(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2022-527163
(P2022-527163A)
(43)公表日　令和4年5月31日(2022.5.31)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/64	*(2013.01)*	G06F 21/64		5B160
G06F 21/79	*(2013.01)*	G06F 21/79		
G06F 21/81	*(2013.01)*	G06F 21/81		
G06F 12/02	*(2006.01)*	G06F 12/02	510A	

審査請求 有　予備審査請求 未請求　（全 33 頁）

(21)出願番号　特願2021-557309(P2021-557309)
(86)(22)出願日　令和2年3月16日(2020.3.16)
(85)翻訳文提出日　令和3年11月22日(2021.11.22)
(86)国際出願番号　PCT/US2020/022931
(87)国際公開番号　WO2020/197821
(87)国際公開日　令和2年10月1日(2020.10.1)
(31)優先権主張番号　16/363,100
(32)優先日　平成31年3月25日(2019.3.25)
(33)優先権主張国・地域又は機関
米国(US)

(71)出願人　595168543
マイクロン　テクノロジー，インク．
アメリカ合衆国，アイダホ州　８３７１６－９６３２，ボイズ，サウス　フェデラル　ウェイ　８０００
(74)代理人　100121083
弁理士　青木　宏義
(74)代理人　100138391
弁理士　天田　昌行
(74)代理人　100074099
弁理士　大菅　義之
(72)発明者　トロイア　アルベルト
ドイツ連邦共和国　８１９２５　ミュンヘン　ホッホシュティフトシュ　１１

最終頁に続く

(54)【発明の名称】暗号ハッシュを用いたメモリに格納されたデータの正当性確認

(57)【要約】
本開示は、暗号ハッシュを用いたメモリに格納されたデータの正当性を確認するための装置、方法、及びシステムを含む。実施形態は、メモリと、回路であって、メモリを複数のセグメントに分割することであって、各セグメントがそれぞれ異なる暗号ハッシュに関連付けられている、分割することと、メモリへの電力供給時に、複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた暗号ハッシュを使用して確認することと、メモリへの電力供給後に、複数のセグメントのうちの第２の数のセグメントに格納されたデータ、複数のセグメントのうちの第２の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた暗号ハッシュを使用して確認することとを行うように構成されている、回路とを備える。

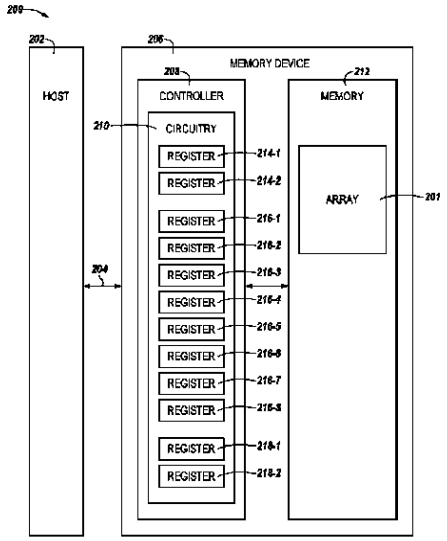


Fig. 2

【特許請求の範囲】
【請求項１】
メモリと、
回路であって、
前記メモリを複数のセグメントに分割することであって、各セグメントがそれぞれ異なる暗号ハッシュに関連付けられている、前記分割することと、
前記メモリへの電力供給時に、前記複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと、
前記メモリへの前記電力供給後に、前記複数のセグメントのうちの第２の数のセグメントに格納されたデータ、前記複数のセグメントのうちの第２の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと
を行うように構成されている、前記回路と
を備える、装置。
【請求項２】
前記回路が、前記第１の数の前記セグメントの１つ１つにそれぞれ格納された前記データの正当性を、
前記第１の数の前記セグメントの１つ１つにそれぞれ格納された前記データに対して異なる実行時暗号ハッシュを生成することと、
各セグメントにそれぞれ格納された前記データに対して生成した前記実行時暗号ハッシュを、その各セグメントに関連付けられた前記暗号ハッシュと比較することと
によって確認するように構成されている、請求項１に記載の装置。
【請求項３】
前記回路が、前記第２の数の前記セグメントの１つ１つにそれぞれ格納された前記データの正当性を、
前記第２の数の前記セグメントの１つ１つにそれぞれ格納された前記データに対して異なる実行時暗号ハッシュを生成することと、
各セグメントにそれぞれ格納された前記データに対して生成した前記実行時暗号ハッシュを、その各セグメントに関連付けられた前記暗号ハッシュと比較することと
によって確認するように構成されている、請求項１に記載の装置。
【請求項４】
前記回路が、
前記メモリへの前記電力供給後に、前記第１の数の前記セグメントの１つ１つにそれぞれ格納された前記データを、その前記第１の数の前記セグメントの１つ１つにそれぞれ格納された前記データの正当性を確認すると、ホストに送ることと、
前記第２の数の前記セグメントの１つ１つにそれぞれ格納された前記データを、その前記第２の数の前記セグメントの１つ１つにそれぞれ格納された前記データの正当性を確認すると、前記ホストに送ることと
を行うように構成されている、請求項１に記載の装置。
【請求項５】
前記メモリが、メモリセルのセキュアアレイを備える、請求項１～４のいずれか１項に記載の装置。
【請求項６】
前記回路が、
前記セキュアアレイのアドレスを設定するように構成されたレジスタと、
前記セキュアアレイのサイズを設定するように構成されたレジスタと
を含む、請求項５に記載の装置。
【請求項７】
前記回路が、各セグメントにそれぞれ関連付けられた前記暗号ハッシュを格納するよう

に構成されたレジスタを含み、
前記レジスタが、前記メモリのユーザにとってアクセス不可能である、請求項１～４のいずれか１項に記載の装置。
【請求項８】
メモリを動作させる方法であって、
前記メモリを複数のセグメントに分割することであって、各セグメントがそれぞれ異なる暗号ハッシュに関連付けられている、前記分割することと、
前記メモリへの電力供給時に、前記複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータに対して異なる実行時暗号ハッシュを生成することと、
前記メモリへの前記電力供給時に、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を、その各セグメントに格納された前記データに対して生成した前記実行時暗号ハッシュと、その各セグメントに関連付けられた前記暗号ハッシュとを比較することによって確認することと、
前記メモリへの前記電力供給後に、前記複数のセグメントのうちの第２の数のセグメントの１つ１つにそれぞれ格納されたデータに対して異なる実行時暗号ハッシュを生成することと、
前記メモリへの前記電力供給後に、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を、その各セグメントに格納された前記データに対して生成した前記実行時暗号ハッシュと、その各セグメントに関連付けられた前記暗号ハッシュとを比較することによって確認することと
を含む、前記方法。
【請求項９】
前記方法が、
前記複数のセグメントのうちの前記第１の数のセグメントについての前記比較により、その各セグメントに格納された前記データに対して生成された前記実行時暗号ハッシュが、その各セグメントに関連付けられた前記暗号ハッシュと一致することが示されることに基づいて、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を確認することと、
前記複数のセグメントのうちの前記第２の数のセグメントについての前記比較により、その各セグメントに格納された前記データに対して生成された前記実行時暗号ハッシュが、その各セグメントに関連付けられた前記暗号ハッシュと一致することが示されることに基づいて、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を確認することと
を含む、請求項８に記載の方法。
【請求項１０】
前記方法が、
前記複数のセグメントのうちの前記第１の数のセグメントについての前記比較により、その各セグメントに格納された前記データに対して生成された前記実行時暗号ハッシュが、その各セグメントに関連付けられた前記暗号ハッシュと一致しないことが示されることに基づいて、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを修復することと、
前記複数のセグメントのうちの前記第２の数のセグメントについての前記比較により、その各セグメントに格納された前記データに対して生成された前記実行時暗号ハッシュが、その各セグメントに関連付けられた前記暗号ハッシュと一致しないことが示されることに基づいて、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データを修復することと
を含む、請求項８に記載の方法。
【請求項１１】
前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納さ

れた前記データを修復することが、前記メモリから前記データを回復させることを含み、
前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データを修復することが、前記メモリから前記データを回復させることを含む、請求項１０に記載の方法。
【請求項１２】
メモリを動作させる方法であって、
前記メモリを複数のセグメントに分割することであって、各セグメントがそれぞれ異なる暗号ハッシュに関連付けられている、前記分割することと、
前記メモリへの電力供給時に、前記複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと、
前記メモリへの前記電力供給後に、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを、その前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれに格納された前記データの正当性を確認すると、ホストに送ることと、
前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを前記ホストに送っている間に、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと
を含む、前記方法。
【請求項１３】
前記方法が、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを前記ホストに送った後に、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データを、その前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を確認すると、前記ホストに送ること
を含む、請求項１２に記載の方法。
【請求項１４】
前記方法が、前記ホストから受け取った認証済みコマンドを使用して、各セグメントにそれぞれ関連付けられた前記暗号ハッシュを生成すること
を含む、請求項１２～１３のいずれか１項に記載の方法。
【請求項１５】
メモリを有するメモリデバイスであって、
前記メモリが複数のセグメントに分割され、各セグメントがそれぞれ異なる暗号ハッシュに関連付けられており、
前記メモリデバイスが、
前記メモリへの電力供給時に、前記複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと、
前記メモリへの電力供給後に、前記複数のセグメントのうちの第２の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと
を行うように構成されている、
前記メモリデバイスと、
ホストであって、前記ホストが、
前記複数のセグメントのうちの前記第２の数のセグメントに格納された前記データの正当性を前記メモリデバイスが確認している間に、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを、その前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を前記メモリデバイスが確認すると、前記メモリデバイスから受け取ることと、

前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを前記メモリデバイスから受け取った後に、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データを、その前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を前記メモリデバイスが確認すると、前記メモリデバイスから受け取ることと
を行うように構成されている、前記ホストと
を備える、システム。
【請求項１６】
前記メモリデバイスが、
前記複数のセグメントの１つ１つそれぞれのアドレスを設定するように構成されたレジスタと、
前記複数のセグメントの１つ１つそれぞれのサイズを設定するように構成されたレジスタと
を含む、請求項１５に記載のシステム。
【請求項１７】
前記メモリデバイスが、
前記複数のセグメントの１つ１つにそれぞれ格納された前記データの前記正当性確認の状況の表示を提供するように構成されたレジスタと、
前記複数のセグメントの１つ１つにそれぞれ格納された前記データの前記正当性確認の結果の表示を提供するように構成されたレジスタと
を含む、請求項１５に記載のシステム。
【請求項１８】
前記メモリデバイスが、
前記複数のセグメントの１つ１つにそれぞれ格納された前記データの修復が許可されているかどうかの表示を提供するように構成されたレジスタと、
前記複数のセグメントの１つ１つにそれぞれ格納された前記データを、修復時に、回復させることができる前記メモリのアドレスを設定するように構成されたレジスタと、
前記複数のセグメントの１つ１つにそれぞれ格納された前記データの前記修復の結果の表示を提供するように構成されたレジスタと
を含む、請求項１５に記載のシステム。
【請求項１９】
前記複数のセグメントのうちの前記第１の数のセグメントが、前記ホストによって設定された特定の数量のセグメントを含み、
前記メモリデバイスが、前記特定の数量のセグメントを格納するように構成されたレジスタを含む、請求項１５～１８のいずれか１項に記載のシステム。
【請求項２０】
前記複数のセグメントのうちの前記第１の数のセグメントが、特定の時間内に前記メモリデバイスによって正当性確認することが可能な数量のセグメントを含み、
前記メモリデバイスが、前記特定の時間を格納するように構成されたレジスタを含む、請求項１５～１８のいずれか１項に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、一般に、半導体メモリ及び方法に関し、より詳細には、暗号ハッシュを用いたメモリに格納されたデータの正当性確認に関する。
【背景技術】
【０００２】
メモリデバイスは、通常、コンピュータまたは他の電子デバイスにおいて内部の半導体、集積回路及び／または外部の着脱可能なデバイスとして提供される。メモリには、揮発

性メモリ及び不揮発性メモリを含む様々な種類がある。揮発性メモリは、データを保持するために電力を要求することが可能であり、揮発性メモリには、特に、ランダムアクセスメモリ（ＲＡＭ）、ダイナミックランダムアクセスメモリ（ＤＲＡＭ）、及び同期ダイナミックランダムアクセスメモリ（ＳＤＲＡＭ）が含まれ得る。不揮発性メモリは、電力が供給されていないときにも格納データを保持することで永続的データを提供することが可能であり、不揮発性メモリには、特に、ＮＡＮＤフラッシュメモリ、ＮＯＲフラッシュメモリ、読み出し専用メモリ（ＲＯＭ）、ならびに、相変化ランダムアクセスメモリ（ＰＣＲＡＭ）、抵抗変化型ランダムアクセスメモリ（ＲＲＡＭ）、及び磁気ランダムアクセスメモリ（ＭＲＡＭ）などの抵抗可変メモリが含まれ得る。

【０００３】

メモリデバイスを組み合わせて、ソリッドステートドライブ（ＳＳＤ）、エンベデッドマルチメディアカード（ｅ．ＭＭＣ）、及び／またはユニバーサルフラッシュストレージ（ＵＦＳ）デバイスを形成することができる。ＳＳＤ、ｅ．ＭＭＣ、及び／またはＵＦＳデバイスには、各種の不揮発性メモリ及び揮発性メモリの中でも特に、不揮発性メモリ（例えば、ＮＡＮＤフラッシュメモリ及び／またはＮＯＲフラッシュメモリ）が含まれ得、及び／または揮発性メモリ（例えば、ＤＲＡＭ及び／またはＳＤＲＡＭ）が含まれ得る。不揮発性メモリは、特に、パーソナルコンピュータ、ポータブルメモリスティック、デジタルカメラ、携帯電話、ＭＰ３プレーヤなどのポータブル音楽プレーヤ、ムービプレーヤなど、幅広いエレクトロニクス用途に使用され得る。

【０００４】

フラッシュメモリデバイスは、例えば浮遊ゲートなどの電荷蓄積構造にデータを格納するメモリセルを含み得る。フラッシュメモリデバイスは、一般的には、高記憶密度、高信頼性、及び低消費電力を可能にする１トランジスタメモリセルを使用する。抵抗可変メモリデバイスは、記憶要素（例えば、可変抵抗を有する抵抗変化型メモリ要素）の抵抗状態に基づいてデータを記憶することができる抵抗変化型メモリセルを含み得る。

【０００５】

メモリセルは、アレイ状に配置され得、アレイアーキテクチャにおけるメモリセルを、目標の（例えば、所望の）状態にプログラムすることができる。例えば、電荷がフラッシュメモリセルの電荷蓄積構造（例えば、浮遊ゲート）上に置かれるか、またはそこから電荷が除去されて、セルが特定のデータ状態にプログラムされ得る。セルの電荷蓄積構造に蓄積された電荷により、セルの閾値電圧（Ｖｔ）が示され得る。フラッシュメモリセルの状態は、セルの電荷蓄積構造に蓄積された電荷（例えば、Ｖｔ）をセンスすることによって判別され得る。

【０００６】

多くの脅威が、メモリデバイスのメモリセルに格納されたデータに影響を与える可能性がある。そのような脅威には、例えば、メモリデバイスに発生する故障、及び／またはハッカーまたはその他の悪意のあるユーザからの脅威が含まれ得る。そのような脅威により、重大な金銭的損失が生じるおそれがあり、及び／または安全性及び／またはセキュリティに重大な問題が生じるおそれがある。

【図面の簡単な説明】

【０００７】

【図１】本開示の実施形態による、いくつかの物理ブロックを有するメモリアレイの一部分の図を示す。

【図２】本開示の実施形態による、ホストと、メモリデバイスの形態の装置とを含むコンピューティングシステムのブロック図である。

【図３Ａ】本開示の実施形態によるセキュアメモリアレイを設定するために使用されるレジスタの例を示す。

【図３Ｂ】本開示の実施形態に従って設定されたセキュアメモリアレイを含むメモリアレイの一部分の図を示す。

【図４】本開示の一実施形態による、メモリアレイに格納されたデータを複数のセグメン

トに分割し、各セグメントにそれぞれ格納されたデータの正当性確認及び修復を行うために使用されるレジスタの例を示す。
【図５】本開示の実施形態による、暗号ハッシュを使用して、メモリに格納されたデータのセグメントを正当性確認する方法を示す。
【図６】本開示の実施形態による、ホスト及びメモリデバイスを含む例示的なシステムのブロック図である。
【図７】本開示の実施形態による、いくつかのパラメータを決定するための例示的なプロセスのブロック図である。
【図８】本開示の実施形態による、いくつかのパラメータを決定するための例示的なプロセスのブロック図である。
【図９】本開示の実施形態による、証明書を検証するための例示的なプロセスのブロック図である。
【図１０】本開示の実施形態による、署名を検証するための例示的なプロセスのブロック図である。
【図１１】本開示の実施形態による、例示的なメモリデバイスのブロック図である。
【発明を実施するための形態】
【０００８】
本開示は、暗号ハッシュを用いたメモリに格納されたデータの正当性を確認するための装置、方法、及びシステムを含む。実施形態は、メモリと、回路であって、メモリを複数のセグメントに分割することであって、各セグメントがそれぞれ異なる暗号ハッシュに関連付けられている、分割することと、メモリへの電力供給時に、複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた暗号ハッシュを使用して確認することと、メモリへの電力供給後に、複数のセグメントのうちの第２の数のセグメントに格納されたデータ、複数のセグメントのうちの第２の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた暗号ハッシュを使用して確認することとを行うように構成されている、回路とを備える。
【０００９】
多くの脅威が、メモリ（例えば、メモリデバイス）に格納されたデータに影響を与える可能性がある。例えば、メモリのアレイ及び／または回路に故障が発生することがあり、その結果、データにエラーが生じることになる場合がある。追加の例として、ハッカーまたはその他の悪意のあるユーザが、悪意のある目的でデータに不正な変更を加える行為をしようとする可能性がある。例えば、悪意のあるユーザは、幾つかあるハッキング行為のタイプの中でも特に、メモリを使用して実行されている商取引に悪影響を与える（例えば、商取引の流れを悪い方向に変える）こと（例えば、支払いを確認するコードをスキップすることにより、提供されているサービスに対して支払いが行われたと偽って示すこと）、メモリで実行されているソフトウェアライセンスチェックに悪影響を与える（例えば、ソフトウェアライセンスチェックの流れを悪い方向に変える）こと（例えば、ライセンスを確認するコードをスキップすることにより、メモリのソフトウェアが適切にライセンスされていると偽って示すこと）、またはメモリを使用して実行されている自動車制御に悪影響を与える（例えば、自動車制御の流れを悪い方向に変える）こと（例えば、部品の真正性のチェック、環境チェック、または誤動作アラームのチェックをスキップすること）のために、メモリに格納されたデータを変更しようとする可能性がある。そのようなハッキング行為（攻撃など）により、重大な金銭的損失が生じるおそれがあり、及び／または安全性及び／またはセキュリティに重大な問題が生じるおそれがある。
【００１０】
そのため、セキュアなメモリシステムを確保するには、メモリに保存されているデータが真正であり（例えば、最初にプログラムされたものと同じであり）、ハッキング行為またはその他の不正な及び／または意図しない変更によって改ざんされていないことを確認（例えば、認証及び／または証明）することが重要である。そのようなデータ正当性確認

は、例えば、メモリへの電力供給時（例えば、本明細書では「起動」と呼ばれることがあるメモリの電源オン時及び／または電源投入時）に行われ得る。しかし、データ正当性確認の実行により、メモリへの電力の供給に必要な時間が増加する可能性があり（例えば、起動時間の待ち時間が増加する可能性があり）、それによってメモリシステムのユーザ体験に悪影響を与えることがある。

【００１１】

一方、本開示の実施形態では、メモリへの電力供給時に、メモリへの電力供給に必要な時間を短縮しながらも（例えば、メモリ起動時間の待ち時間を減少させる）、メモリに格納されたデータの正当性を効果的に確認し、それによってセキュアなメモリシステムを確保することができる。例えば、本開示の実施形態では、メモリをセグメントに分割し、それらのセグメントの１つ１つにそれぞれ関連付けられた異なる暗号ハッシュを使用して、メモリへの電力供給時（例えば、起動時）に、セグメントの（例えば、セグメント全てよりも少ない）一部分にのみ格納されたデータの正当性を確認することができる。そして、メモリの残りのセグメントに格納されたデータを、メモリへの電力供給が完了した後に、それらのセグメントの１つ１つにそれぞれ関連付けられた異なる暗号ハッシュを使用して、正当性確認することができる。

【００１２】

本明細書で使用するとき、「ａ」、「ａｎ」、または「いくつかの（ａ　ｎｕｍｂｅｒ　ｏｆ）」とは、あるものの１つ以上のことを指す場合があり、「複数の（ａ　ｐｌｕｒａｌｉｔｙ　ｏｆ）」とは、２つ以上のそのようなものを指し得る。例えば、１つのメモリデバイス（ａ　ｍｅｍｏｒｙ　ｄｅｖｉｃｅ）は、１つ以上のメモリデバイスを指す場合があり、複数のメモリデバイスは２つ以上のメモリデバイスを指し得る。さらに、特に図面の参照数字に対して本明細書で使用される識別子「Ｒ」、「Ｂ」、「Ｓ」、「Ｎ」、及び「Ｋ」は、そのように称されるいくつかの特定の特徴が、本開示のいくつかの実施形態に含まれ得ることを示す。番号は、呼称の間で同じであってもよく、または異なっていてもよい。

【００１３】

本明細書の図は、最初の一桁または複数桁が図面の図番に対応し、残りの桁が図面内の要素または構成要素を識別する番号付け規則に従う。異なる図面間の類似した要素または構成要素は、類似した数字を使用することによって識別してもよい。例えば、１０１が図１の要素「０１」を参照することができ、類似した要素を図２の２０１として参照することができる。

【００１４】

図１は、本開示の実施形態による、いくつかの物理ブロックを有するメモリアレイ１０１の一部分の図を示す。メモリアレイ１０１は、例えば、ＮＡＮＤフラッシュメモリアレイなどのフラッシュメモリアレイであり得る。追加の例として、メモリアレイ１０１は、特に、ＰＣＲＡＭ、ＲＲＡＭ、ＭＭＲＡＭ、またはスピントルクトランスファ（ＳＴＴ）アレイなどの抵抗可変メモリアレイであってもよい。しかし、本開示の実施形態は、特定のタイプのメモリアレイに限定されるものではない。さらに、メモリアレイ１０１を、本明細書で詳述するように、セキュアなメモリアレイとすることができる。さらに、図１に示していないが、メモリアレイ１０１は、その動作に関連する様々な周辺回路と共に、特定の半導体ダイ上に設置され得る。

【００１５】

図１に示すように、メモリアレイ１０１は、メモリセルの物理ブロック１０７－０（ブロック０）、１０７－１（ブロック１）、・・・、１０７－Ｂ（ブロックＢ）を、いくつか有する。メモリセルは、シングルレベルセル、及び／または例えば、２レベルセル、３レベルセル（ＴＬＣ）、または４レベルセル（ＱＬＣ）などのマルチレベルセルであり得る。一例として、メモリアレイ１０１内の物理ブロックの数は、１２８ブロック、５１２ブロック、または１，０２４ブロックであり得るが、実施形態は、メモリアレイ１０１内の２の特定の累乗または任意の特定の数の物理ブロックに限定されない。

【００１６】
いくつかのメモリセルの物理ブロック（例えば、ブロック１０７－０、１０７－１、・・・、１０７－Ｂ）が、メモリセルの平面内に含まれ得、いくつかのメモリセルの平面がダイ上に含まれ得る。例えば、図１に示す例では、各物理ブロック１０７－０、１０７－１、・・・、１０７－Ｂは、単一のダイの一部であってもよい。すなわち、図１に示すメモリアレイ１０１の部分は、メモリセルのダイであってもよい。
【００１７】
図１に示すように、各物理ブロック１０７－０、１０７－１、・・・、１０７－Ｂは、アクセス線（例えば、ワード線）に結合されたいくつかのメモリセルの物理行（例えば、１０３－０、１０３－１、・・・、１０３－Ｒ）を含む。各物理ブロックの行（例えば、ワード線）の数は３２であってもよいが、実施形態では、物理ブロック当たりの行１０３－０、１０３－１、・・・、１０３－Ｒの数は特定の数に限定されない。さらに、図１には示さないが、メモリセルは、センス線（例えば、データ線及び／またはディジット線）の列に結合され得る。
【００１８】
当業者であれば理解されるように、各行１０３－０、１０３－１、・・・、１０３－Ｒは、いくつかのメモリセルのページ（例えば物理ページ）を含み得る。物理ページは、プログラム及び／またはセンスの単位（例えば、機能グループとしてまとめてプログラム及び／またはセンスされるいくつかのメモリセル）を意味する。図１に示す実施形態では、各行１０３－０、１０３－１、・・・、１０３－Ｒは、メモリセルの物理ページを１つ含む。しかし、本開示の実施形態は、そのように限定されるものではない。例えば、実施形態においては、各行が、メモリセルの複数の物理ページ（例えば、偶数番データ線に結合されたメモリセルの１つ以上の偶数ページと、奇数番データ線に結合されたメモリセルの１つ以上の奇数ページ）を含む場合がある。さらに、マルチレベルセルを含む実施形態の場合、メモリセルの物理ページが、データの複数のページ（例えば、論理ページ）を格納し得る（例えば、物理ページ内の各セルが、データの上位ページに対して１つ以上のビットを記憶し、データの下位ページに対して１つ以上のビットを記憶している状態で、メモリセルの物理ページが、データの上位ページ及びデータの下位ページを記憶し得る）。
【００１９】
図１に示すように、メモリセルのページは、いくつかの物理セクタ１０５－０、１０５－１、・・・、１０５－Ｓ（例えば、メモリセルのサブセット）を含み得る。セルの各物理セクタ１０５－０、１０５－１、・・・、１０５－Ｓは、いくつかのデータの論理セクタを格納し得る。さらに、データの各論理セクタは、データの特定のページの部分に対応し得る。一例として、特定の物理セクタに格納されたデータの第１の論理セクタが、データの第１のページに対応する論理セクタに対応してもよく、その特定の物理セクタに格納されたデータの第２の論理セクタが、データの第２のページに対応してもよい。各物理セクタ１０５－０、１０５－１、・・・、１０５－Ｓは、システムデータ及び／またはユーザデータを格納することがあり、及び／またはエラー訂正コード（ＥＣＣ）データ、論理ブロックアドレス（ＬＢＡ）データ、及びメタデータなどのオーバーヘッドデータを含むことがある。
【００２０】
論理ブロックアドレス指定は、データの論理セクタを識別するためにホストによって使用され得るスキームである。例えば、各論理セクタは、一意の論理ブロックアドレス（ＬＢＡ）に対応してもよい。さらに、ＬＢＡがまた、メモリ内のデータのその論理セクタの物理的位置を示し得る、物理ブロックアドレス（ＰＢＡ）などの物理アドレスに対応する（例えば、動的にマッピングされる）場合もある。データの論理セクタは、幾バイトかのデータ（例えば、２５６バイト、５１２バイト、１，０２４バイト、または４，０９６バイトのデータ）であり得る。しかし、実施形態は、これらの例に限定されるものではない。
【００２１】

物理ブロック１０７－０、１０７－１、・・・、１０７－Ｂ、行１０３－０、１０３－１、・・・、１０３－Ｒ、セクタ１０５－０、１０５－１、・・・、１０５－Ｓ、及びページについては、他の構成も可能であることに留意されたい。例えば、物理ブロック１０７－０、１０７－１、．．．、１０７－Ｂの行１０３－０、１０３－１、．．．、１０３－Ｒは、それぞれ例えば５１２バイトよりも多いかまたは少ないデータを含み得る単一の論理セクタに対応するデータを記憶してもよい。

【００２２】

図２は、本開示の実施形態による、ホスト２０２と、メモリデバイス２０６の形態の装置とを含むコンピューティングシステム２００のブロック図である。本明細書で使用される「装置」は、例えば、回路もしくは複数の回路、ダイもしくは複数のダイ、モジュールもしくは複数のモジュール、デバイスもしくは複数のデバイス、またはシステムもしくは複数のシステムなどの様々な構造または構造の組み合わせのうちのいずれかを指し得るが、これらに限定されない。さらに、実施形態では、コンピューティングシステム２００は、メモリデバイス２０６に類似しているいくつかのメモリデバイスを含み得る。

【００２３】

図２に示す実施形態では、メモリデバイス２０６は、メモリアレイ２０１を有するメモリ２１２を含み得る。メモリアレイ２０１は、図１に関連して前に述べたメモリアレイ１０１に類似していてもよい。図２では１つのメモリアレイ２０１が図示されているが、メモリ２１２は、メモリアレイ２０１に類似した任意の数のメモリアレイを含むことができる。

【００２４】

実施形態では、メモリアレイ２０１（例えば、アレイ２０１のサブセット、または全アレイ２０１）を、セキュアアレイ（例えば、制御下に置かれることになるメモリ２１２の領域）とすることができる。例えば、メモリアレイ２０１に格納されたデータには、機密情報にまつわる用途のために実行されることになるホストファームウェア及び／またはコードなど、機密データ（例えば、非ユーザデータ）が含まれてもよい。そのような実施形態では、１つ以上の不揮発性レジスタが、セキュアアレイを設定するために使用されてもよい。例えば、図２に示す実施形態では、回路２１０は、セキュアアレイを設定するために使用することができる１対のレジスタ２１４－１及び２１４－２を含む。例えば、レジスタ２１４－１が、セキュアアレイのアドレス（例えば、データの開始ＬＢＡ）を設定してもよく、レジスタ２１４－２が、セキュアアレイのサイズ（例えば、データの終了ＬＢＡ）を設定してもよい。そのようなレジスタの例と、セキュアアレイを設定する際のそれらの使用とについて、本明細書では（例えば、図３Ａ～図３Ｂに関連して）さらに説明する。

【００２５】

図２に示すように、ホスト２０２は、インターフェース２０４を介してメモリデバイス２０６に結合され得る。ホスト２０２とメモリデバイス２０６とは、インターフェース２０４上で通信する（例えば、コマンド及び／またはデータを送る）ことができる。ホスト２０２及び／またはメモリデバイス２０６は、幾つかあるホストシステムの中で特に、ラップトップコンピュータ、パーソナルコンピュータ、デジタルカメラ、デジタル記録再生装置、移動電話、ＰＤＡ、メモリカードリーダ、インターフェースハブ、または例えば、自動車用（例えば、乗り物用及び／または交通インフラストラクチャ用）のモノのインターネット（ＩｏＴ）対応機種、もしくは医療用（例えば、インプラント型及び／または健康管理用）のＩｏＴ対応機種など、ＩｏＴ対応機種であるか、あるいはそれらの一部であってもよく、メモリアクセスデバイス（例えば、プロセッサ）を含むことができる。当業者であれば、「プロセッサ」とは、並列処理システム、いくつかのコプロセッサなど、１つ以上のプロセッサを意味することがあり得ることを理解されよう。

【００２６】

インターフェース２０４は、規格化された物理インターフェースの形態をとり得る。例えば、メモリデバイス２０６がコンピューティングシステム２００の情報ストレージに使

用される場合、インターフェース２０４は、幾つかある物理コネクタ及び／または物理インターフェースの中で特に、シリアルアドバンスドテクノロジアタッチメント（ＳＡＴＡ）物理インターフェース、周辺機器相互接続エクスプレス（ＰＣＩｅ）物理インターフェース、ユニバーサルシリアルバス（ＵＳＢ）物理インターフェース、または小型コンピュータシステムインターフェース（ＳＣＳＩ）であり得る。また一方、一般に、インターフェース２０４は、インターフェース２０４に対して互換性のある受信器を有するメモリデバイス２０６とホスト（例えば、ホスト２０２）との間で、制御、アドレス、情報（例えば、データ）、及びその他の信号を渡すためのインターフェースを提供し得るものである。

【００２７】

メモリデバイス２０６は、ホスト２０２及びメモリ２１２（例えば、メモリアレイ２０１）と通信するコントローラ２０８を含む。例えば、コントローラ２０８は、幾つかある動作の中でも特に、データのセンス（例えば、読み出し）、プログラム（例えば、書き込み）、移動、及び／または消去を行う動作を含む動作をメモリアレイ２０１で実行するためのコマンドを送ることがあり得る。

【００２８】

コントローラ２０８は、メモリ２１２と同じ物理デバイス（例えば、同じダイ）上に含まれてもよい。あるいは、コントローラ２０８は、メモリ２１２を含む物理デバイスに通信可能に結合される別個の物理デバイス上に含まれてもよい。実施形態では、コントローラ２０８の構成要素を、分散型コントローラとして複数の物理デバイス（例えば、メモリと同じダイ上のいくつかの構成要素、及び異なるダイ、モジュール、またはボード上のいくつかの構成要素）に散在させてもよい。

【００２９】

ホスト２０２は、メモリデバイス２０６と通信するためのホストコントローラ（図２には示していない）を含み得る。ホストコントローラは、インターフェース２０４を介してメモリデバイス２０６にコマンドを送信し得る。ホストコントローラは、メモリデバイス２０６及び／またはメモリデバイス２０６上のコントローラ２０８と通信して、幾つかある動作の中でも特に、データの読み出し、書き込み、及び／または消去を行い得る。さらに、実施形態では、ホスト２０２は、本明細書で上記のとおり、ＩｏＴ通信能力を有するＩｏＴ対応機種であってもよい。

【００３０】

メモリデバイス２０６のコントローラ２０８、及び／またはホスト２０２のホストコントローラは、制御回路及び／またはロジック（例えば、ハードウェア及びファームウェア）を含み得る。実施形態では、メモリデバイス２０６のコントローラ２０８及び／またはホスト２０２のホストコントローラは、物理インターフェースを含むプリント回路基板に接続された特定用途向け集積回路（ＡＳＩＣ）であり得る。また、メモリデバイス２０６及び／またはホスト２０２は、揮発性メモリ及び／または不揮発性メモリのバッファと、いくつかのレジスタとを含み得る。

【００３１】

例えば、図２に示されるように、メモリデバイスは、回路２１０を含み得る。図２に示される実施形態では、回路２１０は、コントローラ２０８に含まれる。しかし、本開示の実施形態は、そのように限定されるものではない。例えば、実施形態では、回路２１０が（例えばコントローラ２０８の代わりに）メモリ２１２に（例えば同じダイ上に）含まれてもよい。回路２１０は、例えば、ハードウェア、ファームウェア、及び／またはソフトウェアを含むことが可能であり、メモリ２１２（例えば、メモリアレイ２０１）に格納されたデータの正当性を確認する（例えば、認証する、及び／または証明する）ために使用され得る。

【００３２】

例えば、回路２１０は、メモリアレイ２０１に格納されたデータを複数のセグメントに分割し、各セグメントにそれぞれ異なる暗号ハッシュを関連付けることができる。例えば

、回路２１０は、ホスト２０２から受け取った、認証された（例えば、セキュリティ保護され）、アンチリプレイ保護されたコマンドを使用して、各セグメントに対してそれぞれ異なる暗号ハッシュを生成（例えば、計算）することが可能である（例えば、メモリデバイス２０６のみがこれらの暗号ハッシュを認識し、メモリデバイス２０６のみがこれらの暗号ハッシュの生成及び更新を行うことができるようにする）。各セグメントに対してそれぞれ生成される暗号ハッシュを、本明細書では、そのセグメントのゴールデンハッシュと呼ぶことがあり、この暗号ハッシュは、例えば、ＳＨＡ－２５６暗号ハッシュを含み得る。これらのゴールデンハッシュは、メモリデバイス２０６及び／またはホスト２０２のユーザがアクセスできない（例えば、メモリデバイス２０６の「隠れた」領域にある）回路２１０に含まれる不揮発性レジスタ２１６－３に格納されてもよく、本明細書で詳述するように、メモリアレイ２０１に格納されたデータを正当性確認する過程で使用されてもよい。

【００３３】

さらに、図２に示すように、回路２１０は、複数のセグメントを設定するために使用することができる１つ以上の不揮発性レジスタ（例えば、レジスタ２１６－１及び２１６－２）を含むことができる。例えば、レジスタ２１６－１は、複数のセグメントの１つ１つそれぞれのアドレス（例えば、データの開始ＬＢＡ）を設定してもよく、レジスタ２１６－２は、複数のセグメントの１つ１つそれぞれのサイズ（例えば、データの終了ＬＢＡ）を設定してもよい。複数のセグメントは、それぞれ同じサイズに（例えば、同じ量のデータを格納）してもよく、異なるサイズに（例えば、異なる量のデータを格納）してもよい。レジスタ２１６－１、２１６－２、及び２１６－３の例を、本明細書で（例えば、図４に関連して）さらに説明する。

【００３４】

メモリデバイス２０６への電力供給（例えば、電源オン及び／または電源投入）中に、回路２１０は、複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータを、その各セグメントに関連付けられたゴールデンハッシュを用いて正当性確認する（例えば、正当性確認するかどうかを判定する）ことができる。本明細書で使用するとき、データを正当性確認するとは、データが真正であり（例えば、最初にプログラムされたものと同じであり）、ハッキング行為またはその他の不正な及び／または意図しない変更によって改ざんされていないことを認証すること、及び／または証明することを含むこと、及び／または指すことがあり得る。

【００３５】

例えば、回路２１０は、第１の数のセグメントの１つ１つにそれぞれ格納されたデータに対して異なる実行時暗号ハッシュを生成（例えば、計算）し、各セグメントにそれぞれ格納されたデータに対して生成した実行時暗号ハッシュを、レジスタ２１６－３に格納された、その各セグメントのゴールデンハッシュと比較してもよい。その比較により、各セグメントに格納されたデータに対して生成した実行時暗号ハッシュが、その各セグメントのゴールデンハッシュと一致することが示されると、その各セグメントに格納されたデータは改ざんされてないと判定することができ、したがって、その各セグメントに格納されたデータの正当性を確認することができる（例えば、正当であると判定することができる）。そのため、各セグメントにそれぞれ格納されたデータを、他のセグメントに格納されたデータとは無関係に正当性確認することが可能である。

【００３６】

複数のセグメントのうちの第１の数のセグメントは、メモリアレイ２０１に格納されたデータが分割された複数のセグメントの（例えば、セグメント全てよりも少ない）一部分のみを含み得る。一例を挙げると、複数のセグメントのうちの第１の数のセグメントは、ホスト２０２によって（例えば、ホスト２０２のユーザによって）設定された特定の数量のセグメントを含み得る。この数量は、回路２１０に含まれる不揮発性レジスタ２１８－１に格納されてもよい。追加の例として、複数のセグメントのうちの第１の数のセグメントは、特定の時間内に回路２１０によって正当性確認することが可能な数量のセグメント

を含み得る。この時間は、メモリデバイス２０６への電力供給が継続する時間に対応してもよく、メモリデバイス２０６によって（例えば、回路２１０によって）自動的に決定され、回路２１０に含まれる不揮発性レジスタ２１８－２に格納されてもよい。

【００３７】

しかし、比較により、各セグメントに格納されたデータに対して生成した実行時暗号ハッシュが、その各セグメントのゴールデンハッシュと一致しないことが示された場合には、それによって、その各セグメントに格納されたデータは（例えば、ハッカーまたはメモリの故障によって）改ざんされたことが示され得、したがって、その各セグメントに格納されたデータは正当ではない可能性がある（例えば、正当ではないと判定され得る）。そのような場合には、回路２１０は、そのセグメントに格納されたデータを修復してもよい（例えば、修復しようと試みてもよい）。セグメントに格納されたデータを修復することは、例えば、データの修復が許可されているかどうかを判定することと、修復が許可されている場合には、メモリ２１２から（例えば、図１１に関連して詳述する修復ブロック１１１７など、メモリに含まれる修復ブロックから）データを回復させる（例えば、復元する）こととを含み得る。

【００３８】

図２に示すように、回路２１０は、追加のレジスタ２１６－４、２１６－５、２１６－６、２１６－７、及び２１６－８を含むことがあり、これらのレジスタは、正当性確認及び修復の過程で回路２１０によって使用され得る。レジスタ２１６－４は、複数のセグメントの１つ１つにそれぞれ格納されたデータの正当性確認の状況の表示（例えば、データの正当性確認が行われたかどうかの表示）を提供することができる揮発性レジスタであってもよく、レジスタ２１６－５は、各セグメントにそれぞれ格納されたデータの正当性確認の結果の表示（例えば、データが正当であると判定されたかどうかの表示）を提供することができる揮発性レジスタであってもよく、これらのレジスタは、各セグメントにそれぞれ格納されたデータの修復を試みるべきかどうかを判定するために、回路２１０によって使用されてもよい。

【００３９】

レジスタ２１６－６は、複数のセグメントの１つ１つにそれぞれ格納されたデータの修復が許可されているかどうかの表示を提供することができる不揮発性レジスタであってもよく、データが正当ではなく、修復を試みるべきであると判定されると、セグメントに格納されたデータの修復が許可されているかどうかを判定するために、回路２１０によって使用されてもよい。レジスタ２１６－７は、複数のセグメントの１つ１つにそれぞれ格納されたデータを、そこから回復させることができるメモリ２１２（例えば、修復ブロック）のアドレスを設定するために使用され得る不揮発性レジスタであってもよく、このレジスタは、そのデータの修復時にデータを回復させるために、回路２１０によって使用されてもよい。レジスタ２１６－８は、複数のセグメントの１つ１つにそれぞれ格納されたデータの修復の結果（例えば、データが修復されたかどうか）の表示を、そのデータの修復が許可されている場合に提供することができる揮発性レジスタであってもよい。レジスタ２１６－４～２１６－８の例、ならびに正当性確認及び修復の過程でのそれらの使用については、本明細書で（例えば、図４に関連して）さらに説明する。

【００４０】

メモリデバイス２０６への電力供給が完了した後（例えば、起動後）に、回路２１０は、複数のセグメントのうちの第２の数のセグメントの１つ１つにそれぞれ格納されたデータを、その各セグメントに関連付けられたゴールデンハッシュを用いて正当性確認する（例えば、正当性確認するかどうかを判定する）ことができる。複数のセグメントのうちの第２の数のセグメントは、メモリアレイ２０１に格納されたデータが分割された残りのセグメント（例えば、複数のセグメントのうちの第１の数のセグメントに含まれないセグメント）を含み得る。しかし、本開示の実施形態は、第１の数及び第２の数のセグメントに限定されない（例えば、複数のセグメントは、第１の数及び第２の数のセグメントよりも多くのセグメントを含むことができる）。

【００４１】
複数のセグメントのうちの第２の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を確認するプロセスは、本明細書で既に説明した複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を確認するプロセスに類似し得る。例えば、回路２１０は、第１の数のセグメントについて本明細書で前に説明したのと同様にして、第２の数のセグメントの１つ１つにそれぞれ格納されたデータに対して異なる実行時暗号ハッシュを生成し、各セグメントにそれぞれ格納されたデータに対して生成した実行時暗号ハッシュを、レジスタ２１６－３に格納された、その各セグメントのゴールデンハッシュと比較してもよい。さらに、複数のセグメントのうちの第２の数のセグメントの１つに格納されたデータが正当ではないと判定された場合、回路２１０は、複数のセグメントのうちの第１の数のセグメントについて本明細書で前に説明したのと同様にして、そのセグメントに格納されたデータを修復してもよい。さらに、回路２１０は、複数のセグメントのうちの第２の数のセグメントに格納されたデータの正当性確認及び修復の過程で、第１の数のセグメントについて本明細書で前に説明したのと同様にして、レジスタ２１６－４～２１６－８を使用してもよい。

【００４２】
さらに、メモリデバイス２０６への電力供給が完了した後（例えば、複数のセグメントのうちの第２の数のセグメントに格納されたデータの正当性が確認されている間）に、回路２１０は、第１の数のセグメントの１つ１つにそれぞれ格納されたデータを、その第１の数のセグメントの１つ１つにそれぞれ格納されたデータが正当性確認されるかまたは修復されることで、インターフェース２０４を介してホスト２０２に送ることができる（例えば、ホスト２０２は、メモリデバイス２０６からデータを受け取ることができる）。例えば、第１の数のセグメントの１つ１つにそれぞれ格納されたデータは、その各セグメントに格納されたデータが、正当ではないと判定され、修復されていない場合には、ホスト２０２に送ることができず、各セグメントにそれぞれ格納されたデータは、正当であると判定され、または修復された場合にのみ、ホスト２０２に送ることができる。回路２１０は、本明細書で既に述べたように、レジスタ２１６－４～２１６－８を用いて、第１の数のセグメントの１つ１つにそれぞれ格納されたデータが正当であると判定されたか、または修復されたかを判定してもよい。

【００４３】
複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータを送った後に、回路２１０は、第２の数のセグメントの１つ１つにそれぞれ格納されたデータを、その第２の数のセグメントの１つ１つにそれぞれ格納されたデータが正当性確認されるかまたは修復されることで、インターフェース２０４を介してホスト２０２に送ることができる（例えば、ホスト２０２は、メモリデバイス２０６からデータを受け取ることができる）。例えば、第２の数のセグメントの１つ１つにそれぞれ格納されたデータは、その各セグメントに格納されたデータが、正当ではないと判定され、修復されていない場合には、ホスト２０２に送ることができず、各セグメントにそれぞれ格納されたデータは、正当であると判定され、または修復された場合にのみ、ホスト２０２に送ることができる。回路２１０は、本明細書で既に述べたように、レジスタ２１６－４～２１６－８を用いて、第２の数のセグメントの１つ１つにそれぞれ格納されたデータが正当であると判定されたか、または修復されたかを判定してもよい。

【００４４】
図２に示した実施形態は、本開示の実施形態を不明瞭にしないために図示していない、追加の回路、論理回路、及び／または構成要素を含み得る。例えば、メモリデバイス２０６は、Ｉ／Ｏ回路によってＩ／Ｏコネクタ上に提供されるアドレス信号をラッチするためのアドレス回路を含むことがある。アドレス信号が、行デコーダ及び列デコーダによって受け取られてデコードされて、メモリアレイ２０１にアクセスすることができる。さらに、メモリデバイス２０６は、メモリアレイ２０１とは別個の、及び／またはメモリアレイ２０１に加えて、例えば、ＤＲＡＭまたはＳＤＲＡＭなどのメインメモリを含んでもよい

。メモリデバイス２０６の追加の回路、論理回路、及び／または構成要素をさらに例示する例を、本明細書で（例えば、図１１に関連して）詳述する。

【００４５】

図３Ａは、本開示の実施形態によるセキュアメモリアレイを設定するために使用されるレジスタ３１４－１及び３１４－２の例を示す。図３Ｂは、本開示の実施形態に従ってレジスタ３１４－１及び３１４－２を使用して設定されたセキュアメモリアレイを含むメモリアレイ３０１の一部分の図を示す。レジスタ３１４－１及び３１４－２は、例えば、それぞれ図２に関連して既に説明したレジスタ２１４－１及び２１４－２であり得る。セキュアメモリアレイ３０１は、例えば、図２に関連して既に説明したメモリアレイ２０１であり得る。例えば、図３Ｂに示すように、セキュアメモリアレイ３０１は、図１に関連して既に説明したメモリアレイ１０１と同様にして、メモリセルのいくつかの物理ブロック３０７－０、３０７－１、・・・、３０７－Ｂを含むことが可能であり、それぞれが、メモリセルのいくつかのセクタを有するいくつかの物理行３０３－０、３０３－１、・・・、３０３－Ｒを含む。

【００４６】

図３Ａに示すように、レジスタ３１４－１は、セキュアアレイのアドレス（例えば、セキュアアレイの異なる部分のアドレス）を設定してもよく、レジスタ３１４－２は、セキュアアレイのサイズ（例えば、セキュアアレイの異なる部分のサイズ）を設定してもよい。レジスタ３１４－１によって設定されるセキュアアレイのアドレスは、例えば、セキュアアレイの開始点（例えば、開始ＬＢＡ）（例えば、セキュアアレイの異なる部分の開始点）に対応してもよく、レジスタ３１４－２によって設定されるセキュアアレイのサイズは、例えば、セキュアアレイの終了点（例えば、終了ＬＢＡ）（例えば、セキュアアレイの異なる部分の終了点）に対応してもよい。

【００４７】

例えば、図３Ａに示すように、レジスタ３１４－１及び３１４－２は、Ｎペアの値を設定することが可能であり、各ペアはそれぞれ、レジスタ３１４－１によって設定されるアドレス値（例えば、ａｄｄｒ）と、レジスタ３１４－２によって設定されるサイズ値（例えば、ｓｉｚｅ）とを含む。例えば、図３Ａに示す例では、ペア$_0$はアドレス値$addr_0$及びサイズ値$size_0$を含み（例えば、ペア$_0$＝［$addr_0$，$size_0$］）、ペア$_1$はアドレス値$addr_1$及びサイズ値$size_1$を含み（例えば、ペア$_1$＝［$addr_1$，$size_1$］）、他にも同じように、ペアＮはアドレス値$addr_N$及びサイズ値$size_N$を含む（例えば、ペア$_N$＝［$addr_N$，$size_N$］）。ペアのアドレス値は、セキュアアレイの一部分の開始点（例えば、開始ＬＢＡ）に対応してもよく、そのペアのアドレス値とサイズ値との合計は、セキュアアレイのその部分の終了点（例えば、終了ＬＢＡ）に対応し得る。したがって、セキュアアレイ全体（例えば、セキュアアレイ全体を含む部分）を、［$addr_0$，$addr_0+size_0$］∪［$addr_1$，$addr_1+size_1$］∪・・・∪［$addr_N$，$addr_N+size_N$］によって指定することができる。

【００４８】

レジスタ３１４－２によって設定されるサイズ値がゼロである最初のペアにより、セキュアアレイの設定を終了させることができる。例えば、図３Ａに示した例では、ペア$_2$のサイズ値がゼロである場合、セキュアアレイは、［$addr_0$，$addr_0+size_0$］∪［$addr_1$，$addr_1+size_1$］によって指定されることになる。

【００４９】

レジスタ３１４－１及び３１４－２によって（例えば、レジスタ３１４－２によって設定される全てのサイズ値を非ゼロにして）設定されたセキュアアレイの例が、図３Ｂに示されている。例えば、図３Ｂに示すように、メモリアレイ３０１のセクタ３０５－０に割り当てられたアドレス（例えば、ＬＢＡ）は$addr_0$であり、メモリアレイ３０１のセクタ３０５－１に割り当てられたアドレスは$addr_0+size_0$であり、メモリアレイ３０１のセクタ３０５－２に割り当てられたアドレスは$addr_1$であり、メモリアレ

イ３０１のセクタ３０５－３に割り当てられたアドレスはａｄｄｒ$_1$＋ｓｉｚｅ$_1$であり、メモリアレイ３０１のセクタ３０５－４に割り当てられたアドレスはａｄｄｒ$_N$であり、メモリアレイ３０１のセクタ３０５－５に割り当てられたアドレスはａｄｄｒ$_N$＋ｓｉｚｅ$_N$である。したがって、セキュアアレイは、セクタ（例えば、セクタに格納されたデータ）３０５－０～３０５－１、セクタ３０５－２～３０５－３、及びセクタ３０５－４～３０５－５を含む。ただし、メモリアレイ３０１のセクタ３０５－０よりも前のセクタ、及びメモリアレイ３０１のセクタ３０５－１～３０５－２は、セキュアアレイの一部ではない（例えば、セキュアアレイはアレイ３０１のサブセットを含む）。

【００５０】

図４は、本開示の一実施形態による、メモリアレイに格納されたデータを複数のセグメントに分割し、各セグメントにそれぞれ格納されたデータの正当性確認及び修復を行うために使用されるレジスタ４１６－１～４１６－８の例を示す。レジスタ４１６－１～４１６－８は、例えば、図２に関連して前に説明したレジスタ２１６－１～２１６－８であり得、メモリアレイは、例えば、図２に関連して前に説明したメモリアレイ２０１であり得る。

【００５１】

図４に図示され、本明細書で以前に説明した例に示すように、メモリアレイに格納されたデータを複数の（例えば、Ｎ個の）セグメントに分割することができ、そのうちの５つ（例えば、セグメント４２０－１、４２０－２、４２０－３、４２０－４、及び４２０－５）が図４に図示されている。さらに、本明細書で（例えば、図２に関連して）前に述べたように、複数のセグメントは、メモリへの電力供給時にデータの正当性確認及び／または修復を行い得る第１の数（例えば、Ｋ個）のセグメントと、メモリへの電力供給後にデータの正当性確認及び／または修復を行い得る第２の数（例えば、Ｎ－Ｋ個）のセグメントとを含み得る。図４に示された例では、セグメント４２０－１、４２０－２、及び４２０－３は、複数のセグメントのうちの第１の数のセグメントに含まれ、セグメント４２０－４及び４２０－５は、複数のセグメントのうちの第２の数のセグメントに含まれる。

【００５２】

図４に示すように、レジスタ４１６－１は、複数のセグメントの１つ１つそれぞれのアドレス（例えば、アドレス値）を設定することができ、レジスタ４１６－２は、複数のセグメントの１つ１つそれぞれのサイズ（例えば、サイズ値）を設定することができる。レジスタ４１６－１によって設定される各セグメントそれぞれのアドレスは、例えば、そのセグメントの開始点（例えば、開始ＬＢＡ）に対応してもよく、レジスタ４１６－２によって設定される各セグメントそれぞれのサイズは、例えば、そのセグメントの終了点（例えば、終了ＬＢＡ）に対応してもよい。例えば、図４に示した例では、セグメント４２０－１のアドレスは、レジスタ４１６－１によって０ｘａａｂｂｃｃと設定され、セグメント４２０－１のサイズは、レジスタ４１６－２によって０ｘ１００００と設定される。同様に、図４に示すように、セグメント４２０－２、４２０－３、４２０－４、及び４２０－５のアドレスは、レジスタ４１６－１によって、それぞれ０ｘａａ１１２２、０ｘ１２３４４４、０ｘｄｄｅｅｆｆ、及び０ｘａａ５５ｂｂと設定され、セグメント４２０－２、４２０－３、４２０－４、及び４２０－５のサイズは、レジスタ４１６－２によって、それぞれ０ｘ１００００、０ｘ２００００、０ｘ１００００、及び０ｘ２００００と設定される。

【００５３】

本明細書で（例えば、図２に関連して）既述のように、データの複数のセグメントの１つ１つそれぞれは、そのセグメントに格納されたデータの正当性確認用にそのセグメントに関連付けられた異なる暗号ハッシュ（例えば、ゴールデンハッシュ）を有し得る。例えば、図４に示す例では、セグメント４２０－１は、それに関連付けられたゴールデンハッシュ＃１を有し、セグメント４２０－２は、それに関連付けられたゴールデンハッシュ＃２を有し、セグメント４２０－３は、それに関連付けられたゴールデンハッシュ＃Ｋを有し、セグメント４２０－４は、それに関連付けられたゴールデンハッシュ＃Ｋ＋１を有し

、セグメント４２０－５は、それに関連付けられたゴールデンハッシュＮを有する。図４に示すように、各セグメントにそれぞれ関連付けられたゴールデンハッシュを、レジスタ４１６－３に格納することができる。

【００５４】

図４に示すように、レジスタ４１６－４は、複数のセグメントの１つ１つにそれぞれ格納されたデータの正当性確認状況の表示（例えば、正当性確認状況を示す値）を提供してもよい。図４に示した例では、複数のセグメントのうちの第１の数のセグメントに格納されたデータの正当性確認は完了しているが、複数のセグメントのうちの第２の数のセグメントに格納されたデータの正当性確認はまだ完了していない（例えば、メモリへの電力供給は完了しているが、第２の数のセグメントに格納されたデータの正当性確認はまだ開始されていない）。したがって、レジスタ４１６－４は、図４に示すように、セグメント４２０－１に格納されたデータの正当性確認が行われたことを示す表示、セグメント４２０－２に格納されたデータの正当性確認が行われたことを示す表示、セグメント４２０－３に格納されたデータの正当性確認が行われたことを示す表示、セグメント４２０－４に格納されたデータの正当性確認が行われていないことを示す表示、及びセグメント４２０－５に格納されたデータの正当性確認が行われていないことを示す表示を提供することができる。

【００５５】

図４に示すように、セグメントに格納されたデータの正当性確認が（例えば、レジスタ４１６－４によって提供される、そのセグメントの値によって示されるように）行われた場合、レジスタ４１６－５は、そのセグメントに格納されたデータの正当性確認の結果の表示（例えば、結果を示す値）を提供してもよい。図４に示した例では、レジスタ４１６－５は、図４に示すように、セグメント４２０－１に格納されたデータが正当であると判定されたことを示す表示、セグメント４２０－２に格納されたデータが正当ではないと判定されたことを示す表示、及びセグメント４２０－３に格納されたデータが正当ではないと判定されたことを示す表示を提供している。さらに、セグメント４２０－４及び４２０－５に格納されたデータは（例えば、レジスタ４１６－４によって提供される、それらのセグメントの値によって示されるように）まだ正当性確認されていないので、図４に示したように、レジスタ４１６－５は、セグメント４２０－４または４２０－５の値を提供していない（例えば、値を含まない）。

【００５６】

本明細書で（例えば、図２に関連して）既述のように、セグメントに格納されたデータの正当性確認の結果、データが（例えば、レジスタ４１６－５によって提供される、そのセグメントの値によって示されるように）正当ではないと判定された場合、そのセグメントに格納されたデータを修復してもよい。図４に示すように、レジスタ４１６－６は、複数のセグメントの１つ１つにそれぞれ格納されたデータの修復が許可されているかどうかの表示（例えば、許可されているかどうかを示す値）を提供してもよい。例えば、図４に示した例では、レジスタ４１６－６は、セグメント４２０－１に格納されたデータの修復が許可されていることを示す表示、セグメント４２０－２に格納されたデータの修復が許可されていることを示す表示、セグメント４２０－３に格納されたデータの修復が許可されていないことを示す表示、セグメント４２０－４に格納されたデータの修復が許可されていないことを示す表示、及びセグメント４２０－５に格納されたデータの修復が許可されていることを示す表示を提供している。

【００５７】

図４に示すように、セグメントに格納されたデータの修復が（例えば、レジスタ４１６－６によって提供される、そのセグメントの値によって示されるように）許可されている場合、レジスタ４１６－７は、そのセグメントに格納されたデータを、修復時に、そこから回復させることができるアドレス（例えば、アドレス値）を設定してもよい。レジスタ４１６－７によって設定されるアドレスは、例えば、データを、そこから回復させることができるメモリの修復ブロック内の位置に対応し得る。例えば、図４に示した例では、セ

グメント４２０－１に格納されたデータを、そこから回復させることができるアドレスは、レジスタ４１６－７によってａｄｄｒ１と設定されており、セグメント４２０－２に格納されたデータを、そこから回復させることができるアドレスは、レジスタ４１６－７によってａｄｄｒ２と設定されており、セグメント４２０－５に格納されたデータを、そこから回復させることができるアドレスは、レジスタ４１６－７によってａｄｄｒ３と設定されている。さらに、セグメント４２０－３及び４２０－４に格納されたデータの修復が（例えば、レジスタ４１６－６によって提供される、それらのセグメントの値によって示されるように）許可されていないので、レジスタ４１６－７は、図４に示したように、セグメント４２０－３または４２０－４に対してはアドレス値を設定していない（例えば、含まない）。

【００５８】

図４に示すように、セグメントに格納されたデータの修復が（例えば、レジスタ４１６－６によって提供される、そのセグメントの値によって示されるように）許可されている場合、レジスタ４１６－８は、修復の結果の表示（例えば、結果を示す値）を提供してもよい。図４に示した例では、レジスタ４１６－８は、（例えば、セグメント４２０－１に格納されたデータが正当であると判定された結果、そのデータを修復する必要がなかったので）セグメント４２０－１に格納されたデータが修復されていないという表示、（例えば、セグメント４２０－２に格納されたデータが正当ではないと判定されたが、修復することが許可されているので）セグメント４２０－２に格納されたデータが修復されているという表示、及び（例えば、セグメント４２０－５に格納されたデータが、まだ正当性確認されていないので）セグメント４２０－５に格納されたデータが修復されていないという表示を提供している。さらに、セグメント４２０－３及び４２０－４に格納されたデータの修復が（例えば、レジスタ４１６－６によって提供される、それらのセグメントの値によって示されるように）許可されていないので、レジスタ４１６－７は、図４に示したように、セグメント４２０－３または４２０－４に対する値を提供していない（例えば、含まない）。

【００５９】

図５は、本開示の実施形態による、暗号ハッシュを使用して、メモリに格納されたデータのセグメントを正当性確認する（例えば、正当性確認するかどうかを判定する）方法５２５を示す。メモリは、例えば、図２に関連して既に説明したメモリアレイ２０１であり得、本明細書で既に説明したように、複数のセグメントに分割され得る。方法５２５は、例えば、図２に関連して前に説明したメモリデバイス２０６（例えば、回路２１０）によって行い得る。

【００６０】

ブロック５２７において、方法５２５は、複数のメモリセグメントの１つに格納されたデータをメモリから取り出すことを含む。セグメントに格納されたデータは、本明細書で（例えば、図２に関連して）既に説明したように、レジスタ２１６－１及び２１６－２で設定された、そのセグメントのアドレス及びサイズを使用して取得することができる。

【００６１】

ブロック５２９において、方法５２５は、メモリセグメントに格納されたデータに対して実行時暗号ハッシュを生成することを含み、ブロック５３１において、方法５２５は、メモリセグメントに関連付けられたゴールデンハッシュを取得することを含む。ゴールデンハッシュは、本明細書で（例えば、図２に関連して）前に述べたように、レジスタ２１６－３から取得することができる。

【００６２】

ブロック５３３において、方法５２５は、実行時暗号ハッシュをゴールデンハッシュと比較することを含み、ブロック５３５において、方法５２５は、実行時暗号ハッシュがゴールデンハッシュと一致するかどうかを判定することを含む。実行時暗号ハッシュがゴールデンハッシュと一致すると判定された場合、ブロック５３７において、メモリセグメントに格納されたデータが正当であると確認される（例えば、正当であると判定される）。

実行時暗号ハッシュがゴールデンハッシュと一致しないと判定された場合、方法５２５はブロック５３９に進む。

【００６３】

ブロック５３９において、方法５２５は、メモリセグメントに格納されたデータの修復が許可されているかどうかを判定することを含む。メモリセグメントに格納されたデータの修復が許可されているかどうかの判定は、本明細書で（例えば、図２に関連して）既に説明したように、レジスタ２１６－６を用いて行うことができる。

【００６４】

メモリセグメントに格納されたデータの修復が許可されていると判定された場合、ブロック５４１においてデータが修復される。データの修復は、本明細書で（例えば、図２に関連して）既に説明したように、レジスタ２１６－７を使用してメモリからデータを回復させることを含み得る。メモリセグメントに格納されたデータの修復が許可されていないと判定された場合、ブロック５４３において、メモリセグメントに格納されたデータが正当ではないと確認される（例えば、正当ではないと判定される）。

【００６５】

図６は、本開示の実施形態による、ホスト６０２及びメモリデバイス６０６を含む例示的なシステムのブロック図である。ホスト６０２及びメモリデバイス６０６は、例えば、それぞれ図２に関連して既に説明したホスト２０２及びメモリデバイス２０６であり得る。

【００６６】

コンピューティングデバイスは、レイヤを使用して段階的に起動することができ、各レイヤが、後続のレイヤを認証してロードし、各レイヤで次第に高度化するランタイムサービスを提供する。あるレイヤが先行するレイヤからサービスを受け、後続のレイヤにサービスを提供することで、下位のレイヤの上に構築され、上位のレイヤにサービスを提供するレイヤの相互接続網が形成される。図６に示されているように、レイヤ０（「L_0」）６５１とレイヤ１（「L_1」）６５３とはホスト内にある。レイヤ０　６５１は、ファームウェアデリバティブシークレット（ＦＤＳ）鍵６５２をレイヤ１　６５３に提供し得る。ＦＤＳ鍵６５２は、レイヤ１　６５３のコードの識別情報及びその他のセキュリティ関連データを記述し得る。例では、特定のプロトコル（ロバストなモノのインターネット（ＲＩＯＴ）コアプロトコルなど）がＦＤＳ６５２を使用して、ロードするレイヤ１　６５３のコードの正当性を確認することができる。例では、特定のプロトコルは、デバイス識別構成エンジン（ｄｅｖｉｃｅ　ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ｃｏｍｐｏｓｉｔｉｏｎ　ｅｎｇｉｎｅ（ＤＩＣＥ））及び／またはＲＩＯＴコアプロトコルを含み得る。例として、ＦＤＳには、レイヤ１ファームウェアのイメージそのもの、認証されたレイヤ１ファームウェアを暗号で識別するマニフェスト、セキュアブート実装との関連で署名されたファームウェアのバージョン番号、及び／またはデバイス用のセキュリティクリティカル構成設定が含まれ得る。デバイスシークレット６５８が、ＦＤＳ６５２を作成するために使用され、ホスト６０２のメモリに格納され得る。

【００６７】

ホストは、矢印６５４で示されるように、データをメモリデバイス６０６に伝送し得る。伝送データには、公開されている外部識別、証明書（例えば、外部識別証明書）、及び／または外部公開鍵が含まれ得る。メモリデバイス６０６のレイヤ２（「L_2」）６５５は、伝送データを受け取り、オペレーティングシステム（「ＯＳ」）６５７の動作の際に、第１のアプリケーション６５９－１及び第２のアプリケーション６５９－２でデータを実行し得る。

【００６８】

例示的な動作では、ホスト６０２は、デバイスシークレット６５８を読み出し、レイヤ１　６５３の識別情報をハッシュし、

K_{L1}＝ＫＤＦ［Ｆｓ（ｓ），Ｈａｓｈ（「不変情報」）］

を含む計算を実行し得る。

上式で、K_{L1}は外部公開鍵であり、ＫＤＦ（例えば、Ｎａｔｉｏｎａｌ　Ｉｎｓｔｉｔｕｔｅ　ｏｆ　Ｓｔａｎｄａｒｄｓ　ａｎｄ　Ｔｅｃｈｎｏｌｏｇｙ（ＮＩＳＴ）　Ｓｐｅｃｉａｌ　Ｐｕｂｌｉｃａｔｉｏｎ　８００－１０８で定義されているＫＤＦ）は、鍵導出関数（例えば、ＨＭＡＣ－ＳＨＡ２５６）であり、Ｆｓ（ｓ）はデバイスシークレット６５８である。ＦＤＳ６５２は、

ＦＤＳ＝ＨＭＡＣ－ＳＨＡ２５６［Ｆｓ（ｓ），ＳＨＡ２５６（「不変情報」）］

を実行することで決定できる。

同様に、メモリデバイス６０６は、矢印６５６で示されるように、データをホスト６０２に伝送し得る。

【００６９】

図７は、本開示の実施形態による、いくつかのパラメータを決定するための例示的なプロセスのブロック図である。図７は、外部公開識別、外部証明書、及び外部公開鍵を含むパラメータの決定の例であり、これらは、その後、矢印７５４によって示されるように、メモリデバイス（例えば、図６の６０６）のレイヤ２（例えば、レイヤ２　６５５）に送られる。図７のレイヤ０（「L_0」）７５１は図６のレイヤ０　６５１に対応し、同様にＦＤＳ７５２はＦＤＳ６５２に対応し、レイヤ１　７５３はレイヤ１　６５３に対応し、矢印７５４及び７５６は、それぞれ矢印６５４及び６５６に対応する。

【００７０】

レイヤ０　７５１からのＦＤＳ　７５２は、レイヤ１　７５３に送られ、非対称ＩＤ生成器７６１によって使用されて、公開識別（「$ID_{lk公開}$」）７６５及び秘密識別７６７が生成される。略された「$ID_{lk公開}$」中、「ｌｋ」はレイヤｋ（この例ではレイヤ１）を示し、「公開」は、識別がオープンに共有されていることを示す。公開識別７６５は、ホストのレイヤ１　７５３の右側及び外側に延びる矢印によって共有されるように図示されている。生成された秘密識別７６７は、暗号化装置７７３に入力される鍵として使用される。暗号化装置７７３は、データを暗号化するために使用される任意のプロセッサ、コンピューティングデバイスなどであり得る。

【００７１】

ホストのレイヤ１　７５３は、非対称鍵生成器７６３を含み得る。少なくとも１つの例では、乱数発生器（ＲＮＤ）７３６が、非対称鍵生成器７６３に乱数を任意選択で入力し得る。非対称鍵生成器７６３は、図６のホスト６０２などのホストに関連付けられた公開鍵（「$K_{Lk公開}$」）７６９（外部公開鍵と呼ばれる）及び秘密鍵（「$K_{LK秘密}$」）７７１（外部秘密鍵と呼ばれる）を生成し得る。外部公開鍵７６９は、暗号化装置７７３への（「データ」としての）入力であり得る。暗号化装置７７３は、外部秘密識別７６７及び外部公開鍵７６９の入力を用いて、結果Ｋ’７７５を生成し得る。外部秘密鍵７７１及び結果Ｋ’７７５は、追加の暗号化装置７７７に入力することができ、その結果、出力Ｋ’’７７９が得られる。出力Ｋ’’７７９は、レイヤ２（図６の６５５）に伝送される外部証明書（「ID_{L1}証明書」）７８１である。外部証明書７８１は、デバイスから送られたデータの出所を検証及び／または認証する機能を提供し得る。例として、ホストから送られたデータは、図９に関連してさらに説明するように、証明書を検証することにより、ホストの識別情報に関連付けられ得る。さらに、外部公開鍵（「K_{L1}公開鍵」）７８３がレイヤ２に伝送され得る。したがって、ホストの公開識別７６５、証明書７８１、及び外部公開鍵７８３が、メモリデバイスのレイヤ２に伝送され得る。

【００７２】

図８は、本開示の実施形態による、いくつかのパラメータを決定するための例示的なプロセスのブロック図である。図８は、デバイス識別（「ID_{L2}公開」）８６６、デバイス証明書（「ID_{L2}証明書」）８８２、及びデバイス公開鍵（「K_{L2}公開鍵」）８８４を生成するメモリデバイス（例えば、図６のメモリデバイス６０６）のレイヤ２　８５５を示す。

【００７３】

図７で説明したように、ホストのレイヤ１からメモリデバイスのレイヤ２　８５５に伝

送された外部公開鍵（「K_{L1}公開鍵」）８８３は、メモリデバイスの非対称ＩＤ生成器８６２によって使用されて、メモリデバイスの公開識別（「$ID_{1k公開}$」）８６６及び秘密識別８６８を生成する。略された「$ID_{1k公開}$」中、「１ｋ」はレイヤｋ（この例ではレイヤ２）を示し、「公開」は、識別がオープンに共有されていることを示す。公開識別８６６は、レイヤ２　８５５の右側及び外側に延びる矢印によって共有されるように図示されている。生成された秘密識別８６８は、暗号化装置８７４に入力される鍵として使用される。

【００７４】

図８に示すように、外部証明書８８１及び公開識別８６５は、外部公開鍵８８３と共に、証明書検証器８９９によって使用される。証明書検証器８９９は、ホストから受け取られた外部証明書８８１を検証し、外部証明書８８１が検証されたことまたは検証されなかったことに応答して、ホストから受け取られたデータを受け入れるかまたは破棄するかを判定することができる。外部証明書８８１の検証の追加的な詳細については、本明細書で（例えば、図９に関連して）詳述する。

【００７５】

メモリデバイスのレイヤ２　８５５は、非対称鍵生成器８６４を含み得る。少なくとも１つの例では、乱数発生器（ＲＮＤ）８３８が、非対称鍵生成器８６４に乱数を任意選択で入力し得る。非対称鍵生成器８６４は、図６のメモリデバイス６０６などのメモリデバイスに関連付けられた公開鍵（「$K_{Lk公開}$」）８７０（デバイス公開鍵と呼ばれる）及び秘密鍵（「$K_{LK秘密}$」）８７２（デバイス秘密鍵と呼ばれる）を生成し得る。デバイス公開鍵８７０は、暗号化装置８７４への（「データ」としての）入力であり得る。暗号化装置８７４は、デバイス秘密識別８６８及びデバイス公開鍵８７０の入力を用いて、結果Ｋ’８７６を生成し得る。デバイス秘密鍵８７２及び結果Ｋ’８７６は、追加の暗号化装置８７８に入力することができ、その結果、出力Ｋ’’８８０が得られる。出力Ｋ’’８８０は、レイヤ１（図６の６５３）に返送されるデバイス証明書（「ID_{L2}証明書」）８８２である。デバイス証明書８８２は、デバイスから送られたデータの出所を検証及び／または認証する機能を提供し得る。例として、メモリデバイスから送られたデータは、図９に関連してさらに説明するように、証明書を検証することにより、メモリデバイスの識別情報に関連付けられ得る。さらに、デバイス公開鍵（「K_{L2}公開鍵」）８８４がレイヤ１に伝送され得る。したがって、メモリデバイスの公開識別８６６、証明書８８２、及びデバイス公開鍵８８４が、ホストのレイヤ１に伝送され得る。

【００７６】

例では、ホストがメモリデバイスから公開鍵を受け取ることに応答して、ホストは、デバイス公開鍵を使用して、メモリデバイスに送るべきデータを暗号化し得る。逆に、メモリデバイスは、外部公開鍵を使用して、ホストに送るべきデータを暗号化し得る。メモリデバイスが、デバイス公開鍵を用いて暗号化されたデータを受け取ったことに応答して、メモリデバイスは、それ自体のデバイス秘密鍵を用いてデータを復号化してもよい。同様に、ホストが、外部公開鍵を用いて暗号化されたデータを受け取ることに応答して、ホストは、それ自体の外部秘密鍵を用いてデータを復号化してもよい。デバイス秘密鍵はメモリデバイス以外の別のデバイスとは共有されず、外部秘密鍵はホスト以外の別のデバイスとは共有されないので、メモリデバイス及びホストに送られるデータはセキュアに保たれる。

【００７７】

図９は、本開示の実施形態による、証明書を検証するための例示的なプロセスのブロック図である。図９の図示された例では、公開鍵９８３、証明書９８１、及び公開識別９６５がホストから（例えば、図６のホスト６０２のレイヤ１　６５３から）提供される。証明書９８１及び外部公開鍵９８３のデータは、復号器９８５への入力として使用され得る。復号器９８５は、データを復号化するために使用される任意のプロセッサ、コンピューティングデバイスなどであり得る。証明書９８１及び外部公開鍵９８３の復号化の結果は、公開された識別と共に、二次復号器９８７への入力として使用することができ、出力を

もたらす。外部公開鍵９８３と復号器９８７からの出力とは、９８９に示されているように、証明書が検証されているかどうかを示すことができ、出力として「はい」または「いいえ」９９１をもたらす。証明書が検証されたことに応答して、検証されたデバイスから受け取られたデータを受け入れ、復号化し、処理することができる。証明書が検証されなかったことに応答して、検証されたデバイスから受け取られたデータを破棄し、削除し、及び／または無視することができる。このようにして、不正なデータを送る不正なデバイスを検出して回避することができる。例として、処理対象のデータを送信しているハッカーを特定し、ハッキングデータを処理しないようにすることができる。

【００７８】

図１０は、本開示の実施形態による、署名を検証するための例示的なプロセスのブロック図である。デバイスが後の否認を回避するために検証可能なデータを送信している場合では、署名を生成してデータと共に送信することができる。例として、第１のデバイスが第２のデバイスにリクエストを行い、第２のデバイスがそのリクエストを実行すると、第１のデバイスは、第１のデバイスがそのようなリクエストを行っていないことを示すことがある。署名を使用するなどの否認防止アプローチにより、第１のデバイスによる否認を回避し、第２のデバイスが、要求されたタスクを、その後の支障もなく実行できることを保証することができる。

【００７９】

メモリデバイス１００６（図２のメモリデバイス２０６など）が、データ１０９０をホスト（図２のホスト２０２など）に送り得る。メモリデバイス１００６は、１０９４で、デバイス秘密鍵１０７１を用いて、署名１０９６を生成し得る。署名１０９６は、ホスト１００２に伝送され得る。ホスト１００２は、１０９８で、以前に受け取ったデータ１０９２及び外部公開鍵１０６９を使用して署名を検証し得る。このようにして、署名は秘密鍵を使用して生成され、公開鍵を使用して検証される。このようにして、一意の署名を生成するために使用される秘密鍵は、署名を送るデバイスに対しては非公開のままにすることができ、一方で受信デバイスは、検証のために送信デバイスの公開鍵を使用して署名を復号化することができる。このことは、送信デバイスが受信デバイスの公開鍵を用いて暗号化し、受信デバイスが受信側の秘密鍵を用いて復号化するデータの暗号化／復号化とは対照的である。少なくとも１つの例では、デバイスは、内部暗号プロセス（例えば、楕円曲線デジタル署名（ＥＣＤＳＡ））または同様のプロセスを使用してデジタル署名を検証することができる。

【００８０】

図１１は、本開示の実施形態による、例示的なメモリデバイス１１０６のブロック図である。メモリデバイス１１０６は、例えば、図２に関連して既に説明したメモリデバイス２０６であり得る。

【００８１】

図１１に示すように、メモリデバイス１１０６は、いくつかのメモリアレイ１１０１－１～１１０１－７を含み得る。メモリアレイ１１０１－１～１１０１－７は、図１に関連して既に説明したメモリアレイ１０１に類似し得る。さらに、図１０に示す例では、メモリアレイ１１０１－３がセキュアアレイであり、メモリアレイ１１０１－６のサブセット１１１１がセキュアアレイを含み、メモリアレイ１１０１－７のサブセット１１１３及び１１１５がセキュアアレイを含む。サブセット１１１１、１１１３、及び１１１５はそれぞれ、例えば、４キロバイトのデータを含んでもよい。ただし、本開示の実施形態は、メモリアレイまたはセキュアアレイの特定の数または配置に限定されるものではない。

【００８２】

図１１に示すように、メモリデバイス１１０６は、修復（例えば、回復）ブロック１１１７を含み得る。修復ブロック１１１７は、メモリデバイス１１０６の動作中に発生する可能性のあるエラー（例えば、不一致）の場合に、及び／または本明細書で以前に説明したように、アレイ１１０１－１～１１０１－７に格納されたデータが正当ではないと判定された場合に、データのソースとして使用することができる。修復ブロック１１１７は、

ホストによってアドレス指定可能なメモリデバイス１１０６の領域の外側にあってもよい。

【００８３】

図１１に示すように、メモリデバイス１１０６は、シリアルペリフェラルインターフェース（ＳＰＩ）１１０４及びコントローラ１１０８を含み得る。メモリデバイス１１０６は、本明細書で（例えば、図２に関連して）既に説明したように、ＳＰＩ１１０４及びコントローラ１１０８を使用して、ホスト及びメモリアレイ１１０１－１～１１０１－７と通信し得る。

【００８４】

図１１に示すように、メモリデバイス１１０６は、メモリデバイス１１０６のセキュリティを管理するためのセキュアレジスタ１１１９を含んでもよい。例えば、セキュアレジスタ１１１９は、アプリケーションコントローラを構成し、アプリケーションコントローラと外部的に通信し得る。さらに、セキュアレジスタ１１１９は、認証コマンドによって変更可能であってもよい。

【００８５】

図１１に示すように、メモリデバイス１１０６は、鍵１１２１を含み得る。例えば、メモリデバイス１１０６は、ルート鍵、ＤＩＣＥ－ＲＩＯＴ鍵、及び／または他の外部セッション鍵などの鍵を格納するために、８つの異なるスロットを含み得る。

【００８６】

図１１に示すように、メモリデバイス１１０６は、電子的に消去可能なプログラマブルリードオンリーメモリ（ＥＥＰＲＯＭ）１１２３を含み得る。ＥＥＰＲＯＭ１１２３は、ホストが利用できるセキュアな不揮発性領域を提供することができ、その中でデータの個々のバイトを消去し、プログラムすることが可能である。

【００８７】

図１１に示すように、メモリデバイス１００６は、カウンタ（例えば、単調カウンタ）１１２４を含み得る。カウンタ１１２４は、ホストから受け取られる、及び／またはホストに送られる（例えば、コマンドセットまたはシーケンスに署名する）コマンドのアンチリプレイ機構（例えば、フレッシュネス生成器）として使用することができる。例えば、メモリデバイス１１０６は、６つの異なる単調カウンタを含むことができ、そのうちの２つは、認証されたコマンドのためにメモリデバイス１１０６によって使用されてもよく、そのうちの４つは、ホストによって使用されてもよい。

【００８８】

図１１に示すように、メモリデバイス１１０６は、ＳＨＡ－２５６暗号ハッシュ関数１１２６、及び／またはＨＭＡＣ－ＳＨＡ２５６暗号ハッシュ関数１１２８を含み得る。ＳＨＡ－２５６及び／またはＨＭＡＣ－ＳＨＡ２５６暗号ハッシュ関数１１２６及び１１２８は、メモリデバイス１１０６によって使用されて、例えば、本明細書で既に説明したように、メモリアレイ１１０１－１～１１０１－７に格納されたデータの正当性を確認するために使用される実行時暗号ハッシュ及び／またはゴールデンハッシュなどの暗号ハッシュを生成することができる。さらに、メモリデバイス１１０６は、ＤＩＣＥ－ＲＩＯＴ１１３０のＬ０及びＬ１をサポートすることができる。

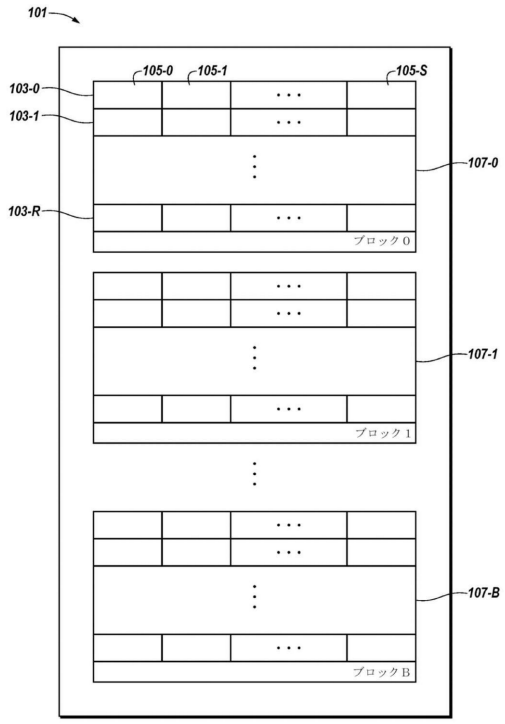
【００８９】

本明細書には、特定の実施形態を示して説明してきたが、当業者であれば、同じ結果を得るように意図された構成が、示した特定の実施形態の代わりになり得ることを理解するであろう。本開示は、本開示のいくつかの実施形態の適合形態または変形形態を含むことを意図する。上記の説明は、例示目的であり、限定目的ではないことを理解されたい。上記の実施形態の組み合わせ、及び本明細書に具体的に記載されていない他の実施形態は、上記の説明を検討することで、当業者には明らかとなるであろう。本開示のいくつかの実施形態の範囲は、上記の構造及び方法が使用される他の用途を含む。したがって、本開示のいくつかの実施形態の範囲は、添付の特許請求の範囲と、添付の特許請求の範囲に権利を与えられた内容と同等物の全範囲とを参照して、特定されるべきである。

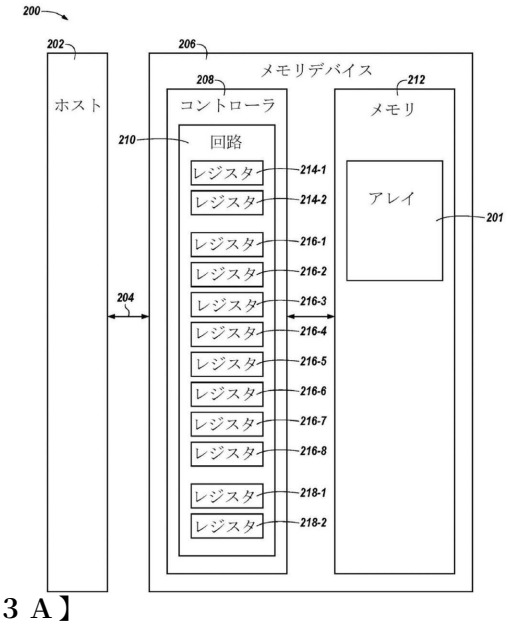
【００９０】

前述の発明を実施するための形態では、本開示を簡素化する目的で、いくつかの特徴が単一の実施形態にまとめられている。本開示の方法は、本開示の開示された実施形態が、各請求項に明確に列挙された特徴より多くの特徴を使用する必要があるという意図を反映するものとして、解釈されるべきではない。むしろ、下記の特許請求の範囲が反映するように、発明の主題は、開示された単一の実施形態の全ての特徴よりも少ない特徴で存在する。したがって、以下の特許請求の範囲は、本明細書によって詳細な説明に組み込まれ、各請求項は別個の実施形態として自立する。

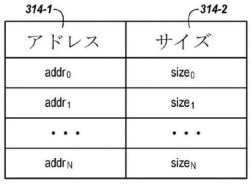
【図１】



【図２】

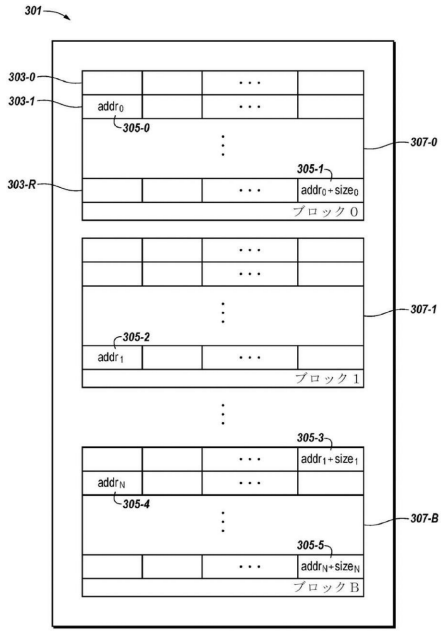


【図３Ａ】

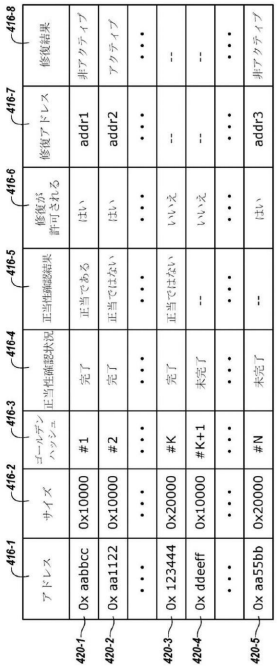


314-1 アドレス	314-2 サイズ
$addr_0$	$size_0$
$addr_1$	$size_1$
・・・	・・・
$addr_N$	$size_N$

【図３Ｂ】

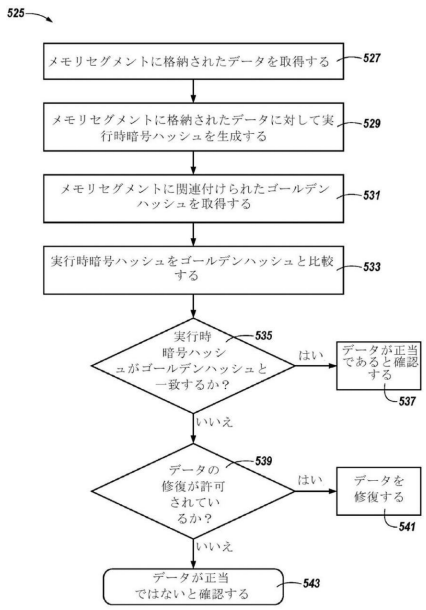


【図４】

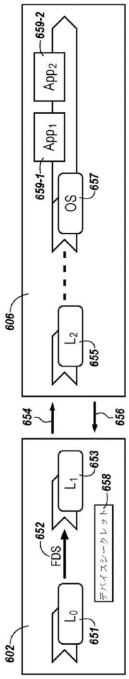


	416-1 アドレス	416-2 サイズ	416-3 ゴールデンハッシュ	416-4 正当性確認状況	416-5 正当性確認結果	416-6 修復が許可される	416-7 修復アドレス	416-8 修復結果
420-1	0x aabbcc	0x10000	#1	完了	正当である	はい	addr1	非アクティブ
420-2	0x aa1122	0x10000	#2	完了	正当ではない	はい	addr2	アクティブ
	...	...	...	...	...	...	...	...
420-3	0x 123444	0x20000	#K	完了	正当ではない	いいえ	--	--
420-4	0x ddeeff	0x10000	#K+1	未完了	--	いいえ	--	--
	...	...	...	...	...	...	...	...
420-5	0x aa55bb	0x20000	#N	未完了	--	はい	addr3	非アクティブ

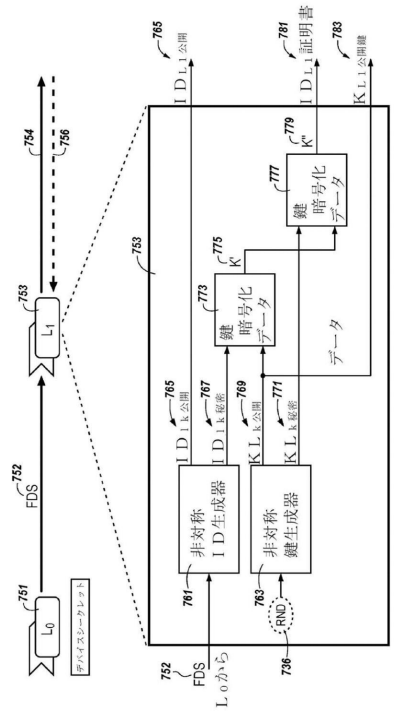
【図５】



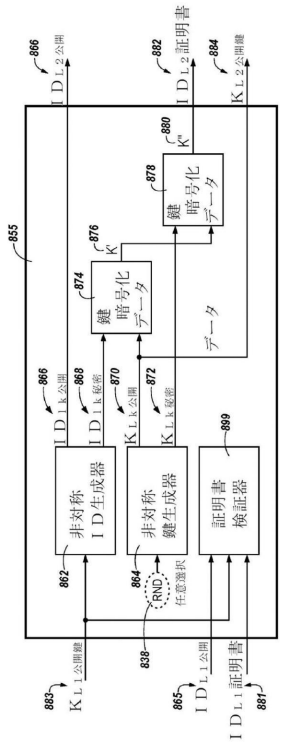
【図６】



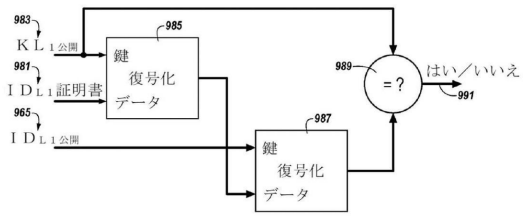
【図７】



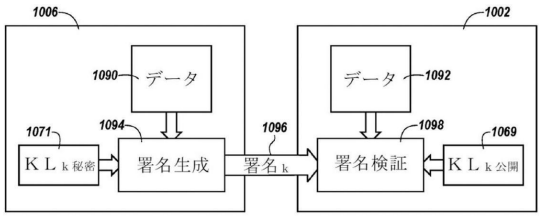
【図８】



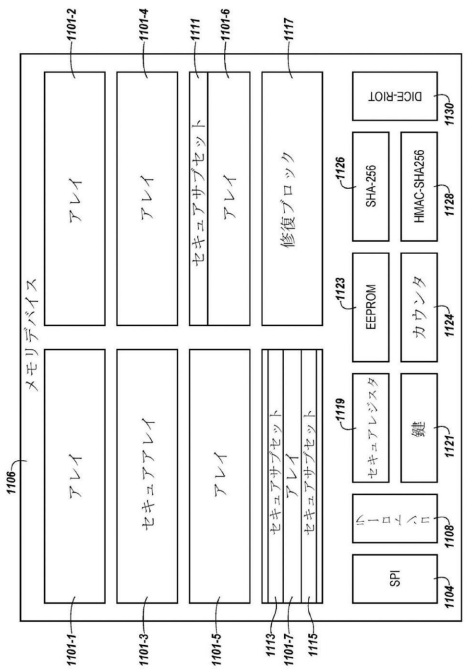
【図９】



【図１０】



【図１１】



【手続補正書】
【提出日】令和3年11月22日(2021.11.22)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
メモリと、
回路であって、
前記メモリを複数のセグメントに分割することであって、各セグメントがそれぞれ異なる暗号ハッシュに関連付けられている、前記分割することと、
前記メモリへの電力供給時に、前記複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと、
前記メモリへの前記電力供給後に、前記複数のセグメントのうちの第２の数のセグメントに格納されたデータ、前記複数のセグメントのうちの第２の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと
を行うように構成されている、前記回路と
を備える、装置。
【請求項２】
前記回路が、前記第１の数の前記セグメントの１つ１つにそれぞれ格納された前記データ、または前記第２の数の前記セグメントの１つ１つにそれぞれ格納された前記データの正当性を、
前記第１の数の前記セグメントの１つ１つにそれぞれ格納された前記データに対して、または前記第２の数の前記セグメントの１つ１つにそれぞれ格納された前記データに対して、異なる実行時暗号ハッシュを生成することと、
各セグメントにそれぞれ格納された前記データに対して生成した前記実行時暗号ハッシュを、その各セグメントに関連付けられた前記暗号ハッシュと比較することと
によって確認するように構成されている、請求項１に記載の装置。
【請求項３】
前記回路が、
前記メモリへの前記電力供給後に、前記第１の数の前記セグメントの１つ１つにそれぞれ格納された前記データを、その前記第１の数の前記セグメントの１つ１つにそれぞれ格納された前記データの正当性を確認すると、ホストに送ることと、
前記第２の数の前記セグメントの１つ１つにそれぞれ格納された前記データを、その前記第２の数の前記セグメントのそれぞれ１つに格納された前記データの正当性を確認すると、前記ホストに送ることと
を行うように構成されている、請求項１に記載の装置。
【請求項４】
前記メモリが、メモリセルのセキュアアレイを備え、
前記回路が、
前記セキュアアレイのアドレスを設定するように構成されたレジスタと、
前記セキュアアレイのサイズを設定するように構成されたレジスタと
を含む、請求項１～３のいずれか１項に記載の装置。
【請求項５】
前記回路が、各セグメントにそれぞれ関連付けられた前記暗号ハッシュを格納するように構成されたレジスタを含み、

前記レジスタが、前記メモリのユーザにとってアクセス不可能である、請求項１～３のいずれか１項に記載の装置。
【請求項６】
メモリを動作させる方法であって、
前記メモリを複数のセグメントに分割することであって、各セグメントがそれぞれ異なる暗号ハッシュに関連付けられている、前記分割することと、
前記メモリへの電力供給時に、前記複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータに対して異なる実行時暗号ハッシュを生成することと、
前記メモリへの前記電力供給時に、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を、その各セグメントに格納された前記データに対して生成した前記実行時暗号ハッシュと、その各セグメントに関連付けられた前記暗号ハッシュとを比較することによって確認することと、
前記メモリへの前記電力供給後に、前記複数のセグメントのうちの第２の数のセグメントの１つ１つにそれぞれ格納されたデータに対して異なる実行時暗号ハッシュを生成することと、
前記メモリへの前記電力供給後に、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を、その各セグメントに格納された前記データに対して生成した前記実行時暗号ハッシュと、その各セグメントに関連付けられた前記暗号ハッシュとを比較することによって確認することと
を含む、前記方法。
【請求項７】
前記方法が、
前記複数のセグメントのうちの前記第１の数のセグメントについての前記比較により、その各セグメントに格納された前記データに対して生成された前記実行時暗号ハッシュが、その各セグメントに関連付けられた前記暗号ハッシュと一致することが示されることに基づいて、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を確認することと、
前記複数のセグメントのうちの前記第２の数のセグメントについての前記比較により、その各セグメントに格納された前記データに対して生成された前記実行時暗号ハッシュが、その各セグメントに関連付けられた前記暗号ハッシュと一致することが示されることに基づいて、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を確認することと
を含む、請求項６に記載の方法。
【請求項８】
前記方法が、
前記複数のセグメントのうちの前記第１の数のセグメントについての前記比較により、その各セグメントに格納された前記データに対して生成された前記実行時暗号ハッシュが、その各セグメントに関連付けられた前記暗号ハッシュと一致しないことが示されることに基づいて、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを修復することと、
前記複数のセグメントのうちの前記第２の数のセグメントについての前記比較により、その各セグメントに格納された前記データに対して生成された前記実行時暗号ハッシュが、その各セグメントに関連付けられた前記暗号ハッシュと一致しないことが示されることに基づいて、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データを修復することと
を含む、請求項６に記載の方法。
【請求項９】
メモリを動作させる方法であって、
前記メモリを複数のセグメントに分割することであって、各セグメントがそれぞれ異な

る暗号ハッシュに関連付けられている、前記分割することと、
前記メモリへの電力供給時に、前記複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと、
前記メモリへの前記電力供給後に、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを、その前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を確認すると、ホストに送ることと、
前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを前記ホストに送っている間に、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと
を含む、前記方法。
【請求項１０】
前記方法が、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを前記ホストに送った後に、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データを、その前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を確認すると、前記ホストに送ること
を含む、請求項９に記載の方法。
【請求項１１】
前記方法が、前記ホストから受け取った認証済みコマンドを使用して、各セグメントにそれぞれ関連付けられた前記暗号ハッシュを生成すること
を含む、請求項９～１０のいずれか１項に記載の方法。
【請求項１２】
メモリを有するメモリデバイスであって、
前記メモリが複数のセグメントに分割され、各セグメントがそれぞれ異なる暗号ハッシュに関連付けられており、
前記メモリデバイスが、
前記メモリへの電力供給時に、前記複数のセグメントのうちの第１の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと、
前記メモリへの電力供給後に、前記複数のセグメントのうちの第２の数のセグメントの１つ１つにそれぞれ格納されたデータの正当性を、その各セグメントに関連付けられた前記暗号ハッシュを使用して確認することと
を行うように構成されている、前記メモリデバイスと、
ホストであって、前記ホストが、
前記複数のセグメントのうちの前記第２の数のセグメントに格納された前記データの正当性を前記メモリデバイスが確認している間に、前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを、その前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を前記メモリデバイスが確認すると、前記メモリデバイスから受け取ることと、
前記複数のセグメントのうちの前記第１の数のセグメントの１つ１つにそれぞれ格納された前記データを前記メモリデバイスから受け取った後に、前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データを、その前記複数のセグメントのうちの前記第２の数のセグメントの１つ１つにそれぞれ格納された前記データの正当性を前記メモリデバイスが確認すると、前記メモリデバイスから受け取ることと
を行うように構成されている、前記ホストと
を備える、システム。

【請求項１３】
前記メモリデバイスが、
前記複数のセグメントの１つ１つそれぞれのアドレスを設定するように構成されたレジスタと、
前記複数のセグメントの１つ１つそれぞれのサイズを設定するように構成されたレジスタと、
前記複数のセグメントの１つ１つにそれぞれ格納された前記データの前記正当性確認の状況の表示を提供するように構成されたレジスタと、
前記複数のセグメントの１つ１つにそれぞれ格納された前記データの前記正当性確認の結果の表示を提供するように構成されたレジスタと、
前記複数のセグメントの１つ１つにそれぞれ格納された前記データの修復が許可されているかどうかの表示を提供するように構成されたレジスタと、
前記複数のセグメントの１つ１つにそれぞれ格納された前記データを、修復時に、回復させることができる前記メモリのアドレスを設定するように構成されたレジスタと、
前記複数のセグメントの１つ１つにそれぞれ格納された前記データの前記修復の結果の表示を提供するように構成されたレジスタと
を含む、請求項１２に記載のシステム。
【請求項１４】
前記複数のセグメントのうちの前記第１の数のセグメントが、前記ホストによって設定された特定の数量のセグメントを含み、
前記メモリデバイスが、前記特定の数量のセグメントを格納するように構成されたレジスタを含む、請求項１２～１３のいずれか１項に記載のシステム。
【請求項１５】
前記複数のセグメントのうちの前記第１の数のセグメントが、特定の時間内に前記メモリデバイスによって正当性確認することが可能な数量のセグメントを含み、
前記メモリデバイスが、前記特定の時間を格納するように構成されたレジスタを含む、請求項１２～１３のいずれか１項に記載のシステム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2020/022931

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/79(2013.01)i, G06F 21/60(2013.01)i, G06F 21/72(2013.01)i, G06F 12/14(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/79; G06F 12/02; G06F 12/14; G06F 21/00; G06F 21/56; G06F 21/57; G06F 9/50; H04L 9/32; G06F 21/60; G06F 21/72

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: memory, divide, segment, hash, validate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010-0106976 A1 (ONUR ACIICMEZ et al.) 29 April 2010 Paragraphs [0020], [0037]-[0040], [0055]-[0059], [0064], [0070]; claims 22-24; and figures 1C, 3B	1-20
Y	US 2014-0351544 A1 (DAVID ABZARIAN et al.) 27 November 2014 Paragraphs [0005], [0018]-[0019], [0023], [0028]-[0031], [0042]; claims 1, 5, 8; and figures 1, 5	1-20
A	US 2016-0246736 A1 (TELEPUTERS, LLC) 25 August 2016 Paragraphs [0016]-[0017], [0040], [0058]; and figure 1	1-20
A	US 2015-0324588 A1 (KEVIN B. LOCKE) 12 November 2015 Paragraphs [0027], [0032]; claim 1; and figure 2	1-20
A	KR 10-2018-0126379 A (SAMSUNG ELECTRONICS CO., LTD.) 27 November 2018 Paragraphs [0034], [0109]; and figure 6	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 July 2020 (09.07.2020)	**09 July 2020 (09.07.2020)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
YANG JEONG ROK
Telephone No. +82-42-481-5709

Form PCT/ISA/210 (second sheet) (July 2019)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/022931

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0106976 A1	29/04/2010	US 8788841 B2	22/07/2014
US 2014-0351544 A1	27/11/2014	US 2010-0174921 A1	08/07/2010
		US 8806220 B2	12/08/2014
		US 9542337 B2	10/01/2017
US 2016-0246736 A1	25/08/2016	US 2010-0281273 A1	04/11/2010
		US 2018-0045189 A1	15/02/2018
		US 8738932 B2	27/05/2014
		US 9784260 B2	10/10/2017
		US 9989043 B2	05/06/2018
US 2015-0324588 A1	12/11/2015	US 9317691 B2	19/04/2016
KR 10-2018-0126379 A	27/11/2018	CN 108959113 A	07/12/2018
		US 2018-0336140 A1	22/11/2018

フロントページの続き

(81)指定国・地域 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

(72)発明者 モンデッロ アントニノ
イタリア共和国 ９８１４８ メッシーナ ヴィア コムナーレ サント ３７０／Ａ

Ｆターム(参考) 5B160 AA12