(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2013-527533
(P2013-527533A)
(43)公表日　平成25年6月27日(2013.6.27)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/62	(2013.01)	G06F	21/24	166A	5J104
H04L 9/08	(2006.01)	G06F	21/24	166B	
H04L 9/14	(2006.01)	G06F	21/24	166E	
		H04L	9/00	601C	
		H04L	9/00	641	

審査請求 未請求　予備審査請求 未請求　（全 37 頁）

(21)出願番号　特願2013-511233 (P2013-511233)
(86)(22)出願日　平成23年5月13日 (2011.5.13)
(85)翻訳文提出日　平成24年11月30日 (2012.11.30)
(86)国際出願番号　PCT/US2011/036368
(87)国際公開番号　WO2011/146325
(87)国際公開日　平成23年11月24日 (2011.11.24)
(31)優先権主張番号　13/092,758
(32)優先日　平成23年4月22日 (2011.4.22)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/346,819
(32)優先日　平成22年5月20日 (2010.5.20)
(33)優先権主張国　米国 (US)

(71)出願人　512300148
アブシオ　コーポレイション
ＡＢＳＩＯ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国　８０１２７－６４２５
コロラド州　リトルトン　サウス　サングレ　デ　クリスト　ロード　８３２１　スイート　３０２
(74)代理人　100068755
弁理士　恩田　博宣
(74)代理人　100105957
弁理士　恩田　誠
(74)代理人　100142907
弁理士　本田　淳

最終頁に続く

(54)【発明の名称】コンテンツを提供するための方法および装置

(57)【要約】
コンテンツが安全かつ便利に許可されたユーザに配信されるようにするための方法およびシステムが提供される。さらに詳細には、コンテンツは、送信および受信デバイス上で暗号化形式で、転送中に保持される。加えて、コンテンツの使用、アクセス、および配信に関連するポリシーが実施されてもよい。ユーザに関連する情報の公開を制御するための機能も提供される。コンテンツの配信および制御は、コンテンツを提示してキーを管理するクライアント・アプリケーションに関連して実行されてもよい。

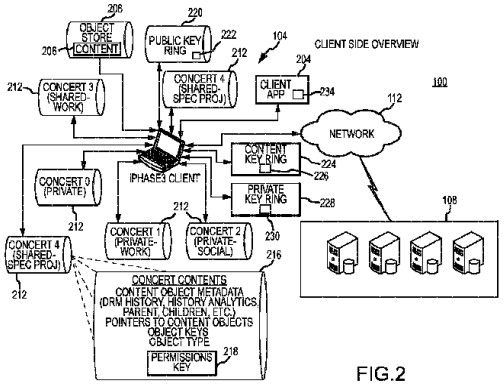


FIG.2

【特許請求の範囲】
【請求項１】
コンテンツを配信するための方法であって、
第１のコンテンツを第１のデバイス上に作成すること、
第１のコンテンツ・キーを使用して該第１のコンテンツを暗号化すること、
暗号化された第１のコンテンツを該第１のデバイスに格納すること、
該第１のコンテンツの第１の受信者を識別すること、
該第１の受信者の公開キーを使用して、暗号化された第１のコンテンツ、第１のコンテンツ・キー、および第１のコンテンツに関連する第１の情報を暗号化すること、
通信ネットワークを介して、暗号化された第１のコンテンツ、第１のコンテンツ・キー、および第１のコンテンツに関連する少なくとも第１の情報を第２のデバイスに配信すること
を備える方法。
【請求項２】
第２のコンテンツを前記第１のデバイス上に作成すること、
第２のコンテンツ・キーを使用して該第２のコンテンツを暗号化すること
をさらに備える、請求項１に記載の方法。
【請求項３】
前記暗号化された第１のコンテンツ、第１のコンテンツ・キー、および第１のコンテンツに関連する少なくとも第１の情報を前記第２のデバイスにおいて受信すること、
前記第２のデバイスで動作しているクライアント・アプリケーションを使用して、前記第１の受信者の秘密キーを少なくとも第１のコンテンツ・キーに適用すること、
前記第１の受信者の秘密キーを前記暗号化された第１のコンテンツ・キーに適用した後、該クライアント・アプリケーションを使用して前記第１のコンテンツ・キーを適用して、前記第１のコンテンツにアクセスし、該クライアント・アプリケーションを使用して、前記第１のコンテンツに関連する情報を前記第２のデバイスに表示すること
をさらに備える、請求項１に記載の方法。
【請求項４】
前記暗号化された第１のコンテンツ、第１のコンテンツ・キー、および第１のコンテンツに関連する少なくとも第１の情報を前記第２のデバイスにおいて受信すること、
前記第２のデバイスで動作しているクライアント・アプリケーションを使用して、前記第１の受信者の秘密キーを前記暗号化された第１のコンテンツ・キーに適用し、暗号化されていない第１のコンテンツ・キーを使用して、暗号化された第１のコンテンツおよび前記第１のコンテンツに関連する少なくとも第１の情報にアクセスすること、
前記暗号化された第１のコンテンツを前記第２のデバイス上のオブジェクト・ストアに格納すること、
前記暗号化された第１のコンテンツ・キーを前記第２のデバイス上のキー・リングに格納すること
をさらに備える、請求項１に記載の方法。
【請求項５】
前記暗号化された第１のコンテンツ、第１のコンテンツ・キー、および第１のコンテンツに関連する少なくとも第１の情報を前記第２のデバイスにおいて受信すること、
第１のシステム復号キーを前記第２のデバイスで受信すること
をさらに備える、請求項４に記載の方法。
【請求項６】
クライアント・アプリケーション・プログラミングおよび前記第２のデバイス上の第１の許可復号キーを使用して、前記第１のコンテンツ・キーを前記暗号化された第１のコンテンツに適用すること、
前記第１のコンテンツを前記第２のデバイスに表示すること
をさらに備える、請求項５に記載の方法。

【請求項７】
前記暗号化された第１のコンテンツを前記第２のデバイスに配信することをさらに備え、前記暗号化された第１のコンテンツは、コンテンツ・システム・サーバを通じて前記第２のデバイスに配信される、請求項１に記載の方法。
【請求項８】
コンテンツを配信するためのシステムであって、
第１のデバイスと、
該第１のデバイスで動作しているクライアント・アプリケーションと、
該第１のデバイスに関連付けられている第１のデータ・ストレージと、
該第１のデバイスの第１のデータ・ストレージに格納された第１の暗号化された文書と、
該第１のデバイスの第１のデータ・ストレージに第１のコンテンツ・キー・リングの一部として格納された該第１の暗号化された文書を復号するための第１のコンテンツ・キーであって、第１のクライアント・アプリケーションは、該第１のキーが該第１の暗号化された文書を復号するために使用されるようにし、該第１のコンテンツ・キー・リングの一部として格納された該第１の暗号化された文書を復号するための該第１のキーは、該第１のデバイスのユーザにより直接アクセスされることができない、前記第１のコンテンツ・キーと
を備えるシステム。
【請求項９】
前記第１のデバイスに関連付けられているディスプレイをさらに備え、前記第１の暗号化された文書は、前記第１の文書を復号するために前記第１のコンテンツ・キーを使用する前記第１のクライアント・アプリケーションを通じて該ディスプレイに提示されることが可能である、請求項８に記載のシステム。
【請求項１０】
前記第１のクライアント・アプリケーションに関連付けられている第１の情報の少なくとも一部は、前記第１のコンテンツ・キーを適用することなく前記ディスプレイ上に提示されることが可能である、請求項９に記載のシステム。
【請求項１１】
通信ネットワークと、
第１のクライアント・デバイス上の第１の通信インターフェイスであって、該通信ネットワークに動作可能に相互接続された前記第１の通信インターフェイスと
をさらに備え、前記第１のデバイスは該通信ネットワークを介した配信のための文書パッケージを作成するように動作可能であり、該文書パッケージは、前記第１の暗号化された文書、および前記第１の文書を復号するために使用される前記第１のキーを含み、少なくとも前記第１のキーは、第１の受信者公開キーにより暗号化されている、請求項８に記載のシステム。
【請求項１２】
前記第１のデバイスに関連付けられている第２のデータ・ストレージをさらに備え、前記クライアント・アプリケーションは、前記第１のデータ・ストレージに格納され、前記第１の暗号化された文書は、該第２のデータ・ストレージに格納されている、請求項１１に記載のシステム。
【請求項１３】
第２のデバイスと、
該第２のデバイスで動作しているクライアント・アプリケーションと、
該第２のデバイスに関連付けられている第１のデータ・ストレージと、
前記第１のデバイスの第１のデータ・ストレージに格納された第１の暗号化された文書と、
該第２のデバイスの第１のデータ・ストレージに第１のコンテンツ・キー・リングの一部として格納された第１の暗号化された文書を復号するための第１のコンテンツ・キーと

をさらに備え、該第２のデバイス上のクライアント・アプリケーションは、該第１のキーが該第１の暗号化された文書を復号するために使用されるようにし、該第１のコンテンツ・キー・リングの一部として格納された第１の暗号化された文書を復号するための第１のキーは、該第２のデバイスのユーザにより直接アクセスされることができない、請求項１１に記載のシステム。

【請求項１４】

コンテンツを配信するための方法であって、

第１の暗号化されたコンテンツを含む第１のデータラッパを第１のコンピュータにおいて受信すること、

該第１のコンピュータで動作している第１のコンピュータ・プログラミングを使用して第１のユーザキーを適用することであって、該第１の暗号化されたコンテンツは該ラッパから取り除かれる、前記第１のユーザキーを適用すること、

該第１のコンピュータで動作している第１のコンピュータ・プログラミングを使用して第１のコンテンツ・キーを適用することであって、該第１の暗号化されたコンテンツは復号されて第１の復号されたコンテンツを形成する、前記第１のコンテンツ・キーを適用すること

を備える方法。

【請求項１５】

前記第１の復号されたコンテンツは、第１のクライアント・アプリケーションを通じて前記第１のコンピュータのユーザに使用可能である、請求項１４に記載の方法。

【請求項１６】

第１のクライアント・アプリケーションは、第１の復号された文書へのアクセスを制御する、請求項１４に記載の方法。

【請求項１７】

前記第１の復号された文書へのアクセスは、前記第１の復号された文書の表示、前記第１の復号された文書の転送、前記第１の復号された文書の変更、前記復号された文書からの引用のうちの少なくとも１つを含む、請求項１６に記載の方法。

【請求項１８】

前記第１のデータラッパは、文書メタデータを付加的に含み、該文書メタデータの少なくとも一部は、第１の許可キーの前記ラッパへの適用後、および前記第１のコンテンツ・キーのラッパコンテンツへの適用前にアクセス可能である、請求項１４に記載の方法。

【請求項１９】

受信者コンピュータにおいて前記第１のコンテンツを受信することをさらに備え、前記第１のコンテンツ・キーは、前記第１のデータラッパが前記受信者コンピュータにより受信される場合に前記受信者コンピュータにより受信される、請求項１４に記載の方法。

【請求項２０】

第２のデータラッパで、前記第１の暗号化されたコンテンツを前記第１のコンピュータから第２のコンピュータに転送することであって、前記第１のコンテンツ・キーは、該第２のデータラッパのコンテンツに含まれていない、前記転送すること、

前記第２のコンピュータにおいて第３のデータラッパを受信することであって、該第３のデータラッパは、前記第１のコンテンツ・キーを含み、該第３のデータラッパは、コンテンツ・システム・サーバにより前記第２のコンピュータに提供される、前記受信すること

をさらに備える、請求項１４に記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

コンテンツを提供するための方法および装置が提供される。さらに詳細には、コンテンツが通信ネットワーク上で安全に提供されるようにするための方法およびシステムが提供される。

【背景技術】
【０００２】
インターネットは、コンテンツの配信手段を続々と提供するようになっている。しかし、インターネットは本質的にセキュリティ保護されてはいない。その結果、コンテンツ・プロバイダが、特に、集合的にワールド・ワイド・ウェブ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）または単に「ウェブ」として知られるインターネット上で実行するアプリケーションおよびサービスを使用して、インターネット上で配信されるコンテンツに対する報酬を得ることは困難であった。たとえば、従来の新聞発行者を含む発行者は、一般にコンテンツにアクセスするためのサブスクリプション料金の支払いを要求する課金の壁（ｐａｙ　ｗａｌｌ）を構築しているが、そのような壁は通常、難なく回避されてしまうこともある。さらに、許可ユーザが、合法的にアクセスされるコンテンツを容易に作成して配信することができるので、正当なコピーから作成された違法コピーが一般に利用可能である。したがって、若干の例外はあるものの、従来の発行者は、インターネット上で入手可能になるコンテンツに関連して報酬を得ることに、思わしい成果を上げることができなかった。
【０００３】
サブスクリプションの仕組みの代替として、コンテンツの提供を貨幣化するための他のメカニズムが開発されてきた。たとえば、広告にサポートされるコンテンツは、インターネットで一般に利用可能である。広告サポートのコンテンツに関する１つの問題は、コンテンツに関連付けられている広告に価値を割り当てることであった。たとえば、広告は、広告対象となる商品およびサービスの購入者と見込まれる人々に向けられることが望ましい。しかし、広告対象となる商品およびサービスの消費者を正確に絞り込むためには、消費者のニーズと要望に関する情報が必要となる。この情報は、ユーザが入力した検索語および／またはユーザが視聴したコンテンツから推測することができる。インターネット・サービス・プロバイダはまた、加入者電子メールを分析してプロファイルを作成して、それを広告主に販売することも、消費者の絞り込みに使用することもできる。さらに、検索語、視聴されたコンテンツ、およびユーザのニーズまたは要望を示すその他のデータは、時間の経過と共に、広告主または関連エンティティにより蓄積されてゆく。しかし、個人情報をそのように使用することは、多くの場合、好ましくないと見なされる。
【０００４】
インターネット・アクティビティにプライバシーおよびセキュリティをもたらすため、さまざまなセキュリティ・アプリケーションおよび手順を適用することができる。しかし、セキュリティ・アプリケーションの使用は任意であって、ウェブ上に広く普及してはいない。加えて、通常実施されているセキュリティでは、キーの数が不十分であり、その結果として、１つのキーの解読が、往々にして、膨大量のデータへのアクセスにつながるおそれもある。加えて、たとえ暗号化が適用されていたとしても、そのような暗号化は孤立させられている。たとえば、データが、クラウドとエンド・ユーザのコンピュータの両方に暗号化されていない形態で格納されることも頻繁に行なわれている。加えて、たとえば個人情報の公開を防止または制限するためのセキュリティ機能のアプリケーションは、そのような機能の動作が情報へのフリーアクセスを前提としているので、ウェブの多くの機能を利用できなくするおそれがある。したがって、インターネット上のプライバシーおよびセキュリティが相対的に欠如していることは依然として問題であり、コンテンツの電子配信に悪影響を及ぼしている。
【発明の概要】
【課題を解決するための手段】
【０００５】
本発明の実施形態は、たとえ安全ではないネットワーク上であっても、コンテンツが、許可されたユーザに安全かつ便利に配信されるようにするための方法およびシステムを提供することを対象とする。本発明の実施形態によれば、クライアント・アプリケーションは、コンテンツのコレクション、およびそのコンテンツにアクセスするために必要なキーを管理するために提供される。本発明のさらなる実施形態によれば、クライアント・アプ

リケーションは、コンテンツの項目に関連するアクセス制御を実施することに関与する。そのような制御により、コンテンツ・プロバイダは、コンテンツへのアクセスをそのようなアクセスの受け入れ対価に条件付けること、および／またはコンテンツの使用とアクセスに関連するその他のポリシーを実施することができるようになる。さらに、本発明の実施形態により、コンテンツへのさまざまなレベルのアクセスがさまざまなユーザに提供されるようになり、さらには、さまざまな条件でさまざまなユーザがコンテンツを利用できるようになる。

【０００６】

本発明の実施形態によるシステムは、インターネットのような通信ネットワークを介してクライアント・デバイスに接続されたサーバ側コンポーネントを含む。サーバ側コンポーネントは、コンテンツが格納されるストレージデバイスを含むことができる。システムは、同期化、コンテンツ管理、認証、マッチメーク、分類形成、課金、およびその他の機能を含む、さまざまな機能を実行するためのエージェントまたはモジュールを含むことができる。システムに含まれるクライアント・デバイスは、クライアント・アプリケーションを特徴付ける。クライアント・アプリケーションはインターフェイスを提供し、そのインターフェイスを通じてユーザは利用可能なコンテンツにアクセスする。さらに、クライアント・アプリケーションは、コンテンツ・オブジェクトに関するメタデータ、コンテンツの取り出しまたは更新のための情報、もしくはターゲット広告を含むユーザへのその他の情報を保持する。１つの態様において、クライアント・アプリケーションは、暗号化されたコンテンツへのアクセスを可能にするキーを含む１つまたは複数のキー・リングを保持して管理する。

【０００７】

本発明の実施形態による方法は、コンテンツを暗号化形式で受信側クライアント・デバイスに配信することを含む。さらに詳細には、ユーザが文書またはその他のコンテンツを作成する場合、新しい暗号キー、特にコンテンツ・キーが、その文書を暗号化するために適用される。次いで、文書は、暗号化形式で作成者のクライアント・デバイスに格納される。加えて、文書に関連するメタデータは、コンテンツ暗号キーを使用して暗号化されてもよい。作成者が、コンテンツを別のユーザに提供することを決定する場合、文書に関連付けられている暗号化済みまたは暗号化されていないヘッダおよびメタデータ情報は、許可キーを使用して暗号化されてもよい。次に、文書の受信者が識別され、受信者の公開キーが要求される。次いで、許可キーおよびコンテンツ・キーは、受信者の公開キーにより暗号化される。次いで、受信者は、暗号化されたコンテンツ、暗号化されたコンテンツ・キー、コンテンツに関連するメタデータ、および関連付けられているコンテンツおよび許可キーを含む、文書パッケージのコピーを提供される。コンテンツが複数の受信者に提供される場合、受信者ごとに別個の文書パッケージが作成され、個別の文書パッケージは各々受信者の公開キーを使用して暗号化されている。

【０００８】

クライアント・デバイスにおいてコンテンツが受信されると、受信者の秘密キーは、受信者の公開キーを使用して作成されたラッパから配信データを取り除くために適用される。暗号化された文書は、クライアント・デバイス上のオブジェクト・ストアに格納される。さらに詳細には、暗号化されたコンテンツ、メタデータ、およびコンテンツの許可キーを含むコンテナは、オブジェクト・ストアに格納される。コンテンツ・キーは、クライアント・デバイス上でクライアント・アプリケーションによって保持されるキー・リングに追加される。このキー・リングは、本明細書においてコンサートとも呼ばれる、データ・オブジェクトの特定のコレクションに関連付けられてもよい。したがって、コンテンツが、暗号化形式でクライアント・デバイスに配信されることが理解されうる。加えて、コンテンツが、暗号化形式でクライアント・デバイスに格納されることが理解されうる。本発明のさらなる実施形態によれば、クライアント・デバイスのユーザは、暗号化されたコンテンツに関連付けられているキー・リング、またはそのキー・リングの個々のキーには直接アクセスすることができない。その代わり、キー・リングのキーへのアクセスは、ユー

ザの秘密キーを保持するクライアント・アプリケーションを通じてしか行なうことができない。秘密キーへの直接アクセスは、クライアント・アプリケーションおよびクライアント側システム・キーにより妨げられる。したがって、コンテンツの報酬を伴わない配信を防止または制限するポリシーを含む、暗号化されたコンテンツに関して作成者および／または発行者により確立されたポリシーが実施されてもよい。

【０００９】

クライアント・デバイス上のコンサートに含まれるコンテンツにアクセスするため、クライアント・アプリケーションは、サブジェクトコンサートのクライアント側システム・キーを適用して、そのコンサートのキー・リングの一部として格納されている必要なコンテンツ・キーにアクセスする。クライアント側システム・キーは、ユーザの秘密キーで保護されている対称キーであってもよい。さらに、ユーザは、そのユーザのコンサート・キー・リングにアクセスするために使用されるクライアント側システム・キーを認識している必要はない。次いで、コンテンツ・キーは、コンテンツ、および任意のヘッダ情報、またはコンテンツ・キーを使用して暗号化されたその他のメタデータを復号するために、クライアント・アプリケーションにより適用されてもよい。次いで、暗号化されたコンテンツおよびその他の情報は、クライアント・アプリケーションを通じてクライアント・デバイスのユーザに表示されてもよい。クライアント・デバイスのユーザはコンテンツ・キーを使用可能にすることができるが、ユーザはそのキーに直接アクセスすることはできない。加えて、ユーザはコンテンツ・キーを管理する必要はない。

【００１０】

本発明の実施形態のさらなる他の態様によれば、コンテンツまたはコンテンツに関連するメタデータの少なくとも一部は、暗号化されていない形式で入手可能であってもよい。たとえば、文書またはその他のコンテンツの概要、および文書の作成者および／または発行者を識別する情報から成るメタデータは公開されてもよい。公開されているデータであっても、システムによく知られているキーを使用して暗号化形式で格納されてもよい。公開されている情報を表示した後、ある人物が文書の完全なコピーを入手することに関心を持つ場合、その人物は適切な支払いまたはその他の対価を手配し、それと引き換えにそのコンテンツのアクセス権を受け取ることができる。

【００１１】

本開示の追加の利点および特徴は、特に添付の図面と併せて、後段の説明を読むことでさらに容易に明らかとなろう。

【図面の簡単な説明】

【００１２】

【図１】本発明の実施形態によるコンテンツを提供するためのシステムの要素を示す図。

【図２】本発明の実施形態によるコンテンツを提供するためのシステムのその他の要素を示す図。

【図３】本発明の実施形態によるコンテンツを提供するためのシステムのコンポーネントを示すブロック図。

【図４】本発明の実施形態による文書を作成するための方法の態様を示す図。

【図５】本発明の実施形態による文書を読み取るための方法の態様を示す図。

【図６】本発明の実施形態による文書を転送するための方法の態様を示す図。

【図７】本発明の実施形態による暗号キーを要求するための方法の態様を示す図。

【図８】本発明の実施形態による文書を組み立てるための方法の態様を示す図。

【図９】本発明の実施形態によるコンサート・キー・リングのキーを生成するための方法を示す図。

【図１０】本発明の実施形態によるコンテンツにアクセスするために実施されうるセキュリティ手順を示す図。

【図１１】本発明の実施形態によるコンテンツにアクセスするために実施されうるセキュリティ手順を示す図。

【図１２】本発明の実施形態によるコンテンツにアクセスするために実施されうるセキュ

リティ手順を示す図。
【図１３】本発明の実施形態によるコンテンツにアクセスするために実施されうるセキュリティ手順を示す図。
【図１４】本発明の実施形態によるコンサート情報を格納するためのオプションを示す図。
【図１５】本発明の実施形態によるコンサート情報を格納するためのオプションを示す図。
【図１６】本発明の実施形態によるコンサート情報を格納するためのオプションを示す図。
【図１７】本発明の実施形態によるコンサート情報を格納するためのオプションを示す図。
【図１８】本発明の実施形態によるコンサート情報を格納するためのオプションを示す図。
【図１９】本発明の実施形態による例示的なシステムアーキテクチャを示す図。
【図２０】本発明の実施形態によるユーザ・インターフェイスの例を示す図。
【発明を実施するための形態】
【００１３】
図１は、本発明の実施形態によるコンテンツを提供するためのシステム１００の態様を示す。一般に、システム１００は、通信ネットワーク１１２によりコンテンツ・システム・サーバ１０８に相互接続された１つまたは複数のクライアント・デバイス１０４を含む。クライアント・デバイス１０４は、本明細書の他の箇所においてさらに詳細に説明されるように、ラップトップまたはデスクトップ・パーソナル・コンピュータのような汎用コンピュータを備えることができるが、これらに限定されることはない。通信ネットワーク１１２は、インターネットを含む１つまたは複数のネットワークを備えることができる。コンテンツ・システム・サーバ１０８は、通信ネットワーク１１２上のクライアント・デバイス１０４へのコンテンツの提供をサポートして機能を実行する１つまたは複数のデバイスを備えることができる。
【００１４】
さらに詳細には、本発明の実施形態によるコンテンツ・システム・サーバ１０８は、１つまたは複数のファイアウォール１１６、ゲートウェイ１２０、エッジ・サーバクラスタ１２４、およびコア・サーバ１２６を含むことができる。コンテンツ・システム・サーバ１０８の一部として提供されるエッジ・サーバクラスタ１２４および／またはコア・サーバ１２６は、１つまたは複数のデータベース１２８、データ・ウェアハウス／レポーティング・エンジンまたはモジュール１３２、および会計データ収集エンジンまたはモジュール１３６を含むことができる。コンテンツ・システム・サーバ１０８は、分析１４０、会計１４４、および顧客対応１４８エンジンまたはモジュールを付加的に含むことができる。コンテンツ・システム・サーバ１０８のさまざまなコンポーネントが相互接続されたハードウェアの別個の要素として図１に示されているが、本発明の実施形態がそのような構成に限定されないことを理解されたい。たとえば、コンテンツ・システム・サーバ１０８は、１つまたは少数のサーバコンピュータデバイスを使用して実施されてもよい。コンテンツ・システム・サーバ１０８はまた、多数の異なるデバイス間で分散されてもよく、コンテンツ・システム・サーバ１０８により実行されるさまざまな機能は、そのようなデバイス間で分散されてもよく、コンテンツ・システム・サーバ１０８を構成するデバイスは、さまざまな場所に分散されてもよい。
【００１５】
図２は、本発明の実施形態によるコンテンツ配信システム１００のもう１つの図を示し、特にクライアント・デバイス１０４の追加の態様を示す。クライアント・デバイス１０４は、クライアント・アプリケーションまたはコンサート・アプリケーション２０４を実行する。クライアント・アプリケーション２０４は、通信ネットワーク１１２を介してコンテンツ・システム・サーバ１０８からコンテンツを取り出して、そのコンテンツにアク

セスできるようにし、そのコンテンツに関連付けられているルールを実施するように機能することができる。クライアント・アプリケーション２０４はまた、クライアント・デバイス１０４から、その他のクライアント・デバイス１０４および／またはコンテンツ・システム・サーバ１０８に配信するためのコンテンツを準備するように機能することもできる。クライアント・アプリケーション２０４はまた、クライアント・デバイス１０４に関連付けられているユーザに関する人口統計情報、クライアント・デバイス１０４に関連付けられているユーザの関心、またはその他の個人情報のような、情報の収集および公開を制御することもできる。本発明の実施形態によれば、コンテンツは、クライアント・デバイス１０４上、またはクライアント・デバイス１０４に関連付けられているオブジェクト・ストア（ｓｔｏｒｅ）２０８に保持されてもよい。さらに、本発明の実施形態によれば、および本明細書の他の箇所においてさらに詳細に説明されるように、コンテンツ２０６は暗号化形式でオブジェクト・ストア２０８に格納される。コンテンツ２０６は、本明細書においてコンサート２１２と称される、１つまたは複数のグループ分けの一部としてオブジェクト・ストア２０８に保持されてもよい。さらに、コンテンツ２０６へのアクセスは、関連するコンサート（ｃｏｎｃｅｒｔ）２１２を通じて行なわれてもよい。各コンサート２１２は、コンテンツ・オブジェクト・メタデータ（たとえば、デジタル著作権管理（ＤＲＭ：ｄｉｇｉｔａｌ　ｒｉｇｈｔｓ　ｍａｎａｇｅｍｅｎｔ）情報、親オブジェクト、子オブジェクトの履歴、分析、識別情報など）、コンテンツ・オブジェクトを指すポインタ、許可キー２１８、オブジェクト・キー、オブジェクト・タイプ情報のような、さまざまな情報またはコンサート・コンテンツ２１６を含むことができる。各コンサート２１２はまた、アクセス・キーに関連付けられており、アクセス・キーはクライアント側システム２３４の形態であってもよい。加えて、さまざまなコンサート２１２は、コンテンツ２０６の同一項目をアクセスまたは共有することができる。

【００１６】

クライアント・デバイス１０４はまた、公開キー・リング２２０、１つまたは複数のコンテンツ（コンサート）・キー・リング２２４、および秘密キー・リング２２８も含む。公開キー・リング２２０は、クライアント・デバイス１０４が、他のクライアント・デバイス１０４またはコンテンツ・システム・サーバ１０８に送信される情報を暗号化するために使用する公開キーまたは暗号キー２２２を保持することができる。公開キー２２２は、クライアント・デバイス１０４により要求されると、コンテンツ・システム・サーバ１０８によりクライアント・デバイス１０４に配信されてもよい。コンテンツ・キー・リング２２４は暗号化されてもよく、オブジェクト・ストア２０８で保持されるコンテンツ２０６の項目を復号するためのアクセスまたはコンテンツ・キー２２６を備えることができる。クライアント・デバイス１０４に関連付けられている複数のコンテンツ・キー・リング２２４がある場合、異なるコンテンツ・キー・リング２２４は、それらが関連するコンサート２１２に従ってグループ分けされるコンサート・キー・リングを備えることができる。秘密キー・リング２２８は、対応する公開キーを使用して、クライアント・デバイス１０４に送信されるメッセージを復号するために必要な秘密キー２３０を含むことができる。本発明の実施形態によれば、クライアント・デバイス１０４のユーザは、コンテンツ・キー・リング２２４で保持されるコンテンツ・キー２２６、または秘密キー・リング２２８で保持される秘密キー２３０には直接アクセスすることができない。その代わり、コンテンツ・キー・リング２２４および秘密キー・リング２２８は、クライアント・アプリケーション２０４のみがアクセスすることができる隠しキーまたはシステム・キー２３４を使用して暗号化され、アクセスされる。したがって、コンテンツ・キー・リング２２４および秘密２２８キー・リングへのアクセスは、クライアント・アプリケーション２０４を通じて行なわれる必要があり、それにより作成者、発行者、または他の権限により確立されたコンテンツ２０６の配信および／または使用に関するポリシーが実施されるようにする。さらに、クライアント側システム・キーは、ユーザの秘密キーにより保護されている対称キーであってもよい。

【００１７】

図３は、本発明の実施形態によるコンテンツを提供するためのシステム１００のコンポーネントを示すブロック図である。さらに詳細には、クライアント・デバイス１０４およびコンテンツ・システム・サーバ１０８の追加のコンポーネントが示される。一般に、クライアント・デバイス１０４は、汎用コンピュータ、スマートフォン、または通信ネットワーク１１２上の通信をサポートすることができ、クライアント・アプリケーション２０４の適切なバージョンを実行することができるその他のデバイスを備えることができる。サーバ・システム１０８は、通信ネットワーク１１２上で通信することができ、適切なサーバ・アプリケーション３０２を実行することができる１つまたは複数のサーバコンピュータを備えることができる。一般に、クライアント・デバイス１０４およびサーバ・システム１０８は、プロセッサ３０４、メモリ３０８、データ・ストレージ３１２、および通信またはネットワーク・インターフェイス３１６を含む。加えて、クライアント・デバイス１０４および／またはサーバ・システム１０８は、キーボードおよびポインティング・デバイスのような、１つまたは複数のユーザ入力デバイス３２０、およびディスプレイおよびスピーカのような、１つまたは複数のユーザ出力デバイスを含むことができる。

【００１８】

プロセッサ３０４は、ソフトウェアまたはファームウェアで符号化された命令を実行することができる任意のプロセッサを含むことができる。本発明のその他の実施形態によれば、プロセッサ３０４は、コントローラ、もしくは論理回路で符号化された命令を有するかまたは実行することができる特殊用途向け集積回路（ＡＳＩＣ）を備えることができる。メモリ３０８は、プログラム、またはコンテンツ２０６を備えるデータを含むデータを格納するために使用されてもよい。例として、メモリ３０８は、ＲＡＭ、ＳＤＲＡＭ、またはその他のソリッドステートメモリを備えることができる。あるいは、または加えて、データ・ストレージ３１２が提供されてもよい。データ・ストレージ３１２は、一般に、プログラムおよびデータのためのストレージを含むことができる。たとえば、データ・ストレージ３１２は、さまざまなデータおよびアプリケーションを格納することができる。たとえば、クライアント・デバイス１０４に関して、データ・ストレージ３１２は、クライアント・アプリケーション２０４、オブジェクト・ストア２０８、コンサート２１２およびコンサート・コンテンツ２１６、ならびに公開キー・リング２２０のためのストレージを提供することができる。クライアント・デバイス１０４に関連付けられているデータ・ストレージ３１２はまた、コンテンツ・キー・リング２２４、およびクライアント・デバイス１０４の秘密キー・リング２２８も提供することができる。加えて、オペレーティング・システム３２８命令、電子メール・アプリケーション３３０、その他の通信アプリケーション３３２、またはその他のアプリケーションおよびデータが、データ・ストレージ３１２に格納されてもよい。サーバ・システム１０８に関連付けられているデータ・ストレージ３１２は、コンテンツ・データベース１２８、データ・ウェアハウス１３２、分析情報１４０、会計情報１４４、ならびに、たとえばコンテンツ２０６、ユーザ情報、およびその他の情報の格納と編成に関連して使用するためのさまざまな索引３３４を含むことができる。サーバ・システム１０８オペレーティング・システム３２８に関連する命令はまた、サーバ・システム１０８のデータ・ストレージ３１２に格納されてもよい。

【００１９】

データ・ストレージ３１２は、１つまたは複数の内部ハードディスク・ドライブ、または論理パーティションのような、固定のデータ・ストレージを備えることができる。さらにその他の実施形態によれば、外部データ・ストレージ３３６は、たとえば通信インターフェイス３１６を介して、クライアント・デバイス１０４に相互接続されてもよい。外部データ・ストレージ３３６は、システム１００アプリケーション、および特定のユーザに関連付けられているデータの一部または全部のためのデータ・ストレージを提供することができる。したがって、外部データ・ストレージ３３６は、クライアント・アプリケーション２０４、オブジェクト・ストア２０８、コンサート２１２およびコンサート・コンテンツ２１６、キー・リング２２０、２２４、２２８および／または任意の他のアプリケーションまたはデータを格納するために提供することができる。外部データ・ストレージ３

３６の特定の例は、外部ハードディスク・ドライブ、フラッシュ・ドライブを含むＵＳＢ（ｕｎｉｖｅｒｓａｌ　ｓｅｒｉａｌ　ｂｕｓ）ドライブ、またはその他の外部データ・ストレージまたはメモリデバイスを含む。

【００２０】

図４は、本発明の実施形態による、この例では文書であるコンテンツ２０６を作成するための方法の態様を示す流れ図である。工程４０４において、ユーザ、たとえばクライアント・デバイス１０４のユーザは、文書またはその他のコンテンツ２０６を作成する。コンテンツが送信の準備が整っているか、または少なくとも部分的に作成された場合、新しいコンテンツ暗号キー２２６が要求される（工程４０８）。工程４１２において、文書は組み立てられる。文書の組み立ては、ヘッダ情報を文書に関連付けることを含むことができる。本発明の実施形態によれば、ヘッダ情報の一部は、文書のコンテンツと共に暗号化されてもよいが、ヘッダデータのその他の部分は、文書コンテンツに適用されるコンテンツ・キー２２６を使用しては暗号化されない。文書がその他のユーザに送信される場合、それらのその他のユーザの公開暗号キー２２２が要求される。必要なキー（複数可）２２２または２２６を取得した後、文書は暗号化される（工程４２０）。

【００２１】

工程４２４において、作成された文書はコンサート２１２に追加される。特に、コンテンツ・オブジェクト・メタデータは、文書が割り当てられるコンサート（複数可）２１２に追加される。加えて、工程４０８で要求されたコンテンツ・キー２２６は、ユーザのコンテンツ・キー・リング２２４に追加される（工程４２８）。工程４３２において、暗号化された文書は、格納および／または配信のためにキューに入れられる。本発明の実施形態によれば、文書およびその他のコンテンツは、暗号化形式でオブジェクト・ストア２０８に格納される。したがって、格納は、コンテンツ・キー２２６を使用して暗号化された文書を、クライアント・デバイス１０４に関連付けられているデータ・ストレージ３１２に格納することを含むことができる。本明細書の他の箇所においてさらに詳細に説明されるように、別のクライアント・デバイス１０４またはサーバデバイス１０８に送信される文書の場合、コンテンツ・キー２２６は、受信者（ｒｅｃｉｐｉｅｎｔ）の公開キー２３０を使用して暗号化される。次いで、暗号化されたコンテンツ２０６、暗号化されたコンテンツ・キー２２６、およびヘッダまたはその他の情報（受信者デバイス１０４および／または１０８のユーザの公開キー２３０を使用して暗号化されてもよい）を備える文書パッケージ、文書に関連付けられているメタデータ（許可キー２１８および／またはコンテンツ・キー２２６で復号または暗号化される）、許可キー２１８、および暗号化されたコンテンツ・キー２２６は、たとえばパブリックネット・ワークにわたり、受信者デバイスに配信されてもよい。

【００２２】

図５は、本発明の実施形態による文書またはその他のコンテンツ２０６を読み取るための方法の態様を示す。最初に、工程５０４において、文書を開くための命令が受信される。開かれる文書は、初めて開かれる文書であってもよいか、または以前アクセスされた文書を開くために使用されているクライアント・デバイス１０４上のコンサート２１２内の既存の文書であってもよい。工程５０８において、文書が以前表示されたことがあるかどうかについて決定が行なわれる。文書が以前表示されたことがある場合、クライアント・アプリケーション２０４は、文書を含むコンサート２１２のコンサート・キー・リング２２４にその文書のコンテンツ・キー２２６を要求する（工程５１２）。特に、以前表示されたことのある文書の場合、クライアント・デバイス１０４上のコンテンツの復号は、クライアント・アプリケーション２０４が許可キー２１８にアクセスするためにユーザの秘密キー２３０を適用することを含み、それによりコンテンツ・キー・リング２２４に含まれる必要なコンテンツ・キー２２６にアクセスできるようになる。文書が以前表示されたことがない場合、アクセス可能な情報は、ユーザの秘密キー２２２２を使用して復号される（工程５１６）。文書のコンテンツ・キー２２６は、クライアント・アプリケーション２０４から抽出され、コンテンツ・キー・リング２２４に追加され、メタデータおよび許

可（関連する許可キー２１８により確立される）は、コンサート情報２１６の一部として含まれるコンテンツ特性ストアに格納される（工程５２０）。したがって、ヘッダからコンテンツ・キー２２６を抽出するか、またはコンテンツ・キー・リング２２４からコンテンツ・キー２２６を取得するかどうかにかかわりなく、クライアント・アプリケーション２０４は、ユーザの秘密キー２３０を適用することが要求されてもよい。文書ヘッダ情報からコンテンツ・キー２２６を抽出した後、またはコンテンツ・キー・リング２２４からコンテンツ・キー２２６を取得した後、クライアント・アプリケーションは、メモリ内の文書を復号するために、必要なコンテンツ復号キー２２６を適用する（工程５２４）。復号化に続いて、メモリ内のコンテンツ・キー２２６は上書きされ（工程５２８）、文書はクライアント・アプリケーション２０４により表示される（工程５３２）。文書のアクセスおよび表示はクライアント・アプリケーション２０４を通じて行なわれるので、文書に関してユーザが行なうことができるアクションは、文書に関連付けられている許可に決定されるとおり制限されてもよい。

【００２３】

工程５３６において、文書が保存されるべきであるかどうかについて決定が行なわれる。文書が保存されるべきではない場合、メモリは上書きされ、コンテンツ・キー２２６はコンテンツ・キー・リング２２４から削除され、コンテンツ２０６に関連付けられているメタデータおよび許可はコンサート・コンテンツまたは特性ストア２１６から削除され、文書に関連するその他のコンサートオブジェクトメタデータは削除される（工程５４０）。文書が保存されるべきである場合、文書のコンテンツ・キー２２６がコンテンツ・キー・リング２２４に要求され（工程５４４）、文書はメモリに暗号化される（工程５４８）。次いで、暗号化された文書は、オブジェクト・ストア２０８に保存または再保存される（工程５５２）。工程５５６において、文書に関連するメタデータは更新される。次いで、文書の暗号化されていないバージョンまたは部分をメモリから除去するために、メモリは上書きされる（工程５６０）。

【００２４】

図６は、本発明の実施形態による文書またはその他のコンテンツ２０６を転送するための方法の態様を示す。最初に、工程６０４において、ユーザは、たとえば図５に関連して説明されている、クライアント・デバイス１０４を使用して文書を開く（読み込む）。工程６０８において、ユーザはメモリに転送メッセージを作成する。メッセージの送信に備えて、クライアント・デバイス１０４で動作しているクライアント・アプリケーション２０４は、新しいコンテンツ暗号キー２２６を要求する（工程６１２）。文書は組み立てられ（工程６１６）、受信者（複数可）の公開暗号キー２２２が要求される（工程６２０）。文書は次に暗号化され（工程６２４）、文書が割り当てられるコンサート（複数可）２１２に追加される（工程６２８）。工程６３２において、コンテンツ・キー２２６は、ユーザのコンテンツ・キー・リング２２４に追加される。次いで、暗号化された文書は、格納および／または配信のためにキューに入れられる（工程６３６）。

【００２５】

図７は、本発明の実施形態によるコンテンツ暗号キー２２６を要求するための方法の態様を示す。コンテンツ暗号キー２２６の要求に応答して（工程７０４）、暗号化アルゴリズムが選択される（工程７０８）。当業者には理解されるように、一部の暗号化アルゴリズムは、他のコンテンツよりも、特定のタイプの暗号化されたコンテンツに適している。加えて、暗号化されているコンテンツ２０６に必要と見なされるセキュリティのレベルに基づいて、さまざまな暗号化アルゴリズムが選択されてもよい。それらのさまざまな考慮事項にかんがみて、本発明の実施形態は、複数の暗号化アルゴリズムをサポートする。アルゴリズムが選択された後、コンテンツ・キー２２６が生成され（工程７１２）、そのキー２２６の強さが検査される（工程７１６）。コンテンツ・キー２２６が弱いと決定される場合、新しいコンテンツ暗号キー２２６が生成され（工程７１２）、その新しいキー２２６の強さが再度検査される（工程７１６）。承認されるキー２２６が生成された後、キーはクライアント・アプリケーション２０４に返される（工程７２０）。承認されたキー

が返されることは（ステップ７１２）、クライアント・デバイス１０４上のキー・リングの１つにコンテンツ・キー２２６を配置することを含むことができる。次いで、メモリ内のコンテンツ・キー２２６のバージョンが上書きされる（工程７１６）。

【００２６】

図８は、本発明の実施形態による文書またはその他のコンテンツ２０６を組み立てるための方法の態様を示す。工程８０４において、文書またはコンテンツ・キー２２６と共に暗号化されるべきメタデータが収集される。暗号のためのメタデータは、たとえば、引用、または文書のグラフィカル要素の解像度に関連する情報のような、文書が実際に表示されるまで必要とされないメタデータを含むことができる。工程８０８において、文書および関連するメタデータは、一意のコンテンツ・キー２２６を使用して暗号化される。工程８１２において、文書ヘッダの一部であるが、コンテンツ・キー２２６を使用して暗号化されなくてもよいメタデータが収集される。暗号化されなくてもよいメタデータの例は、作成者またはその他の権限が公表を望む引用、作成者、文書のサイズ、作成日などを含むことができる。次いで、文書にアクセスするために必要とされるコンテンツ・キー２２６を含む文書のヘッダは、許可キー２１８で暗号化される（工程８１６）。この時点において、文書および関連する情報は、コンテンツ・システム・サーバ１０８に送信されてもよい。

【００２７】

工程８２０において、文書の受信者が識別され、コンテンツ・システム・サーバ１０８は、文書の受信者ごとに公開キーを要求することができる（工程８２４）。次いで、適切な許可キー２１８、および文書またはコンテンツ・キー２２６を使用して暗号化されたヘッダ情報は、受信者の公開キー２２２でラップされ、暗号化された文書に付加される（工程８２８）。次いで、文書は受信者クライアント・デバイス１０４に配信される（工程８３２）。したがって、公開キー２２２のペアである秘密キーの保持者は、ヘッダ情報にアクセスすることができ、適切な秘密キー２３０を適用することによりコンテンツ・キー２２６にアクセスすることができるが、許可キー２１８により使用可能にされたアクションしか実行することはできない。

【００２８】

図９は、コンテンツ・キー２２６を管理するための方法の態様を示す。一般に、コンテンツ・キー２２６は、各々コンサートすなわちコンテンツのグループ分け２１２に関連付けられている暗号化されたキー・リングに格納される。したがって、工程９０４において、コンサート２１２が作成される。工程９０８において、コンテンツ（コンサート）キー・リング２２４のキーが生成される。工程９１２において、コンサート２１２に関連付けられているコンテンツ・オブジェクト２０６のコンテンツ・キー２２６が暗号化に使用可能であるかどうかについて決定が行なわれてもよい。コンテンツ・キー２２６が暗号化に使用可能である場合、そのコンテンツ・キー２２６は、コンテンツ・キー・リング２２４（すなわち、該当するコンサート２１２のコンテンツ・キー・リング２２４）のキーを使用して暗号化される（工程９１６）。

【００２９】

工程９２０において、コンサート２１２に含まれるコンテンツ・オブジェクト２０６にアクセスする必要があるかどうかについて決定が行なわれてもよい。コンテンツ２０６にアクセスする必要がある場合、そのコンテンツ・キー２２６を含むコンテンツ・キー・リングから必要とされるコンテンツのコンテンツ・キー２２６を取得するために、必要なシステム・キー２３４が適用される（工程９２４）。システム・キー２３４の適用は、クライアント・アプリケーション２０４がシステム・キー２３４にアクセスするために秘密キー２３０を使用することを含むことができる。次いで、コンテンツ２０６は、クライアント・アプリケーション２０４を通じてユーザに表示されてもよい（工程９２８）。工程９３２において、コンサート２１２へのアクセスが中止されるべきであるかどうかについて決定が行なわれてもよい。アクセスが続行される場合、方法は工程９１２に戻る。あるいは、方法は終了してもよい。

【００３０】
図１０～図１３は、本発明の実施形態による、オブジェクト・ストア２０８の一部として格納され、１つまたは複数のコンサート２１２に関連付けられているコンテンツにアクセスするために実施されうるさまざまなセキュリティ手順を示す。セキュリティの第１のレベルは、図１０に示される方法により実施される。その方法によれば、クライアント・アプリケーションまたはコンサート・アプリケーション２０４が開始される（工程１００４）。次いで、マウントされるコンサート・ストアまたはコンサート２１２が選択され（工程１００８）、そのコンサート・ストアのパスワードが入力される（工程１０１２）。パスワードが入力されると、コンテンツ２０６はアクセスされてもよく、そのコンテンツでの作業が開始される（工程１０１６）。

【００３１】
図１１において、セキュリティの次のレベルが示される。最初に、クライアント・アプリケーションまたはコンサート・アプリケーション２０４が開始され（工程１１０４）、マウントするコンサート・ストアが選択され（工程１１０８）、必要なパスワードがユーザによって入力される（工程１１１２）。したがって、工程１１０４から１１１２は概ね、工程１００４から１０１２に対応する。工程１１１６において、チャレンジ質問がユーザに表示される。工程１１２０において、ユーザの応答が入力される。適正な応答が入力される場合、コンテンツ２０６はアクセスされてもよく、作業が開始されてもよい（工程１１２４）。

【００３２】
図１２において、実施されうるセキュリティのさらなるレベルが示される。最初に、工程１２０４において、クライアント・アプリケーションまたはコンサート・アプリケーション２０４が開始され、マウントするコンサート・ストアが選択され（工程１２０８）、ユーザが必要なパスワードを入力する（工程１２１２）。工程１２１６において、システムは、ユーザにキー・ファイル名を入力するよう要求する。次いで、さまざまなオプションが実施されてもよい。たとえば、ユーザは、クライアント・デバイス１０４に直接にアクセス可能なコンテンツ２０６のキー・ファイル名を入力することができ（工程１２２０）、そのコンテンツへのアクセスが許可されて作業が開始されてもよい（工程１２２４）。代替として、ユーザは、複数のキー・ファイルの名前を入力することができ（工程１２２８）、そのコンテンツへのアクセスが許可されて作業が開始されてもよい（工程１２３２）。さらにもう１つのオプションとして、複数のキー・ファイル名の要求が行なわれた後、ユーザは取り外し可能ボリュームをマウントすることができ（工程１２３６）、所望のコンテンツのキー・ファイル（複数可）の名前を入力することができる（工程１２４０）。次いで、所望のコンテンツ２０６へのアクセスが許可されて、作業が開始されてもよい（工程１２４４）。

【００３３】
図１３において、セキュリティのさらなるレベルが実施される。最初に、工程１３０４において、クライアント・アプリケーションまたはコンサート・アプリケーション２０４が開始され、マウントするコンサート・ストアが選択され（工程１３０８）、ユーザが必要なパスワードを入力する（工程１３１２）。工程１３１６において、クライアント・アプリケーション２０４は、ユーザに要求されたコンテンツ２０６のキー・ファイル名を入力するよう要求する。要求に応答して、さまざまな手順がサポートされてもよい。たとえば、ユーザは、キーまたはその他の必要な情報を含むスマートカードを挿入することができる（工程１３２０）。加えて、次いでユーザは、個人識別番号またはパスワードを入力することができる（工程１３２４）。代替として、キー・ファイル名の要求に応答して、ユーザは、ＰＩＮ暗号化ディスクを挿入して（工程１３２８）、さらにＰＩＮを入力することができる（工程１３３２）。工程１３２４または１３３２においてＰＩＮを入力した後、ユーザは、必要なキー・ファイル名を入力するか（工程１３３６）、または複数のキー・ファイルの名前を入力することができる（工程１３４０）。次いで、所望のコンテンツ２０６はアクセスされて、作業が開始されてもよい（工程１３４４）。

【００３４】
図１４～１８は、コンサート情報を格納するためのさまざまなオプションを示す。さらに詳細には、図１４において、クライアントシステム１０４にローカルなデータ・ストレージ３１２は、オブジェクトまたはボリューム・ファイル・ストア２０８内のオブジェクトデータ、コンサートオブジェクトメタデータおよび関連するコンサートのキー２１２、ログファイル・データベース１４０４、およびクライアント・アプリケーション２０４のすべてを含むことができる。
【００３５】
図１５において、オブジェクト・ストア２０８、コンサート２１２、およびログファイル・データベース１４０４は、クライアント・アプリケーション２０４が格納されるデータ・ストレージ３１２ａを備える第１のデータデバイスとは別個の第２のデータ・ドライブを備えるデータ・ストレージ３１２ｂに格納される。たとえば、第１のデータ・ドライブは、クライアント・デバイス１０４の内部にある第１のハードディスク・ドライブまたはフラッシュ・ドライブを備えることができ、一方第２のデータ・ドライブは、同様にクライアント・デバイス１０４の内部にある第２のハードディスク・ドライブまたはフラッシュ・ドライブを備えることができる。たとえば、オブジェクト・ストア２０８、コンサート２１２、およびログファイル・データベース１４０４は、クライアント・デバイス１０４の一部として提供される第２の内蔵ハードドライブに格納されてもよい。本発明の実施形態によれば、ログファイル・データベース１４０４は、特定のコンテンツ・オブジェクト２０６が供給されるコンサート２１２を示すレコード、バージョン情報、またはコンサート２１２内のコンテンツ２０６の編成および保守に関連するその他の情報を含むことができる。
【００３６】
図１６において、オブジェクト・ストア２０８、コンサート２１２、およびログファイル・データベース１４０４は、クライアント・アプリケーション２０４と共に、クライアント・デバイス１０４のローカル・ディスク・ドライブを備えるデータ・ストレージ３１２に格納される。加えて、第２のオブジェクト・ストア２０８、その他のコンサート２１２、およびそれらのコンサート２１２に関連付けられているログファイル・データベース１４０４は、取り外し可能ＵＳＢドライブを備えるデータ・ストレージ３３６に格納される。
【００３７】
図１７において、クライアント・アプリケーション２０４は、クライアント・デバイス１０４のローカル・ディスク・ドライブを備えるデータ・ストレージ２１２に格納される。オブジェクト・ストア２０８、コンサート２１２、およびログファイル・データベース１４０４はすべて、取り外し可能ＵＳＢドライブを備えるデータ・ストレージ３３６上にある。
【００３８】
図１８において、クライアント・デバイス１０４のローカル・ディスク・ドライブを備えるデータ・ストレージ２１２は、オペレーティング・システム・ソフトウェア３０４を含むが、クライアント・アプリケーション２０４、オブジェクト・ストア２０８、またはコンサート２１２は含まない。その代わり、それらのコンポーネントはすべて、取り外し可能ＵＳＢドライブを備えるデータ・ストレージ３３６に格納される。
【００３９】
図１９は、本発明の実施形態による例示的なシステム１００のアーキテクチャを示す。特に、コンテンツ・システム・サーバ１０８は、複数のエッジ・サーバ１２４と協働して動作するコア・サーバ１２６として実施されてもよい。コア・サーバ１２６は、セキュリティおよびキー管理、ディレクトリ更新、検索、キャッシュ管理、分析、マッチメーク、分類形成、およびバックアップ機能を含む、さまざまなコンテンツ配信機能を実施することができる。加えて、コア・サーバ１２６は、データセンター管理、コールセンター管理、課金および会計のような、さまざまな管理機能を実行することができる。エッジ・サー

バ１２４はまた、セキュリティおよびキー管理を提供することもできる。加えて、エッジ・サーバ１２４は、同期化エージェント、自動更新、コンテンツ管理、管理プラグイン、キャッシュ、ディレクトリ、およびメッセージ認証を実行することができる。システム１００に含まれるクライアント・デバイス１０４は、セキュリティおよびキー管理を実施することができる。加えて、協調、商取引、メディアおよび記事ビルダー機能およびサービスがサポートされてもよい。さらに、さまざまなコンテンツおよび機能が、さまざまなモジュールおよびサービスを通じてアクセスされてもよい。

【００４０】

図２０は、たとえばクライアント・デバイス１０４に含まれるか、またはクライアント・デバイス１０４に関連付けられているディスプレイによって、ユーザに提示されうるユーザ・インターフェイス２０００の実施形態を示す。ユーザ・インターフェイス２０００および本明細書において説明されるその他のユーザ・インターフェイスは、ユーザの表示デバイスのウィンドウに提示されるビジュアル表示であってもよい。一部の実施形態において、クライアント・アプリケーション２０４は、表示のためにユーザ・インターフェイスを描画し、１つまたは複数のユーザ入力デバイス（たとえば、選択可能ボタン、メニュー、アイコンなど）を通じてユーザ入力を受信する。しかし、その他の実施形態において、コンテンツ・システム・サーバ１０８は、クライアント１０４に送信されてクライアント・アプリケーション２０４でドキュメントとして表示されるマルチメディア文書としてユーザ・インターフェイスを描画することができる。さらに、マルチメディア文書でのユーザによる選択は、クライアント１０４からコンテンツ・システム・サーバ１０８に送信される要求を生成させることができる。

【００４１】

ユーザ・インターフェイス２０００は、クライアント・アプリケーション２０４の第１の情報ウィンドウとなりうるウィンドウ２００２をもたらす。ウィンドウ２００２は、コンテンツ２０６を表示するための表示領域２００４を含むことができる。加えて、ユーザがコンテンツを検索することができる検索フィールド２００６が含まれてもよい。さらに、ウィンドウ２００２は、ユーザのコンテンツを編成するユーザ選択可能フォルダ２０１０のセットを表示することができる第２の表示領域２００８を含むことができる。ウィンドウ２００２は、ユーザ選択を受信するためのユーザ選択可能デバイス（たとえば、メニュー・バー２０１２、またはメニュー２０１４）をさらに含むことができる。

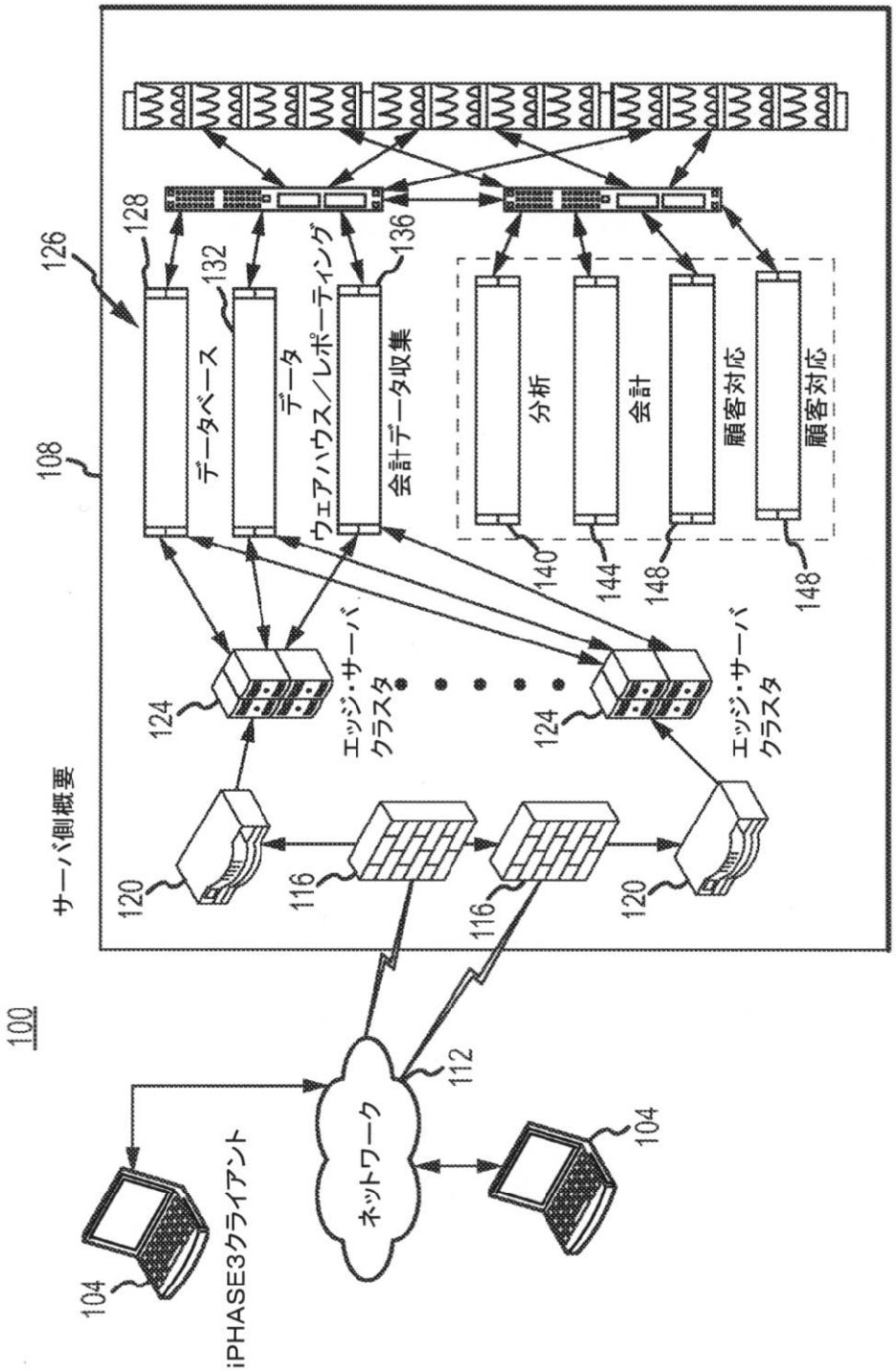
【００４２】

本明細書において提供される特定の例は、文書を備えるコンテンツ２０６の暗号化およびこれに関わる操作を説明するが、本発明の実施形態は、文書に関連して使用することに限定されない。その代わり、コンピュータまたは類似のデバイスにより格納され交換されうる任意の形態のコンテンツ、情報、データなどは、本発明の開示の目的でコンテンツを備えることができる。

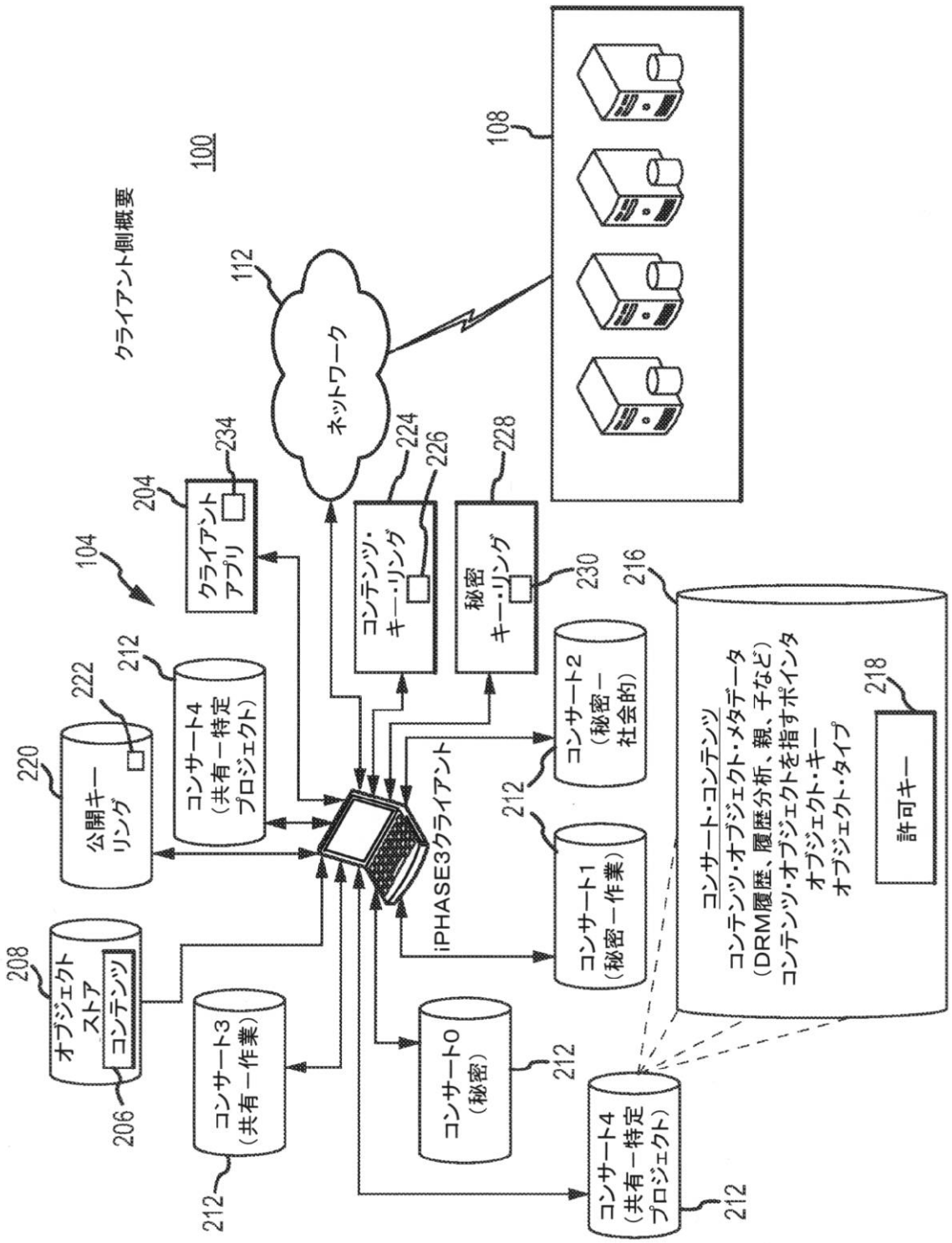
【００４３】

本発明の前述の説明は、例示および説明の目的で提示されてきた。さらに、説明は、本明細書において開示される形態に本発明を限定することを意図していない。したがって、従来技術の技量または知識の範囲内で、上記の教示に相応する変形および変更は、本発明の範囲に含まれる。上記で説明される実施形態は、本発明を実施する現在知られている最良の態様を説明すること、および他の当業者が、そのようなまたは他の実施形態において、本発明の特定の適用または使用に必要なさまざまな変更を加えて、本発明を使用できるようにすることがさらに意図されている。添付の特許請求の範囲が、従来技術の許す範囲で代替的実施形態を含むものと解釈されることが意図される。

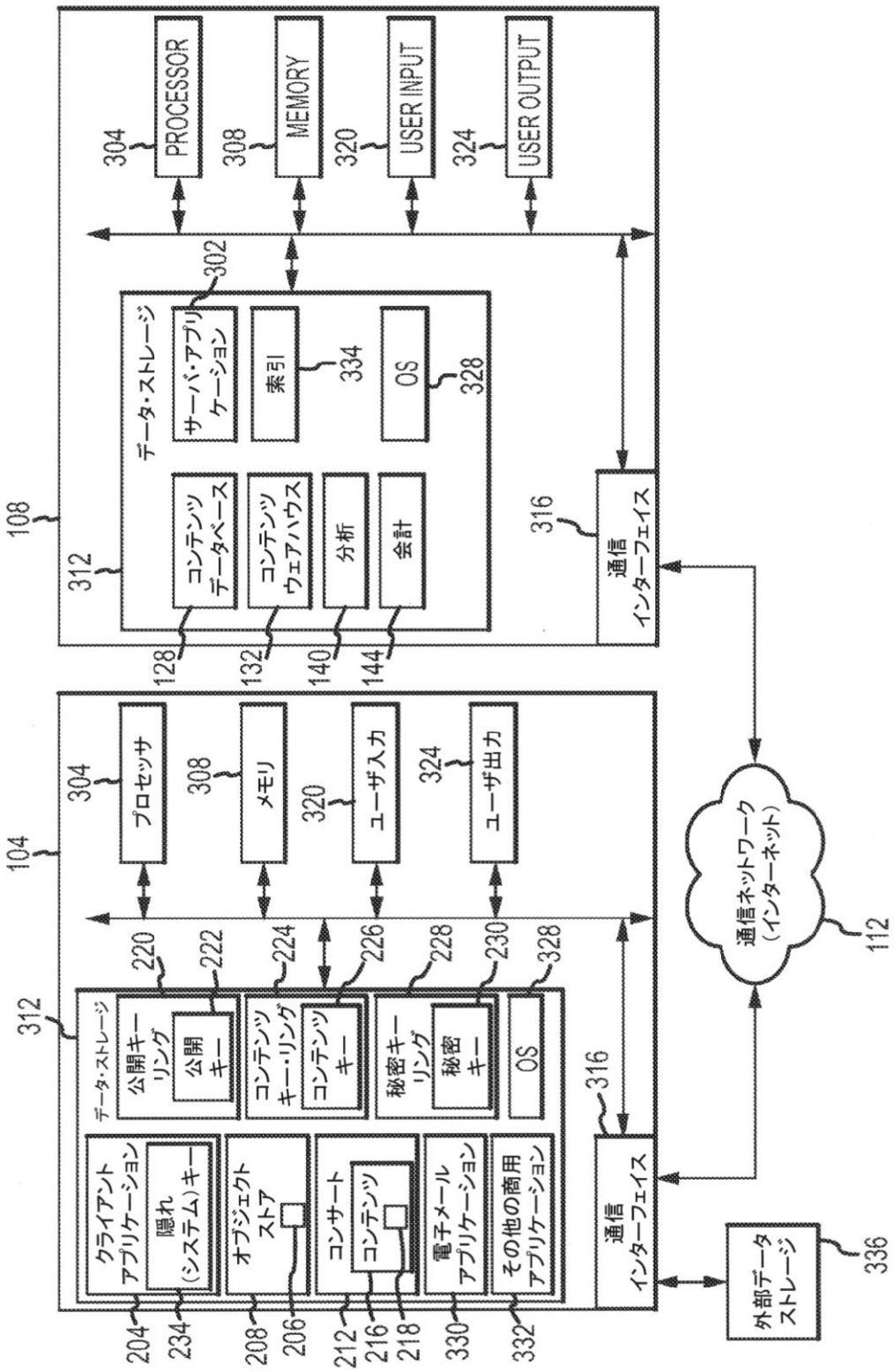
【図１】


100
サーバ側概要
108
126
128
132
136
データベース
データウェアハウス／レポーティング
会計データ収集
分析
会計
顧客対応
顧客対応
140
144
148
148
124
124
エッジ・サーバクラスタ
エッジ・サーバクラスタ
120
116
116
120
112
ネットワーク
104
104
iPHASE3クライアント

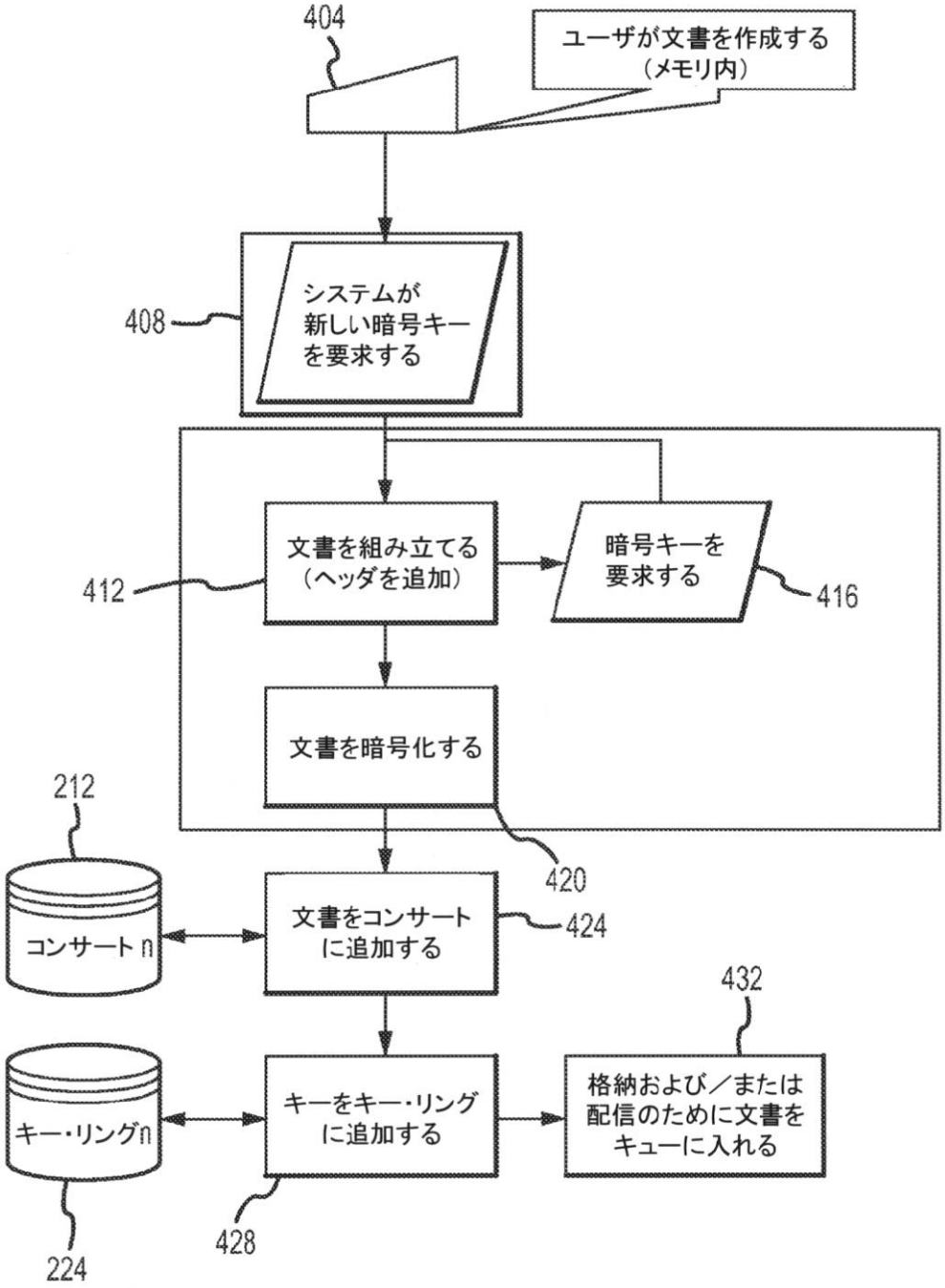
【図２】


クライアント側概要
100
108
112
ネットワーク
104
204
クライアント
アプリ
234
224
コンテンツ・
キー・リング
226
228
秘密
キー・リング
230
216
222
公開キー
リング
212
コンサート4
（共有－特定
プロジェクト）
220
コンサート2
（秘密－
社会的）
212
iPHASE3クライアント
208
オブジェクト
ストア
コンテンツ
206
コンサート1
（秘密－作業）
コンサート・コンテンツ
コンテンツ・オブジェクト・メタデータ
（DRM履歴、履歴分析、親、子など）
コンテンツ・オブジェクトを指すポインタ
オブジェクト・キー
オブジェクト・タイプ
218
許可キー
コンサート3
（共有－作業）
212
コンサート0
（秘密）
212
コンサート4
（共有－特定
プロジェクト）
212

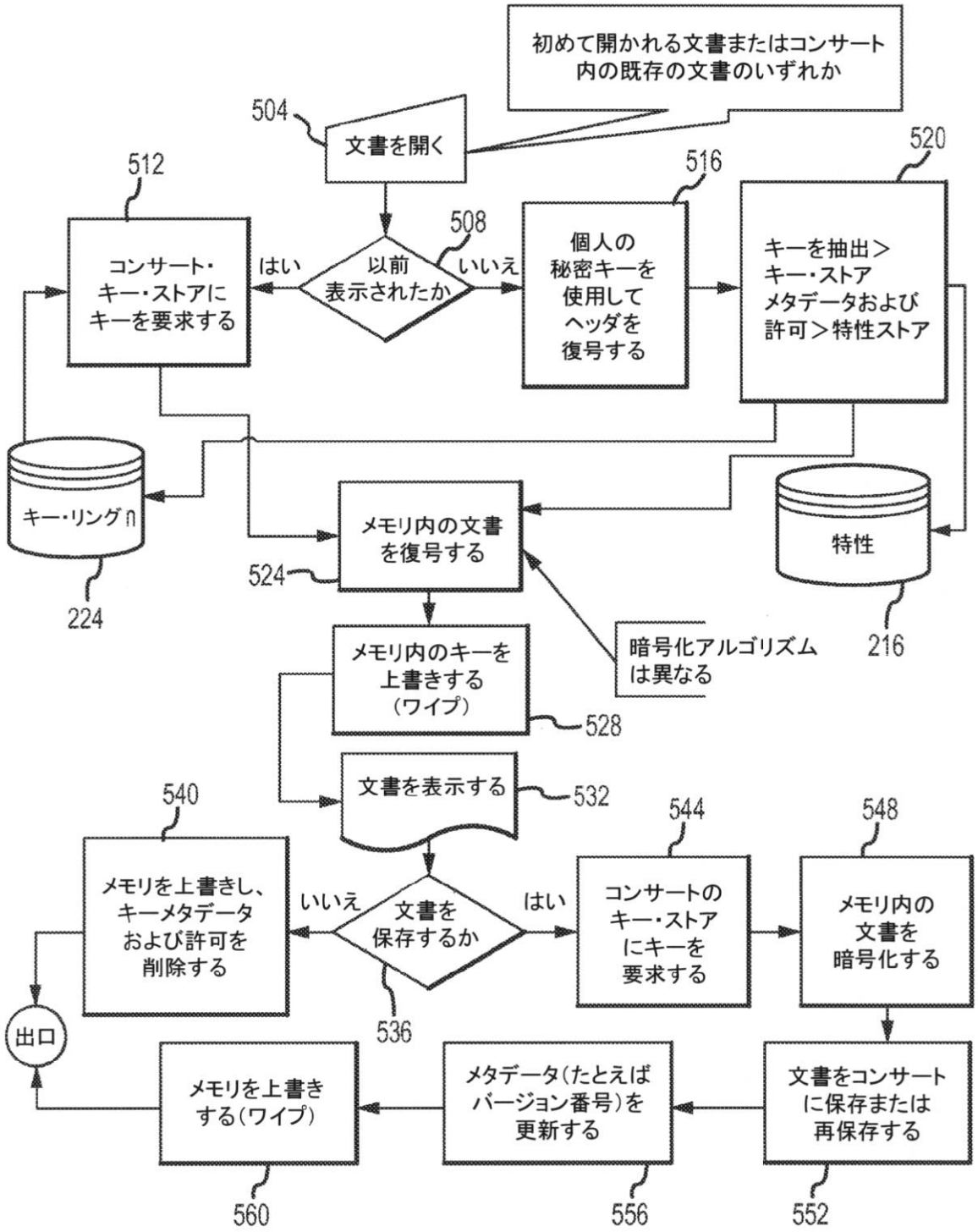
【図３】


108
312
304
PROCESSOR
308
MEMORY
320
USER INPUT
324
USER OUTPUT
302
データ・ストレージ
サーバ・アプリケーション
索引
334
OS
328
コンテンツデータベース
コンテンツウェアハウス
分析
会計
128
132
140
144
316
通信インターフェイス
104
プロセッサ
メモリ
ユーザ入力
ユーザ出力
220
222
224
226
228
230
328
データ・ストレージ
公開キーリング
公開キー
コンテンツキー・リング
コンテンツキー
秘密キーリング
秘密キー
OS
クライアントアプリケーション
隠れ（システム）キー
オブジェクトストア
コンサート
コンテンツ
電子メールアプリケーション
その他の商用アプリケーション
204
234
208
206
212
216
218
330
332
316
通信インターフェイス
通信ネットワーク（インターネット）
112
外部データストレージ
336

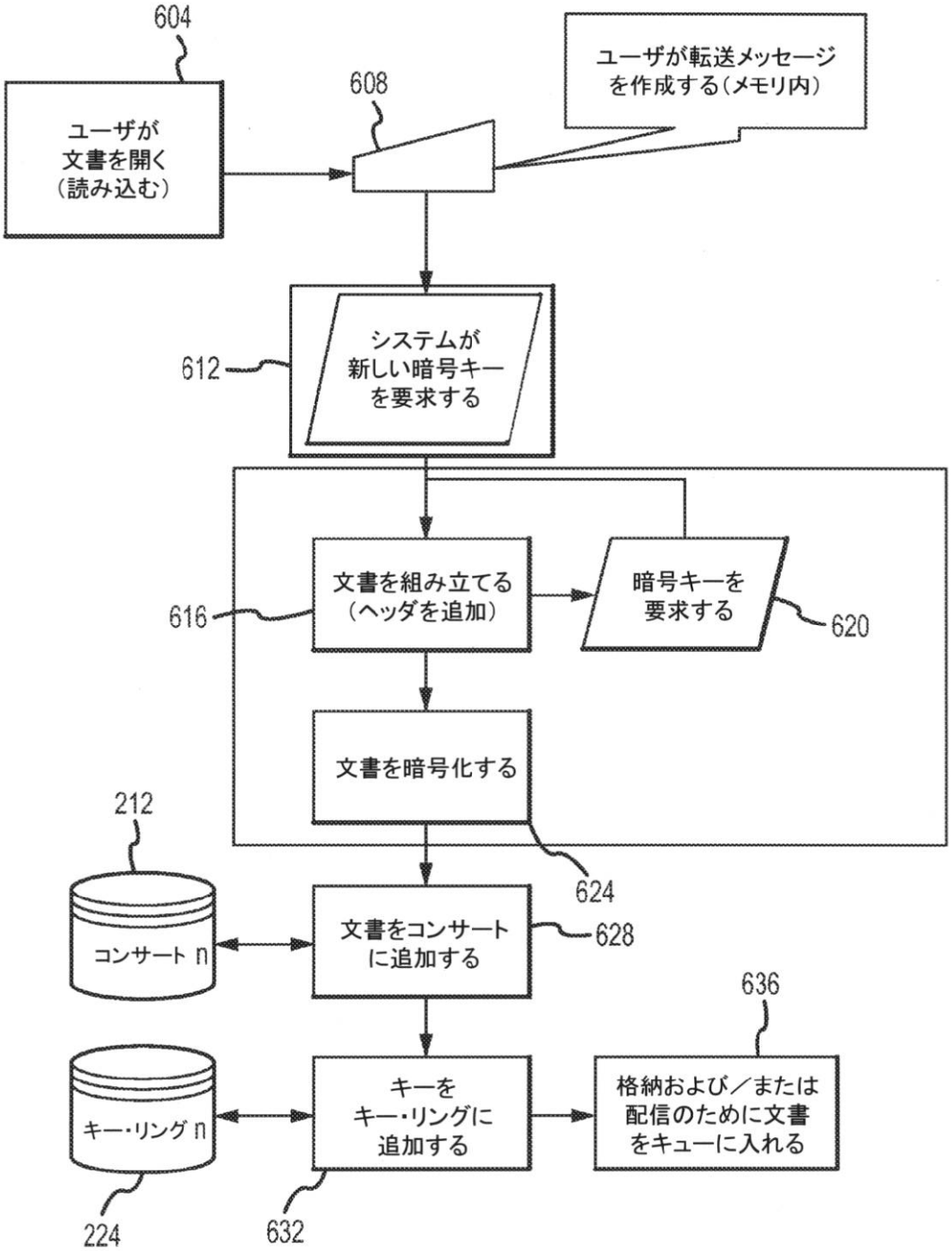
【図４】


404
ユーザが文書を作成する
（メモリ内）
408
システムが
新しい暗号キー
を要求する
412
文書を組み立てる
（ヘッダを追加）
暗号キーを
要求する
416
文書を暗号化する
420
212
コンサート n
文書をコンサート
に追加する
424
432
キー・リング n
キーをキー・リング
に追加する
格納および／または
配信のために文書を
キューに入れる
428
224

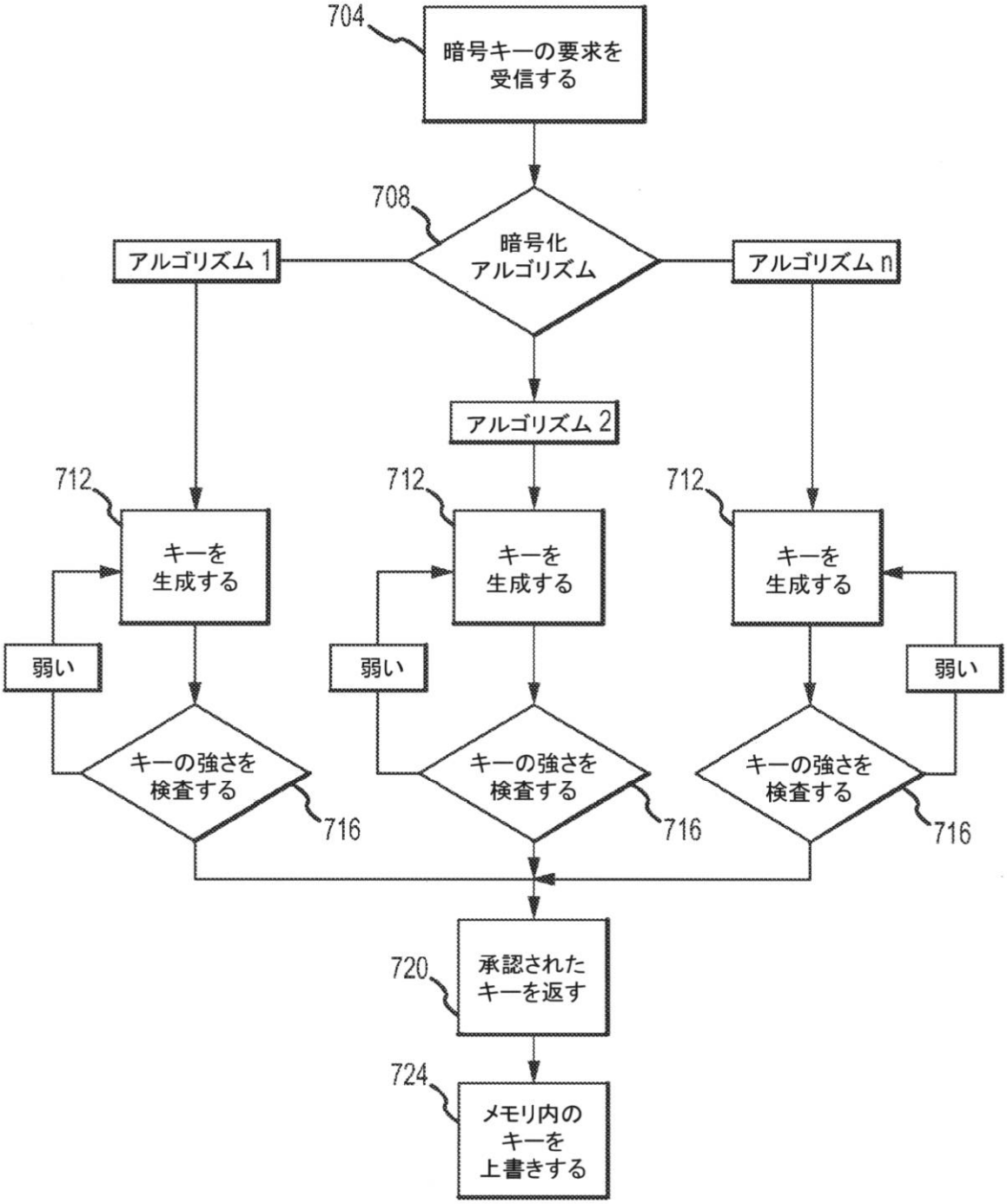
【図５】


初めて開かれる文書またはコンサート内の既存の文書のいずれか
504
文書を開く
512
コンサート・キー・ストアにキーを要求する
はい
508
以前表示されたか
いいえ
516
個人の秘密キーを使用してヘッダを復号する
520
キーを抽出＞キー・ストアメタデータおよび許可＞特性ストア
キー・リング n
224
メモリ内の文書を復号する
524
特性
216
暗号化アルゴリズムは異なる
メモリ内のキーを上書きする（ワイプ）
528
文書を表示する
532
540
メモリを上書きし、キーメタデータおよび許可を削除する
いいえ
文書を保存するか
はい
536
544
コンサートのキー・ストアにキーを要求する
548
メモリ内の文書を暗号化する
出口
メモリを上書きする（ワイプ）
560
メタデータ（たとえばバージョン番号）を更新する
556
文書をコンサートに保存または再保存する
552

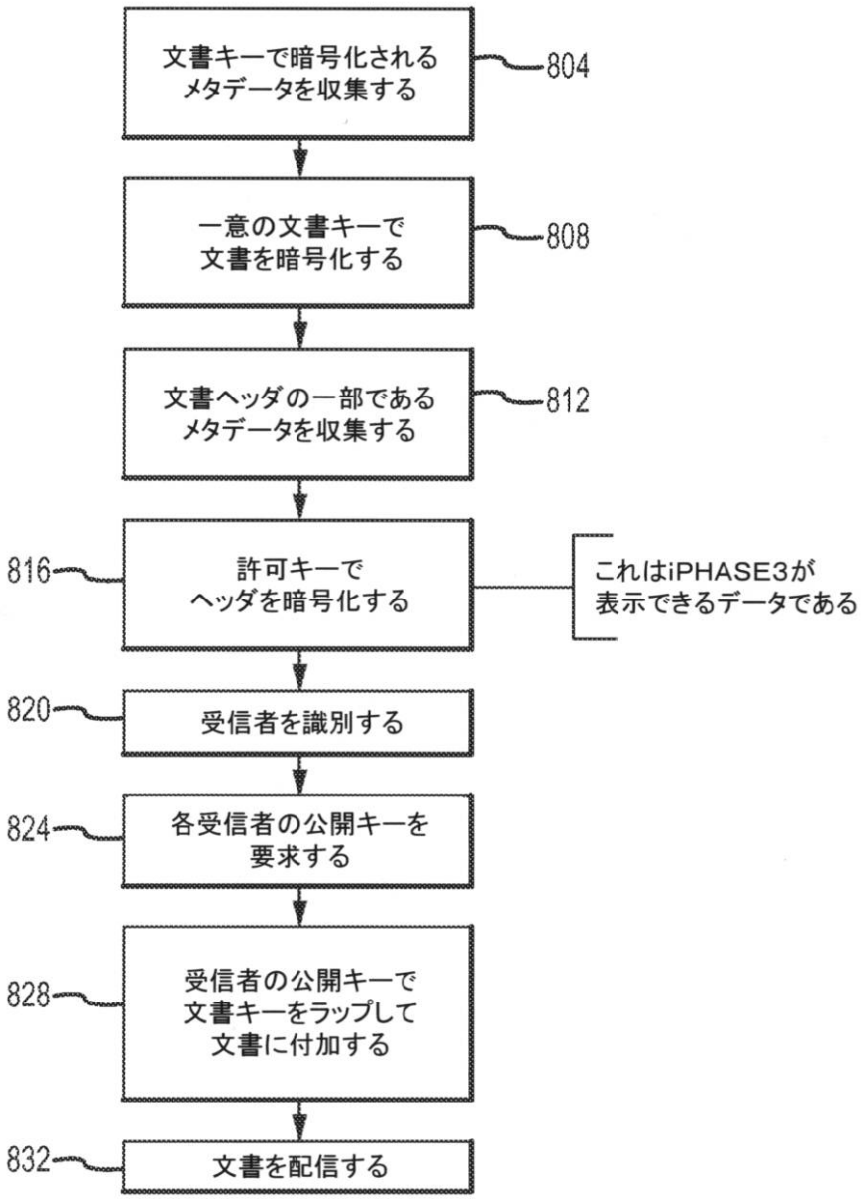
【図６】


604
ユーザが
文書を開く
（読み込む）
608
ユーザが転送メッセージ
を作成する（メモリ内）
612
システムが
新しい暗号キー
を要求する
616
文書を組み立てる
（ヘッダを追加）
暗号キーを
要求する
620
文書を暗号化する
212
624
コンサート n
文書をコンサート
に追加する
628
636
キー・リング n
キーを
キー・リングに
追加する
格納および／または
配信のために文書
をキューに入れる
224
632

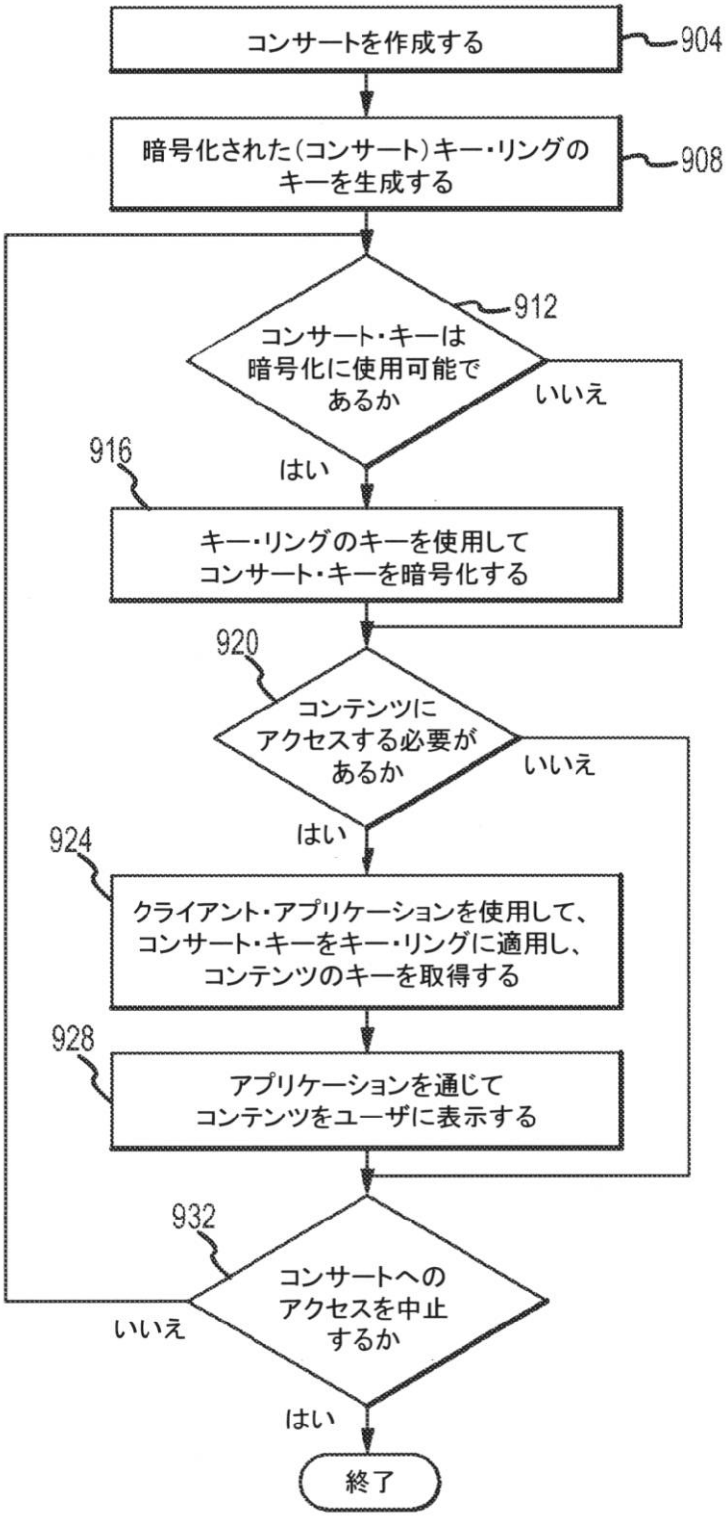
【図７】


704
暗号キーの要求を受信する
708
暗号化アルゴリズム
アルゴリズム 1
アルゴリズム 2
アルゴリズム n
712
キーを生成する
712
キーを生成する
712
キーを生成する
弱い
弱い
弱い
キーの強さを検査する
716
キーの強さを検査する
716
キーの強さを検査する
716
720
承認されたキーを返す
724
メモリ内のキーを上書きする

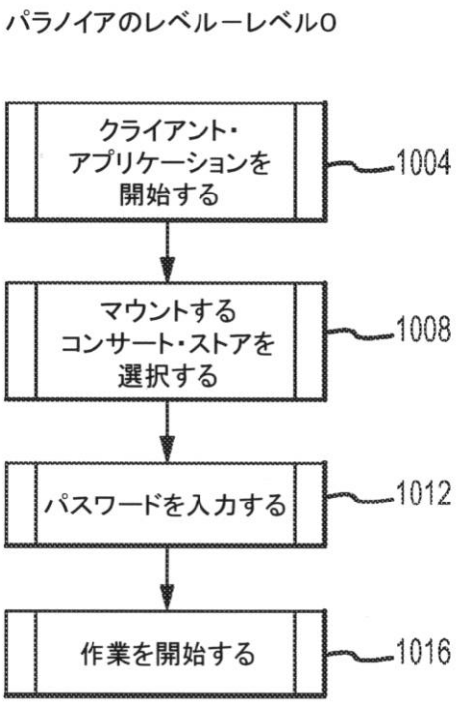
【図８】


文書キーで暗号化される
メタデータを収集する
804
一意の文書キーで
文書を暗号化する
808
文書ヘッダの一部である
メタデータを収集する
812
816
許可キーで
ヘッダを暗号化する
これはiPHASE3が
表示できるデータである
820
受信者を識別する
824
各受信者の公開キーを
要求する
828
受信者の公開キーで
文書キーをラップして
文書に付加する
832
文書を配信する

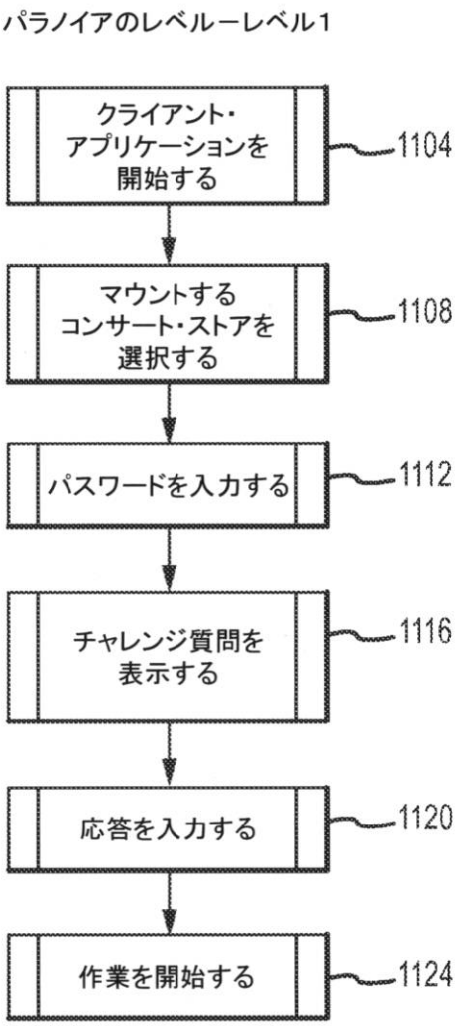
【図９】


コンサートを作成する
904
暗号化された(コンサート)キー・リングの
キーを生成する
908
912
コンサート・キーは
暗号化に使用可能で
あるか
いいえ
916
はい
キー・リングのキーを使用して
コンサート・キーを暗号化する
920
コンテンツに
アクセスする必要が
あるか
いいえ
はい
924
クライアント・アプリケーションを使用して、
コンサート・キーをキー・リングに適用し、
コンテンツのキーを取得する
928
アプリケーションを通じて
コンテンツをユーザに表示する
932
コンサートへの
アクセスを中止
するか
いいえ
はい
終了

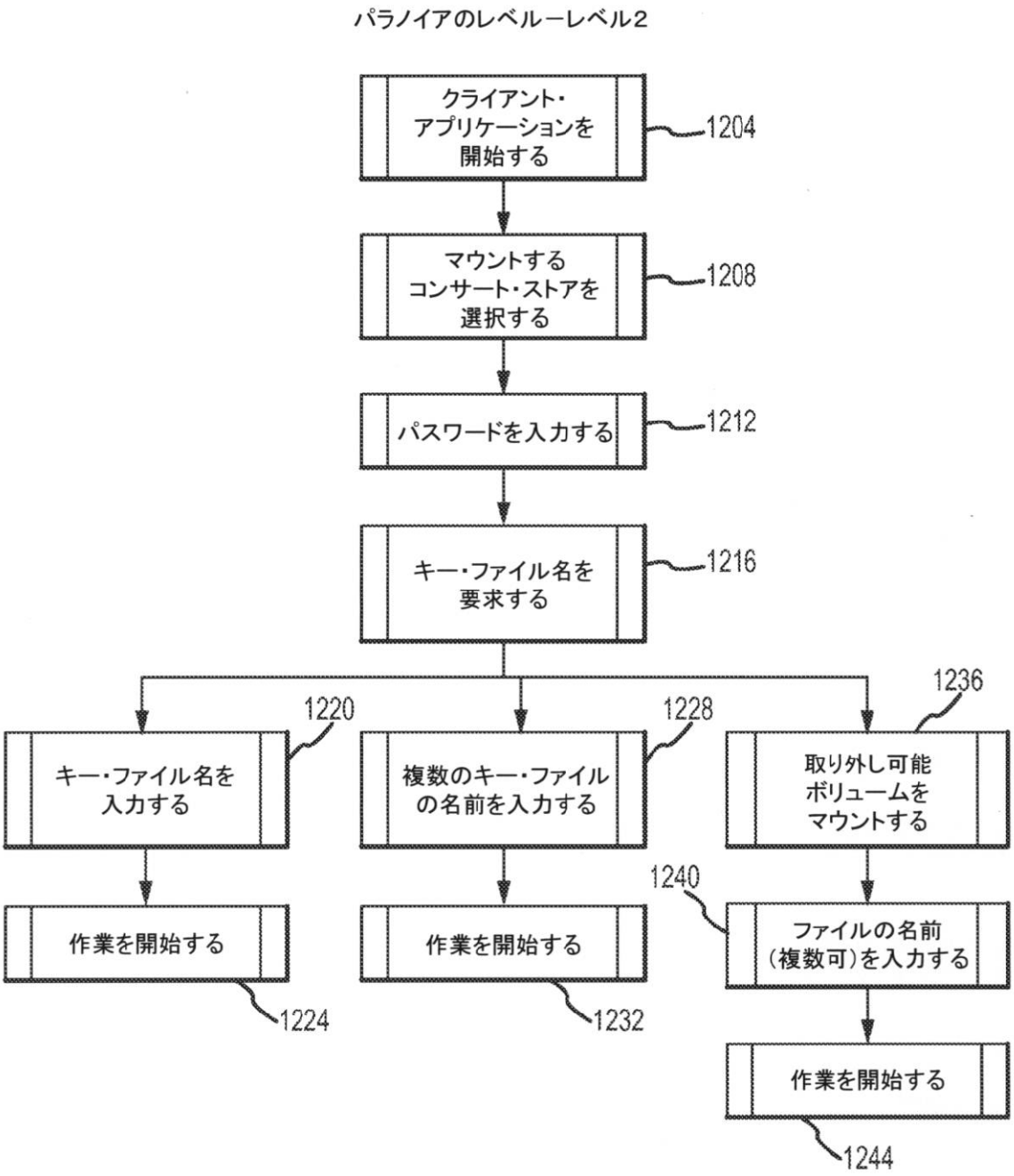
【図１０】


パラノイアのレベルーレベル0
クライアント・アプリケーションを開始する
1004
マウントするコンサート・ストアを選択する
1008
パスワードを入力する
1012
作業を開始する
1016

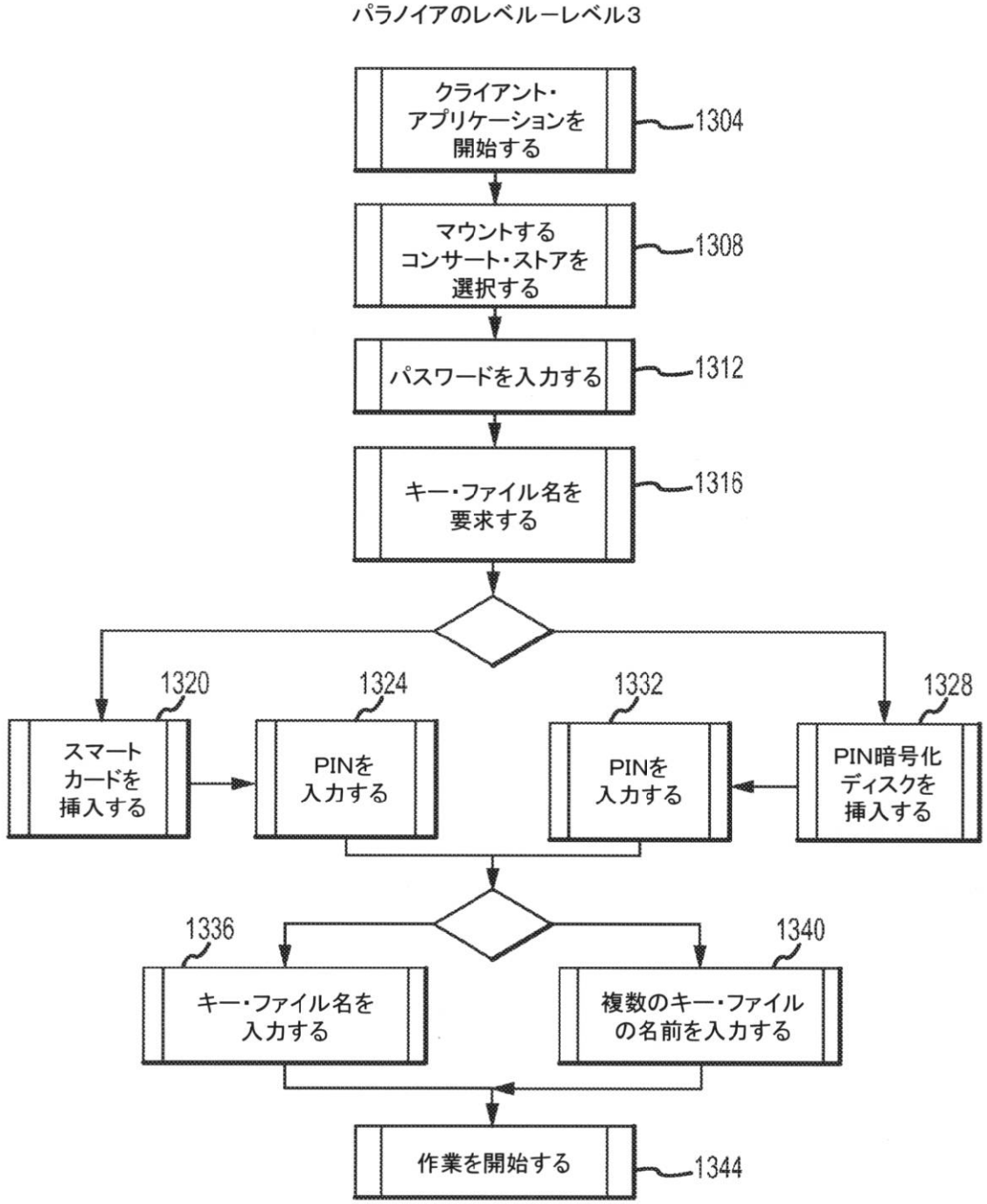
【図１１】


パラノイアのレベルーレベル1
クライアント・アプリケーションを開始する
1104
マウントするコンサート・ストアを選択する
1108
パスワードを入力する
1112
チャレンジ質問を表示する
1116
応答を入力する
1120
作業を開始する
1124

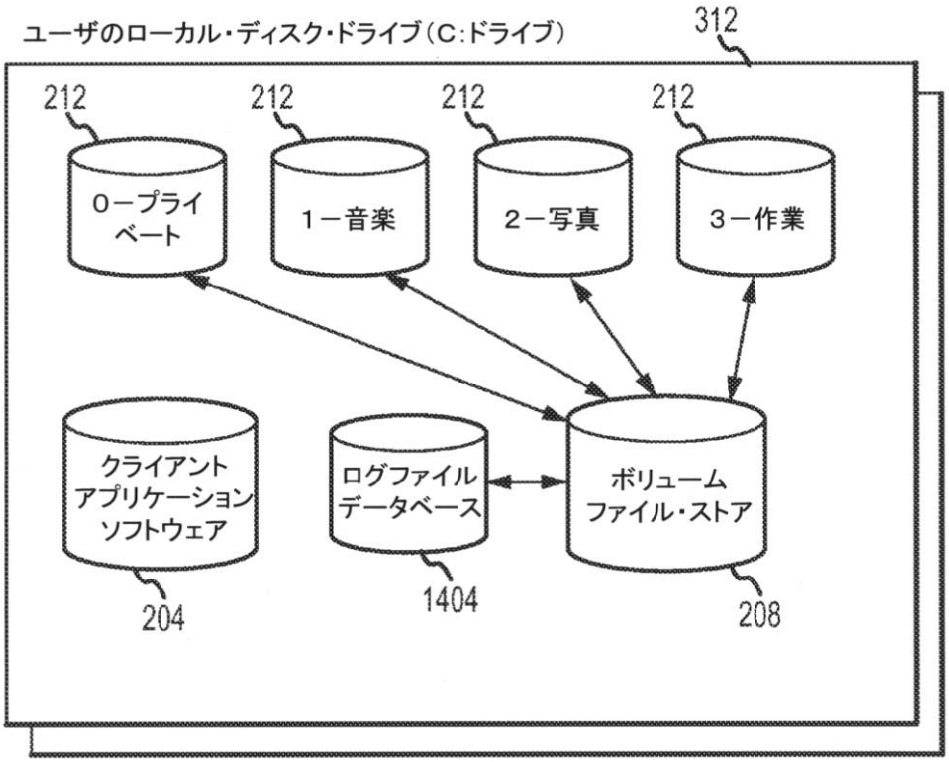
【図１２】


パラノイアのレベルーレベル2
クライアント・アプリケーションを開始する
1204
マウントするコンサート・ストアを選択する
1208
パスワードを入力する
1212
キー・ファイル名を要求する
1216
1220
キー・ファイル名を入力する
1228
複数のキー・ファイルの名前を入力する
1236
取り外し可能ボリュームをマウントする
1240
作業を開始する
1224
作業を開始する
1232
ファイルの名前（複数可）を入力する
作業を開始する
1244

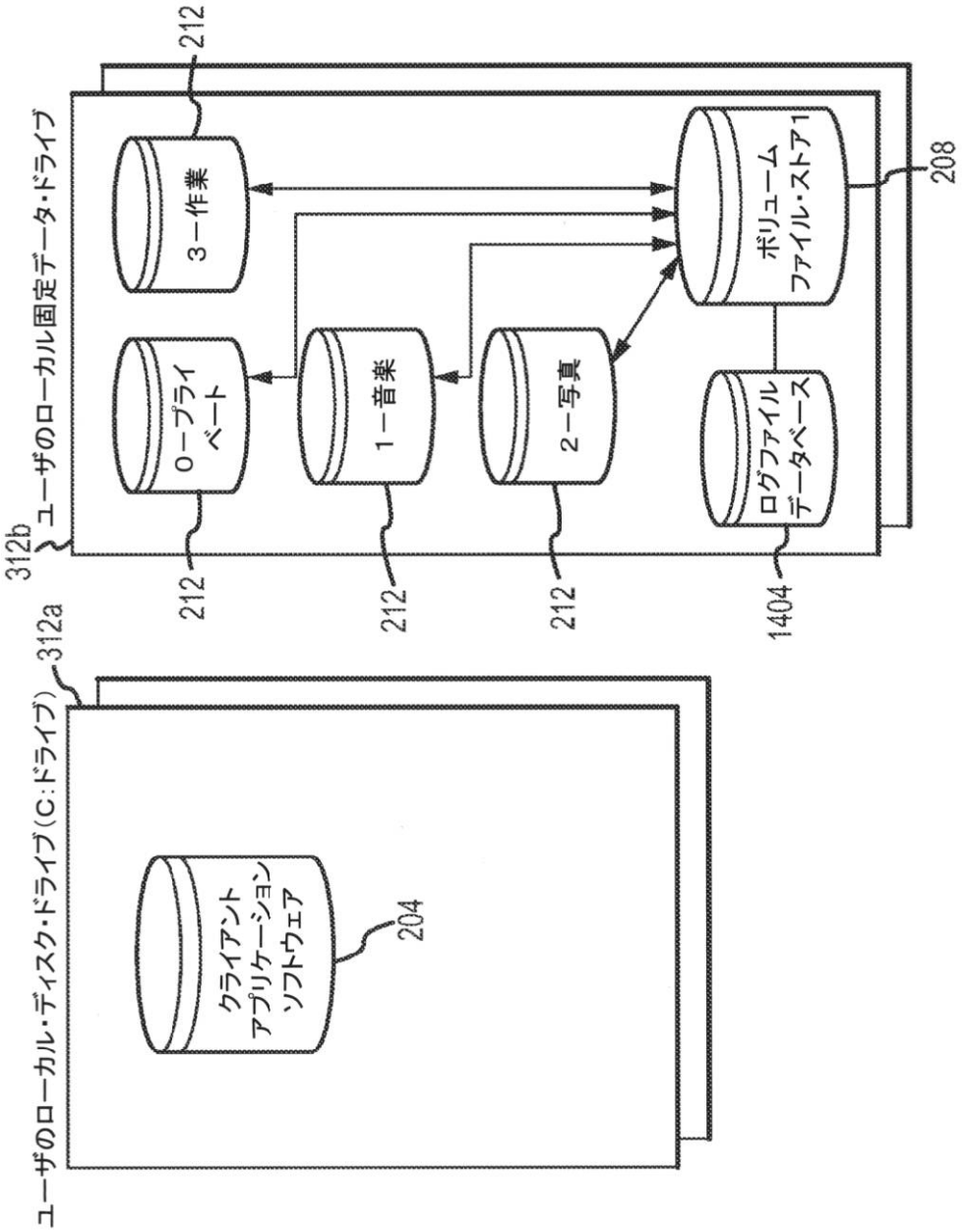
【図１３】


パラノイアのレベルーレベル3
クライアント・アプリケーションを開始する
1304
マウントするコンサート・ストアを選択する
1308
パスワードを入力する
1312
キー・ファイル名を要求する
1316
1320
スマートカードを挿入する
1324
PINを入力する
1332
PINを入力する
1328
PIN暗号化ディスクを挿入する
1336
キー・ファイル名を入力する
1340
複数のキー・ファイルの名前を入力する
作業を開始する
1344

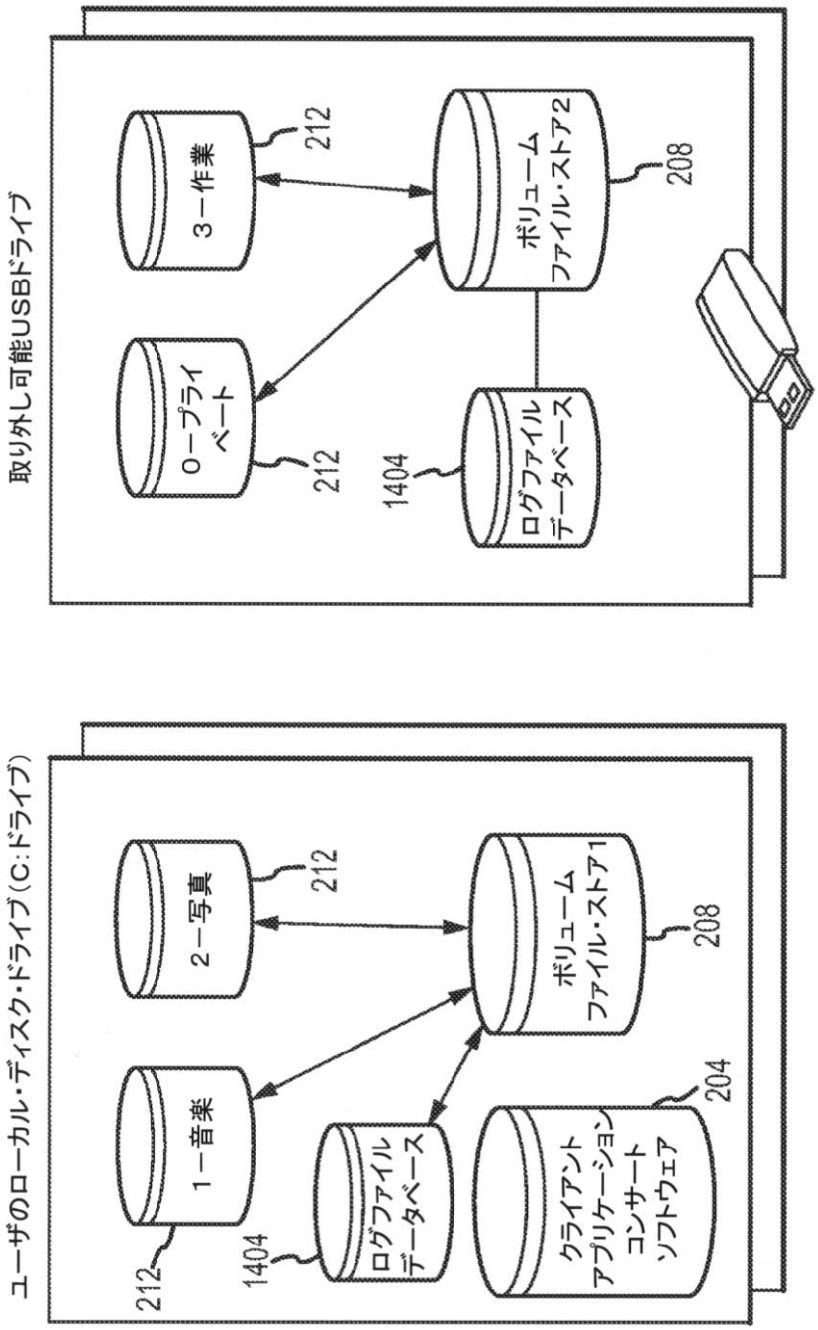
【図１４】


ユーザのローカル・ディスク・ドライブ（C:ドライブ）
312
212
212
212
212
0－プライベート
1－音楽
2－写真
3－作業
クライアントアプリケーションソフトウェア
ログファイルデータベース
ボリュームファイル・ストア
204
1404
208

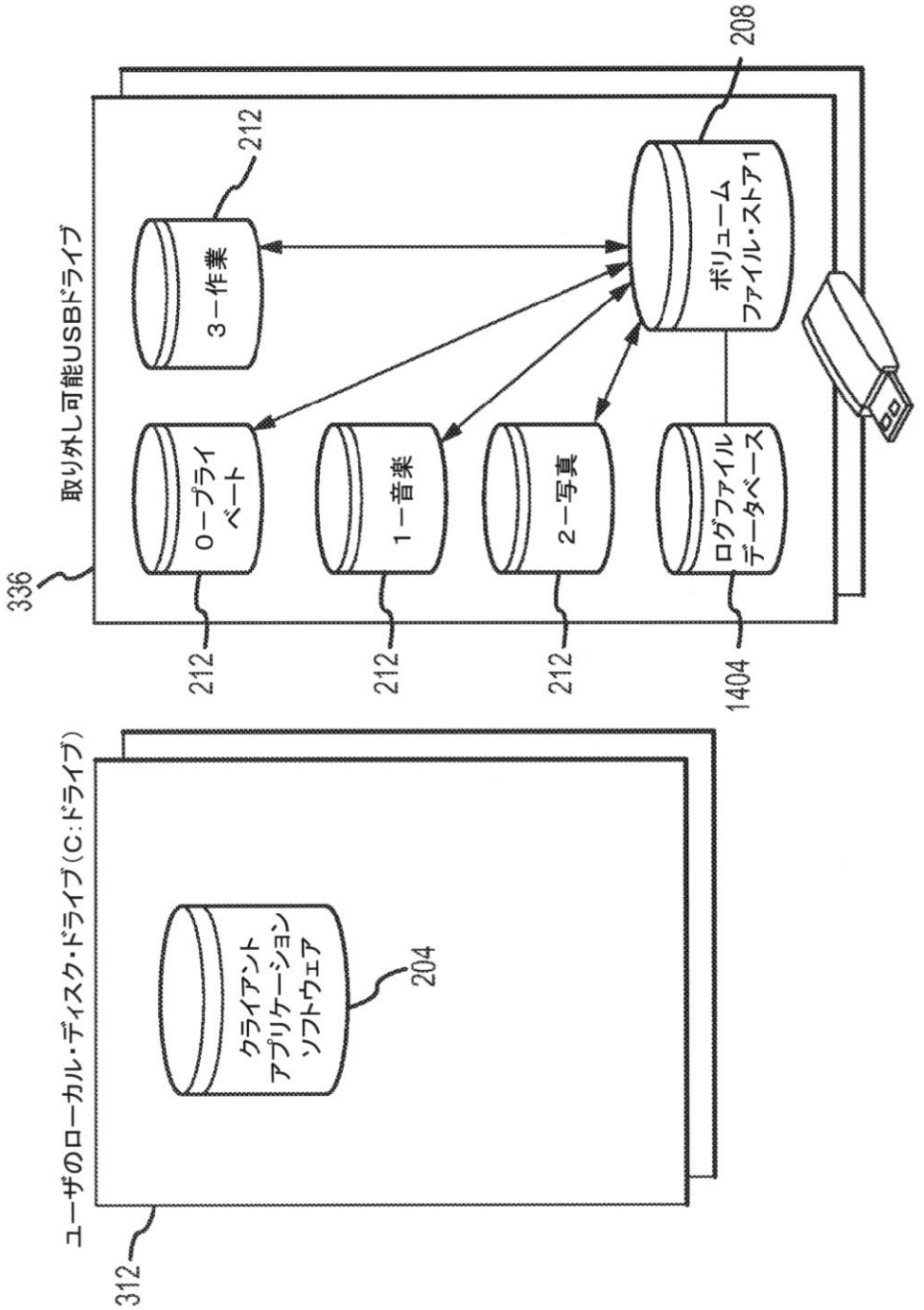
【図１５】


ユーザのローカル・ディスク・ドライブ(C:ドライブ)
312a
クライアント
アプリケーション
ソフトウェア
204
ユーザのローカル固定データ・ドライブ
312b
0－プライベート
1－音楽
2－写真
3－作業
ボリューム
ファイル・ストア1
ログファイル
データベース
212
212
212
212
208
1404

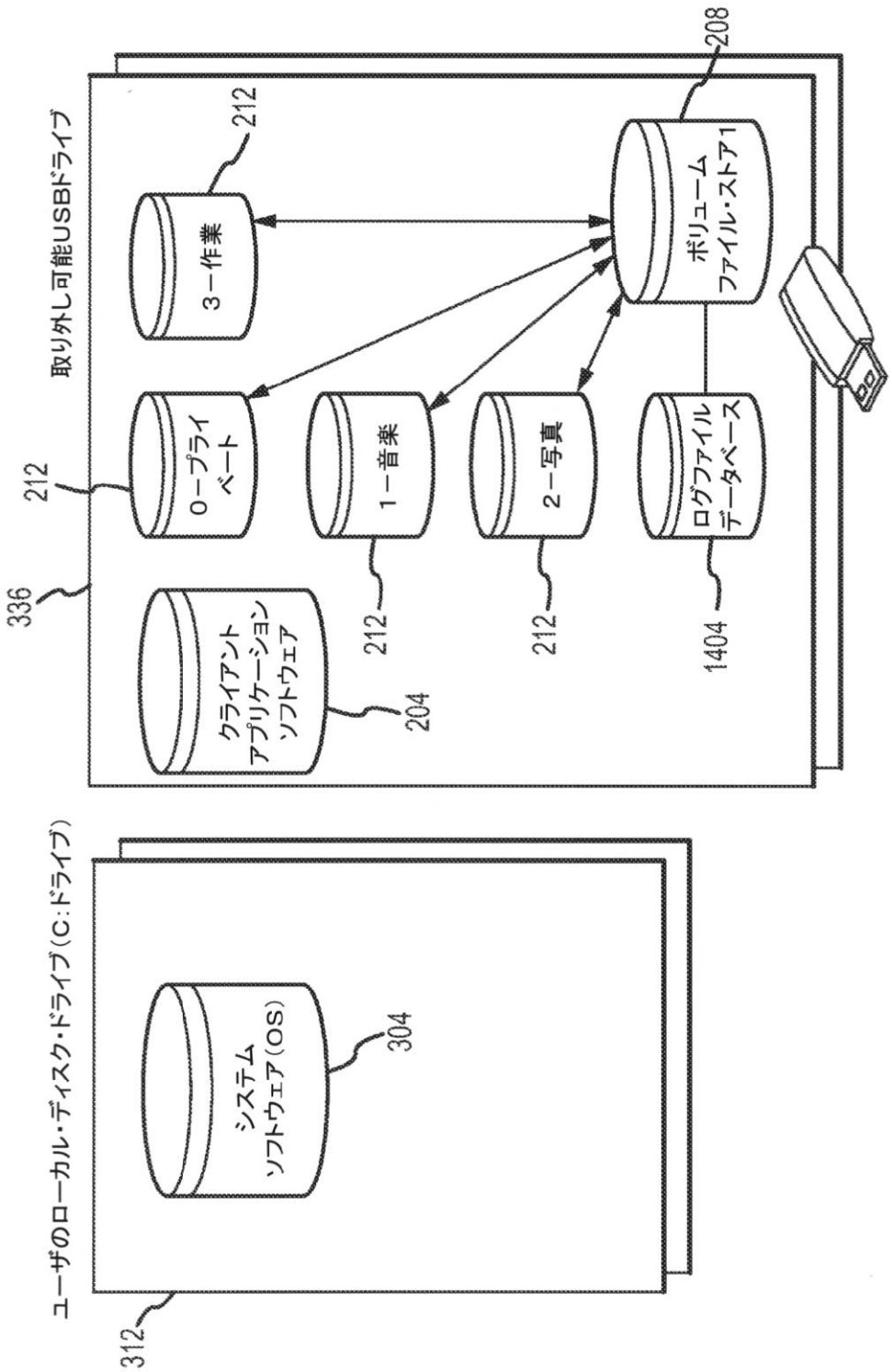
【図１６】


ユーザのローカル・ディスク・ドライブ(C:ドライブ)
1－音楽
2－写真
ボリューム
ファイル・ストア1
208
212
212
1404
ログファイル
データベース
クライアント
アプリケーション
コンサート
ソフトウェア
204
取り外し可能USBドライブ
3－作業
0－プライベート
ボリューム
ファイル・ストア2
208
212
212
1404
ログファイル
データベース

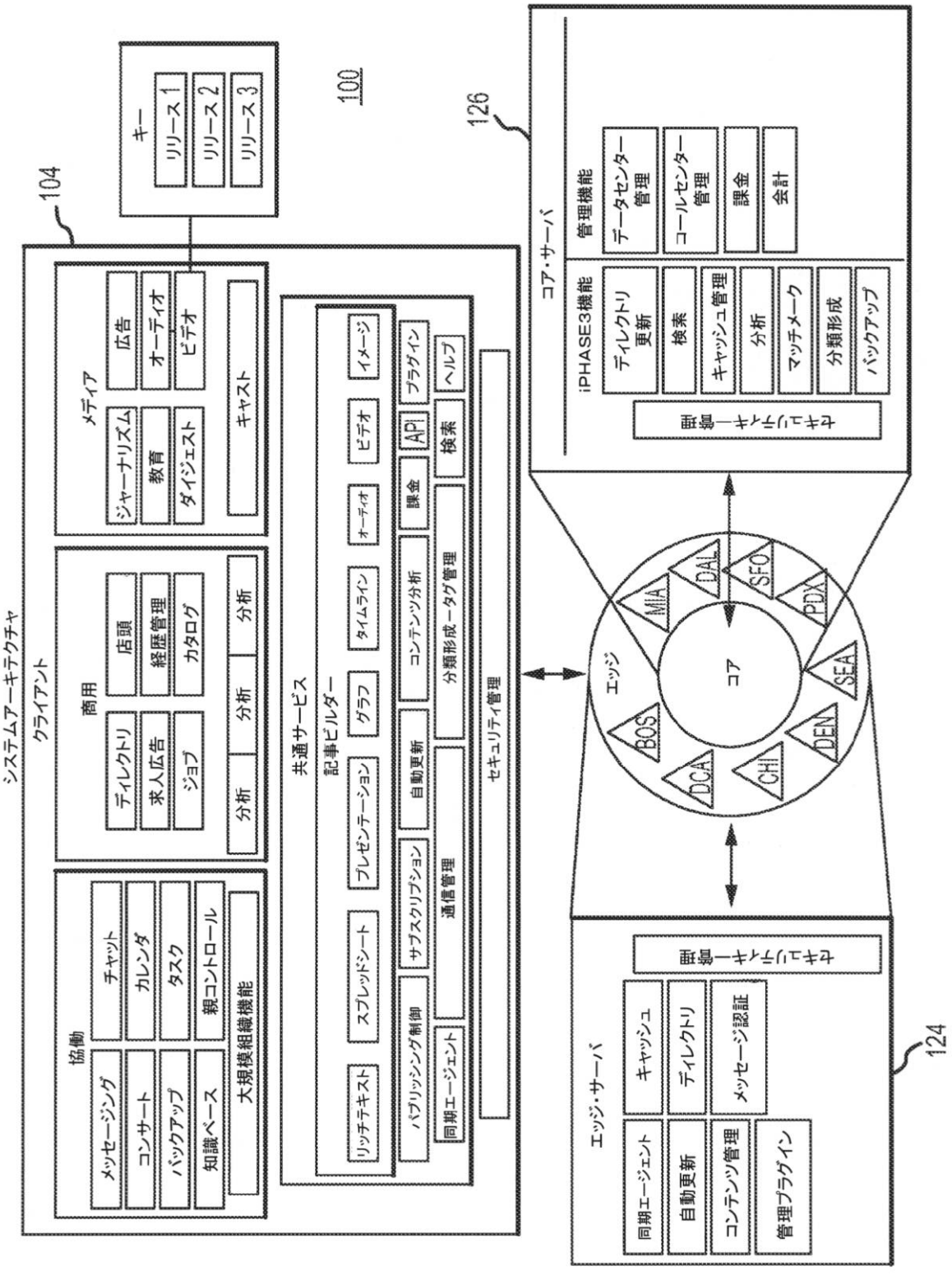
【図１７】


ユーザのローカル・ディスク・ドライブ(C:ドライブ)
312
クライアント
アプリケーション
ソフトウェア
204
取り外し可能USBドライブ
336
0－プライベート
1－音楽
2－写真
3－作業
ログファイル
データベース
ボリューム
ファイル・ストア1
212
212
212
212
1404
208

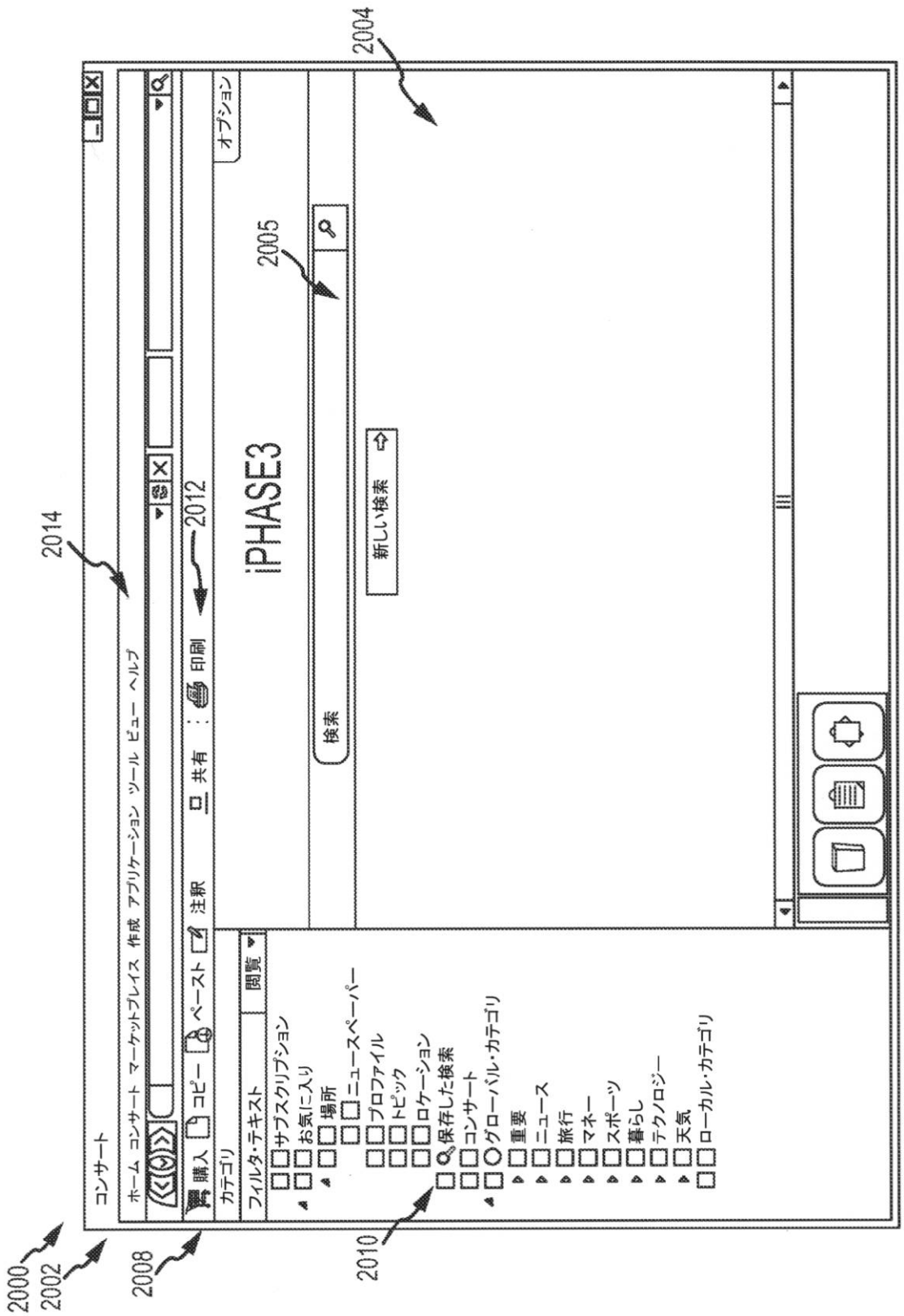
【図１８】


ユーザのローカル・ディスク・ドライブ(C:ドライブ)
システム
ソフトウェア(OS)
304
312
取り外し可能USBドライブ
208
ボリューム
ファイル・ストア1
212
3－作業
0－プライベート
1－音楽
2－写真
ログファイル
データベース
1404
336
クライアント
アプリケーション
ソフトウェア
204

【図１９】


システムアーキテクチャ
クライアント
104
100
126
124
キー
リソース1
リソース2
リソース3
協働
メッセージング
チャット
コンサート
カレンダ
バックアップ
タスク
知識ベース
親コントロール
大規模組織機能
商用
ディレクトリ
店頭
求人広告
経歴管理
ジョブ
カタログ
分析
分析
分析
メディア
ジャーナリズム
広告
教育
オーディオ
ダイジェスト
ビデオ
キャスト
共通サービス
記事ビルダー
リッチテキスト
スプレッドシート
プレゼンテーション
グラフ
タイムライン
オーディオ
ビデオ
イメージ
パブリッシング制御
サブスクリプション
自動更新
コンテンツ分析
課金
API
プラグイン
同期エージェント
通信管理
分類形成－タグ管理
検索
ヘルプ
セキュリティ管理
コア・サーバ
管理機能
データセンター管理
コールセンター管理
課金
会計
iPHASE3機能
ディレクトリ更新
検索
キャッシュ管理
分析
マッチメーク
分類形成
バックアップ
キャッシュ
エッジ
MIA
DAL
SFO
PDX
SEA
DEN
CHI
DCA
BOS
コア
エッジ・サーバ
同期エージェント
キャッシュ
自動更新
ディレクトリ
コンテンツ管理
メッセージ認証
管理プラグイン
キャッシュ

【図２０】


2000
2002
2008
2010
2012
2014
2004
2005
コンサート
ホーム コンサート マーケットプレイス 作成 アプリケーション ツール ビュー ヘルプ
購入 コピー ペースト 注釈 共有 印刷
オプション
カテゴリ
フィルタ・テキスト
閲覧
サブスクリプション
お気に入り
場所
ニュースペーパー
プロファイル
トピック
ロケーション
保存した検索
コンサート
グローバル・カテゴリ
重要
ニュース
旅行
マネー
スポーツ
暮らし
テクノロジー
天気
ローカル・カテゴリ
iPHASE3
検索
新しい検索

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 11/36368

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 12/14, G06Q 20/00 (2011.01)
USPC - 726/18, 705/71
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC:726/18, 705/71

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 726/1-5, 16-18, 21; 705/50, 64, 67, 71; 700/1, 90 (keyword limited; terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Electronic Database Searched: PubWEST (PGPB, USPT, EPAB, JPAB), Google Scholar
Search Terms Used: content, document, file, video, audio, music, song, key, recipient, receiver, destination, user, person, individual, member, receive, get, send, to, public, PK, community, asymmetric, encrypt, encode, database, ring, group, store, repository, appli

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X – Y	US 2006/0107285 A1 (Medvinsky) 18 May 2006 (18.05.2006), see entire document; especially para [0005], [0015]-[0021], [0024]-[0029], [0031]-[0045], [0053]-[0062], [0067]-[0068], Fig. 1-4, 6-7	1-10,14-19 11-13, 20
Y	US 2009/0276829 A1 (Sela et al.) 05 November 2009 (05.11.2009), see para [0014]-[0015], [0019], [0032], [0040], [0042], [0053]-[0057], [0073]-[0076], [0079], [0082]-[0087], [0096], [0099], [0109]-[0110], [0116], [0118]-[0119], Fig. 1-2, 4-5, 8	11-13, 20
A	US 2008/0131861 A1 (Redd et al.) 05 June 2008 (05.06.2008), see entire document	1-20
A	US 2007/0198413 A1 (Nagao) 23 August 2007 (23.08.2007), see entire document	1-20
A	US 2005/0131832 A1 (Fransdonk) 16 June 2005 (16.06.2005), see entire document	1-20
A	US 2005/0100161 A1 (Husemann et al.) 12 May 2005 (12.05.2005), see entire document	1-20
A	US 2005/0044016 A1 (Irwin et al.) 24 February 2005 (24.02.2005), see entire document	1-20
A	US 2002/0026582 A1 (Futamura et al.) 28 February 2002 (28.02.2002), see entire document	1-20

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
22 August 2011 (22.08.2011)	30 AUG 2011
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

フロントページの続き

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

(72)発明者 タネンバウム、ミッチェル ジェイ.
アメリカ合衆国 ８０１２７ コロラド州 リトルトン サウス ワトスン ガルチ ロード ９３３６
(72)発明者 クルーガー、ダニエル エル.
アメリカ合衆国 ８０４３９ コロラド州 エバーグリーン スプルース ロード ２９７８３

Ｆターム(参考) 5J104 AA16 AA32 EA04 EA18 EA19 JA03 JA21 NA02 NA37 PA07