

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4981981号

(P4981981)

(45) 発行日 平成24年7月25日(2012.7.25)

(24) 登録日 平成24年4月27日(2012.4.27)

(51) Int.Cl.		F I			
G06F	21/24	(2006.01)	G06F	21/24	166A
G06F	3/06	(2006.01)	G06F	3/06	301J
G09C	1/00	(2006.01)	G09C	1/00	660D

請求項の数 5 (全 33 頁)

(21) 出願番号	特願2011-180202 (P2011-180202)	(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
(22) 出願日	平成23年8月22日(2011.8.22)	(74) 代理人	100145827 弁理士 水垣 親房
(62) 分割の表示	特願2006-48943 (P2006-48943) の分割	(72) 発明者	伊藤 秋生 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
原出願日	平成18年2月24日(2006.2.24)	(72) 発明者	田頭 信博 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
(65) 公開番号	特開2011-253561 (P2011-253561A)	審査官	和田 財太
(43) 公開日	平成23年12月15日(2011.12.15)		
審査請求日	平成23年8月22日(2011.8.22)		

最終頁に続く

(54) 【発明の名称】 データ処理装置およびデータ処理方法

(57) 【特許請求の範囲】

【請求項1】

記憶装置と前記記憶装置を制御する制御装置の間に接続されるデータ処理装置であって、

前記制御装置から受信して前記記憶装置へ送信すべきデータに対して暗号化処理を実行する暗号化手段と、

前記記憶装置から受信して前記制御装置に送信すべきデータに対して復号化処理を実行する復号化手段と、

前記制御装置から受信したコマンドのうち前記記憶装置へ送信すべきコマンドを特定するための特定情報を記憶する記憶手段と、

前記記憶手段に記憶された前記特定情報に基づいて、前記制御装置から受信したコマンドを前記記憶装置へ送信するか否かを判断する判断手段と、

前記判断手段により前記記憶装置へ送信すると判断されたコマンドを前記記憶装置へ送信する送信手段と、

前記記憶装置へ送信すると前記判断手段により判断されて前記送信手段により送信されたコマンドが暗号化されていないデータを前記記憶装置から読み出すための第1のコマンドである場合は、前記第1のコマンドの送信によって前記記憶装置から受信するデータに対して前記復号化処理を前記復号化手段に実行させず、前記記憶装置へ送信すると前記判断手段により判断されて前記送信手段により送信されたコマンドが前記第1のコマンドとは異なる、暗号化されているデータを前記記憶装置から読み出すための第2のコマンドで

10

20

ある場合は、前記第2のコマンドの送信によって前記記憶装置から受信するデータに対して前記復号化処理を前記復号化手段に実行させる制御手段と、を有することを特徴とするデータ処理装置。

【請求項2】

前記第1のコマンドは、前記制御装置から前記記憶装置へ転送されたデータとは異なる、前記記憶装置の固有情報を前記記憶装置から読み出すためのコマンドであることを特徴とする請求項1に記載のデータ処理装置。

【請求項3】

コマンドまたは暗号化されていないデータを前記制御装置から受信する第1の受信手段と、

暗号化されているデータまたは暗号化されていないデータを前記記憶装置から受信する第2の受信手段と、

前記復号化手段によって復号化されたデータまたは前記記憶装置から受信した暗号化されていないデータを前記制御装置に送信する第1の送信手段と、

前記制御装置から受信したコマンドまたは前記暗号化手段によって暗号化されたデータを前記記憶装置に送信する第2の送信手段とを有することを特徴とする請求項1または2に記載のデータ処理装置。

【請求項4】

前記第2の受信手段で受信したデータを前記復号化手段に転送するか、前記第2の受信手段で受信したデータを前記復号化手段を介することなく前記第1の送信手段に転送するかを選択的に切り替えるセレクトを有し、

前記制御手段は、前記第1のコマンドの送信によって前記記憶装置から受信するデータに対して前記復号化処理が実行されないよう前記セレクトを制御し、前記第2のコマンドの送信によって前記記憶装置から受信するデータに対して前記復号化処理が実行されるよう前記セレクトを制御することを特徴とする請求項3に記載のデータ処理装置。

【請求項5】

記憶装置と前記記憶装置を制御する制御装置の間に接続され、前記制御装置から受信して前記記憶装置へ送信すべきデータに対して暗号化処理を実行する暗号化手段と、前記記憶装置から受信して前記制御装置に送信すべきデータに対して復号化処理を実行する復号化手段とを有するデータ処理装置におけるデータ処理方法であって、

前記データ処理装置の記憶手段に記憶された、前記制御装置から受信したコマンドのうち前記記憶装置へ送信すべきコマンドを特定するための特定情報に基づいて、前記制御装置から受信したコマンドを前記記憶装置へ送信するか否かを判断する判断ステップと、

前記判断ステップにより前記記憶装置へ送信すると判断されたコマンドを前記記憶装置へ送信する送信ステップと、

前記記憶装置へ送信すると前記判断ステップにより判断されて前記送信ステップにより送信されたコマンドが暗号化されていないデータを前記記憶装置から読み出すための第1のコマンドである場合は、前記第1のコマンドの送信によって前記記憶装置から受信するデータに対して前記復号化処理を前記復号化手段に実行させず、前記記憶装置へ送信すると前記判断ステップにより判断されて前記送信ステップにより送信されたコマンドが前記第1のコマンドとは異なる、暗号化されているデータを前記記憶装置から読み出すための第2のコマンドである場合は、前記第2のコマンドの送信によって前記記憶装置から受信するデータに対して前記復号化処理を前記復号化手段に実行させる制御ステップと、

を有することを特徴とするデータ処理方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、データ処理装置およびデータ処理方法に関するものである。

【背景技術】

【0002】

10

20

30

40

50

コンピュータシステムにおいて、データは外部記憶装置に保持されることが多い。外部記憶装置は、HDDに代表されるように、コンピュータシステムとはケーブル（例えば、IDE、SCSI、USB、IEEE1395）等で接続されていて、コンピュータシステムとの物理的な一体感が小さく、分離することが可能である。したがって、外部記憶装置をコンピュータシステムから分離し、解析することによって、外部記憶装置内のデータが漏洩してしまうという脅威が存在する。

【0003】

上記の脅威に対抗する対策の一つとして、外部記憶装置に保持するデータを暗号化する方法がある。この方法は、外部記憶装置に書き込むデータを暗号化し、また外部記憶装置から読み込みデータを復号することによって、外部記憶装置に保持されているデータの漏洩を防止するものである。

10

【0004】

既存のコンピュータシステムに、新たに暗号化復号機能を追加する方法として、以下の3つの方法が考えられる。

【0005】

第1の方法は、コンピュータシステムに暗号化復号機能を新規に追加する方法である。この方法の場合、既存のコンピュータシステムに対して、暗号化復号機能を新規に追加する必要があり、コンピュータシステムの変更が大きくなるという問題がある。

【0006】

第2の方法は、外部記憶装置に暗号化復号機能を追加する方法である。この方法の場合、外部記憶装置自身に暗号化復号機能を追加する必要があり、汎用的な外部記憶装置が利用できないという問題がある。

20

【0007】

第3の方法は、コンピュータシステムと外部記憶装置との間をブリッジする新たな装置を設ける方法である。なお、第3の方法に関連した提案として、特許文献1（特開平4-98552号公報）と特許文献2（特開平11-85621号公報）がある。

【0008】

特許文献1は、暗号化手段、復号手段、データ処理手段および外部記憶装置から構成される電子ファイリング装置であって、外部記憶装置に記録するデータを暗号化し、外部記憶装置から読み出すデータを復号する。また、暗号化または復号に必須の情報を取り外し可能な構造を有する。

30

【0009】

特許文献2は、コンピュータシステムと外部記憶装置の間に接続される記録データ暗号化装置102であり、鍵情報を記憶する記憶手段と、コンピュータシステムから送られたデータを前記鍵情報を加味して暗号化し外部記憶装置へ転送する暗号化手段を備える。また、外部記憶装置から読み出した暗号化されたデータを前記鍵情報を加味して復号化しコンピュータシステムへ転送する復号化手段と、暗号化手段と復号化手段を監視しそれらの動作を制御するプロトコル制御手段を備える。このような構成により、コンピュータシステムおよび外部記憶装置に変更を加えることなく、外部記憶装置に記憶するデータの暗号化を実現し、外部記憶装置内のデータの漏洩を防止している。また、鍵情報をICカード等の着脱可能な第2の外部記憶装置に記憶可能である。

40

【先行技術文献】

【特許文献】

【0010】

【特許文献1】特開平4-98552号公報

【特許文献2】特開平11-85621号公報

【発明の概要】

【発明が解決しようとする課題】

【0011】

上記特許文献1は、イメージスキャナ、ディスプレイ、プリンタまたは操作パネルを制

50

御するデータ処理手段が暗号化手段および復号手段を制御している。つまり、当該従来例は、暗号化手段および復号手段がデータ処理手段から分離可能となっており、物理的な構成においては上記第3の方法（ブリッジする新たな装置を設ける方法）に分類できる。

【0012】

しかし、データ処理手段が暗号化手段および復号手段を制御しており、機能的な構成においては上記第1の方法（コンピュータシステムに暗号化復号機能を追加する方法）であり、コンピュータシステムの変更が大きくなるという問題がある。

【0013】

上記特許文献2は、コンピュータシステムおよび外部記憶装置に変更を加えることなく、外部記憶装置に記憶するデータを暗号化し、外部記憶装置内のデータの漏洩を防止した。つまり、外部記憶装置単体の盗難という脅威に対しては、データの暗号化によって対抗していた。

10

【0014】

しかし、記憶装置には暗号化されていないデータが記憶されていることもあり、そのようなデータを記憶装置から読み出せるようにする必要もある。

【0015】

本発明の目的は、記憶装置と記憶装置を制御する制御装置の間に接続され、暗号化手段と復号化手段とを有するデータ処理装置において、記憶装置への不要なアクセスを防止して、セキュリティを強化する仕組みを提供することである。また、制御装置から受信したコマンドのうち記憶装置へ送信すべき適切なコマンドを記憶装置へ送信するとともに、暗号化されていないデータを記憶装置から読み出せる仕組みを提供することである。

20

【課題を解決するための手段】

【0016】

上記目的を達成する本発明のデータ処理装置は、以下に示す構成を備える。

記憶装置と前記記憶装置を制御する制御装置の間に接続されるデータ処理装置であって、前記制御装置から受信して前記記憶装置へ送信すべきデータに対して暗号化処理を実行する暗号化手段と、前記記憶装置から受信して前記制御装置に送信すべきデータに対して復号化処理を実行する復号化手段と、前記制御装置から受信したコマンドのうち前記記憶装置へ送信すべきコマンドを特定するための特定情報を記憶する記憶手段と、前記記憶手段に記憶された前記特定情報に基づいて、前記制御装置から受信したコマンドを前記記憶装置へ送信するか否かを判断する判断手段と、前記判断手段により前記記憶装置へ送信すると判断されたコマンドを前記記憶装置へ送信する送信手段と、前記記憶装置へ送信すると前記判断手段により判断されて前記送信手段により送信されたコマンドが暗号化されていないデータを前記記憶装置から読み出すための第1のコマンドである場合は、前記第1のコマンドの送信によって前記記憶装置から受信するデータに対して前記復号化処理を前記復号化手段に実行させず、前記記憶装置へ送信すると前記判断手段により判断されて前記送信手段により送信されたコマンドが前記第1のコマンドとは異なる、暗号化されているデータを前記記憶装置から読み出すための第2のコマンドである場合は、前記第2のコマンドの送信によって前記記憶装置から受信するデータに対して前記復号化処理を前記復号化手段に実行させる制御手段と、を有することを特徴とする。

30

40

【発明の効果】

【0017】

本発明によれば、記憶装置と前記記憶装置を制御する制御装置の間に接続され、暗号化手段と復号化手段とを有するデータ処理装置において、記憶装置への不要なアクセスを防止して、セキュリティを強化することができる。また、制御装置から受信したコマンドのうち記憶装置へ送信すべき適切なコマンドを記憶装置へ送信するとともに、送信するコマンドが暗号化されていないデータを記憶装置から読み出すための特定コマンドである場合に読み出したデータに対して復号化処理を実行しないようにすることができる。

【図面の簡単な説明】

【0018】

50

【図 1】本発明のデータ暗号化装置 102 を適用可能なシステムの一例を示すブロック図である。

【図 2】本発明における第 1 の制御処理プログラムの一例を示すフローチャートである。

【図 3】データを外部記憶装置（HDD）に書き込む場合のデータフローを示す図である。

【図 4】データを外部記憶装置（HDD）から読み込む場合のデータフローを示す図である。

【図 5】データ暗号化装置 102 の動作モードを説明する状態遷移図である。

【図 6】図 1 に示した ATA バスセクタの構成を説明するブロック図である。

【図 7】データ暗号化装置の各動作モードにおける図 6 に示した ATA バスセクタの動作について説明する図である。 10

【図 8】データ暗号化装置の実行可能な拡張コマンドを示す図である。

【図 9】データ暗号化装置が通常モードにおいて実行可能なコマンドを示す図である。

【図 10】本発明における第 2 の制御処理プログラムの一例を示すフローチャートである。

【図 11A】本発明における第 3 の制御処理プログラムの一例を示すフローチャートである。

【図 11B】本発明における第 3 の制御処理プログラムの一例を示すフローチャートである。

【図 12】本発明における第 4 の制御処理プログラムの一例を示すフローチャートである 20

【図 13】本発明における第 5 の制御処理プログラムの一例を示すフローチャートである。

【図 14】本発明における第 6 の制御処理プログラムの一例を示すフローチャートである。

【図 15】本発明における第 7 の制御処理プログラムの一例を示すフローチャートである。

【図 16】本発明に係るデータ暗号化装置で読み取り可能な各種データ処理プログラムを格納する記憶媒体（記録媒体）のメモリマップを説明する図である。

【発明を実施するための形態】 30

【0019】

次に本発明を実施するための最良の形態について図面を参照して説明する。

<システム構成の説明>

〔第 1 実施形態〕

本発明の実施形態について図面を参照して詳細に説明する。

【0020】

図 1 は、本発明のデータ処理装置としてのデータ暗号化装置を適用可能なシステムの一例を示すブロック図である。

【0021】

ず、本発明のデータ暗号化装置の利用環境について説明し、次に、データ暗号化装置の構成を説明し、最後に、データ暗号化装置でデータの機密性を維持する動作を説明する。 40

【0022】

<データ暗号化装置の利用環境>

図 1 に示すように、データ暗号化装置 102 は、コンピュータシステム（制御装置）100 と外部記憶装置としての HDD 103 間をブリッジするように接続される。データ暗号化装置 102 は、コンピュータシステム 100 が備える HDD コントローラ 101 と、HDD 103 の間にデータの暗号化を行う回路基板（ボード）として機能する。なお、データ暗号化装置 102 は、コンピュータシステム 100 及び HDD 103 と、汎用のインターフェース（例えば、ATA バスインターフェース）を介して接続されている。このようにデータ暗号化装置 102 を接続する際に、汎用のインターフェースを用いることで、 50

コンピュータシステム100や外部記憶装置103の構成を変更する必要がない。

【0023】

データ暗号化装置102は、コンピュータシステム100から送信されたデータを暗号化し、HDD103に転送し、かつHDD103から読み込まれたデータを復号化してコンピュータシステム100に転送する。なお、HDD103には、後述するように、データ暗号化装置102が保持する鍵により暗号化されたデータが記憶されるため、第三者がHDD103のみを持ち出されたとしてもHDD103をデータ暗号化装置102なしにはデータを復号化することができない。よって、HDD103のみが持ち出されたとしても、データのセキュリティを保つことができる。

【0024】

コンピュータシステム100は、バンキングシステム、DTP(Desktop Publishing)システム、またはMFP(Multi Function peripheral)等のデータ処理装置であり、特定のデータ処理装置に限定しない。外部記憶装置は、データを保持する装置であって、HDD(Hard Disk Drive)、またはCD-R/CD-RW/DVD-R/DVD-RWのような書き換え可能な磁気ディスク等であり、特定の外部記憶装置に限定しない。なお、図1では、一例としてHDDと記載している。

【0025】

なお、本実施形態において、コンピュータシステム100は、大きな筐体や入退室管理が実施されている居室に設置されている筐体であり、物理的に盗難が困難であるものと想定する。したがって、本実施形態においては、HDD103やデータ暗号化装置102が盗難されることによるデータ漏洩を防止する点に着目する。

【0026】

<データ暗号化装置102の構成>

図1に示すように、データ暗号化装置102は、コンピュータシステム100内のHDDコントローラ101とHDD103に挿入される。コンピュータシステム100のHDDコントローラ101とデータ暗号化装置102、及びデータ暗号化装置102とHDD103は、HDDの汎用的な通信規格であるもATAバス(104及び105)で接続される。データ暗号化装置102は、HDDコントローラ101からHDD103へ送られる制御コマンドの解釈処理、HDD103へ格納するデータの暗号化処理、及びHDD103から読み出したデータの復号化処理を行う。

【0027】

CPU106はデータ暗号化装置102の全体を制御するものである。また、メモリ111は、CPU106が実行する制御プログラム、及び各種のデータの格納が可能である。メモリ111は、データの暗号化に必要な鍵情報などのデータを格納することができる不揮発性メモリとして機能する。RAM112は、CPU106がメモリ111から読み出した制御プログラム等を実行するためのワークメモリとして用いられる。

【0028】

ATAバスセクタ(ATA BUS SELECTOR)107は、HDDコントローラ101とHDD103とを接続するためのインターフェースである。

【0029】

デバイスI/F(DEVICE I/F)108は、ATAバスセクタ107を介してHDDコントローラ101とアドレス・データバス113を接続するためのインターフェースである。

【0030】

コンピュータシステム100のHDDコントローラ101は、HDD103を制御するための制御コマンドを発行し、発行された制御コマンドは、デバイスI/F108で一旦受信される。実行可能であると判断されたコマンドはCPU106からHOST I/F(HOST I/F)110に対して発行され、HDD103へ送られる。

【0031】

10

20

30

40

50

CPU106は、コンピュータシステム100から受信したデータをHDD103へ格納する際には、受信したデータを、暗号・復号部109で暗号化してHDD103へ転送する。また、CPU106は、HDD103からデータを読み出してコンピュータシステム100に送信する際には、暗号・復号部109でデータを復号化して、ATAバス(ATA BUS)104を介してコンピュータシステム100へ転送する。

【0032】

暗号・復号部109は、コンピュータシステム100から送信されたデータをHDD103へ格納する際にデータの暗号化を行うとともに、HDD103からデータを読み出してコンピュータシステム100に転送する際にデータの復号化を行うブロックである。

【0033】

なお、暗号・復号部109が行うデータの暗号化においては、種々の暗号化アルゴリズムを用いることができる。例えば、AES(Advanced Encryption Standard)など共通鍵暗号方式、RSAなど公開鍵暗号方式、または共通鍵方式と公開鍵方式を組み合わせたハイブリッド方式などが利用可能である。

【0034】

ホストI/F110は、ATAバスセクタ107を介してHDD103とアドレス・データバス113を接続するためのインターフェースである。

【0035】

また、データ暗号化装置102内の各ブロックは、アドレス・データバス113を介してCPU106により制御される。

【0036】

なお、データ暗号化装置102は、ATAバスセクタ107により、HDDコントローラ101とHDD103に対する通信を全て標準インターフェース(ATAバスインターフェース)を介して実行することが可能である。

【0037】

以下、データ暗号化装置102の機能について説明する。なお、データ暗号化装置102は、以下の各機能をメモリ111に格納されているプログラムを実行することによって実現する。

【0038】

<認証機能>

データ暗号化装置102は、ATAバスと接続するインターフェース(ATAバスセクタ107)を有しているので、ATAバスと接続するインターフェースを有するコンピュータシステムであれば、どのようなシステムとも物理的には接続可能である。しかし、データ暗号化装置102が、どのようなコンピュータシステムとも接続可能な構成としてみると、問題が生じる。例えば、データ暗号化装置102及びHDD103が第三者により盗難されてしまった場合、盗難されたものがコンピュータシステム100とは別のコンピュータシステムに接続されることで、HDD103に記憶されたデータの内容が漏洩してしまう可能性がある。そこで、本実施形態では、データ暗号化装置102に、データ暗号化装置102が接続されるコンピュータシステムが正当なコンピュータシステムであるかどうかを認証するための認証機能を設けている。

【0039】

なお、認証機能を実現するための具体的な方法としては、種々の方法を用いることができるが、例えば以下の方法がある。

【0040】

第1の方法は、コンピュータシステム100とデータ暗号化装置102の各々に共通の認証情報を保持させておく。そして、コンピュータシステム100から受信した認証情報とデータ暗号化装置102で保持している認証情報が一致する場合に、コンピュータシステム100が正当であると認証する方法である。

【0041】

また、第2の方法は、コンピュータシステム100とデータ暗号化装置102の各々に

10

20

30

40

50

共通の認証情報を保持させておく。そして、認証情報を用いてチャレンジアンドレスポンス認証することにより、コンピュータシステムが正当であることを認証する方法である。

【0042】

また、第3の方法は、データ暗号化装置102にコンピュータシステム100の公開鍵証明書を保持させておく。そして、データ暗号化装置102がコンピュータシステム100のデジタル署名を受信し、デジタル署名を検証することにより、コンピュータシステム100が正当であることを認証する方法である。なお、データ暗号化装置102は、デジタル署名を受信するとともに公開鍵証明書を受信するようにしても良い。

【0043】

＜暗号化・復号機能＞

暗号化・復号機能は、暗号・復号部109が、鍵情報を用いてコンピュータシステム100から送信されたデータを暗号化し、HDD103から読み込んだデータを復号する機能である。

【0044】

＜制御機能＞

制御機能は、コンピュータシステム100から送信された情報がコマンド等の制御情報であるか、またはデータであるかを判断し、データの場合だけ暗号・復号部109を動作させ暗号化する機能である。なお、制御機能は、CPU106がメモリ111に格納されるプログラムを実行することにより実現される。さらに、制御機能は、HDD103から読み込んだ情報がコンピュータシステム100から送信された制御情報に対する応答等の制御情報であるか、またはデータであるかを判断し、データの場合だけ暗号・復号部109を動作させ復号する。

【0045】

なお、制御機能は、暗号・復号部109で用いる鍵情報が存在しない等の初期状態である場合、コンピュータシステム100とHDD103間の情報の送受信を遮断する。鍵情報の存在の有無は、後述の状態管理機能によって判断される。

【0046】

＜鍵生成機能＞

次に、暗号・復号部109がデータの暗号化・復号化をするために用いる鍵情報を生成する鍵生成機能について説明する。

【0047】

ここで、暗号・復号部109が用いる鍵情報は、第三者に漏洩するとHDD103内の暗号化されたデータの復号化が可能になってしまう情報である。従って、暗号・復号部109が用いる鍵情報は、データ暗号化装置102以外には漏洩しないようにする必要がある。そこで、データ暗号化装置102は、自装置内で鍵情報を生成する鍵生成機能を有している。

【0048】

鍵生成機能を実現するために、データ暗号化装置102は、コンピュータシステム100からコンピュータシステム100の固有情報（以下、固有情報）を受信する。固有情報は個々のコンピュータシステム100に固有の情報であって、シリアル番号、LAN I/Fを持つコンピュータシステム100におけるMACアドレス、またはそれらの情報を組み合わせた情報など、さまざまな情報を利用することが可能である。

【0049】

鍵生成機能は、コンピュータシステム100から受信した固有情報とメモリ111に保持しているシード情報から鍵情報を生成する。なお、シード情報の生成方法は、鍵情報の生成方法と暗号化アルゴリズムに依存する。乱数を暗号化アルゴリズムにおける鍵情報として利用できる場合は、シード情報も乱数または擬似乱数として生成することも可能である。一方、特定の条件を満たす情報を暗号化アルゴリズムにおける鍵情報として利用しなければならない場合は、例えば、鍵情報を生成し、生成した鍵情報とシード情報から「鍵

10

20

30

40

50

情報 = f (シード情報, 固有情報)」を満たすシード情報を求める必要がある。

【0050】

ここで、固有情報とシード情報から鍵情報を生成する方法としては種々の方法を用いることができるが、例えば以下の方法が考えられる。

【0051】

(1) 固有情報とシード情報の排他的論理和を鍵情報とする方法。

【0052】

(2) 一方方向性ハッシュ関数に固有情報とシード情報を入力し、出力された情報を鍵情報とする方法。

【0053】

(3) 固有情報を暗号化関数の鍵とし、シード情報を暗号化処理し、出力された情報を鍵情報とする方法。

【0054】

(4) シード情報を暗号化関数の鍵とし、固有情報を暗号化処理し、出力された情報を鍵情報とする方法。

【0055】

(5) DH (Diffie-Hellman) 鍵共有方式 (RFC 2631) に基づいて鍵情報を共有する方法。

【0056】

ただし、データ暗号化装置 102 だけが鍵情報を保持できればよいので、例えば、シード情報をデータ暗号化装置 102 の DH 鍵共有方式の秘密鍵とし、固有情報をデータ暗号化装置 102 の公開鍵とコンピュータシステムの固有の情報から得られる情報とする。

【0057】

上記の各方法は、固有情報とシード情報から鍵情報を生成する一例であって、本実施形態における鍵情報の生成方法は、2 入力関数 f 「鍵情報 = f (シード情報, 固有情報)」であればどのような関数でもよい。

【0058】

また、鍵情報と鍵情報検証情報とをセットで鍵情報として管理することで、鍵情報の正当性を検証することも可能である。なお、鍵情報検証情報は、一例として、鍵情報のハッシュ値が考えられる。

【0059】

<状態管理機能>

状態管理機能は、データ暗号化装置 102 の状態に関して、初期状態であるか否かを判断するものである。

【0060】

ここで、「初期状態」とは、鍵生成機能で鍵情報を生成するときに利用する鍵のシード情報がメモリ 111 に保持されていて鍵情報を生成可能な状態である場合に対応する。また、「初期状態でない」とは、シード情報をメモリ 111 に保持しておらず鍵情報を生成不可能な状態である場合に対応する。

【0061】

なお、状態管理機能では、シード情報がメモリ 111 に保持されていないと判断した場合に、シード情報を新たに生成し、生成したシード情報をメモリ 111 に保持させる。なお、シード情報は、データ暗号化装置 102 に固有の情報であり、データ暗号化装置 102 以外の装置からは知ることができない情報である。

【0062】

<データ暗号化装置 102 の動作について>

以下、図 2 を参照して、本実施形態におけるデータ暗号化装置 102 の動作を説明する。

【0063】

図 2 は、本実施形態における第 1 の制御処理プログラムの一例を示すフローチャートで

10

20

30

40

50

ある。なお、このフローチャートの処理は、CPU 106がメモリ 111に格納されるプログラムを実行することにより実現される。なお、図中、S 301～S 307は各ステップを示す。

【0064】

まず、ステップS 301において、CPU 106は状態管理機能により、データ暗号化装置102のメモリ 111内に保持されているシード情報の有無を検査する。そして、CPU 106は、シード情報がメモリ 111に保持されていないと判定した場合には、ステップS 302に処理を進める。ステップS 302で、CPU 106は、状態管理機能により、シード情報を新たに生成し、メモリ 111内に格納する。

【0065】

一方、ステップS 301で、CPU 106が、データ暗号化装置102のメモリ 111内にシード情報が保持されていると判定した場合、そのままステップS 302に処理を進める。

【0066】

次に、ステップS 303で、CPU 106は、認証機能により、コンピュータシステム100が正当であるか否かを認証する。CPU 106は、認証に成功するまで認証処理を繰り返す。

【0067】

そして、CPU 106は、コンピュータシステム100の認証に成功したと判定した場合には、ステップS 304に処理を進める。ステップS 304で、CPU 106は、コンピュータシステム100から固有情報を受信する。

【0068】

そして、CPU 106は鍵生成機能により、固有情報とシード情報から鍵情報を生成し、暗号・復号部109にセットする。なお、鍵情報として鍵情報検証情報をセットで管理している場合、生成した鍵情報の正当性を検証することが可能である。

【0069】

次に、ステップS 306において、CPU 106は状態管理機能によりデータ暗号化装置102の状態を監視する。そして、CPU 106は、鍵情報を保持していない等の初期状態となった場合、制御機能によりコンピュータシステム100とHDD 103間の情報の送受信を遮断するように制御する。なお、状態管理機能は、鍵情報の正当性を検証可能であって、鍵情報の正当性を検証できなかった場合、鍵情報を保持していないと判断することも可能である。

【0070】

一方、ステップS 306で、CPU 106は制御機能により、コンピュータシステム100から送信された情報がコマンド等の制御情報であるか、又はデータであるかを判断する。そして、コンピュータシステム100から送信された情報がデータであると判定した場合のみ、ステップS 307に処理を以降させ、暗号・復号部109を動作させて、該データを暗号化する。さらに、CPU 106は制御機能により、HDD 103から読み込んだ情報が応答等の制御情報であるか、又はデータであるかを判断し、データであると判定した場合のみ、ステップS 307に処理を以降させ、暗号・復号部109を動作させ復号する。なお、暗号・復号部109は、ステップS 305で生成した鍵情報を用いて、データの暗号化または復号を行う。

【0071】

以上の手順によって、HDD 103に保持されているデータを暗号化することを実現できる。

【0072】

<データの暗号化・復号化処理の詳細>

図2のステップS 306に示したデータの暗号化及び復号化に関して、図3，図4のデータのフローを例示して詳細に説明する。

【0073】

図3は、コンピュータシステム100から送信されるデータをHDD103に書き込む場合のデータフローを示す図である。

【0074】

図3に示すように、CPU106の制御機能は、コンピュータシステム100から実行可能な「コマンド」と「データ」からなる情報を受け取る。ここで、この「コマンド」はHDD103へのデータの書き込みに相当する制御情報であり、「データ」はHDD103に書き込まれるデータとする。

【0075】

CPU106の制御機能は、暗号・復号部109を動作させ、「データ」を暗号化する。そして、CPU106の制御機能は、「コマンド」と暗号化処理によって得られた「暗号化データ」からなる情報をHDD103に送信する。

10

【0076】

次に、CPU106の制御機能は、HDD103から、暗号化データがHDD103に書き込まれたことに応じて送信される「応答」を受け取り、制御情報である「応答」をそのままコンピュータシステム100へ送信する。

【0077】

図4は、コンピュータシステム100が、データをHDD103から読み込む場合のデータフローを示す図である。

【0078】

CPU106の制御機能は、コンピュータシステム100から実行可能な「コマンド」を受け取る。ここで、この「コマンド」はHDD103からのデータの読み込みに相当する制御情報である。

20

【0079】

CPU106の制御機能は、コンピュータシステム100から受信した「コマンド」をそのままHDD103に送信する。

【0080】

次に、CPU106の制御機能は、HDD103から、暗号化データがHDD103から読み込まれたことに応じて送信される「応答」と「暗号化データ」を受け取る。

【0081】

さらに、CPU106の制御機能は、暗号・復号部109を動作させ、HDD103から読み込んだ「暗号化データ」を復号化する。そして、CPU106の制御機能は、「応答」と「データ」（復号済）からなる情報をコンピュータシステム100へ送信する。

30

【0082】

なお、図3および図4に示したデータフローは、一例である。複数のインターフェースに係る具体的なデータフローは、コンピュータシステム100とデータ暗号化装置102間のインターフェースの仕様、およびデータ暗号化装置102とHDD103間のインターフェース仕様に依存する。

【0083】

例えば、「データ」がなく、「コマンド」と「応答」だけのデータフローも考えら得る。さらに、コンピュータシステム100とデータ暗号化装置102間のインターフェースとデータ暗号化装置102とHDD103間のインターフェースが異なる場合も考えられる。この場合、CPU106の制御機能は、データの暗号化復号処理に加えて、インターフェース仕様の変換処理を同時に行うことで実現可能である。

40

【0084】

なお、図3および図4で示したとおり、データ暗号化装置102において暗号化される情報は「データ」である。したがって、鍵情報を保持しない等、データ暗号化装置102が初期状態の場合、CPU106の制御機能は、コンピュータシステム100とHDD103間の送受信を遮断する情報を「データ」に限定することも可能である。

【0085】

また、上述のとおり、データ暗号化装置102におけるコンピュータシステム100の認

50

証方法はさまざまな方法を利用できる。

【0086】

したがって、ステップS303のコンピュータシステム100の認証時に、コンピュータシステム100から固有情報を受信することも可能である。例えば、コンピュータシステム100からデジタル署名と公開鍵証明書を受信して認証する認証方法の場合、公開鍵証明書をコンピュータシステム100の固有情報として利用することができる。このように、ステップS303において、コンピュータシステム100の固有情報を受信可能な場合、ステップS304を省略することも可能である。

【0087】

本実施形態は、コンピュータシステム100とHDD103をインターフェースを介して接続するデータ暗号化装置102であって、CPU106の制御により暗号・復号部109でHDD103に書き込むデータを暗号化するものである。本実施形態では、この構成によって、HDD103に記憶されるデータの機密性を保つことができる。

10

【0088】

特に暗号化または復号化に用いる鍵情報は、コンピュータシステム100の固有情報とデータ暗号化装置102に固有のシード情報から生成される。そのため、コンピュータシステム100とデータ暗号化装置102の異なる組から正当な鍵情報を生成することができない。

【0089】

さらに、コンピュータシステム100の固有情報の受信前にコンピュータシステム100を認証することによって、正当なコンピュータシステム100の固有情報の受信を実現している。

20

【0090】

従って、データ暗号化装置102とHDD103をセットで盗難されたとしても、HDD103内のデータの機密性を維持することができる。また、データ暗号化装置102は、状態管理機能によって、鍵情報に関する状態としてシード情報の有無を管理し、鍵情報を保持していない場合は自動的に鍵情報を生成するためのシード情報を生成するので、鍵情報の管理の自動化を実現している。

【0091】

<データ暗号化装置102の動作モード>

30

以下、データ暗号化装置102の動作モードについて、図5を用いて説明する。

【0092】

図5は、データ暗号化装置102の動作モードを説明する状態遷移図である。

【0093】

データ暗号化装置102の動作モードは、大きく分けて「遮断モード」と「起動モード」の2種類がある。また、「起動モード」には、「通常モード」と「バイパスモード」と「暗号・復号モード」が含まれるものとする。なお、データ暗号化装置102をいずれのモードにて動作させるかは、CPU106がメモリ111に記憶されたプログラムを実行することにより判断するものとする。

【0094】

データ暗号化装置102に電源が投入されると、データ暗号化装置102は、まず遮断モードS701に設定される。この遮断モードは、HDDコントローラ101が送信する如何なる情報もHDD103へ到達させないモードである。

40

【0095】

このとき、HDDコントローラ101からHDD103へのアクセスであるレジスタのリードライトは、全てデータ暗号化装置102に対して行われ、HDD103へのアクセスは遮断される。

【0096】

また、このとき使用可能なコマンドは、HDD103にアクセスするために使用する通常コマンド以外の、新たに定義した拡張コマンド（後述する図8）のみが使用可能である

50

。

【0097】

この遮断モードS701においてCPU106は、前述した認証機能のみが実行可能である。認証機能によりコンピュータシステム100が正当であると認証された場合にのみ、データ暗号化装置102は、遮断モードS701から通常モードS702に移行できる。

。

【0098】

なお、HDDコントローラ101が発行するコマンドがHDD103にて実行可能か不可能であるかは、データ暗号化装置102内のメモリ111に格納された参照データに基づいて判断される。データ暗号化装置102は、HDDコントローラ101が発行するコマンドを、図1に示したATAバスセクタ107を介してデバイスI/F108にて受信し、アドレス・データバス113を介してCPU106が認識する。そして、CPU106が、メモリ111内の参照データと比較し、コマンドがHDD103にて実行可能かを判断する。

10

【0099】

通常モードS702は、HDDコントローラ101がHDD103に対してアクセスを行うモードである。ただし、HDDコントローラ101が発行するコマンドは全てデータ暗号化装置102がHDD103にて実行可能か否かを判断し、実行可能なコマンド（図9）のみがHDD103へ渡される。それ以外のコマンドは、実行不可能なコマンドとしてHDD103に転送しないものとする。

20

【0100】

コンピュータシステム100から受信したコマンドが実行可能であるか不可能であるかの判断は、上述の遮断モードS701と同様であり、動作モードごとにメモリ111内の参照データを変更している。ただし、実行可能なコマンドは動作モード毎に異なる。

【0101】

また、通常モードS702において、CPU106により実行可能であると判断されたコマンドは、ホストI/F110に対してCPU106により設定される。そして、データ暗号化装置102により、ATAバスセクタ107を介してHDD103へ転送（発行）される。

【0102】

次に、HDD103に対するレジスタアクセスコマンド（後述する「PIO READ」タイプのコマンド）を受け取ると、データ暗号化装置102は動作モードを通常モードS702からバイパスモードS703へ移行させる。詳細は後述する。

30

【0103】

一方、データ暗号化装置102は、コンピュータシステム100から、HDD103に対するデータの格納、読み出しを示すDMA転送タイプのコマンドを受け取ると、動作モードを通常モードS702から暗号・復号モードS704へ移行させる。

【0104】

また、この通常モードS702で、特別に定義された拡張コマンドの内「CHANGE INTERCEPT」コマンド（図8）を受信すると、データ暗号化装置102は動作モードを通常モードS702から遮断モードS701へ移行させる。

40

【0105】

バイパスモードS703は、通常モードS702において、HDD103へのレジスタアクセス（「PIO READ」タイプのアクセス）行うときに実行されるモードである。このバイパスモードS703は、HDDコントローラ101のレジスタアクセスをHDD103へバイパスさせるモードである。HDD103のレジスタデータのコンピュータシステム100への転送完了後、データ暗号化装置102は動作モードをバイパスモードS703から通常モードS702へ移行させる。

【0106】

暗号・復号モードS704は、DMA転送によるHDD103へのデータ格納、読み出

50

し時にデータに対してデータを暗号化または復号化するモードである。データ暗号化装置102は、DMA転送が完了した時点で動作モードを暗号・復号モードS704から通常モードS702へ移行させる。

【0107】

＜ATAバスセクタ107の構成＞

以下、図6を参照して、図1に示したATAバスセクタ107の構成について説明する。

【0108】

図6は、図1に示したATAバスセクタ107の構成を説明するブロック図である。

【0109】

図6に示すように、HDDコントローラ101は、HDDコントローラサイド入出力信号801と接続され、信号の入出力が行われる。また、HDD103は、HDDサイド入出力信号802と接続されている。

【0110】

HDDコントローラサイド入出力信号801は、セクタ803を介してデバイスI/F108あるいはバイパス回路804に接続される。

【0111】

同様に、HDDサイド入出力信号802は、セクタ805を介して、HOST I/F110あるいはバイパス回路804に接続される。

【0112】

各セクタ803、805は、制御回路806を介してCPU106により制御される。

【0113】

HDDコントローラ101とHDD103は、バイパス回路804を介して接続されたり、暗号・復号部109を介してデータ転送されたり、あるいはCPU106を介して接続される。

【0114】

＜ATAバスセクタ107の動作＞

以下、図7を用いて、データ暗号化装置102の各動作モードにおける図6に示したATAバスセクタ107の動作について説明する。

【0115】

図7は、データ暗号化装置102の各動作モードにおける図6に示したATAバスセクタ107の動作について説明する図であり、各動作モードにおけるデータバスの接続関係および転送方向を示す。

【0116】

図7に示すように、太い線の矢印は、データの送受信行うPIO/DMAバスを示す。また、細い線の矢印は、動作設定、状態確認などで使用するレジスタ等のアクセスを示す。

【0117】

図7(a)を参照して、遮断モードにおけるATAバスセクタ107の動作について説明する。

【0118】

このとき、ATAバスセクタ107内のHDDコントローラサイド入出力信号801はデバイスI/F108に接続され、HDDサイド入出力信号802はHOST I/F110に接続される。

【0119】

これにより、相互認証が終了するまでHDDコントローラ101からHDD103へのいかなるアクセスも禁止される。

【0120】

図7(b)を参照して、通常モードにおけるATAバスセクタ107の動作について

10

20

30

40

50

説明する。

【0121】

通常モードでは、P I O / D M A バスは、デバイス I / F 1 0 8 と、ホスト I / F 1 1 0 に接続される。

【0122】

また、図7 (b) では、H D D コントローラ 1 0 1 から H D D 1 0 3 のレジスタへの書き込みアクセスが発行されると (「W」)、H D D コントローラ サイド 入出力信号 8 0 1 から、アクセスするレジスタの種類に応じて、アクセス先が変更されることを示す。例えば、デバイス I / F 1 0 8 内のレジスタだけに書き込まれたり、あるいは H D D サイド 入出力信号 8 0 2 にそのまま接続され H D D 1 0 3 内のレジスタだけに書き込まれたり、あるいは双方に書き込まれることを示す。例えば、H D D コントローラ 1 0 1 からパラメータを設定するレジスタにアクセスすると、データはデータ暗号化装置 1 0 2 と H D D 1 0 3 内の双方のレジスタに書き込まれる。

10

【0123】

レジスタリード (「R」) においても同様で、H D D 1 0 3 のデータがそのまま読み出せたり、ホスト I / F 1 1 0 で読まれたデータをデバイス I / F 1 0 8 を介して読み出したりすることを示す。

【0124】

図7 (c) を参照して、バイパスモードにおける A T A バスセクタ 1 0 7 の動作について説明する。

20

【0125】

バイパスモードにおいては、ホストサイドの入出力信号と、H D D サイド 入出力信号 8 0 2 は、直接接続される。一部のレジスタの書き込みアクセスに関しては、H D D 1 0 3 のレジスタと、デバイス I / F 1 0 8 内のレジスタに同じものが書かれる。

【0126】

<データ暗号化装置が遮断モードにて実行可能な拡張コマンド>

図8は、データ暗号化装置 1 0 2 が実行可能な拡張コマンドを示す図である。

【0127】

図8に示す拡張コマンドは、通常の H D D アクセスで使用する A T A コマンドとは異なり、データ暗号化装置 1 0 2 のみが処理可能なコマンドである。これらのコマンドは、図1に示したメモリ 1 1 1 内に実行可能な拡張コマンドとして登録されている。

30

【0128】

図8に示す拡張コマンドは、図5に示した遮断モード S 7 0 1 において、データ暗号化装置 1 0 2 が実行可能なコマンドである。

【0129】

図8において、コマンド名 1 0 0 1 は、動作可能なコマンドの名称を示す。タイプ 1 0 0 2 は、アクセスの種類を示す。例えば、「N o n D A T A」タイプはデータの転送を伴わないコマンドであり、ステータスの確認、遮断モードから通常モードへ移行などがある。「W R I T E」タイプ、「R E A D」タイプはデータの書き込み、読み出しを伴うコマンドであり、バージョン情報の取得、認証のチャレンジで使用する。

40

【0130】

<データ暗号化装置が通常モードにて実行可能な A T A コマンド>

図9は、データ暗号化装置 1 0 2 が通常モード S 7 0 2 において実行可能なコマンドを示す図である。なお、H D D コントローラ 1 0 1 から H D D 1 0 3 に対して転送可能なコマンドは、図9に示すコマンドに限定される。これは、データ暗号化装置 1 0 2 がコンピュータシステム 1 0 0 を正当なものと認証して通常モードにて動作する場合に限って、図9に示すコマンドが実行可能となることを意味する。このような構成とすることで、H D D 1 0 3 に対する不要なアクセスが防止されセキュリティを確保することができる。これらのコマンドは、図1に示したメモリ 1 1 1 内に A T A コマンドとして登録されている。

【0131】

50

図9において、コマンド名1101は、実行可能なコマンドの名称を示す。タイプ1102は、アクセスの種類を示す。「NONDATA」転送タイプはデータの転送を伴わないコマンドである。「PIO READ」転送タイプは、データの読み出しを伴うコマンドである。「DMA」転送（暗号・復号）タイプは、データの書き込み、読み出しを伴うコマンドである。

【0132】

なお、「PIO READ」転送タイプは、コンピュータシステム100内のメインメモリとHDD103との間のデータ転送を、コンピュータシステム100内のCPUが管理して行うタイプのコマンドである。

【0133】

一方、「DMA」転送タイプは、コンピュータシステム100内のRAMとHDD103との間のデータ転送を、コンピュータシステム100内のCPUを介さずに行うタイプのコマンドである。

【0134】

通常モードS702において、HDDコントローラ101からコマンドが発行されるとデータ暗号化装置102内部でコマンドを一旦保持し、CPU106がそのコマンドがHDD103にて実行可能かをチェックする。そして、HDD103にて実行可能なコマンド（図9に示すコマンド）のみが、HDD103へ送られる。実行不可能であると判断されたコマンド（図9に示す以外のコマンド）については、HDD103へは送られずにエラー（アボートエラー）としてHDDコントローラ101へ通知される。

【0135】

<コンピュータシステム100を認証する認証処理の詳細>

以下、図10、図11を用いてHDDコントローラ101とデータ暗号化装置102間の認証処理について説明を行う。なお、認証処理を行うケースとしては、データ暗号化装置102を初めてHDDコントローラ101に接続したケースと、データ暗号化装置102とHDDコントローラ101が予め接続されているケースの2種類がある。図10を用いてデータ暗号化装置102を初めてHDDコントローラ101に接続した設置時の状態での認証処理を説明する。

【0136】

図10は、本実施形態における第2の制御処理プログラムの一例を示すフローチャートであり、コンピュータシステム100に初めてデータ暗号化装置102が設置されたときのケースに対応する。なお、図10において、S1201～S1215は各ステップを示す。なお、このフローチャートにおいてデータ暗号化装置102のステップは、CPU106がメモリ111に格納されるプログラムを実行することにより実現される。また、HDDコントローラ101のステップは、HDDコントローラ101内の図示しないCPUがメモリに格納されるプログラムを実行することにより実現される。さらに、HDD103のステップは、HDD103内の図示しないCPUがメモリに格納されるプログラムを実行することにより実現される。

【0137】

ステップS1201において、コンピュータシステム100、データ暗号化装置102、HDD103の全てに電源が入力される。そして、ステップS1202において、データ暗号化装置102のCPU106は、データ暗号化装置102を遮断モードで起動する。

【0138】

また、HDDコントローラ101は、ステップS1203において、データ暗号化装置102がコンピュータシステム100に接続されているか否かの確認を行う。ここでは、コンピュータシステム100がデータ暗号化装置102に接続されているものとする。次に、ステップS1204において、HDDコントローラ101はデータ暗号化装置102に対して、「GET STATUS」コマンド（図8）を発行し、データ暗号化装置102の動作状態を認識する。初めてデータ暗号化装置102を設置したときには、未だ鍵情

10

20

30

40

50

報が生成されていないので、ステップS 1 2 0 5において、データ暗号化装置1 0 2のCPU 1 0 6は、未インストールのステータスをHDDコントローラ1 0 1に戻す。

【0 1 3 9】

未インストール状態を認識した場合、HDDコントローラ1 0 1は、ステップS 1 2 0 6において、インストールの実行コマンド「INSTALL」をデータ暗号化装置1 0 2に送信する。

【0 1 4 0】

これに応じて、データ暗号化装置1 0 2は、ステップS 1 2 0 7において、鍵情報を生成するためのシード情報を生成する。

【0 1 4 1】

また、ステップS 1 2 0 8において、HDDコントローラ1 0 1は、コンピュータシステム1 0 0の固有情報をデータ暗号化装置1 0 2に送信する。

【0 1 4 2】

固有情報を受信したデータ暗号化装置1 0 2のCPU 1 0 6は、ステップS 1 2 0 9において、固有情報をRAM 1 1 2に保持する。

【0 1 4 3】

次に、ステップS 1 2 1 0において、データ暗号化装置1 0 2のCPU 1 0 6は、シード情報と固有情報に基づいて、鍵情報を生成し、メモリ1 1 1に書き込む。鍵情報の生成が終了すると、ステップS 1 2 1 1において、データ暗号化装置1 0 2のCPU 1 0 6は、鍵情報の生成が終了したことを示すステータスをHDDコントローラ1 0 1に返信する。

【0 1 4 4】

これを受けて、HDDコントローラ1 0 1は、データ暗号化装置1 0 2にて鍵情報が生成されたことを認識する。そして、ステップS 1 2 1 2において、「CHANGE NORMAL」コマンド（通常モードへ移行するコマンド）を、データ暗号化装置1 0 2に送信する。

【0 1 4 5】

これを受けて、データ暗号化装置1 0 2のCPU 1 0 6は、鍵情報の生成が終わったことで、コンピュータシステム1 0 0が正当なものと認証されたとみなす。そして、ステップS 1 2 1 3において、データ暗号化装置1 0 2の動作モードを遮断モードから通常モードへ移行させる。通常モード移行後、ステップS 1 2 1 4において、データ暗号化装置1 0 2のCPU 1 0 6は、通常モードに移行した旨を示すステータスをHDDコントローラ1 0 1に戻す。

【0 1 4 6】

これを受け取った後、HDDコントローラ1 0 1は、ステップS 1 2 1 5において、ATAの各種コマンドをデータ暗号化装置1 0 2に送信する。そして、データ暗号化装置1 0 2は、HDDコントローラ1 0 1から受信したATAコマンドに基づいて制御を行う。

【0 1 4 7】

以下、図1 3を用いてデータ暗号化装置1 0 2とHDDコントローラ1 0 1が予め接続されているケースにおける認証処理を説明する。

【0 1 4 8】

図1 1 A、図1 1 Bは、本実施形態における第3の制御処理プログラムの一例を示すフローチャートであり、コンピュータシステム1 0 0にデータ暗号化装置1 0 2が予め接続されているケースに対応する。なお、図1 1において、S 1 3 0 1～S 1 3 2 5は各ステップを示す。なお、このフローチャートにおいてデータ暗号化装置1 0 2のステップは、CPU 1 0 6がメモリ1 1 1に格納されるプログラムを実行することにより実現される。また、HDDコントローラ1 0 1のステップは、HDDコントローラ1 0 1内の図示しないCPUがメモリに格納されるプログラムを実行することにより実現される。さらに、HDD 1 0 3のステップは、HDD 1 0 3内の図示しないCPUがメモリに格納されるプロ

10

20

30

40

50

グラムを実行することにより実現される。

【0149】

なお、ここでは、認証方法として、チャレンジアンドレスポンス認証方法を用いる例を説明するが、認証方法は他の方法であっても良い。

【0150】

ステップS1301において、コンピュータシステム100、データ暗号化装置102、HDD103の全てに電源が入力される。ステップS1302において、データ暗号化装置102のCPU106は、データ暗号化装置102を遮断モードで起動する。

【0151】

また、HDDコントローラ101は、ステップS1303において、データ暗号化装置102がコンピュータシステム100に接続されているか否かの確認を行う。ここでは、コンピュータシステム100がデータ暗号化装置102に接続されているものとする。次に、ステップS1304において、HDDコントローラ101はデータ暗号化装置102に対して、「GET STATUS」コマンド(図8)を発行し、データ暗号化装置102の動作状態を認識する。ここでは、既にデータ暗号化装置102をコンピュータシステム100に接続済みであり鍵情報が生成済なので、データ暗号化装置102のCPU106は、ステップS1305において、インストール済みのステータスをHDDコントローラ101に戻す。

10

【0152】

インストール済み状態を認識した場合、HDDコントローラ101は、ステップS1306, S1307において、チャレンジの実行を示すチャレンジコマンド「SEND CHA1」、チャレンジ乱数をデータ暗号化装置102に送信して、認証確認に移る。

20

【0153】

これを受けたデータ暗号化装置102のCPU106は、ステップS1308において、HDDコントローラ101へステータスを返信する。

【0154】

続いて、ステップS1309において、HDDコントローラ101は、レスポンス要求コマンド「REQUEST CHA1」をデータ暗号化装置102に送信する。これを受けたデータ暗号化装置102のCPU106は、ステップS1310において、上述のチャレンジ乱数に対応するレスポンスをHDDコントローラ101へ返信する。さらに、ステップS1311において、データ暗号化装置102のCPU106は、ステータスをHDDコントローラ101へ返信する。

30

【0155】

上記レスポンスを受けて、HDDコントローラ101はレスポンスが正しいか判断し、正しいければ、ステップS1315に処理を移行させ、データ暗号化装置102からHDDコントローラ101へのチャレンジの実行に移る。

【0156】

ステップS1312において、HDDコントローラ101は、チャレンジ実行の要求を行うコマンド「REQUEST CHA2」をデータ暗号化装置102に送信する。

【0157】

これを受けたデータ暗号化装置102のCPU106は、ステップS1313, S1314において、チャレンジ乱数、ステータスをHDDコントローラ101へ送信する。

40

【0158】

これを受けたHDDコントローラ101は、ステップS1315, S1316において、レスポンスの実行を要求するコマンド、レスポンスをデータ暗号化装置102に送信する。

【0159】

このレスポンスを受けてデータ暗号化装置102は、レスポンスが正しいか判断し、ステータスを返信する。正しいければ、認証終了となり、ステップS1317に処理を移し、鍵情報の作成に移る。なお、以下のステップS1318~S1325は、図10のステッ

50

プ S 1 2 0 8 ～ S 1 2 1 5 と同一であるので説明は省略する。

【0160】

＜起動モードにおける動作の詳細＞

図5で示したように、遮断モード S 7 0 1 で認証が終了すると、通常モード S 7 0 2 に移行する。以下、図12～図15を用いて、起動モードで実行可能なコマンドの詳細シーケンスを示す。

【0161】

起動モードで実行可能なコマンドは、図9に示したものであり、データの転送タイプで3つにわけられる。データ転送を伴わない「NonDATA」転送タイプ、「PIO READ」転送タイプ、「DMA」転送（暗号・復号）タイプの3つである。順に説明する。

10

【0162】

（1）NonDATA転送タイプ

「NonDATA転送タイプ」のコマンドの実行は、2ステップの処理で行われる。まず、HDDコントローラ101は、実行するコマンドに必要なパラメータを設定する。設定されたパラメータは、HDD103のコマンドブロック内の関連するレジスタ（T/Fレジスタ、I/Oレジスタやコマンドブロックレジスタなどとも呼ばれる）に書き込まれる。

【0163】

次に、HDDコントローラ101は、データ暗号化装置102のコマンドレジスタに「NonDATA」転送タイプのコマンドコードを書き込む。これにより、HDD103は、（一旦、データ暗号化装置102を介して）コマンドを実行する。

20

【0164】

なお、パラメータ設定を行うレジスタやコマンドコードを書き込むレジスタには、HDDコントローラ101から書き込む場合と、読み出す場合で、意味の異なるものがある。ERROR/FEATURESレジスタや、STATUS/COMMANDレジスタなどで、読み出し時にはHDDのエラーやステータスを示すが、書き込み時にはコマンドの実行を示す。

【0165】

「NonDATA」転送タイプのコマンドとしては、RECALIBRATE、SEEKなどのコマンドがある。

30

【0166】

RECALIBRATEコマンドは、HDD103のREZERO動作を行うもので、SEEKコマンドは、HDDの指定されたトラックへのシークおよびヘッドの選択が行われる。

【0167】

以下、図12のフローチャートを用いて説明する。

【0168】

図12は、本実施形態における第4の制御処理プログラムの一例を示すフローチャートであり、「NonDATA」転送タイプのコマンドシーケンスに対応する。なお、図中、S1401～S1411は各ステップを示す。なお、このフローチャートにおいてデータ暗号化装置102のステップは、CPU106がメモリ111に格納されるプログラムを実行することにより実現される。また、HDDコントローラ101のステップは、HDDコントローラ101内の図示しないCPUがメモリに格納されるプログラムを実行することにより実現される。さらに、HDD103のステップは、HDD103内の図示しないCPUがメモリに格納されるプログラムを実行することにより実現される。

40

【0169】

まず、通常モードにおいて、HDDコントローラ101は、「NonDATA」転送タイプのコマンドの発行を行う場合、ステップS1401で、HDD103にアクセスするためにパラメータ設定を行う。パラメータ設定とは、データ暗号化装置102が有するレ

50

ジスタとHDD103が有するレジスタの両方にデータ転送を実行するためのパラメータを設定する動作である。

【0170】

続いて、ステップS1402において、HDDコントローラ101は、データ暗号化装置102が有するコマンドレジスタに、HDD103にて実行させるATAコマンド（NonDATA転送タイプのコマンド）を発行する。HDDコントローラ101からNonDATA転送タイプのATAコマンドを受信したデータ暗号化装置102は、デバイスI/F108のレジスタにATAコマンドを設定する。

【0171】

そして、ステップS1403において、データ暗号化装置102のCPU106は、コマンドレジスタに設定されたコマンドがHDD103にて実行可能なコマンドであるか否かの判断を行う。そして、実行可能なコマンド（メモリ111内の参照データ内に登録されているコマンド（図9））のみHDD103のコマンドレジスタに設定を行う（転送する）。即ち「NonDATA」転送のコマンドは、一旦、データ暗号化装置102で実行可能か否かが確認され、実行可能なコマンドのみHDD103へ転送される。ここでは、NonDATAタイプのATAコマンドはHDD103にて実行可能と判断されデータ暗号化装置102からHDD103に転送されるものとする。

【0172】

するとステップS1404において、HDD103は、データ暗号化装置102から転送されたATAコマンドを解釈して実行し、コマンド処理が終了する。そして、HDD103は、ステップS1405において、割り込み信号をデータ暗号化装置102に出力する。この割り込み信号は、データ暗号化装置102にだけに出力される。この割り込み信号を受けたデータ暗号化装置102のCPU106は、ステップS1406において、HDD103のレジスタから、ステータス、エラーなどの情報を読み出す。

【0173】

HDD103のレジスタがデータ暗号化装置102により読まれると、ステップS1407において、HDD103は割り込み信号を元に戻す（クリアする）。

【0174】

次に、ステップS1408において、データ暗号化装置102のCPU106は、HDD103のレジスタから読み出したHDD103のステータス、エラーのデータをデータ暗号化装置102のレジスタに設定する。そして、ステップS1409において、データ暗号化装置102のCPU106は、HDDコントローラ101へ割り込み信号を送信する。

【0175】

HDDコントローラ101は、データ暗号化装置102から割り込み信号が入力されたので、ステップS1410において、データ暗号化装置102のレジスタから、ステータス、エラー等の情報を読み出す。

【0176】

これに応じて、ステップS1411において、データ暗号化装置102のCPU106は、割り込み信号を元に戻し（クリアし）、「Non Data」転送タイプのコマンドが終了する。

【0177】

（2）PIO READ転送タイプ

以下、図13を用いて、「PIO READ」転送タイプのコマンドのフローについて説明する。

【0178】

通常モードで実行可能な「PIO READ」転送タイプのコマンドとしては、図9に示したように「IDENTIFY DEVICE」コマンドがある。「IDENTIFY DEVICE」コマンドを実行すると、HDD103のパラメータ情報（512バイト）を読み出すことができる。パラメータ情報としては、HDD103が有するシリンダ数

10

20

30

40

50

、ヘッド数、HDD103のシリアル番号、などのHDD103に固有の情報である。このHDD103に固有の情報は、HDDコントローラ101からHDD103へ書き込まれたデータとは異なる。即ち、HDD103に固有の情報は暗号化されていないデータである。

【0179】

図13は、本実施形態における第5の制御処理プログラムの一例を示すフローチャートであり、「PIO READ」転送タイプのコマンドシーケンスに対応する。なお、図13において、S1501～S1518は各ステップを示す。なお、このフローチャートにおいてデータ暗号化装置102のステップは、CPU106がメモリ111に格納されるプログラムを実行することにより実現される。また、HDDコントローラ101のステップは、HDDコントローラ101内の図示しないCPUがメモリに格納されるプログラムを実行することにより実現される。さらに、HDD103のステップは、HDD103内の図示しないCPUがメモリに格納されるプログラムを実行することにより実現される。

10

【0180】

まず、通常モードにおいて、HDDコントローラ101は、「PIO READ」転送タイプのコマンドの発行を行う場合、ステップS1501で、レジスタにHDD103にアクセスするためのパラメータ設定を行う。パラメータ設定は、データ暗号化装置102とHDD103の両方のレジスタに設定される。

【0181】

続いて、ステップS1502において、HDDコントローラ101は、データ暗号化装置102が有するコマンドレジスタに、HDD103にて実行させるATAコマンド（PIO READ転送タイプのコマンド）を発行する。HDDコントローラ101からPIO READ転送タイプのATAコマンドを受信したデータ暗号化装置102は、デバイスI/F108のレジスタにATAコマンドを設定する。

20

【0182】

そして、ステップS1503において、データ暗号化装置102のCPU106は、コマンドレジスタに設定されたコマンドがHDD103にて実行可能なコマンドであるか否かの判断を行う。そして、実行可能なコマンド（メモリ111内の参照データ内に登録されているコマンド（図9））のみHDD103のコマンドレジスタに設定を行う（転送する）。即ち「PIO READ」転送のコマンドは、一旦、データ暗号化装置102で実行可能か否かが確認され、実行可能なコマンドのみHDD103へ転送される。ここでは、PIO READタイプのATAコマンドはHDD103にて実行可能と判断されデータ暗号化装置102からHDD103に転送されるものとする。

30

【0183】

ステップS1504において、HDD103は、データ暗号化装置102から転送されたATAコマンドを解釈して実行する。例えば、「IDENTIFY DEVICE」コマンドであると、HDD103内のセクタバッファに要求されたパラメータ情報を入れて、レジスタに発行されたコマンドに対するステータスを書き込む。そして、ステップS1505において、HDD103は、割り込み信号をデータ暗号化装置102に出力する。

【0184】

この割り込み信号を受信したデータ暗号化装置102のCPU106は、ステップS1506において、HDD103のレジスタを読みだし、HDD103のステータスを確認する。HDD103のレジスタがデータ暗号化装置102により読まれると、HDD103は、ステップS1507において、割り込み信号を元に戻す（クリアする）。

40

【0185】

次に、ステップS1508において、データ暗号化装置102のCPU106は、データ暗号化装置102の動作モードを通常モードからバイパスモードへ移行させるための設定をATAバスセクタ107に対して行う。バイパスモード設定が終了すると、ステップS1509において、データ暗号化装置102のCPU106は、HDDコントローラ101へ割り込み信号を出力し、HDD103の準備ができていることを通知する。

50

【0186】

この割り込み信号を受けたHDDコントローラ101は、ステップS1510において、HDD103レジスタからHDD103のステータス・エラー等の情報を読み出す。ここで、HDD103のスタートレジスタから情報が読み出されたことを、データ暗号化装置102が認識し、ステップS1511において、割り込み信号をHDDコントローラ101に出力する。

【0187】

その後、ステップS1512において、HDDコントローラ101は、HDD103内のセクタバッファに設定されたデータ（パラメータ情報等）を読み出す。

【0188】

そして、所定数のデータの読み出しが終了すると、データ暗号化装置102のCPU106がこれを監視し、ステップS1514において、バイパスモードが終了するようにATAバスセクタ107に設定する。

【0189】

バイパスモードが終了すると、ステップS1515において、データ暗号化装置102のCPU106は、ステータスとエラーの状態をデータ暗号化装置102のレジスタをセットする。さらに、データ暗号化装置102のCPU106は、ステップS1516において、HDDコントローラ101へ割り込み信号を出力する。

【0190】

HDDコントローラ101は、データ暗号化装置102から割り込み信号が入力されたので、ステップS1517において、データ暗号化装置102のステータスとエラーレジスタを読み出す。

【0191】

これに応じてデータ暗号化装置102のCPU106は、ステップS1518において、割り込み信号を元に戻し（クリアし）、「PIO READ」転送タイプのコマンドが終了する。

【0192】

(3) DMA転送タイプ

続いて、図14を用いてHDD103へのデータの書き込み、読み出しを行うDMA転送について説明する。

【0193】

DMA転送としては、HDD103からデータを読み出す「READ DMA」と、HDD103へデータを書き込む「WRITE DMA」の2種類がある。「WRITE DMA」時には、データ暗号化装置102でデータの暗号化を行い、「READ DMA」時には、データの復号化を行う。

【0194】

図14は、本実施形態における第6の制御処理プログラムの一例を示すフローチャートであり、DMA転送タイプのコマンドシーケンスに対応する。なお、図中、S1601～S1615は各ステップを示す。なお、このフローチャートにおいてデータ暗号化装置102のステップは、CPU106がメモリ111に格納されるプログラムを実行することにより実現される。また、HDDコントローラ101のステップは、HDDコントローラ101内の図示しないCPUがメモリに格納されるプログラムを実行することにより実現される。さらに、HDD103のステップは、HDD103内の図示しないCPUがメモリに格納されるプログラムを実行することにより実現される。

【0195】

まず、通常モードにおいて、HDDコントローラ101は、DMA転送タイプのコマンドの発行を行う場合、ステップS1601で、HDD103にアクセスするためにパラメータ設定を行う。

【0196】

続いて、ステップS1602において、HDDコントローラ101は、データ暗号化装

10

20

30

40

50

置102が有するコマンドレジスタに、HDD103にて実行させるATAコマンド（DMA転送タイプのコマンド）を発行する。HDDコントローラ101からDMA転送タイプのATAコマンドを受信したデータ暗号化装置102は、デバイスI/F108のレジスタにATAコマンドを設定する。

【0197】

そして、ステップS1603において、データ暗号化装置102のCPU106は、コマンドレジスタに設定されたコマンドがHDD103にて実行可能なコマンドであるか否かの判断を行う。そして、実行可能なコマンド（メモリ111内の参照データ内に登録されているコマンド（図9））のみHDD103のコマンドレジスタに設定を行う（転送する）。即ち、DMA転送のコマンドは、一旦、データ暗号化装置102で実行可能か否かが確認され、実行可能なコマンドのみHDD103へ転送される。ここでは、DMA転送タイプのATAコマンドはHDD103にて実行可能と判断され、データ暗号化装置102からHDD103に転送されるものとする。

10

【0198】

すると、HDD103はDMA転送の準備を行い、準備が終了すると、ステップS1604において、データ暗号化装置102へDMA転送要求信号を出力する。

【0199】

データ暗号化装置102のCPU106は、HDD103からDMA転送要求信号を受け取ると、ステップS1605において、暗号・復号部109が暗号化を行うか復号化を行うかの設定を行う。CPU106は、HDDコントローラ101が発行したコマンド名がREAD__DMAであれば暗号・復号部109に復号化を行うよう設定し、WRITE__DMAであれば暗号・復号部109に暗号化を行うよう設定する。

20

【0200】

続いて、データ暗号化装置102のCPU106は、ステップS1606において、DMA転送要求をHDDコントローラ101へ出力する。

【0201】

その後、ステップS1607において、HDDコントローラ101とHDD103は、データ暗号化装置102を介してDMA転送を行う。なお、DMA転送時に、データ暗号化装置102の暗号・復号部109は、DMA転送されるデータの暗号化あるいは復号化を実行する。

30

【0202】

そして、所定データ数のDMA転送が終了すると、ステップS1607において、HDD103は、割り込み信号をデータ暗号化装置102へ出力する。

【0203】

この割り込み信号を受信したデータ暗号化装置102のCPU106は、HDD103のステータスレジスタを確認する。これに応じて、HDD103は、ステップS1610において、割り込み信号を元に戻す（クリアする）。

【0204】

これに応じて、データ暗号化装置102のCPU106は、ステップS1611で、HDD103からHDDコントローラ101へのデータのDMA転送を停止させる。DMA転送が終了すると、データ暗号化装置102のCPU106は、内部の設定を行いデータ暗号化装置102の状態を暗号・復号モードから通常モードに移行させる。

40

【0205】

次に、ステップS1612において、データ暗号化装置102のCPU106は、ステップS1609でHDD103のステータスレジスタから読み出したステータス、エラーの状態を示す情報を、データ暗号化装置102のレジスタに記憶させる。さらにステップS1613において、データ暗号化装置102のCPU106は、HDDコントローラ101へ割り込み信号を送信する。

【0206】

HDDコントローラ101は、データ暗号化装置102から割り込み信号が入力された

50

ので、ステップS1614において、データ暗号化装置102のレジスタに記憶されたHDD103のステータス、エラーの情報を読み出す。

【0207】

これに応じて、データ暗号化装置102のCPU106は、ステップS1615において、割り込み信号を元に戻し（クリアし）、DMA転送タイプのコマンドが終了する。

【0208】

（4）PIO WRITEタイプ

続いて、図15を用いてHDDへのデータの書き込みを行う「PIO WRITE」転送タイプのコマンドを扱う処理について説明する。

【0209】

一般的なATAコマンドには、HDDへのデータ書き込みコマンドとして、「WRITE MULTIPLE」コマンド等の「PIO WRITE」転送タイプのコマンドがある。しかし、本実施形態では、HDD103に対するデータの書き込みを制限する。そのため、使用可能なコマンド（HDD103にて実行可能なコマンド）に「WRITE MULTIPLE」コマンド等の「PIO WRITE」転送タイプのコマンドは認めていない。即ち、メモリ111内の参照データ内に使用可能なATAコマンドとして登録していない。

【0210】

このため、HDDコントローラ101により「WRITE MULTIPLE」コマンド等の「PIO WRITE」転送タイプコマンドが発行されても、データ暗号化装置102のCPU106は、HDD103にて実行不可能と判断し、HDD103へはコマンドを転送しない。

【0211】

図15は、本実施形態における第7の制御処理プログラムの一例を示すフローチャートであり、「PIO WRITE」転送タイプのコマンドシーケンスに対応する。なお、図15において、S1701～S1706は各ステップを示す。なお、このフローチャートにおいてデータ暗号化装置102のステップは、CPU106がメモリ111に格納されるプログラムを実行することにより実現される。また、HDDコントローラ101のステップは、HDDコントローラ101内の図示しないCPUがメモリに格納されるプログラムを実行することにより実現される。さらに、HDD103のステップは、HDD103内の図示しないCPUがメモリに格納されるプログラムを実行することにより実現される。

【0212】

まず、通常モードにおいて、HDDコントローラ101は、「PIO WRITE」転送タイプのコマンドの発行を行う場合、ステップS1701で、レジスタにHDD103にアクセスするためのパラメータ設定を行う。パラメータ設定は、データ暗号化装置102とHDD103の両方のレジスタに設定される。

【0213】

続いて、ステップS1702において、HDDコントローラ101は、データ暗号化装置102が有するコマンドレジスタに、HDD103にて実行させるATAコマンド（「PIO WRITE」転送タイプのコマンド）を発行する。HDDコントローラ101からPIO WRITE転送タイプのATAコマンドを受信したデータ暗号化装置102は、デバイスI/F108のレジスタにATAコマンドを設定する。

【0214】

そして、ステップS1703において、データ暗号化装置102のCPU106は、コマンドレジスタに設定されたコマンドがHDD103にて実行可能なコマンドであるか否かの判断を行う。そして、実行可能なコマンド（メモリ111内の参照データ内に登録されているコマンド（図9））のみHDD103のコマンドレジスタに設定を行う（転送する）。即ち、「PIO WRITE」転送のコマンドは、データ暗号化装置102で実行不可能なコマンドであると確認され、HDD103へは転送されない。

【0215】

ステップS1703において、データ暗号化装置102のCPU106は、コマンドエラーである旨の情報をデータ暗号化装置102のレジスタに設定して、ステップS1704において、HDDコントローラ101へ割り込み信号を送信する。

【0216】

HDDコントローラ101は、データ暗号化装置102から割り込み信号が入力されたので、ステップS1705において、データ暗号化装置102のステータス、エラーのレジスタを読み出す。これにより、HDDコントローラ101は、コマンドエラーであることを確認できる。

【0217】

そしてステップS1706において、データ暗号化装置102のCPU106は、割り込み信号を元に戻し（クリアし）、「PIO WRITE」転送タイプのコマンドがエラー終了する。

【0218】

例えば、コンピュータシステム100をMFPとすると、上述の「PIO WRITE」転送タイプのコマンドは、MFPでは標準で使用されない。よって、図15に示したように、MFPが標準で使用しないコマンド（例えば、「PIO WRITE」転送タイプのコマンド）が不正に発行された場合、HDD103への転送を禁止する。この構成により、データが暗号化されずにバイパスしてHDD103へ転送されてしまうことを確実に防止することができる。

【0219】

よって、本実施形態の構成では、HDD103とデータ暗号化装置102をセットで盗難され、他のコンピュータシステムに接続された場合でも、データの漏洩を防止することができる。

【0220】

なお、本実施形態では、一例として「PIO WRITE」転送タイプのコマンドを、HDD103への転送を禁止するコマンドとして説明した。しかし、データ暗号化装置102のCPU106は、メモリ111内の参照データ（図9）にATAコマンドとして登録されていないコマンドは、全て通常モードでは、実行不可能なコマンドとして、HDD103への転送を禁止するように制御する。これによりHDD103のデータセキュリティを確保することができる。

【0221】

なお、メモリ111内の参照データに登録されているコマンド、登録されていないコマンドは、それぞれ上述した例（図8，図9）に限られるものではない。

【0222】

以上説明したように、本実施形態のデータ暗号化装置102は、コンピュータシステムおよび外部記憶装置間をブリッジするものである。そして、CPU106の制御の元、暗号・復号部109で、HDD103に書き込むデータを暗号化することによって、HDD103のデータの機密性を維持することを実現している。特に、暗号化または復号に用いる鍵情報は、コンピュータシステムの固有情報とデータ暗号化装置102の固有情報から生成されるため、コンピュータシステムとデータ暗号装置の異なる組から正当な鍵情報を生成することができず、高い機密性を実現可能である。

【0223】

また、コンピュータシステム100がHDD103にアクセス前に、コンピュータシステム100とデータ暗号化装置102との認証を設け、認証が正常に終了しないとHDD103にアクセスできない構成となっている。

【0224】

また、認証終了後、HDD103にアクセスする際にも、コンピュータシステム100が発行するコマンドは全てデータ暗号化装置102が認識する。データ暗号化装置102のCPU106は、コマンドが実行可能であるか判断し、実行するコマンドを制限し、不

10

20

30

40

50

要なHDD103へのアクセスを防止している。

【0225】

さらに、データ暗号化装置102は、HDDコントローラ101とHDD103に対するこれらの通信、データの送受信を全て標準インタフェースを介して実行することが可能であり、追加の信号線を必要としない。即ち、コンピュータシステムや外部記憶装置の仕様を変更する必要がない。

【0226】

以上のような構成により、コンピュータシステムと外部記憶装置の間に挿入して、データの暗号化を行うデータ暗号化装置において、データのセキュリティを適切に保つことができる等の効果を奏する。

10

【0227】

従って、データ暗号化装置と外部記憶装置のセットで盗難された場合にも高度に機密性を維持可能なデータ暗号化記憶システムを、既存のコンピュータシステム及び外部記憶装置の仕様を変更することなく、低コストで構築することができる等の効果を奏する。

【0228】

なお、上述した図8、図9で示した各種コマンドの構成及びその内容はこれに限定されるものではなく、用途や目的に応じて、様々な構成や内容で構成されることは言うまでもない。

【0229】

以上、一実施形態について示したが、本発明は、例えば、システム、装置、方法、プログラムもしくは記憶媒体等としての実施態様をとることが可能である。具体的には、複数の機器から構成されるシステムに適用しても良いし、また、一つの機器からなる装置に適用しても良い。

20

【0230】

以下、図16に示すメモリマップを参照して、本発明に係るデータ暗号化装置で読み取り可能な各種データ処理プログラムを格納する記憶媒体のメモリマップの構成について説明する。

【0231】

図16は、本発明に係るデータ暗号化装置で読み取り可能な各種データ処理プログラムを格納する記憶媒体（記録媒体）のメモリマップを説明する図である。

30

【0232】

なお、特に図示しないが、記憶媒体に記憶されるプログラム群を管理する情報、例えばバージョン情報、作成者等も記憶され、かつ、プログラム読み出し側のOS等に依存する情報、例えばプログラムを識別表示するアイコン等も記憶される場合もある。

【0233】

さらに、各種プログラムに従属するデータも上記ディレクトリに管理されている。また、各種プログラムをコンピュータにインストールするためのプログラムや、インストールするプログラムが圧縮されている場合に、解凍するプログラム等も記憶される場合もある。

【0234】

本実施形態における図2、図10、図11A、図11B、図12、図13、図14、図15に示す機能が外部からインストールされるプログラムによって、ホストコンピュータにより遂行されていてもよい。そして、その場合、CD-ROMやフラッシュメモリやFD等の記憶媒体により、あるいはネットワークを介して外部の記憶媒体から、プログラムを含む情報群を出力装置に供給される場合でも本発明は適用されるものである。

40

【0235】

以上のように、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給する。そして、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、本発明の目的が達成されることは言うまでもない。

50

【0236】

この場合、記憶媒体から読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【0237】

従って、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、OSに供給するスクリプトデータ等、プログラムの形態を問わない。

【0238】

プログラムを供給するための記憶媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、MO、CD-ROM、CD-R、CD-RW、磁気テープ、不揮発性のメモ리카ード、ROM、DVDなどを用いることができる。

【0239】

この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【0240】

その他、プログラムの供給方法としては、クライアントコンピュータのブラウザを用いてインターネットのホームページに接続し、該ホームページから本発明のプログラムそのものをハードディスク等の記憶媒体にダウンロードすることによっても供給できる。また、該ホームページから圧縮され自動インストール機能を含むファイルをハードディスク等の記憶媒体にダウンロードすることによっても供給できる。また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるWWWサーバやFTPサーバ等も本発明の請求項に含まれるものである。

【0241】

また、本発明のプログラムを暗号化してCD-ROM等の記憶媒体に格納してユーザに配布する。さらに、所定の条件をクリアしたユーザに対し、インターネットを介してホームページから暗号化を解く鍵情報をダウンロードさせる。さらに、その鍵情報を使用することにより暗号化されたプログラムを実行してコンピュータにインストールさせて実現することも可能である。

【0242】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、以下のような構成も含まれることは言うまでもない。例えば、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているOS（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0243】

さらに、記憶媒体から読み出されたプログラムコードを、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込む。そして、該メモリに書き込まれたプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0244】

また、本発明は、複数の機器から構成されるシステムに適用しても、1つの機器からなる装置に適用してもよい。また、本発明は、システムあるいは装置にプログラムを供給することによって達成される場合にも適用できることは言うまでもない。この場合、本発明を達成するためのソフトウェアによって表されるプログラムを格納した記憶媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果

10

20

30

40

50

を享受することが可能となる。

【0245】

本発明は上記実施形態に限定されるものではなく、本発明の趣旨に基づき種々の変形（各実施形態の有機的な組合せを含む）が可能であり、それらを本発明の範囲から排除するものではない。

【0246】

本発明の様々な例と実施形態を示して説明したが、当業者であれば、本発明の趣旨と範囲は、本明細書内の特定の説明に限定されるのではない。

【0247】

なお、上述した実施形態の各変形例を組み合わせた構成も全て本発明に含まれるものである。 10

【0248】

以上示したように、本実施形態によれば、記憶装置（HDD103）と記憶装置を制御する制御装置（HDDコントローラ101）の間に接続され、記憶装置と制御装置との間で転送されるデータのセキュリティを適切に保つデータ処理装置（記録データ暗号化装置102）を提供することができる等の効果を奏する。

【0249】

本発明の各工程は、ネットワーク又は各種記憶媒体を介して取得したソフトウェア（プログラム）をパソコン（コンピュータ）等の処理装置（CPU、プロセッサ）にて実行することも実現できる。 20

【0250】

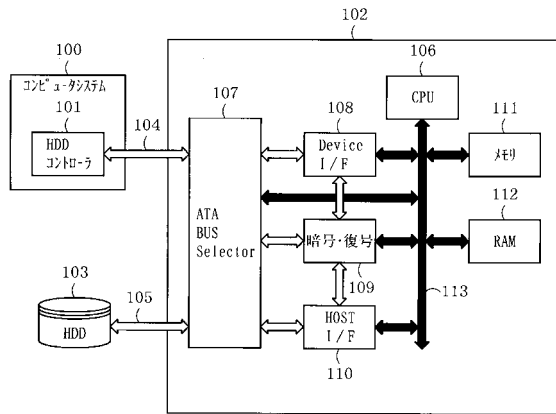
本発明は上記実施形態に限定されるものではなく、本発明の趣旨に基づき種々の変形（各実施形態の有機的な組合せを含む）が可能であり、それらを本発明の範囲から除外するものではない。

【符号の説明】

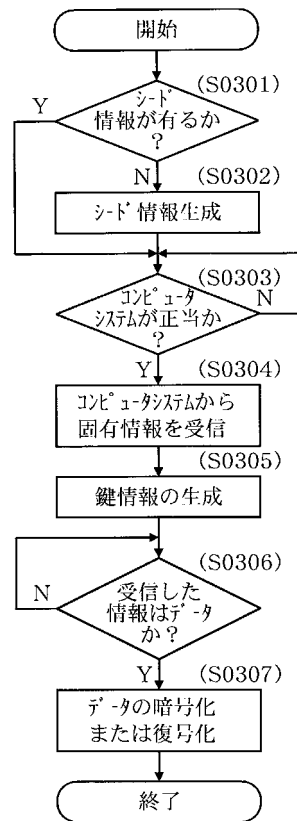
【0251】

- 100 コンピュータシステム
- 101 HDDコントローラ
- 102 データ暗号化装置
- 102 記録データ暗号化装置
- 103 外部記憶装置（HDD）
- 105 ATAバス
- 106 CPU
- 107 ATAバスセクタ
- 109 暗号・復号部
- 111 メモリ
- 112 RAM
- 113 アドレス・データバス

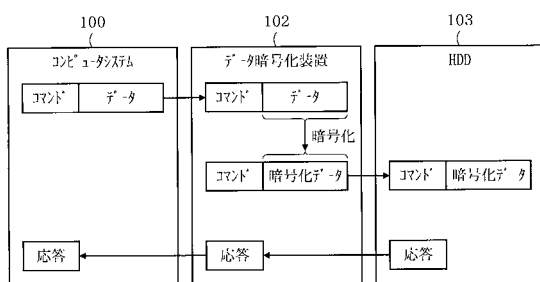
【図 1】



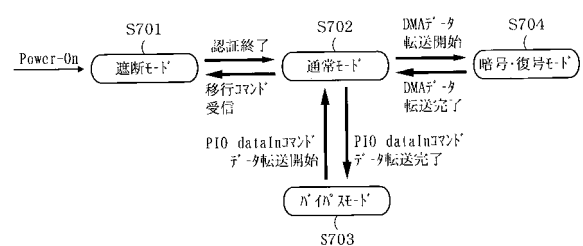
【図 2】



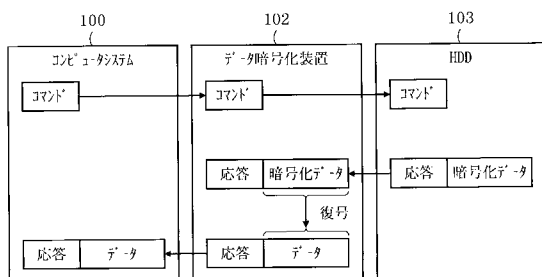
【図 3】



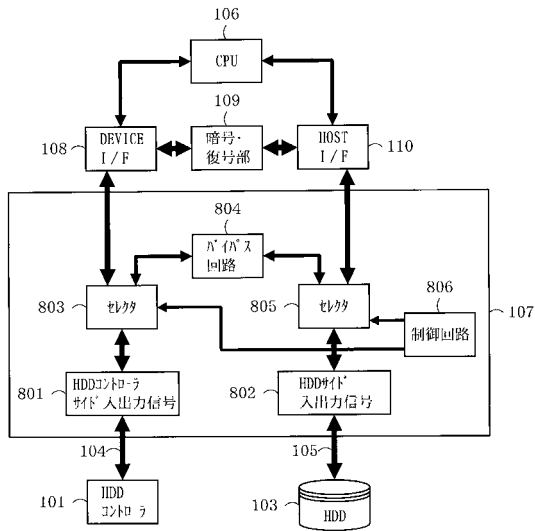
【図 5】



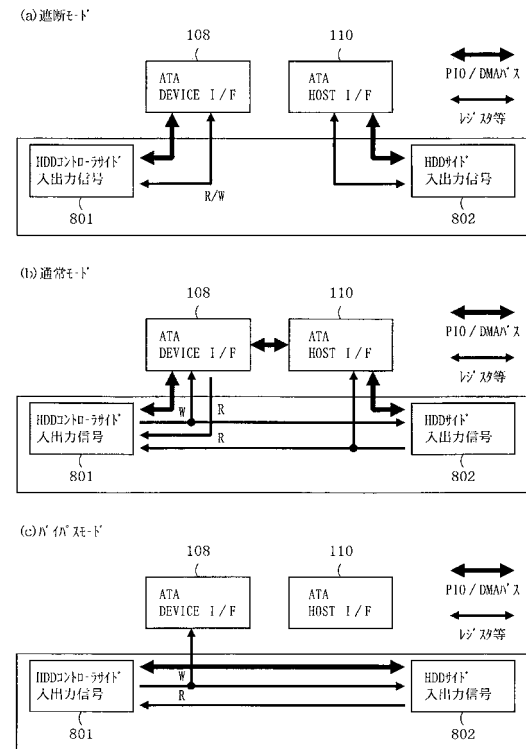
【図 4】



【図 6】



【図 7】



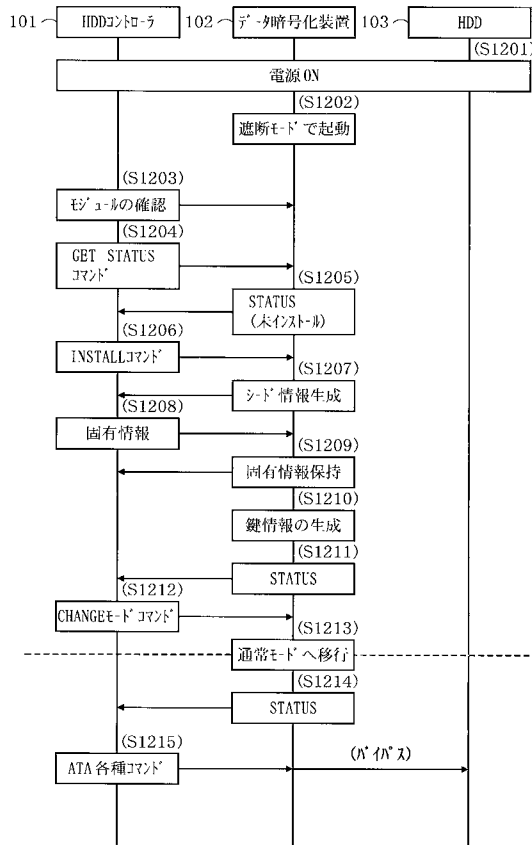
【図 8】

1001 コマンド名	1002 タイプ
GET STATUS	Non DATA
INSTALL	WRITE
VERSION INFORMATION	READ
CHANGE NORMAL	Non DATA
CHANGE INTERCEPT	Non DATA
⋮	⋮
SEND CHA1	WRITE
REQUEST RES1	READ
REQUEST CHA2	READ
SEND RES2	WRITE

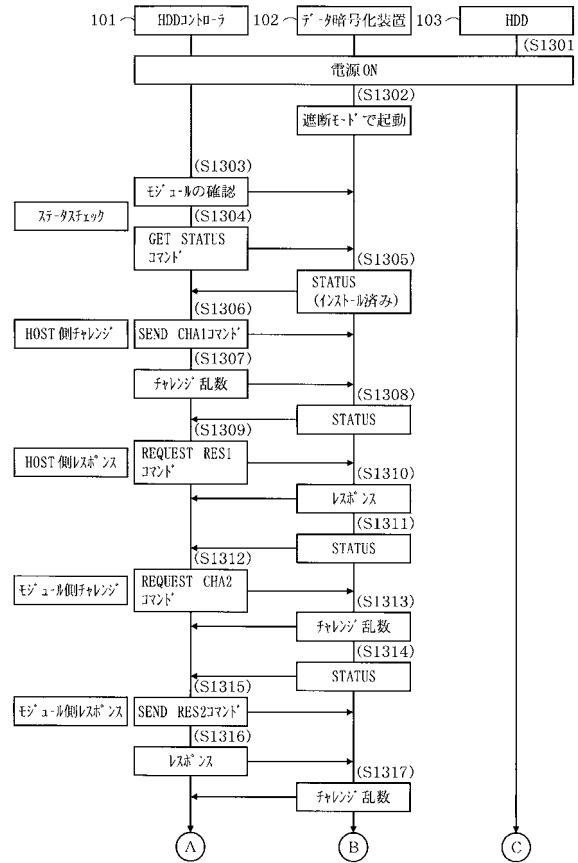
【図 9】

1101 コマンド名	1102 タイプ
RECALIBRATE	Non DATA
SEEK	Non DATA
EXECUTIVE DEVICE DIAGNOSTIC	Non DATA
⋮	⋮
READ DMA	DMA
WRITE DMA	DMA
⋮	⋮
FLUSH CACHE	Non DATA
IDENTIFY DEVICE	PIO READ
SET FEATURES	Non DATA

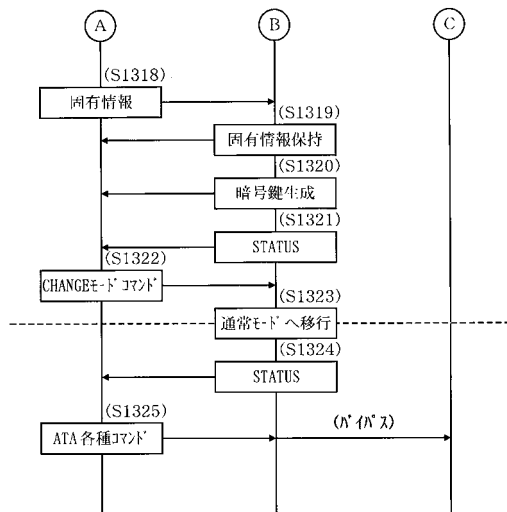
【図 10】



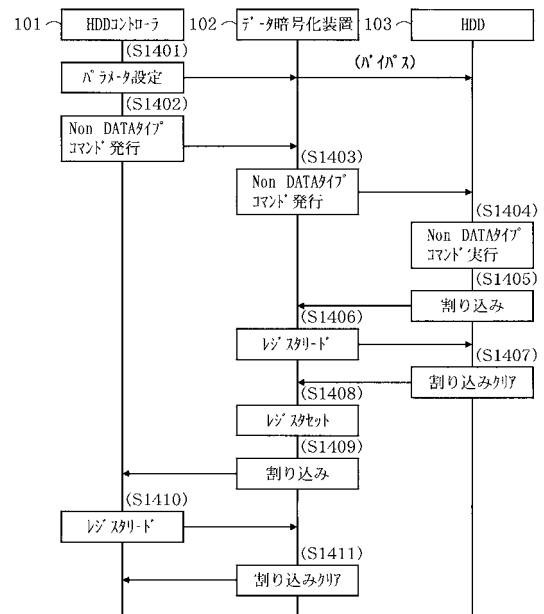
【図 11 A】



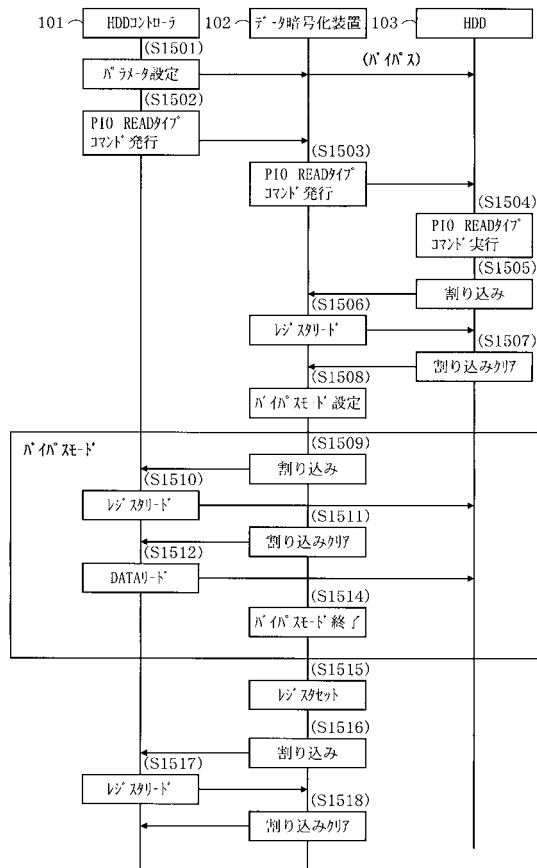
【図 11 B】



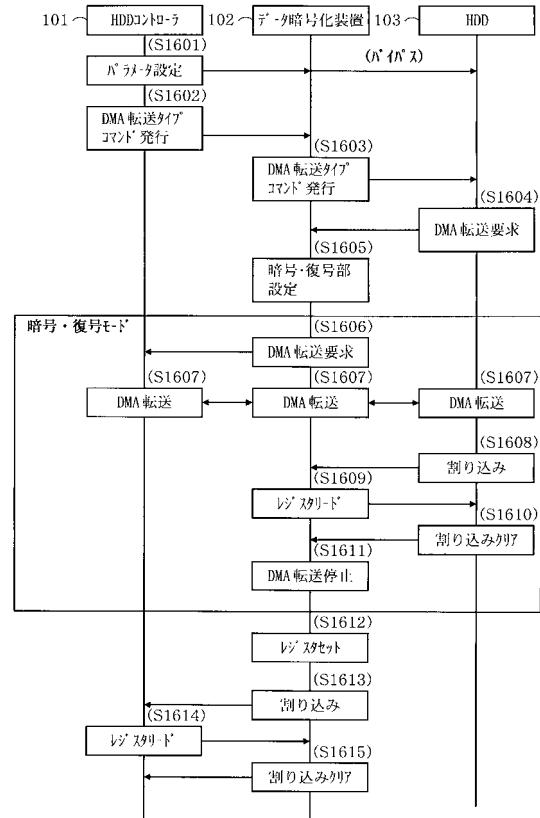
【図 12】



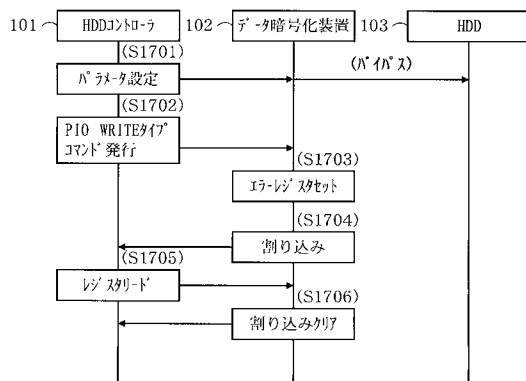
【図 13】



【図 14】



【図 15】



【図 16】

FD/CD-ROM等の記憶媒体	
ディレクトリ情報	
第1のデータ処理プログラム	図2に示すフローチャートのステップに対応するプログラムコード群
第2のデータ処理プログラム	図10に示すフローチャートのステップに対応するプログラムコード群
第3のデータ処理プログラム	図11A、図11Bに示すフローチャートのステップに対応するプログラムコード群
第4のデータ処理プログラム	図12に示すフローチャートのステップに対応するプログラムコード群
第5のデータ処理プログラム	図13に示すフローチャートのステップに対応するプログラムコード群
第6のデータ処理プログラム	図14に示すフローチャートのステップに対応するプログラムコード群
第7のデータ処理プログラム	図15に示すフローチャートのステップに対応するプログラムコード群

記憶媒体のメモリマップ

フロントページの続き

(56)参考文献 国際公開第02/037239 (WO, A1)
国際公開第2005/029272 (WO, A1)

(58)調査した分野(Int.Cl., DB名)
G06F 21/24
G06F 3/06
G09C 1/00