(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6047553号
(P6047553)

(45)発行日　平成28年12月21日(2016.12.21)　(24)登録日　平成28年11月25日(2016.11.25)

(51)Int.Cl.		F I		
G06F 21/10	(2013.01)	G06F	21/10	
G06F 21/62	(2013.01)	G06F	21/62	309
G06F 21/60	(2013.01)	G06F	21/60	320
G06F 21/64	(2013.01)	G06F	21/64	

請求項の数 23　(全 32 頁)

(21)出願番号　特願2014-505260 (P2014-505260)
(86)(22)出願日　平成24年4月11日 (2012.4.11)
(65)公表番号　特表2014-512056 (P2014-512056A)
(43)公表日　平成26年5月19日 (2014.5.19)
(86)国際出願番号　PCT/US2012/033150
(87)国際公開番号　WO2012/142178
(87)国際公開日　平成24年10月18日 (2012.10.18)
審査請求日　平成27年4月9日 (2015.4.9)
(31)優先権主張番号　61/474,212
(32)優先日　平成23年4月11日 (2011.4.11)
(33)優先権主張国　米国(US)

(73)特許権者　397072765
インタートラスト　テクノロジーズ　コーポレイション
アメリカ合衆国，カリフォルニア　９４０８５，サニーベール，ステュアート　ドライブ　９２０
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100141162
弁理士　森　啓
(74)代理人　100141254
弁理士　榎原　正巳

最終頁に続く

(54)【発明の名称】情報セキュリティのためのシステムと方法

(57)【特許請求の範囲】
【請求項１】
プロセッサによりデジタル・リソースの使用を管理するための方法であって、
該プロセッサが、１つ以上の規則と、１つ以上の計算のセットとをデジタル・リソースと結びつけるステップを含み、
前記規則は、デジタル・リソースにアクセスするための１つ以上の条件に対応し、前記計算は、前記デジタル・リソースとは異なる、前記デジタル・リソースの特定のビューを提供するために、前記デジタル・リソース上で行われる、デジタル・リソースの使用を管理するための方法であり、
少なくとも１つの計算は、前記デジタル・リソースに適用されるとき、前記デジタル・リソースの制限されたビューを生成し、
前記デジタル・リソースの該制限されたビューからは、前記デジタル・リソースを再形成できず、
前記デジタル・リソースをおおい隠すために、少なくとも１つの計算が、ランダムまたは疑似ランダム情報を組み込む、方法。
【請求項２】
前記デジタル・リソースと結びついた少なくとも１つの計算が、前記デジタル・リソースに含まれる情報が所定のユーザに明かされる前に、前記計算を前記デジタル・リソースに適用することを要求することによって、前記情報への該ユーザのアクセスを制限するために、該ユーザと結びついている、請求項１に記載の方法。

【請求項３】
少なくとも１つの計算は、個々のユーザよりも、むしろユーザのセットと結びついている、請求項２に記載の方法。
【請求項４】
ビューが前記計算によって制限されるエンティティは、所与のレンダリング装置など、人間以外の主体である、請求項２に記載の方法。
【請求項５】
前記ユーザのセットは、前記計算が適用されるユーザを明示的にリストすることによって特定される、請求項３に記載の方法。
【請求項６】
前記ユーザのセットは、前記ユーザのセットに共通の属性が適用されるいかなるユーザに対しても前記計算が要求されるように、前記属性を提供することによって特定される、請求項３に記載の方法。
【請求項７】
計算された前記制限されたビューは、ユーザ、ユーザの組、または、計算が適用される他の主体、に依存する、請求項１に記載の方法。
【請求項８】
前記デジタル・リソースをおおい隠すのに用いられる疑似ランダム情報は、種情報の確定的セットに基づく、請求項１に記載の方法。
【請求項９】
前記疑似ランダム情報を生成するのに用いられる前記種情報の確定的セットは、同じ主体は、常に、デジタル・リソースの同じおおい隠されたビューを受信するように、所与の主体と結びついている、請求項８に記載の方法。
【請求項１０】
前記プロセッサが、計算の新しいセットを前記デジタル・リソースと結びつける要求を受信するステップをさらに含む請求項１に記載の方法。
【請求項１１】
前記プロセッサが、計算の新しいセットを前記デジタル・リソースと結びつける要求を承認するステップをさらに含む請求項１０に記載の方法。
【請求項１２】
プロセッサによりデジタル・リソースの使用を管理するための方法であって、
該プロセッサが、１つ以上の規則と、１つ以上の計算のセットとをデジタル・リソースと結びつけるステップを含み、
前記規則は、デジタル・リソースにアクセスするための１つ以上の条件に対応し、前記計算は、前記デジタル・リソースとは異なる、前記デジタル・リソースの特定のビューを提供するために、前記デジタル・リソース上で行われる、デジタル・リソースの使用を管理するための方法であり、
前記プロセッサが、計算を前記デジタル・リソースと結びつけるために暗号化手法を使用するステップをさらに含み、
結びつけは、デジタル・リソースの一意的表現と、前記計算を前記デジタル・リソースに結びつける前記計算の一意的表現との組合せから成るデジタル署名文書をつくることによってつくられる、方法。
【請求項１３】
前記デジタル・リソースの前記一意的表現は、一方向関数の適用の結果である、請求項１２に記載の方法。
【請求項１４】
前記一方向関数は、ＳＨＡ－１ハッシュ関数から成る、請求項１３に記載の方法。
【請求項１５】
前記デジタル・リソースの前記一意的表現は、前記デジタル・リソースと結びついた一意的識別子ある、請求項１２に記載の方法。

【請求項１６】
前記デジタル・リソースと結びついた一意的識別子は、高信頼第三者機関（ＴＴＰ）によって割り当てられたものである、請求項１５に記載の方法。
【請求項１７】
前記高信頼第三者機関は、前記一意的識別子と前記デジタル・リソースの両方、または前記デジタル・リソースの表現を含む文書にデジタル署名することによって、前記一意的識別子とデジタル・リソースの間で結びつけを行った、請求項１６に記載の方法。
【請求項１８】
前記デジタル・リソースに結びつけられる前記計算の前記一意的表現は、機械可読フォーマットで表された前記計算それ自体である、請求項１２に記載の方法。
【請求項１９】
前記デジタル・リソースに結びつけられる前記計算の前記一意的表現は、一方向関数を、前記計算の機械可読表現に適用した結果である、請求項１２に記載の方法。
【請求項２０】
前記デジタル・リソースに結びつけられる前記計算の前記一意的表現は、前記計算と結びついた一意的識別子である、請求項１２に記載の方法。
【請求項２１】
前記計算と結びついた前記一意的識別子は、高信頼第三者機関（ＴＴＰ）によって割り当てられたものである、請求項２０に記載の方法。
【請求項２２】
前記高信頼第三者機関は、前記一意的識別子と前記計算の両方、または前記計算の表現を含む文書にデジタル署名することによって、前記一意的識別子と前記計算との間の結びつけを行った、請求項２１に記載の方法。
【請求項２３】
前記計算の機械可読表現を、前記規則を前記デジタル・リソースに結びつけるのに用いられる同一セキュア・パッケージにパッケージすることによって、前記計算は、デジタル・リソースに暗号によって結びつけられる、請求項１２に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
［関連出願の相互参照］
本出願は、２０１１年４月１１日に出願された仮出願番号第６１／４７４２１２４号による優先度の利益を主張するものである。その内容の全体が、ここに、参照により組み込まれる。
【０００２】
情報コンテンツのセキュアな持続的管理を容易にするためにシステムと方法が提示される。このシステムと方法は、多くのコンポーネント、システム、および、その中で採用される方法と同様に、新規であることが認識される。
【背景技術】
【０００３】
デジタル権利管理（ＤＲＭ）システムは、持続的にリソースをそのリソースへのアクセスを管理するための規則のセットに結びつけるために、典型的には、暗号を使用する。多くの場合、保護すべきリソースは、例えば、電子ブック、オーディオ・ビジュアル・ストリーム、または、ビデオゲームなどデジタル・コンテンツの一部である。リソースにアクセスするために、ユーザに、実行すべき行為を示す必要があるかもしれない。それは、その特定の行為に対して、リソースを管理している規則の評価の引き金となる。その行為が規則の下で許されるならば、ＤＲＭシステムは、リソースへのアクセスを、当初パッケージされたままで提供する。当初パッケージされた形で（デコーディング、デコンプレッション、あるいは、リソースの使用において、事実上暗黙に必要な他の計算を最初に適用する必要があるかもしれないのであるが、）ユーザに提示されるので、この種のリソースは

、「静的」であるとみなすことができる。
【０００４】
いくつかのＤＲＭシステムは、アクセスのために一部のリソースを選択することができる。例えば、ＤＲＭ対応ビデオ・プレーヤーは、たとえ複数トラックが１つのファイルでエンコードされるとしても、単一のビデオトラックへのアクセスを提供することができる。規則評価エンジンは、典型的には、ユーザが、リソースのどのサブセットが、アクセスされるものなのかを特定することを可能にする。ビジネス・モデルに依存して、パッケージされたリソースの異なるビューを提供するいくつかの努力もまた行われた。例えば、ＤＲＭシステムを、ビデオ・アクセスに支払う価格に依存して、ビデオへの低解像度あるいは高解像度のアクセスを可能にするＭＰＥＧ－４　ＳＶＣエンコーディング・スキームと統合することが可能である。しかしながら、これらの両方のケースにおいて、そのリソースと、可能な全てのバリエーションは、それらを修正することができないように事前に計算され、デジタル署名される。
【０００５】
静的リソース（またはその部分）は、パッケージ器によってエンコードされたそのままで、ユーザに提示される。対照的に、導出リソースは、計算によって当初のリソースから計算されるリソースである（典型的には、ユーザへの提示の前に消費の時点で実行されるが、しかし、そうとは限らない）。
【発明の概要】
【０００６】
本願発明の詳しい説明が、以下で提供される。いくつかの実施形態が記述されるが、本願発明は、どの一つの実施形態にも限定されるものではなく、多くの選択肢、修正、および、等価物にわたるものであることが理解されるべきである。なお、本願発明の完全な理解を提供するために、多くの特定の詳細が以下の記載で述べられるが、いくつかの実施形態は、これらの詳細の一部もしくは全てなしも実施することができる。そのうえ、明快さの目的で、関連技術領域で知られている特定の技術的な資料は、本願発明を不必要におおい隠すことを避けるために詳述しなかった。
【０００７】
情報コンテンツのセキュアな持続的管理を容易にするためのシステムと方法が提示される。このシステムと方法は、多くのコンポーネント、システム、および、その中で採用される方法と同様に、新規であることが認識される。
【図面の簡単な説明】
【０００８】
本願発明は、添付の図面とともに以下の詳しい説明を参照することによって、容易に理解される。
【０００９】
【図１Ａ】図１Ａは、導出リソースを配布するための図解的なシステムを示す。
【００１０】
【図１Ｂ】図１Ｂは、導出リソースへのアクセスを提供するための図解的なシステムを示す。
【００１１】
【図２】図２は、１つの実施形態にしたがって、リソースに対して行われる計算の例を示す。
【００１２】
【図３】図３は、電子リソースを管理するための図解的なシステムを示す。
【００１３】
【図４】図４は、本願発明の実際的な実施形態に使用することができたシステムのより詳細な例を示す。
【発明を実施するための形態】
【００１４】

本願発明の詳しい説明が、以下で提供される。いくつかの実施形態が記述されるが、本願発明は、どの一つの実施形態にも限定されるものではなく、多くの選択肢、修正、および、等価物にわたるものであることが理解されるべきである。なお、本願発明の完全な理解を提供するために、多くの特定の詳細が以下の記載で述べられるが、いくつかの実施形態は、これらの詳細の一部もしくは全てなしも実施することができる。そのうえ、明快さの目的で、関連技術領域で知られている特定の技術的な資料は、本願発明を不必要におおい隠すことを避けるために詳述しなかった。

【００１５】

情報コンテンツのセキュアな持続的管理を容易にするためのシステムと方法が提示される。このシステムと方法は、多くのコンポーネント、システム、および、その中で採用される方法と同様に、新規であることが認識される。

【００１６】

デジタル権利管理（ＤＲＭ）システムは、持続的にリソースをそのリソースへのアクセスを管理するための規則のセットに結びつけるために、典型的には、暗号を使用する。多くの場合、保護すべきリソースは、例えば、電子ブック、オーディオ・ビジュアル・ストリーム、または、ビデオゲームなどデジタル・コンテンツの一部である。リソースにアクセスするために、ユーザに、実行すべき行為を示す必要があるかもしれない。それは、その特定の行為に対して、リソースを管理している規則の評価の引き金となる。その行為が規則の下で許されるならば、ＤＲＭシステムは、リソースへのアクセスを、当初パッケージされたままで提供する。当初パッケージされた形で（デコーディング、デコンプレッション、あるいは、リソースの使用において、事実上暗黙に必要な他の計算を最初に適用する必要があるかもしれないのであるが、）ユーザに提示されるので、この種のリソースは、「静的」であるとみなすことができる。

【００１７】

いくつかのＤＲＭシステムは、アクセスのために一部のリソースを選択することができる。例えば、ＤＲＭ対応ビデオ・プレーヤーは、たとえ複数トラックが１つのファイルでエンコードされるとしても、単一のビデオトラックへのアクセスを提供することができる。規則評価エンジンは、典型的には、ユーザが、リソースのどのサブセットが、アクセスされるものなのかを特定することを可能にする。ビジネス・モデルに依存して、パッケージされたリソースの異なるビューを提供するいくつかの努力もまた行われた。例えば、ＤＲＭシステムを、ビデオ・アクセスに支払う価格に依存して、ビデオへの低解像度あるいは高解像度のアクセスを可能にするＭＰＥＧ－４　ＳＶＣエンコーディング・スキームと統合することが可能である。しかしながら、これらの両方のケースにおいて、そのリソースと、可能な全てのバリエーションは、それらを修正することができないように事前に計算され、デジタル署名される。

【００１８】

静的リソース（またはその部分）は、パッケージ器によってエンコードされたそのままで、ユーザに提示される。対照的に、導出リソースは、計算によって当初のリソースから計算されるリソースである（典型的には、ユーザへの提示の前に消費の時点で実行されるが、しかし、そうとは限らない）。

【００１９】

好適な実施形態において、導出リソースを生成する計算は、当初のリソースの特定のビューを生成するために当初のリソースを操作するコンピュータ可読な命令として表される。いくつかの実施形態において、計算は、数学的な計算の使用を含むかもしれないけれども、ここで用いられる「計算」という用語は、それに制限されず、命令セット、手順、方法、または、当初のリソースの特定の提示を生成する他のメカニズム（例えば、当初のリソースにおける情報の全てを開示しないもの）を含むものである。例えば、当初のリソースが「名前－生年月日－身長」の３つのリストであるならば、計算の例は、生成アプリケーションに、「生年月日－身長」ペアのリストだけを示す（すなわち、「名前」データを表示から省略する）ように適切な方法で命令することである。計算の別の例は、表示のた

めの身長の中央値と平均身長を生成するために、当初のデータ・セットを操作する命令のセットである。

【００２０】

計算は、種々の方法で特定することができる。その例は、以下の一部もしくは全部を含むが、それらに限定されるものではない。

【００２１】

●それらは、当初のパッケージ器（リソースを最初に暗号化するエンティティ）によってパッケージングの時に関連づけすることができる。

【００２２】

●それらは、パッケージングの後に生成することができ、セキュアに、リソースと関連づけることができる。これらの事後の計算は、データのパッケージ器によって、または、いくつかの実施形態において、計算に、保護リソースを調べて欲しい第三者によって、つくることができる。

【００２３】

いくつかの実施形態において、リソースは、どんな関連計算がなくても、保護することができる。いくつかの実施形態において、ＤＲＭシステムは、その関連計算に従って、（例えば、パッケージされた、および／または、そのように識別されるリソース）導出リソースにアクセスするように設計されることがあり得た。そのような実施形態において、リソースと関連した計算がないならば、アクセスは、効果的に妨げられる。他の実施形態において、リソースは、関連規則によって禁止されない限り、デフォルトにより、アクセス可能であることができた。そのような実施形態において、リソースに関連する計算がないならば、リソースと関連した規則が、リソースへのアクセスを認可するために１つ以上の計算を持つことを要求しない限り、リソースは、（いかなる関連規則に従っても、）アクセス可能である。

【００２４】

リソースへのアクセスが、例えば、行為を実行する主体、規則評価の際の環境（例えば、計算の能力）の考慮、ＤＲＭシステムによって管理される状態変数（例えば、支払い状態）、リソースについてすでに明らかにされた情報の量、および／または、その他の要因に依存するような場合において、導出リソースは、特に有用である。これらの場合において、目的は、典型的には、おそらく、評価の際のコンテキストに基づいて、当初のリソースの導出部物へのアクセスを提供することである。

【００２５】

導出リソースは、静的リソースに比較して特に有用であるいくつかのプロパティを有することができる。そのようなプロパティは、以下のいくつか、あるいは、すべてであり得る。

【００２６】

［遅延バインディング］

【００２７】

生のリソースの必要とされる正確なビューは、前もって計算される必要はなく、パッケージ器は、導出リソースを生成する計算を結びつけることができる。新たなタイプの計算されたリソースが重要になると、データのパッケージ器は、再計算、再パッケージ、当初のリソース全体（大きなデータ・セットであり得る）の再送信ではなく、むしろ、単に、規則と計算の新しいセットを提供することができる。

【００２８】

例えば、当初のリソースが、人間のゲノム情報シーケンスであるとする。リソースは、ゲノムに関する特定の限られた情報を明らかにするいくつかの計算により暗号化し、パッケージすることができる。主体が、男性であるか、女性であるか、主体が、ＢＲＣＡ２遺伝子の特定の突然変異を有するか、などである。後日において、データの所有者は、例えば、ＣＣＬ３遺伝子のパーツ数など、そのシーケンスの新しい態様にアクセスを提供することが重要であることを決定する。それは、ＨＩＶの危険性に関連がある。パッケージ器

は、新たな計算をつくり、それを当初のリソースに結びつけ、それを利害関係者に配布する。パッケージ器は、事前にこの計算を知っていることも、そのデータへの無制限のアクセスを提供することも必要ない。

【００２９】

［第三者計算］

【００３０】

計算は、パッケージ情報のユーザによって提案されることができ、次に、例えば、そうする権利を有する当初のパッケージ器や別のエンティティによって、セキュアにリソースと結びつけられることができる。

【００３１】

人間のゲノム情報シーケンスの例を続け、そのシーケンスが暗号化されて、自分の研究にそのシーケンスに関する情報を組み込むことを望む研究者に送られるとする。当初のパッケージの一部として、その研究者は、データの種々のビューを提供する計算のセットを受信する。その研究者は、特定の病気の危険性を推定するためにいくつかの遺伝子からの情報を結合する新たなアルゴリズムを発見した。しかし、データの所有者によって提供された計算を使用して、彼が、必要とする情報の全てを得ることができるというわけではない。その研究者は、そのシーケンスに対して動作するとき、彼の推定を生成する計算をつくる。彼は、所有者にこの計算を送る。所有者が同意すると仮定すると、新たな計算は、セキュアにリソースと結びつけられ、彼がそのシーケンスに対して計算を走らせるのを許す形でその研究者に送り返される。

【００３２】

類似した例は、ゲノム情報シーケンスを分析することによって特定の薬の適切な投与を推定するために、製薬会社によってつくられる計算である。この種の投与感度分析は、しばしば、抗凝固剤、ワルファリンを処方するために実行される。ＣＹＰ２Ｃ９とＶＫＯＲＣ１遺伝子の特定の変異体を持つ患者は、この薬に多少なりとも敏感である可能性がある。導出リソースにより、以前に格納され、更なる生物実験なしに保護された（例えば、出生時において）ゲノム情報シーケンスの上でこの感受性テストを走らせることができる。

【００３３】

［計算の構成］

【００３４】

第三者の計算が、リソースにバインドされるべきであると決定するとき、パッケージ器は、計算を進行させることを望むかもしれない、しかし、導出リソースを生成する計算のフローに、独自の前提条件または事後条件を追加することができる。

【００３５】

例えば、管理されたリソースが、アドレス情報をともなう所与の（大きな）領域のマップであるとする。第三者は、アドレスを与えられると、そのアドレスに結びついた空間座標を返す計算を提案する。パッケージ器は、この計算をよろこんで受け入れることがあり得るが、一般的には、しかしながら、正確な座標を開示することを望まない。そのかわりに、その計算が都市だけ、または、その近郊等を返すのを好む、次に、所有者／パッケージ器は、第三者によって提案される計算の出力を消費し、より多くの詳細をおおい隠すために、それを修正する第２の計算をつくる。第三者の計算をリソースにバインドするとき、その出力を要求者に返すことができる前に、自身の第２の計算が適用されることを要求する。

【００３６】

いくつかの実施形態において、計算は、いつ、誰によって、どのような状況で、そのリソースが導出されたのかに関する情報を含んでいる監査レコードを策定し、送るリソースと結びついていることができた。

【００３７】

図１Ａは、いくつかの実施形態にしたがうデジタル・リソース１５２を管理するためのシステム例１５０を示す。図１Ａで示すように、デジタル・リソース１５２（例えば、科

学研究データ、ヘルスケア記録、遺伝情報、メディア・コンテンツ、および／または、その他）は、第１のエンティティ１５１（例えば、デジタル・リソース１５２の所有者またはディストリビュータ、または、その代理をしているエンティティ）によって計算１５４と規則１５６とのセットと共にパッケージされる。例えば、リソース１５２は、暗号化され、デジタル署名され、および／または、さもなければ保護され、セキュアに、計算１５４と規則１５６とに結びつけられることができる。リソース１５２は、計算１５４や規則１５６と共に、遠隔エンティティ１５８に、いかなる適切な通信メディア（例えば、インターネットのようなコンピュータ・ネットワーク、移動通信ネットワーク、等）を介してでも、配布することができる。代替的に、または、追加的に、リソース１５２は、計算１５４や規則１５６とは独立に、遠隔エンティティ１６０に配布することができる。別のエンティティ１６２は、第１のエンティティ１５１に、リソース１５２に関係しているさらなる計算１６６を提案することができる。第１のエンティティは、計算１６６をリソース１５２にセキュアに結びつけることができ（例えば、エンティティ１６２によって提案される形で、または、修正された形で、または、計算１６６で実行されることを要求される更なる事前または事後計算で、または、その他）、リソース１５２に関連した使用のためにそのような計算１６６’を配布する（または、配布に使用可能にする）。

【００３８】

［プライバシー維持計算］

【００３９】

上述の例におけるように、導出リソースは、当初のデータのプライバシーを維持するのを助けるのに用いることができる。いくつかの実施形態において、いくつかの要因は、リソースにバインドされる場合がある計算のタイプを決定するのを助けることができる。例えば、リソースにバインドされた計算の既知の履歴は、開示が望ましい量だけ起こることを確実にするために分析することができる。例えば、パッケージ器は、一緒に使用されるとき、さもなければ、意図したよりも多くの情報を明らかにするかもしれない計算を発行したかもしれない。したがって、例えば、パッケージ器は、連続した計算によって明らかにされるデータの解像度を次第に減少させることに決めることができる。この目的のために、パッケージ器は、また、リソースの上での種々の計算の実行の際に要求された監査レコードを考慮することも望むことができる。

【００４０】

いくつかの実施形態において、少なくとも部分的に、データのプライバシー／秘密を保護するために、計算はランダム化することができる。例えば、計算は、出力の前にリソースにランダムノイズを追加することによって匿名化することができる。敵対者がその計算を複数回実行するかもしれず、返された導出リソースの統計（例えば平均値）を評価かもしれないけれども、いくつかの実施形態において、パッケージ器は、例えば、そのような要求の数を制限すること、ますます多くの要求がなされると統計を変えること、同じ主体が、計算（それによって統計的攻撃を防止する）の各々のアプリケーション、および／または、その他に際して、同じランダム化されたデータを得るように、状態変数（例えば、乱数の種）を覚えていること、により、この攻撃をやわらげることができる。

【００４１】

［異なる主体に対する異なるビュー］

【００４２】

いくつかの実施形態において、計算は、情報にアクセスしている主体などの条件に依存することができる。そのような実施形態において、パッケージされたリソースの異なる利害関係者は、異なるビューを得ることができる。異なる計算は、異なる主体と関係している場合がある。この能力は、全体的なリソースへのアクセスをゲートする規則において、特定の主体を特定する能力と相互作用する。規則のそのセットは、所与の主体が、すこしでも、リソースにアクセスする機会を有するか否かを述べることができる。したがって、それは、導出リソースがそもそも計算されるかどうかを決定する。しかしながら、それが動作する場合には、要求をしている主体、あるいは、主体の属性（例えば、所与のクラス

のメンバーシップ）に依存して、計算は、異なる導出を生成することに決めることができる。

【００４３】

この技術を用いて、例えば、病院のすべての医者がアクセスすることができる保護された健康記録をつくることができた。しかし、それは、患者の主治医がアクセスしたときには、追加的な詳細を含む。導出リソースのアプローチは、異なる主体に対して複数のパッケージを必要とすることと対照的に、管理されたリソースが、単一のパッケージのままであることを可能にする。

【００４４】

［異なるコンテキストにおける異なるビュー］

【００４５】

ちょうど、いくつかの実施形態において、リソースのビューは、リソースへのアクセスを要求している主体に依存することができ、そして、そのビューは、計算が実行されるポイントに存在する他のコンテキスト情報に依存することができる。

【００４６】

例えば、コンテンツを管理している規則のセットは、所与のユーザに登録されたいかなる装置へのアクセスをも許すことができる。しかし、計算は、装置の特定のタイプに対して所与解像度でリソースを出力することができる。または、特定の抜粋だけを、装置の特定のタイプの上で示すことができる。一方、完全な解像度は、他のデバイス・タイプで利用可能である。

【００４７】

［データ忠実性の保存］

【００４８】

例えば、プライバシーを維持するために、ユーザに提示されるデータの正確さ、または、忠実度は減少する等の、いくつかの例が与えられたけれども、いくつかの実施形態において、導出リソースを生成する計算は、必ずしも損失性ではないことが認識される。すなわち、計算は、導出リソースを生成するプロセスにおいて、当初情報から何も取り除く必要はない。導出リソースを使用して、当初のデータは、繰り返しフィルタリングされる必要がなく、再パッケージされる必要もない。したがって、情報は失われず、将来において役に立つ場合がある。

【００４９】

例えば、リソースは、所与の患者に対する（加速度計によって記録される）一連の活動レベルであるとする。一般に、理学療法士は、平均の日常活動レベルに興味を持っているだけかもしれないので、リソースは、これらの平均を生成する計算のセットを伴って来るかもしれない。それらの平均を提供する１つのアプローチは、当初のリソースをとりあげて、平均を実行し、そして、別のリソースとして。平均のシーケンスを保護することである。しかしながら、このアプローチは、例えば、所与の運動セッションの強度を決定するために、高解像度のデータに戻る能力を提供しない。もしも、その代わりに、導出リソース・アプローチの好適な実施形態に従って平均が実行されるならば、新たな計算は、フィルタリングされ、再パッケージされた活動データから得ることができなかった情報を提供することができる。当初の生データは、まだ、そのような新たな計算による使用が可能であるからである。

【００５０】

［監査能力］

【００５１】

いくつかの実施形態において、レンダリングの条件として実行される計算は、リソースの当初のパッケージ器が、特定の計算の結果を確認し、頼ることができる、または、それらが事前に同意されたセマンティックを使用して説明的に表されることができるように、標準化されたマシンで、表すことができる。

【００５２】

いくつかの実施形態において、パッケージ器が計算をリソースに結びつけるとき、計算は、（特に、それが第三者によって生成される場合）最初に確認される。一般に、計算の機能性の自動評価は、難しく、計算のフレームワークが、より表現力豊かであれば、より難しいものとなる。したがって、パッケージ器は、計算を記述するメタデータを調べ、それを承認する前にテスト環境で計算を走らせる、提案された計算が高信頼第三者機関によって署名されたかどうかを検証し、提案者のアイデンティティを認証すること、および／または、その他のような、種々の発見的方法に頼ることができる。一様な計算のフレームワークは、例えば、計算が表される特定の言語は、パッケージ器が、提案された計算を確認することの助けとなる。

【００５３】

［複数のサブ・リソースを管理する計算］

【００５４】

導出リソース・アプローチで管理することができるリソースの１つのタイプは、１つ以上のキーで保護されているデータベースを有する、サブ・リソースの全データベースである場合がある。この定式化において、リソースに対する計算を実行することは、データベースに問い合わせることと類似している。パッケージ器は、計算を拘束することによってリソース上で実行することができる問合せの種類を制限することができる。

【００５５】

例えば、管理されたリソースは、完全な遺伝子配列のセットと、特定の人口の健康記録とであるとする。結びついた計算は、ユーザが、例えば、人口における何人の女性ＢＲＣＡ１遺伝子を表すかを決定するリソースを問い合わせるのを可能にする。または、この遺伝子に対して、１８歳から４５歳の年齢の女性のどれだけが、符号化されているか、などである。この例において、データ・リソースと、その上で動作する計算との組合せは、ユーザが、そのデータを探索するのを可能にする。この例において、そのデータ・セット上で実行することができる計算のタイプは、当初のパッケージ器によって定義されることができ、パッケージ器は、将来必要に応じて更なる計算を追加することができる。例えば、ある特定の相関関係が仮定されるならば、パッケージ器は、他のユーザが当初のデータ・セットでその相関関係を探索するのを可能にする計算のセットを提供することができる。静的リソースでは、パッケージングの前に、データが減らされ、情報が失われる。導出リソースでは、必要に応じて将来与えられる更なるアクセスを有する完全なデータ・セットを保存することができる。

【００５６】

［計算のバインディングの委任］

【００５７】

いくつかの実施形態において、リソースの発信者または作者は、リソースと計算の間のすべてのバインディングを実行することを必ずしも要求されない。例えば、発信者は、計算のバインディングを、例えば、一組のリソースを単一の論理的リソースとして管理するように設計されたデータベースなど第三者に委任することができる。

【００５８】

例えば、遺伝子のシーケンス・マシンは、オンラインのサーバとの信頼されたチャネルを確立し、シーケンス情報をそこへアップロードすることができる。このように、どの種類の計算が、将来、そのシーケンスの上で動くことができるかを決定する能力をサービスに委任する。

【００５９】

［導出リソースを返すこと］

【００６０】

いくつかの実施形態において、導出リソースを、別の導出リソースの上での計算の実行の結果として、返すことができる。

【００６１】

例えば、当初のリソースは、サブ・リソースの管理されたセットを含むことができる。

結びついた計算が、特定のサブ・リソースについて、情報を抽出するためにリソースの上で実行されるとき、その計算は、結果として、その下位リソースに質問するために下位リソースと計算のセットとを含む第２の導出リソースの生成となることができる。

【００６２】

［計算の場所］

【００６３】

好適な実施形態において、管理されたリソースと関連した計算は、保護された処理環境で実行される。いくつかの実施形態において、この保護された処理環境の場所の論理的制約はない。いくつかの実施形態において、リソースの所有者／パッケージ器は、種々の消費エンティティが処理するために、バーチャルなセキュア・パッケージを世界に送り出す。計算（ならびに規則評価）は、消費者サイトにおいて保護された処理環境で起こる。そのようなシナリオの例が、図１Ｂに示される。それは、本願発明の１つの実施形態に従って、導出リソースを管理する図解的なシステムを示す。図１Ｂで示すように、バーチャルなセキュア・パッケージ１０２は、規則１０４、計算１０６、キー１０８、および、当初のリソース１１０を含む。バーチャルなセキュア・パッケージ１０２は、導出リソース１１４を生み出すために、安全なコンピューティング環境１１２によって、その規則にしたがって処理される。図１Ｂに示されるバーチャルなセキュア・パッケージ１０２の周囲の破線は、示された（１０４、１０６、１０８と１１０）の４つのサブ・コンポーネントを一緒に、または、別々に配布することができが、しかし、例えば、暗号手法を使用して互いに持続的に結びついていることを示すことを意味するものである。図１Ｂに示されるコンテキスト情報１１６は、例えば、リソース導出が実行されている環境からの情報を含むことができる。それは、例えば、システムのユーザから集めた情報を含むことができる。図１Ｂに示される意図情報１１８は、例えば、ユーザがそのデータからつくることを望む使用を特定することができ、少なくとも部分的に、どの規則１０４と計算１０６が評価されなければならないかを決定するのに用いることができる。

【００６４】

説明の目的のために図１Ｂが提示され、多くの他の実行可能なものがあることが認識される。例えば、リソースの所有者／パッケージ器は、それ自身の保護された処理環境において、計算の一部もしくは全部を実行することができ、例えば、例えば認証されたアイデンティティなど要求者の特定の属性に基づいて、要求者に戻すことができる。代替的に（あるいは、追加的に）、リソースの上の計算は、リソース発信者が、これらの計算を加えるか、実行する権限を委任した代理人によって行われることができる。

【００６５】

［遠隔リソースに対するコンピューティング］

【００６６】

計算の場所に関して記述された技術で上に記載された第三者の計算テクニックを結合することによって、遠隔リソースに対して動作する計算を提案することが可能になる。１つのそのような実施形態において、リソースの所有者は、提案された計算を認証し、確認し、そして、それ自身のリソースに対して計算を実行し、要求者に結果を返すために必要なステップを決定することができた。そのような構成の１つの例が、図２に図示される。

【００６７】

いくつかの実施形態において、計算とリソースと間の論理的バインディングが、例えば、以下を含む１つ以上の方法で起こりえる。

【００６８】

名称により：

計算は、それが動作するリソースを特定するメタデータを伴う。

【００６９】

属性により：

計算は、動作するリソースに当てはまる属性のセットとともに送られる。例えば、要求者は、受取人が、計算が動作するリソースのセットを決定するために使用する問合せスト

リングを送ることができる。

【００７０】

図２は、リソースに対して動作する計算をどのように提案することができるかの例を示す、ユーザ２０２は、リソースに関する要求をして、認証者Ａ２０４によって認証される。計算２０８を含むセキュア・パッケージ２０６は、評価器システム２１０に送信される。それは、評価器２１０によって検証され、認証される。ポリシーＰ２１４により、リソースＲ２１２対して動作する。結果２１６が、おそらく、一連の仲介者を通してユーザ２０２に返される。

【００７１】

ここに記述されるシステムと方法は、実質的にコンテンツのいかなるタイプ、下に含まれるいくつかの非限定的な例にも適用することができることが認識される。

【００７２】

［導出リソースの例］

【００７３】

スケーラブル・ビデオいくつかの実施形態において、事前計算された解像度の種々のレベルへのアクセスは、支払った額に基づいて与えられる上述のＳＶＣ（「スケーラブル・ビデオ符号化」）メディア例は、単一の高解像度のビデオ・リソースと計算のセットとの組合せによって置き換えることができる。それらの、各々が、独自の規則によって管理される。例えば、ユーザは、特定の条件が合致し、リソースが最初に、特定された計算によってフィルタリングされた提供されるビデオの低解像度のバージョンにアクセスするかもしれない。解像度の各々のレベルは、レンダリングのために適切な信号を生成する特定の計算と結びついていることができた。

【００７４】

フィルタ処理した健康データ：いくつかの実施形態において、一連の健康関連の測定（例えば、最後の数ヵ月の間、毎秒測定されるパルスレート）から成るデータ・シリーズを与えられると、異なる主体は、異なるデータ解像度にアクセスを与えられることができる。患者自身は、フル解像度で全てのデータ・シリーズにアクセスすることができるが、一方、彼の医者は、より粗いビュー、最近の２週間の、安静時および運動時の平均パルスなど、にアクセスすることができる。このケースにおいて、医者は、さらに、個人情報にアクセスすることができるが、完全に無関係な第三者（例えば、伝染病学者または研究者）は、完全に、または、部分的に匿名化されたデータだけにアクセスできる。データの低解像度化を実行する計算は、当初のデータ・リソースとともにパッケージすることができる。このケースにおいて、そのデータ・シリーズへのアクセスを管理している規則は、異なる主体または役割と結びつけることができる。

【００７５】

仮想ワールドいくつかの実施形態において、当初のリソースは、十分に強力なレンダリングエンジンが、空間の３次元対話型モデルを生成することができる十分な詳細にエンコードされた仮想空間の記述から成るゲームでありえる。例えば、仮想空間の１つの領域は、ゲームにおいて特定のレベルを達成したユーザだけに利用可能であるかもしれない。リソースを管理している規則は、ビューの計算、またはビューを生成するために必須である計算を実行する。

【００７６】

普遍的デコーディングいくつかの実施形態において、当初のリソースは、特定の独自のフォーマットでエンコードされたインタラクティブ・オーディオビジュアル表現から成ることができる。リソースをレンダリングすることに結びついた計算は、それがターゲット・プラットホームの上でレンダリングされるのを可能とする方法で、当初のリソースをデコードするデータに対するフル・デコーダを含むことができた。

【００７７】

遺伝情報の管理：いくつかの実施形態において、管理されたリソースは、上で述べたように、例えば、完全な遺伝子配列のセット、特定の人口の健康測定値等であることができ

た。
【００７８】
科学研究：
科学研究において、まだそれが保護されていることが保障されている間に、最大限にデータを利用可能に、検証可能にすることは、しばしば重要である。著名な科学的出版物は、公表された研究において、結論を出したデータは、それを検証することができるように、他の科学者が利用できることを確実にするのを典型的には好む。そのデータを処理するのに用いられたアルゴリズムは、ピア・レビューにも使えなければならない。同時に、データは、不正操作に影響されやすくてはいけない。このように、いくつかの実施形態において、データは、そのデータ・セット上で実行することができる特定の計算を特定している規則を有する保護された形で発表されることができる。この取り決めは、開放性／公表性と完全性保護のニーズを同時に満たす。
【００７９】
広告ロードの交渉：
別の例において、メディア（例えば、ビデオまたはオーディオ）ストリームは、広告によって部分的に資金を供給されるかもしれない。この例において、リソースは、メインプログラムと、特定の位置において、メインプログラム・ストリームに挿入される一組の広告を含むことができる。リソースがアクセスされるときに返された導出リソースは、例えば、例えば、コンテンツ・リソースを要求している主体、その主体の属性、および／または、レンダリングのポイントでのコンテキストに基づいた、これら特定の数の広告を含むことができる。例えば、主体が、所与のプログラムにおいて、広告の所与のセットをすでに見たならば、計算は、代替のセットに置き換えることができる。視聴者が購読申込の料金を払ったならば、計算は、広告を全部除くことができる。
【００８０】
クーポン価値の交渉別の例は、上述の広告例でのバリエーションである。しかしながら、この例で返されるリソースは、メディア・ストリームではなく、デジタル・クーポンである。クーポンの額面は、計算とユーザとの間での相互作用によって決定することができる。ユーザが当初のリソースの一部として含まれる広告を見る気があるならば、ユーザは、クーポンのより良い償還価値を得る。
【００８１】
以前に、図１Ｂに関連して示されたように、いくつかの実施形態において、バーチャルなセキュア・パッケージ１０２の要素は、互いに結び付けられている。図１Ｂで示すように、これらの要素は、当初のリソース１１０、リソースを暗号化および／または復号化するのに用いられる１つ以上のキー１０８、当初のリソース、および、当初リソースおよび／または導出リソースへのアクセスを管理する１つ以上の規則１０４のセットに基づいて、導出リソースを生成する一組の１つ以上の計算１０６含むことができる。
【００８２】
いくつかの実施形態において、バインディングは、これらの要素を単一のパッケージに一緒にパッケージすることを含むことができる。しかし、それは、また、そらが別々に配布されるときでも、これらの要素を結びつけるために暗号（または他の計算）技術を適用することを含むこともできる。いくつかの要因を、計算がリソースに結びつけるべきか否かを決定するためにパッケージ器によって使用することができる。これらは、例えば、計算をつくった団体の認証、その団体の属性（例えば、信頼できるグループのメンバーシップ）、計算と関連したメタデータの検査、テスト環境において計算を走らせた結果等を含むかもしれない。
【００８３】
いくつかの実施形態において、計算は、下記のように、異なる強さで結び付けられることができる。
【００８４】
［強いバインディング］

【００８５】
強いバインディングの例において、計算、規則、リソース、および、キーは、バーチャルなセキュア・パッケージに暗号によって結びついている。リソースに計算を結び付けるのに用いることができる１つのメカニズムは、全体的なリソースへのアクセスをゲートする規則として、その計算を同じパッケージに含むようになっている。ユーザは、これらの規則のどれを評価するべきかについて選ぶことができる。そして、条件が合う場合には、結びついた計算が、それが返される前に、リソースに適用される。いかなる適切なメカニズムはも、リソースに規則を結び付けるのに用いることができることが認識される。例えば、いくつかの実施形態において、同一出願人により出願中の、２００６年１０月１８日に出願された米国特許出願第１１／５８３６９３（米国特許出願公開第２００７／０１８０５１９号明細書）（「ｅ６９３出願」）で記述されたバインディング技術を、使用することができる。
【００８６】
いくつかの実施形態において、バインディングは、計算をリソースにセキュアに結びつける別々のバインディング・オブジェクトを使用して達成することができる。そのバインディング・オブジェクトは、例えば、リソースのハッシュ、リソースＩＤ、リソースを暗号化するキーへの参照、および／または、その他結び付けられているリソースをユニークに識別するいくつかの情報を含むことができる。このバインディング・オブジェクトは、また、計算そのもの、または、例えば計算のプログラムのハッシュなど計算へのレファレンス、一意的識別子等を含むことができる。バインディング・オブジェクトは、バインディングの完全性保護を備え、評価の際にバインディングをつくった、その団体を認証するために、それ自身が署名されることができる。
【００８７】
このアプローチを使用して、計算は、規則、リソース、および、キーから、離れて進むことができる。しかし、論理的に、安全なバーチャルなパッケージの内に留まる。いくつかの実施形態において、事前または事後計算として使用される他のバインディング・オブジェクトへポイントするバインディング・オブジェクトの使用を通して、計算は、チェーンする（成り立つ）ことができる。また、バインディング・オブジェクト・アプローチでは、先験的に、リソースと計算との間で結びつけをつくることは必要でない。計算は、あとで結び付けることができ、いくつかの実施形態において、それらは、他の団体が提案することができる。
【００８８】
［弱いバインディング］
【００８９】
いくつかの実施形態において、比較的弱いバインディングを、例えば、暗号を使用するのではなく、むしろ名前または属性によって計算を識別することに基づいて、代わりに用いることができる。
【００９０】
図１Ｂで示すように、好適な実施形態において、セキュアなコンピューティング環境が、規則を評価して、当初のリソースの上で計算を適用するのに使用される。いくつかの実施形態において、セキュアなコンピューティング環境は、以下のプロパティの一部もしくは全部を有する。
【００９１】
●それは、セキュア・パッケージにおいて要素のソースが信頼できるかどうかを検証する。いくつかの実施形態において、それは、既知あるいは信頼できるソースであるバーチャルなセキュア・パッケージと、そうではないものとを区別する能力を有する。後者の場合、セキュアなコンピューティング環境は、規則を評価こと、あるいは、リソース導出を実行することを避けることができる。
【００９２】
●それは、コンテンツへのアクセスの際に、規則またはリソース導出計算の不正操作す

ることまたは評価に対する干渉を防止する。

【００９３】

●許可されていないアクセスから、コンテンツを暗号化するのに使用されるキーを保護する。

【００９４】

いくつかの実施形態において、明確に定義された計算のエンジンが、導出リソースを生成するのに用いられる。この計算エンジンの実施形態は、計算が表される方法に依存して設計することができる。例えば：

【００９５】

宣言的な計算は、当初のリソースに対して実行される必要があるが、これらの計算がどのように効果を生じるかについてガイダンスをする必要がない計算を示す専用言語で書かれた文書を使用して、宣言的に表すことができる。そのようなケースにおいて、計算エンジンは、バーチャルなセキュア・パッケージの当初の作者が、その計算が期待されるように実行されるのを保証されることができるように、計算が特定される専用言語のセマンティックを理解しなければならない。パッケージ器とユーザは、典型的には、事前に宣言型言語に同意する。

【００９６】

手続き計算は、また、標準化されたマシンのために書かれたプログラムとして表すことができる。特に、システム設計は、これらの計算が表されるバーチャルなマシン語を特定することができる。計算の当初の作者は、標準化されたマシンの仕様を知っているので、彼は、事前に、実行されている計算の高水準セマンティックを特定することを要求されることなく、その動作を完全に理解して、手続き計算をつくることができる。

【００９７】

いくつかの実施形態において、オプションの保護されたデータベースをも、例えば、規則評価の際に、計算への入力として使用される、または、さもなければ計算に影響する状態変数を保存するために、使用することができる。

【００９８】

［例］

【００９９】

本願発明の実施形態に従って、導出リソースのインプリメンテーションと使用のいくつかの更なる例が、下で提示される。例の多くが生物学と疫学に関するものであるが、本願発明は、これらの分野に限られていないことが認識される。

【０１００】

［大規模な調査におけるプライバシー維持］

【０１０１】

この例において、国家調査は、特定のタイプの病気、職業、そして、住所の間でのリンクを決定しようとしている。調査の目的は、病気の異なるタイプに対する高リスク、中リスク、低リスクのマップを生成することである。このマップは、ズーミング・システムに組み込まれ、それで、マップを見る人は、グローバル・ビューからローカル・ビューまでズームすることができる。問合せインターフェースによって、見る人が、条件と職業の異なるタイプの表示を求めることができる。

【０１０２】

調査は、多くの異なるデータベースからセキュアな環境において結果を結合することができ、管理された導出リソースとして結果をパッケージする。

【０１０３】

この例において、管理された導出リソースの中に結果を問い合わせるための規則は、以下のようなものであり得る。

【０１０４】

●問合せの結果が広域にわたっているときは、結果ははっきりしており、たとえば、特定の状態において病気の先生の数が、１００以上の結果が戻された場合には、１０のオー

ダーの正確さで報告される。１００より少ない結果が戻された場合には、報告された値は、５０のあたりの平均と、１０の偏差値を有するランダムな値である。

【０１０５】

●次第により小さな領域に対して、結果の正確さは、低下し、３０の結果のオーダーよりよい正確さを得ることができない。

【０１０６】

●ランダムな結果は、調査における選択を狭めることによって個人が識別できないことを確かめるために戻り値に挿入される。しかしながら、要求者がデータ・ビューが要求される状態において、彼または彼女を公認の医者として識別する証明書を提供することができるならば、すべての結果は、２のオーダーまで正確である。

【０１０７】

結果として生じる管理された導出リソースは、調査センターからダウンロードされることができ、セキュアなコンピューティング環境において、いかなるコンピュータでも見ることができる。

【０１０８】

位置と、病気の診断された症例との間で、なんらかの影響があるとしても、その状態の実際の個人を識別することができることなく、これは、臨時のオブザーバーが影響を見るのを可能にする。その状態において、公認の医者は、ずっと正確なビューを得ることができる。

【０１０９】

この例を実装するために、調査を行っている人は、関連したデータをいくつかのデータベースを問い合わせることができ、これらの結果から新たなデータベースを構築することができる。このデータベースは、ファイルとして実装することができた。データベースへのアクセス機構の２つの異なるセットが、コンピュータ・プログラムとして実装することができた。プログラムは、コンピュータシステムのメモリに格納されるプログラムファイルに存在することができた。

【０１１０】

公認の医者に関連するプログラムは、公認の認識状態の公開キーで暗号化されることができた。これを行う１つの方法は、対称キーをつくり、このキーでプログラムを暗号化し、それから、公認状態の公開鍵で、対称キーを暗号化することである。

【０１１１】

データベースファイル、公衆に関連するアクセス・プログラム・ファイル、および、公認の医者に関連する暗号化されたプログラムは、すべて、搬送ファイルにパッケージすることができた。このファイルは、共通のセキュア・コンピューティング環境プロバイダーの公開鍵で暗号化されることができ、調査を見たい人は誰にでも配布することができた。

【０１１２】

ユーザがビューアーによって調査を見たいとき、彼／彼女は、証明書を最初に提示する。証明書は、セキュア・コンピューティング環境に付属している標準的な証明書でもありえ、または、例えば、そのユーザは、資格のある公認の医者であることを主張できる権威者からの証明書であり得る。

【０１１３】

あとで、調査が発表されたあと、医者は、特定の遺伝子ＡＢＣ１と、環境要因、そして、病気の特定診断との関連に気がつく、彼のデータと調査データとの間の高解像度相関関係を調べるために、一般開業医証明書を交付した彼の州の委員会を使って彼は調査の作成者に手紙を書き、高解像度研究を実行する許可を求める。彼は、ファイルにおいてコンピュータ・プログラムとして行いたい計算を提供する。コンピュータ・プログラムと一緒に、彼は、また、彼自身の証明書を送る。

【０１１４】

調査において利害関係者は、コンピュータ・プログラムと医者の証明書を調べる。彼らは、管理された導出リソースと共にロードされる命令のパッケージおよび、医者が高解像

度データを見てもよいという署名された表明文を送り返す。
【０１１５】
次に、医者は、新たな命令パッケージと共に当初の管理された導出リソースおよび、彼の署名された証明書をロードする。セキュアな環境において、新たな命令は、調査利害関係者から、そのものであると認められる。署名された証明書も認められる。管理された導出リソースは、次に、それ自体に新たな命令を組み込む。これは、それが、彼の特別な計算に対する実行という医者の証明書のコンテキストにおいて動作する場合以外のすべてのケースにおいて、古い管理された導出リソースとして動作する管理された導出リソースを生成する。
【０１１６】
［個人化されたヘルスケア］
【０１１７】
スーザンは、彼女の運動療法を追跡するために、オンラインサービスを使用する。サービスは、個人の健康記録を維持して、スーザンが彼女の健康を追跡するのに使用する種々の生物測定センサから集められる情報を格納する。そのセンサは、体重計、および、スーザンの活動レベル、場所、心拍数、パルス酸素測定、皮膚電気反応（ＧＳＲ）を（毎秒）記録する多機能フィットネス腕時計を含む。
【０１１８】
スーザンは、彼女の腕時計からデータを、彼女のＰＣに（例えば、ブルートゥース、ブルートゥースＬＥ、ＡＮＴ＋、シックスロウパン（６ＬｏｗＰＡＮ）、ＵＳＢ接続、彼女のコンピュータに接続された小さな低出力無線基地局、および／または、その他を使用して、）アップロードする。それは、自動的に、サービスに対して、インターネットにデータをアップロードする。アップロードは、セキュアチャネルの上で、ＨＴＴＰＳプロトコルのような標準的なテクノロジーを使用して行われる。
【０１１９】
このサービスを通して、スーザンは、彼女のルーチンを微調整するのを援助するパーソナル・トレーナーの所在を突き止める。このサービスを通してトレーナーとの関係を樹立した後に、トレーナーは、スーザンのデータへのアクセスの要求を生成する。日曜日の夕方ごとに、トレーナーは、その週の間のスーザンのトレーニングの各々のリスト、および、各々のトレーニングに対する、
（ａ）トレーニングの開始時刻と終了時刻、
（ｂ）トレーニングの距離、
（ｃ）開始時の心拍数、ピークの心拍数、および、スーザンがピーク心拍数の５％以内にあった時間の長さ、
（ｄ）ピーク心拍数の電気皮膚反応（ＧＳＲ）
のような統計を受信したいと考える。
【０１２０】
サービスは、トレーナーに、この要求を作って、スーザンに送るユーザ・インターフェースを提供する。データの要求は、毎週集められるデータの人間が読み取れる記述を含む。スーザンは、その要求を受信して、それを承認するが、しかし、午前７時から午後７時の間に収集したデータだけを見ることができるという更なる条件を追加する。
【０１２１】
日曜日の夕方毎に、そのサービスは、前の週の間にスーザンが生成したデータの全てを集め、それを、チェックのために彼女のパーソナル・トレーナーに送られる単一のリソースとしてパッケージする。
【０１２２】
そのサービスは、データの全てを週毎に、生のフォーマットで、単一の束として集め、そのサービスによって生成されるユニークな対称キーで、束を暗号化する。
【０１２３】
このサービスは、トレーナーがこのデータにアクセスことを可能にする規則を生成する

。この規則は、例えば、データ・パッケージがトレーナーによってアクセスされるときに評価されるスーザンとトレーナーとの関係のいくつかのデジタル表現に基づくことができる。

【０１２４】

さらに、サービスは、各々のトレーニングに対して、トレーナーが要求した要素を計算するデータ・パッケージと結びつける計算のセットを生成する。これらの計算は、トレーナーがデータをレビューするために使用するクライアントソフトウェアに埋め込まれた仮想マシンで動作するために書かれている。

【０１２５】

そのサービスは、データ・パッケージ、規則、そして、計算を暗号によって結びつけるライセンス・オブジェクトを作成する１つのインスタンス生成例を提供するために、ライセンス・オブジェクトは、以下のサブ・コンポーネントの一部もしくは全部を含むことができる。

【０１２６】

●識別子にデータ・パッケージを結び付けるデータ構造。これは、データそのものの識別子と暗号ハッシュを含む。

【０１２７】

●キー識別子にデータ・パッケージを暗号化するのに用いられる対称暗号化キーを結び付けるデータ構造。これは、キー識別子と実際のキーを含む。

【０１２８】

●各規則について１つのデータ構造のシリーズとなっており、実行可能な規則のバイトコードの暗号ハッシュと共に、規則識別子をパッケージすることによって、それらのそれぞれの識別子に規則を結び付けるデータ構造。

【０１２９】

●各計算について１つのデータ構造のシリーズになっており、実行可能な計算のバイトコードの暗号ハッシュと共に、計算識別子をパッケージすることによって、それらのそれぞれの識別子に計算を結び付けるデータ構造。

【０１３０】

●データ・パッケージの識別子と、データを暗号化するために使用されるキーの識別子とを含んでいるデータ構造。

【０１３１】

●データ・パッケージの識別子と、データ・パッケージへのアクセスを管理するために使用される規則セットの識別子とを含んでいるデータ構造。

【０１３２】

●データ・パッケージの識別子と、データ・パッケージにおいて情報のビューを生成する、結びついた計算の識別子とを含んでいるデータ構造。

【０１３３】

●バイトコード・フォーマットの、受信者によって仮想マシンで実行される、規則のセット。

【０１３４】

●バイトコード・フォーマットの、受信者によって仮想マシンで実行される、計算のセット。および／または、

【０１３５】

●パッケージにおいてデータが何を表すか（例えば、それが集められた週のスーザンのデータであったかどうか、等）を確立するのに用いられるメタデータ。

【０１３６】

パーソナル・トレーナーは、彼のクライアントの全てに対してデータを探索するのを可能にするソフトウェアパッケージを使用する。このソフトウェアは、データにアクセスするためにセキュアな実行環境を実装するソフトウェア開発キット（ＳＤＫ）を使用して構築される。月曜日の朝に、トレーナーは、ソフトウェアパッケージを開けて開始する。そ

れはサービスにつながって、彼がクライアントから受信したかもしれないいかなる新情報をもダウンロードする。

【０１３７】

スーザンのデータをレビューするために、ソフトウェアによって提示されるユーザ・インターフェースにおいて、トレーナーはスーザンの名前をクリックする。ソフトウェアは、そのセキュアな処理環境において、例えば、以下の一部もしくは全部を含むいくつかのことをすることができる。

【０１３８】

●種々のライセンス・オブジェクトにおいて、スーザンのデータ・パッケージを識別することを知っているメタデータを使用する。（この情報は、いくつかのローカル・データベースにおいて、インデックス化することができる。）

【０１３９】

●先週のライセンス・オブジェクトを開き、データ・パッケージと関連した規則を見つけてロードするために、データ・パッケージを規則セットにリンクするデータ構造を使用する。

【０１４０】

●規則をインスタンス化するバイトコードを実行し、規則において表される条件が満たされるか否かに基づいて、処理を続けるかどうかの決定をする。

【０１４１】

●規則の評価がうまくされたとして、キーを得て、データを復号化するために、暗号化キーにデータ・パッケージを結び付けているデータ構造を使用する。

【０１４２】

●ロードして、計算を実行するために、その計算にデータ・パッケージを結び付けているデータ構造を使用する。それは、データ・パッケージのいくつかのビュー、計算ごとに１つを生成する。

【０１４３】

●表示のためのソフトウェアパッケージのユーザ・インターフェース部分が利用できる、これらの計算の結果を得る。

【０１４４】

●監査レコードをオンラインサービスに送り返す。スーザンは、彼女のデータがどのように使用されているか決定するために、定期的にチェックすることができる。

【０１４５】

トレーナーは、これらの計算の結果を、彼のユーザ・インターフェースにおいて見る。これらの結果が導出された根底にあるデータが、トレーナーにさらされていなかったことに留意する。したがって、例えば、たとえ、スーザンによってアップロードされて、データ・パッケージにおいてトレーナーに送られる生データにおいて、その情報が含まれるとしても、トレーナーは、トレーニングがどこで起こったかについて学ぶことができない。

【０１４６】

数週間スーザンのデータを評価した後に、パーソナル・トレーナーは、より様々な地形で彼女のトレーニングをすることによって、彼女のスタミナを増やすように、スーザンを励ます。この療法の効果性を評価するために、トレーナーは、彼が地域のマップ上でそれをプロットして、比較的フラットな地域で、彼女が上り坂なのかどうか決定する等ができるように、どこで、スーザンが運動しているかについて情報を有したいと思う。彼は、場所に対して心拍数を相関させることができるように詳細な心拍数データとともに、このデータを受信することを望む。トレーナーは、スーザンからこの追加情報を要求するためにオンラインサービスによって提供されるインターフェースを使用する。

【０１４７】

スーザンは、要求を受信するが、トレーナーに詳細な位置情報へのアクセスを与えることに安心感がない。何といっても、彼女は直接トレーナーにこれまでに会ったことがなく、そのような情報を伝えることについていくぶん慎重である。しかしながら、彼女には、

このデータを求めるトレーナーの理由を理解し、彼の分析をサポートしたいと思っている。それで、トレーナーの要求を受け入れるよりは、むしろ、スーザン自身が、高度データへのアクセスを許すが、しかし、緯度と経度は許さない計算をつくるためにオンラインサービスでインターフェースを使用する。

【０１４８】

サービス・インターフェースは、テンプレート・ライブラリにおいて利用できる異なる計算に対して、体系化されたブラウザを提示する。ブラウザは、例えば、「場所」、「フィットネス」、その他データの異なるタイプに関係している計算を提示する。

【０１４９】

スーザンは、「場所」の地域に目を通して、いくつかの計算は、彼女が利用できることに気付く。「完全な位置情報」、「緯度／経度」、「高度」について。

【０１５０】

スーザンは、「高度」を選択し、次に、インターフェースによって、彼女は、時間的に、空間的に、計算のデータ解像度を選択することができる。例えば、スーザンは、時間的解像度に対して、「３０秒ごと」または「５分の追跡平均」を、空間的解像度に対して、「フル解像度」または「＋／－１０m内のランダム化」を選択することができる。

【０１５１】

類似した手順を用いて、スーザンは、３０秒の間隔で心拍数データを提供する計算を選択する。

【０１５２】

一旦スーザンが、適用したい計算を選択すると、彼女は、パーソナル・トレーナーに、この計算を得る許可を与えるために、さらなるインターフェースを使用する。その時から（またはスーザンが認可を取り消すまで）、この計算は、トレーナーに送られる週報の一部として含まれる。

【０１５３】

トレーナーは、高度と、詳細な心拍数データを受信し始める、彼は、スーザンのトレーニングの効果を評価して、フィードバックを提供するために、それを使用する。１週間に相当するデータを評価した後に、彼は、この新情報が有用であることを見つけ、スーザンの過去のデータで類似した情報に対する要求を行い、それをスーザンは認可する。その結果、トレーナーは、彼がすでに受信し、格納したデータ・パッケージで高度／心拍数計算を提供するオンラインサービスから新たなライセンス・オブジェクトを受信する。サービスは、データ・パッケージ自体を再送信する必要はなく、新たな許可オブジェクトだけである。

【０１５４】

新たな療法の二ヵ月後に、スーザンの心血管効率は、期待されたようには良くなっていないように見える。彼女のトレーニングの動きは気まぐれであり、途中に頻繁な休みがあった。スタッフでスポーツ医学を専門とする医者を有する組織で働くトレーナーは、スタッフの医者からのいくつかのインプットを得たいと望む。彼らは、異なる場所で働いている。サービスを通して、トレーナーは、それが受け入れ可能であるかどうかを、スーザンに尋ね、彼女は、それに同意する。トレーナーは、スーザンのこの１か月分のデータを、直接医者にフォワードする。そのデータ・パッケージと許可が、含まれている。

【０１５５】

医者は、計算を走らせるためにデータを開けようとし、（まだ、まったくデータにアクセスする許可を与えられていないので）彼のソフトウェアによって、スーザンからの認可を要求するように促される。彼は、そのようにして、認可要求がスーザンに送られ、スーザンは、それを承認する。

【０１５６】

データを分析した後に、医者は、酸素負荷が良くないという問題を疑い、オンラインサービスを通して，スーザンのパルス・オキシメトリ・データへの更なるアクセスを要求し、スーザンは、医者に認可を与える。トレーナーが、同じデータにアクセスしないことに

注意すべきである。そのサービスは、医者へのパルス・オキシメトリ・データに対して別々の計算をつくり、医者だけに、それらの計算を含むライセンスを送った。

【０１５７】

医者は、そのデータからなんらかの結論を引出し、彼の勧告をトレーナーに提供する。トレーナーは、医者のインプットを反映して、スーザンの療法を修正する。彼女の心血管パフォーマンスは、よくなり始める。

【０１５８】

ある時間の経過後に、サービスにおける彼女のデータの使用と、行動に認可とをリビューして、スーザンは、医者は、まだ彼女の情報にアクセスしていることを認識し、このコンサルテーションが終了したので、このアクセスを無効にすることを選択する。医者に発行されたライセンスは、無効であるとマークされ、医者のソフトウェアは、この事実を通知される。そして、将来の許可はつくられないか、この認可において医者には送られない。他の実施形態において、ライセンスは、指定された期間経過の後に自動的に期限切れになるようにできる。

【０１５９】

［ビデオ・ダウンロード・サービス］

【０１６０】

イアンは、彼に彼の種々のレンダリング・デバイスに対して幅広い種類のムービーに無制限のアクセスを与えるオンライン・ムービー・サービスに申し込む。

【０１６１】

よりストリーミング指向のモデルと対照的に、そのサービスは、プログラムのダウンロードと、持続的なストレージのために設計されている。ストリーミングは、ビデオの漸進的なダウンロードによってシミュレートできるが、しかし、このモデルにおいてでさえ、ライセンスは、最初に得られ、そして、漸進的にダウンロードされたストリームがレンダリングされる前に、規則が評価される。

【０１６２】

このサービスは、広告によってサポートされる標準的定義の無料の層を含む購読申込層を提供する。これは、当初のイアンのオプションである。他のオプション（料金表に関して）は、広告なしの標準的な定義提供、および、高解像度提供を含む。

【０１６３】

そのサービスは、高解像度ビデオ・ファイルを、ピア・ツー・ピア配布ネットワーク上のカスタマーに提供するようになっている。各々のムービーの複数のバージョンと解像度を配布するロジスティックスは、あまりに複雑であると考えられたので、あらゆるカスタマーは、彼らの購読申込層に関係なく正確に同じ高解像度ビデオ・ファイルを受信する。

【０１６４】

ビデオ・ファイルは、ライセンスとは別に配信される。カスタマーがライセンスを要求するときに、ライセンスは、データの特定のカスタマーのビューを導出する計算を含み、レンダリング・システムに正確にカスタマーが見る権利があるビデオストリームを提供する。

【０１６５】

無料の広告でサポートされた標準的定義層の場合、３つの計算が、各々のライセンスにおいて含まれる。（ｉ）パッケージされたビデオから標準的な定義ストリームを抽出する計算。（ｉｉ）広告ファイルを広告サーバから定期的にダウンロードし、それらを出力ストリームに挿入し、広告サーバが到達可能でない場合にいくつかのデフォルト広告に後戻りする計算。（ｉｉｉ）広告の印象の監査レコードを広告サーバに送る返す計算。

【０１６６】

これらの計算は、前の例で記載したように、非常にビデオ・ファイルに結びついている。

【０１６７】

これらの計算は、ライセンスを評価するセキュア・コンピューティング環境によって、

クライアントソフトウェアにおいて実行され、コンテンツを復号化し、クライアントのネイティブ・レンダリングエンジンにそれを戻す前にコンテンツに出力計算を適用する。

【０１６８】

カスタマーが、お金がかかるが、プレミアム層に申し込むときには、レンダリングの前にこれらの出力計算の一方または両方を適用する要求は、取り除かれる。

【０１６９】

このサービスは、カスタマーが自由に保護されたコンテンツを配布するのを許すことによって広告収入を最大にするように設計されている。保護されたコンテンツの受取人が、支払った加入者であるならば、彼が代金を払った解像度でコンテンツをレンダリングするライセンスを透過的に得ることができる。受取人が加入者でないならば、クライアントソフトウェアをインストールするまで、彼は、まったくビデオをレンダリングすることができない。直接配布されたビデオは、受取人に標準的な定義ビデオを広告で見させるデフォルト・ライセンスとバンドルされている。

【０１７０】

イアンは、出張に行く前に、彼のタブレットの上へムービーをダウンロードする。彼は、そのムービーが非常に好きで、友人のジムにコピーをあげたいほどである。彼は、単に（パッケージされたビデオ・コンテンツとデフォルト・ライセンスを含む）ムービー・ファイルをジムのシステムにコピーし、ジムはそのムービーを見ることができる。

【０１７１】

ムービーを楽しんだ後に、ジムは、サービスに購読申込の代金を払うことに決める。一旦、彼がそうするならば、彼は、自分が持っているコンテンツを広告なしでレンダリングできるライセンスを得る。これらのライセンスは、非常に速くダウンロードされ、アップグレードは、比較的大きなビデオ・ファイルを再ダウンロードしなければならないことなく、すぐに実施される。

【０１７２】

より家族向けの試みにおいて、「Ｍｏｖｉｅｓ４Ｆａｍｉｌｉｅｓ」と呼ばれている組織との協力を、ムービー・サービスは結ぶ。この組織は、サービスによって提供されるフィルムの全てをレビューして、どのシーンがより若い視聴者には不適当であるかについて決定し、タイプによってそれらを分類する（例えば、軽い暴力、ののしり、ヌード、不快な暗示、等）。

【０１７３】

各シーンに対して、その組織は、好ましくないシーンを除く、２秒の間スクリーンを消す、ビープ音を入れる、代替の筋書きをつなぎ合わせる、または、ムービーをより家族向けにするために、要求されるいかなる他の処置でもとる出力ストリームを修正する計算をつくる。

【０１７４】

これらの計算は、ユーザ設定に依存する。例えば、親が子のクライアントを１０歳と設定するならば、特定のデフォルト計算が、適用され得る。それは、１５歳に適用される計算とは異なる。

【０１７５】

ペアレンタル・コントロールは、同様にフィルタリングを微調整する能力を含むことができる。

【０１７６】

イアンは、「Ｍｏｖｉｅｓ４Ｆａｍｉｌｉｅｓ」サービスの契約をする。その結果、彼が、主要なビデオ・サービスからダウンロードするあらゆるムービーに対して、適切なフィルタを適用する「Ｍｏｖｉｅｓ４Ｆａｍｉｌｉｅｓ」サービスから、彼のクライアントは、計算も引き離す。ムービーが彼の若い息子の装置上でレンダリングされるとき、フィルタにより、確実に、彼が不適当な断面を見ていないことになる。

【０１７７】

技術的に、「Ｍｏｖｉｅｓ４Ｆａｍｉｌｉｅｓ」によってつくられる計算は、同一ビデ

オ・サービスがそれらを結び付けたのと同じ方法で、ビデオの識別子と、計算のための識別子を結びつけるオブジェクトを作成することにより、彼らが管理するムービーに結びついている。

【０１７８】

この例において、ムービー・サービスにおいて使用されるビデオ・クライアントは、認証キーを持つエンティティによってデジタル署名されるライセンスと計算を信頼するだけであるとする。ここで、この認証キーはムービー・サービスそのものによって発行されたものである。このケースにおいて、ムービー・サービスは、「Ｍｏｖｉｅｓ４Ｆａｍｉｌｉｅｓ」に、彼らがムービーとフィルタリング計算を結びつけるオブジェクトにデジタル署名するのを可能にする認証キーを発行した。

【０１７９】

「Ｍｏｖｉｅｓ４Ｆａｍｉｌｉｅｓ」は、計算そのものと、計算とムービーとの間のバインディングを、クライアントに送信する。ビデオ・サービスに由来するキーですべてがデジタル署名される。このように、ビデオ・クライアントは、署名を認識し、そして、レンダリングの時に要求された計算を適用する。

【０１８０】

フィルタの機能は、クライアントにおける設定に依存する。例えば、イアンと彼の若い息子の両方が、彼らのそれぞれのクライアントを用いて、同じムービーを見るかもしれない。しかし、息子のクライアントが１０歳に設定されたので、彼のストリームは、かなりフィルタがかかっているが、ところが、イアンは、当初のフィルタ処理されてないフィルムを見る。この例は、クライアント側で維持された状態変数が、どのように、実行される計算にインパクトを与え得るかを示す。

【０１８１】

［デジタル・リミックスとマッシュアップ］

【０１８２】

ジョンは、有力なファンク・トラックをつくった音楽家で、コピーを許可しないライセンスで、デジタル的にそれを配布した。

【０１８３】

マルコムは、ＤＪで、ジョンのオリジナル・トラックの４秒のサンプルを組み込み、いくつかの他のオーディオ・トラックにミックスして、デジタル・マッシュアップを作りたい（そして、売りたい）と思っている。

【０１８４】

デジタル・ミキシング・ソフトウェアを使用して、マルコムは、ジョンのトラックから関連した４秒を抽出する計算をつくり、それをフランジャーを通して、フィルタ処理し、彼のミックスにそれを適切なポイントに入れる。

【０１８５】

マルコムは、ジョンにこの計算を送り、ジョンは、演奏毎に半セント支払われる限りこの特定の使用を承認する。彼は、計算に署名し、彼のオリジナル・トラックにそれを結び付け、そして、抜粋が演奏されるたびに彼に監査レコードを送り、課金のための使用を追跡するのを可能にするという事後条件を追加する。

【０１８６】

マルコムは、ジョンのオリジナル・トラックと、４秒のサンプルを抽出してフィルタ処理する計算とを含めて、彼自身のマッシュアップをパッケージする、レンダリングの上で、ジョンの計算は、適切なポイントで適用され、結局、ジョンは彼のオリジナル・サンプルの使用に対して支払を受ける。

【０１８７】

［遺伝学］

【０１８８】

エリザベスは、彼女のゲノムをシーケンスすることを要求される臨床試験に登録された。その試験は、特定の遺伝子型と、制癌薬物のための最適投与との間の関係を調査するこ

とが目的であった。

【０１８９】

エリザベスは、最初に、彼女のゲノムを格納して、アクセスを管理する遺伝子情報サービスのアカウントを設定することを要求された。一旦、彼女がこのアカウントを登録すると、サービスは、ランダムなサンプル番号（とバーコード）を生成し、彼女はそれを印刷して、シーケンス・ラボにそれをもっていった。

【０１９０】

エリザベスは、彼女のサンプルを提供し、ラボの技術者が、バーコードを調べ、エリザベスのゲノム情報シーケンスをランダム・サンプル番号に結びつけた。

【０１９１】

ゲノムは、セキュアに情報サービスにアップロードされ、ランダム・サンプル番号が、エリザベスのアカウントを調べ、彼女のゲノムと彼女の他のアカウント情報との間にバインディングをつくるのに用いられた。

【０１９２】

遺伝子シーケンス自体が、保護された形で複数の研究施設の間で自由にコピーすることができるような方法で、遺伝子の情報サービスはつくられた。しかし、そのシーケンスを復号化する、あるいは、そのシーケンスにアクセスする許可は、サービスによって認証されるようにエリザベス自身によって与えられなければならない。このアーキテクチャは、エリザベスの（数ギガバイトより大きなファイルである）遺伝子シーケンスを研究においてそれを使用することに興味を持っているかもしれない研究者に配布することを可能にする。しかし、すべてのそのような使用は、エリザベスによって監査され、制御される。

【０１９３】

エリザベスが臨床試験に登録したとき、彼女は、研究を設計している科学者が求めたゲノムに対して特定の問合せを承認するよう頼まれた。例えば、その研究が、乳がんについてであり、研究者は、ＢＲＣＡ１、ＢＲＣＡ２およびＴＰ５３遺伝子についての情報を求めていたとする。

【０１９４】

エリザベスが、これらの特定の研究者に対して彼女のゲノムの使用を承認したので、遺伝学サービスは、エリザベスのゲノムに対して動作するいくつかの計算をつくった。その計算は、必要情報をとても抽出して、認可された団体にそれを提供する。これらの計算は、同様に監査条件を有する。それは、計算が実行されるたびに、監査報告書が遺伝学サービスに送られることである。このように、エリザベスは、彼女の情報がどのように、誰によって使用されているかについて追跡することができる、サービスは、例えば、本願明細書のどこか他所に記述されたように、ゲノムと計算を暗号によって結びつけるデータ構造にデジタル署名することによって、ゲノムにこれらの計算を結び付ける。

【０１９５】

ある後の日において、研究に参加していた研究者の一人が、制ガン剤のパフォーマンスと、これまで未知の遺伝子のメカニズムとの間の新しい関係と思えるものを発見する。

【０１９６】

遺伝学サービスを使用して、研究者は、このサービスにおいてアカウントを有するすべての人々の中からありそうな研究仲間を識別する問合せを実行する。この問合せは、その研究者に、彼らのアイデンティティを示すことなく乳がんに関する以前の研究に参加した人を識別する。

【０１９７】

研究者は、彼の新たな研究に対して１３０人の候補を見つける。しかし、彼は、彼らが誰であるかわからない。このシステムには、他の候補がいるかもしれない、。しかし、彼らは、将来の研究に参加することに興味がないと、シグナルを送った。そのため、彼らは、研究者への候補として示されていない。

【０１９８】

遺伝学サービスによって提供されるインターフェースを用いて、研究者は、仮定された

パターンに対して検査するためにゲノムを問い合わせるシステムに計算をアップロードする。

【０１９９】

研究者は、彼のラボにおいてソフトウェアを使用しているこの計算をつくり、彼がフル・アクセスを有するゲノムに対してそれを走らせることによって、それを検証した。

【０２００】

彼は、サービスに、計算を、彼が、計算についてのメタデータ（何に使用されか、等）を特定し、彼が制御するキーを使用して計算にデジタル署名することを可能とするインターフェースを介してアップロードした。

【０２０１】

遺伝学サービスを使用して、研究者は、１３０人の候補者の各々に、参加する気があるかどうかを尋ねる。同意するものに対して、このサービスは、新たな計算を、発信者（計算に署名するのに使用される公開キーに対応する秘密キーの保有者）だけが、その計算を走らせることができる条件で彼らのそれぞれのゲノム情報シーケンスに結び付ける。

【０２０２】

これらの計算は、入ってくると、研究者にフォワードされ、研究者は、それらを、彼がラボにすでに有しているゲノム情報シーケンスに適用する。あるいは、彼がコピーをもはや有していないならば関連したゲノム情報シーケンスのコピーをダウンロードする。

【０２０３】

研究者は、エリザベスの特定のシーケンスについて独特な何かを発見し、彼女に、彼に連絡するよう依頼する匿名のメッセージを送るために、サービスを使用する。電話で、研究者は、彼が発見したものについて説明し、エリザベスに、さらに調査することができるように彼女の全部のシーケンスにアクセスする許可を求める。

【０２０４】

このサービスを使用して、エリザベスは、計算をつくり、彼女のゲノムにそれを結び付け、研究者に、それを送る。計算は、その特定の研究者が、彼が信頼された環境においてそれを走らせ。各アクセスが監査されることを義務づける限り、彼女のゲノムに対して任意のさらなる計算を走らせることを可能にする。

【０２０５】

実質的に、エリザベスは、彼が認証されて、計算を実行するために信頼された環境を使用している限り彼女のゲノムに任意の新たな計算を結び付ける能力を研究者に委任した。これは、彼女が単に研究者に保護されていないファイルを与えるならば有することのない、彼女のゲノムに対するある程度の制御をエリザベスに与える。

【０２０６】

技術的に、これは、そのエリザベスが設定した条件にしたがう（研究者によって提案された）チェーンにおいて次の計算を認証する、エリザベスによって要求される事前計算の形をとることができる。それは、最初は、研究者の提案された計算を走らせ、そして、条件によって、アウトプットを認めるか、認めない、事後条件としてインプリメントすることもできる。

【０２０７】

研究者は、他のタイプの計算（例えば、協力者がエリザベスのゲノムの質問をするのを許す）を結び付ける能力を要求ことができる。しかし、彼は、これらの計算を結び付けて、それらを配布するために、エリザベスの許可を最初に取得しなければならない。

【０２０８】

［科学研究］

【０２０９】

ジョシュは、政治的な含みのある領域において論文を発表している社会科学研究者である。調査結果が特定の政治団体の間で論争の的であるということを、彼は事前に知っており、彼自身の政治課題に合うように、データをフィルタ処理したとして、彼は訴えられる。彼は、例えば、不都合なサンプルを省略することをしなかったと証明することができる

必要がある。しかし、彼は、生データそのものを明らかにすることなくこれを証明することができる必要がある。生データは、それは彼の研究対象を識別するのに用いることができる。

【０２１０】

ジョシュは、明確に定義されたフォーマットで、彼のデータを集める、彼のデータのソースを慎重に文書化する（そして、理想的には、後の検証のために使用することができる署名または生物認証を収集する）。データを処理して、統計を抽出する研究の一部として、彼は一連のプログラムを作成する。一旦、彼がデータについていくつかの結論を出すと、彼は、１つのコンテナにデータをパッケージして、生成した対称キーで、それを暗号化する。

【０２１１】

ジョシュは、以下を含む、彼が最終結果を計算するために使用した計算をパッケージする。例えば、彼の論文に現れる特定の統計表を生成する一連の計算、彼の論文の種々の数字／グラフを生成する計算、および／または、その他である。

【０２１２】

ジョシュは、本明細書の他所で開示した技術を用いて、彼の生データにこれらの計算を結び付け、公にアクセスできるウェブサイトに、パッケージされたデータと計算を入れる。

【０２１３】

ジョシュは、彼の論文を発表する。批評家が、彼に選択的なデータ操作だと非難するとき、ジョシュは、批評家にウェブサイトまでの道を教える。ここで、彼は、彼自身実験を実行するために、ジョシュの当初のデータ・パッケージと計算とをダウンロードすることができる。

【０２１４】

批評家はデータ・セットをダウンロードして、データがパッケージされてから手を入れられなかったこと、計算がジョシュの論文において示される結果を生成すること、人間が読み取れるフォーマットになっている計算自体、結論をサポートしないデータを除こうとしないことを検証する。

【０２１５】

これらを検証した後に、批評家は、まだジョシュの結論を受け入れない。批評家は、ジョシュが特定の要因のバイアス影響を無視したと信じている。批評家は、バイアス要因を説明するジョシュの計算の１つの修正版を作成する、そして、ジョシュにその計算を提案する。

【０２１６】

ジョシュは、その批判を有効であると認め、彼のデータ・セットにそれを結び付けるために、計算に署名し、そして、批評家にバインディングを送り返す。批評家は、そのデータに対して新たな計算を走らせる。結局、ジョシュの結論は、依然として維持され、ジョシュは、次に、彼の結果を検証するための彼の公的なパッケージの一部として批評家の提案された計算を含める。

【０２１７】

ここに記述されるシステムと方法を実装する多くの方法があることが認識される。例えば、いくつかの実施形態において、ここに記述されたシステムと方法は、’６９３特許出願に記載されたデジタル権利管理技術、および／または、同一出願人の米国特許出願第１０／８６３，５５１（米国特許出願公開第２００５／００２７８７１号明細書）（「’５５１出願」）に記載されたデジタル権利管理またはサービス編成技術に関連して使用することができる（’６９３出願と’５５１出願の内容は、その全体が引用により本明細書に組み込まれる）。しかしながら、他のどの適切なＤＲＭやサービス技術も、その代わりに使用することができる。

【０２１８】

図３は、ここに記述されるような導出リソースを含む電子コンテンツを管理するための

図解的なシステム３００を示す。図３で示すように、電子コンテンツ３０３において権利を持っているエンティティ３０２は、エンドユーザ３０８ａ－ｅ（全体的に「エンドユーザ３０８」と称される、ここで、参照番号３０８は、コンテキストから明らかように、エンドユーザまたはエンドユーザのコンピューティング・システムをさす。）による配布と消費のためにコンテンツをパッケージする。例えば、エンティティ３０２は、コンテンツのオーナー、作者、または、プロバイダー、例えば、個人、研究者、音楽家、映画スタジオ、出版社、ソフトウェア会社、著者、移動サービス提供者、ネットワーク間のコンテンツ・ダウンロードまたは購読サービス、ケーブルまたは衛星テレビ・プロバイダー、会社の従業員、または、その他、または、その代理をしているエンティティを含むことができる。コンテンツ３０３は、例えば、個人のヘルスケア・データ、遺伝情報、研究結果、デジタル・ビデオ、オーディオ、または、テキストのコンテンツ、ムービー、歌、ビデオゲーム、ソフトウェア、電子メール・メッセージ、携帯メール、ワープロ文書、レポート、または、他のいかなるエンターテイメント、事業、または、他のコンテンツなどいかなる電子コンテンツをも含むことができる。

【０２１９】

図３において示される例において、エンティティ３０２は、ライセンス３０６と１つ以上の計算３０７とを、パッケージされたコンテンツ３０４に結びつけるパッケージング・エンジン３０９を使用する。ライセンス３０６は、エンティティ３０２のポリシー３０５または他の願望に基づき、コンテンツの許されたおよび／または禁止された使用、および／または、コンテンツを利用するために満たされなければならない、または、使用の条件または結果として満たされなければならない１つ以上の条件を特定する。計算３０７は、ライセンス３０６によって特定されるポリシーにしたがってコンテンツの種々のビューを提供する。コンテンツは、また、例えば、信用当局３１０が、適切な暗号鍵、証明書、および／または、その他を得るのに用いることができる暗号化またはデジタル署名技術など１つ以上の暗号メカニズムによってセキュアにされる。

【０２２０】

図３で示すように、パッケージされたコンテンツ３０４、ライセンス３０６、および、計算３０７は、例えば、インターネットのようなネットワーク３１２、ローカル・エリア・ネットワーク３１１、無線ネットワーク、仮想専用ネットワーク３１５、広域ネットワーク、および／または、その他を介して、ケーブル、衛星、ブロードキャスト、または、セルラ方式通信３１４を介して、および／または、コンパクトディスク（ＣＤ）デジタル多用途ディスク（ＤＶＤ）、フラッシュメモリカード（例えば、セキュア・ディジタル（ＳＤ）カード）、および／または、その他のような記録できるメディア３１６を通して、いかなる適当な手段でもエンドユーザ３０８に提供することができる。パッケージされたコンテンツは、ユーザ３０４に、ライセンス３０６や計算３０７と共に、単一パッケージ、または、送信３１３、または、同一または異なるソースから受信される別々のパッケージまたは送信で配達することができる。

【０２２１】

エンドユーザのシステム（例えば、パソコン３０８ｅ、移動電話３０８ａ、テレビジョンやテレビジョン・セットトップボックス３０８ｃ、タブレット３０８ｄ、携帯型オーディオやビデオ・プレーヤー、電子ブック・リーダ、および／またはその他）は、アプリケーション・ソフトウェア３１７、ハードウェア、および／または、コンテンツを読み出し、レンダリングするために使用可能である特殊用途ロジックを含む。ユーザのシステムも、ソフトウェアやハードウェアを含み、ここでは、デジタル権利管理エンジン３１８と称する。これは、パッケージされたコンテンツ３０４と関連したライセンス３０６と計算３０７を評価し、ライセンス３０６によって許可された場合のみ、計算３０７に従って、コンテンツへのユーザクセスを選択的に与えることによって、その項目を実施する（および／または、アプリケーション３１７がそのような項目を実施するのを可能にする）。デジタル権利管理エンジン３１８は、アプリケーション３１７と、構造的に、または、機能的に統合することができる。あるいは、ソフトウェアおよび／またはハードウェアの別々の

部分を含むことができる。代替的に、または、追加的に、例えば、システム３０８ｃなどユーザのシステムは、例えば、ユーザに、ユーザが事前に得た、あるいは、要求したコンテンツへのアクセスを許すかどうかに関して決定３２０をするデジタル権利管理エンジンを使用するシステム３０８ｂなど（例えば、サーバ、複数装置のユーザのネットワークにおける別の装置、例えば、パソコンまたはテレビジョン・セットトップボックス、および／またはその他）リモートシステムで通信することができる。

【０２２２】

デジタル権利管理エンジン、および／または、ユーザのシステム上の、または、それと遠隔コミュニケーションする他のソフトウェアは、また、保護されたコンテンツへのユーザのアクセス、または、保護されたコンテンツの他の使用についての情報を記録することができる。いくつかの実施形態において、この情報の一部もしくは全部は、遠隔団体（例えば、情報センター３２２、コンテンツ作者、所有者、または、プロバイダー３０２、ユーザのマネージャ、その代理をしているエンティティ、および／または、その他）に伝えることができる。例えば、所有者の個人情報の使用を追跡するために、収益（例えば、著作権使用料、広告ベースの収益、等）を割り当てるため、利用者選好を決定するため、システム・ポリシー（例えば、秘密の情報が使用されるときおよび方法をモニターすること）を実施するため、および／または、その他である。図３が、図解的なアーキテクチャ、および、一組の図解的な関係を示しているが、ここに記述されるシステムと方法は、いかなる適切なコンテキストにおいても実施することができることが認識される。よって、図３は、図示と説明のために提供され、制限のためにでないことが認識される。

【０２２３】

図４は、本願発明の実際的な実施形態に使用することができたシステム４００のより詳細な例を示す。例えば、システム４００は、エンドユーザの装置３０８、コンテンツ・プロバイダの装置３０２、および／または、その他の実施形態を含むことができる。例えば、システム４００は、例えばパソコン３０８ｅまたはネットワークサーバー３１５など多目的コンピューティング装置、または、例えば、移動電話３０８ａ、パーソナル携帯情報機器、携帯型オーディオまたはビデオ・プレーヤー、テレビジョン・セットトップボックス、キオスク、ゲーム・システム、または、その他専用コンピューティング装置を含むことができる。システム４００は、典型的には、プロセッサー４０２、メモリ４０４、ユーザ・インターフェース４０６、取り外し可能なメモリ４０８を受け入れるためのポート４０７、ネットワークインターフェース４１０、および、前記の要素をつなぐための１つ以上のバス４１２を含む。システム４００の動作は、典型的には、メモリ４０４に格納されるプログラムのガイダンスによって動作するプロセッサー４０２で制御される。メモリ４０４は、通常、両方の高速のランダムアクセスメモリー（ＲＡＭ）、および、不揮発性メモリー（例えば磁気ディスクやフラッシュＥＥＰＲＯＭ）を含む。メモリ４０４のいくつかの部分は、システム４００の他のコンポーネントによって読まれることができない、あるいは、書き込むことができないように制限することができる。ポート４０７は、ディスクドライブまたは、フロッピー（登録商標）ディスケットのようなコンピュータ可読なメディア４０８を受け入れるためのメモリー・スロット、ＣＤ－ＲＯＭ、ＤＶＤ、メモリーカード、ＳＤカード、他の磁気または光学メディア、および／または、その他を含むことができる。ネットワークインターフェース４１０は、典型的には、例えばインターネットまたはイントラネット（例えば、ＬＡＮ、ＷＡＮ、ＶＰＮ、等）などネットワーク４２０を介して、システム４００と他のコンピューティング装置との間の接続（および／または、コンピューティング装置のネットワーク）を提供するために使用可能であり、物理的にそのような接続をする１つ以上の通信技術（例えば、無線、イーサネット（登録商標）、および／または、その他）を使用することができる。いくつかの実施形態において、システム４００は、また、システム４００または他のエンティティのユーザによって不正操作することから保護されている処理ユニット４０３を含むことができる。そのようなセキュアな処理ユニットは、センシティブな操作、例えば、鍵管理、署名照合、および、デジタル権利管理プロセスの他の態様のセキュリティを強化するのに役立つ。

【０２２４】
図４で示すように、コンピューティング装置４００のメモリ４０４は、コンピューティング装置４００の動作を制御するための種々のプログラムまたはモジュールを含むことができる。例えば、メモリ４０４は、典型的には、アプリケーションの実行を管理するためのオペレーティングシステム４２０、周辺機器、その他、保護された電子コンテンツをレンダリングするためのホスト・アプリケーション４３０、および、ここに記述される権利管理機能性の一部もしくは全部を実装するためのＤＲＭエンジン４３２を含む。本明細書の他所で記載されているように、ＤＲＭエンジン４３２は、制御プログラムを実行するための仮想マシン４２２などの種々の他のモジュール、機密情報を格納するための保護されたデータベース４２４、および／または、例えば、コンテンツの暗号化や復号化など暗号動作を実行し、ハッシュ関数とメッセージ認証コードを計算し、デジタル署名を評価すること、および／または、その他のための１つ以上の暗号モジュール４２６を含み、相互運用し、および／または制御することができる。メモリ４０４は、また、典型的には、保護されたコンテンツ４２８と、結びついたライセンスと、計算４２９、ならびに暗号鍵、証明書、等（図示されない）を含む。

【０２２５】
当業者は、ここに記述されるシステムと方法は、図４において図示されたものに類似のあるいは同一のコンピューティング装置で、または、実質的にいかなる他の適切なコンピューティング装置でも、実施することができることを認識する。これらは、図４において示されるコンポーネントのいくつかを所有しないコンピューティング装置を含み、および／または、示されない他のコンポーネントを所有するコンピューティング装置を含む。このように、図４が、説明のために提供されたものであり、制限のために提供されたものではないことが理解されるべきである。

【０２２６】
上では、明快さのためにいくつかの詳細に記述されたが、ある変更や修正を、付帯する特許請求の範囲の中で行うことができることは明らかである。例えば、いくつかの例では、’６９３特許出願において記述されたようなＤＲＭエンジンを使用して記述されたが、ここに記述されるシステムと方法の実施形態は、規則またはポリシーにしたがうコンテンツを管理するためのいかなる適切なソフトウェアおよび／または、ハードウェアを使用しても、インプリメントすることができることが認識される。ここに記載した方法及び装置の両方をインプリメントする多くの代替的方法があることに留意する。したがって、本願の実施形態は、図解的なものであり、制限的ではないと考えられ、本願発明は、ここに与えられた詳細に限られるものではなく、添付の特許請求の範囲と均等物の範囲で修正できるものである。

【図１Ａ】

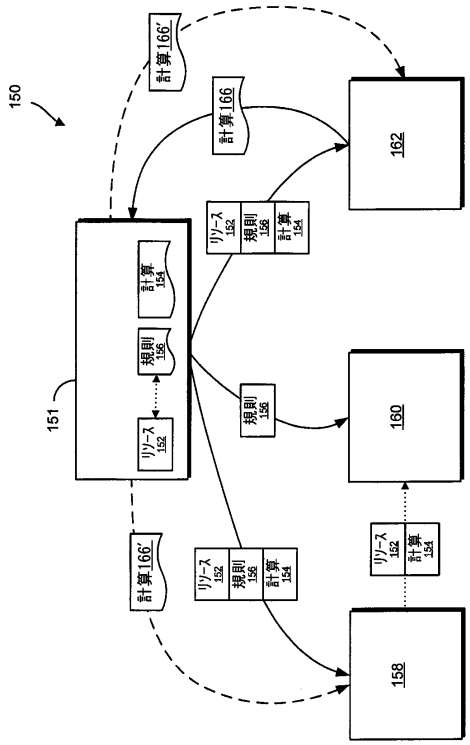

FIG. 1A

【図１Ｂ】

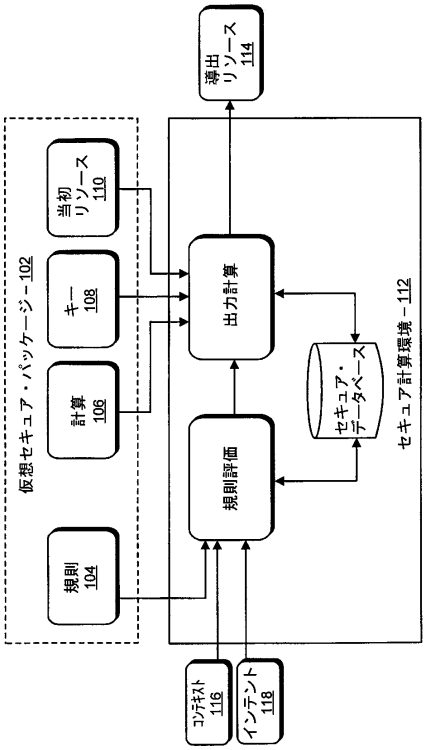

FIG. 1B

【図２】

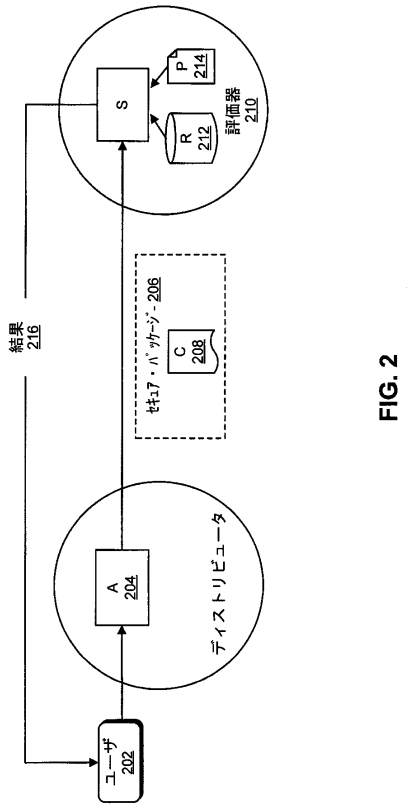

FIG. 2

【図３】

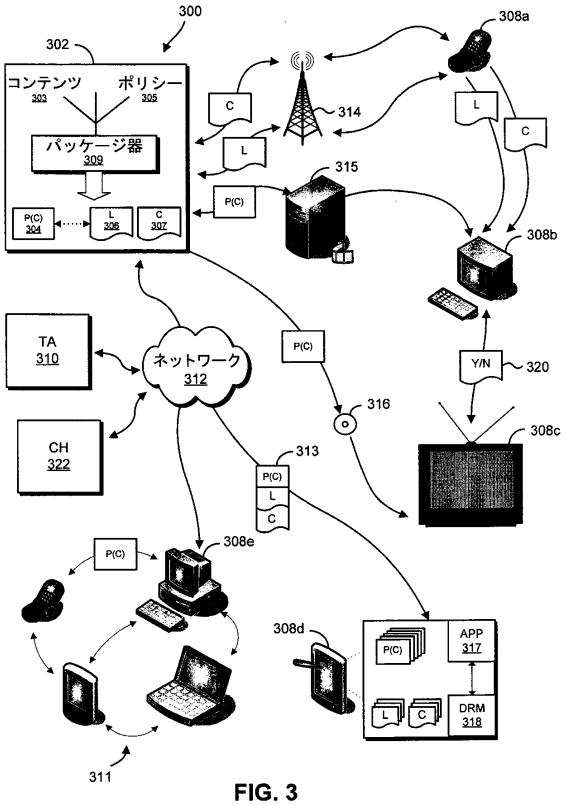

FIG. 3

【図４】

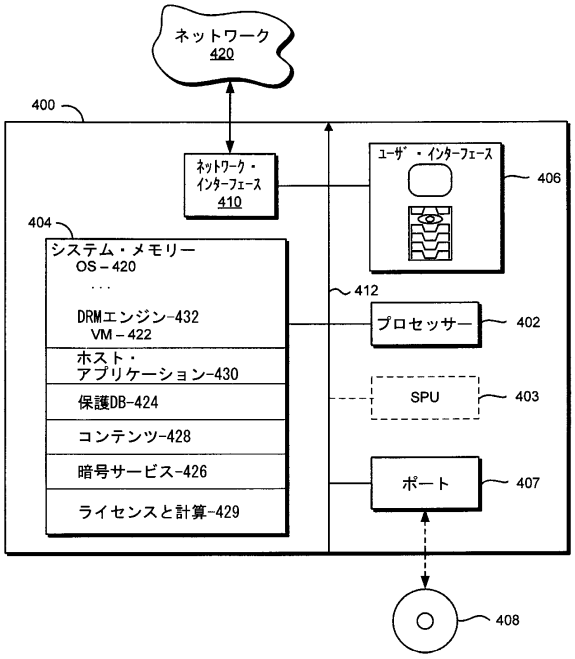
ネットワーク
420
400
ネットワーク・
インターフェース
410
ユーザ・インターフェース
406
404
システム・メモリー
OS－420
・・・
DRMエンジン-432
VM－422
ホスト・
アプリケーション-430
保護DB-424
コンテンツ-428
暗号サービス-426
ライセンスと計算-429
412
プロセッサー
402
SPU
403
ポート
407
408

FIG. 4

フロントページの続き

(72)発明者　ダブリュ．ノックス　キャリー
アメリカ合衆国，カリフォルニア　９４０４３，マウンテン　ビュー，ステアリン　ロード　４０８
(72)発明者　ジャール　ニルソン
アメリカ合衆国，カリフォルニア　９４０４３，マウンテン　ビュー，セントラル　アベニュ　４６３

審査官　宮司　卓佳

(56)参考文献　特開２００７－０６６３０２（ＪＰ，Ａ）
特開２００２－２０７６３７（ＪＰ，Ａ）
特表２００９－５０８２４０（ＪＰ，Ａ）
特開２００９－０２６０１３（ＪＰ，Ａ）
特開２００５－２５９０１５（ＪＰ，Ａ）
特開２００３－２２８５６０（ＪＰ，Ａ）
特開２００６－１８５３１１（ＪＰ，Ａ）
特開平１１－１４３８７１（ＪＰ，Ａ）
特開２００９－１７６２５３（ＪＰ，Ａ）
特表２００５－５１５７２４（ＪＰ，Ａ）
米国特許出願公開第２００９／０１１２８６７（ＵＳ，Ａ１）
特開２００４－２８７９９４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００－２１／８８