

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7426475号
(P7426475)

(45)発行日 令和6年2月1日(2024.2.1)

(24)登録日 令和6年1月24日(2024.1.24)

(51)国際特許分類		F I	
H 0 4 L	9/32 (2006.01)	H 0 4 L	9/32 2 0 0 Z
G 0 6 F	21/33 (2013.01)	G 0 6 F	21/33
G 0 6 F	21/64 (2013.01)	G 0 6 F	21/64
G 0 6 F	21/56 (2013.01)	G 0 6 F	21/56 3 5 0
請求項の数 13 (全31頁)			
(21)出願番号	特願2022-508466(P2022-508466)	(73)特許権者	520107951
(86)(22)出願日	令和2年8月17日(2020.8.17)		アメリカン エクスプレス トラヴェル
(65)公表番号	特表2022-545627(P2022-545627 A)		リレイテッド サーヴィシーズ カンパニ
(43)公表日	令和4年10月28日(2022.10.28)		ー, インコーポレイテッド
(86)国際出願番号	PCT/US2020/046652		AMERICAN EXPRESS TR
(87)国際公開番号	WO2021/041075		AVEL RELATED SERVIC
(87)国際公開日	令和3年3月4日(2021.3.4)		ES COMPANY, INC.
審査請求日	令和4年4月6日(2022.4.6)		アメリカ合衆国 1 0 2 8 5 - 4 9 0 0
(31)優先権主張番号	16/555,638		ニューヨーク州、ニューヨーク、ヴィー
(32)優先日	令和1年8月29日(2019.8.29)		ジー ストリート 2 0 0
(33)優先権主張国・地域又は機関	米国(US)	(74)代理人	100083116
			弁理士 松浦 憲三
		最終頁に続く	

(54)【発明の名称】 分散化されたデータ認証

(57)【特許請求の範囲】

【請求項1】

プロセッサ及びメモリを含むコンピューティングデバイスと、
前記メモリに記憶された機械可読命令と、を含み、前記機械可読命令は、前記プロセッ
サによって実行されると、前記コンピューティングデバイスに少なくとも、
データ項目のIDキーを生成することと、
前記データ項目の認証の要求を、セキュリティ又は信頼性を評価するために実行される
セキュリティサービスに送信することであって、前記要求は、前記IDキー及び前記デー
タ項目を含む、ことと、
前記セキュリティサービスから前記データ項目が確認されたことを示す単数又は複数の
アサーションを含む確認済みクレームを受信することと、
身分証明書を生成することであって、前記身分証明書は、前記データ項目の前記IDキ
ー及び前記確認済みクレームを含み、前記IDキーは前記身分証明書に関連づけられた個
人又はエンティティを一意に識別することと、
前記身分証明書を分散型台帳に保管することと、を行わせる、システム。

【請求項2】

前記機械可読命令は、前記コンピューティングデバイスによって実行されると、更に、
前記コンピューティングデバイスに少なくとも、
前記データ項目の要求を受信することと、
前記要求への応答を送信することであって、前記応答は前記データ項目及び前記IDキ

一を含む、ことと、
を行わせる、請求項 1 に記載のシステム。

【請求項 3】

前記 ID キーは第 2 の ID キーであり、
前記身分証明書は第 2 の身分証明書であり、
前記データ項目の認証の前記要求は、認証の第 2 の要求であり、
前記機械可読命令は、更に、前記コンピューティングデバイスに少なくとも、
前記機械可読命令のオペレータの前記 ID の認証の要求を認証サービスに送信することと、

前記認証サービスから第 1 の ID キー及び確認済みクレームを受信することと、
第 1 の身分証明書を作成することであって、前記第 1 の身分証明書は、前記第 1 の ID キー及び前記確認済みクレームを含む、ことと、

前記第 1 の身分証明書を分散型台帳に記憶することと、を行わせ、
前記データ項目の認証の前記第 2 の要求は、前記第 1 の身分証明書が前記分散型台帳に記憶されるのに続いて送信される、請求項 1 又は 2 に記載のシステム。

【請求項 4】

前記機械可読命令は、前記プロセッサによって実行されると、更に、前記コンピューティングデバイスに少なくとも、

前記データ項目に一意に関連付けられた非対称キー対を生成することを行わせ、
前記身分証明書は、前記非対称キー対の公開キーを更に含む、請求項 1 乃至 3 のいずれか 1 項に記載のシステム。

【請求項 5】

前記機械可読命令は、前記プロセッサによって実行されると、更に、前記コンピューティングデバイスに少なくとも、

前記公開キーで暗号化された暗号化トークンを含む確認要求を受信することと、
暗号化されていないトークンを生成するために、前記非対称キー対の秘密キーを使用して前記暗号化されたトークンを復号化することと、

前記秘密キーを使用して、前記暗号化されていないトークンの暗号化署名を作成することと、

前記暗号化されていないトークン及び前記暗号化署名を含む確認応答を提供することと、
を行わせる、請求項 4 に記載のシステム。

【請求項 6】

前記データ項目がネットワークアドレスである、請求項 1 乃至 5 のいずれか 1 項に記載のシステム。

【請求項 7】

前記データ項目がファイルである、請求項 1 乃至 5 のいずれか 1 項に記載のシステム。

【請求項 8】

コンピュータにより行われる、

データ項目の認証要求を受信することであって、前記認証要求は、ID キー及び前記データ項目を含む、ことと、

前記データ項目が少なくとも一つの確認規則に準拠していることを決定する、前記確認規則は、データ項目が安全であるというアサーションを行うための要件を含み、前記データ項目が前記要件を満たすか否かにより前記決定をすることと、

前記データ項目の確認済みクレームを生成することであって、前記確認済みクレームは、前記 ID キーが前記データ項目に関連付けられており、前記データ項目が前記少なくとも一つの確認規則に準拠していることを示す、ことと、

前記データ項目の認証の前記要求への応答として前記確認済みクレームを提供することと、

前記 ID キー及び前記確認済みクレームを含む身分証明書を作成することと、

前記身分証明書を分散型台帳に登録することと、を含む、方法。

【請求項 9】

前記 ID キーは第 2 の ID キーであり、

前記少なくとも一つの確認規則は、前記データ項目が認証されたエンティティから発信されていることを示し、

前記認証要求は、前記認証されたエンティティに関連付けられた第 1 の ID キーを更に含み、

前記データ項目が前記少なくとも一つの確認規則に準拠していることを決定することは、前記認証要求が前記認証されたエンティティから発信されていることを、少なくとも部分的に前記第 1 の ID キーに基づいて確認することを更に含み、

前記確認済みクレームの生成は、前記認証要求が前記認証済みエンティティから発信されているとの確認に応答して発生する、請求項 8 に記載の方法。

10

【請求項 10】

少なくとも部分的に前記第 1 の ID キーに基づいて、前記認証要求が前記認証されたエンティティから発信されていることを確認することは、

前記第 1 の ID キーに関連付けられた身分証明書を取得することであって、前記身分証明書には、それぞれの非対称キー対の公開暗号化キーが含まれている、ことと、

暗号化されたトークンを作成するために、前記公開暗号化キーを使用してトークンを暗号化することと、

前記認証要求を送信した発信元エンティティに前記暗号化されたトークンを送信することと、

20

前記それぞれの非対称キー対の秘密キーで作成された前記トークン及びデジタル署名を受信することと、

前記公開暗号化キーを使用して前記デジタル署名を確認することと、を更に含む、請求項 9 に記載の方法。

【請求項 11】

前記少なくとも一つの確認規則は、前記データ項目が指定されたセキュリティポリシーに準拠していることを示し、

前記データ項目が前記少なくとも一つの確認規則に準拠していることを決定することは、前記データ項目のセキュリティ分析を実行することを更に含む、請求項 8 乃至 10 のいずれか 1 項に記載の方法。

30

【請求項 12】

前記データ項目がネットワークアドレスである、請求項 8 乃至 11 のいずれか 1 項に記載の方法。

【請求項 13】

前記データ項目がファイルである、請求項 8 乃至 11 のいずれか 1 項に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

本願は、2019 年 8 月 29 日に出願され、「分散化されたデータ認証」と題された米国特許出願第 16 / 555, 638 号の優先権及び利益を主張する。

40

【背景技術】

【0002】

多くのセキュリティ脅威は、ユーザをだまして、信頼できるソースによって提供されたデータにアクセスしていると信じ込ませることに依存している。実際には、ユーザはデータ自体がマルウェアであるか、又はマルウェアを含んでいることに気付くことがよくある。また、データにアクセスすると、ユーザのコンピューティングデバイスにマルウェアがインストールされる。

【0003】

例えば、一般的なセキュリティの脅威はフィッシングとして知られており、悪意のある

50

攻撃者（「フィッシング詐欺師」）が、有効なウェブサイトと視覚的に区別できない偽のウェブサイトを作成する。個人が偽のウェブサイトアクセスすると、その個人のデータが収集されたり、コンピュータを悪用しようとしてマルウェアがブラウザに読み込まれたりする可能性がある。ターゲットが偽のウェブサイトアクセスするように誘導するために、フィッシング詐欺師は、有効なウェブサイトのネットワークアドレスに類似しているか、又は関連しているように見えるネットワークアドレスを有するリンクを作成することができる。

【0004】

同様の例として、別の一般的なセキュリティの脅威は、マルウェアを含むファイルの配布である。マルウェアファイルは、スプレッドシート、プレゼンテーション、レポート、オーディオファイル、画像ファイル、又はビデオファイルなど、ユーザが通常開いたり、対話したり、消費したりする正当なファイルに偽装されている可能性がある。ファイルは、信頼できるエンティティによって書かれた又は作成されたものとして偽装又は提示される場合もある。その結果、ユーザがだまされて、実際には、ユーザは自分のコンピュータにマルウェアをロードさせている場合、信頼できるソースから発信された無害なファイルであると信じるファイルを開く可能性がある。

【発明の概要】

【課題を解決するための手段】

【0005】

本開示の様々な実施形態は、プロセッサ及びメモリを含むコンピューティングデバイスと、メモリに記憶された機械可読命令と、を含むシステムを含み、機械可読命令は、プロセッサによって実行されると、コンピューティングデバイスに少なくとも、データ項目のIDキーを生成することと、データ項目の認証要求をセキュリティサービスに送信することとであって、この要求は、IDキーとデータ項目を含む、ことと、セキュリティサービスからデータ項目の確認済みクレームを受信することと、身分証明書を生成することとであって、身分証明書は、データ項目のIDキーと確認済みクレームを含む、ことと、身分証明書を分散型台帳に記憶することと、を行わせる。システムの一部の実装形態では、機械可読命令は、コンピューティングデバイスによって実行されると、更に、コンピューティングデバイスに少なくとも、データ項目の要求を受信することと、要求への応答を送信することとであって、応答はデータ項目及びIDキーを含む、ことと、を行わせる。システムの一部の実装では、IDキーは第2のIDキーであり、身分証明書は第2の身分証明書であり、データ項目の認証要求は、認証の第2の要求であり、機械可読命令は、更に、コンピューティングデバイスに少なくとも、機械可読命令のオペレータのIDの認証要求を認証サービスに送信することと、認証サービスから第1のIDキー及び確認済みクレームを受信することと、第1の身分証明書を生成することとであって、身分証明書は、IDキー及び確認済みクレームを含む、ことと、第1の身分証明書を分散型台帳に記憶することとであって、データ項目の認証のための第2の要求は、第1の身分証明書が分散型台帳に記憶されるのに続いて送信される、こととを行わせる。システムの一部の実装形態では、機械可読命令は、プロセッサによって実行されると、コンピューティングデバイスに少なくとも、データ項目に一意に関連付けられた非対称キー対を生成させ、身分証明書は、非対称キー対の公開キーを更に含む。システムの一部の実装では、機械可読命令は、プロセッサによって実行されると、コンピューティングデバイスに少なくとも、公開キーで暗号化された暗号化トークンを含む確認要求を受信することと、非対称キー対の秘密キーを使用して暗号化されたトークンを復号化し、暗号化されていないトークンを生成することと、秘密キーを使用して、暗号化されていないトークンの暗号化署名を作成することと、暗号化されていないトークン及び暗号化署名を含む確認応答を提供することと、を行わせる。システムの一部の実装では、データ項目はネットワークアドレスである。システムの一部の実装では、データ項目はファイルである。

【0006】

本開示の様々な実施形態は方法を含み、この方法は、データ項目の確認要求を受信する

ことであって、確認要求は、IDキー及びデータ項目を含む、ことと、データ項目が少なくとも一つの確認規則に準拠していることを決定することと、データ項目の確認済みクレームを生成することであって、確認済みクレームは、IDキーがデータ項目に関連付けられており、データ項目が少なくとも一つの確認規則に準拠していることを示す、ことと、データ項目の認証要求への応答として確認済みクレームを提供することと、を含む。方法の一部の実装では、IDキーは第2のIDキーである。少なくとも一つの確認規則は、データ項目が認証されたエンティティから発信されていることを示す。認証要求は、認証されたエンティティに関連付けられた第1のIDキーを更に含む。データ項目が少なくとも一つの確認規則に準拠していることを決定することは、認証要求が認証されたエンティティから発信されていることを、少なくとも部分的に第1のIDキーに基づいて確認することを更に含む。確認済みクレームの生成は、認証要求が認証済みエンティティから発信されているとの確認に応答して発生する。この方法の一部の実装では、少なくとも部分的に第1のIDキーに基づいて、認証要求が認証されたエンティティから発信されていることを確認することは、第1のIDキーに関連付けられた身分証明書を取得することであって、身分証明書には、それぞれの非対称キー対の公開暗号化キーが含まれる、ことと、公開暗号化キーを使用してトークンを暗号化して、暗号化されたトークンを作成することと、認証要求を送信した発信元エンティティに暗号化されたトークンを送信することと、それぞれの非対称キー対の秘密キーで作成されたトークン及びデジタル署名を受信することと、公開暗号化キーを使用してデジタル署名を確認することと、を更に含む。方法の一部の実装では、少なくとも一つの確認規則は、データ項目が指定されたセキュリティポリシーに準拠していることを示す。データ項目が少なくとも一つの確認規則に準拠していることを決定することは、データ項目のセキュリティ分析を実行することを更に含む。この方法の一部の実装形態では、この方法は、IDキー及び確認済みクレームを含む身分証明書を作成することと、身分証明書を分散型台帳に登録することと、を更に含む。方法の一部の実装では、データ項目はネットワークアドレスである。方法の一部の実装では、データ項目はファイルである。

【0007】

機械可読命令を含む非一時的なコンピュータ可読媒体の様々な実施形態が開示され、機械可読命令は、コンピューティングデバイスのプロセッサによって実行されると、コンピューティングデバイスに少なくとも、データ項目の要求をアプリケーションに送信することと、アプリケーションからデータ項目及びIDキーを受け取ることであって、IDキーはデータ項目にリンクされている、ことと、分散型台帳からIDキーによって識別される身分証明書を取得することであって、身分証明書には、データ項目に関連する少なくとも一つの確認済みクレームが含まれる、ことと、身分証明書に少なくとも部分的に基づいてデータ項目を確認することと、データ項目の確認の結果に少なくとも部分的に基づいてユーザインタフェースをレンダリングすることと、を行わせる。非一時的なコンピュータ可読媒体のいくつかの実装では、機械可読命令は、プロセッサによって実行されると、更に、コンピューティングデバイスに少なくとも、身分証明書に含まれている公開キーを使用してトークンを暗号化し、暗号化されたトークンを作成することと、暗号化されたトークンをアプリケーションに送信することと、アプリケーションからトークンを受け取り、トークンに関連付けられた暗号化署名を受信することと、暗号化署名を確認することと、を行わせる。非一時的なコンピュータ可読媒体の一部の実装形態では、コンピューティングデバイスに身分証明書に少なくとも部分的に基づいてデータ項目を確認させる機械可読命令は、コンピューティングデバイスに確認済みクレームにおける少なくとも一つのクレームを更に少なくとも評価させる。少なくとも一つのクレームは、データ項目の少なくとも一つの確認規則への準拠に関するアサーションを含む。非一時的なコンピュータ可読媒体の一部の実装形態では、コンピューティングデバイスに少なくとも一つのクレームを少なくとも評価させる機械可読命令は、コンピューティングデバイスに、クレームが信頼できるエンティティによって行われたと更に決定させる。非一時的なコンピュータ可読媒体の一部の実装では、データ項目はネットワークアドレスである。非一時的なコンピュータ可

10

20

30

40

50

読媒体の一部の実装では、データ項目はファイルである。

【0008】

本開示の多くの態様は、以下の図面を参照することにより、よりよく理解することができる。図面の構成要素は必ずしも原寸に比例しておらず、代わりに、開示の原理を明確に示すことに重点が置かれている。更に、図面では、同様の参照番号は、いくつかの図すべてを通じて対応する部分を示している。

【図面の簡単な説明】

【0009】

【図1】本開示の様々な実施形態によるネットワーク環境の図である。

【0010】

【図2】本開示の様々な実施形態による、図1のネットワーク環境に実装された機能の一例を示すシーケンス図である。

【0011】

【図3】本開示の様々な実施形態による、図1のネットワーク環境に実装された機能の一例を示すシーケンス図である。

【0012】

【図4】本開示の様々な実施形態による、図1のネットワーク環境に実装された機能の一例を示すシーケンス図である。

【0013】

【図5】本開示の様々な実施形態による、図1のネットワーク環境に実装された機能の一例を示すシーケンス図である。

【0014】

【図6】本開示の様々な実施形態による、図1のネットワーク環境に実装された機能の一例を示すシーケンス図である。

【0015】

【図7】本開示の様々な実施形態による、図1のネットワーク環境においてクライアントによってレンダリングされた例示的なユーザインタフェースの絵図である。

【0016】

【図8】本開示の様々な実施形態による、図1のネットワーク環境においてクライアントによってレンダリングされた例示的なユーザインタフェースの絵図である。

【発明を実施するための形態】

【0017】

データ又はコンテンツを認証するための、又はコンテンツの作成者、発信者、若しくは配布者のIDを確認するための様々なアプローチが開示される。データ又はコンテンツの確認に使用される文書は、分散して記憶できる。分散化は、認証又は確認プロセスにおける単一障害点から保護する。例えば、認証局がセキュリティ違反に見舞われたり又はアクセスできなくなったりした場合、コンテンツ又はデータに関連付けられた証明書を確認するために認証局に依存する認証アプローチは、認証局が保護されるか、又は再びアクセス可能になるまで失敗する。対照的に、認証データ若しくはコンテンツへの分散型アプローチ、又はコンテンツの作成者、発信者、若しくは配布者のIDの確認は、より回復力があり、様々な状況で利用できなくなる可能性はない。更に、分散型アプローチは、認証局のオペレータなどの単一のエンティティが、データ若しくはコンテンツの認証プロセス、又はコンテンツの作成者、発信者、若しくは配布者のIDの確認プロセスを独占又は制御することを防ぐ。以下の説明では、システム及びその構成要素の一般的な説明を提供し、続いてシステムの動作について説明する。

【0018】

図1に示されるように、様々な実施形態によるネットワーク環境100が示されている。ネットワーク環境100は、コンピューティング環境103、クライアントデバイス106、IDハブ109、及び分散型台帳113を含み、これらは、ネットワーク116を介して互いにデータ通信している。ネットワーク116は、ワイドエリアネットワーク（

10

20

30

40

50

WAN) 及びローカルエリアネットワーク (LAN) を含む。これらのネットワークには、有線若しくは無線の構成要素、又はそれらの組み合わせを含めることができる。有線ネットワークには、イーサネットネットワーク、ケーブルネットワーク、光ファイバーネットワーク、並びにダイヤルアップ、デジタル加入者回線 (DSL)、及び統合サービスデジタルネットワーク (ISDN) ネットワークなどの電話ネットワークが含まれ得る。無線ネットワークには、セルラーネットワーク、衛星ネットワーク、Institute of Electrical and Electronic Engineers (IEEE) 802.11 無線ネットワーク (すなわち、WIFI (登録商標))、Bluetooth (登録商標) ネットワーク、マイクロ波伝送ネットワーク、及び無線放送に依存するその他のネットワークが含まれ得る。ネットワーク 116 はまた、二つ以上のネットワーク 116 の組み合わせを含むことができる。ネットワーク 116 の例は、インターネット、イントラネット、エクストラネット、仮想プライベートネットワーク (VPN)、及び同様のネットワークを含むことができる。

【0019】

コンピューティング環境 103 は、サーバコンピュータ又はコンピューティング機能を提供する任意の他のシステムを含むことができる。或いは、コンピューティング環境 103 は、一つ又は複数のサーババンク又はコンピュータバンク又は他の構成に配置することができる複数のコンピューティングデバイスを使用することができる。このようなコンピューティングデバイスは、単一の設備に配置することも、又は地理的に離れた多くの場所に分散させることもできる。例えば、コンピューティング環境 103 は、ホストされたコンピューティングリソース、グリッドコンピューティングリソース、又は任意の他の分散コンピューティング構成と一緒に含むことができる複数のコンピューティングデバイスを含むことができる。場合によっては、コンピューティング環境 103 は、処理、ネットワーク、ストレージ、又は他のコンピューティング関連リソースの割り当てられた容量が時間と共に変化し得る弾性コンピューティングリソースに対応することができる。

【0020】

様々な実施形態による、様々なアプリケーション又は他の機能をコンピューティング環境 103 で実行することができる。コンピューティング環境 103 上で実行される構成要素は、ホストされたアプリケーション 119、セキュリティサービス 121、及び本明細書で詳細に説明されない他のアプリケーション、サービス、プロセス、システム、エンジン、又は機能を含む。ホストされたアプリケーション 119 及びセキュリティサービス 121 は、同じコンピューティング環境で動作するように示されているが、ホストされたアプリケーション 119 及びセキュリティサービス 121 は、別個のコンピューティング環境で動作又は実行され得ることが理解される。同様に、ホストされたアプリケーション 119 及びセキュリティサービス 121 は、特定の実装に応じて、同じエンティティ又は異なるエンティティによって動作及び制御することができる。

【0021】

ホストされたアプリケーション 119 は、ホストされたデータストア 123 に記憶されたデータへのアクセスをユーザに提供するために、或いはユーザに代わって一つ若しくは複数の機能を実行するか、又は一つ若しくは複数のトランザクションを開始するために実行され得る。ホストされたアプリケーション 119 の例には、ウェブサーバ、メールサーバ、ファイルサーバが含まれ、これらは、電子バンキングアプリケーション、電子コマース又はショッピングアプリケーション、ソーシャルメディアアプリケーション、インターネット又はウェブベースの電子メール (ウェブメール) アプリケーション、ファイル共有アプリケーション又はサービス、インターネット又はウェブベースの生産性アプリケーション (ワードプロセッサ、スプレッドシート、プレゼンテーションアプリケーションなど)、メディアストリーミングアプリケーションなどのウェブベースのアプリケーションを提供するために使用され得る。しかしながら、クライアントデバイス 106 にコンテンツ、コンテンツへのアクセス、又はデータ若しくはコンテンツがアクセスされ得る解決可能なネットワークアドレスを提供するコンピューティング環境 103 によってホストされる

任意のアプリケーションは、本開示の様々な実施形態の目的のためのホストされたアプリケーション 119 と見なすことができる。

【0022】

認証プロバイダ 120 は、ユーザ又はエンティティの ID を認証又は確認するために実行することができる。これには、特定のサービス、アプリケーション、又はデバイスがユーザ又はエンティティによって動作又は制御されていることを認証又は別の方法で確認することが含まれ得る。例えば、認証プロバイダ 120 を実行して、特定のネットワークアドレス（例えば、`http://www.examplebank.com`）で利用可能なウェブサイトが実際に「Example Bank」という会社によって運営されていることを決定することができる。

10

【0023】

セキュリティサービス 121 は、リソースのセキュリティ又は信頼性を評価するために実行することができる。これには、例えば、ファイル、ネットワークアドレス、又はその他のデータの信頼性の確認又は認証、並びにファイル、ネットワークアドレス、又はその他のデータの作成者又はプロバイダの信頼性の確認又は認証が含まれ得る。例えば、セキュリティサービス 121 を実行して、ファイルが特定の個人又は組織によって作成又は配布されたかどうかを評価できる。別の例として、セキュリティサービス 121 を実行して、リンク又はネットワークアドレスが実際に特定のエンティティの制御下にあるリソースに対するものであるかどうかを評価することができる。例えば、セキュリティサービス 121 は、銀行のウェブサイトへのリンクが実際に銀行の実際のウェブサイトへのリンクであるか、又は代わりになりすましのウェブサイトへのリンクであるかを決定できる。セキュリティスキャナ 212 を実行して、ファイルにマルウェアが含まれているかどうか、又はネットワークアドレスで利用可能なウェブサイトセキュリティの脆弱性があるかどうかを評価することもできる。これらの評価は、ファイル若しくはネットワークアドレスの受信に応じて、又は別のアプリケーションが受信した要求に応じて自動的に実行できる。

20

【0024】

また、コンピューティング環境 103 にアクセス可能なホストされたデータストア 123 に様々なデータを記憶することができる。ホストされたデータストア 123 は、複数のホストされたデータストア 123 を表すことができ、リレーショナルデータベース、オブジェクト指向データベース、階層データベース、ハッシュテーブル又は同様のキー値データストア、並びに他のデータストレージアプリケーション又はデータ構造を含むことができる。ホストされたデータストア 123 に記憶されたデータは、以下に説明する様々なアプリケーション又は機能エンティティの動作に関連付けられている。このデータは、一つ又は複数の認証レコード 126 及び一つ又は複数の確認規則 129 を含むことができる。

30

【0025】

認証レコード 126 は、ID キー 131 とデータ項目 133 との間の関係を表すことができる。関係は、例えば、ID キー 131 を使用して、一つ又は複数の確認規則 129 に少なくとも部分的に基づいて作成されたデータ項目 133 に関するアサーションを確認するために記憶され得る。

【0026】

40

ID キー 131 は、身分証明書 136 のネットワーク位置を指定するネットワークアドレスなど、身分証明書 136 を見つけることができる場所を指定する一意のアドレスを表すことができる。ID キー 131 は、身分証明書 136 を見つけることができる保管場所、身分証明書 136 の一意の識別子、及び潜在的に他の情報を含むことができる。ID キー 131 は、他の身分証明書 136 に関して身分証明書 136 を一意に識別することができるので、ID キー 131 は、個人、エンティティ、組織、又はデータ項目 133 の一意の識別子としても使用することができる。ID キー 131 の実例は、World Wide Web Consortium (W3C) によって定義された分散型識別子 (DID) である。しかしながら、データフォーマットを、本開示の様々な実施形態において、ID キー 131 として使用することができる。

50

【0027】

DIDの例では、IDキー131は、一意のユニフォームリソース識別子（URI）又は一意のユニフォームリソースロケータ（URL）を含めることができ、IDキー131のタイプ、身分証明書136を配置できる特定の分散型台帳113、及び身分証明書136の識別子を指定する。例えば、身分証明書136がETHEREUMプロトコルの実装を使用して記憶された場合、DIDとしてフォーマットされたIDキー131は、「did:ethereum:123456abcdefg」のURL又はURIスキーマの例を有する。次に、この例示的なIDキー131は、分散型台帳113から身分証明書136を取得するためのキーとして使用することができる。

【0028】

データ項目133は、データの任意のデジタル表現を含むことができる。例えば、データ項目133は、ファイル又はデータストリームであり得る。別の例として、データ項目133は、ファイル、アプリケーション、又はウェブページが配置されているアドレス（例えば、URL、URI、又は同様のリンク若しくはネットワークアドレス）であり得る。

【0029】

確認規則129は、特定のデータ項目133又はデータ項目133のクラスに関するアサーションの基礎として使用されるコンプライアンス規則又はポリシーを表すことができる。例えば、確認規則129は、データ項目133が安全であるというアサーションを行うための要件を指定することができる。これには、ウェブサイトがセキュリティサービス121によって実行されるセキュリティスキャンを通過するという要件、又はファイルがマルウェアを含まないことをセキュリティサービス121によって確認されるという要件が含まれる。別の例として、確認規則129は、特定のウェブサイト所有者が特定のリンクの発信者であると決定するための要件など、データ項目133の所有者又は作成者に関するアサーションを行うための要件を指定することができる。

【0030】

クライアントデバイス106は、ネットワーク116に結合することができる複数のクライアントデバイスを表す。クライアントデバイス106は、コンピュータシステムなどのプロセッサベースのシステムを含むことができる。そのようなコンピュータシステムは、パーソナルコンピュータ（例えば、デスクトップコンピュータ、ラップトップコンピュータ、又は同様のデバイス）、モバイルコンピューティングデバイス（例えば、パーソナルデジタルアシスタント、携帯電話、スマートフォン、ウェブパッド、タブレットコンピュータシステム、音楽プレーヤー、ポータブルゲームコンソール、電子ブックリーダー、及び同様のデバイス）、メディア再生デバイス（例えば、メディアストリーミングデバイス、BluRay（登録商標）プレーヤー、デジタルビデオディスク（DVD）プレーヤー、セットトップボックス、及び同様のデバイス）、ビデオゲームコンソール、又は同様の機能を備えた他のデバイスの形で具体化することができる。クライアントデバイス106は、液晶ディスプレイ（LCD）、ガスプラズマベースのフラットパネルディスプレイ、有機発光ダイオード（OLED）ディスプレイ、電気泳動インク（「Eインク」）ディスプレイ、プロジェクタ、又は他のタイプのディスプレイデバイスなどの一つ又は複数のディスプレイ139を含むことができる。場合によっては、ディスプレイ139は、クライアントデバイス106の構成要素であり得るか、又は有線若しくは無線接続を介してクライアントデバイス106に接続され得る。

【0031】

クライアントデバイス106は、クライアントアプリケーション143又は他のアプリケーションなどの様々なアプリケーションを実行するように構成することができる。クライアントアプリケーション143は、クライアントデバイス106によって実行されて、コンピューティング環境103又は他のサーバによって提供されるネットワークコンテンツにアクセスし、それによって、ディスプレイ139上にユーザインタフェース146をレンダリングすることができる。この目的のために、クライアントアプリケーション143は、ブラウザ又は専用アプリケーション（例えば、電子メールアプリケーション、ソー

10

20

30

40

50

シャルネットワーキングアプリケーション、メッセージングアプリケーション、バンキングアプリケーション、ショッピングアプリケーションなど）を含むことができ、ユーザインタフェース146は、ネットワークページ、アプリケーション画面、ユーザ入力を取得するための他のユーザメカニズムを含むことができる。

【0032】

IDハブ109は、一つ又は複数のコンピューティングデバイスによってホストされ、個々のユーザの身分証明書を安全に記憶し、許可された要求に応答して身分証明書を提供するために利用されるサービス又はサービスの集合を表すことができる。例えば、IDハブ109は、クレデンシャルマネージャ149及びボルト（vault）153を含むことができる。IDハブ109は、明確にするためにコンピューティング環境103とは別個のものとして示されているが、ボルトマネージャ149及びボルト153を含むIDハブ109の機能は、コンピューティング環境103内に実装され得ることが理解される。更に、一部の实装形態では、ボルトマネージャ149及びボルト153を含むIDハブ109は、特定の实装に応じて、同じエンティティ又は異なるエンティティによって動作され得る。

【0033】

ボルトマネージャ149を実行して、ボルト153へのアクセスを制御することができる。例えば、ボルトマネージャ149は、ボルト153に記憶された様々なデータを追加、削除、又は変更するために使用することができる。別の例として、ボルトマネージャ149を使用して、個々のユーザを認証し、ボルト153へのアクセスを許可されたユーザ又はエンティティに制限することができる。

【0034】

ボルト153は、クレデンシャルマネージャ149にアクセス可能な安全なデータストアを表す。ボルト153に記憶されたデータは、個々のユーザ又はエンティティのみがアクセスできる暗号化された形式で記憶することができる。個々のユーザ又はエンティティは、一つ又は複数のキーレコード156を含む様々なタイプのデータをボルト153に記憶できる。キーレコード156は、特定のIDキー131とそれぞれのキー対159との間の関連又は関係を追跡するために使用することができる。

【0035】

キー対159は、公開キー163及び秘密キー166を含む非対称暗号化キー対を表すことができる。キー対159内の暗号化キーは、後述するように、エンティティ又はユーザが、IDキー131に関連付けられたデータとの関係を確認若しくは他の方法で認証又はデータを制御するために使用することができる。キー対159は、楕円曲線暗号（ECC）アプローチなど、様々なアプローチ又はRivest-Shamir-Adleman（RSA）アルゴリズムを使用して生成できる。

【0036】

分散型台帳113は、異なる地理的又はネットワークの場所にある複数のノードにまたがる同期された、結果整合性のあるデータストアを表す。分散型台帳113内の各ノードは、分散型台帳113に記憶されたすべてのデータを含む、分散型台帳113の複製されたコピーを含むことができる。分散型台帳113を含むトランザクションの記録は、分散型台帳113を形成する個々のノードを接続するピアツーピアネットワークを使用して共有又は複製することができる。トランザクション又はレコードが分散型台帳113に記録されると、レコードが最終的にすべてのノードで記録されるまで、それをピアツーピアネットワーク全体に複製することができる。分散型台帳113にデータが確実に書き込まれるようにするために、様々なコンセンサス方式を使用できる。分散型台帳の例には、ブロックチェーン、分散ハッシュテーブル（DHT）、及び同様のデータ構造が含まれる。

【0037】

分散型台帳113には、様々なデータを記憶することもできる。これは、一つ又は複数の身分証明書136を含むことができる。しかしながら、本開示で論じられる他のデータは、データの公的な利用可能性がその特定の实装において許容可能である場合、分散型台

10

20

30

40

50

帳 1 1 3 に記憶することもできる。

【 0 0 3 8 】

身分証明書 1 3 6 は、ユーザを識別及び認証するための情報を提供する文書である。身分証明書 1 3 6 は、身分証明書 1 3 6、したがって、身分証明書 1 3 6 に関連付けられた個人又はエンティティを一意に識別するために使用することができる I D キー 1 3 1 を含むことができる。身分証明書 1 3 6 はまた、身分証明書 1 3 6 の信頼性を確認するために第三者によって使用され得る、身分証明書 3 1 1 に関連付けられた非対称キー対 1 5 9 からの公開キー 1 6 3 を含むことができる。身分証明書 1 3 6 はまた、一つ又は複数の確認済みクレーム 1 6 9 を含むことができる。身分証明書 1 6 3 の例示的な例は、W 3 C によって定義された分散型識別子文書（D 身分証明書）である。しかしながら、データフォーマットは、本開示の様々な実施形態において身分証明書 1 6 3 として使用することができる。

10

【 0 0 3 9 】

確認済みクレーム 1 7 3 は、身分証明書 1 3 6 によって記述された特定のエンティティ又はデータ項目 1 3 3 についての一つ又は複数の確認されたアサーションを表す。アサーションは、例えば、データ項目 1 3 3 が一つ又は複数の確認規則 1 2 9 に準拠している（例えば、ファイルにマルウェアが含まれていない、又はウェブサイトへのリンクがウェブサイトのオペレータからの有効なリンクである）というものであり得る。別の例として、アサーションは、特定のエンティティがその者がクレームする人物である、又はコンテンツの発信者又はコミュニケーションの作成者がその者が主張する人物であるというものであり得る。したがって、確認済みクレーム 1 6 9 は、一つ又は複数のクレーム 1 7 3 及び各クレーム 1 7 3 のそれぞれの署名 1 7 6 を含むことができる。

20

【 0 0 4 0 】

クレーム 1 7 3 は、エンティティ、個人、又はデータ項目 1 3 3 に関するアサーションを表す。例えば、クレーム 1 7 3 は、特定のネットワークアドレスに位置するウェブサイトが、一つ又は複数の確認規則 1 2 9 に記載された基準に従って安全であると見なされると述べ得る。例えば、クレーム 1 7 3 は、ウェブサイトが既知のセキュリティの脆弱性が含まれていないか、又は既知のマルウェアが含まれていないことを指定できる。別の例として、クレーム 1 7 3 は、ユーザをウェブサイト又はウェブアプリケーションなどのネットワークサービスに誘導するネットワークアドレスが、ウェブサイト又はウェブアプリケーションのオペレータによって提供される本物又は有効なネットワークアドレスであることを指定することができる。同様に、クレーム 1 7 3 は、ファイルにマルウェアが含まれていないこと、又はファイルの作成者が本人であることを指定できる。

30

【 0 0 4 1 】

署名 1 7 6 は、クレーム 1 7 3 の正確さ及び信頼性を確認するために使用される任意の暗号化署名を含むことができる。例えば、署名 1 7 6 は、アサーションを行う当事者を識別でき、また、当事者エンティティを所有する秘密暗号化キー 1 6 6 によって生成されたデジタル署名と、署名 1 7 6 の確認に使用できる対応する公開暗号化キー 1 6 3 を識別するデジタル指紋の両方を含むことができる。署名 1 7 6 はまた、クレーム 1 7 3 を行うエンティティの同意なしにクレーム 1 7 3 が変更されたかどうかを決定するために使用することができる。例えば、クレーム 1 7 3 への無許可の変更は、署名 1 7 6 とクレーム 1 7 3 との間の不一致をもたらすであろう。

40

【 0 0 4 2 】

次に、ネットワーク環境 1 0 0 の様々な構成要素の動作の一般的な説明が提供される。個々の構成要素の動作のより詳細な説明は、図 2 ～ 7 の説明に提供されている。更に、以下の説明は、図 1 のネットワーク環境 1 0 0 に示される様々な構成要素間の相互作用の一例を提供するが、それらは、後で説明されるように、他の方法で動作するように構成することができる。

【 0 0 4 3 】

始めに、認証プロバイダ 1 2 0 は、最初に、ホストされたアプリケーション 1 1 9 の I

50

Dを確認することができ、これは、ホストされたアプリケーション119のオペレータのIDを確認することを含むことができる。したがって、ホストされたアプリケーション119は、ホストされたアプリケーション119のIDを認証するために使用されるキー対159を生成するか、又はその目的のために以前に作成された既存のキー対159を使用することができる。ホストされたアプリケーション119はまた、ホストされたアプリケーション119のIDを認証又は確認するために使用され得る新しいIDキー131を生成することができる。

【0044】

次に、ホストされたアプリケーション119は、IDキー131を認証プロバイダ120に送信し、ホストされたアプリケーション119の認証情報を送信して、そのIDを確認又は認証することができる。これらの認証クレデンシャルには、ユーザ名及びパスワード、暗号化証明書、既存のキー対159からの公開キー163、以前に発行された認証トークン又はCookie、生体認証クレデンシャルなどが含まれ得る。

【0045】

次に、認証プロバイダ120は、認証クレデンシャルを使用して、ホストされたアプリケーション119のIDを認証することができる。これには、ユーザ名及びパスワードの確認、証明書又は公開キー163を使用した暗号化チャレンジの発行及び暗号化応答の確認、以前に発行された認証トークン又はCookieの確認などが含まれ得る。ホストされたアプリケーション119のIDが確認されると、認証プロバイダ120は、ホストされたアプリケーション119のオペレータのIDを主張するクレーム173を含む確認済みクレーム169及びクレーム173の署名176を作成することができる。次に、確認済みクレーム169は、ホストされたアプリケーション119に返されることができ、これは、確認済みクレーム169、IDキー131、及びそのIDを証明するためにホストされたアプリケーション119によって使用される公開キー163を含む分散型台帳に身分証明書136を作成及び記憶することができる。

【0046】

続いて、ホストされたアプリケーション119は、セキュリティサービス121が、ファイル又はネットワークアドレス（例えば、ウェブサイト又はウェブアプリケーションを指定するURL）などのデータ項目133を確認することを要求することができる。確認は、ホストされたアプリケーション119がデータ項目133の発行者（例えば、ファイルの作成者又は配布者、又はネットワークアドレスによって識別されるウェブサイト又はウェブアプリケーションのホスト）であること、又はデータ項目133は安全である（例えば、ファイルに既知のマルウェアが含まれていない、又はネットワークアドレスにあるウェブサイト若しくはウェブアプリケーションに既知の脆弱性が含まれていないなど）であることを証明することであり得る。要求は、データ項目133に固有の新しく生成されたキー対159、データ項目133に固有の新しく作成されたIDキー131、並びにホストされたアプリケーション119自体のIDを確認するために使用されるIDキー131を含むことができる。

【0047】

ホストされたアプリケーション119からの要求を受信すると、セキュリティサービス121は、最初に、ホストされたアプリケーション119のIDを確認することができる。例えば、セキュリティサービス121は、分散型台帳113から、ホストされたアプリケーション119の識別に関する確認済みクレーム169及びホストされたアプリケーション119のIDを確認するために使用される公開キー163を含む身分証明書136を取得することができる。次に、セキュリティサービス121は、公開キー163を使用して、チャレンジ応答交換を開始し、ホストされたアプリケーション119のIDを確認することができる。場合によっては、セキュリティサービス121は、リレーサービス又は解決サービスを使用して、複数の分散型台帳113が使用される実装において、どの分散型台帳113が身分証明書136を含むかを決定することができる。このようなリレーサービス又は解決サービスの例は、W3Cで定義されているDIDリゾルバである。

【0048】

ホストされたアプリケーション119のIDが確認されると、セキュリティサービス121は、データ項目133を確認することができる。例えば、データ項目133がウェブサイト又はウェブアプリケーションのネットワークアドレス（例えば、URL）である場合、セキュリティサービス121は、最初に自動化された脅威評価を実行することができる。脅威評価では、一般的なウェブサイトの設定ミスや又は既知のサーバ若しくはアプリケーションの脆弱性をチェックできる。別の例として、セキュリティサービス121は、ネットワークアドレスが（例えば、フィッシングサイトを指すネットワークアドレスの代わりに）ウェブサイト又はウェブアプリケーションのオペレータによって制御される本物のネットワークアドレスであることを確認することができる。データ項目133がファイルである場合、セキュリティサービス121は、マルウェアスキャンを実行して、ファイルがマルウェアを含むかどうかを決定することができる。別の例として、セキュリティサービス121は、ホストされたアプリケーション119のオペレータがファイルの作成者又は発信者であることを確認することができる。これは、ホストされたアプリケーション119によって作成されたファイルの暗号化署名を確認することによって行うことができる。

10

【0049】

データ項目133を確認した後、セキュリティサービス121は、データ項目133に関連する一つ又は複数の確認済みクレーム169を作成することができる。例えば、セキュリティサービス121は、ネットワークアドレスがホストされたアプリケーション119のオペレータによって制御されるという第1のクレーム173と、ネットワークアドレスで利用可能なウェブサイト又はウェブアプリケーションに既知のセキュリティの脆弱性は含まれていない第2のクレーム173とを含む確認済みクレーム169を作成することができる。セキュリティサービス121はまた、第1のクレーム173のために第1の署名176を作成し、第2のクレーム173のために第2の署名176を作成し、これらの署名を確認済みクレーム169に含めることができる。しかし、セキュリティサービス121は、複数の確認済みクレーム169を作成でき、各確認済みクレーム169は単一のクレーム173を表す。次に、セキュリティサービス121は、データ項目133について確認済みクレーム169を返すことができ、一部の実装形態では、データ項目133に関連付けられたIDキー131を返すことができる。

20

30

【0050】

ホストされたアプリケーション119は、確認済みクレーム169を受信すると、データ項目133に関連付けられたIDキー131、セキュリティサービス121によって提供された確認済みクレーム169、及びIDキー131に関連付けられている公開キー163を含む身分証明書136を作成することができる。次に、ホストされたアプリケーション119は、身分証明書136を分散型台帳113に記憶することができる。

【0051】

クライアントアプリケーション143がデータ項目133を要求するとき、それは、分散型台帳113に記憶された身分証明書136を使用して、データ項目133のセキュリティ又は信頼性を認証するか、他の方法で確認することができる。例えば、ブラウザがURLを使用してウェブページを要求した場合、ホストされたアプリケーション119は、ネットワークアドレスに関連するIDキー131をブラウザに提供することができる。次に、ブラウザは、URLの身分証明書136を取得し、URLがホストされたアプリケーション119によって提供されるウェブページの有効なネットワークアドレスであるというクレーム173を含む身分証明書136で確認済みクレーム169を識別でき、公開キー163及び署名176を使用してクレーム173を確認する。同様に、ブラウザは、ウェブページがセキュリティサービス121によって実行された最近のセキュリティスキャンを通過したことを示す身分証明書136内の第2のクレーム173を識別し、公開キー163及び署名176を使用してクレーム173を確認することができる。データ項目133がファイルである場合、クライアントアプリケーション143は、同様のプロセスを

40

50

使用して、ファイルの作成者及びセキュリティを確認することができる。

【0052】

図2を次に参照すると、ネットワーク環境100の構成要素の動作の一例を提供するシーケンス図が示されている。図2のシーケンス図は、ネットワーク環境100の図示された部分の動作を実装するために使用することができる多くの異なるタイプの機能的配置の単なる例を提供する。別の方法として、図2のシーケンス図は、ネットワーク環境100内に実装された方法の要素の例を描写していると見なすことができる。

【0053】

ステップ203から始めて、ホストされたアプリケーション119は、ホストされたアプリケーション119又はホストされたアプリケーション119のオペレータのIDを認証するために使用されるキー対159及びIDキー131の両方を生成することができる。キー対159及びIDキー131を生成した後、ホストされるアプリケーション119は、キー対159をボルト153に記憶することができる。したがって、ホストされたアプリケーション119は、ホストされたアプリケーション119の認証クレデンシャル並びにIDキー131及びキー対159を含むことができる要求をボルトマネージャ149に送信することができる。認証クレデンシャルを確認した後、ボルトマネージャ149は、IDキー131をキー対159に関連付けるキーレコードをボルト153に作成することができる。ホストされたアプリケーション119が、IDキー131に関連付けられた秘密キー166を必要とする場合、それは、ボルトマネージャ149からの秘密キー166のコピー又はアクセスを要求することができる。

【0054】

次に、ステップ206で、ホストされたアプリケーション119は、確認のために、キー対159及びIDキー131を認証プロバイダ120に送信することができる。一部の実装形態では、ホストされたアプリケーション119は、認証クレデンシャルを認証プロバイダ120に送信して、ホストされたアプリケーション119自体又はホストされたアプリケーション119のオペレータのIDを証明することもできる。

【0055】

次に、ステップ209で、認証プロバイダ120は、ホストされたアプリケーション119によって提供される認証クレデンシャルを確認する。例えば、認証プロバイダ120は、ユーザ名及びパスワード、事前共有シークレット、トークン、又はCookieなど、ホストされたアプリケーション119によって提供される認証クレデンシャル又は、ホストされたアプリケーション119によって提供される他の認証クレデンシャルは、認証プロバイダ120にすでにファイルされている認証クレデンシャルと一致することを確認することができる。

【0056】

続いて、ステップ213で、認証クレデンシャルがステップ209で有効であると決定された場合、認証プロバイダ120は、確認済みクレーム169を作成し、ホストされたアプリケーション119に返すことができる。確認済みクレーム169は、認証プロバイダ120がホストされたアプリケーション119又はホストされたアプリケーション119のオペレータのIDを確認したことを主張するクレーム173を含むことができ、これには、ホストされたアプリケーション119によって提供されるIDキー131が、ホストされたアプリケーション119又はホストされたアプリケーション119のオペレータによって制御されることが含まれる。確認済みクレーム169はまた、確認済みクレーム169に含まれる各クレーム173のそれぞれの署名176を含むことができる。署名176は、認証プロバイダ120によって制御される秘密キー166を使用して、認証プロバイダ120によって生成することができる。結果として、第三者は、認証プロバイダ120によって制御される秘密キー166のそれぞれの公開キー163を使用して、署名176をクレーム173と比較することによって、クレーム173を確認することができる。認証プロバイダ120の公開キー163を使用して署名176を確認できなかった場合、これは、クレーム173が許可なしに変更されたか、又はクレーム173が認証プロバ

イダ 120 によって行われたことがないことを示し得る。次に、確認済みクレーム 169 は、ホストされたアプリケーション 119 に返される。

【0057】

次に、ステップ 216 で、ホストされたアプリケーション 119 は、他のアプリケーション又は第三者がホストされたアプリケーション 119 又はホストされたアプリケーション 119 のオペレータの ID を確認することを可能にすることができる身分証明書 136 を作成することができる。例えば、ホストされたアプリケーション 119 は、ステップ 203 で作成された ID キー 131 及びキー対 159、並びにステップ 213 で作成された確認済みクレーム 169 を含む身分証明書 136 を作成することができる。身分証明書 136 を作成した後、ホストされたアプリケーション 119 は、身分証明書 136 を分散型台帳 113 に記憶させることができる。

10

【0058】

次に図 3 を参照すると、ネットワーク環境 100 の構成要素の動作の別の例を提供するシーケンス図が示されている。図 3 のシーケンス図は、ネットワーク環境 100 の図示された部分の動作を実装するために使用することができる多くの異なるタイプの機能的配置の単なる例を提供する。別の方法として、図 3 のシーケンス図は、ネットワーク環境 100 内に実装された方法の要素の例を描写していると見なすことができる。

【0059】

ステップ 303 から始めて、ホストされたアプリケーション 119 は、それぞれのデータ項目 133（例えば、ファイル、ネットワークアドレス又は他のタイプのデータ）のためのキー対 159 及び ID キー 131 を作成する。ID キー 131 とデータ項目 133 の間の関係は、認証レコード 126 としてホストされたデータストア 123 に記録することもでき、ID キー 131 及びデータ項目 133 のコピー又は識別子を含めることができる。

20

【0060】

次に、ステップ 306 で、ホストされたアプリケーション 119 は、確認要求をセキュリティサービス 121 に送信することができる。確認要求は、データ項目 133 に関連付けられた ID キー 131、データ項目 133 自体、及びホストされたアプリケーション 119 を識別する ID キー 131 を含むことができる。場合によっては、ホストされたアプリケーション 119 は、データ項目 133 を評価するときに考慮されるべき一つ又は複数の確認規則 129 の指示を提供することもできる。

30

【0061】

ステップ 309 に進むと、セキュリティサービス 121 は、確認要求の受信に応答して、ホストされたアプリケーション 119 を識別する ID キー 131 に関連付けられた身分証明書 136 を取得する。例えば、セキュリティサービス 121 は、ID キー 131 を使用して、分散型台帳 113 に記憶されたそれぞれの身分証明書 136 を検索し、それを取得することができる。複数の分散型台帳 113 が使用される場合、セキュリティサービス 121 は、ID キー 131 を D ID リゾルバなどのリレー又はリゾルバサービスに送信して、どの分散型台帳 113 が身分証明書 136 を含むかを決定することができる。これらの例では、リレー又はリゾルバサービスは、セキュリティサービス 121 に代わって身分証明書 136 を取得し、それをセキュリティサービス 121 に返すことができる。

40

【0062】

ステップ 311 に進むと、セキュリティサービス 121 は、ホストされたアプリケーション 119 に認証チャレンジを送信して、ホストされたアプリケーション 119 がステップ 306 で要求を行ったことを確認することができる。したがって、セキュリティサービス 121 は、ステップ 309 で取得された身分証明書 136 内の公開キー 163 を使用して、認証チャレンジとして使用するためにトークン又はノンスを暗号化することができる。次に、認証チャレンジをホストされたアプリケーション 119 に送信できる。

【0063】

ステップ 313 を次に参照すると、ホストされたアプリケーション 119 は、認証チャレンジをボルトマネージャ 149 に転送することができる。認証チャレンジは、ホスト

50

されたアプリケーション 119 を認証する ID キー 131 に関連付けられた秘密キー 166 を使用して、認証チャレンジを復号化及び署名するためのボルトマネージャ 149 の要求の一部として転送できる。ホストされたアプリケーション 119 はまた、ホストされたアプリケーション 119 に代わって動作が実行されるべきであることをボルトマネージャ 149 に確認するための認証クレデンシャルを含み得る。

【0064】

ステップ 316 での応答において、ボルトマネージャ 149 は、認証チャレンジを復号化して署名し、復号化された認証チャレンジ及び認証チャレンジのための署名をホストされたアプリケーション 119 に提供することができる。例えば、ボルトマネージャ 149 は、最初に、ホストされたアプリケーション 119 を識別する ID キー 131 に関連付けられたキー対 159 の秘密キー 166 を取得することができる。次に、ボルトマネージャ 149 は、暗号化されたチャレンジを復号化して、セキュリティサービス 121 によって提供された元のトークン又はノンスを再作成することができる。次に、ボルトマネージャ 149 は、秘密キー 166 を用いてトークン又はノンスに署名して、暗号化されていないトークン又はノンスを他の手段で取得する代わりに、ホストされたアプリケーション 119 の秘密キー 166 の所有者がチャレンジを復号化したことを証明することができる。次に、ボルトマネージャ 149 は、暗号化されていないトークン又はノンス、並びにそれぞれの署名を、ホストされたアプリケーション 119 に提供することができる。

【0065】

次に、ステップ 319 で、ホストされたアプリケーション 119 は、認証応答をセキュリティサービス 121 に送信して、その ID を証明することができる。これには、認証チャレンジからの暗号化されていないトークン又はノンス、並びに暗号化されていないトークン又はノンスの署名を含めることができる。

【0066】

次に、ステップ 323 で、セキュリティサービス 121 は、データ項目 133 を確認又は認証することができる。例えば、セキュリティサービス 121 は、データ項目 133 を評価して、データ項目 133 が、ステップ 306 でホストされたアプリケーション 119 によって指定された一つ又は複数の確認規則 129 に準拠するかどうかを決定することができる。別の例として、セキュリティサービス 121 は、データ項目 133 に適用される確認規則 129 を識別し、データ項目 133 のコンプライアンスを評価することができる。例えば、データ項目 133 がウェブサイトのネットワークアドレスである場合、セキュリティサービス 121 は、ネットワークアドレス又はウェブサイトに応用可能なすべての確認規則 129 を識別し、データ項目 133 のコンプライアンスを評価することができる。同様に、データ項目 133 がファイルである場合、セキュリティサービス 121 は、ファイルに応用可能なすべての確認規則 129 を識別し、データ項目のコンプライアンスを評価することができる。

【0067】

セキュリティサービス 121 がデータ項目 133 を評価すると、セキュリティサービスは、データ項目 133 について確認済みクレーム 169 を作成することができる。これは、データ項目 133 が準拠する各確認規則 129 に関するクレーム 173 を含むことができる。これはまた、データ項目 133 が従わない各確認規則 129 に関するクレーム 173 を含むことができる。例えば、セキュリティサービス 121 が、ネットワークアドレスが、なりすましアプリケーションのネットワークアドレスではなく、ホストされたアプリケーション 119 の有効なネットワークアドレスであると決定した場合、セキュリティサービス 121 は、ネットワークアドレスが、ホストされたアプリケーション 119 に到達するための有効なネットワークアドレスであるべきであると述べている確認規則 129 に準拠しているというクレーム 173 を行うことができる。しかし、セキュリティサービス 121 によって実行される自動セキュリティスキャンが、ホストされたアプリケーション 119 に脆弱性の存在を示した場合、セキュリティサービス 121 は、ホストされたアプリケーション 119 が安全でなく、ホストされたアプリケーション 119 には、脆弱性又

10

20

30

40

50

は特定の脆弱性があるとはならないという確認規則 1 2 9 に準拠していないという第 2 のクレームを行うことができる。同様のクレーム 1 7 3 は、ファイルの作成者若しくは配布者の ID 又はファイルにマルウェアが含まれているかどうかなど、ファイルについても行うことができる。セキュリティサービス 1 2 1 はまた、確認済みクレーム 1 6 9 のクレーム 1 7 3 ごとにそれぞれの署名 1 7 6 を作成することができる。次に、確認済みクレーム 1 6 9 は、ホストされたアプリケーション 1 1 9 に返すことができる。

【0068】

最後に、ステップ 3 2 6 で、ホストされたアプリケーション 1 1 9 は、セキュリティサービス 1 2 1 によって提供される確認済みクレーム 1 6 9 を含むデータ項目 1 3 3 の身分証明書 1 3 6 を作成及び記録することができる。これにより、他のアプリケーション又は第三者が、ネットワークアドレスへのリンクが本物か若しくは偽物か、ホストされたアプリケーション 1 1 9、ウェブサイト、若しくはファイルにマルウェアが含まれているか若しくはその他の点で安全でないか、又はファイルの作成者、発信者、若しくは配布者であると称するエンティティが、実際にファイルの作成者、作成者、若しくは配布者であるかどうかなど、データ項目 1 3 3 の信頼性又はセキュリティを確認できる。したがって、ホストされたアプリケーション 1 1 9 は、ステップ 3 0 3 で作成された ID キー 1 3 1 及びキー対 1 5 9、並びにステップ 3 2 3 で作成された確認済みクレーム 1 6 9 を含む身分証明書 1 3 6 を作成することができる。身分証明書 1 3 6 を作成した後、ホストされたアプリケーション 1 1 9 は、身分証明書 1 3 6 を分散型台帳 1 1 3 に記憶させることができる。

【0069】

次に図 4 を参照すると、ネットワーク環境 1 0 0 の構成要素の動作の別の例を提供するシーケンス図が示されている。図 4 のシーケンス図は、ネットワーク環境 1 0 0 の図示された部分の動作を実装するために使用することができる多くの異なるタイプの機能的配置の単なる例を提供する。別の方法として、図 4 のシーケンス図は、ネットワーク環境 1 0 0 内に実装された方法の要素の例を描写していると見なすことができる。

【0070】

図 4 のシーケンス図は、図 3 の範囲と同様であることに留意されたい。しかしながら、図 3 のシーケンス図は、ボルトマネージャ 1 4 9 の使用を示し、一方、図 4 のシーケンス図は、ボルトマネージャ 1 4 9 の使用を省略した代替の実装を示している。

【0071】

ステップ 4 0 3 から始めて、ホストされたアプリケーション 1 1 9 は、それぞれのデータ項目 1 3 3（例えば、ファイル、ネットワークアドレス又は他のタイプのデータ）のためのキー対 1 5 9 及び ID キー 1 3 1 を作成する。ID キー 1 3 1 とデータ項目 1 3 3 の間の関係は、認証レコード 1 2 6 としてホストされたデータストア 1 2 3 に記録することもでき、ID キー 1 3 1 及びデータ項目 1 3 3 のコピー又は識別子を含めることができる。

【0072】

次に、ステップ 4 0 6 で、ホストされたアプリケーション 1 1 9 は、確認要求をセキュリティサービス 1 2 1 に送信することができる。確認要求は、データ項目 1 3 3 に関連付けられた ID キー 1 3 1、データ項目 1 3 3 自体、及びホストされたアプリケーション 1 1 9 を識別する ID キー 1 3 1 を含むことができる。場合によっては、ホストされたアプリケーション 1 1 9 は、データ項目 1 3 3 を評価するときに考慮されるべき一つ又は複数の確認規則 1 2 9 の指示を提供することもできる。

【0073】

ステップ 4 0 9 に進むと、セキュリティサービス 1 2 1 は、確認要求の受信に応答して、ホストされたアプリケーション 1 1 9 を識別する ID キー 1 3 1 に関連付けられた身分証明書 1 3 6 を取得する。例えば、セキュリティサービス 1 2 1 は、ID キー 1 3 1 を使用して、分散型台帳 1 1 3 に記憶されたそれぞれの身分証明書 1 3 6 を検索し、それを取得することができる。複数の分散型台帳 1 1 3 が使用される場合、セキュリティサービス 1 2 1 は、ID キー 1 3 1 を D ID リゾルバなどのリレー又はリゾルバサービスに送信して、どの分散型台帳 1 1 3 が身分証明書 1 3 6 を含むかを決定することができる。これら

の例では、リレー又はリゾルバサービスは、セキュリティサービス 121 に代わって身分証明書 136 を取得し、それをセキュリティサービス 121 に返すことができる。

【0074】

ステップ 411 に進むと、セキュリティサービス 121 は、ホストされたアプリケーション 119 に認証チャレンジを送信して、ホストされたアプリケーション 119 がステップ 406 で要求を行ったことを確認することができる。したがって、セキュリティサービス 121 は、ステップ 409 で取得された身分証明書 136 内の公開キー 163 を使用して、認証チャレンジとして使用するためにトークン又はノンスを暗号化することができる。次に、認証チャレンジをホストされたアプリケーション 119 に送信できる。

【0075】

ステップ 416 で、ホストされたアプリケーション 119 は、認証チャレンジを復号化して署名し、復号化された認証チャレンジ及び認証チャレンジのための署名をホストされたアプリケーション 119 に提供することができる。例えば、ホストされたアプリケーション 119 は、キー対 159 のそれぞれの秘密キー 166 を使用して、暗号化されたチャレンジを復号化し、セキュリティサービス 121 によって提供される元のトークン又はノンスを再作成できる。次に、ホストされたアプリケーション 119 は、秘密キー 166 を用いてトークン又はノンスに署名して、暗号化されていないトークン又はノンスを他の手段で取得する代わりに、ホストされたアプリケーション 119 がチャレンジを復号化したことを証明することができる。

【0076】

次に、ステップ 419 で、ホストされたアプリケーション 119 は、認証応答をセキュリティサービス 121 に送信して、その ID を証明することができる。これには、認証チャレンジからの暗号化されていないトークン又はノンス、並びに暗号化されていないトークン又はノンスの署名を含めることができる。

【0077】

ステップ 423 において、セキュリティサービス 121 は、データ項目 133 を確認又は認証することができる。例えば、セキュリティサービス 121 は、データ項目 133 を評価して、データ項目 133 が、ステップ 406 でホストされたアプリケーション 119 によって指定された一つ又は複数の確認規則 129 に準拠するかどうかを決定することができる。別の例として、セキュリティサービス 121 は、データ項目 133 に適用される確認規則 129 を識別し、データ項目 133 のコンプライアンスを評価することができる。例えば、データ項目 133 がウェブサイトのネットワークアドレスである場合、セキュリティサービス 121 は、ネットワークアドレス又はウェブサイトに適用可能なすべての確認規則 129 を識別し、データ項目 133 のコンプライアンスを評価することができる。同様に、データ項目 133 がファイルである場合、セキュリティサービス 121 は、ファイルに適用可能なすべての確認規則 129 を識別し、データ項目のコンプライアンスを評価することができる。

【0078】

セキュリティサービス 121 がデータ項目 133 を評価すると、セキュリティサービスは、データ項目 133 について確認済みクレーム 169 を作成することができる。これは、データ項目 133 が準拠する各確認規則 129 に関するクレーム 173 を含むことができる。これはまた、データ項目 133 が従わない各確認規則 129 に関するクレーム 173 を含むことができる。例えば、セキュリティサービス 121 が、ネットワークアドレスがなりすましアプリケーションのネットワークアドレスではなく、ホストされたアプリケーション 119 の有効なネットワークアドレスであると決定した場合、セキュリティサービス 121 は、ネットワークアドレスが確認規則 129 に準拠しているとクレーム 173 を行うことができ、ネットワークアドレスは、ホストされているアプリケーション 119 に到達するための有効なネットワークアドレスである必要があることを示す。しかし、セキュリティサービス 121 によって実行される自動セキュリティスキャンが、ホストされたアプリケーション 119 に脆弱性の存在を示した場合、セキュリティサービス 121 は

10

20

30

40

50

、ホストされたアプリケーション 119 が安全でなく、ホストされたアプリケーション 119 には、脆弱性又は特定の脆弱性があるという確認規則 129 に準拠していないという第 2 のクレームを行うことができる。同様のクレーム 173 は、ファイルの作成者若しくは配布者の ID 又はファイルにマルウェアが含まれているかどうかなど、ファイルについても行うことができる。セキュリティサービス 121 はまた、確認済みクレーム 169 のクレーム 173 ごとにそれぞれの署名 176 を作成することができる。次に、確認済みクレーム 169 は、ホストされたアプリケーション 119 に返すことができる。

【0079】

最後に、ステップ 426 で、ホストされたアプリケーション 119 は、セキュリティサービス 121 によって提供される確認済みクレーム 169 を含むデータ項目 133 の身分証明書 136 を作成及び記録することができる。これにより、他のアプリケーション又は第三者が、ネットワークアドレスへのリンクが本物か若しくは偽物か、ホストされたアプリケーション 119、ウェブサイト、若しくはファイルにマルウェアが含まれているか若しくはその他の点で安全でないか、又はファイルの作成者、発信者、若しくは又は配布者であると称するエンティティが、実際にファイルの作成者、作成者、若しくは又は配布者であるかどうかなど、データ項目 133 の信頼性又はセキュリティを確認できる。したがって、ホストされたアプリケーション 119 は、ステップ 403 で作成された ID キー 131 及びキー対 159、並びにステップ 423 で作成された確認済みクレーム 169 を含む身分証明書 136 を作成することができる。身分証明書 136 を作成した後、ホストされたアプリケーション 119 は、身分証明書 136 を分散型台帳 113 に記憶させることができる。

【0080】

次に図 5 を参照すると、ネットワーク環境 100 の構成要素の動作の別の例を提供するシーケンス図が示されている。図 5 のシーケンス図は、ネットワーク環境 100 の図示された部分の動作を実装するために使用することができる多くの異なるタイプの機能的配置の単なる例を提供する。別の方法として、図 5 のシーケンス図は、ネットワーク環境 100 内に実装された方法の要素の例を描写していると見なすことができる。

【0081】

ステップ 503 から始めて、クライアントアプリケーション 143 は、データ項目 133 の要求をホストされたアプリケーション 119 に送信する。これには、例えば、ファイルの要求、ウェブページの要求などが含まれる。

【0082】

ステップ 506 で、ホストされたアプリケーション 119 は、要求に応答して、それぞれの認証レコード 126 で識別されたそれぞれの ID キー 131 と共に、データ項目 136 を提供する。ID キー 131 は、様々なカスタムプロトコル又は既存のプロトコルの拡張機能を使用して提供できる。例えば、追加のハイパーテキストトランスポートプロトコル (HTTP) ヘッダを応答に含めて、データ項目 133 に関連付けられた ID キーを示すことができる。

【0083】

続いて、ステップ 509 で、クライアントアプリケーション 143 は、応答中の ID キー 131 を認識し、それぞれの身分証明書 136 を取得する。例えば、クライアントアプリケーション 143 は、ID キー 131 を使用して、分散型台帳 113 に記憶されたそれぞれの身分証明書 136 を検索し、それを取得することができる。複数の分散型台帳 113 が使用される場合、クライアントアプリケーション 143 は、ID キー 131 を D ID リゾルバなどのリレー又はリゾルバサービスに送信して、どの分散型台帳 113 が身分証明書 136 を含むかを決定することができる。これらの例では、リレー又はリゾルバサービスは、クライアントアプリケーション 143 に代わって身分証明書 136 を取得し、それをセキュリティサービス 121 に返すことができる。

【0084】

次に、ステップ 513 で、クライアントアプリケーション 143 は、暗号化チャレンジ

を作成し、ホストされたアプリケーション 119 に送信することができる。したがって、クライアントアプリケーション 143 は、ステップ 509 で取得された身分証明書 136 の公開キー 163 を使用して、暗号化チャレンジとして使用するためにトークン又はノンスを暗号化することができ、これをホストされたアプリケーション 119 に送信することができる。

【0085】

ステップ 516 で、ホストされたアプリケーション 119 は、暗号化チャレンジをボルトマネージャ 149 に転送することができる。暗号化チャレンジは、認証レコード 126 によってデータ項目 133 にリンクされた ID キー 131 に関連付けられた秘密キー 166 を使用して、暗号化チャレンジを復号化及び署名するためのボルトマネージャ 149 の要求の一部として転送できる。

10

【0086】

ステップ 519 での応答において、ボルトマネージャ 149 は、暗号化チャレンジを復号化及び署名し、復号化された暗号化チャレンジ及び暗号化チャレンジのための署名をホストされたアプリケーション 119 に提供することができる。例えば、ボルトマネージャ 149 は、最初に、データ項目 133 にリンクされた ID キー 131 に関連付けられたキー対 159 の秘密キー 166 を取得することができる。次に、ボルトマネージャ 149 は、暗号化されたチャレンジを復号化して、クライアントアプリケーション 143 によって提供された元のトークン又はノンスを再作成することができる。次に、ボルトマネージャ 149 は、秘密キー 166 を用いてトークン又はノンスに署名して、他のアプローチを通じて暗号化されていないトークン又はノンスを取得する代わりに、ホストされたアプリケーション 119 の秘密キー 166 の所有者がチャレンジを復号化したことを証明することができる。次に、ボルトマネージャ 149 は、暗号化されていないトークン又はノンス、並びにそれぞれの署名を、ホストされたアプリケーション 119 に提供することができる。

20

【0087】

次に、ステップ 523 において、ホストされたアプリケーション 119 は、暗号化されていないノンス又はトークン、及びノンス又はトークンの署名をクライアントアプリケーション 143 に送信することができる。これは、クライアントアプリケーション 143 によって取得された身分証明書 136 がデータ項目 133 に関連付けられており、データ項目 133 に関する有効な確認済みクレーム 169 を含むことを示すことができる。

30

【0088】

次に、ステップ 526 で、クライアントアプリケーション 143 は、ステップ 509 で取得された身分証明書 136 に含まれる確認済みクレーム 169 を評価することができる。例えば、クライアントアプリケーション 143 は、各クレーム 173 を評価して、データ項目 133 について何が主張されているか（例えば、それが安全であるか、マルウェアが含まれているか、ファイルの作成者とされる有効なサイト又はなりすましサイトへのリンクであるかなど）を決定することができる。クライアントアプリケーション 143 はまた、確認済みクレーム 169 の各クレーム 173 のそれぞれの署名 176 が正しいことを確認して、各クレーム 173 が有効であることを保証することができる。

40

【0089】

場合によっては、クライアントアプリケーション 143 はまた、クレーム 173 においてアサーションを行う当事者を信頼するかどうかを決定することができる。例えば、署名 176 は、クレーム 173 を行ったセキュリティサービス 121 を指定することができる。あるセキュリティサービス 121 は、別のセキュリティサービス 121 よりもクライアントアプリケーション 143 によってより信頼され得る（例えば、一つのセキュリティサービス 121 は、より徹底的又はより正確であったという履歴を有する可能性がある）。したがって、クライアントアプリケーション 143 は、特定のセキュリティサービス 121 によって行われる場合、特定のクレーム 173 を無視することを選択することができ、又は、信頼できないセキュリティサービス 121 による特定のアサーションを信頼できる

50

ようにするために、複数の信頼できないセキュリティサービス 1 2 1 がそれぞれのクレーム 1 7 3 で同じアサーションを行うことを要求する場合がある。

【0 0 9 0】

最後に、ステップ 5 2 9 で、クライアントアプリケーション 1 4 3 は、確認済みクレーム 1 6 9 に含まれるクレーム 1 7 3 に少なくとも部分的に基づいて、ユーザインタフェース 1 4 6 をレンダリングする。一部の実装形態では、信頼できるソースからのものである、確認済みクレーム 1 6 9 のクレーム 1 7 3 のみが、ユーザインタフェース 1 4 6 に組み込まれ得る。例えば、クライアントアプリケーション 1 4 3 は、データ項目 1 3 3 のステータスの表示と共にデータ項目 1 3 3 を表示するユーザインタフェース 1 4 6 をレンダリングすることができる。例えば、ユーザインタフェースは、ウェブサイトが安全であること、リンクがウェブサイトの有効なリンクであること、ファイルにマルウェアが含まれていないこと、又はファイルの作成者又は配布者が本人であることを示すことができる。

10

【0 0 9 1】

次に図 6 を参照すると、ネットワーク環境 1 0 0 の構成要素の動作の別の例を提供するシーケンス図が示されている。図 6 のシーケンス図は、ネットワーク環境 1 0 0 の図示された部分の動作を実装するために使用することができる多くの異なるタイプの機能的配置の単なる例を提供することが理解される。別の方法として、図 6 のシーケンス図は、ネットワーク環境 1 0 0 内に実装された方法の要素の例を描写していると見なすことができる。

【0 0 9 2】

図 6 のシーケンス図は、図 5 の範囲と同様であることに留意されたい。しかしながら、図 5 のシーケンス図は、ボルトマネージャ 1 4 9 の使用を示し、一方、図 6 のシーケンス図は、ボルトマネージャ 1 4 9 の使用を省略した代替の実装を示している。

20

【0 0 9 3】

ステップ 6 0 3 から始めて、クライアントアプリケーション 1 4 3 は、データ項目 1 3 3 の要求をホストされたアプリケーション 1 1 9 に送信する。これには、例えば、ファイルの要求、ウェブページの要求などが含まれる。

【0 0 9 4】

ステップ 6 0 6 で、ホストされたアプリケーション 1 1 9 は、それぞれの認証レコード 1 2 6 で識別されたそれぞれの ID キー 1 3 1 と共に、応答してデータ項目 1 3 6 を提供する。ID キー 1 3 1 は、様々なカスタムプロトコル又は既存のプロトコルの拡張機能を使用して提供できる。例えば、追加のハイパーテキストトランスポートプロトコル (HTTP) ヘッダを応答に含めて、データ項目 1 3 3 に関連付けられた ID キーを示すことができる。

30

【0 0 9 5】

続いて、ステップ 6 0 9 で、クライアントアプリケーション 1 4 3 は、応答中の ID キー 1 3 1 を認識し、それぞれの身分証明書 1 3 6 を取得する。例えば、クライアントアプリケーション 1 4 3 は、ID キー 1 3 1 を使用して、分散型台帳 1 1 3 に記憶されたそれぞれの身分証明書 1 3 6 を検索し、それを取得することができる。複数の分散型台帳 1 1 3 が使用される場合、クライアントアプリケーション 1 4 3 は、ID キー 1 3 1 を D I D リゾルバなどのリレー又はリゾルバサービスに送信して、どの分散型台帳 1 1 3 が身分証明書 1 3 6 を含むかを決定することができる。これらの場合、リレー又はリゾルバサービスは、クライアントアプリケーション 1 4 3 に代わって身分証明書 1 3 6 を取得し、それをセキュリティサービス 1 2 1 に返すことができる。

40

【0 0 9 6】

次に、ステップ 6 1 3 で、クライアントアプリケーション 1 4 3 は、暗号化チャレンジを作成し、ホストされたアプリケーション 1 1 9 に送信することができる。したがって、クライアントアプリケーション 1 4 3 は、ステップ 5 0 9 で取得された身分証明書 1 3 6 の公開キー 1 6 3 を使用して、暗号化チャレンジとして使用するためにトークン又はノンスを暗号化することができ、これをホストされたアプリケーション 1 1 9 に送信することができる。

50

【0097】

ステップ619で、ホストされたアプリケーション119は、暗号化チャレンジを復号化して署名し、復号化された暗号化チャレンジ及び暗号化チャレンジのための署名をホストされたアプリケーション119に提供することができる。例えば、ホストされたアプリケーション119は、データ項目133にリンクされたIDキー131に関連付けられたキー対159の秘密キー166を使用して、暗号化されたチャレンジを復号化し、クライアントアプリケーション143によって提供された元のトークン又はノンスを再作成できる。次に、ホストされたアプリケーション119は、秘密キー166を用いてトークン又はノンスに署名して、暗号化されていないトークン又はノンスを他の手段で取得する代わりに、ホストされたアプリケーション119の秘密キー166の所有者がチャレンジを復号化したことを証明することができる。

10

【0098】

次に、ステップ623において、ホストされたアプリケーション119は、暗号化されていないノンス又はトークン、及びノンス又はトークンの署名をクライアントアプリケーション143に送信することができる。これは、クライアントアプリケーション143によって取得された身分証明書136がデータ項目133に関連付けられており、データ項目133に関する有効な確認済みクレーム169を含むことを示すことができる。

【0099】

次に、ステップ626で、クライアントアプリケーション143は、ステップ609で取得された身分証明書136に含まれる確認済みクレーム169を評価することができる。例えば、クライアントアプリケーション143は、各クレーム173を評価して、データ項目133について何が主張されているか（例えば、それが安全であるか、マルウェアが含まれているか、ファイルの作成者とされる有効なサイト又はなりすましサイトへのリンクであるかなど）を決定することができる。クライアントアプリケーション143はまた、確認済みクレーム169の各クレーム173のそれぞれの署名176が正しいことを確認して、各クレーム173が有効であることを保証することができる。

20

【0100】

場合によっては、クライアントアプリケーション143はまた、クレーム173においてアサーションを行う当事者を信頼するかどうかを決定することができる。例えば、署名176は、クレーム173を行ったセキュリティサービス121を指定することができる。あるセキュリティサービス121は、別のセキュリティサービス121よりもクライアントアプリケーション143によってより信頼され得る（例えば、あるセキュリティサービス121は、より徹底的又はより正確であったという履歴を有する可能性がある）。したがって、クライアントアプリケーション143は、特定のセキュリティサービス121によって行われる場合、特定のクレーム173を無視することを選択することができ、又は信頼できないセキュリティサービス121による特定のアサーションを信頼できるようにするために、複数の信頼できないセキュリティサービス121がそれぞれのクレーム173で同じアサーションを行うことを要求する場合がある。

30

【0101】

最後に、ステップ629で、クライアントアプリケーション143は、確認済みクレーム169に含まれるクレーム173に少なくとも部分的に基づいて、ユーザインタフェース146をレンダリングする。一部の実装形態では、信頼できるソースからのものである、確認済みクレーム169のクレーム173のみが、ユーザインタフェース146に組み込まれ得る。例えば、クライアントアプリケーション143は、データ項目133のステータスの表示と共にデータ項目133を表示するユーザインタフェース146をレンダリングすることができる。例えば、ユーザインタフェースは、ウェブサイトが安全であること、リンクがウェブサイトの有効なリンクであること、ファイルにマルウェアが含まれていないこと、又はファイルの作成者又は配布者が本人であることを示すことができる。

40

【0102】

図7は、本開示の様々な実施形態による、クライアントアプリケーション143によっ

50

てディスプレイ 139 上にレンダリングされたユーザインタフェース 146 の例を示している。図 7 に示されるユーザインタフェース 146 は、本開示の実施の一例を示しているが、図 7 のユーザインタフェース 146 に開示されている原理は、同様の目的に使用される他のユーザインタフェース 146 に適合させることができる。

【0103】

図 7 の例は、ブラウザなどのクライアントアプリケーション 143 によってレンダリングされたユーザインタフェース 146 を示しており、これは、図 5 又は図 6 に先に示した確認プロセスの結果を組み込んでいる。ユーザインタフェース 146 には、前に図 5 又は図 6 に示したようなプロセスを使用して確認された複数のリンクが表示されている。各リンクについて確認済みクレーム 169 の評価に応答して、ユーザインタフェース要素 703 が、リンクのステータスを示すために各リンクの隣に挿入されている。例えば、一部のリンクには「承認済み」と表示されている場合がある。このステータスは、これらのリンクが、正当なウェブサイトになりすましたウェブサイトユーザを誘導するかどうか、又はリンクによって到達可能なウェブサイトにセキュリティの脆弱性が含まれるかどうかなど、該当するすべての確認規則 129 に準拠していることを示し得る。対照的に、他のリンクには、これらのリンクが少なくとも一つの該当する確認規則 129 に準拠していないことをユーザに警告するために、「クリックしないでください」という指示が含まれている場合がある。これらすべてのユーザインタフェース要素 703 は、情報がどのようにユーザに伝達され得るかについての例示的な例を含み、他のアプローチが適宜使用され得る。

【0104】

図 8 は、本開示の様々な実施形態による、クライアントアプリケーション 143 によってディスプレイ 139 上にレンダリングされたユーザインタフェース 146 の例を示している。図 8 に示されるユーザインタフェース 146 は、本開示の実装の一例を示しており、図 8 のユーザインタフェース 146 に開示されている原理は、同様の目的に使用される他のユーザインタフェース 146 に適合させることができる。

【0105】

図 8 の例は、ブラウザなどのクライアントアプリケーション 143 によってレンダリングされたユーザインタフェース 146 を示しており、これは、図 5 又は図 6 に先に示した確認プロセスの結果を組み込んでいる。ユーザインタフェース 146 には、前に図 5 又は図 6 に示したようなプロセスを使用して確認された複数のリンクが表示されている。ユーザがアクセスしようとしているファイルについての確認済みクレーム 169 の評価に応答して、ファイルのステータスを示すためにダイアログボックス 803 がレンダリングされた。ダイアログボックス 803 で任意のステータスをレンダリングすることができるが、一部の实装形態は、ファイルが少なくとも一つの確認規則 129 に準拠しない場合にのみダイアログボックス 803 をレンダリングすることを選択することができる。例えば、ファイルにマルウェアが含まれている場合、又はファイルがファイルの作成者又は配布者から発信されたのではないように見える場合、ダイアログボックス 803 がレンダリングされ得る。

【0106】

前述のいくつかのソフトウェア構成要素は、それぞれのコンピューティングデバイスのメモリに記憶され、プロセッサのそれぞれのコンピューティングデバイスによって実行可能である。この点で、「実行可能」という用語は、最終的にプロセッサが実行できる形式のプログラムファイルを意味する。実行可能プログラムの例としては、メモリのランダムアクセス部分にロードしてプロセッサで実行できる形式のマシンコード、メモリのランダムアクセス部分にロードされてプロセッサによって実行され得るオブジェクトコードなどの適切な形式で表現できるソースコード、又は別の実行可能プログラムによって解釈されて、プロセッサによって実行されるメモリのランダムアクセス部分に命令を生成できるソースコードに変換できるコンパイル済みプログラムであり得る。実行可能なプログラムは、ランダムアクセスメモリ (RAM)、読み取り専用メモリ (ROM)、ハードドライブ、ソリッドステートドライブ、ユニバーサルシリアルバス (USB) フラッシュドライブ

、メモ리카ード、コンパクトディスク（ＣＤ）若しくはデジタル多用途ディスク（ＤＶＤ）などの光学ディスク、フロッピーディスク、磁気テープ、又はその他のメモリ構成要素を含む、メモリの任意の部分又は構成要素に記憶できる。

【０１０７】

メモリは、揮発性及び不揮発性メモリ及びデータストレージ構成要素の両方を含む。揮発性構成要素とは、電力が失われたときにデータ値を保持しない構成要素である。不揮発性構成要素とは、電力が失われたときにデータを保持する構成要素である。したがって、メモリには、ランダムアクセスメモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、ハードディスクドライブ、ソリッドステートドライブ、ＵＳＢフラッシュドライブ、メモ리카ードリーダーを介してアクセスされるメモ리카ード、関連するフロッピーディスクドライブを介してアクセスされるフロッピーディスク、光ディスクドライブを介してアクセスされる光ディスク、適切なテープドライブを介してアクセスされる磁気テープ、若しくは他のメモリ構成要素、又はこれらのメモリ構成要素の任意の二つ以上の組み合わせを含めることができる。更に、ＲＡＭには、スタティックランダムアクセスメモリ（ＳＲＡＭ）、ダイナミックランダムアクセスメモリ（ＤＲＡＭ）、又は磁気ランダムアクセスメモリ（ＭＲＡＭ）などのデバイスを含めることができる。ＲＯＭは、プログラム可能な読み取り専用メモリ（ＰＲＯＭ）、消去可能なプログラム可能な読み取り専用メモリ（ＥＰＲＯＭ）、電氣的に消去可能なプログラム可能な読み取り専用メモリ（ＥＥＰＲＯＭ）、又は他の同様のメモリデバイスを含むことができる。

【０１０８】

本明細書に記載のアプリケーション及びシステムは、上記のように汎用ハードウェアによって実行されるソフトウェア又はコードで具体化することができるが、代替として、同じものを専用ハードウェア又はソフトウェア／汎用ハードウェア及び専用ハードウェアの組み合わせで具体化することもできる。専用のハードウェアで具体化されている場合、それぞれは、いくつかの技術のいずれか一つ又は組み合わせを採用する回路又はステートマシンとして実装できる。これらの技術には、一つ若しくは複数のデータ信号の適用時に様々な論理機能を実装するための論理ゲートを備えたディスクリート論理回路、適切な論理ゲートを備えた特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラム可能なゲートアレイ（ＦＰＧＡ）、又は他の構成要素などが含まれ得るが、これらに限定されない。そのような技術は、一般に当業者によく知られており、したがって、本明細書では詳細に説明されていない。

【０１０９】

シーケンス図は、本開示の様々な実施形態の一部の実装の機能及び動作を示す。ソフトウェアで具体化される場合、各ブロックは、指定された論理機能を実装するためのプログラム命令を含むモジュール、セグメント、又はコードの一部を表すことができる。プログラム命令は、プログラミング言語で書かれた人間が読めるステートメントを含むソースコード、又はコンピュータシステムのプロセッサなどの適切な実行システムによって認識可能な数値命令を含むマシンコードの形式で具体化することができる。マシンコードは、様々なプロセスを通じてソースコードから変換できる。例えば、マシンコードは、対応するアプリケーションを実行する前に、コンパイラを使用してソースコードから生成できる。別の例として、マシンコードは、インタプリタによる実行と同時にソースコードから生成できる。他のアプローチも使用できる。ハードウェアで具体化される場合、各ブロックは、指定された論理機能（複数可）を実装するための回路又は相互接続されたいくつかの回路を表すことができる。

【０１１０】

シーケンス図は特定の実行順序を示しているが、実行順序は図示されているものとは異なる可能性があることが理解される。例えば、二つ以上のブロックの実行順序は、示されている順序に対してスクランブルすることができる。また、連続して表示される二つ以上のブロックは、同時に実行することも、又は部分的に同時に実行することもできる。更に、いくつかの実施形態では、シーケンス図に示される一つ又は複数のブロックをスキップ

10

20

30

40

50

又は省略することができる。更に、ユーティリティ、アカウンティング、性能測定の強化、又はトラブルシューティング支援の提供などの目的で、本明細書で説明する論理フローに任意の数のカウンタ、状態変数、警告セマフォ、又はメッセージを追加できる。そのようなすべての変形は、本開示の範囲内であることが理解される。

【0111】

また、ソフトウェア又はコードを含む本明細書に記載の任意の論理又はアプリケーションは、コンピュータシステム又は他のシステムのプロセッサなどの命令実行システムによって、又はそれに関連して使用するために、任意の非一時的なコンピュータ可読媒体に具現化することができる。この意味で、論理は、コンピュータ可読媒体からフェッチされ、命令実行システムによって実行され得る命令及び宣言を含むステートメントを含むことができる。本開示の文脈において、「コンピュータ可読媒体」は、命令実行システムによって、又はそれに関連して使用するために、本明細書に記載の論理又はアプリケーションを含む、記憶する、又は維持することができる任意の媒体であり得る。

【0112】

コンピュータ可読媒体は、磁気媒体、光学媒体、又は半導体媒体などの多くの物理媒体のいずれか一つを含むことができる。適切なコンピュータ可読媒体のより具体的な例には、磁気テープ、磁気フロッピーディスク、磁気ハードドライブ、メモリカード、ソリッドステートドライブ、USBフラッシュドライブ、又は光ディスクが含まれるが、これらに限定されない。また、コンピュータ可読媒体は、スタティックランダムアクセスメモリ（SRAM）及びダイナミックランダムアクセスメモリ（DRAM）を含むランダムアクセスメモリ（RAM）、又は磁気ランダムアクセスメモリ（MRAM）であり得る。更に、コンピュータ可読媒体は、読み取り専用メモリ（ROM）、プログラム可能な読み取り専用メモリ（PROM）、消去可能なプログラム可能な読み取り専用メモリ（EPROM）、電氣的に消去可能なプログラム可能な読み取り専用メモリ（EEPROM）又は他のタイプのメモリデバイスであり得る。

【0113】

更に、本明細書に記載の任意の論理又はアプリケーションは、様々な方法で実装及び構造化することができる。例えば、説明されている一つ又は複数のアプリケーションは、単一のアプリケーションのモジュール又は構成要素として実装できる。更に、本明細書で説明される一つ又は複数のアプリケーションは、共有若しくは別個のコンピューティングデバイス又はそれらの組み合わせで実行することができる。例えば、本明細書で説明される複数のアプリケーションは、同じコンピューティングデバイスで、又は同じコンピューティング環境内の複数のコンピューティングデバイスで実行することができる。

【0114】

特に明記されていない限り、「X、Y、又はZの少なくとも一つ」というフレーズなどの選言的文言は、アイテム、用語などがX、Y、若しくはZのいずれか、又はそれらの任意の組み合わせ（例えば、X、Y、又はZ）である可能性があることを示すために一般的に使用される文脈で別の方法で理解される。したがって、そのような選言的文言は、一般に、特定の実施形態がそれぞれ存在するためにXの少なくとも一つ、Yの少なくとも一つ、又はZの少なくとも一つを必要とすることを意味することを意図せず、また意味するべきではない。

【0115】

本開示の上記の実施形態は、本開示の原理を明確に理解するために提示された実装例の単なる可能な例であることを強調すべきである。本開示の趣旨及び原理から実質的に逸脱することなく、上記の実施形態に対して多くの変形及び修正を行うことができる。そのようなすべての修正及び変形は、本開示の範囲内に本明細書に含まれ、以下の特許請求の範囲によって保護されることが意図されている。

【0116】

一つ又は複数の例示的な実装は、以下の条項に示されている。以下の条項は実装例を説明しているが、本開示の他の実装も前のページ及び図で説明されている。したがって、以

下の条項は、本開示の例示的な例を説明しているが、本開示の唯一の実装を説明しているわけではない。

【0117】

条項1－プロセッサ及びメモリを含むコンピューティングデバイスと、メモリに記憶された機械可読命令と、を含むシステムであって、機械可読命令は、プロセッサによって実行されると、コンピューティングデバイスに少なくとも、データ項目のIDキーを生成することと、データ項目の認証要求をセキュリティサービスに送信することであって、この要求は、IDキー及びデータ項目を含む、ことと、セキュリティサービスからデータ項目の確認済みクレームを受信することと、身分証明書を生成することであって、身分証明書は、データ項目のIDキー及び確認済みクレームを含む、ことと、身分証明書を分散型台帳に記憶する、ことと、行わせる、システム。

10

【0118】

条項2－条項1のシステムであって、機械可読命令は、コンピューティングデバイスによって実行されると、更に、コンピューティングデバイスに少なくとも、データ項目の要求を受信する、ことと、要求への応答を送信することであって、応答はデータ項目及びIDキーを含む、ことと、を行わせる、システム。

【0119】

条項3－条項1又は2のシステムであって、IDキーは、第2のIDキーであり、身分証明書は第2の身分証明書であり、データ項目の認証要求は、認証の第2の要求であり、機械可読命令は更に、コンピューティングデバイスに少なくとも、機械可読命令のオペレータのIDの認証要求を認証サービスに送信することと、認証サービスから第1のIDキー及び確認済みクレームを受信することと、第1の身分証明書を作成することであって、身分証明書は、IDキー及び確認済みクレームを含む、ことと、第1の身分証明書を分散型台帳に記憶することであって、データ項目の認証のための第2の要求は、第1の身分証明書が分散型台帳に記憶されるのに続いて送信される、ことと、を行わせる、システム。

20

【0120】

条項4－条項1～3のシステムであって、機械可読命令は、プロセッサによって実行されると、コンピューティングデバイスに少なくとも、データ項目に一意に関連付けられた非対称キー対を生成させ、身分証明書は、非対称キー対の公開キーを更に含む、システム。

【0121】

条項5－条項4のシステムであって、機械可読命令は、プロセッサによって実行されると、更に、コンピューティングデバイスに少なくとも、公開キーで暗号化された暗号化トークンを含む確認要求を受信することと、暗号化されていないトークンを生成するために、非対称キー対の秘密キーを使用して暗号化されたトークンを復号化することと、秘密キーを使用して、暗号化されていないトークンの暗号化署名を作成することと、暗号化されていないトークン及び暗号化署名を含む確認応答を提供することと、を行わせる、システム。

30

【0122】

条項6－データ項目がネットワークアドレスである、条項1～5のシステム。

【0123】

条項7－データ項目がファイルである、条項1～5のシステム。

40

【0124】

第8項－データ項目の確認要求を受信することであって、確認要求は、IDキー及びデータ項目を含む、ことと、データ項目が少なくとも一つの確認規則に準拠していることを決定することと、データ項目の確認済みクレームを生成することであって、確認済みクレームは、IDキーがデータ項目に関連付けられており、データ項目が少なくとも一つの確認規則に準拠していることを示す、ことと、データ項目の認証要求への応答として確認済みクレームを提供することと、を含む、方法。

【0125】

条項9－条項8の方法であって、IDキーは、第2のIDキーである。少なくとも一つ

50

の確認規則は、データ項目が認証されたエンティティから発信されていることを示す。認証要求は、認証されたエンティティに関連付けられた第1のIDキーを更に含む。データ項目が少なくとも一つの確認規則に準拠していることを決定することは、認証要求が認証されたエンティティから発信されていることを、少なくとも部分的に第1のIDキーに基づいて確認することを更に含む。確認済みクレームの生成は、認証要求が認証済みエンティティから発信されているとの確認に応答して発生する。

【0126】

第10項－第9項の方法であって、少なくとも部分的に第1のIDキーに基づいて、認証要求が認証されたエンティティから発信されていることを確認することは、第1のIDキーに関連付けられた身分証明書を取得することであって、身分証明書は、それぞれの非対称キー対の公開暗号化キーを含む、ことと、暗号化されたトークンを作成するために、公開暗号化キーを使用してトークンを暗号化することと、認証要求を送信した発信元エンティティに暗号化されたトークンを送信することと、それぞれの非対称キー対の秘密キーで作成されたトークン及びデジタル署名を受信することと、公開暗号化キーを使用してデジタル署名を確認することと、を更に含む。

【0127】

条項11－条項8～10の方法であって、少なくとも一つの確認規則は、データ項目が指定されたセキュリティポリシーに準拠していることを示し、データ項目が少なくとも一つの確認規則に準拠していることを決定することは、データ項目のセキュリティ分析を実行することを更に含む。

【0128】

条項12－条項8～11の方法であって、IDキー及び確認済みクレームを含む身分証明書を作成することと、身分証明書を分散型台帳に登録することと、を更に含む、方法。

【0129】

条項13－データ項目がネットワークアドレスである、条項8～12の方法。

【0130】

条項14－データ項目がファイルである、条項8～12の方法。

【0131】

条項15－機械可読命令を含む非一時的なコンピュータ可読媒体であって、機械可読命令は、コンピューティングデバイスのプロセッサによって実行されると、コンピューティングデバイスに少なくとも、データ項目の要求をアプリケーションに送信することと、アプリケーションからデータ項目及びIDキーを受信することであって、IDキーはデータ項目にリンクされている、ことと、分散型台帳からIDキーによって識別される身分証明書を取得することであって、身分証明書には、データ項目に関連する少なくとも一つの確認済みクレームが含まれる、ことと、身分証明書に少なくとも部分的に基づいてデータ項目を確認することと、データ項目の確認の結果に少なくとも部分的に基づいてユーザインタフェースをレンダリングすることと、を行わせる、非一時的なコンピュータ可読媒体。

【0132】

条項16－条項15の非一時的なコンピュータ可読媒体であって、機械可読命令は、プロセッサによって実行されると、更に、コンピューティングデバイスに少なくとも、暗号化されたトークンを作成するために、身分証明書に含まれている公開鍵を使用してトークンを暗号化することと、暗号化されたトークンをアプリケーションに送信することと、アプリケーションからトークンを受け取り、トークンに関連付けられた暗号化署名を受信することと、暗号化署名を確認することと、を行わせる、非一時的なコンピュータ可読媒体。

【0133】

条項17－条項15又は16の非一時的なコンピュータ可読媒体であって、コンピューティングデバイスに、少なくとも部分的に身分証明書に基づいてデータ項目を確認させる機械可読命令は、コンピューティングデバイスに、確認済みクレームの少なくとも一つのクレームを少なくとも評価させ、少なくとも一つのクレームは、データ項目の少なくとも一つの確認規則への準拠に関するアサーションを含む、非一時的なコンピュータ可読媒体。

【 0 1 3 4 】

条項 1 8 – 条項 1 7 の非一時的なコンピュータ可読媒体であって、コンピューティングデバイスに少なくとも一つのクレームを少なくとも評価させる機械可読命令は、コンピューティングデバイスに、クレームが信頼できるエンティティによって行われたことを決定させる、非一時的なコンピュータ可読媒体。

【 0 1 3 5 】

条項 1 9 – データ項目がネットワークアドレスである、条項 1 5 ～ 1 8 の非一時的なコンピュータ可読媒体。

【 0 1 3 6 】

条項 2 0 – データ項目がファイルである、請求項 1 5 ～ 1 8 の非一時的なコンピュータ可読媒体。

10

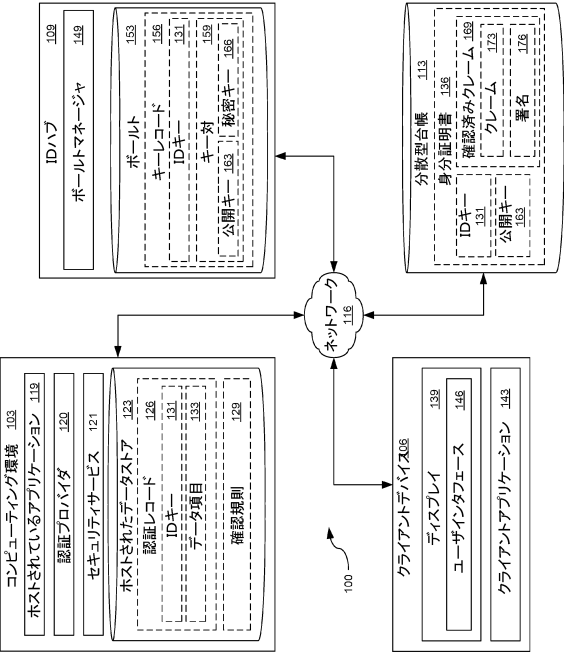
20

30

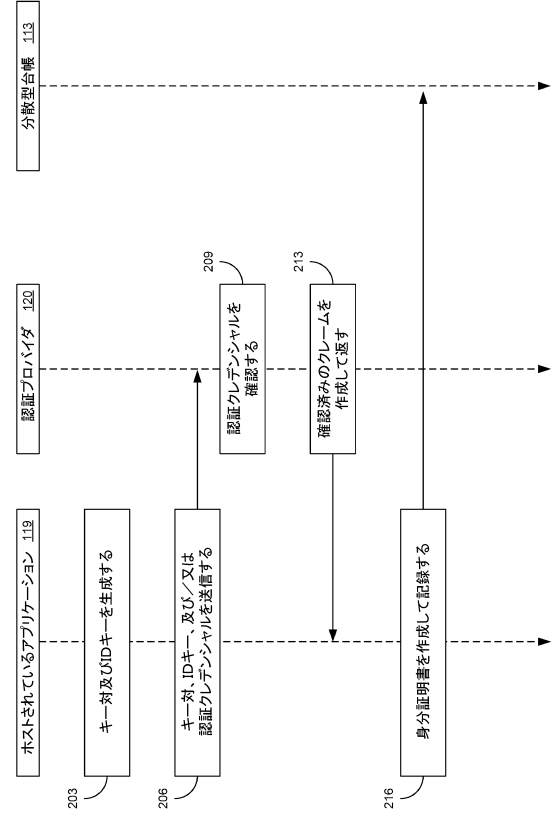
40

50

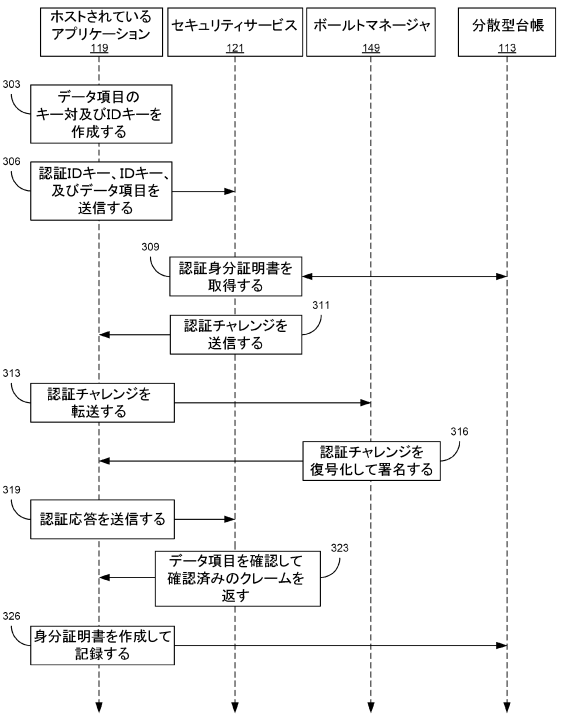
【図面】
【図 1】



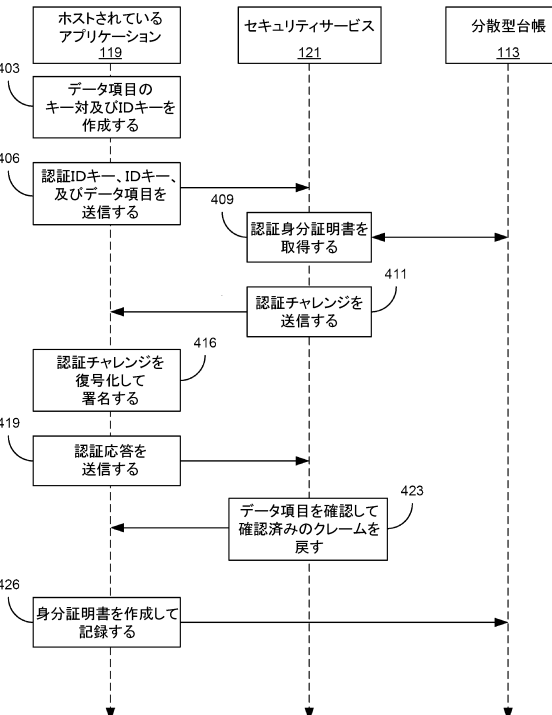
【図 2】



【図 3】



【図 4】



10

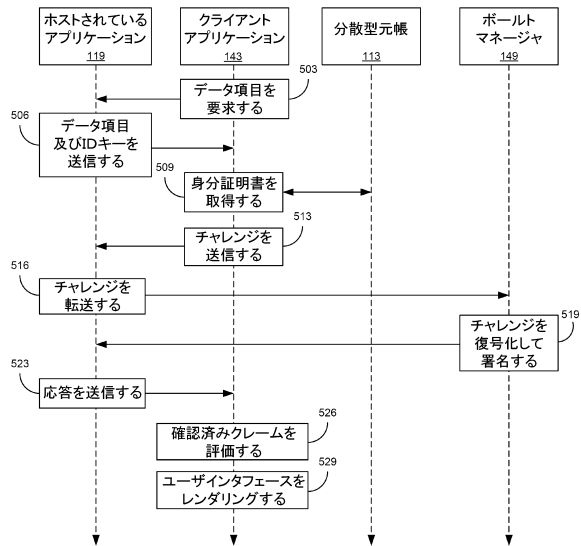
20

30

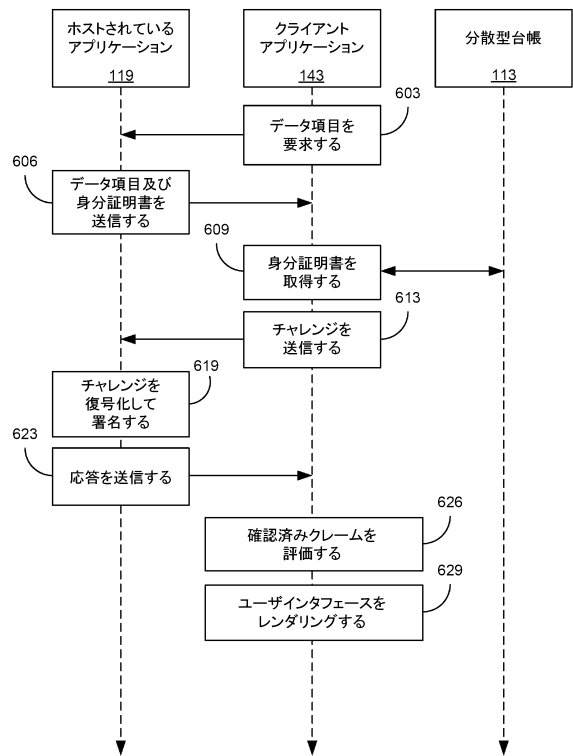
40

50

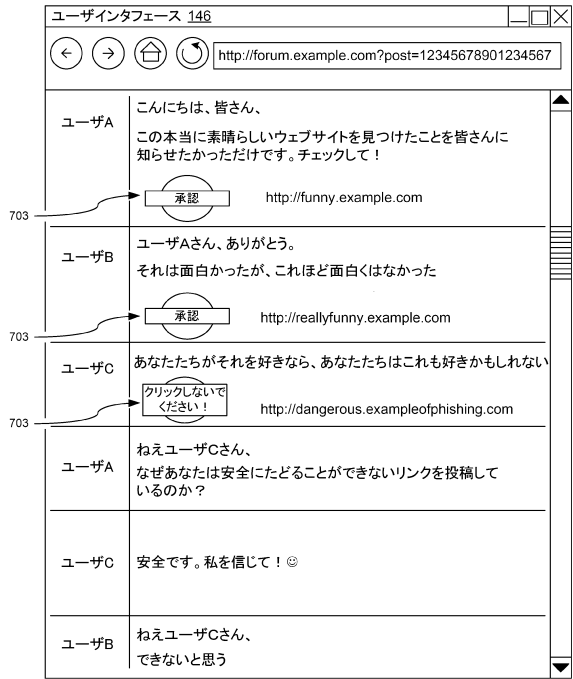
【図 5】



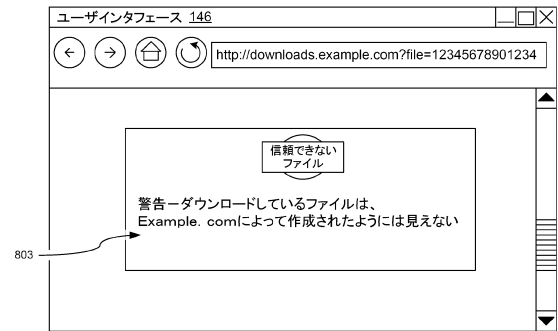
【図 6】



【図 7】



【図 8】



10

20

30

40

50

フロントページの続き

(72)発明者 フェレンツィ, アンドラス, エル.
 アメリカ合衆国 1 0 2 8 5 - 4 9 0 0 ニューヨーク州、ニューヨーク、ヴィージー ストリート
 2 0 0、アメリカン エクスプレス トラヴェル リレイテッド サーヴィシーズ カンパニー, イ
 ンコーポレイテッド 内

 審査官 金沢 史明

(56)参考文献 特開 2 0 0 5 - 1 9 0 4 5 2 (J P , A)
 米国特許第 1 0 2 9 8 3 9 6 (U S , B 1)
 中国特許出願公開第 1 0 7 9 5 8 3 7 1 (C N , A)

(58)調査した分野 (Int.Cl., D B 名)
 H 0 4 L 9 / 0 0 - 9 / 4 0
 G 0 9 C 1 / 0 0 - 5 / 0 0
 G 0 6 F 2 1 / 0 0 - 2 1 / 8 8