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

特許第6328045号
(P6328045)

(45)発行日　平成30年5月23日(2018.5.23)　(24)登録日　平成30年4月27日(2018.4.27)

(51)Int.Cl.		F I		
G06F 21/56	(2013.01)	G06F	21/56	350
G06F 21/12	(2013.01)	G06F	21/12	310
G06F 21/60	(2013.01)	G06F	21/60	
H04L 9/32	(2006.01)	H04L	9/00	675A

請求項の数 8　(全 10 頁)

(21)出願番号　特願2014-251095(P2014-251095)
(22)出願日　平成26年12月11日(2014.12.11)
(65)公開番号　特開2016-115002(P2016-115002A)
(43)公開日　平成28年6月23日(2016.6.23)
審査請求日　平成29年3月1日(2017.3.1)

(73)特許権者　317006041
東芝メモリ株式会社
東京都港区芝浦一丁目１番１号
(74)代理人　100091982
弁理士　永井　浩之
(74)代理人　100091487
弁理士　中村　行孝
(74)代理人　100082991
弁理士　佐藤　泰和
(74)代理人　100105153
弁理士　朝倉　悟
(74)代理人　100107582
弁理士　関根　毅
(74)代理人　100118843
弁理士　赤岡　明

最終頁に続く

(54)【発明の名称】メモリデバイス

(57)【特許請求の範囲】
【請求項１】
第１スクリプトを記憶するスクリプト記憶部と、
第２スクリプトを暗号化した第２ハッシュ鍵を記憶するハッシュ鍵記憶部と、
前記第１スクリプトを第１ハッシュ鍵へと暗号化するハッシュ計算部と、
前記第１スクリプトを実行するスクリプト処理部と、
通信部と、
前記通信部のネットワークへのアクセスに用いる秘匿情報を記憶する秘匿情報記憶部と、を備え、
前記スクリプト処理部は、前記第１ハッシュ鍵が前記第２ハッシュ鍵と異なる場合に、前記第１スクリプトに含まれる前記秘匿情報記憶部へのアクセスが可能なスクリプトを実行しないことで前記第１スクリプトの実行を制限する、メモリデバイス。
【請求項２】
前記第２スクリプトを前記第２ハッシュ鍵へと暗号化可能な署名文字情報を記憶する署名文字情報記憶部を更に備え、
前記ハッシュ計算部は、前記署名文字情報に基づいて前記第１スクリプトを前記第１ハッシュ鍵へと暗号化する、請求項１に記載のメモリデバイス。
【請求項３】
前記スクリプト記憶部に対する外部からのリードライトアクセスを許容するインターフェースを更に備える、請求項１に記載のメモリデバイス。

【請求項４】
前記署名文字情報記憶部は、外部からのリードライトアクセスが不可能である、請求項２に記載のメモリデバイス。
【請求項５】
前記署名文字情報記憶部は、前記通信部を通じた外部からのリードライトアクセスが不可能である、請求項４に記載のメモリデバイス。
【請求項６】
前記スクリプト記憶部に対する外部からのリードライトアクセスを許容するインターフェースを更に備え、
前記署名文字情報記憶部は、前記インターフェースを通じた外部からのリードライトアクセスが不可能である、請求項４に記載のメモリデバイス。
【請求項７】
前記第１ハッシュ鍵は、前記第１スクリプトに一意に対応する情報であり、
前記第２ハッシュ鍵は、前記第２スクリプトに一意に対応する情報である、請求項１に記載のメモリデバイス。
【請求項８】
第１スクリプトを第１ハッシュ鍵へと暗号化する計算部と、
第２スクリプトを暗号化した第２ハッシュ鍵を記憶する記憶部と、
通信部と、
前記通信部のネットワークへのアクセスに用いる秘匿情報を記憶する秘匿情報記憶部と、を備え、
前記計算部は、前記第１ハッシュ鍵と前記第２ハッシュ鍵とを比較し、前記第１ハッシュ鍵が前記第２ハッシュ鍵と異なる場合に、前記第１スクリプトに含まれる前記秘匿情報記憶部へのアクセスが可能なスクリプトを実行しないことで前記第１スクリプトの実行を制御する、メモリデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、メモリデバイスに関する。
【背景技術】
【０００２】
無線通信機能を備えたＳＤカードは、ホスト機器の無線通信機能に頼らず、自らの無線通信機能でクラウドサイトへダイレクトにアクセスできる。このようなクラウドサイトへのアクセスは、ＳＤカードに記憶されたスクリプトをＳＤカードのスクリプト処理部が実行することで行われる。
【０００３】
ここで、スクリプトは、コンパイルが不要であるといった利便性を有する。一方で、ソースコードを秘匿できないため、第三者に改変され易い。
【０００４】
このため、従来の無線通信機能を備えたＳＤカードにおいては、スクリプトが第三者によって改変され、ユーザが意図しないスクリプトが実行されるという問題があった。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特許第５４１０６２６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
意図しないスクリプトの実行を制限するメモリデバイスを提供する。
【課題を解決するための手段】

【０００７】
本実施形態によるメモリデバイスは、スクリプト記憶部と、ハッシュ鍵記憶部と、ハッシュ計算部と、スクリプト処理部と、通信部と、秘匿情報記憶部とを備える。スクリプト記憶部は、第１スクリプトを記憶する。ハッシュ鍵記憶部は、第２スクリプトを暗号化した第２ハッシュ鍵を記憶する。ハッシュ計算部は、第１スクリプトを第１ハッシュ鍵へと暗号化する。スクリプト処理部は、第１スクリプトを実行する。秘匿情報記憶部は、通信部のネットワークへのアクセスに用いる秘匿情報を記憶する。スクリプト処理部は、第１ハッシュ鍵が第２ハッシュ鍵と異なる場合に、第１スクリプトに含まれる秘匿情報記憶部へのアクセスが可能なスクリプトを実行しないことで第１スクリプトの実行を制限する。
【図面の簡単な説明】
【０００８】
【図１】本実施形態を示すメモリシステム１のブロック図である。
【図２】図１のメモリシステム１におけるメモリデバイス２の動作例を示すフローチャートである。
【図３】図１のメモリシステム１におけるメモリデバイス２の動作例を示す模式図である。
【発明を実施するための形態】
【０００９】
以下、図面を参照して本発明に係る実施形態を説明する。本実施形態は、本発明を限定するものではない。
【００１０】
図１は、本実施形態を示すメモリシステム１のブロック図である。メモリシステム１は、メモリデバイス２とホストデバイス３とを備える。メモリデバイス２は、例えば無線通信機能を備えたＳＤカードなどである。ホストデバイス３は、例えばデジタルカメラ、携帯電話機、スマートフォンまたはパーソナルコンピュータといったコンピュータ端末である。
【００１１】
メモリデバイス２は、ホストデバイス３に接続され、ホストデバイス３から電源供給を受ける。また、メモリデバイス２は、ホストデバイス３からのアクセスに応じた処理を実行する。
【００１２】
図１に示すように、メモリデバイス２は、ホストインターフェース（Ｉ／Ｆ）２１と、バッファ２２と、主制御部２３とを備える。ホストインターフェース２１はホスト１とメモリデバイス２とを接続するインターフェースである。また、メモリデバイス２は、メモリコントローラ２４と、ＮＡＮＤフラッシュメモリ２５と、通信部２６と、秘匿情報記憶部２７と、署名文字情報記憶部２８とを備える。ＮＡＮＤフラッシュメモリ２５は、スクリプト記憶部２５１およびハッシュ鍵記憶部２５２を備える。
【００１３】
主制御部２３は、ＣＰＵ２３１と、ＲＯＭ２３２と、ＲＡＭ２３３とを備える。また、通信部２６は、無線通信インターフェース（Ｉ／Ｆ）２６１と、無線ＬＡＮ信号処理部２６２と、無線通信信号処理部２６３と、アンテナ２６４、２６５とを備える。また、ＣＰＵ２３１は、スクリプト処理部２３１１およびハッシュ計算部２３１２を備える。
【００１４】
バッファ２２と、ＣＰＵ２３１と、ＲＯＭ２３２と、ＲＡＭ２３３と、メモリコントローラ２４と、無線通信インターフェース２６１とは、共通のバスＢ１に接続される。また、バッファ２２は、ホストインターフェース２１に接続される。
【００１５】
また、メモリコントローラ２４は、ＮＡＮＤフラッシュメモリ２５、秘匿情報記憶部２７および署名文字情報記憶部２８に接続される。また、無線通信インターフェース２６１は、無線ＬＡＮ信号処理部２６２および無線通信信号処理部２６３に接続される。また、

無線ＬＡＮ信号処理部２６２は、アンテナ２６４に接続され、無線通信信号処理部２６３は、アンテナ２６５に接続される。

【００１６】

ホストインターフェース２１は、ホストデバイス３に接続可能である。ホストインターフェース２１は、ホストデバイス３との接続状態において、ホストデバイス３との間で、コマンドの受信やデータの授受などを行う。例えば、ホストインターフェース２１は、ホストデバイス３からのライトアクセスにともなって、ホストデバイス３から書き込み対象データ（例えば、写真や動画など）を受信する。

【００１７】

バッファ２２は、メモリデバイス２が処理するデータを一時的に保存する。例えば、バッファ２２は、ホストデバイス３からの書き込み対象データを一時的に保存する。

【００１８】

ＮＡＮＤフラッシュメモリ２５は、外部からのリードライトアクセスが自由なユーザデータ領域である。例えば、ＮＡＮＤフラッシュメモリ２５には、ホストデバイス３からのライトアクセスに従って書き込み対象データが書き込まれる。

【００１９】

メモリコントローラ２４は、ＮＡＮＤフラッシュメモリ２５、秘匿情報記憶部２７および署名文字情報記憶部２８に対して、データの書き込みや読み出しを行う。例えば、メモリコントローラ２４は、ＮＡＮＤフラッシュメモリ２５に対して、ホストデバイス３からのライトアクセスに従った書き込み対象データの書き込みや、ホストデバイス３からの送信指令に従った送信対象データ（例えば、写真や動画など）の読み出しを行う。

【００２０】

通信部２６は、メモリデバイス２を外部ネットワークに接続する。外部ネットワークは、例えば、ＨＴＴＰやＨＴＴＰＳをサポートするクラウドサイト（インターネット上のサーバ）などである。

【００２１】

例えば、メモリコントローラ２４は、ＮＡＮＤフラッシュメモリ２５から読み出した送信対象データを、無線通信インターフェース２６１へ送信する。そして、無線ＬＡＮ信号処理部２６２は、無線通信インターフェース２６１から取得された送信対象データを、無線ＬＡＮ方式でアンテナ２６４を通じてクラウドサイトに送信する。

【００２２】

また、通信部２６は、メモリデバイス２を外部ネットワーク以外の通信先にも接続可能である。具体的には、無線通信信号処理部２６３は、メモリコントローラ２４がＮＡＮＤフラッシュメモリ２５から読み出された送信対象データを、無線通信インターフェース２６１を介して取得する。そして、無線通信信号処理部２６３は、取得した送信対象データを、無線ＬＡＮ以外の通信方式（例えば、近接無線通信）でアンテナ２６５を通じてポータブル端末（例えば、スマートフォン）に送信する。

【００２３】

主制御部２３は、メモリデバイス２の全体の動作を制御する。主制御部２３の制御は、ＣＰＵ２３１がＲＯＭ２３２に記憶されているファームウェアを実行することで行う。ファームウェアは、所定のＡＰＩ(Application Programming Interface)をサポートしている。

【００２４】

ここで、ＡＰＩは、或るコンピュータプログラムの機能や管理するデータなどを、外部の他のプログラムから呼び出して利用するための手順やデータ形式などを定めた規約である。ファームウェアの一部の機能を呼び出す短いプログラムは、このようなＡＰＩに従って記述可能である。ファームウェアのすべてをプログラミングする必要がないので、このようなＡＰＩに従った記述を使う場合、ファームウェアの開発コストは削減可能である。

【００２５】

このようなＡＰＩに従った短いプログラムとして、スクリプト言語で記述されたスクリ

プトがある。スクリプトは、機械語への変換や実行可能ファイルの作成などの過程を省略または自動化する。従って、スクリプトは、そのソースコードを記述したら即座に実行できるプログラムである。

【００２６】

このようなスクリプトの利便性に鑑みて、本実施形態では、ファームェアの一部の機能を呼び出すために、第１スクリプトがスクリプト記憶部２５１に記憶されている。そして、スクリプト処理部２３１１は、この第１スクリプトを実行可能である。その結果、ファームウェアにおける一部の機能は、スクリプト処理部２３１１からの呼び出しに応じて実行可能である。

【００２７】

なお、第１スクリプトは、例えば、文字列データなどである。また、スクリプト処理部２３１１は、第１スクリプトを実行することで、秘匿された外部ネットワークにアクセスする機能を実行するファームウェアを呼び出して実行してもよい。

【００２８】

ここで、第１スクリプトは、外部ネットワークへのアクセスに用いる秘匿情報を取得することを内容とする場合がある。秘匿情報を用いてアクセスする外部ネットワークとしては、例えばＯＡｕｔｈシステムを採用するクラウドサイトなどがある。また、秘匿情報は、外部ネットワークへのアクセスに用いる秘匿すべき情報であり、例えば、ユーザＩＤやパスワードなどを暗号化したアクセストークンなどである。

【００２９】

このような外部ネットワークへのアクセスに用いる秘匿情報は、秘匿情報記憶部２７に記憶されている。したがって、第１スクリプトが秘匿情報を取得することを内容とする場合、第１スクリプトは、秘匿情報記憶部２７へのアクセスが可能なスクリプトとなる。

【００３０】

そして、第１スクリプトが秘匿情報記憶部２７へのアクセスが可能なスクリプトである場合、スクリプト処理部２３１１は、第１スクリプトを実行することで、秘匿情報記憶部２７にアクセスして秘匿情報を取得できる。さらに、スクリプト処理部２３１１は、取得された秘匿情報を、通信部２６を通じてクラウドサイトに送信することで、クラウドサイトからアクセスの許可を得ることができる。

【００３１】

このように、スクリプト処理部２３１１が第１スクリプトを実行して秘匿情報を取得することで、メモリデバイス２は、自らの無線通信機能で外部ネットワークにアクセスできる。例えば、メモリデバイス２は、ＮＡＮＤフラッシュメモリ２５に書き込まれている送信対象データを、ホストデバイス３からの送信指令に従ってクラウドサイトにアップロードできる。

【００３２】

しかし、第１スクリプトの実行を制限しない場合、スクリプト記憶部２５１にアクセスした第三者が第１スクリプトを改変し、その結果、第三者が改変後の第１スクリプトに基づいて秘匿情報を不正取得してしまうおそれがある。そして、第三者が、不正取得した秘匿情報を悪用して、ユーザがアップロードしたデータに不正アクセスしてしまうおそれがある。

【００３３】

そこで、メモリデバイス２は、第１スクリプトが改変されることで意図しないスクリプトが実行されることを制限するために、ハッシュ鍵記憶部２５２と、署名文字情報記憶部２８と、ハッシュ計算部２３１２とを備えている。

【００３４】

具体的には、ハッシュ鍵記憶部２５２は、第２スクリプトを暗号化した第２ハッシュ鍵を記憶している。

【００３５】

ここで、第２スクリプトは、改変されていない正規（すなわち真正）の第１スクリプト

に一致する。逆に、第２スクリプトは、改変された第１スクリプトと異なる。
【００３６】
また、第２ハッシュ鍵は、第２スクリプトに一意に対応する情報であり、第２ハッシュ鍵から第２スクリプトを復号することがほぼ不可能な不可逆的な情報である。第２ハッシュ鍵は、例えば、暗号学的ハッシュ関数（一方向性関数）に基づく所定長さのビット列などであってもよい。
【００３７】
また、第２ハッシュ鍵は、正規の第１スクリプトとともにＮＡＮＤフラッシュメモリ２５に書き込まれたものであってもよい。このような第２ハッシュ鍵および正規の第１スクリプトの書き込みは、メモリデバイス２の製造段階で行ってもよく、または、更新の段階で行ってもよい。
【００３８】
第１スクリプトおよび第２ハッシュ鍵が更新可能であれば、その目的に合わせた自由な改変が可能であるといったスクリプトの利便性を確保することができる。なお、第１スクリプトおよび第２ハッシュ鍵の更新は、通信部２６を用いたサーバとの通信や、ホストデバイス３（例えば、パーソナルコンピュータ）の通信機能を利用したサーバとの通信で行ってもよい。また、第１スクリプトおよび第２ハッシュ鍵の更新は、後述する署名文字情報の更新をともなってもよい。
【００３９】
署名文字情報記憶部２８は、第２スクリプトを第２ハッシュ鍵へと暗号化可能な署名文字情報を記憶している。署名文字情報記憶部２８は、外部からのリードライトアクセスが不可能な秘匿領域である。
【００４０】
具体的には、署名文字情報記憶部２８は、ホストインターフェース２１および通信部２６のいずれを経由したリードライトアクセスも不可能である。署名文字情報は、例えば文字列データなどである。
【００４１】
ハッシュ計算部２３１２は、署名文字情報に基づいて、第１スクリプトを第１ハッシュ鍵へと暗号化する。すなわち、ハッシュ計算部２３１２は、署名文字情報と第１スクリプトとに基づくハッシュ計算を行うことで、第１ハッシュ鍵を算出する。第１ハッシュ鍵は、第１スクリプトに一意に対応する情報である。
【００４２】
ハッシュ計算の具体的な態様は、第２スクリプトを署名文字情報に基づいて第２ハッシュ鍵へと暗号化できる手法と同一であれば特に限定されず、例えば、署名文字情報と第１スクリプトとを、所定のアルゴリズムのハッシュ関数に入力してもよい。
【００４３】
ハッシュ計算が正規の第１スクリプトに対して行われた場合、算出された第１ハッシュ鍵は、第２ハッシュ鍵に一致する。逆に、ハッシュ計算が改変した第１スクリプトに対して行われた場合、算出された第１ハッシュ鍵は、第２ハッシュ鍵と異なる。
【００４４】
そして、スクリプト処理部２３１１は、第１ハッシュ鍵が第２ハッシュ鍵と異なる場合に、第１スクリプトの実行を制限する。例えば、スクリプト処理部２３１１は、第１スクリプトに含まれる秘匿情報記憶部２７へのアクセスが可能なAPIを実行しない。また、例えば、スクリプト処理部２３１１は、第１スクリプトのすべてを実行しないようにしてもよい。
【００４５】
したがって、メモリデバイス２は、改変された第１スクリプトが実行されることを制限できる。そのため、秘匿情報を不正取得されることを防ぐ効果を有する。メモリデバイス２の動作の詳細は後述する。
【００４６】

図１に示すように、ホストデバイス３は、ＣＰＵ３１と、ＲＯＭ３２と、ハードディスクドライブ３３（ＨＤＤ）と、ＲＡＭ３４と、ホストコントローラ３５とを備える。これらの構成部３１～３５は、バスＢ２を介して互いに接続されている。

【００４７】

ＣＰＵ３１は、ホストデバイス３全体を制御する。ＲＯＭ３２は、ＣＰＵ３１が実行するファームウェアを記憶している。ＲＡＭ３４は、ＣＰＵ３１の動作領域である。ハードディスクドライブ３３は、写真や動画などの各種のデータを記憶している。ホストコントローラ３５は、メモリデバイス２へのアクセスを実行する。

【００４８】

図２は、図１のメモリデバイス２の動作例を示すフローチャートである。図３は、図１のメモリデバイス２の動作例を示す模式図である。以下、図２および図３を用いてメモリデバイス２の動作の一例を説明する。

【００４９】

図２に示すように、スクリプト処理部２３１１は、先ず、スクリプト記憶部２５１から第１スクリプトを読みだす（ステップＳ１）。この第１スクリプトの読みだしは、スクリプト処理部２３１１がホストデバイス３からのアクセスに従ってファームウェアを実行することを契機としてもよい。

【００５０】

次いで、ハッシュ計算部２３１２は、第１スクリプトと署名文字情報とに基づくハッシュ計算を行うことで、第１スクリプトを第１ハッシュ鍵へと暗号化する（ステップＳ２）。

【００５１】

次いで、スクリプト処理部２３１１は、ハッシュ計算で算出された第１ハッシュ鍵と、ハッシュ鍵記憶部２５２に記憶されている第２ハッシュ鍵とを比較し、一致するか否かを判定する（ステップＳ３）。

【００５２】

そして、第１ハッシュ鍵が第２ハッシュ鍵に一致する場合（ステップＳ３：Ｙｅｓ）、スクリプト処理部２３１１は、第１スクリプトに記述された秘匿情報記憶部２７にアクセスする機能（スクリプト部分）をオン（有効）にする（ステップＳ４）。

【００５３】

一方、第１ハッシュ鍵が第２ハッシュ鍵に一致しない場合（ステップＳ３：Ｎｏ）、スクリプト処理部２３１１は、第１スクリプトに記述された秘匿情報記憶部２７にアクセスする機能（スクリプト部分）をオフ（無効）にする（ステップＳ５）。

【００５４】

次いで、スクリプト処理部２３１１は、第１スクリプトを、実行の制限のない範囲（有効な範囲）で実行する（ステップＳ６）。

【００５５】

なお、スクリプト処理部２３１１は、第１スクリプトを読みだし（ステップＳ１）した後に、第１スクリプトに秘匿情報記憶部２７へのアクセス機能が含まれているか否かを判定してもよい。この場合、スクリプト処理部２３１１は、第１スクリプトに当該アクセス機能が含まれている場合に、ハッシュ計算（ステップＳ２）に移行し、第１スクリプトに当該アクセス機能が含まれていない場合に、直ちに第１スクリプトの実行（ステップＳ６）に移行してもよい。

【００５６】

例えば、図３Ａに示すように、第２ハッシュ鍵Ｈ２＿ａがスクリプトａを暗号化したものであるのに対して、第１スクリプトが正規のスクリプトａである場合、ハッシュ計算で得られる第１ハッシュ鍵Ｈ１＿ａは、第２ハッシュ鍵Ｈ２＿ａに一致する。この場合、スクリプト処理部２３１１は、第１スクリプトａにおける秘匿情報記憶部２７へのアクセス機能を実行できる。

【００５７】

一方、図３Ｂに示すように、第２ハッシュ鍵Ｈ２＿ａがスクリプトａを暗号化したものであるのに対して、第１スクリプトが正規のスクリプトａを改変したスクリプトｂである場合、ハッシュ計算で得られる第１ハッシュ鍵Ｈ１＿ｂは、第２ハッシュ鍵Ｈ２＿ａに一致しない。この場合、スクリプト処理部２３１１は、第１スクリプトａにおける秘匿情報記憶部２７へのアクセス機能を実行できない。

【００５８】

また、図３Ｃに示すように、第２ハッシュ鍵を、スクリプトｃを暗号化したＨ２＿ｃに更新する場合がある。第２ハッシュ鍵をＨ２＿ｃに更新する場合は、同時に第１スクリプトをスクリプトｃに更新する。

【００５９】

そして、図３Ｃに示すように、第１スクリプトが更新後の正規のスクリプトｃである場合、ハッシュ計算で得られる第１ハッシュ鍵Ｈ１＿ｃは、更新後の第２ハッシュ鍵Ｈ２＿ｃに一致する。この場合、スクリプト処理部２３１１は、更新後の第１スクリプトｃにおける秘匿情報記憶部２７へのアクセス機能を実行できる。

【００６０】

以上説明したように、本実施形態によれば、第１ハッシュ鍵と第２ハッシュ鍵との比較結果に応じて秘匿情報記憶部２７へのアクセスが制御されるので、ユーザが意図しないスクリプトが実行されることを制限できる。

【００６１】

なお、実行が制限される第１スクリプトは、改変された第１スクリプトであればよく、秘匿情報記憶部２７にアクセスできるように改変されたものに限定されない。また、第１スクリプトにおける実行が制限される内容は、秘匿情報記憶部２７へのアクセスに限定されず、例えば、第１スクリプトの改変の態様に応じて異なってもよい。

【００６２】

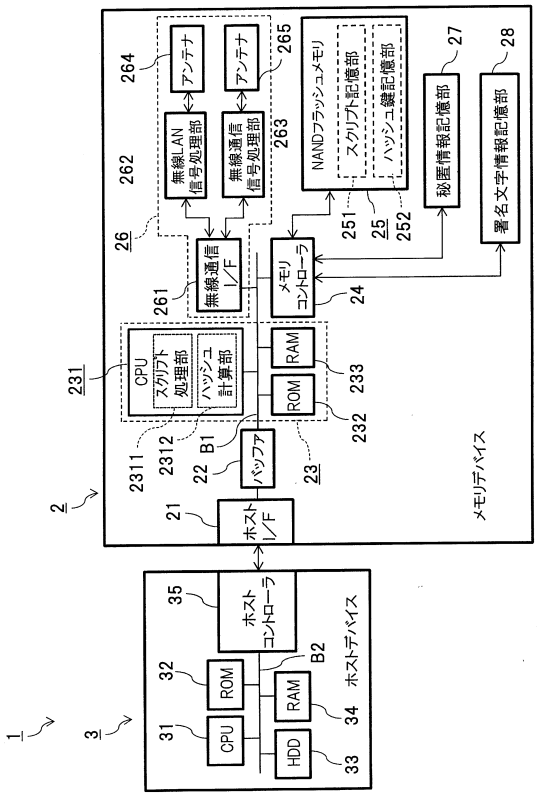
本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれると同様に、特許請求の範囲に記載された発明とその均等の範囲に含まれるものである。

【符号の説明】

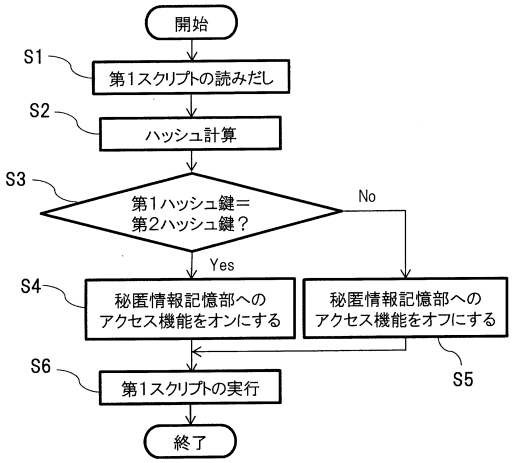
【００６３】

２　メモリデバイス
２３１１　スクリプト処理部
２３１２　ハッシュ計算部
２５１　スクリプト記憶部
２５２　ハッシュ鍵記憶部

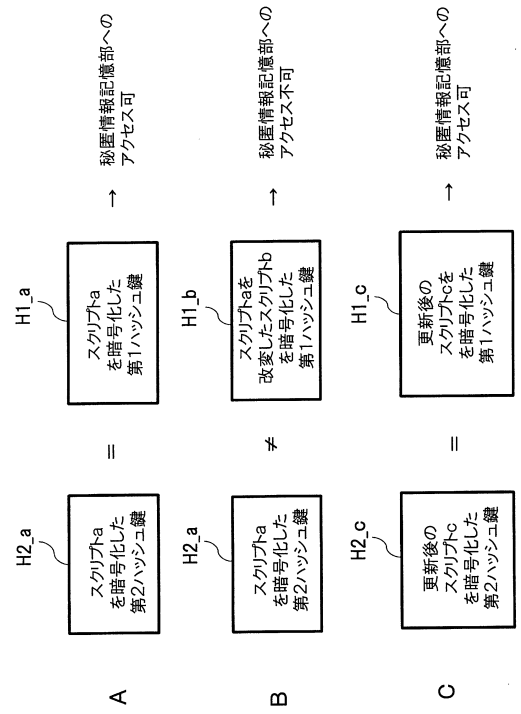
【図１】


1
2
3
21
ホストI/F
22
B1
バッファ
23
231
CPU
スクリプト処理部
ハッシュ計算部
2311
2312
RAM
ROM
232
233
メモリデバイス
24
メモリコントローラ
251
25
252
NANDフラッシュメモリ
スクリプト記憶部
ハッシュ鍵記憶部
26
261
無線通信I/F
262
無線LAN信号処理部
263
無線通信信号処理部
264
アンテナ
265
アンテナ
27
秘匿情報記憶部
28
署名文字情報記憶部
31
CPU
32
ROM
33
HDD
34
RAM
B2
35
ホストコントローラ
ホストデバイス

【図２】


開始
S1
第1スクリプトの読みだし
S2
ハッシュ計算
S3
第1ハッシュ鍵＝
第2ハッシュ鍵？
No
Yes
S4
秘匿情報記憶部への
アクセス機能をオンにする
秘匿情報記憶部への
アクセス機能をオフにする
S5
S6
第1スクリプトの実行
終了

【図３】


A
H2_a
スクリプトa
を暗号化した
第2ハッシュ鍵
=
H1_a
スクリプトa
を暗号化した
第1ハッシュ鍵
→
秘匿情報記憶部への
アクセス可
B
H2_a
スクリプトa
を暗号化した
第2ハッシュ鍵
≠
H1_b
スクリプトaを
改変したスクリプトb
を暗号化した
第1ハッシュ鍵
→
秘匿情報記憶部への
アクセス不可
C
H2_c
更新後の
スクリプトc
を暗号化した
第2ハッシュ鍵
=
H1_c
更新後の
スクリプトc
を暗号化した
第1ハッシュ鍵
→
秘匿情報記憶部への
アクセス可

フロントページの続き

(74)代理人 100120385
弁理士 鈴木 健之
(72)発明者 伊藤 晋朗
東京都港区芝浦一丁目１番１号 株式会社東芝内

審査官 平井 誠

(56)参考文献 米国特許出願公開第２００９／０１０６６２８（ＵＳ，Ａ１）
国際公開第２０１３／０９４１１０（WO，Ａ１）
特開２０１３－２１０９７２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１