

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6669929号  
(P6669929)

(45) 発行日 令和2年3月18日 (2020.3.18)

(24) 登録日 令和2年3月2日 (2020.3.2)

|                             |                |
|-----------------------------|----------------|
| (51) Int. Cl.               | F I            |
| <b>H04L 9/08 (2006.01)</b>  | H04L 9/00 601B |
| <b>G06F 21/41 (2013.01)</b> | G06F 21/41     |
| <b>G06F 21/60 (2013.01)</b> | G06F 21/60 320 |

請求項の数 13 (全 23 頁)

|                    |                               |           |                       |
|--------------------|-------------------------------|-----------|-----------------------|
| (21) 出願番号          | 特願2019-500214 (P2019-500214)  | (73) 特許権者 | 501113353             |
| (86) (22) 出願日      | 平成28年12月28日 (2016.12.28)      |           | シマンテック コーポレーション       |
| (65) 公表番号          | 特表2019-511890 (P2019-511890A) |           | Symantec Corporation  |
| (43) 公表日           | 平成31年4月25日 (2019.4.25)        |           | アメリカ合衆国, カリフォルニア州 94  |
| (86) 国際出願番号        | PCT/US2016/069036             |           | 043, マウンテン ビュー, エリス ス |
| (87) 国際公開番号        | W02017/171955                 |           | トリート 350              |
| (87) 国際公開日         | 平成29年10月5日 (2017.10.5)        | (74) 代理人  | 100147485             |
| 審査請求日              | 平成30年9月19日 (2018.9.19)        |           | 弁理士 杉村 憲司             |
| (31) 優先権主張番号       | 15/083,032                    | (74) 代理人  | 100134119             |
| (32) 優先日           | 平成28年3月28日 (2016.3.28)        |           | 弁理士 奥町 哲行             |
| (33) 優先権主張国・地域又は機関 | 米国 (US)                       | (72) 発明者  | ソコロフ・イリヤ              |
|                    |                               |           | アメリカ合衆国 マサチューセッツ州 O   |
|                    |                               |           | 2113 ポストン クーパーストリート   |
|                    |                               |           | 52 #8                 |
|                    |                               |           | 最終頁に続く                |

(54) 【発明の名称】 シングルサインオンアプリケーション用の暗号化鍵を管理するためのシステム及び方法

(57) 【特許請求の範囲】

【請求項 1】

シングルサインオンアプリケーション用の暗号化鍵を管理するためのコンピュータ実装方法であって、前記方法の少なくとも一部分は、少なくとも1つのプロセッサを含むコンピューティングデバイスによって実施され、前記方法は、

アイデンティティサービスから、クラウドサービス上の暗号化されたデータへのアクセス要求の通知であって、クラウドサービス鍵を復号するためのマスタ鍵を暗号化及び復号するためのセッション鍵を含む、通知を受信することと、

ユーザから受信した少なくとも1つの認証要素に基づいて、前記マスタ鍵を導出することと、

前記マスタ鍵を使用して、前記クラウドサービス上のデータを復号するためのクラウドサービス鍵を復号することと、

前記セッション鍵を使用して暗号化された前記マスタ鍵をクライアント鍵記憶部に記憶することと、

前記アイデンティティサービスから、追加のクラウドサービス上の暗号化されたデータへの追加のアクセス要求の追加の通知であって、前記セッション鍵を含む、通知を受信することと、

再度前記ユーザから前記認証要素を取得することなしに、前記セッション鍵を使用することによって前記マスタ鍵を復号することと、

前記マスタ鍵を使用して、前記追加のクラウドサービス上のデータを復号するための追

加のクラウドサービス鍵を復号することと、を含む、方法。

【請求項 2】

前記マスタ鍵を導出することは、前記ユーザから受信した前記認証要素にハッシュ関数を適用することを含む、請求項 1 に記載のコンピュータ実装方法。

【請求項 3】

前記暗号化されたデータを復号するために、前記復号されたクラウドサービス鍵を前記クラウドサービスに提供することを更に含む、請求項 1 に記載のコンピュータ実装方法。

【請求項 4】

クライアント上で、前記復号されたクラウドサービス鍵を使用して復号するために、前記暗号化されたデータを前記クラウドサービスから受信することを更に含む、請求項 1 に記載のコンピュータ実装方法。

10

【請求項 5】

前記暗号化されたクラウドサービス鍵を前記クラウドサービスから受信することを更に含む、請求項 1 に記載のコンピュータ実装方法。

【請求項 6】

前記暗号化されたクラウドサービス鍵を前記アイデンティティサービスから受信することを更に含む、請求項 1 に記載のコンピュータ実装方法。

【請求項 7】

前記暗号化されたクラウドサービス鍵を受信することは、  
前記セッション鍵と共に前記クラウドサービス鍵を受信することと、  
前記クラウドサービス鍵を提供することを求める前記アイデンティティサービスに対する要求に応答して前記クラウドサービス鍵を受信することと、の少なくとも 1 つを含む、請求項 1 又は 6 に記載のコンピュータ実装方法。

20

【請求項 8】

クラウドサービス鍵を復号するための前記マスタ鍵を暗号化及び復号するための前記セッション鍵をクライアントエージェントに提供することによって前記クラウドサービス上の暗号化されたデータへのアクセスを容易化することを求める要求を、前記アイデンティティサービスにおいて受信することと、

前記セッション鍵を前記クライアントエージェントに提供することと、を更に含む、請求項 1 に記載のコンピュータ実装方法。

30

【請求項 9】

シングルサインオンアプリケーション用の暗号化鍵を管理するためのシステムであって、

アイデンティティサービスから、クラウドサービス上の暗号化されたデータへのアクセス要求の通知であって、クラウドサービス鍵を復号するためのマスタ鍵を暗号化及び復号するためのセッション鍵を含む、通知を受信する、メモリに記憶された受信するための手段と、

ユーザから受信した少なくとも 1 つの認証要素に基づいて前記マスタ鍵を導出する、メモリに記憶された導出するための手段と、

前記マスタ鍵を使用して、前記クラウドサービス上のデータを復号するためのクラウドサービス鍵を復号する、メモリに記憶された復号するための手段と、

40

前記セッション鍵を使用して暗号化された前記マスタ鍵をクライアント鍵記憶部に記憶する、メモリに記憶された記憶するための手段と、を備え、

前記受信するための手段は、アイデンティティサービスから、追加のクラウドサービス上の暗号化されたデータへの追加のアクセス要求の追加の通知であって、前記セッション鍵を含む、通知を受信し、

前記復号するための手段は、再度前記ユーザから前記認証要素を取得することなしに、前記セッション鍵を使用することによって前記マスタ鍵を復号し、

前記復号するための手段は、前記マスタ鍵を使用して、前記追加のクラウドサービス上のデータを復号するための追加のクラウドサービス鍵を復号し、

50

前記システムは更に、前記受信するための手段、前記導出するための手段、前記復号するための手段、及び前記記憶するための手段を実行するように構成された少なくとも1つの物理プロセッサを備える、システム。

【請求項10】

前記導出するための手段は、前記ユーザから受信した前記認証要素にハッシュ関数を適用することによって前記マスタ鍵を導出する、請求項9に記載のシステム。

【請求項11】

前記復号するための手段は、前記暗号化されたデータを復号するために、前記復号されたクラウドサービス鍵を前記クラウドサービスに提供する、請求項9に記載のシステム。

【請求項12】

前記復号するための手段は、クライアント上で、前記復号されたクラウドサービス鍵を使用して復号するために、前記暗号化されたデータを前記クラウドサービスから受信する、請求項9に記載のシステム。

【請求項13】

前記復号するための手段は、

前記暗号化されたクラウドサービス鍵を前記クラウドサービス又は前記アイデンティティサービスの少なくとも1つから受信する、請求項9に記載のシステム。

【発明の詳細な説明】

【背景技術】

【0001】

ますます多くの個人及び組織は、機密データについてさえ、データ格納のためにクラウドベースのシステムを使用している。たいてい、クラウドデータ格納システムは、ベストプラクティスを頼りとしてクライアントのデータのセキュリティを確保する評判の良い大企業によって運用されている。残念ながら、広く報道されているクラウドサービスに格納された機密データのいくつかの漏洩によって証明されるように、ベストプラクティスでさえ、機密データを十全には保護し得ない。

【0002】

クラウドサービスに格納されたデータは、いくつかの点で脆弱である場合が多い。ユーザのクラウドサービスアカウントへのアクセスは、そのアカウントのユーザ名及びパスワードを取得又は推測することができる任意の人からアクセス可能であることがある。データは、ユーザとクラウドサービスとの間のいずれかの方向において暗号化されずに、又は弱い暗号化のみで送信されることがある。システム管理者又はクラウドサービスによって用いられるデータバックアップサービスは、ユーザデータにアクセスし、それを不正な受信者に送信することができることがある。また、クラウドサービスはユーザデータを暗号化された形式で格納し得るが、データを復号するのに必要な暗号鍵は、依然としてクラウドサービスのシステム管理者からアクセス可能であることがある。

【0003】

クラウドサービスによって使用されるセキュリティプラクティスの大部分は典型的に秘密であるので、適切なセキュリティ対策が実装されているとユーザを安心させるものはクラウドサービスの評判だけであることがある。一部の大規模組織は、自らのクラウドストレージサービスを運用することによって、機密データが必ず十全に保護されているようにしようとする。たとえそうでも、これらの組織は依然として、データセキュリティポリシーが必ず適切に実装されるように雇用するシステム管理者の能力及び高潔性を頼りとする。

【0004】

たとえユーザが他人からアクセス不能な強力なパスワードで自分のアカウントを保護し、クラウドサービスへ、及びクラウドサービスから送信されるデータをセキュアに暗号化し、クラウドサービスがデータセキュリティのベストプラクティスを実装していても、クラウドサービスは依然として、政府によって法的に要求される場合、機密データを利用可能にする義務を有し得る。これらの対策を実装し、クラウドベースのアプリケーションに

10

20

30

40

50

アクセスする度に認証証明書を提供することをユーザに要求することは、ユーザにとって不便であり得る。従って、本開示は、シングルサインオンアプリケーション用の暗号化鍵を管理するための追加の、かつ改善されたシステム及び方法に対する必要性を識別し、それに対処するものである。

#### 【発明の概要】

#### 【0005】

詳細に後述するように、本開示は、シングルサインオンアプリケーション用の暗号化鍵を管理するための様々なシステム及び方法を記載する。開示するシステム及び方法は、マスタ鍵を使用して鍵を暗号化し、暗号化された形式で鍵を格納することによって、データを復号するための鍵をクラウドサービス内に維持する。開示するシステム及び方法は、クラウドサービスのニーズ及び所望のデータセキュリティレベルに応じて様々な場所に暗号化鍵を格納することを容易にする。高度なデータセキュリティレベルが望ましい状況では、開示するシステム及び方法は、クラウドサービスが、暗号化されていないデータ、又はユーザデータを復号するための鍵のいずれかにアクセスすることを許可しないことがある。

10

#### 【0006】

一実施例では、シングルサインオンアプリケーション用の暗号化鍵を管理するためのコンピュータ実装方法は、(1) アイデンティティサービスから、クラウドサービス上の暗号化されたデータへのアクセス要求の通知であって、クラウドサービス鍵を復号するためのマスタ鍵を暗号化及び復号するためのセッション鍵を含む、通知を受信することと、(2) ユーザから受信した少なくとも1つの認証要素に基づいて、マスタ鍵を導出することと、(3) マスタ鍵を使用して、クラウドサービス上のデータを復号するためのクラウドサービス鍵を復号することと、(4) セッション鍵を使用して暗号化されたマスタ鍵をクライアント鍵記憶部内に格納することと、(5) アイデンティティサービスから、追加のクラウドサービス上の暗号化されたデータへの追加のアクセス要求の追加の通知であって、セッション鍵を含む、通知を受信することと、(6) 再度ユーザから認証要素を取得することなしに、セッション鍵を使用することによってマスタ鍵を復号することと、(7) マスタ鍵を使用して、追加のクラウドサービス上のデータを復号するための追加のクラウドサービス鍵を復号することと、を含んでもよい。

20

#### 【0007】

一部の例では、マスタ鍵を導出することは、ユーザから受信した認証要素にハッシュ関数を適用することを含んでもよい。一部の例では、マスタ鍵を導出することは、(1) ユーザから受信した認証要素に基づいてユーザを認証すること、(2) ユーザを認証することに応答して、マスタ鍵を暗号化及び復号するための秘密鍵を検索すること、(3) 秘密鍵を使用してマスタ鍵を復号すること、を含んでもよい。

30

#### 【0008】

一部の例では、コンピュータ実装方法は、暗号化されたデータを復号するために、復号されたクラウドサービス鍵をクラウドサービスに提供することを更に含んでもよい。一実施形態では、コンピュータ実装方法は、クライアント上で、復号されたクラウドサービス鍵を使用して復号するために、暗号化されたデータをクラウドサービスから受信することを更に含んでもよい。一部の例では、コンピュータ実装方法は、暗号化されたクラウドサービス鍵をクラウドサービスから受信することを更に含んでもよい。一部の例では、コンピュータ実装方法は、暗号化されたクラウドサービス鍵をアイデンティティサービスから受信することを更に含んでもよい。

40

#### 【0009】

一部の例では、暗号化されたクラウドサービス鍵を受信することは、セッション鍵と共にクラウドサービス鍵を受信すること、及び／又はクラウドサービス鍵を提供することを求めるアイデンティティサービスに対する要求に応答してクラウドサービス鍵を受信することを含んでもよい。一実施形態では、コンピュータ実装方法は、クラウドサービス鍵を復号するためのマスタ鍵を暗号化及び復号するためのセッション鍵を

50

クライアントエージェントに提供することによってクラウドサービス上の暗号化されたデータへのアクセスを容易にすることを求める要求を、アイデンティティサービスにおいて受信することと、セッション鍵をクライアントエージェントに提供することと、を更に含んでもよい。

#### 【0010】

一実施形態では、上記の方法を実装するためのシステムは、(1) アイデンティティサービスから、クラウドサービス上の暗号化されたデータへのアクセス要求の通知であって、クラウドサービス鍵を復号するためのマスタ鍵を暗号化及び復号するためのセッション鍵を含む、通知を受信し、アイデンティティサービスから、追加のクラウドサービス上の暗号化されたデータへの追加のアクセス要求の追加の通知であって、セッション鍵を含む、通知を受信するセッションモジュール、(2) ユーザから受信した少なくとも1つの認証要素に基づいてマスタ鍵を導出する導出モジュール、(3) マスタ鍵を使用して、クラウドサービス上のデータを復号するためのクラウドサービス鍵を復号し、マスタ鍵を使用して、追加のクラウドサービス上のデータを復号するための追加のクラウドサービス鍵を復号するサービスモジュール、(4) セッション鍵を使用して暗号化されたマスタ鍵をクライアント鍵記憶部に格納する暗号化モジュール、及び／又は(5) 再度ユーザから認証要素を取得することなしに、セッション鍵を使用してマスタ鍵を復号する復号モジュール、などのメモリに格納されたいくつかのモジュールを含んでもよい。本システムはまた、セッションモジュール、導出モジュール、サービスモジュール、暗号化モジュール、及び復号モジュールを実行するように構成された少なくとも1つの物理プロセッサを含んでもよい。

10

20

#### 【0011】

いくつかの実施例では、上述の方法は、非一時的コンピュータ可読媒体上のコンピュータ可読命令としてコード化されてもよい。例えば、コンピュータ可読媒体は、コンピューティングデバイスの少なくとも1つのプロセッサによって実行されるとき、コンピューティングデバイスに、(1) アイデンティティサービスから、クラウドサービス上の暗号化されたデータへのアクセス要求の通知であって、クラウドサービス鍵を復号するためのマスタ鍵を暗号化及び復号するためのセッション鍵を含む、通知を受信することと、(2) ユーザから受信した少なくとも1つの認証要素に基づいて、マスタ鍵を導出することと、(3) マスタ鍵を使用して、クラウドサービス上のデータを復号するためのクラウドサービス鍵を復号することと、(4) セッション鍵を使用して暗号化されたマスタ鍵をクライアント鍵記憶部に格納することと、(5) アイデンティティサービスから、追加のクラウドサービス上の暗号化されたデータへの追加のアクセス要求の追加の通知であって、当該セッション鍵を含む、通知を受信することと、(6) 再度ユーザから認証要素を取得することなしに、セッション鍵を使用することによってマスタ鍵を復号することと、(7) マスタ鍵を使用して、追加のクラウドサービス上のデータを復号するための追加のクラウドサービス鍵を復号することと、を行わせる1つ又は2つ以上のコンピュータ実行可能命令を含んでもよい。

30

#### 【0012】

上述の実施形態のいずれかによる特徴は、本明細書に記載される一般原理に従って、互いに組み合わせて使用されてもよい。これら及び他の実施形態、特徴、及び利点は、添付の図面及び特許請求の範囲と併せて以下の発明を実施するための形態を読むことによって更に十分に理解されるだろう。

40

#### 【図面の簡単な説明】

#### 【0013】

添付の図面は、いくつかの例示的な実施形態を図示するものであり、本明細書の一部である。以下の説明と併せて、これらの図面は、本開示の様々な原理を実証及び説明する。

【図1】 シングルサインオンアプリケーション用の暗号化鍵を管理するための例示的なシステムのブロック図である。

【図2】 シングルサインオンアプリケーション用の暗号化鍵を管理するための追加の例示

50

的なシステムのブロック図である。

【図3】シングルサインオンアプリケーション用の暗号化鍵を管理するための例示的な方法の流れ図である。

【図4】シングルサインオンアプリケーション用の暗号化鍵を管理するための追加の例示的なシステムのブロック図である。

【図5】本明細書に記載及び／又は図示される実施形態のうち1つ又は2つ以上を実装することができる例示的なコンピューティングシステムのブロック図である。

【図6】本明細書に記載及び／又は図示される実施形態のうち1つ又は2つ以上を実装することができる例示的なコンピューティングネットワークのブロック図である。図面を通して、同一の参照符号及び記述は、必ずしも同一ではないが、類似の要素を示す。本明細書で説明される例示の実施形態は、様々な修正物及び代替的な形態が可能であるが、特定の実施形態が例として図面に示されており、本明細書に詳細に記載される。しかしながら、本明細書に記載される例示の実施形態は、開示される特定の形態に限定されることを意図しない。むしろ、本開示は、添付の特許請求の範囲内にある全ての修正物、等価物、及び代替物を網羅する。

【発明を実施するための形態】

【0014】

本開示は、一般に、シングルサインオンアプリケーション用の暗号化鍵を管理するためのシステム及び方法を対象にする。詳細に後述するように、本明細書に記載するシステム及び方法は、暗号化されたデータのセキュリティを損なうことなしに、シングルサインオンを容易にするように暗号化鍵を管理し得る。本明細書に記載するシステム及び方法は、再認証なしに、かつ暗号化されたデータと共に暗号化鍵を格納する必要なしに、複数のクラウドサービスに常駐する暗号化されたデータへのユーザアクセスを提供し得る。開示するシステムの一部の実施形態では、クラウドサービスは、データストアを復号するのに必要な鍵に決してアクセスせず、各暗号化されたデータストアのデータは、一意の暗号化鍵を使用して暗号化され得る。一部の実施形態では、開示するシステム及び方法は、複数のデバイスからのシングルサインオンを容易にし得る。クラウドアプリケーションにシングルサインオンを提供することに加えて、開示するシステム及び方法は、クライアントアプリケーションにも適用され得る。

【0015】

以下において、図1、図2、及び図4を参照しながら、シングルサインオンアプリケーション用の暗号化鍵を管理するための例示的なシステムの詳細な説明を提供する。対応するコンピュータ実装方法の詳細な説明も図3に関連して提供される。それに加えて、本明細書に記載する実施形態のうち1つ又は2つ以上を実装することができる例示的なコンピューティングシステム及びネットワークアーキテクチャの詳細な説明が、それぞれ図5及び図6に関連して提供されることになる。

【0016】

図1は、シングルサインオンアプリケーション用の暗号化鍵を管理するための例示的なシステム100のブロック図である。この図に図示されるように、例示的なシステム100は、1つ以上のタスクを実施するための1つ以上のモジュール102を含んでもよい。例えば、詳細に後述するように、例示的なシステム100は、アイデンティティサービスから、クラウドサービス上の暗号化されたデータへのアクセス要求の通知であって、クラウドサービス鍵を復号するためのマスタ鍵を暗号化及び復号するためのセッション鍵を含む、通知を受信するセッションモジュール104を含んでもよい。それに加えて、例示的なシステム100は、ユーザから受信した少なくとも1つの認証要素に基づいてマスタ鍵を導出する導出モジュール106を含んでもよい。例示的なシステム100はまた、マスタ鍵を使用して、クラウドサービス上のデータを復号するためのクラウドサービス鍵を復号するサービスモジュール108を含んでもよい。それに加えて、例示的なシステム100は、セッション鍵を使用して暗号化されたマスタ鍵をクライアント鍵記憶部内に格納する暗号化モジュール110を含んでもよい。セッションモジュール104は、アイデンテ

ィティサービスから、追加のクラウドサービス上の暗号化されたデータへの追加のアクセス要求の追加の通知であって、セッション鍵を含む、通知を更に受信し得る。例示的なシステム100はまた、再度ユーザから認証要素を取得することなしに、セッション鍵を使用してマスタ鍵を復号する復号モジュール112を含んでもよい。サービスモジュール108は、マスタ鍵を使用して、追加のクラウドサービス上のデータを復号するための追加のクラウドサービス鍵を更に復号してもよい。別々の要素として図示されるが、図1のモジュール102のうちの1つ以上は、単一のモジュール又はアプリケーションの部分を表してもよい。

#### 【0017】

特定の実施形態では、図1のモジュール102のうち1つ以上は、コンピューティングデバイスによって実行されると、コンピューティングデバイスに1つ以上のタスクを実施させ得る、1つ以上のソフトウェアアプリケーション又はプログラムを表し得る。例えば、詳細に後述するように、モジュール102のうち1つ又は2つ以上は、図2に図示するデバイス（例えば、クライアント202及び／若しくはクラウドサービス206）、図5のコンピューティングシステム510、並びに／又は図6の例示的なネットワークアーキテクチャ600の部分などの、1つ又は2つ以上のコンピューティングデバイスに格納され、そこで作動するように構成されたソフトウェアモジュールを表し得る。図1のモジュール102のうち1つ以上はまた、1つ以上のタスクを実施するように構成されている1つ以上の専用コンピュータの全て又は一部を表し得る。

#### 【0018】

図1に示すように、例示的なシステム100はまた、データベース120などの1つ以上のデータベースを含んでもよい。一実施例では、データベース120は、ユーザアカウントデータ、クラウドサービス情報、及び／又は暗号鍵を格納するように構成してもよい。データベース120は、単一のデータベース若しくはコンピューティングデバイスの部分、又は複数のデータベース若しくはコンピューティングデバイスの部分を表してもよい。例えば、データベース120は、図2のクラウドサービス206若しくはアイデンティティサービス210の一部分、図5のコンピューティングシステム510、及び／又は図6の例示的なネットワークアーキテクチャ600の部分を表してもよい。あるいは、図1のデータベース120は、図2のクラウドサービス206若しくはアイデンティティサービス210、図5のコンピューティングシステム510、及び／又は図6の例示的なネットワークアーキテクチャ600の部分などの、コンピューティングデバイスによってアクセスすることができる1つ又は2つ以上の物理的に別個のデバイスを表してもよい。

#### 【0019】

図1の例示的なシステム100は、様々な方法で実装され得る。例えば、例示的なシステム100の全て又は一部は、図2における例示的なシステム200の部分を表してもよい。図2に示されるように、システム200は、ネットワーク204を介してクラウドサービス206及びアイデンティティサービス210と連通するクライアント202を含んでもよい。一実施例では、クライアント202は、モジュール102のうち1つ若しくは2つ以上を用いてプログラムされてもよく、かつ／又はデータベース120内のデータの全て若しくは一部分を格納してもよい。それに加えて、又は別の方法として、クラウドサービス206又はアイデンティティサービス210は、モジュール102のうち1つ若しくは2つ以上を用いてプログラムされてもよく、かつ／又はデータベース120内のデータの全て若しくは一部分を格納してもよい。

#### 【0020】

一実施形態では、図1からの1つ又は2つ以上のモジュール102は、クライアント202の少なくとも1つのプロセッサ、クラウドサービス206、及び／又はアイデンティティサービス210によって実行されるとき、クライアント202、クラウドサービス206、及び／又はアイデンティティサービス210がシングルサインアプリケーション用の暗号化鍵を管理することを可能にしてもよい。例えば、詳細に後述するように、1つ又は2つ以上のモジュール102は、クライアント202、クラウドサービス206、及び

／又はアイデンティティサービス 210 に、シングルサインオンアプリケーション用の暗号化鍵を管理させてもよい。例えば、詳細に後述するように、セッションモジュール 104 は、

アイデンティティサービス 210 から、クラウドサービス 208 (1) 上の暗号化されたデータへのアクセス要求の通知 212 であって、クラウドサービス鍵を復号するためのマスタ鍵 218 を暗号化及び復号するためのセッション鍵 214 を含む、通知 212 を受信してもよい。導出モジュール 106 は、ユーザから受信した少なくとも 1 つの認証要素 216 に基づいて、マスタ鍵 218 を導出してもよい。サービスモジュール 108 は、マスタ鍵 218 を使用して、クラウドサービス 208 (1) 上のデータを復号するためのクラウドサービス鍵 220 を復号してもよい。

10

#### 【0021】

一部の例では、暗号化モジュール 110 は、セッション鍵 214 を使用してストアマスタ鍵 218 を暗号化して、暗号化されたマスタ鍵 224 を生成し、暗号化されたマスタ鍵 224 をクライアント鍵記憶部 222 内に格納してもよい。セッションモジュール 104 は、アイデンティティサービス 210 から、追加のクラウドサービス 208 (2) 上の暗号化されたデータへの追加のアクセス要求の追加の通知 226 であって、通知 212 はセッション鍵 214 を含む、追加の通知 226 を受信してもよい。復号モジュール 112 は、再度ユーザから認証要素 216 を取得することなしに、セッション鍵 214 を使用してマスタ鍵 218 を復号してもよい。サービスモジュール 108 は、マスタ鍵 218 を使用して、追加のクラウドサービス 208 (2) 上のデータを復号するための追加のクラウドサービス鍵 230 を復号してもよい。

20

#### 【0022】

クライアント 202 は、一般に、コンピュータ実行可能命令を読み取ることができる任意のタイプ又は形態のコンピューティングデバイスを表す。クライアント 202 の例としては、ラップトップ、タブレット、デスクトップ、サーバ、携帯電話、携帯情報端末 (PDA)、マルチメディアプレーヤー、埋め込みシステム、ウェアラブルデバイス (例えば、スマートウォッチ、スマートグラスなど)、ゲーム機、それらの 1 つ若しくは 2 つ以上の組み合わせ、図 5 の例示的なコンピューティングシステム 510、又は他の任意の好適なコンピューティングデバイスが挙げられるが、これらに限定されない。

#### 【0023】

クラウドサービス 206 及びアイデンティティサービス 210 は、一般に、データを通信、比較、及び／又は格納することができる任意のタイプ又は形態のコンピューティングデバイスを表す。クラウドサービス 206 及びアイデンティティサービス 210 の例としては、様々なデータベースサービスを提供し、かつ／又は特定のソフトウェアアプリケーションを作動させるように構成されたアプリケーションサーバ及びデータベースサーバが挙げられるが、これらに限定されない。

30

#### 【0024】

ネットワーク 204 は、一般に、通信若しくはデータ転送を容易にすることが可能な、任意の媒体又はアーキテクチャを表す。ネットワーク 204 の例としては、イントラネット、広域ネットワーク (WAN)、ローカルエリアネットワーク (LAN)、パーソナルエリアネットワーク (PAN)、インターネット、電力線通信 (PLC)、セルラーネットワーク (例えば、Global System for Mobile Communications (GSM (登録商標)) ネットワーク)、図 6 の例示的なネットワークアーキテクチャ 600 などが挙げられるが、これらに限定されない。ネットワーク 204 は、無線接続又は有線接続を使用して、通信又はデータ転送を容易にしてもよい。一実施形態では、ネットワーク 204 は、クライアント 202、クラウドサービス 206、及びアイデンティティサービス 210 の間の通信を容易にしてもよい。

40

#### 【0025】

図 3 は、シングルサインオンアプリケーション用の暗号化鍵を管理するための例示的なコンピュータ実装方法 300 の流れ図である。図 3 に示されるステップは、任意の好適な

50

コンピュータ実行可能コード及び／又はコンピューティングシステムによって実施されてもよい。一部の実施形態では、図3に示すステップは、図1のシステム100、図2のシステム200、図5のコンピューティングシステム510、及び／又は図6の例示的なネットワークアーキテクチャ600の部分の構成要素のうち1つ又は2つ以上によって実施されてもよい。

#### 【0026】

図3に示すように、ステップ302では、本明細書に記載するシステムの1つ又は2つ以上は、アイデンティティサービスから、クラウドサービス上の暗号化されたデータへのアクセス要求の通知であって、クラウドサービス鍵を復号するためのマスタ鍵を暗号化及び復号するためのセッション鍵を含む、通知を受信してもよい。例えば、セッションモジュール104は、図2のクライアント202の一部として、アイデンティティサービス210から、クラウドサービス208(1)上の暗号化されたデータへのアクセス要求の通知212を受信してもよい。通知212は、マスタ鍵218を暗号化及び復号するためのセッション鍵214を含んでもよく、マスタ鍵218は、その後、クラウドサービス鍵を復号するために使用されてもよい。

10

#### 【0027】

「アイデンティティサービス」という用語は、本明細書で使用する時、一般に、ユーザが提供する認証証明書に基づいて本人確認を行うネットワークサービスを指す。アイデンティティサービスは、他のネットワークサービスプロバイダとの契約下で、プライベート組織内で、又はクラウドサービスの一部として、本人確認サービスを提供する独立したサービスプロバイダとして動作してもよい。

20

#### 【0028】

一実施形態では、アイデンティティサービス210は、クラウドサービス208(1)上の暗号化されたデータへのアクセスを容易にすることを求める要求を受信してもよい。この要求に応答して、アイデンティティサービス210は、クライアント202上のセッションモジュール104にセッション鍵214を提供してもよい。詳細に後述するように、本明細書に記載するシステムは、セッション鍵214を使用してマスタ鍵218を復号してもよく、マスタ鍵218は、その後、クラウドサービス鍵を復号するために使用されてもよい。

#### 【0029】

セッションモジュール104は、クラウドサービス上の暗号化されたデータへのアクセス要求の通知を様々な方法で受信してもよい。例えば、セッションモジュール104は、クライアント202上のクライアントエージェントの一部として実行し、クライアント202がクラウドサービス208(1)上に格納されたデータにアクセスすることができるように、クライアント202上のユーザの本人確認を行うことを求める要求をアイデンティティサービス210がクラウドサービス208(1)から受信したという通知212をアイデンティティサービス210から受信してもよい。セッションモジュール104は、クライアントエージェントによって確立されるロングポーリング接続を介して、又は他の任意の好適なメカニズムによって、HTTPサーバプッシュ通信として通知212を受信してもよい。

30

40

#### 【0030】

ステップ304では、本明細書に記載するシステムの1つ又は2つ以上は、ユーザから受信した1つ又は2つ以上の認証要素に基づいて、マスタ鍵を導出してもよい。例えば、導出モジュール106は、図2のクライアント202の一部として、ユーザから受信した1つ又は2つ以上の認証要素216に基づいて、マスタ鍵218を導出してもよい。詳細に後述するように、導出モジュール106は、ユーザから認証要素を取得し、シングルサインオンセッションの始めにマスタ鍵を導出してもよい。その後、本明細書に記載するシステムは、ユーザとの追加の相互作用なしに暗号化鍵を管理してもよい。

#### 【0031】

導出モジュール106は、マスタ鍵を様々な方法で導出してもよい。例えば、導出モジ

50

ジュール106は、ユーザから受信した認証要素にハッシュ関数を適用することによってマスタ鍵を導出してもよい。例えば、導出モジュール106は、パスワードベースの鍵導出機能2(PBKDF2)又は任意の好適な鍵導出機能を使用して、パスワード又は他の認証因子を暗号鍵に変換してもよい。

#### 【0032】

一部の例では、導出モジュール106は、マスタ鍵をアルゴリズムによって導出するのではなく、セキュアな鍵記憶部からマスタ鍵を検索してもよい。例えば、図2に示すように、導出モジュール106は、ユーザから受信した1つ又は2つ以上の認証要素216に基づいてユーザを最初に認証することにより、マスタ鍵218を導出してもよい。導出モジュール106は、ユーザを認証した後、マスタ鍵を暗号化及び復号するための秘密鍵を検索し、暗号化されたマスタ鍵をクライアント鍵記憶部222から検索し、秘密鍵を使用してマスタ鍵218を復号してもよい。詳細に後述するように、秘密鍵は、携帯電話などのパーソナルデバイス上に格納されてもよい。暗号化されたマスタ鍵は、クライアント鍵記憶部222内に格納されてもよく、クライアント鍵記憶部222は、クライアント202上、又はアイデンティティサービス210に常駐してもよい。

10

#### 【0033】

ステップ306では、本明細書に記載するシステムの1つ又は2つ以上は、マスタ鍵を使用して、クラウドサービス上のデータを復号するためのクラウドサービス鍵を復号してもよい。例えば、サービスモジュール108は、図2のクライアント202の一部として、マスタ鍵218を使用して、クラウドサービス208(1)上のデータを復号するためのクラウドサービス鍵220を復号してもよい。

20

#### 【0034】

サービスモジュール108は、クラウドサービス鍵を様々な方法で復号してもよい。例えば、サービスモジュール108は、暗号化されたクラウドサービス鍵をクラウドサービス208(1)から検索し、この暗号化された鍵をマスタ鍵218を使用して復号してクラウドサービス鍵220を生成してもよい。一部の例では、クライアント鍵記憶部222は、アイデンティティサービス210に常駐してもよい。サービスモジュール108は、暗号化されたクラウドサービス鍵をアイデンティティサービス210から検索し、マスタ鍵218を使用してクラウドサービス鍵を暗号化してクラウドサービス鍵220を生成してもよい。一部の例では、サービスモジュール108は、セッション鍵と共にクラウドサービス鍵を受信すること、及び／又は暗号化されたクラウドサービス鍵を提供することを求めるアイデンティティサービス210に対する要求に応答してクラウドサービス鍵を受信することによって、暗号化されたクラウドサービス鍵を受信してもよい。

30

#### 【0035】

クラウドサービス鍵220を復号した後、サービスモジュール108は、クラウドサービス鍵220を使用して、クラウドサービス208(1)が格納する暗号化されたデータを復号してもよい。一部の例では、サービスモジュール108は、暗号化されたデータを復号するために、復号されたクラウドサービス鍵220をクラウドサービス208(1)に提供してもよい。データを復号した後、クラウドサービス208(1)は、復号されたデータをクライアント202に送信してもよい。次いで、クラウドサービス208(1)は、クラウドサービス鍵220が、暗号化されたデータと共にクラウドサービス208(1)上に残らないように、クラウドサービス鍵220を破棄してもよい。一部の例では、サービスモジュール108は、クラウドサービス208(1)から暗号化されたデータを受信し、クラウドサービス鍵220を使用してデータを復号してもよい。この例では、クラウドサービス208(1)は、クラウドサービス208(1)上に格納されたデータを復号するために必要なクラウドサービス鍵220を一時的にでさえ取得しない。

40

#### 【0036】

ステップ308では、本明細書に記載するシステムの1つ又は2つ以上は、セッション鍵を使用して暗号化されたマスタ鍵をクライアント鍵記憶部内に格納してもよい。例えば、暗号化モジュール110は、図2のクライアント202の一部として、セッション鍵2

50

14を使用して暗号化されたマスタ鍵218をクライアント鍵記憶部222内に格納してもよい。

#### 【0037】

暗号化モジュール110は、暗号化されたマスタ鍵を様々な方法で格納してもよい。例えば、暗号化モジュール110は、セッション鍵214を使用してマスタ鍵218を暗号化し、暗号化されたマスタ鍵をクライアント鍵記憶部222内に格納してもよく、クライアント鍵記憶部222は、クライアント202上に常駐してもよい。あるいは、暗号化モジュール110は、暗号化されたマスタ鍵を、アイデンティティサービス210上に常駐するクライアント鍵記憶部222内に格納してもよい。詳細に後述するように、クライアント鍵記憶部222をアイデンティティサービス210上に配置することは、複数のクライアントからのクラウドサービスへのシングルサインオンを容易にし得る。

10

#### 【0038】

ステップ310では、本明細書に記載するシステムの1つ又は2つ以上は、アイデンティティサービスから、追加のクラウドサービス上の暗号化されたデータへの追加のアクセス要求の追加の通知であって、セッション鍵を含む、通知を受信してもよい。例えば、セッションモジュール104は、図2のクライアント202の一部として、アイデンティティサービス210から、クラウドサービス208(2)上の暗号化されたデータへの追加のアクセス要求の追加の通知226を受信してもよく、通知212はセッション鍵214を含む。

#### 【0039】

20

セッションモジュール104は、クラウドサービス上の暗号化されたデータへの追加のアクセス要求を様々な方法で受信してもよい。例えば、セッションモジュール104は、アイデンティティサービス210からセッション鍵214を含む追加の通知226を受信してもよい。別の例では、クライアント鍵記憶部222は、アイデンティティサービス210上に配置されてもよい。この例では、セッションモジュール104は、セッション鍵214と、マスタ鍵218で暗号化された追加のクラウドサービス鍵230とを含む追加の通知226を受信してもよい。

#### 【0040】

ステップ312では、本明細書に記載するシステムの1つ又は2つ以上は、再度ユーザから認証要素を取得することなしに、セッション鍵を使用してマスタ鍵を復号してもよい。例えば、復号モジュール112は、図2のクライアント202の一部として、再度ユーザから認証要素216を取得することなしに、セッション鍵214を使用してマスタ鍵218を復号してもよい。

30

#### 【0041】

復号モジュール112は、マスタ鍵218を様々な方法で復号してもよい。例えば、復号モジュール112は、セッション鍵214を使用して暗号化された、暗号化されたマスタ鍵224をクライアント鍵記憶部222から検索してもよい。復号モジュール112は、セッション鍵214を使用して暗号化されたマスタ鍵224を復号して、復号されたマスタ鍵228を生成してもよい。別の例では、詳細に後述するように、復号モジュール112は、暗号化されたマスタ鍵224を携帯電話などのパーソナルデバイスから検索してもよい。

40

#### 【0042】

ステップ314では、本明細書に記載するシステムの1つ又は2つ以上は、マスタ鍵を使用して、追加のクラウドサービス上のデータを復号するための追加のクラウドサービス鍵を復号してもよい。例えば、サービスモジュール108は、図2のクライアント202の一部として、復号されたマスタ鍵228を使用して、追加のクラウドサービス208(2)上のデータを復号するための追加のクラウドサービス鍵230を復号してもよい。

#### 【0043】

サービスモジュール108は、追加のクラウドサービス鍵230を様々な方法で復号してもよい。例えば、サービスモジュール108は、マスタ鍵218を使用して暗号化され

50

た追加のクラウドサービス鍵 230 をクラウドサービス 208 (2) から検索してもよい。サービスモジュールは、復号されたマスタ鍵 228 を使用して追加のクラウドサービス鍵 230 を復号してもよい。別の例では、サービスモジュール 108 は、追加のクラウドサービス鍵 230 をアイデンティティサービス 210 から検索してもよい。

#### 【0044】

図 4 は、シングルサインオンアプリケーション用の暗号化鍵を管理するための追加の例示的なシステム 400 のブロック図である。例示的なシステム 400 は、本明細書に記載するシステムがどのようにして複数のクライアントデバイスからのシングルサインオンを容易にするように暗号化鍵を管理し得るかを図示する。例示的なシステム 400 は、クライアント 202、ネットワーク 204、クラウドサービス 206、及びアイデンティティサービス 210 などの、図 2 の例示的なシステム 200 のいくつかのコンポーネントを含む。クライアント鍵記憶部 222 は、アイデンティティサービス 210 上に配置されてもよい。例示的なシステム 400 はまた、パーソナルデバイス 402 を含み、パーソナルデバイス 402 は、秘密鍵記憶部 404 を含む。例示的なシステム 400 はまた、追加のクライアント 408 を含み、追加のクライアント 408 は、クライアント 202 のように、図 1 に示すモジュール 102 を含む。

#### 【0045】

一実施例では、ユーザは、クラウドサービス 208 (1) 上の暗号化されたデータにクライアント 202 からアクセスしようと試みてもよい。クラウドサービス 208 (1) は、クライアント 202 がクラウドサービス 208 (1) 上のデータにアクセスすることを許可する前に、アイデンティティサービス 210 がユーザの本人確認を行うことを要求してもよい。アイデンティティサービス 210 は、クライアント 202 上のモジュール 102 に通知 212 を送信してもよく、通知 212 は、セッション鍵 214 と、パーソナルデバイス 402 上の秘密鍵記憶部 404 内に格納された秘密鍵 406 を使用して暗号化された、暗号化されたマスタ鍵 224 と、マスタ鍵 218 を使用して暗号化された、暗号化されたクラウドサービス鍵 410 とを含んでもよい。通知 212 を受信することに応答して、クライアント 202 上のモジュール 102 は、ユーザを認証してもよい。あるいは、クライアント 202 上のモジュール 102 は、ユーザに、パーソナルデバイス 402 上でパスワードを入力するか、又は認証用の他の認証要素を提供するように指示してもよい。

#### 【0046】

ユーザが認証された後、クライアント 202 上のモジュール 102 は、セッション鍵 214 をパーソナルデバイス 402 に送信してもよい。パーソナルデバイス 402 は、セッション鍵 215 を使用して秘密鍵 406 を暗号化して、暗号化された秘密鍵 414 を生成し、次いで、暗号化された秘密鍵 414 をクライアント 202 に送信してもよい。クライアント 202 上のモジュール 102 は、セッション鍵 214 を使用して秘密鍵 406 を復号し、次いで、秘密鍵 406 を使用して暗号化されたマスタ鍵 224 を復号して、マスタ鍵 218 を生成してもよい。次いで、モジュール 102 は、セッション鍵 214 を使用してマスタ鍵 218 を再暗号化し、暗号化されたマスタ鍵を、秘密鍵記憶部 404 内に格納するために、パーソナルデバイス 402 に送信してもよい。次いで、モジュール 102 は、マスタ鍵 218 を使用してクラウドサービス鍵 220 を復号してもよい。次いで、クライアント 202 は、クラウドサービス 208 (1) 上に格納された暗号化されたデータを復号するために、復号されたクラウドサービス鍵 220 をクラウドサービス 208 (1) に提供してもよい。あるいは、クライアント 202 は、クラウドサービス 208 (1) から暗号化されたデータを検索し、暗号化されたデータをクライアント 202 上でクラウドサービス鍵 220 を使用して復号してもよい。

#### 【0047】

クラウドサービス 208 (1) 上のデータにクライアント 202 からアクセスした後、ユーザは、クラウドサービス 208 (2) 上の暗号化されたデータに追加のクライアント 408 からアクセスしようと試みてもよい。クラウドサービス 208 (2) は、追加のクライアント 408 がクラウドサービス 208 (2) 上のデータにアクセスすることを許可

10

20

30

40

50

する前に、アイデンティティサービス 210 がユーザの本人確認を行うことを要求してもよい。アイデンティティサービス 210 は、追加の通知 226 を追加のクライアント 408 上のモジュール 102 に送信してもよい。通知 212 と同様に、追加の通知 226 は、セッション鍵 214 を含んでもよい。追加の通知 226 はまた、マスタ鍵 218 を使用して暗号化された、暗号化された追加クラウドサービス鍵 412 を含んでもよい。

#### 【0048】

ユーザの本人確認は既に行われているため、パスワード又は他の認証要素を提供する代わりに、ユーザがクラウドサービス 208 (2) 上の暗号化されたデータにアクセスしようと試みたこと、及びこのアクセスは既に確立済みのシングルサインオンセッションを使用して許可されるべきであることを、パーソナルデバイス 402 上で確認するようにユーザに指示してもよい。暗号化されたデータへのアクセスが許可されるべきであることをユーザが確認した後、パーソナルデバイス 402 は、セッション鍵 214 を使用して以前暗号化され、秘密鍵記憶部 406 内に格納されているマスタ鍵 218 を追加のクライアント 408 に送信してもよい。追加のクライアント 408 上のモジュール 102 は、アイデンティティサービス 210 から受信したセッション鍵 214 を使用してマスタ鍵 218 を復号してもよい。次いで、追加のクライアント 408 上のモジュール 102 は、マスタ鍵 218 を使用して、暗号化された追加のクラウドサービス鍵 412 を復号し、追加のクラウドサービス鍵 230 を生成してもよい。次いで、追加のクライアント 408 上のモジュール 102 は、追加のクラウドサービス鍵 230 をクラウドサービス 208 (2) に提供すること、又はクラウドサービス 208 (2) から暗号化されたデータを検索し、追加のクライアント 408 上のデータを復号することのいずれかによって、追加のクラウドサービス鍵 230 を使用してクラウドサービス 208 (2) 上の暗号化されたデータを復号してもよい。

#### 【0049】

上記で詳細に記載したように、本明細書に記載するシステム及び方法は、アプリケーションと共に格納される暗号化されたデータのセキュリティを維持しながら、複数のクラウドアプリケーションへのシングルサインオンを容易にするように暗号化鍵を管理してもよい。本明細書に記載するシステム及び方法は、暗号化鍵が暗号化されたデータと共に格納される必要なしに、暗号化されたデータストアへのユーザアクセスを提供してもよい。一部の実施形態では、クラウドサービスは、決して、一時的にでさえ、サービスに格納されたユーザデータを復号するために必要な鍵にアクセスしない。

#### 【0050】

図 5 は、本明細書に記載及び／又は図示される実施形態のうち 1 つ又は 2 つ以上を実装することができる例示的なコンピューティングシステム 510 のブロック図である。例えば、コンピューティングシステム 510 の全て又は一部は、単独で又は他の要素と組み合わせてのいずれかで、(図 3 に示されるステップのうち 1 つ又は 2 つ以上などの) 本明細書に記載するステップのうち 1 つ又は 2 つ以上を実施してもよく、かつ／又はそれを実施するための手段となってもよい。コンピューティングシステム 510 の全て又は一部はまた、本明細書に記載及び／又は図示される他の任意のステップ、方法、若しくは処理を実施してもよく、かつ／又はそれを実施するための手段であってもよい。

#### 【0051】

コンピューティングシステム 510 は、コンピュータ可読命令を実行することができる任意のシングル若しくはマルチプロセッサのコンピューティングデバイス又はシステムを幅広く表す。コンピューティングシステム 510 の例としては、ワークステーション、ラップトップ、クライアント側端末、サーバ、分散型コンピューティングシステム、ハンドヘルドデバイス、又は他の任意のコンピューティングシステム若しくはデバイスが挙げられるが、これらに限定されない。その最も基本的な構成において、コンピューティングシステム 510 は、少なくとも 1 つのプロセッサ 514 及びシステムメモリ 516 を含んでもよい。

#### 【0052】

プロセッサ 514 は、一般に、データの処理又は命令の解釈及び実行が可能な任意のタイプ又は形態の物理的処理ユニット（例えば、ハードウェア実装型中央処理ユニット）を表す。特定の実施形態では、プロセッサ 514 は、ソフトウェアアプリケーション又はモジュールから命令を受信してもよい。これらの命令は、プロセッサ 514 に、本明細書に記載及び／又は図示される例示的な実施形態のうち 1 つ又は 2 つ以上の機能を実施させてもよい。

#### 【0053】

システムメモリ 516 は、一般に、データ及び／又は他のコンピュータ可読命令を格納することができる任意のタイプ又は形態の揮発性又は不揮発性の記憶デバイス又は媒体を表す。システムメモリ 516 の例としては、ランダムアクセスメモリ（RAM）、読み取り専用メモリ（ROM）、フラッシュメモリ、又は他の任意の好適なメモリデバイスが挙げられるが、これらに限定されない。必須ではないが、特定の実施形態では、コンピューティングシステム 510 は、揮発性メモリユニット（例えば、システムメモリ 516 など）、及び不揮発性記憶デバイス（例えば、詳細に後述するような、一次記憶デバイス 532 など）の両方を含んでもよい。一実施例では、図 1 のモジュール 102 のうち 1 つ又は 2 つ以上がシステムメモリ 516 内にロードされてもよい。

#### 【0054】

特定の実施形態では、例示的なコンピューティングシステム 510 はまた、プロセッサ 514 及びシステムメモリ 516 に加えて、1 つ又は 2 つ以上の構成要素又は要素を含んでもよい。例えば、図 5 に示されるように、コンピューティングシステム 510 は、メモリコントローラ 518、入力／出力（I/O）コントローラ 520、及び通信インターフェース 522 を含んでもよいが、それらはそれぞれ通信基盤 512 を介して相互接続されてもよい。通信基盤 512 は、一般に、コンピューティングデバイスの 1 つ又は 2 つ以上の構成要素間の通信を容易にすることができる、任意のタイプ又は形態の基盤を表す。通信インフラストラクチャ 512 の例としては、通信バス（産業標準構成（ISA）、周辺装置相互接続（PCI）、PCI エクスプレス（PCIe）、又は類似のバスなど）及びネットワークが挙げられるが、これらに限定されない。

#### 【0055】

メモリコントローラ 518 は、一般に、メモリ若しくはデータを扱うこと、又はコンピューティングシステム 510 の 1 つ若しくは 2 つ以上の構成要素間の通信を制御することができる、任意のタイプ又は形態のデバイスを表す。例えば、特定の実施形態では、メモリコントローラ 518 は、通信基盤 512 を介して、プロセッサ 514、システムメモリ 516、及び I/O コントローラ 520 の間の通信を制御してもよい。

#### 【0056】

I/O コントローラ 520 は、一般に、コンピューティングデバイスの入出力機能を調整及び／又は制御することができる、任意のタイプ又は形態のモジュールを表す。例えば、特定の実施形態では、I/O コントローラ 520 は、プロセッサ 514、システムメモリ 516、通信インターフェース 522、ディスプレイアダプタ 526、入力インターフェース 530、及び記憶インターフェース 534 などの、コンピューティングシステム 510 の 1 つ又は 2 つ以上の要素間におけるデータの転送を制御し、又はそれを容易にしてもよい。

#### 【0057】

通信インターフェース 522 は、例示的なコンピューティングシステム 510 と 1 つ又は 2 つ以上の追加のデバイスとの間の通信を容易にすることができる、任意のタイプ又は形態の通信デバイス又はアダプタを幅広く表す。例えば、特定の実施形態では、通信インターフェース 522 は、コンピューティングシステム 510 と、追加のコンピューティングシステムを含む私設又は公衆ネットワークとの間の通信を容易にしてもよい。通信インターフェース 522 の例としては、有線ネットワークインターフェース（ネットワークインターフェースカードなど）、無線ネットワークインターフェース（無線ネットワークインターフェースカードなど）、モデム、及び他の任意の好適なインターフェースが挙げら

10

20

30

40

50

れるが、これらに限定されない。少なくとも1つの実施形態では、通信インターフェース522は、インターネットなどのネットワークへの直接リンクを介して、リモートサーバへの直接接続を提供してもよい。通信インターフェース522はまた、例えば、ローカルエリアネットワーク（イーサネット（登録商標）ネットワークなど）、パーソナルエリアネットワーク、電話若しくはケーブルネットワーク、セルラー電話接続、衛星データ接続、又は他の任意の好適な接続を通して、このような接続を間接的に提供してもよい。

#### 【0058】

特定の実施形態では、通信インターフェース522はまた、外部バス又は通信チャネルを介して、コンピューティングシステム510と1つ又は2つ以上の追加のネットワーク又は記憶デバイスとの間の通信を容易にするように構成された、ホストアダプタを表してもよい。ホストアダプタの例としては、非限定的に、小型コンピュータシステムインターフェース（SCSI）ホストアダプタ、ユニバーサルシリアルバス（USB）ホストアダプタ、米国電気電子学会（IEEE）1394ホストアダプタ、アドバンスドテクノロジーアタッチメント（ATA）、パラレルATA（PATA）、シリアルATA（SATA）、及び外部SATA（eSATA）ホストアダプタ、ファイバーチャネルインターフェースアダプタ、イーサネット（登録商標）アダプタなどが挙げられる。通信インターフェース522はまた、コンピューティングシステム510が分散型又はリモートコンピューティングに参与することを可能にしてもよい。例えば、通信インターフェース522は、実行のためにリモートデバイスから命令を受信し、又はリモートデバイスに命令を送信してもよい。

#### 【0059】

図5に示すように、コンピューティングシステム510はまた、ディスプレイアダプタ526を介して通信基盤512に連結される少なくとも1つのディスプレイデバイス524を含んでもよい。ディスプレイデバイス524は、一般に、ディスプレイアダプタ526によって送付される情報を視覚的に表示することができる、任意のタイプ又は形態のデバイスを表す。同様に、ディスプレイアダプタ526は、一般に、ディスプレイデバイス524上に表示するために、通信基盤512から（又は当該技術分野において既知であるように、フレームバッファから）グラフィックス、テキスト、及び他のデータを送付するように構成された、任意のタイプ又は形態のデバイスを表す。

#### 【0060】

図5に示すように、例示的なコンピューティングシステム510はまた、入力インターフェース530を介して通信基盤512に連結される少なくとも1つの入力デバイス528を含んでもよい。入力デバイス528は、一般に、コンピュータ又は人間のいずれかが生成した入力を、例示的なコンピューティングシステム510に提供することができる、任意のタイプ又は形態の入力デバイスを表す。入力デバイス528の例としては、キーボード、ポインティングデバイス、音声認識デバイス、又は他の任意の入力デバイスが挙げられるが、これらに限定されない。

#### 【0061】

図5に示すように、例示的なコンピューティングシステム510はまた、記憶インターフェース534を介して通信基盤512に連結される、一次記憶デバイス532及びバックアップ記憶デバイス533を含んでもよい。記憶デバイス532及び533は、一般に、データ及び／又は他のコンピュータ可読命令を格納することができる、任意のタイプ又は形態の記憶デバイス又は媒体を表す。例えば、記憶デバイス532及び533は、磁気ディスクドライブ（例えば、いわゆるハードドライブ）、ソリッドステートドライブ、フロッピーディスクドライブ、磁気テープドライブ、光ディスクドライブ、フラッシュドライブなどであってもよい。記憶インターフェース534は、一般に、記憶デバイス532及び533とコンピューティングシステム510の他の構成要素との間でデータを転送するための、任意のタイプ又は形態のインターフェース又はデバイスを表す。一実施例では、図1のデータベース120は、一次記憶デバイス532内に格納されてもよい。

#### 【0062】

特定の実施形態では、記憶デバイス 532 及び 533 は、コンピュータソフトウェア、データ、又は他のコンピュータ可読情報を格納するように構成された取外し可能な記憶ユニットから読み取り、かつ／又はそれに書き込むように構成されてもよい。好適な取外し可能な記憶ユニットの例としては、非限定的に、フロッピーディスク、磁気テープ、光ディスク、フラッシュメモリデバイスなどが挙げられる。記憶デバイス 532 及び 533 はまた、コンピュータソフトウェア、データ、又は他のコンピュータ可読命令がコンピューティングシステム 510 内にロードされることを可能にする、他の同様の構造体又はデバイスを含んでもよい。例えば、記憶デバイス 532 及び 533 は、ソフトウェア、データ、又は他のコンピュータ可読情報を読み取り、かつ書き込むように構成されてもよい。記憶デバイス 532 及び 533 はまた、コンピューティングシステム 510 の一部であってもよく、又は他のインターフェースシステムを通してアクセスされる別個のデバイスであってもよい。

10

#### 【0063】

他の多くのデバイス又はサブシステムが、コンピューティングシステム 510 に接続されてもよい。反対に、図 5 に示す構成要素及びデバイスの全てが、本明細書に記載及び／又は図示される実施形態を實踐するために存在する必要があるわけではない。上記で言及したデバイス及びサブシステムはまた、図 5 に示されるものとは異なる方法で相互接続されてもよい。コンピューティングシステム 510 はまた、任意の数のソフトウェア、ファームウェア、及び／又はハードウェア構成を用いてもよい。例えば、本明細書で開示する例示的な実施形態の 1 つ以上は、コンピュータ可読媒体上で、コンピュータプログラム（コンピュータソフトウェア、ソフトウェアアプリケーション、コンピュータ可読命令、又はコンピュータ制御論理とも称される）としてコード化されてもよい。「コンピュータ可読媒体」という用語は、本明細書で使用する時、一般に、コンピュータ可読命令を格納又は保有することができる、任意の形態のデバイス、キャリア、又は媒体を指す。コンピュータ可読媒体の例としては、非限定的に、搬送波などの伝送型媒体、並びに磁気記憶媒体（例えば、ハードディスクドライブ、テープドライブ、及びフロッピーディスク）、光学記憶媒体（例えば、コンパクトディスク（CD）、デジタルビデオディスク（DVD）、及びブルーレイ（BLU-RAY（登録商標））ディスク）、電子記憶媒体（例えば、ソリッドステートドライブ及びフラッシュメディア）、及び他の分散システムなどの非一時的媒体が挙げられる。

20

30

#### 【0064】

コンピュータプログラムを包含するコンピュータ可読媒体は、コンピューティングシステム 510 内にロードされてもよい。コンピュータ可読媒体に格納されたコンピュータプログラムの全て又は一部は、次いで、システムメモリ 516 内に、及び／又は記憶デバイス 532 及び 533 の様々な部分内に格納されてもよい。プロセッサ 514 によって実行されるとき、コンピューティングシステム 510 内にロードされたコンピュータプログラムは、プロセッサ 514 に、本明細書に記載及び／又は図示される例示的な実施形態のうち 1 つ又は 2 つ以上の機能を実施させてもよく、かつ／又はそれらを実施するための手段とならせてもよい。追加的に又は代替案として、本明細書に記載及び／又は図示される例示的な実施形態の 1 つ以上は、ファームウェア及び／又はハードウェアに実装されてもよい。例えば、コンピューティングシステム 510 は、本明細書で開示する例示的な実施形態のうち 1 つ又は 2 つ以上を実装するように適合された特定用途向け集積回路（ASIC）として構成されてもよい。

40

#### 【0065】

図 6 は、クライアントシステム 610、620、及び 630、並びにサーバ 640 及び 645 がネットワーク 650 に連結され得る、例示的なネットワークアーキテクチャ 600 のブロック図である。上記に詳述したように、ネットワークアーキテクチャ 600 の全て又は一部は、単独で又は他の要素と組み合わせてのいずれかで、（図 3 に示されるステップのうち 1 つ又は 2 つ以上などの）本明細書で開示するステップのうち 1 つ又は 2 つ以上を実施してもよく、かつ／又はそれを実施するための手段となってもよい。ネットワー

50

クアーキテクチャ 600 の全て又は一部はまた、本開示に記載される他のステップ及び特徴を実施するために使用されてもよく、かつ／又はそれを実施するための手段となってもよい。

#### 【0066】

クライアントシステム 610、620、及び 630 は、一般に、図 5 の例示的なコンピューティングシステム 510 などの、任意のタイプ又は形態のコンピューティングデバイス又はシステムを表す。同様に、サーバ 640 及び 645 は、一般に、様々なデータベースサービスを提供し、かつ／又は特定のソフトウェアアプリケーションを実行するように構成された、アプリケーションサーバ又はデータベースサーバなどのコンピューティングデバイス又はシステムを表す。ネットワーク 650 は、一般に、例えばイントラネット、WAN、LAN、PAN、又はインターネットを含む、任意の電気通信ネットワーク又はコンピュータネットワークを表す。一実施例では、クライアントシステム 610、620、及び／若しくは 630、並びに／又はサーバ 640 及び／若しくは 645 は、図 1 からのシステム 100 の全て又は一部を含んでもよい。

#### 【0067】

図 6 に示すように、1 つ又は 2 つ以上の記憶デバイス 660 (1) ~ (N) は、サーバ 640 に直接取り付けられてもよい。同様に、1 つ又は 2 つ以上の記憶デバイス 670 (1) ~ (N) は、サーバ 645 に直接取り付けられてもよい。記憶デバイス 660 (1) ~ (N) 及び記憶デバイス 670 (1) ~ (N) は、一般に、データ及び／又は他のコンピュータ可読命令を格納することができる、任意のタイプ又は形態の記憶デバイス又は媒体を表す。特定の実施形態では、記憶デバイス 660 (1) ~ (N) 及び記憶デバイス 670 (1) ~ (N) は、ネットワークファイルシステム (NFS)、サーバメッセージブロック (SMB)、又は共通インターネットファイルシステム (CIFS) などの、様々なプロトコルを使用して、サーバ 640 及び 645 と通信するように構成された、ネットワーク接続ストレージ (NAS) デバイスを表してもよい。

#### 【0068】

サーバ 640 及び 645 はまた、ストレージエリアネットワーク (SAN) ファブリック 680 に接続されてもよい。SAN ファブリック 680 は、一般に、複数の記憶デバイス間の通信を容易にすることができる、任意のタイプ又は形態のコンピュータネットワーク又はアーキテクチャを表す。SAN ファブリック 680 は、サーバ 640 及び 645 と、複数の記憶デバイス 690 (1) ~ (N) 及び／又はインテリジェント記憶アレイ 695 との間の通信を容易にしてもよい。SAN ファブリック 680 はまた、記憶デバイス 690 (1) ~ (N) 及びインテリジェント記憶アレイ 695 が、クライアントシステム 610、620、及び 630 にローカルで取り付けられたデバイスとして現れるような方式で、ネットワーク 650 並びにサーバ 640 及び 645 を介して、クライアントシステム 610、620、及び 630 と、記憶デバイス 690 (1) ~ (N) 及び／又はインテリジェント記憶アレイ 695 との間の通信を容易にしてもよい。記憶デバイス 660 (1) ~ (N) 及び記憶デバイス 670 (1) ~ (N) と同様に、記憶デバイス 690 (1) ~ (N) 及びインテリジェント記憶アレイ 695 は、一般に、データ及び／又は他のコンピュータ可読命令を格納することができる任意のタイプ又は形態の記憶デバイス又は媒体を表す。

#### 【0069】

特定の実施形態では、また図 5 の例示的なコンピューティングシステム 510 を参照すると、図 5 の通信インターフェース 522 などの通信インターフェースは、それぞれのクライアントシステム 610、620、及び 630 とネットワーク 650 との間の接続を提供するために使用されてもよい。クライアントシステム 610、620、及び 630 は、例えば、ウェブブラウザ又は他のクライアントソフトウェアを使用して、サーバ 640 又は 645 上の情報にアクセスすることができてよい。かかるソフトウェアは、クライアントシステム 610、620、及び 630 が、サーバ 640、サーバ 645、記憶デバイス 660 (1) ~ (N)、記憶デバイス 670 (1) ~ (N)、記憶デバイス 690 (1)

10

20

30

40

50

）～（N）、又はインテリジェント記憶アレイ 6 9 5 によってホストされるデータにアクセスすることを可能にしてもよい。図 6 は、データを交換するために（インターネットなどの）ネットワークを使用することを示しているが、本明細書に記載及び／又は図示される実施形態は、インターネット又は任意の特定のネットワークベースの環境に限定されない。

#### 【0070】

少なくとも 1 つの実施形態では、本明細書で開示する例示的な実施形態のうち 1 つ又は 2 つ以上の全て又は一部は、コンピュータプログラムとしてコード化され、サーバ 6 4 0、サーバ 6 4 5、記憶デバイス 6 6 0（1）～（N）、記憶デバイス 6 7 0（1）～（N）、記憶デバイス 6 9 0（1）～（N）、インテリジェント記憶アレイ 6 9 5、又はこれらの任意の組み合わせ上にロードされ、これらによって実行されてもよい。本明細書で開示する例示的な実施形態のうち 1 つ又は 2 つ以上の全て又は一部はまた、コンピュータプログラムとしてコード化され、サーバ 6 4 0 内に格納され、サーバ 6 4 5 によって作動し、ネットワーク 6 5 0 上でクライアントシステム 6 1 0、6 2 0、及び 6 3 0 に分散されてもよい。

#### 【0071】

上記に詳述したように、コンピューティングシステム 5 1 0 及び／又はネットワークアーキテクチャ 6 0 0 の 1 つ若しくは 2 つ以上の構成要素は、単独で又は他の要素と組み合わせてのいずれかで、シングルサインオンアプリケーション用の暗号化鍵を管理するための例示的な方法の 1 つ又は 2 つ以上のステップを実施してもよく、かつ／又は実施するための手段となってもよい。

#### 【0072】

前述の開示は、特定のブロック図、フローチャート、及び実施例を使用して様々な実施形態を記載しているが、本明細書に記載及び／又は図示されるそれぞれのブロック図の構成要素、フローチャートのステップ、動作、及び／又は構成要素は、個別にかつ／又は集合的に、広範なハードウェア、ソフトウェア、又はファームウェア（若しくはそれらの任意の組み合わせ）の構成を使用して実装されてもよい。それに加えて、同じ機能性を達成するように他の多くのアーキテクチャを実装することができるので、他の構成要素内に包含される構成要素のあらゆる開示は、本質的に例示と見なされるべきである。

#### 【0073】

一部の実施例では、図 1 の例示的なシステム 1 0 0 の全て又は一部は、クラウドコンピューティング環境又はネットワークベースの環境の一部を表してもよい。クラウドコンピューティング環境は、インターネットを介して、様々なサービス及びアプリケーションを提供してもよい。これらのクラウドベースのサービス（例えば、サービスとしてのソフトウェア、サービスとしてのプラットフォーム、サービスとしての基盤など）は、ウェブブラウザ又は他のリモートインターフェースを通してアクセス可能であってもよい。本明細書に記載する様々な機能は、リモートデスクトップ環境又は他の任意のクラウドベースのコンピューティング環境を通して提供されてもよい。

#### 【0074】

様々な実施形態では、図 1 の例示的なシステム 1 0 0 の全て又は一部は、クラウドベースのコンピューティング環境内におけるマルチテナンシーを容易にしてもよい。換言すれば、本明細書に記載するソフトウェアモジュールは、本明細書に記載する機能の 1 つ以上に対するマルチテナンシーを容易にするように、コンピューティングシステム（例えば、サーバ）を構成してもよい。例えば、本明細書に記載するソフトウェアモジュールの 1 つ以上は、2 つ以上のクライアント（例えば、顧客）がサーバ上で作動しているアプリケーションを共有するのを可能にするように、サーバをプログラムしてもよい。このようにプログラムされたサーバは、複数の顧客（即ち、テナント）の間で、アプリケーション、オペレーティングシステム、処理システム、及び／又は記憶システムを共有してもよい。本明細書に記載するモジュールの 1 つ以上はまた、ある顧客が別の顧客のデータ及び／又は設定情報にアクセスできないように、顧客ごとにマルチテナントアプリケーションのデー

タ及び／又は設定情報を分割してもよい。

#### 【0075】

様々な実施形態によれば、図1の例示的なシステム100の全て又は一部は仮想環境内で実装されてもよい。例えば、本明細書に記載するモジュール及び／又はデータは、仮想機械内で常駐及び／又は実行してもよい。本明細書で使用するとき、「仮想機械」という用語は、一般に、仮想機械マネージャ（例えば、ハイパーバイザ）によってコンピューティングハードウェアから抽出される、任意のオペレーティングシステム環境を指す。それに加えて、又は別の方法として、本明細書に記載するモジュール及び／又はデータは、仮想化層内で常駐及び／又は実行してもよい。本明細書で使用するとき、「仮想化層」という用語は、一般に、オペレーティングシステム環境にオーバーレイする、並びに／あるいはそこから抽出される、任意のデータ層及び／又はアプリケーション層を指す。仮想化層は、基礎となる基本オペレーティングシステムの一部であるかのように仮想化層を提示する、ソフトウェア仮想化ソリューション（例えば、ファイルシステムフィルタ）によって管理されてもよい。例えば、ソフトウェア仮想化ソリューションは、最初に基本ファイルシステム及び／又はレジストリ内の場所に方向付けられる呼び出しを、仮想化層内の場所にリダイレクトしてもよい。

10

#### 【0076】

一部の実施例では、図1の例示的なシステム100の全て又は一部は、モバイルコンピューティング環境の一部を表してもよい。モバイルコンピューティング環境は、携帯電話、タブレットコンピュータ、電子ブックリーダー、携帯情報端末、ウェアラブルコンピューティングデバイス（例えば、ヘッドマウントディスプレイを備えたコンピューティングデバイス、スマートウォッチなど）などを含む、広範なモバイルコンピューティングデバイスによって実装されてもよい。一部の実施例において、モバイルコンピューティング環境は、例えば、バッテリー電力への依存、任意の所与の時間での1つのみのフォアグラウンドアプリケーションの提示、リモート管理特性、タッチスクリーン特性、位置及び移動データ（例えば、グローバルポジショニングシステム、ジャイロ스코プ、加速度計などによって提供される）、システムレベルの構成への修正を制限する、及び／又は第3者のソフトウェアが他のアプリケーションの挙動を検査する能力を限定する制限されたプラットフォーム、アプリケーションのインストールを（例えば、認可されたアプリケーションストアからのみ生じるように）制限する制御などを含む、1つ以上の個別の特性を有することができる。本明細書で説明される様々な機能は、モバイルコンピューティング環境に対して提供され得る、及び／又はモバイルコンピューティング環境と相互作用し得る。

20

30

#### 【0077】

それに加えて、図1の例示的なシステム100の全て又は一部は、情報管理のための1つ以上のシステムの部分を表してもよく、それと相互作用してもよく、それによって生成されるデータを消費してもよく、かつ／又はそれによって消費されるデータを生成してもよい。本明細書で使用するとき、「情報管理」という用語は、データの保護、組織化、及び／又は記憶を指してもよい。情報管理のためのシステムの例としては、非限定的に、記憶システム、バックアップシステム、アーカイブシステム、複製システム、高可用性システム、データ検索システム、仮想化システムなどを挙げることができる。

40

#### 【0078】

一部の実施形態では、図1の例示的なシステム100の全て又は一部は、情報セキュリティのための1つ以上のシステムの部分を表してもよく、それによって保護されるデータを生成してもよく、かつ／又はそれと通信してもよい。本明細書で使用するとき、「情報セキュリティ」という用語は、保護されたデータに対するアクセスの制御を指してもよい。情報セキュリティのためのシステムの例としては、非限定的に、管理されたセキュリティサービスを提供するシステム、データ損失防止システム、本人認証システム、アクセス制御システム、暗号化システム、ポリシー遵守システム、侵入検出及び防止システム、電子証拠開示システムなどを挙げることができる。

#### 【0079】

50

一部の実施例によれば、図1の例示的なシステム100の全て又は一部は、エンドポイントセキュリティのための1つ以上のシステムの部分を表してもよく、それと通信してもよく、かつ／又はそれから保護を受けてもよい。本明細書で使用するとき、「エンドポイントセキュリティ」という用語は、不正及び／若しくは違法な使用、アクセス、並びに／又は制御からのエンドポイントシステムの保護を指してもよい。エンドポイント保護のためのシステムの例としては、非限定的に、アンチマルウェアシステム、ユーザ認証システム、暗号化システム、プライバシーシステム、スパムフィルタリングサービスなどを挙げることができる。

#### 【0080】

本明細書に記載及び／又は図示されるプロセスパラメータ及びステップの順序は、単なる例として与えられるものであり、所望に応じて変更することができる。例えば、本明細書に図示及び／又は記載されるステップは特定の順序で図示又は考察されることがあるが、これらのステップは、必ずしも図示又は考察される順序で実施される必要はない。本明細書に記載及び／又は図示される様々な例示的な方法はまた、本明細書に記載若しくは図示されるステップの1つ以上を省略するか、又は開示されるものに加えて追加のステップを含んでもよい。

#### 【0081】

様々な実施形態を、完全に機能的なコンピューティングシステムの文脈で本明細書に記載及び／又は図示してきたが、これらの例示的な実施形態の1つ以上は、実際に配布を実施するのに使用されるコンピュータ可読媒体の特定のタイプにかかわらず、様々な形態のプログラム製品として配布されてもよい。本明細書に開示される実施形態はまた、特定のタスクを実施するソフトウェアモジュールを使用して実装されてもよい。これらのソフトウェアモジュールは、コンピュータ可読記憶媒体又はコンピューティングシステムに格納されてもよい、スクリプト、バッチ、若しくは他の実行可能ファイルを含んでもよい。一部の実施形態では、これらのソフトウェアモジュールは、本明細書に開示される例示的な実施形態の1つ以上を実施するようにコンピューティングシステムを構成してもよい。

#### 【0082】

それに加えて、本明細書に記載するモジュールの1つ以上は、データ、物理的デバイス、及び／又は物理的デバイスの表現を、1つの形態から別の形態へと変換してもよい。例えば、本明細書に記載のモジュールのうち1つ又は2つ以上は、変換されるべき認証要素を受信し、認証要素を変換し、変換結果を出力して1つ又は2つ以上の暗号鍵を生成し、変換結果を使用して暗号鍵を管理し、変換結果を格納して1つ又は2つ以上のクラウドサービスによって維持される暗号化されたデータへのシングルサインオンアクセスを容易にしてもよい。それに加えて、又は別の方法として、本明細書に列挙されるモジュールの1つ以上は、コンピューティングデバイス上で実行し、コンピューティングデバイスにデータを格納し、並びに／あるいは別の方法でコンピューティングデバイスと相互作用することによって、プロセッサ、揮発性メモリ、不揮発性メモリ、及び／又は物理的コンピューティングデバイスの他の任意の部分を、1つの形態から別の形態へと変換してもよい。

#### 【0083】

上述の記載は、本明細書に開示される例示的な実施形態の様々な態様を他の当業者が最良に利用するのを可能にするために提供されてきた。この例示的な記載は、網羅的であることを意図するものではなく、又は開示される任意の正確な形態に限定することを意図するものではない。本開示の趣旨及び範囲から逸脱することなく、多くの修正及び変形が可能である。本明細書に開示される実施形態は、あらゆる点で例示的であり、限定的ではないものと見なされるべきである。本開示の範囲を決定する際に、添付の特許請求の範囲及びそれらの等価物を参照するべきである。

#### 【0084】

別途記載のない限り、「～に接続される」及び「～に連結される」という用語（並びにそれらの派生語）は、本明細書及び特許請求の範囲で使用するとき、直接的接続及び間接的接続（即ち、他の要素若しくは構成要素を介する）の両方を許容するものとして解釈さ

れるものである。それに加えて、「a」又は「a n」という用語は、本明細書及び特許請求の範囲で使用する時、「～のうち少なくとも1つ」を意味するものとして解釈されるものである。最後に、簡潔にするため、「含む」及び「有する」という用語（並びにそれらの派生語）は、本明細書及び特許請求の範囲で使用する時、「備える」という単語と互換性があり、同じ意味を有する。

【図 1】

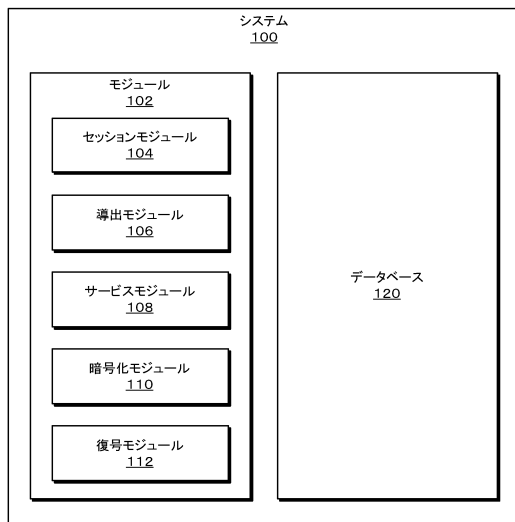


FIG. 1

【図 2】

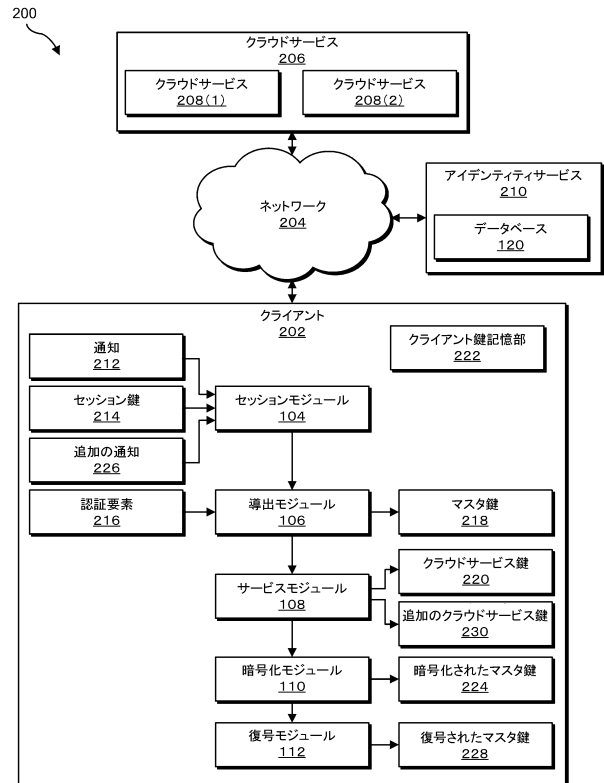


FIG. 2

【図 3】

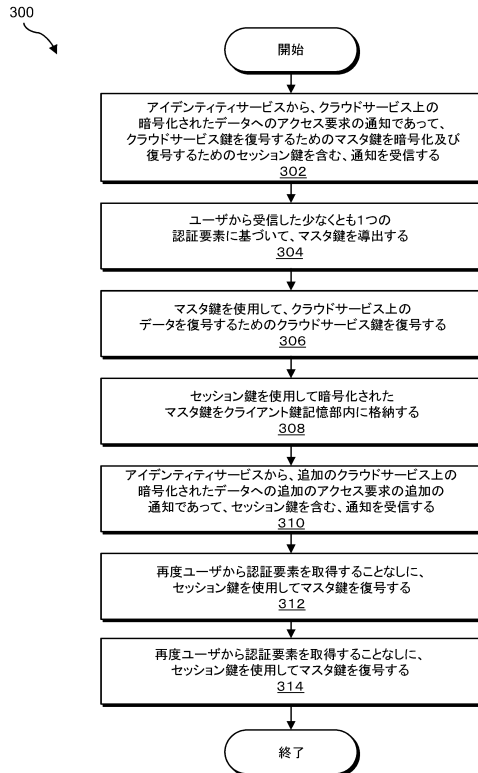


FIG. 3

【図 4】

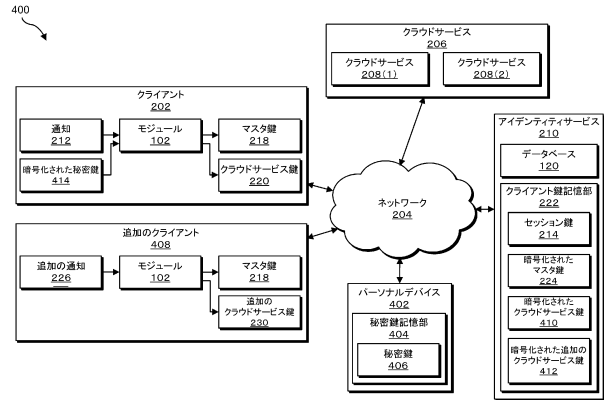


FIG. 4

【図 5】

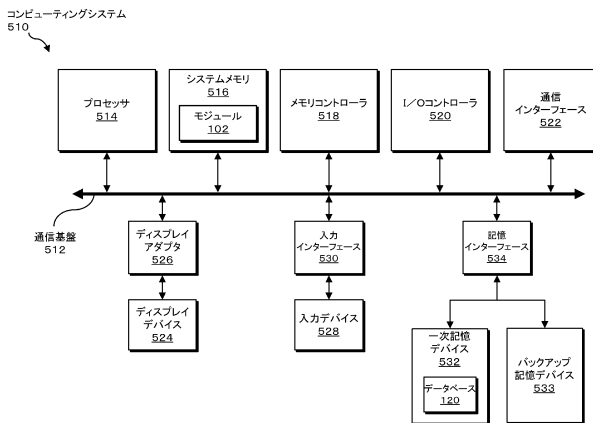


FIG. 5

【図 6】

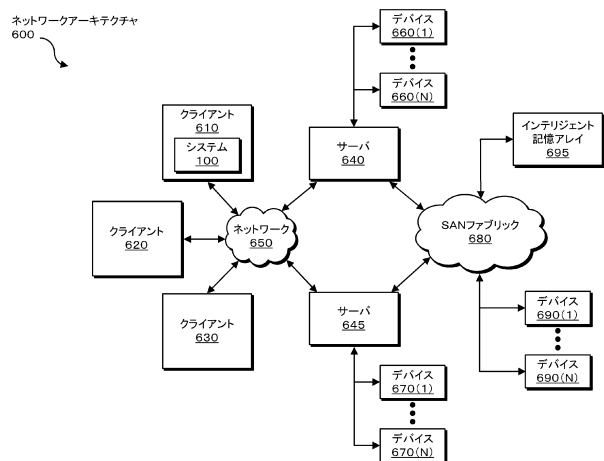


FIG. 6

---

フロントページの続き

(72)発明者 ニュースタッド・キース  
アメリカ合衆国 マサチューセッツ州 02465 ウェストニュートン マートルストリート  
18

審査官 行田 悦資

(56)参考文献 特開2005-209118 (JP, A)  
特表2008-506139 (JP, A)  
特開2015-127859 (JP, A)  
特開2008-124649 (JP, A)  
特開2014-063069 (JP, A)  
米国特許出願公開第2015/0089579 (US, A1)

(58)調査した分野(Int.Cl., DB名)  
H04L 9/08  
G06F 21/41  
G06F 21/60