(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7421771号
(P7421771)

(45)発行日　令和6年1月25日(2024.1.25)

(24)登録日　令和6年1月17日(2024.1.17)

(51)国際特許分類		FI		
H04L 9/08 (2006.01)		H04L	9/08	F
H04L 9/32 (2006.01)		H04L	9/32	200B
G06F 21/44 (2013.01)		H04L	9/32	200F
		G06F	21/44	

請求項の数　11　（全24頁）

(21)出願番号　特願2020-540501(P2020-540501)
(86)(22)出願日　平成31年1月28日(2019.1.28)
(65)公表番号　特表2021-511743(P2021-511743A)
(43)公表日　令和3年5月6日(2021.5.6)
(86)国際出願番号　PCT/CN2019/073518
(87)国際公開番号　WO2019/144963
(87)国際公開日　令和1年8月1日(2019.8.1)
審査請求日　令和4年1月18日(2022.1.18)
(31)優先権主張番号　201810078175.2
(32)優先日　平成30年1月26日(2018.1.26)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　519195453
ヴィチェーン グローバル テクノロジー エス・アー エール・エル
ルクセンブルク、ポストコード ２３５１、リュ デ プリムヴェール １６
(74)代理人　100136319
弁理士　北原 宏修
(74)代理人　100148275
弁理士　山内 聡
(74)代理人　100142745
弁理士　伊藤 世子
(74)代理人　100143498
弁理士　中西 健
(72)発明者　ヤンユー チェン
中華人民共和国， シャンハイ ２００１
最終頁に続く

(54)【発明の名称】　ＩＯＴサービスを実施するための方法、アプリケーションサーバ、ＩＯＴ装置および媒体

(57)【特許請求の範囲】
【請求項１】
ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施するためのＩｏＴ装置であって、
ＩｏＴ装置公開鍵(P_{IoT})とＩｏＴ装置秘密鍵(K_{IoT})との対で構成され、
メモリとプロセッサとを備え、
前記メモリは、機械実行可能命令を格納し、
前記機械実行可能命令は、前記プロセッサによって実行されると、前記ＩｏＴ装置に処理を実行させ、
前記処理は、
使用者装置から認証要求を受信することと、
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記認証要求とに基づいて前記使用者装置を認証して使用者公開鍵(P_u)を取得することと、
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することと、
前記ＩｏＴ装置の前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するという判定に応じて、前記使用者装置の認証が成功すると判定することとを含み、
前記使用者装置は、前記使用者公開鍵(P_u)と使用者秘密鍵(K_u)との対で構成され、
前記認証要求は、前記使用者装置の使用者データのハッシュ値と、前記ＩｏＴ装置公開鍵(P_{IoT})を使用して使用者乱数(R_u)を暗号化することに基づいて取得される第１の暗号化

情報と、前記使用者秘密鍵(K_u)を使用して前記ハッシュ値を暗号化することによって前記使用者装置の使用者署名を生成すると共に前記使用者乱数(R_u)を使用して前記使用者署名を暗号化することに基づいて取得される第２の暗号化情報とを含む、
ＩｏＴ装置。
【請求項２】
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記認証要求とに基づいて前記使用者装置を認証して使用者公開鍵(P_u)を取得することは、
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記第１の暗号化情報とに基づいて前記使用者乱数(R_u)を計算することと、
前記使用者乱数(R_u)と前記第２の暗号化情報とに基づいて前記使用者装置の前記使用者署名を計算することと、
楕円曲線暗号を使用して前記使用者署名と前記ハッシュ値に基づいて前記使用者公開鍵(P_u)を決定することとをさらに備える、
請求項１に記載のＩｏＴ装置。
【請求項３】
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記第１の暗号化情報とに基づいて前記使用者乱数(R_u)を計算することは、
「$R_u = K^{-1}_{IoT}(P_{IoT}(R_u))$」式に従って前記使用者乱数($R_u$)を計算することを備え、
$P_{IoT}(R_u)$は、前記第１の暗号化情報を表し、
K^{-1}_{IoT}は、前記ＩｏＴ装置秘密鍵(K_{IoT})を使用する復号化演算を表し、
前記使用者乱数(R_u)と前記第２の暗号化情報とに基づいて前記使用者装置の使用者署名を計算することは、
「$K_u(H) = R^{-1}_u(R_u(K_u(H)))$」式に従って前記使用者署名を計算することを備え、
$K_u(H)$は、前記使用者署名を表し、
Ｈは、前記使用者データの前記ハッシュ値を表し、
$R_u(K_u(H))$は、前記第２の暗号化情報を表し、
R^{-1}_uは、前記使用者乱数(R_u)を使用する復号化演算を表す、
請求項２に記載のＩｏＴ装置。
【請求項４】
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することは、
前記使用者公開鍵(P_u)を前記ＩｏＴ装置の提供者に送信することを備え、
前記提供者は、前記提供者に属する各ＩｏＴ装置のアクセス許可使用者装置一覧を保存し、
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することは、
前記ＩｏＴ装置の前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうかを示す検索結果を、前記提供者から受信することをさらに備える、
請求項３に記載のＩｏＴ装置。
【請求項５】
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することは、
前記ＩｏＴ装置によって保存された前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することを備える、
請求項３に記載のＩｏＴ装置。
【請求項６】
ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施するための方法であって、
ＩｏＴ装置公開鍵(P_{IoT})とＩｏＴ装置秘密鍵(K_{IoT})との対で構成されるＩｏＴ装置によって実行され、

使用者装置から認証要求を受信することと、
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記認証要求とに基づいて前記使用者装置を認証して使用者公開鍵(P_u)を取得することと、
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することと、
前記ＩｏＴ装置の前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するという判定に応じて、前記使用者装置の認証が成功すると判定することとを備え、
前記使用者装置は、前記使用者公開鍵(P_u)と使用者秘密鍵(K_u)との対で構成され、
前記認証要求は、前記使用者装置の使用者データのハッシュ値と、前記ＩｏＴ装置公開鍵(P_{IoT})を使用して使用者乱数(R_u)を暗号化することに基づいて取得される第１の暗号化情報と、前記使用者秘密鍵(K_u)を使用して前記ハッシュ値を暗号化することによって前記使用者装置の使用者署名を生成すると共に前記使用者乱数(R_u)を使用して前記使用者署名を暗号化することに基づいて取得される第２の暗号化情報とを含む、
方法。
【請求項７】
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記認証要求とに基づいて前記使用者装置を認証して使用者公開鍵(P_u)を取得することは、
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記第１の暗号化情報とに基づいて前記使用者乱数(R_u)を計算することと、
前記使用者乱数(R_u)と前記第２の暗号化情報とに基づいて前記使用者装置の前記使用者署名を計算することと、
楕円曲線暗号を使用して前記使用者署名と前記ハッシュ値に基づいて前記使用者公開鍵(P_u)を決定することとをさらに備える、
請求項６に記載の方法。
【請求項８】
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記第１の暗号化情報とに基づいて前記使用者乱数(R_u)を計算することは、
「$R_u = K^{-1}_{IoT}(P_{IoT}(R_u))$」式に従って前記使用者乱数($R_u$)を計算することを備え、
$P_{IoT}(R_u)$は、前記第１の暗号化情報を表し、
K^{-1}_{IoT}は、前記ＩｏＴ装置秘密鍵(K_{IoT})を使用する復号化演算を表し、
前記使用者乱数(R_u)と前記第２の暗号化情報とに基づいて前記使用者装置の使用者署名を計算することは、
「$K_u(H) = R^{-1}_u(R_u(K_u(H)))$」式に従って前記使用者署名を計算することを備え、
$K_u(H)$は、前記使用者署名を表し、
Hは、前記使用者データの前記ハッシュ値を表し、
$R_u(K_u(H))$は、前記第２の暗号化情報を表し、
R^{-1}_uは、前記使用者乱数(R_u)を使用する復号化演算を表す、
請求項７に記載の方法。
【請求項９】
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することは、
前記使用者公開鍵(P_u)を前記ＩｏＴ装置の提供者に送信することを備え、
前記提供者は、前記提供者に属する各ＩｏＴ装置のアクセス許可使用者装置一覧を保存し、
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することは、
前記ＩｏＴ装置の前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうかを示す検索結果を、前記提供者から受信することをさらに備える、
請求項８に記載の方法。
【請求項１０】

前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することは、
前記ＩｏＴ装置によって保存された前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することを備える、
請求項８に記載の方法。
【請求項１１】
ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施するための不揮発性コンピュータ可読記憶媒体であって、
機械実行可能命令を備え、
前記機械実行可能命令は、機械によって実行されると、請求項６から１０のいずれか１項に記載の方法を前記機械に実施させるように適合される、
不揮発性コンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は一般に、Internet of Things（ＩｏＴ）の分野に関し、より詳細には、ブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するための方法、アプリケーションサーバ、ＩｏＴ装置、使用者装置およびコンピュータ可読記憶媒体に関する。
【背景技術】
【０００２】
現在、ＩｏＴ技術の発展に伴い、ますます多くのＩｏＴ装置が使用されている。これらのＩｏＴ装置は、通常、異なる装置提供者によって提供され、異なる製品規格を使用する。これらのＩｏＴ装置の識別子形式、物理的な接続方式または通信プロトコル、および、データ形式は統一されていないことがあり得るため、異なる提供者からのＩｏＴ装置を相互接続することは困難である。
【０００３】
これらのＩｏＴ装置を管理するため、各装置提供者は、集中制御センタを提供して、装置提供者が提供する対応ＩｏＴ装置を管理しなければならない。このような分散制御センタは比較的高い構築費用が必要になる。
【０００４】
一方、ますます多くのＩｏＴ装置が相互接続されるにつれて、付随するセキュリティ問題がますます顕著になっている。例えば、２０１５年７月、フィアット・クライスラーＵ．Ｓ．は、Ｕｃｏｎｎｅｃｔ車載システムを搭載した１４００万台の自動車をリコールすることを発表した。ハッカーが、遠隔ソフトウェアを使用して車載システムに指令を送り、減速、エンジンの停止およびブレーキの無効化などの車両の運転者および同乗者の安全に深刻な影響を及ぼす様々な操作を行うことができるからである。
【０００５】
さらに、各装置提供者によって提供されるＩｏＴ装置が各制御センタによって独立して管理される場合、制御センタは、ＩｏＴ装置のデータを完全に制御する。このため、異なる提供者によって提供されるＩｏＴ装置が相互作用する際に、取得データが改竄されていないことを保証しない場合がある。
【発明の概要】
【発明が解決しようとする課題】
【０００６】
上記の問題の少なくとも１つに鑑みて、本開示の実施形態は、信頼性ＩｏＴサービスを実施するための方法、アプリケーションサーバ、ＩｏＴ装置、使用者装置およびコンピュータ可読記憶媒体を提供する。
【課題を解決するための手段】
【０００７】
本開示の第１の局面によれば、ブロックチェーンに基づいて信頼性ＩｏＴサービスを実

施するためのアプリケーションサーバが提供される。前記アプリケーションサーバは、メモリとプロセッサとを含み、前記メモリは、機械実行可能命令を格納する。前記機械実行可能命令は、前記プロセッサによって実行されると、前記アプリケーションサーバに処理を実行させる。前記処理は、少なくとも１の提供者によって提供される複数のＩｏＴ装置の統一装置識別子規格を決定することと、前記複数のＩｏＴ装置の各ＩｏＴ装置の固有識別子を決定することと、ブロックチェーンプラットフォームに前記ＩｏＴ装置の前記固有識別子を登録することとを含む。前記固有識別子は、前記統一装置識別子規格に準拠し、前記ＩｏＴ装置の秘密鍵と対をなす前記ＩｏＴ装置の公開鍵である。

【０００８】

本開示の第２の局面によれば、ブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するための方法が提供される。前記方法は、少なくとも１の提供者によって提供される複数のＩｏＴ装置の統一装置識別子規格を決定することと、前記複数のＩｏＴ装置の各ＩｏＴ装置の固有識別子を決定することと、ブロックチェーンプラットフォームに前記ＩｏＴ装置の前記固有識別子を登録することとを含む。前記固有識別子は、前記統一装置識別子規格に準拠し、前記ＩｏＴ装置の秘密鍵と対をなす前記ＩｏＴ装置の公開鍵である。

【０００９】

本開示の第３の局面によれば、ブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するための不揮発性コンピュータ可読記憶媒体が提供される。前記記憶媒体は機械実行可能命令を含み、前記機械実行可能命令は、機械によって実行されると、前記第２の局面で説明した前記方法を前記機械に実施させるように適合される。

【００１０】

本開示の第４の局面によれば、ブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するためのＩｏＴ装置が提供される。前記ＩｏＴ装置は、ＩｏＴ装置公開鍵とＩｏＴ装置秘密鍵との対で構成される。前記ＩｏＴ装置は、メモリとプロセッサとを含み、前記メモリは、機械実行可能命令を格納する。前記機械実行可能命令は、前記プロセッサによって実行されると、前記ＩｏＴ装置に処理を実行させる。前記処理は、使用者装置から認証要求を受信することと、前記ＩｏＴ装置秘密鍵と前記認証要求とに基づいて前記使用者装置を認証して使用者公開鍵を取得することと、前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵が存在するかどうか判定することと、前記ＩｏＴ装置の前記アクセス許可使用者装置一覧に前記使用者公開鍵が存在するという判定に応じて、前記使用者装置の認証が成功すると判定することとを含む。前記使用者装置は、前記使用者公開鍵と使用者秘密鍵との対で構成される。前記認証要求は、前記使用者装置の使用者データのハッシュ値と、前記ＩｏＴ装置公開鍵と使用者乱数とに基づいて取得される第１の暗号化情報と、前記使用者秘密鍵と前記使用者乱数と前記ハッシュ値とに基づいて取得される第２の暗号化情報とを含む。

【００１１】

本開示の第５の局面によれば、ブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するための方法が提供される。前記方法は、ＩｏＴ装置公開鍵とＩｏＴ装置秘密鍵との対で構成されるＩｏＴ装置によって実行される。前記方法は、使用者装置から認証要求を受信することと、前記ＩｏＴ装置秘密鍵と前記認証要求とに基づいて前記使用者装置を認証して使用者公開鍵を取得することと、前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵が存在するかどうか判定することと、前記ＩｏＴ装置の前記アクセス許可使用者装置一覧に前記使用者公開鍵が存在するという判定に応じて、前記使用者装置の認証が成功すると判定することとを含む。前記使用者装置は、前記使用者公開鍵と使用者秘密鍵との対で構成される。前記認証要求は、前記使用者装置の使用者データのハッシュ値と、前記ＩｏＴ装置公開鍵と使用者乱数とに基づいて取得される第１の暗号化情報と、前記使用者秘密鍵と前記使用者乱数と前記ハッシュ値とに基づいて取得される第２の暗号化情報とを含む。

【００１２】

本開示の第６の局面によれば、ブロックチェーンに基づいて信頼性ＩｏＴサービスを実

施するための不揮発性コンピュータ可読記憶媒体が提供される。前記記憶媒体は機械実行可能命令を含み、前記機械実行可能命令は、機械によって実行されると、第５の局面で説明した方法を前記機械に実施させるように適合される。

【００１３】

本開示の第７の局面によれば、ブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するための使用者装置が提供される。前記使用者装置は、使用者公開鍵と使用者秘密鍵との対で構成される。前記使用者装置は、メモリとプロセッサとを含み、前記メモリは、機械実行可能命令を格納する。前記機械実行可能命令は、前記プロセッサによって実行されると、前記使用者装置に処理を実行させる。前記処理は、前記使用者装置の使用者データに対してハッシュ演算を実行して前記使用者データのハッシュ値を生成することと、ＩｏＴ装置のＩｏＴ装置公開鍵と使用者乱数とに基づいて第１の暗号化情報を取得することと、前記使用者秘密鍵と前記使用者乱数と前記ハッシュ値とに基づいて第２の暗号化情報を取得することと、認証要求を前記ＩｏＴ装置に送信することとを含む。前記認証要求は、前記使用者データの前記ハッシュ値と、前記第１の暗号化情報と、前記第２の暗号化情報とを含む。

【００１４】

本開示の第８の局面によれば、ブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するための方法が提供される。前記方法は、使用者公開鍵と使用者秘密鍵との対で構成される使用者装置によって実行される。前記方法は、前記使用者装置の使用者データに対してハッシュ演算を実行して前記使用者データのハッシュ値を生成することと、ＩｏＴ装置のＩｏＴ装置公開鍵と使用者乱数とに基づいて第１の暗号化情報を取得することと、前記使用者秘密鍵と前記使用者乱数と前記ハッシュ値に基づいて第２の暗号化情報を取得することと、認証要求を前記ＩｏＴ装置に送信することとを含む。前記認証要求は、前記使用者データの前記ハッシュ値と、前記第１の暗号化情報と、前記第２の暗号化情報とを含む。

【００１５】

本開示の第９の局面によれば、ブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するための不揮発性コンピュータ可読記憶媒体が提供される。前記記憶媒体は機械実行可能命令を含み、前記機械実行可能命令は、機械によって実行されると、前記第８の局面で説明した前記方法を前記機械に実施させるように適合される。

【図面の簡単な説明】

【００１６】

以下の図面と併せて示される本開示の具体的な実施形態の説明から、本開示はより良く理解され、本開示の他の目的、詳細、特徴および利点はより明らかになるのであろう。

【図１】本開示の実施形態によるブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するためのシステムの概略図を示す。

【図２】本開示の実施形態によるブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するためのアプリケーションサーバのブロック図を示す。

【図３】本開示の実施形態によるブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するための方法のフローチャートを示す。なお、本方法は、本開示の実施形態によるアプリケーションサーバにおいて実施される。

【図４】本開示の実施形態によるブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するための方法のフローチャートを示す。なお、本方法は、本開示の実施形態による使用者装置において実施される。

【図５】本開示の実施形態によるブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するための方法のフローチャートを示す。なお、本方法は、本開示の実施形態によるＩｏＴ装置において実施される。

【図６】本開示の実施形態を実施するための例示的な装置の概略ブロック図を示す。

【発明を実施するための形態】

【００１７】

ここで、本開示の実施形態を、添付の図面と併せてより詳細に説明する。本開示の実施形態は添付の図面に示されているが、本開示は、様々な方法で実施することができて本明細書に示された実施形態に限定されないことを理解されたい。その代わりとして、本明細書で提供される実施形態は、本開示をより完全にし、本開示の範囲を当業者に伝えるためのものである。

【００１８】

図１は、本開示の実施形態によるブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するためのシステム１００の概略図を示す。図１に示されるように、システム１００は、ブロックチェーンプラットフォーム１０、アプリケーションサーバ２０、１以上のＩｏＴ装置３０（図では１つだけが例示的に示されている）および少なくとも１の使用者装置４０（図では１つだけが例示的に示されている）を含む。本明細書では、ＩｏＴ装置３０にアクセスしてデータを取得する装置を使用者装置４０と呼ぶ。しかし、これは単に説明を明確にするためである。実際、使用者装置４０は、異なるＩｏＴ装置間の相互接続をＩｏＴ装置３０と共に実行する別のＩｏＴ装置であり得る。したがって、ＩｏＴ装置３０に関する本明細書における説明は、使用者装置４０にも適用され得る。複数のＩｏＴ装置３０は少なくとも１の装置提供者によって提供されるため、それらは異なる通信プロトコルおよび／またはデータ形式を使用する。アプリケーションサーバ２０は、システム１００における複数のＩｏＴ装置３０に統一装置識別子規格およびデータ形式を提供するために使用され、異なる提供者によって提供されるＩｏＴ装置３０間における相互接続を可能にする。

【００１９】

信頼性ＩｏＴサービスを実施するためには、ＩｏＴ装置の識別確立（図１に示されるプロセス１１０）、ＩｏＴ装置間における識別証明（図１に示されるプロセス１２０）およびＩｏＴ装置間における相互接続（図１に示されるプロセス１３０）などの対処すべき様々な問題がある。以下、図２～図５を参照して、アプリケーションサーバ２０、ＩｏＴ装置３０および使用者装置４０の構成および処理について説明する。

【００２０】

図２は、本開示の実施形態によるブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するためのアプリケーションサーバ２０のブロック図を示す。図２に示されるように、アプリケーションサーバ２０は、送受信機２２とプロセッサ２４とメモリ２６とを備える。いくつかの実施形態では、メモリ２６はコンピュータプログラムコードを格納し、コンピュータプログラムコードは、プロセッサ２４によって実行されると方法３００（図３と共に後述）を実行する。プロセッサ２４は、送受信機２２を介して有線方式または無線方式で複数のＩｏＴ装置３０_{1}～３０_{N}（本明細書ではまとめてＩｏＴ装置３０と呼ぶ）と相互作用するように構成される。さらに、プロセッサ２４はまた、送受信機２２を介して有線方式または無線方式で少なくとも１の使用者装置４０_{1}～４０_{M}（本明細書ではまとめて使用者装置４０と呼ぶ）と相互作用するように構成される。図１に関連して上述したように、使用者装置４０は、従来型使用者端末または別のＩｏＴ装置であり得る。

【００２１】

アプリケーションサーバ２０は、有線または無線ネットワーク６０を介して（例えば、図示しないブロックチェーンアプリケーションインタフェースを介して）、ブロックチェーンプラットフォーム１０の各ブロックチェーンノード１２と通信し得る。

【００２２】

さらに、アプリケーションサーバ２０は、分散データベース５０に結合され得る。分散データベース５０は、アプリケーションサーバ２０の一部であり得るか、アプリケーションサーバ２０から独立して複数のネットワークノード間で分散され得る。

【００２３】

図３は、本開示の実施形態によるブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するための方法３００のフローチャートを示す。方法３００は、本開示の実施形態によるアプリケーションサーバにおいて実施される。アプリケーションサーバは、例えば、

図２に示されるアプリケーションサーバ２０であり得る。

【００２４】

ブロック３０２において、アプリケーションサーバ２０は、複数のＩｏＴ装置３０に対する統一装置識別子規格を決定する。ここで、統一装置識別子規格は、アプリケーションサーバ２０の管理者によって定義され得るか、信頼性ＩｏＴ同盟などの上位組織によって定義され得る。

【００２５】

ブロック３０４において、アプリケーションサーバ２０は、複数のＩｏＴ装置３０それぞれに対して固有識別子を決定する。固有識別子は、統一装置識別子規格に準拠しなければならない。固有識別子は、ＩｏＴ装置３０の秘密鍵と対をなすＩｏＴ装置３０の公開鍵である。

【００２６】

固有識別子を生成する主体に応じて、ブロック３０４の多種多様な実施形態が存在し得る。

【００２７】

いくつかの実施形態では、アプリケーションサーバ２０は、複数のＩｏＴ装置３０それぞれの公開鍵と秘密鍵との対を生成する。公開鍵は、統一装置識別子規格に準拠する。アプリケーションサーバ２０は、公開鍵と秘密鍵とをＩｏＴ装置３０に送信して読み取り不可能な方法でＩｏＴ装置３０に秘密鍵を格納し、ＩｏＴ装置３０の固有識別子として公開鍵を使用する。これらの実施形態では、ＩｏＴ装置３０の秘密鍵がＩｏＴ装置３０自身の中にのみ存在することを保証するために、アプリケーションサーバ２０は、生成した秘密鍵をＩｏＴ装置３０に送信した後に、生成した秘密鍵を破棄しなければならない。

【００２８】

いくつかの他の実施形態では、固有識別子は各ＩｏＴ装置３０自身によって生成される。この場合、アプリケーションサーバ２０は、統一装置識別子規格の複数のＩｏＴ装置３０に信号を送り、複数のＩｏＴ装置３０それぞれから固有識別子を受信する。固有識別子は、この統一装置識別子規格に準拠する。本開示の実施形態によれば、ＩｏＴ装置３０は、統一装置識別子規格に従って公開鍵と秘密鍵との対を生成し、ＩｏＴ装置３０の固有識別子として公開鍵をアプリケーションサーバ２０に送信し、ＩｏＴ装置３０内（例えば、図４に関連して以下に示されるＩｏＴ装置３０の不可読メモリ３６内）に秘密鍵を格納する。

【００２９】

さらに他の実施形態では、固有識別子はまた、ＩｏＴ装置３０が納品される前後に、ＩｏＴ装置３０の提供者によって生成され得る。この場合、アプリケーションサーバ２０は、ＩｏＴ装置３０の少なくとも１の提供者に統一装置識別子規格を通知し、複数のＩｏＴ装置３０の対応するＩｏＴ装置の提供者によって生成される固有識別子を、少なくとも１の提供者から受信する。固有識別子は、統一装置識別子規格に準拠している。本開示の実施形態によれば、ＩｏＴ装置３０の提供者は、ＩｏＴ装置３０の公開鍵と秘密鍵との対を生成し、ＩｏＴ装置３０の固有識別子として公開鍵をアプリケーションサーバ２０に送信すると共に、秘密鍵を、ＩｏＴ装置３０に送信して不可読な方法でＩｏＴ装置３０内（例えば、図４に関連して以下に示されるＩｏＴ装置３０の不可読メモリ３６内に）に格納する。

【００３０】

方法３００に戻ると、各ＩｏＴ装置３０の固有識別子が決定された後、アプリケーションサーバ２０は、ブロック３０６において、固有識別子をブロックチェーンプラットフォーム１０に登録する。

【００３１】

上述の方法３００のブロック３０２～３０６を通じて、多種多様な提供者によって提供されるＩｏＴ装置３０の装置識別子は統一されているため、各ＩｏＴ装置３０は、複数のＩｏＴ装置提供者にかけて、システム１００内で統一かつ一意に識別され得る。

【００３２】
いくつかのアプリケーションの概要では、ＩｏＴ装置３０の固有識別子を介してのみＩｏＴ装置３０を特定することは依然として困難である。これに対処するために、方法３００は、ブロック３０８とブロック３１０とをさらに含み得る。ブロック３０８では、アプリケーションサーバ２０が、ＩｏＴ装置３０の索引情報をＩｏＴ装置３０からさらに受信し得る。ブロック３１０では、アプリケーションサーバ２０が、索引情報をブロックチェーンプラットフォーム１０に登録する。ＩｏＴ装置３０の索引情報は、ＩｏＴ装置３０の固有識別子と組み合わせて使用され、ＩｏＴ装置３０の所在を特定する。例えば、ＩｏＴ装置３０の索引情報は、ＩｏＴ装置３０の所在を含み得る。この場合、索引情報は、対応するＩｏＴ装置３０を探すための使用者用案内情報とみなされ得る。
【００３３】
ここで、ＩｏＴ装置３０の索引情報は、アプリケーションサーバ２０からの明示的な合図によって要求され得るか、アプリケーションサーバ２０によって統一装置識別子規格と共にＩｏＴ装置３０に送信され得るか、システム１００によって予め定義され得る。
【００３４】
さらに、異なる提供者からのＩｏＴ装置３０間の相互接続を達成するために、統一データ形式またはプロトコルもまた、各ＩｏＴ装置３０の通信用に提供されるべきである。この目的のために、方法３００はブロック３１２をさらに含み得る。ブロック３１２では、アプリケーションサーバ２０は、複数のＩｏＴ装置３０に統一装置データ規格を提供する。ここで、統一装置データ規格は、アプリケーションサーバ２０の管理者によって定義され得るか、信頼性ＩｏＴ同盟等の上位組織によって定義され得る。
【００３５】
ブロック３１４において、アプリケーションサーバ２０は、ＩｏＴ装置３０から生データを受信する。生データは、ＩｏＴ装置３０の提供者に特有の形式である。ブロック３１６において、アプリケーションサーバ２０は、生データを、統一装置データ規格に準拠する装置データに変換する。ブロック３１８において、アプリケーションサーバ２０は、ブロックチェーンプラットフォーム１０に装置データを格納する。
【００３６】
アプリケーションの概要に応じて、ブロック３１４～３１８は、異なる実施形態を有し得る。
【００３７】
いくつかの実施形態では、生データは生履歴データを含み、装置データは装置履歴データを含む。この場合、ブロック３１４において、アプリケーションサーバ２０は、例えば、ＩｏＴ装置３０から生履歴データを定期的に受信し、生履歴データを装置履歴データに変換し（ブロック３１６）、ブロックチェーンプラットフォーム１０に装置履歴データを格納する（ブロック３１８）。
【００３８】
この場合、使用者装置４０がＩｏＴ装置３０の装置履歴データをアプリケーションサーバ２０に要求すると、アプリケーションサーバ２０は、例えば、図４～図５を参照して後述するように、使用者装置４０を認証した後に、要求された装置履歴データをブロックチェーンプラットフォーム１０から取得する。そして、アプリケーションサーバ２０は、装置履歴データを使用者装置４０に直接送信する（図示せず）。
【００３９】
他のいくつかの実施形態では、生データは生実時間データを含み、装置データは装置実時間データを含む。この場合、例えば、使用者装置４０からの、ＩｏＴ装置３０の実時間データの要求に応じて、アプリケーションサーバ２０は、ＩｏＴ装置３０の生実時間データをＩｏＴ装置３０に要求する。次に、ブロック３１４において、アプリケーションサーバ２０は、ＩｏＴ装置３０から生実時間データを受信し、生実時間データを装置実時間データに変換し（ブロック３１６）、ブロックチェーンプラットフォーム１０に装置実時間データを格納する（ブロック３１８）。

【００４０】
この場合、アプリケーションサーバ２０は、生実時間データを装置実時間データに変換した後、使用者装置４０に装置実時間データを直接送信する（ブロック３１６）。
【００４１】
アプリケーションサーバ２０によって変換された装置データをブロックチェーンプラットフォーム１０に直接格納する場合、比較的大きな記憶領域が占有されることになる。このため、一実施形態では、ブロック３１８において、アプリケーションサーバ２０は、装置データのハッシュ値と装置データ自体とを分散型データベース（図２に示されるデータベース５０など）に送信して記憶させ、装置データのハッシュ値とＩｏＴ装置３０の固有識別子とをブロックチェーンプラットフォーム１０に送信して記憶させ得る。このようにして、安全に保管すると共に、保管費用を低減することができる。
【００４２】
方法３００の上記ブロック３１２～３１８を経ることで、多種多様な提供者によって提供されるＩｏＴ装置３０のデータ形式またはプロトコルが統一されるため、多様な提供者によって提供されるＩｏＴ装置３０は互いにデータを交換することができる。
【００４３】
方法３００の上記の説明では、生データから装置データへの変換が、ブロック３１６においてアプリケーションサーバ２０によって集中的に実行されるものとして説明されている。しかし、本開示がこれに限定されず、各ＩｏＴ装置３０の生データが各提供者によって変換されてアプリケーションサーバ２０に送信されてブロックチェーンプラットフォーム１０に記憶されることも可能であることを当業者は理解し得る。この場合、アプリケーションサーバ２０は、各ＩｏＴ装置３０の提供者に統一装置データ規格を通知しなければならない。
【００４４】
図４は、方法４００のフローチャートを示し、方法４００は、本開示の実施形態によるブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するためのものであり、本開示の実施形態による使用者装置において実施される。使用者装置は、例えば、図１に示されるような使用者装置４０であり得る。使用者装置４０がＩｏＴ装置３０にアクセスしたい場合、図４に示される方法４００が開始される。ＩｏＴ装置３０はＩｏＴ装置公開鍵(P_{IoT})とＩｏＴ装置秘密鍵(K_{IoT})との対で構成され、使用者装置４０は使用者公開鍵(P_u)と使用者秘密鍵(K_u)との対で構成されると仮定される。
【００４５】
ブロック４０２で、使用者装置４０は、使用者データに対してハッシュ演算を実行して使用者データのハッシュ値Ｈを生成する。ここで、使用者データは、使用者装置４０がＩｏＴ装置３０から取得しようとするアクセス内容の種類を含み得る。
【００４６】
ブロック４０４において、使用者装置４０は、アクセス予定のＩｏＴ装置３０のＩｏＴ装置公開鍵P_{IoT}と、使用者乱数R_uとに基づいて第１の暗号化情報を取得する。例えば、使用者装置４０は、ＩｏＴ装置公開鍵P_{IoT}を使用して使用者乱数R_uを暗号化し、第１の暗号化情報$P_{IoT}(R_u)$を生成し得る。
【００４７】
次に、ブロック４０６において、使用者装置４０は、使用者秘密鍵K_uと使用者乱数R_uと使用者データのハッシュ値Ｈとに基づいて、第２の暗号化情報を取得する。例えば、使用者装置４０は、使用者秘密鍵K_uを使用してハッシュ値Ｈを暗号化し、使用者装置４０の使用者署名$K_u(H)$を生成し得るとともに、使用者乱数R_uを使用して使用者署名$K_u(H)$を暗号化し、第２の暗号化情報$R_u(K_u(H))$を生成し得る。
【００４８】
ブロック４０８において、使用者装置４０は、認証要求をＩｏＴ装置３０に送信する。認証要求は、ブロック４０２で生成された使用者データのハッシュ値Ｈと、ブロック４０４で生成された第１の暗号化情報と、ブロック４０６で生成された第２の暗号化情報とを

含む。

【００４９】

方法４００により、識別認証処理時に、使用者装置４０は使用者データに対して複数の暗号化を実行し得る。使用者装置４０からＩｏＴ装置３０に送信されるアクセス要求は、平文情報を含んでいない。このため、安全性を向上させることができる。

【００５０】

図５は方法５００のフローチャートを示す。方法５００は、本開示の実施形態によるブロックチェーンに基づいて信頼性ＩｏＴサービスを実施するためのものであり、本開示の実施形態によるＩｏＴ装置において実施される。ＩｏＴ装置は、例えば、図１に示されるようなＩｏＴ装置３０であり得る。

【００５１】

ブロック５０２において、ＩｏＴ装置３０は、使用者装置４０から認証要求を受信する。認証要求は、上記のように、使用者データのハッシュ値Hと、第１の暗号化情報と、第２の暗号化情報とを含む。

【００５２】

ブロック５０４において、ＩｏＴ装置３０は、ＩｏＴ装置秘密鍵K_{IoT}と認証要求とに基づいて使用者装置４０を認証し、使用者公開鍵P_uを取得する。

【００５３】

いくつかの実施形態では、ＩｏＴ装置３０は、ＩｏＴ装置秘密鍵K_{IoT}および第１の暗号化情報に基づいて使用者乱数R_uを計算し、次に、使用者乱数R_uおよび第２の暗号化情報に基づいて使用者装置４０の使用者署名$K_u(H)$を計算する。ここで、使用者秘密鍵K_uを使用してハッシュ値Hを暗号化することによって、使用者署名$K_u(H)$が取得される。次に、ＩｏＴ装置３０は、楕円曲線暗号を使用して使用者署名$K_u(H)$およびハッシュ値Hに基づいて使用者公開鍵P_uを決定する。

【００５４】

例えば、使用者乱数R_uは、以下の式（１）に従って計算され得る。

【００５５】

$$R_u = K^{-1}_{IoT}(P_{IoT}(R_u)) \quad \cdots (1)$$

【００５６】

ここで、$P_{IoT}(R_u)$は、第１の暗号化情報を表し、K^{-1}_{IoT}は、ＩｏＴ装置秘密鍵K_{IoT}を使用する復号化演算を表す。

【００５７】

例えば、使用者署名は、以下の式（２）に従って計算され得る。

【００５８】

$$K_u(H) = R^{-1}_u(R_u(K_u(H))) \quad \cdots (2)$$

【００５９】

ここで、$K_u(H)$は使用者署名を表し、Hは使用者データのハッシュ値を表し、$R_u(K_u(H))$は第２の暗号化情報を表し、R^{-1}_uは使用者乱数R_uを使用する復号化演算を表す。

【００６０】

ブロック５０４で使用者公開鍵P_uを取得した後、ＩｏＴ装置３０は、ＩｏＴ装置３０のアクセス許可使用者装置一覧に使用者公開鍵P_uがあるかどうかを、ブロック５０６で判定する。ここでは、ＩｏＴ装置３０と同様に、使用者装置４０の公開鍵P_uが、使用者装置の固有識別子として用いられる。

【００６１】

ブロック５０６は、ＩｏＴ装置３０のアクセス許可使用者装置一覧の作成者に応じて、異なる方法で実施され得る。

【００６２】

いくつかの実施形態では、一覧はＩｏＴ装置３０の提供者によって作成される。例えば、一覧は、提供者によって許可されたＩｏＴ装置の一覧を記録する。この場合、ブロック５０６において、ＩｏＴ装置３０は、ブロック５０４で取得される使用者公開鍵P_uをその

提供者に送信し得る。提供者は、提供者によって保存されたアクセス許可使用者装置一覧内の使用者公開鍵P_uを検索し、検索結果をＩｏＴ装置３０に返す。

【００６３】

いくつかの他の実施形態では、一覧はＩｏＴ装置３０の所有者によって作成される。例えば、一覧は、所有者によって許可されたＩｏＴ装置の一覧（特定一覧とも呼ばれ得る）を記録する。この場合、ブロック５０６において、ＩｏＴ装置３０は、ＩｏＴ装置３０によって保存されたアクセス許可使用者装置一覧に使用者装置４０の使用者公開鍵P_uが存在するかどうかを直接判定し得る。

【００６４】

ＩｏＴ装置３０のアクセス許可使用者装置一覧に使用者公開鍵P_uが存在するというブロック５０６における判定に応じて、ブロック５０８において使用者装置４０の認証が成功する。一方、方法５００はブロック５１０をさらに含み得る。使用者公開鍵P_uがＩｏＴ装置３０のアクセス許可使用者装置一覧に存在しないというブロック５０６における判定に応じて、ブロック５１０において使用者装置４０の認証が失敗する。

【００６５】

方法５００により、ＩｏＴ装置と使用者装置との間、または、異なるＩｏＴ装置間で識別認証を達成することが可能である。また、認証処理時に、ＩｏＴ装置３０が使用者装置４０から受信したアクセス要求は、平文情報を含んでいない。このため、安全性を向上させることができる。

【００６６】

当業者は、方法４００および５００を別々に、または、方法４００および５００を図３に関連して説明した方法３００と組み合わせて実行可能であることを理解することができる。

【００６７】

図６は、本開示の実施形態を実施するための例示的な装置６００の概略ブロック図を示す。図示されるように、装置６００は中央処理装置（ＣＰＵ）６１０を含む。ＣＰＵ６１０は、コンピュータプログラム命令に従って、適切な機能または処理を実行し得る。コンピュータプログラム命令は、読み出し専用メモリ（ＲＯＭ）６２０に記憶されるか、記憶装置６８０からランダムアクセスメモリ（ＲＡＭ）６３０に読み込まれる。ＲＡＭ ６３０では、装置６００の処理に必要な各種プログラムやデータもまた格納され得る。ＣＰＵ６１０、ＲＯＭ ６２０およびＲＡＭ ６３０は、バス６４０を介して互いに接続されている。入出力（Ｉ／Ｏ）インタフェース６５０もまた、バス６４０に接続されている。

【００６８】

装置６００内の複数の構成要素は、Ｉ／Ｏインタフェース６５０に接続されており、キーボードやマウス等の入力装置６６０と、各種表示装置やスピーカー等の出力装置６７０と、磁気ディスクや光ディスク等の記憶装置６８０と、ネットワークカードやモデムや無線通信送受信機等の通信装置６９０とを含む。通信装置６９０は、装置６００がインターネットおよび／または様々な電気通信ネットワークのようなコンピュータネットワークを介して他の装置と情報／データを交換することを可能にする。

【００６９】

方法３００、４００および５００などの上述の様々な処理および工程は、処理装置６１０によって実行され得る。例えば、いくつかの実施形態では、方法３００、４００および５００は、記憶装置６８０などの機械可読媒体に実体的に具体化されたコンピュータソフトウェアプログラムとして実施され得る。いくつかの実施形態において、コンピュータプログラムの一部または全部は、ＲＯＭ６２０および／または通信装置６９０を介して、装置６００に読込まれ得る（および／またはインストールされ得る。）。コンピュータプログラムがＲＡＭ６３０に読み込まれてＣＰＵ６１０によって実行されると、上述した方法３００、４００および５００の少なくとも１方法が実行され得る。

【００７０】

装置６００は、図１～５に関連して本明細書で説明されるように、アプリケーションサ

ーバ２０、ＩｏＴ装置３０および使用者装置４０のいずれかとして実装され得る。特に、装置６００がＩｏＴ装置３０として実装される場合、不可読メモリ（図示せず）がさらに含まれるべきである。ＩｏＴ装置３０は公開鍵と秘密鍵との対で構成され得て、公開鍵は可読メモリ（ＲＯＭ６２０など）に格納され、秘密鍵は不可読メモリに格納される。このように、ＩｏＴ装置３０自体のみが秘密鍵を使用することができることが保証され、他の主体は可読メモリからＩｏＴ装置３０の公開鍵のみを取得することができる。このため、使用者装置４０または他のＩｏＴ装置３０は、公開鍵を利用してＩｏＴ装置３０の同一性を認証することができる。

【００７１】

１つまたは複数の例示的な設計では、本開示の実施形態によって説明される機能は、ハードウェア、ソフトウェア、ファームウェアまたはそれらの任意の組合せで実施され得る。ソフトウェアで実施される場合、コンピュータ可読媒体上の１つまたは複数の命令またはコードとして、機能が記憶され得るか送信され得る。

【００７２】

本明細書で説明される装置の個々のユニットは、個別のハードウェア構成要素を用いて実装され得るか、プロセッサなどの単一のハードウェア構成要素に一体的に実装され得る。例えば、本開示に関連して説明された様々な例示的な論理ブロック、モジュールおよび回路は、汎用プロセッサ、デジタル信号プロセッサ（ＤＳＰ）、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）または他のプログラマブル論理装置、ディスクリートゲートまたはトランジスタロジック、ディスクリートハードウェア構成要素、あるいは、本明細書で説明された機能を実行するために設計されたそれらの任意の組合せで実装され得るか実行され得る。

【００７３】

当業者は、本明細書における本開示の実施形態に関連して説明された様々な例示的な論理ブロック、モジュール、プロセッサ、手段、回路およびアルゴリズムステップのいずれかが電子ハードウェア、コンピュータソフトウェアまたはそれらの組合せとして実装され得ることをさらに理解するであろう。

【００７４】

本開示の実施形態の前述の説明が提供されることで、あらゆる当業者が本開示を実現または使用することが可能になる。本開示の実施形態に対する様々な修正は、当業者には自明であり、本明細書で定義される一般的な原理は、本開示の精神および範囲から逸脱しなければ他の局面に適用され得る。したがって、本開示は、本明細書で示される例および設計に限定されることを意図するものではなく、本明細書で開示される原理および新規な特徴と一致する最も広い範囲を与えられるべきである。

【００７５】

本開示の実施形態は、以下の番号付けされた項で表される一連の実施形態を含むが、これらに限定されない。

【００７６】

１．

ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施するためのアプリケーションサーバであって、

メモリとプロセッサとを備え、

前記メモリは、機械実行可能命令を格納し、

前記機械実行可能命令は、前記プロセッサによって実行されると、前記アプリケーションサーバに処理を実行させ、

前記処理は、

少なくとも１の提供者によって提供される複数のＩｏＴ装置の統一装置識別子規格を決定することと、

前記複数のＩｏＴ装置の各ＩｏＴ装置の固有識別子を決定することと、

ブロックチェーンプラットフォームに前記ＩｏＴ装置の前記固有識別子を登録すること

とを含み、
前記固有識別子は、前記統一装置識別子規格に準拠し、前記ＩｏＴ装置の秘密鍵と対をなす前記ＩｏＴ装置の公開鍵である、
アプリケーションサーバ。
【００７７】
２．
前記複数のＩｏＴ装置の各ＩｏＴ装置の固有識別子を決定することは、
前記統一装置識別子規格を前記複数のＩｏＴ装置に送信することと、
前記複数のＩｏＴ装置の各ＩｏＴ装置から前記固有識別子を受信することとを備え、
前記固有識別子は、前記ＩｏＴ装置によって生成され、前記統一装置識別子規格に準拠し、
前記ＩｏＴ装置の前記秘密鍵は、前記ＩｏＴ装置によって生成され、不可読な方法で前記ＩｏＴ装置内に単に格納される、
項１に記載のアプリケーションサーバ。
【００７８】
３．
前記複数のＩｏＴ装置の各ＩｏＴ装置の固有識別子を決定することは、
前記統一装置識別子規格を前記少なくとも１の提供者に送信することと、
前記少なくとも１の提供者から前記固有識別子を受信することとを備え、
前記固有識別子は、前記複数のＩｏＴ装置の対応するＩｏＴ装置の前記提供者によって生成され、前記統一装置識別子規格に準拠し、
前記ＩｏＴ装置の前記秘密鍵は、前記提供者によって生成され、不可読な方法で前記ＩｏＴ装置内に単に格納される、
項１に記載のアプリケーションサーバ。
【００７９】
４．
前記複数のＩｏＴ装置の各ＩｏＴ装置の固有識別子を決定することは、
前記複数のＩｏＴ装置の各ＩｏＴ装置の前記公開鍵と前記秘密鍵とを生成することと、
前記公開鍵と前記秘密鍵とを前記ＩｏＴ装置に送信して不可読な方法で前記ＩｏＴ装置内に前記秘密鍵を格納し、前記公開鍵を前記ＩｏＴ装置の前記固有識別子とすることと、
生成した前記ＩｏＴ装置の前記公開鍵を破棄することとを備え、
前記公開鍵は、前記統一装置識別子規格に準拠する、
項１に記載のアプリケーションサーバ。
【００８０】
５．
前記処理は、
前記複数のＩｏＴ装置の各ＩｏＴ装置から、前記ＩｏＴ装置の索引情報を受信することと、
前記ＩｏＴ装置の前記索引情報を前記ブロックチェーンプラットフォームに登録することとをさらに含む、
項１に記載のアプリケーションサーバ。
【００８１】
６．
前記索引情報は、前記ＩｏＴ装置の所在を含む、
項５に記載のアプリケーションサーバ。
【００８２】
７．
前記処理は、
前記複数のＩｏＴ装置の統一装置データ規格を決定することと、
前記複数のＩｏＴ装置の各ＩｏＴ装置から生データを受信することと、

前記生データを装置データに変換することと、
前記装置データを前記ブロックチェーンプラットフォームに格納することとをさらに含み、
前記生データは、前記ＩｏＴ装置の提供者に特有の形式であり、
前記装置データは、前記統一装置データ規格に準拠する、
項１に記載のアプリケーションサーバ。
【００８３】
８．
前記生データは、生履歴データを含み、
前記装置データは、装置履歴データを含み、
前記処理は、
使用者装置からの、前記ＩｏＴ装置の前記装置履歴データの要求に応答し、前記ブロックチェーンプラットフォームから前記装置履歴データを取得することと、
前記装置履歴データを前記使用者装置に送信することとをさらに含む、
項７に記載のアプリケーションサーバ。
【００８４】
９．
前記生データは、生実時間データを含み、
前記装置データは、装置実時間データを含み、
前記処理は、
前記ＩｏＴ装置から前記生データを受信する前に、使用者装置から前記ＩｏＴ装置の前記実時間データの要求を受信することと、
前記ＩｏＴ装置の前記生実時間データを前記ＩｏＴ装置に要求することと、
前記生実時間データを、前記統一装置データ規格に準拠する前記装置実時間データに変換した後、前記装置実時間データを前記使用者装置に送信することとをさらに含む、
項７に記載のアプリケーションサーバ。
【００８５】
１０．
ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施するための方法であって、
少なくとも１の提供者によって提供される複数のＩｏＴ装置の統一装置識別子規格を決定することと、
前記複数のＩｏＴ装置の各ＩｏＴ装置の固有識別子を決定することと、
ブロックチェーンプラットフォームに前記ＩｏＴ装置の前記固有識別子を登録することとを含み、
前記固有識別子は、前記統一装置識別子規格に準拠し、前記ＩｏＴ装置の秘密鍵と対をなす前記ＩｏＴ装置の公開鍵である、
方法。
【００８６】
１１．
前記複数のＩｏＴ装置の各ＩｏＴ装置の固有識別子を決定することは、
前記統一装置識別子規格を前記複数のＩｏＴ装置に送信することと、
前記複数のＩｏＴ装置の各ＩｏＴ装置から前記固有識別子を受信することとを備え、
前記固有識別子は、前記ＩｏＴ装置によって生成され、前記統一装置識別子規格に準拠し、
前記ＩｏＴ装置の前記秘密鍵は、前記ＩｏＴ装置によって生成され、不可読な方法で前記ＩｏＴ装置内に単に格納される、
項１０に記載の方法。
【００８７】
１２．

前記複数のＩｏＴ装置の各ＩｏＴ装置の固有識別子を決定することは、
前記統一装置識別子規格を前記少なくとも１の提供者に送信することと、
前記少なくとも１の提供者から前記固有識別子を受信することとを備え、
前記固有識別子は、前記複数のＩｏＴ装置の対応するＩｏＴ装置の前記提供者によって生成され、前記統一装置識別子規格に準拠し、
前記ＩｏＴ装置の前記秘密鍵は、前記提供者によって生成され、不可読な方法で前記ＩｏＴ装置内に単に格納される、
項１０に記載の方法。
【００８８】
１３．
前記複数のＩｏＴ装置の各ＩｏＴ装置の固有識別子を決定することは、
前記複数のＩｏＴ装置の各ＩｏＴ装置の前記公開鍵と前記秘密鍵とを生成することと、
前記公開鍵と前記秘密鍵とを前記ＩｏＴ装置に送信し、不可読な方法で前記ＩｏＴ装置内に前記秘密鍵を格納し、前記公開鍵を前記ＩｏＴ装置の前記固有識別子として使用することと、
生成した前記ＩｏＴ装置の前記公開鍵を破棄することとを備え、
前記公開鍵は、前記統一装置識別子規格に準拠する、
項１０に記載の方法。
【００８９】
１４．
前記複数のＩｏＴ装置の各ＩｏＴ装置から、前記ＩｏＴ装置の索引情報を受信することと、
前記ＩｏＴ装置の前記索引情報を前記ブロックチェーンプラットフォームに登録することとをさらに備える、
項１０に記載の方法。
【００９０】
１５．
前記索引情報は、前記ＩｏＴ装置の所在を含む、
項１４に記載の方法。
【００９１】
１６．
前記複数のＩｏＴ装置の統一装置データ規格を決定することと、
前記複数のＩｏＴ装置の各ＩｏＴ装置から生データを受信することと、
前記生データを装置データに変換することと、
前記装置データを前記ブロックチェーンプラットフォームに格納することとをさらに備え、
前記生データは、前記ＩｏＴ装置の提供者に特有の形式であり、
前記装置データは、前記統一装置データ規格に準拠する、
項１０に記載の方法。
【００９２】
１７．
前記生データは、生履歴データを含み、
前記装置データは、装置履歴データを含み、
使用者装置からの、前記ＩｏＴ装置の前記装置履歴データの要求に応答し、前記ブロックチェーンプラットフォームから前記装置履歴データを取得することと、
前記装置履歴データを前記使用者装置に送信することとをさらに備える、
項１６に記載の方法。
【００９３】
１８．
前記生データは、生実時間データを含み、

前記装置データは、装置実時間データを含み、
前記ＩｏＴ装置から前記生データを受信する前に、使用者装置から前記ＩｏＴ装置の前記実時間データの要求を受信することと、
前記ＩｏＴ装置の前記生実時間データを前記ＩｏＴ装置に要求することと、
前記生実時間データを、前記統一装置データ規格に準拠する前記装置実時間データに変換した後、前記装置実時間データを前記使用者装置に送信することとをさらに備える、
項１６に記載の方法。
【００９４】
１９．
ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施するための不揮発性コンピュータ可読記憶媒体であって、
機械実行可能命令を備え、
前記機械実行可能命令は、機械によって実行されると、項１０から１８のいずれか１項に記載の方法を前記機械に実施させるように適合される、
不揮発性コンピュータ可読記憶媒体。
【００９５】
２０．
ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施するためのＩｏＴ装置であって、
ＩｏＴ装置公開鍵(P_{IoT})とＩｏＴ装置秘密鍵(K_{IoT})との対で構成され、
メモリとプロセッサとを備え、
前記メモリは、機械実行可能命令を格納し、
前記機械実行可能命令は、前記プロセッサによって実行されると、前記ＩｏＴ装置に処理を実行させ、
前記処理は、
使用者装置から認証要求を受信することと、
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記認証要求とに基づいて前記使用者装置を認証して使用者公開鍵(P_u)を取得することと、
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することと、
前記ＩｏＴ装置の前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するという判定に応じて、前記使用者装置の認証が成功すると判定することとを含み、
前記使用者装置は、前記使用者公開鍵(P_u)と使用者秘密鍵(K_u)との対で構成され、
前記認証要求は、前記使用者装置の使用者データのハッシュ値と、前記ＩｏＴ装置公開鍵(P_{IoT})と使用者乱数(R_u)とに基づいて取得される第１の暗号化情報と、前記使用者秘密鍵(K_u)と前記使用者乱数(R_u)と前記ハッシュ値とに基づいて取得される第２の暗号化情報とを含む、
ＩｏＴ装置。
【００９６】
２１．
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記認証要求とに基づいて前記使用者装置を認証して使用者公開鍵(P_u)を取得することは、
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記第１の暗号化情報とに基づいて前記使用者乱数(R_u)を計算することと、
前記使用者乱数(R_u)と前記第２の暗号化情報とに基づいて前記使用者装置の使用者署名を計算することと、
楕円曲線暗号を使用して前記使用者署名と前記ハッシュ値に基づいて前記使用者公開鍵(P_u)を決定することとをさらに備え、
前記使用者署名は、前記使用者秘密鍵(K_u)を使用して前記ハッシュ値を暗号化することによって取得される、

項２０に記載のＩｏＴ装置。
【００９７】
２２．
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記第１の暗号化情報とに基づいて前記使用者乱数(R_u)を計算することは、
「$R_u = K^{-1}_{IoT}(P_{IoT}(R_u))$」式に従って前記使用者乱数($R_u$)を計算することを備え、
$P_{IoT}(R_u)$は、前記第１の暗号化情報を表し、
K^{-1}_{IoT}は、前記ＩｏＴ装置秘密鍵(K_{IoT})を使用する復号化演算を表し、
前記使用者乱数(R_u)と前記第２の暗号化情報とに基づいて前記使用者装置の使用者署名を計算することは、
「$K_u(H) = R^{-1}_u(R_u(K_u(H)))$」式に従って前記使用者署名を計算することを備え、
$K_u(H)$は、前記使用者署名を表し、
Ｈは、前記使用者データの前記ハッシュ値を表し、
$R_u(K_u(H))$は、前記第２の暗号化情報を表し、
R^{-1}_uは、前記使用者乱数(R_u)を使用する復号化演算を表す、
項２１に記載のＩｏＴ装置。
【００９８】
２３．
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することは、
前記使用者公開鍵(P_u)を前記ＩｏＴ装置の提供者に送信することを備え、
前記提供者は、前記提供者に属する各ＩｏＴ装置のアクセス許可使用者装置一覧を保存し、
前記ＩｏＴ装置の前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうかを示す検索結果を、前記提供者から受信することを備える、
項２２に記載のＩｏＴ装置。
【００９９】
２４．
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することは、
前記ＩｏＴ装置によって保存された前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することを備える、
項２２に記載のＩｏＴ装置。
【０１００】
２５．
ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施するための方法であって、
ＩｏＴ装置公開鍵(P_{IoT})とＩｏＴ装置秘密鍵(K_{IoT})との対で構成されるＩｏＴ装置によって実行され、
使用者装置から認証要求を受信することと、
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記認証要求とに基づいて前記使用者装置を認証して使用者公開鍵(P_u)を取得することと、
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することと、
前記ＩｏＴ装置の前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するという判定に応じて、前記使用者装置の認証が成功すると判定することとを備え、
前記使用者装置は、前記使用者公開鍵(P_u)と使用者秘密鍵(K_u)との対で構成され、
前記認証要求は、前記使用者装置の使用者データのハッシュ値と、前記ＩｏＴ装置公開鍵(P_{IoT})と使用者乱数(R_u)とに基づいて取得される第１の暗号化情報と、前記使用者秘密鍵(K_u)と前記使用者乱数(R_u)と前記ハッシュ値とに基づいて取得される第２の暗号化情報

とを含む、
方法。
【０１０１】
２６．
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記認証要求とに基づいて前記使用者装置を認証して使用者公開鍵(P_u)を取得することは、
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記第１の暗号化情報とに基づいて前記使用者乱数(R_u)を計算することと、
前記使用者乱数(R_u)と前記第２の暗号化情報とに基づいて前記使用者装置の使用者署名を計算することと、
楕円曲線暗号を使用して前記使用者署名と前記ハッシュ値に基づいて前記使用者公開鍵(P_u)を決定することとをさらに備え、
前記使用者署名は、前記使用者秘密鍵(K_u)を使用して前記ハッシュ値を暗号化することによって取得される、
項２５に記載の方法。
【０１０２】
２７．
前記ＩｏＴ装置秘密鍵(K_{IoT})と前記第１の暗号化情報とに基づいて前記使用者乱数(R_u)を計算することは、
「$R_u = K^{-1}_{IoT}(P_{IoT}(R_u))$」式に従って前記使用者乱数($R_u$)を計算することを備え、
$P_{IoT}(R_u)$は、前記第１の暗号化情報を表し、
K^{-1}_{IoT}は、前記ＩｏＴ装置秘密鍵(K_{IoT})を使用する復号化演算を表し、
前記使用者乱数(R_u)と前記第２の暗号化情報とに基づいて前記使用者装置の使用者署名を計算することは、
「$K_u(H) = R^{-1}_u(R_u(K_u(H)))$」式に従って前記使用者署名を計算することを備え、
$K_u(H)$は、前記使用者署名を表し、
Hは、前記使用者データの前記ハッシュ値を表し、
$R_u(K_u(H))$は、前記第２の暗号化情報を表し、
R^{-1}_uは、前記使用者乱数(R_u)を使用する復号化演算を表す、
項２６に記載の方法。
【０１０３】
２８．
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することは、
前記使用者公開鍵(P_u)を前記ＩｏＴ装置の提供者に送信することを備え、
前記提供者は、前記提供者に属する各ＩｏＴ装置のアクセス許可使用者装置一覧を保存し、
前記ＩｏＴ装置の前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうかを示す検索結果を、前記提供者から受信することを備える、
項２７に記載の方法。
【０１０４】
２９．
前記ＩｏＴ装置のアクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することは、
前記ＩｏＴ装置によって保存された前記アクセス許可使用者装置一覧に前記使用者公開鍵(P_u)が存在するかどうか判定することを備える、
項２７に記載の方法。
【０１０５】
３０．
ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施する

ための不揮発性コンピュータ可読記憶媒体であって、
機械実行可能命令を備え、
前記機械実行可能命令は、機械によって実行されると、項２５から２９のいずれか１項に記載の方法を前記機械に実施させるように適合される、
不揮発性コンピュータ可読記憶媒体。
【０１０６】
３１．
ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施するための使用者装置であって、
使用者公開鍵(P_u)と使用者秘密鍵(K_u)との対で構成され、
メモリとプロセッサとを備え、
前記メモリは、機械実行可能命令を格納し、
前記機械実行可能命令は、前記プロセッサによって実行されると、前記使用者装置に処理を実行させ、
前記処理は、
前記使用者装置の使用者データに対してハッシュ演算を実行して前記使用者データのハッシュ値を生成することと、
ＩｏＴ装置のＩｏＴ装置公開鍵(P_{IoT})と使用者乱数(R_u)とに基づいて第１の暗号化情報を取得することと、
前記使用者秘密鍵(K_u)と前記使用者乱数(R_u)と前記ハッシュ値とに基づいて第２の暗号化情報を取得することと、
認証要求を前記ＩｏＴ装置に送信することとを含み、
前記認証要求は、前記使用者データの前記ハッシュ値と、前記第１の暗号化情報と、前記第２の暗号化情報とを含む、
使用者装置。
【０１０７】
３２．
ＩｏＴ装置のＩｏＴ装置公開鍵(P_{IoT})と使用者乱数(R_u)とに基づいて第１の暗号化情報を取得することは、
前記ＩｏＴ装置公開鍵(P_{IoT})使用して前記使用者乱数(R_u)を暗号化し、前記第１の暗号化情報($P_{IoT}(R_u)$)を生成することを備え、
前記使用者秘密鍵(K_u)と前記使用者乱数(R_u)と前記ハッシュ値とに基づいて第２の暗号化情報を取得することは、
前記使用者秘密鍵(K_u)を使用して前記ハッシュ値を暗号化し、前記使用者装置の使用者署名($K_u(H)$)生成することと、
前記使用者乱数を使用して前記使用者署名を暗号化し、前記第２の暗号化情報($R_u(K_u(H))$)を生成することとを備え、
Ｈは、前記ハッシュ値を表す、
項３１に記載の使用者装置。
【０１０８】
３３．
ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施するための方法であって、
使用者公開鍵(P_u)と使用者秘密鍵(K_u)との対で構成される使用者装置によって実行され、
前記使用者装置の使用者データに対してハッシュ演算を実行して前記使用者データのハッシュ値を生成することと、
ＩｏＴ装置のＩｏＴ装置公開鍵(P_{IoT})と使用者乱数(R_u)とに基づいて第１の暗号化情報を取得することと、
前記使用者秘密鍵(K_u)と前記使用者乱数(R_u)と前記ハッシュ値とに基づいて第２の暗号

化情報を取得することと、
　認証要求を前記ＩｏＴ装置に送信することとを備え、
　前記認証要求は、前記使用者データの前記ハッシュ値と、前記第１の暗号化情報と、前記第２の暗号化情報とを含む、
方法。
【０１０９】
　３４．
　ＩｏＴ装置のＩｏＴ装置公開鍵(P_{IoT})と使用者乱数(R_u)とに基づいて第１の暗号化情報を取得することは、
　前記ＩｏＴ装置公開鍵(P_{IoT})使用して前記使用者乱数(R_u)を暗号化し、前記第１の暗号化情報($P_{IoT}(R_u)$)を生成することを備え、
　前記使用者秘密鍵(K_u)と前記使用者乱数(R_u)と前記ハッシュ値とに基づいて第２の暗号化情報を取得することは、
　前記使用者秘密鍵(K_u)を使用して前記ハッシュ値を暗号化し、前記使用者装置の使用者署名($K_u(H)$)生成することと、
　前記使用者乱数を使用して前記使用者署名を暗号化し、前記第２の暗号化情報($R_u(K_u(H))$)を生成することとを備え、
　Ｈは、前記ハッシュ値を表す、
項３３に記載の方法。
【０１１０】
　３５．
　ブロックチェーンに基づいて信頼性Internet of Things（ＩｏＴ）サービスを実施するための不揮発性コンピュータ可読記憶媒体であって、
　機械実行可能命令を備え、
　前記機械実行可能命令は、機械によって実行されると、項３３または３４に記載の方法を前記機械に実施させるように適合される、
不揮発性コンピュータ可読記憶媒体。

【図面】

【図１】

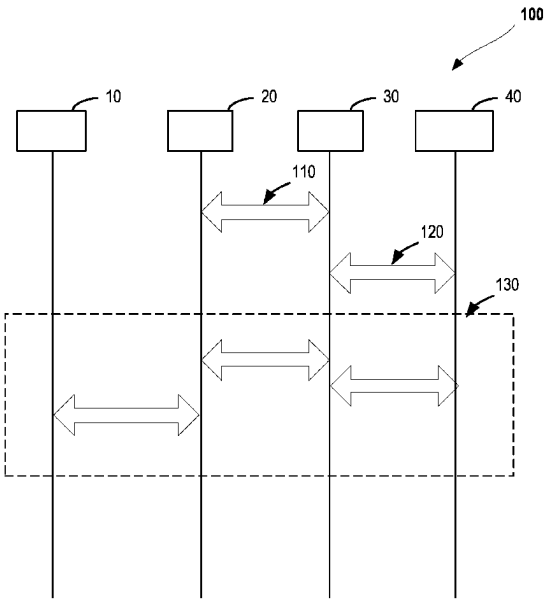


FIG. 1

【図２】

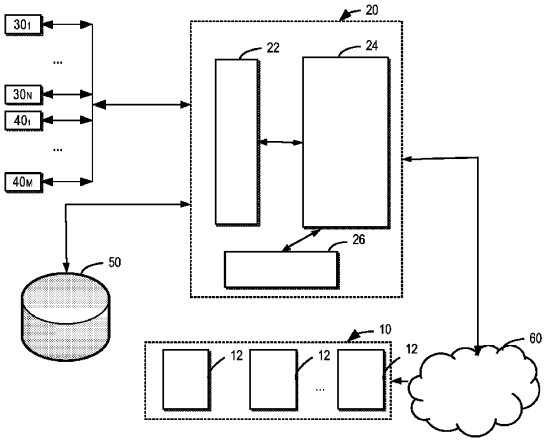
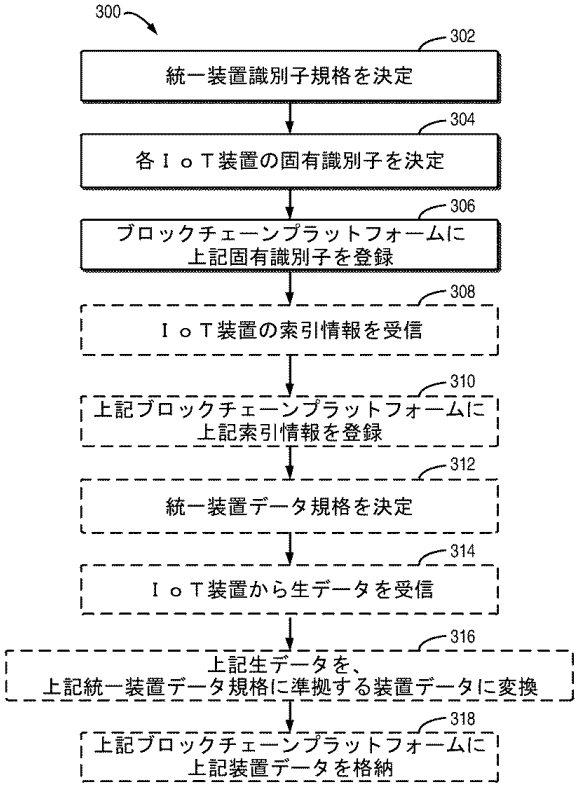
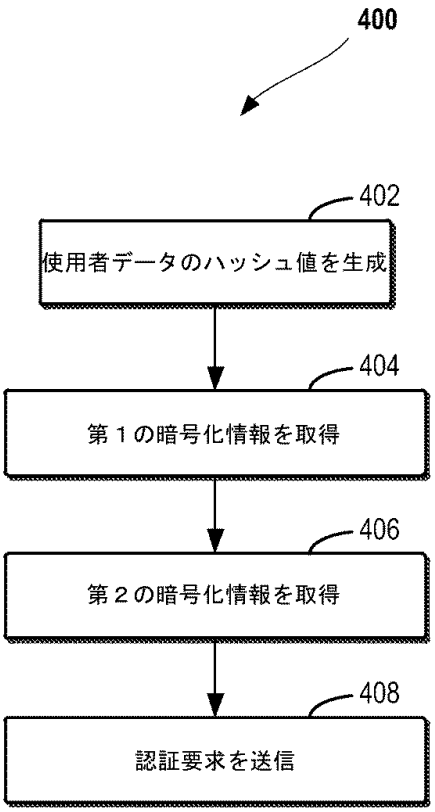


FIG. 2

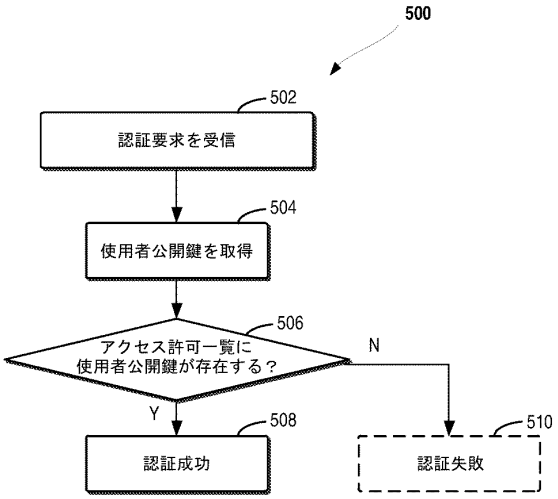
【図３】



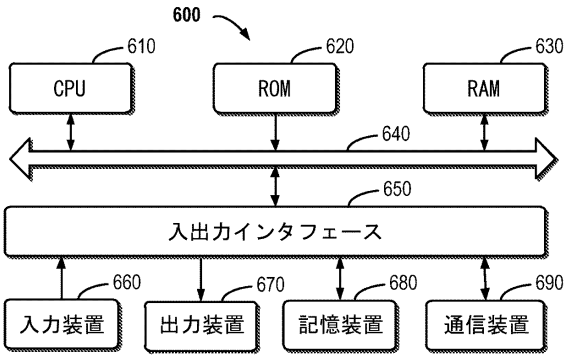
【図４】



【図５】


500
502
認証要求を受信
504
使用者公開鍵を取得
506
アクセス許可一覧に
使用者公開鍵が存在する？
N
Y
508
認証成功
510
認証失敗

【図６】


600
610
CPU
620
ROM
630
RAM
640
650
入出力インタフェース
660
入力装置
670
出力装置
680
記憶装置
690
通信装置

フロントページの続き

２５， プードン ディストリクト， チェンシャン ロード， レーン １７２８， ブロック ２，
ルーム ５０１
(72)発明者 ジャンリャン グ
中華人民共和国， シャンハイ ２０００８０， ホンコウ ディストリクト， ハイルン ロード，
レーン ５５５， ブロック シー， ルーム ２３０１
(72)発明者 ジヘン ジョウ
中華人民共和国， シャンハイ ２００２３５， シュイホイ ディストリクト， グーイー ロード，
レーン １８０， ブロック １， ルーム ８０５

審査官 金沢 史明

(56)参考文献
米国特許出願公開第２０１７／０１２４５３４（ＵＳ，Ａ１）
特開２０１８－００５８１８（ＪＰ，Ａ）
国際公開第２０１７／０３５３３３（WO，Ａ１）
特表２０１８－５２８６９１（ＪＰ，Ａ）
国際公開第２０１７／２０７３１６（WO，Ａ１）
特開２０１７－１６３６１２（ＪＰ，Ａ）
米国特許出願公開第２０１７／０１７１１８０（ＵＳ，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／００－ ９／４０
Ｇ０６Ｆ ２１／４４