

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6829161号  
(P6829161)

(45) 発行日 令和3年2月10日(2021.2.10)

(24) 登録日 令和3年1月25日(2021.1.25)

(51) Int. Cl. F 1  
G 0 6 F 21/62 (2013.01) G 0 6 F 21/62

請求項の数 31 (全 29 頁)

|                    |                              |           |  |
|--------------------|------------------------------|-----------|--|
| (21) 出願番号          | 特願2017-146478 (P2017-146478) | (73) 特許権者 | 390019839<br>三星電子株式会社<br>Samsung Electronics<br>Co., Ltd.<br>大韓民国京畿道水原市靈通区三星路129<br>129, Samsung-ro, Yeon<br>gtong-gu, Suwon-si, G<br>yeonggi-do, Republic<br>of Korea |
| (22) 出願日           | 平成29年7月28日(2017.7.28)        | (74) 代理人  | 110000051<br>特許業務法人共生国際特許事務所   |
| (65) 公開番号          | 特開2018-22486 (P2018-22486A)  | (72) 発明者  | ソンボン ポール オラリグ<br>アメリカ合衆国, カリフォルニア州 9<br>4566, プレザントン, パセオグ<br>ラナダ, 3050  |
| (43) 公開日           | 平成30年2月8日(2018.2.8)          |           |  |
| 審査請求日              | 令和2年7月28日(2020.7.28)         |           |  |
| (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・地域又は機関 | 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・地域又は機関 | 米国 (US)                      |           |  |
| 早期審査対象出願           |                              |           | 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) 【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、  
 前記比較器による比較にて、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  
 化するには用いず、  
 前記受信パスワードは、前記比較器にて前記格納パスワードと一致しない前記受信パス  
 ワードに基づいて、前記パスワード格納部に格納され、  
 前記メモリが保安(secure)モードの場合、前記メモリの全体が前記保安モード  
 になり、前記メモリが非保安モード(non-secure)の場合、前記メモリの全体  
 が前記非保安モードになることを特徴とするメモリ。

10

20

## 【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 ( s e c u r e ) モードで動作している否かを特定するための直列ブレゼンス検出 ( S e r i a l P r e s e n c e D e t e c t : S P D ) 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。

10

## 【請求項 5】

前記 S P D に少なくとも部分的に基づいて、前記ブロックロジックは、前記メモリコントローラが前記比較器の呼び出しなしに前記データ格納部にアクセスすることを許可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】

前記格納パスワードとはすべて異なる受信パスワードの閾値回数に少なくとも部分的に基づいて、消去ロジックは、前記データ格納部内のデータを消去するように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クロックドライバー ( R e g i s t e r C l o c k D r i v e r : R C D ) 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。

20

## 【請求項 8】

前記ブロックロジック及び前記消去ロジックは、電力が遮断された後、前記第 1 使用者に対するデータへのアクセスを防止するように動作し、それにより、揮発性メモリにデータを失わせることを特徴とする請求項 1 に記載のメモリ。

## 【請求項 9】

前記メモリは、前記保安モードまたは非保安モードのいずれかであることを特徴とする請求項 1 に記載のメモリ。

30

## 【請求項 10】

前記受信パスワードは、前記メモリコントローラによって生成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 11】

前記メモリは、揮発性メモリの代わりに使用される不揮発性デュアルインラインメモリモジュール ( N V D I M M ) を含むことを特徴とする請求項 1 に記載のメモリ。

## 【請求項 12】

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又は非保安 ( n o n - s e c u r e ) モードで動作しているという信号をメモリコントローラで前記メモリから受信する段階と、

40

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には用いず、

前記パスワードは、前記メモリに格納されたパスワードと一致しないパスワードに少なくとも部分的に基づいて前記メモリに格納され、

前記メモリが前記保安モードの場合、前記メモリの全体が前記保安モードになり、前記メモリが前記非保安モードの場合、前記メモリの全体が前記非保安モードになることを特徴とするメモリへの不正アクセス防止方法。

50

## 【請求項 13】

前記非保安モードで動作している前記メモリに少なくとも部分的に基づいて、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 12 に記載のメモリへの不正アクセス防止方法。

## 【請求項 14】

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 ( t h r e s h o l d ) 回数、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 12 に記載のメモリへの不正アクセス防止方法。

## 【請求項 15】

前記メモリへのアクセスを受ける段階は、第 2 パスワードと一致しないパスワードに少なくとも部分的に基づいて、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 12 に記載のメモリへの不正アクセス防止方法。

10

## 【請求項 16】

前記メモリがリセットされた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後の時間量に少なくとも部分的に基づいて、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、  
前記ソフトウェア誘導リセット後、前記メモリコントローラが前記メモリ内のデータにアクセスするための認証を要求する段階と、をさらに有する請求項 12 に記載のメモリへの不正アクセス防止方法。

20

## 【請求項 17】

前記メモリは、揮発性メモリの代わりに使用される不揮発性デュアルインラインメモリモジュール ( N V D I M M ) を含むことを特徴とする請求項 12 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は、認証を実行せずに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 12 に記載のメモリへの不正アクセス防止方法。

## 【請求項 19】

前記メモリが保安モード又は非保安モードで動作しているという信号をメモリコントローラで前記メモリから受信する段階は、前記メモリが前記保安モード又は前記非保安モードのいずれかであることを含むことを特徴とする請求項 12 に記載のメモリへの不正アクセス防止方法。

30

## 【請求項 20】

前記使用者に対するパスワードを選択する段階は、前記メモリコントローラによって前記使用者に対するパスワードを生成する段階を含むことを特徴とする請求項 12 に記載のメモリへの不正アクセス防止方法。

## 【請求項 21】

電力が遮断された後、前記メモリ内のデータへのアクセスを防止するように動作し、それにより、前記揮発性メモリにデータを失わせることを特徴とする請求項 17 に記載のメモリへの不正アクセス防止方法。

40

## 【請求項 22】

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、  
前記格納パスワードと一致しない前記受信パスワードに少なくとも部分的に基づいて、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ず、

50

前記メモリは、前記保安モード及び非保安モードをサポートし、

前記メモリが前記保安モードの場合、前記メモリの全体が前記保安モードになり、前記メモリが前記非保安モードの場合、前記メモリの全体が前記非保安モードになる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 2 3】

前記格納パスワードと一致する前記受信パスワードに少なくとも部分的に基づいて、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 2 2 に記載のメモリへの不正アクセス防止方法。

【請求項 2 4】

前記メモリを消去する前に、前記受信パスワードを受信し、受信パスワードと前記格納パスワードを閾値回数、比較する段階をさらに有することを特徴とする請求項 2 2 に記載のメモリへの不正アクセス防止方法。

【請求項 2 5】

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回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 2 2 に記載のメモリへの不正アクセス防止方法。

【請求項 2 6】

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関する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 2 2 に記載のメモリへの不正アクセス防止方法。

【請求項 2 7】

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受信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 2 2 に記載のメモリへの不正アクセス防止方法。

【請求項 2 8】

前記メモリは、前記保安モード又は前記非保安モードのいずれかであることを特徴とする請求項 2 2 に記載のメモリへの不正アクセス防止方法。

【請求項 2 9】

電力が遮断された後、前記メモリ内のデータへのアクセスを防止するように動作し、それにより、揮発性メモリにデータを失わせることを特徴とする請求項 2 2 に記載のメモリへの不正アクセス防止方法。

【請求項 3 0】

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は、前記メモリコントローラによって使用者に対するパスワードを生成する段階を含むことを特徴とする請求項 2 2 に記載のメモリへの不正アクセス防止方法。

【請求項 3 1】

前記メモリは、揮発性メモリの代わりに使用される不揮発性デュアルインラインメモリモジュール ( N V D I M M ) を含み、

前記メモリは、前記メモリが前記非保安モードで動作しているときに、認証なしで前記メモリへのアクセスを提供することを特徴とする請求項 2 2 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】

【 0 0 0 1】

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】

【 0 0 0 2】

不揮発性メモリ ( N V M s ) 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

10

20

30

40

50

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、前記比較器による比較にて、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には用いず、前記受信パスワードは、前記比較器にて前記格納パスワードと一致しない前記受信パスワードに基づいて、前記パスワード格納部に格納され、前記メモリが保安(secure)モードの場合、前記メモリの全体が前記保安モードになり、前記メモリが非保安モード(non-secure)の場合、前記メモリの全体が前記非保安モードになることを特徴とする。

【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又は非保安

10

20

30

40

50

(non-secure)モードで動作しているという信号をメモリコントローラで前記メモリから受信する段階と、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には用いず、前記パスワードは、前記メモリに格納されたパスワードと一致しないパスワードに少なくとも部分的に基づいて前記メモリに格納され、前記メモリが前記保安モードの場合、前記メモリの全体が前記保安モードになり、前記メモリが前記非保安モードの場合、前記メモリの全体が前記非保安モードになることを特徴とする。

10

## 【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、前記格納パスワードと一致しない前記受信パスワードに少なくとも部分的に基づいて、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には用いず、前記メモリは、前記保安モード及び非保安モードをサポートし、前記メモリが前記保安モードの場合、前記メモリの全体が前記保安モードになり、前記メモリが前記非保安モードの場合、前記メモリの全体が前記非保安モードになることを特徴とする。

20

## 【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ユーザーデータが消去されるので、メモリに格納されたユーザー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。

30

## 【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。

40

【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

50

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

10

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

20

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。

30

【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

40

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

50

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、システムは通常の(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、任意の利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を使用する利用者と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、利用者が自宅に配達されることができる製品を購入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は利用者が購買を選択し、決済を完了する間に利用者のショッピングカートを格納するために利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を含むことができる。

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

10

20

30

40

50



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。

10

【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。

20

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。

30

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。

40

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

50

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。

10

【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。

20

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がリソースの使用権貸が終了(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。

30

【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に問い合わせるメモリ145が保安モードで動作しているかどうかを決定する。

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。

40

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。

50

この時、R C D 3 0 5 は受信されたパスワードと格納部 3 5 5 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 2 0 5 はメモリ 1 4 5 へのアクセスが承認され、このような信号は D Q バスを通じて伝送される。

そうでない場合、メモリ 1 4 5 はメモリチップ ( 3 1 0 ~ 3 4 5 ) 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 2 0 5 はメモリ 1 4 5 へのアクセスが承認される。

#### 【 0 0 3 3 】

以後のアクセスを容易にするために、R C D 3 0 5 はまた受信されたパスワードを格納部 3 5 5 に格納し、メモリコントローラ 2 0 5 が受信されたパスワードを利用して以後のメモリ 1 4 5 に対する認証をできるようにする。

R C D 3 0 5 は、また格納部 3 5 5 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 1 4 5 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。

#### 【 0 0 3 4 】

メモリコントローラ 2 0 5 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 I D のハッシュ ( h a s h ) を生成するか、或いは保安プラットフォームモジュール ( T P M : T r u s t e d P l a t f o r m M o d u l e ) 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。

#### 【 0 0 3 5 】

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 1 4 5 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 1 4 5 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。

#### 【 0 0 3 6 】

既存のシステムに対する有用な比喻は、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るれば、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い、これはアクセスを遅くするようにする。

#### 【 0 0 3 7 】

これに反して、メモリ 1 4 5 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 1 4 5 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。

#### 【 0 0 3 8 】

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】

これがどのく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。

10

20

30

40

50

このような順序の例示として米国国防省 ( Department of Defense : 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、パスワード書き込みロジック440を含む。

パスワード書き込みロジック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、パスワード書き込みロジック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。

10

20

30

40

50

## 【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

10

20

30

40

50

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S705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からの要請に回答して、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S730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

10

20

30

40

50

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 S 735 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 7 A のステップ S 720 に戻る。

【0061】

代案として、ステップ S 740 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 S 735 とステップ S 740 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。

10

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 S 745 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 7 C のステップ S 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。

20

次に、ステップ S 755 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 S 760 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。

30

図 8 のステップ S 805 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 S 810 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 S 815 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 S 820 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。

40

【0065】

図 9 A ~ 図 9 C 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 9 A のステップ S 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 S 910 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

50



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送信する。

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S935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S960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S935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14

10

20

30

40

50

5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の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 Engineers)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ア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

10

20

30

40

50

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。

【 0 0 7 5 】

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種類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。

【 0 0 7 6 】

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。

10

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。

20

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。

【 0 0 7 7 】

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

ステートメント ( S t a t e m e n t ) 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には用いない。

30

40

【 0 0 7 8 】

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 ( S P D ) 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

50

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。 10

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、 20  
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。 30

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クロックドライバ(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、 40

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 50

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送信する段階は、パスワードを閾値回数、メモリに送信する段階を含む。

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。

10

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後の時間量を測定する段階と、

メモリがリセットされた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送信する段階と、をさらに有する。

#### 【 0 0 8 3 】

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。

20

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 ( I D ) のハッシュをパスワードとして生成する段階を含む。

30

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。

#### 【 0 0 8 4 】

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送信する段階と、

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。

40

#### 【 0 0 8 5 】

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、

50

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ตอบสนอง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ตอบสนอง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ตอบสนอง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。

#### 【 0 0 8 6 】

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ตอบสนอง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ตอบสนอง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。

#### 【 0 0 8 7 】

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 ( i n s t r u c t i o n ) 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には用いない。

#### 【 0 0 8 8 】

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。

10

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後の時間量を測定する段階と、

メモリがリセットされた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。

20

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。

30

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、

40

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

50

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、リセット命令に回答してメモリをリセットする段階と、をさらに有する。

#### 【 0 0 9 2 】

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、リセット命令に回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、リセット命令に回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、リセット命令に回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、リセット命令に回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。

#### 【 0 0 9 3 】

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。

#### 【 0 0 9 4 】

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 】

#### 【 0 0 9 5 】

- 1 0 5      データセンター
- 1 1 0、1 1 5、1 2 0、1 2 5      ホストマシン
- 1 3 0      クライアントマシン
- 1 3 5      ネットワーク

10

20

30

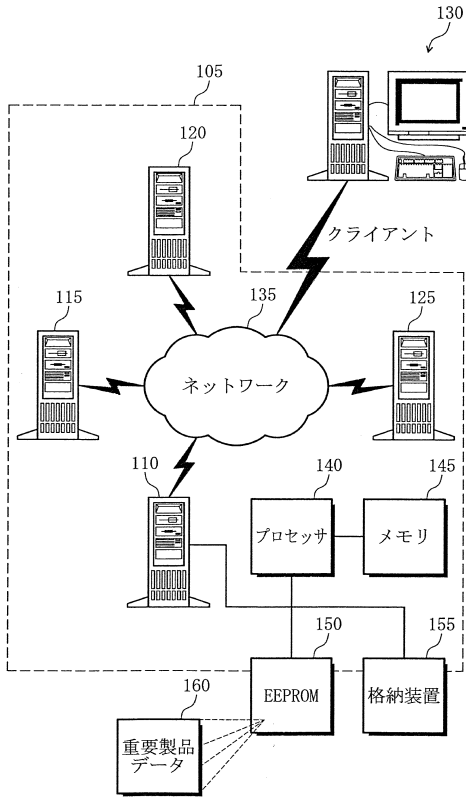
40

50

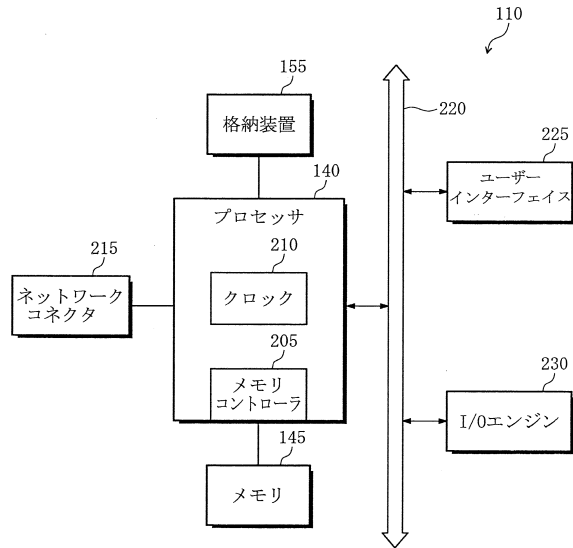


|   |                        |    |
|---|------------------------|----|
| 1 4 0   | プロセッサ                  |    |
| 1 4 5   | メモリ                    |    |
| 1 5 0   | E E P R O M            |    |
| 1 5 5   | 格納装置                   |    |
| 1 6 0   | 重要製品データ                |    |
| 2 0 5、6 2 0                                     | メモリコントローラ              |    |
| 2 1 0   | クロック                   |    |
| 2 1 5   | ネットワークコネクタ             |    |
| 2 2 0   | バス                     |    |
| 2 2 5   | ユーザーインターフェイス           | 10 |
| 2 3 0   | 入/出力 ( I / O ) エンジン    |    |
| 3 0 5   | レジスタクロックドライバ ( R C D ) |    |
| 3 1 0、3 1 5、3 2 0、3 2 5、3 3 0、3 3 5、3 4 0、3 4 5 | メモリチップ                 |    |
| ( データ格納部 )                                      |                        |    |
| 3 5 0   | 直列プレゼンス検出 ( S P D )    |    |
| 3 5 5、4 5 5                                     | 格納部 ( パスワード格納部 )       |    |
| 4 0 5   | データ読出しロジック             |    |
| 4 1 0   | データ書込みロジック             |    |
| 4 1 5   | 認証ロジック                 |    |
| 4 2 0   | 受信機                    | 20 |
| 4 2 5   | ブロックロジック               |    |
| 4 3 0   | 比較器                    |    |
| 4 3 5   | 消去ロジック                 |    |
| 4 4 0   | パスワード書込みロジック           |    |
| 5 0 5   | 受信パスワード                |    |
| 5 1 0   | 格納パスワード                |    |
| 5 1 5   | 比較結果                   |    |
| 5 2 0   | 閾値                     |    |
| 6 0 5、6 1 0                                     | 部分                     |    |
| 6 1 5   | インターフェイス               | 30 |

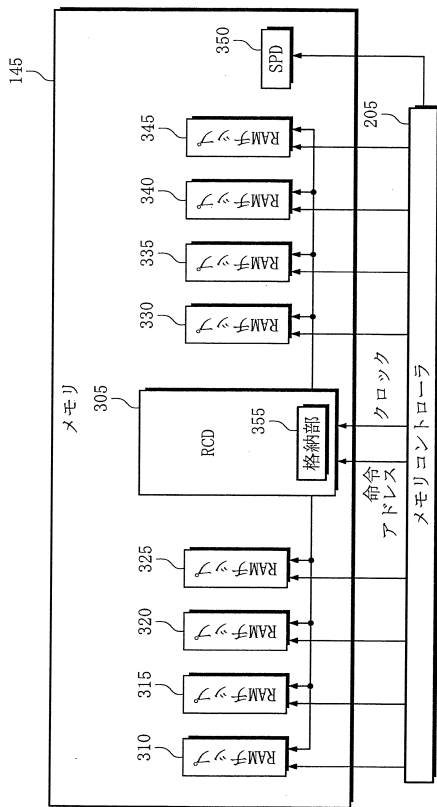
【図1】



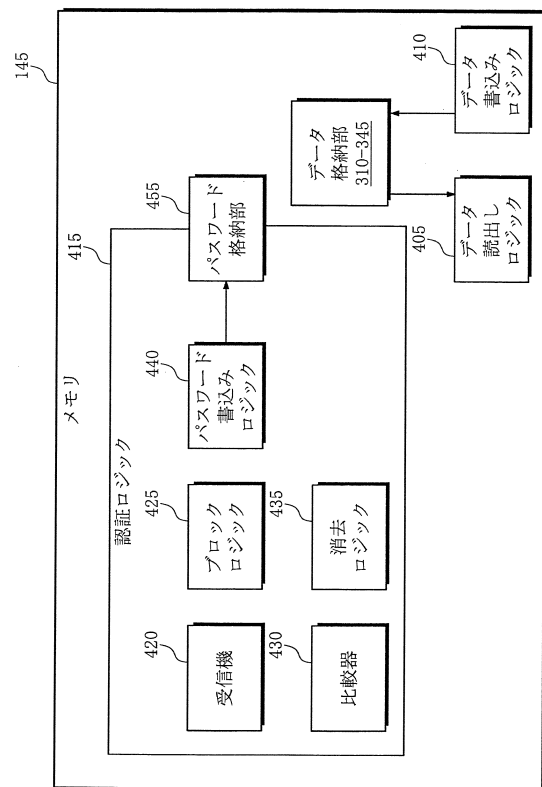
【図2】



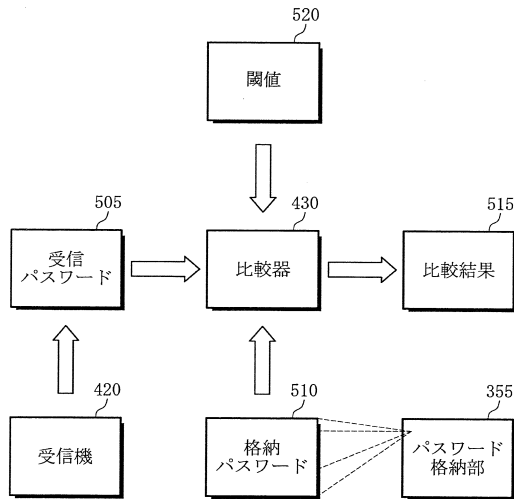
【図3】



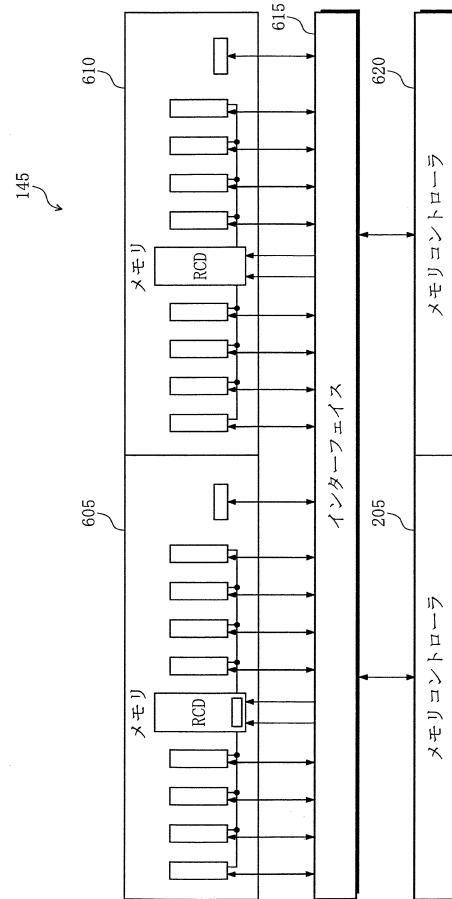
【図4】



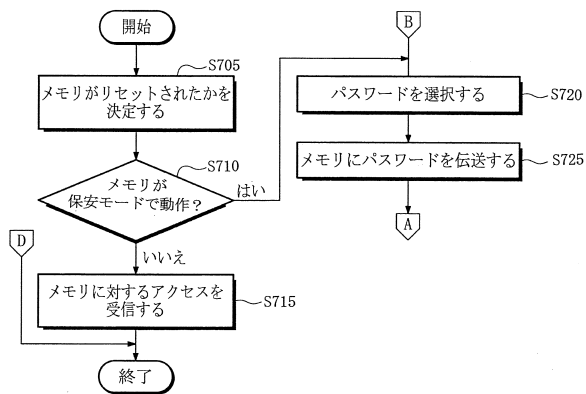
【図5】



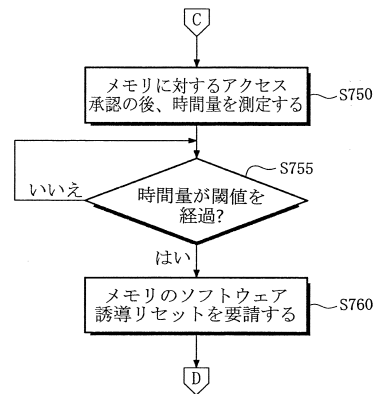
【図6】



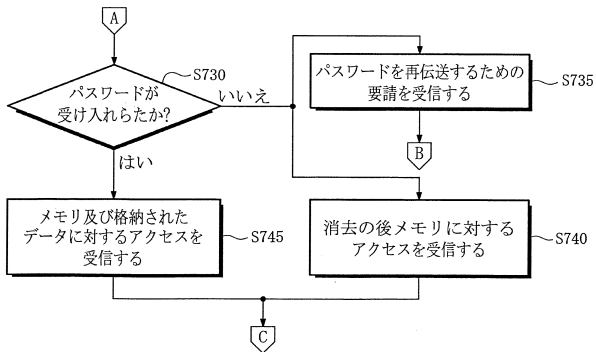
【図7A】



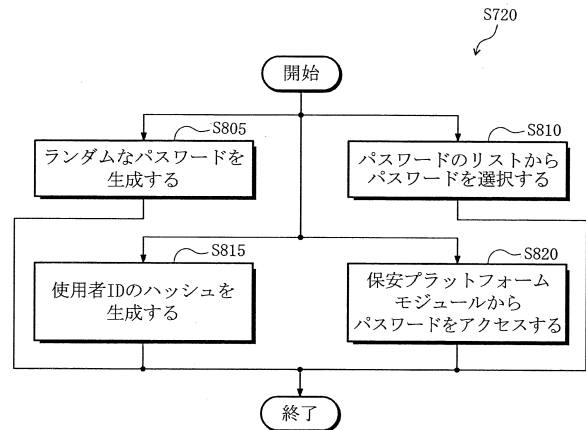
【図7C】



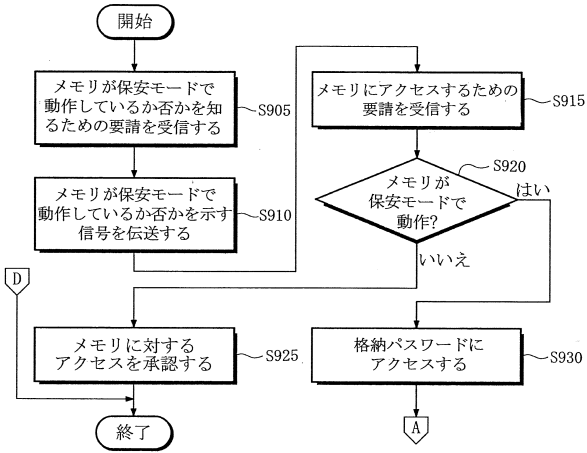
【図7B】



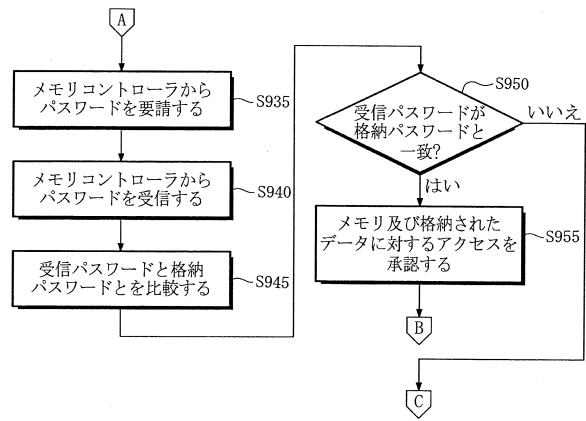
【図8】



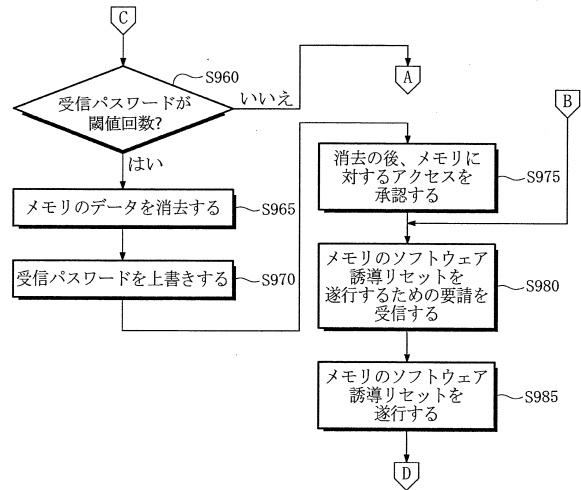
【図9A】



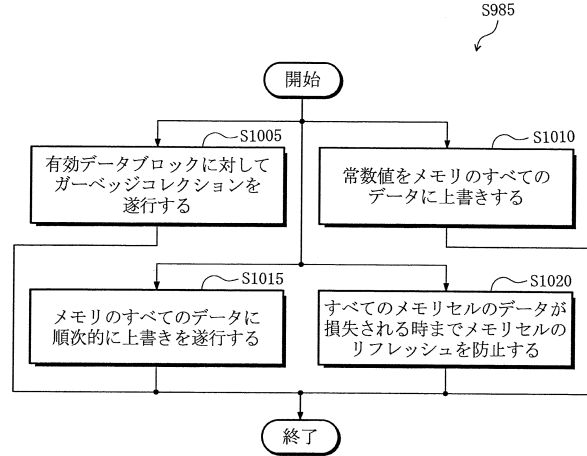
【図9B】



【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

審査官 平井 誠

(56)参考文献 米国特許出願公開第2014/0289488 (US, A1)

(58)調査した分野(Int.Cl., DB名)

G06F 21/00 - 88

G06F 12/14