを暗号化し、それをボブへ送信することができる。

【０１６２】

$A \rightarrow B : E(K_{M1}, M_1)$

【０１６３】

アリスは、ボブに、暗号化された透かし入りのコピーのための対応する一次ライセンスも送信する。アリスは、透かしを入れない実施形態と同じ形式でこの一次ライセンスを作成するが、透かしのハッシュを映画Ｍのハッシュと連結する。

【０１６４】

$A \rightarrow B : N^k_A E(K^k_A, H(M) H(D_1))$

【０１６５】
ボブは、暗号化された透かし入りのＭのコピーと、それに対応するアリスにより署名された一次ライセンスとを受信すると、透かしを入れない実施形態と同様に、それぞれの一次ライセンスを認証する。上記で述べたように、ボブによるそれぞれの一次ライセンスの認証は必須ではないが、通信システムに一層の保護とセキュリティをもたらす。ボブはまず、トレントへメッセージP_5を送信することにより、トレントから多数の数／鍵の対を入手する。
【０１６６】
$B \rightarrow T : N_B E(K_B, P_5)$
【０１６７】
先と同様に、トレントは、ボブからのメッセージを受信し、要求される多数の数／鍵の対を生成し、それらをK_Bで暗号化してボブに送り返す。
【０１６８】
$T \rightarrow B : E(K_B, \{N^i_B, K^i_B)\})$
【０１６９】
ここでも、ボブは、アリスから暗号化された透かし入りのコピーを受信する前にこの数／鍵の対を要求しても、後に要求してもよい。
【０１７０】
透かしを入れない実施形態と同様に、ボブは、トレントから数／鍵の対を受信すると、配布可能ライセンスを作成することができる。
【０１７１】
$N^m_A E(K^m_A, N^k_A E(K^k_A, H(M) H(D_1)))$
【０１７２】
ボブは、彼が配布したい配布可能ライセンスの数だけ、またはアリスにより配布を許可された配布可能ライセンスの数だけこの手順を繰り返す。
【０１７３】
キャロルがコンテンツＭを視聴したい場合、キャロルは、Ｍの要求（Ｍを求める要求）をボブへ送信する。
【０１７４】
$C \rightarrow B : M_{id}$を送信
【０１７５】
先に述べたように、キャロルの要求にさらなる暗号化を適用して、キャロルのメッセージが損なわれないことを保証することもできる。
【０１７６】
先と同様に、ボブは、キャロルからの要求を受信し、彼が以前に生成した配布可能ライセンスの１つを選択することにより、応答する。ボブは、配布可能ライセンスをキャロルへ送信する。
【０１７７】
$B \rightarrow C : N^m_B E(K^m_B, N^k_A E(K^k_A, H(M) H(D_1)))$
【０１７８】
ボブから配布可能ライセンスを受信すると、キャロルは、透かしを入れない実施形態と全く同様に、そのライセンスを彼女の鍵K_Cで暗号化し、彼女の数N_Cを先頭に付加し、暗号化した配布可能ライセンスをトレントへ送信する。
【０１７９】
$C \rightarrow T : N_C E(K_C, N^m_B E(K^m_B, N^k_A E(K^k_A, H(M) H(D_1))))$
【０１８０】
キャロルから暗号化された配布可能ライセンスを受信すると、トレントは、その暗号化をすべて解くことができる。なぜなら、彼は、キャロル、ボブ、およびアリスの秘密を知っているからであり、彼は、キャロルが有効なライセンスを受け取ったこと、及び透かしD_1で透かしが入れられたコンテンツＭの解読鍵を必要としていることを、判断すること

ができる。透かしを入れない実施形態と同様に、トレントはボブへの受領証を生成する。
【０１８１】
$T \rightarrow B : N^{m}{}_{B} E(K^{m}{}_{B}, N^{k}{}_{A} E(K^{k}{}_{A}, H(M) H(D_{1})) C_{id})$
【０１８２】
ボブがトレントから受信する受領証は、キャロルが消費者として権限（許可）を与えられていることをボブに通知するだけでなく、ハッシュH（M）およびH（D_{1}）で指定されるコンテンツの対応する暗号化コピーをキャロルへ送信することをボブに指示する。
【０１８３】
$B \rightarrow C : E(K_{M1}, M_{1})$
【０１８４】
透かしを入れない実施形態と同様に、トレントは、キャロルがボブから受信する映画の暗号化された透かし入りのコピーの解読鍵を、キャロルが今後の要求に使用できる新しい数／鍵の対とともに、送信する。
【０１８５】
$T \rightarrow C : E(K_{C}, N'_{C} K'_{C} K_{M1})$
【０１８６】
先に述べたように、トレントは、要求されたコンテンツの、全エンティティに知られている識別子を知っている場合には、この時点で最終的な許可を追加的に要求することもできる。トレントは、キャロルへその識別子を提供し、キャロルは、彼女が受け取ろうとしている解読鍵が、彼女が要求したコンテンツのものであることを、検証することができる。トレントは、キャロルの確認を受信すると、必要とされる解読鍵を送信することができる。
【０１８７】
これで、キャロルは、映画Mを見るために必要なものをすべて持つ。
【０１８８】
先と同様に、トレントは、この時点でアリスへの受領証を生成して、アリスが特定の透かし入りコピーまで消費者を追跡できるようにしてもよい。トレントは、Mのラベルと、透かしのハッシュH（D_{1}）と、キャロルの識別Cとを連結し、すべてのエレメントをアリスの鍵$K^{k}{}_{A}$で暗号化し、キャロルへ送信したライセンスで使用された数$N^{k}{}_{A}$を先頭に付加することができる。
【０１８９】
$T \rightarrow A : N^{k}{}_{A} E(K^{k}{}_{A}, H(M) H(D_{1}) C_{id})$
【０１９０】
トレントは、取引中に遭遇されるすべての数／鍵の対（$\{K^{k}{}_{A}, N^{k}{}_{A}\}$，$\{K^{m}{}_{B}, N^{m}{}_{B}\}$，$\{K_{C}, N_{C}\}$）と透かし$D_{1}$とを使用済みとマークすることもでき、それにより、それらがその後に使用されると不正行為と認識できる。
【０１９１】
あるいは、別の透かしの実施形態では、アリスではなくボブがコンテンツのコピーに透かしを適用する。アリスは、ボブに、映画Mの暗号化されたバージョンを１つ送信し、適用する透かしのリストも提供してよい。次いで、ボブは、トレントと連携してコンテンツの解読鍵を受信する。解読鍵を受信すると、ボブは、暗号化されたコンテンツを復号し、解読されたコンテンツに透かしを適用し、透かしを入れたコンテンツを、アリスにより使用された最初の鍵とは異なる別の暗号鍵で暗号化する。ボブが配布可能コンテンツに透かしを入れられるようにすることにより、コンテンツ提供者とサービス提供者の間で必要とされる通信が少なくなり、送信されるデータが少なくなる。サービス提供者は、コンテンツの要求がなされた時にオンザフライで解読と透かしの適用を行ってもよい。必要時にコンテンツに透かしを入れることにより、サービス提供者は、コンテンツの暗号化された透かし入りのバージョンを複数個保持する必要がなくなるので、サービス提供者に必要とされる記憶量が減る。アリスは、暗号化されているが透かしは入れない状態で彼女のコンテンツを提供するので、アリスのコンテンツを解読し、透かしを適用し、消費者へ送信され

る前に透かし入りコンテンツを再度暗号化するために、本プロトコルの別のエンティティが信頼されなければならない。この解読および透かしの適用を行うためにボブが信頼されてもよいが、アリスは、ボブに、アリスのコンテンツのセキュリティを保護する特殊なハードウェアを使用するように、要求してもよい。解読と透かしの適用がハードウェア（サービス提供者からはアクセスできない）でリアル・タイムで行われることを必要とすることにより、アリスのコンテンツのセキュリティが保たれる。コンテンツは、サービス提供者の特殊なハードウェアへ送信され、そのハードウェアが、コンテンツを復号し、透かしを適用し、コンテンツを再び符号化する。このハードウェアは、サービス提供者が解読されたコンテンツにアクセスすることを阻止する。なぜなら、コンテンツは、ハードウェアに暗号化された状態で入り、透かしが入れられ且つ暗号化された状態でハードウェアを出るからである。プロトコルを機能させるために、コンテンツ提供者は、この特殊なハードウェアのセキュリティを信頼しなければならない。アリスから提供されたコンテンツを復号して透かしを入れる、権限のある特殊ハードウェアまたは復号を行うエンティティを、以下の詳細な例ではＢ’または「ブレンダ」と表記する。

【０１９２】

先と同様に、アリスは、彼女の映画Ｍの配布を希望しており、彼女の映画の特定のコピーまで消費者を追跡したい。しかし、ボブは、暗号化され、透かしの入ったアリスのコンテンツのコピーを複数受け取り、記憶することは望まない。アリスとボブとの間の通信とデータ・トラフィックを減らすために、ボブは、アリスから提供されたコンテンツに透かしを入れ、暗号化する。

【０１９３】

先の２つの実施形態と異なり、アリスは、暗号化された透かしのリストを作成するために彼女が使用する多数の数／鍵の対をトレントに要求することから、開始する。アリスは、数／鍵の対をトレントから受信すると、映画Ｍの暗号鍵を要求する。また、アリスは、透かしを適用するために、誰が映画の復号を許されるのかを、トレントへの要求で指定することができる。現在の例では、ブレンダが透かしの適用を許可される。アリスは、解読情報を送信する前に要求の正当性を確認するために、トレントに使用されることができる映画の既知の識別子M_{id}も含めてよい。

【０１９４】

$A \rightarrow T : N_A E(K_A, H(M) M_{id} B')$

【０１９５】

トレントは、映画の暗号鍵K_Mで応答する。

【０１９６】

$T \rightarrow A : E(K_A, K_M)$

【０１９７】

アリスは、暗号鍵K_Mを受信すると、映画Ｍと映画のハッシュＨ（Ｍ）とを暗号化し、暗号化したコンテンツをボブへ送信することができる。

【０１９８】

$A \rightarrow B : E(K_M, H(M) M)$

【０１９９】

アリスは、暗号化コンテンツのコピーに適用される透かしD_1、D_2、．．．，D_nのリストも生成する。それぞれの透かしは、映画のハッシュＨ（Ｍ）と、可能性としては映画の既知の識別子M_{id}と連結される。連結されたそれぞれのリストは、アリスがトレントから受信した数／鍵の対の１つで暗号化される。アリスは、暗号化された透かしのリストをボブへ送信する。あるいは、アリスは、ボブに、アリスのコンテンツに適用する透かしを生成させることもできる。ボブに透かしを作成させることにより、アリスとボブとの間で通信される通信とデータが更に少なくなる。

【０２００】

$A \rightarrow B : N^1{}_A E(K^1{}_A, H(M) D_1 M_{id}), N^2{}_A E(K^2{}_A, H(M) D_2 M_{id}), \ldots, N^3{}_A E(K^3{}_A, H(M) D_3 M_{id})$

【０２０１】
ボブは、この時点で、ブレンダのみにより解読されることが可能な暗号化された透かしのリストと暗号化された映画Ｍとを得ている。ブレンダのみによる解読が可能なのは、それがアリスからトレントへの要求でアリスにより指定されたからである。コンテンツの配布を準備するために、ボブとブレンダは、トレントに多数の数／鍵の対を要求する。
【０２０２】
ボブは、キャロルから映画Ｍの要求を受信すると、暗号化透かしをブレンダに提供する。暗号化透かしは、トレントから提供されたリストから任意に選択された数／鍵の対で暗号化されたものであり、ボブがアリスから受信したものである。
【０２０３】
$B \rightarrow B' : N^{a}{}_{B} E(K^{a}{}_{B}, N^{1}{}_{A} E(K^{1}{}_{A}, H(M) D_{1} M_{id}))$
【０２０４】
ブレンダは、トレントにより生成されたリストから任意の数／鍵の対を選択し、ボブから受信した二重に暗号化された透かしを更に暗号化する。ブレンダは次いで、三重に暗号化された透かしをトレントへ送信する。
【０２０５】
$B' \rightarrow T : N^{a}{}_{B}{}', E(K^{a}{}_{B}{}', N^{a}{}_{B} E(K^{a}{}_{B}, N^{1}{}_{A} E(K^{1}{}_{A}, H(M) D_{1} M_{id})))$
【０２０６】
トレントは、全員の秘密を知っているので、暗号化したものをすべて復号し、映画のハッシュＨ（Ｍ）、透かしD_{1}、映画を復号する鍵K_{M}、映画を符号化するための新しい鍵K_{M}'、およびボブの識別B_{id}を、ブレンダに返す。
【０２０７】
$T \rightarrow B' : E(K^{a}{}_{B}{}', H(M) D_{1} K_{M} K_{M}', B_{id})$
【０２０８】
ブレンダも、ボブから受信した同じ二重に暗号化された透かしを、任意に選択された別の数／鍵の対で暗号化する。ブレンダは、この第２の三重に暗号化された透かしをキャロルへ送信する。
【０２０９】
$B' \rightarrow C : N^{b}{}_{B}{}', E(K^{b}{}_{B}{}', N^{a}{}_{B} E(K^{a}{}_{B}, N^{1}{}_{A} E(K^{1}{}_{A}, H(M) D_{1} M_{id})))$
【０２１０】
キャロルは、受信したメッセージを彼女の１つの数／鍵の対で暗号化し、先と同様に、暗号化したメッセージをトレントへ送る。
【０２１１】
$C \rightarrow T : N_{C} E(K_{C}, N^{b}{}_{B}{}', E(K^{b}{}_{B}{}', N^{a}{}_{B} E(K^{a}{}_{B}, N^{1}{}_{A} E(K^{1}{}_{A}, H(M) D_{1} M_{id}))))$
【０２１２】
トレントは、暗号化をすべて解き、キャロルがそのメッセージで識別される映画を確かに入手するつもりであることを確認する。
【０２１３】
$T \rightarrow C : E(K_{C}, N'_{C} K'_{C} M_{id})$
【０２１４】
キャロルは、コンテンツ識別子M_{id}が、彼女が要求したコンテンツに対応する場合、許可をもって応答する。
【０２１５】
$C \rightarrow T : E(K_{C}, \text{許可})$
【０２１６】
次いで、トレントは、解読鍵K_{M}をキャロルへ送信し、ボブへの受領証を生成する。ボブの受領証は、キャロルの識別と共に、ボブが初めにキャロルへ送信した暗号化された透

かしを含んでいる。

【０２１７】

$T \rightarrow B : N^{a}{}_{B} E(N^{1}{}_{A} E(K^{1}{}_{A}, H(M) D_{1} M_{id}) C_{id})$

【０２１８】

トレントは、アリスが映画Ｍの透かし入りのコピーをキャロルに関連付けることができるように、アリスへの受領証も生成する。アリスの受領証は、映画のハッシュＨ（Ｍ）、適用された透かしD_{1}、および消費者の識別子C_{id}を含む。アリスの受領証は、キャロルにライセンスが付与されたコンテンツに関連付けられることになる透かしを暗号化するためにアリスが使用した数／鍵の対で、暗号化される。

【０２１９】

$T \rightarrow A : N^{1}{}_{A} E(K^{1}{}_{A}, H(M) D_{1} C_{id})$

【０２２０】

トレントから受領証を受信すると、ボブは、アリスから受信した暗号化された映画をブレンダへ送信する。

【０２２１】

$B \rightarrow B' : E(K_{M}, H(M) M)$

【０２２２】

ブレンダは、トレントから解読鍵K_{M}を受信しているので、暗号化された映画を解読する。ブレンダは、映画を復号して映画Ｍを復元し、透かしD_{1}を適用し、透かし入りの映画$W(D_{1}, M)$を新しい暗号鍵K_{M}で暗号化する。映画とともにアリスが暗号化した映画のハッシュＨ（Ｍ）により、ブレンダは、その映画が別の映画と取り替えられておらず、また、トレントから受信した解読鍵が暗号化コンテンツのための一致する鍵であることを、確認することができる。映画Ｍが解読され、透かしが入れられ、暗号化されると、ブレンダは、その暗号化され、透かしが入れられたコンテンツをキャロルへ送信する。

【０２２３】

$B' \rightarrow C : E(K_{M}', W(D_{1}, M))$

【０２２４】

キャロルは、トレントからすでに解読鍵を受け取っているため、暗号化され、透かしが入ったコンテンツを解読して、映画Ｍを視聴することができる。

【０２２５】

キャロルが、受信したコンテンツの不法なコピーを作製して配布することを決めた場合、キャロルが配布した市場で見つかる不法コピーは、何れも、コンテンツに適用された透かしによりキャロルまでたどられることができる（透かしを適用するために使用される本発明のこの特定の実施形態に関係なく）。ボブとアリスはともに、特定の透かしを特定の消費者にリンクする受領証を受け取る。コピーがキャロルまでたどられることができるため、この事を知っていることにより、キャロルは、コンテンツの不法コピーの配布を思いとどまる可能性がある。キャロルはまた、誰かが自分のコンテンツを手に入れ、不法に配布しないように、彼女のコピーをより厳重に監視することもできる。透かしの使用を通じて、コンテンツ提供者とサービス提供者との権利が強化される。

【０２２６】

不法コピーの量を減らすことが可能な別の構成は、映画またはコンテンツのリアル・タイムの復号を必要とするようにすることである。選択されるハードウェア実装によっては、リアル・タイムの復号が可能であり得、その復号では、ここに提案されるシステムを介してダウンロードされたコンテンツを記録するために、そのコンテンツを意図される再生速度で視聴または消費するために必要な時間と同じ時間を必要とする。復号出力は、その後の記録の忠実度を低下させるアナログ信号として実施されることもできる。

【０２２７】

次いで、本発明の実施形態の追加的な態様について、図４～１６に関して説明する。

【０２２８】

図５は、本発明の一実施形態でコンテンツを要求する消費者２６のプロセス全体を示す

。初めに、消費者２６は、特定のコンテンツに対する要求を行う（ステップ５０）。この要求は、消費者が検索エンジンまたは使用可能コンテンツのカタログを使用して見つけた特定のコンテンツに関連した識別子またはラベルを含むことができる。ラベルは、映画の題名や歌曲の題名などのコンテンツの題名であってもよい。サービス提供者２４は次いで、所望されるコンテンツに関連した暗号化ライセンス５２をコンテンツ提供者２２に要求する。サービス提供者は、ライセンス５２を消費者２６へ送信する（ステップ５４）。消費者のハードウェア（例えばセット・トップ・ボックス）は、変化ＩＤ（認証者２８から事前に受信）でライセンス５２を暗号化し、その二重に暗号化されたライセンス５２を認証者２８へ送信する（ステップ５６）。認証者２８は、ライセンス５２が有効であるかどうかを確認する。ライセンスが有効である場合、認証者２８は、サービス提供者にその旨を通知する（ステップ５８）。サービス提供者は次いで、コンテンツを消費者２６へ送信する（ステップ６０）。同時に、またはほぼ同時に、認証者２８は、消費者２６へ復号の情報を送信する（ステップ６２）。

【０２２９】

上記の説明から明らかなように、ライセンス５２は、複数回暗号化されるという意味で複数回の変形を施される。図４にこのプロセスを示す。コンテンツ提供者は、特定のコンテンツの要求を受信するとライセンス５２を作成する。ライセンスは、コンテンツ提供者がその対象のコンテンツのために作成した、ランダムに決定された秘密の識別子の暗号化されたものである。この時点で１回暗号化されたバージョンのライセンス（図４のライセンス６３）は、サービス提供者２４へ送信される。サービス提供者２４は、ライセンスを再度暗号化し（図４のライセンス６４）、この時点で二重に暗号化されたバージョンが消費者２６へ送信される。二重に暗号化されたライセンスは、消費者の変化ＩＤで暗号化されて、３重に暗号化されたバージョンを作成する（図４のライセンス６５）。次いで、ライセンスの認証または検証、および情報の最終的な配信と復号が、図５に関して上記の説明で述べたように行われる。図６に、複数回の暗号化ステップを含むこのプロセスの別の図を提供する。

【０２３０】

図７は、本発明の実施形態が複数のサービス提供者を含んでよいことを示す。更に、サービス提供者は、他のサービス提供者が所望する可能性のある独自のコンテンツまたは特定のコンテンツのライセンスを有してよいことが企図される。そのため、システム２０に参加する各種のサービス提供者の最終的な消費者に対して、多種のコンテンツを使用可能にするために、ライセンスを求める各種の要求とライセンスの転送と（図示）を、サービス提供者の間で行うことができる。

【０２３１】

図８は、本発明の一実施形態で変化ＩＤが実装される方式を示す。図示するように、消費者２６に第１の変化ＩＤ１００が割り当てられる。消費者はその変化ＩＤを使用して自身の識別を裏づける（図５のステップ５６に対応する枠１０２に示す）。しかし、ライセンス１００が使用されると、枠１０４に示すように、認証者は、ライセンス１００に変更を加える、即ち、消費者に新しい鍵の対を送信する。新しい鍵の対は、事実上、新しい変化ＩＤ１０６を作る。

【０２３２】

図９ａおよび図９ｂは、コンテンツ鍵を管理する方式の１つを説明する。要求される場合、システム２０は、コンテンツ提供者２２がコンテンツ鍵のリストを認証者２８に提供するように設定または構成されてよい。システム２０がそのように実装された場合、消費者２６によりなされたコンテンツの要求は、コンテンツ提供者２２に転送される（１または複数の仲介のサービス提供者および／または他のコンテンツ提供者を通じて）（図９ｂのステップ１１０）。そして、コンテンツ提供者は、ライセンスを消費者２６へ送信する（この場合も１または複数の仲介のサービス提供者を通じて）（ステップ１１２）。そして、消費者２６は、正当性の検証または認証のために自身のコンテンツ・ライセンスを認証者へ送信する（ステップ１１４）。正当性が検証された場合は、検証情報がコンテンツ

提供者２２へ送信される（ステップ１１６）。次いで、認証者２８は、コンテンツが復号され、視聴されることができるようにコンテンツ鍵を消費者２６へ送信する（ステップ１１８）。

【０２３３】

図１０ａおよび図１０ｂは、別の鍵管理方式を説明する。認証者２８へ鍵が送信されず、コンテンツ提供者２２で保持されること以外、全体のプロセスは、図９ａおよび図９ｂに関して述べたものと同様である。

【０２３４】

図１１～図１３は、望まれるされる場合には、サービス提供者とコンテンツ提供者がコンテンツを共有できる方式を説明する。コンテンツを共有する方式の１つは、それぞれのコンテンツ提供者が特定のコンテンツの権利を保持して、所望のコンテンツの要求を受信するとライセンスを作成するものである（図１１）。あるいは、コンテンツ提供者は、所定数のライセンスを下流の提供者に配布して、コンテンツ提供者がそれぞれの要求に個別に応答しなくてよいようにして、それにより、下流の提供者が、末端の消費者から受け取る個々の要求に対して、承認（承認は、ライセンスの供給を拒否する行為により、否定される可能性がある）を得る必要なく、あるコンテンツの一定数の「コピー」を配布する能力を持てるようにする（図１２および図１３）。

【０２３５】

図１４は、透かしの入ったコンテンツのライセンスを生成し、使用するプロセスを説明する。上記で述べたように、コンテンツのライセンスは、複数回暗号化されるという意味で複数回の変形を施される。コンテンツ提供者２２は、特定のコンテンツの要求を受信すると、または消費者２６による将来の要求に備えて、ライセンスを作成する。このライセンスは、コンテンツ提供者が対象コンテンツに対して作成したランダムに決定される秘密の識別子１３０と、そのコンテンツのコピーに適用される透かし１３２の関数とを暗号化したバージョンである。この時点で１回暗号化されたバージョンのライセンス（図１４のライセンス１３４）は、サービス提供者２４へ送信される。サービス提供者２４は、再度ライセンスを暗号化し（図１４のライセンス１３６）、この時点で二重に暗号化されたバージョンが消費者２６へ送信される。二重に暗号化されたライセンスは、消費者の変化ＩＤで暗号化されて、三重に暗号化されたバージョン（図１４のライセンス１３８）を作成する。次いで、ライセンスの認証または検証と、情報の最終的な配信と復号とが、図５に関して上記の説明で述べたように行われるが、暗号化されたコンテンツと解読の情報が、ライセンス中で識別される透かし入りコンテンツに固有であることをが異なる。図１５に、複数回の暗号化ステップを含むこのプロセスの別の図示を提供する。

【０２３６】

図１６は、コンテンツを配布するために使用されるデバイスの例示的実施形態を示す。消費者２６は、セット・トップ・デバイス１５０として示される。セット・トップ・デバイス１５０は、コンテンツを表示することが可能なディスプレイ１５１に結合され、リモート・コントロール１５２を通じてセット・トップ・デバイスとのインタフェースを提供する。ユーザ１５３は、リモート・コントロール１５２を使用してセット・トップ・デバイス１５０と対話する。ユーザ１５３は、リモート・コントロール１５２を使用して、使用可能なコンテンツのリストを閲覧し、ディスプレイ１５１で視聴するコンテンツを選択する。リモート・コントロール１５２の使用を通じてアクセスされるインタフェースはまた、ディスプレイ１５１上で選択されたコンテンツの名前を強調表示または点滅させることにより、ユーザ１５３がコンテンツの選択を行った時に表示する。

【０２３７】

ユーザ１５３がコンテンツを選択すると、セット・トップ・デバイス１５０は、選択されたコンテンツの要求を生成する。要求は次いで、コンテンツ提供者２２へ送信される。コンテンツ提供者２２のデバイスは、プロセッサ１５６、メモリ・モジュール１５８、および入出力モジュール１６０を備えるサーバとして示されている。メモリ・モジュール１５８は、コンテンツ提供者２２のコンテンツ・アイテムと少なくとも１つの変化識別子を

保持している。コンテンツ提供者２２が認証者２８に多数の変化識別子を要求した場合には、メモリ・モジュール１５８は、他の変化識別子を保持し得る。メモリ・モジュール１５８は、１または複数の形態のＲＯＭ、１または複数のディスク・ドライブ、ＲＡＭ、他のメモリ、またはそれらの組み合わせ等の不揮発性メモリを含み得る。

【０２３８】

コンテンツ提供者２２は、入出力モジュール１６０を通じて要求を受信し、その要求をプロセッサ１５６へ送る。プロセッサ１５６は、メモリ・モジュール１５８にアクセスして変化識別子を入手する。この変化識別子は、同じくメモリ・モジュール１５８に記憶された当該コンテンツ・アイテム用のライセンスを暗号化するために使用する。プロセッサ１５６は、ライセンスを暗号化し、入出力モジュール１６０を通じてライセンスを消費者２６へ送る。

【０２３９】

消費者２６は、暗号化されたライセンスを受信し、暗号化されたライセンスを処理し（下記で説明する）、暗号化されたライセンスを認証者２８へ送る。認証者は、プロセッサ１６２、メモリ・モジュール１６４、および入出力モジュール１６６を備えるサーバとして示されている。コンテンツ提供者２２のメモリ・モジュール１５８と異なり、認証者２８のメモリ・モジュール１６４は、配布されるコンテンツは保持しない。この場合も、メモリ・モジュール１６２は、１または複数の形態のＲＯＭ、１または複数のディスク・ドライブ、ＲＡＭ、他のメモリ、またはそれらの組み合わせ等の不揮発性メモリを含み得る。

【０２４０】

認証者２８のプロセッサ１６２は、入出力モジュール１６６で受信された暗号化ライセンスを解読して、要求されるコンテンツと当該配布に関わるエンティティを明らかにする。関係エンティティの識別が分かると、プロセッサ１６２は、それらの識別を検証し、コンテンツ提供者２２への受領証を生成する。プロセッサはまた、ライセンスで識別されるコンテンツに関連した解読鍵にアクセスし、メモリ・モジュール１６４の１または複数の新しい変化識別子にアクセスする。プロセッサは次いで、受領証、１または複数の新しい変化識別子、および解読鍵が、入出力モジュール１６６から個々の当事者へ送信されるように指示する。また、認証者のプロセッサ１６２は、現在の取引で使用される変化識別子がすでに使用されており、今後に遭遇された場合は受理されるべきことを、メモリ・モジュール１６４内で示す。

【０２４１】

消費者２６は、解読鍵と新しい変化識別子を受け取り、コンテンツ提供者２２は、要求したコンテンツ・アイテムの受領証と、必要な場合は新しい変化識別子を受け取る。次いで、コンテンツ提供者２２は、暗号化されたコンテンツを消費者２６へ送信し、消費者２６がコンテンツを受信したことを記録することができる。

【０２４２】

消費者２６がコンテンツ提供者から暗号化コンテンツを受信すると、消費者２６はこの時点で映画を視聴するために必要なものをすべて持っている。そして、セット・トップ・デバイス１５０は、接続されたディスプレイ１５１に映画を表示することができる。

【０２４３】

図１７は、セット・トップ・デバイス１５０で使用されることが可能なハードウェアを示す。図の例示的コンフィギュレーションでは、セット・トップ・デバイス１５０は、プロセッサ１７０、メモリ・モジュール１７２、入出力モジュール１７４、およびリモート・コントロール・モジュール１７５を含む。このハードウェアは、この他のモジュールも含んでよい。

【０２４４】

メモリ・モジュール１７２は、消費者２６の変化識別子を保持するために使用され、また、コンテンツ提供者２２および／または認証者２８から送信されたコンテンツ、メッセージ、鍵を保持するためにも使用されてよい。メモリ・モジュール１７２は、１または複

数の形態のＲＯＭ、１または複数のディスク・ドライブ、ＲＡＭ、他のメモリ、またはそれらの組み合わせ等の不揮発性メモリを含み得る。

【０２４５】

プロセッサ１７０は、要求を生成し、受信したメッセージを暗号化し、メモリ・モジュール１７２にアクセスしてデータを記憶し、受信したコンテンツを解読するように構成される。入出力モジュール１７４は、システムの他のエンティティ（即ちコンテンツ提供者２２と認証者２８）および表示デバイス１５１とインタフェースをとるように構成される。リモート・コントロール・モジュール１７５は、コンテンツの要求を開始するためにユーザ１５３により使用されるリモート・コントロール１５２とインタフェースをとるように構成される。

【０２４６】

プロセッサはメモリと対にされ、この配布システムで使用される３つのデバイスすべてについて入出力モジュールが示されているが、当業者には、ハードウェア、ソフトウェア、またはそれらの組み合わせが使用されて、関係するエンティティ間でコンテンツを通信および配布してよいことが明らかであろう。プロセッサは、集積回路、マイクロプロセッサ、またはコンテンツを配布するために必要な動作を行うことができるハードウェアとソフトウェアの組み合わせ等である。

【０２４７】

明らかなように、システム２０とその実装に使用されるプロトコルは、コンテンツのセキュアな配布以外の各種の用途で使用されることができる。電子メールから、テレビ会議およびマルチメディア会議、データおよび遠隔測定データの収集、およびその他のものにわたっての、多種の通信が、セキュリティと信頼性を強化するという利益を、システム２０のすべてまたは一部を使用することから得られる。そうした追加的な用途の幾つかを次いで説明する。

【０２４８】

地理的位置の確定

周知のように、多くの人間の活動は、人間の関係者が他の関係者を信頼することに依存する。更に、関係者は、他の関係者が信頼でき（即ち詐欺者や偽者でなく）、なされる約束や誓約を破らないことについて安心できなければならない。大半の活動が直接会って行われた時代には、信頼性についての不安の多くは軽減された。例えば、電話やインターネットが存在する以前には、詐欺師は、だまそうとする相手に物理的に会い、欺かなければならなかった。現代の通信では、当事者が、実際に通信している相手や、それらの当事者がいる場所を知ることが不可能であることが多い。

【０２４９】

信頼性と信用に関する不安に対処するために使用されることができる各種のバイオメトリック・デバイスおよび他のデバイスが存在し、そうしたデバイスの多くは、ここに記載されるシステム２０の実施形態と共に、または実施形態に追加して使用されることができる。しかし、システム２０は、信頼性の不安を軽減する固有の機能も備える。そうした機能の１つは、コンテンツを注文している消費者の場所を、少なくとも比較的具体的な地点までたどれることである。

【０２５０】

先に述べたように、本発明の実施形態では変化ＩＤが実装され、消費者２６に第１の変化ＩＤ１００が割り当てられる。その後の変化ＩＤは、消費者がコンテンツの入手を希望するたびに割り当てられる。更に、それぞれの消費者２６は、復号用のプロセッサまたは同様のデバイス（例えばセット・トップ・ボックス、家庭用コンピュータ等）を持ち、消費者の住所と名前がそのハードウェアに関連付けられる。それぞれのサービス提供者とコンテンツ提供者も実際の物理的な場所と住所を持つ。システム２０の実施形態は、多重暗号化かつカプセル化された識別子を解明することに依拠するので、消費者の場所は、少なくとも、その消費者のサービス提供者のサービス・エリアまではたどることができる。

【０２５１】

例えば、顧客または窃盗者が顧客のハードウェアをサービス提供者２４のサービス・エリア外の場所に移動し、コンテンツを要求した場合、新しいサービス提供者は、そのハードウェアに記憶された変化ＩＤに基づいて復号に必要とされる適切な鍵を送信することができないので、多重暗号化され、カプセル化された識別子の解明は失敗する。

【０２５２】

リアル・タイムのユーザ認証とリアル・タイムのコンテンツ再生

先に述べたように、現在の通信システムに伴う困難の１つは、通信当事者の信頼性を保証することである。本発明の一実施形態では、システム２０が使用されて、１つの当事者から別の当事者へ送信される電子メール・メッセージ等の情報を符号化することができる。送信側の当事者がコンテンツ提供者／サービス提供者のような役割を果たし、受信側の当事者が顧客のような役割を果たす。

【０２５３】

信頼性の追加的な保証を提供する方法の１つは、何らかのランダムの情報を受信側当事者へ送信し、受信者がその情報を、価値のある情報の通信が始まる前に、処理し、送信者へ送り返すことを要求するものである。例えば、合衆国憲法やゲティスバーグの演説からランダムに選択されたテキスト箇所、更に言えば議会図書館にある何千もの文書の任意のテキストを、受信側当事者へ送信することができる。有価値のコンテンツまたは情報が受信側当事者へ送信される前に、ランダムに選択されたテキストが正しく解読されなければならず、その情報の複製が受信者へ送り返されねばならない。受信側当事者がこれを行うことができない場合は、不適正な通信接続がなされているか、または、受信側当事者が、例えば、真の受信者の通信リンクを傍受しているかまたは通信リンクに侵入している詐欺者であることになる。しかし、適正な変化ＩＤを所有しないと、ランダムのテキストの解読は行うことができない。

【０２５４】

システム２０に追加されることが可能な追加的なセキュリティ機能は、コンテンツのリアル・タイムの再生である。先に述べたように、著作権および他の法的権利の保持者にとっての問題の１つは、デジタル・コンテンツは（少なくとも理論的には）無限の回数にわたってコピーされることができ、それぞれのコピーを作製するのに必要な時間が非常に短いことである。例えば、７０分間の音楽を保持しているＣＤは、数分間で完全にコピーされることができる。圧縮ファイルは、更に高速にコピーされることが可能である。このために、潜在的な犯罪者にとっては、コンテンツを大規模に不法コピーすることが非常に魅力的となっている。価値のあるコンテンツのコピーが１つ入手されると、何百、可能性としては何千もの劣化のないコピーが迅速に作製され、販売される可能性がある。

【０２５５】

システム２０の実施形態では、消費者２６または受信者のコンテンツの復号は、リアル・タイム方式で行われる。つまり、システム２０における再生は、最終的な視聴者または消費者に対して意図されるコンテンツの再生速度を超えない速度で行われる。従って、ある映画の上映時間が２時間２０分である場合には、消費者へ送信されるこのコンテンツを記録するには、それと同じ時間量がかかり、それによりコンテンツの大規模なコピーを阻止する。また、このシステムは、行われる解読の回数を制限するように構成されることにも留意されたい。一般には、１回のみの解読が顧客により行われることができる。これは不正コピーを減らす助けとなる。また、コンテンツは、暗号化される前に、周知のコピー保護機構またはコードを含んでよいことにも留意されたい。その機構が使用されて、同様に不法コピーを防止または低減することができる。

【０２５６】

データおよびテレメトリ（遠隔測定データ）の収集

先に述べたように、本発明の実施形態は、３つの当事者のみが関与する場合に実装されることが可能である。それらの当事者は、認証者、送信側当事者（類推によると、コンテンツ提供者およびサービス提供者の役割と機能とを包含する）、および、受信側当事者（類推によると、消費者の役割と機能とを包含する）を含む。先に述べたように、システム

２０は、セキュアな電子メール・システムを実装するように構成されることができる。明らかであるように、システム２０は、電気メータおよびガス・メータからのデータの収集や、機器および人間の監視システム、他のデータおよびテレメトリ収集の用途等、セキュアな通信が有用であり得る各種の他の用途で実装されることもできる。一般に、多くの既存のシステムは、ここに記載される多重暗号化およびカプセル化された識別子のアーキテクチャを使用した通信を可能にするように、既存の処理および通信のハードウェアで容易に変更されることができる。

【０２５７】

電子商取引

変化識別子は、電子商取引のプロトコルでも使用されることができる。一部の実施形態では、４つの関係者（コンテンツ提供者、サービス提供者、消費者、および認証者）の役割の名前を、ベンダ、購入者、支払い認証者、および認証者を含むように変更できる。変化識別子は、ベンダ、購入者、および支払い認証者が取引を完了できるようにするために、認証者により発行および管理されることができる。

【０２５８】

図１８は、電子商取引を行うように構成された例示的システム２００を示す。実際には、当業者には明らかなように、インターネット、電話システム、ワイヤレス・ネットワーク、衛星ネットワーク、ケーブルＴＶネットワーク、および各種の他の私設および公衆ネットワーク等の１または複数のネットワークまたは通信システムが、各種の組み合わせで使用されて、本発明の実施形態または実装を作り出すために要求または必要とされる通信リンクを提供することができる。従って、本発明は、何れの特定のネットワークまたはネットワークの組み合わせにも限定されない。しかし、使用されるネットワークまたは通信システムは、Ｒｉｊｎｄａｅｌ暗号化の１バージョンでデータが暗号化される通信や、セキュア・ソケット・レイヤ（「ＳＳＬ」）通信、またはその他等のセキュアな通信を支援する能力を有することが好ましい。更に、データは、有線、デジタル衛星サービス（「ＤＳＳ」）、または１つの当事者から別の当事者へ物理的に搬送される物理的媒体で１つの当事者から別の当事者へ送られることができる。

【０２５９】

図１８に示す実施形態では、システム２００は、ベンダ２２０、クレジット・カード会社や金融機関等の支払い認証者２４０、購入者２６０、および認証者２８０、の４つの関係者を含む。図には１つのみのベンダ２２０、支払い認証者２４０、および購入者２６０が示されるが、大半の実装では、多数のベンダ、支払い認証者、および購入者が関係する。更に、必須なのは１つのみであるが、複数の認証者２８０があってよい。実際には、次の関係、すなわち、［認証者の数＜支払い認証者の数＜ベンダの数＜購入者の数］、が存在する可能性が高いが、ここでも、関係者の数の制限や、各種関係者の数の間の特定の関係の要件はない。

【０２６０】

一部の実施形態では、ベンダ２２０、支払い認証者２４０、および購入者２６０は、双方向リンク３００、３２０、３４０で認証者２８０に接続される。ベンダ２２０と購入者２６０は、双方向リンク３６０を介しても接続される。これらのリンクは、上述のネットワークのすべてまたは一部から構築されることができる。一部の実施形態では、リンク３６０は、非セキュアなハイパーテキスト転送プロトコル（「ＨＴＴＰ」）リンクを含む。

【０２６１】

ベンダ２２０は、自身の商品および／またはサービスを電子的に販売することを望む小売会社等のエンティティである。ベンダ２２０は、システム２０を使用して交換される商品および／またはサービス（以下では両方を「商品」と称する）について公正に支払いを受けることを望むとものとする。そのため、本発明の一実施形態では、システム２００は、ベンダ２２０が販売された商品の売渡証を生成できるように構成される。売渡証は、取引識別子を含むことができる。一部の実施形態では、取引識別子は、ベンダ識別子を含む。

【０２６２】
購入者とベンダは、売渡証と価格について合意する。購入者２６０は、売渡証に掲載された商品の合意された価格での取引の掛け売り（ｆｉｎａｎｃｉｎｇ）を許可することができる。購入者、ベンダ、および支払い認証者は、上記のように、偽造不可能な取引の受領証を受け取ることができる。少なくとも一部の購入者は、支払いをせずに、あるいはその購入者が管理する権限のない口座からの資金で、電子的に商品を購入することを望んだり試みたりすると想定される。また、購入者は、支払い情報が損なわれることのないセキュアな取引を要求するものと想定される。従って、商品の不正な購入を防止し、セキュアな取引を提供するための措置が提供される。変化ＩＤは、購入を制御するための機構を提供する。

【０２６３】
支払い認証者２４０は、取引にに対する金融処理で使用できる口座（金銭または他の支払いの形態または機構の形）を保持するクレジット・カード会社や金融機関などのエンティティである。支払い認証者２４０は、口座から電子商取引の金融処理を行うことに同意することができ、従って、口座識別子は機密に保たれる。そのため、本発明の一部の実施形態では、システム２００は、購入者２６０と支払い認証者２４０が、購入者２６０の口座についての秘密の口座識別子に合意するように、構成される。更に、口座からの取引の支払いの許可は、変化ＩＤで暗号化される。

【０２６４】
認証者２８０は、セキュアな電子取引を行うために必要なデータを保持するリポジトリである。ここで論じる実施形態では、認証者２８０は、電子商取引が行われるのを許可する前に、ベンダ２２０、支払い認証者２４０、および購入者２６０を、それらの変化ＩＤで検証する。認証者２８０は、購入者、ベンダ、および支払い認証者の受領証を検証することができる。認証者２８０はまた、購入者の口座情報や取引の詳細を知ることなく、上記の動作を行うことができる。認証者２８０は、変化ＩＤの供給元でもあり、データベースまたは同様の機構を使用してそのようなＩＤを追跡する。

【０２６５】
次いで、数個の例を使用して本発明の例示的実施形態を説明する。

【０２６６】
通信プロトコルの説明の多くのように、このプロトコルで使用される各種エンティティ（またはそれらのエンティティに関連したコンピュータ・システム）には名前が割り当てられる。一実施形態では、ボブ（Ｂ）、ヴェラ（Ｖ）、およびキャロル（Ｃ）が、プロトコルの様々な関係者を表し、トレント（Ｔ）は、信頼される通信の調整者を表す。下記の表、表２は、このプロトコルの複数の実施形態を説明するために本文献で使用される他の記号の一覧である。

【０２６７】

【表２】

記号	意味
B, V, C, T	プロトコルを用いるエンティティ
S	売渡証
P	商品の合意した価格
Rx	Xの受領書
Mx	第３者を介して送られた、トレントにより作成されたXに対するメッセージ
xx, yx	Xのアカウント番号
Xid	Xの何らかの（秘密ではない）デジタル識別子（例えば、eメール・アドレス、名前など）
Xcred	パーティーXおよびT（および、適用可能な場合にはC）のみが知り、Tによりランダムに選択可能な、Xを識別する秘密の情報。このデータの知識を提供することにより、X、Cおよび／またはTは、互いに認証できる。
Kx	何らかのエンティティXと関連する対称鍵暗号の鍵
Nx	何らかの鍵Kxと関連する一回使用番号（当座）
H（X）	Xのセキュアなハッシュを作る関数
E（K, X）	XをKで暗号化する暗号
X→Y：X	XからYへ送られるメッセージZ

【０２６８】

このプロトコルの例示的な実施形態は、上記の４つの関係者に関連する。エンティティ・ボブ（「Ｂ」）が購入者２６０の役割を行い、エンティティ・ヴェラ（「Ｖ」）がベンダ２２０の役割を行い、エンティティ・キャロル（「Ｃ」）が支払い認証者２４０の役割を行い、エンティティ・トレント（「Ｔ」）が認証者２８０の役割を行う。このプロトコルは、ボブがヴェラから商品を購入することに関連する。ボブは、キャロルにより保持されている口座を使用して商品の購入、またはその支払いをする。トレントは、ボブ、ヴェラ、キャロルの間の通信を調整する。このプロトコルは、信頼される権限者に依拠するので、ボブ、ヴェラ、およびキャロルは、トレントを信頼する。更に、割り当てられる数と鍵は、すべてトレントにより割り当てられ知られる。ボブ、ヴェラ、キャロルはそれぞれ、トレントにより発行された秘密の数／鍵の対（N_B, K_B）、（N_V, K_V）、および（N_C, K_C）をすでに保持しているものとする。

【０２６９】

この例では、ボブがヴェラから商品を購入したいとする。ボブとヴェラは、売渡証（Ｓ）に合意する。ボブは、キャロルに保持されている口座から引き出される資金で支払いをすることを希望する。口座は、証明（B_{cred}）で識別される。証明（B_{cred}）は、ボブ、キャロル、およびトレントのみに知られている、または認識可能な秘密である。一部の実施形態では、証明（B_{cred}）は、ボブの口座番号を表す。他の実施形態では、証明（B_{cred}）は、トレントにより割り当てられる。プロトコルを機能させるために、トレントは、先天的又は事前に証明を「知る」必要はない。一部の実施形態では、トレントは、キャロルに証明を転送するのみである。更に、一部の実施形態では、トレントは、証明に含まれるデータ（口座番号等）を入手することができない。これは、プロトコルのセキュリティを高める助けとなる。

【０２７０】

証明（B_{cred}）は、ボブ、トレント、キャロルのみに知られているので、トレント

とキャロルは、証明（B_{cred}）を使用して、ボブが特定のメッセージを作成したことを検証することができる。キャロルは、証明（B_{cred}）を使用してボブの口座番号を検証してもよい。一部の実施形態では、証明（B_{cred}）は、ボブとキャロルのみに知られた秘密（ボブの口座番号等）から構築される。証明（B_{cred}）は、現在の取引に関する詳細から構築されることもできる。一部の実施形態では、証明（B_{cred}）は、次のように決定される。

【０２７１】

$B_{cred}=E(H(x),H(S)P)$

【０２７２】

上記の数式で、ｘは、ボブとキャロルのみに知られた秘密（ボブの口座番号等）であり、Ｓは売渡証であり、Ｐは、売渡証に含まれる商品の合意された価格である。一部の実施形態では、ボブは、ハッシュではなく、平文バージョンの売渡証および／または価格から、彼の証明（B_{cred}）を構築する。しかし、ハッシュを使用すると、取引の詳細を抽象化することができる。証明を決定するために、更なる数式や機構が使用されてよいことを理解されたい。

【０２７３】

ボブとキャロルはｘ（および適用可能な場合は、ハッシュ関数）を知っているので、ボブとキャロルは、証明（B_{cred}）を解読し、ボブの口座に関するセキュアな情報を得ることができる。一部の実施形態では、トレントとヴェラは、ボブの口座や、価格等の取引の詳細に関するセキュアな情報を、得ることができない。

【０２７４】

ボブは、取引ごとに証明（B_{cred}）を生成することができ、キャロル（ボブの口座番号を知っており、Ｈ（ｘ）を生成することができる）は、証明（B_{cred}）を解読して、売渡証とそれに対応する価格を得ることができる。一部の実施形態では、キャロルが、それぞれ口座番号x_1、x_2、・・・，x_nを有するボブの口座を複数個保持している場合、キャロルは、それぞれの口座番号に対するハッシュを生成する。それらハッシュの１つが証明（B_{cred}）を解読できる場合、キャロルは、何れの口座から資金を引き出すべきかが分かる。ボブは、証明（B_{cred}）に口座識別子を先頭に付加して、特定の口座を識別するようにもできる。

【０２７５】

一部の実施形態では、口座のハッシュを作成することは、$H(x_i)=H(x_j)$で、かつ、x_iがx_jに等しくない場合に、ハッシュの衝突を発生させる可能性がある。ハッシュの衝突は、口座を作る際に検出されることができ、ハッシュの衝突を防止するために、衝突する口座番号は生成し直すことができる。

【０２７６】

図１９に示すように、購入プロセスを開始するために、ヴェラは、署名されたベンダ取引データをボブへ送信する。一部の実施形態では、ベンダ取引データは、売渡証（Ｓ）および／またはその売渡証（Ｓ）に対応する合計価格（Ｐ）を含む。平文の売渡証（Ｓ）と対応する価格（Ｐ）に加えて、またはその代わりに、ベンダ取引データは、売渡証（Ｓ）および／または価格（Ｐ）のハッシュを含むことができる。一部の実施形態では、ベンダ取引データは、ヴェラの証明（V_{cred}）も含む。ヴェラの証明（V_{cred}）は、ヴェラ、キャロル、およびトレントのみに知られた、または認識可能な秘密である。一部の実施形態では、上記のように、ヴェラの証明（V_{cred}）は、ヴェラの口座番号等の、ヴェラとキャロルのみに知られた秘密から構築されることができる。他の実施形態では、トレントが、ヴェラに証明（V_{cred}）を割り当てることができる。キャロルとトレントは、ヴェラの証明（V_{cred}）を使用して、ベンダ取引データがヴェラにより生成されたことを検証することができる。ベンダ取引データは、取引に関連する購入者（例えばボブ）および／または支払い認証者（例えばキャロル）の識別子も含むことができる。ヴェラは、ベンダ取引データに「署名」するが、これは、そのデータを彼女の秘密鍵（K_V）で暗号化し、自身の秘密の数（N_V）を先頭に付加することによりなされる。ヴェラは

、署名したベンダ取引データをボブへ送信する。

【０２７７】

$V \rightarrow T : SN_V E(K_V, H(S) P)$

【０２７８】

署名されたデータをヴェラから受信すると、ボブは、ヴェラが行ったのと同じように、署名された購入者取引データを提供する。購入者取引データは、売渡証を含み、この売渡証は、ボブが適正かつ誠実に振舞った場合には、ヴェラにより署名された売渡証と同一または等価となる。ボブは、彼の証明（B_{cred}）と、彼以外の取引の関係者（即ちヴェラとキャロル）の識別も、購入者取引データに含めることができる。ボブは購入者取引データに署名するが、これは、そのデータを彼の秘密鍵（K_B）で暗号化し、彼の秘密の数（N_B）を先頭に付加することによりなされる。ボブは、署名した購入者取引データを、ヴェラにより署名されたベンダ取引データと連結し、連結したメッセージをトレントへ送信する。

【０２７９】

$B \rightarrow T : N_B E(K_B, H(S) P) B_{cred} V_{id} C_{id} N_V E(K_V, H(S) P)$

【０２８０】

ボブが購入プロセスを開始することもできることを、理解されたい。一部の実施形態では、ボブは、ヴェラへ、ヴェラとキャロルの識別を含む署名された購入者取引データを送信する。ヴェラは、ボブから提供された署名データに、署名されたベンダ取引データを追加し、連結したメッセージをトレントへ送る。

【０２８１】

トレントは、連結されたメッセージを展開することができる（トレントはボブとヴェラの秘密鍵を知っているから）。一部の実施形態では、トレントは、ボブから送信された購入者取引データまたはその一部（例えば、売渡証、価格、および／または、売渡証および／または価格のハッシュ）が、ヴェラから送信されたベンダ取引データまたはその一部と一致することを検証する。データが一致しない場合は、ヴェラとボブが共通の売渡証および／または関連する価格において合意しなかった可能性があり、トレントは、その不一致をボブとヴェラに通知することができる。

【０２８２】

データが一致する場合、トレントは、支払い要求を生成する。一部の実施形態では、支払い要求は、ボブとヴェラの間の取引の支払いを要求するためにキャロルへ送信される。支払い要求は、ヴェラ、ボブ、キャロルへの受領証を含むことができる。それぞれの受領証は、３つの関係者のうち２つの鍵（即ち、その受領証が対象としない関係者の鍵）、売渡証、および価格を含むことができる。一部の実施形態では、それぞれの受領証は、受信者および／または他の関係者の証明も含む。受信者は、証明を使用して、受領証がトレントにより生成されたことを検証することができる。取引のセキュリティと秘密性を更に増すために、平文データに代えて、鍵、売渡証、価格、および／または証明のハッシュが含まれることも可能であることを、理解されたい。ハッシュが提供された場合、トレントは、ハッシュは入手することができるが、取引の詳細は解読することができない。ヴェラ、ボブ、キャロルへの例示的な受領証は、次のように構成されることができる。

【０２８３】

$R_V = E(K_V, H(K_B K_C P) H(S) P)$
$R_B = E(K_B, H(K_V K_C P) H(S) P)$
$R_C = E(K_C, H(K_B K_V P) H(S) P)$

【０２８４】

支払い要求は、ヴェラ、ボブ、キャロルへの新しい数／鍵の対を含むこともできる。

【０２８５】

$M_V = E(K_V, N'_V K'_V)$
$M_B = E(K_B, N'_B K'_B)$

$M_C = E(K_C, N'_C K'_C)$

【０２８６】

支払い要求は更に、ボブとヴェラへ送信するキャロルのためのメッセージを含むことができる。一部の実施形態では、トレントは、１つの「受理」メッセージと１つの「拒絶」メッセージを生成する。キャロルは、取引の支払いの要求を彼女が受け入れる場合には、「承認（ａｐｐｒｏｖｅｄ）」メッセージまたはその一部を、ボブとヴェラへ送信し、支払い要求を受け入れない場合は、「拒絶（ｄｅｃｌｉｎｅｄ）」メッセージまたはその一部を、ボブとヴェラへ送信する。

【０２８７】

$M_{approved} = E(K_V, \text{“承認”}) E(K_B, \text{“承認”})$

$M_{declined} = E(K_V, \text{“拒絶”}) E(K_V, \text{“拒絶”})$

【０２８８】

トレントが生成する支払い要求は、これより多くの又は少ないメッセージを含んでよいことを理解されたい。例えば、トレントは、それぞれの関係者につき受領証と新しい数／鍵の対の両方を含むメッセージを生成することができる。トレントは、ボブとヴェラからの別々の「承認」メッセージおよび「拒絶」メッセージを生成することもできる。

【０２８９】

トレントは、ボブの証明（B_{cred}）と売渡証の価格（Ｐ）も復号する。一部の実施形態では、トレントは、ボブの証明（B_{cred}）を復号することができず、従って、キャロルに保持されているボブの口座に関する機密情報を得ることができない。この理由から、トレントは、ボブの証明（B_{cred}）は入手するが、ボブの口座情報を入手することはできない。

【０２９０】

支払い要求は、ボブの証明（B_{cred}）と価格（Ｐ）とを含む証明メッセージも含むことができる。トレントは、キャロル以外の者にその証明メッセージに含まれるデータを入手させないために、キャロルの秘密鍵（K_C）で証明メッセージを再度暗号化する。トレントは、キャロルの秘密の数（N_C）を証明メッセージの先頭に付加することもできる。

【０２９１】

$M_{cred} = E(K_C, B_{cred} P)$

【０２９２】

支払い要求は、取引関係者（キャロル以外）の識別も含むことができる。

【０２９３】

トレントは、支払い要求をキャロルへ送信する。一部の実施形態では、トレントは、キャロルに、支払い要求に含まれるメッセージと受領証とを個別に送信することもできる。一部の実施形態では、トレントは、キャロルの秘密鍵（K_C）で支払い要求（または個々のメッセージおよび／または受領証）を暗号化する。トレントは、支払い要求を復号する方法をキャロルに指示するために、キャロルの秘密の数（N_C）を先頭に付加することもできる。

【０２９４】

$T \rightarrow C : N_C E(K_C, B_{id} V_{id}) (R_C R_B R_V) (M_C M_B M_V) (M_{accept} M_{decline}) (M_{cred}))$

【０２９５】

キャロルは、支払い要求を受信し、その売渡証の支払いを承認するかどうかを決定する。一部の実施形態では、キャロルは、ボブの口座（B_{cred}で識別される）にその売渡証の価格（Ｐ）をまかなうのに十分な資金があるかどうかを判断することにより、支払いを承認するか否かを決める。ボブの口座に、価格をまかなうのに十分な資金がある場合、キャロルは、ボブの口座からヴェラの口座へ資金を送る。一部の実施形態では、キャロルは、エスクロー（ｅｓｃｒｏｗ）の役目を果たすことができ、売渡証に含まれる商品がボブに発送および／または提供されたことをヴェラがキャロルに通知するまで、ボブの口座

からの資金を保持することができる。商品がボブに提供されると、キャロルは、ボブの口座からの資金をヴェラの口座に転送することができる。支払いを承認すると、キャロルは、受領証、新しい数／鍵の対、および承認メッセージを含む応答を、ボブとヴェラの両方へ送信することができる。

【０２９６】

$C \rightarrow B$：（K_B，“承認”）$M_B R_B$

$C \rightarrow V$：（K_V，“承認”）$M_V R_V$

【０２９７】

ボブ、ヴェラ、およびキャロルは、取引の検証のために、この取引で使用した数（N_B、N_V、またはN_C）、価格、および、各自の受領証を、トレントに呈示することができる。例えば、トレントは、それらの受領証が同じであることを検証することができる。

【０２９８】

ボブの口座に、価格をまかなうのに十分な資金がない場合、キャロルは、ボブの口座からヴェラの口座に資金を転送しない。しかし、キャロルは、新しい数／鍵の対と拒絶メッセージとを含む応答を、ボブとヴェラの両方へ送信する。キャロルは、ボブとヴェラに、取引の拒絶を知らせる受領証を送信することもできる。

【０２９９】

$C \rightarrow B$：E（K_B，“拒絶”）$M_B R_B$

$C \rightarrow V$：E（K_V，“拒絶”）$M_V R_V$

【０３００】

図１９は、別の例示的な通信プロトコルを模式的に示す。この例示的プロトコルは、ボブが、キャロルにより保持されている口座を使用して、ヴェラから売渡証（Ｓ）にリストされた商品を購入することに関連する。この場合も、トレントが、ボブ、ヴェラ、およびキャロルの間の通信を調整する。また、この提案されるプロトコルは、信頼される権限者に依拠するので、ボブ、ヴェラ、キャロルは、トレントを信頼する。更に、割り当てられる数および鍵はすべて、トレントにより割り当てられ、トレントに知られる。

【０３０１】

この例では、ボブがヴェラから商品を購入したいものとする。先の例と異なり、ヴェラとボブが商品を交換するために、トレントは初めに、ボブとヴェラとの間にセキュアな通信を確立する。

【０３０２】

ボブは、トレントに、取引鍵の要求を送信する。要求は、ボブが通信したいベンダの識別を含むことができる。一部の実施形態では、ボブは、彼の秘密鍵（K_B）で彼の要求を暗号化し、彼の秘密の数（N_B）を先頭に付加する。

【０３０３】

セキュリティを更に保証するために、ボブは、更なる要求識別データＸを、要求に含めることができる。一部の実施形態では、データＸは、ランダムまたは擬似ランダムなデータを含む。例えば、データＸは、ボブとトレントのみに知られたボブの秘密の証明を含むことができる。データＸを使用してトレントを認証することができる。要求はボブの秘密鍵で暗号化されるので、ボブとトレントだけがメッセージを復号することができる。トレントは、自身が認証者であることを証明することができ、それは、ボブの要求を復号し、ボブへの応答にデータＸを含めることにより、なされる。従って、トレントは、彼がボブの要求を復号したことを証明する。

【０３０４】

データＸは、トレントからの応答を、特定の要求と関連付けるために使用されることもできる。トレントは、ボブが彼の要求で識別するベンダに、データＸを渡すこともできる。

【０３０５】

$B \rightarrow T$：$N_B E$（K_B，$V_{id} X$）

【０３０６】

一部の実施形態では、ボブは、トレントが通信を望むベンダ（例えばヴェラ）に、取引鍵を求める要求（取引鍵の要求）を送信することができ、ベンダはベンダ自身の、取引鍵の要求を、連結することができる。ベンダにより生成された要求は、最初の取引鍵の要求をベンダへ送信した購入者の識別を含むことができる。ベンダにより生成された要求は、要求識別データＹを含むこともでき、データＹは、ランダムまたは擬似ランダムのデータを含むことができる。例えば、データＹは、ベンダとトレントのみに知られたベンダの秘密の証明を含むことができる。ベンダは、自身の秘密鍵（K_V）で取引鍵の要求を暗号化し、自身の秘密の数（N_V）を先頭に付加することができる。そして、ベンダは、連結後の取引鍵の要求を、トレントへ送信することができる。トレントは、連結された要求を使用して、それぞれの当事者が取引鍵の確立に同意することを確認することができる。

【０３０７】

トレントは、ボブからの取引鍵の要求を解読し、そして、ボブとヴェラが通信して取引の交渉を行うために使用することができる秘密の取引鍵K_{BV}を、生成する。トレントは、ボブとヴェラの新しい数／鍵の対も生成することができる。トレントは、鍵と、新しい数／鍵の対とを、ボブの鍵とヴェラの鍵とで、それぞれ、暗号化して、２つのメッセージを作成する。このメッセージは、受信者からの取引鍵の要求においてメッセージの受信者により提供された秘密データ（例えば、証明）を含むことができる。上記のように、受信者は、この秘密データを使用して、トレントがそのメッセージを生成したことを検証することができる。トレントは、１つのメッセージをボブへ送信し、１つのメッセージをヴェラへ送信する。トレントは、それらメッセージを連結したものをヴェラまたはボブへ送信することもできる。一部の実施形態では、連結されたメッセージの第１の部分（$N_V E(K_V, B_{id} K_{BV} X N'_V K'_V)$）は、ヴェラの情報を含むことができ、連結されたメッセージの第２の部分（$E(K_B, K_{BV} N'_B K'_B)$）は、ボブの情報を含む。連結されたメッセージを受信した者（ヴェラまたはボブ）は、何れのものであっても、連結されたメッセージから自身の暗号化メッセージを取り出し、残りの連結メッセージをもう一方の参加者に渡すことができる。

【０３０８】

$T \rightarrow V : N_V E(K_V, B_{id} K_{BV} X N'_V K'_V) E(K_B, K_{BV} N'_B K'_B)$

【０３０９】

例えば、ヴェラがメッセージを受信し、メッセージの第１の部分を解読することができる。しかし、メッセージの第２の部分はボブの秘密鍵K_Bで暗号化されているので、ヴェラは第２の部分は解読することができない。メッセージの第１の部分を解読すると、ヴェラは、ヴェラとボブとが通信するようにトレントにより生成された秘密の取引鍵K_{BV}を、復元することができる。ヴェラは、メッセージの第２の部分をボブに転送する。上記で述べたように、一部の実施形態において、トレントがメッセージの第１の部分にデータＸを含めた場合は、ヴェラは、秘密鍵K_{BV}で暗号化されたデータＸをボブへ送ることもできる。

【０３１０】

$V \rightarrow B : E(K_B, K_{BV}, N'_B K'_B) E(K_{BV}, X)$

【０３１１】

ボブとヴェラとが各自のメッセージをトレントおよび／または互いから受信した後には、ボブとヴェラは、取引を交渉するために使用できる秘密鍵（K_{BV}）を共有している。図１９に示すように、ボブとヴェラは、秘密鍵（K_{BV}）を使用して取引の交渉を行い、購入者情報とベンダ情報とを交換することができる。購入者情報は、購入者から提供された輸送情報を含むことができる。ボブとヴェラが取引について合意すると、ボブとヴェラは、支払いの交渉をできる状態となる。

【０３１２】

ある口座に関連したすべての取引は、購入者が他の者を除外するように購入者自身を識別することを必要とするものと想定する。従来の商取引では、これには、特定の口座番号と署名の入ったカードを使用することを伴う。電子商取引では、口座番号および他のデー

タ（課金用の住所の郵便番号など）が使用されて購入者を識別する。

【０３１３】

一部の実施形態では、購入者（ボブ）は、取引で同時に識別される。購入者を識別するために静的な口座番号を使用する代わりに、購入者と取引とのエレメントが組み合わせられて、購入者の証明を生成する。一部の実施形態では、購入者と、購入者の口座を保持する支払い認証者とのみに知られた購入者のエレメント（例えばx_Bとy_B）、ベンダのエレメント（V_{id}）、売渡証（Ｓ）、および同意された価格（Ｐ）が組み合わせられて、購入者の証明（B_{cred}）を生成する。購入者は、購入時にこの証明を計算することができる。

【０３１４】

例えば、x_Bとy_Bがボブの口座番号の一部分であるとする。販売時に、ボブは、自分の証明を次のように生成することができる。

【０３１５】

$B_{cred}=E(x_B, y_B V_{id} H(SP) P)$

【０３１６】

x_Bを知っている者のみがこのメッセージを復号することができる。一部の実施形態では、ボブとキャロルだけがx_B（およびy_B）を知っているので、このメッセージは、安全にトレントに渡されることができる。なぜなら、トレントは、メッセージを復号することができず、従って、口座情報を入手することができないからである。

【０３１７】

一部の実施形態では、ボブが価格をごまかさないことを保証するために、ヴェラは、同様の証明を生成する。キャロルは、ヴェラの証明を使用して、ボブとヴェラとが売渡証（Ｓ）および価格（Ｐ）に合意することを確認することができる。

【０３１８】

$V_{cred}=E(x_V, y_V B_{id} H(SP) P)$

【０３１９】

ボブとヴェラは、例えば、電子商取引プロトコルの先の実施形態で説明した機構などのような他の機構を使用して、各自の証明を構築できることを理解されたい。

【０３２０】

購入プロトコルを開始するために、ヴェラは、ボブへ、署名されたベンダ取引データを送信する。ベンダ取引データは、売渡証および価格のハッシュ（Ｈ（ＳＰ））とヴェラの証明（V_{cred}）を含むことができる。価格を平文ではなくハッシュに含めることにより、トレントは、売渡証とそれに対応する価格を知らされない。ヴェラは、彼女の秘密鍵（K'_V）でデータを暗号化し、暗号化したデータに彼女の秘密の数（N'_V）を先頭に付加する。

【０３２１】

$V \rightarrow B : N'_V E(K'_V, H(SP) V_{cred})$

【０３２２】

ボブは、このメッセージを、署名された購入者取引データと連結する。購入者取引データは、ボブの証明（B_{cred}）と、売渡証と価格の別のハッシュ（Ｈ（ＳＰ））を含むことができる。購入者取引データは、キャロルの識別（C_{id}）も含むことができる。ボブは、彼の署名を提供するために、彼の秘密鍵（K'_B）で購入者取引データを暗号化し、彼の秘密の数（N'_B）を先頭に付加する。ボブは、連結されたベンダ取引データと購入者取引データをトレントへ送信する。

【０３２３】

$B \rightarrow T : N'_B E(K'_B, C_{id} H(SP) B_{cred} N'_V E(K'_V, H(SP) V_{cred}))$

【０３２４】

ボブが購入プロセスを開始することもできることを理解されたい。一部の実施形態では、ボブは、署名された購入者取引データをヴェラへ送信する。ヴェラは、署名されたベン

ダ取引データを、受信したデータに連結し、連結したデータをトレントへ送ることができる。

【０３２５】

一部の実施形態では、セキュリティを保証するためのトレントへの制約の一部として、トレントは、取引の詳細を知ることができない。しかし、トレントは、受領証を検証するために取引データを識別することはできる。トレントは、取引データを使用して、ボブとヴェラとが取引について価格と売渡証とに合意したかどうかを判定することができる。売渡証と価格とのハッシュを作成することにより、トレントは、取引データを受信するが、売渡証および／または関連する価格の詳細は判断することができない。

【０３２６】

ベンダ取引データと購入者取引データとを含むメッセージを受信すると、トレントは、データを復号し、購入者取引データとベンダ取引データとを復元する。一部の実施形態では、トレントは、ボブとヴェラとが売渡証と価格について合意したことを検証する。売渡証および／または価格がハッシュとして提供された場合は、トレントは、ヴェラにより提供されたハッシュが、ボブから提供されたハッシュと一致するかどうかを判定する。

【０３２７】

一部の実施形態では、トレントは、ボブの口座番号（x_Bおよびy_B）を知らないので、ボブの証明（B_{cred}）を復号することができない。同様に、トレントは、ヴェラの証明（V_{cred}）を導出することができない。

【０３２８】

取引データを復号した後、トレントは、支払い要求を生成する。トレントは、ボブとヴェラとの間の取引の支払いを要求するために、キャロルへ支払い要求を送信することができる。支払い要求は、ボブ、ヴェラ、キャロルに対しての受領証を含むことができる。それぞれの受領証は、署名入りバージョンの取引データを提供することができる。一部の実施形態では、受領証は、売渡証と価格とのハッシュを含む。それぞれの関係者（参加者）の受領証は、他の２人の関係者の２つの数／鍵の対で暗号化される。例えば、キャロルに対する取引の受領証は、次のようになる。

【０３２９】

$$R_C = N'_B E(K'_B, N'_V E(K'_V, B_{id} V_{id} H(SP)))$$

【０３３０】

受領証は、ボブとヴェラとの両方の秘密鍵を必要とするので、トレントだけがこの値を構築することができる。この意味では、受領証は、認知できるように偽造できない。

【０３３１】

同様に、トレントは、ボブとヴェラへの受領証を作成することができる。

【０３３２】

$$R_B = N_C E(K_C, N'_V E(K'_V, C_{id} V_{id} H(SP)))$$
$$R_V = N'_B E(K'_B, N_C E(K_C, B_{id} C_{id} H(SP)))$$

【０３３３】

支払い要求は、ボブとヴェラとの識別と証明、取引データ、キャロルの受領証、キャロルの新しい数／鍵の対、および／または、売渡証および／または価格のハッシュを含むこともできる。トレントは、キャロル以外の者が要求に含まれるデータを入手できないようにするために、キャロルの現在の秘密鍵（K_C）で支払い要求を暗号化することができる。トレントは、キャロルの秘密の数（N_C）を要求の先頭に付加することもできる。一部の実施形態では、キャロルは、複数の認証者により発行された秘密の数／鍵の対を有し、トレントは、キャロルが要求の復号に使用すべき秘密鍵を識別するために、キャロルの秘密の数を先頭に付加することができる。

【０３３４】

$$M_C = N_C E(K_C, B_{id} B_{cred} V_{id} V_{cred} H(SP) R_C N'_C K'_C)$$

【０３３５】

一部の実施形態では、支払い要求は更に、ボブとヴェラとへ送信するキャロルのメッセ

ージを含む。一部の実施形態では、トレントは、ボブへの２つのメッセージとヴェラへの２つのメッセージを生成する。それぞれのメッセージの対は、「受理」メッセージと「拒絶」メッセージを含む。キャロルは、取引の支払いの要求を引き受ける場合は、ボブとヴェラへ「受理」メッセージを送信する。キャロルは、支払いの要求を引き受けない場合は、ボブとヴェラへ「拒絶」メッセージを送信する。「受理」メッセージはボブとヴェラとへの受領証を含み、従って、支払いの要求が引き受けられる場合、ボブとヴェラとが取引の受領証を受け取る。「受理」メッセージと「拒絶」メッセージとは両方とも、ボブとヴェラとの両方への新しい数／鍵の対も含むことができる。下記のような、新しい数／鍵の対および／または受領証を含む別々のメッセージが生成されて、送信されることもできる。

【０３３６】

$M_B = E(K'_B, \text{“承認”} R_B N''_B K''_B)$
$M'_B = E(K'_B, \text{“拒絶”} R_B N''_B K''_B)$
$M_V = E(K'_V, \text{“承認”} R_V N''_V K''_V)$
$M'_V = E(K'_V, \text{“拒絶”} R_V N''_V K''_V)$

【０３３７】

トレントは、キャロルへ支払い要求を送信する。

【０３３８】

$T \rightarrow C : M_C M_B M'_B M_V M'_V$

【０３３９】

キャロルは、要求を受信すると、ボブとヴェラとの証明（B_{cred}およびV_{cred}）を取り出すことができる。キャロルは、ボブとヴェラとの口座番号を知っているので、両方の証明を解読することができる。キャロルは、ボブとヴェラとが売渡証と価格に合意することも検証することができる。更に、キャロルは、支払いの要求を引き受けるかどうかを決定することができる。キャロルが支払いの要求を引き受ける場合、キャロルは、それぞれに「承認」メッセージを含む応答を、ボブとヴェラとへ送信する。

【０３４０】

$C \rightarrow B : M_B$
$C \rightarrow V : M_V$

【０３４１】

逆に、キャロルが支払いの要求を引き受けない場合、キャロルは、それぞれに「拒絶」メッセージを含む応答を、ボブとヴェラへ送信する。

【０３４２】

$C \rightarrow B : M'_B$
$C \rightarrow V : M'_V$

【０３４３】

キャロルが支払いの要求を引き受ける場合、キャロルはまた、価格Ｐで示されるように、ボブの口座とヴェラの口座との間で資金を移転する。一部の実施形態では、キャロルは、エスクローの役目を果たすことができ、そして、売渡証に含まれる商品がボブへ発送および／または提供されたことをヴェラがキャロルに通知するまで、ボブの口座からの資金を保持することができる。

【０３４４】

上記のプロトコルは、少数の通信と接続とを伴うセキュアな電子商取引プロトコルを説明する。しかし、状況によっては、このプロトコルの適用は、不適当あるいは非効率的である。例えば、上記のプロトコルでは、ヴェラは、彼女の口座情報を、キャロルに到達する前にボブとトレントの両方を通じて、送信する。これは完全に安全であるが、たとえ口座情報がセキュアな暗号化された形態であったとしても、口座情報の配布を回避することが好ましい場合もある。

【０３４５】

上記のプロトコルは、ボブとヴェラとの両方が機密性のある口座情報を直接キャロルに

通信するように、変更が加えられることができる。図２０は、システム２００の別の実施形態を示し、この実施形態は、購入者２６０、ベンダ２２０、支払い認証者２４０、および認証者２８０を含む。図１８と比べると、図２０に示すシステム２００は、それぞれの関係者をシステム２００のすべての他の関係者と接続している。ベンダ２２０、支払い認証者２４０、購入者２６０は、それぞれ、双方向リンク３００、３８０、３６０を介して認証者２８０に接続される。購入者２６０は、双方向リンク３６０と３８０を介してベンダ２２０と支払い認証者２４０にも接続される。更に、ベンダ２２０は、双方向リンク４００を介して支払い認証者２４０に接続される。これらのリンクは、上述のネットワークのすべてまたは一部から構築されることができる。

【０３４６】

図２１は、図２０に示すシステムで使用される通信プロトコルを説明する。ボブとヴェラが売渡証と支払い方法について合意すると、２人は、トレントを通じて間接的にではなく、それぞれ直接キャロルと通信する。一部の実施形態では、これは、キャロルとボブの間、およびキャロルとヴェラの間で秘密の取引鍵を確立することにより達成されることができる。例えば、ボブは、ボブが直接キャロルと通信することを可能にする取引鍵（K_{BC}）の要求を、トレントへ送信する。ヴェラも、キャロルと直接通信できるように、トレントに取引鍵（K_{CV}）を要求することができる。取引鍵（K_{BC}およびK_{CV}）が確立されると、ヴェラとボブとの証明がキャロルへ直接に送信されることができる。

【０３４７】

証明は直接にキャロルへ提供されることができるので、上記のプロトコルは、口座データがトレントを通じて間接的に送信されないように、変更されることができる。ヴェラとボブとが売渡証（Ｓ）および価格（Ｐ）に合意すると、ヴェラは、ベンダ取引データに署名し、署名したデータをボブへ送信する。一部の実施形態では、ベンダ取引データは、売渡証と価格とのハッシュ（Ｈ（ＳＰ））を含む。

【０３４８】

$V \rightarrow B : N'_V E(K'_V, H(SP))$

【０３４９】

上記のプロトコルと異なり、ヴェラは、ベンダ取引データに彼女の証明を含めるのではなく、彼女の証明をトレントから発行された秘密鍵（K_{CV}）で暗号化して直接にキャロルへ送信する。

【０３５０】

$V \rightarrow C : E(K_{CV}, V_{cred})$

【０３５１】

ヴェラから署名されたベンダ取引データを受信すると、ボブは、ヴェラから受信した署名されたベンダ・データを、彼の秘密の鍵／数の対で署名された購入者取引データと連結する。一部の実施形態では、購入者取引データは、売渡証と価格とのハッシュを含む。購入者取引データは、キャロルの識別も含むことができる。ボブは、連結した購入者取引データとベンダ取引データとをトレントへ送信する。

【０３５２】

$B \rightarrow T : N'_B E(K'_B, C_{id} H(SP) N'_V E(K'_V, H(SP)))$

【０３５３】

また、ボブはキャロルとセキュアに直接通信することができるので、ボブはキャロルへ彼の証明（取引の詳細を含むことができる）を送信する。ボブは、彼の証明を、キャロルと共有する秘密鍵（K_{BC}）で暗号化する。

【０３５４】

$B \rightarrow C : E(K_{BC}, B_{cred})$

【０３５５】

トレントは、連結された取引データを受信し、キャロルへの支払い要求を作成する。この支払い要求は、ボブの証明およびヴェラの証明以外は、上記のプロトコルで説明した情報と同じ情報を含むことができる。

【０３５６】
トレントからの支払い要求とボブおよびヴェラからの証明とを受信すると、キャロルは、先のプロトコルで受信した情報と同じ情報を持つことになるが、この情報は異なる通信路または接続を通じて受信している。何者かがキャロルに提供されるメッセージの１つを不法に入手し、再送した場合でも、キャロルは、支払いを承認する前に、それぞれの関係者からのメッセージを受信し、検証しなければならない。更に、トレントからの支払い要求は変化識別子を含んでおり、そのため、キャロルは、不法に再送されたトレントからのメッセージを復号することができない。なぜなら、変化識別子は前回の使用以降に変動または変化しているからである。
【０３５７】
そして、キャロルは、その取引の支払いの要求を引き受けるかどうかを決定する。キャロルが支払いの要求を引き受ける場合、キャロルは、「承認」メッセージを含む応答をボブとヴェラへ送信する。キャロルは、支払いの要求を引き受けない場合、「拒絶」メッセージを含む応答をボブとヴェラへ送信する。一部の実施形態では、キャロルは、トレントにより発行された秘密の鍵でボブおよびヴェラへの応答を暗号化して、取引を更にセキュアにする。例えば、キャロルが支払いの要求を引き受ける場合は、次の応答を送信する。
【０３５８】
$C \rightarrow B : E(K_{BC}, M_B)$
$C \rightarrow V : E(K_{CV}, M_V)$
【０３５９】
キャロルが要求を受け入れる場合、キャロルは、ボブの口座からヴェラの口座へ資金を送る。しかし、一部の実施形態では、キャロルは、エスクローの役目を果たすことができ、ボブの口座からヴェラの口座に資金を送る前に、その取引に含まれる商品がボブへ発送および／または提供された旨の通知をヴェラおよび／またはボブから受信するまで待つ。
【０３６０】
一方、キャロルが支払いの要求を受け入れない場合は、次の暗号化した応答を送信する。
【０３６１】
$C \rightarrow B : E(K_{BC}, M'_B)$
$C \rightarrow V : E(K_{CV}, M'_V)$
【０３６２】
理解されるように、上記のプロトコルを使用して、電子商取引と非電子商取引との両方で、セキュアな商取引を行うことができる。更に、認証者と支払い認証者との役割は組み合わせられることもできることを理解されたい。例えば、それぞれの支払い認証者は、その支払い認証者自身の変化識別子を、そのクライアント（口座を保持する個人）に提供することができる。
【０３６３】
また、上記のプロトコル（またはその一部）は、組み合わせられることが可能であることも理解されたい。例えば、コンテンツ提供者またはサービス提供者からのデジタル・コンテンツの購入に、電子商取引が含められることもできる。また、電子商取引に透かしを入れて、取引データとそれに対応する受領証との一意性を保証することができる。更なる組み合わせおよびコンフィギュレーションも可能である。
【０３６４】
送信されるデータの可能な限り最良のセキュリティを保証するために、変化ＩＤの秘密鍵（例えば、K_B、K_C、K_V）は、秘密に保たれる必要がある。例えば、トレントがボブに、ボブの現在の秘密鍵（例えばK_B）で暗号化された新しい変化ＩＤを提供する場合、ボブの現在の秘密鍵を特定した盗聴者は、トレントから提供されるボブの新しい変化ＩＤを入手することができる。そして、盗聴者は、新しい変化ＩＤを使用して、偽のデータを送信すること及び／又はボブとトレントとの間で交換されるその後のデータの平文を入手することができる。

【０３６５】
理論的には、１人または複数の盗聴者が、力任せ攻撃（brute force attack、ブルート・フォース攻撃／総当たり攻撃）を行うことにより特定のデータを暗号化するために使用される鍵を特定する（または特定を試みる）ことが可能である（本文献の先の部分で述べたように現実性はごく低いが）。図２２に示すように、ブルート・フォース攻撃は、整合性のあるデータまたは認識可能なデータ（例えば、人間に読めるデータ）を生成する鍵が見つかるまで、すべての可能な鍵で暗号文を解読することを含む。図２２に示すように、盗聴者は、最初の候補の鍵、即ち、ゼロの候補鍵を決定する（ステップ４００）。盗聴者は次いで、その候補鍵を使用して暗号文を解読する（ステップ４０２）。暗号文を解読すると、盗聴者は、その結果（即ち、候補の平文）を調べて、候補鍵で解読された暗号文が、整合性のある平文または整合性のあるパターンを生成するかどうかを判定する（ステップ４０４）。盗聴者が、入手された暗号文に対応する平文（またはその一部またはパターン）を入手している又は知っている場合、正しい候補鍵が見つかったかどうかをより容易に判定することができる。例えば、盗聴者が暗号文を入手し、その暗号文が、個人名と、その後に続く４桁の暗証番号（「ＰＩＮ」）を含むことを知っている場合、盗聴者は、候補の鍵が、個人名を含む平文を生成するまで候補鍵を適用することができる。そして、盗聴者は、生成された平文に含まれる残りの情報がそのＰＩＮに対応することを、ある程度の確実性をもって推測することができる。

【０３６６】
図２２に示すように、盗聴者が、特定の候補鍵で暗号文を解読することにより生成された候補の平文中に整合性のあるパターンを見つけると（ステップ４０６）、盗聴者は、現在の候補鍵が、暗号文を生成するのに使用された鍵と等しい、またはその鍵であることをある程度の確実性で知る（ステップ４０７）。

【０３６７】
盗聴者が、特定の候補鍵で暗号文を解読することにより生成された候補の平文に整合性のあるパターンを見つけられない場合（ステップ４０６）、盗聴者は、候補鍵に変更を加え（例えば、候補鍵を増分し）（ステップ４０８）、変更を加えた候補鍵を使用して暗号文を解読し（ステップ４０２）、生成された候補平文に整合性のある平文または整合性のあるパターンがあるか調べる（ステップ４０４）。十分な処理力と時間とがあれば、盗聴者は、特定の候補鍵が整合性のある平文または整合性のあるパターンを有する候補平文を生成するまで、このプロセスを継続することができ、従って、暗号文を生成するために使用された鍵を特定することができる。

【０３６８】
しかし、盗聴者が平文または平文のパターンについて何の知識も持たない場合（即ち、内容の手がかりを持たない場合）、正しい候補鍵が見つかったかどうかを判定する盗聴者の能力は大きく低下し、恐らくは、なくなる。例えば、平文が、特定の鍵で暗号化された乱数を含む場合には、盗聴者がブルート・フォース攻撃で何個の鍵を試みても、盗聴者には、候補の平文が、暗号文に対応する真の平文であるかどうかを判定する手段がない。暗号化された乱数を任意の候補鍵で解読すると乱数が生成され、その乱数は、他の候補鍵で生成される他の乱数のような、当初の乱数のようなものである。

【０３６９】
ボブ、ヴェラ、トレントに関連する上記の取引鍵を交換する例を参照すると、暗号化されたメッセージの何れかの部分が認識可能であるか、既知であるか、既知になるか、または何らかの内容の手がかりを含む場合、盗聴者は、暗号化されたメッセージに平文攻撃または部分平文攻撃を行い、そのメッセージを暗号化するために使用されたボブまたはヴェラの秘密鍵を発見できる可能性がある。例えば、ボブが次のメッセージをトレントへ送信し、このメッセージが盗聴者に傍受されるとする。

【０３７０】
$B \rightarrow T : N_B E(K_B, V_{id} X)$

【０３７１】

盗聴者は、ヴェラの識別V_{id}と上記メッセージの形式とが既知であるか、あるいは公開されているので、傍受したメッセージにブルート・フォース攻撃を行うことができる。従って、盗聴者は、ボブの秘密鍵K_BとデータXを入手することができる。更に、盗聴者は、ボブの秘密鍵K_Bを入手すると、ボブの現在の秘密鍵K_Bを使用して、ボブの次の変化ＩＤ（例えばN_B'およびK_B'）などのような、ボブの現在の秘密鍵K_Bで暗号化されたすべてのデータを入手することができる。

【０３７２】

盗聴者は、暗号化されたメッセージまたは暗号化されたメッセージを生成するために使用された通信プロトコルについての他の知識を使用して、ブルート・フォース攻撃を行うことができる。例えば、盗聴者は、暗号化しないで渡される変化ＩＤの数（例えばN_B）を使用してブルート・フォース攻撃を行うことができる。盗聴者は、変化ＩＤの数を生成するために使用されるアルゴリズムについての知識も使用して、ブルート・フォース攻撃を行うこともできる。

【０３７３】

上記で指摘したように、発見不可能なデータ（すなわち、ランダムのデータまたは内容の手がかりを持たないデータ）を暗号化するために使用された鍵は、ブルート・フォース攻撃を使用して特定または発見されることはできない。なぜなら、盗聴者は、正しい候補鍵が見つかった時にそれを判断することができないからである。しかし、発見可能データ（即ち、既知のデータ、後に開示される可能性のあるデータ、認識可能なデータ、または既知の形式や容易に推測される形式を持つデータ）を暗号化するために使用された鍵は、ブルート・フォース攻撃を使用して特定されることができる（理論的には）。発見可能データおよび発見不可能データが、一緒に、または同じ暗号鍵で暗号化された場合、発見可能データを使用してブルート・フォース攻撃を通じて特定される鍵は、発見不可能データを暗号化するために使用された鍵でもあり、従って、発見不可能データが発見されることができる。

【０３７４】

暗号化データのセキュリティを高め、盗聴者がブルート・フォース攻撃を使用して暗号鍵を入手するのを阻止するために、本発明の実施形態は、変化ＩＤに含まれる秘密鍵などのような発見不可能データのセキュリティを保護する暗号化方式を提供する。

【０３７５】

図２３は、暗号化されるデータに含められることが可能なデータの種類を示す。暗号化され、特定の受信者へ送信されるデータ４２０は、データのタイプまたはクラスに区分される。第１のクラスのデータは、発見不可能データ、即ち、秘密データのクラス４３０を含む。秘密データ・クラス４３０は、秘密に保たれ、権限のあるエンティティのみに知られたデータを含むことができる。例えば、秘密データ・クラス４３０は、変化ＩＤの秘密鍵および／またはエンティティの証明を含むことができ、これらは両方ともランダムであり、認証者および／または支払い認証者と、その証明および秘密鍵の所持者とのみにより知られ得る。

【０３７６】

第２のクラスのデータは、発見可能データ・クラス４４０を含む。発見可能データ・クラス４４０は、既知のデータ、後に知られる可能性のあるデータ、認識可能な（例えば、人間が読める）データ、または既知の形式や容易に推測される形式を持つデータを含むことができる。一部の実施形態では、発見可能データ４４０は更に、幾つかの下位クラスに分割される。例えば、発見可能データ・クラス４４０は、第１のタイプの発見可能データを含む第１の発見可能データ・サブクラス４４２を含むことができる。第１のタイプの発見可能データは、標準化されたヘッダや、既知のパターンや、他の公的に使用可能な形式等のような、容易に区別される特徴を有するデータを含み得る。一部の実施形態では、第１の発見可能データ・サブクラス４４２は、エンティティ間で送信されるコンテンツと、認証者により提供される変化ＩＤの数（例えば、N_B、N_V、N_C）を含む。

【０３７７】

発見可能データ・クラス４４０は、第２のタイプの発見可能データを含む第２の発見可能データ・サブクラス４４４を含むこともできる。第２のタイプの発見可能データは、第１のタイプの発見可能データを含むメッセージを暗号化するために使用された鍵を含むことができる。一部の実施形態では、第２の発見可能データ。サブクラス４４４は、変化ＩＤの秘密鍵（例えば、K_B、K_V、K_C）を含む。例えば、取引鍵の交換プロトコルに関して上記で述べたように、ボブは、彼の秘密鍵K_Bで暗号化されたヴェラの公に知られた識別子V_{id}を含むメッセージを、トレントへ送信する。

【０３７８】

$B \rightarrow T : N_B E(K_B, V_{id} X)$

【０３７９】

ヴェラの識別子V_{id}は、公に知られており、従って、第１のタイプの発見可能データであることから、ボブの秘密鍵K_Bは、第２のタイプの発見可能データと考えることができる。なぜなら、ボブの秘密鍵K_Bは、第１のタイプの発見可能データを暗号化しているからである。

【０３８０】

発見可能データ・クラス４４０は更に、第３の発見可能データ・サブクラス４４６を含むことができ、このサブクラスは、本来は発見不可能なデータであるが、第２のタイプの発見可能データとみなされる鍵で暗号化されているために発見可能になるデータを含む。例えば、ボブからトレントへ送信される上記のメッセージに示すように、データＸは、ランダムにボブに割り当てられ、ボブとトレントのみに知られる。従って、データＸは、発見不可能である。しかし、データＸはボブの秘密鍵K_B（これは、発見可能データ（例えばV_{id}）を暗号化するために使用されるため、第２のタイプの発見可能データである）で暗号化されているので、データＸは、第３のタイプの発見可能データと考えられることができる。

【０３８１】

図２４および図２５は、発見不可能データのセキュリティを保護する暗号化方式を説明する。発見不可能データ、即ち、秘密データのセキュリティを保護するために、別個の鍵が使用されて異なるタイプのデータを暗号化する（以後「分離暗号化プロトコル」と称する）。例えば、１または複数の鍵（例えば、１または複数の変化ＩＤ）が使用されて発見不可能データを暗号化し、１または複数の鍵（例えば、１または複数の変化ＩＤ）が使用されて発見可能データを暗号化することができる。下記で述べるように、発見不可能データと発見可能データとを暗号化するために同じ鍵は決して使用されないので、第３のタイプの発見可能データがなくなる。

【０３８２】

図２４に示すように、秘密データ・クラス４３０に含まれるデータは、秘密データ・クラス４３０に含まれるデータの暗号化のみに使用される１または複数の鍵４５０（この例では以後「発見不可能データ鍵４５０」と称する）で暗号化されることができる。オプションとして、発見可能データ・クラス４４０に含まれるデータは、発見可能データ・クラス４４０に含まれるデータの暗号化のみに使用される１または複数の鍵４６０（この例では以後「発見可能データ鍵４６０」と称する）で暗号化されることができる。秘密データ・クラス４３０に含まれるデータを暗号化するために使用される発見不可能データ鍵４５０は、発見可能データ・クラス４４０に含まれるデータを暗号化するために使用される発見可能データ鍵４６０から特定されることはできない（即ち、鍵４６０とは無関係である）ことを理解されたい。データ４２０は、そのデータ４２０の個々の部分が所属するデータ・クラスに従って分けて、連続したデータ・ブロックに入れるようにする必要はないことも理解されたい。図２５に示すように、秘密データ・クラス４３０と発見可能データ・クラス４４０とに含まれるデータは、混在させた幾つかの部分に分割されることができる。

【０３８３】

上記で述べたように、発見不可能データから発見可能データを分離し、発見不可能デー

タを、発見可能データを暗号化するために使用された発見可能データ鍵４６０と異なる発見不可能データ鍵４５０で暗号化することにより、発見可能データ鍵４６０は発見不可能データの暗号化には決して使用されないので、第３のタイプの発見可能データがなくなる。従って、発見可能データを暗号化するために使用された発見可能データ鍵４６０がブルート・フォース攻撃を使用して特定されたとしても、その特定された発見可能データ鍵４６０を使用して、発見不可能データまたは秘密データを入手することはできない。

【０３８４】

例えば、ボブが、ヴェラとの通信に使用する取引鍵をトレントに要求したいと思っており、従って、ボブがトレントへデータＸとヴェラの識別子V_{id}とを送信するとする。また、ボブが、発見不可能データのみに使用される数N_{B1}とそれに対応する鍵K_{B1}（この例では、以後それぞれを「発見不可能データの数N_{B1}」、「発見不可能データ鍵K_{B1}」と称する）を含む変化ＩＤと、第１のタイプおよび第２のタイプの発見可能データのみに使用される数N_{B2}と鍵K_{B2}（この例では、以後それぞれ「発見可能データの数N_{B2}」、「発見可能データ鍵K_{B2}」と称する）を含む変化ＩＤを有するとする。ヴェラの識別子V_{id}は第１のタイプの発見可能データ（即ち、公に知られている）なので、ボブは、彼の発見可能データ鍵K_{B2}でヴェラの識別子V_{id}を暗号化することができる。同様に、ボブは、彼の発見不可能データ鍵K_{B1}でデータＸを暗号化することができる。ヴェラの識別子V_{id}は、データＸとは別に暗号化されることから、データＸは、発見可能データを暗号化する鍵で暗号化されないので、上記のようにもはや第３のタイプの発見可能データとはみなされない。従って、データＸは、発見不可能データになる。一部の実施形態では、ボブはまた、トレントに対してボブ自身とメッセージの個々の部分とを識別するために、別々に暗号化された部分に、発見不可能データの数N_{B1}と発見可能データの数N_{B2}を付加する。ボブは、その結果として作成されたメッセージをトレントへ送信することができる。

【０３８５】

$B \rightarrow T : N_{B1} E(K_{B1}, X) N_{B2} E(K_{B2}, V_{id})$

【０３８６】

盗聴者が、ボブからトレントへ送信される上記の送信を入手した場合、盗聴者は、ヴェラの識別子V_{id}を暗号化した発見可能データ鍵K_{B2}を、ブルート・フォース攻撃を使用して入手することができる（理論的には）。しかし、第２の秘密鍵K_{B2}を知ることでは、盗聴者は発見不可能データ鍵K_{B1}を取得することはできず、従って、同じく、発見不可能データ鍵K_{B1}で暗号化されたデータＸまたは他のデータは取得できない。上記で述べたように、ボブは、ヴェラの識別子V_{id}を暗号化せず、平文で送信することを選択することもできる。

【０３８７】

鍵の交換を完了するために、ヴェラが、発見不可能データのみに使用される数N_{V1}およびそれに対応する鍵K_{V1}を含む変化ＩＤ（この例では、以後それぞれを「発見不可能データの数N_{V1}」および「発見不可能データ鍵K_{V1}」と称する）と、発見可能データのみに使用される数N_{V2}および鍵K_{V2}（この例では、以後それぞれ「発見可能データの数N_{V2}」、「発見可能データ鍵K_{V2}」と称する）を含む変化ＩＤと、ヴェラおよびトレントのみに知られたデータＹとを有するものとする。

【０３８８】

トレントは、ボブとヴェラに割り当てられた変化ＩＤを知っており、ボブからのメッセージを解読することができ、ボブとヴェラへの取引鍵K_{BV}を生成することができる。取引鍵K_{BV}は、第１のタイプの発見可能データを暗号化するためにボブおよび／またはヴェラにより使用される可能性があるので、取引鍵K_{BV}は、第２のタイプの発見可能データと考えることができ、ボブとヴェラの発見可能データ鍵（例えば、K_{B2}およびB_{V2}）で暗号化されることができる。トレントは、別々の応答で、取引鍵K_{BV}をボブとヴェラとへ提供する。

【０３８９】

一部の実施形態では、トレントのボブへの応答は、取引鍵K_{BV}と、データXと、発見不可能データのみに使用されるボブの新しい数N_{B1}'および新しい鍵K_{B1}'（この例では、以後それぞれを「新しい発見不可能データの数N_{B1}'」および「新しい発見不可能データ鍵K_{B1}'」と称する）を含む変化ＩＤと、第１のタイプおよび第２のタイプの発見可能データのみに使用されるボブの新しい数N_{B2}'および新しい鍵K_{B2}'（この例では、以後それぞれを「新しい発見可能データの数N_{B2}'」および「新しい発見可能データ鍵K_{B2}'」と称する）を含む変化ＩＤとを含む。取引鍵K_{BV}は、第１のタイプの発見可能データを暗号化するために使用されることができるので、トレントは、ボブの現在の発見不可能鍵K_{B1}で取引鍵K_{BV}を暗号化する。データXも発見不可能データなので、トレントは、データXもボブの現在の発見不可能データ鍵K_{B1}で暗号化する。更に、ボブの新しい発見不可能データ鍵K_{B1}'は発見不可能データと考えられるので（発見不可能データの暗号化のみに使用されるランダムの秘密鍵だから）、トレントは、ボブの現在の発見不可能データ鍵K_{B1}で新しい発見不可能データ鍵K_{B1}'を暗号化する。しかし、新しい発見不可能データの数N_{B1}'と新しい発見可能データの数N_{B2}'とは、暗号化されないで渡されるため、第１のタイプの発見可能データである。従って、トレントは、ボブの現在の発見可能データ鍵K_{B2}で、新しい発見不可能データの数N_{B1}'と新しい発見可能データの数N_{B2}'を暗号化する。また、ボブの新しい発見可能データ鍵K_{B2}'は第１および第２のタイプの発見可能データを暗号化するために使用されるので、トレントは、ボブの現在の発見可能データ鍵K_{B2}を使用して、鍵K_{B2}'を暗号化する。オプションとして、トレントの応答は、ヴェラの識別子V_{id}を含むことができ、ヴェラの識別子V_{id}は第１のタイプの発見可能データなので、トレントは、ボブの現在の発見可能データ鍵K_{B2}を使用してヴェラの識別子V_{id}を暗号化することができる。一部の実施形態では、トレントは、ボブの現在の発見不可能データの数N_{B1}を、ボブの現在の発見不可能データ鍵K_{B1}で暗号化された応答の部分に付加し、ボブの現在の発見可能データの数N_{B2}を、ボブの現在の発見可能データ鍵K_{B2}で暗号化された応答の部分に付加して、応答の別々の部分を識別するようにする。トレントは、次いで応答をボブへ送信することができる。

【０３９０】

$T \rightarrow B : N_{B1} E(K_{B1}, K_{B1}' X) N_{B2} E(K_{B2}, N_{B1}' N_{B2}' K_{B2}' V_{id} K_{BV})$

【０３９１】

トレントは、同様の応答を生成し、ヴェラへ送信することができる。

【０３９２】

$T \rightarrow V : N_{V1} E(K_{V1}, K_{V1}' Y) N_{V2} E(K_{V2}, N_{V1}' N_{V2}' K_{V2}' B_{id} K_{BV})$

【０３９３】

上記のプロトコルは、メッセージ単位で何れのプロトコルに対しても一般化されることができる。例えば、$N_x E(K_x, D_1 D_2 \ldots)$が送信されようとするメッセージであるとし、$N_x$は、オプションのパラメータであるとする。上記の分離暗号化プロトコルを使用してこのメッセージを送信するために、メッセージの元の形式に基づいて、データD_1、D_2、．．．を発見不可能なデータと３つのタイプの発見可能データに分ける。例えば、D_1^*、D_2^*，．．．を発見不可能データであるとし、D_1^+、D_2^+，．．．を第１のタイプおよび第２のタイプの発見可能データであるとし、$D_1^\#$、$D_2^\#$，．．．を第３のタイプの発見可能データであるとする。そして、発見不可能データ（D_1^*、D_2^*，．．．）と第３のタイプの発見可能データ（$D_1^\#$、$D_2^\#$，．．．）とを第１の鍵K_1で暗号化し、第１のタイプおよび第２のタイプの発見可能データ（D_1^+、D_2^+，．．．）を第２の鍵K_2で暗号化することにより、メッセージが構築されることができ、ここで、第１の鍵K_1と第２の鍵K_2とは異なり、互いから計算で導出することはできない。

【０３９４】

一部の実施形態では、エンティティが、第２のタイプの発見可能データを更に保護することを望む可能性がある。例えば、上記のように、トレントが取引鍵K_{BV}をボブに提供する際、トレントは、ボブの現在の発見可能データ鍵K_{B2}で取引鍵K_{BV}を暗号化する。しかし、発見可能鍵K_{B2}は、公に知られているヴェラの識別子V_{id}の暗号化にも使用される。そのため、盗聴者が、ボブの現在の発見可能データ鍵K_{B2}で暗号化されたトレントからの応答の部分にブルート・フォース攻撃を行い、K_{B2}だけでなく、取引鍵K_{BV}も入手することができる。この技術を使用して、盗聴者は、取引鍵K_{BV}がボブまたはヴェラに使用される前に、または、ボブおよび／またはヴェラが発見可能データを暗号化するために取引鍵K_{BV}を使用しなくとも、取引鍵K_{BV}を入手することができる。

【０３９５】

上記の問題を克服することを試みるために、第２のタイプの発見可能データは、第１のタイプの発見可能データの暗号化に使用される鍵とは別の鍵で暗号化されることができる。一部の実施形態では、第２のタイプの発見可能データの暗号化のみに使用される数と秘密鍵を含んだ別個の変化ＩＤが、エンティティに割り当てられる。例えば、ボブが、第２のタイプの発見可能データの暗号化のみに使用される代替の数N_{B3}と代替の鍵K_{B3}を含む代替の変化ＩＤを持っているとすると、トレントからボブへ送信される上記の応答は、代替の鍵K_{B3}で暗号化された取引鍵K_{BV}を含むように変更されることができる。

【０３９６】

$T \rightarrow B : N_{B1} E(K_{B1}, K_{B1}', X) N_{B2} E(K_{B2}, N_{B1}', N_{B2}', K_{B2}', V_{id}) N_{B3} E(K_{B3}, K_{B3}', K_{BV})$

【０３９７】

取引鍵K_{BV}と第１のタイプの発見可能データ（例えば、N_{B1}'、N_{B2}'、およびV_{id}）を別々に暗号化することにより、盗聴者は、トレントからボブへの応答にブルート・フォース攻撃を行うことで取引鍵K_{BV}を入手することはできない。応答に対するブルート・フォース攻撃で第２のタイプの発見可能データが明らかになるのを阻止するために、発見可能データ鍵K_{B2}'および／または他の第２のタイプの発見可能データは、発見可能データ鍵K_{B2}で暗号化するのではなく、代替の鍵K_{B3}で暗号化されることもできることを理解されたい。

【０３９８】

一部の実施形態では、第２のタイプの発見可能データを暗号化するための代替の変化ＩＤを受け取る代わりに、エンティティは、１回使用されるたびに又は別の時程で（例えば、何回かの使用後や、特定の期間後など）変動する又は変動しない一つの代替の鍵を受け取る。この代替鍵は、認証者と、その代替鍵を割り当てられたエンティティとのみに知られる秘密鍵である。一部の実施形態では、エンティティは、その代替鍵を使用して、第２のタイプの発見可能データを直接に暗号化する。他の実施形態では、エンティティは、自身の代替鍵と発見不可能データ鍵とを使用して、第２のタイプの発見可能データの暗号化に使用される新しい鍵を生成する。例えば、ボブが、ヴェラと取引鍵の交換を開始することを希望しており、従って、ボブがトレントへヴェラの識別子V_{id}とデータＸを送信するものとする。また、ボブが、発見不可能データのみに使用される数N_{B1}とそれに対応するデータ鍵K_{B1}（この例では、以後それぞれを「発見不可能データの数N_{B1}」、「発見不可能データ鍵K_{B1}」と称する）を含む変化ＩＤと、第１のタイプの発見可能データのみに使用される数N_{B2}と鍵K_{B2}（この例では、以後それぞれ「発見可能データの数N_{B2}」、「発見可能データ鍵K_{B2}」と称する）を含む変化ＩＤと、取引鍵K_{BV}等のような第２のタイプの発見可能データの暗号化のみに使用される代替鍵L_Bとを有するものとする。一部の実施形態では、ボブは、彼の発見可能データ鍵K_{B2}を自身の代替鍵L_Bとして使用する。他の実施形態では、ボブは、データＸを彼の代替鍵L_Bとして使用することができる。ボブの発見不可能データ鍵K_{B1}、発見可能データ鍵K_{B2}、および代替鍵L_Bは、すべてトレントに知られており、１回使用されるたびに又は別の時程で変動する（即ち、トレントにより再度割り当てられる）ことができる。

【０３９９】

上記のように、取引鍵の交換を開始するために、ボブは、データＸとヴェラの識別子V_{id}を含む要求を生成する。ボブは、上記のように要求を分け、暗号化することができる。ボブは、トレントへその要求を送信する。

【０４００】

要求を受信すると、トレントは、要求される取引鍵K_{BV}を生成することができる。ボブへ取引鍵K_{BV}を送信するために、トレントは、新しい暗号鍵を生成するために、ボブの発見不可能データ鍵K_{B1}とボブの代替鍵K_{B3}（またはL_B）のＸＯＲを生成することができる。

【０４０１】

$XOR(K_{B1}, K_{B3})$

【０４０２】

ＸＯＲ演算では、ボブの発見不可能データ鍵K_{B1}とボブの代替鍵K_{B3}とのビット単位の排他的「ｏｒ」演算を行う。従って、このＸＯＲ演算では、ボブの発見不可能データ鍵K_{B1}とボブの代替鍵K_{B3}とのうちの、より長い鍵の長さと等しい長さのビット列を生成する。生成されるビット列のそれぞれのビット位置は、ボブの発見不可能データ鍵K_{B1}とボブの代替鍵K_{B3}との対応する位置が同じ（即ち、両方とも「０」または両方とも「１」）である場合に「０」と等しくなり、ボブの発見不可能データ鍵K_{B1}とボブの代替鍵K_{B3}との対応する位置が同じでない場合に「１」に等しくなるように設定される。ＸＯＲ演算は、一般に、入力の１つ（例えば、ボブの発見不可能データ鍵K_{B1}またはボブの代替鍵K_{B3}）が既知でない場合に、不可逆となる。

【０４０３】

トレントは、生成されたビット列（即ち、ＸＯＲ演算の結果）を使用して、取引鍵K_{BV}を暗号化する。トレントは、暗号化された取引鍵K_{BV}を応答でボブへ送信する。トレントは、上記のように応答を分け、暗号化することができる。

【０４０４】

$T \rightarrow B : N_{B1} E(K_{B1}, K_{B1}\text{'}X) N_{B2} E(K_{B2}, N_{B1}\text{'}N_{B2}\text{'}K_{B2}\text{'}V_{id}) E(XOR(K_{B1}, K_{B3}), K_{BV})$

【０４０５】

ボブは、解読鍵を生成し、取引鍵K_{BV}を入手するために、トレントと同じＸＯＲ演算を行うことができる。盗聴者が、取引鍵K_{BV}を入手し、ブルート・フォース攻撃を通じて暗号鍵（即ち、ＸＯＲ演算の結果として得られるビット列）を入手しようとしても、盗聴者は、盗んだ鍵を使用して、ボブの発見不可能データ鍵K_{B1}、ボブの代替鍵K_{B3}、データＸを入手することはできない。また、ボブの発見不可能データ鍵K_{B1}とボブの代替鍵K_{B3}との少なくとも一方が、１回の使用ごとに又は別の時程で変動する場合には、盗まれた鍵は、その後のメッセージに含まれるデータの暗号化には使用されない。従って、盗まれた鍵を使用して、そのようなメッセージに含まれるデータを入手することはできない。

【０４０６】

一部の実施形態では、さらなるセキュリティを提供するために、発見可能データと発見不可能データを暗号化するために使用される異なる鍵は、入れ子（ネスト）にされる（以後「入れ子型分離暗号化プロトコル」と呼ぶ）。例えば、上記のようにボブが次のメッセージをトレントへ送信するとする。

【０４０７】

$B \rightarrow T : N_{B1} E(K_{B1}, X) N_{B2} E(K_{B2}, V_{id})$

【０４０８】

このメッセージは、２つの別個の部分を含む。例えば、このメッセージは、暗号化された発見不可能データを含む第１の部分$N_{B1} E(K_{B1}, X)$と、暗号化された発見可能データを含む第２の部分$N_{B2} E(K_{B2}, V_{id})$を含む。これらの部分は、別々に暗号化され、ともに連結されるので、盗聴者は、それら部分を別々に攻撃することができる。

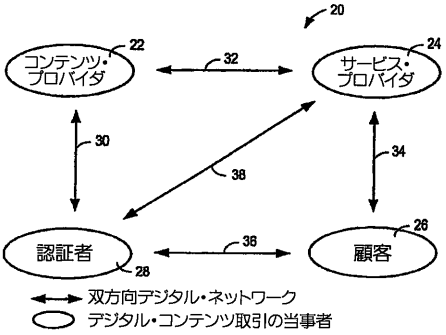
【０４０９】
例えば、盗聴者は、第２の部分にブルート・フォース攻撃を行うことができ（ヴェラの識別子V_{id}が公に知られているため）、ボブの発見可能データ鍵K_{B2}を入手することができる。ボブの発見可能データ鍵K_{B2}を入手すると、盗聴者は、ボブがトレントへ送信した要求の詳細を入手することができる。恐らくは、より損害が大きいが、盗聴者は、中間者攻撃（ｍａｎ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅ　ａｔｔａｃｋ）を行うこともできる。中間者攻撃は、盗聴者が送信データを傍受し、そのデータを読むこと及び／又は改変することを試みる場合に起き、多くの場合、データの送信者と意図されるデータの受信者とに知られずに行われる。例えば、盗聴者は、ボブの盗まれた発見可能データ鍵K_{B2}を使用して、ボブのメッセージの第２の部分を、ボブの発見可能データ鍵K_{B2}で暗号化された盗聴者の識別子に置き換えることにより、ボブのメッセージの第２の部分を改変または再構築することができる。そして、盗聴者は、改変されたメッセージをトレントへ送信することができる。
【０４１０】
トレントは、改変されたメッセージを入手すると、それぞれの部分を解読し、要求される処理を行う。メッセージの第１の部分と第２の部分とは基本的に関係しないので、トレントは、第２の部分に含まれる証明が正当なものであるかどうかを判断する手段を持たない。
【０４１１】
上記の状況を克服するために、ボブは、発見不可能データ鍵K_{B1}と発見可能データ鍵K_{B2}とを使用して、入れ子構造の暗号化を行うことができる。例えば、ボブが、データＸとヴェラの識別子V_{id}とを含むトレントへの要求を生成するとする。ボブは、発見不可能データ鍵K_{B1}でデータＸ（即ち、発見不可能データ）を暗号化することができる。一部の実施形態では、ボブは、彼の発見不可能データの数N_{B1}を、暗号化の結果に付加する。そして、ボブは、暗号化したデータＸにヴェラの識別子V_{id}を付加し、その結果を、発見可能データ鍵K_{B2}で暗号化することができる。そして、ボブは、その結果に、彼の発見可能データの数N_{B2}を付加することができる。
【０４１２】
$B \rightarrow T : N_{B2} E(K_{B2}, V_{id} E(K_{B1}, X))$
【０４１３】
上記の要求は、発見不可能データと発見可能データとの両方に依存する。なぜなら、両形態のデータが最終的な暗号化ステップで含められるからである。入れ子化は、どちらの方向にも行えることを理解されたい。例えば、ボブは、ヴェラの識別子V_{id}を発見可能データ鍵K_{B2}で暗号化し、データＸをその結果に付加し、その組み合わせを発見不可能データ鍵K_{B1}で暗号化することができる。
【０４１４】
$B \rightarrow T : N_{B1} E(K_{B1}, XE(K_{B2}, V_{id}))$
【０４１５】
上記のメッセージに示すように、一部の実施形態では、エンティティは、変化ＩＤの鍵（例えば、K_{B1}およびK_{B2}）が入れ子にされる場合には、自身をメッセージの発信者として識別するために１つの変化ＩＤの数（例えばN_{B1}）のみを必要とすることもある。例えば、ボブには、発見不可能データのみまたは発見可能データのみを暗号化するためにボブが使用することができる１つの数N_Bおよび１つの秘密鍵K_Bを含む１つの変化ＩＤと、その変化ＩＤの秘密鍵K_Bで暗号化されないデータ・タイプを暗号化するためにボブが使用することができる代替鍵L_B等のような一つの別の鍵とが、割り当てられることができる。ボブは、代替鍵L_Bを使用して、秘密鍵K_Bで暗号化されたデータの中に入れ子にされたデータを暗号化することができる。そして、ボブは、その結果に、彼の数N_Bを付加することができる。
【０４１６】
$B \rightarrow T : N_B E(K_B, XE(L_B, V_{id}))$

【０４１７】
上記のプロトコル（例えば、変化ＩＤプロトコル、分離暗号化プロトコル、および入れ子型分離暗号化プロトコル）は、ブルート・フォース攻撃を困難にするか、そのような攻撃の有用性を低下させる機能を含むことができることを理解されたい。例えば、上記のプロトコルは、ブルート・フォース攻撃が成功して鍵が発見されるまでに何日も何ヶ月も、あるいは何年も必要とするような、強い暗号化技術を用いることができる。そのため、理論的には攻撃の手段になると思われるものが、実際的にはそれの使用が困難あるいは不可能となりうる。
【０４１８】
また、盗聴者がブルート・フォース攻撃を行うために必要とされる時間の間にエンティティと認証者の間で複数のメッセージが送信される可能性があるため、盗聴者に傍受されたメッセージに関連した変化ＩＤは、そのエンティティに割り当てられた現在の変化ＩＤとは異なる可能性がある。従って、あるエンティティに割り当てられた現在の変化ＩＤを暴くことを試みる盗聴者は、メッセージをたどって、現在の変化ＩＤを入手するには、そのエンティティと認証者の間で送信されるすべてのメッセージを追跡し、記憶しなければならない。例えば、盗聴者がブルート・フォース攻撃を使用してあるエンティティの変化ＩＤの特定を試みる場合に、認証者は、盗聴者がブルート・フォース攻撃を行っている間に、複数回変化ＩＤを割り当て直すこと、即ち、変動させることができる。盗聴者が最も新しい変化ＩＤの鍵を欲する場合、盗聴者は、現在割り当てられている変化ＩＤを特定するには、現在は無効になっている過去の変化ＩＤを一旦入手すると、その発見した変化ＩＤを使用して、認証者からエンティティへ送信されたそれぞれのメッセージを解読し、変動または割り当て直されたそれぞれの変化ＩＤを入手しなければならない。そのようなトレースを行うための追跡と記憶の要件は、ブルート・フォース攻撃を行うことを試みる盗聴者にとって非常に厳しいものであり得る。
【０４１９】
また、盗聴者は、「有用な」情報を発見するためには複数回のブルート・フォース攻撃を行わなければならない可能性がある。例えば、上記の分離暗号化プロトコルでは、盗聴者は、取引鍵（例えばK_{BV}）で暗号化されたメッセージにブルート・フォース攻撃を行うことができ、従って、取引鍵（例えばK_{BV}）を入手できる可能性がある。しかし、その取引鍵を使用してエンティティの秘密鍵を入手するには、盗聴者は、認証者から送信されたメッセージ、すなわち、そのエンティティの秘密鍵で暗号化された、現在既知となったその取引鍵を含むメッセージに、第２のブルート・フォース攻撃を行うことを必要とされる。上記のように、１回のブルート・フォース攻撃は、計算に何日も何ヶ月も、あるいは何年も要する可能性があり、従って、第２のブルート・フォース攻撃を行うと、「有用な」情報（例えば、変化ＩＤの秘密鍵）を入手するのに必要な時間が倍になり得る。更に、盗聴者は、「有用な」情報を入手するために、入れ子になったブルート・フォース攻撃を行わなければならない可能性もあり、その場合、盗聴者は、それぞれの第１の候補鍵を試し、それぞれの第１の候補鍵について、それぞれの第２の候補鍵を試すことが必要となる。例えば、上記の入れ子型分離暗号化プロトコルでは、下記のメッセージからデータＸを入手するには、盗聴者は、外側の暗号化結果Ｅ（K_B，ＸＥ（L_B，V_{id}）について、すべての候補鍵を試し、そして、外側の暗号化結果の候補鍵ごとに、入れ子になった暗号化結果Ｅ（L_B，V_{id}）についてすべての候補鍵を試す必要がある。
【０４２０】
Ｂ→Ｔ：N_BＥ（K_B，ＸＥ（L_B，V_{id}））
【０４２１】
１回のブルート・フォース攻撃にＮ個の処理時間単位が必要とされる場合、１回の入れ子型のブルート・フォース攻撃（即ち、別のブルート・フォース攻撃の中に入れ子になった１回のブルート・フォース攻撃）には、約N^2個の処理時間単位が必要となり得、その結果、盗聴者にとってブルート・フォース攻撃は、処理要件から見て、非実際的または不可能になり得ることを理解されたい。

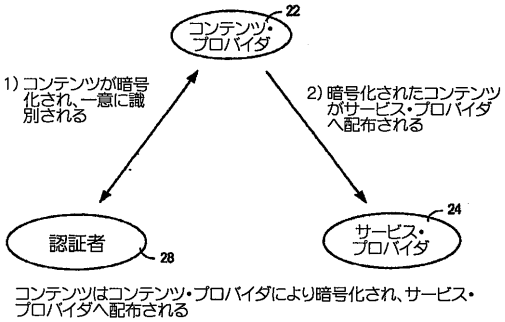
【０４２２】
上記から理解できるように、種々の実施形態は、セキュリティとコンテンツ所有者の法的権利を保護する機能を備える、コンテンツおよび情報を配布するシステムおよび方法を提供する。実施形態は、セキュリティと、取引関係者の機密性のある金融情報を保護する機能を備える電子商取引を行うシステムおよび方法も提供する。本発明の追加的な特徴と態様は、特許請求の範囲に示される。
【図面の簡単な説明】
【０４２３】
【図１】図１は、４つのエンティティが通信に関係する、本発明の一例示的実施形態のシステムの概略図である。
【図２】図２は、３つのエンティティが通信に関係する、本発明の別の例示的実施形態のシステムの概略図である。
【図３ａ】図３ａは、本発明の一実施形態で使用されるビット・ストリーム（「変化識別子」と称される）の図である。
【図３ｂ】図３ｂおよび図３ｃは、変化ＩＤを配布する方式の説明図である。
【図３ｃ】図３ｂおよび図３ｃは、変化ＩＤを配布する方式の説明図である。
【図４】図４は、本発明の一例示的実施形態のためのライセンス構造の概略図である。
【図５】図５は、図１に示されるシステムの一部の概略図である。
【図６】図６は、図１に示されるシステムで使用される通信プロトコルの説明図である。
【図７】図７は、図１に示されるシステムの一部の概略図であり、複数のサービス提供者へのライセンスの配布を説明する。
【図８】図８は、本発明の一形態で使用される変化識別子のサイクルの説明図である。
【図９ａ】図９ａは、本発明の一実施形態におけるコンテンツ鍵の管理の例示的な説明図である。
【図９ｂ】図９ｂは、図９ａに示される状況でコンテンツが要求された時に発生するデータの流れの例示的説明図である。
【図１０ａ】図１０ａは、本発明の別の実施形態におけるコンテンツ鍵の管理の例示的説明図である。
【図１０ｂ】図１０ｂは、図１０ａに示される状況でコンテンツが要求された時に発生するデータの流れの例示的説明図である。
【図１１】図１１は、コンテンツ要求の例示的説明図である。
【図１２】図１２は、承認段階を示すコンテンツ要求の例示的説明図である。
【図１３】図１３は、配信段階を示すコンテンツ要求の例示的説明図である。
【図１４】図１４は、透かしが使用される、本発明の別の例示的実施形態のライセンス構造の説明図である。
【図１５】図１５は、コンテンツに透かしを入れることを追加した、図１に示されるシステムで使用される通信プロトコルの説明図である。
【図１６】図１６は、３つのエンティティが通信に関係する場合におけるコンテンツを配布するために使用されるデバイスの例示的実施形態の概略図である。
【図１７】図１７は、図１６に示される周辺機器の１つの内部のハードウェアの概略図である。
【図１８】図１８は、４つのエンティティが電子商取引を行うための通信に関係する、本発明の例示的一実施形態のシステムの説明図である。
【図１９】図１９は、図１８に示されるシステムで使用される通信プロトコルの説明図である。
【図２０】図２０は、４つのエンティティが電子商取引を行うための通信に関係する、本発明の別の例示的実施形態のシステムの説明図である。
【図２１】図２１は、図２０に示されるシステムで使用される通信プロトコルの説明図である。
【図２２】図２２は、本発明の一実施形態によるブルート・フォース手法を説明する。

【図２３】図２３は、本発明の一実施形態により暗号化されるデータに含まれるデータのタイプを示す。
【図２４】図２４および２５は、本発明の一実施形態による、発見不可能データのセキュリティを保護する暗号化方式を示す。
【図２５】図２４および２５は、本発明の一実施形態による、発見不可能データのセキュリティを保護する暗号化方式を示す。

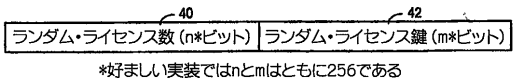
【図１】



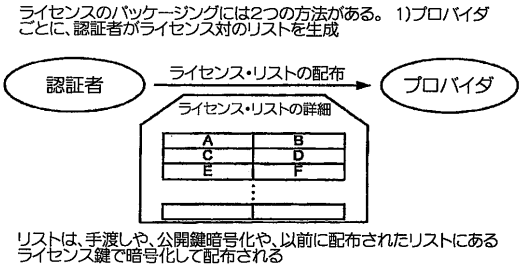
【図２】



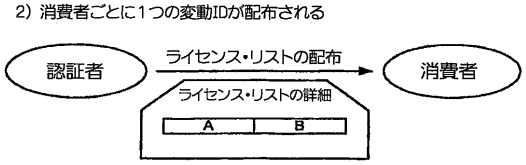
【図３ａ】



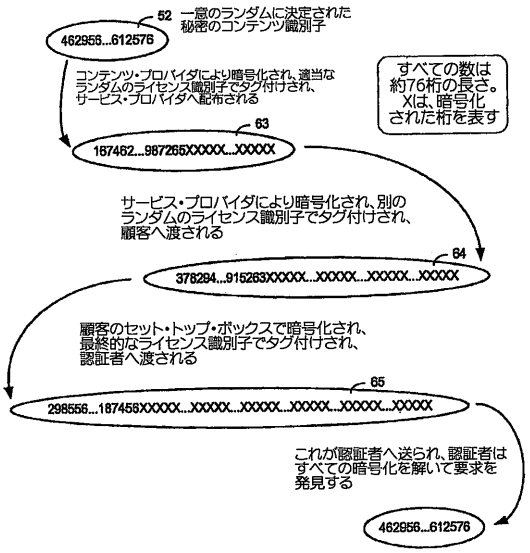
【図３ｂ】



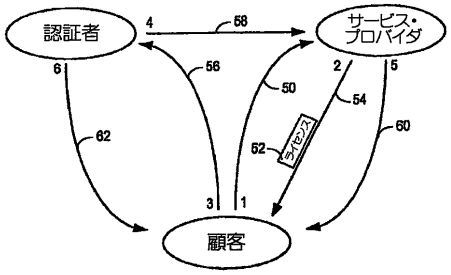
【図３ｃ】



【図４】

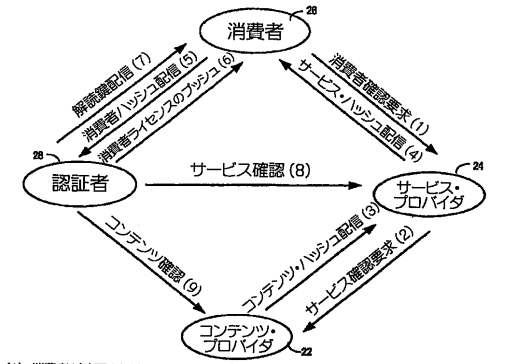


【図５】

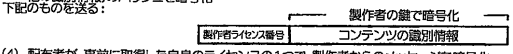


1 顧客が何らかのコンテンツを視聴する要求をサービス・プロバイダに対して行う
2 サービス・プロバイダが、コンテンツ・プロバイダから受け取られてサービス・プロバイダで暗号化された暗号化ライセンスを、顧客へ送る
3 顧客のセット・トップ・ボックスまたはデバイスが、そのライセンスを自身のライセンスで暗号化し、認証者へ送る
4 認証者がライセンスの有効性を確認し、有効である場合、認証者は、顧客がコンテンツに対する支払いに同意したことを、サービス・プロバイダに通知する
5 次いでコンテンツ・プロバイダが暗号化コンテンツを顧客へ送る
6 認証者が復号情報を送る

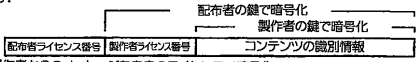
【図６】



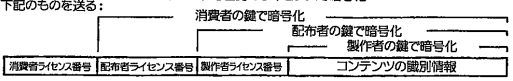
(1) 消費者が映画またはコンテンツの要求を行う
(2) 配布者またはサービス・プロバイダが要求を製作者またはコンテンツ・プロバイダへ中継
(3) 製作者が、事前に取得したライセンスの1つを使用してコンテンツの題名(または何らかの他の識別情報)のハッシュを暗号化
下記のものを送る：



(4) 配布者が、事前に取得した自身のライセンスの1つで、製作者からのメッセージを暗号化
下記のものを送る：

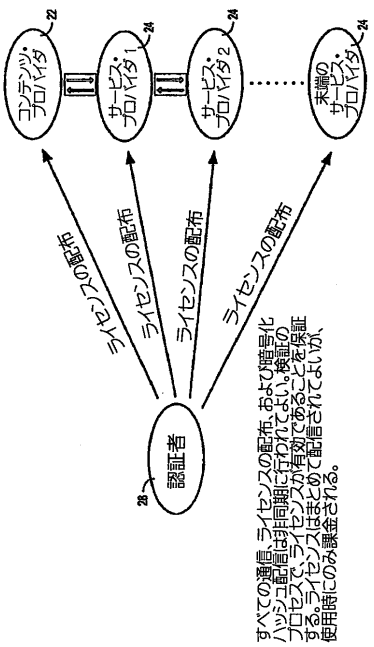


(5) 消費者が、製作者からのメッセージを自身のライセンスで暗号化
下記のものを送る：

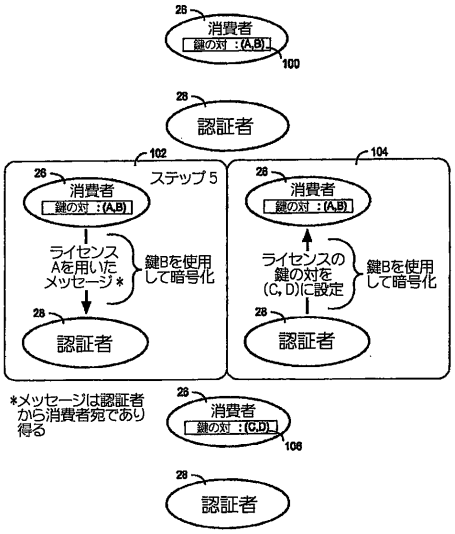


(6) 鍵マスタまたは認証者により新しいライセンスが消費者へ送られる
(7) 製作者が望む場合、製作者のライセンスが使用されたことが製作者に通知される。あるいは、認証者によりライセンスの使用が追跡されてもよい。
(8) ビデオまたはコンテンツの解読鍵が消費者へ配信される
(9) 配布者のライセンスが使用されたことが配布者に通知され(例えば課金のため)、暗号化された映画データまたはコンテンツの送信を開始するように通知される

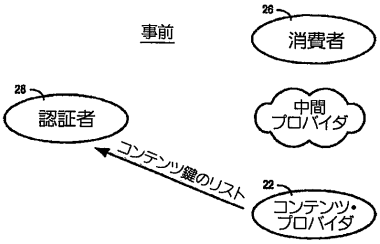
【図７】



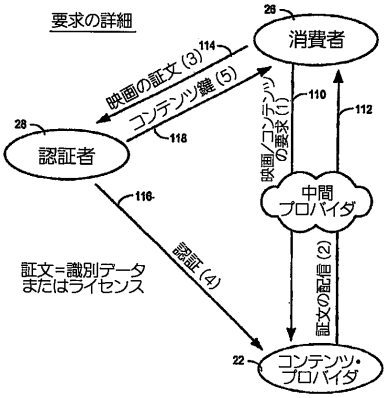
【図８】



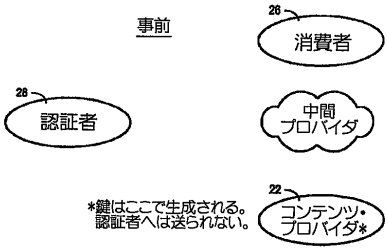
【図９ａ】



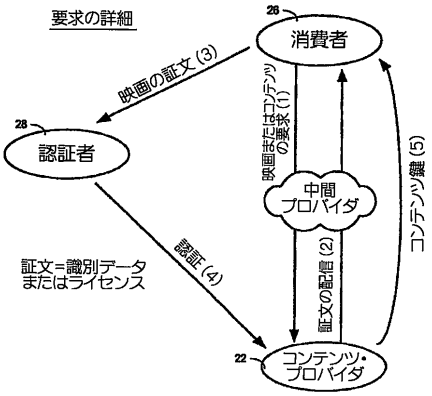
【図９ｂ】



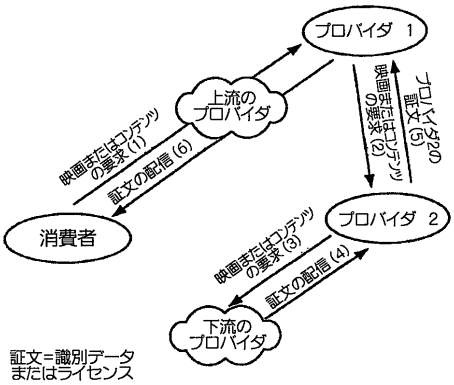
【図１０ａ】



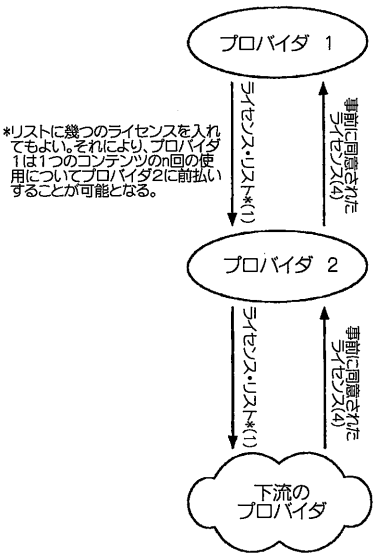
【図１０ｂ】



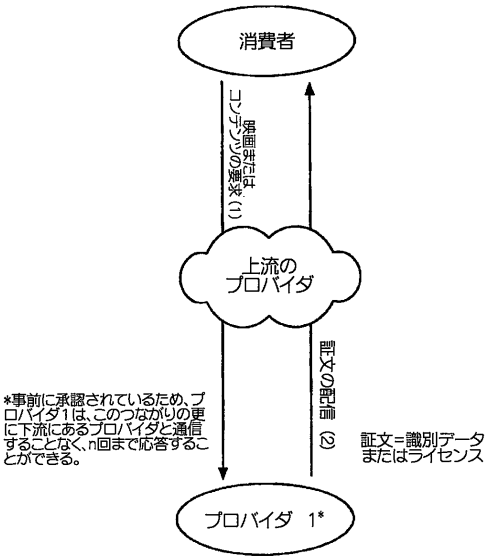
【図１１】



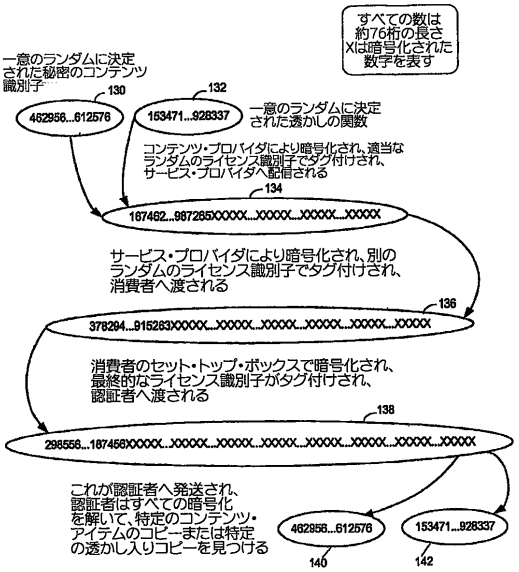
【図１２】



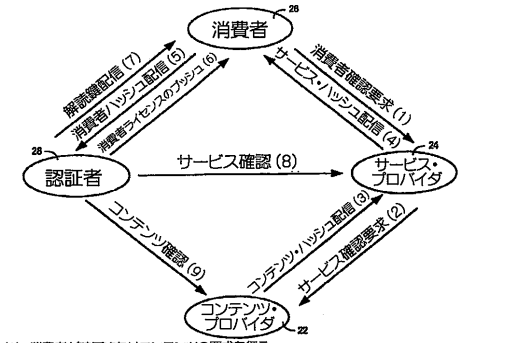
【図１３】



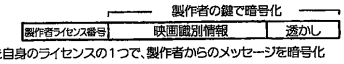
【図１４】



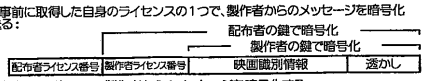
【図１５】



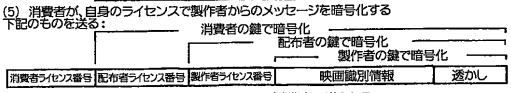
(1) 消費者が映画またはコンテンツの要求を行う
(2) 配布者またはサービス・プロバイダが要求を製作者またはコンテンツ・プロバイダへ中継
(3) 製作者またはコンテンツ・プロバイダが、事前に取得したライセンスの1つを使用して映画の題名(または他の識別情報)の関数と一意の透かしの関数とを暗号化
下記のものを送る：



(4) 配布者が、事前に取得した自身のライセンスの1つで、製作者からのメッセージを暗号化
下記のものを送る：

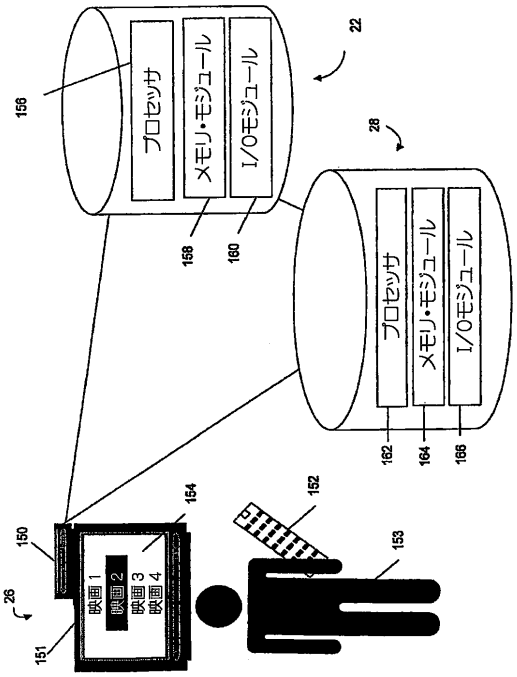


(5) 消費者が、自身のライセンスで製作者からのメッセージを暗号化する
下記のものを送る：

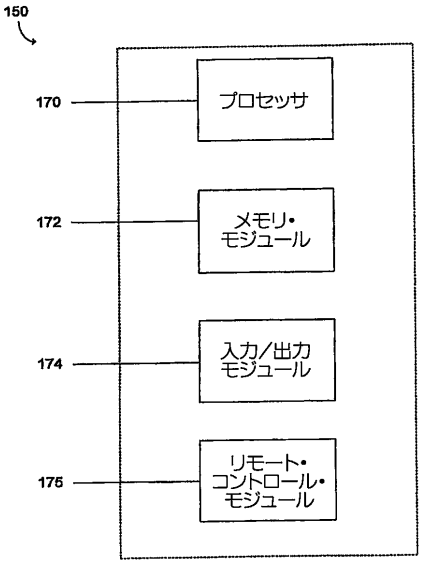


(6) 鍵マスタまたは認証者から新しいライセンスが消費者へ送られる
(7) 製作者が鍵む場合、製作者のライセンスが使用されたことが製作者に通知され、顧客を透かし入りのコンテンツ項目と結びつける。あるいは、鍵マスタにより ライセンスの使用が追跡されてもよい
(8) 透かし入りの映画またはコンテンツに対応する解読鍵が消費者へ配信される
(9) 配布者のライセンスが使用されたことが配布者に通知され(例えば課金のため)、対応する暗号化された透かし入りの映画またはコンテンツの送信を開始するように通知される

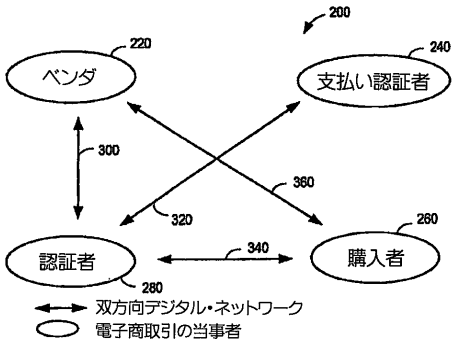
【図１６】



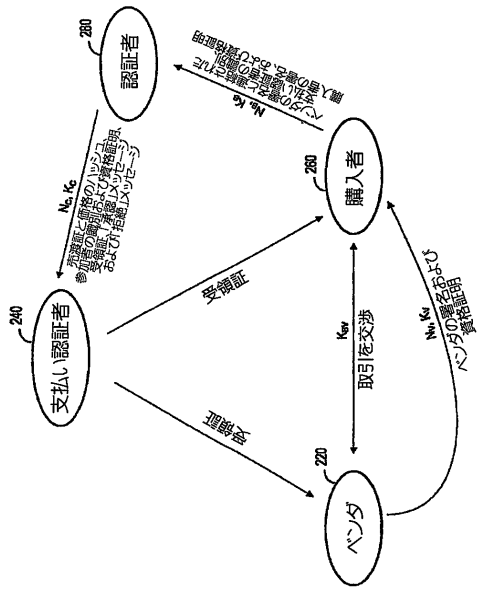
【図１７】



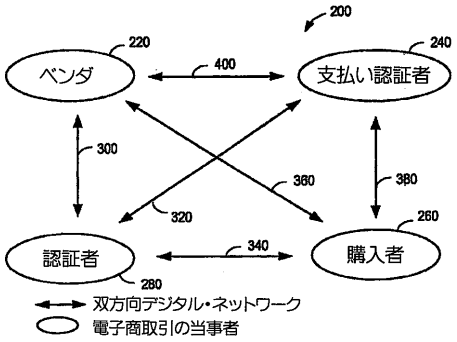
【図１８】



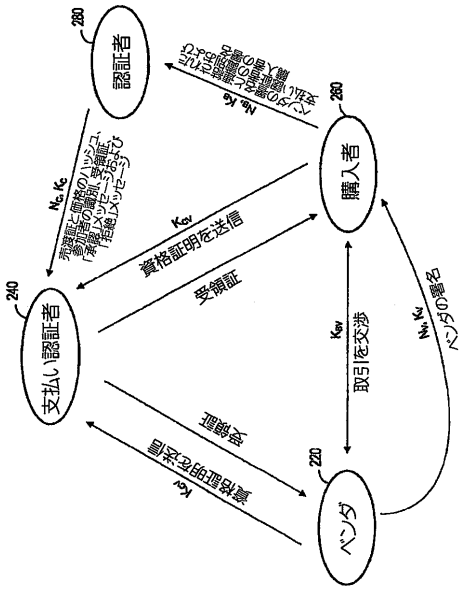
【図１９】



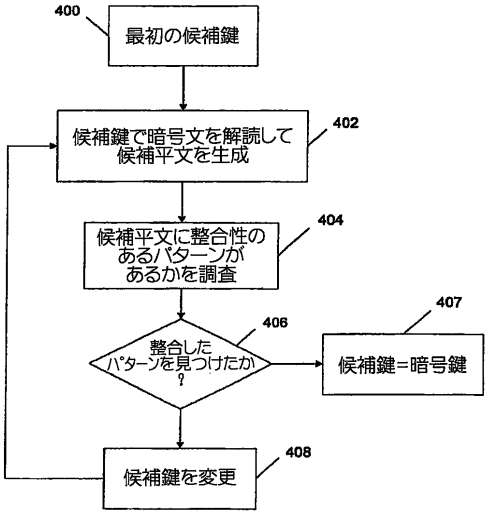
【図２０】



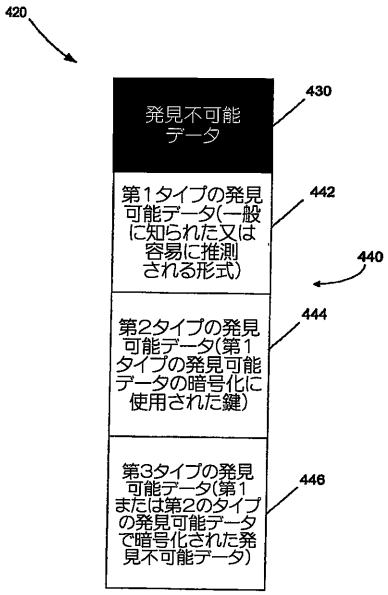
【図２１】



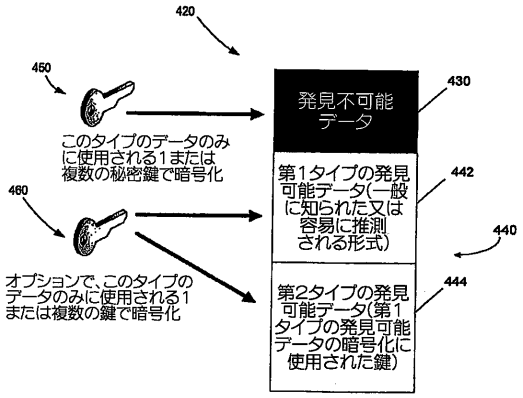
【図２２】



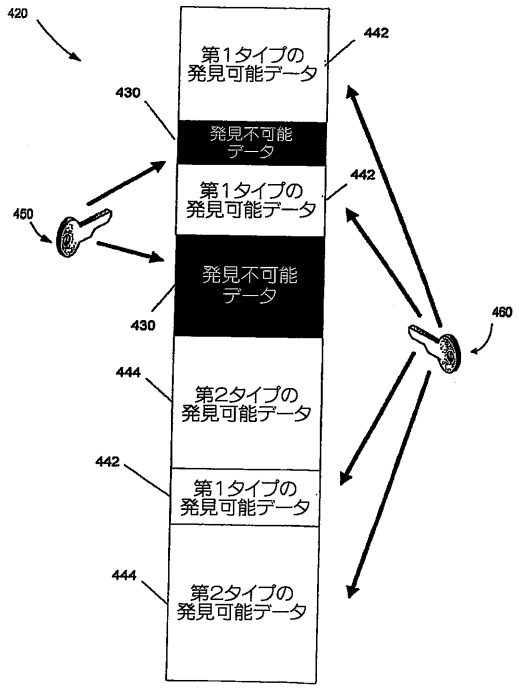
【図２３】



【図２４】



【図２５】


420
442
第1タイプの
発見可能データ
430
発見不可能
データ
442
第1タイプの
発見可能データ
450
発見不可能
データ
430
460
444
第2タイプの
発見可能データ
442
第1タイプの
発見可能データ
444
第2タイプの
発見可能データ

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 06/45110

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04K 1/00 (2008.01)
USPC - 705/57
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8): H04K 1/00 (2008.01)
USPC: 705/57

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/1, 50, 57, 75, 77; 713/150, 164, 168, 189

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Electronic databases: USPTO WEST (PGPB, USPT, EPAB, JPAB); Google Scholar
Search Terms Used: electronic commerce or e-commerce transaction or payment, mutating identifiers or IDs, user or consumer or customer identifier, merchant or vendor or retailer identifier, encrypting or decrypting data, authentication or keys etc.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/0010536 A1 (Cochran et al.) 13 January 2005 (13.01.2005) (abstract, and para [0007]-[0015], [0044]-[0056], [0072]-[0080], [0094]-[0103])	1-18 and 70-72
A	US 2004/0210449 A1 (Breck et al.) 21 October 2004 (21.10.2004)	1-18 and 70-72
A	US 6,675,153 B1 (Cook et al.) 06 January 2004 (06.01.2004)	1-18 and 70-72
A	US 2003/0187799 A1 (Sellars et al.) 02 October 2003 (02.10.2003)	1-18 and 70-72
A	US 2003/0126094 A1 (Fisher et al.) 03 July 2003 (03.07.2003)	1-18 and 70-72

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
11 February 2008 (11.02.2008)

Date of mailing of the international search report
28 MAR 2008

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer:
Lee W. Young
PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774
07.10.2008

Form PCT/ISA/210 (second sheet) (April 2007)

60800550017

2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 06/45110

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See Extra Sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
Group 1, claims 1-18 and 70-72

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

フロントページの続き

(51)Int.Cl.	F I		テーマコード（参考）
	Ｇ０６Ｆ 17/60	３３２	
	Ｇ０６Ｆ 17/60	５１２	

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(74)代理人 100096013
弁理士 富田 博行
(74)代理人 100096068
弁理士 大塚 住江
(72)発明者 セラーズ，ウィリアム
アメリカ合衆国ウィスコンシン州５３２１１，ミルウォーキー，ノース・ハケット・アベニュー ３４５２
(72)発明者 マリナ，リチャード
アメリカ合衆国ウィスコンシン州５３０９７，メコン，イースト・フィールド・サークル ７９１４
(72)発明者 コックラン，ウィリアム
アメリカ合衆国イリノイ州６１８２０，シャンペーン，ウエスト・ワシントン・ストリート ３０７

Ｆターム(参考) 5J104 AA15 AA16 EA17 EA18 EA26 PA07 PA10