(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2018-22486
(P2018-22486A)
(43)公開日　平成30年2月8日(2018.2.8)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/62 (2013.01)	G06F 21/62	

審査請求 未請求　請求項の数 20　ＯＬ　（全 28 頁）

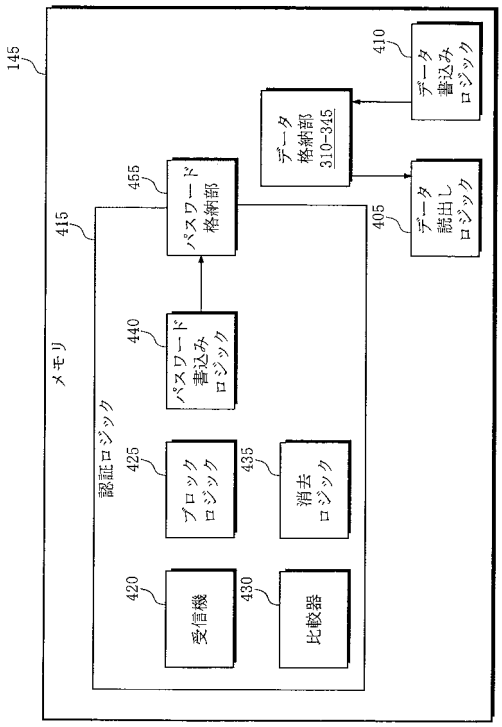
(21)出願番号	特願2017-146478 (P2017-146478)
(22)出願日	平成29年7月28日 (2017.7.28)
(31)優先権主張番号	62/370,230
(32)優先日	平成28年8月2日 (2016.8.2)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	15/275,337
(32)優先日	平成28年9月23日 (2016.9.23)
(33)優先権主張国	米国 (US)

(71)出願人　390019839
三星電子株式会社
Ｓａｍｓｕｎｇ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｃｏ．，Ｌｔｄ．
大韓民国京畿道水原市霊通区三星路１２９　１２９，Ｓａｍｓｕｎｇ－ｒｏ，Ｙｅｏｎｇｔｏｎｇ－ｇｕ，Ｓｕｗｏｎ－ｓｉ，Ｇｙｅｏｎｇｇｉ－ｄｏ，Ｒｅｐｕｂｌｉｃ　ｏｆ　Ｋｏｒｅａ
(74)代理人　110000051
特許業務法人共生国際特許事務所
(72)発明者　ソンポン　ポール　オラリグ
アメリカ合衆国，　カリフォルニア州　９４５６６，　プレザントン，　パセオ　グラナダ，　３０５０

最終頁に続く

(54)【発明の名称】メモリ及びメモリへの不正アクセス防止方法

(57)【要約】
【課題】メモリに格納されたデータに対する不正アクセスを防止するために保安化されたメモリ、及びメモリへの不正アクセス防止方法を提供する。
【解決手段】本発明によるメモリは、第１使用者に対するデータのためのデータ格納部と、データ格納部からデータを読み出すデータ読出しロジックと、データ格納部にデータを書き込むデータ書込みロジックと、格納パスワードのためのパスワード格納部と、メモリコントローラから受信パスワードを受信する受信機と、受信パスワードと格納パスワードとを比較する比較器と、受信パスワードが格納パスワードと異なる場合、データ格納部のデータを消去する消去ロジックと、比較器が動作を完了する時までメモリコントローラからデータ格納部へのアクセスを遮断するブロックロジックと、を有し、受信パスワード又は格納パスワードは、メモリに格納されたデータを暗号化するのには用いない。
【選択図】　図４



【特許請求の範囲】
【請求項１】
メモリであって、
第１使用者に対するデータのためのデータ格納部と、
前記データ格納部からデータを読み出すデータ読出しロジックと、
前記データ格納部にデータを書き込むデータ書込みロジックと、
格納パスワードのためのパスワード格納部と、
メモリコントローラから受信パスワードを受信する受信機と、
前記受信パスワードと前記格納パスワードとを比較する比較器と、
前記受信パスワードが前記格納パスワードと異なる場合、前記データ格納部の前記データを消去する消去ロジックと、
前記比較器が動作を完了する時まで前記メモリコントローラから前記データ格納部へのアクセスを遮断するブロックロジックと、を有し、
前記受信パスワード又は前記格納パスワードは、前記メモリに格納されたデータを暗号化するのには用いないことを特徴とするメモリ。
【請求項２】
前記ブロックロジックは、前記消去ロジックが動作を完了する時まで前記メモリコントローラから前記データ格納部へのアクセスを遮断するよう動作することを特徴とする請求項１に記載のメモリ。
【請求項３】
前記パスワード格納部に前記受信パスワードを書き込むパスワード書込みロジックをさらに有することを特徴とする請求項１に記載のメモリ。
【請求項４】
前記メモリが保安（ｓｅｃｕｒｅ）モードで動作している否かを明示するための直列プレゼンス検出（Ｓｅｒｉａｌ　Ｐｒｅｓｅｎｃｅ　Ｄｅｔｅｃｔ：ＳＰＤ）をさらに有することを特徴とする請求項１に記載のメモリ。
【請求項５】
前記ブロックロジックは、前記メモリが前記保安モードで動作していないと前記ＳＰＤが明示した場合、前記比較器の呼び出しなしに、前記メモリコントローラが前記データ格納部にアクセスすることを許容することを特徴とする請求項４に記載のメモリ。
【請求項６】
前記消去ロジックは、閾値（ｔｈｒｅｓｈｏｌｄ）回数の受信パスワードが全て前記格納パスワードと異なる場合、前記データ格納部の前記データを消去するよう動作することを特徴とする請求項１に記載のメモリ。
【請求項７】
前記メモリは、揮発性メモリモジュール、不揮発性メモリモジュール、及び揮発性メモリ及び不揮発性メモリ装置の任意に組み合わせを含むセットから引き出されることを特徴とする請求項１に記載のメモリ。
【請求項８】
前記受信機、前記比較器、前記消去ロジック、及び前記ブロックロジックを含むレジスタークロックドライバー（Ｒｅｇｉｓｔｅｒ　Ｃｌｏｃｋ　Ｄｒｉｖｅｒ：ＲＣＤ）をさらに有することを特徴とする請求項１に記載のメモリ。
【請求項９】
メモリがリセットされたかどうかを決定する段階と、
前記メモリが保安モードで動作しているか、非保安（ｎｏｎ－ｓｅｃｕｒｅ）モードで動作しているかを決定する段階と、
前記メモリが前記保安モードで動作している場合、使用者に対するパスワードを選択する段階と、
前記メモリに前記パスワードを伝送する段階と、
前記メモリへのアクセスを受ける段階と、を有し、

前記パスワードは、前記メモリに格納されたデータを暗号化するのには用いないことを特徴とするメモリへの不正アクセス防止方法。
【請求項１０】
前記メモリが前記非保安モードで動作している場合、前記パスワードを用いることなしに、前記メモリへのアクセスを受ける段階をさらに有することを特徴とする請求項９に記載のメモリへの不正アクセス防止方法。
【請求項１１】
前記メモリに前記パスワードを伝送する段階は、前記パスワードを閾値（ｔｈｒｅｓｈｏｌｄ）回数にて前記メモリに伝送する段階を含むことを特徴とする請求項９に記載のメモリへの不正アクセス防止方法。
【請求項１２】
前記メモリへのアクセスを受ける段階は、消去されたメモリへのアクセスを受ける段階を含むことを特徴とする請求項９に記載のメモリへの不正アクセス防止方法。
【請求項１３】
前記メモリがリセットされた以後の時間量を測定する段階と、
前記メモリがリセットされた以後の前記時間量が閾値より大きい場合、前記メモリにソフトウェア誘導リセットを伝送する段階と、をさらに有する請求項９に記載のメモリへの不正アクセス防止方法。
【請求項１４】
メモリが保安モードで動作していることを示す信号を前記メモリからメモリコントローラに伝送する段階と、
前記メモリコントローラから受信パスワードを受信する段階と、
前記受信パスワードと格納パスワードとを比較する段階と、
前記受信パスワードが前記格納パスワードと一致しない場合、前記メモリを消去する段階と、
前記メモリへのアクセスを前記メモリコントローラに提供する段階と、を有し、
前記受信パスワード又は前記格納パスワードは、前記メモリに格納されたデータを暗号化するのには用いないことを特徴とするメモリへの不正アクセス防止方法。
【請求項１５】
前記受信パスワードが前記格納パスワードと一致しない場合、前記メモリに前記受信パスワードを格納する段階をさらに有することを特徴とする請求項１４に記載のメモリへの不正アクセス防止方法。
【請求項１６】
前記受信パスワードが前記格納パスワードと一致する場合、前記メモリへのアクセスを前記メモリコントローラに提供する段階をさらに有することを特徴とする請求項１４に記載のメモリへの不正アクセス防止方法。
【請求項１７】
前記メモリを消去する前に、閾値回数にて前記受信パスワードと前記格納パスワードとを比較する段階をさらに有することを特徴とする請求項１４に記載のメモリへの不正アクセス防止方法。
【請求項１８】
前記メモリコントローラからリセット命令を受信する段階と、
前記リセット命令に応答して前記メモリをリセットする段階と、をさらに有することを特徴とする請求項１４に記載のメモリへの不正アクセス防止方法。
【請求項１９】
前記メモリが前記保安モードで動作していることを示す前記信号を前記メモリから前記メモリコントローラに伝送する段階は、前記メモリが前記保安モードで動作しているかどうかに対して前記メモリコントローラからの要請を受信する段階を含むことを特徴とする請求項１４に記載のメモリへの不正アクセス防止方法。
【請求項２０】

前記メモリコントローラから前記受信パスワードを受信する段階は、前記メモリコントローラから前記パスワードを要請する段階を含むことを特徴とする請求項１４に記載のメモリへの不正アクセス防止方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明はメモリに関し、時に、メモリに格納されたデータに対する不正アクセスを防止するために保安化されたメモリに関する。
【背景技術】
【０００２】
不揮発性メモリ（ＮＶＭｓ）に格納された内容は永久的である。長期的な格納装置として使用される時、このような永久的な作動が期待され、意図され、データの保存が要求される。
しかし、メモリ空間で不揮発性メモリが使用される場合、様々な問題が発生する可能性がある。
【０００３】
メモリ空間に保管される多くの形式のデータはしばしば保安上の理由のため、一時的であるように意図される。
ＮＶＭｓがこのような仮定を破り（即ち、一時的に維持されなく、格納状態を維持する）、ＮＶＭが盗まれたか、或いはＮＶＭのリソースが再割り当てされた場合、問題を引き起こす可能性がある。
例えば、実際にデータがＮＶＭに格納される時、クラウドーベースのウェブサービスは揮発性メモリとしてみなされるものに関する消費者データを格納することができる。
ウェブサービスがメモリ内容を明確に消去することなく終了した場合、その時、そのデータは、例えばＮＶＭが盗まれたか、又はＮＶＭのリソースが他のクラウド使用者に与えられたかのように、他の使用者が取得する可能性がある。
【０００４】
従って、メモリモジュール、特にＮＶＭを利用するメモリモジュールに対する不正アクセスを防止するために保安化されたメモリを具現するための方案が必要となっている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】米国特許第８、５１６、２７１号明細書
【特許文献２】米国特許出願公開第２０１４／０２８９４８８号明細書
【特許文献３】米国特許出願公開第２０１６／００９２３７７号明細書
【特許文献４】国際特許公開第ＷＯ２０１５／０１６９１８号明細書
【発明の概要】
【発明が解決しようとする課題】
【０００６】
本発明は上記従来のメモリに対する不正アクセス防止の課題点に鑑みてなされたものであって、本発明の目的は、メモリに格納されたデータに対する不正アクセスを防止するために保安化されたメモリ、及びメモリへの不正アクセス防止方法を提供することにある。
【課題を解決するための手段】
【０００７】
上記目的を達成するためになされた本発明によるメモリは、メモリであって、第１使用者に対するデータのためのデータ格納部と、前記データ格納部からデータを読み出すデータ読出しロジックと、前記データ格納部にデータを書き込むデータ書込みロジックと、格納パスワードのためのパスワード格納部と、メモリコントローラから受信パスワードを受信する受信機と、前記受信パスワードと前記格納パスワードとを比較する比較器と、前記

受信パスワードが前記格納パスワードと異なる場合、前記データ格納部の前記データを消去する消去ロジックと、前記比較器が動作を完了する時まで前記メモリコントローラから前記データ格納部へのアクセスを遮断するブロックロジックと、を有し、前記受信パスワード又は前記格納パスワードは、前記メモリに格納されたデータを暗号化するのには用いないことを特徴とする。

【０００８】

上記目的を達成するためになされた本発明によるメモリへの不正アクセス防止方法は、メモリがリセットされたかどうかを決定する段階と、前記メモリが保安モードで動作しているか、非保安（ｎｏｎ－ｓｅｃｕｒｅ）モードで動作しているを決定する段階と、前記メモリが前記保安モードで動作している場合、使用者に対するパスワードを選択する段階と、前記メモリに前記パスワードを伝送する段階と、前記メモリへのアクセスを受ける段階と、を有し、前記パスワードは、前記メモリに格納されたデータを暗号化するのには用いないことを特徴とする。

【０００９】

また、上記目的を達成するためになされた本発明によるメモリへの不正アクセス防止方法は、メモリが保安モードで動作していることを示す信号を前記メモリからメモリコントローラに伝送する段階と、前記メモリコントローラから受信パスワードを受信する段階と、前記受信パスワードと格納パスワードとを比較する段階と、前記受信パスワードが前記格納パスワードと一致しない場合、前記メモリを消去する段階と、前記メモリへのアクセスを前記メモリコントローラに提供する段階と、を有し、前記受信パスワード又は前記格納パスワードは、前記メモリに格納されたデータを暗号化するのには用いないことを特徴とする。

【発明の効果】

【００１０】

本発明に係るメモリ及びメモリへの不正アクセス防止方法によれば、メモリに格納されたパスワードとメモリコントローラで提供するパスワードとが一致する場合、メモリコントローラがメモリのデータにアクセスすることができ、一致しなければ、メモリに格納された使用者データが消去されるので、メモリに格納された使用者データに対する不正アクセスが防止することができるという効果がある。

【図面の簡単な説明】

【００１１】

【図１】本発明の一実施形態に係る保安メモリを使用する多様なホストマシンを具備するデータセンターを示す概要図である。

【図２】図１のホストマシンの追加的な細部構成を示すブロック図である。

【図３】図１のメモリの細部構成を示すブロック図である。

【図４】図１のメモリを他の観点で見た構成を示すブロック図である。

【図５】図３及び図４のメモリに格納されたデータに対するアクセスを承認するか、又図３及び図４のメモリに格納されたデータを消去するかを決定するために、図３のメモリコントローラから受信されたパスワードを使用する図３及び図４のメモリの動作を説明するための図である。

【図６】本発明の実施形態に係る２名の使用者の間でリソースを共有する図１のメモリを例示的に示すブロック図である。

【図７Ａ】本発明の実施形態による図３のメモリコントローラが図１のメモリにアクセスを要請する例示的な手続を説明するためのフローチャートである。

【図７Ｂ】本発明の実施形態による図３のメモリコントローラが図１のメモリにアクセスを要請する例示的な手続を説明するためのフローチャートである。

【図７Ｃ】本発明の実施形態による図３のメモリコントローラが図１のメモリにアクセスを要請する例示的な手続を説明するためのフローチャートである。

【図８】本発明の実施形態による図３のメモリコントローラが図１のメモリにアクセスを要請するためにパスワードを選択する例示的な手続を説明するためのフローチャートであ

る。
【図９Ａ】本発明の実施形態による図１のメモリがデータに対するアクセスを図３のメモリコントローラに承認するか、又はデータを消去するかを決定する例示的な手続を説明するためのフローチャートである。
【図９Ｂ】本発明の実施形態による図１のメモリがデータに対するアクセスを図３のメモリコントローラに承認するか、又はデータを消去するかを決定する例示的な手続を説明するためのフローチャートである。
【図９Ｃ】本発明の実施形態による図１のメモリがデータに対するアクセスを図３のメモリコントローラに承認するか、又はデータを消去するかを決定する例示的な手続を説明するためのフローチャートである。
【図１０】本発明の実施形態による図４の消去ロジックが図１のメモリからデータを消去する例示的な手続を説明するためのフローチャートである。
【発明を実施するための形態】
【００１２】
次に、本発明に係るメモリ及びメモリへの不正アクセス防止方法を実施するための形態の具体例を図面を参照しながら詳細に説明する。
【００１３】
以下の詳細な説明で、本発明を完全に理解できるように多くの特別な細部事項が提示する。
しかし、当業者はこのような特別な細部事項無しで本発明を実行できることを理解すべきである。
他の例で、広く公知された方法、手続、構成要素、回路、及びネットワークが例示的な実施形態を不必要に理解する難くしないために具体的に説明しない。
たとえば、本明細書で多様な構成要素を説明するために「第１」及び「第２」のような用語が使用することができるがこのような構成要素がこのような用語に制限されないことを理解すべきである。
このような用語は１つの構成要素を他の構成要素と区別するために使用される。
例えば、第１モジュールは第２モジュールを称することができ、同様に第２モジュールは本発明の範囲を逸脱しない限度で第１モジュールを称することができる。
【００１４】
本発明の詳細な説明に使用する用語は、ただ特定実施形態を説明するために使用するものであって、本発明を制限することではない。
本発明の詳細な説明及び添付された請求項で使用したように、単数形態は文脈が明確に異なることを示さなければ、複数形態を含むものとみなす。
また、本明細書で使用した用語“及び／又は”は１つ以上の関連され、列挙された目録の任意のそしてすべての可能な結合を示し、含むことと理解されるべきである。“含む”及び／又は“含んでいる”のような用語は、本明細書で使用される時、明示した特徴、整数、段階、動作、構成、及び／又は構成要素の存在を明示するが、その存在を排除することはなく、また１つ以上の他の特徴、整数、段階、動作、構成、構成要素及び／又はそれのグループの追加を明示することとよりさらに理解されるべきである。
図面の構成要素及び特徴は必ず特定比率に示しているものではない。
【００１５】
保安（ｓｅｃｕｒｅ）化された不揮発性メモリ（ＮＶＭ）モジュールは、メモリ空間に使用することができる。
ＮＶＭはパスワード及び認証ロジックを備えることができ、ＮＶＭのデータは、ただ使用者がマッチングキーを有する時のみに、アクセスすることができる。
【００１６】
保安化モジュールに対する制御の流れは次のように進行することができる。
１）メモリコントローラはリセットの時（パワーアップのようなハードウェア誘導リセット、又はソフトウェア誘導リセット）デュアルインラインメモリモジュール（ＤＩＭＭ

）ＳＰＤ（Ｓｅｒｉａｌ　Ｐｒｅｓｅｎｃｅ　Ｄｅｔｅｃｔ：直列プレゼンス検出）の直列プレゼンス検出（ＳＰＤ）を読み出してＤＩＭＭが保安モードを有しているどうかを確認する。

２）ＤＩＭＭが保安モードを有しなければ、その次に、システムは通常的（ｎｏｒｍａｌ）に進行する。

３）そうでなければ、メモリコントローラは新しく定義されたモードレジスターセット（ＭＲＳ）命令を通じてＤＩＭＭにパスワードを送る。

４）パスワードが認識されれば、ＤＩＭＭはロックを解除され、ＤＩＭＭは一般的なＤＩＭＭとして進行する。

ＤＩＭＭはメモリコントローラへのアクセスを承認してくれという信号をメモリコントローラに送ることができる。

“認証”信号は、ＤＱバスを通じて伝送することができる。システムはその次に通常的に進行する。

５）パスワードが認識されなければ、ＤＩＭＭはメモリコントローラに再試行を要請する。

再試行信号もやはりＤＱバスを通じて伝送することができる。メモリコントローラはその次にＭＲＳ命令を通じてキーを再び送る。

６）再試行の回数が閾値（ｔｈｒｅｓｈｏｌｄ）を超過すれば、ＤＩＭＭはメモリコントローラが再試行することを停止する。

代わりに、ＤＩＭＭはＤＱバスを通じてメモリコントローラに“非認証”信号を送る。

その次に、ＤＩＭＭはメモリコントローラがＤＩＭＭに対するアクセスを承認する前にＤＩＭＭの内容を消去する。

【００１７】

図１は、本発明の一実施形態に係る保安メモリを使用する多様なホストマシンを具備するデータセンターを示す概要図である。

図１でデータセンター１０５は、ホストマシン（１１０、１１５、１２０、１２５）のような多様なホストマシン（サーバーと称される）を含む。

【００１８】

データセンター１０５は、任意の使用者によって使用することができるクライアントマシン１３０のようなクライアントマシンを支援する。

クライアントマシン１３０を使用する使用者は何か必要であるサービスがあれば、データセンター１０５からリソースを効果的に賃貸（リース、ｌｅａｓｅ）することができる。

例えば、データセンター１０５は、使用者が自宅に配達されることができる製品を購買するための能力を備えるようにすることができ、このためにデータセンター１０５は使用者が購買を選択し、決済を完了する間に使用者のショッピングカートを格納するために使用者にメモリを賃貸することができる。

【００１９】

図１は、４つのホストマシン（１１０、１１５、１２０、１２５）及び１つのクライアントマシン１３０を含むデータセンター１０５を示したが、本発明の実施形態はこれに限定されず、データセンター１０５は多様な数のホストマシン及び／又はクライアントマシン含むことができる。

ホストマシン（１１０、１１５、１２０、１２５）は、本発明の目的のために交換可能であるので、ホストマシン１１０に対する追加的な参照はホストマシン（１１５、１２０、１２５）に対する参照を含むものとみなされる。

【００２０】

また、図１は、ネットワーク１３５を含むデータセンター１０５を示すものである。

ネットワーク１３５はローカルネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、及びインターネットのようなグローバルネットワーク、有線又は無線ネットワークを含む任意の望む形態を有することができる。

追加的に、ネットワーク１３５は、これらのようなネットワークの任意の組み合わせであってもよく、データセンター１０５が単一の地理的位置に位置するよりは分散させることが可能である。

【００２１】

図１は、またホストマシン１１０の細部構成を示しているが、データセンター１０５内のホストマシン（１１０、１１５、１２０、１２５）の中で任意のホストマシンもやはり同一の細部構成を有することができる。

ホストマシン１１０は、プロセッサ１４０、メモリ１４５、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｏｎｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１５０、及び格納装置１５５を含む。

【００２２】

プロセッサ１４０は、任意の多様なプロセッサであり、例えばインテル（登録商標）ジーオン（登録商標）（Ｉｎｔｅｌ（登録商標） Ｘｅｏｎ（登録商標））、セレロン（Ｃｅｌｅｒｏｎ（登録商標））、イタニウム（登録商標）（Ｉｔａｎｉｕｍ（登録商標））、又はアトム（登録商標）（Ａｔｏｍ（登録商標））プロセッサ、ＡＭＤ（登録商標）オプテロン（登録商標）（Ｏｐｔｅｒｏｎ（登録商標））、ＡＲＭプロセッサ等であってもよい。

【００２３】

メモリ１４５は、ＤＲＡＭ（Ｄｙｎａｍｉｃ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ＰＲＡＭ（Ｐｅｒｓｉｓｔｅｎｔ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ＳＲＡＭ（Ｓｔａｔｉｃ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ＦＲＡＭ（登録商標）（Ｆｅｒｒｏｅｌｅｃｔｒｉｃ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、又はＭＲＡＭ（Ｍａｇｎｅｔｏｒｅｓｉｓｔｉｖｅ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）のようなＮＶＲＡＭ（Ｎｏｎ－Ｖｏｌａｔｉｌｅ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）等任意の多様なメモリであってもよい。

また、メモリ１４５は、シングルメモリモジュールで揮発性及び不揮発性メモリ装置の任意の所望する組み合わせを含むハイブリッドメモリであってもよい。

しかし、一般的なメモリモジュールと異なりに、メモリ１４５は以下に説明するように保安メモリモジュールであってもよい。

格納装置１５５は、他の可能性もあるが、一般的なハードディスクドライブ又はフラッシュメモリを含む任意の多様な格納装置であってもよい。

【００２４】

ＥＥＰＲＯＭ１５０は、重要製品データ（Ｖｉｔａｌ Ｐｒｏｄｕｃｔ Ｄａｔａ：ＶＰＤ）１６０を含む。

以下で詳細に説明するように、たとえば、メモリ１４５はメモリ１４５そのものが保安メモリであるか否かを明示することができるが、重要製品データ１６０はこのような情報に対する代替ソースを提供することができる。

図１には重要製品データ１６０がＥＥＰＲＯＭ１５０に格納されることを示しているが、本発明の実施形態は重要製品データ１６０を格納するために任意の他の格納媒体を使用することを支援することができる。

例えば、ＥＥＰＲＯＭ１５０は、公知されている幾つかの代案として、ＥＰＲＯＭ（Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ ｍｅｍｏｒｙ）又はフラッシュメモリで代替することができる。

【００２５】

図２は、図１のホストマシン（１１０、１１５、１２０、１２５）の追加的な細部構成を示すブロック図である。

図２を参照すると、一般的に、ホストマシン（１１０、１１５、１２０、１２５）は、１つ又はそれ以上のプロセッサ１４０を含み、プロセッサ１４０は各々ホストマシン（１１０、１１５、１２０、１２５）の構成要素の動作を制御するために使用されるメモリコントローラ２０５及びクロック２１０を含む。

【００２６】
プロセッサ１４０は、ＲＡＭ（ｒａｎｄｏｍ　ａｃｃｅｓｓ　ｍｅｍｏｒｙ）、ＲＯＭ（ｒｅａｄ－ｏｎｌｙ　ｍｅｍｏｒｙ）、又は他の状態保持媒体を含むことができるメモリ１４５に接続される。
プロセッサ１４０は、また格納装置１５５、及びイーサネット（登録商標）コネクタ又は無線コネクタのようなネットワークコネクタ２１５に接続される。
プロセッサ１４０は、またバス２２０に接続され、他の構成要素の中でユーザーインターフェイス２２５及び入／出力エンジン２３０を使用して管理される入出力インターフェイスポートがバス２２０に接続される。
【００２７】
図３は、図１のメモリ１４５の細部構成を示すブロック図である。
図３で、メモリ１４５はレジスタークロックドライバー（Ｒｅｓｉｓｔｅｒ　Ｃｌｏｃｋ　Ｄｒｉｖｅｒ：以下、ＲＣＤと記す）３０５及びメモリチップ（３１０、３１５、３２０、３２５、３３０、３３５、３４０、３４５）を含む。
図３は、データを格納する８個のチップを具備する一般的なＤＲＡＭモジュールを示しているが、本発明の実施形態は他のタイプのメモリモジュールを含むことができ、任意の要求される数のチップ又は他の代替されるチップを含むことができる。
【００２８】
メモリコントローラ２０５は、メモリ１４５とインターフェイスする。
メモリコントローラ２０５は、直接的にメモリチップ（３１０～３４５）にデータを読み出す又は書き込むための命令を送る。
メモリコントローラ２０５は、また命令／アドレス信号及びクロック信号を使用してＲＣＤ３０５とインターフェイスする。
【００２９】
メモリ１４５がリセット動作を遂行した後に、メモリコントローラ２０５はメモリ１４５が保安モードで動作しているかどうかを決定する。
リセット動作は、図１のホストマシン１１０が最初に電源を入れる（ｐｏｗｅｒ　ｕｐ）時のようなハードウェア誘導リセット又はメモリコントローラ２０５がリソースの使用者賃貸が終了（以下で、より詳細に説明する）されたことをメモリ１４５に通知する時のようなソフトウェア誘導リセットである。
【００３０】
メモリコントローラ２０５は、直列プレゼンス検出（Ｓｅｒｉａｌ　Ｐｒｅｓｅｎｃｅ　Ｄｅｔｅｃｔ：ＳＰＤ）３５０に問い合わせてメモリ１４５が保安モードで動作しているどうかを決定する。
代案として（Ａｌｔｅｒｎａｔｉｖｅｌｙ）、先に図１を参照して説明したように、メモリコントローラ２０５はＥＥＰＲＯＭ１５０からメモリ１４５が保安モードで動作しているか否かを示す図１の重要製品データ１６０にアクセスすることができる。
【００３１】
メモリ１４５が保安モードに動作しなければ、その時、メモリコントローラ２０５は従来の方法にメモリ１４５をアクセスする。
しかし、メモリ１４５が保安モードで動作していれば、その時メモリコントローラ２０５はメモリ１４５に対する認証を試みてアクセスを取得する。
（ここで、“アクセスを取得するための認証”はメモリコントローラ２０５がメモリ１４５へのアクセスすることを拒否されることを意味するものではなく、むしろ、後述するように、メモリ１４５が任意の以前データを消去した後にのみ、メモリコントローラ２０５はメモリ１４５へのアクセスが付与されることを示す。）
【００３２】
メモリコントローラ２０５は、モードレジスターセット（ＭＲＳ）命令を通じてパスワードをＲＣＤ３０５に伝送する。
この時、ＲＣＤ３０５は受信されたパスワードと格納部３５５に格納されたパスワード

とを比較する。
受信されたパスワードが格納されたパスワードと一致する場合、その時、メモリコントローラ２０５はメモリ１４５へのアクセスが承認され、このような信号はＤＱバスを通じて伝送される。
そうでない場合、メモリ１４５はメモリチップ（３１０～３４５）に格納された任意のデータを消去し、その後、メモリコントローラ２０５はメモリ１４５へのアクセスが承認される。
【００３３】
以後のアクセスを容易にするために、ＲＣＤ３０５はまた受信されたパスワードを格納部３５５に格納し、メモリコントローラ２０５が受信されたパスワードを利用して以後のメモリ１４５に対する認証をできるようにする。
ＲＣＤ３０５は、また格納部３５５の既存パスワードを上書きして古い格納されたパスワードが将来受け入れられることを防止する。
格納されたパスワードを消去することはまたメモリ１４５に格納されたデータを消去することの一部であり、古い格納されたパスワードが将来受け入れられることを防止することができる。
【００３４】
メモリコントローラ２０５は、任意の所望する方式でパスワードを生成する。
例示的な方法としてランダムにパスワードを生成するか、予め設定されたパスワードのリストからパスワードを選択するか、使用者ＩＤのハッシュ（ｈａｓｈ）を生成するか、或いは保安プラットフォームモジュール（ＴＰＭ：Ｔｒｕｓｔｅｄ　Ｐｌａｔｆｏｒｍ　Ｍｏｄｕｌｅ）を使用してパスワードを生成することができる。
本発明の実施形態はパスワードを生成するための他の技術を支援することもできる。
【００３５】
本発明の実施形態は既存の一般的なシステムに比べて幾つか長所を有する。
メモリ１４５を保護するためのメカニズムを提供することによって、ある使用者が他の使用者のデータを読み出す危険性大幅に減少させる。
しかし、使用者のデータがメモリに格納される時、暗号化されないので、暗号化されたデータを管理するための暗号ロジックを含む必要がない。
また、データを暗号化する必要が無いことはメモリ１４５からデータをアクセスするために要求される時間を減少させ、これは暗号化／復号化を遂行するために消費される時間を必要としないからである。
【００３６】
既存のシステムに対する有用な比喩は、メモリを銀行の安全金庫システムと比較することである。
銀行の安全金庫にある何かにアクセスするためにはその金庫に対するキーを提示する必要がある。
使用者が他の金庫のデータにアクセスしようとすれば、第１番目の金庫が閉じ、次の金庫が開かなければならない。
これはデータを暗号化する従来のシステムと同様であり、データのある特定部分にアクセスするためには該当データが解読されなければならなく、これはアクセスを遅くするようにする。
【００３７】
これに反して、メモリ１４５は家と比較され、パスワードはドアに対するキーとしてメモリ１４５をアクセスするのに使用される。
ドアが開けられる時まで、家の内容物が保護される。
一旦、ドアが開けられれば、データは遅滞無く自由にアクセスされることができ、データが暗号化されていないので、それ以上の遅滞が発生しない。
【００３８】
図４は、図１のメモリ１４５を他の観点で見た構成を示すブロック図である。

メモリ１４５の特定実施形態を示す図３と対照的に、図４はメモリ１４５をより抽象的な概念で示すブロック図である。
メモリ１４５は、実際の使用者データを格納するデータ格納部（３１０～３４５）（図３のメモリチップに対応）、データ格納部（３１０～３４５）からデータを読み出すデータ読出しロジック４０５、及びデータ格納部（３１０～３４５）にデータを書き込むデータ書込みロジック４１０を含む。
【００３９】
メモリ１４５はまた、使用者がメモリ１４５へのアクセスを承認されるべきか否かを決定する認証ロジック４１５（図３のＲＣＤに対応）を含む。
前述したように、“承認されたアクセス”は、使用者がメモリ１４５を使用することに対して許容されない可能性を意味することではなく、使用者がアクセスの承認を受ける前にメモリ１４５がデータ格納部（３１０～３４５）にある任意のデータを消去することができることを意味する。
【００４０】
認証ロジック４１５は、受信機４２０、ブロックロジック４２５、比較器４３０、及び消去ロジック４３５を含む。
受信機４２０は、図３のメモリコントローラ２０５からパスワードを受信する。
ブロックロジック４２５は、認証ロジック４１５が図３のメモリコントローラ２０５がアクセスの承認を受ける前にデータ格納部（３１０～３４５）が消去されなければならないか否かを決定する間、図３のメモリコントローラ２０５からメモリ１４５へのアクセスを遮断する。
比較器４３０は、図３のメモリコントローラ２０５から受信されたパスワードとパスワード格納部４５５（図３の格納部に対応）に格納されたパスワードとを比較してパスワードが一致するか否かを確認する。
パスワードが一致しなければ、その時、消去ロジック４３５は図３のメモリコントローラ２０５がメモリ１４５へのアクセスの承認を受ける前にデータ格納部（３１０～３４５）の内容を消去する。
【００４１】
消去ロジック４３５は、メモリ１４５によって備えられた形態に適合する任意の方式で動作することができる。
例えば、メモリ１４５が揮発性メモリのみを使用すれば、消去ロジック４３５はデータ格納部（３１０～３４５）内の値のリフレッシュを十分に長い時間の間、防止することによって、その間に格納されたすべての値が失われるようにしてメモリ１４５を効果的に消去することができる。
即ち、データ格納部（３１０～３４５）に格納された任意の値はそれ以上格納されない。
【００４２】
これがどのぐらい長くかかるかはデータ格納部（３１０～３４５）の特定タイプ及び形態によって変わり、さらにデータ格納部（３１０～３４５）の製造に関連した特異性（ｅｃｃｅｎｔｒｉｃｉｔｉｅｓ）のような他の要因によって変わる。
例えば、メモリ１４５が揮発性メモリを使用し、寒い環境にあれば、消去ロジック４３５はメモリ１４５の内容が適切な時間内に失われないので、メモリ１４５を消去するためにメモリ１４５に値を書き込む必要がある。
本発明の他の実施形態で、消去ロジック４３５はデータ格納部（３１０～３４５）に格納されたすべての値を望むように「０」又は「１」のような定数値に上書きすることができる。
【００４３】
本発明のその他の実施形態で、消去ロジック４３５は設計された順に書込みの動作を遂行して任意の値を消去することができる。
このような順序の例示として米国国防省（Ｄｅｐａｒｔｍｅｎｔ　ｏｆ　Ｄｅｆｅｎｓ

ｅ：ＤｏＤ）又は他の政府機関及び非政府グループによって設計された順序を含むことができる。
例えば、このような順序は全て「０」を書き込み、その次に全て「１」を書き込み、その次にメモリにランダムなパターンを書き込むことを含むことができる。
フラッシュメモリと共に使用される本発明のその他の実施形態で、メモリ１４５内のすべてのデータブロック（又は少なくとも有効データを含むブロック）は、図３のメモリコントローラ２０５がメモリ１４５へのアクセスの承認を受ける前に、即時ガーベッジコレクションの対象になることができる。
【００４４】
認証ロジック４１５はまた、パスワード書込みロジック４４０を含む。
パスワード書込みロジック４４０は、パスワード格納部４５５にパスワードを書き込む。
例えば、図３のメモリコントローラ２０５から受信されたパスワードがパスワード格納部４５５に格納されたパスワードと一致しなければ、消去ロジック４３５がデータ格納部（３１０～３４５）の内容を消去した後に、パスワード書込みロジック４４０はパスワード格納部３５５に図３のメモリコントローラ２０５から受信されたパスワードを書き込むことができる。
このような方式に、図３のメモリコントローラ２０５は、以後に同一のパスワードを使用するメモリ１４５に対して認証することができ、任意の他のメモリコントローラは認証することができなく（他のメモリコントローラが同一のパスワードを生成する予想外の場合を禁止）、これによって非認証アクセスから使用者のデータを保護することができる。
【００４５】
図３及び図４で、メモリ１４５をリセットするための時期を決定することはシステムに任されている。
即ち、メモリ１４５は、所定の特定使用者がどのぐらい長い間、メモリ１４５を賃貸したかが分からない。
それで、図３のメモリコントローラ２０５（又は図１のデータセンター１０５のサービス提供者）はタイマーを通じて使用者がどのぐらい長い間、メモリ１４５へのアクセスをしたかを追跡することができる。
一旦、使用者の賃貸が満了されれば、図３のメモリコントローラ２０５（又は図１のホストマシン１１０の任意の他の希望する構成要素）、使用者のデータが他の使用者によって読み出されることを防止できるように、メモリ１４５（又はより一般的に、図１のサーバー１１０）にソフトウェア誘導リセット指示を発行することができる。
【００４６】
図３及び図４で、パスワード格納部３５５は、ＳＰＤ３５０から分離されている。
しかし。本発明の一部実施形態で、必要であれば、ＳＰＤ３５０の使用されない部分又はベンダー特定（ｖｅｎｄｏｒ－ｓｐｅｃｉｆｉｅｄ）領域にパスワードを格納することができる。
このような処理方法は、パスワードのためだけに新しい格納部が導入することを防止することができる。
【００４７】
図５は、図３及び図４のメモリ１４５に格納されたデータに対するアクセスを承認するか、又は図３及び図４のメモリ１４５に格納されたデータを消去するかを決定するために、図３のメモリコントローラ２０５から受信されたパスワードを使用する図３及び図４のメモリの動作を説明するための図である。
図５で、受信機４２０は図３のメモリコントローラ２０５から受信パスワード５０５を受信する。
この時、比較器４３０は受信パスワード５０５とパスワード格納部３５５から取得した格納パスワード５１０とを比較する。
【００４８】

受信パスワード５０５が格納パスワード５１０と一致すれば、その時、比較結果５１５は図３のメモリコントローラ２０５が図４のメモリ１４５への即時アクセスの承認を受けることができることを示し、そうでなければ、比較結果５１５は図３及び図４のデータ格納部（３１０～３４５）のデータが図４の消去ロジック４３５によって消去される時まで図３のメモリコントローラ２０５が遮断されなければならないことを示す。

【００４９】

図５はまた、閾値（ｔｈｒｅｓｈｏｌｄ）５２０の使用を示す。

本発明の一部実施形態で、比較器４３０は、図３のメモリコントローラ２０５が図３及び図４のメモリ１４５へのアクセスの承認を受けるか否かを決定するために受信パスワード５０５と格納パスワード５１０とを単一に比較する。

しかし、本発明の他の実施形態では図３のメモリコントローラ２０５が多数の受信パスワード５０５を提供するようにすることもできる。

【００５０】

例えば、比較器４３０が受信パスワード５０５と格納パスワード５１０とが一致しないと決定した後に、図４の認証ロジック４１５は、図３のメモリコントローラ２０５が受信パスワード５０５を再伝送するよう要請する信号をＤＱバスを通じて図３のメモリコントローラ２０５に送ることができる。

再試行を許容することは、データの予期しない変更（例えば、受信パスワード５０５が伝送される時の干渉による変更）を防ぐことができる。

その次に比較器４３０は閾値５２０によって指定された回数分受信パスワード５０５をテストすることができ、その後、一致が発見されなければ、比較結果５１５は図３及び４のメモリ１４５のデータ格納部（３１０～３４５）からデータを消去するように指定する。

【００５１】

閾値５２０は、任意の望む整数値に設定することができる。

しかし、本発明の実施形態が図３及び図４のデータ格納部（３１０～３４５）のデータを消去するか否か（必要であれば、消去が遂行される）を決定する時まで、図３のメモリコントローラ２０５が図３及び図４のメモリ１４５へアクセスすることを一時的に遮断するので、図３のメモリコントローラ２０５が遮断される時間を減少させるために閾値５２０を低い整数値に維持することが望ましい。

【００５２】

図６は本発明の実施形態に係る２名の使用者の間でリソースを共有する図１のメモリ１４５を例示的に示すブロック図である。

図６で、メモリ１４５はメモリの２つの部分（６０５、６１０）を含み、これらの各々は分離されたメモリモジュールとして取り扱われる。

【００５３】

例えば、メモリ１４５は、テラバイト或いはそれ以上の容量を具備するＤＩＭＭである。

このようなメモリの容量は、単一使用者が必要とするより多い可能性があるため、単一使用者にメモリ１４５の全体を割り当てることは無駄が多い。

代わりに、メモリ１４５の一部分、部分６０５のように、使用者に割り当て、残りの部分６１０は他の使用者を含んで他の用途で利用するように残される。

【００５４】

インターフェイス６１５を使用して、２つのメモリコントローラ（２０５、６２０）がメモリ１４５とインターフェイスする。

例えば、メモリコントローラ２０５は、メモリ１４５の部分６０５とインターフェイスし、メモリコントローラ６２０はメモリ１４５の部分６１０とインターフェイスする。

このような方式により、メモリ１４５は２名の異なる使用者に対するデータを格納することができるが、各使用者はただ自分のデータにのみアクセスすることができ、他の使用者のデータにアクセスすることができない。

このようなメカニズムは各々のデータを保護する。

【００５５】

メモリ１４５の該当部分の一人の使用者の賃貸が終了する時、メモリ１４５のソフトウェア誘導リセットが開始される。

例えば、部分６０５を賃貸した使用者が賃貸を終了したと仮定する。

この時、メモリ１４５がリセットされる。

メモリ１４５のソフトウェア誘導リセットが完了する時、メモリコントローラ６２０はメモリ１４５に自分のパスワードを提示する。

メモリコントローラ６２０はメモリ１４５に対して再び認証をして、部分６１０に格納された使用者のデータへのアクセスを再び取得することができる。

ソフトウェア誘導リセットと認証手続が部分６１０の使用者のデータに対するアクセスを遅延させることは事実であるが、このような遅延は重要ではなく、使用者さえも気が付かない可能性が高い。

【００５６】

一方では、メモリコントローラ２０５は、メモリ１４５に新しいパスワードを提示することができる。

このようなパスワードは認識されないので、メモリコントローラ２０５はメモリ１４５に対して認証することができない。

したがって、部分６０５は他の使用者が部分６０５を賃貸する前に消去することができ、部分６０５に以前に格納されたデータの使用者を保護することができる。

【００５７】

図６は、２つの部分（６０５、６１０）に区分されたメモリ１４５を示しているが、本発明の実施形態で、メモリ１４５は任意の数の部分に区分されてもよい。

図６で２つの部分を使用したことは単なる例示として提示したに過ぎない。

追加的に、メモリ１４５の実施形態により、メモリ１４５はメモリ１４５の各部分に対して１つずつ配置されたＲＣＤを含むか、或いはメモリ１４５のすべての部分に対して１つのＲＣＤを含むか、又はすべての部分にＲＣＤを配置しなくともよい。

【００５８】

図７Ａ～図７Ｃは、本発明の実施形態による図３のメモリコントローラ２０５が図１のメモリ１４５にアクセスを要請する例示的な手続を説明するためのフローチャートである。

図７Ａのステップ７０５で、図３のメモリコントローラ２０５は図１のメモリ１４５がリセット（ハードウェア誘導リセット又はソフトウェア誘導リセットを通じて）されたかどうかを決定する。

【００５９】

ステップＳ７１０で、メモリコントローラ２０５は、例えば図３のＳＰＤ３５０から関連データを読み出すことによって、図１のメモリ１４５が保安モードで動作しているか否かを決定する。

ステップＳ７１５で、図１のメモリ１４５が保安モードで動作していなければ、次に図３のメモリコントローラ２０５は図１のメモリ１４５に対するアクセスを受信する。

一方、図１のメモリ１４５が保安モードで動作していれば、次にステップＳ７２０で、図３のメモリコントローラ２０５は図１のメモリ１４５に使用するためのパスワードを選択する。

次に、ステップＳ７２５で、図１のメモリ１４５からの要請に応答して、図３のメモリコントローラ２０５は図１のメモリ１４５にパスワードを伝送する。

【００６０】

図７Ｂのステップ７３０で、図３のメモリコントローラ２０５はパスワードが受け入れられたか否かを決定する。

前述したように、図１のメモリ１４５はパスワードが受け入れられ、図３のメモリコントローラ２０５が許可されたか否かを示す信号をＤＱバスを通じて伝送する。

パスワードが受け入れられなければ、次にステップＳ７３５で、図３のメモリコントローラ２０５はパスワード再伝送に対する要請を受信し、図７Ａのステップ７２０に戻る。

【００６１】

代案として、ステップＳ７４０で、図３のメモリコントローラ２０５は、図１のメモリ１４５が図３及び図４のデータ格納部（３１０～３４５）のすべてのデータを消去した後のみに、図１のメモリ１４５へのアクセスを受信する。

ステップＳ７３５とステップＳ７４０の差異点は、メモリ１４５が閾値回数繰り返してパスワード比較を遂行したか否かで示される。

図３のメモリコントローラ２０５は、閾値が分からないので、図３のメモリコントローラ２０５は図１のメモリ１４５によって行われる追加的なパスワード要請に対しての応答のみをする。

一方、パスワードが受け入れられれば、次にステップＳ７４５で、図３のメモリコントローラ２０５は、図３及び図４のデータ格納部（３１０～３４５）のデータを最初に消去することなしに、図１のメモリ１４５に対するアクセスを受信する。

【００６２】

図７Ｃのステップ７５０で、図３のメモリコントローラ２０５は、図３のメモリコントローラ２０５が図１のメモリ１４５に対するアクセスを承認受けた時からどのぐらい時間が経過したかを測定する。

次に、ステップＳ７５５で、図３のメモリコントローラ２０５は、使用者が図１のメモリ１４５を賃貸した時間量が閾値時間量を経過したか否かを決定する。

経過しなかったら、次に図３のメモリコントローラ２０５はしばらくの間待機し、どのぐらい時間が経過したかを再び測定する。

賃貸時間が経過したら、ステップＳ７６０で、図３のメモリコントローラ２０５は図１のメモリ１４５がソフトウェアリセットを遂行するように指示し、その後に処理が終了される。

【００６３】

図８は、本発明の実施形態による図３のメモリコントローラ２０５が図１のメモリ１４５にアクセスを要請するためにパスワードを選択する例示的な手続を説明するためのフローチャートである。

図８のステップＳ８０５で、図３のメモリコントローラ２０５は、ランダムなパスワードを生成して図１のメモリ１４５に対する認証に使用する。

【００６４】

代案として、ステップＳ８１０で、図３のメモリコントローラ２０５は、パスワードのリストからパスワードを選択して図１のメモリ１４５に対する認証に使用する。

代案として、ステップＳ８１５で、図３のメモリコントローラ２０５は、図１のメモリ１４５に対する認証に使用するために、使用者ＩＤをハッシュ（ｈａｓｈ）してパスワードを生成する。

代案として、ステップＳ８２０で、図３のメモリコントローラ２０５は、保安プラットフォームモジュールからパスワードにアクセスして図１のメモリ１４５に対する認証に使用する。

【００６５】

図９Ａ～図９Ｃは、本発明の実施形態による図１のメモリ１４５がデータへのアクセスを図３のメモリコントローラ２０５に承認するか、又はデータを消去するかを決定する例示的な手続を説明するためのフローチャートである。

図９Ａのステップ９０５で、図１のメモリ１４５は、図１のメモリ１４５が保安モードで動作しているか否かを知るための要請を受信する。

【００６６】

ステップＳ９１０で、図１のメモリ１４５は図３のメモリコントローラ２０５に図１のメモリ１４５が保安モードで動作しているか否かを示す信号を伝送する。

ステップＳ９１５で、図１のメモリ１４５は図１のメモリ１４５へアクセスするための要請を図３のメモリコントローラ２０５から受信する。
ステップＳ９２０で、図１のメモリ１４５は、メモリ１４５が保安モードで動作しているか否かを決定する。
図１のメモリ１４５が保安モードで動作していなければ、次にステップＳ９２５で、図１のメモリ１４５は図３のメモリコントローラ２０５のアクセスを承認する。
そうでなければ、ステップＳ９３０で、認証ロジック４１５は図３のパスワード格納部３５５から図５の格納パスワード５１０にアクセスする。
【００６７】
図９Ｂのステップ９３５で、図１のメモリ１４５は図３のメモリコントローラ２０５から図５の受信パスワード５０５を要請する。
ステップＳ９４０で、図１のメモリ１４５は図３のメモリコントローラ２０５から図５の受信パスワード５０５を受信する。
ステップＳ９４５で、図４の比較器４３０は、図５の受信パスワード５０５と図５の格納パスワード５１０とを比較する。
ステップＳ９５０で、図４の認証ロジック４１５は、図５の受信パスワード５０５と図５の格納パスワード５１０との比較で一致するか否かを示す図５の比較結果５１５を決定する。
一致すれば、次にステップＳ９５５で、図１のメモリ１４５は図３のメモリコントローラ２０５が図１のメモリ１４５へアクセスすることを承認する。
【００６８】
図９Ｃのステップ９６０でも受信パスワード５０５が図５の格納パスワード５１０と一致しないと仮定すれば、図４の認証ロジック４１５はパスワード比較の回数が閾値回数まで到達したか否かを決定する。
閾値回数に到達しなかったら、次に図９Ｂのステップ９３５に戻って図１のメモリ１４５が図３のメモリコントローラ２０５に新しいパスワードを要請する。
そうでなければ、ステップＳ９６５で、図４の消去ロジック４３５は図３及び図４のデータ格納部（３１０～３４５）からデータを消去する。
次に、ステップＳ９７０で、図４のパスワード書込みロジック４４０は図５の受信パスワード５０５を図３のパスワード格納部３５５に書き込み、以後にステップＳ９７５で、図１のメモリ１４５は図３のメモリコントローラ２０５が図１のメモリ１４５へのアクセスを承認する。
次に、ステップＳ９８０で、図１のメモリ１４５が図３及び図４のデータ格納部（３１０～３４５）のデータを消去したか消去しなかったに関わらず、図３のメモリコントローラ２０５に図１のメモリ１４５へアクセスすることを承認し、また、ステップＳ９８０で、図１のメモリ１４５は図３のメモリコントローラ２０５からソフトウェア誘導リセットを遂行する信号を受信し、ステップＳ９８５で、図１のメモリ１４５はソフトウェア誘導リセットを遂行し、その後、手続が終了する。
【００６９】
図１０は本発明の実施形態による図４の消去ロジック４３５が図１のメモリ１４５からデータを消去する例示的な手続を説明するためのフローチャートである。
図１０のステップＳ１００５で、図４の消去ロジック４３５は使用者によって使用されたメモリブロックに対するガーベッジコレクションを遂行する。
代案として、ステップＳ１０１０で、図４の消去ロジック４３５は定数値（ｃｏｎｓｔａｎｔ　ｖａｌｕｅ）を図１のメモリ１４５のすべてのデータに上書きする。
代案として、ステップＳ１０１５で、図４の消去ロジック４３５は図１のメモリ１４５のすべてのデータに対して、全て「０」を書き込み、その次に全て「１」を書き込み、その次にランダムなパターンを書き込むような上書き順序を遂行する。
代案として、ステップＳ１０２０で、図４の消去ロジック４３５は、図１のメモリ１４５ですべての格納されたデータ値が失われたことを保障するまで、図１のメモリ１４５の

セルがリフレッシュされることを防止する。
【００７０】
図７Ａ～図１０で、本発明の一部の実施形態を示した。
しかし、当業者はステップの順序を変更するか、ステップを省略するか、又は図に示していないリンクを含むことによって、本発明の他の実施形態も可能であることが認識され得る。
フローチャートのすべてのこのような変形は、明示的に記述されているか否かに関わらず、本発明の実施形態として看做される。
【００７１】
次の説明は本発明の特定な形態を具現することができる適切なマシン又はマシン群に対する一般的な説明を簡略に提供するためのものある。
マシン及びマシン群は、少なくとも一部分として、キーボードやマウスのような一般的な入力装置からの入力のみでなく、他のマシン、仮想現実（ＶＲ：Ｖｉｒｔｕａｌ　Ｒｅａｌｉｔｙ）環境との相互作用、生体測定フィードバック、又は他の入力信号から受信された指示によって制御することができる。
【００７２】
本明細書で使用された用語“マシン”は単一マシン、仮想マシン、又は共に動作するように通信可能であるように結合されたマシン、仮想マシン、又は装置のシステム等を幅広く含む。
例示的に、マシンは個人用コンピュータ、ワークステーション、サーバー、携帯用コンピュータ、携帯することができる装置、電話機、タブレット等のようなコンピューティング装置のみならず、自動車、汽車、タクシー等の個人又は大衆交通のような運送装置を含む。
【００７３】
マシン及びマシン群は、プログラムできる又はプログラムできないロジックデバイス又はアレイ、ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔｓ）、内蔵型コンピュータ、スマートカードのような、内蔵型コントローラを含み得る。
マシン及びマシン群は、ネットワークインターフェイス、モデム、又は他の通信カップリングのような１つ以上の遠隔機械に対する１つ以上の接続を活用することができる。
マシンは、イントラネット、インターネット、ローカル領域ネットワーク、広域ネットワーク等のような物理的及び／又は論理的ネットワークを通じて相互接続することができる。
当業者は、ネットワーク通信がラジオ周波数（ＲＦ）、衛星、マイクロウェーブ、ＩＥＥＥ（Ｉｎｓｔｉｔｕｔｅ　ｏｆ　Ｅｌｅｃｔｒｉｃａｌ　ａｎｄ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｅｎｇｉｎｎｅｅｒｓ）８０２．１１、ブルートゥース（登録商標）、紫外線、ケーブル、レーザー等を含む多様な無線及び／又は有線近距離又は長距離キャリヤー及びプロトコルを活用できることが分かる。
【００７４】
本発明の実施形態は、機能、手続、データ構造、アプリケーションプログラム等を含む関連データと結合して、又はこれを参照して説明することができる。
マシンによってアクセスされる時、マシンがタスクを遂行するか、或いは抽象的なデータタイプ又は低レベルハードウェアコンテキストを定義する。
関連データは、例えば、ＲＡＭ、ＲＯＭ等のような揮発性及び／又は不揮発性メモリ、又はハードードライブ、フロッピー（登録商標）ディスク、光学格納装置、テープ、フラッシュメモリ、メモリスティック、デジタルビデオディスク、生物学的格納装置等を含む他の格納装置及び関連された格納媒体に格納することができる。
関連データは、物理的及び／又は論理的ネットワークを含む伝送環境を通じてパケット、シリアルデータ、並列データ、伝播された信号等の形態に伝達することができ、圧縮又は暗号化されたフォーマットを使用することができる。

関連データは、分散環境で使用することができ、マシンアクセスのためにローカル及び／又は遠隔で格納することができる。

【００７５】

本発明の実施形態は、１つ以上のプロセッサによって遂行することができる命令を含む類型の非一時的マシン読出可能媒体を含むことができ、このような命令は本明細書で説明したような本発明の構成要素を遂行するための命令を含む。

【００７６】

図で示した実施形態を参照して本発明の原理を説明したが、図に示した実施形態はこのような原理から逸脱せず、配列及び細部事項を修正することによって任意の望む方式に組み合わされることが分かる。

そして、前述した説明は特定実施形態に焦点を絞っているが、他の構成も考慮される。

特に、“本発明の実施形態に係る”のような表現が本明細書で使用されても、このような文句は実施形態可能性を一般的に参照することを意味し、特定実施形態構成に本発明を制限するものではない。

本明細書で使用したように、このような用語は他の実施形態と組み合わせることができる同一又は他の実施形態である。

前述した実施形態は本発明を制限するものと解釈されてはならない。

たとえ幾つかの実施形態を説明したが、当業者は本発明の新規な教示及び長所から実質的に逸脱しなく、このような実施形態に多い修正が可能であることを容易に分かるはずである。

したがって、このようなすべての修正は請求項で定義された本発明の権利範囲内に含まれること看做される。

【００７７】

本発明の実施形態は、制限無しで、次のステートメント（ｓｔａｔｅｍｅｎｔｓ）に拡張することができる。

ステートメント（Ｓｔａｔｅｍｅｎｔ）１．本発明の実施形態は、メモリを含み、メモリは、

第１使用者に対するデータのためのデータ格納部と、

データ格納部からデータを読み出すデータ読出しロジックと、

データ格納部にデータを書き込むデータ書込みロジックと、

格納パスワードのためのパスワード格納部と、

メモリコントローラから受信パスワードを受信する受信機と、

受信パスワードと格納パスワードとを比較する比較器と、

受信パスワードが格納パスワードと異なる場合、データ格納部のデータを消去する消去ロジックと、

比較器が動作を完了する時までメモリコントローラから前記データ格納部に対するアクセスを遮断するブロックロジックと、を有し、

受信パスワード又は格納パスワードはメモリに格納されたデータを暗号化するのには用いない。

【００７８】

ステートメント２．本発明の実施形態はステートメント１にしたがうメモリを含み、ブロックロジックは消去ロジックが動作を完了する時までメモリコントローラからデータ格納部に対するアクセスを遮断するように動作する。

ステートメント３．本発明の実施形態はステートメント１にしたがうメモリを含み、パスワード格納部に受信パスワードを書き込むパスワード書込みロジックをさらに含む。

ステートメント４．本発明の実施形態はステートメント１にしたがうメモリを含み、メモリが保安モードで動作しているか否かを明示するための直列プレゼンス検出（ＳＰＤ）をさらに含む。

ステートメント５．本発明の実施形態はステートメント４にしたがうメモリを含み、ブロックロジックはメモリが保安モードで動作していないとＳＰＤが明示した場合、比較器

の呼び出しなしに、メモリコントローラがデータ格納部にアクセスすることを許容する。
ステートメント６．本発明の実施形態はステートメント１にしたがうメモリを含み、メモリが保安モードで動作しているかを明示する重要製品データ（ＶＰＤ）をさらに含む。
ステートメント７．本発明の実施形態はステートメント６にしたがうメモリを含み、ＶＰＤを格納するＥＥＰＲＯＭ（Ｅｌｅｃｔｒｏｎｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）をさらに含む。
ステートメント８．本発明の実施形態はステートメント６にしたがうメモリを含み、ブロックロジックはメモリが保安モードで動作していないとＶＰＤが明示すれば、比較器を呼び出すことなく、メモリコントローラがデータ格納部にアクセスすることを許容する。
ステートメント９．本発明の実施形態はステートメント１にしたがうメモリを含み、消去ロジックは閾値回数の受信パスワードが全て格納パスワードと異なる場合、データ格納部のデータを消去するよう動作する。

【００７９】

ステートメント１０．本発明の実施形態はステートメント１にしたがうメモリを含み、
メモリは第２使用者に対する第２データを格納するための第２データ格納部をさらに含み、
データ読出しロジックは、第２データ格納部から第２データを読み出すよう動作し、
データ書込みロジックは、第２データ格納部に第２データを書き込むよう動作し、
パスワード格納部は、第２格納パスワードを格納するよう動作し、
受信機は、第２メモリコントローラから第２受信パスワードを受信するよう動作し、
比較器は、第２受信パスワードと第２格納パスワードとを比較するよう動作し、
消去ロジックは、第２受信パスワードが第２格納パスワードと異なる場合、第２データ格納部の第２データを消去するよう動作し、
ブロックロジックは、比較器が動作を完了する時まで第２メモリコントローラから第２データ格納部へのアクセスを遮断するよう動作する。

【００８０】

ステートメント１１．本発明の実施形態はステートメント１０にしたがうメモリを含み、メモリコントローラは第２メモリコントローラである。
ステートメント１２．本発明の実施形態はステートメント１にしたがうメモリを含み、
メモリは、揮発性メモリ、不揮発性メモリ、及び任意に結合した揮発性及び不揮発性メモリ装置を含むセットから形成される。
ステートメント１３．本発明の実施形態はステートメント１にしたがうメモリを含み、受信機、比較器、消去ロジック、及びブロックロジックを含むレジスタークロックドライバー（ＲＣＤ）をさらに含む。
ステートメント１４．本発明の実施形態はステートメント１３にしたがうメモリを含み、ＲＣＤはデータ読出しロジック及びデータ書込みロジックをさらに含む。

【００８１】

ステートメント１５．本発明の実施形態はメモリへの不正アクセス防止方法を含み、メモリへの不正アクセス防止方法は、
メモリがリセットされたか否かを決定する段階と、
メモリが保安モード又は非保安モードで動作しているかを決定する段階と、
メモリが保安モードで動作している場合、
使用者に対するパスワードを選択する段階と、
メモリにパスワードを伝送する段階と、
メモリに対するアクセスを受信する段階と、を有し、
パスワードは、メモリに格納されたデータを暗号化するのには用いない。

【００８２】

ステートメント１６．本発明の実施形態はステートメント１５にしたがう方法を含み、メモリが非保安モードで動作している場合、パスワードを用いることなしに、メモリに対するアクセスを受信する段階をさらに含む。

ステートメント１７．本発明の実施形態はステートメント１５にしたがう方法を含み、メモリにパスワードを伝送する段階は、パスワードを閾値回数、メモリに伝送する段階を含む。

ステートメント１８．本発明の実施形態はステートメント１５にしたがう方法を含み、メモリに対するアクセスを受信する段階は、消去されたメモリに対するアクセスを受信する段階を含む。

ステートメント１９．本発明の実施形態はステートメント１５にしたがう方法を含み、メモリに対するアクセスを受信する段階は、メモリに格納されたデータへのアクセスを受信する段階を含む。

ステートメント２０．本発明の実施形態はステートメント１５にしたがう方法を含み、メモリがリセットされた以後の時間量を測定する段階と、

メモリがリセットされた以後の時間量が閾値より大きければ、メモリに対するソフトウェア誘導リセットを伝送する段階と、をさらに有する。

【００８３】

ステートメント２１．本発明の実施形態はステートメント１５にしたがう方法を含み、メモリは、揮発性メモリ、不揮発性メモリ、及び任意に結合した揮発性及び不揮発性メモリ装置を含むセットから形成される。

ステートメント２２．本発明の実施形態はステートメント１５にしたがう方法を含み、メモリは第１使用者に割り当てられる第１部分、及び第２使用者に割り当てられる第２部分を含む。

ステートメント２３．本発明の実施形態はステートメント１５にしたがう方法を含み、使用者に対するパスワードを選択する段階は、ランダムなパスワードを発生する段階を含む。

ステートメント２４．本発明の実施形態はステートメント１５にしたがう方法を含み、使用者に対するパスワードを選択する段階は、利用することができるパスワードのリストからパスワードを選択する段階を含む。

ステートメント２５．本発明の実施形態はステートメント１５にしたがう方法を含み、使用者に対するパスワードを選択する段階は、使用者に対する識別子（ＩＤ）のハッシュをパスワードとして生成する段階を含む。

ステートメント２６．本発明の実施形態はステートメント１５にしたがう方法を含み、使用者に対するパスワードを選択する段階は、保安プラットフォームモジュールからパスワードにアクセスする段階を含む。

【００８４】

ステートメント２７．本発明の実施形態はメモリへの不正アクセス防止方法を含み、前記方法は、

メモリが保安モードで動作していることを示す信号をメモリからメモリコントローラに伝送する段階と、

メモリコントローラから受信パスワードを受信する段階と、

受信パスワードと格納パスワードとを比較する段階と、

受信パスワードが前記格納パスワードと一致しない場合、

メモリを消去する段階と、

メモリへのアクセスをメモリコントローラに提供する段階と、を有し、

受信パスワード又は格納パスワードはメモリに格納されたデータを暗号化するのには用いない。

【００８５】

ステートメント２８．本発明の実施形態はステートメント２７にしたがう方法を含み、受信パスワードが格納パスワードと一致しない場合、メモリで受信パスワードを格納する段階をさらに有する。

ステートメント２９．本発明の実施形態はステートメント２７にしたがう方法を含み、受信パスワードが格納パスワードと一致する場合、メモリへのアクセスをメモリコントロ

ーラに提供する段階をさらに有する。
ステートメント３０．本発明の実施形態はステートメント２７にしたがう方法を含み、メモリを消去する前に閾値回数にて受信パスワードと格納パスワードとを比較する段階をさらに有する。
ステートメント３１．本発明の実施形態はステートメント２７にしたがう方法を含み、メモリコントローラからリセット命令を受信する段階と、
リセット命令に応答して前記メモリをリセットする段階と、をさらに有する。
ステートメント３２．本発明の実施形態はステートメント３１にしたがう方法を含み、リセット命令に応答してメモリをリセットする段階はメモリ内のすべてのデータに対してガーベッジコレクションを遂行する段階を含む。
ステートメント３３．本発明の実施形態はステートメント３１にしたがう方法を含み、リセット命令に応答してメモリをリセットする段階はメモリ内のすべてのデータに対して順次に上書きを遂行する段階を含む。

【００８６】

ステートメント３４．本発明の実施形態はステートメント３１にしたがう方法を含み、リセット命令に応答してメモリをリセットする段階はメモリ内のすべてのデータを定数値に上書きをする段階を含む。
ステートメント３５．本発明の実施形態はステートメント３１にしたがう方法を含み、リセット命令に応答してメモリをリセットする段階はメモリ内のすべてのデータがメモリにそれ以上格納されなくなる時までメモリ内のすべてのデータに対するリフレッシュを防止する段階を含む。
ステートメント３６．本発明の実施形態はステートメント２７にしたがう方法を含み、メモリが保安モードで動作しているかどうかを示す信号をメモリからメモリコントローラに伝送する段階はメモリが保安モードで動作しているかに対してメモリコントローラからの要請を受信する段階を含む。
ステートメント３７．本発明の実施形態はステートメント２７にしたがう方法を含み、メモリコントローラから受信パスワードを受信する段階はメモリコントローラからパスワードを要請する段階を含む。
ステートメント３８．本発明の実施形態はステートメント２７にしたがう方法を含み、メモリは揮発性メモリ、不揮発性メモリ、及び任意に結合した揮発性及び不揮発性メモリ装置を含むセットから形成される。
ステートメント３９．本発明の実施形態はステートメント２７にしたがう方法を含み、メモリは第１使用者に割て当てられる第１部分及び第２使用者に割り当てられる第２部分を含む。

【００８７】

ステートメント４０．本発明の実施形態は有形の記憶媒体を含む物品を含み、有形の記憶媒体上に非一時的に命令（ｉｎｓｔｒｕｃｔｉｏｎ）が格納され、有形の記憶媒体がマシンによって実行される時、このような実行は、メモリがリセットされたかどうかを決定する段階と、
メモリが保安モード又は非保安モードで動作しているかどうかを決定する段階と、
メモリが保安モードで動作している場合、
使用者に対するパスワードを選択する段階と、
メモリにパスワードを伝送する段階と、
メモリへのアクセスを受信する段階と、を有し、
パスワードはメモリに格納されたデータを暗号化するのには用いない。

【００８８】

ステートメント４１．本発明の実施形態はステートメント４０にしたがう物品を含み、有形の記憶媒体上に非一時的に命令が格納され、有形の記憶媒体がマシンによって実行される時、このような実行は、メモリが非保安モードで動作している場合、パスワードを使用せずに、メモリへのアクセスを受信する段階をさらに含む。

ステートメント４２．本発明の実施形態はステートメント４０にしたがう物品を含み、メモリにパスワードを伝送する段階はパスワードを閾値回数、メモリに伝送する段階を含む。

ステートメント４３．本発明の実施形態はステートメント４０にしたがう物品を含み、メモリへのアクセスを受信する段階は消去されたメモリへのアクセスを受信する段階を含む。

ステートメント４４．本発明の実施形態はステートメント４０にしたがう物品を含み、メモリへのアクセスを受信する段階はメモリに格納されたデータへのアクセスを受信する段階を含む。

ステートメント４５．本発明の実施形態はステートメント４０にしたがう物品を含み、有形の記憶媒体上に非一時的な命令が格納され、有形の記憶媒体がマシンによって実行される時、このような実行は、

メモリがリセットされた以後の時間量を測定する段階と、

メモリがリセットされた以後の時間量が閾値より大きければ、メモリに対するソフトウェア誘導リセットを伝送する段階と、をさらに有する。

【００８９】

ステートメント４６．本発明の実施形態はステートメント４０にしたがう物品を含み、メモリは揮発性メモリ、不揮発性メモリ、及び任意に結合した揮発性及び不揮発性メモリ装置を含むセットから形成される。

ステートメント４７．本発明の実施形態はステートメント４０にしたがう物品を含み、メモリは第１使用者に割り当てられる第１部分及び第２使用者に割り当てられる第２部分を含む。

ステートメント４８．本発明の実施形態はステートメント４０にしたがう物品を含み、使用者に対するパスワードを選択する段階はランダムなパスワードを発生する段階を含む。

ステートメント４９．本発明の実施形態はステートメント４０にしたがう物品を含み、使用者に対するパスワードを選択する段階は利用することができるパスワードのリストからパスワードを選択する段階を含む。

ステートメント５０．本発明の実施形態はステートメント４０にしたがう物品を含み、使用者に対するパスワードを選択する段階は使用者に対する識別子のハッシュをパスワードとして生成する段階を含む。

ステートメント５１．本発明の実施形態はステートメント４０にしたがう物品を含み、使用者に対するパスワードを選択する段階は保安プラットフォームモジュールからパスワードにアクセスする段階を含む。

【００９０】

ステートメント５２．本発明の実施形態は有形の記憶媒体を含む物品を含み、有形の記憶媒体上に非一時的に命令が格納され、有形の記憶媒体がマシンによって実行される時、このような実行は、メモリが保安モードで動作しているかどうかを示す信号をメモリからメモリコントローラに伝送する段階と、

メモリコントローラから受信パスワードを受信する段階と、

受信パスワードと格納パスワードとを比較する段階と、

受信パスワードが格納パスワードと一致しない場合、

メモリを消去する段階と、

メモリへのアクセスをメモリコントローラに提供する段階と、を有し、

受信パスワード又は格納パスワードはメモリに格納されたデータを暗号化するのには用いない。

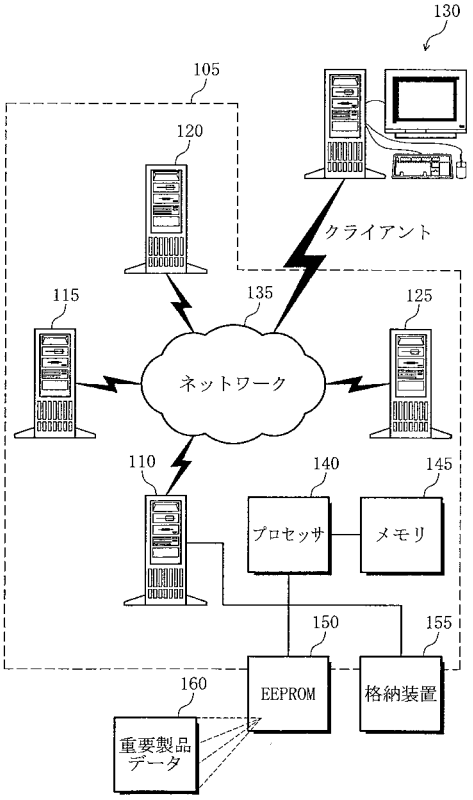
【００９１】

ステートメント５３．本発明の実施形態はステートメント５２にしたがう物品を含み、有形の記憶媒体上に非一時的に命令が格納され、有形の記憶媒体がマシンによって実行される時、このような実行は、受信パスワードが格納パスワードと一致しない場合、メモリ

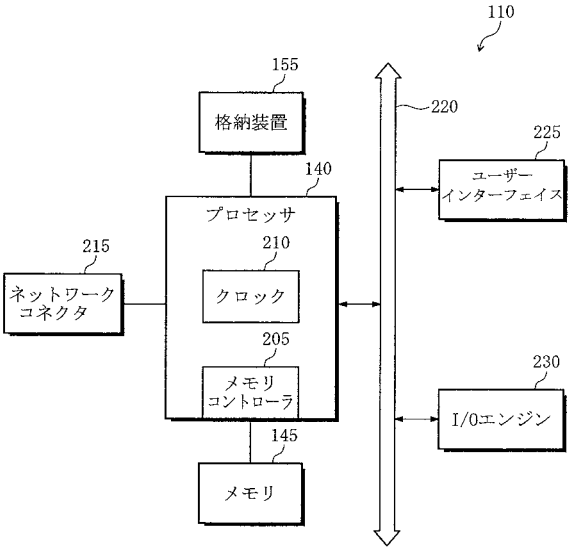
に受信パスワードを格納する段階をさらに有する。
ステートメント５４．本発明の実施形態はステートメント５２にしたがう物品を含み、受信パスワードが格納パスワードと一致する場合、メモリへのアクセスをメモリコントローラに提供する段階をさらに有する。
ステートメント５５．本発明の実施形態はステートメント５２にしたがう物品を含み、有形の記憶媒体上に非一時的に命令が格納され、有形の記憶媒体がマシンによって実行される時、このような実行は、メモリを消去する前に閾値回数、受信パスワードと格納パスワードとを比較する段階をさらに有する。
ステートメント５６．本発明の実施形態はステートメント５２にしたがう物品を含み、有形の記憶媒体上に非一時的に命令が格納され、有形の記憶媒体がマシンによって実行される時、このような実行は、メモリコントローラからリセット命令を受信する段階と、
リセット命令に応答してメモリをリセットする段階と、をさらに有する。
【００９２】
ステートメント５７．本発明の実施形態はステートメント５６にしたがう物品を含み、リセット命令に応答してメモリをリセットする段階はメモリ内のすべてのデータに対してガーベッジコレクションを遂行する段階を含む。
ステートメント５８．本発明の実施形態はステートメント５６にしたがう物品を含み、リセット命令に応答してメモリをリセットする段階はメモリ内のすべてのデータに対して順次に上書きを遂行する段階を含む。
ステートメント５９．本発明の実施形態はステートメント５６にしたがう物品を含み、リセット命令に応答してメモリをリセットする段階はメモリ内のすべてのデータを定数値に上書きをする段階を含む。
ステートメント６０．本発明の実施形態はステートメント５６にしたがう物品を含み、リセット命令に応答してメモリをリセットする段階はメモリ内のすべてのデータがメモリにそれ以上格納されなくなる時までメモリ内のすべてのデータに対するリフレッシュを防止する段階を含む。
【００９３】
ステートメント６１．本発明の実施形態はステートメント５２にしたがう物品を含み、メモリが保安モードで動作しているかどうかを示す信号をメモリからメモリコントローラに伝送する段階はメモリが保安モードで動作しているかどうかに対してメモリコントローラからの要請を受信する段階を含む。
ステートメント６２．本発明の実施形態はステートメント５２にしたがう物品を含み、メモリコントローラから受信パスワードを受信する段階はメモリコントローラからパスワードを要請する段階を含む。
ステートメント６３．本発明の実施形態はステートメント５２にしたがう物品を含み、メモリは揮発性メモリ、不揮発性メモリ、及び任意に結合した揮発性及び不揮発性メモリ装置を含むセットから形成される。
ステートメント６４．本発明の実施形態はステートメント５２にしたがう物品を含み、メモリは第１使用者に割り当てられる第１部分及び第２使用者に割り当てられる第２部分を含む。
【００９４】
尚、本発明は、上述の実施形態に限られるものではない。本発明の技術的範囲から逸脱しない範囲内で多様に変更実施することが可能である。
【符号の説明】
【００９５】
１０５　データセンター
１１０、１１５、１２０、１２５　ホストマシン
１３０　クライアントマシン
１３５　ネットワーク
１４０　プロセッサ

１４５　メモリ
１５０　ＥＥＰＲＯＭ
１５５　格納装置
１６０　重要製品データ
２０５、６２０　メモリコントローラ
２１０　クロック
２１５　ネットワークコネクタ
２２０　バス
２２５　ユーザーインターフェイス
２３０　入／出力（Ｉ／Ｏ）エンジン
３０５　レジスタークロックドライバー（ＲＣＤ）
３１０、３１５、３２０、３２５、３３０、３３５、３４０、３４５　メモリチップ（データ格納部）
３５０　直列プレゼンス検出（ＳＰＤ）
３５５、４５５　格納部（パスワード格納部）
４０５　データ読出しロジック
４１０　データ書込みロジック
４１５　認証ロジック
４２０　受信機
４２５　ブロックロジック
４３０　比較器
４３５　消去ロジック
４４０　パスワード書込みロジック
５０５　受信パスワード
５１０　格納パスワード
５１５　比較結果
５２０　閾値
６０５、６１０　部分
６１５　インターフェイス

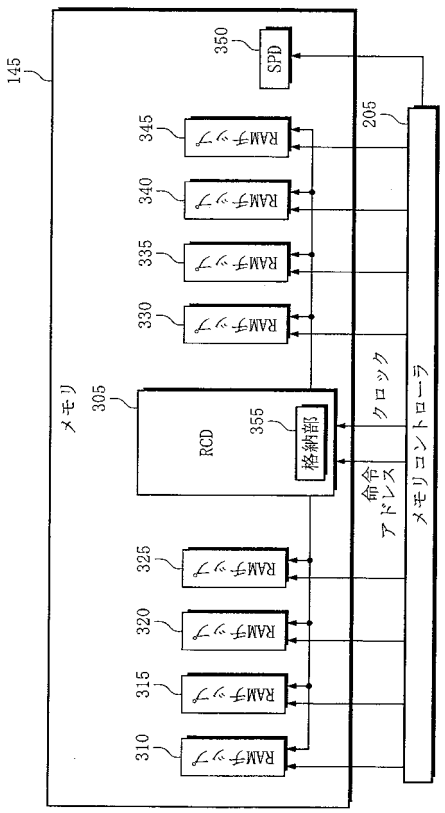
【図１】


130
105
120
クライアント
115
135
125
ネットワーク
110
140
145
プロセッサ
メモリ
150
155
160
EEPROM
格納装置
重要製品データ

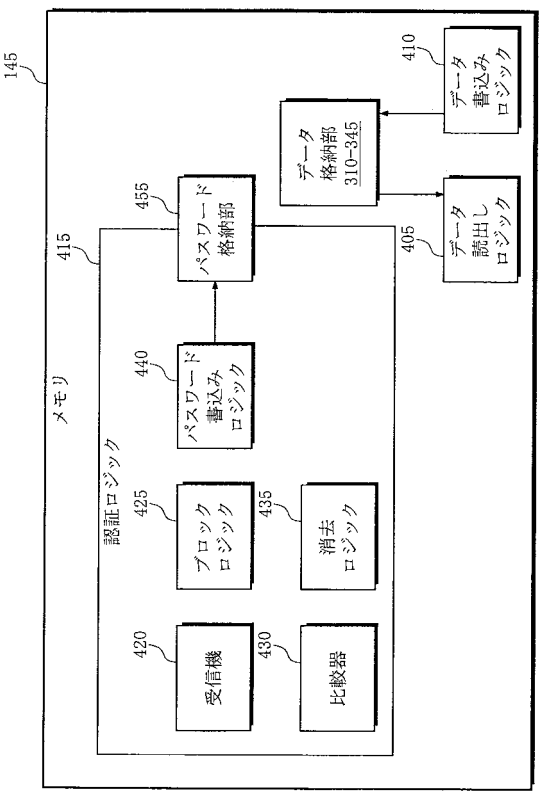
【図２】


110
155
格納装置
220
225
ユーザーインターフェイス
140
プロセッサ
215
210
ネットワークコネクタ
クロック
205
メモリコントローラ
230
I/Oエンジン
145
メモリ

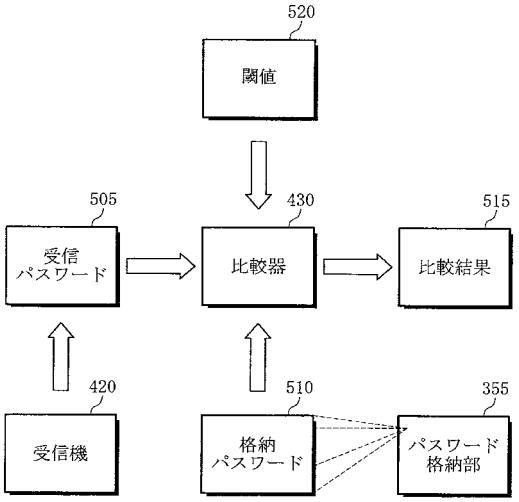
【図３】


145
350
SPD
345
340
335
330
RAMチップ
205
メモリ
305
RCD
355
格納部
クロック
命令アドレス
メモリコントローラ
325
320
315
310

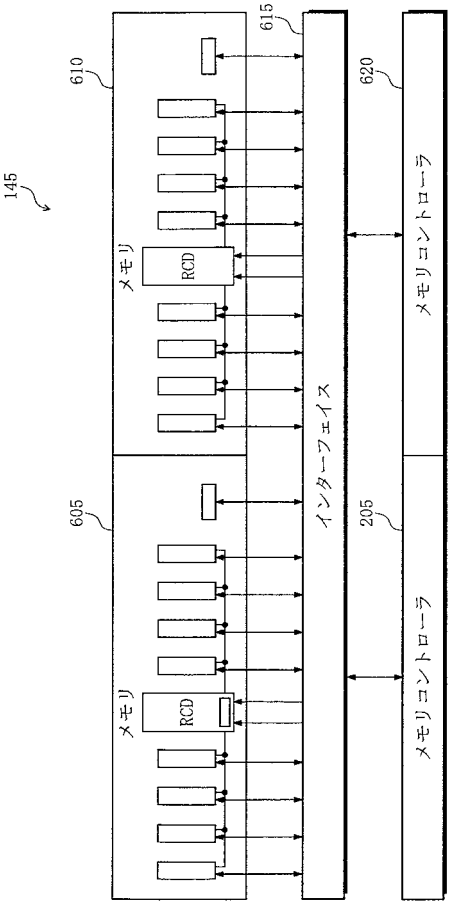
【図４】


145
410
データ書込みロジック
データ格納部310-345
455
パスワード格納部
415
405
データ読出しロジック
メモリ
440
パスワード書込みロジック
認証ロジック
425
435
ブロックロジック
消去ロジック
420
430
受信機
比較器

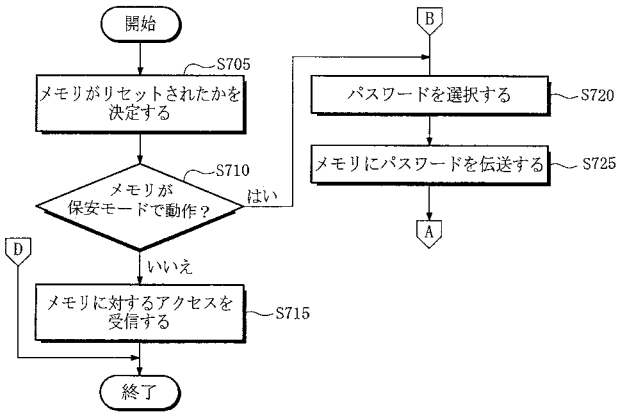
【図５】



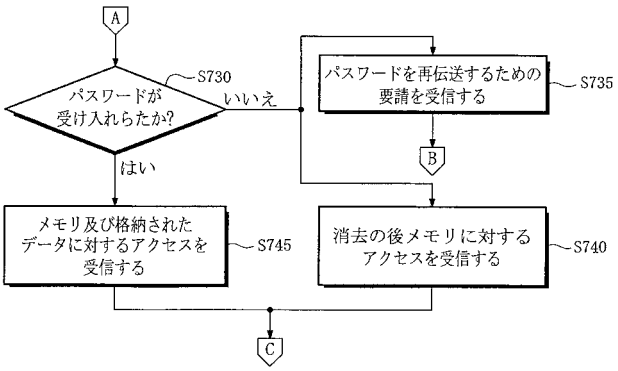
【図６】



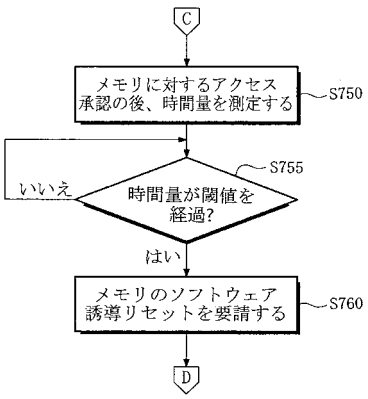
【図７Ａ】



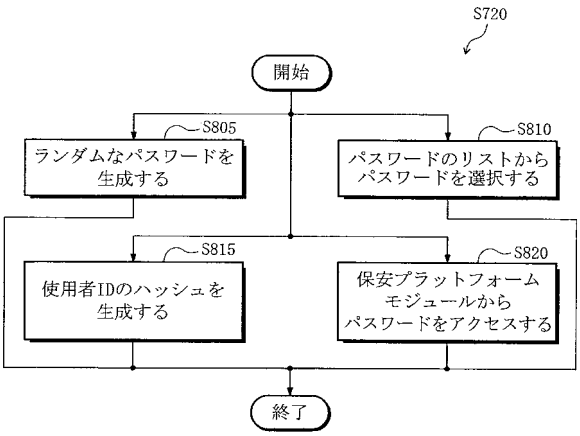
【図７Ｂ】



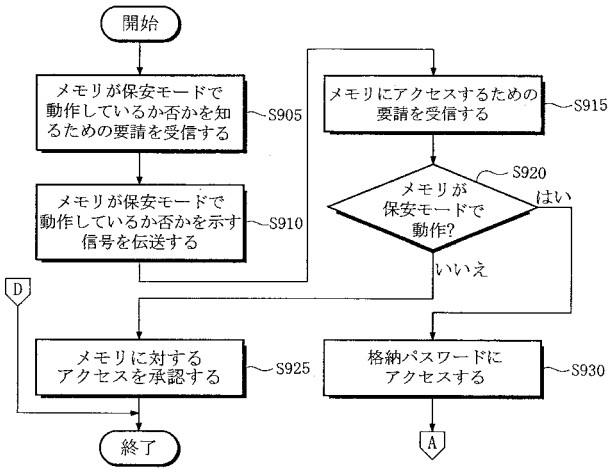
【図７Ｃ】



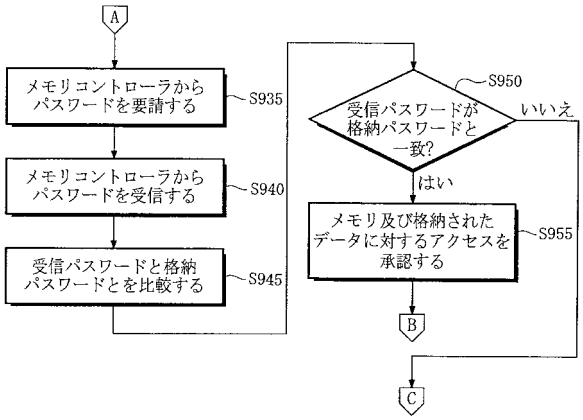
【図８】



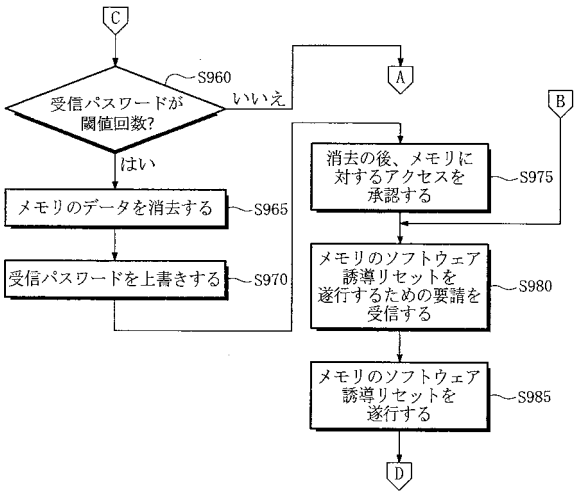
【図９Ａ】



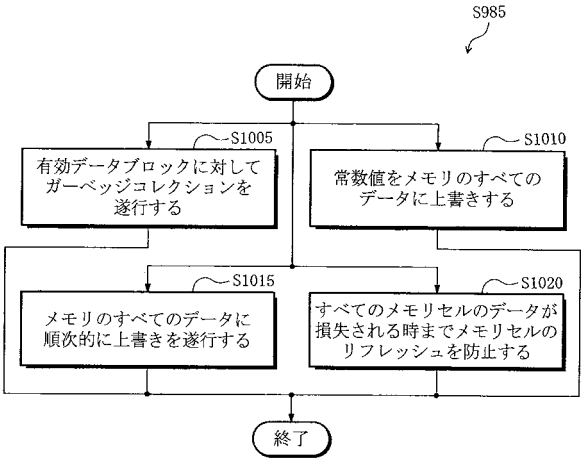
【図９Ｂ】



【図９Ｃ】



【図１０】



フロントページの続き

(72)発明者　張　牧　天
アメリカ合衆国,　カリフォルニア州　９５０５１,　サンタクララ,　ビア　トリノ　プレイス
,　２９２０