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

特許第6265783号
(P6265783)

(45)発行日　平成30年1月24日(2018.1.24)　(24)登録日　平成30年1月5日(2018.1.5)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601A
G09C	1/00	(2006.01)	G09C	1/00	660D
G06F	21/62	(2013.01)	G06F	21/62	336
G06F	21/12	(2013.01)	G06F	21/12	360

請求項の数 14　(全 15 頁)

(21)出願番号　特願2014-43834(P2014-43834)
(22)出願日　平成26年3月6日(2014.3.6)
(65)公開番号　特開2015-170952(P2015-170952A)
(43)公開日　平成27年9月28日(2015.9.28)
審査請求日　平成29年3月1日(2017.3.1)

(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　100125254
弁理士　別役　重尚
(72)発明者　松本　昭浩
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

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】暗号化／復号化システム及びその制御方法、並びにプログラム

(57)【特許請求の範囲】

【請求項１】

ホスト装置との間でデータを送受信する暗号化／復号化システムであって、

前記ホスト装置との間で送受信されるデータに対して暗号化処理又は復号化処理を行うためのプログラムを暗号化した状態で格納する格納手段と、

前記格納されたプログラムを復号化するための鍵を前記暗号化／復号化システムの起動に応じて生成する鍵生成手段と、

所定の方法で前記暗号化／復号化システムを起動する要求があった場合には、前記鍵生成手段によって生成された鍵を用いて前記格納されたプログラムを復号化して所定の通信インタフェースに対して出力し、前記所定の方法とは別の方法で前記暗号化／復号化システムを起動する要求があった場合には、前記格納されたプログラムを復号化したプログラムの前記所定の通信インタフェースに対する出力を行わない出力手段とを備えることを特徴とする暗号化／復号化システム。

【請求項２】

少なくとも１つのレジスタ値によって構成される第１のレジスタと、

少なくとも１つのレジスタ値によって構成される第２のレジスタと、

前記第１のレジスタを構成する少なくとも１つのレジスタ値から少なくとも１つの第１のレジスタ値を選択すると共に前記第２のレジスタを構成する少なくとも１つのレジスタ値から少なくとも１つの第２のレジスタ値とを選択する選択手段と、

前記選択された第１のレジスタ値と前記選択された第２のレジスタ値の組み合わせによ

って構成される情報値を生成する情報値生成手段とを更に備え、
前記鍵生成手段は、前記情報値生成手段によって生成された情報値に基づいて前記鍵を生成することを特徴とする請求項１に記載の暗号化／復号化システム。
【請求項３】
前記情報値に他の情報値を結合する結合手段を更に備えることを特徴とする請求項２記載の暗号化／復号化システム。
【請求項４】
前記他の情報値は平文で構成されていることを特徴とする請求項３記載の暗号化／復号化システム。
【請求項５】
前記情報値生成手段は、前記暗号化／復号化システムが起動してから第１の時間が経過した時及び第２の時間が経過した時に前記情報値を生成することを特徴とする請求項２乃至４のいずれか1項に記載の暗号化／復号化システム。
【請求項６】
前記鍵生成手段は、前記情報値生成手段によって前記第１の時間が経過した時及び前記第２の時間が経過した時に生成された２つの情報値を夫々疑似乱数化して演算処理を施す演算処理手段を更に備えることを特徴とする請求項５記載の暗号化／復号化システム。
【請求項７】
前記演算処理手段は前記２つの情報値に排他的論理和演算を施すことを特徴とする請求項６記載の暗号化／復号化システム。
【請求項８】
前記暗号化／復号化システムは２以上の起動方法を有し、
前記情報値は、前記暗号化／復号化システムの起動方法に応じて異なる値となることを特徴とする請求項２乃至７のいずれか１項に記載の暗号化／復号化システム。
【請求項９】
前記第１のレジスタのレジスタ値及び前記第２のレジスタのレジスタ値の少なくとも一方は時刻に応じて変化することを特徴とする請求項２乃至８のいずれか１項に記載の暗号化／復号化システム。
【請求項１０】
前記所定の方法で前記暗号化／復号化システムを起動する前記要求は、前記所定の通信インタフェースを介して送信され、前記所定の方法とは別の方法で前記暗号化／復号化システムを起動する前記要求は、前記所定の通信インタフェースとは別の通信インタフェースを介して送信されることを特徴とする請求項１乃至９のいずれか１項に記載の暗号化／復号化システム。
【請求項１１】
前記所定の方法とは別の方法で前記暗号化／復号化システムを起動する前記要求は、デバッグプログラムによって発行されることを特徴とする請求項１乃至１０のいずれか１項に記載の暗号化／復号化システム。
【請求項１２】
所定の値を記憶するレジスタをさらに備え、
前記所定の方法で前記暗号化／復号化システムを起動する前記要求があった場合のみ、前記レジスタに対して特定の値が記憶され、前記特定の値を用いて前記復号化処理が実行されることを特徴とする請求項１乃至１１のいずれか１項に記載の暗号化／復号化システム。
【請求項１３】
ホスト装置との間でデータを送受信する暗号化／復号化システムの制御方法であって、
前記ホスト装置との間で送受信されるデータに対して暗号化処理又は復号化処理を行うためのプログラムを暗号化した状態で格納する格納ステップと、
前記格納されたプログラムを復号化するための鍵を前記暗号化／復号化システムの起動に応じて生成する鍵生成ステップと、

所定の方法で前記暗号化／復号化システムを起動する要求があった場合には、前記鍵生成ステップで生成された鍵を用いて前記格納されたプログラムを復号化して所定の通信インタフェースに対して出力し、前記所定の方法とは別の方法で前記暗号化／復号化システムを起動する要求があった場合には、前記格納されたプログラムを復号化したプログラムの前記所定の通信インタフェースに対する出力を行わない出力ステップとを備えることを特徴とする暗号化／復号化システムの制御方法。

【請求項１４】

ホスト装置との間でデータを送受信する暗号化／復号化システムの制御方法をコンピュータに実行させるプログラムであって、

前記暗号化／復号化システムの制御方法は、

前記ホスト装置との間で送受信されるデータに対して暗号化処理又は復号化処理を行うためのプログラムを暗号化した状態で格納する格納ステップと、

前記格納されたプログラムを復号化するための鍵を前記暗号化／復号化システムの起動に応じて生成する鍵生成ステップと、

所定の方法で前記暗号化／復号化システムを起動する要求があった場合には、前記鍵生成ステップで生成された鍵を用いて前記格納されたプログラムを復号化して所定の通信インタフェースに対して出力し、前記所定の方法とは別の方法で前記暗号化／復号化システムを起動する要求があった場合には、前記格納されたプログラムを復号化したプログラムの前記所定の通信インタフェースに対する出力を行わない出力ステップとを備えることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、暗号化／復号化システム及びその制御方法、並びにプログラムに関する。

【背景技術】

【０００２】

従来の印刷装置はセキュリティを強化するために暗号化機能及び復号化機能を備える。暗号化機能は印刷装置が備えるＨＤＤのようなストレージデバイスに格納されているデータを暗号化し、復号化機能は暗号化されたデータを、いわゆる暗号鍵によって復号化する。

【０００３】

上記印刷装置は、日本やアメリカをはじめとする各国政府やセキュリティに対する意識が高い一般企業において、製品認証制度の１つとしての「暗号モジュール試験及び認証制度」に基づく第三者機関の認証を取得していることが求められ、具体的には、当該制度において定められているセキュリティレベルが２以上の認証を取得していることが求められる。

【０００４】

暗号化機能はＩＣチップによって提供されるが、暗号鍵のような秘密情報及び暗号化プログラム等を格納する不揮発性メモリダイと暗号化ロジックダイを１つのパッケージに封止したＳｉＰ（System in a Package）で提供することがセキュリティ上の堅牢性をより強固にする観点から望ましい。

【０００５】

一般的に、ＩＣチップはデータの入出力に使用される入出力ＩＦ、故障解析時に使用されるデバッグＩＦ、及びＩＣチップ内部の不揮発性メモリに暗号化プログラムを格納するときに使用されるメモリＩＦを有するが、ＩＣチップ内部の解析がデバッグＩＦやメモリＩＦを介して行われる場合がある。

【０００６】

暗号化機能がＩＣチップによって提供され、且つ「暗号モジュール試験及び認証制度」におけるセキュリティレベル２以上の認証を取得するためには、デバッグＩＦやメモリＩＦにアクセスされたとしてもＩＣチップに含まれる情報が解析されるのを防止する必要が

ある。この対策として不揮発性メモリに格納される秘密情報や暗号化プログラムの一部又は全部に暗号化を施す方法がある。

【０００７】

不揮発性メモリに格納される秘密情報や暗号化プログラムの暗号化は、例えば、共通鍵暗号方式の１つであるＡＥＳ（Advanced Encryption Standard）によって行われるが、第三者がデバッグＩＦやメモリＩＦを介して得られた情報から暗号化されている秘密情報や暗号化プログラムの暗号鍵が再現されることがある。そこで、秘密情報や暗号化プログラムの暗号鍵が第三者によって簡単に再現されることを防止するために、暗号化装置が有する暗号鍵生成部によって生成された暗号鍵とレジスタに平文で設定された初期入力値とを乱数生成回路に入力して得られる乱数を用いてデータに暗号化処理を行っている（例えば、特許文献１参照）。

【先行技術文献】

【特許文献】

【０００８】

【特許文献１】特開平１０－２２９９４号公報

【発明の概要】

【発明が解決しようとする課題】

【０００９】

しかしながら、レジスタに設定される初期入力値は平文で設定されるため、当該初期入力値が盗まれると暗号鍵が再現されてデータの暗号化が簡単に解除されてしまう。

【００１０】

本発明の目的は、データの暗号化が簡単に解除されるのを防止することができる暗号化／復号化システム及びその制御方法、並びにプログラムを提供することにある。

【課題を解決するための手段】

【００１１】

上記目的を達成するために、本発明の暗号化／復号化システムは、ホスト装置との間でデータを送受信する暗号化／復号化システムであって、前記ホスト装置との間で送受信されるデータに対して暗号化処理又は復号化処理を行うためのプログラムを暗号化した状態で格納する格納手段と、前記格納されたプログラムを復号化するための鍵を前記暗号化／復号化システムの起動に応じて生成する鍵生成手段と、所定の方法で前記暗号化／復号化システムを起動する要求があった場合には、前記鍵生成手段によって生成された鍵を用いて前記格納されたプログラムを復号化して所定の通信インタフェースに対して出力し、前記所定の方法とは別の方法で前記暗号化／復号化システムを起動する要求があった場合には、前記格納されたプログラムを復号化したプログラムの前記所定の通信インタフェースに対する出力を行わない出力手段とを備えることを特徴とする。

【発明の効果】

【００１２】

本発明によれば、データの暗号化が簡単に解除されるのを防止することができる。

【図面の簡単な説明】

【００１３】

【図１】本発明の実施の形態に係る暗号化処理装置を有する画像形成システムの構成を概略的に示すブロック図である。

【図２】図１における暗号化ＩＣの接続状態を示すブロック図である。

【図３】図２における暗号化ＩＣの内部構成を概略的に示すブロック図である。

【図４】図３のフラッシュメモリ及びＲＡＭに格納される主要なデータを示す図である。

【図５】図４における秘密情報用暗号鍵を生成する際に必要となる情報ａの生成方法について説明するのに用いられる図である。

【図６Ａ】図４における秘密情報用暗号鍵の生成に用いられるシード値を示す図である。

【図６Ｂ】図６Ａのシード値を用いて秘密情報用暗号鍵を生成する方法を説明するのに用いられる図である。

【図７】図６Ｂにおける時刻ｔ１に生成される情報ａとしてのＸ１のビット列である。
【図８】図４におけるデータ暗号化プログラム及び秘密情報を暗号化する暗号化処理の手順を示すフローチャートである。
【図９】図４における秘密情報暗号化プログラム及びデータ暗号化プログラムを実行するプログラム実行処理の手順を示すフローチャートである。
【発明を実施するための形態】
【００１４】
以下、本発明の実施の形態を図面を参照しながら詳述する。
【００１５】
図１は、本発明の実施の形態に係る暗号化処理装置を有する画像形成システムの構成を概略的に示すブロック図である。
【００１６】
図１の画像形成システムは、ホストコントローラ１０１及びホストコンピュータ９０７を備え、これらは、ネットワーク９０６を介して互いに接続されている。ホストコントローラ１０１は、ＣＰＵ９０１、メモリ制御部９０２、ＬＡＮ－ＩＦ部９０５、リーダＩＦ部９０８、ＦＡＸ－ＩＦ部９１０、画像処理部９１２、パネルＩＦ部９１３、ＨＤＤ－ＩＦ部９１５、及びビデオＩＦ部９１６を備え、これらはバス９１８を介して互いに接続されている。
【００１７】
また、ホストコントローラ１０１は、ＲＯＭ９０３及びＲＡＭ９０４を備え、これらはメモリ制御部９０２に接続されている。ホストコントローラ１０１のＬＡＮ－ＩＦ部９０５、リーダＩＦ部９０８、ＦＡＸ－ＩＦ部９１０、パネルＩＦ部９１３、ＨＤＤ－ＩＦ部９１５、及びビデオＩＦ部９１６には夫々ネットワーク９０６、スキャナ装置９０９、ＦＡＸ装置９１１、パネル装置９１４、暗号化ＩＣ１０２、及び印刷部９１７が接続され、ＦＡＸ装置９１１は公衆電話回線に接続されている。また、暗号化ＩＣ１０２にはＨＤＤ１０３が接続されている。
【００１８】
ホストコントローラ１０１は、例えば、ＭＦＰ（Multi-Function Printer）に備えられている。ＣＰＵ９０１はシステム制御や演算処理を行い、メモリ制御部９０２は各種メモリデバイスへの入出力制御やＤＭＡ（Direct Memory Access）制御を行う。
【００１９】
ＲＯＭ９０３は、起動プログラム、各種処理プログラム、及び制御パラメータ等を格納する。ＲＡＭ９０４はＤＤＲ（Double Data Rate）メモリに代表される書き換え専用メモリである。
【００２０】
画像処理部９１２は、ＬＡＮ－ＩＦ部９０５、リーダＩＦ部９０８、ＦＡＸ－ＩＦ部９１０を介して取得された画像データに対して各種画像処理を行う。スキャナ装置９０９は原稿を読み取って画像データに変換する。ＦＡＸ装置９１１は公衆電話回線９１９を介して通信制御及びデータ送受信処理を行う。パネル装置９１４はユーザインターフェイスであると共に液晶表示されるボタン等が操作される。この操作によってホストコントローラ１０１に接続されているスキャナ装置９０９等の各種設定が行われる。印刷部９１７は、印刷装置本体、給紙部、及び排紙部を備えるプリンタであって、主にビデオＩＦ部９１６からのコマンド情報に従って印刷データを紙面上に印刷する。
【００２１】
暗号化ＩＣ１０２は、暗号化ＩＣ１０２が有する後述のＳＡＴＡ－ＩＦ１０４等を介して送受信されるデータの暗号化処理又は復号化処理を行う。ＨＤＤ１０３は、不揮発性の大容量記憶装置であり、画像データや各種プログラムが格納されると共に、一時作業領域として使用されるデータ領域（図示せず）とＨＤＤ１０３のバージョン情報等が格納されているシステム領域（図示せず）を有する。
【００２２】

図２は、図１における暗号化ＩＣ１０２の接続状態を示すブロック図である。

【００２３】

図２において、暗号化ＩＣ１０２は、外部記憶装置と接続するためのＳＡＴＡ（Serial Advanced Technology Attachment）規格に準拠したＩＦであるＳＡＴＡ－ＩＦ１０４，１０５を介してホストコントローラ１０１及びＨＤＤ１０３と夫々接続されている。また、暗号化ＩＣ１０２は、デバッグＩＦ１０６及びフラッシュメモリＩＦ１０８を介してデバッガ１０７、フラッシュ治具１０９と夫々接続されている（暗号化／復号化システム）。デバッガ１０７はソフト開発時や故障時の検証用に使用される。フラッシュ治具１０９は、例えば、後述のフラッシュメモリ１１１を接続するための治具である。なお、デバッガ１０７及びフラッシュ治具１０９は暗号化ＩＣ１０２の通常起動時には使用されない。

【００２４】

暗号化ＩＣ１０２は、暗号化チップ１１０とフラッシュメモリチップ１１１が１つのパッケージに封止されているＳｉＰとして構成される。暗号化チップ１１０はＨＤＤ１０３に格納されるデータ等に暗号化処理を行う。フラッシュメモリチップ１１１は各種データを格納する。フラッシュメモリチップ１１１は暗号化ＩＣ１０２に内蔵されている必要はなく、外付けされていてもよい。

【００２５】

図３は、図２における暗号化ＩＣ１０２の内部構成を概略的に示すブロック図である。

【００２６】

図３の暗号化ＩＣ１０２は、ＣＰＵ２０１、フラッシュメモリ２０２、ＲＡＭ２０３、メモリ制御部２０４、暗号化／復号化処理部２０５、ＳＡＴＡデバイス－ＩＦ２０６、ＳＡＴＡホスト－ＩＦ２０７、フラッシュ－ＩＦ２０８、及びデバッグ－ＩＦ２０９を備え、これらは、バス２１０を介して互いに接続されている。暗号化ＩＣ１０２は、ＳＡＴＡデバイス－ＩＦ２０６、ＳＡＴＡホスト－ＩＦ２０７、フラッシュ－ＩＦ２０８、及びデバッグ－ＩＦ２０９を介してホストコントローラ１０１、ＨＤＤ１０３、フラッシュ治具１０９、及びデバッガ１０７に夫々接続されている。

【００２７】

ＣＰＵ２０１は、フラッシュメモリ２０２やＲＡＭ２０３に格納された暗号化プログラム、擬似乱数プログラム、及びＳＡＴＡ－ＩＦ制御プログラム等のプログラムを実行する。

【００２８】

フラッシュメモリ２０２は、不揮発性メモリであり、各種プログラム、各種制御パラメータ、及び暗号化のための秘密情報等が格納される。ＲＡＭ２０３は、揮発性メモリであり、プログラムの実行領域、一時作業領域、及び生成された暗号鍵の保存領域等に使用される。メモリ制御部２０４はフラッシュメモリ２０２及びＲＡＭ２０３のデータへの入出力制御を行う。暗号化／復号化処理部２０５はデータの暗号化処理及び復号化処理を、例えば、共通鍵暗号方式としてのＡＥＳによって行う。

【００２９】

図４は、図３のフラッシュメモリ２０２及びＲＡＭ２０３に格納される主要なデータを示す図である。

【００３０】

図４において、フラッシュメモリ２０２は、秘密情報暗号化プログラム３０１、データ暗号化プログラム３０２、秘密情報３０３、及び情報ｂ３０４を格納し、ＲＡＭ２０３は、秘密情報用暗号鍵３０５及びデータ用暗号鍵３０６を格納する。

【００３１】

秘密情報暗号化プログラム３０１は、データ暗号化プログラム３０２や秘密情報３０３の一部又は全部の暗号化／復号化処理を、例えば、ＡＥＳによって行うと共に、情報ｂ３０４及び後述の情報ａ４１０を用いて秘密情報用暗号鍵３０５をＲＡＭ２０３上に生成する。データ暗号化プログラム３０２は、ＳＡＴＡ－ＩＦ１０４，１０５を介してホストコントローラ１０１及びＨＤＤ１０３との間で送受信されるデータの暗号化／復号化処理を

、例えば、ＡＥＳによって行うと共に、秘密情報３０３を用いてデータ用暗号鍵３０６をＲＡＭ２０３上に生成する。

【００３２】

秘密情報３０３は、暗号化ＩＣ１０２を使用可能にするための認証情報やデータ用暗号鍵３０６を生成するための機密性の高い重要な情報であり、ＳＡＴＡ－ＩＦ１０４を介して接続されているホストコントローラ１０１から受信される。

【００３３】

情報ｂ３０４は、ビット値で構成され、後述の情報ａ４１０に組み合わせることができる。また、情報ｂ３０４は、ホストコントローラ１０１から受信され、例えば、受信先のホストコントローラ１０１の個々に応じて、又はホストコントローラ１０１から受信するタイミングに応じて異なるビット値で構成される。秘密情報暗号化プログラム３０１及び情報ｂ３０４は平文で、データ暗号化プログラム３０２及び秘密情報３０３は暗号文でフラッシュメモリ２０２に格納される。

【００３４】

図５は、図４における秘密情報用暗号鍵３０５を生成する際に必要となる情報ａ４１０の生成方法について説明するのに用いられる図である。

【００３５】

図５において、暗号化ＩＣ１０２はブロックＡ４０１、ブロックＢ４０２、及びブロックＣ４０３の複数の機能ブロックを備え、各機能ブロックは、制御レジスタ４０４及びステータスレジスタ４０５を備え、各レジスタはビット列からなるレジスタ値で構成される。

【００３６】

制御レジスタ４０４はハードモジュールを制御するためのレジスタであり、ステータスレジスタ４０５はＣＰＵ２０１の演算状態を示すレジスタである。すなわち、ステータスレジスタ４０５は、ＣＰＵ２０１の演算状態によって構成するレジスタ値が変化し、例えば、暗号化ＩＣの起動方法によって構成するレジスタ値が変化する。

【００３７】

情報ａ４１０は、例えば、或る時間において、制御レジスタ４０４のレジスタ値から選択されたレジスタ値Ａｃ１，Ａｃ２，及びＣｃ１と、ステータスレジスタ４０５のレジスタ値から選択されたレジスタ値Ａｓ２，Ｂｓ２，及びＣｓ１とを組み合わせることによって生成される（情報値生成手段）。上述したように、ステータスレジスタ４０５のレジスタ値はＣＰＵ２０１の演算状態によって変化する。換言すれば、ステータスレジスタ４０５のレジスタ値は時間の経過に応じて変化するため、ステータスレジスタ４０５のレジスタ値を含む情報ａ４１０も生成される時間に応じて変化する。

【００３８】

図６Ａは、図４における秘密情報用暗号鍵３０５の生成に用いられるシード値を示す図である。

【００３９】

図６Ａにおいて、シード値５０１は、情報ａ４１０及び情報ｂ３０４を結合して得られる。

【００４０】

図６Ｂは、図６Ａのシード値５０１を用いて秘密情報用暗号鍵３０５を生成する方法を説明するのに用いられる図である。

【００４１】

図６Ｂにおいて、時間軸５０２は、暗号化ＩＣ１０２の電源をＯＮにしたときを時刻ｔ＝０とした時間の経過を示す。例えば、時刻ｔ１には、時刻ｔ１に生成される情報ａ４１０としてのＸ１と情報ｂ３０４を組み合わせてシード値５０３を得、該得られたシード値５０３を疑似乱数モジュール５０４に入力してビット列５０５を得る（疑似乱数化）。時刻ｔ２には、時刻ｔ２に生成される情報ａ４１０としてのＸ２と情報ｂ３０４を組み合わせてシード値５０６を得、該得られたシード値５０６を疑似乱数モジュール５０４に入力

してビット列５０７を得る。その後、ビット列５０５，５０７を用いて排他的論理和演算（ＥｘＯＲ）５０８を行うことによって秘密情報用暗号鍵３０５が生成される（暗号鍵生成手段）。

【００４２】

なお、シード値５０３，５０６には、必ずしも情報ｂ３０４が組み合わされる必要はなく、情報ａ４１０単独でシード値５０３，５０６を構成してもよい。但し、市場に多数流通しているような暗号化ＩＣチップ（以下、「量産型暗号化ＩＣチップ」という）を用いた場合、情報ｂ３０４を組み合わせずに秘密情報用暗号鍵３０５を生成すると、時刻ｔ１及び時刻ｔ２における情報ａ４１０としてのＸ１及びＸ２はいずれの量産型暗号化ＩＣチップにおいても同一のレジスタ値から生成されるため、得られる秘密情報用暗号鍵３０５は同一となり、容易に秘密情報用暗号鍵３０５が再現されるおそれがある。

【００４３】

そこで、これに対応して、例えば、ホストコントローラ１０１の個々に応じて異なるビット値で構成される情報ｂ３０４を組み合わすことによって暗号化ＩＣチップ個別の秘密情報用暗号鍵３０５を生成し、秘密情報用暗号鍵３０５が同一となることを回避するのがよい。これにより、セキュリティレベルを向上させることができる。

【００４４】

また、情報ａ４１０と情報ｂ３０４から秘密情報用暗号鍵３０５を生成した場合、情報ｂ３０４のみを変更する秘密情報用暗号鍵３０５の無効化（ゼロ化）処理を行うことができる。情報ｂ３０４を変更すると、情報ｂ３０４の変更前に生成された秘密情報用暗号鍵３０５は使用できないので、例えば、秘密情報用暗号鍵３０５を用いて暗号化した秘密情報３０３を破棄しても、当該暗号化された秘密情報３０３は、情報ｂ３０４の変更後に永久に復号化されることがなく、より一層セキュリティレベルを向上させることができる。

【００４５】

図７は、図６Ｂにおける時刻ｔ１に生成される情報ａ４１０としてのＸ１のビット列である。図中、Ｘ１_normal６０１は暗号化ＩＣ１０２を通常起動した場合に生成される情報a４１０に対応し、Ｘ１_debug６０２は暗号化ＩＣ１０２をデバッガ１０７の使用によって起動した場合に生成される情報ａ４１０に対応する。

【００４６】

上述したように、ステータスレジスタ４０５は暗号化ＩＣ１０２の起動方法が２以上ある場合、起動方法によって構成するレジスタ値が変化するため、ステータスレジスタ４０５のレジスタ値を含む情報ａ４１０も暗号化ＩＣ１０２の起動方法に応じて当該情報ａ４１０を構成するビット値が異なる。例えば、図７に示すように、Ｘ１_normal６０１とＸ１_debug６０２には互いに異なるビット６０３～６０６が存在する。

【００４７】

すなわち、暗号化ＩＣ１０２の起動方法を変更することによって情報ａ４１０を変更することができ、もって、当該情報ａ４１０を組み合わせて生成される秘密情報用暗号鍵３０５を変更することができる。これにより、秘密情報用暗号鍵３０５のセキュリティレベルを向上させることができる。

【００４８】

図８は、図４におけるデータ暗号化プログラム３０２及び秘密情報３０３を暗号化する暗号化処理の手順を示すフローチャートである。

【００４９】

図８の暗号化処理は暗号化ＩＣ１０２が備えるＣＰＵ２０１によって実行される。

【００５０】

図８において、時刻ｔ１及びｔ２における情報ａ４１０としてのＸ１及びＸ２を、図５の生成方法によって夫々生成し（ステップＳ７０１）、暗号化ＩＣ１０２がホストコントローラ１０１と接続されているか否かを判別する（ステップＳ７０２）。

【００５１】

ステップＳ７０２の判別の結果、ホストコントローラ１０１と接続されている場合（ス

テップＳ７０２でＹＥＳ）、ホストコントローラ１０１から秘密情報３０３及び情報ｂ３０４を受信する（ステップＳ７０３）。

【００５２】

次いで、Ｘ１と情報ｂ３０４を組み合わせて得られるシード値５０３を疑似乱数モジュール５０４に入力してビット列５０５を得ると共に、Ｘ２と情報ｂ３０４を組み合わせて得られるシード値５０６を疑似乱数モジュール５０４に入力してビット列５０７を得、該得られたビット列５０５，５０７を用いて排他的論理和演算（ＥｘＯＲ）５０８を行い、秘密情報用暗号鍵３０５を生成する（ステップＳ７０４）。

【００５３】

次いで、生成された秘密情報用暗号鍵３０５を用いてデータ暗号化プログラム３０２及び秘密情報３０３の暗号化処理を行い（ステップＳ７０５）、暗号化処理が完了したか否かを判別する（ステップＳ７０６）。

【００５４】

ステップＳ７０６の判別の結果、暗号化処理が完了していない場合はステップＳ７０５に戻り（ステップＳ７０６でＮＯ）、暗号化処理が完了している場合（ステップＳ７０６でＹＥＳ）、暗号化したデータ暗号化プログラム３０２、秘密情報３０３、及び秘密情報用暗号鍵３０５を生成する際に用いた情報ｂ３０４をフラッシュメモリ２０２に格納して（ステップＳ７０７）、本処理を終了する。

【００５５】

ステップＳ７０２の判別の結果、ホストコントローラ１０１と接続されていない場合、ホストコントローラ１０１から秘密情報３０３及び情報ｂ３０４を受信することなく、直ちに本処理を終了する。

【００５６】

図８の暗号化処理によれば、時間の経過に応じて変化するステータスレジスタ４０５の複数のレジスタ値から選択されたレジスタ値を用いて生成された情報ａ４１０としてのＸ１やＸ２を用いて（ステップＳ７０１）秘密情報用暗号鍵３０５を生成する（ステップＳ７０４）ので、時刻ｔ１やｔ２とは異なる時刻に暗号化ＩＣ１０２を起動する第三者が同じレジスタ値を用いて情報ａ４１０を生成するのは困難であり、これにより、秘密情報用暗号鍵３０５の再現性を困難にすることができる。その結果、第三者によってデータ暗号化プログラム３０２及び秘密情報３０３の暗号化が簡単に解除されるのを防止できる。

【００５７】

また、図８の暗号化処理によれば、情報ａ４１０に情報ｂ３０４を組み合わせることによって秘密情報用暗号鍵３０５の生成を行うが（ステップＳ７０４）、当該情報ｂ３０４を構成するビット値は、例えば、ホストコントローラ１０１の個々に応じて異なるので、暗号化ＩＣチップ固有の秘密情報用暗号鍵３０５を生成することができ、その結果、秘密情報用暗号鍵３０５の再現性をより困難にすることができ、もってセキュリティレベルをより向上させることができる。

【００５８】

さらに、図８の暗号化処理によれば、情報ａ４１０に情報ｂ３０４を組み合わせることによって秘密情報用暗号鍵３０５の生成を行う（ステップＳ７０４）ので、秘密情報用暗号鍵３０５の無効化（ゼロ化）処理をすることができ、より一層セキュリティレベルを向上させることができる。

【００５９】

図９は、図４における秘密情報暗号化プログラム３０１及びデータ暗号化プログラム３０２を実行するプログラム実行処理の手順を示すフローチャートである。

【００６０】

図９のプログラム実行処理は暗号化ＩＣ１０２が備えるＣＰＵ２０１によって実行される。

【００６１】

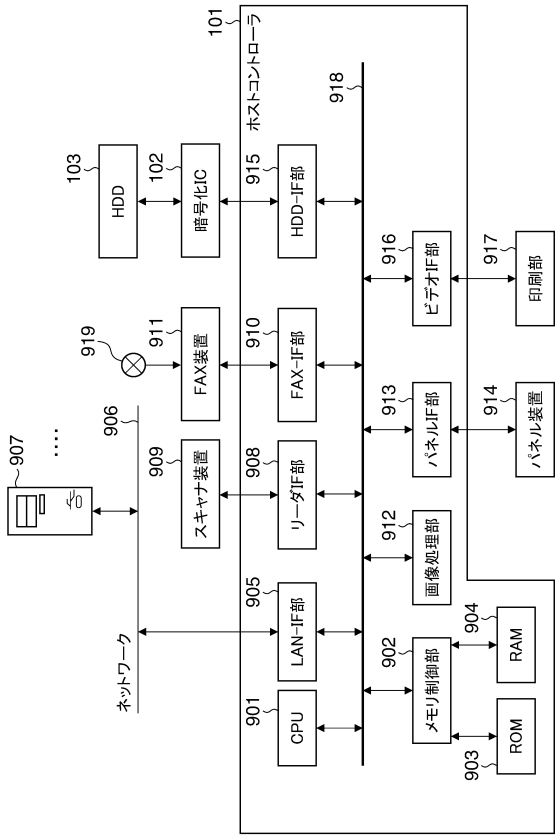
図９において、まず、時刻ｔ１及びｔ２における情報ａ４１０としてのＸ１及びＸ２を

、図５の生成方法によって夫々生成する（ステップＳ８０１）。
【００６２】
次いで、Ｘ１とフラッシュメモリ２０２に格納されている情報ｂ３０４を組み合わせて得られるシード値５０３を疑似乱数モジュール５０４に入力してビット列５０５を得ると共に、Ｘ２とフラッシュメモリ２０２に格納されている情報ｂ３０４を組み合わせて得られるシード値５０６を疑似乱数モジュール５０４に入力してビット列５０７を得、該得られたビット列５０５，５０７を用いて排他的論理和演算（ＥｘＯＲ）５０８を行い、秘密情報用暗号鍵３０５を生成する（ステップＳ８０２）。
【００６３】
ところで、同じ時刻においてステータスレジスタ４０５のレジスタ値は同じ値を示すため、時刻が共通するステップＳ７０１及びステップＳ８０１で生成されるＸ１、Ｘ２は互いに同じであり、ステップＳ７０４及びステップＳ８０２で生成される秘密情報用暗号鍵３０５も同じとなる。したがって、ステップＳ７０４で生成された秘密情報用暗号鍵３０５を用いて暗号化されたデータ暗号化プログラム３０２及び秘密情報３０３は、ステップＳ８０２で生成される秘密情報用暗号鍵３０５によって復号化することができる。
【００６４】
次いで、ステップＳ８０２で生成された秘密情報用暗号鍵３０５を用いてデータ暗号化プログラム３０２及び秘密情報３０３（いずれもステップＳ７０４で生成された秘密情報用暗号鍵３０５を用いて暗号化されている）の復号化処理を行ってＲＡＭ２０３に展開し（ステップＳ８０３）、復号化処理が完了したか否かを判別する（ステップＳ８０４）。
【００６５】
ステップＳ８０４の判別の結果、暗号化処理が完了していない場合はステップＳ８０３に戻り（ステップＳ８０４でＮＯ）、復号化処理が完了している場合（ステップＳ８０４でＹＥＳ）は、ＲＡＭ２０３に復号化され、且つ展開された秘密情報３０３を用いてデータ用暗号鍵３０６の生成を行い（ステップＳ８０５）、ホストコントローラ１０１と接続するか否かを判別する（ステップＳ８０６）。
【００６６】
ステップＳ８０６の判別の結果、ホストコントローラ１０１と接続するとき（ステップＳ８０６でＹＥＳ）は、ホストコントローラ１０１とＨＤＤ１０３の間での通信が確立されてホストコントローラ１０１からのコマンドの受付が可能となる。
【００６７】
ステップＳ８０６の判別の結果、ホストコントローラ１０１と接続しないときは（ステップＳ８０６でＮＯ）、ホストコントローラ１０１からのコマンド要求の有無にかかわらず、直ちに本処理を終了する。
【００６８】
次いで、ホストコントローラ１０１からコマンドが要求されたか否かを判別し（ステップＳ８０７）、ホストコントローラ１０１からコマンドが要求された場合（ステップＳ８０７でＹＥＳ）、要求されたコマンドが、ＨＤＤ１０３のシステム領域からシステム情報を読み出し、又はＨＤＤ１０３のシステム領域にシステム情報を書き込むシステム系コマンドであるか否かを判別する（ステップＳ８０８）。
【００６９】
ステップＳ８０８判別の結果、システム系コマンドである場合（ステップＳ８０８でＹＥＳ）は、システム情報は平文であり、暗号化する必要性が高くないことからシステム情報を暗号化することなく（非暗号化）平文のまま（ステップＳ８０９）、システム情報のホストコントローラ１０１又はＨＤＤ１０３への送信を（ステップＳ８１４）送信完了まで（ステップＳ８１７でＹＥＳ）実行する。
【００７０】
一方、ステップＳ８０８の判別の結果、要求されたコマンドがシステム系コマンドではないときは（ステップＳ８０８でＮＯ）、要求されたコマンドがＨＤＤ１０３のデータ領域からデータ情報を読み出すリード系コマンドかＨＤＤ１０３のデータ領域にデータ情報

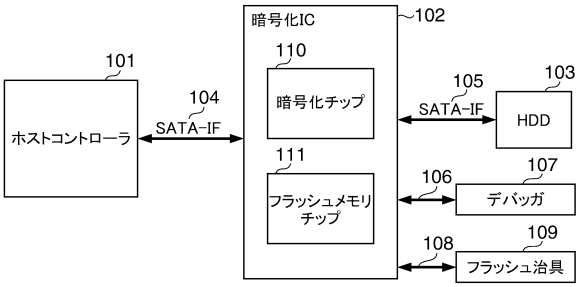
を書き込むライト系コマンドかを判別する（ステップＳ８１０）。
【００７１】
ステップＳ８１０の判別の結果、要求されたコマンドがリード系コマンドのときはＨＤＤ１０３から暗号文データを読み出して（ステップＳ８１１）当該暗号文データをデータ用暗号鍵３０６を用いて復号化し（ステップＳ８１２）、ホストコントローラ１０１への送信を（ステップＳ８１５）送信完了まで（ステップＳ８１８でＹＥＳ）実行する。
【００７２】
ステップＳ８１０の判別の結果、要求されたコマンドがライト系コマンドのときは、ホストコントローラ１０１から受信したデータをデータ用暗号鍵３０６によって暗号化し（ステップＳ８１３）、ＨＤＤ１０３への送信を（ステップＳ８１６）送信完了まで（ステップＳ８１９でＹＥＳ）実行する。
【００７３】
データの送信が完了した（ステップＳ８１７でＹＥＳ，Ｓ８１８でＹＥＳ，Ｓ８１９でＹＥＳ）後、暗号化ＩＣ１０２への電源供給を停止したとき（ステップＳ８２０でＹＥＳ）は、本処理を終了し、暗号化ＩＣ１０２への電源供給を停止しない（ステップＳ８２０でＮＯ）ときはステップＳ８０７以降の処理を繰り返す。
【００７４】
図９のプログラム実行処理によれば、図８の暗号化処理と同様に、時間の経過に応じて変化するステータスレジスタ４０５の複数のレジスタ値から選択されたレジスタ値を用いて生成された情報ａ４１０としてのＸ１やＸ２を用いて（ステップＳ８０１）秘密情報用暗号鍵３０５を生成し（ステップＳ８０２）、当該秘密情報用暗号鍵３０５によって暗号化プログラム３０２と秘密情報３０３の復号化処理を行う（ステップＳ８０３）。上述したように、時刻ｔ１やｔ２とは異なる時刻に暗号化ＩＣ１０２を起動する第三者が同じレジスタ値を用いて情報ａ４１０を生成するのは困難であり、これにより、秘密情報用暗号鍵３０５の再現性を困難にすることができる。その結果、秘密情報３０３の暗号化が簡単に解除されるのを防止することができる。
【００７５】
また、図９のプログラム実行処理によれば、秘密情報３０３が復号化されない限り、データ用暗号鍵３０６は生成されない（ステップＳ８０５）ので、ＨＤＤ１０３に格納されているデータ用暗号鍵３０６を用いて暗号化された暗号化データを第三者によって解析されることを防止できる。
【００７６】
なお、秘密情報用暗号鍵３０５は、暗号化ＩＣ１０２の起動時（ｔ１＝ｔ２＝０）に生成されてもよい。すなわち、データ暗号化プログラム３０２及び秘密情報３０３を復号化するための秘密情報用暗号鍵３０５を暗号化ＩＣ１０２の起動に応じて生成する（ステップＳ８０１～Ｓ８０３）ので、データ暗号化プログラム３０２及び秘密情報３０３を暗号化して復号化するまでの間に第三者がデータ暗号化プログラム３０２及び秘密情報３０３を解読する可能性を排除できる。
【００７７】
本発明は、上述した実施形態の機能を実現するソフトウエア（プログラム）をネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（又はＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理において、そのプログラム、及び該プログラムを格納するコンピュータ読み取り可能な記憶媒体によって構成されてもよい。
【符号の説明】
【００７８】
１０２　暗号化ＩＣ
２０２　フラッシュメモリ
３０２　データ暗号化プログラム
３０３　秘密情報

３０４　情報ｂ
３０５　秘密情報用暗号鍵
４０４　制御レジスタ
４０５　ステータスレジスタ
４１０　情報ａ

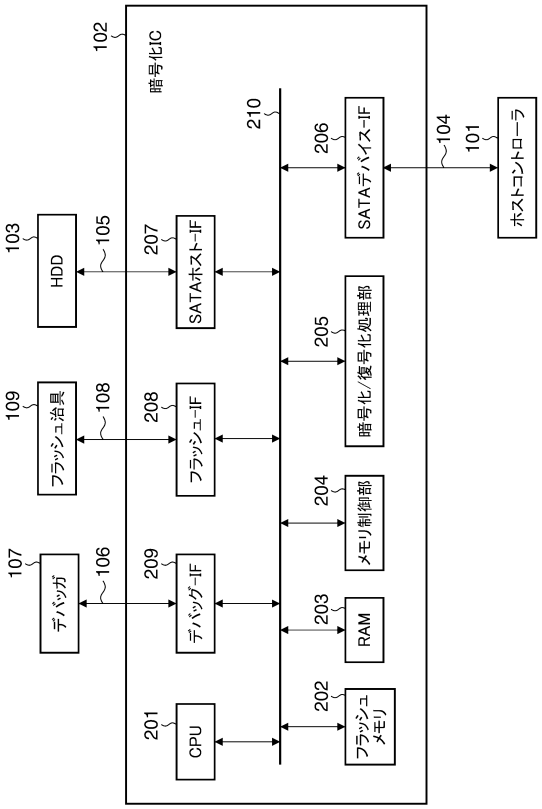
【図１】



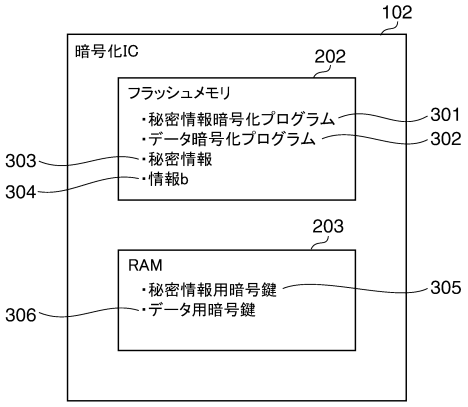
【図２】



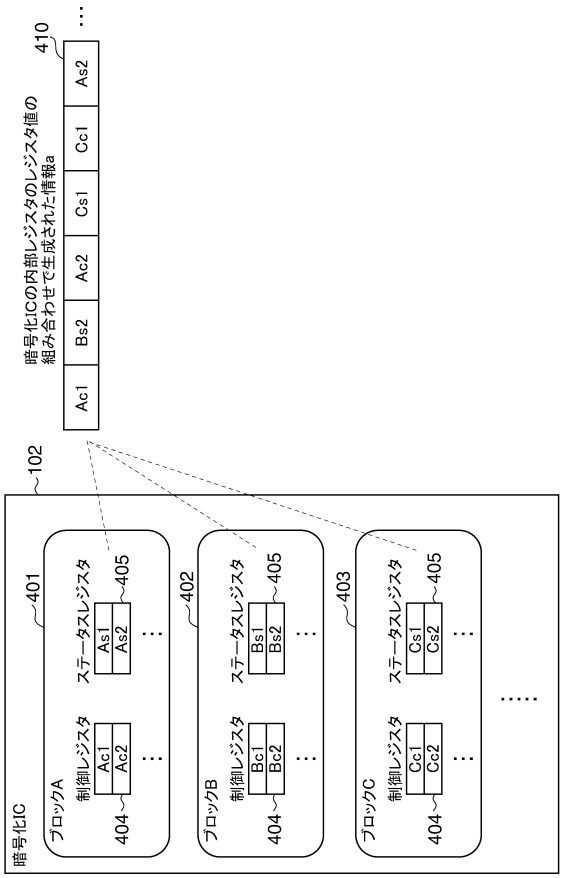
【図３】



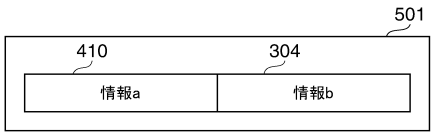
【図４】



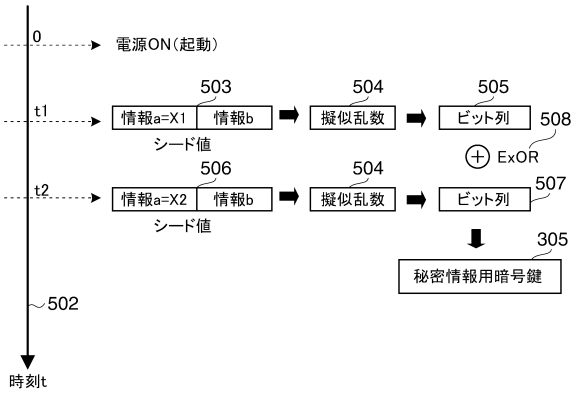
【図５】



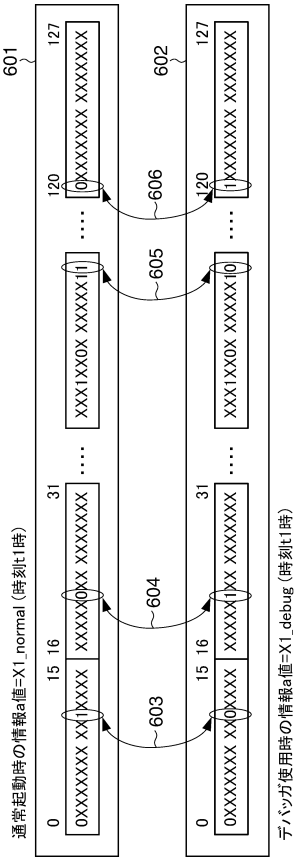
【図６Ａ】



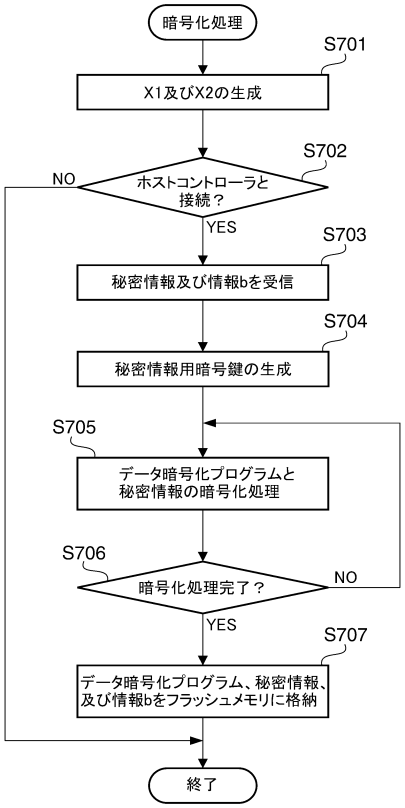
【図６Ｂ】



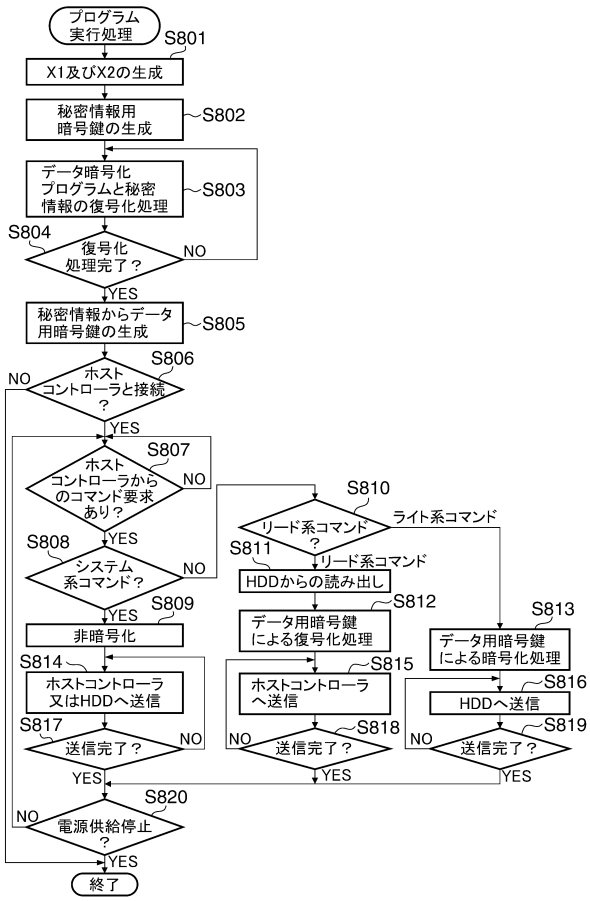
【図７】


601
602
127
120
31
16
15
0
0XXXXXXX XXXXXXX
1XXXXXXX XXXXXXX
XXX1XX0X XXXXX1
XXX1XX0X XXXXX0
XXXXX0XX XXXXXXX
XXXXX1XX XXXXXXX
0XXXXXXX XX1XXXX
0XXXXXXX XX0XXXX
606
605
604
603
通常起動時の情報a値=X1_normal（時刻t1時）
デバッガ使用時の情報a値=X1_debug（時刻t1時）

【図８】


暗号化処理
S701
X1及びX2の生成
S702
ホストコントローラと接続？
NO
YES
S703
秘密情報及び情報bを受信
S704
秘密情報用暗号鍵の生成
S705
データ暗号化プログラムと秘密情報の暗号化処理
S706
暗号化処理完了？
NO
YES
S707
データ暗号化プログラム、秘密情報、及び情報bをフラッシュメモリに格納
終了

【図９】


プログラム実行処理
S801
X1及びX2の生成
秘密情報用暗号鍵の生成
S802
データ暗号化プログラムと秘密情報の復号化処理
S803
S804
復号化処理完了？
NO
YES
秘密情報からデータ用暗号鍵の生成
S805
S806
ホストコントローラと接続？
NO
YES
S807
ホストコントローラからのコマンド要求あり？
NO
YES
S808
システム系コマンド？
NO
YES
S809
非暗号化
S814
ホストコントローラ又はHDDへ送信
S817
送信完了？
NO
YES
S810
リード系コマンド？
ライト系コマンド
S811
リード系コマンド
HDDからの読み出し
S812
データ用暗号鍵による復号化処理
S815
ホストコントローラへ送信
S818
送信完了？
NO
YES
S813
データ用暗号鍵による暗号化処理
S816
HDDへ送信
S819
送信完了？
NO
YES
S820
電源供給停止？
NO
YES
終了

フロントページの続き

(56)参考文献 特開２００８－８５９８６（ＪＰ，Ａ）
特開２００９－７６０４５（ＪＰ，Ａ）
特開２００１－２３０７７０（ＪＰ，Ａ）
米国特許出願公開第２０１１／００８１０１５（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／１２
Ｇ０６Ｆ　２１／６２
Ｇ０９Ｃ　　１／００