

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6906521号
(P6906521)

(45) 発行日 令和3年7月21日 (2021.7.21)

(24) 登録日 令和3年7月1日 (2021.7.1)

(51) Int. Cl.	F I
H04L 9/32 (2006.01)	H04L 9/00 675A
G06F 21/32 (2013.01)	H04L 9/00 673D
	G06F 21/32

請求項の数 19 (全 43 頁)

(21) 出願番号	特願2018-528936 (P2018-528936)	(73) 特許権者	516373948
(86) (22) 出願日	平成28年8月22日 (2016.8.22)		ヴェリディウム アイビー リミテッド
(65) 公表番号	特表2018-529299 (P2018-529299A)		イギリス国 イーシー4 ヴィ 6 ジェイエ
(43) 公表日	平成30年10月4日 (2018.10.4)		イ ロンドン、ニュー ブリッジ ストリ
(86) 国際出願番号	PCT/US2016/048068		ート 100
(87) 国際公開番号	W02017/035085	(74) 代理人	100092783
(87) 国際公開日	平成29年3月2日 (2017.3.2)		弁理士 小林 浩
審査請求日	令和1年8月13日 (2019.8.13)	(74) 代理人	100120134
(31) 優先権主張番号	62/241,392		弁理士 大森 規雄
(32) 優先日	平成27年10月14日 (2015.10.14)	(74) 代理人	100103182
(33) 優先権主張国・地域又は機関			弁理士 日野 真美
	米国 (US)	(74) 代理人	100126354
(31) 優先権主張番号	62/208,328		弁理士 藤田 尚
(32) 優先日	平成27年8月21日 (2015.8.21)	(74) 代理人	100104282
(33) 優先権主張国・地域又は機関			弁理士 鈴木 康仁
	米国 (US)		最終頁に続く

(54) 【発明の名称】 生体認証プロトコル標準のシステムおよび方法

(57) 【特許請求の範囲】

【請求項 1】

ユーザコンピューティング装置とサーバコンピューティング装置との間にセキュアな通信を提供するための方法であって、

分散クライアントソフトウェアアプリケーションに応じて、複数のユーザコンピューティング装置の各々を、

各それぞれのコンピューティング装置のそれぞれのユーザに関連付けられた初期生体認証ベクトル（「IBV」）を獲得し、

前記 IBV に対して暗号分割動作を行い、少なくとも前記 IBV の暗号化済み第1の部分および前記 IBV の暗号化済み第2の部分を生成し、

前記 IBV の前記暗号化済み第1の部分を含むエンロールメントリクエストを生成し、

前記コンピューティング装置に前記 IBV の前記暗号化済み第2の部分を保存し、

前記 IBV の前記暗号化済み第2の部分を含む認証リクエストを生成するように構成するステップと、

前記サーバコンピューティング装置によって、前記ユーザコンピューティング装置の1つから前記ユーザコンピューティング装置の前記1つのユーザに関連付けられた IBV の第1の部分を含むエンロールメントリクエストを受信するステップと、

前記サーバコンピューティング装置によってネットワークにおいて前記ユーザコンピューティング装置の前記1つをエンロールするステップであって、前記サーバコンピューテ

10

20

ィング装置によってアクセス可能である、または該サーバコンピューティング装置の一部である非一時的なプロセッサ可読媒体に、前記ユーザコンピューティング装置の前記1つの前記ユーザに関連付けられた前記 I B V の前記暗号化済み第1の部分を記憶することを含む、ステップと、

続いて、前記ユーザコンピューティング装置の前記1つから、i) 前記ユーザコンピューティング装置のユーザに関連付けられた前記 I B V の暗号化済み第2の部分、および i i) 前記ユーザコンピューティング装置の前記1つのユーザに関連付けられた新たにキャプチャされた現在の生体認証ベクトル (「C B V」) を含む認証リクエストを、前記サーバコンピューティング装置によって受信するステップと、

前記サーバコンピューティング装置によって、前記受信された前記 I B V の暗号化済み第1の部分を前記受信された前記 I B V の暗号化済み第2の部分と結合するステップと、

前記サーバコンピューティング装置によって、前記結合された I B V を解読するステップと、

前記サーバコンピューティング装置によって、前記結合された I B V と前記 C B V とが同様である度合 (degree) を表す値を決定するステップと、

前記サーバコンピューティング装置によって前記ユーザコンピューティング装置の前記1つを前記値が最小閾値を上回る場合に、認証するステップとを含む、方法。

【請求項2】

前記エンロールメントリクエストおよび前記認証リクエストに含まれる証明書を、前記サーバコンピューティング装置によって前記ユーザコンピューティング装置の前記1つに提供するステップであって、前記サーバコンピューティング装置が、前記認証リクエストを前記処理し、前記証明書が現行のものであり取り消されていないかを判断することを含む、ステップをさらに含む、請求項1に記載の方法。

【請求項3】

アクティブな監視を行い、かつ前記証明書のスプーフィングを防止する侵入検出システムを利用することをさらに含む、請求項2に記載の方法。

【請求項4】

防止される前記スプーフィングは前記証明書のリプレイを含む、請求項3に記載の方法。

【請求項5】

前記サーバコンピューティング装置によって、一方向暗号化に応じて暗号化済み空間において少なくとも1回の照合動作を行うことをさらに含む、請求項1に記載の方法。

【請求項6】

前記一方向暗号化はランダムなワンタイムパッドを使用して行われる、請求項5に記載の方法。

【請求項7】

デジタルアセットへのアクセスのために1つまたは複数のルールによって定義されるロール収集を前記サーバコンピューティング装置によって提供することと、

前記サーバコンピューティング装置によって、前記ロール収集に応じて前記ユーザコンピューティング装置によって前記デジタルアセットへのアクセスを提供するまたは拒否することとをさらに含む、請求項1に記載の方法。

【請求項8】

前記アクセスは、任意アクセス制御および強制アクセス制御のうちの少なくとも1つに応じて提供される、請求項7に記載の方法。

【請求項9】

前記サーバコンピューティング装置によって、前記ユーザコンピューティング装置の前記1つから受信される第2のエンロールメントリクエストを処理することであって、前記第2のエンロールメントリクエストは、前記ユーザコンピューティング装置の前記1つの第2のユーザをエンロールするために使用可能であり、前記第2のエンロールメントリクエストは、前記ユーザコンピューティング装置の前記1つのユーザに関連付けられた第2

10

20

30

40

50

の暗号化済み部分初期生体認証ベクトル（「IBV」）を含み、前記第2のエンロールメントリクエストを前記処理することは、前記サーバコンピューティング装置によってアクセス可能である、または該サーバコンピューティング装置の一部である非一時的なプロセッサ可読媒体に前記第2の暗号化済み部分IBVを記憶することを含む、処理することをさらに含む、請求項1に記載の方法。

【請求項10】

前記サーバコンピューティング装置によって、前記ユーザコンピューティング装置に関連付けられた前記第1のユーザの前記エンロールメントを取り消すことをさらに含む、請求項9に記載の方法。

【請求項11】

ユーザコンピューティング装置と信頼されるサーバとの間にセキュアな通信を提供するためのシステムであって、

1つまたは複数の非一時的なプロセッサ可読媒体に動作可能に連結される少なくとも1つのプロセッサを備え、

前記1つまたは複数の非一時的なプロセッサ可読媒体は、前記少なくとも1つのプロセッサが、

分散クライアントソフトウェアアプリケーションに応じて、複数のユーザコンピューティング装置の各々を、

各それぞれのコンピューティング装置のそれぞれのユーザに関連付けられた初期生体認証ベクトル（「IBV」）を獲得し、

前記IBV上で暗号分割動作を行い、前記IBVの少なくとも暗号化済み第1の部分および前記IBVの暗号化済み第2の部分を生成し、

前記暗号化済み第1の部分を含むエンロールメントリクエストを生成し、

前記コンピューティング装置に前記IBVの前記暗号化済み第2の部分を保存し、

前記IBVの前記暗号化済み第2の部分を含む認証リクエストを生成するように構成し、

分散クライアントソフトウェアアプリケーションで構成される前記ユーザコンピューティング装置の1つから受信されるエンロールメントリクエストを受信することであって、前記エンロールメントリクエストは、前記ユーザコンピューティング装置の前記1つのユーザに関連付けられたIBVの第1の部分を含む、受信することと、

前記サーバコンピューティング装置によって、前記ユーザコンピューティング装置の前記1つをエンロールすることであって、前記サーバコンピューティング装置によってアクセス可能である、または該サーバコンピューティング装置の一部である非一時的なプロセッサ可読媒体に前記ユーザコンピューティング装置の前記1つのユーザに関連付けられた前記IBVの前記暗号化済み第1の部分を記憶することを含む、エンロールすることと、

続いて、i) 前記ユーザコンピューティング装置のユーザに関連付けられた前記IBVの暗号化済み第2の部分、およびii) 前記ユーザコンピューティング装置の前記1つのユーザに関連付けられた新たにキャプチャされた現行の生体認証ベクトル（「CBV」）を含む認証リクエストを前記ユーザコンピューティング装置の前記1つから受信することと、

前記IBVの前記受信された暗号化済み第1の部分を前記IBVの前記受信された暗号化済み第2の部分と結合することと、

前記サーバコンピューティング装置によって、前記結合されたIBVを解読することと、

前記サーバコンピューティング装置によって、前記結合されたIBVと前記CBVとが同様である度合を表す値を決定することと、

前記ユーザコンピューティング装置の前記1つを、前記ユーザコンピューティング装置は前記値が最小閾値を上回る場合に認証することとを可能にするための命令を含む、システム。

【請求項12】

前記1つまたは複数の非一時的なプロセッサ可読媒体は、前記少なくとも1つのプロセッサが、前記エンロールメントリクエストおよび前記認証リクエストに含まれる証明書を、前記ユーザコンピューティング装置の前記1つに提供し、前記少なくとも1つのプロセッサが前記認証リクエストを前記処理し、前記証明書が現行のものであり取り消されていないかを判断することを可能にするための命令をさらに含む、請求項11に記載のシステム。

【請求項13】

前記1つまたは複数の非一時的なプロセッサ可読媒体は、前記少なくとも1つのプロセッサが、アクティブな監視を行い、かつ前記証明書の代替のもののスプーフィングを防止する侵入検出システムを利用することを可能にするための命令をさらに含む、請求項11

10

【請求項14】

防止される前記スプーフィングは前記証明書の代替のもののリプレイを含む、請求項13に記載のシステム。

【請求項15】

前記1つまたは複数の非一時的なプロセッサ可読媒体は、前記少なくとも1つのプロセッサが、一方向暗号化に応じて暗号化済み空間において少なくとも1回の照合動作を行うことを可能にするための命令をさらに含む、請求項11に記載のシステム。

【請求項16】

前記一方向暗号化はランダムなワンタイムパッドを使用して行われる、請求項15に記載のシステム。

20

【請求項17】

前記1つまたは複数の非一時的なプロセッサ可読媒体は、前記少なくとも1つのプロセッサが、

デジタルアセットへのアクセスのために1つまたは複数のルールによって定義されるロール収集を提供することと、

前記ロール収集に応じて前記ユーザコンピューティング装置によって前記デジタルアセットへのアクセスを提供するまたは拒否することを可能にする命令をさらに含む、請求項11に記載のシステム。

【請求項18】

30

前記アクセスは、任意アクセス制御および強制アクセス制御のうちの少なくとも1つに応じて提供される、請求項17に記載のシステム。

【請求項19】

前記1つまたは複数の非一時的なプロセッサ可読媒体は、前記少なくとも1つのプロセッサが、前記ユーザコンピューティング装置の前記1つから受信される第2のエンロールメントリクエストを処理することであって、前記第2のエンロールメントリクエストは、前記ネットワークにおいて前記ユーザコンピューティング装置の前記1つの第2のユーザをエンロールするために使用可能であり、前記第2のエンロールメントリクエストは、前記ユーザコンピューティング装置の前記1つのユーザに関連付けられた第2の暗号化済み部分初期生体認証ベクトル（「IBV」）を含み、前記第2のエンロールメントリクエストを前記処理することは、前記サーバコンピューティング装置によってアクセス可能である、または該サーバコンピューティング装置の一部である非一時的なプロセッサ可読媒体に前記第2の暗号化済み部分IBVを記憶することを含む、処理することを可能にするための命令をさらに含む、請求項11に記載のシステム。

40

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、一般的に、セキュリティに関し、より詳細には、ユーザを識別するまたは認証するためのシステムおよび方法に関する。

【背景技術】

50

【0002】

あらゆる種類の情報は、データ通信ネットワーク上でアクセス可能な記憶装置などに、リモートに記憶されかつアクセスされ続けている。例えば、多くの人々および会社は、インターネットまたは他の通信ネットワーク上で、財務情報、健康および医療情報、商品およびサービス情報、購買情報、娯楽情報、マルチメディア情報を記憶しかつこれらにアクセスする。情報へのアクセスに加えて、ユーザは金銭の振替（例えば、購買、送金、または販売など）を行うことができる。典型的なシナリオでは、ユーザは情報へアクセスするために登録を行い、その後、ユーザ名およびパスワードを提示して、「ログイン」し、情報にアクセスする。データ／通信ネットワークに記憶されるかかる情報およびデータへ（から）のアクセスをセキュリティ保護することは、依然として最も重要な懸念事項である。

10

【発明の概要】

【課題を解決するための手段】

【0003】

本開示は、以下の〔1〕から〔20〕を含む。

〔1〕 ユーザコンピューティング装置とサーバコンピューティング装置との間にセキュアな通信を提供するための方法であって、

上記サーバコンピューティング装置によって、分散クライアントソフトウェアアプリケーションで構成されるユーザコンピューティング装置から受信されるエンロールメントリクエストを処理することであって、上記エンロールメントリクエストは、ネットワークにおいて上記ユーザコンピューティング装置をエンロールするために使用可能であり、上記リクエストは、上記ユーザコンピューティング装置のユーザに関連付けられた暗号化済み部分初期生体認証ベクトル（「IBV」）を含み、上記エンロールメントリクエストを上記処理することは、上記サーバコンピューティング装置によってアクセス可能である、または該サーバコンピューティング装置の一部である非一時的なプロセッサ可読媒体に上記暗号化済み部分IBVを記憶することを含む、処理することと、

20

上記ユーザコンピューティング装置から後に受信され、暗号化済み部分第2生体認証ベクトルを含み、かつ上記ユーザコンピューティング装置のユーザに関連付けられる認証リクエストを上記サーバコンピューティング装置によって処理することであって、上記認証リクエストを上記処理することは、

30

アルゴリズムに応じて、上記暗号化済み部分初期生体認証ベクトルと上記暗号化済み部分第2生体認証ベクトルとの比較を行うこと、および

上記比較を表す値を生成することを含む、処理することと、

上記比較を表す上記値を、上記サーバコンピューティング装置によって上記ユーザコンピューティング装置に送信することであって、上記ユーザコンピューティング装置は上記値が最小閾値を上回る場合認証され、上記ユーザコンピューティング装置は上記値が最小閾値を下回る場合認証されない、送信することを含む、方法。

〔2〕 上記エンロールメントリクエストおよび上記認証リクエストに含まれる証明書を、上記サーバコンピューティング装置によって上記ユーザコンピューティング装置に提供することであって、上記認証リクエストを上記処理することは、証明書が現行のものであり取り消されていないかを判断することを含む、提供することをさらに含む、上記〔1〕に記載の方法。

40

〔3〕 アクティブな監視を行い、かつ上記証明書のスプーフィングを防止する侵入検出システムを利用することをさらに含む、上記〔2〕に記載の方法。

〔4〕 防止される上記スプーフィングは上記証明書のリプレイを含む、上記〔3〕に記載の方法。

〔5〕 上記認証リクエストを処理することは、一方向暗号化に応じて暗号化済み空間において少なくとも1回の照合動作を行うことをさらに含む、上記〔1〕に記載の方法。

〔6〕 上記一方向暗号化はランダムなワンタイムパッドを使用して行われる、上記〔5〕に記載の方法。

50

〔 7 〕 デジタルアセットへのアクセスのために 1 つまたは複数のルールによって定義されるロール収集を上記サーバコンピューティング装置によって提供することと、

上記サーバコンピューティング装置によって、上記ロール収集に応じて上記ユーザコンピューティング装置によって上記デジタルアセットへのアクセスを提供するまたは拒否することとをさらに含む、上記〔 1 〕に記載の方法。

〔 8 〕 上記アクセスは、任意アクセス制御および強制アクセス制御のうちの少なくとも 1 つに応じて提供される、上記〔 7 〕に記載の方法。

〔 9 〕 上記サーバコンピューティング装置によって、分散クライアントソフトウェアアプリケーションで構成される上記ユーザコンピューティング装置から受信される第 2 のエンロールメントリクエストを処理することであって、上記第 2 のエンロールメントリクエストは、上記ネットワークにおいて上記ユーザコンピューティング装置の第 2 のユーザをエンロールするために使用可能であり、上記第 2 のエンロールメントリクエストは、上記ユーザコンピューティング装置のユーザに関連付けられた第 2 の暗号化済み部分初期生体認証ベクトル（「 I B V 」）を含み、上記第 2 のエンロールメントリクエストを上記処理することは、上記サーバコンピューティング装置によってアクセス可能である、または該サーバコンピューティング装置の一部である非一時的なプロセッサ可読媒体に上記第 2 の暗号化済み部分 I B V を記憶することを含む、処理することをさらに含む、上記〔 1 〕に記載の方法。

〔 1 0 〕 上記サーバコンピューティング装置によって、上記ユーザコンピューティング装置に関連付けられた上記第 1 のユーザの上記エンロールメントを取り消すことをさらに含む、上記〔 9 〕に記載の方法。

〔 1 1 〕 ユーザコンピューティング装置と信頼されるサーバとの間にセキュアな通信を提供するためのシステムであって、

1 つまたは複数の非一時的なプロセッサ可読媒体に動作可能に連結される少なくとも 1 つのプロセッサを備え、

上記 1 つまたは複数の非一時的なプロセッサ可読媒体は、上記少なくとも 1 つのプロセッサが、

分散クライアントソフトウェアアプリケーションで構成されるユーザコンピューティング装置から受信されるエンロールメントリクエストを処理することであって、上記エンロールメントリクエストは、ネットワークにおいて上記ユーザコンピューティング装置をエンロールするために使用可能であり、上記リクエストは、上記ユーザコンピューティング装置のユーザに関連付けられた暗号化済み部分初期生体認証ベクトル（「 I B V 」）を含み、上記エンロールメントリクエストを上記処理することは、上記サーバコンピューティング装置によってアクセス可能である、または該サーバコンピューティング装置の一部である非一時的なプロセッサ可読媒体に上記暗号化済み部分 I B V を記憶することを含む、処理することと、

上記ユーザコンピューティング装置から後に受信され、暗号化済み部分第 2 生体認証ベクトルを含み、かつ上記ユーザコンピューティング装置のユーザに関連付けられる認証リクエストを処理することであって、上記認証リクエストを上記処理することは、

アルゴリズムに応じて、上記暗号化済み部分初期生体認証ベクトルと上記暗号化済み部分第 2 生体認証ベクトルとの比較を行うこと、および

上記比較を表す値を生成することを含む、処理することと、

上記比較を表す上記値を上記ユーザコンピューティング装置に送信することであって、上記ユーザコンピューティング装置は上記値が最小閾値を上回る場合認証され、上記ユーザコンピューティング装置は上記値が最小閾値を下回る場合認証されない、送信することとを可能にするための命令を含む、システム。

〔 1 2 〕 上記 1 つまたは複数の非一時的なプロセッサ可読媒体は、上記少なくとも 1 つのプロセッサが、上記エンロールメントリクエストおよび上記認証リクエストに含まれる証明書を、上記ユーザコンピューティング装置に提供することであって、上記認証リクエストを上記処理することは、上記証明書が現行のものであり取り消されていないかを判断す

10

20

30

40

50

ることを含む、提供することを可能にするための命令をさらに含む、上記〔11〕に記載のシステム。

〔13〕上記1つまたは複数の非一時的なプロセッサ可読媒体は、上記少なくとも1つのプロセッサが、アクティブな監視を行い、かつ上記証明書の代替のもののスプーフィングを防止する侵入検出システムを利用することを可能にするための命令をさらに含む、上記〔11〕に記載のシステム。

〔14〕防止される上記スプーフィングは上記証明書の代替のもののリプレイを含む、上記〔13〕に記載のシステム。

〔15〕上記認証リクエストを処理することは、一方向暗号化に応じて暗号化済み空間において少なくとも1回の照合動作を行うことをさらに含む、上記〔11〕に記載のシステム。

〔16〕上記一方向暗号化はランダムなワンタイムパッドを使用して行われる、上記〔15〕に記載のシステム。

〔17〕上記1つまたは複数の非一時的なプロセッサ可読媒体は、上記少なくとも1つのプロセッサが、

デジタルアセットへのアクセスのために1つまたは複数のルールによって定義されるロール収集を提供することと、

上記ロール収集に応じて上記ユーザコンピューティング装置によって上記デジタルアセットへのアクセスを提供するまたは拒否することとを可能にする命令をさらに含む、上記〔11〕に記載のシステム。

〔18〕上記アクセスは、任意アクセス制御および強制アクセス制御のうちの少なくとも1つに応じて提供される、上記〔17〕に記載のシステム。

〔19〕上記1つまたは複数の非一時的なプロセッサ可読媒体は、上記少なくとも1つのプロセッサが、分散クライアントソフトウェアアプリケーションで構成される上記ユーザコンピューティング装置から受信される第2のエンロールメントリクエストを処理することであって、上記第2のエンロールメントリクエストは、上記ネットワークにおいて上記ユーザコンピューティング装置の第2のユーザをエンロールするために使用可能であり、上記第2のエンロールメントリクエストは、上記ユーザコンピューティング装置のユーザに関連付けられた第2の暗号化済み部分初期生体認証ベクトル（「IBV」）を含み、上記第2のエンロールメントリクエストを上記処理することは、上記サーバコンピューティング装置によってアクセス可能である、または該サーバコンピューティング装置の一部である非一時的なプロセッサ可読媒体に上記第2の暗号化済み部分IBVを記憶することを含む、処理することを可能にするための命令をさらに含む、上記〔11〕に記載のシステム。

〔20〕ユーザコンピューティング装置とサーバコンピューティング装置との間にセキュアな通信を提供するための方法であって、

上記サーバコンピューティング装置によって、分散クライアントソフトウェアアプリケーションで構成されるユーザコンピューティング装置から受信されるエンロールメントリクエストを処理することであって、上記エンロールメントリクエストは、ネットワークにおいて上記ユーザコンピューティング装置をエンロールするために使用可能であり、上記リクエストは、上記ユーザコンピューティング装置のユーザに関連付けられた第1の生体認証ベクトルの第1の部分を含み、上記エンロールメントリクエストを上記処理することは、上記サーバコンピューティング装置によってアクセス可能である、または該サーバコンピューティング装置の一部である非一時的なプロセッサ可読媒体に上記第1の生体認証ベクトルの上記第1の部分を記憶することを含む、処理することと、

上記ユーザコンピューティング装置から後に受信され、上記第1の生体認証ベクトルの後にキャプチャされる第2の生体認証ベクトルを含み、かつ上記ユーザコンピューティング装置のユーザに関連付けられる認証リクエストを上記サーバコンピューティング装置によって処理することであって、上記認証リクエストは上記第1の生体認証ベクトルの第2の部分をさらに含み、上記認証リクエストを上記処理することは、

10

20

30

40

50

上記第1の生体認証ベクトルの少なくとも上記第1の部分および上記第2の部分を結合すること、

アルゴリズムに応じて、結合された上記第1の部分および上記第2の部分と上記第2の生体認証ベクトルとの比較を行うこと、および

上記比較を表す値を生成することを含む、処理することと、

上記比較を表す上記値を上記サーバコンピューティング装置によって上記ユーザコンピューティング装置に送信することであって、上記ユーザコンピューティング装置は、上記値が最小閾値を上回る場合認証され、上記ユーザコンピューティング装置は上記値が最小閾値を下回る場合認証されない、送信することを含む、方法。

本願の1つまたは複数の実装形態では、ユーザコンピューティング装置とサーバコンピューティング装置との間にセキュアな通信が提供される。分散クライアントソフトウェアアプリケーションで構成されるユーザコンピューティング装置から受信されるエンロールメントリクエストが処理される。エンロールメントリクエストは、ネットワークにおいてユーザコンピューティング装置をエンロールするために使用可能であり、ユーザに関連付けられた、暗号化済み部分初期生体認証ベクトルを含む。暗号化済み部分第2生体認証ベクトルを含む、その後受信される認証リクエストが処理され、かつユーザコンピューティング装置のユーザに関連付けられる。暗号化済み部分初期生体認証ベクトルと暗号化済み部分第2生体認証ベクトルとの比較が行われ、この比較を表す値が生成され、かつ、ユーザコンピューティング装置に送信される。この値が最小閾値を上回る場合、ユーザコンピューティング装置は認証される。

【0004】

1つまたは複数の実装形態では、ユーザコンピューティング装置とサーバコンピューティング装置との間にセキュアな通信が提供される。分散クライアントソフトウェアアプリケーションで構成されるユーザコンピューティング装置から受信されるエンロールメントリクエストが処理される。エンロールメントリクエストは、ネットワークにおいてユーザコンピューティング装置をエンロールするために使用可能であり、ユーザに関連付けられた第1の生体認証ベクトルの第1の部分を含む。第1の生体認証ベクトルの第1の部分は記憶され、第2の生体認証ベクトル、および第1の生体認証ベクトルの第2の部分を含む、後に受信される認証リクエストが処理される。第1の部分および第2の部分は結合され、かつ、第2の生体認証ベクトルと比較される。この比較を表す値が生成され、かつ、ユーザコンピューティング装置に送信される。この値が最小閾値を上回る場合、ユーザコンピューティング装置は認証される。

【0005】

1つまたは複数の実装形態では、エンロールメントリクエストおよび認証リクエストに含まれる証明書が提供され、ここで、認証リクエストを処理することは、証明書が現行のものであり取り消されていないかを判断することを含む。

【0006】

1つまたは複数の実装形態では、アクティブな監視を行い、かつ証明書のリプレイを含む証明書のスプーフィングを防止する侵入検出システムが提供される。

【0007】

1つまたは複数の実装形態では、認証リクエストを処理することは、一方向暗号化に応じて暗号化済み空間において少なくとも1回の照合動作を行うことを含む。一方向暗号化はランダムな一方向のパッドを使用して行われ得る。

【0008】

1つまたは複数の実装形態では、ロール収集が提供され、かつ、デジタルアセットへのアクセスのために1つまたは複数のルールによって定義され、サーバコンピューティング装置は、ロール収集に応じてユーザコンピューティング装置によってデジタルアセットへのアクセスを提供するまたは拒否する。任意アクセス制御および強制アクセス制御のうちの少なくとも1つに応じて、アクセスできるようにする。

【0009】

1つまたは複数の実装形態では、サーバコンピューティング装置は、分散クライアントソフトウェアアプリケーションで構成されるユーザコンピューティング装置から受信される第2のエンロールメントリクエストを処理する。第2のエンロールメントリクエストは、ネットワークにおいてユーザコンピューティング装置の第2のユーザをエンロールするために使用可能であり、第2のエンロールメントリクエストは、ユーザコンピューティング装置のユーザに関連付けられた第2の暗号化済み部分初期生体認証ベクトル（「IBV」）を含む。第2のエンロールメントリクエストを処理することは、サーバコンピューティング装置によってアクセス可能である、またはこの一部である非一時的なプロセッサ可読媒体に第2の暗号化済み部分IBVを記憶することを含む。

【0010】

10

1つまたは複数の実装形態では、サーバコンピューティング装置はユーザのエンロールメントを取り消すことができる。

【0011】

本発明の他の特徴および利点は、添付の図面に言及する、本発明の以下の説明から明らかとなるであろう。

【0012】

本開示のさらなる態様は、添付の図面と併せると、後述されるこのさまざまな実施形態の詳細な説明を検討することでより容易に理解されるであろう。

【図面の簡単な説明】

【0013】

20

【図1】本願の1つまたは複数の実装形態による複数の装置および構成要素を示すブロック図である。

【図2】BOPS実装形態の例に関連して、装置、およびこれらの間の情報フローを示す図である。

【図3】BOPS実装形態の例に関連して、装置、およびこれらの間の情報フローを示す図である。

【図4】BOPS実装形態の例に関連して、装置、およびこれらの間の情報フローを示す図である。

【図5】BOPS実装形態の例に関連して、装置、およびこれらの間の情報フローを示す図である。

30

【図6】BOPS実装形態の例に関連して、装置、およびこれらの間の情報フローを示す図である。

【図7A】1つまたは複数の実装形態に従って、特にデータの機密性を強調したエンロールメントプロセスの例に関連付けられた装置およびステップを示す図である。

【図7B】本願によるユーザインターフェースにおいて提供される管理コンソールの例を示す図である。

【図8】エンロールメントプロセスに関連して、データのアクセスおよびやりとりを含む概要を示す図である。

【図9】本願の1つまたは複数の実装形態によるセキュリティアーキテクチャの構成要素を示す図である。

40

【図10A】本願の1つまたは複数の実装形態による、対応する代替のエンロールメントプロセスに関連付けられた装置およびステップを示す図である。

【図10B】本願の1つまたは複数の実装形態による、対応する代替のエンロールメントプロセスに関連付けられた装置およびステップを示す図である。

【図11】本願に従って、Genesisプロセスの種々のレベルに関連付けられた可能な要件および例を示すブロック図である。

【図12】エンロールメントプロセスおよび認証プロセス中に初期生体認証ベクトルに関連付けられた情報フローの例を示す図である。

【図13】本願に関連して実装される視覚暗号法（VC）の例を示す図である。

【図14】BOPS実装形態の例に関連して、それぞれのビットを共有資源に暗号化する

50

視覚暗号スキーム（VCS）における2つの共有資源（2、2）の重ね合わせの例を示す図である。

【図15】本願によるロール階層のインスタンスを示す図である。

【図16】実装形態の例に従って、リプレイ防止に関連した装置および送信フローを示すブロック図である。

【図17】実装形態の例によるトークンに関連したステップを示す高レベルフロー図である。

【図18】多対多関係のGenesisプロセスに関連した装置および特徴の例を示す図である。

【図19A】単一のクライアント装置においてエンロールメントプロセスの例を開始する複数のユーザを示す図である。

10

【図19B】複数のユーザアカウントに関する情報を記憶するクライアント装置から認証セッションを開始するユーザの1つの例を示す図である。

【図19C】ユーザのアカウントの取り消しに関連付けられたステップの例を示す図である。

【図20A】クライアント装置とBOPSサーバとの間のクライアント証明書の初期化、検証、および確認に関連付けられたステップを実証することを簡略的に示す図である。

【図20B】サードパーティのサーバおよびBOPSサーバに関連したクライアント証明書登録の例を示す図である。

【図21】本願の実装形態の例による、QRコード（登録商標）認証フローの例を示す図である。

20

【発明を実施するための形態】

【0014】

本特許出願の1つまたは複数の実装形態に従って、本明細書では、概して、生体認証オープンプロトコル標準（「BOPS」）と称される、ユーザを認証するためのフレームワークをまとめてまたは少なくとも部分的に含む、新しい標準のセットが提供される。1つまたは複数のBOPS実装形態は、識別アサーション、ロール収集、マルチレベルアクセス制御、保証、および監査のための1つまたは複数のモジュールを提供することができる。

【0015】

30

図1は、ハードウェア配置構成100の例を示し、かつ、1つまたは複数のBOPS実装形態に関連したデータ通信を表示する。配置構成100は、クライアント装置（例えば、スマートフォンまたはモバイル装置）104、サーバコンピューティング装置（本明細書では概して「BOPSサーバ」と称される）102、サードパーティのサーバ106、および、本明細書に示されかつ説明される機能性をサポートしかつ有効にするために複数のコンピューティング装置112を含むことができる侵入検出システム（「IDS」）などの複数のコンピューティング装置を構成する1つまたは複数のソフトウェアアプリケーションを含むことができる。さらに、BOPSサーバ102は、稼働状況監視装置108および解析エンジン装置110と通信または接続できる。装置108および110は両方共、BOPSサーバ102の一部として構成可能である、または個々の装置とすることができる。

40

【0016】

下記は、本明細書において言及される略語および頭字語の非限定的なリストである：admin＝管理部、AOP＝アスペクト指向プログラミング、API＝アプリケーションプログラミングインターフェース、AWS＝アマゾンウェブサービス、appa＝クライアントアプリケーション、BOPS＝生体認証オープンプロトコル標準、CPU＝中央処理装置、CBV＝現行の生体認証識別子、CSRF＝クロスサイトリクエストフォージェリ、ID＝識別子、IDS＝侵入検出システム、IBV＝初期生体認証ベクトル、IP＝インターネットプロトコル、JSON＝JavaScript（登録商標）object notation、LDAP＝ライトウェイトディレクトリアクセスプロトコル、

50

MAC=強制アクセス制御、MCA=モバイルクライアントアプリケーション、NSA=国家安全保障局（米国）、QRコード（登録商標）=Quick Response code、RDBMS=リレーショナルデータベース管理システム、REST=representational state transfer、SSL=セキュアソケット層、TCSEC=trusted computer system evaluation criteria、TLS=トランスポート層セキュリティ、URL=uniform resource identifier、XNTP=extended network time protocol、XOR=「排他的論理和」二項演算、1:M=一対多、4F=4本指、専有生体認証技術、5タプル=5タプルのデータパラメータ。

【0017】

本願の利点は、1つまたは複数の対応するBOPS実装形態が、機能性を提供する構成要素を含むことができ、これが企業の既存の構成要素と共に働くまたはこの代わりになることで、相対的に非常に短い期間で現行の動作環境と統合させるようにすることである。さらに、1つまたは複数の対応するBOPS実装形態は、高感度でプライベートのリソースへのアクセスを判定するなどのために形態の保護を継続的に行う。製作システムのみならず開発時のシステムにも適切なセキュリティを加えるように「ポイントカット」機構の形態としての実装形態をサポートする1つまたは複数のアプリケーションプログラミングインターフェース（API）に少なくとも部分的に応じて、受け入れた目標を満たすまたはこれを超えるようなサービスレベルのセキュリティが、BOPS実装形態において提供可能である。

【0018】

1つまたは複数のBOPS実装形態は、1つまたは複数のデータ通信ネットワークを介してクライアント装置104から、本明細書では概して初期生体認証ベクトル（「IBV」）と称される生体認証ベクトルを受信でき、かつ、あるアルゴリズムに従ったベクトルを、識別に関連付けられた複数部に分割するBOPSサーバ102を含むことができる。個数に関係なく、無鍵式を含んでIBVは暗号化でき、後の生体認証照合プロセスは、オプションとして、管理側パラメータによって示されるように、例えば、クライアント装置104またはサーバ102上で行うことができる。

【0019】

1つまたは複数のBOPS実装形態は、パブリッククラウド（例えばアマゾンウェブサービス）またはプライベートクラウドなどにおけるさまざまなオンライン環境において実装されてよい。

【0020】

本明細書に示されかつ説明される装置の組織的な構造および機能性によると、ユーザ認証は、承認の代わりに、かつ、サーバがクライアント情報を保持するのではなく、むしろ、クライアント同士の認識を可能にするのに十分な量の情報を維持するように提供可能である。1つまたは複数のBOPS実装形態に従ってセキュリティに配慮した構成要素は、識別アサーション、ロール収集、アクセス制御、監査、および保証を含むことができる。よって、1つまたは複数のBOPS実装形態は、大部分は、終端間の生体認証ソリューションにおけるサーバ側の構成要素を考慮する。

【0021】

識別アサーションに関連して、1つまたは複数のBOPS実装形態は、リソースの継続的な保護を提供でき、判定のクラス分けおよび実行可能性、ならびに他の鍵特徴を保証することができる。1つまたは複数のBOPS実装形態はさらに、人間の生体認証に直接頼らずに、指名されたユーザが主張している人物であることを確認する助けとなるように、識別アサーションを補佐することができる。本明細書に示されかつ説明される標準は、同指名されたユーザに関連付けられる任意の識別アサーション部または多数の異なるアサーション部を事実上組み込むことができる相互運用可能な標準について含む。（例えばクライアント装置112を介した）IDSのアプリケーションは、信用証明書のセットのスプーフィングを防止する助けとなるように、および／または、1回または複数回の悪意のあ

る試みを行ったと判断された、または行うことを試みている主体または装置をブラックリストに載せるように、アクティブな監視のために提供できる。

【0022】

さらに、ロール収集は、データの機密性、および、例えば、既知のシステムによって定義されるルールに基づくおよび／または該システムによって実施される特権アクセスに応じてサポートされる。例えば、アクセスの特定のモードが許可されるかどうか判断するために、対応するロールに関連付けられる特定の特権は、グループの分類と比較可能である。対象の構造はアクセス制御によって定義されることが可能であり、ロール収集は、システムレベルで、またはクライアント／サーバ呼び出しを通して行うことができる。例えば、BOPSサーバ102は、一意のユーザを一意の装置104に関連付けるためにロール収集情報を記憶することができる。アクセス制御情報は、所与の主体（例えば、人、装置、またはサービス（例えば、ソフトウェアプログラム））が、アクセスする、および／または所与の対象を、読み取る、書き出す、実行する、または削除するなどのように働き出すことに対して承認されるかを判断するコンピューティング装置上で考えられる1つまたは複数のモジュールを実装することを含むことができる。

10

【0023】

一般的に、アクセス制御は、任意とすることができ、また、または代替的には、より粒度の細かい可能性がある強制アクセス制御を含むことができる。任意アクセス制御は、例えば、指名されたユーザおよび指名された対象（例えば、ファイルおよびプログラム）に応じて、1つまたは複数の対象へのアクセスを制御することと見なす。判定機構は、例えば、ロールベースとすることができ、ユーザおよび管理部が、指名された個人によっておよび／または個人の定義されたグループによって対象の共有を規定および制御することができるようにする。任意アクセス制御機構は、1つまたは複数の実装形態において、対象が、対象の単体またはグループにわたるグループまたは個々のレベルで承認されないアクセスから保護されるように提供される。よって、任意アクセスに関連付けられた粒度は個人からグループに及ぶ可能性がある。

20

【0024】

1つまたは複数のBOPS実装形態は、対応する実装形態内の制御下で全ての主体および記憶対象（例えば、プロセス、ファイル、セグメント、装置）上で強制アクセス制御ポリシーを実施することができる。これらの主体および対象には、感受性ラベルがアサインされ得、これは、階層的分類ラベルおよび非階層的カテゴリの結合とすることができ。ラベルは、強制アクセス制御決定のための基準として判定時に使用可能である。例えば、クライアント装置104上で実行するソフトウェアは、装置にラベルを維持させる、またはBOPSサーバ102にデータを維持させることで主体および対象のラベリングに強制的に順守させる。BOPSサーバ102は、BOPS実装形態の構成要素として信頼される記憶装置を維持できる。本明細書で使用されるように、信頼される記憶装置は、概して、アクセス制御（DACまたはMAC）によって、主体が正しい対象を受信するように保証し、かつ否認不可および機密性をさらに保証するようにセキュアなやり方でデータを記憶することに言及する。

30

【0025】

下記では、1つまたは複数のBOPS実装形態の例においてサポートされるアクセス制御ルールおよびオプションを識別する。主体は、主体のセキュリティレベルの階層的分類が対象のセキュリティレベルにおける階層的分類を上回るまたはこれに等しい場合のみ対象を読み取るためにアクセスできるようにすることが可能である。主体のセキュリティレベルにおける1つまたは複数の非階層的カテゴリは、対象のセキュリティレベルにおける非階層的カテゴリ全てを含むことができる。主体は、主体のセキュリティレベルにおける階層的分類が対象のセキュリティレベルにおける階層的分類を下回るまたはこれに等しく、かつ、主体のセキュリティレベルにおける非階層的カテゴリ全てが対象のセキュリティレベルにおける非階層的カテゴリに含まれる場合のみ、対象に書き込むおよび／またはこの対象を実行することができる。識別および認証データは、ユーザの識別情報を認証し、

40

50

かつ、個々のユーザの代わりに作動するように作成可能であるBOPS実装形態の外部の主体のセキュリティレベルおよび承認がそのユーザによる取り扱い許可および承認によって方向づけられるように保証するために、BOPSサーバ装置102によって使用可能である。

【0026】

本願は、本明細書では概して保証と称される、セキュリティモデルが稼働中であるかの監査および検証を行う1つまたは複数のモジュールに応じて含むアカウントビリティを高めるように動作する。BOPS実装形態内のコンピューティング装置が危険にさらされるという思いもよらない事態が生じた場合、かかるモジュールは危険にさらされたシステムが検出されずに動作しないようにする。例えば、BOPS実装形態において、監査リクエストは、当技術分野では既知であるアスペクト指向プログラミングに応じて含む主体／対象レベルでまたはグループレベルでサポート可能である。これによって、呼び出しが監査証跡に安全に書き込まれる可能性が高まる。さらに、RESTfulウェブサービスおよびJavaScript（登録商標）object notation（JSON）のインターフェースは、監査証跡を読み取るための機構を提供できる。アクションごとの主体、アクションごとの対象、またはアクションごとのグループで監査を行うことができる。例えば、ユーザのグループは特定のな名前（例えば、「会計」）によって指定でき、かつ、総勘定台帳への全ての書き込みを監査できる。さらに、個人、例えば、最高財務責任者には、損益計算書を読み取るための監査情報を与えることができる。

【0027】

JUnitテストのスイートにおける1つまたは複数の、1つまたは複数のBOPS実装形態において、システム内の境界構成要素および条件をテストすることを含むことができる、境界条件をテストおよび監視するために使用可能である。1つまたは複数のBOPS実装形態では、APIに応じて少なくとも部分的にセキュリティ規定を満たすことができる。APIの使用によって、リレーショナルデータベース管理システム、検索エンジン、または事実上任意の他のアーキテクチャといった基礎を成すシステムに準拠するようにBOPS実装形態を識別するおよび／またはカスタマイズすることを必要としないようにする。対応するBOPS実装形態によって提供される機能性は、製作時のシステムのみならず開発時のシステムにも適切なセキュリティを加えるように「ポイントカット」機構を与えることができる。さらに、通信インターフェースを提供するために、例えば、REST、JSON、およびSSLをサポートする1つまたは複数のBOPS実装形態のアーキテクチャは、言語に依存しない。1つまたは複数の実装形態において、サブレット仕様、オープンSSL、Java（登録商標）、JSON、REST、および永続的記憶装置に対してアーキテクチャがビルドされる。ツールはオープン標準に順守でき、図1などに示されるように装置の相互運用性を最大にすることができる。

【0028】

1つまたは複数のBOPS実装形態において、識別アサーション、ロール収集、マルチレベルアクセス制御、監査、および保証が提供される。これらは、少なくとも1つの特別に構成されたクライアント装置104（例えば、スマートフォンまたはモバイル装置）、BOPSサーバ102、および装置112を含む侵入検出システム（IDS）の結合に応じて実装可能である。1つまたは複数の実装形態では、クライアント装置104は、BOPSサーバ102とのセキュアな最初の通信セッションを確立するために、アプリケーションを実行し、かつ、ワンタイムの二方向セキュアソケット層（「SSL」）／トランスポート層セキュリティ（「TLS」）鍵をロードする。ワンタイム鍵は、少なくとも機能的に、（本明細書では概して「Genesis」と称される）識別フェーズ中に生成されるおよび／または提供される主体の二方向SSL／TLS鍵で置き換えられる。Genesisは、概して、生体認証のセットを所与の主体と融合させるプロセスにおける最初のまたは早期のステップを含む。本明細書では概してエンロールメントと称される別のフェーズは、BOPS実装形態においてユーザおよび／または装置を登録することに関連付けられたステップを含み、クライアント装置104の証明書を発行すること、クライアント

証明書を保護すること、および、クライアントにおいて記憶された極秘データを保護することを含むことができる。

【0029】

1つまたは複数のBOPS実装形態において、データ暗号化、およびセキュアなクライアント／サーバ通信をハンドリングするインフラストラクチャが提供される。BOPSインフラストラクチャは、Genesisおよびエンロールメントのプロセスを切り離すこと、および、これらのプロセスをさまざまなエンロールメント要素と共に調整することをサポートできる。これらの従属性は、BOPSサーバ102のインフラストラクチャを識別でき、かつ、BOPS DNS、BOPS Trust Store、BOPS Key Store、およびBOPS鍵ネゴシエーションプロトコルを含むことができる。証明書管理に関して、BOPSサーバ102のホスト名に対するDNS入力は、一方向SSLに対する鍵記憶装置において鍵を有するように構成可能である。1つまたは複数のBOPS構成におけるTrust Storeは、全ての対応する証明書に署名するための認証局を定義する二方向SSL機構である。トランスポートレベルでは、ハンドシェイクを行うことによって、二方向証明書および信頼される記憶装置を通してBOPS識別が行われ得る。キーストアはキーストアにおける鍵によってトランスポートレベルセキュリティをサポートし、キーストアにおける鍵は、SSL／TLSでの暗号化のためにホストを識別するのに使用可能であるVERISIGN、GODADDY、または他の機関といった明確に定義されかつ認識される認証局を使用することができる。本明細書に述べられるように、1つまたは複数のBOPS実装形態は、クライアント装置104が、二方向SSL証明書をロック解除するパスワードをリクエストするワンタイムパスワード（OTP）プロセスを使用する。これは、二方向SSLセッションの開始後に証明書をロック解除するように鍵を戻すためにOTPを同期するクライアント装置104およびサーバ102によって行われ得る。

【0030】

1つまたは複数の実装形態において、いくつかの鍵エンロールメント要素は、クライアント装置104がBOPSサーバ102にリクエストを送る時にクライアント証明書認証をサポートする。トークンは例えば、データ要素、例えば、「共通名」などに応じて、サーバ上のプロファイルを識別情報に連係させる識別子として構成できる。OTPプロセスは、二方向SSL（x.509）証明書をロック解除するパスワードをサーバからリクエストする1つまたは複数の機構を含む。パスワードは、サーバコンピューティング装置102とクライアントコンピューティング装置104との間で調整されるあらかじめ定義されたアルゴリズムによって使用ごとに変更可能であり、OTPに対して使用されるチャネルは、個々の証明書に対して使用されるチャネルと異なっているのが好ましい。例えば、プッシュ通知は、個々の証明書をロック解除するために使用されるパスワードを送ることができる。異なる証明書を使用して、個々の証明書をロック解除するためのパスワードを入手することができる。いずれにしても、証明書をロック解除する機構は、クライアント装置104上のそのパスワードの記憶を伴わない場合がある。

【0031】

ある例では、アプリケーションは、Genesisおよびエンロールメントのためのデフォルトの（例えば、あらかじめロードされた）証明書を使用する。後の処理では、現行のOTPでデフォルトの証明書を使用できる。その結果（例えば、HTTP応答）は証明書をロック解除するためのパスワードを含むことができる。OTPは、次いで、クライアントおよびサーバにおいてロールフォワードすることになる。1つまたは複数のBOPS実装形態において、リプレイアタックを防止するために使用される5タプルは高エントロピー値である。この値は、エンロールメント時に生じる可能性があり、クライアント装置104とサーバ102との間の将来的な通信の一部となり得る。

【0032】

BOPS実装形態におけるクライアント／サーバアプリケーションの相互作用は、3ステップのプロセスと考えることができ、少なくとも2つの可能な変型が最初の第1のステ

10

20

30

40

50

ップの後に生じ得る。このような場合、BOPSクライアント／サーバアプリケーションアーキテクチャは、3つの構成要素：クライアント装置104上で実行するクライアントアプリケーション、BOPSサーバ102上で実行するアプリケーション、および（図面では「アプリサーバ」と称される）サーバ側アプリケーションを参照して、本明細書では説明される。図2～図6に示される例では、サーバ側アプリケーションは、SSL／TLS接続がアプリケーションサーバで終点となる可能性があるため、必ずしも、BOPSサーバ102を通して起動するわけではない。さらに、対応するBOPS実装配置は、非暗号化コンテンツによるBOPSシステムを当てにするアプリケーションを必要としない。図2を参照すると、Genesisプロセス中に、クライアント装置104はBOPSサーバ102への呼び出しを行い、かつ、ユーザおよびクライアント側アプリケーションソフトウェアを認証する。その後、クライアント装置104は、BOPSサーバ102によって割り当てられた、かつ、特定のアプリケーションのクライアント識別情報に固有の証明書を受信する。

10

【0033】

次のステップ中（図3）、クライアント装置／アプリケーションはアプリケーションサーバを直接呼び出す。アプリケーションのクライアント部およびサーバ部の間のSSL／TLS接続は、これらの箇所で始められかつ終わる。コンテンツのやりとりは、好ましくは、アプリケーションの外部でBOPSサーバ102にはまたはこのアプリケーションエンティティ内で信頼されない他のものには不可視である。クライアントセッション中（図4）、アプリケーションサーバ106は、BOPS102サーバを呼び出して識別詳細を入手し、かつ、証明書が以前に取り消されていないかを確認する。

20

【0034】

（一部図5に示される）第2の変型では、（図2～図3に示されるものを含む）Genesisステップは同じとすることができる。その後、BOPSサーバ102は、アプリケーションサーバ106構成要素に連絡して、新しいクライアント104が登録され、かつ割り当てられたことを通知する。第2の変型のフローは、少なくとも2つのやり方：識別詳細が異なっている、および取り消しチェックがクライアントセッションにおいてもたらされる（図6）という点で、第1の変型のフローと異なっている。第3のステップでは、クライアント装置104がアプリケーションサーバ106を直接呼び出す時、アプリケーションサーバ106はBOPSサーバ102を呼び出して、証明書が以前に取り消されていないかを確認する。

30

【0035】

BOPS実装形態の例に関連して本明細書に示されかつ説明される特徴は、本明細書に提供されるアクセス制御モジュールによってまたはこれに関連して使用可能である、または、既存のフレームワークの識別アサーション要素に追加可能である。よって、BOPS実装形態は、制作環境において最小のアクションを行うことによって信頼される処理を可能にし、それによって、アプリケーションソフトウェアの変更を必要としないようになることが多くなる。

【0036】

図7Aは、1つまたは複数のBOPS実装形態に従って、エンロールメントプロセスおよび関連のデータの機密性の例に関連付けられた装置およびステップ700を示す。本願において一方向SSL／TLSに加えてビルドされる二方向SSL／TLSは、クライアント装置104において始める通信を提供する。最初の（例えば、Genesis）通信は、クライアント104の識別の起点を定義し、かつクライアント装置104が後の通信のためにセッション指向識別アサーションと併せて使用できるというBOPS対応二方向証明書を渡す。1つまたは複数の実装形態では、クライアントアプリケーションは、後のGenesis動作に対して可能であるあらかじめロードされた二方向SSL／TLS鍵を有することができる。

40

【0037】

1つまたは複数の実装形態によると、BOPSサーバ102は、クライアント装置10

50

4からの識別情報を二方向SSL/TLSによる一方向SSL/TLS通信で受信する。一方向SSL/TLSおよび二方向SSL/TLS両方を介して通信は行われる。1つまたは複数の実装形態では、サーバ102は、信頼される識別情報を入手し、かつ対応する識別情報の代わりに処理するためのロールを収集するためにデータ記憶装置を使用する。また、監査は、継続した検証および信頼されるアクセスの妥当性検査に対して適切なアーティファクトを最大化する。マルチレベルアクセス制御機構の簡略化および文書化に応じて、保証を行うことができる。1つまたは複数のBOPS実装形態において、グラフィカルユーザインターフェースにおける管理コンソール（以降「アドミンコンソール」）は、提供された後、登録プロセスは完了し、これによって、ユーザ、グループ、およびロールの動的な修正が可能になり、このことは本明細書においてより詳細に説明される。アドミンコンソールの例は図7Bに示される。

10

【0038】

図7Aを参照すると、トークンリクエスト（RESTful）は、クライアント装置104から送信され（1）、BOPSサーバ102から受信され、検証される（2）。BOPSサーバ102のホスト名に対するDNSエントリは、キーストアにおいて鍵を有するように構成でき（3）、リクエストはフォーマットされ（4A）、mのトークン応答は二方向SSL/TLSを介してクライアント装置104に送信される（4B）。その後、cのトークン（例えば、5タプルおよびTimestamp）はクライアント装置104から送信され（5）、これは、リクエストにおいてmのTimestampに応じて含んで、検証される（6、7）。その後、欠けている5タプルは信頼される記憶装置に対して判断され（8）、リクエストはフォーマットされ（9）、SHA512トークンはクライアント装置104に送信される（10）。

20

【0039】

続けて図7Aを参照すると、SHA512トークンを含む登録リクエストは、クライアント装置104から送信され（11）、BOPSサーバ102による妥当性検査のために受信され（12）、クライアント署名リクエストは、ワンタイムパスワードを算出しかつキーストアに対してトークン数をチェックすること（14）、および外部の通知サービスへとクライアント証明書パスワードを外部にプッシュすること（15）を含んで、証明書をロック解除するために処理される（13）。加えて、12における検証ステップは、解析に関連付けられたステップに分岐し、かつ、装置情報（16）、プロファイル情報（17）

30

【0040】

加えて、クライアント装置の証明書パスワードは、フォーマットされたリクエスト（2）およびSHA512トークン（21）と共に再びクライアント装置104に送信される。その後、SHA512トークンを含むカスタムセキュリティリクエストは、クライアント装置104から送信され（22）、これはBOPSサーバ102によって検証される（23）。リクエストはフォーマットされ（24）、（SHA512トークンを含む）カスタムセキュリティ応答はクライアント装置104に送信される（25）。

【0041】

1つまたは複数のBOPS実装形態では、装置112を介することを含んで、アクティブな侵入検出システムが提供される。アクティブな侵入検出システムは、ブルートフォースアタック、サービスの妨害（例えば、分散したまたは単一のサービスの妨害）、または他のアタックに対して効果的である。二方向SSL/TLS証明書偽装の偽造を行う試み、セッションリプレイ、偽造したパケット、または、どうにかしてBOPSサーバ装置102を危険にさらそうとするさまざまな裏をかく技法を識別しかつ追跡するカスタムルールが定義されかつ施行可能である。

40

【0042】

1つまたは複数のBOPS実装形態において、視覚暗号法は、初期生体認証ベクトル（IBV）を暗号化するために使用される。この技法によって、生体認証照合を行う特定の

50

装置上でXOR演算を使用することなどによって、IBVの早い組み替えという利点もたらされる。例えば、秘密共有スキームのために提供する、Moni NaorおよびAdi Shamirによって開発された技法が使用できる。動作の例では、ベクトルは、Nの共有資源に分けられ、初期ベクトルの組み替えはNの共有部全てを必要とする。各装置は、BOPSサーバ102およびモバイルクライアントアプリケーション104を含み、エンロールされたベクトルは2つの共有部に分けることができ、このうちの1つはBOPSサーバ102によってアクセス可能であるBOPSレポジトリに記憶され、もう1つはモバイルコンピューティング装置104に記憶される。

【0043】

本願の1つまたは複数の実装形態では、データの機密性を徹底する暗号化および／または機構の他の形態は、利用可能である。例えば、楕円曲線暗号は視覚暗号法の代わりに（または場合によってこれに加えて）使用可能である。

【0044】

ある例の生体認証アクション中、新しく取得されたベクトル、およびエンロールされたベクトルの両方の共有資源は、単一の場所（例えば、モバイルコンピューティング装置アプリケーション104またはBOPSサーバ102）において、または複数の場所において使用可能とすることができる。どんな場合でも、エンロールされたベクトル共有を使用して、初期ベクトルは、メモリにおいて組み替え可能であることで、これに対して生じる認証をサポートすることができる。図8は、エンロールメントプロセスに関連して、データのアクセスおよびやりとりを含む概要を示す。BOPSサーバ102に関して、主体のアカウントおよび装置に応じて識別情報が提供される。主体のアカウントおよび装置は、所与の主体のプロファイル情報の一部である。プロファイル情報はクラスタ化されたデータ記憶装置に記憶される。照合させるために、IBVは、共有資源に取り入れられ、再構成され、解読される。照合アルゴリズムがユークリッドの照合が可能でない場合、プレーンテキストとしての照合が生じ、他の状況では、暗号化されたドメインでの照合が生じる。

【0045】

代替的な実装形態では、準同形の暗号化が用いられ、これによって、計算が暗号文に対して行われるため、暗号化済みの結果を生成することが可能になる。照合動作は暗号化済み空間で可能であることで、プライバシーおよびセキュリティを高めることができる。例えば、一方向暗号化を使用して暗号化済み空間において照合を行うことによって、高レベルのプライバシーをもたらし、かつ、元のプレーンテキストのIBVを得る能力を効果的に妨げることができる。

【0046】

1つまたは複数の実装形態において、1つはクライアント、もう1つはサーバの2つの部分を有するようにするアルゴリズムによって一方向暗号化が行われる。照合において当技術分野で既知であるユークリッド距離（例えば、ハミング距離）を使用する場合、暗号化済み空間で照合を行う。代替的には、照合にハミング距離を使用しない場合、本明細書に説明されるように、プレーンテキスト空間において照合を行う。

【0047】

1つまたは複数の実装形態において、ランダムなワンタイムパッド（ROTP）は、暗号化済み空間における照合を可能にする一方向暗号化を行うために使用される。代替的には、視覚暗号法は、プレーンテキストにおける照合の場合に可逆暗号のために使用される。例えば、ハミング距離を有さない場合、視覚暗号法はメモリにおいて照合を行うようにプレーンテキストに返すために使用される。好ましくは、暗号化および解読は、2つの暗号化アルゴリズム：1. ビットマスク、または2. マトリックス変換のうちの1つを使用する。理想的には、全ての照合アルゴリズムがハミング距離を有するようにし、従って、サーバはプレーンテキストのIBVを有さない。

【0048】

下記は、2つの二値ベクトル間のハミング距離を計算することに応じて行われる虹彩認

10

20

30

40

50

識に関連したアルゴリズムの例である。このアルゴリズムの例では、生体認証の暗号化された二等分に対して、これらを以下のようにプレーンテキストに変換することなく直接照合を行うことができる（ $\wedge$ はビット単位のXOR演算を示す）。

【0049】

サーバは、ベクトル $\wedge$ ノイズをエンロールする、を記憶する。

【0050】

電話は、ベクトル $\wedge$ 同じノイズを検証する、を送る。

【0051】

サーバに対して比較が行われる：（ベクトル $\wedge$ ノイズをエンロールする） $\wedge$ （ベクトル $\wedge$ 同じノイズを検証する）。

10

【0052】

XORは、可換であり、かつ結合的であり、そのため、これは、（ベクトルをエンロールする $\wedge$ ベクトルを検証する） $\wedge$ （ノイズ $\wedge$ 同じノイズ）、に並び替え可能である。

【0053】

XORは自己逆元であり、従って、（ノイズ $\wedge$ 同じノイズ）= Iであり、式中、IはXORの識別要素であり、これは0である。

【0054】

従って、式は、（ベクトルをエンロールする $\wedge$ ベクトルを検証する） $\wedge$ I = （ベクトルをエンロールする $\wedge$ ベクトルを検証する）に簡略化する。

20

【0055】

AとBとの間のハミング距離はA $\wedge$ Bの関数である。

【0056】

従って、ノイズのあるベクトル間のハミング距離は、元のベクトル間のハミング距離と同一である。

【0057】

エンロールメントに基づく実装形態の例では、下記が生じる。

【0058】

a) . エンロールメントベクトル：

【0059】

0 0 1 1 0 0 1 1

30

【0060】

b) . ランダムシーケンス（ベクトルの前半）：サーバに対して記憶する。

【0061】

0 1 0 1 0 1 0 1

【0062】

c) . ベクトルの後半（算出済み）：電話に対して記憶する。

【0063】

0 1 1 0 0 1 1 0

【0064】

検証に基づく：

40

【0065】

e) . 検証ベクトル：（エンロールと検証との間で変更された最後のビットのみを通知するが、これは照合が良好であるからである）。

【0066】

0 0 1 1 0 0 1 0

【0067】

ベクトルの後半：電話に対して記憶する。

【0068】

0 1 1 0 0 1 1 0

【0069】

50

f) . ベクトルの前半 (e から c まで) に対する近似を算出する。

【0070】

0 1 0 1 0 1 0 0

【0071】

照合に基づいて：

【0072】

g) . この「前半の検証」(f) をサーバに送る。

【0073】

h) . サーバはここで以下を有する。

【0074】

ベクトルの前半のエンロールメント b) :

【0075】

0 1 0 1 0 1 0 1

【0076】

ベクトルの前半の検証 f) :

【0077】

0 1 0 1 0 1 0 0

【0078】

b と f との間で変更された全てのビットに 1 でフラグを立てる：

【0079】

0 0 0 0 0 0 0 1

【0080】

システムによって、最後のビットのみがエンロールと検証との間で変更され、これは良好な照合を表し、どのようにしてサーバがスクランブルをかけられたデータのみを取り扱ったのかを通知すること、および、実際のベクトルがサーバで既知ではなく、ベクトルの差異のみが算出できることが分かる。

【0081】

代替的な実装形態では、テンプレートベクトル間のユークリッド距離を算出することによって、顔認識が行われ、この場合顔はベクトルから解析して模倣できない。2つの顔の画像が照合される時、例えば、ニューラルネットワークを使用して、それぞれの顔は最初に、128バイトのサイズの浮動ベクトルに変換される。この符号ベクトルの表現は任意であり、元の顔に戻すように解析して模倣できない。これらの顔を比較するために、2つのベクトルのユークリッド距離が算出される。同じ人からの2つの顔は同様のベクトルを有すべきであり、異なる人達の顔はユークリッド空間においてさらにばらばらであるべきである。検証ベクトルはモバイル装置に対して算出可能であり、記憶されたエンロールメントベクトルに照合させるため、リモートサーバに送信される。それ故に、元の生体認証(例えば、顔)は、ユーザの装置を離れることはなく、全ての照合はサーバに対して算出可能である。

【0082】

さらに別の実装形態において、テンプレートベクトル間のユークリッド距離を算出することによって、指紋認識が行われ、ここで、指紋はベクトルから解析して模倣できない。同様に、上述されるように、ニューラルネットワークは指紋照合のために適用可能である。このような場合、指紋は装置においてベクトルに変換可能であり、このベクトルは送信されることになり、それによって、ネットワーク出力ベクトルから元の指紋画像を再構築するやり方が排除される。

【0083】

1つまたは複数の実装形態では、装置上で暗号鍵がランダムに生成され、これは、ニューラルネットワークから出力されたベクトルを分かりにくくさせるために使用される。例えば、暗号化生体認証ベクトル=暗号化マトリックス×プレーンテキスト生体認証ベクトル、である。このような場合、暗号化マトリックス変換は、ユークリッド距離が保全され

10

20

30

40

50

るという特別な特性を有するため、マトリックスは厳密な変換であるはずである。このような場合、生体認証ベクトルは非暗号化フォーマットで装置を離れず、サーバは、2つの暗号化された生体認証を比較し、かつ、プレーンテキストを知ることなく、ユークリッド距離を算出する。ユーザが新しい装置からの検証を望む時、ユーザは、暗号化データを、QRコード（登録商標）などによって新しい装置に転送することができる。これは、古い装置が利用可能であることを必要とする。古い装置が失われるまたは別の状況では利用不可能である場合、ユーザは、本明細書に示されかつ説明されるように、再エンロールする。

【0084】

それ故に、生体認証ベクトルが分割され、かつ暗号化されて装置間で記憶されるのに応じて、向上したプライバシーがもたらされる。ディスクまたはメモリどちらにもプレーンテキスト形式でサーバ上に存在する生体認証ベクトルは部分的にもない。さらに、各認証および認証の失敗に対する「仮説の」解析を行うことを希望するユーザは、ファセット、検索、および解析などをサポートする管理側インターフェースを介してこの解析を行うことができるため、本願は向上した解析をもたらす。

【0085】

図9は、1つまたは複数のBOPS実装形態によるセキュリティアーキテクチャ900の例の構成要素を示す。図9に示されるように、BOPSセキュリティクラスタ902は、仮想プライベートネットワーク（VPN）上でBOPSインスタンスを起動するように構成可能である。認証局エンティティ、BOPS Key Store、およびBOPS Trust Storeのコア属性は、例えば、BOPSインスタンス上に位置することができる。BOPSインスタンスはまた、DNS、OPSライブラリ、通知サービス鍵、ビジネスアダプタ、BOPS構成特性に関連付けられたおよび／またはこれらを表すデータを包含することができる。ロードバランサクラスタ904は、作業負荷を分散した、BOPSサービスの信頼性および可用性を徹底する1つまたは複数の装置を含むことができる。構成されたBOPSロードバランサ904は、スループットを最大化し、応答時間を最小化し、BOPSアーキテクチャ900におけるいずれの単一のリソースの過負荷も回避するように動作可能である。

【0086】

続けて図9を参照すると、永続クラスタ906は、1つまたは複数のデータベースセキュリティグループを含むことができ、かつ、BOPSデータクラスタを自動スケーリングするように構成可能である。認証サービスは、大きいデータオブジェクトを取扱い、大きいデータセット、NoSQLなどのビッグデータ記憶装置をハンドリングし、データのデータ（「シャード」）の1つまたは複数の水平パーティションは、シャードから同時に読み取り、かつ結果をマージすることによって、性能を改善するために利用可能である。データベースセキュリティアーキテクチャ900は、BOPSアーキテクチャを実装し、かつ、単一の場所における極秘データの記憶の集中を防止する。また、IDS装置112を含むことができる監視クラスタ908も図9に示されている。

【0087】

図10Aおよび図10Bは、1つまたは複数のBOPS実装形態による、対応する代替のエンロールメントプロセス1000および1010それぞれに関連付けられた装置およびステップを示す。図10Aおよび図10Bに示される実装形態は、アカウントまたは装置に関連付けられた暗号化済み生体認証データを記憶する、生体認証データの変更全てについての情報を記憶する、認証サービスおよびこの対応する生体認証ライブラリ（例えば、顔、4F、虹彩）をロードしかつ使用する、および、新しいフロー（例えば、エンロールメントおよび認証）をサポートするためのAPI動作を提供する機構を提供する。

【0088】

図10Aに示される実装形態において、モバイルコンピューティング装置104上で実行するソフトウェアアプリケーション（「MCA」）は、認証フローの方法がクライアント104側で行われるように構成される時、初期生体認証ベクトル（IBV）の取得、エン

10

20

30

40

50

ロールメントプロセス中に暗号分割動作を行いかつこのプロセスをサーバ側のCPU負荷を低くするために分散すること、BOPSサーバ102によってエンロールメントリクエスト（登録）を行うこと、および、暗号照合動作を行うことをもたらす。BOPSサーバ102は、例えば、エンロールメントプロセス中にBOPSビッグデータ記憶装置1002において、共有されたベクトルと共にユーザ識別データを保存するように構成可能である。さらに、BOPSサーバ102は、認証フローを管理し、かつ認証サービス通信構成要素を統合することができる（1004）。認証サービス（1006）は、1つまたは複数の認証アルゴリズム、生体認証エンジンライブラリを動的にロードし、認証エンジンバージョン管理に対するサポートを提供して、BOPSサーバ102と1つまたは複数の生体認証エンジンとの間の通信を正規化し、認証エンジンバージョン管理に対するサポートを提供し、および、BOPSサーバ102と認証エンジンとの間の通信を正規化することができる。認証サービスは、認証を行う際に生体認証サービスをラップする。

10

【0089】

本明細書に説明されるように、プラグブル認証サービスおよびこの対応する生体認証エンジンのための1つまたは複数の機構が提供される。それ故に、BOPS実装形態は（例えば、認証サービスおよび生体認証ライブラリの場所を介して）構成可能とすることができ、利用可能なサービスを自動的にロードしてシステムに登録することができる。

【0090】

この結果、発音サービスのリストは、システムレベル、例えば、4Fエンジン、顔エンジン、虹彩エンジン、音声エンジンで利用可能である。認証部のリストは、FIDO認証部またはBOPS認証部を含む。

20

【0091】

本願は、以下の特徴をサポートすることによって、生体認証統合認証サービスに対する改善をもたらす。BOPSサーバ102によってアクセス可能であるアカウントまたは装置において暗号化された生体認証データを記憶するための、1つまたは複数の機構が提供可能である。さらに、生じる生体認証データ変更を表す情報を記憶するための機構が提供可能である。加えて、例えば、同一出願人による、米国特許出願第14/201,462号明細書、米国特許出願第14/201,499号明細書、米国特許出願第14/988,833号明細書、および米国特許出願第14/819,639号明細書に示されかつ説明されるような、顔、4本指、および虹彩の生体測定による認証に関連して含む、認証サービスにアクセスしかつこれを使用する「汎用」機構が提供可能である。

30

【0092】

本願の1つまたは複数の実装形態において、モバイルコンピューティング装置104は、エンロールメントベクトルを取得し、かつ、エンロールメントプロセス中に暗号分割動作を行う。これによって、サーバ側でプロセスを分散しかつCPU負荷を低下させることによって計算機能性の改善がもたらされる。さらに、モバイル装置104は、BOPSサーバ102に対するエンロールメントリクエスト（登録）を行い、かつ、認証フローからの「生体認証妥当性検査」ステップが携帯で行われるように構成される時、暗号照合動作を行うことができる。

【0093】

本願の1つまたは複数の実装形態において、BOPSサーバ102は、例えば、エンロールメントプロセス中にAPACHE SOLRレポジトリにおいて、共有ベクトルの少なくとも一部分と共にユーザ識別情報を記憶する。さらに、BOPSサーバ102は、認証情報およびプロセスフローを管理し、かつ、少なくとも1つの生体認証サービス通信構成要素を統合するように構成可能である。

40

【0094】

本願によるアーキテクチャにおいて提供される他の構成要素は、1つまたは複数の認証サービスおよび1つまたは複数の生体認証エンジンを含むことができる。認証サービスは、1つまたは複数の認証サービスのバージョン管理をサポートするように構成される1つまたは複数のライブラリの動的なロードを行うように、BOPSサーバ102と認証サー

50

ビスとの間の通信を正規化するように、および、1つまたは複数のBOPSインスタンスが、自身でスケーリングすることができる別個のクラウドを離れるまたは該クラウドである場合のウェブアプリケーション機械といった、1つまたは複数の配置シナリオをもたらすように構成可能である。

【0095】

1つまたは複数の実装形態において、生体認証エンジンは、インターフェースの主体である、管理されていない生体認証ライブラリを含むように構成され、BOPS実装されたシステムにプラグインされるそれぞれの対応するライブラリによって定義されかつ実装される。生体認証エンジンは、好ましくは、必要に応じてエンジンをロードする「ロード」方法、エンジンを無料リソース（例えば、メモリ、一時ファイル）にアンロードする「U 10 n l o a d L o a d」方法、ステータス情報（例えば、INIT_FAILED、OK、ERROR、OUT_OF_MEMORY）を提供する「Get Status」、エンロールメント中に取得したベクトルを暗号化する「分割」方法、例えば、初期ベクトルの共有部に基づいて、ベクトルを認証する「照合」方法、「アクティブ化／登録」方法、および、エンジンの記述をもたらす。記述は、例えば、生体認証タイプ識別子、名前および記述、エンジンバージョン、および生体認証フォーマットを含むことができる。この情報を使用して、本願に関連付けられる1つまたは複数のプロセスは、特定の生体認証エンジンを自動的にロードしかつ登録することができる。

【0096】

1つまたは複数の実装形態において、プラグブル認証サービスのための機構は、システムが、構成可能であり（認証サービス場所）、利用可能なライブラリを自動的にロードしかつシステムに登録できるようにサポートされる。認証サービスと呼ばれるそれぞれの生体認証ライブラリは、それ自体を記述するように、定数列（生体認証タイプ）、対応するバージョン、名前および記述といった情報を提供できる。さらに、ペア（生体認証タイプ、生体認証バージョン）などの情報は、一意の生体認証エンジンを識別することができる。

【0097】

認証サービスおよびこの対応するレベルが低くなった生体認証エンジンの例は、列挙可能であり、例えば、同一出願人による、米国特許出願第14／201，462号明細書、米国特許出願第14／201，499号明細書、米国特許出願第14／988，833号 30 明細書、および米国特許出願第14／819，639号明細書に示されかつ説明されるような、4F、顔、虹彩、および音声を含むシステムレベルで利用可能である。

【0098】

本明細書に述べられるように、1つまたは複数のBOPS実装形態において、Genesisおよびエンロールメントプロセスは効果的に切り離され、これによって、生体認証ベクトル、証明書、または、その他の状況では自動化処理に必要とされる他の機密情報にBOPSサーバ102が直接アクセスする必要なく、主体の識別情報を判断することが可能になる。それ故に、BOPSソリューションは、「オープンである」と解釈でき、事実上、Genesisおよびエンロールメントにおけるいずれのカスタマイズも可能にすることができる。例えば、Genesisは、アクティブなディレクトリ、電子メールまたは 40 テキストメッセージの妥当性検査、または、識別情報を物理的に検証するための組織のオフィサにアクセスするためにユーザ名およびパスワードを使用することを含むことができる。例えば、バッチで生じる場合があるユーザアカウントの予備登録は、ビジネス要件に基づくことができる。さらに、Genesisプロセスは、リスク管理に対する完全な従属関係を形成でき、さらに、下流処理を判断することができる。例としてのGenesisの後処理の間、ユーザは、対応してエンロールされた装置に対して発行される一意のクライアント証明書を含むことができる、自身の生体認証をエンロールする。さらに、ワンタイムパスワード（例えば、「シード」）は、クライアント装置104とサーバ装置102との間で確立可能であり、さらなるシード値はリプレイアタック防止のために使用可能である。

10

20

30

40

50

【0099】

本明細書において、単一ユーザが多くの装置を有する場合がある、および／または、単一装置が多くのユーザを有する場合がある（すなわち、単一装置が多くの生体認証を有する場合がある）ことは認識されたい。よって、多対多関係の形態は、Genesisおよびエンrollmentプロセスを分離することに応じて生じる可能性がある。それ故に、Genesisによって識別された主体は、多くの生体認証によって何度もエンrollmentする可能性がある。1つまたは複数のBOPS実装形態において、エンrollmentプロセスは、二方向セキュアソケット層／トランスポート層セキュリティ（SSL／TLS）証明書を使用し、これはサーバ側で生成可能である。かかる生成は、Genesisプロセス後に行うことができるため、明確に定義された主体に対して証明書が適正であることが保証される。

10

【0100】

また、1つまたは複数のBOPS実装形態は、さまざまなレベルのプロビジョニングを有することができ、これによって、種々のセキュリティレベルに対する柔軟性がもたらされる。例えば、高いレベルのGenesisは、ユーザが、オフィサなど、物理的に誰かの正面で妥当性検査を行うことを含む。低いレベルは、代替策では、ユーザによって受信される電子メールの妥当性検査と併せてユーザ名およびパスワードだけを定義することを含むことができる。さまざまなレベルのGenesisおよび検証プロセスは、1つまたは複数の対応する組織に一意であるまたは固有であるとして行うことができる1つまたは複数のビジネス上の決定に応じて、実装可能である。さらに、後の処理は、対応するGenesisレベルに基づいて変更可能である。例えば、システムは、高いレベルのGenesisに関連した1000、000ドルの振替を可能にするだけでなく、より低いレベルのGenesisに関連した100ドルの振替も可能にする。

20

【0101】

図11は、本願に従って、種々のレベルのGenesisに関連付けられた可能な要件および例1100を示すブロック図である。検証プロセスにおいてさらなる要件が必要とされるため、各セキュリティレベルはそれに対応して上昇する可能性がある。図11のレベルの例では、第1のレベルおよび第2のレベルは組織的な考察に基づいてスワップ可能である。例えば、目標がビジネスビジタに対するWi-Fiアクセスを検証しかつ与えることである場合、検証は、モバイル装置を介して送ることが可能であり、本明細書では低い検証レベルであると考えられる。

30

【0102】

エンrollmentフェーズ中、例えば、モバイルコンピューティング装置104上で実行しているモバイルアプリケーションは、対応するビルトイン機能に基づいて生体認証をエンrollmentする。例えば、特定の統合でビルドされ、デフォルトの生体認証を必要としているモバイルアプリケーションは、アプリケーションにおいてこのような具体的にハードコードされたモジュールを有することができる。

【0103】

1つまたは複数のBOPS実装形態は、生体認証トランザクションの速度に対処し、かつ、モバイル装置上の仮想化の脅威の問題を解決する。かかる脅威の例は、侵入者がモバイル装置のコピーされた仮想画像上のコードを逆コンパイルし、このソースコードを使用して電話認証を停止し、認証しかつ許可を与えるサーバを制御しようとすることである。

40

【0104】

これらのリスクを軽減するために、BOPS実装形態におけるプロセスでは、暗号鍵なしで初期生体認証値（IBV）を暗号化し、その後、IBVの半分はクライアント装置104に記憶され、もう半分はサーバ102に記憶される、または別の状況では該サーバによってアクセス可能である。生体認証照合はサーバ102上で行うことができる。図12は、エンrollmentプロセスおよび認証プロセス中に初期生体認証ベクトル（「IBV」）に関連付けられた情報フローの例1200を示す。図12に示されるフローの例では、エンrollment中、IBVはキャプチャされかつ分割され、IBVの一部（例えば

50

、半分)はクライアント装置104に記憶される。IBVの一部分(例えば、半分または1/2)はエンrollmentリクエストにおいてBOPSサーバ102に送信され、この部分は、例えば、BOPSサーバ102によってアクセス可能なデータ記憶装置に記憶される。その後、BOPSサーバ102によってエンrollmentの確認が送信される。

【0105】

続けて図12を参照すると、現行の生体認証ベクトル(「CBV」)は後続の生体認証プロセス中にキャプチャされ、かつ、残りの部分(2/2)を含んで認証(「Auth」)リクエストに関連してBOPSサーバ102に送られる。BOPSサーバ102は、認証リクエストにおける受信されたIBVの一部分を結合し、かつこれをIBVの記憶された一部分に結合して解読するように構成される。受信されたCBVは、IBV全体のプレーンテキストと比較され、比較中の判断に応じて、クライアントコンピューティング装置104に数(例えば、浮動小数点数)が返される。照合するものがある場合、ユーザは、認証されたとして登録可能である。さらに、認証プロセスの結果は、クライアントコンピューティング装置104上に表示可能である。

10

【0106】

よって、図12に示されるステップに示され、かつ本明細書に説明されるように、本願によるBOPS実装形態は、生体認証トランザクションの速度に対処し、かつクライアント装置上の仮想化の脅威に関連付けられた問題を解決する。このような脅威は、例えば、侵入者が、例えば、モバイル装置のコピーされた仮想画像に対してソフトウェアを逆コンパイルし、このソースコードを使用して電話認証を停止し、認証しかつ許可を与えるサーバを制御しようとした後に生じる可能性がある。

20

【0107】

これらのリスクを軽減するために、BOPS実装形態に関連付けられた特徴は、暗号鍵なしでIBVを暗号化し、クライアント装置上のIBVの一部分(例えば、半分)、およびサーバ、またはサーバによってアクセス可能な装置上の一部分(例えば、もう半分)を記憶するように動作可能である。サーバ上で生体認証照合を行うことができる。このように、盗まれた装置は認証を無視することができないが、これは少なくとも部分的に、危険にさらされた装置またはサーバが攻撃者に対して有用となる情報を与えないからである。

【0108】

1つまたは複数の実装形態によると、下記は、1つまたは複数のBOPS実装形態における生体測定による認証に対する処理協約を確立するために提供する。生体認証ベクトルは、少なくとも、クライアントとサーバとの間で分割され、認証へのアプローチは不可知論的な生体認証である。例えば、顔認識に関連して、初期生体認証ベクトルのサイズは、およそ20KBとすることができ、これは、HTTPリクエストおよびHTTP応答の上/下によって最小になる可能性があるため、受け入れられる。顔認識に関連するIBVの分割アルゴリズムは、次のように、ゼロビットが白であり、1ビットが黒である可能性がある。それ故に、BOPS実装形態は、視覚暗号法(VC)に対応することができる。本明細書に述べられるように、本願は、事実上任意の生体認証で使用可能であり、IBVを取り入れかつVCで暗号化する機構を提供する。VCでは、照合はプレーンテキストで生じる。代替的には、ランダムに、照合は、暗号化ドメインで生じる。

30

40

【0109】

具体的に図12を参照して、クライアントコンピューティング装置104を動作させるユーザは、生体認証エンrollmentを進め(1)、初期生体認証ベクトル(IBV)をキャプチャする(2)。ステップ(3)では、IBVは暗号化されかつ分割され、IBVの2/2はローカルにクライアントコンピューティング装置104にまたは該装置によって記憶され(4)、エンrollmentリクエストはIBVの1/2を含んで送られ、(二方向SSL/TLS)を介して)トランスポート層を介してBOPSサーバ102に送信される(5)。IBVの1/2は、BOPSビッグデータなどにおいて、BOPSサーバ102によって記憶され(6)、エンrollmentの確認はBOPSサーバ102からクライアントコンピューティング装置104に戻って送信される(7)。

50

【0110】

続けて図12を参照すると、エンロールメントの後に、クライアントコンピューティング装置104において生体測定による認証が行われ(8)、現行の生体認証ベクトルはキャプチャされる(9)。その後、認証リクエストは、トランスポート層を介して送られ(10)、BOPSサーバ102によって受信され、IBVの2/2と結合され、解読のために使用される(11)。その後、CBVはIBVのプレーンテキストと比較され(12)、浮動小数点数はクライアント104に戻るよう送信され(14)、結果が表示される(15)。

【0111】

ここで図13に移ると、本願に関連して実装される視覚暗号法(VC)の例1300が示される。VCは、暗号化による良好な相乗効果、IBVの分割、および、鍵管理の必要がないIBVの再構築をもたらす。図13に示される視覚暗号法の例では、黒は1に等しい可能性があり、白は0に等しい可能性がある。例では、IBVは00100110に等しい。XOR再構築はソリューションがブーリアンであるため使用可能である。元の生体認証ベクトル暗号化プロセスは資格暗号法を使用して行われ、この結果は、シートに記される2つのベクトルとなる可能性があり、白のノイズのみを包含する。モバイル記憶域(例えば、クライアント装置104)は該シートのうちの1つを包含し、サーバ装置102はもう1つを包含するまたはこれにアクセスする。検証プロセスは簡易なブール演算を使用して2つのシートを結合し、この結果、元の生体認証ベクトルは完全に再構築される。

【0112】

XOR演算に関連したIBVの再構築の例は、以下の表1に示される。

【0113】

10

20

【表 1】

元	0	0	1	0	0	1	1	0
共有資源 1	01	10	10	01	10	10	01	01
共有資源 2	01	10	01	01	10	01	10	01
OR - 再構築	01	10	11	01	10	11	11	01
XOR - 再構築	00	00	11	00	00	11	11	00

表 1

【0 1 1 4】

表 1 を参照すると、BOPS 実装形態の例に関連して、元の生体認証ベクトル暗号化プロセスは視覚暗号法を使用して行うことができ、この暗号化の結果は、白のノイズのみを包含するシートに記される 2 つのベクトルとなる。本明細書に述べられるように、クライアント装置 104 に関連付けられた記憶域はシートのうちの 1 つを含み、サーバ装置 102 に関連付けられた記憶域はもう 1 つを包含する。検証プロセスは簡易なブール演算を使用して 2 つのシートを結合し、この結果、元の生体認証ベクトルは完全に再構築される。

【0 1 1 5】

図 14 は、BOPS 実装形態の例に関連して、それぞれのビットが共有資源に暗号化する視覚暗号スキーム（VCS）における 2 つの共有資源（2、2）の重ね合わせの例を示す図である。図 14 に示される例では、ゼロおよび 1 ビットの共有資源の選定はランダムなプロセスである。ゼロまた 1 ビットを符号化する時、表から 1 の共有資源に対する値、および表におけるもう 1 つの共有資源に対する隣接値が得られる。プロセスの終わりに、共有資源のどちらも、元のビットについて何の手がかりも与えない。（OR または XOR を使用して）2 つの共有資源を重ね合わせることによって、元のビットの値を判断する。

【0 1 1 6】

続けて図 14 に示される例を参照すると、2 つの共有資源（2、2）の重ね合わせは視

覚暗号スキーム（VCS）で示され、この場合、それぞれのビットを共有資源に暗号化する。ゼロおよび1ビットに対する共有資源の選定はランダムなプロセスにおいて実装可能であることは留意されたい。ゼロまたは1ビットを符号化する時、表（例えば、表1）から1の共有資源に対する値、および、表におけるもう1つの共有資源に対する隣接値が得られる。プロセスの終わりに、共有資源のどちらも、元のビットについて何の手がかりも与えない。その後、例えば、ORまたはXORを使用して、2つの共有資源を重ね合わせることによって、元のビットの値を判断する。これは、（2、2）VCSに対する例である。VCSは、ランダムなプロセスの確率を変更することによって、2つ以上の共有資源に拡張できる。ランダムなプロセスの確率を0.5から0.25に変更することによって、共有資源は0.5の例に存在する2つのビットの代わりに4つのビットを有することになる。さらに、ランダムなプロセスの確率を0.125に変更することによって、それぞれの入力ビットに対して8ビットの暗号化が生じる。

10

【0117】

照合を検出することに関して、BOPS実装形態の例における1つまたは複数のモジュールは複数の初期生体認証ベクトルを利用する。そして、それぞれの生体認証に対して1つをSSL/TLSを介して通信する2つのRESTfulウェブサービス呼び出しがある。1つの呼び出しは、認証セッションにおける現行の生体認証に加えて、IBVの二等分を含むことができ、照合の強度を表す浮動小数点値を返す。もう1つの呼び出しは、1度に1つのIBV（半分）を、および現行の生体認証をもたらしことができ、照合の強度を表す浮動小数点値を返すことができる。第2の呼び出しについて、数回の連続した呼び出し、例えば、照合を判断するために1回に1つのIBVがある可能性がある。

20

【0118】

BOPS実装形態に関連した照合協約に従ったサイズ変更算出は、次のように、顔ベクトル当たり20kb、毎秒5フレームで、10秒=50ベクトル、 $50 \times 20 \text{ kb} = 1000 \text{ kb}$ となり得る。

【0119】

上で識別された実装形態に関連した照合ロジスティックの例は以下のように説明される。照合のために1,000KBがサーバに送られる。照合がない場合、次の100KBが送られ、浮動小数点値が判断されるまで以下同様に続く。1つまたは複数のBOPS実装形態において、最小閾値が定義され、浮動小数点値は少なくとも最小閾値内にある。照合アルゴリズムの例によると、現行のフレームは、200ミリ秒に加えて、サーバに対する上/下の時間の125ミリ秒を必要とする。よって、照合に加えて、フレーム送信はトランザクション速度を1フレーム当たり325ミリ秒にする。照合の上限が100ミリ秒である時、フレーム送信はおおむね425ミリ秒で行われる。失敗が生じた時、フレームのバッチ（例えば、1回に5）は送信可能であり、再び照合を試みることができる。好ましくは、1秒間未満で照合が行われるが、ある特定の好適とは言えないケースでは、数秒間など、照合により長くかかる可能性がある。

30

【0120】

本明細書に示されかつ説明されるように、本願の、柔軟性がある認証部および生体認証の不可知論的性質は、認証に使用可能であり、かつデフォルトの生体認証として定義され得る対応する認証部および生体認証を、組織が定義することを可能にする。下流のトランザクションの一部としての生体認証の仕様はないが、デフォルトの生体認証は、組織的レベル、グループユーザレベル、またはトランザクションレベルなどにおいて、1つまたは複数のユーザインターフェースを介して規定可能である。

40

【0121】

1つまたは複数の実装形態では、管理コンソールは、グラフィカルユーザインターフェースで構成可能であり、かつ、各承認済みユーザにはアクセス可能とすることができる。管理コンソールは、選択される時、デフォルトの生体認証タイプに対して構成されることになるグラフィカルコントロールを含むことができる。例えば、ACME Plumbingの組織は、ある特定のアクセスについて、ACMEの被雇用者全てに対してデフォル

50

トの生体認証に顔が使用されるものとする」と規定している。さらに、ACME Plumbingは、他の状況では、全ての顧客に対して生体認証に4本指が使用されるものとする」と規定しており、またさらに、さらなる他の状況では、10,000ドルを上回る全ての被雇用者のトランザクションに対して4本指および顔が両方共使用されるものとする」と規定している。これらのオプションは、ACME Plumbing 管理部が定義するための管理コンソールに提示される。よって、本願は、1つまたは複数の生体認証の柔軟性のある動的な応用を提供する。

【0122】

認証に関して、生体認証のための複数の情報源は、例えば、条件エンジン、メンバプロフィール、およびメンバ定義などの特定の組織セットアップにおいて使用可能である。条件エンジンはシステムにおいて定義される動的ルールに基づくことができる。例として、1Kドルを超えるいずれのトランザクションも、生体認証検証の少なくとも2つの形態を必要とする。メンバプロフィールは、ユーザロール、および対応する特権を定義する。例として、メンバプロフィール「情報セキュリティー第1の応答部」は、コミットトランザクションがある度になど、10分毎、または他の条件での認証を必要とする場合がある。メンバ定義は、組織／統合レベルにおけるデフォルトの認証を定義することができる。例えば、システムにおいて利用可能な4つのタイプの生体認証－4F、顔、虹彩－があり、かつ、特定のBOPS／企業実装形態について、デフォルトの生体認証が「顔」である場合、顔認証はデフォルトとして利用可能であり、例えば、グラフィカルユーザインターフェースによって提供され、かつ本明細書では概してBOPSアドミンダッシュボードと称されるダッシュボードなどにおいて提供可能である。また、上述されるような各条件は優先順位を指示することができる。例えば、メンバ定義は、最低優先順位と見なすことができ、条件エンジンは、最高優先順位と見なすことができる。最高優先順位は、認証方法となる。

【0123】

下記は、本願に従って、エンrollmentプロセスに関連付けられたステップの例を表す。モバイルクライアントアプリケーションで構成されるモバイルコンピューティング装置104は、生誕認証ベクトルを取得し、暗号化を行った後、API呼び出し登録を行う。特に、生体認証を取得後、BOPSサーバ102への登録呼び出しは、IBVの半分を含み、これはサーバ102によるアクセスのために記憶される。登録プロセスは、組織内でBOPS実装形態を開始するために使用可能である。本明細書に示される説明および図の多くは、クラスタとして出現するBOPS実装形態を表すが、BOPSはビジネス構成要素として構成可能であると考えられる。BOPS管理部（「BOPSアドミン」）が環境をセットアップする前に、組織はBOPSサーバ102から対応するAPI鍵について登録する。個々の開発者も、さまざまな実装形態において、API鍵を適用する。

【0124】

エンrollmentプロセス終了後に、元のサイト管理部（「元のサイトアドミン」）は追加のサイト管理部（「サイトアドミン」）を作成できる。さまざまなサイトアドミンに関連付けられることを含む、エンrollment情報は、組織に関連付けられた対応するAPI鍵に関連付け可能である。1つまたは複数の実装形態では、API登録は、エンrollmentされた元のサイトアドミン、および発行されたAPI鍵の2つのドメインに関連する可能性があり、これらは、エンrollment情報、組織、および使用ケースに基づくことができる。アプリケーション開始の了承後、登録プロセスは終了する。その後、BOPSアドミンは組織のための元のサイトアドミンを作成し、元のサイトアドミンはサイトアドミンを作成してよい（例えば、図15に示されるロール階層図を参照）。

【0125】

BOPSサービスを用いる開発プロセスの前に、開発者は例えば、BOPSアドミンコンソールにおけるオプションを使用して登録するのが好ましい。アプリケーション名を提供し、かつ開発者を識別するための質疑指向型識別機構を使用することによって、新しいアカウントは確立でき、かつAPI鍵は作成でき、これは、アプリケーション名で識別さ

れ、かつアプリケーションに関連付けられることになる。

【0126】

1つまたは複数のBOPS実装形態において、クライアント装置104上で動作するアプリケーションと、BOPSサーバ102との間の通信は、二方向SSL/TLSに加えて確立される。Genesisプロセスはかかる接続を確立し、かつ、ユーザが自身をBOPSサーバ102に対してどのように識別するかを規定することで、サーバ102が二方向SSL/TLS通信をセットアップするためのプライベート鍵を生成できるようにする。秘密の質問を提供することは、ユーザが自身を識別するための1つの機構であり、これは公理的アプローチであり、その対応するパーティ（例えば、ベンダ）は、「Genesis」フェーズ中に個人を一意に説明する質問のセットを提供できる。

10

【0127】

ユーザコンピューティング装置104上で動作するクライアントアプリケーションは、エンドユーザの装置104を識別する一意の識別子（ID）を提供するために応答可能である。アプリケーションは、ユーザとユーザの装置104との間の関係についてBOPSサーバ102に通知するために装置104および関連のAPIを使用できる。5タプルは装置104を識別するために使用できるかかる機構の1つである。

【0128】

1つまたは複数のBOPS実装形態において、システムがアタックおよびアタックベクトルを打ち負かすために使用可能である対応するRESTful呼び出しおよび／またはビヘイビアが規定される。さらに、既知のおよび未知のアタックからリアルタイムでデータを保護するためのリクエストのフォーマットが規定され、（例えば、装置112を介して）IDSにおいて提示できる。例えば、リプレイの軽減は、アクセスの妥当性検査を行うために暗号ワンタイムトークンで使用可能である。このような場合、IDSは、クライアント104およびサーバ102が互いに気づいているかを検証する3ティアであるため、サーバ102がアプリケーション層で完全に保護されるように徹底する。

20

【0129】

図16は、リプレイ防止に関連した装置および送信フローを示すブロック図1600である。図16に示されるように、暗号ワンタイムトークンによって、アクセスの妥当性検査を行い、かつリプレイ、分散サービス妨害（DDoS）および他のアタックを含む、国際標準化機構（ISO）層7サイバーアタックからアプリケーション層におけるサーバ102を保護する。トークンおよびIDSの結合は、リプレイ、分散サービス妨害（DDoS）および同様のアタックを含む、国際標準化機構（ISO）層7サイバーアタックを検出するのに有用である。トークンは1回の使用に有効であり、通常、クライアント104からサーバ102に渡された後、RESTful呼び出しを使用してBOPSに返される。

30

【0130】

1つまたは複数のBOPS実装形態における前提は、DDoS検出のために全トークンが特異的でなければならず、クライアントとサーバとの間で利用される少なくとも1つのアルゴリズムは、時間に変化する場合があります、値がクライアント間のみならずアクセス間で異なっていなければならないことを考慮に入れることである。図17は、BOPS実装形態の例による、トークンのアルゴリズムに関連付けられたステップ1700を示す高レベルフロー図である。ステップ1702では、Genesisステップ中、ウェブ、モバイル、または組み込み装置（クライアント装置104）は、トークンをリクエストするためのRESTful呼び出しを発行する。トークンは次いで、受信され、かつ、クライアント104からサーバ102への暗号化メッセージに埋め込まれる（1704）。サーバ102は、トークンを受信し、かつそのトークンをIDSに渡すことによってメッセージの妥当性検査を行い（1706）、次いで、トークンが有効であるかを検証し、かつ、作成時間と現時間との間の差異が、規定された60秒間内にあるように徹底する（1708）。

40

【0131】

50

図18は、多対多関係のGenesis／エンロールメントおよびユーザ／装置の製品を示す。モバイルクライアント104上で、それぞれのアカウントと連係される識別要素が示される。図18のサーバ側で、BOPSサーバ102は、識別属性、アカウント、およびそれぞれの識別情報と関係のある装置に関連して示される。データ暗号化を行いかつ高レベルの保証によってクライアント／サーバ通信をセキュリティ保護するために、識別情報はセキュア要素に関連するものであり、これによって、ユーザアカウント（例として、図18に示されるAliceのアカウントまたはBobのアカウント）は、該ユーザの対応する識別情報に応じて適正に認証される。

【0132】

Genesisステップを開始するために、クライアント装置104は、以下の表2に示される各値のいずれかまたは全てを規定することによって5タプルを確立するように選定することができる。IDSは、クライアントによって設定されない5つの値のいずれかを判断でき、かつ、トークンをRESTfulフォーマットでクライアントに返すことができる。クライアント104およびサーバ102は、同じ5タプルを共有し、そして、これを使用して、タイムスタンプを計算し、この結果、IDSまたはBOPSサーバ102によってSHA512が符号化されかつ比較される。計算されたタイムスタンプは5タプルに基づく時間へと後方に移動し、それぞれの呼び出しに対して一意である。

10

【0133】

それ故に、1つまたは複数の実装形態において、トークンにおける値全てが比較のためにSHA512合計に変換されるため、トークンはタイムスタンプ自体を包含しない。これによって、値を分ごとの値の間隔で変更して見境のないリプレイを防止することができる。また、トークンの分範囲は、十分に大きいエントロピー（48，771，072）を可能にするために3（60にならない）になるように構成可能であるため、試しのおよびエラーアタックを防止することができる。

20

【0134】

さらに、セマンティックエンジンは、セキュリティ管理部が、任意の国際標準の範囲外にある場合があるアタック検出および防止のための追加のカスタムパラメータを作成し、かつ、ありとあらゆるアタックに対してさらなるチェックおよび均衡を提供できるように、構成可能である。

【0135】

1つまたは複数の実装形態では、リプレイ検出は5タプルから機能させていく。上の表1に表されるような値は、サーバ102に提供可能である。代替的には、サーバ102は、値をランダムに選択できる。リプレイに従って、受け入れ可能な値の範囲およびエントロピーは最初に判断される。Genesisステップ中に規定される5タプルの値がない場合、アルゴリズムは下記の値を使用することができる。

30

【0136】

【表 2】

値	エントロピー
0 年から現在の年(2016)まで	2017
0～11 月	12
0～27 日	28
0～23 時	24
0～2 分(分のエントロピーは3であるため、値は、同時アタックの数を限定する3分についても同じものになるだけである)	3
エントロピーの合計 = $2016 \times 12 \times 28 \times 24 \times 3 = 48,771,072$	

表 2

【0 1 3 7】

実装形態の例によると、後方に回転するアルゴリズムが実行される。対応する月が現在の月に満たないまたはこれに等しい場合、年は等しくてよい。代替的には、月が現在の月を超える場合、年は戻るように回転しなければならない。これら2つのケースはアルゴリズムを示す。

【0 1 3 8】

【表 3】

Genesis の例 1			Genesis の例 2		
GMT = 2016-08-10 15:30			GMT = 2016-08-10 15:30		
	Genesis	値		Genesis	値
年	5	2011	年	5	2015
月	11	11	月	4	4
日	4	8	日	4	8
時	6	12	時	6	12
分	2	28	分	2	28

表 3

10

20

30

40

50

【0139】

例1の現在の月が8（8月）であり、かつ月のGenesisの値が11であり、 $11 > 8$ であるため、年を5の間隔で遡って調べると、年は2011になる。残りの値は、実際の日の値を下回るGenesisの倍数である。

【0140】

同じ現在の日および時間を使用する第2の例に関連して、現在の月は8（8月）であり、月のGenesisの値は4であり、 $4 \leq 8$ である。年は、5の間隔で2015に相当するまで詳しく調べられる。よって、年は2015になり、残りの値は、実際の日の値を下回るGenesisの倍数である。

【0141】

1つまたは複数のBOPS実装形態において、さまざまなレベルのデータプライバシーが提供可能であり、それぞれ、暗号化された生体認証情報を含むことで、誰かが生体認証情報を再設定するおよび／または危険にさらすことを妨げるようにすることができる。1つのプライバシーレベルは、非生体認証データ全てがプレーンテキストで記憶される（パッシブにされる）と定義することができる。これによって、使用パターンおよび認証記録の報告および解析が簡略化され、またこれには、否認不可、場所、日付、およびファセット検索などの他の因子が含まれ得る。例えば、2016年6月にClevelandで認証の試みが多数失敗に終わり、個人および装置に関連する情報が提供可能であることが比較的容易に理解できる。この第1のプライバシーレベルは、プレーンテキストのパッシベーション処理されたデータに基づいて動作する洗練されたツールに応じて実現可能である。別のより高いレベルのプライバシーは、全ての非生体認証データが暗号化されたフォーマットに記憶されるが、クライアントごとの別個の解読鍵を必要としないと定義することができる。よって、クライアント装置104は、同じ解読鍵を使用するように構成可能であり、このことは、侵入者がアクセスすることができない、または、解読鍵にアクセスできない可能性が最も高い点で、先に説明した第1のレベルのプライバシーより安全と考えられる。なおより高いレベルのプライバシーは、全ての非生体認証データが暗号化されたフォーマットで記憶され、かつ解読鍵がそれぞれの識別情報ごとに一意であることを必要とする可能性がある。これによって、それぞれのユーザのデータが生体認証に関連付けられた鍵で暗号化されるため、プライバシーおよび分離が高められる。高いレベルのプライバシーでは、例えば、個人的に識別可能な情報（「PII」）を含むユーザデータが、ことによるとメモリ内で照合を行う時を除いて、常にクライアント装置104上で暗号化されると想定される。1つまたは複数のBOPS実装形態では、ユーザは、トランザクションを承認するように認証を行い、かつ、ユーザデータを解読する（例えば、信用証明書またはファイルなどにログインする）ために認証を行う。また、保存データ（例えば、パッシブデータ）は、サーバコンピューティング装置102上でおよびクライアント装置104上で常に暗号化される。プレーンテキストデータは、照合プロセスが行われている時のメモリだけに存在するのが好ましい。

【0142】

1つまたは複数のBOPS実装形態において、Genesisフローに対する事実上任意のカスタマイズを可能にするためにオープンプラットフォームが提供される。Genesisのいくつかの例は、アクティブディレクトリにアクセスするためのユーザ名およびパスワード、電子メールまたはテキストメッセージの妥当性検査、または個人の識別を含むことができ、これらは、運転免許証、出生証明書、パスポート、社会保障番号、または他の適した信用証明書などに応じて、物理的に検証可能である。

【0143】

ユーザアカウントの事前登録は、ビジネスルールを実装するバッチプロセスにおいて行うことができ、組織のポリシーおよび手続きは、これらのビジネスルールの一因となる可能性がある。ビジネスルールは、アクセス管理プラットフォームと統合可能であり、このプラットフォームは、特権のレベル、およびロールの管理側におけるいくつかの特定の必要性に適合させるようにする他の属性を判断するグループまたはディレクトリにユーザを編

成する。これによって、BOPSサーバ102によってアクセスされるメンバ定義の入力として適用可能である、メンバプロフィール（例えば、ユーザプロフィール、アドミンプロフィール、管理者プロフィール、およびスーパーアドミンプロフィール）の定式化を、開発者が構築できるようにする柔軟性がもたらされる。本願によるGenesisプロセスは、リスク管理に対する完全な従属性を形成でき、それ故に、下流処理を判断できる。

【0144】

図19Aは、単一のクライアント装置104においてエンロールメントを開始する複数のユーザに関連付けられた装置およびステップ1900を示す。ユーザと装置104との関係は「多対多」(M:M)とすることができる。第1のエンロールメントステップが追加可能である(A1 生体認証エンロールメントを開始する、A2 エンロールメントをリクエストする(x, 509)、A3 エンロールメント要件を返す、A4 アカウント登録をリクエストする(dev ID、user ID+1/2 IBV)、A5 登録を返す)。これらのステップは、第2のユーザに対して繰り返され得る(B1~B5)。多対多関係は、Genesisおよびエンロールメントの分離に応じて生じ得る。また、Genesisによる識別された主体は、多くの生体認証で何度もエンロールすることができる。クライアント/サーバ通信を開始するために、ユーザは、クライアント装置上で自身の生体認証をキャプチャし、これによって、クライアント装置に対して発行された一意のクライアント証明書のエンロールメントプロセスが実行に移される。エンロールメントのセキュリティ部が済むと、ユーザの生体認証情報の登録は実施され、これによってエンロールメントプロセスは終了する。ユーザは多くの装置(クライアント)を有してよく、装置(クライアント)は多くのユーザを有してよい。装置(クライアント)は多くの生体認証をサポートすることができる。

【0145】

図19Bは、複数のユーザアカウントに関する情報を記憶するクライアント装置104から認証セッションを開始するユーザの1つの例、Aliceに関連した装置およびステップ1910を示す。図19Bに示される例では、Aliceは認証セッションを始め(1)、クライアント装置104上で動作するアプリケーションは生体測定による認証をリクエストする(2)。生体測定による認証の完了(3)後、クライアント装置104上で動作するアプリケーションは、装置104が、TLSを介してAliceの識別属性を送るように構成する(4)。その後、BOPSサーバ102は全てのエンロールメント要素の保全性を考慮して認証リクエストを処理し、結果を返す(5)。

【0146】

図19Bに示される例を参照すると、Aliceが誤ってBobのアカウントを使用して認証セッションを開始する場合には、クライアント装置104はいずれのリクエストもサーバに返さないが、これは、CBVが、エンロールメント中に作成されたIBVと異なることになるからであり、認証は成功しないことになる。

【0147】

図19Cは、ユーザのアカウントの取り消しに関連付けられた装置およびステップ1920の例を示す。図19Cに示される例では、3人のユーザ(Eve、Bob、およびAlice)に関連付けられた情報が示される。1つまたは複数の取り消しルールは、管理側のグラフィカルユーザインターフェースによって構成されるアドミンコンソールなどによって、ユーザごとに定義可能である。(同様に生体測定による認証が可能である)管理部に関連付けられたルールは、ルールを実装することを担うことができる。図19Cに示される例では、Aliceのアカウントはアクティブな証明書を有し、Bobのアカウントはトランスポートセキュリティレベルでブロックされる期限切れの証明書を有し、EveのアカウントはBOPSアドミンによって取り消されている。より詳細には、Eveの証明書がBOPSサーバ102を介して取り消されており(1)、認証リクエストはEveのアカウントに関連付けられたクライアント装置104から受信される(2)。BOPSサーバ102は、Eveのアクセスがブロックされることを表すメッセージまたは他の適したコンテンツを返す(3)。Bobの証明書に関して、90日の期間が定義

され、この期間後、B o bの証明書は期限切れになる（「T T L」）（4）。その後、認証リクエストはB o bのアカウントに関連付けられたクライアント装置1 0 4から受信され（5）、E v eのケースと同様に、B o bのアクセスがブロックされることを表すメッセージまたは他の適したコンテンツがB O P Sサーバ1 0 2によってクライアント装置1 0 4に送信される（6）。A l i c eのアカウントに関して、追加の9 0日の期間の延長期間が設けられ（7）、認証リクエストはA l i c eのアカウントに関連付けられたクライアント装置1 0 4から受信される（8）。B O P Sサーバ1 0 2は、A l i c eが認証されることを、本明細書に示されかつ説明されるような認証結果を表すメッセージまたは他の適したコンテンツを返す（9）。

【0 1 4 8】

本明細書に示されかつ説明されるモジュールに関連して解決される問題のうちの1つは、リプレイアタックの防止である。1つまたは複数の実装形態において、D D o S検出について、典型的には、サーバ上のプロファイルを共通名（C N）フィールドにおける識別情報に連係する識別子であるあらゆるトークンは特異的である。クライアント1 0 4とサーバ1 0 2との間のアルゴリズムは、時間が増加し得ること、および、値がクライアント1 0 4間のみならずアクセス間で異ならなければならないことを考慮に入れる。

【0 1 4 9】

1つまたは複数の実装形態において、証明書の分散は以下のように働く。X. 5 0 9証明書はクライアント装置1 0 4にインストールされるアプリケーションソフトウェアに依拠することを含んで、クライアント装置1 0 4にあらかじめロードされる。G e n e s i sプロセスの前に、クライアント1 0 4は、（本明細書に示されかつ説明されるように）タプルのいずれかまたは全てを規定することによって、5タプルの値を確立する。エンロールメントプロセス中、クライアント1 0 4はB O P Sサーバ1 0 2からトークンをリクエストするためにR E S T f u l呼び出しを発行する。トークンは、受信される時、サーバに対するクライアントの暗号化メッセージに埋め込まれる。サーバは、トークンを受信し、かつ、作成時間と現時間との間の差異が、規定された6 0秒間以内にあるように徹底することによってメッセージの妥当性検査を行う。サーバ1 0 2は、5タプルの値のどれが無くなっているかを判断し、かつ、トークンをR E S T f u lフォーマットでクライアントに返す。クライアント1 0 4およびサーバ1 0 2は、同じ5タプルの値を共有し、そして、この値を使用して、タイムスタンプを計算し、この結果、例えば解析に応じて、S H A 5 1 2がI D Sによって符号化されかつ比較される。例えば、本明細書に説明されるように、計算されたタイムスタンプは5タプルに基づく時間へと後方に移動し、それぞれの呼び出しに対して一意である。

【0 1 5 0】

本願は、クライアント証明書の時間の長さを有効のままであるように（有効時間またはT T L）構成できる。認証されたユーザの取り消された証明書は、新しい証明書と暗黙的に置き換え可能である。よって、T T Lは、ユーザ認証をサポートするためにI B VおよびC B Vと併せて働く「ベルトおよびサスペンダー」式のアプローチである。トークンの取り消しは、ユーザロールに対して条件付きとすることもでき、特定の要件を行う他の因子は承認に必要である。例えば、条件yおよび／またはzが満たされない場合など、財務トランザクションに対する認証の試みが1回またはx回失敗した後に、証明書はブロックされ得る。

【0 1 5 1】

図2 0 Aは、クライアント装置1 0 4とB O P Sサーバ1 0 2との間のクライアント証明書の初期化、検証、および確認に関連付けられたステップ2 0 0 0を実証することを簡略的に示す図である。クライアント署名リクエスト（「C S R」）の処理に関連付けられたステップは、公開—プライベート鍵ペアをクライアント装置1 0 4において生成し、公開鍵、およびB O P Sサーバ1 0 2に送信される主体名を署名すること（本明細書では概して「所有証明」を行うことと称される）を含むことができる。本明細書に述べられるように、クライアントは二方向S S Lを使用して登録アカウントリクエストを送る。証明書の

主体名をチェックし、BOPS認証局(CA)のプライベート鍵によってクライアントリクエストに署名し、およびOTP機構によってクライアント証明書のパスワードを生成した後、BOPSサーバ102はクライアント証明書パスワードをクライアント装置104に返す。登録されたクライアントは、証明書の署名をチェックし、かつ、p12コンテナを作成して、パスワードではなく、クライアントプライベート鍵および署名済み証明書を記憶する。OTP機構がそれぞれのクライアントリクエストに対して1回使用のパスワードを生成するため、パスワードはクライアント装置に一度も記憶されないのが好ましい。

【0152】

図20Bは、サードパーティのサーバおよびBOPS統合におけるクライアント証明書プロセス2010の例を示す。例えば、図20Aに示されるようなCSRプロセスは、広く実証され、ユーザエンロールメントで始められる。図20Bに示される例では、「ユーザアカウントを登録する」は、Genesisおよびエンロールメントに関連付けられたステップを説明するために使用され、クライアント証明書は識別属性を表し、アカウントは識別構成要素を表す。

【0153】

図20Bに示される実装形態の例では、ユーザがエンロールメントプロセスを開始し、かつ自身の生体認証情報をアカウント登録リクエストによってBOPSサーバ102に送った後、鍵ペア/CSR生成はクライアント104においてトリガされる。登録プロフィールリクエストが受信されると、BOPSサーバ102はこのリクエストをさらに、プロフィール妥当性検査を表す図20Bに示されるように、(サードパーティの企業によって用いられるアクセス管理ソリューション/プラットフォームとすることができる)アクセス管理アダプタに、その後さらに、アカウントログイン検証および妥当性検査のためにサードパーティのサーバに送る。サードパーティのサーバは、ログインデータの妥当性検査後認証トークンを提供し、その後、妥当性検査の結果をアクセス管理アダプタに送り返し、これによって、認証結果および認証トークンが再びBOPSサーバ102に回されて、アカウント/プロフィール登録を終了する。BOPSサーバ102は、認証トークンを暗号化し、生体認証データを記憶し、BOPS CAによってCSRに署名し、暗号化された認証トークンをクライアントアプリケーションに送る。これは、生体測定による認証に応じてより高度の検証を行うために、既にレポジトリに何十億ものアカウントを蓄積している企業(例えば、銀行)と統合した実装の例を表す。

【0154】

1つまたは複数の実装形態において、quick response code (QRコード(登録商標))は、本明細書に示されかつ説明される1つまたは複数のモジュールの実行をトリガするために使用可能である。例えば、ビジネスパートナー(例えば、銀行)のログインページは、対応するセッション時機識別子を包含するQRコード(登録商標)画像を表示するように構成可能である。クライアントコンピューティング装置104上で実行するMCAは、QRコード(登録商標)をスキャンし、該コードがセッションにタッチされるように、セッションを信号に登録し、本明細書における教示によるユーザの生体認証で認証するための、1つまたは複数のモジュール(例えば、認証ウィザード)を実行することができる。図21は、QRコード(登録商標)認証フロー2100の例を示し、ここで、サードパーティのサーバは、BOPSサーバ102によるセッション時機に登録し、それに応じて、新しい認証セッションに使用可能な情報はBOPSサーバ102によってサードパーティのサーバに提供可能であり、この情報はQRコード(登録商標)の範囲内で提供(例えば表示)可能である。サードパーティのサーバは、セッションステータス情報に対する1つまたは複数のリクエストを送信することができる。図21における(「アクタ」と指定される)ユーザは、QRコード(登録商標)をスキャンし、かつ、BOPSサーバ102によるセッションに登録し、これは、外部のサードパーティのサーバに通知可能である。本明細書に示されかつ説明されるような生体測定による認証が行われると、ユーザセッションは、サードパーティのサーバとによるのを含めて確立可能である。

10

20

30

40

50

【0155】

上述される主題は、例示としてのみ提供され、限定するものと解釈されるべきではない。例示されかつ説明される実施形態および応用の例に従うことなく、かつ、以下の特許請求の範囲のそれぞれおよびいずれかにおいて示されるように、本発明の真の趣旨および範囲から逸脱することなく、本明細書に説明した主題に対してさまざまな修正および変更をなすことが可能である。

【符号の説明】

【0156】

- 102 BOPSサーバ
- 104 クライアント装置
- 106 サードパーティのサーバ
- 108 稼働状況監視装置
- 110 解析エンジン
- 112 クライアント装置
- 902 BOPSクラスタ
- 904 ロードバランサクラスタ
- 906 永続クラスタ
- 908 監視クラスタ

10

【図1】

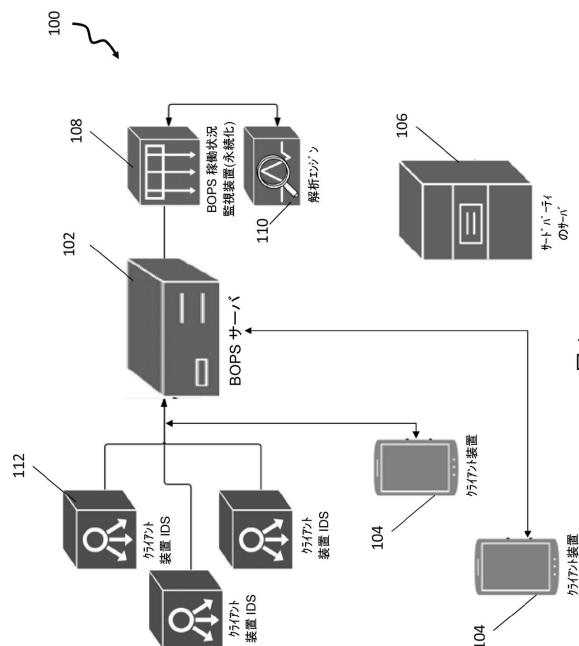


図 1

【図2】

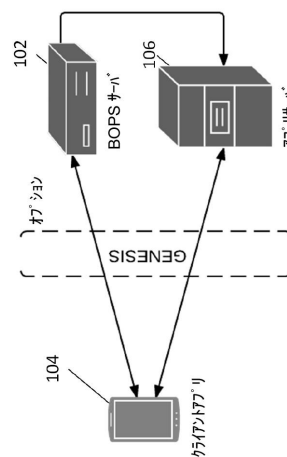


図 2

【図 3】

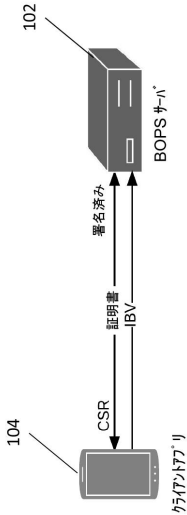


図 3

【図 4】

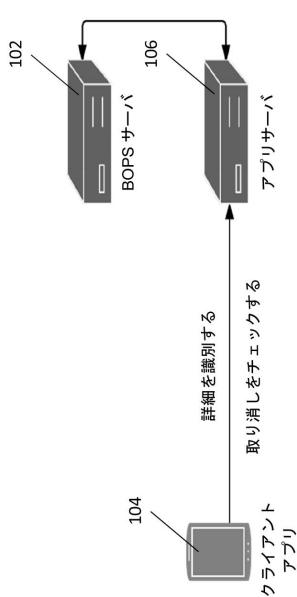


図 4

【図 5】

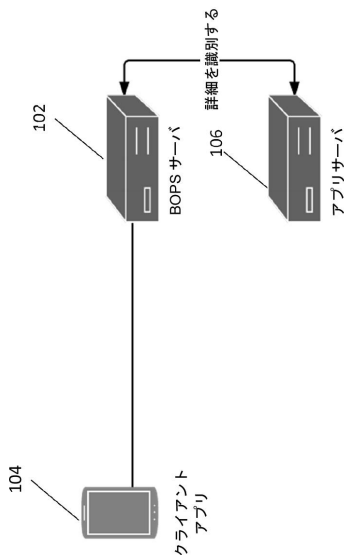


図 5

【図 6】

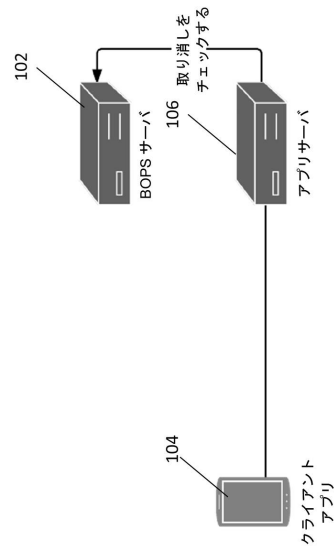


図 6

【図 7 A】

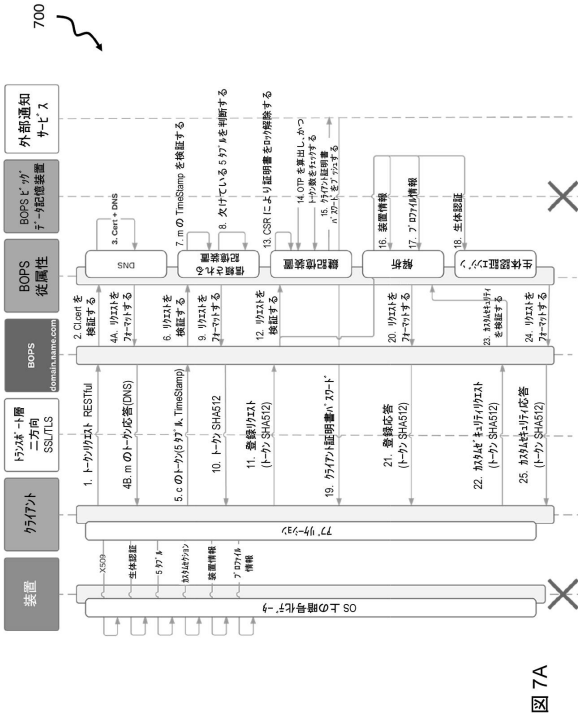


図 7A

【図 7 B】

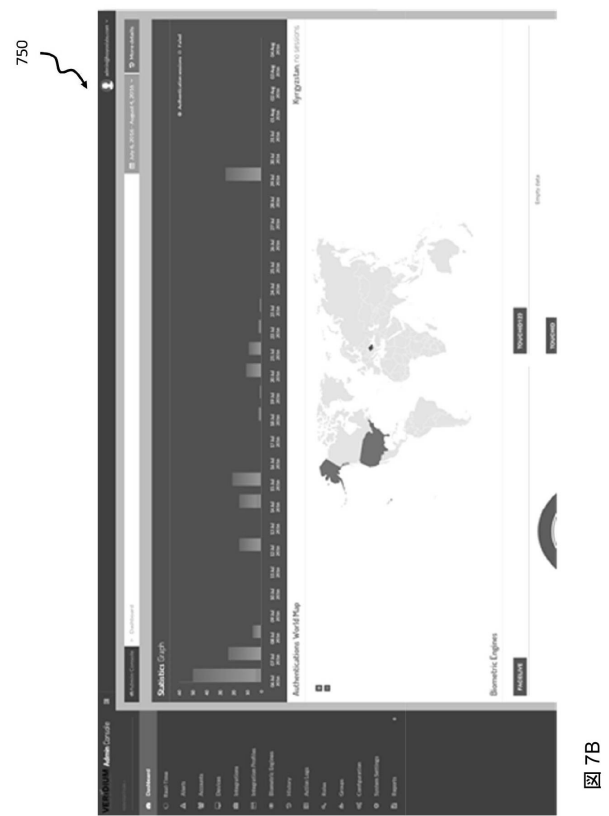


図 7B

【図 8】

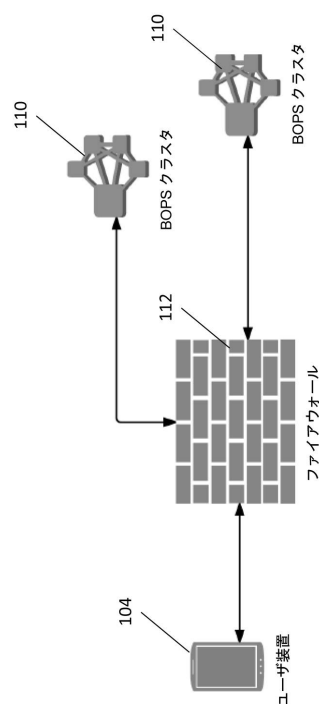


図 8

【図 9】

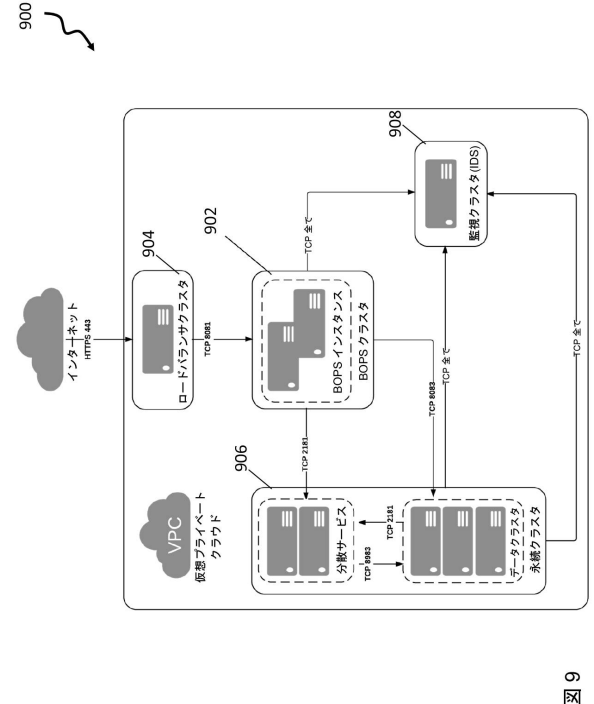


図 9

【図10A】

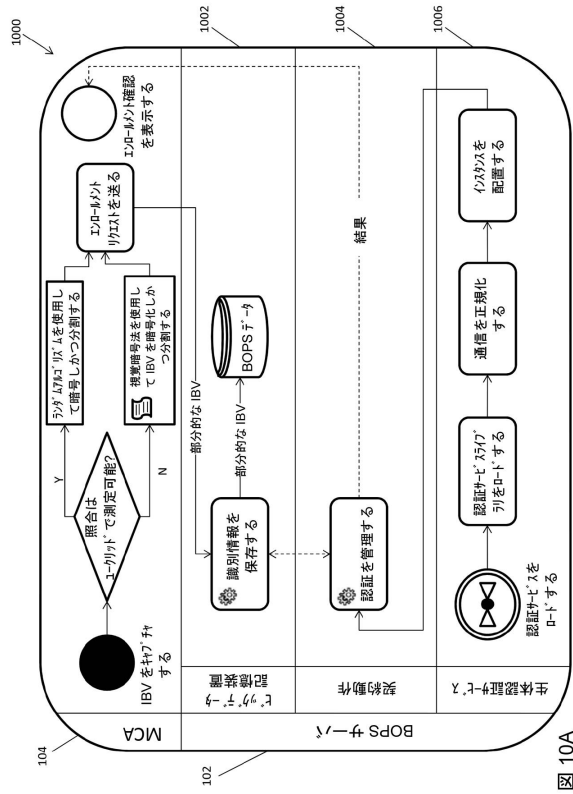


図 10A

【図10B】

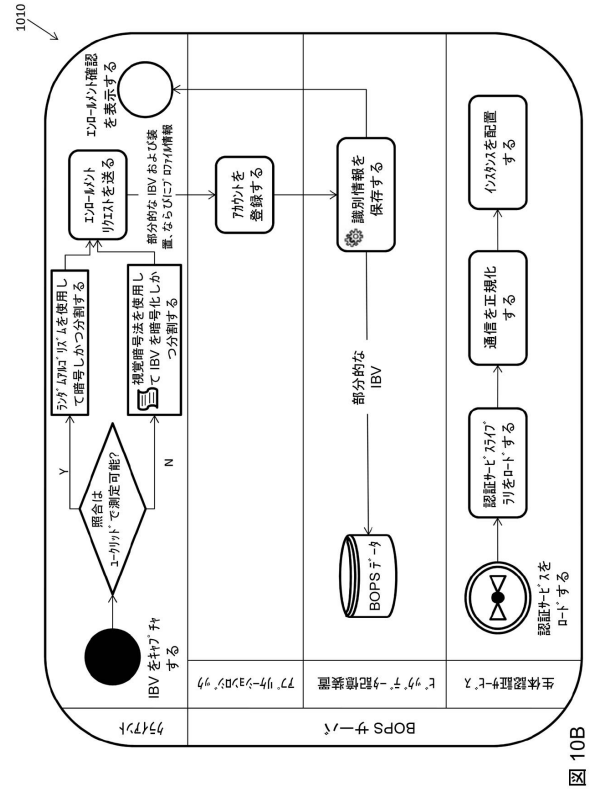


図 10B

【図11】

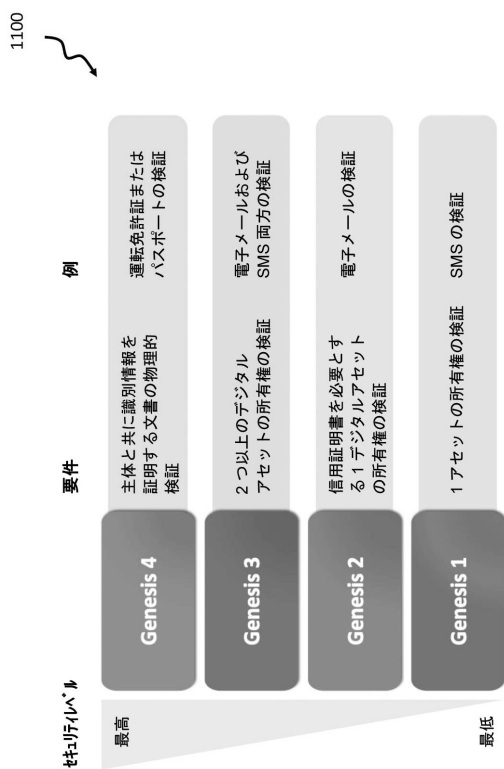


図 11

【図12】

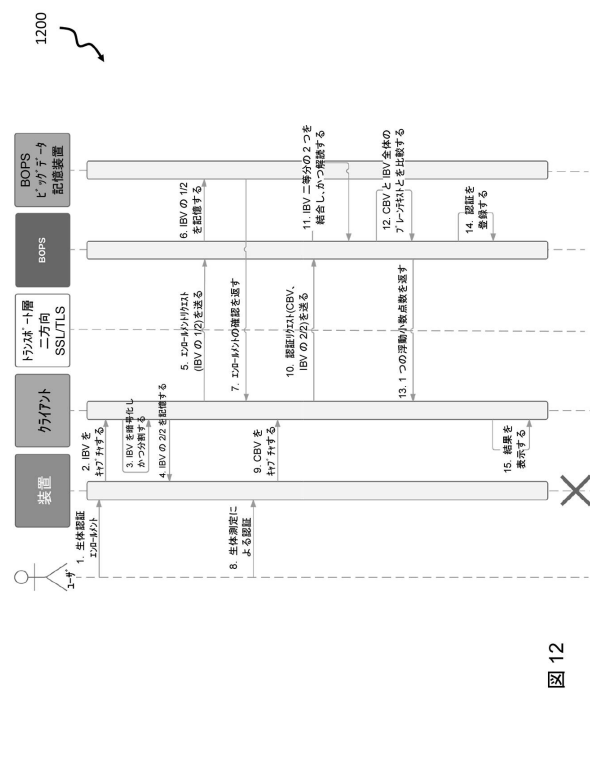
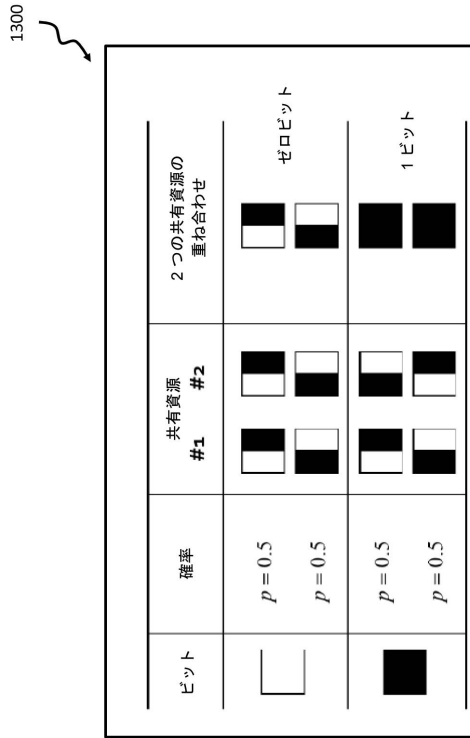
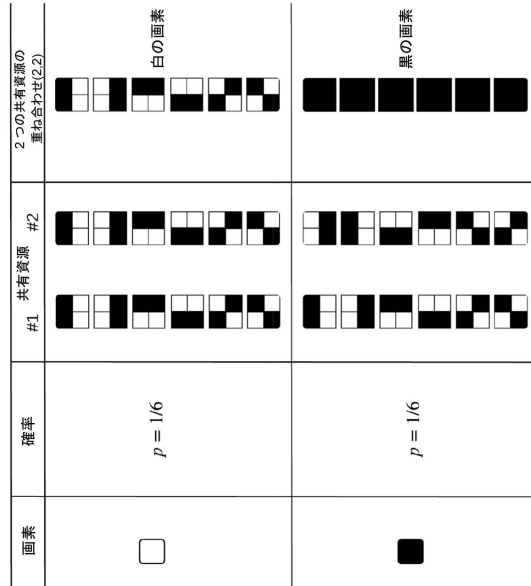


図 12

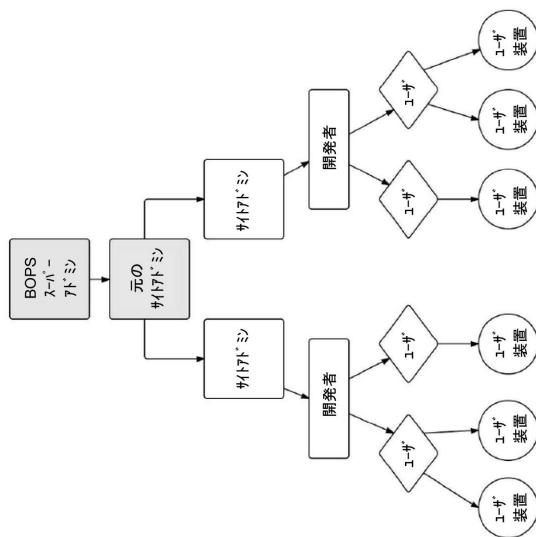
【図 1 3】



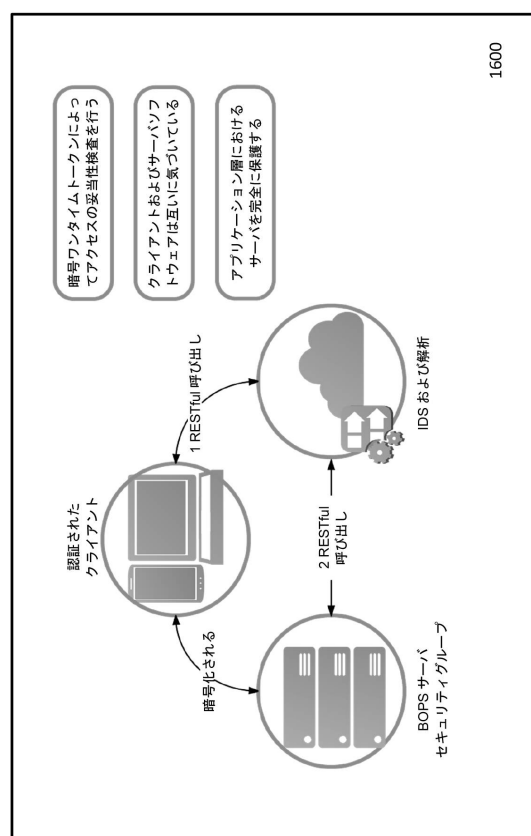
【図 14】



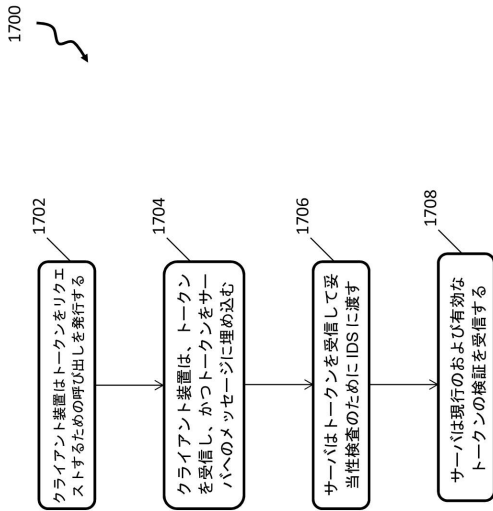
【図 15】



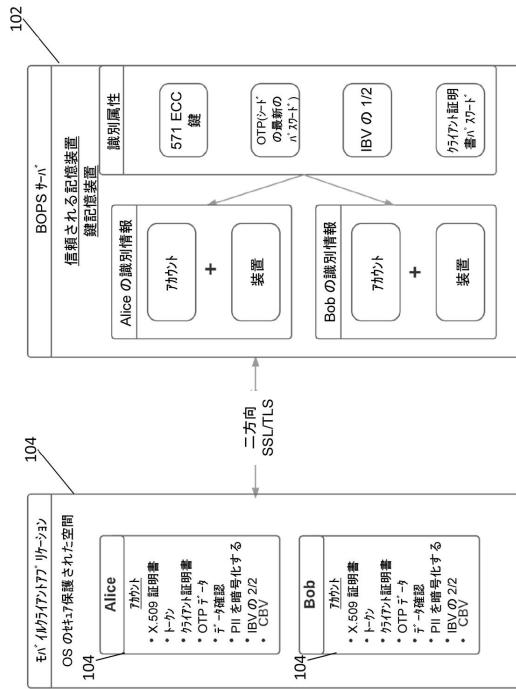
【图 16】



【図 17】

17

【図 18】



18

【図 19 A】

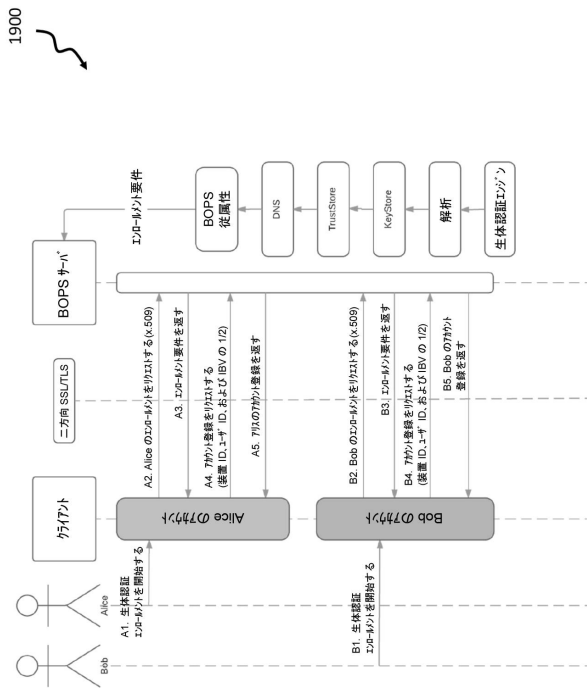


図 19A

【図 19 B】

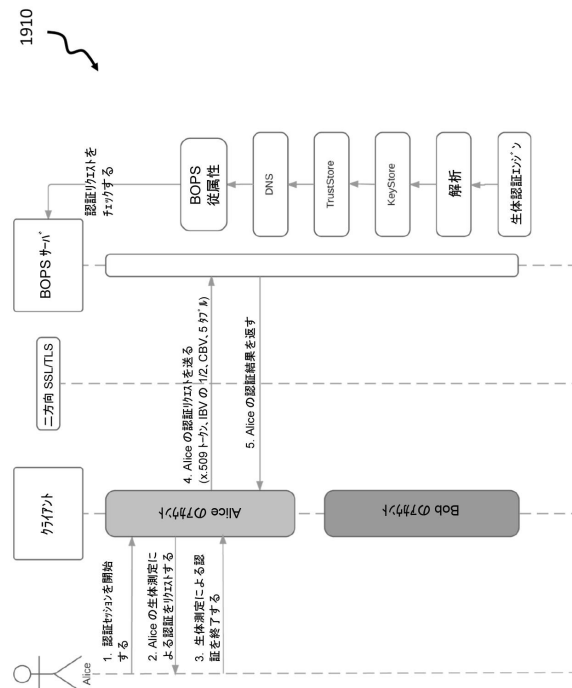


图 19B

【図 19 C】

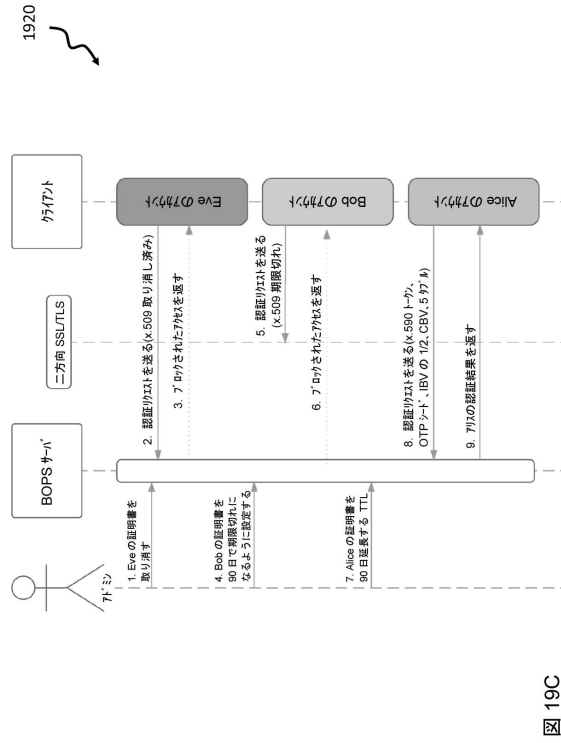


図 19C

【図 20 B】

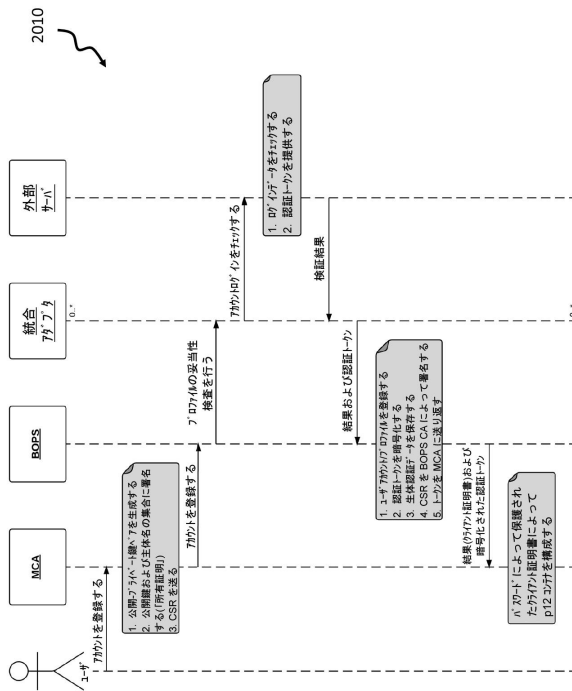


図 20B

【図 20 A】

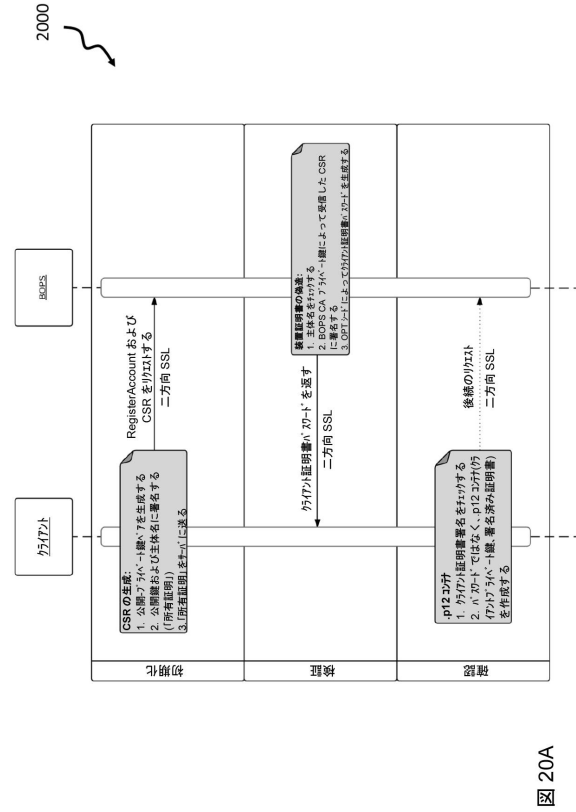


図 20A

【図 21】

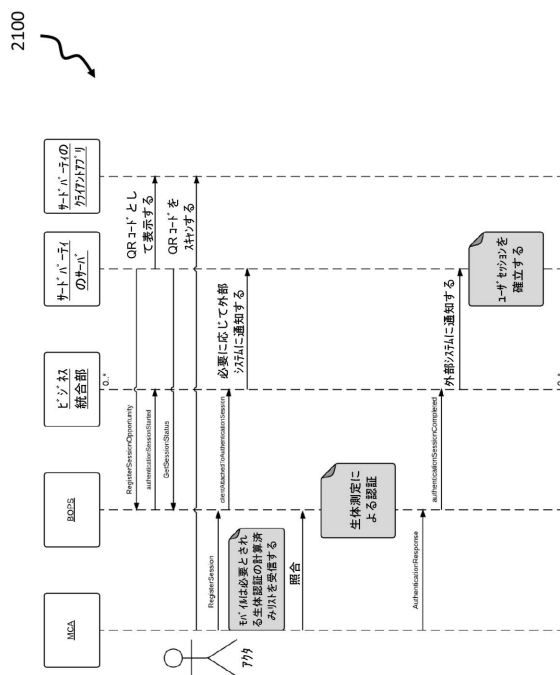


図 21

フロントページの続き

- (72)発明者 ストレイト, スコット
アメリカ合衆国 マサチューセッツ州 02171, クインシー, 100 ハンコック ストリート テンス エフエル.
- (72)発明者 マザー, ジョナサン, フランシス
イギリス国 オックスフォード オーエックス4 4キューエス, イースターン アベニュー 29
- (72)発明者 オスマン, アセム
アメリカ合衆国 マサチューセッツ州 01545, シュルーズベリー, アローウッド ドクター 55
- (72)発明者 ドゥミトラン, イオナット
ルーマニア国 ブチャレスト 060891, エーピー. 53, イー5, ナンバー 20, ドレプタチ ストリート
- (72)発明者 ウッド, トーマス
イギリス国 オーエックス4 6アールエフ, サムファイア ロード オックスフォード 21

審査官 児玉 崇晶

- (56)参考文献 特開2009-289253 (JP, A)
特表2009-533735 (JP, A)
特開2012-181802 (JP, A)
特開2005-122478 (JP, A)
吉浦 紀晃, 生体情報による認証への一方向関数の応用, 電気学会論文誌C, 日本, (社)電気学会, 2004年 8月 1日, Vol. 124 No. 8, pp.1538-1545

- (58)調査した分野(Int.Cl., DB名)
H04L 9/32
G06F 21/32