

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号
特許第5663083号
(P5663083)

(45) 発行日 平成27年2月4日(2015.2.4)

(24) 登録日 平成26年12月12日(2014.12.12)

(51) Int.Cl.
G06F 21/62 (2013.01)

F I
G O 6 F 21/24 1 6 6 D

請求項の数 22 (全 175 頁)

(21) 出願番号	特願2013-502866 (P2013-502866)	(73) 特許権者	512252526
(86) (22) 出願日	平成23年3月31日 (2011.3.31)		セキュリティ ファースト コープ.
(65) 公表番号	特表2013-525876 (P2013-525876A)		アメリカ合衆国 カリフォルニア 926
(43) 公表日	平成25年6月20日 (2013.6.20)		88, ランチョ サンタ マルガリータ
(86) 国際出願番号	PCT/US2011/030811		, サンタ マルガリータ パークウェイ
(87) 国際公開番号	W02011/123699		29811, スイート 600
(87) 国際公開日	平成23年10月6日 (2011.10.6)	(73) 特許権者	512253084
審査請求日	平成26年3月26日 (2014.3.26)		オルシーニ, リック エル.
(31) 優先権主張番号	61/320,242		アメリカ合衆国 テキサス 75028,
(32) 優先日	平成22年4月1日 (2010.4.1)		フラワー マウンド, キングス フォ
(33) 優先権主張国	米国 (US)		レスト レーン 2100
(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)		
早期審査対象出願		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) 【特許請求の範囲】

【請求項 1】

一組のデータを読み出し、書き込むための方法であって、
該方法は、
情報分散アルゴリズムを使用して、該一組のデータを1つ以上のデータシェアに分割することと、
該1つ以上のデータシェアをシェア場所の中に記憶することと、
該シェア場所のうちの少なくとも1つがデータ記憶動作について利用不可能であることを決定することであって、該データ記憶動作は、データ書き込み動作またはデータ読み出し動作を含む、ことと、

該利用不可能なシェア場所の各々と関連付けられた着信データ記憶動作を該利用不可能なシェア場所の各々に特有のそれぞれのジャーナリング待ち行列の中に記憶することとを含む、方法。

【請求項 2】

前記利用不可能なシェア場所のうちの少なくとも1つが、既に利用可能にされていることを決定することと、

該既に利用可能にされている少なくとも1つの利用不可能なシェア場所に特有の前記ジャーナリング待ち行列の中に記憶されている前記データ記憶動作を実行することとをさらに含む、請求項 1 に記載の方法。

【請求項 3】

前記実行されたデータ記憶動作をフラッシュすることをさらに含む、請求項 2 に記載の方法。

【請求項 4】

前記ジャーナリング待ち行列は、メモリの中に記憶されており、
前記方法は、
データ記憶動作の量と関連付けられる待ち行列限界を確立することと、
該待ち行列限界が該ジャーナリング待ち行列のうちの少なくとも 1 つについて超えていることを決定することと、
該待ち行列限界を超えている該ジャーナリング待ち行列の各々について、メモリからディスク記憶にそのジャーナリング待ち行列をフラッシュすることと
をさらに含む、請求項 1 に記載の方法。

10

【請求項 5】

シェア場所がデータ記憶動作について利用不可能である最大時間量を確立することと、
該最大時間量が前記利用不可能なシェア場所のうちの少なくとも 1 つについて超えていることを決定することと、
該最大時間量を超えている該利用不可能なシェア場所の各々について、着信データ記憶動作を拒絶することと
をさらに含む、請求項 1 に記載の方法。

【請求項 6】

一組のデータを読み出し、書き込むための方法であって、
該方法は、
情報分散アルゴリズムを使用して、該一組のデータを 1 つ以上のデータシェアに分割することと、
該 1 つ以上のデータシェアをシェア場所の中に記憶することと、
失敗したデータ記憶動作の最大数を確立することであって、該データ記憶動作は、データ書き込み動作またはデータ読み出し動作を含む、ことと、
該シェア場所の各々と関連付けられる失敗した着信データ記憶動作を、それぞれのジャーナリング待ち行列の中に記憶することと、
該ジャーナリング待ち行列のうちの少なくとも 1 つの中に記憶された該失敗した着信データ記憶動作が、該確立された最大数を超えていることを決定することと、
該確立された最大数を超えている該ジャーナリング待ち行列のうちの該少なくとも 1 つの中に記憶された該失敗した着信データ記憶動作を破棄することと
を含む、方法。

20

30

【請求項 7】

着信データ記憶動作を破棄することをさらに含み、該着信データ記憶動作は、前記確立された最大数を超えているそれぞれのジャーナリング待ち行列の各々と関連付けられる、請求項 6 に記載の方法。

【請求項 8】

前記 1 つ以上のデータシェアの各々を 2 つ以上のシェア場所の中に記憶することと、
前記確立された最大数を超えている前記ジャーナリング待ち行列のうちの少なくとも 1 つと関連付けられる各シェア場所について、該確立された最大数を超えなかった該ジャーナリング待ち行列のうちの少なくとも 1 つと関連付けられる該 2 つ以上のシェア場所のうちの少なくとも 1 つを使用して、該 1 つ以上のデータシェアのうちの少なくとも 1 つを再構築することと
をさらに含む、請求項 6 に記載の方法。

40

【請求項 9】

一組のデータを読み出し、書き込むための方法であって、
該方法は、
情報分散アルゴリズムを使用して、該一組のデータを 1 つ以上のデータシェアに分割することと、

50

該1つ以上のデータシェアをシェア場所の中に記憶することであって、該シェア場所が、再構築中のシェア場所を含み、該再構築中のシェア場所が、該データシェアのうちの少なくとも1つを修復するように構成されている、ことと、

該一組のデータに対するデータ記憶動作を行う要求を受信することであって、該データ記憶動作は、データ書き込み動作またはデータ読み出し動作である、ことと、

該1つ以上のデータシェアのうちの少なくとも1つが、該再構築中のシェア場所の中において修復されることを決定することと、

該決定に基づいて、該データ記憶動作を、該再構築中のシェア場所と関連付けられるジャーナリング待ち行列の中に記憶することと

を含む、方法。

10

【請求項10】

前記1つ以上のデータシェアが、前記再構築中のシェア場所の中において修復されないことを決定することと、

該1つ以上のデータシェアが該再構築中のシェア場所の中において修復されないという決定に基づいて、前記データ記憶動作を破棄することと

をさらに含む、請求項9に記載の方法。

【請求項11】

前記再構築中のシェア場所が、データ記憶動作に利用可能であることを決定することと

、
該再構築中のシェア場所がデータ記憶動作に利用可能であるという決定に基づいて、該再構築中のシェア場所と関連付けられる前記ジャーナリング待ち行列の中に記憶された前記データ記憶動作を実行することと

をさらに含む、請求項9に記載の方法。

20

【請求項12】

一組のデータを読み出し、書き込むためのシステムであって、該システムは、少なくとも1つのプロセッサを含み、

該少なくとも1つのプロセッサは、

情報分散アルゴリズムを使用して、該一組のデータを1つ以上のデータシェアに分割することと、

該1つ以上のデータシェアをシェア場所の中に記憶することと、

30

該シェア場所のうちの少なくとも1つがデータ記憶動作に利用不可能であることを決定することであって、該データ記憶動作は、データ書き込み動作またはデータ読み出し動作を含む、ことと、

該利用不可能なシェア場所の各々と関連付けられる着信データ記憶動作を、該利用不可能なシェア場所の各々に特有のそれぞれのジャーナリング待ち行列の中に記憶することと
を行うように構成されている、システム。

【請求項13】

前記少なくとも1つのプロセッサは、

前記利用不可能なシェア場所のうちの少なくとも1つが、既に利用可能にされていることを決定することと、

40

既に利用可能にされている該利用不可能なシェア場所のうちの少なくとも1つに特有の前記ジャーナリング待ち行列の中に記憶された前記データ記憶動作を実行することと

を行うようにさらに構成されている、請求項12に記載のシステム。

【請求項14】

前記少なくとも1つのプロセッサは、前記実行されたデータ記憶動作をフラッシュするようにさらに構成されている、請求項13に記載のシステム。

【請求項15】

メモリおよびディスク記憶をさらに備え、前記少なくとも1つのプロセッサが、

前記ジャーナリング待ち行列を該メモリの中に記憶することと、

データ記憶動作の量と関連付けられる待ち行列限界を確立することと、

50

該待ち行列限界が該ジャーナリング待ち行列のうちの少なくとも1つについて超えていることを決定することと、

該待ち行列限界を超えている該ジャーナリング待ち行列の各々について、該メモリから該ディスク記憶にそのジャーナリング待ち行列をフラッシュすることと

を行うようにさらに構成されている、請求項12に記載のシステム。

【請求項16】

前記少なくとも1つのプロセッサは、

シェア場所がデータ記憶動作について利用不可能である最大時間量を確認することと、

前記利用不可能なシェア場所のうちの少なくとも1つについて該最大時間量を超えていることを決定することと、

該最大時間量を超えている該利用不可能なシェア場所の各々について、着信データ記憶動作を拒絶することと

を行うようにさらに構成されている、請求項12に記載のシステム。

【請求項17】

一組のデータを読み出し、書き込むためのシステムであって、該システムは、少なくとも1つのプロセッサを含み、

該少なくとも1つのプロセッサは、

情報分散アルゴリズムを使用して、該一組のデータを1つ以上のデータシェアに分割することと、

該1つ以上のデータシェアをシェア場所の中に記憶することと、

失敗したデータ記憶動作の最大数を確認することであって、該データ記憶動作は、データ書き込み動作またはデータ読み出し動作を含む、ことと、

該シェア場所の各々と関連付けられる失敗した着信データ記憶動作を、それぞれのジャーナリング待ち行列の中に記憶することと、

該ジャーナリング待ち行列のうちの少なくとも1つの中に記憶された該失敗した着信データ記憶動作が、該確立された最大数を超えていることを決定することと、

該確立された最大数を超えている該ジャーナリング待ち行列のうちの少なくとも1つの中に記憶された該失敗した着信データ記憶動作を破棄することと

を行うように構成されている、システム。

【請求項18】

前記少なくとも1つのプロセッサは、前記確立された最大数を超えているそれぞれのジャーナリング待ち行列の各々と関連付けられる着信データ記憶動作を破棄するようにさらに構成されている、請求項17に記載のシステム。

【請求項19】

前記少なくとも1つのプロセッサは、

前記1つ以上のデータシェアの各々を2つ以上のシェア場所の中に記憶することと、

前記確立された最大数を超えている前記ジャーナリング待ち行列のうちの少なくとも1つと関連付けられる各シェア場所について、該確立された最大数を超えなかった該ジャーナリング待ち行列のうちの少なくとも1つと関連付けられる該2つ以上のシェア場所のうちの少なくとも1つを使用して、該1つ以上のデータシェアのうちの少なくとも1つを再構築することと

を行うようにさらに構成されている、請求項17に記載のシステム。

【請求項20】

一組のデータを読み出し、書き込むためのシステムであって、該システムは、少なくとも1つのプロセッサを含み、

該少なくとも1つのプロセッサは、

情報分散アルゴリズムを使用して、該一組のデータを1つ以上のデータシェアに分割することと、

該1つ以上のデータシェアをシェア場所の中に記憶することであって、該シェア場所が、再構築中のシェア場所を含み、該再構築中のシェア場所が、該データシェアのうちの少

10

20

30

40

50

なくとも1つを修復するように構成されている、ことと、

該一組のデータに対するデータ記憶動作を行う要求を受信することであって、該データ記憶動作は、データ書き込み動作またはデータ読み出し動作である、ことと、

該1つ以上のデータシェアのうちの少なくとも1つが、該再構築中のシェア場所の中において修復されることを決定することと、

該決定に基づいて、該データ記憶動作を、該再構築中のシェア場所と関連付けられるジャーナリング待ち行列の中に記憶することと

を行うように構成されている、システム。

【請求項21】

前記少なくとも1つのプロセッサは、

前記1つ以上のデータシェアが、前記再構築中のシェア場所において修復されないことを決定することと、

該1つ以上のデータシェアが該再構築中のシェア場所の中において修復されないという決定に基づいて、前記データ記憶動作を破棄することと

を行うようにさらに構成されている、請求項20に記載のシステム。

【請求項22】

前記少なくとも1つのプロセッサは、

前記再構築中のシェア場所が、データ記憶動作について利用可能であることを決定することと、

該再構築中のシェア場所がデータ記憶動作に利用可能であるという決定に基づいて、該再構築中のシェア場所と関連付けられる前記ジャーナリング待ち行列の中に記憶された前記データ記憶動作を実行することと

を行うようにさらに構成されている、請求項20に記載のシステム。

【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

【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)

ジャーナリングサービスを使用して、一組のデータを読み出し、書き込むためのシステムおよび方法を提供する。ジャーナリングサービスは、1つ以上のシェア場所に記憶された1つ以上のデータのシェアと関連付けられるデータ記憶動作を識別および記録するために使用され得る。シェア場所は、ローカルまたはネットワークハードディスク、USBキー等のリムーバブル記憶装置、あるいはDropBoxまたはAmazon S3等のクラウド記憶プロバイダのリソース等の、任意の好適なデータ記憶設備またはデータ記憶設備の組み合わせを含んでもよい。ジャーナリングサービスは、シェア場所へ読み出しおよび書き込み要求のそれぞれを記録するためにログを使用してもよい。いくつかの実施形態では、ログは、失敗したデータ記憶動作と関連付けられる情報を記憶する待ち行列データ構造であってもよい。

10

【課題を解決するための手段】

【0004】

いくつかの実施形態では、ジャーナリング待ち行列は、各シェア場所の状態と関連付けられる情報を維持してもよい。例えば、ジャーナリングサービスは、シェア場所のうちの1つ以上がデータ記憶動作を処理するために利用不可能であることを決定してもよい。次いで、ジャーナリング待ち行列は、利用不可能なシェア場所のそれぞれについて確立および維持されてもよい。いくつかの実施形態では、ジャーナリング待ち行列は、利用不可能なシェア場所のそれぞれに関して固有であってもよい。いくつかの実施形態では、ジャーナリング待ち行列は、利用不可能なシェア場所のそれぞれと関連付けられる着信データ記憶動作を記憶してもよい。特定のシェア場所が利用可能になると、ジャーナリングサービスは、そのシェア場所に特有のジャーナリング待ち行列に記憶されたデータ記憶動作を実行してもよい。

20

【0005】

いくつかの実施形態では、ジャーナリングサービスは、ジャーナリング待ち行列を維持するために、メモリおよびディスク記憶の両方を活用してもよい。例えば、ジャーナリング待ち行列の中に記憶され得るデータ記憶動作の量を規定する限界が確立されてもよい。待ち行列限界が特定のジャーナリング待ち行列について超えていることをジャーナリングサービスが決定した場合、ジャーナリングサービスは、メモリからディスク記憶までジャーナリング待ち行列の中のメッセージを転送してもよい。このようにして、ジャーナリングサービスは、ジャーナリングサービスを実行するシステムのメモリが超えていないことを保証する。

30

【0006】

いくつかの実施形態では、ジャーナリングサービスは、シェア場所がデータ記憶動作に利用不可能である最大時間を規定してもよい。この最大時間量が特定のシェア場所について超えていることをジャーナリングサービスが決定した場合、ジャーナリングサービスは、特定のシェアに対する着信データ記憶動作を受け入れることを拒絶してもよい。このようにして、特定のシェア場所は、突発的故障として印付けられ、シェア場所と関連付けられる全てのデータ記憶動作は、シェア場所が修復または再構築されるまで中断させられる。

40

【0007】

いくつかの実施形態では、ジャーナリングサービスは、特定のシェア場所の中のデータの完全性をもはや信用することができないと決定してもよい。ジャーナリングサービスは、特定のシェア場所について失敗したデータ記憶動作の数に基づいて、この決定を行ってもよい。この数が確立された最大数を超えている場合、ジャーナリングサービスは、致命的な故障状態にあるものとしてシェア場所を印付けてもよく、そのシェア場所と関連付け

50

られるジャーナリング待ち行列の中に記憶されたデータ記憶動作は破棄されてもよい。加えて、ジャーナリングサービスは、致命的な故障状態のシェア場所に対する任意の着信データ記憶動作を破棄してもよい。このようにして、ジャーナリングサービスは、ジャーナリングサービスを実行するシステムのメモリまたはディスクスペースが節約されることを保証する。

【0008】

いくつかの実施形態では、ジャーナリングサービスは、通常の使用に利用可能であるものとしてシステム上の他のシェアを維持しながら、シェアが再構築されることを可能にしてもよい。この再構築過程は、オンラインであり、再構築されているシェア場所と同様のデータを含むする他のシェア場所を使用してもよい。いくつかの実施形態では、ジャーナリングサービスは、再構築されているシェア場所で修復されたファイルのリストを維持してもよい。再構築されているシェア場所と関連付けられるファイルにデータ記憶動作を行う要求が受信されたときに、ジャーナリングサービスは、ファイルがリストの中にあるか否かを決定してもよい。ファイルがリストの中にある場合、データ記憶動作は、いったんシェア場所が再構築し終わると、記録をつけられ、実行され得る。ファイルがリスト上にない場合、ジャーナリングサービスは、データ記憶動作を破棄してもよい。

本願明細書は、例えば、以下の項目も提供する。

(項目1)

一組のデータを読み出し、書き込むための方法であって、

該方法は、

情報分散アルゴリズムを使用して、該一組のデータを1つ以上のデータシェアに分割することと、

該1つ以上のデータシェアをシェア場所の中に記憶することと、

該シェア場所のうちの少なくとも1つがデータ記憶動作について利用不可能であることを決定することと、

該利用不可能なシェア場所の各々と関連付けられた着信データ記憶動作を該利用不可能なシェア場所の各々に特有のそれぞれのジャーナリング待ち行列の中に記憶することと

を含む、方法。

(項目2)

前記利用不可能なシェア場所のうちの少なくとも1つが、既に利用可能にされていることを決定することと、

該既に利用可能にされている少なくとも1つの利用不可能なシェア場所に特有の前記ジャーナリング待ち行列の中に記憶されている前記データ記憶動作を実行することと

をさらに含む、項目1に記載の方法。

(項目3)

前記実行されたデータ記憶動作をフラッシュすることをさらに含む、項目2に記載の方法。

(項目4)

前記ジャーナリング待ち行列は、メモリの中に記憶されており、

該ジャーナリング待ち行列は、

データ記憶動作の量と関連付けられる待ち行列限界を確立することと、

該待ち行列限界が該ジャーナリング待ち行列のうちの少なくとも1つについて超えていることを決定することと、

該待ち行列限界を超えてる該ジャーナリング待ち行列の各々について、メモリからディスク記憶に該ジャーナリング待ち行列をフラッシュすることと

をさらに含む、項目1に記載の方法。

(項目5)

シェア場所がデータ記憶動作について利用不可能である最大時間量を確認することと、

該最大時間量が利用不可能なシェア場所のうちの少なくとも1つについて超えていることを決定することと、

10

20

30

40

50

該最大時間量を超えている該利用不可能なシェア場所の各々について、着信データ記憶動作を拒絶することと

をさらに含む、項目 1 に記載の方法。

(項目 6)

一組のデータを読み出し、書き込むための方法であって、

該方法は、

情報分散アルゴリズムを使用して、該一組のデータを 1 つ以上のデータシェアに分割することと、

該 1 つ以上のデータシェアをシェア場所の中に記憶することと、

失敗したデータ記憶動作の最大数を確立することと、

該シェア場所の各々と関連付けられる失敗した着信データ記憶動作を、それぞれのジャーナリング待ち行列の中に記憶することと、

該ジャーナリング待ち行列のうちの少なくとも 1 つの中に記憶された該失敗した着信データ記憶動作が、該確立された最大数を超えていることを決定することと、

該確立された最大数を超えている該ジャーナリング待ち行列のうちの該少なくとも 1 つの中に記憶された該失敗した着信データ記憶動作を破棄することと

を含む、方法。

(項目 7)

着信データ記憶動作を破棄することをさらに含み、該着信データ記憶動作は、前記確立された最大数を超えているそれぞれのジャーナリング待ち行列の各々と関連付けられる、
項目 6 に記載の方法。

(項目 8)

前記 1 つ以上のデータシェアの各々を 2 つ以上のシェア場所の中に記憶することと、

前記確立された最大数を超えている前記ジャーナリング待ち行列のうちの少なくとも 1 つと関連付けられる各シェア場所について、オンラインである該 2 つ以上のシェア場所のうちの少なくとも 1 つを使用して、該シェアを再構築することと

をさらに含む、項目 6 に記載の方法。

(項目 9)

一組のデータを読み出し、書き込むための方法であって、

該方法は、

情報分散アルゴリズムを使用して、該一組のデータを 1 つ以上のデータシェアに分割することと、

該 1 つ以上のデータシェアをシェア場所の中に記憶することであって、シェア場所のうちの少なくとも 1 つは再構築中である、ことと、

再構築中である該シェア場所のうちの 1 つと関連付けられるファイルにデータ記憶動作を行う要求を受信することと、

該ファイルが、再構築中である該シェア場所のうちの 1 つの中において修復されることを決定することと、

該決定に基づいて、該データ記憶動作を、再構築中である該シェア場所のうちの 1 つと関連付けられるジャーナリング待ち行列の中に記憶することと

を含む、方法。

(項目 10)

前記ファイルが、再構築中である前記 1 つ以上のシェア場所の中において修復されないことを決定することと、

該決定に基づいて、前記データ記憶動作を破棄することと

をさらに含む、項目 9 に記載の方法。

(項目 11)

再構築中である前記シェア場所のうちの前記 1 つが、データ記憶動作に利用可能であることを決定することと、

該決定に基づいて、再構築中である該シェア場所のうちの該 1 つと関連付けられる前記

10

20

30

40

50

ジャーナリング待ち行列の中に記憶された前記データ記憶動作を実行することと
をさらに含む、項目 9 に記載の方法。

(項目 1 2)

一組のデータを読み出し、書き込むためのシステムであって、該システムは、処理回路を含み、

該処理回路は、

情報分散アルゴリズムを使用して、該一組のデータを 1 つ以上のデータシェアに分割することと、

該 1 つ以上のデータシェアをシェア場所の中に記憶することと、

該シェア場所のうちの少なくとも 1 つがデータ記憶動作に利用不可能であることを決定することと、

該利用不可能なシェア場所の各々と関連付けられる着信データ記憶動作を、該利用不可能なシェア場所の各々に特有のそれぞれのジャーナリング待ち行列の中に記憶することと
を行うように構成される、システム。

(項目 1 3)

前記処理回路は、

前記利用不可能なシェア場所のうちの少なくとも 1 つが、既に利用可能にされていることを決定することと、

既に利用可能にされている前記少なくとも 1 つの利用不可能なシェア場所に特有の前記ジャーナリング待ち行列の中に記憶された前記データ記憶動作を実行することと

を行うように構成される、項目 1 2 に記載のシステム。

(項目 1 4)

前記処理回路は、前記実行されたデータ記憶動作をフラッシュするようにさらに構成される、項目 1 3 に記載のシステム。

(項目 1 5)

メモリおよびディスク記憶をさらに備え、前記処理回路が、

前記ジャーナリング待ち行列を該メモリの中に記憶することと、

データ記憶動作の量と関連付けられる待ち行列限界を確立することと、

該待ち行列限界が該ジャーナリング待ち行列のうちの少なくとも 1 つについて超えていることを決定することと、

該待ち行列限界を超えている該ジャーナリング待ち行列の各々について、該メモリから該ディスク記憶に該ジャーナリング待ち行列をフラッシュすることと

を行うようにさらに構成される、項目 1 2 に記載のシステム。

(項目 1 6)

前記処理回路は、

シェア場所がデータ記憶動作について利用不可能である最大時間量を確立することと、

該最大時間量が、利用不可能なシェア場所のうちの少なくとも 1 つについて超えていることを決定することと、

該最大時間量を超えている該利用不可能なシェア場所の各々について、着信データ記憶動作を拒絶することと

を行うようにさらに構成される、項目 1 2 に記載のシステム。

(項目 1 7)

一組のデータを読み出し、書き込むためのシステムであって、該システムは、処理回路を含み、

該処理回路は、

情報分散アルゴリズムを使用して、該一組のデータを 1 つ以上のデータシェアに分割することと、

該 1 つ以上のデータシェアをシェア場所の中に記憶することと、

失敗したデータ記憶動作の最大数を確立することと、

該シェア場所の各々と関連付けられる失敗した着信データ記憶動作を、それぞれのジャーナリング待ち行列の中に記憶することと、

10

20

30

40

50

ジャーナリング待ち行列の中に記憶することと、

該ジャーナリング待ち行列のうちの少なくとも1つの中に記憶された該失敗した着信データ記憶動作が、該確立された最大数を超えていることを決定することと、

該確立された最大数を超えている該ジャーナリング待ち行列のうちの少なくとも1つの中に記憶された該失敗した着信データ記憶動作を破棄することと

を行うように構成される、システム。

(項目18)

前記処理回路は、前記確立された最大数を超えているそれぞれのジャーナリング待ち行列の各々と関連付けられる着信データ記憶動作を破棄するようにさらに構成される、項目17に記載のシステム。

(項目19)

前記処理回路は、

前記1つ以上のデータシェアの各々を2つ以上のシェア場所の中に記憶することと、

前記確立された最大数を超えている前記ジャーナリング待ち行列のうちの少なくとも1つと関連付けられる各シェア場所について、オンラインである該2つ以上のシェア場所のうちの少なくとも1つを使用して、該シェアを再構築することと

を行うようにさらに構成される、項目17に記載のシステム。

(項目20)

一組のデータを読み出し、書き込むためのシステムであって、該システムは、処理回路を含み、

該処理回路は、

情報分散アルゴリズムを使用して、該一組のデータを1つ以上のデータシェアに分割することと、

該1つ以上のデータシェアをシェア場所の中に記憶することであって、シェア場所のうちの少なくとも1つは再構築中である、ことと、

再構築中である該シェア場所のうちの1つと関連付けられるファイルにデータ記憶動作を実行する要求を受信することと、

該ファイルが、再構築中である該シェア場所のうちの該1つにおいて修復されることを決定することと、

該決定に基づいて、該データ記憶動作を、再構築中である該シェア場所のうちの該1つと関連付けられるジャーナリング待ち行列の中に記憶することと

を行うように構成される、システム。

(項目21)

前記処理回路は、

前記ファイルが、再構築中である前記1つ以上のシェア場所において修復されないことを決定することと、

該決定に基づいて、前記データ記憶動作を破棄することと

を行うようにさらに構成される、項目20に記載のシステム。

(項目22)

前記処理回路は、

再構築中である前記シェア場所のうちの前記1つが、データ記憶動作について利用可能であることを決定することと、

該決定に基づいて、再構築中である該シェア場所のうちの該1つと関連付けられる前記ジャーナリング待ち行列の中に記憶された該データ記憶動作を実行することと

を行うようにさらに構成される、項目20に記載のシステム。

【0009】

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】

【0010】

10

20

30

40

50

【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。

10

【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 9 A】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 9 B】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。

20

【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。

30

【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。

40

【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。

50

【図 2 5】図 2 5 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 2 6】図 2 6 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 2 7】図 2 7 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 2 8】図 2 8 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 2 9】図 2 9 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。

10

【図 3 0】図 3 0 - 3 2 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 3 1】図 3 0 - 3 2 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 3 2】図 3 0 - 3 2 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 3 3】図 3 3 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 3 4】図 3 4 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。

20

【図 3 5】図 3 5 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 3 6】図 3 6 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 3 7】図 3 7 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 3 8】図 3 8 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。

30

【図 3 9】図 3 9 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 4 0】図 4 0 A および 4 0 B 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 4 1】図 4 1 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。

40

【図 4 2】図 4 2 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 4 3】図 4 3 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 4 4】図 4 4 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 4 5】図 4 5 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

50

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。

10

【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。

20

【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。

30

【図５７】図５７は、本発明の例示的实施形態による、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、本発明の例示的实施形態による、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５９】図５９は、本発明の実施形態による、ジャーナリングサービス进行操作するための例示的な過程である。

【図６０】図６０は、本発明の実施形態による、ジャーナリングサービス进行操作するための例示的な過程である。

【図６１】図６１は、本発明の実施形態による、致命的故障状態を使用してジャーナリングサービス进行操作するための例示的な過程である。

40

【図６２】図６２は、本発明の実施形態による、重要再構築状態を使用してジャーナリングサービス进行操作するための例示的な過程である。

【発明を実施するための形態】

【００１１】

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。

【００１２】

50

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。

【0013】

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。

【0014】

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。

【0015】

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。

【0016】

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。

【0017】

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

クを含む。

【0018】

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。

10

【0019】

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。

20

30

【0020】

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。

【0021】

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、暗号機能で利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。

40

【0022】

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

50

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。

【0023】

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。

10

【0024】

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。

【0025】

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。

20

30

【0026】

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。

【0027】

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)

40

50

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。

【0028】

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。

【0029】

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。

【0030】

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規定される。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。

【0031】

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。

【0032】

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規定、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。

【0033】

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。

【0034】

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。

【0035】

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。

【0036】

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。

【0037】

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 2 2 5 に有利に記憶されてもよい。

【0038】

図 2 はまた、保管場所 2 1 0 も図示する。一実施形態によれば、保管場所 2 1 0 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 2 1 0 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 1 1 0 に、またはユーザあるいはベンダ等の暗号システム 1 0 0 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 1 1 0 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。

10

【0039】

一実施形態によれば、トランザクションエンジン 2 0 5 から認証エンジン 2 1 5 および暗号エンジン 2 2 0 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 2 1 0 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。

【0040】

前述のように、保管場所 2 1 0 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。

20

【0041】

図 2 はまた、認証エンジン 2 1 5 を含む信頼エンジン 1 1 0 も図示する。一実施形態によれば、認証エンジン 2 1 5 は、トランザクションエンジン 2 0 5 からのデータを保管場所 2 1 0 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 2 0 5 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 1 1 0 に供給する。前述のように、トランザクションエンジン 2 0 5 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 2 1 5 に送る。また、要求に応じて、保管場所 2 1 0 は、ユーザに対応する登録認証データを認証エンジン 2 1 5 に転送する。したがって、認証エンジン 2 1 5 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。

30

【0042】

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 1 1 0 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 2 1 5 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 2 1 0 もまた、認証エンジン 2 1 5 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。

40

【0043】

図 2 に示されるように、信頼エンジン 1 1 0 はまた、暗号エンジン 2 2 0 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

50

。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。

【0044】

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。

【0045】

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。

【0046】

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。

【0047】

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。

【0048】

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、Ne

10

20

30

40

50

t s c a p e、I S O、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。

10

【0049】

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。

【0050】

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。

20

【0051】

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。

30

【0052】

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、部分的に一致、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。

40

【0053】

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。

【0054】

50

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。

【0055】

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。

10

【0056】

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。

【0057】

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。

20

30

【0058】

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。

40

【0059】

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。

50

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。

【0060】

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。

10

【0061】

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。

20

【0062】

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。

30

【0063】

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。

40

【0064】

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

50

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 D 1 乃至 D 4 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 7 0 0 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 D 1 乃至 D 4 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 1 1 0 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 D 1 乃至 D 4 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。

10

【0065】

保管場所システム 7 0 0 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 7 0 0 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 7 0 0 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。

20

【0066】

前述のように、認証エンジン 2 1 5 および暗号エンジン 2 2 0 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 5 2 0 および 6 1 0 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 8 0 0 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 8 0 0 は、機密データ「S」が認証エンジン 2 1 5 または暗号エンジン 2 2 0 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 8 0 5 から始まる。好ましくは、次いで、ステップ 8 1 0 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。

30

【0067】

加えて、ステップ 8 2 0 では、データ分割過程 8 0 0 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、 $A \oplus S$ という 2 値組み合わせを備えてもよく、数字 D は、 $C \oplus S$ という 2 値組み合わせを備えてもよい。 $\oplus$ 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 8 2 5 および 8 3 0 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 8 0 0 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 8 3 5 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 D 1 乃至 D 4 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 D 1 乃至 D 4 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 8 0 0 中に、対合 AC は、例えば、D 2 の IP アドレスの無作為選択を通して、保管場所 D 2 に送信されてもよい。次いで、第 2 のデータ分割過程 8 0 0 中に、対合 AC は、例

40

50

えば、D 4 の I P アドレスの無作為選択を通して、保管場所 D 4 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。

【0068】

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 D 1 乃至 D 4 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 D 1 乃至 D 4 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 D 1 乃至 D 4 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。

10

【0069】

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。

20

30

【0070】

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 D 1 乃至 D 4 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 D 1 乃至 D 4 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、A C、A D、B C、および B D 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。 $S = A \oplus B$ または $S = C \oplus D$ 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 D 1 乃至 D 4 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。

40

【0071】

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 21

50

5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。

【0072】

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、組み合わせられ、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。

10

【0073】

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わせを行う、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、問い合わせ過程中に、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。

20

【0074】

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。

30

40

【0075】

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。

【0076】

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

50

、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。

【0077】

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。

【0078】

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。

【0079】

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。

【0080】

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。

【0081】

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。

【0082】

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。

【0083】

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。

【0084】

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。

【0085】

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。

【0086】

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、Base32またはBase64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。

【0087】

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97

10

20

30

40

50

0 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。

10

【0088】

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。

20

【0089】

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。

30

【0090】

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。

40

【0091】

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

50

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。

【0092】

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。

10

【0093】

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。

【0094】

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。

20

【0095】

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。

30

【0096】

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。

40

50

【0097】

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。

【0098】

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
10
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。

【0099】

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
20
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。

【0100】

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
30
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。

【0101】

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。

【0102】

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。

【0103】

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
50

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。

【0104】

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。

10

【0105】

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。

20

【0106】

加えて、認証過程 1000 は、機密データボ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 桁であるランダムな英数字の文字列を選択してもよい。

30

【0107】

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。

40

【0108】

さらに別の実施形態においては、データボルトは、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 1

50

10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。

【0109】

前述のデータボ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。

10

【0110】

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。

20

【0111】

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。

30

【0112】

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。

40

【0113】

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

50

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。

【0114】

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。

10

【0115】

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。

20

【0116】

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。

30

【0117】

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。

40

【0118】

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

50

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。

【0119】

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の全体を通じた伝送は、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。

【0120】

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るとしてもよい、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。

【0121】

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。

【0122】

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。

【0123】

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。

10

【0124】

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。

【0125】

20

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。

30

【0126】

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るとしてもよい、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。

40

【0127】

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

50

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ン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。

【0128】

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。

【0129】

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。

【0130】

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。

【0131】

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、ペンダシステム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。

【0132】

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。

【0133】

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。

【0134】

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の部分の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。

【0135】

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。

【0136】

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。

【0137】

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。

10

【0138】

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。

【0139】

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。

20

30

【0140】

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。

40

【0141】

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。

50

【0142】

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。

【0143】

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。

【0144】

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。

【0145】

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。

【0146】

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。

【0147】

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）。

【0148】

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。

【0149】

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。

10

【0150】

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。

20

【0151】

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。

30

【0152】

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。

40

【0153】

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

50

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。

【0154】

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。

10

【0155】

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。

20

【0156】

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じた登録、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。

【0157】

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。

30

【0158】

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。

40

【0159】

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。

【0160】

50

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。

【0161】

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。

10

【0162】

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。

20

【0163】

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。

【0164】

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、いくつかは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。

30

40

【0165】

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

50

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。

【0166】

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。

10

【0167】

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。

20

【0168】

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。

30

【0169】

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。

40

【0170】

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。

【0171】

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（

50

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。

【0172】

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、認証リクエストによって使用されるモジュールを含んでもよい。

10

【0173】

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。

20

【0174】

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。)

30

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。

【0175】

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。)

40

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

50

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、 $14\% \times 25\% \times 28\% = 0.98\%$ の不信頼性という累積的不信頼性を得る。

【0176】

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）。

【0177】

さらに、異なるベンダまたは他の認証リクエストが、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。

【0178】

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。

【0179】

そのような様々な加重は、1つの動作モードで、認証リクエストによって、または認証要求を生成する際に規定され、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、認証リクエストに対する初期の登録過程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。

【0180】

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、認証リクエスト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。

【0181】

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。

【0182】

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

10

20

30

40

50

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。

【0183】

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。

10

【0184】

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

20

【0185】

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

30

【0186】

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トによって信頼エンジン110に特定されてもよい。認証リクエストはまた、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ト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。

40

【0187】

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

50

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。

【0188】

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。

10

【0189】

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。

20

【0190】

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。

30

【0191】

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。

40

【0192】

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

50

ンダまたはユーザの選好に基づいて、決定されてもよい。

【0193】

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。

10

【0194】

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。

20

【0195】

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。

【0196】

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。

30

【0197】

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。

40

【0198】

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

50

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。

【0199】

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。

10

【0200】

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。

20

【0201】

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。

30

【0202】

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ず、デフォルトの一組の要件を使用してもよいので、有益であってもよい。

40

【0203】

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、

50

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。

【0204】

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。

【0205】

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。

【0206】

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

【0207】

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。

【0208】

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。

【0209】

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。

【0210】

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。

【0211】

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。

【0212】

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動作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。

【0213】

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。

【0214】

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。

【0215】

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。

【0216】

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。

【0217】

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。

【0218】

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。

10

【0219】

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。

20

【0220】

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。

【0221】

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。

30

【0222】

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。

40

【0223】

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、

50

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。

【0224】

そのような暗号機能は、通常、C A P I 2 0 1 0 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 1 0 5、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（S P M）2 0 1 5、2 0 2 0 によって提供される。そのような S P M は、暗号化または復号動作を行うソフトウェアライ
10
ブラリ 2 0 1 5、または生体測定走査デバイス等の特殊ハードウェア 2 0 2 5 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 2 0 2 0 を含んでもよい。C A P I 2 0 1 0 がシステム 1 0 5 のアプリケーション 2 0 0 0 によって使用されてもよい機能を提供するのとはほぼ同じように、S P M 2 0 1 5、2 0 2 0 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 C A P I に提供する。

【0225】

本発明によれば、信頼エンジン 1 1 0 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、C A P I 2 0 1 0 を通してアプリケーション 2 0 0 0 に利用可能にすることが可能である、暗号 S P M 2 0 3 0 を提供することが可能である。C A P I 2 0 1 0 が、
20
S P M 2 0 1 5、2 0 2 0 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 S P M 2 0 3 0 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 1 1 0 に提出することが可能となる。

【0226】

例えば、アプリケーション 2 0 0 0 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 2 0 0 0 は、適切な C A P I 2 0 1 0 機能への機能呼出しを行う。C A P I 2 0 1 0 は順に、この関数を実行し、S P M 2 0 1 5、2 0 2 0 および暗号 S P M 2 0 3 0 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 S P M 2 0 3 0 は、通信リンク 1 2 5 にわたって信頼エンジン 1 1 0 に送信
30
される適切な要求を生成する。

【0227】

暗号 S P M 2 0 3 0 と信頼エンジン 1 1 0 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 1 1 0 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 1 0 5 自体の上でローカルにて利用可能と思われるように、C A P I 2 0 1 0 を通してユーザシステム 1 0 5 に効果的に利用可能となる。しかしながら、通常の S P M 2 0 1 5、2 0 2 0 と違って、機能は、遠隔信頼エンジン 1 1 0 上で実行されており、結果は、通信リンク 1 2 5 にわたって適切な要求に応じて暗号 S P M 2 0 3 0 に中継される。

【0228】

この暗号 S P M 2 0 3 0 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 1 0 5 またはベンダシステム 1 2 0 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。

【0229】

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
50

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。

【0230】

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。

【0231】

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トの必要性に応じて、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。

【0232】

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。

【0233】

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

10

20

30

40

50

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（ r_1 、 r_2 、 r_3 乃至 r_{23} ）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 r_1 の中へ、第2のバイトをシェア r_2 の中へ、第3のバイトをシェア r_3 の中へ、乃至データの第23のバイトをシェア r_{23} 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。

【0234】

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。

【0235】

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せられ、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、

$$(\text{主要シェア数} + \text{バックアップシェア数}) \text{MOD } 4 = \text{第3のシェア数}$$

である。

【0236】

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。

【0237】

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。

【0238】

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、以下のである。

```
DATA [1 : 24] ー 分割されるデータを有するバイトのアレイ 10
SHARES [0 : 3 ; 1 : 24] ー 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] ー 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 20
                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 30
                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。

【0239】

2組の数を生成し、Primary Share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]) mod 4]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。

【0240】

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

10

20

30

40

50

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。

【0241】

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うまであり、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。

10

【0242】

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。

20

【0243】

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。

30

【0244】

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。

【0245】

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。

【0246】

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。

40

【0247】

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。

【0248】

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。

【0249】

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。

50

【0250】

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。

【0251】

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。

10

【0252】

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。

【0253】

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。

【0254】

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的トランザクション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。

20

【0255】

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。

【0256】

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。

【0257】

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。

30

【0258】

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。

【0259】

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。

40

【0260】

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。

【0261】

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。

【0262】

50

2. 一意のセッションマスターキーを生成する。

【0263】

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。

【0264】

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。

【0265】

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。

10

【0266】

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。

【0267】

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。

【0268】

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。

20

【0269】

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。

【0270】

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。

【0271】

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。

30

【0272】

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。

【0273】

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。

40

【0274】

2. 一意のセッションマスターキーを生成する。

【0275】

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。

【0276】

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。

【0277】

50

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。

【0278】

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。

10

【0279】

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。

【0280】

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。

【0281】

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。

【0282】

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。

20

【0283】

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。

【0284】

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нта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нта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нта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、 $x \oplus y$ は、xおよびyのビット排他論理和を意味する。

30

【0285】

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。

40

【0286】

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

$b = a \oplus s$

50

を設定する。

【0287】

式を介して「s」を導出できることに留意されたい。

$$s = a \text{ XOR } b$$

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。

【0288】

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

10

秘密キー5をセキュア化し、
 $S = D \text{ XOR } K5$ である。

【0289】

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、

$$SD1 = S1 \text{ XOR } K1、$$

20

$$SD2 = S2 \text{ XOR } K2、$$

$$SD3 = S3 \text{ XOR } K3、$$

$$SDn = Sn \text{ XOR } Kn$$

である。

【0290】

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

30

保管場所3：SD3，K2

保管場所n：SDn，K3

に記憶される。

【0291】

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

40

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

50

に分割される。

【0292】

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。

【0293】

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、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。

【0294】

（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RC4TM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。

【0295】

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

$$SD1 = S1 \quad XOR \quad E(K1)$$

$$SD2 = S2 \quad XOR \quad E(K2)$$

$$SD3 = S3 \quad XOR \quad E(K3)$$

$$SDn = Sn \quad XOR \quad E(Kn)$$

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。

【0296】

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、RC4TM、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。

【0297】

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

理的な場所であってもよい、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分に低減される。

【0298】

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。

10

【0299】

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。

【0300】

1. データセットの全てのシェアまたは部分。

20

【0301】

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。

【0302】

3. セッションマスターキーへのアクセス。

【0303】

4. パーサマスターキーへのアクセス。

【0304】

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。

30

【0305】

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。

【0306】

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。

40

【0307】

（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。

50

【0308】

(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。

【0309】

(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。

10

【0310】

(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。

20

【0311】

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。

30

【0312】

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。

40

【0313】

(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。

【0314】

(2. セッションマスターキー)

50

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。

【0315】

(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。

10

【0316】

(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。

【0317】

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。

20

30

【0318】

(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する、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。

40

【0319】

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、およびデータスループットは、ユーザが自由に使える状態で有するハードウェアのみに限定される。

【0320】

50

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 2 3 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。

【0321】

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、組織によって規定されるような役割、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。

【0322】

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ル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。

【0323】

図 2 5 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規定される 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。

【0324】

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。

【0325】

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、措置は以下ようになる。

【0326】

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）。

【0327】

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。

【0328】

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。

【0329】

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。

【0330】

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。

【0331】

いったん共有信任状が規定されると、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。

【0332】

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。

【0333】

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。

10

20

30

40

50

【0334】

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。

【0335】

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。

【0336】

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2502を含む。解析されたデータの一部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。

【0337】

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）。

【0338】

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。

10

【0339】

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。

20

【0340】

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。

30

【0341】

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。

40

【0342】

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）。

50

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。

【0343】

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、Wi-Fi）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ともよいように、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。

10

【0344】

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、Wi-Fi、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。

20

30

【0345】

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、Wi-Fi、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。

40

50

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。

【0346】

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。

【0347】

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。

【0348】

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。

【0349】

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 Smart Phones 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。

【0350】

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、Apple IPOD または他の MP3 プレーヤ）、フラッシュメモリ、データを輸送するために使用される任意の他の好適な媒体、またはそれらの任意の組み合わせの上で行われてもよい

。

【0351】

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、 $n \leq m$ 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。

10

【0352】

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るとしてもよい。

【0353】

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。

20

【0354】

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。

30

【0355】

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。

40

【0356】

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））。

【0357】

50

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。

【0358】

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。

【0359】

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。

【0360】

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。

【0361】

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。

【0362】

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。

【0363】

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

10

20

30

40

50

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。

【0364】

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。

【0365】

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、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。

【0366】

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、ラップ層 3022 を通過させられ、ステップ 3102 において、ラップ層 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、ラップ層 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、ラップ層 3022 が、記憶された情報 3106 から、（すなわち、ステップ 3102 においてラップ 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、ラップ層 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）。

【0367】

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、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、ラップ層 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。ラップ層 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

10

20

30

40

50

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。

【0368】

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。

10

【0369】

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。

20

【0370】

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。

30

【0371】

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、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。

40

【0372】

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。

【0373】

50

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。

【0374】

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。

10

【0375】

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。

20

【0376】

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。

30

【0377】

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乱数値の対応するバイトに行われてもよいように、乱数または擬似乱数値は、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。

40

【0378】

50

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。

【0379】

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じた後に、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。

【0380】

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る。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。

【0381】

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。

【0382】

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。

【0383】

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。

【0384】

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。

【0385】

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。

【0386】

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。

【0387】

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。

【0388】

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。

【0389】

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。

【0390】

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A o N T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、A o N Tが適用されてもよいことが理解されるであろう。同様に、A o N Tは、分割キーに適用されてもよい。

【0391】

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。

10

【0392】

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。

【0393】

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、B l a k e l y等の他のキー分割（例えば、秘密共有）アルゴリズムが、S h a m i rの代わりに使用されてもよく、またはA E S暗号化を、T r i p l e D E S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。

20

【0394】

(1) 3 6 1 0、3 6 1 2、3 6 1 4、3 6 1 5、3 6 1 6、3 6 1 7、3 6 1 8、3 6 1 9)

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、A l l o r N o t h i n g T r a n s f o r m (A o N T) 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。

30

【0395】

(2) 3 1 1 1、3 6 1 2、3 6 1 4、3 6 1 5、3 6 1 6、3 6 1 7、3 6 1 8、3 6 1 9)

40

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、A l l o r N o t h i n g T r a n s f o r m (A o N T) 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

50

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。

【0396】

(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。

【0397】

(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。

【0398】

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。

【0399】

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。

【0400】

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。

【0401】

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。

【0402】

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。

【0403】

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。

【0404】

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。

【0405】

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。

【0406】

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。

【0407】

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。

【0408】

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。

【0409】

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

10

20

30

40

50

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。

【0410】

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。

10

【0411】

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。

【0412】

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。

20

【0413】

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。

【0414】

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。

30

【0415】

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。

【0416】

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。

40

【0417】

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

50

用されている技法を以下に規定する。

【0418】

(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／ dongle）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 of 両方へのアクセスを必要とする、多因子認証を提供する。

10

【0419】

(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。

【0420】

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。

20

【0421】

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

30

40

50

ーションと一体化してもよい。

【0422】

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。

【0423】

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。

【0424】

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。

【0425】

（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。

【0426】

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。

【0427】

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。

【0428】

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。

【0429】

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。

【0430】

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。

【0431】

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。

【0432】

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。

【0433】

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と呼び出すと、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。

【0434】

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。

【0435】

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。

【0436】

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タ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、Bit Segment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Block Segment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。

【0437】

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。

【0438】

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Bit SegmentあるいはBlock Segment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。

【0439】

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、暗号化されたデ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的に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、暗号化されたデータセットシェア

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。

【0440】

10

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 $(X_1, Y_1), \dots, (X_c, Y_c)$ 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 $\perp$ 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。

【0441】

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可能性がある。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。

20

【0442】

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。

【0443】

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。

30

【0444】

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への入力ブロック $M = M_1 \dots M_l$ 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、Block Segment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。

40

【0445】

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。

【0446】

50

賢明な I D A 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、I D A がどれだけ高性能であろうと、どのような目標が H K 1 / H K 2 との関連で I D A を用いて達成されようとしていても、知能は、I D A 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 I D A とともに残される。

【0447】

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 I D A $\Pi^{I D A}$ が使用されてもよい。例えば、全ての暗号化スキーム $\Pi^{E n c}$ について、1 対 ($\Pi^{I D A}$, $\Pi^{E n c}$) 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、I D A が提供される。

10

【0448】

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 R C S S 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、I D A を伴って H K 1 / H K 2 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。

【0449】

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。

20

【0450】

共有キーは、多因子または 2 因子秘密共有 (2 F S S) 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るであってもよく、(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) 必要があるであってもよい。

30

【0451】

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 R C S S 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)。

40

【0452】

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 $S_1 = (S_1[1], \dots, S_1[n])$ 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 であると考えられるビット 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

50

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。

【0453】

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 $M_1, \dots, M_q$ 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 $S_1, \dots, S_q$ 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、 $\{M_1, \dots, M_q\}$ 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。

10

【0454】

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、Blakeley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。

【0455】

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。

20

【0456】

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。

【0457】

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。

30

40

【0458】

（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

50

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。

【0459】

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。

【0460】

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。

10

20

30

40

50

【0461】

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。

10

【0462】

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。

【0463】

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。

20

30

【0464】

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。

【0465】

40

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を通して移動するときに、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は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。

【0466】

50

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。

【0467】

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。

【0468】

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。

【0469】

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。

【0470】

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。

【0471】

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。

【0472】

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。

【0473】

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

10

20

30

40

50

【0474】

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。

【0475】

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。

【0476】

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送信してもよい

。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。さらなる例示的实施例として、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。

【0477】

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の例示的实施形態においては、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。

【0478】

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。

【0479】

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。

【0480】

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Extended (SPX) 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。

【0481】

いくつかの実施形態では、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個の別個の、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。

【0482】

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、ユーザのリムーバブル記憶デバイス5104の中および大容量記憶デバイス5106上において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必要とされるので、障害からのロバスト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の実施形態では、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必要とされる。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必要と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。リムーバブル記憶デバイス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必要とされ得る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では、リムーバブル記憶デバイス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では、ユーザは、暗号化キー自体を管理してもよい。これらの実施形態では、ユーザのキーは、リムーバブル記憶デバイス（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。他の実施形態では、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。

10

【0483】

いくつかの実施形態では、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。

20

30

【0484】

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に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等のリムーバブル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必要とされるので、障害からのロバスト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の実施形態では、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必要とされる。したがって、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必要と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等のリムーバブル記憶デバイスが失われ

40

50

た場合、またはそれらの任意の組み合わせにおいて生じる場合がある。

【0485】

いくつかの実施形態では、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。さらなる例示的实施例として、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。

【0486】

いくつかの実施形態では、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伴う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。

【0487】

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において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5306aおよび5306b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

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必要と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、生じる場合がある。

【0488】

図51-53の実施形態のそれぞれにおいて、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必要とされるので、障害からのロバスト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、上記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、またはリムーバブル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に、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に、任意の単一の解析されたシェアは法廷的に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状態のままであり得る。言い換えれば、単一の解析されたシェアは、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がなければ、再構成、復号、不正侵入、または復旧されることができない。

【0489】

いくつかの実施形態では、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において使用されてもよい。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。

【0490】

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では、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では、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では、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の実施形態では、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に実装される。いくつかの実施形態では、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。

【0491】

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

10

20

30

40

50

たは主要プロセッサ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み出し専用メモリ(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。

【0492】

いくつかの実施形態では、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では、RPU5404は、アレイ構築型計算および/またはRAID計算を行うために、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では、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では、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では、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、上記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、上記で説明されるもの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では、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る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。

【0493】

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、この例示的实施形態では、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によって果たされ得る一方で、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によって果たされ得ることを図示する。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表示がある、図55の右側に示されている。

【0494】

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、この例示的实施形態では、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によって果たされ得る一方で、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によって果たされ得ることを図示する。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表示がある、図55の右側に示されている。

【0495】

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得ることを認識するであろう。

【0496】

いくつかの実施形態では、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では、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得る。したがって、軽微な変更のみがデータファイルにおいて行われるときに、データファイル全体の修復が、行われることも、必要とされることもない。

【0497】

いくつかの実施形態では、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では、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、データシェア内にも記憶される。いくつかの実施形態では、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では、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、リムーバブル

ル記憶デバイス、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。

【0498】

いくつかの実施形態では、スタブは、データシェアとは別の場所、データシェアと同じ場所、または両方に記憶されてもよい。いくつかの実施形態では、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では、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、後に上記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。

10

【0499】

いくつかの実施形態では、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。

【0500】

いくつかの実施形態では、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、上記の技法を使用して、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を試みる。

20

【0501】

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得、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得る。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／承認システムとともに機能してもよい。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ることはない。

30

40

【0502】

いくつかの実施形態では、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では、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、本発明の例示的实施形態による、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、本発明の例示的实施形態による、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のそれぞれにおいて、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

50

い。

【0503】

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において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において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必要と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において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。

【0504】

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か、失われているか、またはそうでなければアクセス不可能であるため、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か、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)。

【0505】

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、上記の図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では、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に記憶される。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、リムーバブル記憶デバイス、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において記憶されてもよい。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させ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。

【0506】

いくつかの実施形態では、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。例示的实施例として、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させる。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させ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させることはできない。

【0507】

いくつかの実施形態では、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アルゴリズムによって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得な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。これらの実施形態では、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では、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、この認証値に合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、リムーバブル記憶デバイス、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では、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では、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。

【0508】

いくつかの実施形態では、本発明のセキュアなパーサは、上記で説明されたように、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、リムーバブル記憶デバイス、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。上記の実施例と同様に、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。

【0509】

いくつかの実施形態では、ディスクへの読み出しおよび書き込みの失敗等の入出力失敗から保護するために、ジャーナリングサービスが使用されてもよい。これらの実施形態では、ジャーナリングサービスは、1つ以上のシェア場所に記憶された1つ以上のデータのシェアと関連付けられる読み出しおよび書き込み要求等のデータ記憶動作のそれぞれを識別および記録するために使用されてもよい。1つ以上のデータのシェアは、キーのあるIDA等の任意の好適な情報分散アルゴリズムを使用して、一組の元のデータから作成されてもよい。データのシェアは、上記で開示される任意の好適な無作為化または決定論的技法を使用して無秩序にされ、次いで、分割されたデータを含んでもよい。シェア場所は、ローカルまたはネットワークハードディスク、USBキー等のリムーバブル記憶装置、あるいはDropBoxまたはAmazon S3等のクラウド記憶プロバイダのリソース等の、上記で説明された任意の好適なデータ記憶設備またはデータ記憶設備の組み合わせを含んでもよい。加えて、シェア場所は、データのシェアと関連付けられる任意の好適な数のファイルを記憶してもよい。いくつかの実施形態では、ジャーナリングサービスは、セキュアなデータパーサがデータを記憶するために使用するシェア場所でデータの健全を維持するために、図37の例示的な概観過程3700のセキュアなデータパーサ3706等のセキュアなデータパーサと一体化してもよい。いくつかの実施形態では、ジャーナリングサービスは、1つ以上のマイクロプロセッサまたは処理回路を有する汎用コンピュータ上で実装されてもよい。

【0510】

いくつかの実施形態では、ジャーナリングサービスは、シェア場所へ読み出しおよび書き込み要求のそれぞれを記録するためにログを使用してもよい。このログは、ジャーナリングサービスを実行する設備で中央管理されてもよく、またはシェア場所自体に位置してもよい。いくつかの実施形態では、ログは、特定のシェア場所と関連付けられる、読み出しおよび書き込み動作等の失敗したデータ記憶動作と関連付けられる情報を記憶する待ち行列データ構造であってもよい。いくつかの実施形態では、ジャーナリング待ち行列は、ジャーナリングサービスと関連付けられる各シェア場所について維持されてもよい。ジャーナリング待ち行列は、ファイルレベル、ブロックレベル、ビットレベル、または任意の好適な粒度のレベルにおいて、失敗したデータ記憶動作に対する情報を記憶してもよい。いくつかの実施形態では、ジャーナリング待ち行列は、ジャーナリングサービスを実行するサーバのRAM等のジャーナリングサービスと関連付けられるメモリに維持されてもよい。いくつかの実施形態では、ジャーナリング待ち行列は、ジャーナリングサービスと関連付けられるディスク記憶に維持されてもよい。例えば、ジャーナリング待ち行列は、ジャーナリングサービスを実行するサーバ内のディスク上に記憶された構成ファイルに維持されてもよい。図60に関して以下で説明されるように、いくつかの実施形態では、ジャーナリングサービスは、ジャーナリング待ち行列を維持するために、メモリおよびディスク記憶の両方を活用してもよい。

【0511】

図59は、本発明の実施形態による、ジャーナリングサービスを操作するための例示的な過程5900である。過程5900は、ステップ5910から始まる。ステップ5910において、1つ以上のデータのシェアがシェア場所に記憶され得る。上記で論議されたように、1つ以上のデータのシェアは、任意の好適なIDAを使用して作成されてもよく、任意の好適な無作為化または決定論的技法を使用して無秩序化および分割されたデータを含んでもよい。次いで、過程5900は、ステップ5920へと進む。ステップ5920において、ジャーナリングサービスは、特定のシェア場所がオフラインであるか、また

はデータ記憶動作に利用不可能であるか否かを決定してもよい。この決定は、特定のシェア場所と関連付けられる試行したデータ記憶動作に起因してもよい。例えば、ジャーナリングサービスは、データシェアを特定のシェア場所書き込もうとしてもよい。書き込み動作が成功しなかった場合、ジャーナリングサービスは、書き込み動作が失敗したという通知を受信してもよい。したがって、ジャーナリングサービスは、将来の読み出しまたは書き込み動作に利用不可能であるか、またはオフラインであるものとして、特定のシェア場所を印付けてもよい。いくつかの実施形態では、シェア場所がオフラインであるという表示は、ジャーナリングサービスの中心となるメモリまたはディスクに維持された任意の好適なデータフラグに、またはデータシェア自体の上に記憶されてもよい。次いで、過程5900は、ステップ5930へと進む。

10

【0512】

ステップ5930において、ジャーナリング待ち行列が、オフラインと指定されている特定のシェア場所に対して確立および維持されてもよい。いくつかの実施形態では、シェア場所がオフラインと指定されている限り、ジャーナリングサービスは、シェア場所に関係する着信データ記憶動作と関連付けられる情報を、ジャーナリング待ち行列に記憶してもよい。例えば、シェア場所がオフラインとして印付けられた場合、そのシェア場所に関係する将来の読み出しおよび書き込み動作は、そのシェア場所について確立されたジャーナリング待ち行列に記憶される。いくつかの実施形態では、ジャーナリングサービスによって維持される各ジャーナリング待ち行列は、固有のシェア場所と関連付けられてもよい。加えて、ジャーナリングサービスによって維持される各ジャーナリング待ち行列は、別個の処理スレッドによって管理されてもよい。次いで、過程5900は、ステップ5940へと進む。

20

【0513】

ステップ5940において、ジャーナリングサービスは、オフライン記憶場所が利用可能になっているか否かを決定してもよい。いくつかの実施形態では、この決定は、シェア場所が修復されたという表示についてオフラインシェア場所を常に監視するジャーナリングサービスによって行われてもよい。この表示は、例えば、ジャーナリングサービスまたはジャーナリングサービスの管理者によるシェア場所の修復によって引き起こされる、シェア場所と関連付けられたデータフラグの変更であってもよい。次いで、過程5900は、ステップ5950へと進む。

30

【0514】

ステップ5950において、ジャーナリングサービスは、利用可能になったシェア場所に対するジャーナリング待ち行列に記憶された、失敗したデータ記憶動作を再生してもよい。いくつかの実施形態では、失敗した動作を再生することは、ジャーナリング待ち行列に記憶されている失敗した読み出しおよび書き込み動作を実行することを含んでもよい。いったんジャーナリング待ち行列に記憶された失敗した動作が実行されると、ジャーナリングサービスは、選択的に、ジャーナリング待ち行列を消去するか、またはフラッシュしてもよい。ジャーナリング待ち行列をフラッシュする際に、ジャーナリングサービスは、ジャーナリング待ち行列と関連付けられる任意のメモリまたはディスク記憶を解放してもよい。いったんジャーナリング待ち行列に記憶された失敗した動作が再生されると、次いで、過程5900は終了する。

40

【0515】

図60は、本発明の実施形態による、ジャーナリングサービスを操作するための例示的な過程6000である。過程6000は、ステップ6010から始まる。ステップ6010において、ジャーナリングサービスが、関連ジャーナリング待ち行列を有する各シェア場所に対する待ち行列限界を確立してもよい。この待ち行列限界は、ジャーナリングサービスと関連付けられるメモリに記憶することができる、ジャーナリング待ち行列と関連付けられるメッセージ（例えば、失敗した読み出しおよび書き込み動作）の最大数を特定してもよい。次いで、ジャーナリングサービスは、例えば、各ジャーナリング待ち行列の中のメッセージの数のログを維持することによって、各ジャーナリング待ち行列の中のメッ

50

セージの数を追跡してもよい。次いで、過程6000は、ステップ6020へと進む。ステップ6020において、ジャーナリングサービスは、待ち行列限界が特定のジャーナリング待ち行列について超えていることを決定してもよい。例えば、ジャーナリングサービスは、特定の待ち行列に記憶された失敗した動作の数が事前構成された最大数を超えることを決定してもよい。待ち行列限界が超えていることをジャーナリングサービスが決定した場合、過程6000は、ステップ6030へと進む。

【0516】

ステップ6030において、ジャーナリング待ち行列は、ジャーナリングサービスと関連付けられるディスク記憶に維持されるファイルにフラッシュされるか、または記憶されてもよい。いくつかの実施形態では、ファイルは、シェア場所が利用可能になるまで、ディスク記憶に維持されてもよい。例えば、シェア場所が利用可能になった後に、ジャーナリングサービスは、ファイルに記憶された各動作を再生し、次いで、ディスク記憶からファイルを除去してもよい。このようにして、ジャーナリングサービスによって記録された失敗した動作の数が、ジャーナリングサービスを実行するシステムのメモリ限界を上回ることを許容される。いくつかの実施形態では、メモリに記憶されているジャーナリング待ち行列のコンテンツは、システム動作停止（例えば、ジャーナリングサービスを実行するシステムへの電力の損失）の場合に、ファイルにフラッシュされてもよい。このようにして、ジャーナリングサービスは、いったんジャーナリングサービスを実行するシステムが修復されると、データ完全性の損失を伴わずに動作を復旧し得る。次いで、過程6000は終了する。待ち行列限界が超えていないことをジャーナリングサービスが決定した場合、過程6000は、ステップ6040へと進む。ステップ6040において、ジャーナリングサービスは、失敗した動作をメモリの中の待ち行列に書き込み続けてもよい。次いで、過程6000は終了する。

【0517】

いくつかの実施形態では、過剰に多くの失敗したデータ記憶動作がシェア場所に対して記録された場合、ジャーナリングサービスは、「致命的故障」状態を記録する。この致命的故障状態は、シェア場所内のデータの完全性をもはや信用することができず、修復または再構築動作が必要とされることを示してもよい。図61に関して説明されるように、致命的故障状態であるものとしてシェア場所を印付けることは、ジャーナリングサービスを実行するシステムによって使用されるメモリおよび／またはディスクスペースの量に上限を効果的に課してもよい。図61は、本発明の実施形態による、致命的故障状態を使用してジャーナリングサービスを操作するための例示的な過程6100である。過程6100は、ステップ6110から始まる。ステップ6110において、ジャーナリングサービスが、最大失敗数を確立する。いくつかの実施形態では、この最大失敗数は、シェア場所が致命的故障状態であるものとして印付けられる前に、ジャーナリングサービスが、そのシェア場所と関連付けられるジャーナリング待ち行列に記録することが許可される事前構成された数の失敗した動作である。次いで、過程6100は、ステップ6120へと進む。ステップ6120において、ジャーナリングサービスは、各シェア場所に対する失敗した動作の数を監視する。いくつかの実施形態では、この監視は、ジャーナリングサービスが、各シェア場所に対するジャーナリング待ち行列に記憶された失敗した動作の数の集計を維持することを含んでもよい。次いで、過程6100は、ステップ6130へと進む。

【0518】

ステップ6130において、ジャーナリングサービスは、最大失敗数が特定のシェア場所について超えているか否かを決定してもよい。いくつかの実施形態では、ジャーナリングサービスは、特定のシェア場所と関連付けられるジャーナリング待ち行列に記憶された失敗したデータ記憶動作の数の集計を、最大失敗数と比較することによってこの決定を行ってもよい。最大失敗数が超えている場合、過程6100は、ステップ6140へと進む。いくつかの実施形態では、最大失敗数が特定のシェア場所について超えている場合、ジャーナリングサービスは、そのシェア場所を致命的故障状態であるものとして印付けてもよい。いくつかの実施形態では、シェア場所が致命的故障状態であるという表示は、ジャ

ジャーナリングサービスの中心となるメモリまたはディスクに維持された任意の好適なデータフラグに、またはデータシェア自体の上で記憶されてもよい。

【0519】

ステップ6140において、ジャーナリングサービスは、致命的故障状態であるシェア場所と関連付けられるジャーナリング待ち行列に記憶された任意の失敗したデータ記憶動作を破棄してもよい。いくつかの実施形態では、ジャーナリングサービスは、致命的故障状態であるシェア場所と関連付けられるジャーナリング待ち行列を消去することによって、これらの失敗した動作を破棄してもよい。代替として、ジャーナリングサービスは、致命的故障状態であるシェア場所と関連付けられるジャーナリング待ち行列全体を削除してもよい。加えて、ステップ6140において、ジャーナリングサービスは、致命的故障状態であるシェア場所と関連付けられる失敗した動作を記録につけることを止めてもよい。例えば、ジャーナリングサービスは、致命的故障状態であるシェア場所と関連付けられるジャーナリング待ち行列をもはや更新しなくてもよい。過程6100は、ステップ6150へと進む。

10

【0520】

ステップ6150において、ジャーナリングサービスは、致命的故障状態であるシェア場所を再構築してもよい。いくつかの実施形態では、セキュアなデータパーサの修復機能が、シェア場所を再構築するために使用されてもよい。例えば、致命的故障状態であるシェア場所に記憶されたデータは、任意の好適な情報分散アルゴリズムを使用して任意の数のデータシェアに分割された元のデータと関連付けられてもよい。これらのデータシェアのそれぞれは、公衆または私的クラウド、リムーバブル記憶デバイス、あるいは大容量記憶デバイスの任意の好適な組み合わせ等の、2つ以上のシェア場所に記憶されてもよい。セキュアなパーサが、オンラインである（言い換えれば、致命的故障状態ではない）他のシェア場所のうちの少なくとも1つから、このデータを復旧することができる限り、次いで、セキュアなデータパーサは、シェア場所を再構築してもよい。いくつかの実施形態では、シェア場所は、最初から再構築されてもよい。例えば、シェア場所において修復される全てのファイルは、再構築過程が最初にシェア場所において実行される前に除去されてもよい。いくつかの実施形態では、再構築過程がシェア場所において実行されるために、シェア場所に読み出しおよび書き込みする管理許可が必要とされてもよい。

20

【0521】

図62に関して以下で説明されるように、いくつかの実施形態では、再構築される過程にあるシェア場所は、「重要再構築状態」であるものとして印付けられてもよい。この重要再構築状態は、ある失敗した動作が記録につけられるべきであることを、ジャーナリングサービスに示してもよい。これらの動作は、ファイルレベル、ブロックレベル、ビットレベル、または任意の好適なファイル粒度のレベルであってもよい。いくつかの実施形態では、ステップ6150は随意的であってもよい。次いで、過程6100は、ステップ6160へと進む。ステップ6160において、ジャーナリングサービスは、ステップ6150において再構築されたシェア場所に対するジャーナリング待ち行列を維持することを再開してもよい。いくつかの実施形態では、ステップ6150は随意的であってもよい。次いで、過程6100は終了してもよい。

30

40

【0522】

特定のシェア場所に対する最大失敗数が超えられていないことをステップ6130においてジャーナリングサービスが決定した場合、過程6100は、ステップ6170へと進んでもよい。ステップ6170において、ジャーナリングサービスは、特定のシェア場所に対する失敗した動作を記録し続けてもよい。次いで、過程6100は終了する。

【0523】

いくつかの実施形態では、過程6100は、シェア場所が突発的故障状態であるか否かを決定するために、ステップ6110、6120、および6130において、最大失敗数に加えて最大タイムアウトを使用してもよい。いくつかの実施形態では、最大タイムアウトは、シェア場所が突発的故障状態であるものとして印付けられる前に、特定のシェア場

50

所がオフラインのままになることができる事前構成された時間量であってもよい。突発的故障状態は、シェアが修復されるか、または修復される過程にあるまで、シェアに対する全ての読み出しおよび書き込み動作が拒絶されるべきであることを、ジャーナリングサービスに示してもよい。いくつかの実施形態では、シェアは、ステップ6150に関して説明される再構築過程に従って修復されてもよい。他の実施形態では、シェア場所は、シェア場所を手動で修復することによって、ジャーナリングサービスの管理者によって修復されてもよい。例えば、ジャーナリングサービスの管理者は、シェア場所と関連付けられるデータ記憶設備を交換または再配置してもよい。

【0524】

いくつかの実施形態では、ジャーナリングサービスは、再構築される過程にあるシェア場所に対する重要再構築状態を記録につけてもよい。いくつかの実施形態では、ジャーナリングサービスは、再構築過程が始まるとすぐに、特定のシェア場所に対する重要再構築状態を記録してもよい。いくつかの実施形態では、この再構築過程は、図61のステップ6150に関して説明されるものと同様であってもよい。図62に関して以下で説明されるように、この重要再構築状態は、再構築されているシェア場所においてすでに修復されているファイルに対する失敗した動作を記録するべきであることを、ジャーナリングサービスに示してもよい。

【0525】

図62は、本発明の実施形態による、重要再構築状態を使用してジャーナリングサービスを操作するための例示的な過程6200である。過程6200は、ファイルレベルで動作するものとして説明されているが、ジャーナリングサービスは、ブロックレベルまたはビットレベル等の任意の好適な粒度のレベルにおいて、過程6200を実行してもよいことが認識されるであろう。過程6200は、ステップ6210から始まる。ステップ6210において、ジャーナリングサービスは、重要再構築状態であるシェア場所と関連付けられるファイルにデータ記憶動作を行う要求を受信する。いくつかの実施形態では、このデータ記憶動作は、ファイル上の読み出しまたは書き込み要求であってもよい。シェア場所が重要再構築状態であることに起因して、シェア場所に対する読み出しまたは書き込み要求が失敗する。例えば、ジャーナリングサービスは、スライドショープレゼンテーションを含有するファイルに書き込む要求を受信し得る。スライドショープレゼンテーションを含有するファイルと関連付けられるデータのシェアは、再構築され、重要再構築状態であるシェア場所、ならびにオンライン状態である3つの他のシェア場所に記憶されてもよい。ファイルに書き込む要求は、重要再構築状態であるシェア場所に関しては失敗するが、オンライン状態にあるシェア場所に関しては成功する。過程6200は、ステップ6220へと進む。

【0526】

ステップ6220において、ジャーナリングサービスは、ファイルが重要再構築状態であるシェア場所に存在するか否かを決定する。いくつかの実施形態では、ジャーナリングサービスは、重要再構築状態にあるシェア場所において既に修復されているファイルのリストを維持してもよい。データ記憶動作と関連付けられるファイルがリスト上にある場合、ジャーナリングサービスは、ファイルがシェア場所に存在すると決定し得る。次いで、過程6200は、ステップ6240へと進む。ステップ6240において、ジャーナリングサービスは、ステップ6210において失敗した読み出しまたは書き込み要求等のデータ記憶動作を記録する。いくつかの実施形態では、この失敗した動作は、図59の過程5900に関して説明されるものと同様に、ジャーナリング待ち行列に記憶されてもよい。次いで、過程6200は、ステップ6250へと進む。ステップ6250において、ジャーナリングサービスは、いったん再構築過程が完了すると、失敗した動作を再生する。いくつかの実施形態では、ジャーナリングサービスは、シェア場所と関連付けられるファイルの全てが修復されたときに、再構築過程がシェア場所に関して完了したことを知らされてもよい。シェア場所と関連付けられる全てのファイルが修復されたときに、シェア場所は、データ記憶動作に利用可能であるものとして印付けられてもよい（すなわち、オンラ

10

20

30

40

50

イン状態である)。このようにして、重要再構築状態は、ファイルシステムの中の1つ以上のシェア場所が再構築されている間に、ジャーナリングサービスがファイルシステムの健全を維持し続けることを可能にする。次いで、過程6200は終了する。

【0527】

ステップ6210において動作を実行する要求からのファイルが再構築されているシェア場所に存在しない（すなわち、まだ修復されていない）ことを、ジャーナリングサービスがステップ6220で決定した場合、過程6200は、ステップ6230へと進む。ステップ6230において、ステップ6210で失敗した動作が、ジャーナリングサービスによって破棄される。いくつかの実施形態では、ジャーナリングサービスは、これらの失敗した動作を、重要再構築状態にあるシェア場所と関連付けられるジャーナリング待ち行列に書き込まないことによって、これらを破棄してもよい。そのような実施形態では、ジャーナリングサービスは、ジャーナリングサービスと関連付けられる他のデータ記憶に関して成功しているファイルへの動作に依存してもよい。例えば、スライドショープレゼンテーションを含有するファイルへの更新は重要再構築状態にあり、スライドショープレゼンテーションを含有するファイルをまだ修復していないシェア場所に関して破棄されてもよい。しかしながら、更新動作は、オンライン状態であり、ファイルを含有する3つの他のシェア場所に関して成功してもよい。次いで、過程6200は終了する。

【0528】

セキュアなデータパーサのいくつかの用途が上記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。

【0529】

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】

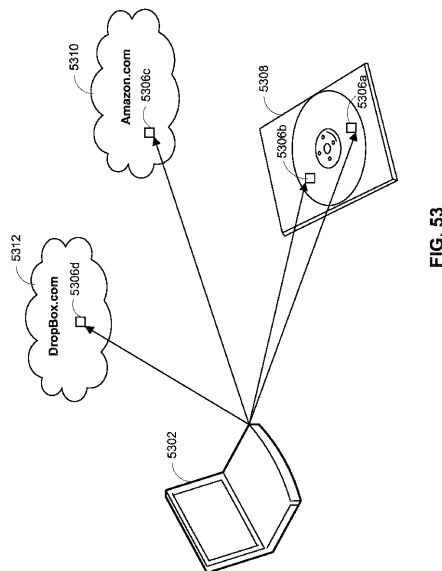


FIG. 53

【図 1】

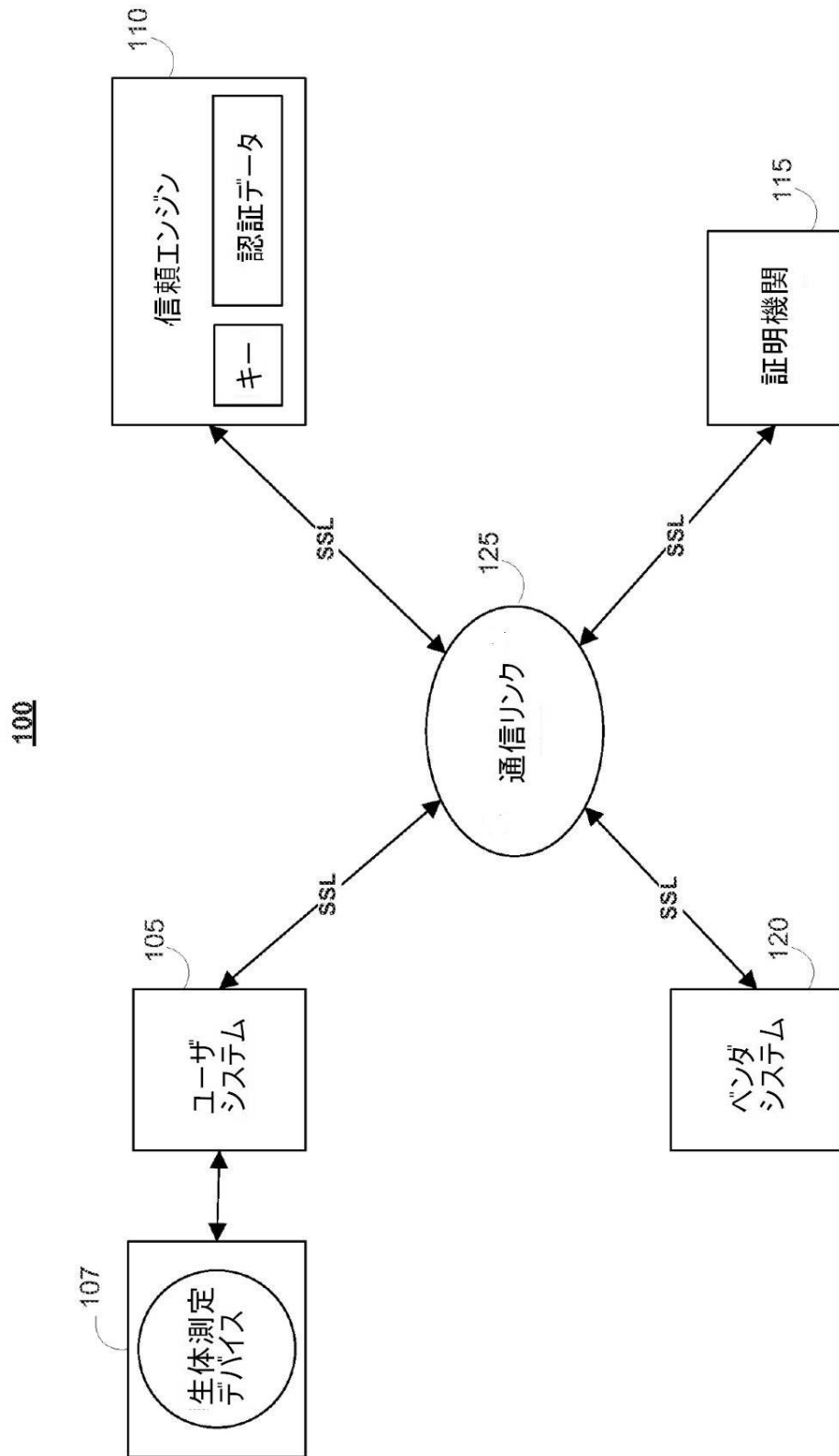


FIG. 1

【図 2】

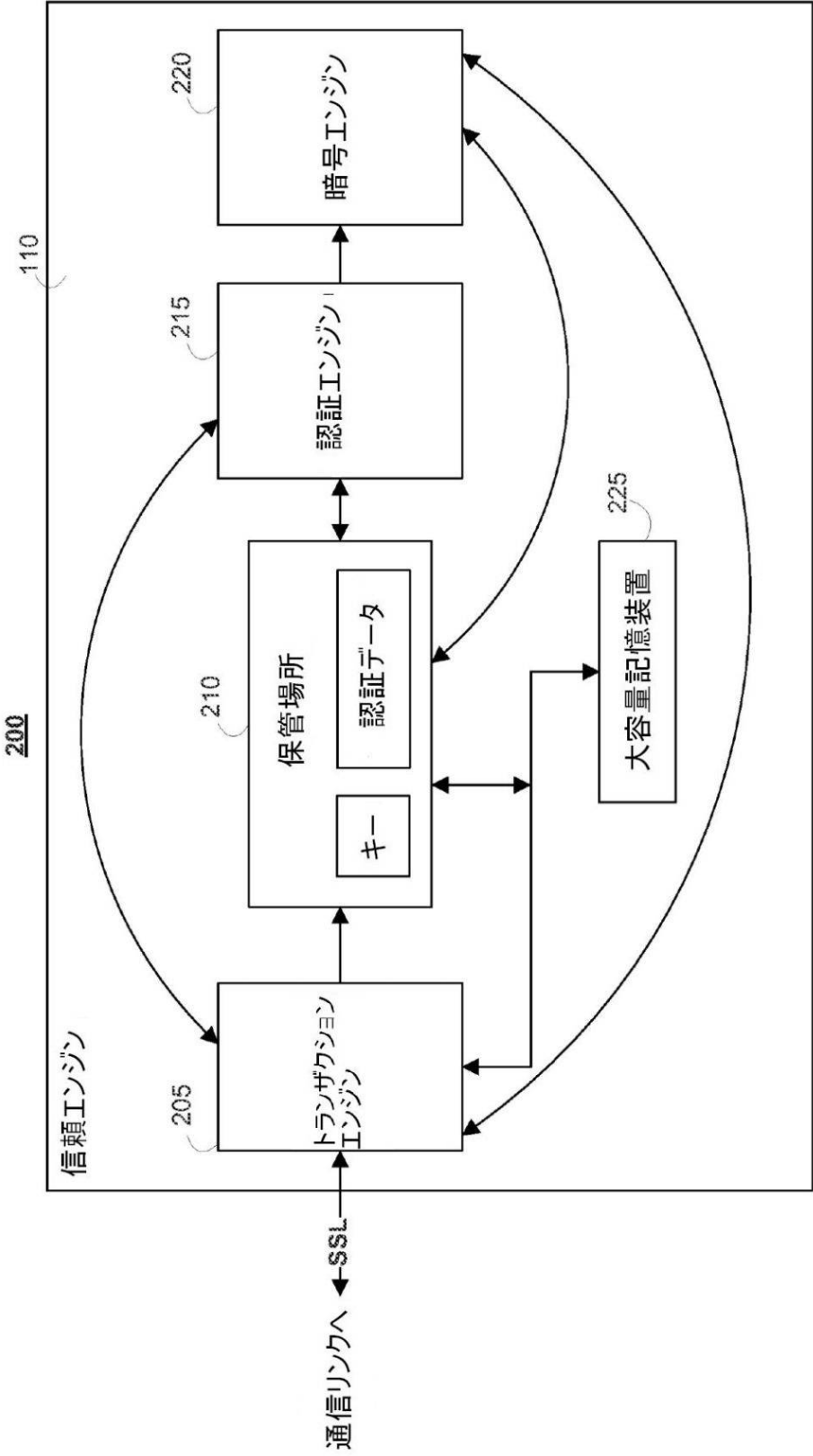


FIG. 2

【図 3】

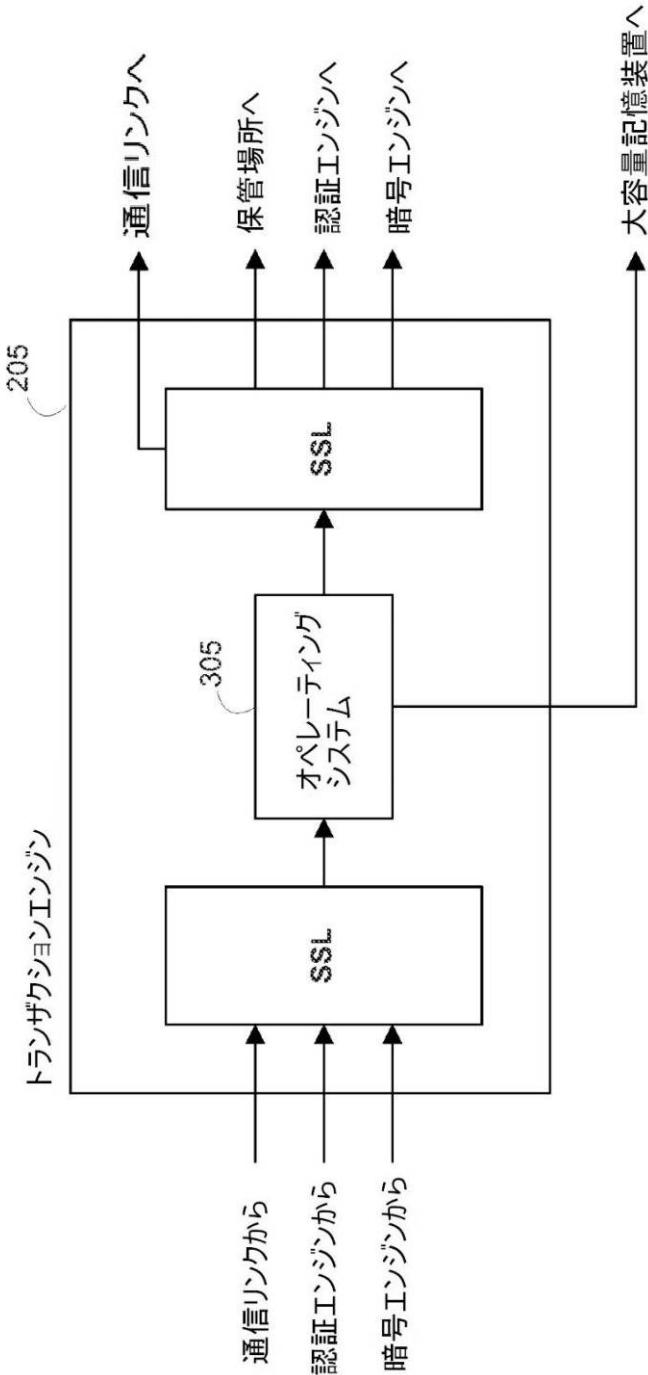


FIG. 3

【図 4】

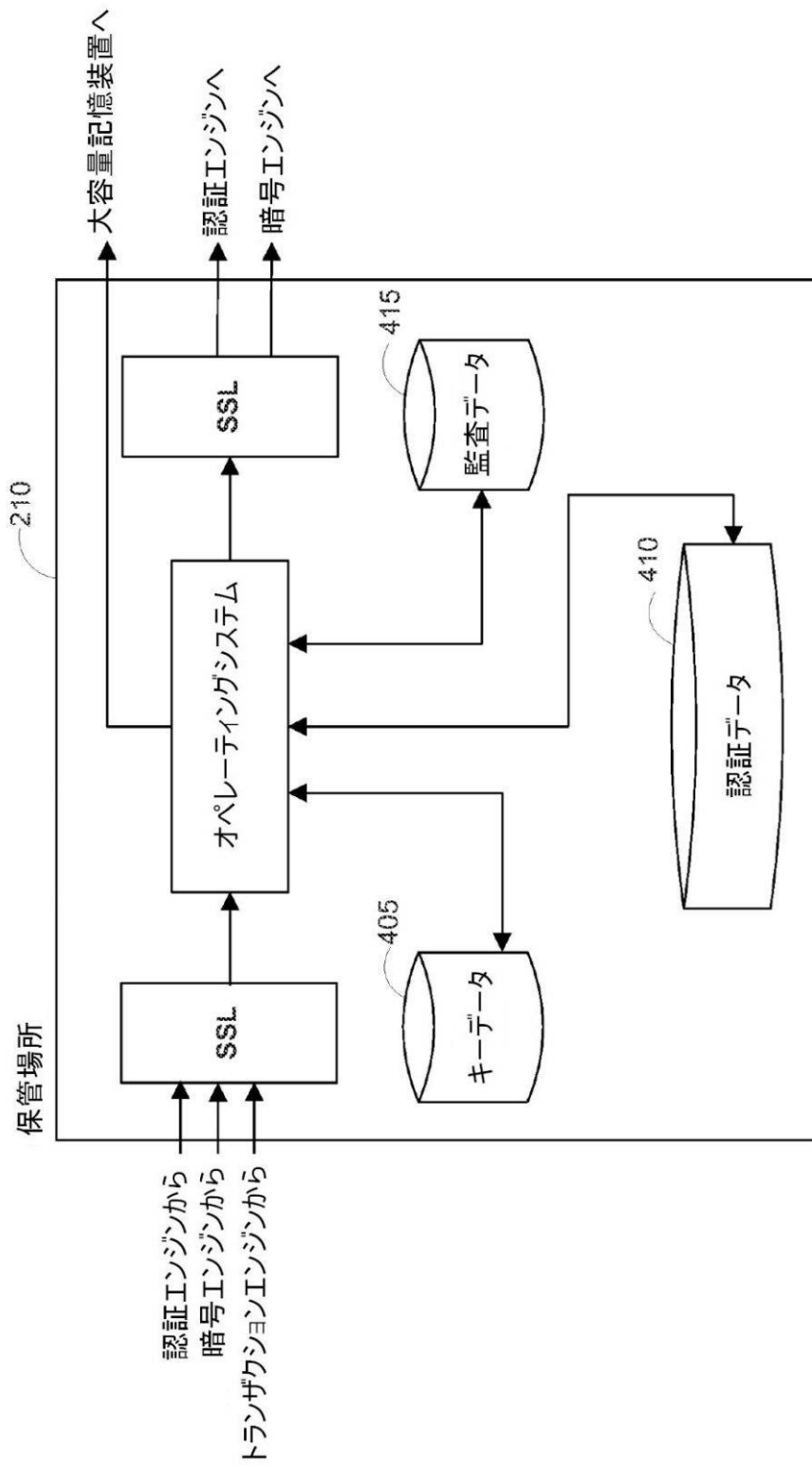


FIG. 4

【図 5】

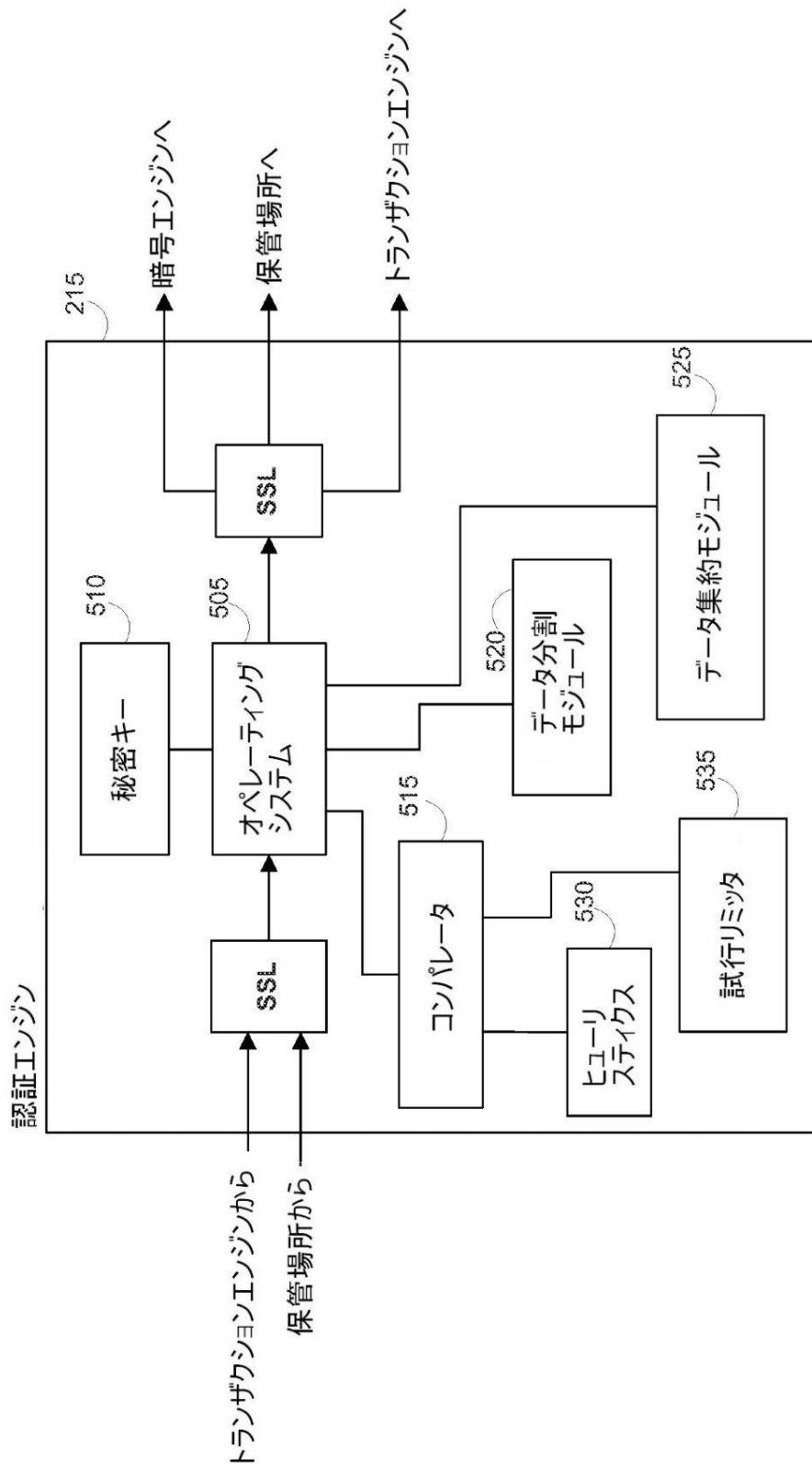


FIG. 5

【図 6】

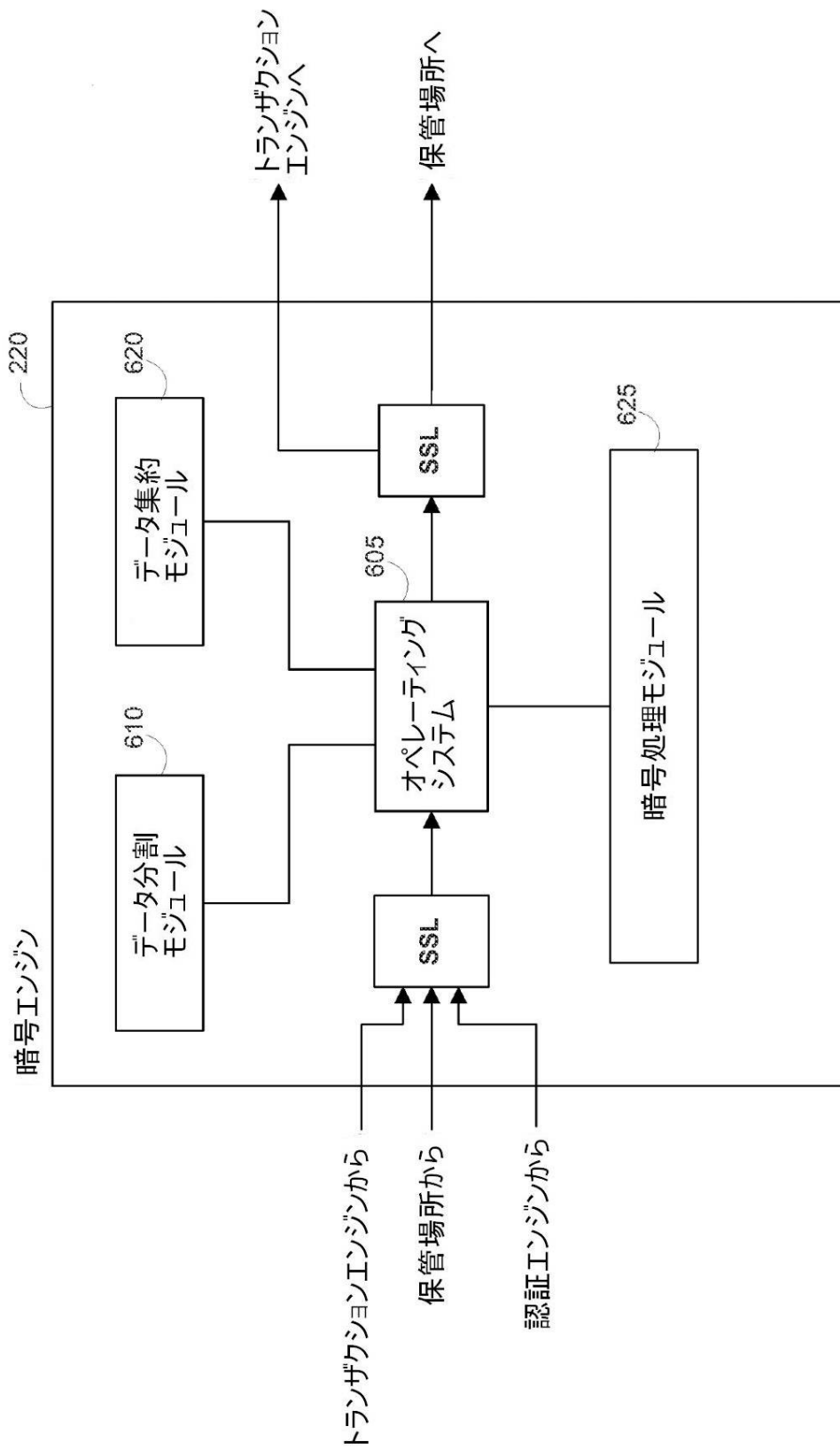


FIG. 6

【図 7】

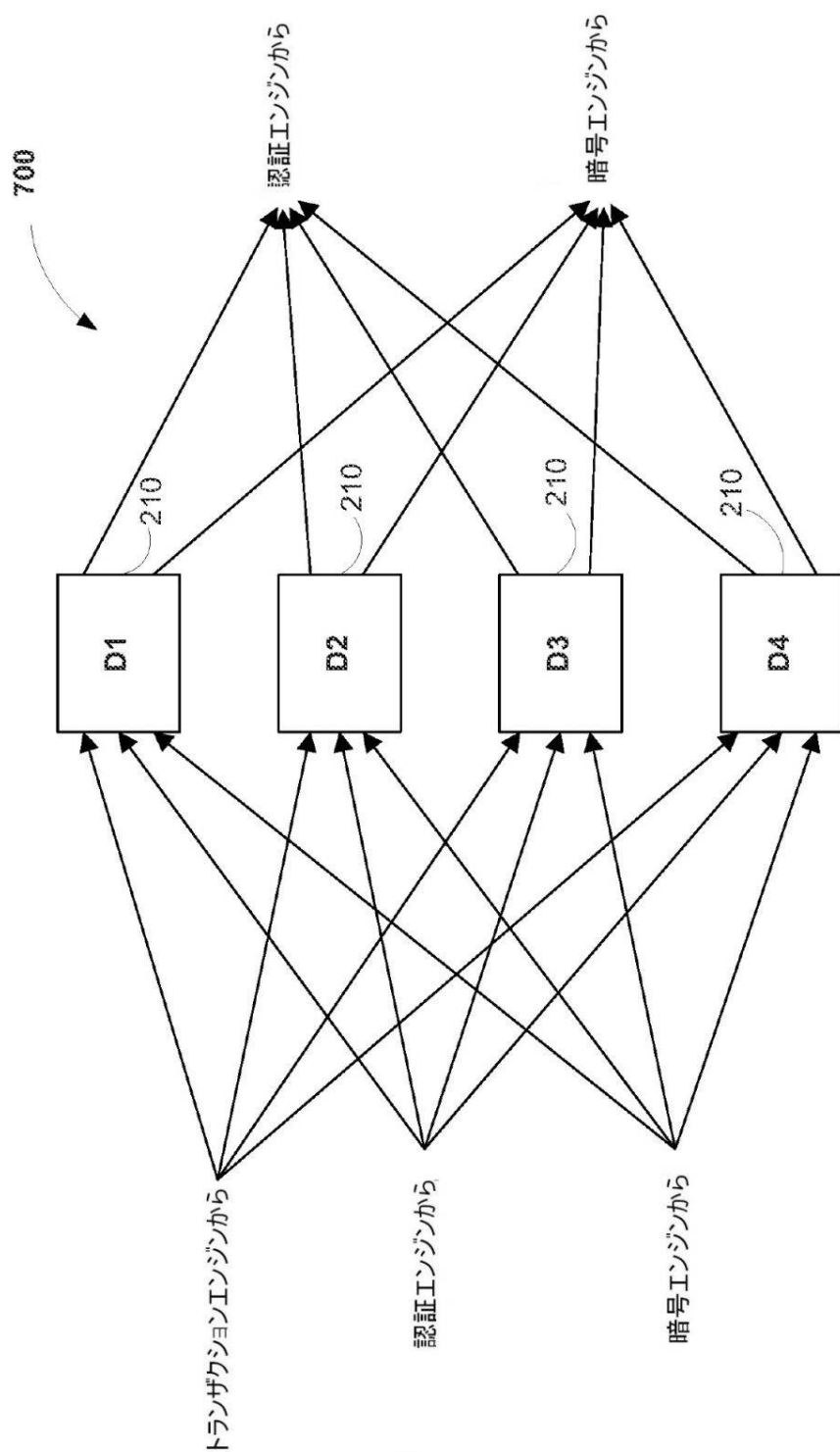


FIG. 7

【図 8】

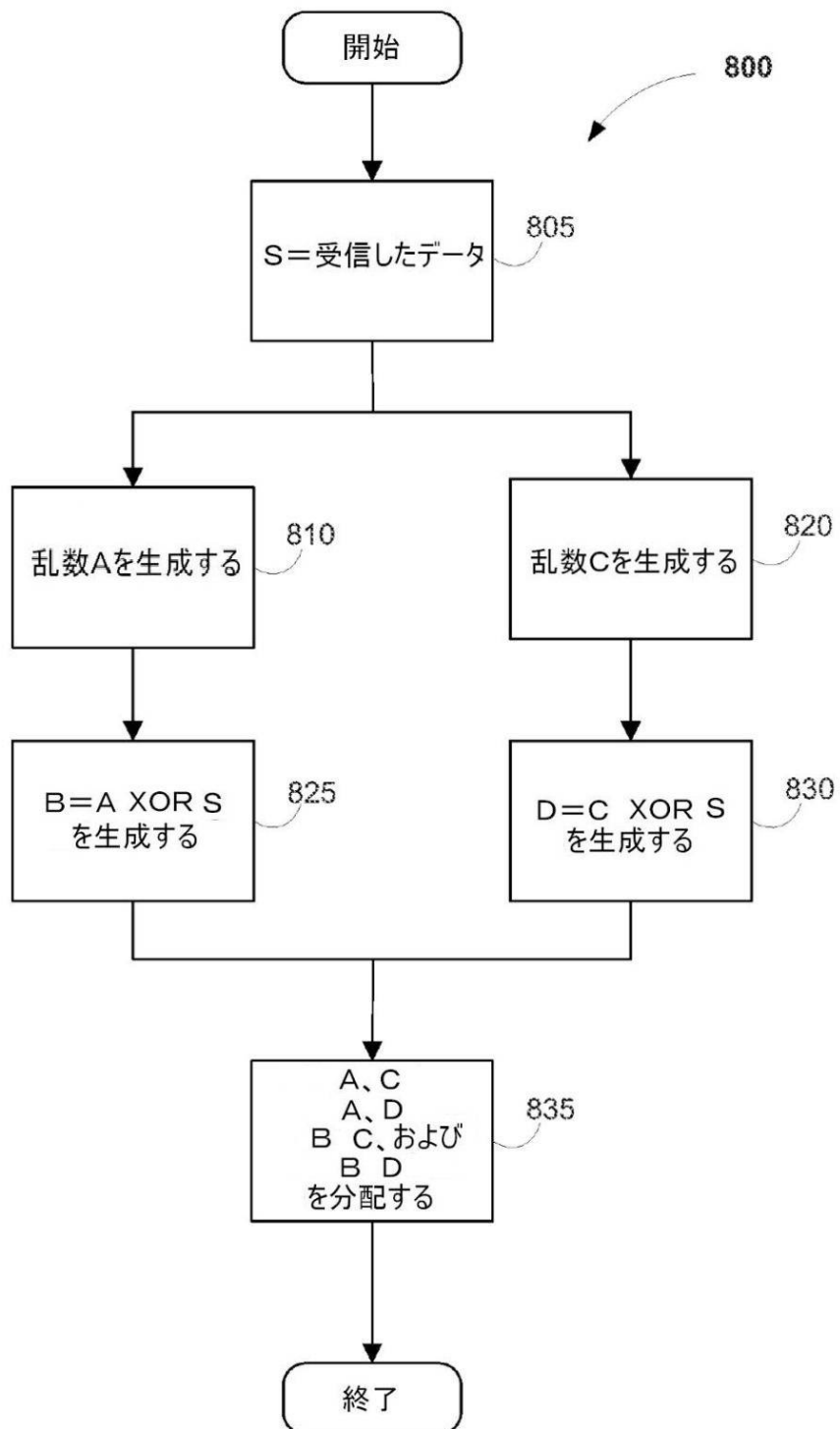


FIG. 8

【図 9 A】

900



登録データフロー			
送信	受信	SSL	動作
ユーザ	トランザクション エンジン(TE)	1/2	(PUB_AE(UID, B))として、認証 エンジン(AE)を用いて暗号化された 登録認証データ(B)およびユーザID (UID)を伝送する
TE	AE	完全	伝送を転送する
			AEが転送データを復号および分割する
AE	X番目の 保管場所(DX)	完全	データの各部分を記憶する
デジタル証明書が要求されたとき			
AE	暗号エンジン (CE)	完全	キー生成を要求する
			CEがキーを生成および分割する
CE	TE	完全	デジタル証明書の要求を伝送する
TE	認証機関(CA)	1/2	要求を伝送する
CA	TE	1/2	デジタル証明書を伝送する
TE	ユーザ	1/2	デジタル証明書を伝送する
TE	MS	完全	デジタル証明書を記憶する
CE	DX	完全	キーの各部分を記憶する

FIG. 9, パネル A

【図 9 B】

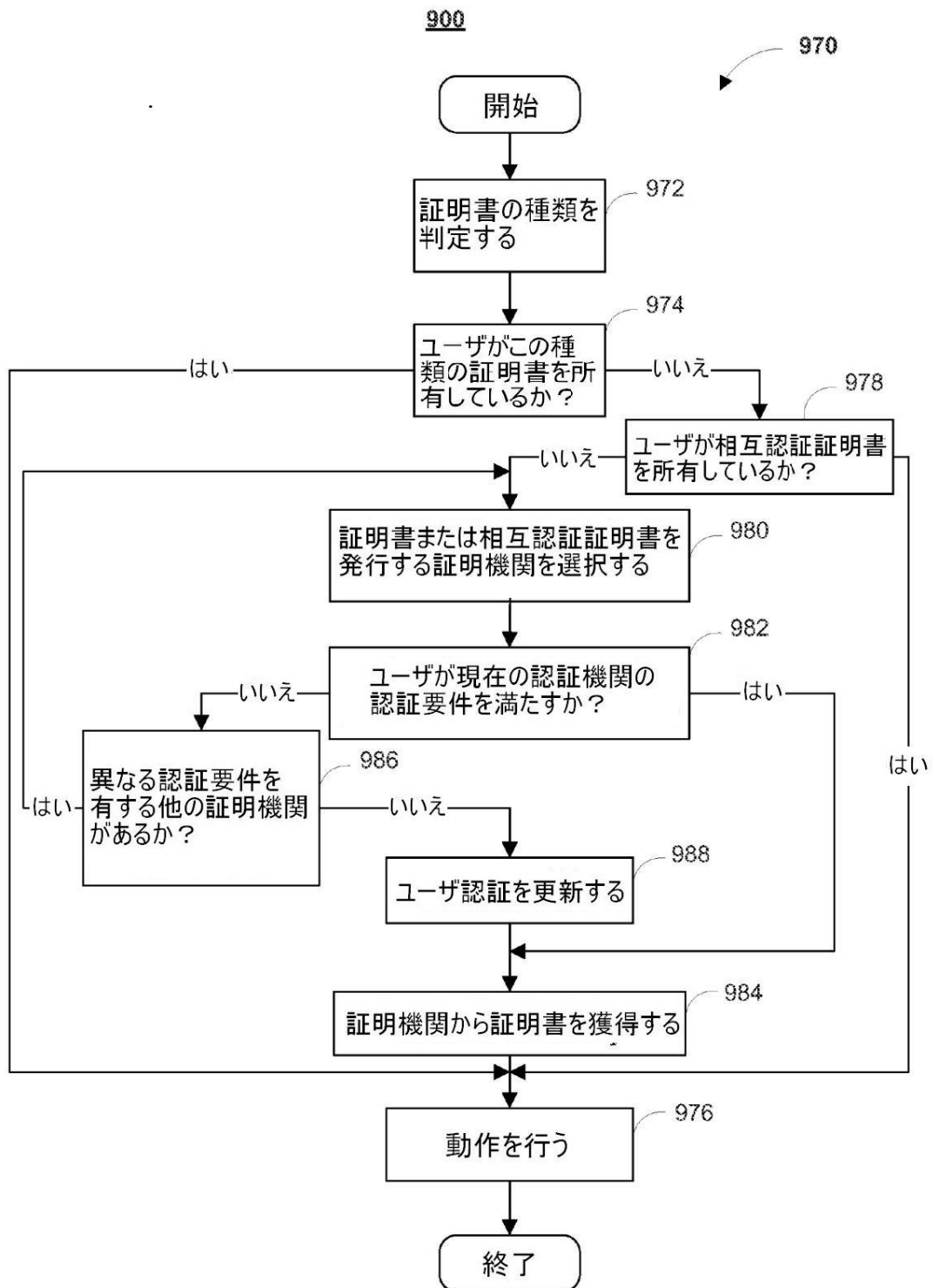


FIG. 9, パネル B

【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)を送送する
			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')を送送する
TE	AE	完全	転送を送送する
			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'))を送送する
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)を送送する
			元のベンダメッセージがAEに伝送される
TE	AE	完全	h(M)を送送する
1103			AEがBを収集し、B'と比較し、h(M)をh(M')と比較する
1105	AE	暗号エンジン(CE)	完全
1110	AE	DX	完全
1115	DX	CE	完全
1120			
1125	CE	AE	完全
1130	AE	TE	完全
1135	TE	ベンダ	完全
1140	TE	ユーザ	1/2

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 1205
AE	CE	完全	PUB__USER(SYNC)をCEに転送する 1210
AE	DX	完全	UID, TID 1215
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 1220
			CEが暗号キーを収集し、syncを復号する 1225
CE	AE	完全	TID、復号syncを含んでARに記入 1230
AE	TE	完全	TEに転送する
TE	要求APP／ベンダ	1/2	TID、はい／いいえ、Sync
暗号化			
要求APP／ベンダ	TE	1/2	ユーザの公開キーの要求 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】

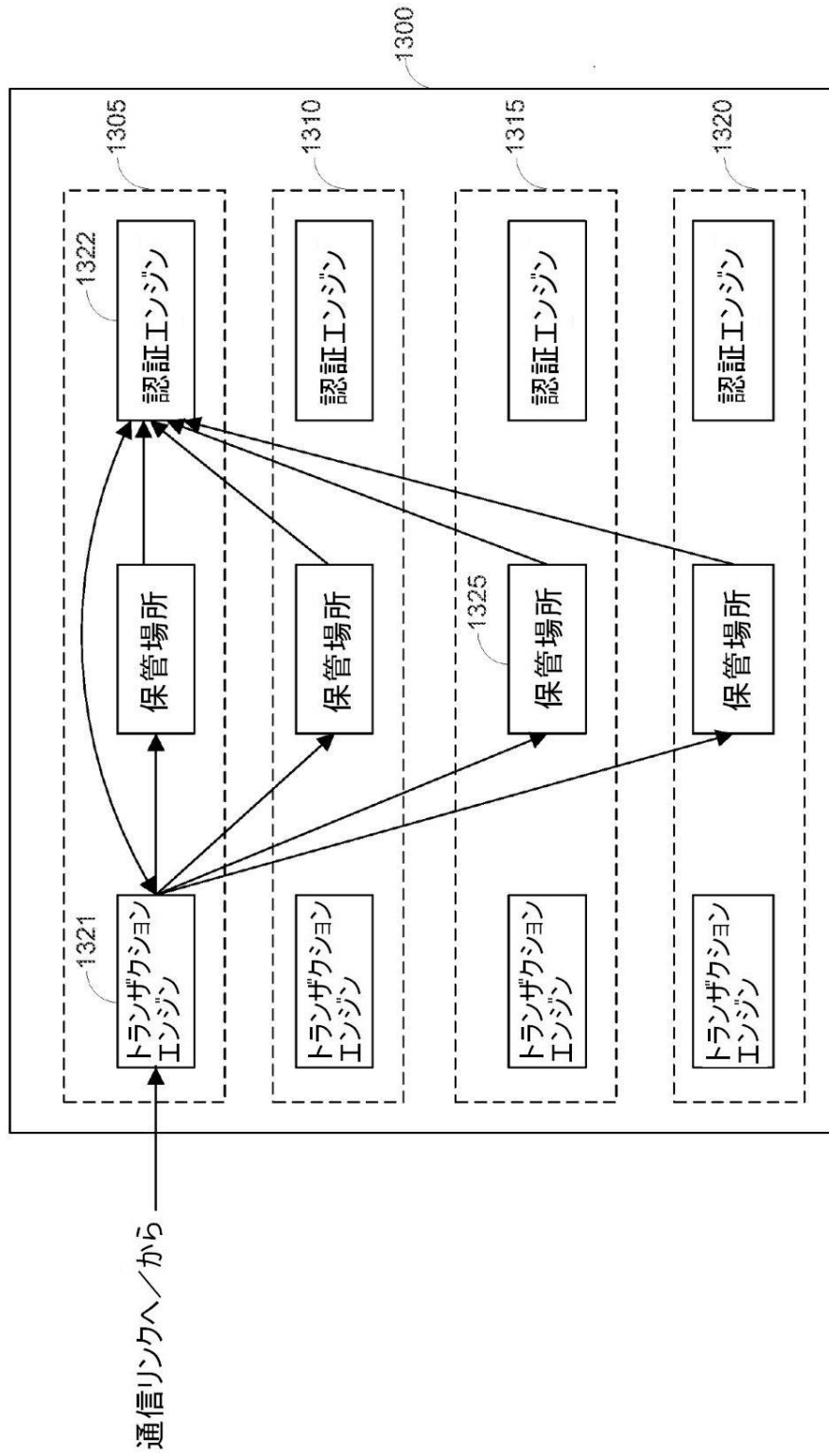


FIG. 13

【図 14】

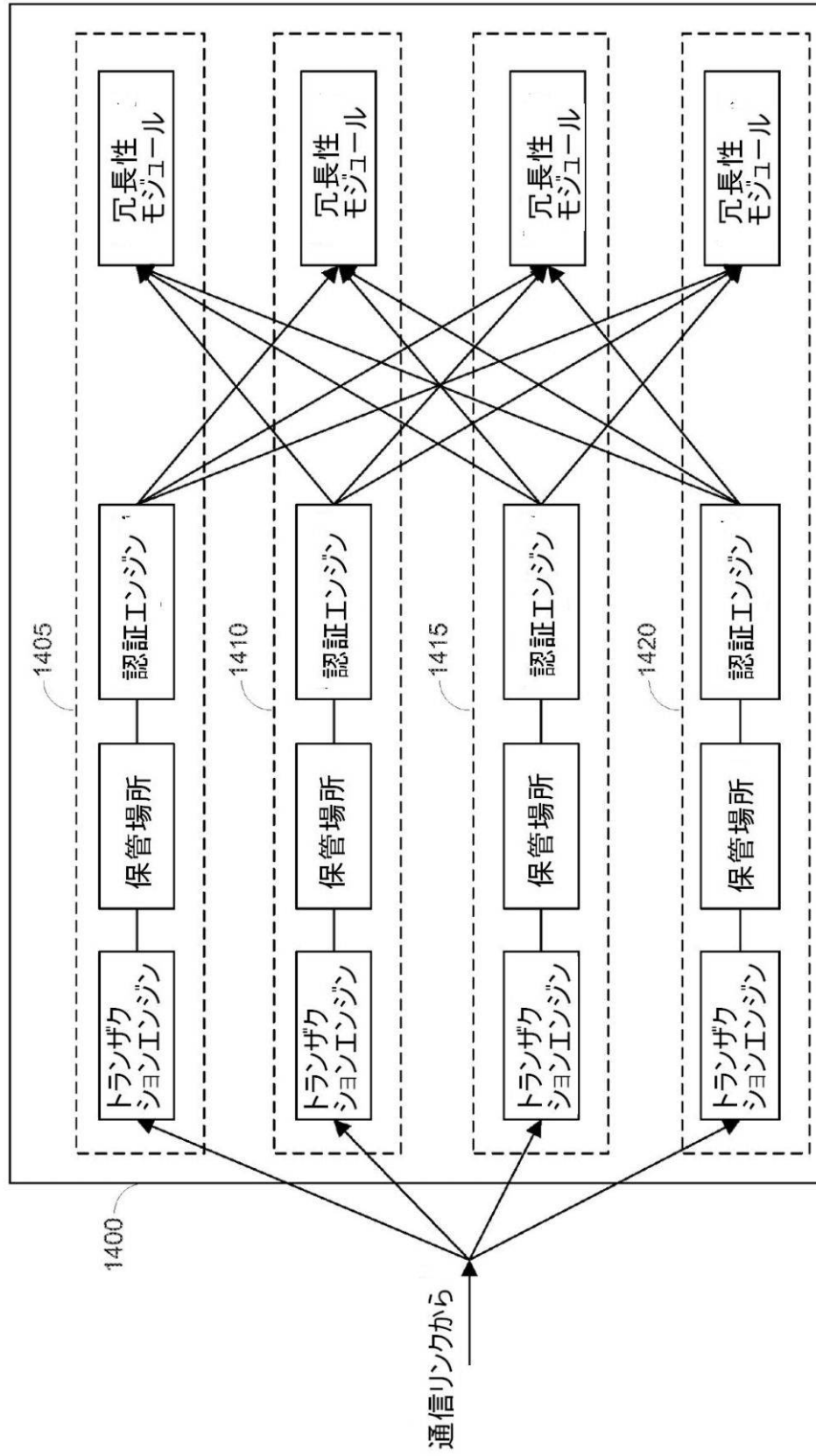


FIG. 14

【図 15】

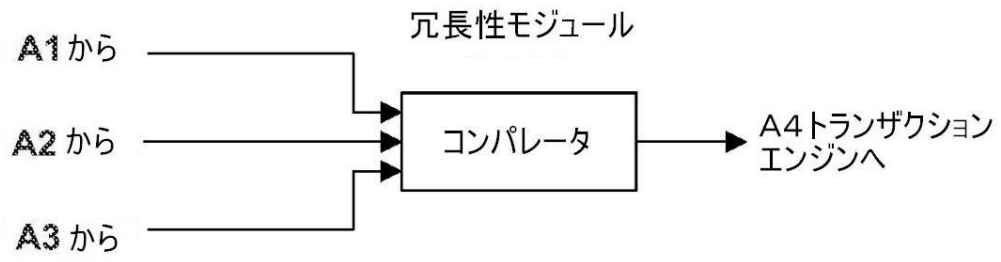


FIG. 15

【図 16】

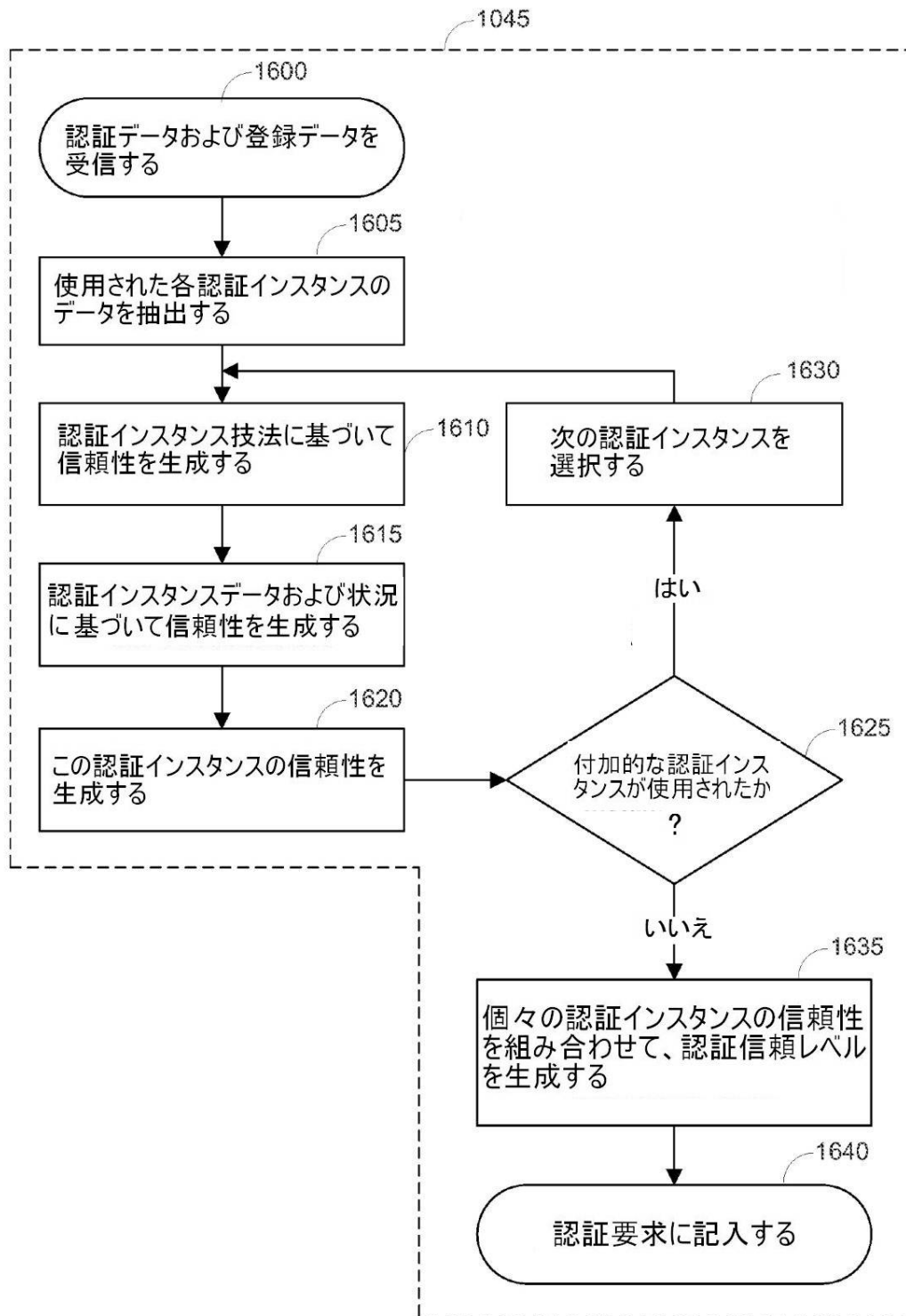


FIG. 16

【図 17】

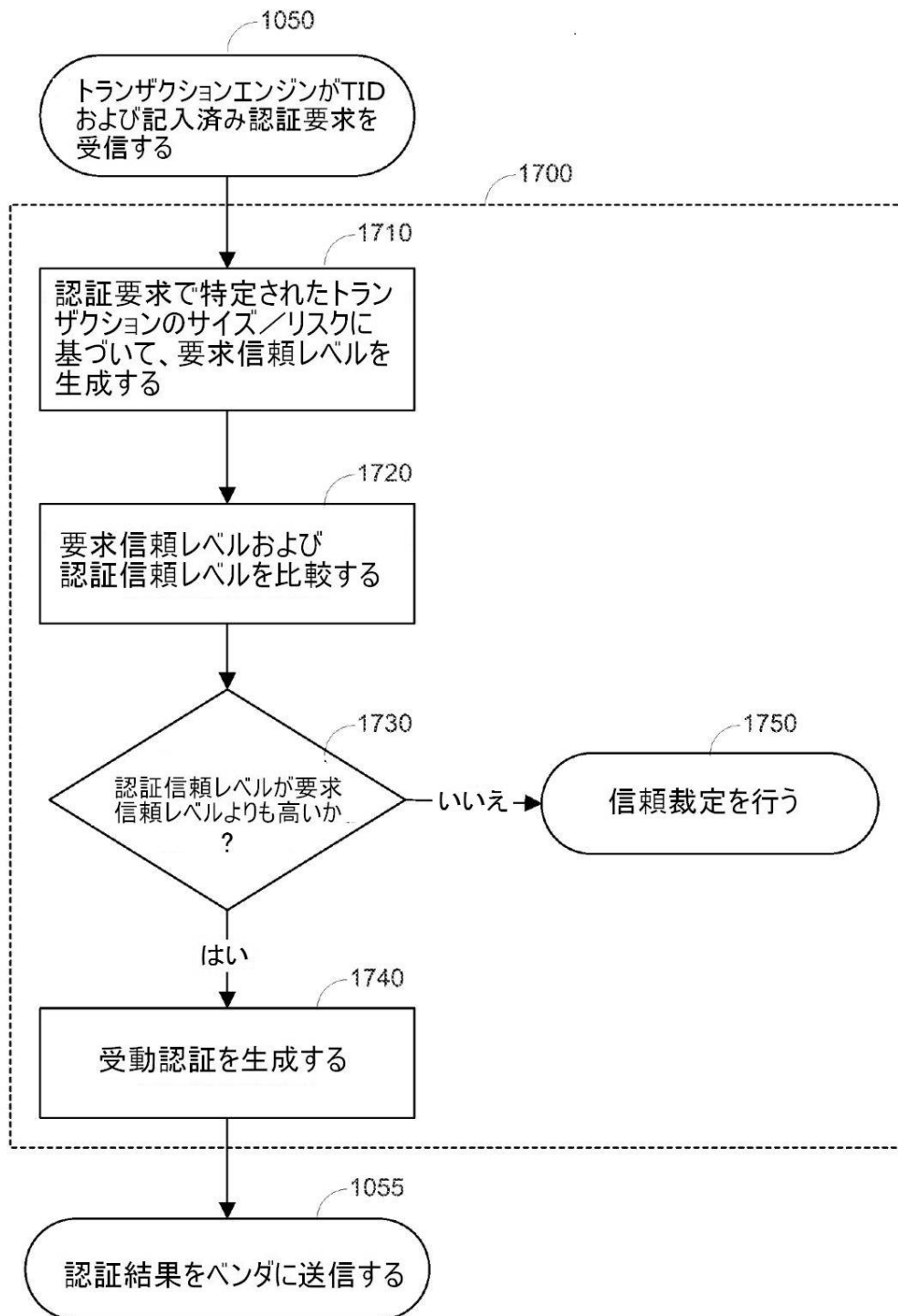


FIG. 17

【図 18】

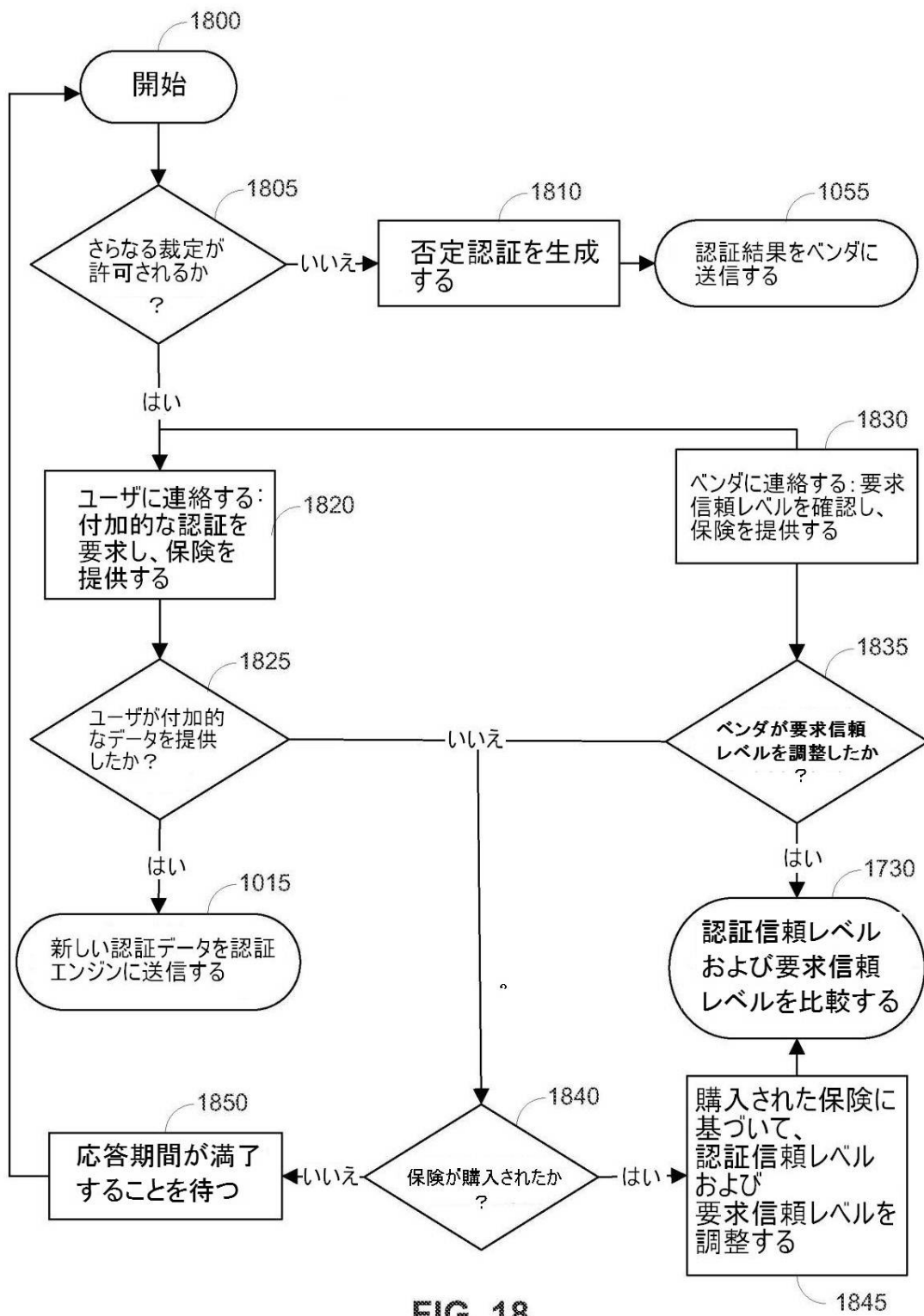


FIG. 18

【図 19】

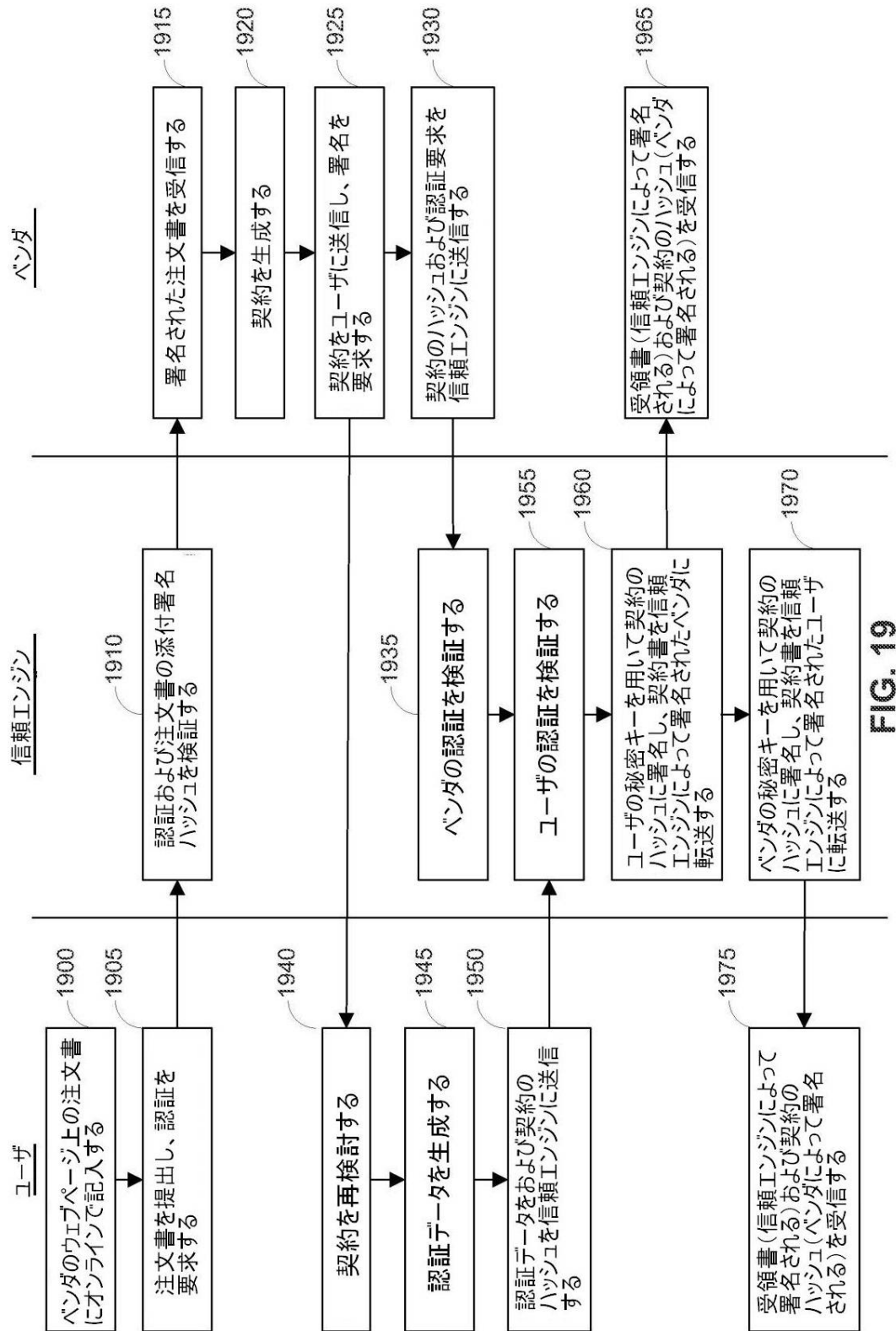


FIG. 19

【図 20】

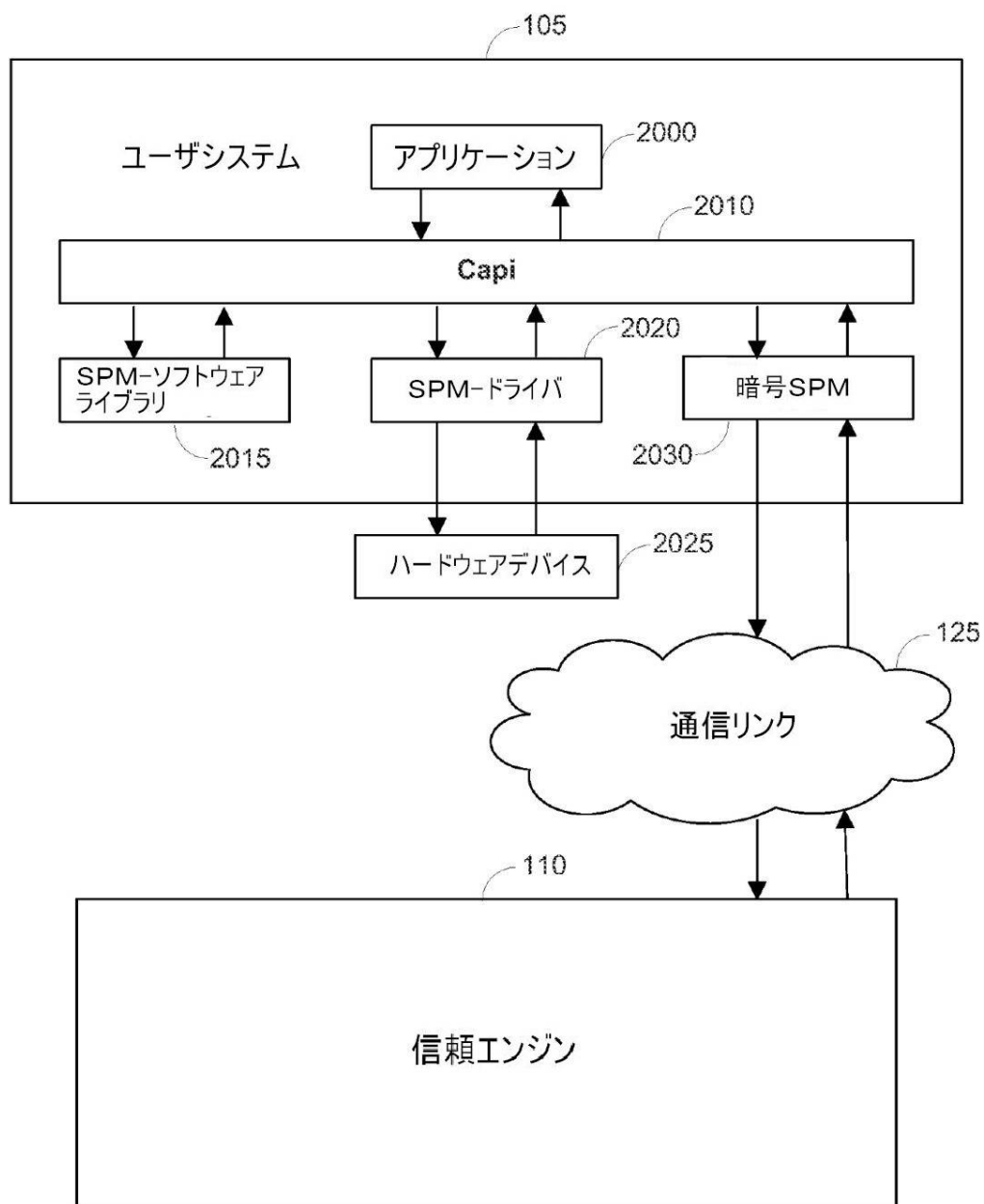


FIG. 20

【図 21】

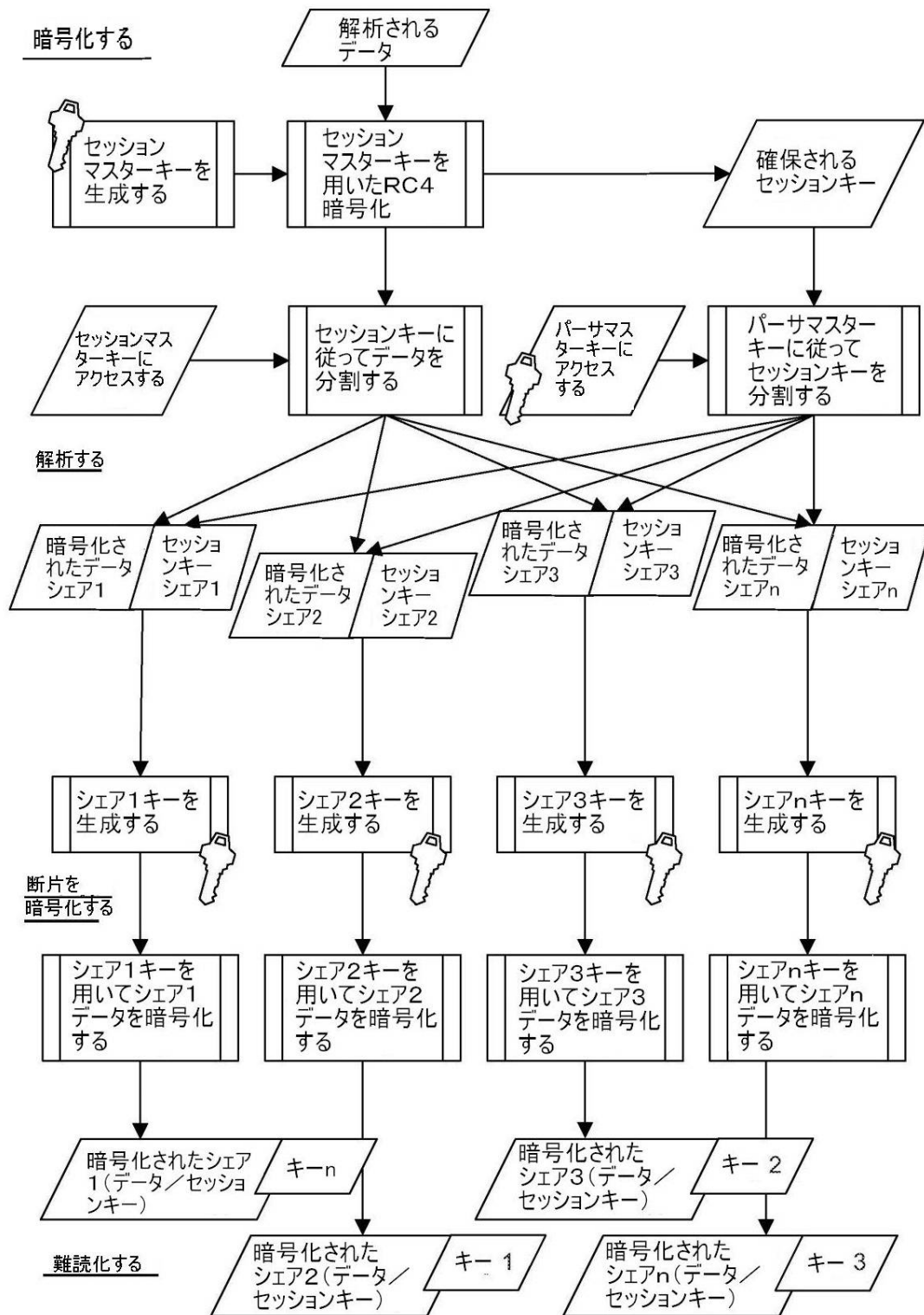


FIG. 21

【図 22】

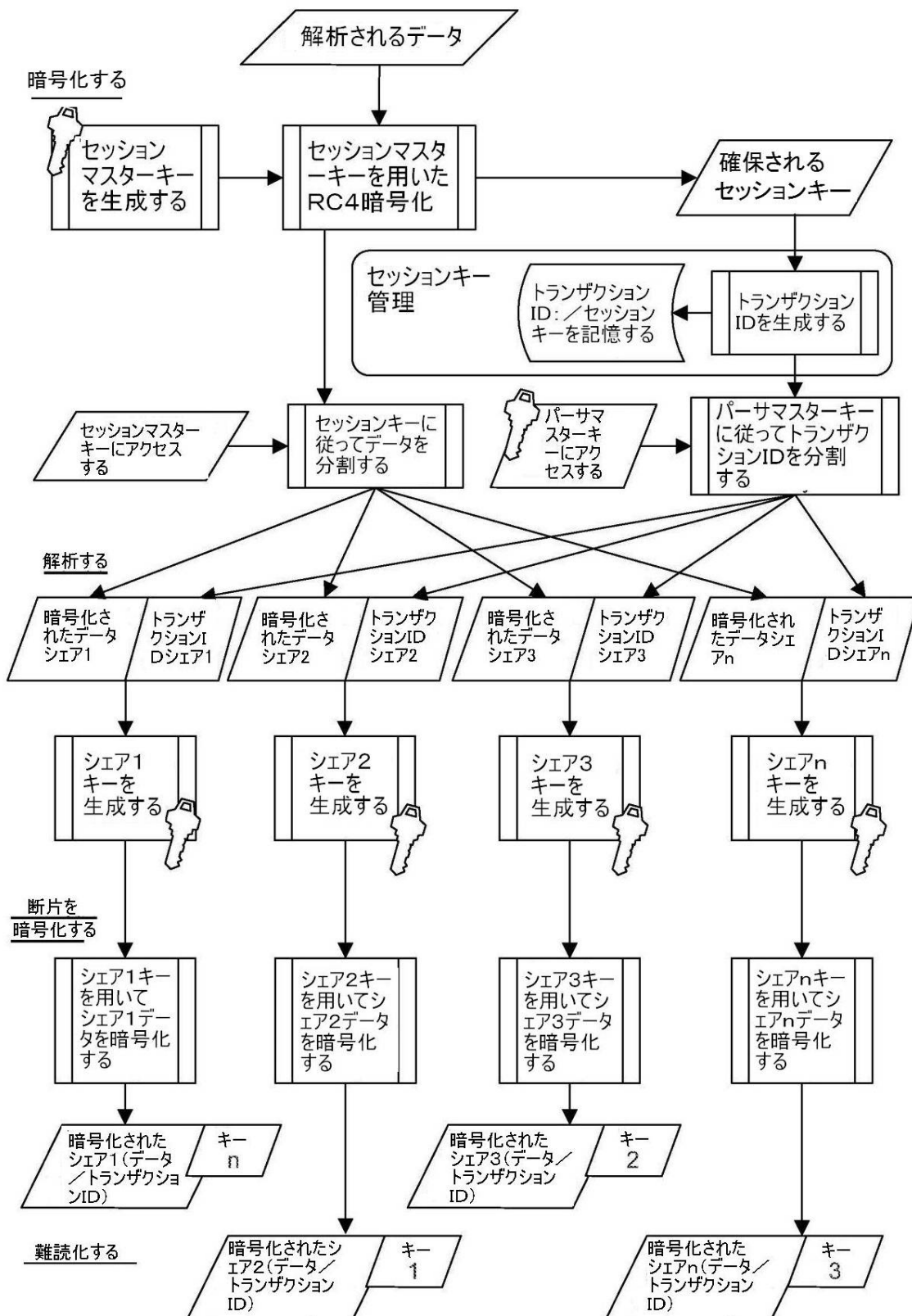


FIG. 22

【図 23】

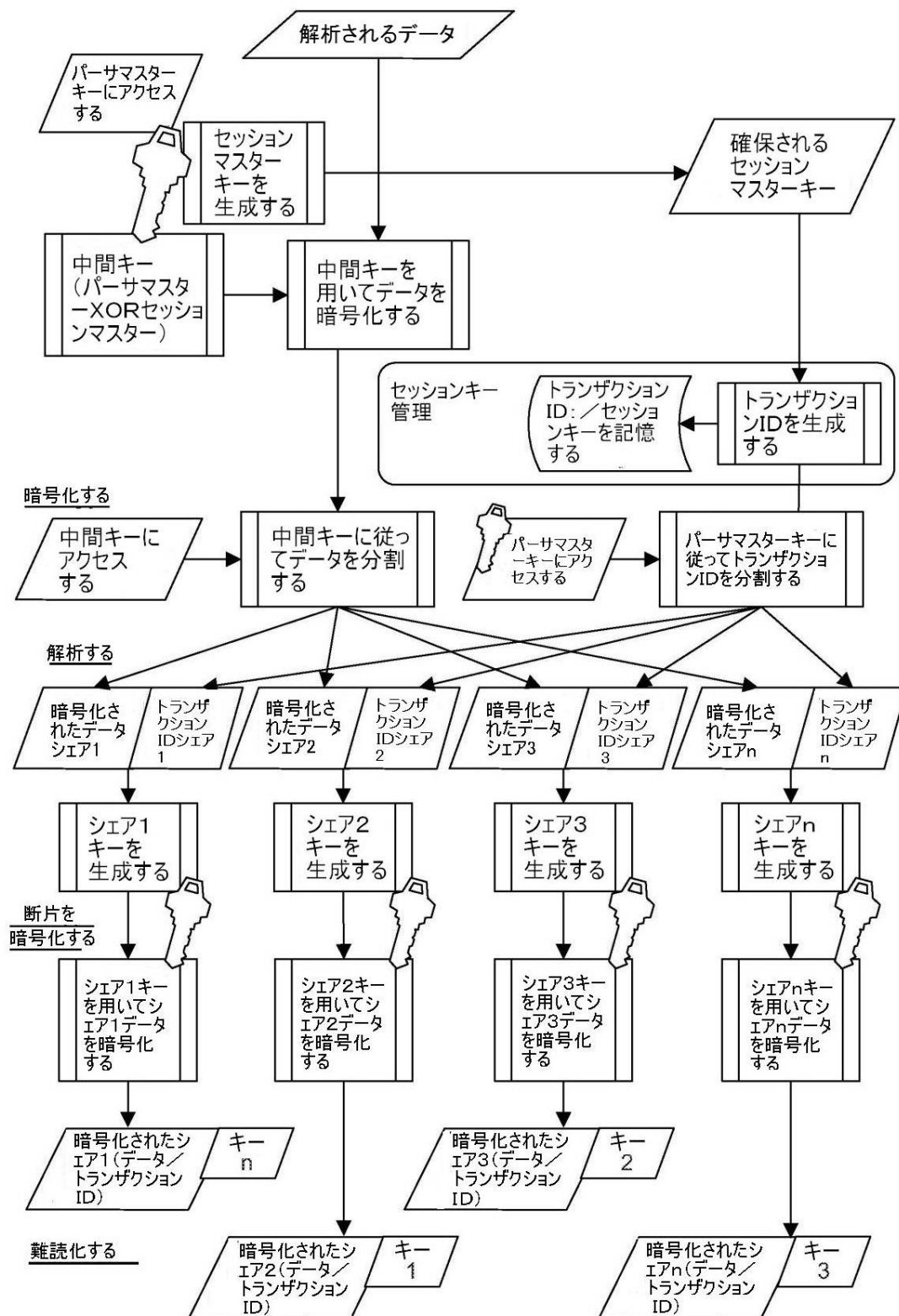


FIG. 23

【図 24】

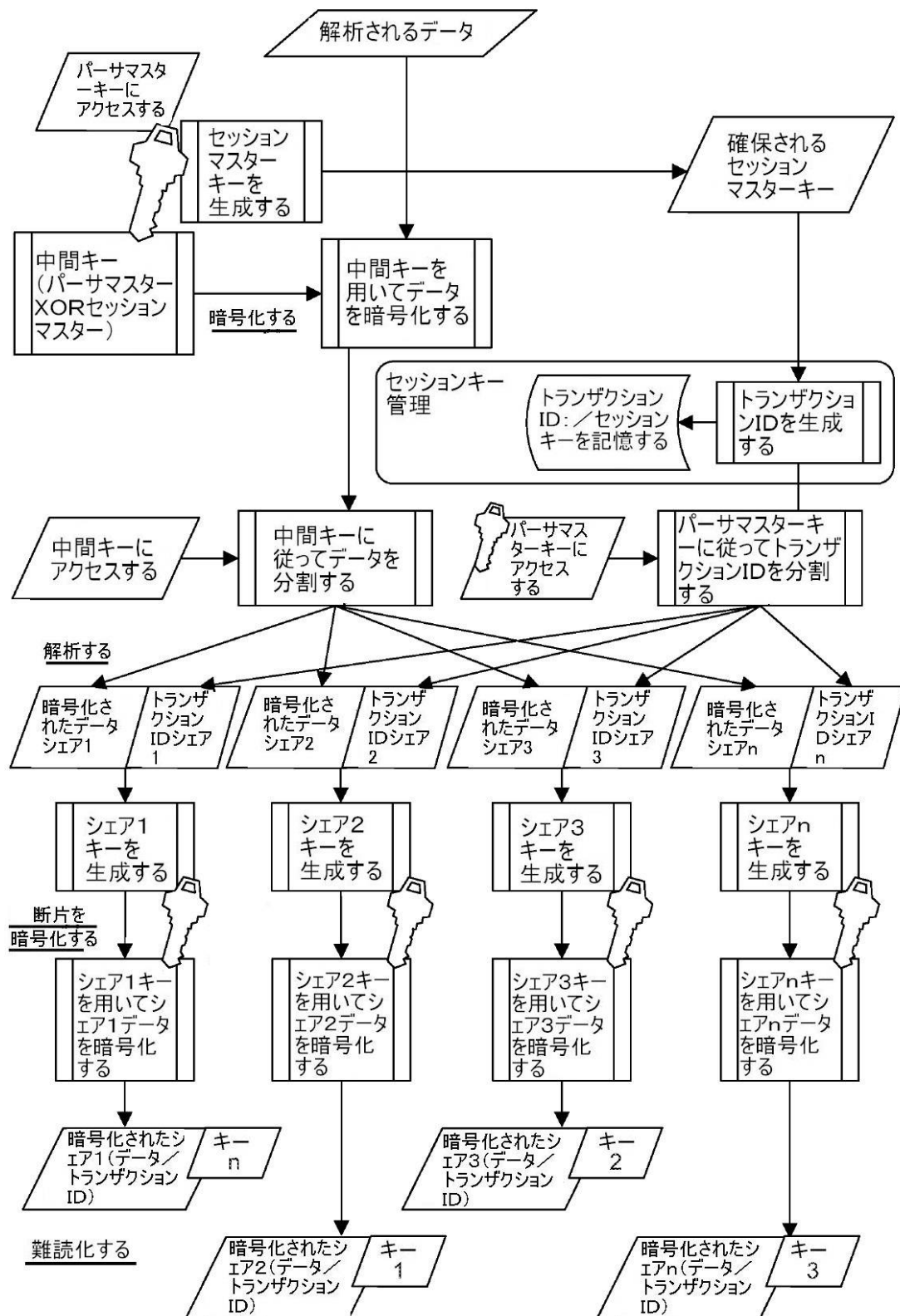


FIG. 24

【図 25】

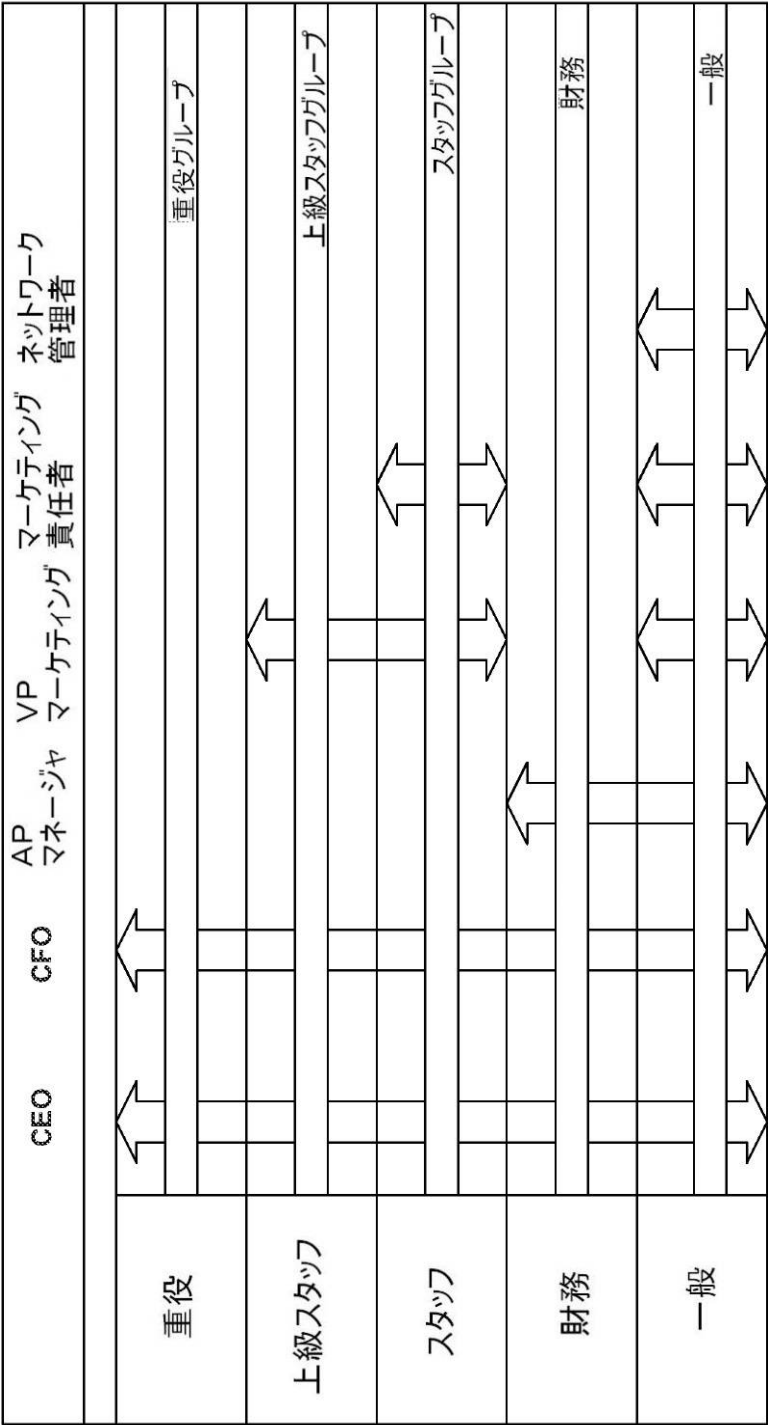


FIG. 25

【図 26】

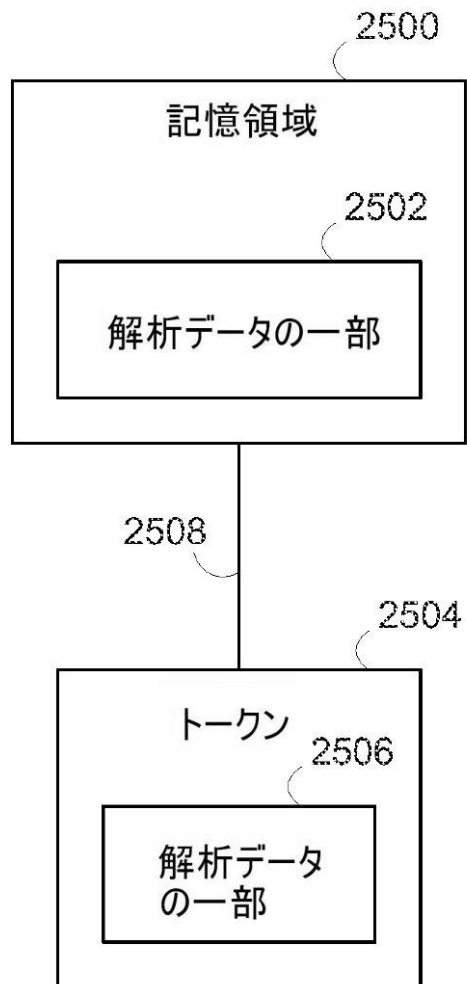


FIG. 26

【図 27】

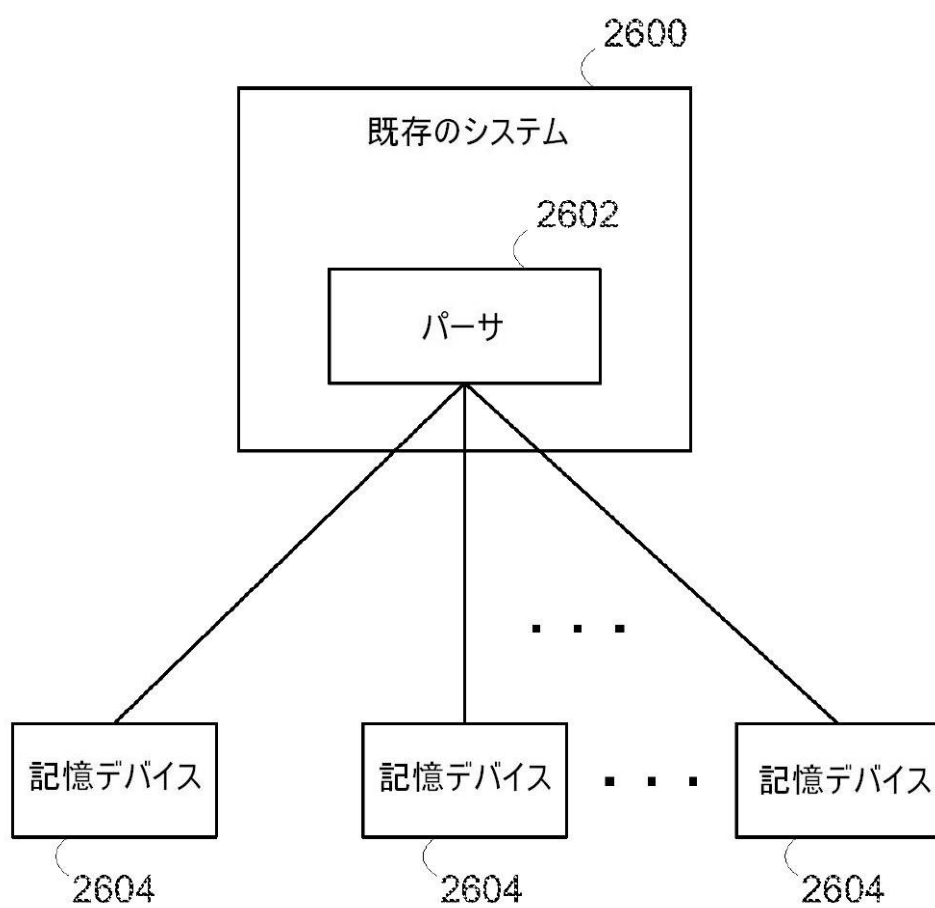


FIG. 27

【図 28】

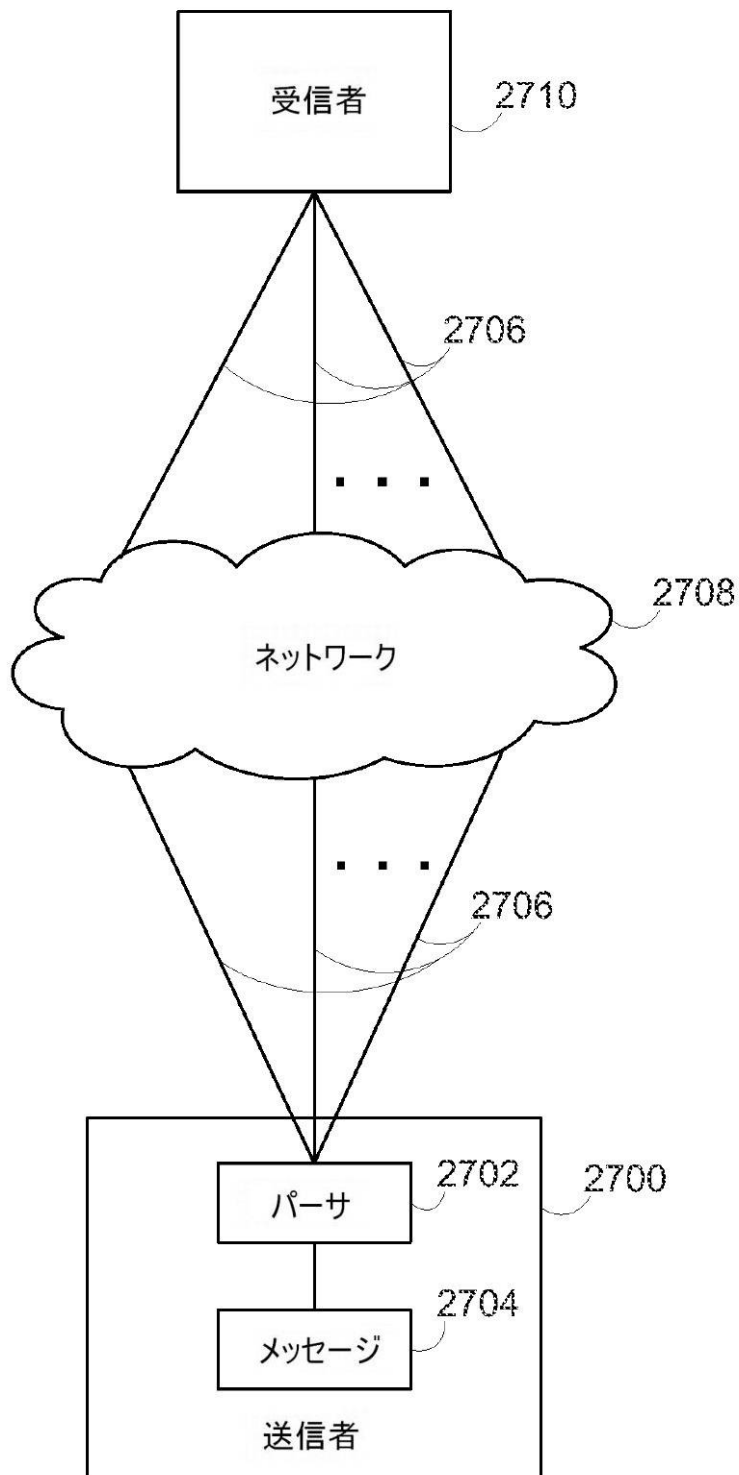


FIG. 28

【図 29】

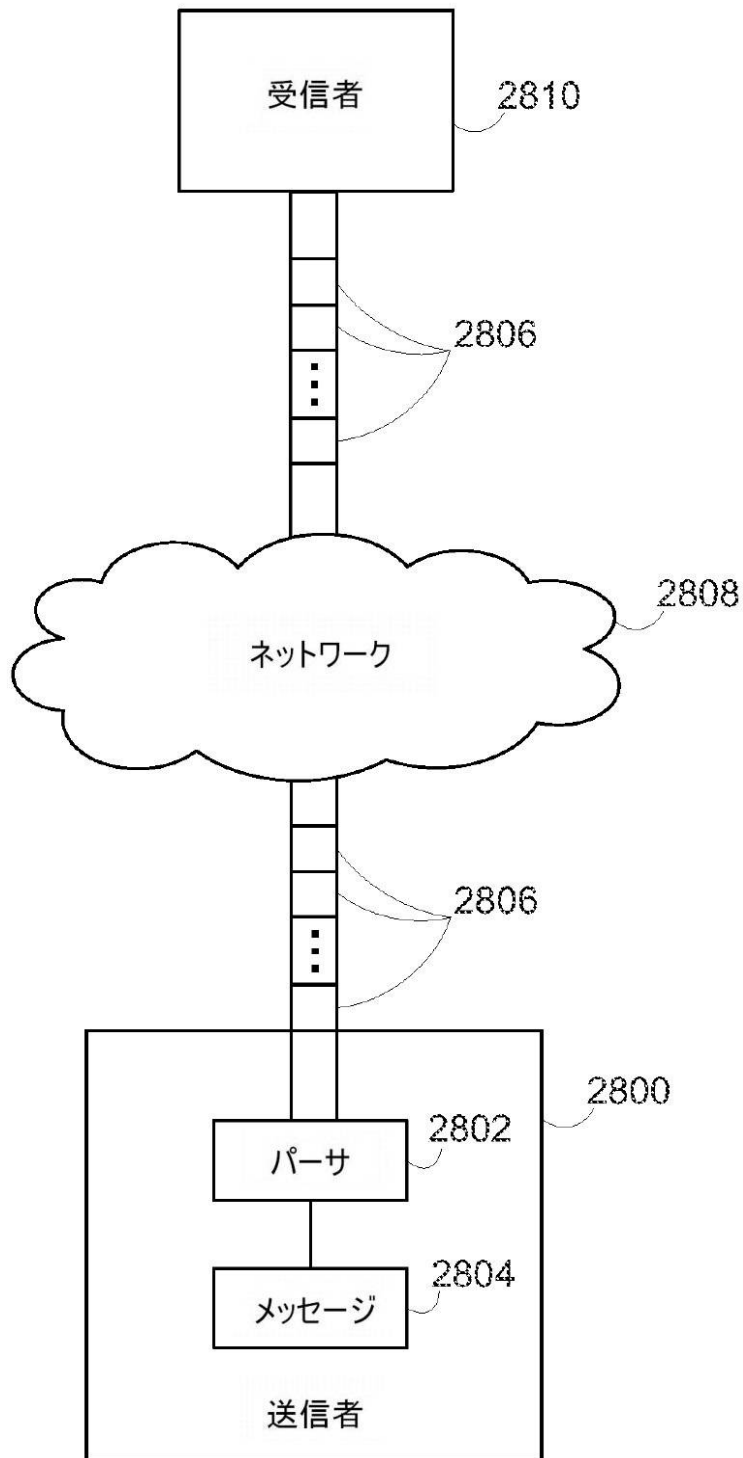


FIG. 29

【図 30】

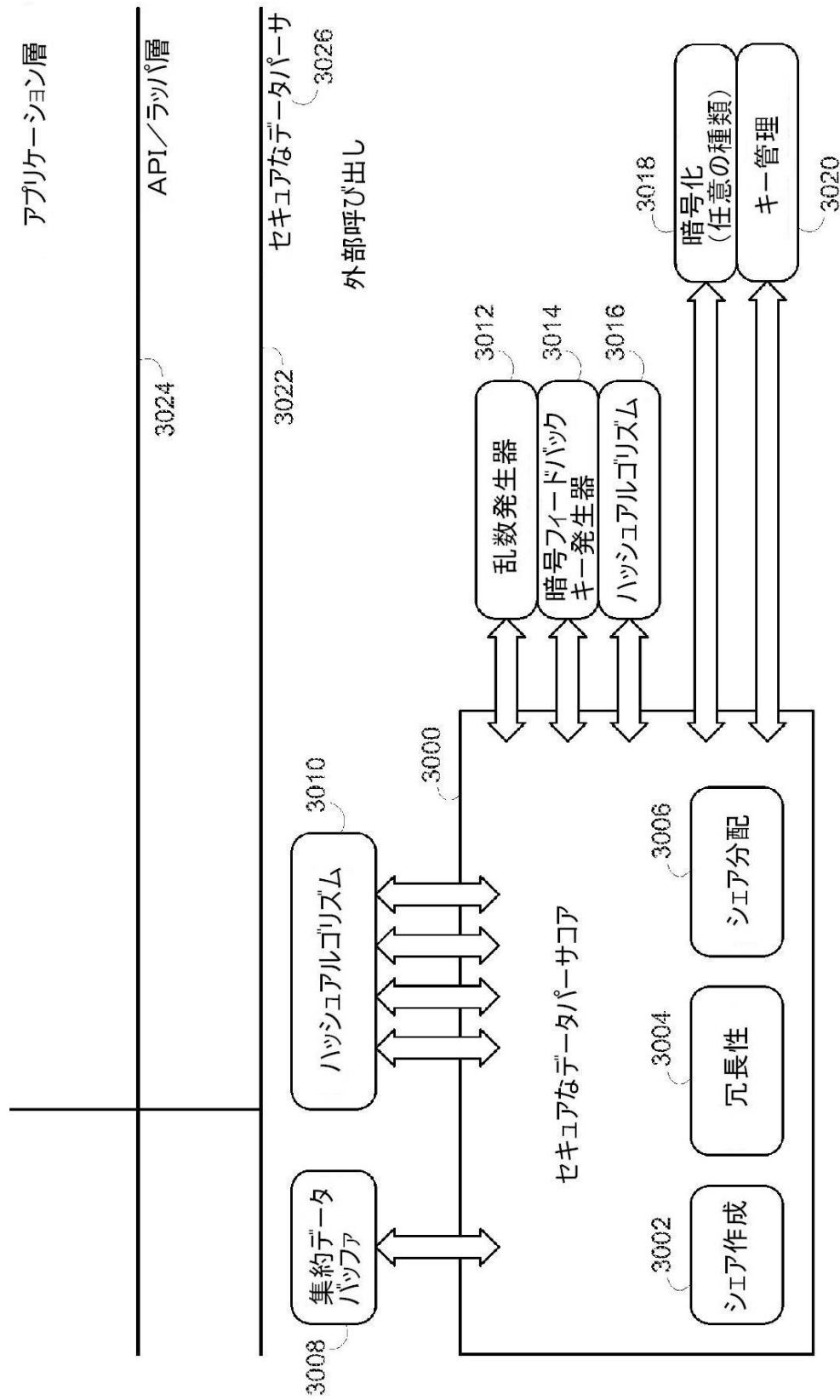


FIG. 30

【図 31】

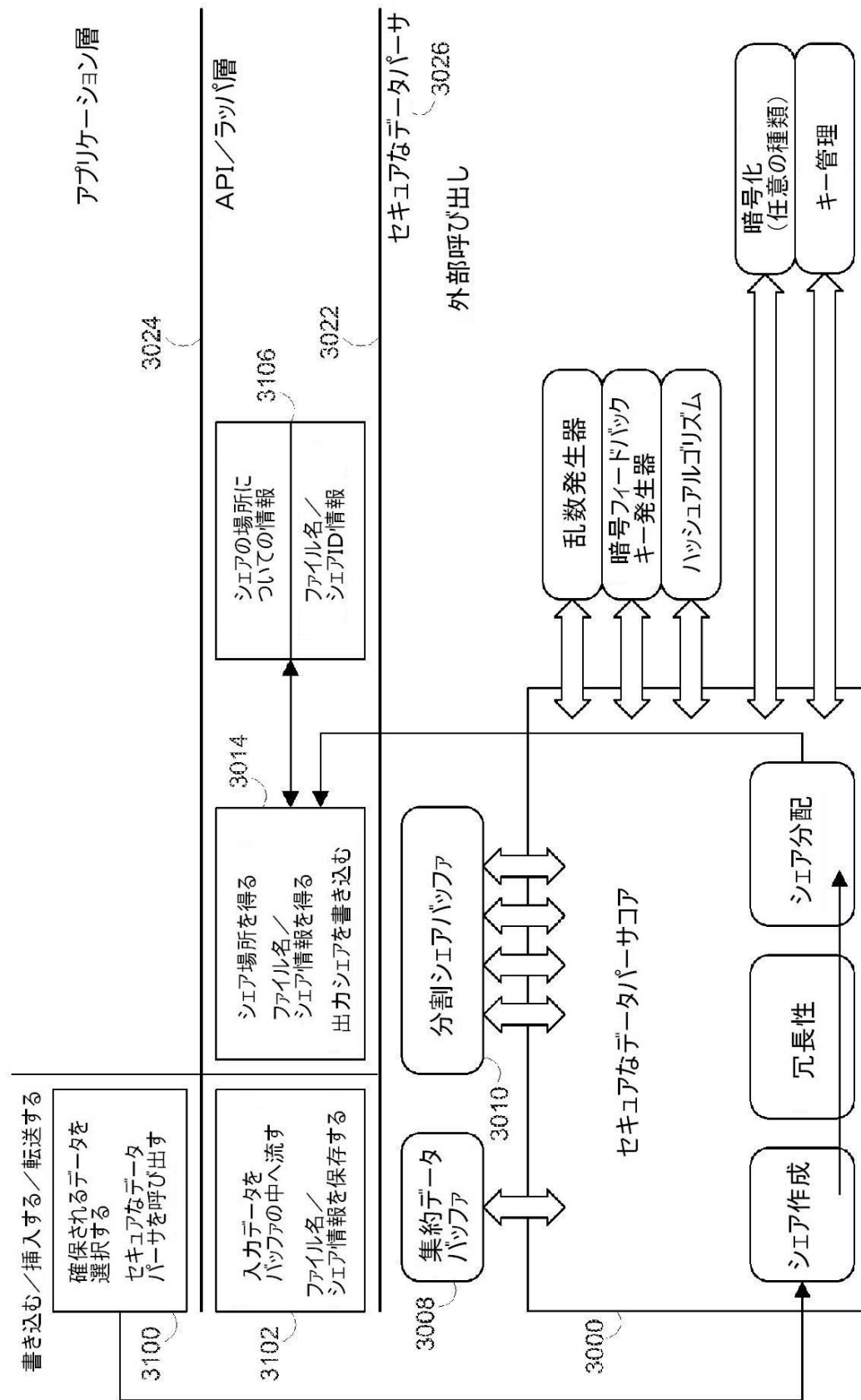
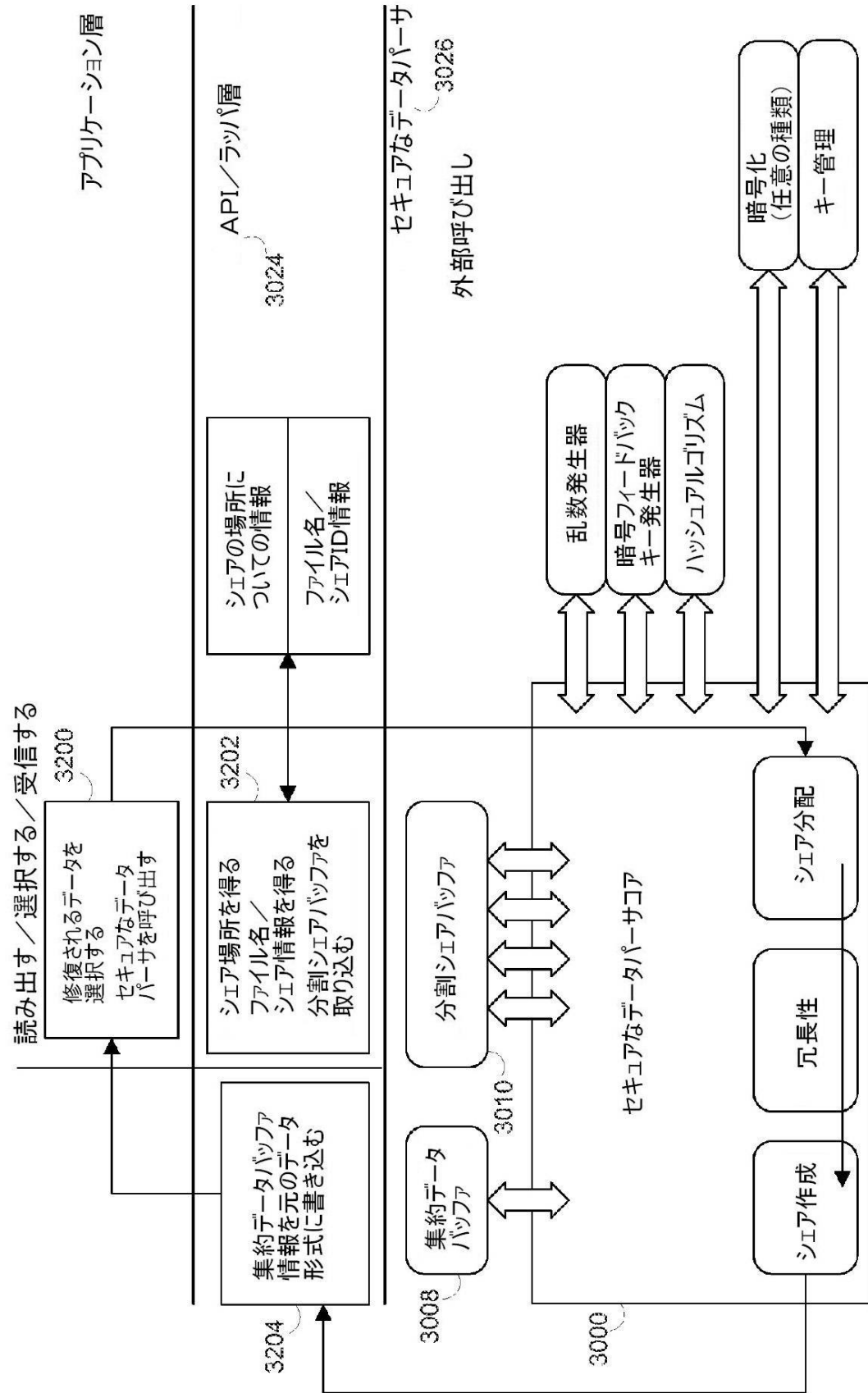


FIG. 31

【図 32】



【図 33】

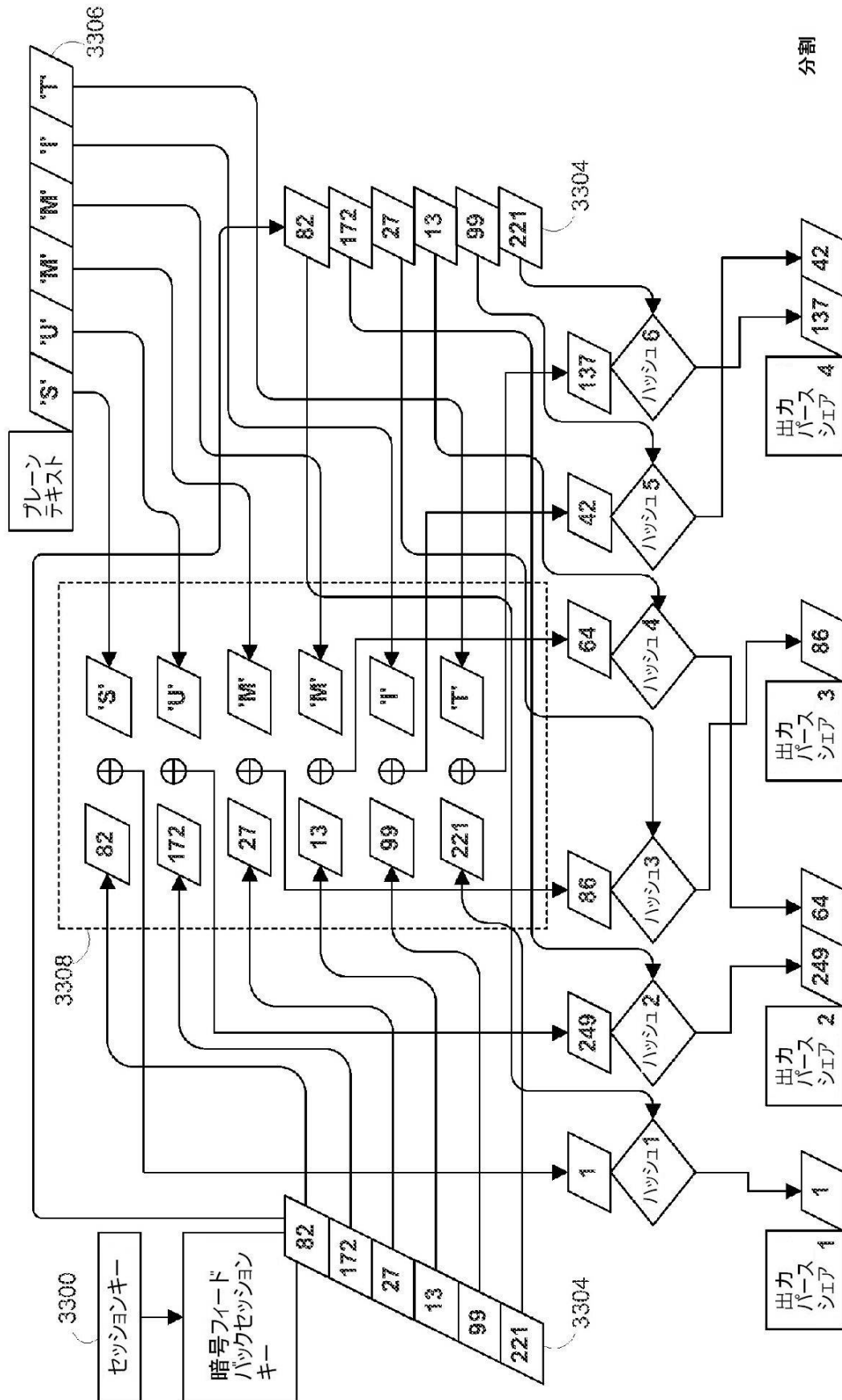


FIG. 33

【図 34】

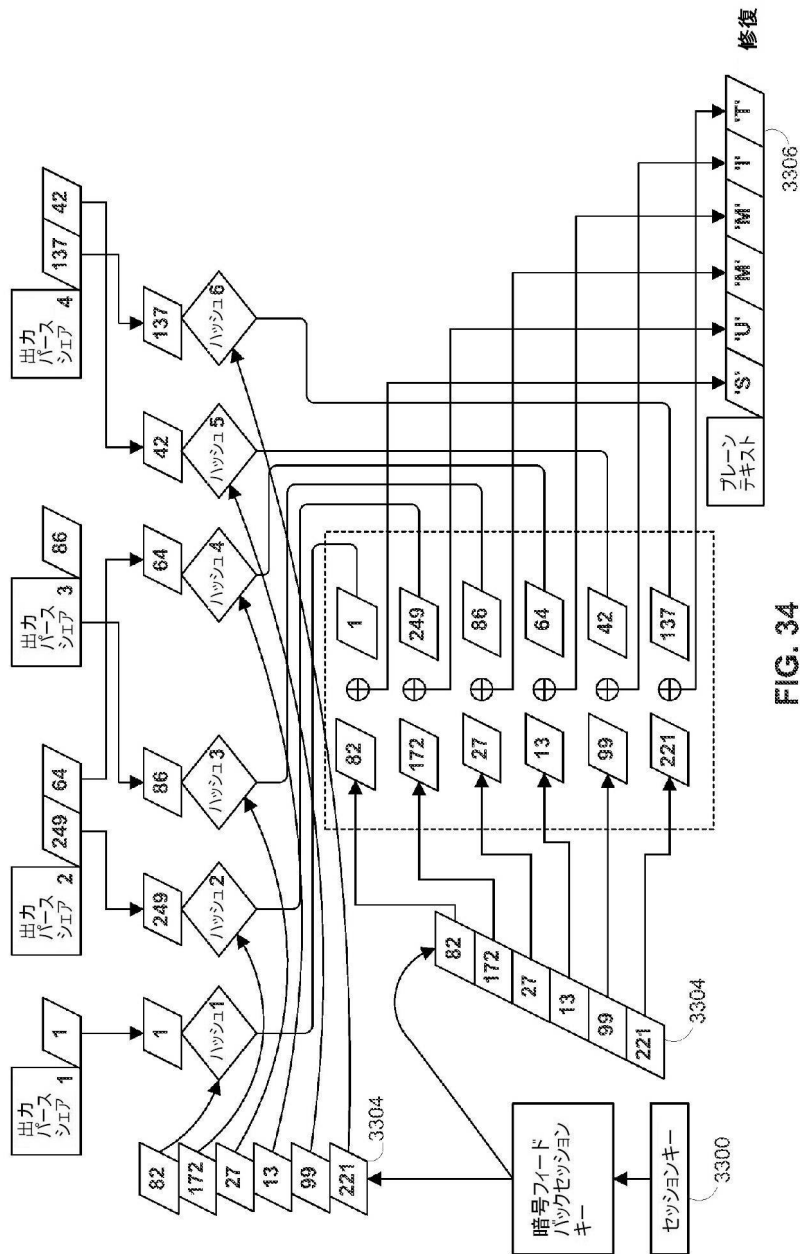
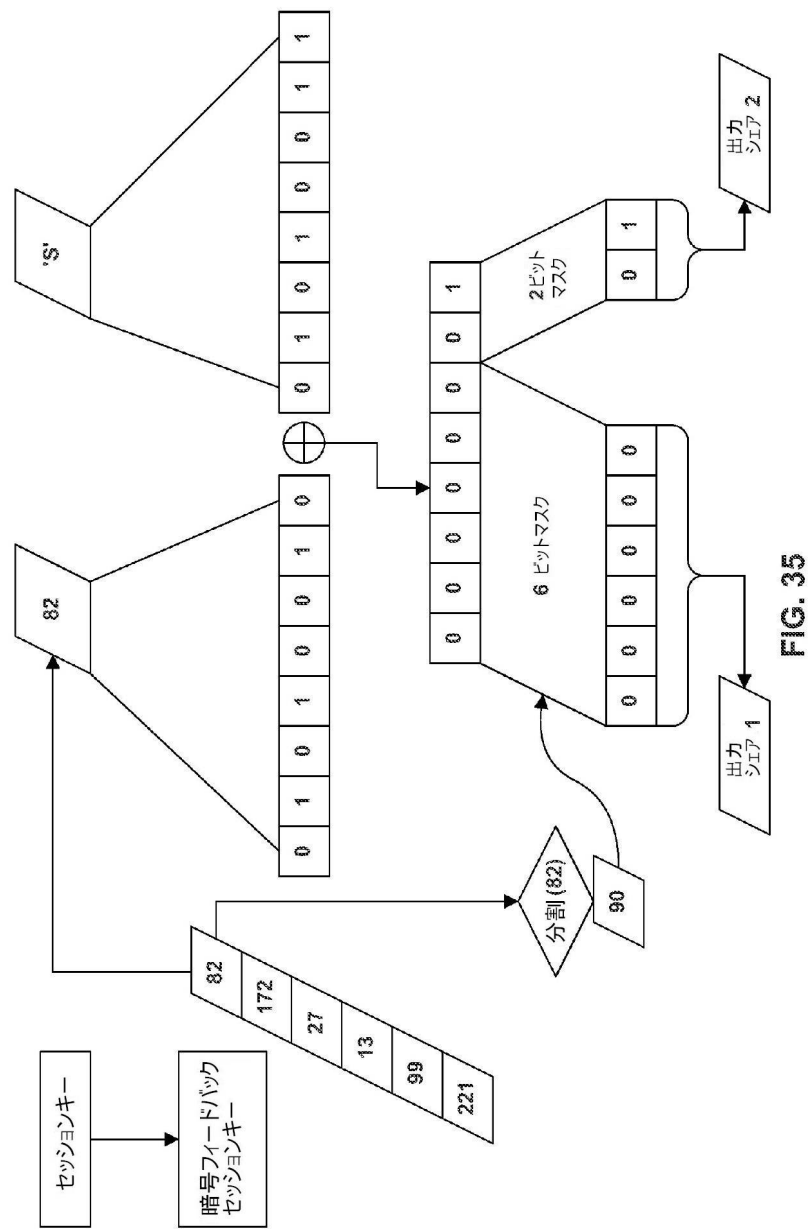


FIG. 34

【図 35】



【図 37】

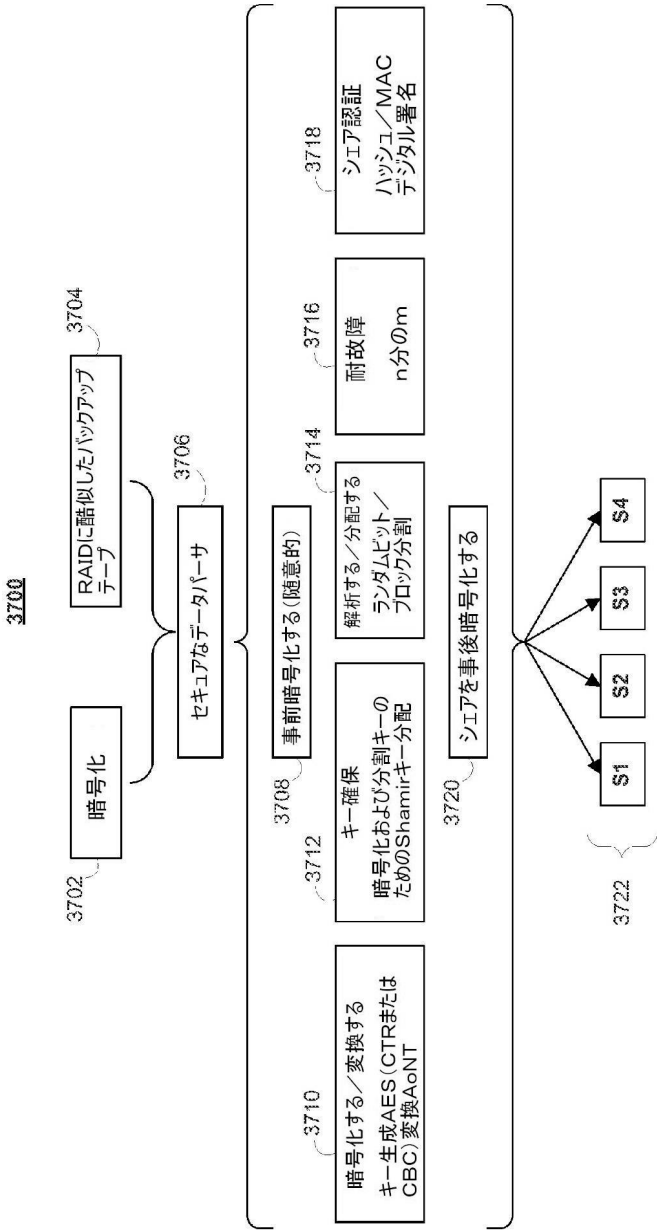


FIG. 37

3800

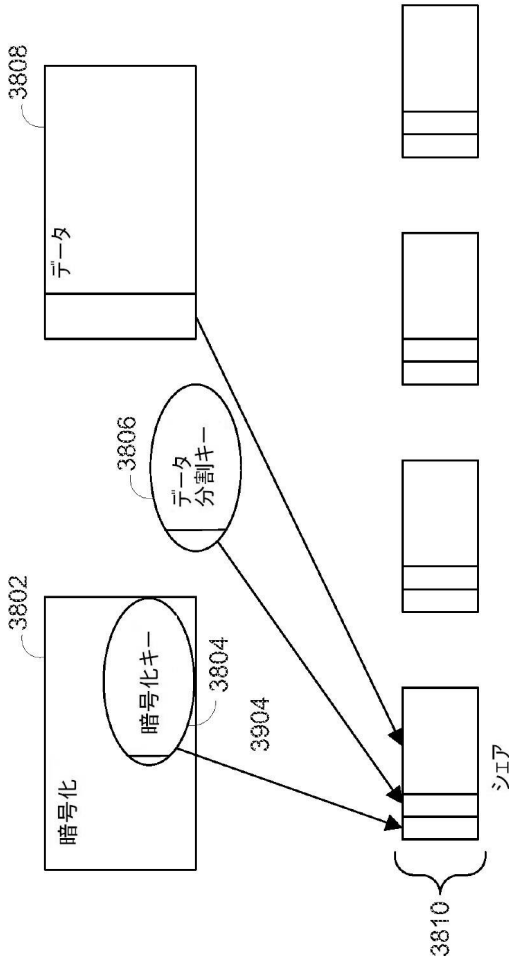


FIG. 38

【図 39】

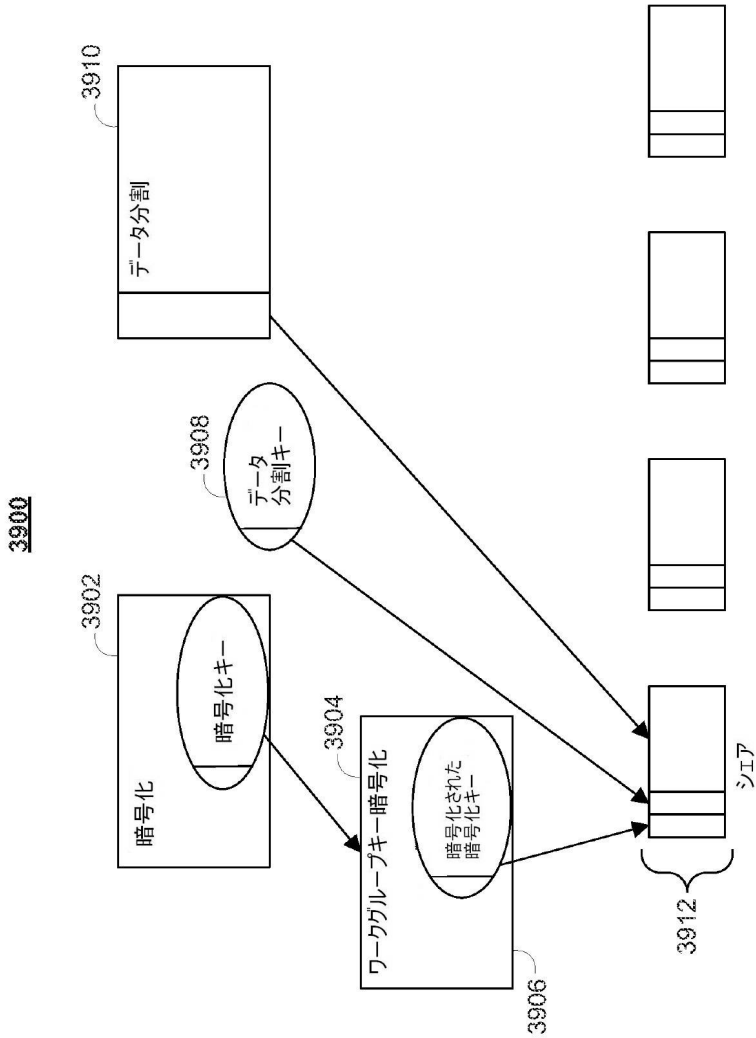


FIG. 39

【図 40】

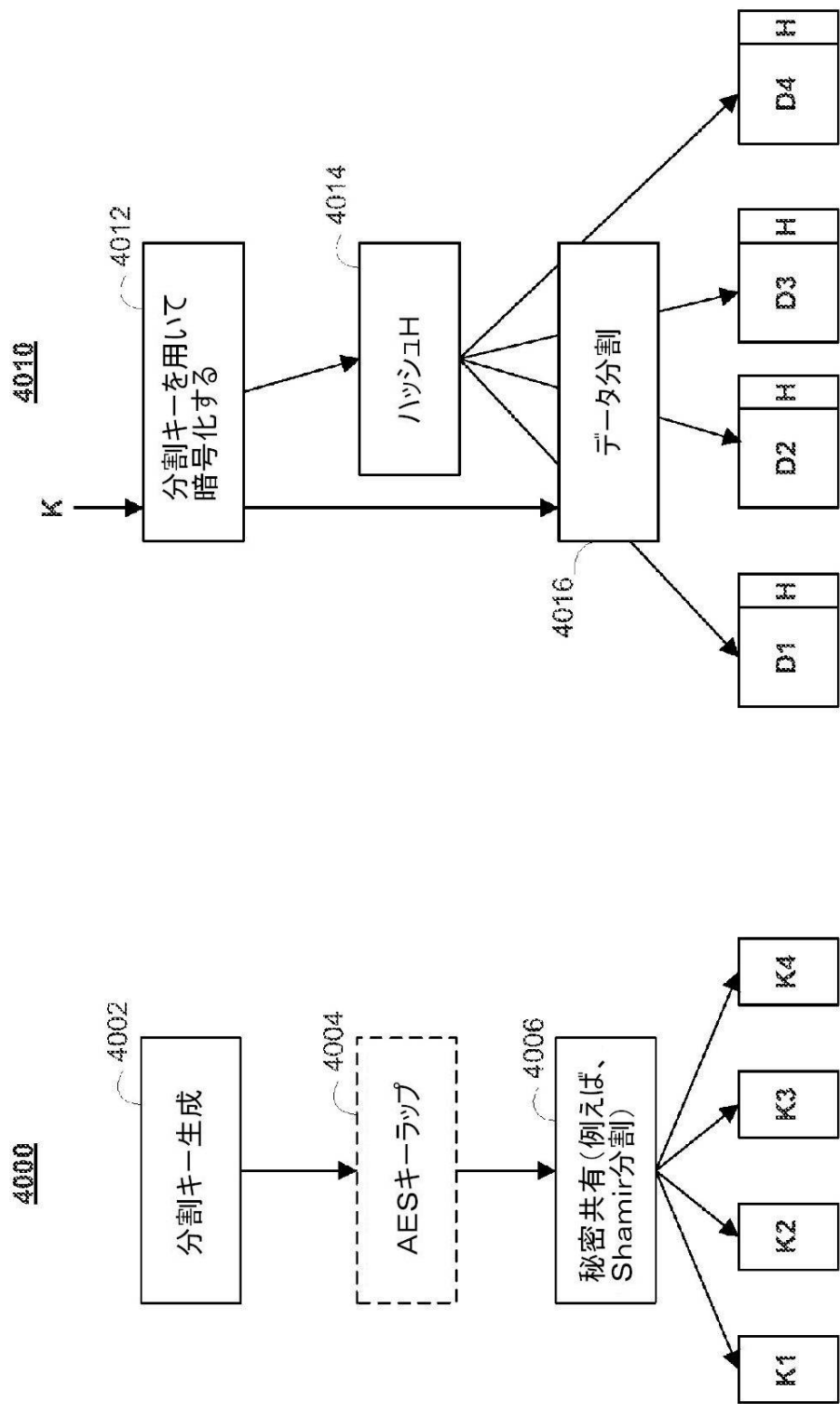


FIG. 40B

FIG. 40A

4100

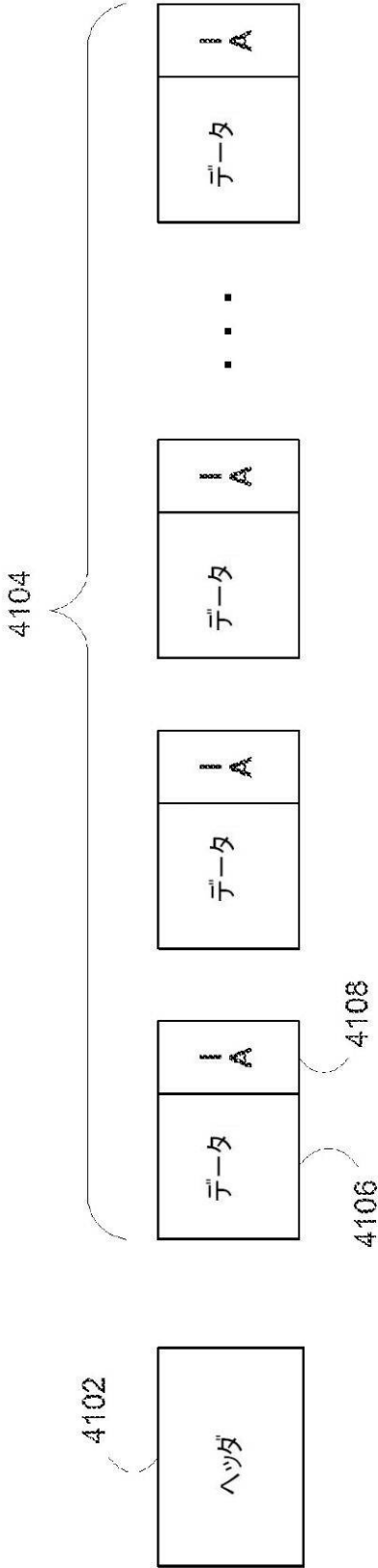


FIG. 41

【図 4 2】

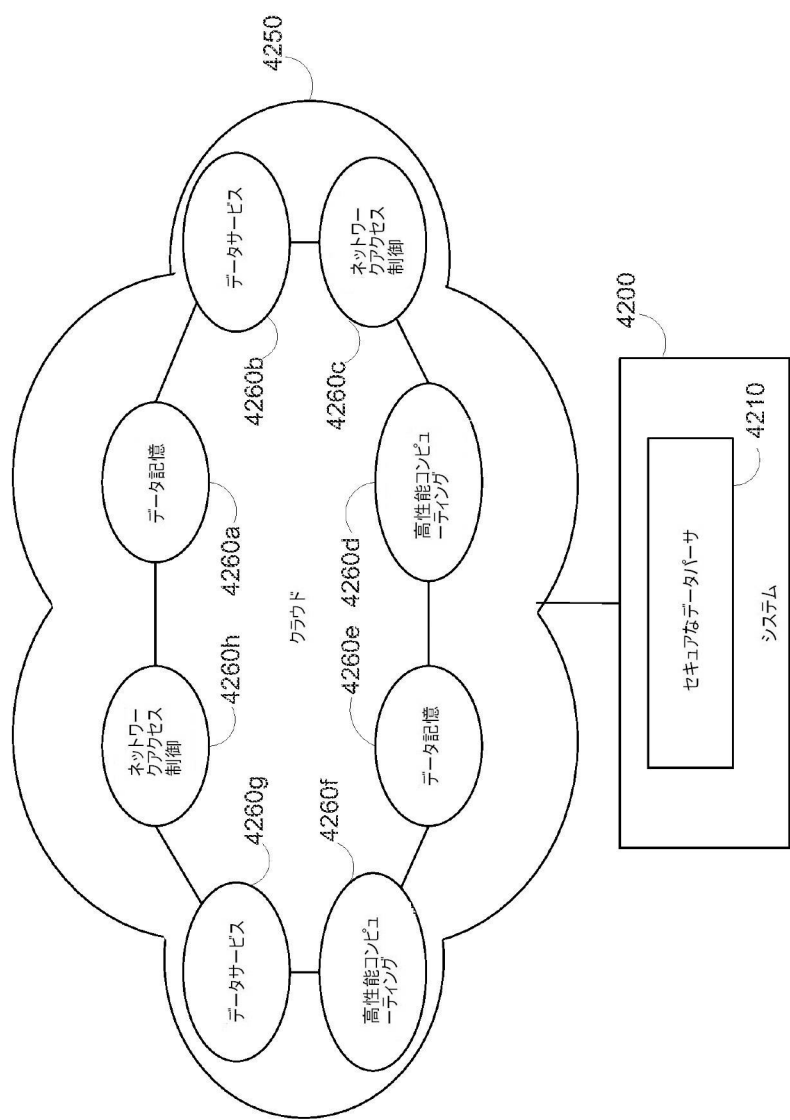


FIG. 42

【図 4 3】

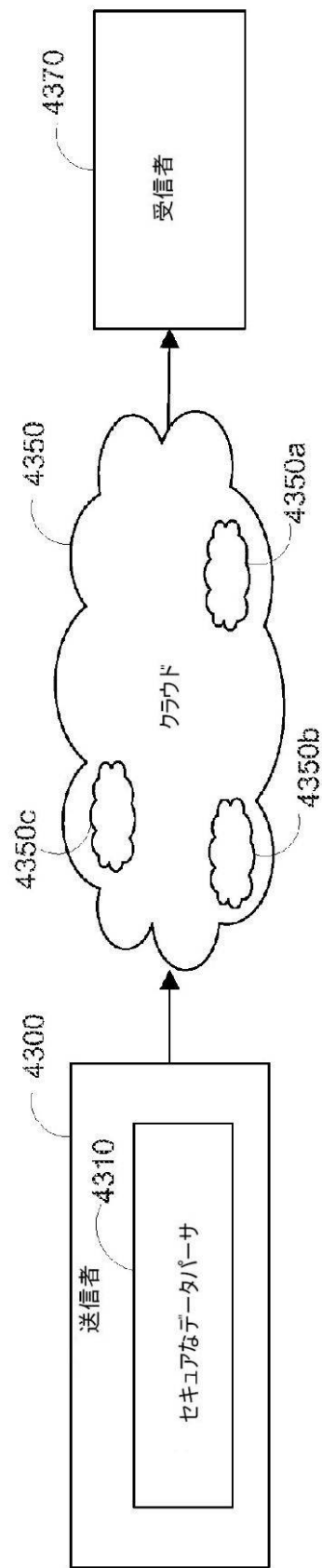


FIG. 43

【図 4 4】

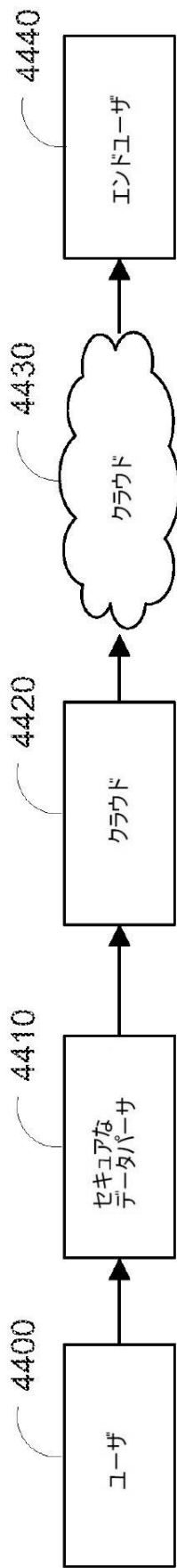


FIG. 44

【図 4 5】

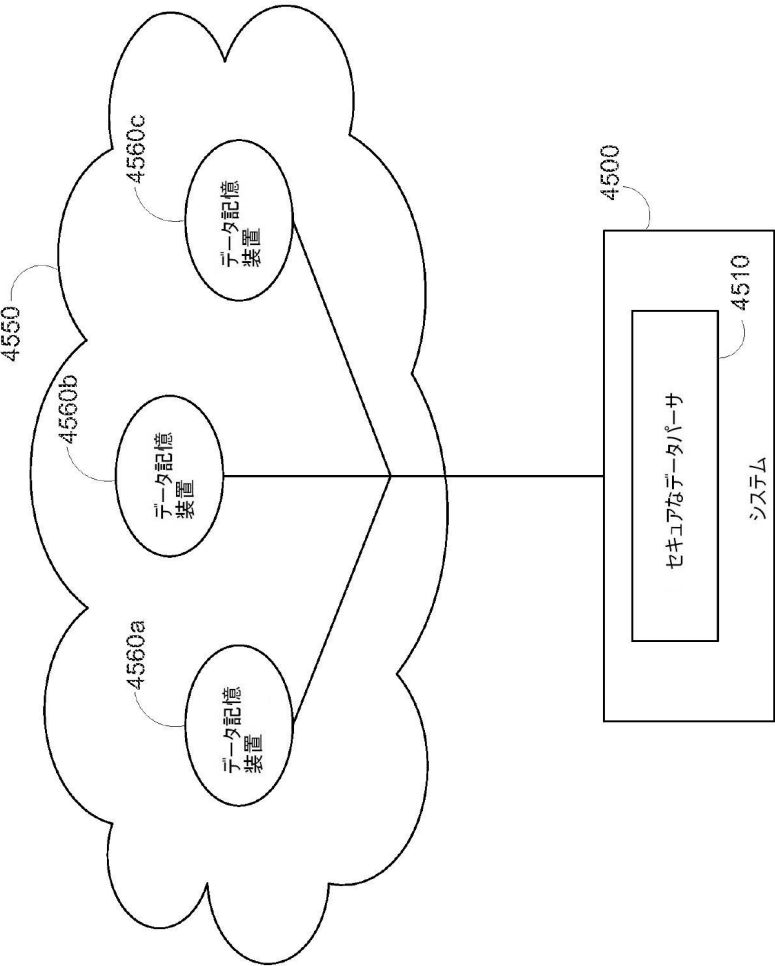


FIG. 45

【図 4 6】

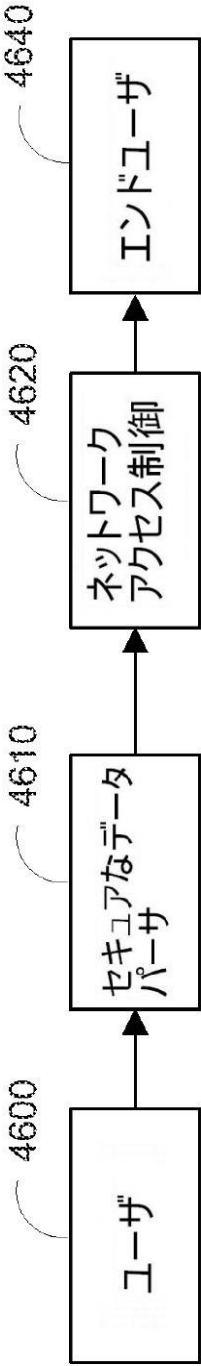


FIG. 46

【図 47】

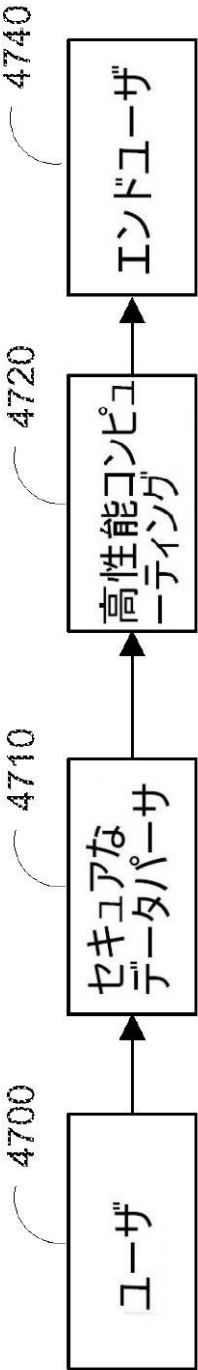


FIG. 47

【図 48】

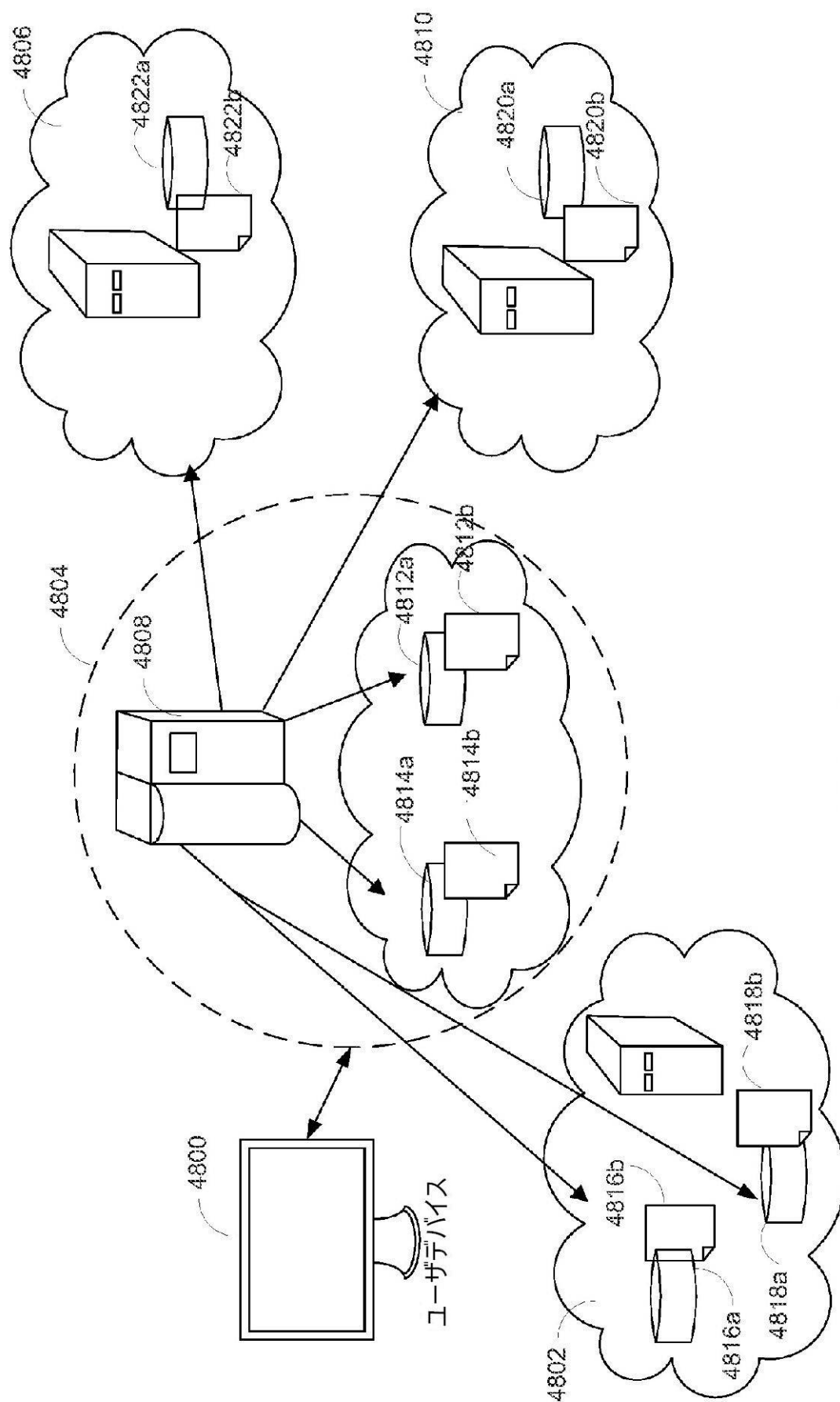


FIG. 48

【図 49】

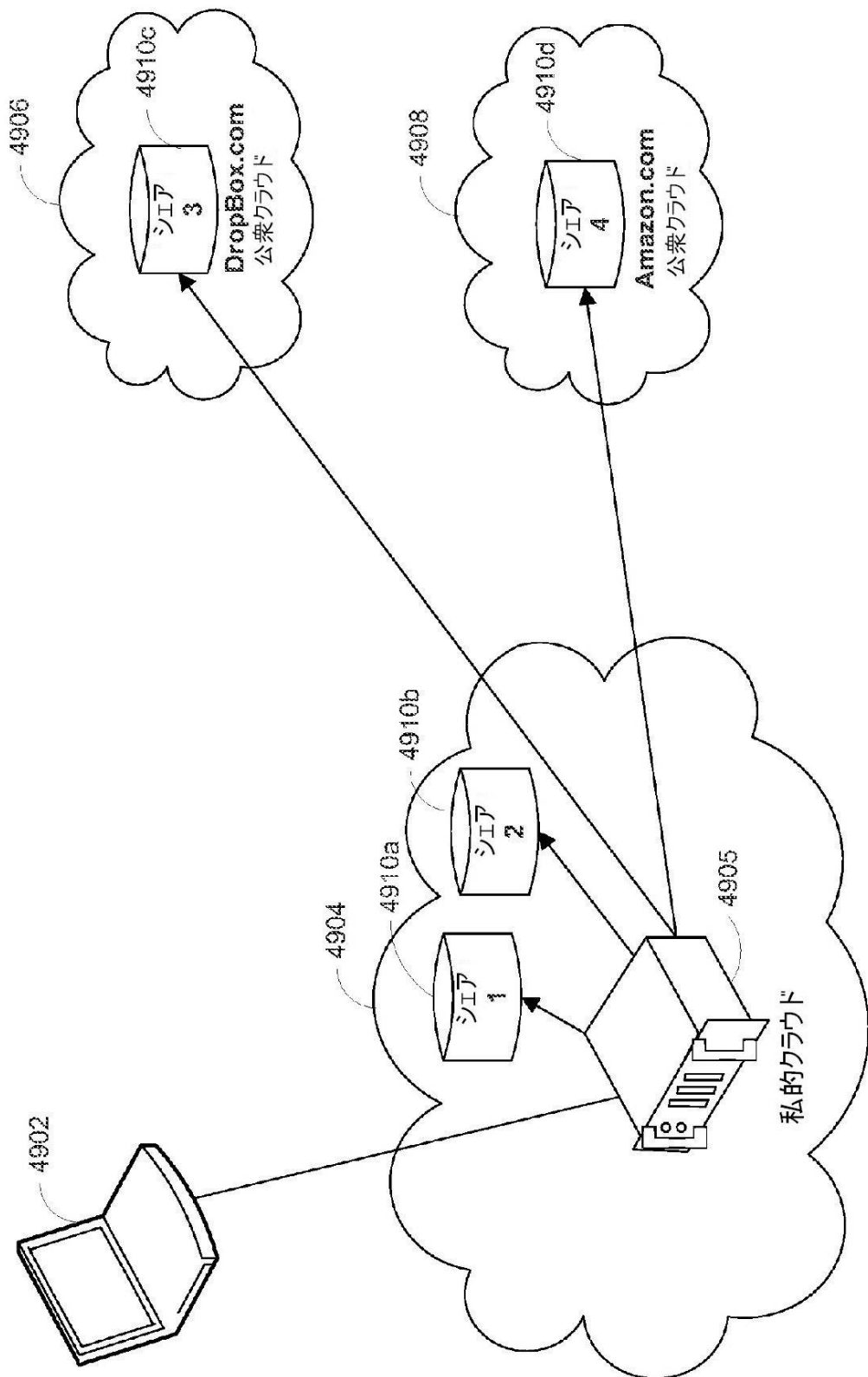


FIG. 49

【図 50】

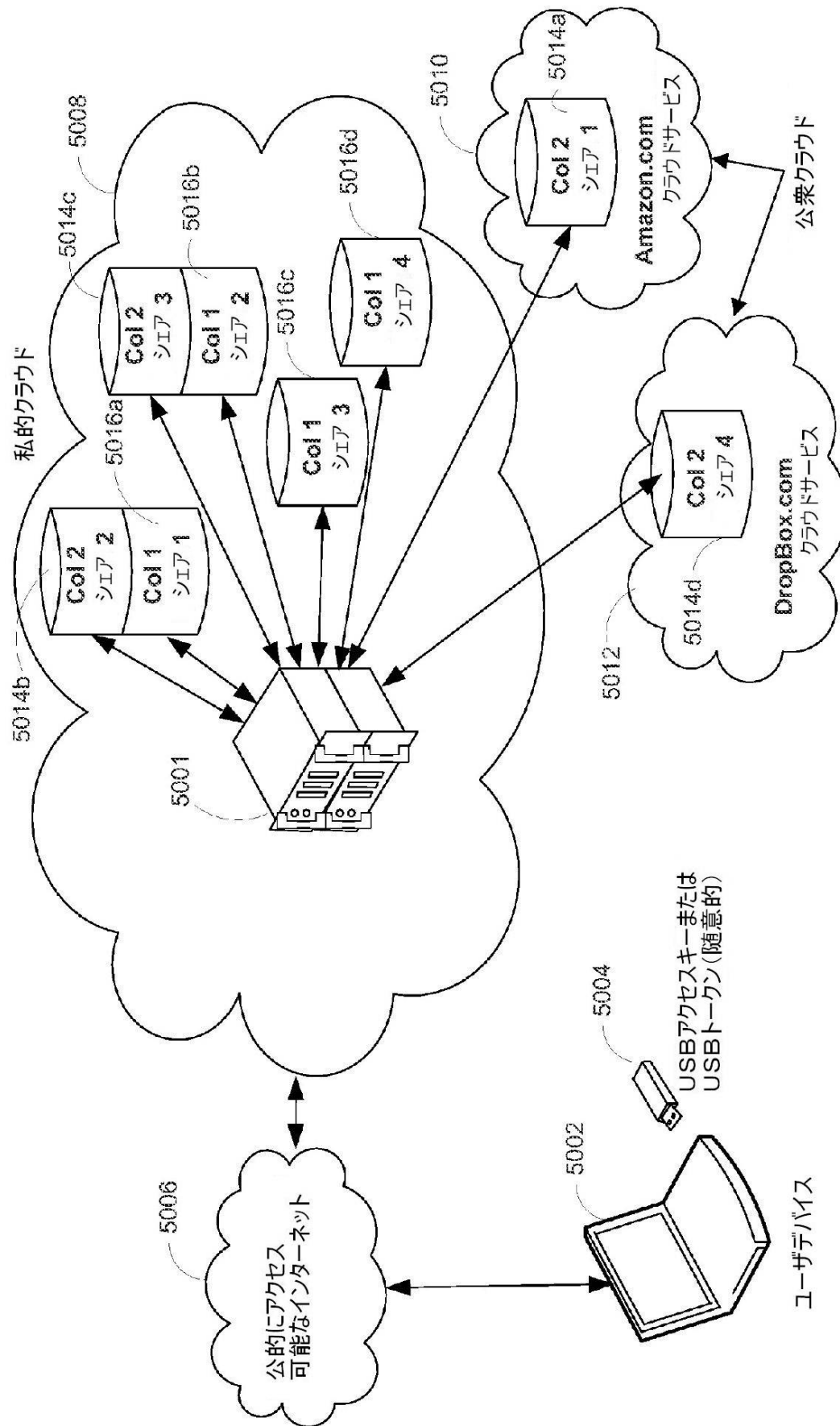


FIG. 50

【図 51】

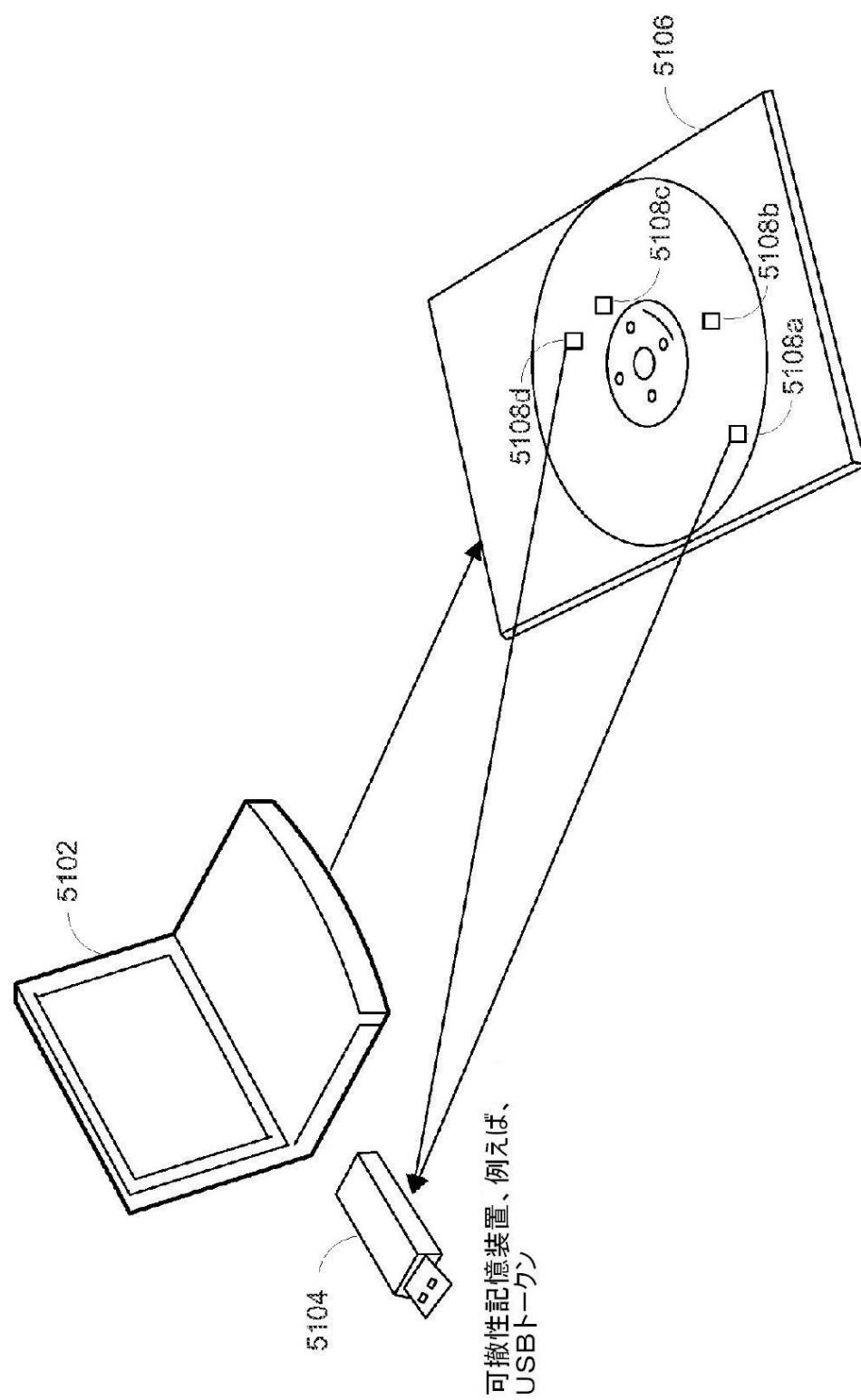


FIG. 51

【図 52】

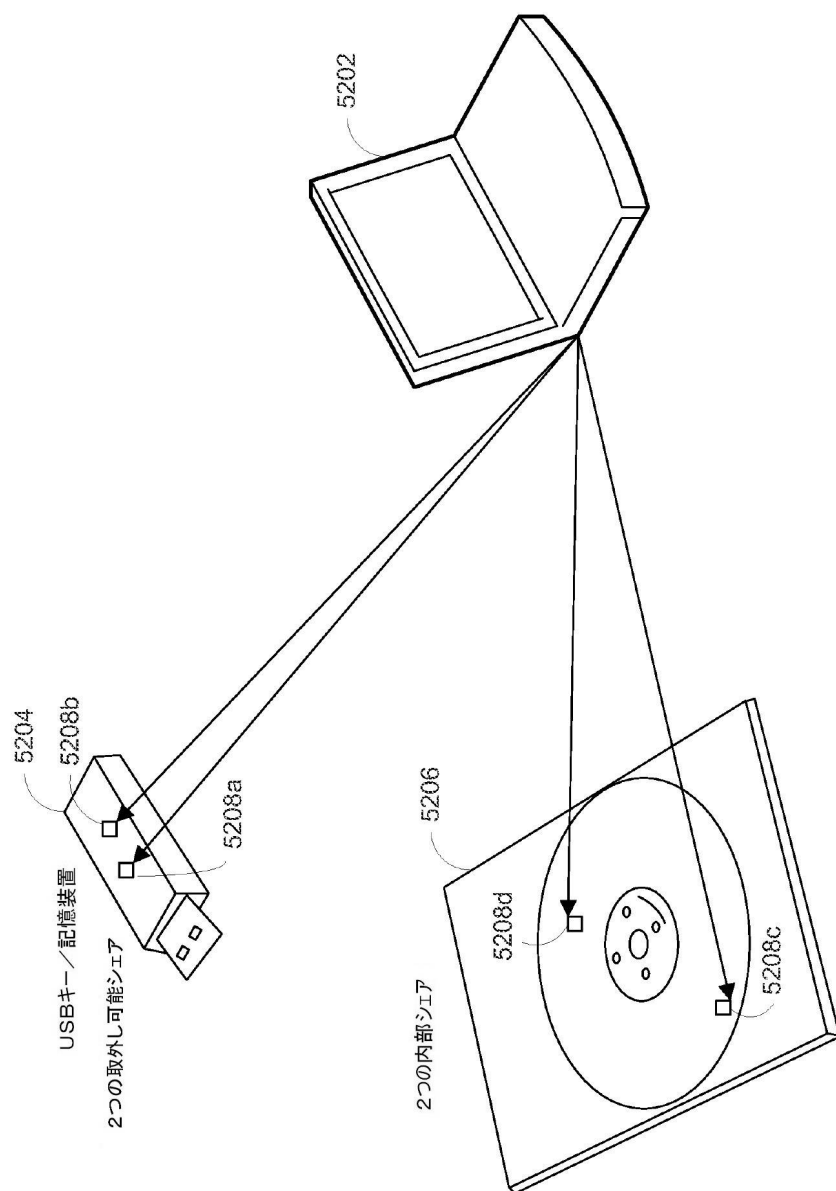


FIG. 52

【図 5 4】

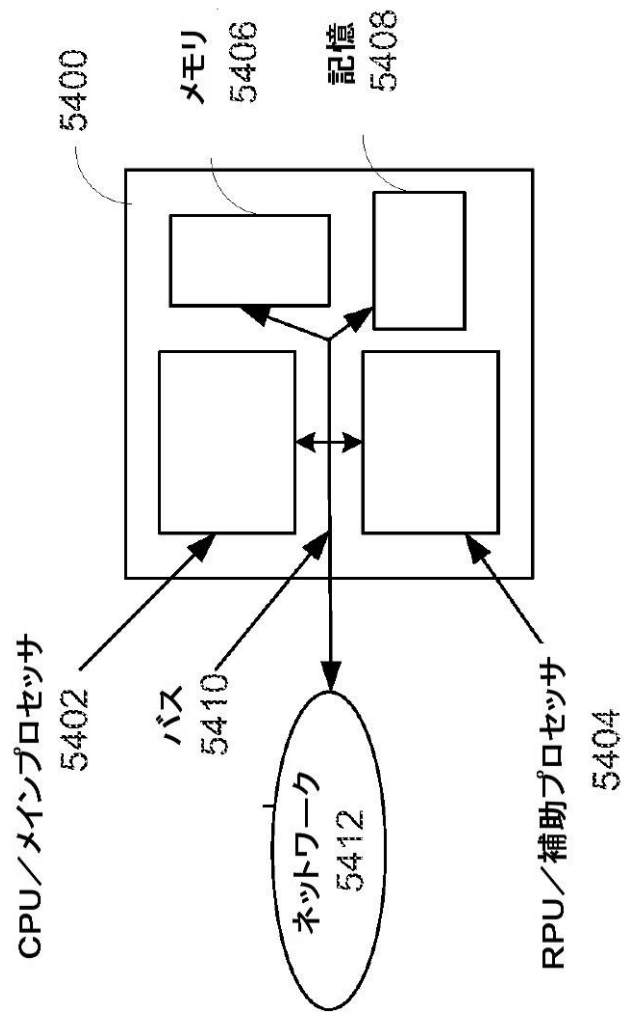


FIG. 54

【図 55】

5500

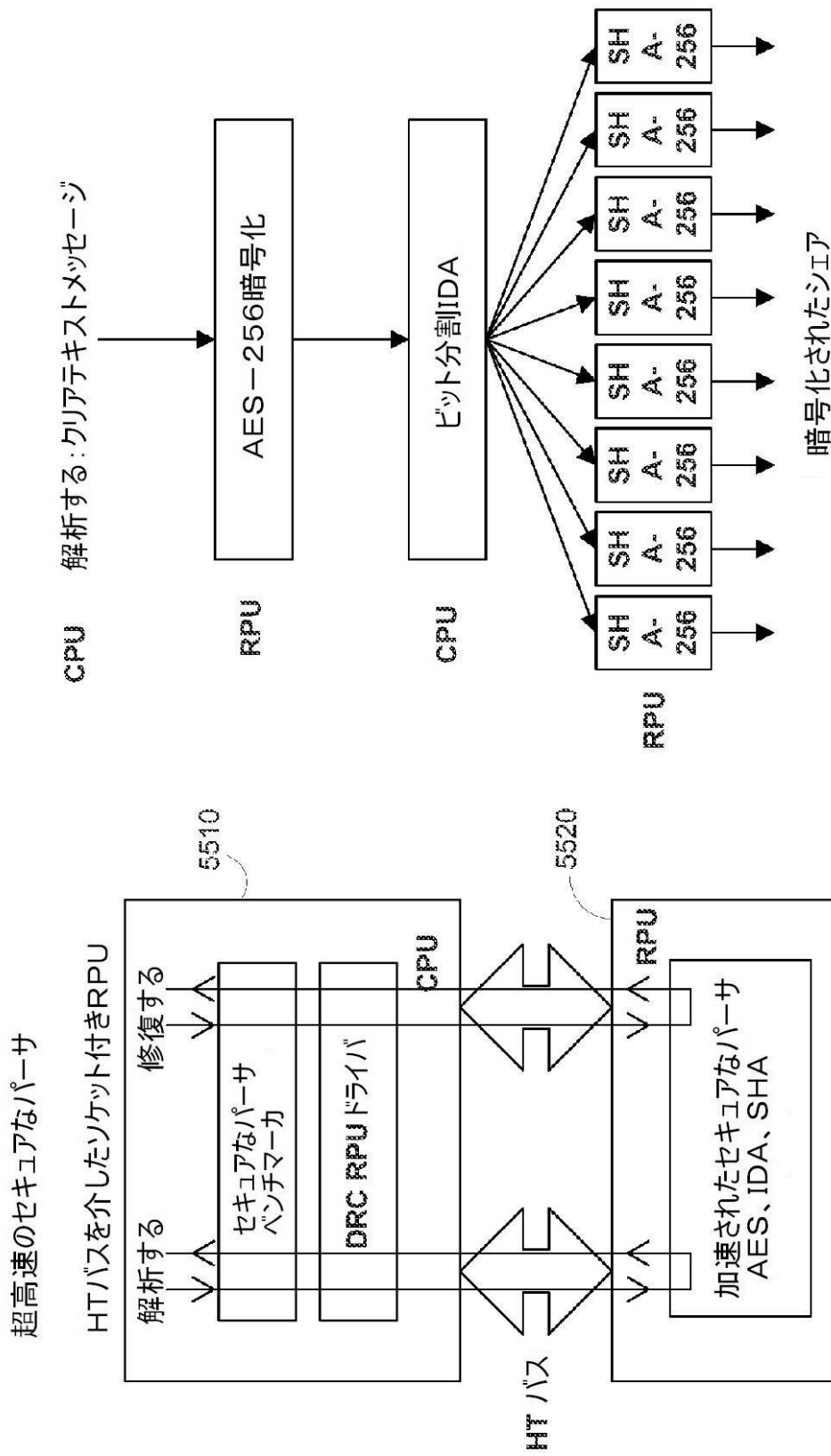


FIG. 55

【図 56】

5600

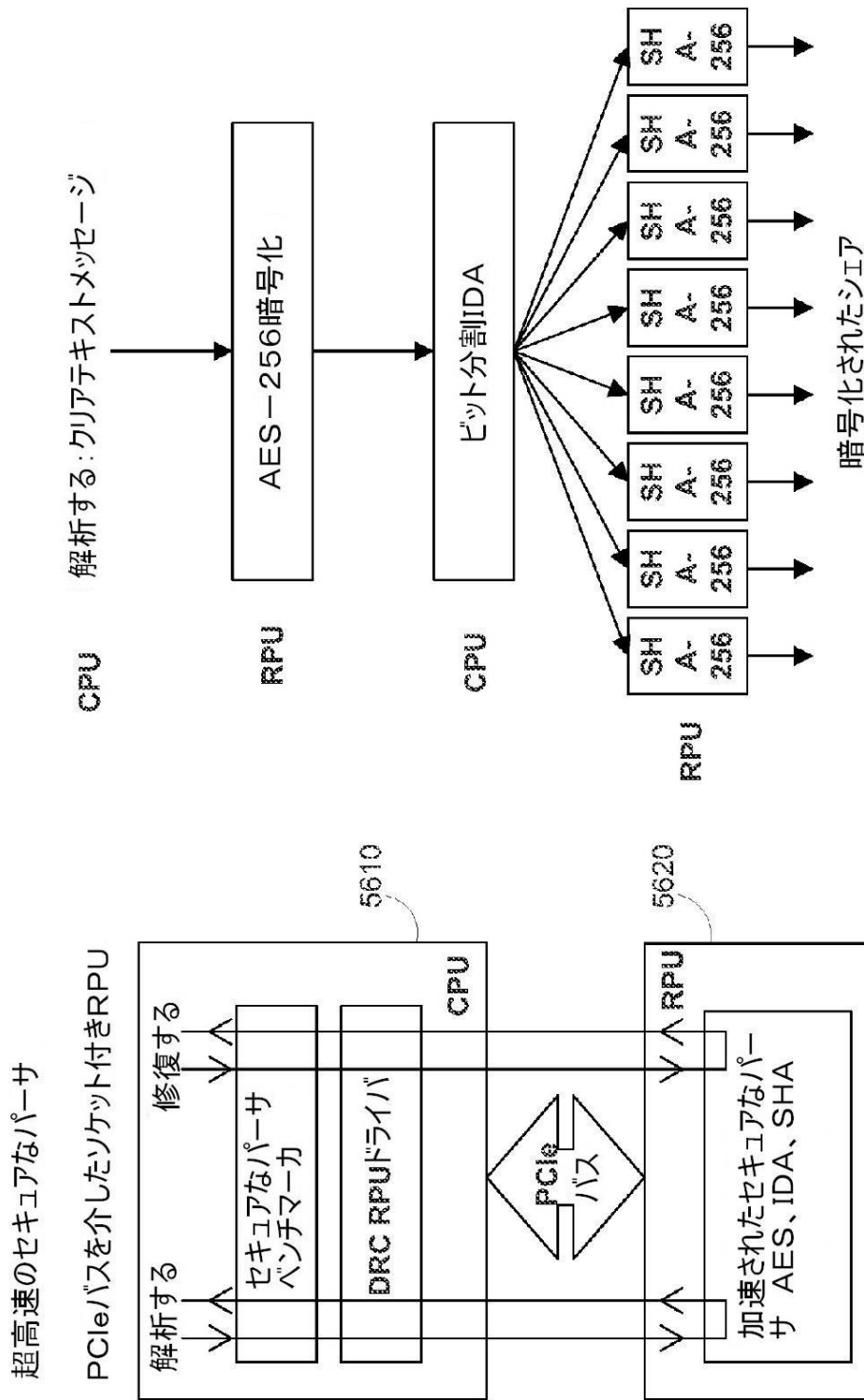


FIG. 56

【図 57】

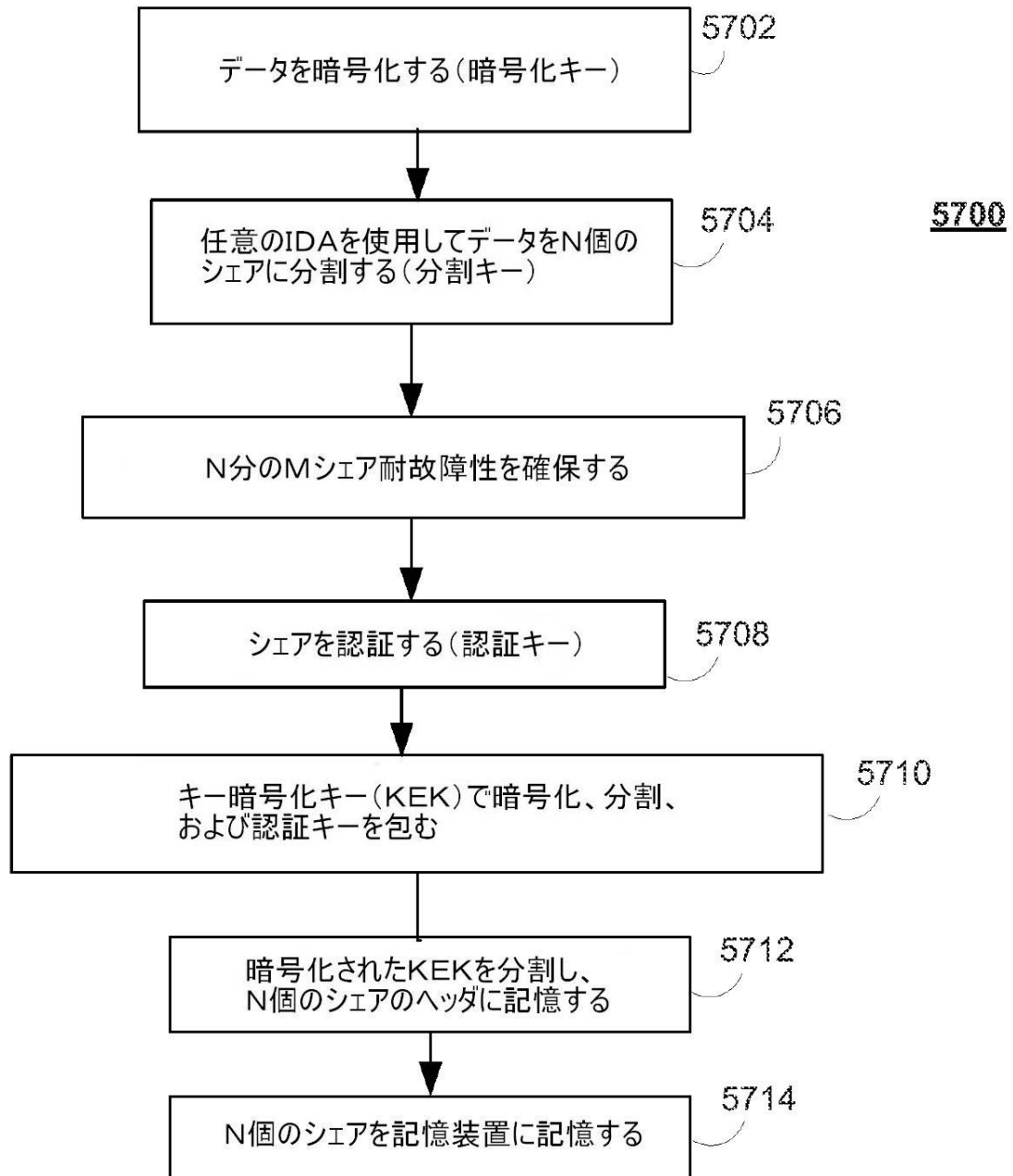


FIG. 57

【図 58】

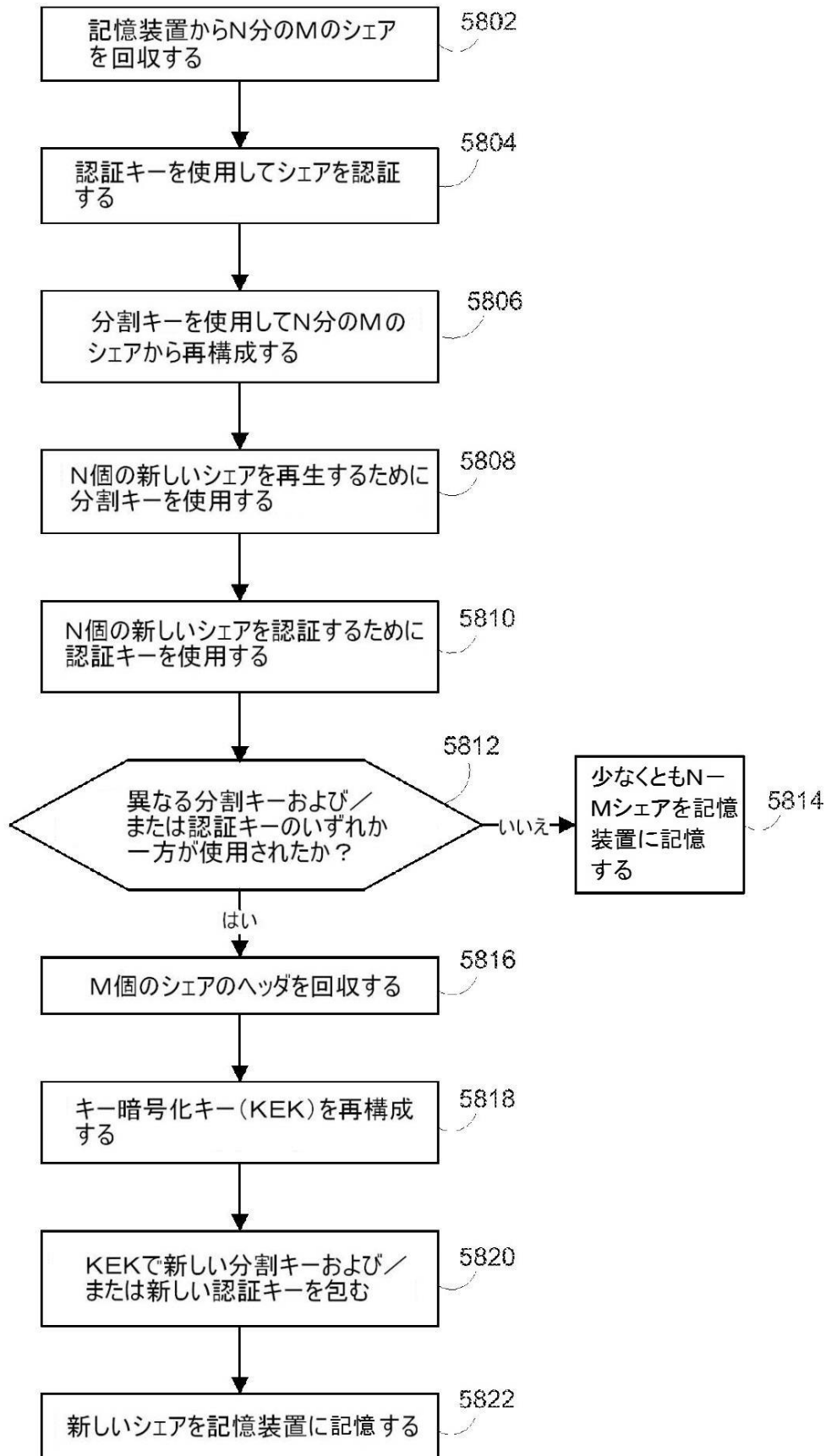


FIG. 58

【図 59】

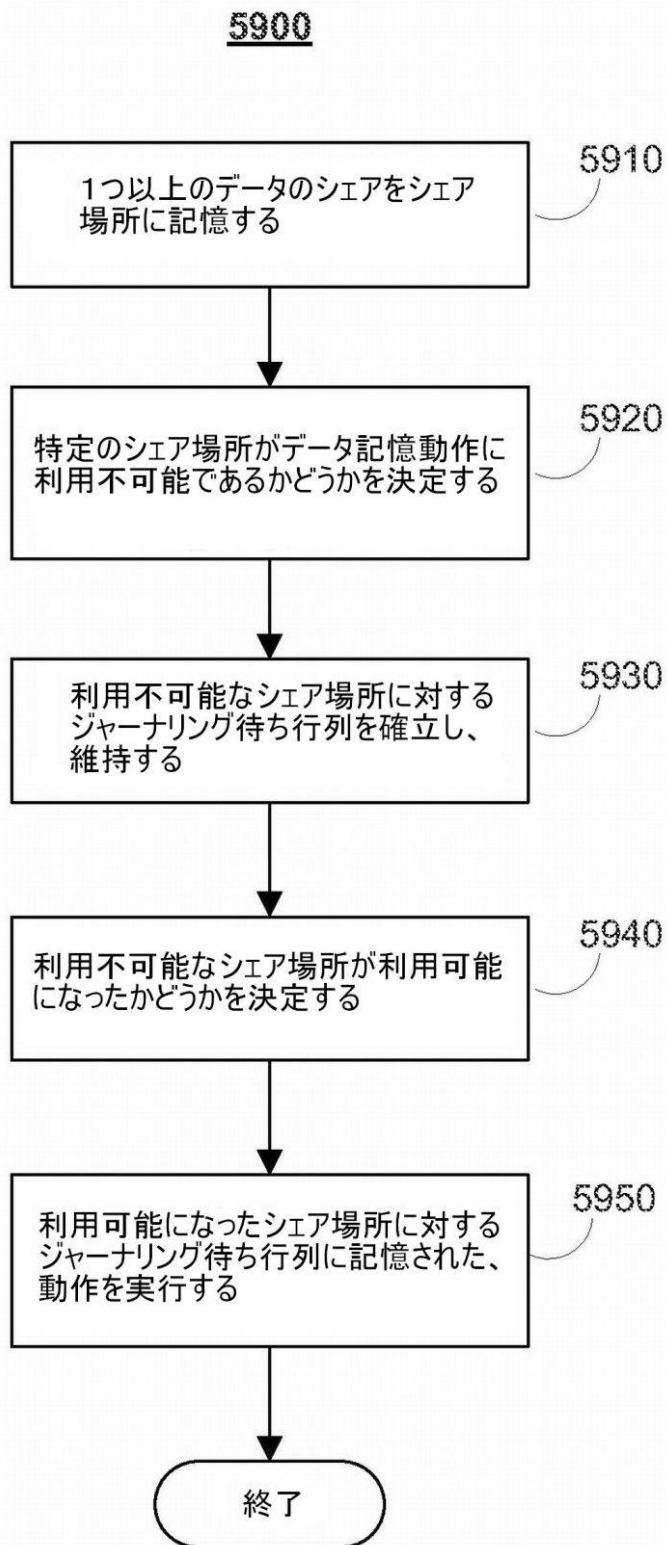


FIG. 59

【図 60】

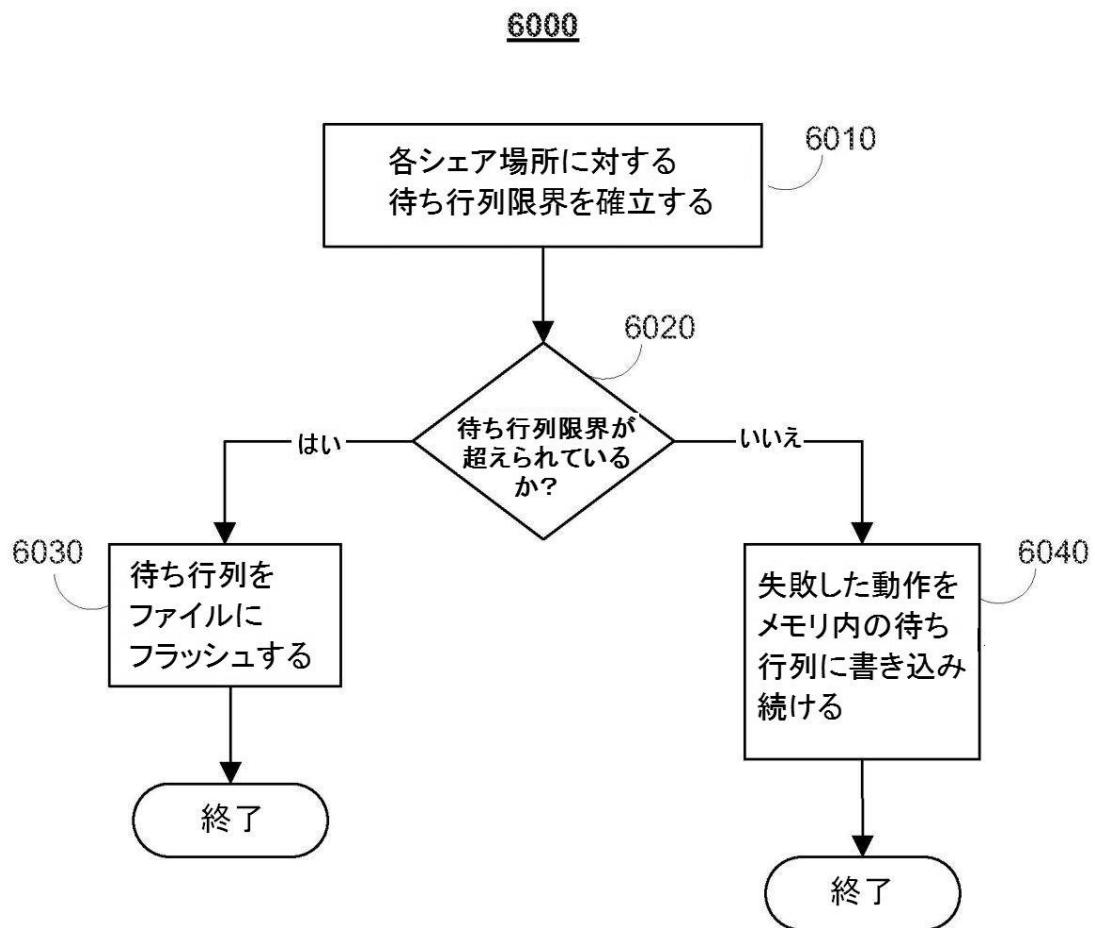


FIG. 60

【図 6 1】

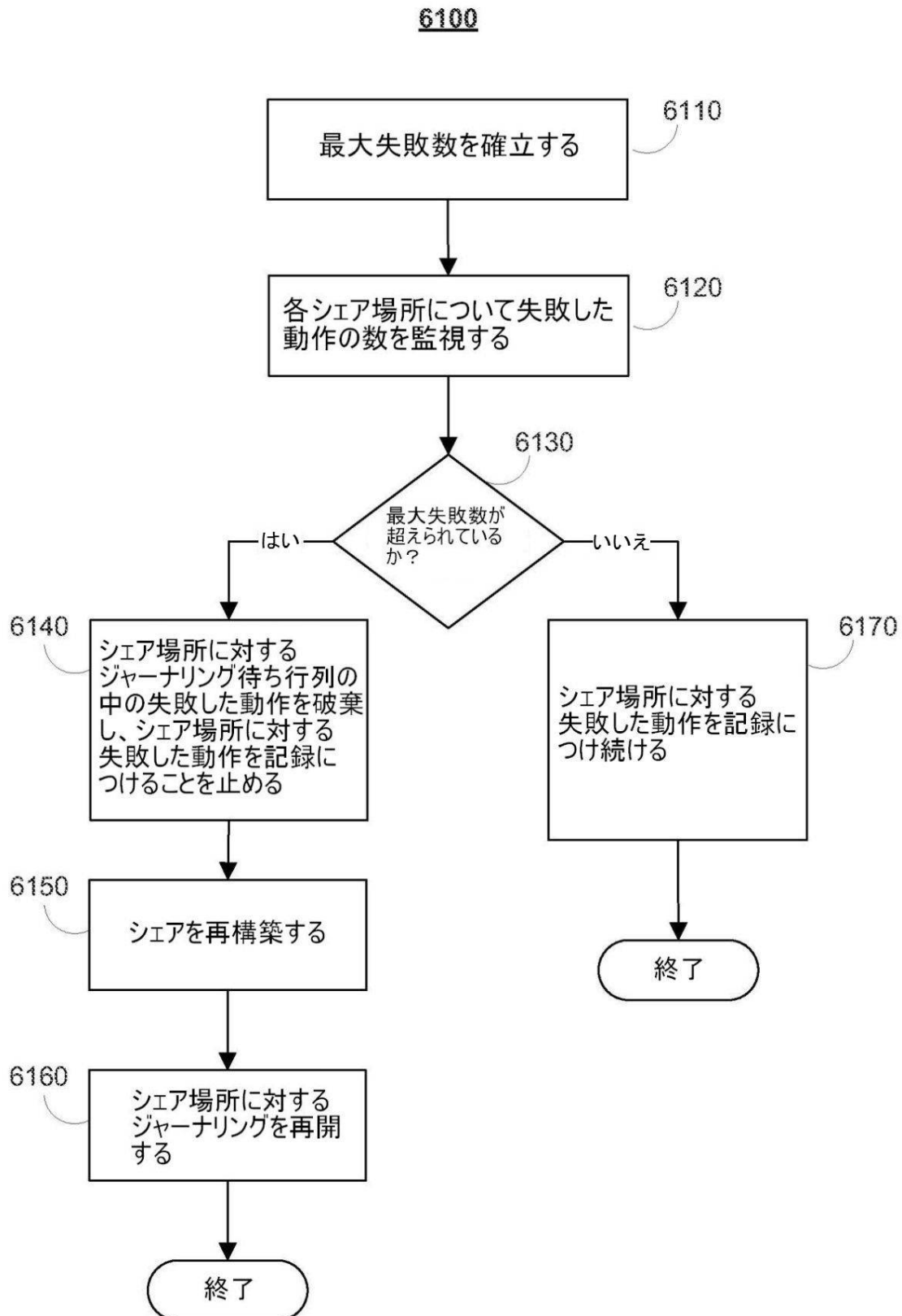


FIG. 61

【図 6 2】

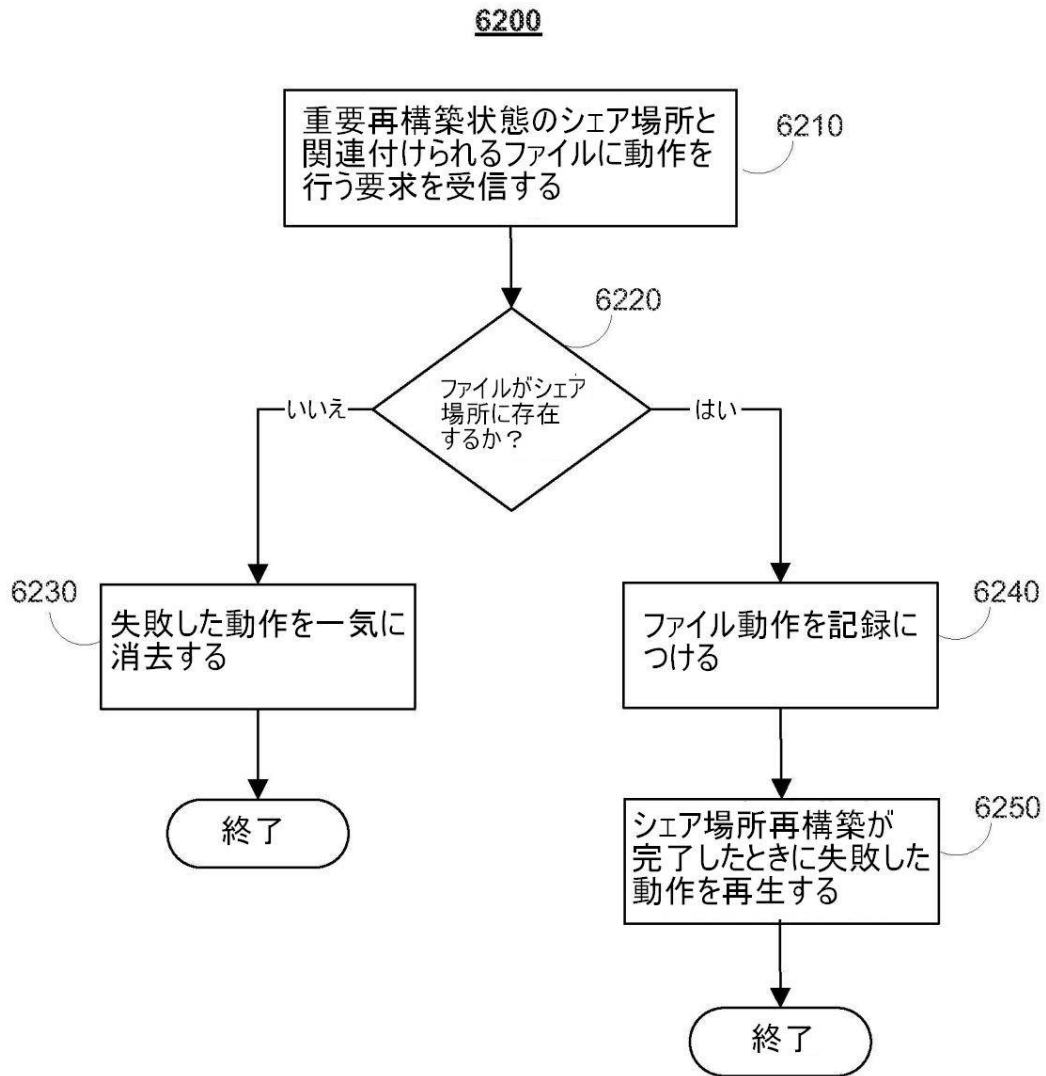


FIG. 62

フロントページの続き

(73)特許権者 512136536

オヘアー, 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

(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

(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

審査官 宮司 卓佳

(56)参考文献 特開2007-334836 (JP, A)

特開2004-185573 (JP, A)

特開2010-045670 (JP, A)

米国特許第07577689 (US, B1)

特開平09-259089 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F21/00-21/88