(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6517359号
(P6517359)
(45)発行日　令和1年5月22日(2019.5.22)　(24)登録日　平成31年4月26日(2019.4.26)

(51)Int.Cl.　　F I
G06F 21/45 (2013.01)　　G06F 21/45
H04L 9/08 (2006.01)　　H04L 9/00 6O1E

請求項の数 24　(全 28 頁)

(21)出願番号　特願2017-544834(P2017-544834)
(86)(22)出願日　平成27年11月4日(2015.11.4)
(65)公表番号　特表2018-503199(P2018-503199A)
(43)公表日　平成30年2月1日(2018.2.1)
(86)国際出願番号　PCT/US2015/059060
(87)国際公開番号　WO2016/077121
(87)国際公開日　平成28年5月19日(2016.5.19)
審査請求日　平成29年6月16日(2017.6.16)
(31)優先権主張番号　62/080,125
(32)優先日　平成26年11月14日(2014.11.14)
(33)優先権主張国　米国(US)
(31)優先権主張番号　14/928,443
(32)優先日　平成27年10月30日(2015.10.30)
(33)優先権主張国　米国(US)

(73)特許権者　505418238
マカフィー，　エルエルシー
アメリカ合衆国、９５０５４　カリフォルニア州、サンタ　クララ、ミッション　カレッジ　ブールバード　２８２１
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　レネ、マチュー
カナダ国、エイチ２ケイ　３ピー４　ケベック州、モントリオール　フュリャム　２４８６
(72)発明者　プルークス、フランシス
カナダ国、エイチ４ジー　１ゼッド２　ケベック州、ベルダン　ラザル　ブールバール　３４１３

最終頁に続く

(54)【発明の名称】アカウント復元プロトコル

(57)【特許請求の範囲】
【請求項１】
コンピュータに、
ユーザに関連するアカウントの復元のための要求をユーザデバイスから受信することと、
前記ユーザに関連する前記ユーザデバイスへＣＡＰＴＣＨＡチャレンジを送信することと、
前記ＣＡＰＴＣＨＡチャレンジへの回答、および、暗号化鍵によってラップされた確認コードを受信することであって、前記暗号化鍵は前記ユーザによって提供される仮マスターパスワードから導出される、受信することと、
前記ユーザによって指定されている、前記ユーザに関連する１つまたは複数の信頼済エンティティへ復元のための前記要求の通知を送信することと、
前記１つまたは複数の信頼済エンティティから前記要求の確認を受信することであって、前記確認は、前記１つまたは複数の信頼済エンティティに関連する復元トークン、および、前記確認コードを含む、受信することと
を少なくとも実行させるためのコンピュータコードであって、
新しいマスターパスワードは、前記復元トークンを使用して生成され、
前記確認コードは、前記復元トークンの検証のために使用される、
コンピュータコード。
【請求項２】

前記コンピュータに、
前記１つまたは複数の信頼済エンティティから、所定の数の前記復元トークンを受信したことを示すコンセンサス状態が達成されたと判定することと、
前記１つまたは複数の信頼済エンティティの各々に関連する前記復元トークンを前記ユーザデバイスへ送信することと、
を更に実行させるための、請求項１に記載のコンピュータコード。
【請求項３】
前記コンピュータに、前記コンセンサス状態の通知を前記ユーザデバイスへ送信することを更に実行させるための、請求項２に記載のコンピュータコード。
【請求項４】
前記コンピュータに、前記コンセンサス状態が達成されたという判定に応答して前記アカウントのための前記新しいマスターパスワードを設定することを更に実行させるための、請求項２に記載のコンピュータコード。
【請求項５】
受信された前記復元トークンは、前記アカウントの復元のための前記要求を行う場合に前記ユーザデバイスが一時的に生成する一時的秘密鍵を使用して前記ユーザデバイスによって復号される、請求項２から４のいずれか一項に記載のコンピュータコード。
【請求項６】
前記新しいマスターパスワードは、復号化された前記復元トークンを組み合わせることに基づいて設定される、請求項５に記載のコンピュータコード。
【請求項７】
前記新しいマスターパスワードは、前記ユーザデバイスによって生成される、請求項４に記載のコンピュータコード。
【請求項８】
前記コンピュータに、前記１つまたは複数の信頼済エンティティの指定を前記ユーザから受信することを更に実行させるための、請求項１から７のいずれか一項に記載のコンピュータコード。
【請求項９】
少なくとも１つのプロセッサおよび少なくとも１つのメモリ要素を備えるシステムであって、
ユーザに関連するアカウントの復元のための要求をユーザデバイスから受信する段階と、
前記ユーザに関連する前記ユーザデバイスへＣＡＰＴＣＨＡチャレンジを送信する段階と、
前記ＣＡＰＴＣＨＡチャレンジへの回答、および、暗号化鍵によってラップされた確認コードを受信する段階であって、前記暗号化鍵は前記ユーザによって提供される仮マスターパスワードから導出される、受信する段階と、
前記ユーザによって指定されている、前記ユーザに関連する１つまたは複数の信頼済エンティティへ復元のための前記要求の通知を送信する段階と、
前記１つまたは複数の信頼済エンティティから前記要求の確認を受信する段階であって、前記確認は、前記１つまたは複数の信頼済エンティティに関連する復元トークン、および、前記確認コードを含む、段階と、
を行い、
新しいマスターパスワードは、前記復元トークンを使用して生成され、
前記確認コードは、前記復元トークンの検証のために使用される、
システム。
【請求項１０】
前記システムは更に、
前記１つまたは複数の信頼済エンティティから所定の数の前記復元トークンを受信したことを示すコンセンサス状態が達成されたと判定する段階と、

前記１つまたは複数の信頼済エンティティの各々に関連する前記復元トークンを前記ユーザデバイスへ送信する段階と、
を更に行う、請求項９に記載のシステム。
【請求項１１】
前記システムは更に、
前記コンセンサス状態の通知を前記ユーザデバイスへ送信する、請求項１０に記載のシステム。
【請求項１２】
前記システムは更に、前記コンセンサス状態が達成されたという判定に応答して、前記アカウントのための新しいマスターパスワードを生成する、請求項１１に記載のシステム。
【請求項１３】
前記新しいマスターパスワードは、受信された前記復元トークンを使用して設定される、請求項１２に記載のシステム。
【請求項１４】
受信された前記復元トークンは、前記アカウントの復元のための前記要求を行う場合に前記ユーザデバイスが一時的に生成する一時的秘密鍵を使用して復号される、請求項１３に記載のシステム。
【請求項１５】
前記新しいマスターパスワードは、前記ユーザデバイスによって生成される、請求項１２に記載のシステム。
【請求項１６】
前記システムは更に、前記１つまたは複数の信頼済エンティティの指定を前記ユーザから受信する、請求項９から１５のいずれか一項に記載のシステム。
【請求項１７】
ユーザに関連するアカウントの復元のための要求をユーザデバイスから受信する段階と、
前記ユーザに関連する前記ユーザデバイスへＣＡＰＴＣＨＡチャレンジを送信する段階と、
前記ＣＡＰＴＣＨＡチャレンジへの回答、および、暗号化鍵によってラップされた確認コードを受信する段階であって、前記暗号化鍵は前記ユーザによって提供される仮マスターパスワードから導出される、受信する段階と、
前記ユーザによって指定されている、前記ユーザに関連する１つまたは複数の信頼済エンティティへ復元のための前記要求の通知を送信する段階と、
前記１つまたは複数の信頼済エンティティから前記要求の確認を受信する段階であって、前記確認は、前記１つまたは複数の信頼済エンティティに関連する復元トークン、および、暗号化された前記確認コードを含む、段階と、
を少なくとも含む、プロセッサにより実装される方法であって、
新しいマスターパスワードは、前記復元トークンを使用して生成され、
前記確認コードは、前記復元トークンの検証のために使用される、
方法。
【請求項１８】
前記プロセッサが、前記１つまたは複数の信頼済エンティティから、所定の数の前記復元トークンを受信したことを示すコンセンサス状態が達成されたと判定する段階と、
前記プロセッサが、前記１つまたは複数の信頼済エンティティの各々に関連する前記復元トークンを前記ユーザデバイスへ送信する段階と、
を更に含む、請求項１７に記載の方法。
【請求項１９】
前記プロセッサが、前記コンセンサス状態の通知を前記ユーザデバイスへ送信する段階を更に含む、請求項１８に記載の方法。

【請求項２０】
前記プロセッサが、前記コンセンサス状態が達成されたという判定に応答して、前記アカウントのための前記新しいマスターパスワードを設定する段階を更に含む、請求項１８に記載の方法。
【請求項２１】
受信された前記復元トークンは、前記アカウントの復元のための前記要求を行う場合に前記ユーザデバイスが一時的に生成する一時的秘密鍵を使用して前記ユーザデバイスによって復号される、請求項１８に記載の方法。
【請求項２２】
ユーザに関連するアカウントの復元のための要求をユーザデバイスから受信する手段と、
前記ユーザに関連する前記ユーザデバイスへＣＡＰＴＣＨＡチャレンジを送信する手段と、
前記ＣＡＰＴＣＨＡチャレンジへの回答、および、暗号化鍵によってラップされた確認コードを受信する手段であって、前記暗号化鍵は前記ユーザによって提供される仮マスターパスワードから導出される、受信する手段と、
復元のための前記要求の通知を、前記ユーザによって指定されている、前記ユーザに関連する１つまたは複数の信頼済エンティティへ送信する手段と、
前記１つまたは複数の信頼済エンティティから前記要求の確認を受信する手段であって、前記確認は、前記１つまたは複数の信頼済エンティティに関連する復元トークン、および、前記確認コードを含む、手段と、
を含む、アカウント復元のための装置であって、
新しいマスターパスワードは、前記復元トークンを使用して生成され、
前記確認コードは、前記復元トークンの検証のために使用される、
装置。
【請求項２３】
所定の数の前記復元トークンを前記１つまたは複数の信頼済エンティティから受信したことを示すコンセンサス状態が達成されたと判定する手段と、
前記１つまたは複数の信頼済エンティティの各々に関連する前記復元トークンを前記ユーザデバイスへ送信する手段と、
を更に含む、請求項２２に記載の装置。
【請求項２４】
前記コンセンサス状態が達成されたという判定に応答して、前記アカウントのための新しいマスターパスワードを設定する段階を更に含む、請求項２３に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
［関連出願の相互参照］
本出願は、参照によって全体が本明細書に組み込まれる、２０１４年１１月１４日に申請された、「アカウント復元プロトコル」と題する米国特許出願第６２／０８０，１２５号、および、２０１５年１０月３０日に申請された、「アカウント復元プロトコル」と題する米国特許出願第１４／９２８，４４３号の利益および優先権を主張する。
【０００２】
本出願は、コンピューティングの分野に関し、より具体的には、ユーザアカウント復元のためのシステム、方法、およびプロトコルに関する。
【背景技術】
【０００３】
ユーザが利用できるサービスおよびアプリケーションの普及に伴い、多くの場合、特定のユーザが、そのユーザに関連する、数多くのサービスおよび／またはアプリケーションのアカウントのためのパスワードなどのログイン認証情報を覚えておくことが必要となっ

ている。ユーザがアカウントに関連するパスワードを失念または紛失した場合、ユーザは通常、アカウントへのアクセスを取り戻すべく、パスワード復元手順を開始する必要がある。しかしながら、多くの既存のパスワード復元手順は、セキュリティの脆弱性を伴う。

【図面の簡単な説明】

【０００４】

添付の図面の図には、例として、非限定的な実施形態が示されている。ここでは、類似の参照符号は同様の要素を示す。

【０００５】

【図１】一実施形態による、クライアント側およびサーバ側のコンポーネントを含む、ユーザアカウント復元のための高レベルのアーキテクチャを示す。

【０００６】

【図２】一実施形態によるユーザアカウント復元のための通信システムを示す。

【０００７】

【図３Ａ】一実施形態による、アカウント復元プロトコルのセットアップおよび管理のためのプロセスフローの例を示す。

【図３Ｂ】一実施形態による、アカウント復元プロトコルのセットアップおよび管理のためのプロセスフローの例を示す。

【０００８】

【図４Ａ】一実施形態によるアカウント復元プロトコルのためのアカウント復元要求確立プロセスフローの例を示す。

【図４Ｂ】一実施形態によるアカウント復元プロトコルのためのアカウント復元要求確立プロセスフローの例を示す。

【０００９】

【図５】一実施形態によるアカウント復元プロトコルのためのアカウント復元要求招待プロセスフローの例を示す。

【００１０】

【図６Ａ】一実施形態によるアカウント復元プロトコルのためのアカウント復元要求完了プロセスフローの例を示す。

【図６Ｂ】一実施形態によるアカウント復元プロトコルのためのアカウント復元要求完了プロセスフローの例を示す。

【００１１】

【図７】クライアントデバイスの実施形態の簡略化されたブロック図を示す。

【００１２】

【図８】認証サーバの実施形態の簡略化されたブロック図を示す。

【発明を実施するための形態】

【００１３】

１つまたは複数の例示的な実施形態は、アカウント復元プロトコル（ＡＲＰ）のためのシステムおよび方法に関する。これらは、マスターパスワードを再設定するための機構であり、パスワードマネージャであるユーザが関連する「マスターパスワード」を失念した場合に、クラウドサービスなどのネットワークサービスに関連する、自身のアカウントへのアクセス、および、暗号化された保存データを復元することを可能にする。１つまたは複数の実施形態において、システム運用者は、サービスに関連するマスターパスワードの情報をそれ自体で保持していない。特定の実施形態において、アカウント復元プロトコルは、「マスターパスワード」復元ではなく、「アカウント／アクセス」復元を促進する。なぜなら、サービスプロバイダの観点からさえもユーザのプライバシーおよびデータ機密性を保護するべく、一部のパスワードマネージャは、いかなるときもマスターパスワードの保存されたコピーを保持していないからである。

【００１４】

１つまたは複数の実施形態において、パスワードマネージャは、本明細書に記載されて

いるようなユーザ認証を統合するための多面的アーキテクチャを含む認証プラットフォームの一部である。様々な実施形態において、パスワードマネージャは、クラウド内サービスなどのネットワークサービスへの中央集中型認証アクセスを提供する。１つまたは複数の実施形態において、「リライングパーティ（Ｒｅｌｙｉｎｇ　Ｐａｒｔｙ）（ＲＰ）」と呼ばれる、認証サービスに登録しているサービスまたはエンティティは、ＲＰがユーザにサービスを提供する前に、認証サービスを使用して、ユーザに要求される認証因子をセットアップする。１つまたは複数の実施形態において、パスワードマネージャアプリケーションは、登録しているユーザに対してダッシュボードを提示し、ユーザが使用するクラウドサービス全てをダッシュボード内に表示する。それにより、ユーザが利用するサービスの認証要件を入力すること、要求された認証因子を必要なときに提供すること、冗長な別のログインを試行することなく中央集中型方式でこれらのサービスにアクセスすることが可能となる。パスワードマネージャはユーザに対し、アカウント所持者だけに知られるマスターパスワードをセットアップするように要求する。マスターパスワードは、他のパスワードと同様に、ユーザ認証に利用され、アカウントへのログイン、および、ユーザのサービスへのアクセスの獲得を容易にするが、他の重要な役割も有する。それは、ユーザデータの暗号化に使用される鍵、および、復元プロセスにおいて役立つ他の鍵を生成することである。

【００１５】

図１は、一実施形態による、クライアント側およびサーバ側のコンポーネントを含む、ユーザアカウント復元のための高レベルのアーキテクチャ１００を示す。図１に示されている特定の実施形態において、アーキテクチャ１００は、認証コンポーネント１０２および登録／管理コンポーネント１０４を含む。本明細書において後で更に記載されているように、認証コンポーネント１０２は、クライアントデバイスからの認証要求を処理するように構成されている１つまたは複数の認証モジュールを含む。示されている実施形態において、認証コンポーネント１０２の認証モジュールは、フロー・アンド・アクションハンドラモジュール、管理構成用アプリケーションプログラミングインタフェース（ＡＰＩ）、構成保存部、Ｒｅｐｒｅｓｅｎｔａｔｉｏｎａｌ　Ｓｔａｔｅ　Ｔｒａｎｓｆｅｒ（ＲＥＳＴ）サーバ、セッション保存部、および、ＲＥＳＴ　ＡＰＩを含む。特定の実施形態において、認証モジュールは、ＯＡｕｔｈオープン規格にしたがって構成される。登録／管理コンポーネント１０４は、コンテキストデータモジュール、リライングパーティ管理ツール、ユーザ／アプリケーションポリシー管理モジュール、および、プライベートＲＥＳＴ　ＡＰＩを含む。

【００１６】

認証コンポーネント１０２および登録／管理コンポーネント１０４は各々、クラウドサービス１０６、サーバ１０８、ＩＤ認証サービス１１０と更に通信する。クラウドサービス１０６は更に、データ抽象化層（ＤＡＬ）、コンテキストモジュール、ユーザプロファイルモジュール、リスク分析エンジン、および、ＲＥＳＴ　ＡＰＩを含む。サーバ１０８は、ハードウェア登録／検証モジュール、証明モジュール、および、ＲＥＳＴ　ＡＰＩを含む。ＩＤ認証サービス１１０は、アーキテクチャ１００内の他のコンポーネントとの通信を容易にするように構成されているＲＥＳＴ　ＡＰＩを含む。クラウドサービス１０６は更に、１つまたは複数のデータベース１１２と通信する。示されている特定の実施形態において、データベース１１２は、セッションデータベース、バイオメトリックデータベース、および、認証データベースを含む。

【００１７】

アーキテクチャ１００は更に、１つまたは複数のリライングパーティエンティティに関連する１つまたは複数のサーバ上にある、リライングパーティウェブサイト１１４、および、リライングパーティアプリケーション１１６を含む。リライングパーティウェブサイト１１４およびリライングパーティアプリケーション１１６の各々は、認証コンポーネント１０２と通信する。リライングパーティウェブサイトは、ウェブソフトウェア開発キット（ＳＤＫ）を含み、更に認証ウェブインタフェース１１８と通信する。認証ウェブイン

タフェース１１８は更に、登録／管理コンポーネント１０４と通信する。リライングパーティアプリケーション１１６は更に、認証クライアントアプリケーション１２０と通信する。認証クライアントアプリケーション１２０は更に、登録／管理コンポーネント１０４と通信する。アーキテクチャ１００は更に、登録／管理コンポーネント１０４と通信する認証ＯＳログインコンポーネント１２２を含む。認証クライアントアプリケーション１２０および認証ＯＳログインコンポーネント１２２の各々は、ユーザからバイオメトリックデータを取得することを容易にするローカルバイオメトリックライブラリを含む。

【００１８】

認証コンポーネント１０２は、認証機能のための認証要求を処理すること、ならびに、認証要求を処理するための、ユーザプロファイル、ポリシー、および、バイオメトリックコンポーネントなどのコンポーネントとインタラクトする、認証固有のフロー・アンド・アクションハンドラを生成することを行うように構成されている。登録手順中、登録／管理コンポーネント１０４は、プライベートＲＥＳＴ　ＡＰＩを介して、様々なコンポーネントとインタフェースで接続し、特定のユーザのためのユーザプロファイルを生成し、特定のＲＰクライアントを識別するリライングパーティ（ＲＰ）クライアント識別子（ＩＤ）にユーザプロファイルを関連付ける。１つまたは複数の実施形態において、ユーザプロファイルおよびＲＰクライアントポリシーが生成され、１つまたは複数のデータベース（ＤＢ）１１２内に保存される。特定の実施形態において、ユーザプロファイル、ＲＰアプリケーションポリシー、および、コンテキストデータのＤＢ構造は、認証要求のために認証モジュール１０２と共有される。

【００１９】

例示的な一実施形態において、１つまたは複数の認証サーバ内のポリシーエンジンは、１つまたは複数のＲＰエンティティに対するユーザの認証のためのポリシーを管理する。特定の実施形態において、ＲＰエンティティが提供するリソースに対する、ユーザによるアクセスを制御するべく、ユーザに関連するポリシーは、登録するＲＰエンティティと、ユーザ自身のセキュリティ設定との両方によって構成できる。特定の実施形態において、認証因子の使用についてのセキュリティレベルは最低限に設定され、ユーザおよび／またはＲＰエンティティは、認証の因子のレベルおよび数を増加させ得るが、減少させ得ない。

【００２０】

様々な実施形態にしたがって、アカウント復元プロトコル（ＡＲＰ）は、復元機構として、様々な実施形態においてユーザに提供される。１つまたは複数の実施形態において、ユーザには、復元機構をセットアップするための選択肢が予め提供され得る。それにより、関連するマスターパスワードをユーザが失念した場合、ユーザは、ユーザのサービスに対するアクセスの喪失から復元し、回復できる。

【００２１】

図２は、一実施形態による、ユーザアカウント復元のための通信システム２００を示す。通信システム２００は、ユーザＡに関連する第１クライアントデバイス２０２ａ、ユーザＢに関連する第２クライアントデバイス２０２ｂ、ユーザＣに関連する第３クライアントデバイス２０２ｃ、ユーザＤに関連する第４クライアントデバイス２０２ｄ、ユーザＥに関連する第５クライアントデバイス２０２ｅ、ユーザＦに関連する第６クライアントデバイス２０２ｆを含む。クライアントデバイス２０２ａ－２０２ｆの各々は、１つまたは複数のネットワーク２０４を介して認証サーバ２０６と通信する。ネットワーク２０４は、モバイルアクセスネットワーク、インターネット、または、他のいずれかの好適なネットワークのうち１つまたは複数を含み得て、それにより、クライアントデバイス２０２ａ－２０２ｆが認証サーバ２０６と通信することを可能にする。認証サーバ２０６は更に、インターネット２０８を介して、リライングパーティ（ＲＰ）サーバ２１０と通信する。第１クライアントデバイス２０２ａは、第１パスワードアプリケーション２１２ａを含み、第２クライアントデバイス２０２ｂは、第２パスワードアプリケーション２１２ｂを含み、第３クライアントデバイス２０２ｃは、第３パスワードアプリケーション２１２ｃを

含み、第４クライアントデバイス２０２ｄは、第４パスワードアプリケーション２１２ｄを含み、第５クライアントデバイス２０２ｅは、第５パスワードアプリケーション２１２ｅを含み、第６クライアントデバイス２０２ｆは、第６パスワードアプリケーション２１２ｆを含む。本明細書において後で更に記載されているように、パスワードアプリケーション２１２ａ－２１２ｆの各々は、様々なパスワードのセットアップおよび復元手順を実行するべく、それぞれのクライアントデバイス２０２ａ－２０２ｆのユーザが認証サーバ１０２と通信することを可能にするように構成されている。

【００２２】

認証サーバ２０６は、認証コンポーネント１０２を含む。認証コンポーネントは、パスワードアプリケーションＲＥＳＴ　ＡＰＩ２１４を含む。特定の実施形態において、認証サーバ２０６は、サービスプロバイダの基幹ネットワーク内に配置され得る。パスワードアプリケーションＲＥＳＴ　ＡＰＩ２１４は、クライアントデバイス２０２ａ－２０２ｆのパスワードアプリケーション２１２ａ－２１２ｆのそれぞれとインタフェース接続するように構成されている。これにより、認証コンポーネント１０２が、本明細書に記載されているようなパスワードのセットアップおよび後のパスワード復元操作を実行することを可能にし、クライアントデバイス２０２ａ－２０２ｆのうち１つまたは複数に関連するユーザが、ＲＰサーバ２１０に関連する、リソース、サービス、アプリケーション、および／または、コンテンツ（ＲＰサーバ２１０によって提供されるストリーミング音声、ストリーミングビデオ、ビデオコンテンツ、音声コンテンツ、または、他のいずれかの所望のコンテンツなどの）にアクセスすることを可能にする。

【００２３】

クライアントデバイス２０２ａ－２０２ｆは、ＲＰサーバ２１０によって提供されるリソースにアクセスできる、いずれかの電子デバイスまたはコンピューティングデバイスを含み得る。これらのクライアントデバイス２０２ａ－２０２ｆは、例えば、モバイルフォン、デスクトップＰＣ、ラップトップコンピュータ、タブレットコンピュータ、パーソナルデータアシスタント（ＰＤＡ）、スマートフォン、ポータブルメディアファイルプレイヤー、電子書籍リーダー、ポータブルコンピュータ、ヘッドマウントディスプレイ、インタラクティブキオスク、ネットブック、シングルボードコンピュータ（ＳＢＣ）、組み込みコンピュータシステム、ウェアラブルコンピュータ（例えば、腕時計または眼鏡）、ゲームコンソール、ホームシアターＰＣ（ＨＴＰＣ）、テレビ、ＤＶＤプレイヤー、デジタルケーブルボックス、デジタルビデオレコーダー（ＤＶＲ）、ウェブブラウザを実行可能なコンピュータシステム、または、これらのうちいずれか２つまたはより多くの組み合わせを含み得る。コンピューティングデバイスは、これらに限定されないが、Ａｎｄｒｏｉｄ、Ｂｅｒｋｅｌｅｙ　Ｓｏｆｔｗａｒｅ　Ｄｉｓｔｒｉｂｕｔｉｏｎ（ＢＳＤ）（登録商標）、ｉＰｈｏｎｅ　ＯＳ（ｉＯＳ）（登録商標）、Ｌｉｎｕｘ（登録商標）、ＯＳ　Ｘ（登録商標）、Ｕｎｉｘ－ｌｉｋｅ　Ｒｅａｌ－ｔｉｍｅ　Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ（登録商標）（例えば、ＱＮＸ）、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）、Ｗｉｎｄｏｗ　Ｐｈｏｎｅ（登録商標）、および、ＩＢＭ　ｚ／ＯＳ（登録商標）を含むオペレーティングシステムを使用し得る。

【００２４】

リライングパーティ（ＲＰ）サーバ２１０は、ユーザがリソースにアクセスする前にユーザが識別および認証されることを必要とする、ウェブサイト、ベンダ、ならびに、その他、データ、サービス、および、アプリケーションのプロバイダなどのエンティティに関連するサーバを含み得る。

【００２５】

例示的な実装において、クライアントデバイス２０２ａ－２０２ｆ、認証サーバ２０６、および、ＲＰサーバ２１０は、ネットワーク環境において情報を交換するように操作可能な、ネットワーク機器、サーバ、ルータ、スイッチ、ゲートウェイ、ブリッジ、ロードバランサ、プロセッサ、モジュール、または、他のいずれかの好適なデバイス、コンポーネント、要素、もしくはオブジェクトを包含するように意図されているネットワーク要素

である。ネットワーク要素は、それらの操作を容易にする、いずれかの好適なハードウェア、ソフトウェア、コンポーネント、モジュール、または、オブジェクトを含み得て、更に、ネットワーク環境において、データまたは情報を受信、送信、および／または、さもなければ通信するための好適なインタフェースを含み得る。これは、データまたは情報の効果的な交換を可能にする適切なアルゴリズム、および、通信プロトコルを包含し得る。

【００２６】

通信システム２００に関連する内部構造については、クライアントデバイス２０２ａ－２０２ｆ、認証サーバ２０６、および、ＲＰサーバ２１０の各々は、本明細書に記載されている操作で使用される情報を保存するためのメモリ要素を含み得る。クライアントデバイス２０２ａ－２０２ｆ、認証サーバ２０６、および、ＲＰサーバ２１０の各々は、特定の必要性に基づいて適宜、いずれかの好適なメモリ要素（例えば、ランダムアクセスメモリ（ＲＡＭ）、リードオンリーメモリ（ＲＯＭ）、消去可能プログラマブルＲＯＭ（ＥＰＲＯＭ）、電気的消去可能プログラマブルＲＯＭ（ＥＥＰＲＯＭ）、特定用途向け集積回路（ＡＳＩＣ）など）、ソフトウェア、ハードウェア、ファームウェア、または、他のいずれかの好適なコンポーネント、デバイス、要素、もしくはオブジェクト内に情報を保持し得る。本明細書に記載されているいずれかのメモリアイテムは、「メモリ要素」という広義の用語に包含されると解釈されるべきである。更に、通信システム２００において使用、追跡、送信、または、受信される情報は、いずれかのデータベース、レジスタ、キュー、テーブル、キャッシュ、制御リスト、または、他のストレージ構造内に提供できるであろう。それらは全て、いずれかの好適な間隔で参照できる。そのようなストレージの選択肢のいずれも、本明細書に使用される「メモリ要素」という広義の用語内に含まれ得る。

【００２７】

特定の例示的な実装において、本明細書に記載されている機能は、非揮発性コンピュータ可読媒体を含み得る１つまたは複数の有形媒体内に符号化されている論理（例えば、ＡＳＩＣ内に提供される組み込み論理、デジタル信号プロセッサ（ＤＳＰ）命令、プロセッサによって実行される（場合によっては、オブジェクトコードおよびソースコードを含む）ソフトウェア、または、他の同様の機械など）によって実装され得る。これらのインスタンスのいくつかにおいて、メモリ要素は、本明細書に記載されている操作に使用されるデータを保存できる。これは、本明細書に記載されているアクティビティを遂行するべく実行されるソフトウェア、論理、コンピュータコード、または、プロセッサ命令を保存できるメモリ要素を含む。

【００２８】

例示的な実装において、クライアントデバイス２０２ａ－２０２ｆ、認証サーバ２０６、および、ＲＰサーバ２１０など、通信システム２００のネットワーク要素は、本明細書に記載されている操作を実現または助長するためのソフトウェアモジュールを含み得る。これらのモジュールは、特定の構成および／またはプロビジョニングの必要性に基づき得る、いずれかの適切な手法で好適に組み合わせられ得る。特定の実施形態において、そのような操作は、ハードウェアによって遂行されるか、これらの要素の外部で実装されるか、または、意図された機能を実現する他の何らかのネットワークデバイス内に含まれ得る。更に、モジュールは、ソフトウェア、ハードウェア、ファームウェア、または、それらのいずれかの好適な組み合わせとして実装できる。これらの要素は、本明細書に記載されているような操作を実現するべく他のネットワーク要素と連携できるソフトウェアも含み得る。

【００２９】

加えて、クライアントデバイス２０２ａ－２０２ｆ、認証サーバ２０６、および、ＲＰサーバ２１０の各々は、本明細書に記載されているアクティビティを実行するためのソフトウェアまたはアルゴリズムを実行できるプロセッサを含み得る。プロセッサは、本明細書に詳しく記載されている操作を実現するためのデータに関連する任意の種類の命令を実行できる。一例において、プロセッサは、１つの状態または物から、他の状態または物へ

と、要素または品目（例えば、データ）を変換できるであろう。他の例において、本明細書に記載されているアクティビティは、固定論理またはプログラマブル論理（例えば、プロセッサによって実行されるソフトウェア／コンピュータ命令）によって実装され得る。本明細書において特定されている要素は、デジタル論理、ソフトウェア、コンピュータコード、電子命令、または、それらのいずれかの好適な組み合わせを含む、何らかの種類のプログラマブルプロセッサ、プログラマブルデジタル論理（例えば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、ＥＰＲＯＭ、ＥＥＰＲＯＭ）、または、ＡＳＩＣであり得る。本明細書に記載されている、処理のための潜在的な要素、モジュール、機械のいずれも、「プロセッサ」という広義の用語に包含されると解釈されるべきである。

【００３０】

１つまたは複数の実施形態において、本明細書に記載されているアカウント復元プロトコル（ＡＲＰ）は、アカウント復元が必要となった場合に使用されるパスワードマネージャアプリケーションのユーザによってセットアップされるオプションの機能として実装され得る。１つまたは複数の実施形態において、第１クライアント２０２に関連するユーザＡなどのアカウント所持者は、パスワードマネージャアプリケーションへのアクセスを獲得するべく、マスターパスワードをセットアップする。１つまたは複数の実施形態において、マスターパスワードには、１）ユーザ認証、および、２）ユーザデータの暗号化という、２つの使用法がある。様々な実施形態において、２つの暗号鍵が、マスターパスワードから導出される。第１の暗号鍵は、アカウント所持者の電子メールアドレスを（認証に使用される）ソルトとして使用し、第２の暗号鍵は、ユーザデータの暗号化に使用される固有／ランダムのソルトを使用する。ソルトとは、暗号鍵の生成のための追加的な入力として使用されるデータである。

【００３１】

本明細書に記載されているアカウント復元プロトコル（ＡＲＰ）の１つまたは複数の実施形態の背景にある主要な概念は、アカウント復元鍵（ＡＲＫ）である。これは、ランダムに生成される秘密鍵であり、アカウント復元バンドル（ＡＲＢ）を暗号化するのに使用される。特定の実施形態において、ＡＲＢは、ＪａｖａＳｃｒｉｐｔ Ｏｂｊｅｃｔ Ｎｏｔａｔｉｏｎ（ＪＳＯＮ）（登録商標）形式のドキュメントであり、他の復元属性の中で、復元データの２つの重要な部分である、認証トークンワンタイムパスワード（ＯＴＰ）およびコンテンツ暗号化鍵（ＣＥＫ）を含む。特定の実施形態において、ＯＴＰおよびＣＥＫは両方、アカウントを復元するのに必要であり、アカウント復元要求（ＡＲＲ）を完了するべく要求されるまで、サーバ上で秘密情報として維持される。

【００３２】

１つまたは複数の特定の実施形態において、ＡＲＢは、ＡＲＢ＿ＡＲＫと呼ばれるＡＲＫによって暗号化される。ＡＲＫ秘密情報は、アカウント所持者（例えば、失念しやすいユーザ）だけによって保持または保存される。１つまたは複数の実施形態において、ＡＲＫ秘密情報は、所定の数であるｍ個の断片に分割され、各断片は、ＡＲＰ信頼済フレンド（ＡＲＰＴＦ）へセキュアに分散され、必要となるまで供託される。その間、ＡＲＫ秘密情報および断片の内容は、ＡＲＰＴＦの立場からは隠されている。

【００３３】

１つまたは複数の実施形態において、ＡＲＰＴＦ自体も、パスワードマネージャアプリケーションの有効なアカウント所持者である。特定の実施形態において、信頼済フレンドは、ＡＲＰＴＦとなるべく、アカウント所持者によって招待され、招待を承認するか、拒否する選択肢を有する。特定の実施形態において、アカウント所持者は、ＡＲＰＴＦのリストを自在に修正できる。１つまたは複数の実施形態において、ＡＲＫ秘密情報は分割され、シャミアの秘密分散法（ＳＳＳ）を介してＡＲＰＴＦへ分散される。ＳＳＳは、秘密情報が所定の数の部分へと分割される暗号アルゴリズムであり、各参加者に対して、自身に固有の部分を与える。当該部分のいくつか、または、全ては、秘密情報を再構築するのに必要である。いくつかの実施形態において、ユーザの支配下にあるオブジェクトまたはデバイス（例えば、スマートフォン、タブレット、ＰＣ、ＵＳＢ鍵、バーコードが印刷さ

れた紙片など）も、ＳＳＳからの１つの断片を保持することによって、ＡＲＰＴＦとして機能できる。図２に示されている実施形態において、第２クライアントデバイス２０２ｂに関連するユーザＢ、第３クライアントデバイス２０２ｃに関連するユーザＣ、第４クライアントデバイス２０２ｄに関連するユーザＤ、第５クライアントデバイス２０２ｅに関連するユーザＥ、および、第６クライアントデバイス２０２ｆに関連するユーザＦは各々、第１クライアントデバイス２０２ａに関連するアカウント所持者ユーザＡの信頼済フレンド、すなわちＡＲＰＴＦとして指定されている。

【００３４】

アカウントを復元する必要が生じた場合、アカウント所持者は、アカウント復元のための要求を認証サーバ２０６に対して発行する。復元プロセスを開始するとき、アカウント所持者は、バリデーションループを提示される。特定の実施形態において、バリデーションループは、アカウント所持者の電子メールアドレスと、ＣＡＰＴＣＨＡチャレンジ（例えば、応答者が人間であることを証明するためのテキストまたは画像の検証）への応答と、復元プロセスにおいて使用される、ユーザが選択および入力する仮のマスター鍵とを収集することを含む。ＣＡＰＴＣＨＡ（「コンピュータと人間を区別するための、完全自動の公開チューリングテスト」の略語）とは、ユーザが人間かどうか判定するためのチャレンジ／レスポンス試験の一種である。認証サーバ２０６は次に、アウトオブバンド確認コード（ＯＣＣ）を生成する。これは、アウトオブバンド（ＯＯＢ）通信が改ざんなく完了したことを確認するための確認目的でＡＲＰＴＦに提供され、ＡＲＰＴＦによって使用される、小さい秘密情報（例えば、４桁のコード）である。

【００３５】

１つまたは複数の実施形態において、認証サーバ２０６は次に、アカウント所持者に指示して、ＡＲＰＴＦリストのメンバに連絡し、復元に協力する要求を当該メンバへ通知し、ＡＲＰＴＦのメンバの各々にＯＣＣを提供させる。特定の実施形態において、その過程にある全てのエントリおよびエンティティは、認証サーバ２０６によって検証される。ＡＲＰＴＦは各々、ＯＣＣを含む、アカウント復元に協力する要求を受信し、要求を確認するよう促される。認証サーバ２０６は、確認を受信すると、ＡＲＰＴＦの復元トークンを取得することが可能になる。アカウント所持者のパスワードアプリケーションは次に、取得されたトークンの各々を復号し、ＡＲＰＴＦ応答のコンセンサスを構築する。１つまたは複数の実施形態において、所定の数または部分（例えば、５０％か、それより多い、または、５分の３など）の応答がＡＲＰＴＦから受信された場合にコンセンサス状態が達成されるように、ＳＳＳパラメータがセットアップされる。コンセンサス状態が達成されると、ＡＲＫを再構築するべく、受信された復元トークンは復号され、組み立てられる。ＡＲＫは、復元プロセスを実行するためのＡＲＢを復号するのに使用される。復元プロセス中、要求される全てのシード、鍵、新しい断片、ならびに、新しい最新の鍵材料の再生、および、仮のマスター鍵を新しいマスター鍵へ昇格させるための再暗号化をするための手順が実行され、それにより、ユーザは、新しいマスター鍵を介してログインし、ユーザのアカウントおよびリソースの支配を取り戻すことが可能になる。

【００３６】

本明細書に記載されている様々な実施形態は、認証およびユーザデータ暗号化両方のための暗号鍵生成のソースとして、マスターパスワードを利用する。１つまたは複数の実施形態において、認証サーバ２０６は、暗号化に基づく、ユーザデータの認証および復元に同一の秘密情報（例えば、マスターパスワード）を使用する。復元情報は、信頼および検証されたエンティティ、ならびに、認証サーバ２０６の間で分散される。その間、復元鍵の正確な内容は知られることがない。これは、認証サーバ２０６を隔離すること、および、パスワード復元データを狙ったセキュリティ上の脅威に対抗することを目的としている。

【００３７】

１つまたは複数の実施形態において提供される復元機構では、仮のパスワードはチェックおよび暗号操作を受け、データの分散情報に基づいて完全に検証されたときだけ、以前

に知られた良いマスターパスワードと置き換わることが承認される。特定の実施形態において、ＳＳＳアルゴリズムは、復元鍵を断片化し、信頼される複数のエンティティ間で分散させることに使用される。以下の項では、１つまたは複数の具体的な実施形態による、ＡＲＰの様々なシーケンスの例示的な高レベルの操作を記載する。１つまたは複数の実施形態は、ＡＥＳ－ＣＣＭを使用する。これは、関連データ付き認証付き暗号（ＡＥＡＤ）アルゴリズムであり、同時に全体を認証しながら、メッセージの一部または全体を暗号化できる、ブロック暗号モード操作の一種である。高度暗号化規格（ＡＥＳ）は、システム内の全てのデータを暗号化するのに使用されるブロック暗号である。Ｃｏｕｎｔｅｒ ｗｉｔｈ ＣＢＣ－ＭＡＣ（ＣＣＭ）は、暗号化データの機密性および完全性の両方を提供するべく、ＡＥＳと共に使用されるブロック暗号モード操作である。１つまたは複数の実施形態において、メッセージの一部だけが暗号化され、残りは暗号化されていないが認証されている状態を維持する。特定の実施形態において、（ＥＮＣ）は、暗号化および認証されていることを示すのに使用され、（ＭＡＣ）は認証だけされていることを示すのに使用される。

【００３８】

以下の例示的なシーケンスにおいて、以下のエンティティが使用される。

【００３９】

ユーザＡは、自身のマスターパスワードを時折失念し得るのでＡＲＰを使用する「失念しやすい人」である。ユーザＡは、ユーザＡが認証サーバ２０６とインタラクトするのに使用するクライアント、アプリケーション、パスワードアプリケーション２１２ａを有する第１クライアントデバイス２０２ａに関連する。

【００４０】

ユーザＢ、Ｃ、Ｄ、Ｅ、Ｆは、ユーザＡの信頼済フレンド（すなわちＡＲＰＴＦ）のメンバであり、ユーザＡが自身のアカウント復元鍵（ＡＲＫ）の断片を分散する相手である。記載されているように、ＡＲＫは、ランダムに生成される秘密鍵であり、アカウント所持者（ユーザＡ）だけに保持されるＡＲＢを暗号化するのに使用され、ｍ個の断片へ分割され、各々、信頼済フレンド（例えば、ユーザＢ、Ｃ、Ｄ、Ｅ、Ｆ）とセキュアに分散される。特定の実施形態において、ユーザＢ－Ｆは、それぞれ、クライアントデバイス２０２ｂ－２０２ｆに関連し、それぞれ、パスワードマネージャアプリケーション２１２ｂ－２１２ｆを各々有する。

【００４１】

パスワードＲＥＳＴ ＡＰＩ２１４は、認証し、資産を保存し、分散を可能にし、ＡＲＰを制御するように機能する、認証サーバ２０６の認証コンポーネント１０２内のサービスである。

【００４２】

図３Ａ－図３Ｂは、一実施形態による、アカウント復元プロトコルのセットアップおよび管理のためのプロセスフロー３００の例を示す。セットアップ前、ユーザＡは、パスワードアプリケーション２１２ａに関連するアカウントを生成する。１つまたは複数の実施形態において、アカウントを生成する段階は、アカウントのためのマスターパスワードを指定する段階を含む。アカウント生成後、ユーザＡは、自身のアカウントに関連するフレンドとして、ユーザＢ、ユーザＣ、ユーザＤ、ユーザＥ、および、ユーザＦの各々に対し、招待要求を送信する。１つまたは複数の実施形態において、ユーザＢ、ユーザＣ、ユーザＤ、ユーザＥ、ユーザＦは、既に自身のアカウントを持っていることもあるが、持っていない場合、要求の受信に応答して、自身のアカウントを生成するように促され得る。ユーザＢ、ユーザＣ、ユーザＤ、ユーザＥ、および、ユーザＦのうち１つまたは複数は、フレンドシップ要求を確認し得て、その結果、ユーザＡのアカウントにリンクされているフレンドは、アカウント復元プロトコル（ＡＲＰ）セットアップのフェーズへ進むのに十分な数となる。１つまたは複数の実施形態において、ユーザＡと、ユーザＢ、ユーザＣ、ユーザＤ、ユーザＥ、および、ユーザＦの各々との間のフレンドとしての関係は、認証サーバ２０６によってデータベース内に保存される。

【００４３】
３０２において、第１クライアントデバイス２０２ａのユーザＡは、自身のマスターパスワードを使用して、第１クライアントデバイス２０２ａのパスワードアプリケーション２１２ａに対し、ログイン手順を開始する。特定の実施形態において、ユーザＡは、第１クライアントデバイス２０２ａに関連するグラフィカルユーザインタフェース（ＵＩ）を使用して、電子メールアドレスおよびマスターパスワードをパスワードアプリケーション２１２ａに入力する。ユーザＡは次に、ＡＲＰセットアップを開始するべく、ＵＩ内のＡＲＰセットアップ画面へ移動し得る。３０４において、パスワードアプリケーション２１２ａは、ユーザＡの認証のための要求（ＰＯＳＴ／ａｐｉ＿ｌｏｇｉｎ）を認証サーバ２０６のパスワードアプリケーションＲＥＳＴ　ＡＰＩ２１４へ送信する。特定の実施形態において、認証のための要求は、ユーザＡに関連する電子メールアドレス、および、認証トークンを含む。３０６において、認証サーバ２０６は、電子メールアドレスおよび認証トークンを使用して、データベースと照会して、ユーザＡを認証する。３０８において、パスワードアプリケーション２１２ａは、ユーザＡが認証されたことを示す認証応答（ＨＴＴＰ　２００　Ａｕｔｈ＿ＯＫ）を認証サーバ２０６から受信する。特定の実施形態において、認証応答は、セッショントークンを含む。３１０において、パスワードアプリケーション２１２ａは、ユーザＡがログインしたという通知をユーザＡに提供する。

【００４４】
３１２において、ユーザＡは、パスワードマネージャアプリケーション２１２ａによって提供される、ＵＩ内のＡＲＰセットアップ画面を見て、ＡＲＰセットアップを開始する。３１４において、パスワードアプリケーション２１２ａは、ユーザＡのフレンドとして指定されているアカウント（例えば、ユーザＢ、ユーザＣ、ユーザＤ、ユーザＥ、ユーザＦ）に対応する連絡先リストを含むメンバオブジェクト（ＨＴＴＰ　ＧＥＴ／ｍｅｍｂｅｒ／｛ｍｅｍｂｅｒ＿ｉｄ｝／）を取得するための要求を認証サーバ２０６へ送信する。３１６において、パスワードマネージャアプリケーション２１２ａは、ユーザＡのアカウントに関連する連絡先（例えばフレンド）リストを受信するが、フレンドの一部は信頼済フレンド（すなわちＡＲＰＴＦ）として指定済みであり得る。アカウントが既にＡＲＰについてセットアップされた場合、リストはＡＲＢ＿ＡＲＫ　ＪＳＯＮ属性を含むが、認証トークンワンタイムパスワード（ＡＵＴＨ－ＴＯＫ－ＯＴＰ）ＪＳＯＮ属性を含まない。なぜなら、それは認証サーバ２０６上に秘密情報として保存され続けているからである。連絡先リストを含む、受信された応答メッセージ（／ｃｏｎｔａｃｔｓ／）は、ＡＲＰＴＦと見なされる、いくつかの連絡先を含み得る。ＡＲＰＴＦである連絡先は、ＡＲＫ－Ｐｘ　ＪＳＯＮ属性、すなわち、供託するべくＡＲＰＴＦへ送信されるＡＲＫ断片を含む。３１８において、パスワードマネージャアプリケーション２１２ａは、ユーザＡが、アカウント復元プロトコルのセットアップを継続するのに十分な連絡先を有するかどうか判定する。ユーザＡが十分な連絡先を有する場合、セットアップ手順は継続する。そうでなければ、ユーザＡは、パスワードマネージャアプリケーション２１２ａによって、より多くのフレンドを招待して、アカウント復元に参加させるように促される。

【００４５】
３２０において、パスワードマネージャアプリケーション２１２ａは、連絡先リストをユーザＡに表示する。３２２において、ユーザＡは、連絡先リストから、ユーザＡが信頼するフレンドを、アカウント復元プロトコル（ＡＲＰ）に参加するＡＲＰＴＦとして選択する。３２４において、パスワードアプリケーション２１２ａは、更新された連絡先リストをユーザＡに表示し、選択を確認するようにユーザＡに促す。３２６において、ユーザＡは、ＡＲＰＴＦの招待を、パスワードマネージャアプリケーション２１２ａに対して確認する。

【００４６】
３２８において、パスワードアプリケーション２１２ａは、ユーザＡのための最新のアカウント復元鍵（ＡＲＫ）を生成する。特定の実施形態において、パスワードアプリケーション２１２ａは、秘密鍵を生成するのに使用されるプリミティブとして機能する暗号論

的擬似乱数生成器（ＣＳＰＲＮＧ）を使用して、２５６ビットのアカウント復元鍵（ＡＲＫ）を生成する。３３０において、パスワードアプリケーション２１２ａは、最新の認証トークンワンタイムパスワード（ＡＵＴＨ－ＴＯＫ－ＯＴＰ）を生成する。特定の実施形態において、ＡＵＴＨ－ＴＯＫ－ＯＴＰは、２５６ビットの値である。３３２において、パスワードアプリケーション２１２ａは、ＡＵＴＨ－ＴＯＫ－ＯＴＰと、ＡＲＫを使用して暗号化されたコンテンツ暗号化鍵（ＣＥＫ）とを含む、暗号化されたアカウント復元バンドル（ＡＲＢ）を生成する。１つまたは複数の実施形態において、ＡＲＢは、バンドルスキームおよび作成日を識別するメッセージ認証コード（ＭＡＣ）部分と、ＡＵＴＨ－ＴＯＫＥＮ－ＯＴＰ（ＥＮＣ）、および、アカウントのコンテンツ暗号化鍵（ＣＥＫ）（ＥＮＣ）を含む暗号化部分とを有するＪＳＯＮドキュメントである。

【００４７】

３３４において、パスワードアプリケーション２１２ａは、ＡＲＫを所定の数（選択されたＡＲＰＴＦの数）であるｍ個の断片へ分割する。特定の実施形態において、パスワードアプリケーション２１２ａは、シャミアの秘密分散法（ＳＳＳ）を使用して、ＡＲＫを所定の数の断片に分割する。その結果、分散断片の完全なリストが生成される。この中の各分散断片（ＡＲＫ－Ｐｘ）は、隠された状態でＡＲＰＴＦのアカウント内に供託され、ＡＲＫを復元するべく、後に使用され得る。１つまたは複数の実施形態において、ユーザＡのＡＲＰＴＦのコンセンサス（例えば、５０％、または、それより多い）があるように、ＳＳＳパラメータがセットアップされる。すなわち、ＡＲＫを復元するには、５分の３が要求される。特定の実施形態において、これらのセキュリティパラメータは、利便性とコンセンサスとの間のトレードオフとして調節され得る。

【００４８】

３３６において、パスワードアプリケーション２１２ａは、ＡＲＫによって暗号化されたＡＲＢ（ＡＲＢ＿ＡＲＫ）、および、ＡＵＴＨ－ＴＯＫ－ＯＴＰで、認証サーバ２０６に保存された、ユーザＡのメンバオブジェクトを更新する。特定の実施形態において、パスワードアプリケーション２１２ａは、認証サーバ２０５のパスワードアプリケーションＲＥＳＴ　ＡＰＩ２１４へ、ＡＲＢ＿ＡＲＫおよびＡＵＴＨ－ＴＯＫ－ＯＴＰ、ならびに、ユーザＡの識別情報（ｍｅｍｂｅｒ＿ｉｄ）を含むＨＴＴＰ　ＰＵＴ／ｍｅｍｂｅｒ／｛ｍｅｍｂｅｒ＿ｉｄ｝／メッセージを送信する。３３８において、パスワードアプリケーションＲＥＳＴ　ＡＰＩ２１４は、更新されたメンバオブジェクトのコピーを返すが、これにはＡＵＴＨ－ＴＯＫ－ＯＴＰは含まれない。なぜなら、それは秘密情報として認証サーバ２０６上に保存され続けているからである。

【００４９】

３４０において、パスワードアプリケーション２１２ａは、ユーザＡのＡＲＰＴＦの各々のためのＡＲＰ招待（ＡＲＰＩ）を使用して、ＡＲＫ－Ｐｘの各断片を、ユーザＡの異なるＡＲＰＴＦへ分散する。特定の実施形態において、パスワードアプリケーション２１２ａは、連絡先識別子（ｃｏｎｔａｃｔ＿ｉｄ）によって識別される各ＡＲＰＴＦへＨＴＴＰ　ＰＵＴ／ｃｏｎｔａｃｔ／｛ｃｏｎｔａｃｔ＿ｉｄ｝／メッセージを送信する。このメッセージが有する更新された連絡先オブジェクトは、このＡＲＰＴＦのための公開鍵で暗号化された、特定のＡＲＫ－Ｐｘを含む。パスワードＲＥＳＴ　ＡＰＩ２１４は、ＡＲＰＴＦの立場からは隠れるように指定することで、ＡＲＫ－Ｐｘ断片を供託する。１つまたは複数の実施形態において、ＡＲＰ招待（ＡＲＰＩ）を完了するべく、ＡＲＰＴＦは、受信者の連絡先の１つがＡＲＰＴＦになるように依頼していると説明する通知を受信する。受信者は、ＡＲＰＩを承認または拒否できる。特定の実施形態において、パスワードＲＥＳＴ　ＡＰＩ２１４は、特定のＡＲＰＴＦが招待を承認したかどうかについての通知を含むＨＴＴＰ２００メッセージを送信する。

【００５０】

３４２において、パスワードアプリケーション２１２ａは、ユーザＡに対し、招待が送信されたという確認応答と、ＡＲＰＴＦの各々が招待を承認したかどうかについての通知とを含む、確認応答メッセージを送信する。特定の実施形態において、ユーザＡは後に、

上述の手順のうち１つまたは複数を再度実行することにより、ＡＲＰＴＦのリストを管理できる。ユーザＡが、以前の手順を少なくとも１回、良好に完了した場合、既存の属性は、ユーザＡが後に修正できる認証サーバ２０６によって保存される。

【００５１】

図４Ａおよび図４Ｂは、一実施形態によるアカウント復元プロトコルのためのアカウント復元要求確立プロセスフロー４００の例を示す。アカウント復元要求確立プロセスは、新しいアカウント復元要求を確立する。図４Ａおよび図４Ｂの例示的な第１プロセスフローは、ＡＲＰセットアップをすぐに実行するするのに十分なＡＲＰＴＦをユーザＡが既に持っていることを前提としている。図４Ａおよび図４Ｂの実施形態において、ユーザＡは、不運にも自分のマスターパスワードを失念し、自分のアカウントへログインできない。しかしながら、ユーザＡは過去にＡＲＰをセットアップしたので、ＡＲＰＴＦを使用して、自分のアカウントへのアクセスを復元できる。４０２において、ユーザＡは、自分のマスターパスワードを失念する。４０４において、ユーザＡは、クライアントデバイス２０２ａのパスワードアプリケーション２１２ａによって提供されるグラフィカルユーザインタフェース内の「マスターパスワードを失念した」という選択肢をクリックする。

【００５２】

４０６において、パスワードアプリケーション２１２ａは、最新のＣＡＰＴＣＨＡチャレンジを取得するための要求を認証サーバ２０６へ送信する。特定の実施形態において、パスワードアプリケーション２１２ａは、ＣＡＰＴＣＨＡチャレンジを要求するべく、認証サーバ２０６のパスワードアプリケーションＲＥＳＴ　ＡＰＩ２１４に対し、ＧＥＴ／ｃａｐｔｃｈａメッセージを送信する。４０８において、クライアントデバイス２０２ａのパスワードアプリケーション２１２ａは、認証サーバ２０６から、ＣＡＰＴＣＨＡチャレンジ応答メッセージを受信する。特定の実施形態において、認証サーバ２０６は、クライアントデバイス２０２ａに対し、ＨＴＴＰ２００　ＣＡＰＴＣＨＡチャレンジを送信する。

【００５３】

４１０において、クライアントデバイス２０２ａのパスワードアプリケーション２１２ａは、ＣＡＰＴＣＨＡチャレンジ応答メッセージの受信に応答して、ユーザＡに対し、グラフィカルユーザインタフェース内にアカウント復元確立画面を表示する。１つまたは複数の実施形態において、アカウント復元確立画面は、電子メールのフォームフィールド、ＣＡＰＴＣＨＡチャレンジの画像表現、ＣＡＰＴＣＨＡ回答のフォームフィールド、仮マスターパスワードを入力するためのパスワードフィールド、および、「アカウント復元の要求」ボタンのうち、１つまたは複数のアイテムを含むＧＵＩフォームを表示する。４１２において、クライアントデバイス２０２ａのパスワードアプリケーション２１２ａは、ユーザＡに対し、グラフィカルユーザインタフェース内にＣＡＰＴＣＨＡ画像を表示する。４１４において、ユーザＡは、アカウント復元確立画面内のフォームを見る。４１６において、ユーザＡは、フォームに記入し、確認ボタンをクリックする。

【００５４】

４１８において、クライアントデバイス２０２ａのパスワードアプリケーション２１２ａは、仮マスターパスワードおよび電子メールを使用して、仮認証トークン（ＰＢＫＤＦ２）を導出する。４２０において、パスワードアプリケーション２１２ａは、一時的リベスト・シャミア・エーデルマン（ＲＳＡ）鍵ペア（ＥｐｈＫｅｙＰａｉｒ）を生成する。特定の実施形態において、ＥｐｈＫｅｙＰａｉｒは、２０４８ビットのＲＳＡ鍵ペアである。４２２において、パスワードアプリケーション２１２ａは、一時的鍵暗号化鍵（ＫＥＫ）導出ソルト（ＥｐｈＫＥＫＳａｌｔ）を生成する。鍵暗号化鍵（ＫＥＫ）は、マスターパスワード、および、ランダムに生成されるソルトから導出される秘密鍵である。特定の実施形態において、ＥｐｈＫＥＫＳａｌｔは、２５６ビットの値である。４２４において、パスワードアプリケーション２１２ａは、アウトオブバンド確認コード（ＯＣＣ）を生成する。特定の実施形態において、ＯＣＣは、４桁の数値コードである。４２６において、パスワードアプリケーション２１２ａは、一時的鍵暗号化鍵（ＥｐｈＫＥＫ）（Ｅｐ

ｈＫＥＫＳａｌｔ、マスターパスワードによるＰＢＫＤＦ２）を導出する。鍵暗号化鍵（ＫＥＫ）は、マスターパスワード、および、ランダムに生成されたソルトから導出される秘密鍵（ＰＢＫＤＦ２）である。４２８において、パスワードアプリケーション２１２ａは、ＥｐｈＫＥＫでＥｐｈＫｅｙＰａｉｒをラップする。４３０において、パスワードアプリケーション２１２ａは、ＥｐｈＫＥＫによってＯＣＣをラップする。

【００５５】

４３２において、クライアントデバイス２０２ａのパスワードアプリケーション２１２ａは、アカウント復元要求メッセージを生成し、認証サーバ２０６のパスワードアプリケーションＲＥＳＴ　ＡＰＩ２１４に対し、アカウント復元要求メッセージを送信する。特定の実施形態において、アカウント復元要求メッセージは、電子メールアドレス、ｃａｐｔｃｈａ＿ｃｈａｌｌｅｎｇｅ、ｃａｐｔｃｈａ＿ａｎｓｗｅｒ、ｐｒｏｖｉｓｉｏｎａｌ＿ａｕｔｈ＿ｔｏｋｅｎ（認証トークンとして導出される新しいマスターパスワード）、ｅｐｈｅｍｅｒａｌ＿ｋｅｋ＿ｄｅｒｉｖａｔｉｏｎ＿ｓａｌｔ、ｅｐｈｅｍｅｒａｌ＿ｐｕｂｌｉｃ＿ｋｅｙ、ｅｎｃｒｙｐｔｅｄ＿ｅｐｈｅｍｅｒａｌ＿ｋｅｙｐａｉｒ、および、ｅｎｃｒｙｐｔｅｄ＿ｏｃｃ（アウトオブバンド確認コード）を含むＪＳＯＮリクエストボディを有する未認証のＰＯＳＴ／ａｃｃｏｕｎｔ＿ｒｅｃｏｖｅｒｙ／メッセージの形式である。４３４において、認証サーバ２０６のパスワードアプリケーションＲＥＳＴ　ＡＰＩ２１４は、クライアントデバイス２０２ａのパスワードアプリケーション２１２ａに対してアカウント復元応答メッセージを送信する。特定の実施形態において、アカウント復元応答メッセージは、アカウント復元要求ＩＤ（ａｒｒ＿ｉｄ）、ｃｒｅａｔｉｏｎ＿ｄａｔｅ＝ＮＯＷ、ｅｘｐｉｒａｔｉｏｎ＿ｄａｔｅ＝ＮＯＷ＋ｅｘｐｉｒａｔｉｏｎ　ｉｎｔｅｒｖａｌ（例えば、４８時間）、および、ｓｔａｔｕｓ＝"ｒｅｑｕｅｓｔ＿ｃｏｎｆｉｒｍａｔｉｏｎ＿ｐｅｎｄｉｎｇ"を含むＪＳＯＮレスポンスボディを有するＨＴＴＰ２００メッセージである。特定の実施形態において、アカウント復元要求ＩＤは、新しいＡＲＲの生成が成功したときにパスワードＲＥＳＴ　ＡＰＩ２１４によって返される固有のランダムＩＤである。

【００５６】

アカウント復元応答メッセージを受信すると、４３６において、クライアントデバイス２０２ａのパスワードアプリケーション２１２ａは、ユーザＡに対して、電子メールを読むこと、および、送信したばかりの電子メールに含まれるリンクをクリックして要求を確認することを促す。４３８において、ユーザＡは、電子メールを読む。４４０において、ユーザＡは、確認用リンクをクリックし、クライアントデバイス２０２ａのパスワードアプリケーション２１２ａは、確認を示す確認メッセージを、認証サーバ２０６のパスワードアプリケーションＲＥＳＴ　ＡＰＩ２１４に送信する。１つまたは複数の実施形態において、確認メッセージは、要求確認トークン（ｒｅｑｕｅｓｔ＿ｃｏｎｆｉｒｍａｔｉｏｎ＿ｔｏｋｅｎ）を含む。特定の実施形態において、要求確認トークンは、ランダムに生成されたトークンであり、電子メール検証ループを通して、ＡＲＰの開始を確認するのに使用される。

【００５７】

４４２において、認証サーバ２０６のパスワードアプリケーションＲＥＳＴ　ＡＰＩ２１４は、ユーザＢ、ユーザＣ、ユーザＤ、ユーザＥ、および、ユーザＦの各々に対して、ユーザＡが自分のアカウントを復元するべく、それらのユーザの協力を要求したことを示す電子メールを送信する。４４４において、認証サーバ２０６のＲＥＳＴ　ＡＰＩ２１４は、クライアントデバイス２０２ａのパスワードアプリケーション２１２ａに確認応答を送信する。４４６において、クライアントデバイスのパスワードアプリケーション２１２ａは次に、ＯＣＣをユーザＡに表示し、各ＡＲＰＴＦに連絡することをユーザＡに指示する命令を表示し得る。特定の実施形態において、メッセージは、確認用リンクを含む電子メールを含み得る。特定の実施形態において、ユーザＡが１つまたは複数のＡＲＰＴＦのＩＤを失念した場合、ユーザＡは、ユーザＡに関連するＡＲＰＴＦのＩＤを呼び出すべく、ＧＵＩを使用し得る。４４８において、ユーザＡは、各ＡＲＰＴＦに連絡してＯＣＣを

提供する。これは、フィッシングを防止し、信頼済フレンドが実際にプロトコル以外の他の手段で連絡されたことを保証する手段である。これで手順４００は終了する。特定の実施形態において、ユーザＡは、クライアントデバイス２０２ａを使用して、各ＡＲＰＴＦに連絡し得る。

【００５８】

図４Ａおよび図４Ｂに記載されている特定の実施形態において、電子メール検証ループは、アカウント復元プロセスを発生させるための認証の手段として使用される。ユーザの大部分は、スマートフォンなどの電子デバイスの使用を通して、電子メールにほぼ常時アクセスしている。したがって、これらのユーザにとって、特定のユーザが自分のマスターパスワードを失念し、同時に、電子メールに対する、全ての形式のアクセスを失い得るという状況が発生する確率は低い。しかしながら、その電子メールアカウントへのアクセスは、復元のセキュリティに何らかの影響を及ぼすので（アウトオブバンド確認コードは他の部分を提供する）、他の実施形態において、アカウント復元要求確立手順を発生させるための他の方法が使用され得る。例えば、特定の実施形態において、アカウントの所持を検証または主張するべく、画像認証方式（ＩＢＡ）またはマイクロペイメントが使用され得る。

【００５９】

図５は、一実施形態によるアカウント復元プロトコルのためのアカウント復元要求招待プロセスフロー５００の例を示す。１つまたは複数の実施形態において、プロセスフロー５００は、図４Ａおよび図４Ｂのアカウント復元要求確立フローの終了後、自動的に開始される。５０２において、ユーザＡは、自身の手段で、ユーザＢ（信頼済フレンド）に連絡し、アウトオブバンド確認コード（ＯＣＣ）をユーザＢに提供する。これにより、ユーザＡは自分のアカウントを復元するべく、ユーザの協力を要求していることを通知する。図５には示されていないが、ユーザＡは、ＡＲＰＴＦ（例えば、信頼済フレンド）の各々にも連絡し、ＯＣＣを提供する。５０４において、ユーザＡは、ユーザＢおよび各ＡＲＰＴＦからの応答を待つ。５０６において、ユーザＢは、第２ユーザデバイス２０２ｂを使用して、ユーザＢのパスワードアプリケーション２１２へのログインを実行する。５０８において、第２パスワードアプリケーション２１２ｂは、認証サーバ２０６のパスワードＲＥＳＴ　ＡＰＩ２１４に対し、ユーザＢのログインを示すログインコールを送信する。特定の実施形態において、ログインコールは、ＰＯＳＴ　ＡＰＩコールである。５１０において、パスワードＲＥＳＴ　ＡＰＩ２１４は、第２パスワードアプリケーション２１２ｂに対し、セッショントークン（ｓｅｓｓｉｏｎ＿ｔｏｋｅｎ）を含むログイン確認応答を送信する。５１２において、第２パスワードアプリケーション２１２ｂは、第２クライアントデバイス２１２のＧＵＩを介して、ユーザＢに対し、ログイン成功の通知を提供する。

【００６０】

５１４において、第２パスワードアプリケーション２１２ｂは、認証サーバ２０６のパスワードＲＥＳＴ　ＡＰＩ２１４に対し、何らかのアカウント復元要求招待の取得のための要求を送信する。特定の実施形態において、要求は、ＧＥＴ／ａｃｃｏｕｎｔ＿ｒｅｃｏｖｅｒｙ／ｒｅｑｕｅｓｔ＿ｉｎｖｉｔａｔｉｏｎｓの形式である。５１６において、パスワードＡＰＩ２１４は、ユーザＢをＡＲＰＴＦとして認証し、アカウント復元要求招待のリストを第２パスワードアプリケーション２１２ｂに送信する。特定の実施形態において、アカウント復元要求招待リストは、メンバ識別子（ｍｅｍｂｅｒ＿ｉｄ）、アカウント復元要求復元識別子（ａｒｒ＿ｓｈａｒｅ＿ｂａｃｋ＿ｉｄ）、一時的公開鍵（ｅｐｈｅｍｅｒａｌ＿ｐｕｂｌｉｃ＿ｋｅｙ）、ユーザＢの公開鍵で暗号化されたアカウント復元鍵分散断片（ａｒｋ＿ｐｘ＿ｐｕｂ＿ｋｅｙ）を含む。５１８において、第２パスワードアプリケーション２１２ｂが空でないリストを受信する場合、第２パスワードアプリケーション２１２ｂは、ユーザＢに対して、アカウント復元に協力するべく、供託されている自分のＡＲＫ分散断片（ＡＲＫ－Ｐｘ）を戻すように促す。５２０において、ユーザＢは、アカウント復元を確認するべく、ＯＣＣおよび確認を第２パスワードアプリケーシ

ョン２１２に提供する。特定の実施形態において、ユーザＢは、ＯＣＣを入力し、第２ユーザデバイス２０２ｂのＧＵＩ内の「確認」ボタンをクリックし得る。

【００６１】

５２２において、第２パスワードアプリケーション２１２ｂは、ユーザＢ自身の秘密鍵を使用して、「ａｒｋ＿ｐｘ＿ｐｕｂ＿ｋｅｙ」を復号し、平文ＡＲＫ－Ｐｘ、すなわち、断片の１つを生み出す。５２４において、第２パスワードアプリケーション２１２ｂは、一時的公開鍵（ＥｐｈＰｕｂＫｅｙ）で平文ＡＲＫ－Ｐｘを再暗号化する。５２６において、第２パスワードアプリケーション２１２ｂは、アウトオブバンド確認コード（ＯＣＣ）によって鍵をかける鍵付ハッシュ関数メッセージ認証コード（ＨＭＡＣ））｛ＨＭＡＣ（ＯＣＣ、ＡＲＫ－Ｐｘ｝を使用して、ＯＯＢトランザクションに署名する。特定の実施形態において、トランザクションは、ＳＨＡ－２５６暗号ハッシュ関数を使用して署名される。５２８において、第２パスワードアプリケーション２１２ｂは、認証サーバ２０６のパスワードＲＥＳＴ　ＡＰＩ２１４に対し、ＡＲＲ復元ＩＤ｛ａｒｒ＿ｓｈａｒｅ＿ｂａｃｋ　ＩＤ｝と、ＡＲＲ一時的公開鍵（ＡＲＲＥｐｈＰｕｂＫ）で暗号化されたＡＲＫ－Ｐｘ｛ａｒｋ＿ｐｘ＿ｅｐｈ＿ｐｕｂ＿ｋｅｙ｝と、アウトオブバンド確認コードを鍵として使用した、ＡＲＫ－ＰｘのＨＭＡＣ｛ｈｍａｃ＿ｏｃｃ＿ａｒｋ＿ｐｘ｝とを送信する。特定の実施形態において、ＡＲＲ一時的公開鍵は、ＡＲＲの期間だけ有効な公開鍵である。特定の実施形態において、第２パスワードアプリケーション２０２ｂは、ａｒｒ＿ｓｈａｒｅ＿ｂａｃｋ＿ｉｄ、ａｒｋ＿ｐｘ＿ｅｐｈ＿ｐｕｂ＿ｋｅｙ、ｈｍａｃ＿ｏｃｃ＿ａｒｋ＿ｐｘを含むＪＳＯＮリクエストボディを有する、ＰＯＳＴ／ａｃｃｏｕｎｔ＿ｒｅｃｏｖｅｒｙ／ｍｅｍｂｅｒ／｛ｍｅｍｂｅｒ＿ｉｄ｝／という形式のＰＯＳＴメッセージを使用する。５３０において、パスワードＲＥＳＴ　ＡＰＩ２１４は、確認応答を第２パスワードアプリケーション２１２ｂに送信する。特定の実施形態において、確認応答は、ＨＴＴＰ２００メッセージである。５３２において、第２パスワードアプリケーション２１２ｂは、特定のＡＲＫ－Ｐｘ断片が良好に分散されたことを示す確認メッセージをユーザＢに提示する。５０２～５３２の手順は、ユーザＡの残りのＡＲＰＴＦのうちの１つまたは複数について、それぞれのパスワードアプリケーションを使用して繰り返される。それぞれのパスワードアプリケーションにおいて、パスワードＲＥＳＴ　ＡＰＩ２１４は、１つまたは複数の分散ＡＲＫ－Ｐｘ断片を各ＡＲＰＴＦから受信する。パスワードＲＥＳＴ　ＡＰＩ２１４が十分な分散ＡＲＫ－Ｐｘ断片を受信したとき、パスワードＲＥＳＴ　ＡＰＩ２１４は、５３４において、アカウント復元要求のステータスを「ｃｏｎｓｅｎｓｕｓ＿ｒｅａｃｈｅｄ」へと更新し、手順５００が終了する。

【００６２】

図６Ａおよび図６Ｂは、一実施形態によるアカウント復元プロトコルのアカウント復元要求完了プロセスフロー６００の例を示す。１つまたは複数の実施形態において、プロセスフロー６００は、アカウント復元要求に関するコンセンサスが達成された、図５のアカウント復元要求招待プロセスフローの終了後に開始される。６０２において、ユーザＡは、アカウント復元要求手順を再開する。特定の実施形態において、ユーザＡは、仮認証トークン（ＰＢＫＤＦ２）の導出を必要とする、自分の仮マスターパスワードを入力する。６０４において、第１パスワードアプリケーション２１２ａは、ＡＲＲレコードの更新版を認証サーバ２０６のパスワードＲＥＳＴ　ＡＰＩ２１４から取得するための要求を送信する。特定の実施形態において、取得要求は、ＧＥＴ／ａｃｃｏｕｎｔ＿ｒｅｃｏｖｅｒｙ／｛ａｒｒ＿ｉｄ｝／という形式のＧＥＴ要求である。特定の実施形態において、要求は未認証であるが、汎用固有識別子（ＵＵＩＤ）を介してだけアクセスでき、全てのデータは暗号化され、読み取り専用である。６０６において、パスワードＲＥＳＴ　ＡＰＩ２１４は、アカウント復元に必要な情報を含む応答を送信する。特定の実施形態において、応答は、以下のＪＳＯＮレスポンスボディを含むＨＴＴＰ２００応答である。

ａ．アカウント復元要求ＩＤ（ａｒｒ＿ｉｄ）

ｂ．メンバＩＤ（ｍｅｍｂｅｒ＿ｉｄ）

ｃ．要求の作成日（ｃｒｅａｔｉｏｎ＿ｄａｔｅ）

ｄ．要求の期限日（ｅｘｐｉｒａｔｉｏｎ＿ｄａｔｅ）
ｅ．ステータス＝「ｃｏｎｓｅｎｓｕｓ＿ｒｅａｃｈｅｄ」
ｆ．ＡＲＲ復元ＩＤ（ａｒｒ＿ｓｈａｒｅ＿ｂａｃｋ＿ｉｄ）
ｇ．ＡＲＫによって暗号化されたＡＲＢ（ａｒｂ＿ａｒｋ）
ｈ，一時的鍵暗号化鍵（ＫＥＫ）導出ソルト（ｅｐｈｅｍｅｒａｌ＿ｋｅｋ＿ｄｅｒｉｖａｔｉｏｎ＿ｓａｌｔ）
ｉ．一時的公開鍵（ｅｐｈｅｍｅｒａｌ＿ｐｕｂｌｉｃ＿ｋｅｙ）
ｊ．暗号化された一時的鍵ペア｛ｅｎｃｒｙｐｔｅｄ＿ｅｐｈｅｍｅｒａｌ＿ｋｅｙｐａｉｒ｝
ｋ．暗号化されたＯＣＣ（ｅｎｃｒｙｐｔｅｄ＿ｏｃｃ）
ｌ．ＡＲＰＴＦリスト（ａｒｐｔｆ＿ｌｉｓｔ）（ＪＳＯＮアレイ）
１．ニックネーム
２．ａｒｋ＿ｐｘ＿ｅｐｈ＿ｐｕｂ＿ｋｅｙ（参加したＡＲＰＴＦの場合、ヌルではない）
３．ｈｍａｃ＿ｏｃｃ＿ａｒｋ＿ｐｘ

【００６３】

６０８において、第１パスワードアプリケーション２１２ａは、現在のＡＲＲステータスが「コンセンサス達成」であるという通知をユーザＡに送信する。６１０において、ユーザＡは、アカウント復元に進む。６１２において、第１パスワードアプリケーション２１２ａは、仮マスターパスワードおよびランダムに生成されたソルトを使用して、一時的鍵暗号化鍵（ＥｐｈＫＥＫ）を導出する。６１４において、第１パスワードアプリケーション２１２ａは、一時的鍵ペア（ＥｐｈＫｅｙＰａｉｒ）をラップ解除して、一時的ＲＳＡ秘密鍵（ＥｐｈＰｒｉｖＫｅｙ）へのアクセスを提供する。６１６において、第１パスワードアプリケーション２１２ａは、暗号化されたＯＣＣをラップ解除する。第１パスワードアプリケーション２１２ａは次に、各ＡＲＫ－Ｐｘについて繰り返されるループ６２０に入る。６２２において、第１パスワードアプリケーション２１２ａは、暗号化された各ＡＲＫ－Ｐｘを、一時的ＲＳＡ秘密鍵（ＥｐｈＰｒｉｖＫｅｙ）で復号する。６２４において、第１パスワードアプリケーション２１２ａは、鍵付ハッシュ関数メッセージ認証コード｛ＨＭＡＣ（ＯＣＣ，ＡＲＫ－Ｐｘ）｝を計算する。６２６において、第１パスワードアプリケーション２１２ａは、鍵付ハッシュ関数メッセージ認証コード（ＨＭＡＣ）と、アウトオブバンド確認コードを鍵として使用したＡＲＫ－ＰｘのＨＭＡＣ（ｈｍａｃ＿ｏｃｃ＿ａｒｋ＿ｐｘ）とを比較して、的確なＡＲＫ－Ｐｘが復元されたことを示す、ＨＭＡＣ（ＯＣＣ，ＡＲＫ－Ｐｘ）＝＝ｈｍａｃ＿ｏｃｃ＿ａｒｋ＿ｐｘという条件が満たされているかどうか判定する。６２２～６２６のループは、ＡＲＰＴＦから受信した各ＡＲＫ－Ｐｘが復元および検証されるまで、各ＡＲＫ－Ｐｘについて実行される。

【００６４】

６３０において、第１パスワードアプリケーション２１２ａは、ＳＳＳを使用して、復号されたＡＲＫ－Ｐｘの全てを統合し、アカウント復元鍵で暗号化されたアカウント復元バンドル（ＡＲＢ）（ＡＲＢ＿ＡＲＫ）を復元する。６３２において、第１パスワードアプリケーション２１２ａは、アカウント復元バンドル（ＡＲＢ）を復元するべく、ＡＲＢ＿ＡＲＫを復号する。６３４において、第１パスワードアプリケーション２１２ａは、ＡＲＢから、認証トークンワンタイムパスワード（ＡＵＴＨ－ＴＯＫ－ＯＴＰ）およびコンテンツ暗号化鍵（ＣＥＫ）を抽出する。

【００６５】

６３６において、第１パスワードアプリケーション２１２ａは、新しいＫＥＫ導出ソルトを生成する。６３８において、第１パスワードアプリケーション２１２ａは、新しいソルトおよび仮マスターパスワードで、更新されたＫＥＫを導出する。６４０において、第１パスワードアプリケーション２１２ａは、抽出されたＣＥＫを更新されたＫＥＫでラップする。

【００６６】

６４２において、第１パスワードアプリケーション２１２ａは、認証されたアカウント復元要求メッセージを認証サーバ２０６のパスワードＲＥＳＴ　ＡＰＩ２１４に送信する。認証されたアカウント復元要求メッセージは、要求の完了時に検証されるＡＵＴＨ－ＴＯＫ－ＯＴＰと、この要求の仮認証トークンと照合されるｐｒｏｖｉｓｉｏｎａｌ＿ａｕｔｈ＿ｔｏｋｅｎと、新しいＫＥＫのための最新ソルト（ｕｐｄａｔｅｄ＿ｋｅｋ＿ｄｅｒｉｖａｔｉｏｎ＿ｓａｌｔ）と、更新されたコンテンツ暗号化鍵の鍵暗号化鍵（ｕｐｄａｔｅｄ＿ｃｅｋ＿ｋｅｋ）とを含む。特定の実施形態において、要求メッセージは、ＡＵＴＨ－ＴＯＫ－ＯＴＰ、ｐｒｏｖｉｓｉｏｎａｌ＿ａｕｔｈ＿ｔｏｋｅｎ、ｕｐｄａｔｅｄ＿ｋｅｋ＿ｄｅｒｉｖａｔｉｏｎ＿ｓａｌｔ（新しいＫＥＫのための最新のソルト）、および、ｕｐｄａｔｅｄ＿ｃｅｋ＿ｋｅｋを含むＪＳＯＮリクエストボディを有する、ＰＵＴ／ａｃｃｏｕｎｔ＿ｒｅｃｏｖｅｒｙ／｛ａｒｒ＿ｉｄ｝／という形式のＰＵＴメッセージである。６４４において、パスワードＲＥＳＴ　ＡＰＩ２１４は、アカウント復元要求が完了したという確認を第１パスワードアプリケーション２１２ａに送信する。特定の実施形態において、確認メッセージは、ＨＴＴＰ２００メッセージである。６４６において、第１パスワードアプリケーション２１２ａは、アカウント復元要求が完了したという確認をユーザＡに提供する。６４８において、ユーザＡは、アカウントへのアクセスを取り戻すべく、マスターパスワードに昇格された仮マスターパスワードを使用して、第１パスワードアプリケーション２１２ａにログインできる。これでフロー６００は終了する。

【００６７】

これより図７を参照する。図７は、クライアントデバイス２０２ａの実施形態の簡略化されたブロック図である。クライアントデバイス２０２ａは、プロセッサ７０２、メモリ要素７０４、グラフィカルユーザインタフェース７０６、および、パスワードアプリケーション２１２ａを含む。プロセッサ７０２は、本明細書に記載されているような、クライアントデバイス２０２ａの様々な操作を実行するためのソフトウェア命令を実行するように構成されている。メモリ要素７０４は、クライアントデバイス２０２ａに関連するソフトウェア命令およびデータを保存するように構成され得る。プロセッサ７０２は、マイクロプロセッサ、組み込みプロセッサ、デジタル信号プロセッサ（ＤＳＰ）、ネットワークプロセッサ、または、コードを実行するための他のデバイスなど、任意の種類のプロセッサであり得る。図７には、１つのプロセッサ７０２だけが示されているが、いくつかの実施形態において、クライアントデバイス２０２ａは、１つより多くのプロセッサを含み得ることを理解されたい。

【００６８】

グラフィカルユーザインタフェース７０６は、本明細書に記載されているような、パスワードのセットアップおよび復元の手順を容易にするべく、クライアントデバイス２０２ａのユーザにグラフィカルユーザインタフェースを提供するように構成されている。パスワードアプリケーション２１２ａは、本明細書に記載されているクライアントデバイス２０２ａに関連する、パスワードのセットアップおよび復元の機能を実行するように構成されている。

【００６９】

これより図８を参照する。図８は、認証サーバ２０６の実施形態の簡略化されたブロック図である。認証サーバ２０６は、プロセッサ８０２、メモリ要素８０４、認証コンポーネント１０２、および、パスワードＲＥＳＴ　ＡＰＩ２１４を含む。プロセッサ８０２は、本明細書に記載されているような、認証サーバ２０６の様々な操作を実行するためのソフトウェア命令を実行するように構成されている。メモリ要素８０４は、認証サーバ２０６に関連するソフトウェア命令およびデータを保存するように構成され得る。プロセッサ８０２は、マイクロプロセッサ、組み込みプロセッサ、デジタル信号プロセッサ（ＤＳＰ）、ネットワークプロセッサ、または、コードを実行するための他のデバイスなど、任意の種類のプロセッサであり得る。図８には、１つのプロセッサ６０２だけが示されているが、いくつかの実施形態において、認証サーバ２０６は、１つより多くのプロセッサを含

み得ることを理解されたい。

【００７０】

認証コンポーネント１０２は、本明細書に記載されているような、認証サーバ２０６の認証およびパスワード復元の機能を容易にするように構成されている。パスワードＲＥＳＴ　ＡＰＩ２１４は、本明細書に記載されているような、パスワードＲＥＳＴ　ＡＰＩ２１４のパスワードのセットアップおよび復元の機能を容易にするように構成されている。

【００７１】

１つまたは複数の実施形態は、既存のソリューションと比較して、（１）ユーザの認証、および、後に復元されるユーザデータの暗号化に、同一のパスワードが使用されること、（２）マスターパスワードの（暗号化されている、またはクリアテキストの）コピーを保持しないこと、（３）ユーザのマスターパスワードのデータベースを保持しないこと、（４）復元プロセスにおけるアカウント所持者の初期検証中、電子メールによる確認、ＢＯＴアクティビティなどを排除するためのＣＡＰＴＣＨＡ検証など、従来の検証方法を利用し得るが、ユーザの身元を検証する他の従来の方法（例えば、単純な秘密の質問を尋ねる）を利用せず、その結果、この初期検証に基づいて、パスワードを容易に再設定することが可能であること、（５）セキュリティ上の理由から、マスターパスワード自体の具体的な情報を自身で有していないことのうち、１つまたは複数の利点を提供し得る。従来と異なり、マスターパスワード復元鍵の情報の断片を、暗号化されたトークンの形式で分散させ、複数の信頼済エンティティの間で供託する。信頼済エンティティのいずれも、トークンの内容の具体的な情報を持たない。トークンは必要なときに呼び出されて組み合わされ、失念しやすいユーザが失敗した状態から復元するように手助けし、それにより、これらのリソースへの適切なアクセスを回復する。したがって、これは単一障害点を生じさせることなく、遥かにセキュアな復元方法を提示する。

【００７２】

従来のシステムは主に、認証の目的のために、システムパスワードを使用する。対称的に、ＡＲＰは、ユーザを認証するための別個の暗号鍵を生成すること、および、ユーザのデータを暗号化することに、同一のパスワードを使用する。従来のシステムは、ユーザが予めセットアップしておいた単純な秘密の質問を使用するか、または、ユーザに関する既知の事実に基づく質問をいくつか尋ねるものであり、ユーザのアカウントに不正侵入するための盗難および再利用に遭う可能性が非常に高い。保存されているパスワードおよびパスワードファイルは、盗難および再利用に遭うことがある。本明細書に記載されているＡＲＰの１つまたは複数の実施形態は、過程における様々な暗号操作を介して、パスワード鍵およびコンテンツの使用および送信に関するセキュリティを強化することにより、パスワード鍵およびコンテンツに対する、多くの同様のセキュリティ上の脅威を排除する。また、これらの実施形態は、単純に１つのアクセストークンを他のアクセストークンに置き換えるのではなく、結果としてユーザの資産を再暗号化するという革新的な手段で復元を実行する。

【００７３】

本明細書に記載されている１つまたは複数の実施形態は、パスワードマネージャおよびマスターパスワードの使用に関するが、本明細書に記載されている原理は、例えばファイル共有サービス上のファイル、暗号化されたバックアップなど、保存／暗号化された任意の種類のユーザの資産に対するアクセスの復元などのための、パスワードに基づく他のユーザデータ暗号化システムおよび／またはアプリケーションに適用可能であることを理解されたい。

【００７４】

［実施形態の例］

【００７５】

以下の例は、更なる実施形態に関する。

【００７６】

例１は、ユーザに関連するアカウントの復元のための要求を受信するコンピュータコー

ドと、ユーザに関連するユーザデバイスへＣＡＰＴＣＨＡチャレンジを送信するためのコンピュータコードと、ＣＡＰＴＣＨＡチャレンジへの回答、および、仮マスターパスワードから導出された暗号化鍵によってラップされた確認コードを受信するためのコンピュータコードと、復元のための要求の通知をユーザに関連する１つまたは複数の信頼済エンティティへ送信するためのコンピュータコードと、信頼済エンティティのうち１つまたは複数からの要求の確認（この確認は、特定の信頼済エンティティおよび暗号化された確認コードに関連する復元トークンを含む）を受信するためのコンピュータコードとを含むコンピュータコードを保存するための、少なくとも１つの不揮発性コンピュータ記憶媒体である。

【００７７】

例２において、例１の主題は、１つまたは複数の信頼済エンティティから所定の数の復元トークンを受信したことに応答して、コンセンサス状態を達成したと判定するコンピュータコードと、１つまたは複数の信頼済エンティティの各々に関連する復元トークンをユーザデバイスへ送信するコンピュータコードとを任意で含み得る。

【００７８】

例３において、例２の主題は、コンセンサス状態の通知をユーザデバイスへ送信するコンピュータコードを任意で含み得る。

【００７９】

例４において、例２の主題は、コンセンサス状態が達成されたと判定したことに応答して、アカウントのための新しいマスターパスワードを再設定するコンピュータコードを任意で含み得る。

【００８０】

例５において、例４の主題は、受信された復元トークンを使用して、新しいマスターパスワードが再設定されることを任意で含み得る。

【００８１】

例６において、例５の主題は、一時的秘密鍵を使用して、受信された復元トークンが復号されることを任意で含み得る。暗号化確認コードは、復元トークンの検証として使用され得る。

【００８２】

例７において、例６の主題は、復号された復元トークンを組み合わせることに基づいて、新しいマスターパスワードが再設定されることを任意で含み得る。

【００８３】

例８において、例４の主題は、新しいマスターパスワードがユーザデバイスによって生成されることを任意で含み得る。

【００８４】

例９において、例１－８のいずれの主題も、１つまたは複数の信頼済エンティティの指定をユーザから受信するためのコンピュータコードを任意で含み得る。

【００８５】

例１０は、少なくとも１つのプロセッサおよび少なくとも１つのメモリ要素を備えるシステムであり、当該システムは、ユーザに関連するアカウントの復元のための要求を受信すること、ユーザに関連するユーザデバイスへＣＡＰＴＣＨＡチャレンジを送信すること、ＣＡＰＴＣＨＡチャレンジ対する回答、および、仮マスターパスワードから導出された暗号化鍵によってラップされた確認コードを受信すること、ユーザに関連する１つまたは複数の信頼済エンティティへ復元のための要求の通知を送信すること、ならびに、１つまたは複数の信頼済エンティティから要求の確認を受信することを行うように構成され、当該確認は、特定の信頼できるエンティティに関連する復元トークンおよび暗号化された確認コードを含む。

【００８６】

例１１において、例１９の主題は、システムが更に、１つまたは複数の信頼済エンティティから、所定の数の復元トークンを受信したことに応答して、コンセンサス状態が達成

されたことを判定すること、および、１つまたは複数の信頼済エンティティの各々に関連する復元トークンをユーザデバイスへ送信することを行うように構成されていることを任意で含み得る。

【００８７】

例１２において、例１１の主題は、システムが更に、コンセンサス状態の通知をユーザデバイスへ送信するように構成されていることを任意で含み得る。

【００８８】

例１３において、例１２の主題は、システムが更に、コンセンサス状態が達成されたという判定に応答して、アカウントのための新しいマスターパスワードを生成するように構成されていることを任意で含み得る。

【００８９】

例１４において、例１３の主題は、新しいマスターパスワードが、受信された復元トークンを使用して再設定されることを任意で含み得る。

【００９０】

例１５において、例１４の主題は、受信された復元トークンが、一時的秘密鍵を使用して復号されること、および、暗号化された確認コードが、復元トークンの検証に使用されることを任意で含み得る。

【００９１】

例１６において、例１３の主題は、新しいマスターパスワードがユーザデバイスによって生成されることを任意で含み得る。

【００９２】

例１７において、例１０－１６のいずれかの主題は、システムが更に、１つまたは複数の信頼済エンティティの指定をユーザから受信するように構成されていることを任意で含み得る。

【００９３】

例１８は、コンピュータ実装方法でありユーザに関連するアカウントの復元のための要求を受信すること、ユーザに関連するユーザデバイスへＣＡＰＴＣＨＡチャレンジを送信すること、ＣＡＰＴＣＨＡチャレンジへの回答、および、仮マスターパスワードから導出された暗号化鍵によってラップされた確認コードを受信すること、ユーザに関連する１つまたは複数の信頼済エンティティへ復元のための要求の通知を送信すること、ならびに、１つまたは複数の信頼済エンティティから要求の確認を受信することを含み、当該確認は、特定の信頼済エンティティに関連する復元トークンおよび暗号化された確認コードを含む。

【００９４】

例１９において、例１８の主題は、所定の数の復元トークンを１つまたは複数の信頼済エンティティから受信したことに応答して、コンセンサス状態が達成されたことを判定すること、ならびに、１つまたは複数の信頼済エンティティの各々に関連する復元トークンをユーザデバイスへ送信することを任意で含み得る。

【００９５】

例２０において、例１９の主題は、コンセンサス状態の通知をユーザデバイスへ送信することを任意で含み得る。

【００９６】

例２１において、例１９の主題は、コンセンサス状態が達成されたことの判定に応答して、アカウントのための新しいマスターパスワードを再設定することを任意で含み得る。

【００９７】

例２２において、例２１の主題は、新しいマスターパスワードが、受信された復元トークンを使用して再設定されることを任意で含み得る。

【００９８】

例２３において、例２２の主題は、受信された復元トークンが、一時的秘密鍵を使用して復号されること、および、暗号化された確認コードが復元トークンの検証に使用される

ことを任意で含む。

【００９９】

例２４において、例２３の主題は、新しいマスターパスワードがユーザデバイスによって生成されることを任意で含み得る。

【０１００】

例２５において、例１８－２４のいずれかの主題は、システムが更に、１つまたは複数の信頼済エンティティの指定をユーザから受信するように構成されていることを任意で含み得る。

【０１０１】

例２６は、アカウント復元のための装置であり、ユーザに関連するアカウントの復元のための要求を受信する手段と、ユーザに関連するユーザデバイスへＣＡＰＴＣＨＡチャレンジを送信する手段と、ＣＡＰＴＣＨＡチャレンジへの回答、および、仮マスターパスワードから導出された暗号化鍵によってラップされた確認コードを受信するための手段と、ユーザに関連する１つまたは複数の信頼済エンティティへ復元のための要求の通知を送信するための手段と、１つまたは複数の信頼済エンティティから要求の確認を受信するための手段とを含み、当該確認は、特定の信頼済エンティティに関連する復元トークン、および、暗号化された確認コードを含む。

【０１０２】

例２７において、例２６の主題は、所定の数の復元トークンを１つまたは複数の信頼済エンティティから受信したことに応答して、コンセンサス状態が達成されたことを判定する手段と、１つまたは複数の信頼済エンティティの各々に関連する復元トークンをユーザデバイスへ送信する手段とを任意で含み得る。

【０１０３】

例２８において、例２７の主題は、コンセンサス状態が達成されたという判定に応答して、アカウントのための新しいマスターパスワードを生成する手段を任意で含み得る。

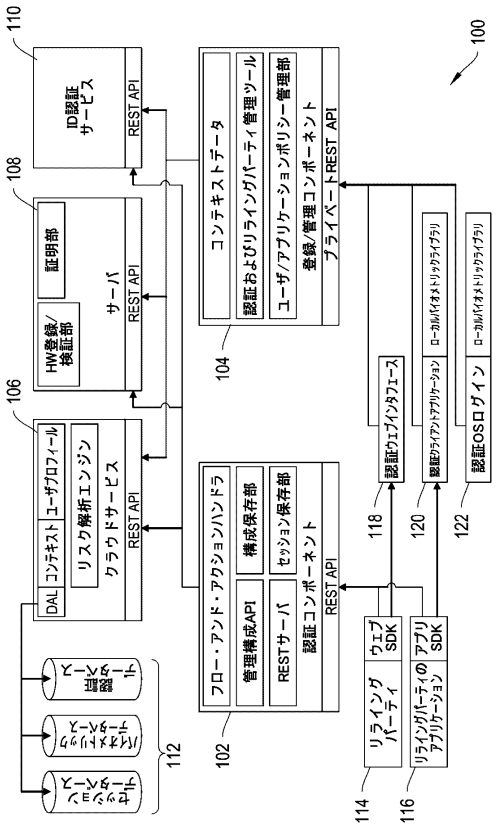
【０１０４】

例２９は、上述のいずれかの例において主張されている方法を実行する手段を含む装置である。

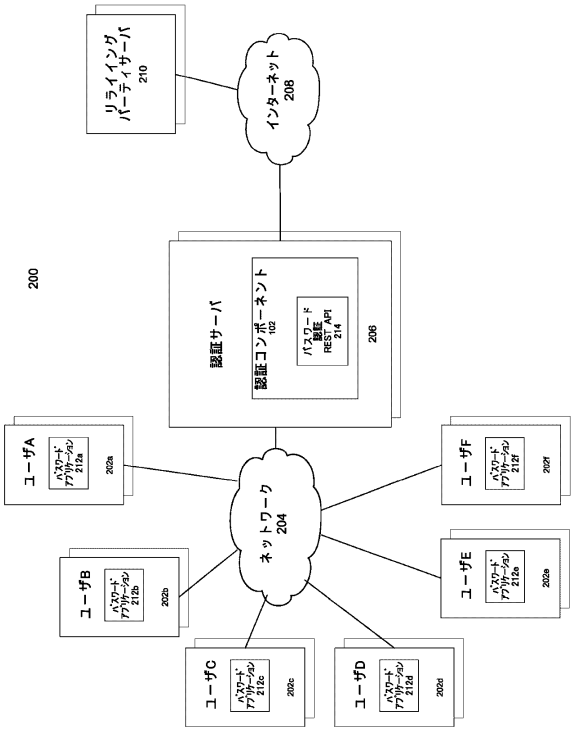
【０１０５】

例３０は、実行されたときに、上述の例のいずれかに記載されている方法を実装するか、装置を実現する機械可読命令を含む機械可読ストレージである。

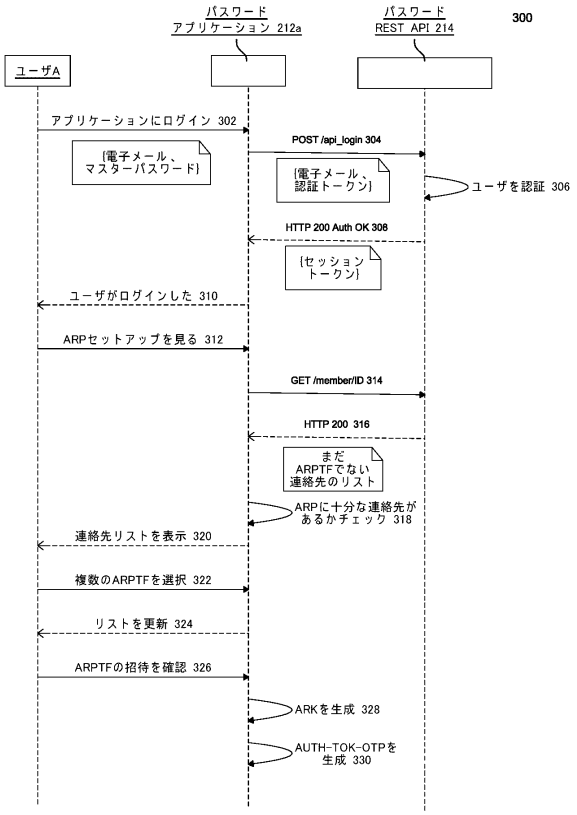
【図１】


100
110
ID認証サービス
REST API
108
サーバ
証明部
HW登録/検証部
REST API
106
クラウドサービス
ユーザプロフィール
コンテキスト
リスク解析エンジン
DAL
REST API
112
104
コンテキストデータ
認証およびリライングパーティ管理ツール
ユーザ/アプリケーションポリシー管理部
登録/管理コンポーネント
プライベート REST API
102
フロー・アンド・アクションハンドラ
管理構成API
構成保存部
RESTサーバ
セッション保存部
認証コンポーネント
REST API
118
認証ウェブインタフェース
120
認証クライアントアプリケーション
ローカルバイオメトリックライブラリ
122
認証OSログイン
ローカルバイオメトリックライブラリ
114
ウェブ SDK
リライング パーティ
116
アプリ SDK
リライングパーティのアプリケーション

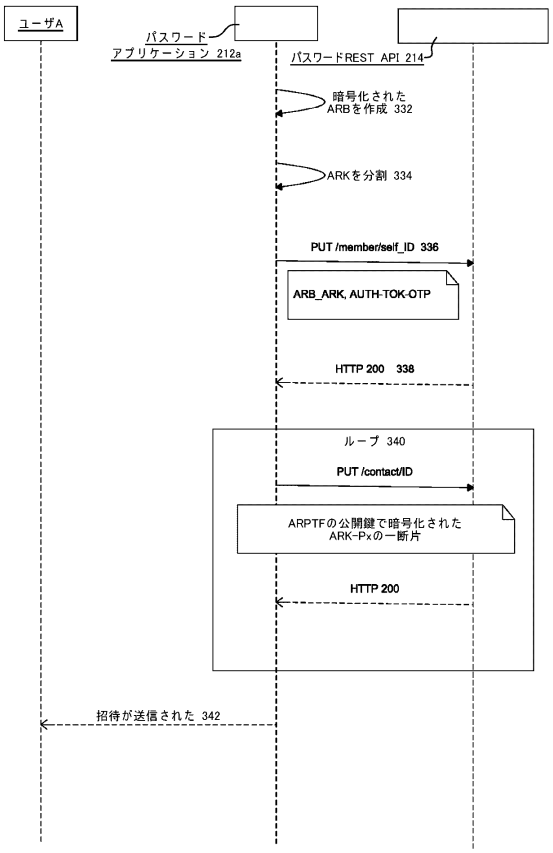
【図２】


リライイング パーティサーバ 210
インターネット 208
200
認証サーバ
認証コンポーネント 102
パスワード 認証 REST API 214
206
ユーザA
パスワード アプリケーション 212a
202a
ユーザB
パスワード アプリケーション 212b
202b
ユーザC
パスワード アプリケーション 212c
202c
ユーザD
パスワード アプリケーション 212d
202d
ユーザE
パスワード アプリケーション 212e
202e
ユーザF
パスワード アプリケーション 212f
202f
ネットワーク 204

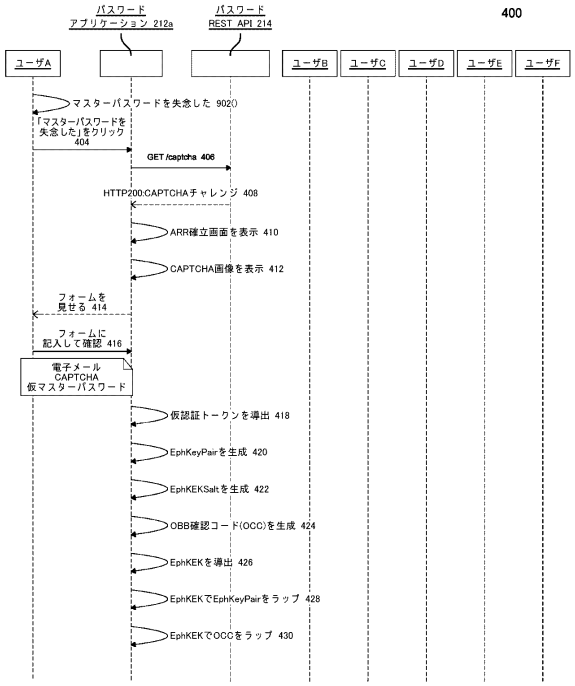
【図３Ａ】


300
パスワード アプリケーション 212a
パスワード REST API 214
ユーザA
アプリケーションにログイン 302
{電子メール、マスターパスワード}
POST /api_login 304
{電子メール、認証トークン}
ユーザを認証 306
HTTP 200 Auth OK 308
{セッション トークン}
ユーザがログインした 310
ARPセットアップを見る 312
GET /member/ID 314
HTTP 200 316
まだ ARPTFでない 連絡先のリスト
ARPに十分な連絡先があるかチェック 318
連絡先リストを表示 320
複数のARPTFを選択 322
リストを更新 324
ARPTFの招待を確認 326
ARKを生成 328
AUTH-TOK-OTPを生成 330

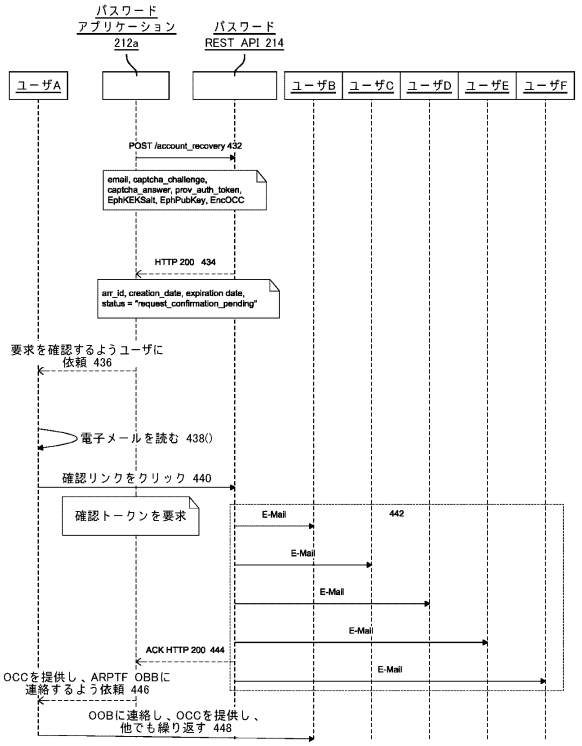
【図３Ｂ】


ユーザA
パスワード アプリケーション 212a
パスワードREST API 214
暗号化された ARBを作成 332
ARKを分割 334
PUT /member/self_ID 336
ARB_ARK, AUTH-TOK-OTP
HTTP 200 338
ループ 340
PUT /contact/ID
ARPTFの公開鍵で暗号化された ARK-Pxの一断片
HTTP 200
招待が送信された 342

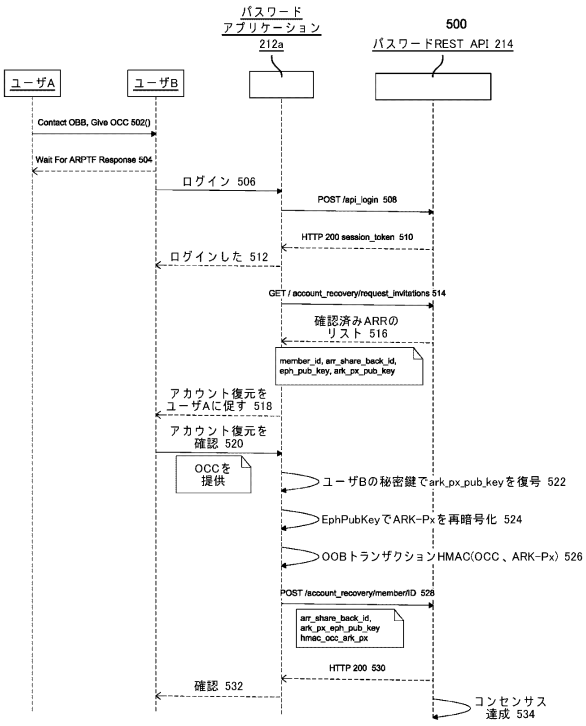
【図４Ａ】



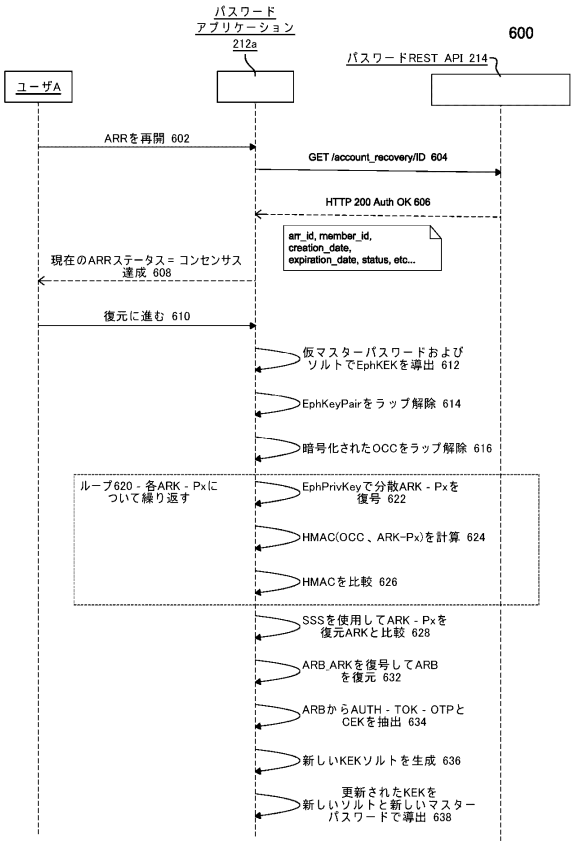
【図４Ｂ】



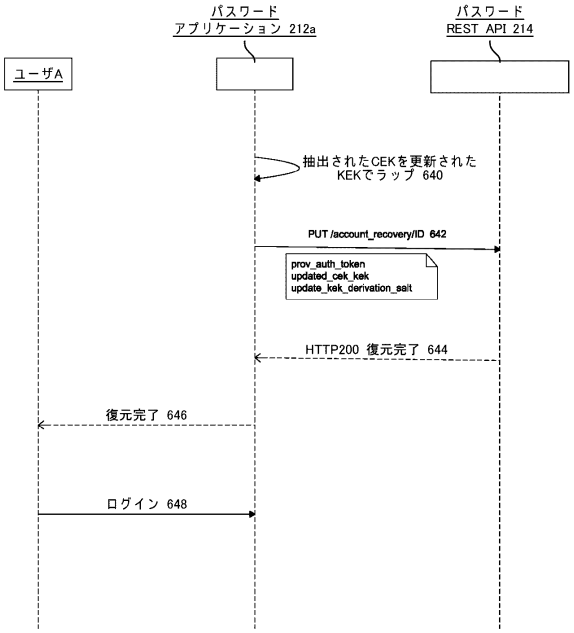
【図５】



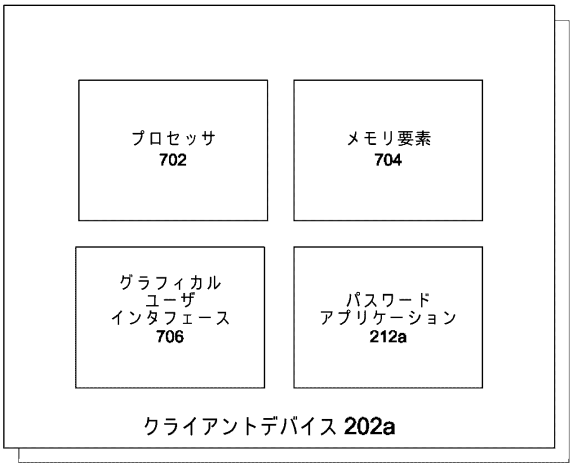
【図６Ａ】



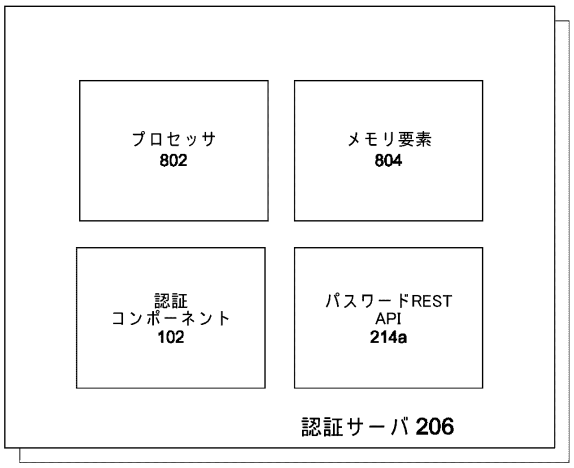
【図６Ｂ】


パスワード
アプリケーション 212a
パスワード
REST API 214
ユーザA
抽出されたCEKを更新された
KEKでラップ 640
PUT /account_recovery/ID 642
prov_auth_token
updated_cek_kek
update_kek_derivation_salt
HTTP200 復元完了 644
復元完了 646
ログイン 648

【図７】


プロセッサ
702
メモリ要素
704
グラフィカル
ユーザ
インタフェース
706
パスワード
アプリケーション
212a
クライアントデバイス 202a

【図８】


プロセッサ
802
メモリ要素
804
認証
コンポーネント
102
パスワードREST
API
214a
認証サーバ 206

フロントページの続き

(72)発明者　レイナー、リチャード
カナダ国、エル５アール　４ビー１　オンタリオ州、ミシサガ　スウィート　２１８、キングスブリッジ　ガーデン　サークル　２５
(72)発明者　ホワイトサイド、グレゴリー
カナダ国、エイチ３アール　３ビー３　ケベック州、モントリオール　リュ　メナール　７３４５

審査官　和平　悠希

(56)参考文献　特開平１０－１２６４０４（ＪＰ，Ａ）
特開２００５－１００２５５（ＪＰ，Ａ）
特表２０１３－５４１９０８（ＪＰ，Ａ）
米国特許出願公開第２０１２／０１７４２０３（ＵＳ，Ａ１）
米国特許出願公開第２０１３／０１９８８２４（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４５
Ｈ０４Ｌ　９／０８