(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4689539号
(P4689539)
(45)発行日　平成23年5月25日(2011.5.25)　(24)登録日　平成23年2月25日(2011.2.25)

(51)Int.Cl.　F I
G06F 7/58 (2006.01)　G06F 7/58 A
G09C 1/00 (2006.01)　G09C 1/00 650B

請求項の数 8　(全 10 頁)

(21)出願番号　特願2006-153985(P2006-153985)
(22)出願日　平成18年6月1日(2006.6.1)
(65)公開番号　特開2007-323442(P2007-323442A)
(43)公開日　平成19年12月13日(2007.12.13)
審査請求日　平成21年3月5日(2009.3.5)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　石川　学
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

最終頁に続く

(54)【発明の名称】データ処理装置およびその方法

(57)【特許請求の範囲】
【請求項１】
任意のデータに任意の処理を施すデータ処理手段と、
前記データ処理手段からデータを取得し、前記取得したデータから乱数生成用のシードを生成するシード生成手段と、
前記データ処理手段の動作状態情報を取得し、前記動作状態情報に基づき前記シード生成手段によるシード生成を制御する制御手段とを有し、
前記制御手段は前記動作状態情報に基づき前記データ処理手段が出力するデータの重みを決定し、前記シード生成手段は前記重みに応じて前記データ処理手段のデータを取得することを特徴とするデータ処理装置。
【請求項２】
さらに、前記シード生成手段が生成したシードから乱数を生成する乱数生成手段を有することを特徴とする請求項1に記載されたデータ処理装置。
【請求項３】
前記制御手段は、前記動作状態情報として前記データ処理手段の活性化率を示す情報を取得することを特徴とする請求項1または請求項2に記載されたデータ処理装置。
【請求項４】
前記制御手段は、活性化を示す前記データ処理手段が存在しない場合、前記シード生成手段を制御して、前回生成したシードをフィードバックさせることを特徴とする請求項3に記載されたデータ処理装置。

【請求項５】
前記データ処理手段として、画像データを符号化する手段、データを暗号化する手段、カメラを制御する手段の少なくとも一つを含むことを特徴とする請求項1から請求項4の何れかに記載されたデータ処理装置。
【請求項６】
任意のデータに任意の処理を施すデータ処理手段を有するデータ処理装置のデータ処理方法であって、
前記データ処理手段からデータを取得し、前記取得したデータから乱数生成用のシードを生成する生成ステップと、
前記データ処理手段の動作状態情報を取得して、前記動作状態情報に基づき前記シード生成を制御する制御ステップとを有し、
前記制御ステップは前記動作状態情報に基づき前記データ処理手段が出力するデータの重みを決定し、前記生成ステップは前記重みに応じて前記データ処理手段のデータを取得することを特徴とするデータ処理方法。
【請求項７】
情報処理装置を制御して、請求項6に記載されたデータ処理を実現することを特徴とするコンピュータプログラム。
【請求項８】
請求項7に記載されたコンピュータプログラムが記録されたことを特徴とするコンピュータが読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、乱数生成用のシードを生成するデータ処理に関する。
【背景技術】
【０００２】
インターネットの普及に伴い、様々なデータがネットワークを経由してやり取りされている。そのため、データ通信のセキュリティに対する関心が高まり、暗号処理技術が一般に知られるようになった。
【０００３】
共通鍵暗号を用いたり、共通鍵を共有するために公開鍵暗号を用いたデータ通信が行われている。鍵の生成には、乱数が用いられ、乱数生成技術は不可欠である。
【０００４】
乱数は、シミュレーションやゲームなど応用範囲が広いが、近年はセキュリティの目的で乱数を使用する機会が増えた。具体的には、暗号化に使用する鍵の生成、認証用メッセージの生成などに乱数が利用される。従って、外部から推測することができない安全な乱数（「高品質の乱数」と呼ぶ場合がある）を高速に生成して、安全な鍵を生成する必要がある。もし、乱数に規則性、周期性が存在する場合、その性質を利用して、攻撃者に乱数を推定される危惧がある。従って、乱数のシードには、偶然性、予測不可能性、非再現性が必要である。
【０００５】
乱数の生成方法として、自然界の物理現象に基づき乱数を生成する物理乱数生成方式と、所定のアルゴリズムを用いる数学的な演算により乱数を生成する擬似乱数生成方式が存在する。
【０００６】
物理乱数生成方式は、熱雑音や発振回路を利用する方式、あるいは、通信パケットの遅延時間の揺らぎやハードディスクのシークタイムの揺らぎなどを利用する方式などがある。このようにして生成された乱数は、数学的に真性乱数に近い乱数になる。しかし、この物理乱数生成方式は、特別な回路など専用の部品・機構を必要とし、一般に、回路規模の大型化を招く。また、実用化の実績が乏しい。

【０００７】
一方、擬似乱数生成方式は、ある長さのシード（種）を基に、所定のアルゴリズムに基づく演算によって乱数を生成する。擬似乱数生成方式による生成物の非再現性を高めるには、主に質の高い攪拌関数を用いるのが一般的である。攪拌関数としてはハッシュ関数や共通鍵暗号などがある。また、シードを取得する方法として、時刻やシリアル番号などを利用する方式、外部イベントとしてのキーボード入力またはマウス操作を利用する方式、あるいは、移動端末の固有の情報を利用する方式（特許文献1参照）などが知られている。

【０００８】
しかし、擬似乱数生成方式において乱数を生成する演算は周知のアルゴリズムを利用するから、シードと攪拌関数を知った第三者は生成された乱数を再現することが可能である。また、シードの質が低いと生成した乱数には一様性（規則性）が出現し、予測が可能で、再現性もあり、偶然性に乏しい。このため、使用した乱数が推測される危惧があり、安全性に問題がある。つまり、擬似乱数生成方式の乱雑性はシードの乱雑性に大きく影響を受けるため、シードが予測できてはいけない。そこで、システムで得られる変動要素をシードに加味するのがよいとされる。また、一般に、シードのビット量が多いほど質の高い乱数ができると言われている。

【０００９】
上述したシリアル番号を用いる方式はシードの推測が容易である。また、外部イベントを利用する方式は人的操作が頻繁に必要である。また、特許文献1の方式において変動する可能性が高いのは通信内容のみであるが、その内容には偏りがあると考えられる。言い替えれば、特許文献1の方式は変動要素が少なく、ハッシュが必須である。

【００１０】
【特許文献１】特開2002-215030公報
【発明の開示】
【発明が解決しようとする課題】
【００１１】
本発明は、エントロピが高いシード生成を目的とする。
【課題を解決するための手段】
【００１２】
本発明は、前記の目的を達成する一手段として、以下の構成を備える。

【００１３】
本発明にかかるデータ処理装置は、任意のデータに任意の処理を施すデータ処理手段と、前記データ処理手段からデータを取得し、前記取得したデータから乱数生成用のシードを生成するシード生成手段と、前記データ処理手段の動作状態情報を取得し、前記動作状態情報に基づき前記シード生成手段によるシード生成を制御する制御手段とを有し、前記制御手段は前記動作状態情報に基づき前記データ処理手段が出力するデータの重みを決定し、前記シード生成手段は前記重みに応じて前記データ処理手段のデータを取得することを特徴とする。

【００１４】
本発明にかかるデータ処理装置は、任意のデータに任意の処理を施すデータ処理手段を有するデータ処理装置のデータ処理方法であって、前記データ処理手段からデータを取得し、前記取得したデータから乱数生成用のシードを生成する生成ステップと、前記データ処理手段の動作状態情報を取得して、前記動作状態情報に基づき前記シード生成を制御する制御ステップとを有し、前記制御ステップは前記動作状態情報に基づき前記データ処理手段が出力するデータの重みを決定し、前記生成ステップは前記重みに応じて前記データ処理手段のデータを取得することを特徴とする。

【発明の効果】
【００１５】
本発明によれば、エントロピが高いシード生成を実現することができる。そのため、乱

雑な値のシードを生成して、良質な乱数を生成することができる。
【発明を実施するための最良の形態】
【００１６】
以下、本発明にかかる実施例の情報処理を図面を参照して詳細に説明する。
【実施例１】
【００１７】
［装置の構成］
図1は実施例のデータ処理装置100の構成例を示すブロック図である。
【００１８】
マイクロプロセッサ111は、例えばワンチップマイクロコントローラで、内蔵RAM をワークエリアとして、内蔵ROMなどに格納されたプログラムを実行し、システムバス109を介して後述する各構成を制御する。
【００１９】
データ処理モジュール105としては、データの暗号化モジュール、認証用メッセージの生成モジュールなど、データ処理装置100のデータ処理に必要なモジュールが搭載される。
【００２０】
乱数生成モジュール101は、制御部102、シード収集・加工部103および乱数系列生成部104を備え、本実施例における乱数生成処理を実行する。データ処理モジュール105と乱数生成モジュール101との間は、専用の信号線またはシステムバス109を利用して通信を行えばよい。
【００２１】
外部インタフェイス106は、例えばネットワークやUSBなどのシリアルバスを介して、データ処理装置100に外部装置107を接続するインタフェイスを提供する。なお、外部装置107としては暗号化や認証対象のデータを格納するストレージや、暗号化や認証処理を行うデータ処理装置が好適である。
【００２２】
なお、乱数生成モジュール101が生成した乱数は、データ処理モジュール105の暗号化や認証に利用される。ただし、乱数生成モジュール101にデータを供給するデータ処理モジュール105は、乱数を利用するものに限られるわけではなく、任意のデータ処理モジュールを利用することができる。また、データ処理モジュール105は複数存在することが好ましいが、一つだけでもよい。
【００２３】
［乱数生成モジュールの構成］
図2A、図2Bは乱数生成モジュール101の詳細な構成例を示すブロック図である。
【００２４】
図2Aは乱数系列生成部104が乱数生成部205のみをもつ構成を示し、シード収集・加工部103の出力は、乱数生成部205の入力であり、擬似乱数生成に必要なシードである。一方、図2Bは乱数系列生成部104が乱数生成部205、ランダムプール206および攪拌部207を備える構成を示す。この構成において、シード収集・加工部103の出力は、攪拌部207の入力であり、ランダムプール206を攪拌する素である。なお、シード収集・加工部103の出力からシード収集・加工部103の入力に戻る信号線は後述するフィードバック用の信号線である。
【００２５】
●シード収集・加工部
図3はシード収集・加工部103の構成例を示すブロック図である。
【００２６】
データ収集部301は、詳細は後述するが、データ処理モジュール105が出力するデータそれぞれを制御部102が出力する重み係数ω1～ωnに応じて重み付けする。データ合成部303は、重み付けされたデータを所定の方法で合成し、合成したデータをシードとしてを乱数系列生成部104に出力する。

【００２７】
データ合成部303のデータの合成方法には加算、排他的論理和、連結などを用いることができる。
【００２８】
●制御部の動作
図4は制御部102の動作を説明するフローチャートである。
【００２９】
制御部102は、シード収集・加工部103の実行要求イベントの発生を待つ(S100)。シード収集・加工部103が乱数系列生成部104から攪拌要求やシード要求を受信した場合、制御部102がデータ処理モジュール105や外部インタフェイス106から活性化を示す動作状況通知信号を受信した場合に、実行要求イベントが発生する。また、乱数系列生成部104がランダムプール206をもつ構成（図2B）の場合は、ランダムプール206内に残存するデータが少なくなった場合やランダムプール206が長時間放置された場合にも発生する。
【００３０】
実行要求イベントが発生すると、制御部102は、シード収集・加工部103に接続されたデータ処理モジュール105の活性化率を調査する(S101)。活性化率の調査は、例えば、定期的または不定期に、データ処理モジュール105ごとに、出力データをサンプリングし、サンプリングデータを微分することでデータの変化を検知すればよい。あるいは、データ処理モジュール105から活性化を示す信号を入力することで活性化率を調査する仕組みでもよい。
【００３１】
次に、制御部102は、活性化率の調査結果に基づき、活性化したデータ処理モジュール105（以下「活性化モジュール」と呼ぶ）が存在するか否かを判定する(S102)。活性化モジュールが存在しない場合は、シード収集・加工部103に前回のシードの値をフィードバックさせるか、乱数系列生成部104にランダムプール206の攪拌を指示することで、活性化モジュールが存在しない状態を回避する(S105)。そして、処理をステップS100に戻す。
【００３２】
一方、活性化モジュールが存在する場合、制御部102は、活性化率の調査結果に基づき、データ処理モジュール105それぞれに対する重み係数ωｉ（i=1-n)を決定する。さらに、データ処理モジュール105の動作状況通知信号108を取得し、所定の操作によりランク付けした動作状況通知信号108を制御パラメータとしてシード収集・加工部103へ出力する(S103)。なお、制御パラメータには、例えば動作状況通知信号108によって通知される活性化率やエントロピなどの指標を用いていもよい。
【００３３】
次に、制御部102は、シード収集・加工部103にデータの取得および合成、つまりシードの生成を指示し(S104)、処理をステップS100に戻す。この指示に従いシード収集・加工部103は、データ処理モジュール105から出力され、重み付したデータを所定の方法により合成して乱数系列生成部104に出力する。
【００３４】
［重み付け方法］
シード収集・加工部103は、制御部102から指示される重み係数ωiに応じて、各データ処理モジュール105に対するデータの取得回数を動的に変更することで、データの重み付けを実現する。なお、データの取得回数を動的変更の代わりに、データの取得時間の比率を動的に変更する、または、データの取得ビット数を動的に切り替えるなどでもよい。
【００３５】
図5A、図5B、図5Cは実行要求イベントの発生時に活性化率を用いてデータ取得回数を動的に変更する方法を説明する図である。なお、図5Cに示すように、データ処理モジュール105としてモジュールA、B、Cの三つのモジュールが存在するとする。また、図5Aは横軸に時間、縦軸に各モジュールの活性化率を表現する図、図5Bは重み係数の実現例を説明する図である。

【００３６】
図5Aに示すように、時間t1で実行要求イベント1が発生した際のモジュールA、B、Cの活性化率は符号311、321、331で示される。これら活性化率の比率を100%積み上げ棒グラフで表すと図5Bのようになる。そして、この比率に基づき重み係数ωiを決定すると、実行要求イベント1の発生時のモジュールA、B、Cの重み係数ω1～3はそれぞれ8、33、58になる。例えば60バイトのデータを取得すると仮定すると、モジュールAからは8/99×60=5回、モジュールBからは33/99×60=20回、モジュールCからは58/99×60=35回を取得することになる。つまり、モジュールA、B、Cからそれぞれ5、20、35バイトを取得する。
【００３７】
実行要求イベント2～4においても、上記と同様に活性化率の比率に応じてデータを取得する。従って、データ処理モジュール105の活性化率に応じてデータの取得が動的に変更され、取得したデータに基づき生成するシードの値をより乱雑にすることができる。その結果、乱数系列生成部104は、乱雑な値のシードに基づき、高品質な乱数を生成することができる。
【００３８】
なお、データ処理モジュール105が一つの場合、あるいは、複数のデータ処理モジュール105のうち一つの活性化率が極めて高い場合は、データの取得回数等を動的に変更することができない。このような場合は、制御部102において実在しないデータ処理モジュールに対応する例えば所定周期の変動をもつ擬似活性化率信号を生成し、データ処理モジュール105の活性化率信号と擬似活性化率信号により重み係数ωiを決定すればよい。
【実施例２】
【００３９】
以下、本発明にかかる実施例2の情報処理を説明する。なお、実施例2において、実施例1と略同様の構成については、同一符号を付して、その詳細説明を省略する。
【００４０】
図6は実施例2のデータ処理装置100の構成例を示すブロック図である。
【００４１】
データ処理装置100は、データ処理モジュール105としてカメラ制御モジュール501、画像符号化モジュール502、暗号化モジュール503、メッセージダイジェスト(MD)生成モジュール504、その他データ処理モジュール505を有する。また、外部インタフェイス106としてストレージ510を接続するためのストレージインタフェイス509、ネットワークインタフェイス511を有する。
【００４２】
画像符号化モジュール504が出力する符号データは、エントロピが高いことが知られている。ただし、ネットワークインタフェイス511を介して外部へ転送される符号データをシードの生成に用いれば、第三者に鍵を推測する手掛かりを与える可能性があり、好ましくない。一方、外部へ転送されない符号データは、符号化の性質上エントロピが高いためシードの生成に最適である。そこで、画像符号化モジュール504の符号化結果をシード生成用のデータに利用する。
【００４３】
画像符号化モジュール504に入力される符号化前の画像データのLSBは量子化によって消失する。そのため、第三者が符号化データを入手したとしても画像データのLSBを推測することはできない。従って、乱数生成モジュール101は、符号化前の画像データのLSBをシード生成用のデータとして取得する。
【００４４】
また、カメラ制御モジュール501が出力する設定データは、パン、チルト、ズームが指示された場合、撮像画像に急激な変化が起きる。そこで、カメラ制御モジュール501が出力する設定データも積極的にシードの生成に利用する。
【００４５】
［他の実施例］

なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。

【００４６】

また、本発明の目的は、上記実施例の機能を実現するソフトウェアを記録した記憶媒体（記録媒体）をシステムまたは装置に供給し、そのシステムまたは装置のコンピュータ（CPUやMPU）が前記ソフトウェアを実行することでも達成される。この場合、記憶媒体から読み出されたソフトウェア自体が上記実施例の機能を実現することになり、そのソフトウェアを記憶した記憶媒体は本発明を構成する。

【００４７】

また、前記ソフトウェアの実行により上記機能が実現されるだけでなく、そのソフトウェアの指示により、コンピュータ上で稼働するオペレーティングシステム(OS)などが実際の処理の一部または全部を行い、それによって上記機能が実現される場合も含む。

【００４８】

また、前記ソフトウェアがコンピュータに接続された機能拡張カードやユニットのメモリに書き込まれ、そのソフトウェアの指示により、前記カードやユニットのCPUなどが実際の処理の一部または全部を行い、それによって上記機能が実現される場合も含む。

【００４９】

本発明を前記記憶媒体に適用する場合、その記憶媒体には、先に説明したフローチャートに対応するソフトウェアが格納される。

【図面の簡単な説明】

【００５０】

【図１】実施例のデータ処理装置の構成例を示すブロック図、

【図２Ａ】乱数生成モジュールの詳細な構成例を示すブロック図、

【図２Ｂ】乱数生成モジュールの詳細な構成例を示すブロック図、

【図３】シード収集・加工部の構成例を示すブロック図、

【図４】制御部の動作を説明するフローチャート、

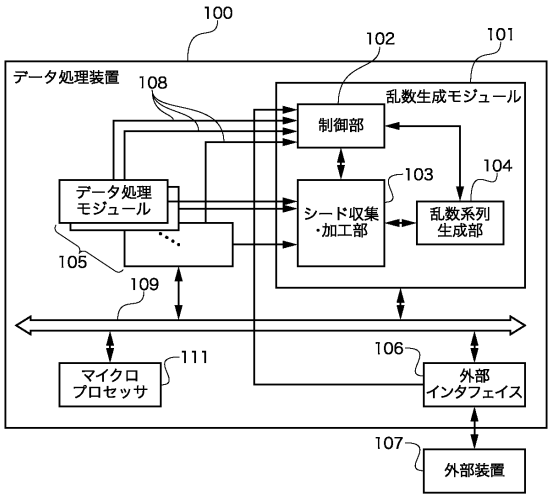
【図５Ａ】実行要求イベントの発生時に活性化率を用いてデータ取得回数を動的に変更する方法を説明する図、

【図５Ｂ】実行要求イベントの発生時に活性化率を用いてデータ取得回数を動的に変更する方法を説明する図、

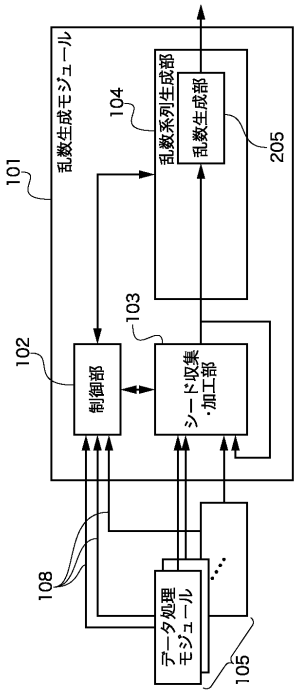
【図５Ｃ】実行要求イベントの発生時に活性化率を用いてデータ取得回数を動的に変更する方法を説明する図、

【図６】実施例2のデータ処理装置の構成例を示すブロック図である。

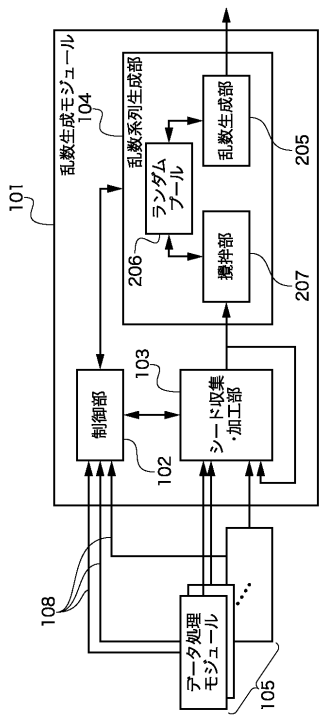
【図１】


100
102
101
データ処理装置
108
乱数生成モジュール
制御部
103
104
データ処理
モジュール
シード収集
・加工部
乱数系列
生成部
105
109
111
106
マイクロ
プロセッサ
外部
インタフェイス
107
外部装置

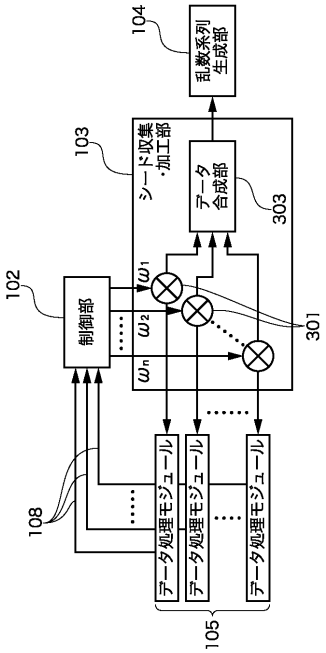
【図２Ａ】


乱数生成モジュール
101
104
乱数系列生成部
乱数生成部
205
103
102
制御部
シード収集
・加工部
108
データ処理
モジュール
105

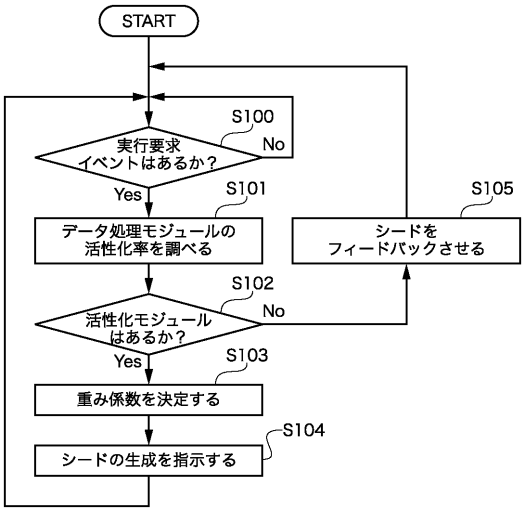
【図２Ｂ】


乱数生成モジュール
101
104
乱数系列生成部
乱数生成部
205
ランダム
プール
206
攪拌部
207
103
制御部
シード収集
・加工部
102
108
データ処理
モジュール
105

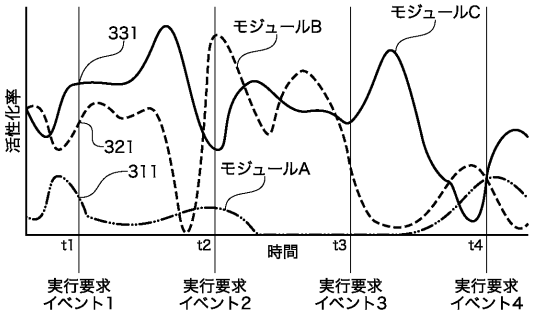
【図３】


104
乱数系列
生成部
103
シード収集
・加工部
データ
合成部
303
102
制御部
ω_1
ω_2
ω_n
301
108
データ処理モジュール
データ処理モジュール
データ処理モジュール
105

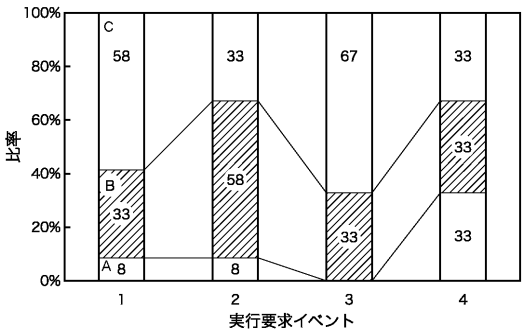
【図４】



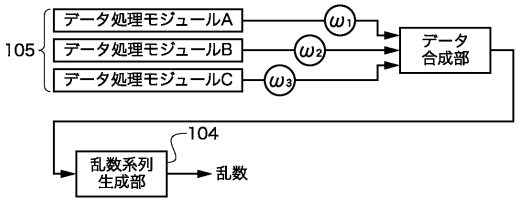
【図５Ａ】



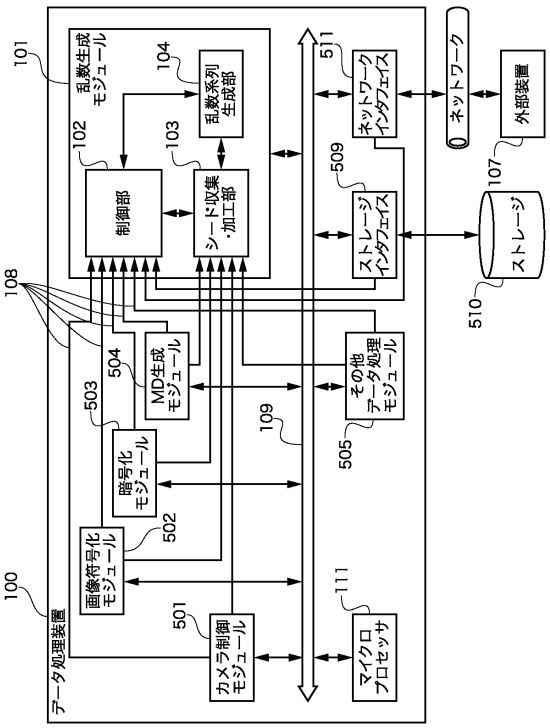
【図５Ｂ】



【図５Ｃ】



【図６】



フロントページの続き

審査官　田中　友章

(56)参考文献　特開２００２－２６８８７４（ＪＰ，Ａ）
特開２０００－２４２４７０（ＪＰ，Ａ）
特開２００５－０１１３５６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　７／５８
Ｇ０９Ｃ　　１／００