(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2013-524352
(P2013-524352A)
(43)公表日　平成25年6月17日(2013.6.17)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/62	(2013.01)	G06F	21/24	166D	5J104
H04L 9/08	(2006.01)	H04L	9/00	601B	

審査請求 未請求　予備審査請求 未請求　（全 183 頁）

(21)出願番号	特願2013-502862 (P2013-502862)
(86)(22)出願日	平成23年3月31日 (2011.3.31)
(85)翻訳文提出日	平成24年11月21日 (2012.11.21)
(86)国際出願番号	PCT/US2011/030801
(87)国際公開番号	WO2011/123692
(87)国際公開日	平成23年10月6日 (2011.10.6)
(31)優先権主張番号	61/319,658
(32)優先日	平成22年3月31日 (2010.3.31)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	61/320,242
(32)優先日	平成22年4月1日 (2010.4.1)
(33)優先権主張国	米国 (US)

(71)出願人　512252526
セキュリティー　ファースト　コーポレイション
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　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹

最終頁に続く

(54)【発明の名称】移動中のデータをセキュア化するためのシステムおよび方法

(57)【要約】
本発明のシステムおよび方法は、データを証明可能にセキュアかつアクセス可能にするソリューション、つまり、ビットレベルにおいてデータセキュリティに対処し、それにより、複数の周辺ハードウェアおよびソフトウェア技術の必要性を排除することを提供する。データセキュリティは、ビットレベルにおいてデータに直接組み込まれるか、または織り込まれる。本発明のシステムおよび方法は、関心の企業コミュニティが共通企業インフラストラクチャを活用することを可能にする。セキュリティがすでにデータに織り込まれているので、データセキュリティおよびアクセス制御を損なうことなく、この共通インフラストラクチャを使用することができる。いくつかの用途において、データは、複数の場所、例えば、私的または公衆クラウドに送信される前に、認証され、暗号化され、複数のシェアに解析または分割される。

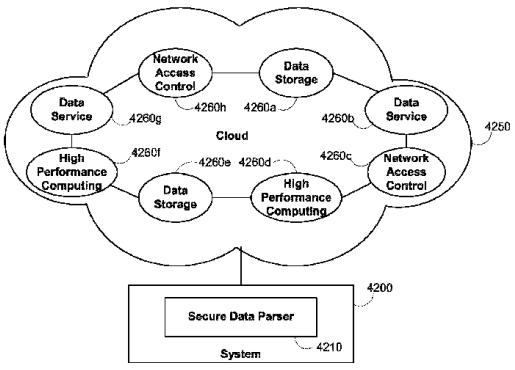

FIG. 42

【特許請求の範囲】
【請求項１】
一組のデータシェアを再構築するための方法であって、該一組のデータシェアは、第１の分割キーを使用して、情報分散アルゴリズムによって暗号化データセットから生成されたものであり、
該方法は、
該一組のデータシェアを再構築するために必要な少なくとも最小数のデータシェアを受信することと、
該最小数のデータシェアを復号することなしに、該最小数のデータシェアから該一組のデータシェアを再構築することと
を含む、方法。
【請求項２】
前記再構築することは、前記データシェアのうちの１つ以上が既に損なわれているという決定に応じて行われる、請求項１に記載の方法。
【請求項３】
前記再構築されたデータシェアのうちの少なくとも１つを記憶ネットワーク上に記憶することをさらに含む、請求項１に記載の方法。
【請求項４】
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む、請求項３に記載の方法。
【請求項５】
前記再構築することは、
認証キーによって前記最小数のデータシェアを認証することと、
前記分割キーを使用して、該認証された最小数のデータシェアから前記暗号化データを再構成することと、
該分割キーを使用して該暗号化データを分割することによって、前記一組のデータシェアを再生することと
を含む、請求項１に記載の方法。
【請求項６】
一組のデータシェアのキーを再生成するための方法であって、該一組のデータシェアは、第１の暗号化キーを使用して、情報分散アルゴリズムによって暗号化データセットから生成されたものであり、
該方法は、
該一組のデータシェアを再構築するために必要な少なくとも最小数のデータシェアを受信することと、
該最小数のデータシェアを第１の認証キーと関連付けることと、
該最小数のデータシェアを復号することなしに、該最小数のデータシェアから該一組のデータシェアを再構築することと、
該再構築された一組のデータシェアを第２の暗号化キーと関連付けることによって、該再構築された一組のデータシェアのキーを再生成することと
を含む、方法。
【請求項７】
前記最小数のデータシェアと関連付けられるヘッダを回収することと、
該回収されたヘッダからキー暗号化キーを抽出することと、
該キー暗号化キーによって第２の暗号化キーを暗号化することと、
前記キー再生成されたデータシェアのヘッダ内に暗号化された第２の認証キーを記憶することと
をさらに含む、請求項６に記載の方法。
【請求項８】

記憶ネットワーク上に前記キー再生成されたデータシェアのうちの少なくとも１つを記憶することをさらに含む、請求項６に記載の方法。
【請求項９】
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む、請求項８に記載の方法。
【請求項１０】
一組のデータシェアのキーを再生成するための方法であって、該一組のデータシェアは、第１の分割キーを使用して、情報分散アルゴリズムによって暗号化データセットから生成されたものであり、
該方法は、
該一組のデータシェアのキーを再生成するために必要な少なくとも最小数のデータシェアを受信することと、
該最小数のデータシェアを復号することなしに、該最小数のデータシェアから該一組のデータシェアを再構築することと、
該再構築された一組のデータシェアを第２の分割キーと関連付けることによって、該再構築された一組のデータシェアのキーを再生成することと
を含む、方法。
【請求項１１】
前記最小数のデータシェアと関連付けられるヘッダを回収することと、
該回収されたヘッダからキー暗号化キーを抽出することと、
該キー暗号化キーによって第２の分割キーを暗号化することと、
前記キー再生成されたデータシェアのヘッダ内に該暗号化された第２の分割キーを記憶することと
をさらに含む、請求項１０に記載の方法。
【請求項１２】
記憶ネットワーク上に前記キー再生成されたデータシェアのうちの少なくとも１つを記憶することをさらに含む、請求項１０に記載の方法。
【請求項１３】
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む、請求項１１に記載の方法。
【請求項１４】
スタブを記憶ネットワークのファイルシステム上の一組のデータシェアと関連付けるための方法であって、
該方法は、
情報分散アルゴリズムによって、暗号化データセットから該一組のデータシェアを生成することと、
該生成されたデータシェアと関連付けられる一組のスタブを生成することであって、各スタブは、それぞれのデータシェアに対応し、各スタブは、該それぞれのデータシェアと関連付けられる情報を含む、ことと、
該記憶ネットワーク上の場所に該一組のスタブを記憶することと
を含む、方法。
【請求項１５】
前記情報は、前記それぞれのデータシェアの名前、該それぞれのデータシェアが作成された日付、該それぞれのデータシェアが最後に修正された時間、前記ファイルシステム内の該それぞれのデータシェアの場所へのポインタのうちの１つを含む、請求項１４に記載の方法。
【請求項１６】
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外

し可能記憶デバイス、および大容量記憶デバイスのうちの１つと関連付けられる、１つ以上の記憶デバイスを含む、請求項１４に記載の方法。

【請求項１７】

前記生成されたデータシェアと関連付けられる前記情報を閲覧するコマンドを受信することと、

前記記憶ネットワーク上の前記場所から前記スタブを回収することと、

データシェアのファイルシステムを作成するために、該スタブから該情報を抽出することと、

該データシェアのファイルシステムを表示することと

をさらに含む、請求項１４に記載の方法。

【請求項１８】

前記スタブは、前記生成されたデータシェアのヘッダ内に記憶され、回収することが、該生成されたデータシェアの該ヘッダを回収することを含む、請求項１４に記載の方法。

【請求項１９】

全てよりも少ない前記ヘッダが回収される、請求項１８に記載の方法。

【請求項２０】

前記スタブは、スタブディレクトリの中に記憶され、回収することが、該スタブディレクトリから該スタブを回収することを含む、請求項１４に記載の方法。

【請求項２１】

前記スタブを中に記憶している前記記憶ネットワークの中の仮想ディレクトリまたは物理ディレクトリの指示を受信することをさらに含む、請求項１４に記載の方法。

【請求項２２】

前記指示は、ユーザから受信される、請求項２１に記載の方法。

【請求項２３】

セキュアなデータ処理の加速のためのコプロセッサ加速デバイスであって、

該コプロセッサ加速デバイスは、

データを記憶するためのメモリと、

該メモリに連結されるメインプロセッサと、

該メインプロセッサおよび該メモリに連結されるコプロセッサであって、該メインプロセッサおよび該メモリは、データを暗号化すること、データを分割すること、およびデータを復号することのうちの少なくとも１つを含む専用のセキュアな解析機能を実行するように構成される、コプロセッサと

を含む、コプロセッサ加速デバイス。

【請求項２４】

データを分割することは、情報分散アルゴリズム（ＩＤＡ）の使用を含む、請求項２３に記載のデバイス。

【請求項２５】

前記コプロセッサに連結されるフィールドプログラマブルゲートアレイをさらに含む、請求項２３に記載のデバイス。

【請求項２６】

前記ＦＰＧＡは、前記解析されたデータを暗号化すること、または暗号化データを復号することのうちの少なくとも１つを実行する、請求項２５に記載のデバイス。

【請求項２７】

前記コプロセッサは、ＰＣＩｅバスを介して前記メインプロセッサに連結される、請求項２３に記載のデバイス。

【請求項２８】

前記コプロセッサは、ＨＴバスを介して前記メインプロセッサに連結される、請求項２３に記載のデバイス。

【請求項２９】

前記メモリは、前記メインプロセッサ用の専用メモリを含む、請求項２３に記載のデバ

イス。
【請求項３０】
前記メモリは、前記コプロセッサ用の専用メモリを含む、請求項２３に記載のデバイス。
【請求項３１】
前記コプロセッサは、１つ以上の独立ディスクの冗長アレイ（ＲＡＩＤ）機能を実装する、ＲＡＩＤ処理ユニットである、請求項２３に記載のデバイス。
【請求項３２】
携帯用デバイスを使用してデータをセキュア化するための方法であって、
該方法は、
１つのキーに少なくとも部分的に基づいて、一組のデータからデータの少なくとも２つの部分を生成することであって、該データの少なくとも２つの部分および該キーは、該一組のデータを再構成することに十分である、ことと、
該携帯用デバイス上に該キーを記憶することと
を含む、方法。
【請求項３３】
前記携帯用デバイスは、取外し可能記憶デバイスである、請求項３２に記載の方法。
【請求項３４】
前記取外し可能記憶デバイスは、ユニバーサルシリアルバス（ＵＳＢ）インターフェースを介してエンドユーザデバイスに連結する、請求項３３に記載の方法。
【請求項３５】
前記携帯用デバイス上に前記生成されたデータ部分のうちの少なくとも１つを記憶することをさらに含む、請求項３２に記載の方法。
【請求項３６】
前記キーは、暗号化キー、分割キー、および認証キーのうちの１つである、請求項３２に記載の方法。
【請求項３７】
前記データの少なくとも２つの部分は、情報分散アルゴリズム（ＩＤＡ）および該ＩＤＡと関連付けられる分割キーを使用して生成される、請求項３２に記載の方法。
【請求項３８】
携帯用デバイスを使用してデータをセキュア化するための方法であって、
該方法は、
１つのキーに少なくとも部分的に基づいて、一組のデータからデータの少なくとも２つの部分を生成することであって、該データの少なくとも２つの部分および該キーは、該一組のデータを再構成するために十分である、ことと、
該携帯用デバイス上に該生成されたデータ部分のうちの少なくとも１つを記憶することと
を含む、方法。
【請求項３９】
前記携帯用デバイスは、取外し可能記憶デバイスである、請求項３８に記載の方法。
【請求項４０】
前記取外し可能記憶デバイスは、ユニバーサルシリアルバス（ＵＳＢ）インターフェースを介してエンドユーザデバイスに連結する、請求項３９に記載の方法。
【請求項４１】
前記携帯用デバイス上に前記キーを記憶することをさらに含む、請求項３８に記載の方法。
【請求項４２】
前記キーは、暗号化キー、分割キー、および認証キーのうちの１つである、請求項３８に記載の方法。
【請求項４３】

前記データの少なくとも２つの部分は、情報分散アルゴリズム（ＩＤＡ）および該ＩＤＡと関連付けられる分割キーを使用して生成される、請求項３８に記載の方法。
【請求項４４】
分割され、記憶ネットワーク上に記憶されるファイルのファイル名をセキュア化するための方法であって、
該方法は、
認証値を取得するために、認証アルゴリズムを使用して該ファイルの該ファイル名を処理することと、
該ファイルの該認証値に一致する０認証値を有するデータシェアのファイル名について、該記憶ネットワーク上のシェア場所を検索することによって、該ファイルに対応する該データシェアを回収することと
を含む、方法。
【請求項４５】
情報分散アルゴリズムを使用して、前記認証されたファイル名と関連付けられる１つ以上のデータシェアを生成することと、
前記記憶ネットワーク内の１つ以上のデータシェア場所に該生成されたデータシェアを記憶することと
をさらに含む、請求項４４に記載の方法。
【請求項４６】
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む、請求項４４に記載の方法。
【請求項４７】
前記認証アルゴリズムは、ＨＭＡＣ－ＳＨＡ２５６アルゴリズムである、請求項４４に記載の方法。
【請求項４８】
前記処理前に、付加的な情報を前記ファイルの前記ファイル名に付加することをさらに含む、請求項４４に記載の方法。
【請求項４９】
前記付加的な情報は、データシェア場所と関連付けられる数を含む、請求項４８に記載の方法。
【請求項５０】
分割され、および記憶ネットワーク上に記憶されるべきファイルのファイル名をセキュア化するための方法であって、
該方法は、
暗号化アルゴリズムを使用して、該ファイルの該ファイル名を暗号化することと、
情報分散アルゴリズムを使用して、該暗号化されたファイル名と関連付けられる１つ以上のデータシェアを生成することと、
該記憶ネットワーク内の１つ以上のデータシェア場所に該生成されたデータシェアを記憶することと、
該生成されたデータシェアのうちの１つのファイル名を復号することによって、該ファイルの該ファイル名を再生することと
を含む、方法。
【請求項５１】
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む、請求項５０に記載の方法。
【請求項５２】
前記暗号化アルゴリズムは、ＡＥＳアルゴリズムである、請求項５０に記載の方法。
【請求項５３】

前記暗号化前に、付加的な情報を前記ファイルの前記ファイル名に付加することをさらに含む、請求項５０に記載の方法。
【請求項５４】
前記付加的な情報は、データシェア場所と関連付けられる数を含む、請求項５３に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願の相互参照）
本願は、米国仮特許出願第６１／３１９，６５８号（２０１０年３月３１日出願）および米国仮特許出願第６１／３２０，２４２号（２０１０年４月１日出願）の利益を主張する。これらの仮特許出願の各々の内容は、その全体が本明細書に参照することによって援用される。
【０００２】
（発明の分野）
本発明は、概して、移動中のデータをセキュア化するためのシステムおよび方法に関する。本明細書に記載のシステムおよび方法は、所有者共通の米国特許第７，３９１，８６５号ならびに所有者共通の米国特許出願第１１／２５８，８３９号（２００５年１０月２５日出願）、同第１１／６０２，６６７号（２００６年１１月２０日出願）、同１１／９８３，３５５号（２００７年１１月７日出願）、同第１１／９９９，５７５号（２００７年１２月５日出願）、同第１２／１４８，３６５号（２００８年４月１８日出願）、同第１２／２０９，７０３号（２００８年９月１２日出願）、同第１２／３４９，８９７号（２００９年１月７日出願）、同第１２／３９１，０２８号（２００９年２月２３日出願）、同第１２／７８３，２７６号（２０１０年５月１９日出願）および同第１２／９５３，８７７号（２０１０年１１月２４日出願）、ならびに米国仮特許出願６１／４３６，９９１号（２０１１年１月２７日出願）、同第６１／２６４，４６４号（２００９年１１月２５日出願）、同第６１／３１９，６５８号（２０１０年３月３１日出願）、同第６１／３２０，２４２号（２０１０年４月１日出願）、同第６１／３４９，５６０号（２０１０年５月２８日出願）、同第６１／３７３，１８７号（２０１０年８月１２日出願）、同第６１／３７４，９５０号（２０１０年８月１８日出願）、および同第６１／３８４，５８３号（２０１０年９月２０日出願）に記載のシステムおよび方法とともに使用され得る。上記の先に出願された出願の各々の開示は、その全体が本明細書に参照することによって援用される。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
（概要）
共同する必要性は、企業がそのデータを共有することを要求する。この共有する要求は、維持することが高コストであり、拡張しないレガシーストーブパイプアーキテクチャによって複雑化される。これらの複雑なインフラストラクチャは、リスク軽減および障害回復条件および方針によってより制限的にされる。さらに、これらの制限は、直接的に、不良なリソース利用、高価なポイント製品、および一貫性のない情報共有につながる。レガシーストーブパイプ環境の重要な要因は、データの機密性、可用性、および完全性を保護する必要性であった。この環境が経時的に進化するにつれて、セキュリティの懸念および脆弱性により、情報共有および共同が限定されてきた。経時的に、これらのレガシー環境は、情報共有および共同をさらに制限する多数の臨時セキュリティ修正を要求してきた。しかしながら、これらの修正は、データ可用性とデータセキュリティとの間のトレードオフの根本原因に対処していない。
【０００４】
既存の情報保証（ＩＡ）ソリューションは、複雑で、拡張し難く、セキュリティの脆弱

性に反応する。設計によって、これらのソリューションは、データセキュリティおよび可用性の両方を提供することができない。そのようなＩＡソリューションに基づく障害回復計画は、しばしば劣っており、めったに効果的に実装されず、維持することが高コストであり、企業によって共有されるデータの量が増大するにつれて拡張することが困難である。

【０００５】

あるデータセキュリティソリューション、例えば、ＶＰＮおよびトークンベースのインフラストラクチャは、高価であり、配備および維持の両方を行う重要な課題を有する。さらに、いくつかの製品は、標的のセキュリティ問題に対処するのみであるが、管理するのが非効率的、高価、煩雑、かつ複雑である。さらに、これらのソリューションは、１つ以上のモバイルデバイスを使用してクラウドの中のデータにますますアクセスしている、遠隔に位置するエンドユーザのためのセキュアな接続性およびデータ転送といった、基本的な問題への徹底したソリューションを提供しない。

【０００６】

クラウド記憶（「クラウド」）を使用することに移行した、拡大する数の遠隔ユーザはまた、クラウドの中と、クラウドを往復してデータを輸送する時との両方で、データセキュリティのエスカレートする問題も生じている。具体的には、そのようなクラウド記憶は、公衆、私的、セキュア、またはそれらの任意の組み合わせであってもよい。さらに、クラウド記憶は、１つよりも多くの記憶プロバイダによって提供されてもよい。新しい高度なデータセキュリティ脅威に遭遇したときに、これらの脅威は、個別ユーザおよび企業にとって同様に重要である。遠隔ユーザは、記憶用の媒体としてクラウドを使用して、他者と協調する融通性を必要とするが、データをセキュリティリスクにさらすことなくそうする必要がある。

【０００７】

したがって、企業データをセキュア化する（ｓｅｃｕｒｅ）とともに、それへのアクセスを同時に提供する必要性がある。加えて、サービス途絶を伴うことなく、ユーザの場所に構わず、このセキュアなアクセスを提供する必要性がある。実際に、配備しやすく、ユーザ介入を要求せず、付加的なハードウェアの必要性を排除し、高度にセキュアであり、生産性を損なわない徹底したソリューションの必要性がある。実際に、１つの場所から別の場所への移動または輸送中である間に、データのセキュリティを依然としてサポートしながら、セキュリティがユーザ場所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】

【０００８】

したがって、本発明の一側面は、複数の周辺ハードウェアおよびソフトウェア技術の必要性を排除しながら、データを証明可能にセキュアかつアクセス可能にするサーバベースの（例えば、Ｓｅｃｕｒｉｔｙ　Ｆｉｒｓｔ　Ｃｏｒｐ．からのＢｉｔｆｉｌｅｒ）セキュアデータソリューションを提供することである。サーバベースのソリューションは、ビットレベルでセキュリティに対処する。言い換えれば、データセキュリティは、ビットレベルでデータに直接組み込まれるか、または織り込まれる。いくつかの実施形態においては、サーバベースのソリューションは、Ｗｉｎｄｏｗｓ（登録商標）またはＬｉｎｕｘ（登録商標）プラットフォーム上で作動する、ソフトウェアアプリケーションであってもよい。いくつかの実施形態においては、カーネルレベルで動作することによって、性能および使い易さの多大な向上が達成される。いくつかの実施形態においては、サーバベースのソリューションは、ハードウェアおよびソフトウェアの両方に関して、共通企業インフラストラクチャを活用することができる、関心の企業コミュニティ（ＣＯＩ）が確立されることを可能にする。セキュリティがすでにデータに織り込まれているので、データセキュリティおよびアクセス制御を損なうことなく、この共通インフラストラクチャを使用することができる。複数のＣＯＩが、同じインフラストラクチャ内に、および単一のセキュア記憶システム内に共存することができる。サーバベースのソリューションを用いると、法

廷で認識できるデータが、いずれのデバイスまたは媒体にも記憶されない。サーバベースのソリューションは、既存の企業アクセス制御システムと一体化し、現在の確立されたアクセスソリューションの修正を伴わずに、簡略化された配備を可能にしてもよい。

【０００９】

別の側面では、本発明のサーバベースのソリューションは、ハードウェアおよびソフトウェア独立型である。サーバベースのソリューションは、既存の企業ネットワーク、記憶、およびセキュリティソリューションに適用される。サーバベースのソリューションはまた、任意の協調、ＣＲＭ、およびＥＲＰ用途にも適用される。サーバベースのソリューションによって提供される内蔵セキュリティは、クラウドベースの記憶、クラウドベースのコンピューティング、およびクラウドベースのアプリケーション用のインフラストラクチャ等の新興の費用効率的な技術およびサービスの使用を可能にする。

【００１０】

本発明のサーバベースのソリューションは、Ｓｅｃｕｒｉｔｙ Ｆｉｒｓｔ Ｃｏｒｐ．のセキュアなパーサＥχｔｅｎｄｅｄ^{TM}（ＳＰχ）コア技術を活用してもよい。いくつかの実施形態においては、セキュアなパーサＳＰχは、防衛レベルのセキュリティを実現するために、多因子秘密共有アルゴリズムを利用する。データは、複数の場所に送信される（例えば、私的または公衆クラウド内で局所的および／または地理的に分散される）前に、認証され、暗号化され（ＦＩＰＳ １４０－２認定、Ｓｕｉｔｅ Ｂ準拠）、冗長ビットを追加され、完全性チェックされ、再び暗号化される。データは、任意の好適な情報分散アルゴリズム（ＩＤＡ）を使用して分割されてもよい。データは、記憶場所へ輸送中である間に隠され、アクセスのための正しい信用証明を持たないユーザにはアクセス不可能である。

【００１１】

本発明の別の側面は、セキュア化され、記憶ネットワーク内に記憶される一組のデータシェアの第１の一部を再構築する方法を含む。方法は、セキュア記憶ネットワークからデータシェアの第２の一部を回収するステップを含む。このデータシェアの第２の一部は、データを再構成するのに十分である。方法は、データシェアの第２の一部を認証するステップと、データシェアの第１の一部を使用して、一組のデータシェアに対応する暗号化データを再構築するステップとをさらに含む。方法は、暗号化データを分割することによって、一組のデータシェアを再生するステップと、再生されたデータシェアを再認証するステップとをさらに含む。方法はさらに、記憶ネットワーク内に再生されたデータシェアの少なくとも第１の一部を記憶するステップを含む。

【００１２】

いくつかの実施形態においては、分割するステップは、情報分散アルゴリズムの使用を含む。いくつかの実施形態においては、認証するステップは、認証キーの使用を含む。いくつかの実施形態においては、一組のデータシェアの再生は、分割キーの使用を含む。いくつかの実施形態においては、記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む。いくつかの実施形態においては、ヘッダは、シェアの中の全てよりも少ないヘッダに対応する。

【００１３】

いくつかの実施形態においては、再認証するステップは、認証に使用される第１の認証キーとは異なる第２の認証キーの使用を含む。いくつかの実施形態においては、この過程は、セキュア記憶ネットワークからデータシェアの第２の一部と関連付けられるヘッダを回収するステップと、回収されたヘッダからキー暗号化キーを抽出するステップと、キー暗号化キーで第２の認証キーを暗号化するステップと、記憶ネットワークの中の再生されたデータシェアのヘッダ内に暗号化された第２の認証キーを記憶するステップとを含む。

【００１４】

いくつかの実施形態においては、再生するステップは、一組のデータシェアを再生するために使用された第１の分割キーとは異なる第２の分割キーの使用を含む。いくつかの実

施形態においては、この過程は、セキュア記憶ネットワークからデータシェアの第２の一部と関連付けられるヘッダを回収するステップと、回収されたヘッダからキー暗号化キーを抽出するステップと、キー暗号化キーで第２の分割キーを暗号化するステップと、記憶ネットワークの中の再生されたデータシェアのヘッダ内に暗号化された第２の分割キーを記憶するステップとを含む。

【００１５】

別の側面では、本発明は、データをセキュア化するためのシステムに関する。システムは、データを記憶するためのメモリと、データ分割およびデータ暗号化のうちの少なくとも１つを行うように構成される、メモリに連結されるメインプロセッサと、メインプロセッサおよびメモリに連結されるコプロセッサとを含む。コプロセッサは、解析されたデータを暗号化すること、または暗号化データを復号することのうちの少なくとも１つを含む、専用のセキュア解析機能を果たすように構成される。いくつかの実施形態においては、システムは、コプロセッサに連結されるフィールドプログラマブルゲートアレイを含む。ＦＰＧＡは、解析されたデータを暗号化すること、または暗号化データを復号することのうちの少なくとも１つを行う。いくつかの実施形態においては、コプロセッサは、ＰＣＩｅバスを介してメインプロセッサに連結される。いくつかの実施形態においては、コプロセッサは、ＨＴバスを介してメインプロセッサに連結される。

【００１６】

別の側面では、本発明は、携帯用デバイスを使用してデータをセキュア化するための方法に関する。方法は、少なくとも部分的に暗号化キーに基づいて、一組のデータからデータの少なくとも２つの部分を生成するステップと、携帯用デバイス上にキーを記憶するステップとを含む。データの２つの部分およびキーは、一組のデータを再構成するのに十分である。いくつかの実施形態においては、携帯用デバイスは、取外し可能記憶デバイスである。いくつかの実施形態においては、取外し可能記憶デバイスは、ユニバーサルシリアルバス（ＵＳＢ）インターフェースを介してエンドユーザデバイスに連結する。いくつかの実施形態においては、方法はさらに、携帯用デバイス上にデータの少なくとも２つの部分を記憶するステップを含む。

【００１７】

別の側面では、本発明は、携帯用デバイスを使用してデータをセキュア化するための方法に関する。方法は、少なくとも部分的に暗号化キーに基づいて、一組のデータからデータの少なくとも２つの部分を生成するステップと、携帯用デバイス上に生成されたデータ部分の少なくとも一部分を記憶するステップとを含む。データの部分およびキーは、一組のデータを再構成するのに十分である。いくつかの実施形態においては、携帯用デバイスは、取外し可能記憶デバイスである。いくつかの実施形態においては、取外し可能記憶デバイスは、ユニバーサルシリアルバス（ＵＳＢ）インターフェースを介してエンドユーザデバイスに連結する。いくつかの実施形態においては、方法はさらに、携帯用デバイス上にキーを記憶するステップを含む。

【００１８】

いくつかの実施形態においては、１つ以上の暗号化キーは、ＵＳＢメモリデバイス等のユーザデバイス上に記憶されてもよい。これらの暗号化キーは、エンドユーザデバイス自体の上、または他の場所に、例えば、公衆または私的クラウド記憶の中に記憶されたデータを暗号化または復号するために使用されてもよい。例えば、ユーザは、ＵＳＢメモリデバイス上に暗号化キーを記憶し、Ｄｒｏｐｂｏｘによって提供される公衆クラウドの中で遠隔に記憶された暗号化されたデータのシェアを復号するために、このキーを使用してもよい。

【００１９】

いくつかの実施形態においては、複数の明確に異なるエンドユーザデバイスのそれぞれにおいて、データ閲覧および／または再構成を可能にするために、１つ以上の暗号化キーおよび／または１つ以上のデータシェアが、ＵＳＢメモリデバイス等の携帯用ユーザデバイス上に記憶されてもよい。加えて、データシェアのうちの１つ以上はまた、クラウド記

憶デバイス上に記憶されてもよい。したがって、携帯用ユーザデバイスを保有しているユーザは、異なるエンドユーザデバイスから携帯用ユーザデバイスにアクセスして、携帯用ユーザデバイスおよび必要であればクラウド記憶デバイスにわたって分散されたシェアから、データを閲覧および／または再構築してもよい。

【００２０】

別の側面では、本発明は、第１の分割キーを使用して、情報分散アルゴリズムによって暗号化データセットから生成された、一組のデータシェアを再構築するための方法に関する。方法は、一組のデータシェアを再構築するために必要な少なくとも最小数のデータシェアを受信するステップと、最小数のデータシェアを復号することなく、最小数のデータシェアから一組のデータシェアを再構築するステップとを含む。いくつかの実施形態においては、再構築するステップは、一組のデータシェアが損なわれているという決定に応じて行われる。いくつかの実施形態においては、最小数のデータシェアは、第１の認証キーと関連付けられ、再構築するステップは、再構築された一組のデータシェアを第２の認証キーと関連付けるステップを含む。

【００２１】

いくつかの実施形態においては、方法は、最小数のデータシェアと関連付けられるヘッダを回収するステップと、回収されたヘッダからキー暗号化キーを抽出するステップと、キー暗号化キーで第２の認証キーを暗号化するステップと、再構築されたデータシェアのヘッダ内で暗号化された第２の認証キーを修復するステップとをさらに含む。いくつかの実施形態においては、最小数のデータシェアは、第１の分割キーとは異なる第２の分割キーを使用して再構築される。いくつかの実施形態においては、方法は、最小数のデータシェアと関連付けられるヘッダを回収するステップと、回収されたヘッダからキー暗号化キーを抽出するステップと、キー暗号化キーで第２の分割キーを暗号化するステップと、再構築されたデータシェアのヘッダ内で暗号化された第２の分割キーを修復するステップとをさらに含む。いくつかの実施形態においては、方法は、記憶ネットワーク上に再構築されたデータシェアのうちの少なくとも１つを記憶するステップを含む。いくつかの実施形態においては、記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む。

【００２２】

別の側面では、本発明は、スタブを記憶ネットワークのファイルシステム上の一組のデータシェアと関連付けるための方法に関する。方法は、情報分散アルゴリズムによって、暗号化データセットから一組のデータシェアを生成するステップと、生成されたデータシェアと関連付けられる一組のスタブを生成するステップとを含む。各スタブは、それぞれのデータシェアに対応し、各スタブは、それぞれのデータシェアと関連付けられる情報を含む。一組のスタブは、記憶ネットワーク上の場所に記憶される。情報は、それぞれのデータシェアの名前、それぞれのデータシェアが作成された日付、それぞれのデータシェアが最後に修正された時間、ファイルシステム内のそれぞれのデータシェアの場所へのポインタのうちの１つを含む。記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つと関連付けられる１つ以上の記憶デバイスを含む。いくつかの実施形態においては、方法はさらに、生成されたデータシェアと関連付けられる情報を閲覧するコマンドを受信するステップと、記憶ネットワーク上の場所からスタブを回収するステップと、データシェアのファイルシステムを作成するように、スタブから情報を抽出するステップと、データシェアのファイルシステムを表示するステップとを含む。いくつかの実施形態においては、スタブは、生成されたデータシェアのヘッダ内に記憶され、回収するステップは、生成されたデータシェアのヘッダを回収するステップを含む。　いくつかの実施形態においては、全てよりも少ないヘッダが回収される。いくつかの実施形態においては、スタブは、スタブディレクトリに記憶され、回収するステップは、スタブディレクトリからスタブを回収するステップを含む。いくつかの実施形態においては、方法はさらに、スタブを記憶する仮想ディレクトリまたは物理ディレクトリの指示を受信するステップを含む。いくつかの実施

形態においては、指示は、ユーザから受信される。
【００２３】
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。
【図面の簡単な説明】
【００２４】
【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、データ分割過程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、登録過程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、相互運用性過程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、認証過程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、署名過程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／復号過程を図示する。
【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過程を図示する。
【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過程を図示する。
【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過程を図示する。
【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過程、およびデータを伴った暗号化マスターキーの記憶を図示する。

【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キーを記憶するための過程を図示する。
【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キー過程、およびデータを伴った暗号化マスターキーの記憶を図示する。
【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キーを記憶するための中間キー過程を図示する。
【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、セキュア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、セキュア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、統合されたセキュア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、統合されたセキュア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、統合されたセキュア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過程の過程フロー図である。
【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過程の過程フロー図である。
【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過程の過程フロー図である。
【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過程フロー図である。
【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過程フロー図である。
【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、シェア内のキー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、ワークグループキーを使用したシェア内のキー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、データのヘッダ生成およびデータ分割に対する簡略化した例示的な過程フローである。
【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、例示的な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、セキュア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る、例示的な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、セキュアなデータパーサがクラウドを

通してデータを送信するためのシステムに統合される、例示的な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、セキュアなデータパーサがクラウドの中でデータサービスをセキュア化するために使用される、例示的な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、セキュアなデータパーサがクラウドの中でデータ記憶をセキュア化するために使用される、例示的な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、セキュアなデータパーサがネットワークアクセス制御をセキュア化するために使用される、例示的な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、セキュア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セキュア化するために使用される、例示的な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、セキュアなデータパーサがクラウドの中の複数の記憶デバイス内のデータ記憶をセキュア化するために使用される、例示的な配設の概略図である。
【図４９】図４９は、本発明の一実施形態による、セキュアなデータパーサが複数の私的および公衆クラウドの中でデータ記憶をセキュア化するために使用される、例示的な配設の概略図である。
【図５０】図５０は、本発明の一実施形態による、セキュアなデータパーサが複数の私的および公衆クラウドの中でデータ記憶をセキュア化するために使用される、例示的な配設の概略図である。
【図５１】図５１は、本発明の一実施形態による、セキュアなデータパーサがユーザの取外し可能記憶デバイスの中でデータ記憶をセキュア化するために使用される、例示的な配設の概略図である。
【図５２】図５２は、本発明の一実施形態による、セキュアなデータパーサが複数のユーザ記憶デバイスの中でデータ記憶をセキュア化するために使用される、例示的な配設の概略図である。
【図５３】図５３は、本発明の一実施形態による、セキュアなデータパーサが複数の公衆および私的クラウドならびに少なくとも１つのユーザ記憶デバイスの中でデータ記憶をセキュア化するために使用される、例示的な配設の概略図である。
【図５４】図５４は、本発明の一実施形態による、セキュアなデータパーサ用のコプロセッサ加速デバイスの概略図である。
【図５５】図５５は、本発明の一実施形態による、セキュアなデータパーサ用の図５４のコプロセッサ加速デバイスを使用する、例示的な加速過程の第１の過程フロー図である。
【図５６】図５６は、本発明の一実施形態による、セキュアなデータパーサ用の図５４のコプロセッサ加速デバイスを使用する、例示的な加速過程の第２の過程フロー図である。
【図５７】図５７は、本発明の例示的実施形態による、データがＮ個のシェアに分割されて記憶される、過程を図示する。
【図５８】図５８は、本発明の例示的実施形態による、データのシェアが再構築および／またはキー再生成される、過程を図示する。
【発明を実施するための形態】
【００２５】
本発明の一側面は、１つ以上のセキュアなサーバ、または信頼エンジンが、暗号キー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。システムは、クラウドの中の１つ以上の記憶デバイスにわたってデータを記憶し得る。クラウドは、私的記憶デバイス（特定の一組のユーザのみにアクセス可能である）または公衆記憶デバイス（記憶プロバイダと契約する任意の意識のユーザにアクセス可能である）を含んでもよい。
【００２６】
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、実際のキーおよび他の認証データを公開せず、し

たがって、キーおよびデータはセキュアに保管された状態のままである。このキーおよび認証データについて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。

【００２７】

ユーザが、ユーザ認証および文書認証ならびに他の暗号機能を行うための暗号システムを確信または信頼できることに起因して、多種多様な機能性がシステムに組み込まれて得る。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、同意を否認することから守ることができる。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得る。

【００２８】

本発明の完全な理解を促進するために、発明を実施するための形態の残りの部分は、類似要素が全体を通して類似数字で参照される図を参照して、本発明を説明する。

【００２９】

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を通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。

【００３０】

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、かつ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。

【００３１】

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通して、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通して、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。

【００３２】

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、デジタルアシスタント、携帯電話、ラップトップ、または同等物等のパーソナルモバイルコンピューティングデバイス、無線通信デバイス、スマートカード、組み込みコンピューティングデバイス、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。

【００３３】

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キー等であるが、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つ以上のセキュアなサーバを備える。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、登録中等のそのとき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。

【００３４】

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を通して信頼エンジン１１０に転送される。

【００３５】

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キーは、信頼エンジン１１０外で使用可能とならず、それにより、暗号キーの完全性を保証する。

【００３６】

一実施形態によれば、信頼エンジン１１０は、暗号キーを生成し、記憶する。別の実施形態によれば、少なくとも１つの暗号キーは、各ユーザと関連付けられる。また、暗号キーは、公開キー技術を含み、ユーザと関連付けられる各秘密キーは、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キーを使用して暗号機能を果たしてもよい。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通して暗号機能にアクセスすることを有利に可能にする。

【００３７】

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に生成されたキーペアを使用して、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一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キーペアを使用する。

【００３８】

当業者であれば、暗号キーが、対称キー、公開キー、および秘密キー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、前述のキーが、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。

【００３９】

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通して、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。

【００４０】

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。この実施形態においては、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、キー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。

【００４１】

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。典型的なウェブサーバは、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してもよい。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。

【００４２】
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。

【００４３】
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。本開示の全体を通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においては、インターネットルーティングハブは、当技術分野において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。

【００４４】
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、典型的には、「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。

【００４５】
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。

【００４６】
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。

【００４７】

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を通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。

【００４８】

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、典型的には、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通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。

【００４９】

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の全体を通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とき等に、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。

【００５０】

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。本開示の全体を通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、「完全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とき、通信は１／２または完全ＳＳＬを含んでもよい。

【００５１】

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の全体を通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。

【００５２】
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、暗号キーおよび登録認証データを記憶する。暗号キーは、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。
【００５３】
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技術等のセキュアな通信を含む。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。
【００５４】
前述のように、保管場所２１０は、複数のセキュア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においては、セキュア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キー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、暗号キー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、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、任意の暗号キー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。
【００５５】
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。
【００５６】
一実施形態によれば、認証エンジンへの通信は、例えば、ＳＳＬ技術等のセキュアな通信を含む。加えて、例えば、公開キー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の公開キーを用いて、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の公開キーを用いて、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キーのみを使用することができる。
【００５７】
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、公開キー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キーを有利に発行し得る。このようにして、少なくとも秘密暗号キーが信頼エンジン１１０外

で利用可能とならないように、暗号キーは暗号エンジン２２０において生成され、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キー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、分割過程は、記憶されたキーが暗号エンジン２２０外で利用可能ではないことを保証する。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。

【００５８】

一実施形態によれば、暗号エンジンを往復する通信は、ＳＳＬ技術等のセキュアな通信を含む。加えて、データを転送する、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。

【００５９】

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キー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。

【００６０】

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内に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。

【００６１】

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において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技術を通して、有利にセキュア化されてもよい。

【００６２】

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、暗号キーに対応するデータ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キー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保証する機構を含む。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キー暗号化を用いて、有利に暗号化されてもよい。

【００６３】

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。

【００６４】

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つの秘密キー５１０へのアクセスを含む。秘密キー５１０は、例えば、認証エンジン２１５の対応する公開キー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。

【００６５】

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と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。

【００６６】

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一致のみを返信し得る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、部分的一致、例えば、９０％一致、７５％一致、または１０％一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。

【００６７】

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否かを決定することが望ましい。

【００６８】

ときには、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。

【００６９】

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。

【００７０】

確信レベルおよびトランザクションの値と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。

【００７１】

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済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済ます自動試行を、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を通して、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。

【００７２】

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。

【００７３】

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、暗号キーデータを処理する。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せら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。

【００７４】

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、暗号キー生成、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ベースの公開キーシステム、または多数の代替的なキー管理システム等の公開キー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、公開キー暗号化、対称キー暗号化、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、シームレスな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。

【００７５】

当業者であれば、暗号機能性が、概して暗号キー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。

【００７６】

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を通して、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。

【００７７】

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。

【００７８】

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、解読不可能であるので、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においては、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。

【００７９】

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。

【００８０】

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、および暗号キー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過程８００のフローチャートを図示する。図８に示されるように、データ分割過程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、あるいは一組のビット「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。

【００８１】

加えて、ステップ８２０では、データ分割過程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２値組み合わせを備えてもよく、数字Ｄは、Ｃ　ＸＯＲ　Ｓという２値組み合わせを備えてもよい。ＸＯＲ関数または「排他的論理和」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、データ分割過程８００は、対合のうちのいずれも、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が対合される、ステップ８３５へと進む。例えば、番号は、ＡＣ、ＡＤ、ＢＣ、およびＢＤのように対合される。一実施形態によれば、前述の対合のそれぞれは、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、前述の対合のそれぞれは、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のデータ分割過程８００中に、対合ＡＣは、例えば、Ｄ２のＩＰアドレスの無作為選択を通して、保管場所Ｄ２に送信されてもよい。次いで、第２のデータ分割過程８００中に、対合ＡＣは、例えば、Ｄ４のＩＰアドレスの無作為選択を通して、保管場所Ｄ４に送信されてもよい。加えて、対合は、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。

【００８２】

前述の内容に基づいて、データ分割過程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。

【００８３】

データ分割過程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、データ分割過程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、データ分割過程は、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通してＡおよびＢを無作為に分配してもよい。また、データ分割過程８００は、付加的な乱数の生成を通して、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、分割過程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回復しにくくし、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、固定された一組の異なるサイズ、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。

【００８４】

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。この過程は、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のデータ分割過程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の対合は、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。

【００８５】

前述のデータ分割および集約過程に基づいて、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とき、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が秘密暗号キーデータを含むとき、使用可能な無作為化されていない秘密暗号キーデータは、暗号エンジン２２０のみで利用可能

である。

【００８６】

データ分割および集約過程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、公開キー暗号化は、データ記憶設備Ｄ１乃至Ｄ４においてデータをさらにセキュア化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においてもあることが、当業者にとって容易に明白である。

【００８７】

図９Ａは、本発明の実施形態の側面による、登録過程９００のデータフローを図示する。図９Ａに示されるように、登録過程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、問い合せ過程中に、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保証する。ユーザＩＤが一意ではないとき、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文書を通して、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の公開キーを用いて符号化される。

【００８８】

一実施形態によれば、ユーザは、登録過程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　ユーザ等の特定の個人として自分を登録する。Ｊｏｅ　ユーザがＭｅｇａ　Ｃｏｒｐ．のＣＥＯであるＪｏｅ　ユーザとして登録することを所望するとき、次いで、この実施形態によれば、Ｊｏｅ　ユーザは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、登録過程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、前述の実施例では、信頼エンジン１１０は、Ｊｏｅ　ユーザの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　ユーザ、慈善団体のメンバーであるＪｏｅ　ユーザ、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、一組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。

【００８９】

登録過程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。

【００９０】

他方で、登録過程は、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過程９００中に発生してもよいことを本明細書の本開示から理解するであろう。

【００９１】

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、従来の完全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の秘密キーを使用して、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２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。

【００９２】

しばしば登録過程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キーを含む。

【００９３】

ユーザがデジタル証明書を登録時に要求しようと、別のときに要求しようと、要求は信頼エンジン１１０を通して認証エンジン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、暗号キーまたはキーペアを生成するように暗号エンジン２２０に命令する。

【００９４】

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つの暗号キーを生成する。一実施形態によれば、暗号処理モジュール６２５は、一方のキーが秘密キーとして使用され、もう一方が公開キーとして使用される、キーペアを生成する。暗号エンジン２２０は、秘密キー、および一実施形態によれば公開キー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。

【００９５】

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、典型的には、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。

【００９６】
暗号キーを発行した後はいつでも、暗号エンジン２２０は、暗号キー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、前述で説明されるデータ分割過程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。
【００９７】
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、完全ＳＳＬまたは公開キー暗号化技術を有利に含んでもよい。また、登録過程は、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。
【００９８】
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キーを発行するので、各証明書は秘密キーに対応する。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通して、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一致する秘密キーを所有するか否かを決定してもよい。そのような証明書が存在するとき、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キーを使用してもよい。そのような証明書が存在しないとき、暗号処理モジュール６２５は、適切なキー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が適切なキーを使用して暗号機能を果たすことを保証する前述のステップを開示する、相互運用性過程９７０のフローチャートを図示する。
【００９９】
図９Ｂに示されるように、相互運用性過程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。
【０１００】
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、対称キー、公開キー、２５６ビットキー等の強力な暗号化キー、あまりセキュアではないキー、または同等物等の１つ以上のキー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キーのうちの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。
【０１０１】
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、相互運用性過程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一致する証明書を所有するか否かを決定する。ユーザが一致する証明書を有する、例えば、信頼エン

ジン１１０が、例えば、その以前の記憶を通して、一致する証明書にアクセスできるとき、暗号処理モジュール８２５は、一致する秘密キーも信頼エンジン１１０内に記憶されていることを知る。例えば、一致する秘密キーは、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、一致する秘密キーが、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、一致する秘密キーを使用してもよい。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。

【０１０２】

ユーザが一致する証明書を所有しないとき、相互運用性過程９７０は、ユーザが相互認定された証明書を所有するか否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、登録過程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とき、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。

【０１０３】

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一致させてもよい。

【０１０４】

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、相互運用性過程９７０は、ステップ９７６へと進み、相互認定された公開キー、秘密キー、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、相互運用性過程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否かを決定する。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。

【０１０５】

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に提供したとき、相互運用性過程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、登録過程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に利用可能なキーペアのうちの１つ以上から、１つ以上の公開キー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つ以上の新しいキー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キーを使用してもよい。

【０１０６】

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、相互運用性過程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キー、秘密キー、または両方を使用して、暗号措置または機能を果たす。

【０１０７】

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に提供していないとき、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否かを決定する。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。

【０１０８】

より低い要件を有する前述の証明機関が存在するとき、相互運用性過程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とき、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、相互運用性過程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。

【０１０９】

前述の相互運用性過程９７０を通して、暗号処理モジュール６２５は、異なる暗号システム間で、シームレスな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、相互運用性過程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、相互運用性過程９７０は、相互運用性を保証すること、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。

【０１１０】

図１０は、本発明の実施形態の側面による、認証過程１０００のデータフローを図示する。一実施形態によれば、認証過程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、認証過程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。

【０１１１】

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。

【０１１２】

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。

【０１１３】

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の公開キーを用いて、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。

【０１１４】

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、好ましい完全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通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、その秘密キー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。

【０１１５】

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一致しない場合、より低い確信の一致が生じる。特定の実施形態においては、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。

【０１１６】

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、認証過程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を完了するの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。

【０１１７】

前述の内容に基づいて、認証過程１０００は、有利に機密データをセキュアに保持し、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の内側のみで集約される。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の秘密キー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否かさえも分からない場合がある。

【０１１８】

認証過程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、認証過程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、認証過程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過程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。

【０１１９】

また、認証過程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、よりセキュアな暗号システム１００を作成する。

【０１２０】

加えて、認証過程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、もはや関連性を通して思い出す必要がないので、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、認証過程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。

【０１２１】

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。

【０１２２】

さらに別の実施形態においては、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。

【０１２３】

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、様々な時に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ごとに、周期的に、１つ以上のセッションごとに、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ごとに、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。

【０１２４】

図１１は、本発明の実施形態の側面による、署名過程１１００のデータフローを図示する。図１１に示されるように、署名過程１１００は、図１０を参照して前述される認証過程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、署名過程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、署名過程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とき等の任意の他の場合に、有利に使用されてもよい。

【０１２５】

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、署名過程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保証する。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一致するか否か決定するために、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否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。

【０１２６】

ステップ１１０３において、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一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保証する。

【０１２７】

ステップ１１０５において、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技術を通して伝達されるＸＭＬ文書を備える。

【０１２８】

ステップ１１１０において、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キー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キーを決定し、適切な一致キー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過程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に記憶されたキーのうちの１つ以上を有利に要求してもよい。

【０１２９】

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キーを有利に要求する。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。この実施形態においては、信頼エンジン１１０は、認証過程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に属するキー等の信頼エンジン１１０の暗号キーを要求する。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。この実施形態においては、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。この実施形態においては、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キー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に対応する暗号キーの集約を有利に要求してもよい。

【０１３０】

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キーを要求する。この実施形態によれば、署名過程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、認証過程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。

【０１３１】

前述の内容に基づいて、ステップ１１１０において、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から暗号キーを要求した。ステップ１１１５において、データ記憶設備Ｄ１乃至Ｄ４が、署名当事者に対応する暗号キー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の暗号キーを用いて、有利に多重暗号化されてもよい。

【０１３２】

ステップ１１２０において、暗号エンジン２２０が、署名当事者の前述の暗号キーを集約し、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。署名過程１１００のステップ１１２５において、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において、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において、トランザクションエンジン２０５が、トランザクションＩＤ、認証が成功したか否かという指示、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、その秘密キー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。

【０１３３】

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。署名過程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、署名過程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所望してもよい。そのような実施形態においては、署名過程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。

【０１３４】

加えて、当業者であれば、署名過程１１００のステップ１１０５乃至１１２０が、図９Ｂの相互運用性過程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。

【０１３５】

図１２は、本発明の実施形態の側面による、暗号化／復号過程１２００のデータフローを図示する。図１２に示されるように、復号過程１２００は、認証過程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、認証過程１０００は、認証要求に同期セッションキーを含む。例えば、従来のＰＫＩ技術では、公開および秘密キー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、対称キー暗号システム、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キー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、同期セッションキーを生成し、より単純かつ迅速な対称キー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、受信者の公開キーを用いてセッションキーを暗号化する。暗号化されたセッションキーは、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、セッションキーを復号するために自分の秘密キーを使用し、次いで、メッセージを復号するためにセッションキーを使用する。前述の内容に基づいて、より単純かつ迅速な対称キーシステムが、暗号化／復号処理の大部分に使用される。したがって、復号過程１２００において、復号は、同期キーがユーザの公開キー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キーは、認証要求に含まれる。

【０１３６】

復号過程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キーを暗号エンジン２２０に転送する。ステップ１２１０において、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、ユーザの暗号キーデータを要求する。ステップ１２１５において、各データ記憶設備Ｄ１乃至Ｄ４が、暗号キー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の公開キーを用いて暗号化される。

【０１３７】

復号過程１２００のステップ１２２０において、暗号エンジン２２０が、暗号キーを集約し、それを用いてセッションキーを復号する。ステップ１２２５において、暗号エンジンが、セッションキーを認証エンジン２１５に転送する。ステップ１２２７において、認証エンジン２１５が、復号されたセッションキーを含む認証要求を満たし、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において、トランザクションエンジン２０５が、セッションキー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キーを使用する。

【０１３８】

復号過程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、復号過程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、復号過程１２００は、同期キー暗号化を差し控え、完全公開キー技術に依存してもよい。そのような実施形態においては、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。

【０１３９】

暗号化／復号過程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において、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、ユーザの公開キー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キー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キーを使用するので、要求アプリケーションまたはベンダは、この要求を行う。登録過程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、暗号化過程１２００のステップ１２４０において、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において、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において、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、暗号化過程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キーのみを必要とし、いずれの機密データも要求していないためである。

【０１４０】

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、登録過程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／復号過程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／復号過程１２００のステップ１２２０および１２３５乃至１２５０が、図９Ｂの相互運用性過程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。

【０１４１】

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。

【０１４２】

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。

【０１４３】

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。

【０１４４】

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１３２０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。

【０１４５】

前述に基づいて、信頼エンジンシステム１３００は、認証過程を行うために、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過程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。

【０１４６】

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。

【０１４７】

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。

【０１４８】

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。

【０１４９】

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、認証過程中に、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ので、これらの通信の全てを図示するわけではない。認証過程を続けて、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一致するか否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。

【０１５０】

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一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。

【０１５１】

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保証する。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。

【０１５２】

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。

【０１５３】

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、秘密暗号キー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、秘密キーをユーザに公開してもよく、秘密キーは、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キーペアを有利に発行し、次いで、新しい暗号キーペアの秘密キーを公開してもよい。次いで、いったん秘密暗号キーが公開されると、信頼エンジン１１０は、もはや信頼エンジン１１０によってセキュア化可能ではなくなるので、そのような秘密キーの内部有効使用を即時に失効させる。

【０１５４】

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。

【０１５５】

前述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。

【０１５６】

前述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

過程である。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。

【０１５７】

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。

【０１５８】

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、他の誰かの指紋に一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。

【０１５９】

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過程を広く指す。「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。

【０１６０】

図１０を参照して、ユーザを認証する過程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過程の一部は、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。この過程の１つの特定の実施形態を図１６に示し、以下で説明する。

【０１６１】

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において認証エンジン２１５によって受信される。これらのデータの両方は、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において、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一部と比較されるために必要である（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）。

【０１６２】

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、登録過程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り得る手段（例えば、ユーザが現在の場所に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的に認証するために、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。

【０１６３】

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。

【０１６４】

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。

【０１６５】

図１６に示されるように、いったん認証データ内において表された個別認証インスタンスがステップ１６０５において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において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において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の信頼性、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一致の程度、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。

【０１６６】

認証技法の固有の信頼性は、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いている。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ので、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ので、中程度の信頼性しか有し得ない。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ので、同様に、単独で使用されると信頼性が低い。

【０１６７】

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ので、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ので、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に、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。

【０１６８】

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、各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、具体的な実装の間に変化し得ることを認識するであろう。

【０１６９】

信頼性が評価され得る第２の要素は、登録の信頼性である。これは、前述において参照される「等級別登録」過程の一部である。この信頼性因子は、最初の登録過程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、データが、登録に際して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。

【０１７０】

異なるレベルの信頼性を有する他の登録技法は、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。

【０１７１】

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過程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。

【０１７２】

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一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。

【０１７３】

前述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。一実施形態においては、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。

【０１７４】

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。

【０１７５】

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一致を反映する。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一致するか否かの基本的な質問である。通常、データが一致しないとき、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。

【０１７６】

例えば、パスワードの一致は、概して、２値様式で評価される。言い換えれば、パスワードは、完全一致または一致失敗である。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一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とき、コンパレータ５１５によって返信される認証の信頼性は、典型的には、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。

【０１７７】

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２値認証符号となる傾向がある。

【０１７８】

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、２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一致してもよい。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ので、データは、完璧とは言えない程度に一致してもよい。（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ので、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一致するが、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一致は、望ましくは、コンパレータ５１５によって部分一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％一致であるといわれ、声紋は６５％一致であるといわれ、質問表は８０％一致であるといわれる場合がある。

【０１７９】

コンパレータ５１５によって生成されるこの尺度（一致の程度）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、前述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得る因子のうちの１つにすぎない。いくらかの部分的な程度での一致が決定されてもよいものの、最終的には、部分一致に基づいて２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、一致の程度が一致の特定の閾値レベルに合格するか否かに基づいて、２値、すなわち、完全一致（１００％）または一致失敗（０％）のいずれか一方として、部分

一致を取り扱うことも可能である。そのような過程は、そうでなければ部分一致を生成する、システムの一致の単純な合格／失敗レベルを提供するために使用されてもよい。

【０１８０】

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。前述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。

【０１８１】

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否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とき）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とき）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ので、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。

【０１８２】

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。

【０１８３】

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。

【０１８４】

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において前述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。

【０１８５】

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通して送られ（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一致が良好である（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。

【０１８６】

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。

【０１８７】

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、前述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において前述で説明されるように評価される。

【０１８８】

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一致の程度は、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。）

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。

【０１８９】

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、この過程は、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。）

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、前述で説明される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。

【０１９０】

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の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）。

【０１９１】

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所望してもよい。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。

【０１９２】

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。

【０１９３】

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過程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。

【０１９４】

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。

【０１９５】

前述で説明される過程は例示的にすぎず、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。

【０１９６】

本発明のさらなる側面では、前述で説明される過程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とき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。この過程は、本明細書では「信頼裁定」と呼ばれる。

【０１９７】

信頼裁定は、図１０および１１を参照して前述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２値認証を提供する。これらの状況等の状況では、肯定的な認証をセキュア化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。

【０１９８】

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。

【０１９９】

信頼裁定の過程は、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過程が、図１７に示されるように発生する。単純な２値認証が行われる状況では、図１７に示された過程は、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を参照して前述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。

【０２００】

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。

【０２０１】

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。

【０２０２】

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ので、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。

【０２０３】

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。

【０２０４】

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、過程は、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。

【０２０５】

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、この過程は、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ので、過程は、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、信頼裁定過程は、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。

【０２０６】

前述のように、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セキュア化しようとして、ベンダとユーザとの間の交渉を仲介する過程である。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否か、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。

【０２０７】

裁定が可能ではない、そのような状況では、過程は、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。

【０２０８】

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。

【０２０９】

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。

【０２１０】

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。

【０２１１】

加えて、ステップ１８２０において、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することのみを所望してもよい。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高いレベルに依然として正常に認証してもよい。

【０２１２】

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。

【０２１３】

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ので、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。

【０２１４】

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ので、ベンダ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所望してもよい。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所望してもよく、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所望してもよい。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否かを決定する際に評価されてもよい。

【０２１５】

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。過程はここから続き、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での信頼裁定過程に戻るか、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。

【０２１６】

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所望するか否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、デフォルトの一組の要件を使用していてもよいので、有益であってもよい。

【０２１７】

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ので、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所望してもよい。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、前述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。

【０２１８】

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、許可される場合に前述で論議されるように試行されてもよい。

【０２１９】

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前述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前述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。

【０２２０】

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。前述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。

【０２２１】

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ので、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。

【０２２２】

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、過程が前述で説明されるように続く。

【０２２３】

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のみされる場合がある。

【０２２４】

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における信頼裁定過程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、裁定過程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、過程が所望に応じて繰り返されてもよい。

【０２２５】

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。

【０２２６】

前述で説明され、図１６－１８で示される過程は、信頼エンジン１１０を参照して前述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、前述で説明される裁定を仲介するために、セキュアな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。

【０２２７】

図１９に関する以下の説明は、前述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過程を図示する。前述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、図示された過程は、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。

【０２２８】

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所望する。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前述で説明されるように使用される、認証データも提供する。

【０２２９】

ステップ１９１０において、認証データが、前述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、ユーザの秘密キー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。

【０２３０】

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。

【０２３１】

前述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一致しない場合、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に正常に認証するために、信頼裁定が行われてもよい。
【０２３２】
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を参照して前述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。
【０２３３】
信頼エンジン１１０は、ユーザの秘密キー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の秘密キー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（ユーザの秘密キー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の秘密キー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。
【０２３４】
信頼エンジン１１０は、同様に、ステップ１９７０でベンダの秘密キー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。
【０２３５】
前述の内容に加えて、本発明の付加的な側面は、前述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。
【０２３６】
例えば、典型的なシステム上で、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、一組の機能呼び出しを提供する。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。
【０２３７】
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、特定のキー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。

【０２３８】
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、前述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。

【０２３９】
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を通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を通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。

【０２４０】
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は順に、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。

【０２４１】
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を通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。

【０２４２】
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。

【０２４３】
別個の実施形態においては、本発明は、任意のデータセットで本発明のデータセキュア化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においては、本明細書ではセキュア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

ルまたはセキュアなデータパーサは、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。この解析過程は、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。

【０２４４】

本発明の解析過程は、一実施形態においては、モジュラー階層状に設計されてもよく、任意の暗号化過程が、本発明の過程での使用に好適である。本発明の解析および分割過程のモジュラー階層は、１）暗号分割し、分散され、複数の場所でセキュアに記憶される、２）暗号化し、暗号分割し、分散され、複数の場所でセキュアに記憶される、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、複数の場所でセキュアに記憶される、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、複数の場所でセキュア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。

【０２４５】

過程は、一実施形態においては、生成された乱数のコンテンツまたはキー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、一実施形態において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において使用されるキー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に再び記憶し、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、固定または取外し可能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、別の実施形態においては、暗号化は、分割モジュールまたはセキュア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。この実施形態において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、セキュア化される。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。暗号化キー管理は、一実施形態においては、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においては、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。

【０２４６】

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一組の値に基づいて、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、データをよりセキュア化してもよい。次いで、単位は、（無作為に、または所定の一組の値によって）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。

【０２４７】

この暗号の分割過程または暗号分割の１つの実施例は、データをサイズが２３バイトになるものと見なし、データ単位サイズは１バイトになるように選択され、シェアの数は４になるように選択される。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）を作成するようにキーが取得される。データの単位のそれぞれ（この実施例において、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の中に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、本発明の暗号分割過程で使用されてもよく、前述の実施例は、データを暗号分割するための１つの過程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。

【０２４８】

本発明の暗号分割過程の別の実施形態においては、暗号分割過程のオプションは、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回復するためにシェアの一部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回復するために、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。本発明の暗号分割過程では、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。

【０２４９】

本発明の暗号分割過程の一実施形態においては、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。前述で説明される「４分の３」暗号分割過程を使用すると、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ので、欠落データ単位がない元のデータを再構築または回復するのに十分である。本明細書において説明されるように、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、キーに基づいて対応するシェアに記憶される。この実施形態においては、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つのキーが使用される。本発明の暗号分割過程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の一組の乱数（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の別の一組の乱数（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一組の乱数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と３との間の第３のシェア数を作成するために、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）ＭＯＤ４＝第３のシェア数

である。

【０２５０】

主要シェア数が０と３との間であり、バックアップシェア数が１と３との間である前述で説明される実施形態においては、第３のシェア数が主要シェア数とは異なることを保証する。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に配置された後に、またはシェアが満杯になった後に行われてもよい。

【０２５１】

本明細書で説明される種々の暗号分割過程およびデータ入れ替え過程、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。

【０２５２】

本明細書において説明される暗号分割過程を行うソースコードの一実施形態の実施例は、以下のようである。

```
ＤＡＴＡ［１：２４］－分割されるデータを有するバイトのアレイ
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過程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。

【０２５３】

２組の数を生成し、ＰｒｉｍａｒｙＳｈａｒｅは０から３であり、バックアップＳｈａｒｅは１から３である。次いで、前述で説明される暗号分割と同じ過程を用いて、各データ単位をｓｈａｒｅ［ｐｒｉｍａｒｙｓｈａｒｅ［１］］およびｓｈａｒｅ［（ｐｒｉｍａｒｙｓｈａｒｅ［１］＋ｂａｃｋｕｐｓｈａｒｅ［１］）ｍｏｄ４に入れる。この方法は、任意のサイズＮにカクダイ縮小可能となり、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。

【０２５４】

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。

【０２５５】

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、キー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つ以上のキーに依存する。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。本発明のセキュアなデータパーサは、一実施形態においては、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、別の実施形態においては好ましくは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取外し可能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、セキュア化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。

【０２５６】

本発明のセキュア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、本発明のセキュアなデータパーサは、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、一実施形態においては、セキュアなデータパーサは、外部セッションキー管理またはセッションキーのセキュア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セキュア化するので、および暗号化目的で使用されるパーサマスターキーが生成される。結果として生じるセキュア化されたデータの中のパーサマスターキーの組み込みは、ワークグループ、企業、または拡張聴衆内の個人によるセキュア化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。

【０２５７】

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キーを記憶するように、データパーサによってデータにおいて行われる過程のステップを示す。

【０２５８】

１．セッションマスターキーを生成し、ＲＳ１ストリーム暗号を使用してデータを暗号化する。

【０２５９】

２．セッションマスターキー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。

【０２６０】

３．方法のこの実施形態においては、セッションマスターキーは、セキュア化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。パーサマスターキーのパターンに従ってセッションマスターキーを分離し、キーデータを暗号化された解析データに付加する。

【０２６１】

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キー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キーを生成する。

【０２６２】

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キーを記憶する。シェア１はキー４を得て、シェア２はキー１を得て、シェア３はキー２を得て、シェア４はキー３を得る。

【０２６３】

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。

【０２６４】

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、または回復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セキュア化されてもよい。

【０２６５】

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つ以上の別個のキー管理テーブルにセッションマスターキーデータを記憶するように、セキュアなデータパーサによってデータにおいて行われる、過程のステップを含む。

【０２６６】

１．セッションマスターキーを生成し、ＲＳ１ストリーム暗号を使用してデータを暗号化する。

【０２６７】

２．セッションマスターキー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。

【０２６８】

３．本発明の方法のこの実施形態においては、セッションマスターキーは、データ保管場所で別個のキー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キーを別個のキー管理テーブルに記憶する。パーサマスターキー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。

【０２６９】

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。

【０２７０】

５．４つのデータシェアのそれぞれにストリーム暗号キーを生成する。

【０２７１】

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キーを記憶する。シェア１はキー４を得て、シェア２はキー１を得て、シェア３はキー２を得て、シェア４はキー３を得る。

【０２７２】

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。

【０２７３】

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において行われてもよい。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、または回復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セキュア化されてもよい。

【０２７４】

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キーを記憶するために、セキュアなデータパーサによってデータにおいて行われる過程のステップを示す。

【０２７５】

１．認証されたユーザと関連付けられるパーサマスターキーにアクセスする。

【０２７６】

２．一意のセッションマスターキーを生成する。

【０２７７】

３．パーサマスターキーおよびセッションマスターキーの排他的論理和関数から中間キーを導出する。

【０２７８】

４．中間キーを用いて入力される既存または新しい暗号化キーアルゴリズムを使用した、データの任意的な暗号化。

【０２７９】

５．中間キー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。

【０２８０】

６．方法のこの実施形態においては、セッションマスターキーは、セキュア化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。パーサマスターキーのパターンに従ってセッションマスターキーを分離し、キー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。

【０２８１】

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キーの複数部分を含有する。

【０２８２】

８．任意に、４つのデータシェアのそれぞれに暗号化キーを生成する。

【０２８３】

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キーを記憶する。例えば、シェア１はキー４を得て、シェア２はキー１を得て、シェア３はキー２を得て、シェア４はキー３を得る。

【０２８４】

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。

【０２８５】

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、または回復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セキュア化されてもよい。

【０２８６】

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つ以上の別個のキー管理テーブルにセッションマスターキーデータを記憶するように、セキュアなデータパーサによってデータにおいて行われる過程のステップを含む。

【０２８７】

１．認証されたユーザと関連付けられるパーサマスターキーにアクセスする。

【０２８８】

２．一意のセッションマスターキーを生成する。

【０２８９】

３．パーサマスターキーおよびセッションマスターキーの排他的論理和関数から中間キーを導出する。

【０２９０】

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

【０２９１】

５．中間キー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。

【０２９２】
６．本発明の方法のこの実施形態においては、セッションマスターキーは、データ保管場所で別個のキー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キーを別個のキー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キー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。パーサマスターキー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。
【０２９３】
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。
【０２９４】
８．任意に、４つのデータシェアのそれぞれに暗号化キーを生成する。
【０２９５】
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キーを記憶する。例えば、シェア１はキー４を得て、シェア２はキー１を得て、シェア３はキー２を得て、シェア４はキー３を得る。
【０２９６】
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。
【０２９７】
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、または回復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セキュア化されてもよい。
【０２９８】
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、最もセキュア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、セキュア化されるデータと同じくらいの長さであるキーが生成されることを必要とする。この方法の使用は、セキュア化されるデータセットのサイズにより非常に長いキー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）アルゴリズムにおいては、排他的論理和関数のＸＯＲが使用される。同じ長さの２値ストリームｘおよびｙについて、ｘ　ＸＯＲ　ｙは、ｘおよびｙのビット排他論理和を意味する。
【０２９９】
ビットレベルでは、以下の
０　ＸＯＲ　０＝０
０　ＸＯＲ　１＝１
１　ＸＯＲ　０＝１
１　ＸＯＲ　１＝０
が生成される。
【０３００】
この過程の実施例は、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。過程は、ｎバイトの乱数値ａを生成し、次いで、以下の
ｂ＝ａ　ＸＯＲ　ｓ
を設定する。
【０３０１】

式を介して「ｓ」を導出できることに留意されたい。
ｓ＝ａ　ＸＯＲ　ｂ
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、セキュアな方式で破棄される。
【０３０２】
本発明のセキュアなデータパーサは、複数の別個の秘密キー値Ｋ１、Ｋ２、Ｋ３、Ｋｎ、Ｋ５を組み込む複数のＸＯＲ関数を行う、この機能を利用してもよい。動作の開始時に、セキュア化されるデータは、第１の暗号化動作を通過させられ、データ＝データＸＯＲ秘密キー５をセキュア化し、
Ｓ＝Ｄ　ＸＯＲ　Ｋ５である。
【０３０３】
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にセキュアに記憶するために、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、残りの秘密キー値を用いて各シェアで行われてもよく、例えば、セキュアなデータセグメント１＝暗号化されたデータシェア１ＸＯＲ秘密キー１であり、
ＳＤ１＝Ｓ１　ＸＯＲ　Ｋ１、
ＳＤ２＝Ｓ２　ＸＯＲ　Ｋ２、
ＳＤ３＝Ｓ３　ＸＯＲ　Ｋ３、
ＳＤｎ＝Ｓｎ　ＸＯＲ　Ｋｎ
である。
【０３０４】
一実施形態においては、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キーは、異なるデータ保管場所
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
に記憶される。
【０３０５】
加えて、各シェアには、元のセッション暗号化キー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キー管理の実施例では、元のセッションマスターキーは、インストール依存パーサマスターキー（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キーの実施例では、セッションマスターキーは、インストール依存パーサマスターキー（ＳＫ１、ＳＫ２、ＳＫ３、ＳＫｎ）のコンテンツに従って、「ｎ」個のシェア
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
に分割される。
【０３０６】

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キーおよびパーサマスターキーにアクセスせずに、元の情報を再構築または回復するという可能性はない。

【０３０７】

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、別の実施形態においては、秘密認証材料を形成するよう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、キーサイズが記憶されるデータと同じサイズであるので、セキュア化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。

【０３０８】

（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、擬似乱数のキーがはるかに小さいシード数から生成されることである。ＲＳ１ストリーム暗号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関数で使用されるキー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。

【０３０９】

前述のキー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に配置されている。

【０３１０】

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つのシェアにつきセキュア化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、単純により短いので、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。

【０３１１】

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。

【０３１２】

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過程を提供するようにデータをセキュア化するための、本発明の方法のステップの組み合わせである。データは、セキュアなキーで暗号化され、セキュアなキーに従って、１つ以上のシェア、一実施形態においては４つのシェアに分割される。セキュアなキーは、セキュアなキーに従って４つのシェアの中へセキュア化される、参照ポインタを用いてセキュアに記憶される。次いで、データシェアは個別に暗号化され、キーは異なる暗号化されたシェアを用いてセキュアに記憶される。組み合わせられると、本明細書で開示される方法に従ってデータをセキュア化するための過程全体が、データセキュリティのための包括的パッケージになる。

【０３１３】

本発明の方法に従ってセキュア化されるデータは、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回復され、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。

【０３１４】

１．データセットの全てのシェアまたは部分。

【０３１５】

２．データをセキュア化するために使用される方法の過程フローを再現する知識および能力。

【０３１６】

３．セッションマスターキーへのアクセス。

【０３１７】

４．パーサマスターキーへのアクセス。

【０３１８】

したがって、前述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、セキュアなインストールを計画することが望ましくてもよい。

【０３１９】

データセキュア化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、パーサマスターキーの使用によって実施されてもよい。セキュア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においては、任意の措置が講じられる前に必要とされてもよい。

【０３２０】

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、セキュアなデータパーサは、４つのシェアおよびセッションマスターキー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。

【０３２１】

（キー管理）

本発明の一実施形態においては、データセキュア化方法は、暗号化動作に３組のキーを使用する。各組のキーは、インストールに基づいて、個別キー記憶、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。使用されてもよいキーは、以下を含むが、それらに限定されない。

【０３２２】

（パーサマスターキー）

このキーは、セキュアなデータパーサのインストールと関連付けられる個別キーである。これは、セキュア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キー記憶、標準キー記憶、カスタムキー記憶、またはセキュア化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、このキーをセキュア化するために好適な種々のオプションがある。

【０３２３】

（セッションマスターキー）

セッションマスターキーは、データがセキュア化される度に生成されてもよい。セッションマスターキーは、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キー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キーは、例えば、標準キー記憶、カスタムキー記憶、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セキュア化されるか、または暗号化されたシェア内にセキュア化されてもよい。

【０３２４】

（シェア暗号化キー）

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、個別シェア暗号化キーが生成されてもよい。シェア暗号化キーは、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。

【０３２５】

本発明のデータセキュア化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、本発明のデータセキュア化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セキュア化されてもよい。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、データをセキュア化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。本発明のデータセキュア化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。

【０３２６】

本発明の別の実施形態においては、データセキュア化方法は、暗号化動作に３組のキーを使用する。各組のキーは、インストールに基づいて、個別キー記憶、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。使用されてもよいキーは、以下を含むが、それらに限定されない。

【０３２７】

（１．パーサマスターキー）

このキーは、セキュアなデータパーサのインストールと関連付けられる個別キーである。これは、セキュア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キー記憶、標準キー記憶、カスタムキー記憶、またはセキュア化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、このキーをセキュア化するために好適な種々のオプションがある。

【０３２８】

（２．セッションマスターキー）

セッションマスターキーは、データがセキュア化される度に生成されてもよい。セッションマスターキーは、中間キーを導出するためのパーサマスターキーと併せて使用される

。セッションマスターキーは、例えば、標準キー記憶、カスタムキー記憶、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セキュア化されるか、または暗号化されたシェア内にセキュア化されてもよい。

【０３２９】

（３．中間キー）

中間キーは、データがセキュア化される度に生成されてもよい。中間キーは、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。

【０３３０】

（４．シェア暗号化キー）

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、個別シェア暗号化キーが生成されてもよい。シェア暗号化キーは、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。

【０３３１】

本発明のデータセキュア化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。インターネット上において、または顧客とベンダとの間において運営される商用アプリケーションに加えて、本発明のデータセキュア化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セキュア化されてもよい。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、データをセキュア化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。本発明のデータセキュア化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。

【０３３２】

（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）

本発明のデータセキュア化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セキュア化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、データをセキュア化する方法およびコンピュータシステムを提供する。

【０３３３】

本発明のデータセキュア化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、この過程の下でセキュア化されることが可能である。本発明のデータをセキュア化する方法の拡張性、速度、およびデー多スループットは、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。

【０３３４】

本発明の一実施形態においては、データセキュア化方法は、ワークグループ環境において、以下で説明されるように利用される。一実施形態においては、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セキュア化方法は、ユーザ／グループ関係、およびユーザのグループがセキュアなデータを共有するために必要な関連秘密キー（パーサグループマスターキー）を記憶するために、信頼エンジンの秘密キー管理機能性を使用する。本発明の方法は、パーサマスターキー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セキュア化する能力を有する。

【０３３５】

一実施形態においては、付加的なキー管理およびユーザ／グループ管理プログラムが提供されてもよく、運営およびキー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。キー生成、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。別の実施形態においては、キー管理はまた、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、セキュア化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、セキュア化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、セキュア化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セキュア化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。

【０３３６】

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。パーサマスターキーが、組織へのセキュア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。パーサマスターキー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セキュア化方法は、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。

【０３３７】

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人のユーザが存在している。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。

【０３３８】

この実施例において使用することに対してセキュアなデータパーサを構成する場合、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キーを生成し、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。

【０３３９】

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。

【０３４０】

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キーにアクセスする（利用可能でない場合はキーを生成する）。

【０３４１】
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。
【０３４２】
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。
【０３４３】
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。
【０３４４】
同じ一組の措置が、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キーは、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通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。
【０３４５】
いったん共有信任状が定義されると、解析および分割過程は同じ状態のままになる。ファイル、文書、またはデータ要素がセキュア化されるとき、ユーザは、標的グループがデータをセキュア化するときに使用されるために促される。結果として生じるセキュア化されたデータは、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。
【０３４６】
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、一実施形態においては、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において使用されてもよい。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セキュア化するための本発明の方法の構成要素になってもよい。
【０３４７】
セキュアなデータパーサは、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、本発明によるセキュア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保証するために、ハッシュ値が一部分内に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、（セキュア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、セキュア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、一致する、および一致しない値の報告、一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。
【０３４８】
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。

【０３４９】

本発明のセキュアなデータパーサは、任意の好適な用途において使用されてもよい。すなわち、本明細書で説明されるセキュアなデータパーサは、計算および技術の異なる分野において種々の用途を有する。いくつかのそのような分野を以下において論議する。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セキュア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。

【０３５０】

本発明のセキュアなデータパーサは、セキュア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において有用である。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。

【０３５１】

本発明のセキュアなデータパーサは、セキュア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、セキュア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、秘密暗号化キー、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キードライブ等）、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過程に提供する（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）。

【０３５２】

本発明のセキュアなデータパーサは、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、セキュアなデータパーサ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、セキュアなデータパーサ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。セキュアなデータパーサ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、セキュアなデータパーサ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、セキュアなデータパーサ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。セキュアなデータパーサ２６０２は、本発明に従って１つ以上の記憶デバイス２６０４の間においてデータを解析および分割するために使用されてもよい。それに統合されたセキュア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。

【０３５３】

本発明のセキュアなデータパーサは、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セキュア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において記憶される。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。

【０３５４】

本発明のセキュアなデータパーサは、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、セキュア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）セキュア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。セキュア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において、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。

【０３５５】

１つの好適なアプローチでは、本発明のセキュアなデータパーサは、（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セキュアな記憶を可能にする。

【０３５６】

本発明のセキュアなデータパーサは、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においては、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。

【０３５７】
本発明のセキュアなパーサは、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においては、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、セキュア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せられることをシステムが要求してもよいので、元のメッセージはセキュアなままである。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せられてもよい。

【０３５８】
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、本発明によるセキュアなデータパーサ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に関して前述において説明されるように、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。

【０３５９】
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、本発明によるセキュアなデータパーサ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に関して前述において説明されるように、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。

【０３６０】
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においては、図２８および２９のシステムの特徴が組み合わせられてもよく、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。
【０３６１】
セキュアなデータパーサは、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において、セキュアなデータパーサは、ユーザインターフェースレベルにおいて（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セキュアなパーサの特徴の使用を制御してもよい。代替として、セキュアなパーサは、交換サーバ等のバックエンド構成要素において実装されてもよく、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。
【０３６２】
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。本発明のセキュアなデータパーサは、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。
【０３６３】
セキュアなデータパーサは、例えば、有線、無線、または物理的媒体を含む、任意の輸送媒体を通して、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、本発明のセキュアなデータパーサを利用してもよい。本発明のセキュア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セキュア化されてもよい。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、セキュア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。
【０３６４】
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、セキュア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、取外し可能ハードドライブ、フラッシュメモリを伴う家庭用電子デバイス（例えば、ＡｐｐｌｅＩＰＯＤ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。
【０３６５】

本発明のセキュアなデータパーサは、障害復旧のための能力を有するセキュリティを提供してもよい。本発明によれば、セキュア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個は、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。

【０３６６】

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エンティティに、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、それぞれ本発明のセキュア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有する２つ以上の明確に異なるエンティティが、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。

【０３６７】

本発明のセキュアなデータパーサは、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、グループ全体のキーをエンティティのグループに提供するために使用されてもよい。グループキーは、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せられることを要求されてもよい、本発明によるセキュア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、グループ間のセキュア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。

【０３６８】

このセキュア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過程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において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において伝達されてもよい、企業または他の組織にも適用可能である。

【０３６９】

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、本発明のセキュアなパーサは、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。

【０３７０】

本発明のセキュアなパーサの前述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、グループキー用途は、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、ネットワーク上において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）。

【０３７１】

本発明のセキュアなデータパーサは、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セキュア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、組み込まれたセキュア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。

【０３７２】

本発明のセキュアなデータパーサは、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においては、例えば、セキュアなデータパーサが、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、セキュア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通して得られてもよい。

【０３７３】

図３０は、例えば、セキュアなデータパーサ３０００としてのセキュアなデータパーサの例示的な実装を示す。セキュアなデータパーサ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、セキュアなデータパーサ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。セキュアなデータパーサ３０００はまた、モジュール３００４を使用して、例えば、前述で説明される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。セキュアなデータパーサ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セキュアなデータパーサ３０００に組み込まれてもよいことが、理解されるであろう。

【０３７４】

集約データバッファ３００８は、セキュアなデータパーサ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、入力をセキュアなデータパーサ３００８に提供する。修復動作では、集約データバッファ３００８は、セキュアなデータパーサ３０００の出力を記憶するために使用されてもよい。

【０３７５】

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、セキュアなデータパーサの出力を保持する。修復動作においては、分割シェアバッファは、セキュアなデータパーサ３０００への入力を保持する。

【０３７６】

能力の任意の他の好適な配設が、セキュアなデータパーサ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。

【０３７７】

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、セキュアなデータパーサ３０００によって呼び出されてもよく、またはセキュアなデータパーサ３０００を呼び出してもよい。所望であれば、セキュアなデータパーサ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キー発生器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、およびキー管理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。

【０３７８】

暗号フィードバックキー発生器３０１４は、セキュアなデータパーサ３０００の外部で、それぞれのセキュアなデータパーサの動作のために、元のセッションキーサイズ（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、一意のキーまたは乱数（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キー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キー生成に使用されてもよい。

【０３７９】

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）へのセキュアなデータパーサ３０００およびその外部モジュール（すなわち、セキュアなデータパーサ層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へのセキュアなデータパーサ層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。

【０３８０】

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において発行されるときに、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において、セキュア化されるデータが識別され、セキュアなデータパーサへ呼び出しが行われる。呼び出しは、ラッパ層３０２２を通過させられ、ステップ３１０２において、ラッパ層３０２２が、ステップ３１００において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において、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、ラッパ層３０２２における情報３１０６として）。次いで、セキュア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において、ラッパ層３０２２が、記憶された情報３１０６から、（すなわち、ステップ３１０２においてラッパ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）。

【０３８１】

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において、修復されるデータが識別され、セキュアなデータパーサ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において、ラッパ層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。ラッパ層３０２２は、ステップ３２００において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、セキュアなデータパーサ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、セキュアなデータパーサ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において、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。

【０３８２】

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回復は、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、任意の他の好適な過程、構成要素、または両方が使用されてもよい。

【０３８３】

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過程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。セッションキー３３００が生成される。セッションキー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キー３３０４が生成されてもよい。

【０３８４】

１つの好適なアプローチにおいては、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キー３３０４を用いて、または任意の他の好適な値を用いて）排他的論理和がとられてもよい。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、ビットレベルにおいて、または任意の他の好適なレベルにおいて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。

【０３８５】

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キー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キー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。

【０３８６】

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過程のブロック図である。過程は、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キー３３０４の関数として（すなわち、図３３の過程とは）逆に該部分のハッシュ値を計算することを伴う。次いで、暗号化キーが、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キー３３０４が使用される）。これは元のデータ３３０６を修復する。

【０３８７】

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キーの関数として、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。

【０３８８】

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。

【０３８９】

前述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通して、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対合の形態で）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、セッションキー、暗号フィードバックセッションキー、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、どの宛先の対合を選択するか（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。

【０３９０】

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。

【０３９１】

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、ビットごと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、セッションキー、暗号フィードバックセッションキー等）、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において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。

【０３９２】

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、ビットごと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。

【０３９３】

本発明の一実施形態においては、セキュア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、およびセキュア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）、たとえセキュアなデータパーサが、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。

【０３９４】

１つの好適なアプローチでは、セキュアなデータパーサまたはセキュア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、異なる暗号化キーで暗号化されてもよい。例えば、この特徴は、よりセキュアな「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の暗号化キーを使用して、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、それぞれの暗号化キーを有し、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、公開キーが使用されてもよい。次いで、元のデータに回復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キーが使用されてもよい。

【０３９５】

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、必須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。

【０３９６】

本発明の１つの好適な実施形態においては、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。

【０３９７】

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つのシェア間でセキュア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。

【０３９８】
セキュアなデータパーサは、セキュアな（またはほぼセキュアな）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、セキュアなデータパーサは、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。
【０３９９】
本発明の別の実施形態によれば、セキュアなデータパーサは、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、セキュアなデータパーサは、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、セキュアなデータパーサが、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。
【０４００】
１つの好適なアプローチでは、データ部分のサイズは、暗号化キー、分割キー、任意の他の好適なキー、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。
【０４０１】
以前に論議されたように、セキュアなデータパーサは、データの解析および分割においてキーを使用してもよい。明確かつ簡略にする目的で、これらのキーは、本明細書では「分割キー」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キーは、一種の分割キーである。また、以前に論議されたように、分割キーは、セキュア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セキュア化されてもよい。分割キーをセキュア化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セキュア化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キーをセキュア化するために使用されてもよく、それにより、分割キー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。
【０４０２】
同様に、任意の好適な暗号化キーが、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セキュア化されてもよい。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キー、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キー、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セキュア化されてもよい。
【０４０３】
本発明の一実施形態によれば、分割キー、暗号化キー、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、データをさらにセキュア化するために、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キーは、ＡｏＮＴアルゴリズムによって変換されてもよい。次いで、変換された暗号化キーは、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。暗号化キー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）。元の暗号化キーが回収されると、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。
【０４０４】

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キーの暗号化および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キーに、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、分割キーに適用されてもよい。

【０４０５】

本発明の一実施形態においては、本発明に従って使用されるような暗号化キー、分割キー、または両方は、追加レベルのセキュリティをセキュア化されたデータセットに提供するために、例えば、ワークグループキーを使用して、さらに暗号化されてもよい。

【０４０６】

本発明の一実施形態においては、セキュア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。

【０４０７】

図３６は、本発明による、セキュア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によって標識される。セキュアなデータパーサは、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等の他のキー分割（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において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。

【０４０８】

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

ステップ３６１０において、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得る。分割アルゴリズムがキーを必要とする場合、暗号でセキュアな擬似乱数発生器を使用して、分割暗号化キーがステップ３６１２において生成されてもよい。分割暗号化キーは、任意に、ステップ３６１５において耐故障性を有する所定数のシェアにキー分割される前に、Ａｌｌ　ｏｒ　Ｎｏｔｈｉｎｇ　Ｔｒａｎｓｆｏｒｍ（ＡｏＮＴ）を使用して、ステップ３６１４において変換分割キー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において事後暗号化されてもよい。

【０４０９】

（　２）３１１１、３６１２、３６１４、３６１５、３６１６、３６１７、３６１８、３６１９）

いくつかの実施形態においては、ユーザまたは外部システムによって提供される暗号化キーを使用して、入力データが暗号化されてもよい。外部キーがステップ３６１１において提供される。例えば、キーは、外部キー記憶から提供されてもよい。分割アルゴリズムがキーを必要とする場合、暗号でセキュアな擬似乱数発生器を使用して、分割暗号化キーがステップ３６１２において生成されてもよい。分割キーは、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キー分割される前に、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キー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。

【０４１０】

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

いくつかの実施形態においては、データを変換するために、暗号でセキュアな擬似乱数発生器を使用して、暗号化キーがステップ３６１２において生成されてもよい。生成された暗号化キー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。暗号化キーは、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キーに変換されてもよい。次いで、変換暗号化キーおよび／または生成された暗号化キーは、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キーを必要とする場合、暗号でセキュアな擬似乱数発生器を使用した、分割暗号化キーの生成が、ステップ３６１２において発生してもよい。分割キーは、任意に、ステップ３６１５において耐故障性を有する所定数のシェアにキー分割される前に、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キー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。

【０４１１】

（４）３６１２、３６１４、３６１５、３６１６、３６１７、３６１８、３６１９）

いくつかの実施形態においては、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キーを必要とする場合、暗号でセキュアな擬似乱数発生器を使用した、分割暗号化キーの生成が、ステップ３６１２において発生してもよい。分割キーは、任意に、ステップ３６１５において耐故障性を有する所定数のシェアにキー分割される前に、Ａｌｌ　ｏｒ　Ｎｏｔｈｉｎｇ　Ｔｒａｎｓｆｏｒｍ（ＡｏＮＴ）を使用して、ステップ３６１４において変換分割キー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。

【０４１２】

オプションの前述の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において使用されるが、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、他の実施形態においてセキュアなデータパーサとともに使用されてもよい。

【０４１３】

セキュアなデータパーサは、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得る。データは、最初に暗号化され、次いで、「ｎ分のｍ」耐故障性を有する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。

【０４１４】

シェアを作成するために、いくつかのキーが、任意に、セキュアなデータパーサによって利用される。これらのキーは、以下のうちの１つ以上を含んでもよい。

【０４１５】

事前暗号化キー：シェアの事前暗号化が選択されると、外部キーがセキュアなデータパーサに渡されてもよい。このキーは、生成されて外部からキー記憶（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。

【０４１６】

分割暗号化キー：このキーは、内部で生成され、分割前にデータを暗号化するためにセキュアなデータパーサによって使用されてもよい。次いで、このキーは、キー分割アルゴリズムを使用して、シェア内でセキュアに記憶されてもよい。

【０４１７】

分割セッションキー：このキーは、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、分割セッションキーが内部で生成され、データをシェアに区分化するためにセキュアなデータパーサによって使用されてもよい。このキーは、キー分割アルゴリズムを使用して、シェア界でセキュアに記憶されてもよい。

【０４１８】

事後暗号化キー：シェアの事後暗号化が選択されると、外部キーがセキュア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。このキーは、生成され、外部からキー記憶または他の好適な場所に記憶されてもよい。

【０４１９】

いくつかの実施形態においては、このようにして、セキュアなデータパーサを使用してデータがセキュア化されると、必要なシェアおよび外部暗号化キー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。

【０４２０】

図３７は、いくつかの実施形態において本発明のセキュアなデータパーサを使用するための例示的な概観過程３７００を示す。前述で説明されるように、セキュアなデータパーサ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、セキュアなデータパーサ３７０６は、いくつかの実施形態においては、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。

【０４２１】

セキュアなデータパーサ３７０６と関連付けられる主要なキー過程は、事前暗号化過程３７０８、暗号化／変換過程３７１０、キーセキュア化過程３７１２、解析／分配過程３７１４、耐故障性過程３７１６、共有認証過程３７１６、および事後暗号化過程３７２０のうちの１つ以上を含んでもよい。これらの過程は、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。使用される過程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、任意的な事後暗号化、事後暗号化、または両方が所望されるか否か、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。

【０４２２】

例示的過程３７００の出力は、２つ以上のシェア３７２２であってもよい。前述で説明されるように、いくつかの実施形態においては、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。他の実施形態においては、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。

【０４２３】

情報資産の個別保護に加えて、ときには、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においては、ワークグループキーがグループメンバーに配備されてもよい。ワークグループキー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ので、ワークグループキーは保護され、内密にされるべきである。ワークグループキー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。

【０４２４】

ワークグループキー概念は、シェア内に記憶されたキー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キーが発見されたとしても、ワークグループキー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。

【０４２５】

図３８は、シェア内でキー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。概略図３８００の実施例では、任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。

【０４２６】

データを分割するための簡略化した過程は、暗号化段階３８０２において暗号化キー３８０４を使用してデータを暗号化することを含む。次いで、暗号化キー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。分割暗号化キー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、分割暗号化キーを使用して、データ３８０８が分割され、シェア３８１０に記憶される。

【０４２７】

データを修復するために、分割暗号化キー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。暗号化キー３８０４も回収および修復されてもよく、次いで、暗号化キーを使用して、暗号文が復号されてもよい。

【０４２８】

ワークグループキーが利用されるときに、前述の過程は、ワークグループキーで暗号化キーを保護するように、わずかに変更されてもよい。次いで、暗号化キーは、シェア内に記憶される前にワークグループキー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。

【０４２９】

ワークグループキーを使用してデータを分割するための簡略化した過程は、段階３９０２において暗号化キー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、暗号化キーは、段階３９０４においてワークグループキーで暗号化されてもよい。次いで、ワークグループキーで暗号化された暗号化キーは、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。分割キー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、分割キー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。

【０４３０】

データを修復するために、分割キーが、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。（ワークグループキーで暗号化された）暗号化キーが回収および修復されてもよい。次いで、ワークグループキーを使用して、暗号化キーが復号されてもよい。最終的に、暗号化キーを使用して、暗号文が復号されてもよい。

【０４３１】

ワークグループキーを配備し、保護するためのいくつかのセキュアな方法がある。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において使用される、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。

【０４３２】

（ハードウェアベースのキー記憶）
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／復号キー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キー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）または非携帯用キー記憶周辺機器にキーを記憶する、改ざん防止キー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キー材料の容易な複製を防止するように設計されている。キーは、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、多くのキー記憶システムは、キー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。

【０４３３】
（ソフトウェアベースのキー記憶）
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）の上に直接キー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。

【０４３４】
ディスク上でキーをセキュア化するために、ソフトウェアベースのキー管理はしばしば、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）他のキーの存在、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キーの下で、暗号化された形態でキーを記憶することによって、キーを保護する。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キー保護機構から、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。

【０４３５】
本発明のセキュアなデータパーサは、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セキュア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、セキュア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、任意の輸送媒体を通して、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、本発明のセキュア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。セキュアなデータパーサは、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、セキュアなデータパーサは、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、あるいはセキュア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。

【０４３６】

いくつかの実施形態においては、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において、本発明のセキュア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過程４０００および簡略化したデータ区分化過程４０１０が、それぞれ、図４０Ａおよび４０Ｂに示されている。これらの過程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。

【０４３７】

いくつかの実施形態においては、ヘッダ生成過程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においては、無作為（または擬似無作為）な分割暗号化キーＫが生成されてもよい。次いで、分割暗号化キーＫは、任意に、ＡＥＳキーラップステップ４００４において（例えば、前述で説明されるワークグループキーを使用して）暗号化されてもよい。ＡＥＳキーラップがいくつかの実施形態において使用されてもよいが、任意の好適なキー暗号化またはキーラップアルゴリズムが他の実施形態において使用されてもよい。ＡＥＳキーラップステップ４００４は、分割暗号化キーＫ全体に作用してもよく、または分割暗号化キーは、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キーラップステップ４００４は、所望であれば、分割暗号化キーのブロックに作用してもよい。

【０４３８】

ステップ４００６においては、分割暗号化キーＫをキー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、各キーシェアは、（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適合するように設計されてもよい。

【０４３９】

（例えば、簡略化したヘッダ生成過程４０００を使用して）ヘッダ生成が完了した後に、セキュアなデータパーサは、簡略化したデータ分割過程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キー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、本発明に従って前述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においては、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においては、任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。

【０４４０】

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、暗号キーシェア、キー同一性、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限化するために、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。

【０４４１】

例えば、いくつかの実施形態においては、シェアヘッダは、暗号化されず、Ｓｈａｍｉｒキーシェア、セッションごとのノンス、シェアごとのノンス、キー識別子（例えば、ワークグループキー識別子および事後承認キー識別子）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、分割暗号化キーで暗号化される、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。

【０４４２】

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適合するように設計されてもよい。いくつかの実施形態においては、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。

【０４４３】

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。前述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セキュア化されてもよい。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、セキュアなデータパーサは、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。

【０４４４】

前述のように、本発明のいくつかの実施形態においては、セキュアなデータパーサは、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。

【０４４５】

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。

【０４４６】

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。

【０４４７】

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。

【０４４８】

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。

【０４４９】

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ので、高速修復を可能にする。

【０４５０】

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、または決定論的および確率論的両方のデー多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のを防止するために、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。

【０４５１】

いくつかの実施形態においては、キーのある情報分散を使用して（例えば、キーのある情報分散アルゴリズムまたは「ＩＤＡ」を通して）、キーのある秘密共有ルーチンが採用されてもよい。キーのあるＩＤＡ用のキーはまた、１つ以上の外部ワークグループキー、１つ以上の共有キー、またはワークグループキーおよび共有キー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においては、少なくとも「Ｍ」個のシェアならびにワークグループキー（および／または共有キー）が必要とされてもよい。ＩＤＡ（またはＩＤＡ用のキー）はまた、暗号化過程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。

【０４５２】

例えば、いくつかの実施形態においては、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、キーのある情報分散が使用される。キーのある情報分散は、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、セッションキーを使用してもよい。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あるいはＢｌｏｃｋＳｅｇｍｅｎｔ等の前述で説明される方法）が使用されてもよい。次いで、セッションキーは、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（またはキーのある情報分散およびセッションキー）を使用して共有されてもよい。

【０４５３】

いくつかの実施形態においては、キーの一意の部分が２つ以上のセッションキーシェアの中へ分配または共有される前に、共有キー（例えば、ワークグループキー）を使用してセッションキー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つのセッションキー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においては、少なくとも１つのセッションキーシェアが、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。他の実施形態においては、少なくとも部分的に共有ワークグループキーに基づく場所において、少なくとも１つのセッションキーシェアが、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、各セッションキー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、キー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キーに基づく場所において、セッションキーシェアを、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。他の実施形態においては、ユーザシェアを形成するように、１つ以上のセッ

ションキー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、承認された一組のユーザシェアおよび共有ワークグループキーが要求されてもよい。

【０４５４】

キーのある情報分散は、キー回収オラクルに直面してもセキュアであってもよい。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のキー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$Y_i = E_K(X_i)$）と一致するキーＫを返信する。オラクルは、一致するキー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キーを回復してもよい、暗号解読攻撃をモデル化してもよい。

【０４５５】

標準ブロック暗号ベースのスキームは、キー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、キー回収オラクルの存在下で完全に非セキュアになる場合がある。

【０４５６】

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場合には、（Π^{IDA}，Π^{Enc}）は、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）と組み合わせられると、ロバストな計算秘密共有（ＲＣＳＳ）目標を達成するならば、キー回収攻撃に直面してセキュリティを提供するが、敵がキー回収オラクルを有するモデルにおける。

【０４５７】

１対のスキームがキー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。

【０４５８】

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においては、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．．．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。そのような弱い秘密の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。

【０４５９】

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においては、単一暗号化の代わりに二重暗号化とともにＣＢＣモードを使用してもよい。ここで、任意のＩＤＡ、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キー回収オラクルを有することは、敵にとって役に立たない。

【０４６０】

賢明なＩＤＡは、値を有するが、キー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」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においては、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から押し出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。

【０４６１】

前述に基づいて、いくつかの実施形態においては、「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}）がキー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。

【０４６２】

いくつかの実施形態においては、キー回収オラクルに直面してＲＣＳＳによりセキュアである、暗号化スキームが提供される。スキームは、キー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、キー回収攻撃に対して対称暗号化スキームをよりセキュア化するために、特に有用であってもよい。

【０４６３】

前述のように、古典的な秘密共有概念は、典型的にはキーがない。たがって、任意の種類の対称または非対称キーを保持するために、秘密を再構成するディーラも当事者も必要としない方法で、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セキュアなデータパーサは、任意に、キー付きである。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、対称キーを提供してもよい。セキュアなデータパーサは、セキュア化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、対称キーを使用してもよい。

【０４６４】

共有キーは、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通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）一組の承認されたプレーヤ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キーを取得する（またはそのキー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。

【０４６５】

いくつかの実施形態においては、新しい一組の付加的な要件がＲＣＳＳ目標に追加される。付加的な要件は、「第２の因子」であるキー所有を含んでもよい。これらの付加的な要件は、元の一組の要件を軽減することなく追加されてもよい。一組の要件は、秘密キーを知っているが、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、他方の一組の要件は、秘密キーを持たないが、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）。

【０４６６】

いくつかの実施形態においては、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、秘密キー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、同じキー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。敵のプライバシー利点は、ｂ＝ｂ’という確率の２倍未満のものである。この方策は、全てのシェアを習得しても、秘密キーが欠けていれば、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捕らえる。

【０４６７】
真正性要件では、環境が秘密キーＫを選択し、これを共有（シェア）および回復（Ｒｅｃｏｖｅｒ）への後続の呼び出しで使用する、方策が関与してもよい。共有および回復は、いくつかの実施形態においては、このキー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$M_1, \ldots, M_q$のシェア要求を行う。各共有要求に応じて、敵は、シェアの対応するｎベクトル$S_1, \ldots, S_q$を得る。敵の目的は、新しい平文を築くことであり、回復アルゴリズムに供給されると、$\{M_1, \ldots, M_q\}$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。

【０４６８】
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。

【０４６９】
潜在的により効率的なアプローチは、共有キーがワークグループキーとなることを可能にすることである。すなわち、（１）共有キーを使用して、（Ｒ）ＣＳＳスキームの無作為に生成されたセッションキー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、性能の最小限の劣化のみを伴ってもよい。

【０４７０】
セキュアなデータパーサのいくつかの用途が前述で説明されるが、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。

【０４７１】
本発明のセキュアなデータパーサは、クラウドコンピューティングデータ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、コンピューティングおよび記憶リソースが、ネットワーク上の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コンピューティング、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私的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それらの基礎的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）との間で抽象化のレベルを提供し、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、集合的に「クラウド」と呼ばれてもよい。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の上で、動的に拡張可能であり、しばしば仮想化されたリソースをサービスとして提供するために使用されてもよい。

【０４７２】
（例えば、企業の私的ネットワークからの）私的データが、公衆ネットワーク上で転送されてもよく、公的にアクセス可能または共有システム（例えば、Ｇｏｏｇｌｅ（例えば、Ｇｏｏｇｌｅ　Ａｐｐｓ　Ｓｔｏｒａｇｅ）、Ｄｒｏｐｂｏｘ、またはＡｍａｚｏｎ（例えば、ＡｍａｚｏｎのＳ３記憶設備））内で処理および記憶されてもよいので、セキュリティが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。これらの公的にアクセス可能なシステムは、必ずしも暗号化された記憶空間を提供するわけではないが、サーバ上に一組のファイルを記憶する能力をユーザに提供する。セキュアなデータパーサは、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、セキュアなデータパーサは、クラウドの中のデータ記憶、クラウドへ／から移動しているデータ、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、およびクラウドの中の任意の他の演算をセキュア化するために使用されてもよい。

【０４７３】

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。セキュアなデータパーサ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。セキュアなデータパーサ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、セキュアなデータパーサ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、セキュアなデータパーサ４２１０は、十分な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。好適なシステム内のセキュアなデータパーサの統合は、例えば、図２７および２８に関して、前述でさらに詳細に説明されている。クラウド４２５０は、データ記憶リソース４２６０ａおよび４２６０ｅと、データサービスリソース４２６０ｂおよび４２６０ｇと、ネットワークアクセス制御リソース４２６０ｃおよび４２６０ｈと、高性能コンピューティングリソース４２６０ｄおよび４２６０ｆとを含む、複数の例示的なクラウドリソース４２６０を含む。クラウドリソースは、複数のクラウドリソースプロバイダ、例えば、Ａｍａｚｏｎ、Ｇｏｏｇｌｅ、またはＤｒｏｐｂｏｘによって提供されてもよい。これらのクラウドコンピューティングリソースのそれぞれは、図４３－５６に関して、以下でさらに説明される。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。

【０４７４】

クラウドコンピューティングの１つの利点は、システム４２００のユーザが、専用記憶ハードウェアに投資する必要なく、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できてもよいことである。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で、オンデマンド記憶リソースを提供されてもよい。いくつかの実施形態においては、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、インターネットウェブブラウザが、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に連結するために使用されてもよい。いくつかの実施形態においては、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。両方の実施形態においては、セキュアなデータパーサ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セキュア化してもよい。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には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には専用ハードウェアリソースのように見えてもよい。

【０４７５】

いくつかの実施形態においては、セキュアなデータパーサ４２１０は、法廷で認識でき

るデータが、横断しない、またはクラウド内に記憶されないように、データを暗号化および分割してもよい。クラウドの基礎的ハードウェア構成（例えば、サーバ、記憶デバイス、ネットワーク）は、電力網の故障、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継続性を保証するために地理的に分散されてもよい。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、クラウドリソースが依然としてアクセス可能であってもよい。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てもよい。

【０４７６】

いくつかの実施形態においては、本発明のセキュアなパーサは、最初に、元のデータを無作為化し、次いで、無作為化または決定論的技法に従ってデータを分割してもよい。例えば、ビットレベルで無作為化する場合、本発明のセキュアなパーサは、一連の無作為化されたビットを形成するように、無作為化技法に従って（例えば、無作為または疑似無作為セッションキーに従って）元のデータのビットを混同してもよい。次いで、セキュアなパーサは、以前に論議されたように、任意の好適な技法（例えば、好適な情報分散アルゴリズム（ＩＤＡ））によって、ビットを所定数のシェアに分割してもよい。

【０４７７】

図４３は、クラウドを通して移動している（すなわち、１つの場所から別の場所へのデータの輸送中の）データをセキュア化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なブロック図である。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、本発明によるセキュアなデータパーサ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。

【０４７８】

クラウド４３５０は、クラウド４３５０ａ、４３５０ｂ、および４３５０ｃとして例示的に示される、公衆および私的クラウド記憶の任意の好適な組み合わせを含んでもよい。例えば、クラウド４３５０ａおよび４３５０ｃは、Ａｍａｚｏｎ、Ｇｏｏｇｌｅ、またはＤｒｏｐｂｏｘによって提供されるもの等の、公的にアクセス可能であるクラウド記憶リソースであってもよい。クラウド４３５０ｂは、特定の組織、例えば、企業または教育機関の外側の任意の個人またはグループにアクセス不可能である、私的クラウドであってもよい。他の実施形態においては、クラウドは、公衆および私的クラウドのハイブリッドであってもよい。

【０４７９】

システム４３００の受信者システム４３７０は、送信者システム４３００に関して前述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。別個のデータ部分が、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で再結合されてもよい。クラウド４３１０を通って移動するときに、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または無線通信ネットワーク、あるいはそれらの任意の組み合わせを含む、１つ以上の通信経路を横断して伝達されてもよい。図２８および２９に関して前述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、セキュアなデータパーサによってセキュア化される。

【０４８０】

図４４は、クラウドの中でデータサービスをセキュア化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なブロック図である。この実施形態におい

ては、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。セキュアなパーサ４４１０は、開示された実施形態に従ってデータサービスをセキュア化してもよい。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および実行されてもよい。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にとって仮想化リソースのように見えることを可能にする。セキュアなパーサ４４１０は、データサービス４４２０とエンドユーザ４４４０との間で移動しているデータをセキュア化してもよい。セキュアなパーサ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セキュア化してもよい。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／または別個のセキュアなクラウドデータ記憶デバイス内でセキュア化されてもよく、それは、以下でさらに詳細に説明される。図４４のデータサービス４４２０および他の部分は、クラウド４４３０の外側に示されているが、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。

【０４８１】

図４５は、クラウドの中でデータ記憶リソースをセキュア化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なブロック図である。セキュアなデータパーサ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。セキュアなデータパーサ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析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。セキュアなデータパーサ４５１０によって提供されてもよいセキュリティは、複数のユーザ／システムからのデータが、クラウド記憶プロバイダの同じ記憶デバイスまたはリソー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にとって単一の仮想化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、またはそこから読み出されるときに、セキュアなデータパーサ４５１０は、エンドユーザに見えなくてもよい方法で、データを分割および再結合してもよい。このようにして、エンドユーザは、要求に応じて、動的に拡張可能な記憶にアクセスできてもよい。

【０４８２】

セキュアなデータパーサ４５１０を使用するクラウドの中のデータ記憶は、セキュアで回復力があり、持続的かつ私的である。セキュアなデータパーサ４５１０は、法廷で認識できるデータがクラウドを横断しない、または単一記憶デバイスに記憶されないことを保証することによって、データをセキュア化する。クラウド記憶システムは、セキュアなデータパーサによって提供される冗長性により、回復力がある（すなわち、全てよりも少ないデータの分離された部分が、元のデータを再構成するために必要とされる）。記憶デバイス内に、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つ以上が故障した、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ので、持続的である。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ていたデータ部分は、データを暴露する必要なく、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は（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記憶デバイスでさえも）、複数の故障のリスクを正弦するように、地理的に分散されてもよい。最終的に、クラウドに記憶されたデータは、１つ以上のキーを使用して秘密に保たれてもよい。前述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、独特のキーによって、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。

【０４８３】

セキュアなデータパーサを使用するクラウドの中のデータ記憶はまた、従来のローカルまたはネットワーク記憶上で性能向上を提供してもよい。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に別個のデータの部分を書き込み、読み出すこと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大幅に影響を及ぼすことなく、より遅く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。

【０４８４】

図４６は、開示された実施形態による、セキュアなデータパーサを使用してネットワークアクセスをセキュア化するための例示的なブロック図である。セキュアなデータパーサ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との間にセキュア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においては、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）の中の１つ以上のネットワークリソースのためのセキュアなネットワークアクセスを提供してもよい。承認されたユーザ（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、および／またはセキュア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、グループ全体のキーが提供されてもよい。セキュア化されたネットワークリソースは、適正な信用証明（例えば、グループキー）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、ポート走査攻撃、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キング攻撃を防止してもよい。

【０４８５】

通信ネットワーク内に記憶された静止時のデータに対するセキュリティ、および通信ネットワークを通して移動している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、異なる関心のユーザまたはコミュニティのグループの間で情報を共有するために、セキュアなデータパーサ４６２０とともに使用されてもよい。協調グループが、セキュアな仮想ネットワーク上でセキュアな関心のコミュニティとして参加するように設定されてもよい。ワークグループキーが、ネットワークおよびネットワーク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ように、グループメンバーに配備されてもよい。ワークグループキー配備のためのシステムおよび方法は、前述で論議されている。

【０４８６】

図４７は、開示された実施形態による、セキュア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へのアクセスをセキュア化するための例示的なブロック図である。セキュアなデータパーサ４７１０は、高性能コンピューティングリソース４７２０へのセキュアなアクセスを提供するために使用される。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においては、セキュアなデータパーサ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セキュア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。

【０４８７】
本発明のセキュアなデータパーサは、サーバベースのセキュアなデータソリューションを実装するように構成されてもよい。本発明のセキュアなパーサのサーバベースのソリューションは、バックエンドサーバベースの静止時データ（ＤＡＲ）ソリューションを指す。サーバは、任意のＷｉｎｄｏｗｓ（登録商標）ベース、Ｌｉｎｕｘ（登録商標）ベース、Ｓｏｌａｒｉｓベース、または任意の他の好適なオペレーティングシステムであってもよい。このサーバベースのソリューションは、透明なファイルシステムをユーザに提示し、すなわち、ユーザは、いずれのデータの分割の指示も観察しない。データが本発明のセキュアなデータパーサのバックエンドサーバに提示されるときに、データはＮ個のシェアに分割され、サーバに載置された／取り付けられたＮ個のアクセス可能な（したがって利用可能な）データ記憶場所に送信される。しかしながら、これらのシェアのうちのいくらかの数Ｍのみが、データを再構築するために必要とされる。いくつかの実施形態においては、本発明のセキュアなパーサのサーバベースのソリューションは、最初に、元のデータを無作為化し、次いで、無作為化または決定論的技法に従ってデータを分割してもよい。例えば、ビットレベルで無作為化する場合、本発明のセキュアなパーサは、一連の無作為化されたビットを形成するように、無作為化技法に従って（例えば、無作為または疑似無作為セッションキーに従って）元のデータのビットを混同してもよい。次いで、本発明のセキュアなパーサのサーバベースのソリューションは、以前に論議されたような任意の公的な技法（例えば、ラウンドロビン）によって、ビットを所定数のシェアに分割してもよい。前述の図４２－４７の実施形態および以下の図の実施形態について、本発明のセキュアなパーサは、最初に、無作為化または決定論的技法に従ってデータを分割してもよいことが仮定される。さらに、以下で説明される実施形態においては、データを分割することは、前述で説明されるようなラウンドロビンまたは無作為ビット分割を含む、任意の好適な情報分散アルゴリズム（ＩＤＡ）を使用して、データを分割することを含んでもよい。

【０４８８】
データが、最初に無作為化され、次いで、無作為化または決定論的技法に従って分割されるときでさえも、データがＮ個のデータシェアのうちのいずれかＭ個から再構築されてもよいので、前述のソリューションは、単一または複数のクラウド等のローカル記憶または遠隔記憶からのデータの復旧を可能にする。本発明のセキュアなパーサのサーバベースのソリューションのさらなる説明は、特に図４８－５６に関して、以下で提供される。いくつかの実施形態においては、サーバベースのソリューションは、図４２－４７に関して前述で説明されるクラウドコンピューティングの実施形態と併せて使用されてもよい。

【０４８９】
図４８－５０の実施形態においては、本発明のセキュアなパーサのサーバベースのソリューションの実施形態は、公衆クラウド（例えば、Ｄｒｏｐｂｏｘ）、ならびに他の私的、公衆、およびハイブリッドクラウドまたはクラウドコンピューティングリソースに関連した、それらの実装に関して説明される。

【０４９０】
図４８は、本発明の一実施形態による、セキュアなデータパーサが私的および公衆クラウドの中の複数の記憶デバイス内のデータ記憶をセキュア化するために使用される、例示的な配設の概略図である。私的クラウド４８０４は、本発明のセキュアなパーサのサーバベースのソリューションを実装し、暗号化されたデータシェア４８１６ｂ、４８１８ｂ、４８１４ｂ、４８１２ｂ、４８２０ｂ、および４８２２ｂを生成するように構成される、プロセッサ４８０８を含む。私的クラウド４８０４は、任意に、例えば、インターネット接続を介して、エンドユーザデバイス４８００にアクセス可能であってもよい。遠隔ユーザは、エンドユーザデバイス４８００を介して、私的クラウド４８０４上に記憶されたデータにアクセスしてもよく、また、エンドユーザデバイス４８００からクラウド４８０４のプロセッサ４８０４へデータシェア生成および管理に関するコマンドを伝送してもよい。これらの暗号化されたデータシェアの一部は、私的クラウド４８０４内の記憶デバイス上に記憶される。特に、データシェア４８１４ｂが記憶デバイス４８１４ａ上に記憶され

る一方で、データシェア４８１２ｂは記憶デバイス４８１２ａ上に記憶される。プロセッサ４８０８はまた、他の公衆、私的、またはハイブリッドクラウド４８０２、４８０６、または４８１０に暗号化されたデータシェアの他の部分を記憶するように構成される。例えば、クラウド４８０６が、Ａｍａｚｏｎによって提供される公衆クラウドリソースを含んでもよい一方で、クラウド４８０２は、Ｄｒｏｐｂｏｘによって提供される公衆クラウドリソースを含んでもよい。この図示した実施形態においては、シェア４８１８ｂおよび４８１６ｂは、それぞれ、クラウド４８０２の中の記憶デバイス４８１８ａおよび４８１６ａ上に記憶され、シェア４８２２ｂは、クラウド４８０６の中の記憶デバイス４８２２ａ上に記憶され、シェア４８２０ｂは、クラウド４８１０の中の記憶デバイス４８２０ａ上に記憶される。このようにして、私的クラウド４８０４のプロバイダは、データシェアを記憶するように、他のクラウド記憶プロバイダの記憶リソースを活用し、それにより、クラウド４８０４による記憶デバイスへの記憶負担を低減してもよい。私的クラウド４８０４のセキュアなパーサは、Ｍ＜Ｎである、Ｎ個の解析されたシェアのうちのＭ個のみが、データを再構築するために要求されるので、障害からの頑丈なデータ生存性を提供しながら、同時にデータをセキュア化する。例えば、公衆または私的クラウド４８０６、４８１０、または４８０２のうちの１つへのアクセスが中断または損失された場合、暗号化されたデータシェアの利用可能な一部を使用して、依然としてデータにアクセスし、復旧することができる。一般に、Ｍ＜Ｎである、Ｎ個の解析されたシェアのうちのＭ個のみが、データを再構築するために要求される。例えば、公衆または私的クラウド４８０６、４８１０、または４８０２のうちの１つへのアクセスが中断または損失された場合、暗号化されたデータシェアの利用可能な一部を使用して、依然としてデータにアクセスし、復旧することができる。さらなる例示的実施例として、公衆または私的クラウド４８０６、４８１０、または４８０２のうちの１つ以上内の記憶リソースがダウンしているか、またはそうでなければアクセス不可能である場合、クラウド内の暗号化されたデータシェアのアクセス可能な一部を使用して、依然としてデータにアクセスし、復旧することができる。

【０４９１】

図４９は、本発明の一実施形態による、図４８の配設と同様である、セキュアなデータパーサが複数の私的および公衆クラウドの中でデータ記憶をセキュア化するために使用される、例示的な配設の概略図である。図４９は、例えば、インターネット接続を介して、ラップトップ４９０２等のエンドユーザデバイスに連結され、かつインターネット接続を介して、公衆クラウド４９０６および４９０８に連結される、私的クラウド４９０４を図示する。公衆クラウドは、ＤｒｏｐｂｏｘおよびＡｍａｚｏｎ（例えば、ＡｍａｚｏｎのＳ３記憶設備）によって提供されるもの等の、公的にアクセス可能であるクラウド記憶リソースを含む。前述のインターネット接続は、セキュアであってもよく、またはセキュアでなくてもよい。図４９の例示的実施形態においては、公衆クラウド４９０６がＤｒｏｐｂｏｘによって提供される一方で、公衆クラウド４９０８はＡｍａｚｏｎによって提供される。エンドユーザデバイス４９０２からのデータは、私的クラウド４９０４に伝送されてもよい。私的クラウド４９０４のプロセッサ４９０５は、本発明のセキュアなパーサのサーバベースのソリューションを実装し、暗号化されたデータシェア４９１０ａ、４９１０ｂ、４９１０ｃ、および４９１０ｄを生成するように構成されてもよい。シェア４９１０ａおよび４９１０ｂが、私的クラウド４９０４内の記憶デバイス上に記憶される一方で、シェア４９１０ｃおよび４９１０ｄは、それぞれ、公衆クラウド４９０６および４９０８に伝送され、その上に記憶される。図４８の配設と同様に、私的クラウド４９０４のプロバイダは、データシェアを記憶するように、他のクラウド記憶プロバイダの記憶リソースを活用し、それにより、クラウド４９０４による記憶デバイスへの記憶負担を低減してもよい。私的クラウド４９０４のセキュアなパーサは、Ｍ＜Ｎである、Ｎ個の解析されたシェアのうちのＭ個のみが、データを再構築するために要求されるので、障害からの頑丈なデータ生存性を提供しながら、同時にデータをセキュア化する。例えば、公衆または私的クラウド４９０６または４９０８のうちの１つへのアクセスが中断または損失された場合、暗号化されたデータシェアの利用可能な一部を使用して、依然としてデータにアクセ

スし、復旧することができる。

【０４９２】

図５０は、本発明の一実施形態による、セキュアなデータパーサが、インターネット５００６を介して複数の私的および公衆クラウドの中でデータ記憶をセキュア化するために使用される、別の例示的な配設の概略図である。図４８および４９の配設と同様である、図５０の配設では、エンドユーザデバイス５００２が、公的にアクセス可能なインターネット５００６を介して私的クラウド５００８に連結される。私的クラウド５００８は、本発明のセキュアなパーサのサーバベースのソリューションを実装し、２組の暗号化されたデータシェア５０１４ａ－ｄおよび５０１６ａ－ｄを生成するように構成される、プロセッサ５００１を含む。これらの暗号化されたデータシェアのうちのいくつか、例えば、シェア５０１４ｂおよび５０１６ａ、ならびにシェア５０１４ｃおよび５０１６ｂが、同じ記憶デバイスに記憶される一方で、他のシェア、例えば、シェア５０１６ｃおよび５０１６ｄは、異なる記憶デバイスに記憶される。シェア５０１４ａおよび５０１４ｄは、それぞれ前述で説明された、公衆クラウド記憶プロバイダ、Ｇｏｏｇｌｅ、Ａｍａｚｏｎ、およびＤｒｏｐｂｏｘによって提供される、公衆クラウド５０１０および５０１２にそれぞれ伝送され、その上に記憶される。図４８および４９の配設と同様に、私的クラウド５００８のプロバイダは、データシェアを記憶するように、他のクラウド記憶プロバイダの記憶リソースを活用し、それにより、私的クラウド５００８内の記憶デバイスへの記憶負担を低減してもよい。したがって、私的クラウド５００８のセキュアなパーサは、Ｍ＜Ｎである、Ｎ個の解析されたシェアのうちのＭ個のみが、データを再構築するために要求されるので、障害からの頑丈なデータ生存性を提供しながら、同時にデータをセキュア化する。したがって、公衆または私的クラウド５０１０または５０１２のうちの１つへのアクセスが中断または損失された場合、暗号化されたデータシェアの利用可能な一部を使用して、依然としてデータにアクセスし、復旧することができる。いくつかの実施形態においては、私的クラウド５００８のプロセッサ５００１によって管理されるデータを閲覧、暗号化、または復号することを希望する遠隔ユーザの身元を認証するために、ＵＳＢアクセスキー５００４等の取外し可能記憶デバイスがエンドユーザデバイス５００２で要求されてもよい。いくつかの実施形態においては、私的クラウド５００８のプロセッサ５００１によるデータの暗号化、復号、または分割を開始するために、ＵＳＢトークン５００４等の取外し可能記憶デバイスが、エンドユーザデバイス５００２で要求されてもよい。いくつかの実施形態においては、データは、任意の好適な情報分散アルゴリズム（ＩＤＡ）を使用して分割される。いくつかの実施形態においては、データは、最初に、分割する前に無作為化される。いくつかの実施形態においては、ユーザは、暗号化キー自体を管理してもよい。これらの実施形態においては、ユーザのキーは、ＵＳＢトークン５００４またはエンドユーザデバイス５００２等のユーザのエンドデバイス上に記憶されてもよい。他の実施形態においては、任意の好適な集中型または分散型キー管理システムが、ユーザまたはワークグループの暗号化キーを管理するために使用されてもよい。

【０４９３】

いくつかの実施形態においては、複数の明確に異なるエンドユーザデバイスのそれぞれにおいてデータ閲覧および／または再構成を可能にするために、１つ以上の暗号化キーおよび／または１つ以上のデータシェアが、ＵＳＢメモリデバイス５００４上に記憶されてもよい。加えて、データシェアのうちの１つ以上はまた、クラウド５０１０および／または５０１２上に記憶されてもよい。したがって、携帯用ユーザデバイスを保有しているユーザは、デバイス５００２とは異なるエンドユーザデバイスからＵＳＢメモリデバイス５００４にアクセスして、ＵＳＢメモリデバイス５００４および必要であればクラウドにわたって分散されたシェアから、データを閲覧および／または再構築してもよい。例えば、２つのデータシェアは、ＵＳＢメモリデバイス５００４上に記憶されてもよく、２つのデータシェアは、クラウド５０１０および５０１２のそれぞれに記憶されてもよい。ＵＳＢメモリデバイス５００４を保有しているユーザは、デバイス５００４上に記憶された２つのデータシェアにアクセスするために、ＵＳＢメモリデバイス５００４に連結された本発

明のセキュアなパーサを有する任意のコンピュータデバイスを使用してもよい。例えば、ユーザは、ＵＳＢメモリデバイス５００４およびクラウドにわたってシェアを作成し、分散させるために、第１のラップトップコンピュータを使用してもよく、次いで、ＵＳＢメモリデバイス５００４および／またはクラウド５０１０および５０１２からシェアを回収するために、第２の異なるラップトップコンピュータを使用し、次いで、回収されたシェアからデータを再構成／再構築してもよい。

【０４９４】

いくつかの実施形態においては、本発明のセキュアなパーサは、失った、または盗まれたデバイスのデータがセキュアで解読不能なままであることを保証することによって、機密性、可用性、および完全性を提供してもよい。いくつかの実施形態においては、本発明は、任意のＷｉｎｄｏｗｓ（登録商標）またはＬｉｎｕｘ（登録商標）対応ＰＣまたはエンドユーザデバイス（例えば、携帯電話、ラップトップコンピュータ、パーソナルコンピュータ、タブレットコンピュータ、スマートフォン、セットトップボックス等）の背景においてカーネルレベルで作動するソフトウェアを含んでもよい。いくつかの実施形態においては、Ｓｅｃｕｒｉｔｙ　Ｆｉｒｓｔ　Ｃｏｒｐ．のＦＩＰＳ　１４０－２認定、Ｓｕｉｔｅ　Ｂ準拠のセキュアなパーサＥχｔｅｎｄｅｄ（ＳＰχ）等のセキュアなパーサが、セキュア化されるデータを分割するために使用されてもよい。いくつかの実施形態においては、ＦＩＰＳ　１４０－２　ＡＥＳ　２５６暗号化、無作為ビットデータ分割、完全性チェック、および分割シェアの再暗号化が行われる。いくつかの実施形態においては、データは、任意の好適な情報分散アルゴリズム（ＩＤＡ）を使用して分割される。いくつかの実施形態においては、分割は決定論的である。いくつかの実施形態においては、データはまた、分割する前に無作為化されてもよい。いくつかの実施形態においては、ユーザのエンドデバイス上のセキュアな場所（例えば、「Ｃ：」ドライブ）に記憶されたあらゆるファイルは、適正な信用証明およびアクセスなしでは見えない。いくつかの実施形態においては、ファイル名でさえも、必要暗号化キーおよび認証過程なしでは見ること、または回復することができない。

【０４９５】

いくつかの実施形態においては、一組のＮ個のシェアが作成され、本発明のセキュアなパーサは、Ｎ個の別個で、おそらく地理的に分散された記憶場所に、これらのＮ個のシェアを記憶する。例えば、４つの暗号化されたシェアが作成されてもよく、次いで、本発明のセキュアなパーサは、４つの別個の記憶場所に、これらの４つの暗号化されたシェアを記憶する。図５１－５３は、４つの暗号化されたシェアが作成される、本発明のセキュアなパーサの２つのそのような実施形態を図示する。

【０４９６】

図５１は、本発明の一実施形態による、セキュアなデータパーサが、ユーザの取外し可能記憶デバイス５１０４の中および大容量記憶デバイス５１０６上でデータ記憶をセキュア化するために使用される、例示的な配設の概略図である。図５１は、４つの暗号化されたシェア５１０８ａ、５１０８ｂ、５１０８ｃ、および５１０８ｄを生成したラップトップコンピュータ５１０２等のエンドユーザデバイスを示す。これらの暗号化されたシェア５１０８ａ－ｄのそれぞれは、エンドユーザデバイス５１０２の大容量記憶デバイス５１０６内の異なる記憶セクタに記憶される。エンドユーザデバイスのセキュアなパーサは、Ｍ＜Ｎである、Ｎ個の解析されたシェアのうちのＭ個のみが、データを再構築するために要求されるので、障害からの頑丈なデータ生存性を提供しながら、同時にデータをセキュア化する。図５１の実施形態においては、４つのシェアがあり、これらのシェアのうちの２つまたは３つが、データを再構成するために要求される。４つの暗号化されたシェアのうちの２つだけ、または４つの暗号化されたシェアのうちの３つが、データを再構成するために要求されると仮定すると、暗号化されたシェアのうちの１つまたは２つが失われた場合、例えば、大容量記憶装置５１０６のセクタのうちの１つが破損した場合に、障害復旧過程が加速される。取外し可能記憶デバイス５１０４は、エンドユーザデバイス５１０２の大容量記憶装置５１０６内のデータを閲覧および／または復号および／または暗号化

するために要求されてもよい、１つ以上の暗号アクセスキーを記憶するために使用されてもよい。いくつかの実施形態においては、取外し可能記憶デバイス５１０４上に暗号化キーがないと、暗号化されたデータシェア５１０８ａ－ｄを復号および／または再構成することができない。いくつかの実施形態においては、ユーザは、暗号化キー自体を管理してもよい。これらの実施形態においては、ユーザのキーは、取外し可能記憶デバイス（例えば、ＵＳＢメモリ）５１０４またはエンドユーザデバイス５１０２等のユーザのエンドデバイス上に記憶されてもよい。他の実施形態においては、任意の好適な集中型または分散型キー管理システムが、ユーザまたはワークグループの暗号化キーを管理するために使用されてもよい。

【０４９７】

いくつかの実施形態においては、複数の明確に異なるエンドユーザデバイスのそれぞれにおいてデータ閲覧および／または再構成を可能にするために、１つ以上の暗号化キーおよび／または１つ以上のデータシェアが、ＵＳＢメモリデバイス５１０４上に記憶されてもよい。加えて、データシェアのうちの１つ以上はまた、クラウド上に記憶されてもよい。したがって、携帯用ユーザデバイスを保有しているユーザは、デバイス５１０２とは異なるエンドユーザデバイスからＵＳＢメモリデバイス５１０４にアクセスして、ＵＳＢメモリデバイス５１０４および必要であればクラウドにわたって分散されたシェアから、データを閲覧および／または再構築してもよい。例えば、２つのデータシェアは、ＵＳＢメモリデバイス５１０４上に記憶されてもよく、２つのデータシェアは、エンドユーザデバイス５１０２に記憶されてもよい。ＵＳＢメモリデバイス５１０４を保有しているユーザは、ＵＳＢメモリデバイス５１０４上に記憶された２つのデータシェアにアクセスするために、ＵＳＢメモリデバイス５１０４に連結された本発明のセキュアなパーサを有する任意のコンピュータデバイスを使用してもよい。例えば、ユーザは、ＵＳＢメモリデバイス５１０４およびエンドユーザデバイス５１０２にわたってシェアを作成し、分散させるために、第１のラップトップコンピュータを使用してもよく、次いで、ＵＳＢメモリデバイス５１０４からシェアを回収するために、第２の異なるラップトップコンピュータを使用し、これら２つのシェアがデータを再構成するために十分であると仮定して、これら２つのシェアからデータを再構成／再構築してもよい。

【０４９８】

図５２は、本発明の一実施形態による、セキュアなデータパーサが複数のユーザ記憶デバイスの中でデータ記憶をセキュア化するために使用される、例示的な配設の概略図である。図５２は、４つの暗号化されたシェア５２０８ａ、５２０８ｂ、５２０８ｃ、および５２０８ｄを生成したラップトップコンピュータ５２０２等のエンドユーザデバイスを示す。これらの暗号化されたシェア５２０８ａ－ｄのそれぞれは、地理的に分散された記憶場所および／または同じ記憶場所の異なる部分に記憶される。具体的には、暗号化されたシェア５２０８ｃおよび５２０８ｄが、ラップトップコンピュータ５２０２の大容量記憶デバイス５２０６上の２つの異なる記憶セクタに記憶される一方で、暗号化されたシェア５３０８ａおよび５３０８ｂは、ＵＳＢメモリデバイス５２０４等の取外し可能記憶デバイス上に記憶される。エンドユーザデバイスのセキュアなパーサは、Ｍ＜Ｎである、Ｎ個の解析されたシェアのうちのＭ個のみが、データを再構築するために要求されるので、障害からの頑丈なデータ生存性を提供しながら、同時にデータをセキュア化する。図５２の実施形態においては、４つのシェアがあり、これらのシェアのうちの２つまたは３つが、データを再構成するために要求される。したがって、これらの暗号化されたシェアは、地理的および物理的に分散され、４つの暗号化されたシェアのうちの２つだけ、または４つの暗号化されたシェアのうちの３つが、データを再構成するために要求されると仮定すると、暗号化されたシェアのうちの１つまたは２つが失われた場合に、障害復旧過程が加速される。そのような損失は、例えば、大容量記憶装置５２０２のセクタのうちの１つが破損した場合、またはＵＳＢメモリデバイス５２０４等の取外し可能記憶デバイスが失われた場合、またはそれらの任意の組み合わせで、起こる場合がある。

【０４９９】

いくつかの実施形態においては、ＵＳＢメモリデバイス５２０４上に暗号化されたシェアを記憶する代わりに、またはそれに加えて、１つ以上のキー（例えば、暗号化キー、分割キー、または認証キー）が、ＵＳＢメモリデバイス５２０４上に記憶される。これらのキーは、ＵＳＢメモリデバイス５２０４自体の上、または他の場所に、例えば、エンドユーザデバイス大容量記憶装置５２０２の中、あるいは公衆または私的クラウド記憶の中に記憶されたデータのシェアを分割、暗号化／復号、または認証するために使用されてもよい。例えば、ユーザは、ＵＳＢメモリデバイス５２０４上にキーを記憶し、大容量記憶デバイス５２０２上に記憶された暗号化されたデータのシェアを復号するために、このキーを使用してもよい。さらなる例示的実施例として、２つのデータシェアは、ＵＳＢメモリデバイス５２０４上に記憶されてもよく、２つのデータシェアは、エンドユーザデバイス大容量記憶装置５２０２に記憶されてもよい。ＵＳＢメモリデバイス５２０４を保有しているユーザは、ＵＳＢメモリデバイス５２０４上に記憶されたキーにアクセスするために、ＵＳＢメモリデバイス５２０４に連結された本発明のセキュアなパーサを有する任意のコンピュータデバイスを使用してもよい。例えば、ユーザは、ＵＳＢメモリデバイス５２０４内にキーを記憶するために、第１のラップトップコンピュータを使用してもよく、次いで、ＵＳＢメモリデバイス５２０４からシェアを回収するために、第２の異なるラップトップコンピュータを使用してもよい。次いで、このキーは、データを暗号化／復号、分割、または認証するために使用されてもよい。

【０５００】

いくつかの実施形態においては、複数の明確に異なるエンドユーザデバイスのそれぞれにおいてデータ閲覧および／または再構成を可能にするために、１つ以上の暗号化キーおよび／または１つ以上のデータシェアが、ＵＳＢメモリデバイス５２０４上に記憶されてもよい。加えて、データシェアのうちの１つ以上はまた、クラウド上に記憶されてもよい。したがって、携帯用ユーザデバイスを保有しているユーザは、デバイス５２０２とは異なるエンドユーザデバイスからＵＳＢメモリデバイス５２０４にアクセスして、ＵＳＢメモリデバイス５２０４および必要であればクラウドにわたって分散されたシェアから、データを閲覧および／または再構築してもよい。例えば、２つのデータシェアは、ＵＳＢメモリデバイス５２０４上に記憶されてもよく、２つのデータシェアは、エンドユーザデバイス５２０２に記憶されてもよい。ＵＳＢメモリデバイス５２０４を保有しているユーザは、ＵＳＢメモリデバイス５２０４上に記憶された２つのデータシェアにアクセスするために、ＵＳＢメモリデバイス５２０４に連結された本発明のセキュアなパーサを有する任意のコンピュータデバイスを使用してもよい。例えば、ユーザは、ＵＳＢメモリデバイス５２０４およびエンドユーザデバイス５２０２にわたってシェアを作成し、分散させるために、第１のラップトップコンピュータを使用してもよく、次いで、ＵＳＢメモリデバイス５２０４からシェアを回収するために、第２の異なるラップトップコンピュータを使用し、これら２つのシェアがデータを再構成するために十分であると仮定して、これら２つのシェアからデータを再構成／再構築してもよい。

【０５０１】

図５３は、本発明の一実施形態による、セキュアなデータパーサが複数の公衆および私的クラウドならびに少なくとも１つのユーザ記憶デバイスの中でデータ記憶をセキュア化するために使用される、例示的な配設の概略図である。図５３は、４つの暗号化されたシェア５３０６ａ、５３０６ｂ、５３０６ｃ、および５３０６ｄを生成したラップトップコンピュータ５３０２等のエンドユーザデバイスを示す。これらの暗号化されたシェア５３０６ａ－ｄのそれぞれは、地理的に分散された記憶場所および／または同じ記憶場所の異なる部分に記憶される。具体的には、暗号化されたシェア５３０６ｃおよび５３０６ｄが、ラップトップコンピュータ５３０２の大容量記憶デバイス５３０８上の２つの異なる記憶セクタに記憶される一方で、暗号化されたシェア５３０６ｃは、セキュアなネットワーク接続上の伝送によって、ＡｍａｚｏｎのＳ３クラウド記憶５３１０等の公的にアクセス可能なクラウド記憶に記憶され、暗号化されたシェア５３０６ｄは、セキュアなネットワーク接続上の伝送によって、Ｄｒｏｐｂｏｘのクラウド記憶５３１２等の公的にアクセス

可能なクラウド記憶に記憶される。このようにして、暗号化されたシェアは、地理的および物理的に分散され、４つの暗号化されたシェアのうちの２つだけ、または４つの暗号化されたシェアのうちの３つが、データを再構成するために要求されると仮定すると、暗号化されたシェアのうちの１つまたは２つが失われた場合に、障害復旧過程が加速される。そのような損失は、例えば、大容量記憶装置５３０８のセクタのうちの１つが破損した場合、エンドユーザデバイス５３０２とクラウド５３１０および５３１２との間のインターネット接続が失われた場合に、起こる場合がある。

【０５０２】

図５１－５３の実施形態のそれぞれでは、暗号化データシェア生成過程および分割過程は、ユーザに見えない。さらに、本発明のセキュアなパーサは、Ｍ＜Ｎである、Ｎ個の解析されたシェアのうちのＭ個のみが、データを再構築するために要求されるので、障害からの頑丈なデータ生存性を提供しながら、同時にデータをセキュア化する。例えば、前述で説明される実施形態のうちのいくつかでは、４つの解析されたシェアのうちの２つまたは３つのみが、データを再構成または再構築するために必要とされる。ハードドライブのセクタが故障した、または取外し可能ＵＳＢデバイスが失われた、または遠隔記憶場所がダウンしているか、あるいはアクセス不可能である場合、依然としてデータにアクセスし、復旧することができる。さらに、故障したドライブのシェアが復旧された場合、またはシェアが盗まれた、オフラインになった、あるいは不正侵入された場合、任意の単一の解析されたシェアが法廷で認識できる情報を含有しないので、データは安全で保護されたままであってもよい。言い換えれば、最初に、対応する第２および／または第３のシェア、適正なユーザ認証、本発明のセキュアなパーサ、および場合によっては、ＵＳＢキーまたはＵＳＢメモリデバイスを有することなく、単一の解析されたシェアを再構成、復号、不正侵入、または復旧することができない。

【０５０３】

いくつかの実施形態においては、本発明のセキュアなパーサは、Ａｐｐｌｅ　ｉＰａｄ、ＲＩＭ　Ｂｌａｃｋｂｅｒｒｙ、Ａｐｐｌｅ　ｉＰｈｏｎｅ、Ｍｏｔｏｒｏｌａ　Ｄｒｏｉｄ　ｐｈｏｎｅ、または任意の好適なモバイルデバイス等のモバイルデバイスで使用されてもよい。当業者であれば、本明細書で開示されるシステムおよび方法が、モバイルデバイス、パーソナルコンピュータ、タブレットコンピュータ、スマートフォン、および同等物を含むが、それらに限定されない、種々のエンドユーザデバイスへの適用であることを認識するであろう。

【０５０４】

本発明のセキュアなパーサは、１つ以上のプロセッサを使用して実装されてもよく、そのそれぞれは、キー生成、データ暗号化、シェア生成、データ復号等のセキュアなパーサ機能のうちの１つ以上を果たす。いくつかの実施形態においては、データを分割することは、データを暗号分割すること、例えば、無作為ビット分割を含む。いくつかの実施形態においては、データは、任意の好適な情報分散アルゴリズム（ＩＤＡ）を使用して分割される。プロセッサは、任意の好適なプロセッサ、例えば、ＩｎｔｅｌまたはＡＭＤであってもよく、サーバベースのプラットフォーム用のバックエンドを実行してもよい。いくつかの実施形態においては、１つ以上の専用コプロセッサが、本発明のセキュアなパーサの動作を加速するために使用されてもよい。以下で説明される図５４－５６の実施形態においては、本発明のセキュアなパーサの１つ以上の機能は、セキュアなパーサ機能の加速を可能にする、１つ以上の専用コプロセッサ上で実装される。いくつかの実施形態においては、コプロセッサは、セキュアなパーサハードウェアフォームの主要マザーボードまたはドーターボード、あるいはそれらの任意の好適な組み合わせに含まれてもよい。

【０５０５】

図５４は、本発明の一実施形態による、セキュアなデータパーサ用のコプロセッサ加速デバイス５４００の概略図である。デバイス５４００は、中央処理ユニット（ＣＰＵ）またはメインプロセッサ５４０２、および高速処理ユニット（ＲＰＵ）または補助プロセッサ５４０４といった、２つのプロセッサを含む。プロセッサ５４０２および５４０４は、

相互に連結され、また、メモリデバイス５４０６および大容量記憶デバイス５４０８にも連結される。これらのデバイスの連結は、相互接続バスの使用を含む。ＣＰＵおよびＲＰＵのそれぞれは、マルチプロセッサシステムとしてＣＰＵおよび／またはＲＰＵを構成するための単一のマイクロプロセッサまたは複数のマイクロプロセッサを含んでもよい。メモリ５４０６は、動的ランダムアクセスメモリ（ＤＲＡＭ）および／または高速キャッシュメモリを含んでもよい。メモリ５４０６は、ＣＰＵ５４０２およびＲＰＵ５４０４のそれぞれに１つずつ、少なくとも２つの専用メモリデバイスを含んでもよい。大容量記憶デバイス５４０８は、ＣＰＵ５４０２および／またはＲＰＵ５４０６によって使用するためのデータおよび命令を記憶するために、１つ以上の磁気ディスクまたはテープドライブ、あるいは光ディスクドライブを含んでもよい。大容量記憶デバイス５４０８はまた、ＣＰＵ５４０２および／またはＲＰＵ５４０６にデータおよびコードを入力し、およびそこから出力するように、フロッピー（登録商標）ディスク、コンパクトディスク読取専用メモリ（ＣＤ－ＲＯＭ）、ＤＶＤ、ＦＬＡＳＨドライブ、または集積回路不揮発性メモリアダプタ（すなわち、ＰＣ－ＭＣＩＡアダプタ）等の種々の携帯用媒体用の１つ以上のドライブを含んでもよい。ＣＰＵ５４０２および／またはＲＰＵ５４０６はまた、それぞれ、一例として、通信バス５４１０として示される、通信用の１つ以上の入力／出力インターフェースを含んでもよい。通信バスはまた、ネットワーク５４１２を介したデータ通信用のインターフェースを含んでもよい。ネットワーク５４１２は、１つ以上の記憶デバイス、例えば、クラウド記憶デバイス、ＮＡＳ、ＳＡＮ等を含んでもよい。通信バス５４１０を介したネットワーク５４１２へのインターフェースは、モデム、ネットワークカード、シリアルポート、バスアダプタ、または航空機上あるいは地上の１つ以上のシステムと通信するための任意の他の好適なデータ通信機構であってもよい。ネットワーク５４１２への通信リンクは、例えば、光学、有線、または（例えば、衛星またはセルラーネットワークを介した）無線であってもよい。

【０５０６】

いくつかの実施形態においては、ＲＰＵは、コプロセッサ加速デバイス５４００と関連付けられる１つ以上の記憶デバイスに対する１つ以上の独立ディスク冗長アレイ（ＲＡＩＤ）機能を実装する、ＲＡＩＤ処理ユニットを含んでもよい。いくつかの実施形態においては、ＲＰＵ５４０４は、アレイ構築型計算および／またはＲＡＩＤ計算を行うように、汎用または特殊用途集積回路（ＩＣ）を含んでもよい。いくつかの実施形態においては、ＲＰＵ５４０４は、ＲＰＵに連結されたＰＣＩｅバス等のＰＣＩｅ接続を介して、ＣＰＵ５４０２に連結されてもよい。ＲＰＵがＲＡＩＤ処理ユニットを含む場合、ＰＣＩｅ接続は、特殊ＲＡＩＤアダプタを含んでもよい。いくつかの実施形態においては、ＰＣＩｅカードは、１０ギガビット／ｓｅｃ（Ｇｂ／ｓ）以上で作動してもよい。いくつかの実施形態においては、ＲＰＵ５４０４は、ＨＴバスに接続されたソケット付きＲＰＵ等のＨＴ接続を介して、ＣＰＵ５４０２に連結されてもよい。プロセッサ５４０２および５４０４は、典型的には、同じデータがこれらのプロセッサにアクセス可能であるように、同じメモリおよび大容量記憶デバイスにアクセスする。コプロセッサは、データ分割、暗号化、および復号を含むが、それらに限定されない、専用のセキュアな解析加速機能を果たしてもよい。これらの機能は、相互から独立しており、異なるアルゴリズムを使用して果たされてもよい。例えば、暗号化が、前述の技法のうちのいずれかを使用して行われてもよい一方で、分割は、前述で説明されるもの等の任意の好適な情報分散アルゴリズム（ＩＤＡ）を使用して行われてもよい。いくつかの実施形態においては、ＲＰＵは、コプロセッサ加速デバイス５４００の外部で本発明のセキュアなパーサの専用加速機能も果たすことができるフィールドプログラマブルゲートアレイ（ＦＰＧＡ）デバイスに連結されてもよい。

【０５０７】

図５５は、本発明の一実施形態による、セキュアなデータパーサ用の図５４のコプロセッサ加速デバイス５４００を使用する、例示的な加速過程の第１の過程フロー図である。図５４および５５を引き続き参照すると、この例示的実施形態においては、ＲＰＵ５５１０は、ＨＴバスを介したソケット付きＲＰＵ等のＨＴ接続を介して、ＣＰＵ５５２０に連

結されてもよい。図５５の左側は、データ分割およびシェア生成機能（図３９の３９１０および３９１２）等のセキュアなパーサのある機能が、ＣＰＵによって果たされてもよい一方で、暗号化等の他の機能（例えば、ＡＥＳ、ＩＤＡ、ＳＨＡアルゴリズム）（図３９の３９０２、３９０４、３９０６）は、ＲＰＵによって果たされてもよいことを図示する。これらの暗号化および暗号化シェア生成の機能は、ＣＰＵまたはＲＰＵが特定のセキュアなパーサ機能を果たすか否かという指示がある、図５５の右側に示されている。

【０５０８】

図５６は、本発明の一実施形態による、セキュアなデータパーサ用の図５４のコプロセッサ加速デバイス５４００を使用する、例示的な加速過程の第２の過程フロー図である。図５４および５６を引き続き参照すると、この例示的実施形態においては、ＲＰＵ５６１０は、ＨＴバスを介したソケット付きＲＰＵ等のＨＴ接続を介して、ＣＰＵ５６２０に連結されてもよい。図５６の左側は、データ分割およびシェア生成機能（図３９の３９１０および３９１２）等のセキュアなパーサのある機能が、ＣＰＵによって果たされてもよい一方で、暗号化等の他の機能（例えば、ＡＥＳ、ＩＤＡ、ＳＨＡアルゴリズム）（図３９の３９０２、３９０４、３９０６）は、ＲＰＵによって果たされてもよいことを図示する。これらの暗号化および暗号化シェア生成の機能は、ＣＰＵまたはＲＰＵが特定のセキュアなパーサ機能を果たすか否かという指示がある、図５５の右側に示されている。

【０５０９】

本発明のセキュアなパーサのサーバベースのソリューションを説明する図４８－５６の実施形態に関して、サーバベースのソリューションによって有効化または提供されてもよい、本発明のセキュアなパーサのいくつかの付加的な機能および特性がある。暗号分割およびデータシェア再構築を行うことに加えて、暗号化されたデータシェアのブロックレベル更新および暗号化キー管理等の他の機能性が含まれてもよい。以下の説明は、これらの機能のそれぞれを説明する。当業者であれば、この機能性は、図４８－５６に関して説明される実施形態のうちのいずれかに容易に組み込まれてもよいことを認識するであろう。

【０５１０】

いくつかの実施形態においては、本発明のセキュアなパーサのサーバベースのソリューションは、データファイル全体への更新／変更の代わりに、ファイルへのブロックレベル更新／変更を可能にする。いくつかの実施形態においては、いったんデータシェアがセキュアなパーサからクラウド記憶デバイスへ送信されると、より効率的に動作するために、基礎的データがユーザまたはワークグループによって更新されるときに、データファイル全体を修復する代わりに、本発明の暗号システムを使用して、特定のデータシェアのファイルブロックレベルにおける更新のみが、クラウド記憶デバイスに伝送されてもよい。したがって、軽微な変更のみがデータファイルに行われるときに、データファイル全体の修復が行われることも、要求されることもない。

【０５１１】

いくつかの実施形態においては、本発明のセキュアなパーサのサーバベースのソリューションは、データシェアのそれぞれのためのスタブを生成する。いくつかの実施形態においては、スタブは、その関連データシェアに対する属性のリストを含んでもよく、データシェア内にともに記憶される。いくつかの実施形態においては、スタブは、例えば、データシェアの名前、データシェアが作成された日付、データシェアが最後に修正された時間、記憶デバイスのファイルシステム内のデータシェアの場所へのポインタを含む、データシェアに関する情報を含んでもよい。そのような情報は、データシェアに関する情報をユーザに迅速に提供するために使用することができる。いくつかの実施形態においては、ユーザは、スタブを記憶するスタブディレクトリを指定してもよい。例えば、ユーザは、その上でスタブディレクトリが記憶されるべきである、記憶デバイス上の特定の仮想または物理ドライブを指定してもよい。例えば、スタブディレクトリが、ユーザのために作成されてもよく、ディレクトリの中のスタブのそれぞれは、セキュアなパーサによって、大容量記憶デバイス、取外し可能記憶デバイス、公衆クラウド、私的クラウド、またはそれらの任意の組み合わせに記憶されたデータをセキュア化するように、ユーザに指摘する。こ

のようにして、スタブは、ユーザに対するデータシェアの仮想ファイルシステムを生成するために利用されてもよい。

【０５１２】

いくつかの実施形態においては、スタブは、データシェアとは別の場所に、データシェアと同じ場所に、または両方に記憶されてもよい。いくつかの実施形態においては、ユーザがデータシェアについての何らかの情報を閲覧することを希望するときに、スタブディレクトリにアクセスしてもよい。いくつかの実施形態においては、スタブディレクトリを直接閲覧する代わりに、スタブがスタブディレクトリから回収され、本発明のセキュアなパーサのサーバベースのソリューションによって処理され、後に前述の情報をユーザに提供するために使用される。このようにして、スタブは、ユーザに対するデータシェアの仮想ファイルシステムを生成するために利用されてもよい。

【０５１３】

いくつかの実施形態においては、スタブは、データシェアのそれぞれのヘッダに記憶される。したがって、ユーザがスタブの中の情報を閲覧することを希望する場合、スタブがヘッダから回収され、本発明のセキュアなパーサのサーバベースのソリューションによって処理され、後にスタブディレクトリが生成され、ユーザに提供される。

【０５１４】

いくつかの実施形態においては、本発明のセキュアなパーサのサーバベースのソリューションは、前述の技法を使用して、データ完全性についてスタブおよび／または暗号化データシェアを頻繁にチェックする。本発明のセキュアなパーサは、ユーザによって開始または催促されないときでさえも、本質的に積極的にデータシェアを回収し、データ完全性について調査する。データシェアまたはスタブが欠落または損傷している場合、本発明のセキュアなパーサは、スタブまたはデータシェアを再作成および修復しようとする。

【０５１５】

本発明のセキュアなパーサのサーバベースのソリューションは、集中型暗号化キー管理設備を提供するように構成されてもよい。具体的には、データ、データシェア、ならびに複数の記憶デバイスおよびシステムにわたる通信セッションを暗号化／復号するために使用される暗号化キーが、企業の記憶設備、例えば、企業の私的クラウド内の中心の場所に記憶されてもよい。この集中型キー管理設備はまた、ＳａｆｅＮｅｔ，Ｉｎｃ．（Ｂｅｌｃａｍｐ，ＭＤ）によって提供されるもの等のハードウェアベースのキー管理ベースのソリューションと、またはソフトウェアベースのキー管理システムと連動してもよい。例えば、既存の私的クラウドは、認証／アクセス／承認システムを介して、暗号化されたデータのシェアへのアクセスを制御してもよく、サーバベースのソリューションは、これらのシェアを暗号化するために使用される暗号化キーへのアクセスを可能にするために認証情報を使用し、それにより、ユーザがデータを暗号分割することを可能にするか、または暗号化されたデータのシェアを修復してもよい。言い換えれば、本発明のセキュアなパーサのサーバベースのソリューションは、既存の認証／アクセス／承認システムと併せて作用してもよい。このようにして、企業は、データへのユーザおよびワークグループのアクセスを管理する現在の方法を強制的に変更させられない。

【０５１６】

いくつかの実施形態においては、発明のセキュアなパーサのサーバベースのソリューションは、暗号化されたデータシェアのうちのいずれも復号することなく、シェア再構築を行ってもよい。いくつかの実施形態においては、発明のセキュアなパーサのサーバベースのソリューションは、暗号化されたデータシェアのうちのいずれも復号することなく、１つ以上の新しいキーを使用してデータの分割を再生してもよい。図５７は、本発明の例示的実施形態による、データがＮ個のシェアに分割されて記憶される、過程５７００を図示する。図５８は、本発明の例示的実施形態による、データのシェアが再構築および／またはキー再生成される、過程を図示する。図５７および５８のそれぞれでは、過程のステップのそれぞれは任意的であってもよい。例えば、データを分割する前に、データを暗号化する必要はない。

【０５１７】
図５７を参照すると、セキュアなパーサは、最初に、暗号化キーを使用してデータを暗号化する（５７０２）。暗号化キーは、本発明のセキュアなパーサ内で内部的に生成されてもよい。暗号化キーは、少なくとも部分的に外部ワークグループキーに基づいて生成されてもよい。次いで、セキュアなパーサは、分割キーを使用してデータをＮ個のシェアに分割する（５７０４）。分割キーは、本発明のセキュアなパーサ内で内部的に生成されてもよい。分割キーは、少なくとも部分的に外部ワークグループキーに基づいて生成されてもよい。次いで、セキュアなパーサは、Ｎ個のシェアのうちのＭ個のみがデータを再構築するために要求されることを保証し（５７０６）、認証キーを使用してＮ個のシェアを認証する（５７０８）。認証キーは、本発明のセキュアなパーサ内で内部的に生成されてもよい。認証キーは、少なくとも部分的に外部ワークグループキーに基づいて生成されてもよい。認証、分割、および暗号化キーはそれぞれ、キー暗号化キーを使用して包まれる（５７１０）。次いで、ＫＥＫは、分割され、Ｎ個のシェアのヘッダ内に記憶される（５７１２）。次いで、Ｎ個のシェアは、Ｎ個の記憶場所にわたって分散される。

【０５１８】
場合によっては、ユーザまたは企業が、一組のデータシェアに対する新しい分割キーおよび／または新しい認証キーを使用することが望ましい。本発明のセキュアなパーサのサーバベースのソリューションを用いると、このデータのキー再生成は、データシェアのうちのいずれも復号することなく行われてもよい。他の場合において、１つ以上の既存のデータシェアが破損している、失われている、またはそうでなければアクセス不可能であるので、ユーザまたは企業が一組の新しいデータシェアを再生することが望ましい。本発明のセキュアなパーサのサーバベースのソリューションを用いると、この失われたデータシェアの再構築は、残りの利用可能なデータシェアのうちのいずれも復号することなく行われてもよい。図５８を参照すると、Ｎ－Ｍ個のデータのシェアが破損している、またはそうでなければアクセス不可能であると仮定すると、セキュアなパーサは、それらの記憶場所からＮ個のシェアのうちの残りのＭ個を回収する（５８０２）。これらのＭ個のシェアは、認証キーを使用して認証される（５８０４）。認証されたＭ個のシェアを使用して、暗号化データがセキュアなパーサによって再構成される（５８０６）。次いで、分割キーは、Ｎ個のシェアを再生するために使用され（５８０８）、認証キーは、Ｎ個のシェアを認証するために使用される（５８１０）。異なる分割キーまたは認証キーがステップ５８０８または５８１０に使用された場合（５８１２）、Ｍ個のシェアのそれぞれのヘッダが回収され（５８１６）、キー暗号化キーが再構成され（５８１８）、ステップ５７１０および５７１２（図５７）の過程と同様に、キー暗号化キーを使用して、新しい分割キーおよび／または認証キーが包まれる／暗号化される（５８２０）。次いで、Ｎ個のシェアは、本発明のセキュアなパーサの１つ以上の記憶デバイスに記憶される（５８２２）。異なる分割キーまたは認証キーがステップ５８０８または５８１０に使用されなかった場合（５８１２）、失われた／アクセス不可能なＮ－Ｍ個のシェアが、本発明のセキュアなパーサの１つ以上の記憶デバイスに記憶される（５８１４）。

【０５１９】
発明のセキュアなパーサのサーバベースのソリューションは、前述の図４２－５８の実施形態に関して説明されるデータシェア等のデータシェアのファイル名をセキュア化するように構成されてもよい。いくつかの実施形態においては、例えば、ＩＤＡを使用して、ファイルをＮ個のデータシェアに分割するときに、生成されたデータシェアは、記憶ネットワーク内の１つ以上のシェア場所で記憶される。記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、大容量記憶デバイス、またはそれらの任意の組み合わせを含んでもよい。多くの用途では、分割され、記憶ネットワーク内のシェア場所に記憶される、１つよりも多くのファイルが生じる。言い換えれば、いくつかのファイルがあってもよく、そのそれぞれは、（例えば、ＩＤＡを使用して）Ｎ個のデータシェアに分割されてもよく、生成されたデータシェアのそれぞれは、ファイルとしてシェア場所で記憶されてもよい。これらの用途では、シェア場所におけるデー

タシェアを、それが生成されたファイルと関連付ける、ファイル名等の一意的な識別子を有することが有利である。

【０５２０】

いくつかの実施形態においては、本発明のセキュアなパーサは、元のファイルと同じ名前でデータシェアを名付けるために、元のファイル（すなわち、分割されるファイル）のファイル名の一部分を使用するように構成されてもよい。例示的実施例として、元のファイル「２０１０Ｂｕｄｇｅｔ．ｘｌｓ」が４つのデータシェアに分割される場合、これらのデータシェアは、「２０１０Ｂｕｄｇｅｔ．ｘｌｓ．１」、「２０１０Ｂｕｄｇｅｔ．ｘｌｓ．２」、「２０１０Ｂｕｄｇｅｔ．ｘｌｓ．３」、および「２０１０Ｂｕｄｇｅｔ．ｘｌｓ．４」と名付けられてもよく、それにより、それぞれの生成されたデータシェアを元のファイルと関連付ける。この過程によって、本発明のセキュアなパーサは、効率的にデータシェアの場所を特定し、それらを元のファイルと関連付けることが可能となる。しかしながら、この過程の欠点は、バッジ情報が２０１０年に対するものであるという事実等の情報を第三者に暴露する場合があることである。多くの用途では、このようにしてファイル名を暴露することは容認可能ではなく、したがって、データシェアのファイル名を元のファイルのファイル名と容易に関連付けることはできない。

【０５２１】

いくつかの実施形態においては、本発明のセキュアなパーサは、最初に、ファイル名となるものをセキュア化して、逆転させることができない値に元のファイルのファイル名をハッシュ値変換するためにＨＭＡＣ－ＳＨＡ２５６等の認証アルゴリズムを使用するように構成されてもよい。したがって、本発明のセキュアなパーサは、ＨＭＡＣ－ＳＨＡ２５６アルゴリズムで元のファイルのファイル名を処理して、「ハッシュ化」ファイル名を取得し、セキュアであり、元のファイルのファイル名に逆転されなくてもよい認証値を受信する。次いで、元のファイルのファイル名の代わりに、このハッシュ化ファイル名を使用して、元のファイルと関連付けられるデータシェアのファイル名が生成される。これらの実施形態においては、元のファイルのファイル名と関連付けられる（記憶ネットワーク上の）データシェアの場所を特定するために、本発明のセキュアなパーサは、もう一度、元のファイル名でＨＭＡＣ－ＳＨＡ２５６アルゴリズムを使用し、認証値を再生する。いくつかの実施形態においては、元のファイル名および生成されたシェアのファイル名に対する認証値は、実質的に等しい。次いで、本発明のセキュアなパーサは、この認証値に一致するデータシェアファイル名について、記憶ネットワーク上のシェア場所を検索する。記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、大容量記憶デバイス、またはそれらの任意の組み合わせを含んでもよい。いくつかの実施形態においては、例えば、「＼Ｍａｒｋｅｔｉｎｇ＼２０１０Ｂｕｄｇｅｔ．ｘｌｓ」というフルパスを有するファイルに対して生成された認証値が、例えば、「＼Ｓａｌｅｓ＼２０１０Ｂｕｄｇｅｔ．ｘｌｓ」というフルパスを有するファイルに対して生成された認証値とは異なるように、元のファイル名のフルパスが使用される。いくつかの実施形態においては、各データシェア場所に対応する、結果として生じるデータシェアファイル名は、シェア場所を含むフルパスである、ファイルに対するフルパスのハッシュ値を計算することによって、異なるものにされる。例えば、「＼Ｓａｌｅｓ＼２０１０Ｂｕｄｇｅｔ．ｘｌｓ．１」といった、例えば、データシェアのシェア数を元のファイルのフルパスに付加することによって、結果として生じるデータシェアファイル名は、各データシェア場所について異なる。

【０５２２】

いくつかの実施形態においては、本発明のセキュアなパーサは、前述で説明されるように、ＡＥＳ等の暗号化アルゴリズムを使用して、元のファイルのフルパスを暗号化することによって、ファイルのファイル名をセキュア化する。そのような暗号化は、元のファイルのファイル名が、記憶ネットワーク上のシェア場所への認証されたアクセス、回収されたデータシェア、および暗号化キーに基づいて、本発明のセキュアなパーサによって復号されるまでセキュアであることを保証する。記憶ネットワークは、私的クラウド、公衆ク

ラウド、ハイブリッドクラウド、取外し可能記憶デバイス、大容量記憶デバイス、またはそれらの任意の組み合わせを含んでもよい。前述の実施例と同様に、最初に、データシェアのシェア数等の付加的な情報を元のファイルのフルパスに付加することによって、各シェア場所に対する一意的なデータシェアファイル名を作成することができる。

【０５２３】

セキュアなデータパーサのいくつかの用途が前述で説明されているが、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。

【０５２４】

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

【図５３】

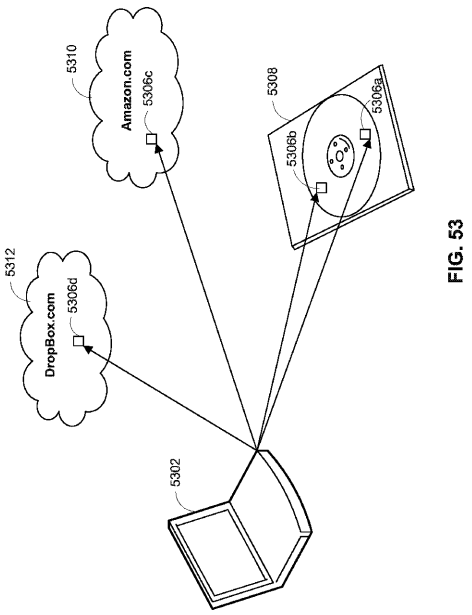

FIG. 53

【図１】

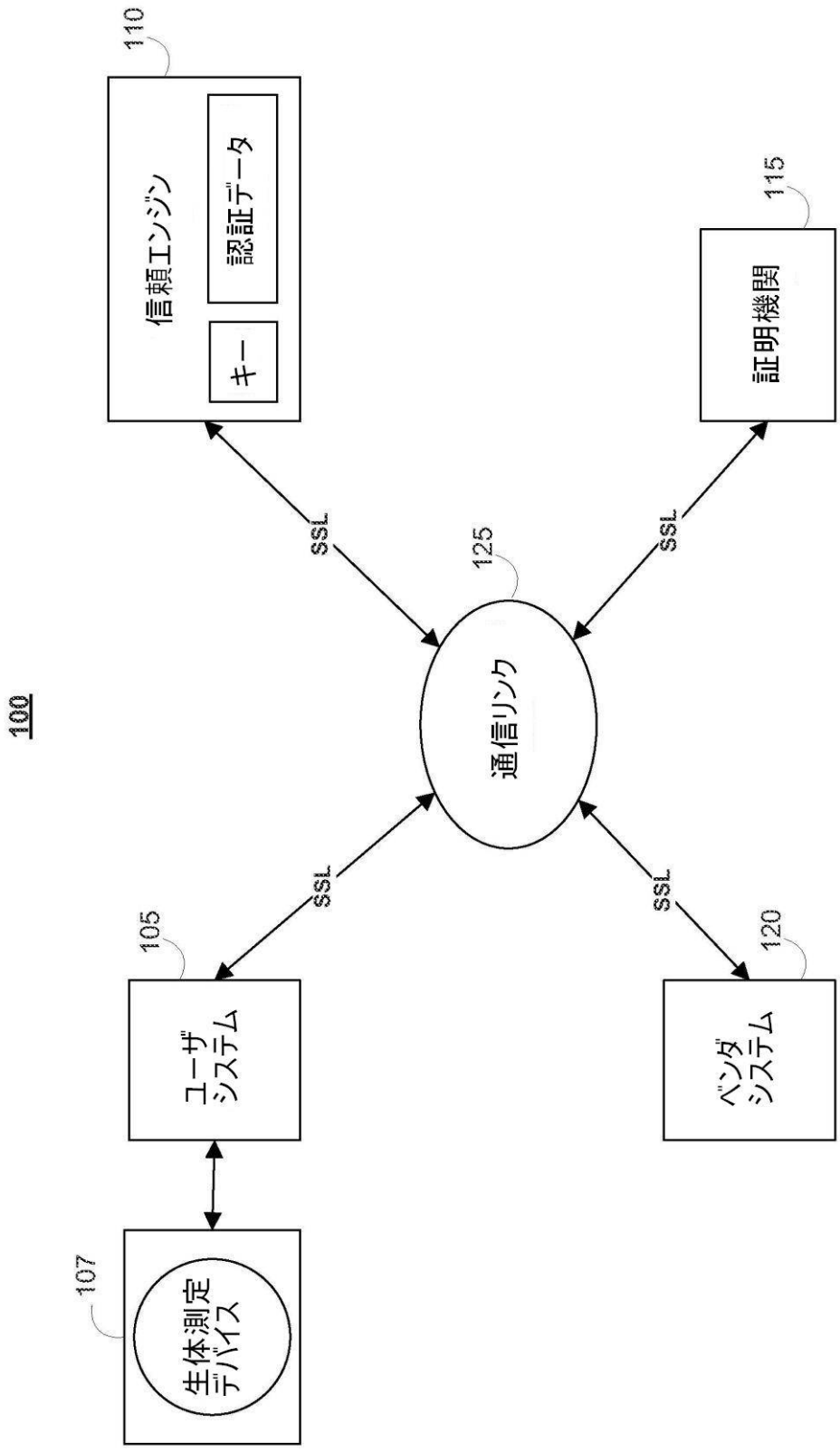
100
110
信頼エンジン
キー
認証データ
115
証明機関
SSL
SSL
125
通信リンク
SSL
SSL
105
ユーザ
システム
120
ベンダ
システム
107
生体測定
デバイス

FIG. 1

【図２】

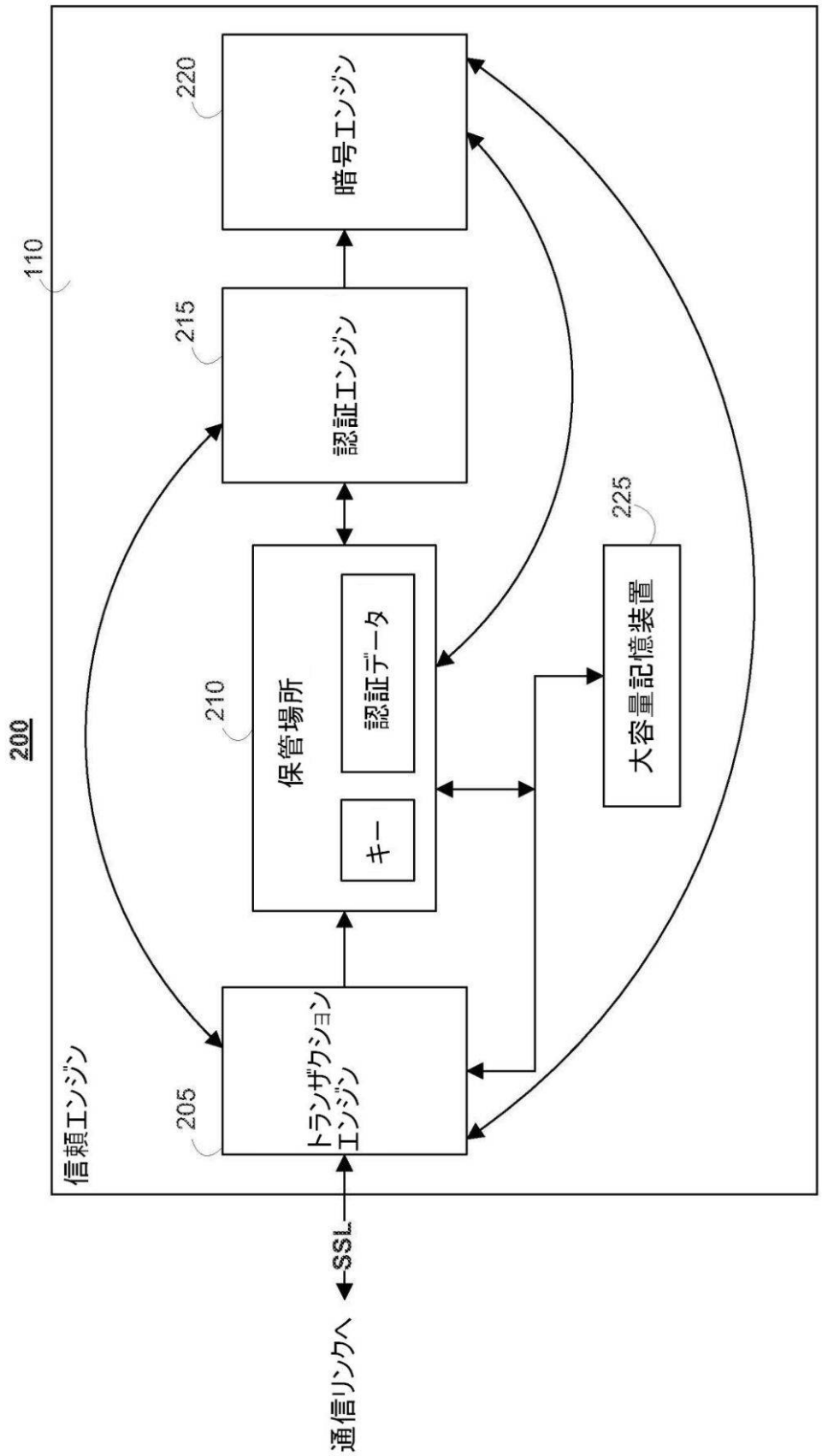
200
110
信頼エンジン
205
トランザクション
エンジン
210
保管場所
キー
認証データ
215
認証エンジン
220
暗号エンジン
225
大容量記憶装置
SSL
通信リンクへ

FIG. 2

【図３】

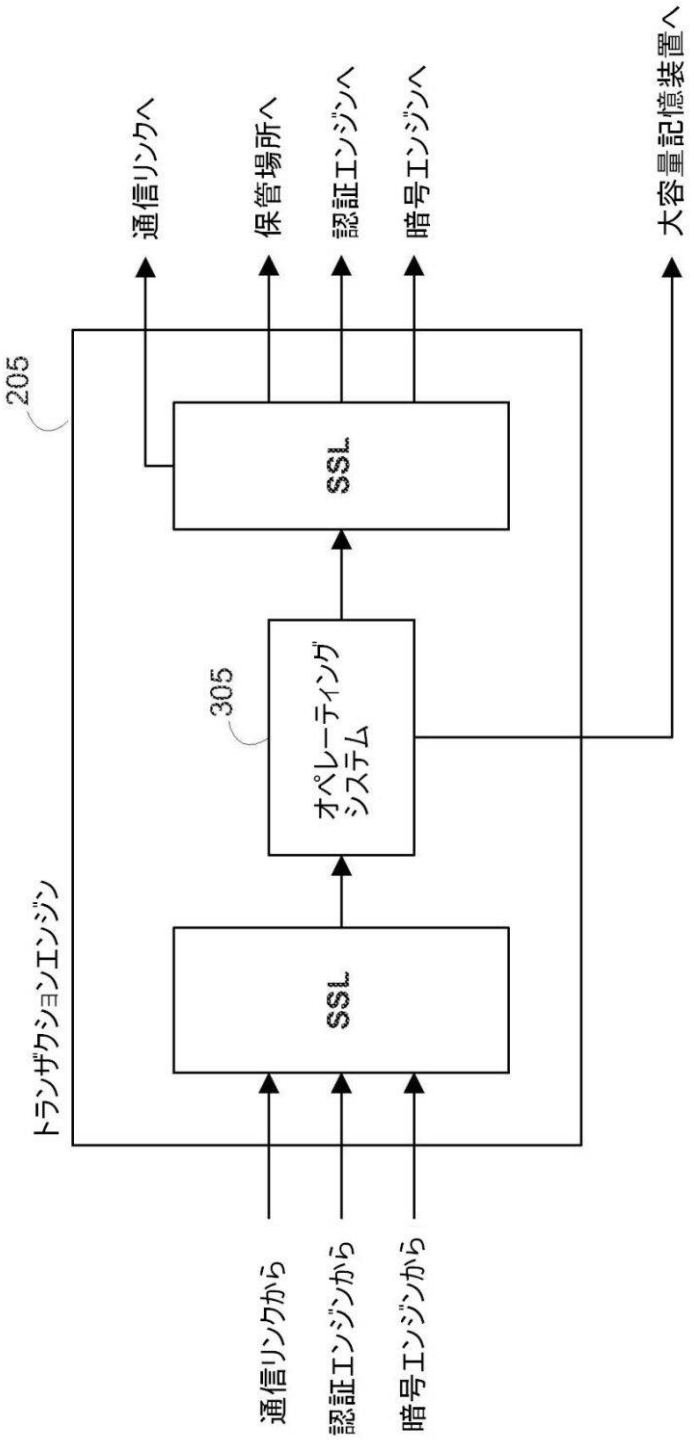
通信リンクへ
保管場所へ
認証エンジンへ
暗号エンジンへ
大容量記憶装置へ
205
SSL
305
オペレーティング
システム
SSL
トランザクションエンジン
通信リンクから
認証エンジンから
暗号エンジンから

FIG. 3

【図４】

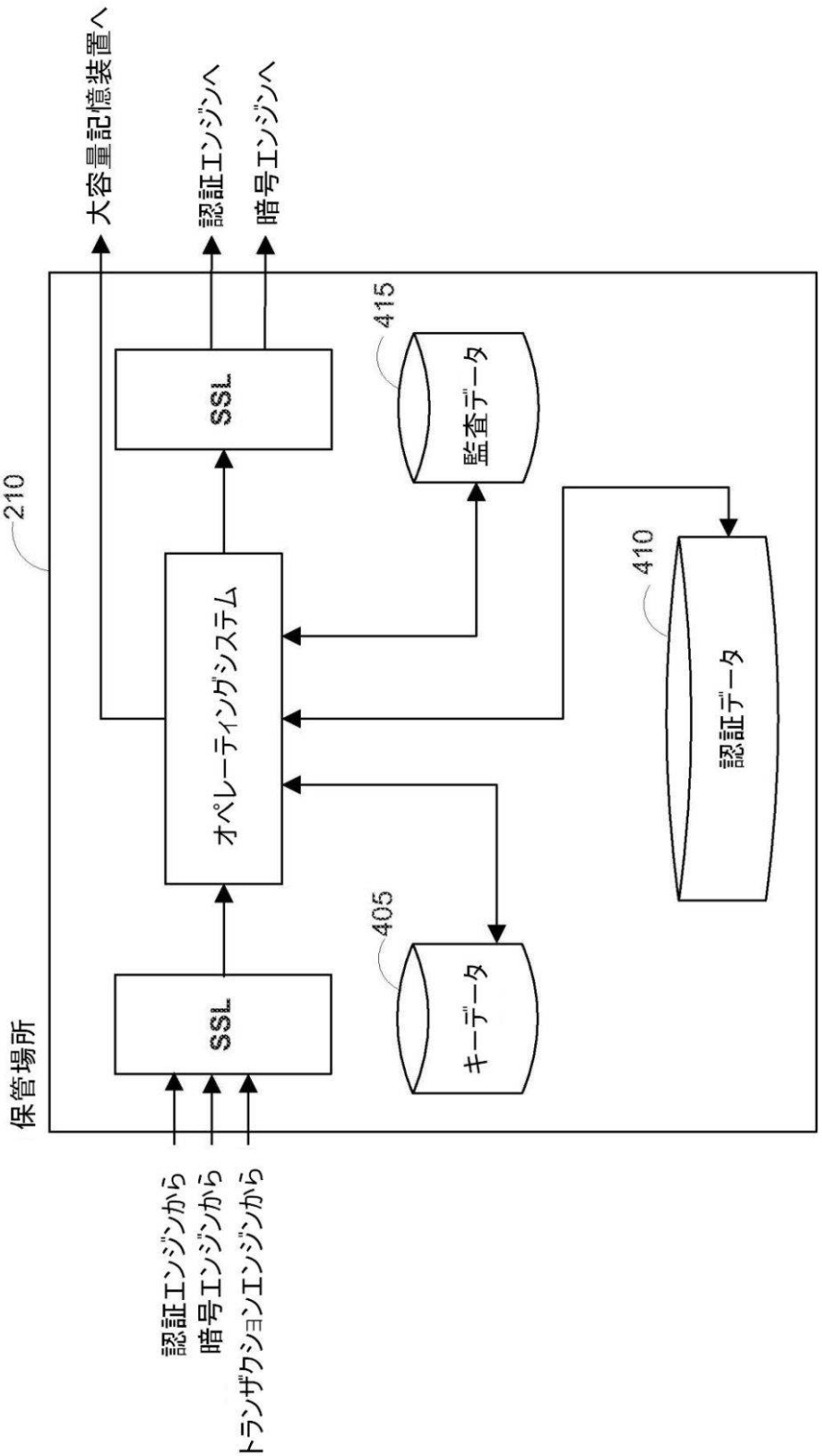
大容量記憶装置へ
認証エンジンへ
暗号エンジンへ
210
SSL
415
監査データ
オペレーティングシステム
410
認証データ
405
キーデータ
SSL
保管場所
認証エンジンから
暗号エンジンから
トランザクションエンジンから

FIG. 4

【図５】

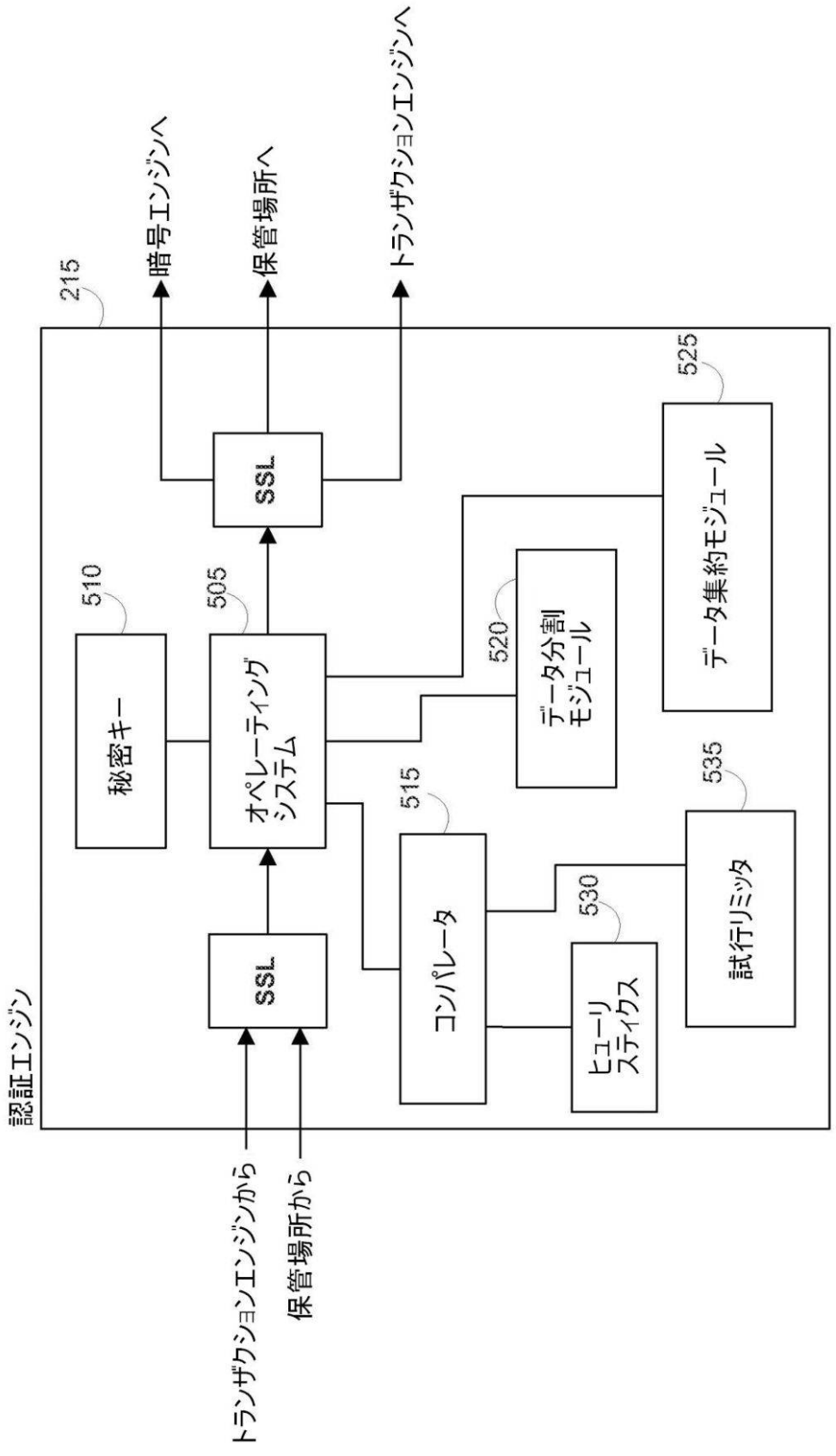
認証エンジン
215
トランザクションエンジンから
保管場所から
暗号エンジンへ
保管場所へ
トランザクションエンジンへ
SSL
SSL
秘密キー
510
オペレーティング
システム
505
コンパレータ
515
ヒューリ
スティクス
530
データ分割
モジュール
520
試行リミッタ
535
データ集約モジュール
525

FIG. 5

【図６】

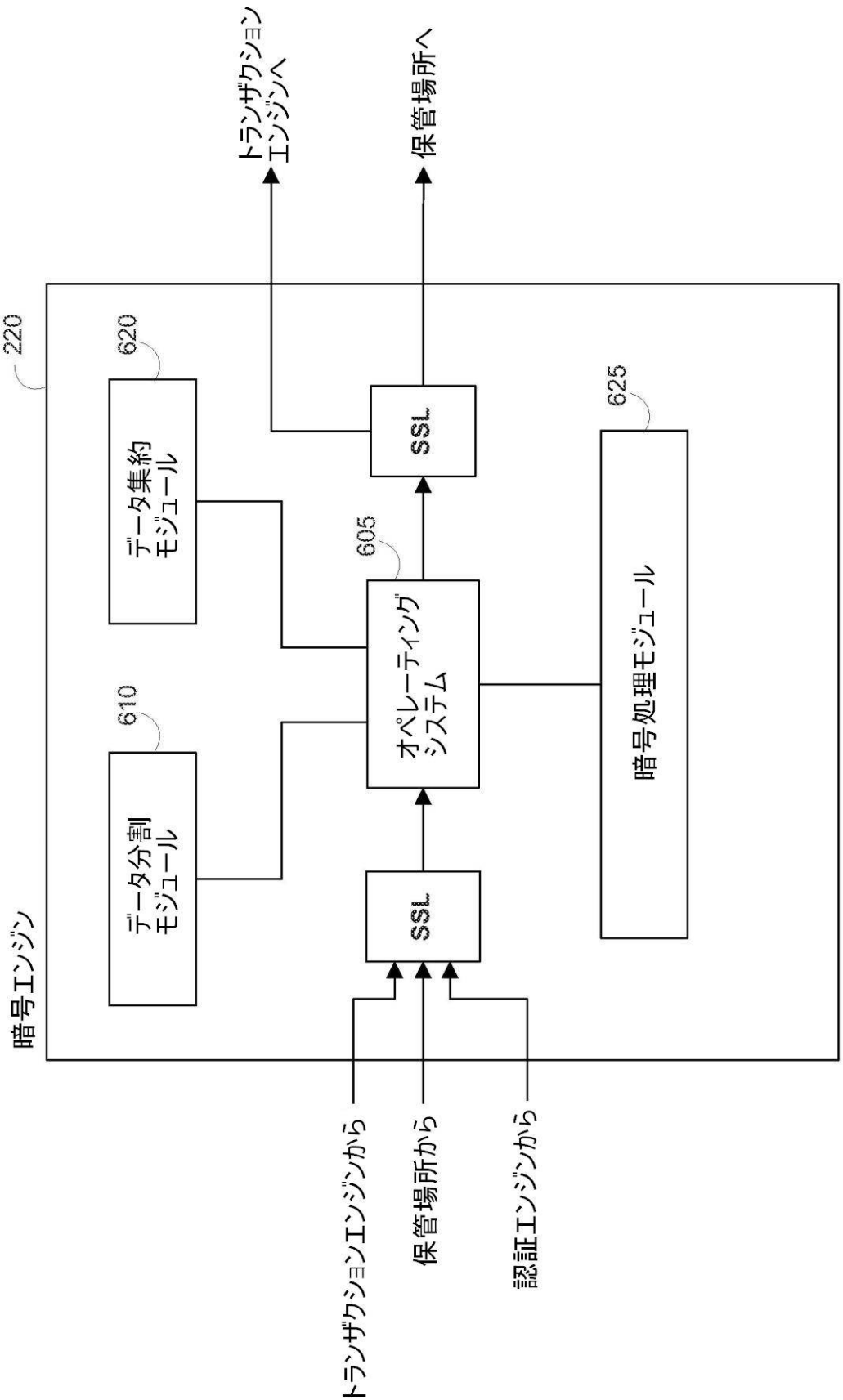
暗号エンジン
220
データ分割
モジュール
610
データ集約
モジュール
620
SSL
SSL
オペレーティング
システム
605
暗号処理モジュール
625
トランザクションエンジンから
保管場所から
認証エンジンから
トランザクション
エンジンへ
保管場所へ

FIG. 6

【図７】

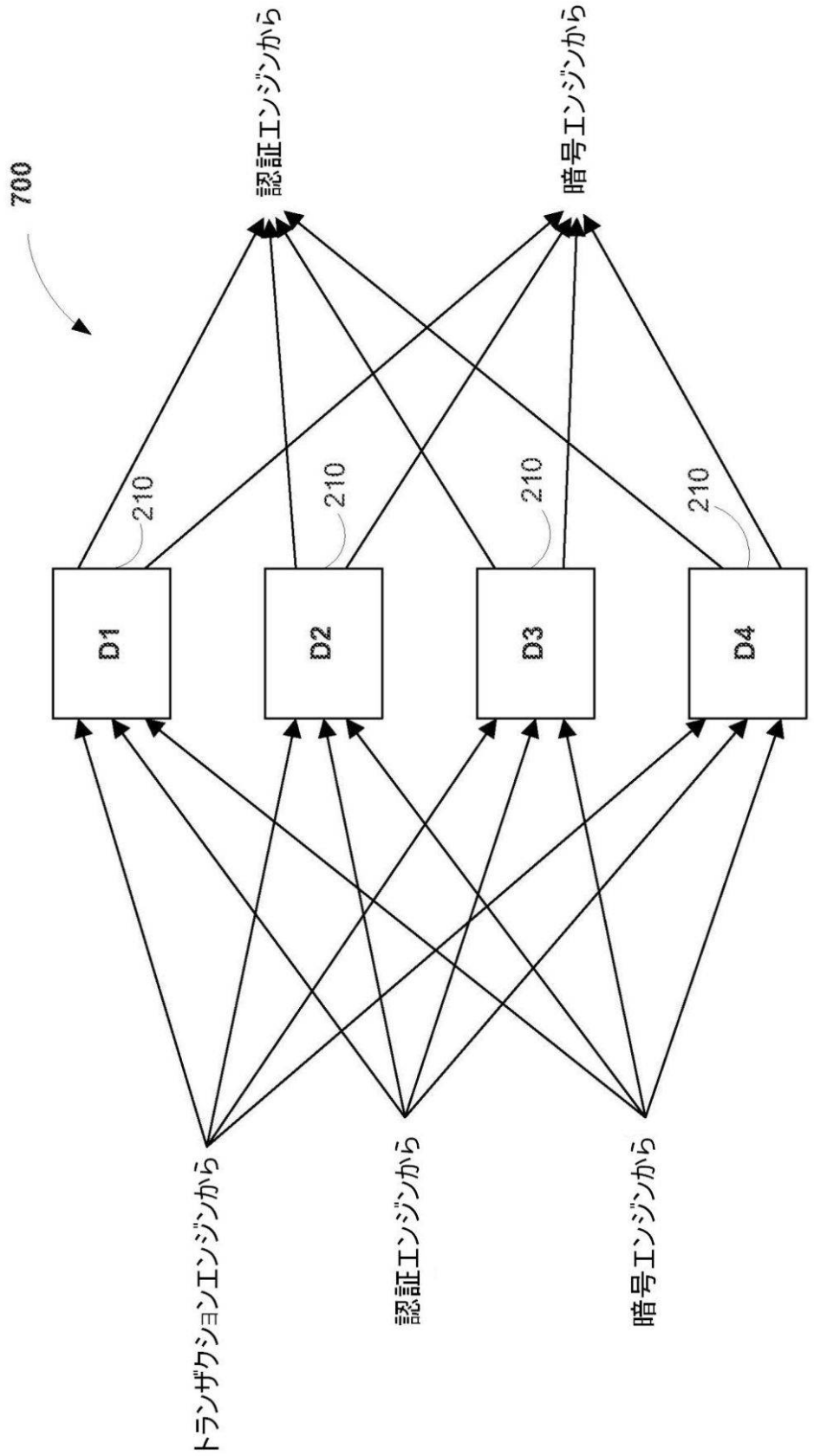
700
認証エンジンから
暗号エンジンから
210
210
210
210
D1
D2
D3
D4
トランザクションエンジンから
認証エンジンから
暗号エンジンから

FIG. 7

【図８】

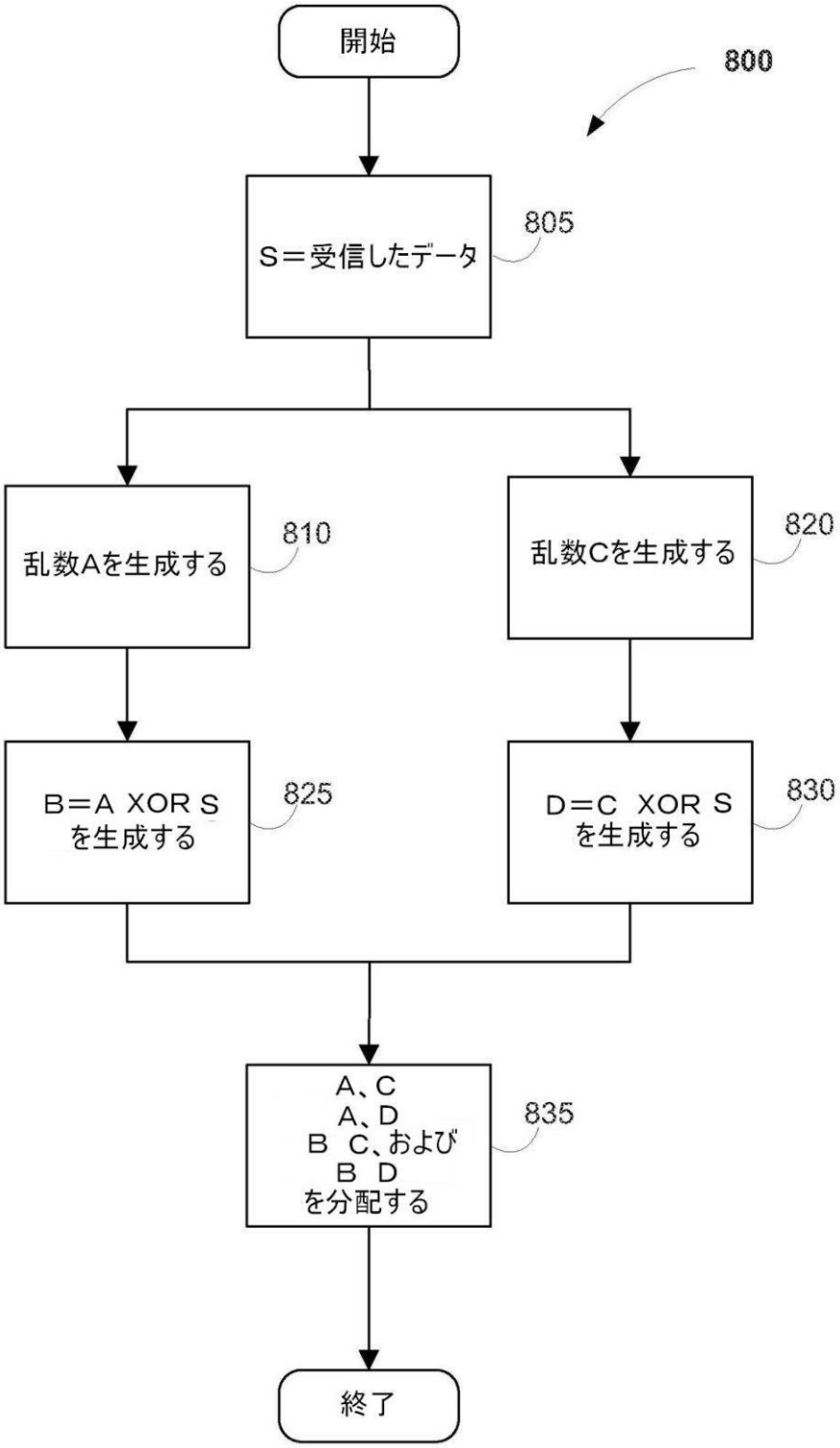
開始
800
S＝受信したデータ
805
乱数Aを生成する
810
乱数Cを生成する
820
B＝A XOR S
を生成する
825
D＝C XOR S
を生成する
830
A、C
A、D
B C、および
B D
を分配する
835
終了

FIG. 8

【図９Ａ】

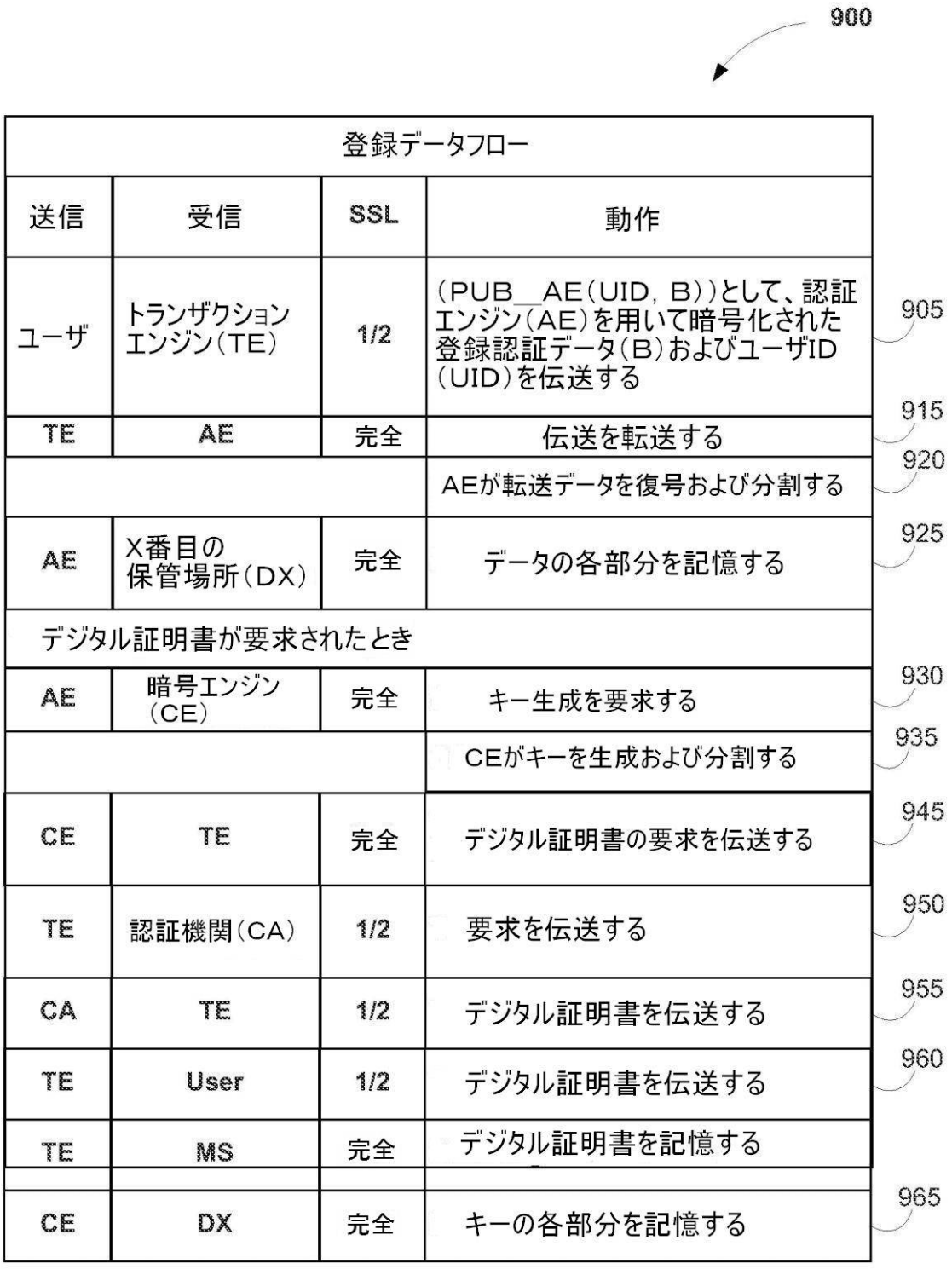

FIG. 9, パネル A

【図９Ｂ】

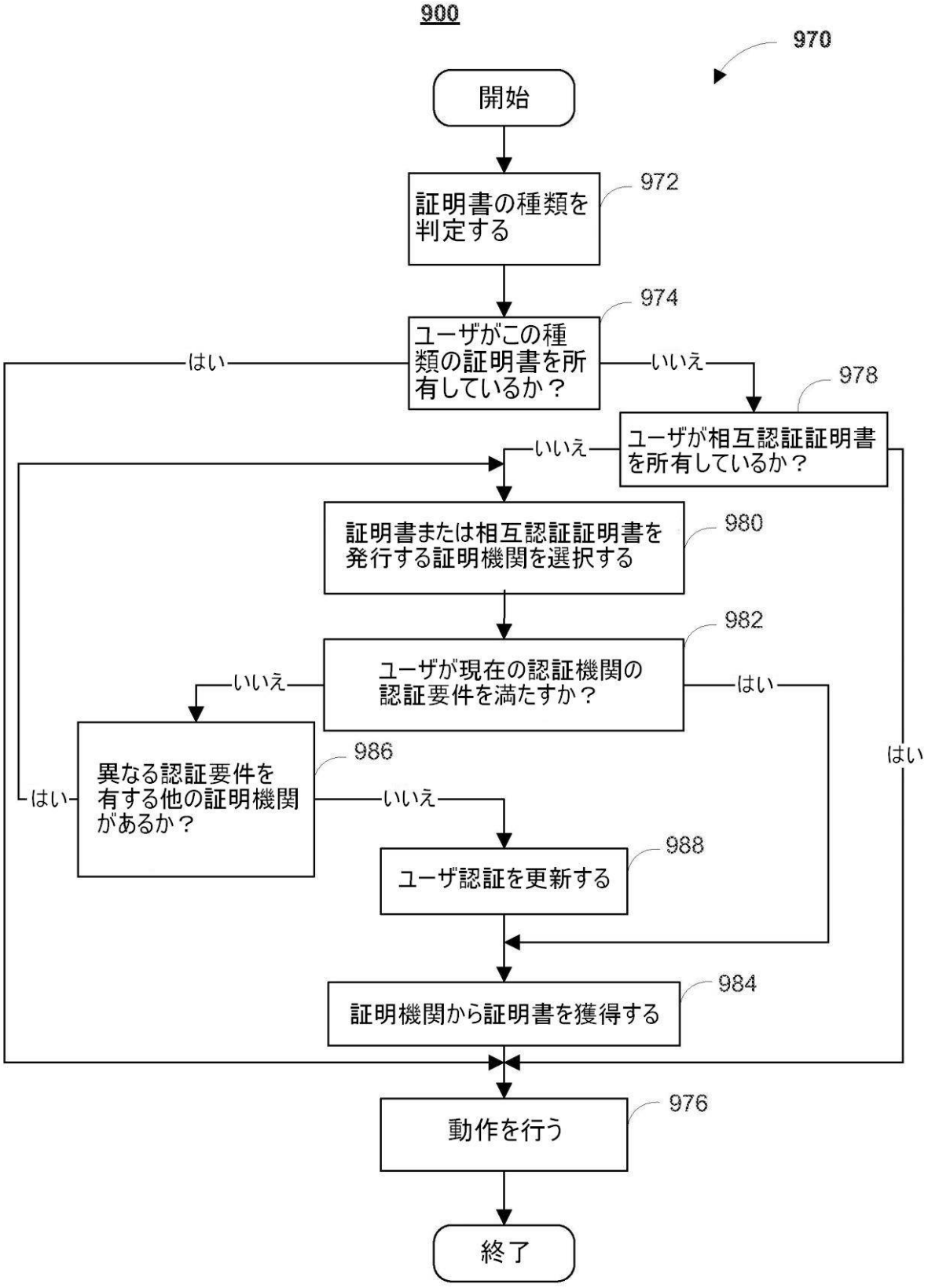

FIG. 9, パネル B

【図１０】

1000

	認証データフロー			
	送信	受信	SSL	動作
1005	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
1010	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
1015	ユーザ	TE	1/2	（PUB_AE（TID, B'））として、認証エンジン（AE）の公開キーに包まれたTIDおよびB'を伝送する
1020	TE	AE	完全	伝送を転送する
				登録認証データ（B）が要求および収集される
1025	ベンダ	トランザクションエンジン（TE）	完全	TID、ARを伝送する
1030	TE	大容量記憶装置（MS）	完全	データベースに記録を作成する
1035	TE	X番目の保管場所（DX）	完全	UID, TID
1040	DX	AE	完全	（PUB_AE（TID, BX））として、TIDおよび登録に記憶された認証データの部分（BX）を伝送する
1045				AEがBを収集し、B'と比較する
1050	AE	TE	完全	TID、ARに記入
1055	TE	ベンダ	完全	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	動作
ユーザ	ベンダ	1/2	取引の合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）、および合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	（PUB__AE（TID，B’，h（M’））として、認証エンジンの（AE）の公開キーに包まれたTID、B’、AR、およびh（M’）を伝送する
TE	AE	完全	転送を伝送する
			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）	完全	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）	完全	データベースに記録を作成する
TE	X番目の保管場所（DX）	完全	UID，TID
DX	AE	完全	（PUB AE（TID，BX））として、TIDおよび登録に記憶された認証データの部分（BX）を伝送する
			元のベンダメッセージがAEに伝送される
TE	AE	完全	h（M）を伝送する
			AEがBを収集し、B’と比較し、h（M）をh（M’）と比較する
AE	暗号エンジン（CE）	完全	デジタル署名および署名されるメッセージ、例えば、ハッシュ化メッセージの要求
AE	DX	完全	TID、署名UID
DX	CE	完全	署名者に対応する暗号キーの部分を伝送する
			CEがキーを収集し、署名する
CE	AE	完全	署名者のデジタル署名（S）を伝送する
AE	TE	完全	TID、ARに記入、h（M）、およびS
TE	ベンダ	完全	TID、受領書＝（TID、はい／いいえ、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を用いて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

1103 1105 1110 1115 1120 1125 1130 1135 1140

FIG. 11

【図１２】

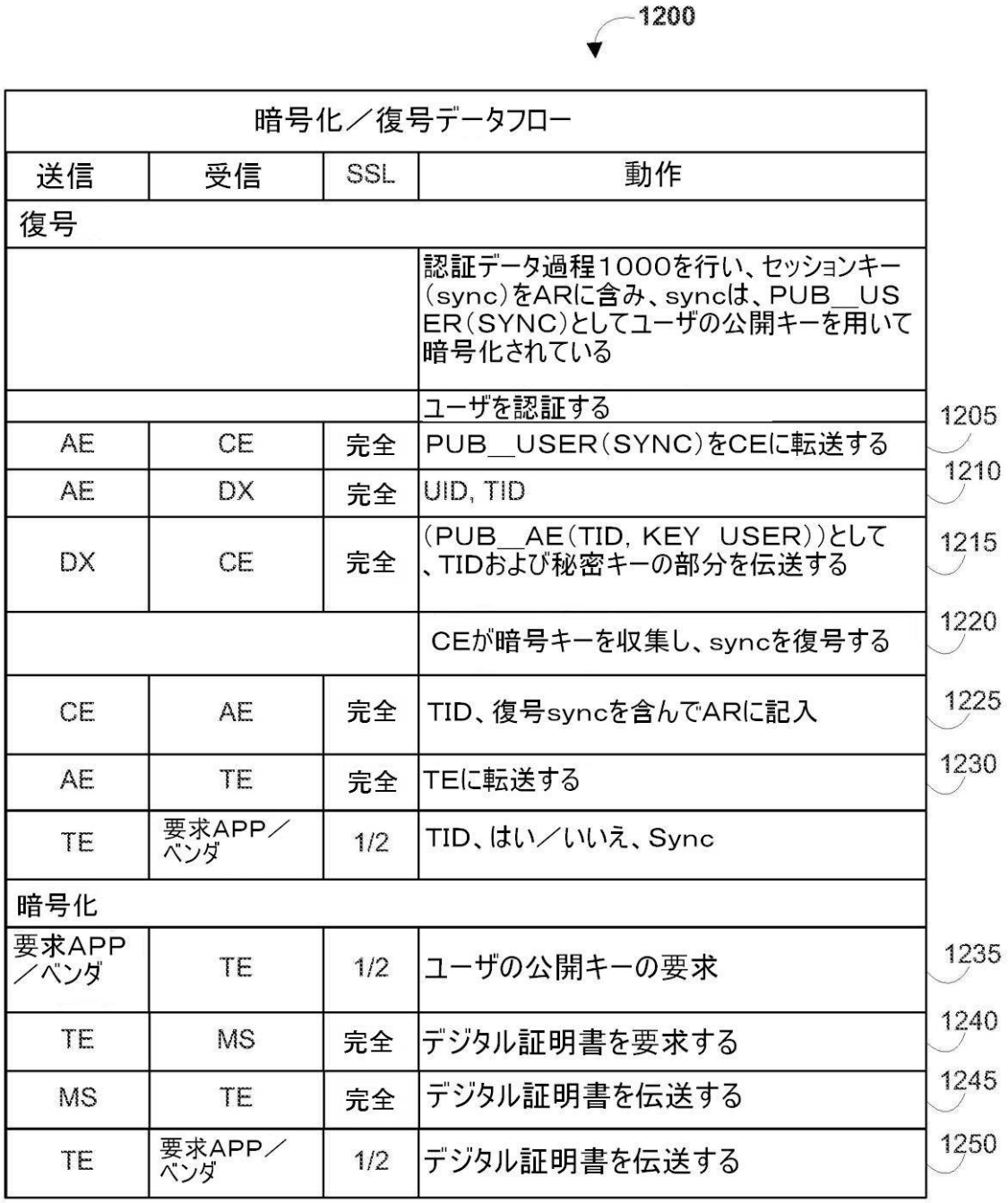
1200
暗号化／復号データフロー
送信
受信
SSL
動作
復号
認証データ過程1000を行い、セッションキー（sync）をARに含み、syncは、PUB__USER（SYNC）としてユーザの公開キーを用いて暗号化されている
ユーザを認証する
AE
CE
完全
PUB__USER（SYNC）をCEに転送する
1205
AE
DX
完全
UID, TID
1210
DX
CE
完全
（PUB__AE（TID, KEY USER））として、TIDおよび秘密キーの部分を伝送する
1215
CEが暗号キーを収集し、syncを復号する
1220
CE
AE
完全
TID、復号syncを含んでARに記入
1225
AE
TE
完全
TEに転送する
1230
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
ユーザの公開キーの要求
1235
TE
MS
完全
デジタル証明書を要求する
1240
MS
TE
完全
デジタル証明書を伝送する
1245
TE
要求APP／ベンダ
1/2
デジタル証明書を伝送する
1250

FIG. 12

【図１３】

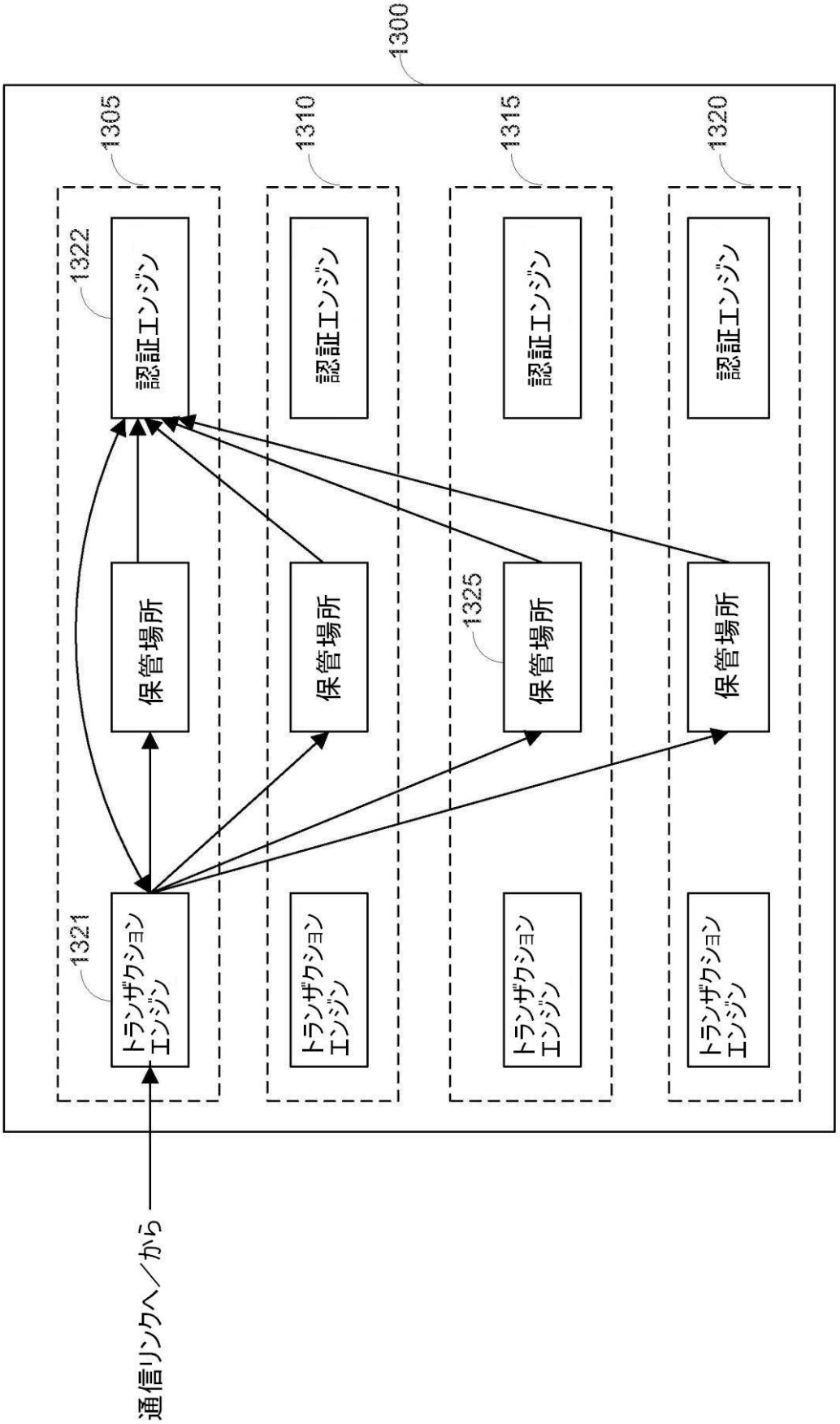
1300
1305
1310
1315
1320
1322
1325
1321
認証エンジン
保管場所
トランザクション
エンジン
通信リンクへ／から

FIG. 13

【図１４】

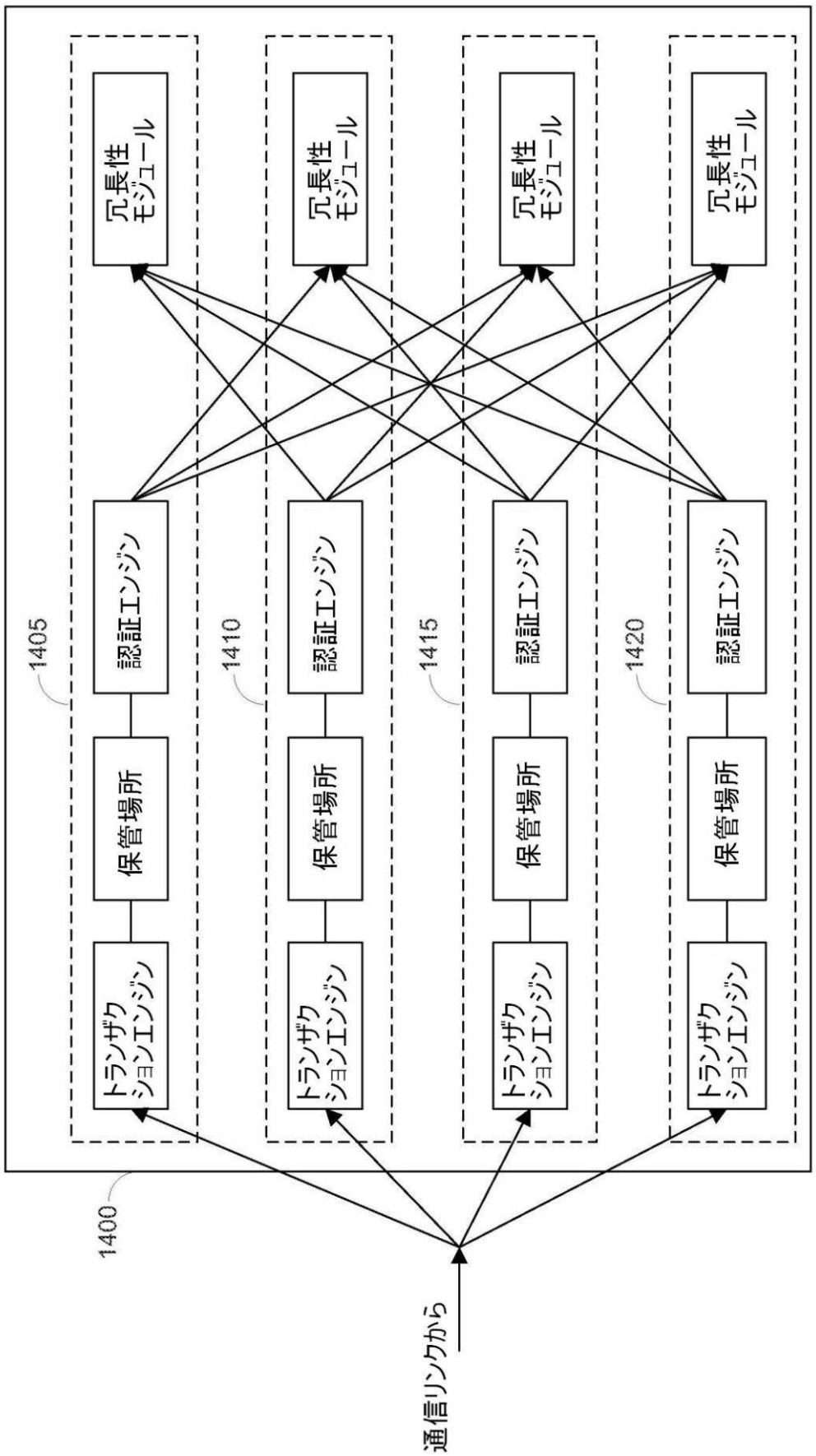
通信リンクから
1400
1405
1410
1415
1420
トランザクションエンジン
保管場所
認証エンジン
冗長性モジュール

FIG. 14

【図１５】

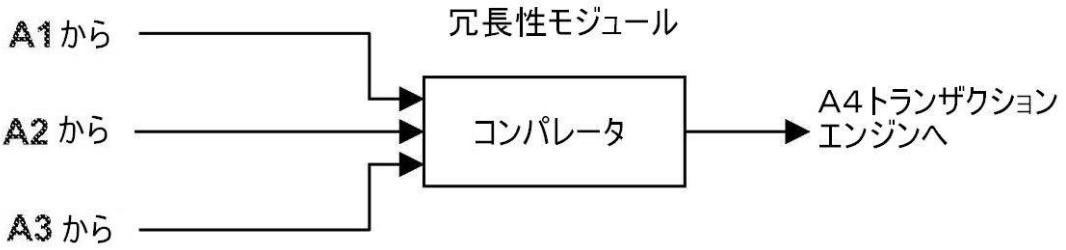

FIG. 15

【図１６】

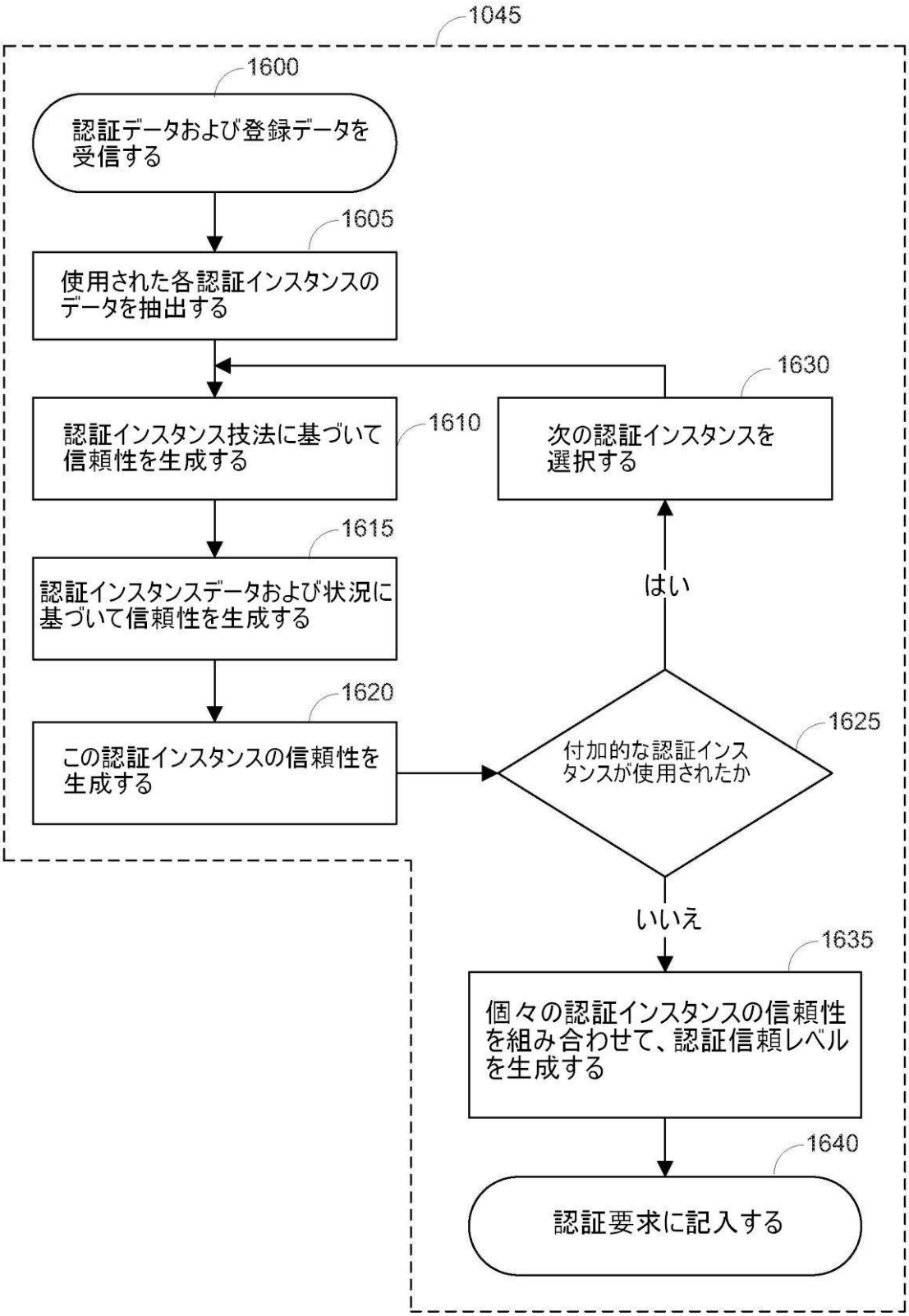
1045
1600
認証データおよび登録データを受信する
1605
使用された各認証インスタンスのデータを抽出する
1610
認証インスタンス技法に基づいて信頼性を生成する
1615
認証インスタンスデータおよび状況に基づいて信頼性を生成する
1620
この認証インスタンスの信頼性を生成する
1625
付加的な認証インスタンスが使用されたか
はい
1630
次の認証インスタンスを選択する
いいえ
1635
個々の認証インスタンスの信頼性を組み合わせて、認証信頼レベルを生成する
1640
認証要求に記入する

FIG. 16

【図１７】

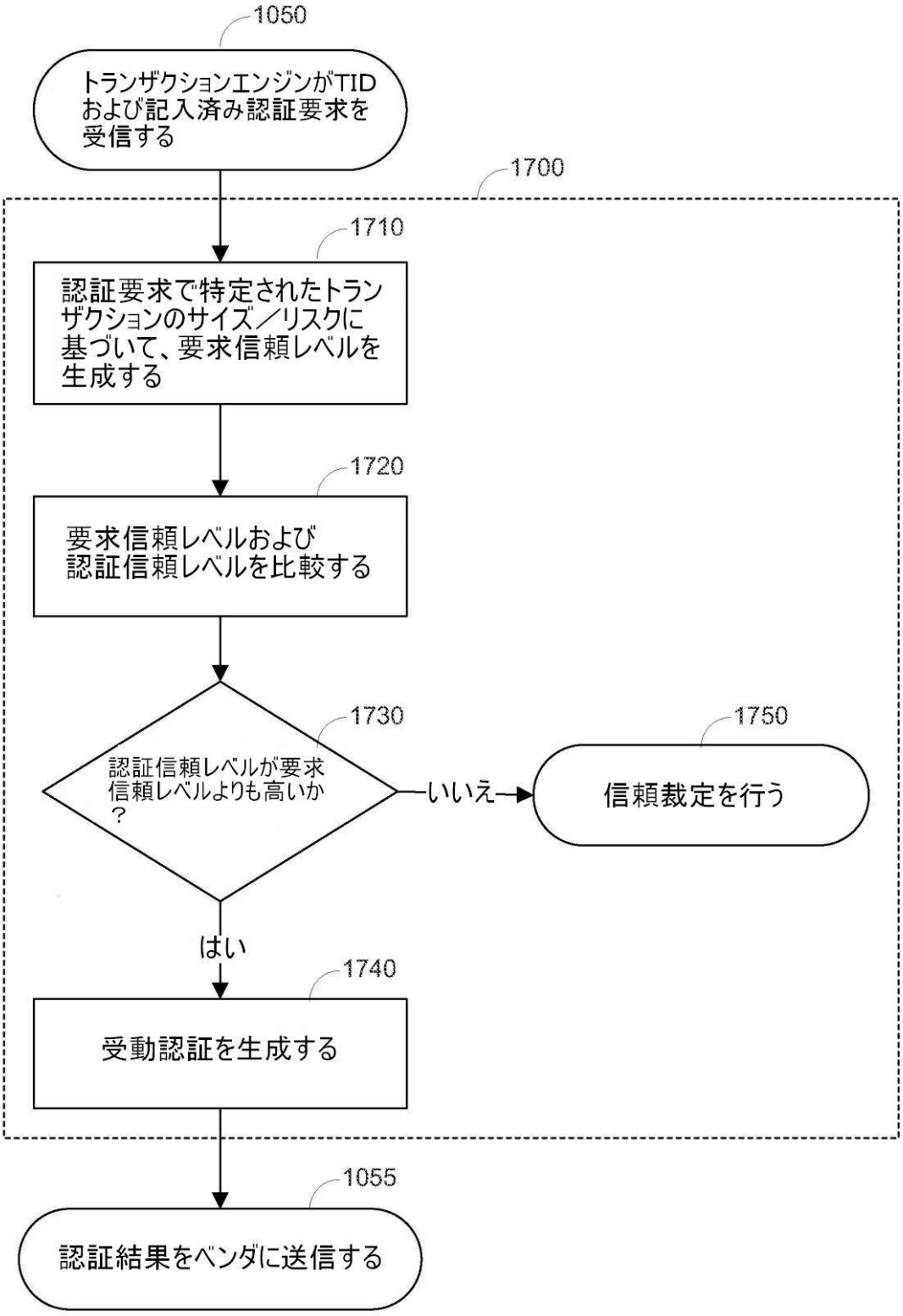
1050
トランザクションエンジンがTIDおよび記入済み認証要求を受信する
1700
1710
認証要求で特定されたトランザクションのサイズ／リスクに基づいて、要求信頼レベルを生成する
1720
要求信頼レベルおよび認証信頼レベルを比較する
1730
認証信頼レベルが要求信頼レベルよりも高いか？
いいえ
1750
信頼裁定を行う
はい
1740
受動認証を生成する
1055
認証結果をベンダに送信する

FIG. 17

【図１８】

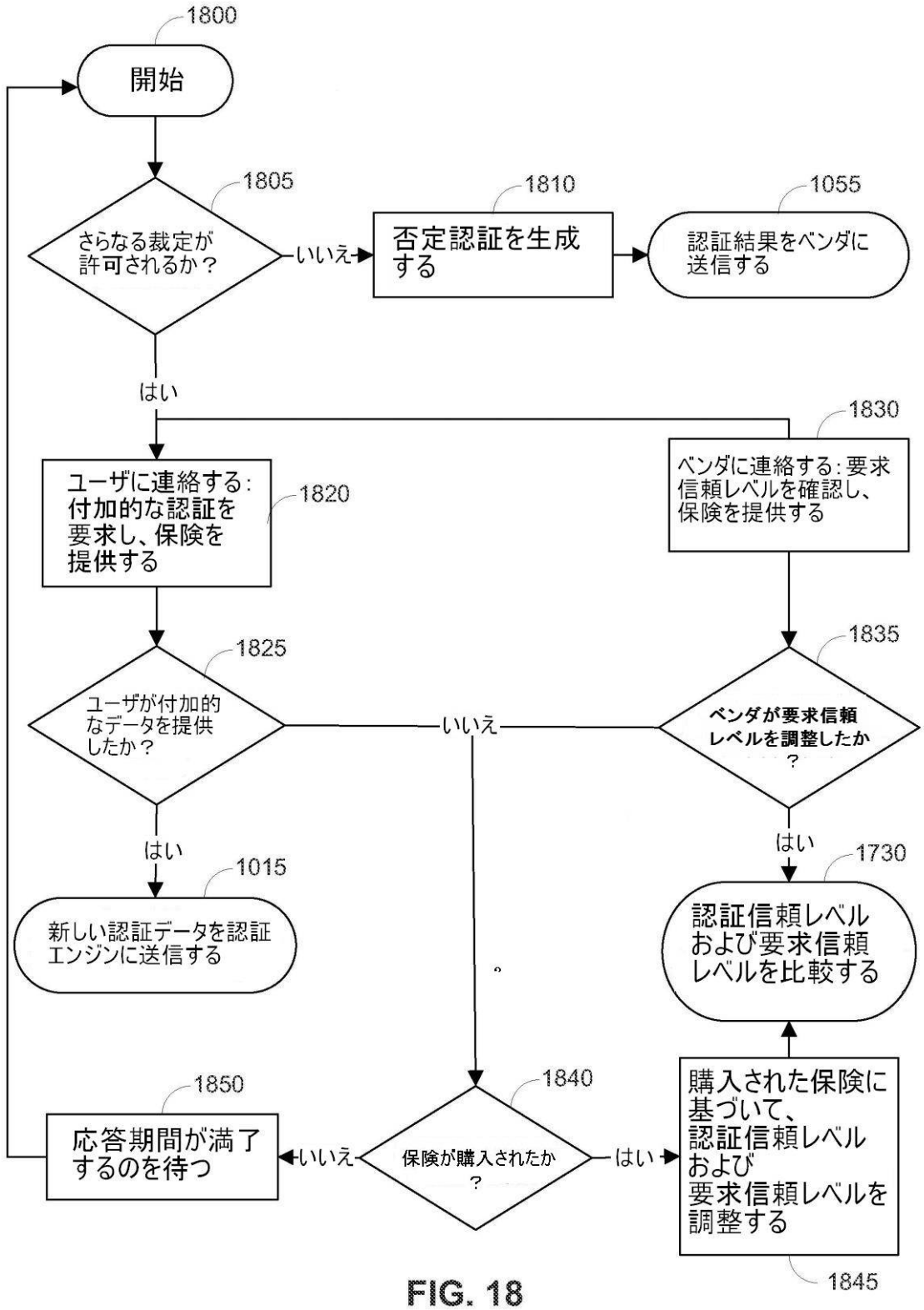
1800
開始
1805
さらなる裁定が許可されるか？
いいえ
1810
否定認証を生成する
1055
認証結果をベンダに送信する
はい
1830
ベンダに連絡する：要求信頼レベルを確認し、保険を提供する
ユーザに連絡する：付加的な認証を要求し、保険を提供する
1820
1825
ユーザが付加的なデータを提供したか？
いいえ
1835
ベンダが要求信頼レベルを調整したか？
はい
1015
新しい認証データを認証エンジンに送信する
はい
1730
認証信頼レベルおよび要求信頼レベルを比較する
1850
応答期間が満了するのを待つ
いいえ
1840
保険が購入されたか？
はい
購入された保険に基づいて、認証信頼レベルおよび要求信頼レベルを調整する
1845

FIG. 18

【図１９】

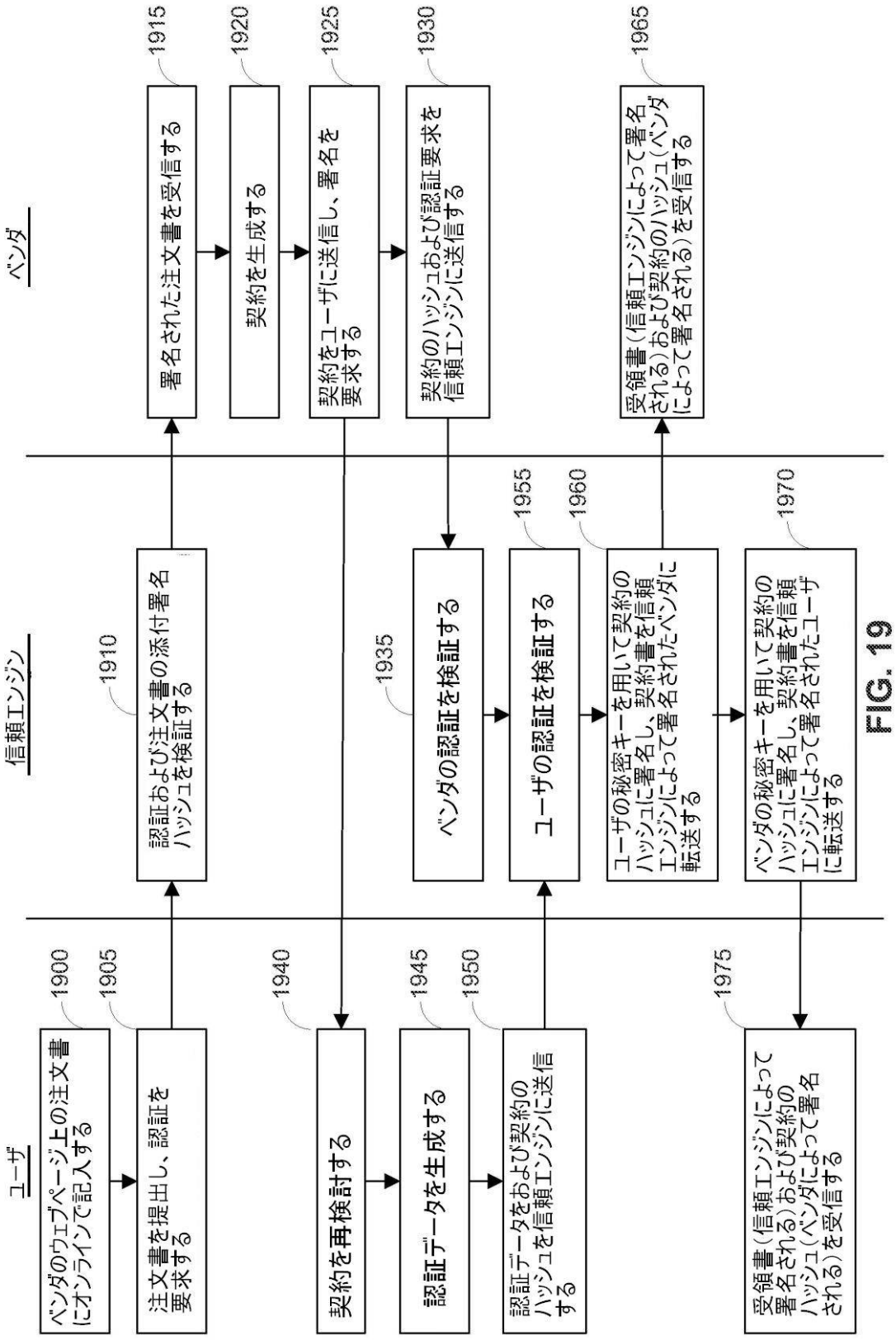
ユーザ
ベンダ
信頼エンジン
ベンダのウェブページ上の注文書にオンラインで記入する
1900
注文書を提出し、認証を要求する
1905
認証および注文書の添付署名ハッシュを検証する
1910
署名された注文書を受信する
1915
契約を生成する
1920
契約をユーザに送信し、署名を要求する
1925
契約のハッシュおよび認証要求を信頼エンジンに送信する
1930
契約を再検討する
1940
認証データを生成する
1945
認証データをおよび契約のハッシュを信頼エンジンに送信する
1950
ベンダの認証を検証する
1935
ユーザの認証を検証する
1955
ユーザの秘密キーを用いて契約のハッシュに署名し、契約書を信頼エンジンによって署名されたベンダに転送する
1960
受領書（信頼エンジンによって署名される）および契約のハッシュ（ベンダによって署名される）を受信する
1965
ベンダの秘密キーを用いて契約のハッシュに署名し、契約書を信頼エンジンによって署名されたユーザに転送する
1970
受領書（信頼エンジンによって署名される）および契約のハッシュ（ベンダによって署名される）を受信する
1975

FIG. 19

【図２０】

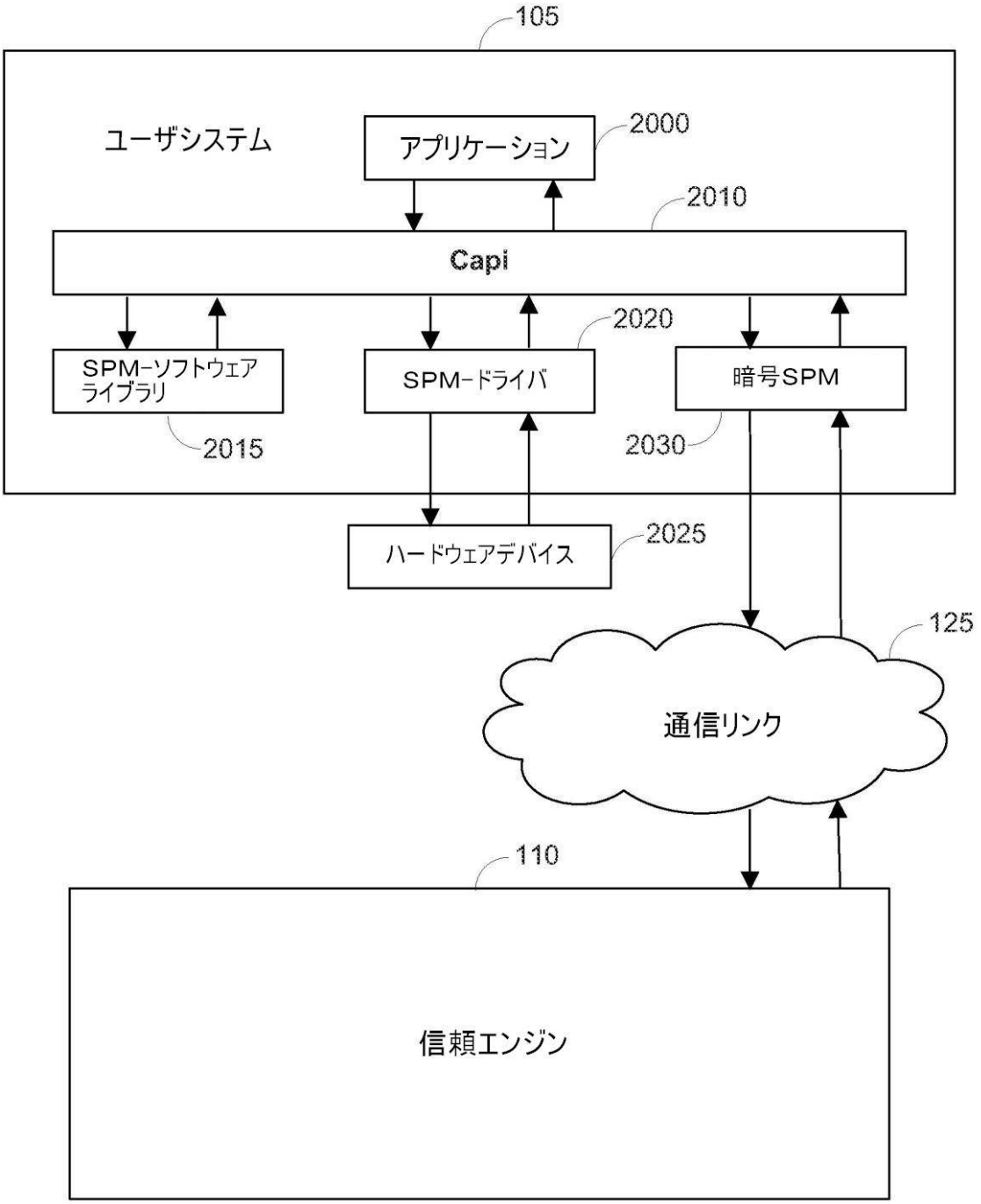
105
ユーザシステム
アプリケーション
2000
2010
Capi
SPM−ソフトウェア
ライブラリ
2015
SPM−ドライバ
2020
暗号SPM
2030
ハードウェアデバイス
2025
125
通信リンク
110
信頼エンジン

FIG. 20

【図２１】

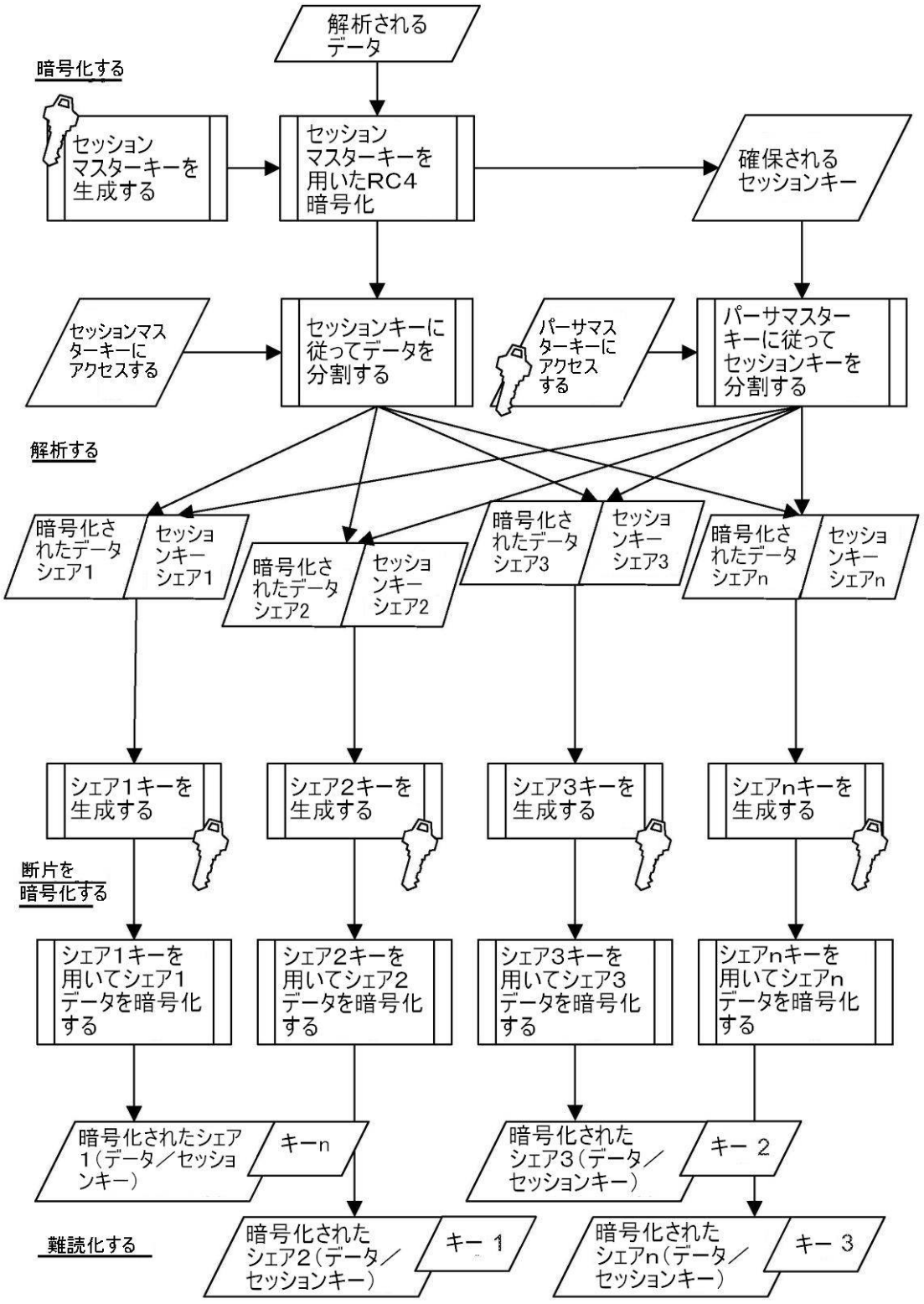
解析される
データ
暗号化する
セッション
マスターキーを
生成する
セッション
マスターキーを
用いたRC4
暗号化
確保される
セッションキー
セッションマス
ターキーに
アクセスする
セッションキーに
従ってデータを
分割する
パーサマス
ターキーに
アクセス
する
パーサマスター
キーに従って
セッションキーを
分割する
解析する
暗号化さ
れたデータ
シェア1
セッショ
ンキー
シェア1
暗号化さ
れたデータ
シェア2
セッショ
ンキー
シェア2
暗号化さ
れたデータ
シェア3
セッショ
ンキー
シェア3
暗号化さ
れたデータ
シェアn
セッショ
ンキー
シェアn
シェア1キーを
生成する
シェア2キーを
生成する
シェア3キーを
生成する
シェアnキーを
生成する
断片を
暗号化する
シェア1キーを
用いてシェア1
データを暗号化
する
シェア2キーを
用いてシェア2
データを暗号化
する
シェア3キーを
用いてシェア3
データを暗号化
する
シェアnキーを
用いてシェアn
データを暗号化
する
暗号化されたシェア
1（データ／セッショ
ンキー）
キーn
暗号化された
シェア3（データ／
セッションキー）
キー 2
難読化する
暗号化された
シェア2（データ／
セッションキー）
キー 1
暗号化された
シェアn（データ／
セッションキー）
キー 3

FIG. 21

【図２２】

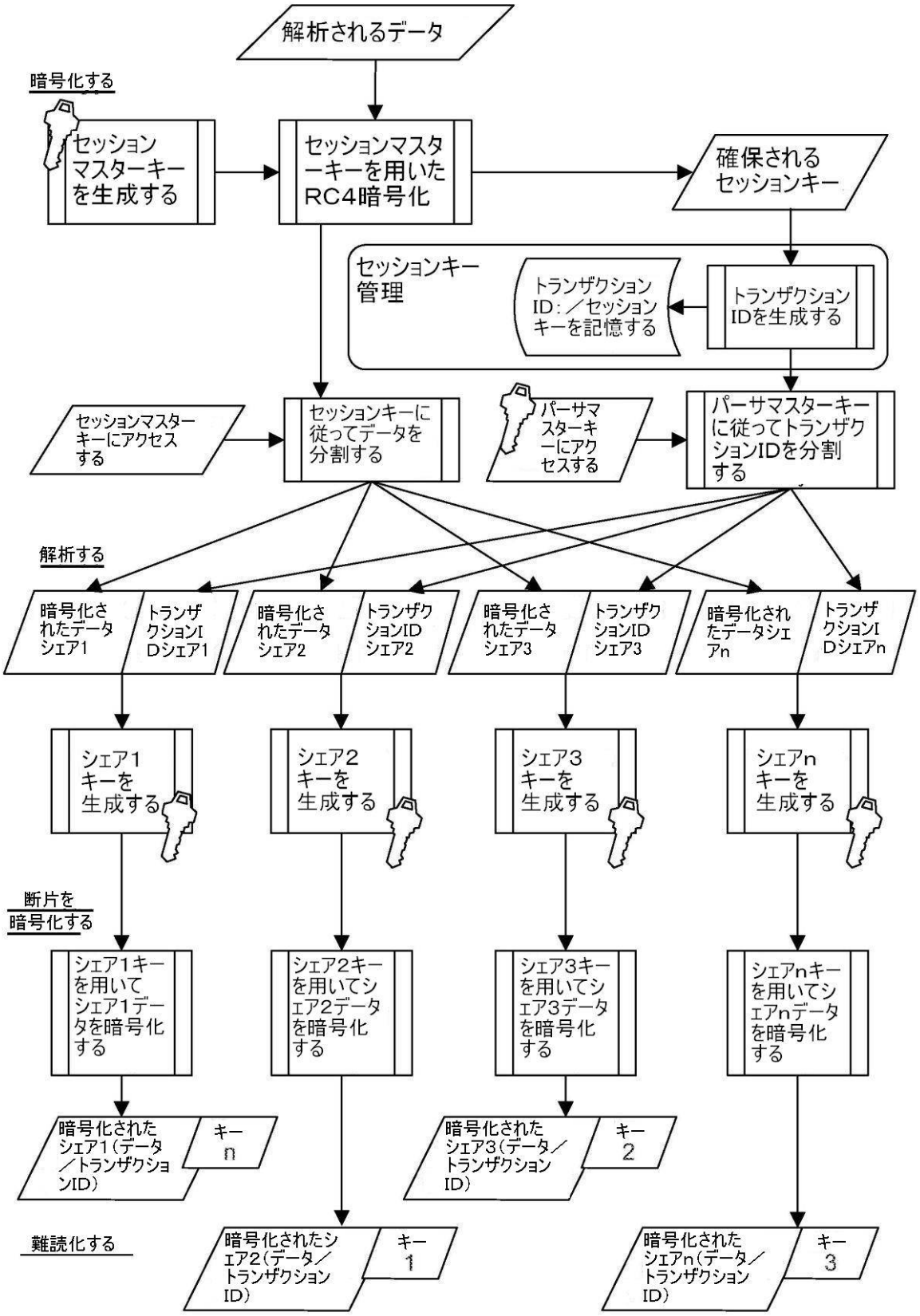
解析されるデータ
暗号化する
セッション
マスターキー
を生成する
セッションマスター
キーを用いた
RC4暗号化
確保される
セッションキー
セッションキー
管理
トランザクション
ID：／セッション
キーを記憶する
トランザクション
IDを生成する
セッションマスター
キーにアクセス
する
セッションキーに
従ってデータを
分割する
パーサマ
スターキ
ーにアク
セスする
パーサマスターキー
に従ってトランザク
ションIDを分割
する
解析する
暗号化さ
れたデータ
シェア1
トランザ
クションI
Dシェア1
暗号化さ
れたデータ
シェア2
トランザク
ションID
シェア2
暗号化さ
れたデータ
シェア3
トランザク
ションID
シェア3
暗号化され
たデータシェ
アn
トランザ
クションI
Dシェアn
シェア1
キーを
生成する
シェア2
キーを
生成する
シェア3
キーを
生成する
シェアn
キーを
生成する
断片を
暗号化する
シェア1キー
を用いて
シェア1デー
タを暗号化
する
シェア2キー
を用いてシ
ェア2データ
を暗号化
する
シェア3キー
を用いてシ
ェア3データ
を暗号化
する
シェアnキー
を用いてシ
ェアnデータ
を暗号化
する
暗号化された
シェア1（データ
／トランザクショ
ンID）
キー
n
暗号化された
シェア3（データ／
トランザクション
ID）
キー
2
難読化する
暗号化されたシ
ェア2（データ／
トランザクション
ID）
キー
1
暗号化された
シェアn（データ／
トランザクション
ID）
キー
3

FIG. 22

【図２３】

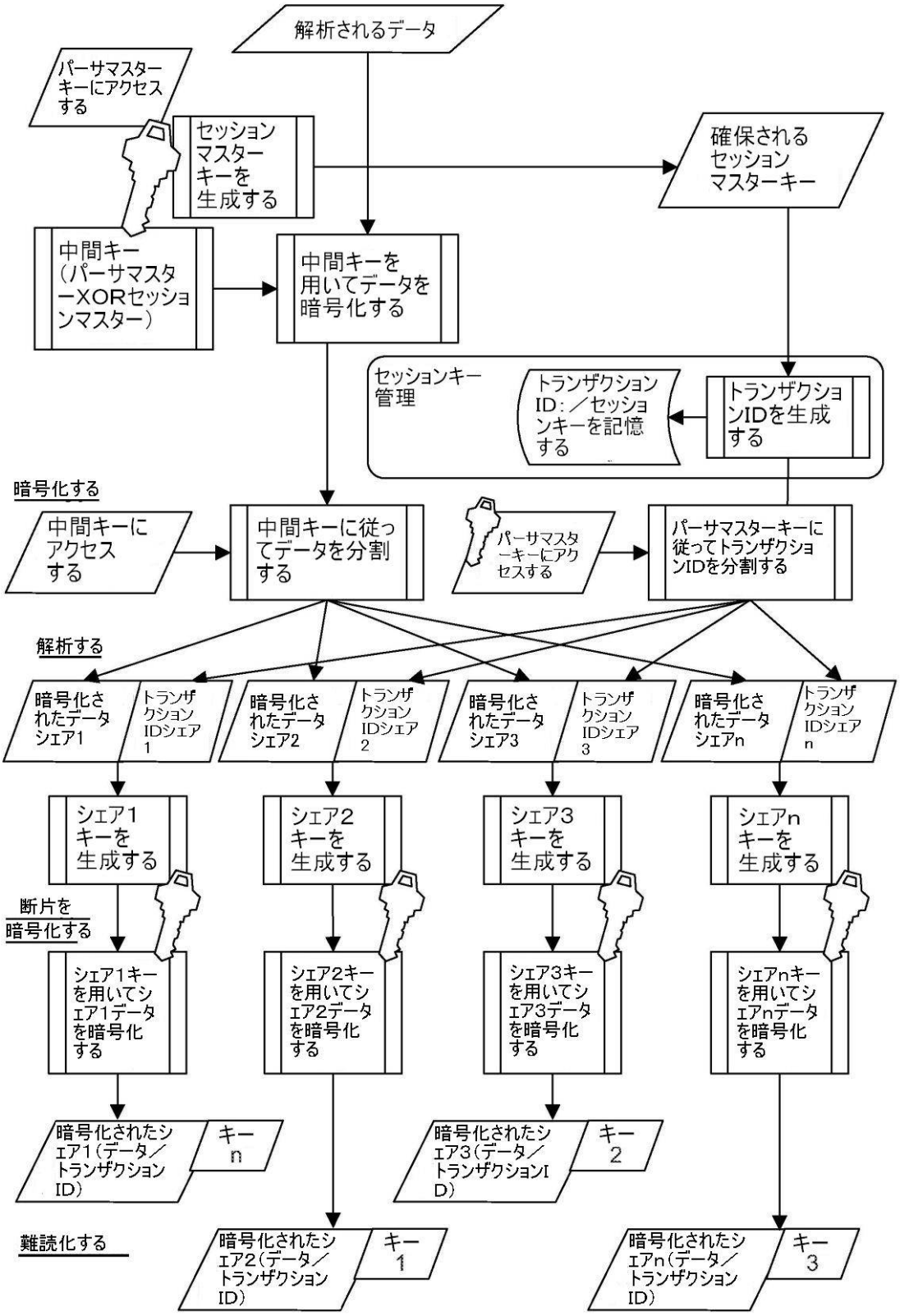
解析されるデータ
パーサマスターキーにアクセスする
セッションマスターキーを生成する
確保されるセッションマスターキー
中間キー（パーサマスターXORセッションマスター）
中間キーを用いてデータを暗号化する
セッションキー管理
トランザクションID：／セッションキーを記憶する
トランザクションIDを生成する
暗号化する
中間キーにアクセスする
中間キーに従ってデータを分割する
パーサマスターキーにアクセスする
パーサマスターキーに従ってトランザクションIDを分割する
解析する
暗号化されたデータシェア1
トランザクションIDシェア1
暗号化されたデータシェア2
トランザクションIDシェア2
暗号化されたデータシェア3
トランザクションIDシェア3
暗号化されたデータシェアn
トランザクションIDシェアn
シェア1キーを生成する
シェア2キーを生成する
シェア3キーを生成する
シェアnキーを生成する
断片を暗号化する
シェア1キーを用いてシェア1データを暗号化する
シェア2キーを用いてシェア2データを暗号化する
シェア3キーを用いてシェア3データを暗号化する
シェアnキーを用いてシェアnデータを暗号化する
暗号化されたシェア1（データ／トランザクションID）
キーn
暗号化されたシェア3（データ／トランザクションID）
キー2
難読化する
暗号化されたシェア2（データ／トランザクションID）
キー1
暗号化されたシェアn（データ／トランザクションID）
キー3

FIG. 23

【図２４】

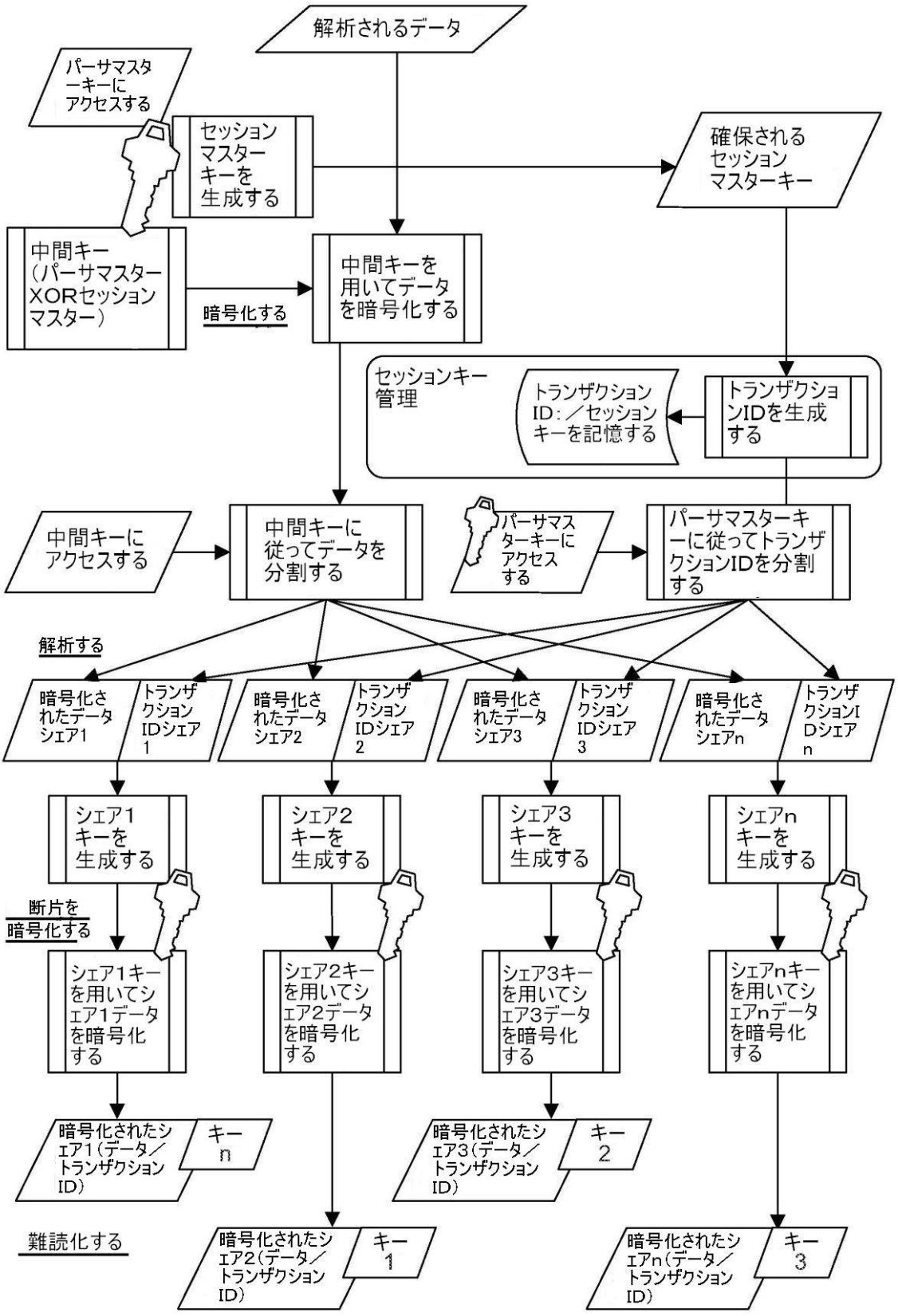
解析されるデータ
パーサマスターキーにアクセスする
セッションマスターキーを生成する
確保されるセッションマスターキー
中間キー（パーサマスターXORセッションマスター）
暗号化する
中間キーを用いてデータを暗号化する
セッションキー管理
トランザクションID：／セッションキーを記憶する
トランザクションIDを生成する
中間キーにアクセスする
中間キーに従ってデータを分割する
パーサマスターキーにアクセスする
パーサマスターキーに従ってトランザクションIDを分割する
解析する
暗号化されたデータシェア1
トランザクションIDシェア1
暗号化されたデータシェア2
トランザクションIDシェア2
暗号化されたデータシェア3
トランザクションIDシェア3
暗号化されたデータシェアn
トランザクションIDシェアn
シェア1キーを生成する
シェア2キーを生成する
シェア3キーを生成する
シェアnキーを生成する
断片を暗号化する
シェア1キーを用いてシェア1データを暗号化する
シェア2キーを用いてシェア2データを暗号化する
シェア3キーを用いてシェア3データを暗号化する
シェアnキーを用いてシェアnデータを暗号化する
暗号化されたシェア1（データ／トランザクションID）
キーn
暗号化されたシェア3（データ／トランザクションID）
キー2
難読化する
暗号化されたシェア2（データ／トランザクションID）
キー1
暗号化されたシェアn（データ／トランザクションID）
キー3

FIG. 24

【図２５】

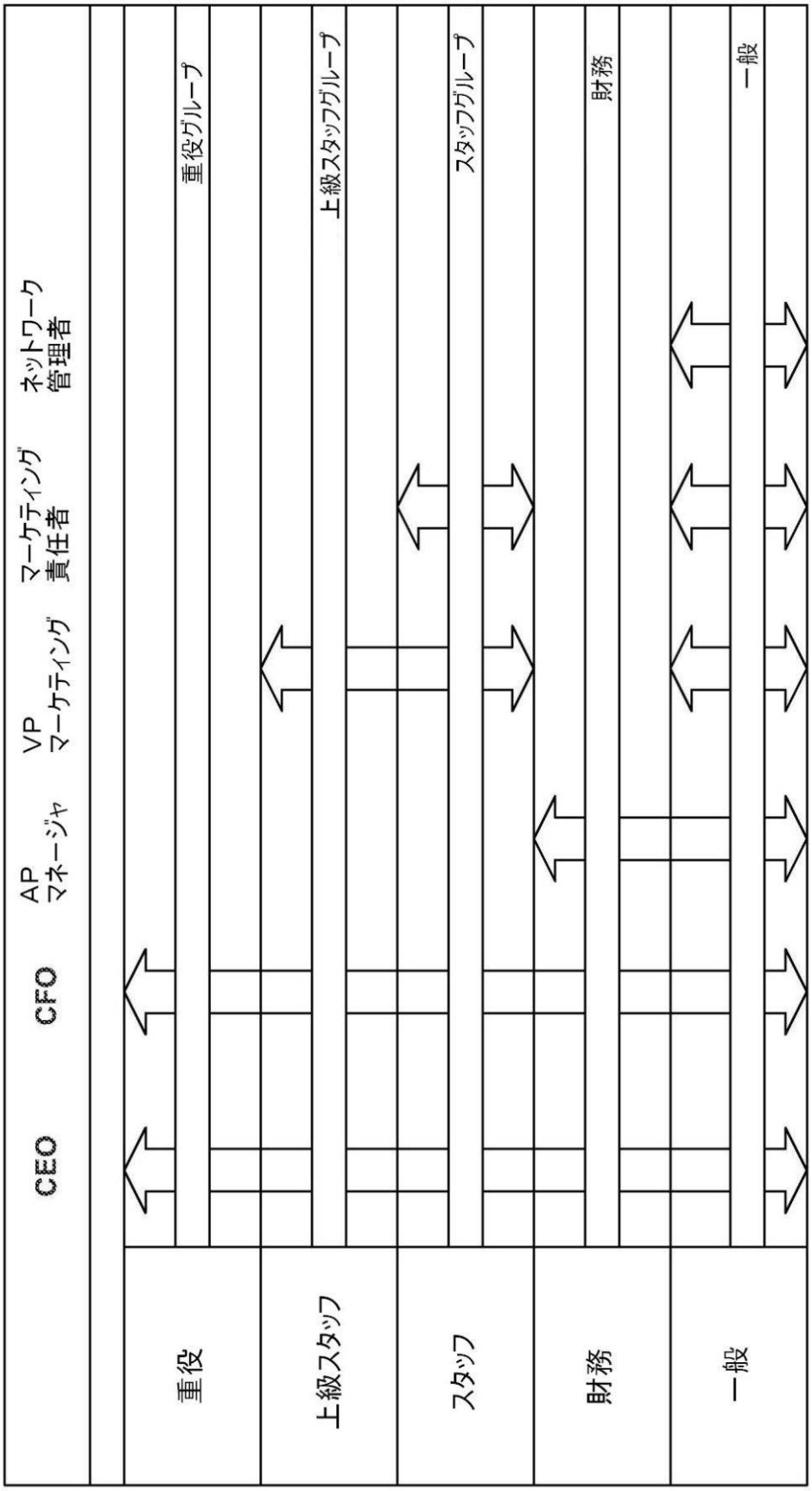
CEO
CFO
AP
マネージャ
VP
マーケティング
マーケティング
責任者
ネットワーク
管理者
重役
上級スタッフ
スタッフ
財務
一般
重役グループ
上級スタッフグループ
スタッフグループ
財務
一般

FIG. 25

【図２６】

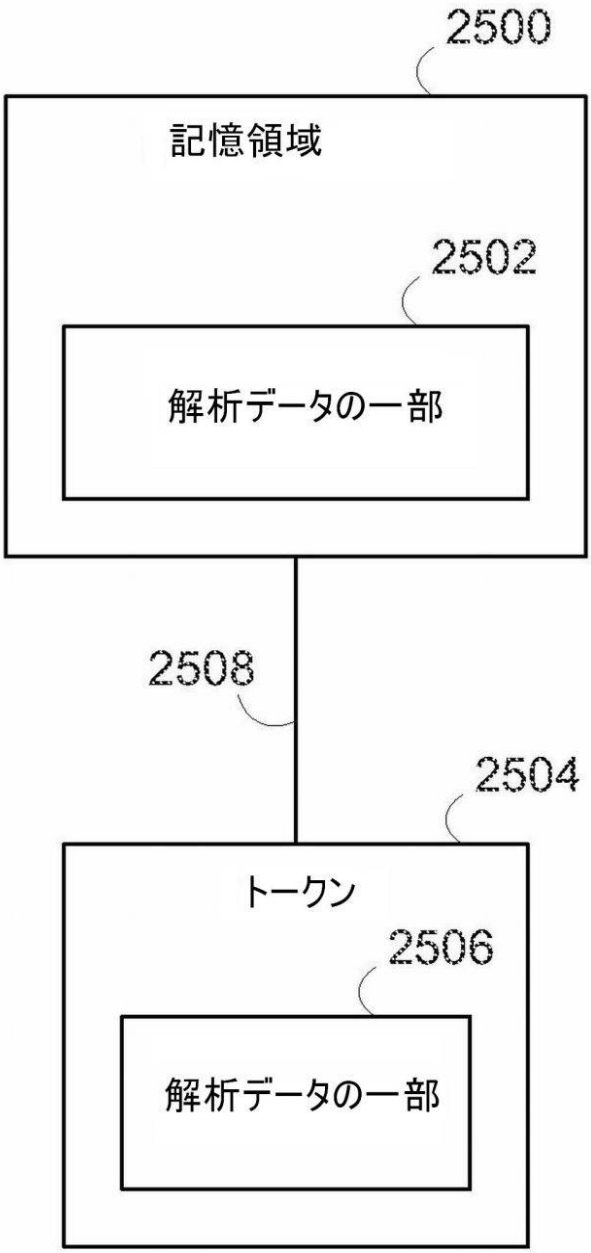

FIG. 26

【図２７】

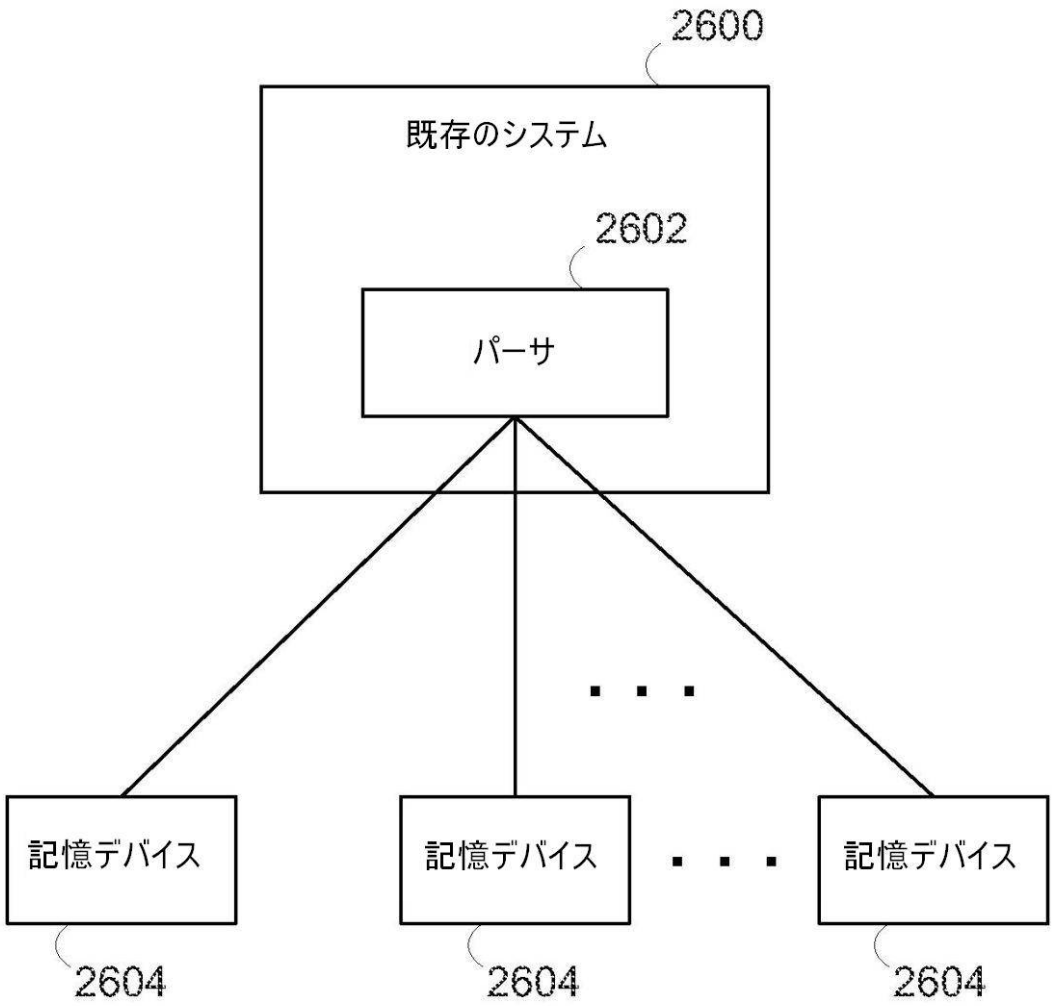

FIG. 27

【図２８】

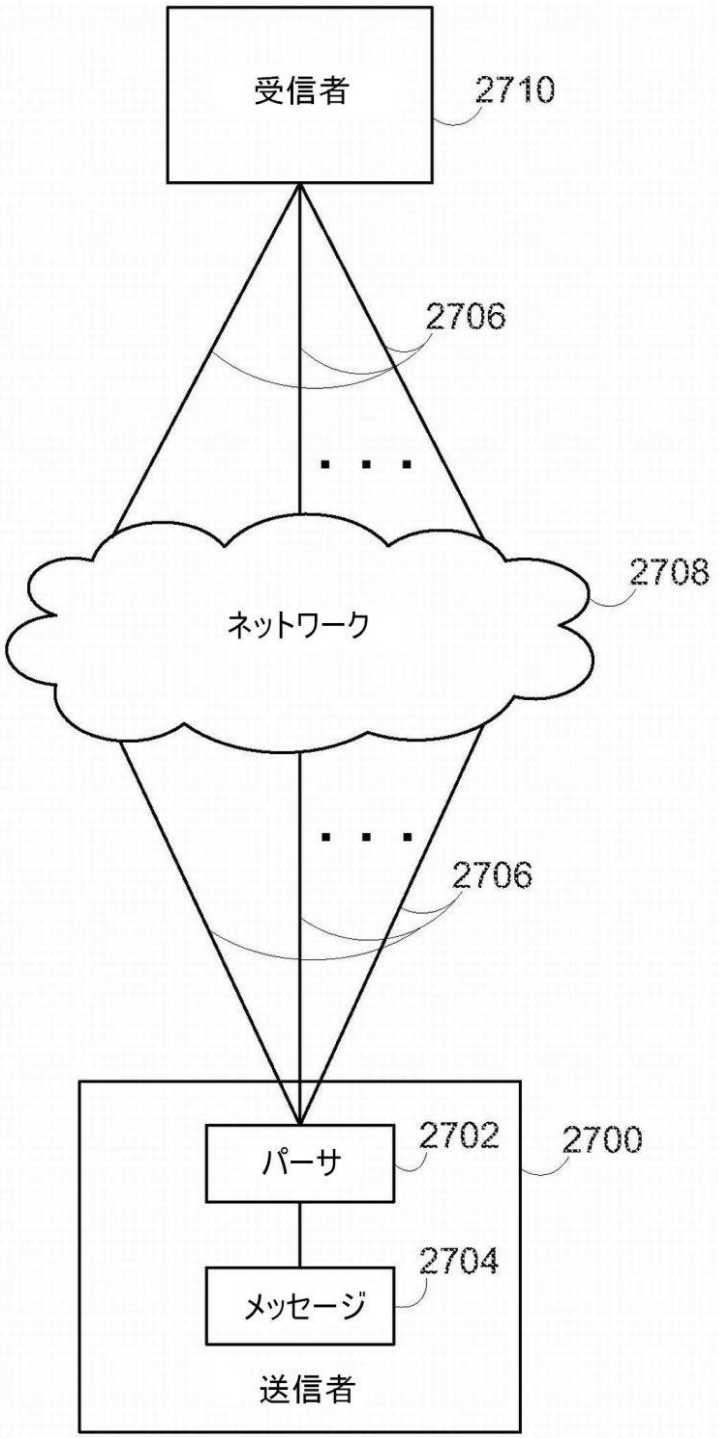

FIG. 28

【図２９】

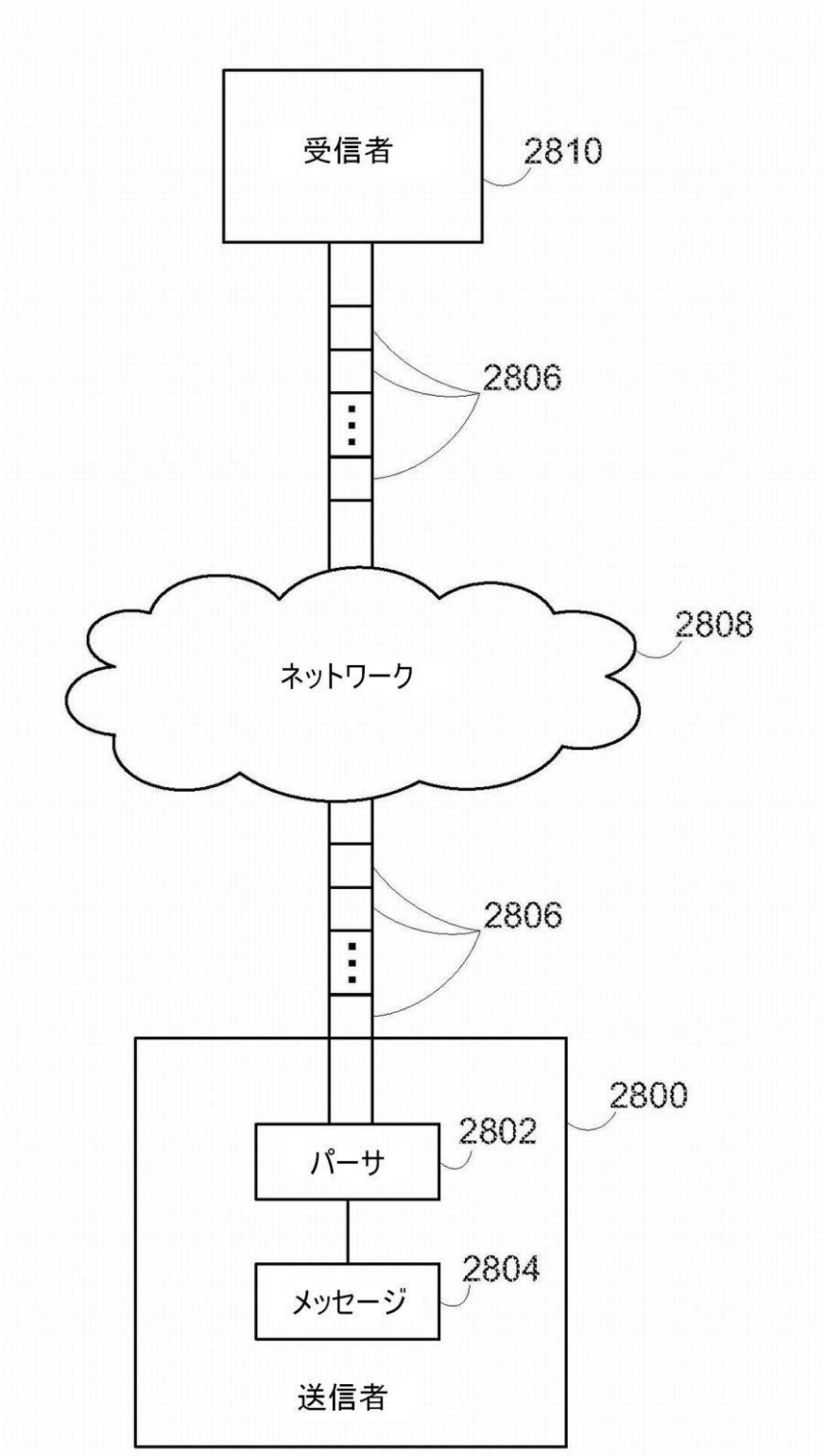

FIG. 29

【図３０】

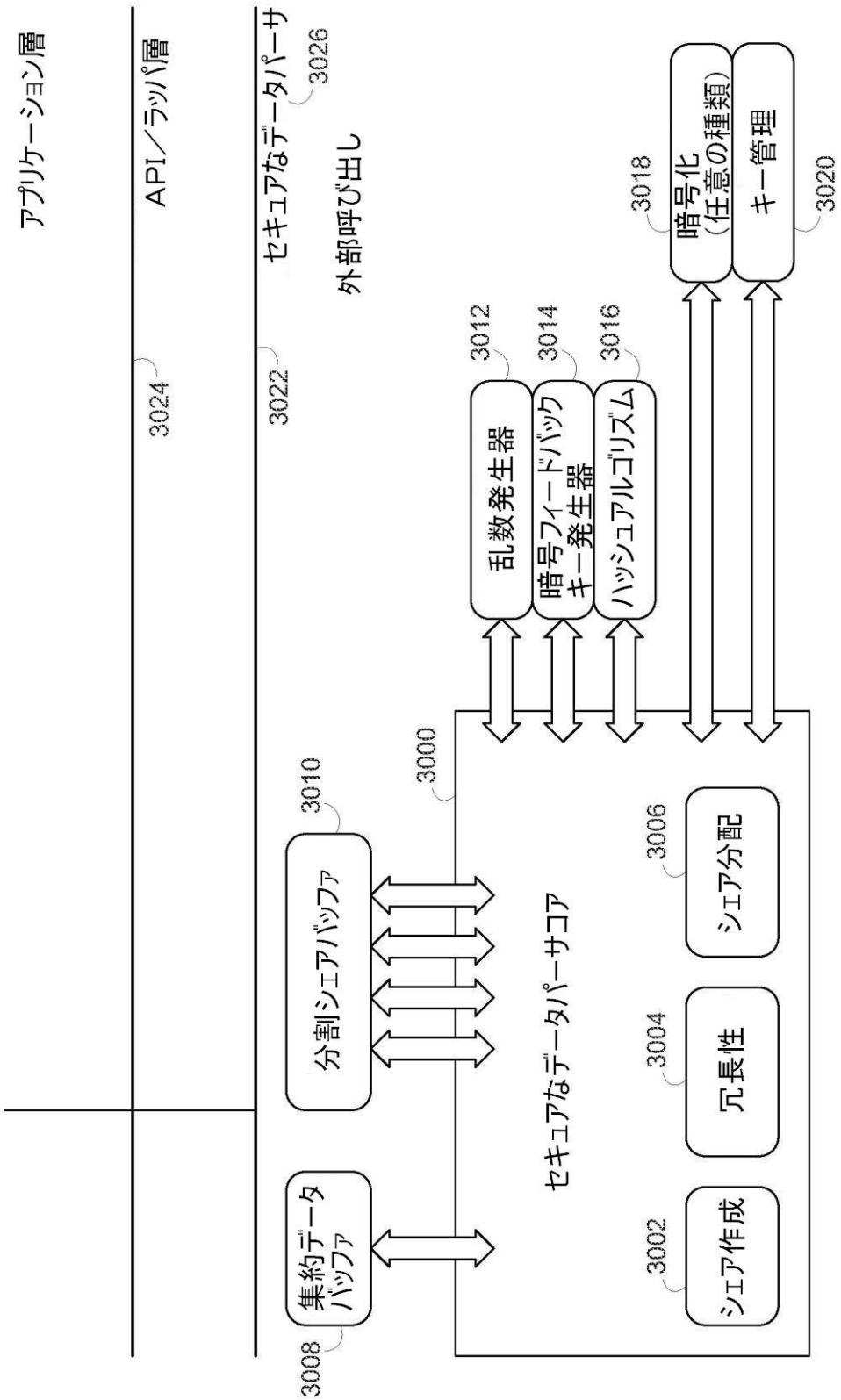
アプリケーション層
API／ラッパ層
セキュアなデータパーサ
3026
外部呼び出し
3024
3022
3012
乱数発生器
3014
暗号フィードバック
キー発生器
3016
ハッシュアルゴリズム
3018
暗号化
（任意の種類）
3020
キー管理
3000
3010
分割シェアバッファ
3006
シェア分配
セキュアなデータパーサコア
3004
冗長性
3002
シェア作成
3008
集約データ
バッファ

FIG. 30

【図３１】

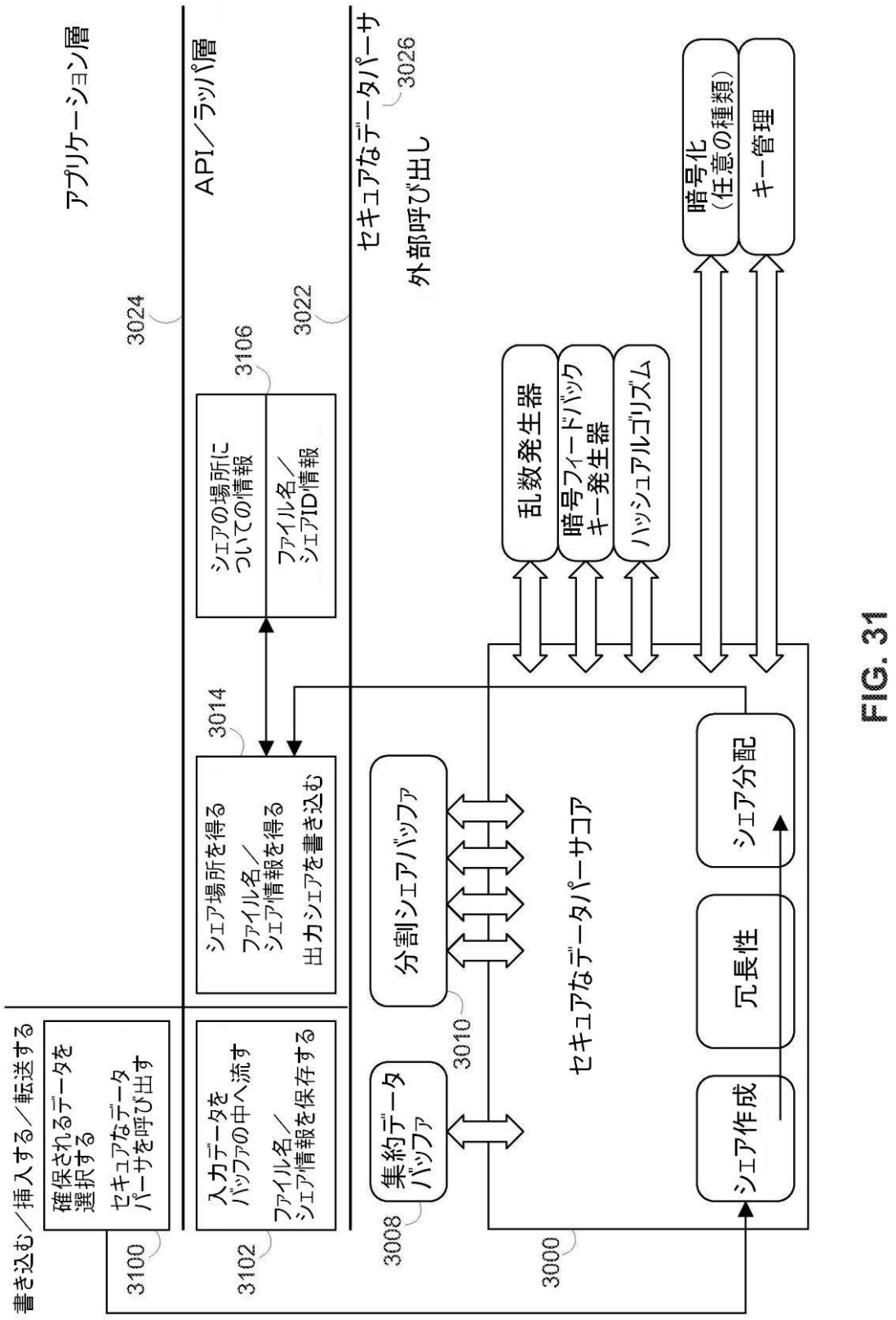
アプリケーション層
API／ラッパ層
セキュアなデータパーサ
外部呼び出し
3024
3022
3026
3106
3014
3100
3102
3008
3010
3000
書き込む／挿入する／転送する
確保されるデータを選択する
セキュアなデータパーサを呼び出す
入力データをバッファの中へ流す
ファイル名／シェア情報を保存する
シェア場所を得るファイル名／シェア情報を得る出力シェアを書き込む
シェアの場所についての情報
ファイル名／シェアID情報
集約データバッファ
分割シェアバッファ
セキュアなデータパーサコア
シェア作成
冗長性
シェア分配
乱数発生器
暗号フィードバックキー発生器
ハッシュアルゴリズム
暗号化（任意の種類）
キー管理

FIG. 31

【図３２】

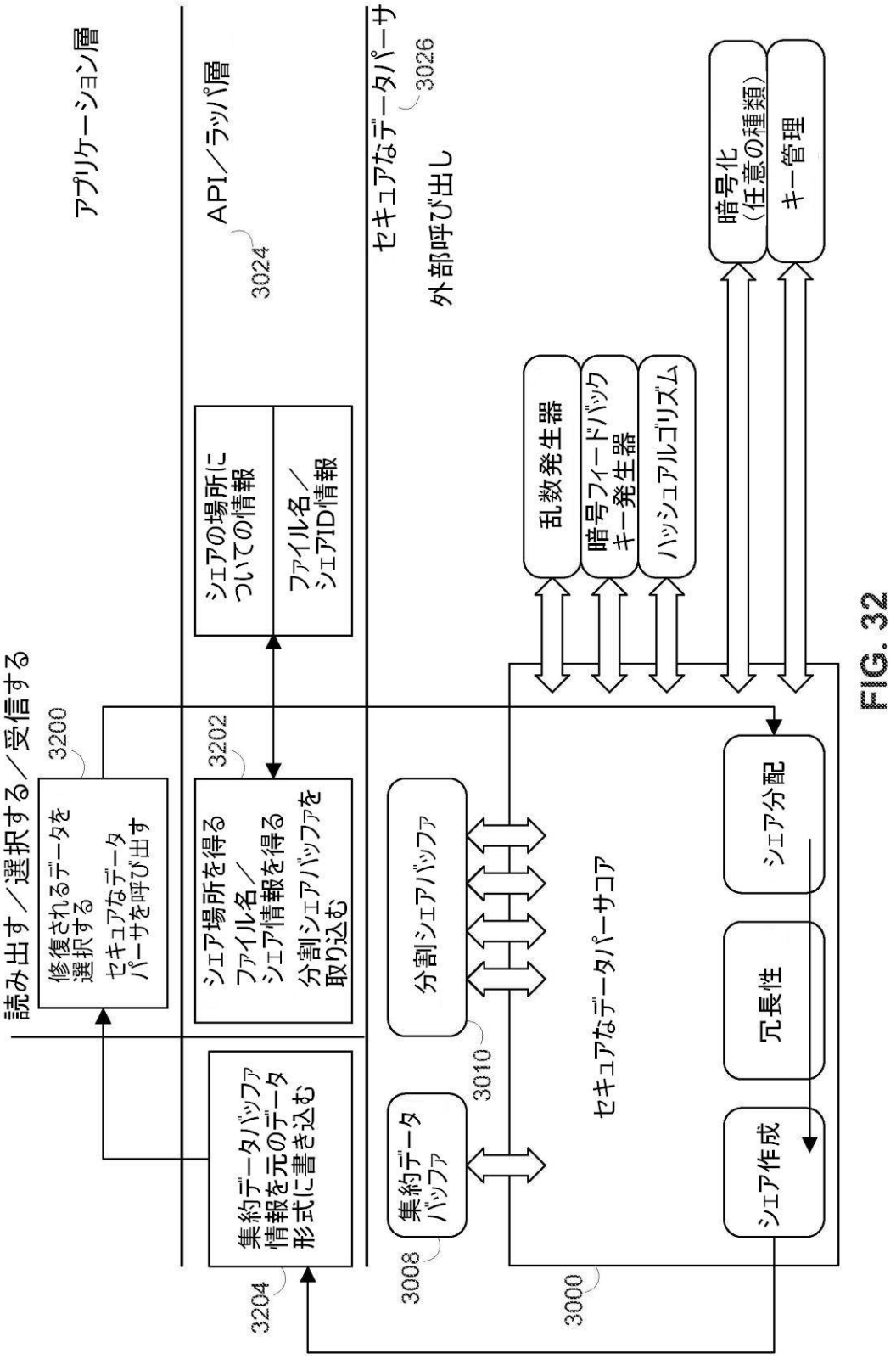
アプリケーション層
API／ラッパ層
3024
セキュアなデータパーサ
3026
外部呼び出し
読み出す／選択する／受信する
3200
修復されるデータを選択する
セキュアなデータパーサを呼び出す
3202
シェア場所を得る
ファイル名／シェア情報を得る
分割シェアバッファを取り込む
シェアの場所についての情報
ファイル名／シェアID情報
集約データバッファ情報を元のデータ形式に書き込む
3204
集約データバッファ
3008
分割シェアバッファ
3010
セキュアなデータパーサコア
3000
乱数発生器
暗号フィードバックキー発生器
ハッシュアルゴリズム
暗号化（任意の種類）
キー管理
シェア分配
冗長性
シェア作成

FIG. 32

【図３３】

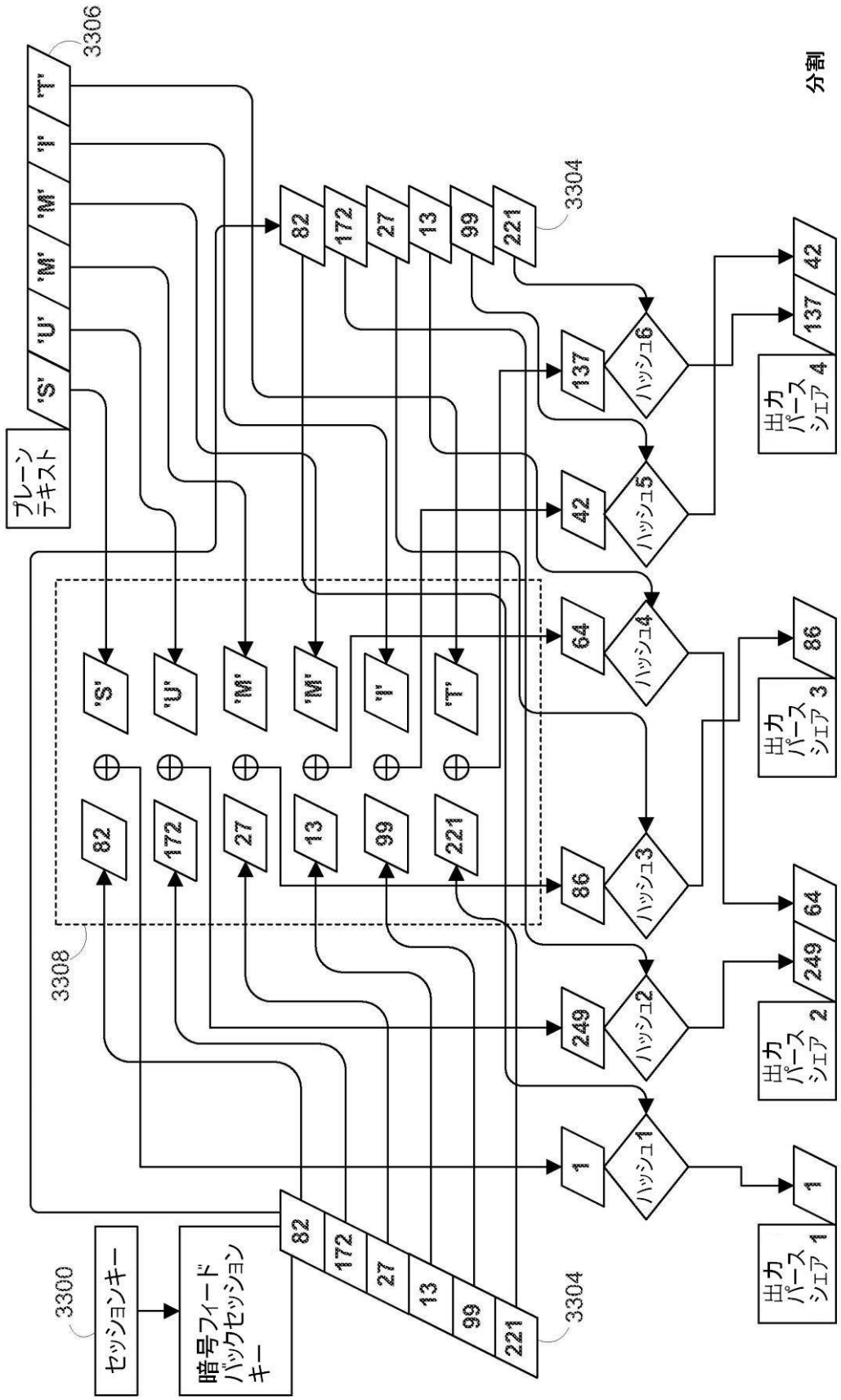
3306
プレーンテキスト
'S' 'U' 'M' 'M' 'I' 'T'
3300
セッションキー
暗号フィードバックセッションキー
82 172 27 13 99 221
3304
3308
82 172 27 13 99 221
'S' 'U' 'M' 'M' 'I' 'T'
1 249 86 64 42 137
ハッシュ1
ハッシュ2
ハッシュ3
ハッシュ4
ハッシュ5
ハッシュ6
出力パースシェア 1
出力パースシェア 2
出力パースシェア 3
出力パースシェア 4
分割

FIG. 33

【図３４】

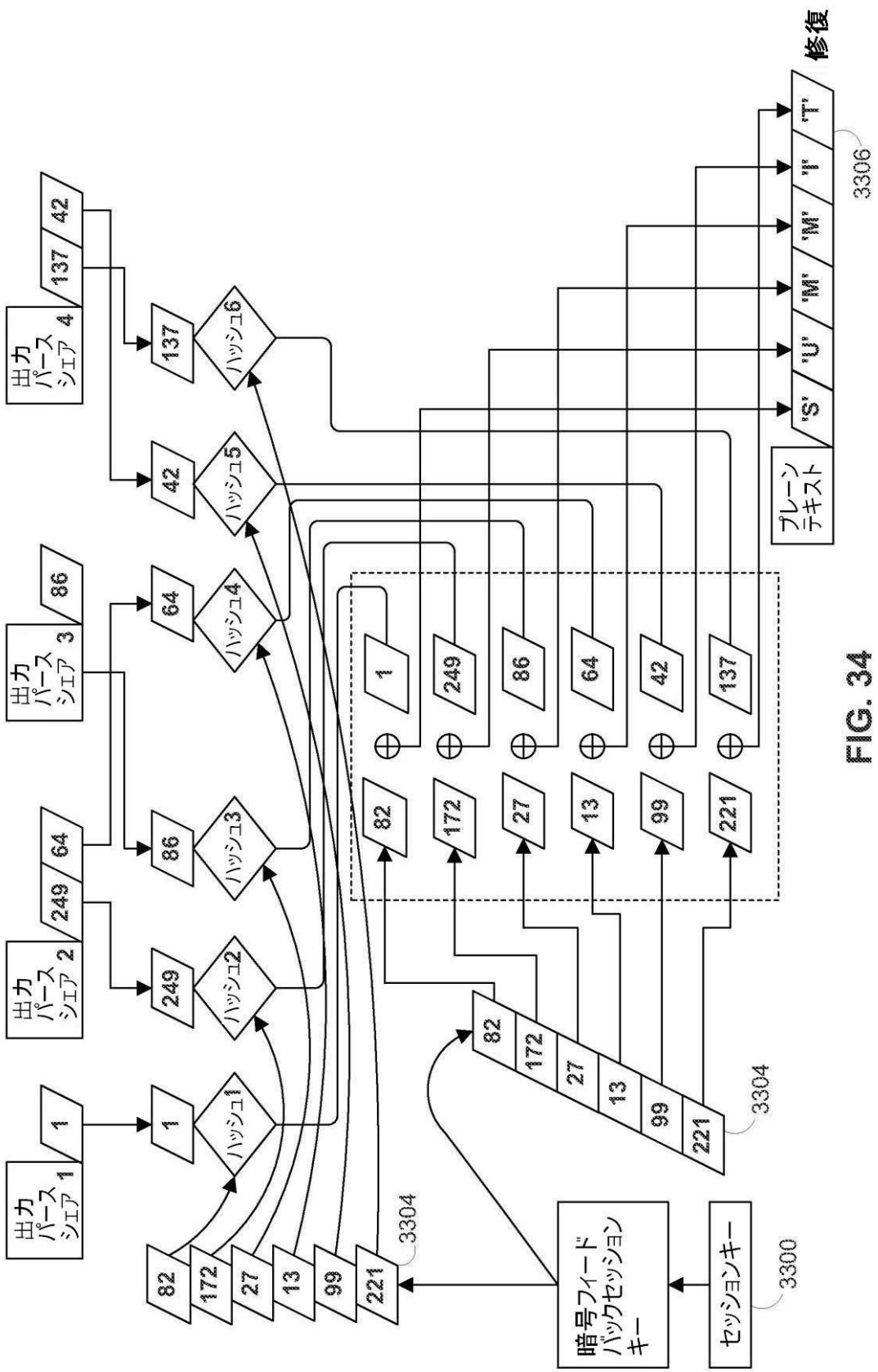
出力
パース
シェア 1
出力
パース
シェア 2
出力
パース
シェア 3
出力
パース
シェア 4
ハッシュ1
ハッシュ2
ハッシュ3
ハッシュ4
ハッシュ5
ハッシュ6
1
249
86
64
42
137
82
172
27
13
99
221
3304
3300
暗号フィード
バックセッション
キー
セッションキー
プレーン
テキスト
'S'
'U'
'M'
'M'
'I'
'T'
修復
3306

FIG. 34

【図３５】

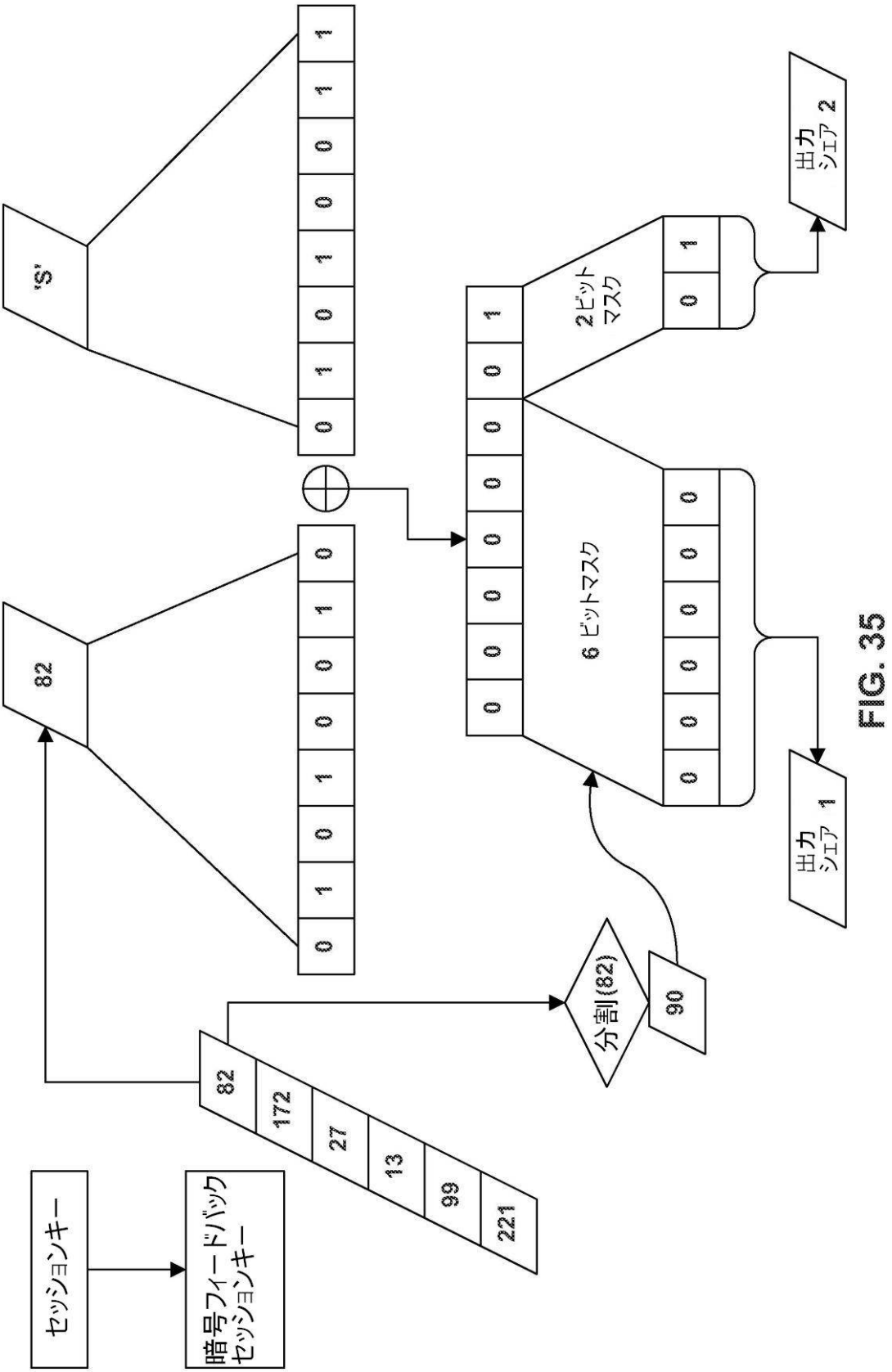
セッションキー
暗号フィードバック
セッションキー
82
172
27
13
99
221
分割(82)
90
'S'
0 1 0 1 0 0 1 0
0 1 0 1 0 1 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
6 ビットマスク
2ビット
マスク
0 1
0 1
出力
シェア 1
出力
シェア 2

FIG. 35

【図３６】

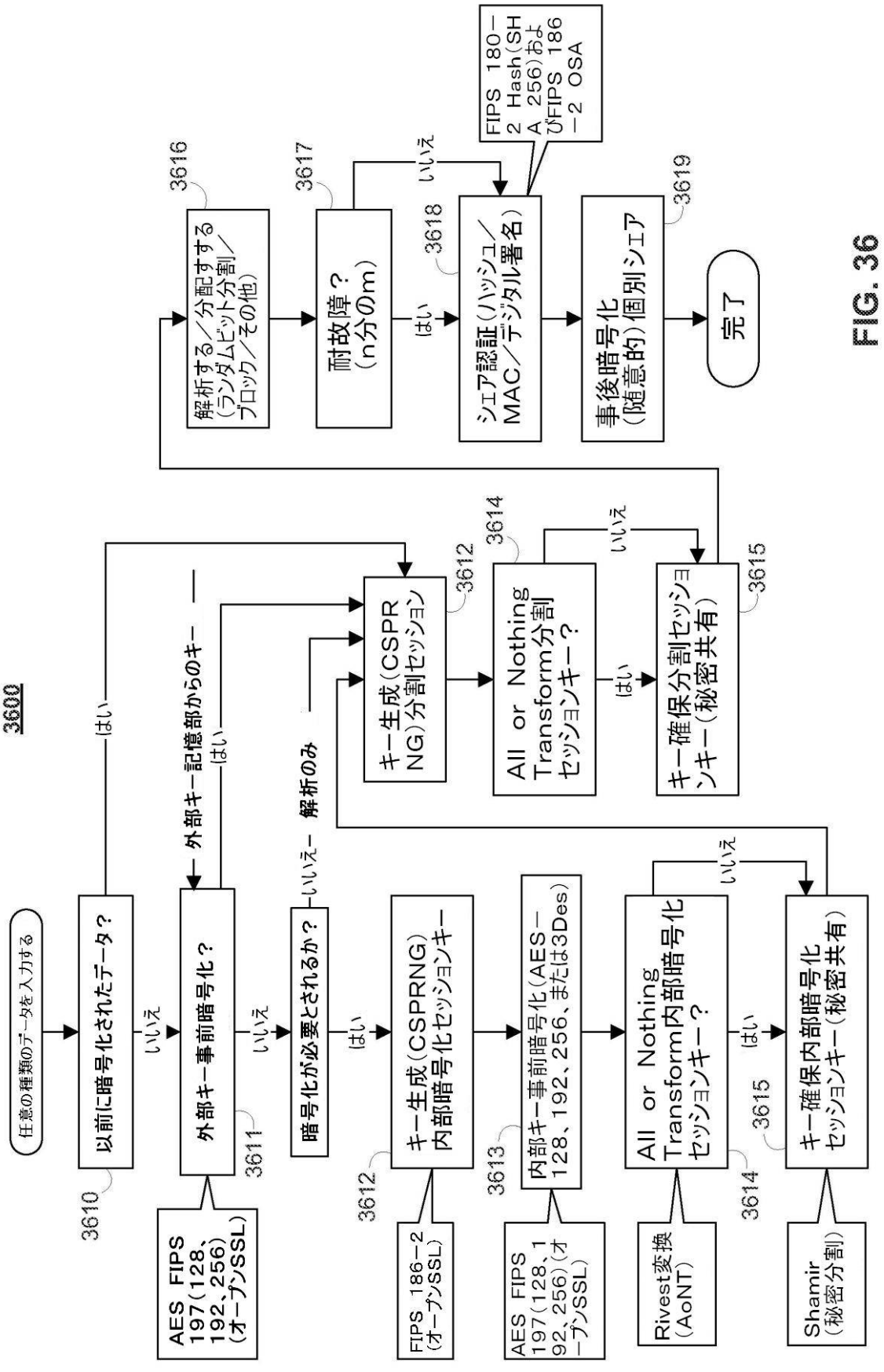
3600
任意の種類のデータを入力する
以前に暗号化されたデータ？
3610
はい
いいえ
外部キー事前暗号化？
3611
AES FIPS 197(128、192、256)(オープンSSL)
外部キー記憶部からのキー
はい
いいえ
暗号化が必要とされるか？
いいえ－解析のみ
はい
キー生成(CSPRNG)内部暗号化セッションキー
3612
FIPS 186－2(オープンSSL)
内部キー事前暗号化(AES－128、192、256、または3Des)
3613
AES FIPS 197(128、192、256)(オープンSSL)
All or Nothing Transform内部暗号化セッションキー？
3614
Rivest変換(AoNT)
キー確保内部暗号化セッションキー(秘密共有)
3615
Shamir(秘密分割)
キー生成(CSPRNG)分割セッション
3612
All or Nothing Transform分割セッションキー？
3614
キー確保分割セッションキー(秘密共有)
3615
解析する／分配する(ランダムビット分割／ブロック／その他)
3616
耐故障？(n分のm)
3617
はい
いいえ
3618
FIPS 180－2 Hash(SHA 256)およびFIPS 186－2 OSA
シェア認証(ハッシュ／MAC／デジタル署名)
事後暗号化(随意的)個別シェア
3619
完了

FIG. 36

【図３７】

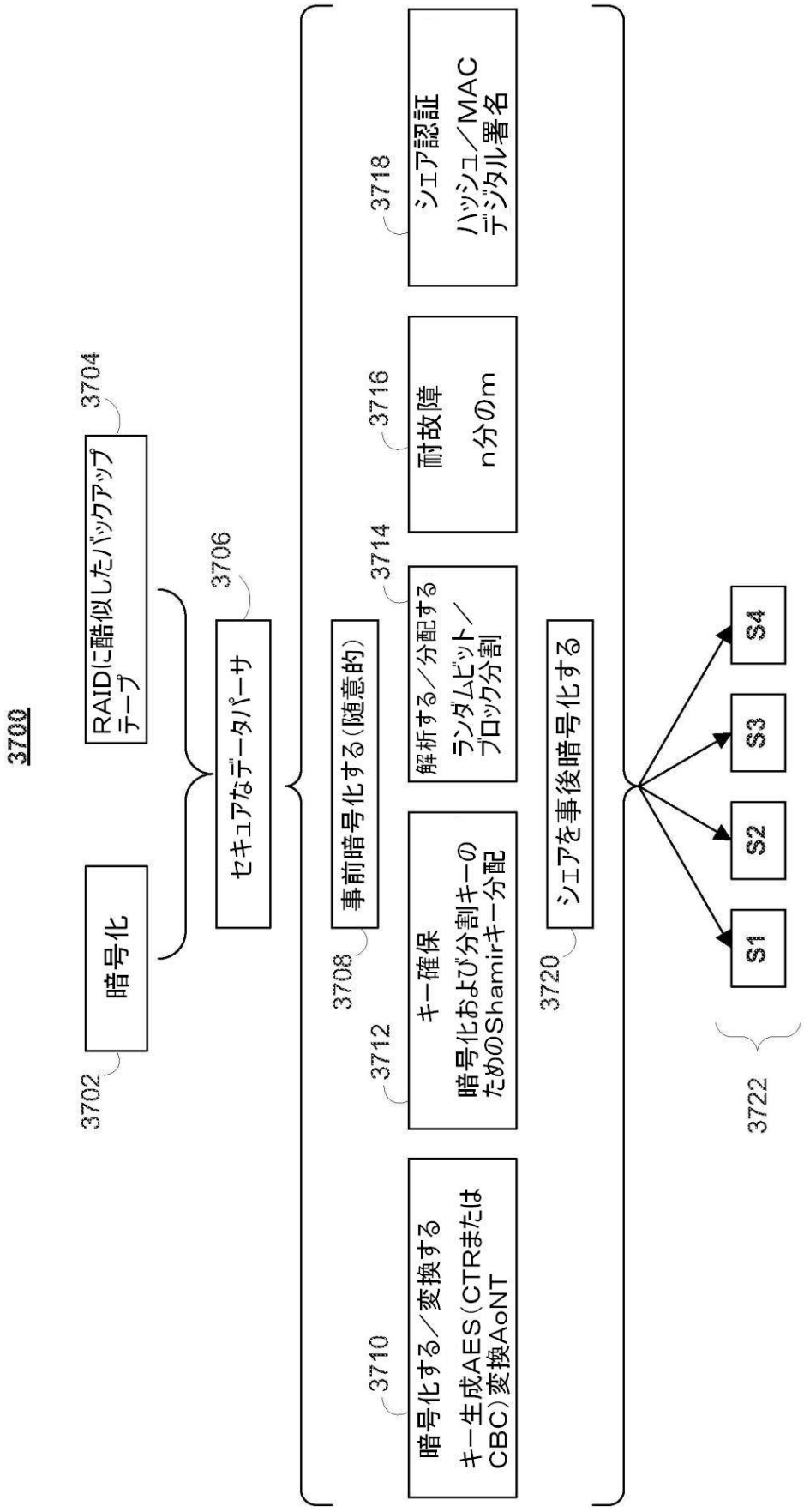
3700
暗号化
3702
RAIDに酷似したバックアップテープ
3704
セキュアなデータパーサ
3706
事前暗号化する（随意的）
3708
キー確保
暗号化および分割キーのためのShamirキー分配
3712
暗号化する／変換するキー生成AES（CTRまたはCBC）変換AoNT
3710
解析する／分配するランダムビット／ブロック分割
3714
耐故障
n分のm
3716
シェア認証
ハッシュ／MACデジタル署名
3718
シェアを事後暗号化する
3720
S1
S2
S3
S4
3722

FIG. 37

【図３８】

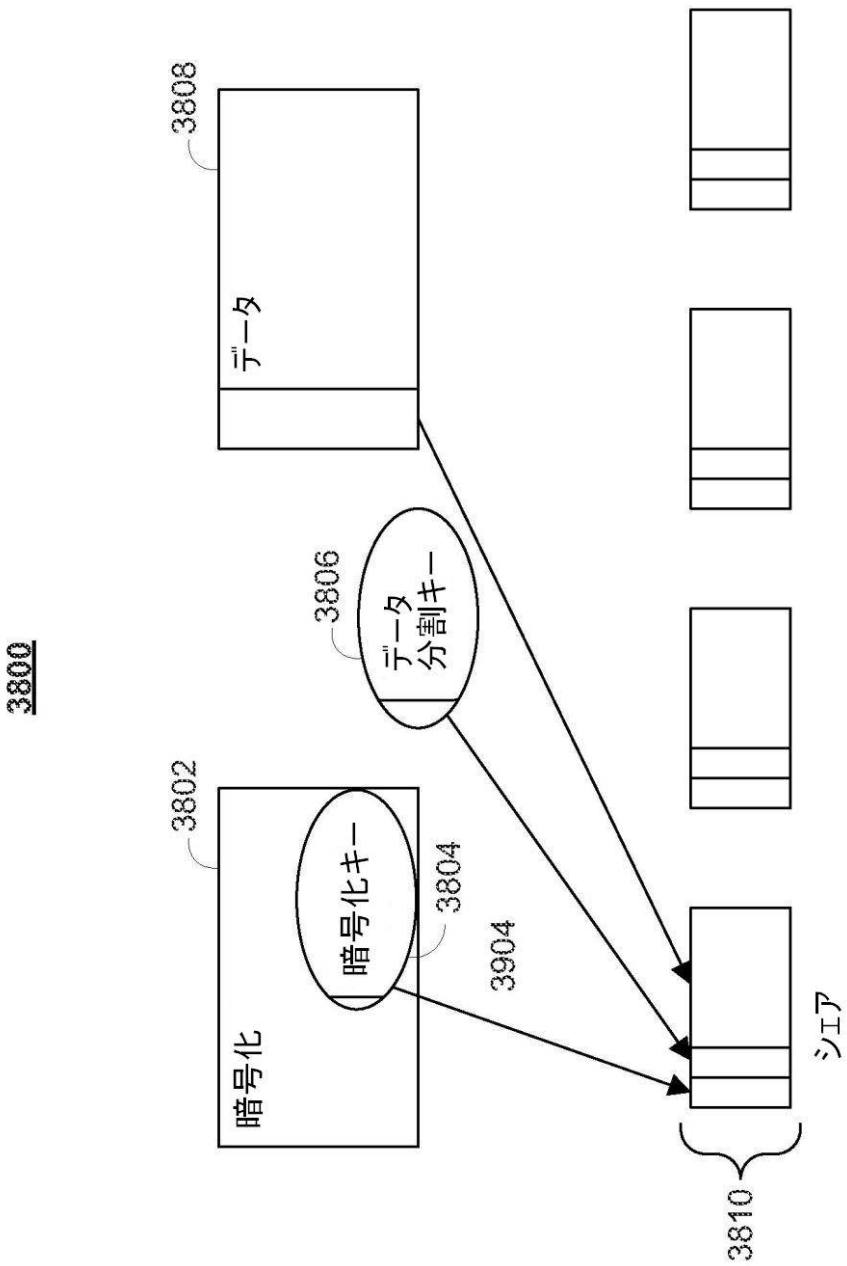

FIG. 38

【図３９】

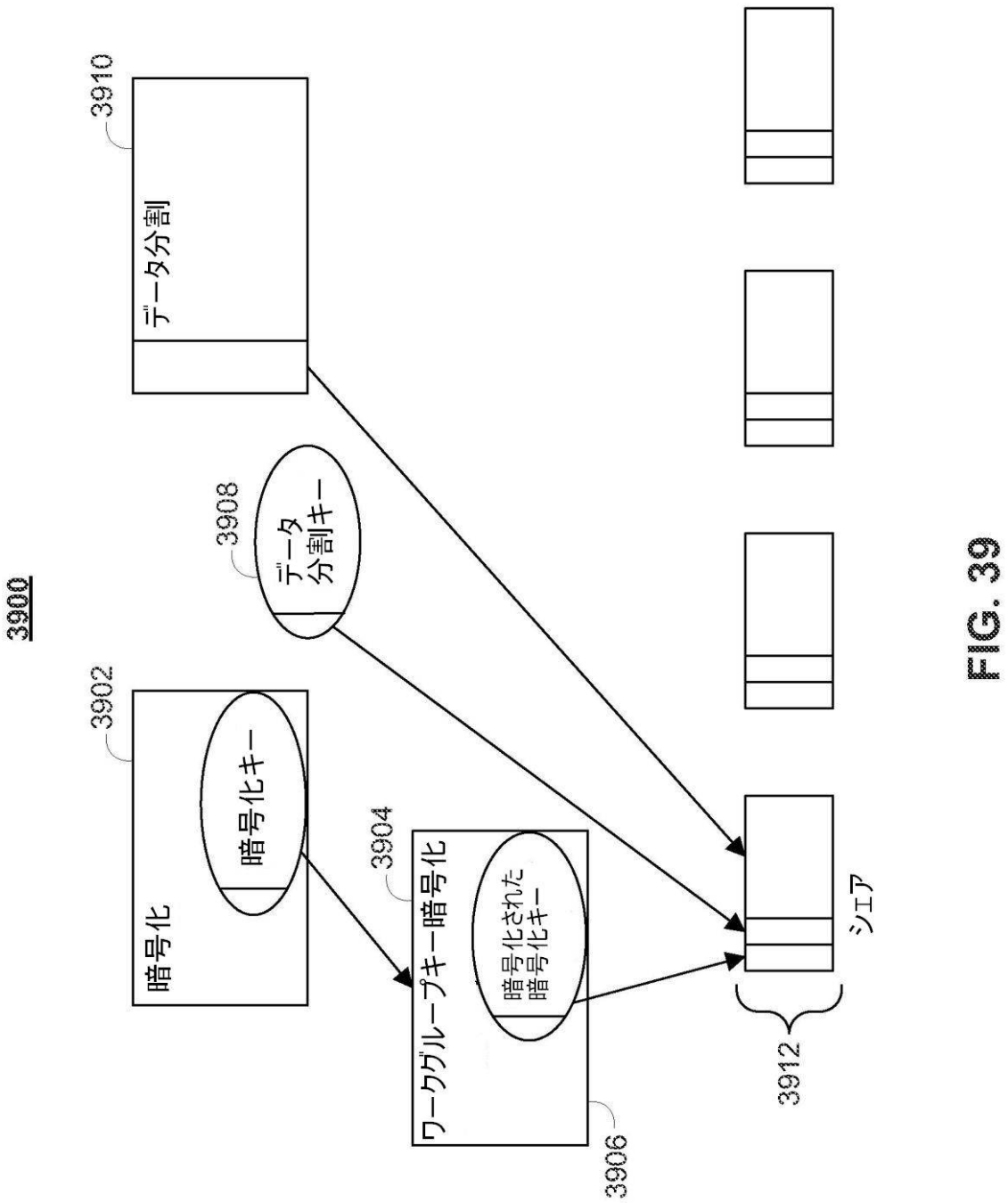
3900
3910
データ分割
3908
データ
分割キー
3902
暗号化
暗号化キー
3904
ワークグループキー暗号化
暗号化された
暗号化キー
3906
3912
シェア

FIG. 39

【図４０】

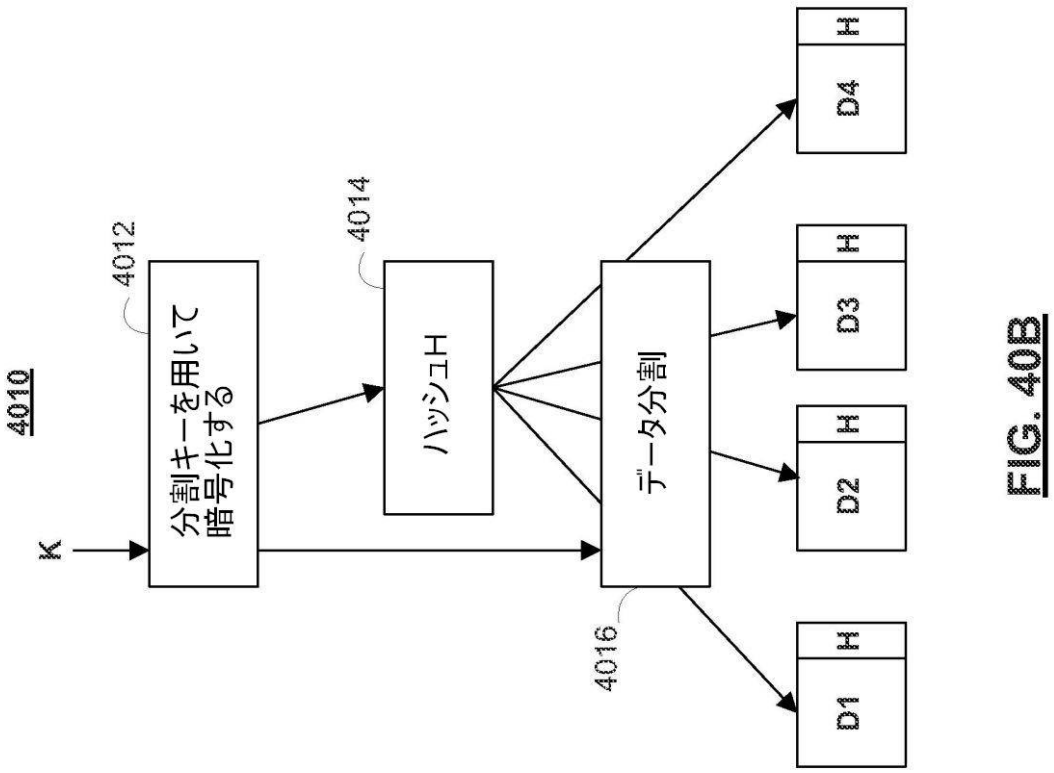

FIG. 40B

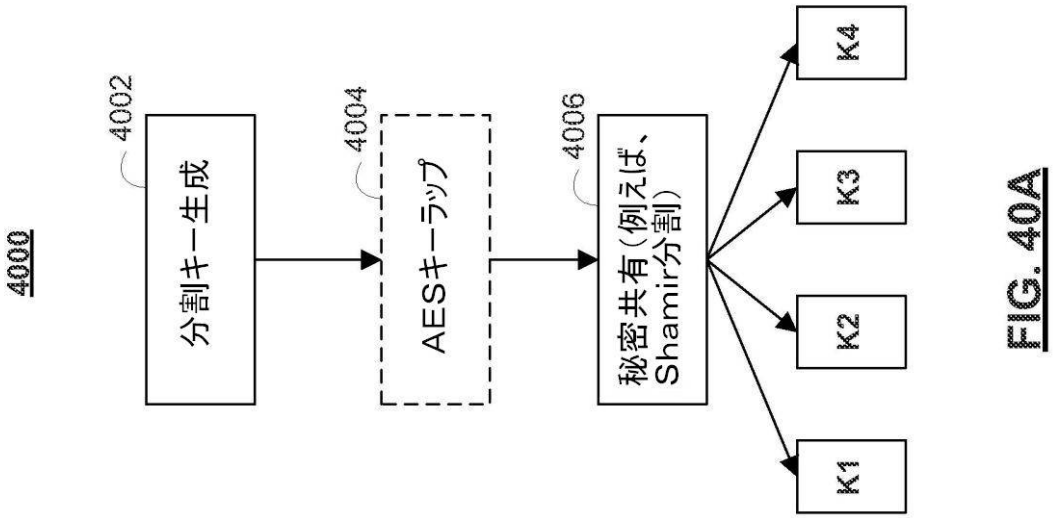

FIG. 40A

【図４１】

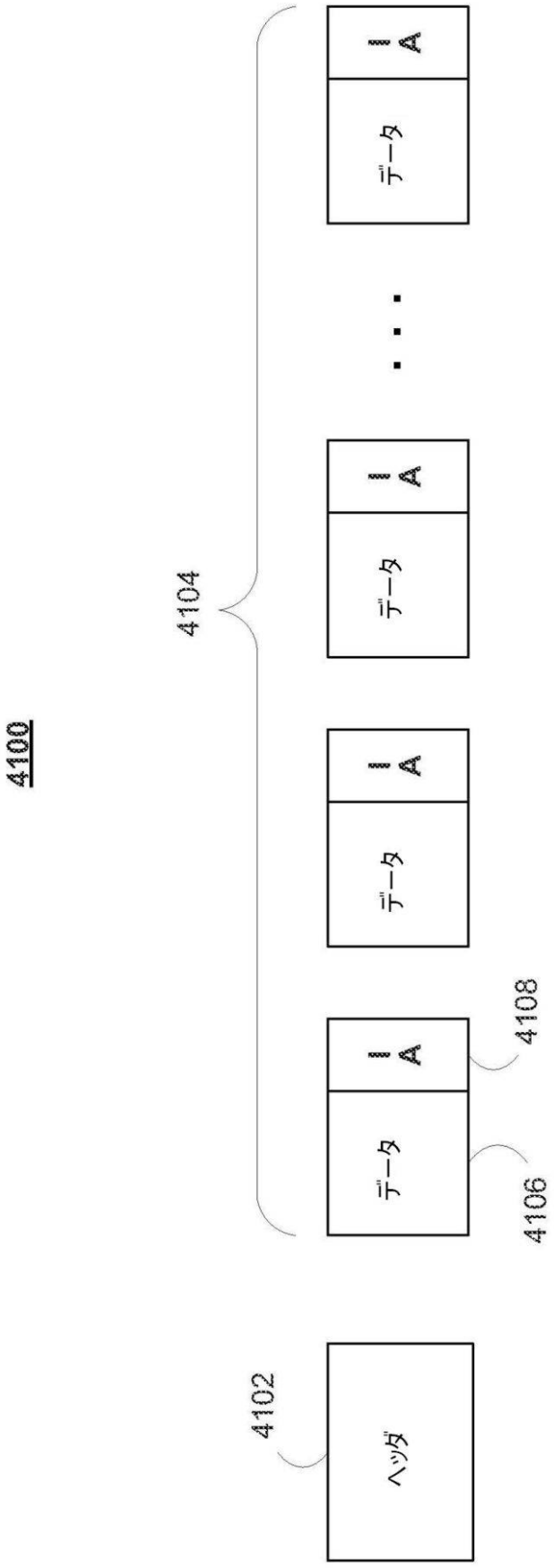

FIG. 41

【図４２】

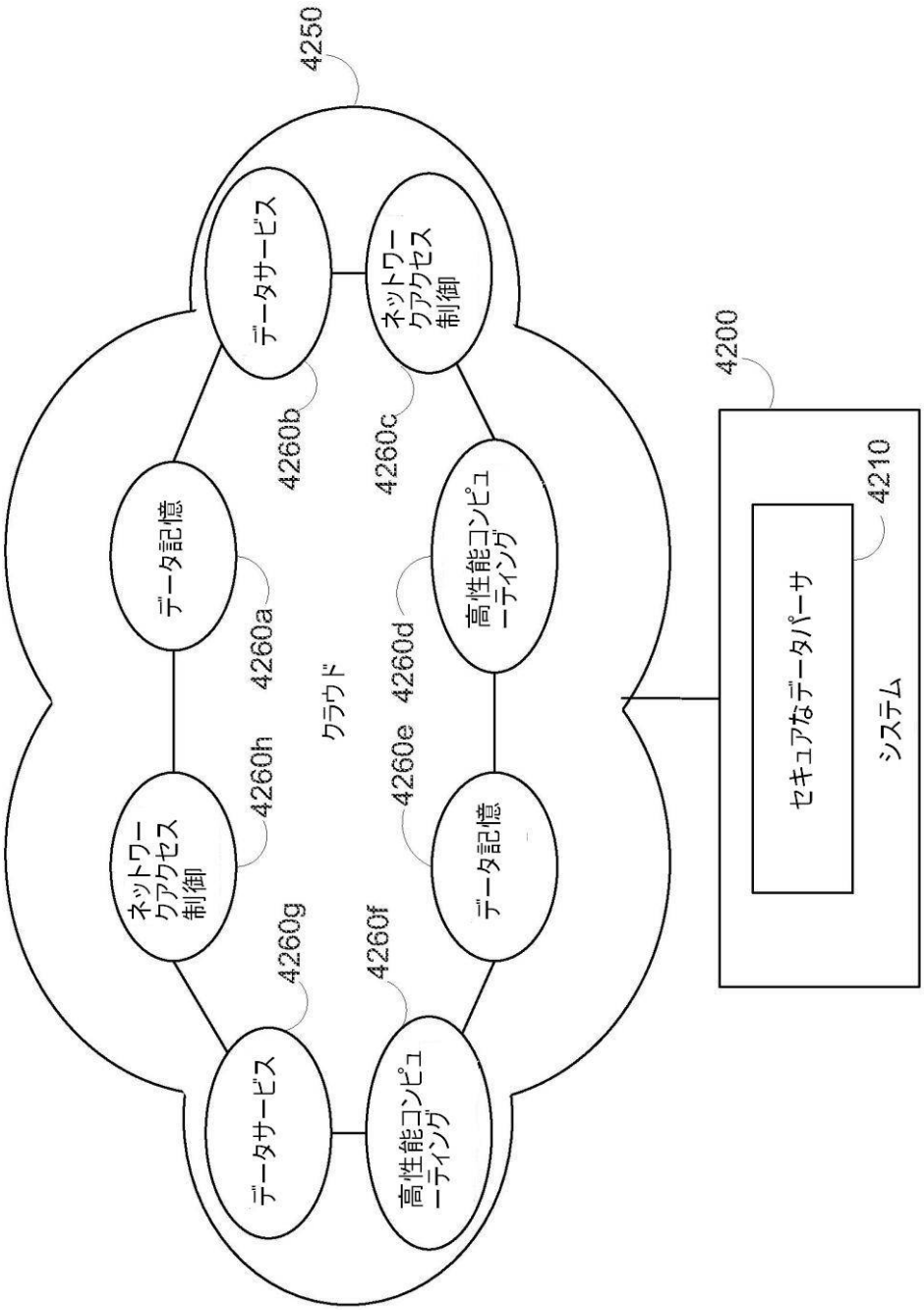
4250
データサービス
ネットワークアクセス制御
4260b
4260c
データ記憶
高性能コンピューティング
4260a
4260d
クラウド
4260h
4260e
ネットワークアクセス制御
データ記憶
4260g
4260f
データサービス
高性能コンピューティング
4200
セキュアなデータパーサ
4210
システム

FIG. 42

【図４３】

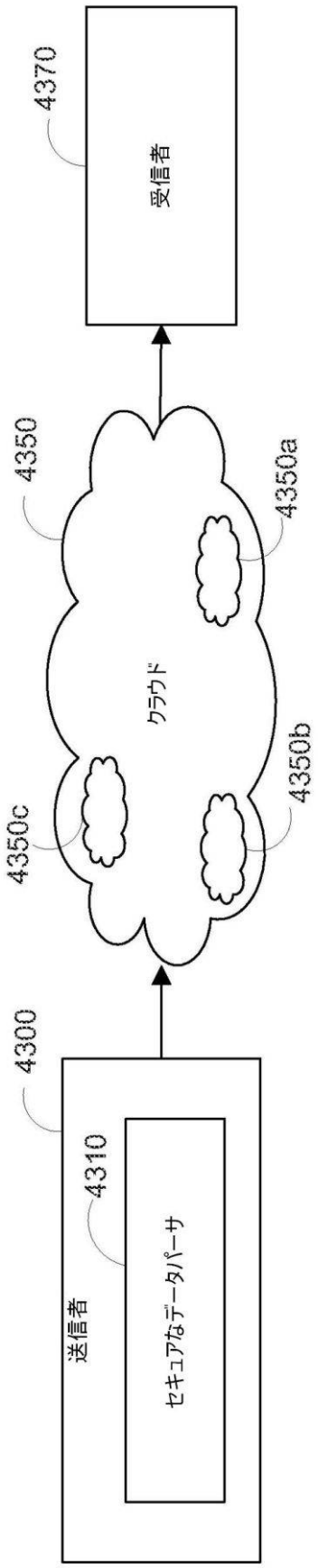
4370
受信者
4350
4350a
クラウド
4350b
4350c
4300
4310
送信者
セキュアなデータパーサ

FIG. 43

【図４４】

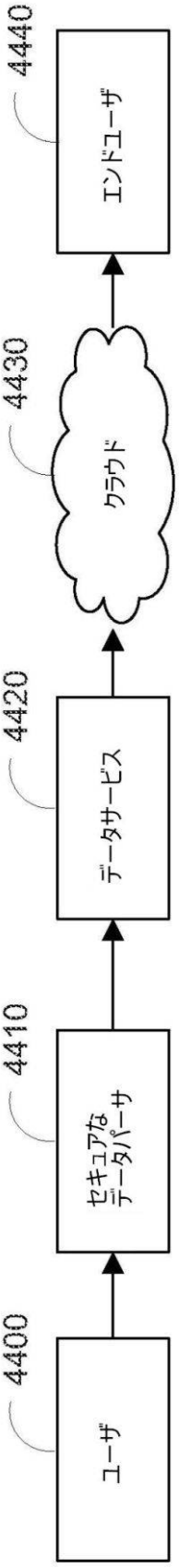
4400
ユーザ
4410
セキュアな
データパーサ
4420
データサービス
4430
クラウド
4440
エンドユーザ

FIG. 44

【図４５】

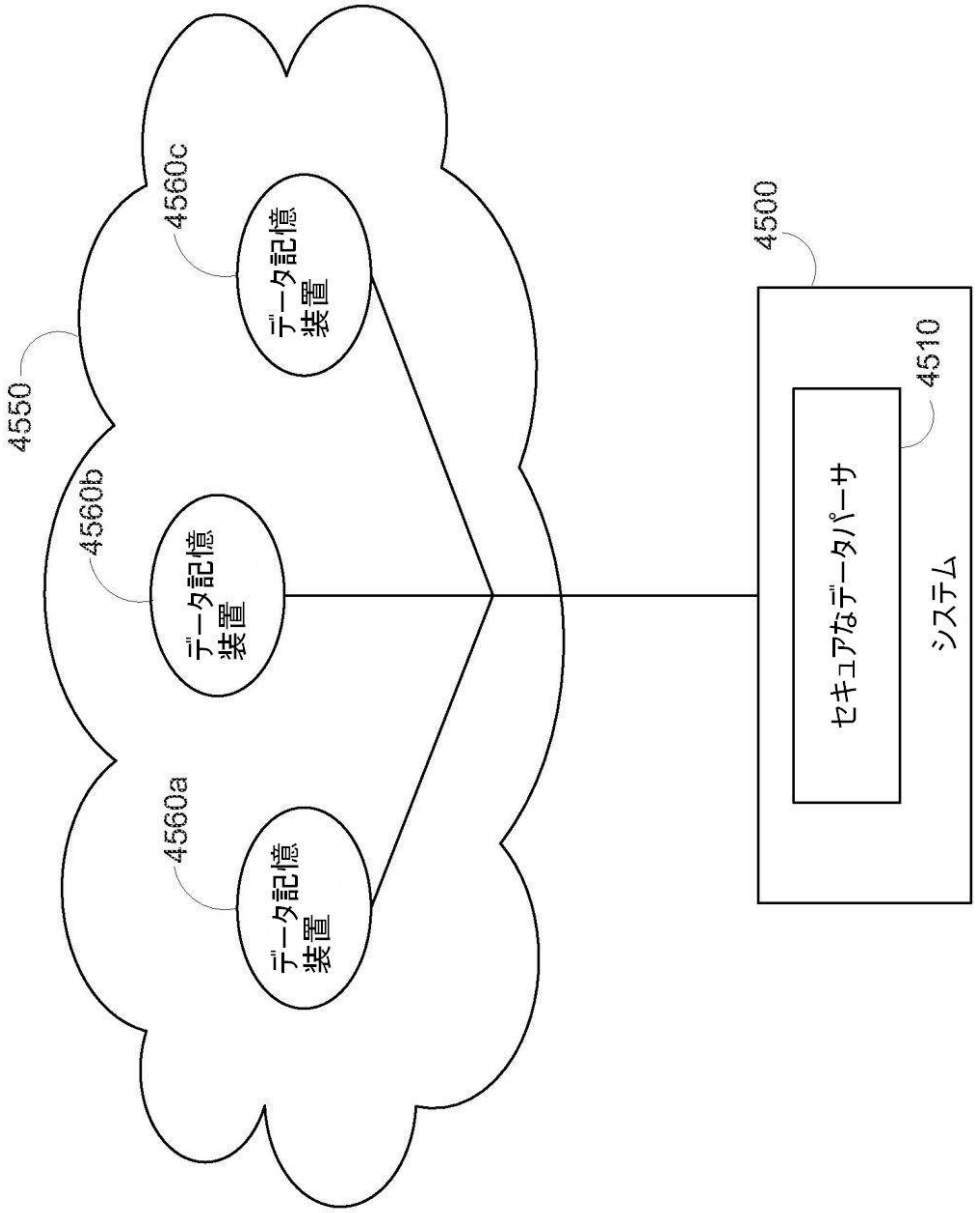
4550
4560c
データ記憶装置
4560b
データ記憶装置
4560a
データ記憶装置
4500
4510
セキュアなデータパーサ
システム

FIG. 45

【図４６】

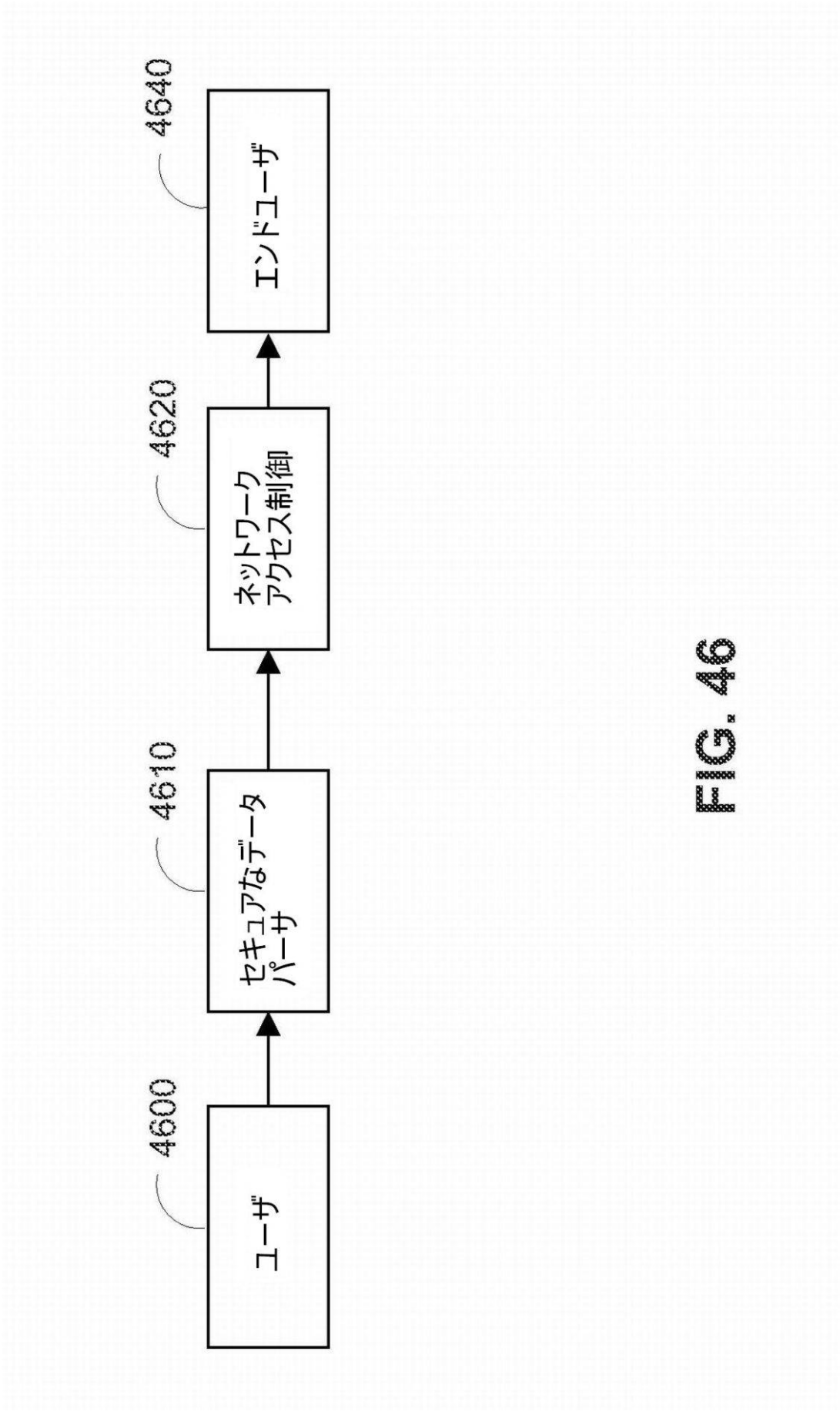

FIG. 46

【図４７】

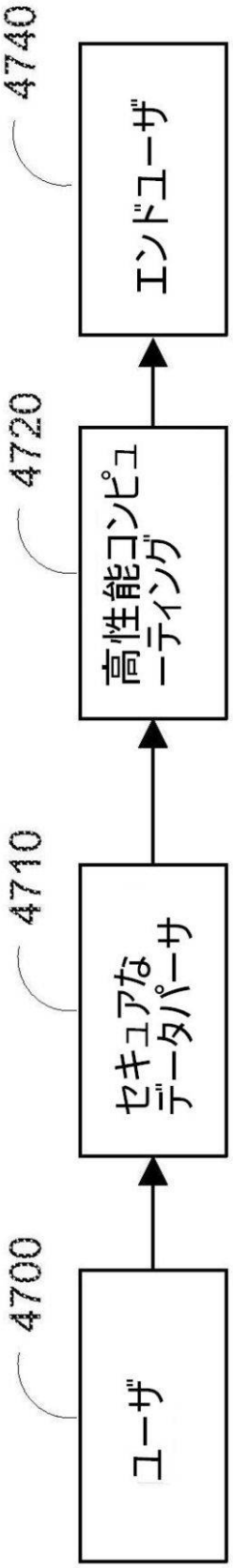

FIG. 47

【図４８】

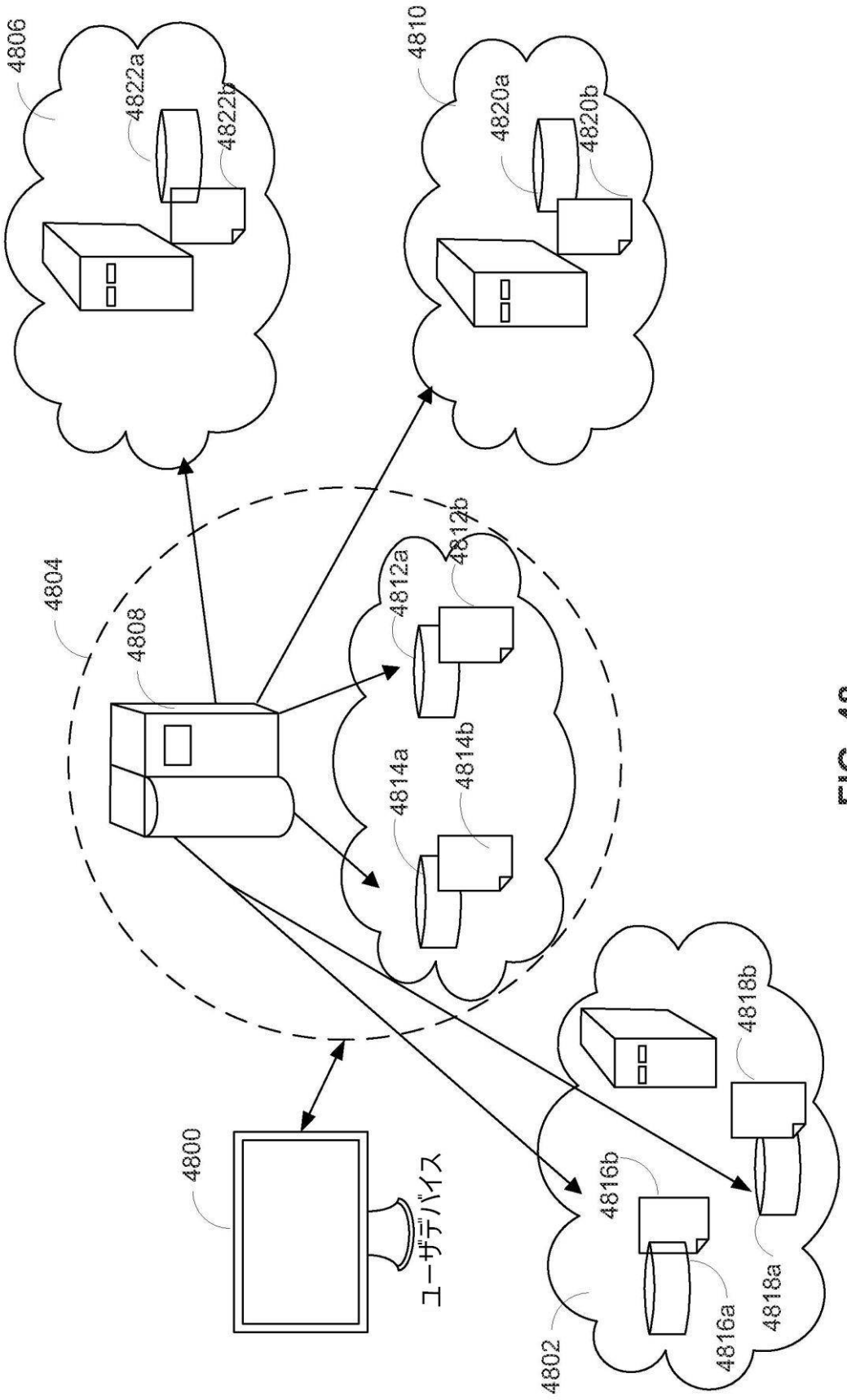
4806
4822a
4822b
4810
4820a
4820b
4804
4808
4812b
4812a
4814a
4814b
4800
ユーザデバイス
4816b
4816a
4818b
4818a
4802

FIG. 48

【図４９】

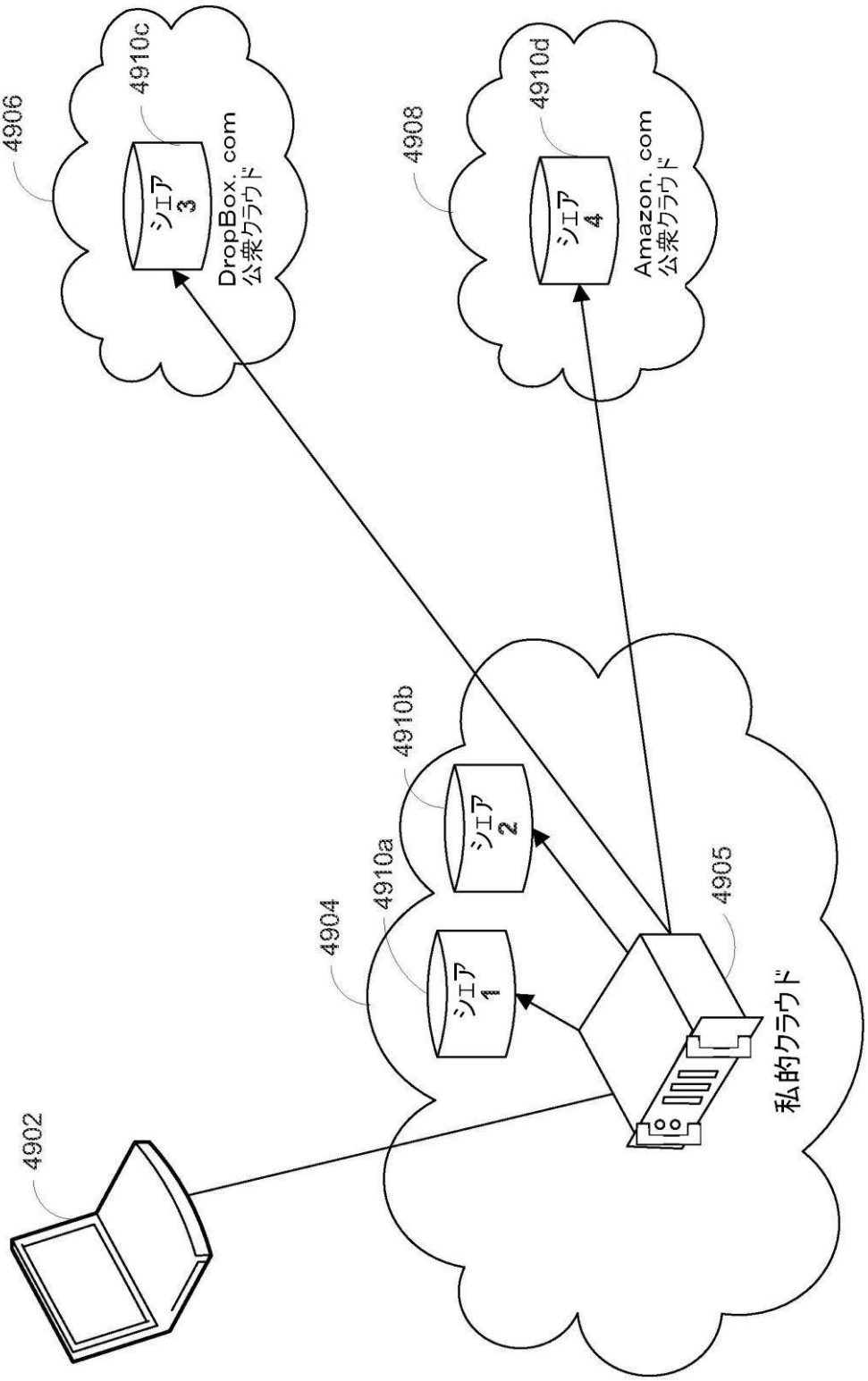
4906
4910c
シェア 3
DropBox. com 公衆クラウド
4908
4910d
シェア 4
Amazon. com 公衆クラウド
4910b
シェア 2
4910a
4904
シェア 1
4905
私的クラウド
4902

FIG. 49

【図５０】

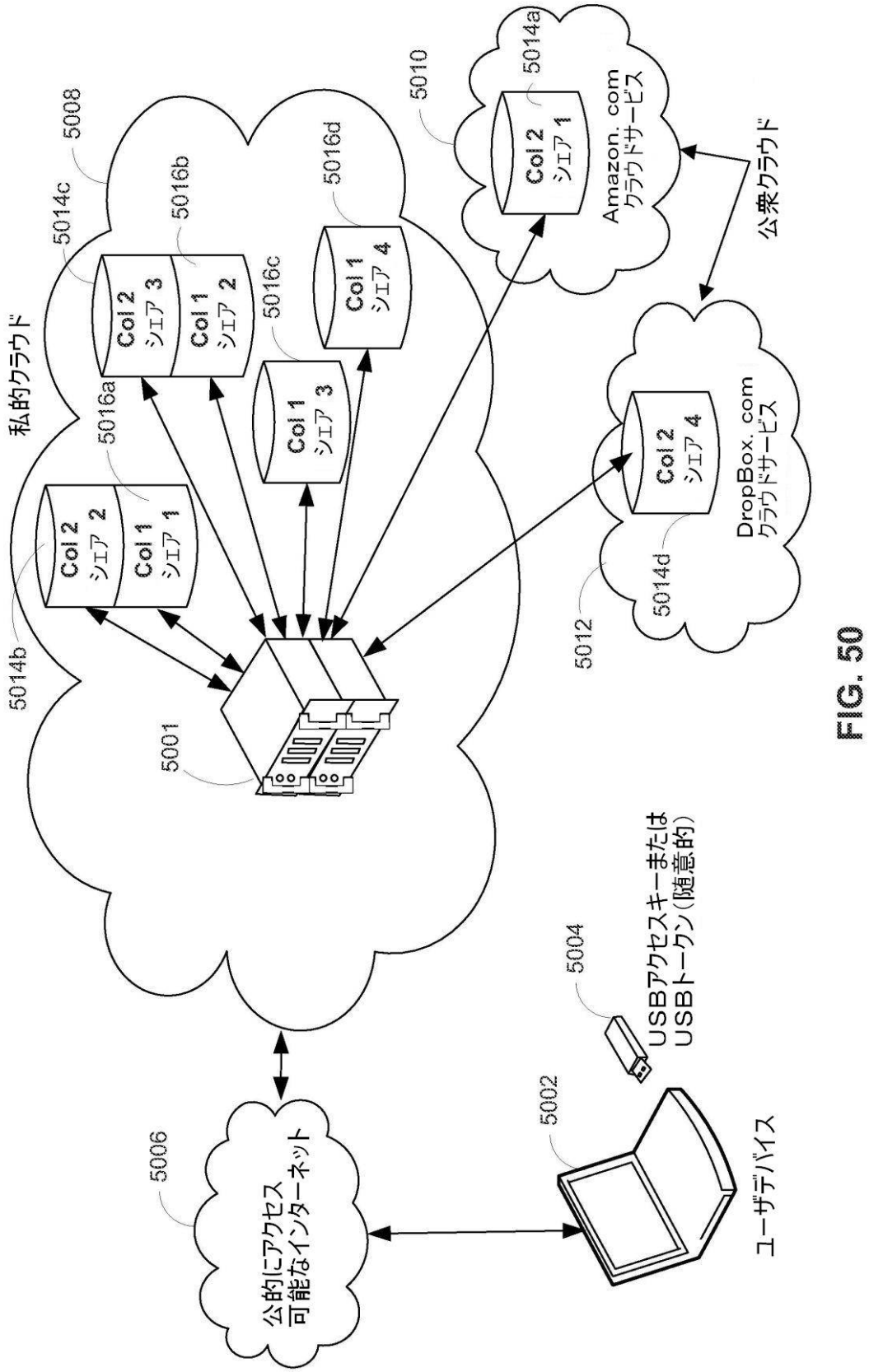
私的クラウド
5008
5014c
5016b
5016d
5010
5014a
Col 2 シェア 3
Col 1 シェア 2
Col 1 シェア 4
Col 2 シェア 1
Amazon.com クラウドサービス
公衆クラウド
5016a
5016c
Col 1 シェア 3
Col 2 シェア 2
Col 1 シェア 1
Col 2 シェア 4
DropBox.com クラウドサービス
5014b
5001
5012
5014d
5004
USBアクセスキーまたは USBトークン（随意的）
5006
公的にアクセス 可能なインターネット
5002
ユーザデバイス

FIG. 50

【図５１】

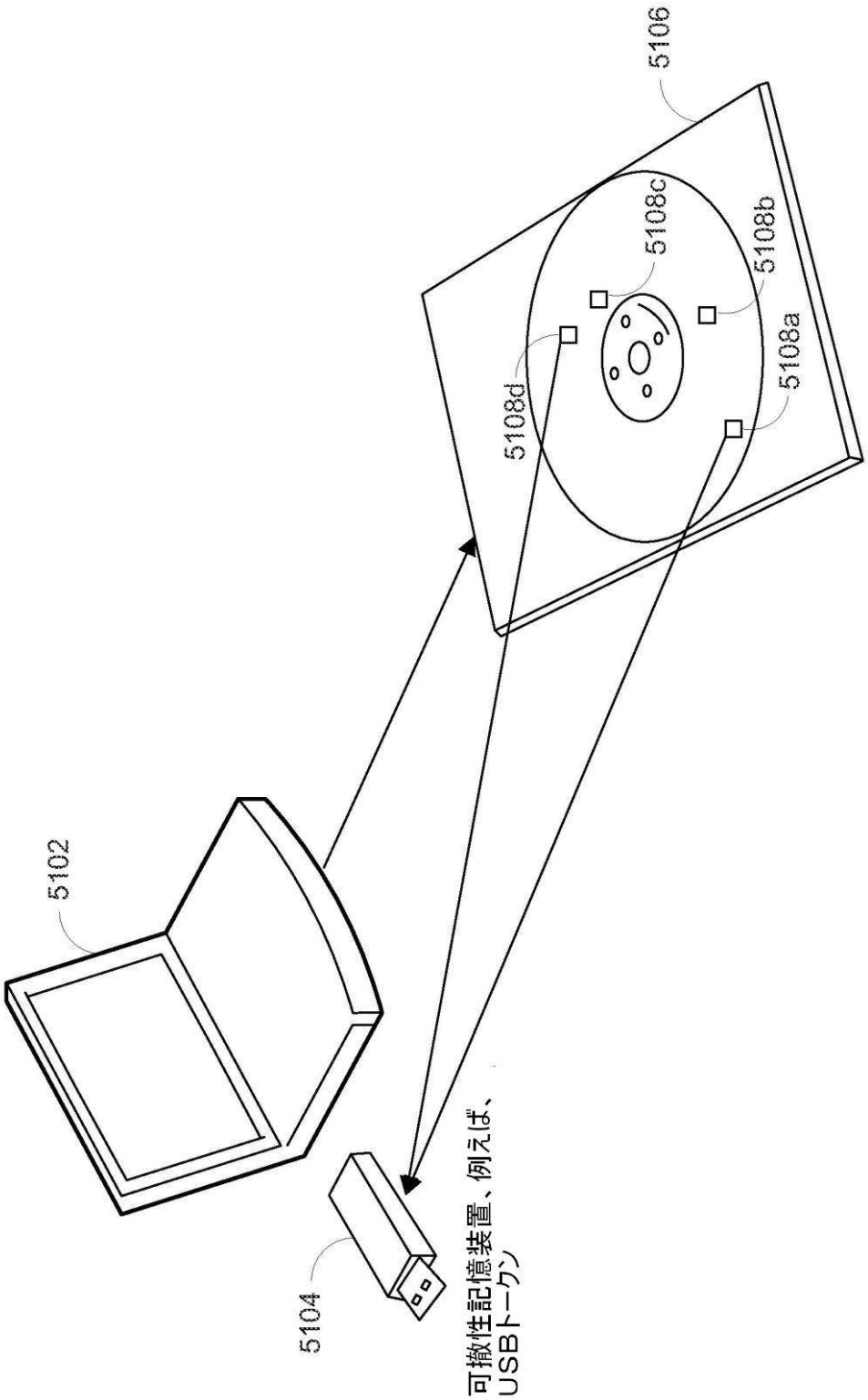

FIG. 51

【図５２】

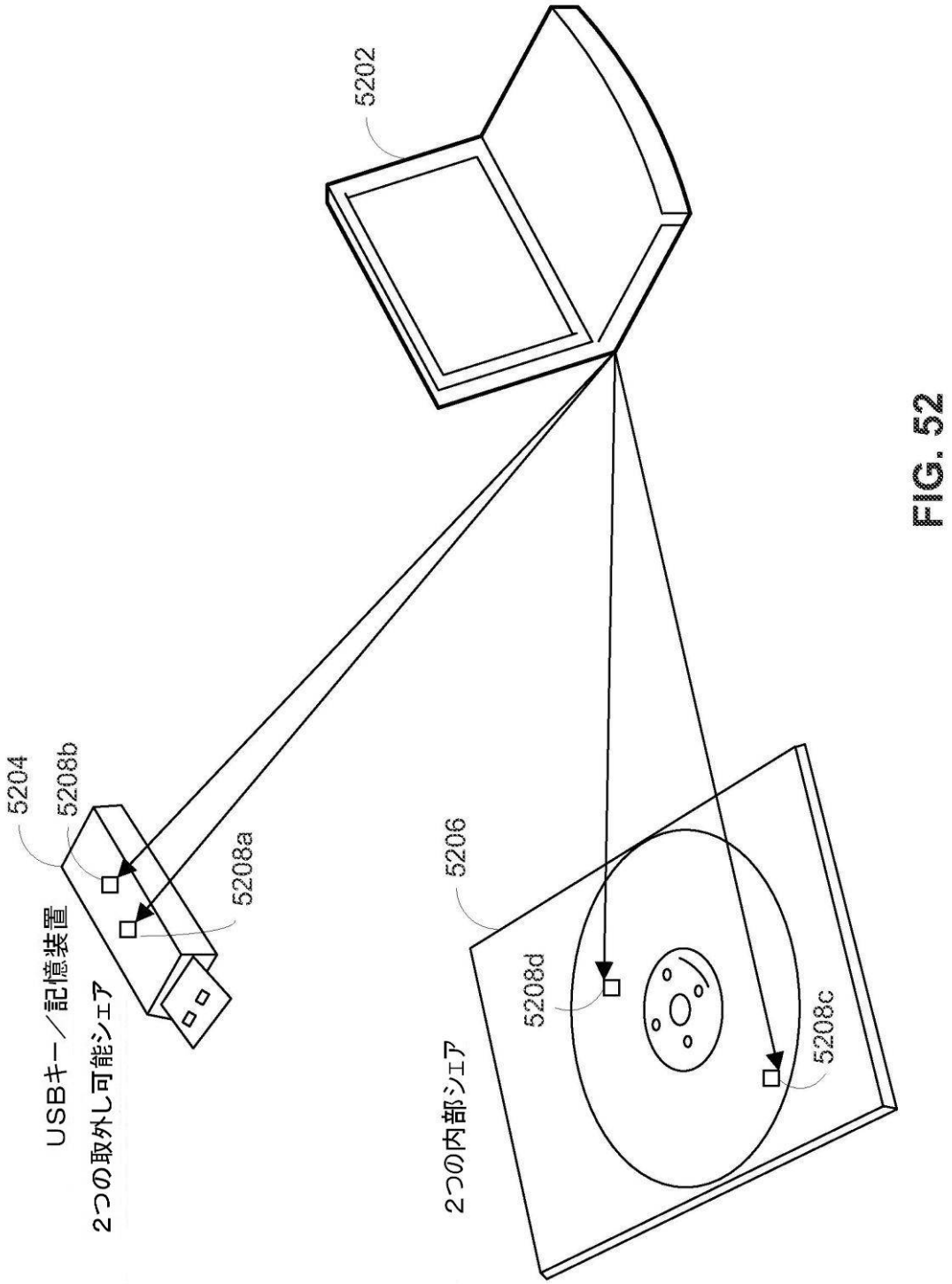
5202
5204
5208b
5208a
USBキー／記憶装置
2つの取外し可能シェア
5206
5208d
5208c
2つの内部シェア

FIG. 52

【図５４】

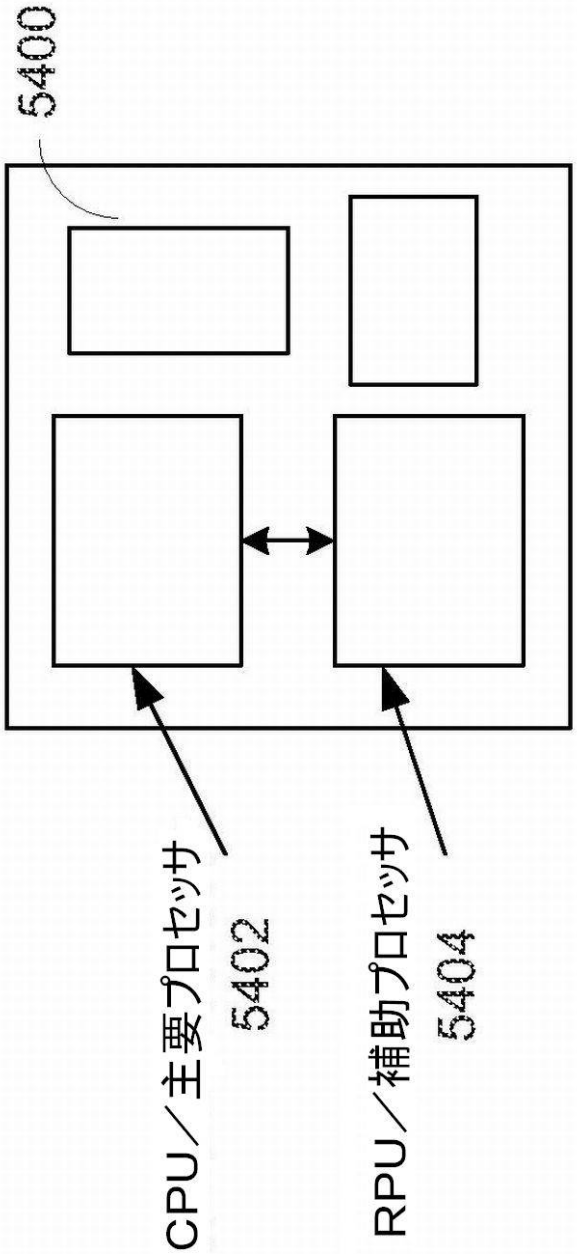

FIG. 54

【図５５】

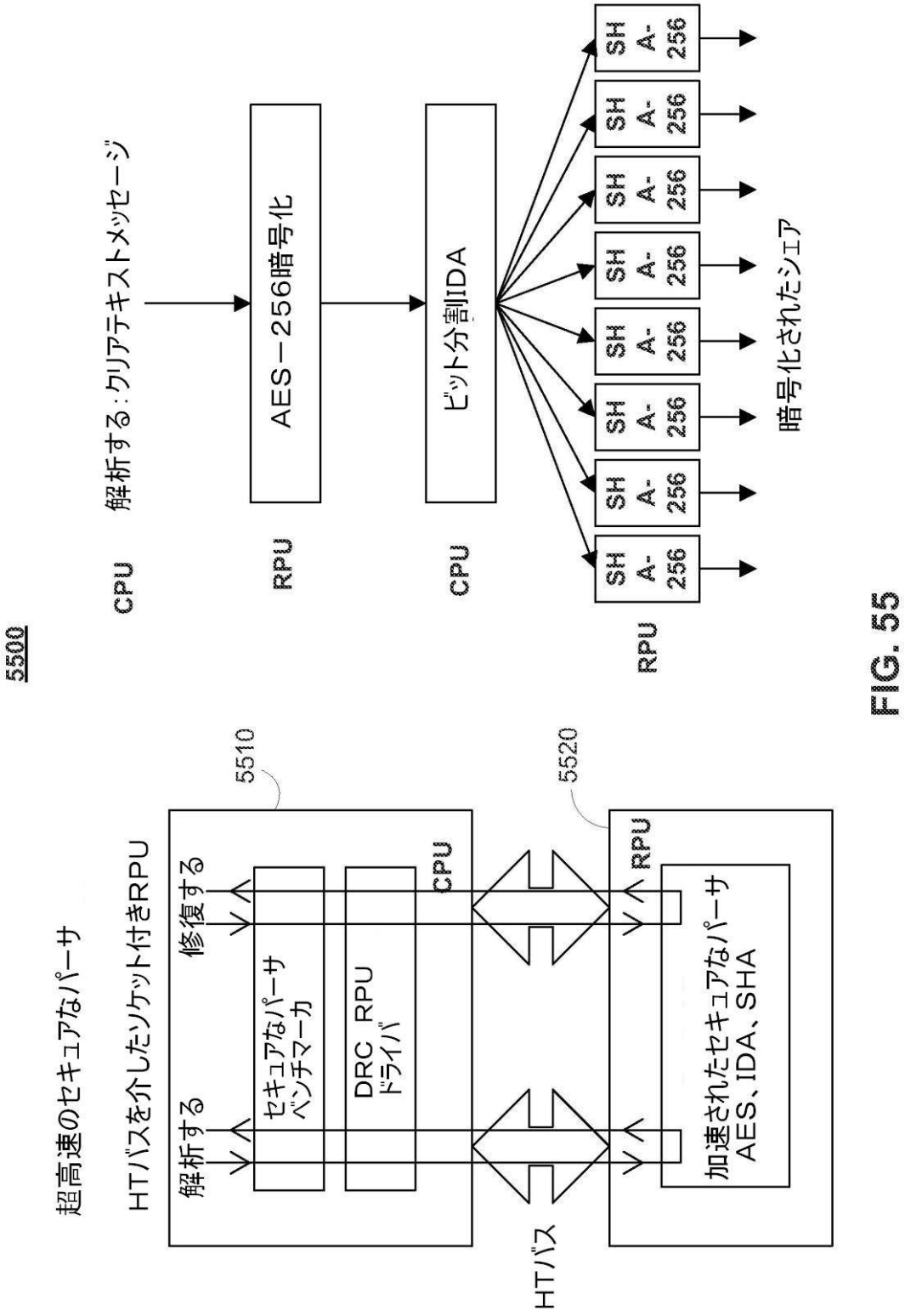
5500
超高速のセキュアなパーサ
HTバスを介したソケット付きRPU
解析する
修復する
セキュアなパーサ
ベンチマーカ
DRC RPU
ドライバ
CPU
5510
RPU
加速されたセキュアなパーサ
AES、IDA、SHA
5520
HTバス
CPU
解析する：クリアテキストメッセージ
AES－256暗号化
RPU
ビット分割IDA
CPU
SHA-256
SHA-256
SHA-256
SHA-256
SHA-256
SHA-256
SHA-256
RPU
暗号化されたシェア

FIG. 55

【図５６】

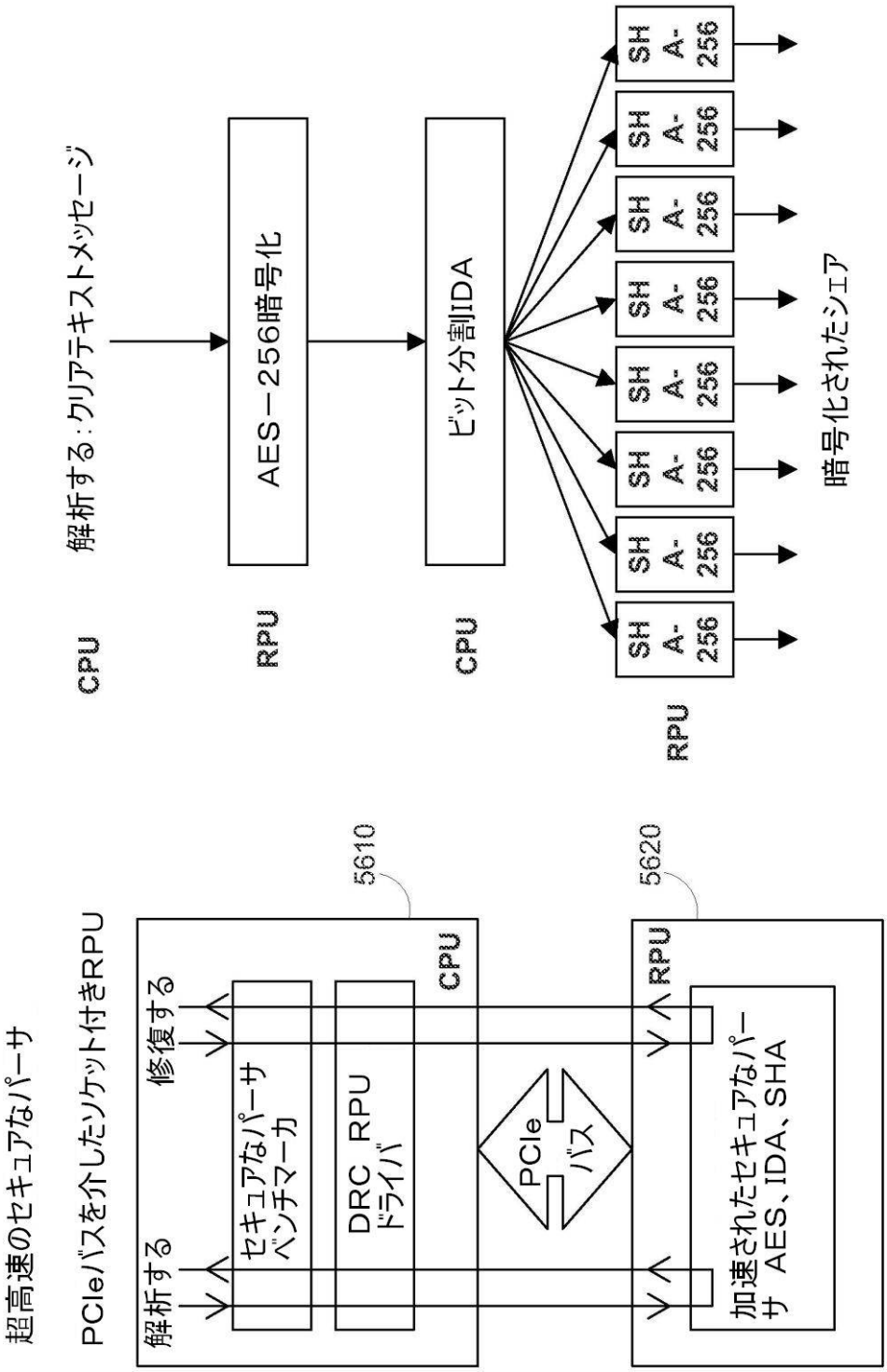
5600
超高速のセキュアなパーサ
PCIeバスを介したソケット付きRPU
解析する
修復する
セキュアなパーサ
ベンチマーカ
DRC RPU
ドライバ
CPU
5610
PCIe
バス
RPU
加速されたセキュアなパーサ AES、IDA、SHA
5620
CPU
解析する：クリアテキストメッセージ
AES－256暗号化
RPU
ビット分割IDA
CPU
SHA-256
暗号化されたシェア
RPU

FIG. 56

【図５７】

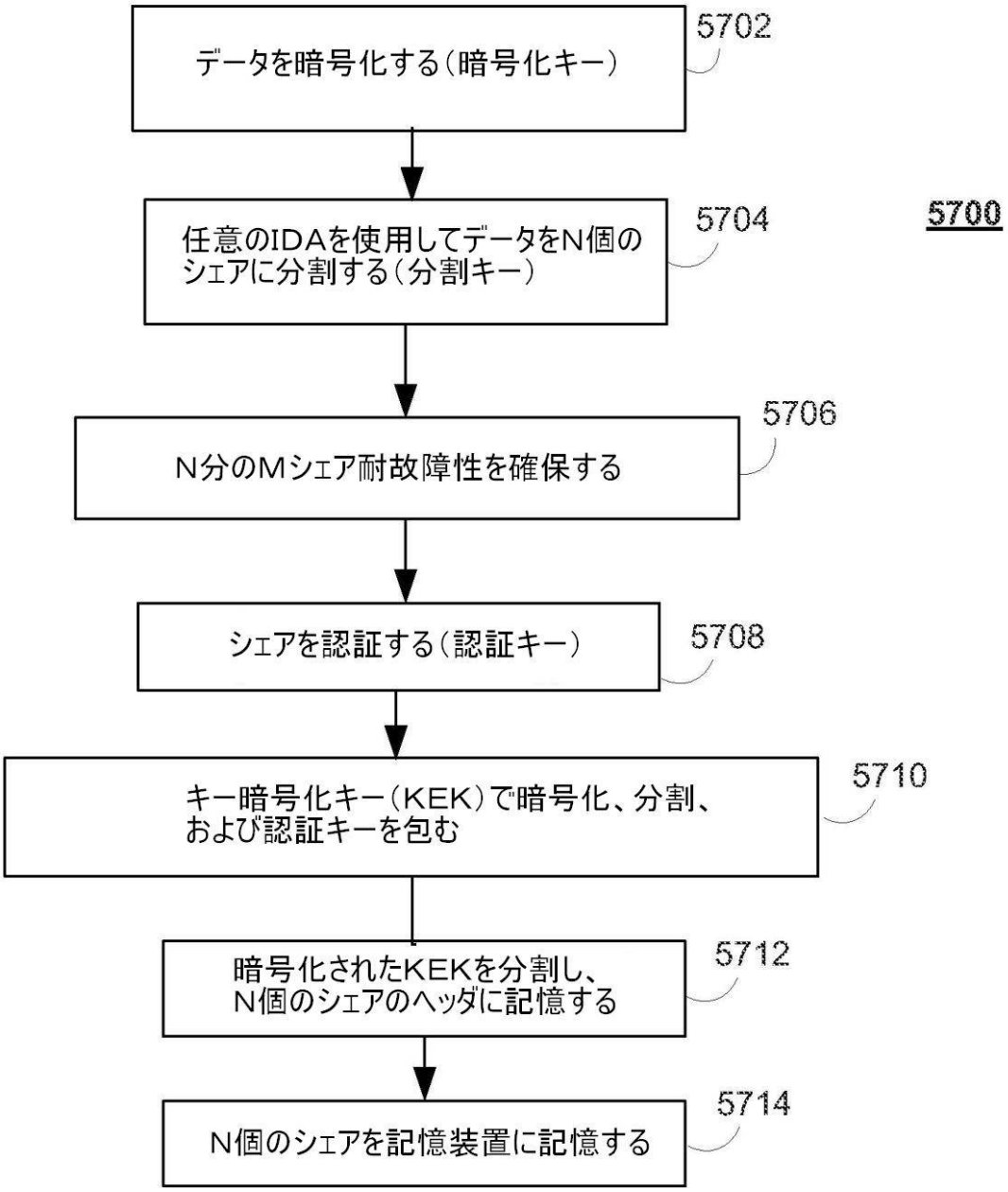
データを暗号化する（暗号化キー）
5702
任意のIDAを使用してデータをN個のシェアに分割する（分割キー）
5704
5700
N分のMシェア耐故障性を確保する
5706
シェアを認証する（認証キー）
5708
キー暗号化キー（KEK）で暗号化、分割、および認証キーを包む
5710
暗号化されたKEKを分割し、N個のシェアのヘッダに記憶する
5712
N個のシェアを記憶装置に記憶する
5714

FIG. 57

【図５８】

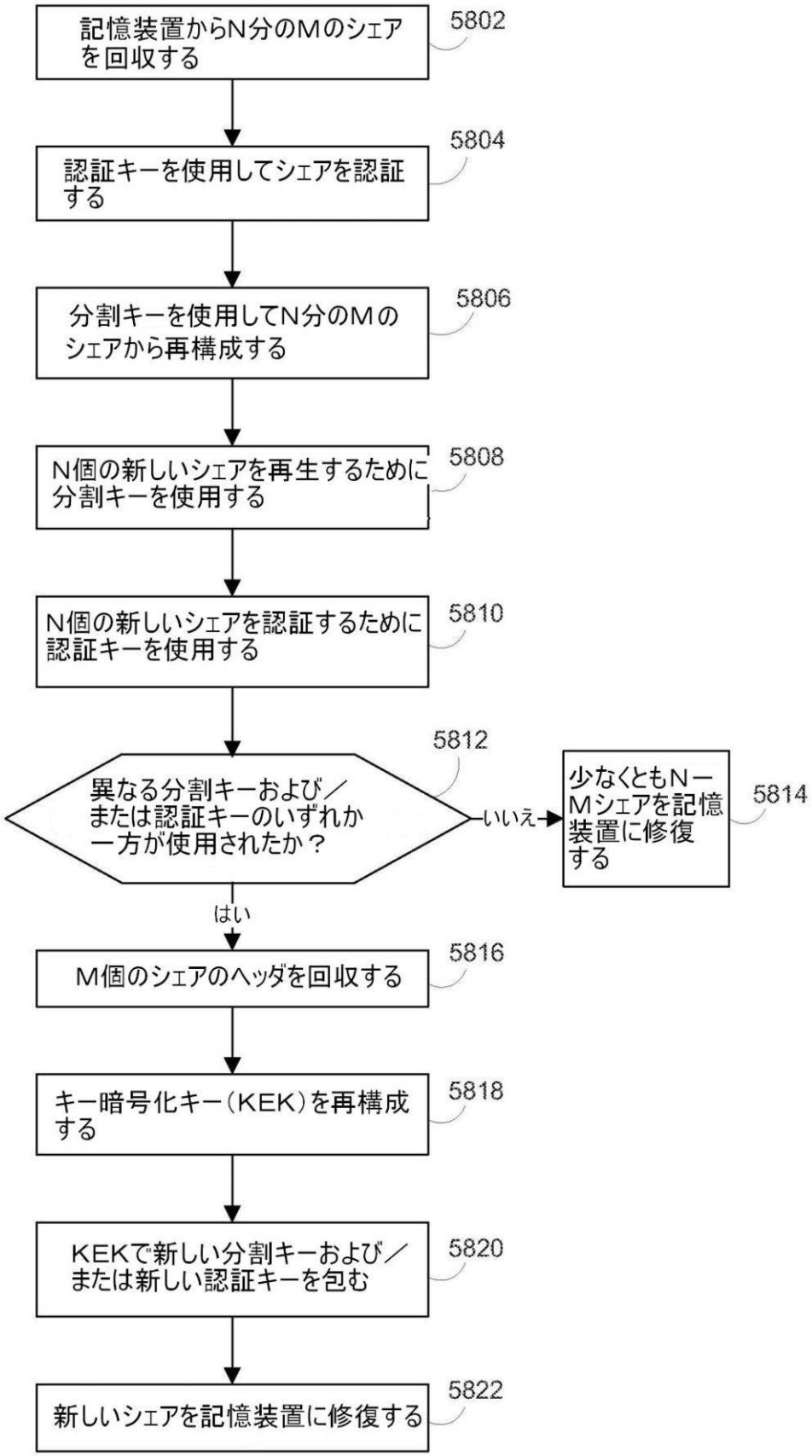

FIG. 58

【手続補正書】

【提出日】平成24年11月29日(2012.11.29)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
一組のデータシェアを再構築するための方法であって、該一組のデータシェアは、第１の分割キーを使用して、情報分散アルゴリズムによって暗号化データセットから生成されたものであり、
該方法は、
該一組のデータシェアを再構築するために必要な少なくとも最小数のデータシェアを受信することと、
該最小数のデータシェアを復号することなしに、該最小数のデータシェアから該一組のデータシェアを再構築することと
を含む、方法。
【請求項２】
前記再構築することは、前記データシェアのうちの１つ以上が既に損なわれているという決定に応じて行われる、請求項１に記載の方法。
【請求項３】
前記再構築することは、
認証キーによって前記最小数のデータシェアを認証することと、
前記分割キーを使用して、該認証された最小数のデータシェアから前記暗号化データを再構成することと、
該分割キーを使用して該暗号化データを分割することによって、前記一組のデータシェアを再生することと
を含む、請求項１に記載の方法。
【請求項４】
一組のデータシェアのキーを再生成するための方法であって、該一組のデータシェアは、第１の暗号化キーを使用して、情報分散アルゴリズムによって暗号化データセットから生成されたものであり、
該方法は、
該一組のデータシェアを再構築するために必要な少なくとも最小数のデータシェアを受信することと、
該最小数のデータシェアを第１の認証キーと関連付けることと、
該最小数のデータシェアを復号することなしに、該最小数のデータシェアから該一組のデータシェアを再構築することと、
該再構築された一組のデータシェアを第２の暗号化キーと関連付けることによって、該再構築された一組のデータシェアのキーを再生成することと
を含む、方法。
【請求項５】
前記最小数のデータシェアと関連付けられるヘッダを回収することと、
該回収されたヘッダからキー暗号化キーを抽出することと、
該キー暗号化キーによって第２の暗号化キーを暗号化することと、
前記キー再生成されたデータシェアのヘッダ内に暗号化された第２の認証キーを記憶することと
をさらに含む、請求項４に記載の方法。
【請求項６】
一組のデータシェアのキーを再生成するための方法であって、該一組のデータシェアは

、第１の分割キーを使用して、情報分散アルゴリズムによって暗号化データセットから生成されたものであり、
該方法は、
該一組のデータシェアのキーを再生成するために必要な少なくとも最小数のデータシェアを受信することと、
該最小数のデータシェアを復号することなしに、該最小数のデータシェアから該一組のデータシェアを再構築することと、
該再構築された一組のデータシェアを第２の分割キーと関連付けることによって、該再構築された一組のデータシェアのキーを再生成することと
を含む、方法。
【請求項７】
前記最小数のデータシェアと関連付けられるヘッダを回収することと、
該回収されたヘッダからキー暗号化キーを抽出することと、
該キー暗号化キーによって第２の分割キーを暗号化することと、
前記キー再生成されたデータシェアのヘッダ内に該暗号化された第２の分割キーを記憶することと
をさらに含む、請求項６に記載の方法。
【請求項８】
記憶ネットワーク上に前記キー再生成されたデータシェアのうちの少なくとも１つを記憶することをさらに含む、請求項１、４または６に記載の方法。
【請求項９】
スタブを記憶ネットワークのファイルシステム上の一組のデータシェアと関連付けるための方法であって、
該方法は、
情報分散アルゴリズムによって、暗号化データセットから該一組のデータシェアを生成することと、
該生成されたデータシェアと関連付けられる一組のスタブを生成することであって、各スタブは、それぞれのデータシェアに対応し、各スタブは、該それぞれのデータシェアと関連付けられる情報を含む、ことと、
該記憶ネットワーク上の場所に該一組のスタブを記憶することと
を含む、方法。
【請求項１０】
前記情報は、前記それぞれのデータシェアの名前、該それぞれのデータシェアが作成された日付、該それぞれのデータシェアが最後に修正された時間、前記ファイルシステム内の該それぞれのデータシェアの場所へのポインタのうちの１つを含む、請求項９に記載の方法。
【請求項１１】
前記生成されたデータシェアと関連付けられる前記情報を閲覧するコマンドを受信することと、
前記記憶ネットワーク上の前記場所から前記スタブを回収することと、
データシェアのファイルシステムを作成するために、該スタブから該情報を抽出することと、
該データシェアのファイルシステムを表示することと
をさらに含む、請求項９に記載の方法。
【請求項１２】
前記スタブは、前記生成されたデータシェアのヘッダ内に記憶され、回収することが、該生成されたデータシェアの該ヘッダを回収することを含む、請求項９に記載の方法。
【請求項１３】
全てよりも少ない前記ヘッダが回収される、請求項１２に記載の方法。
【請求項１４】

前記スタブは、スタブディレクトリの中に記憶され、回収することが、該スタブディレクトリから該スタブを回収することを含む、請求項９に記載の方法。
【請求項１５】
前記スタブを中に記憶している前記記憶ネットワークの中の仮想ディレクトリまたは物理ディレクトリの指示を受信することをさらに含む、請求項９に記載の方法。
【請求項１６】
前記指示は、ユーザから受信される、請求項１５に記載の方法。
【請求項１７】
セキュアなデータ処理の加速のためのコプロセッサ加速デバイスであって、
該コプロセッサ加速デバイスは、
データを記憶するためのメモリと、
該メモリに連結されたメインプロセッサと、
該メインプロセッサおよび該メモリに連結されたコプロセッサであって、該メインプロセッサおよび該メモリは、データを暗号化すること、データを分割すること、およびデータを復号することのうちの少なくとも１つを含む専用のセキュアな解析機能を実行するように構成されている、コプロセッサと
を含む、コプロセッサ加速デバイス。
【請求項１８】
データを分割することは、情報分散アルゴリズム（ＩＤＡ）の使用を含む、請求項１７に記載のデバイス。
【請求項１９】
前記コプロセッサに連結されたフィールドプログラマブルゲートアレイをさらに含む、請求項１７に記載のデバイス。
【請求項２０】
前記ＦＰＧＡは、前記解析されたデータを暗号化すること、または暗号化データを復号することのうちの少なくとも１つを実行する、請求項１９に記載のデバイス。
【請求項２１】
前記コプロセッサは、ＰＣＩｅバスを介して前記メインプロセッサに連結されている、請求項１７に記載のデバイス。
【請求項２２】
前記コプロセッサは、ＨＴバスを介して前記メインプロセッサに連結されている、請求項１７に記載のデバイス。
【請求項２３】
前記メモリは、前記メインプロセッサ用の専用メモリを含む、請求項１７に記載のデバイス。
【請求項２４】
前記メモリは、前記コプロセッサ用の専用メモリを含む、請求項１７に記載のデバイス。
【請求項２５】
前記コプロセッサは、１つ以上の独立ディスクの冗長アレイ（ＲＡＩＤ）機能を実装する、ＲＡＩＤ処理ユニットである、請求項１７に記載のデバイス。
【請求項２６】
携帯用デバイスを使用してデータをセキュア化するための方法であって、
該方法は、
１つのキーに少なくとも部分的に基づいて、一組のデータからデータの少なくとも２つの部分を生成することであって、該データの少なくとも２つの部分および該キーは、該一組のデータを再構成することに十分である、ことと、
該携帯用デバイス上に該キーかまたは該生成されたデータ部分のうちの少なくとも１つを記憶することと
を含む、方法。

【請求項２７】
前記携帯用デバイスは、取外し可能記憶デバイスである、請求項２６に記載の方法。
【請求項２８】
前記取外し可能記憶デバイスは、ユニバーサルシリアルバス（ＵＳＢ）インターフェースを介してエンドユーザデバイスに連結する、請求項２７に記載の方法。
【請求項２９】
前記キーは、暗号化キー、分割キー、および認証キーのうちの１つである、請求項２６に記載の方法。
【請求項３０】
前記データの少なくとも２つの部分は、情報分散アルゴリズム（ＩＤＡ）および該ＩＤＡと関連付けられる分割キーを使用して生成される、請求項２６に記載の方法。
【請求項３１】
分割され、および記憶ネットワーク上に記憶されるべきファイルのファイル名をセキュア化するための方法であって、
該方法は、
認証値を取得するために、認証アルゴリズムを使用して該ファイルの該ファイル名を処理することと、
該ファイルの該認証値に一致する認証値を有するデータシェアのファイル名について、該記憶ネットワーク上のシェア場所を検索することによって、該ファイルに対応する該データシェアを回収することと
を含む、方法。
【請求項３２】
情報分散アルゴリズムを使用して、前記認証されたファイル名と関連付けられる１つ以上のデータシェアを生成することと、
前記記憶ネットワーク内の１つ以上のデータシェア場所に該生成されたデータシェアを記憶することと
をさらに含む、請求項３１に記載の方法。
【請求項３３】
前記認証アルゴリズムは、ＨＭＡＣ－ＳＨＡ２５６アルゴリズムである、請求項３１に記載の方法。
【請求項３４】
分割され、および記憶ネットワーク上に記憶されるべきファイルのファイル名をセキュア化するための方法であって、
該方法は、
暗号化アルゴリズムを使用して、該ファイルの該ファイル名を暗号化することと、
情報分散アルゴリズムを使用して、該暗号化されたファイル名と関連付けられる１つ以上のデータシェアを生成することと、
該記憶ネットワーク内の１つ以上のデータシェア場所に該生成されたデータシェアを記憶することと、
該生成されたデータシェアのうちの１つのファイル名を復号することによって、該ファイルの該ファイル名を再生することと
を含む、方法。
【請求項３５】
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む、請求項８、９、３１または３４に記載の方法。
【請求項３６】
前記暗号化アルゴリズムは、ＡＥＳアルゴリズムである、請求項３４に記載の方法。
【請求項３７】
前記暗号化前に、付加的な情報を前記ファイルの前記ファイル名に付加することをさら

に含む、請求項３１または３４に記載の方法。
【請求項３８】
前記付加的な情報は、データシェア場所と関連付けられる数を含む、請求項３７に記載の方法。

【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２２
【補正方法】変更
【補正の内容】
【００２２】
別の側面では、本発明は、スタブを記憶ネットワークのファイルシステム上の一組のデータシェアと関連付けるための方法に関する。方法は、情報分散アルゴリズムによって、暗号化データセットから一組のデータシェアを生成するステップと、生成されたデータシェアと関連付けられる一組のスタブを生成するステップとを含む。各スタブは、それぞれのデータシェアに対応し、各スタブは、それぞれのデータシェアと関連付けられる情報を含む。一組のスタブは、記憶ネットワーク上の場所に記憶される。情報は、それぞれのデータシェアの名前、それぞれのデータシェアが作成された日付、それぞれのデータシェアが最後に修正された時間、ファイルシステム内のそれぞれのデータシェアの場所へのポインタのうちの１つを含む。記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つと関連付けられる１つ以上の記憶デバイスを含む。いくつかの実施形態においては、方法はさらに、生成されたデータシェアと関連付けられる情報を閲覧するコマンドを受信するステップと、記憶ネットワーク上の場所からスタブを回収するステップと、データシェアのファイルシステムを作成するように、スタブから情報を抽出するステップと、データシェアのファイルシステムを表示するステップとを含む。いくつかの実施形態においては、スタブは、生成されたデータシェアのヘッダ内に記憶され、回収するステップは、生成されたデータシェアのヘッダを回収するステップを含む。　いくつかの実施形態においては、全てよりも少ないヘッダが回収される。いくつかの実施形態においては、スタブは、スタブディレクトリに記憶され、回収するステップは、スタブディレクトリからスタブを回収するステップを含む。いくつかの実施形態においては、方法はさらに、スタブを記憶する仮想ディレクトリまたは物理ディレクトリの指示を受信するステップを含む。いくつかの実施形態においては、指示は、ユーザから受信される。
例えば、本発明は以下の項目を提供する。
（項目１）
一組のデータシェアを再構築するための方法であって、該一組のデータシェアは、第１の分割キーを使用して、情報分散アルゴリズムによって暗号化データセットから生成されたものであり、
該方法は、
該一組のデータシェアを再構築するために必要な少なくとも最小数のデータシェアを受信することと、
該最小数のデータシェアを復号することなしに、該最小数のデータシェアから該一組のデータシェアを再構築することと
を含む、方法。
（項目２）
前記再構築することは、前記データシェアのうちの１つ以上が既に損なわれているという決定に応じて行われる、項目１に記載の方法。
（項目３）
前記再構築されたデータシェアのうちの少なくとも１つを記憶ネットワーク上に記憶することをさらに含む、項目１に記載の方法。

（項目４）
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む、項目３に記載の方法。
（項目５）
前記再構築することは、
認証キーによって前記最小数のデータシェアを認証することと、
前記分割キーを使用して、該認証された最小数のデータシェアから前記暗号化データを再構成することと、
該分割キーを使用して該暗号化データを分割することによって、前記一組のデータシェアを再生することと
を含む、項目１に記載の方法。
（項目６）
一組のデータシェアのキーを再生成するための方法であって、該一組のデータシェアは、第１の暗号化キーを使用して、情報分散アルゴリズムによって暗号化データセットから生成されたものであり、
該方法は、
該一組のデータシェアを再構築するために必要な少なくとも最小数のデータシェアを受信することと、
該最小数のデータシェアを第１の認証キーと関連付けることと、
該最小数のデータシェアを復号することなしに、該最小数のデータシェアから該一組のデータシェアを再構築することと、
該再構築された一組のデータシェアを第２の暗号化キーと関連付けることによって、該再構築された一組のデータシェアのキーを再生成することと
を含む、方法。
（項目７）
前記最小数のデータシェアと関連付けられるヘッダを回収することと、
該回収されたヘッダからキー暗号化キーを抽出することと、
該キー暗号化キーによって第２の暗号化キーを暗号化することと、
前記キー再生成されたデータシェアのヘッダ内に暗号化された第２の認証キーを記憶することと
をさらに含む、項目６に記載の方法。
（項目８）
記憶ネットワーク上に前記キー再生成されたデータシェアのうちの少なくとも１つを記憶することをさらに含む、項目６に記載の方法。
（項目９）
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む、項目８に記載の方法。
（項目１０）
一組のデータシェアのキーを再生成するための方法であって、該一組のデータシェアは、第１の分割キーを使用して、情報分散アルゴリズムによって暗号化データセットから生成されたものであり、
該方法は、
該一組のデータシェアのキーを再生成するために必要な少なくとも最小数のデータシェアを受信することと、
該最小数のデータシェアを復号することなしに、該最小数のデータシェアから該一組のデータシェアを再構築することと、
該再構築された一組のデータシェアを第２の分割キーと関連付けることによって、該再構築された一組のデータシェアのキーを再生成することと

を含む、方法。
（項目１１）
前記最小数のデータシェアと関連付けられるヘッダを回収することと、
該回収されたヘッダからキー暗号化キーを抽出することと、
該キー暗号化キーによって第２の分割キーを暗号化することと、
前記キー再生成されたデータシェアのヘッダ内に該暗号化された第２の分割キーを記憶することと
をさらに含む、項目１０に記載の方法。
（項目１２）
記憶ネットワーク上に前記キー再生成されたデータシェアのうちの少なくとも１つを記憶することをさらに含む、項目１０に記載の方法。
（項目１３）
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む、項目１１に記載の方法。
（項目１４）
スタブを記憶ネットワークのファイルシステム上の一組のデータシェアと関連付けるための方法であって、
該方法は、
情報分散アルゴリズムによって、暗号化データセットから該一組のデータシェアを生成することと、
該生成されたデータシェアと関連付けられる一組のスタブを生成することであって、各スタブは、それぞれのデータシェアに対応し、各スタブは、該それぞれのデータシェアと関連付けられる情報を含む、ことと、
該記憶ネットワーク上の場所に該一組のスタブを記憶することと
を含む、方法。
（項目１５）
前記情報は、前記それぞれのデータシェアの名前、該それぞれのデータシェアが作成された日付、該それぞれのデータシェアが最後に修正された時間、前記ファイルシステム内の該それぞれのデータシェアの場所へのポインタのうちの１つを含む、項目１４に記載の方法。
（項目１６）
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つと関連付けられる、１つ以上の記憶デバイスを含む、項目１４に記載の方法。
（項目１７）
前記生成されたデータシェアと関連付けられる前記情報を閲覧するコマンドを受信することと、
前記記憶ネットワーク上の前記場所から前記スタブを回収することと、
データシェアのファイルシステムを作成するために、該スタブから該情報を抽出することと、
該データシェアのファイルシステムを表示することと
をさらに含む、項目１４に記載の方法。
（項目１８）
前記スタブは、前記生成されたデータシェアのヘッダ内に記憶され、回収することが、該生成されたデータシェアの該ヘッダを回収することを含む、項目１４に記載の方法。
（項目１９）
全てよりも少ない前記ヘッダが回収される、項目１８に記載の方法。
（項目２０）
前記スタブは、スタブディレクトリの中に記憶され、回収することが、該スタブディレ

クトリから該スタブを回収することを含む、項目１４に記載の方法。
（項目２１）
前記スタブを中に記憶している前記記憶ネットワークの中の仮想ディレクトリまたは物理ディレクトリの指示を受信することをさらに含む、項目１４に記載の方法。
（項目２２）
前記指示は、ユーザから受信される、項目２１に記載の方法。
（項目２３）
セキュアなデータ処理の加速のためのコプロセッサ加速デバイスであって、
該コプロセッサ加速デバイスは、
データを記憶するためのメモリと、
該メモリに連結されるメインプロセッサと、
該メインプロセッサおよび該メモリに連結されるコプロセッサであって、該メインプロセッサおよび該メモリは、データを暗号化すること、データを分割すること、およびデータを復号することのうちの少なくとも１つを含む専用のセキュアな解析機能を実行するように構成される、コプロセッサと
を含む、コプロセッサ加速デバイス。
（項目２４）
データを分割することは、情報分散アルゴリズム（ＩＤＡ）の使用を含む、項目２３に記載のデバイス。
（項目２５）
前記コプロセッサに連結されるフィールドプログラマブルゲートアレイをさらに含む、項目２３に記載のデバイス。
（項目２６）
前記ＦＰＧＡは、前記解析されたデータを暗号化すること、または暗号化データを復号することのうちの少なくとも１つを実行する、項目２５に記載のデバイス。
（項目２７）
前記コプロセッサは、ＰＣＩｅバスを介して前記メインプロセッサに連結される、項目２３に記載のデバイス。
（項目２８）
前記コプロセッサは、ＨＴバスを介して前記メインプロセッサに連結される、項目２３に記載のデバイス。
（項目２９）
前記メモリは、前記メインプロセッサ用の専用メモリを含む、項目２３に記載のデバイス。
（項目３０）
前記メモリは、前記コプロセッサ用の専用メモリを含む、項目２３に記載のデバイス。
（項目３１）
前記コプロセッサは、１つ以上の独立ディスクの冗長アレイ（ＲＡＩＤ）機能を実装する、ＲＡＩＤ処理ユニットである、項目２３に記載のデバイス。
（項目３２）
携帯用デバイスを使用してデータをセキュア化するための方法であって、
該方法は、
１つのキーに少なくとも部分的に基づいて、一組のデータからデータの少なくとも２つの部分を生成することであって、該データの少なくとも２つの部分および該キーは、該一組のデータを再構成することに十分である、ことと、
該携帯用デバイス上に該キーを記憶することと
を含む、方法。
（項目３３）
前記携帯用デバイスは、取外し可能記憶デバイスである、項目３２に記載の方法。
（項目３４）

前記取外し可能記憶デバイスは、ユニバーサルシリアルバス（ＵＳＢ）インターフェースを介してエンドユーザデバイスに連結する、項目３３に記載の方法。
（項目３５）
前記携帯用デバイス上に前記生成されたデータ部分のうちの少なくとも１つを記憶することをさらに含む、項目３２に記載の方法。
（項目３６）
前記キーは、暗号化キー、分割キー、および認証キーのうちの１つである、項目３２に記載の方法。
（項目３７）
前記データの少なくとも２つの部分は、情報分散アルゴリズム（ＩＤＡ）および該ＩＤＡと関連付けられる分割キーを使用して生成される、項目３２に記載の方法。
（項目３８）
携帯用デバイスを使用してデータをセキュア化するための方法であって、
該方法は、
１つのキーに少なくとも部分的に基づいて、一組のデータからデータの少なくとも２つの部分を生成することであって、該データの少なくとも２つの部分および該キーは、該一組のデータを再構成するために十分である、ことと、
該携帯用デバイス上に該生成されたデータ部分のうちの少なくとも１つを記憶することと
を含む、方法。
（項目３９）
前記携帯用デバイスは、取外し可能記憶デバイスである、項目３８に記載の方法。
（項目４０）
前記取外し可能記憶デバイスは、ユニバーサルシリアルバス（ＵＳＢ）インターフェースを介してエンドユーザデバイスに連結する、項目３９に記載の方法。
（項目４１）
前記携帯用デバイス上に前記キーを記憶することをさらに含む、項目３８に記載の方法。
（項目４２）
前記キーは、暗号化キー、分割キー、および認証キーのうちの１つである、項目３８に記載の方法。
（項目４３）
前記データの少なくとも２つの部分は、情報分散アルゴリズム（ＩＤＡ）および該ＩＤＡと関連付けられる分割キーを使用して生成される、項目３８に記載の方法。
（項目４４）
分割され、記憶ネットワーク上に記憶されるファイルのファイル名をセキュア化するための方法であって、
該方法は、
認証値を取得するために、認証アルゴリズムを使用して該ファイルの該ファイル名を処理することと、
該ファイルの該認証値に一致する０認証値を有するデータシェアのファイル名について、該記憶ネットワーク上のシェア場所を検索することによって、該ファイルに対応する該データシェアを回収することと
を含む、方法。
（項目４５）
情報分散アルゴリズムを使用して、前記認証されたファイル名と関連付けられる１つ以上のデータシェアを生成することと、
前記記憶ネットワーク内の１つ以上のデータシェア場所に該生成されたデータシェアを記憶することと
をさらに含む、項目４４に記載の方法。

（項目４６）
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む、項目４４に記載の方法。
（項目４７）
前記認証アルゴリズムは、ＨＭＡＣ－ＳＨＡ２５６アルゴリズムである、項目４４に記載の方法。
（項目４８）
前記処理前に、付加的な情報を前記ファイルの前記ファイル名に付加することをさらに含む、項目４４に記載の方法。
（項目４９）
前記付加的な情報は、データシェア場所と関連付けられる数を含む、項目４８に記載の方法。
（項目５０）
分割され、および記憶ネットワーク上に記憶されるべきファイルのファイル名をセキュア化するための方法であって、
該方法は、
暗号化アルゴリズムを使用して、該ファイルの該ファイル名を暗号化することと、
情報分散アルゴリズムを使用して、該暗号化されたファイル名と関連付けられる１つ以上のデータシェアを生成することと、
該記憶ネットワーク内の１つ以上のデータシェア場所に該生成されたデータシェアを記憶することと、
該生成されたデータシェアのうちの１つのファイル名を復号することによって、該ファイルの該ファイル名を再生することと
を含む、方法。
（項目５１）
前記記憶ネットワークは、私的クラウド、公衆クラウド、ハイブリッドクラウド、取外し可能記憶デバイス、および大容量記憶デバイスのうちの１つを含む、項目５０に記載の方法。
（項目５２）
前記暗号化アルゴリズムは、ＡＥＳアルゴリズムである、項目５０に記載の方法。
（項目５３）
前記暗号化前に、付加的な情報を前記ファイルの前記ファイル名に付加することをさらに含む、項目５０に記載の方法。
（項目５４）
前記付加的な情報は、データシェア場所と関連付けられる数を含む、項目５３に記載の方法。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/030801

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/08 G06F21/00 H04L9/08 G06F17/30 G06F11/10
G06F11/20 G06F3/06
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	RABIN M O: "EFFICIENT DISPERSAL OF INFORMATION FOR SECURITY, LOAD BALANCING, AND FAULT TOLERANCE", JOURNAL OF THE ASSOCIATION FOR COMPUTING MACHINERY, ACM, NEW YORK, NY, US, vol. 36, no. 2, 1 April 1989 (1989-04-01), pages 335-348, XP000570108, ISSN: 0004-5411, DOI: DOI:10.1145/62044.62050 the whole document ----- -/--	1

[X] Further documents are listed in the continuation of Box C.
[X] See patent family annex.

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

Date of the actual completion of the international search	Date of mailing of the international search report
15 November 2011	23/11/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Mäenpää, Jari

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/030801

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HUGO KRAWCZYK: "Secret Sharing Made Short", INTERNET CITATION, 1998, pages 1-11, XP002505270, Retrieved from the Internet: URL:http://www.cs.cornell.edu/courses/cs754/2001fa/secretshort.pdf [retrieved on 2008-11-24]	1,5
Y	the whole document	2-4
Y	US 2008/183975 A1 (FOSTER LYNN [US] ET AL) 31 July 2008 (2008-07-31) paragraph [0041] the whole document	2-4
A	SHAMIR ET AL: "HOW TO SHARE A SECRET", IP.COM JOURNAL, IP.COM INC., WEST HENRIETTA, NY, US, 30 March 2007 (2007-03-30), XP013119902, ISSN: 1533-0001 the whole document	1-5
A	GANGER G R ET AL: "Survivable storage systems", DARPA INFORMATION SURVIVABILITY CONFERENCE & EXPOSITION II, 2001. DISC EX '01. PROCEEDINGS 12-14 JUNE 2001, PISCATAWAY, NJ, USA,IEEE, vol. 2, 12 June 2001 (2001-06-12), pages 184-195, XP010548746, ISBN: 978-0-7695-1212-9 the whole document	1-5
X	US 2008/147821 A1 (DIETRICH BRADLEY W [US] ET AL) 19 June 2008 (2008-06-19) paragraph [0042] - paragraph [0056] paragraph [0084] - paragraph [0089] paragraphs [0139] - [0144]	6-13
X	Gregory R Ganger ET AL: "PASIS: A Distributed Framework for Perpetually Available and Secure Information Systems, Final technical rept. Jun 1999-Dec 2003", , 1 July 2005 (2005-07-01), pages 1-203, XP55011444, Retrieved from the Internet: URL:http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA436245&Location=U2&doc=GetTRDoc.pdf [retrieved on 2011-11-07] page 1 - page 18 paragraph [0003]	14-22

-/--

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/030801

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2009/254572 A1 (REDLICH RON M [US] ET AL) 8 October 2009 (2009-10-08) paragraph [0073] paragraph [3155] - paragraph [3160] figures D-10	23-31
Y	EASTER R J ET AL: "S/390 parallel enterprise server CMOS cryptographic coprocessor", IBM JOURNAL OF RESEARCH AND DEVELOPMENT, INTERNATIONAL BUSINESS MACHINES CORPORATION, NEW YORK, NY, US, vol. 43, no. 5, 1 January 1999 (1999-01-01), pages 761-776, XP002335589, ISSN: 0018-8646 the whole document	23-31
X	US 2009/177894 A1 (ORSINI RICK L [US] ET AL) 9 July 2009 (2009-07-09) figure 36 the whole document paragraph [0434]	32-43
Y	US 5 485 474 A (RABIN MICHAEL O [US]) 16 January 1996 (1996-01-16) the whole document	44-54
Y	US 2004/267832 A1 (WONG THOMAS K [US] ET AL) 30 December 2004 (2004-12-30) paragraph [0050] - paragraph [0051]	44-54

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/030801

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

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

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

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

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

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

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

see additional sheet

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

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

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

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

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

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

☒ No protest accompanied the payment of additional search fees.

International Application No. PCT/US2011/030801

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-5

A method for rebuilding dispersed data wherein rebuilding is performed in response to a determination that one or more of the data shares have been compromised. The problem to be solved is to achieve better integrity protection and reliability of the storing method.

---

2. claims: 6-13

A method for rekeying a set of data shares dispersed using a key.The problem to be solved is to achieve better confidentiality protection of the stored data.

---

3. claims: 14-22

A method for associating stubs with a set of data shares on the file system of a storage network. The problem to be solved is to implement an efficient storage network.

---

4. claims: 23-31

A co-processor acceleration device for secure parsing functions. The problem to be solved is to implement an efficient hardware based secure parser.

---

5. claims: 32-43

A method for securing data using a portable device. The problem to be solved is to implement a data security system adapted to portable devices.

---

6. claims: 44-54

A method for securing the file name of a file to be split. The problem to be solved is to implement an efficient file name security.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2011/030801

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008183975 A1	31-07-2008	EP 2260387 A2	15-12-2010
		US 2008183975 A1	31-07-2008
		US 2010161916 A1	24-06-2010
		WO 2009123865 A2	08-10-2009
US 2008147821 A1	19-06-2008	NONE	
US 2009254572 A1	08-10-2009	NONE	
US 2009177894 A1	09-07-2009	AU 2009204512 A1	16-07-2009
		CA 2710868 A1	16-07-2009
		CN 101939946 A	05-01-2011
		EP 2106642 A1	07-10-2009
		US 2009177894 A1	09-07-2009
		WO 2009089015 A1	16-07-2009
US 5485474 A	16-01-1996	NONE	
US 2004267832 A1	30-12-2004	NONE	

フロントページの続き

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

(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 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

Ｆターム(参考) 5J104 AA08 AA16 AA32 EA02 EA04 EA18 EA19 FA00 JA03 JA21
LA06 MA05 NA02 NA37 NA38 PA07