(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-57827
(P2019-57827A)
(43)公開日　平成31年4月11日(2019.4.11)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
H04L	9/08	(2006.01)	H04L	9/00	601F	
G09C	1/00	(2006.01)	G09C	1/00	640D	

審査請求 未請求　請求項の数 8　ＯＬ　（全 18 頁）

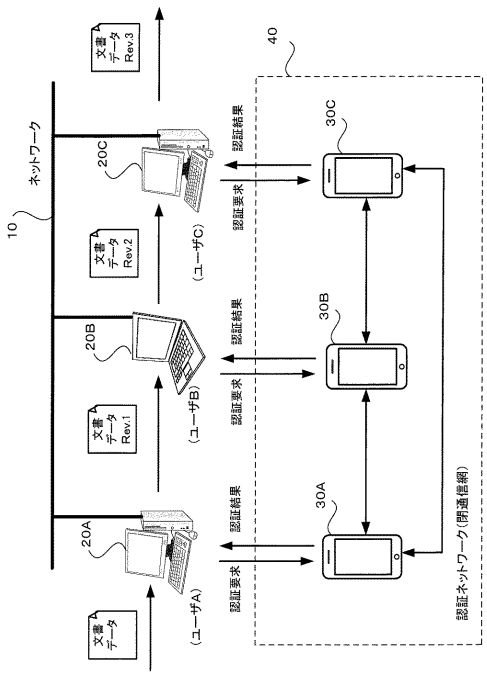
(21)出願番号　特願2017-181179 (P2017-181179)
(22)出願日　平成29年9月21日 (2017.9.21)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　110000039
特許業務法人アイ・ピー・ウィン
(72)発明者　布施　透
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックス株式会社内

Ｆターム(参考)　5J104 AA08 AA16 EA19 JA21 LA01 NA02 NA12 NA37 PA07

(54)【発明の名称】分散認証システムおよびプログラム

(57)【要約】
【課題】判定対象情報の真正性を検証する認証処理を行う際に、中央管理機能を必要とすることなく、ブロックチェーン技術を用いた場合と比較して演算処理の処理負荷を少なくする。
【解決手段】認証装置３０は１つ以上の秘密鍵を格納し、複数の制御装置２０はこの秘密鍵に対応した公開鍵を格納する。制御装置２０は、他の制御装置２０から文書データと暗号化されたハッシュ値が送信されてきた場合、その文書データのハッシュ値を算出して自装置内に格納している公開鍵により暗号化する。そして、制御装置２０は、他の制御装置２０からの暗号化されたハッシュ値および自装置内で暗号化したハッシュ値を含む認証要求をいずれかの認証装置３０に送信する。認証装置３０は、自装置または他の認証装置３０内に記憶されている秘密鍵により２つのハッシュ値を復号し、復号した２つのハッシュ値が一致した場合、文書データは真正なものである旨の認証結果を返信する。
【選択図】図１



【特許請求の範囲】
【請求項１】
それぞれ少なくとも１つ以上の秘密鍵を格納する第１の格納手段を有する複数の認証装置と、
前記複数の認証装置のいずれかにおいて記憶されている秘密鍵に対応した公開鍵を格納する第２の格納手段を有し、他の制御装置から判定対象情報と暗号化されたハッシュ値が送信されてきた場合、当該判定対象情報のハッシュ値を算出して、算出されたハッシュ値を前記第２の格納手段に格納されている公開鍵により暗号化し、他の制御装置から送信されてきた暗号化されたハッシュ値および自装置内で暗号化したハッシュ値を含む認証要求を前記複数の認証装置のうちの通信可能ないずれかの認証装置に送信する複数の制御装置とを備え、
前記複数の認証装置は、それぞれ、前記複数の制御装置のいずれかの制御装置から暗号化された２つのハッシュ値を含む認証要求を受信した場合、自装置内の前記第１の格納手段に記憶されている秘密鍵または他の認証装置内の前記第１の格納手段に記憶されている秘密鍵のいずれかにより復号した２つのハッシュ値が一致した場合に、判定対象情報は真正なものである旨を前記認証要求に対して返信する
分散認証システム。
【請求項２】
前記複数の認証装置は、それぞれ、前記複数の制御装置のいずれかの制御装置から暗号化された２つのハッシュ値を含む認証要求を受信した場合、自装置内の前記第１の格納手段に記憶されている秘密鍵により復号可能であれば当該秘密鍵により暗号化されたハッシュ値を復号し、復号不可能の場合には、暗号化されたハッシュ値を含む復号要求を他の認証装置に転送することにより、暗号化された２つのハッシュ値の復号を行う請求項１記載の分散認証システム。
【請求項３】
前記複数の認証装置は、それぞれ、お互いに対応した公開鍵、秘密鍵を格納する第３の格納手段を有し、他の認証装置に復号要求を転送する際には、前記第３の格納手段に格納されている自装置の公開鍵を前記復号要求に含め、
暗号化されたハッシュ値を復号した認証装置は、復号したハッシュ値を、復号要求を行った認証装置の公開鍵で暗号化して返信する請求項２記載の分散認証システム。
【請求項４】
前記複数の制御装置は、それぞれ、
判定対象情報のハッシュ値を算出する算出手段と、
前記算出手段により算出されたハッシュ値を前記第２の格納手段に格納されている公開鍵により暗号化する暗号化手段とをさらに有し、
他の制御装置から判定対象情報と暗号化されたハッシュ値が送信されてきた場合、前記算出手段により当該判定対象情報のハッシュ値を算出して、算出されたハッシュ値を前記暗号化手段において公開鍵により暗号化する請求項１から３のいずれか記載の分散認証システム。
【請求項５】
前記複数の制御装置は、それぞれ、前記第２の格納手段に格納されている公開鍵に対応する秘密鍵を保有する認証装置を特定するための情報を有していない請求項４記載の分散認証システム。
【請求項６】
前記複数の認証装置は、閉じられたネットワークにより相互に接続されている請求項１から５のいずれか記載の分散認証システム。
【請求項７】
他の制御装置から判定対象情報と暗号化されたハッシュ値が送信されてきた場合、当該判定対象情報のハッシュ値を算出するステップと、
算出されたハッシュ値を、複数の認証装置のいずれかにおいて記憶されている秘密鍵に

対応した公開鍵により暗号化するステップと、
　他の制御装置から送信されてきた暗号化されたハッシュ値および自装置内で暗号化したハッシュ値を含む認証要求を複数の認証装置のうちの通信可能ないずれかの認証装置に送信するステップと、
　をコンピュータに実行させるためのプログラム。
【請求項８】
　複数の制御装置のいずれかの制御装置から暗号化された２つのハッシュ値を含む認証要求を受信した場合、自装置内に記憶されている秘密鍵または他の認証装置に格納されている秘密鍵のいずれかにより復号するステップと、
　復号された２つのハッシュ値を比較するステップと、
　比較した２つのハッシュ値が一致した場合に、判定対象情報は真正なものである旨を前記認証要求に対して返信するステップと、
　をコンピュータに実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、分散認証システムおよびプログラムに関する。
【背景技術】
【０００２】
　特許文献１には、分散認証サーバを構成する装置を含む通信システムにおいて、認証されることを求める証明者側装置が、分散認証サーバの各装置に、証明者及び認証者の識別子を含む認証要求メッセージを送信し、分散認証サーバの各装置が共同して、認証要求メッセージに基づいて、認証者に関する秘密鍵で暗号化された認証子を生成し、認証子を証明者に関する秘密鍵で暗号化して認証メッセージを生成し、分散認証サーバの各装置が、認証メッセージを証明者側装置に送信し、認証メッセージを受信した証明者側装置が、認証メッセージを復号し、得られた認証子を認証者側装置に送信し、認証子を受信した認証者側装置が、認証子を復号して証明者を認証するようにした認証方法が開示されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特許第３６１０１０６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
　生成された情報を複数の装置間で更新しながら順次次の宛先に配信するようなシステムでは、途中で改ざんされていないことを確認するために認証システムが必要となる。一般的には１つの認証サーバ等において配信内容を一元的に管理して認証処理を行う中央管理機能を備えた認証システムが用いられている。
【０００５】
　しかし、このような中央管理機能を備えた認証システムでは、認証処理が１つの認証サーバに集中するため、処理能力が高い装置が必要となる。
【０００６】
　このような処理負荷の集中を分散するため、いわゆるブロックチェーン技術（分散型台帳技術）と呼ばれる技術が提案されている。このブロックチェーン技術とは、トランザクションの結果を一方向性関数を利用して検証する仕組みにより情報の改ざんを防止している。しかし、このブロックチェーン技術による検証には計算負荷の大きな演算処理が必要なため、検証環境を備えることが容易ではない。
【０００７】
　本発明の目的は、判定対象情報の真正性を検証する認証処理を行う際に、中央管理機能を必要とすることなく、ブロックチェーン技術を用いた場合と比較して、演算処理の処理

負荷を少なくすることが可能な分散認証システムおよびプログラムを提供することである。

【課題を解決するための手段】

【０００８】

［分散認証システム］

請求項１に係る本発明は、それぞれ少なくとも１つ以上の秘密鍵を格納する第１の格納手段を有する複数の認証装置と、

前記複数の認証装置のいずれかにおいて記憶されている秘密鍵に対応した公開鍵を格納する第２の格納手段を有し、他の制御装置から判定対象情報と暗号化されたハッシュ値が送信されてきた場合、当該判定対象情報のハッシュ値を算出して、算出されたハッシュ値を前記第２の格納手段に格納されている公開鍵により暗号化し、他の制御装置から送信されてきた暗号化されたハッシュ値および自装置内で暗号化したハッシュ値を含む認証要求を前記複数の認証装置のうちの通信可能ないずれかの認証装置に送信する複数の制御装置とを備え、

前記複数の認証装置は、それぞれ、前記複数の制御装置のいずれかの制御装置から暗号化された２つのハッシュ値を含む認証要求を受信した場合、自装置内の前記第１の格納手段に記憶されている秘密鍵または他の認証装置内の前記第１の格納手段に記憶されている秘密鍵のいずれかにより復号した２つのハッシュ値が一致した場合に、判定対象情報は真正なものである旨を前記認証要求に対して返信する分散認証システムである。

【０００９】

請求項２に係る本発明は、前記複数の認証装置が、それぞれ、前記複数の制御装置のいずれかの制御装置から暗号化された２つのハッシュ値を含む認証要求を受信した場合、自装置内の前記第１の格納手段に記憶されている秘密鍵により復号可能であれば当該秘密鍵により暗号化されたハッシュ値を復号し、復号不可能の場合には、暗号化されたハッシュ値を含む復号要求を他の認証装置に転送することにより、暗号化された２つのハッシュ値の復号を行う請求項１記載の分散認証システムである。

【００１０】

請求項３に係る本発明は、前記複数の認証装置が、それぞれ、お互いに対応した公開鍵、秘密鍵を格納する第３の格納手段を有し、他の認証装置に復号要求を転送する際には、前記第３の格納手段に格納されている自装置の公開鍵を前記復号要求に含め、

暗号化されたハッシュ値を復号した認証装置は、復号したハッシュ値を、復号要求を行った認証装置の公開鍵で暗号化して返信する請求項２記載の分散認証システムである。

【００１１】

請求項４に係る本発明は、前記複数の制御装置が、それぞれ、

判定対象情報のハッシュ値を算出する算出手段と、

前記算出手段により算出されたハッシュ値を前記第２の格納手段に格納されている公開鍵により暗号化する暗号化手段とをさらに有し、

他の制御装置から判定対象情報と暗号化されたハッシュ値が送信されてきた場合、前記算出手段により当該判定対象情報のハッシュ値を算出して、算出されたハッシュ値を前記暗号化手段において公開鍵により暗号化する請求項１から３のいずれか記載の分散認証システムである。

【００１２】

請求項５に係る本発明は、前記複数の制御装置が、それぞれ、前記第２の格納手段に格納されている公開鍵に対応する秘密鍵を保有する認証装置を特定するための情報を有していない請求項４記載の分散認証システムである。

【００１３】

請求項６に係る本発明は、前記複数の認証装置が、閉じられたネットワークにより相互に接続されている請求項１から５のいずれか記載の分散認証システムである。

【００１４】

[プログラム]

請求項７に係る本発明は、他の制御装置から判定対象情報と暗号化されたハッシュ値が送信されてきた場合、当該判定対象情報のハッシュ値を算出するステップと、
算出されたハッシュ値を、複数の認証装置のいずれかにおいて記憶されている秘密鍵に対応した公開鍵により暗号化するステップと、
他の制御装置から送信されてきた暗号化されたハッシュ値および自装置内で暗号化したハッシュ値を含む認証要求を複数の認証装置のうちの通信可能ないずれかの認証装置に送信するステップとをコンピュータに実行させるためのプログラムである。

【００１５】

請求項８に係る本発明は、複数の制御装置のいずれかの制御装置から暗号化された２つのハッシュ値を含む認証要求を受信した場合、自装置内に記憶されている秘密鍵または他の認証装置に格納されている秘密鍵のいずれかにより復号するステップと、
復号された２つのハッシュ値を比較するステップと、
比較した２つのハッシュ値が一致した場合に、判定対象情報は真正なものである旨を前記認証要求に対して返信するステップとをコンピュータに実行させるためのプログラムである。

【発明の効果】

【００１６】

請求項１に係る本発明によれば、判定対象情報の真正性を検証する認証処理を行う際に、中央管理機能を必要とすることなく、ブロックチェーン技術を用いた場合と比較して、演算処理の処理負荷を少なくすることが可能な分散認証システムを提供することができる。

【００１７】

請求項２に係る本発明によれば、判定対象情報の真正性を検証する認証処理を行う際に、中央管理機能を必要とすることなく、ブロックチェーン技術を用いた場合と比較して、演算処理の処理負荷を少なくすることが可能な分散認証システムを提供することができる。

【００１８】

請求項３に係る本発明によれば、暗号化されていないハッシュ値が、複数の認証装置間で送受信されるのを防ぐことが可能な分散認証システムを提供することができる。

【００１９】

請求項４に係る本発明によれば、判定対象情報の真正性を検証する認証処理を行う際に、中央管理機能を必要とすることなく、ブロックチェーン技術を用いた場合と比較して、演算処理の処理負荷を少なくすることが可能な分散認証システムを提供することができる。

【００２０】

請求項５に係る本発明によれば、複数の制御装置は、それぞれ、複数の認証装置のうちのいずれの認証装置に、自装置を格納している公開鍵に対応した秘密鍵を保有しているかの情報を管理する必要をなくすことが可能な分散認証システムを提供することができる。

【００２１】

請求項６に係る本発明によれば、複数の認証装置が開かれたネットワークにより相互に接続されている場合と比較して、認証処理の正確性を向上させることが可能な分散認証システムを提供することができる。

【００２２】

請求項７に係る本発明によれば、判定対象情報の真正性を検証する認証処理を行う際に、中央管理機能を必要とすることなく、ブロックチェーン技術を用いた場合と比較して、演算処理の処理負荷を少なくすることが可能なプログラムを提供することができる。

【００２３】

請求項８に係る本発明によれば、判定対象情報の真正性を検証する認証処理を行う際に、中央管理機能を必要とすることなく、ブロックチェーン技術を用いた場合と比較して、演算処理の処理負荷を少なくすることが可能なプログラムを提供することができる。

【図面の簡単な説明】
【００２４】
【図１】本発明の一実施形態の分散認証システムのシステム構成を示す図である。
【図２】本発明の一実施形態の分散認証システムのシステム構成を示す他の図である。
【図３】本発明の一実施形態における制御装置２０のハードウェア構成を示すブロック図である。
【図４】本発明の一実施形態における制御装置２０の機能構成を示すブロック図である。
【図５】本発明の一実施形態における認証装置３０のハードウェア構成を示すブロック図である。
【図６】本発明の一実施形態における認証装置３０の機能構成を示すブロック図である。
【図７】制御装置２０Ｂが制御装置２０Ａからの文書データを受信した際に、この文書データが制御装置２０Ａからのものであるという真正性を確認する際の認証処理を行う様子を説明するための図である。
【図８】制御装置２０Ａ、２０Ｂおよび認証ネットワーク４０内の認証装置３０における公開鍵と秘密鍵の対応関係を説明するための図である。
【図９】制御装置２０Ｂにおいて文書データの真正性を確認する処理が行われる前の制御装置２０Ａにおける処理を説明するためのフローチャートである。
【図１０】制御装置２０Ｂにおける認証要求処理を説明するためのフローチャートである。
【図１１】制御装置２０Ａにおける処理と制御装置２０Ｂにおける処理の流れを図示した図である。
【図１２】制御装置２０Ｂからの認証要求を受けた認証装置３０Ｂにおける認証処理の動作を説明するためのフローチャートである。
【図１３】認証装置３０Ｂから、暗号化されたハッシュ値Ａ、Ｂおよび認証装置３０Ｂの公開鍵ＰＫを含む復号要求が送信される様子を示す図である。
【図１４】認証装置３０Ｂから送信された認証要求を、認証装置３０Ｂ以外の認証装置３０が受信して復号処理を行う際の動作を説明するためのフローチャートである。
【図１５】図１４において説明する復号処理の様子を示す図である。
【図１６】暗号化されたハッシュ値Ａ、Ｂが返信されてきた認証装置３０Ｂにおける動作を説明するための図である。
【発明を実施するための形態】
【００２５】
次に、本発明の実施の形態について図面を参照して詳細に説明する。
【００２６】
図１は本発明の一実施形態の分散認証システムのシステム構成を示す図である。
【００２７】
本発明の一実施形態の分散認証システムは、図１に示されるように、文書データに対する更新処理を順次行う複数の制御装置（データフロー制御装置）２０Ａ～２０Ｃと、認証ネットワーク４０を構成する複数の認証装置３０Ａ～３０Ｃとから構成されている。
【００２８】
なお、図１では、３台の制御装置２０Ａ～２０Ｃと、３台の認証装置３０Ａ～３０Ｃとが示されているが、それぞれ、実際には３台以上存在する。
【００２９】
また、以降の説明においては、複数の制御装置２０Ａ～２０Ｃうちの１つの装置を特定せずに共通して説明する場合には制御装置２０として示し、複数の認証装置３０Ａ～３０Ｃうちの１つの装置を特定せずに共通して説明する場合には認証装置３０として示す。
【００３０】
複数の制御装置２０は、文書データに対する更新処理を順次行うデータフロー制御装置であり、具体的には可搬式あるいは据え置き型の各種のパーソナルコンピュータに専用のソフトウェアをインストールすることにより実現することができる。なお、スマートフォ

ンやタブレット端末を制御装置２０として用いることも可能である。
【００３１】
この複数の制御装置２０は、例えば同一のフロア、同一のビル、同一の法人内等の限定された範囲で、利用可能なネットワーク１０により相互に接続されており、文書データの送受信やインターネットに接続して各種の情報を取得することが可能となっている。
【００３２】
また、複数の認証装置３０は、例えば、お互いに無線接続されており、この複数の認証装置３０により認証ネットワーク４０が構成されている。
この認証ネットワーク４０は閉じられたネットワークであり、複数の認証装置３０は、この閉じられたネットワークである認証ネットワーク４０により相互に接続されている。
【００３３】
なお、本実施形態では、認証ネットワーク４０はメッシュネットワークである場合を用いて説明するが、本発明はこのようなネットワーク構成に限定されるものではない。認証ネットワーク４０におけるネットワークトポロジーの種類が本発明を制約するものではないため、認証ネットワーク４０を、ツリーネットワーク、スターネットワーク、リングネットワーク、あるいはバスネットワークにより構成するようにしても良い。
【００３４】
さらに、認証装置３０は、具体的な構成として、通信機能を有する小型の計算機（温度や湿度等を計測して通信機能によってその測定値を任意の他の計算機へ送信できる計算機や、スマートフォン等の高機能な小型計算機を含む）とそのリソース上で動作するソフトウェアで構成できる。また、認証ネットワーク４０は閉通信網（閉ネットワーク）である場合を用いて説明するが、認証ネットワーク４０を移動体通信網で構成することも可能である。
【００３５】
そして、本実施形態の分散認証システムでは、制御装置２０Ａ～２０Ｂは、それぞれ順序が前の他の制御装置２０から更新済みの文書データを受信して、自装置内で新たなに文書の削除・追加・変更等の各種処理を行うことにより更新して、順序が次の制御装置２０に送信するような処理が実行される。
【００３６】
その際に、受信した文書データが、本当に順序が前の制御装置２０からのものであるのか否か、つまり悪意のある第三者が他のユーザになりすましてすり替えたものではないか否かを確認する認証処理が行われる。
【００３７】
例えば、ユーザＡが制御装置２０Ａにおいて文書データを更新してユーザＢの制御装置２０Ｂに渡し、ユーザＢが受け取った文書データを更新してユーザＣの制御装置２０Ｃに渡し、ユーザＣが受け取った文書データを更新して次のユーザの制御装置２０に渡すような場合を用いて説明する。
【００３８】
このような場合、ユーザＢがユーザＡから受け取った文書データが、本当にユーザＡからの文書データであるのか否かを確認するために、ユーザＢは、制御装置２０Ｂから認証ネットワーク４０に対して認証要求を行う。そして、制御装置２０Ｂが、認証ネットワーク４０からユーザＡの文書データである、つまり真正な文書データである旨の認証結果が得られた場合、その文書データをユーザＡからのものとして処理を行う。
【００３９】
なお、実際には認証ネットワーク４０は、図２に示すように、数多くの認証装置３０Ａ～３０Ｉにより構成されているが、各制御装置２０は認証ネットワーク４０内の全ての認証装置３０と通信可能なわけではなく、それぞれの制御装置２０が通信可能な認証装置３０が決まっている。例えば、図１、図２に示した分散認証システムでは、制御装置２０Ａ～２０Ｃは、それぞれ、認証装置３０Ａ～３０Ｃとのみ通信可能となっている。
【００４０】

そして、制御装置２０Ａ～２０Ｃは、他の制御装置２０から文書データを受信すると、受信した文書データが真正な文書データであるか否かを、それぞれ通信可能な認証装置３０Ａ～３０Ｃに対して確認する認証要求を行い、真正である旨の認証結果を受信することによりその文書データを真正なものとして扱うような構成となっている。

【００４１】

次に、本実施形態の分散認証システムにおける制御装置２０と認証装置３０の構成についてそれぞれ順次説明する。

【００４２】

先ず、本実施形態の分散認証システムにおける制御装置２０Ａのハードウェア構成を図３に示す。なお、ここでは制御装置２０Ａの構成について説明するが、制御装置２０Ｂ、２０Ｃも同様な構成であるためその説明は省略する。

【００４３】

制御装置２０Ａは、図３に示されるように、ＣＰＵ１１、メモリ１２、ハードディスクドライブ（ＨＤＤ）等の記憶装置１３、ネットワーク１０を介して外部の装置等との間でデータの送信及び受信を行い、また認証ネットワーク４０を介して認証装置３０Ａとの間でデータの送受信を行う通信インタフェース（ＩＦ）１４、タッチパネル又は液晶ディスプレイ並びにキーボードを含むユーザインタフェース（ＵＩ）装置１５を有する。これらの構成要素は、制御バス１６を介して互いに接続されている。

【００４４】

ＣＰＵ１１は、メモリ１２または記憶装置１３に格納された制御プログラムに基づいて所定の処理を実行して、制御装置２０Ａの動作を制御する。なお、本実施形態では、ＣＰＵ１１は、メモリ１２または記憶装置１３内に格納された制御プログラムを読み出して実行するものとして説明したが、当該プログラムをＵＳＢメモリやＣＤ－ＲＯＭ等の記憶媒体に格納してＣＰＵ１１に提供することも可能である。

【００４５】

図４は、上記の制御プログラムが実行されることにより実現される制御装置２０Ａの機能構成を示すブロック図である。

【００４６】

本実施形態の制御装置２０Ａは、図４に示されるように、制御部２１と、ハッシュ値算出部２２と、暗号化部２３と、公開鍵格納部２４と、通信部２５とを備えている。

【００４７】

公開鍵格納部２４は、複数の認証装置３０のいずれかにおいて記憶されている秘密鍵に対応した公開鍵を格納する。なお、図４では、制御装置２０Ａ内に格納されている公開鍵をＰＫ（Ａ）として示している。同様に以降の説明においては、制御装置２０Ｂ内に格納されている公開鍵をＰＫ（Ｂ）として説明する。

【００４８】

ハッシュ値算出部２２は、判定対象情報である文書データのハッシュ値（要約値）を算出する。なお、ハッシュ値を算出するためのアルゴリズム（算出方式）としては様々なアルゴリズムが存在するが、本実施形態では、例えばＳＨＡ（Secure Hash Algorithm）－２という規格のハッシュ関数を用いたハッシュ値算出アルゴリズムを用いてハッシュ値の算出が行われる。このＳＨＡ－２規格に含まれる１つの方式であるＳＨＡ－２５６というアルゴリズムでは、ハッシュ長が２５６ビットのハッシュ値が算出される。

【００４９】

暗号化部２３は、ハッシュ値算出部２２により算出されたハッシュ値を公開鍵格納部２４に格納されている公開鍵ＰＫ（Ａ）により暗号化する。

【００５０】

通信部２５は、対応する認証装置３０Ａとの間のデータ送受信や、ネットワーク１０を介して他の制御装置２０Ｂ、２０Ｃとの間のデータ送受信を行う。

【００５１】

制御部２１は、他の制御装置２０から判定対象情報である文書データと暗号化されたハ

ッシュ値が送信されてきた場合、その文書データのハッシュ値をハッシュ値算出部２２により算出して、算出されたハッシュ値を公開鍵格納部２４に格納されている公開鍵ＰＫ（Ａ）により暗号化する。そして、制御部２１は、他の制御装置２０から送信されてきた暗号化されたハッシュ値および自装置内で暗号化したハッシュ値を含む認証要求を複数の認証装置３０のうちの通信可能ないずれかの認証装置に送信する。ここでは、制御装置２０Ａが通信可能なのは認証装置３０Ａであるため、制御部２１は、認証要求を認証装置３０Ａに対して行う。

【００５２】

また、制御部２１は、他の制御装置２０から文書データと暗号化されたハッシュ値が送信されてきた場合、ハッシュ値算出部２２によりその文書データのハッシュ値を算出して、算出されたハッシュ値を暗号化部２３において公開鍵ＰＫ（Ａ）により暗号化する。

【００５３】

そして、制御部２１は、暗号化したハッシュ値および他の制御装置２０から送信されてきた暗号化済みのハッシュ値と、文書データを送信してきた制御装置２０および自装置の識別子とを含めた認証要求を対応する認証装置３０Ａに送信して、他の制御装置２０からの文書データが真正なものであるのか否かを確認する。

【００５４】

ここで、複数の制御装置２０は、それぞれ、公開鍵格納部２４に格納されている公開鍵ＰＫ（Ａ）、ＰＫ（Ｂ）、・・・に対応する秘密鍵ＳＫ（Ａ）、ＳＫ（Ｂ）、・・・を保有する認証装置３０を特定するための情報を有していない。つまり、制御装置２０Ａは、自装置内に格納されている公開鍵ＰＫ（Ａ）に対応する秘密鍵ＳＫ（Ａ）を、認証装置３０Ａ～３０Ｉのうちのいずれの認証装置が保有しているかを特定するための情報を有していない。

【００５５】

次に、本実施形態の分散認証システムにおける認証装置３０のハードウェア構成を図５に示す。

【００５６】

認証装置３０は、図５に示されるように、ＣＰＵ４１、メモリ４２、ハードディスクドライブ（ＨＤＤ）等の記憶装置４３、認証ネットワーク４０を介して外部の装置等との間でデータの送信及び受信を行う通信インタフェース（ＩＦ）４４を有する。また、認証装置３０はタッチパネル又は液晶ディスプレイ並びにキーボードを含むユーザインタフェース（ＵＩ）装置４５を有してもよい。これらの構成要素は、制御バス４６を介して互いに接続されている。

【００５７】

ＣＰＵ４１は、メモリ４２または記憶装置４３に格納された制御プログラムに基づいて所定の処理を実行して、認証装置３０の動作を制御する。なお、本実施形態では、ＣＰＵ４１は、メモリ４２または記憶装置４３内に格納された制御プログラムを読み出して実行するものとして説明したが、当該プログラムをＵＳＢメモリ等の記憶媒体に格納してＣＰＵ４１に提供することも可能である。

【００５８】

図６は、上記の制御プログラムが実行されることにより実現される認証装置３０の機能構成を示すブロック図である。

【００５９】

本実施形態の認証装置３０は、図６に示されるように、制御部３１と、暗号化／復号部３２と、鍵ペア格納部３３と、秘密鍵格納部３４と、通信部３５とを備えている。

【００６０】

暗号化／復号部３２は、秘密鍵格納部３４に格納されている秘密鍵ＳＫ（Ｎ）により、制御装置２０から送信されてきたハッシュ値の復号を行ったり、復号されたハッシュ値を、他の認証装置３０からの復号要求に含まれる公開鍵ＰＫにより暗号化する処理を行う。

【００６１】

秘密鍵格納部３４は、制御装置２０において格納されている公開鍵ＰＫ（Ｎ）に対応する少なくとも１つ以上の秘密鍵ＳＫ（Ｎ）を格納する。なお、公開鍵ＰＫ（Ｎ）と秘密鍵（Ｎ）とは、公開鍵暗号方式において用いられる鍵ペアとして対応関係にあることを示すため、「Ｎ」として示している。例えば、公開鍵ＰＫ（Ａ）に対応するのは秘密鍵ＳＫ（Ａ）であり、公開鍵ＰＫ（Ｂ）に対応するのは秘密鍵ＳＫ（Ｂ）であある。

【００６２】

なお、本実施形態では、公開鍵暗号方式としてＲＳＡ暗号方式を用いた場合について説明するが、ＲＳＡ暗号方式以外の公開鍵暗号方式を用いる場合でも本発明は同様に適用可能である。

【００６３】

通信部３５は、対応する制御装置２０との間のデータ送受信や、認証ネットワーク４０内の他の認証装置３０の間のデータ送受信を行う。

【００６４】

制御部３１は、複数の制御装置２０のいずれかの制御装置から暗号化された２つのハッシュ値を含む認証要求を受信した場合、自装置内の秘密鍵格納部３４に記憶されている秘密鍵ＳＫ（Ｎ）または他の認証装置３０内の秘密鍵格納部３４に記憶されている秘密鍵ＳＫ（Ｎ）のいずれかにより復号した２つのハッシュ値が一致した場合に、判定対象の文書データは真正なものである旨を認証要求に対して返信する。

【００６５】

具体的には、制御部３１は、複数の制御装置２０のいずれかの制御装置から暗号化された２つのハッシュ値を含む認証要求を受信した場合、自装置内の秘密鍵格納部３４に記憶されている秘密鍵ＳＫ（Ｎ）により復号可能であればその秘密鍵ＳＫ（Ｎ）により暗号化されたハッシュ値を復号する。そして、制御部３１は、自装置内の秘密鍵格納部３４に記憶されている秘密鍵ＳＫ（Ｎ）では復号が不可能な場合には、暗号化されたハッシュ値を含む復号要求を他の認証装置３０に転送することにより、暗号化された２つのハッシュ値の復号を行う。

【００６６】

鍵ペア格納部３３は、お互いに対応した公開鍵ＰＫ、秘密鍵ＳＫを格納する。つまり、認証装置３０では、各装置毎にそれぞれ異なる対応する鍵ペアである公開鍵ＰＫ、秘密鍵ＳＫを保有している。

【００６７】

そして、制御部３１は、他の認証装置３０に復号要求を転送する際には、鍵ペア格部３３に格納されている自装置の公開鍵ＰＫを復号要求に含める。

【００６８】

また、制御部３１は、他の認証装置３０からの復号要求を通信部３５を介して受信して、自装置の秘密鍵格納部３４内の秘密鍵ＳＫ（Ｎ）で復号できた場合には、復号したハッシュ値を、復号要求を行った認証装置の公開鍵ＰＫで暗号化して返信する。

【００６９】

つまり、他の認証装置３０からの復号要求に基づいて暗号化されたハッシュ値を復号した認証装置３０は、復号したハッシュ値を、復号要求を行った認証装置３０の公開鍵で暗号化して返信する。

【００７０】

次に、本実施形態の分散認証システムの動作を図面を参照して詳細に説明する。

【００７１】

先ず、以下の説明においては、図７に示すように、制御装置２０Ｂが制御装置２０Ａからの文書データを受信した際に、この文書データが制御装置２０Ａ（つまりユーザＡ）からのものであるという真正性を確認する際の認証処理が行われる場合を用いて説明する。

【００７２】

つまり、制御装置２０ＢのユーザＢが、受信した文書データが本当にユーザＡからものであるのか、つまり真正であるのか、あるいは途中で悪意のある第三者により何らかの改

ざんが加えられたものであるのか、つまり不正なものであるのかを確認するための認証処理を実行する場合を用いて説明する。

【００７３】

ここで、制御装置２０Ｂが通信可能な認証装置は認証装置３０Ｂのみであるため、制御装置２０Ｂは認証装置３０Ｂに対して認証要求を行い、認証装置３０Ｂからの認証結果を受信することにより文書データの真正性を確認する。

【００７４】

先ず、以降の説明をする前に、制御装置２０Ａ、２０Ｂおよび認証ネットワーク４０内の認証装置３０における公開鍵と秘密鍵の対応関係を図８を参照して説明する。

【００７５】

先ず、制御装置２０Ａ内には公開鍵ＰＫ（Ａ）が格納され、制御装置２０Ｂ内には公開鍵ＰＫ（Ｂ）が格納されている。そして、公開鍵ＰＫ（Ａ）に対応する秘密鍵ＳＫ（Ａ）は認証装置３０Ｈ内に格納され、公開鍵ＰＫ（Ｂ）に対応する秘密鍵ＳＫ（Ｂ）は認証装置３０Ｇ内に格納されているものとして説明する。

【００７６】

また、それぞれの認証装置３０内には対応する鍵ペアが格納されているが、ここでは認証装置３０Ｂ内に格納されている鍵ペアを公開鍵ＰＫ、秘密鍵ＳＫとして示す。

【００７７】

次に、制御装置２０Ｂにおいて文書データの真正性を確認する処理が行われる前の制御装置２０Ａにおける処理を図９のフローチャートを参照して説明し、制御装置２０Ｂにおける認証要求処理を図１０のフローチャートを参照して説明する。また、この制御装置２０Ａにおける処理と制御装置２０Ｂにおける処理の流れを図１１に図示する。

【００７８】

先ず、図９のフローチャートを参照して説明すると、制御装置２０Ａでは、制御装置２０Ｂに送信しようとする文書データのハッシュ値（ハッシュ値Ａ）を算出する（ステップＳ１０１）。なお、この制御装置２０Ａ内のハッシュ値算出部２２により算出されるハッシュ値をハッシュ値Ａとして表現する。

【００７９】

そして、制御装置２０Ａでは、このハッシュ値Ａは暗号化部２３により、公開鍵格納部２４に格納されている公開鍵ＰＫ（Ａ）により暗号化（ＲＳＡ暗号化）される（ステップＳ１０２）。

【００８０】

そして、制御装置２０Ａでは、暗号化されたハッシュ値Ａと、文書データおよび自装置の識別子（ＩＤ）の情報を制御装置２０Ｂに送信する（ステップＳ１０３）。

【００８１】

このようにして、図１１に示されるように、制御装置２０Ａから制御装置２０Ｂに対して、文書データとともにこの文書データのハッシュ値を、制御装置２０Ａ内に格納されている公開鍵ＰＫ（Ａ）により暗号化された情報が送信される。

【００８２】

次に、図１０のフローチャートを参照して説明すると、制御装置２０Ｂは、制御装置２０Ａから暗号化されたハッシュ値Ａ、制御装置２０Ａの識別子、および文書データを受信すると（ステップＳ２０１）、受信した文書データのハッシュ値（ハッシュ値Ｂ）を算出する（ステップＳ２０２）。なお、この制御装置２０Ｂ内のハッシュ値算出部２２により算出されるハッシュ値をハッシュ値Ｂとして表現する。

【００８３】

そして、制御装置２０Ｂでは、このハッシュ値Ｂは暗号化部２３により、公開鍵格納部２４に格納されている公開鍵ＰＫ（Ｂ）により暗号化（ＲＳＡ暗号化）される（ステップＳ２０３）。

【００８４】

そして、制御装置２０Ｂは、暗号化されたハッシュ値Ａ、Ｂと、制御装置２０Ａ、２０

Ｂの識別子（ＩＤ）の情報を含む認証要求を、通信可能な認証装置３０Ｂに送信する（ステップＳ２０４）。

【００８５】

ここで、制御装置２０Ｂは、認証装置３０Ｂから返信されてきた認証結果を受信して、この認証結果が文書データは真正である旨であった場合（ステップＳ２０５においてｙｅｓ）、受信した文書データはユーザＡからの真正なものであると判定する（ステップＳ２０６）。

【００８６】

また、制御装置２０Ｂは、認証装置３０Ｂから返信されてきた認証結果を受信して、この認証結果が文書データは真正ではない旨であった場合（ステップＳ２０５においてｎｏ）、受信した文書データはユーザＡからのものではない不正なものであると判定する（ステップＳ２０７）。

【００８７】

次に、制御装置２０Ｂからの認証要求を受けた認証装置３０Ｂにおける認証処理の動作を図１２のフローチャートを参照して説明する。

【００８８】

先ず、認証装置３０Ｂは、制御装置２０Ｂから、制御装置２０Ａ、２０Ｂの識別子、暗号化されたハッシュ値Ａ、Ｂを含む認証要求を受信する（ステップＳ３０１）。

【００８９】

ここで、認証装置３０Ｂは、自装置内の秘密鍵格納部３４に、ハッシュ値Ａ、Ｂのいずれかを復号可能な秘密鍵、つまり秘密鍵ＳＫ（Ａ）、ＳＫ（Ｂ）のいずれかを保有している場合（ステップＳ３０２においてＹｅｓ）、暗号化されたハッシュ値Ａ、Ｂのいずれかを自装置内の秘密鍵で復号する（ステップＳ３０３）。

【００９０】

そして、認証装置３０Ｂは、復号できなかったハッシュ値Ａまたはハッシュ値Ｂ、制御装置２０Ａ、２０Ｂの識別子に加えて自装置の公開鍵ＰＫを含む復号要求を他の認証装置３０に送信する（ステップＳ３０４）。

【００９１】

なお、ここでは、認証装置３０Ｂには、秘密鍵ＳＫ（Ａ）、ＳＫ（Ｂ）のいずれかも保有されていないため（ステップＳ３０２においてｎｏ）、認証装置３０Ｂは、暗号化されたハッシュ値Ａ、Ｂ、制御装置２０Ａ、２０Ｂの識別子に加えて自装置の公開鍵ＰＫを含む復号要求を他の認証装置３０に送信する（ステップＳ３０５）。

【００９２】

このようにして認証装置３０Ｂから、暗号化されたハッシュ値Ａ、Ｂおよび認証装置３０Ｂの公開鍵ＰＫを含む復号要求が送信される様子を図１３に示す。

【００９３】

そして、認証装置３０Ｂでは、他の認証装置３０から暗号化されたハッシュ値（ハッシュ値Ａ、Ｂのいずれか又は両方）を受信すると（ステップＳ３０６）、受信したハッシュ値を自装置の秘密鍵ＳＫで復号する処理が行われる（ステップＳ３０７）。

【００９４】

そして、認証装置３０Ｂでは、復号された２つのハッシュ値Ａ、Ｂが比較され、この２つのハッシュ値が一致する場合（ステップＳ３０８においてｙｅｓ）、認証装置３０Ｂは、受信した認証要求に対して、判定対象の文書データは真正である旨の認証結果を制御装置２０Ｂに返信する（ステップＳ３０９）。

【００９５】

なお、この２つのハッシュ値Ａ、Ｂが一致しない場合（ステップＳ３０８においてｎｏ）、認証装置３０Ｂは、受信した認証要求に対して、判定対象の文書データは真正でない旨、つまり不正である旨の認証結果を制御装置２０Ｂに返信する（ステップＳ３１０）。

【００９６】

次に、このようにして送信された復号要求を、認証装置３０Ｂ以外の認証装置３０が受

信して復号処理を行う際の動作を図１４のフローチャートを参照して説明する。また、この図１４において説明する復号処理の様子を図１５に図示する。

【００９７】

認証装置３０Ｂは、認証ネットワーク４０内の認証装置３０Ｂ以外の他の認証装置３０に対して、上記で説明した復号要求を一斉送信する。

【００９８】

そのため、認証装置３０Ｂ以外の認証装置３０では、制御装置２０Ａ、２０Ｂの識別子、暗号化されたハッシュ値Ａ、Ｂ及び認証装置３０Ｂの公開鍵ＰＫを含む復号要求がそれぞれ受信される（ステップＳ４０１）。

【００９９】

ここで、自装置内にハッシュ値Ａ、Ｂのいずれかを復号可能な秘密鍵ＳＫ（Ａ）、ＳＫ（Ｂ）を保有していない認証装置３０がこのような復号要求を受信した場合にはいずれの処理も実行されない（ステップＳ４０２においてｎｏ）。

【０１００】

そして、自装置内にハッシュ値Ａ、Ｂのいずれかを復号可能な秘密鍵ＳＫ（Ａ）、ＳＫ（Ｂ）を保有している認証装置３０、つまり本実施形態では認証装置３０Ｇ、３０Ｈがこのような復号要求を受信した場合（ステップＳ４０２においてｙｅｓ）、暗号化されたハッシュ値Ａ、Ｂは、認証装置３０Ｇ、３０Ｈ内に格納されている、制御装置２０Ａ、２０Ｂが暗号化に用いた公開鍵ＰＫ（Ａ）、ＰＫ（Ｂ）と対応する秘密鍵ＳＫ（Ａ）、またはＳＫ（Ｂ）により復号される（ステップＳ４０３）。

【０１０１】

つまり、図１５に示されるように、認証装置３０Ｇでは、公開鍵ＰＫ（Ｂ）により暗号化されていたハッシュ値Ｂは、秘密鍵ＳＫ（Ｂ）により復号される。また、認証装置３０Ｈでは、公開鍵ＰＫ（Ａ）により暗号化されていたハッシュ値Ａは、秘密鍵ＳＫ（Ａ）により復号される。

【０１０２】

そして、認証装置３０Ｇ、Ｈのいずれにおいても、復号したハッシュ値Ａ、Ｂは、復号要求を送信してきた認証装置３０Ｂの公開鍵ＰＫで暗号化される（ステップＳ４０４）。

【０１０３】

そして、このようにして暗号化されたハッシュ値Ａ、Ｂは、認証装置３０Ｂに返信される（ステップＳ４０５）。

【０１０４】

次に、暗号化されたハッシュ値Ａ、Ｂが返信されてきた認証装置３０Ｂにおける動作について図１６を参照して説明する。

【０１０５】

このようにして認証装置３０Ｂに返信されてきたハッシュ値Ａ、Ｂは、いずれも認証装置３０Ｂの公開鍵ＰＫにより暗号化されているため、図１６に示すように、認証装置３０Ｂ内に格納されている秘密鍵ＳＫにより復号される。

【０１０６】

そして、認証装置３０Ｂでは、復号された２つのハッシュ値Ａ、Ｂが比較されて、その比較結果に基づいた認証結果が制御装置２０Ｂに送信される。つまり、ユーザＢがユーザＡから受信した文書データが真正なものである場合、ハッシュ値Ａとハッシュ値Ｂとは同じ値となっているため、比較した２つのハッシュ値Ａ、Ｂが一致した場合には、その判定対象の文書データは、ユーザＡからの真正なものである旨の認証結果が返信される。また、比較した２つのハッシュ値Ａ、Ｂが一致しなかった場合には、その判定対象の文書データは、ユーザＡからのものではなく、途中で改ざんされた可能性がある不正なものである旨の認証結果が返信される。

【０１０７】

本実施形態の分散認証システムでは、認証装置３０内においては判定対象情報である文書データを扱わずにハッシュ値のみを扱って認証処理が行われる。そのため、認証装置３

０に対する処理負荷が軽く、大容量のリソースを有する装置を認証装置３０とする必要がない。

【０１０８】

[変形例]

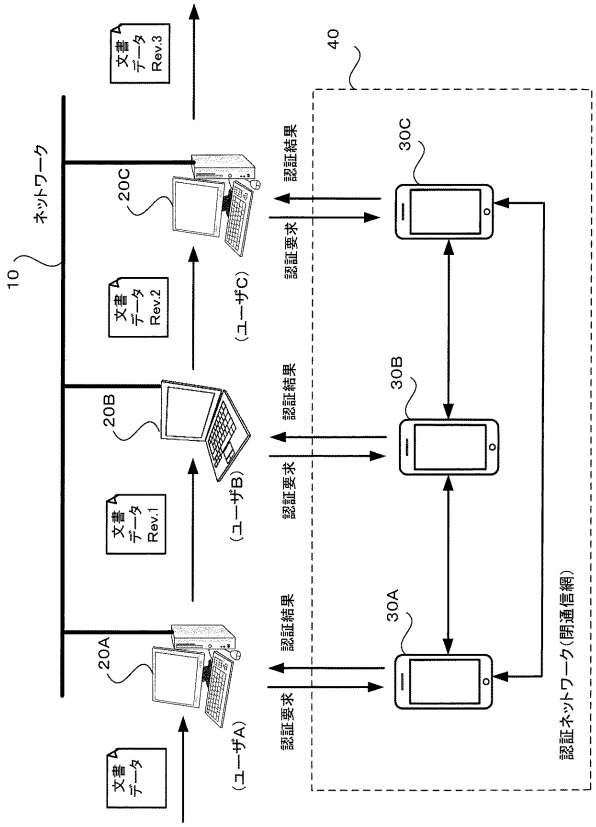
上記実施形態では、複数の制御装置間で文書データの送受信を行う場合を用いて説明したが、本発明はこれに限定されるものではなく、電子マネーのトランザクション、利用履歴等の文書データ以外の判定対象情報を複数の制御装置間で送受信するような場合でも同様に本発明を適用することができるものである。

【符号の説明】

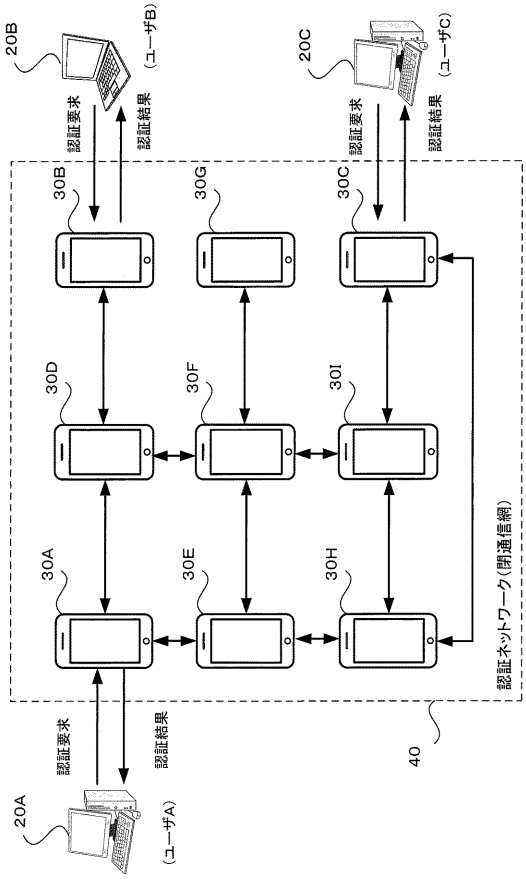
【０１０９】

１０　ネットワーク
１１　ＣＰＵ
１２　メモリ
１３　記憶装置
１４　通信インタフェース（ＩＦ）
１５　ユーザインタフェース（ＵＩ）装置
１６　制御バス
２０、２０Ａ～２０Ｃ　制御装置（データフロー制御装置）
２１　制御部
２２　ハッシュ値算出部
２３　暗号化部
２４　公開鍵格納部
２５　通信部
３０、３０Ａ～３０Ｉ　認証装置
３１　制御部
３２　暗号化／復号部
３３　鍵ペア格納部
３４　秘密鍵格納部
３５　通信部
４０　認証ネットワーク
４１　ＣＰＵ
４２　メモリ
４３　記憶装置
４４　通信インタフェース（ＩＦ）
４５　ユーザインタフェース（ＵＩ）装置
４６　制御バス

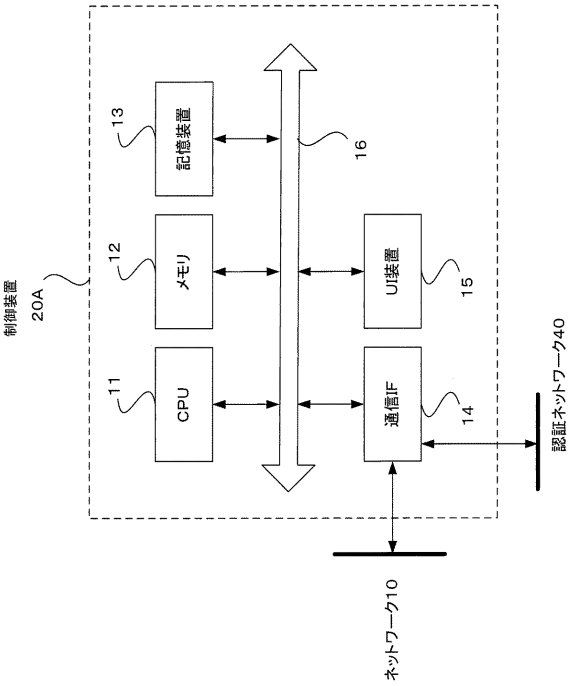
【図１】


10
ネットワーク
文書データ
文書データ Rev.1
文書データ Rev.2
文書データ Rev.3
20A
20B
20C
（ユーザA）
（ユーザB）
（ユーザC）
30A
30B
30C
40
認証要求
認証結果
認証ネットワーク（閉通信網）

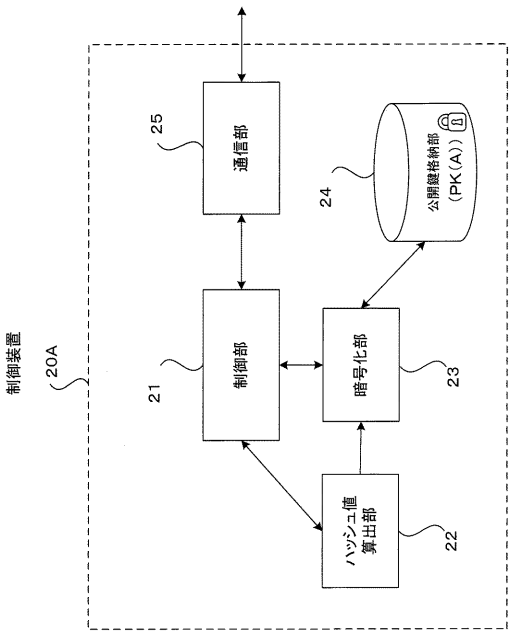
【図２】


20A
20B
20C
（ユーザA）
（ユーザB）
（ユーザC）
30A
30B
30C
30D
30E
30F
30G
30H
30I
40
認証要求
認証結果
認証ネットワーク（閉通信網）

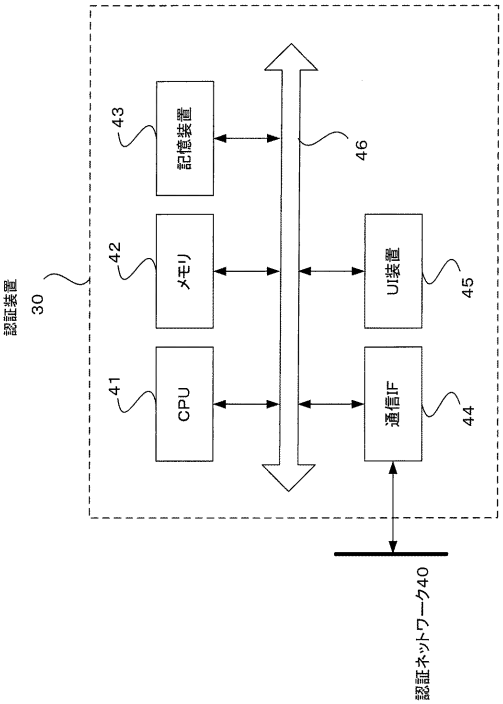
【図３】


制御装置
20A
11
CPU
12
メモリ
13
記憶装置
14
通信IF
15
UI装置
16
ネットワーク10
認証ネットワーク40

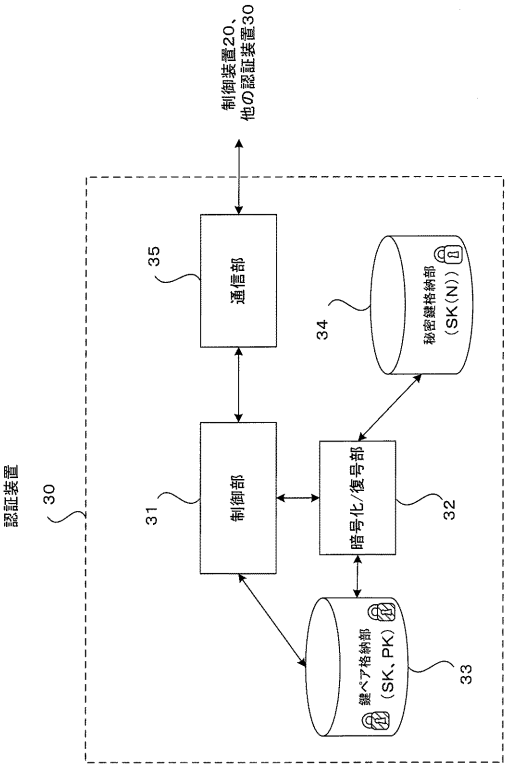
【図４】


制御装置
20A
21
制御部
22
ハッシュ値算出部
23
暗号化部
24
公開鍵格納部
（PK(A)）
25
通信部

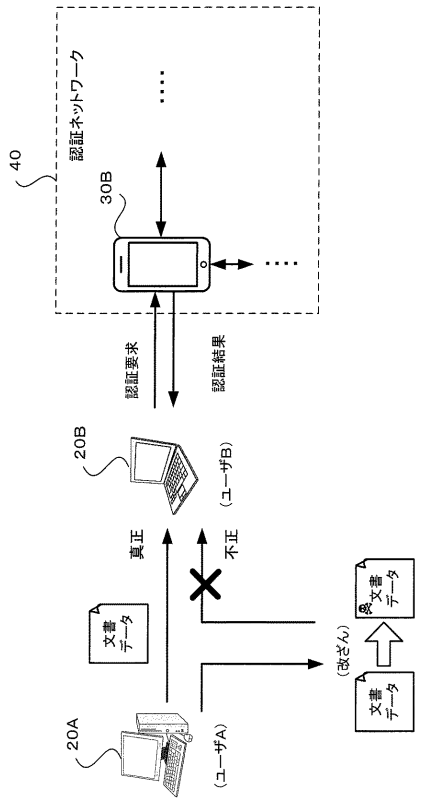
【図５】


認証装置
30
CPU
41
メモリ
42
記憶装置
43
通信IF
44
UI装置
45
46
認証ネットワーク40

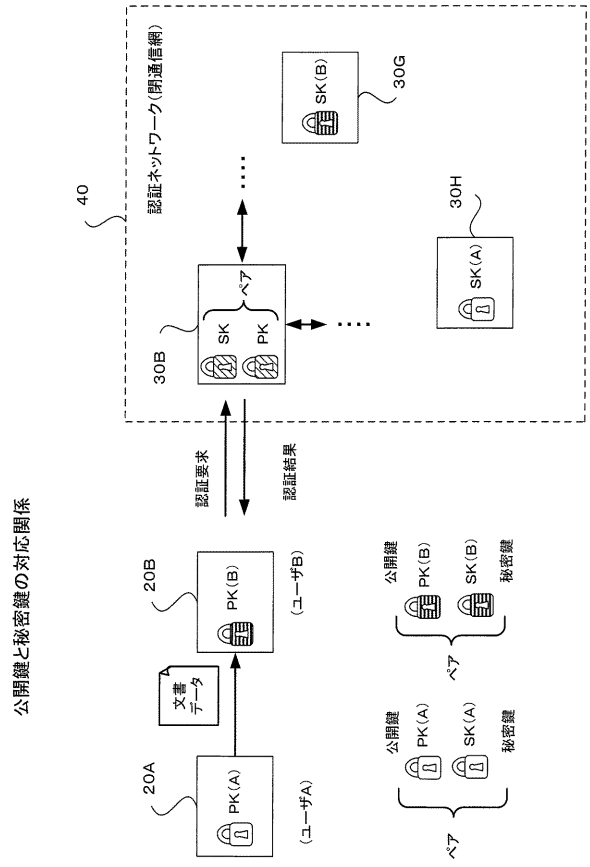
【図６】


制御装置20、
他の認証装置30
認証装置
30
通信部
35
制御部
31
暗号化/復号部
32
秘密鍵格納部
（SK(N)）
34
鍵ペア格納部
（SK、PK）
33

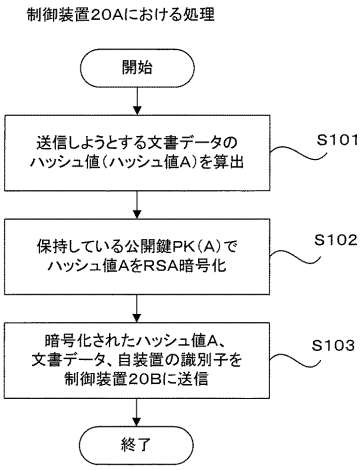
【図７】


40
認証ネットワーク
30B
認証要求
認証結果
20B
（ユーザB）
真正
不正
文書データ
20A
（ユーザA）
（改ざん）
文書データ

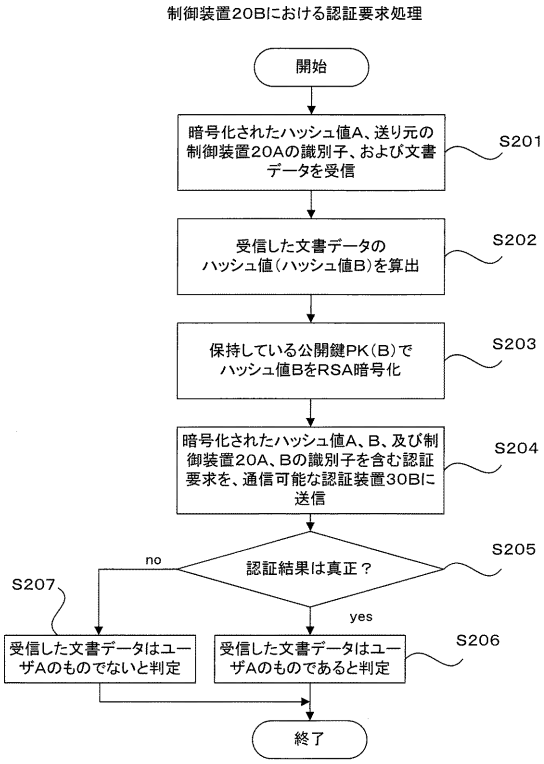
【図８】


公開鍵と秘密鍵の対応関係
40
認証ネットワーク(閉通信網)
30B
SK
PK
ペア
SK(B)
30G
30H
SK(A)
認証要求
認証結果
20B
PK(B)
（ユーザB）
文書データ
20A
PK(A)
（ユーザA）
公開鍵
PK(B)
SK(B)
秘密鍵
ペア
公開鍵
PK(A)
SK(A)
秘密鍵
ペア

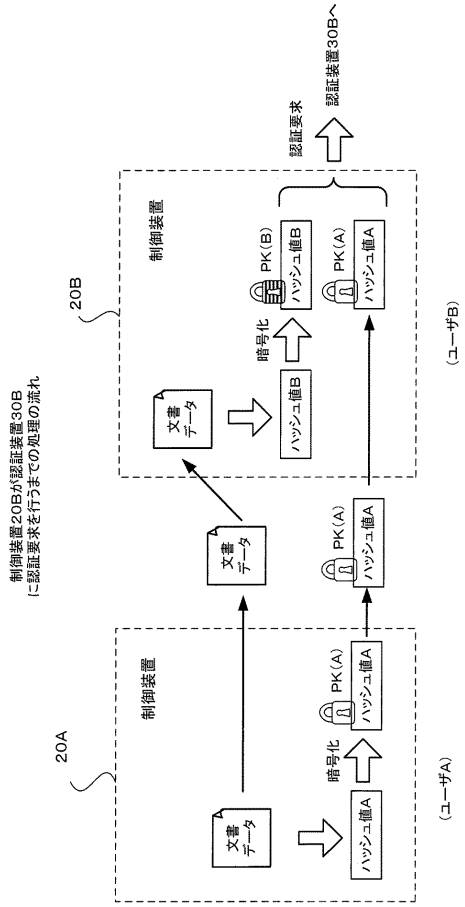
【図９】



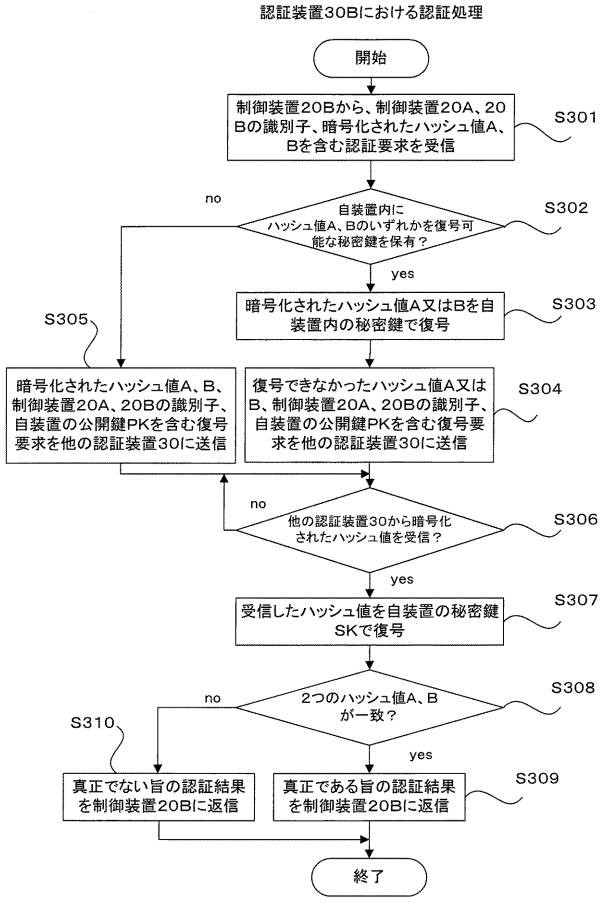
【図１０】



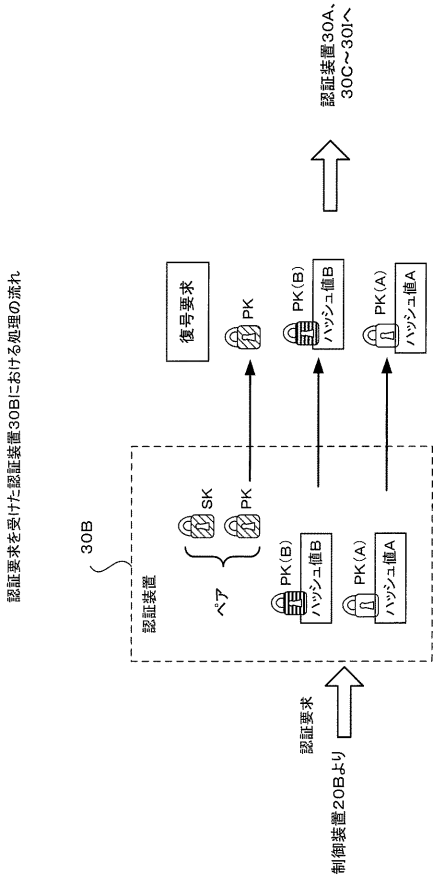
【図１１】



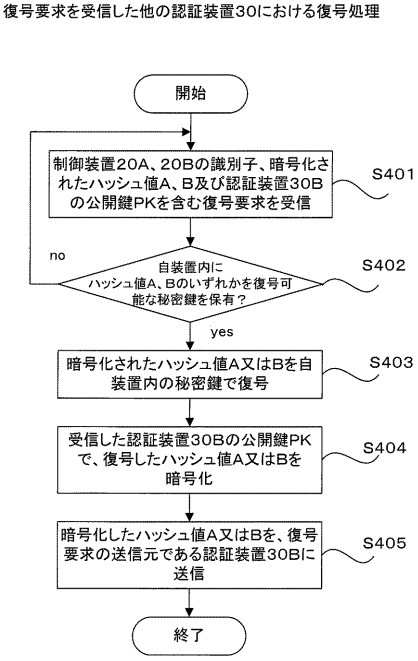
【図１２】



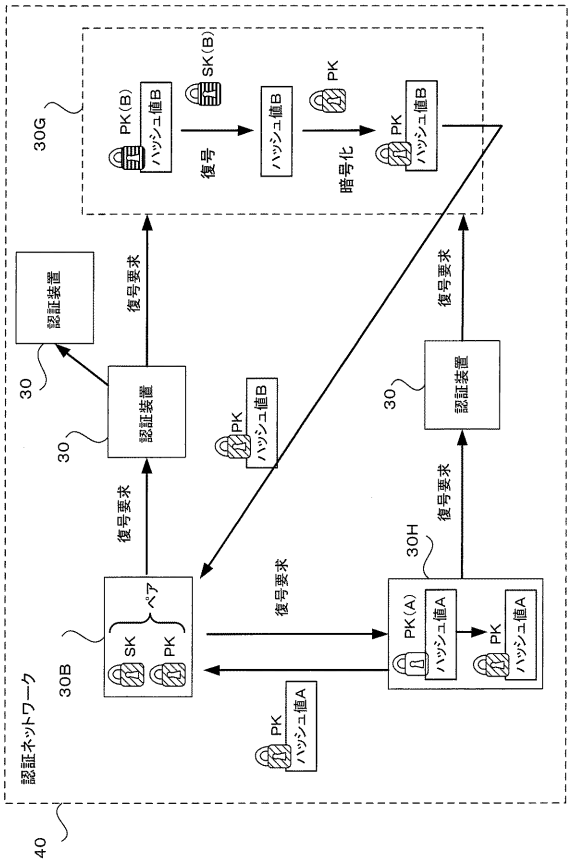
【図１３】



【図１４】



【図１５】



【図１６】