(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2005-117232
(P2005-117232A)
(43)公開日　平成17年4月28日(2005.4.28)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/14	H04L	9/00	641	5B011
G06F	1/28	G06F	1/00	333C	5J104
H04L	9/10	H04L	9/00	621Z	

審査請求 未請求　請求項の数 32　OL　（全 32 頁）

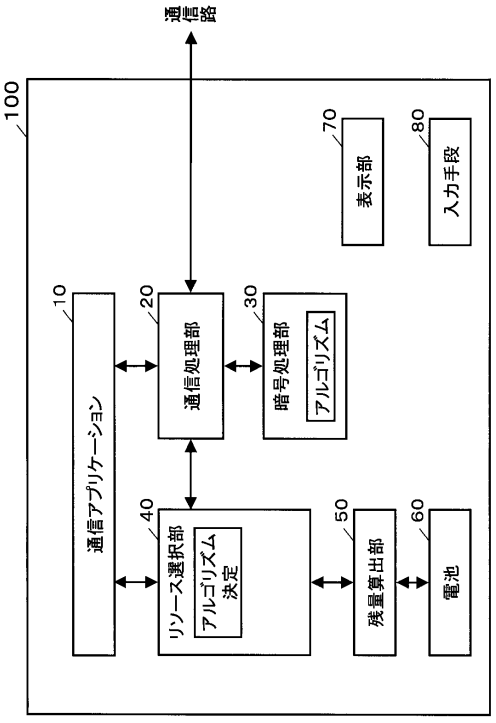
(21)出願番号　特願2003-346812(P2003-346812)
(22)出願日　平成15年10月6日(2003.10.6)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100097445
弁理士　岩橋　文雄
(74)代理人　100103355
弁理士　坂口　智康
(74)代理人　100109667
弁理士　内藤　浩樹
(72)発明者　横田　博史
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

Ｆターム(参考)　5B011 DA06　GG14
5J104 DA04　DA05　NA43

(54)【発明の名称】データ通信装置、データ通信方法、データ変換装置および変換選択方法

(57)【要約】
【課題】セキュリティを確保するために用いられる暗号通信は、ＣＰＵ処理ではＣＰＵ時間を多く要し、専用論理回路では回路中のブロックを多く稼動させる必要があるため、電力を多く要する。電源を電池に頼るポータブル機器において暗号通信を行う場合は、ＡＣ電源による通信の場合よりも、電池残容量に注意を払わないと、電池消耗により通信断となる可能性が高い。
【解決手段】リソース選択部は、残量算出部が計測した電池残容量と、通信アプリケーションが通知してくる通信予定時間や必要暗号強度等を基に、通信で利用する暗号アルゴリズムを選択する。そして通信相手機器との間で、前記暗号アルゴリズムを利用するように調整して、暗号通信を行う。
【選択図】図１



【特許請求の範囲】
【請求項１】
通信処理部、変換処理部、リソース選択部、残量算出部、電池を備え、通信データを変換処理部において所定の変換アルゴリズムにより変換処理して通信処理部により送信するデータ通信装置、または、通信処理部により受信した変換済データを変換処理部において所定の変換アルゴリズムにより元のデータに変換処理し受信するデータ通信装置であって、
残量算出部は電池の残容量を算出し、
リソース選択部は、処理負荷情報に基づき通信終了時の残容量に余裕がある変換アルゴリズムを候補変換アルゴリズムとして選択し、
前記候補変換アルゴリズムから前記所定の変換アルゴリズムを選ぶことを特徴とするデータ通信装置。
【請求項２】
通信処理部、変換処理部、リソース選択部、残量算出部、電池、モジュール管理部を備え、通信データを変換処理部において所定の変換アルゴリズムにより変換処理して通信処理部により送信するデータ通信装置、または、通信処理部により受信した変換済データを変換処理部において所定の変換アルゴリズムにより元のデータに変換処理するデータ通信装置であって、
変換処理部は、複数のモジュールのいずれかの上において変換処理を行うことができ、
残量算出部は電池の残容量を算出し、
リソース選択部は、処理負荷情報に基づき通信終了時の残容量に余裕があるモジュール・変換アルゴリズム対を候補モジュール・変換アルゴリズム対として選択し、前記候補モジュール・変換アルゴリズム対に含まれる変換アルゴリズムを候補変換アルゴリズムとして選択し、
前記候補変換アルゴリズムから前記所定の変換アルゴリズムを選び、前記所定の変換アルゴリズムに対応するモジュール・変換アルゴリズム対のモジュールを、前記モジュール管理部が形成させ、形成されたモジュール上で前記変換処理部が前記変換処理を行うことを特徴とするデータ通信装置。
【請求項３】
前記リソース選択部は、通信開始前に、処理負荷情報に基づき通信終了時の残容量に余裕がある前記候補変換アルゴリズムを選択することを特徴とする請求項１または２記載のデータ通信装置。
【請求項４】
前記リソース選択部は、通信開始後に、処理負荷情報に基づき通信終了時の残容量に余裕がある前記候補変換アルゴリズムを選択することを特徴とする請求項１または２記載のデータ通信装置。
【請求項５】
前記変換アルゴリズムは、データ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズム、暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの何れかを含み、前記変換アルゴリズムがデータ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズムの場合には、前記変換アルゴリズムは同一アルゴリズムで圧縮率の異なる複数のアルゴリズムを含み、前記変換アルゴリズムが暗号認証アルゴリズムの場合には、前記変換アルゴリズムはハッシュ処理を含まない暗号アルゴリズムのみ使用するの場合、認証アルゴリズムのみ使用する場合、暗号、認証、両アルゴリズムを使用する場合ハッシュ処理が付属した暗号アルゴリズムを含む場合を含みのいずれかとし、、前記変換アルゴリズムが暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの場合には、前記所定の変換アルゴリズムは通信相手機器とのネゴシエーションにより決定され、前記変換アルゴリズムが暗号アルゴリズムの場合には、暗号強度や耐改ざん性が高い暗号アルゴリズムが前記所定の変換アルゴリズムとして選択されることを特徴とする請求項１または２記載のデータ通信装置。
【請求項６】

前記モジュール管理部は、前記モジュールをＣＰＵ、専用ＬＳＩの何れかの上に形成させることを特徴とする請求項２記載のデータ通信装置。
【請求項７】
電源検知部を更に備え、電源検知部が電源モードの変化を検知すると、前記変換処理部がＣＰＵ上で動作する場合に、前記リソース選択部は、処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合、変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする請求項１記載のデータ通信装置。
【請求項８】
電源検知部を更に備え、電源検知部が電源モードの変化を検知すると、前記変換処理部がＣＰＵ上のモジュールで動作する場合に、前記リソース選択部は、処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合には、モジュールまたは変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする請求項２記載のデータ通信装置。
【請求項９】
通信終了予定時刻まで、通信を続けさせるデータ通信方法であって、
　電池の現在残容量を算出する手順、
　処理負荷情報を参照して消費電力を各変換アルゴリズムについて算出する手順、
　通信終了予定時刻での最終残容量を算出する手順、
　通信終了予定時刻での残容量に余裕がある変換アルゴリズムを候補変換アルゴリズムとして選択する手順、
　通信相手機器とネゴシエーションを行い、変換アルゴリズムを決定する手順、
　を含み、前記決定した変換アルゴリズムを使用してデータ通信を行うデータ通信方法。
【請求項１０】
通信終了予定時刻まで、通信を続けさせるデータ通信方法であって、
　電池の現在残容量を算出する手順、
　処理負荷情報を参照して、ＣＰＵモジュールでのソフト処理による消費電力と、専用ＬＳＩモジュールでのハード処理による消費電力の少なくとも一方を、各変換アルゴリズムについて算出する手順、
　通信終了予定時刻での最終残容量を算出する手順、
　通信終了予定時刻での残容量に余裕があるモジュール・変換アルゴリズム対を候補モジュール・変換アルゴリズム対として選択する手順、
　通信相手機器とネゴシエーションを行い、変換アルゴリズムを決定する手順、
　前記決定した変換アルゴリズムにより使用モジュールを決定する手順、
　を含み、前記決定したモジュール、前記決定した変換アルゴリズムを使用してデータ通信を行うデータ通信方法。
【請求項１１】
請求項９、１０項の何れか記載の手順を、通信開始前に実行することを特徴とするデータ通信方法。
【請求項１２】
請求項９、１０項の何れか記載の手順を、通信開始後に実行することを特徴とするデータ通信方法。
【請求項１３】
前記変換アルゴリズムは、データ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズム、暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの何れかを含み、前記変換アルゴリズムがデータ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズムの場合には、前記変換アルゴリズムは同一アルゴリズムで圧縮率の異なる複数のアルゴリズム

を含み、前記変換アルゴリズムが暗号認証アルゴリズムの場合には、前記変換アルゴリズムはハッシュ処理を含まない暗号アルゴリズムのみの使用する場合、認証アルゴリズムのみ使用する場合、暗号、認証、両アルゴリズムを使用する場合を含み、ハッシュ処理が付属した暗号アルゴリズムを含む場合のいずれかとし、前記変換アルゴリズムが暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの場合には、前記所定の変換アルゴリズムは通信相手機器とのネゴシエーションにより決定され、前記変換アルゴリズムが暗号アルゴリズムの場合には、暗号強度や耐改ざん性が高い暗号アルゴリズムが前記所定の変換アルゴリズムとして選択されることを特徴とする請求項９または１０いずれか記載のデータ通信方法。

【請求項１４】

電源検知部が電源モードの変化を検知した場合、前記変換アルゴリズムがＣＰＵ上で実行されていれば、前記処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合、変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする請求項９記載のデータ通信方法。

【請求項１５】

電源モードの変化を検知した場合、前記変換アルゴリズムがＣＰＵ上で実行されていれば、前記処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合には、モジュールまたは変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする請求項１０記載のデータ通信方法。

【請求項１６】

変換処理部、リソース選択部、残量算出部、電池を備え、データを変換処理部において所定の変換アルゴリズムにより変換処理するデータ変換装置であって、

残量算出部は電池の残容量を算出し、

リソース選択部は、処理負荷情報に基づき変換終了時の残容量に余裕がある変換アルゴリズムを候補変換アルゴリズムとして選択し、

前記候補変換アルゴリズムから前記所定の変換アルゴリズムを選ぶことを特徴とするデータ変換装置。

【請求項１７】

変換処理部、リソース選択部、残量算出部、電池、モジュール管理部を備え、データを変換処理部において所定の変換アルゴリズムにより変換処理するデータ変換装置であって、

変換処理部は、複数のモジュールのいずれかの上において変換処理を行うことができ、

残量算出部は電池の残容量を算出し、

リソース選択部は、処理負荷情報に基づき変換終了時の残容量に余裕があるモジュール・変換アルゴリズム対を候補モジュール・変換アルゴリズム対として選択し、前記候補モジュール・変換アルゴリズム対に含まれる変換アルゴリズムを候補変換アルゴリズムとして選択し、

前記候補変換アルゴリズムから前記所定の変換アルゴリズムを選び、前記所定の変換アルゴリズムに対応するモジュール・変換アルゴリズム対のモジュールを、前記モジュール管理部が形成させ、形成されたモジュール上で前記変換処理部が前記変換処理を行うことを特徴とするデータ変換装置。

【請求項１８】

前記リソース選択部は、変換開始前に、処理負荷情報に基づき変換終了時の残容量に余裕がある前記候補変換アルゴリズムを選択することを特徴とする請求項１６または１７記載のデータ変換装置。

【請求項１９】

前記リソース選択部は、変換開始後に、処理負荷情報に基づき変換終了時の残容量に余裕

がある前記候補変換アルゴリズムを選択することを特徴とする請求項１６または１７記載のデータ変換装置。
【請求項２０】
前記変換アルゴリズムは、データ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズム、暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの何れかを含み、前記変換アルゴリズムがデータ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズムの場合には、前記変換アルゴリズムは同一アルゴリズムで圧縮率の異なる複数のアルゴリズムを含み、前記変換アルゴリズムが暗号認証アルゴリズムの場合には、前記変換アルゴリズムはハッシュ処理を含まない暗号アルゴリズムのみ使用するの場合、認証アルゴリズムのみ使用する場合、暗号、認証、両アルゴリズムを使用する場合を含み、ハッシュ処理が付属した暗号アルゴリズムを含む場合のいずれかとし、前記変換アルゴリズムが暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの場合には、前記所定の変換アルゴリズムは通信相手機器とのネゴシエーションにより決定され、前記変換アルゴリズムが暗号アルゴリズムの場合には、暗号強度や耐改ざん性が高い暗号アルゴリズムが前記所定の変換アルゴリズムとして選択されることを特徴とする請求項１６または１７記載のデータ変換装置。
【請求項２１】
前記モジュール管理部は、前記モジュールをＣＰＵ、専用ＬＳＩの何れかの上に形成させることを特徴とする請求項１７記載のデータ変換装置。
【請求項２２】
電源検知部を更に備え、電源検知部が電源モードの変化を検知すると、前記変換処理部がＣＰＵ上で動作する場合に、前記リソース選択部は、処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合、変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする請求項１６記載のデータ変換装置。
【請求項２３】
電源検知部を更に備え、電源検知部が電源モードの変化を検知すると、前記変換処理部がＣＰＵ上のモジュールで動作する場合に、前記リソース選択部は、処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合には、モジュールまたは変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする請求項１７記載のデータ変換装置。
【請求項２４】
変換終了予定時刻まで、変換を続けさせる変換選択方法であって、
　電池の現在残容量を算出する手順、
　処理負荷情報を参照して消費電力を各変換アルゴリズムについて算出する手順、
　変換終了予定時刻での最終残容量を算出する手順、
　変換終了予定時刻での残容量に余裕がある変換アルゴリズムを候補変換アルゴリズムとして選択する手順、
　変換アルゴリズムを決定する手順、
　を含み、前記決定した変換アルゴリズムを使用してデータ変換を行う変換選択方法。
【請求項２５】
変換終了予定時刻まで、変換を続けさせる変換選択方法であって、
　電池の現在残容量を算出する手順、
　処理負荷情報を参照して、ＣＰＵモジュールでのソフト処理による消費電力と、専用ＬＳＩモジュールでのハード処理による消費電力の少なくとも一方を、各変換アルゴリズムについて算出する手順、
　変換終了予定時刻での最終残容量を算出する手順、

変換終了予定時刻での残容量に余裕があるモジュール・変換アルゴリズム対を候補モジュール・変換アルゴリズム対として選択する手順、
変換アルゴリズムを決定する手順、
前記決定した変換アルゴリズムより使用モジュールを決定する手順、
を含み、前記決定したモジュール、前記決定した変換アルゴリズムを使用してデータ変換を行う変換選択方法。
【請求項２６】
請求項２４、２５項の何れか記載の手順を、変換開始前に実行することを特徴とする変換選択方法。
【請求項２７】
請求項２４、２５項の何れか記載の手順を、変換開始後に実行することを特徴とする変換選択方法。
【請求項２８】
前記変換アルゴリズムは、データ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズム、暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの何れかを含み、前記変換アルゴリズムがデータ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズムの場合には、前記変換アルゴリズムは同一アルゴリズムで圧縮率の異なる複数のアルゴリズムを含み、前記変換アルゴリズムが暗号アルゴリズムの場合には、前記変換アルゴリズムはハッシュ処理を含まない暗号アルゴリズムのみ使用するの場合、認証アルゴリズムのみ使用する場合、暗号、認証、両アルゴリズムを使用する場合を含み、ハッシュ処理が付属した暗号アルゴリズムを含む場合のいずれかとし、前記変換アルゴリズムが暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの場合には、前記所定の変換アルゴリズムは通信相手機器とのネゴシエーションにより決定され、前記変換アルゴリズムが暗号アルゴリズムの場合には、暗号強度や耐改ざん性が高い暗号アルゴリズムが前記所定の変換アルゴリズムとして選択されることを特徴とする請求項２４または２５いずれか記載の変換選択方法。
【請求項２９】
電源検知部が電源モードの変化を検知した場合、前記変換アルゴリズムがＣＰＵ上で実行されていれば、前記処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合、変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする請求項２４記載の変換選択方法。
【請求項３０】
電源モードの変化を検知した場合、前記変換アルゴリズムがＣＰＵ上で実行されていれば、前記処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合には、モジュールまたは変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする請求項２５記載の変換選択方法。
【請求項３１】
請求項９～１５、２４～３０何れか記載の方法をコンピュータで実行するプログラム。
【請求項３２】
請求項９～１５、２４～３０何れか記載の方法をコンピュータで実行するプログラムを記録した記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータデータや映像、音声、テキストなどのデータを送受信する場合にデータ変換方法やデータ変換手段を選択できるデータ通信装置、データ通信方法、およ

び、データ変換方法やデータ変換手段を選択するデータ変換装置および変換選択方法に関するものである。

【背景技術】

【０００２】

近年、インターネットが身近で利用されるようになってきている。今までは、主にパーソナルコンピュータ（ＰＣ）やルータ装置などがインターネットにつながっており、そのユーザはコンピュータネットワークに関する知識を有する技術者や彼らのサポートを受けることができるオフィスワーカが主にオフィスワークのために利用していた。しかし今後は、ポータブル端末や家電製品などが、現在以上にインターネットにつながり、一般の人でも様々なサービスを受けられるようになってくる。すなわち、今後は、今までと違って、（１）据え置きではなく電池を電源とするポータブル端末が増え、（２）さまざまなサービスが提供され、プライバシー情報のように保護が必要なデータが送信されることが多くなる。すなわち、暗号化してデータを送受しなければならないケースが増える。

【０００３】

ポータブル端末は、一般的にＰＣに比べて、そのＣＰＵ能力やメモリ量など通信処理に使えるリソース量が少ない。そのため、機能や性能を限定せざるを得ない場合がある。またポータブル端末は、電池を利用するため、その利用に際しては消費電力や電池寿命に注意を払わなければならない。そこで、これらに対応するため、従来のポータブル型のデータ通信装置においては、端末リソースや消費電力を考慮してデータ通信を行っていた。

【０００４】

例えば、特許文献１では、暗号通信ができるかどうかなど通信相手の能力を基に、暗号通信をするかどうか判定している。

【０００５】

また、特許文献２においては、最初から最大負荷に対応できる復号ＬＳＩを持つとコスト高になるのを避けるため、受信処理能力を受信データ速度に適合できるようする。具体的には、受信データ速度や消費電力要件に適するように、暗号復号ＬＳＩの処理クロックを変更している。

【特許文献１】特開平１１－２８８４０３号公報

【特許文献２】特開２００２－３１２０５６号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

しかしながら、以上の従来例では、ポータブル機器における電源管理が考慮されていない。すなわち、特許文献１では、相手の通信能力は考慮するが電源事情は考慮されていない。また、特許文献２では、時々刻々と減っていく電池容量に関して考慮されていない。

【０００７】

本発明の目的は、上記のように電池の電源容量を考慮しながら暗号通信を行い、ポータブル機器の通信セキュリティと通信継続時間を確保することである。

【課題を解決するための手段】

【０００８】

上記従来の課題を解決するために、本発明のデータ通信装置、データ通信方法、データ変換装置および変換選択方法は、以下のような構成および手順を有する。

【０００９】

（１）　通信処理部、変換処理部、リソース選択部、残量算出部、電池を備え、通信データを変換処理部において所定の変換アルゴリズムにより変換処理して通信処理部により送信するデータ通信装置、または、通信処理部により受信した変換済データを変換処理部において所定の変換アルゴリズムにより元のデータに変換処理し受信するデータ通信装置であって、残量算出部は電池の残容量を算出し、リソース選択部は、処理負荷情報に基づき通信終了時の残容量に余裕がある変換アルゴリズムを候補変換アルゴリズムとして選択し、前記候補変換アルゴリズムから前記所定の変換アルゴリズムを選ぶことを特徴とする

データ通信装置。
【００１０】
本構成によって、通信予定時間の間、電池消耗による通信断が起きない。
【００１１】
（２） 通信処理部、変換処理部、リソース選択部、残量算出部、電池、モジュール管理部を備え、通信データを変換処理部において所定の変換アルゴリズムにより変換処理して通信処理部により送信するデータ通信装置、または、通信処理部により受信した変換済データを変換処理部において所定の変換アルゴリズムにより元のデータに変換処理するデータ通信装置であって、変換処理部は、複数のモジュールのいずれかの上において変換処理を行うことができ、残量算出部は電池の残容量を算出し、リソース選択部は、処理負荷情報に基づき通信終了時の残容量に余裕があるモジュール・変換アルゴリズム対を候補モジュール・変換アルゴリズム対として選択し、前記候補モジュール・変換アルゴリズム対に含まれる変換アルゴリズムを候補変換アルゴリズムとして選択し、前記候補変換アルゴリズムから前記所定の変換アルゴリズムを選び、前記所定の変換アルゴリズムに対応するモジュール・変換アルゴリズム対のモジュールを、前記モジュール管理部が形成させ、形成されたモジュール上で前記変換処理部が前記変換処理を行うことを特徴とするデータ通信装置。
【００１２】
本構成によって、複数のモジュールが使用できる場合にも、通信予定時間の間、電池消耗による通信断が起きない。
【００１３】
（３） 前記リソース選択部は、通信開始前に、処理負荷情報に基づき通信終了時の残容量に余裕がある前記候補変換アルゴリズムを選択することを特徴とする（１）、（２）いずれか記載のデータ通信装置。
【００１４】
（４） 前記リソース選択部は、通信開始後に、処理負荷情報に基づき通信終了時の残容量に余裕がある前記候補変換アルゴリズムを選択することを特徴とする（１）、（２）いずれか記載のデータ通信装置。
【００１５】
本構成により、通信途中で電池消耗が予定以上に進んでも、通信予定時間の間、電池消耗による通信断が起きない。
【００１６】
（５） 前記変換アルゴリズムは、データ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズム、暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの何れかを含み、前記変換アルゴリズムがデータ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズムの場合には、前記変換アルゴリズムは同一アルゴリズムで圧縮率の異なる複数のアルゴリズムを含み、前記変換アルゴリズムが暗号認証アルゴリズムの場合には、前記変換アルゴリズムはハッシュ処理を含まない暗号アルゴリズムのみのを使用する場合、認証アルゴリズムのみ使用する場合、暗号、認証、両アルゴリズムを使用する場合を含み、ハッシュ処理が付属した暗号アルゴリズムを含む場合のいずれかとし、前記変換アルゴリズムが暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの場合には、前記所定の変換アルゴリズムは通信相手機器とのネゴシエーションにより決定され、前記変換アルゴリズムが暗号アルゴリズムの場合には、暗号強度や耐改ざんが高い暗号アルゴリズムが前記所定の変換アルゴリズムとして選択されることを特徴とする（１）、（２）いずれか記載のデータ通信装置。
【００１７】
（６） 前記モジュール管理部は、前記モジュールをＣＰＵ、専用ＬＳＩの何れかの上に形成させることを特徴とする（２）記載のデータ通信装置。
【００１８】
（７） 電源検知部を更に備え、電源検知部が電源モードの変化を検知すると、前記変

換処理部がＣＰＵ上で動作する場合に、前記リソース選択部は、処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合、変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする（１）記載のデータ通信装置。

【００１９】

本構成により、通信途中で電源モードが変更になっても、通信断が起きない。

【００２０】

（８）　電源検知部を更に備え、電源検知部が電源モードの変化を検知すると、前記変換処理部がＣＰＵ上のモジュールで動作する場合に、前記リソース選択部は、処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合には、モジュールまたは変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする（２）記載のデータ通信装置。

【００２１】

本構成により、通信途中で電源モードが変更になっても、通信断が起きない。

【００２２】

（９）　通信終了予定時刻まで、通信を続けさせるデータ通信方法であって、電池の現在残容量を算出する手順、処理負荷情報を参照して消費電力を各変換アルゴリズムについて算出する手順、通信終了予定時刻での最終残容量を算出する手順、通信終了予定時刻での残容量に余裕がある変換アルゴリズムを候補変換アルゴリズムとして選択する手順、通信相手機器とネゴシエーションを行い、変換アルゴリズムを決定する手順、を含み、前記決定した変換アルゴリズムを使用してデータ通信を行うデータ通信方法。

【００２３】

本手順によって、通信予定時間の間、電池消耗による通信断が起きない。

【００２４】

（１０）　通信終了予定時刻まで、通信を続けさせるデータ通信方法であって、電池の現在残容量を算出する手順、処理負荷情報を参照して、ＣＰＵモジュールでのソフト処理による消費電力と、専用ＬＳＩモジュールでのハード処理による消費電力の少なくとも一方を、各変換アルゴリズムについて算出する手順、通信終了予定時刻での最終残容量を算出する手順、通信終了予定時刻での残容量に余裕があるモジュール・変換アルゴリズム対を候補モジュール・変換アルゴリズム対として選択する手順、通信相手機器とネゴシエーションを行い、変換アルゴリズムを決定する手順、前記決定した変換アルゴリズムにより使用モジュールを決定する手順、を含み、前記決定したモジュール、前記決定した変換アルゴリズムを使用してデータ通信を行うデータ通信方法。

【００２５】

本手順によって、複数のモジュールが使用できる場合にも、通信予定時間の間、電池消耗による通信断が起きない。

【００２６】

（１１）上記（９）、（１０）の何れか記載の手順を、通信開始前に実行することを特徴とするデータ通信方法。

【００２７】

（１２）上記（９）、（１０）の何れか記載の手順を、通信開始後に実行することを特徴とするデータ通信方法。

【００２８】

本手順により、通信途中で電池消耗が予定以上に進んでも、通信予定時間の間、電池消耗による通信断が起きない。

【００２９】

（１３） 前記変換アルゴリズムは、データ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズム、暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの何れかを含み、前記変換アルゴリズムがデータ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズムの場合には、前記変換アルゴリズムは同一アルゴリズムで圧縮率の異なる複数のアルゴリズムを含み、前記変換アルゴリズムが暗号認証アルゴリズムの場合には、前記変換アルゴリズムはハッシュ処理を含まない暗号アルゴリズムのみの使用する場合、認証アルゴリズムのみ使用する場合、暗号、認証、両アルゴリズムを使用する場合を含み、ハッシュ処理が付属した暗号アルゴリズムを含む場合のいずれかとし、前記変換アルゴリズムが暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの場合には、前記所定の変換アルゴリズムは通信相手機器とのネゴシエーションにより決定され、前記変換アルゴリズムが暗号アルゴリズムの場合には、暗号強度や耐改ざん性が高い暗号アルゴリズムが前記所定の変換アルゴリズムとして選択されることを特徴とする（９）、（１０）いずれか記載のデータ通信方法。

【００３０】

（１４） 電源検知部が電源モードの変化を検知した場合、前記変換アルゴリズムがＣＰＵ上で実行されていれば、前記処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合、変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする（９）記載のデータ通信方法。

【００３１】

本手順により、通信途中で電源モードが変更になっても、通信断が起きない。

【００３２】

（１５） 電源モードの変化を検知した場合、前記変換アルゴリズムがＣＰＵ上で実行されていれば、前記処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合には、モジュールまたは変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする（１０）記載のデータ通信方法。

【００３３】

本手順により、通信途中で電源モードが変更になっても、通信断が起きない。

【００３４】

（１６） 変換処理部、リソース選択部、残量算出部、電池を備え、データを変換処理部において所定の変換アルゴリズムにより変換処理するデータ変換装置であって、残量算出部は電池の残容量を算出し、リソース選択部は、処理負荷情報に基づき変換終了時の残容量に余裕がある変換アルゴリズムを候補変換アルゴリズムとして選択し、前記候補変換アルゴリズムから前記所定の変換アルゴリズムを選ぶことを特徴とするデータ変換装置。

【００３５】

本構成により、変換予定時間の間、電池消耗による、変換中断が起きない。

【００３６】

（１７） 変換処理部、リソース選択部、残量算出部、電池、モジュール管理部を備え、データを変換処理部において所定の変換アルゴリズムにより変換処理するデータ変換装置であって、変換処理部は、複数のモジュールのいずれかの上において変換処理を行うことができ、残量算出部は電池の残容量を算出し、リソース選択部は、処理負荷情報に基づき変換終了時の残容量に余裕があるモジュール・変換アルゴリズム対を候補モジュール・変換アルゴリズム対として選択し、前記候補モジュール・変換アルゴリズム対に含まれる変換アルゴリズムを候補変換アルゴリズムとして選択し、前記候補変換アルゴリズムから前記所定の変換アルゴリズムを選び、前記所定の変換アルゴリズムに対応するモジュール・変換アルゴリズム対のモジュールを、前記モジュール管理部が形成させ、形成されたモジュール上で前記変換処理部が前記変換処理を行うことを特徴とするデータ変換装置。

【００３７】
本構成により、変換予定時間の間、電池消耗による、変換中断が起きない。
【００３８】
（１８）前記リソース選択部は、変換開始前に、処理負荷情報に基づき変換終了時の残容量に余裕がある前記候補変換アルゴリズムを選択することを特徴とする（１６）、（１７）いずれか記載のデータ変換装置。
【００３９】
（１９）前記リソース選択部は、変換開始後に、処理負荷情報に基づき変換終了時の残容量に余裕がある前記候補変換アルゴリズムを選択することを特徴とする（１６）、（１７）いずれか記載のデータ変換装置。
【００４０】
本構成により、変換処理の途中で電池消耗が予定以上に進んでも、変換予定時間の間、電池消耗による、変換中断が起きない。
【００４１】
（２０）前記変換アルゴリズムは、データ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズム、暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの何れかを含み、前記変換アルゴリズムがデータ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズムの場合には、前記変換アルゴリズムは同一アルゴリズムで圧縮率の異なる複数のアルゴリズムを含み、前記変換アルゴリズムが暗号認証アルゴリズムの場合には、前記変換アルゴリズムはハッシュ処理を含まない暗号アルゴリズムのみの使用する場合、認証アルゴリズムのみ使用する場合、暗号、認証、両アルゴリズムを使用する場合を含み、ハッシュ処理が付属した暗号アルゴリズムを含む場合のいずれかとし、前記変換アルゴリズムが暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの場合には、前記所定の変換アルゴリズムは通信相手機器とのネゴシエーションにより決定され、前記変換アルゴリズムが暗号アルゴリズムの場合には、暗号強度や耐改ざん性が高い暗号アルゴリズムが前記所定の変換アルゴリズムとして選択されることを特徴とする（１６）、（１７）いずれか記載のデータ変換装置。
【００４２】
（２１）前記モジュール管理部は、前記モジュールをＣＰＵ、専用ＬＳＩの何れかの上に形成させることを特徴とする（１７）記載のデータ変換装置。
【００４３】
（２２）電源検知部を更に備え、電源検知部が電源モードの変化を検知すると、前記変換処理部がＣＰＵ上で動作する場合に、前記リソース選択部は、処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合、変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする（１６）記載のデータ変換装置。
【００４４】
本構成により、変換予定時間の途中で電源モードが変更になっても、変換中断が起きない。
【００４５】
（２３）電源検知部を更に備え、電源検知部が電源モードの変化を検知すると、前記変換処理部がＣＰＵ上のモジュールで動作する場合に、前記リソース選択部は、処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合には、モジュールまたは変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする（１７）記載のデータ変換装置。
【００４６】

本構成により、変換予定時間の途中で電源モードが変更になっても、変換中断が起きない。

【００４７】

（２４） 変換終了予定時刻まで、変換を続けさせる変換選択方法であって、電池の現在残容量を算出する手順、処理負荷情報を参照して消費電力を各変換アルゴリズムについて算出する手順、変換終了予定時刻での最終残容量を算出する手順、変換終了予定時刻での残容量に余裕がある変換アルゴリズムを候補変換アルゴリズムとして選択する手順、変換アルゴリズムを決定する手順、を含み、前記決定した変換アルゴリズムを使用してデータ変換を行う変換選択方法。

【００４８】

本手順により、変換予定時間の間、電池消耗による変換中断が起きない。

【００４９】

（２５） 変換終了予定時刻まで、変換を続けさせる変換選択方法であって、電池の現在残容量を算出する手順、処理負荷情報を参照して、ＣＰＵモジュールでのソフト処理による消費電力と、専用ＬＳＩモジュールでのハード処理による消費電力の少なくとも一方を、各変換アルゴリズムについて算出する手順、変換終了予定時刻での最終残容量を算出する手順、変換終了予定時刻での残容量に余裕があるモジュール・変換アルゴリズム対を候補モジュール・変換アルゴリズム対として選択する手順、変換アルゴリズムを決定する手順、前記決定した変換アルゴリズムより使用モジュールを決定する手順、を含み、前記決定したモジュール、前記決定した変換アルゴリズムを使用してデータ変換を行う変換選択方法。

【００５０】

本手順により、変換予定時間の間、電池消耗による変換中断が起きない。

【００５１】

（２６）上記（２４）、（２５）の何れか記載の手順を、変換開始前に実行することを特徴とする変換選択方法。

【００５２】

（２７）上記（２４）、（２５）の何れか記載の手順を、変換開始後に実行することを特徴とする変換選択方法。

【００５３】

本手順により、電池消耗が予定以上に進んでも、変換予定時間の間、変換中断が起きない。

【００５４】

（２８） 前記変換アルゴリズムは、データ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズム、暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの何れかを含み、前記変換アルゴリズムがデータ圧縮アルゴリズム、映像もしくは音声符号化アルゴリズムの場合には、前記変換アルゴリズムは同一アルゴリズムで圧縮率の異なる複数のアルゴリズムを含み、前記変換アルゴリズムが暗号認証アルゴリズムの場合には、前記変換アルゴリズムはハッシュ処理を含まない暗号アルゴリズムのみの使用する場合、認証アルゴリズムのみ使用する場合、暗号、認証、両アルゴリズムを使用する場合を含み、ハッシュ処理が付属した暗号アルゴリズムを含む場合のいずれかとし、前記変換アルゴリズムが暗号アルゴリズム、認証アルゴリズム、暗号認証アルゴリズムの場合には、前記所定の変換アルゴリズムは通信相手機器とのネゴシエーションにより決定され、前記変換アルゴリズムが暗号アルゴリズムの場合には、暗号強度や耐改ざん性が高い暗号アルゴリズムが前記所定の変換アルゴリズムとして選択されることを特徴とする（２４）、（２５）項いずれか記載の変換選択方法。

【００５５】

（２９） 電源検知部が電源モードの変化を検知した場合、前記変換アルゴリズムがＣＰＵ上で実行されていれば、前記処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判

定し、越える場合、変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする（２４）記載の変換選択方法。

【００５６】

本手順により、変換予定時間の途中で、電源モードが変わっても、変換中断が起きない。

【００５７】

（３０） 電源モードの変化を検知した場合、前記変換アルゴリズムがＣＰＵ上で実行されていれば、前記処理負荷情報に基づき、変換処理に必要な処理能力が、ＣＰＵに許可された電源モード変更後の変換処理用ＣＰＵ処理能力を超えないかどうか判定し、越える場合には、モジュールまたは変換アルゴリズムを変更して、前記電源モード変更後の変換処理用ＣＰＵ処理能力を超えることがないようにした後に、電源モードによるＣＰＵの動作モードを変更することを特徴とする（２５）記載の変換選択方法。

【００５８】

本手順により、変換予定時間の途中で、電源モードが変わっても、変換中断が起きない。

【００５９】

（３１）上記（９）～（１５）、（２４）～（３０）何れか記載の方法をコンピュータで実行するプログラム。

【００６０】

（３２）上記（９）～（１５）、（２４）～（３０）何れか記載の方法をコンピュータで実行するプログラムを記録した記録媒体。

【発明の効果】

【００６１】

本発明のデータ通信方式によれば、ポータブル機器使用時においてその電池残容量に鑑みて通信処理負荷を変えることにより、電池容量を節約しながら出来るだけセキュアな通信方法を提供することができる。

【発明を実施するための最良の形態】

【００６２】

以下、本発明の実施の形態を、図面を参照しながら説明する。

【００６３】

（実施の形態１）

図１は、本発明の実施の形態１におけるデータ通信装置であるポータブル機器１００の構成図である。図１において、ポータブル機器１００は、通信アプリケーション１０、通信処理部２０、暗号処理部３０、リソース選択部４０、残量算出部５０、電池６０、表示部７０、入力手段８０を備える。

【００６４】

なお、暗号処理部３０は、一般的には、後述するように、変換アルゴリズムを実行する変換処理部３０と呼ぶべきであるが、本実施の形態での説明では、暗号アルゴリズムを実行する暗号処理部３０として説明する。

【００６５】

通信アプリケーション１０はデータ通信装置におけるアプリケーションを格納しており、通信すべきデータを生成する。通信処理部２０は、通信アプリケーション１０からデータを受け取り、暗号処理部３０において所定の暗号化処理を行なわせた後、暗号化したデータを送出する。また、通信処理部２０は、暗号処理部３０において、通信路から受け取ったデータに対して暗号の復号化処理を行わせ、復号化したデータを通信アプリケーション１０に渡す。暗号処理部３０は、通信処理部２０の指示により、通信処理部２０から受け取ったデータに対して所定の暗号化あるいは復号化の変換を行い、処理後のデータを通信処理部２０に返す。暗号処理部３０は、複数の暗号アルゴリズムを内部で実行可能とする。電池６０は、本データ通信装置に電力を供給する。残量算出部５０は、電池の残容量

を計測しリソース選択部４０に知らせる。リソース選択部４０は、電池の残容量データや複数の暗号アルゴリズム処理および暗号通信処理に関連した処理負荷情報に基づき、複数の負荷条件の下での電池の継続利用可能時間を予測し、暗号処理部３０における暗号アルゴリズム、一般的には、変換方法を選択し、その選択結果を通信処理部２０に知らせる。表示部７０は、電池残量や選択すべきアルゴリズムを知らせるための表示手段である。入力手段８０は、ユーザがアルゴリズムを選択したりするための入力手段である。

【００６６】

＜暗号処理の負荷＞

最初に、暗号処理の負荷について説明する。

【００６７】

図２（ａ）は、暗号アルゴリズムとその処理時間を示す図である。図２（ａ）に示すように、同じ処理能力のＣＰＵにより処理を行う場合、暗号やハッシュアルゴリズムによってその処理時間は変わる。すなわち、３ＤＥＳによる暗号処理はＤＥＳによるものより３倍の時間を要する。これは、暗号アルゴリズムによって、必要とする処理ステップ数が異なるためである。処理時間が長いほど単位データ量当たりの消費電力が大きいことになる。よって、単位データ量当たりの消費電力は、適用するアルゴリズムによって変わることになる。なお、暗号処理に要する時間が長いと、それに伴って通信処理できる時間当たりの最大データ量も制限されることになる。図２（ａ）には、暗号強度に関係する鍵長も示す。一般的に、鍵長が長い方が処理負荷が大きくなる。

【００６８】

図２（ｂ）は暗号アルゴリズムの鍵長と処理時間の関係を示す図である。一般に同じ暗号アルゴリズムならその鍵長が長いほど暗号強度が強い。図２（ｂ）では、ＡＥＳアルゴリズムの鍵長とその処理に必要とする繰り返し処理回数（ラウンド数）との関係を示したものである。同図より分るように、鍵長が長くなれば、繰り返し処理回数（ラウンド数）が大きくなり、すなわち処理ステップ数が多くなり、より多くの電力を必要とする。

【００６９】

＜電池残量の算出＞

電池残量の計測予測には各種方法がある。図３は、電池の残容量と電圧の関係を示したものである。図３に示すように、電池は残容量が減るに伴い電圧も減る。現在の電池電圧を測定すれば、電池の残容量を予測することができる。電池からこれまでに取り出した電力累算値を計測しておき、前回充電時の電池残量からの残りを電池残量としてもよい。また、消費電流と電池電圧の変化度合いを計測しておき、その関係から電池の残容量を計算するようにしてもよい。また、充電電力を計測しておき、残容量が分るようにしておいてもよい。これらの組み合わせにより、残容量を求めるようにしても良い。

【００７０】

＜暗号アルゴリズムの決定＞

本実施の形態１では、暗号通信に先立って、残容量と通信予定時間をもとに、使用可能なアルゴリズムを選択する。

【００７１】

図４（ａ）は、ポータブル機器における消費電力、すなわち、負荷の大小と電池の残容量との基本的な関係を示した経過予測図である。図４（ａ）において、負荷１は負荷２よりも負荷が小さい。負荷１と負荷２は、図２（ａ）におけるＤＥＳと３ＤＥＳに相当するものとする。負荷１でポータブル機器を利用した場合は、時間長ｔ１で電池残容量がなくなる、すなわちポータブル機器をｔ１時間のあいだ利用することができる。同様に、負荷２の場合はポータブル機器をｔ２時間のあいだ利用することができる。このように、負荷の大小によって、電池の減り方が異なり、利用可能時間も異なる。一般的に、暗号強度が高い暗号アルゴリズムほど消費電力が大きく負荷が大きいので電池動作において利用可能時間が短くなる。

【００７２】

図４（ｂ）は、ポータブル機器を利用したい利用希望時間ＴａもしくはＴｂが分ってい

る場合の経過予測図である。まず、ポータブル機器を時間Ｔａだけ利用できればよい場合に関して説明する。Ｔａは、ｔ１やｔ２よりも小さい。すなわち、負荷１でも負荷２でも利用時間の要件は満たすことになる。負荷１であれば、時間Ｔａ経過後、電池容量ＷＨ１が残り、負荷２であれば、時間Ｔａ経過後、電池容量ＷＨ２の余裕があることになる。ＤＥＳと３ＤＥＳの両方共、必要とする暗号強度を満たしているのであれば、負荷１、負荷２のどちらを選んでもよい。なるだけ長時間利用したいのなら軽い負荷である負荷１を採用すればよい。利用希望時間にこだわらなくてよい場合は、より強い強度の暗号を使用する負荷２を採用すればよい。このように複数候補がある場合に、リソース選択部４０は、その中から１つのアルゴリズムを選択する。選択は、後述するように自動的に行ってもよいし、表示部７０と入力手段８０を利用してユーザが決めても良い。

【００７３】

次に、ポータブル機器を利用希望時間Ｔｂまで利用したい場合に関して説明する。Ｔｂはｔ２よりも大きく、ｔ１よりも小さい。すなわち、負荷２ならば時間Ｔｂまでに電池を消耗してしまうが、負荷１ならば電池容量ＷＨ３を残してＴｂまで利用することができる。

【００７４】

以上のように、電池の残容量と通信予定時間を基に、使用可能な暗号アルゴリズムを選べば、電池残容量に余裕を残して通信アプリケーションを終了できる。また、なるだけ長時間利用したり、なるだけ強い暗号を選んだりなど、ユーザの要求に応えることができ、利便性を高めることもできる。

【００７５】

図１のデータ通信装置は、上記機能を実現するために、以下のように動作する。ポータブル機器１００において、そのユーザが通信アプリケーション１０を使用して、相手の機器にデータを送信する際、まず、どのような暗号アルゴリズムを使用するかを決め、つぎに暗号用の鍵を生成するネゴシエーションを行うが、その前に、リソース候補として候補暗号アルゴリズムの選択を行う。残量算出部５０は、電池６０の残容量を計測推定し、推定した残容量データをリソース選択部４０に与える。通信アプリケーション１０は、通信予定時間の情報をリソース選択部４０に与える。通信処理部２０は、暗号処理部３０が保有する複数の暗号アルゴリズムそれぞれの処理負荷に関する情報を、リソース選択部４０に与える。リソース選択部４０は、入手した残容量データ、通信予定時間、処理負荷情報を元に、適用可能な候補暗号アルゴリズムを１つまたは複数種類選択する。この候補選択の手法については後述する。リソース選択部４０は、候補暗号アルゴリズムを通信処理部２０に知らせる。

【００７６】

通信処理部２０は、上記候補暗号アルゴリズムを候補として、通信相手機器との間で、実際にどの暗号アルゴリズムを使用するかのネゴシエーションを行い、１つを選択、決定する。ここで候補を挙げて相手と調整するのは、相手機器において復号化可能な暗号アルゴリズムを選択する必要があるからである。ネゴシエーションの仕組みや手順については周知であるので説明を省く。

【００７７】

通信処理部２０は、ネゴシエーションにより決定した暗号アルゴリズムを暗号処理部３０に知らせる。つぎに、暗号処理部３０を使用して通信相手機器との間で暗号通信に使用する鍵を生成する。この後、通信アプリケーション１０から受け取る送信用の通信データを暗号処理部３０に渡して、決定した暗号アルゴリズムにより暗号化させ、暗号化した通信データを通信路へ送出する。

【００７８】

ポータブル機器１００が、他の機器からデータを受信する場合も、ネゴシエーションの前に、通信処理部２０は、相手機器から通信予定時間を入手してリソース選択部４０に渡し、リソース選択部４０が候補暗号アルゴリズムを選択し、通信処理部２０が通信相手機器とネゴシエーションを行うことにより、候補暗号アルゴリズムから１つの暗号アルゴリ

ズムを選択決定する。

【００７９】

つぎに、候補暗号アルゴリズムの選択の方法について、その一例を説明する。以下のような各種情報を取り扱うことにより、暗号通信に必要な電力や、動作可能時間を計算することができる。

【００８０】

上記残量算出部５０が推計した電池の残容量をＰｂ（Ｗ・秒）とする。単位Ｗは、ワットである。通信アプリケーションが行う通信が継続する通信予定時間をＴｓ（秒）とする。通信アプリケーションが生成する通信データ（この場合は、送信用データ）の生成レート、すなわち、通信データ速度をＤｒ（Ｂｙｔｅ／秒）とする。音声データであれば、さほど大きな数値ではないが、高画質の動画データであれば大きな数値になる。

【００８１】

通信処理部２０がデータを通信する際に必要な電力を、通信固定電力Ｐｆｋ（Ｗ）と通信電力係数Ｐｋ（Ｗ・秒／Ｂｙｔｅ）で表す。Ｐｆｋ（Ｗ）は、通信データ速度に関わらず必要な電力であり、Ｐｋは、通信データ速度に比例して必要とする電力である。元の通信データは暗号化や圧縮や符号化によりそのデータ量が、一般的に変わる。暗号化の場合は、一般的にデータ量が増える。圧縮や符号化では、一般的にデータ量が減る。データ量の圧縮されるが、その圧縮率変化係数をｑとする。をｑ（０＜ｑ＜１）とする。ｑは、暗号アルゴリズム、圧縮アルゴリズム、符号化アルゴリズムなどによって決まる。圧縮アルゴリズムの場合、通信データのランダム性が高い場合とそうでない場合とでは、ｑの値は異なる。通信データの内容が予知できないと、ｑが正確にわからない場合もある。その場合は、１あるいは１に近い適切な値としてもよい。通信処理部２０が通信処理に費やす通信電力ＰＴ（Ｗ）は、ＰＴ（Ｗ）＝Ｐｋ＊（Ｄｒ＊ｑ）＋Ｐｆｋにより表せる。

【００８２】

ポータブル機器１００内のＣＰＵを使用して暗号アルゴリズムをソフトウェア処理する場合に、暗号処理部３０がＣＰＵ上で消費する電力は、次のような処理負荷情報を用いて計算できる。変換固定処理量Ｃｆａ（ＭＩＰＳ）は、データがなくとも必要な処理ステップである。単位ＭＩＰＳは、秒あたりの１００万処理ステップ数である。変換処理係数Ｃａ（ＭＩ／Ｂｙｔｅ）は、処理データ数に比例して必要とする処理ステップ数であり、Ｂｙｔｅ当たり１００万処理ステップ数を単位として表す。暗号アルゴリズムの処理に必要な処理能力は、（Ｃａ＊Ｄｒ＋Ｃｆａ）（ＭＩＰＳ）で表される。通信データ速度が大きいほど、多くの処理能力を必要とする。

【００８３】

暗号アルゴリズムの起動によりこれらの処理ステップを実行すると、ＣＰＵは以下の処理負荷情報に基づき電力を消費する。ＣＰＵ電力係数Ｐｍ（Ｗ／ＭＩＰＳ）は、１ＭＩＰＳ当たりの平均的な消費電力である。また、ＣＰＵは、命令処理の実行、非実行に関わらずＯＳ処理やカーネル処理により、ＣＰＵ固定部電力Ｐｆｍ（Ｗ）を消費するものとする。

【００８４】

通信処理にＣＰＵも使用する場合は、Ｐｆｍ（Ｗ）には、通信処理にかかわるＣＰＵの命令の実行に要する固定的な消費電力などが含まれる。通信データ速度によって、通信処理に必要なＣＰＵの処理能力が変化する部分がある場合は、Ｃａ（ＭＩＰＳ／Ｂｙｔｅ）に織り込んでもよい。

【００８５】

暗号アルゴリズムをＣＰＵ処理により実行する場合のポータブル機器１００の全消費電力Ｐｔ（Ｗ）は、Ｐｔ（Ｗ）＝Ｐｍ＊（Ｃａ＊Ｄｒ＋Ｃｆａ）＋Ｐｆｍ＋ＰＴ＋ＰＡで表すことができる。ＰＴは、上記説明した通信処理部２０の消費電力である。ＰＡ（Ｗ）は、表示部７０や入力手段８０、ＣＰＵが行う暗号アルゴリズム処理以外のタスク実行による消費電力である。

【００８６】

なお、変換処理用のＣＰＵ処理能力、すなわち、ＣＰＵが暗号アルゴリズム処理に割けるＣＰＵ最大処理能力をＭ（ＭＩＰＳ）とすると、（Ｃａ＊Ｄｒ＋Ｃｆａ）は、Ｍ（ＭＩＰＳ）以下である必要がある。

【００８７】

電池の残容量Ｐｂ（Ｗ・秒）を消費電力Ｐｃ（Ｗ）で割ると、予測電池寿命、あるいは、通信可能時間Ｔ（秒）が算出できる。すなわち、Ｔ（秒）＝Ｐｂ／Ｐｔである。通信可能時間Ｔ（秒）を各暗号アルゴリズムについて算出し、通信予定時間Ｔｓに対して、Ｔｓ＜Ｔを満足する暗号アルゴリズムを候補暗号アルゴリズムとして選択する。あるいは、通信予定時間Ｔｓ後に予測される電池の残容量（Ｐｂ－Ｐｃ＊Ｔｓ）が、正の値である暗号アルゴリズムを候補暗号アルゴリズムとして選択してもよい。なお、予測には誤差が避けられないので、適切な余裕、たとえば、１０％～３０％程度を見込むのが好ましい。

【００８８】

上記説明の方法では、前記処理負荷情報とは、通信データ速度Ｄｒ（Ｂｙｔｅ／秒）、通信固定電力Ｐｆｋ（Ｗ）、通信電力係数Ｐｋ（Ｗ・秒／Ｂｙｔｅ）、暗号化の圧縮率変化係数ｑ、各暗号アルゴリズムの変換固定処理量Ｃｆａ（ＭＩＰＳ）、変換処理係数Ｃａ（ＭＩ／Ｂｙｔｅ）、ＣＰＵ固定部電力Ｐｆｍ（Ｗ）、ＣＰＵ電力係数Ｐｍ（Ｗ／ＭＩＰＳ）、および、その他の消費電力ＰＡである。

【００８９】

図４（ａ）における負荷１、負荷２に対する予測電池寿命ｔ１、ｔ２も上記のような計算により算出できる。図４（ｂ）においては、Ｔａを通信予定時間とすれば、負荷１を適用した場合は、通信終了時の電池残量は、ＷＨ１＝Ｐｂ－Ｐｔとなることが予測できる。ＷＨ２、ＷＨ３についても同様に算出できる。

【００９０】

候補暗号アルゴリズムから使用する暗号アルゴリズムが１つ決定されれば、通信処理部２０は、暗号処理部３０に使用する暗号アルゴリズムを知らせて、暗号アルゴリズム処理を起動し、通信相手の機器との間で決定された暗号アルゴリズムに従った鍵を作成し、通信データの暗号化を開始し、暗号通信を始めることができる。なお、候補暗号アルゴリズムが１つだけの場合も、ネゴシエーションを行うことは言うまでもない。

【００９１】

（実施の形態２）

実施の形態１においては通信開始時における暗号アルゴリズムの選択に関して説明したが、本実施の形態では通信途中において暗号アルゴリズムを変更することができるようにする。

【００９２】

図５（ａ）は、通信途中で負荷を重たい負荷から軽い負荷に変更する場合の電池残容量の経過予測図である。データ通信装置は、時刻Ｔｂまで通信を継続する必要があるものとする。負荷２の処理を行っていたところ、時刻ｔ３になったときに、このままではＴｂより早い時刻であるｔ２で電池がなくなり、通信をそれ以上継続できないことが判明したとする。ここで、ポータブル機器１００は、通信相手機器に対して、消費電力が小さくなるような暗号アルゴリズムに変更する旨の要求を出す。通信相手機器とのネゴシエーションの結果、負荷１の処理で済むようになれば、時刻ｔ３以降は、負荷１で通信を行う。その結果、時刻Ｔｂにおいては容量ＷＨ４を残せることになり、Ｔｂまで通信を継続するという初期の目的を達することができる。負荷１の暗号アルゴリズムは、負荷２の暗号アルゴリズムに比べて、一般的に暗号強度が弱いが、通信を完了することを優先することになる。通信予定時間以内に電池残容量がなくなるのは、通信の途中で別のアプリケーションが発生して、予定外の電力を消費し始めた場合などが想定される。

【００９３】

図５（ｂ）は、通信途中で、より重たい負荷に変更する場合の経過予測図である。データ通信装置は、時刻Ｔｂまで通信を継続する必要があるとする。負荷１の処理を行っていたが、時刻ｔ５になったときに、このままで通信すると時刻ＴｂにおいてＷＨ５の電池容

量を残すことが判明したとする。そのとき、より強い暗号を使いたいならば、通信相手に対して、時刻Ｔｂまで電池の残容量がゼロにならない範囲で、暗号強度が強くなるような暗号アルゴリズムに変更する旨の要求を出す。通信相手とネゴシエーションが成功して負荷２の処理を行うことになると、時刻ｔ５以降は負荷２で通信を行う。時刻Ｔｂには残容量ＷＨ６を残して通信を終了できる。時刻ｔ５から時刻Ｔｂまでは、より強い暗号アルゴリズムにより通信を行い、最終的にＴｂまで通信を継続するという初期の目的も達することになる。通信途中で電池残容量に余裕ができるのは、別のアプリケーションが通信の途中で完了し、電力消費が減った場合などが想定される。

【００９４】

このような機能をポータブル機器１００に持たせるには、図１の残量算出部５０とリソース選択部４０が、実施の形態１で説明した電池の残容量Ｐｂ（Ｗ・秒）と消費電力Ｐｃ（Ｗ）の算出を、通信開始後も適当な時間間隔で、それぞれ行い、リソース選択部４０が、通信可能時間Ｔ（秒）、または、通信終了時の電池の残容量を算出するようにすればよい。なお、通信予定時間Ｔｓ（秒）には、今後送信を続ける残りの通信時間を、電池の残容量Ｐｂ（Ｗ・秒）には、その時刻における電池の残容量データを適用する。

【００９５】

上記、通信開始後の適当な時間間隔は、通信開始と通信終了予定時刻の１／２、１／３などの中間時刻でも良い。

【００９６】

時刻ｔｘにおける通信可能時間Ｔ（秒）が、残りの通信予定時間（Ｔｂ－ｔｘ）より小さければ、図５（ａ）の状態が予測される。この場合、リソース選択部４０は、通信処理部２０に対して、使用可能な電力消費の少ない暗号アルゴリズムを知らせると共に、ネゴシエーションを行うように指示する。通信処理部２０は、通信相手機器とネゴシエーションを行い、ネゴシエーションが成功すれば、負荷２１に相当する電力消費の少ない暗号アルゴリズムを適用できることになる。

【００９７】

時刻ｔｘにおける通信可能時間Ｔ（秒）が、残りの通信予定時間（Ｔｂ－ｔｘ）より大幅に大きければ、図５（ｂ）の状態が予測される。この場合、リソース選択部４０は、通信可能時間Ｔ（秒）が、（Ｔｂ－ｔｘ）より大きくなる条件で、使用中の暗号アルゴリズムよりも暗号強度が強い暗号アルゴリズムがあるかどうかを調べる。より強い暗号アルゴリズムが使用可能な場合、リソース選択部４０は、通信処理部２０に対して、より暗号強度の強い暗号アルゴリズムで使用可能なものを知らせると共に、ネゴシエーションを行うように指示する。通信処理部２０は、通信相手機器とネゴシエーションを行う。ネゴシエーションが成功すれば、負荷２に相当する暗号強度がより強い暗号アルゴリズムを適用できることになる。なお、ネゴシエーションが成功しなければ、負荷１のままとなる。

【００９８】

新たな暗号アルゴリズムが決定した後、直ちに新アルゴリズムを使用せず、以下のようにしてもよい。しても、直ちに切り替えて使用することはできない。元の暗号アルゴリズムを使用した暗号通信を継続しながら、新たな暗号アルゴリズムを起動し、通信相手機器との間で新暗号アルゴリズムに従った鍵の生成を行い、鍵の生成後に、新暗号アルゴリズムによる暗号通信を開始できるする。この段階で、元の暗号アルゴリズムの処理は不要になる。したがって、ＣＰＵは、一時的に、元の暗号アルゴリズムと新暗号アルゴリズムとを並列に処理できるようにする必要がある。ＣＰＵの処理能力が大きい場合には、並列処理は容易である。

【００９９】

ＣＰＵが元の暗号アルゴリズムによる暗号処理を行う合間、たとえば、送信データの所定のパケット長の暗号化が終わり、次のパケットの暗号化までの待ち時間に、新暗号アルゴリズムによる鍵の生成処理を行えば、ＣＰＵの暗号処理能力は、１つの暗号アルゴリズムの処理能力程度で済む。

【０１００】

１回の合間に新しい鍵の生成が完了できない場合は、数回の合間を使用して時分割的に生成を進めてゆくようにする。このためには、ＣＰＵは、２つの暗号アルゴリズム処理を切り替える機能だけでなく、鍵生成途中で暗号アルゴリズムを切り替える直前の状態を退避記憶し、鍵生成途中の状態を再現して生成を継続できる機能が必要である。ＣＰＵは、通常マルチタスクに対応できる。２つの暗号アルゴリズムのプログラムを起動しておき、新暗号アルゴリズムの優先度を低くしておくと、ＣＰＵは、複数に分割した処理区間の大部分を優先的に暗号通信処理に割り当てて実行し、残りで新暗号アルゴリズムの処理を行う。新暗号アルゴリズムによる鍵は、やや時間がかかるものの生成できる。鍵の生成処理は、基本的にデータの暗号化と同様の演算を基本とする繰り返し処理であり、鍵のデータ量はせいぜい数十Ｂｙｔｅであるので、図２（ａ）から分るように、割けるＣＰＵ処理能力が低くても、数百ミリ秒を越えない。したがって、鍵の生成に必要とする消費電力や新暗号アルゴリズムへの切り替えの遅れは、上記推定した電池寿命の値に影響を与えるほどではない。鍵が生成されると、新暗号アルゴリズムによる暗号通信を開始することができる。

【０１０１】

（実施の形態３）

つぎに、リソース選択部４０が、暗号アルゴリズム以外のリソースの選択も行う場合の実施の形態について説明する。

【０１０２】

暗号アルゴリズムの処理は、一般的に、ＣＰＵに極めて大きな処理能力を要求する重い処理である。ＣＰＵに対する過重な負荷の発生を避けるためには、専用の暗号アルゴリズム処理ＬＳＩを設けて暗号アルゴリズムの処理を行わせればよい。高画質の映像データのような高速通信データに暗号強度の高い暗号処理を行う場合に有効である。このような高能力の暗号アルゴリズム処理ＬＳＩは、消費電力が比較的大きいので、低速通信データに使用したり、暗号強度が高くない暗号処理を行ったりするのには、電力の有効利用の点で、適当とは言えない場合がある。最近では、専用ＬＳＩでありながら、目的の機能を実行するのに最適な回路構成に変更することができる、リコンフィギュアラブルロジックが使用可能になっている。暗号アルゴリズム処理ＬＳＩの場合には、ハードウェア処理の回路方式を変えて、消費電力は大きいが高速の暗号処理ができる回路構成と、処理速度はやや低下するかもしれないが、消費電力を減らすことができる回路構成とに切り替えることが可能である。

【０１０３】

一方、ポータブル機器の場合、ＡＣ電源使用時には、通常のＣＰＵ処理能力により処理を行い、ＡＣ電源が使用できない電池利用時には、ＣＰＵのクロック周波数を低下させて、ＣＰＵ処理能力を下げて使用する省電力モードを設けることが行われる。省電力モードでのＣＰＵ処理能力の場合は、暗号アルゴリズムに割けるＣＰＵ処理能力は制限されるので、低速通信データや暗号強度が高くない暗号アルゴリズムにしか使用できないことも起きる。

【０１０４】

暗号通信においては、暗号アルゴリズムを実行する手段として、上記説明のように、高速ハードウェア処理、中速～低速ハードウェア処理、中速ソフトウェア処理、低速ソフトウェア処理などの複数の処理から選択して使用することができる環境を備えたデータ通信装置であるポータブル機器を構成することができる。図６は、このようなポータブル機器１００ａにおいて、本発明を適用した場合の要部のブロック構成図である。図１で説明した実施の形態１の場合と同じ構成要素については同じ番号を付与し、その説明を省くことがある。なお、暗号処理部３０ａは、後述するように一般的には、変換アルゴリズムを実行する変換処理部３０ａであるが、本実施の形態での説明では、暗号アルゴリズムを実行する暗号処理部３０ａとして説明する。

【０１０５】

図６において、暗号処理部３０ａは、実施の形態１で説明したと同様に、プログラムメ

モリ（図示しない）内に設けられたプログラムの処理手順に従って、ＣＰＵ内部でソフトウェア処理により実行される場合と、ＣＰＵとは別の処理装置である専用ＬＳＩの内部に設けられたハードウェアにより実行される場合があるものとする。ポータブル機器１００ａの電源モードがＡＣ電源から電池の電源に切り替えられると、ＣＰＵ（図６には示していない）の動作モードは、通常モードから省電力モードに切り替わるようになっている。専用ＬＳＩの内部に設けられたハードウェア構成も高速モードと通常モードの２つの状態が切り替えられるようになっている。また、専用ＬＳＩを使用しない場合は、専用ＬＳＩを非選択にして消費電力をほぼゼロに近い最低値にすることができるものとする。ＣＰＵの通常モードにおける暗号処理、省電力モードにおける暗号処理、専用ＬＳＩの高速モード、通常速モードを、それぞれ暗号処理のモジュールと呼ぶことにする。モジュール管理部９０は、暗号処理のモジュールの切り替えと専用ＬＳＩの非選択モードの切り替えとを行う。また、後述するように、各モジュールに関わる処置負荷情報を記憶しておく。

【０１０６】

リソース選択部４０ａは、暗号アルゴリズムの選択だけでなく、暗号処理モジュールの選択も行う。本実施の形態３においては、実施の形態１で行った電池の残容量Ｐｂ（Ｗ・秒）、ソフトウェア処理による消費電力Ｐｃ（Ｗ）、および、その場合の予測電池寿命（または通信可能時間）Ｔ（秒）、または、通信終了時の最終の残容量の算出に加えて、以下の演算処理を行う。

【０１０７】

モジュール管理部９０は、ハードウェア処理における処理負荷情報として、変換固定電力Ｃｆｈ（Ｗ）と変換電力係数Ｃｈ（Ｗ・秒／Ｂｙｔｅ）を、高速モード、通常モード毎に保有している。変換固定電力Ｃｆｈ（Ｗ）は、データ入力がなくとも専用ＬＳＩが消費する電力値である。変換電力係数Ｃｈ（Ｗ・秒／Ｂｙｔｅ）は、暗号処理に伴ってＢｙｔｅ当たり必要とする電力を表す電力係数である。通信データ速度Ｄｒ（Ｂｙｔｅ／秒）に対して、専用ＬＳＩが消費する電力は、（Ｃｈ＊Ｄｒ＋Ｃｆｈ）となる。したがって、ポータブル機器１００ａが消費する電力は、Ｐｃ（Ｗ）＝Ｃｈ＊Ｄｒ＋Ｃｆｈ＋ＰＴ＋ＰＡにより表される。ＰＴ、ＰＡは、実施の形態１において説明したものである。この演算により、高速モードと通常速モードでの２種類の消費電力が求められる。

【０１０８】

専用ＬＳＩが、複数の暗号アルゴリズム処理を行える場合は、それぞれの暗号アルゴリズムに対応して、変換固定電力Ｃｆｈ（Ｗ）と変換電力係数Ｃｈ（Ｗ・秒／Ｂｙｔｅ）の値が異なることもある。この場合は、高速モード、通常速モードの２種類と、暗号アルゴリズムの種類数との積だけの組み合わせができ、それぞれに対応してＰｃ（Ｗ）が演算される。全組み合わせのそれぞれに対して、電池の残容量Ｐｂ（Ｗ・秒）と消費電力Ｐｃ（Ｗ）の比である予測電池寿命（または通信可能時間）Ｔ（秒）＝Ｐｂ／Ｐｔを算出し、通信の予定時間Ｔｓに対して、Ｔｓ＜Ｔを満足するＬＳＩ構成と暗号アルゴリズムの組を、候補モジュール・暗号アルゴリズム対として選択する。複数の組がある場合、その全てを候補モジュール・暗号アルゴリズム対として選択する。

【０１０９】

なお、専用ＬＳＩが、上記高速モードと通常速モードを備えておらず、１種類のモードだけの場合もある。この場合は、専用ＬＳＩ上で実行できる暗号アルゴリズムに対して、上記演算を行えばよい。専用ＬＳＩは、モジュールとしては１種類となる。

【０１１０】

一方、ＣＰＵによるソフトウェア処理の場合、変換処理用ＣＰＵ処理能力、すなわち、暗号処理用の最大処理能力の通常モードにおける値をＭ１（ＭＩＰＳ）、省電力モードにおける値をＭ２（ＭＩＰＳ）とした場合、モジュールは２種類となる。これらのモジュールにおいては、次の条件を満たす必要がある。すなわち、通信予定時間Ｔｓに対して、通信予定時間Ｔｓ（秒）＜予測電池寿命（または通信可能時間）Ｔ（秒）を満足する暗号アルゴリズムであっても、その暗号アルゴリズム処理に必要なＣＰＵ処理能力（Ｃａ＊Ｄｒ＋Ｃｆａ）は、Ｍ１、または、Ｍ２以下である必要がある。複数の暗号アルゴリズムの内

、上記条件を満たす暗号アルゴリズムが１つ以上ある場合、その電力モードと暗号アルゴリズムの組み合わせを候補モジュール・暗号アルゴリズム対として選択する。

【０１１１】

選択された専用ＬＳＩでの候補モジュール・暗号アルゴリズム対と、ソフトウェア処理における候補モジュール・暗号アルゴリズム対の、何れかに含まれる暗号アルゴリズムは、１つ、複数を問わず、候補暗号アルゴリズムとして通信処理部２０に通知される。通信処理部２０では、候補暗号アルゴリズムについて、通信相手とネゴシエーションを行う。通信処理部２０は、ネゴシエーションで使用可能となった暗号アルゴリズムの内から暗号強度が最も高いものを１つ選び、所定暗号アルゴリズムとして、リソース選択部４０ａに通知する。リソース選択部４０ａは、通知された前記所定暗号アルゴリズムに対応する候補モジュール・暗号アルゴリズム対を探し、その暗号アルゴリズムに対応するモジュールを決定モジュールとしてモジュール管理部９０と通信処理部２０に通知する。対応するモジュールが複数ある場合、リソース選択部４０ａは、消費電力Ｐｃ（Ｗ）が小さい数値となるモジュールを１つ選択決定する。モジュール管理部９０は、通知されたモジュール名、または、モジュール識別子にしたがって、暗号アルゴリズム実行モジュールの設定を行う。具体的には、ＣＰＵの電力モード、すなわち、クロック周波数の切り替え指示、あるいは、専用ＬＳＩの回路構成の切り替え指示、専用ＬＳＩの選択・非選択の切り替え指示を行う。これらの切り替え処理が完了後、通信処理部２０は、選択されたモジュール上で選択された前記所定暗号アルゴリズムを使用して通信相手機器との間で鍵の生成処理を行い、通信アプリケーション１０は通信データの生成を開始し、通信処理部２０は通信処理を行うことになる。

【０１１２】

上記ネゴシエーションで使用可能となった暗号アルゴリズムの内で暗号強度が最も高い前記所定暗号アルゴリズムに対応できるモジュールが複数ある場合とは、通常モードと省電力モードのどちらでもソフトウェア処理できる場合や、ハードウェア処理、ソフトウェア処理のどちらも、上記各条件を満たしている場合などがある。また、ソフトウェア処理は、ハードウェア処理よりも、消費電力が小さいとは限らないことに注意すべきである。ハードウェア処理の回路構成が適切に構成されている場合、ＣＰＵが行うよりも合理的な処理手順を簡素な回路で実行できる場合がある。したがって、リソース選択部４０ａは、１つの暗号アルゴリズムに対して、消費電力の観点から、ＣＰＵでなく専用ＬＳＩをモジュールとして選択する場合もあり得る。リソース選択部４０の選択の基準は、通信予定時間Ｔｓ（秒）＜予測電池寿命（または通信可能時間）Ｔ（秒）、暗号強度、消費電力の順とするのが一般的に好ましい。しかし、他に実行すべきアプリケーションが存在する場合など、場合によっては、この限りではない。

【０１１３】

本実施の形態３では、処理負荷情報は、通信データ速度Ｄｒ（Ｂｙｔｅ／秒）、通信固定電力Ｐｆｋ（Ｗ）、通信電力係数Ｐｋ（Ｗ・秒／Ｂｙｔｅ）、暗号化の場合の圧縮率変化係数ｑ、各暗号アルゴリズムの変換固定処理量Ｃｆａ（ＭＩＰＳ）、変換処理係数Ｃａ（ＭＩ／Ｂｙｔｅ）、ＣＰＵ固定部電力Ｐｆｍ（Ｗ）、ＣＰＵ電力係数Ｐｍ（Ｗ／ＭＩＰＳ）、および、その他の消費電力ＰＡ、に加えて、変換固定電力Ｃｆｈ（Ｗ）、変換電力係数Ｃｈ（Ｗ・秒／Ｂｙｔｅ）、ＣＰＵの電力モードに対応した暗号アルゴリズム処理能力Ｍ１（ＭＩＰＳ）、Ｍ２（ＭＩＰＳ）となる。これらの情報は、リソース選択部４０ａ内部に保持していてもよいし、通信アプリケーション１０、通信処理部２０、暗号処理部３０ａ、モジュール管理部９０内に分けて保持しておくようにしてもよい。

【０１１４】

上記リソース選択部４０ａが行う候補モジュール・暗号アルゴリズム対の選択処理と候補暗号アルゴリズムの選択処理は、通信開始前に行うようにすればよい。

【０１１５】

なお、上記説明では、モジュールとして、ＣＰＵの通常モード、省電力モード、専用ＬＳＩで少なくとも１種類の内部構成を想定して説明した。専用ＬＳＩを備えていない場合

には、モジュールはＣＰＵの通常モードと省電力モードの２種類になる。

【０１１６】

（実施の形態４）

上記実施の形態３において、実施の形態２の場合と同様に、通信開始後にも定期的に、電池の残容量による通信可能な時間Ｔ（秒）と残りの通信予定時間Ｔｓ（秒）との比較、あるいは、通信終了時の電池残容量の予測計算を行い、図５（ａ）の時刻ｔ３や、図５（ｂ）の時刻ｔ５の場合と同様の状態が起こったときには、最適な新モジュールの選択と最適な新暗号アルゴリズムの選択決定を行うようにしてもよい。ただし、新モジュールへの切り替えや新暗号アルゴリズムへの切り替えの間、通信を行うことができないと、動画伝送などの場合、画面が途切れる恐れがあるので、ひとまとまりの送信データの処理が完了した時間の後の空隙時間内に、切り替えを行うことが望ましい。

【０１１７】

すなわち、新たな暗号アルゴリズムが決定しても、直ちに切り替えての使用は行わない。元のモジュールと元の暗号アルゴリズムを使用した暗号通信を継続しながら、新たなモジュールと新たな暗号アルゴリズムを起動し、通信相手機器との間で新暗号アルゴリズムに従った鍵の生成を行い、鍵の生成後に、始めて新モジュールと新暗号アルゴリズムによる暗号通信が開始できる。この段階で、元のモジュールと元の暗号アルゴリズムの処理は不要になる。

【０１１８】

元のモジュールと新モジュールが共にＣＰＵ処理の場合は、ＣＰＵは、一時的に、元の暗号アルゴリズムと新暗号アルゴリズムとを並列に処理できるようにする必要がある。ＣＰＵが２つの暗号アルゴリズムを並列処理するには、実施の形態２において説明したと同様の方法を適用すればよい。なお、専用ＬＳＩを備えている場合、これを一時的に起動して、新暗号アルゴリズムによる鍵の生成を専用ＬＳＩ上で行うようにしてもよい。

【０１１９】

元のモジュールと新モジュールの一方がＣＰＵ、他方が専用ＬＳＩの場合は、それぞれにおいて、暗号アルゴリズム処理を動作させることができるので、元のモジュールにおいて、元の暗号アルゴリズムにより暗号通信を継続しながら、新モジュールにおいて新暗号アルゴリズムによる鍵の生成を並列的に行うことができる。

【０１２０】

元のモジュールと新モジュールの両方が専用ＬＳＩで、元の暗号アルゴリズムと新暗号アルゴリズムとが同一内部構成では動作できず、新暗号アルゴリズムのために内部構成を変更する必要がある場合には、つぎのいずれかのようにすればよい。

【０１２１】

元のモジュールによる送信データの所定のパケット長の暗号化が終わった後、次の所定パケットの暗号化までに、内部構成変更と新暗号アルゴリズムによる鍵の生成を完了する時間の余裕がある場合は、前記所定のパケット長の暗号化が終わった後、直ちにモジュールの変更と鍵の生成処理を行えばよい。専用ＬＳＩの処理能力が高い場合、このような手段の適用が可能になる。

【０１２２】

専用ＬＳＩが、２つのモジュールの切り替えと２つの暗号アルゴリズムの切り替えについて、切り替え直前の状態を記憶退避できるようにし、再びもとのモジュールと暗号アルゴリズムに戻ったときに継続して暗号化や鍵生成を行えるようにしてもよい。専用ＬＳＩが２の暗号アルゴリズムをマルチタスクとして処理するように構成して、それぞれの暗号アルゴリズムに割り当てる処理能力を変化できるようにしてもよい。鍵の生成後に、新暗号アルゴリズム専用に構成しなおすようにしてもよい。

【０１２３】

専用ＬＳＩでは、元のモジュール、元の暗号アルゴリズムによる暗号処理と暗号通信を続行しておき、専用ＬＳＩ上で実行すべき新暗号アルゴリズムを一時的にＣＰＵ上で行うようにして、鍵の生成をＣＰＵ上で行い、鍵の生成完了後で、送信データの所定パケット

長の暗号化が完了した直後に、専用ＬＳＩを新モジュールの内部構成に切り替え、生成した鍵を使用して、新暗号アルゴリズムによる暗号通信を開始するようにしてもよい。新暗号アルゴリズムの鍵の生成は、多少の時間がかかってもよいので、ＣＰＵ上の新暗号アルゴリズム処理の速度は遅くてもよい。したがって、この場合のＣＰＵの暗号処理能力は、Ｍ１程必要とせず、Ｍ２並あるいはそれより低くても差し支えない。

【０１２４】

なお、上記説明では、モジュールとして、ＣＰＵの通常モード、省電力モード、専用ＬＳＩでの少なくとも１種類の内部構成を想定して説明した。専用ＬＳＩを備えていない場合、モジュールはＣＰＵの通常モードと省電力モードの２種類になる。

【０１２５】

（実施の形態５）

つぎに、利用している電源の種類によって、ＣＰＵの処理能力を異ならせる場合について説明する。実施の形態３において触れたように、例えば、ＡＣアダプタ利用状態から電池利用時に切り替わると、ＣＰＵは、通常モードから省電力モードに切り替わるようにする。

【０１２６】

図７に、ポータブル機器の電源状況に応じた負荷の切り替え図を示す。図７（ａ）において、区間ＴＡＣでは、ポータブル機器１００ａを、ＡＣアダプタで電源供給しながら通常モードで使用している。時刻ｔＤＣになったとき、ＡＣアダプタをはずし、ポータブルでの利用（電池利用）になったとする。ｔＤＣ以降の区間ＴＤＣでは、ポータブル機器を、電池利用による省電力モードに移行しなくてはならない。

【０１２７】

区間ＴＡＣにおいて、負荷３をＣＰＵにより処理していると、時刻ｔＤＣになった途端に、ＣＰＵ処理能力が不足となる。例えば、ポータブル機器で映像ストリームを受信している場合だと、途切れ途切れの受信や表示になってしまう。

【０１２８】

そこで、図７（ｂ）に示すように、時刻ｔＤＣになった場合にすぐにＣＰＵが電池利用時の省電力モードに移行するのではなく、しばらくの間通常モードを維持しておき、その間に、省電力モードで通信を維持できる新暗号アルゴリズムに切り替えるためのネゴシエーションを行い、時刻ｔＤＣ１に負荷４に移行した後、ｔＤＣ２においてＣＰＵを省電力モードに切り替えるようにする。このようにすれば、映像ストリームなどを途切れさせることなく暗号通信できる。

【０１２９】

このためには、図８に示すように、モジュール管理部９０ａ、電源検知部１１０、ＣＰＵクロック１２０を設ける。他の部分は図６の場合と同様である。電源検知部１１０は、使用電源の切り替えを検知し、使用電源をモジュール管理部９０ａに知らせる。モジュール管理部９０ａは、使用電源切り替えが起きたことと、現在のＣＰＵが通常モードか、省電力モードかをリソース選択部４０ａに知らせ、リソース選択処理を依頼する。リソース選択部４０ａは、通信処理部２０が暗号通信実行中かどうか調べ、実行中の場合には、現在モジュールがＣＰＵで、かつ、省電力モードでない場合、現暗号アルゴリズムによる変換処理量（Ｃａ＊Ｄｒ＋Ｃｆａ）が、変換処理用のＣＰＵ処理能力Ｍ２（ＭＩＰＳ）より小さいかどうか判定する。

【０１３０】

小さい場合は、残量算出部５０とリソース選択部４０ａが、現時点における電池の残容量Ｐｂ（Ｗ・秒）と消費電力Ｐｃ（Ｗ）を算出し、リソース選択部４０ａが、予測電池寿命（または通信可能時間）Ｔ（秒）を算出する。予測電池寿命（または通信可能時間）Ｔ（秒）が今後送信を続けるべき残りの通信予定時間Ｔｓ（秒）を上回れば、リソース選択部４０ａは、モジュール管理部９０ａに指示して、ＣＰＵを通常モードから省電力モードに切り替える処理を行わせる。モジュール管理部９０ａは、ＣＰＵクロック１２０がクロック周波数を省電力モードに変更するように制御する。よって、モジュールは、ＣＰＵ省

電力モードに変更されるが、暗号アルゴリズムは現状のままとなる。

【０１３１】

一方、現暗号アルゴリズムによる変換処理量（Ｃａ＊Ｄｒ＋Ｃｆａ）が変換処理用のＣＰＵ処理能力Ｍ２（ＭＩＰＳ）より大きい場合は、ＣＰＵの動作モードを省電力モードに切り替えると通信データ速度に対応した暗号処理が行えなくなる。リソース選択部４０ａは、実施の形態４で説明したと同様に、候補モジュール・暗号アルゴリズム対の選択を行い、通信処理部２０にネゴシエーションを行わせる。ＣＰＵ省電力モードでも残りの通信予定時間の暗号通信を行えるような暗号アルゴリズムをネゴシエーションすることができれば、上記説明した切り替え手順により、暗号通信をこの新暗号アルゴリズムに切り替えた後、リソース選択部４０ａは、モジュール管理部９０ａに指示して、ＣＰＵを通常モードから省電力モードに切り替える処理を行わせる。モジュール管理部９０ａは、ＣＰＵクロック１２０がクロック周波数を省電力モードに変更するように制御する。

【０１３２】

現在モジュールが専用ＬＳＩである場合も、上記説明と同様に、リソース選択部４０ａは、候補モジュール・暗号アルゴリズム対の選択を行い、通信処理部２０にネゴシエーションを行わせる。ＣＰＵ省電力モードでも残りの通信予定時間の暗号通信を行えるような暗号アルゴリズムをネゴシエーションすることができれば、暗号通信をこの新暗号アルゴリズムに切り替えた後、リソース選択部４０ａは、モジュール管理部９０ａに指示して、ＣＰＵを通常モードから省電力モードに切り替える処理を行わせる。モジュール管理部９０ａは、ＣＰＵクロック１２０がクロック周波数を省電力モードに変更するように制御する。

【０１３３】

なお、専用ＬＳＩをモジュールとして選択した方が、ＣＰＵ省電力モードをモジュールとする場合より電力消費が少ない場合もあるので、この場合は、専用ＬＳＩを使用して暗号通信を行い、ＣＰＵが省電力モードに切り替えられることになる。

【０１３４】

専用ＬＳＩを備えていない場合も、ＣＰＵ通常モードと省電力モードとが２つのモジュールに対応することになる。

【０１３５】

（実施の形態６）

上記各実施の形態での暗号アルゴリズムの決定処理やモジュールの決定処理は、ＣＰＵ上でプログラムにより実行できる。すなわち、リソース選択部４０、４０ａ、モジュール管理部９０、９０ａは、ＣＰＵ上に構成できる。プログラムの手順は、上記各実施の形態での処理の説明から明らかであるが、念のため、以下に、若干説明する。

【０１３６】

図９は、上記実施の形態３で説明した処理を、ＣＰＵが行う場合のフローチャートで示したものである。

【０１３７】

図９において、まず（Ｓ１０）において、電池の現在残容量を算出し、（Ｓ１１）に進む。（Ｓ１１）において、処理負荷情報を参照しＣＰＵモジュールでのソフト処理による消費電力を各暗号アルゴリズムについて算出し、（Ｓ１２）に進む。（Ｓ１２）において、処理負荷情報を参照し、専用ＬＳＩモジュールでのハード処理による消費電力を各暗号アルゴリズムについて算出し、（Ｓ１３）に進む。（Ｓ１３）において、通信終了予定時刻Ｔｂでの最終残容量を算出し、（Ｓ１４）に進む。（Ｓ１４）において、全モジュール、全暗号アルゴリズムについて最終残容量の算出を完了したかどうか判定する。Ｎｏの場合（Ｓ１１）に戻る。（Ｓ１４）においてＹｅｓの場合（Ｓ１５）に進み、時刻Ｔｂで残容量に余裕があるものを選択する。つぎに、（Ｓ１６）に進み、通信相手と暗号アルゴリズムのネゴシエーションを行い暗号強度が高いものを選ぶ。つぎに、（Ｓ１７）に進み、選択した暗号アルゴリズムより使用モジュールを決定する。つぎに、（Ｓ１８）に進み、決定したモジュールを設定させ決定した暗号アルゴリズムにより鍵を生成する。つぎに、

（Ｓ１９）に進み、生成した鍵、決定したモジュール、決定した暗号アルゴリズムを使用して暗号通信を行う。

【０１３８】

各ステップにおける演算は、上記実施の形態１、３で説明した各数式を適用すればよい。

【０１３９】

専用ＬＳＩを使用しない実施の形態１、２の場合には、（Ｓ１２）は不要である。

【０１４０】

モジュールが１通りである場合には、（Ｓ１１）、（Ｓ１２）はどちらか一方になり、（Ｓ１７）は不要である。（Ｓ１８）におけるモジュールの設定も不要である。

【０１４１】

実施の形態１、３の動作を行う場合は、暗号通信開始の前に、上記フローチャートの手順を実行すればよい。実施の形態２、４の動作を行う場合は、暗号通信開始の前と開始後定期的に、上記フローチャートの手順を実行すればよい。実施の形態５の場合は、電源モードが変更になったときに上記フローチャートの手順を実行し、その後ＣＰＵの動作モードを変更すればよい。

【０１４２】

（実施の形態７）

上記各実施の形態では、データ通信において本発明を適用する場合について説明したが、本発明は、通信用途以外にも適用が可能である。デジタルテレビ放送やドキュメンタリ番組を収録して、ＨＤＤ（ハードディスクドライブ）に保存する場合に、番組の途中で、電池の電力がなくなる事態を避けるために、画質が劣化するのを許容しても消費電力の少ない符号化アルゴリズムに変更して最後まで収録する場合に適用できる。ＨＤＤに保存された映像情報を最後まで見るために、画質が劣化するのを許容しても消費電力の少ない復号化アルゴリズムに切り替えて最後まで映像情報を再生する用途もある。また、デジタルデータを圧縮して保存する装置においてはその圧縮アルゴリズムや圧縮率によって処理負荷が変わるので、電池残容量に合わせて、圧縮アルゴリズムや圧縮率を変更するようにすればよい。すなわち、一般的な名前を付けるなら、電池の残容量に合わせて変換アルゴリズムを選択する変換選択装置である。

【０１４３】

図１０に本発明の変換選択装置のブロック構成図を示す。図１０において、一般的なアプリケーション１０ｂが、ポータブル機器１００ｂ内部で、一連のデータの変換処理を行って、処理結果をＨＤＤに保存する場合を想定する。アプリケーション１０ｂが、データ変換予定時間の処理負荷情報をリソース選択部４０ｂに与える。変換処理部３０ｂも各変換アルゴリズムに関する処理負荷情報をリソース選択部４０ｂに与える。モジュール管理部９０ｂも各モジュールに関する処理負荷情報をリソース選択部４０ｂに与える。リソース選択部４０ｂは、各処理負荷情報を元に演算を行い、既に説明した方法により、候補モジュール・変換アルゴリズム対を選択する。リソース選択部４０ｂまたは、アプリケーション１０ｂが、候補モジュール・変換アルゴリズム対の中から１つの対を選択決定するようにする。決定されたモジュールをモジュール管理部９０ｂが、ＣＰＵまたは、専用ＬＳＩ上に生成する。変換処理部３０ｂは、生成されたモジュール上で、決定された変換アルゴリズムを使用して、データ変換処理を行う。

【０１４４】

電源モードが切り替わった場合の、ＣＰＵの動作モードの切り替えに伴う変換アルゴリズムの変更やモジュールの切り替えについては、上記実施の形態５において図６と共に説明したのと同様の動作を行うことができる。

【０１４５】

モジュールを備えない場合は、モジュール管理部９０ｂは不要である。上記実施の形態１、２において図１と共に説明した場合と同様に、リソース選択部４０ｂは、候補モジュール・変換アルゴリズムの代わりに候補変換アルゴリズムを選択し、１つに決定すること

になる。

【０１４６】

（実施の形態８）

上記実施の形態７での変換アルゴリズムの決定処理やモジュールの決定処理は、ＣＰＵ上でプログラムにより実行できる。すなわち、リソース選択部４０ｂ、モジュール管理部９０ｂは、ＣＰＵ上に構成できる。プログラムの手順は、上記実施の形態７での処理の説明から明らかであるが、念のため、以下に、若干説明する。

【０１４７】

図１１は、上記実施の形態７で説明した処理を、ＣＰＵが行う場合のフローチャートで示したものである。

【０１４８】

図１１において、まず（Ｓ３０）において、電池の現在残容量を算出し、（Ｓ３１）に進む。（Ｓ３１）において、処理負荷情報を参照しＣＰＵモジュールでのソフト処理による消費電力を各変換アルゴリズムについて算出し、（Ｓ３２）に進む。（Ｓ３２）において、処理負荷情報を参照し、専用ＬＳＩモジュールでのハード処理による消費電力を各変換アルゴリズムについて算出し、（Ｓ３３）に進む。（Ｓ３３）において、変換終了予定時刻Ｔｂでの最終残容量を算出し、（Ｓ３４）に進む。（Ｓ３４）において、全モジュール、全変換アルゴリズムについて最終残容量の算出を完了したかどうか判定する。Ｎｏの場合（Ｓ３１）に戻る。（Ｓ３４）においてＹｅｓの場合（Ｓ３５）に進み、時刻Ｔｂで残容量に余裕があるものを選択する。つぎに、（Ｓ３６）に進み、性能が高い変換アルゴリズムを選ぶ。性能が高いとは、アプリケーションによって異なる。圧縮アルゴリズムでは、圧縮率が高いもの、符号化アルゴリズムでは、画質や音質劣化が少ないものなどが上げられるが、評価尺度はこれらに限らない。つぎに、（Ｓ３７）に進み、選択した暗号アルゴリズムより使用モジュールを決定し、モジュールを設定する。つぎに、（Ｓ３８）に進み、決定したモジュール、決定した変換アルゴリズムを使用して変換処理を行う。

【０１４９】

各ステップにおける演算は、上記実施の形態１、３で説明した数式を適用すればよい。

【０１５０】

専用ＬＳＩを使用しない場合には、（Ｓ３２）は不要である。

【０１５１】

モジュールが１通りである場合には、（Ｓ３１）、（Ｓ３２）はどちらか一方になり、（Ｓ３７）は不要である。

【０１５２】

上記フローチャートの手順は、変換処理開始の前、変換処理の途中などに実行すればよい。電源モードが変更になったときにも、上記フローチャートの手順を実行すればよい。

【０１５３】

（その他の実施の形態および補足）

上記実施の形態５では、暗号通信の途中で、電源モードが変化した場合に、暗号アルゴリズムを変更する方法であったが、最初から、ポータブル利用、すなわち、電池利用モードへの移行が予測される場合には、暗号通信の途中でＡＣ利用から電池利用になっても良いように、ＡＣ電源時の段階から、電池時のＣＰＵ処理能力で処理できる負荷を利用するようにしても良いのは言うまでもない。候補アルゴリズムや候補モジュールを電源モードと共に表示部７０に表示し、使用者が入力手段８０により選択するようにし、その後ネゴシエーションを行うようにすればよい。ネゴシエーションにより、候補アルゴリズムや候補モジュールから使用可能なものを絞り込んだ後で、使用者が選択するようにしても良い。

【０１５４】

上記暗号通信においては、暗号アルゴリズム自体を変更する方法を例としてあげたが、通信データのパケットに対して暗号処理（秘匿性確保のため）とハッシュ処理（パケットの正当性の認証のため）を施す暗号認証アルゴリズムしているの場合には、認証用のハッ

シュ演算処理を除いて暗号処理だけにして負荷を軽くすることにより、負荷を減らすようにしてもよい。逆に、暗号処理の方を省いて、認証処理のみにすることにより、負荷を減らすようにしてもよい。本発明において、認証専用の認証アルゴリズムを使用する場合も、アルゴリズムを変更して負荷を減らしたり、認証の強度を変更したりできることはいうまでもない。暗号認証アルゴリズムや認証アルゴリズムでは、上記所定の変換アルゴリズムとして、ネゴシエーションにおいて、耐改ざん性がより高いアルゴリズムを選択すればよい。

【０１５５】

上記暗号通信では、負荷の変更の仕方として、暗号アルゴリズムを変える方法をあげたが、それ以外に、同じ暗号アルゴリズムにおいて、鍵長を変えるようにしてもよい。

【０１５６】

上記暗号アルゴリズム、暗号認証アルゴリズム、認証アルゴリズムの変更や鍵長の変更は、リキー処理の中で行ってもよい。

【０１５７】

暗号アルゴリズム、暗号認証アルゴリズム、認証アルゴリズムを使用する場合、通信データ量を減らして、処理負荷を軽くするために、予め圧縮アルゴリズムの処理を行う場合がある。この場合は、圧縮アルゴリズムも含めて、総合的な負荷に対して、本発明を適用して、最適負荷を選択するようにしてもよい。暗号アルゴリズム、暗号認証アルゴリズム、認証アルゴリズムの何れかに符号化アルゴリズムを併用する場合も同様である。

【０１５８】

上記暗号通信の各実施の形態の説明では、自機器の電池の状況により、暗号アルゴリズムを通信相手に提案する動作を説明した。通信相手機器から暗号アルゴリズムの提案、あるいは、その変更の提案があった場合には、（１）自機器の電源事情に鑑みて、対応可能な提案（暗号アルゴリズムの種類など）に応える、（２）適切なアルゴリズムが提案されてこなかった場合は、対応可能な提案を行う、などにより、通信相手機器も合わせたシステムとしての暗号通信利用可能時間を延ばすことができる。この場合も、上記説明した暗号アルゴリズムやモジュールの選択手順が使用できる。

【０１５９】

上記暗号通信では、１対１の場合の通信を想定して説明したが、本発明では、３つ以上の機器グループ間で通信する場合には、グループ内で一番低い能力に合わせてネゴシエーションを行うことにより、より長時間の暗号通信が行えることになる。

【０１６０】

上記各実施の形態１～６では、暗号通信について説明したが、本発明は、暗号通信に限らない。すなわち、通信データを特定の形式に変換する、暗号アルゴリズム以外の変換アルゴリズムについても、本発明を適用できる。たとえば、デジタルデータを圧縮して通信する装置においてはその圧縮アルゴリズムや圧縮率によって処理負荷が変わるので、電池残容量に合わせて、圧縮アルゴリズムや圧縮率を変更するようにすればよい。映像音声を符号化して通信する装置においては符号化アルゴリズムを、その電池残容量に合わせて変更するようにすればよい。同じ符号化アルゴリズムにおける圧縮率を選択してその電池残容量に合わせて変更するようにしてもよい。このように、暗号アルゴリズム以外の変換アルゴリズムを使用する場合は、図１、６、８の暗号処理部３０、３０ａの代わりに変換処理部を設ければよい。なお、圧縮アルゴリズムや符号化アルゴリズムを変更する場合にも、新アルゴリズムに通信相手機器が対応できるかどうかのネゴシエーションが必要であるが、ネゴシエーションが成功すれば、次の通信データパケットから新アルゴリズムを使用することができる。暗号通信で鍵の生成時のように、新旧２つの暗号アルゴリズムを並列的に動作させる必要はない。

【０１６１】

上記変換アルゴリズムの動作は、変換処理、あるいは、逆変換処理の何れかを指すことはいうまでも無い。圧縮アルゴリズムの場合、送信時には圧縮処理を行い、受信時には圧縮解除処理を行う。暗号アルゴリズムの場合、送信時には暗号化処理を行い、受信時には

暗号化に対する復号化処理を行う。映像音声の符号化アルゴリズムの場合、送信時には符号化処理を行い、受信時には符号化に対する復号化処理を行う。

【０１６２】

上記、処理負荷情報、各電力、通信可能時間などの算出式は一例である。ＣＰＵや専用ＬＳＩの消費電力特性に合わせて、他の処理負荷情報や算出式を用いても良い。また、既に述べたように、算出式には、１０％～３０％程度の余裕が得られるようにすることが好ましい。処理負荷情報の値を近似値とし、上記余裕を持たせるようにしても良い。

【０１６３】

上記各処理負荷情報は、通信アプリケーション、通信処理部、モジュール管理部から得られ、リソース選択部が参照するように説明したが、情報の記憶場所は、上記に限定されない。

【０１６４】

上記説明では、ネゴシエーションにより、モジュールや暗号アルゴリズムを自動的に決定するようにしたが、候補の暗号アルゴリズムや、候補モジュール・暗号アルゴリズム対を表示部７０に表示して、使用者が、人為的に、候補から絞り込んだり、選択したりしてもよい。

【０１６５】

上記ネゴシエーションの結果、通信可能時間Ｔ（秒）が、通信予定時間Ｔｓ（秒）を上回る暗号アルゴリズムがない場合は、表示部７０にその旨を表示し、利用者に対策を促すようにしても良い。対策としては、緊急でないアプリケーションの実行を停止する、ＡＣ電源に接続できるようにする、などが考えられる。

【産業上の利用可能性】

【０１６６】

本発明にかかるデータ通信方式およびデータ通信装置は、ポータブル機器の電池を有効利用しながら所期の通信時間と安全な通信環境を提供するという効果を有し、ポータブル機器における暗号通信方法等として有用である。

【０１６７】

本発明にかかるデータ通信方式およびデータ通信装置は、ポータブル機器の電池を有効利用しながら所期の通信時間と適切なデータ変換方法を提供するという効果を有し、ポータブル機器におけるＡＶデータ通信方法等の用途にも適用できる。

【０１６８】

本発明にかかる変換選択方式および変換選択装置は、ポータブル機器の電池を有効利用しながら所期の変換時間と適切なデータ変換方法を提供するという効果を有し、ポータブル機器におけるＡＶデータ通信方法等の用途にも適用できる。

【図面の簡単な説明】

【０１６９】

【図１】本発明によるデータ通信装置の１例の構成図
【図２】暗号アルゴリズムの処理時間の図
【図３】電池電圧と残容量の関係図
【図４】負荷による電池残容量の変化を示す経過予測図
【図５】負荷の切り替えによる電池残容量の変化を示す経過予測図
【図６】本発明によるデータ通信装置の別の例の構成図
【図７】電源モードの切り替え前後の負荷の状況を示す図
【図８】本発明によるデータ通信装置の更に別の例の構成図
【図９】本発明によるデータ通信方法の処理手順のフローチャート
【図１０】本発明による変換選択装置の１例の構成図
【図１１】本発明による変換選択方法の処理手順のフローチャート

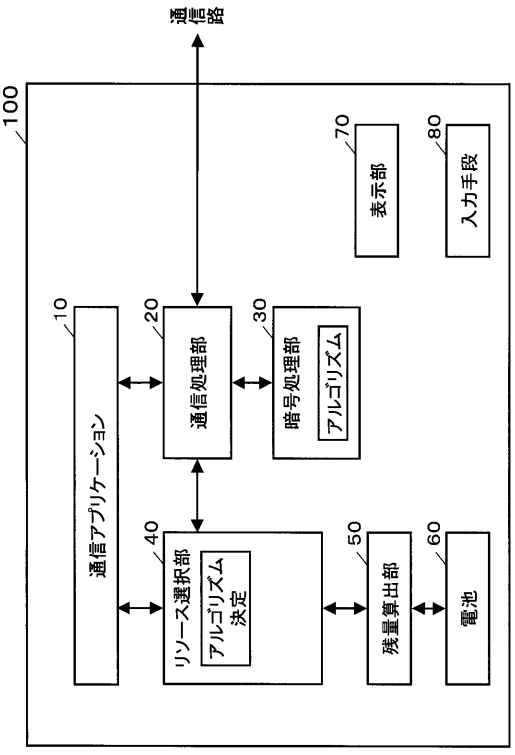
【符号の説明】

【０１７０】

１０　通信アプリケーション

１０ｂ　　アプリケーション
２０　　通信処理部
３０，３０ａ　　暗号処理部
３０ｂ　　変換処理部
４０，４０ａ，４０ｂ　　リソース選択部
５０　　残量算出部
６０　　電池
７０　　表示部
８０　　入力手段
９０，９０ａ，９０ｂ　　モジュール管理部
１００，１００ａ，１００ｂ　　ポータブル機器
１１０　　電源検知部
１２０　　ＣＰＵクロック

【図１】



【図２】

(a) アルゴリズムと処理時間、鍵長

アルゴリズム	処理時間	鍵長(ビット)
DES	1ミリ秒	56
3DES	3ミリ秒	168
MD5	0.5ミリ秒	128
SHA1	1ミリ秒	160

1280バイト長データ一列に対する処理時間
(CPU処理能力:約100MIPSの場合)

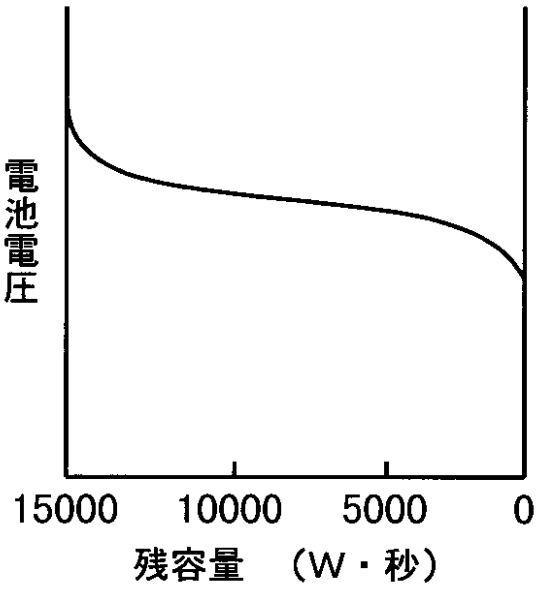
(b) 鍵長と処理時間

鍵長(ビット)	ラウンド数
128	11
192	13
256	15

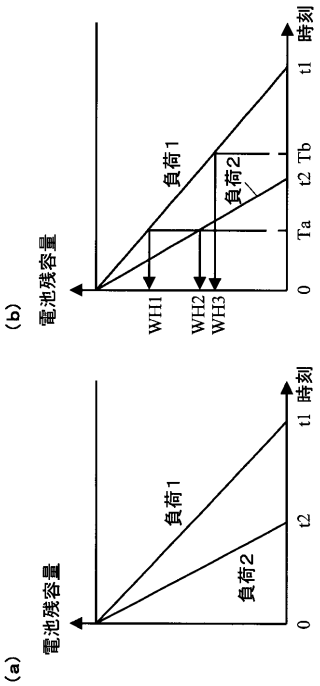
AESの鍵長とラウンド数
(ラウンド数:繰り返し処理回数)

『情報処理論文誌 VOL44 NO5 pp1321～
共通鍵暗号AESの低消費電力論理回路構成法』より

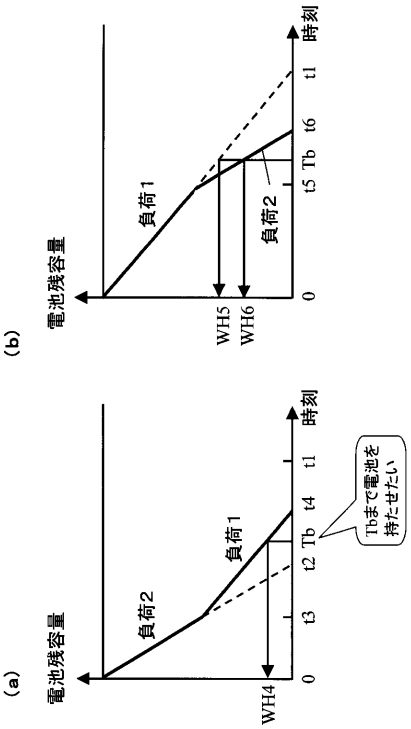
【図３】


電池電圧
15000
10000
5000
0
残容量 （W・秒）

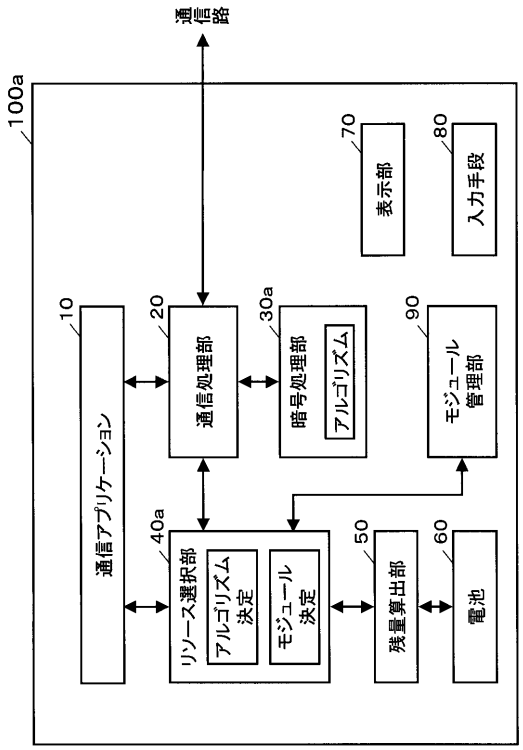
【図４】


(b)
電池残容量
負荷1
負荷2
WH1
WH2
WH3
0
Ta
t2 Tb
t1 時刻
(a)
電池残容量
負荷1
負荷2
0
t2
t1 時刻

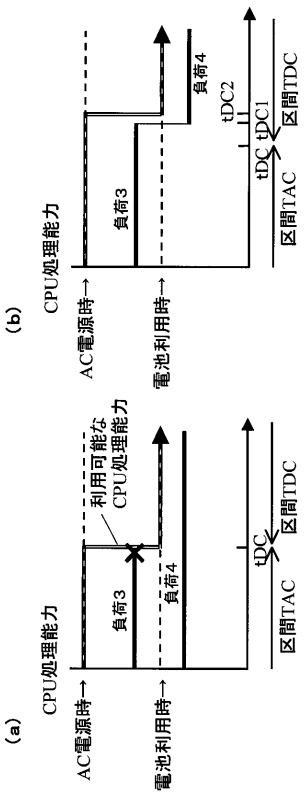
【図５】


(b)
電池残容量
負荷1
負荷2
WH5
WH6
0
t5 Tb t6
t1 時刻
(a)
電池残容量
負荷2
負荷1
WH4
0
t3
t2 Tb
t4
t1 時刻
Tbまで電池を持たせたい

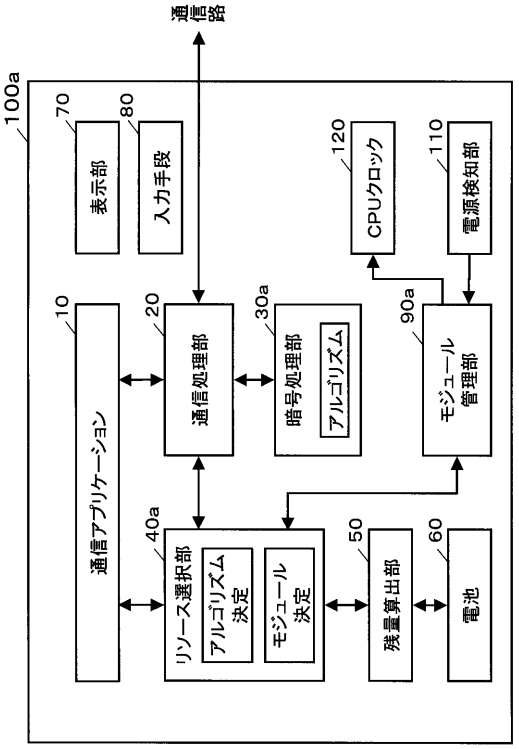
【図６】


通信路
100a
10
通信アプリケーション
20
通信処理部
30a
暗号処理部
アルゴリズム
40a
リソース選択部
アルゴリズム決定
モジュール決定
50
残量算出部
60
電池
70
表示部
80
入力手段
90
モジュール管理部

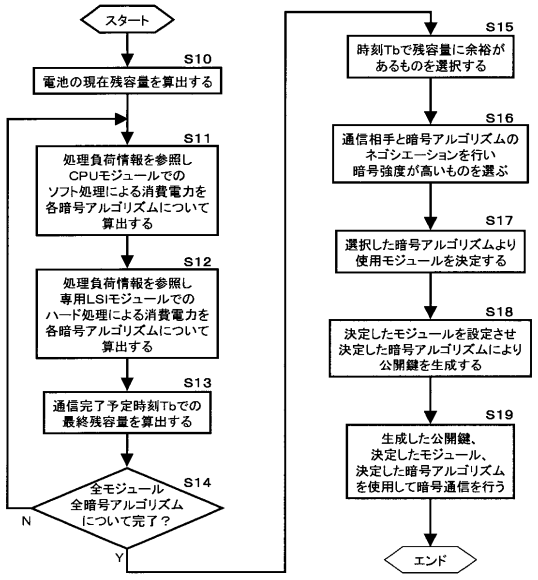
【図７】


(b)
CPU処理能力
AC電源時→
負荷3
負荷4
tDC2
tDC1
tDC
区間TAC
区間TDC
電池利用時→
(a)
CPU処理能力
利用可能なCPU処理能力
AC電源時→
負荷3
負荷4
tDC
区間TAC
区間TDC
電池利用時→

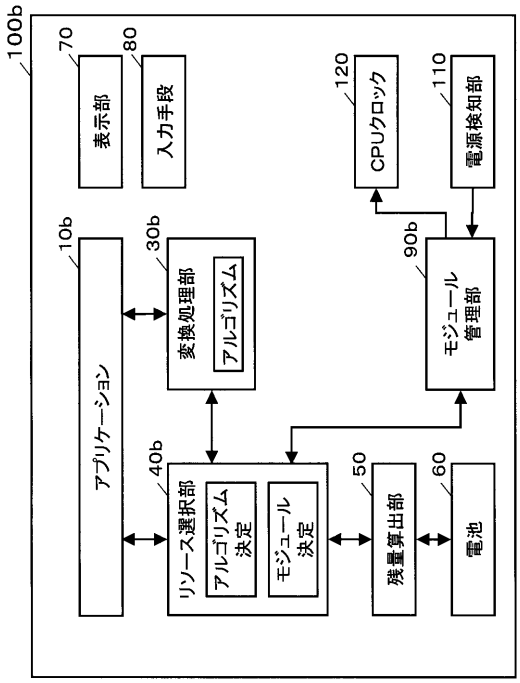
【図８】


通信路
100a
70
表示部
80
入力手段
120
CPUクロック
110
電源検知部
10
通信アプリケーション
20
通信処理部
30a
暗号処理部
アルゴリズム
90a
モジュール管理部
40a
リソース選択部
アルゴリズム決定
モジュール決定
50
残量算出部
60
電池

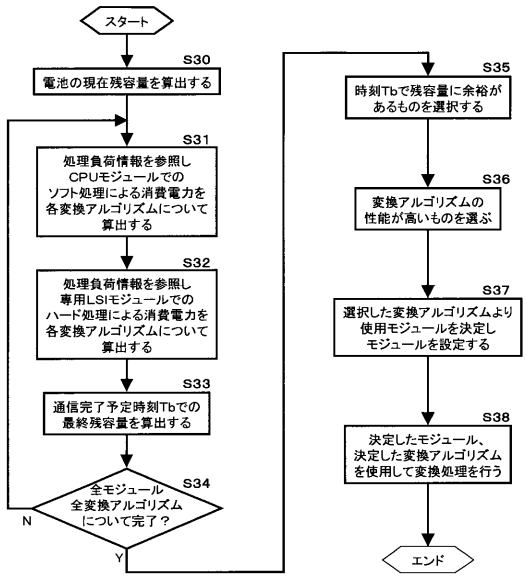
【図９】


スタート
S10
電池の現在残容量を算出する
S11
処理負荷情報を参照し
CPUモジュールでの
ソフト処理による消費電力を
各暗号アルゴリズムについて
算出する
S12
処理負荷情報を参照し
専用LSIモジュールでの
ハード処理による消費電力を
各暗号アルゴリズムについて
算出する
S13
通信完了予定時刻Tbでの
最終残容量を算出する
S14
全モジュール
全暗号アルゴリズム
について完了？
N
Y
S15
時刻Tbで残容量に余裕が
あるものを選択する
S16
通信相手と暗号アルゴリズムの
ネゴシエーションを行い
暗号強度が高いものを選ぶ
S17
選択した暗号アルゴリズムより
使用モジュールを決定する
S18
決定したモジュールを設定させ
決定した暗号アルゴリズムにより
公開鍵を生成する
S19
生成した公開鍵、
決定したモジュール、
決定した暗号アルゴリズム
を使用して暗号通信を行う
エンド

【図１０】


100b
70
表示部
80
入力手段
120
CPUクロック
110
電源検知部
10b
アプリケーション
30b
変換処理部
アルゴリズム
90b
モジュール管理部
40b
リソース選択部
アルゴリズム決定
モジュール決定
50
残量算出部
60
電池

【図１１】


スタート
S30
電池の現在残容量を算出する
S31
処理負荷情報を参照し
CPUモジュールでの
ソフト処理による消費電力を
各変換アルゴリズムについて
算出する
S32
処理負荷情報を参照し
専用LSIモジュールでの
ハード処理による消費電力を
各変換アルゴリズムについて
算出する
S33
通信完了予定時刻Tbでの
最終残容量を算出する
S34
全モジュール
全変換アルゴリズム
について完了？
N
Y
S35
時刻Tbで残容量に余裕が
あるものを選択する
S36
変換アルゴリズムの
性能が高いものを選ぶ
S37
選択した変換アルゴリズムより
使用モジュールを決定し
モジュールを設定する
S38
決定したモジュール、
決定した変換アルゴリズム
を使用して変換処理を行う
エンド