(19)日本国特許庁(JP)　(12)特 許 公 報(B2)　(11)特許番号 特許第5288901号 (P5288901)

(45)発行日 平成25年9月11日(2013.9.11)　(24)登録日 平成25年6月14日(2013.6.14)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
H04L 9/00 601E

請求項の数 22 (全 58 頁)

(21)出願番号 特願2008-162769(P2008-162769)
(22)出願日 平成20年6月23日(2008.6.23)
(65)公開番号 特開2010-4420(P2010-4420A)
(43)公開日 平成22年1月7日(2010.1.7)
審査請求日 平成23年4月4日(2011.4.4)

(73)特許権者 000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人 100099461
弁理士 溝井 章司
(74)代理人 100151220
弁理士 八巻 満隆
(72)発明者 辻 宏郷
東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内
(72)発明者 米田 健
東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内

最終頁に続く

(54)【発明の名称】鍵管理サーバ、端末、通信システム、鍵配信方法、鍵配信プログラム、鍵受信方法及び鍵受信プログラム

(57)【特許請求の範囲】
【請求項１】
複数の端末と通信可能な鍵管理サーバにおいて、
上記複数の端末間の通信の暗号化処理に用いるマスター鍵を上記複数の端末が受信する際に使用するデバイス鍵の更新を指示するデバイス鍵更新命令であって、所定の一方向性関数により現在のデバイス鍵から次の世代のデバイス鍵への更新を指示するデバイス鍵更新命令を処理装置により作成するデバイス鍵更新命令作成部と、
上記複数の端末のいずれかの端末へマスター鍵を配信するためのマスター鍵配信命令であって、管理するデバイス鍵の現在の世代情報を含むマスター鍵配布命令を処理装置により作成するマスター鍵配布命令作成部と、
上記デバイス鍵更新命令作成部が作成したデバイス鍵更新命令を上記複数の端末の少なくともいずれかの端末を宛先として通信装置により送信するとともに、上記マスター鍵配布命令作成部が作成したマスター鍵配布命令を上記マスター鍵を使用する端末を宛先として通信装置により送信するデータ送信部と
を備えることを特徴とする鍵管理サーバ。
【請求項２】
上記鍵管理サーバは、さらに、
上記データ送信部がデバイス鍵更新命令を送信した場合、上記所定の一方向性関数により現在のデバイス鍵から次の世代のデバイス鍵を処理装置により生成するとともに、次の世代のデバイス鍵を生成した場合、上記現在のデバイス鍵を削除するデバイス更新鍵生成

部
を備えることを特徴とする請求項１に記載の鍵管理サーバ。
【請求項３】
　上記デバイス更新鍵生成部は、管理するデバイス鍵に有効期限が付されている場合、上記有効期限を過ぎると、現在のデバイス鍵から次の世代のデバイス鍵を生成する
ことを特徴とする請求項２に記載の鍵管理サーバ。
【請求項４】
　上記鍵管理サーバは、さらに、
　所定の一方向性関数により現在のマスター鍵から次の世代のマスター鍵への更新を指示するマスター鍵更新命令を処理装置により作成するマスター鍵更新命令作成部と、
　上記マスター鍵更新命令作成部が作成したマスター鍵更新命令を上記マスター鍵を使用する端末を宛先として通信装置により送信するデータ送信部と
を備えることを特徴とする請求項１から３までのいずれかに記載の鍵管理サーバ。
【請求項５】
　上記マスター鍵更新命令作成部は、管理するデバイス鍵の現在の世代情報をマスター鍵更新命令に含めて作成する
ことを特徴とする請求項４に記載の鍵管理サーバ。
【請求項６】
　上記鍵管理サーバは、さらに、
　上記データ送信部がマスター鍵更新命令を送信した場合、所定の一方向性関数により現在のマスター鍵から次の世代のマスター鍵を処理装置により生成するとともに、次の世代のマスター鍵を生成した場合、上記現在のマスター鍵を削除するマスター更新鍵生成部
を備えることを特徴とする請求項４又は５に記載の鍵管理サーバ。
【請求項７】
　上記マスター更新鍵生成部は、管理するマスター鍵に有効期限が付されている場合、上記有効期限を過ぎると、現在のマスター鍵から次の世代のマスター鍵を生成する
ことを特徴とする請求項６に記載の鍵管理サーバ。
【請求項８】
　他の端末との通信の暗号化処理に使用するマスター鍵を鍵管理サーバから受信する場合に使用するデバイス鍵の更新を指示するデバイス鍵更新命令であって、現在のデバイス鍵から次の世代のデバイス鍵への更新を指示するデバイス鍵更新命令を通信装置を介して受信するとともに、マスター鍵を配信するためのマスター鍵配布命令であって、上記鍵管理サーバが管理する現在のデバイス鍵の世代情報を含むマスター鍵配布命令を通信装置を介して受信するデータ受信部と、
　上記データ受信部が受信したデバイス鍵更新命令に従い、所定の一方向性関数により現在のデバイス鍵から次の世代のデバイス鍵を処理装置により生成するとともに、上記所定の一方向性関数により上記マスター鍵配布命令に含まれる世代情報が示す世代まで現在のデバイス鍵を更新する更新鍵生成部と
を備えることを特徴とする端末。
【請求項９】
　上記更新鍵生成部は、次の世代のデバイス鍵を生成した場合、上記現在のデバイス鍵を削除する
ことを特徴とする請求項８に記載の端末。
【請求項１０】
　上記更新鍵生成部は、管理するデバイス鍵に有効期限が付されている場合、上記有効期限を過ぎると、現在のデバイス鍵から次の世代のデバイス鍵を生成する
ことを特徴とする請求項８又は９に記載の端末。
【請求項１１】
　上記端末は、さらに、
　上記データ受信部が受信したデバイス鍵更新命令を他の端末へ通信装置を介して送信す

るデバイス鍵機器間通信部
を備えることを特徴とする請求項８から１０までのいずれかに記載の端末。
【請求項１２】
上記データ受信部は、鍵管理サーバが送信したマスター鍵の更新を指示するマスター鍵更新命令を受信し、
上記更新鍵生成部は、上記マスター鍵更新命令に従い、所定の一方向性関数により現在のマスター鍵から次の世代のマスター鍵を生成する
ことを特徴とする請求項８から１１までのいずれかに記載の端末。
【請求項１３】
上記更新鍵生成部は、次の世代のマスター鍵を生成した場合、上記現在のマスター鍵を削除する
ことを特徴とする請求項１２に記載の端末。
【請求項１４】
上記データ受信部は、上記鍵管理サーバが管理する現在のデバイス鍵の世代情報を含むマスター鍵更新命令を受信し、
上記更新鍵生成部は、所定の一方向性関数により上記マスター鍵更新命令に含まれる世代情報が示す世代まで現在のデバイス鍵を更新する
ことを特徴とする請求項１２又は１３に記載の端末。
【請求項１５】
上記端末は、さらに、
上記データ受信部が受信したマスター鍵更新命令を他の端末へ通信装置を介して送信するマスター鍵機器間通信部
を備えることを特徴とする請求項１２から１４までのいずれかに記載の端末。
【請求項１６】
上記更新鍵生成部は、管理するマスター鍵に有効期限が付されている場合、上記有効期限を過ぎると、現在のマスター鍵から次の世代のマスター鍵を生成する
ことを特徴とする請求項８から１５までのいずれかに記載の端末。
【請求項１７】
他の端末から所定の通信情報を受信する場合に、上記他の端末との通信に使用するマスター鍵の上記他の端末における現在の世代情報を上記所定の通信情報とともに通信装置を介して受信するマスター鍵世代情報通信部を備え、
上記更新鍵生成部は、所定の一方向性関数により上記マスター鍵世代情報通信部が受信した現在のマスター鍵の世代情報が示す世代まで現在のマスター鍵を更新する
ことを特徴とする請求項８から１６までのいずれかに記載の端末。
【請求項１８】
鍵管理サーバと複数の端末とを備える通信システムにおいて、
上記鍵管理サーバは、
上記複数の端末間の通信の暗号化処理に用いるマスター鍵を上記複数の端末が受信する際に使用するデバイス鍵の更新を指示するデバイス鍵更新命令であって、所定の一方向性関数により現在のデバイス鍵から次の世代のデバイス鍵へ更新させるデバイス鍵更新命令を処理装置により作成するデバイス鍵更新命令作成部と、
上記複数の端末のいずれかの端末へマスター鍵を配信するためのマスター鍵配信命令であって、管理するデバイス鍵の現在の世代情報を含むマスター鍵配布命令を処理装置により作成するマスター鍵配布命令作成部と、
上記デバイス鍵更新命令作成部が作成したデバイス鍵更新命令を上記複数の端末の少なくともいずれかの端末を宛先として通信装置により送信するとともに、上記マスター鍵配布命令作成部が作成したマスター鍵配布命令を上記マスター鍵を使用する端末を宛先として通信装置により送信するデータ送信部とを備え、
上記端末は、
上記データ送信部が送信したデバイス鍵更新命令とマスター鍵配布命令とを通信装置を

介して受信するデータ受信部と、

上記データ受信部が受信したデバイス鍵更新命令に従い、所定の一方向性関数により現在のデバイス鍵から次の世代のデバイス鍵を処理装置により生成するとともに、上記所定の一方向性関数により上記マスター鍵配布命令に含まれる世代情報が示す世代まで現在のデバイス鍵を更新する更新鍵生成部とを備えることを特徴とする通信システム。

【請求項１９】

複数の端末と通信可能な鍵管理サーバにおける鍵配信方法において、

処理装置が、上記複数の端末間の通信の暗号化処理に用いるマスター鍵を上記複数の端末が受信する際に使用するデバイス鍵の更新を指示するデバイス鍵更新命令であって、所定の一方向性関数により現在のデバイス鍵から次の世代のデバイス鍵への更新を指示するデバイス鍵更新命令を作成するデバイス鍵更新命令作成ステップと、

処理装置が、上記複数の端末のいずれかの端末へマスター鍵を配信するためのマスター鍵配信命令であって、管理するデバイス鍵の現在の世代情報を含むマスター鍵配布命令を作成するマスター鍵配布命令作成ステップと、

通信装置が、上記デバイス鍵更新命令作成ステップで作成したデバイス鍵更新命令を上記複数の端末の少なくともいずれかの端末を宛先として送信するとともに、上記マスター鍵配布命令作成ステップで作成したマスター鍵配布命令を上記マスター鍵を使用する端末を宛先として送信するデータ送信ステップと

を備えることを特徴とする鍵配信方法。

【請求項２０】

複数の端末と通信可能な鍵管理サーバにおける鍵配信プログラムにおいて、

上記複数の端末間の通信の暗号化処理に用いるマスター鍵を上記複数の端末が受信する際に使用するデバイス鍵の更新を指示するデバイス鍵更新命令であって、所定の一方向性関数により現在のデバイス鍵から次の世代のデバイス鍵への更新を指示するデバイス鍵更新命令を作成するデバイス鍵更新命令作成処理と、

上記複数の端末のいずれかの端末へマスター鍵を配信するためのマスター鍵配信命令であって、管理するデバイス鍵の現在の世代情報を含むマスター鍵配布命令を作成するマスター鍵配布命令作成処理と、

上記デバイス鍵更新命令作成処理で作成したデバイス鍵更新命令を上記複数の端末の少なくともいずれかの端末を宛先として送信するとともに、上記マスター鍵配布命令作成処理で作成したマスター鍵配布命令を上記マスター鍵を使用する端末を宛先として送信するデータ送信処理と

をコンピュータに実行させることを特徴とする鍵配信プログラム。

【請求項２１】

通信装置が、他の端末との通信の暗号化処理に使用するマスター鍵を鍵管理サーバから受信する場合に使用するデバイス鍵の更新を指示するデバイス鍵更新命令であって、現在のデバイス鍵から次の世代のデバイス鍵への更新を指示するデバイス鍵更新命令を受信するとともに、マスター鍵を配信するためのマスター鍵配布命令であって、上記鍵管理サーバが管理する現在のデバイス鍵の世代情報を含むマスター鍵配布命令を受信するデータ受信ステップと、

処理装置が、上記データ受信ステップで受信したデバイス鍵更新命令に従い、所定の一方向性関数により現在のデバイス鍵から次の世代のデバイス鍵を生成するとともに、上記所定の一方向性関数により上記マスター鍵配布命令に含まれる世代情報が示す世代まで現在のデバイス鍵を更新する更新鍵生成ステップと

を備えることを特徴とする鍵受信方法。

【請求項２２】

他の端末との通信の暗号化処理に使用するマスター鍵を鍵管理サーバから受信する場合に使用するデバイス鍵の更新を指示するデバイス鍵更新命令であって、現在のデバイス鍵から次の世代のデバイス鍵への更新を指示するデバイス鍵更新命令を受信するとともに、マスター鍵を配信するためのマスター鍵配布命令であって、上記鍵管理サーバが管理する

現在のデバイス鍵の世代情報を含むマスター鍵配布命令を受信するデータ受信処理と、
　上記データ受信処理で受信したデバイス鍵更新命令に従い、所定の一方向性関数により現在のデバイス鍵から次の世代のデバイス鍵を生成するとともに、上記所定の一方向性関数により上記マスター鍵配布命令に含まれる世代情報が示す世代まで現在のデバイス鍵を更新する更新鍵生成処理と
をコンピュータに実行させることを特徴とする鍵受信プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、例えば、複数の端末間において暗号化通信を行う場合に使用する暗号鍵の配布及び暗号鍵の共有技術に関する。
【背景技術】
【０００２】
　複数の通信機器において、暗号アルゴリズムの鍵を共有し、通信機器間の通信内容の電子署名や暗号化を行うことによって、通信内容の盗聴防止や改ざん検出を実現することができる。この時、暗号アルゴリズムとして共通鍵暗号アルゴリズムを用いる場合は、全ての通信機器が同一の共通鍵を共有する必要がある。また、暗号アルゴリズムとして公開鍵暗号アルゴリズムを用いる場合は、全ての通信機器が機器自身の秘密鍵と他の機器の公開鍵を持っている必要がある。即ち、通信機器間で、秘密鍵または秘密鍵に対応付けされた公開鍵を共有する必要がある。この時、同一の鍵を継続利用し続けると、鍵解析や紛失した通信機器からの鍵読み出し等によって、鍵が漏洩する可能性があるため、共有した鍵を更新する必要がある。
【０００３】
　従来の複数通信機器における共有鍵の更新に関する技術としては、以下のような技術がある。
　特許文献１には鍵配信システムについての記載がある。この鍵配信システムでは、利用者を木構造でグルーピングして、グループ内で共有するグループ鍵を、利用者の新規入会あるいは脱会要求に基づいて鍵管理サーバで生成する。そして、鍵管理サーバと各々の利用者の間で事前共有しておいた利用者の個人鍵で暗号化することによって、グループ鍵の更新・配布を行う。
【０００４】
　特許文献２には、鍵交換システムについての記載がある。この鍵交換システムでは、ＤＨＣＰ（Ｄｙｎａｍｉｃ　Ｈｏｓｔ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）サーバであるゲートウェイ装置と通信端末との間で、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎの鍵交換方式を用いて、鍵データを交換することによって共有鍵を更新する。特に、この鍵交換システムでは、通信端末がネットワーク情報の有効期限切れまでにゲートウェイ装置に対して行うネットワーク情報の延長申請要求から始まるＤＨＣＰ通信時に、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎの鍵交換方式を用いて、鍵データを新たに交換する。
【０００５】
　特許文献３には、鍵更新方法についての記載がある。この鍵更新方法では、予め秘密情報に対して一方向性関数を繰り返し適用して作成されたｎ個の各値から導出された鍵の系列を、作成した順番の逆方向の順番に、即ち秘密情報に対して一方向性関数をｎ回適用した値から導出された鍵から順番に、更新するグループ鍵として利用する。これにより、この鍵更新方法では、最新のグループ鍵のみを保持していれば、過去のグループ鍵を用いて暗号化された情報を復号可能である。
【特許文献１】特開２００６－２０３３６３号公報
【特許文献２】特開２００１－２９２１３５号公報
【特許文献３】特開２０００－２４４４７４号公報
【発明の開示】
【発明が解決しようとする課題】

【０００６】
　従来の複数通信機器における共有鍵の更新方式には、以下のような課題がある。
　まず、上記鍵配信システムでは、グループ鍵を更新しているものの、鍵管理サーバで生成した更新グループ鍵を配布する際に、鍵管理サーバと各々の利用者の間で事前共有しておいた利用者の個人鍵を繰り返し利用する。そのため、暗号化された通信内容と暗号化されて配布される更新グループ鍵を入手・記録しておき、利用者の個人鍵の解読に成功した場合、解読した個人鍵からグループ鍵が漏洩し、最終的に全ての通信内容が漏洩してしまうという課題がある。
　また、上記鍵配信システムでは、グループ鍵の更新は、グループを構成する利用者の新規入会あるいは脱会要求が発生した時のみ行われる。そのため、グループ構成する利用者の新規入会あるいは脱会要求が発生しない場合、同一のグループ鍵を繰り返し利用することになり、グループ鍵の解読攻撃に晒されやすいという課題がある。
【０００７】
　また、上記鍵交換システムでは、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎの鍵交換方式を用いている。そのため、ゲートウェイ装置と通信端末のそれぞれにおいて、素数を含む複雑な演算を行う必要があり、処理負荷が高いという課題がある。
　また、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎの鍵交換方式では通信相手の認証、即ち正当性の確認は行えないため、例えば、公開鍵暗号アルゴリズムと組み合わせて使用しなければならないという課題がある。
【０００８】
　また、上記鍵更新方法では、最新のグループ鍵から過去の全てのグループ鍵を導出することが可能である。そのため、暗号化された通信内容を入手・記録しておき、最新のグループ鍵の解読や入手に成功すれば、過去のグループ鍵全てが漏洩し、最終的に全ての通信内容が漏洩してしまうという課題がある。
【０００９】
　この発明は、例えば、通信機器にかかる処理負荷を低くおさえつつ、安全性の高い通信機器間の通信を可能とする鍵配信（鍵共有）を行うことを目的とする。
【課題を解決するための手段】
【００１０】
　本発明に係る鍵管理サーバは、例えば、複数の端末と通信可能な鍵管理サーバにおいて、
　上記複数の端末間の通信の暗号化処理に用いるマスター鍵を上記複数の端末が受信する際に使用するデバイス鍵の更新を指示するデバイス鍵更新命令であって、所定の一方向性関数により現在のデバイス鍵から次の世代のデバイス鍵への更新を指示するデバイス鍵更新命令を処理装置により作成するデバイス鍵更新命令作成部と、
　上記デバイス鍵更新命令作成部が作成したデバイス鍵更新命令を上記複数の端末の少なくともいずれかの端末を宛先として通信装置により送信するデータ送信部と
を備えることを特徴とする。
【発明の効果】
【００１１】
　本発明に係る鍵配信サーバによれば、デバイス鍵を更新するため、マスター鍵の配信を安全に行うことができる。特に、一方向性関数によりデバイス鍵を更新するため、たとえ現在のデバイス鍵が漏洩しても、過去のデバイス鍵により通信した情報が漏洩することはない。また、本発明に係る鍵配信サーバによれば、デバイス鍵自体を配信しないため、通信を傍受されることによりデバイス鍵が漏洩することがない。さらに、本発明に係る鍵配信サーバによれば、デバイス鍵自体を配信しないため、通信情報を暗号化する必要がない、つまり複雑な暗号化演算をする必要がない。そのため、鍵管理サーバと端末とにおける処理負荷が低い。
【発明を実施するための最良の形態】
【００１２】

実施の形態１．
図１は実施の形態１におけるシステム構成図である。
図１において、鍵管理サーバ１０１は通信機器１０２間の通信に用いる暗号鍵（マスター鍵）を作成して配布し、また通信機器１０２間で共有されたマスター鍵や後述するデバイス鍵の更新を指示するサーバである。通信機器１０２は他の通信機器１０２との間でマスター鍵を用いて暗号化処理を行い通信をする機器である。ネットワーク１０３は鍵管理サーバ１０１と通信機器１０２の間、および通信機器１０２同士の間の通信路として用いられるバックボーンネットワークである。
鍵管理サーバ１０１と通信機器１０２とは、通信機器１０２毎に異なる暗号鍵（デバイス鍵）を予め共有しており、鍵管理サーバ１０１と通信機器１０２の間で、様々な命令データを暗号化や改ざん防止を施した上で通信することが可能となっている。
実施の形態１では、鍵管理サーバ１０１と通信機器１０２とで共有したデバイス鍵を所定のタイミングに新たなデバイス鍵に更新することにより、鍵管理サーバ１０１から通信機器１０２へのマスター鍵等の配信の安全性を高める。
【００１３】
まず、デバイス鍵更新命令の配布による鍵管理サーバ１０１と通信機器１０２との間の共有鍵（デバイス鍵）の更新の動作の概要について説明する。
デバイス鍵の更新は、デバイス鍵一括更新命令６００を用いて全てのデバイス鍵を一括更新する方法と、デバイス鍵個別更新命令７００を用いて特定の通信機器１０２との間で共有するデバイス鍵のみを更新する方法との二通りがある。さらに、これらの命令（デバイス鍵一括更新命令６００、デバイス鍵個別更新命令７００）にデバイス鍵の有効期限が記載されていた場合、鍵管理サーバ１０１と通信機器１０２において、有効期限に従って自動的にデバイス鍵の更新を行う。
【００１４】
図２は図１に示したシステム構成において、全てのデバイス鍵を一括に更新する際のデータの流れを示した図である。
鍵管理サーバ１０１は、全てのデバイス鍵の一括更新を指示する命令を作成し、各々の通信機器１０２が命令の正当性を検証するための電子署名集合を付与して、デバイス鍵一括更新命令６００を作成する。次に、鍵管理サーバ１０１は、ネットワーク１０３を介して、デバイス鍵一括更新命令６００を全ての通信機器１０２に向けて送信する。そして、鍵管理サーバ１０１は、全てのデバイス鍵を更新する。一方、通信機器１０２は、ネットワーク１０３を介して、デバイス鍵一括更新命令６００を受信し、命令に含まれる電子署名集合を検証して命令の正当性を確認し、デバイス鍵の更新を行う。
【００１５】
次に、図３に基づき、鍵管理サーバ１０１が配布するデバイス鍵一括更新命令６００について説明する。
図３は、図２におけるデバイス鍵一括更新命令６００のデータ形式を示した図である。
図３において、デバイス鍵一括更新命令６００は、データ種別６０１、デバイス鍵一括更新命令情報６０２、電子署名集合６０３を備える。
データ種別６０１は命令データの種類がデバイス鍵一括更新命令であることを示すフラグである。デバイス鍵一括更新命令情報６０２は全ての通信機器１０２においてデバイス鍵を更新するための具体的な指示内容である。電子署名集合６０３はこのデバイス鍵一括更新命令６００が鍵管理サーバ１０１で作成された正規命令であることを確認するために、宛先である通信機器１０２毎に作成された個別電子署名６０４の集合である。個別電子署名６０４は各々の通信機器１０２が検証可能な電子署名である。
デバイス鍵一括更新命令情報６０２は、更新後世代番号６１１、有効期限６１２を備える。更新後世代番号６１１は何世代目のデバイス鍵に更新すればよいかを示す世代番号である。有効期限６１２は更新後のデバイス鍵に有効期限を設定する場合に指定する日時であり、有効期限を設定しない場合は省略可能である。
個別電子署名６０４は、デバイスＩＤ６２１、署名鍵世代番号６２２、署名値６２３を

備える。デバイスＩＤ６２１はその個別電子署名６０４が対象とする通信機器１０２を示す、機器毎に異なる値である。署名鍵世代番号６２２は署名を生成する際に用いたデバイス鍵の世代番号である。署名値６２３はデバイスＩＤ６２１の通信機器１０２に対応する署名鍵世代番号６２２のデバイス鍵を用いて、データ種別６０１およびデバイス鍵一括更新命令情報６０２に対して施された署名である。

【００１６】

図４は図１に示したシステム構成において、特定のデバイス鍵のみを個別に更新する際のデータの流れを示した図である。

鍵管理サーバ１０１は、特定の通信機器１０２のデバイス鍵の個別更新を指示する命令を作成し、該当する通信機器１０２が命令の正当性を検証するための電子署名を付与して、デバイス鍵個別更新命令７００を作成する。次に、鍵管理サーバ１０１は、ネットワーク１０３を介して、デバイス鍵個別更新命令７００を該当する通信機器１０２に向けて送信する。そして、鍵管理サーバ１０１は、該当するデバイス鍵を更新する。一方、通信機器１０２は、ネットワーク１０３を介して、デバイス鍵個別更新命令７００を受信し、命令が自分宛であるかどうか確認し、命令に含まれる電子署名を検証して命令の正当性を確認し、デバイス鍵の更新を行う。

【００１７】

次に、図５に基づき、鍵管理サーバ１０１が配布するデバイス鍵個別更新命令７００について説明する。

図５は、図４におけるデバイス鍵個別更新命令７００のデータ形式を示した図である。

図５において、デバイス鍵個別更新命令７００は、データ種別７０１、デバイス鍵個別更新命令情報７０２、電子署名７０３を備える。

データ種別７０１は命令データの種類がデバイス鍵個別更新命令であることを示すフラグである。デバイス鍵個別更新命令情報７０２は特定の通信機器１０２においてデバイス鍵を更新するための具体的な指示内容である。電子署名７０３はこのデバイス鍵個別更新命令７００が鍵管理サーバ１０１で作成された正規命令であることを確認するために作成された、該当する通信機器１０２が検証可能な電子署名である。

デバイス鍵個別更新命令情報７０２は、デバイスＩＤ７１１、更新後世代番号７１２、有効期限７１３を備える。デバイスＩＤ７１１はデバイス鍵更新を指示する通信機器１０２を示す、機器毎に異なる値である。更新後世代番号７１２は何世代目のデバイス鍵に更新すればよいかを示す世代番号である。有効期限７１３は更新後のデバイス鍵に有効期限を設定する場合に指定する日時であり、有効期限を設定しない場合は省略可能である。

電子署名７０３は、署名鍵世代番号７２１、署名値７２２を備える。署名鍵世代番号７２１は署名を生成する際に用いたデバイス鍵の世代番号である。署名値７２２はデバイスＩＤ７１１の通信機器１０２に対応する署名鍵世代番号７２１のデバイス鍵を用いて、データ種別７０１およびデバイス鍵個別更新命令情報７０２に対して施された署名である。

【００１８】

次に、図６、図７に基づき、実施の形態１における鍵管理サーバ１０１の機能について説明する。

図６は実施の形態１における鍵管理サーバ１０１の機能ブロック図である。鍵管理サーバ１０１は、入力インタフェース２０１、データ送信部２０２、更新鍵生成部２０４（デバイス更新鍵生成部、マスター更新鍵生成部）、署名値計算部２０６、鍵管理データベース２０７、デバイス鍵更新命令作成部２０８を備える。

入力インタフェース２０１は、鍵管理サーバ１０１の操作者による入力を入力装置を介して受け付ける。

データ送信部２０２は、鍵管理サーバ１０１で作成した各種命令データを、ネットワーク１０３を介して通信装置により通信機器１０２へ送信する。

更新鍵生成部２０４は、一方向性関数により現在の鍵から次の世代の鍵を処理装置により生成する。

署名値計算部２０６は、署名対象のデータに対して、指定されたデバイス鍵を用いて署

名を処理装置により生成する。
鍵管理データベース２０７は、鍵管理サーバ１０１が管理する必要のある全ての鍵を記憶装置に記憶（管理）する。
デバイス鍵更新命令作成部２０８は、デバイス鍵一括更新命令６００やデバイス鍵個別更新命令７００を処理装置により作成する。
【００１９】
図７は実施の形態１における鍵管理サーバ１０１内部の鍵管理データベース２０７が記憶する情報を示す図である。鍵管理データベース２０７は、デバイス鍵管理テーブル３０１を備える。
デバイス鍵管理テーブル３０１は、鍵管理サーバ１０１と各々の通信機器１０２との間で共有しているデバイス鍵を、通信機器１０２を特定するデバイスＩＤ、鍵の世代番号、鍵の有効期限との組合せで管理する。なお、鍵の世代番号とは、デバイス鍵が何回更新されたかを示す世代情報であり、例えば、初めに共有したデバイス鍵を１（第１世代）とし、その後デバイス鍵の更新がされる度に２（第２世代）、３（第３世代）、・・・とインクリメント（＋１）される。
【００２０】
次に、図８、図９に基づき、実施の形態１における通信機器１０２の機能について説明する。
図８は実施の形態１における通信機器１０２の機能ブロック図である。通信機器１０２は、データ受信部４０１、更新鍵生成部４０３、署名値検証部４０５、管理データベース４０６、デバイス鍵更新命令解釈部４０７を備える。
データ受信部４０１は、ネットワーク１０３を介して鍵管理サーバ１０１から送られてくる各種命令データを通信装置により受信する。
更新鍵生成部４０３は、一方向性関数により現在の鍵から次の世代の鍵を処理装置により生成する。
署名値検証部４０５は、署名対象のデータおよび署名値に対して、指定された鍵を用いて処理装置により署名を検証する。
管理データベース４０６は、通信機器１０２が管理する必要のある全ての情報および鍵を記憶装置に記憶（管理）する。
デバイス鍵更新命令解釈部４０７は、データ受信部４０１で受信したデバイス鍵一括更新命令６００やデバイス鍵個別更新命令７００を解釈し、更新鍵生成部４０３にデバイス鍵を更新させる。
【００２１】
図９は実施の形態１における通信機器１０２内部の管理データベース４０６が記憶する情報を示す図である。管理データベース４０６は、デバイスＩＤ管理テーブル５０１、デバイス鍵管理テーブル５０２を備える。
デバイスＩＤ管理テーブル５０１は、通信機器１０２毎に異なる様に、機器に割り当てられたデバイスＩＤの値を管理する。
デバイス鍵管理テーブル５０２は、鍵管理サーバ１０１との間で共有しているデバイス鍵を、鍵の世代番号、鍵の有効期限との組合せで管理する。
【００２２】
次に動作について説明する。
まず、デバイス鍵を一括更新する場合の動作について説明する。図１０は、デバイス鍵を一括更新する場合の通信システムの動作を示すフローチャートである。
デバイス鍵一括更新命令作成処理（Ｓ１０１）では、鍵管理サーバ１０１のデバイス鍵更新命令作成部２０８は、デバイス鍵一括更新命令６００を作成する。この際、署名値計算部２０６は、鍵管理データベース２０７のデバイス鍵管理テーブル３０１で管理する全てのデバイス鍵を入力として、データ種別６０１とデバイス鍵一括更新命令情報６０２に対する署名値６２３を通信機器１０２毎に生成する。
データ送信処理（Ｓ１０２）では、データ送信部２０２は、デバイス鍵一括更新命令６

００を全ての通信機器１０２へ送信する。

サーバ側デバイス鍵更新処理（Ｓ１０３）では、更新鍵生成部２０４は、デバイス鍵一括更新命令６００の送信に成功した後、一方向関数により全てのデバイス鍵を更新し、鍵管理データベース２０７のデバイス鍵管理テーブル３０１に格納すると共に、更新前のデバイス鍵全てを削除する。

データ受信処理（Ｓ１０４）では、通信機器１０２のデータ受信部４０１は、デバイス鍵一括更新命令６００を受信する。デバイス鍵更新命令解釈部４０７は、デバイス鍵一括更新命令６００のデータ種別６０１により、受信した情報がデバイス鍵一括更新命令６００であることを認識する。

署名判定処理（Ｓ１０５）では、署名値検証部４０５は、管理データベース４０６のデバイスＩＤ管理テーブル５０１で管理するデバイスＩＤを用いて、電子署名集合６０３から自分宛の個別電子署名６０４を選択する。署名値検証部４０５は、管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵を入力として、データ種別６０１とデバイス鍵一括更新命令情報６０２に対する署名値を計算し、自分宛の個別電子署名６０４の署名値６２３と比較して、デバイス鍵一括更新命令６００の正当性を確認する。この時、署名に用いられたデバイス鍵の署名鍵世代番号６２２が管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵の世代番号より新しい場合、署名値検証部４０５は、一時的に新しい世代の鍵を更新鍵生成部４０３に生成させて、生成された鍵により確認する。一方、署名に用いられたデバイス鍵の署名鍵世代番号６２２が管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵の世代番号より古い場合、署名値検証部４０５は、不正な署名と判定する。

ここで、一時的に生成する新しい世代の鍵とは、署名に用いられたデバイス鍵の世代番号６２２が示す世代のデバイス鍵である。つまり、署名に用いられたデバイス鍵の世代番号６２２が、管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵の世代番号よりも２世代新しい場合、更新鍵生成部４０３は一方向関数を２度通すことにより新しい世代の鍵を生成する。また、一時的にとは、デバイス鍵一括更新命令６００の正当性を確認できなければ、生成した新しい世代の鍵は削除して元の世代の鍵のままとすることを意味する。

署名の検証に成功した場合（Ｓ１０５でＹＥＳ）、デバイス鍵更新命令解釈部４０７は（Ｓ１０６）へ進む。一方、署名の検証に失敗した場合（Ｓ１０５でＮＯ）、デバイス鍵更新命令解釈部４０７はデバイス鍵一括更新命令６００を正当でないと判断し、処理を終了する。

端末側デバイス鍵更新処理（Ｓ１０６）では、署名の検証に成功した場合、更新鍵生成部４０３は、鍵管理サーバ１０１と同一の一方向性関数によりデバイス鍵を更新し、管理データベース４０６のデバイス鍵管理テーブル５０２に格納すると共に、更新前のデバイス鍵を削除する。なお、（Ｓ１０５）において、新しい世代の鍵を生成して確認を行った場合には、新しい世代の鍵をさらに次世代以降の世代に更新した鍵を更新後のデバイス鍵として管理データベース４０６のデバイス鍵管理テーブル５０２に格納する。つまり、デバイス鍵一括更新命令６００の更新後世代番号６１１が示す世代のデバイス鍵を生成して、管理データベース４０６のデバイス鍵管理テーブル５０２に格納する。

【００２３】

次に特定のデバイス鍵のみを更新する場合の動作について説明する。図１１は、特定のデバイス鍵のみを更新する場合の通信システムの動作を示すフローチャートである。

デバイス鍵個別更新命令作成処理（Ｓ２０１）では、鍵管理サーバ１０１のデバイス鍵更新命令作成部２０８は、デバイス鍵個別更新命令７００を作成する。この際、署名値計算部２０６は、鍵管理データベース２０７のデバイス鍵管理テーブル３０１で管理する該当する通信機器１０２のデバイス鍵を入力として、データ種別７０１とデバイス鍵個別更新命令情報７０２に対する署名値７２２を生成する。

データ送信処理（Ｓ２０２）では、データ送信部２０２は、デバイス鍵個別更新命令７００を該当する通信機器１０２へ送信する。

サーバ側デバイス鍵更新処理（Ｓ２０３）では、更新鍵生成部２０４は、デバイス鍵個別更新命令７００の送信に成功した後、一方向性関数により該当するデバイス鍵を更新し、鍵管理データベース２０７のデバイス鍵管理テーブル３０１に格納すると共に、更新前の該当デバイス鍵を削除する。

データ受信処理（Ｓ２０４）では、通信機器１０２のデータ受信部４０１は、デバイス鍵個別更新命令７００を受信する。デバイス鍵更新命令解釈部４０７は、デバイス鍵個別更新命令７００のデータ種別７０１により、受信した情報がデバイス鍵個別更新命令７００であることを認識する。

宛先判定処理（Ｓ２０５）では、デバイス鍵更新命令解釈部４０７は、管理データベース４０６のデバイスＩＤ管理テーブル５０１で管理するデバイスＩＤとデバイス鍵個別更新命令７００に含まれるデバイスＩＤ７１１とが一致するか確認して、デバイス鍵個別更新命令７００が自分宛か否か確認する。

デバイス鍵個別更新命令７００が自分宛である場合（Ｓ２０５でＹＥＳ）、デバイス鍵更新命令解釈部４０７は（Ｓ２０６）へ進む。一方、デバイス鍵個別更新命令７００が自分宛でない場合（Ｓ２０５でＮＯ）、デバイス鍵更新命令解釈部４０７はデバイス鍵個別更新命令７００を無視し、処理を終了する。

署名判定処理（Ｓ２０６）では、デバイス鍵個別更新命令７００が自分宛である場合は、署名値検証部４０５は、管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵を入力として、データ種別７０１とデバイス鍵個別更新命令情報７０２に対する署名値を計算し、デバイス鍵個別更新命令７００の署名値７２２と比較して、デバイス鍵個別更新命令７００の正当性を確認する。デバイス鍵個別更新命令７００の正当性を確認する時、署名に用いられたデバイス鍵の署名鍵世代番号７２１が管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵の世代番号より新しい場合、署名値検証部４０５は、一時的に新しい世代の鍵を更新鍵生成部４０３に生成させて確認する。署名に用いられたデバイス鍵の署名鍵世代番号７２１が管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵の世代番号より古い場合、署名値検証部４０５は、不正な署名と判定する。

署名の検証に成功した場合（Ｓ２０６でＹＥＳ）、デバイス鍵更新命令解釈部４０７は（Ｓ２０７）へ進む。一方、署名の検証に失敗した場合（Ｓ２０６でＮＯ）、デバイス鍵更新命令解釈部４０７はデバイス鍵個別更新命令７００を正当でないと判断し、処理を終了する。

端末側デバイス鍵更新処理（Ｓ２０７）では、署名の検証に成功した場合、更新鍵生成部４０３は、鍵管理サーバ１０１と同一の一方向性関数によりデバイス鍵を更新し、管理データベース４０６のデバイス鍵管理テーブル５０２に格納すると共に、更新前のデバイス鍵を削除する。

【００２４】

次に、デバイス鍵の有効期限に従って、鍵管理サーバ１０１および通信機器１０２においてデバイス鍵を自動的に更新する場合の動作について説明する。

鍵管理サーバ１０１は、鍵管理データベース２０７のデバイス鍵管理テーブル３０１において、デバイス鍵を有効期限と共に管理している。有効期限を経過した場合は、更新鍵生成部２０４はデバイス鍵を更新し、鍵管理データベース２０７のデバイス鍵管理テーブル３０１に格納すると共に、更新前の該当デバイス鍵を削除する。

同様に、通信機器１０２は、管理データベース４０６のデバイス鍵管理テーブル５０２において、デバイス鍵を有効期限と共に管理している。有効期限を経過した場合は、更新鍵生成部４０３はデバイス鍵を更新し、管理データベース４０６のデバイス鍵管理テーブル５０２に格納すると共に、更新前のデバイス鍵を削除する。

【００２５】

以上のように、鍵管理サーバ１０１は、通信機器１０２との間で予め共有しておいた鍵（デバイス鍵）を更新するので、事前共有鍵の繰り返し利用に起因する事前共有鍵の解読による通信内容の漏洩を防止することができる。また、デバイス鍵を更新する際、更新す

る鍵自体をネットワーク１０３経由で配布しないので、暗号化して配布されるデバイス鍵の解読による通信内容の漏洩を防止することができる。事前共有するデバイス鍵を用いた電子署名値の計算、一方向性関数を用いた鍵更新を行っているので、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換方式の様な複雑な演算や公開鍵暗号アルゴリズムなどとの組合せ利用を不要として、デバイス鍵の更新を行うことができる。一方向性関数を用いてデバイス鍵を更新し、更新前のデバイス鍵を削除しているので、最新のデバイス鍵の解読による過去の通信内容の漏洩を防止することができる。

【００２６】

実施の形態２．

実施の形態２では、鍵管理サーバ１０１からのマスター鍵配布命令８００の配布による、通信機器１０２同士の間の暗号化通信に用いる暗号鍵（マスター鍵）の配布と、鍵管理サーバ１０１と通信機器１０２の間の暗号化通信に用いる共有鍵（デバイス鍵）の更新とについて説明する。

【００２７】

まず、マスター鍵配布命令８００の配布によるマスター鍵の配布およびデバイス鍵の更新の動作の概要について説明する。

鍵管理サーバ１０１は、通信機器１０２同士が暗号化通信を行う際に用いる暗号鍵（マスター鍵）を生成し、鍵を利用する通信機器１０２のデバイス鍵で暗号化し、マスター鍵配布命令８００として該当通信機器１０２へ送信する。マスター鍵配布命令８００を受信した通信機器１０２は、マスター鍵配布命令８００の正当性を検証する際、鍵管理サーバ１０１と共有するデバイス鍵に世代のずれが生じていることを検出した場合、必要に応じてデバイス鍵の更新処理を行う。さらに、これらの命令にマスター鍵の有効期限が記載されていた場合、鍵管理サーバ１０１と通信機器１０２において、有効期限に従って自動的にマスター鍵の更新を行う。

【００２８】

図１２は図１に示したシステム構成において、通信機器１０２間の暗号化に用いるマスター鍵を配布する際のデータの流れを示した図である。

鍵管理サーバ１０１は、特定の通信機器１０２同士の間で暗号化通信に用いるマスター鍵の配布を指示する命令を作成し、該当する通信機器１０２が命令の正当性を検証するための署名値を付与して、マスター鍵配布命令８００を作成する。次に、鍵管理サーバ１０１は、ネットワーク１０３を介して、マスター鍵配布命令８００を該当する通信機器１０２に向けて送信する。そして、鍵管理サーバ１０１は、該当するマスター鍵を記憶する。一方、通信機器１０２は、ネットワーク１０３を介して、マスター鍵配布命令８００を受信し、命令が自分宛であるかどうか確認し、命令に含まれる署名値を検証して命令の正当性を確認し、マスター鍵の取得を行う。

【００２９】

次に、図１３に基づき、鍵管理サーバ１０１が配布するマスター鍵配布命令８００について説明する。

図１３は、図１２におけるマスター鍵配布命令８００のデータ形式を示した図である。

図１３において、マスター鍵配布命令８００は、データ種別８０１、受信者デバイスＩＤ８０２、マスター鍵配布命令情報（暗号化後）８０３、デバイス鍵世代番号８０４、署名値８０５を備える。

データ種別８０１は命令データの種類がマスター鍵配布命令であることを示すフラグである。受信者デバイスＩＤ８０２はこの命令によってマスター鍵を配布される通信機器１０２を示すデバイスＩＤである。マスター鍵配布命令情報（暗号化後）８０３はマスター鍵配布命令情報（暗号化前）８１１を該当する通信機器１０２のデバイス鍵で暗号化した内容である。デバイス鍵世代番号８０４は暗号化および署名を生成する際に用いたデバイス鍵の世代番号である。署名値８０５はこのマスター鍵配布命令８００が鍵管理サーバ１０１で作成された正規命令であることを確認するために、受信者デバイスＩＤ８０２の通信機器１０２に対応するデバイス鍵世代番号８０４のデバイス鍵を用いて、データ種別８

０１、受信者デバイスＩＤ８０２およびマスター鍵配布命令情報（暗号化後）８０３に対して施された署名である。

マスター鍵配布命令情報（暗号化前）８１１はマスター鍵配布命令情報（暗号化後）８０３をデバイス鍵により復号した情報であり、通信機器１０２同士の間の暗号化に用いるマスター鍵の内容である。マスター鍵配布命令情報（暗号化前）８１１は、マスター鍵ＩＤ８２１、利用者デバイスＩＤ８２２、マスター鍵８２３、有効期限８２４を備える。

マスター鍵ＩＤ８２１は鍵管理サーバ１０１によってマスター鍵毎に一意に割り当てられた値である。利用者デバイスＩＤ８２２はマスター鍵８２３を利用する二台以上の通信機器１０２を示す、機器毎に異なる値の集合である。マスター鍵８２３はマスター鍵ＩＤ８２１の第１世代目のマスター鍵である。有効期限８２４はマスター鍵８２３に有効期限を設定する場合に指定する日時であり、有効期限を設定しない場合は省略可能である。

【００３０】

次に、図１４、図１５に基づき、実施の形態２における鍵管理サーバ１０１の機能について説明する。

図１４は実施の形態２における鍵管理サーバ１０１の機能ブロック図である。実施の形態２における鍵管理サーバ１０１は、実施の形態１における鍵管理サーバ１０１に加え、初期鍵生成部２０３、暗号化部２０５、マスター鍵配布命令作成部２０９を備える。

初期鍵生成部２０３は、乱数生成機能を持ち、第１世代目の鍵を処理装置により生成する。

暗号化部２０５は、暗号化対象のデータに対して、指定されたデバイス鍵を用いて所定の情報を処理装置により暗号化する。

マスター鍵配布命令作成部２０９は、マスター鍵配布命令８００を処理装置により作成する。

【００３１】

図１５は実施の形態２における鍵管理サーバ１０１内部の鍵管理データベース２０７が記憶する情報を示す図である。実施の形態２における鍵管理データベース２０７は、実施の形態１における鍵管理データベース２０７に加え、マスター鍵管理テーブル３０２を備える。

マスター鍵管理テーブル３０２は、鍵管理サーバ１０１において生成配布し、通信機器１０２同士の間の暗号化に用いるマスター鍵を、マスター鍵ＩＤ、鍵の世代番号、鍵を利用する通信機器１０２を示す利用者デバイスＩＤ、鍵の有効期限との組合せで管理する。

【００３２】

次に、図１６、図１７に基づき、実施の形態２における通信機器１０２の機能について説明する。

図１６は実施の形態２における通信機器１０２の機能ブロック図である。実施の形態２における通信機器１０２は、実施の形態１における通信機器１０２に加え、復号部４０４、マスター鍵配布命令解釈部４０８を備える。

復号部４０４は、暗号化されたデータに対して、指定された鍵を用いて処理装置により復号する。

マスター鍵配布命令解釈部４０８は、データ受信部４０１で受信したマスター鍵配布命令８００を処理装置により解釈し、第１世代目のマスター鍵を管理データベース４０６に記憶させる。

【００３３】

図１７は実施の形態２における通信機器１０２内部の管理データベース４０６が記憶する情報を示す図である。実施の形態２における管理データベース４０６は、実施の形態１における管理データベース４０６に加え、マスター鍵管理テーブル５０３を備える。

マスター鍵管理テーブル５０３は、他の通信機器１０２との間で共有しているマスター鍵を、マスター鍵ＩＤ、鍵の世代番号、この鍵を利用する全ての通信機器１０２を示す利用者デバイスＩＤの集合、鍵の有効期限との組合せで管理する。

【００３４】

次に動作について説明する。図１８は、マスター鍵を配信する場合の通信システムの動作を示すフローチャートである。

マスター鍵生成処理（Ｓ３０１）では、鍵管理サーバ１０１の初期鍵生成部２０３はマスター鍵を生成し、鍵管理データベース２０７に記憶させる。

そして、鍵管理サーバ１０１は、生成したマスター鍵を利用する通信機器１０２に対して、以下の操作を繰り返し行い、該当する通信機器１０２の全てにマスター鍵配布命令８００を送信する。

マスター鍵配布命令作成処理（Ｓ３０２）では、マスター鍵配布命令作成部２０９は、マスター鍵配布命令８００を作成する。この際、暗号化部２０５は、鍵管理データベース２０７のデバイス鍵管理テーブル３０１で管理する該当通信機器１０２のデバイス鍵を用いて、マスター鍵配布命令情報（暗号化前）８１１を暗号化し、マスター鍵配布命令情報（暗号化後）８０３を作成する。署名値計算部２０６は、鍵管理データベース２０７のデバイス鍵管理テーブル３０１で管理する該当通信機器１０２のデバイス鍵を入力として、データ種別８０１と受信者デバイスＩＤ８０２とマスター鍵配布命令情報（暗号化後）８０３に対する署名値８０５を計算する。

データ送信処理（Ｓ３０３）では、データ送信部２０２は、マスター鍵配布命令８００を該当する通信機器１０２へ送信する。

データ受信処理（Ｓ３０４）では、通信機器１０２のデータ受信部４０１は、マスター鍵配布命令８００を受信する。マスター鍵配布命令解釈部４０８は、マスター鍵配布命令８００のデータ種別８０１により、受信した情報がマスター鍵配布命令８００であることを認識する。

宛先判定処理（Ｓ３０５）では、マスター鍵配布命令解釈部４０８は、管理データベース４０６のデバイスＩＤ管理テーブル５０１で管理するデバイスＩＤとマスター鍵配布命令８００に含まれる受信者デバイスＩＤ８０２とが一致するか確認して、マスター鍵配布命令８００が自分宛か否か確認する。

マスター鍵配布命令８００が自分宛である場合（Ｓ３０５でＹＥＳ）、マスター鍵配布命令解釈部４０８は（Ｓ３０６）へ進む。一方、マスター鍵配布命令８００が自分宛でない場合（Ｓ３０５でＮＯ）、マスター鍵配布命令解釈部４０８はマスター鍵配布命令８００を無視し、処理を終了する。

署名判定処理（Ｓ３０６）では、マスター鍵配布命令８００が自分宛である場合、署名値検証部４０５は、管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵を入力として、データ種別８０１と受信者デバイスＩＤ８０２とマスター鍵配布命令情報（暗号化後）８０３に対する署名値を計算し、マスター鍵配布命令８００の署名値８０５と比較して、マスター鍵配布命令８００の正当性を確認する。マスター鍵配布命令８００の正当性を確認する時、署名に用いられたデバイス鍵の世代番号８０４が管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵の世代番号より新しい場合、署名値検証部４０５は、更新鍵生成部４０３を用いて一時的に新しい世代の鍵を生成して確認する。署名に用いられたデバイス鍵の世代番号８０４が管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵の世代番号より古い場合、署名値検証部４０５は、不正な署名と判定する。

署名の検証に成功した場合（Ｓ３０６でＹＥＳ）、マスター鍵配布命令解釈部４０８は（Ｓ３０７）へ進む。一方、署名の検証に失敗した場合（Ｓ３０６でＮＯ）、マスター鍵配布命令解釈部４０８はマスター鍵配布命令８００を正当でないと判断し、処理を終了する。

マスター鍵記憶処理（Ｓ３０７）では、署名の検証に成功した場合、復号部４０４はマスター鍵配布命令情報（暗号化後）８０３を復号する。そして、マスター鍵配布命令解釈部４０８は、マスター鍵配布命令情報（暗号化前）８１１から取り出したマスター鍵８２３を管理データベース４０６のマスター鍵管理テーブル５０３に格納する。

端末側デバイス鍵更新処理（Ｓ３０８）では、署名の検証時、デバイス鍵を一時的に新しい世代の鍵に更新を行って検証に成功した場合は、更新鍵生成部４０３は署名の検証時

に生成した新しい世代の鍵を新たなデバイス鍵として管理データベース４０６のデバイス鍵管理テーブル５０２に格納すると共に、更新前のデバイス鍵を削除する。

【００３５】

次に、マスター鍵の有効期限に従って、鍵管理サーバ１０１および通信機器１０２においてマスター鍵を自動的に更新する場合の動作について説明する。

鍵管理サーバ１０１は、鍵管理データベース２０７のマスター鍵管理テーブル３０２において、マスター鍵を有効期限と共に管理している。有効期限を経過した場合は、更新鍵生成部２０４はマスター鍵を更新し、鍵管理データベース２０７のマスター鍵管理テーブル３０２に格納すると共に、更新前の該当マスター鍵を削除する。

同様に、通信機器１０２において、管理データベース４０６のマスター鍵管理テーブル５０３において、マスター鍵を有効期限と共に管理している。有効期限を経過した場合は、更新鍵生成部４０３はマスター鍵を更新し、管理データベース４０６のマスター鍵管理テーブル５０３に格納すると共に、更新前のマスター鍵を削除する。

【００３６】

以上のように、鍵管理サーバ１０１は、通信機器１０２との間で予め共有しておいた鍵（デバイス鍵）を用いてマスター鍵を配布し、鍵管理サーバ１０１と通信機器１０２の間でデバイス鍵の世代に矛盾が生じていた場合修正する。そのため、通信機器１０２がデバイス鍵一括更新命令６００やデバイス鍵個別更新命令７００の受信に失敗していたとしてもデバイス鍵を更新し、事前共有鍵の繰り返し利用に起因する事前共有鍵の解読による通信内容の漏洩を防止することができる。

【００３７】

実施の形態３．

実施の形態３では、鍵管理サーバ１０１からのマスター鍵一括更新命令９００またはマスター鍵個別更新命令１０００の配布による、通信機器１０２同士の間の暗号化通信に用いる暗号鍵（マスター鍵）の更新と、鍵管理サーバ１０１と通信機器１０２の間の暗号化通信に用いる共有鍵（デバイス鍵）の更新とについて説明する。

【００３８】

まず、マスター鍵更新命令の配布による通信機器１０２同士の間の共有鍵（マスター鍵）の更新およびデバイス鍵の更新の動作の概要について説明する。

マスター鍵の更新は、マスター鍵一括更新命令９００を用いて全てのマスター鍵を一括更新する方法と、マスター鍵個別更新命令１０００を用いて特定のマスター鍵のみを更新する方法の二通りがある。マスター鍵一括更新命令９００またはマスター鍵個別更新命令１０００を受信した通信機器１０２は、これらの命令の正当性を検証する際、鍵管理サーバ１０１と共有するデバイス鍵に世代のずれが生じていることを検出した場合、必要に応じてデバイス鍵の更新処理を行う。さらに、これらの命令にマスター鍵の有効期限が記載されていた場合、鍵管理サーバ１０１と通信機器１０２において、有効期限に従って自動的にマスター鍵の更新を行う。

【００３９】

図１９は図１に示したシステム構成において、全てのマスター鍵を一括に更新する際のデータの流れを示した図である。

鍵管理サーバ１０１は、全てのマスター鍵の一括更新を指示する命令を作成し、各々の通信機器１０２が命令の正当性を検証するための電子署名集合を付与して、マスター鍵一括更新命令９００を作成する。次に、鍵管理サーバ１０１は、ネットワーク１０３を介して、マスター鍵一括更新命令９００を全ての通信機器１０２に向けて送信する。そして、鍵管理サーバ１０１は、全てのマスター鍵を更新する。一方、通信機器１０２は、ネットワーク１０３を介して、マスター鍵一括更新命令９００を受信し、命令に含まれる電子署名集合を検証して命令の正当性を確認し、マスター鍵の更新を行う。マスター鍵一括更新命令９００の正当性を検証する際、鍵管理サーバ１０１と共有するデバイス鍵に世代のずれが生じていることを検出した場合、必要に応じてデバイス鍵の更新処理を行う。

【００４０】

次に、図２０に基づき、鍵管理サーバ１０１が配布するマスター鍵一括更新命令９００について説明する。
図２０は、図１９におけるマスター鍵一括更新命令９００のデータ形式を示した図である。
図２０において、マスター鍵一括更新命令９００は、データ種別９０１、マスター鍵一括更新命令情報９０２、電子署名集合９０３を備える。
データ種別９０１は命令データの種類がマスター鍵一括更新命令であることを示すフラグである。マスター鍵一括更新命令情報９０２は全ての通信機器１０２においてマスター鍵を更新するための具体的な指示内容である。電子署名集合９０３はこのマスター鍵一括更新命令９００が鍵管理サーバ１０１で作成された正規命令であることを確認するために、宛先である通信機器１０２毎に作成された個別電子署名９０４の集合である。個別電子署名９０４は各々の通信機器１０２が検証可能な電子署名である。
マスター鍵一括更新命令情報９０２は、更新後世代番号９１１、有効期限９１２を備える。更新後世代番号９１１は何世代目のマスター鍵に更新すればよいかを示す世代番号である。有効期限９１２は更新後のマスター鍵に有効期限を設定する場合に指定する日時であり、有効期限を設定しない場合は省略可能である。
個別電子署名９０４は、デバイスＩＤ９２１、署名鍵世代番号９２２、署名値９２３を備える。デバイスＩＤ９２１はその個別電子署名９０４が対象とする通信機器１０２を示す、機器毎に異なる値である。署名鍵世代番号９２２は署名を生成する際に用いたデバイス鍵の世代番号である。署名値９２３はデバイスＩＤ９２１の通信機器１０２に対応する署名鍵世代番号９２２のデバイス鍵を用いて、データ種別９０１およびマスター鍵一括更新命令情報９０２に対して施された署名である。
【００４１】
図２１は図１に示したシステム構成において、特定のマスター鍵のみを個別に更新する際のデータの流れを示した図である。
鍵管理サーバ１０１は、特定のマスター鍵の個別更新を指示する命令を作成し、該当する通信機器１０２が命令の正当性を検証するための電子署名集合を付与して、マスター鍵個別更新命令１０００を作成する。次に、鍵管理サーバ１０１は、ネットワーク１０３を介して、マスター鍵個別更新命令１０００を該当する通信機器１０２に向けて送信する。そして、鍵管理サーバ１０１は、該当するマスター鍵を更新する。一方、通信機器１０２は、ネットワーク１０３を介して、マスター鍵個別更新命令１０００を受信し、命令が自分宛であるかどうか確認し、命令に含まれる電子署名集合を検証して命令の正当性を確認し、マスター鍵の更新を行う。マスター鍵個別更新命令１０００の正当性を検証する際、鍵管理サーバ１０１と共有するデバイス鍵に世代のずれが生じていることを検出した場合、必要に応じてデバイス鍵の更新処理を行う。
【００４２】
次に、図２２に基づき、鍵管理サーバ１０１が配布するマスター鍵個別更新命令１０００について説明する。
図２２は、図２１におけるマスター鍵個別更新命令１０００のデータ形式を示した図である。
図２２において、マスター鍵個別更新命令１０００は、データ種別１００１、マスター鍵個別更新命令情報１００２、電子署名集合１００３を備える。
データ種別１００１は命令データの種類がマスター鍵個別更新命令であることを示すフラグである。マスター鍵個別更新命令情報１００２は特定のマスター鍵を更新するための具体的な指示内容である。電子署名集合１００３はこのマスター鍵個別更新命令１０００が鍵管理サーバ１０１で作成された正規命令であることを確認するために、宛先である通信機器１０２毎に作成された個別電子署名１００４の集合である。個別電子署名１００４は各々の通信機器１０２が検証可能な電子署名である。ここで、マスター鍵個別更新命令は、同一のマスター鍵を使用する通信機器１０２全てへ送信するため、宛先は複数であり、署名値１０２３も複数になる。

マスター鍵個別更新命令情報１００２は、マスター鍵ＩＤ１０１１、更新後世代番号１０１２、有効期限１０１３を備える。マスター鍵ＩＤ１０１１は鍵更新を指示するマスター鍵を示す、鍵毎に異なる値である。更新後世代番号１０１２は何世代目のマスター鍵に更新すればよいかを示す世代番号である。有効期限１０１３は更新後のマスター鍵に有効期限を設定する場合に指定する日時であり、有効期限を設定しない場合は省略可能である。

個別電子署名１００４は、デバイスＩＤ１０２１、署名鍵世代番号１０２２、署名値１０２３を備える。デバイスＩＤ１０２１はその個別署名１００４が対象とする通信機器１０２を示す、機器毎に異なる値である。署名鍵世代番号１０２２は署名を生成する際に用いたデバイス鍵の世代番号である。署名値１０２３はデバイスＩＤ１０２１の通信機器１０２に対応する署名鍵世代番号１０２２のデバイス鍵を用いて、データ種別１００１およびマスター鍵個別更新命令情報１００２に対して施された署名である。

【００４３】

次に、図２３に基づき、実施の形態３における鍵管理サーバ１０１の機能について説明する。

図２３は実施の形態３における鍵管理サーバ１０１の機能ブロック図である。実施の形態３における鍵管理サーバ１０１は、実施の形態２における鍵管理サーバ１０１に加え、マスター鍵更新命令作成部２１０を備える。

マスター鍵更新命令作成部２１０は、マスター鍵一括更新命令９００やマスター鍵個別更新命令１０００を処理装置により作成する。

実施の形態３における鍵管理データベース２０７は、実施の形態２における鍵管理データベース２０７と同一である。

【００４４】

次に、図２４に基づき、実施の形態３における通信機器１０２の機能について説明する。

図２４は実施の形態３における通信機器１０２の機能ブロック図である。実施の形態３における通信機器１０２は、実施の形態２における通信機器１０２に加え、マスター鍵更新命令解釈部４０９を備える。

マスター鍵更新命令解釈部４０９は、データ受信部４０１で受信したマスター鍵一括更新命令９００やマスター鍵個別更新命令１０００を処理装置により解釈し、更新鍵生成部４０３にマスター鍵を更新させる。

実施の形態３における管理データベース４０６は、実施の形態２における管理データベース４０６と同一である。

【００４５】

次に動作について説明する。

まず、マスター鍵を一括更新する場合の動作について説明する。図２５は、マスター鍵を一括更新する場合の通信システムの動作を示すフローチャートである。

マスター鍵一括更新命令作成処理（Ｓ４０１）では、鍵管理サーバ１０１のマスター鍵更新命令作成部２１０は、マスター鍵一括更新命令９００を作成する。この際、署名値計算部２０６は、鍵管理データベース２０７のデバイス鍵管理テーブル３０１で管理する全てのデバイス鍵を入力として、データ種別９０１とマスター鍵一括更新命令情報９０２に対する署名値９２３を通信機器１０２毎に生成する。

データ送信処理（Ｓ４０２）では、データ送信部２０２は、マスター鍵一括更新命令９００を全ての通信機器１０２へ送信する。

サーバ側マスター鍵更新処理（Ｓ４０３）では、マスター鍵一括更新命令９００の送信に成功した後、更新鍵生成部２０４は、一方向性関数により全てのマスター鍵を更新し、鍵管理データベース２０７のマスター鍵管理テーブル３０２に格納すると共に、更新前のマスター鍵全てを削除する。

データ受信処理（Ｓ４０４）では、通信機器１０２のデータ受信部４０１は、マスター鍵一括更新命令９００を受信する。マスター鍵更新命令解釈部４０９は、マスター鍵一括

更新命令９００のデータ種別９０１により、受信した情報がマスター鍵一括更新命令９００であることを認識する。

署名判定処理（Ｓ４０５）では、署名値検証部４０５は、管理データベース４０６のデバイスＩＤ管理テーブル５０１で管理するデバイスＩＤを用いて、電子署名集合９０３から自分宛の個別電子署名９０４を選択する。署名値検証部４０５は、管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵を入力として、データ種別９０１とマスター鍵一括更新命令情報９０２に対する署名値を計算し、自分宛の個別電子署名９０４の署名値９２３と比較して、命令の正当性を確認する。この時、署名に用いられたデバイス鍵の世代番号９２２が管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵の世代番号より新しい場合、署名値検証部４０５は、更新鍵生成部４０３に一時的に新しい世代の鍵を生成させて確認する。一方、署名に用いられたデバイス鍵の世代番号９２２が管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵の世代番号より古い場合、署名値検証部４０５は、不正な署名と判定する。

署名の検証に成功した場合（Ｓ４０５でＹＥＳ）、マスター鍵更新命令解釈部４０９は（Ｓ４０６）へ進む。一方、署名の検証に失敗した場合（Ｓ４０５でＮＯ）、マスター鍵更新命令解釈部４０９はマスター鍵一括更新命令９００を正当でないと判断し、処理を終了する。

端末側マスター鍵更新処理（Ｓ４０６）では、署名の検証に成功した場合、更新鍵生成部４０３は、鍵管理サーバ１０１と同一の一方向性関数により管理データベース４０６のマスター鍵管理テーブル５０３に格納されている全てのマスター鍵を更新し、管理データベース４０６のマスター鍵管理テーブル５０３に格納すると共に、更新前のマスター鍵を削除する。

端末側デバイス鍵更新処理（Ｓ４０７）では、署名の検証時、デバイス鍵を一時的に新しい世代の鍵に更新を行って検証に成功した場合は、更新鍵生成部４０３は署名の検証時に生成した新しい世代の鍵を新たなデバイス鍵として管理データベース４０６のデバイス鍵管理テーブル５０２に格納すると共に、更新前のデバイス鍵を削除する。

【００４６】

次に特定のマスター鍵のみを更新する場合の動作について説明する。図２６は、特定のマスター鍵のみを更新する場合の通信システムの動作を示すフローチャートである。

マスター鍵個別更新命令作成処理（Ｓ５０１）では、鍵管理サーバ１０１のマスター鍵更新命令作成部２１０は、マスター鍵個別更新命令１０００を作成する。署名値計算部２０６は、鍵管理データベース２０７のデバイス鍵管理テーブル３０１で管理する宛先通信機器１０２のデバイス鍵を入力として、データ種別１００１とマスター鍵個別更新命令情報１００２に対する署名値１０２３を通信機器１０２毎に生成する。

データ送信処理（Ｓ５０２）では、データ送信部２０２は、マスター鍵個別更新命令１０００を該当する通信機器１０２へ送信する。該当する通信機器１０２とは、更新対象のマスター鍵を使用する（利用する）通信機器１０２である。

サーバ側デバイス鍵更新処理（Ｓ５０３）では、マスター鍵個別更新命令１０００の送信に成功した後、更新鍵生成部２０４は、一方向性関数により該当するマスター鍵を更新し、鍵管理データベース２０７のマスター鍵管理テーブル３０２に格納すると共に、更新前の該当マスター鍵を削除する。

データ受信処理（Ｓ５０４）では、通信機器１０２のデータ受信部４０１は、マスター鍵個別更新命令１０００を受信する。マスター鍵更新命令解釈部４０９は、マスター鍵個別更新命令１０００のデータ種別１００１により、受信した情報がマスター鍵個別更新命令１０００であることを認識する。

宛先判定処理（Ｓ５０５）では、マスター鍵更新命令解釈部４０９は、管理データベース４０６のマスター鍵管理テーブル５０３で管理するマスター鍵ＩＤとマスター鍵個別更新命令１０００に含まれるマスター鍵ＩＤ１０１１とが一致するか確認してマスター鍵個別更新命令１０００が自分宛か否か確認する。

マスター鍵個別更新命令１０００が自分宛である場合（Ｓ５０５でＹＥＳ）、マスター鍵更新命令解釈部４０９は（Ｓ５０６）へ進む。一方、マスター鍵個別更新命令１０００が自分宛でない場合（Ｓ５０５でＮＯ）、マスター鍵更新命令解釈部４０９はマスター鍵個別更新命令１０００を無視し、処理を終了する。

署名判定処理（Ｓ５０６）では、マスター鍵個別更新命令１０００が自分宛である場合は、署名値検証部４０５は、管理データベース４０６のデバイスＩＤ管理テーブル５０１で管理するデバイスＩＤを用いて、電子署名集合１００３から自分宛の個別電子署名１００４を選択する。署名値検証部４０５は、管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵を入力として、データ種別１００１とマスター鍵個別更新命令情報１００２に対する署名値を計算し、マスター鍵個別更新命令１０００から選択した署名値１０２３と比較して、命令の正当性を確認する。マスター鍵個別更新命令１０００の正当性を確認する時、署名に用いられたデバイス鍵の世代番号１０２２が管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵の世代番号より新しい場合、署名値検証部４０５は、更新鍵生成部４０３に一時的に新しい世代の鍵を生成させて確認する。署名に用いられたデバイス鍵の世代番号１０２２が管理データベース４０６のデバイス鍵管理テーブル５０２で管理するデバイス鍵の世代番号より古い場合、署名値検証部４０５は、不正な署名と判定する。

署名の検証に成功した場合（Ｓ５０６でＹＥＳ）、マスター鍵更新命令解釈部４０９は（Ｓ５０７）へ進む。一方、署名の検証に失敗した場合（Ｓ５０６でＮＯ）、マスター鍵更新命令解釈部４０９はマスター鍵個別更新命令１０００を正当でないと判断し、処理を終了する。

端末側マスター鍵更新処理（Ｓ５０７）では、署名の検証に成功した場合、更新鍵生成部４０３は、鍵管理サーバ１０１と同一の一方向性関数により該当するマスター鍵を更新し、管理データベース４０６のマスター鍵管理テーブル５０３に格納すると共に、更新前のマスター鍵を削除する。

端末側デバイス鍵更新処理（Ｓ５０８）では、署名の検証時、デバイス鍵を一時的に新しい世代の鍵に更新を行って検証に成功した場合は、更新鍵生成部４０３は署名の検証時に生成した新しい世代の鍵を新たなデバイス鍵として管理データベース４０６のデバイス鍵管理テーブル５０２に格納すると共に、更新前のデバイス鍵を削除する。

【００４７】

次に、マスター鍵の有効期限に従って、鍵管理サーバ１０１および通信機器１０２においてマスター鍵を自動的に更新する場合の動作について説明する。

鍵管理サーバ１０１は、鍵管理データベース２０７のマスター鍵管理テーブル３０２において、マスター鍵を有効期限と共に管理している。有効期限を経過した場合は、更新鍵生成部２０４はマスター鍵を更新し、鍵管理データベース２０７のマスター鍵管理テーブル３０２に格納すると共に、更新前の該当マスター鍵を削除する。

同様に、通信機器１０２において、管理データベース４０６のマスター鍵管理テーブル５０３において、マスター鍵を有効期限と共に管理している。有効期限を経過した場合は、更新鍵生成部４０３はマスター鍵を更新し、管理データベース４０６のマスター鍵管理テーブル５０３に格納すると共に、更新前のマスター鍵を削除する。

【００４８】

以上のように、鍵管理サーバ１０１の指示によって、通信機器１０２は他の通信機器１０２との間で予め共有しておいた鍵（マスター鍵）を更新するので、事前共有鍵の繰り返し利用に起因する事前共有鍵の解読による通信内容の漏洩を防止することができる。また、マスター鍵を更新する際、更新する鍵自体をネットワーク１０３経由で配布しないので、暗号化して配布されるマスター鍵の解読による通信内容の漏洩を防止することができる。事前共有するデバイス鍵を用いた電子署名値の計算、一方向性関数を用いた鍵更新を行っているので、Ｄｉｆｆｉｅ−Ｈｅｌｌｍａｎ鍵交換方式の様な複雑な演算や公開鍵暗号アルゴリズムなどとの組合せ利用を不要として、マスター鍵の更新を行うことができる。一方向性関数を用いてマスター鍵を更新し、更新前のマスター鍵を削除しているので、最

新のマスター鍵の解読による過去の通信内容の漏洩を防止することができる。さらに、鍵管理サーバ１０１と通信機器１０２の間でデバイス鍵の世代に矛盾が生じていた場合修正するので、通信機器１０２がマスター鍵一括更新命令９００やマスター鍵個別更新命令１０００の受信に失敗していたとしてもデバイス鍵を更新し、事前共有鍵の繰り返し利用に起因する事前共有鍵の解読による通信内容の漏洩を防止することができる。

【００４９】

実施の形態４．

実施の形態４では、通信機器１０２同士の間の機器間通信データ１１００のやり取りによる、通信機器１０２同士の間の暗号化通信に用いる暗号鍵（マスター鍵）の更新について説明する。

【００５０】

まず、機器間通信データ１１００のやり取りによる通信機器１０２同士の間の共有鍵（マスター鍵）の更新の動作の概要について説明する。

図２７は図１に示したシステム構成において、機器間通信データ１１００のやり取りによってマスター鍵を更新する際のデータの流れを示した図である。

通信機器１０２同士が通信を行う場合、第三者による盗聴や改ざんを防止するため、機器間通信データ１１００に対して暗号化や電子署名の付与を行う。送信者側の通信機器１０２は、受信者側の通信機器１０２との間で共有するマスター鍵を用いて暗号化や電子署名の生成を行い、機器間通信データ１１００を作成する。次に、送信者側の通信機器１０２は、ネットワーク１０３を介して、機器間通信データ１１００を受信者側の通信機器１０２に向けて送信する。一方、受信者側の通信機器１０２は、ネットワーク１０３を介して、機器間通信データ１１００を受信し、送信者側の通信機器１０２との間で共有するマスター鍵を用いて、復号や電子署名の検証を行う。この時、受信者側の通信機器１０２は、機器間通信データ１１００に含まれるマスター鍵の世代情報から、送信者側の通信機器１０２との間でマスター鍵の世代が一致しているか否かを確認し、世代のずれが生じていた場合はマスター鍵の更新を行う。

【００５１】

次に、図２８に基づき、通信機器１０２がやり取りする機器間通信データ１１００について説明する。

図２８は、図２７における機器間通信データ１１００のデータ形式を示した図である。

図２８において、機器間通信データ１１００は、保護された通信内容１１０１、マスター鍵情報１１０２、署名値１１０３を備える。

保護された通信内容１１０１は通信機器１０２間でやり取りするデータの内容である。盗聴を防止する必要がある場合は、保護された通信内容１１０１はマスター鍵情報１１０２が示すマスター鍵を用いて暗号化されている。改ざん防止のみで十分な場合は、保護された通信内容１１０１は暗号化されていなくてもよい。マスター鍵情報１１０２は保護された通信内容１１０１の暗号化や電子署名に用いたマスター鍵を指定するための情報である。署名値１１０３はマスター鍵情報１１０２が示すマスター鍵を用いて、保護された通信内容１１０１に対して施された署名である。

マスター鍵情報１１０２は、マスター鍵ＩＤ１１１１、マスター鍵世代番号１１１２、有効期限１１１３を備える。マスター鍵ＩＤ１１１１は暗号化や電子署名に用いられたマスター鍵を示す、鍵毎に異なる値である。マスター鍵世代番号１１１２はマスター鍵ＩＤ１１１１のマスター鍵の現時点での世代を示す世代番号である。有効期限１１１３はマスター鍵ＩＤ１１１１かつマスター鍵世代番号１１１２のマスター鍵に設定された有効期限を示す日時であり、有効期限が設定されていない場合は省略可能である。

【００５２】

次に、図２９に基づき、実施の形態４における通信機器１０２の機能について説明する。

図２９は実施の形態４における通信機器１０２の機能ブロック図である。実施の形態４における通信機器１０２は、実施の形態３における通信機器１０２に加え、機器間通信部

４０２、機器間通信データ作成解釈部４１０（マスター鍵世代情報通信部）、署名値生成部４１１、暗号化部４１２を備える。

機器間通信部４０２は、ネットワーク１０３を介して通信装置により他の通信機器１０２との間でデータのやり取りを行う。

機器間通信データ作成解釈部４１０は、機器間通信データ１１００を処理装置により作成する。また、機器間通信データ作成解釈部４１０は、他の通信機器１０２から受信した機器間通信データ１１００を処理装置により解釈し、必要に応じてマスター鍵を更新鍵生成部４０３に更新させる。

署名値生成部４１１は、署名対象のデータに対して、指定された鍵を用いて署名を生成して署名値を処理装置により作成する。

暗号化部４１２は、暗号化対象のデータに対して、指定された鍵を用いて処理装置により暗号化する。

実施の形態４における管理データベース４０６は、実施の形態２～実施の形態３における管理データベース４０６と同一である。

【００５３】

次に動作について説明する。図３０は、機器間通信データ１１００のやり取りによってマスター鍵を更新する場合の通信システムの動作を示すフローチャートである。

機器間通信データ作成処理（Ｓ６０１）では、送信者側の通信機器１０２の機器間通信データ作成解釈部４１０は、機器間通信データ１１００を作成する。署名値生成部４１１は、管理データベース４０６のマスター鍵管理テーブル５０３で管理する宛先通信機器１０２と共有するマスター鍵を入力として、保護された通信内容１１０１に対する署名値１１０３を生成する。暗号化を行う場合、暗号化部４１２は、管理データベース４０６のマスター鍵管理テーブル５０３で管理する宛先通信機器１０２と共有するマスター鍵を入力として、保護された通信内容１１０１を暗号化する。

データ送信処理（Ｓ６０２）では、機器間通信部４０２は、機器間通信データ１１００を通信相手の通信機器１０２へ送信する。

データ受信処理（Ｓ６０３）では、受信者側の通信機器１０２の機器間通信部４０２は、機器間通信データ１１００を受信する。

マスター鍵検索処理（Ｓ６０４）では、機器間通信データ作成解釈部４１０は、マスター鍵ＩＤ１１１１と一致するマスター鍵を、管理データベース４０６のマスター鍵管理テーブル５０３で管理するマスター鍵から探し出す。

マスター鍵ＩＤ１１１１と一致するマスター鍵が見つかった場合（Ｓ６０４でＹＥＳ）、機器間通信データ作成解釈部４１０は（Ｓ６０５）へ進む。一方、マスター鍵ＩＤ１１１１と一致するマスター鍵が見つからない場合（Ｓ６０４でＮＯ）、マスター鍵更新命令解釈部４０９は機器間通信データ１１００を無視し、処理を終了する。

復号署名判定処理（Ｓ６０５）では、保護された通信内容１１０１が暗号化されていた場合は、復号部４０４はマスター鍵を指定して保護された通信内容１１０１の復号を行う。また、署名値検証部４０５は、マスター鍵を入力として、保護された通信内容１１０１に対する署名値を計算し、機器間通信データ１１００の署名値１１０３と比較して、通信内容が改ざんされていないことを確認する。復号や署名の検証を行った時、署名や暗号化に用いられたマスター鍵の世代番号１１１２が管理データベース４０６のマスター鍵管理テーブル５０３で管理するマスター鍵の世代番号より新しい場合、署名値検証部４０５は、更新鍵生成部４０３に一時的に新しい世代の鍵を生成させて確認する。署名や暗号化に用いられたマスター鍵の世代番号１１１２が管理データベース４０６のマスター鍵管理テーブル５０３で管理するマスター鍵の世代番号より古い場合、署名値検証部４０５は、不正な署名と判定する。

署名の検証に成功した場合（Ｓ６０５でＹＥＳ）、機器間通信データ作成解釈部４１０は（Ｓ６０６）へ進む。一方、署名の検証に失敗した場合（Ｓ６０５でＮＯ）、機器間通信データ作成解釈部４１０は機器間通信データ１１００を正当でないと判断し、処理を終了する。

マスター鍵更新処理（Ｓ６０６）では、署名の検証に成功した場合であって、署名の検証時、マスター鍵を一時的に新しい世代の鍵に更新を行って検証に成功した場合は、更新鍵生成部４０３は署名の検証時に生成した新しい世代の鍵を新たなマスター鍵として管理データベース４０６のマスター鍵管理テーブル５０３に格納すると共に、更新前のマスター鍵を削除する。

【００５４】

以上のように、通信機器１０２は、鍵管理サーバ１０１の指示がなくても、通信機器１０２同士の通信機器１０２間のデータのやり取りによって、通信機器１０２同士の間でマスター鍵の世代に矛盾が生じていた場合修正する。そのため、通信機器１０２がマスター鍵一括更新命令やマスター鍵個別更新命令の受信に失敗していたとしてもマスター鍵を更新することができる。したがって、事前共有鍵の繰り返し利用に起因する事前共有鍵の解読による通信内容の漏洩を防止することができる。また、マスター鍵を更新する際、更新する鍵自体をネットワーク１０３経由で配布しないので、暗号化して配布されるマスター鍵の解読による通信内容の漏洩を防止することができる。事前共有するマスター鍵を用いた電子署名値の計算、一方向性関数を用いた鍵更新を行っているので、Ｄｉｆｆｉｅ−Ｈｅｌｌｍａｎ鍵交換方式の様な複雑な演算や公開鍵暗号アルゴリズムなどと組合せ利用を不要として、マスター鍵の更新を行うことができる。一方向性関数を用いてマスター鍵を更新し、更新前のマスター鍵を削除しているので、最新のマスター鍵の解読による過去の通信内容の漏洩を防止することができる。

【００５５】

実施の形態５．

実施の形態５では、通信機器１０２同士の間で鍵管理サーバ１０１から受信したデバイス鍵一括更新命令を転送することによる、鍵管理サーバ１０１と通信機器１０２の間の暗号化通信に用いる共有鍵（デバイス鍵）の更新について説明する。

【００５６】

まず、鍵管理サーバ１０１から受信したデバイス鍵一括更新命令を転送することによる鍵管理サーバ１０１と通信機器１０２の間の共有鍵（デバイス鍵）の更新の動作の概要について説明する。

図３１は図１に示したシステム構成において、デバイス鍵一括更新命令６００を転送することによってマスター鍵を更新する際のデータの流れを示した図である。

通信機器１０２は、鍵管理サーバ１０１から送信されたデバイス鍵一括更新命令６００を受信した場合、これらの命令を一時的に通信機器１０２の内部に保管する。通信機器１０２は、他の通信機器１０２との間でデータのやり取りを行う際、あるいは任意のタイミングで、保管しておいたデバイス鍵一括更新命令６００を他の通信機器１０２に転送する。

他の通信機器１０２から転送されたデバイス鍵一括更新命令６００を受信した通信機器１０２は、鍵管理サーバ１０１から受信した場合と同様に、デバイス鍵一括更新命令６００に含まれる電子署名集合を検証してデバイス鍵一括更新命令６００の正当性を確認し、デバイス鍵の更新を行う。また、このデバイス鍵一括更新命令６００を一時的に通信機器１０２の内部に保管し、さらに別の通信機器１０２に転送してもよい。

【００５７】

次に、図３２に基づき、実施の形態５における通信機器１０２の機能について説明する。

図３２は実施の形態５における通信機器１０２の機能ブロック図である。実施の形態５における通信機器１０２は、実施の形態４における通信機器１０２に加え、デバイス鍵更新命令転送部４２１（デバイス鍵機器間通信部）を備える。

デバイス鍵更新命令転送部４２１は、受信したデバイス鍵一括更新命令６００を一時的に通信機器１０２内部に保管して、他の通信機器１０２へ通信装置により転送する。

実施の形態５における管理データベース４０６は、実施の形態２から実施の形態４までにおける管理データベース４０６と同一である。

【００５８】

次に動作について説明する。図３３は、デバイス鍵一括更新命令６００を転送することによってデバイス鍵を更新する場合の通信システムの動作を示すフローチャートである。

デバイス鍵一括更新命令保管処理（Ｓ７０１）では、転送元の通信機器１０２は、鍵管理サーバ１０１から送信されたデバイス鍵一括更新命令６００を受信した場合は、実施の形態１で説明した手順（（Ｓ１０４）から（Ｓ１０６）まで）に従って命令の正当性を確認し、デバイス鍵を更新する。その後、転送元の通信機器１０２のデバイス鍵更新命令転送部４２１は、受信したデバイス鍵一括更新命令６００を一時的に通信機器１０２内部（記憶装置）に保管する。

データ転送処理（Ｓ７０２）では、他の通信機器１０２との間で通信が発生した場合、機器間通信部４０２は、デバイス鍵一括更新命令６００を通信相手の通信機器１０２へ送信する。あるいは、デバイス鍵更新命令転送部４２１は、任意のタイミングで他の通信機器１０２との間で新たに通信を開始し、機器間通信部４０２に、デバイス鍵一括更新命令６００を通信相手の通信機器１０２へ送信させる。

転送データ受信処理（Ｓ７０３）では、転送先の通信機器１０２の機器間通信部４０２は、デバイス鍵一括更新命令６００を受信する。デバイス鍵更新命令転送部４２１は、デバイス鍵一括更新命令６００のデータ種別６０１により、受信した情報がデバイス鍵一括更新命令６００であることを認識する。

転送データ解釈処理（Ｓ７０４）では、デバイス鍵更新命令転送部４２１は、受信したデバイス鍵一括更新命令６００をデバイス鍵更新命令解釈部４０７に引き渡し、鍵管理サーバ１０１から受信した場合と同様の処理（（Ｓ１０５）と（Ｓ１０６））を行う。さらに、デバイス鍵更新命令転送部４２１は、転送されたデバイス鍵一括更新命令６００を一時的に通信機器１０２内部に保管してもよい。

【００５９】

以上のように、通信機器１０２同士の間のデバイス鍵一括更新命令６００の転送によって、通信機器１０２は鍵管理サーバ１０１との間で予め共有しておいた鍵（デバイス鍵）を更新する。そのため、事前共有鍵（デバイス鍵）の繰り返し利用に起因する事前共有鍵の解読による通信内容の漏洩を防止することができる。また、デバイス鍵を更新する際、更新する鍵自体をネットワーク１０３経由で配布しないので、暗号化して配布されるデバイス鍵の解読による通信内容の漏洩を防止することができる。事前共有するデバイス鍵を用いた電子署名値の計算、一方向性関数を用いた鍵更新を行っているので、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換方式の様な複雑な演算や公開鍵暗号アルゴリズムなどとの組合せ利用を不要として、デバイス鍵の更新を行うことができる。一方向性関数を用いてデバイス鍵を更新し、更新前のデバイス鍵を削除しているので、最新のデバイス鍵の解読による過去の通信内容の漏洩を防止することができる。さらに、鍵管理サーバ１０１と通信機器１０２の間でデバイス鍵の世代に矛盾が生じていた場合修正するので、通信機器１０２がデバイス鍵一括更新命令６００やデバイス鍵個別更新命令７００の受信に失敗していたとしてもデバイス鍵を更新し、事前共有鍵の繰り返し利用に起因する事前共有鍵の解読による通信内容の漏洩を防止することができる。

【００６０】

実施の形態６．

実施の形態６では、通信機器１０２同士の間で鍵管理サーバ１０１から受信したマスター鍵一括更新命令９００を転送することによる、通信機器１０２同士の間の暗号化通信に用いる暗号鍵（マスター鍵）の更新について説明する。

【００６１】

まず、鍵管理サーバ１０１から受信したマスター鍵一括更新命令９００を転送することによる通信機器１０２同士の間の共有鍵（マスター鍵）の更新の動作の概要について説明する。

図３４は図１に示したシステム構成において、マスター鍵一括更新命令９００を転送することによってマスター鍵を更新する際のデータの流れを示した図である。

通信機器１０２は、鍵管理サーバ１０１から送信されたマスター鍵一括更新命令９００を受信した場合、これらの命令を一時的に通信機器１０２の内部に保管する。通信機器１０２は、他の通信機器１０２との間でデータのやり取りを行う際、あるいは任意のタイミングで、保管しておいたマスター鍵一括更新命令９００を他の通信機器１０２に転送する。

他の通信機器１０２から転送されたマスター鍵一括更新命令９００を受信した通信機器１０２は、鍵管理サーバ１０１から受信した場合と同様に、マスター鍵一括更新命令９００に含まれる電子署名集合を検証してマスター鍵一括更新命令９００の正当性を確認し、マスター鍵の更新を行う。また、このマスター鍵一括更新命令９００を一時的に通信機器１０２の内部に保管し、さらに別の通信機器１０２に転送してもよい。

【００６２】

次に、図３５に基づき、実施の形態６における通信機器１０２の機能について説明する。

図３５は実施の形態６における通信機器１０２の機能ブロック図である。実施の形態６における通信機器１０２は、実施の形態５における通信機器１０２に加え、マスター鍵更新命令転送部４２２（マスター鍵機器間通信部）を備える。

マスター鍵更新命令転送部４２２は、受信したマスター鍵一括更新命令９００を一時的に通信機器１０２内部に保管して、他の通信機器１０２へ通信装置により転送する。

実施の形態６における管理データベース４０６は、実施の形態２から実施の形態５までにおける管理データベース４０６と同一である。

【００６３】

次に動作について説明する。図３６は、マスター鍵一括更新命令９００を転送することによってマスター鍵を更新する場合の通信システムの動作を示すフローチャートである。

マスター鍵一括更新命令保管処理（Ｓ８０１）では、転送元の通信機器１０２は、鍵管理サーバ１０１から送信されたマスター鍵一括更新命令９００を受信した場合は、実施の形態３で説明した手順（（Ｓ４０３）から（Ｓ４０７）まで）に従って命令の正当性を確認し、マスター鍵を更新するとともに、必要に応じてデバイス鍵を更新する。その後、転送元の通信機器１０２のマスター鍵更新命令転送部４２２は、受信したマスター鍵一括更新命令９００を一時的に通信機器１０２内部（記憶装置）に保管する。

データ転送処理（Ｓ８０２）では、他の通信機器１０２との間で通信が発生した場合、機器間通信部４０２は、マスター鍵一括更新命令９００を通信相手の通信機器１０２へ送信する。あるいは、マスター鍵更新命令転送部４２２は、任意のタイミングで他の通信機器１０２との間で新たに通信を開始し、機器間通信部４０２に、マスター鍵一括更新命令９００を通信相手の通信機器１０２へ送信させる。

転送データ受信処理（Ｓ８０３）では、転送先の通信機器１０２の機器間通信部４０２は、マスター鍵一括更新命令９００を受信する。マスター鍵更新命令転送部４２２は、マスター鍵一括更新命令９００のデータ種別９０１により、受信した情報がマスター鍵一括更新命令９００であることを認識する。

転送データ解釈処理（Ｓ８０４）では、マスター鍵更新命令転送部４２２は、受信したマスター鍵一括更新命令９００をマスター鍵更新命令解釈部４０９に引き渡し、鍵管理サーバ１０１から受信した場合と同様の処理（（Ｓ４０５）から（Ｓ４０７）まで）を行う。さらに、マスター鍵更新命令転送部４２２は、転送されたマスター鍵一括更新命令９００を一時的に通信機器１０２内部に保管してもよい。

【００６４】

以上のように、通信機器１０２同士の間のマスター鍵一括更新命令９００の転送によって、通信機器１０２は他の通信機器１０２との間で予め共有しておいた鍵（マスター鍵）を更新する。そのため、事前共有鍵（マスター鍵）の繰り返し利用に起因する事前共有鍵の解読による通信内容の漏洩を防止することができる。また、マスター鍵を更新する際、更新する鍵自体をネットワーク１０３経由で配布しないので、暗号化して配布されるマスター鍵の解読による通信内容の漏洩を防止することができる。事前共有するデバイス鍵を

用いた電子署名値の計算、一方向性関数を用いた鍵更新を行っているので、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換方式の様な複雑な演算や公開鍵暗号アルゴリズムなどとの組合せ利用を不要として、マスター鍵の更新を行うことができる。一方向性関数を用いてマスター鍵を更新し、更新前のマスター鍵を削除しているので、最新のマスター鍵の解読による過去の通信内容の漏洩を防止することができる。さらに、鍵管理サーバ１０１と通信機器１０２の間でデバイス鍵の世代に矛盾が生じていた場合修正するので、通信機器１０２がデバイス鍵一括更新命令６００やデバイス鍵個別更新命令７００の受信に失敗していたとしてもデバイス鍵を更新し、事前共有鍵の繰り返し利用に起因する事前共有鍵の解読による通信内容の漏洩を防止することができる。

【００６５】

実施の形態７．

以上の実施の形態１から実施の形態６まででは、鍵管理サーバ１０１から通信機器１０２へ送信する命令の盗聴防止や改ざん防止に共通鍵暗号アルゴリズムを用いていた。そして、鍵管理サーバ１０１と各々の通信機器１０２が共有している共通鍵であるデバイス鍵を用いた暗号化や署名値の計算を行っていた。実施の形態７では、鍵管理サーバ１０１から通信機器１０２へ送信する命令の暗号化や署名値の計算に公開鍵暗号アルゴリズムを用いた場合のデバイス鍵更新命令の配布による鍵管理サーバ１０１と通信機器１０２との間のデバイス鍵の更新について説明する。

【００６６】

まず、デバイス鍵更新命令の配布による鍵管理サーバ１０１と通信機器１０２との間のデバイス鍵の更新の動作の概要について説明する。ここで、デバイス鍵とは、各通信機器１０２の秘密鍵であるデバイス秘密鍵と、そのデバイス秘密鍵と対をなすデバイス公開鍵とである。一方、鍵管理サーバ１０１の秘密鍵と公開鍵とは、サーバ秘密鍵とサーバ公開鍵と呼ぶ。

デバイス鍵の更新は、実施の形態１と同様に、デバイス鍵一括更新命令１２００を用いて全てのデバイス鍵を一括更新する方法と、デバイス鍵個別更新命令１３００を用いて特定の通信機器１０２との間で共有するデバイス鍵のみを更新する方法との二通りがある。さらに、これらの命令（デバイス鍵一括更新命令１２００、デバイス鍵個別更新命令１３００）にデバイス鍵の有効期限が記載されていた場合、鍵管理サーバ１０１と通信機器１０２において、有効期限に従って自動的にデバイス鍵の更新を行う。

【００６７】

図３７は図１に示したシステム構成において、全てのデバイス鍵を一括に更新する際のデータの流れを示した図である。

鍵管理サーバ１０１は、全てのデバイス鍵の一括更新を指示する命令を作成し、各々の通信機器１０２が命令の正当性を検証するための電子署名をサーバ秘密鍵により付与して、デバイス鍵一括更新命令１２００を作成する。次に、鍵管理サーバ１０１は、ネットワーク１０３を介して、デバイス鍵一括更新命令１２００を全ての通信機器１０２に向けて送信する。そして、鍵管理サーバ１０１は、全てのデバイス公開鍵を更新する。一方、通信機器１０２は、ネットワーク１０３を介して、デバイス鍵一括更新命令１２００を受信し、命令に含まれる電子署名を検証して命令の正当性を確認し、デバイス秘密鍵とデバイス公開鍵との更新を行う。

【００６８】

図３８は、デバイス鍵一括更新命令１２００のデータ形式を示した図である。

図３８に基づき、鍵管理サーバ１０１が配布するデバイス鍵一括更新命令１２００について、デバイス鍵一括更新命令６００と異なる部分について説明する。

デバイス鍵一括更新命令１２００は、電子署名１２０３を１つ備えている。つまり、デバイス鍵一括更新命令６００は、通信機器１０２毎に異なる個別電子署名を備えていたが、デバイス鍵一括更新命令１２００は、全ての通信機器１０２に共通の電子署名１２０３を１つ備えている。

電子署名１２０３は、全ての通信機器１０２に共通であるから、デバイスＩＤは備えて

いない。また、電子署名１２０３の署名値１２２２は、鍵管理サーバ１０１の秘密鍵であるサーバ秘密鍵を用いて施された署名である。

【００６９】

図３９は図１に示したシステム構成において、特定のデバイス鍵のみを個別に更新する際のデータの流れを示した図である。

鍵管理サーバ１０１は、特定の通信機器１０２のデバイス鍵の個別更新を指示する命令を作成し、該当する通信機器１０２が命令の正当性を検証するための電子署名をサーバ秘密鍵により付与して、デバイス鍵個別更新命令１３００を作成する。次に、鍵管理サーバ１０１は、ネットワーク１０３を介して、デバイス鍵個別更新命令１３００を該当する通信機器１０２に向けて送信する。そして、鍵管理サーバ１０１は、該当するデバイス公開鍵を更新する。一方、通信機器１０２は、ネットワーク１０３を介して、デバイス鍵個別更新命令１３００を受信し、命令が自分宛であるかどうか確認し、命令に含まれる電子署名を検証して命令の正当性を確認し、デバイス秘密鍵とデバイス公開鍵との更新を行う。

【００７０】

図４０は、デバイス鍵個別更新命令１３００のデータ形式を示した図である。

図４０に基づき、鍵管理サーバ１０１が配布するデバイス鍵個別更新命令１３００について、デバイス鍵個別更新命令７００と異なる部分について説明する。

デバイス鍵個別更新命令１３００の署名値１３２２は、鍵管理サーバ１０１の秘密鍵であるサーバ秘密鍵を用いて施された署名である。

【００７１】

次に、図４１、図４２に基づき、実施の形態７における鍵管理サーバ１０１の機能について説明する。

図４１は実施の形態７における鍵管理サーバ１０１の機能ブロック図である。鍵管理サーバ１０１は、入力インタフェース２０１、データ送信部２０２、更新鍵生成部２２０４、電子署名生成部２２０６、鍵管理データベース２２０７、デバイス鍵更新命令作成部２２０８を備える。入力インタフェース２０１、データ送信部２０２は、実施の形態１における鍵管理サーバ１０１の機能と同一である。

更新鍵生成部２２０４は、所定の方法により現在のデバイス公開鍵から次の世代のデバイス公開鍵を処理装置により生成する。現在のデバイス公開鍵から次の世代のデバイス公開鍵を生成する方法については後述する。

電子署名生成部２２０６は、署名対象のデータに対して、サーバ秘密鍵を用いて署名を生成する。

鍵管理データベース２２０７は、実施の形態７における鍵管理サーバ１０１が管理する必要のある全ての鍵を記憶装置に記憶（管理）する。

デバイス鍵更新命令作成部２２０８は、デバイス鍵一括更新命令１２００やデバイス鍵個別更新命令１３００を処理装置により作成する。

【００７２】

図４２は実施の形態７における鍵管理サーバ１０１内部の鍵管理データベース２２０７が記憶する情報を示す図である。鍵管理データベース２２０７は、サーバ公開鍵ペア管理テーブル３３０１、デバイス公開鍵管理テーブル３３０２、デバイスシード管理テーブル３３０３、サーバシード管理テーブル３３０４を備える。

サーバ公開鍵ペア管理テーブル３３０１は、鍵管理サーバ１０１の公開鍵ペア、即ちサーバ秘密鍵とサーバ公開鍵とを、鍵の世代番号、鍵の有効期限との組合せで管理する。

デバイス公開鍵管理テーブル３３０２は、各々の通信機器１０２のデバイス公開鍵を、通信機器１０２を特定するデバイスＩＤ、鍵の世代番号、鍵の有効期限との組合せで管理する。

デバイスシード管理テーブル３３０３は、デバイス公開鍵を生成する場合に、公開鍵暗号方式の鍵を生成する関数への入力（シード）となるデバイス鍵生成用シードを管理する。デバイスシード管理テーブル３３０３で管理するデバイス鍵生成用シードは、各々の通信機器１０２と予め共有している。

サーバシード管理テーブル３３０４は、サーバ秘密鍵とサーバ公開鍵とを生成する場合に、公開鍵暗号方式の鍵を生成する関数への入力（シード）となるサーバ鍵生成用シードを管理する。サーバシード管理テーブル３３０４で管理するサーバ鍵生成用シードは、各々の通信機器１０２と予め共有している。

【００７３】

次に、図４３、図４４に基づき、実施の形態７における通信機器１０２の機能について説明する。

図４３は実施の形態７における通信機器１０２の機能ブロック図である。通信機器１０２は、データ受信部４０１、更新鍵生成部４４０３、電子署名検証部４４０５、管理データベース４４０６、デバイス鍵更新命令解釈部４４０７を備える。データ受信部４０１は、実施の形態１における通信機器１０２の機能と同一である。

更新鍵生成部４４０３は、所定の方法により現在のデバイス秘密鍵から次の世代のデバイス秘密鍵を処理装置により生成するとともに、現在のデバイス公開鍵から次の世代のデバイス公開鍵を処理装置により生成する。現在のデバイス秘密鍵・デバイス公開鍵から次の世代のデバイス秘密鍵・デバイス公開鍵を生成する方法については後述する。

電子署名検証部４４０５は、署名対象のデータおよび署名値に対して、サーバ公開鍵を用いて処理装置により署名を検証する。

管理データベース４４０６は、通信機器１０２が管理する必要のある全ての情報および鍵を記憶装置に記憶（管理）する。

デバイス鍵更新命令解釈部４４０７はデータ受信部４０１で受信したデバイス鍵一括更新命令１２００やデバイス鍵個別更新命令１３００を解釈し、更新鍵生成部４０３にデバイス秘密鍵とデバイス公開鍵とを更新させる。

【００７４】

図４４は実施の形態７における通信機器１０２内部の管理データベース４４０６が記憶する情報を示す図である。管理データベース４４０６は、デバイスＩＤ管理テーブル５０１、サーバ公開鍵管理テーブル５５０１、デバイス公開鍵ペア管理テーブル５５０２、デバイスシード管理テーブル５３０３、サーバシード管理テーブル５３０４を備える。

サーバ公開鍵管理テーブル５５０１は、サーバの公開鍵を、鍵の世代番号、鍵の有効期限との組合せで管理する。

デバイス公開鍵ペア管理テーブル５５０２は、デバイス公開鍵ペア、即ちデバイス公開鍵とデバイス秘密鍵を、鍵の世代番号、鍵の有効期限との組合せで管理する。

デバイスシード管理テーブル５３０３は、デバイス秘密鍵とデバイス公開鍵とを生成する場合に、公開鍵暗号方式の鍵を生成する関数への入力（シード）となるデバイス鍵生成用シードを管理する。デバイスシード管理テーブル５３０３で管理するデバイス鍵生成用シードは、鍵管理サーバ１０１と予め共有している。

【００７５】

次に動作について説明する。

まず、デバイス鍵を一括更新する場合の動作について説明する。図４５は、デバイス鍵を一括更新する場合の通信システムの動作を示すフローチャートである。

デバイス鍵一括更新命令作成処理（Ｓ９０１）では、鍵管理サーバ１０１のデバイス鍵更新命令作成部２２０８は、デバイス鍵一括更新命令１２００を作成する。この際、電子署名生成部２２０６は、鍵管理データベース２２０７のサーバ公開鍵ペア管理テーブル３３０１で管理するサーバ秘密鍵を入力として、データ種別１２０１とデバイス鍵一括更新命令情報１２０２に対する署名値１２２２を生成する。

データ送信処理（Ｓ９０２）では、データ送信部２０２は、デバイス鍵一括更新命令１２００を全ての通信機器１０２へ送信する。

サーバ側デバイス鍵更新処理（Ｓ９０３）では、更新鍵生成部２２０４は、デバイス鍵一括更新命令１２００の送信に成功した後、一方向関数により鍵管理データベース２２０７のデバイスシード管理テーブル３３０３で管理する全てのデバイス鍵生成用シードを更新して、更新後の各デバイス鍵生成用シードを所定の公開鍵暗号方式の鍵を生成する関数

へ入力して新たなデバイス公開鍵を生成する。そして、更新鍵生成部２２０４は鍵管理データベース２２０７のデバイス公開鍵管理テーブル３３０２に生成したデバイス公開鍵を格納すると共に、前のデバイス公開鍵を全て削除する。

データ受信処理（Ｓ９０４）では、通信機器１０２のデータ受信部４０１は、デバイス鍵一括更新命令１２００を受信する。デバイス鍵更新命令解釈部４４０７は、デバイス鍵一括更新命令１２００のデータ種別１２０１により、受信した情報がデバイス鍵一括更新命令１２００であることを認識する。

署名判定処理（Ｓ９０５）では、電子署名検証部４４０５は、管理データベース４４０６のサーバ公開鍵管理テーブル５５０１で管理するサーバ公開鍵を入力として、電子署名１２０３の署名値１２２２を検証して、デバイス鍵一括更新命令１２００の正当性を確認する。この時、署名に用いられたサーバ秘密鍵の署名鍵世代番号１２２１が管理データベース４４０６のサーバ公開鍵管理テーブル５５０１で管理するサーバ公開鍵の世代番号より古い場合、電子署名検証部４４０５は、不正な署名と判定する。

署名の検証に成功した場合（Ｓ９０５でＹＥＳ）、デバイス鍵更新命令解釈部４４０７は（Ｓ９０６）へ進む。一方、署名の検証に失敗した場合（Ｓ９０５でＮＯ）、デバイス鍵更新命令解釈部４４０７はデバイス鍵一括更新命令１２００を正当でないと判断し、処理を終了する。

端末側デバイス鍵更新処理（Ｓ９０６）では、署名の検証に成功した場合、更新鍵生成部４４０３は、鍵管理サーバ１０１と同一の一方向性関数により管理データベース４４０６のデバイスシード管理テーブル５３０３で管理するデバイス鍵生成用シードを更新して、更新後の各デバイス鍵生成用シードを所定の公開鍵暗号方式の鍵を生成する関数へ入力して新たなデバイス秘密鍵とデバイス公開鍵とを生成する。更新鍵生成部４４０３は、管理データベース４４０６のデバイス公開鍵ペア管理テーブル５５０２に生成したデバイス秘密鍵とデバイス公開鍵とを格納すると共に、更新前のデバイス秘密鍵とデバイス公開鍵とを削除する。

【００７６】

次に特定のデバイス鍵のみを更新する場合の動作について説明する。図４６は、特定のデバイス鍵のみを更新する場合の通信システムの動作を示すフローチャートである。

デバイス鍵個別更新命令作成処理（Ｓ１００１）では、鍵管理サーバ１０１のデバイス鍵更新命令作成部２２０８は、デバイス鍵個別更新命令１３００を作成する。この際、電子署名生成部２２０６は、鍵管理データベース２２０７のサーバ公開鍵ペア管理テーブル３３０１で管理するサーバ秘密鍵を入力として、データ種別１３０１とデバイス鍵個別更新命令情報１３０２に対する署名値１３２２を生成する。

データ送信処理（Ｓ１００２）では、データ送信部２０２は、デバイス鍵個別更新命令１３００を該当する通信機器１０２へ送信する。

サーバ側デバイス鍵更新処理（Ｓ１００３）では、更新鍵生成部２２０４は、デバイス鍵個別更新命令１３００の送信に成功した後、一方向関数により鍵管理データベース２２０７のデバイスシード管理テーブル３３０３で管理する該当の通信機器１０２と共有したデバイス鍵生成用シードを更新して、更新後のデバイス鍵生成用シードに基づき新たなデバイス公開鍵を生成する。そして、更新鍵生成部２２０４は鍵管理データベース２２０７のデバイス公開鍵管理テーブル３３０２の該当する通信機器１０２の欄に生成したデバイス公開鍵を格納すると共に、前のデバイス公開鍵を削除する。

データ受信処理（Ｓ１００４）では、通信機器１０２のデータ受信部４０１は、デバイス鍵個別更新命令１３００を受信する。デバイス鍵更新命令解釈部４４０７は、デバイス鍵個別更新命令１３００のデータ種別１３０１により、受信した情報がデバイス鍵個別更新命令１３００であることを認識する。

宛先判定処理（Ｓ１００５）では、デバイス鍵更新命令解釈部４４０７は、管理データベース４４０６のデバイスＩＤ管理テーブル５０１で管理するデバイスＩＤとデバイス鍵個別更新命令１３００に含まれるデバイスＩＤ１３１１とが一致するか確認して、デバイス鍵個別更新命令１３００が自分宛か否か確認する。

デバイス鍵個別更新命令１３００が自分宛である場合（Ｓ１００５でＹＥＳ）、デバイス鍵更新命令解釈部４４０７は（Ｓ１００６）へ進む。一方、デバイス鍵個別更新命令１３００が自分宛でない場合（Ｓ１００５でＮＯ）、デバイス鍵更新命令解釈部４４０７はデバイス鍵個別更新命令１３００を無視し、処理を終了する。

署名判定処理（Ｓ１００６）では、デバイス鍵個別更新命令１３００が自分宛である場合は、電子署名検証部４４０５は、管理データベース４４０６のサーバ公開鍵管理テーブル５５０１で管理するサーバ公開鍵を入力として、デバイス鍵個別更新命令１３００の署名値１３２２を検証して、デバイス鍵個別更新命令１３００の正当性を確認する。デバイス鍵個別更新命令１３００の正当性を確認する時、署名に用いられたサーバ秘密鍵の署名鍵世代番号１３２１が管理データベース４４０６のサーバ公開鍵管理テーブル５５０１で管理するサーバ公開鍵の世代番号より古い場合、電子署名検証部４４０５は、不正な署名と判定する。

署名の検証に成功した場合（Ｓ１００６でＹＥＳ）、デバイス鍵更新命令解釈部４４０７は（Ｓ１００７）へ進む。一方、署名の検証に失敗した場合（Ｓ１００６でＮＯ）、デバイス鍵更新命令解釈部４４０７はデバイス鍵個別更新命令１３００を正当でないと判断し、処理を終了する。

端末側デバイス鍵更新処理（Ｓ１００７）では、署名の検証に成功した場合、更新鍵生成部４４０３は、鍵管理サーバ１０１と同一の一方向性関数によりデバイスシード管理テーブル５３０３で管理するデバイス鍵生成用シードを更新して、更新後のデバイス鍵生成用シードを所定の公開鍵暗号方式の鍵を生成する関数へ入力して新たなデバイス秘密鍵とデバイス公開鍵とを生成する。更新鍵生成部４４０３は、管理データベース４４０６のデバイス公開鍵ペア管理テーブル５５０２に生成したデバイス秘密鍵とデバイス公開鍵とを格納すると共に、更新前のデバイス秘密鍵とデバイス公開鍵とを削除する。

【００７７】

上記説明では、鍵管理サーバ１０１は、デバイス鍵（デバイス秘密鍵、デバイス公開鍵）を生成するためのデバイス鍵生成用シードを保持している。つまり、上記説明では、鍵管理サーバ１０１は、デバイス公開鍵を生成するとしたが、デバイス秘密鍵もデバイス公開鍵とともに生成される。つまり、通信機器１０２の秘密鍵であるデバイス秘密鍵を鍵管理サーバ１０１が知り得る状態である。しかし、ここでは、鍵管理サーバ１０１は信用できることが前提である。そのため、鍵管理サーバ１０１はデバイス秘密鍵を悪用することはなく、安全性は保たれるものとする。なお、鍵管理サーバ１０１は、生成されるとすぐにデバイス秘密鍵を削除するものとし、デバイス秘密鍵が漏洩することを防止する。

【００７８】

また、鍵管理サーバ１０１はデバイス公開鍵を生成せず、鍵管理サーバ１０１がデバイス秘密鍵を生成できないようにすることも可能である。この場合、鍵管理サーバ１０１はデバイス公開鍵を生成しないため、デバイス鍵生成用シードを保持する必要がない。したがって、鍵管理サーバ１０１がデバイス秘密鍵を生成できないため、デバイス秘密鍵の安全性が高くなる。

これを実現するためには、デバイス鍵の更新命令を受信した通信機器１０２が生成したデバイス公開鍵を鍵管理サーバ１０１へ送信する必要がある。つまり、鍵管理サーバ１０１は自身でデバイス公開鍵を生成するのではなく、通信機器１０２が生成したデバイス公開鍵を取得する。

すなわち、上記サーバ側デバイス鍵更新処理（Ｓ９０３）（Ｓ１００３）では、鍵管理サーバ１０１はデバイス公開鍵の更新を行わない。代わりに、端末側デバイス鍵更新処理（Ｓ９０６）（Ｓ１００７）で新たなデバイス公開鍵を生成した後、通信機器１０２から鍵管理サーバ１０１へデバイス公開鍵を送信する。この際、送信するデバイス公開鍵には、更新前のデバイス秘密鍵で署名を付すことにより改ざん検出可能としてもよい。なお、デバイス公開鍵は公開情報であるため、暗号化する必要はない。また、この場合には、通信機器１０２から鍵管理サーバ１０１へ向けて通信できることが必要になる。

【００７９】

また、上記説明では、デバイス鍵生成用シードを所定の公開鍵暗号方式の鍵を生成する関数への入力として用いた。しかし、デバイス秘密鍵を所定の公開鍵暗号方式の鍵を生成する関数への入力として用いてもよい。この場合、デバイス秘密鍵は、通信機器１０２のみが保持しているため、通信機器１０２が生成したデバイス公開鍵を鍵管理サーバ１０１へ送信する必要がある。

また、サーバ秘密鍵とサーバ公開鍵の更新に関しては、サーバ秘密鍵を所定の公開鍵暗号方式の鍵を生成する関数への入力として用いて鍵管理サーバ１０１でサーバ秘密鍵とサーバ公開鍵とを更新した後、更新後のサーバ公開鍵を各通信機器１０２へ送信する。

【００８０】

次に、有効期限に従って、鍵管理サーバ１０１および通信機器１０２においてデバイス鍵、サーバ鍵を自動的に更新する場合の動作について説明する。

鍵管理サーバ１０１は、鍵管理データベース２２０７のデバイス公開鍵管理テーブル３３０２において、デバイス公開鍵を有効期限と共に管理している。有効期限を経過した場合は、更新鍵生成部２２０４はデバイス公開鍵を更新し、鍵管理データベース２２０７のデバイス公開鍵管理テーブル３３０２に格納すると共に、更新前の該当デバイス公開鍵を削除する。また、鍵管理サーバ１０１は、鍵管理データベース２２０７のサーバ公開鍵ペア管理テーブル３３０１において、サーバ秘密鍵とサーバ公開鍵とを有効期限と共に管理している。有効期限を経過した場合は、更新鍵生成部２２０４はサーバ秘密鍵とサーバ公開鍵とを更新し、鍵管理データベース２２０７のサーバ公開鍵ペア管理テーブル３３０１に格納すると共に、更新前のサーバ秘密鍵とサーバ公開鍵とを削除する。さらに、鍵管理サーバ１０１は、更新したデバイス公開鍵を全ての通信機器１０２に配布する。

同様に、通信機器１０２は、管理データベース４４０６のデバイス公開鍵ペア管理テーブル５５０２において、デバイス秘密鍵とデバイス公開鍵とを有効期限と共に管理している。有効期限を経過した場合は、更新鍵生成部４４０３はデバイス秘密鍵とデバイス公開鍵とを更新し、管理データベース４４０６のデバイス公開鍵ペア管理テーブル５５０２に格納すると共に、更新前のデバイス秘密鍵とデバイス公開鍵とを削除する。

【００８１】

以上のように、鍵管理サーバ１０１と通信機器１０２の通信に公開鍵暗号アルゴリズムを用いても、実施の形態１と同一の効果を得ることができる。

【００８２】

実施の形態８．

実施の形態８では、鍵管理サーバ１０１から通信機器１０２へ送信する命令の暗号化や署名値の計算に公開鍵暗号アルゴリズムを用いた場合のマスター鍵配布命令１４００の配布による通信機器１０２同士の間の暗号化通信に用いる暗号鍵（マスター鍵）の配布及びデバイス秘密鍵、デバイス公開鍵の更新について説明する。

【００８３】

まず、マスター鍵配布命令１４００の配布によるマスター鍵の配布およびデバイス鍵の更新の動作の概要について説明する。

鍵管理サーバ１０１は、通信機器１０２同士が暗号化通信を行う際に用いる暗号鍵（マスター鍵）を生成し、鍵を利用する通信機器１０２のデバイス公開鍵で暗号化し、マスター鍵配布命令１４００として該当通信機器１０２へ送信する。マスター鍵配布命令１４００を受信した通信機器１０２は、マスター鍵配布命令１４００の正当性を検証する際、デバイス秘密鍵、デバイス公開鍵に世代のずれが生じていることを検出した場合、必要に応じてデバイス秘密鍵、デバイス公開鍵の更新処理を行う。さらに、これらの命令にマスター鍵の有効期限が記載されていた場合、鍵管理サーバ１０１と通信機器１０２において、有効期限に従って自動的にマスター鍵の更新を行う。

【００８４】

図４７は図１に示したシステム構成において、通信機器１０２間の暗号化に用いるマスター鍵を配布する際のデータの流れを示した図である。

鍵管理サーバ１０１は、特定の通信機器１０２同士の間で暗号化通信に用いるマスター

鍵の配布を指示する命令を作成し、該当する通信機器１０２が命令の正当性を検証するための電子署名を付与して、マスター鍵配布命令１４００を作成する。次に、鍵管理サーバ１０１は、ネットワーク１０３を介して、マスター鍵配布命令１４００を該当する通信機器１０２に向けて送信する。そして、鍵管理サーバ１０１は、該当するマスター鍵を記憶する。一方、通信機器１０２は、ネットワーク１０３を介して、マスター鍵配布命令１４００を受信し、命令が自分宛であるかどうか確認し、命令に含まれる電子署名を検証して命令の正当性を確認し、マスター鍵の取得を行う。

【００８５】

図４８は、マスター鍵配布命令１４００のデータ形式を示した図である。

図４８に基づき、鍵管理サーバ１０１が配布するマスター鍵配布命令１４００について、マスター鍵配布命令８００と異なる部分について説明する。

マスター鍵配布命令１４００は、デバイス鍵世代番号１４０４とサーバ鍵世代番号１４０６とを備えている。デバイス鍵世代番号１４０４は、マスター鍵配布命令情報１４０３を暗号化する際に用いたデバイス公開鍵の世代番号である。サーバ鍵世代番号１４０６は、署名値を計算する際に用いたサーバ秘密鍵の世代番号である。

【００８６】

次に、図４９、図５０に基づき、実施の形態８における鍵管理サーバ１０１の機能について説明する。

図４９は実施の形態８における鍵管理サーバ１０１の機能ブロック図である。実施の形態８における鍵管理サーバ１０１は、実施の形態７における鍵管理サーバ１０１に加え、初期鍵生成部２０３、暗号化部２２０５、マスター鍵配布命令作成部２２０９を備える。初期鍵生成部２０３は、実施の形態２の機能と同様である。

暗号化部２２０５は、暗号化対象のデータに対して、指定されたデバイス公開鍵を用いて内容を処理装置により暗号化する。

マスター鍵配布命令作成部２２０９は、マスター鍵配布命令１４００を処理装置により作成する。

【００８７】

図５０は実施の形態８における鍵管理サーバ１０１内部の鍵管理データベース２２０７が記憶する情報を示す図である。実施の形態８における鍵管理データベース２２０７は、実施の形態７における鍵管理データベース２２０７に加え、マスター鍵管理テーブル３０２を備える。

実施の形態８におけるマスター鍵管理テーブル３０２は、実施の形態２における鍵管理サーバ１０１の鍵管理データベース２０７のマスター鍵管理テーブル３０２と同一である。

【００８８】

次に、図５１、図５２に基づき、実施の形態８における通信機器１０２の機能について説明する。

図５１は実施の形態８における通信機器１０２の機能ブロック図である。実施の形態８における通信機器１０２は、実施の形態７における通信機器１０２に加え、復号部４４０４、マスター鍵配布命令解釈部４４０８を備える。

復号部４４０４は、暗号化されたデータに対して、指定された鍵を用いて処理装置により復号する。

マスター鍵配布命令解釈部４４０８は、データ受信部４０１が受信したマスター鍵配布命令８００を解釈し、第１世代目のマスター鍵を管理データベース４４０６に格納させる。

【００８９】

図５２は実施の形態８における通信機器１０２内部の管理データベース４４０６が記憶する情報を示す図である。実施の形態８における管理データベース４４０６は、実施の形態７における管理データベース４４０６に加え、マスター鍵管理テーブル５０３を備える。

実施の形態８におけるマスター鍵管理テーブル５０３は、実施の形態２における通信機器１０２の管理データベース４０６のマスター鍵管理テーブル５０３と同一である。

【００９０】

次に動作について説明する。図５３は、マスター鍵を配信する場合の通信システムの動作を示すフローチャートである。

マスター鍵生成処理（Ｓ１１０１）では、鍵管理サーバ１０１の初期鍵生成部２０３はマスター鍵を生成し、鍵管理データベース２２０７に記憶させる。

そして、鍵管理サーバ１０１は、生成したマスター鍵を利用する通信機器１０２に対して、以下の操作を繰り返し行い、該当する通信機器１０２の全てにマスター鍵配布命令１４００を送信する。

マスター鍵配布命令作成処理（Ｓ１１０２）では、マスター鍵配布命令作成部２２０９は、マスター鍵配布命令１４００を作成する。この際、暗号化部２２０５は、鍵管理データベース２２０７のデバイス公開鍵管理テーブル３３０２で管理する該当通信機器１０２のデバイス公開鍵を用いて、マスター鍵配布命令情報（暗号化前）１４１１を暗号化し、マスター鍵配布命令情報（暗号化後）１４０３を作成する。電子署名生成部２２０６は、鍵管理データベース２２０７のサーバ公開鍵ペア管理テーブル３３０１で管理するサーバ秘密鍵を入力として、データ種別１４０１と受信者デバイスＩＤ１４０２とマスター鍵配布命令情報（暗号化後）１４０３に対する署名値１４０５を計算する。

データ送信処理（Ｓ１１０３）では、データ送信部２０２は、マスター鍵配布命令１４００を該当する通信機器１０２へ送信する。

データ受信処理（Ｓ１１０４）では、通信機器１０２のデータ受信部４０１は、マスター鍵配布命令１４００を受信する。マスター鍵配布命令解釈部４４０８は、マスター鍵配布命令１４００のデータ種別１４０１により、受信した情報がマスター鍵配布命令１４００であることを認識する。

宛先判定処理（Ｓ１１０５）では、マスター鍵配布命令解釈部４４０８は、管理データベース４４０６のデバイスＩＤ管理テーブル５０１で管理するデバイスＩＤとマスター鍵配布命令１４００に含まれる受信者デバイスＩＤ１４０２とが一致するか確認して、マスター鍵配布命令１４００が自分宛か否か確認する。

マスター鍵配布命令１４００が自分宛である場合（Ｓ１１０５でＹＥＳ）、マスター鍵配布命令解釈部４４０８は（Ｓ１１０６）へ進む。一方、マスター鍵配布命令１４００が自分宛でない場合（Ｓ１１０５でＮＯ）、マスター鍵配布命令解釈部４４０８はマスター鍵配布命令１４００を無視し、処理を終了する。

署名判定処理（Ｓ１１０６）では、マスター鍵配布命令１４００が自分宛である場合、電子署名検証部４４０５は、管理データベース４４０６のサーバ公開鍵管理テーブル５５０１で管理するサーバ公開鍵を入力として、マスター鍵配布命令１４００の署名値１４０５を検証して、マスター鍵配布命令１４００の正当性を確認する。マスター鍵配布命令１４００の正当性を確認する時、署名に用いられたサーバ秘密鍵のサーバ鍵世代番号１４０６が管理データベース４４０６のサーバ公開鍵管理テーブル５５０１で管理するサーバ公開鍵の世代番号より古い場合、電子署名検証部４４０５は、不正な署名と判定する。

署名の検証に成功した場合（Ｓ１１０６でＹＥＳ）、マスター鍵配布命令解釈部４４０８は（Ｓ１１０７）へ進む。一方、署名の検証に失敗した場合（Ｓ１１０６でＮＯ）、マスター鍵配布命令解釈部４４０８はマスター鍵配布命令１４００を正当でないと判断し、処理を終了する。

マスター鍵記憶処理（Ｓ１１０７）では、署名の検証に成功した場合、復号部４４０４はマスター鍵配布命令情報（暗号化後）１４０３をデバイス秘密鍵を用いて復号する。そして、マスター鍵配布命令解釈部４４０８は、マスター鍵配布命令情報（暗号化前）１４１１から取り出したマスター鍵を管理データベース４４０６のマスター鍵管理テーブル５０３に格納する。なお、復号する時、暗号化に用いられたデバイス公開鍵のデバイス鍵世代番号１４０４が管理データベース４４０６のデバイス公開鍵ペア管理テーブル５５０２で管理するデバイス秘密鍵の世代番号より新しい場合、復号部４４０４は、一時的に新し

い世代のデバイス秘密鍵とデバイス公開鍵とを更新鍵生成部４４０３に生成させて復号する。暗号化に用いられたデバイス公開鍵のデバイス鍵世代番号１４０４が管理データベース４４０６のデバイス公開鍵ペア管理テーブル５５０２で管理するデバイス秘密鍵の世代番号より古い場合、復号部４４０４は、不正なマスター鍵配布命令１４００と判定する。
　端末側デバイス鍵更新処理（Ｓ１１０８）では、（Ｓ１１０７）において、新しい世代のデバイス秘密鍵を生成して復号した場合には、新しい世代のデバイス秘密鍵とデバイス公開鍵とを更新後のデバイス秘密鍵とデバイス公開鍵として管理データベース４４０６のデバイス公開鍵ペア管理テーブル５５０２に格納すると共に、更新前のデバイス秘密鍵とデバイス公開鍵とを削除する。
【００９１】
　有効期限に従いマスター鍵を更新する方法については、実施の形態２の方法と同様である。
【００９２】
　以上のように、鍵管理サーバ１０１と通信機器１０２の通信に公開鍵暗号アルゴリズムを用いても、実施の形態２と同一の効果を得ることができる。
【００９３】
　実施の形態９．
　実施の形態９では、鍵管理サーバ１０１から通信機器１０２へ送信する命令の暗号化や署名値の計算に公開鍵暗号アルゴリズムを用いた場合のマスター鍵一括更新命令１５００またはマスター鍵個別更新命令１６００の配布による通信機器１０２同士の間の暗号化通信に用いる暗号鍵（マスター鍵）の更新について説明する。
【００９４】
　まず、マスター鍵更新命令の配布による通信機器１０２同士の間の共有鍵（マスター鍵）の更新の動作の概要について説明する。
　マスター鍵の更新は、マスター鍵一括更新命令１５００を用いて全てのマスター鍵を一括更新する方法と、マスター鍵個別更新命令１６００を用いて特定のマスター鍵のみを更新する方法の二通りがある。さらに、これらの命令にマスター鍵の有効期限が記載されていた場合、鍵管理サーバ１０１と通信機器１０２において、有効期限に従って自動的にマスター鍵の更新を行う。
【００９５】
　図５４は図１に示したシステム構成において、全てのマスター鍵を一括に更新する際のデータの流れを示した図である。
　鍵管理サーバ１０１は、全てのマスター鍵の一括更新を指示する命令を作成し、各々の通信機器１０２が命令の正当性を検証するための電子署名を付与して、マスター鍵一括更新命令１５００を作成する。次に、鍵管理サーバ１０１は、ネットワーク１０３を介して、マスター鍵一括更新命令１５００を全ての通信機器１０２に向けて送信する。そして、鍵管理サーバ１０１は、全てのマスター鍵を更新する。一方、通信機器１０２は、ネットワーク１０３を介して、マスター鍵一括更新命令１５００を受信し、命令に含まれる電子署名を検証して命令の正当性を確認し、マスター鍵の更新を行う。
【００９６】
　図５５は、マスター鍵一括更新命令１５００のデータ形式を示した図である。
　図５５に基づき、鍵管理サーバ１０１が配布するマスター鍵一括更新命令１５００について、マスター鍵一括更新命令９００と異なる部分について説明する。
　マスター鍵一括更新命令１５００は、電子署名１５０３を１つ備えている。つまり、マスター鍵一括更新命令９００は、通信機器１０２毎に異なる個別電子署名９０４を備えていたが、マスター鍵一括更新命令１５００は、全ての通信機器１０２に共通の電子署名１５０３を１つ備えている。
　電子署名１５０３は、全ての通信機器１０２に共通であるから、デバイスＩＤは備えていない。また、電子署名１５０３の署名値１５２２は、鍵管理サーバ１０１の秘密鍵であるサーバ秘密鍵を用いて施された署名である。

【００９７】
図５６は図１に示したシステム構成において、特定のマスター鍵のみを個別に更新する際のデータの流れを示した図である。
鍵管理サーバ１０１は、特定のマスター鍵の個別更新を指示する命令を作成し、該当する通信機器１０２が命令の正当性を検証するための電子署名を付与して、マスター鍵個別更新命令１６００を作成する。次に、鍵管理サーバ１０１は、ネットワーク１０３を介して、マスター鍵個別更新命令１６００を該当する通信機器１０２に向けて送信する。そして、鍵管理サーバ１０１は、該当するマスター鍵を更新する。一方、通信機器１０２は、ネットワーク１０３を介して、マスター鍵個別更新命令１６００を受信し、命令が自分宛であるかどうか確認し、命令に含まれる電子署名を検証して命令の正当性を確認し、マスター鍵の更新を行う。
【００９８】
図５７は、マスター鍵個別更新命令１６００のデータ形式を示した図である。
図５７に基づき、鍵管理サーバ１０１が配布するマスター鍵個別更新命令１６００について、マスター鍵個別更新命令１０００と異なる部分について説明する。
マスター鍵個別更新命令１６００は、電子署名１６０３を１つ備えている。つまり、マスター鍵個別更新命令１０００は、通信機器１０２毎に異なる個別電子署名１００４を備えていたが、マスター鍵個別更新命令１６００は、全ての通信機器１０２に共通の電子署名１６０３を１つ備えている。
電子署名１６０３は、全ての通信機器１０２に共通であるから、デバイスＩＤは備えていない。また、電子署名１６０３の署名値１６２２は、鍵管理サーバ１０１の秘密鍵であるサーバ秘密鍵を用いて施された署名である。
【００９９】
次に、図５８に基づき、実施の形態９における鍵管理サーバ１０１の機能について説明する。
図５８は実施の形態９における鍵管理サーバ１０１の機能ブロック図である。実施の形態９における鍵管理サーバ１０１は、実施の形態８における鍵管理サーバ１０１に加え、マスター鍵更新命令作成部２２１０を備える。
マスター鍵更新命令作成部２２１０は、マスター鍵一括更新命令１５００やマスター鍵個別更新命令１６００を処理装置により作成する。
実施の形態９における鍵管理データベース２２０７は、実施の形態８における鍵管理データベース２２０７と同一である。
【０１００】
次に、図５９に基づき、実施の形態９における通信機器１０２の機能について説明する。
図５９は実施の形態９における通信機器１０２の機能ブロック図である。実施の形態９における通信機器１０２は、実施の形態８における通信機器１０２に加え、マスター鍵更新命令解釈部４４０９を備える。
マスター鍵更新命令解釈部４４０９は、データ受信部４０１が受信したマスター鍵一括更新命令１５００やマスター鍵個別更新命令１６００を解釈し、マスター鍵を処理装置により更新する。
実施の形態９における管理データベース４４０６は、実施の形態８における管理データベース４４０６と同一である。
【０１０１】
次に動作について説明する。
まず、マスター鍵を一括更新する場合の動作について説明する。図６０は、マスター鍵を一括更新する場合の通信システムの動作を示すフローチャートである。
マスター鍵一括更新命令作成処理（Ｓ１２０１）では、鍵管理サーバ１０１のマスター鍵更新命令作成部２２１０は、マスター鍵一括更新命令１５００を作成する。電子署名生成部２２０６は、鍵管理データベース２２０７のサーバ公開鍵ペア管理テーブル３３０１

で管理するサーバ秘密鍵を入力として、データ種別１５０１とマスター鍵一括更新命令情報１５０２に対する署名値１５２２を生成する。

データ送信処理（Ｓ１２０２）では、データ送信部２０２は、マスター鍵一括更新命令１５００を全ての通信機器１０２へ送信する。

サーバ側マスター鍵更新処理（Ｓ１２０３）では、マスター鍵一括更新命令１５００の送信に成功した後、更新鍵生成部２２０４は、全てのマスター鍵を更新し、鍵管理データベース２２０７のマスター鍵管理テーブル３０２に格納すると共に、更新前のマスター鍵全てを削除する。なお、マスター鍵については、実施の形態３と同様に所定の一方向関数を通すことにより更新する。

データ受信処理（Ｓ１２０４）では、通信機器１０２のデータ受信部４０１は、マスター鍵一括更新命令１５００を受信する。マスター鍵更新命令解釈部４４０９は、マスター鍵一括更新命令１５００のデータ種別１５０１により、受信した情報がマスター鍵一括更新命令１５００であることを認識する。

署名判定処理（Ｓ１２０５）では、電子署名検証部４４０５は、管理データベース４４０６のサーバ公開鍵管理テーブル５５０１で管理するサーバ公開鍵を入力として、電子署名１５０３の署名値１５２２を検証して、マスター鍵一括更新命令１５００の正当性を確認する。この時、署名に用いられたサーバ秘密鍵の署名鍵世代番号１５２１が管理データベース４４０６のサーバ公開鍵管理テーブル５５０１で管理するサーバ公開鍵の世代番号より古い場合、電子署名検証部４４０５は、不正な署名と判定する。

署名の検証に成功した場合（Ｓ１２０５でＹＥＳ）、マスター鍵更新命令解釈部４４０９は（Ｓ１２０６）へ進む。一方、署名の検証に失敗した場合（Ｓ１２０５でＮＯ）、マスター鍵更新命令解釈部４４０９はマスター鍵一括更新命令１５００を正当でないと判断し、処理を終了する。

端末側マスター鍵更新処理（Ｓ１２０６）では、署名の検証に成功した場合、更新鍵生成部４４０３は、管理データベース４０６のマスター鍵管理テーブル５０３に格納した全てのマスター鍵を更新させ、管理データベース４０６のマスター鍵管理テーブル５０３に格納すると共に、更新前のマスター鍵を削除する。

【０１０２】

次に特定のマスター鍵のみを更新する場合の動作について説明する。図６１は、特定のマスター鍵のみを更新する場合の通信システムの動作を示すフローチャートである。

マスター鍵個別更新命令作成処理（Ｓ１３０１）では、鍵管理サーバ１０１のマスター鍵更新命令作成部２２１０は、マスター鍵個別更新命令１６００を作成する。電子署名生成部２２０６は、鍵管理データベース２２０７のサーバ公開鍵ペア管理テーブル３３０１で管理するサーバ秘密鍵を入力として、データ種別１６０１とマスター鍵個別更新命令情報１６０２に対する署名値１６２２を生成する。

データ送信処理（Ｓ１３０２）では、データ送信部２０２は、マスター鍵個別更新命令１６００を該当する通信機器１０２へ送信する。

サーバ側デバイス鍵更新処理（Ｓ１３０３）では、マスター鍵個別更新命令１６００の送信に成功した後、更新鍵生成部２２０４は、該当するマスター鍵を更新し、鍵管理データベース２２０７のマスター鍵管理テーブル３０２に格納すると共に、更新前の該当マスター鍵を削除する。

データ受信処理（Ｓ１３０４）では、通信機器１０２のデータ受信部４０１は、マスター鍵個別更新命令１６００を受信する。マスター鍵更新命令解釈部４４０９は、マスター鍵個別更新命令１６００のデータ種別１６０１により、受信した情報がマスター鍵個別更新命令１６００であることを認識する。

宛先判定処理（Ｓ１３０５）では、マスター鍵更新命令解釈部４４０９は、管理データベース４４０６のマスター鍵管理テーブル５０３で管理するマスター鍵ＩＤとマスター鍵個別更新命令１６００に含まれるマスター鍵ＩＤ１６１１とが一致するか確認してマスター鍵個別更新命令１６００が自分宛か否か確認する。

マスター鍵個別更新命令１６００が自分宛である場合（Ｓ１３０５でＹＥＳ）、マスタ

ー鍵更新命令解釈部４４０９は（Ｓ１３０６）へ進む。一方、マスター鍵個別更新命令１６００が自分宛でない場合（Ｓ１３０５でＮＯ）、マスター鍵更新命令解釈部４４０９はマスター鍵個別更新命令１６００を無視し、処理を終了する。
署名判定処理（Ｓ１３０６）では、マスター鍵個別更新命令１６００が自分宛である場合は、電子署名検証部４４０５は、管理データベース４４０６のサーバ公開鍵管理テーブル５５０１で管理するサーバ公開鍵を入力として、マスター鍵個別更新命令１６００の署名値１６２２を検証して、マスター鍵個別更新命令１６００の正当性を確認する。マスター鍵個別更新命令１６００の正当性を確認する時、署名に用いられたサーバ秘密鍵の署名鍵世代番号１６２１が管理データベース４４０６のサーバ公開鍵管理テーブル５５０１で管理するサーバ公開鍵の世代番号より古い場合、電子署名検証部４４０５は、不正な署名と判定する。
署名の検証に成功した場合（Ｓ１３０６でＹＥＳ）、マスター鍵更新命令解釈部４４０９は（Ｓ１３０７）へ進む。一方、署名の検証に失敗した場合（Ｓ１３０６でＮＯ）、マスター鍵更新命令解釈部４４０９はマスター鍵個別更新命令１６００を正当でないと判断し、処理を終了する。
端末側マスター鍵更新処理（Ｓ１３０７）では、署名の検証に成功した場合、更新鍵生成部４４０３は該当するマスター鍵を更新し、管理データベース４４０６のマスター鍵管理テーブル５０３に格納すると共に、更新前のマスター鍵を削除する。
【０１０３】
有効期限に従いマスター鍵を更新する方法については、実施の形態３の方法と同様である。
【０１０４】
以上のように、鍵管理サーバ１０１と通信機器１０２の通信に公開鍵暗号アルゴリズムを用いても、実施の形態３と同一の効果を得ることができる。
【０１０５】
実施の形態１０．
実施の形態１０では、鍵管理サーバ１０１から通信機器１０２へ送信する命令の暗号化や署名値の計算に公開鍵暗号アルゴリズムを用いた場合の通信機器１０２同士の間の機器間通信データ１１００のやり取りによるマスター鍵の更新と、デバイス鍵一括更新命令１２００の転送によるデバイス鍵（デバイス秘密鍵、デバイス公開鍵）の更新と、マスター鍵一括更新命令１５００の転送によるマスター鍵の更新とについて説明する。
【０１０６】
機器間通信データ１１００のやり取りによるマスター鍵の更新については、公開鍵暗号アルゴリズムを用いた場合であっても、実施の形態４で説明した動作と同一の動作で実現することができる。
【０１０７】
デバイス鍵一括更新命令１２００の転送によるデバイス鍵（デバイス秘密鍵、デバイス公開鍵）の更新は、実施の形態５で説明した（Ｓ７０１）の「実施の形態１で説明した手順（（Ｓ１０４）から（Ｓ１０６）まで）」を、「実施の形態７で説明した（（Ｓ９０４）から（Ｓ９０６）まで）と置き換え、（Ｓ７０４）の「（（Ｓ１０５）と（Ｓ１０６））」を「（（Ｓ９０５）と（Ｓ９０６））」と置き換えれば、実施の形態５で説明した方法を適用できる。
同様に、マスター鍵一括更新命令１５００の転送によるマスター鍵の更新は、実施の形態６で説明した（Ｓ８０１）の「実施の形態３で説明した手順（（Ｓ４０５）から（Ｓ４０７）まで）」を、「実施の形態９で説明した手順（（Ｓ１２０５）から（Ｓ１２０６）まで）」と置き換え、（Ｓ８０４）の「（（Ｓ４０５）から（Ｓ４０７）まで）」を「（（Ｓ１２０５）から（Ｓ１２０６）まで）」と置き換えれば、実施の形態６で説明した方法を適用できる。なお、実施の形態６では、マスター鍵一括更新命令９００の転送によってデバイス鍵を更新する場合が存在したが、実施の形態１０では、マスター鍵一括更新命令１５００の転送によってデバイス鍵（デバイス秘密鍵、デバイス公開鍵）を更新するこ

とはない。
【０１０８】
　以上のように、鍵管理サーバ１０１と通信機器１０２の通信に公開鍵暗号アルゴリズムを用いても、実施の形態４から実施の形態６までと同一の効果を得ることができる。
【０１０９】
　実施の形態１１．
　以上の実施の形態では、図１に示すように、鍵管理サーバ１０１と通信機器１０２との間をネットワーク１０３で接続して鍵管理サーバ１０１から通信機器１０２へネットワーク１０３を介してデータを配信すると説明した。実施の形態１１では、鍵管理サーバ１０１から通信機器１０２へのデータの配信方法について説明する。
【０１１０】
　図６２は、鍵管理サーバ１０１が衛星通信を用いた一方向通信により各通信機器１０２へデータを配信する場合のシステム構成図である。
　図６２において、鍵管理サーバ１０１は、配信するデータ（デバイス鍵一括更新命令６００等）を地上局１０４を介して、通信衛星１０５から通信機器１０２へ配信する。地上局１０４は鍵管理サーバ１０１から各通信機器１０２に向けて発信された各種データを、通信衛星１０５を通して送信するための中継設備である。通信衛星１０５は地上局１０４から中継された各種データを、各通信機器１０２へ向けて送信する衛星設備である。また、ネットワーク１０３は、通信機器１０２同士の通信の通信路として用いられるバックボーンネットワークである。
　つまり、鍵管理サーバ１０１は、通信衛星１０５から一方向通信により各種データを各通信機器１０２へ同報通信する。つまり、鍵管理サーバ１０１は、通信衛星１０５を介して各種データを各通信機器１０２へ一方的に送信する。
【０１１１】
　図６３は、鍵管理サーバ１０１が地上波放送を用いた一方向通信により各通信機器１０２へデータを配信する場合のシステム構成図である。
　図６３において、鍵管理サーバ１０１は、配信するデータ（デバイス鍵一括更新命令６００等）を地上波放送設備１０６から通信機器１０２へ配信する。地上波放送設備１０６は鍵管理サーバ１０１から送信された各種データを、各通信機器１０２へ向けて送信する放送設備である。また、ネットワーク１０３は、通信機器１０２同士の通信の通信路として用いられるバックボーンネットワークである。
　つまり、鍵管理サーバ１０１は、地上波放送設備１０６から一方向通信により各種データを各通信機器１０２へ同報通信する。つまり、鍵管理サーバ１０１は、各種データを各通信機器１０２へ一方的に送信する。
【０１１２】
　図６４は、鍵管理サーバ１０１が双方向通信可能な通信路を用いて各通信機器１０２へデータを配信する場合のシステム構成図である。
　図６４において、鍵管理サーバ１０１は、配信するデータ（デバイス鍵一括更新命令６００等）をインターネット放送設備１０７からインターネット網１０８を介して通信機器１０２へ配信する。インターネット放送設備１０７は鍵管理サーバ１０１から送信された各種データを、各通信機器１０２へ向けてインターネット網１０８を介して送信する放送設備である。また、インターネット網１０８は、通信機器１０２同士の通信及び通信機器１０２とインターネット放送設備１０７との間の通信の通信路として用いられるバックボーンネットワークである。
　つまり、鍵管理サーバ１０１は、インターネット放送設備１０７から双方向通信により各種データを各通信機器１０２へ同報通信する。
【０１１３】
　図６５は、上記実施の形態における鍵管理サーバ１０１、通信機器１０２のハードウェア資源の一例を示す図である。
　図６５において、鍵管理サーバ１０１、通信機器１０２は、プログラムを実行するＣＰ

Ｕ１９１１（Ｃｅｎｔｒａｌ・Ｐｒｏｃｅｓｓｉｎｇ・Ｕｎｉｔ、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう）を備えている。ＣＰＵ１９１１は、バス１９１２を介してＲＯＭ１９１３、ＲＡＭ１９１４、ＬＣＤ１９０１（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）、キーボード１９０２（Ｋ／Ｂ）、通信ボード１９１５、磁気ディスク装置１９２０と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装置１９２０の代わりに、光ディスク装置、メモリカード読み書き装置などの記憶装置でもよい。

【０１１４】

ＲＯＭ１９１３、磁気ディスク装置１９２０は、不揮発性メモリの一例である。ＲＡＭ１９１４は、揮発性メモリの一例である。ＲＯＭ１９１３とＲＡＭ１９１４と磁気ディスク装置１９２０とは、記憶装置（メモリ）の一例である。また、キーボード１９０２、通信ボード１９１５は、入力装置の一例である。また、通信ボード１９１５は、通信装置の一例である。さらに、ＬＣＤ１９０１は、表示装置の一例である。

【０１１５】

磁気ディスク装置１９２０又はＲＯＭ１９１３などには、オペレーティングシステム１９２１（ＯＳ）、ウィンドウシステム１９２２、プログラム群１９２３、ファイル群１９２４が記憶されている。プログラム群１９２３のプログラムは、ＣＰＵ１９１１、オペレーティングシステム１９２１、ウィンドウシステム１９２２により実行される。

【０１１６】

プログラム群１９２３には、上記の説明において「入力インタフェース２０１」、「データ送信部２０２」、「初期鍵生成部２０３」、「更新鍵生成部２０４」、「暗号化部２０５」、「署名値計算部２０６」、「鍵管理データベース２０７」、「デバイス鍵更新命令作成部２０８」、「マスター鍵配布命令作成部２０９」、「マスター鍵更新命令作成部２１０」、「データ受信部４０１」、「機器間通信部４０２」、「更新鍵生成部４０３」、「復号部４０４」、「署名値検証部４０５」、「管理データベース４０６」、「デバイス鍵更新命令解釈部４０７」、「マスター鍵配布命令解釈部４０８」、「マスター鍵更新命令解釈部４０９」、「機器間通信データ作成解釈部４１０」、「署名値生成部４１１」、「暗号化部４１２」等として説明した機能を実行するソフトウェアやプログラムやその他のプログラムが記憶されている。プログラムは、ＣＰＵ１９１１により読み出され実行される。

ファイル群１９２４には、上記の説明において「デバイス鍵一括更新命令６００」、「デバイス鍵個別更新命令７００」、「マスター鍵配布命令８００」、「マスター鍵一括更新命令９００」、「マスター鍵個別更新命令１０００」、「機器間通信データ１１００」、「デバイス鍵一括更新命令１２００」、「デバイス鍵個別更新命令１３００」、「マスター鍵配布命令１４００」、「マスター鍵一括更新命令１５００」、「マスター鍵個別更新命令１６００」等の情報やデータや信号値や変数値やパラメータが、「ファイル」や「データベース」の各項目として記憶される。「ファイル」や「データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してＣＰＵ１９１１によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのＣＰＵ１９１１の動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示のＣＰＵ１９１１の動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。

また、上記の説明におけるフローチャートの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、ＲＡＭ１９１４のメモリ、その他光ディスク等の記録媒体に記録される。また、データや信号は、バス１９１２や信号線やケーブルその他の伝送媒体によりオンライン伝送される。

【０１１７】

また、上記の説明において「～部」として説明するものは、「～回路」、「～装置」、

「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。また、「～装置」として説明するものは、「～回路」、「～装置」、「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。さらに、「～処理」として説明するものは「～ステップ」であっても構わない。すなわち、「～部」として説明するものは、ＲＯＭ１９１３に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、ＲＯＭ１９１３等の記録媒体に記憶される。プログラムはＣＰＵ１９１１により読み出され、ＣＰＵ１９１１により実行される。すなわち、プログラムは、上記で述べた「～部」としてコンピュータ等を機能させるものである。あるいは、上記で述べた「～部」の手順や方法をコンピュータ等に実行させるものである。

【図面の簡単な説明】

【０１１８】

【図１】システム構成図。

【図２】全てのデバイス鍵を一括に更新する際のデータの流れを示した図。

【図３】デバイス鍵一括更新命令６００のデータ形式を示した図。

【図４】特定のデバイス鍵のみを個別に更新する際のデータの流れを示した図。

【図５】デバイス鍵個別更新命令７００のデータ形式を示した図。

【図６】実施の形態１における鍵管理サーバ１０１の機能ブロック図。

【図７】実施の形態１における鍵管理サーバ１０１内部の鍵管理データベース２０７を示す図。

【図８】実施の形態１における通信機器１０２の機能ブロック図。

【図９】実施の形態１における通信機器１０２内部の管理データベース４０６を示す図。

【図１０】デバイス鍵を一括更新する場合の通信システムの動作を示すフローチャート。

【図１１】特定のデバイス鍵のみを更新する場合の通信システムの動作を示すフローチャート。

【図１２】通信機器１０２間の暗号化に用いるマスター鍵を配布する際のデータの流れを示した図。

【図１３】マスター鍵配布命令８００のデータ形式を示した図。

【図１４】実施の形態２における鍵管理サーバ１０１の機能ブロック図。

【図１５】実施の形態２における鍵管理サーバ１０１内部の鍵管理データベース２０７を示す図。

【図１６】実施の形態２における通信機器１０２の機能ブロック図。

【図１７】実施の形態２における通信機器１０２内部の管理データベース４０６を示す図。

【図１８】マスター鍵を配信する場合の通信システムの動作を示すフローチャート。

【図１９】全てのマスター鍵を一括に更新する際のデータの流れを示した図。

【図２０】マスター鍵一括更新命令９００のデータ形式を示した図。

【図２１】特定のマスター鍵のみを個別に更新する際のデータの流れを示した図。

【図２２】マスター鍵個別更新命令１０００のデータ形式を示した図。

【図２３】実施の形態３における鍵管理サーバ１０１の機能ブロック図。

【図２４】実施の形態３における通信機器１０２の機能ブロック図。

【図２５】マスター鍵を一括更新する場合の通信システムの動作を示すフローチャート。

【図２６】特定のマスター鍵のみを更新する場合の通信システムの動作を示すフローチャート。

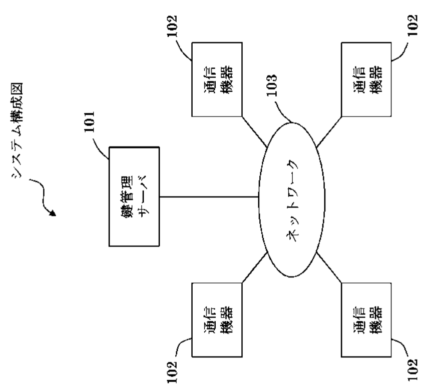
【図２７】機器間通信データ１１００のやり取りによってマスター鍵を更新する際のデータの流れを示した図。

【図２８】機器間通信データ１１００のデータ形式を示した図。

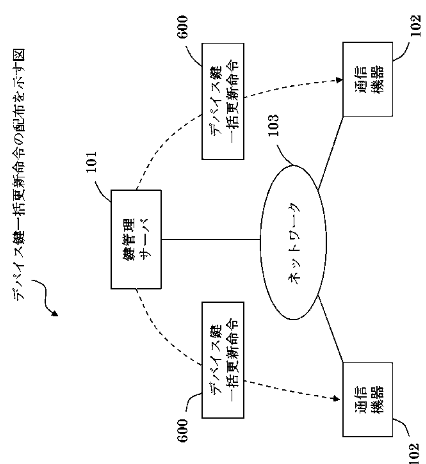
【図２９】実施の形態４における通信機器１０２の機能ブロック図。
【図３０】機器間通信データ１１００のやり取りによってマスター鍵を更新する場合の通信システムの動作を示すフローチャート。
【図３１】デバイス鍵一括更新命令６００を転送することによってマスター鍵を更新する際のデータの流れを示した図。
【図３２】実施の形態５における通信機器１０２の機能ブロック図。
【図３３】デバイス鍵一括更新命令６００を転送することによってマスター鍵を更新する場合の通信システムの動作を示すフローチャート。
【図３４】マスター鍵一括更新命令９００を転送することによってマスター鍵を更新する際のデータの流れを示した図。
【図３５】実施の形態６における通信機器１０２の機能ブロック図。
【図３６】マスター鍵一括更新命令９００を転送することによってマスター鍵を更新する場合の通信システムの動作を示すフローチャート。
【図３７】全てのデバイス鍵を一括に更新する際のデータの流れを示した図。
【図３８】デバイス鍵一括更新命令１２００のデータ形式を示した図。
【図３９】特定のデバイス鍵のみを個別に更新する際のデータの流れを示した図。
【図４０】デバイス鍵個別更新命令１３００のデータ形式を示した図。
【図４１】実施の形態７における鍵管理サーバ１０１の機能ブロック図。
【図４２】実施の形態７における鍵管理サーバ１０１内部の鍵管理データベース２２０７を示す図。
【図４３】実施の形態７における通信機器１０２の機能ブロック図。
【図４４】実施の形態７における通信機器１０２内部の管理データベース４４０６を示す図。
【図４５】デバイス鍵を一括更新する場合の通信システムの動作を示すフローチャート。
【図４６】特定のデバイス鍵のみを更新する場合の通信システムの動作を示すフローチャート。
【図４７】通信機器１０２間の暗号化に用いるマスター鍵を配布する際のデータの流れを示した図。
【図４８】マスター鍵配布命令１４００のデータ形式を示した図。
【図４９】実施の形態８における鍵管理サーバ１０１の機能ブロック図。
【図５０】実施の形態８における鍵管理サーバ１０１内部の鍵管理データベース２２０７を示す図。
【図５１】実施の形態８における通信機器１０２の機能ブロック図。
【図５２】実施の形態８における通信機器１０２内部の管理データベース４４０６を示す図。
【図５３】マスター鍵を配信する場合の通信システムの動作を示すフローチャート。
【図５４】全てのマスター鍵を一括に更新する際のデータの流れを示した図。
【図５５】マスター鍵一括更新命令１５００のデータ形式を示した図。
【図５６】特定のマスター鍵のみを個別に更新する際のデータの流れを示した図。
【図５７】マスター鍵個別更新命令１６００のデータ形式を示した図。
【図５８】実施の形態９における鍵管理サーバ１０１の機能ブロック図。
【図５９】実施の形態９における通信機器１０２の機能ブロック図。
【図６０】マスター鍵を一括更新する場合の通信システムの動作を示すフローチャート。
【図６１】特定のマスター鍵のみを更新する場合の通信システムの動作を示すフローチャート。
【図６２】鍵管理サーバ１０１が衛星通信を用いた一方向通信により各通信機器１０２へデータを配信する場合のシステム構成図。
【図６３】鍵管理サーバ１０１が地上波放送を用いた一方向通信により各通信機器１０２へデータを配信する場合のシステム構成図。
【図６４】鍵管理サーバ１０１が双方向通信可能な通信路を用いて各通信機器１０２へデ

ータを配信する場合のシステム構成図。
【図６５】鍵管理サーバ１０１、通信機器１０２のハードウェア資源の一例を示す図。
【符号の説明】
【０１１９】
　１０１　鍵管理サーバ、１０２　通信機器、２０１　入力インタフェース、２０２　データ送信部、２０３　初期鍵生成部、２０４，２２０４　更新鍵生成部、２０５，２２０５　暗号化部、２０６　署名値計算部、２２０６　電子署名生成部、２０７，２２０７　鍵管理データベース、２０８，２２０８　デバイス鍵更新命令作成部、２０９，２２０９　マスター鍵配布命令作成部、２１０，２２１０　マスター鍵更新命令作成部、４０１　データ受信部、４０２　機器間通信部、４０３，４４０３　更新鍵生成部、４０４，４４０４　復号部、４０５　署名値検証部、４４０５　電子署名検証部、４０６，４４０６　管理データベース、４０７，４４０７　デバイス鍵更新命令解釈部、４０８，４４０８　マスター鍵配布命令解釈部、４０９，４４０９　マスター鍵更新命令解釈部、４１０　機器間通信データ作成解釈部、４１１　署名値生成部、４１２　暗号化部、４２１　デバイス鍵更新命令転送部、４２２　マスター鍵更新命令転送部、６００，１２００　デバイス鍵一括更新命令、７００，１３００　デバイス鍵個別更新命令、８００，１４００　マスター鍵配布命令、９００，１５００　マスター鍵一括更新命令、１０００，１６００　マスター鍵個別更新命令、１１００　機器間通信データ。

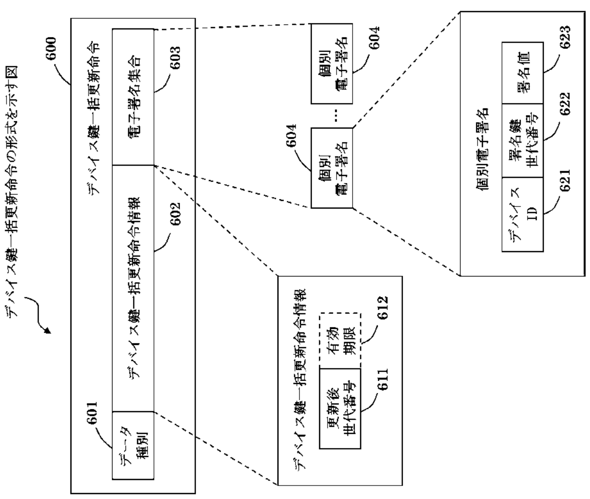
【図１】



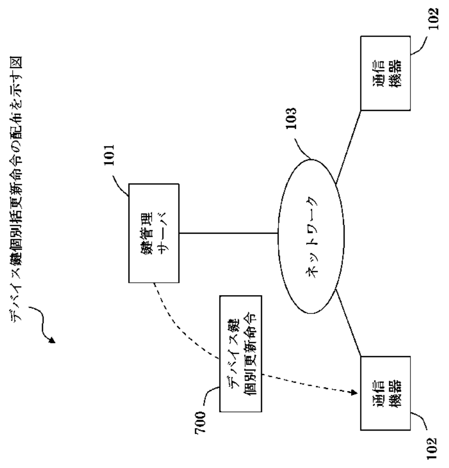
【図２】



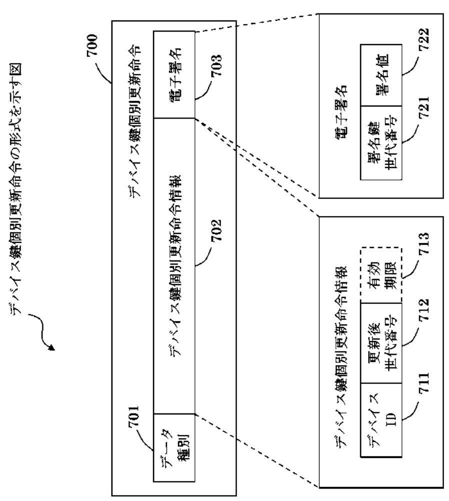
【図３】


デバイス鍵一括更新命令の形式を示す図
600
デバイス鍵一括更新命令
601
データ種別
デバイス鍵一括更新命令情報
602
電子署名集合
603
デバイス鍵一括更新命令情報
更新後世代番号
611
有効期限
612
604
個別電子署名
…
個別電子署名
604
個別電子署名
デバイスID
621
署名鍵世代番号
622
署名値
623

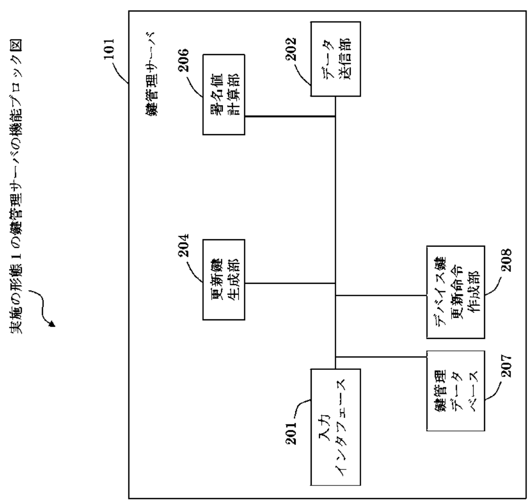
【図４】


デバイス鍵個別括更新命令の配布を示す図
101
鍵管理サーバ
103
ネットワーク
102
通信機器
700
デバイス鍵個別更新命令
通信機器
102

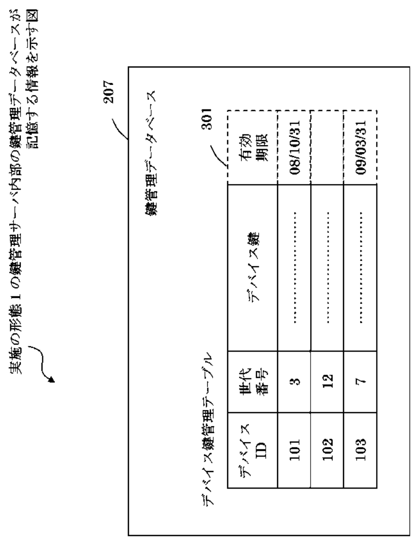
【図５】


デバイス鍵個別更新命令の形式を示す図
700
デバイス鍵個別更新命令
701
データ種別
デバイス鍵個別更新命令情報
702
電子署名
703
デバイス鍵個別更新命令情報
デバイスID
711
更新後世代番号
712
有効期限
713
電子署名
署名鍵世代番号
721
署名値
722

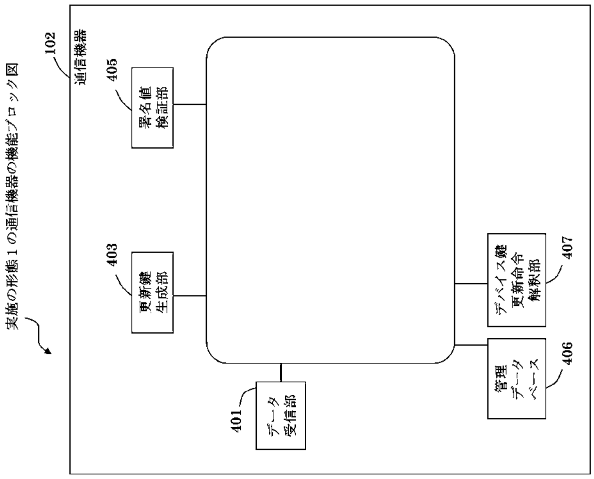
【図６】


実施の形態１の鍵管理サーバの機能ブロック図
101
鍵管理サーバ
206
署名値計算部
202
データ送信部
204
更新鍵生成部
デバイス鍵更新命令作成部
208
201
入力インタフェース
鍵管理データベース
207

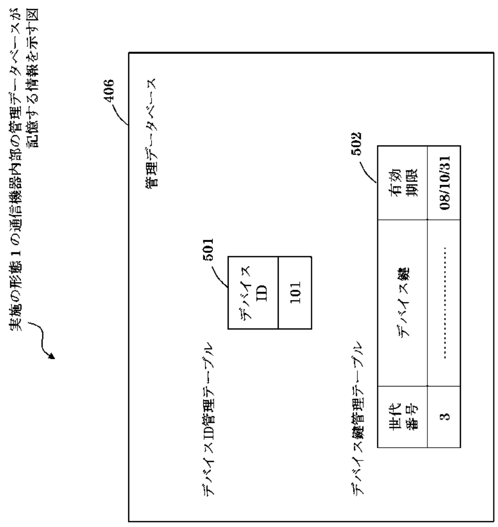
【図７】


実施の形態１の鍵管理サーバ内部の鍵管理データベースが記憶する情報を示す図
207
鍵管理データベース
デバイス鍵管理テーブル
301
デバイスID
世代番号
デバイス鍵
有効期限
101
3
08/10/31
102
12
103
7
09/03/31

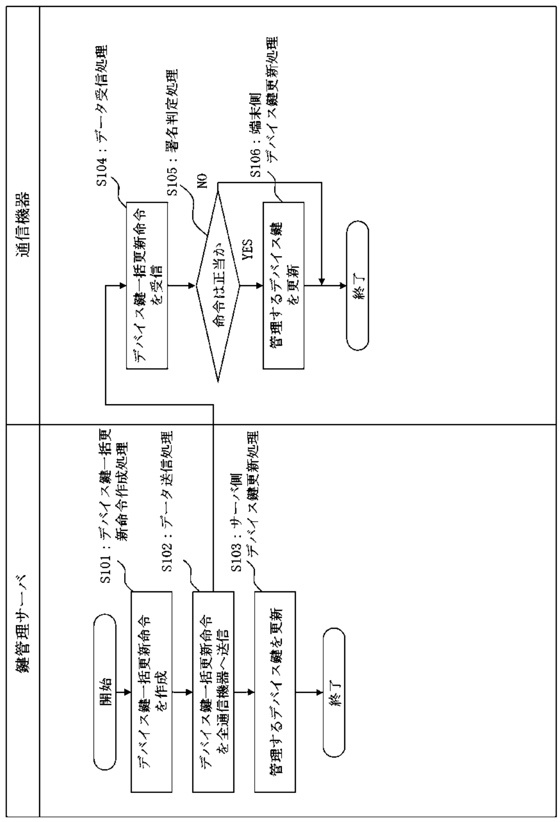
【図８】


実施の形態１の通信機器の機能ブロック図
102
通信機器
405
署名値検証部
403
更新鍵生成部
401
データ受信部
406
管理データベース
407
デバイス鍵更新命令解釈部

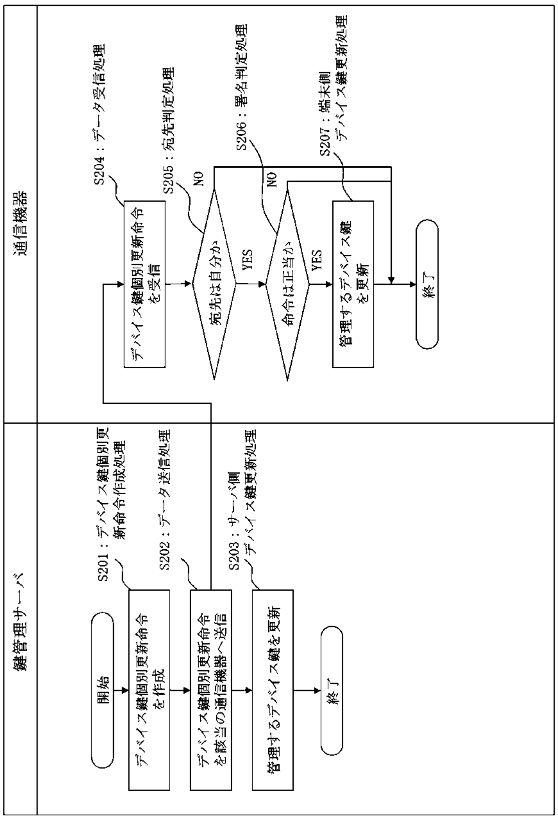
【図９】


実施の形態１の通信機器内部の管理データベースが記憶する情報を示す図
406
管理データベース
デバイスID管理テーブル
501
デバイスID
101
デバイス鍵管理テーブル
502
世代番号
デバイス鍵
有効期限
3
08/10/31

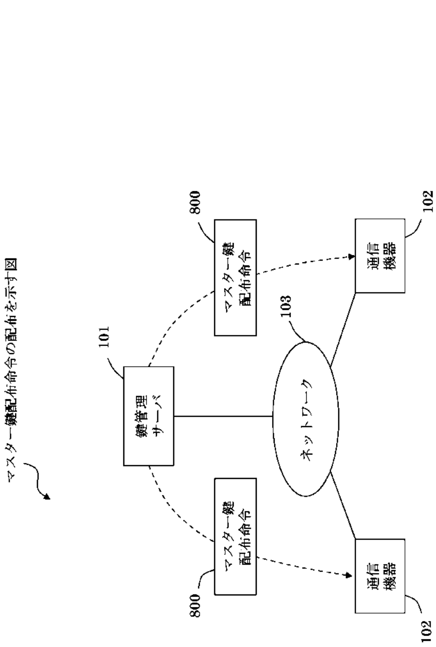
【図１０】


鍵管理サーバ
通信機器
開始
デバイス鍵一括更新命令を作成
S101：デバイス鍵一括更新命令作成処理
デバイス鍵一括更新命令を全通信機器へ送信
S102：データ送信処理
管理するデバイス鍵を更新
S103：サーバ側デバイス鍵更新処理
終了
デバイス鍵一括更新命令を受信
S104：データ受信処理
命令は正当か
S105：署名判定処理
NO
YES
管理するデバイス鍵を更新
S106：端末側デバイス鍵更新処理
終了

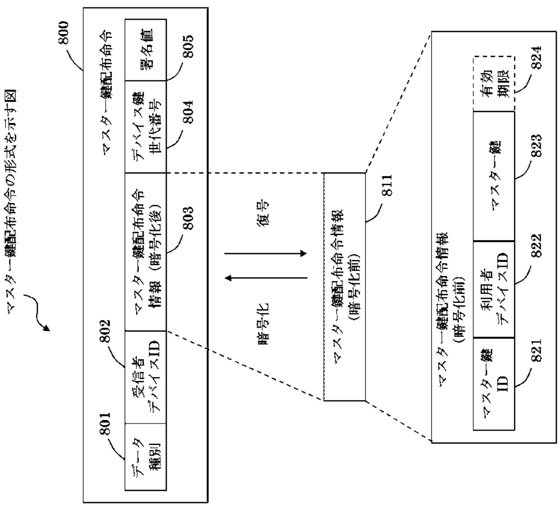
【図１１】



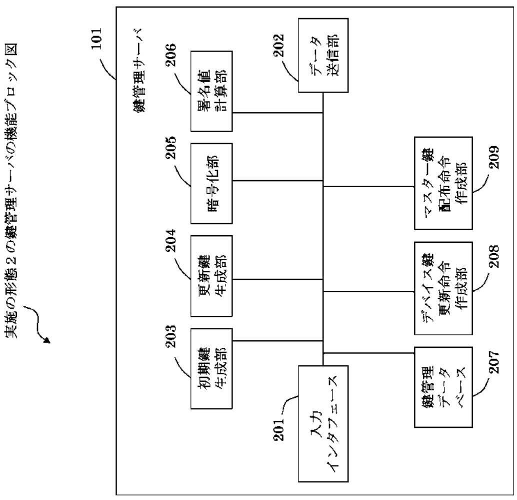
【図１２】



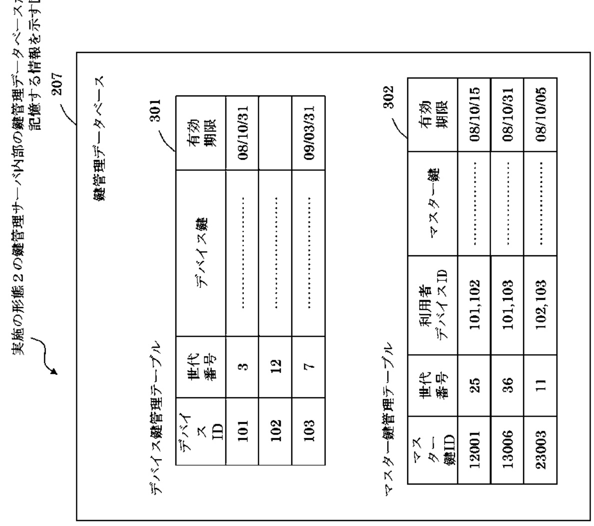
【図１３】



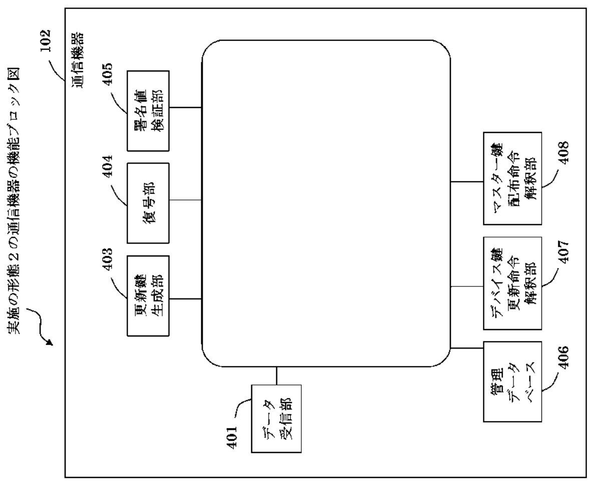
【図１４】



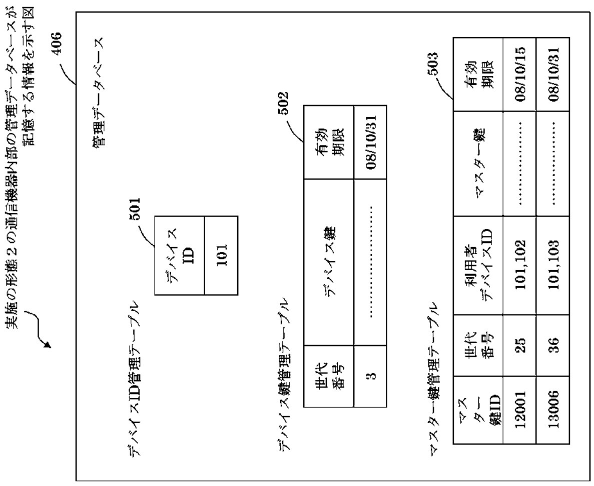
【図１５】



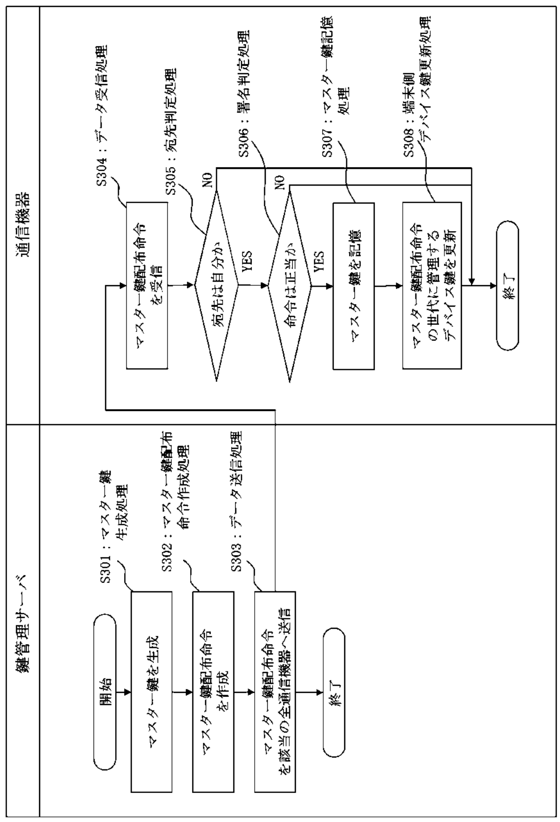
【図１６】



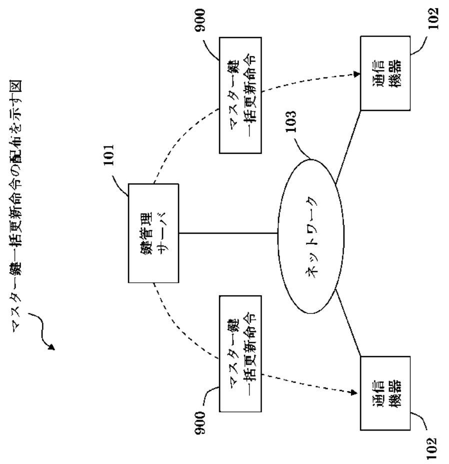
【図１７】



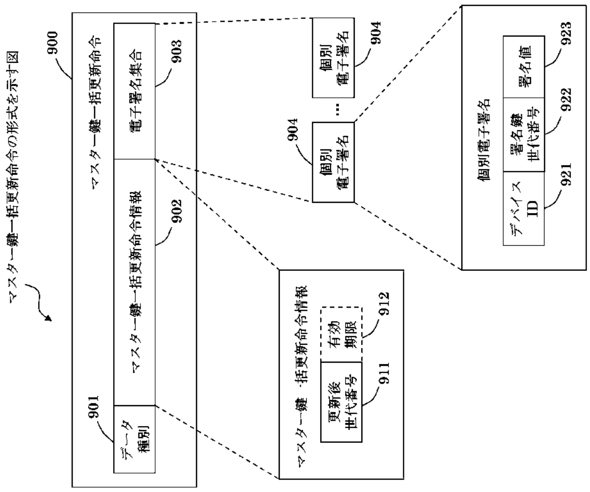
【図１８】



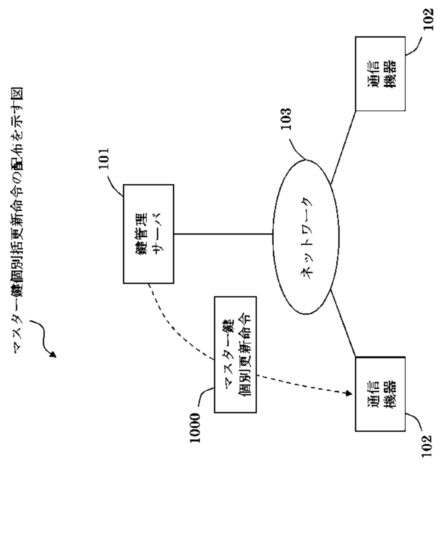
【図１９】



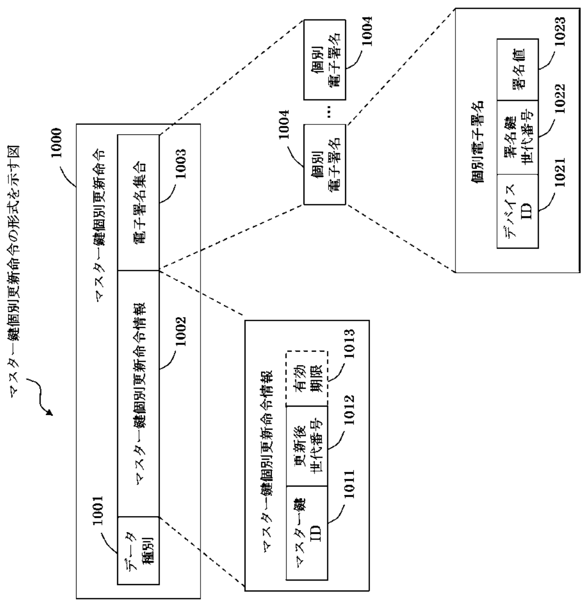
【図２０】



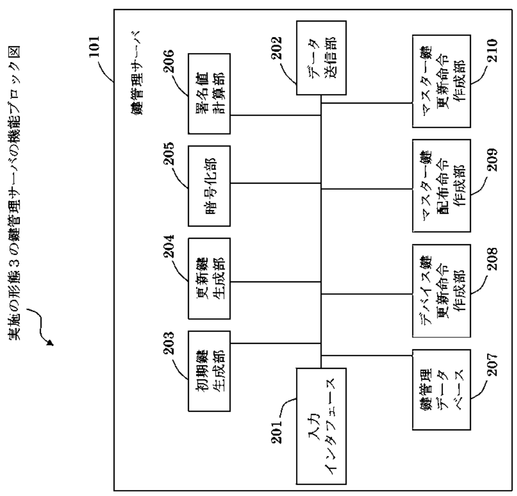
【図２１】



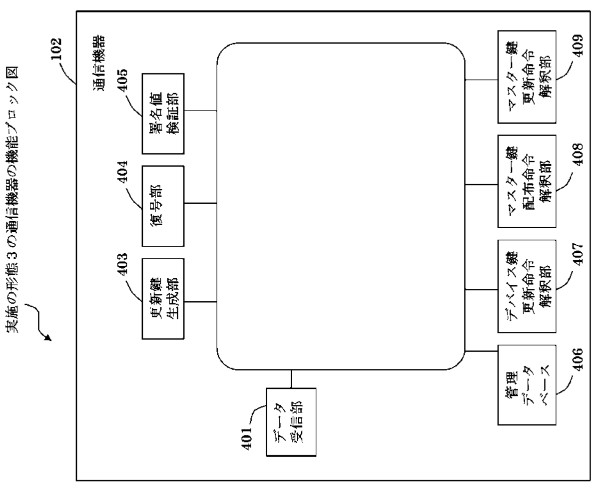
【図２２】



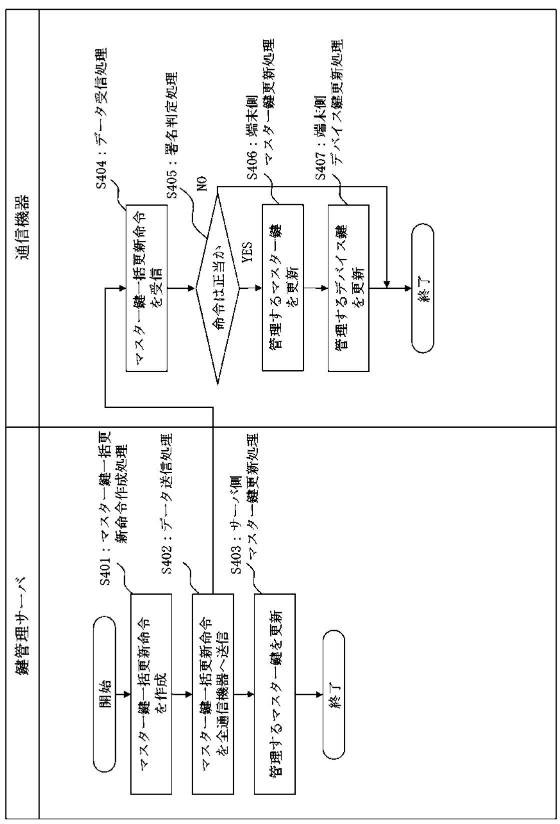
【図２３】



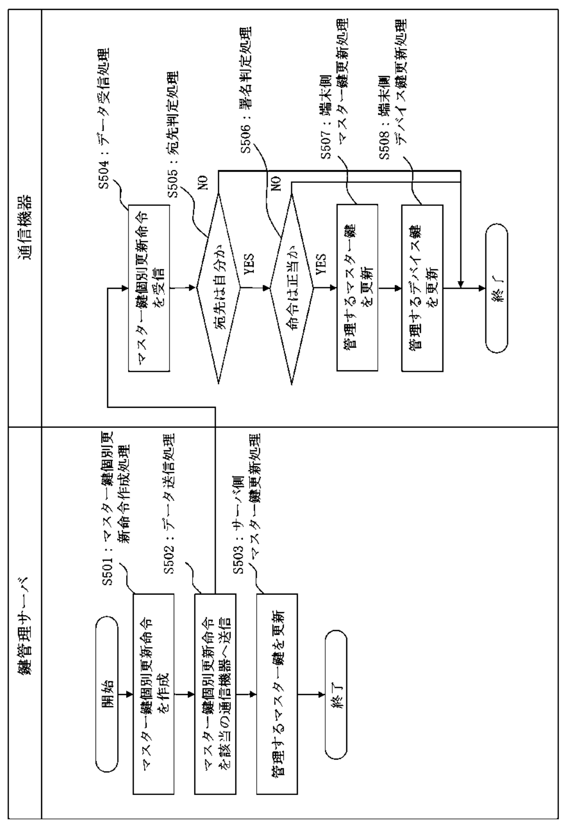
【図２４】



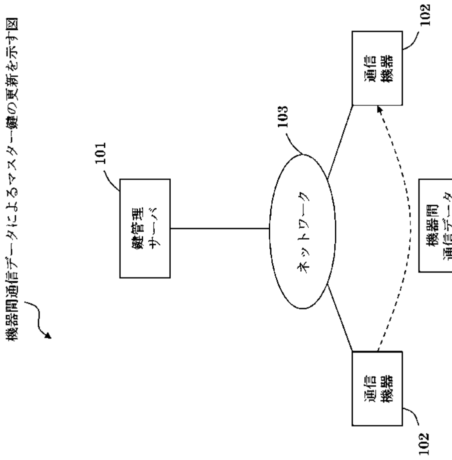
【図２５】



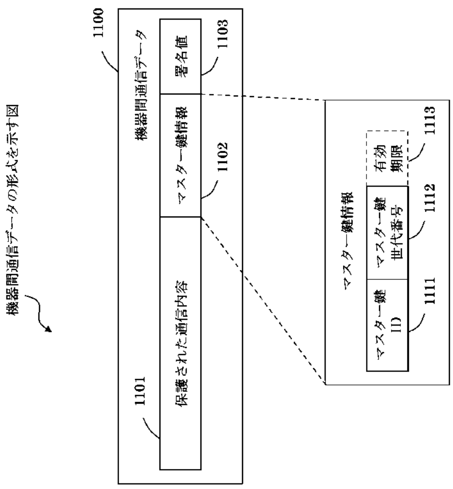
【図２６】



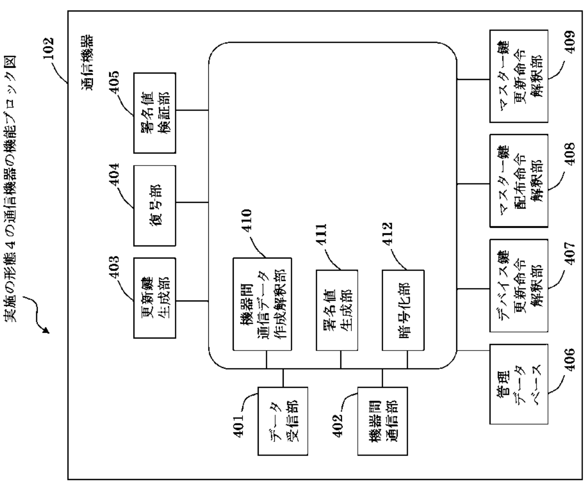
【図２７】



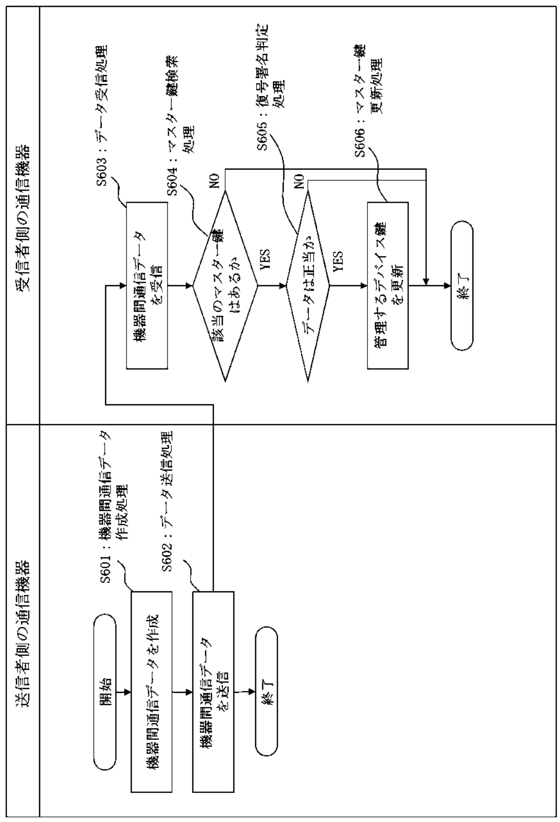
【図２８】



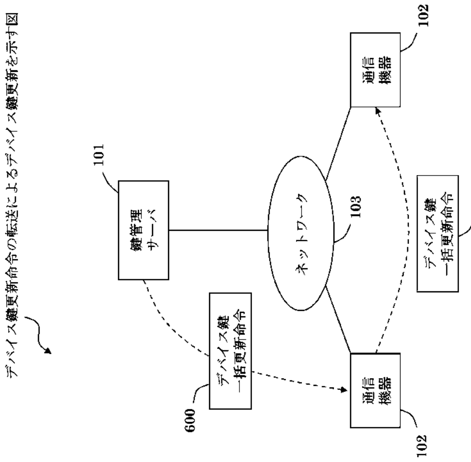
【図２９】



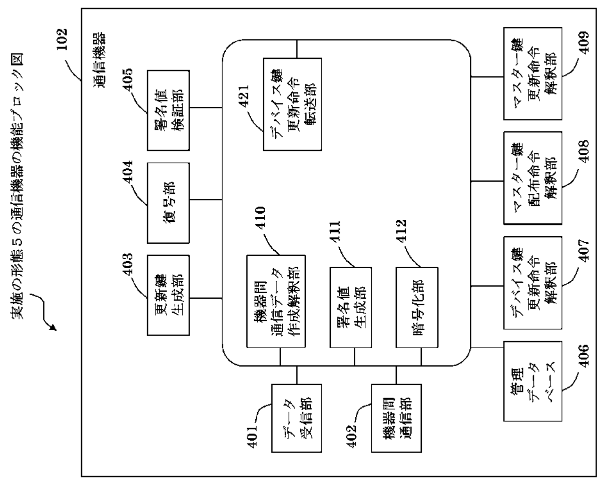
【図３０】



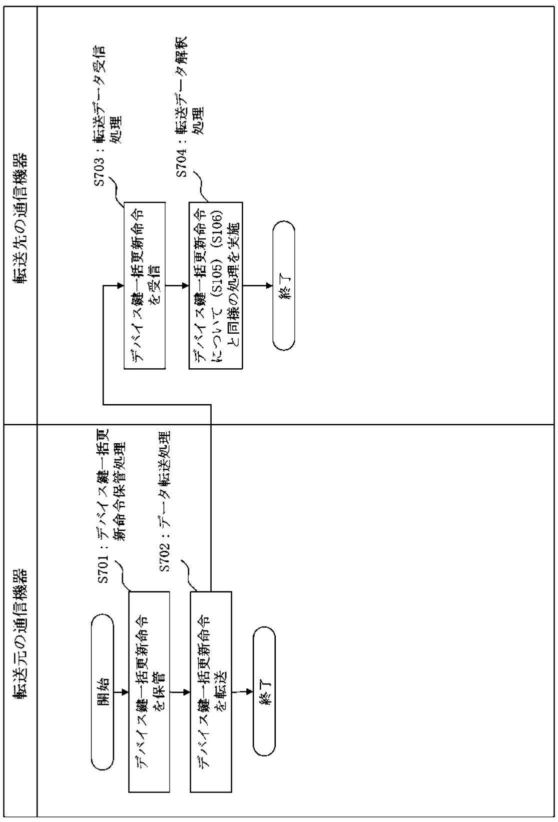
【図３１】



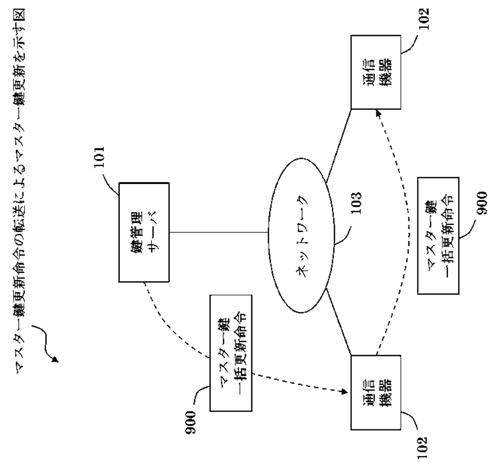
【図３２】



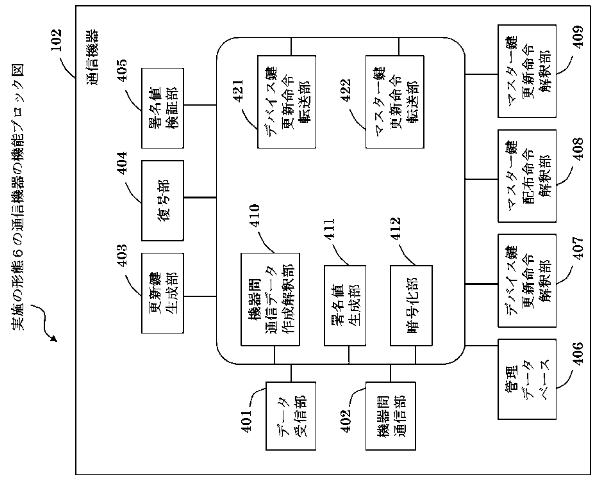
【図３３】



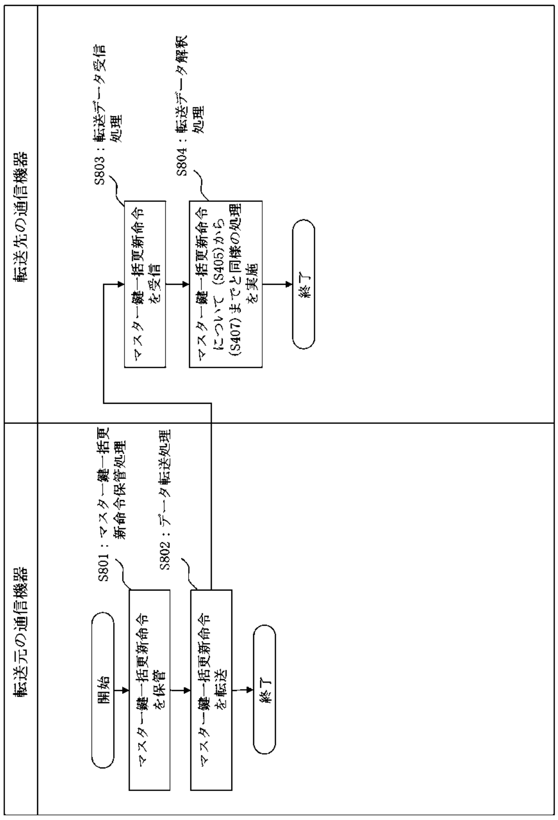
【図３４】



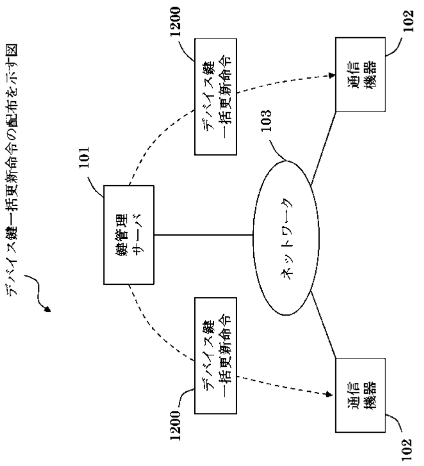
【図３５】



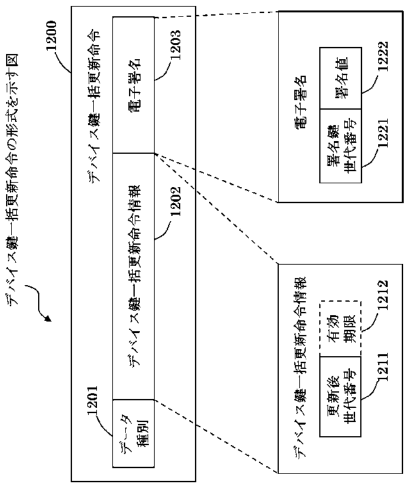
【図３６】



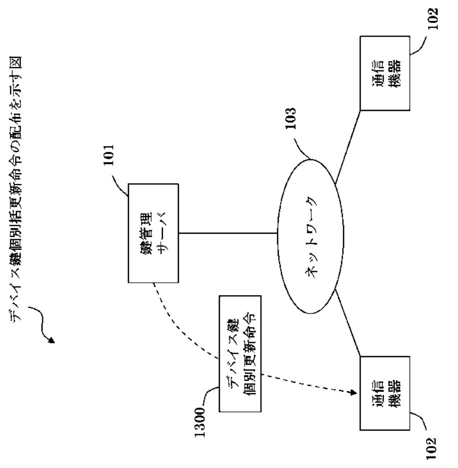
【図３７】



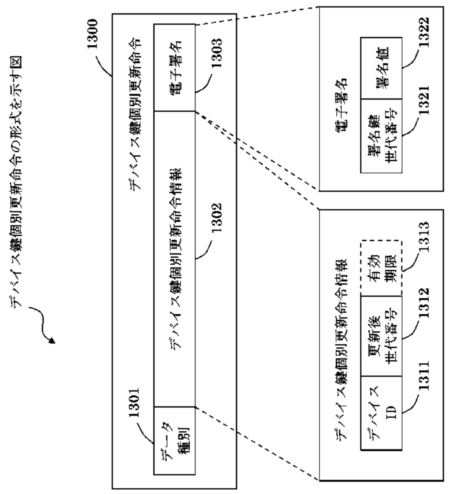
【図３８】



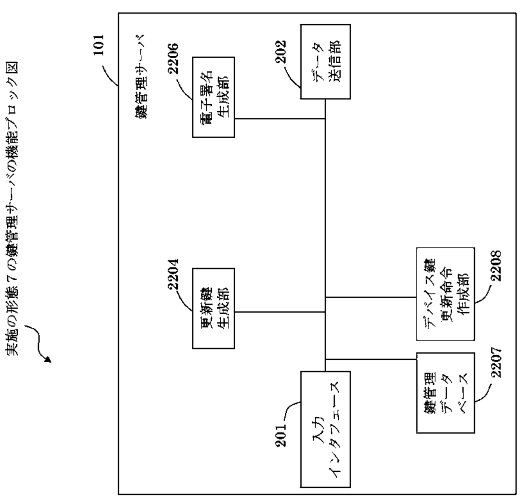
【図３９】



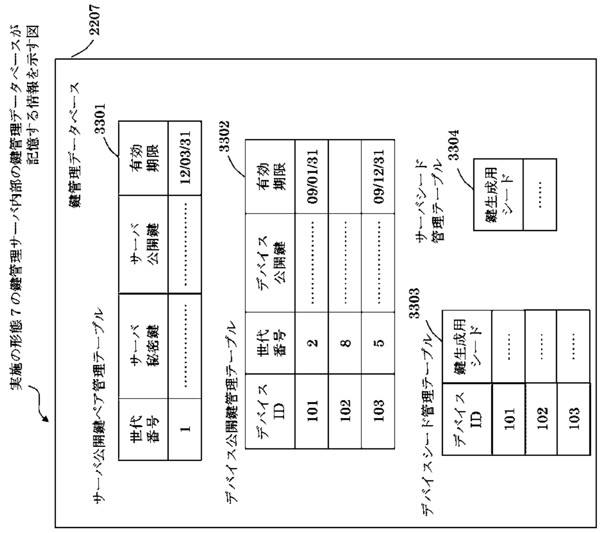
【図４０】



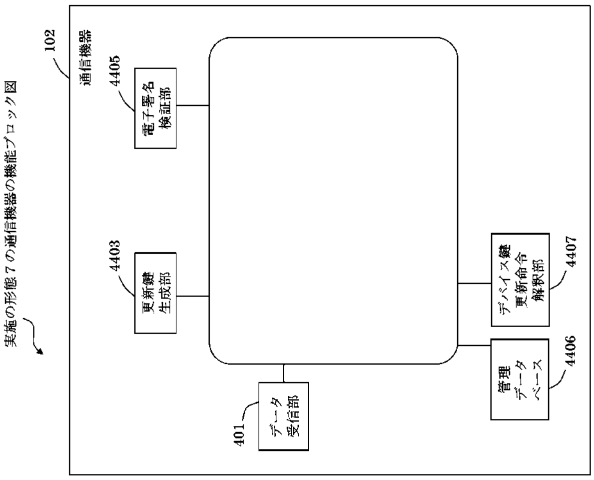
【図４１】



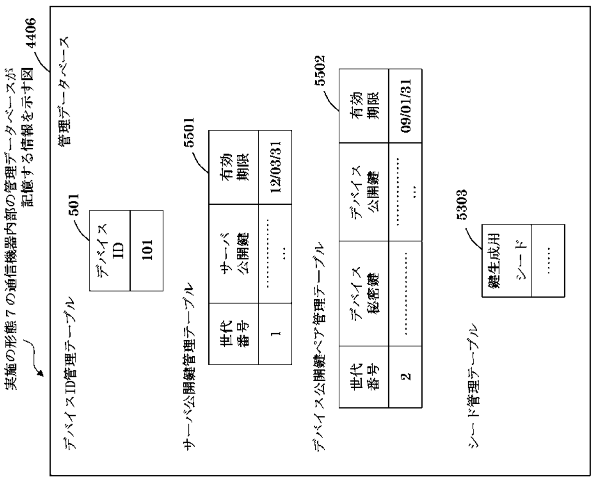
【図４２】



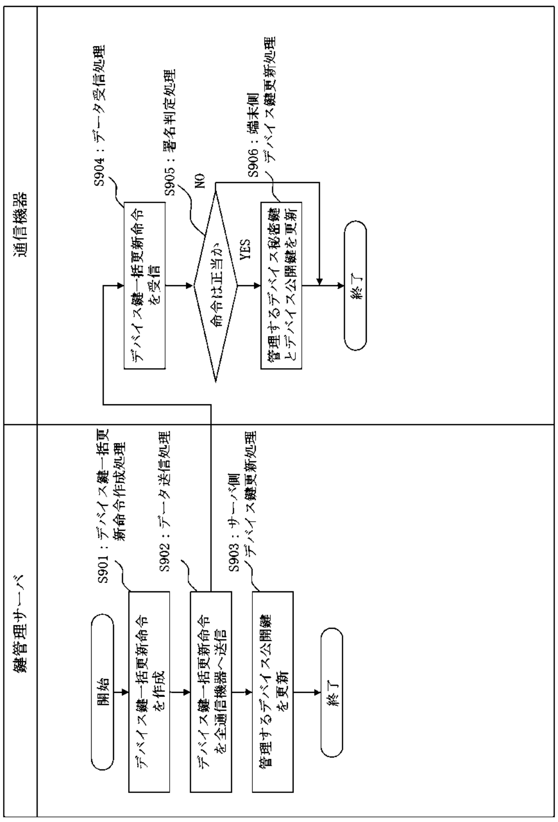
【図４３】



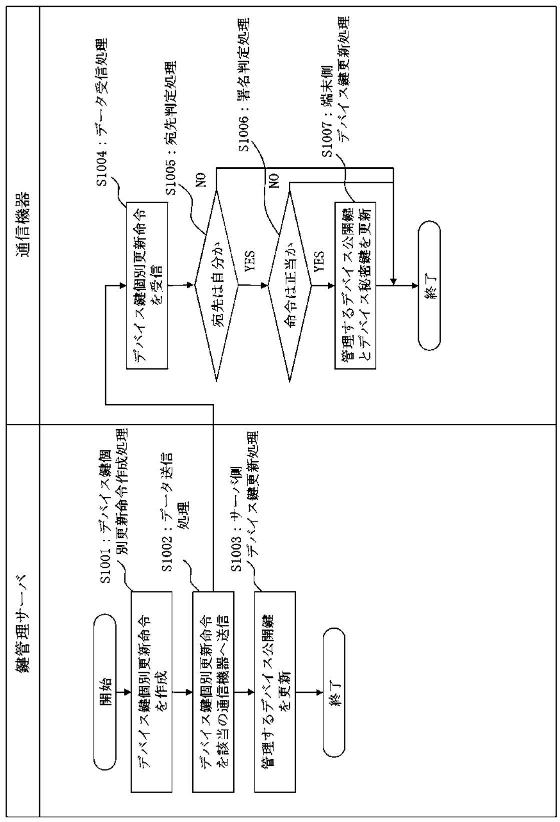
【図４４】



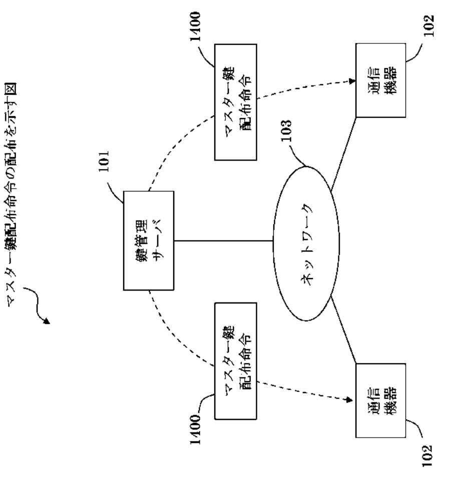
【図４５】



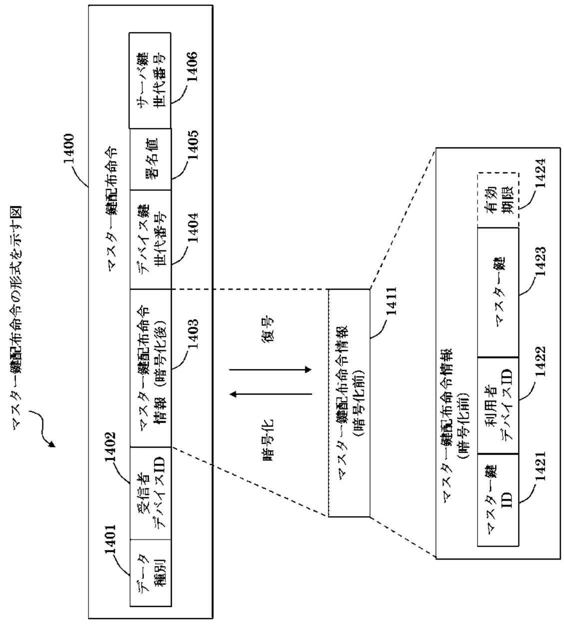
【図４６】



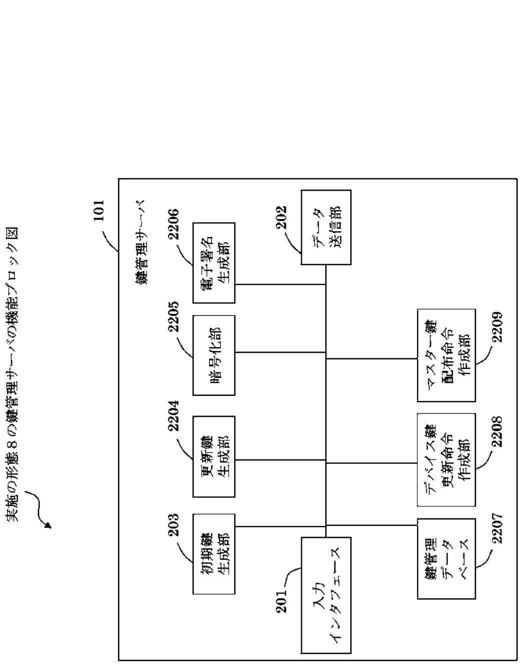
【図４７】



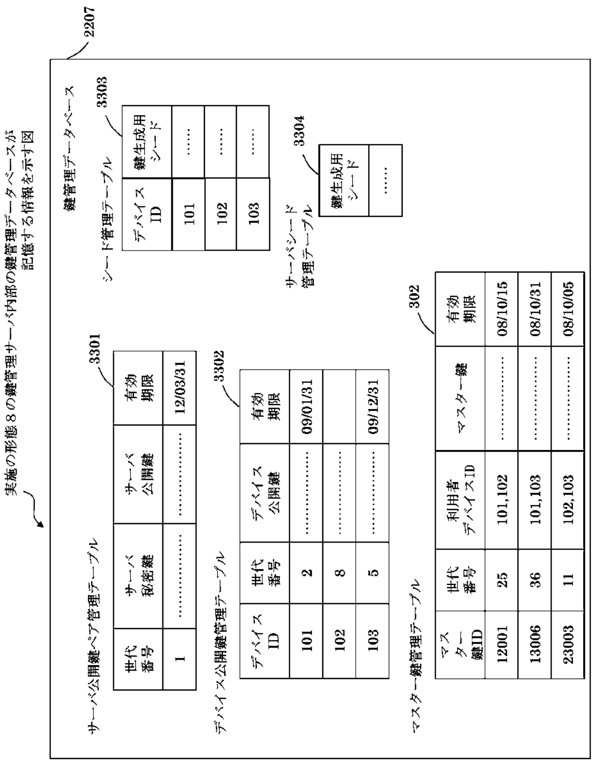
【図４８】



【図４９】



【図５０】



世代番号	サーバ秘密鍵	サーバ公開鍵	有効期限
1	…………	…………	12/03/31

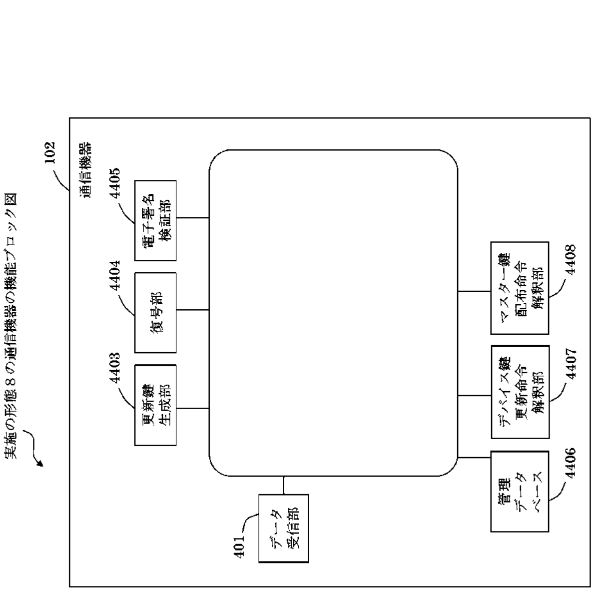
デバイスID	世代番号	デバイス公開鍵	有効期限
101	2	…………	09/01/31
102	8	…………	
103	5	…………	09/12/31

マスター鍵ID	世代番号	利用者デバイスID	マスター鍵	有効期限
12001	25	101,102	…………	08/10/15
13006	36	101,103	…………	08/10/31
23003	11	102,103	…………	08/10/05

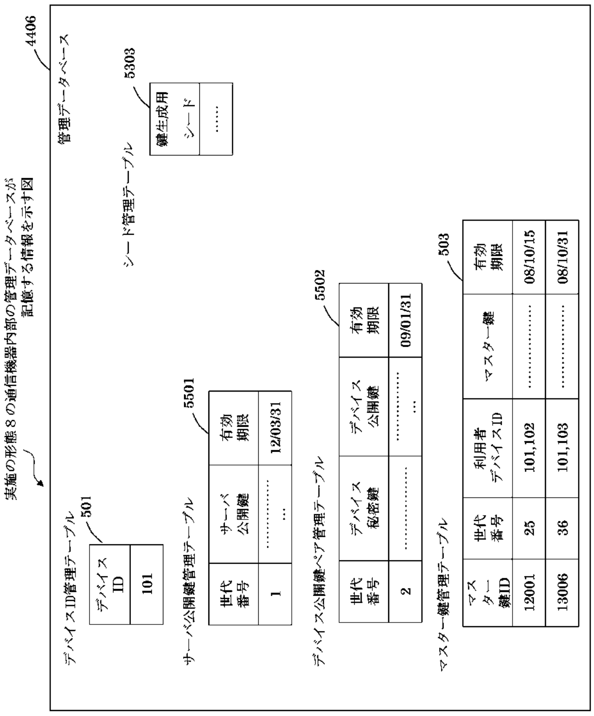
デバイスID	鍵生成用シード
101	……
102	……
103	……

鍵生成用シード
……

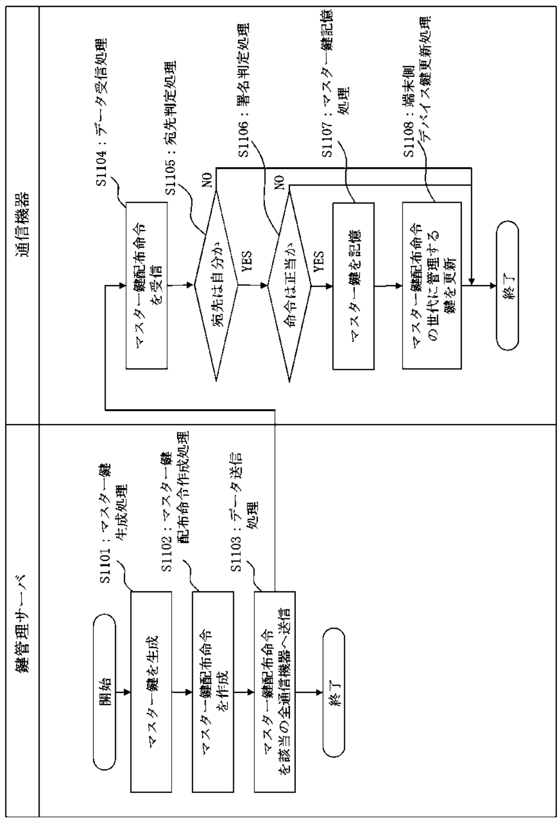
【図５１】



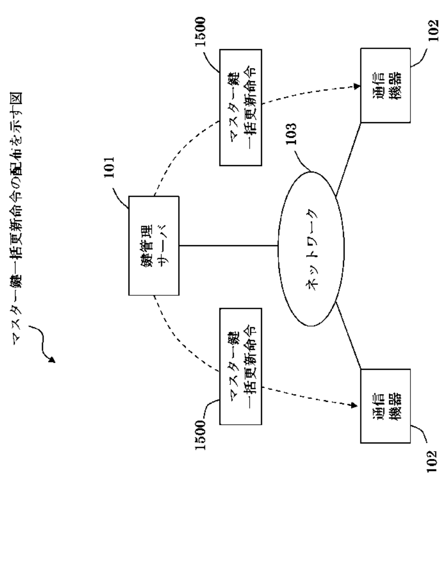
【図５２】



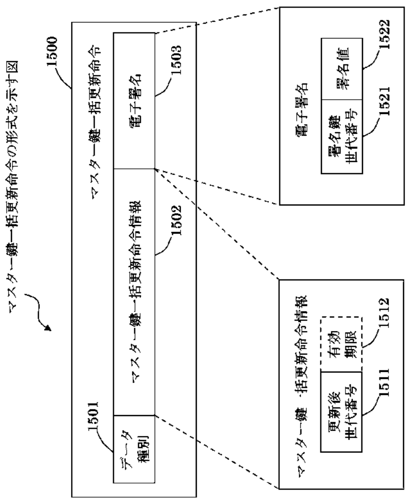
【図５３】



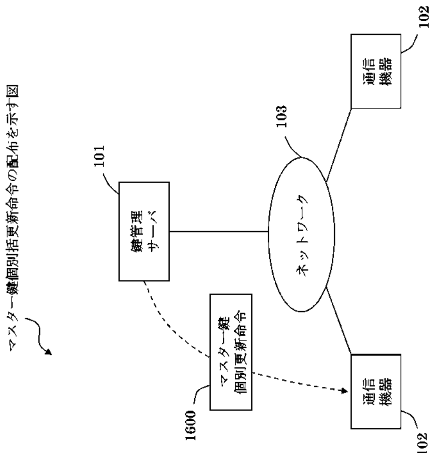
【図５４】



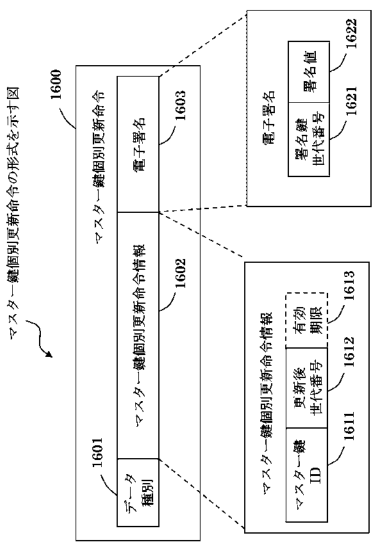
【図５５】



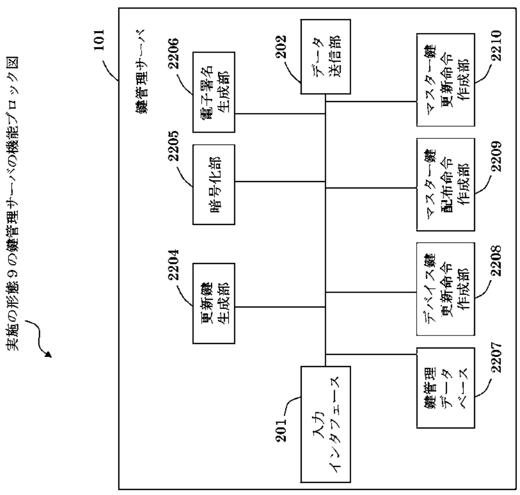
【図５６】



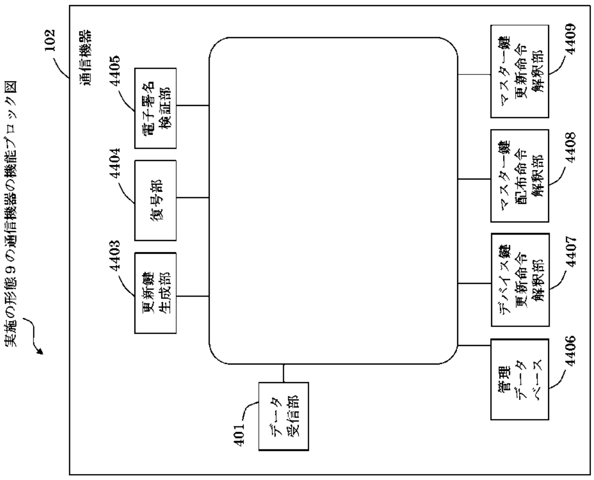
【図５７】



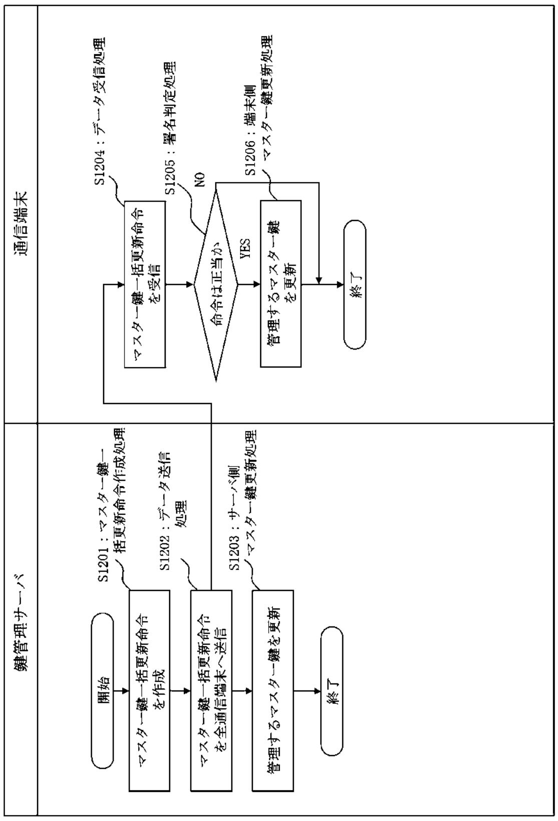
【図５８】



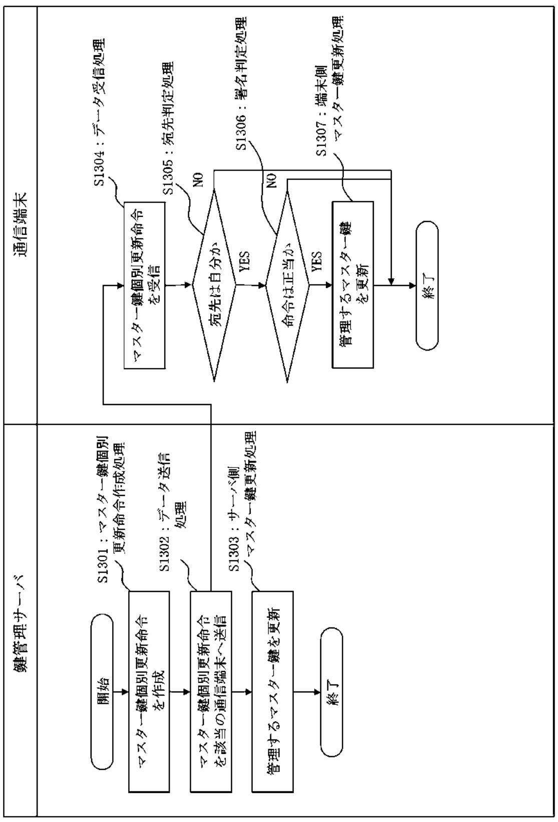
【図５９】



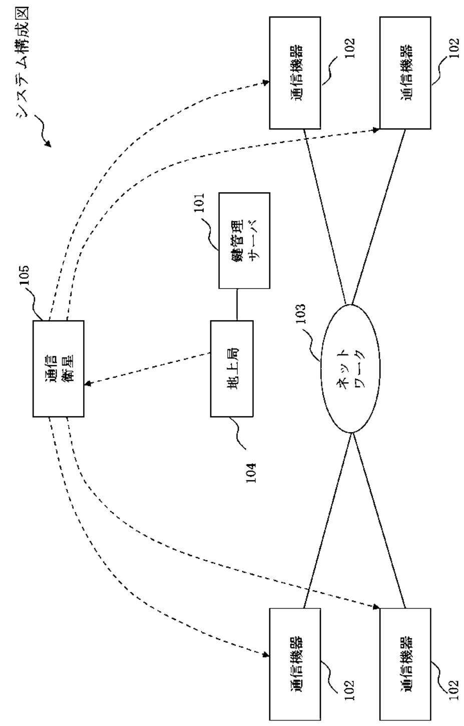
【図６０】



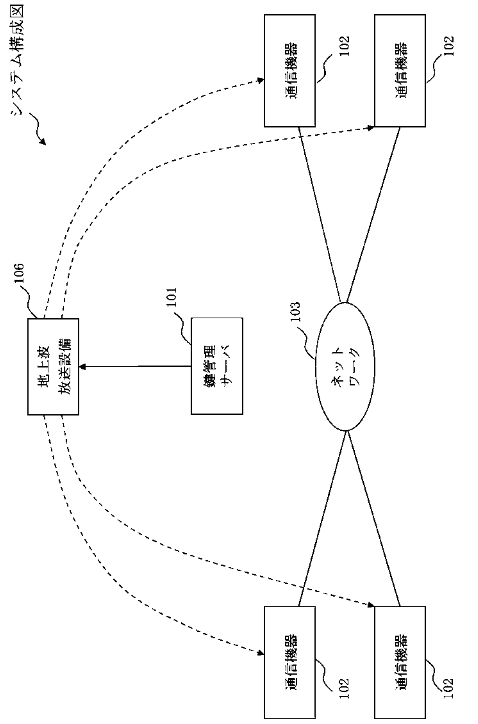
【図６１】



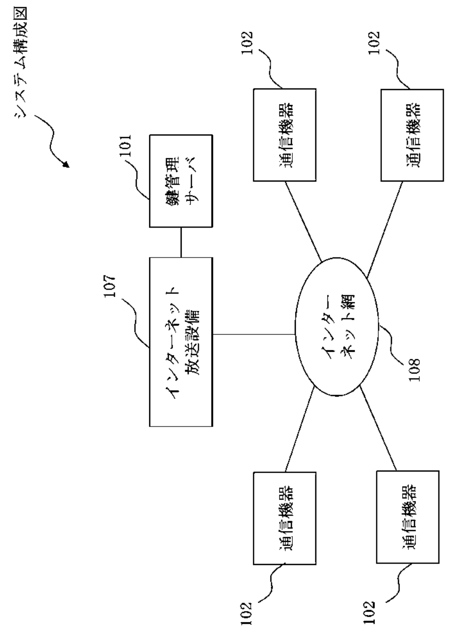
【図６２】



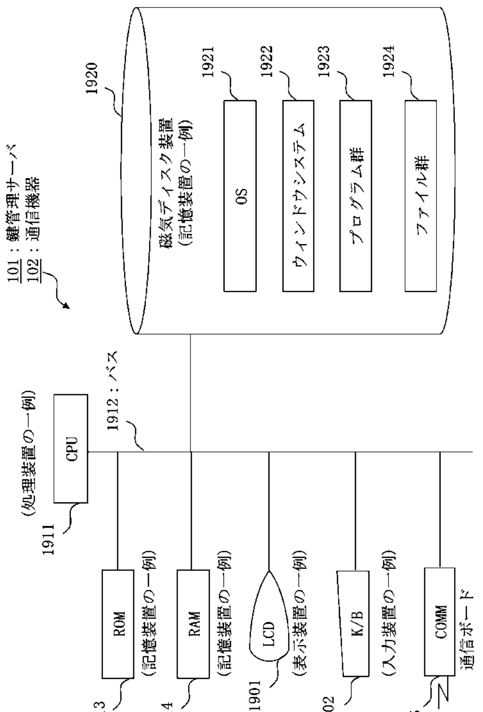
【図６３】


システム構成図
106
地上波
放送設備
101
鍵管理
サーバ
103
ネット
ワーク
通信機器
102
通信機器
102
通信機器
102
通信機器
102

【図６４】


システム構成図
101
鍵管理
サーバ
107
インターネット
放送設備
インター
ネット網
108
通信機器
102
通信機器
102
通信機器
102
通信機器
102

【図６５】


101：鍵管理サーバ
102：通信機器
1920
磁気ディスク装置
(記憶装置の一例)
1921
OS
1922
ウィンドウシステム
1923
プログラム群
1924
ファイル群
1911
CPU
(処理装置の一例)
1912：バス
1913
ROM
(記憶装置の一例)
1914
RAM
(記憶装置の一例)
1901
LCD
(表示装置の一例)
1902
K/B
(入力装置の一例)
1915
COMM
通信ボード

フロントページの続き

(72)発明者　太田　英憲
　　　　　東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　松田　規
　　　　　東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　伊藤　隆
　　　　　東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　服部　充洋
　　　　　東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

　審査官　松平　英

(56)参考文献　特開２００８－１３５８１６（ＪＰ，Ａ）
　　　　　　特開２０００－１９６６１６（ＪＰ，Ａ）
　　　　　　特開２００７－１８１２１３（ＪＰ，Ａ）
　　　　　　特開２００７－１７４０８３（ＪＰ，Ａ）
　　　　　　特表２００７－５０８７７８（ＪＰ，Ａ）
　　　　　　特開２００１－１４８７３１（ＪＰ，Ａ）
　　　　　　特開２００１－１４８７３５（ＪＰ，Ａ）
　　　　　　特開２００６－２４５６６３（ＪＰ，Ａ）
　　　　　　特開２００７－２０１５２２（ＪＰ，Ａ）
　　　　　　特開２００８－１８７３９９（ＪＰ，Ａ）
　　　　　　宝木　和夫　他，暗号方式と応用，情報処理　，日本，社団法人情報処理学会，１９９１年　６月１５日，第３２巻　第6号，ｐ．７１４～７２３
　　　　　　大津　一樹　他，Ｐ２Ｐファイル共有システムにおける鍵管理効率化手法の検討，マルチメディア，分散，協調とモバイル（ＤＩＣＯＭＯ　２００５）シンポジウム論文集，日本，社団法人情報処理学会，２００５年　7月　6日，ｐ．６０９～６１２
　　　　　　大津　一樹　他，Ｐ２Ｐファイル共有システムにおける鍵管理効率化手法の実装評価，情報処理学会論文誌，日本，社団法人情報処理学会，２００６年　8月１５日，第４７巻　第8号，ｐ．２４６４～２４７６

(58)調査した分野(Int.Cl.，ＤＢ名)
　　　　　　Ｈ０４Ｌ　　９／００
　　　　　　Ｇ０９Ｃ　　１／００
　　　　　　Ｇ０６Ｆ　２１／２４
　　　　　　Ｈ０４Ｌ　１２／００
　　　　　　Ｈ０４Ｌ　２９／００
　　　　　　Ｈ０４Ｗ　　４／００