(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2014-17595
(P2014-17595A)
(43)公開日　平成26年1月30日(2014.1.30)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/14	(2006.01)	H04L	9/00	641	5J104

審査請求 未請求　請求項の数 15　ＯＬ　（全 17 頁）

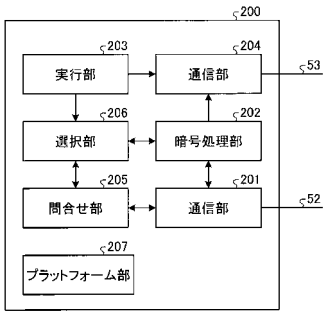
(21)出願番号　特願2012-152426 (P2012-152426)
(22)出願日　平成24年7月6日 (2012.7.6)

(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　谷澤　佳道
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　馬場　伸一
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 AA16　EA04　EA15　EA16　JA03
NA02　NA37

(54)【発明の名称】通信装置、鍵生成装置、通信方法、プログラムおよび通信システム

(57)【要約】
【課題】アプリケーションの要求に照らして、スループットとコストをも考慮した上で最適な暗号通信方式を選択する。
【解決手段】暗号鍵を生成する鍵生成装置と接続される通信装置であって、問合せ部と、暗号処理部と、選択部と、を備える。問合せ部は、鍵生成装置が暗号鍵を生成する能力を表す能力情報を鍵生成装置に問い合わせる。暗号処理部は、複数の暗号機能を実行する。選択部は、複数の暗号機能のうち、能力情報に応じた暗号機能を選択する。暗号処理部は、選択部により選択された暗号機能を実行する。
【選択図】図３



【特許請求の範囲】
【請求項１】
暗号鍵を生成する鍵生成装置と接続される通信装置であって、
前記鍵生成装置が前記暗号鍵を生成する能力を表す能力情報を前記鍵生成装置に問い合わせる問合せ部と、
複数の暗号機能を実行する暗号処理部と、
複数の前記暗号機能のうち、前記能力情報に応じた前記暗号機能を選択する選択部と、
を備え、
前記暗号処理部は、選択された前記暗号機能を実行する、
通信装置。
【請求項２】
前記暗号機能を用いた通信処理を実行する通信部をさらに備え、
前記問合せ部は、前記通信部によって通信処理が実行されている間に、前記能力情報を前記鍵生成装置に問い合わせる、
請求項１に記載の通信装置。
【請求項３】
前記選択部は、前記能力情報に応じた複数の前記暗号機能を選択し、
前記暗号処理部は、選択された複数の前記暗号機能を実行する、
請求項１に記載の通信装置。
【請求項４】
選択された複数の前記暗号機能それぞれに対応する複数の通信を確立し、確立した複数の通信を用いた通信処理を実行する通信部をさらに備える、
請求項３に記載の通信装置。
【請求項５】
前記選択部は、複数の前記暗号機能のうち、前記能力情報と、前記暗号鍵を利用する処理の要求を表す要求情報と、に応じた前記暗号機能を選択する
請求項１に記載の通信装置。
【請求項６】
暗号鍵を利用する通信装置と接続される鍵生成装置であって、
前記暗号鍵を生成する生成部と、
前記通信装置が実行可能な複数の暗号機能を示す暗号機能情報を前記通信装置から受信する受信部と、
前記暗号機能情報が示す複数の前記暗号機能のうち、前記生成部が前記暗号鍵を生成する能力を表す能力情報に応じた前記暗号機能を選択する選択部と、
を備える鍵生成装置。
【請求項７】
生成された前記暗号鍵を前記通信装置に送信する通信部をさらに備える、
請求項６に記載の鍵生成装置。
【請求項８】
前記選択部は、前記能力情報に応じた複数の前記暗号機能を選択する、
請求項６に記載の鍵生成装置。
【請求項９】
前記受信部は、さらに、前記暗号鍵を利用する処理の要求を表す要求情報を前記通信装置から受信し、
前記選択部は、複数の前記暗号機能のうち、前記能力情報と前記要求情報とに応じた前記暗号機能を選択する
請求項６に記載の鍵生成装置。
【請求項１０】
暗号鍵を生成する鍵生成装置と接続される通信装置で実行される通信方法であって、
前記暗号鍵を生成する機能の能力を表す能力情報を前記鍵生成装置に問い合わせる問合

せステップと、
複数の暗号機能を実行する暗号処理ステップと、
複数の前記暗号機能のうち、前記能力情報に応じた前記暗号機能を選択する選択ステップと、を含み、
前記暗号処理ステップは、選択された前記暗号機能を実行する、
通信方法。
【請求項１１】
暗号鍵を利用する通信装置と接続される鍵生成装置で実行される通信方法であって、
前記暗号鍵を生成する生成ステップと、
前記通信装置が実行可能な複数の暗号機能を示す暗号機能情報を前記通信装置から受信する受信ステップと、
前記暗号機能情報が示す複数の前記暗号機能のうち、前記生成ステップが前記暗号鍵を生成する能力を表す能力情報に応じた前記暗号機能を選択する選択ステップと、
を含む通信方法。
【請求項１２】
暗号鍵を生成する鍵生成装置と接続されるコンピュータを、
前記暗号鍵を生成する機能の能力を表す能力情報を前記鍵生成装置に問い合わせる問合せ部と、
複数の暗号機能を実行する暗号処理部と、
複数の前記暗号機能のうち、前記能力情報に応じた前記暗号機能を選択する選択部と、として機能させるためのプログラムであって、
前記暗号処理部は、選択された前記暗号機能を実行する、
プログラム。
【請求項１３】
暗号鍵を利用する通信装置と接続されるコンピュータを、
前記暗号鍵を生成する生成部と、
前記通信装置が実行可能な複数の暗号機能を示す暗号機能情報を前記通信装置から受信する受信部と、
前記暗号機能情報が示す複数の前記暗号機能のうち、前記生成部が前記暗号鍵を生成する能力を表す能力情報に応じた前記暗号機能を選択する選択部と、
として機能させるためのプログラム。
【請求項１４】
暗号鍵を生成する鍵生成装置と通信装置とを備える通信システムであって、
前記通信装置は、
前記暗号鍵を生成する機能の能力を表す能力情報を前記鍵生成装置に問い合わせる問合せ部と、
複数の暗号機能を実行する暗号処理部と、
複数の前記暗号機能のうち、前記能力情報に応じた前記暗号機能を選択する選択部と、を備え、
前記暗号処理部は、選択された前記暗号機能を実行し、
前記鍵生成装置は、
前記暗号鍵を生成する生成部と、
前記問合せ部からの問合せに応じて前記能力情報を前記通信装置に送信する通信部と、を備える、
通信システム。
【請求項１５】
暗号鍵を生成する鍵生成装置と通信装置とを備える通信システムであって、
前記鍵生成装置は、
前記暗号鍵を生成する生成部と、
前記通信装置が実行可能な複数の暗号機能を示す暗号機能情報を前記通信装置から受信

する受信部と、
前記暗号機能情報が示す複数の前記暗号機能のうち、前記生成部が前記暗号鍵を生成する能力を表す能力情報に応じた前記暗号機能を選択する選択部と、を備え、
前記通信装置は、
前記暗号機能情報を前記鍵生成装置に送信する送信部と、
選択された前記暗号機能を実行する暗号処理部と、
を備える通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、通信装置、鍵生成装置、通信方法、プログラムおよび通信システムに関する。
【背景技術】
【０００２】
複数のリンクによって相互に接続され、ネットワーク化された複数のノードから構成される暗号通信ネットワークが知られている。各ノードは、リンクによって接続された対向ノードとの間で乱数を生成して共有する機能（以下、生成共有ともいう）と、その乱数を暗号鍵（以下、リンク鍵）として利用して、リンク上で暗号通信を行う機能とを備える。また、ノードのうちの幾つかは、リンクとは独立に乱数を生成する機能と、別のノードに対し、生成した乱数を送信する機能とを備える。暗号通信ネットワークにおけるアプリケーションは、ノードから、乱数を取得し、これを暗号鍵（以下、アプリケーション鍵）として利用して、別のアプリケーションとの間で暗号通信を行う機能を備える。アプリケーションは、ノードと一体として実現されてもよいし、ノードと独立した端末として実現されてもよい。
【０００３】
ノードにおいて、リンクによって接続された対向ノードとの間で乱数（リンク鍵）を生成共有する機能は、例えば、一般に量子暗号通信と呼ばれる技術により実現する。この場合、ノードにおいて、リンクとは独立に乱数（アプリケーション鍵）を生成し、生成した乱数を別のノードにリンクを介して送信する技術は、量子鍵配送（Quantum Key Distribution、ＱＫＤ）と呼ばれることがある。
【先行技術文献】
【非特許文献】
【０００４】
【非特許文献１】Dianati, M., Alleaume, R., Gagnaire, M. and Shen, X. (2008), Architecture and protocols of the future European quantum key distribution network. Security and Communication Networks, 1: 57-74. DOI: 10.1002/sec.13
【発明の概要】
【発明が解決しようとする課題】
【０００５】
暗号通信ネットワーク上のノードにおいて、リンクとは独立に生成する乱数（すなわちアプリケーション鍵）は、暗号通信ネットワークにおける有限なリソースである。また、アプリケーション鍵の生成速度に関しても技術的に上限がある。従って、アプリケーションにとって、ノードからアプリケーション鍵を取得して暗号通信する方法が最もセキュアな通信であるとしても、コスト等も考慮した場合には最適な暗号通信であるとは限らない。例えば、通信スループットの制約、および、有限リソースを利用することによるコストの観点から、他の（すなわち暗号通信ネットワーク上のノードからアプリケーション鍵を取得して暗号通信する方式以外の）暗号通信方式を用いる方が、セキュリティは低くなるとしても、アプリケーションの要求を満たした通信である場合もある。このように、ノードからアプリケーション鍵を取得して暗号通信する方法が常に最適とは限らない。すなわ

ち、従来の方式では、アプリケーションの要求に照らして、スループットとコストをも考慮した上で最適な暗号通信方式を選択することができない。

【課題を解決するための手段】

【０００６】

実施形態の通信装置は、暗号鍵を生成する鍵生成装置と接続される通信装置であって、問合せ部と、暗号処理部と、選択部と、を備える。問合せ部は、鍵生成装置が暗号鍵を生成する能力を表す能力情報を鍵生成装置に問い合わせる。暗号処理部は、複数の暗号機能を実行する。選択部は、複数の暗号機能のうち、能力情報に応じた暗号機能を選択する。暗号処理部は、選択部により選択された暗号機能を実行する。

【図面の簡単な説明】

【０００７】

【図１】実施形態にかかる通信システムのネットワーク構成図。

【図２】第１の実施形態のノードのブロック図。

【図３】第１の実施形態におけるアプリケーションのブロック図。

【図４】第１の実施形態の通信システムによる通信処理のシーケンス図。

【図５】第２の実施形態にかかるノードのブロック図。

【図６】第２の実施形態にかかるアプリケーションのブロック図。

【図７】第２の実施形態の通信システムによる通信処理のシーケンス図。

【図８】第１および第２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】

【０００８】

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

【０００９】

（第１の実施形態）

第１の実施形態にかかる通信システムは、アプリケーションがノードに対し、アプリケーション鍵を生成する能力を表す能力情報（以下、アプリケーション鍵情報という）を問い合わせる。アプリケーションは、アプリケーション鍵を取得した場合に可能な暗号機能および性能と、アプリケーション鍵を取得することなく可能な暗号機能および性能と、を比較する。そして、アプリケーション要求に照らして最適な暗号通信方式を選択する。

【００１０】

アプリケーション鍵情報は、例えば以下のような情報である。

（Ａ）ノードが現在、該当アプリケーションに対して提供可能なアプリケーション鍵の量

（Ｂ）ノードが現在、生成共有を行っているアプリケーション鍵のスループットのうち、該当アプリケーションに割当て可能なアプリケーション鍵のスループットに関する情報

（Ｃ）アプリケーション鍵の量またはスループットを該当アプリケーションに割り当てる場合に必要となるコストに関する情報

【００１１】

図１は、本実施形態にかかる通信システムのネットワーク構成例を示す図である。通信システムは、鍵生成装置としてのノード１００ａ～１００ｃと、アプリケーション２００ａ、２００ｃと、を含む。

【００１２】

ノード１００ａ～１００ｃを区別する必要がない場合は、単にノード１００という場合がある。アプリケーション２００ａ、２００ｃを区別する必要がない場合は、単にアプリケーション２００という場合がある。ノード１００の個数は３に限られるものではない。また、アプリケーション２００の個数は２に限られるものではない。

【００１３】

ノード１００ａ～１００ｃは、上述のように、対向ノードとの間で乱数を生成共有する機能と、生成した乱数をリンク鍵として利用して、リンク（リンク３００ａ、３００ｂ）上で暗号通信を行う機能とを備える。ノード１００は、リンクとは独立に乱数を生成する

機能と、別のノードに対して生成した乱数を送信する機能とを備えてもよい。

【００１４】

図２は、ノード１００の構成の一例を示すブロック図である。図２に示すように、ノード１００は、第１通信部１０１と、生成部１０２と、鍵管理部１０３と、第２通信部１０４と、プラットフォーム部１０５と、を備えている。

【００１５】

第１通信部１０１は、他のノード１００（外部装置）との間の通信リンク（ノード間通信リンク）であるリンク５１によって接続された他のノード（以下、対向ノードともいう）との間で、量子暗号通信技術を用いて、乱数を生成共有し、生成した乱数をリンク鍵として管理する。なお、量子暗号通信技術以外の方法でリンク鍵を生成共有してもよい。また、第１通信部１０１は、リンク５１によって接続された他のノードとの間でデータの送受信（ノード間データ通信）を行う際に利用される。ここで、データ通信の相手となる他のノードとは、リンク５１によって直接接続された対向ノードである場合もあるし、その対向ノードの別のリンクを介してさらに接続される別のノードである場合もある。この場合、第１通信部１０１は、暗号通信ネットワークにおいて、複数のノード１００を介して通信を行うためのルーティング機能を提供してもよい。また、ノード間データ通信は、第１通信部１０１が管理するリンク鍵を用いて暗号化された通信であってもよい。

【００１６】

生成部１０２は、第１通信部１０１とは独立に、乱数を生成し、生成した乱数を他のノード１００と共有する機能を持つ。他のノード１００と乱数を共有する際に、第１通信部１０１の機能を用いてもよい。生成部１０２が生成共有した乱数を、アプリケーション鍵と呼ぶ。

【００１７】

また、生成部１０２は、第２通信部１０４を介したアプリケーション２００からの問い合わせに対して、現在提供可能なアプリケーション鍵の量、現在生成共有を行っているアプリケーション鍵のうち該当アプリケーション２００に割当て可能なアプリケーション鍵のスループットに関する情報、および、スループットや鍵の量を実現するために必要なコストに関する情報、を通知する機能を持つ。ノード１００がこれらの情報を把握する方法はどのような方法であってもよい。ノード１００は、何らかの方法により、これらの情報を把握していればよい。

【００１８】

鍵管理部１０３は、生成部１０２が生成共有したアプリケーション鍵を管理する。鍵管理部１０３は、第２通信部１０４からの要求に応じて、適切なアプリケーション鍵を選択して受け渡す。

【００１９】

第２通信部１０４は、アプリケーション２００との間の通信リンクであるリンク５２（アプリケーション通信リンク）を介して、アプリケーション２００と接続して通信する。第２通信部１０４は、アプリケーション２００からの要求を受け付け、アプリケーション２００に対してアプリケーション鍵を提供する。

【００２０】

ここで、アプリケーション通信リンクについては特に規定しないため、アプリケーション２００は、何らかのネットワークを介してノード１００と接続される別のコンピュータ上に存在していてもよい。この場合、ノード１００とアプリケーション２００とを接続するネットワーク上では、ファイアウォール、データの暗号化、およびデータの認証等、既存のネットワークセキュリティ機能が実現されていてもよい。アプリケーション２００がノード１００上に存在し、ソフトウェアのＡＰＩ（Application Program Interface）を介して第２通信部１０４と接続していてもよい。

【００２１】

プラットフォーム部１０５は、ノード１００上の他の構成要素の管理や、動作に必要なコンピュータのオペレーティングシステム機能等を提供する。

【００２２】
以上、第１の実施形態におけるノード１００の構成について説明した。次に、第１の実施形態におけるアプリケーション２００の構成例について説明する。図３は、第１の実施形態におけるアプリケーション２００の構成例を示すブロック図である。図３に示すように、アプリケーション２００は、通信部２０１と、暗号処理部２０２と、実行部２０３と、通信部２０４と、問合せ部２０５と、選択部２０６と、プラットフォーム部２０７と、を備えている。
【００２３】
通信部２０１は、アプリケーション通信リンク（リンク５２）を介して、ノード１００（具体的にはノード１００の第２通信部１０４）と接続して各種データを送受信する。例えば、通信部２０１は、暗号通信を行うために必要なアプリケーション鍵をノード１００から取得する。
【００２４】
暗号処理部２０２は、データの暗号化処理および復号処理の機能を提供する。第１の実施形態の暗号処理部２０２は、複数の暗号機能のうち、選択された暗号機能を実行する。アプリケーション２００が備えるセキュリティチップやＣＰＵ（Central Processing Unit）等のハードウェアリソース、および、暗号ライブラリ等のソフトウェアリソースにより、提供可能な暗号機能や性能は異なる。提供可能な暗号機能の１つとして、通信部２０１が取得したアプリケーション鍵を保持し、アプリケーション鍵を利用して、暗号通信を行う上で必要なデータの暗号化処理と復号処理を行ってもよい。
【００２５】
なお、暗号機能が利用する暗号アルゴリズム（暗号方式）については特に限定は行わない。アプリケーション鍵を利用してもしなくても良いし、また、例えば、ＡＥＳ（Advanced Encryption Standard）の様なブロック暗号であってもよいし、ＯＴＰ（One-time Pad）の様なバーナム暗号であってもよい。
【００２６】
暗号処理部２０２はさらに、提供可能な暗号機能に関する情報に加え、性能に関する情報を把握してこれを選択部２０６等へ通知可能であってもよい。暗号機能に関する情報とは、一般的にはサポートする暗号アルゴリズムおよび認証アルゴリズムやその鍵長の情報である。例えば、「ＡＥＳ－１２８－ＣＢＣ」、「ＡＥＳ－２５６－ＣＢＣ」、「ＤＥＳ－ＥＤＥ３」等のアルゴリズム・鍵長・モードを示す文字列でもよい。性能に関する情報とは、その暗号機能を利用した場合に処理可能な一定時間あたりのデータ量、および、暗号機能を利用したときのＣＰＵ負荷などに関する情報である。例えば、１０Ｇｂｐｓ、１００Ｍｂｐｓといったスループットの形式、ＣＰＵ負荷（％表示）である。または、一定サイズのデータを処理するのに必要なＣＰＵ命令数等で表現してもよい。
【００２７】
なお、第１の実施形態においては、暗号処理部２０２がこれらの情報を把握する方法はどのような方法であってもよい。暗号処理部２０２は、何らかの方法により、これらの情報を把握していればよい。
【００２８】
暗号処理部２０２がいずれの暗号機能を利用するかは、後述する選択部２０６等によって決定および設定される。また、暗号処理部２０２が、どのような暗号機能を利用しているかは、実行部２０３や通信部２０４には隠蔽されてもよい。
【００２９】
実行部２０３は、暗号通信を行うアプリケーション機能を実行する。通信を行うものであれば特にアプリケーション機能の種類は限定しない。例えば、実行部２０３は、ビデオ送信等の機能を実行する。実行部２０３は、送信データを通信部２０４へと受け渡し、受信データを通信部２０４から受け取る。
【００３０】
実行部２０３は、何らかの方法（例えばユーザ、管理者、および、アプリケーション開

発者による設定、統計情報処理、および、自動制御等の方法）により、アプリケーション要求に関する情報（要求情報）を保持しているものとする。要求情報とは、例えば、セキュリティ（暗号化処理および復号処理の安全性に対する要求）、スループット（通信速度に対する要求）、コスト（アプリケーション鍵という有限リソースを消費することに伴って発生する、（例えば金銭的な）コストに対する要求）、および、それらの優先度等を数値化した値である。

【００３１】

通信部２０４は、実行部２０３の動作に必要な通信機能を提供する。また、データ通信の際には、暗号処理部２０２を用いてデータの暗号化と復号を行うことができる。通信部２０４は、アプリケーション２００から送信データを受けとると、暗号処理部２０２を用いてこれを暗号化し、データ通信リンク（リンク５３）を介してデータを送信する。データ通信リンクは、通信相手のアプリケーション２００との間でデータを送受信するためのリンクである。また、通信部２０４は、データ通信リンクからデータを受信すると、暗号処理部２０２を用いて受信したデータを復号し、アプリケーション２００へと復号したデータを受け渡す。

【００３２】

問合せ部２０５は、通信部２０１を介して、上述の（Ａ）～（Ｃ）のようなアプリケーション鍵情報をノード１００に対して問い合わせる。問い合わせによって得られた結果は、選択部２０６に渡される。

【００３３】

選択部２０６は、得られたアプリケーション鍵情報等を参照し、アプリケーション２００を実行する際に、最適な暗号機能を選択する。選択部２０６は、ノード１００に問い合わせて得られたアプリケーション鍵情報の他に、以下のようなアプリケーション２００に関する情報（以下、アプリケーション情報という）を用いて暗号機能を選択してもよい。選択部２０６が選択時に参照する情報は、これらに限定されないし、このうちの一部のみ参照してもよい。

（１）実行部２０３から取得した要求情報

（２）暗号処理部２０２から取得した、アプリケーション２００が自身で実現可能な暗号機能および性能に関する情報（以下、暗号機能情報という）

（３）プラットフォーム部２０７等から取得した、現在のアプリケーション２００におけるリソース使用状況に関する情報（以下、リソース情報という）

【００３４】

プラットフォーム部２０７は、アプリケーション２００上の他の構成要素の管理や、動作に必要なコンピュータのオペレーティングシステム機能等を提供する。

【００３５】

以上、第１の実施形態におけるアプリケーション２００の構成について説明した。ただし、上記説明は一例である。

【００３６】

なお、ノード１００およびアプリケーション２００の各部は、例えば、ＣＰＵ（Central Processing Unit）などの処理装置にプログラムを実行させること、すなわち、ソフトウェアにより実現してもよいし、ＩＣ（Integrated Circuit）などのハードウェアにより実現してもよいし、ソフトウェアおよびハードウェアを併用して実現してもよい。

【００３７】

次に、第１の実施形態を実現するシーケンスについて説明する。図４は、第１の実施形態の通信システムによる通信処理の一例を示すシーケンス図である。図４は、アプリケーション２００が暗号通信を開始する際に、ノード１００に対してアプリケーション鍵の生成状況について問い合わせを行い、アプリケーション２００が最適な暗号機能を選択する場合のシーケンスである。

【００３８】

アプリケーション２００の実行部２０３は、アプリケーション実行開始の前に、自身が

保持する要求情報を選択部２０６に対して通知し、本アプリケーション実行に伴う最適な暗号機能を問い合わせる。選択部２０６は、この問い合せを受けて、問合せ部２０５に対して、アプリケーション鍵の問い合わせ（鍵問い合わせ）を指示する。問合せ部２０５は、この問合せを受けて、通信部２０１を介して、ノード１００に対し、鍵問い合わせのためのメッセージを送信する（ステップＳ１０１）。

【００３９】

ノード１００の第２通信部１０４は、鍵問い合わせのメッセージを受け取る。第２通信部１０４は、鍵問い合わせを鍵管理部１０３に通知する。鍵管理部１０３は、鍵問い合わせに対して、上述の（Ａ）～（Ｃ）のアプリケーション鍵情報のうち少なくとも１つを、第２通信部１０４を介して、アプリケーション２００へ回答する（ステップＳ１０２）。アプリケーション２００の通信部２０１は、受信したアプリケーション鍵情報を問合せ部２０５へ通知する。問合せ部２０５は、アプリケーション鍵情報を選択部２０６へ通知する。

【００４０】

選択部２０６は、問合せ部２０５からアプリケーション鍵情報を取得する。選択部２０６は、さらに、提供可能な暗号機能に関して暗号処理部２０２に問い合わせを行ってもよい。この問い合わせを受けて、暗号処理部２０２は、暗号機能情報を選択部２０６に提供する。暗号機能情報は、より具体的には、利用可能なセキュリティチップ（ハードウェア）の機能および性能に関する情報、並びに、利用可能な暗号ライブラリ（ソフトウェア）の機能および性能に関する情報などである。

【００４１】

選択部２０６は、さらに、プラットフォーム部２０７に対して、アプリケーションにおけるリソース使用状況に関して問い合わせを行ってもよい。本問い合わせを受けて、プラットフォーム部２０７は、リソース情報を選択部２０６に提供する。リソース情報は、より具体的には、ＣＰＵ負荷、メモリ使用量、他ジョブの実行状況、および、セキュリティチップの利用状況などである。

【００４２】

なお、選択部２０６による問合せ部２０５からのアプリケーション鍵情報取得と、暗号処理部２０２およびプラットフォーム部２０７への問い合わせおよび情報取得のタイミングは特に限定しない。どちらが先に行われても構わない。あるいは、本シーケンス実行より前に事前に行われていても構わない。

【００４３】

選択部２０６は、以上により、実行部２０３からの要求情報、問合せ部２０５からのアプリケーション鍵情報、暗号処理部２０２からの暗号機能情報、および、プラットフォーム部２０７からのリソース情報を、受けとることができる。ただし、これは一例であり、以上のうちのいくつかの情報のみを利用してもよいし、これ以外の情報を取得してもよい。

【００４４】

選択部２０６は、以上の情報を元に、アプリケーション要求（要求情報）に照らして最適な暗号機能を選択する（ステップＳ１０３）。選択の方法には様々な方法がありえ、ここでは特に限定しない。例えば、「スループットＸを確保した上で、最もセキュリティの高い通信を行いたい」というアプリケーション要求があった場合、以下のような選択方法を適用できる。なお、この例では簡単化のため、アプリケーション２００は、セキュリティチップにより、ＡＥＳのみをサポートしているものとする。また、暗号機能によっては、

（Ｃ１）アプリケーション鍵を利用したＯＴＰ暗号（以下、ＱＫＤ　ＯＴＰ）
（Ｃ２）アプリケーション鍵を利用したＡＥＳブロック暗号（以下、ＱＫＤ　ＡＥＳ）
（Ｃ３）通常のＡＥＳ暗号

が可能であるものとする。また、これらの３種類の暗号機能にコストの差はなく、（Ｃ１）、（Ｃ２）、（Ｃ３）の順にセキュリティが高いと仮定する。

【００４５】
まず、選択部２０６は、最もセキュリティの高い（Ｃ１）の暗号機能を適用した場合のスループットＡがＸ以上であるか否かを判断する。スループットＡは、取得したアプリケーション鍵情報のうち、該当アプリケーション２００に割当て可能なアプリケーション鍵のスループットに関する情報を用いて算出できる。選択部２０６は、Ｘ＜Ａであれば、暗号機能（Ｃ１）を用いることが最適であると判断する。そうでない場合は、（Ｃ１）は最適ではない。
【００４６】
次に、選択部２０６は、２番目にセキュリティの高い（Ｃ２）のスループットＢがＸ以上か否かを判断する。スループットＢは、アプリケーション鍵情報のうち、該当アプリケーション２００に割当て可能なアプリケーション鍵のスループットに関する情報と、（Ｃ２）で用いるＡＥＳの鍵長および利用可能なセキュリティチップまたは暗号ライブラリの性能と、から算出できる。選択部２０６は、Ｘ＜Ｂであれば、暗号機能（Ｃ２）を用いることが最適であると判断する。そうでない場合は、（Ｃ２）は最適ではない。
【００４７】
最後に、選択部２０６は、３番目にセキュリティの高い（Ｃ３）のスループットＣがＸ以上か否かを判断する。スループットＣは、（Ｃ３）で用いるＡＥＳの鍵長および利用可能なセキュリティチップまたは暗号ライブラリの性能から算出できる。選択部２０６は、Ｘ＜Ｃであれば、暗号機能（Ｃ３）を用いることが最適であると判断する。
【００４８】
以上の例では、アプリケーション要求として、スループット要求のみを考慮した。例えば「コストＹ以下を確保した上で、最もセキュリティの高い通信を行いたい」というようなコストに関するアプリケーション要求（コスト要求）に対しても、同様に比較および判断してよい。また、今回の例では利用しなかったが、例えばアプリケーション２００に対して「通信データ量がＺである」ことが明らかである場合、アプリケーション２００に対して提供可能なアプリケーション鍵の量についても比較してもよい。
【００４９】
なお、アプリケーション要求を満たす暗号機能が１つも見つからなかった場合の動作はいくつか可能である。例えば、最もアプリケーション要求に近い暗号機能を選択し、選択した暗号機能を最適なものと判断する方法、および、最適な暗号機能が見つからないためエラーとしてアプリケーション２００またはユーザに通知する方法などが利用できる。
【００５０】
選択部２０６は、最適と判断した（選択した）暗号機能を利用するように、暗号処理部２０２を設定する（ステップＳ１０４）。また、選択部２０６は、実行部２０３に対して、暗号機能の選択が完了したこと、または、その結果選択された暗号機能を通知してもよい。
【００５１】
実行部２０３は、アプリケーション２００の実行を開始する（ステップＳ１０５）。アプリケーション２００は、データ通信の際、通信部２０４を利用する。このとき、選択部２０６によって最適に設定された暗号処理部２０２によって、通信データの暗号化処理および復号処理が行われる。なお、ノード１００から提供されるアプリケーション鍵が不要な場合は、アプリケーション２００はアプリケーション鍵を利用せずに別の暗号方式による暗号機能および別の暗号鍵を利用して暗号通信してもよい。
【００５２】
このように、第１の実施形態にかかる通信システムでは、アプリケーションが、ノードに問い合わせて得たアプリケーション鍵情報とアプリケーション要求とを用いて最適な暗号機能を選択することができる。
【００５３】
（変形例）
第１の実施形態では、アプリケーション機能（暗号通信）の実行開始前に暗号機能を選

択した。変形例では、暗号通信の最中であっても、利用する暗号機能を動的に変更可能とする（変形機能１）。また、第１の実施形態では、最適な１つの暗号通信方式（暗号機能）を選択したが、選択する暗号機能の個数は１に限られるものではない。変形例にかかる通信システムは、最適な暗号通信方式の組み合わせ（複数の暗号機能）を選択する（変形機能２）。なお、変形機能１および変形機能２のうちいずれか一方のみを実行してもよい。

【００５４】

変形例では、アプリケーション２００の構成要素のうち、以下の点が第１の実施形態と異なる。

【００５５】

暗号処理部２０２は、暗号通信の最中であっても、利用する暗号機能を動的に変更することができる。また、暗号処理部２０２は、複数の暗号機能（暗号アルゴリズム）を同時に設定し、暗号通信することができる。さらに、暗号処理部２０２は、通信部２０４から、送信するデータ（送信データ）と共に、送信データの重要度および機密レベルなどのメタデータを受け取り、メタデータに基づいて、送信データの暗号化に利用する暗号機能（暗号アルゴリズム）を選択することができる。なお、通信部２０４からメタデータを受け取らず、暗号処理部２０２が受け取ったデータを元にして暗号アルゴリズムを選択するように構成してもよい。

【００５６】

通信部２０４は、さらに、暗号処理部２０２に対して、データの重要度等のメタデータを受け渡すことができる。

【００５７】

問合せ部２０５は、暗号通信の最中であっても、問い合わせと、暗号処理部２０２への結果の受け渡しを行うことができる。

【００５８】

選択部２０６は、暗号通信の最中であっても、判断を行うことができる。さらに選択部２０６が、アプリケーション要求に照らして最も適切な暗号機能の組み合わせを選択してもよい。

【００５９】

以上、変形例のノードおよびアプリケーションの構成について説明した。ただし、上記説明は一例である。

【００６０】

次に、本変形例を実現するシーケンスについて説明する。処理の流れは第１の実施形態のシーケンスを表す図４と同様である。本変形例のシーケンスは、例えば、アプリケーション２００が暗号通信を行っている最中に、ノード１００に対してアプリケーション鍵の生成状況について問い合わせを行い、アプリケーション２００が最適な暗号機能を選択する場合のシーケンスである。以下、第１の実施形態との違いに着目して説明する。

【００６１】

選択部２０６は、アプリケーション実行中においても、定期的に、問合せ部２０５に対して、鍵問い合わせを指示する。問合せ部２０５は、この指示を受けて、通信部２０１を介して、ノード１００に対して鍵問い合わせを実行する（ステップＳ１０１）。

【００６２】

ノード１００は、鍵問い合わせに回答する（ステップＳ１０２）。このとき、ノードの回答は、暗号通信中である現在のアプリケーション鍵情報を返す。なお、鍵問い合わせ（ステップＳ１０１）を実行せず、ノード１００からアプリケーション２００に対してアプリケーション鍵情報を直接通知（ステップＳ１０２）するように構成してもよい。

【００６３】

アプリケーション２００の通信部２０１は、アプリケーション鍵情報を問合せ部２０５へと通知する。問合せ部２０５は、アプリケーション鍵情報を、選択部２０６へと通知する。

【００６４】
選択部２０６は、問合せ部２０５から、上述のアプリケーション鍵情報を取得する。選択部２０６は、通信中の動的な情報を受けとることができる。具体的には、選択部２０６は、実行部２０３から要求情報を受け取り、問合せ部２０５からアプリケーション鍵情報を受け取り、暗号処理部２０２から暗号機能情報を受け取り、プラットフォーム部２０７からリソース情報を受け取る。ただし、これは一例であり、以上のうちのいくつかの情報のみを利用してもよいし、これ以外の情報を取得してもよい。
【００６５】
選択部２０６は、以上の情報を元に、アプリケーション要求に照らして最適な暗号機能を選択する（ステップＳ１０３）。
【００６６】
例えば、このときの選択結果として、選択部２０６は、「暗号機能Ａと暗号機能Ｂの組み合わせ」が最適であるといった判断を行うこともできる。また、例えば判断の基準として、要求スループットを維持するために、どの暗号機能を併用すればよいか、といったロジックであってもよい。
【００６７】
選択部２０６は、最適と判断した（選択した）暗号機能を利用するように、暗号処理部２０２を設定する。この設定は、暗号通信の最中であっても反映される。暗号方式のネゴシエーションが通信相手のアプリケーションとの間で必要な場合はこれを行ってもよい。
【００６８】
また、複数の暗号機能を選択した場合、それぞれの暗号機能を利用する場合の基準（暗号機能の選択基準）も決定する。選択基準は、例えば、送信データの種別、および、付加的に渡される送信データのメタデータ等によって暗号機能を決定するための基準である。
【００６９】
実行部２０３は、アプリケーション２００の実行を継続する。アプリケーション２００には透過的であるが、データ通信の際に、暗号処理部２０２が利用している暗号機能は、アプリケーション開始時と変更しているかもしれない。この変更により、アプリケーション２００が利用可能な通信スループットは、実際にノード１００の機能により利用可能なアプリケーション鍵のスループットが変動したとしても、維持することができる。
【００７０】
なお、複数の暗号機能（暗号機能Ａと暗号機能Ｂ）を組み合わせて併用する場合には、いくつかの方法が考えられる。
【００７１】
例えば、１つのデータパケットにおいて、前半は暗号機能Ａによって暗号化したデータを含み、後半は暗号機能Ｂによって暗号化したデータを含むような新しい暗号機能を定義することで併用を実現することも可能である。この方法はデータパケットに限るものではない。例えば、データストリームを用いる通信においても、一定のデータサイズ等によって、暗号機能Ａによって暗号化したデータと暗号機能Ｂによって暗号化したデータとを交互に含むストリームを用いることも可能である。
【００７２】
また、暗号機能ごとに異なるデータ通信を行なってもよい。すなわち、通信部２０４において、例えば暗号機能Ａによって通信を行うＴＣＰ（Transmission Control Protocol）コネクションと暗号機能Ｂによって通信を行うＴＣＰコネクションの両方を確立し、並行してこれらを利用してデータ通信を行うことも可能である。ただしこの場合、データを受信する受信側のアプリケーション２００の通信部２０４にて、複数のＴＣＰコネクションによって受信したデータを、データまたはヘッダに含まれるシーケンス番号等の情報から順序制御処理等を行った上で、実行部２０３に受け渡す必要がある。
【００７３】
なお、これらの併用を行う場合であっても（併用しない場合であっても当然であるが）、通信相手となるアプリケーション２００との間でどのような暗号機能、暗号機能の組み

合わせ、および、併用方式を行うかについて、ネゴシエーションを実行し、合意する必要がある。このためのネゴシエーションの方法としては、通信部２０４が備えるハンドシェイク機能における暗号アルゴリズムネゴシエーションが利用できる。これらの暗号アルゴリズムネゴシエーションの方法は、ＴＬＳ（Transport Layer Security）／ＳＳＬ（Secure Socket Layer）等で一般的に知られた既知の方法である。暗号機能の組み合わせや併用方式に関してのネゴシエーションも合わせて行う場合、組み合わせる暗号機能や併用方法を表現する表現方法について定義し、アプリケーション間で事前に合意がなされている必要がある。

【００７４】

（第２の実施形態）

第２の実施形態にかかる通信システムは、アプリケーションではなく、ノードが最適な暗号機能を選択する。すなわち、ノードが、アプリケーションから要求情報、暗号機能情報、および、リソース情報の提供を受け、これらの情報と、ノードにて把握できるアプリケーション鍵情報とを用いて、最適な暗号機能を選択してアプリケーションに通知する。

【００７５】

図５は、第２の実施形態にかかるノード１００－２の構成の一例を示すブロック図である。図５に示すように、ノード１００－２は、第１通信部１０１と、生成部１０２と、鍵管理部１０３と、第２通信部１０４－２と、プラットフォーム部１０５と、選択部１０６－２と、を備えている。

【００７６】

第２の実施形態では、選択部１０６－２を追加したこと、および、第２通信部１０４－２の機能が第１の実施形態と異なっている。その他の構成および機能は、第１の実施形態にかかるノード１００のブロック図である図２と同様であるので、同一符号を付し、ここでの説明は省略する。

【００７７】

第２通信部１０４－２は、第１の実施形態の第２通信部１０４の機能に加え、第２の実施形態のアプリケーション２００－２（後述）から要求情報等を受信する機能を備える。すなわち、第２通信部１０４－２は、受信部５０１を備える。受信部５０１は、アプリケーション２００－２が実行可能な複数の暗号機能を示す暗号機能情報をアプリケーション２００－２から受信する。

【００７８】

選択部１０６－２は、第１の実施形態の選択部２０６と同様に、アプリケーション２００－２から受信した暗号機能情報、および、鍵管理部１０３から得られるアプリケーション鍵情報等を参照し、最適な暗号機能を選択する。また、選択部１０６－２は、選択した暗号機能を実行するように、第２通信部１０４－２を介してアプリケーション２００－２の暗号処理部２０２を設定する。

【００７９】

図６は、第２の実施形態にかかるアプリケーション２００－２の構成の一例を示すブロック図である。図６に示すように、アプリケーション２００－２は、通信部２０１－２と、暗号処理部２０２と、実行部２０３と、通信部２０４と、プラットフォーム部２０７と、情報提供部２０８－２と、を備えている。

【００８０】

第２の実施形態では、情報提供部２０８－２を追加したこと、通信部２０１－２の機能、および、問合せ部２０５および選択部２０６を削除したことが第１の実施形態と異なっている。その他の構成および機能は、第１の実施形態にかかるアプリケーション２００のブロック図である図３と同様であるので、同一符号を付し、ここでの説明は省略する。

【００８１】

情報提供部２０８－２は、暗号処理部２０２などから取得されるアプリケーション情報を、送信部６０１を介してノード１００－２に提供する。例えば、情報提供部２０８－２は、実行部２０３から要求情報を取得し、暗号処理部２０２から暗号機能情報を取得し、

プラットフォーム部２０７からリソース情報を取得する。そして、情報提供部２０８－２は、取得したアプリケーション情報を、送信部６０１を介してノード１００－２に通知する。

【００８２】

通信部２０１－２は、第１の実施形態の通信部２０１の機能に加え、送信部６０１を備えている。送信部６０１は、情報提供部２０８－２から提供される暗号機能情報などをノード１００－２に送信する。

【００８３】

なお、暗号処理部２０２は第１の実施形態と同様であるが、いずれの暗号機能を実行するかは、例えば選択結果を受信した通信部２０１－２によって設定される。すなわち、例えば、ノード１００－２が選択した暗号機能を示す暗号設定情報をアプリケーション２００－２に送信する。そして、アプリケーション２００－２内の構成部（例えば通信部２０１－２）が、受信した暗号設定情報に対応する暗号機能を実行するように暗号処理部２０２を設定する。なお、通信部２０１－２を介して、ノード１００－２の選択部１０６－２が、選択した暗号機能を実行するように暗号処理部２０２を設定するように構成してもよい。

【００８４】

次に、第２の実施形態を実現するシーケンスについて説明する。図７は、第２の実施形態の通信システムによる通信処理の一例を示すシーケンス図である。図７は、アプリケーション２００－２が暗号通信を開始する際に、ノード１００－２に対して、アプリケーション情報を提供し、ノード１００－２において、アプリケーション鍵の生成状況についても加味した上でアプリケーション２００－２にとって最適な暗号機能を選択し、これをアプリケーション２００－２に回答する場合のシーケンスである。

【００８５】

アプリケーション２００－２の実行部２０３は、アプリケーション実行開始の前に、自身が保持する要求情報を、情報提供部２０８－２に通知する。情報提供部２０８－２は、さらに、暗号処理部２０２に対して、提供可能な暗号機能に関して問い合わせを行ってもよい。この問い合わせを受けて、暗号処理部２０２は、暗号機能情報を情報提供部２０８－２に提供する。

【００８６】

情報提供部２０８－２は、さらに、プラットフォーム部２０７に対して、アプリケーションにおけるリソース使用状況に関して問い合わせを行ってもよい。この問い合わせを受けて、プラットフォーム部２０７は、リソース情報を情報提供部２０８－２に提供する。

【００８７】

情報提供部２０８－２は、以上により、実行部２０３から要求情報を収集し、暗号処理部２０２から暗号機能情報を収集し、プラットフォーム部２０７からリソース情報を収集することができる。ただし、これは一例であり、以上のうちのいくつかの情報のみを利用してもよいし、これ以外の情報を取得してもよい。

【００８８】

情報提供部２０８－２は、収集したアプリケーション情報（要求情報、暗号機能情報、および、リソース情報）を、通信部２０１－２を介して、ノード１００－２に対して通知する（ステップＳ２０１）。

【００８９】

ノード１００－２の第２通信部１０４－２は、アプリケーション情報を受信する。アプリケーション情報を受信すると、第２通信部１０４－２は、アプリケーション情報を、選択部１０６－２に通知する。

【００９０】

選択部１０６－２は、鍵管理部１０３に対し、保持しているアプリケーション鍵情報を問い合わせる。なお、選択部１０６－２による鍵管理部１０３への問い合わせのタイミング、および、第２通信部１０４－２を介したアプリケーション２００－２からのアプリケ

ーション情報の取得のタイミングは特に限定しない。すなわち、いずれが先に行われても構わないし、並行して実行されても構わない。

【００９１】

選択部１０６－２は、以上により、第２通信部１０４－２から要求情報、暗号機能情報、および、リソース情報を取得し、鍵管理部１０３からアプリケーション鍵情報を取得することができる。ただし、これは一例であり、以上のうちのいくつかの情報のみを利用してもよいし、これ以外の情報を取得してもよい。

【００９２】

選択部１０６－２は、以上の情報を元に、アプリケーション要求に照らして最適な暗号機能を選択する（ステップＳ２０２）。選択方法は第１の実施形態と同様に様々な方法を適用できる。また、アプリケーション要求を満たす暗号機能が１つも見つからなかった場合の動作も第１の実施形態と同様に様々な方法を適用できる。

【００９３】

選択部１０６－２は、最適と判断した（選択した）暗号機能（選択結果）を、第２通信部１０４－２を介して、アプリケーション２００－２に通知する（ステップＳ２０３）。

【００９４】

アプリケーション２００－２の通信部２０１－２は暗号機能の選択結果を受け取る。通信部２０１－２は、選択結果をもとにして、最適と判断された暗号機能を利用するように、暗号処理部２０２を設定する（ステップＳ２０４）。また、通信部２０１－２は、情報提供部２０８－２または実行部２０３に対し、暗号機能の選択が完了したこと、および、選択された暗号機能、を通知してもよい。

【００９５】

実行部２０３は、アプリケーション２００－２の実行を開始する（ステップＳ２０５）。アプリケーション２００－２は、データ通信の際、通信部２０４を利用する。このとき、選択部１０６－２によって最適に設定された暗号処理部２０２によって、通信データの暗号化処理および復号処理が行われる。

【００９６】

このように、第２の実施形態にかかる通信システムでは、ノードが、アプリケーション鍵情報と、アプリケーションから得られるアプリケーション情報とを用いて最適な暗号機能を選択することができる。

【００９７】

なお、第２の実施形態についても、第１の実施形態の変形例のように、暗号通信の最中に暗号機能を動的に変更する機能（変形機能１）、および、最適な暗号通信方式の組み合わせ（複数の暗号機能）を選択する機能（変形機能２）の少なくとも一方をさらに備えるように構成してもよい。

【００９８】

以上説明したとおり、第１および第２の実施形態によれば、アプリケーションの要求に照らして、スループットとコストなども考慮した上で最適な暗号通信方式を選択することができる。

【００９９】

次に、第１および第２の実施形態にかかる装置（通信装置、鍵生成装置）のハードウェア構成について図８を用いて説明する。図８は、第１および第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。

【０１００】

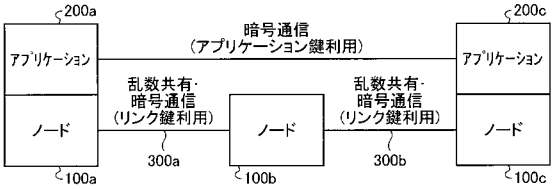
第１および第２の実施形態にかかる装置は、ＣＰＵ（Central Processing Unit）５１などの制御装置と、ＲＯＭ（Read Only Memory）５２やＲＡＭ（Random Access Memory）５３などの記憶装置と、ネットワークに接続して通信を行う通信Ｉ／Ｆ５４と、各部を接続するバス６１を備えている。

【０１０１】

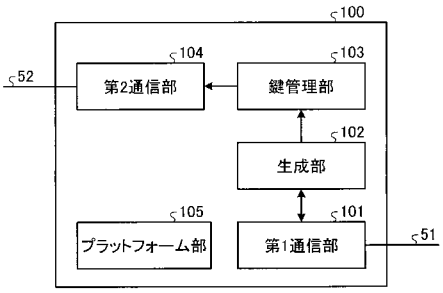
第１および第２の実施形態にかかる装置で実行されるプログラムは、ＲＯＭ５２等に予

め組み込まれて提供される。
【０１０２】
第１および第２の実施形態にかかる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ＣＤ－ＲＯＭ（Compact Disk Read Only Memory）、フレキシブルディスク（ＦＤ）、ＣＤ－Ｒ（Compact Disk Recordable）、ＤＶＤ（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し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ように構成してもよい。
【０１０３】
さらに、第１および第２の実施形態にかかる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および第２の実施形態にかかる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。
【０１０４】
第１および第２の実施形態にかかる装置で実行されるプログラムは、コンピュータを上述した装置の各部として機能させうる。このコンピュータは、ＣＰＵ５１がコンピュータ読取可能な記憶媒体からプログラムを主記憶装置上に読み出して実行することができる。
【０１０５】
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。
【符号の説明】
【０１０６】
１００　ノード
１０１　第１通信部
１０２　生成部
１０３　鍵管理部
１０４　第２通信部
１０５　プラットフォーム部
２００　アプリケーション
２０１　通信部
２０２　暗号処理部
２０３　実行部
２０４　通信部
２０５　問合せ部
２０６　選択部
２０７　プラットフォーム部
２０８　情報提供部

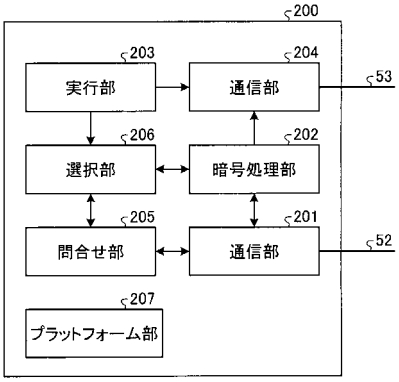
【図１】



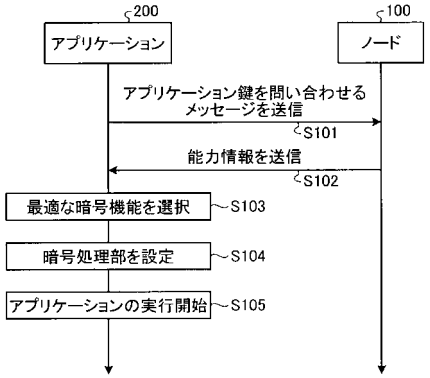
【図２】



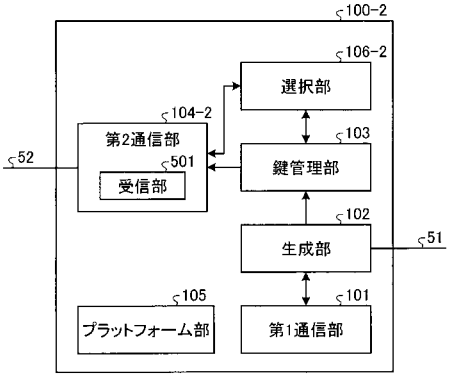
【図３】



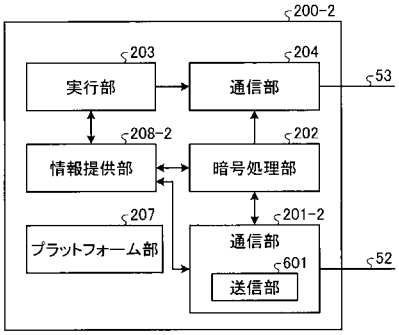
【図４】



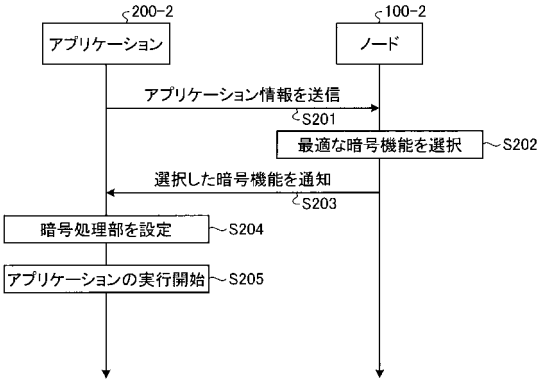
【図５】



【図６】



【図７】



【図８】