

(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2013-207376

(P2013-207376A)

(43) 公開日 平成25年10月7日(2013.10.7)

(51) Int. Cl.		F I		テーマコード (参考)		
H04L	9/08	(2006.01)	H04L	9/00	601B	5J104
H04L	9/32	(2006.01)	H04L	9/00	601E	
G09C	1/00	(2006.01)	H04L	9/00	675B	
G06F	21/62	(2013.01)	G09C	1/00	640D	
			G06F	21/24	166E	
審査請求 未請求 請求項の数 9 O L (全 21 頁)						

(21) 出願番号 特願2012-71657 (P2012-71657)
 (22) 出願日 平成24年3月27日 (2012. 3. 27)

(71) 出願人 000003078
 株式会社東芝
 東京都港区芝浦一丁目1番1号
 (74) 代理人 100089118
 弁理士 酒井 宏明
 (74) 代理人 100112656
 弁理士 宮田 英毅
 (72) 発明者 花谷 嘉一
 東京都港区芝浦一丁目1番1号 株式会社
 東芝内
 (72) 発明者 上林 達
 東京都港区芝浦一丁目1番1号 株式会社
 東芝内

最終頁に続く

(54) 【発明の名称】 情報処理装置およびプログラム

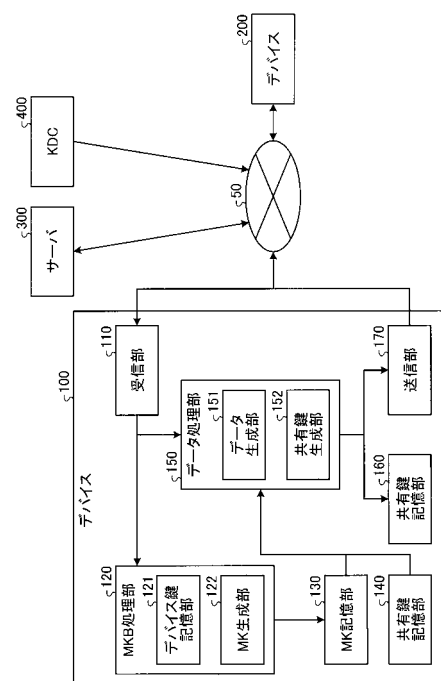
(57) 【要約】 (修正有)

【課題】 安全性と効率を両立した鍵共有方式を実現する

。

【解決手段】 情報処理装置100は、外部装置200とサーバ装置300とに接続される。情報処理装置100は、デバイス鍵記憶部121と、MKB処理部120と、共有鍵生成部152と、を備える。デバイス鍵記憶部121は、デバイス鍵を記憶する。MKB処理部120は、デバイス鍵とメディアキーブロックとからメディア鍵を生成する。共有鍵生成部152は、サーバ装置300から送信される秘密情報とメディア鍵とから、外部装置200との間で共有する共有鍵を生成する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

外部装置とサーバ装置とに接続される情報処理装置であって、
デバイス鍵を記憶するデバイス鍵記憶部と、
前記デバイス鍵とメディアキーブロックとからメディア鍵を生成するMKB処理部と、
前記サーバ装置から送信される秘密情報と前記メディア鍵とから、前記外部装置との間で共有する共有鍵を生成する共有鍵生成部と、
を備える情報処理装置。

【請求項 2】

前記サーバ装置から送信された前記メディアキーブロックを受信する受信部をさらに備え、
前記MKB処理部は、前記デバイス鍵と、前記サーバ装置から受信した前記メディアキーブロックとから前記メディア鍵を生成する、
請求項 1 に記載の情報処理装置。 10

【請求項 3】

前記受信部は、さらに、鍵配布装置から送信された前記メディアキーブロックの署名情報を、前記サーバ装置を介して受信し、
前記MKB処理部は、前記署名情報を用いて前記メディアキーブロックを検証し、検証された前記メディアキーブロックと前記デバイス鍵とから前記メディア鍵を生成する、
請求項 2 に記載の情報処理装置。 20

【請求項 4】

前記メディアキーブロックは、前記サーバ装置とは異なる装置である鍵配布装置により生成され、
前記鍵配布装置から送信された前記メディアキーブロックを受信する受信部をさらに備え、
前記MKB処理部は、前記デバイス鍵と、前記鍵配布装置から受信した前記メディアキーブロックとから前記メディア鍵を生成する、
請求項 1 に記載の情報処理装置。

【請求項 5】

前記サーバ装置との間で事前に共有した事前共有鍵を記憶する共有鍵記憶部と、
前記サーバ装置によって前記事前共有鍵を用いて前記秘密情報を含むデータが暗号化された暗号化情報を、前記共有鍵記憶部に記憶された前記事前共有鍵で復号して前記秘密情報を生成するデータ生成部と、をさらに備え、
前記共有鍵生成部は、生成された前記秘密情報と前記メディア鍵とから、前記外部装置との間で共有する共有鍵を生成する、
請求項 1 に記載の情報処理装置。 30

【請求項 6】

前記サーバ装置との間で事前に共有した事前共有鍵を記憶する共有鍵記憶部と、
前記サーバ装置によって前記事前共有鍵と前記メディア鍵を用いて予め決められた方法で計算される暗号化鍵により前記秘密情報を含むデータが暗号化された暗号化情報を、前記共有鍵記憶部に記憶された前記事前共有鍵と前記メディア鍵より前記予め決められた方法により計算される復号化鍵により復号して前記秘密情報を生成するデータ生成部と、をさらに備え、
前記共有鍵生成部は、生成された前記秘密情報と前記メディア鍵とから、前記外部装置との間で共有する共有鍵を生成する、
請求項 1 に記載の情報処理装置。 40

【請求項 7】

前記秘密情報を用いて暗号化情報を生成するデータ生成部と、
前記暗号化情報を前記外部装置に送信する送信部と、
送信した前記暗号化情報に対して前記外部装置が送信した情報を用いて、前記秘密情報 50

を検証する検証部と、をさらに備え、

前記共有鍵生成部は、前記秘密情報が検証に合格した場合に、前記秘密情報と前記メディア鍵とから、前記共有鍵を生成する、

請求項 1 に記載の情報処理装置。

【請求項 8】

前記データ生成部は、前記メディア鍵と前記秘密情報とを用いて前記暗号化情報を生成する、

請求項 7 に記載の情報処理装置。

【請求項 9】

外部装置とサーバ装置とに接続されるコンピュータを、

デバイス鍵とメディアキーブロックとからメディア鍵を生成する M K B 処理部と、

前記サーバ装置から送信される秘密情報と前記メディア鍵とから、前記外部装置との間で共有する共有鍵を生成する共有鍵生成部、

として機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明の実施形態は、情報処理装置およびプログラムに関する。

【背景技術】

【0002】

事前共有鍵に基づく認証付鍵交換は、プロトコル実行中の処理は効率的であるが、各デバイス内での共有鍵の管理コストが増大するという問題がある。このような問題を回避する方法として、信頼できるサーバを導入する技術が知られている。この技術では、まず各デバイスとそのサーバが相互に認証を行い、安全に事前共有鍵を共有しておく。そして、ある 2 つのデバイス間で認証付鍵交換を行うにあたって、そのサーバがデバイスの認証と鍵発行に用いるデータを配布する。このような技術として、K e r b e r o s 認証などが知られている。

【先行技術文献】

【非特許文献】

【0003】

【非特許文献 1】D. Harkins et al、"RFC2409、The Internet Key Exchange (IKE)" [online]、November 1998、retrieved from the Internet: <URL: <http://www.ietf.org/rfc/rfc2409.txt>>

【非特許文献 2】C.Neuman, T.Yu, S.Hartman, and K.Raeburn、"RFC4120、The Kerberos Network Authentication Service (V5)" [online]、July 2005、retrieved from the Internet: <URL: <http://www.ietf.org/rfc/rfc4120.txt>>

【発明の概要】

【発明が解決しようとする課題】

【0004】

しかしながら、従来の K e r b e r o s 認証のように、サーバを介した事前共有鍵型の認証付鍵交換方式では、デバイス間の通信のための共有鍵の生成、認証、および通信の可否の判断の全てを信頼できるサーバに委ねている。さらに、そのようなサーバはデバイス間の通信に使う共有鍵を知ることができるため、サーバが全ての通信を盗聴できるという問題があった。すなわち、サーバの信頼性に大きく依存したシステム構成となっている。

【課題を解決するための手段】

【0005】

実施形態の情報処理装置は、外部装置とサーバ装置とに接続される。情報処理装置は、デバイス鍵記憶部と、M K B 処理部と、共有鍵生成部と、を備える。デバイス鍵記憶部は、デバイス鍵を記憶する。M K B 処理部は、デバイス鍵とメディアキーブロックとからメディア鍵を生成する。共有鍵生成部は、サーバ装置から送信される秘密情報とメディア鍵

10

20

30

40

50

とから、外部装置との間で共有する第1共有鍵を生成する。

【図面の簡単な説明】

【0006】

【図1】第1の実施形態にかかるシステムのブロック図。

【図2】KDCのブロック図。

【図3】デバイスのブロック図。

【図4】サーバのブロック図。

【図5】MKB配布処理のシーケンス図。

【図6】鍵共有処理のシーケンス図。

【図7】変形例4の鍵共有処理のシーケンス図。

【図8】第2の実施形態における鍵共有処理のシーケンス図。

【図9】第3の実施形態における鍵共有処理のシーケンス図。

【図10】変形例13における鍵共有処理のシーケンス図。

【図11】変形例14における鍵共有処理のシーケンス図。

【図12】第1から第3の実施形態にかかる装置のハードウェア構成図。

【発明を実施するための形態】

【0007】

以下に添付図面を参照して、この発明にかかる情報処理装置の好適な実施形態を詳細に説明する。

【0008】

(第1の実施形態)

上記のように、従来の方法は、サーバの信頼性に大きく依存したシステム構成となっている。そのため、サーバを安全に構築および運用せねばならず、大きなコストが必要となるだけでなく、屋外など、物理的解析のような強力な攻撃の対象となりうる場所にサーバを設置できないというシステム構成上の問題があった。

【0009】

そこで、第1の実施形態にかかる情報処理装置を含むシステムは、サーバを利用したデバイス間の鍵共有方法を適用しつつ、通信の可否を判断する機能をサーバから分離し、サーバへの依存度を軽減する。これにより、サーバの構築および運用コストの低減を実現する。本システムでは、MKBの更新によって、情報漏洩が生じていないデバイスにのみ共通のメディア鍵を配布する。これにより、サーバが通信の可否を判断することなく、情報漏洩を防ぐ。

【0010】

本実施形態にかかる情報処理装置（デバイス）を含むシステムでは、所定の鍵共有方式で用いる共有鍵を算出するために適したメディア鍵を導出（生成）できるMKB（メディアキーブロック）を用いる。そして、このMKBを鍵配布装置（以下、KDC（Key Distribution Center）という。）から各デバイスに配布する。各デバイスは、MKBと自装置のデバイス鍵とからメディア鍵を生成し、生成したメディア鍵とサーバより配布されたデータを正しく処理すると得られるデータとを用いて、他のデバイス（外部装置）との間の通信に用いる共有鍵を生成する。

【0011】

このため、デバイス間での通信にあたって、従来のように、サーバが通信の可否を判断する必要がない。すなわち、KDCが通信を認めるデバイスのグループ毎に共通のMKBを生成し、それらを任意の方法で配布することで、デバイス間の通信の可否を制御する。サーバは、デバイスからの要求に対して、デバイス間で共有鍵を生成するための情報の発行のみを行えばよい。また、あるデバイスの通信を認めない場合は、当該デバイスが正しく処理できないように更新した共通のMKBをKDCが再配布するだけでよい。すなわち、KDCがMKBを配布するだけで、各デバイスが属するグループの更新が可能であり、かつ、デバイスの通信の可否を容易に制御できる。KDCにより、あるデバイスが処理できないMKBが配布されたとき、そのデバイスまたはそのデバイスが備えるデバイス鍵は

10

20

30

40

50

無効化されたという。

【0012】

図1は、第1の実施形態にかかるシステムの構成の一例を示すブロック図である。図1に示すように、本実施形態のシステムは、情報処理装置としての複数のデバイス100、200と、サーバ装置としてのサーバ300と、KDC400とが、ネットワーク50で接続された構成となっている。ネットワーク50は、インターネットなどのあらゆるネットワーク形態を適用できる。

【0013】

デバイス100、200は2つに限られるものではなく、3以上のデバイス100、200を備えるように構成してもよい。また、サーバ300は1つに限られるものではなく、2以上のサーバ300を備えるように構成してもよい。また、KDC400は1つに限られるものではなく、2以上のKDC400を備えるように構成してもよい。

【0014】

KDC400は、メディア鍵の生成、MKBの生成、およびMKBの配布などを行う。図2は、KDC400の構成例を示すブロック図である。図2に示すように、KDC400は、受信部410と、送信部440と、MKB生成部420と、鍵記憶部430と、を備えている。

【0015】

受信部410は、デバイス100、200やサーバ300などの装置から各種データを受信する。送信部440は、デバイス100、200やサーバ300などの装置に対して各種データを送信する。例えば、送信部440は、MKB生成部420により生成されたMKBをデバイス100、200に送信する。なお、デバイス100、200にMKBを入力する方法はこれに限られるものではない。例えば、MKBを記憶した記憶媒体を介してデバイス100、200にMKBを入力するように構成してもよい。また、サーバ300が送信するデータにMKBを加えて入力するように構成してもよい。

【0016】

鍵記憶部430は、デバイス100、200に割り当てられるデバイス鍵を記憶する。鍵記憶部430は、MKB方式における、すべてのデバイス鍵を記憶する。

【0017】

MKB生成部420は、このデバイス鍵を用いてMKBを作成する。MKBの生成方法は、CS (Complete Sub-tree) 方式、SD (Subset Difference) 方式およびLKH (Logical Key Hierarchy) 方式などのあらゆる方法を適用できる。

【0018】

KDC400には、公開情報として、署名検証用の公開鍵KPが与えられている。KDC400は、KDC400だけが知る秘密の情報として、公開鍵KPに対する秘密鍵KSを保持している。公開鍵KPと秘密鍵KSは、例えば、楕円曲線を用いたデジタル署名の公開鍵と秘密鍵を用いることができる。

【0019】

図1に戻る。デバイス100、200には、少なくとも1つのデバイス鍵が割り当てられている。KDC400は、MKBのメディア鍵として、所定の長さ以上のビット列xを与える。xはKDC400が選んだビット列である。以下では、ビット列xをメディア鍵xという。

【0020】

MKBを受信後、デバイス100、200は、当該デバイス100に割り当てられているデバイス鍵によってMKBを処理し、メディア鍵xを取得して、MK記憶部130に保存する。この際、当該デバイス100がMKBによって無効化されている場合、当該デバイス100はMKBを正しく復号処理することができず、メディア鍵xを正しく取得することはできない。

【0021】

デバイス100、200は、サーバ300との間で共有する事前共有鍵を保持している。例えば、デバイス100とサーバ300とは、共に事前共有鍵psk1を保持している。デバイス100、200、および、サーバ300は、予め、PKINITのような公開鍵暗号系を利用した認証付鍵交換などを用いることで、このような事前共有鍵psk1を共有することができる。

【0022】

デバイス100は、受信部110と、MKB処理部120と、MK記憶部130と、共有鍵記憶部140と、データ処理部150と、共有鍵記憶部160と、送信部170と、を備えている。

【0023】

受信部110は、デバイス200やサーバ300などの装置から各種データを受信する。なお、デバイス200が、デバイス100にとっての外部装置に相当する。例えば、受信部110は、サーバ300が送付した暗号文やKDC400が送付したMKBなどを受信する。受信部110は、受信したデータをMKB処理部120やデータ処理部150に送る。

【0024】

MKB処理部120は、デバイス100のデバイス鍵を格納（記憶）する。例えば、MKB処理部120は、受信部110よりMKBを受け取る。デバイス100のデバイス鍵が無効化されていない場合、MKB処理部120は、MKBからメディア鍵xを生成できる。MKB処理部120は、生成したメディア鍵xをMK記憶部130に送る。

【0025】

MK記憶部130は、MKB処理部120からメディア鍵xを受け取り、保存する。そして、データ処理部150からの要求に応じて、保存しているメディア鍵xをデータ処理部150に送る。

【0026】

共有鍵記憶部140は、デバイス100とサーバ300との間で事前に共有された共有鍵（以下、事前共有鍵K10とする）を保存する。事前に事前共有鍵K10を共有する方法は特に限定されておらず、公開鍵暗号を用いる方法や、ネットワーク50を利用せずメディア等で直接共有するなど、事前に定められたあらゆる手段を用いてよい。

【0027】

データ処理部150は、デバイス200との間で共有する共有鍵（共有鍵2）を生成するための各種データ処理を実行する。例えば、データ処理部150は、サーバ300から受信したデータを受信部110から受け取り、メディア鍵xをMK記憶部130から受け取り、事前共有鍵K10を共有鍵記憶部140から受け取る。データ処理部150は、受け取ったデータを用いて、サーバ300またはデバイス200に送付するデータを生成する。データ処理部150は、デバイス200との通信に用いる共有鍵2を生成する。

【0028】

共有鍵記憶部160は、データ処理部150より共有鍵2を受け取り、保存する。

【0029】

送信部170は、デバイス200やサーバ300などの装置に対して各種データを送信する。例えば、送信部170は、データ処理部150より受け取ったデータを、サーバ300またはデバイス200に送付する。

【0030】

MKBの偽造を防止するために、MKB処理部120がMKBの署名を確認するように構成してもよい。この場合、例えば、KDC400は、MKBの正当性を示すために秘密鍵KSを用いてMKBに対応するデジタル署名を生成してMKBと共に送信する。MKB処理部120は、KDC400の公開鍵KPを記憶しておき、公開鍵KPを用いてMKBの署名を確認する。

【0031】

また、デバイスに送付するMKBのデータサイズを抑えるために、KDC400は、デ

10

20

30

40

50

バイスをいくつかのグループに分類して管理するように構成してもよい。この場合、各デバイスは、例えば木構造で分類されたデバイス鍵のリーフに当たる番号、または、デバイス固有のIDなどで自分の属するグループをKDC400に伝える。KDC400は、そのグループに対応するMKBの一部とそれに対応する署名を送付する。この場合、MKBに対する署名は、各グループに対応するMKB毎に作成する。

【0032】

また、MKB処理部120は、MK記憶部130やデータ処理部150を通じるなどして、送信部170に対してMKBのバージョン番号を送るようにしてもよい。MKBのバージョン番号は、MKBに付随する順序を持つデータである。デバイス100は、デバイス200と鍵共有処理を行う前に、バージョン番号を交換するようにしてもよい。その場合、デバイス100またはデバイス200は、バージョンが古い相手とは鍵交換を行わない。また、デバイス100とデバイス200は、鍵共有後にデータ交換を行い、デバイス100とデバイス200間で共有鍵が正しく共有できたことの確認を行うようにしてもよい。

10

【0033】

次に、MKB処理部120の詳細な構成例を説明する。図1に示すように、MKB処理部120は、デバイス鍵記憶部121と、MK生成部122と、を備えている。

【0034】

デバイス鍵記憶部121は、デバイス100に割り当てられているデバイス鍵を記憶する。MK生成部122は、MKBを読み取り、デバイス鍵記憶部121が記憶するデバイス鍵によってMKBを処理し、メディア鍵xを生成する。MK生成部122は、生成したメディア鍵xをMK記憶部130に送付する。この際、MK記憶部130の代わりにMKB記憶部（図示せず）を設け、必要に応じて都度MKBを処理し、MK生成部122が生成したメディア鍵xをデータ処理部150に直接送るように構成してもよい。

20

【0035】

次に、データ処理部150の詳細な構成例を説明する。図1に示すように、データ処理部150は、データ生成部151と、共有鍵生成部152と、を備えている。

【0036】

データ生成部151は、共有鍵記憶部140より受け取った事前共有鍵K10と受信部110から受け取ったデータとから、送信部170に送るデータと共有鍵生成部152に送るデータとを生成する。

30

【0037】

例えば、データ生成部151は、受信部110から暗号文T1および暗号文T2を受け取る。例えば、暗号文T1は、サーバ300とデバイス100との間で共有されている事前共有鍵K10を用いて秘密情報Kを暗号化した暗号文である。なお、秘密情報Kとは、共有鍵の生成のために用いられる情報であり、サーバ300により生成される。暗号文T2は、サーバ300とデバイス200との間で共有されている事前共有鍵を用いて秘密情報Kを暗号化した暗号文である。この場合、データ生成部151は、事前共有鍵K10を用いて暗号文T1を復号して秘密情報Kを得て、共有鍵生成部152に秘密情報Kを送る。データ生成部151は、送信部170を通じてデバイス200に暗号文T2を送る。

40

【0038】

共有鍵生成部152は、MK記憶部130より受け取ったメディア鍵xと、データ処理部150から受け取ったデータとから、共有鍵2を算出する。データ処理部150から秘密情報Kを受け取った場合、共有鍵生成部152は、秘密情報Kとメディア鍵xに対して、予め定められた処理を適用し、共有鍵2を算出する。

【0039】

なお、共有鍵2の算出には、予め定められた暗号学的に安全なハッシュ関数Hや疑似ランダム関数などを用いてもよい。

【0040】

また、上記例では、メディア鍵xおよび秘密情報Kという2つの変数を入力して共有鍵

50

2を算出する例を説明したが、2以上の変数を入力して共有鍵2を算出してもよい。

【0041】

なお、上記各記憶部（デバイス鍵記憶部121、MK記憶部130、共有鍵記憶部140、共有鍵記憶部160）は、HDD（Hard Disk Drive）、光ディスク、メモリカード、RAM（Random Access Memory）などの一般的に利用されているあらゆる記憶媒体により構成することができる。

【0042】

次に、デバイス200の構成例について説明する。図3は、デバイス200の構成例を示すブロック図である。図3に示すように、デバイス200は、受信部210と、MK B処理部220と、MK記憶部230と、共有鍵記憶部240と、データ処理部250と、共有鍵記憶部260と、送信部270と、を備えている。

10

【0043】

デバイス100とデバイス200では、データ処理部250内のデータ生成部251の機能が、デバイス100のデータ生成部151と異なる。その他の受信部210、MK B処理部220、MK記憶部230、共有鍵記憶部240、共有鍵記憶部260、および、送信部270の機能は、それぞれデバイス100の、受信部110、MK B処理部120、MK記憶部130、共有鍵記憶部140、共有鍵記憶部160、および、送信部170と同様であるため説明を省略する。

【0044】

先の例のように、デバイス200は、デバイス100より暗号文T2を受け取ったら、データ生成部251に送る。データ生成部251は、例えば、サーバ300との間で共有されている事前共有鍵を用いて暗号文T2を復号して秘密情報Kを取得して共有鍵生成部252に送る機能、および、秘密情報Kを算出したことを示すデータを計算して、このデータを送信部270に送る機能を備えている。

20

【0045】

秘密情報Kを算出したことを示すデータは、単純な真理値、予めデバイス100より指定された文書に対する秘密情報Kを用いたメッセージ認証コード、および、秘密情報Kを用いた暗号文など、あらゆるデータを用いることができる。

【0046】

次に、サーバ300の構成例について説明する。図4は、サーバ300の構成例を示すブロック図である。図4に示すように、サーバ300は、受信部310と、共有鍵記憶部320と、データ処理部330と、送信部340と、を備えている。

30

【0047】

受信部310は、デバイス100、200などの装置から各種データを受信する。

【0048】

共有鍵記憶部320は、デバイス100、200と何らかの手段で事前に共有した事前共有鍵を保存する。

【0049】

データ処理部330は、受信部310よりデータを受け取ると、そのデータに応じて共有鍵記憶部320より適切な事前共有鍵を読み出し、読み出した事前共有鍵を用いて出力データを算出し、送信部340に送る。例えば、データ処理部330は、読み出した事前共有鍵を用いて秘密情報Kを暗号化した暗号文を出力データとして生成する。

40

【0050】

次に、このように構成された本実施形態にかかるKDC400と、デバイス100、200によるMK B配布処理について図5を用いて説明する。図5は、本実施形態におけるMK B配布処理の全体の流れを示すシーケンス図である。

【0051】

まず、KDC400のMK B生成部420は、デバイスのうち通信を許可しないデバイスを特定する情報（リポーク機器情報）とデバイス鍵とを用いてMK Bを生成する（ステップS101）。そして、KDC400は、生成したMK Bに対して、秘密鍵KSを用い

50

てMKBの署名S i gを生成する（ステップS 1 0 2）。K D C 4 0 0の送信部4 4 0は、MKBと生成した署名S i gとをデバイス1 0 0に配布する（ステップS 1 0 3）。

【0 0 5 2】

デバイス1 0 0のMKB処理部1 2 0は、公開鍵K Pを用いてMKBの署名S i gを検証する（ステップS 1 0 4）。署名S i gが正しいことを確認できない場合は、以降の処理を中止する。

【0 0 5 3】

MKB処理部1 2 0は、デバイス鍵記憶部1 2 1に記憶されたデバイス鍵を用いてMKBを処理し、メディア鍵xを生成する（ステップS 1 0 5）。MKB処理が実行できなかった場合、デバイス1 0 0は通信が許可されていないため処理は中止する。

【0 0 5 4】

デバイス1 0 0のMK記憶部1 3 0は、メディア鍵xを保存する（ステップS 1 0 6）。

【0 0 5 5】

デバイス2 0 0などの他のデバイスも同様に、MKBの署名の検証、メディア鍵xの生成、および、生成したメディア鍵xの記憶を各々実行する。

【0 0 5 6】

次に、デバイス1 0 0、デバイス2 0 0、サーバ3 0 0による鍵共有処理について図6を用いて説明する。

【0 0 5 7】

P K I N I Tなど、既存の方法を用いて、サーバ3 0 0とデバイス1 0 0とが事前共有鍵K 1 0を共有しており、サーバ3 0 0とデバイス1 0 0とが事前共有鍵K 2 0を共有しているものとする。また、デバイス1 0 0とデバイス2 0 0は、MKBと各々のデバイス鍵とを用いて、共通のメディア鍵MKを共有しているものとする。

【0 0 5 8】

図6は、本実施形態における鍵共有処理の全体の流れを示すシーケンス図である。以下では、デバイス1 0 0がデバイス2 0 0と通信を行うための鍵共有処理を例に示す。

【0 0 5 9】

まず、デバイス1 0 0は、デバイス1 0 0の識別子I D 1と、デバイス2 0 0の識別子I D 2と、を指定してサーバ3 0 0に送付する（ステップS 2 0 1、ステップS 2 0 2）。

【0 0 6 0】

サーバ3 0 0のデータ処理部3 3 0は、I D 1およびI D 2それぞれに対応する事前共有鍵を共有鍵記憶部3 2 0より読み出す。もし、いずれか一方でも対応する事前共有鍵が記録されていない場合は、以降の処理を中止する。

【0 0 6 1】

サーバ3 0 0のデータ処理部3 3 0は、ランダムに秘密情報Kを選択する（ステップS 2 0 3）。データ処理部3 3 0は、I D 2 | | KをK 1 0で暗号化して暗号文T 1を生成する（ステップS 2 0 4）。また、データ処理部3 3 0は、I D 1 | | KをK 2 0で暗号化し暗号文T 2を生成する（ステップS 2 0 5）。なお、記号「| |」は、データの連結を表す。各データを特定できる方法であれば、連結以外の方法を用いてもよい。

【0 0 6 2】

データ処理部3 3 0は、送信部3 4 0を介して暗号文T 1と暗号文T 2をデバイス1 0 0に送付する（ステップS 2 0 6）。

【0 0 6 3】

デバイス1 0 0のデータ処理部1 5 0は、共有鍵記憶部1 4 0に記憶された事前共有鍵K 1 0を用いて暗号文T 1を復号し、I D 2 'とK 'とを得る（ステップS 2 0 7）。データ処理部1 5 0は、もし、I D 2 ' ≠ I D 2であれば、以降の処理を中止する（ステップS 2 0 8）。

【0 0 6 4】

10

20

30

40

50

次に、データ処理部150は、ランダムにRを選択する（ステップS209）。データ処理部150は、ID1||RをK'で暗号化し、暗号文T3を生成する（ステップS210）。データ処理部150は、送信部170を介して、暗号文T2と暗号文T3とをデバイス200に送付する（ステップS211）。

【0065】

デバイス200のデータ処理部250は、共有鍵記憶部260に記憶された事前共有鍵K20を用いて暗号文T2を復号し、ID1'とK'を得る（ステップS212）。データ処理部250は、暗号文T3をK'で復号してID1'とR'を得る（ステップS213）。データ処理部250は、もし、ID1'≠ID1'であれば、以降の処理を中止する（ステップS214）。 10

【0066】

次に、データ処理部250は、R'をK'で暗号化し暗号文T4を算出する（ステップS215）。データ処理部250は、送信部270を介して、T4をデバイス100に送付する（ステップS216）。

【0067】

次に、共有鍵生成部252が、ハッシュ関数Hを用いて、H(K', MK)を計算し、共有鍵記憶部260に保存する（ステップS219）。H(K', MK)が、デバイス100との間で共有する共有鍵（上述の共有鍵2に相当）として利用される。

【0068】

デバイス100のデータ処理部150は、暗号文T4をK'で復号してR'を得て、R'≠Rならば、以降の処理を中止する（ステップS217）。次に、共有鍵生成部152が、ハッシュ関数Hを用いて、H(K', MK)を計算し、共有鍵記憶部160に保存する（ステップS218）。H(K', MK)が、デバイス200との間で共有する共有鍵（上述の共有鍵2に相当）として利用される。 20

【0069】

サーバ300が手順どおりに発行した暗号文T1および暗号文T2を、各々正しい事前共有鍵K10とK20で復号すると、デバイス100とデバイス200は、秘密情報Kを共有できる。すなわち、K'=K'であるため、デバイス100、200は、K'=K'から生成される共有鍵を正しく共有することができる。また、正しい事前共有鍵（事前共有鍵K10とK20）を持たないデバイスは、共通鍵暗号の安全性より、秘密情報K 30 に関する情報を一切得ることができない。

【0070】

また、サーバ300は、メディア鍵MKを持たないため、デバイス100とデバイス200の間で通信に用いる共有鍵H(K, MK)を算出できない。このため、サーバ300が通信を盗聴しようとしても、デバイス100とデバイス200間の通信の安全性は保証される。

【0071】

また、KDC400、サーバ300、デバイス100、および、デバイス200が個別に不正を行ったとしても、なり済ましや盗聴などの攻撃からシステムを守ることができる。 40

【0072】

（変形例1）

変形例1では、サーバ300もMKBを処理するデバイス鍵を持つ。そして、上述の実施形態では、サーバ300はデバイスと共有する事前共有鍵のみを用いて暗号化を行っていたが、本変形例では、暗号化（図6ではステップS204、ステップS205など）の際にMKBを処理して得られたメディア鍵MKと事前共有鍵を用いる。このようにシステムを構成することで、KDC400は、MKBを更新することでサーバ300の通信の可否を制御することができる。

【0073】

（変形例2）

 50

先のシステムでは、1つのMKBを用いていたが、複数のMKBを用いてもよい。変形例2では、例えば、サーバ300はMKB1とMKB1を処理するデバイス鍵を備える。また、デバイス100、200は、MKB1とMKB1を処理するデバイス鍵、および、MKB2とMKB2を処理するデバイス鍵を各々備える。

【0074】

本変形例のサーバ300は、MKB1を処理して得られるメディア鍵MK1と各デバイスと共有する事前共有鍵で暗号文を生成する。また、本変形例のデバイス100、200は、MKB2を処理して得られるメディア鍵MK2とサーバ300から受信した暗号文とを処理して得られる秘密情報Kから、デバイス間で共有する共有鍵を算出する。

【0075】

このようにシステムを構成することで、サーバ300からの盗聴を防ぎつつ、サーバ300の通信の可否を制御する機能を実現できる。

【0076】

(変形例3)

先のシステムでは、各デバイスは共通のMKBを用いていたが、変形例3では、異なるMKBを用いる。例えば、上述のようにデバイスをグループに分類し、グループごとにMKBを割り当てるように構成することができる。

【0077】

例えば、デバイス100が、MKB1とMKB1を処理するデバイス鍵を備え、デバイス200が、MKB2とMKB2を処理するデバイス鍵を備えるものとする。デバイス100は、MKB1を処理してメディア鍵MK1を得て、デバイス200はMKB2を処理してメディア鍵MK2を得る。以降の処理は、先の実施形態と同じである。

【0078】

この場合、デバイス100とデバイス200は、手順に従っている限り、正しく共有鍵を算出できない。言い換えると、異なるグループに属するデバイス間の通信を防止することができる。各デバイスに異なるメディア鍵MKを配布することで、単一のサーバ300を用いて、複数のグループを安全に管理することができる。

【0079】

(変形例4)

先の実施形態では、各デバイスはKDC400から直接MKBを受信していた。変形例4では、サーバ300から暗号文を受け取る際に、合わせてMKBを受信する。図7は、変形例4の鍵共有処理の全体の流れを示すシーケンス図である。

【0080】

KDC400は、MKBと、MKBの署名Sigと、をサーバ300に送信する（ステップS301）。サーバ300は、デバイス100およびデバイス200との間で、それぞれ事前共有鍵K10およびK20を生成する（ステップS302、ステップS303）。

【0081】

デバイス100は、図6のステップS202と同様にして、デバイス100の識別子ID10と、デバイス200の識別子ID20と、をサーバ300に送付する（ステップS304）。

【0082】

サーバ300のデータ処理部330は、図6のステップS203と同様にして、ランダムに秘密情報Kを選択する（ステップS305）。

【0083】

本変形例では、データ処理部330は、MKBを含むデータを暗号化した暗号文を生成する。例えば、データ処理部330は、K||MKB||SigをK10で暗号化した暗号文、および、ID10||K||MKB||SigをK20で暗号化した暗号文を生成して、送信部340を介してデバイス100に送信する（ステップS306）。

【0084】

10

20

30

40

50

デバイス100では、例えばデータ生成部151が、サーバ300から受信した暗号文を復号することによりMKBを得ることができる。デバイス100のMK生成部122は、得られたMKBを処理してメディア鍵MKを生成する（ステップS307）。次に、データ処理部150は、ランダムにRを選択する（ステップS308）。

【0085】

また、本変形例では、データ処理部150は、MKBを含むデータを暗号化した暗号文を生成する。例えば、データ処理部150は、ID10||K||MKBをK20で暗号化した暗号文、および、ID10||RをKで暗号化した暗号文を生成して、送信部170を介してデバイス200に送信する（ステップS309）。

【0086】

デバイス200では、例えばデータ生成部251が、デバイス100から受信した暗号文を復号することによりMKBを得ることができる。デバイス200のMK生成部222は、得られたMKBを処理してメディア鍵MKを生成する（ステップS310）。データ処理部250は、デバイス100から受信した暗号文を復号してKおよびRを得て、RをKで暗号化した暗号文を、送信部270を介してデバイス100に送信する（ステップS311）。

【0087】

デバイス100、200は、それぞれ、共有鍵 $SK = H(K, MK)$ を算出して（ステップS312、ステップS313）通信に利用する。

【0088】

サーバ300から送信される暗号文は、KDC400で付与されたMKBの署名Sigを含んでいる。このため、デバイス100は、署名Sigによりサーバ300から送信されるMKBを検証することができる。従って、例えばサーバ300内でMKBが改ざんされたとしても、デバイス100で不正なMKBによる処理を回避できる。

【0089】

先に述べたように、KDC400がグループに分割してMKBと署名を生成しておき、MKBと署名の組をサーバ300に送付するように構成してもよい。この場合、サーバ300は、デバイスから受け取った2つのIDに応じて、対応するMKBと署名の組を選択し、送付するようにしてもよい。

【0090】

（変形例5）

先の実施形態では、サーバ300とKDC400とは異なる機器であったが、同一の機器内に、先のサーバ300の機能とKDC400の機能とを備えるように構成してもよい。このように構成することで、耐タンパ技術など物理的解析から保護する技術などを用いて、KDCに相当する機能のみを安全に実現すれば、サーバ300とKDC400の機能を併せ持つ機器であっても、安全にシステムを実現できる。この例では、従来方式と比較し、耐タンパ技術を適用すべき機能が少ないため、実現・運用コストを軽減したり、サーバ300の処理効率を増したりという効果が得られる。

【0091】

（第2の実施形態）

第2の実施形態では、情報処理装置をスマートグリッドに適用した実施形態を説明する。図8は、第2の実施形態における鍵共有処理の全体の流れを示すシーケンス図である。本実施形態では、集約器820が、第1の実施形態のサーバ300に相当する。また、メーター830およびMDMS810が、第1の実施形態のデバイスに相当する。MDMS810およびメーター830は、それぞれ異なるデバイス鍵（デバイス鍵Aおよびデバイス鍵B）が割り当てられている。図8は、集約器820を通じて、メーター830が収集した情報をMDMS810に送付するシステムの例を表している。

【0092】

KDC400は、MKBをMDMS810に送信する（ステップS401）。MDMS810は、MKBを処理してメディア鍵MKを生成する（ステップS402）。KDC4

10

20

30

40

50

00は、MKBを集約器820に送信する（ステップS403）。

【0093】

集約器820は、MDMS810およびメーター830との間で、それぞれ事前共有鍵K20およびK10を生成する（ステップS404、ステップS405）。

【0094】

メーター830は、メーター830の識別子ID10と、MDMS810の識別子ID20と、を集約器820に送付する（ステップS406）。

【0095】

集約器820は、ランダムに秘密情報Kを選択する（ステップS407）。集約器820は、KとMKBを含むデータ（例えば、K || MKBやID20 || K || MKB）をK10で暗号化した暗号文E1、および、Kを含むデータ（例えば、ID10 || KやK）をK20で暗号化した暗号文E2を生成して、メーター830に送信する（ステップS408）。

【0096】

メーター830は、受信した暗号文のうちE1を復号することによりMKBを得ることができる。メーター830は、得られたMKBを処理してメディア鍵MKを生成する（ステップS409）。メーター830は、KおよびMKを用いて共有鍵H（K，MK）を生成できる。

【0097】

メーター830は、ID10 || dataを共有鍵H（K，MK）で暗号化した暗号文E3を生成して、集約器820より受信したID10 || KをK20で暗号化した暗号文E2、および、E3を集約器820に送信する（ステップS410）。なお、「data」は任意の情報を表す。例えば、メーター830は、収集した情報を「data」に含めることができる。

【0098】

集約器820は、受信した暗号文をMDMS810に転送する（ステップS411）。

【0099】

（変形例6）

変形例5では、MKBを含むデータより、E1、E2を作成していたが、MKBは暗号化せずに送付してもよい。また、デバイスに応じて、MKBのうち必要な部分集合のみを添付するようにしてもよい。

【0100】

（変形例7）変形例5では、E1としてK || MKBを暗号化したものと、E2としてID10 || Kを暗号化したものを用いていたが、E1としてRN || K || MKBを暗号化したものと、E2としてRN || Kを暗号化したものを用いてもよい。ただし、RNは集約器820が通信ごとに生成する乱数とする。このように構成することで、メーター830は自身のIDをMDMS810に秘匿したままでデータを安全に送付することができ、MDMS810はIDが秘匿されているがMKBにより通信を許可されているメーターよりデータを安全に受信できる。

【0101】

（変形例8）

第2の実施形態では、KDC400とMDMS810とは異なる機器であったが、同一の機器内に、KDC400の機能とMDMS810の機能とを備えるように構成してもよい。この場合、MDMS810が通信の可否の制御も行う。このように構成することで、KDC400の機能のみを安全に実現することで、通信の可否の制御を安全に実現できる。

【0102】

（変形例9）

第2の実施形態では、KDC400と集約器820とは異なる機器であったが、同一の機器内に、先のKDC400の機能と集約器820の機能とを備えるように構成してもよ

10

20

30

40

50

い。この場合、集約器 820 が通信の可否の制御も行う。このように構成することで、集約器が備える KDC400 以外の機能の安全性が全て破られたとしても、少なくとも KDC400 が安全を保っていれば、通信の可否の制御を安全に実現でき、システムへの被害を抑えることが可能となる。このように、安全に実現すべき機能を絞り込むことが可能となり、実現・運用コストを軽減したり KDC400 の処理効率を増したりという効果が得られる。

【0103】

(第 3 の実施形態)

第 3 の実施形態では、集約器を利用して、複数のメーター同士が通信を行う。図 9 は、第 3 の実施形態における鍵共有処理の全体の流れを示すシーケンス図である。本実施形態では、集約器 920 が、第 1 の実施形態のサーバ 300 に相当する。また、メーター 930 および 940 が、第 1 の実施形態のデバイスに相当する。

10

【0104】

KDC400 は、MKB を集約器 920 に送信する (ステップ S501)。集約器 920 は、メーター 930 およびメーター 940 との間で、それぞれ事前共有鍵 K10 および K20 を生成する (ステップ S502、ステップ S503)。

【0105】

メーター 930 は、メーター 930 の識別子 ID10 と、メーター 940 の識別子 ID20 と、を集約器 920 に送付する (ステップ S504)。

20

【0106】

集約器 920 は、ランダムに秘密情報 K を選択する (ステップ S505)。集約器 920 は、K と MKB を含むデータ (例えば K || MKB や ID20 || MKB || K) を K10 で暗号化した暗号文 E1、および、K と MKB を含むデータ (例えば、ID10 || K || MKB) を K20 で暗号化した暗号文 E2 を生成して、メーター 930 に送信する (ステップ S506)。

【0107】

メーター 930 は、受信した暗号文のうち E1 を復号することにより MKB を得ることができる。メーター 930 は、得られた MKB を処理してメディア鍵 MK を生成する (ステップ S507)。

【0108】

メーター 930 は、ランダムに R を選択する (ステップ S508)。メーター 930 は、ID10 || R を K で暗号化した暗号文 E3 を生成して、集約器 920 より受信した ID10 || K || MKB を K20 で暗号化した暗号文 E2、および、E3 をメーター 940 に送信する (ステップ S509)。

30

【0109】

メーター 940 は、受信した暗号文のうち E2 を復号することにより MKB を得ることができる。メーター 940 は、得られた MKB を処理してメディア鍵 MK を生成する (ステップ S510)。メーター 940 は、受信した暗号文のうち E3 を復号して K および R を得て、R を含むデータを K で暗号化した暗号文 E4 を、メーター 930 に送信する (ステップ S511)。

40

【0110】

メーター 930、メーター 940 は、それぞれ、共有鍵 $SK = H(K, MK)$ を算出して (ステップ S512、ステップ S513) 通信に利用する。

【0111】

(変形例 10)

第 3 の実施形態では、KDC400 とメーター 930 とは異なる機器であったが、同一の機器内に、先の KDC400 の機能とメーター 930 の機能とを備えるように構成してもよい。この場合、メーター 930 が通信の可否の制御も行う。このように構成することで、メーター 940 が備える KDC400 以外の機能の安全性が全て破られたとしても、少なくとも KDC400 が安全を保っていれば、通信の可否の制御を安全に実現でき、シ

50

システムへの被害を抑えることが可能となる。このように、安全に実現すべき機能を絞り込むことが可能となり、実現・運用コストを軽減したりKDC400の処理効率を増したりという効果が得られる。

【0112】

(変形例11)

第3の実施形態では、KDC400と集約器920とは異なる機器であったが、同一の機器内に、先のKDC400の機能と集約器920の機能とを備えるように構成してもよい。この場合、集約器920が通信の可否の制御も行う。このように構成することで、集約器920が備えるKDC400以外の機能の安全性が全て破られたとしても、少なくともKDC400が安全を保っていれば、通信の可否の制御を安全に実現でき、システムへの被害を抑えることが可能となる。このように、安全に実現すべき機能を絞り込むことが可能となり、実現・運用コストを軽減したりKDC400の処理効率を増したりという効果が得られる。

10

【0113】

(変形例12)

第3の実施形態では、ステップS509で送付される暗号文のうちE2とステップS511で送付される暗号文E3は、Kで暗号化されていたが、それぞれ、ステップS512とステップS513で生成されるSKを用いて暗号化し、送付してもよい。

【0114】

(変形例13)

20

図10は、変形例13における鍵共有処理の全体の流れを示すシーケンス図である。本変形例では、メーターの属するグループごとに異なるMKBを用いる。

【0115】

図10の例では、メーター1130が、MKB1を処理するデバイス鍵（デバイス鍵A）を備え、メーター1140が、MKB2を処理するデバイス鍵（デバイス鍵B）を備える。

【0116】

KDC400は、MKB1およびMKB2を集約器1120に送信する（ステップS701）。

【0117】

30

ステップS702～ステップS709は、図9のステップS502～ステップS509と同様である。

【0118】

本変形例では、メーター1140は、MKB1を処理するデバイス鍵Aを備えていないため、メディア鍵MKを正しく取得できない（ステップS710）。

【0119】

メーター1140が、デバイス鍵Bを用いてMKB1を処理して得られるメディア鍵をMK'とする。また、メーター1140が、メディア鍵MK'を用いて生成される共有鍵（H(K, MK'））によりRを暗号化した暗号文をメーター1130に送信したとする（ステップS711）。この場合、メーター1130は、メディア鍵MKと異なるメディア鍵MK'から生成された共有鍵で暗号化された暗号文を正しく復号できないため、処理を中止する。

40

【0120】

このように、本変形例では、複数のMKBを用いてデバイス（メーター）をグループ管理できるため、異なるグループに属する機器同士の混信を防止することができる。

【0121】

(変形例14)

変形例14では、集約器を利用して、複数のメーター同士が通信を行い、集約器とメーターの通信の可否をKDCが管理する。

【0122】

50

図 1 1 は、変形例 1 4 における鍵共有処理の全体の流れを示すシーケンス図である。本変形例では、集約器 1 0 2 0 も M K B を処理するデバイス鍵（デバイス鍵 C）を持つ。そして、本変形例では、暗号化の際に M K B を処理して得られたメディア鍵 M K と事前共有鍵を用いる。図 1 1 では、ステップ S 6 0 2 を追加したこと、および、ステップ S 6 0 7、ステップ S 6 1 0 の処理が、第 3 の実施形態の図 9 と異なる。他のステップは図 9 と同様である。

【0 1 2 3】

ステップ S 6 0 2 では、集約器 1 0 2 0 は、K D C 4 0 0 から受信した M K B を処理してメディア鍵 M K を生成する（ステップ S 6 0 2）。集約器 1 0 2 0 が M K B によって無効化されている場合、集約器 1 0 2 0 は M K B を正しく処理復号することができず、メディア鍵 M K を正しく取得することはできない。すなわち、K D C 4 0 0 は、M K B を更新することで集約器 1 0 2 0 の通信の可否を制御することができる。

10

【0 1 2 4】

ステップ S 6 0 7 およびステップ S 6 1 0 は、メディア鍵 M K を用いて生成する鍵によって暗号文を生成し、M K B は暗号化せずに送付するが、図 9 のステップ S 5 0 6 およびステップ S 5 0 9 と異なる。ここで、M K B の改ざんへの対策として、K D C 4 0 0 によって発行された M K B に対する署名と共に送付してもよい。

【0 1 2 5】

（変形例 1 5） 変形例 1 4 では、ステップ S 6 1 0 で送付される暗号文は K で暗号化された暗号文を含み、ステップ S 6 1 2 で送付される暗号文も K で暗号化されていたが、それぞれ、S 6 1 3 と S 6 1 4 で生成される S K を用いて暗号化し、送付してもよい。

20

【0 1 2 6】

以上説明したとおり、第 1 から第 3 の実施形態によれば、安全性と効率を両立した鍵共有方式が実現できる。

【0 1 2 7】

次に、第 1 から第 3 の実施形態にかかる各装置（サーバ、デバイス（情報処理装置）、K D C）のハードウェア構成について図 1 2 を用いて説明する。図 1 2 は、第 1 または第 2 の実施形態にかかる装置のハードウェア構成を示す説明図である。

【0 1 2 8】

第 1 から第 3 の実施形態にかかる装置は、C P U（Central Processing Unit）5 1 などの制御装置と、R O M（Read Only Memory）5 2 や R A M（Random Access Memory）5 3 などの記憶装置と、ネットワークに接続して通信を行う通信 I / F 5 4 と、H D D（Hard Disk Drive）、C D（Compact Disc）ドライブ装置などの外部記憶装置と、ディスプレイ装置などの表示装置と、キーボードやマウスなどの入力装置と、各部を接続するバス 6 1 を備えており、通常のコンピュータを利用したハードウェア構成となっている。

30

【0 1 2 9】

第 1 から第 3 の実施形態にかかる情報処理装置で実行されるプログラムは、インストール可能な形式又は実行可能な形式のファイルで C D - R O M（Compact Disk Read Only Memory）、フレキシブルディスク（F D）、C D - R（Compact Disk Recordable）、D V D（Digital Versatile Disk）等のコンピュータで読み取り可能な記録媒体に記録されてコンピュータプログラムプロダクトとして提供される。

40

【0 1 3 0】

また、第 1 から第 3 の実施形態にかかる情報処理装置で実行されるプログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成してもよい。また、第 1 または第 2 の実施形態にかかる情報処理装置で実行されるプログラムをインターネット等のネットワーク経由で提供または配布するように構成してもよい。

【0 1 3 1】

また、第 1 から第 3 の実施形態のプログラムを、R O M 等に予め組み込んで提供するよ

50

うに構成してもよい。

【0132】

第1から第3の実施形態にかかる情報処理装置で実行されるプログラムは、上述した各部（MKB処理部、データ処理部）を含むモジュール構成となっており、実際のハードウェアとしてはCPU51（プロセッサ）が上記記憶媒体からプログラムを読み出して実行することにより上記各部が主記憶装置上にロードされ、上述した各部が主記憶装置上に生成されるようになっている。

【0133】

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

10

【符号の説明】

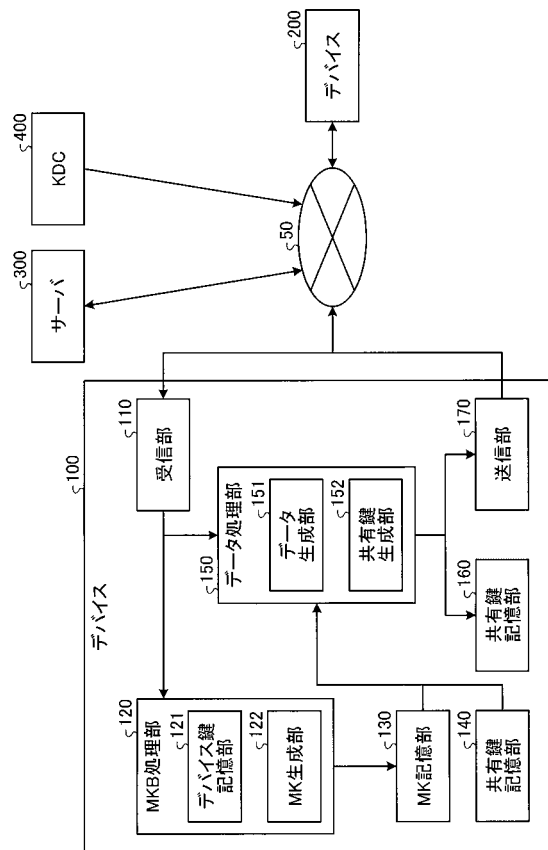
【0134】

100、200 デバイス
110、210 受信部
120、220 MKB処理部
121、221 デバイス鍵記憶部
122、222 MK生成部
130、230 MK記憶部
140、240 共有鍵記憶部
150、250 データ処理部
151、251 データ生成部
152、252 共有鍵生成部
160、260 共有鍵記憶部
170、270 送信部
300 サーバ
310 受信部
320 共有鍵記憶部
330 データ処理部
340 送信部
410 受信部
420 MKB生成部
430 鍵記憶部
440 送信部

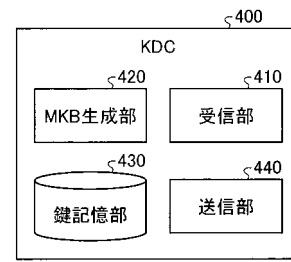
20

30

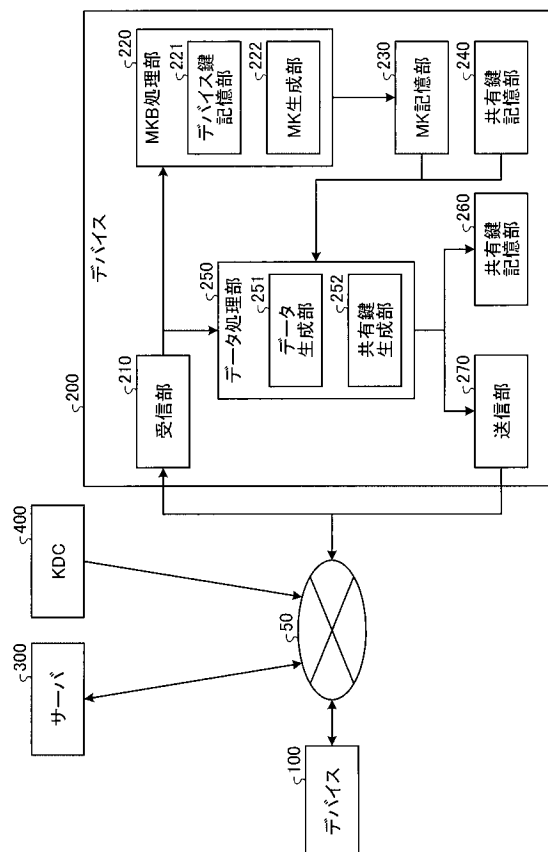
【図 1】



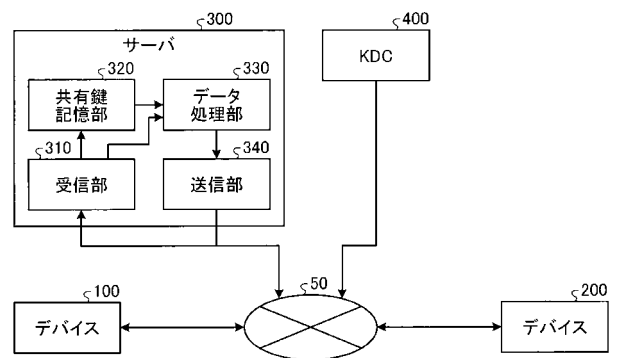
【図 2】



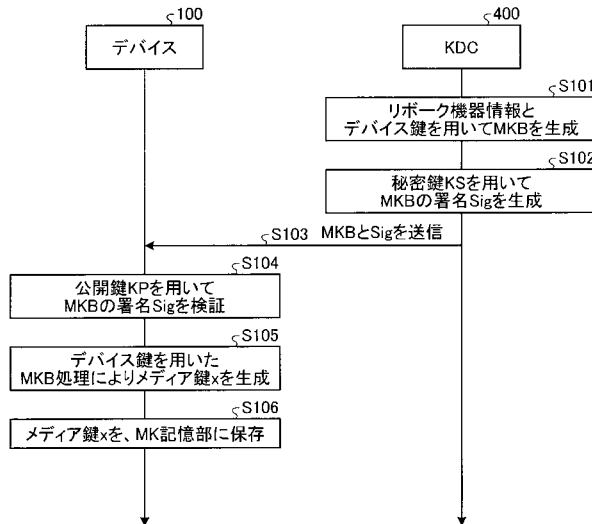
【図 3】



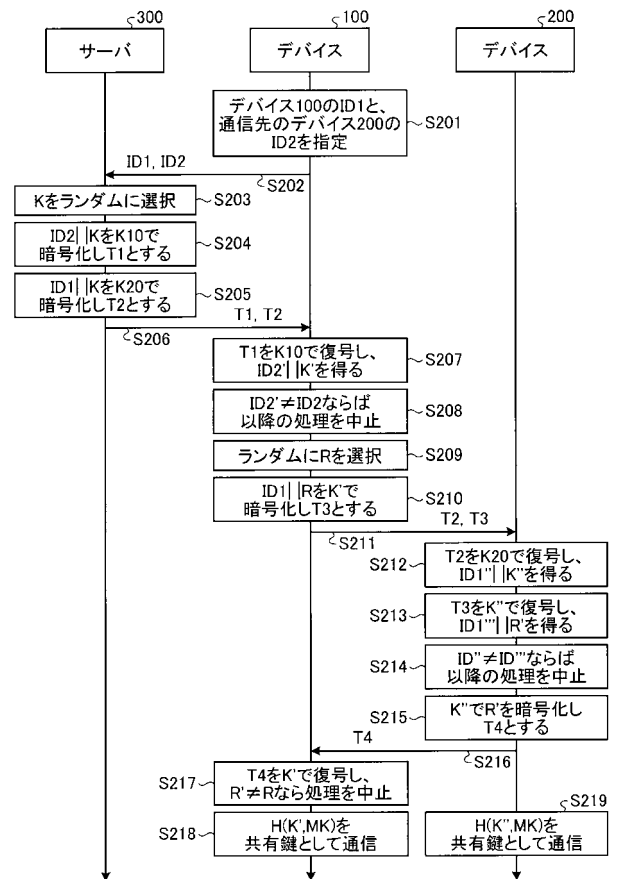
【図 4】



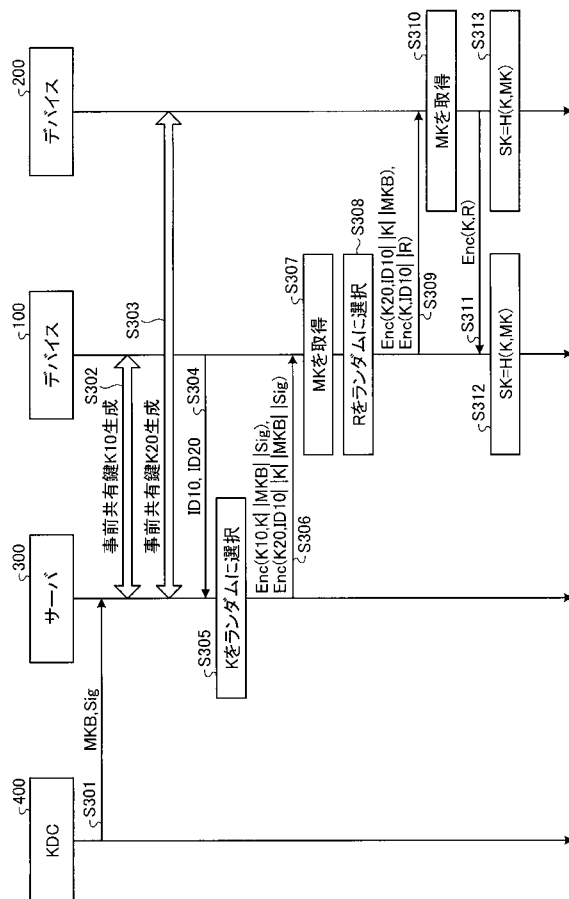
【図 5】



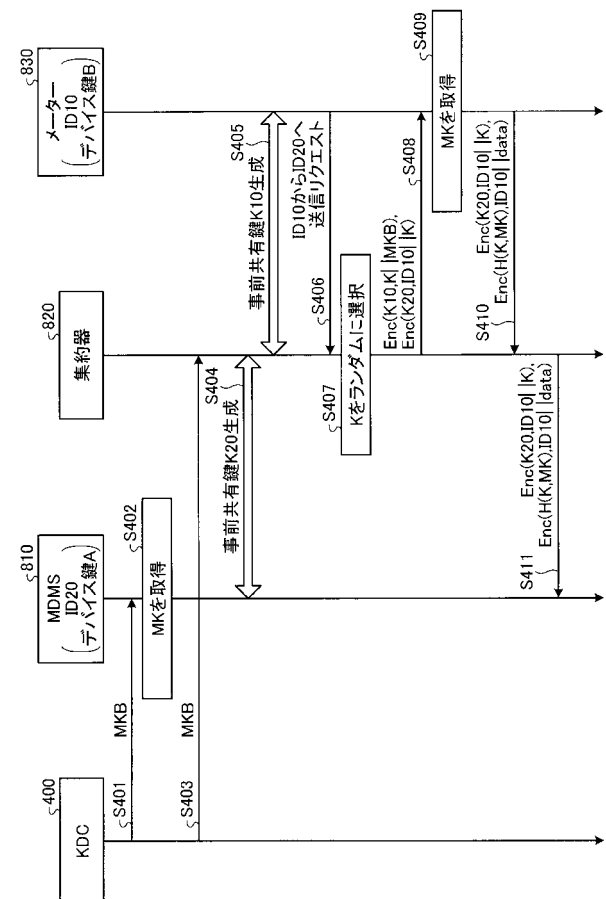
【図 6】



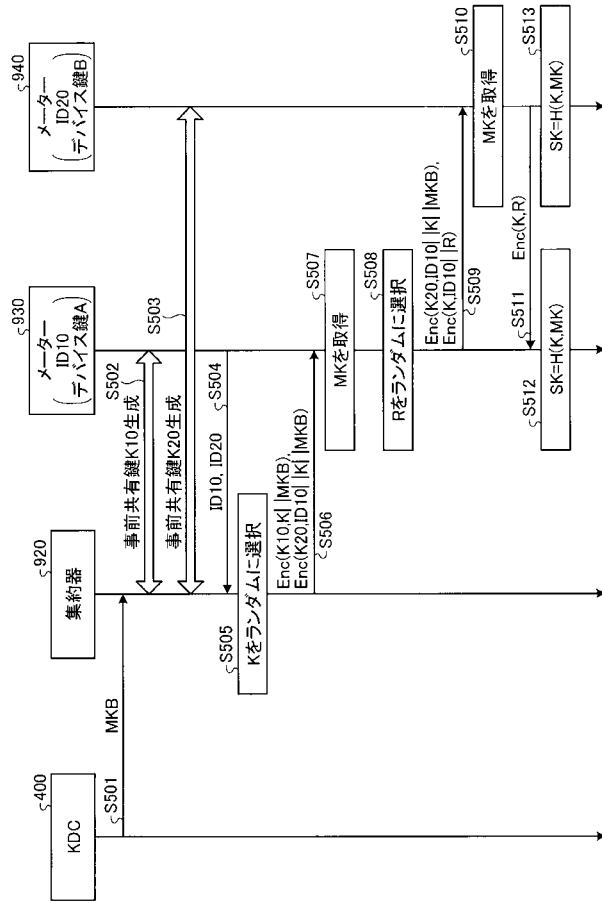
【図 7】



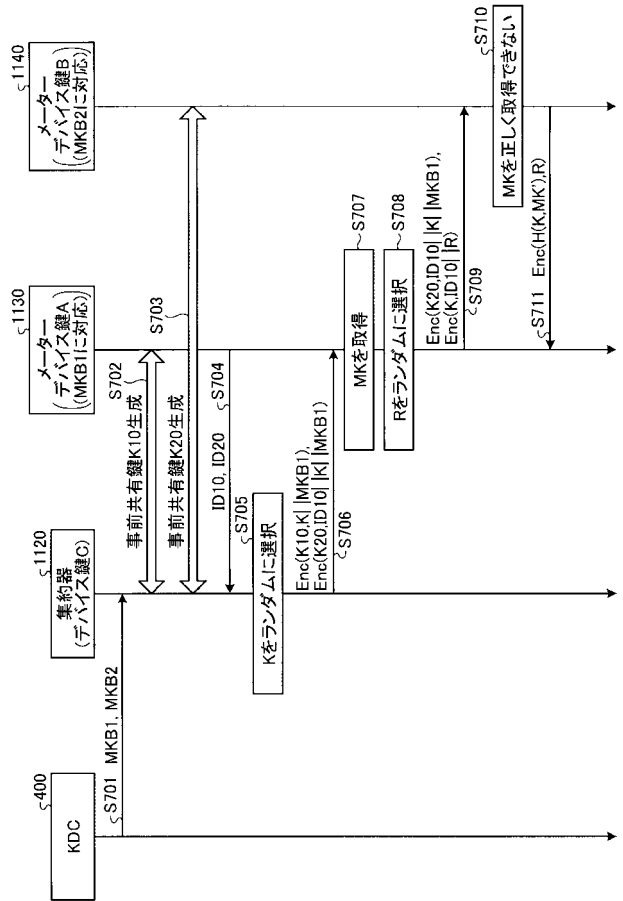
【図 8】



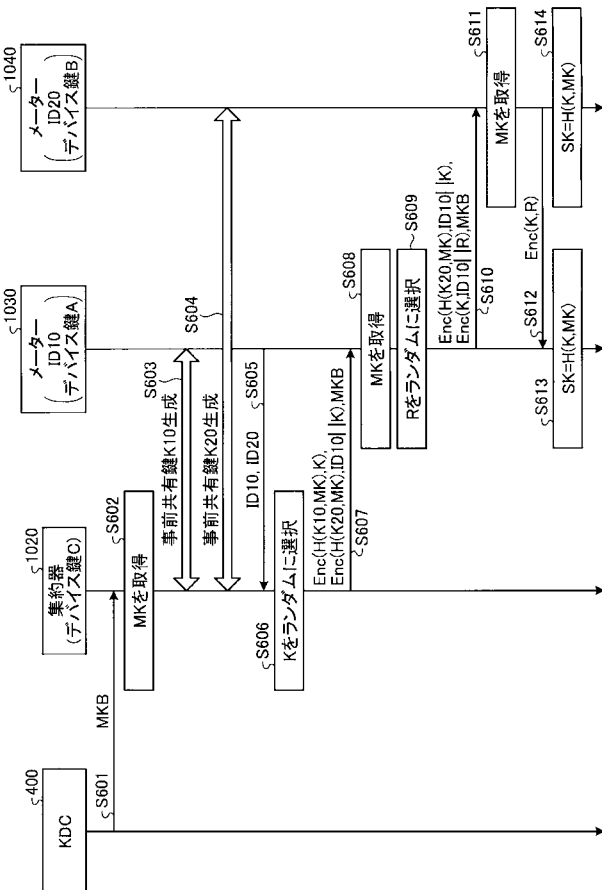
【図 9】



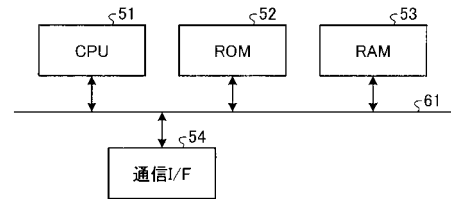
【図 10】



【図 11】



【図 12】



フロントページの続き

(72)発明者 石山 政浩

東京都港区芝浦一丁目1番1号 株式会社東芝内

Fターム(参考) 5J104 AA08 AA16 EA17 EA18 LA03