

(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 O L (全 18 頁)

(21) 出願番号	特願2017-181179 (P2017-181179)	(71) 出願人	000005496
(22) 出願日	平成29年9月21日 (2017.9.21)		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

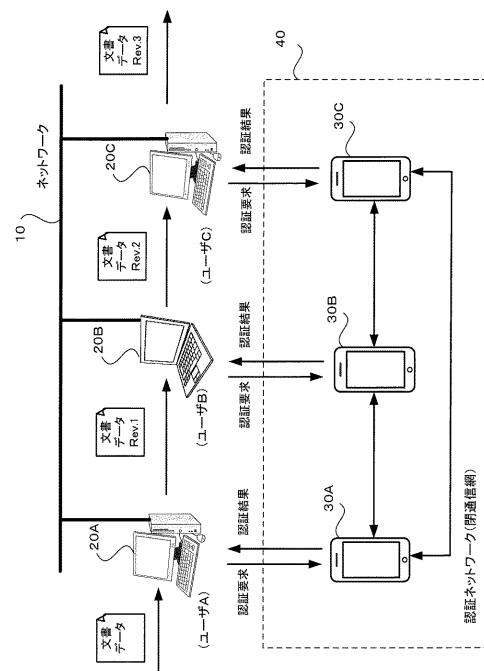
(54) 【発明の名称】 分散認証システムおよびプログラム

(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、

10

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。

20

【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。

30

【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。

40

【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

50

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 3 6 1 0 1 0 6 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のため、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

10

20

30

40

50

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〕

10

20

30

40

50

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。

【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。

10

【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。

20

【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。

30

【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】

40

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

50

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。

10

【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。

20

【0035】

そして、本実施形態の分散認証システムでは、制御装置 20 A～20 B 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。

30

【0037】

例えば、ユーザ A が制御装置 20 A において文書データを更新してユーザ B の制御装置 20 B 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 20 C 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 20 B 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 20 B 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。

40

【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 30 A～30 I 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 20 A～20 C は、それぞれ、認証装置 30 A～30 C とのみ通信可能となっている。

【0040】

50

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】

まず、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。

10

【0043】

制御装置 20Aは、図 3に示されるように、CPU 11、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】

CPU 11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、CPU 11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CPU 11に提供することも可能である。

20

【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。

30

【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。

40

【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

50

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 P K (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 20 A が通信可能なのは認証装置 30 A であるため、制御部 21 は、認証要求を認証装置 30 A 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 P K (A) により暗号化する。

10

【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 30 A 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 P K (A) 、 P K (B) 、・・・に対応する秘密鍵 S K (A) 、 S K (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 20 A は、自装置内に格納されている公開鍵 P K (A) に対応する秘密鍵 S K (A) を、認証装置 30 A ~ 30 I 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。

20

【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、 C P U 41 、メモリ 42 、ハードディスクドライブ (H D D) 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 (I F) 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 (U I) 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。

30

【0057】

C P U 41 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、 C P U 41 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 U S B メモリ等の記憶媒体に格納して C P U 41 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。

40

【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 S K (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 P K により暗号化する処理を行う。

【0061】

50

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】

まず、以下の説明においては、図 7 に示すように、制御装置 20 B が制御装置 20 A 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 20 A (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 20 B 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

10

20

30

40

50

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】

まず、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】

まず、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】

まず、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

10

20

30

40

50

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）。

10

【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】

まず、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）。

20

【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）。

30

【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）。

40

【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

50

信して復号処理を行う際の動作を図 1 4 のフローチャートを参照して説明する。また、この図 1 4 において説明する復号処理の様子を図 1 5 に図示する。

【0097】

認証装置 30 B は、認証ネットワーク 40 内の認証装置 30 B 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 30 B 以外の認証装置 30 では、制御装置 20 A、20 B の識別子、暗号化されたハッシュ値 A、B 及び認証装置 30 B の公開鍵 P K を含む復号要求がそれぞれ受信される（ステップ S 401）。

【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 S K（A）、S K（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 S 402 において n o）。

【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 S K（A）、S K（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 30 G、30 H がこのような復号要求を受信した場合（ステップ S 402 において y e s）、暗号化されたハッシュ値 A、B は、認証装置 30 G、30 H 内に格納されている、制御装置 20 A、20 B が暗号化に用いた公開鍵 P K（A）、P K（B）と対応する秘密鍵 S K（A）、または S K（B）により復号される（ステップ S 403）。

【0101】

つまり、図 1 5 に示されるように、認証装置 30 G では、公開鍵 P K（B）により暗号化されていたハッシュ値 B は、秘密鍵 S K（B）により復号される。また、認証装置 30 H では、公開鍵 P K（A）により暗号化されていたハッシュ値 A は、秘密鍵 S K（A）により復号される。

【0102】

そして、認証装置 30 G、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 30 B の公開鍵 P K で暗号化される（ステップ S 404）。

【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 30 B に返信される（ステップ S 405）。

【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 30 B における動作について図 1 6 を参照して説明する。

【0105】

このようにして認証装置 30 B に返信されてきたハッシュ値 A、B は、いずれも認証装置 30 B の公開鍵 P K により暗号化されているため、図 1 6 に示すように、認証装置 30 B 内に格納されている秘密鍵 S K により復号される。

【0106】

そして、認証装置 30 B 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 20 B 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

10

20

30

40

50

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 3 0 とする必要がある。

【0 1 0 8】

[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】

【0 1 0 9】

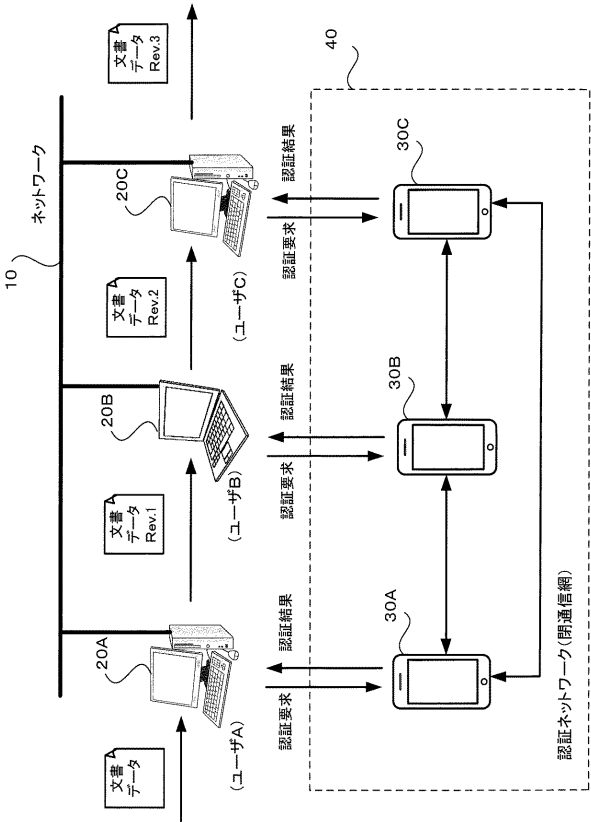
- 1 0 ネットワーク
- 1 1 C P U
- 1 2 メモリ
- 1 3 記憶装置
- 1 4 通信インタフェース (I F)
- 1 5 ユーザインタフェース (U I) 装置
- 1 6 制御バス
- 2 0、2 0 A ~ 2 0 C 制御装置 (データフロー制御装置)
- 2 1 制御部
- 2 2 ハッシュ値算出部
- 2 3 暗号化部
- 2 4 公開鍵格納部
- 2 5 通信部
- 3 0、3 0 A ~ 3 0 I 認証装置
- 3 1 制御部
- 3 2 暗号化 / 復号部
- 3 3 鍵ペア格納部
- 3 4 秘密鍵格納部
- 3 5 通信部
- 4 0 認証ネットワーク
- 4 1 C P U
- 4 2 メモリ
- 4 3 記憶装置
- 4 4 通信インタフェース (I F)
- 4 5 ユーザインタフェース (U I) 装置
- 4 6 制御バス

10

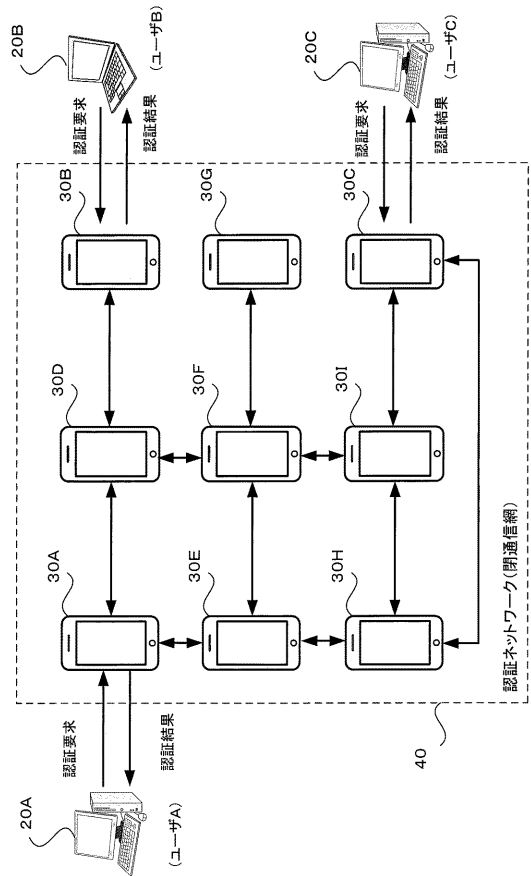
20

30

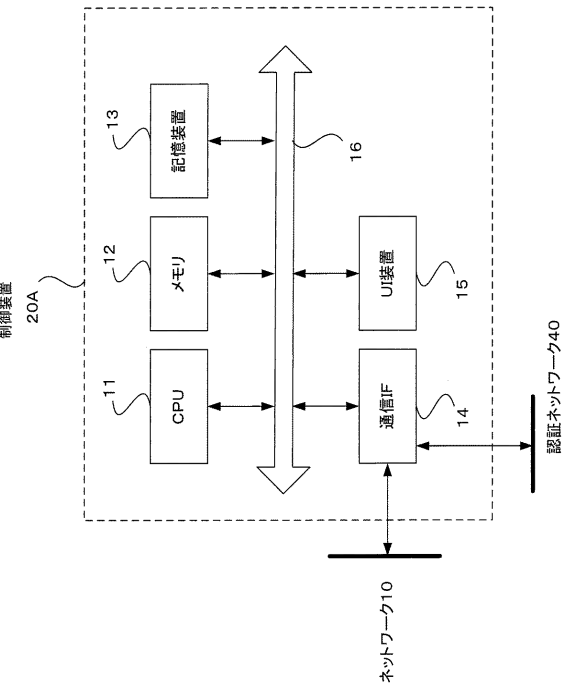
【図 1】



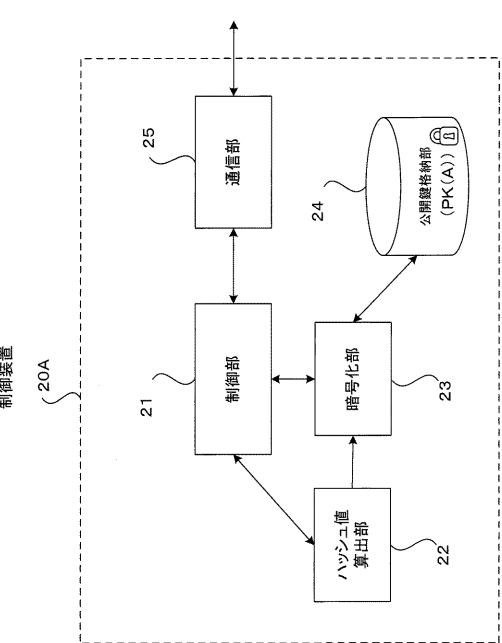
【図 2】



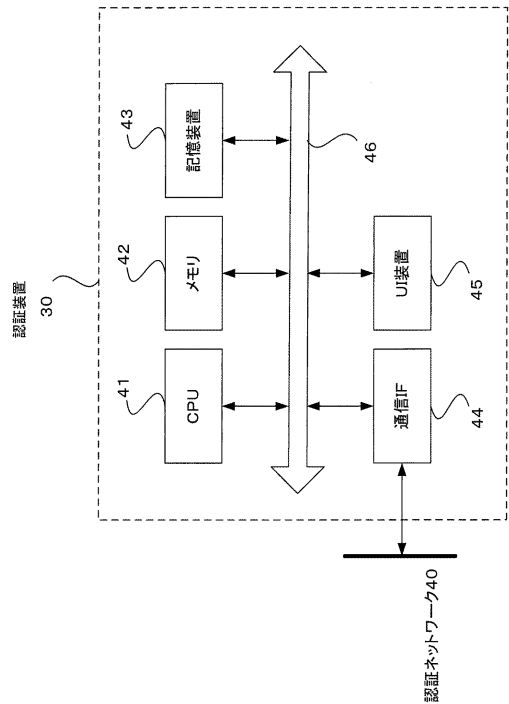
【図 3】



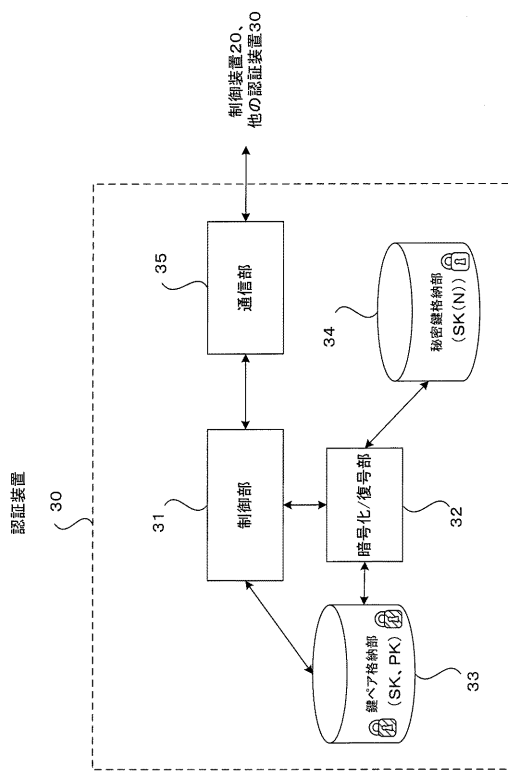
【図 4】



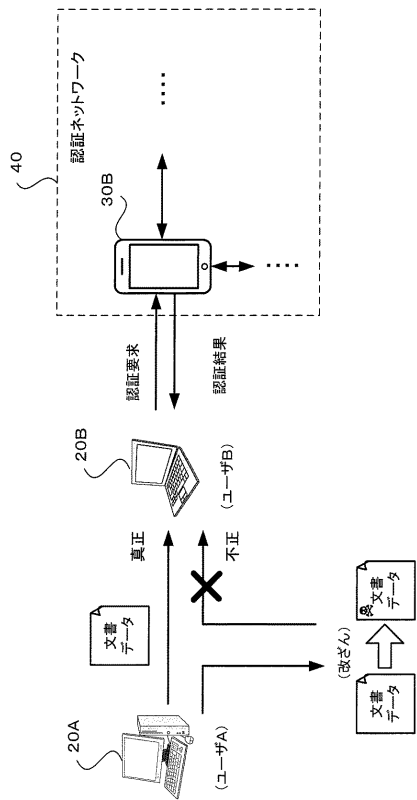
【図 5】



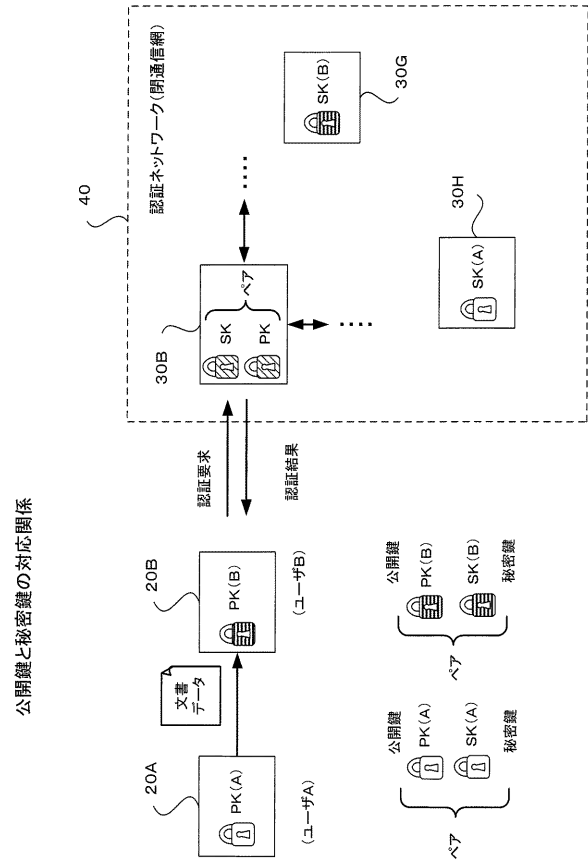
【図 6】



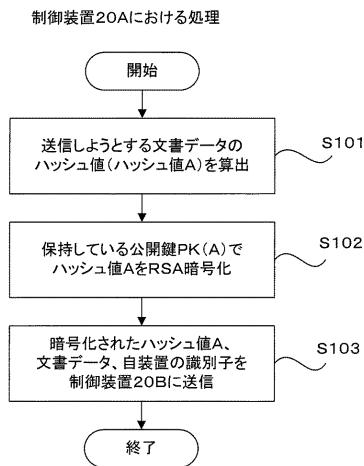
【図 7】



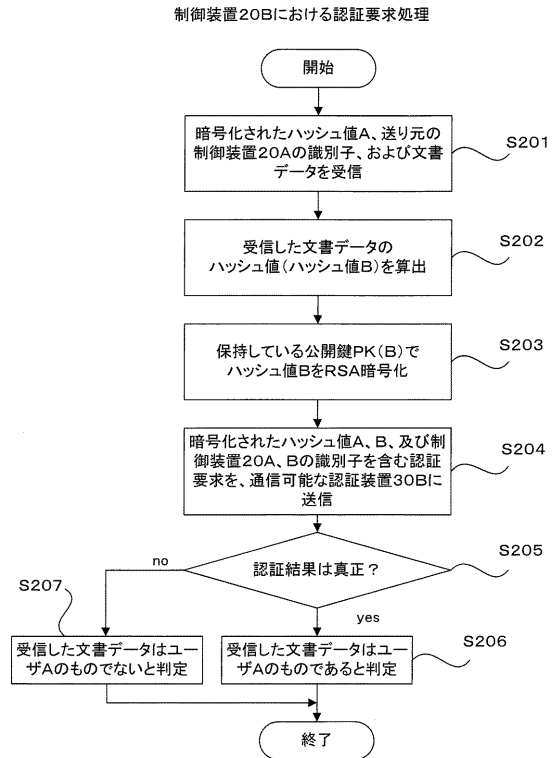
【図 8】



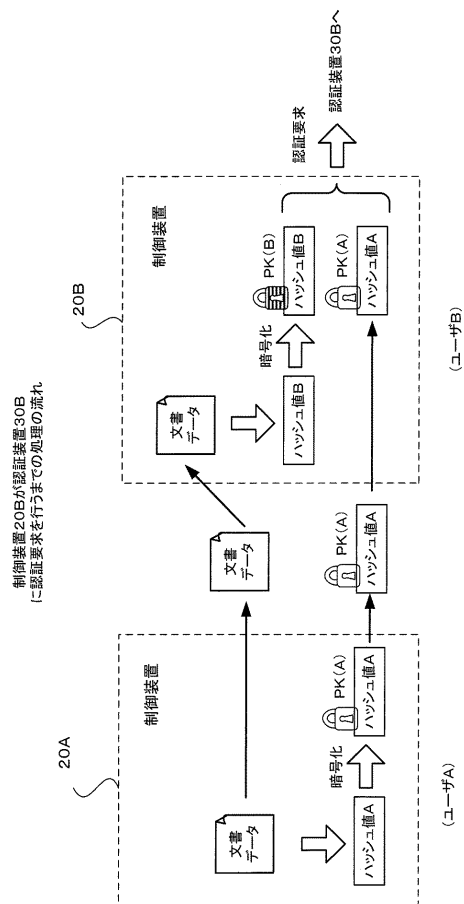
【図 9】



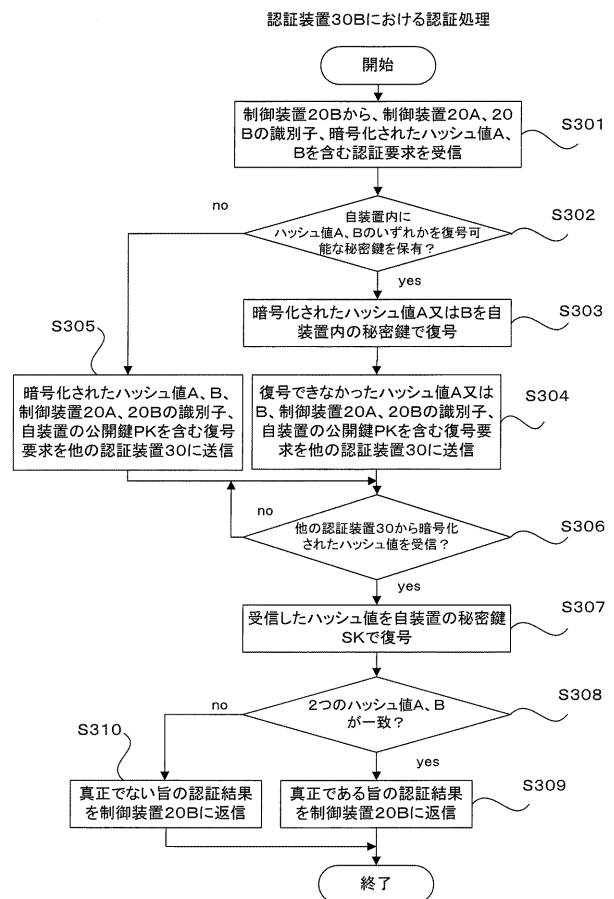
【図 10】



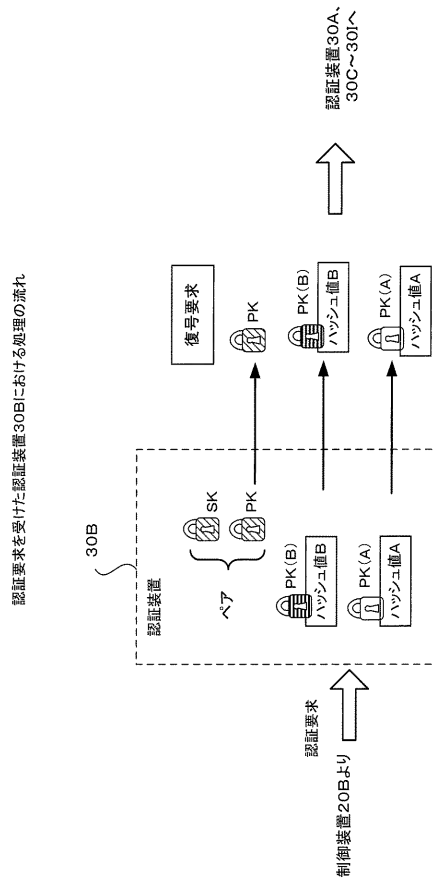
【図 11】



【図 12】

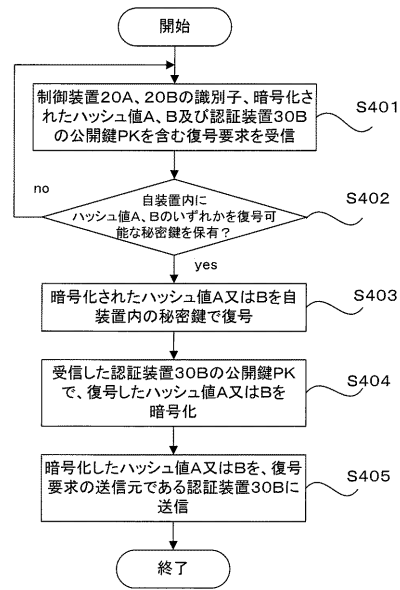


【図 13】

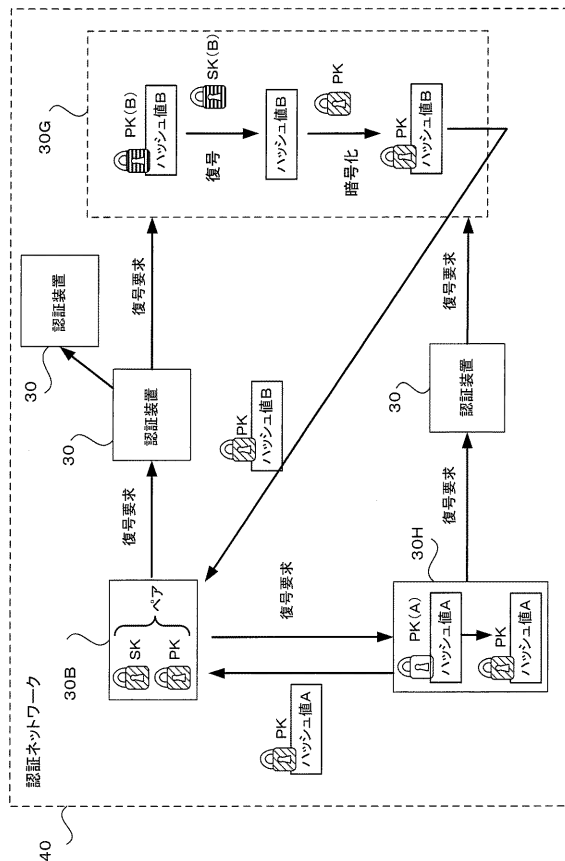


【図 14】

復号要求を受信した他の認証装置30における復号処理



【図 15】



【図 16】

