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

特許第5757536号
(P5757536)

(45)発行日　平成27年7月29日(2015.7.29)　(24)登録日　平成27年6月12日(2015.6.12)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601A
G06F 21/10	(2013.01)	G06F	21/10	
G09C 1/00	(2006.01)	G09C	1/00	660D
		G09C	1/00	650Z

請求項の数 16　(全 109 頁)

(21)出願番号	特願2012-511985 (P2012-511985)
(86)(22)出願日	平成22年5月19日 (2010.5.19)
(65)公表番号	特表2012-527838 (P2012-527838A)
(43)公表日	平成24年11月8日 (2012.11.8)
(86)国際出願番号	PCT/US2010/035377
(87)国際公開番号	WO2010/135412
(87)国際公開日	平成22年11月25日 (2010.11.25)
審査請求日	平成25年5月8日 (2013.5.8)
(31)優先権主張番号	61/179,481
(32)優先日	平成21年5月19日 (2009.5.19)
(33)優先権主張国	米国(US)

前置審査

(73)特許権者　512252526
セキュリティー　ファースト　コープ.
アメリカ合衆国　カリフォルニア　９２６８８，　ランチョ　サンタ　マルガリータ，　サンタ　マルガリータ　パークウェイ　２９８１１，　スイート　６００

(74)代理人　100078282
弁理士　山本　秀策

(74)代理人　100113413
弁理士　森下　夏樹

(74)代理人　100181674
弁理士　飯田　貴敏

(74)代理人　100181641
弁理士　石川　大輔

最終頁に続く

(54)【発明の名称】クラウド内にデータを確保するシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

クラウドコンピューティング記憶ネットワークを使用して、データを確保する方法であって、該方法は、

第１のシステムにおいて、データセットから少なくとも２つのデータ部分を生成することと、

該少なくとも２つのデータ部分を、通信ネットワーク上で該第１のシステムから該クラウドコンピューティング記憶ネットワークまで伝達することであって、該クラウドコンピューティング記憶ネットワークは、少なくとも２つの記憶デバイスを含み、該少なくとも２つの記憶デバイスのそれぞれは、該第１のシステムから遠隔に配置され、該クラウドコンピューティング記憶ネットワークは、他のネットワーク記憶デバイスに記憶されたデータから再生される置換データ部分を記憶するための少なくとも１つのネットワーク接続された記憶デバイスをさらに備え、該置換データ部分は、該データセットを露出することなく、かつ、該少なくとも２つの記憶デバイスのいずれかの故障の検出に応答して、再生され、それにより、該クラウドコンピューティング記憶ネットワークに復元力があるようにする、ことと、

該クラウドコンピューティング記憶ネットワーク内において該少なくとも２つのデータ部分を該少なくとも２つの記憶デバイスに記憶することであって、それにより、該データセットは、全部よりは少ない閾値数のデータ部分を備えるサブセットから、該サブセットからのデータを再結合することによって復元可能である、ことと

を含む、方法。
【請求項２】
前記少なくとも２つのデータ部分を生成することと、該少なくとも２つのデータ部分を前記クラウドコンピューティング記憶ネットワークに伝達することは、前記第１のシステムに対して透過的である、請求項１に記載の方法。
【請求項３】
前記通信ネットワークは、安全でない公衆ネットワークを備える、請求項１に記載の方法。
【請求項４】
前記データセットは、前記第１のシステムでアクセス可能である、請求項１に記載の方法。
【請求項５】
前記データセットは、ワークグループが該データセットにアクセスすることを可能にするためのワークグループ鍵を用いて承認される任意のシステムによってアクセス可能であり、該ワークグループは、前記第１のシステムを備える、請求項１に記載の方法。
【請求項６】
仮想マシンイメージを生成することをさらに含み、それにより、該仮想マシンイメージは、前記クラウドコンピューティング記憶ネットワーク内において前記データセットにアクセスするように動作可能である、請求項１に記載の方法。
【請求項７】
前記仮想マシンイメージを第２のシステムに伝送することをさらに含み、該第２のシステムは、前記クラウドコンピューティング記憶ネットワーク内において前記データセットにアクセスするように動作可能である、請求項６に記載の方法。
【請求項８】
前記データセットは、データサービスを備え、該データサービスへの確実なアクセスは、前記クラウドコンピューティング記憶ネットワーク上で提供される、請求項１に記載の方法。
【請求項９】
クラウドコンピューティング記憶ネットワーク内にデータを確保する装置であって、該装置は、第１のシステムを備え、
該第１のシステムは、
データセットから少なくとも２つのデータ部分を生成することと、
通信ネットワーク上で、該少なくとも２つのデータ部分を該クラウドコンピューティング記憶ネットワークまで伝達することであって、該クラウドコンピューティング記憶ネットワークは、少なくとも２つの記憶デバイスを含み、該少なくとも２つの記憶デバイスのそれぞれは、該第１のシステムから遠隔に配置され、該クラウドコンピューティング記憶ネットワークは、他のネットワーク記憶デバイスに記憶されたデータから再生される置換データ部分を記憶するための少なくとも１つのネットワーク接続された記憶デバイスをさらに備え、該置換データ部分は、該データセットを露出することなく、かつ、該少なくとも２つの記憶デバイスのいずれかの故障の検出に応答して、生成され、それにより、該クラウドコンピューティング記憶ネットワークに復元力があるようにする、ことと、
該クラウドコンピューティング記憶ネットワーク内において該少なくとも２つのデータ部分を該少なくとも２つの記憶デバイスに記憶することであって、それにより、該データセットは、全部よりは少ない閾値数のデータ部分を備えるサブセットから、該サブセットからのデータを再結合することによって復元可能である、ことと、
該少なくとも２つの記憶デバイスのいずれかの故障の検出に応答して、該データセットを露出することなく、残りの記憶デバイスに記憶された該データ部分から置換データ部分を再生することと
を行うように動作可能である、装置。
【請求項１０】

前記第１のシステムは、透過的な態様で、前記少なくとも２つのデータ部分を生成するように、および該少なくとも２つのデータ部分を前記クラウドコンピューティング記憶ネットワークに伝達するように動作可能である、請求項９に記載の装置。
【請求項１１】
前記通信ネットワークは、安全でない公衆ネットワークを備える、請求項９に記載の装置。
【請求項１２】
前記第１のシステムは、前記クラウドコンピューティング記憶ネットワーク内において前記データセットにアクセスするようにさらに動作可能である、請求項９に記載の装置。
【請求項１３】
前記データセットは、ワークグループが該データセットにアクセスすることを可能にするためのワークグループ鍵を用いて承認される任意のユーザシステムによってアクセス可能であり、該ワークグループは、前記第１のシステムを備える、請求項９に記載の装置。
【請求項１４】
前記第１のシステムは、仮想マシンイメージを生成するようにさらに動作可能であり、それにより、該仮想マシンイメージは、前記クラウドコンピューティング記憶ネットワーク内において前記データセットにアクセスするように動作可能である、請求項９に記載の装置。
【請求項１５】
前記第１のシステムは、前記仮想マシンイメージを第２のシステムに伝送するようにさらに動作可能であり、該第２のシステムは、前記クラウドコンピューティング記憶ネットワーク内において前記データセットにアクセスするように動作可能である、請求項１４に記載の装置。
【請求項１６】
前記データセットは、データサービスを備え、前記第１のシステムは、前記クラウドコンピューティング記憶ネットワーク上で該データサービスに確実にアクセスするようにさらに動作可能である、請求項９に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願の相互参照）
本願は、米国仮特許出願第６１／１７９，４８１号（名称「Ｓｙｓｔｅｍｓ ａｎｄ Ｍｅｔｈｏｄｓ ｆｏｒ Ｓｅｃｕｒｉｎｇ Ｄａｔａ ｉｎ ＳＯＡ，Ｃｌｏｕｄ，ａｎｄ Ｈｉｇｈ Ｐｅｒｆｏｒｍａｎｃｅ Ｅｎｖｉｒｏｎｍｅｎｔｓ」、２００９年５月１９日出願）の利益を主張し、この出願は、その全体が本明細書に参照により援用される。
【０００２】
（発明の分野）
本発明は、一般に、クラウド内にデータを確保するシステムおよび方法に関する。本明細書で説明されるシステムおよび方法は、その全てが全体として参照することにより本明細書に組込まれる共同所有される米国特許第７，３９１，８６５号、および共同所有される米国特許出願第１１／２５８，８３９号（２００５年１０月２５日出願）、第１１／６０２，６６７号（２００６年１１月２０日出願）、第１１／９８３，３５５号（２００７年１１月７日出願）、第１１／９９９，５７５号（２００７年１２月５日出願）、第１２／１４８，３６５号（２００８年４月１８日出願）、第１２／２０９，７０３号（２００８年９月１２日出願）、第１２／３４９，８９７号（２００９年１月７日出願）、第１２／３９１，０２５号（２００９年２月２３日出願）で説明されている、他のシステムおよび方法と併せて使用されてもよい。
【背景技術】
【０００３】

現在の社会では、個人および事業が、コンピュータシステムにおいて増え続ける量の活動を行っている。専用および非専用のコンピュータネットワークを含むこれらのコンピュータシステムは、しばしば全種類の機密情報を記憶し、アーカイブに保管し、伝送している。したがって、読み取ることができないか、または損なわれる、これらのシステムにおいて記憶および伝送されるデータを確保するための高まる必要性が存在する。

【０００４】

コンピュータシステムを確保するための１つの一般的解決法は、ログインおよびパスワード機能性を提供することである。しかしながら、パスワード管理は、ヘルプデスクへの電話の大部分を占めるパスワード問題に関する電話によって、極めて費用がかかることが証明されている。また、パスワードは、例えば、強引な攻撃を介する不適切なアクセスの影響を受けやすいファイルに概して記憶されるという点で、ほとんどセキュリティを提供しない。

【０００５】

コンピュータシステムを確保するための別の解決法は、暗号インフラストラクチャを提供することである。暗号化とは、一般的に、データを不可読形式に変換または暗号化することによって、データを保護することを指す。暗号化への鍵を保有する者のみが、データを使用可能な形式に復号することができる。暗号化は、ユーザを識別し、例えば、認証を行い、アクセス権を許可し、例えば、承認を行い、デジタル証明書および署名、ならびに同等物を作成するために使用される。１つのよく知られている暗号化システムは、全員に知られている公開鍵、および個人またはその事業所有者のみに知られている秘密鍵といった、２つの鍵を使用する公開鍵システムである。概して、一方の鍵で暗号化された鍵は、他方の鍵で復号され、いずれの鍵も他方からは再作成可能ではない。

【０００６】

残念ながら、前述の一般的な公開鍵暗号システムは、依然としてセキュリティについてユーザに依存している。例えば、暗号システムは、例えば、ユーザのブラウザを介して秘密鍵をユーザに発行する。次いで、単純なユーザは、概して、例えば、インターネット等の開放型コンピュータシステムを介して他者にアクセス可能なハードドライブ上に秘密鍵を記憶する。他方で、ユーザは、例えば、秘密鍵を含有するファイルに対して、「鍵」等の貧弱な名前を選択する場合がある。先述および他の行為の結果は、１つまたは複数の鍵にセキュリティ侵害の影響を受けやすくさせることである。

【０００７】

先述のセキュリティ侵害に加えて、ユーザは、潜在的に複数のコンピュータ記憶デバイスまたは他のシステムを通って進行する秘密鍵のコピーをもたらす、アーカイビングまたはバックアップシステムを伴って構成されたコンピュータシステム上に自分の秘密鍵を保存する場合がある。このセキュリティ違反はしばしば、「鍵移動」と呼ばれる。鍵移動と同様に、多くのアプリケーションは、最大でも、単純なログインおよびパスワードアクセスを介して、ユーザの秘密鍵へのアクセスを提供する場合がある。前述のように、ログインおよびパスワードアクセスはしばしば、十分なセキュリティを提供しない。

【０００８】

前述の暗号システムのセキュリティを増大させるための１つの解決法は、認証または承認の一部として生体測定を含むことである。生体測定は、概して、例えば、指紋パターンまたは発話パターンのパターン照合または認識等の自動システムによってチェックすることができる、例えば、指紋または発話等の測定可能な身体的特性を含む。そのようなシステムでは、ユーザの生体測定および／または鍵が、例えば、スマートカード、ラップトップ、携帯情報端末、または携帯電話等の携帯コンピュータデバイス上に記憶されてもよく、それにより、生体測定または鍵が移動環境で使用できることを可能にする。

【０００９】

前述の携帯生体測定暗号システムは、依然として種々の欠点を抱えている。例えば、携帯ユーザが、スマートカードまたは携帯用コンピュータデバイスを紛失または破損し、それにより、潜在的に重要なデータへのアクセスを完全に遮断させる場合がある。代替とし

て、悪意のある個人が、携帯ユーザのスマートカードまたは携帯用コンピュータデバイスを盗み、携帯ユーザのデジタル信任状を効果的に盗むためにそれを使用する場合がある。他方で、携帯用コンピュータデバイスは、インターネット等の開放型システムに接続される場合があり、パスワードのように、生体測定が記憶されるファイルが、ユーザのセキュリティへの不注意または悪意のある侵入者を通したセキュリティ侵害の影響を受けやすくなる場合がある。

【発明の概要】

【発明が解決しようとする課題】

【００１０】

前述の内容に基づいて、依然として携帯ユーザを支援しながら、セキュリティがユーザ独立型である、暗号システムを提供する必要性が存在する。

【課題を解決するための手段】

【００１１】

したがって、本発明の一側面は、不正アクセスまたは使用から事実上あらゆる種類のデータを確保するための方法を提供することである。方法は、確保されるデータを解析し、２つ以上の部品または部分に分割および／または分離する１つ以上のステップを含む。方法はまた、確保されるデータを暗号化するステップも含む。データの暗号化は、データの第１の解析、分割、および／または分離の前または後に行われてもよい。加えて、暗号化ステップは、１つ以上のデータ部分について繰り返されてもよい。同様に、解析、分割、および／または分離するステップは、１つ以上のデータ部分について繰り返されてもよい。方法はまた、任意に、１つの場所または複数の場所で暗号化されている、解析、分割、および／または分離されたデータも備える。この方法はまた、任意に、承認されたアクセスまたは使用のために、確保されたデータをその元の形式に再構成または再構築するステップも含む。この方法は、方法の所望のステップを実行することが可能である、任意のコンピュータ、サーバ、エンジン、または同等物の動作に組み込まれてもよい。

【００１２】

本発明の別の側面は、不正アクセスまたは使用から事実上あらゆる種類のデータを確保するためのシステムを提供する。このシステムは、データ分割モジュール、暗号処理モジュール、および任意にデータアセンブリモジュールを備える。システムはさらに、一実施形態では、確実なデータが記憶されてもよい、１つ以上のデータ記憶設備を備えてもよい。

【００１３】

したがって、本発明の一側面は、サーバ中心の鍵を有するか、または言い換えれば、サーバ上に暗号鍵およびユーザ認証データを記憶する確実なサーバまたは信頼エンジンを提供することである。この実施形態によれば、ユーザは、例えば、認証、承認、デジタル署名および生成、記憶、および証明書の回収、暗号化、公証および委任状のような措置、および同等物等であるが、それらに限定されない、認証および暗号機能を果たすために、信頼エンジンにアクセスする。

【００１４】

本発明の別の側面は、信頼性があるか、または信頼されている認証プロセスを提供することである。また、信頼できる肯定的な認証後に、システムまたはデバイス承認およびアクセスに暗号技術を提供することから、多数の電子デバイスのうちの１つの使用または制御を許可することまで、多数の異なる措置が講じられてもよい。

【００１５】

本発明の別の側面は、暗号鍵および認証データが紛失、盗難、または侵害されない環境においてそれらを提供し、それにより、新しい鍵および認証データを継続的に再発行し、管理する必要性を有利に回避することである。本発明の別の側面によれば、信頼エンジンは、ユーザが、複数の活動、ベンダ、および／または認証要求に１つの鍵ペアを使用することを可能にする。本発明のさらに別の側面によれば、信頼エンジンは、サーバ側で暗号化、認証、または署名すること等であるが、それに限定されない、暗号処理の少なくとも

１つのステップを行い、それにより、クライアントまたはユーザが最小限のコンピューティングリソースのみを保有することを可能にする。

【００１６】

本発明のさらに別の側面によれば、信頼エンジンは、各暗号鍵および認証データの複数部分を記憶するための１つまたは複数の保管場所を含む。該部分は、１つの保管場所の中の１つより多くの場所から、または複数の保管場所からの所定の部分を伴わない再構築を禁止するデータ分割プロセスを介して作成される。別の実施形態によれば、複数の保管場所は、１つの保管場所における不正従業員、またはそうでなければ欠陥システムが、ユーザの鍵または認証データへのアクセスを提供しないように、地理的に遠隔にあってもよい。

【００１７】

さらに別の実施形態によれば、認証プロセスは、信頼エンジンが複数の認証活動を並行して処理することを有利に可能にする。さらに別の実施形態によれば、信頼エンジンは、失敗したアクセス試行を有利に追跡し、それにより、悪意のある侵入者がシステムを妨害しようとし得る回数を制限してもよい。

【００１８】

さらに別の実施形態によれば、信頼エンジンは、各信頼エンジンが処理負荷を予測し、他のエンジンと共有してもよい複数のインスタンス化を含んでもよい。さらに別の実施形態によれば、信頼エンジンは、１つより多くのシステムがユーザを認証することを確実にするように、複数の認証結果をポールするための冗長性モジュールを含んでもよい。

【００１９】

したがって、本発明の一側面は、複数のユーザと関連付けられる複数の秘密暗号鍵を含むが、それらに限定されない任意の種類のデータを記憶するために遠隔でアクセス可能であり得る確実な暗号システムを含む。暗号システムは、複数のユーザの各々を複数の秘密暗号鍵からの１つ以上の異なる鍵と関連付け、複数の秘密暗号鍵をユーザに公開することなく、関連付けられた１つ以上の異なる鍵を使用して、各ユーザに対して暗号機能を果たす。暗号システムは、複数の秘密暗号鍵および複数の登録認証データ等の確保されるデータを記憶する少なくとも１つのサーバを有する保管場所システムを備える。各登録認証データは、複数のユーザのうちの１人を識別し、複数のユーザのそれぞれは、複数の秘密暗号鍵からの１つ以上の異なる鍵と関連付けられる。暗号システムはまた、複数のユーザのうちの１人によって受信された認証データを、複数のユーザのうちの１人に対応し、保管場所システムから受信された登録認証データと比較し、それにより、認証結果を生じる認証エンジンを備えてもよい。暗号システムはまた、認証結果が複数のユーザのうちの１人の適正な識別を示すときに、保管場所システムから受信された、関連付けられた１つ以上の異なる鍵を使用して、複数のユーザのうちの１人に代わって暗号機能を果たす暗号エンジンを備えてもよい。暗号システムはまた、複数のユーザから保管場所サーバシステム、認証エンジン、および暗号エンジンにデータを送るように接続されるトランザクションエンジンを備えてもよい。

【００２０】

本発明の別の側面は、任意に遠隔でアクセス可能である、確実な暗号システムを含む。暗号システムは、複数の登録認証データ等であるが、それらに限定されない、少なくとも１つの秘密鍵および任意の他のデータを記憶する、少なくとも１つのサーバを有する、保管場所システムを備え、各登録認証データは、おそらく複数のユーザのうちの１人を識別する。暗号システムはまた、任意に、ユーザによって受信された認証データを、ユーザに対応し、保管場所システムから受信された登録認証データと比較し、それにより、認証結果を生じる認証エンジンを備えてもよい。暗号システムはまた、認証結果がユーザの適正な識別を示すときに、保管場所システムから受信されてもよい、少なくとも該秘密鍵を使用して、ユーザに代わって暗号機能を果たす暗号エンジンを備える。暗号システムはまた、任意に、複数のユーザから、保管場所サーバシステム、認証エンジン、および暗号エンジン等であるが、それらに限定されない他のエンジンまたはシステムに、データを送るよ

うに接続されるトランザクションエンジンを備えてもよい。

【００２１】

本発明の別の側面は、暗号機能を促進する方法を含む。方法は、複数のユーザからの１人のユーザを、確実なサーバ等の確実な場所に記憶された複数の秘密暗号鍵からの１つ以上の鍵と関連付けるステップを含む。方法はまた、ユーザから認証データを受信し、認証データをユーザに対応する認証データと比較し、それにより、ユーザの身元を検証するステップを含む。方法はまた、１つ以上の鍵をユーザに公開することなく、暗号機能を果たすために１つ以上の鍵を利用するステップも含む。

【００２２】

本発明の別の側面は、ユーザの登録認証データの確実な記憶を介して、ユーザを一意的に識別するための認証システムを含む。認証システムは、１つ以上のデータ記憶設備を備え、各データ記憶設備は、少なくとも１つの登録認証データ部分を記憶する、コンピュータでアクセス可能な記憶媒体を含む。認証システムはまた、１つまたは複数のデータ記憶設備と通信する、認証エンジンも備える。認証エンジンは、複数部分を作成するように登録認証データに作用する、データ分割モジュールと、登録認証データを集約するようにデータ記憶設備のうちの少なくとも１つからの複数部分を処理する、データ集約モジュールと、ユーザから現在の認証データを受信し、現在の認証データを集約した登録認証データと比較して、ユーザが一意的に識別されたかどうかを決定する、データコンパレータモジュールとを備える。

【００２３】

本発明の別の側面は、暗号システムを含む。暗号システムは、１つ以上のデータ記憶設備を備え、各データ記憶設備は、１つ以上の暗号鍵の少なくとも一部分を記憶する、コンピュータでアクセス可能な記憶媒体を含む。暗号システムはまた、データ記憶設備と通信する、認証エンジンも備える。暗号エンジンはまた、複数部分を作成するように暗号鍵に作用する、データ分割モジュールと、暗号鍵を集約するようにデータ記憶設備のうちの少なくとも１つからの複数部分を処理する、データ集約モジュールと、集約した暗号鍵を受信し、それを用いて暗号機能を果たす、暗号処理モジュールとを備える。

【００２４】

本発明の別の側面は、地理的に遠隔にある確実なデータ記憶設備に、認証データを含むがそれに限定されない任意の種類のデータを記憶し、それにより、任意の個別データ記憶設備の組成からデータを保護する方法を含む。方法は、信頼エンジンでデータを受信するステップと、第１の複合値を形成するように、信頼エンジンでデータを第１の実質的に乱数の値と組み合わせるステップと、第２の複合値を形成するように、データを第２の実質的に乱数の値と組み合わせるステップとを含む。方法は、第２の複合値との第１の実質的に乱数の値の第１のペアリングを作成するステップと、第２の実質的に乱数の値との第１の実質的に乱数の値の第２のペアリングを作成するステップと、第１の確実なデータ記憶設備に第１のペアリングを記憶するステップとを含む。方法は、第１の確実なデータ記憶設備から遠隔にある第２の確実なデータ記憶設備に第２のペアリングを記憶するステップを含む。

【００２５】

本発明の別の側面は、データを受信するステップと、第２のセットのビットを形成するように、データを第１のセットのビットと組み合わせるステップと、第４のセットのビットを形成するように、データを第３のセットのビットと組み合わせるステップとを含む認証データを含むがそれに限定されない、任意の種類のデータを記憶する方法を含む。方法はまた、第３のセットのビットとの第１のセットのビットの第１のペアリングを作成するステップも含む。方法はまた、第４のセットのビットとの第１のセットのビットの第２のペアリングを作成するステップと、第１のコンピュータでアクセス可能な記憶媒体に第１および第２のペアリングのうちの一方を記憶するステップとを含む。方法はまた、第２のコンピュータでアクセス可能な記憶媒体に第１および第２のペアリングのうちの他方を記憶するステップも含む。

【００２６】
本発明の別の側面は、地理的に遠隔にある確実なデータ記憶設備に暗号データを記憶し、それにより、任意の個別データ記憶設備の組成からデータを保護する方法を含む。方法は、信頼エンジンで暗号データを受信するステップと、第１の複合値を形成するように、信頼エンジンで暗号データを第１の実質的に乱数の値と組み合わせるステップと、第２の複合値を形成するように、暗号データを第２の実質的に乱数の値と組み合わせるステップとを含む。方法はまた、第２の複合値との第１の実質的に乱数の値の第１のペアリングを作成するステップと、第２の実質的に乱数の値との第１の実質的に乱数の値の第２のペアリングを作成するステップと、第１の確実なデータ記憶設備に第１のペアリングを記憶するステップとを含む。方法はまた、第１の確実なデータ記憶設備から遠隔にある第２の確実なデータ記憶設備に第２のペアリングを記憶するステップも含む。

【００２７】
本発明の別の側面は、認証データを受信するステップと、第２のセットのビットを形成するように、暗号データを第１のセットのビットと組み合わせるステップとを含む、暗号データを記憶する方法を含む。方法はまた、第４のセットのビットを形成するように、暗号データを第３のセットのビットと組み合わせるステップと、第３のセットのビットとの第１のセットのビットの第１のペアリングを作成するステップと、第４のセットのビットとの第１のセットのビットの第２のペアリングを作成するステップとを含む。方法は、また、第１のコンピュータでアクセス可能な記憶媒体に第１および第２のペアリングのうちの一方を記憶するステップと、第２のコンピュータでアクセス可能な記憶媒体に第１および第２のペアリングのうちの他方を記憶するステップとを含む。

【００２８】
本発明の別の側面は、暗号システムにおいて、任意の種類または形態の機密データを処理する方法を含み、機密データは、機密データを採用する承認ユーザによる動作中のみに、使用可能な形態で存在する。方法はまた、第１のコンピュータでアクセス可能な記憶媒体から、実質的に無作為化または暗号化された機密データをソフトウェアモジュールで受信するステップと、１つ以上の他のコンピュータでアクセス可能な記憶媒体から、機密データであってもなくてもよい、実質的に無作為化または暗号化されたデータをソフトウェアモジュールで受信するステップとを含む。方法はまた、機密データを集約するように、実質的に無作為化された事前暗号化機密データ、および機密データであってもなくてもよい、実質的に無作為化または暗号化されたデータを、ソフトウェアモジュールで処理するステップと、措置を行うために、ソフトウェアエンジンで機密データを採用するステップとを含む。措置は、ユーザを認証するステップおよび暗号機能を果たすステップのうちの１つを含むが、それに限定されない。

【００２９】
本発明の別の側面は、確実な認証システムを含む。確実な認証システムは、複数の認証エンジンを備える。各認証エンジンは、ある程度の確実性までユーザを一意的に識別するように設計されている登録認証データを受信する。各認証エンジンは、現在の認証データを受信して登録認証データと比較し、各認証エンジンは、認証結果を決定する。確実な認証システムはまた、認証エンジンのうちの少なくとも２つの認証結果を受信し、ユーザが一意的に識別されているかどうかを決定する、冗長性システムも備える。

【００３０】
本発明の別の側面は、運動システムに確実なデータを含み、それにより、データは、損なわれている任意の一部分が元のデータを修復するのに十分なデータを提供しないように、本発明に従って確保される異なる部分で伝送されてもよい。これは、有線であろうと、無線であろうと、物理的であろうと、任意のデータの伝送に適用されてもよい。

【００３１】
本発明の別の側面は、データが記憶または伝達される任意の好適なシステムへの本発明の確実なデータパーサの統合を含む。例えば、Ｅメールシステム、ＲＡＩＤシステム、ビデオ放送システム、データベースシステム、または任意の好適なシステムが、任意の好適

なレベルで統合された確実なデータパーサを有してもよい。

【００３２】

本発明の別の側面は、データのシェアを生成するために、任意の好適な解析および分割アルゴリズムを使用するステップを含む。乱数、擬似乱数、決定論的、またはそれらの任意の組み合わせが、データを解析および分割するために採用されてもよい。

【００３３】

本発明の別の側面は、データがクラウドコンピューティングリソースに記憶されるか、またはそれと伝達される、任意の好適なシステムへの本発明の確実なデータパーサの統合を含む。確実なデータパーサは、クラウドに記憶されたデータを確保するため、およびクラウドにおいて提供されたデータサービスを確保するために使用されてもよい。クラウドにおけるネットワークアクセスは、ユーザと関心のコミュニティとの間の確実な通信を促進するように確保されてもよい。いくつかの実施形態では、クラウドコンピューティングリソースへの確実なアクセスを提供するように、仮想マシンイメージがユーザに送信されてもよい。

【００３４】

本発明の別の側面は、データネットワークを確保するための任意の好適なシステムへの本発明の確実なデータパーサの統合を含む。確実なデータパーサは、無線上の広帯域または送電線上の広帯域等の直交周波数分割多重（ＯＦＤＭ）ネットワークを確保するために使用されてもよい。確実なデータパーサはまた、電力網等の重要なインフラストラクチャシステムへのアクセスを確保するために使用されてもよい。

本願明細書は、例えば、以下の項目も提供する。

（項目１）

クラウドコンピューティング記憶ネットワークを使用して、データを確保する方法であって、該方法は、

第１のシステムにおいて、データセットから少なくとも２つのデータ部分を生成することと、

該少なくとも２つのデータ部分を、通信ネットワーク上で該第１のシステムから該クラウドコンピューティング記憶ネットワークまで伝達することであって、該クラウドコンピューティング記憶ネットワークは、少なくとも２つのそれぞれに遠隔の記憶デバイスを含む、ことと、

該クラウドコンピューティング記憶ネットワーク内の該少なくとも２つのデータ部分を該少なくとも２つのネットワーク接続された記憶デバイスに記憶することであって、それにより、該データセットは、該少なくとも２つのデータ部分の少なくとも１つのサブセットからデータを再結合することによって、該少なくとも２つのデータ部分の該サブセットから復元可能である、ことと

を含む、方法。

（項目２）

前記少なくとも２つのデータ部分を生成し、該少なくとも２つのデータ部分をクラウドコンピューティングネットワークに伝達することは、前記第１のシステムには実質的に見えない、項目１に記載の方法。

（項目３）

前記通信ネットワークは、安全でない公衆ネットワークを備える、項目１に記載の方法。

（項目４）

前記データセットは、前記第１のシステムにおいてアクセス可能である、項目１に記載の方法。

（項目５）

前記データセットは、前記第１のシステムと関連付けられる関心のコミュニティ内の任意のシステムによってアクセス可能である、項目１に記載の方法。

（項目６）

仮想マシンイメージを生成することをさらに含み、それにより、該仮想マシンイメージは、前記クラウドコンピューティング記憶ネットワーク内において前記データセットにアクセスするように動作可能である、項目１に記載の方法。
（項目７）
前記仮想マシンイメージを第２のシステムに伝送することをさらに含み、該第２のシステムは、前記クラウドコンピューティング記憶ネットワーク内において前記データセットにアクセスするように動作可能である、項目６に記載の方法。
（項目８）
前記データセットは、データサービスを備え、該データサービスへの確実なアクセスは、前記クラウドコンピューティング記憶ネットワーク上で提供される、項目１に記載の方法。
（項目９）
前記クラウドコンピューティング記憶ネットワークは、少なくとも１つの復元力のあるネットワーク接続された記憶デバイスを備える、項目１に記載の方法。
（項目１０）
前記少なくとも１つの復元力のあるネットワーク接続された記憶デバイスに記憶されたデータ部分は、他のネットワーク接続された記憶デバイスから再生される、項目９に記載の方法。
（項目１１）
直交周波数分割多重（ＯＦＤＭ）ネットワークを使用してデータを確保する方法であって、該方法は、
第１の場所において、データセットから少なくとも２つのデータ部分を生成することと、
少なくとも２つのＯＦＤＭチャネル上で、該少なくとも２つのデータ部分を該第１の場所から第２の場所まで伝達することであって、異なるデータ部分は、異なるＯＦＤＭチャネル上で伝達され、それにより、該データセットは、該少なくとも２つのＯＦＤＭチャネル上で受信された該少なくとも２つのデータ部分の少なくとも１つのサブセットからデータを再結合することによって、該少なくとも２つのデータ部分の該サブセットから該第の２の場所において復元可能である、ことと
を含む、方法。
（項目１２）
前記ＯＦＤＭネットワークは、広帯域無線ネットワークを備える、項目１１に記載の方法。
（項目１３）
前記ＯＦＤＭネットワークは、広帯域送電線ネットワークを備える、項目１１に記載の方法。
（項目１４）
クラウドコンピューティング記憶ネットワーク内にデータを確保する装置であって、該装置は、第１のシステムを備え、
該第１のシステムは、
データセットから少なくとも２つのデータ部分を生成することと、
通信ネットワーク上で、該少なくとも２つのデータ部分を該クラウドコンピューティング記憶ネットワークまで伝達することであって、該クラウドコンピューティング記憶ネットワークは、少なくとも２つのそれぞれに遠隔の記憶デバイスを含む、ことと、
該クラウドコンピューティング記憶ネットワーク内において該少なくとも２つのデータ部分を該少なくとも２つの記憶デバイスに記憶することであって、それにより、該データセットは、該少なくとも２つのデータ部分の少なくとも１つのサブセットからデータを再結合することによって、該少なくとも２つのデータ部分の該サブセットから復元可能である、ことと
を行うように動作可能である、装置。

（項目１５）
前記第１のシステムは、実質的に透明な態様で、前記少なくとも２つのデータ部分を生成するように、および該少なくとも２つのデータ部分をクラウドコンピューティングネットワークに伝達するように動作可能である、項目１４に記載の装置。
（項目１６）
前記通信ネットワークは、安全でない公衆ネットワークを備える、項目１４に記載の装置。
（項目１７）
前記第１のシステムは、前記クラウドコンピューティングネットワーク内の前記データセットにアクセスするように動作可能である、項目１４に記載の装置。
（項目１８）
前記データセットは、前記第１のシステムと関連付けられる関心のコミュニティ内の任意のユーザシステムによってアクセス可能である、項目１４に記載の装置。
（項目１９）
前記第１のシステムは、仮想マシンイメージを生成するようにさらに動作可能であり、それにより、該仮想マシンイメージは、前記クラウドコンピューティング記憶ネットワーク内の前記データセットにアクセスするように動作可能である、項目１４に記載の装置。
（項目２０）
前記第１のシステムは、前記仮想マシンイメージを第２のシステムに伝送するようにさらに動作可能であり、該第２のシステムは、前記クラウドコンピューティング記憶ネットワーク内の前記データセットにアクセスするように動作可能である、項目１９に記載の装置。
（項目２１）
前記データセットは、データサービスを備え、前記第１のシステムは、前記クラウドコンピューティング記憶ネットワーク上で該データサービスに確実にアクセスするようにさらに動作可能である、項目１４に記載の装置。
（項目２２）
前記クラウドコンピューティング記憶ネットワークは、少なくとも１つの復元力のあるネットワーク接続された記憶デバイスをさらに備える、項目１４に記載の装置。
（項目２３）
前記第１のシステムは、他のネットワーク接続された記憶デバイスから、前記少なくとも１つの復元力のあるネットワーク接続された記憶デバイスに記憶されたデータ部分を再生するようにさらに動作可能である、項目２２に記載の装置。
（項目２４）
直交周波数分割多重（ＯＦＤＭ）ネットワーク内にデータを確保する装置であって、該装置は、
第１の場所において、データセットから少なくとも２つのデータ部分を生成するように動作可能である確実なデータパーサと、
少なくとも２つのＯＦＤＭチャネル上で、該少なくとも２つのデータ部分を該第１の場所から第２の場所まで伝達するように動作可能であるＯＦＤＭトランシーバであって、異なるデータ部分は、異なるＯＦＤＭチャネル上で伝達され、それにより、該データセットは、該第の２の場所において、該少なくとも２つのＯＦＤＭチャネル上で受信された該少なくとも２つのデータ部分の少なくとも１つのサブセットからデータを再結合することによって、該少なくとも２つのデータ部分の該サブセットから復元可能である、ＯＦＤＭトランシーバと
を備える、装置。
（項目２５）
前記ＯＦＤＭネットワークは、広帯域無線ネットワークを備える、項目２４に記載の装置。
（項目２６）

前記ＯＦＤＭネットワークは、広帯域送電線ネットワークを備える、項目２４に記載の装置。

【図面の簡単な説明】

【００３５】

本発明は、本発明を限定せず、本発明を例示するように意図されている、添付図面に関連して、以下でより詳細に説明される。

【図１】図１は、本発明の実施形態の側面による、暗号システムのブロック図を図示する。

【図２】図２は、本発明の実施形態の側面による、図１の信頼エンジンのブロック図を図示する。

【図３】図３は、本発明の実施形態の側面による、図２のトランザクションエンジンのブロック図を図示する。

【図４】図４は、本発明の実施形態の側面による、図２の保管場所のブロック図を図示する。

【図５】図５は、本発明の実施形態の側面による、図２の認証エンジンのブロック図を図示する。

【図６】図６は、本発明の実施形態の側面による、図２の暗号エンジンのブロック図を図示する。

【図７】図７は、本発明の別の実施形態の側面による、保管場所システムのブロック図を図示する。

【図８】図８は、本発明の実施形態の側面による、データ分割プロセスのフローチャートを図示する。

【図９Ａ】図９のパネルＡは、本発明の実施形態の側面による、登録プロセスのデータフローを図示する。

【図９Ｂ】図９のパネルＢは、本発明の実施形態の側面による、相互運用性プロセスのフローチャートを図示する。

【図１０】図１０は、本発明の実施形態の側面による、認証プロセスのデータフローを図示する。

【図１１】図１１は、本発明の実施形態の側面による、署名プロセスのデータフローを図示する。

【図１２】図１２は、本発明の側面およびさらに別の実施形態による、データフローおよび暗号化／復号プロセスを図示する。

【図１３】図１３は、本発明の別の実施形態の側面による、信頼エンジンシステムの簡略化したブロック図を図示する。

【図１４】図１４は、本発明の別の実施形態の側面による、信頼エンジンシステムの簡略化したブロック図を図示する。

【図１５】図１５は、本発明の実施形態の側面による、図１４の冗長性モジュールのブロック図を図示する。

【図１６】図１６は、本発明の一側面による、認証を評価するためのプロセスを図示する。

【図１７】図１７は、本発明の図１６に図示されるような一側面による、値を認証に割り当てるためのプロセスを図示する。

【図１８】図１８は、図１７に図示されるような本発明の側面において、信頼裁定を行うためのプロセスを図示する。

【図１９】図１９は、最初のウェブベースの連絡が、両者によって署名される販売契約につながる、本発明の実施形態の側面による、ユーザとベンダとの間のサンプルトランザクションを図示する。

【図２０】図２０は、ユーザシステムにセキュリティ機能を提供する、暗号サービスプロバイダモジュールを伴うサンプルユーザシステムを図示する。

【図２１】図２１は、暗号化を用いてデータを解析、分割、および／または分離するため

のプロセス、およびデータを伴った暗号化マスター鍵の記憶を図示する。
【図２２】図２２は、暗号化を用いてデータを解析、分割、および／または分離し、データとは別に暗号化マスター鍵を記憶するためのプロセスを図示する。
【図２３】図２３は、暗号化を用いてデータを解析、分割、および／または分離するための中間鍵プロセス、およびデータを伴った暗号化マスター鍵の記憶を図示する。
【図２４】図２４は、暗号化を用いてデータを解析、分割、および／または分離し、データとは別に暗号化マスター鍵を記憶するための中間鍵プロセスを図示する。
【図２５】図２５は、少人数の作業グループとの本発明の暗号方法およびシステムの利用を図示する。
【図２６】図２６は、本発明の一実施形態による、確実なデータパーサを採用する例示的な物理的トークンセキュリティシステムのブロック図である。
【図２７】図２７は、本発明の一実施形態による、確実なデータパーサがシステムに統合される、例示的配設のブロック図である。
【図２８】図２８は、本発明の一実施形態による、運動システム内の例示的データのブロック図である。
【図２９】図２９は、本発明の一実施形態による、運動システム内の別の例示的データのブロック図である。
【図３０】図３０～３２は、本発明の一実施形態による、統合された確実なデータパーサを有する例示的システムのブロック図である。
【図３１】図３０～３２は、本発明の一実施形態による、統合された確実なデータパーサを有する例示的システムのブロック図である。
【図３２】図３０～３２は、本発明の一実施形態による、統合された確実なデータパーサを有する例示的システムのブロック図である。
【図３３】図３３は、本発明の一実施形態による、データを解析および分割するための例示的プロセスのプロセスフロー図である。
【図３４】図３４は、本発明の一実施形態による、データ部分を元のデータに修復するための例示的プロセスのプロセスフロー図である。
【図３５】図３５は、本発明の一実施形態による、ビットレベルでデータを分割するための例示的プロセスのプロセスフロー図である。
【図３６】図３６は、本発明の一実施形態による、任意の好適な追加、削除、または修正とともに、任意の好適な組み合わせで使用されてもよい、例示的なステップおよび特徴のプロセスフロー図である。
【図３７】図３７は、本発明の一実施形態による、任意の好適な追加、削除、または修正とともに、任意の好適な組み合わせで使用されてもよい、例示的なステップおよび特徴のプロセスフロー図である。
【図３８】図３８は、本発明の一実施形態による、任意の好適な追加、削除、または修正とともに、任意の好適な組み合わせで使用されてもよい、シェア内の鍵およびデータ構成要素の記憶の簡略化したブロック図である。
【図３９】図３９は、本発明の一実施形態による、任意の好適な追加、削除、または修正とともに、任意の好適な組み合わせで使用されてもよい、ワークグループ鍵を使用するシェア内の鍵およびデータ構成要素の記憶の簡略化したブロック図である。
【図４０】図４０Ａおよび４０Ｂは、本発明の一実施形態による、任意の好適な追加、削除、または修正とともに、任意の好適な組み合わせで使用されてもよい、運動中のデータに対するヘッダ生成およびデータ分割の簡略化した例示的なプロセスフロー図である。
【図４１】図４１は、本発明の一実施形態による、任意の好適な追加、削除、または修正とともに、任意の好適な組み合わせで使用されてもよい、例示的シェア形式の簡略化したブロック図である。
【図４２】図４２は、本発明の一実施形態による、確実なデータパーサが、クラウドコンピューティングリソースに接続されたシステムに統合されている、例示的配設のブロック図である。

【図４３】図４３は、本発明の一実施形態による、確実なデータパーサが、クラウドを介してデータを送信するためのシステムに統合されている、例示的配設のブロック図である。
【図４４】図４４は、本発明の一実施形態による、確実なデータパーサが、クラウド内でデータサービスを確保するために使用される、例示的配設のブロック図である。
【図４５】図４５は、本発明の一実施形態による、確実なデータパーサが、クラウド内でデータ記憶を確保するために使用される、例示的配設のブロック図である。
【図４６】図４６は、本発明の一実施形態による、確実なデータパーサが、ネットワークアクセス制御を確保するために使用される、例示的配設のブロック図である。
【図４７】図４７は、本発明の一実施形態による、確実なデータパーサが、高性能コンピューティングリソースを確保するために使用される、例示的配設のブロック図である。
【図４８】図４８は、本発明の一実施形態による、確実なデータパーサが、仮想マシンを使用したアクセスを確保するために使用される、例示的配設のブロック図である。
【図４９】図４９および５０は、本発明の一実施形態による、仮想マシンを使用してアクセスを確保するための代替的な例示的配設のブロック図を示す。
【図５０】図４９および５０は、本発明の一実施形態による、仮想マシンを使用してアクセスを確保するための代替的な例示的配設のブロック図を示す。
【図５１】図５１は、本発明の一実施形態による、確実なデータパーサが、直交周波数分割多重（ＯＦＤＭ）ネットワークを確保するために使用される、例示的配設のブロック図である。
【図５２】図５２は、本発明の一実施形態による、確実なデータパーサが、電力網を確保するために使用される、例示的配設のブロック図である。
【発明を実施するための形態】
【００３６】
本発明の一側面は、１つ以上の確実なサーバ、または信頼エンジンが、暗号鍵およびユーザ認証データを記憶する暗号システムを提供する。ユーザは、信頼エンジンへのネットワークアクセスを介して、従来の暗号システムの機能性にアクセスするが、信頼エンジンは、実際の鍵および他の認証データを公開せず、したがって、鍵およびデータは安全な状態のままである。この鍵および認証データのサーバ中心の記憶は、ユーザ独立型セキュリティ、可搬性、可用性、および単純性を提供する。
【００３７】
ユーザが、ユーザおよび文書認証および他の暗号機能を行うのに暗号システムを確信または信頼できるために、多種多様な機能性がシステムに組み込まれてもよい。例えば、信頼エンジンプロバイダは、例えば、同意当事者を認証し、当事者を代理または代表して同意にデジタル署名し、各当事者によってデジタル署名された同意の記録を記憶することによって、同意に対する拒否を確実にすることができる。加えて、暗号システムは、同意を監視し、例えば、価格、ユーザ、ベンダ、地理的な場所、使用場所、または同等物などに基づいて、様々な程度の認証を適用することを決定してもよい。
【００３８】
本発明の完全な理解を容易にするために、発明を実施するための形態の残りの部分は、類似要素が全体を介して類似数字によって参照される図を参照して、本発明を説明する。
【００３９】
図１は、本発明の実施形態の側面による、暗号システム１００のブロック図を図示する。図１に示されるように、暗号システム１００は、通信リンク１２５を介して通信する、ユーザシステム１０５、信頼エンジン１１０、証明機関１１５、およびベンダシステム１２０を含む。
【００４０】
本発明の一実施形態によれば、ユーザシステム１０５は、例えば、Ｉｎｔｅｌベースのプロセッサ等の１つ以上のマイクロプロセッサを有する、従来の汎用コンピュータを備える。また、ユーザシステム１０５は、Ｗｉｎｄｏｗｓ（登録商標）、Ｕｎｉｘ（登録商標

）、Ｌｉｎｕｘ（登録商標）、または同等物等の、例えば、図形またはウィンドウを含むことが可能なオペレーティングシステム等の適切なオペレーティングシステムを含む。図１に示されるように、ユーザシステム１０５は、生体測定デバイス１０７を含んでもよい。生体測定デバイス１０７は、ユーザの生体測定を有利に捕捉し、捕捉した生体測定を信頼エンジン１１０に転送してもよい。本発明の一実施形態によれば、生体測定デバイスは、その全てが本出願人によって所有され、その全てが参照することにより本明細書に組み込まれる、「ＲＥＬＩＥＦ　ＯＢＪＥＣＴ　ＩＭＡＧＥ　ＧＥＮＥＲＡＴＯＲ」と題された、１９９７年9月5日出願の米国特許出願第０８／９２６，２７７号、「ＩＭＡＧＩＮＧ　ＤＥＶＩＣＥ　ＦＯＲ　Ａ　ＲＥＬＩＥＦ　ＯＢＪＥＣＴ　ＡＮＤ　ＳＹＳＴＥＭ　ＡＮＤ　ＭＥＴＨＯＤ　ＯＦ　ＵＳＩＮＧ　ＴＨＥ　ＩＭＡＧＥ　ＤＥＶＩＣＥ」と題された、２０００年４月２６日出願の米国特許出願第０９／５５８，６３４号、「ＲＥＬＩＥＦ　ＯＢＪＥＣＴ　ＳＥＮＳＯＲ　ＡＤＡＰＴＯＲ」と題された、１９９９年１１月５日出願の米国特許出願第０９／４３５，０１１号、および「ＰＬＡＮＡＲ　ＯＰＴＩＣＡＬ　ＩＭＡＧＥ　ＳＥＮＳＯＲ　ＡＮＤ　ＳＹＳＴＥＭ　ＦＯＲ　ＧＥＮＥＲＡＴＩＮＧ　ＡＮ　ＥＬＥＣＴＲＯＮＩＣ　ＩＭＡＧＥ　ＯＦ　Ａ　ＲＥＬＩＥＦ　ＯＢＪＥＣＴ　ＦＯＲ　ＦＩＮＧＥＲＰＲＩＮＴ　ＲＥＡＤＩＮＧ」と題された、２０００年1月5日出願の米国特許出願第０９／４７７，９４３号で開示されているものと同様の属性および特徴を有する、デバイスを有利に備えてもよい。

【００４１】

加えて、ユーザシステム１０５は、例えば、ダイヤルアップ、デジタル加入者回線（ＤＳＬ）、ケーブルモデム、ファイバ接続、または同等物等の従来のサービスプロバイダを介して、通信リンク１２５に接続してもよい。別の実施形態によれば、ユーザシステム１０５は、例えば、ローカルまたは広域ネットワーク等のネットワーク接続を介して、通信リンク１２５を接続する。一実施形態によれば、オペレーティングシステムは、通信リンク１２５上で渡される全ての着信および発信メッセージを処理する、ＴＣＰ／ＩＰスタックを含む。

【００４２】

ユーザシステム１０５が前述の実施形態を参照して開示されているが、本発明はそれによって限定されることを目的としていない。むしろ、当業者であれば、情報を送信すること、または別のコンピュータシステムから受信することが可能なほとんどあらゆるコンピュータデバイスを含む、ユーザシステム１０５の多数の代替実施形態を本明細書の本開示から認識するであろう。例えば、ユーザシステム１０５は、通信リンク１２５と相互作用することができる、コンピュータワークステーション、双方向テレビ、双方向キオスク、携帯情報端末、携帯電話、ラップトップ、または同等物等の個人用携帯コンピュータデバイス、無線通信デバイス、スマートカード、組込型コンピュータデバイス、または同等物を含んでもよいが、それらに限定されない。そのような代替システムでは、オペレーティングシステムは異なり、特定のデバイスのために適合される可能性が高い。しかしながら、一実施形態によれば、オペレーティングシステムは、通信リンク１２５との通信を確立するために必要とされる適切なプロトコルを有利に提供し続ける。

【００４３】

図１は、信頼エンジン１１０を図示する。一実施形態によれば、信頼エンジン１１０は、テキスト、音声、ビデオ、ユーザ認証データ、ならびに公開および秘密暗号鍵等であるが、それらに限定されない、任意の種類または形態のデータであってもよい、機密情報にアクセスし、記憶するための１つ以上の確実なサーバを備える。一実施形態によれば、認証データは、暗号システム１００のユーザを一意的に識別するように設計されているデータを含む。例えば、認証データは、ユーザ識別番号、１つ以上の生体測定、ならびに信頼エンジン１１０またはユーザによって生成されるが、登録時に最初にユーザによって回答される一連の質問および回答を含んでもよい。前述の質問は、出生地、住所、記念日、または同等物等の人口統計データ、母親の旧姓、好きなアイスクリーム、または同等物等の個人データ、またはユーザを一意的に識別するように設計されている他のデータを含んで

もよい。信頼エンジン１１０は、現在のトランザクションと関連付けられるユーザの認証データを、例えば、登録中等のその時以前に提供された認証データと比較する。信頼エンジン１１０は、各トランザクションのときに認証データを生成するようにユーザに有利に要求してもよく、または信頼エンジン１１０は、一連のトランザクションの開始時または特定のベンダのウェブサイトにログオンするとき等に、ユーザが認証データを周期的に生成することを有利に可能にしてもよい。

【００４４】

ユーザが生体測定データを生成する実施形態によれば、ユーザは、顔面スキャン、手スキャン、耳スキャン、虹彩スキャン、網膜スキャン、血管パターン、ＤＮＡ、指紋、筆跡、または発話等であるがそれらに限定されない、身体的特性を生体測定デバイス１０７に提供する。生体測定デバイスは、身体的特性の電子パターンまたは生体測定を有利に生成する。電子パターンは、登録または認証目的で、ユーザシステム１０５を介して信頼エンジン１１０に転送される。

【００４５】

いったんユーザが適切な認証データを生成し、信頼エンジン１１０が、認証データ（現在の認証データ）と登録時に提供された認証データ（登録認証データ）との間の肯定的な照合を決定すると、信頼エンジン１１０は、ユーザに完全な暗号機能性を提供する。例えば、適正に認証されたユーザは、ハッシング、デジタル署名、暗号化および復号（しばしば一緒に単に暗号化と呼ばれる）、デジタル証明書の作成および配布、ならびに同等物を行うために、信頼エンジン１１０を有利に採用してもよい。しかしながら、暗号機能で使用される秘密暗号鍵は、信頼エンジン１１０外では使用可能とはならず、それにより、暗号鍵の完全性を確実にする。

【００４６】

一実施形態によれば、信頼エンジン１１０は、暗号鍵を生成し、記憶する。別の実施形態によれば、少なくとも１つの暗号鍵は、各ユーザと関連付けられる。また、暗号鍵は、公開鍵技術を含み、ユーザと関連付けられる各秘密鍵は、信頼エンジン１１０内で生成され、そこから公開されない。したがって、ユーザが信頼エンジン１１０にアクセスできる限り、ユーザは、自分の秘密または公開鍵を使用して暗号機能を果たし得る。そのような遠隔アクセスは、ユーザが完全に移動性のままであり、携帯または衛星電話、キオスク、ラップトップ、ホテルの部屋、および同等物等の事実上あらゆるインターネット接続を介して暗号機能にアクセスすることを有利に可能にする。

【００４７】

別の実施形態によれば、信頼エンジン１１０は、信頼エンジン１１０に生成された鍵ペアを使用して、暗号機能性を果たす。この実施形態によれば、信頼エンジン１１０は、最初にユーザを認証し、ユーザが登録認証データに合致する認証データを適正に生成した後、信頼エンジン１１０は、認証されたユーザに代わって暗号機能を果たすために独自の暗号鍵ペアを使用する。

【００４８】

当業者であれば、暗号鍵が、対称鍵、公開鍵、および秘密鍵のうちのいくつかまたは全てを有利に含んでもよいことを本明細書の本開示から認識するであろう。加えて、当業者であれば、前述の鍵が、例えば、ＲＳＡ、ＥＬＧＡＭＡＬ、または同等物等の商業用技術から入手可能な多数のアルゴリズムを用いて実装されてもよいことを本明細書の本開示から認識するであろう。

【００４９】

図１はまた、証明機関１１５も図示する。一実施形態によれば、証明機関１１５は、例えば、ＶｅｒｉＳｉｇｎ、Ｂａｌｔｉｍｏｒｅ、Ｅｎｔｒｕｓｔ、または同等物等のデジタル証明書を発行する、信頼できる第三者組織または企業を有利に備えてもよい。信頼エンジン１１０は、例えば、ＰＫＣＳ１０等の１つ以上の従来のデジタル証明書プロトコルを介して、デジタル証明書の要求を証明機関１１５に有利に伝送してもよい。それに応じて、証明機関１１５は、例えば、ＰＫＣＳ７等のいくつかの異なるプロトコルのうちの１

つ以上で、デジタル証明書を発行する。本発明の一実施形態によれば、信頼エンジン１１０が、任意の要求当事者の証明書基準に対応するデジタル証明書にアクセスできるように、信頼エンジン１１０は、著名な証明機関１１５のうちのいくつかまたは全てからデジタル証明書を要求する。

【００５０】

別の実施形態によれば、信頼エンジン１１０は、証明書発行を内部で行う。この実施形態では、信頼エンジン１１０は、証明書を生成するための証明書システムにアクセスしてもよく、および／または、例えば、鍵生成時等の要求されたときに、または要求時に要求された証明書基準で、証明書を内部で生成してもよい。信頼エンジン１１０を以下でより詳細に開示する。

【００５１】

図１はまた、ベンダシステム１２０も図示する。一実施形態によれば、ベンダシステム１２０は、ウェブサーバを有利に備える。一般的なウェブサーバは、概して、ハイパーテキストマークアップ言語（Ｈｙｐｅｒ－Ｔｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ／ＨＴＭＬ）または拡張可能マークアップ言語（Ｅｘｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ／ＸＭＬ）等のいくつかのインターネットマークアップ言語または文書形式基準のうちの１つを使用して、インターネット上でコンテンツを供給する。ウェブサーバは、ＮｅｔｓｃａｐｅおよびＩｎｔｅｒｎｅｔ Ｅｘｐｌｏｒｅｒのようなブラウザから要求を受け取り、次いで、適切な電子文書を返信する。標準電子文書を送達する能力を超えて、ウェブサーバの権限を増大させるために、いくつかのサーバまたはクライアント側技術を使用することができる。例えば、これらの技術は、共通ゲートウェイインターフェース（Ｃｏｍｍｏｎ Ｇａｔｅｗａｙ Ｉｎｔｅｒｆａｃｅ／ＣＧＩ）スクリプト、セキュアソケットレイヤー（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ／ＳＳＬ）セキュリティ、およびアクティブサーバページ（Ａｃｔｉｖｅ Ｓｅｒｖｅｒ Ｐａｇｅ／ＡＳＰ）を含む。ベンダシステム１２０は、商業用、個人用、教育用、または他のトランザクションに関する電子コンテンツを有利に提供してもよい。

【００５２】

ベンダシステム１２０が前述の実施形態を参照して開示されているが、本発明はそれによって限定されることを目的としていない。むしろ、当業者であれば、ベンダシステム１２０が、ユーザシステム１０５を参照して説明されるデバイスのうちのいずれか、またはそれらの組み合わせを有利に備えてもよいことを、本明細書の本開示から認識するであろう。

【００５３】

図１はまた、ユーザシステム１０５、信頼エンジン１１０、証明機関１１５、およびベンダシステム１２０を接続する、通信リンク１２５も図示する。一実施形態によれば、通信リンク１２５は、好ましくは、インターネットを備える。本開示の全体を介して使用されるようなインターネットは、コンピュータの世界的ネットワークである。当業者に周知である、インターネットの構造は、バックボーンから分岐するネットワークを伴うネットワークバックボーンを含む。これらの分岐は次に、それらから分岐するネットワーク等を有する。ルータは、パケットがその送信先の近隣に到達するまで、ネットワークレベル間で、次いで、ネットワークからネットワークへ情報パケットを移動させる。送信先から、送信先ネットワークのホストが、情報パケットを適切な端末またはノードに方向付ける。１つの有利な実施形態では、インターネットルーティングハブは、当技術分野で周知であるような伝送制御プロトコル／インターネットプロトコル（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ：ＴＣＰ／ＩＰ）を使用する、ドメイン名システム（ＤＮＳ）サーバを備える。ルーティングハブは、高速通信リンクを介して１つ以上の他のルーティングハブに接続する。

【００５４】

インターネットの１つの良く知られている部分は、ワールドワイドウェブである。ワールドワイドウェブは、図形およびテキスト情報を表示することが可能な文書を記憶する、

異なるコンピュータを含有する。ワールドワイドウェブ上で情報を提供するコンピュータは、一般的には、「ウェブサイト」と呼ばれる。ウェブサイトは、関連電子ページを有するインターネットアドレスによって定義される。電子ページは、ユニフォームリソースロケータ／ＵＲＬ）によって識別することができる。概して、電子ページは、テキスト、グラフィック画像、音声、ビデオ等の提示を編成する文書である。

【００５５】

通信リンク１２５がその好ましい実施形態に関して開示されているが、当業者であれば、通信リンク１２５が広範囲の通信リンクを含んでもよいことを、本明細書の本開示から認識するであろう。例えば、通信リンク１２５は、双方向テレビネットワーク、電話ネットワーク、無線データ伝送システム、両方向ケーブルシステム、カスタマイズされた秘密または公開コンピュータネットワーク、双方向キオスクネットワーク、現金自動預払機ネットワーク、直接リンク、衛星またはセルラーネットワーク、および同等物を含んでもよい。

【００５６】

図２は、本発明の実施形態の側面による、図１の信頼エンジン１１０のブロック図を図示する。図２に示されるように、信頼エンジン１１０は、トランザクションエンジン２０５と、保管場所２１０と、認証エンジン２１５と、暗号エンジン２２０とを含む。本発明の一実施形態によれば、信頼エンジン１１０はまた、大容量記憶装置２２５も含む。図２でさらに示されるように、トランザクションエンジン２０５は、大容量記憶装置２２５とともに、保管場所２１０、認証エンジン２１５、および暗号エンジン２２０と通信する。加えて、保管場所２１０は、認証エンジン２１５、暗号エンジン２２０、および大容量記憶装置２２５と通信する。また、認証エンジン２１５は、暗号エンジン２２０と通信する。本発明の一実施形態によれば、前述の通信のうちのいくつかまたは全ては、受信デバイスに対応するＩＰアドレスへのＸＭＬ文書の伝送を有利に含んでもよい。前述のように、ＸＭＬ文書は、設計者が独自のカスタマイズされた文書タグを作成することを有利に可能にし、アプリケーション間および組織間のデータの定義、伝送、検証、および解釈を可能にする。また、前述の通信のうちのいくつかまたは全ては、従来のＳＳＬ技術を含んでもよい。

【００５７】

一実施形態によれば、トランザクションエンジン２０５は、Ｎｅｔｓｃａｐｅ、Ｍｉｃｒｏｓｏｆｔ、Ａｐａｃｈｅ、または同等物から入手可能な従来のウェブサーバ等のデータルーティングデバイスを備える。例えば、ウェブサーバは、通信リンク１２５から着信データを有利に受信してもよい。本発明の一実施形態によれば、着信データは、信頼エンジン１１０用のフロントエンドセキュリティシステムにアドレス指定される。例えば、フロントエンドセキュリティシステムは、ファイアウォール、既知の攻撃プロファイルを検索する侵入検出システム、および／またはウイルススキャナを有利に含んでもよい。フロントエンドセキュリティシステムを通過した後、データはトランザクションエンジン２０５によって受信され、保管場所２１０、認証エンジン２１５、暗号エンジン２２０、および大容量記憶装置２２５のうちの１つに送られる。加えて、トランザクションエンジン２０５は、認証エンジン２１５および暗号エンジン２２０からの着信データを監視し、通信リンク１２５を介して特定のシステムにデータを送る。例えば、トランザクションエンジン２０５は、ユーザシステム１０５、証明機関１１５、またはベンダシステム１２０にデータを有利に送ってもよい。

【００５８】

一実施形態によれば、データは、例えば、ＵＲＬまたはユニフォームリソースインジケータ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｉｎｄｉｃａｔｏｒ／ＵＲＩ）を採用すること等の従来のＨＴＴＰルーティング技法を使用して送られる。ＵＲＩは、ＵＲＬと同様であるが、ＵＲＩは、一般的には、例えば、実行ファイル、スクリプト、および同等物等のファイルまたは動作源を示す。したがって、一実施形態によれば、ユーザシステム１０５、証明機関１１５、ベンダシステム１２０、および信頼エンジン２１０の構成要素は、暗

号システムの全体を介してデータを適正に送るように、トランザクションエンジン２０５の通信ＵＲＬまたはＵＲＩ内で十分なデータを有利に含む。

【００５９】

データルーティングがその好ましい実施形態に関して開示されているが、当業者であれば、多数の可能なデータルーティング解決法または方策を認識するであろう。例えば、トランザクションエンジン２０５が、信頼エンジン１１０の全体を介してデータを適正に送ってもよいように、ＸＭＬまたは他のデータパケットが、有利に解凍され、それらの形式、コンテンツ、または同等物によって認識されてもよい。また、当業者であれば、例えば、通信リンク１２５がローカルネットワークを含む時等に、データルーティングは、特定のネットワークシステムに一致するデータ転送プロトコルに有利に適合されてもよいことを認識するであろう。

【００６０】

本発明のさらに別の実施形態によれば、特定の通信中にトランザクションエンジン２０５を伴って、前述のシステムが自身を認証し、その逆も同様であるように、トランザクションエンジン２０５は、従来のＳＳＬ暗号化技術を含む。本開示の全体を介して使用されるように、「１／２ＳＳＬ」という用語は、サーバがＳＳＬ認証されるが、必ずしもクライアントはＳＳＬ認証されるとは限らない通信を指し、「ＦＵＬＬ　ＳＳＬ」という用語は、クライアントおよびサーバがＳＳＬ認証される通信を指す。本開示が「ＳＳＬ」という用語を使用する時、通信は１／２またはＦＵＬＬ　ＳＳＬを含んでもよい。

【００６１】

トランザクションエンジン２０５が暗号システム１００の種々の構成要素にデータを送るにつれて、トランザクションエンジン２０５は、オーディットトレールを有利に作成してもよい。一実施形態によれば、オーディットトレールは、暗号システム１００の全体を介してトランザクションエンジン２０５によって送られるデータの少なくとも種類および形式の記録を含む。そのようなオーディットデータは、大容量記憶装置２２５に有利に記憶されてもよい。

【００６２】

図２はまた、保管場所２１０も図示する。一実施形態によれば、保管場所２１０は、例えば、ディレクトリサーバ、データベースサーバ、または同等物等の１つ以上のデータ記憶設備を備える。図２に示されるように、保管場所２１０は、暗号鍵および登録認証データを記憶する。暗号鍵は、信頼エンジン１１０に、またはユーザあるいはベンダ等の暗号システム１００のユーザに有利に対応してもよい。登録認証データは、ユーザＩＤ、パスワード、質問への回答、生体測定データ、または同等物等のユーザを一意的に識別するように設計されているデータを有利に含んでもよい。この登録認証データは、ユーザの登録時に、または別の代替的な後の時間に、有利に取得されてもよい。例えば、信頼エンジン１１０は、登録認証データの周期的または他の更新または再発行を含んでもよい。

【００６３】

一実施形態によれば、トランザクションエンジン２０５から認証エンジン２１５および暗号エンジン２２０を往復する通信は、例えば、従来のＳＳＬ技術等の確実な通信を含む。加えて、前述のように、保管場所２１０を往復する通信のデータは、ＵＲＬ、ＵＲＩ、ＨＴＴＰ、またはＸＭＬ文書を使用して転送されてもよく、前述のうちのいずれかは、その中に組み込まれたデータ要求および形式を有利に有する。

【００６４】

上述のように、保管場所２１０は、複数の確実なデータ記憶設備を有利に備えてもよい。そのような実施形態では、確実なデータ記憶設備は、１つの個別データ記憶設備におけるセキュリティの侵害が、その中に記憶された暗号鍵または認証データを損なわないように構成されてもよい。例えば、この実施形態によれば、暗号鍵および認証データは、各データ記憶設備に記憶されたデータを統計的かつ実質的に無作為化するように数学的に操作される。一実施形態によれば、個別データ記憶設備のデータの無作為化は、そのデータを解読不可能にする。したがって、個別データ記憶設備のセキュリティ侵害は、無作為化さ

れた解読不可能な数字のみを生じさせ、任意の暗号鍵または認証データのセキュリティを全体として損なわない。

【００６５】

図２はまた、認証エンジン２１５を含む信頼エンジン１１０も図示する。一実施形態によれば、認証エンジン２１５は、トランザクションエンジン２０５からのデータを保管場所２１０からのデータと比較するように構成されるデータコンパレータを備える。例えば、認証中に、ユーザは、トランザクションエンジン２０５が現在の認証データを受信するように、現在の認証データを信頼エンジン１１０に供給する。前述のように、トランザクションエンジン２０５は、好ましくはＵＲＬまたはＵＲＩでデータ要求を認識し、認証データを認証エンジン２１５に送る。また、要求に応じて、保管場所２１０は、ユーザに対応する登録認証データを認証エンジン２１５に転送する。したがって、認証エンジン２１５は、比較のために現在の認証データおよび登録認証データの両方を有する。

【００６６】

一実施形態によれば、認証エンジンへの通信は、例えば、ＳＳＬ技術等の確実な通信を含む。加えて、例えば、公開鍵技術を使用した多重暗号化を使用して、信頼エンジン１１０の構成要素内でセキュリティを提供することができる。例えば、一実施形態によれば、ユーザは、認証エンジン２１５の公開鍵を用いて、認証データを暗号化する。加えて、保管場所２１０もまた、認証エンジン２１５の公開鍵を用いて、登録認証データを暗号化する。このようにして、伝送を復号するために、認証エンジンの秘密鍵のみを使用することができる。

【００６７】

図２に示されるように、信頼エンジン１１０はまた、暗号エンジン２２０も含む。一実施形態によれば、暗号エンジンは、例えば、公開鍵インフラストラクチャ（ＰＫＩ）機能性等の従来の暗号機能を有利に適用するように構成される暗号処理モジュールを備える。例えば、暗号エンジン２２０は、暗号システム１００のユーザ用の公開および秘密鍵を有利に発行してもよい。このようにして、少なくとも秘密暗号鍵が信頼エンジン１１０外で利用可能とならないように、暗号鍵は暗号エンジン２２０で生成され、保管場所２１０に転送される。別の実施形態によれば、暗号エンジン２２０は、少なくとも秘密暗号鍵データを無作為化して分割し、それにより、無作為化された分割データのみを記憶する。登録認証データの分割と同様に、分割プロセスは、記憶された鍵が暗号エンジン２２０外で利用可能ではないことを確実にする。別の実施形態によれば、暗号エンジンの機能は、認証エンジン２１５と組み合わせ、認証エンジン２１５によって果たすことができる。

【００６８】

一実施形態によれば、暗号エンジンを往復する通信は、ＳＳＬ技術等の確実な通信を含む。加えて、データを転送するか、および／または暗号機能要求を行うために、ＸＭＬ文書が有利に採用されてもよい。

【００６９】

図２はまた、大容量記憶装置２２５を有する信頼エンジン１１０も図示する。前述のように、トランザクションエンジン２０５は、オーディットトレールに対応するデータを保持し、大容量記憶装置２２５にそのようなデータを記憶する。同様に、本発明の一実施形態によれば、保管場所２１０は、オーディットトレールに対応するデータを保持し、大容量記憶デバイス２２５にそのようなデータを記憶する。保管場所オーディットトレールデータは、オーディットトレールデータが保管場所２１０によって受信される要求およびその応答の記録を備えるという点で、トランザクションエンジン２０５のオーディットトレールデータと同様である。加えて、大容量記憶装置２２５は、その中に含有されたユーザの公開鍵を有する、デジタル証明書を記憶するために使用されてもよい。

【００７０】

信頼エンジン１１０がその好ましい代替実施形態に関して開示されているが、本発明はそれによって限定されることを目的としていない。むしろ、当業者であれば、信頼エンジン１１０の多数の代替案を本明細書の本開示において認識するであろう。例えば、信頼エ

ンジン１１０は、認証のみ、または代替として、データ暗号化および復号等の暗号機能のうちのいくつかのみ、あるいは全てを有利に果たしてもよい。そのような実施形態によれば、認証エンジン２１５および暗号エンジン２２０のうちの１つが有利に除去されてもよく、それにより、信頼エンジン１１０にとってより単純な設計を作成する。加えて、暗号エンジン２２０はまた、証明機関が信頼エンジン１１０内で具現化されるように、証明機関と通信してもよい。さらに別の実施形態によれば、信頼エンジン１１０は、認証、および、例えば、デジタル署名等の１つ以上の暗号機能を有利に果たしてもよい。

【００７１】

図３は、本発明の実施形態の側面による、図２のトランザクションエンジン２０５のブロック図を図示する。この実施形態によれば、トランザクションエンジン２０５は、処理スレッドおよびリスニングスレッドを有するオペレーティングシステム３０５を備える。オペレーティングシステム３０５は、例えば、Ａｐａｃｈｅから入手可能なウェブサーバ等の従来の高容量サーバで見出されるものと有利に同様であってもよい。リスニングスレッドは、着信データフローについて、通信リンク１２５、認証エンジン２１５、および暗号エンジン２２０のうちの１つからの着信通信を監視する。処理スレッドは、例えば、前述のデータ構造等の着信データフローの特定のデータ構造を認識し、それにより、通信リンク１２５、保管場所２１０、認証エンジン２１５、暗号エンジン２２０、または大容量記憶装置２２５のうちの１つに着信データを送る。図３に示されるように、着信および発信データは、例えば、ＳＳＬ技術を介して、有利に確保されてもよい。

【００７２】

図４は、本発明の実施形態の側面による、図２の保管場所２１０のブロック図を図示する。この実施形態によれば、保管場所２１０は、１つ以上のライトウェイトディレクトリアクセスプロトコル（ＬＤＡＰ）サーバを備える。ＬＤＡＰディレクトリサーバは、Ｎｅｔｓｃａｐｅ、ＩＳＯ、およびその他等の多種多様な製造業者から入手可能である。図４はまた、ディレクトリサーバが、好ましくは、暗号鍵に対応するデータ４０５および登録認証データに対応するデータ４１０を記憶することも示す。一実施形態によれば、保管場所２１０は、認証データおよび暗号鍵データを一意のユーザＩＤにインデックス付けする単一の論理メモリ構造を備える。単一の論理メモリ構造は、好ましくは、その中に記憶されたデータにおいて、高度の信頼またはセキュリティを確実にする機構を含む。例えば、保管場所２１０の物理的な場所は、限定された従業員アクセス、近代的な監視システム、および同等物等の多数の従来のセキュリティ対策を有利に含んでもよい。物理的なセキュリティに加えて、またはその代わりに、コンピュータシステムまたはサーバは、記憶されたデータを保護するソフトウェアソリューションを有利に含んでもよい。例えば、保管場所２１０は、講じられた措置のオーディットトレールに対応するデータ４１５を有利に作成し、記憶してもよい。加えて、着信および発信通信は、従来のＳＳＬ技術と連結された公開鍵暗号化を用いて、有利に暗号化されてもよい。

【００７３】

別の実施形態によれば、保管場所２１０は、図７を参照してさらに開示されるように、明確に異なる物理的に分離されたデータ記憶設備を備えてもよい。

【００７４】

図５は、本発明の実施形態の側面による、図２の認証エンジン２１５のブロック図を図示する。図３のトランザクションエンジン２０５と同様に、認証エンジン２１５は、例えば、Ａｐａｃｈｅから利用可能なウェブサーバ等の従来のウェブサーバの修正版の少なくともリスニングおよび処理スレッドを有するオペレーティングシステム５０５を備える。図５に示されるように、認証エンジン２１５は、少なくとも１つの秘密鍵５１０へのアクセスを含む。秘密鍵５１０は、例えば、認証エンジン２１５の対応する公開鍵を用いて暗号化された、トランザクションエンジン２０５または保管場所２１０からのデータを復号するために、有利に使用されてもよい。

【００７５】

図５はまた、コンパレータ５１５と、データ分割モジュール５２０と、データ集約モジ

ュール５２５を備える認証エンジン２１５も図示する。本発明の好ましい実施形態によれば、コンパレータ５１５は、前述の生体測定認証データに関連する潜在的に複雑なパターンを比較することが可能な技術を含む。この技術は、例えば、指紋パターンまたは声紋を表すもの等のパターンに対するハードウェア、ソフトウェア、または複合ソリューションを含んでもよい。加えて、一実施形態によれば、認証エンジン２１５のコンパレータ５１５は、比較結果を提出するために、文書の従来のハッシュを有利に比較してもよい。本発明の一実施形態によれば、コンパレータ５１５は、比較に対するヒューリスティクス５３０の適用を含む。ヒューリスティクス５３０は、例えば、時刻、ＩＰアドレスまたはサブネットマスク、購入プロファイル、Ｅメールアドレス、プロセッサシリアル番号またはＩＤ、あるいは同等物等の認証試行を包囲する状況を有意にアドレス指定してもよい。

【００７６】

また、生体測定データ比較の性質は、登録データへの現在の生体測定認証データの照合から、様々な程度の確信を生じさせてもよい。例えば、肯定的または否定的合致のみを返信してもよい、従来のパスワードと違って、指紋は、単に正確または不正確であるかよりもむしろ、部分的合致、例えば、９０％合致、７５％合致、または１０％合致であると決定されてもよい。声紋分析または顔面認識等の他の生体測定識別子は、絶対的認証よりもむしろ、この確率的認証の性質を共有してもよい。

【００７７】

そのような確率的認証と連動するとき、または認証が決して絶対的に信頼できるとは見なされない他の場合において、ヒューリスティクス５３０を適用して、提供された認証の確信のレベルが、行われているトランザクションを認証するのに十分高いかどうかを決定することが望ましい。

【００７８】

時には、問題のトランザクションが、より低いレベルの確信に認証されることが容認可能である、比較的低い値のトランザクションである場合となる。これは、それと関連付けられた低いドル値を有するトランザクション（例えば、＄１０の購入）または低いリスクを伴うトランザクション（例えば、メンバー専用ウェブサイトへの入会）を含むことができる。

【００７９】

逆に、他のトランザクションを認証するために、トランザクションが続行することを可能にする前に、認証への高度の確信を要求することが望ましくてもよい。そのようなトランザクションは、大きいドル値のトランザクション（例えば、数百万ドルの供給契約に署名する）、または不正認証が発生した場合に高いリスクを伴うトランザクション（例えば、政府コンピュータに遠隔でログオンする）を含んでもよい。

【００８０】

確信レベルとトランザクションの値とを組み合わせたヒューリスティクス５３０の使用は、以下で説明されるように、コンパレータが動的な文脈依存認証システムを提供することを可能にするために使用されてもよい。

【００８１】

本発明の別の実施形態によれば、コンパレータ５１５は、特定のトランザクションに対する認証試行を有利に追跡してもよい。例えば、トランザクションが失敗すると、信頼エンジン１１０は、現在の認証データを再入力するようにユーザに要求してもよい。認証エンジン２１５のコンパレータ５１５は、認証試行の数を制限するために、試行リミッタ５３５を有利に採用し、それにより、ユーザの認証データに成りすます強引な試行を禁止してもよい。一実施形態によれば、試行リミッタ５３５は、認証試行を繰り返すためのトランザクションを監視し、例えば、所望のトランザクションに対する認証試行を３回に限定するソフトウェアモジュールを備える。したがって、試行リミッタ５３５は、個人の認証データに成りすます自動試行を、例えば、単に３回の「推測」に限定する。３回失敗すると、試行リミッタ５３５は、付加的な認証試行を有利に拒否してもよい。そのような拒否は、例えば、伝送されている現在の認証データにかかわらず、否定的な結果を返信するコ

ンパレータ５１５を介して、有利に実装されてもよい。他方で、トランザクションエンジン２０５は、３回の試行が以前に失敗したトランザクションに関する付加的な認証試行を有利に阻止してもよい。

【００８２】

認証エンジン２１５はまた、データ分割モジュール５２０と、データ集約モジュール５２５とを含む。データ分割モジュール５２０は、データを実質的に無作為化して複数部分に分割するように、種々のデータに数学的に作用する能力を有する、ソフトウェア、ハードウェア、または複合モジュールを有利に備える。一実施形態によれば、元のデータは、個別部分から再作成可能ではない。データ集約モジュール５２５は、前述の実質的に無作為化された部分の組み合わせが元の解読データを提供するように、それらに数学的に作用するように構成されるソフトウェア、ハードウェア、または複合モジュールを有利に備える。一実施形態によれば、認証エンジン２１５は、登録認証データを無作為化して複数部分に分割するために、データ分割モジュール５２０を採用し、複数部分を使用可能な登録認証データに再構築するためにデータ集約モジュール５２５を採用する。

【００８３】

図６は、本発明の一実施形態の側面による、図２の信頼エンジン２００の暗号エンジン２２０のブロック図を図示する。図３のトランザクションエンジン２０５と同様に、暗号エンジン２２０は、例えば、Ａｐａｃｈｅから利用可能なウェブサーバ等の従来のウェブサーバの修正版の少なくともリスニングおよび処理スレッドを有する、オペレーティングシステム６０５を備える。図６に示されるように、暗号エンジン２２０は、図５のものと同様に機能する、データ分割モジュール６１０と、データ集約モジュール６２０とを備える。しかしながら、一実施形態によれば、データ分割モジュール６１０およびデータ集約モジュール６２０は、前述の登録認証データとは対照的に、暗号鍵データを処理する。しかし、当業者であれば、データ分割モジュール９１０およびデータ分割モジュール６２０が、認証エンジン２１５のモジュールと組み合わされてもよいことを、本明細書の本開示から認識するであろう。

【００８４】

暗号エンジン２２０はまた、多数の暗号機能のうちの１つ、いくつか、または全てを果たすように構成される、暗号処理モジュール６２５も備える。一実施形態によれば、暗号処理モジュール６２５は、ソフトウェアモジュールまたはプログラム、ハードウェア、あるいは両方を備えてもよい。別の実施形態によれば、暗号処理モジュール６２５は、データ比較、データ解析、データ分割、データ分離、データハッシング、データ暗号化または復号、デジタル署名検証または作成、デジタル証明書生成、記憶、または要求、暗号鍵生成、あるいは同等物を行ってもよい。また、当業者であれば、暗号処理モジュール８２５は、プリティーグッドプライバシー（Ｐｒｅｔｔｙ　Ｇｏｏｄ　Ｐｒｉｖａｃｙ／ＰＧＰ）、ＲＳＡベースの公開鍵システム、または多数の代替的な鍵管理システム等の公開鍵インフラストラクチャを有利に備えてもよいことを、本明細書の本開示から認識するであろう。加えて、暗号処理モジュール６２５は、公開鍵暗号化、対称鍵暗号化、または両方を行ってもよい。前述のものに加えて、暗号処理モジュール６２５は、継ぎ目のない透過的な相互運用性機能を実装するための１つ以上のコンピュータプログラムまたはモジュール、ハードウェア、あるいは両方を含んでもよい。

【００８５】

当業者であれば、暗号機能性が、概して暗号鍵管理システムに関する、多数または種々の機能を含んでもよいことも、本明細書の本開示から認識するであろう。

【００８６】

図７は、本発明の実施形態の側面による、保管場所システム７００の簡略化したブロック図を図示する。図７に示されるように、保管場所システム７００は、複数のデータ記憶設備、例えば、データ記憶設備Ｄ１、Ｄ２、Ｄ３、およびＤ４を有利に備える。しかしながら、保管場所システムは１つだけのデータ記憶設備を有してもよいことが、当業者によって容易に理解される。本発明の一実施形態によれば、データ記憶設備Ｄ１乃至Ｄ４のそ

れぞれは、図４の保管場所２１０を参照して開示される要素のうちのいくつかまたは全てを有利に備えてもよい。保管場所２１０と同様に、データ記憶設備Ｄ１乃至Ｄ４は、好ましくは従来のＳＳＬを介して、トランザクションエンジン２０５、認証エンジン２１５、および暗号エンジン２２０と通信する。通信リンクは、例えば、ＸＭＬ文書を転送する。トランザクションエンジン２０５からの通信は、データの要求を有利に含んでもよく、要求は、各データ記憶設備Ｄ１乃至Ｄ４のＩＰアドレスへ有利に送信される。他方で、トランザクションエンジン２０５は、例えば、応答時間、サーバ負荷、メンテナンススケジュール、または同等物等の多数の基準に基づいて、要求を特定のデータ記憶設備に送信する。

【００８７】

トランザクションエンジン２０５からのデータの要求に応じて、保管場所システム７００は、記憶されたデータを認証エンジン２１５および暗号エンジン２２０を有利に転送する。それぞれのデータ集約モジュールは、転送されたデータを受信し、データを使用可能な形式に組み立てる。他方で、認証エンジン２１５および暗号エンジン２２０から、データ記憶設備Ｄ１乃至Ｄ４への通信は、記憶される機密データの伝送を含んでもよい。例えば、一実施形態によれば、認証エンジン２１５および暗号エンジン２２０は、機密データを解読不可能な部分に分けるために、それぞれのデータ分割モジュールを有利に採用し、次いで、機密データの１つ以上の解読不可能な部分を特定のデータ記憶設備に伝送してもよい。

【００８８】

一実施形態によれば、各データ記憶設備Ｄ１乃至Ｄ４は、例えば、ディレクトリサーバ等の別個の独立記憶システムを備える。本発明の別の実施形態によれば、保管場所システム７００は、複数の地理的に分離された独立データ記憶システムを備える。そのうちのいくつかまたは全てが有利に地理的に分離されてもよい、明確に異なる独立記憶設備Ｄ１乃至Ｄ４の中へ、機密データを分配することによって、保管場所システム７００は、付加的なセキュリティ対策とともに冗長性を提供する。例えば、一実施形態によれば、複数のデータ記憶設備Ｄ１乃至Ｄ４のうちの２つからのデータのみが、機密データを解読し、再構築するために必要とされる。したがって、信頼エンジン１１０の機能性に影響を及ぼすことなく、メンテナンス、システム故障、停電、または同等物等により、４つのデータ記憶設備Ｄ１乃至Ｄ４のうちの２つもの設備が、動作不能になってもよい。加えて、一実施形態によれば、各データ記憶設備に記憶されたデータが無作為化され、解読不可能であるため、個別データ記憶設備のセキュリティ侵害は、必ずしも機密データを損なうわけではない。また、データ記憶設備の地理的分離を有する実施形態では、複数の地理的に遠隔の設備のセキュリティ侵害は、ますます困難となる。実際に、不正従業員でさえも、必要とされる複数の独立した地理的に遠隔のデータ記憶設備を妨害するのに多大な努力を必要とする。

【００８９】

保管場所システム７００がその好ましい代替実施形態に関して開示されているが、本発明はそれによって限定されることを目的としていない。むしろ、当業者であれば、保管場所システム７００の多数の代替案を本明細書の本開示から認識するであろう。例えば、保管場所システム７００は、１つ、２つ、またはそれ以上のデータ記憶設備を備えてもよい。加えて、機密データは、２つ以上のデータ記憶設備からの複数部分が、機密データを再構築して解読するために必要とされるように、数学的に操作されてもよい。

【００９０】

前述のように、認証エンジン２１５および暗号エンジン２２０はそれぞれ、例えば、テキスト、音声、ビデオ、認証データ、および暗号鍵データ等の任意の種類または形態のデータを分割するために、それぞれデータ分割モジュール５２０および６１０含む。図８は、本発明の実施形態による、データ分割モジュールによって行われるデータ分割プロセス８００のフローチャートを図示する。図８に示されるように、データ分割プロセス８００は、機密データ「Ｓ」が認証エンジン２１５または暗号エンジン２２０のデータ分割モジ

ュールによって受信されるときに、ステップ８０５から始まる。好ましくは、次いで、ステップ８１０で、データ分割モジュールは、実質的な乱数、値、または文字列、あるいは一式のビット「Ａ」を生成する。例えば、乱数Ａは、暗号用途で使用するために好適な高品質の乱数を生じるために、当業者に利用可能である多数の様々な従来の技法で生成されてもよい。加えて、一実施形態によれば、乱数Ａは、機密データＳの長さよりも短い、長い、または等しい等の任意の好適な長さであってもよい、ビット長を備える。

【００９１】

加えて、ステップ８２０では、データ分割プロセス８００は、別の統計学的乱数「Ｃ」を生成する。好ましい実施形態によれば、統計学的乱数ＡおよびＣの生成は、有利に並行して行われてもよい。次いで、データ分割モジュールは、新しい数字「Ｂ」および「Ｄ」が生成されるように、数字ＡおよびＣを機密データＳと組み合わせる。例えば、数字Ｂは、Ａ　ＸＯＲ　Ｓという二値組み合わせを備えてもよく、数字Ｄは、Ｃ　ＸＯＲ　Ｓという二値組み合わせを備えてもよい。ＸＯＲ関数または「排他的ＯＲ」関数は、当業者に周知である。前述の組み合わせは、好ましくは、それぞれステップ８２５および８３０で発生し、一実施形態によれば、前述の組み合わせはまた、並行して発生する。次いで、データ分割プロセス８００は、ペアリングのうちのいずれも、元の機密データＳを再編成して解読するのに十分なデータを単独では含有しないように、乱数ＡおよびＣならびに数字ＢおよびＤがペアリングされる、ステップ８３５へと進む。例えば、番号は、ＡＣ、ＡＤ、ＢＣ、およびＢＤのようにペアリングされる。一実施形態によれば、前述のペアリングのそれぞれは、図７の保管場所Ｄ１乃至Ｄ４のうちの１つに分配される。別の実施形態によれば、前述のペアリングのそれぞれは、保管場所Ｄ１乃至Ｄ４のうちの１つに無作為に分配される。例えば、第１のデータ分割プロセス８００中に、ペアリングＡＣは、例えば、Ｄ２のＩＰアドレスの無作為選択を介して、保管場所Ｄ２に送信されてもよい。次いで、第２のデータ分割プロセス８００中に、ペアリングＡＣは、例えば、Ｄ４のＩＰアドレスの無作為選択を介して、保管場所Ｄ４に送信されてもよい。加えて、ペアリングは、全て１つの保管場所で記憶されてもよく、該保管場所上の別個の場所に記憶されてもよい。

【００９２】

前述の内容に基づいて、データ分割プロセス８００は、いずれのデータ記憶設備Ｄ１乃至Ｄ４も、元の機密データＳを再作成するのに十分な暗号化されたデータを含まないように、４つのデータ記憶設備Ｄ１乃至Ｄ４のそれぞれの中に機密データ部分を有利に配置する。前述のように、個別に使用不可能な暗号化部分へのデータのそのような無作為化は、セキュリティを増大させ、たとえデータ記憶設備Ｄ１乃至Ｄ４のうちの１つが損なわれても、データに対する維持された信頼を提供する。

【００９３】

データ分割プロセス８００がその好ましい実施形態に関して開示されているが、本発明はそれによって限定されることを目的としていない。むしろ、当業者であれば、データ分割プロセス８００の多数の代替案を本明細書の本開示から認識するであろう。例えば、データ分割プロセスは、データを２つの数字、例えば、乱数Ａおよび数字Ｂに有利に分割し、２つのデータ記憶設備を介してＡおよびＢを無作為に分配してもよい。また、データ分割プロセス８００は、付加的な乱数の生成を介して、多数のデータ記憶設備の間でデータを有利に分割してもよい。データは、１ビット、ビット、バイト、キロバイト、メガバイトまたはそれ以上、あるいはサイズの任意の組み合わせ、もしくは一連のサイズを含むが、それらに限定されない、任意の所望の、選択された、所定の、または無作為に割り当てられたサイズ単位に分割されてもよい。加えて、分割プロセスに起因するデータ単位のサイズを変化させることにより、データを使用可能な形態に復元しにくくし、それにより、機密データのセキュリティを増大させてもよい。分割データ単位サイズは、多種多様なデータ単位サイズ、またはサイズのパターン、あるいはサイズの組み合わせであってもよいことが、当業者にとって容易に明白である。例えば、データ単位サイズは、全て同じサイズ、固定された一式の異なるサイズ、サイズの組み合わせ、または無作為に生成されたサイズとなるように選択または事前決定されてもよい。同様に、データ単位は、固定または

所定データ単位サイズ、データ単位サイズのパターンまたは組み合わせ、あるいは無作為に生成されたデータ単位サイズ、もしくはシェア当たりのサイズに従って、１つ以上のシェアの中へ分配されてもよい。

【００９４】

前述のように、機密データＳを再作成するために、データ部分は、脱無作為化され、再編成される必要がある。このプロセスは、それぞれ認証エンジン２１５および暗号エンジン２２０のデータ集約モジュール５２５および６２０において有利に発生してもよい。データ集約モジュール、例えば、データアセンブリモジュール５２５は、データ記憶設備Ｄ１乃至Ｄ４からデータ部分を受信し、データを使用可能な形態に再構築する。例えば、データ分割モジュール５２０が図８のデータ分割プロセス８００を採用した、一実施形態によれば、データ集約モジュール５２５は、機密データＳを再作成するために、データ記憶設備Ｄ１乃至Ｄ４のうちの少なくとも２つからのデータ部分を使用する。例えば、ＡＣ、ＡＤ、ＢＣ、およびＢＤのペアリングは、いずれか２つが、ＡおよびＢまたはＣおよびＤのうちの１つを提供するように分配された。Ｓ＝Ａ　ＸＯＲ　ＢまたはＳ＝Ｃ　ＸＯＲ　Ｄであることに留意することは、データ集約モジュールが、ＡおよびＢまたはＣおよびＤのうちの１つを受信すると、データ集約モジュール５２５が、機密データＳを有利に再構築できることを示す。したがって、データ集約モジュール５２５は、例えば、データ記憶設備Ｄ１乃至Ｄ４のうちの少なくとも最初２つからデータ部分を受信して、信頼エンジン１１０による集約要求に応答すると、機密データＳを集約してもよい。

【００９５】

上記のデータ分割および集約プロセスに基づいて、機密データＳは、信頼エンジン１１０の限定された領域中のみで使用可能な形式で存在する。例えば、機密データＳが登録認証データを含む時、使用可能な無作為化されていない登録認証データは、認証エンジン２１５のみで利用可能である。同様に、機密データＳが秘密暗号鍵データを含む時、使用可能な無作為化されていない秘密暗号鍵データは、暗号エンジン２２０のみで利用可能である。

【００９６】

データ分割および集約プロセスがその好ましい実施形態に関して開示されているが、本発明はそれによって限定されることを目的としていない。むしろ、当業者であれば、機密データＳを分割および集約するための多数の代替案を本明細書の本開示から認識するであろう。例えば、公開鍵暗号化は、データ記憶設備Ｄ１乃至Ｄ４においてデータをさらに確保するために使用されてもよい。加えて、本明細書で説明されるデータ分割モジュールはまた、任意の既存のコンピュータシステム、ソフトウェアスイート、データベース、またはそれらの組み合わせ、あるいは本明細書で開示および説明される信頼エンジン、認証エンジン、およびトランザクションエンジン等の本発明の他の実施形態に組み込まれ、組み合わされ、またはそうでなければ一部とされてもよい、本発明の別個の明確に異なる実施形態でもあることが、当業者にとって容易に明白である。

【００９７】

図９Ａは、本発明の実施形態の側面による、登録プロセス９００のデータフローを図示する。図９Ａに示されるように、登録プロセス９００は、ユーザが暗号システム１００の信頼エンジン１１０を用いて登録することを所望すると、ステップ９０５から始まる。この実施形態によれば、ユーザシステム１０５は、人口統計データおよび登録認証データ等の登録データを入力するようにユーザに問い合せを行う、Ｊａｖａ（登録商標）ベース等のクライアント側アプレットを有利に含む。一実施形態によれば、登録認証データは、ユーザＩＤ、パスワード、生体測定、または同等物を含む。一実施形態によれば、問い合せプロセス中に、クライアント側アプレットは、好ましくは、信頼エンジン１１０と通信して、選択されたユーザＩＤが一意であることを確実にする。ユーザＩＤが一意ではない時、信頼エンジン１１０は、一意のユーザＩＤを有利に提案してもよい。クライアント側アプレットは、登録データを収集し、例えば、ＸＭＬ文書を介して、登録データを信頼エンジン１１０に、具体的には、トランザクションエンジン２０５に伝送する。一実施形態に

よれば、伝送は、認証エンジン２１５の公開鍵を用いて符号化される。

【００９８】

一実施形態によれば、ユーザは、登録プロセス９００のステップ９０５中に単一の登録を行う。例えば、ユーザは、Ｊｏｅ　Ｕｓｅｒ等の特定の個人として自分を登録する。Ｊｏｅ　ＵｓｅｒがＭｅｇａ　Ｃｏｒｐ．のＣＥＯであるＪｏｅ　Ｕｓｅｒとして登録することを所望する時、次いで、この実施形態によれば、Ｊｏｅ　Ｕｓｅｒは２度目に登録し、第２の一意のユーザＩＤを受信し、信頼エンジン１１０は２つの身元を関連づけない。本発明の別の実施形態によれば、登録プロセス９００は、単一のユーザＩＤに対する複数のユーザの身元を提供する。したがって、上記の実施例では、信頼エンジン１１０は、Ｊｏｅ　Ｕｓｅｒの２つの身元を有利に関連付ける。本明細書の本開示から当業者によって理解されるように、ユーザは、多くの身元、例えば、世帯主であるＪｏｅ　Ｕｓｅｒ、慈善団体のメンバーであるＪｏｅ　Ｕｓｅｒ、および同等物を有してもよい。たとえユーザが複数の身元を有してもよくても、この実施形態によれば、信頼エンジン１１０は、好ましくは、一式の登録データのみを記憶する。また、ユーザは、必要に応じて、身元を有利に追加、編集／更新、または削除してもよい。

【００９９】

登録プロセス９００がその好ましい実施形態に関して開示されているが、本発明はそれによって限定されることを目的としていない。むしろ、当業者であれば、登録データ、具体的には登録認証データの収集の多数の代替案を本明細書の本開示から認識するであろう。例えば、アプレットは、共通オブジェクトモデル（ＣＯＭ）ベースのアプレットまたは同等物であってもよい。

【０１００】

他方で、登録プロセスは、等級別登録を含んでもよい。例えば、最低レベルの登録において、ユーザは、自分の身元に関する文書を生成することなく、通信リンク１２５上で登録してもよい。増加したレベルの登録に従って、ユーザは、デジタル公証人等の信頼できる第三者を使用して登録する。例えば、ユーザは、信頼できる第三者に直接現れ、出生証明書、運転免許書、軍人身分証明書、または同等物を生成してもよく、信頼できる第三者は、例えば、登録提出にデジタル署名を有利に含んでもよい。信頼できる第三者は、実際の公証人、郵便局または陸運局等の政府機関、従業員を登録する大企業の中の人事担当者、または同等物を含んでもよい。当業者であれば、多数の様々なレベルの登録が登録プロセス９００中に発生してもよいことを本明細書の本懐時から理解するであろう。

【０１０１】

登録認証データを受信した後、ステップ９１５では、トランザクションエンジン２０５が、従来のＦＵＬＬ　ＳＳＬ技術を使用して、登録認証データを認証エンジン２１５に転送する。ステップ９２０では、認証エンジン２１５が、認証エンジン２１５の秘密鍵を使用して、登録認証データを復号する。加えて、認証エンジン２１５は、データを少なくとも２つの独立して解読不可能な無作為化された数に分割するよう、登録認証データに数学的に作用するためにデータ分割モジュールを採用する。前述のように、少なくとも２つの数は、統計学的乱数および二値ＸＯＲｅｄ数を備えてもよい。ステップ９２５では、認証エンジン２１５が、無作為化された数の各部分をデータ記憶設備Ｄ１からＤ４のうちの１つに転送する。前述のように、認証エンジン２１５はまた、どの部分がどの保管場所に転送されるかを有利に無作為化してもよい。

【０１０２】

しばしば登録プロセス９００中に、ユーザはまた、暗号システム１００外の他者から暗号化された文書を受信してもよいように、デジタル証明書が発行されることも所望する。前述のように、証明機関１１５は、概して、いくつかの従来の基準のうちの１つ以上に従って、デジタル証明書を発行する。概して、デジタル証明書は、全員に知られているユーザまたはシステムの公開鍵を含む。

【０１０３】

ユーザがデジタル証明書を登録時に要求しようと、別の時に要求しようと、要求は信頼

エンジン１１０を介して認証エンジン２１５に転送される。一実施形態によれば、要求は、例えば、ユーザの適正な名前を有する、ＸＭＬ文書を含む。ステップ９３５によれば、認証エンジン２１５が、要求を暗号エンジン２２０に転送し、暗号鍵または鍵ペアを生成するように暗号エンジン２２０に命令する。

【０１０４】

要求に応じて、ステップ９３５では、暗号エンジン２２０が、少なくとも１つの暗号鍵を生成する。一実施形態によれば、暗号処理モジュール６２５は、一方の鍵が秘密鍵として使用され、もう一方が公開鍵として使用される、鍵ペアを生成する。暗号エンジン２２０は、秘密鍵、および一実施形態によれば公開鍵のコピーを記憶する。ステップ９４５では、暗号エンジン２２０が、デジタル証明書の要求をトランザクションエンジン２０５に伝送する。一実施形態によれば、要求は、例えば、ＸＭＬ文書に組み込まれた、ＰＫＣＳ１０等の標準化要求を有利に含む。デジタル証明書の要求は、１つ以上の証明機関、および証明機関が要求する１つ以上の標準形式に有利に対応してもよい。

【０１０５】

ステップ９５０では、トランザクションエンジン２０５が、ステップ９５５でデジタル証明書を返信する証明機関１１５に、この要求を転送する。返信デジタル証明書は、有利に、ＰＫＣＳ７等の標準化形式、または証明機関１１５のうちの１つ以上の専有形式であってもよい。ステップ９６０では、デジタル証明書がトランザクションエンジン２０５によって受信され、コピーがユーザに転送され、コピーが信頼エンジン１１０を用いて記憶される。信頼エンジン１１０は、信頼エンジン１１０が証明機関１１５の可用性に依存する必要がないように、証明書のコピーを記憶する。例えば、ユーザがデジタル証明書を送信することを所望するか、または第三者がユーザのデジタル証明書を要求すると、デジタル証明書の要求は、一般的には、証明機関１１５に送信される。しかしながら、証明機関１１５がメンテナンスを行っているか、または故障またはセキュリティ侵害の犠牲となっている場合、デジタル証明書が利用可能ではない場合がある。

【０１０６】

暗号鍵を発行した後はいつでも、暗号エンジン２２０は、暗号鍵が独立して解読不可能な無作為化された数に分割されるように、上記で説明されるデータ分割プロセス８００を有利に採用してもよい。認証データと同様に、ステップ９６５では、暗号エンジン２２０が、無作為化された数をデータ記憶設備Ｄ１乃至Ｄ４に転送する。

【０１０７】

当業者であれば、ユーザが登録後にいつでもデジタル証明書を要求してもよいことを本明細書の本開示から認識するであろう。また、システム間の通信は、ＦＵＬＬ　ＳＳＬまたは公開鍵暗号化技術を有利に含んでもよい。また、登録プロセスは、信頼エンジン１１０の内部または外部の１つ以上の専有証明機関を含む複数の証明機関から、複数のデジタル証明書を発行してもよい。

【０１０８】

ステップ９３５乃至９６０で開示されるように、本発明の一実施形態は、最終的に信頼エンジン１１０上に記憶される証明書の要求を含む。一実施形態によれば、暗号処理モジュール６２５が、信頼エンジン１１０によって使用される鍵を発行するため、各証明書は秘密鍵に対応する。したがって、信頼エンジン１１０は、ユーザによって所有されるか、またはユーザと関連付けられる証明書の監視を介して、相互運用性を有利に提供してもよい。例えば、暗号エンジン２２０が暗号機能の要求を受信すると、暗号処理モジュール６２５は、要求ユーザによって所有される証明書を調査して、ユーザが要求の属性に合致する秘密鍵を所有するかどうかを決定してもよい。そのような証明書が存在する時、暗号処理モジュール６２５は、要求された機能を果たすために、証明書またはそれと関連付けられた公開あるいは秘密鍵を使用してもよい。そのような証明書が存在しない時、暗号処理モジュール６２５は、適切な鍵の欠如を改善しようとして、いくつかの措置を有利かつ透過的に行ってもよい。例えば、図９Ｂは、本発明の実施形態の側面による、暗号処理モジュール６２５が適切な鍵を使用して暗号機能を果たすことを確実にする前述のステップを

開示する、相互運用性プロセス９７０のフローチャートを図示する。

【０１０９】

図９Ｂに示されるように、相互運用性プロセス９７０は、暗号処理モジュール９２５が所望される証明書の種類を決定する、ステップ９７２から始まる。本発明の一実施形態によれば、証明書の種類は、暗号機能の要求、または要求側によって提供される他のデータにおいて、有利に特定されてもよい。別の実施形態によれば、証明書の種類は、要求のデータ形式によって解明されてもよい。例えば、暗号処理モジュール９２５は、要求が特定の種類に対応することを有利に認識してもよい。

【０１１０】

一実施形態によれば、証明書の種類は、１つ以上のアルゴリズム基準、例えば、ＲＳＡ、ＥＬＧＡＭＡＬ、または同等物を含んでもよい。加えて、証明書の種類は、対称鍵、公開鍵、２５６ビット鍵等の強力な暗号化鍵、あまり確実ではない鍵、または同等物等の１つ以上の鍵種類を含んでもよい。また、証明書の種類は、前述のアルゴリズム基準または鍵のうちの１つ以上のアップグレードまたは交換、１つ以上のメッセージまたはデータ形式、Ｂａｓｅ　３２またはＢａｓｅ　６４等の１つ以上のデータカプセル化または符号化スキームを含んでもよい。証明書の種類はまた、１つ以上の第三者暗号アプリケーションまたはインターフェース、１つ以上の通信プロトコル、あるいは１つ以上の証明書基準またはプロトコルとの互換性を含んでもよい。当業者であれば、他の差異が証明書の種類に存在してもよく、これらの差異への変換および差異からの変換が本明細書で開示されるように実装されてもよいことを、本明細書の本開示から認識するであろう。

【０１１１】

いったん暗号処理モジュール６２５が証明書の種類を決定すると、相互運用性プロセス９７０は、ステップ９７４へと進み、ユーザがステップ９７４で決定された種類に合致する証明書を所有するかどうかを決定する。ユーザが合致する証明書を有する、例えば、信頼エンジン１１０が、例えば、その以前の記憶を介して、合致する証明書にアクセスできる時、暗号処理モジュール８２５は、合致する秘密鍵も信頼エンジン１１０内に記憶されていることを知る。例えば、合致する秘密鍵は、保管場所２１０または保管場所システム７００内に記憶されてもよい。暗号処理モジュール６２５は、合致する秘密鍵が、例えば、保管場所２１０から集約されることを有利に要求し、次いで、ステップ９７６で、暗号措置または機能を果たすために、合致する秘密鍵を使用してもよい。例えば、前述のように、暗号処理モジュール６２５は、ハッシング、ハッシュ比較、データ暗号化または復号、デジタル署名検証または作成、または同等物を有利に行ってもよい。

【０１１２】

ユーザが合致する証明書を所有しない時、相互運用性プロセス９７０は、ユーザが相互認定された証明書を所有するかどうかを暗号処理モジュール６２５が決定する、ステップ９７８へと進む。一実施形態によれば、証明機関の間の相互認定は、第１の証明機関が第２の証明機関からの証明書を信頼することを決定するときに発生する。言い換えれば、第１の証明機関は、第２の証明機関からの証明書が、ある品質基準を満たし、したがって、第１の証明機関の独自の証明書と同等であるとして「認定」されてもよいと決定する。相互認定は、証明機関が、例えば、信頼のレベルを有する証明書を発行すると、より複雑になる。例えば、第１の証明機関が、通常、登録プロセスにおける信頼度に基づいて、特定の証明書の３つの信頼のレベルを提供してもよい一方で、第２の証明機関は、７つの信頼のレベルを提供してもよい。相互認定は、どのレベルおよび第２の証明機関からのどの証明書が、どのレベルおよび第１の証明機関からのどの証明書に代替されてもよいかを有利に追跡してもよい。前述の相互認定が２つの認定機関の間で公式かつ公的に行われる時、相互への証明書およびレベルのマッピングは、しばしば「連鎖」と呼ばれる。

【０１１３】

本発明の別の実施形態によれば、暗号処理モジュール６２５は、証明機関によって同意されるもの以外の相互認定を有利に進展させてもよい。例えば、暗号処理モジュール６２５は、第１の証明機関の証明書実践規定（ＣＰＳ）または他の公表された方針規定にアク

セスし、例えば、特定の信頼レベルによって要求される認証トークンを使用して、第１の証明機関の証明書を別の証明機関の証明書と合致させてもよい。

【０１１４】

ステップ９７８では、暗号処理モジュール６２５が、ユーザが相互認定された証明書を所有することを決定すると、相互運用性プロセス９７０は、ステップ９７６へと進み、相互認定された公開鍵、秘密鍵、または両方を使用して、暗号措置または機能を果たす。代替として、暗号処理モジュール６２５が、ユーザが相互認定された証明書を所有しないことを決定すると、相互運用性プロセス９７０は、暗号処理モジュール６２５が、要求された証明書の種類、またはそれと相互認定された証明書を発行する証明機関を選択する、ステップ９８０へと進む。ステップ９８２では、暗号処理モジュール６２５が、前述の内容で論議されたユーザ登録認証データが選択された証明機関の認証要件を満たすかどうかを決定する。例えば、ユーザが、例えば、人口統計および他の質問に答えることによって、ネットワーク上で登録した場合、提供される認証データは、生体測定データを提供し、例えば、公証人等の第三者の前に現れるユーザよりも低いレベルの信頼を確立してもよい。一実施形態によれば、前述の認証要件は、選択された認証機関のＣＰＳで有利に規定されてもよい。

【０１１５】

ユーザが、選択された証明機関の要件を満たす登録認証データを信頼エンジン１１０に提供した時、相互運用性プロセス９７０は、暗号処理モジュール８２５が選択された証明機関から証明書を取得する、ステップ９８４へと進む。一実施形態によれば、暗号処理モジュール６２５は、登録プロセス９００のステップ９４５乃至９６０を辿ることによって証明書を取得する。例えば、暗号処理モジュール６２５は、証明機関から証明書を要求するために、すでに暗号エンジン２２０に利用可能な鍵ペアのうちの１つ以上から、１つ以上の公開鍵を有利に採用してもよい。別の実施形態によれば、暗号処理モジュール６２５は、１つ以上の新しい鍵ペアを有利に生成し、証明機関から証明書を要求するために、それに対応する公開鍵を使用してもよい。

【０１１６】

別の実施形態によれば、信頼エンジン１１０は、１つ以上の証明書の種類を発行することが可能な１つ以上の証明書発行モジュールを有利に含んでもよい。この実施形態によれば、証明書発行モジュールは、前述の証明書を提供してもよい。暗号処理モジュール６２５が証明書を取得すると、相互運用性プロセス９７０は、ステップ９７６へと進み、取得された証明書に対応する公開鍵、秘密鍵、または両方を使用して、暗号措置または機能を果たす。

【０１１７】

ステップ９８２で、ユーザが、選択された証明機関の要件を満たす登録認証データを信頼エンジン１１０に提供していない時、暗号処理モジュール６２５は、ステップ９８６で、異なる認証要件を有する他の証明機関があるかどうかを決定する。例えば、暗号処理モジュール６２５は、より低い認証要件を有する証明機関を探してもよいが、依然として選択された証明書またはその相互認定を発行してもよい。

【０１１８】

より低い要件を有する前述の証明機関が存在する時、相互運用性プロセス９７０は、ステップ９８０へと進み、証明機関を選択する。代替として、そのような証明機関が存在しない時、ステップ９８８では、信頼エンジン１１０が、ユーザから付加的な認証トークンを要求してもよい。例えば、信頼エンジン１１０は、例えば、生体測定データを備える、新しい登録認証データを要求してもよい。また、信頼エンジン１１０は、例えば、運転免許証、社会保障カード、銀行のカード、出生証明書、軍人身分証明書、または同等物等を伴って公証人の前に現れること等、ユーザが信頼できる第三者の前に現れ、適切な認証信任状を提供することを要求してもよい。信頼エンジン１１０が更新された認証データを受信すると、相互運用性プロセス９７０は、ステップ９８４へと進み、前述の選択された証明書を取得する。

【０１１９】
前述の相互運用性プロセス９７０を介して、暗号処理モジュール６２５は、異なる暗号システム間で、継ぎ目のない透過的な変換および転換を有利に提供する。当業者であれば、前述の相互運用可能なシステムの多数の利点および実装を本明細書の本開示から認識するであろう。例えば、相互運用性プロセス９７０の前述のステップ９８６は、証明機関が、特殊な状況下で、より低いレベルの相互認定を容認してもよい、以下でさらに詳細に説明される、信頼裁定の側面を有利に含んでもよい。加えて、相互運用性プロセス９７０は、相互運用性を確実にすること、および証明書失効リスト（ＣＲＬ）、オンライン証明書状態プロトコル（ＯＣＳＰ）、または同等物を採用すること等の標準証明書失効の採用を含んでもよい。

【０１２０】
図１０は、本発明の実施形態の側面による、認証プロセス１０００のデータフローを図示する。一実施形態によれば、認証プロセス１０００は、ユーザから現在の認証データを収集し、それをユーザの登録認証データと比較することを含む。例えば、認証プロセス１０００は、ユーザが、例えば、ベンダとのトランザクションを行うことを所望する、ステップ１００５から始まる。そのようなトランザクションは、例えば、購入オプションを選択すること、ベンダシステム１２０の制限領域またはデバイスへのアクセスを要求すること、または同等物を含んでもよい。ステップ１０１０では、ベンダが、トランザクションＩＤおよび認証要求をユーザに提供する。トランザクションＩＤは、１２８ビットランダム数量と連結された３２ビットタイムスタンプを有する１９２ビット数量、または３２ビットのベンダ特異的定数と連結された「ノンス」を有利に含んでもよい。そのようなトランザクションＩＤは、信頼エンジン１１０によって模倣トランザクションを拒絶することができるように、トランザクションを一意的に識別する。

【０１２１】
認証要求は、どのレベルの認証が特定のトランザクションに必要とされるかについてを有利に含んでもよい。例えば、ベンダは、問題のトランザクションに必要とされる特定のレベルの確信を特定してもよい。以下で論議されるように、認証をこのレベルの確信にすることができない場合、確信のレベルを上昇させるユーザによるさらなる認証、またはベンダとサーバとの間の認証に関する変更を伴わずに、トランザクションは発生しない。これらの問題を以下でより完全に論議する。

【０１２２】
一実施形態によれば、トランザクションＩＤおよび認証要求は、ベンダ側アプレットまたは他のソフトウェアプログラムによって有利に生成されてもよい。加えて、トランザクションＩＤおよび認証データの伝送は、例えば、１／２ＳＳＬ等の従来のＳＳＬ技術、または言い換えればベンダ側認証ＳＳＬを使用して暗号化される、１つ以上のＸＭＬ文書を含んでもよい。

【０１２３】
ユーザシステム１０５がトランザクションＩＤおよび認証要求を受信した後、ユーザシステム１０５は、ユーザから、潜在的に現在の生体測定情報を含む現在の認証データを収集する。ユーザシステム１０５は、ステップ１０１５で、認証エンジン２１５の公開鍵を用いて、少なくとも現在の認証データ「Ｂ」およびトランザクションＩＤを暗号化し、そのデータを信頼エンジン１１０に転送する。伝送は、好ましくは、少なくとも従来の１／２ＳＳＬ技術で暗号化されるＸＭＬ文書を備える。ステップ１０２０では、トランザクションエンジン２０５が、伝送を受信し、好ましくはＵＲＬまたはＵＲＩでデータ形式または要求を認識し、伝送を認証エンジン２１５に転送する。

【０１２４】
ステップ１０１５および１０２０中に、ベンダシステム１２０は、ステップ１０２５で、好ましいＦＵＬＬ　ＳＳＬ技術を使用して、トランザクションＩＤおよび認証要求を信頼エンジン１１０に転送する。この通信はまた、ベンダＩＤを含んでもよいが、ベンダ識別はまた、トランザクションＩＤの非ランダム部分を介して伝達されてもよい。ステップ

１０３０および１０３５では、トランザクションエンジン２０５が、通信を受信し、オーディットトレールに記録を作成し、データ記憶設備Ｄ１乃至Ｄ４から集約されるユーザの登録認証データの要求を生成する。ステップ１０４０では、保管場所システム７００が、ユーザに対応する登録認証データ部分を認証エンジン２１５に転送する。ステップ１０４５では、認証エンジン２１５が、その秘密鍵を使用して伝送を復号し、登録認証データをユーザによって提供された現在の認証データと比較する。

【０１２５】

ステップ１０４５の比較は、前述の内容で参照され、以下でさらに詳細に論議されるような発見的文脈依存機密認証を有利に適用してもよい。例えば、受信される生体測定情報が完全に合致しない場合、より低い確信の合致が生じる。特定の実施形態では、認証の確信のレベルは、トランザクションの性質ならびにユーザおよびベンダの両方の所望に対して平衡を保たれる。再度、これを以下でより詳細に論議する。

【０１２６】

ステップ１０５０では、認証エンジン２１５が、ステップ１０４５の比較の結果を用いて認証要求を満たす。本発明の一実施形態によれば、認証要求は、認証プロセス１０００のはい／いいえ（ＹＥＳ／ＮＯ）または真／偽（ＴＲＵＥ／ＦＡＬＳＥ）の結果で満たされる。ステップ１０５５では、例えば、ユーザが認証要求を開始したトランザクションの完了を可能にすることにベンダが作用するために、満たされた認証要求がベンダに返信される。一実施形態によれば、確認メッセージがユーザに渡される。

【０１２７】

前述の内容に基づいて、認証プロセス１０００は、有利に機密データを確実に保持し、機密データの完全性を維持するように構成される結果を生じる。例えば、機密データは、認証エンジン２１５の内部のみで集約される。例えば、登録認証データは、データ集約モジュールによって認証エンジン２１５の中で集約される解読不可能なものであり、現在の認証データは、従来のＳＳＬ技術および認証エンジン２１５の秘密鍵によって解かれるまで解読不可能である。また、ベンダに伝送される認証結果は、機密データを含まず、ユーザは、自分が有効な認証データを生成したかどうかさえも分からない場合がある。

【０１２８】

認証プロセス１０００がその好ましい代替実施形態に関して開示されているが、本発明はそれによって限定されることを目的としていない。むしろ、当業者であれば、認証プロセス１０００の多数の代替案を本明細書の本開示から認識するであろう。例えば、ベンダは、ユーザシステム１０５とともに存在するものでさえ、ほぼあらゆる要求アプリケーションによって有利に置換されてもよい。例えば、Ｍｉｃｒｏｓｏｆｔ　Ｗｏｒｄ等のクライアントアプリケーションが、文書をアンロックする前に、認証を要求するためにアプリケーションプログラムインターフェース（ＡＰＩ）または暗号ＡＰＩ（ＣＡＰＩ）を使用してもよい。代替として、メールサーバ、ネットワーク、携帯電話、パーソナルまたは携帯コンピュータデバイス、ワークステーション、または同等物が全て、認証プロセス１０００によって満たすことができる認証要求を行ってもよい。実際、前述の信頼できる認証プロセス１０００を提供した後、要求アプリケーションまたはデバイスは、多数の電子またはコンピュータデバイスまたはシステムへのアクセスまたはそれらの使用を提供してもよい。

【０１２９】

また、認証プロセス１０００は、認証失敗の場合に多数の代替手順を採用してもよい。例えば、認証失敗は、ユーザが自分の現在の認証データを再入力する、同じトランザクションＩＤおよび要求を維持してもよい。前述のように、同じトランザクションＩＤの使用は、認証エンジン２１５のコンパレータが特定のトランザクションの認証試行の数を監視し、制限することを可能にし、それにより、より確実な暗号システム１００を作成する。

【０１３０】

加えて、認証プロセス１０００は、機密データボールトを解錠すること等の簡潔なシングルサインオン解決法を開発するために、有利に採用されてもよい。例えば、成功した、

または肯定的な認証は、認証ユーザに、ほぼ無限数のシステムおよびアプリケーションに対する任意の数のパスワードに自動的にアクセスする能力を提供してもよい。例えば、ユーザの認証は、ユーザに、複数のオンラインベンダと関連付けられるパスワード、ログイン、財務信任状、または同等物、ローカルエリアネットワーク、種々のパーソナルコンピュータデバイス、インターネットサービスプロバイダ、オークションプロバイダ、投資仲介業者、または同等物へのアクセスを提供してもよい。機密データボールトを採用することによって、ユーザは、もはや関連性を介して思い出す必要がないため、実に大量かつランダムなパスワードを選択してもよい。むしろ、認証プロセス１０００が、それらへのアクセスを提供する。例えば、ユーザは、記憶すべきデータ、名前等と関連付けられるものよりもむしろ、長さが２０数桁であるランダムな英数字の文字列を選択してもよい。

【０１３１】

一実施形態によれば、所与のユーザと関連付けられる機密データボールトは、有利に保管場所２１０のデータ記憶設備に記憶されるか、分割されて保管場所システム７００に記憶されてもよい。この実施形態によれば、肯定的なユーザ認証後、信頼エンジン１１０は、例えば、要求アプリケーションへの適切なパスワード等の要求された機密データを供給する。別の実施形態によれば、信頼エンジン１１０は、機密データボールトを記憶するための別のシステムを含んでもよい。例えば、信頼エンジン１１０は、データボールト機能性を実装し、比喩的に信頼エンジン１１０の前述のフロントエンドセキュリティシステムの「後ろ」に存在する独立型ソフトウェアエンジンを含んでもよい。この実施形態によれば、ソフトウェアエンジンが信頼エンジン１１０から肯定的なユーザ認証を示す信号を受信した後に、ソフトウェアエンジンは要求された機密データを供給する。

【０１３２】

さらに別の実施形態では、データボールトは、第三者システムによって実装されてもよい。ソフトウェアエンジンの実施形態と同様に、第三者システムが信頼エンジン１１０から肯定的なユーザ認証を示す信号を受信した後に、第三者システムは要求された機密データを有利に供給してもよい。さらに別の実施形態によれば、データボールトは、ユーザシステム１０５上で実装されてもよい。ユーザ側ソフトウェアエンジンは、信頼エンジン１１０から肯定的なユーザ認証を示す信号を受信した後に、前述のデータを有利に供給してもよい。

【０１３３】

前述のデータボールトが代替実施形態に関して開示されているが、当業者であれば、多数のその付加的な実装を本明細書の本開示から認識するであろう。例えば、特定のデータボールトは、前述の実施形態のうちのいくつかまたは全てからの側面を含んでもよい。加えて、前述のデータボールトのうちのいずれかは、様々なときに１つ以上の認証要求を採用してもよい。例えば、データボールトのうちのいずれかは、１つ以上のトランザクション毎に、周期的に、１つ以上のセッション毎に、１つ以上のウェブページまたはウェブサイトへのアクセス毎に、１つ以上の他の特定された間隔で、または同等のときに認証を要求してもよい。

【０１３４】

図１１は、本発明の実施形態の側面による、署名プロセス１１００のデータフローを図示する。図１１に示されるように、署名プロセス１１００は、図１０を参照して前述される認証プロセス１０００のステップと同様のステップを含む。本発明の一実施形態によれば、署名プロセス１１００は、以下でより詳細に論議されるように、最初にユーザを認証し、次いで、いくつかのデジタル署名機能のうちの１つ以上を果たす。別の実施形態によれば、署名プロセス１１００は、メッセージまたは文書のハッシュ、あるいは同等物等の、それに関連するデータを有利に記憶してもよい。このデータは、例えば、オーディットで、または参加当事者がトランザクションを拒否しようとする時等の任意の他の場合に、有利に使用されてもよい。

【０１３５】

図１１に示されるように、認証ステップ中に、ユーザおよびベンダは、例えば、契約等

のメッセージに有利に同意してもよい。署名中、署名プロセス１１００は、ユーザによって署名された契約がベンダによって供給された契約と同一であることを有利に確実にする。したがって、一実施形態によれば、認証中、ベンダおよびユーザは、認証エンジン２１５に伝送されるデータに、メッセージまたは契約のそれぞれのコピーのハッシュを含む。メッセージまたは契約のハッシュのみを採用することによって、信頼エンジン１１０は、有意に削減された量のデータを有意に記憶し、より効率的かつ費用効果的な暗号システムを提供してもよい。加えて、問題の文書が当事者のうちのいずれかによって署名されたものに合致するかどうか決定するために、記憶されたハッシュが問題の文書のハッシュと有利に比較されてもよい。文書がトランザクションに関するものと同一であるかどうかを決定する能力は、トランザクションへの当事者による拒否の請求に対して使用することができる、付加的な証拠を提供する。

【０１３６】

ステップ１１０３では、認証エンジン２１５が、登録認証データを集約し、それをユーザによって提供された現在の認証データと比較する。認証エンジン２１５のコンパレータが、登録認証データが現在の認証データに合致することを示すとき、認証エンジン２１５のコンパレータはまた、ベンダによって供給されるメッセージのハッシュを、ユーザによって供給されるメッセージのハッシュと比較する。したがって、認証エンジン２１５は、ユーザによって同意されたメッセージがベンダによって同意されたものと同一であることを有利に確実にする。

【０１３７】

ステップ１１０５では、認証エンジン２１５は、デジタル署名要求を暗号エンジン２２０に伝送する。本発明の一実施形態によれば、要求は、メッセージまたは契約のハッシュを含む。しかしながら、当業者であれば、暗号エンジン２２０は、所望のデジタル署名を形成するように、ビデオ、音声、生体測定、画像、またはテキストを含むがそれらに限定されない、事実上あらゆる種類のデータを暗号化してもよいことを、本明細書の本開示から認識するであろう。ステップ１１０５に戻って、デジタル署名要求は、好ましくは、従来のＳＳＬ技術を介して伝達されるＸＭＬ文書を備える。

【０１３８】

ステップ１１１０では、データ記憶設備Ｄ１乃至Ｄ４のそれぞれが、署名当事者に対応する１つまたは複数の暗号鍵のそれぞれの部分を伝送するように、認証エンジン２１５が要求をデータ記憶設備Ｄ１乃至Ｄ４のそれぞれに伝送する。別の実施形態によれば、暗号エンジン２２０が、最初に、署名当事者に対する保管場所２１０または保管場所システム７００から要求するために１つまたは複数の適切な鍵を決定し、適切な合致鍵を提供する措置を講じるように、暗号エンジン２２０は、前述の内容で論議される相互運用性プロセス９７０のステップのうちのいくつかまたは全てを採用する。なおも別の実施形態によれば、認証エンジン２１５または暗号エンジン２２０は、署名当事者と関連付けられ、保管場所２１０または保管場所システム７００に記憶された鍵のうちの１つ以上を有利に要求してもよい。

【０１３９】

一実施形態によれば、署名当事者は、ユーザおよびベンダの一方または両方を含む。そのような場合、認証エンジン２１５は、ユーザおよび／またはベンダに対応する暗号鍵を有利に要求する。別の実施形態によれば、署名当事者は、信頼エンジン１１０を含む。この実施形態では、信頼エンジン１１０は、認証プロセス１０００がユーザ、ベンダ、または両方を適正に認証したことを認定している。したがって、認証エンジン２１５は、デジタル署名を行うように、例えば、暗号エンジン２２０に属する鍵等の信頼エンジン１１０の暗号鍵を要求する。別の実施形態によれば、信頼エンジン１１０は、デジタル公証のような機能を果たす。この実施形態では、署名当事者は、信頼エンジン１１０とともに、ユーザ、ベンダ、または両方を含む。したがって、信頼エンジン１１０は、ユーザおよび／またはベンダのデジタル署名を提供し、次いで、ユーザおよび／またはベンダが適正に認証されたことを独自のデジタル署名で示す。この実施形態では、認証エンジン２１５は、

ユーザ、ベンダ、または両方に対応する暗号鍵の集約を有利に要求してもよい。別の実施形態によれば、認証エンジン２１５は、信頼エンジン１１０に対応する暗号鍵の集約を有利に要求してもよい。

【０１４０】

別の実施形態によれば、信頼エンジン１１０は、委任状のような機能を果たす。例えば、信頼エンジン１１０は、第三者に代わってメッセージをデジタル署名してもよい。そのような場合、認証エンジン２１５は、第三者と関連付けられる暗号鍵を要求する。この実施形態によれば、署名プロセス１１００は、委任状のような機能を可能にする前に、第三者の認証を有利に含んでもよい。加えて、認証プロセス１０００は、例えば、いつ、どのような状況で、特定の第三者の署名が使用されてもよいかを決定付ける、ビジネス論理または同等物等の第三者制約をチェックしてもよい。

【０１４１】

前述の内容に基づいて、ステップ１１１０では、認証エンジンが、署名当事者に対応するデータ記憶設備Ｄ１乃至Ｄ４から暗号鍵を要求した。ステップ１１１５では、データ記憶設備Ｄ１乃至Ｄ４が、署名当事者に対応する暗号鍵のそれぞれの部分を暗号エンジン２２０に伝送する。一実施形態によれば、前述の伝送は、ＳＳＬ技術を含む。別の実施形態によれば、前述の伝送は、暗号エンジン２２０の暗号鍵を用いて、有利に多重暗号化されてもよい。

【０１４２】

ステップ１１２０では、暗号エンジン２２０が、署名当事者の前述の暗号鍵を集約し、それを用いてメッセージを暗号化し、それにより、デジタル署名を形成する。署名プロセス１１００のステップ１１２５では、暗号エンジン２２０が、デジタル署名を認証エンジン２１５に伝送する。ステップ１１３０では、認証エンジン２１５が、ハッシュ化されたメッセージのコピーおよびデジタル署名とともに、満たされた認証要求をトランザクションエンジン２０５に伝送する。ステップ１１３５では、トランザクションエンジン２０５が、トランザクションＩＤ、認証が成功したかどうかという指示、およびデジタル署名を備える受領書をベンダに伝送する。一実施形態によれば、前述の伝送は、信頼エンジン１１０のデジタル署名を有利に含んでもよい。例えば、信頼エンジン１１０は、その秘密鍵を用いて受領書のハッシュを暗号化し、それにより、ベンダへの伝送に添付されるデジタル署名を形成してもよい。

【０１４３】

一実施形態によれば、トランザクションエンジン２０５はまた、確認メッセージをユーザに伝送する。署名プロセス１１００がその好ましい代替実施形態に関して開示されているが、本発明はそれによって限定されることを目的としていない。むしろ、当業者であれば、署名プロセス１１００の多数の代替案を本明細書の本開示から認識するであろう。例えば、ベンダは、Ｅメールアプリケーション等のユーザアプリケーションと置換されてもよい。例えば、ユーザは、デジタル署名で特定のＥメールにデジタル署名することを希望してもよい。そのような実施形態では、署名プロセス１１００の全体を通した伝送は、メッセージのハッシュの１つだけのコピーを有利に含んでもよい。また、当業者であれば、多数のクライアントアプリケーションがデジタル署名を要求してもよいことを、本明細書の本開示から認識するであろう。例えば、クライアントアプリケーションは、ワードプロセッサ、スプレッドシート、Ｅメール、音声メール、制限されたシステム領域へのアクセス、または同等物を備えてもよい。

【０１４４】

加えて、当業者であれば、署名プロセス１１００のステップ１１０５乃至１１２０が、図９Ｂの相互運用性プロセス９７０のステップのうちのいくつかまたは全てを有利に採用し、それにより、例えば、異なる署名種類の下でデジタル署名を処理する必要があってもよい異なる暗号システム間の相互運用性を提供してもよいことを、本明細書の本開示から認識するであろう。

【０１４５】

図１２は、本発明の実施形態の側面による、暗号化／復号プロセス１２００のデータフローを図示する。図１２に示されるように、復号プロセス１２００は、認証プロセス１０００を使用してユーザを認証することによって始まる。一実施形態によれば、認証プロセス１０００は、認証要求に同期セッション鍵を含む。例えば、従来のＰＫＩ技術では、公開および秘密鍵を使用してデータを暗号化または復号することは、数学的に集中的であり、有意なシステムリソースを必要としてもよいことが当業者によって理解される。しかしながら、対称鍵暗号システム、またはメッセージの送信者および受信者が、メッセージを暗号化および復号するために使用される単一の共通鍵を共有するシステムでは、数学的演算は、有意により単純かつ迅速である。したがって、従来のＰＫＩ技術では、メッセージの送信者が、同期セッション鍵を生成し、より単純かつ迅速な対称鍵システムを使用してメッセージを暗号化する。次いで、送信者は、受信者の公開鍵を用いてセッション鍵を暗号化する。暗号化されたセッション鍵は、同期暗号化されたメッセージに添付され、両方のデータが受信者に送信される。受信者は、セッション鍵を復号するために自分の秘密鍵を使用し、次いで、メッセージを復号するためにセッション鍵を使用する。前述の内容に基づいて、より単純かつ迅速な対称鍵システムが、暗号化／復号処理の大部分に使用される。したがって、復号プロセス１２００では、復号は、同期鍵がユーザの公開鍵を用いて暗号化されていることを有利に仮定する。したがって、前述のように、暗号化されたセッション鍵は、認証要求に含まれる。

【０１４６】

復号プロセス１２００に戻って、ユーザがステップ１２０５で認証された後、認証エンジン２１５は、暗号化されたセッション鍵を暗号エンジン２２０に転送する。ステップ１２１０では、認証エンジン２１５が、要求をデータ記憶設備Ｄ１乃至Ｄ４のそれぞれに転送し、ユーザの暗号鍵データを要求する。ステップ１２１５では、各データ記憶設備Ｄ１乃至Ｄ４が、暗号鍵のそれぞれの部分を暗号エンジン２２０に転送する。一実施形態によれば、前述の伝送は、暗号エンジン２２０の公開鍵を用いて暗号化される。

【０１４７】

復号プロセス１２００のステップ１２２０では、暗号エンジン２２０が、暗号鍵を集約し、それを用いてセッション鍵を復号する。ステップ１２２５では、暗号エンジンが、セッション鍵を認証エンジン２１５に転送する。ステップ１２２７では、認証エンジン２１５が、復号されたセッション鍵を含む認証要求を見たし、満たされた認証要求をトランザクションエンジン２０５に伝送する。ステップ１２３０では、トランザクションエンジン２０５が、セッション鍵とともに認証要求を要求アプリケーションまたはベンダに転送する。次いで、一実施形態によれば、要求アプリケーションまたはベンダは、暗号化されたメッセージを復号するためにセッション鍵を使用する。

【０１４８】

復号プロセス１２００がその好ましい代替実施形態に関して開示されているが、当業者であれば、復号プロセス１２００の多数の代替案を本明細書の本開示から認識するであろう。例えば、復号プロセス１２００は、同期鍵暗号化を差し控え、完全公開鍵技術に依存してもよい。そのような実施形態では、要求アプリケーションが、メッセージ全体を暗号エンジン２２０に伝送してもよく、またはメッセージを暗号エンジン２２０に伝送するために何らかの種類の圧縮または可逆的ハッシュを採用してもよい。当業者であれば、前述の通信がＳＳＬ技術で包まれたＸＭＬ文書を有利に含んでもよいことも、本明細書の本開示から認識するであろう。

【０１４９】

暗号化／復号プロセス１２００はまた、文書または他のデータの暗号化も提供する。したがって、ステップ１２３５では、要求アプリケーションまたはベンダが、信頼エンジン１１０のトランザクションエンジン２０５に、ユーザの公開鍵の要求を有利に伝送してもよい。例えば、文書またはメッセージを暗号化するために使用されるセッション鍵を暗号化するために、要求アプリケーションまたはベンダがユーザの公開鍵を使用するため、要求アプリケーションまたはベンダは、この要求を行う。登録プロセス９００で記述される

ように、トランザクションエンジン２０５は、例えば、大容量記憶装置２２５に、ユーザのデジタル証明書のコピーを記憶する。したがって、暗号化プロセス１２００のステップ１２４０では、トランザクションエンジン２０５は、大容量記憶装置２２５からユーザのデジタル証明書を要求する。ステップ１２４５では、大容量記憶装置２２５が、ユーザに対応するデジタル証明書をトランザクションエンジン２０５に伝送する。ステップ１２５０では、トランザクションエンジン２０５が、デジタル証明書を要求アプリケーションまたはベンダに伝送する。一実施形態によれば、暗号化プロセス１２００の暗号化部分は、ユーザの認証を含まない。これは、要求ベンダがユーザの公開鍵のみを必要とし、いずれの機密データも要求していないためである。

【０１５０】

当業者であれば、特定のユーザがデジタル証明書を持たない場合、信頼エンジン１１０は、その特定のユーザ用のデジタル証明書を生成するために、登録プロセス９００のいくらかまたは全てを採用してもよいことを、本明細書の本開示から認識するであろう。次いで、信頼エンジン１１０は、暗号化／復号プロセス１２００を開始し、それにより、適切なデジタル証明書を提供してもよい。加えて、当業者であれば、暗号化／復号プロセス１２００のステップ１２２０および１２３５乃至１２５０が、図９Ｂの相互運用性プロセスのステップのうちのいくつかまたは全てを有利に採用し、それにより、例えば、暗号化を処理する必要があってもよい、異なる暗号システム間の相互運用性を提供してもよいことを、本明細書の本開示から認識するであろう。

【０１５１】

図１３は、は、本発明のさらに別の実施形態の側面による、信頼エンジンシステム１３００の簡略化したブロック図を図示する。図１３に示されるように、信頼エンジンシステム１３００は、それぞれ、複数の明確に異なる信頼エンジン１３０５、１３１０、１３１５、および１３２０を備える。本発明のより完全な理解を促進するために、図１３は、トランザクションエンジン、保管場所、および認証エンジンを有するものとして、各信頼エンジン１３０５、１３１０、１３１５、および１３２０を図示する。しかしながら、当業者であれば、各トランザクションエンジンが、図１－８を参照して開示される要素および通信チャネルのうちのいくつか、組み合わせ、または全てを有利に備えてもよいことを認識するであろう。例えば、一実施形態は、１つ以上のトランザクションエンジン、保管場所、および暗号サーバ、またはそれらの任意の組み合わせを有する信頼エンジンを有利に含んでもよい。

【０１５２】

本発明の一実施形態によれば、例えば、信頼エンジン１３０５が第１の場所に存在してもよく、信頼エンジン１３１０が第２の場所に存在してもよく、信頼エンジン１３１５が第３の場所に存在してもよく、信頼エンジン１３２０が第４の場所に存在してもよいように、信頼エンジン１３０５、１３１０、１３１５、および１３２０のそれぞれは、地理的に分離される。前述の地理的分離は、全体的な信頼エンジンシステム１３００のセキュリティを増大させながら、システム応答時間を有利に減少させる。

【０１５３】

例えば、ユーザが暗号システム１００にログオンするときに、ユーザは、第１の場所に最も近くてもよく、認証されることを所望してもよい。図１０を参照して説明されるように、認証されるために、ユーザは、生体測定または同等物等の現在の認証データを提供し、現在の認証データは、ユーザの登録認証データと比較される。したがって、一実施例によれば、ユーザは、現在の認証データを地理的に最も近い信頼エンジン１３０５に有利に提供する。次いで、信頼エンジン１３０５のトランザクションエンジン１３２１は、現在の認証データを、同様に第１の場所に存在する認証エンジン１３２２に転送する。別の実施形態によれば、トランザクションエンジン１３２１は、現在の認証データを、信頼エンジン１３１０、１３１５、または１３２０の認証エンジンのうちの１つ以上に転送する。

【０１５４】

トランザクションエンジン１３２１はまた、例えば、信頼エンジン１３０５乃至１３２

０のそれぞれの保管場所から、登録認証データの集約を要求する。この実施形態によれば、各保管場所は、その登録認証データ部分を信頼エンジン１３０５の認証エンジン１３２２に提供する。次いで、認証エンジン１３２２は、応答するために、例えば、最初の２つの保管場所から、暗号化されたデータ部分を採用し、登録認証データを解読された形態に組み立てる。認証エンジン１３２２は、登録認証データを現在の認証データと比較し、認証結果を信頼エンジン１３０５のトランザクションエンジン１３２１に返信する。

【０１５５】

上記に基づいて、信頼エンジンシステム１３００は、認証プロセスを行うために、複数の地理的に分離された信頼エンジン１３０５乃至１３２０のうちの最も近いものを採用する。本発明の一実施形態によれば、最も近いトランザクションエンジンへの情報のルーティングは、ユーザシステム１０５、ベンダシステム１２０、または証明機関１１５のうちの１つ以上の上で実行する、クライアント側アプレットにおいて有利に行われてもよい。代替実施形態によれば、信頼エンジン１３０５乃至１３２０から選択するために、より洗練された決定プロセスが採用されてもよい。例えば、決定は、所与の信頼エンジンの可用性、操作性、接続の速度、負荷、性能、地理的な近接性、またはそれらの組み合わせに基づいてもよい。

【０１５６】

このようにして、信頼エンジンシステム１３００は、各データ記憶設備が無作為化された機密データ部分を記憶する、図７を参照して論議されるもの等の、地理的に遠隔のデータ記憶設備と関連付けられるセキュリティ利点を維持しながら、その応答時間を減らす。例えば、信頼エンジン１３１５の保管場所１３２５におけるセキュリティ侵害は、例えば、信頼エンジンシステム１３００の機密データを必ずしも損なうとは限らない。これは、保管場所１３２５が、それ以上なければ全く役に立たない、解読不可能な無作為化されたデータのみを含有するためである。

【０１５７】

別の実施形態によれば、信頼エンジンシステム１３００は、認証エンジンと同様に配設される複数の暗号エンジンを有利に含んでもよい。暗号エンジンは、図１－８を参照して開示されるもの等の暗号機能を有利に果たしてもよい。さらに別の実施形態によれば、信頼エンジンシステム１３００は、有利に複数の認証エンジンを複数の暗号エンジンと置換し、それにより、図１－８を参照して開示されるもの等の暗号機能を有利に果たしてもよい。本発明のさらに別の実施形態によれば、信頼エンジンシステム１３００は、各複数の認証エンジンを、前述の内容で開示されるような認証エンジン、暗号エンジン、または両方の機能性のいくらかまたは全てを有するエンジンと置換してもよい。

【０１５８】

信頼エンジンシステム１３００がその好ましい代替実施形態に関して開示されているが、当業者であれば、信頼エンジンシステム１３００が信頼エンジン１３０５乃至１３２０の部分を備えてもよいことを認識するであろう。例えば、信頼エンジンシステム１３００は、１つ以上のトランザクションエンジン、１つ以上の保管場所、１つ以上の認証エンジン、または１つ以上の暗号エンジン、あるいはそれらの組み合わせを含んでもよい。

【０１５９】

図１４は、本発明のさらに別の実施形態の側面による、信頼エンジンシステム１４００の簡略化したブロック図を図示する。図１４に示されるように、信頼エンジンシステム１４００は、複数の信頼エンジン１４０５、１４１０、１４１５、および１４２０を含む。一実施形態によれば、信頼エンジン１４０５、１４１０、１４１５、および１４２０のそれぞれは、図１－８を参照して開示される信頼エンジン１１０の要素のうちのいくつかまたは全てを備える。この実施形態によれば、ユーザシステム１０５、ベンダシステム１２０、または証明機関１１５のクライアント側アプレットが、信頼エンジンシステム１４００と通信するときに、これらの通信は、信頼エンジン１４０５乃至１４２０のそれぞれのＩＰアドレスに送信する。さらに、信頼エンジン１４０５、１４１０、１４１５、および１４２０のそれぞれの各トランザクションエンジンは、図１３を参照して開示される信頼

エンジン１３０５のトランザクションエンジン１３２１と同様に挙動する。例えば、認証プロセス中に、信頼エンジン１４０５、１４１０、１４１５、および１４２０のそれぞれの各トランザクションエンジンは、現在の認証データをそれぞれの認証エンジンに伝送し、信頼エンジン１４０５乃至１４２０のそれぞれの保管場所のそれぞれに記憶された無作為化データを集約する要求を伝送する。図１４は、そのような説明図は過度に複雑になるため、これらの通信の全てを図示するわけではない。認証プロセスを続けて、次いで、保管場所のそれぞれは、その無作為化データ部分を、信頼エンジン１４０５乃至１４２０のそれぞれの認証エンジンのそれぞれに伝達する。信頼エンジンのそれぞれの認証エンジンのそれぞれは、現在の認証データが、信頼エンジン１４０５乃至１４２０のそれぞれの保管場所によって提供された登録認証データに合致するかどうかを決定するために、そのコンパレータを採用する。この実施形態によれば、次いで、認証エンジンのそれぞれによる比較の結果は、他の３つの信頼エンジンの冗長性モジュールに伝送される。例えば、信頼エンジン１４０５からの認証エンジンの結果は、信頼エンジン１４１０、１４１５、および１４２０の冗長性モジュールに伝送される。したがって、信頼エンジン１４０５の冗長性モジュールは、同様に、信頼エンジン１４１０、１４１５、および１４２０から認証エンジンの結果を受信する。

【０１６０】

図１５は、図１４の冗長性モジュールのブロック図を図示する。冗長性モジュールは、３つの認証エンジンから認証結果を受信し、その結果を第４の信頼エンジンのトランザクションエンジンに伝送するように構成される、コンパレータを備える。コンパレータは、３つの認証エンジンから認証結果を比較し、結果のうちの２つが一致する場合、コンパレータは、認証結果が２つの同意する認証エンジンの認証結果に合致すると結論を出す。次いで、この結果は、３つの認証エンジンと関連付けられていない信頼エンジンに対応するトランザクションエンジンに返送される。

【０１６１】

前述の内容に基づいて、冗長性モジュールは、好ましくは、その冗長性モジュールの信頼エンジンから地理的に遠隔にある認証エンジンから受信されたデータから、認証結果を決定する。そのような冗長性機能性を提供することによって、信頼エンジンシステム１４００は、信頼エンジン１４０５乃至１４２０のうちの１つの認証エンジンのセキュリティ侵害が、その特定の信頼エンジンの冗長性モジュールの認証結果を損なうのに不十分であることを確実にする。当業者であれば、信頼エンジンシステム１４００の冗長性モジュール機能性はまた、信頼エンジン１４０５乃至１４２０のそれぞれの暗号エンジンに適用されてもよいことを認識するであろう。しかしながら、複雑性を回避するために、図１４ではそのような暗号エンジン通信を示さなかった。また、当業者であれば、図１５のコンパレータに対する多数の代替的な認証結果競合解決アルゴリズムが、本発明で使用するために好適であることを認識するであろう。

【０１６２】

本発明のさらに別の実施形態によれば、信頼エンジンシステム１４００は、暗号比較ステップ中に冗長性モジュールを有利に採用してもよい。例えば、図１４および１５に関する前述の冗長性モジュールの開示のいくらかまたは全ては、特定のトランザクション中に１人以上の当事者によって提供される文書のハッシュ比較中に、有利に実装されてもよい。

【０１６３】

前述の発明は、ある好ましい代替実施形態に関して説明されているが、他の実施形態が、本明細書の本開示から当業者に明白となるであろう。例えば、信頼エンジン１１０は、秘密暗号鍵が所定の期間にわたってユーザに公開される、短期証明書を発行してもよい。例えば、現在の証明書基準は、所定量の時間後に満了するように設定することができる、有効性フィールドを含む。したがって、信頼エンジン１１０は、秘密鍵をユーザに公開してもよく、秘密鍵は、例えば、２４時間にわたって有効となる。そのような実施形態によれば、信頼エンジン１１０は、特定のユーザと関連付けられる新しい暗号鍵ペアを有利に

発行し、次いで、新しい暗号鍵ペアの秘密鍵を公開してもよい。次いで、いったん秘密暗号鍵が公開されると、信頼エンジン１１０は、もはや信頼エンジン１１０によって確保可能ではなくなるため、そのような秘密鍵の内部有効使用を即時に失効させる。

【０１６４】

加えて、当業者であれば、暗号システム１００または信頼エンジン１１０が、ラップトップ、携帯電話、ネットワーク、生体測定デバイス、または同等物等であるがそれらに限定されない、任意の種類のデバイスを認識する能力を含んでもよいことを認識するであろう。一実施形態によれば、そのような認識は、アクセスまたは使用につながる認証の要求、暗号機能性の要求、または同等物等の特定のサービスの要求において供給されるデータに由来してもよい。一実施形態によれば、前述の要求は、例えば、プロセッサＩＤ等の一意のデバイス識別子を含んでもよい。代替として、要求は、特定の認識可能なデータ形式でデータを含んでもよい。例えば、携帯および衛星電話はしばしば、フルＸ５０９．ｖ３多重暗号化証明書に対する処理能力を含まず、したがって、それらを要求しない。この実施形態によれば、信頼エンジン１１０は、提示されるデータ形式の種類を認識し、同じ方法のみで応答してもよい。

【０１６５】

上記で説明されるシステムの付加的な側面では、以下で説明されるような種々の技法を使用して、文脈依存認証を提供することができる。例えば、図１６に示されるような文脈依存認証は、ユーザが自分自身を認証しようとするときにユーザによって送信される実際のデータだけでなく、そのデータの生成および送達をめぐる状況も評価するという可能性を提供する。そのような技法はまた、以下で説明されるように、ユーザと信頼エンジン１１０との間、またはベンダと信頼エンジン１１０との間のトランザクション特異的信頼裁定を支援してもよい。

【０１６６】

上記で論議されるように、認証は、ユーザが自分であると言う者であることを証明するプロセスである。概して、認証は、いくらかの事実を認証機関に実証することを必要とする。本発明の信頼エンジン１１０は、ユーザが自分自身を認証しなければならない機関を表す。ユーザは、ユーザのみが知っているはずのものを知ること（知識ベースの認証）、ユーザのみが持っているはずのものを有すること（トークンベースの認証）、またはユーザのみがなるはずであるものになること（生体測定ベースの認証）によって、ユーザが自分であると言う者であることを信頼エンジン１１０に実証しなければならない。

【０１６７】

知識ベースの認証の実施例は、パスワード、ＰＩＮ番号、またはロックの組み合わせを無制限に含む。トークンベースの認証の実施例は、家の鍵、物理的なクレジットカード、運転免許証、または特定の電話番号を無制限に含む。生体測定ベースの認証の実施例は、指紋、筆跡分析、顔面スキャン、手スキャン、耳スキャン、虹彩スキャン、血管パターン、ＤＮＡ、音声分析、または網膜スキャンを無制限に含む。

【０１６８】

各種類の認証は、特定の利点および不利点を有し、それぞれ異なるレベルのセキュリティを提供する。例えば、概して、誰かのパスワードを耳にしてそれを繰り返すよりも、他の誰かの指紋に合致する偽の指紋を作成するほうが困難である。各種類の認証はまた、その形態の認証を使用する誰かを検証するために、異なる種類のデータが認証機関に知られることを必要とする。

【０１６９】

本明細書で使用されるように、「認証」とは、誰かの身元が自分であると言う者であることを検証する全体的プロセスを広く指す。「認証技法」とは、特定の１つの知識、物理的トークン、または生体測定値に基づく、特定の種類の認証を指す。「認証データ」とは、身元を確立するために認証機関に送信されるか、またはそうでなければ実証される情報を指す。「登録データ」とは、認証データとの比較のための基準を確立するために、最初に認証機関に提出されるデータを指す。「認証インスタンス」とは、認証技法によって認

証する試行と関連付けられるデータを指す。

【０１７０】

図１０を参照して、ユーザを認証するプロセスに関与する内部プロトコルおよび通信を説明する。その内部で文脈依存認証が行われる、このプロセスの一部は、図１０のステップ１０４５として示された比較ステップ内で発生する。このステップは、認証エンジン２１５内で行われ、保管場所２１０から回収された登録データ４１０を集約し、ユーザによって提供された認証データをそれと比較することを伴う。このプロセスの１つの特定の実施形態を図１６に示し、以下で説明する。

【０１７１】

ユーザによって提供された現在の認証データおよび保管場所２１０から回収された登録データは、図１６のステップ１６００で認証エンジン２１５によって受信される。これらのデータのセットの両方は、別個の認証の技法に関連するデータを含有してもよい。認証エンジン２１５は、ステップ１６０５で、各個別認証インスタンスと関連付けられた認証データを分離する。これは、認証データがユーザに対する登録データの適切なサブセットと比較されるため必要である（例えば、指紋認証データは、パスワード登録データよりもむしろ指紋登録データと比較されるべきである）。

【０１７２】

概して、ユーザを認証することは、どの認証技法がユーザに利用可能であるかに応じて、１つ以上の個別認証インスタンスを伴う。これらの方法は、登録プロセス中にユーザによって提供された登録データ（ユーザが登録するときに網膜スキャンを提供しなかった場合、網膜スキャンを使用して自分自身を認証することができなくなる）、ならびに現在ユーザに利用可能であってもよい手段（例えば、ユーザが現在の場所で指紋読取機を持っていない場合、指紋認証は実用的ではなくなる）によって限定される。場合によっては、単一の認証インスタンスがユーザを認証するのに十分であってもよいが、ある状況では、特定のトランザクションのためにユーザをより確信して認証するために、複数の認証インスタンスの組み合わせが使用されてもよい。

【０１７３】

各認証インスタンスは、特定の認証技法に関連するデータ（例えば、指紋、パスワード、スマートカード等）およびその特定の技法のためのデータの捕捉および送達を包囲する状況から成る。例えば、パスワードを介して認証しようとすることの特定のインスタンスは、パスワード自体に関連するデータだけでなく、そのパスワード試行に関連する「メタデータ」として知られている状況データも生成する。この状況データは、特定の認証インスタンスが行われた時間、認証情報が送達されたネットワークアドレス、ならびに、認証データの起源について決定されてもよい、当業者に公知であるような任意の他の情報（接続の種類、プロセッサシリアル番号等）等の情報を含む。

【０１７４】

多くの場合、少量の状況メタデータのみが利用可能となる。例えば、ユーザが、発信元コンピュータのアドレスを隠す、プロキシまたはネットワークアドレス変換あるいは別の技法を使用するネットワーク上に位置する場合、プロキシまたはルータのアドレスのみが決定されてもよい。同様に、多くの場合、使用されているハードウェアまたはオペレーティングシステムの制限、システムの操作者によるそのような特徴の無効化、またはユーザのシステムと信頼エンジン１１０との間の接続の他の制限により、プロセッサシリアル番号等の情報は利用可能とならない。

【０１７５】

図１６に示されるように、いったん認証データ内で表された個別認証インスタンスがステップ１６０５で抽出されて分離されると、認証エンジン２１５は、ユーザが自分であると主張する者であることを示す際に、その信頼性に対する各インスタンスを評価する。単一の認証インスタンスに対する信頼性は、概して、いくつかの因子に基づいて決定される。これらは、ステップ１６１０で評価される、認証技法と関連付けられる信頼性に関する因子、およびステップ１８１５で評価される、提供された特定の認証データの信頼性に関

する因子としてグループ化されてもよい。第１のグループは、使用されている認証技法の固有信頼性、およびその方法とともに使用されている登録データの信頼性を無制限に含む。第２のグループは、登録データと認証インスタンスが提供されたデータとの間の合致の程度、およびその認証インスタンスと関連付けられるメタデータを無制限に含む。これらの因子のそれぞれは、他の因子とは無関係に変化してもよい。

【０１７６】

認証技法の固有信頼性は、詐称者が他の誰かの正しいデータを提供することがどれだけ困難であるか、ならびに認証技法の全体的な誤差率に基づく。パスワードおよび知識ベースの認証方法について、誰かがパスワードを別の個人に明かすことを防止し、その第２の個人がそのパスワードを使用することを防止するものがないため、この信頼性はしばしばかなり低い。さらに複雑な知識ベースのシステムは、知識が個人から個人へかなり容易に移送されてもよいため、中程度の信頼性のみを有してもよい。適正なスマートカードを有すること、または認証を行うために特定の端末を使用すること等のトークンベースの認証は、適任者が適正なトークンを保有しているという保証がないため、同様に、単独で使用されると信頼性が低い。

【０１７７】

しかしながら、意図的でさえ、便宜的に指紋を使用する能力を他の誰かに提供することは概して困難であるため、生体測定技法は、より本質的に信頼性がある。生体測定認証技法を妨害することがより困難であるため、生体測定方法の固有信頼性は、純粋に知識またはトークンベースの認証技法の信頼性よりも概して高い。しかしながら、生体測定技法でさえも、誤った容認または誤った拒絶が生成される機会があり得る。これらの発生は、同じ生体測定技法の異なる実装に対する異なる信頼性によって反映されてもよい。例えば、より高品質の光学部またはより良好な走査解像度、あるいは誤った容認または誤った拒絶の発生を低減する何らかの他の改良を使用するため、１つの企業によって提供される指紋照合システムが、異なる企業によって提供されるものよりも高い信頼性を提供してもよい。

【０１７８】

この信頼性は、異なる方式で表されてもよいことに留意されたい。この信頼性は、望ましくは、確認証の確信レベルを計算するために認証エンジン２１５のヒューリスティクス５３０およびアルゴリズムによって使用することができる、何らかの測定基準で表される。これらの信頼性を表す１つの好ましいモードは、パーセンテージまたは割合としてのものである。例えば、指紋が、９７％の固有信頼性を割り当てられる場合がある一方で、パスワードは、５０％の固有信頼性しか割り当てられない場合がある。当業者であれば、これらの特定の値は例示的にすぎず、具体的な実装の間で変化してもよいことを認識するであろう。

【０１７９】

信頼性が評価されてもよい第２の要素は、登録の信頼性である。これは、上記で参照される「等級別登録」プロセスの一部である。この信頼性因子は、最初の登録プロセス中に提供される識別の信頼性を反映する。例えば、個人が、最初に、身元の証明を公証人または他の役人に物理的に生成する方式で登録し、登録データがそのときに記録されて公証される場合、データは、登録中にネットワーク上で提供され、デジタル署名または正確には個人に結び付けられない他の情報によって保証されるのみであるデータよりも信頼性がある。

【０１８０】

異なるレベルの信頼性を伴う他の登録技法は、信頼エンジン１１０の操作者の物理的なオフィスでの登録、ユーザの勤務先での登録、郵便局または旅券局での登録、信頼エンジン１１０の操作者にとっての提携当事者または信頼できる当事者を通した登録、登録された身元が特定の実際の個人でまだ識別されていない、匿名または変名登録、ならびに当技術分野で公知であるようなそのような他の手段を無制限に含む。

【０１８１】

これらの因子は、信頼エンジン１１０と登録中に提供される識別の供給源との間の信頼を反映する。例えば、身元の証明を提供する初期プロセス中に従業員と関連して登録が行われる場合、この情報は、企業内での目的で極めて信頼性があると見なされてもよいが、政府機関によって、または競合者によって、より少ない程度に信頼されてもよい。したがって、これらの他の組織のそれぞれによって操作される信頼エンジンは、この登録に異なるレベルの信頼性を割り当ててもよい。

【０１８２】

同様に、ネットワークにわたって提出されるが、同じ信頼エンジン１１０を用いた以前の登録中に提供された他の信頼できるデータによって認証される、付加的なデータは、たとえ元の登録データが開放型ネットワークにわたって提出されたとしても、後者のデータと同じくらい信頼性があると見なされてもよい。そのような状況において、後続の公証は、元の登録データと関連付けられる信頼性のレベルを効果的に増加させる。このようにして、次いで、例えば、登録されたデータに合致する個人の身元を、ある登録職員に実証することによって、匿名または変名登録が完全登録に昇進してもよい。

【０１８３】

上記で論議される信頼性因子は、概して、任意の特定の認証インスタンスより前に決定されてもよい値である。これは、それらが実際の認証よりも登録および技法に基づくためである。一実施形態では、これらの因子に基づいて信頼性を生成するステップは、この特定の認証技法の以前に決定された値およびユーザの登録データを調べることを伴う。本発明の有利な実施形態のさらなる側面では、そのような信頼性は、登録データ自体を伴って含まれてもよい。このようにして、これらの因子は、保管場所２１０から送信される登録データとともに、認証エンジン２１５に自動的に送達される。

【０１８４】

これらの因子は、概して、個人認証インスタンスより前に決定されてもよいが、その特定の認証の技法をそのユーザに使用する、各認証インスタンスに依然として影響を及ぼす。さらに、値は経時的に変化してもよい（例えば、ユーザがより信頼性のある様式で再登録する場合）が、認証データ自体には依存していない。対照的に、単一の特定のインスタンスのデータと関連付けられる信頼性因子は、各機会に変化してもよい。これらの因子は、以下で論議されるように、ステップ１８１５で信頼性スコアを生成するために、それぞれの新しい認証について評価されなければならない。

【０１８５】

認証データの信頼性は、特定の認証インスタンスにおいてユーザによって提供されるデータと、認証登録中に提供されるデータとの間の合致を反映する。これは、認証データが、ユーザがそうであると主張する個人に対する登録データに合致するかどうかの基本的な質問である。通常、データが合致しない時、ユーザは認証が成功したと見なされず、認証は失敗する。これが評価される方式は、使用される認証技法に応じて変化してもよい。そのようなデータの比較は、図５に示されるような認証エンジン２１５のコンパレータ５１５の機能によって行われる。

【０１８６】

例えば、パスワードの合致は、概して、二値様式で評価される。言い換えれば、パスワードは、完全合致または合致失敗である。通常、完全に正確でなければ、正確なパスワードに近いパスワードを部分合致として容認することさえ望ましくない。したがって、パスワード認証を評価する時、コンパレータ５１５によって返信される認証の信頼性は、一般的には、１００％（正）または０％（誤）のいずれか一方であり、中間値の可能性はない。

【０１８７】

パスワードについて、これらと同様の規則は、概して、スマートカード等のトークンベースの認証方法に適用される。これは、同様の識別子を有する、または正しいものと同様であるスマートカードを有することが、任意の他の不正確なトークンを有することと同じくらい間違っているためである。したがって、トークンはまた、ユーザが正しいトークン

を有するか、またはそうではないといった、二値認証符号となる傾向がある。

【０１８８】

しかしながら、質問表および生体測定等の、ある種類の認証データは、概して、二値認証符号ではない。例えば、指紋は、様々な程度で参照指紋に合致してもよい。ある程度、これは、初期登録中または後続の認証において捕捉されるデータの質の変動によるものであってもよい。（指紋がはっきりしない場合があるか、または個人が特定の指に依然として治癒中の瘢痕または熱傷を有する場合がある。）他の場合において、情報自体がいくらか可変性であり、パターン照合に基づくため、データは、完璧とは言えない程度に合致してもよい。（背景雑音、音声が録音された環境の音響効果により、または個人が風邪をひいているため、音声分析は、近いが全く正しいとは思われない場合がある。）最終的に、大量のデータが比較されている状況では、単純に、データの大部分が十分に合致するが、いくつかがそうではないという場合であってもよい。（１０の質問の質問表が、個人的な質問に対して８つの正しい答えを生じるが、２つの間違った答えを生じていてもよい。）これらの理由のうちのいずれかについて、登録データと特定の認証インスタンスのデータとの間の合致は、望ましくは、コンパレータ５１５によって部分合致値が割り当てられてもよい。このようにして、例えば、指紋は８５％合致であるといわれ、声紋は６５％合致であるといわれ、質問表は８０％合致であるといわれる場合がある。

【０１８９】

コンパレータ５１５によって生成される、この尺度（合致の程度）は、認証が正しいか否かという基本的な問題を表す因子である。しかしながら、上記で論議されるように、これは、所与の認証インスタンスの信頼性を決定する際に使用されてもよい、因子のうちの１つにすぎない。いくらかの部分的な程度での合致が決定されてもよいものの、最終的には、部分合致に基づいて二値結果を提供することが望ましくてもよいことも留意されたい。代替動作モードでは、合致の程度が合致の特定の閾値レベルに合格するか否かに基づいて、二値、すなわち、完全合致（１００％）または合致失敗（０％）のいずれか一方として、部分合致を取り扱うことも可能である。そのようなプロセスは、そうでなければ部分合致を生成する、システムの合致の単純な合格／失敗レベルを提供するために使用されてもよい。

【０１９０】

所与の認証インスタンスの信頼性を評価する際に考慮される別の因子は、この特定のインスタンスの認証データが提供される状況に関する。上記で論議されるように、状況とは、特定の認証インスタンスと関連付けられるメタデータを指す。これは、決定することができる程度まで認証符号のネットワークアドレス、認証の時間、認証データの伝送モード（電話回線、携帯電話、ネットワーク等）、および認証符号のシステムのシリアル番号等の情報を無制限に含んでもよい。

【０１９１】

これらの要素は、通常ユーザによって要求される認証の種類のプロファイルを生成するために使用することができる。次いで、この情報は、少なくとも２つの方式で信頼性を評価するために使用することができる。１つの方法は、ユーザが、このユーザによる認証の通常のプロファイルと一致する方式で、認証を要求しているかどうかを考慮することである。ユーザが通常、営業日中（ユーザが勤務している時）には１つのネットワークアドレスから、夜間または週末中（ユーザが自宅にいる時）には異なるネットワークアドレスから、認証要求を行う場合、営業日中にホームアドレスから発生する認証は、通常の認証プロファイル外であるため、あまり信頼性がない。同様に、ユーザが通常、夜間に指紋生体測定を使用して認証する場合、パスワードのみを使用して日中に起こる認証は、あまり信頼性がない。

【０１９２】

認証のインスタンスの信頼性を評価するために状況メタデータを使用することができる、付加的な方法は、認証符号がそうであると主張する個人であるという裏付け証拠を状況がどれだけ提供するかを決定することができる。例えば、認証が、ユーザと関連付けられ

ることが分かっているシリアル番号を伴うシステムに由来する場合、これは、ユーザが自分であると主張する個人であるという良好な状況指標である。逆に、ユーザがロンドンに滞在していることが分かっているときに、認証が、ロサンゼルスにあることが分かっているネットワークアドレスに由来している場合、これは、その状況に基づいて、この認証はあまり信頼性がないという指示である。

【０１９３】

ベンダシステムまたは信頼エンジン１１０と相互作用するときに、システムがユーザによって使用されると、クッキーまたは他の電子データが配置されてもよいことも可能である。このデータは、ユーザのシステムの記憶装置に書き込まれ、ユーザシステム上のウェブブラウザまたは他のソフトウェアによって読み出される識別を含有してもよい。このデータが、セッション間にユーザシステム上で存在することを許可される場合（「永続的なクッキー」）、特定のユーザの認証中に、このシステムの過去の使用のさらなる証明として、認証データとともに送信されてもよい。事実上、所与のインスタンスのメタデータ、具体的には永続的なクッキーは、一種のトークンベースの認証符号自体を形成してもよい。

【０１９４】

いったん認証インスタンスの技法およびデータに基づく適切な信頼性因子が、それぞれステップ１６１０および１６１５において上記で説明されるように生成されると、それらはステップ１６２０で提供される認証インスタンスの全体的な信頼性を生成するために使用される。これを行う１つの手段は、単純に、各信頼性をパーセンテージとして表し、次いで、それらを一緒に乗じることである。

【０１９５】

例えば、ユーザの過去の認証プロファイルに完全に従って、認証データが、ユーザのホームコンピュータであることが分かっているネットワークアドレスから送信されており（１００％）、使用されている技法が指紋識別（９７％）であり、初期指紋データが信頼エンジン１１０を用いてユーザの雇用主を介して送られ（９０％）、認証データと登録データの中の元の指紋テンプレートとの間の合致が良好である（９９％）と仮定されたい。次いで、この認証インスタンスの全体的信頼性は、１００％＊９７％＊９０％＊９９％－８６．４％信頼性といった、これらの確率の積として計算することができる。

【０１９６】

この計算された信頼性は、単一の認証のインスタンスの信頼性を表す。単一の認証インスタンスの全体的信頼性はまた、例えば、異なる加重が各信頼性因子に割り当てられる公式を使用することによって、異なる信頼性因子を異なって取り扱う技法を使用して、計算されてもよい。さらに、当業者であれば、使用される実際の値が、パーセンテージ以外の値を表してもよく、かつ非算術システムを使用してもよいことを認識するであろう。一実施形態は、各因子に対する加重、および認証インスタンスの全体的信頼性を確立する際に使用されるアルゴリズムを設定するために、認証リクエスタによって使用されるモジュールを含んでもよい。

【０１９７】

認証エンジン２１５は、ステップ１６２０として示される、単一の認証インスタンスの信頼性を決定するために、上記の技法および変化例を使用してもよい。しかしながら、これは、同時に提供される複数の認証インスタンスに対する多くの認証状況で有用であってもよい。例えば、本発明のシステムを使用して自分を認証しようとするときに、ユーザは、ユーザ識別、指紋認証データ、スマートカード、およびパスワードを提供してもよい。そのような場合、３つの独立認証インスタンスが、評価のために信頼エンジン１１０に提供されている。ステップ１６２５へ進んで、ユーザによって提供されたデータが１つより多くの認証インスタンスを含むと認証エンジン２１５が決定した場合には、各インスタンスは、ステップ１６３０で示されるように選択され、ステップ１６１０、１６１５、および１６２０において上記で説明されるように評価される。

【０１９８】

論議される信頼性因子の多くは、これらのインスタンスによって変化してもよいことを留意されたい。例えば、これらの技法の固有信頼性、ならびに認証データと登録データとの間で提供される合致の程度は、異なる可能性が高い。さらに、ユーザは、これらの技法のそれぞれについて、異なる時間で、かつ異なる状況下で、登録データを提供していてもよく、同様に、これらのインスタンスのそれぞれに対して異なる登録信頼性を提供する。最終的に、たとえこれらのインスタンスのそれぞれに対するデータが提供されている状況が同じであっても、そのような技法の使用は、ユーザのプロファイルに異なって適合してもよく、よって、異なる状況信頼性が割り当てられてもよい。（例えば、ユーザは通常、スマートカードではなく、パスワードおよび指紋を使用してもよい）。

【０１９９】

結果として、これらの認証インスタンスのそれぞれの最終信頼性は、相互に異なってもよい。しかしながら、複数のインスタンスをともに使用することによって、認証の全体的な確信レベルは増加する傾向となる。

【０２００】

いったん認証エンジンが、認証データにおいて提供される認証インスタンスの全てについてステップ１６１０乃至１６２０を行うと、各インスタンスの信頼性は、全体的な認証確信レベルを評価するために、ステップ１６３５で使用される。個別認証インスタンス信頼性を認証確信レベルに組み込むという、このプロセスは、生成される個別信頼性を関係付ける種々の方法によってモデル化されてもよく、また、これらの認証技法のうちのいくつかの間の特定の相互作用をアドレス指定してもよい。（例えば、パスワード等の複数の知識ベースのシステムは、単一のパスワードおよび基本音声分析等のかなり脆弱な生体測定よりも低い確信を生じる場合がある）。

【０２０１】

認証エンジン２１５が、最終確信レベルを生成するように複数の同時認証インスタンスの信頼性を組み合わせる、１つの手段は、合計不信頼性に到達するように、各インスタンスの不信頼性を乗じることである。不信頼性は、概して、信頼性の相補的パーセンテージである。例えば、８４％信頼性がある技法は、１６％信頼性がない。８６％、７５％、および７２％の信頼性を生じる、上記で説明される３つの認証インスタンス（指紋、スマートカード、パスワード）は、それぞれ、（１００－８６）％、（１００－７５）％、および（１００－７２）％、または１４％、２５％、および２８％の対応する不信頼性を有する。これらの不信頼性を乗じることによって、９９．０２％の信頼性に対応する、１４％＊２５％＊２８％－０．９８％の不信頼性という累積的不信頼性を得る。

【０２０２】

付加的な動作モードでは、種々の認証技法の相互依存に対処するように、付加的な要因およびヒューリスティクス５３０が認証エンジン２１５内で適用されてもよい。例えば、誰かが特定のホームコンピュータへの不正アクセスを有する場合、おそらく、そのアドレスにおける電話回線にもアクセスできる。したがって、発信電話番号ならびに認証システムのシリアル番号に基づいて認証することは、認証への全体的確信に多くを加算しない。しかしながら、知識ベースの認証は、大部分がトークンベースン認証とは無関係である（すなわち、誰かが携帯電話または鍵を盗んだ場合、盗まなかった場合よりもＰＩＮまたはパスワードを知る可能性が高いにすぎない）。

【０２０３】

さらに、異なるベンダまたは他の認証リクエスタが、認証の異なる側面に異なって加重することを希望してもよい。これは、個別インスタンスの信頼性を計算する際の別個の加重因子またはアルゴリズムの使用、ならびに複数のインスタンスで認証イベントを評価する異なる手段の使用を含んでもよい。

【０２０４】

例えば、ある種類のトランザクション、例えば、企業Ｅメールシステムのベンダが、デフォルトで主にヒューリスティクスおよび他の状況データに基づいて、認証することを所望してもよい。したがって、それらは、メタデータに関連する因子、および認証イベント

をめぐる状況と関連付けられる他のプロファイル関連情報に高い加重を適用してもよい。この配設は、営業時間中に正しいマシンにログオンしたこと以上をユーザから要求しないことによって、通常営業時間中にユーザへの負担を緩和するために使用することができる。しかしながら、別のベンダは、そのような技法が特定のベンダの目的で認証に最も適しているという方針決定により、特定の技法、例えば、指紋照合に由来する認証に最も重く加重してもよい。

【０２０５】

そのような様々な加重は、１つの動作モードで、認証リクエスタによって、または認証要求を生成する際に定義され、認証要求とともに信頼エンジン１１０に送信されてもよい。そのようなオプションはまた、別の動作モードで、認証リクエスタに対する初期の登録プロセス中に選好として設定し、認証エンジン内に記憶することもできる。

【０２０６】

いったん認証エンジン２１５が、提供される認証データの認証確信レベルを生成すると、この確信レベルは、ステップ１６４０で認証要求を完了するために使用され、この情報は、認証リクエスタへのメッセージを含むために、認証エンジン２１５からトランザクションエンジン２０５に転送される。

【０２０７】

上記で説明されるプロセスは例示的にすぎず、当業者であれば、ステップは示された順番で行われる必要はないこと、またはステップのうちの特定のものだけが行われることを所望されること、またはステップの種々の組み合わせが所望されてもよいことを認識するであろう。さらに、提供される各認証インスタンスの信頼性の評価等の、あるステップは、状況が許可すれば、相互に並行して実行されてもよい。

【０２０８】

本発明のさらなる側面では、上記で説明されるプロセスによって生成される認証確信レベルが、認証を必要とするベンダまたは他の当事者の必要信頼レベルを満たすことができない時の状況に適応する方法が提供される。提供される確信のレベルと所望される信頼のレベルとの間に格差が存在する、これらの状況等の状況では、信頼エンジン１１０の操作者は、この信頼格差を閉鎖するために、一方または両方の当事者が代替データまたは要件を提供するための機会を提供する立場にある。このプロセスは、本明細書では「信頼裁定」と呼ばれる。

【０２０９】

信頼裁定は、図１０および１１を参照して上記で説明されるような暗号認証のフレームワーク内で行われてもよい。その中で示されるように、ベンダまたは他の当事者が、特定のトランザクションと関連して特定のユーザの認証を要求する。１つの状況では、ベンダが、単純に、肯定的または否定的のいずれか一方の認証を要求し、ユーザから適切なデータを受信した後、信頼エンジン１１０が、そのような二値認証を提供する。これらの状況等の状況では、肯定的な認証を確保するために必要とされる確信の程度は、信頼エンジン１１０内で設定される選好に基づいて決定される。

【０２１０】

しかしながら、ベンダが、特定のトランザクションを完了するための特定の信頼のレベルを要求してもよいことも可能である。この必要レベルは、認証要求とともに含まれてもよく（例えば、このユーザを９８％確信で認証する）、またはトランザクションと関連付けられる他の因子に基づいて信頼エンジン１１０によって決定されてもよい（すなわち、このトランザクションについて適宜にこのユーザを認証する）。１つのそのような因子は、トランザクションの経済的価値となる場合がある。より大きい経済的価値を有するトランザクションについては、より高い程度の信頼が必要とされてもよい。同様に、高い程度のリスクを伴うトランザクションについては、高い程度の信頼が必要とされてもよい。逆に、低いリスクまたは低い値のいずれか一方であるトランザクションについては、より低い信頼レベルがベンダまたは他の認証リクエスタによって必要とされてもよい。

【０２１１】

信頼裁定のプロセスは、図１０のステップ１０５０で認証データを受信する信頼エンジン１１０のステップと、図１０のステップ１０５５でベンダに認証結果を返信するステップとの間で発生する。これらのステップ間で、信頼レベルの評価および潜在的な信頼裁定につながるプロセスが、図１７に示されるように発生する。単純な二値認証が行われる状況では、図１７に示されたプロセスは、トランザクションエンジン２０５に、提供された認証データを、図１０を参照して上記で論議されるような識別されたユーザの登録データと直接比較させ、否定的な認証として差異をフラグすることに帰着する。

【０２１２】

図１７に示されるように、ステップ１０５０でデータを受信した後の第１のステップは、トランザクションエンジン２０５が、ステップ１７１０で、この特定のトランザクションの肯定的な認証に必要とされる信頼レベルを決定することである。このステップは、いくつかの異なる方法のうちの１つによって実装されてもよい。必要信頼レベルは、認証要求が行われるときに認証リクエスタによって信頼エンジン１１０に特定されてもよい。認証リクエスタはまた、保管場所２１０またはトランザクションエンジン２０５によってアクセス可能である他の記憶装置内に記憶される選好を事前に設定してもよい。次いで、この選好は、認証要求がこの認証リクエスタによって行われるたびに読み取られ、使用されてもよい。選好はまた、特定のユーザを認証するために、特定の信頼のレベルが常に必要とされるように、セキュリティ対策としてそのユーザと関連付けられてもよく、ユーザ選好は、保管場所２１０またはトランザクションエンジン２０５によってアクセス可能である他の記憶媒体に記憶される。要求レベルはまた、認証されるトランザクションの値およびリスクレベル等の認証要求において提供される情報に基づいて、トランザクションエンジン２０５または認証エンジン２１５によって導出されてもよい。

【０２１３】

１つの動作モードでは、認証要求を生成するときに使用される方針管理モジュールまたは他のソフトウェアが、トランザクションの認証の必要程度の信頼を特定するために使用される。これは、方針管理モジュール内で特定される方針に基づいて必要レベルの信頼を割り当てるときに従う、一連の規則を提供するために使用されてもよい。１つの有利な動作モードは、ベンダのウェブサーバを用いて開始されるトランザクションの必要レベルの信頼を適切に決定するために、そのようなモジュールがベンダのウェブサーバと合併されることである。このようにして、ユーザからのトランザクション要求は、ベンダの方針に従って必要信頼レベルが割り当てられてもよく、そのような情報は、認証要求とともに信頼エンジン１１０に転送されてもよい。

【０２１４】

この必要信頼レベルは、認証する個人が、実際に個人が自分を識別する人物であることを、ベンダが知りたいという確実性の程度と相関する。例えば、トランザクションが、物品が持ち主を変えているため、ベンダがかなりの程度の確実性を求めているものである場合、ベンダは、８５％の信頼レベルを必要としてもよい。ベンダが、チャットルーム上でメンバー専用コンテンツを閲覧すること、または特権を行使することを可能にするようにユーザを認証しているにすぎない状況については、マイナスのリスクは、ベンダが６０％の信頼レベルしか必要としないほど十分小さくてもよい。しかしながら、何万ドルもの価値を伴う生産契約を締結するために、ベンダは、９９％以上の信頼レベルを必要としてもよい。

【０２１５】

この要求信頼レベルは、トランザクションを完了するためにユーザが自分を認証しなければならない測定基準を表す。例えば、要求信頼レベルが８５％である場合、ユーザは、ユーザが自分であると言う者であることを信頼エンジン１１０が８５％の確信で言うために十分な認証を、信頼エンジン１１０に提供しなければならない。（ベンダの満足度にとって）肯定的な認証または信頼裁定の可能性を生じるのは、この必要レベルと認証確信レベルとの間のバランスである。

【０２１６】

図１７に示されるように、トランザクションエンジン２０５は、必要信頼レベルを受信した後、ステップ１７２０で、必要信頼レベルを、（図１６を参照して論議されるように）現在の認証について認証エンジン２１５が計算した認証確信レベルと比較する。認証確信レベルが、ステップ１７３０で、トランザクションの必要信頼レベルよりも高い場合には、プロセスは、このトランザクションの肯定的な認証がトランザクションエンジン２０５によって生成される、ステップ１７４０へと進む。次いで、この効果へのメッセージは、認証結果に挿入され、ステップ１０５５（図１０参照）で示されるようにトランザクションエンジン２０５によってベンダに返信される。

【０２１７】

しかしながら、認証確信レベルがステップ１７３０で必要信頼レベルを満たさない場合には、確信の格差が現在の認証に存在し、信頼裁定がステップ１７５０で行われる。信頼裁定は、以下の図１８を参照してより完全に説明される。以下で説明されるような、このプロセスは、信頼エンジン１１０のトランザクションエンジン２０５内で行われる。（トランザクションエンジン２０５と他の構成要素との間のＳＳＬ通信に必要とされるもの以外に）信頼裁定を実行するために、いずれの認証または他の暗号動作も必要とされないため、プロセスは、認証エンジン２１５の外側で行われてもよい。しかしながら、以下で論議されるように、認証データの任意の再評価、あるいいは他の暗号または認証イベントは、適切なデータを認証エンジン２１５に再提出するように、トランザクションエンジン２０５に要求する。当業者であれば、信頼裁定プロセスは、代替として、認証エンジン２１５自体内で部分的または完全に行われるように構造化できることを認識するであろう。

【０２１８】

上述のように、信頼裁定は、信頼エンジン１１０が、適切な場合に肯定的な認証を確保しようとして、ベンダとユーザとの間の交渉を仲介するプロセスである。ステップ１８０５で示されるように、トランザクションエンジン２０５は、最初に、現在の状況が信頼裁定に適切であるか否かを決定する。これは、以下でさらに論議されるように、認証の状況、例えば、この認証がすでに裁定の複数のサイクルを通っているかどうか、ならびに、ベンダまたはユーザの選好に基づいて、決定されてもよい。

【０２１９】

裁定が可能ではない、そのような状況では、プロセスは、トランザクションエンジン２０５が否定的な認証を生成し、次いで、ステップ１０５５（図１０参照）でベンダに送信される認証結果にそれを挿入する、ステップ１８１０へと進む。認証が無期限に未決となることを防ぐために有利に使用されてもよい、１つの制限は、初期認証要求からタイムアウト期間を設定することである。このようにして、制限時間内に肯定的に認証されないトランザクションは、さらなる裁定を否定され、否定的に認証される。当業者であれば、制限時間は、トランザクションの状況、ならびにユーザおよびベンダの所望に応じて変化してもよいことを認識するであろう。制限はまた、成功した認証を提供する際に行われる試行の数に課されてもよい。そのような認証は、図５に示されるような試行リミッタ５３５によって処理されてもよい。

【０２２０】

裁定がステップ１８０５で禁止されない場合には、トランザクションエンジン２０５は、取引当事者の一方または両方との交渉に従事する。トランザクションエンジン２０５は、ステップ１８２０で示されるように生成される認証確信レベルを高めるために、何らかの形態の付加的な認証を要求するメッセージをユーザに送信してもよい。最も単純な形態では、これは、単純に、認証が不十分であったことを示してもよい。認証の全体的な確信レベルを向上させるように、１つ以上の付加的な認証インスタンスを生成する要求も送信されてもよい。

【０２２１】

ユーザがステップ１８２５でいくつかの付加的な認証インスタンスを提供する場合には、トランザクションエンジン２０５が、トランザクションのためにこれらの認証インスタンスを認証データに追加し、ステップ１０１５でそれを認証エンジン２１５に転送し（図

１０参照）、認証は、このトランザクションのための既存の認証インスタンスおよび新しく提供された認証インスタンスの両方に基づいて再評価される。

【０２２２】

付加的な種類の認証は、例えば、電話によって、信頼エンジン１１０の操作者（または信頼できる提携者）とユーザとの間で何らかの形態の個人対個人の連絡を行う信頼エンジン１１０からの要求であってもよい。この電話または他の非コンピュータ認証は、個人との個人的連絡を提供するために、また、何らかの形態の質問表ベースの認証を行うために使用することができる。これはまた、ユーザが電話をしたときに、発信電話番号、および潜在的にユーザの音声分析を検証する機会を与えてもよい。たとえ付加的な認証データを提供することができなくても、ユーザの電話番号と関連付けられる付加的なコンテキストが、認証コンテキストの信頼性を向上させてもよい。この電話に基づく改訂されたデータまたは状況は、認証要求の考慮で使用するために信頼エンジン１１０に供給される。

【０２２３】

加えて、ステップ１８２０では、信頼エンジン１１０は、ユーザが保険を購入し、より確信した認証を効果的に購入するための機会を提供してもよい。信頼エンジン１１０の操作者は時々、まず認証の確信レベルがある閾値を上回る場合に、そのようなオプションを利用可能にしたいのみであってもよい。事実上、このユーザ側保険は、認証が認証のための信頼エンジン１１０の通常の要求信頼レベルを満たすが、このトランザクションのためのベンダの必要信頼レベルを満たさないときに、信頼エンジン１１０がユーザを保証するための方法である。このようにして、ユーザは、たとえ信頼エンジン１１０にとって十分な確信を生じる認証インスタンスのみを有しても、ベンダによって要求される場合があるような非常に高いレベルに依然として首尾よく認証してもよい。

【０２２４】

この信頼エンジン１１０の機能は、信頼エンジン１１０が、ベンダではなく信頼エンジン１１０が満足するように認証される誰かを保証することを可能にする。これは、署名が文書上に現れる個人が実際にそれを署名した個人であることを、後で文書を読む誰かに示すために、署名を文書に追加する際に公証人によって果たされる機能と同様である。公証人の署名は、ユーザによる署名の行為を証明する。同じように、信頼エンジンは、取引している個人が自分であると言う個人であるという指示を提供している。

【０２２５】

しかしながら、信頼エンジン１１０がユーザによって提供される確信のレベルを人為的に高めるため、ユーザがベンダの必要信頼レベルを実際には満たしていないので、信頼エンジン１１０の操作者にとってより大きなリスクがある。保険の費用は、（ユーザの認証を効果的に公証していてもよい）信頼エンジン１１０への誤決定認証のリスクを相殺するように設計されている。ユーザは、実際に提供されているよりも高いレベルの確信に認証するリスクを冒すように、信頼エンジン１１０の操作者に支払いをする。

【０２２６】

そのような保険システムは、誰かが信頼エンジン１１０からより高い確信評定を効果的に購入することを可能にするため、者およびユーザの両方が、あるトランザクションでユーザ側保険の使用を防止することを希望してもよい。ベンダは、実際の認証データが必要とする確信の程度をサポートすることを知っている状況に、肯定的な認証を限定してもよく、よって、ユーザ側保険が許可されていないことを信頼エンジン１１０に示してもよい。同様に、オンライン身元を保護するために、ユーザは、自分のアカウント上でユーザ側保険の使用を防止することを希望してもよく、または保険のない認証確信レベルがある制限よりも高い状況に、その使用を限定することを希望してもよい。これは、誰かがパスワードを耳にするか、またはスマートカードを盗んで、低レベルの確信に不当に認証するためにそれらを使用し、次いで、非常に高いレベルの（誤った）確信を生じるように保険を購入することを防止するためのセキュリティ対策として使用されてもよい。これらの因子は、ユーザ側保険が許可されているかどうかを決定する際に評価されてもよい。

【０２２７】

ユーザがステップ１８４０で保険を購入する場合には、ステップ１８４５で購入された保険に基づいて認証確信レベルが調整され、認証確信レベルおよび要求信頼レベルがステップ１７３０（図１７参照）で再び比較される。プロセスはここから続き、ステップ１７４０（図１７参照）での肯定的な認証につながるか、または（許可されている場合）さらなる裁定のためにステップ１７５０での信頼裁定プロセスに戻るか、あるいはさらなる裁定が禁止されている場合にステップ１８１０での否定的な認証につながってもよい。

【０２２８】

ステップ１８２０でメッセージをユーザに送信することに加えて、トランザクションエンジン２０５はまた、保留中の認証が現在、必要信頼レベルを下回っていることを示すメッセージを、ステップ１８３０でベンダに送信してもよい。メッセージはまた、どのようにしてベンダへと進むかについて種々のオプションを提供してもよい。これらのオプションのうちの１つは、単純に、現在の認証確信レベルがどのようなものであるかをベンダに知らせ、ベンダが現在の満たされていない必要信頼レベルを維持することを希望するかどうかを尋ねることである。これは、場合によっては、ベンダがトランザクションを認証するための独立した手段を有してもよいか、または、手元の特定のトランザクションに実際に必要とされているよりも高い最初に特定されている必要レベルを概してもたらす、デフォルトのセットの要件を使用していてもよいので、有益であってもよい。

【０２２９】

例えば、ベンダとの全ての着信購入注文トランザクションが９８％信頼レベルを満たすと見込まれることが、標準的実践であってもよい。しかしながら、注文がベンダと長年の顧客との間の電話によって最近論議され、その直後にトランザクションが認証されたが、９３％確信レベルのみで認証された場合、電話が付加的な認証をベンダに効果的に提供するため、ベンダは単純に、このトランザクションのための容認閾値を低くすることを希望してもよい。ある状況では、ベンダは、現在の認証確信のレベルまででではないが、必要信頼レベルを進んで低くしてもよい。例えば、上記の実施例でのベンダは、注文前の電話が、必要とされる信頼の程度の４％低減に値する場合があることを考慮する場合があるが、これは依然として、ユーザによって生成される９３％確信よりも大きい。

【０２３０】

ベンダがステップ１８３５で必要信頼レベルを調整しない場合には、認証によって生成される認証確信レベルおよび必要信頼レベルがステップ１７３０（図１７参照）で比較される。ここで確信レベルが必要信頼レベルを超える場合、肯定的な認証がステップ１７４０（図１７参照）でトランザクションエンジン２０５において生成されてもよい。もしそうでなければ、さらなる裁定が、許可される場合に上記で論議されるように試行されてもよい。

【０２３１】

必要信頼レベルへの調整を要求することに加えて、トランザクションエンジン２０５はまた、認証を要求するベンダにベンダ側保険を提供してもよい。この保険は、ユーザ側保険について上記で説明されるものと同様の目的を果たす。しかしながら、ここでは、費用が、生成される実際の認証確信レベルを上記で認証する際に信頼エンジン１１０によって冒されているリスクに対応するよりもむしろ、保険の費用は、認証おけるより低い信頼レベルを受け入れる際にベンダによって冒されているリスクに対応する。

【０２３２】

実際の必要信頼レベルを単に低くする代わりに、ベンダは、ユーザの認証におけるより低い信頼のレベルと関連付けられる付加的なリスクから自身を保護するように、保険を購入するというオプションを有する。上記で説明されるように、既存の認証がある閾値をすでに上回っている状況で信頼格差を補うように、そのような保険を購入することのみを考慮することが有利であってもよい。

【０２３３】

そのようなベンダ側保険の可用性は、ベンダに、自身にとって付加的な犠牲を払わずに信頼要件を直接低くし、（必要とされるより低い信頼レベルに基づいて）自分で否定的な

認証のリスクを負うオプション、または認証確信レベルと要件との間の信頼格差のための保険を購入し、信頼エンジン１１０の操作者が提供されたより低い確信レベルのリスクを負うオプションを許可する。保険を購入することによって、否定的な認証のリスクが信頼エンジン１１０の操作者に偏移されるため、ベンダは高い信頼レベル要件を効果的に保つことができる。

【０２３４】

ベンダがステップ１８４０で保険を購入する場合、認証確信レベルおよび必要信頼レベルがステップ１７３０（図１７参照）で比較され、プロセスが上記で説明されるように続く。

【０２３５】

ユーザおよびベンダの両方が、信頼エンジン１１０からのメッセージに応答することも可能であると留意されたい。当業者であれば、そのような状況に対処することができる複数の方法があることを認識するであろう。複数の応答の可能性に対処する１つの有利なモードは、単純に、先着順に応答を取り扱うことである。例えば、ベンダが低くなった必要信頼レベルで応答し、その直後にユーザも認証レベルを上昇させるように保険を購入する場合、認証は最初に、ベンダからの低くなった信頼要件に基づいて再評価される。ここで認証が肯定的である場合、ユーザの保険購入は無視される。別の有利な動作モードでは、ユーザは、（低くなったベンダ信頼要件を伴っても信頼格差が依然として残っていた場合）ベンダの新しい低くなった信頼要件を満たすために必要とされる保険のレベルについて請求されるのみである場合がある。

【０２３６】

認証に設定された制限時間内に、いずれか一方の当事者からの応答がステップ１８５０における信頼裁定プロセス中に受信されない場合、裁定はステップ１８０５で再評価される。これは、裁定プロセスを再び効果的に始める。制限時間が最終であるか、または他の状況がステップ１８０５でさらなる裁定を防止する場合、否定的な認証がステップ１８１０でトランザクションエンジン２０５によって生成され、ステップ１０５５（図１０参照）でベンダに返信される。もしそうでなければ、新しいメッセージがユーザおよびベンダに送信されてもよく、プロセスが所望に応じて繰り返されてもよい。

【０２３７】

例えば、トランザクションの一部ではない文書にデジタル署名する、ある種類のトランザクションについては、必ずしもベンダまたは他の第三者がいなくてもよく、したがって、トランザクションは、主にユーザと信頼エンジン１１０との間であることに留意されたい。これら等の状況では、信頼エンジン１１０は、肯定的な認証を生成するために満たされなければならない、独自の必要信頼レベルを有する。しかしながら、そのような状況では、ユーザが独自の署名の確信を引き上げるために信頼エンジン１１０が保険をユーザに提供することは、しばしば望ましくない。

【０２３８】

上記で説明され、図１６－１８で示されるプロセスは、信頼エンジン１１０を参照して上記で説明されるような種々の通信モードを使用して実行されてもよい。例えば、メッセージは、ウェブベースであり、信頼エンジン１１０と、ユーザまたはベンダシステム上で作動するブラウザにリアルタイムでダウンロードされるアプレットとの間のＳＳＬ接続を使用して送信されてもよい。代替的な動作モードでは、そのような裁定および保険トランザクションを促進する、ある専用アプリケーションがユーザおよびベンダによって使用中であってもよい。別の代替的な動作モードでは、上記で説明される裁定を仲介するために、確実なＥメール動作が使用されてもよく、それにより、認証の繰延評価およびバッチ処理を可能にする。当業者であれば、状況およびベンダの認証要件に対して適宜に、異なる通信モードが使用されてもよいことを認識するであろう。

【０２３９】

図１９に関する以下の説明は、上記で説明されるような本発明の種々の側面を統合する、サンプルトランザクションを説明する。この実施例は、信頼エンジン１１０によって仲

介されるようなユーザとベンダとの間の全体的なプロセスを図示する。上記で詳細に説明されるような種々のステップおよび構成要素は、以下のトランザクションを実行するために使用されてもよいが、図示されたプロセスは、信頼エンジン１１０、ユーザ、およびベンダの間の相互作用に焦点を当てる。

【０２４０】

トランザクションは、ユーザが、オンラインでウェブページを閲覧しながらステップ１９００でベンダのウェブサイト上の注文書に記入すると始まる。ユーザは、自分のデジタル署名で署名されたこの注文書をベンダに提出することを希望する。これを行うために、ユーザは、ステップ１９０５で、署名の要求を伴う注文書を信頼エンジン１１０に提出する。ユーザはまた、身元を認証するために上記で説明されるように使用される、認証データも提供する。

【０２４１】

ステップ１９１０では、認証データが、上記で論議されるように信頼エンジン１１０によって登録データと比較され、肯定的な認証が生成された場合、ユーザの秘密鍵で署名された注文書のハッシュが、注文書自体とともにベンダに転送される。

【０２４２】

ベンダは、ステップ１９１５で署名された注文書を受信し、次いで、ベンダは、ステップ１９２０で行われる購入に関連する請求書または他の契約書を生成する。この契約書は、ステップ１９２５で署名の要求とともにユーザに返送される。ベンダはまた、ステップ１９３０で、両方の当業者によって署名される契約書のハッシュを含む、この契約トランザクションの認証要求を信頼エンジン１１０に送信する。契約書が両方の当事者によってデジタル署名されることを可能にするために、ベンダはまた、必要であれば契約書上のベンダの署名を後で検証することができるように、それ自体の認証データも含む。

【０２４３】

上記で論議されるように、信頼エンジン１１０は、次いで、ベンダの身元を確認するようにベンダによって提供される認証データを検証し、データがステップ１９３５で肯定的な認証を生じた場合、データがユーザから受信されるステップ１９５５を続ける。ベンダの認証データが所望の程度でベンダの登録データに合致しない場合、さらなる認証を要求するメッセージがベンダに返信される。ここでは必要であれば、ベンダが自身を信頼エンジン１１０に首尾よく認証するために、信頼裁定が行われてもよい。

【０２４４】

ユーザがステップ１９４０で契約書を受信すると、それを再検討し、ステップ１９４５で認証データを生成して容認可能であれば署名し、次いで、ステップ１９５０で契約書のハッシュおよび認証データを信頼エンジン１１０に送信する。信頼エンジン１１０は、ステップ１９５５で認証データを検証し、認証が良好であれば、続けて以下で説明されるように契約書を処理する。図１７および１８を参照して上記で論議されるように、信頼裁定は、認証確信レベルとトランザクションのための必要認証レベルとの間に存在する信頼格差を埋めるように、適宜に行われてもよい。

【０２４５】

信頼エンジン１１０は、ユーザの秘密鍵で契約書のハッシュに署名し、ステップ１９６０で、自らのために完全メッセージに署名する、すなわち、信頼エンジン１１０の秘密鍵５１０で暗号化された（ユーザの署名を含む）完全メッセージのハッシュを含む、この署名されたハッシュをベンダに送信する。このメッセージは、ステップ１９６５でベンダによって受信される。メッセージは、署名された契約書（ユーザの秘密鍵を使用して暗号化された契約書のハッシュ）および信頼エンジン１１０からの受領書（信頼エンジン１１０の秘密鍵を使用して暗号化された、署名された契約書を含むメッセージのハッシュ）を表す。

【０２４６】

信頼エンジン１１０は、同様に、ステップ１９７０でベンダの秘密鍵を用いて契約書のハッシュを作成し、信頼エンジン１１０によって署名されたこれをユーザに転送する。こ

のようにして、ユーザはまた、ステップ１９７５で、ベンダによって署名された契約書のコピー、ならびに署名された契約書を送達するために信頼エンジン１１０によって署名された受領書も受信する。

【０２４７】

前述の内容に加えて、本発明の付加的な側面は、上記で説明される信頼エンジン１１０によって提供される機能にアクセスする手段として、クライアント側アプリケーションに利用可能であってもよい、暗号サービスプロバイダモジュール（ＳＰＭ）を提供する。そのようなサービスを提供する１つの有利な方法は、暗号ＳＰＭが、第三者アプリケーションプログラミングインターフェース（ＡＰＩ）と、ネットワークまたは他の遠隔接続を介してアクセス可能な信頼エンジン１１０との間の通信を仲介することである。図２０を参照してサンプル暗号ＳＰＭを以下で説明する。

【０２４８】

例えば、一般的なシステム上で、いくつかのＡＰＩがプログラマに利用可能である。各ＡＰＩは、システム上で作動するアプリケーション２０００によって行われてもよい、機能呼び出しのセットを提供する。暗号機能、認証機能、および他のセキュリティ機能に好適なプログラミングインターフェースを提供するＡＰＩの実施例は、そのＷｉｎｄｏｗｓ（登録商標）オペレーティングシステムとともにＭｉｃｒｏｓｏｆｔによって提供される暗号ＡＰＩ（ＣＡＰＩ）２０１０、ならびにＩＢＭ、Ｉｎｔｅｌ、およびＯｐｅｎ Ｇｒｏｕｐの他のメンバーによって後援される共通データセキュリティアーキテクチャ（ＣＤＳＡ）を含む。ＣＡＰＩは、以下に続く論議における例示的なセキュリティＡＰＩとして使用される。しかしながら、説明される暗号ＳＰＭは、当技術分野で公知であるようなＣＤＳＡまたは他のセキュリティＡＰＩとともに使用することができる。

【０２４９】

このＡＰＩは、呼出しが暗号機能について行われるときにユーザシステム１０５またはベンダシステム１２０によって使用される。これらの機能の間には、本明細書で説明されるか、または当業者に公知であるように、特定の鍵で文書を暗号化すること、文書に署名すること、デジタル証明書を要求すること、署名された文書上の署名を検証すること、およびそのような他の暗号機能等の種々の暗号動作を行うことと関連付けられる要求が含まれてもよい。

【０２５０】

そのような暗号機能は通常、ＣＡＰＩ２０１０が位置するシステムにローカルで行われる。これは、概して、呼び出される機能が、指紋読取機等のローカルユーザシステム１０５、またはローカルマシン上で実行されるライブラリを使用してプログラムされるソフトウェア機能のいずれか一方のリソースの使用を必要とするためである。これらのローカルリソースへのアクセスは通常、暗号機能が実行されるリソースを提供する、上記で参照されるような１つ以上のサービスプロバイダモジュール（ＳＰＭ）２０１５、２０２０によって提供される。そのようなＳＰＭは、暗号化または復号動作を行うソフトウェアライブラリ２０１５、または生体測定走査デバイス等の特殊ハードウェア２０２５にアクセスすることが可能なドライバおよびアプリケーション２０２０を含んでもよい。ＣＡＰＩ２０１０がシステム１０５のアプリケーション２０００によって使用されてもよい機能を提供するのとほぼ同じように、ＳＰＭ２０１５、２０２０は、システム上の利用可能なサービスと関連付けられるより低いレベル機能およびリソースへのアクセスをＣＡＰＩに提供する。

【０２５１】

本発明によれば、信頼エンジン１１０によって提供される暗号機能にアクセスし、これらの機能を、ＣＡＰＩ２０１０を介してアプリケーション２０００に利用可能にすることが可能である、暗号ＳＰＭ２０３０を提供することが可能である。ＣＡＰＩ２０１０が、ＳＰＭ２０１５、２０２０を介してローカルで利用可能であるリソースにアクセスすることしかできない実施形態と違って、本明細書で説明されるような暗号ＳＰＭ２０３０は、所望される動作を行うために、暗号動作の要求を遠隔に位置するネットワークアクセス可

能な信頼エンジン１１０に提出することが可能となる。

【０２５２】

例えば、アプリケーション２０００が、文書に署名すること等の暗号動作の必要性を有する場合、アプリケーション２０００は、適切なＣＡＰＩ２０１０機能への機能呼出しを行う。ＣＡＰＩ２０１０は次に、この関数を実行し、ＳＰＭ２０１５、２０２０および暗号ＳＰＭ２０３０によってそれに利用可能となるリソースを利用する。デジタル署名機能の場合、暗号ＳＰＭ２０３０は、通信リンク１２５にわたって信頼エンジン１１０に送信される適切な要求を生成する。

【０２５３】

暗号ＳＰＭ２０３０と信頼エンジン１１０との間で発生する動作は、任意の他のシステムと信頼エンジン１１０との間で可能となる同じ動作である。しかしながら、これらの機能は、ユーザシステム１０５自体の上でローカルにて利用可能と思われるように、ＣＡＰＩ２０１０を介してユーザシステム１０５に効果的に利用可能となる。しかしながら、通常のＳＰＭ２０１５、２０２０と違って、機能は、遠隔信頼エンジン１１０上で実行されており、結果は、通信リンク１２５にわたって適切な要求に応じて暗号ＳＰＭ２０３０に中継される。

【０２５４】

この暗号ＳＰＭ２０３０は、そうでなければ利用可能ではない場合がある、いくつかの動作を、ユーザシステム１０５またはベンダシステム１２０に利用可能にする。これらの機能は、文書の暗号化および復号、デジタル証明書の発行、文書のデジタル署名、デジタル署名の検証、および当業者に明白となるようなそのような他の動作を無限に含む。

【０２５５】

別個の実施形態では、本発明は、任意のデータセットで本発明のデータ確保方法を行うための完全システムを備える。この実施形態のコンピュータシステムは、図８で示され、本明細書で説明される機能性を備える、データ分割モジュールを備える。本発明の一実施形態では、本明細書では確実なデータパーサと呼ばれることもある、データ分割モジュールは、データ分割、暗号化および復号、再構成または再構築機能性を備える、パーサプログラムまたはソフトウェアスイートを備える。この実施形態はさらに、データ記憶設備または複数のデータ記憶設備を備えてもよい。データ分割モジュールまたは確実なデータパーサは、電子インフラストラクチャ内で、またはそのデータの究極のセキュリティを必要とする任意のアプリケーションへのアドオンとして統合する、クロスプラットフォームソフトウェアモジュールスイートを備える。この解析プロセスは、任意の種類のデータセットで、およびありとあらゆるファイル種類で、またはそのデータベース内のデータの任意の横列、縦列、またはセルの上のデータベースの中で、動作する。

【０２５６】

本発明の解析プロセスは、一実施形態では、モジュラー階層状に設計されてもよく、任意の暗号化プロセスが、本発明のプロセスでの使用に好適である。本発明の解析および分割プロセスのモジュラー階層は、１）暗号分割し、分散され、複数の場所で確実に記憶される、２）暗号化し、暗号分割し、分散され、複数の場所で確実に記憶される、３）暗号化し、暗号分割し、各シェアを暗号化し、次いで、分散され、複数の場所で確実に記憶される、および４）暗号化し、暗号分割し、第１のステップで使用されたものとは異なる種類の暗号化を用いて各シェアを暗号化し、次いで、分散され、複数の場所で確実に記憶されることを含んでもよいが、それらに限定されない。

【０２５７】

プロセスは、一実施形態では、生成された乱数のコンテンツまたは鍵に従ったデータの分割と、解析および分割データを２つ以上の部分またはシェアに、一実施形態では好ましくは解析および分割データの４つ以上の部分にデータを分割する暗号化で使用される、鍵の同じ暗号分割を行い、全ての部分を暗号化し、次いで、これらの部分を散乱させてデータベースの中へ再び記憶し、またはプライバシーおよびセキュリティに対するリクエスタの必要性に応じて、固定または可撤性の名前を付けられたデバイスにそれらを移転させる

こととを含む。代替として、別の実施形態では、暗号化は、分割モジュールまたは確実なデータパーサによるデータセットの分割前に発生してもよい。この実施形態で説明されるように処理される元のデータは、暗号化および難読化され、確保される。暗号化された要素の分散は、所望であれば、単一のサーバまたはデータ記憶デバイスを含むが、それらに限定されない、事実上どこにでも、あるいは別個のデータ記憶設備またはデバイスの間にあり得る。暗号化鍵管理は、一実施形態では、ソフトウェアスイート内に含まれてもよく、または別の実施形態では、既存のインフラストラクチャまたは任意の他の所望の場所に組み込まれてもよい。

【０２５８】

暗号の分割（暗号分割）は、データをＮ個のシェアに区分化する。区分化は、個別ビット、ビット、バイト、キロバイト、メガバイト、またはより大きい単位を含む、データの任意のサイズ単位、ならびに、所定であろうと無作為に生成されようと、データ単位サイズの任意のパターンまたは組み合わせにおけるものとなり得る。単位は、無作為または所定の値のセットに基づいて、異なるサイズとなり得る。これは、一連のこれらの単位としてデータを見なすことができることを意味する。このようにして、データ単位自体のサイズは、例えば、データ単位サイズの１つ以上の所定であるか、または無作為に生成されたパターン、順序、または組み合わせを使用することによって、データをより確実にしてもよい。次いで、単位は、（無作為に、または所定の値のセットによって）Ｎ個のシェアに分配される。この分配はまた、シェアにおける単位の順番の入れ替えを伴うこともできる。シェアへのデータ単位の分配は、固定サイズ、所定のサイズ、あるいは所定であるか、または無作為に生成されるデータ単位サイズの１つ以上の組み合わせ、パターン、または順序を含むが、それらに限定されない多種多様な可能な選択に従って行われてもよいことが、当業者に容易に明白となるであろう。

【０２５９】

この暗号分割プロセス、または暗号分割の一実施例は、データをサイズが２３バイトであると見なすことであり、データ単位サイズは１バイトに選択され、シェアの数は４に選択される。各バイトは４つのシェアのうちの１つに分配される。無作為な分配を仮定すると、それぞれ４つのシェアに対応する１と４との間の値を有する一連の２３個の乱数（ｒ１、ｒ２、ｒ３乃至ｒ２３）を作成するように鍵が取得される。データの単位のそれぞれ（この実施例では、データの２３の個別バイト）は、４つのシェアに対応する２３個の乱数のうちの１つと関連付けられる。４つのシェアへのデータのバイトの分配は、データの最初のバイトをシェア番号ｒ１の中へ、第２のバイトをシェアｒ２の中へ、第３のバイトをシェアｒ３の中へ、乃至データの第２３のバイトをシェアｒ２３の中へ配置することによって発生する。データ単位のサイズを含む、多種多様な他の可能ステップ、またはステップの組み合わせ、あるいは一連のステップが、本発明の暗号分割プロセスで使用されてもよく、上記の実施例は、データを暗号分割するための１つのプロセスの非限定的な説明であることが、当業者にとって容易に明白となるであろう。元のデータを再作成するために、逆算が行われる。

【０２６０】

本発明の暗号分割プロセスの別の実施形態では、暗号分割プロセスのオプションは、データをその元の形態または使用可能な形態に再構築または復元するためにシェアのサブセットのみが必要とされるように、シェアにおいて十分な冗長性を提供することである。非限定的な実施例では、暗号分割は、データをその元の形態または使用可能な形態に再構築または復元するために、４つのシェアのうちの３つだけが必要であるように、「４分の３」の暗号分割として行われてもよい。これはまた、「Ｎ分のＭ暗号分割」とも呼ばれ、Ｎはシェアの総数であり、ＭはＮよりも少なくとも１つ少ない。本発明の暗号分割プロセスでは、この冗長性を作成するための多くの可能性があることが、当業者に容易に明白である。

【０２６１】

本発明の暗号分割プロセスの一実施形態では、データの各単位は、主要シェアおよびバ

ックアップシェアといった２つのシェアに記憶される。上記で説明される「４分の３」暗号分割プロセスを使用すると、いずれか１つのシェアが欠落し得て、これは、合計４つのシェアのうちの３つだけが必要とされるため、欠落データ単位がない元のデータを再構築または復元するのに十分である。本明細書で説明されるように、シェアのうちの１つに対応する乱数が生成される。乱数は、データ単位と関連付けられ、鍵に基づいて対応するシェアに記憶される。この実施形態では、主要およびバックアップシェア乱数を生成するために、１つの鍵が使用される。本発明の暗号分割プロセスについて本明細書で説明されるように、データ単位の数に等しい、０から３の乱数のセット（主要シェア数とも呼ばれる）が生成される。次いで、データ単位の数に等しい、１から３の別の乱数のセット（バックアップシェア数とも呼ばれる）が生成される。次いで、データの各単位は、主要シェア数およびバックアップシェア数と関連付けられる。代替として、データ単位の数よりも少なく、乱数セットを繰り返す、乱数のセットが生成されてもよいが、これは機密データのセキュリティを低減する場合がある。主要シェア数は、どのシェアの中にデータ単位が記憶されるかを決定するために使用される。バックアップシェア数は、０から３の間の第３のシェア数を作成するように、主要シェア数と組み合わされ、この数は、どのシェアの中にデータ単位が記憶されるかを決定するために使用される。この実施例では、第３のシェア数を決定する式は、

（主要シェア数＋バックアップシェア数）ＭＯＤ　４＝第３のシェア数ある。

【０２６２】

主要シェア数が０から３の間であり、バックアップシェア数が１から３の間である、上記で説明される実施形態では、第３のシェア数が主要シェア数とは異なることを確実にする。これは、データ単位を２つの異なるシェアに記憶させる。本明細書で開示される実施形態に加えて、冗長な暗号分割および非冗長な暗号分割を行う多くの方法があることが、当業者にとって容易に明白である。例えば、各シェア内のデータ単位は、異なるアルゴリズムを使用して入れ替えることができる。このデータ単位入れ替えは、例えば、元のデータがデータ単位に分割される際に、またはデータ単位がシェアの中へ配置された後に、またはシェアが満杯になった後に行われてもよい。

【０２６３】

本明細書で説明される種々の暗号分割プロセスおよびデータ入れ替えプロセス、ならびに本発明の暗号分割およびデータ入れ替え方法の全ての他の実施形態は、個別ビット、ビット、バイト、キロバイト、メガバイト、またはそれ以上ほどの小さいサイズを含むが、それらに限定されない、任意のサイズのデータ単位で行われてもよい。

【０２６４】

本明細書で説明される暗号分割プロセスを行うソースコードの一実施形態の実施例は、以下である。

```
ＤＡＴＡ［１：２４］－分割されるデータを伴うバイトのアレイ
ＳＨＡＲＥＳ［０：３；１：２４］－各横列がシェアのうちの１つを表す、２次元アレイ
ＲＡＮＤＯＭ［１：２４］-０から３の範囲のアレイ乱数
Ｓ１＝１；
Ｓ２＝１；
Ｓ３＝１；
Ｓ４＝１；
Ｆｏｒ　Ｊ　＝　１　ｔｏ　２４　ｄｏ
    Ｂｅｇｉｎ
    ＩＦ　ＲＡＮＤＯＭ［Ｊ［　＝＝０　ｔｈｅｎ
          Ｂｅｇｉｎ
          ＳＨＡＲＥＳ［１，Ｓ１］　＝　ＤＡＴＡ　［Ｊ］；
          Ｓ１　＝　Ｓ１　＋　１；
          Ｅｎｄ
    ＥＬＳＥ　ＩＦ　ＲＡＮＤＯＭ［Ｊ［　＝＝１　ｔｈｅｎ
```

```
        Ｂｅｇｉｎ
        ＳＨＡＲＥＳ［２，Ｓ２］　＝　ＤＡＴＡ　［Ｊ］；
        Ｓ２　＝　Ｓ２　＋　１；
        ＥＮＤ
ＥＬＳＥ　ＩＦ　ＲＡＮＤＯＭ［Ｊ［　＝＝２　ｔｈｅｎ
        Ｂｅｇｉｎ
        Ｓｈａｒｅｓ［３，Ｓ３］　＝　ｄａｔａ［Ｊ］；
        Ｓ３　＝　Ｓ３　＋　１；
        Ｅｎｄ
Ｅｌｓｅ　ｂｅｇｉｎ
        Ｓｈａｒｅｓ［４，Ｓ４］　＝　ｄａｔａ［Ｊ］；
        Ｓ４　＝　Ｓ４　＋　１；
        Ｅｎｄ；
ＥＮＤ；
```

本明細書で説明される暗号分割ＲＡＩＤプロセスを行うソースコードの一実施形態の実施例は、以下である。

【０２６５】

２つのセットの数を生成し、ＰｒｉｍａｒｙＳｈａｒｅは０から３であり、ＢａｃｋｕｐＳｈａｒｅは１から３である。次いで、上記で説明される暗号分割と同じプロセスを用いて、各データ単位をｓｈａｒｅ［ｐｒｉｍａｒｙｓｈａｒｅ［１］］およびｓｈａｒｅ［（ｐｒｉｍａｒｙｓｈａｒｅ［１］＋ｂａｃｋｕｐｓｈａｒｅ［１］）ｍｏｄ　４に入れる。この方法は、任意のサイズＮに拡大縮小可能となり、データを修復するためにＮ－１個だけのシェアが必要である。

【０２６６】

暗号化されたデータ要素の回収、再結合、再構築、または再構成は、指紋認識、顔面スキャン、手スキャン、虹彩スキャン、網膜スキャン、耳スキャン、血管パターン認識、またはＤＮＡ分析等の生体測定を含むが、それらに限定されない、人の数の認証技法を利用してもよい。本発明のデータ分割および／またはパーサモジュールは、所望に応じて多種多様のインフラストラクチャ製品またはアプリケーションに組み込まれてもよい。

【０２６７】

当技術分野で公知である従来の暗号化技術は、データを暗号化し、鍵がなければそれを使用不可能にするために使用される、１つ以上の鍵に依存する。しかしながら、データは、完全かつ損なわれないままであり、攻撃の影響を受けやすいままである。本発明の確実なデータパーサは、一実施形態では、暗号解析と、暗号化されたファイルの２つ以上の部分またはシェア、別の実施形態では好ましくは４つ以上のシェアへの分割とを行い、暗号化の別の層をデータの各シェアに追加し、次いで、異なる物理的および／または論理的な場所にシェアを記憶することによって、この問題に対処する。データ記憶デバイス等の可撤性デバイスを使用することによって、または別の当事者の制御の下にシェアを置くことによって、１つ以上のデータシェアがシステムから物理的に除去されると、確保されたデータのセキュリティ侵害の可能性が効果的に除去される。

【０２６８】

本発明の確実なデータパーサの一実施形態の実施例、およびどのようにそれが利用されてもよいかという実施例が、図２１に示され、以下で説明される。しかしながら、本発明の確実なデータパーサは、以下の非限定的実施例に加えて、多種多様な方法で利用されてもよいことが、当業者に容易に明白である。配備オプションとして、一実施形態では、確実なデータパーサは、外部セッション鍵管理またはセッション鍵の確実な内部記憶を伴って実装されてもよい。実装時に、アプリケーションを確保するため、および暗号化目的で使用されるパーサマスター鍵が生成される。結果として生じる確保されたデータの中のパーサマスター鍵の組み込みは、ワークグループ、企業、または拡張聴衆内の個人による確保されたデータの共有の融通性を可能にすることも留意されたい。

【０２６９】
図２１に示されるように、本発明のこの実施形態は、解析されたデータとともにセッションマスター鍵を記憶するように、データパーサによってデータに行われるプロセスのステップを示す。
１．セッションマスター鍵を生成し、ＲＳ１ストリーム暗号を使用してデータを暗号化する。
２．セッションマスター鍵のパターンに従って、結果として生じる暗号化されたデータを、解析されたデータの４つのシェアまたは部分に分離する。
３．方法のこの実施形態では、セッションマスター鍵は、確保されたデータシェアとともにデータ保管場所に記憶される。パーサマスター鍵のパターンに従ってセッションマスター鍵を分離し、鍵データを暗号化された解析データに付加する。
４．データの結果として生じる４つのシェアは、元のデータの暗号化された部分およびセッションマスター鍵の複数部分を含有する。４つのデータシェアのそれぞれにストリーム暗号鍵を生成する。
５．各シェアを暗号化し、次いで、暗号化されたデータ部分またはシェアとは異なる場所に暗号化鍵を記憶する。シェア１は鍵４を得て、シェア２は鍵１を得て、シェア３は鍵２を得て、シェア４は鍵３を得る。
元のデータ形式を修復するためには、ステップが逆転される。
【０２７０】
本明細書で説明される方法のあるステップは、所望に応じて、異なる順番で行われるか、または複数回繰り返されてもよいことが、当業者に容易に明白である。データの複数部分は相互に異なって処理されてもよいことも、当業者に容易に明白である。例えば、複数の解析するステップは、解析されたデータの一部分のみで行われてもよい。解析されたデータの各部分は、データがその元の形態または他の使用可能な形態に再構築、再構成、再形成、復号、または復元されてもよいという条件のみで、任意の望ましい方法で一意的に確保されてもよい。
【０２７１】
図２２に示され、本明細書で説明されるように、本発明の別の実施形態は、１つ以上の別個の鍵管理テーブルにセッションマスター鍵データを記憶するように、確実なデータパーサによってデータに行われる、プロセスのステップを含む。
１．セッションマスター鍵を生成し、ＲＳ１ストリーム暗号を使用してデータを暗号化する。
２．セッションマスター鍵のパターンに従って、結果として生じる暗号化されたデータを、解析されたデータの４つのシェアまたは部分に分離する。
３．本発明の方法のこの実施形態では、セッションマスター鍵は、データ保管場所で別個の鍵管理テーブルに記憶される。このトランザクションに一意のトランザクションＩＤを生成する。トランザクションＩＤおよびセッションマスター鍵を別個の鍵管理テーブルに記憶する。パーサマスター鍵のパターンに従ってトランザクションＩＤを分離し、データを暗号化された解析または分離データに付加する。
４．データの結果として生じる４つのシェアは、元のデータの暗号化された部分およびトランザクションＩＤの複数部分を含有する。
５．４つのデータシェアのそれぞれにストリーム暗号鍵を生成する。
６．各シェアを暗号化し、次いで、暗号化されたデータ部分またはシェアとは異なる場所に暗号化鍵を記憶する。シェア１は鍵４を得て、シェア２は鍵１を得て、シェア３は鍵２を得て、シェア４は鍵３を得る。
元のデータ形式を修復するためには、ステップが逆転される。
【０２７２】
本明細書で説明される方法のあるステップは、所望に応じて、異なる順番で行われるか、または複数回繰り返されてもよいことが、当業者に容易に明白である。データの複数部分は相互に異なって処理されてもよいことも、当業者に容易に明白である。例えば、複数

の分離または解析するステップは、解析されたデータの一部分のみで行われてもよい。解析されたデータの各部分は、データがその元の形態または他の使用可能な形態に再構築、再構成、再形成、復号、または復元されてもよいという条件のみで、任意の望ましい方法で一意的に確保されてもよい。

【０２７３】

図２３に示されるように、本発明のこの実施形態は、解析されたデータとともにセッションマスター鍵を記憶するように、確実なデータパーサによってデータに行われる、プロセスのステップを示す。

１．認証されたユーザと関連付けられるパーサマスター鍵にアクセスする。

２．一意のセッションマスター鍵を生成する。

３．パーサマスター鍵およびセッションマスター鍵の排他的ＯＲ関数から中間鍵を導出する。

４．中間鍵を用いて入力される既存または新しい暗号化鍵アルゴリズムを使用した、データの随意的な暗号化。

５．中間鍵のパターンに従って、結果として生じる任意に暗号化されたデータを、解析されたデータの４つのシェアまたは部分に分離する。

６．方法のこの実施形態では、セッションマスター鍵は、確保されたデータシェアとともにデータ保管場所に記憶される。パーサマスター鍵のパターンに従ってセッションマスター鍵を分離し、鍵データを任意に暗号化された解析データシェアに付加する。

７．データの結果として生じる複数のシェアは、元のデータの任意に暗号化された部分およびセッションマスター鍵の複数部分を含有する。

８．任意に、４つのデータシェアのそれぞれに暗号化鍵を生成する。

９．任意に、既存または新しい暗号化アルゴリズムを用いて各シェアを暗号化し、次いで、暗号化されたデータ部分またはシェアとは異なる場所に暗号化鍵を記憶する。例えば、シェア１は鍵４を得て、シェア２は鍵１を得て、シェア３は鍵２を得て、シェア４は鍵３を得る。

【０２７４】

元のデータ形式を修復するためには、ステップが逆転される。

【０２７５】

本明細書で説明される方法のあるステップは、所望に応じて、異なる順番で行われるか、または複数回繰り返されてもよいことが、当業者に容易に明白である。データの複数部分は相互に異なって処理されてもよいことも、当業者に容易に明白である。例えば、複数の解析するステップは、解析されたデータの一部分のみで行われてもよい。解析されたデータの各部分は、データがその元の形態または他の使用可能な形態に再構築、再構成、再形成、復号、または復元されてもよいという条件のみで、任意の望ましい方法で一意的に確保されてもよい。

【０２７６】

図２４に示され、本明細書で説明されるように、本発明の別の実施形態は、１つ以上の別個の鍵管理テーブルにセッションマスター鍵データを記憶するように、確実なデータパーサによってデータに行われる、プロセスのステップを含む。

１．認証されたユーザと関連付けられるパーサマスター鍵にアクセスする。

２．一意のセッションマスター鍵を生成する。

３．パーサマスター鍵およびセッションマスター鍵の排他的ＯＲ関数から中間鍵を導出する。

４．中間鍵を用いて入力される既存または新しい暗号化鍵アルゴリズムを使用して、任意にデータを暗号化する。

５．中間鍵のパターンに従って、結果として生じる任意に暗号化されたデータを、解析されたデータの４つのシェアまたは部分に分離する。

６．本発明の方法のこの実施形態では、セッションマスター鍵は、データ保管場所で別個の鍵管理テーブルに記憶される。このトランザクションに一意のトランザクションＩＤを

生成する。トランザクションＩＤおよびセッションマスター鍵を別個の鍵管理テーブルに記憶するか、または外部管理のためにセッションマスター鍵およびトランザクションＩＤを呼び出しプログラムに戻す。パーサマスター鍵のパターンに従ってトランザクションＩＤを分離し、データを任意に暗号化された解析または分離データに付加する。
７．データの結果として生じる４つのシェアは、元のデータの任意に暗号化された部分およびトランザクションＩＤの複数部分を含有する。
８．任意に、４つのデータシェアのそれぞれに暗号化鍵を生成する。
【０２７７】
９．任意に、各シェアを暗号化し、次いで、暗号化されたデータ部分またはシェアとは異なる場所に暗号化鍵を記憶する。例えば、シェア１は鍵４を得て、シェア２は鍵１を得て、シェア３は鍵２を得て、シェア４は鍵３を得る。
元のデータ形式を修復するためには、ステップが逆転される。
【０２７８】
本明細書で説明される方法のあるステップは、所望に応じて、異なる順番で行われるか、または複数回繰り返されてもよいことが、当業者に容易に明白である。データの複数部分は相互に異なって処理されてもよいことも、当業者に容易に明白である。例えば、複数の分離または解析するステップは、解析されたデータの一部分のみで行われてもよい。解析されたデータの各部分は、データがその元の形態または他の使用可能な形態に再構築、再構成、再形成、復号、または復元されてもよいという条件のみで、任意の望ましい方法で一意的に確保されてもよい。
【０２７９】
当業者に容易に明白であるように、多種多様な暗号化方法が、本発明の方法で使用するために好適である。ワンタイムパッドアルゴリズムがしばしば、最も確実な暗号化方法のうちの１つと見なされ、本発明の方法で使用するために好適である。ワンタイムパッドアルゴリズムを使用することは、確保されるデータと同じくらいの長さである鍵が生成されることを必要とする。この方法の使用は、確保されるデータセットのサイズにより非常に長い鍵の生成および管理をもたらす状況等の、ある状況では、あまり望ましくなくてもよい。ワンタイムパッド（ＯＴＰ）アルゴリズムでは、排他的ｏｒ関数ＸＯＲが使用される。同じ長さの二値ストリームｘおよびｙについて、ｘ　ＸＯＲ　ｙは、ｘおよびｙのビット排他論理輪を意味する。
【０２８０】
ビットレベルでは、以下が生成される。
０　ＸＯＲ　０＝０
０　ＸＯＲ　１＝１
１　ＸＯＲ　０＝１
１　ＸＯＲ　１＝０
このプロセスの実施例は、分割されるｎバイトの秘密ｓ（またはデータセット）について本明細書で説明される。プロセスは、ｎバイトの乱数値ａを生成し、次いで、
ｂ＝ａ　ＸＯＲ　ｓ
を設定する。
【０２８１】
次式：
ｓ＝ａ　ＸＯＲ　ｂ
を介して「ｓ」を導出できることに留意されたい。
【０２８２】
値ａおよびｂは、シェアまたは部分と呼ばれ、別個の保管場所に配置される。いったん秘密ｓが２つ以上のシェアに分割されると、確実な方式で破棄される。
【０２８３】
本発明の確実なデータパーサは、複数の別個の秘密鍵値Ｋ１、Ｋ２、Ｋ３、Ｋｎ、Ｋ５を組み込む複数のＸＯＲ関数を実行する、この機能を利用してもよい。動作の開始時にお

いて、確保されるデータは、第１の暗号化動作を通過させられ、データ＝データＸＯＲ秘密鍵５を確保し、
Ｓ＝Ｄ　ＸＯＲ　Ｋ５である。
【０２８４】
結果として生じる暗号化されたデータを、例えば、４つのシェアＳ１、Ｓ２、Ｓ３、Ｓｎに確実に記憶するために、データは、Ｋ５の値に従って、解析され、「ｎ」個のセグメントに分割され、または共有される。この動作は、元の暗号化されたデータの「ｎ」個の擬似乱数のシェアをもたらす。次いで、後続のＸＯＲ関数は、残りの秘密鍵値を用いて各シェアで行われてもよく、例えば、確実なデータセグメント１＝暗号化されたデータシェア１ＸＯＲ秘密鍵１であり、
ＳＤ１＝Ｓ１　ＸＯＲ　Ｋ１、
ＳＤ２＝Ｓ２　ＸＯＲ　Ｋ２、
ＳＤ３＝Ｓ３　ＸＯＲ　Ｋ３、
ＳＤｎ＝Ｓｎ　ＸＯＲ　Ｋｎである。
【０２８５】
一実施形態では、いずれか１つの保管場所に、そこで保持された情報を復号するのに十分な情報を含有させることは所望されない場合があり、よって、シェアを復号するために必要とされる鍵は、異なるデータ保管場所に記憶される。
保管場所１：ＳＤ１，Ｋｎ
保管場所２：ＳＤ２，Ｋ１
保管場所３：ＳＤ３，Ｋ２
保管場所ｎ：ＳＤｎ，Ｋ３
加えて、各シェアには、元のセッション暗号化鍵Ｋ５を回収するために必要とされる情報が付加されてもよい。したがって、本明細書で説明される鍵管理の実施例では、元のセッションマスター鍵は、インストール依存パーサマスター鍵（ＴＩＤ１、ＴＩＤ２、ＴＩＤ３、ＴＩＤｎ）のコンテンツに従って、「ｎ」個のシェアに分割されるトランザクションＩＤによって参照される。
保管場所１：ＳＤ１，Ｋｎ，ＴＩＤ１
保管場所２：ＳＤ２，Ｋ１，ＴＩＤ２
保管場所３：ＳＤ３，Ｋ２，ＴＩＤ３
保管場所ｎ：ＳＤｎ，Ｋ３，ＴＩＤｎ
本明細書で説明される、組み込まれたセッション鍵の実施例では、セッションマスター鍵は、インストール依存パーサマスター鍵（ＳＫ１、ＳＫ２、ＳＫ３、ＳＫｎ）のコンテンツに従って、「ｎ」個のシェアに分割される。
保管場所１：ＳＤ１，Ｋｎ，ＳＫ１
保管場所２：ＳＤ２，Ｋ１，ＳＫ２
保管場所３：ＳＤ３，Ｋ２，ＳＫ３
保管場所ｎ：ＳＤｎ，Ｋ３，ＳＫｎ
４つ全てのシェアが回収されない限り、この実施例に従ってデータを再構築することはできない。たとえ４つ全てのシェアが捕捉されても、セッションマスター鍵およびパーサマスター鍵にアクセスせずに、元の情報を再構築または復元するという可能性はない。
【０２８６】
この実施例は、本発明の方法の実施形態を説明しており、また、別の実施形態では、秘密認証材料を形成するように全ての保管場所からのシェアを組み合わせることができるように、保管場所の中へシェアを配置するために使用されるアルゴリズムも説明する。必要とされる計算は非常に単純かつ迅速である。しかしながら、ワンタイムパッド（ＯＴＰ）アルゴリズムを用いると、鍵サイズが記憶されるデータと同じサイズであるため、確保される大量のデータセット等の、それをあまり望ましくないものにさせる状況があってもよい。したがって、ある状況下ではあまり望ましくなくてもよい、元のデータの量の約２倍を記憶し、伝送する必要性が生じる。

【０２８７】
（ストリーム暗号ＲＳ１）
ストリーム暗号ＲＳ１分割技法は、本明細書で説明されるＯＴＰ分割技法と極めて同様である。ｎバイトの乱数値の代わりに、ｎ’＝ｍｉｎ（ｎ，１６）バイトの乱数値が生成され、ＲＳ１ストリーム暗号アルゴリズムに入力するために使用される。ＲＳ１ストリーム暗号アルゴリズムの利点は、擬似乱数の鍵がはるかに小さい種子数から生成されることである。ＲＳ１ストリーム暗号化の実行の速度も、セキュリティを損なわずに、当技術分野で周知のＴｒｉｐｌｅ　ＤＥＳ暗号化の速度の約１０倍で定格される。ＲＳ１ストリーム暗号アルゴリズムは、当技術分野で周知であり、ＸＯＲ関数で使用される鍵を生成するために使用されてもよい。ＲＳ１ストリーム暗号アルゴリズムは、ＲＳＡ　Ｓｅｃｕｒｉｔｙ，ＩｎｃのＲＣ４™ストリーム暗号アルゴリズム等の他の市販のストリーム暗号アルゴリズムとともに相互運用可能であり、本発明の方法で使用するために好適である。
【０２８８】
上記の鍵表記法を使用すると、Ｋ１乃至Ｋ５はｎバイトの乱数値であり、以下のように設定し、
ＳＤ１＝Ｓ１　ＸＯＲ　Ｅ（Ｋ１）
ＳＤ２＝Ｓ２　ＸＯＲ　Ｅ（Ｋ２）
ＳＤ３＝Ｓ３　ＸＯＲ　Ｅ（Ｋ３）
ＳＤｎ＝Ｓｎ　ＸＯＲ　Ｅ（Ｋｎ）
式中、Ｅ（Ｋ１）乃至Ｅ（Ｋｎ）は、Ｋ１乃至Ｋｎによって入力されるＲＳ１ストリーム暗号アルゴリズムからの出力の最初のｎバイトである。ここで、シェアは本明細書で説明されるようにデータ保管場所の中へ配置されている。
【０２８９】
このストリーム暗号ＲＳ１アルゴリズムでは、必要とされる計算は、ＯＴＰアルゴリズムとほぼ同じくらい単純かつ迅速である。ＲＳ１ストリーム暗号を使用する、この実施例での有益性としては、システムが、１つのシェアにつき確保される元のデータのサイズより平均で約１６バイトだけ多く記憶し、伝送する必要がある。元のデータのサイズが１６バイトより大きい場合、このＲＳ１アルゴリズムは、単純により短いため、ＯＴＰアルゴリズムよりも効率的である。ＲＳ１、ＯＴＰ、ＲＣ４™、Ｔｒｉｐｌｅ　ＤＥＳ、およびＡＥＳを含むが、それらに限定されない、多種多様な暗号化方法またはアルゴリズムが、本発明で使用するために好適であることが当業者に容易に明白である。
【０２９０】
従来の暗号化方法に優る、本発明のデータセキュリティ方法およびコンピュータシステムによって提供される主な利点がある。１つの利点は、異なる論理的、物理的、または地理的な場所にあってもよい、１つ以上のデータ保管場所または記憶デバイス上の異なる場所にデータのシェアを移動させることから獲得される、セキュリティである。データのシェアは、物理的に分割されて異なる人員の制御の下にあり、例えば、データを損なうという可能性が多大に低減される。
【０２９１】
本発明の方法およびシステムによって提供される別の利点は、機密データのセキュリティを維持する包括的プロセスを提供するようにデータを確保するための、本発明の方法のステップの組み合わせである。データは、確実な鍵で暗号化され、確実な鍵に従って、１つ以上のシェア、一実施形態では４つのシェアに分割される。確実な鍵は、確実な鍵に従って４つのシェアの中へ確保される、参照ポインタを用いて安全に記憶される。次いで、データシェアは個別に暗号化され、鍵は異なる暗号化されたシェアを用いて安全に記憶される。組み合わされると、本明細書で開示される方法に従ってデータを確保するためのプロセス全体が、データセキュリティのための包括的パッケージになる。
【０２９２】
本発明の方法に従って確保されるデータは、容易に回収可能であり、使用のためにその元の形態または他の好適な形態に復元され、再構成され、再構築され、復号され、または

別様に戻される。元のデータを修復するためには、以下のアイテムが利用されてもよい。
１．データセットの全てのシェアまたは部分。
２．データを確保するために使用される方法のプロセスフローを再現する知識および能力。
３．セッションマスター鍵へのアクセス。
４．パーサマスター鍵へのアクセス。

【０２９３】
したがって、上記の要素のうちの少なくとも１つが、（例えば、異なるシステム管理者の制御下にある）システムの残りの構成要素から物理的に分離されてもよい、確実なインストールを計画することが望ましくてもよい。

【０２９４】
データ確保方法アプリケーションを起動する不正アプリケーションからの保護は、パーサマスター鍵の使用によって実施されてもよい。確実なデータパーサとアプリケーションとの間の相互認証ハンドシェイクが、本発明のこの実施形態では、任意の措置が講じられる前に必要とされてもよい。

【０２９５】
システムのセキュリティは、元のデータの再作成のための「バックドア」方法がないことを決定付ける。データ復旧問題が発生する場合があるインストールについて、確実なデータパーサは、４つのシェアおよびセッションマスター鍵保管場所のミラーを提供するように強化することができる。ＲＡＩＤ（いくつかのディスクにわたって情報を広めるために使用される、安価なディスクの冗長アレイ）等のハードウェアオプションおよび複製等のソフトウェアオプションは、データ復旧計画も支援することができる。

【０２９６】
（鍵管理）
本発明の一実施形態では、データ確保方法は、暗号化動作に３つの鍵のセットを使用する。各鍵のセットは、インストールに基づいて、個別鍵記憶、回収、セキュリティ、および復旧オプションを有してもよい。使用されてもよい鍵は、以下を含むが、それらに限定されない。

【０２９７】
（パーサマスター鍵）
この鍵は、確実なデータパーサのインストールと関連付けられる個別鍵である。これは、確実なデータパーサが配備されているサーバ上にインストールされている。例えば、スマートカード、別個のハードウェア鍵記憶、標準鍵記憶、カスタム鍵記憶、または確保されたデータベーステーブル内を含むが、それらに限定されない、この鍵を確保するために好適な種々のオプションがある。

【０２９８】
（セッションマスター鍵）
セッションマスター鍵は、データが確保される度に生成されてもよい。セッションマスター鍵は、解析および分割動作の前にデータを暗号化するために使用される。それはまた、暗号化されたデータを解析する手段として組み込まれてもよい（セッションマスター鍵が解析されたデータに組み込まれていない場合）。セッションマスター鍵は、例えば、標準鍵記憶、カスタム鍵記憶、別個のデータベーステーブルを含むが、それらに限定されない種々の方式で確保されるか、または暗号化されたシェア内に確保されてもよい。

【０２９９】
（シェア暗号化鍵）
作成されるデータセットの各シェアまたは部分について、シェアをさらに暗号化するように、個別シェア暗号化鍵が生成されてもよい。シェア暗号化鍵は、暗号化されたシェアとは異なるシェアに記憶されてもよい。

【０３００】
本発明のデータ確保方法およびコンピュータシステムは、任意の設定または環境で任意

の種類のデータに広く適用可能であることが、当業者に容易に明白である。インターネット上で、または顧客とベンダとの間で運営される商用アプリケーションに加えて、本発明のデータ確保方法およびコンピュータシステムは、非商用または私的設定または環境に極めて適用可能である。未承認ユーザから保護されることが所望されるデータセットが、本明細書で説明される方法およびシステムを使用して確保されてもよい。例えば、企業または組織内の特定のデータベースへのアクセスは、データを確保するための本発明の方法およびシステムを採用することによって、選択されたユーザのみに有利に制限されてもよい。別の実施例は、文書の生成、修正、またはアクセスであり、アクセスを制限すること、あるいは未承認または偶発的アクセス、もしくは選択された個人、コンピュータ、またはワークステーションのグループ外の公開を防止することが所望される。本発明のデータ確保の方法およびシステムが、任意の非商用または商用環境または設定に適用可能である、方法のこれらの実施例および他の実施例は、任意の組織、政府機関、または企業を含むがそれらに限定されない、任意の設定用である。

【０３０１】

本発明の別の実施形態では、データ確保方法は、暗号化動作に３つの鍵のセットを使用する。各鍵のセットは、インストールに基づいて、個別鍵記憶、回収、セキュリティ、および復旧オプションを有してもよい。使用されてもよい鍵は、以下を含むが、それらに限定されない。

【０３０２】

（１．パーサマスター鍵）

この鍵は、確実なデータパーサのインストールと関連付けられる個別鍵である。これは、確実なデータパーサが配備されているサーバ上にインストールされている。例えば、スマートカード、別個のハードウェア鍵記憶、標準鍵記憶、カスタム鍵記憶、または確保されたデータベーステーブル内を含むが、それらに限定されない、この鍵を確保するために好適な種々のオプションがある。

【０３０３】

（２．セッションマスター鍵）

セッションマスター鍵は、データが確保される度に生成されてもよい。セッションマスター鍵は、中間鍵を導出するためのパーサマスター鍵と併せて使用される。セッションマスター鍵は、例えば、標準鍵記憶、カスタム鍵記憶、別個のデータベーステーブルを含むが、それらに限定されない種々の方式で確保されるか、または暗号化されたシェア内に確保されてもよい。

【０３０４】

（３．中間鍵）

中間鍵は、データが確保される度に生成されてもよい。中間鍵は、解析および分割動作の前にデータを暗号化するために使用される。それはまた、暗号化されたデータを解析する手段として組み込まれてもよい。

【０３０５】

（４．シェア暗号化鍵）

作成されるデータセットの各シェアまたは部分について、シェアをさらに暗号化するように、個別シェア暗号化鍵が生成されてもよい。シェア暗号化鍵は、暗号化されたシェアとは異なるシェアに記憶されてもよい。

【０３０６】

本発明のデータ確保方法およびコンピュータシステムは、任意の設定または環境で任意の種類のデータに広く適用可能であることが、当業者に容易に明白である。インターネット上で、または顧客とベンダとの間で運営される商用アプリケーションに加えて、本発明のデータ確保方法およびコンピュータシステムは、非商用または私的設定または環境に極めて適用可能である。未承認ユーザから保護されることが所望されるデータセットが、本明細書で説明される方法およびシステムを使用して確保されてもよい。例えば、企業または組織内の特定のデータベースへのアクセスは、データを確保するための本発明の方法お

よびシステムを採用することによって、選択されたユーザのみに有利に制限されてもよい。別の実施例は、文書の生成、修正、またはアクセスであり、アクセスを制限すること、あるいは未承認または偶発的アクセス、もしくは選択された個人、コンピュータ、またはワークステーションのグループ外の公開を防止することが所望される。本発明のデータ確保の方法およびシステムが、任意の非商用または商用環境または設定に適用可能である、方法のこれらの実施例および他の実施例は、任意の組織、政府機関、または企業を含むがそれらに限定されない、任意の設定用である。

【０３０７】

（ワークグループ、プロジェクト、個別ＰＣ／ラップトップ、またはクロスプラットフォームデータセキュリティ）

本発明のデータ確保方法およびコンピュータシステムはまた、例えば、企業、オフィス、政府機関、または機密データが作成、処理、または記憶される任意の設定で使用される、ワークグループ、プロジェクト、個別ＰＣ／ラップトップ、および任意の他のプラットフォームによってデータを確保するのに有用である。本発明は、政府機関全体にわたって、あるいは州または連邦レベルでの政府間での実装のために、米国政府等の組織によって追求されていることが知られている、データを確保する方法およびコンピュータシステムを提供する。

【０３０８】

本発明のデータ確保方法およびコンピュータシステムは、フラットファイルだけでなく、任意の種類のデータフィールド、セット、および／またはテーブルも解析および分割する能力を提供する。加えて、テキスト、ビデオ、画像、生体測定、および音声データを含むがそれらに限定されない全ての形態のデータが、このプロセスの下で確保されることが可能である。本発明のデータを確保する方法の拡張性、速度、およびデータスループットは、ユーザが自由に使える状態で有するハードウェアのみに限定される。

【０３０９】

本発明の一実施形態では、データ確保方法は、ワークグループ環境で、以下で説明されるように利用される。一実施形態では、図２３に示され、以下で説明されるように、本発明のワークグループスケールデータ確保方法は、ユーザ／グループ関係、およびユーザのグループが確実なデータを共有するために必要な関連秘密鍵（パーサグループマスター鍵）を記憶するために、信頼エンジンの秘密鍵管理機能性を使用する。本発明の方法は、パーサマスター鍵がどのように配備されたかに応じて、企業、ワークグループ、または個別ユーザのためにデータを確保する能力を有する。

【０３１０】

一実施形態では、付加的な鍵管理およびユーザ／グループ管理プログラムが提供されてもよく、運営および鍵管理の単一の点を伴う大規模ワークグループ実装を可能にする。鍵生成、管理、および撤回は、単一の維持プログラムによって処理され、その全ては、ユーザの数が増加するにつれて特に重要になる。別の実施形態では、鍵管理はまた、いずれか１人の個人またはグループが必要に応じてデータを制御することを可能にしなくてもよい、１つまたはいくつかの異なるシステム管理者にわたって設定されてもよい。これは、確保されたデータの管理が、組織によって定義されるような役割、責務、会員資格、権利等によって得られることを可能にし、確保されたデータへのアクセスは、自分が作業している部分のみにアクセスできるように許可または要求される者のみに限定することができる一方で、マネージャまたは重役等の他者は、確保されたデータの全てにアクセスできてもよい。この実施形態は、承認された所定の役割および責務を伴う者等の、ある選択された個人が、データを全体として観察することのみを同時に可能にしながら、企業または組織内の異なるグループ間での確保されたデータの共有を可能にする。加えて、本発明の方法およびシステムのこの実施形態はまた、例えば、別個の企業、または企業の別個の部門あるいは課、または任意の別個の組織部門、グループ、機関、あるいはオフィス、または任意の政府あるいは組織あるいは任意の種類の同等物の間のデータの共有も可能にし、いくらかの共有が必要とされるが、いずれの当事者も全てのデータへのアクセスを有すること

を許可されなくてもよい。本発明のそのような方法およびシステムに対する必要性および有用性の特に明白な実施例は、例えば、政府地域、機関、およびオフィス間で、ならびに大企業の異なる課、部門、またはオフィス間での共有を可能にするが、セキュリティを維持することである。

【０３１１】

より小規模での本発明の方法の適用性の実施例は、以下の通りである。パーサマスター鍵が、組織への確実なデータパーサのシリアライゼーションまたはブランディングとして使用される。パーサマスター鍵の使用の規模が企業全体からより小さいワークグループに縮小されると、本明細書で説明されるデータ確保方法は、ユーザのグループ内でファイルを共有するために使用される。

【０３１２】

図２５に示され、以下で説明される実施例では、組織内の肩書または役割とともに定義される６人のユーザがいる。サイドバーは、ユーザが役割に従って属することができる、５つの可能なグループを表す。矢印は、グループのうちの１つ以上の中のユーザによる会員資格を表す。

【０３１３】

この実施例で使用するために確実なデータパーサを構成するときに、システム管理者は、維持プログラムによって、オペレーティングシステムからユーザおよびグループ情報にアクセスする。この維持プログラムは、パーサグループマスター鍵を生成し、グループの中での会員資格に基づいてユーザに割り当てる。

【０３１４】

この実施例では、上級スタッフグループの中に３人のメンバーがいる。このグループについて、措置は以下のようになる。

１．上級スタッフグループに対するパーサグループマスター鍵にアクセスする（利用可能でない場合は鍵を生成する）。

２．ＣＥＯを上級スタッフグループと関連付けるデジタル証明書を生成する。

３．ＣＦＯを上級スタッフグループと関連付けるデジタル証明書を生成する。

４．マーケティング部長を上級スタッフグループと関連付けるデジタル証明書を生成する。

【０３１５】

同じ一式の措置が、各グループ、および各グループ内の各メンバーに行われる。維持プログラムが完了すると、パーサグループマスター鍵は、グループの各メンバーに対する共有信任状になる。割り当てられたデジタル証明書の撤回は、グループの残りのメンバーに影響を及ぼすことなく、ユーザが維持プログラムを介してグループから除去されると、自動的に行われてもよい。

【０３１６】

いったん共有信任状が定義されると、解析および分割プロセスは同じままになる。ファイル、文書、またはデータ要素が確保されるとき、ユーザは、標的グループがデータを確保するときに使用されるために促される。結果として生じる確保されたデータは、標的グループの他のメンバーのみによってアクセス可能である。本発明の方法およびシステムのこの機能性は、任意の他のコンピュータシステムまたはソフトウェアプラットフォームとともに使用されてもよく、例えば、既存のアプリケーションプログラムに組み込まれるか、またはファイルセキュリティのために独立して使用されてもよい。

【０３１７】

暗号化アルゴリズムのうちのいずれか１つまたは組み合わせが、本発明の方法およびシステムで使用するために好適であることが、当業者に容易に明白である。例えば、暗号化ステップは、一実施形態では、多層暗号化スキームを生成するように繰り返されてもよい。加えて、異なる暗号化アルゴリズムが、多層暗号化スキームの異なる層に適用されるように、異なる暗号化アルゴリズム、または暗号化アルゴリズムの組み合わせが、反復暗号化ステップで使用されてもよい。そのようなものとして、暗号化スキーム自体が、未承認

の使用またはアクセスから機密データを確保するための本発明の方法の構成要素になってもよい。

【０３１８】

確実なデータパーサは、内部構成要素として、外部構成要素として、または両方として、エラーチェック構成要素を含んでもよい。例えば、１つの好適なアプローチでは、本発明による確実なデータパーサを使用して、データ部分が作成されるにつれて、一部分内のデータの完全性を確実にするために、ハッシュ値が一部分内で事前設定された間隔において得られ、間隔の終わりに付加される。ハッシュ値は、データの予測可能かつ再現可能な数値表現である。データ内の任意のビットが変化した場合、ハッシュ値は異なる。次いで、（確実なデータパーサの外部の独立型構成要素として、または内部構成要素としての）走査モジュールが、確実なデータパーサによって生成されるデータ部分を走査してもよい。各データ部分（または代替として、何らかの間隔に従った、またはランダムあるいは擬似ランダムサンプリングによる、全てよりも少ないデータ部分）は、１つまたは複数の付加されたハッシュ値と比較され、措置が講じられてもよい。この措置は、合致する、および合致しない値の報告、合致しない値に対するアラート、またはデータの復旧を誘起する何らかの外部あるいは内部プログラムの起動を含んでもよい。例えば、データの復旧は、本発明に従って元のデータを生成するために、全てよりも少ない部分が必要とされてもよいという概念に基づいて、復旧モジュールを起動することによって行うことができる。

【０３１９】

任意の他の好適な完全性チェックが、データ部分の全てまたは一部の中のどこかに付加された任意の好適な完全性情報を使用して、実装されてもよい。完全性情報は、データ部分の完全性を決定するために使用することができる、任意の好適な情報を含んでもよい。完全性情報の実施例は、任意の好適なパラメータに基づいて（例えば、それぞれのデータ部分に基づいて）計算されるハッシュ値、デジタル署名情報、メッセージ認証コード（ＭＡＣ）情報、任意の他の好適な情報、またなそれらの任意の組み合わせを含んでもよい。

【０３２０】

本発明の確実なデータパーサは、任意の好適な用途で使用されてもよい。すなわち、本明細書で説明される確実なデータパーサは、計算および技術の異なる分野で種々の用途を有する。いくつかのそのような分野を以下で論議する。これらは本質的に例示的にすぎず、任意の他の好適な用途が確実なデータパーサを利用してもよいことが理解されるであろう。さらに、説明される実施例は、任意の好適な所望を満たすために任意の好適な方法で修正されてもよい、例示的な実施形態にすぎないことが理解されるであろう。例えば、解析および分割は、ビットによって、バイトによる、キロバイトによる、メガバイトによる、それらの任意の組み合わせによる、または任意の他の好適な単位による等、任意の好適な単位に基づいてもよい。

【０３２１】

本発明の確実なデータパーサは、確実な物理的トークンを実装するために使用されてもよく、それにより、物理的トークンに記憶されたデータは、別の記憶領域に記憶された付加的なデータにアクセスするために必要とされてもよい。１つの好適なアプローチでは、コンパクトＵＳＢフラッシュドライブ、フロッピー（登録商標）ディスク、光ディスク、スマートカード、または任意の他の好適な物理的トークン等の物理的トークンが、本発明に従って解析されたデータの少なくとも２つの部分のうちの１つを記憶するために使用されてもよい。元のデータにアクセスするために、ＵＳＢフラッシュドライブがアクセスされる必要がある。したがって、解析されたデータの一部分を保持するパーソナルコンピュータは、元のデータにアクセスできる前に添付される、解析されたデータの他の部分を有する、ＵＳＢフラッシュドライブを有する必要がある。図２６は、この用途を図示する。記憶領域２５００は、解析されたデータの一部分２５０２を含む。解析されたデータの一部分２５０６を有する、物理的トークン２５０４は、元のデータにアクセスするために、任意の好適な通信インターフェース２５０８（例えば、ＵＳＢ、直列、並列、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＩＲ、ＩＥＥＥ　１３９４、Ｅｔｈｅｒｎｅｔ（登録商標）、ま

たは任意の他の好適な通信インターフェース）を使用して、記憶領域２５００に連結される必要がある。これは、例えば、コンピュータ上の機密データが放置され、未承認のアクセス試行の影響を受けやすい状況で有用である。物理的トークン（例えば、ＵＳＢフラッシュドライブ）を除去することによって、機密データはアクセス不可能である。物理的トークンを使用するための任意の他の好適なアプローチが使用されてもよいことが理解されるであろう。

【０３２２】

本発明の確実なデータパーサは、確実な認証システムを実装するために使用されてもよく、それにより、確実なデータパーサを使用して、ユーザ登録データ（例えば、パスワード、秘密暗号化鍵、指紋テンプレート、生体測定データ、または任意の他の好適なユーザ登録データ）が解析および分割される。ユーザ登録データは、解析および分割されてもよく、それにより、１つ以上の部分が、スマートカード、政府共通アクセスカード、任意の好適な物理的記憶デバイス（例えば、磁気または光ディスク、ＵＳＢ鍵ドライブ等）、または任意の他の好適なデバイス上に記憶される。解析されたユーザ登録データの１つ以上の他の部分は、認証を行うシステムに記憶されてもよい。これは、セキュリティの追加レベルを認証プロセスに提供する（例えば、生体測定源から取得される生体測定認証情報に加えて、ユーザ登録データも、適切な解析および分割データ部分を介して取得されなければならない）。

【０３２３】

本発明の確実なデータパーサは、各システムのそれぞれの環境でその機能性の使用を提供するために、任意の好適な既存のシステムに組み込まれてもよい。図２７は、任意の好適なアプリケーションを実装するためのソフトウェア、ハードウェア、または両方を含んでもよい、例示的システム２６００のブロック図を示す。システム２６００は、確実なデータパーサ２６０２が統合構成要素として据え付けられてもよい、既存のシステムであってもよい。代替として、確実なデータパーサ２６０２は、例えば、その初期設計段階から、任意の好適なシステム２６００に統合されてもよい。確実なデータパーサ２６００は、システム２６００の任意の好適なレベルで統合されてもよい。例えば、確実なデータパーサ２６０２の存在がシステム２６００のエンドユーザには実質的に見えなくてもよいように、確実なデータパーサ２６０２は、十分にバックエンドレベルでシステム２６００に統合されてもよい。確実なデータパーサ２６０２は、本発明に従って１つ以上の記憶デバイス２６０４の間でデータを解析および分割するために使用されてもよい。それに統合された確実なデータパーサを有する、システムのいくつかの例示的な実施例を以下で論議する。

【０３２４】

本発明の確実なデータパーサは、オペレーティングシステムカーネル（例えば、Ｌｉｎｕｘ（登録商標）、Ｕｎｉｘ（登録商標）、または任意の他の好適な商用あるいは専用オペレーティングシステム）に統合されてもよい。この統合は、デバイスレベルでデータを保護するために使用されてもよく、それにより、例えば、通常は１つ以上のデバイスに記憶されるデータが、オペレーティングシステムに統合された確実なデータパーサによって、ある数の部分に分離され、１つ以上のデバイス間で記憶される。元のデータがアクセスされるように試行されると、同様にオペレーティングシステムに統合された適切なソフトウェアが、エンドユーザには見えなくてもよい方法で、解析されたデータ部分を元のデータに再結合してもよい。

【０３２５】

本発明の確実なデータパーサは、任意または全てのサポートされたプラットフォームにわたって、ローカルのネットワーク接続されたデータ記憶装置を保護するように、記憶システムの容量マネージャまたは任意の他の好適な構成要素に統合されてもよい。例えば、確実なデータパーサが統合されると、記憶システムは、データ損失から保護するために、（すなわち、元のデータを再構成するために、全てよりも少ない分離されたデータ部分を必要とするという特徴を実装するために使用される）確実なデータパーサによって提供さ

れる冗長性を利用してもよい。確実なデータパーサはまた、冗長性を使用するか否かにかかわらず、記憶デバイスに書き込まれた全てのデータが、本発明の解析に従って生成される複数の部分の形態となることを可能にする。元のデータがアクセスされるように試行されると、同様に記憶システムの容量マネージャまたは他の好適な構成要素に統合された適切なソフトウェアが、エンドユーザには見えなくてもよい方法で、解析されたデータ部分を元のデータに再結合してもよい。

【０３２６】

１つの好適なアプローチでは、本発明の確実なデータパーサは、（ハードウェアまたはソフトウェアとして）ＲＡＩＤコントローラに統合されてもよい。これは、ドライブ故障の場合に耐故障性を維持しながら、複数のドライブへのデータの確実な記憶を可能にする。

【０３２７】

本発明の確実なデータパーサは、例えば、機密テーブル情報を保護するために、データベースに組み込まれてもよい。例えば、１つの好適なアプローチでは、データベース特定のセルと関連付けられるデータ（例えば、個別セル、１つ以上の特定の縦列、１つ以上の特定の横列、それらの任意の組み合わせ、またはデータベーステーブル全体）が、本発明に従って解析および分離されてもよい（例えば、異なる部分が、１つ以上の場所における１つ以上の記憶デバイス上で、または単一の記憶デバイス上で記憶される）。元のデータを閲覧するために該部分を再結合するアクセスが、従来の認証方法（例えば、ユーザ名およびパスワードクエリ）によって許諾されてもよい。

【０３２８】

本発明の確実なパーサは、進行中のデータ（すなわち、１つの場所から別の場所へのデータの転送）を伴う任意の好適なシステムに組み込まれてもよい。そのようなシステムは、例えば、Ｅメール、ストリーミングデータ放送、および無線（例えば、ＷｉＦｉ）通信を含む。Ｅメールに関して、１つの好適なアプローチでは、発信メッセージ（すなわち、テキスト、バイナリデータ、または両方（例えば、Ｅメールメッセージに添付されたファイル）を含有する）を解析し、異なる経路に沿って解析されたデータの異なる部分を送信し、したがって、複数のデータのストリームを作成するために、確実なパーサが使用されてもよい。これらのデータのストリームのうちのいずれか１つが損なわれた場合、元のデータを生成するために、本発明に従って、該部分のうちの１つより多くの部分が組み合わされることをシステムが要求してもよいため、元のメッセージは確実なままである。別の好適なアプローチでは、データの異なる部分は、一部分が取得された場合に、元のデータを生成するのに十分でなくてもよいように、連続的に１つの経路に沿って伝達されてもよい。異なる部分は、意図された受信者の場所に到達し、本発明に従って元のデータを生成するように組み合わされてもよい。

【０３２９】

図２８および２９は、そのようなＥメールシステムの例示的なブロック図である。図２８は、コンピュータ端末、パーソナルコンピュータ、手持ち式デバイス（例えば、ＰＤＡ、Ｂｌａｃｋｂｅｒｒｙ）、携帯電話、コンピュータネットワーク、任意の他の好適なハードウェア、またはそれらの任意の組み合わせ等の任意の好適なハードウェアを含んでもよい、送信者システム２７００を示す。送信者システム２７００は、例えば、Ｅメールメッセージ、バイナリデータファイル（例えば、グラフィック、音声、ビデオ等）、または両方であってもよい、メッセージ２７０４を生成および／または記憶するために使用される。メッセージ２７０４は、本発明による確実なデータパーサ２７０２によって解析および分割される。結果として生じたデータ部分は、ネットワーク２７０８（例えば、インターネット、イントラネット、ＬＡＮ、ＷｉＦｉ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、任意の他の好適な配線接続または無線通信手段、またはそれらの任意の組み合わせ）上で１つ以上の別個の通信経路２７０６にわたって受信者システム２７１０に伝達されてもよい。データ部分は、時間的に並行して、または代替として、異なるデータ部分の通信間の任意の好適な時間遅延に従って伝達されてもよい。受信者システム２７１０は、送信者システ

ム２７００に関して上記で説明されるように、任意の好適なハードウェアであってもよい。通信経路２７０６に沿って運ばれる別個のデータ部分は、本発明に従って元のメッセージまたはデータを生成するように、受信者システム２７１０において再結合される。

【０３３０】

図２９は、コンピュータ端末、パーソナルコンピュータ、手持ち式デバイス（例えば、ＰＤＡ）、携帯電話、コンピュータネットワーク、任意の他の好適なハードウェア、またはそれらの任意の組み合わせ等の任意の好適なハードウェアを含んでもよい、送信者システム２８００を示す。送信者システム２８００は、例えば、Ｅメールメッセージ、バイナリデータファイル（例えば、グラフィック、音声、ビデオ等）、または両方であってもよい、メッセージ２８０４を生成および／または記憶するために使用される。メッセージ２８０４は、本発明による確実なデータパーサ２８０２によって解析および分割される。結果として生じたデータ部分は、ネットワーク２８０８（例えば、インターネット、イントラネット、ＬＡＮ、ＷｉＦｉ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、任意の他の好適な通信手段、またはそれらの任意の組み合わせ）上で単一の通信経路２８０６にわたって受信者システム２８１０に伝達されてもよい。データ部分は、相互に対して通信経路２８０６にわたって連続的に伝達されてもよい。受信者システム２８１０は、送信者システム２８００に関して上記で説明されるように、任意の好適なハードウェアであってもよい。通信経路２８０６に沿って運ばれる別個のデータ部分は、本発明に従って元のメッセージまたはデータを生成するように、受信者システム２８１０において再結合される。

【０３３１】

図２８および２９の配設は例示的にすぎないことが理解される。任意の他の好適な配設が使用されてもよい。例えば、別の好適なアプローチでは、図２８および２９のシステムの特徴が組み合わされてもよく、それにより、図２８のマルチパスアプローチが使用され、通信経路２７０６のうちの１つ以上は、図２９との関連で通信経路２８０６が運ぶように、１つより多くのデータ部分を運ぶために使用される。

【０３３２】

確実なデータパーサは、進行中データシステムの任意の好適なレベルで統合されてもよい。例えば、Ｅメールシステムとの関連で、確実なパーサは、ユーザインターフェースレベルで（例えば、Ｍｉｃｒｏｓｏｆｔ（登録商標）　Ｏｕｔｌｏｏｋに）組み込まれてもよく、その場合、ユーザは、Ｅメールを使用するときに確実なデータパーサの特徴の使用を制御してもよい。代替として、確実なパーサは、交換サーバ等のバックエンド構成要素で実装されてもよく、その場合、メッセージは、ユーザ介入を伴わずに、本発明に従って、自動的に解析され、分割され、異なる経路に沿って伝達されてもよい。

【０３３３】

同様に、データ（例えば、音声、ビデオ）のストリーミング放送の場合、発信データは、解析され、それぞれ解析されたデータ部分を含有する複数のストリームに分離されてもよい。複数のストリームは、本発明に従って、１つ以上の経路に沿って伝送され、受信者の場所で再結合されてもよい。このアプローチの有益性のうちの１つは、単一の通信チャネル上の暗号化されたデータの伝送が後に続く、データの従来の暗号化と関連付けられる比較的大きいオーバーヘッドを回避することである。本発明の確実なパーサは、進行中のデータが複数の並列ストリームで送信されることを可能にし、速度および効率を増加させる。

【０３３４】

確実なデータパーサは、例えば、有線、無線、または物理的媒体を含む、任意の輸送媒体を介して、進行中の任意の種類のデータの保護および耐故障性のために統合されてもよいことが理解されるであろう。例えば、ボイスオーバーインターネットプロトコル（ＶｏＩＰ）アプリケーションが、本発明の確実なデータパーサを利用してもよい。本発明の確実なデータパーサを使用して、ＢｌａｃｋｂｅｒｒｉｅｓおよびＳｍａｒｔＰｈｏｎｅｓ等の任意の好適な携帯情報端末（ＰＤＡ）デバイスを往復する無線または有線データ輸送が確保されてもよい。ピアツーピアおよびハブベースの無線ネットワークに無線８０２．

１１プロトコルを使用した通信、衛星通信、ポイントツーポイント無線通信、インターネットクライアント／サーバ通信、または任意の他の好適な通信は、本発明に従って、確実なデータパーサの進行中データ能力を伴ってもよい。コンピュータ周辺デバイス（例えば、プリンタ、スキャナ、モニタ、キーボード、ネットワークルータ、生体測定認証デバイス（例えば、指紋スキャナ）、または任意の他の好適な周辺デバイス）の間、コンピュータとコンピュータ周辺デバイスとの間、コンピュータ周辺デバイスと任意の他の好適なデバイスとの間、またはそれらの任意の組み合わせでのデータ通信は、本発明の進行中データ特徴を利用してもよい。

【０３３５】

本発明の進行中データ特徴はまた、例えば、別個のルート、媒介物、方法、任意の他の好適な物理的輸送、またはそれらの任意の組み合わせを使用して、確実なシェアの物理的輸送に適用してもよい。例えば、データの物理的輸送は、デジタル／磁気テープ、フロッピー（登録商標）ディスク、光ディスク、物理的トークン、ＵＳＢドライブ、可撤性ハードドライブ、フラッシュメモリを伴う家庭用電子デバイス（例えば、Ａｐｐｌｅ　ＩＰＯＤまたは他のＭＰ３プレーヤ）、フラッシュメモリ、データを輸送するために使用される任意の他の好適な媒体、またはそれらの任意の組み合わせの上で行われてもよい。

【０３３６】

本発明の確実なデータパーサは、障害復旧のための能力を伴うセキュリティを提供してもよい。本発明によれば、確実なデータパーサによって生成される、分離されたデータの全てよりも少ない部分が、元のデータを回収するために必要であってもよい。つまり、記憶されたｍ個の部分のうち、ｎは、元のデータを回収するために必要なこれらのｍ個の部分の最小数であってもよく、ｎ＜＝ｍである。例えば、４つの部分のそれぞれが、他の３つの部分に対して異なる物理的場所に記憶される場合、次いで、この実施例ではｎ＝２であれば、場所のうちの２つが損なわれる場合があり、それにより、データが破壊されるか、またはアクセス不可能であり、元のデータは、他の２つの場所の部分から依然として回収されてもよい。ｎまたはｍの任意の好適な値が使用されてもよい。

【０３３７】

加えて、本発明のｍ個の特徴のうちのｎ個が、「２人規則」を作成するために使用されてもよく、それにより、１人の個人または任意の他の実体に、機密データであってもよいものへの完全なアクセスを信託することを回避するために、それぞれ本発明の確実なパーサによって解析される分離されたデータの一部分を伴う、２つ以上の明確に異なる実体が、元のデータを回収するためにそれらの部分をまとめることに同意する必要があってもよい。

【０３３８】

本発明の確実なデータパーサは、グループメンバーが、その特定のグループによってアクセスされるように承認された特定の情報にアクセスすることを可能にする、グループ全体の鍵を実体のグループに提供するために使用されてもよい。グループ鍵は、例えば、求められた情報を回収するために、中央に記憶された別の部分と組み合わされることを要求されてもよい、本発明による確実なパーサによって生成されるデータ部分のうちの１つであってもよい。この特徴は、例えば、グループ間の確実な協調を可能にする。それは、例えば、専用ネットワーク、仮想プライベートネットワーク、インスタンス、または任意の他の好適なネットワークで適用されてもよい。

【０３３９】

この確実なパーサの使用の具体的な用途は、（すなわち、現在使用されている、比較的実質的な手動プロセスを伴う多くのネットワークと比較して）例えば、単一のネットワークまたは二重ネットワーク上で各国に承認されたセキュリティレベルにおいて、動作および別様の機密データを伝達する能力が、多国籍友好政府軍に与えられる、連合情報共有を含む。この能力はまた、情報を閲覧する未承認の個人について心配する必要なく、（組織内または外の）１人以上の特定の個人によって知られる必要がある情報が、単一のネットワーク上で伝達されてもよい、企業または他の組織にも適用可能である。

【０３４０】
別の具体的な用途は、政府システムに対するマルチレベルセキュリティ階層を含む。つまり、本発明の確実なパーサは、単一のネットワークを使用して、機密情報の異なるレベル（例えば、非機密、機密、秘密、極秘）で政府システムを操作する能力を提供してもよい。所望であれば、より多くのネットワークが使用されてもよい（例えば、極秘には別個のネットワーク）が、本発明は、別個のネットワークが各分類レベルに使用される、現在よりも大幅に少ない配設を可能にする。
【０３４１】
本発明の確実なパーサの上記の用途の任意の組み合わせが使用されてもよいことが、理解されるであろう。例えば、グループ鍵用途は、進行中データセキュリティ用途とともに使用することができる（すなわち、それにより、ネットワーク上で伝達されるデータは、それぞれのグループのメンバーのみによってアクセスすることができ、データが進行中である間に、本発明に従って複数の経路間で分割される（または順次部分で送信される）。
【０３４２】
本発明の確実なデータパーサは、アプリケーションまたはデータベースのいずれか一方への修正を伴わずに、アプリケーションが、異なるデータベース製品に、または異なるデバイスにデータを確実に記憶することを可能にするように、任意のミドルウェアアプリケーションに組み込まれてもよい。ミドルウェアは、２つの別個かつ既存のプログラムが通信することを可能にする、任意の製品に対する一般用語である。例えば、１つの好適なアプローチでは、組み込まれた確実なデータパーサを有するミドルウェアは、特定のデータベースのために書き込まれたプログラムが、カスタムコーディングを伴わずに他のデータベースと通信することを可能にするために使用されてもよい。
【０３４３】
本発明の確実なデータパーサは、本明細書で論議されるもの等の任意の好適な能力の任意の組み合わせを有して実装されてもよい。本発明のいくつかの実施形態では、例えば、確実なデータパーサが、ある能力のみを有して実装されてもよい一方で、他の能力は、確実なデータパーサと直接または間接的にインターフェース接続される、外部ソフトウェア、ハードウェア、または両方の使用を介して得られてもよい。
【０３４４】
図３０は、例えば、確実なデータパーサ３０００としての確実なデータパーサの例示的な実装を示す。確実なデータパーサ３０００は、ごく少数の内蔵能力を伴って実装されてもよい。図示されるように、確実なデータパーサ３０００は、本発明によるモジュール３００２を使用して、データを解析し、データ部分（本明細書ではシェアとも呼ばれる）に分割するための内蔵能力を含んでもよい。確実なデータパーサ３０００はまた、モジュール３００４を使用して、例えば、上記で説明されるｎ個の特徴のうちのｍ個を実装することができるために、冗長性を実施する（すなわち、解析および分割されたデータの全てよりも少ないシェアを使用して、元のデータを再作成する）ための内蔵能力を含んでもよい。確実なデータパーサ３０００はまた、本発明に従って、遠隔場所への通信のため、記憶のため等にデータのシェアがそこから送信される、バッファの中へデータのシェアを配置するためのモジュール３００６を使用する、シェア分配能力を含んでもよい。任意の他の好適な能力が確実なデータパーサ３０００に組み込まれてもよいことが、理解されるであろう。
【０３４５】
集約データバッファ３００８は、確実なデータパーサ３０００によって解析および分割される（必ずしもその元の形態ではないが）元のデータを記憶するために使用される、任意の好適なメモリであってもよい。分割動作では、集約データバッファ３００８は、入力を確実なデータパーサ３００８に提供する。修復動作では、集約データバッファ３００８は、確実なデータパーサ３０００の出力を記憶するために使用されてもよい。
【０３４６】
分割シェアバッファ３０１０は、元のデータの解析および分割に起因したデータの複数

のシェアを記憶するために使用されてもよい、１つ以上のメモリモジュールであってもよい。分割動作では、分割シェアバッファ３０１０は、確実なデータパーサの出力を保持する。修復動作では、分割シェアバッファは、確実なデータパーサ３０００への入力を保持する。

【０３４７】

能力の任意の他の好適な配設が、確実なデータパーサ３０００のために内蔵されてもよいことが理解されるであろう。任意の付加的な特徴が内蔵されてもよく、図示された特徴のうちのいずれかは、除去され、よりロバストにされ、あまりロバストにされず、またはそうでなければ任意の好適な方法で修正されてもよい。バッファ３００８および３０１０は、同様に例示的にすぎず、任意の好適な方法で修正、除去、または追加されてもよい。

【０３４８】

ソフトウェア、ハードウェア、または両方で実装される任意の好適なモジュールは、確実なデータパーサ３０００によって呼び出されてもよく、または確実なデータパーサ３０００を呼び出してもよい。所望であれば、確実なデータパーサ３０００に内蔵される能力さえも、１つ以上の外部モジュールに置換されてもよい。図示されるように、いくつかの外部モジュールは、乱数発生器３０１２、暗号フィードバック鍵発生器３０１４、ハッシュアルゴリズム３０１６、いずれか１つ以上の種類の暗号化３０１８、および鍵管理３０２０を含む。これらは例示的な外部モジュールにすぎないことが理解されるであろう。図示されたものに加えて、またはそれらの代わりに、任意の他の好適なモジュールが使用されてもよい。

【０３４９】

暗号フィードバック鍵発生器３０１４は、確実なデータパーサ３０００の外部で、それぞれの確実なデータパーサの動作のために、元のセッション鍵サイズ（例えば、１２８、２５６、５１２、または１０２４ビットの値）を、解析および分割されるデータの長さに等しい値に拡張する、動作のシード値として使用される、一意の鍵または乱数（例えば、乱数発生器３０１２を使用して）を生成してもよい。例えば、ＡＥＳ暗号フィードバック鍵生成アルゴリズムを含む、任意の好適なアルゴリズムが、暗号フィードバック鍵生成に使用されてもよい。

【０３５０】

アプリケーション層３０２４（例えば、Ｅメールアプリケーション、データベースアプリケーション等）への確実なデータパーサ３０００およびその外部モジュール（すなわち、確実なデータパーサ層３０２６）の統合を促進するために、例えば、ＡＰＩ関数呼び出しを利用してもよい、ラッピング層が使用されてもよい。アプリケーション層３０２４への確実なデータパーサ層３０２６の統合を促進するための任意の他の好適な配設が使用されてもよい。

【０３５１】

図３１は、（例えば、記憶デバイスへの）書き込み、（例えば、データベースフィールドの中の）挿入、または（例えば、ネットワークにわたる）伝送コマンドがアプリケーション層３０２４で発行されるときに、図３０の配設がどのように使用されてもよいかを例示的に示す。ステップ３１００では、確保されるデータが識別され、確実なデータパーサへ呼び出しが行われる。呼び出しは、ラッパー層３０２２を通過させられ、ステップ３１０２では、ラッパー層３０２２が、ステップ３１００で識別された入力データを集約データバッファ３００８の中へ流す。また、ステップ３１０２では、任意の好適なシェア情報、ファイル名、任意の他の好適な情報、またはそれらの任意の組み合わせが記憶されてもよい（例えば、ラッパー層３０２２における情報３１０６として）。次いで、確実なデータプロセッサ３０００は、本発明に従って集約データバッファ３００８から入力として受け取る、データを解析および分割する。それは、分割シェアバッファ３０１０の中へデータシェアを出力する。ステップ３１０４では、ラッパー層３０２２が、記憶された情報３１０６から、（すなわち、ステップ３１０２でラッパー３０２２によって記憶される）任意の好適なシェア情報および（例えば、１つ以上の構成ファイルからの）シェア場所を取

得する。次いで、ラッパー層３０２２は、（分割シェアバッファ３０１０から取得された）出力シェアを適切に書き込む（例えば、ネットワーク等の上へ伝達される１つ以上の記憶デバイスに書き込まれる）。

【０３５２】

図３２は、（例えば、記憶デバイスからの）読み出し、（例えば、データベースフィールドからの）選択、または（例えば、ネットワークからの）受信が発生するときに、図３０の配設がどのように使用されてもよいかを例示的に示す。ステップ３２００では、修復されるデータが識別され、確実なデータパーサ３０００への呼び出しがアプリケーション層３０２４から行われる。ステップ３２０２では、ラッパー層３０２２から、任意の好適なシェア情報が取得され、シェア場所が決定される。ラッパー層３０２２は、ステップ３２００で識別されたデータ部分を、分割シェアバッファ３０１０の中へロードする。次いで、確実なデータパーサ３０００は、本発明に従ってこれらのシェアを処理する（例えば、４つのシェアのうちの３つのみが利用可能である場合には、３つだけのシェアを使用して元のデータを修復するために、確実なデータパーサ３０００の冗長性能力が使用されてもよい）。次いで、修復されたデータは、集約データバッファ３００８に記憶される。ステップ３２０４では、アプリケーション層３０２２が、（筆意用であれば）集約データバッファ３００８に記憶されたデータを、その元のデータ形式に変換し、その元の形式の元のデータをアプリケーション層３０２４に提供する。

【０３５３】

図３１に図示された元のデータの解析および分割、ならびに図３２に図示された元のデータへのデータ部分の復元は、例示的にすぎないことが理解されるであろう。図示されたものに加えて、またはそれらの代わりに、任意の他の好適なプロセス、構成要素、または両方が使用されてもよい。

【０３５４】

図３３は、本発明の一実施形態による、元のデータを解析し、２つ以上のデータ部分に分割するための例示的なプロセスフローのブロック図である。図示されるように、解析または分割されることを所望される元のデータは、プレーンテキスト３３０６である（すなわち、「ＳＵＭＭＩＴ」という言葉が実施例として使用される）。任意の種類のデータが本発明に従って解析および分割されてもよいことが理解されるであろう。セッション鍵３３００が生成される。セッション鍵３３００の長さが元のデータ３３０６の長さに適合しない場合には、暗号フィードバックセッション鍵３３０４が生成されてもよい。

【０３５５】

１つの好適なアプローチでは、元のデータ３３０６は、解析、分割、または両方の前に暗号化されてもよい。例えば、図３３が図示するように、元のデータ３３０６は、任意の好適な値を用いて（例えば、暗号フィードバックセッション鍵３３０４を用いて、または任意の他の好適な値を用いて）排他的論理和をとられてもよい。図示されたＸＯＲ技法の代わりに、またはそれに加えて、任意の他の好適な暗号化技法が使用されてもよいことが理解されるであろう。図３３は、バイトごとの動作に関して図示されているが、動作は、ビットレベルで、または任意の他の好適なレベルで行われてもよいことが、さらに理解されるであろう。さらに、所望であれば、どのようなものであれ、元のデータ３３０６の暗号化が全く存在する必要がないことが理解されるであろう。

【０３５６】

次いで、結果として生じた暗号化されたデータ（またはいずれの暗号化も行われなかった場合は元のデータ）は、出力バケット（例えば、図示された実施例では４つある）間で暗号化された（または元の）データをどのように分割するかを決定するように、ハッシュ値計算される。図示された実施例では、ハッシングは、バイトによって行われ、暗号フィードバックセッション鍵３３０４の関数である。これは例示的にすぎないことが理解される。ハッシングは、所望であれば、ビットレベルで行われてもよい。ハッシングは、暗号フィードバックセッション鍵３３０４のほかに、任意の他の好適な値の関数であってもよい。別の好適なアプローチでは、ハッシングは使用される必要がない。むしろ、データを

分割するための任意の他の好適な技法が採用されてもよい。

【０３５７】

図３４は、本発明の一実施形態による、元のデータ３３０６の２つ以上の解析および分割された部分から元のデータ３３０６を修復するための例示的プロセスのブロック図である。プロセスは、暗号化された元のデータ（または解析および分割の前に暗号化がなかった場合は元のデータ）を修復するように、暗号フィードバックセッション鍵３３０４の関数として（すなわち、図３３のプロセスとは）逆に該部分のハッシュ値を計算することを伴う。次いで、暗号化鍵が、元のデータを修復するために使用されてもよい（すなわち、図示された実施例では、暗号化されたデータを用いてそれの排他的論理和をとることによってＸＯＲ暗号化を復号するために、暗号フィードバックセッション鍵３３０４が使用される）。これは元のデータ３３０６を修復する。

【０３５８】

図３５は、ビット分割がどのように図３３および３４の実施例で実装されてもよいかを示す。データの各バイトを分割するビット値を決定するために、ハッシュが使用されてもよい（例えば、暗号フィードバックセッション鍵の関数として、任意の他の好適な値の関数として）。これは、ビットレベルで分割を実装する１つの例示的な方法にすぎないことが理解されるであろう。任意の他の好適な技法が使用されてもよい。

【０３５９】

本明細書で行われるハッシュ機能性への言及は、任意の好適なハッシュアルゴリズムに関して行われてもよいことが理解されるであろう。これらは、例えば、ＭＤ５およびＳＨＡ－１を含む。異なるハッシュアルゴリズムが、異なるときに、かつ本発明の異なる構成要素によって使用されてもよい。

【０３６０】

上記の例示的な手順に従って、または任意の他の手順あるいはアルゴリズムを介して、分割点が決定された後、どのデータ部分を左右のセグメントのそれぞれに付加するかに関して決定が行われてもよい。任意の好適なアルゴリズムが、この決定を行うために使用されてもよい。例えば、１つの好適なアプローチでは、（例えば、左セグメントおよび右セグメントに対する宛先のペアリングの形態で）全ての可能な分配のテーブルが作成されてもよく、それにより、生成され、元のデータのサイズまで拡張されてもよいセッション鍵、暗号フィードバックセッション鍵、または任意の他の好適な乱数または擬似乱数値の中の対応するデータに任意の好適なハッシュ関数を使用することによって、左右のセグメントのそれぞれに対する宛先シェア値が決定されてもよい。例えば、乱数または擬似乱数値の中の対応するバイトのハッシュ関数が作られてもよい。ハッシュ関数の出力は、全ての宛先の組み合わせのテーブルから、どの宛先のペアリングを選択するか（すなわち、左のセグメントに１つ、および右のセグメントに１つ）を決定するために使用される。この結果に基づいて、分割されたデータ単位の各セグメントは、ハッシュ関数の結果として選択されるテーブル値によって示される、それぞれの２つのシェアに付加される。

【０３６１】

冗長性情報は、全てよりも少ないデータ部分を使用して、元のデータの修復を可能にするように、本発明に従ってデータ部分に付加されてもよい。例えば、４つの部分のうちの２つがデータの修復のために十分となるように所望される場合には、シェアからの付加的なデータは、例えば、ラウンドロビン方式で、それに応じて各シェアに付加されてもよい（例えば、元のデータのサイズが４ＭＢである場合には、シェア１が独自のシェアならびにシェア２および３のシェアを得て、シェア２が独自のシェアならびにシェア３および４のシェアを得て、シェア３が独自のシェアならびにシェア４および１のシェアを得て、シェア４が独自のシェアならびにシェア１および２のシェアを得る）。任意のそのような好適な冗長性が本発明に従って使用されてもよい。

【０３６２】

本発明に従って、元のデータセットからデータ部分を生成するために、任意の他の好適な解析および分割アプローチが使用されてもよいことが理解されるであろう。例えば、解

析分割は、ビット毎に無作為または擬似無作為に処理されてもよい。乱数または擬似乱数値が使用されてもよく（例えば、セッション鍵、暗号フィードバックセッション鍵等）、それにより、元のデータの中の各ビットについて、乱数または擬似乱数値の中の対応するデータへのハッシュ関数の結果は、どのシェアをそれぞれのビットに付加するかを示してもよい。１つの好適なアプローチでは、ハッシュ関数が、元のデータの各ビットに関する乱数または擬似欄数値の対応するバイトに行われてもよいように、乱数または擬似欄数値は、元のデータのサイズの８倍として生成されるか、または８倍まで拡張されてもよい。ビットごとのレベルでデータを解析および分割するための任意の他の好適なアルゴリズムが、本発明に従って使用されてもよい。さらに、本発明に従って、例えば、直上で説明される方式等で、冗長性データがデータシェアに付加されてもよいことが理解されるであろう。

【０３６３】

１つの好適なアプローチでは、解析および分割は、無作為または擬似無作為である必要はない。むしろ、データを解析および分割するための任意の好適な決定論アルゴリズムが使用されてもよい。例えば、元のデータを順次シェアに細分化することが、解析および分割アルゴリズムとして採用されてもよい。別の実施例は、ラウンドロビン方式で連続的に各ビットをデータシェアに付加して、ビット毎に元のデータを解析および分割することである。さらに、本発明に従って、例えば、直上で説明される方式等で、冗長性データがデータシェアに付加されてもよいことが理解されるであろう。

【０３６４】

本発明の一実施形態では、確実なデータパーサが元のデータのいくつかの部分を生成した後に、元のデータを修復するために、生成された部分のうちのある１つ以上が必須であってもよい。例えば、該部分のうちの１つが認証シェア（例えば、物理的トークンデバイス上に保存されている）として使用される場合、および確実なデータパーサの耐故障性特徴が使用されている場合（すなわち、全てよりも少ない部分が元のデータを修復するために必要である）、たとえ確実なデータパーサが、元のデータを修復するために元のデータの十分な数の部分にアクセスできてもよくても、元のデータを修復する前に物理的トークンデバイス上に記憶された認証シェアを要求してもよい。例えば、アプリケーション、データの種類、ユーザ、任意の他の好適な因子、またはそれらの任意の組み合わせに応じて、任意の数および種類の特定のシェアが必要とされてもよいことが理解されるであろう。

【０３６５】

１つの好適なアプローチでは、確実なデータパーサまたは確実なデータパーサにとっての何らかの外部構成要素が、元のデータの１つ以上の部分を暗号化してもよい。暗号化された部分は、元のデータを修復するために提供および暗号化されるように要求されてもよい。異なる暗号化された部分が、異なる暗号化鍵で暗号化されてもよい。

例えば、この特徴は、より確実な「２人規則」を実装するために使用されてもよく、それにより、第１のユーザは、第１の暗号化を使用して、特定のシェアを暗号化させる必要があり、第２のユーザは、第２の暗号化鍵を使用して、特定のシェアを暗号化させる必要がある。元のデータにアクセスするために、両方のユーザは、それぞれの暗号化鍵を有し、元のデータのそれぞれの部分を提供する必要がある。１つの好適なアプローチでは、元のデータを修復するために必要とされる必須シェアであってもよい、１つ以上のデータ部分を暗号化するために、公開鍵が使用されてもよい。次いで、元のデータに復元するように使用されるために、シェアを復号するために秘密鍵が使用されてもよい。

【０３６６】

全てよりも少ないシェアが元のデータを修復するために必要とされる、必死シェアを利用する任意のそのような好適なパラダイムが使用されてもよい。

【０３６７】

本発明の１つの好適な実施形態では、統計的予測から、データの任意の特定のシェアがデータの特定の単位を受信する確率が、残りのシェアのうちのいずれか１つがデータの単位を受信する確率に等しいように、データの有限数のシェアの中へのデータの分配は、無

作為または擬似無作為に処理されてもよい。結果として、データの各シェアは、ほぼ等しい量のデータビットを有する。

【０３６８】

本発明の別の実施形態によれば、データの有限数のシェアのそれぞれは、元のデータの解析および分割からデータの単位を受信する等しい確率を有する必要はない。むしろ、ある１つ以上のシェアが、残りのシェアよりも高いまたは低い確率を有してもよい。結果として、あるシェアは、ビットサイズに関して、他のシェアに対してより大きいか、または小さくてもよい。例えば、２つのシェアのシナリオでは、１つのシェアが、データの単位を受信する１％の確率を有してもよい一方で、第２のシェアは、９９％の確率を有する。したがって、いったんデータ単位が２つのシェア間で確実なデータパーサによって分配されると、第１のシェアはデータの約１％を有し、第２のシェアは９９％を有するべきであるということになるべきである。任意の好適な確率が、本発明に従って使用されてもよい。

【０３６９】

確実なデータパーサは、確実な（またはほぼ確実な）パーセンテージに従ってデータをシェアに分配するようにプログラムされてもよいことが理解されるであろう。例えば、確実なデータパーサは、データの８０％を第１のシェアに、データの残りの２０％を第２のシェアに分配するようにプログラムされてもよい。

【０３７０】

本発明の別の実施形態によれば、確実なデータパーサは、データシェアを生成してもよく、そのうちの１つ以上は所定のサイズを有する。例えば、確実なデータパーサは、元のデータを、データ部分のうちの１つが正確に２５６ビットであるデータ部分に分割してもよい。１つの好適なアプローチでは、必要サイズを有するデータ部分を生成することが可能ではない場合には、確実なデータパーサが、該部分を正しいサイズにするように水増ししてもよい。任意の好適なサイズが使用されてもよい。

【０３７１】

１つの好適なアプローチでは、データ部分のサイズは、暗号化鍵、分割鍵、任意の他の好適な鍵、または任意の他の好適なデータ要素のサイズであってもよい。

【０３７２】

以前に論議されたように、確実なデータパーサは、データの解析および分割で鍵を使用してもよい。明確かつ簡略にする目的で、これらの鍵は、本明細書では「分割鍵」と呼ばれるものとする。例えば、以前に紹介されたセッションマスター鍵は、一種の分割鍵である。また、以前に論議されたように、分割鍵は、確実なデータパーサによって生成されるデータのシェア内で確保されてもよい。分割鍵を確保するための任意の好適なアルゴリズムが、データのシェア間でそれらを確保するために使用されてもよい。例えば、Ｓｈａｍｉｒアルゴリズムが分割鍵を確保するために使用されてもよく、それにより、分割鍵を再構成するために使用されてもよい情報が生成され、データのシェアに付加される。任意の他のそのような好適なアルゴリズムが、本発明に従って使用されてもよい。

【０３７３】

同様に、任意の好適な暗号化鍵が、Ｓｈａｍｉｒアルゴリズム等の任意の好適なアルゴリズムに従って、データの１つ以上のシェア内で確保されてもよい。例えば、解析および分割前にデータセットを暗号化するために使用される暗号化鍵、解析および分割後にデータ部分を暗号化するために使用される暗号化鍵、または両方が、例えば、Ｓｈａｍｉｒアルゴリズムまたは任意の他の好適なアルゴリズムを使用して確保されてもよい。

【０３７４】

本発明の一実施形態によれば、分割鍵、暗号化鍵、任意の他の好適なデータ要素、またはそれらの任意の組み合わせを変換することによって、データをさらに確保するために、Ｆｕｌｌ　Ｐａｃｋａｇｅ　Ｔｒａｎｓｆｏｒｍ等のＡｌｌ　ｏｒ　Ｎｏｔｈｉｎｇ　Ｔｒａｎｓｆｏｒｍ（ＡｏＮＴ）が使用されてもよい。例えば、本発明に従って解析および分割前にデータセットを暗号化するために使用される暗号化鍵は、ＡｏＮＴ　アルゴリズ

ムによって変換されてもよい。次いで、変換された暗号化鍵は、例えば、Ｓｈａｍｉｒアルゴリズムまたは任意の他の好適なアルゴリズムに従って、データシェア間で分配されてもよい。暗号化鍵を再構成するためには、当業者に周知であるように、ＡｏＮＴに従った変換に関する必要な情報にアクセスするために、暗号化されたデータセットが修復されなければならない（例えば、冗長性が本発明に従って使用された場合、必ずしも全てのデータシェアを使用するとは限らない）。元の暗号化鍵が回収されると、暗号化されたデータセットを復号して元のデータセットを回収するために使用されてもよい。本発明の耐故障性特徴は、ＡｏＮＴ特徴と併せて使用されてもよいことが理解されるであろう。すなわち、暗号化されたデータセットを修復するために、全てよりも少ないデータ部分が必要であるように、冗長性データがデータ部分に含まれてもよい。

【０３７５】

解析および分割前のデータセットに対応するそれぞれの暗号化鍵の暗号化およびＡｏＮＴの代わりに、またはそれに加えて、解析および分割後にデータ部分を暗号化するために使用される暗号化鍵に、ＡｏＮＴが適用されてもよいことが理解されるであろう。同様に、ＡｏＮＴは、分割鍵に適用されてもよい。

【０３７６】

本発明の一実施形態では、本発明に従って使用されるような暗号化鍵、分割鍵、または両方は、追加レベルのセキュリティを確保されたデータセットに提供するために、例えば、ワークグループ鍵を使用して、さらに暗号化されてもよい。

【０３７７】

本発明の一実施形態では、確実なデータパーサがデータを分割するように起動されるときはいつでも追跡するオーディットモジュールが提供されてもよい。

【０３７８】

図３６は、本発明による、確実なデータパーサの構成要素を使用するための可能なオプション３６００を図示する。オプションの各組み合わせは、以下で概説され、図３６からの適切なステップ番号で標識される。確実なデータパーサは、本質的にモジュール式であり、任意の公知のアルゴリズムが図３６に示された機能ブロックのそれぞれの内側で使用されることを可能にする。例えば、Ｂｌａｋｅｌｙ等の他の鍵分割（例えば、秘密共有）アルゴリズムが、Ｓｈａｍｉｒの代わりに使用されてもよく、またはＡＥＳ暗号化を、Ｔｒｉｐｌｅ　ＤＥＳ等の他の公知の暗号化アルゴリズムに置換することができる。図３６の実施例に示された標識は、本発明の一実施形態で使用するためのアルゴリズムの１つの可能な組み合わせを描写するにすぎない。任意の好適なアルゴリズムまたはアルゴリズムの組み合わせが、標識されたアルゴリズムの代わりに使用されてもよいことを理解されたい。

【０３７９】

１）３６１０、３６１２、３６１４、３６１５、３６１６、３６１７、３６１８、３６１９

ステップ３６１０で以前に暗号化されたデータを使用して、データは、最終的に所定数のシェアに分割されてもよい。分割アルゴリズムが鍵を必要とする場合、暗号で確実な擬似乱数発生器を使用して、分割暗号化鍵がステップ３６１２で生成されてもよい。分割暗号化鍵は、任意に、ステップ３６１５で耐故障性を伴う所定数のシェアに鍵分割される前に、Ａｌｌ　ｏｒ　Ｎｏｔｈｉｎｇ　Ｔｒａｎｓｆｏｒｍ（ＡｏＮＴ）を使用して、ステップ３６１４において変換分割鍵に変換されてもよい。次いで、データは、ステップ３６１６において所定数のシェアに分割されてもよい。総数よりも少ないシェアからのデータの再生を可能にするために、耐故障スキームがステップ３６１７において使用されてもよい。いったんシェアが作成されると、認証／完全性情報がステップ３６１８においてシェアに埋め込まれてもよい。各シェアは、任意に、ステップ３６１９で事後暗号化されてもよい。

【０３８０】

２）３１１１、３６１２、３６１４、３６１５、３６１６、３６１７、３６１８、３６

１９

いくつかの実施形態では、ユーザまたは外部システムによって提供される暗号化鍵を使用して、入力データが暗号化されてもよい。外部鍵がステップ３６１１において提供される。例えば、鍵は、外部鍵記憶から提供されてもよい。分割アルゴリズムが鍵を必要とする場合、暗号で確実な擬似乱数発生器を使用して、分割暗号化鍵がステップ３６１２において生成されてもよい。分割鍵は、任意に、ステップ３６１５において耐故障性を伴う所定数のシェアに鍵分割される前に、Ａｌｌ　ｏｒ　Ｎｏｔｈｉｎｇ　Ｔｒａｎｓｆｏｒｍ（ＡｏＮＴ）を使用して、ステップ３６１４において変換分割暗号化鍵に変換されてもよい。次いで、データは、ステップ３６１６において所定数のシェアに分割される。総数よりも少ないシェアからのデータの再生を可能にするために、耐故障スキームがステップ３６１７において使用されてもよい。いったんシェアが作成されると、認証／完全性情報がステップ３６１８においてシェアに埋め込まれてもよい。各シェアは、任意に、ステップ３６１９において事後暗号化されてもよい。

【０３８１】

３）３６１２、３６１３、３６１４、３６１５、３６１２、３６１４、３６１５、３６１６、３６１７、３６１８、３６１９

いくつかの実施形態では、データを変換するように、暗号で確実な擬似乱数発生器を使用して、暗号化鍵がステップ３６１２において生成されてもよい。生成された暗号化鍵を使用したデータの暗号化は、ステップ３６１３において発生してもよい。暗号化鍵は、任意に、Ａｌｌ　ｏｒ　Ｎｏｔｈｉｎｇ　Ｔｒａｎｓｆｏｒｍ（ＡｏＮＴ）を使用して、ステップ３６１４において変換暗号化鍵に変換されてもよい。次いで、変換暗号化鍵および／または生成された暗号化鍵は、ステップ３６１５において耐故障性を伴う所定数のシェアに分割されてもよい。分割アルゴリズムが鍵を必要とする場合、暗号で確実な擬似乱数発生器を使用した、分割暗号化鍵の生成が、ステップ３６１２において発生してもよい。分割鍵は、任意に、ステップ３６１５において耐故障性を伴う所定数のシェアに鍵分割される前に、Ａｌｌ　ｏｒ　Ｎｏｔｈｉｎｇ　Ｔｒａｎｓｆｏｒｍ（ＡｏＮＴ）を使用して、ステップ３６１４において変換分割暗号化鍵に変換されてもよい。次いで、データは、ステップ３６１６において所定数のシェアに分割されてもよい。総数よりも少ないシェアからのデータの再生を可能にするために、耐故障スキームがステップ３６１７において使用されてもよい。いったんシェアが作成されると、認証／完全性情報がステップ３６１８においてシェアに埋め込まれる。次いで、各シェアは、任意に、ステップ３６１９において事後暗号化されてもよい。

【０３８２】

４）３６１２、３６１４、３６１５、３６１６、３６１７、３６１８、３６１９

いくつかの実施形態では、データは、所定数のシェアに分割されてもよい。分割アルゴリズムが鍵を必要とする場合、暗号で確実な擬似乱数発生器を使用した、分割暗号化鍵の生成が、ステップ３６１２において発生してもよい。分割鍵は、任意に、ステップ３６１５において耐故障性を伴う所定数のシェアに鍵分割される前に、Ａｌｌ　ｏｒ　Ｎｏｔｈｉｎｇ　Ｔｒａｎｓｆｏｒｍ（ＡｏＮＴ）を使用して、ステップ３６１４で変換分割鍵に変換されてもよい。次いで、データは、ステップ３６１６において分割されてもよい。総数よりも少ないシェアからのデータの再生を可能にするために、耐故障スキームがステップ３６１７において使用されてもよい。いったんシェアが作成されると、認証／完全性情報がステップ３６１８においてシェアに埋め込まれてもよい。各シェアは、任意に、ステップ３６１９において事後暗号化されてもよい。

【０３８３】

オプションの上記の４つの組み合わせが、好ましくは本発明のいくつかの実施形態で使用されるが、特徴、ステップ、またはオプションの任意の他の好適な組み合わせが、他の実施形態で確実なデータパーサとともに使用されてもよい。

【０３８４】

確実なデータパーサは、物理的な分離を促進することによって、融通性のあるデータ保

護を提供してもよい。データは、最初に暗号化され、次いで、「ｎ分のｍ」耐故障性を伴うシェアに分割されてもよい。これは、総数よりも少ないシェアが利用可能であるときに元の情報の再生を可能にする。例えば、いくつかのシェアが、伝送中に損失または破損される場合がある。損失または破損したシェアは、以下でより詳細に論議されるように、シェアに付加された耐故障性または完全性情報から再作成されてもよい。

【０３８５】

シェアを作成するために、いくつかの鍵が、任意に、確実なデータパーサによって利用される。これらの鍵は、以下のうちの１つ以上を含んでもよい。

【０３８６】

事前暗号化鍵：シェアの事前暗号化が選択されると、外部鍵が確実なデータパーサに渡されてもよい。この鍵は、生成されて外部から鍵記憶（または他の場所）に記憶されてもよく、任意に、データ分割前にデータを暗号化するために使用されてもよい。

【０３８７】

分割暗号化鍵：この鍵は、内部で生成され、分割前にデータを暗号化するために確実なデータパーサによって使用されてもよい。次いで、この鍵は、鍵分割アルゴリズムを使用して、シェア内で確実に記憶されてもよい。

【０３８８】

分割セッション鍵：この鍵は、暗号化アルゴリズムとともに使用されない。むしろ、無作為分割が選択されたときに、データ区分化アルゴリズムに入力するために使用されてもよい。無作為分割が使用されるときに、分割セッション鍵が内部で生成され、データをシェアに区分化するために確実なデータパーサによって使用されてもよい。この鍵は、鍵分割アルゴリズムを使用して、シェア界で確実に記憶されてもよい。

【０３８９】

事後暗号化鍵：シェアの事後暗号化が選択されると、外部鍵が確実なデータパーサに渡され、個別シェアを事後暗号化するために使用されてもよい。この鍵は、生成され、外部から鍵記憶または他の好適な場所に記憶されてもよい。

【０３９０】

いくつかの実施形態では、このようにして、確実なデータパーサを使用してデータが確保されると、必要なシェアおよび外部暗号化鍵の全てが存在するならば、情報が再構築されるのみであってもよい。

【０３９１】

図３７は、いくつかの実施形態で本発明の確実なデータパーサを使用するための例示的な概観プロセス３７００を示す。上記で説明されるように、確実なデータパーサ３７０６の２つのよく適した機能は、暗号化３７０２およびバックアップ３７０４を含む。そのようなものとして、確実なデータパーサ３７０６は、いくつかの実施形態では、ＲＡＩＤまたはバックアップシステム、あるいはハードウェアまたはソフトウェア暗号化エンジンと一体化してもよい。

【０３９２】

確実なデータパーサ３７０６と関連付けられる主要な鍵プロセスは、事前暗号化プロセス３７０８、暗号化／変換プロセス３７１０、鍵確保プロセス３７１２、解析／分配プロセス３７１４、耐故障性プロセス３７１６、共有認証プロセス３７１６、および事後暗号化プロセス３７２０のうちの１つ以上を含んでもよい。これらのプロセスは、図３６で詳述されるように、いくつかの好適な順番または組み合わせで実行されてもよい。使用されるプロセスの組み合わせおよび順番は、特定の用途または使用、所望されるセキュリティのレベル、随意的な事後暗号化、事後暗号化、または両方が所望されるかどうか、所望される冗長性、基礎または統合システムの能力または性能、あるいは任意の他の好適な因子または因子の組み合わせに依存してもよい。

【０３９３】

例示的プロセス３７００の出力は、２つ以上のシェア３７２２であってもよい。上記で説明されるように、いくつかの実施形態では、データは、無作為に（または擬似無作為に

）これらのシェアのそれぞれに分配されてもよい。他の実施形態では、決定論アルゴリズム（または無作為、擬似無作為、および決定論アルゴリズムの何らかの好適な組み合わせ）が使用されてもよい。

【０３９４】

情報資産の個別保護に加えて、時には、関心のユーザまたはコミュニティの異なるグループ間で情報を共有する要件がある。次いで、そのユーザのグループ内の個別シェアへのアクセスを制御すること、またはグループのメンバーがシェアを再構築することのみを可能にする信任状を、これらのユーザ間で共有することが必要であってもよい。この目的を達成するために、本発明のいくつかの実施形態では、ワークグループ鍵がグループメンバーに配備されてもよい。ワークグループ鍵のセキュリティ侵害が、グループ外部の者が情報にアクセスすることを潜在的に可能にする場合があるため、ワークグループ鍵は保護され、内密にされるべきである。ワークグループ鍵の配備および保護のためのいくつかのシステムおよび方法を以下で論議する。

【０３９５】

ワークグループ鍵概念は、シェア内に記憶された鍵情報を暗号化することによって、情報資産の強化された保護を可能にする。いったんこの動作が行われると、たとえ全ての必要なシェアおよび外部鍵が発見されたとしても、ワークグループ鍵にアクセスすることなく、攻撃者が情報を再作成する望みはない。

【０３９６】

図３８は、シェア内で鍵およびデータ構成要素を記憶するための例示的なブロック図３８００を示す。略図３８００の実施例では、随意的な事前暗号化および事後暗号化ステップが省略されるが、これらのステップは他の実施形態に含まれてもよい。

【０３９７】

データを分割するための簡略化したプロセスは、暗号化段階３８０２において暗号化鍵３８０４を使用してデータを暗号化することを含む。次いで、暗号化鍵３８０４の複数部分が、本発明に従って分割され、シェア３８１０内において記憶されてもよい。分割暗号化鍵３８０６の複数部分もまた、シェア３８１０内において記憶されてもよい。次いで、分割暗号化鍵を使用して、データ３８０８が分割され、シェア３８１０に記憶される。

【０３９８】

データを修復するために、分割暗号化鍵３８０６が、本発明に従って回収され、修復されてもよい。次いで、分割動作は、暗号文を修復するように逆転されてもよい。暗号化鍵３８０４も回収および修復されてもよく、次いで、暗号化鍵を使用して、暗号文が復号されてもよい。

【０３９９】

ワークグループ鍵が利用されるときに、上記のプロセスは、ワークグループ鍵で暗号化鍵を保護するように、わずかに変更されてもよい。次いで、暗号化鍵は、シェア内に記憶される前にワークグループ鍵で暗号化されてもよい。修正されたステップが、図３９の例示的なブロック図３９００に示されている。

【０４００】

ワークグループ鍵を使用してデータを分割するための簡略化したプロセスは、段階３９０２において暗号化鍵を使用して最初にデータを暗号化することを含む。次いで、暗号化鍵は、段階３９０４においてワークグループ鍵で暗号化されてもよい。次いで、ワークグループ鍵で暗号化された暗号化鍵は、複数部分に分割され、シェア３９１２において記憶されてもよい。分割鍵３９０８もまた、分割され、シェア３９１２に記憶されてもよい。最終的に、分割鍵３９０８を使用して、データ部分３９１０が分割され、シェア３９１２に記憶される。

【０４０１】

データを修復するために、分割鍵が、本発明に従って回収され、修復されてもよい。次いで、分割動作は、本発明に従って、暗号文を修復するように逆転されてもよい。（ワークグループ鍵で暗号化された）暗号化鍵が回収および修復されてもよい。次いで、ワーク

グループ鍵を使用して、暗号化鍵が復号されてもよい。最終的に、暗号化鍵を使用して、暗号文が復号されてもよい。

【０４０２】

ワークグループ鍵を配備し、保護するためのいくつかの確実な方法がある。特定の用途にどの方法を使用するかという選択は、いくつかの因子に依存する。これらの因子は、必要とされるセキュリティレベル、費用、利便性、およびワークグループの中のユーザの数を含んでもよい。いくつかの実施形態で使用される、いくつかの一般的に使用されている技法を以下に規定する。

【０４０３】

（ハードウェアベースの鍵記憶）

ハードウェアベースのソリューションは、概して、暗号化システムにおける暗号化／復号鍵のセキュリティの最強の保証を提供する。ハードウェアベースの鍵記憶ソリューションの実施例は、携帯用デバイス（例えば、スマートカード／ドングル）または非携帯用鍵記憶周辺機器に鍵を記憶する、改ざん防止鍵トークンデバイスを含む。これらのデバイスは、未承認の当事者による鍵材料の容易な複製を防止するように設計されている。鍵は、信頼できる機関によって生成されてユーザに分配されてもよく、またはハードウェア内で生成されてもよい。加えて、多くの鍵記憶システムは、鍵の使用が物理的オブジェクト（トークン）およびパスフレーズまたは生体測定の両方へのアクセスを必要とする、多因子認証を提供する。

【０４０４】

（ソフトウェアベースの鍵記憶）

専用ハードウェアベースの記憶が、高セキュリティ配備または用途に望ましくてもよい一方で、他の配備は、ローカルハードウェア（例えば、ディスク、ＲＡＭ、またはＵＳＢドライブ等の不揮発性ＲＡＭ記憶）の上に直接鍵を記憶することを選択してもよい。これは、内部攻撃者に対して、または攻撃者が暗号化マシンに直接アクセスすることができるインスタンスにおいて、より低いレベルの保護を提供する。

【０４０５】

ディスク上で鍵を確保するために、ソフトウェアベースの鍵管理はしばしば、パスワードおよびパスフレーズ、（例えば、ハードウェアベースのソリューションからの）他の鍵の存在、生体測定、または前述の内容の任意の好適な組み合わせを含む、他の認証測定基準の組み合わせから導出される鍵の下で、暗号化された形態で鍵を記憶することによって鍵を保護する。そのような技法によって提供されるセキュリティのレベルは、いくつかのオペレーティングシステム（例えば、ＭＳ　Ｗｉｎｄｏｗｓ（登録商標）およびＬｉｎｕｘ（登録商標））によって提供される比較的弱い鍵保護機構から、多因子認証を使用して実装されるよりロバストなソリューションまで及んでもよい。

【０４０６】

本発明の確実なデータパーサは、いくつかの用途および技術で有利に使用されてもよい。例えば、Ｅメールシステム、ＲＡＩＤシステム、ビデオ放送システム、データベースシステム、テープバックアップシステム、または任意の他の好適なシステムは、任意の好適なレベルで統合された確実なデータパーサを有してもよい。以前に論議されたように、確実なデータパーサはまた、例えば、有線、無線、または物理的媒体を含む任意の輸送媒体を介して、進行中の任意の種類のデータの保護および耐故障性のために統合されてもよいことが理解されるであろう。一実施例として、ボイスオーバーインターネットプロトコル（ＶｏＩＰ）アプリケーションが、ＶｏＩＰで一般的に見られる反響および遅延に関する問題を解決するために、本発明の確実なデータパーサを利用してもよい。ドロップされたパケットへのネットワーク再試行の必要性は、所定数のシェアの損失さえ伴ってパケット送達を保証する、耐故障性を使用することによって排除されてもよい。データのパケット（例えば、ネットワークパケット）はまた、最小限の遅延およびバッファリングを伴って、効率的に分割され、「オンザフライで」修復されてもよく、進行中の種々の種類のデータに対する包括的ソリューションをもたらす。確実なデータパーサは、ネットワークデー

タパケット、ネットワークボイスパケット、ファイルシステムデータブロック、または情報の任意の他の好適な単位に作用してもよい。ＶｏＩＰアプリケーションと一体化することに加えて、確実なデータパーサは、ファイル共有アプリケーション（例えば、ピアツーピアファイル共有アプリケーション）、ビデオ放送アプリケーション、電子投票またはポーリングアプリケーション（Ｓｅｎｓｕｓプロトコル等の電子投票プロトコルおよびブラインド署名を実装してもよい）、Ｅメールアプリケーション、あるいは確実な通信を要求または所望してもよい任意の他のネットワークアプリケーションと一体化してもよい。

【０４０７】

いくつかの実施形態では、進行中のネットワークデータに対する支援は、ヘッダ生成段階およびデータ区分化段階といった、２つの明確に異なる段階で、本発明の確実なデータパーサによって提供されてもよい。簡略化したヘッダ生成プロセス４０００および簡略化したデータ区分化プロセス４０１０が、それぞれ、図４０Ａおよび４０Ｂに示されている。これらのプロセスの一方または両方は、ネットワークパケット、ファイルシステムブロック、または任意の他の好適な情報に行われてもよい。

【０４０８】

いくつかの実施形態では、ヘッダ生成プロセス４０００は、ネットワークパケットストリームの開始時に１回行われてもよい。ステップ４００２では、無作為（または擬似無作為）な分割暗号化鍵Ｋが生成されてもよい。次いで、分割暗号化鍵Ｋは、任意に、ＡＥＳ鍵ラップステップ４００４において（例えば、上記で説明されるワークグループ鍵を使用して）暗号化されてもよい。ＡＥＳ鍵ラップがいくつかの実施形態で使用されてもよいが、任意の好適な鍵暗号化または鍵ラップアルゴリズムが他の実施形態で使用されてもよい。ＡＥＳ鍵ラップステップ４００４は、分割暗号化鍵Ｋ全体に作用してもよく、または分割暗号化鍵は、いくつかのブロック（例えば、６４ビットブロック）に解析されてもよい。次いで、ＡＥＳ鍵ラップステップ４００４は、所望であれば、分割暗号化鍵のブロックに作用してもよい。

【０４０９】

ステップ４００６においては、分割暗号化鍵Ｋを鍵シェアに分割するために、秘密共有アルゴリズム（例えば、Ｓｈａｍｉｒ）が使用されてもよい。次いで、各鍵シェアは、（例えば、シェアヘッダの中の）出力シェアのうちの１つに埋め込まれてもよい。最終的に、シェア完全性ブロックおよび（任意に）事後認証タグ（例えば、ＭＡＣ）が、各シェアのヘッダブロックに付加されてもよい。各ヘッダブロックは、単一のデータパケット内に嵌合するように設計されてもよい。

【０４１０】

（例えば、簡略化したヘッダ生成プロセス４０００を使用して）ヘッダ生成が完了した後に、確実なデータパーサは、簡略化したデータ分割プロセス４０１０を使用して、データ区分化段階に入ってもよい。ストリームの中の各着信データパケットまたはデータブロックは、ステップ４０１２において分割暗号化鍵Ｋを使用して暗号化される。ステップ４０１４においては、シェア完全性情報（例えば、ハッシュＨ）が、ステップ４０１２からの結果として生じる暗号文で計算されてもよい。例えば、ＳＨＡ－２５６ハッシュが計算されてもよい。ステップ４１０６においては、次いで、データパケットまたはデータブロックが、本発明に従って上記で説明されるデータ分割アルゴリズムのうちの１つを使用して、２つ以上のデータシェアに区分化されてもよい。いくつかの実施形態では、データパケットまたはデータブロックは、各データシェアが暗号化されたデータパケットまたはデータブロックの実質的に無作為な分配を含有するように、分割されてもよい。次いで、完全性情報（例えば、ハッシュＨ）は、各データシェアに付加されてもよい。いくつかの実施形態では、随意的な事後認証タグ（例えば、ＭＡＣ）も計算され、各データシェアに付加されてもよい。

【０４１１】

各データシェアは、データブロックまたはデータパケットの正しい再構成を許可するために必要であってもよいメタデータを含んでもよい。この情報は、シェアヘッダに含まれ

てもよい。メタデータは、暗号鍵シェア、鍵同一性、シェアノンス、署名／ＭＡＣ値、および完全性ブロック等の情報を含んでもよい。帯域幅の効率性を最大化するために、メタデータはコンパクトバイナリ形式で記憶されてもよい。

【０４１２】

例えば、いくつかの実施形態では、シェアヘッダは、暗号化されず、Ｓｈａｍｉｒ鍵シェア、セッションごとのノンス、シェアごとのノンス、鍵識別子（例えば、ワークグループ鍵識別子および事後承認鍵識別子）等の要素を含んでもよい、平文ヘッダチャンクを含む。シェアヘッダはまた、分割暗号化鍵で暗号化される、暗号化されたヘッダチャンクを含んでもよい。任意の数の以前のブロック（例えば、以前の２つのブロック）の完全性チェックを含んでもよい完全性ヘッダチャンクも、ヘッダに含まれてもよい。任意の他の好適な値または情報も、シェアヘッダに含まれてもよい。

【０４１３】

図４１の例示的なシェア形式４１００で示されるように、ヘッダブロック４１０２は、２つ以上の出力ブロック４１０４と関連付けられてもよい。ヘッダブロック４１０２等の各ヘッダブロックは、単一のネットワークデータパケット内に嵌合するように設計されてもよい。いくつかの実施形態では、ヘッダブロック４１０２が第１の場所から第２の場所へ伝送された後に、次いで、出力ブロックが伝送されてもよい。代替として、ヘッダブロック４１０２および出力ブロック４１０４が、同時に並行して伝送されてもよい。伝送は、１つ以上の同様または異種の通信経路上で発生してもよい。

【０４１４】

各出力ブロックは、データ部分４１０６および完全性／真正性部分４１０８を含んでもよい。上記で説明されるように、各データシェアは、暗号化された事前区分化データのシェア完全性情報（例えば、ＳＨＡ－２５６ハッシュ）を含む、シェア完全性部分を使用して確保されてもよい。復旧時間における出力ブロックの完全性を検証するために、確実なデータパーサは、各シェアのシェア完全性ブロックを比較し、次いで、分割アルゴリズムを反転させてもよい。次いで、復旧したデータのハッシュは、シェアハッシュに対して検証されてもよい。

【０４１５】

前述のように、本発明のいくつかの実施形態では、確実なデータパーサは、テープバックアップシステムと併せて使用されてもよい。例えば、個別テープが、本発明に従って、ノード（すなわち、部分／シェア）として使用されてもよい。任意の他の好適な配設が使用されてもよい。例えば、２つ以上のテープで構成されている、テープライブラリまたはサブシステムが、単一のノードとして取り扱われてもよい。

【０４１６】

冗長性も、本発明に従ってテープとともに使用されてもよい。例えば、データセットが４つのテープ（すなわち、部分／シェア）の間で割り振られる場合には、４つのテープのうちの２つが元のデータを修復するために必要であってもよい。本発明の冗長性特徴に従って元のデータを修復するために、任意の好適な数のノード（すなわち、総数よりも少ないノード）が必要とされてもよいことが理解されるであろう。これは、１つ以上のテープが満了したときに修復の確率を大幅に増加させる。

【０４１７】

各テープはまた、改ざんに対して保険をかけるように、ＳＨＡ－２５６、ＨＭＡＣハッシュ値、任意の他の好適な値、またはそれらの任意の組み合わせを用いてデジタルで保護されてもよい。テープ上の任意のデータまたはハッシュ値が変化した場合、そのテープは、修復の候補にはならず、データを修復するために、残りのテープのうちの任意の最小必要数のテープが使用される。

【０４１８】

従来のテープバックアップシステムでは、ユーザが、テープに書き込まれるか、またはテープから読み出されるデータを呼び出すと、テープ管理システム（ＴＭＳ）は、物理的テープ量に対応する数を提示する。このテープ量は、データが載置される物理的ドライブ

を指し示す。テープは、人間のテープ操作者によって、またはテープサイロの中のテープロボットによってロードされる。

【０４１９】

本発明の下で、物理的テープ量は、いくつかの物理的テープを指し示す、論理的マウントポイントと見なされてもよい。これは、データ容量を増加させるだけでなく、並列性により性能も向上させる。

【０４２０】

増大した性能のために、テープノードは、テープイメージを記憶するために使用されるディスクのＲＡＩＤアレイであってもよく、またはそれを含んでもよい。これは、データが保護されたＲＡＩＤにおいて常に利用可能であってもよいため、高速修復を可能にする。

【０４２１】

前述の実施形態のうちのいずれかでは、保護されるデータは、決定論的、確率論的、または決定論的と確率論的との両方のデータ分配技法を使用して、複数のシェアに分配されてもよい。攻撃者が任意の暗号ブロックへの秘密攻撃を開始することを防止するために、暗号ブロックからのビットは、決定論的にシェアに分配されてもよい。例えば、分配は、ＢｉｔＳｅｇｍｅｎｔルーチンを使用して行われてもよく、または複数のシェアへのブロック部分の分配を可能にするようにＢｌｏｃｋＳｅｇｍｅｎｔルーチンが修正されてもよい。この方策は、「Ｍ」個よりも少ないシェアを蓄積した攻撃者に対して防衛してもよい。

【０４２２】

いくつかの実施形態では、鍵のある情報分散を使用して（例えば、鍵のある情報分散アルゴリズムまたは「ＩＤＡ」を介して）、鍵のある秘密共有ルーチンが採用されてもよい。鍵のあるＩＤＡ用の鍵はまた、１つ以上の外部ワークグループ鍵、１つ以上の共有鍵、またはワークグループ鍵および共有鍵の任意の組み合わせによって保護されてもよい。このようにして、多因子秘密共有スキームが採用されてもよい。データを再構成するために、いくつかの実施形態では、少なくとも「Ｍ」個のシェアならびにワークグループ鍵（および／または共有鍵）が必要とされてもよい。ＩＤＡ（またはＩＤＡ用の鍵）はまた、暗号化プロセスに組み入れられてもよい。例えば、（例えば、暗号化する前の事前処理層中に）変換が平文に組み入れられてもよく、さらに、暗号化される前に平文を保護してもよい。

【０４２３】

例えば、いくつかの実施形態では、データセットからのデータの一意の部分を２つ以上のシェアの中へ分配するために、鍵のある情報分散が使用される。鍵のある情報分散は、最初にデータセットを暗号化して、データセットからの暗号化されたデータの一意の部分を２つ以上の暗号化されたデータセットシェアの中へ分配するために、またはデータセットを暗号化するとともに、データセットからの暗号化されたデータの一意の部分を２つ以上の暗号化されたデータセットシェアの中へ分配するために、セッション鍵を使用してもよい。例えば、データセットまたは暗号化されたデータセットの一意の部分を分配するために、秘密共有（または、ＢｉｔＳｅｇｍｅｎｔもしくはＢｌｏｃｋＳｅｇｍｅｎｔ等の上記で説明される方法）が使用されてもよい。次いで、セッション鍵は、任意に、（例えば、フルパッケージ変換またはＡｏＮＴ）を使用して変換され、例えば、秘密共有（または鍵のある情報分散およびセッション鍵）を使用して共有されてもよい。

【０４２４】

いくつかの実施形態では、鍵の一意の部分が２つ以上のセッション鍵シェアの中へ分配または共有される前に、共有鍵（例えば、ワークグループ鍵）を使用してセッション鍵が暗号化されてもよい。次いで、２つ以上のユーザシェアが、少なくとも１つの暗号化されたデータセットシェアおよび少なくとも１つのセッション鍵シェアを組み合わせることによって形成されてもよい。ユーザシェアを形成する際に、いくつかの実施形態では、少なくとも１つのセッション鍵シェアが、暗号化されたデータセットシェアの中へ交互配置さ

れてもよい。他の実施形態では、少なくとも部分的に共有ワークグループ鍵に基づく場所において、少なくとも１つのセッション鍵シェアが、暗号化されたセータセットシェアに挿入されてもよい。例えば、各セッション鍵シェアを一意の暗号化されたデータセットシェアの中へ分配してユーザシェアを形成するために、鍵のある情報分散が使用されてもよい。少なくとも部分的に共有ワークグループ鍵に基づく場所において、セッション鍵シェアを、暗号化されたセータセットシェアの中へ交互配置または挿入することは、暗号攻撃に直面して増大したセキュリティを提供してもよい。他の実施形態では、ユーザシェアを形成するように、１つ以上のセッション鍵シェアが暗号化されたデータセットの初めまたは終わりに付加されてもよい。次いで、ユーザシェアの集合が、少なくとも１つのデータ保管場所上で別々に記憶されてもよい。１つまたは複数のデータ保管場所は、（例えば、同じ磁気またはテープ記憶デバイス上の）同じ物理的な場所に位置するか、または（例えば、異なる地理的な場所の物理的に分離されたサーバ上で）地理的に分離されてもよい。元のデータセットを再構成するために、承認された一式のユーザシェアおよび共有ワークグループ鍵が要求されてもよい。

【０４２５】

鍵のある情報分散は、鍵回収オラクルに直面しても確実であってもよい。例えば、ブロック暗号Ｅと、ブロック暗号への入出力ペアのリスト（X_1，Y_1）、．．．、（X_c，Y_c）を得るＥの鍵回収オラクルとを取り込み、入出力例（例えば、全てのｉについて$Y_i = E_K(X_i)$）と一致する鍵Ｋを返信する。オラクルは、一致する鍵がなければ区別された値⊥を返信してもよい。このオラクルは、入出力例のリストから鍵を復元し得る暗号解読攻撃をモデル化してもよい。

【０４２６】

標準ブロック暗号ベースのスキームは、鍵回収オラクルの存在下で失敗する場合がある。例えば、ＣＢＣ暗号化またはＣＢＣ　ＭＡＣは、鍵回収オラクルの存在下で完全に不確実になる場合がある。

【０４２７】

Π^{IDA}がＩＤＡスキームであり、Π^{Enc}が何らかのブロック暗号Ｅの動作モードによって与えられる暗号化スキームであるならば、鍵回収攻撃に直面してセキュリティを提供し、２つのスキームが、ＨＫ１またはＨＫ２の通りに恣意的な完全秘密共有スキーム（ＰＳＳ）と組み合わされると、（Π^{IDA}，Π^{Enc}）は、敵が鍵回収オラクルを有するモデルにｋおける以外において、ロバストな計算秘密共有（ＲＣＳＳ）目標を達成する。

【０４２８】

１対のスキームが鍵回収攻撃に直面してセキュリティを提供するように、ＩＤＡスキームΠ^{IDA}および暗号化スキームΠ^{Enc}が存在する場合には、この１対を達成する１つの方法は、「賢明な」ＩＤＡおよび「能力のない」暗号化スキームを有することであってもよい。この１対のスキームを達成する別の方法は、「能力のない」ＩＤＡおよび「賢明な」暗号化スキームを有することであってもよい。

【０４２９】

賢明なＩＤＡおよび能力のない暗号化スキームの使用を例示するために、いくつかの実施形態では、暗号化スキームはＣＢＣであってもよく、ＩＤＡは「弱いプライバシー」所有物を有してもよい。弱いプライバシー所有物とは、例えば、ＩＤＡへの入力がブロック$M = M_1 \ldots M_l$という無作為な順序であり、敵が未承認の集合からシェアを得る場合には、敵がM_iを計算することが実行不可能であるように、何らかのブロック指数ｉがあることを意味する。そのような弱く秘密のＩＤＡは、最初に、ＳｔｉｎｓｏｎのＡｏＮＴ等の情報論理的なＡｏＮＴにＭを適用し、次いで、ＢｌｏｃｋＳｅｇｍｅｎｔ等の単純ＩＤＡまたはＲａｂｉｎのスキーム（例えば、Ｒｅｅｄ－Ｓｏｌｏｍｏｎ符号化）のようなビット効率的ＩＤＡを適用することによって構築されてもよい。

【０４３０】

能力のないＩＤＡおよび賢明な暗号化スキームの使用を例示するために、いくつかの実施形態では、単一暗号化の代わりに二重暗号化によってＣＢＣモードを使用してもよい。

ここで、任意のＩＤＡが、複製でさえ使用されてもよい。敵が単独で暗号化された入出力例を拒否されるので、ブロック暗号に対する鍵回収オラクルを有することは、敵にとって役に立たない。

【０４３１】

賢明なＩＤＡは、値を有するが、鍵回収攻撃に直面してセキュリティを提供するために必要とされる「知能」が他の場所で「押された（ｐｕｓｈｅｄ）」可能性があるという意味で、いくつかの状況では不必要であってもよい。例えば、いくつかの実施形態では、ＩＤＡがどれだけ高性能であろうと、どのような目標がＨＫ１／ＨＫ２との関連でＩＤＡを用いて達成されようとしていても、知能は、ＩＤＡから押されて暗号化スキームに押し込まれてもよく、固定された能力のないＩＤＡとともに残される。

【０４３２】

上記に基づいて、いくつかの実施形態では、「普遍的に健全な」賢明なＩＤＡΠ^{IDA}が使用されてもよい。例えば、全ての暗号化スキームΠ^{Enc}について、１対（Π^{IDA}，Π^{Enc}）が鍵回収攻撃に直面してセキュリティを提供するように、ＩＤＡが提供される。

【０４３３】

いくつかの実施形態では、鍵回収オラクルに直面してＲＣＳＳにより確実である暗号化スキームが提供される。スキームは、鍵回収に直面してセキュリティを達成するように、ＩＤＡを伴ってＨＫ１／ＨＫ２と一体化されてもよい。新しいスキームを使用することは、例えば、鍵回収攻撃に対して対称暗号化スキームをより確実にするために、特に有用であってもよい。

【０４３４】

上述のように、古典的な秘密共有概念は、一般的には鍵がない。したがって、任意の種類の対称または非対称鍵を保持するために、秘密を再構成するディーラも当事者も必要としない態様で、秘密がシェアに細分化されるか、またはシェアから再構成される。しかしながら、本明細書で説明される確実なデータパーサは、任意に、鍵付きである。ディーラは、データ共有に使用される場合、データ復旧に必要であってもよい対称鍵を提供してもよい。確実なデータパーサは、確保されるメッセージの一意の部分を２つ以上のシェアに分散または分配するために、対称鍵を使用してもよい。

【０４３５】

共有鍵は、多因子または２因子秘密共有（２ＦＳＳ）を有効にしてもよい。次いで、敵は、セキュリティ機構を破壊するために、２つの基本的に異なる種類のセキュリティを介してナビゲートするように要求されてもよい。例えば、秘密共有目標に違反するために、敵は、（１）承認されたプレーヤのセットのシェアを取得する必要があってもよく、（２）取得することが可能であるべきではない秘密鍵を取得する（またはその鍵によって入力される暗号機構を破壊する）必要があってもよい。

【０４３６】

いくつかの実施形態では、付加的な要件の新たなセットがＲＣＳＳ目標に追加される。付加的な要件は、「第２の因子」である鍵所有を含んでもよい。これらの付加的な要件は、要件の元のセットを軽減することなく追加されてもよい。要件のセットは、秘密鍵を知っているが、十分なシェアを取得しない場合に、敵がスキームを破壊できないことに関してもよい（例えば、古典的な、または第１因子要件）一方で、他方の要件のセットは、秘密鍵を持たないが、何とかシェアの全てを入手する場合に、敵がスキームを破壊できないことに関してもよい（例えば、新しい、または第２因子要件）。

【０４３７】

いくつかの実施形態では、プライバシー要件および真正性要件といった、２つの第２因子要件があってもよい。プライバシー要件では、秘密鍵Ｋおよびビットｂが環境によって選択される方策が関与してもよい。ここで、敵は、秘密共有スキームのドメインで、M_1^0およびM_1^1といった１対の等長メッセージを供給する。環境は、M_1^bのシェアを計算し、シェアのベクトルS_1＝（S_1［１］，．．．，S_1［ｎ］）を得て、シェアS_1

（それらの全て）を敵に与える。ここで、敵は、別の１対のメッセージ（M_2^0，M_2^1）を選択してもよく、同じ鍵Ｋおよび隠されたビットｂを使用して、全てが以前のように進む。敵の仕事は、ｂであると考えるビットｂ’を出力することである。敵のプライバシー優位は、ｂ＝ｂ’という確率の２倍未満である。この方策は、全てのシェアを習得しても、秘密鍵が欠けていれば、敵が依然として共有秘密について何も習得できないという概念を表している。

【０４３８】

真正性要件では、環境が秘密鍵Ｋを選択し、これを共有（Ｓｈａｒｅ）および復元（Ｒｅｃｏｖｅｒ）への後続の呼出しにおいて使用する方策が関与してもよい。共有および復元は、いくつかの実施形態では、この鍵の存在を反映するように、それらの構文を修正させてもよい。次いで、敵は、秘密共有スキームのドメインで選択する、あらゆるメッセージM_1、．．．、M_qのＳｈａｒｅ要求を行う。各共有要求に応じて、敵は、シェアの対応するｎベクトルS_1、．．．、S_qを得る。敵の目的は、新しい平文を案出することであり、復元アルゴリズムに供給されると、｛M_1，．．．，M_q｝ではないものをもたらすように、シェアのベクトルＳ’を出力した場合に成功する。これは、「平文の完全性」概念である。

【０４３９】

多因子秘密共有を達成するための２つのアプローチがある。第１は、ブラックボックス方法で基礎的な（Ｒ）ＣＳＳスキームを使用するという意味で一般的である、一般的アプローチである。ＣＳＳ共有されるメッセージを暗号化するために、認証暗号化スキームが使用され、次いで、例えば、ＢｌａｋｅｌｙまたはＳｈａｍｉｒ等の秘密共有アルゴリズムを使用して、結果として生じる暗号文が共有されてもよい。

【０４４０】

潜在的により効率的なアプローチは、共有鍵がワークグループ鍵となることを可能にすることである。すなわち、（１）共有鍵を使用して、（Ｒ）ＣＳＳスキームの無作為に生成されたセッション鍵が暗号化されてもよく、（２）メッセージ（例えば、ファイル）に適用される暗号化スキームは、認証暗号化スキームに置換されてもよい。このアプローチは、性能の最小の劣化のみを伴い得る。

【０４４１】

本発明の確実なデータパーサは、クラウドコンピューティングセキュリティソリューションを実装するために使用されてもよい。クラウドコンピューティングは、計算および記憶リソースが、ネットワーク上でコンピュータシステムおよび他のデバイスに提供されてもよい、ネットワークベースの計算、記憶、または両方である。クラウドコンピューティングリソースは、概して、インターネット上でアクセスされるが、クラウドコンピューティングは、任意の好適な公衆またはプライベートネットワーク上で行われてもよい。クラウドコンピューティングは、コンピューティングリソースと基礎的なハードウェア構成要素（例えば、サーバ、記憶デバイス、ネットワーク）との間にあるレベルの抽象化を提供し、コンピューティングリソースのプールへの遠隔アクセスを可能にしてもよい。これらのクラウドコンピューティングリソースは、「クラウド」と集合的に呼ばれてもよい。クラウドコンピューティングは、インターネットまたは任意の他の好適なネットワークあるいはネットワークの組み合わせ上のサービスとして、動的に拡張可能であり、しばしば可視化されたリソースを提供するために使用されてもよい。

【０４４２】

秘密データが公衆ネットワーク上で転送される場合があり、公的にアクセス可能または共有システム内で処理および記憶される場合があるので、セキュリティはクラウドコンピューティングに対する重要な懸念である。確実なデータパーサは、クラウドコンピューティングリソース、およびクラウドとエンドユーザまたはデバイスとの間で伝達されているデータを保護するために使用されてもよい。例えば、確実なデータパーサは、クラウドの中のデータ記憶、クラウドの中の進行中データ、クラウドの中のネットワークアクセス、クラウドの中のデータサービス、クラウドの中の高性能コンピューティングリソースへの

アクセス、およびクラウドの中の任意の他の動作を確保するために使用されてもよい。

【０４４３】

図４２は、クラウドコンピューティングセキュリティソリューションの例示的なブロック図である。確実なデータパーサ４２１０を含むシステム４２００は、クラウドリソース４２６０を含むクラウド４２５０に連結される。システム４２００は、コンピュータ端末、パーソナルコンピュータ、手持ち式デバイス（例えば、ＰＤＡ、Ｂｌａｃｋｂｅｒｒｙ、スマートフォン、タブレットデバイス）、携帯電話、コンピュータネットワーク、任意の他の好適なハードウェア、またはそれらの任意の組み合わせ等の任意の好適なハードウェアを含んでもよい。確実なデータパーサ４２１０は、システム４２００の任意の好適なレベルで統合されてもよい。例えば、確実なデータパーサ４２１０の存在が、システム４２００のエンドユーザには実質的に見えなくてもよいように、確実なデータパーサ４２１０は、十分にバックエンドレベルでシステム４２００のハードウェアおよび／またはソフトウェアに組み込まれてもよい。好適なシステム内における確実なデータパーサの統合は、例えば、図２７および２８に関して上記でより詳細に説明される。クラウド４２５０は、データ記憶リソース４２６０ａおよび４２６０ｅ、データサービスリソース４２６０ｂおよび４２６０ｇ、ネットワークアクセス制御リソース４２６０ｃおよび４２６０ｈ、ならびに高性能コンピューティングリソース４２６０ｄおよび４２６０ｆを含む、複数の例示的クラウドリソース４２６０を含む。これらのリソースのそれぞれは、図４３－４７に関して以下でより詳細に説明される。これらのクラウドコンピューティングリソースは例示的であるにすぎない。任意の好適な数および種類のクラウドコンピューティングリソースがシステム４２００からアクセス可能であってもよいことを理解されたい。

【０４４４】

クラウドコンピューティングの１つの利点としては、システム４２００のユーザが、専用コンピュータハードウェアに投資する必要がなく、複数のクラウドコンピューティングリソースにアクセスすることが可能であり得る。ユーザは、システム４２００にアクセス可能なクラウドコンピューティングリソースの数および種類を動的に制御する能力を有してもよい。例えば、システム４２００には、現在の必要性に基づいて動的に調整可能である能力を有する、クラウドの中のオンデマンド記憶リソースが提供されてもよい。いくつかの実施形態では、システム４２００上で実行される１つ以上のソフトウェアアプリケーションは、システム４２００をクラウドリソース４２６０に連結してもよい。例えば、インターネット上でシステム４２００を１つ以上のクラウドリソース４２６０に連結するために、インターネットウェブブラウザが使用されてもよい。いくつかの実施形態では、システム４２００と一体化または接続されたハードウェアが、システム４２００をクラウドリソース４２６０に連結してもよい。両方の実施形態では、確実なデータパーサ４２１０は、クラウドリソース４２６０および／またはクラウドリソース４２６０内に記憶されたデータとの通信を確保してもよい。システム４２００へのクラウドリソース４２６０の連結は、クラウドリソース４２６０がシステム４２００にとってローカルハードウェアリソースのように見えるように、システム４２００またはシステム４２００のユーザには見えなくてもよい。さらに、共有クラウドリソース４２６０は、システム４２００にとって専用ハードウェアリソースのように見えてもよい。

【０４４５】

確実なデータパーサ４２１０は、データを暗号化し、分割することにより、いかなる法医学的に識別可能なデータもクラウドを通り抜けないか、またはクラウド内に記憶されないようにし得る。クラウドの基礎的なハードウェア構成要素（例えば、サーバ、記憶デバイス、ネットワーク）は、電力網故障、天気事象、または他の人為的あるいは自然事象の場合に、クラウドリソースの連続性を確保するように地理的に分配されてもよい。結果として、たとえクラウド内のハードウェア構成要素のうちのいくつかが突発故障を被ったとしても、クラウドリソースは依然としてアクセス可能であり得る。クラウドリソース４２６０は、１つ以上のハードウェア故障にもかかわらず、途切れないサービスを提供するように冗長性を伴って設計され得る。

【０４４６】
図４３は、クラウドを介して進行中の（すなわち、１つの場所から別の場所へのデータの転送中の）データを確保するためのクラウドコンピューティングセキュリティソリューションの例示的ブロック図である。図４３は、コンピュータ端末、パーソナルコンピュータ、手持ち式デバイス（例えば、ＰＤＡ、Ｂｌａｃｋｂｅｒｒｙ）、携帯電話、コンピュータネットワーク、任意の他の好適なハードウェア、またはそれらの任意の組み合わせ等の任意の好適なハードウェアを含んでもよい送信者システム４３００を示す。送信者システム４３００は、例えば、Ｅメールメッセージ、バイナリデータファイル（例えば、グラフィック、音声、ビデオ等）、または両方であってもよいデータを生成および／または記憶するために使用される。データは、本発明に従って確実なデータパーサ４３１０によって解析および分割される。結果として生じたデータ部分は、クラウド４３５０上で受信者システム４３７０に伝達されてもよい。受信者システム４３７０は、送信者システム４３００に関して上記で説明されるような任意の好適なハードウェアであってもよい。別個のデータ部分は、本発明に従って、元のデータを生成するように受信者システム４３７０において再結合されてもよい。クラウド４３１０を通って進行するときに、データ部分は、インターネット、および／または１つ以上のイントラネット、ＬＡＮ、ＷｉＦｉ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、任意の他の好適な配線接続あるいは無線通信ネットワーク、またはそれらの任意の組み合わせを含む、１つ以上の通信経路にわたって伝達されてもよい。図２８および２９に関して上記で説明されるように、元のデータは、たとえデータ部分のうちのいくつかが損なわれたとしても、確実なデータパーサによって確保される。
【０４４７】
図４４は、クラウド内でデータサービスを確保するためのクラウドコンピューティングセキュリティソリューションの例示的ブロック図である。この実施形態では、ユーザ４４００は、クラウド４４３０上でデータサービス４４２０をエンドユーザ４４４０に提供してもよい。確実なパーサ４４１０は、開示された実施形態に従ってデータサービスを確保してもよい。データサービス４４２０は、クラウド４４３０上でアクセス可能である任意の好適なアプリケーションまたはソフトウェアサービスであってもよい。例えば、データサービス４４２０は、サービス指向アーキテクチャ（ＳＯＡ）システムの一部として実装されるウェブベースのアプリケーションであってもよい。データサービス４４２０は、クラウド４４３０内の１つ以上のシステム上で記憶され、実行されてもよい。このクラウドコンピューティング実装によって提供される抽象化は、基礎的なハードウェアリソースに関係なく、データサービス４４２０がエンドユーザ４４４０にとって可視化されたリソースのように見えることを可能にする。確実なパーサ４４１０は、データサービス４４２０とエンドユーザ４４４０との間で進行中のデータを確保してもよい。確実なパーサ４４１０はまた、データサービス４４２０と関連付けられる記憶されたデータを確保してもよい。データサービス４４２０と関連付けられる記憶されたデータは、データサービス４４２０を実装する１つまたは複数のシステム内で、および／または別個の確実なクラウドデータ記憶デバイス内で確保されてもよく、これを以下でより詳細に説明する。データサービス４４２０および図４４の他の部分は、クラウド４４３０の外部に示されているが、これらの要素のうちのいずれかがクラウド４４３０内に組み込まれてもよいことを理解されたい。
【０４４８】
図４５は、クラウド内でデータ記憶リソースを確保するためのクラウドコンピューティングセキュリティソリューションの例示的ブロック図である。確実なデータパーサ４５１０を含むシステム４５００は、データ記憶リソース４５６０を含むクラウド４５５０に連結される。確実なデータパーサ４５１０は、１つ以上のデータ記憶リソース４５６０の間でデータを解析および分割するために使用されてもよい。各データ記憶リソース４５６０は、１つ以上のネットワーク接続された記憶デバイスを表してもよい。これらの記憶デバイスは、単一のユーザ／システムに割り当てられてもよく、または複数のユーザ／システムによって共有されてもよい。確実なデータパーサ４５１０によって提供されるセキュリ

ティは、複数のユーザ／システムからのデータが、同じの記憶デバイス上で確実に共存することを可能にしてもよい。このクラウドコンピューティング実装によって提供される抽象化は、基礎的なデータ記憶リソースの数および場所に関係なく、データ記憶リソース４５６０がシステム４５００にとって単一の可視化された記憶リソースのように見えることを可能にする。データがデータ記憶リソース４５６０に書き込まれるか、データ記憶リソース４５６０から読み出されるときに、確実なデータパーサ４５１０は、エンドユーザには見えなくてもよい方法でデータを分割し、再結合してもよい。このようにして、エンドユーザは、オンデマンドで動的に拡張可能な記憶にアクセスすることが可能であってもよい。

【０４４９】

確実なデータパーサ４５１０を使用したクラウド内のデータ記憶は、確実、弾性、持続性、かつ内密である。確実なデータパーサ４５１０は、いずれの法医学的に識別可能なデータもクラウドを通り抜けないか、または単一の記憶デバイス内に記憶されないことを確実にすることによってデータを確保する。クラウド記憶システムは、確実なデータパーサによって提供される冗長性により、弾性である（すなわち、元のデータを再構成するために、データの全てよりも少ない分離された部分が必要とされる）。複数の記憶デバイス内、および／または複数のデータ記憶リソース４５６０内に、分離された部分を記憶することは、たとえ記憶デバイスのうちの１つ以上が故障しても、またはアクセス不可能であっても、データが再構成されてもよいことを確実にする。クラウド記憶システムは、データ記憶リソース４５６０内での記憶デバイスの損失がエンドユーザに影響を及ぼさないように、持続性である。１つの記憶デバイスが故障した場合、その記憶デバイス内に記憶されたデータ部分は、データを露出する必要なく別の記憶デバイスにおいて再構築されてもよい。さらに、記憶リソース４５６０（またはデータ記憶リソース４５６０を構成する複数のネットワーク接続された記憶デバイスさえも）、複数の故障のリスクを制限するために地理的に分散させられてもよい。最終的に、クラウドに記憶されたデータは、１つ以上の鍵を使用して内密に保たれてもよい。上記で説明されるように、データは、関心のユーザまたはコミュニティのみがデータにアクセスできるように、一意の鍵によってそのユーザまたはコミュニティに割り当てられてもよい。

【０４５０】

確実なデータパーサを使用したクラウド内におけるデータ記憶はまた、従来のローカルまたはネットワーク接続記憶上において性能増進を提供してもよい。システムのスループットは、並行して複数の記憶デバイスへのデータの別個の部分の書き込みおよび読み出しによって向上させられてもよい。このスループットの増加は、記憶システムの全体的な速度に実質的に影響を及ぼすことなく、より低速で安価な記憶デバイスが使用されることを可能にしてもよい。

【０４５１】

図４６は、開示された実施形態による、確実なデータパーサを使用してネットワークアクセスを確保するための例示的なブロック図である。確実なデータパーサ４６１０は、ネットワークリソースへのアクセスを制御するために、ネットワークアクセス制御ブロック４６２０とともに使用されてもよい。図４６に図示されるように、ネットワークアクセス制御ブロック４６２０は、ユーザ４６００とエンドユーザ４６４０との間に確実なネットワーク通信を提供するために使用されてもよい。いくつかの実施形態では、ネットワークアクセス制御ブロック４６２０は、クラウド（例えば、クラウド４２５０、図４２）の中で１つ以上のネットワークリソースに対する確実なネットワークアクセスを提供してもよい。承認ユーザ（例えば、ユーザ４６００およびエンドユーザ４６４０）には、ネットワーク上で確実に通信するか、および／または確実なネットワークリソースにアクセスする能力をユーザに提供する、グループ全体の鍵が提供されてもよい。確保されたネットワークリソースは、適正な信任状（例えば、グループ鍵）が提示されない限り応答しない。これは、例えば、サービス攻撃、ポートスキャン攻撃、介入者攻撃、および再生攻撃の拒否等の、一般的なネットワーク攻撃を防止し得る。

【０４５２】
通信ネットワーク内に記憶された静止しているデータに対するセキュリティ、および通信ネットワーク内を介して進行中のデータに対するセキュリティを提供することに加えて、ネットワークアクセス制御ブロック４６２０は、関心のユーザまたはコミュニティの異なるグループ間で情報を共有するために、確実なデータパーサ４６２０とともに使用されてもよい。確実な仮想ネットワーク上で確実な関心のコミュニティとして参加するように協調グループが設定されてもよい。ネットワークおよびネットワーク接続されたリソースへのアクセスをグループのメンバーに提供するために、ワークグループ鍵がグループメンバーに配備されてもよい。ワークグループ鍵配備のためのシステムおよび方法が、上記で論議されている。

【０４５３】
図４７は、開示された実施形態による、確実なデータパーサを使用して高性能コンピューティングリソースを確保するための例示的なブロック図である。確実なデータパーサ４７１０は、高性能コンピューティングリソース４７２０への確実なアクセスを提供するために使用されてもよい。図４７に図示されるように、エンドユーザ４７４０は、高性能コンピューティングリソース４７２０にアクセスしてもよい。いくつかの実施形態では、確実なデータパーサ４７１０は、クラウド（例えば、クラウド４２５０、図４２）の中の高性能リソースへの確実なアクセスを提供してもよい。高性能コンピューティングリソースは、大型コンピュータサーバまたはサーバファームであってもよい。これらの高性能コンピューティングリソースは、融通性があり、拡張可能であり、かつ構成可能なデータサービスおよびデータ記憶サービスをユーザに提供してもよい。

【０４５４】
別の実施形態によれば、仮想マシンを使用してデータアクセスを確保するために、確実なデータパーサが使用されてもよい。仮想マシンモニタ（ＶＭＭ）とも呼ばれるハイパーバイザは、複数の仮想マシンが単一のホストコンピュータ上で作動することを可能にするコンピュータシステムである。図４８は、ハイパーバイザ４８００、およびハイパーバイザ４８００上で作動する一連の仮想マシン４８１０を含む、例示的なブロック図を示す。ハイパーバイザ４８００は、基本オペレーティングシステム（例えば、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）およびＬｉｎｕｘ（登録商標））を実行する。仮想マシン４８１０は、基本オペレーティングシステム上の攻撃（例えば、ウイルス、ワーム、ハッカー等）が仮想マシン４８１０に影響を及ぼさないように、基本オペレーティングシステムからファイアウォールで隔てられてもよい。１つ以上の確実なデータパーサは、仮想マシン４８１０を確保するようにハイパーバイザ４８００と一体化してもよい。具体的には、確実なデータパーサを使用して、仮想マシン４８１０は、１つ以上のサーバまたはエンドユーザと確実に通信してもよい。この実施形態によれば、確実なデータアクセスは、ユーザに確実な仮想マシンイメージを提供することによって、ユーザに配備されてもよい。この実施形態は、データの機密性および完全性を保証しながらオンデマンド情報共有を可能にしてもよい。

【０４５５】
図４９および５０は、確実なデータパーサをハイパーバイザと統合するための代替的実施形態を示す。図４９においては、確実なデータパーサ４９３０は、ハイパーバイザ４９２０より上側に実装されている。例えば、確実なデータパーサ４９３０は、ハイパーバイザ４９２０上で動作するソフトウェアアプリケーションまたはモジュールとして実装されてもよい。いくつかの実施形態では、確実なデータパーサ４９３０は、ハイパーバイザ４９２０上で作動する仮想マシンによって実装されてもよい。ハイパーバイザ４９２０上で作動する仮想マシンは、確実なデータパーサ４９３０を使用して、サーバ４９４０およびエンドユーザ４９５０に確実に連結してもよい。図５０では、確実なデータパーサ５０３０は、ハイパーバイザ５０２０より下側に実装されている。例えば、確実なデータパーサ５０３０は、ハイパーバイザ５０２０のハードウェアの中に実装されてもよい。ハイパーバイザ５０２０上で作動する仮想マシンは、確実なデータパーサ５０３０を使用して、サ

ーバ５０４０およびエンドユーザ５０５０と確実に通信してもよい。
【０４５６】
別の実施形態によれば、確実なデータパーサは、直交周波数分割多重（ＯＦＤＭ）通信チャネルを確保するために使用されてもよい。ＯＦＤＭは、広帯域デジタル通信に使用される多重化スキームである。広帯域無線基準（例えば、ＷｉＭＡＸおよびＬＴＥ）および送電線上の広帯域（ＢＰＬ）は、ＯＦＤＭを使用する。ＯＦＤＭは、全ての隣接するチャネルが真に直交するので、一意である。これは、雑音のクロストーク、消去、および誘発を排除する。現在、これらのＯＦＤＭ基準では、データは、単一のＯＦＤＭ通信チャネルにわたって伝送される。確実なデータパーサは、複数のＯＦＤＭ通信チャネル間でデータを分割することによって、ＯＦＤＭ通信を確保してもよい。上記で説明されるように、確実なデータパーサを使用して複数のデータチャネル間でデータを分割することは、データの一部分のみが各チャネル上において伝送されるので、データを確保する。付加的な有益性として、確実なデータパーサは、複数のデータチャネル上で複数のデータ部分を同時に伝送してもよい。これらの同時伝送は、データ伝送の効果的な帯域幅を増加させてもよい。加えて、または代替として、確実なデータパーサは、複数のデータチャネル上で同じデータ部分を伝送してもよい。この冗長伝送技法は、伝送の信頼性を増加させてもよい。図５１は、ＯＦＤＭ通信ネットワークを確保するための例示的なブロック図である。図５１に図示されるように、エンドユーザ５１１０は、ＯＦＤＭネットワーク５１４０上でデータをエンドユーザ５１５０に送信するために、確実なデータパーサ５１２０を使用してもよい。ＯＦＤＭネットワーク５１４０は、無線上広帯域ネットワーク、送電線上広帯域ネットワーク、または任意の他の好適なＯＦＤＭネットワークであってもよい。
【０４５７】
いくつかの他の実施形態によれば、確実なデータパーサは、例えば、電力網を含む重要インフラストラクチャ制御を保護するために使用されてもよい。インターネットプロトコル（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）バージョン６（ＩＰｖ６）は、次世代インターネットプロトコルである。ＩＰｖ６は、現在のインターネットプロトコルよりも大きいアドレス空間を有する。実装されると、ＩＰｖ６は、より多くのデバイスがインターネット上で直接アクセスされることを可能にする。アクセスを承認された個人に限定するために、重要インフラストラクチャの制御が制限されることが重要である。上記で説明されるように、確実なデータパーサは、ネットワークリソースへのアクセスを承認されたユーザおよびグループに限定してもよい。重要なシステムは、「２人規則（ｔｗｏ　ｍａｎ　ｒｕｌｅ）」を使用して保護されてもよく、それにより、少なくとも２人のユーザが、重要なシステムにアクセスするためにそれぞれの鍵を提供する必要がある。図５２は、電力網を確保するための例示的なブロック図である。図５２に図示されるように、ユーザ５２１０は、エンドユーザ５２５０に対する電力網５２４０への確実なアクセスを提供するために、確実なデータパーサ５２２０を使用してもよい。
【０４５８】
いくつかの実施形態では、電力網システムは、一般的な通信ネットワークのネットワークケーブル配線および関連機器を排除するために、送電線上広帯域ネットワークを使用してインターネットに連結されてもよい。電力網システムをインターネットに連結することは、リアルタイムで使用料を報告することによって電力のより効率的な使用を可能にするスマートグリッド技法を有効にしてもよい。別の有益性として、高性能コンピューティングリソースおよび／またはデータ記憶設備が、インターネット接続された電力監視設備に設置されてもよい。これらのリソースは、クラウドの中のデータを保護するための確実な記憶および処理ノードを提供してもよい。
【０４５９】
確実なデータパーサのいくつかの用途が上記で説明されるが、本発明は、セキュリティ、耐故障性、匿名性、または前述の内容の任意の好適な組み合わせを増大させるために、任意のネットワークアプリケーションと一体化してもよいことを明確に理解されたい。
【０４６０】

加えて、他の組み合わせ、追加、置換、および修正が、本明細書の開示を考慮して当業者に明白となるであろう。

【図１】

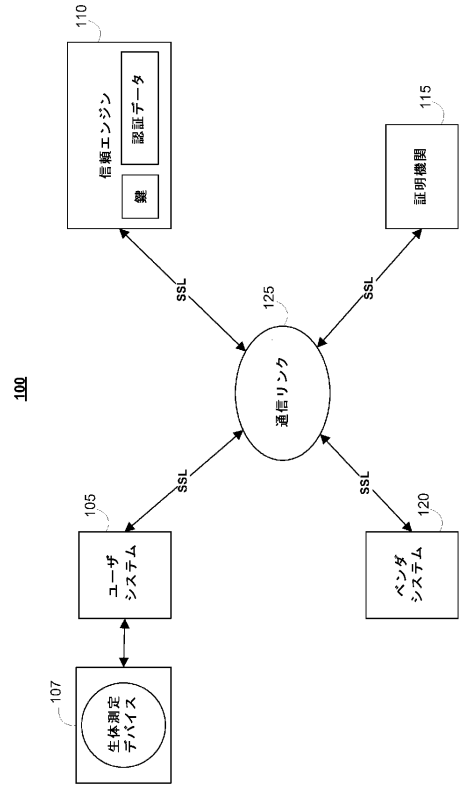

FIG. 1

【図２】

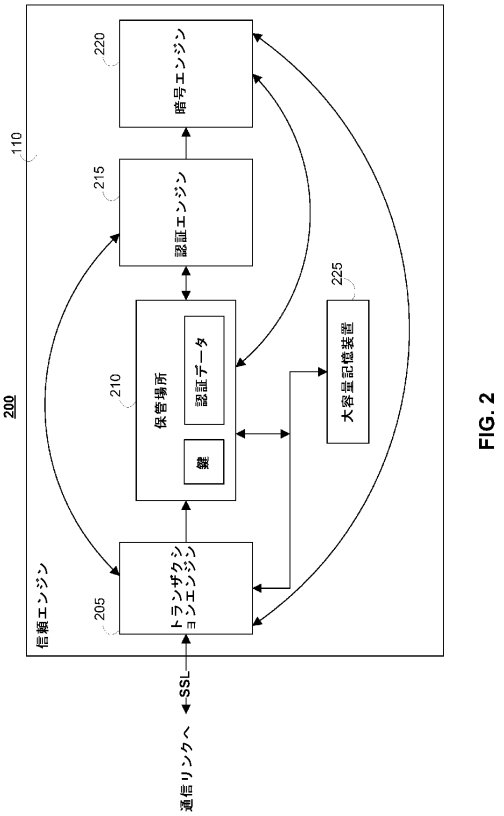

FIG. 2

【図３】

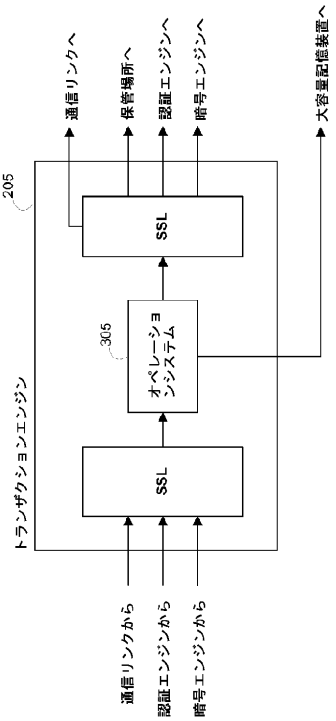

FIG. 3

【図４】

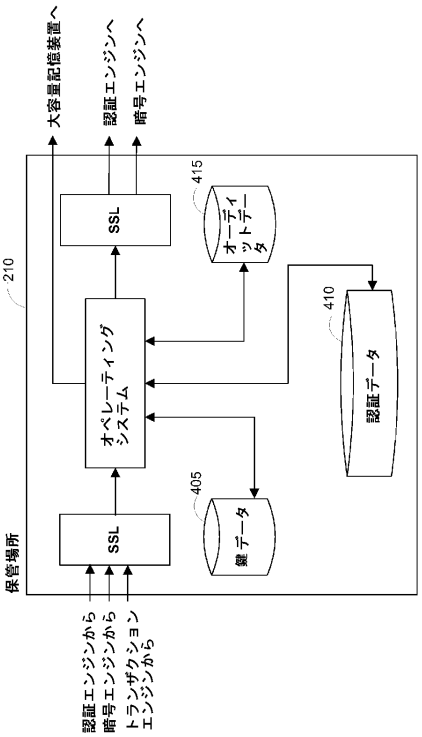

FIG. 4

【図５】

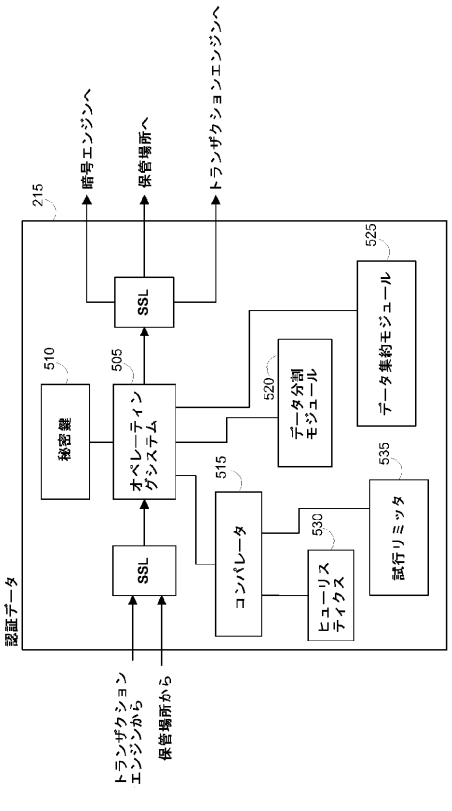

FIG. 5

【図６】

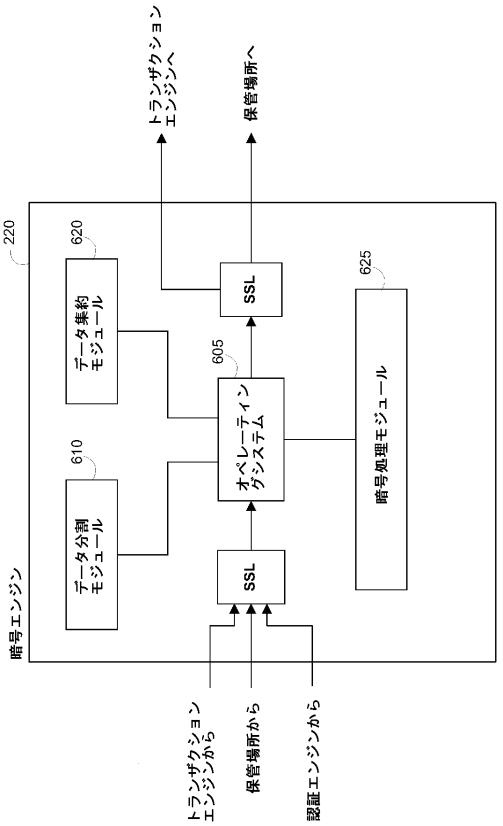

FIG. 6

【図７】

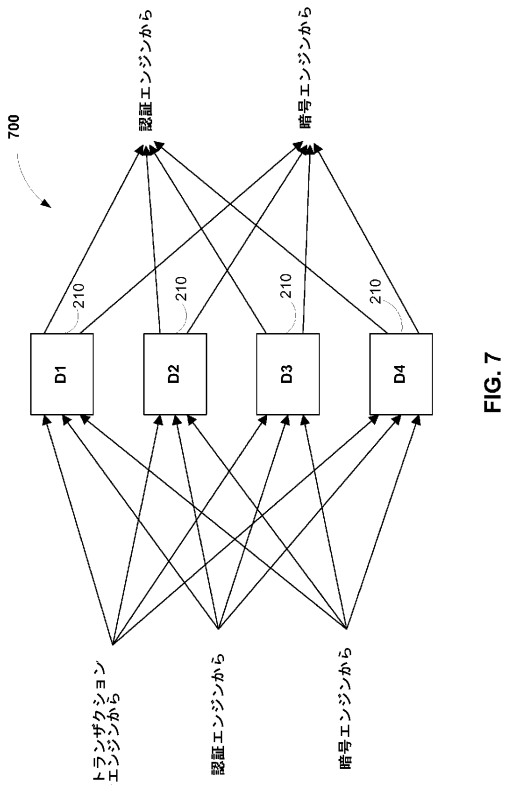

FIG. 7

【図８】

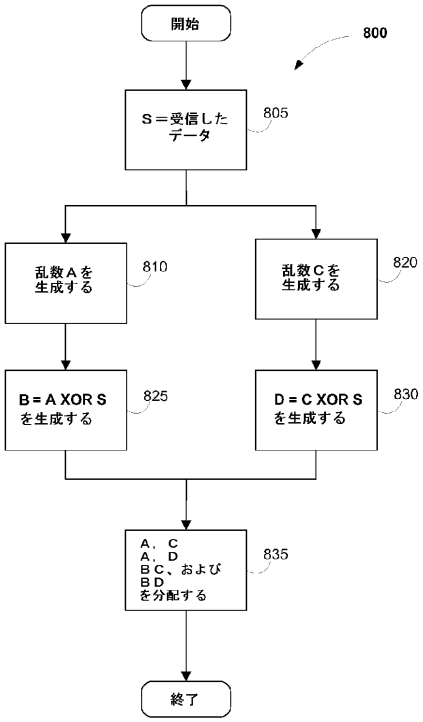

FIG. 8

【図９Ａ】

900

登録データフロー			
送信	受信	SSL	措置
ユーザ	トランザクションエンジン（ＴＥ）	1/2	認証エンジン（ＡＥ）の公開鍵で暗号化された登録認証データ（Ｂ）およびユーザＩＤ（ＵＩＤ）を（ＰＵＢ＿ＡＥ（ＵＩＤ，Ｂ））として伝送する
TE	AE	フル	伝送を転送する
			ＡＥが転送されたデータを復号し、分割する
AE	第Ｘの保管場所（ＤＸ）	フル	それぞれのデータ部分を記憶する
デジタル証明書が要求した時			鍵
AE	暗号エンジン（ＣＥ）	フル	鍵生成を要求する
			ＣＥが鍵を生成し、分割する
CE	TE	フル	デジタル証明書の要求を伝送する
TE	認定機関（ＣＡ）	1/2	要求を伝送する
CA	TE	1/2	デジタル証明書を伝送する
TE	ユーザ	1/2	デジタル証明書を伝送する
TE	MS	フル	デジタル証明書を記憶する
CE	DX	フル	鍵のそれぞれの部分を記憶する

905
915
920
925
930
935
945
950
955
960
965

FIG. 9, Panel A

【図９Ｂ】

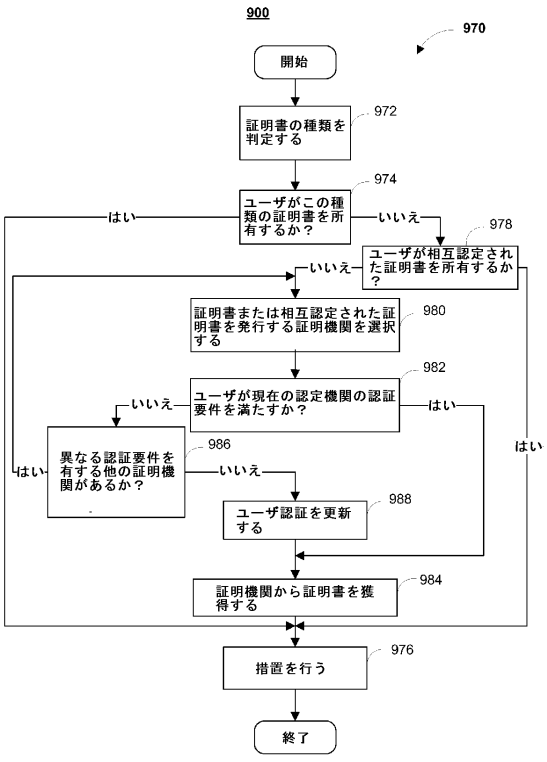

FIG. 9, Panel B

【図１０】

1000

認証データフロー			
送信	受信	SSL	装置
ユーザ	ベンダ	1/2	購入の選択等のトランザクションが発生する
ベンダ	ユーザ	1/2	トランザクションＩＤ（ＴＩＤ）および認証要求（ＡＲ）を伝送する
			認証データ（Ｂ’）がユーザから収集される
ユーザ	ＴＥ	1/2	認証エンジン（ＡＥ）の公開鍵に包まれたＴＩＤおよびＢ’を（ＰＵＢ＿ＡＥ（ＴＩＤ，Ｂ’））として伝送する
ＴＥ	ＡＥ	フル	伝送を転送する
			登録認証データ（Ｂ）が要求され、収集される
ベンダ	トランザクションエンジン（ＴＥ）	フル	ＴＩＤ、ＡＲを伝送する
ＴＥ	大容量記憶装置（ＭＳ）	フル	データベースの中に記録を作成する
ＴＥ	第Ｘの保管場所（DX）	フル	UID, TID
ＤＸ	ＡＥ	フル	ＴＩＤおよび登録時に記憶された認証データ部分（ＢＸ）を（ＰＵＢ＿ＡＥ（ＴＩＤ，ＢＸ））として伝送する
			ＡＥがＢを集約し、Ｂ’と比較する
ＡＥ	ＴＥ	フル	ＴＩＤ、ＡＲに記入される
ＴＥ	ベンダ	フル	ＴＩＤ、はい／いいえ
ＴＥ	ユーザ	1/2	ＴＩＤ、確認メッセージ

FIG. 10

【図１１】

1100

署名データフロー			
送信	受信	SSL	装置
ユーザ	ベンダ	1/2	取引の同意等のトランザクションが発生する
ベンダ	ユーザ	1/2	トランザクション識別番号（ＴＩＤ）、認証要求（ＡＲ）、および同意またはメッセージ（Ｍ）を伝送する
			現在の認証データ（Ｂ’）およびユーザによって受信されるメッセージのハッシュ（ｈ（Ｍ’））がユーザから収集される
ユーザ	ＴＥ	1/2	認証エンジン（ＡＥ）の公開キーに包まれたＴＩＤ，Ｂ’，ＡＲ，およびｈ（Ｍ’）を（ＰＵＢ＿ＡＥ（ＴＩＤ，Ｂ’，ｈ（Ｍ’））として伝送する
ＴＥ	ＡＥ	フル	伝送を転送する
			登録認証データを収集する
ベンダ	トランザクションエンジン（ＴＥ）	フル	ＵＩＤ、ＴＩＤ、ＡＲ、およびメッセージのハッシュ（ｈ（Ｍ’））を伝送する
ＴＥ	大容量記憶装置（ＭＳ）	フル	データベースの中に記録を作成する
ＴＥ	第Ｘの保管場所（DX）	フル	UID, TID
ＤＸ	ＡＥ	フル	ＴＩＤおよび登録時に記憶された認証データ部分（ＢＸ）を（ＰＵＢ＿ＡＥ（ＴＩＤ，ＢＸ））として伝送する
			元のベンダメッセージがＡＥに伝送される
ＴＥ	ＡＥ	フル	ｈ（Ｍ）を伝送する
			ＡＥがＢを集約し、Ｂ’と比較し、ｈ（Ｍ）をｈ（Ｍ’）と比較する
ＡＥ	暗号エンジン（ＣＥ）	フル	デジタル署名の要求、および署名されるメッセージ、例えば、ハッシュ化されたメッセージ
ＡＥ	ＤＸ	フル	ＴＩＤ、ＵＩＤを署名する
ＤＸ	ＣＥ	フル	署名当事者に対応する暗号キーの部分を伝送する
			署名当事者に対応する暗号キーの部分を伝送する
ＣＥ	ＡＥ	フル	署名当事者のデジタル署名（Ｓ）を伝送する
ＡＥ	ＴＥ	フル	ＴＩＤ、ＡＲ、ｈ（Ｍ）、およびＳに記入される
ＴＥ	ベンダ	フル	ＴＩＤ、受領書＝（ＴＩＤ、Ｙｅｓ／Ｎｏ、およびＳ）、および信頼エンジンのデジタル署名、例えば、信頼エンジンの秘密キーで暗号化された受領書のハッシュ（Ｐｒｉｖ＿ＴＥ（ｈ（ｒｅｃｅｉｐｔ）））
ＴＥ	ユーザ	1/2	ＴＩＤ、確認メッセージ

FIG. 11

【図１２】

1200

暗号化／復号データフロー			
送信	受信	SSL	措置
復号			
			認証データプロセス1000を行い、ARにセッション鍵（sync）を含み、syncはユーザの公開鍵によってPUB_USER(SYNC)として暗号化されている
			ユーザを認証する
AE	CE	フル	ＰＵＢ ＵＳＥＲ（ＳＹＮＣ）をＣＥに転送
AE	DX	フル	UID, TID
DX	CE	フル	（ＰＵＢ＿ＡＥ（ＴＩＤ，ＫＥＹ ＵＳＥＲ））としてＴＩＤおよび秘密鍵の部分を伝送する
			ＣＥが暗号鍵を集約し、ｓｙｎｃを復号する
CE	AE	フル	ＴＩＤ、復号されたｓｙｎｃを含むＡＲに記入される
AE	TE	フル	ＴＥに転送する
TE	要求ＡＰＰ／ベンダ	1/2	ＴＩＤ、はい／いいえ Ｓｙｎｃ
暗号化			
要求ＡＰＰ／ベンダ	TE	1/2	ユーザの公開鍵の要求
TE	MS	フル	デジタル証明書を要求する
MS	TE	フル	デジタル証明書を伝送する
TE	要求ＡＰＰ／ベンダ	1/2	デジタル証明書を伝送する

FIG. 12

【図１３】

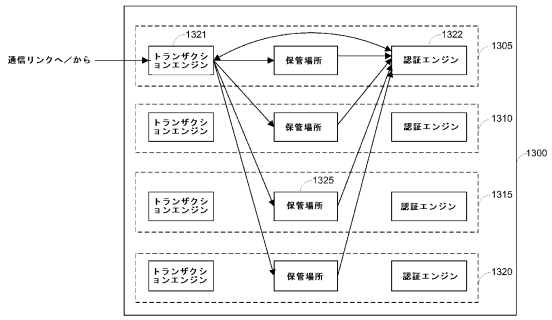

FIG. 13

【図１４】

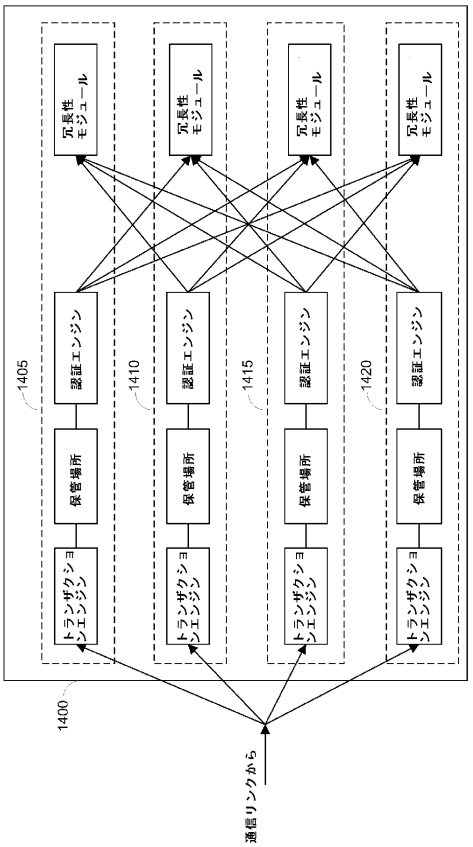

FIG. 14

【図１５】

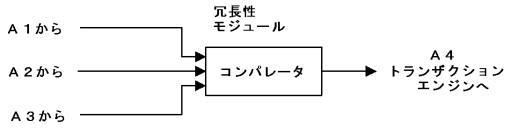

FIG. 15

【図１６】

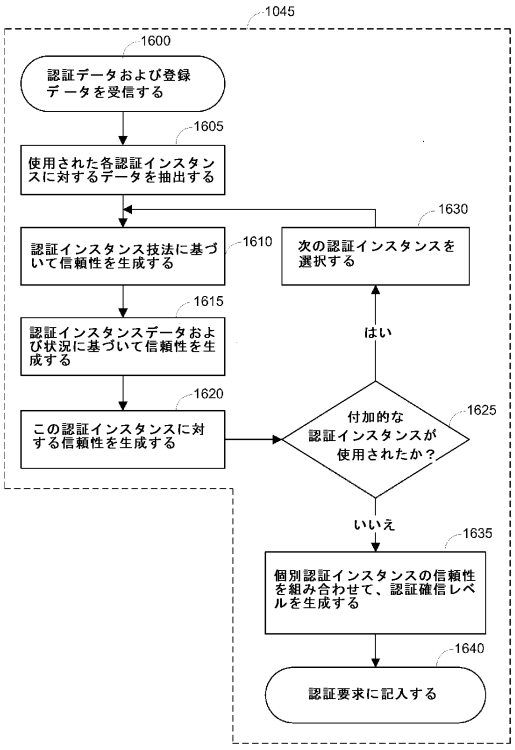

FIG. 16

【図１７】

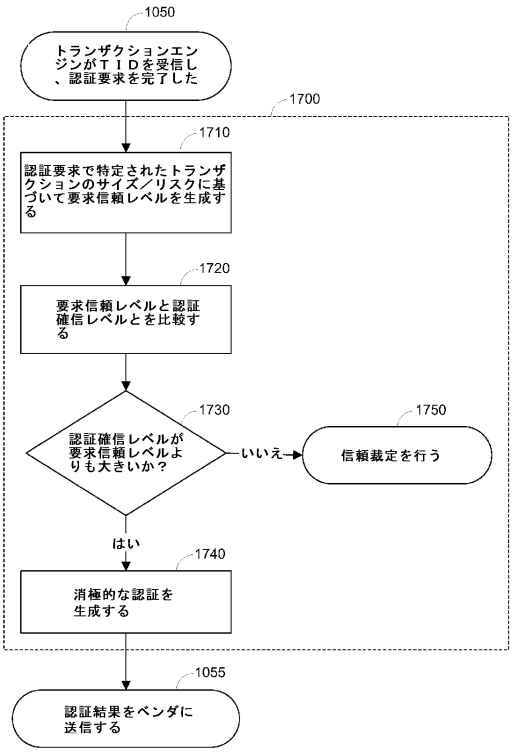

FIG. 17

【図１８】

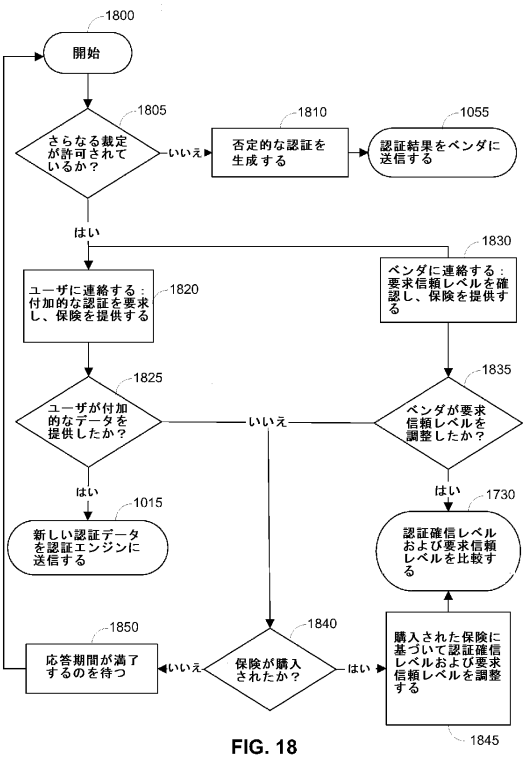

FIG. 18

【図１９】

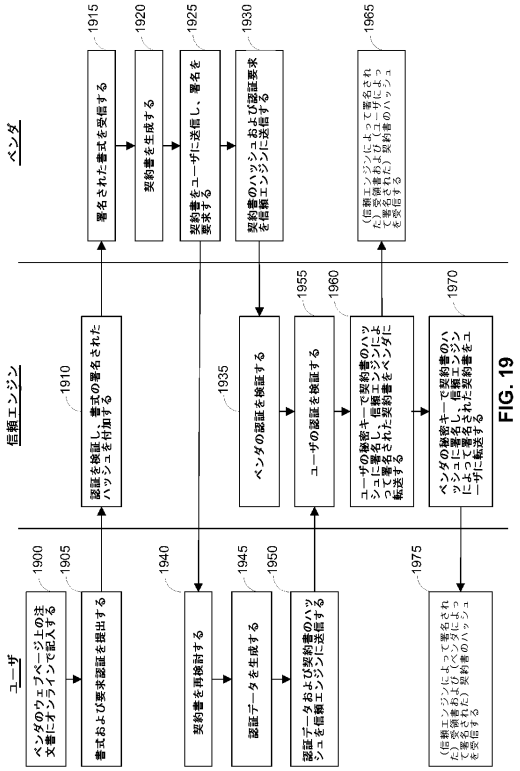

FIG. 19

【図２０】

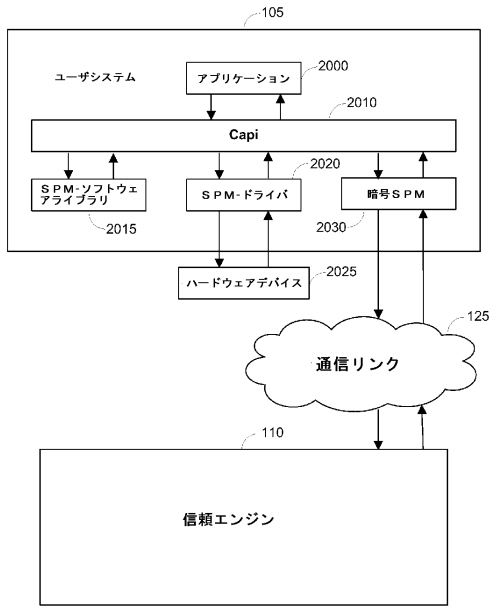

FIG. 20

【図２１】

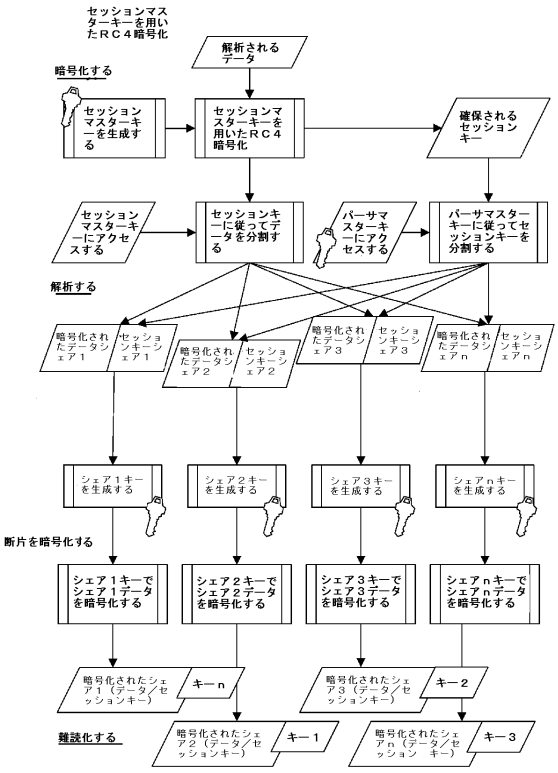

FIG. 21

【図２２】

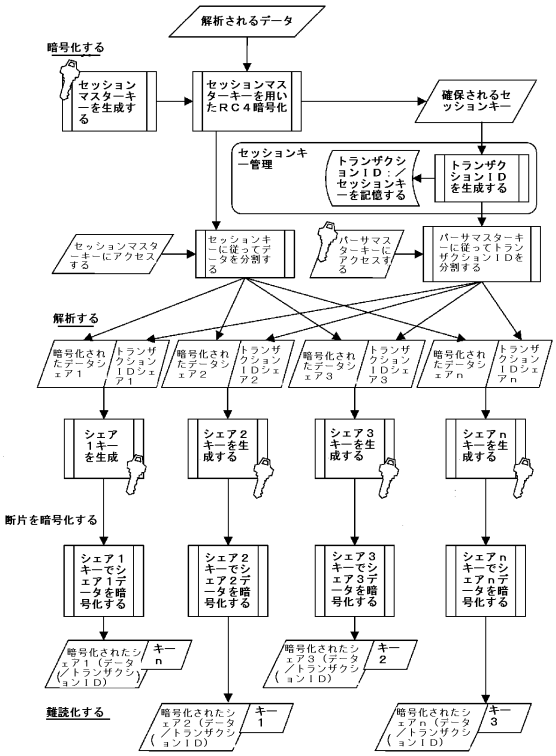

FIG. 22

【図２３】

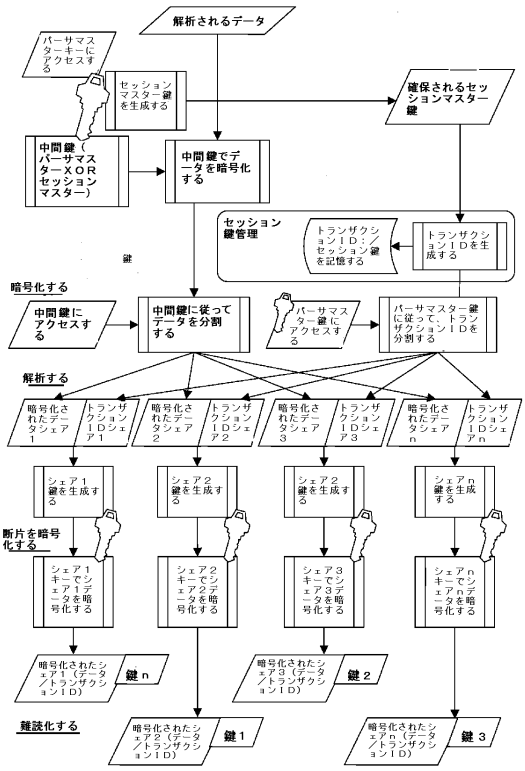

FIG. 23

【図２４】

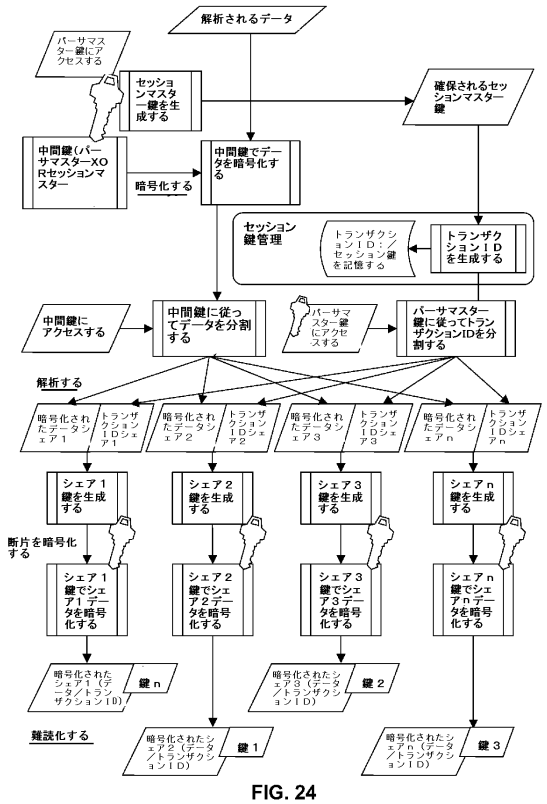

FIG. 24

【図２５】

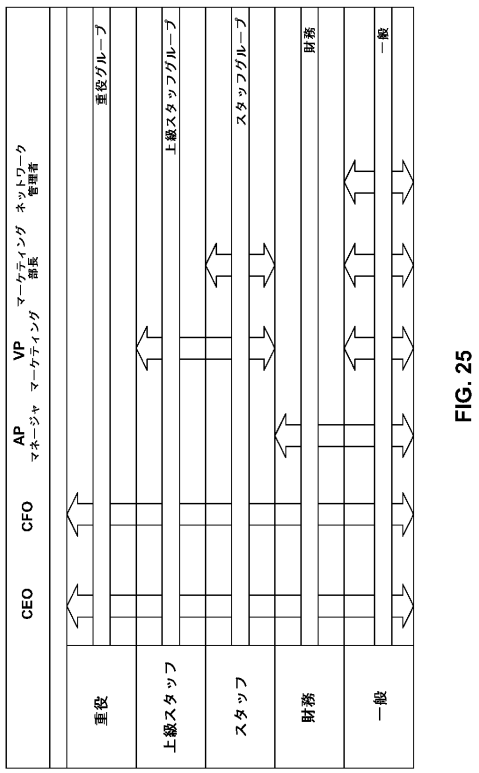

FIG. 25

【図２６】

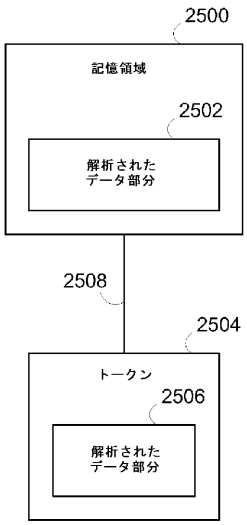

FIG. 26

【図２７】

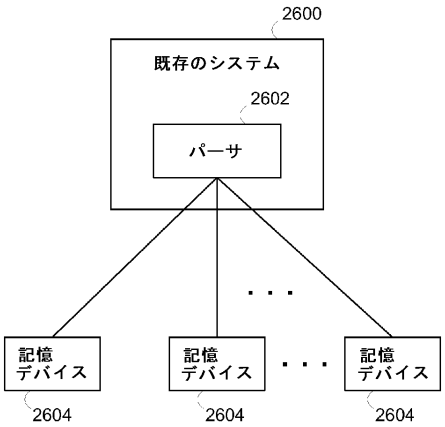

FIG. 27

【図２８】

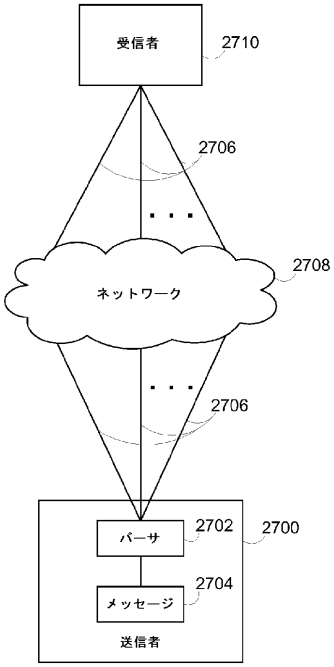

FIG. 28

【図２９】

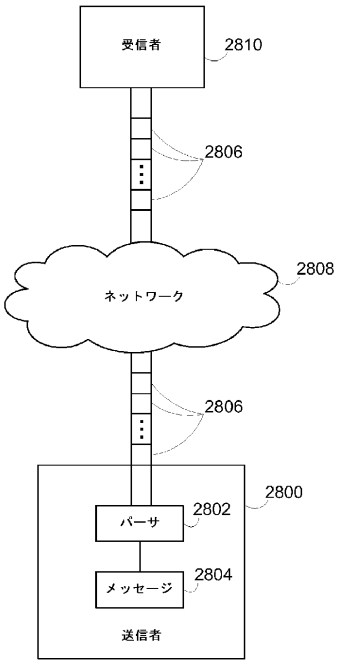

FIG. 29

【図３０】

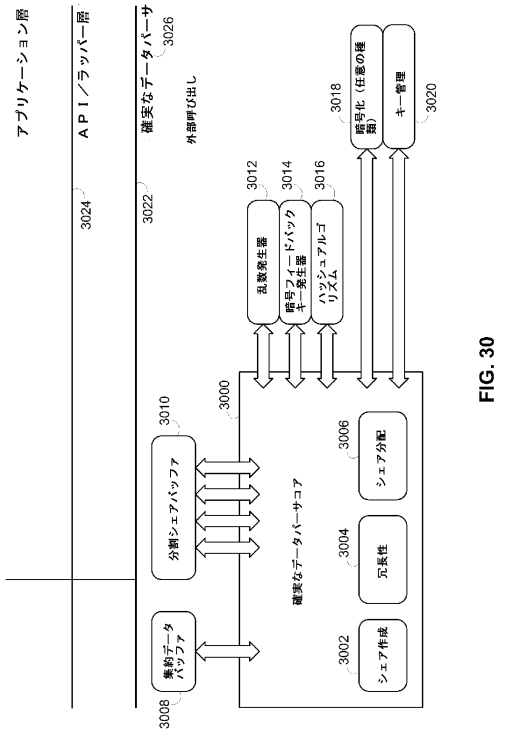

FIG. 30

【図３１】

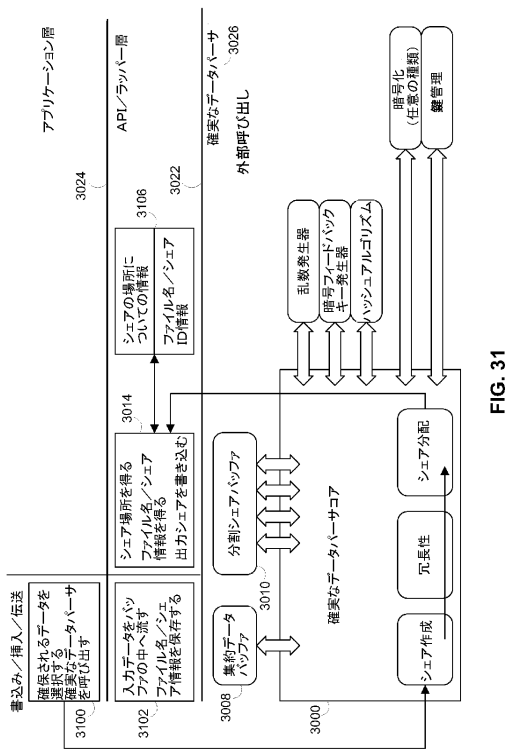

FIG. 31

【図３２】

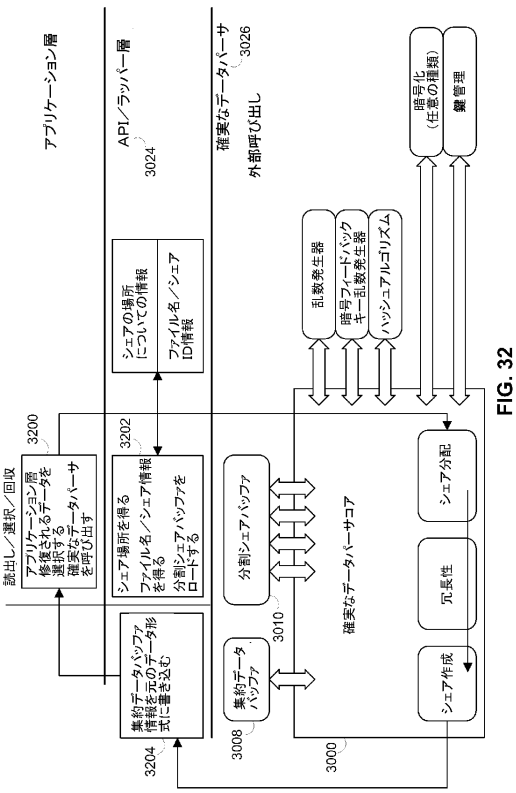

FIG. 32

【図３３】

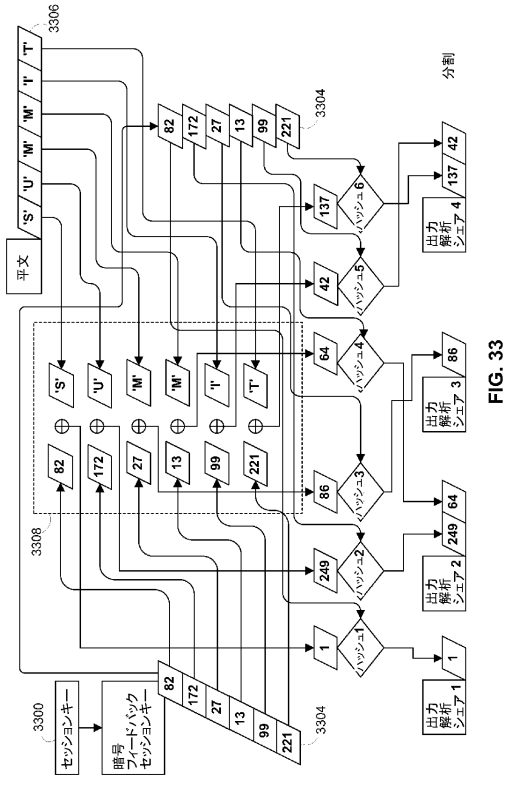

FIG. 33

【図３４】

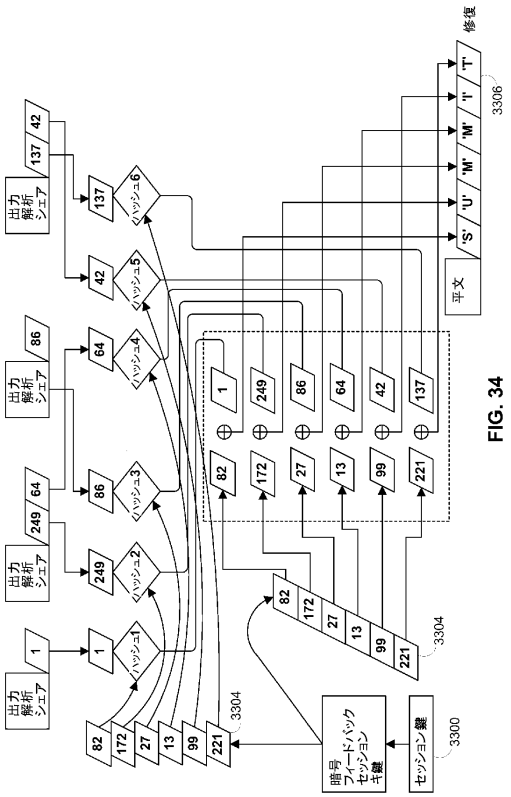

FIG. 34

【図３５】

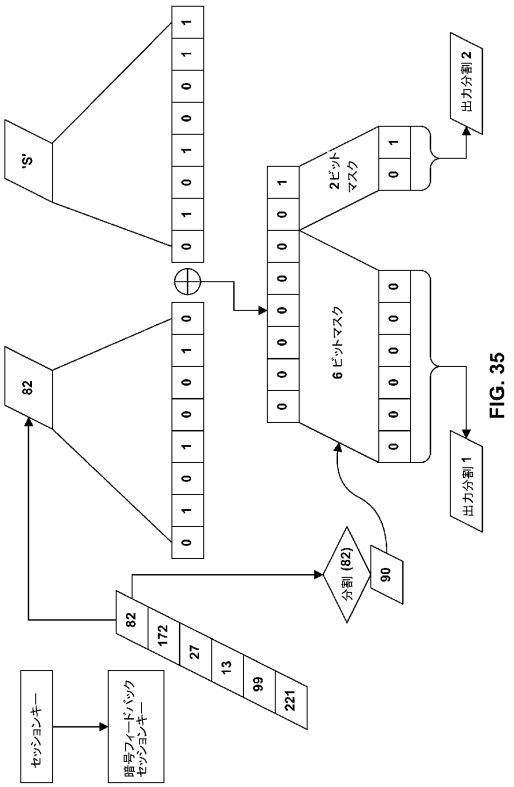

FIG. 35

【図３６】

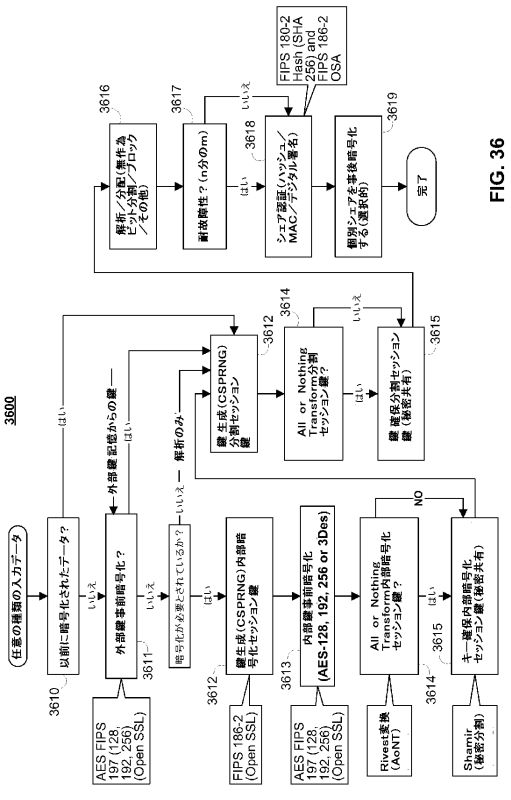

FIG. 36

【図３７】

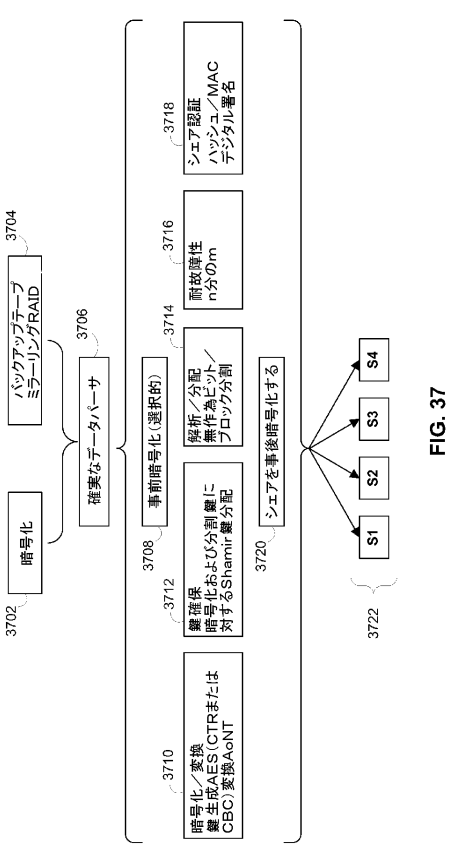

FIG. 37

【図３８】

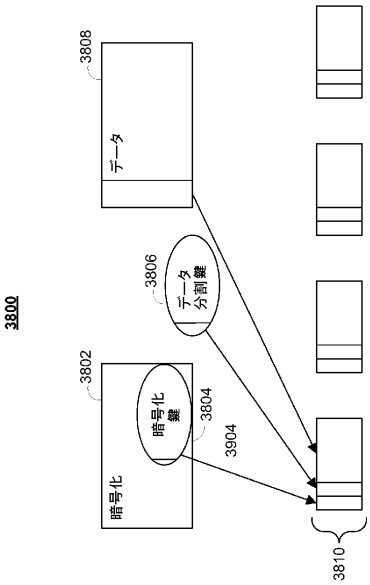

FIG. 38

【図３９】

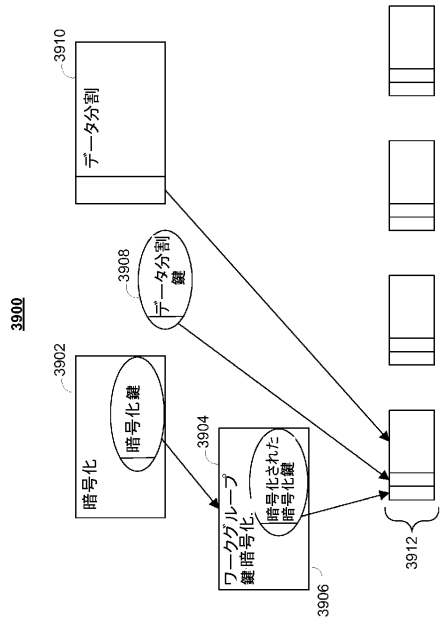

FIG. 39

【図４０】

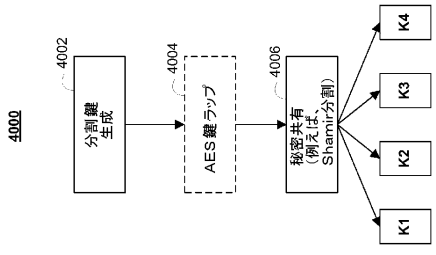

FIG. 40A

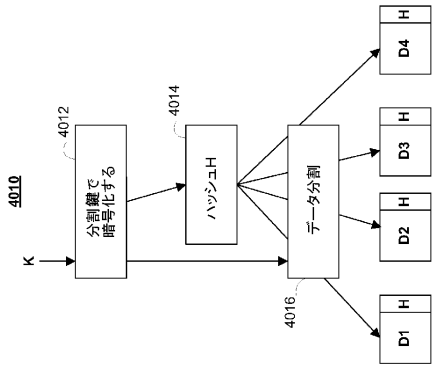

FIG. 40B

【図４１】

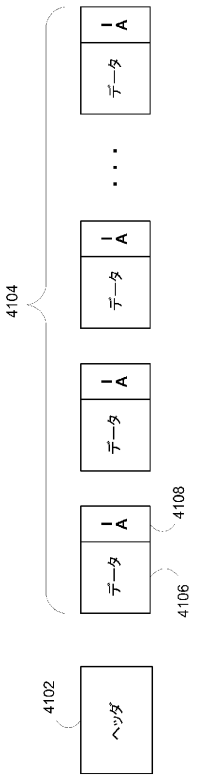

FIG. 41

【図４２】

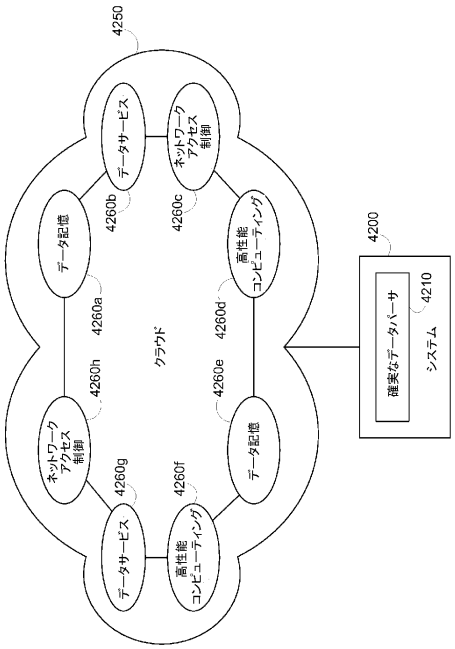

FIG. 42

【図４３】

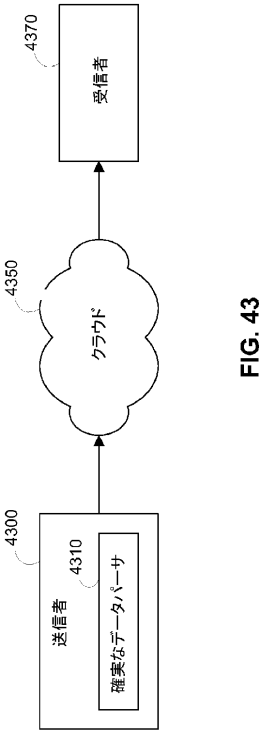

FIG. 43

【図４４】

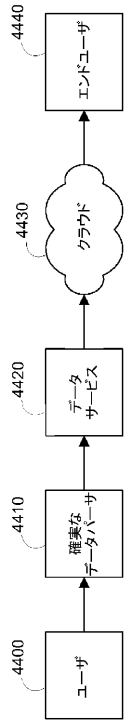

FIG. 44

【図４５】

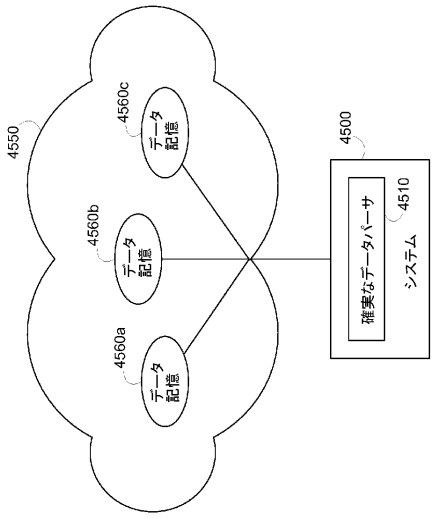

FIG. 45

【図４６】

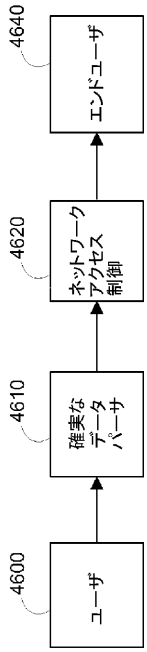

FIG. 46

【図４７】

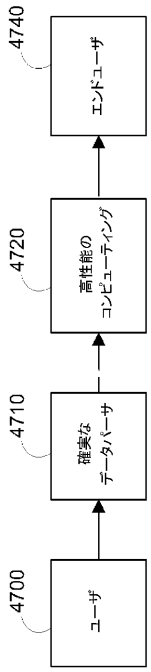

FIG. 47

【図４８】

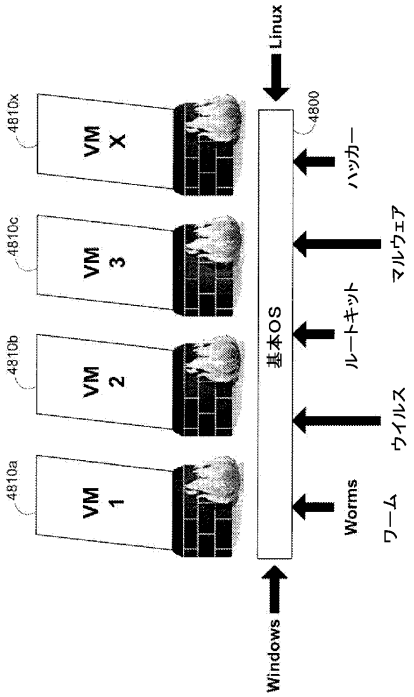

FIG. 48

【図４９】

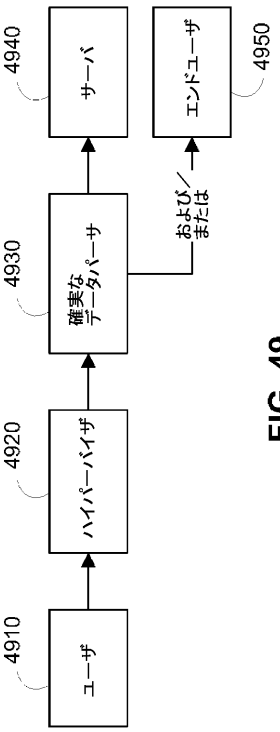

FIG. 49

【図５０】

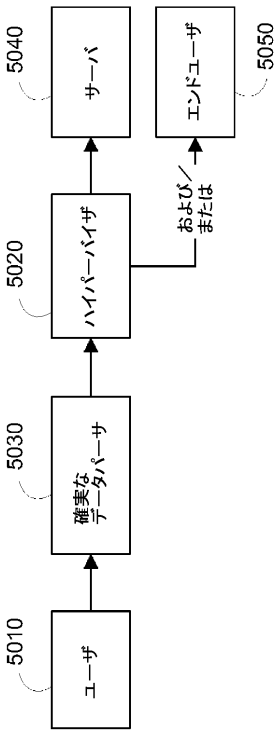

FIG. 50

【図５１】

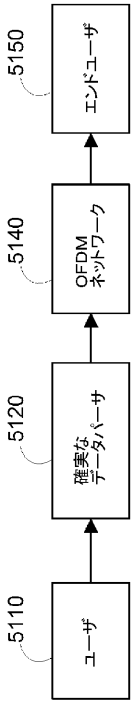

FIG. 51

【図５２】

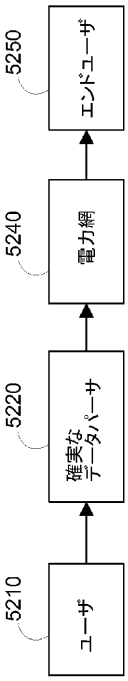

FIG. 52

フロントページの続き

(74)代理人　230113332
弁護士　山本　健策
(72)発明者　オヘア，　マーク　エス.
アメリカ合衆国　カリフォルニア　９２６７９，　コト　デ　カザ，　ケネディー　コート　８
(72)発明者　オルシーニ，　リック　エル.
アメリカ合衆国　テキサス　７５０２８，　フラワー　マウンド，　キングス　フォレスト　レーン　２１００
(72)発明者　マーティン，　ドン
アメリカ合衆国　バージニア　２３８３８，　チェスターフィールド，　スターリング　カバー　ドライブ　１１００６

審査官　青木　重徳

(56)参考文献　米国特許出願公開第２００６／０１７７０６１（ＵＳ，Ａ１）
米国特許出願公開第２００７／０１６０１９８（ＵＳ，Ａ１）
特開２００４－２１３６５０（ＪＰ，Ａ）
国際公開第０１／０４６８０８（WO，Ａ１）
特開２００８－０９８８９４（ＪＰ，Ａ）
特開２００５－２５０８６６（ＪＰ，Ａ）
特表２００８－５２３６６４（ＪＰ，Ａ）
国際公開第００／０４５３５８（WO，Ａ１）
“ｆｒｏｍ　ＮＴＴコミュニケーションズ　次世代ＢｉｚＣＩＴＹを形づくるクラウドコンピューティング構想”，ＮＴＴ技術ジャーナル，日本，社団法人電気通信協会，２００９年　2月　1日，第２１巻，第2号，ｐ．３２－３５
野沢　哲生，“急速に現実性を帯びる電力線通信　3メガのサービスに障害なし　規制緩和でさらなる高速化も”，日経コミュニケーション，日本，日経ＢＰ社，２００１年　2月　5日，第３３５号，ｐ．６５－６７

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／１０
Ｇ０９Ｃ　　１／００