(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6584823号
(P6584823)
(45)発行日　令和1年10月2日(2019.10.2)　(24)登録日　令和1年9月13日(2019.9.13)

(51)Int.Cl.　F I
G06F 21/64 (2013.01)　G06F 21/64
G06F 12/1009 (2016.01)　G06F 12/1009
G06F 12/1036 (2016.01)　G06F 12/1036　100

請求項の数 23　(全 90 頁)

(21)出願番号　特願2015-98395(P2015-98395)
(22)出願日　平成27年5月13日(2015.5.13)
(65)公開番号　特開2016-21224(P2016-21224A)
(43)公開日　平成28年2月4日(2016.2.4)
審査請求日　平成30年2月2日(2018.2.2)
(31)優先権主張番号　特願2014-127601(P2014-127601)
(32)優先日　平成26年6月20日(2014.6.20)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　110001737
特許業務法人スズエ国際特許事務所
(72)発明者　橋本　幹生
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　山田　菜穂子
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　金井　遵
東京都港区芝浦一丁目１番１号　株式会社東芝内

最終頁に続く

(54)【発明の名称】メモリ管理装置、プログラム、及び方法

(57)【特許請求の範囲】
【請求項１】
親テーブル及び子テーブルを含むテーブルツリーと、前記親テーブルに関連付けられる親検証子及び前記子テーブルに関連付けられる子検証子を含む検証子ツリーであって、前記親検証子は前記子テーブル及び前記子検証子に対する検証に用いられる前記検証子ツリーと、を記憶する第１の記憶部に対して読み込み及び書き込みを行う外部入出力部と、
安全な第２の記憶部に記憶されている前記テーブルツリーの一部であるセキュアテーブルツリー及び前記検証子ツリーのうちの一部であるセキュア検証子ツリーに基づいて、仮想アドレスを前記第１の記憶部又は前記第２の記憶部に記憶されているデータを示す第１の物理アドレスに変換するアドレス変換部と、
前記テーブルツリーに含まれており前記仮想アドレスを前記第１の物理アドレスに変換するために必要な第１の子テーブルが、前記セキュアテーブルツリーに含まれていない場合に、前記テーブルツリーにおける前記第１の子テーブルと前記検証子ツリーに含まれており前記第１の子テーブルに関連付けられている第１の子検証子とに基づいて検証情報を計算する検証計算部と、
前記検証情報と、前記セキュア検証子ツリーに含まれており前記第１の子テーブルを参照する第１の親テーブルに関連付けられている第１の親検証子とに基づいて、検証を行う検証部と、
前記検証の結果が正当の場合、前記第１の子テーブル及び前記第１の子検証子を前記セキュアテーブルツリー及び前記セキュア検証子ツリーに組み込む更新部と、

を具備するメモリ管理装置。
【請求項２】
前記更新部は、前記セキュアテーブルツリーが前記第１の子テーブルを含まない場合に、前記セキュアテーブルツリーの前記第１の親テーブルに含まれる前記第１の子テーブルを示すエントリを無効状態とし、前記セキュアテーブルツリーが前記第１の子テーブルを組み込んだ場合に、前記セキュアテーブルツリーの前記エントリを有効状態とする、
請求項１のメモリ管理装置。
【請求項３】
前記検証計算部は、前記セキュアテーブルツリーに含まれている前記第１の子テーブルのエントリに記憶されている前記第１の物理アドレスが前記第１の記憶部に記憶されている前記データを示す場合に、前記第１の記憶部に記憶されている前記データに基づいてデータ検証情報を計算し、
前記検証部は、前記データ検証情報と、前記セキュア検証子ツリーの前記第１の子検証子とに基づいて、データ検証を行い、
前記更新部は、前記データ検証の結果が正当の場合、前記データを前記第２の記憶部の第２の物理アドレスに記憶し、前記第１の子テーブルの前記エントリに記憶されている前記第１の物理アドレスを、前記第２の物理アドレスに更新する、
請求項１のメモリ管理装置。
【請求項４】
前記検証計算部は、前記第１の子テーブルの前記エントリに記憶されている前記第１の物理アドレスに基づいて前記データを検証するための前記データ検証情報を計算する、請求項３のメモリ管理装置。
【請求項５】
前記検証計算部は、前記第２の記憶部に記憶されている前記データを、前記第１の記憶部に記憶する場合に、前記データに基づいてデータ検証情報を計算し、
前記外部入出力部は、前記データを前記第１の記憶部の第２の物理アドレスに記憶し、
前記更新部は、前記セキュアテーブルツリーに含まれている前記第１の子テーブルのエントリに記憶されている前記第１の物理アドレスを、前記第２の物理アドレスに更新し、前記セキュア検証子ツリーに記憶されている前記第１の子検証子を、前記データ検証情報に更新する、
請求項１のメモリ管理装置。
【請求項６】
前記検証計算部は、前記第１の子テーブルの前記エントリに記憶されている前記第２の物理アドレスに基づいて前記データを検証するための前記データ検証情報を計算する、請求項５のメモリ管理装置。
【請求項７】
前記第２の記憶部から前記第１の記憶部へ記憶される前記データを暗号化し、前記第１の記憶部から前記第２の記憶部へ記憶される前記データを復号する暗号復号部、をさらに具備する
請求項１のメモリ管理装置。
【請求項８】
仮想マシンモニタ環境で動作し、
前記セキュアテーブルツリーは、前記仮想マシンモニタに制御されるゲストＯＳ（Operating System）によって参照される中間物理アドレスを前記第１の物理アドレスに変換する、
請求項１のメモリ管理装置。
【請求項９】
前記仮想マシンモニタで管理される前記セキュアテーブルツリーの一部を、前記ゲストＯＳで使用可能とするアドレス領域制限部、をさらに具備する請求項８のメモリ管理装置。

【請求項１０】
前記仮想マシンモニタで管理される前記セキュアテーブルツリーの第１の部分を、第１のゲストＯＳで使用可能とし、前記セキュアテーブルツリーの第２の部分を、第２のゲストＯＳで使用可能とするアドレス領域制限部、をさらに具備する請求項８のメモリ管理装置。
【請求項１１】
前記仮想マシンモニタは、第１及び第２のゲストＯＳを含む複数のゲストＯＳ、第１及び第２のセキュアテーブルツリーを含む複数のセキュアテーブルツリー、第１及び第２のセキュア検証子ツリーを含む複数のセキュア検証子ツリーを管理し、
前記第１のゲストＯＳの実行時に前記第１のゲストＯＳに対応付けられた前記第１のセキュアテーブルツリーと前記第１のセキュア検証子ツリーとによりアドレス変換を実現し、前記第２のゲストＯＳの実行時に前記第２のゲストＯＳに対応付けられた前記第２のセキュアテーブルツリーと前記第２のセキュア検証子ツリーとによりアドレス変換を実現する切替部をさらに具備する、請求項８のメモリ管理装置。
【請求項１２】
前記仮想マシンモニタは、複数のゲストＯＳ毎に対応付けられた複数の秘密鍵を管理し、
前記検証計算部は、前記ゲストＯＳに対応付けられた前記秘密鍵を利用して前記検証情報を計算する、
請求項８のメモリ管理装置。
【請求項１３】
前記検証計算部は、前記第２の記憶部に記憶される前記データに対しては前記中間物理アドレスを用いて前記データの検証子を計算し、前記セキュアテーブルツリーに含まれるテーブルに対しては前記テーブルの物理アドレスを用いて前記テーブルの検証子を計算する、
請求項８のメモリ管理装置。
【請求項１４】
前記セキュア検証子ツリーの最上位検証子に基づいて署名情報を生成する署名生成部と、
前記署名情報を、外部装置に送信する送信部と、
をさらに具備する請求項１乃至請求項１３のいずれか１項のメモリ管理装置。
【請求項１５】
前記検証計算部は、前記セキュアテーブルツリーと前記セキュア検証子ツリーとのうちの少なくとも一方に設定されているデータ保護方式を判断し、
前記データ保護方式が第１の方式を示す場合に、
前記検証計算部は、前記セキュアテーブルツリーに含まれている前記第１の子テーブルのエントリに記憶されている前記第１の物理アドレスが前記第１の記憶部に記憶されている前記データを示す場合に、前記第１の記憶部に記憶されている前記データに基づいてデータ検証情報を計算し、
前記検証部は、前記データ検証情報と、前記セキュア検証子ツリーの前記第１の子検証子とに基づいて、データ検証を行い、
前記更新部は、前記データ検証の結果が正当の場合、前記データを前記第２の記憶部の第２の物理アドレスに記憶し、前記第１の子テーブルの前記エントリに記憶されている前記第１の物理アドレスを、前記第２の物理アドレスに更新し、
前記アドレス変換部は、前記仮想アドレスを前記第２の物理アドレスに変換し、
前記データ保護方式が検証なしを示す場合に、
前記検証計算部は、前記データ検証情報を計算せず、
前記検証部は、前記データ検証を実行せず、
前記更新部は、前記第１の子テーブルの前記エントリに記憶されている前記第１の物理アドレスを更新せず、

前記アドレス変換部は、前記仮想アドレスを前記第１の物理アドレスに変換する、
請求項１のメモリ管理装置。
【請求項１６】
前記データ保護方式が第２の方式を示す場合に、
前記検証計算部は、前記第１の記憶部の前記データに対する複数回のデータ参照のうち前記複数回より少ない少なくとも１回に対して、前記セキュアテーブルツリーに含まれている前記第１の子テーブルのエントリに記憶されている前記第１の物理アドレスで示される前記第１の記憶部の前記データに基づいて前記データ検証情報を計算し、
前記検証部は、前記データ検証情報と、前記セキュア検証子ツリーの前記第１の子検証子とに基づいて、前記データ検証を行い、
前記アドレス変換部は、前記データ検証の結果が正当の場合、前記仮想アドレスを前記第１の物理アドレスに変換する、
請求項１５のメモリ管理装置。
【請求項１７】
前記第１の記憶部は、不揮発性メモリと揮発性メモリとを含み、
前記検証計算部は、前記セキュアテーブルツリーと前記セキュア検証子ツリーとのうちの少なくとも一方に設定されているデータ保護方式を判断し、
前記データ保護方式が第１の方式を示す場合に、
前記検証計算部は、前記セキュアテーブルツリーに含まれている前記第１の子テーブルのエントリに記憶されている前記第１の物理アドレスが前記不揮発性メモリに記憶されている前記データを示す場合に、前記不揮発性メモリに記憶されている前記データに基づいてデータ検証情報を計算し、
前記検証部は、前記データ検証情報と、前記セキュア検証子ツリーの前記第１の子検証子とに基づいて、データ検証を行い、
前記更新部は、前記データ検証の結果が正当の場合、前記データを前記第２の記憶部の第２の物理アドレスに記憶し、前記第１の子テーブルの前記エントリに記憶されている前記第１の物理アドレスを、前記第２の物理アドレスに更新し、
前記アドレス変換部は、前記仮想アドレスを前記第２の物理アドレスに変換し、
前記データ保護方式が検証なしを示す場合に、
前記検証計算部は、前記データ検証情報を計算せず、
前記検証部は、前記データ検証を実行せず、
前記更新部は、前記データを前記揮発性メモリの第３の物理アドレスに記憶し、前記第１の子テーブルの前記エントリに記憶されている前記第１の物理アドレスを、前記第３の物理アドレスに更新し、
前記アドレス変換部は、前記仮想アドレスを前記第３の物理アドレスに変換する、
請求項１のメモリ管理装置。
【請求項１８】
前記データ保護方式が第２の方式を示す場合に、
前記検証計算部は、前記第１の記憶部の前記データに対する複数回のデータ参照のうち前記複数回より少ない少なくとも１回に対して、前記セキュアテーブルツリーに含まれている前記第１の子テーブルのエントリに記憶されている前記第２のアドレスで示される前記不揮発性メモリの前記データに基づいて前記データ検証情報を計算し、
前記検証部は、前記データ検証情報と、前記セキュア検証子ツリーの前記第１の子検証子とに基づいて、前記データ検証を行い、
前記更新部は、前記データ検証の結果が正当の場合、前記データを前記揮発性メモリの第４の物理アドレスに記憶し、前記第１の子テーブルの前記エントリに記憶されている前記第１の物理アドレスを、前記第４の物理アドレスに更新し、
前記アドレス変換部は、前記仮想アドレスを前記第４の物理アドレスに変換する、
請求項１７のメモリ管理装置。
【請求項１９】

前記検証計算部は、前記第１の子テーブルと前記第１の子検証子とを暗号化せず、前記第１の子テーブルと前記第１の子検証子とに対するハッシュ値を暗号化した前記検証情報を計算する、
請求項１のメモリ管理装置。
【請求項２０】
前記検証計算部は、前記データを暗号化するとともに、前記データに対するハッシュ値を暗号化した前記データ検証情報を計算する、
請求項３のメモリ管理装置。
【請求項２１】
第１の記憶部及び安全な第２の記憶部に対する書き込み及び読み出しを行うコンピュータを、
親テーブル及び子テーブルを含むテーブルツリーと、前記親テーブルに関連付けられる親検証子及び前記子テーブルに関連付けられる子検証子を含む検証子ツリーであって、前記親検証子は前記子テーブル及び前記子検証子に対する検証に用いられる前記検証子ツリーと、を記憶する第１の記憶部に対して読み込み及び書き込みを行う外部入出力部、
前記第２の記憶部に記憶されている前記テーブルツリーの一部であるセキュアテーブルツリー及び前記検証子ツリーのうちの一部であるセキュア検証子ツリーに基づいて、仮想アドレスを前記第１の記憶部又は前記第２の記憶部に記憶されているデータを示す物理アドレスに変換するアドレス変換部、
前記テーブルツリーに含まれており前記仮想アドレスを前記物理アドレスに変換するために必要な第１の子テーブルが、前記セキュアテーブルツリーに含まれていない場合に、前記テーブルツリーにおける前記第１の子テーブルと前記検証子ツリーに含まれており前記第１の子テーブルに関連付けられている第１の子検証子とに基づいて検証情報を計算する検証計算部、
前記検証情報と、前記セキュア検証子ツリーに含まれており前記第１の子テーブルを参照する第１の親テーブルに関連付けられている第１の親検証子とに基づいて、検証を行う検証部、
前記検証の結果が正当の場合、前記第１の子テーブル及び前記第１の子検証子を前記セキュアテーブルツリー及び前記セキュア検証子ツリーに組み込む更新部、
として機能させるためのメモリ管理プログラム。
【請求項２２】
不正なアクセスから防御される安全な記憶部に記憶されているアドレス変換用のセキュアテーブルツリーに、仮想アドレスを物理アドレスに変換するために必要なテーブルが含まれていないことを検出し、
前記セキュアテーブルツリーに前記テーブルが含まれていない場合に、他の記憶部に記憶されているテーブルツリーの前記テーブルと、前記他の記憶部に記憶されており前記テーブルツリーと同一のグラフ構造を持つ検証子ツリーの第１の検証子であって前記テーブルと関連付けられている前記第１の検証子と、を読み出し、
前記テーブル及び前記第１の検証子に基づいて検証情報を計算し、
前記安全な記憶部に記憶されており前記セキュアテーブルツリーと同一のグラフ構造を持つセキュア検証子ツリーに含まれており前記テーブル及び前記第１の検証子に対する検証に用いられる第２の検証子と、前記検証情報とに基づいて、検証を行い、
前記検証の結果が正当の場合、前記テーブル及び前記第１の検証子を前記セキュアテーブルツリー及び前記セキュア検証子ツリーに組み込み、
前記セキュアテーブルツリーに基づいて、前記仮想アドレスを前記安全な記憶部又は前記他の記憶部に記憶されているデータを示す前記物理アドレスに変換する、
メモリ管理方法。
【請求項２３】
データと、それぞれが少なくとも１つのエントリを含む複数のテーブルによってツリー構造が形成され仮想アドレスから前記エントリ経由で前記データの物理アドレスを求める

ためのテーブルツリーと、前記データと前記複数のテーブルとに対する複数の検証子を含む検証子ツリーと、を記憶する不揮発性の第１の記憶部と、
前記第１の記憶部から、前記仮想アドレスを前記物理アドレスに変換するアドレス変換に必要な第１のテーブル及び前記第１のテーブルに関連する第１の検証子、を読み出す読み出し部と、
前記第１の記憶部から読み出された前記第１のテーブル及び前記第１の検証子に対して検証を行う検証部と、
前記検証の結果が正当を示す場合に、前記第１のテーブル及び前記第１の検証子を記憶する揮発性の第２の記憶部と、
前記データの参照要求を受けた場合に、前記第２の記憶部に記憶されている検証済みテーブルツリーに基づいて、前記仮想アドレスを、前記データを示す前記物理アドレスに変換するアドレス変換部と、
を具備し、
前記テーブルツリーの少なくとも一部と前記検証子ツリーとが同一のグラフ構造を有するメモリ管理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、メモリ管理装置、プログラム、及び方法に関する。
【背景技術】
【０００２】
不揮発性メモリは、情報処理装置の起動の高速化、及び、いわゆるノーマリーオフによる低消費電力化に寄与する。しかしながら、情報セキュリティの観点において、不揮発性メモリは、揮発性メモリとは異なるメモリ攻撃を受ける可能性がある。
【０００３】
例えば、揮発性メモリでは、稼動中の情報処理装置の電源が切られた場合に、揮発性メモリのデータは消える。このため、電源が切られた後に、物理的に情報処理装置内の揮発性メモリがアクセスされても、電源切断前の揮発性メモリのデータを窃視・改ざんすることは不可能である。
【０００４】
しかしながら、不揮発性メモリは、停止中であってもデータを記憶している。このため、停止中に情報処理装置から不揮発性メモリを取り出し、外部装置で不揮発性メモリのデータを窃視・改ざんし、その後不揮発性メモリを元の情報処理装置に搭載し、情報処理装置を再稼動することで、情報処理装置の動作を不正に変更することができる。このようなメモリ攻撃は、特に、野外で使用される情報処理装置、又は、不正なユーザがアクセス可能な場所に設置されている情報処理装置にとって大きな脅威となる。
【０００５】
データ改ざんの対策として、例えばハッシュ又はメッセージ認証コード（ＭＡＣ：Massage Authentication Code）などのような、様々な検証技術が存在する。一般的に、検証対象データに対するハッシュ値及びＭＡＣ値を、検証子と呼ぶ。データ改ざん検証では、検証対象データに基づいて第１のタイミングで計算された第１の検証子と、検証対象データに基づいて第２のタイミングで計算された第２の検証子とが整合するか否かで、検証対象データの改ざんが判断される。検証対象データに対する検証子が計算され、この検証子に基づいて検証が実行される場合、検証対象データ自体は改ざんされる可能性のある場所に記憶されてもよい。しかしながら、検証子及び秘密鍵は、改ざん及び参照不可能な状態で安全な場所に記憶される必要がある。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２０１２－６８９５９号公報

【特許文献２】特許第５２６００８１号公報
【特許文献３】特許第４０７４６２０号公報
【特許文献４】米国特許第４３０９５６９号明細書
【非特許文献】
【０００７】
【非特許文献１】“The AEGIS Processor Architecture for Tamper-Evident and Tamper-Resistant Processing", G. Edward Suh, Blaise Gassend, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas, Proceedings of the 17th International Conference on Supercomputing (ICS'03), pages 160-171, San Francisco, CA, June 2003
【非特許文献２】Overshadow: “A Virtualization-Based Approach to Retrofitting Protection in Commodity Operating Systems“, Xiaoxin Chen, Tal Garfinkel, E. Christopher Lewis, Pratap Subrahmanyam, Carl A. Waldspurger, Dan Boneh, Jeffrey Dwoskin, and Dan R.K. Ports, In Architectural Support for Programming Languages and Operating Systems (ASPLOS 2008)
【非特許文献３】“Accelerating Two-Dimensional PageWalks for Virtualized Systems”, Bhargava R. et. al, In Architectural Support for Programming Languages and Operating Systems (ASPLOS 2008)
【発明の概要】
【発明が解決しようとする課題】
【０００８】
本実施形態は、データの完全性を検証し、データの改ざんを防止する。
【課題を解決するための手段】
【０００９】
実施形態によれば、メモリ管理装置は、外部入出力部、アドレス変換部、検証計算部、検証部、更新部を備える。外部入出力部は、親テーブル及び子テーブルを含むテーブルツリーと、前記親テーブルに関連付けられる親検証子及び前記子テーブルに関連付けられる子検証子を含む検証子ツリーとに対して読み込み及び書き込みを行う。テーブルツリーと検証子ツリーとは、第１の記憶部に記憶されている。親検証子は子テーブル及び子検証子に対する検証に用いられる。アドレス変換部は、安全な第２の記憶部に記憶されているテーブルツリーの一部であるセキュアテーブルツリー及び検証子ツリーの一部であるセキュア検証子ツリーに基づいて、仮想アドレスを第１の記憶部又は第２の記憶部に記憶されているデータを示す物理アドレスに変換する。検証計算部は、テーブルツリーに含まれており仮想アドレスを物理アドレスに変換するために必要な第１の子テーブルが、セキュアテーブルツリーに含まれていない場合に、テーブルツリーにおける第１の子テーブルと検証子ツリーに含まれており第１の子テーブルに関連付けられている第１の子検証子とに基づいて検証情報を計算する。検証部は、検証情報と、セキュア検証子ツリーに含まれており第１の子テーブルを参照する第１の親テーブルに関連付けられた第１の親検証子とに基づいて、検証を行う。更新部は、検証の結果が正当の場合、第１の子テーブル及び第１の子検証子をセキュアテーブルツリー及びセキュア検証子ツリーに組み込む。
【図面の簡単な説明】
【００１０】
【図１】第１の実施形態に係るメモリ管理装置の構成を例示するブロック図。
【図２】第２の実施形態に係る情報処理装置のハードウェア構成を例示するブロック図。
【図３】２ステージのアドレス変換を実行する構成を例示するブロック図。
【図４】アドレス変換とデータ参照とを実行するハードウェア構成及びページテーブルツリーのデータ構造を例示するブロック図。
【図５】第２の実施形態に係る実施形態に係るブロックの定義を例示する概念図。
【図６】第２の実施形態に係る情報処理装置によるデータ取得及びアドレス変換の概念を例示するブロック図。
【図７】第２の実施形態に係るメモリマップを例示する図。

【図８】第２の実施形態に係るセキュアページテーブルツリー及びセキュア検証子ツリーのＭＡＣツリー構造を例示するデータ構造図。
【図９】第２の実施形態に係るセキュアページテーブルツリー及びセキュア検証子ツリーのＭＡＣ＋カウンタ構造を例示するデータ構造図。
【図１０】セキュアページテーブルツリーとページテーブルツリーとの関係の一例を示すデータ構造図。
【図１１】第２の実施形態に係るデータ参照処理を例示するフローチャート。
【図１２】第２の実施形態に係るアドレス解決処理を例示するフローチャート。
【図１３】第２の実施形態に係る情報処理装置の構成を例示するブロック図。
【図１４】第２の実施形態に係る検証処理を例示するフローチャート。
【図１５】第２の実施形態に係る置き換え処理を例示するフローチャート。
【図１６】第２の実施形態に係る追い出し処理を例示するフローチャート。
【図１７】特定のアーキテクチャのテーブルエントリ構造を例示するデータ構造図。
【図１８】ＨＡＰフィールドの仕様を例示するテーブル。
【図１９】特定のアーキテクチャにおいてデータ参照要求が発生した場合のアドレス解決処理を例示するフローチャート。
【図２０】第３の実施形態に係るページテーブルツリー及び検証子ツリーに関する仮想アドレス領域の第１の制限形態を例示するブロック図。
【図２１】第３の実施形態に係るページテーブルツリー及び検証子ツリーに関する仮想アドレス領域の第２の制限形態を例示するブロック図。
【図２２】アドレスマップと物理アドレス領域との関係を例示するブロック図。
【図２３】ゲストＯＳのステージ２ページテーブルツリーを例示するデータ構造図。
【図２４】第４の実施形態に係るデータの検証、読み込み、アクセス制御を例示するフローチャート。
【図２５】第６の実施形態に係るゲストＯＳごとのページテーブルツリーを例示するデータ構造図。
【図２６】第６の実施形態に係る情報処理装置の構成を例示するブロック図。
【図２７】第６の実施形態に係る情報処理装置の検証処理を例示するフローチャート。
【図２８】第６の実施形態に係る情報処理装置の追い出し処理を例示するフローチャート。
【図２９】第６の実施形態に係るＯＳ切り替え処理を例示するフローチャート。
【図３０】第７の実施形態に係る情報処理システムを例示するシステム構成図。
【図３１】第７の実施形態に係る情報処理システムの構成を例示するブロック図。
【図３２】第７実施形態に係る情報処理システムのフォレンジック処理を例示するフローチャート。
【図３３】第８の実施形態に係るページテーブルエントリのフィールド形式を例示するデータ構造図。
【図３４】第８の実施形態に係る、データ保護方式ごとのデータのコピー状態及び検証状態を例示する状態遷移図。
【図３５】複数のデータ保護方式におけるページテーブルエントリの制御フィールドの状態、ページテーブルエントリが有効か否かを示す有効／無効フラグ、次回参照データの状態、次回参照データの状態を示す符号、の関係を例示する図。
【図３６】第８の実施形態に係る複数のデータ保護方式に対応する検証処理を例示するフローチャート。
【図３７】内部メモリのデータに対する検証の処理を例示するフローチャート。
【図３８】外部メモリのデータに対する検証の処理を例示するフローチャート。
【図３９】第８の実施形態に係る電源断前処理を例示するフローチャート。
【図４０】第８の実施形態に係る１回検証が設定されているデータの更新処理を例示するフローチャート。
【図４１】第８の実施形態に係る外部メモリに格納されているデータに対する更新処理の

一例を示すフローチャート。
【図４２】第８の実施形態に係るメモリ管理装置の構成を例示するブロック図。
【図４３】第９の実施形態に係る情報処理装置のハードウェア構成を例示するブロック図。
【図４４】第９の実施形態に係るページテーブルエントリのフィールド形式を例示するデータ構造図。
【図４５】第９の実施形態に係る、データ保護方式ごとのデータのコピー状態及び検証状態を例示する状態遷移図。
【図４６】複数のデータ保護方式におけるページテーブルエントリのデータ保護方式フィールドの状態、Ｄ／Ｆフラグ、有効／無効フラグ、次回参照データの状態、次回参照データの状態を示す符号、の関係を例示する図。
【図４７】第９の実施形態に係るアドレス解決処理の例示するフローチャート。
【図４８】第９の実施形態に係る複数のデータ保護方式に対応する検証転送処理の一例を示すフローチャート。
【図４９】第９の実施形態に係る稼働中の内部メモリから揮発性メモリへの追い出し処理を例示するフローチャート。
【図５０】第９の実施形態に係る電源断前処理を例示するフローチャート。
【図５１】第９の実施形態に係る揮発性メモリから不揮発性メモリへの追い出し処理を例示するフローチャート。
【図５２】XTS-AESを例示する概念図。
【図５３】第１０の実施形態に係るTweakとSequence Numberの例を示す図。
【図５４】ページテーブルに対する暗号化保護なしの場合のＭＡＣ値計算及び検証処理を例示する概念図。
【図５５】ページデータに対する暗号化保護ありの場合のＭＡＣ値計算及び検証処理を例示する概念図。
【発明を実施するための形態】
【００１１】
以下、図面を参照しながら本発明の各実施の形態について説明する。なお、以下の説明において、略又は実質的に同一の機能及び構成要素については、同一符号を付し、必要に応じて説明を行う。
【００１２】
［第１の実施形態］
本実施形態は、データの完全性を検証し、データの改ざんを防止するメモリ管理装置について説明する。
【００１３】
図１は、本実施形態に係るメモリ管理装置の構成を例示するブロック図である。メモリ管理装置１の各種の構成要素は、ハードウェアで実現されてもよく、プログラムによって制御されるプロセッサによって実現されてもよい。
【００１４】
メモリ管理装置１は、外部入出力部２、アドレス変換部３、検証計算部４、検証部５、更新部６、置換管理部２０を備える。
【００１５】
また、メモリ管理装置１は、第１の記憶部である外部メモリ７と、第２の記憶部である内部メモリ８とに対して、読み込み及び書き込みを行う。
【００１６】
外部メモリ７は、例えば、不揮発性の記憶装置である。例えば、外部メモリ７は、ＮＡＮＤ型フラッシュメモリ、ＮＯＲ型フラッシュメモリ、ＭＲＡＭ（Magnetoresistive Random access memory：磁気抵抗メモリ）、ＰＲＡＭ（Phase change Random access memory：相変化メモリ）、ＲｅＲＡＭ（Resistive Random access memory：抵抗変化型メモリ）、ＦｅＲＡＭ（Ferroelectric Random Access Memory）などの不揮発性半導体メモリでも

よい。外部メモリ７は、主記憶装置として用いられてもよく、ハードディスク、ＳＳＤ（Solid State Drive）などのような補助記憶装置として用いられてもよい。

【００１７】

外部メモリ７は、階層構造を持つページテーブルツリー９と、階層構造を持つ検証子ツリー１０とを記憶する。本実施形態において、ページテーブルツリー９と検証子ツリー１０とは、２段の階層を持つ。しかしながら、ページテーブルツリー９と検証子ツリー１０とは当然に３段以上でもよい。

【００１８】

ページテーブルツリー９は、複数のページテーブルの階層構成で形成される。ページテーブルツリー９は、仮想アドレスを物理アドレスに変換するための親テーブル１０１及び子テーブル２０１～２０ｍを含む。テーブルエントリＥがアドレス情報Ｘを備えており、アドレス情報Ｘが最終のデータＤのアクセス先を決定するための中間のテーブルＴ又はデータＤを指している場合、テーブルエントリＥは、テーブルＴ又はデータＤを参照しているという。テーブルエントリＥの参照先アドレスは、アドレス情報Ｘである。テーブルＴ又はデータＤの参照元は、テーブルエントリＥである。親テーブル１０１に含まれる親エントリｐｅ１～ｐｅｍは、子テーブル２０１～２０ｍを参照するために用いられる。子テーブル２０１～２０ｍに含まれる子エントリｃｅ１～ｃｅｘは、データ３０１～３０ｘを参照するために用いられる。

【００１９】

本実施形態では、典型的な例として、ページテーブルツリー９において、親テーブル１０１の親エントリｐｅ１、子テーブル２０１の子エントリｃｅ１を経由して、データ３０１がアクセスされる場合を説明する。しかしながら、他の親テーブル、他の親エントリ、他の子テーブル、他の子エントリを経由して他のデータがアクセスされる場合も同様である。

【００２０】

検証子ツリー１０は、親検証子ｐｖ１～ｐｖｍ及び子検証子ｃｖ１～ｃｖｘを含む階層構造を持つ。親検証子ｐｖ１～ｐｖｍは、親テーブル１０１に関連付けられる。子検証子ｃｖ１～ｃｖｎは、子テーブル２０１に関連付けられる。他の子検証子と他の子テーブルとの関係についても、子検証子ｃｖ１～ｃｖｎと子テーブル２０１との関係と同様である。

【００２１】

本実施形態において、子テーブル２０１と関連付けられている子検証子ｃｖ１～ｃｖｎは、それぞれ、子テーブル２０１に含まれている子エントリｃｅ１～ｃｅｎによって参照されるデータ３０１～３０ｎに対する検証に用いられる。

【００２２】

親テーブル１０１と関連付けられている親検証子ｐｖ１は、親テーブル２０１に含まれている親エントリｐｅ１によって参照される子テーブル２０１と、子テーブル２０１と関連付けられている子検証子ｃｖ１～ｃｖｎとに対する検証に用いられる。他の親検証子と他の子テーブル及び他の子検証子との関係についても、親検証子ｐｖ１と子テーブル２０１及び子検証子ｃｖ１～ｃｖｎとの関係と同様である。

【００２３】

内部メモリ８は、外部から直接参照不可能な記憶装置であり、不正なアクセスから防御される。例えば、内部メモリ８は、プロセッサパッケージ内部の記憶装置である。具体的には、内部メモリ８は、例えば、下記の第２の実施形態で説明される図２で、プロセッサ６６のパッケージと一体化したハードウェアであり、内部バス５４ｂを経由して外部バス４４との間でデータ転送が行われるが、データ転送はプロセッサ６６の命令実行ユニット４５で実行された命令に基づいて行われる。内部メモリ８の内容は、外部バス４４を経由して直接読み出し及び書き換えることはできないことを前提とする。このような内部メモリ８と同様の特徴を持つメモリを、安全なメモリと呼ぶ。これとは逆に、外部メモリ７は、外部バス４４を経由して任意のアドレスに対して読み出し及び書き換えが可能であり、

安全なメモリとは異なる。

【００２４】

内部メモリ８は、外部メモリ７と同じ物理アドレス空間に配置される。内部メモリ８は、命令実行ユニット４５で実行されるソフトウェアから外部メモリ７と同様にアクセス可能である。

【００２５】

内部メモリ８は、ページテーブルツリー９の一部であるセキュアページテーブルツリー１２１、検証子ツリー１０のうちの一部であるセキュア検証子ツリー１２２を記憶する。内部メモリ８は、親テーブル１０１と親検証子ｐｖ１～ｐｖｍとの検証に用いられるルート検証情報１３を備える。

【００２６】

アドレス変換部３は、内部メモリ８に記憶されている親テーブル１０１の親エントリｐｅ１～ｐｅｍ及び子テーブル２０１～２０ｍの子エントリｃｅ１～ｃｅｘを経由してデータ３０１～３０ｘの物理アドレスを求める。

【００２７】

外部メモリ７から内部メモリ８へ親テーブル１０１がコピー（移動又は読み込み）される場合には、この親テーブル１０１に関連付けられている親検証子ｐｖ１～ｐｖｍも、外部メモリ７から内部メモリ８へコピーされる。

【００２８】

本実施形態において、ページテーブル又はデータは、外部メモリ７から、改ざんに対して安全な内部メモリ８にコピーされ、検証される。内部メモリ８のページテーブル又はデータが変更され、その後内部メモリ８から削除される場合には、変更された内部メモリ８のページテーブル又はデータは、外部メモリ７に書き出される。内部メモリ８のページテーブル又はデータが変更されることなく内部メモリ８から削除される場合には、内部メモリ８のページテーブル又はデータは、書き出されてもよく又はそのまま破棄されもよい。以下において、外部メモリ７と内部メモリ８との間でのページテーブル又はデータのコピーを、ページテーブル又はデータを移動する、読み込む、又は書き出す、と表現する場合がある。例えば、ページテーブルの参照先が内部メモリ８にコピーされたページテーブル又はデータに変更されることを、ページテーブル又はデータの移動又は読み込み、と表現する場合がある。この場合に、外部メモリ７のコピー元のページテーブル又はデータは、消去されなくてもよい。

【００２９】

外部メモリ７から内部メモリ８へ子テーブル２０１がコピーされる場合には、この子テーブル２０１に関連付けられている子検証子ｃｖ１～ｃｖｎも、外部メモリ７から内部メモリ８へコピーされる。

【００３０】

外部入出力部２は、外部メモリ７に記憶されているページテーブルツリー９と検証子ツリー１０とに対する読み込み及び書き込みを行う。

【００３１】

第１に、外部メモリ７から内部メモリ８へ子テーブル２０１及び子検証子ｃｖ１～ｃｖｎがコピーされる場合の例を説明する。

【００３２】

アドレス変換部３は、内部メモリ８に記憶されているセキュアページテーブルツリー１２１に基づいて、仮想アドレスを物理アドレスに変換する。また、アドレス変換部３は、仮想アドレスを物理アドレスに変換するために必要な子テーブル２０１がセキュアページテーブルツリー１２１に含まれていない場合に、テーブル不足通知（フォールト）１４を検証計算部４に送り、更新された後のセキュアページテーブルツリー１２１に基づいて、仮想アドレスを物理アドレスに変換する。

【００３３】

検証計算部４は、テーブル不足通知１４をアドレス変換部３から受けた場合に、外部入

出力部２経由で、外部メモリ７のページテーブルツリー９の子テーブル２０１と検証子ツリー１０の子検証子ｃｖ１～ｃｖｎとを読み込み、読み込まれた子テーブル２０１と子検証子ｃｖ１～ｃｖｎとに基づいて検証情報１５を計算し、検証情報１５を検証部５に送る。

【００３４】

検証部５は、検証計算部４によって計算された検証情報１５と、セキュアページテーブルツリー１２１において参照元エントリｐｅ１を含んでいる親テーブル１０１に関連付けられている親検証子ｐｖ１とに基づいて、検証情報１５と親検証子ｐｖ１とが整合するか否か判断し、検証を行い、検証結果１６を更新部６に送る。

【００３５】

更新部６は、検証部５から検証結果１６を受け、検証結果１６が正当の場合、内部メモリ８のセキュアページテーブルツリー１２１に子テーブル２０１を組み込み、セキュア検証子ツリー１２２に子検証子ｃｖ１～ｃｖｎを組み込む。より具体的には、更新前に、親テーブル１０１の親エントリｐｅ１は、外部メモリ７のページテーブルツリー９に含まれている子テーブル２０１を参照しているとする。更新部６は、セキュアページテーブルツリー１２１における更新前の親テーブル１０１の親エントリｐｅ１を、内部メモリ８におけるセキュアページテーブルツリー１２１に組み込まれた子テーブル２０１を参照するように、更新する。

【００３６】

本実施形態に係るメモリ管理装置１では、例えば、検証結果１６の確認に先立って、外部入出力部２が、内部メモリ８に子テーブル２０１及び子検証子ｃｖ１～ｃｖｎを読み込み、検証結果１６が正当な場合に、セキュアページテーブルツリー１２１及びセキュア検証子ツリー１２２に、子テーブル２０１及び子検証子ｃｖ１～ｃｖを組み込むとしてもよい。

【００３７】

このように、本実施形態において、子テーブル２０１が内部メモリ８に記憶されておらず、外部メモリ７から内部メモリ８へ子テーブル２０１及び子検証子ｃｖ１～ｃｖｎがコピーされる場合には、親テーブル１０１の親エントリｐｅ１は、外部メモリ７の子テーブル２０１を参照する。子テーブル２０１が内部メモリ８に記憶された場合には、内部メモリ８の親テーブル１０１の親エントリｐｅ１は、内部メモリ８の子テーブル２０１を参照するように更新される。

【００３８】

本実施形態において、親テーブル１０１が内部メモリ８に記憶されておらず、外部メモリ７から内部メモリ８へ親テーブル１０１及び親検証子ｐｖ１～ｐｖｎがコピーされる場合には、検証計算部４は、外部メモリ７から読み込まれた親テーブル１０１、親検証子ｐｖ１～ｐｖｎ、外部メモリ７の親テーブル１０１の記憶されている物理アドレスに基づいて検証情報を生成する。外部メモリ７における親テーブル１０１の物理アドレスを用いて検証情報を生成することにより、親テーブル１０１の入れ替え攻撃に対して防御することができる。検証部５は、ルート検証情報１３と生成された検証情報に基づいて検証を行う。更新部６は、検証結果が正当の場合に、セキュアページテーブルツリー１２１に、外部メモリ７から読み込まれた親テーブル１０１を組み込み、セキュア検証子ツリー１２２に、外部メモリ７から読み込まれた親検証子ｐｖ１～ｐｖｎを組み込む。

【００３９】

第２に、外部メモリ７から内部メモリ８へデータ３０１がコピーされる場合の例を説明する。

【００４０】

アドレス変換部３は、仮想アドレスを変換した物理アドレスが外部メモリ７を参照している場合に、データ読み込み通知１７を検証計算部４及び置換管理部２０に送る。

【００４１】

例えば、アドレス変換部３は、データ参照先が外部メモリ７か否かを判断することなく

、参照データの内部メモリ８への読み込み状態を予めページテーブル内の有効／無効フラグにより管理し、データ参照先の判断を高速化してもよい。内部メモリ８に記憶されているデータを参照するセキュアページテーブルツリー１２１のテーブルエントリには、有効フラグがセットされる。外部メモリ７に記憶されているデータを参照するセキュアページテーブルツリー１２１のテーブルエントリには、無効フラグがセットされる。アドレス変換部３は、アドレス変換のページフォールトが発生した場合に、外部メモリ７のページテーブル又はデータを、内部メモリ８にコピーする。アドレス変換部３は、参照されるデータが内部メモリ８に記憶されている場合、ページフォールトを発生することなく、高速にデータを参照することができる。

【００４２】

検証計算部４は、データ読み込み通知１７をアドレス変換部３から受けた場合に、外部入出力部２経由で物理アドレスによって参照される外部メモリ７のデータ３０１を読み込み、読み込まれたデータ３０１、外部メモリ７のデータ３０１の記憶されている物理アドレスに基づいてデータ検証情報１８を計算し、データ検証情報１８を検証部５に送る。外部メモリ７におけるデータの物理アドレスを用いてデータ検証情報１８を生成することにより、データ３０１の入れ替え攻撃に対して防御することができる。

【００４３】

検証部５は、検証計算部４によって計算されたデータ検証情報１８と、セキュアページテーブルツリー１２１において参照元の子テーブル２０１に関連付けられている子検証子ｃｖ１とに基づいて、データ検証情報１８と子検証子ｃｖ１とが整合するか否か判断するデータ検証を行い、データ検証結果１９を更新部６に送る。

【００４４】

更新部６は、検証部５からデータ検証結果１９を受け、データ検証結果１９が正当の場合、内部メモリ８のセキュアページテーブルツリー１２１に、データ３０１を組み込む。より具体的には、更新前に、子テーブル２０１の子エントリｃｅ１は、外部メモリ７のページテーブルツリー９に含まれているデータ３０１を参照しているとする。更新部６は、セキュアページテーブルツリー１２１における更新前の子テーブル２０１の子エントリｃｅ１を、内部メモリ８におけるデータ３０１を参照するように更新する。

【００４５】

本実施形態に係るメモリ管理装置１では、例えば、データ検証結果１９の確認に先立って、外部入出力部２が、内部メモリ８にデータ３０１を読み込んでおき、データ検証結果１９が正当な場合に、セキュアページテーブルツリー１２１に、データ３０１を組み込むとしてもよい。

【００４６】

このように、本実施形態において、データ３０１が内部メモリ８に記憶されておらず、外部メモリ７から内部メモリ８へデータ３０１がコピーされる場合には、子テーブル２０１の子エントリｃｅ１は、外部メモリ７のデータ３０１を参照する。データ３０１が内部メモリ８に記憶された場合には、内部メモリ８の子テーブル２０１の子エントリｃｅ１は、内部メモリ８のデータ３０１を参照するように更新される。

【００４７】

仮想アドレスは、親テーブル１０１の親エントリｐｅ１、子テーブル２０１の子エントリｃｅ１を経由してデータ３０１の物理アドレスに変換される。参照されるデータ３０１は、物理アドレスの示す安全な内部メモリ８に記憶されている。このようなアドレス解決により参照される全てのテーブルとデータは、検証で正当と判断されており、安全な内部メモリ８に配置されている。

【００４８】

第３に、内部メモリ８から外部メモリ７へデータ３０１がコピー（書き出し）される場合の例を説明する。

【００４９】

検証計算部４は、内部メモリ８に記憶されているデータ３０１を外部メモリ７に記憶す

る場合に、内部メモリ８のデータ３０１に基づいて子検証子（データ検証情報）ｃｖ１を計算する。

【００５０】

外部入出力部２は、データ３０１を外部メモリ７に記憶する。

【００５１】

更新部６は、セキュアページテーブルツリー１２１における子テーブル２０１の子エントリ（物理アドレス）ｃｅ１の参照先を、外部メモリ７におけるデータ３０１の記憶位置に更新する。さらに、更新部６は、検証計算部４によって計算された子検証子ｃｖ１を、セキュアページテーブルツリー１２１における子テーブル２０１に関連付けてセキュア検証子ツリー１２２に組み込む。例えば、更新部６は、内部メモリ８のデータ３０１がセキュアページテーブルツリー１２１から参照されていない場合に、子テーブル２０１の子エントリｃｅ１を無効状態とする。次に、データ３０１が参照されたときはページフォールトが発生し、上記の処理にしたがって外部メモリ７のデータ３０１の検証と内部メモリ８へのコピーが行われる。

【００５２】

本実施形態において、更新部６は、セキュアページテーブルツリー１２１が子テーブル２０１を含まない場合に、親テーブル１０１の親エントリｐｅ１を無効状態とし、セキュアページテーブルツリー１２１が子テーブル２０１を組み込んだ場合に、親テーブル１０１の親エントリｐｅ１を有効状態とする。

【００５３】

更新部６は、内部メモリ８がデータ３０１を記憶していない場合に、子テーブル２０１の子エントリｃｅ１を無効状態とし、内部メモリ８がデータ３０１を記憶している場合に、子テーブル２０１の子エントリｃｅ１を有効状態とする。

【００５４】

上記第１及び第２の例において、置換管理部２０は、例えばアドレス変換部３からデータ読み込み通知１７を受けた場合などのように、内部メモリ８にテーブル又はデータが記憶される場合に、内部メモリ８の空き領域の容量を確認する。置換管理部２０は、内部メモリ８の空き領域の容量が不足する場合に、削除するために選択された内部メモリ８のテーブル又はデータに対する検証情報要求２１を検証計算部４に送る。置換管理部２０は、検証計算部４から、検証情報要求２１の応答として、内部メモリ８の選択されたテーブル又はデータに対する検証子を受ける。そして、置換管理部２０は、内部メモリ８の選択されたテーブル又はデータ及びその検証子を、外部入出力部２経由で外部メモリ７に書き出し、内部メモリ８における選択されたテーブル又はデータの領域を解放し、内部メモリ８の空き領域を増やす。

【００５５】

以上説明した本実施形態においては、外部メモリ７に記憶されたページテーブルツリー９、検証子ツリー１０、データ３０１～３０ｘのうちの必要な部分を選択的に検証することができ、検証された必要な部分を外部メモリ７よりも小容量の内部メモリ８に記憶することができる。これにより、外部メモリ７に対する物理攻撃を検出することができ、データの完全性を検証し、データの改ざんを防止することができる。本実施形態においては、改ざん検証後にページテーブルツリー９、検証子ツリー１０及びデータ３０１～３０ｘが改ざんされたことを検出することができ、情報処理装置の安全性を向上させることができる。

【００５６】

本実施形態に係る検証は、仮想化技術に対して適用され、内部メモリ８に記憶されたセキュアページテーブルツリー１２１、セキュア検証子ツリー１２２を参照することにより、ゲストＯＳ（Operating System）及びアプリケーションを変更することなく容易に適用することができる。

【００５７】

本実施形態においては、ページテーブルと検証子との階層構造が合致しており、さらに

、ページテーブルと検証子とが一体で検証される。換言すれば、ページテーブルツリー９と検証子ツリー１０とは同じグラフ構造を持つ。これにより、検証子がページング対象の場合であっても、検証子の配置先アドレスを解決する必要がない。また、ページテーブルと検証子とを階層構造で管理する。したがって、セキュアページテーブルツリー１２１、セキュア検証子ツリー１２２、ページテーブルツリー９、検証子ツリー１０をアドレス空間の不連続なメモリ領域に配置することができ、メモリを効率的に利用することができる。本実施形態においては、検証子を階層構造で管理することにより、効率的に管理することができる。

【００５８】

本実施形態においては、未検証のページテーブル及びデータが、既存のアドレス変換機構のページフォールトにより検出される。このため、新たなハードウェアを加える必要がない。さらに、本実施形態においては、外部メモリ７と内部メモリ８との間で、ページテーブルと検証子とが個別ではなく一体でコピーされる。したがって、ページフォールトが発生した場合であってもオーバーヘッドが増加することを抑制することができる。

【００５９】

本実施形態においては、ページテーブル及びデータが内部メモリ８に記憶されているか否かを、上位のページテーブルのエントリが有効か無効かで管理する。これにより、汎用のハードウェアであるアドレス変換機構を利用して効率よく、ページテーブル及びデータが内部メモリ８に記憶されているか否かを判断することができる。

【００６０】

［第２の実施形態］

本実施形態においては、上記第１の実施形態で説明したメモリ管理装置１を備える情報処理装置を詳細に説明する。情報処理装置は、コンピュータシステムでもよい。

【００６１】

図２は、本実施形態に係る情報処理装置を例示するハードウェア構成図である。

【００６２】

情報処理装置６５は、プロセッサ６６、外部メモリ７、外部デバイス４３、外部バス４４を備える。プロセッサ６６、外部メモリ７、外部デバイス４３は、外部バス４４を介して、データ、信号、命令を互いに送受信可能とする。

【００６３】

情報処理装置６５の仮想化支援機構は、例えば、２ステージのアドレス変換を実行する。

【００６４】

プロセッサ６６は、命令実行ユニット（プロセッサコア）４５、ＭＭＵ（Memory Management Unit）４６、１次キャッシュメモリ４７ａ，４７ｂ、２次キャッシュメモリ４８、１次アドレス変換キャッシュ（ＴＬＢ：Translation Lookaside Buffer）４９、２次アドレス変換キャッシュ５０、内部メモリ８、セキュアＤＭＡ（Direct Memory Access）コントローラ５２、入出力デバイス５３、鍵保存ユニット６７、内部バス５４ａ，５４ｂを備える。プロセッサ６６の各種の構成要素８，４５～５３，６７は、内部バス５４ａ，５４ｂを介して、データ、信号、命令を互いに送受信可能とする。

【００６５】

外部メモリ７は、セキュアＶＭＭ（Virtual Machine Monitor）６８、セキュアＯＳ５６、非セキュアＯＳ５７を記憶する。

【００６６】

本実施形態において、セキュアＯＳ５６、非セキュアＯＳ５７は、セキュアＶＭＭ６８によって管理されるゲストＯＳとする。

【００６７】

外部デバイス４３は、例えばハードディスクなどのような不揮発性記憶装置である。

【００６８】

プロセッサ６６の命令実行ユニット４５は、階層化された１次キャッシュメモリ４７ａ

，４７ｂ、２次キャッシュメモリ４８を用いてデータ参照を行う。以下では、まず、アドレス変換の後に行われるデータ参照について説明し、次に、アドレス変換について説明する。

【００６９】

１次キャッシュメモリ４７ａは、データ用の１次キャッシュメモリである。１次キャッシュメモリ４７ｂは、データ及び命令用の１次キャッシュメモリである。２次キャッシュメモリ４８は、データ及び命令用の２次統合キャッシュメモリである。

【００７０】

命令実行ユニット４５は、２次キャッシュメモリ４８に記憶されているデータ又は命令を、内部メモリ８又は外部メモリ７に記憶されているデータ又は命令よりも高速に参照可能である。また、命令実行ユニット４５は、１次キャッシュメモリ４７ａ，４７ｂを、２次キャッシュメモリ４８よりも高速にアクセス可能である。

【００７１】

命令実行ユニット４５は、１次キャッシュメモリ４７ａ，４７ｂ、２次キャッシュメモリ４８又は内部メモリ８からデータ又は命令を読み込み、処理を実行する。

【００７２】

１次キャッシュメモリ４７ａ，４７ｂが参照対象データを記憶している場合には、２次キャッシュメモリ４８、及び、内部メモリ８へのデータ参照は実行されない。

【００７３】

キャッシュメモリ４７ａ，４７ｂが参照対象データを記憶しておらず、２次キャッシュメモリ４８が参照対象データを記憶している場合には、内部メモリ８へのデータ参照は実行されない。これにより、データ参照が短時間で行われる。

【００７４】

なお、内部メモリ８から読み込まれるデータは、内部メモリ８から、２次キャッシュメモリ４８を経由することなく、１次キャッシュメモリ４７ａ，４７ｂに記憶されてもよい。

【００７５】

鍵保存ユニット６７は、ルート検証情報１３と、情報処理装置６５における暗号化又は検証に使用される鍵情報とを記憶する。

【００７６】

セキュアＤＭＡコントローラ５２は、各種の構成要素間のデータ転送を行う。セキュアＤＭＡコントローラ５２は、例えば、ハードウェアによって実装され、ＭＡＣ値計算を実行する。しかしながら、ＭＡＣ値計算は、ソフトウェアで実行されてもよい。

【００７７】

情報処理装置６５は、仮想記憶管理とメモリ検証処理とを連携させる。本実施形態では、主記憶装置に不揮発性半導体メモリを使用する。本実施形態では、階層構造を持つページテーブルツリー９と階層構造を持つ検証子ツリー１０とを生成する。ページテーブルツリー９と検証子ツリー１０とは、互いに階層構造が整合する。ページテーブルツリー９と検証子ツリー１０とは、不揮発性の外部メモリ７に保存され、必要に応じて一部が内部メモリ８に記憶される。外部メモリ７は不揮発性の記憶装置であるため、電源がＯＦＦされ、その後に電源がＯＮされた場合に、電源ＯＦＦ前の記憶状態を維持する。

【００７８】

例えば、ＣＰＵ（Central Processing Unit）、ＭＰＵ（Micro-Processing Unit）などのようなプロセッサのパッケージと主記憶装置とを一体化した一体型ハードウェアでは、上述したようなデータの窃視・改ざん、及び、物理的攻撃が困難である。しかしながら、一体型ハードウェアは一般に高価であるため、汎用プロセッサパッケージと汎用メモリとの組み合わせで、安全な処理を可能にする技術が求められる。

【００７９】

本実施形態においては、プロセッサ６６のパッケージ内部に設けられた内部メモリ８は、ハードウェア的な攻撃から安全であると仮定する。ただし、不正なソフトウェアを実行

させることで、内部メモリ８からデータを出力させる攻撃は可能であると仮定する。情報処理装置６５への攻撃者は、任意のタイミングで外部メモリ７の任意の位置を自由に書き換えることができると仮定する。

【００８０】

本実施形態において、データ改ざんから保護されるメモリ領域、及び、暗号化されるメモリ領域を、保護メモリと呼ぶ。

【００８１】

情報処理装置６５の主記憶装置に対する攻撃を防ぎ、脅威を取り除くために、安全性とシステム構成との観点から、以下の第１乃至第５の条件を満たすことが要求される。

【００８２】

第１の条件は、安全性に関する条件である。第１の条件では、リプレイ攻撃を含むデータの改ざんを厳密に検出可能であることが要求される。

【００８３】

第２の条件は、ハードウェア構成に関する条件である。第２の条件は、専用のハードウェアが不要であることを要求する。より具体的に説明すると、第２の条件は、メモリ改ざん検証専用のハードウェアが不要であることを要求する。第２の条件は、多数のプロセッサが備えるアドレス変換機構、仮想化支援機構、プロセッサ内の汎用内部メモリ、高速化補助機構、ＤＭＡコントローラと連携した高速暗号エンジンに基づいて、攻撃を防ぎ、脅威を取り除くことを要求する。また、第２の条件は、ファームウェアなどのソフトウェアに基づく処理が可能であることを要求する。さらに、第２の条件は、仮想化技術との親和性が高いことを要求する。第２の条件は、安全な内部メモリ８のメモリサイズが１メガバイト程度のように小さくても動作可能であることを要求する。

【００８４】

第３の条件は、メモリに関する条件である。第３の条件は、大容量のメモリ、例えば３２ビットのアドレス空間もしくはそれを越えるサイズのメモリに適用可能であることを要求する。第３の条件は、メモリの検証対象領域が選択可能なことを要求する。第３の条件は、保護対象のメモリ領域をメモリマップ上でいくつもの不連続な領域に配置可能であり、メモリの必要な部分だけを選択的に改ざん検証の対象にできることを要求する。第３の条件は、メモリのうち選択的に改ざん検証対象に定められた選択領域を定義するデータそのものも、攻撃から保護可能であることを要求する。第３の条件は、保護対象のメモリ領域の配置が不連続の場合であっても、選択領域だけを検証可能なことに加えて、選択領域を除く他の領域に対して検証子用のメモリ領域の確保を不要とし、メモリを効率的に利用可能なことを要求する。

【００８５】

第４の条件は、ソフトウェア構成と安全性とに関する条件である。第４の条件は、ＯＳ全体を保護対象とすることができることを要求する。第４の条件は、改ざん検証が不要な外部との通信用ハードウェアなどは改ざん検証対象とせず非選択領域とすることができることを要求する。第４の条件は、透過性を有すること、換言すれば、ＯＳ及びアプリケーションを修正する必要がないことを要求する。第４の条件は、ＯＳに不具合があって不正な命令が実行された場合に、当該ＯＳ自身が破壊され誤動作することは許容してもその誤動作によってメモリ改ざん検証機能が検証の迂回又は制御情報の破壊に対して安全であり頑健であることを要求する。

【００８６】

第５の条件は、処理の効率性に関する条件である。第５の条件は、例えばメモリアクセスごとの改ざん検証の要・不要の判定などのような頻繁に発生する処理はできる限りハードウェアにより実行することで効率化することを要求する。

【００８７】

本実施形態においては、不揮発性の主記憶装置が適用されることを想定し、セキュア検証子ツリー１２２に基づく検証を行い、セキュアページテーブルツリー１２１に基づいて多段階のアドレス変換を行い、仮想化技術を想定し、上記の第１乃至第５の条件を満たす

情報処理装置６５を実現する。

【００８８】

本実施形態には、主要なポイントが２つある。まず、本実施形態の第１のポイントを説明する。

【００８９】

第１のポイントは、アドレス透過性の担保、未検証データ参照の検出機能の提供に関する。具体的には、ゲストＯＳによるデータ参照が発生した場合に、まずセキュアＶＭＭ６８がページテーブルエントリを確認し、内部メモリ８を経由した検証が必要な場合に、外部メモリ７のデータを内部メモリ８に動的に確保されているバッファメモリに記憶する。

【００９０】

内部メモリ８を経由した検証に成功した場合に、ゲストＯＳのデータ参照先の実態である物理メモリのデータが、本来の外部メモリ７のデータから、内部メモリ８の配置先アドレスのデータに代わるように、セキュアＶＭＭ６８が、管理されているセキュアページテーブルツリー１２１（例えばステージ２ページテーブルツリー）を書き換える。

【００９１】

ゲストＯＳは、参照先の変更を認識する必要がない。このため、本実施形態に係る検証を導入してもゲストＯＳを変更する必要はなく、ゲストＯＳの透過性を得ることができる。

【００９２】

なお、内部メモリ８の書き込み単位はページだが、書き込み単位を小さくしてキャッシュメモリを含むプロセッサ６６全体のメモリ利用効率を向上させるために、外部メモリ７から、１次キャッシュメモリ４７ａ，４７ｂ、２次キャッシュメモリ４８を経由して、命令実行ユニット４５がデータを取得する場合には、ページテーブルエントリの参照先を変更することなく、外部メモリ７から１次キャッシュメモリ４７ａ，４７ｂ、２次キャッシュメモリ４８へデータがコピーされる際に、検証が行われてもよい。この場合、キャッシュメモリからの読み込みと検証処理とを連動させるハードウェア機構が必要となる。

【００９３】

改ざん防止には、外部メモリ７への参照の検出と、検証の実行と、そして検証済みデータの安全な内部メモリ８へのコピー（読み込み）と、参照先の変更とが必要である。ハードウェアキャッシュが用いられる場合には、２次キャッシュメモリ４８への読み込みに対応する参照先変更がソフトウェアの介在なしに専用ハードウェア機構によって行われるため、ゲストＯＳに対するアドレス透過性が保証される。これに対して、ファームウェアによる検証では、検証済みデータの配置先は元のデータのアドレスと異なるため、ゲストＯＳから何らかの方法で参照先の変更を隠ぺいしなければ、ゲストＯＳの変更が必要となり、ゲストＯＳに対するアドレス透過性が担保されない。

【００９４】

本実施形態は、検証済みデータを改ざんなどの攻撃から守り、かつ、内部メモリ８へのコピーをゲストＯＳから隠蔽するために、２段階のアドレス変換を行う仮想化支援機構を利用し、外部メモリ７から内部メモリ８へのデータ読み込み後にセキュアページテーブルツリー１２１のデータ参照先を変更することで、ゲストＯＳに対するアドレス透過性を実現する。

【００９５】

さらに、本実施形態では、未検証データの参照を検出する。このために、本実施形態では、初期状態においてセキュアページテーブルツリー１２１のエントリを「無効」としておき、ページテーブル又はデータの検証と読み込みに成功した場合にセキュアページテーブルツリー１２１のエントリを「有効」とする。これにより、未読み込みのページテーブル又はデータの検出を、汎用のハードウェアであるアドレス変換機構を利用して効率よく行うことができる。

【００９６】

次に、本実施形態の第２のポイントを説明する。

【００９７】
第２のポイントは、セキュアページテーブルツリー１２１とセキュア検証子ツリー１２２の階層構成とを整合させることに関する。本実施形態では、大規模データの検証を可能にするために、外部メモリ７から内部メモリ８への読み込み状態を管理する。本実施形態では、透過的な改ざん検証をファームウェアの処理で実現するために、アドレス変換機構を活用する。もし、アドレス変換機構の動作が妨害され、例えば内部メモリ８が参照されるべきであるにもかかわらず外部メモリ７が参照された場合などのように、不正操作が行われた場合、上記の検証と読み込みデータの保護は正しく機能しない。したがって、本実施形態では、アドレス変換機構の動作を攻撃から守る。

【００９８】
アドレス変換機構は、ページテーブルを参照し、アドレス変換を行う。ページテーブルは、内部メモリ８に配置されており、仮想アドレスを物理アドレスに変換するための定義情報である。アドレス空間が広くなると、ページテーブルを記憶するために必要なサイズも大きくなる。例えば、１つのページテーブルの全アドレス空間を単純に記憶するには、１テラバイトのメモリを保護することを前提とすると、２ギガバイトのサイズが必要になる。このように単純にページテーブルのアドレス空間を物理メモリに固定的に確保することは、情報処理装置にとって大きな負担となる。このため、ページテーブルのアドレス空間を小さくする２つの方法がある。第１の方法は、ページテーブルを階層化し、内部メモリ８の階層的なページテーブルを参照し、ページテーブル自体をページングの対象とする。第２の方法は、第１の方法における階層化と関連する。この第２の方法は、内部メモリ８のメモリ空間の中で参照が不要な部分のテーブル定義状態を未定義のままとし、不連続なメモリ空間定義を許可することでテーブル量を削減する。

【００９９】
アドレス変換機構は、多くのプロセッサに備えられる汎用的な機構である。しかしながら、ページテーブルのページング又は未定義状態を無制限に許すことは、ページング時に正当なページテーブル又はデータを不当なページテーブル又はデータにすり替える、又は、定義されたページテーブル又はデータを一度未定義に書き換えた後に再度初期化する、などの攻撃を引き起こす可能性がある。特に、不揮発性メモリシステムでは、内部メモリ８ではない他の全てのメモリのデータが改ざんされる可能性がある。よって、ＭＭＵによって参照されるページテーブル又はデータは、すべて検証された後に内部メモリ８に配置される必要がある。上述のように、ページテーブルのデータサイズは大きい。プロセッサの内部メモリ８は、例えば、数百キロバイト～数十メガバイト程度である。したがって、ページテーブルに対する検証を伴うページング処理が必要となる。ページテーブルを階層化すると、どのレベルのテーブルまで検証と読み込みが完了しているかに関する状態管理、及び、各テーブルの参照頻度に応じた状態管理が必要となる。

【０１００】
さらに、ページテーブル又はデータに対する検証処理も、限られた容量の内部メモリ８を作業領域として完結する必要がある。単純な検証の方法として、データに対する検証子とは別に、ページテーブル専用の検証子を設ける方法が考えられる。しかしながら、階層的なページテーブルはメモリ上の参照関係によって定義されており、必ずしも連続したアドレス領域にマップされていない。例えば、ページテーブルの第１のエントリがアドレス空間上の最下位番地に配置され、第２のエントリが最上位番地に配置され、第１のエントリと第２のエントリとが参照関係を持つことが、仕様上可能である。このような不連続なページテーブルに対して、連続したアドレス領域に記憶される検証子を適用することは、非効率的である。加えて、検証子も、ページテーブルと同様に階層的な構成を持つ場合、検証子のどの段階まで検証が完了しているか認識し、かつ、検証子の検証済みの部分を再利用するための状態管理を行う必要がある。

【０１０１】
そこで、本実施形態では、第２のポイントとして、ページテーブルの階層構成と検証子の階層構成とを整合させている。ページテーブルの階層構成と検証子の階層構成とを整合

させ、ページテーブルと検証子とが他の検証子によって保護される。本実施形態では、ページテーブルと検証子とで整合した階層構成を持つことで、ページテーブルと検証子との読み込み状態及び検証状態の管理を共通化し、階層構造のデータ管理の処理負荷を軽減する。そして、情報処理装置６５は、広大かつ不連続に定義されたアドレス領域に対して、効率よく検証子を割り当て、安全に管理する。

【０１０２】

例えば、１ページテーブルに５１２個のエントリを格納する３階層のセキュアページテーブルツリー１２１は、グラフとしては、３階層の５１２分木のグラフである。このようなセキュアページテーブルツリー１２１に対するセキュア検証子ツリー１２２は、セキュアページテーブルツリー１２１と同様に、３階層の５１２分木のグラフとし、両者の構造を整合させる。これにより、セキュアページテーブルツリー１２１とセキュア検証子ツリー１２２の読み込み状態及び検証状態の管理単位が整合する。

【０１０３】

外部メモリ７から内部メモリ８へ未読み込みのページテーブル又はデータに対する参照と未読み込みの検証子に対する参照との検出がそれぞれ個別に行われた場合、ＶＭＭによる処理では、ページテーブル又はデータ、及び検証子に対する参照が発生するたびにゲストＯＳからＶＭＭへの切り替えが発生し、切り替えのオーバーヘッドが大きくなる。本実施形態では、ページテーブルと検証子との階層構成を一致させ、未読み込みのページテーブル及び未読み込みの検証子の２種類の制御データに対する参照の検出を同時に行う。これにより、ゲストＯＳからセキュアＶＭＭ６８への切り替え回数を低減させ、さらに処理負荷を軽減させることができる。

【０１０４】

（２ステージのアドレス変換）

図３は、２ステージのアドレス変換を実行する構成を例示するブロック図である。

【０１０５】

セキュアＯＳ５６上でアプリケーション５８１～５８３が実行され、非セキュアＯＳ５７上でアプリケーション５９１～５９３が実行される。

【０１０６】

セキュアＯＳ５６のゲストページテーブル６０１～６０３は、アプリケーション５８１～５８３の仮想アドレスから中間物理アドレス（Intermediate Physical Address）への変換を定義する。

【０１０７】

セキュアＯＳ５６は、ゲストページテーブル６０１～６０３に基づいて、仮想アドレスを中間物理アドレスに変換する。

【０１０８】

非セキュアＯＳ５７のゲストページテーブル６１１～６１３は、アプリケーション５９１～５９３の仮想アドレスから中間物理アドレスへの変換を定義する。

【０１０９】

非セキュアＯＳ５７は、ゲストページテーブル６１１～６１３に基づいて、仮想アドレスを中間物理アドレスに変換する。

【０１１０】

セキュアＶＭＭ６８のＶＭＭページテーブル６２１は、セキュアＯＳ５６の中間物理アドレスから物理アドレスへの変換を定義する。

【０１１１】

セキュアＶＭＭ６８のＶＭＭページテーブル６２２は、非セキュアＯＳ５７の中間物理アドレスから物理アドレスへの変換を定義する。

【０１１２】

セキュアＶＭＭ６８は、ＶＭＭページテーブル６２１，６２２に基づいて、中間物理アドレスを物理アドレスに変換する。

【０１１３】

ここでは、複数のアプリケーション５８１～５８３，５９１～５９３のうちのアプリケーション５８１に基づくアドレス変換について説明するが、他のアプリケーション５８２～５８３，５９１～５９３に基づくアドレス変換も同様である。

【０１１４】

２ステージのアドレス変換では、まずステージ１で、セキュアＯＳ５６によるアドレス変換が実行され、次にステージ２で、セキュアＶＭＭ６８によるアドレス変換が実行される。セキュアＯＳ５６は、セキュアＶＭＭ６８によって管理されるゲストＯＳである。セキュアＯＳ５６によって制御されるアプリケーション５８１は、ゲストページテーブル６０１と対応付けられる。

【０１１５】

アプリケーション５８１は、命令読み込み要求及びデータアクセス要求を仮想アドレスとして発行する。セキュアＯＳ５６は、仮想アドレスを、ゲストページテーブル６０１の定義に基づいて中間物理アドレスに変換する。中間物理アドレスのメモリ領域は、予めセキュアＶＭＭ６８によって各ゲストＯＳに割り当てられている。各ゲストＯＳは、割り当てられたメモリ領域をゲストページテーブルの定義に基づいて、さらに稼働中のアプリケーションに割り当てる。

【０１１６】

セキュアＶＭＭ６８は、中間物理アドレスを、セキュアＶＭＭ６８によって管理されるＶＭＭページテーブル６２１の定義に基づいて、物理アドレスに変換する。仮想アドレスとして発行された要求は、この物理アドレスを用いて処理される。

【０１１７】

（セキュアページテーブルツリー１２１のデータ構造）

図４は、アドレス変換とデータ参照とを実行するハードウェア構成及びセキュアページテーブルツリー１２１のデータ構造を例示するブロック図である。

【０１１８】

この図４で示されるセキュアページテーブルツリー１２１は、例えば、４ギガバイトの仮想アドレス空間を持つ。セキュアページテーブルツリー１２１のデータ構造は、様々なアーキテクチャで適用可能である。特定のアーキテクチャでは、物理ページ拡張のため、ステージ１とステージ２でページテーブルのサイズが異なるが、本実施形態では、ステージ１とステージ２とで同一形式のページテーブルが使用される場合を例として説明する。

【０１１９】

プロセッサ６６は、ＭＭＵ４６を備える。ＭＭＵ４６は、セキュアページテーブルツリー１２１の最上位を示すレジスタ６４を備える。

【０１２０】

レジスタ６４は、物理アドレスにより最上位のページテーブルT101の上位２０ビットを示す。４キロバイト単位で構成されるページテーブルの下位１２ビットは省略される。レジスタ６４によってインデックスされる最上位のページテーブルT101は、テーブルエントリE101-0～E101-3を含む。各テーブルエントリは、８バイトであり、次のレベルのページテーブルへのインデックスと、次のレベルのページテーブルが有効か無効かを示す有効／無効ビットを持つ。

【０１２１】

各テーブルエントリから次レベルのページテーブルへの参照は、ポインタにより行われる。ゆえに、各ページテーブルT101，T101-1，T101-1-0は、メモリでどのような順序で配置されてもよい。同じレベルのページテーブル、例えばレベル２のテーブルT101-1～テーブルT101-n（ｎは２以上の自然数）についても、メモリにおいてどのような順序で配置されてもよい。

【０１２２】

ページテーブルT101-1-0のテーブルエントリE101-1-0～E101-1-511は、それぞれ、データB101-0-0～B101-511-511を参照する。

【０１２３】

図５は、本実施形態に係るブロックの定義を例示する概念図である。

【０１２４】

本実施形態では、ページテーブルツリー９、検証子ツリー１０、セキュアページテーブルツリー１２１、セキュア検証子ツリー１２２を構成するページ単位のブロックを、ページブロックと呼ぶ。ページブロックは、テーブルブロック又はデータブロックである。

【０１２５】

アドレス解決に使用されるページテーブルを、テーブルブロックと呼ぶ。

【０１２６】

実際に読み込み又は書き込みされるデータを、データブロックと呼ぶ。

【０１２７】

あるテーブルブロックから参照可能な１つのページブロックを、参照ブロックと呼ぶ。

【０１２８】

あるテーブルブロックから参照可能な全てのページブロックを、関連ブロックと呼ぶ。

【０１２９】

あるページブロックの参照元となるテーブルブロックを、参照元ブロックと呼ぶ。

【０１３０】

検証に使用されるＭＡＣ値とカウンタ値とは、それぞれ対応するテーブルブロックごとに集約され、管理される。

【０１３１】

ＭＡＣ値を集約して形成されるブロックを、ＭＡＣブロックと呼ぶ。

【０１３２】

カウンタ値を集約して形成されるブロックを、カウンタブロックと呼ぶ。

【０１３３】

あるページブロックに対応するＭＡＣブロックとカウンタブロックとの組合せを、検証ブロックと呼ぶ。なお、カウンタブロックが存在しない場合には、ページブロックに対応するＭＡＣブロックを検証ブロックとする。

【０１３４】

あるページブロックの検証ブロックは、このページブロックの参照元ブロックに付けられる形式を持つ。

【０１３５】

（アドレス変換の詳細）

上記図４を用いて、仮想アドレスMA01=0x40000000が発行された場合を例として、アドレス変換を詳細に説明する。

【０１３６】

仮想アドレスMA01=0x40000000の上位２ビットは01#bである。ページテーブルT101から仮想アドレスの上位２ビット01#bによってインデックスされるテーブルエントリE101-1が参照される。

【０１３７】

次に、テーブルエントリE101-1が持つ次のページテーブルポインタによってアドレス変換が進む。仮想アドレスMA01が0x40000000の場合には、レベル１で選択されるテーブルエントリはE101-1であり、テーブルエントリE101-1によって参照されるレベル２のページテーブルはT101-1である。

【０１３８】

続いて、レベル２で選択されたページテーブルT101-1に対して、仮想アドレスMA01のビット[29:21]によってインデックスされるテーブルエントリが選択される。なお、仮想アドレスのビット[A:B]という表記は、仮想アドレスのAビット目からBビット目までの範囲を表すとする。仮想アドレスMA01のビット[29:21]は全てゼロなので、ページテーブルT101-1のうちのテーブルエントリE101-1-0が選択される。テーブルエントリE101-1-0によって参照されるレベル３のページテーブルはT101-1-0である。

【０１３９】

レベル３で選択されたページテーブルT101-1-0に対して、仮想アドレスMA01のビット[20:12]によってインデックスされるテーブルエントリが選択される。レベル３で選択されるテーブルエントリはE101-1-0-0である。

【０１４０】

このようなアドレス変換により、最終的にデータB101-1-0-0の上位アドレスが決定される。

【０１４１】

（ページテーブルの仮想化）

以下においては、ページテーブルの仮想化について詳細に説明する。

【０１４２】

まず、メモリ空間とページテーブルサイズについて説明する。４ギガバイトの仮想アドレス空間をすべて定義するページテーブルのサイズは、８メガバイト以上になり、物理メモリに固定的にページテーブルを割り当てることはメモリサイズを圧迫する。このため、セキュアＯＳ５６及びセキュアＶＭＭ６８は、ページテーブルを仮想化する。

【０１４３】

ページテーブルの仮想化は、テーブルエントリの有効／無効ビットを用いて行う。テーブルエントリE101-1の場合を例にとって説明する。テーブルエントリE101-1の有効／無効ビットが無効状態を示す場合、当該テーブルエントリE101-1の参照先テーブルT101-1は、物理メモリに存在しない。よって、この参照先ページに対するアクセスが発生した場合、ＭＭＵ４６は、プロセッサ例外(フォールト)を発生させ、参照先ページを物理メモリへ読み込む処理を実行する。フォールトを受けたセキュアＯＳ５６及びセキュアＶＭＭ６８は、例えばハードディスクなどの外部デバイス４３から、参照先テーブルに対応するデータを物理メモリの空きページに記憶し、テーブルエントリE101-1の有効／無効ビットを有効状態に更新し、中断した処理を再開する。

【０１４４】

上記のような制御を行うことで、セキュアＯＳ５６及びセキュアＶＭＭ６８は、巨大な仮想アドレス空間を物理メモリに動的に割り当てることが可能となり、限られたメモリを有効に活用することができる。

【０１４５】

上記図４に示すセキュアページテーブルツリー１２１の構造及び機能は、各種の仮想化アドレス変換機構に適用可能である。後述するように、本実施形態においては、メモリ完全性検証に必要なデータ構造を適用し、ゲストＯＳに対して透過的なメモリ完全性検証機構を実現する。

【０１４６】

（仮想化による複数回ページテーブル参照と１次及び２次アドレス変換キャッシュ４９，５０）

以下で、仮想化による複数回ページテーブル参照と１次及び２次アドレス変換キャッシュ４９，５０について説明する。

【０１４７】

多くのアーキテクチャでは、上記のページテーブル参照は、ＭＭＵによりハードウェアによる処理で実行される。２階層で仮想化されている場合、上記のアドレス変換が２回行われ、ゲストＯＳのページテーブルへのアクセスも、アドレス変換の対象になる。例えば、２ステージのアドレス変換を行うと、最悪の場合には４×３個のページテーブルへの参照が必要になる。

【０１４８】

データ参照ごとにこのようなページテーブル参照が実行され、オーバーヘッドが増加することを避けるため、アドレス変換の結果をキャッシュする１次及び２次アドレス変換キャッシュ４９，５０が用いられる。

【０１４９】

本実施形態では、１次アドレス変換キャッシュ４９と２次アドレス変換キャッシュ５０

とによる２階層の仮想化状態が適用されるとする。
【０１５０】
２ステージのアドレス変換を行う場合、ＭＭＵ４６は、１次アドレス変換キャッシュ４９に、ゲストＯＳの仮想アドレスと、仮想アドレスを２回アドレス変換した後に得られる物理アドレスとを対応付けて記憶する。この場合のタグには仮想アドレスが用いられる。次のデータ参照時に、仮想アドレスと１次アドレス変換キャッシュ４９又は２次アドレス変換キャッシュ５０のタグとが一致すれば、ＭＭＵ４６は、セキュアページテーブルツリー１２１によるアドレス変換を行うことなく、物理アドレスを得ること（アドレス解決）ができる。セキュアページテーブルツリー１２１が複数存在する場合、１次アドレス変換キャッシュ４９及び２次アドレス変換キャッシュ５０は、セキュアページテーブルツリー１２１を識別する識別子とアドレス変換情報とを関連付けて記憶する。識別子としては、例えばセキュアページテーブルツリー１２１の最上位のアドレスを用いてもよい。これにより、同じ仮想アドレスが複数発生しても、正しい物理アドレスを得ることができる。
【０１５１】
アドレス変換はページごとに行われるため、仮想アドレスと物理アドレスとはそれぞれページ内(１２ビット)よりも上位のビットを保持しておくだけでよい。
【０１５２】
２次アドレス変換キャッシュ５０は、１次アドレス変換キャッシュ４９と機能的に同じであるが、１次アドレス変換キャッシュ４９より大容量であり低速である。
【０１５３】
（階層化の概念）
以下に、階層化の概念について説明する。
【０１５４】
例えば、データ参照を高速化するためにキャッシュメモリは２レベルに階層化される。例えば、アドレス変換のためのページテーブルツリーは３レベルに階層化される。例えば、仮想化の制御は２レベルの階層を持っており、３階層のページテーブルによって制御されるアドレス変換が２回適用される。このようなキャッシュメモリのレベル、ページテーブルツリーの階層、仮想化における複数回のアドレス変換の回数（ステージ数）は直交した概念であり、論理的には任意の組み合わせが可能である。例えばキャッシュメモリは３レベルに階層化され、アドレス変換のためのページテーブルツリーは３レベルに階層化され、仮想化によるアドレス変換は２ステージとしてもよい。
【０１５５】
図６は、本実施形態に係る情報処理装置６５によるデータ取得及びアドレス変換の概念を例示するブロック図である。
【０１５６】
命令実行ユニット４５は、１次キャッシュメモリ４７ａ，４７ｂ、２次キャッシュメモリ４８にデータが存在しない場合に、内部メモリ８からデータを取得する。
【０１５７】
命令実行ユニット４５は、アドレス変換が必要な場合に、ＭＭＵ４６に仮想アドレスを送る。
【０１５８】
ＭＭＵ４６は、１次アドレス変換キャッシュ４９又は２次アドレス変換キャッシュ５０に記憶されているアドレス変換情報に基づいて、仮想アドレスを物理アドレスに変換することができない場合に、セキュアページテーブルツリー１２１に基づく２ステージのアドレス変換を実行する。
【０１５９】
このアドレス変換において、ページテーブル又はデータにページフォールトが発生すると、ページフォールトの発生したページテーブル又はデータが、ページングに基づいて、外部メモリ７から内部メモリ８にコピーされる。
【０１６０】

（情報処理装置６５の初期状態）
上述のアドレス変換及び仮想化機構を前提とし、以下で本実施形態に係る情報処理装置６５の初期状態を概説する。
【０１６１】
初期状態において、セキュアＶＭＭ６８、及び、セキュアＶＭＭ６８によって管理されるセキュアＯＳ５６と非セキュアＯＳ５７は、休眠状態である。セキュアＶＭＭ６８、セキュアＯＳ５６、非セキュアＯＳ５７は、不揮発性の外部メモリ７に退避されている。
【０１６２】
本実施形態において、セキュアＶＭＭ６８及びセキュアＯＳ５６の完全性及び秘匿性の信頼の基盤（Root of Trust）となる鍵情報とＭＡＣ値は、プロセッサ６６の内部に記憶される。より具体的に説明すると、プロセッサ６６は、鍵保存ユニット６７を備える。鍵保存ユニット６７は、秘密鍵とルート検証情報１３とを記憶する。プロセッサ６６が書き換え可能な記憶領域を備えていない場合、プロセッサ６６は、安全なメモリとして、鍵保存ユニット６７に記憶されている固定鍵に基づいてバインドされる外部のＴＰＭ（Trusted Platform Module）における不揮発性メモリを用いてもよい。ホストのプロセッサ６６とＴＰＭとの間で認証が行われることで、ＴＰＭの情報が確実に特定のプロセッサと対応付けられる。
【０１６３】
（メモリマップとエンティティ）
以下で、本実施形態に係るメモリマップとエンティティについて説明する。
【０１６４】
図７は、本実施形態に係るメモリマップを例示する図である。
【０１６５】
情報処理装置６５のメモリは、例えば、内部メモリ８、マスクＲＯＭ（Read Only Memory）６９、セキュア永続的領域７０、非セキュアＯＳ領域７５、予備領域７１１、セキュアＯＳ領域７６を含む。内部メモリ８は、割込ベクタ格納領域８ａ、セキュアＶＭＭプログラム領域７７、バッファ領域７１を含む。バッファ領域７１は、バッファ管理情報領域７３、検証バッファ領域７２、一時バッファ領域７４を含む。セキュアＶＭＭ永続的領域７０、非セキュアＯＳ領域７５、予備領域７１１、セキュアＯＳ領域７６は、外部メモリ７に配置される。
【０１６６】
セキュアＶＭＭ永続的（Persistent）領域７０は、セキュアＶＭＭプログラム領域７０１、物理アドレス領域７０２，７０３、セキュアＯＳページテーブル領域７０４、セキュアＶＭＭ作業領域７０５、セキュアＶＭＭ ＭＡＣ領域７０６、予備領域７１０を含む。物理アドレス領域７０２は、レベル１，２のページテーブル、カウンタ値、ＭＡＣ値を記憶する。物理アドレス領域７０３は、レベル３のページテーブル、ページテーブルのカウンタ値及びＭＡＣ値、及び、データ、データのカウンタ値及びＭＡＣ値を記憶する。レベル３の物理アドレス領域７０３は、レベル３のセキュアＶＭＭ６８に対するレベル３エントリ領域７０７、セキュアＯＳ５６に対するレベル３エントリ領域７０８、非セキュアＯＳ５７に対するレベル３エントリ領域７０９を含む。
【０１６７】
セキュアＶＭＭ６８は、セキュアブートされる。セキュアＶＭＭ６８のうちの検証を行うカーネル部分は、外部メモリ７に対する改ざん攻撃から防御するために、安全なメモリに常駐される。本実施形態においては、安全なメモリの一例として、プロセッサ６６のチップ内の内部メモリ８が適用される。本実施形態では、セキュアＶＭＭ６８によるメモリ検証機能は、内部メモリ８に常駐されるメモリ検証プログラムによって実現される。セキュアＶＭＭ６８のうち、メモリ検証プログラムではない他のプログラム、例えば、デバイス仮想化機能のためのプログラムなどは、後述のページング及び検証により、オンデマンドで内部メモリ８に記憶され、実行されてもよい。
【０１６８】

外部メモリ７に記憶されているセキュアＶＭＭ６８は、マスクＲＯＭ６９に記憶されているプログラムに基づいて例えば起動時に検証され、その後、内部メモリ８のセキュアＶＭＭ６８のプログラム領域７７に記憶される。

【０１６９】

検証子ツリー１０は、外部メモリ７のセキュアＶＭＭ永続的領域７０に記憶される。検証子ツリー１０のうちのセキュアＶＭＭ６８によって検証された部分が、内部メモリ８のバッファ領域７１内の検証バッファ領域７２に記憶される。

【０１７０】

バッファ領域７１は、セキュアＶＭＭ６８によって用いられるデータ領域である。バッファ管理情報領域７３は、バッファ管理情報、セキュアＶＭＭ６８で使用される変換リストを記憶する。検証バッファ領域７２は、検証対象データを記憶する。検証バッファ領域７２のうちの未使用の領域を、検証バッファ空き領域と呼ぶ。一時バッファ領域７４は、セキュアＶＭＭ６８の検証時に、一時的に利用されるデータを記憶する。バッファ領域７１のバッファ管理情報とは、バッファ領域７１の使用状況を表す情報であり、例えば、記憶されている又は記憶されていないデータの種別、量、使用頻度などを含む。

【０１７１】

メモリマップは、さらに、非セキュアＯＳ５７の記憶領域７５、セキュアＯＳ５６の記憶領域７６を含む。

【０１７２】

（検証計算の方法）

以下に、本実施形態に係る検証計算の方法について説明する。

【０１７３】

１ページのサイズは４０９６バイト、アドレスサイズは８バイト（６４ビット）、カウンタサイズは１６バイト（１２８ビット）として説明する。しかしながら、各サイズはこれに限定されず、他のサイズを用いてもよい。

【０１７４】

検証計算で用いられるパラメータを以下で説明する。

【０１７５】

Addrは、検証対象ページテーブルの先頭アドレスである。

【０１７６】

D[Addr]は、Addrで始まるiページ分のデータであり、iは任意の自然数である。

【０１７７】

Ctr[Addr]はAddrで始まるページに紐付けられたカウンタ値である。

【０１７８】

Kはメモリ領域全体で共通に使われる機密値である。Kは、常にプロセッサ６６の内部に記憶される。

【０１７９】

Ekは秘密鍵Kによるj-bitブロック暗号である。本実施形態において、暗号化アルゴリズムは、j=128であるAES128であるとする。例えば、ブロック長は１６バイト（１２８ビット）とする。しかしながら、AES128ではない他の暗号アルゴリズムを用いてもよい。

【０１８０】

Paddingはパディングである。

【０１８１】

暗号演算については、Y=MAC[Ek](X)という標記を用いる。ＭＡＣ値Yは、入力Xを共通鍵ブロックサイズに分割した[X0,X1,…,Xn]に対し、秘密鍵Kに基づく共通鍵ブロックベースの固定長ＣＭＡＣアルゴリズムを適用し、計算される。ＭＡＣ値Y、秘密鍵kのデータサイズは、共通鍵ブロックサイズと一致する。入力Xを共通鍵ブロックサイズに分割できない場合は、パディングPaddingが用いられる。

【０１８２】

アドレスAddrから始まるiページ分のデータD[Addr]のＭＡＣ値Yは、D[Addr]を共通鍵ブ

ロックサイズに分割した[D0,D1,D2…D255i]と、Dに紐付けられたカウンタ値Ctr[Addr]、アドレスAddr、パディングPaddingに基づいて、次式で計算される。

【０１８３】

Y=MAC[Ek]([D0,D1,…,D255i] || Ctr[Addr] || Addr || Padding)

D[Addr]、Ctr[Addr]、Addrは、いずれの順番で入力されてもよい。Paddingは、ＭＡＣ関数への入力が共通鍵ブロックサイズに分割できる場合は利用しなくてもよい。アドレスAddrから始まるデータD[Addr]のサイズは、検証子ツリーの構成にしたがって同一の検証ツリー内でも異なる場合がある。

【０１８４】

Ctr[Addr]は、検証対象データのバージョン管理に用いられる。よって、データの読み込み時にはCtr[Addr]はそのまま使用される。データの書き戻し時には、Ctr[Addr]はインクリメントしてから使用される。

【０１８５】

本実施形態において、アドレスAddrは、外部メモリ７のアドレスとして説明する。しかしながら、アドレスAddrは、中間物理アドレスでもよい。

【０１８６】

（セキュア検証子ツリー１２２の構造）

以下に、本実施形態に係るセキュア検証子ツリー１２２のデータ構造について説明する。

【０１８７】

本実施形態では、セキュアページテーブルツリー１２１のデータ構造とセキュア検証子ツリー１２２のデータ構造とを整合させることにより、アドレス解決とデータ検証とを同時に行う。

【０１８８】

セキュアページテーブルツリー１２１とセキュア検証子ツリー１２２との第１のデータ構造として、ページテーブルとＭＡＣ値とで形成されるツリー構造（ＭＡＣツリー構造）を説明する。セキュアページテーブルツリー１２１とセキュア検証子ツリー１２２との第２のデータ構造として、ページテーブルとＭＡＣ値とバージョンを管理するためのカウンタ値とで形成されるツリー構造（ＭＡＣ＋カウンタ構造）を説明する。

【０１８９】

本実施形態では、１ページが４キロバイト、カウンタ値が８バイト、ＭＡＣ値が８バイトの場合を例として説明する。本実施形態においては、テーブルブロックとカウンタブロックとが連続したアドレスに存在するとして説明するが、テーブルブロックとカウンタブロックとでアドレス空間を分けてもよい。

【０１９０】

（ＭＡＣツリー構造）

図８は、本実施形態に係るセキュアページテーブルツリー１２１及びセキュア検証子ツリー１２２のＭＡＣツリー構造を例示するデータ構造図である。

【０１９１】

各データブロックのＭＡＣ値は、データブロックの内容とその配置アドレスとに基づいて生成され、生成されたデータブロックのＭＡＣ値は、そのデータブロックを参照する参照元ブロックに付されるＭＡＣブロックで管理される。上述したように、ＭＡＣブロックは検証ブロックに相当する。

【０１９２】

その一方で、テーブルブロックの検証に用いられるＭＡＣ値は、このテーブルブロックの内容、このテーブルブロックに付されるＭＡＣブロックの内容、そのテーブルブロックの配置アドレスに基づいて、生成される。生成されたテーブルブロックの検証に用いられるＭＡＣ値は、上記のデータブロックのＭＡＣ値と同様に、このテーブルブロックの参照元ブロックに付されるＭＡＣブロックで管理される。この操作を続けていくと、最終的に１つのＭＡＣブロックを頂点とする大規模なツリー構造が形成される。

【０１９３】
例えば、データブロックB201-1-0-511のＭＡＣ値M201-1-0-511は、データブロックB201-1-0-511とアドレスaddr(B201-1-0-511)とに基づいて生成される。
【０１９４】
例えば、テーブルブロックT201-1-0の検証に用いられるＭＡＣ値M201-1-0は、テーブルブロックT201-1-0、このテーブルブロックT201-1-0に付されるＭＡＣブロックT202-1-0、テーブルブロックT201-1-0のアドレスaddr(T201-1-0)に基づいて生成される。データブロックB201-1-0-511のＭＡＣ値M201-1-0-511は参照元ブロックT201-1-0に付随するＭＡＣブロックT202-1-0に、テーブルブロックT201-1-0のＭＡＣ値M201-1-0は参照元ブロックT201-1に付随するＭＡＣブロックT202-1に含まれる。
【０１９５】
ＭＡＣツリー構造において正当性を保証するために、テーブルブロックとこのテーブルブロックに付されるＭＡＣブロックとが同時に読み込まれ、検証される。例えば、テーブルブロックT201-1-0が読み込まれる場合には、このテーブルブロックT201-1-0と合わせてＭＡＣブロックT202-1-0が読み込まれ、テーブルブロックT201-1-0とＭＡＣブロックT202-1-0とを用いて検証が実行される。ＭＡＣツリー構造においては、下位ブロック（子ブロック）の正当性が上位ブロック（親ブロック）に付されているＭＡＣブロックによって保証される。したがって、下位ブロックの検証時には上位ブロックに付されているＭＡＣブロックが検証済みであることが必要である。
【０１９６】
（ＭＡＣ＋カウンタ構造）
図９は、本実施形態に係るセキュアページテーブルツリー１２１及びセキュア検証子ツリー１２２のＭＡＣ＋カウンタ構造を例示するデータ構造図である。
【０１９７】
カウンタ値は、テーブルエントリ単位に設定され、参照ブロックのバージョン管理に使用される。カウンタ値は、値の重複を回避できる条件を満たし、データ又はページテーブルが更新される度に変化する値であればよく、カウントアップ又はカウントダウンされる値でなくてもよい。
【０１９８】
各データブロックのＭＡＣ値は、データブロックの内容と配置アドレスとカウンタ値とに基づいて生成され、使用されたカウンタ値と生成されたデータブロックのＭＡＣ値とはその参照元ブロックに付されたカウンタブロックとＭＡＣブロックとで管理される。一方、テーブルブロックのＭＡＣ値は、テーブルブロック、テーブルブロックに付されているカウンタブロック、テーブルブロックの配置アドレス、テーブルブロックのカウンタ値に基づいて生成される。使用されたカウンタ値と生成されたテーブルブロックのＭＡＣ値は、その参照元ブロックに付されたカウンタブロック、ＭＡＣブロックで管理される。このような操作を続けていくと、一段上位のテーブルブロックに付される検証ブロックに含まれるカウンタブロックでバージョン管理を行い、ＭＡＣブロックで改ざん検証を行う小規模なツリー型データを構成することができる。
【０１９９】
例えば、データブロックB301-1-0-511のＭＡＣ値M301-1-0-511は、データブロックB301-1-0-511、アドレスaddr(B301-1-0-511)、カウンタ値C301-1-0-511に基づいて生成される。
【０２００】
一方、テーブルブロックT301-1-0のＭＡＣ値M301-1-0は、テーブルブロックT301-1-0、カウンタブロックT302-1-0、アドレスaddr(T301-1-0)、テーブルブロックT301-1-0のカウンタ値C301-1-0に基づいて生成される。
【０２０１】
データブロックB301-1-0-511のカウンタ値C301-1-0-511、ＭＡＣ値M301-1-0-511は、参照元ブロックT301-1-0に付されているカウンタブロックT302-1-0、ＭＡＣブロックT303-1

-0に含まれる。
【０２０２】
テーブルブロックT301-1-0のカウンタ値C301-1-0、ＭＡＣ値M301-1-0は、参照元ブロックT301-1に付されているカウンタブロックT302-1、ＭＡＣブロックT303-1に含まれる。
【０２０３】
ＭＡＣ＋カウンタ構造では、テーブルブロックの読み込み時に、テーブルブロックとこのテーブルブロックに付されているカウンタブロックとを共に読み込み、検証する必要がある。しかしながら、テーブルブロックとこのテーブルブロックに付されているＭＡＣブロックとを共に読み込み、検証する必要はない。この理由は、あるページブロックの正しいＭＡＣ値を生成するためには、その上位ブロックに付されているカウンタ値が必要であり、ＭＡＣブロック自体はＭＡＣ値生成に関係しないためである。
【０２０４】
（セキュアページテーブルツリー１２１とページテーブルツリー９）
図１０は、セキュアページテーブルツリー１２１とページテーブルツリー９との関係の一例を示すデータ構造図である。
【０２０５】
内部メモリ８は、アドレス変換に用いられるセキュアページテーブルツリー１２１を記憶する。レジスタ６４は、内部メモリ８のセキュアページテーブルツリー１２１の最上位テーブルＴ４０１を参照する。レジスタ６４によって参照されるセキュアページテーブルツリー１２１の定義に基づいて、物理アドレスへの変換が実行され、命令実行ユニット４５によってメモリ参照が実行される。
【０２０６】
内部メモリ８のセキュアページテーブルツリー１２１を生成するための元データとなるページテーブルツリー９の全体は、外部メモリ７に記憶されている。本実施形態においては、外部メモリ７に記憶されているページテーブルツリー９は、アドレス変換テーブルとして直接参照されることはなく、セキュアページテーブルツリー１２１の元データであることを除いて、特別な機能を持たない。外部メモリ７のページテーブルツリー９は改ざんの危険があるため、本実施形態においては、外部メモリ７のページテーブルツリー９が、検証なしに直接アドレス変換に利用されることを避ける。アドレス変換に用いられるのは、内部メモリ８に記憶されているセキュアページテーブルツリー１２１である。セキュアページテーブルツリー１２１は、ページテーブルツリー９のサブセットである。
【０２０７】
本実施形態に係る情報処理装置６５は、外部メモリ７に記憶されているページテーブルツリー９及びデータの必要部分に対して、内部メモリ８へのコピーとセキュア検証子ツリー１２２に基づく検証を行い、既に内部メモリ８に記憶済みのセキュアページテーブルツリー１２１及びデータに追加する。情報処理装置６５は、内部メモリ８に記憶されていないページテーブル又はデータが参照されると、ページフォールトを発生させ、セキュアＶＭＭ６８がページテーブルツリー９又はデータの必要部分を検証し、検証結果が正当であれば内部メモリ８に記憶する。
【０２０８】
（データブロックの記憶先とアドレス、外部メモリ７のページテーブルツリー９の構成）
以下で、データブロックの記憶先とアドレス、及び、外部メモリ７のページテーブルツリー９の構成について説明する。
【０２０９】
本実施形態においては、外部メモリ７に記憶されたページブロックを、物理改ざんに対して安全な内部メモリ８に一時的にコピーし、処理を実行し、処理後の結果を元の外部メモリ７に書き戻す。
【０２１０】
したがって、同一のページブロックが外部メモリ７のアドレスと内部メモリ８のアドレ

スとに記憶される場合がある。説明を簡略化するために、データブロックB401-0-0-511が記憶されている外部メモリ７のアドレスをEaddr(B401-0-0-511)と表記する。データブロックB401-0-0-511が記憶されている内部メモリ８のアドレスをIaddr(B401-0-0-511)と表記する。厳密に言えば内部メモリ８のアドレスは、検証バッファ領域７２に動的に確保される。このため、Iaddr(B401-0-0-511)の値は、同一のデータブロックB401-0-0-511についても読み込みの度に変化する。しかしながら、以下の読み込みと書き戻しの一連の動作の説明では、この変化を考慮する必要がないため、単純にIaddr(B401-0-0-511)と表記する。

【０２１１】

外部メモリ７に記憶されているページテーブルの各エントリには、Eaddr(B401-0-0-511)のように参照ブロックの外部メモリ７のアドレスが記憶される。ただし、ＭＭＵ４６が認識するページテーブルの実体は、外部メモリ７に記憶されたページテーブルではなく、内部メモリ８に記憶されるとともに検証されたページテーブルである。ＭＭＵ４６は、内部メモリ８に記憶されるとともに検証されたページテーブルを参照する。例えば、上記の図１０において、レジスタ６４によって参照される実体のアドレスは、Iaddr(T401)である。ページテーブルT401-0-0の外部メモリ７のアドレスEaddr(T401-0-0)は、ページテーブル構築時に与えられており、最上位のページテーブルT401から順番に検証読み込みを行うことでアドレス解決を実行することができる。一方、ページテーブルT401-0-0の内部メモリ８上のアドレスIaddr(T401-0-0)は、内部メモリ８の一時バッファ領域７４におけるメモリ確保時に決められる。

【０２１２】

（階層的な検証処理の概要）

以下、階層的な検証処理の概要を説明する。

【０２１３】

データ参照要求から検証を行い、データを取得するまでの一連を動作は、データ参照処理、アドレス解決処理、検証処理、置き換え処理、追い出し処理に分割することができる。それぞれの処理は入れ子的な関係であり、データ参照処理以外は必要がなければ発生しない。

【０２１４】

本実施形態では、アドレス解決時に、解決されたデータの検証処理を行う。このため、階層的に検証処理が発生する。例えば、あるデータに対してデータ参照要求が発生した場合、ページウォークによるアドレス解決処理が発生する。ここでアドレス解決に必要な上位テーブルブロック（親テーブルブロック）が未検証であった場合、まずこの上位テーブルブロックに対する検証処理が実行される。そして、検証されたテーブルブロックが安全な内部メモリ８に読み込まれた後に、下位テーブルブロック（子テーブルブロック）に対する検証処理が実行される。このように、最上位から順に最下位であるデータブロックまで、順次検証が実行される。

【０２１５】

（検証処理発生までの流れ）

以下で、検証処理発生までの流れについて説明する。

【０２１６】

図１１は、本実施形態に係るデータ参照処理を例示するフローチャートである。

【０２１７】

この図１１は、本実施形態に係る検証処理が発生する前までの流れを表す。以下で発生するアドレス変換は、ステージ２ページテーブルを使用する処理であり、ステージ１ページテーブルを使用するゲストＯＳによるアドレス変換はすでに終了しているとする。

【０２１８】

命令実行ユニット４５は、ステップＳ００１において、データ参照要求をＭＭＵ４６に発行する。

【０２１９】

ＭＭＵ４６は、ステップＳ００２において、１次アドレス変換キャッシュ４９又は２次アドレス変換キャッシュ５０に、仮想アドレスと物理アドレスとのアドレス変換情報がキャッシュされているか確認する。

【０２２０】

アドレス変換情報が１次アドレス変換キャッシュ４９又は２次アドレス変換キャッシュ５０にキャッシュされている場合（ＴＬＢヒットの場合）、処理はステップＳ００５に移動する。

【０２２１】

アドレス変換情報が１次アドレス変換キャッシュ４９又は２次アドレス変換キャッシュ５０にキャッシュされていない場合（ＴＬＢミスの場合）、ＭＭＵ４６は、ステップＳ００３において、アドレス解決処理を行い、ステップＳ００４において、解決された仮想アドレスと物理アドレスとのアドレス変換情報を１次アドレス変換キャッシュ４９又は２次アドレス変換キャッシュ５０にキャッシュする。

【０２２２】

ステップＳ００５において、ＭＭＵ４６は、参照要求されたデータを、解決された物理アドレスから読み込む。

【０２２３】

図１２は、本実施形態に係るアドレス解決処理を例示するフローチャートである。

【０２２４】

この図１２で示すアドレス解決処理は、データ参照処理で発生する。

【０２２５】

ステップＳ１０１において、ＭＭＵ４６は、アドレス解決処理を開始すると、ページウォークによるアドレス解決を行う。

【０２２６】

ステップＳ１０２において、ＭＭＵ４６は、ページウォーク中にテーブルエントリが無効か否かチェックする。

【０２２７】

テーブルエントリが有効の場合、処理はステップＳ１０４に移動する。

【０２２８】

テーブルエントリが無効の場合、制御はＭＭＵ４６からセキュアＶＭＭ６８に移り、ステップＳ１０３において、セキュアＶＭＭ６８は、無効のテーブルエントリによって参照されるページブロックの検証処理を行う。検証処理終了後、セキュアＶＭＭ５１６は、無効であった検証されたテーブルエントリを有効にし、制御をセキュアＶＭＭ６８からＭＭＵ４６に移す。ステップＳ１０４において、ＭＭＵ４６は、データブロックまでのアドレスが解決したかチェックする。

【０２２９】

アドレスが解決していない場合には、処理はステップＳ１０１に戻る。これにより、アドレスが解決するまでページウォークが繰り返される。

【０２３０】

アドレスが解決した場合、ステップＳ１０５において、ＭＭＵ４６は、データ参照処理を再開し、アドレス解決処理を終了する。

【０２３１】

このように、検証処理は、ステージ２ページテーブルツリーのページフォールトによるアドレス解決処理時にセキュアＶＭＭ６８によって逐次実行される。ページウォークでは、テーブルブロックとデータブロックとのページングが一度に行われてもよい。この場合、セキュアＶＭＭ６８とＭＭＵ４６との間の遷移回数が削減される。

【０２３２】

（検証処理の発生と検証処理の詳細）

以下で、検証処理の発生と検証処理の詳細とについて説明する。

【０２３３】

ここでは、上記の図９に示すＭＡＣ＋カウンタ構造の検証子ツリーを用いて、データブロックB301-1-0-511に対するデータ参照要求が発生した場合の動作例を説明する。

【０２３４】

まず、説明を簡略化するための前提を記載する。

【０２３５】

検証子ツリーのうちレベル２までのテーブルブロックとカウンタブロックとは、常に内部メモリ８にキャッシュされているとする。例えば、保護される外部メモリ７のサイズが４ギガバイトであり、内部メモリ８にキャッシュされるデータのサイズが５２キロバイトであり、内部メモリ８のサイズが１メガバイトの場合、内部メモリ８は、検証子ツリーのうちレベル２までのテーブルブロックとカウンタブロックとをキャッシュすることが十分な容量を持つ。

【０２３６】

置き換え処理では、置き換え元と同種類のデータが、置き換え対象として、置き換えアルゴリズムにしたがって選択される。すなわち、テーブルブロックの置き換え時には、テーブルブロックが選択される。データブロックの置き換え時は、データブロックが選択される。置き換えアルゴリズムは、ＬＲＵ（Least Recently Used）を用いて説明を行うが、他の置き換えアルゴリズムを用いて置き換え対象を選択してもよい。

【０２３７】

本実施形態においては、内部メモリ８のバッファ管理情報領域７３に、外部メモリ７のアドレスと内部メモリ８のアドレスとの変換リストが記憶されるとする。すなわち、セキュアＶＭＭ６８は、データブロックB301-1-0-511の内部メモリ８のアドレスIaddr(B301-1-0-511)と外部メモリ７のアドレスEaddr(B301-1-0-511)との対応関係を認識する。内部メモリ８のアドレスIaddrと外部メモリ７のアドレスEaddrとの変換は、変換リストを用いる方法ではなく、逆ページウォークなどの方法を用いてもよい。

【０２３８】

ＭＡＣ値計算は、例えば、セキュアＤＭＡコントローラ５２で実行されるが、ソフトウェアで実行されてもよい。

【０２３９】

レベル３以降のテーブルブロックに対して、内部メモリ８でページングが実行される。このため、データブロックB301-1-0-511のアドレス解決に必要な全てのテーブルブロックが内部メモリ８に存在する場合と、存在しない場合とを説明する。データブロックとテーブルブロックではデータ構造及び検証処理が異なるため、以下ではデータブロックとテーブルブロックとのそれぞれについて説明を行う。

【０２４０】

（データブロックの検証処理）

まず、データブロックB301-1-0-511のアドレス解決に必要なページテーブルが全て内部メモリ８に記憶されている場合、すなわちデータブロックB301-1-0-511のみの検証が発生する場合について説明する。テーブルブロックT301，T301-1，T301-1-0とそれらに付随するカウンタブロックT302，T302-1，T302-1-0は全て内部メモリ８の検証バッファ領域７２に記憶されているとする。

【０２４１】

<データブロックに関するアドレス解決処理の詳細>

上記の図１１及び図１２を用いて、データ参照処理と、このデータ参照処理で発生するアドレス解決処理とを説明する。

【０２４２】

ＭＭＵ４６は、データブロックB301-1-0-511のアドレス解決処理を開始し、ステップＳ１０１において、ページウォークによるアドレス解決を行う。

【０２４３】

ＭＭＵ４６は、ステップＳ１０２において、テーブルブロックT301のテーブルエントリE301-1をチェックし、有効であることからテーブルエントリE301-1を参照する。

【０２４４】
ＭＭＵ４６は、ステップＳ１０４において、データブロックB301-1-0-511のアドレスが解決されたかチェックし、未解決であるため、ステップＳ１０１において、ページウォークを繰り返す。
【０２４５】
ＭＭＵ４６は、ステップＳ１０２においてテーブルブロックT301-1-0のテーブルエントリE301-1-0-511が無効であることを検出すると、制御をＭＭＵ４６からセキュアＶＭＭ６８に移す。セキュアＶＭＭ６８は、ステップＳ１０３において、テーブルエントリE301-1-0-511によって参照されるデータブロックB301-1-0-511の検証処理を行う。検証処理終了後、無効であったテーブルエントリE301-1-0-511は有効になり、セキュアＶＭＭ６８は制御をＭＭＵ４６に戻す。ＭＭＵ４６は、ステップＳ１０４において、データブロックB301-1-0-511までのアドレスが解決したかチェックする。ＭＭＵ４６は、アドレスが解決したため、ステップＳ１０５において、データ参照処理を再開し、アドレス解決処理を終了する。
【０２４６】
<情報処理装置６５の構成>
図１３は、本実施形態に係る情報処理装置６５の構成を例示するブロック図である。
【０２４７】
情報処理装置６５は、命令実行ユニット４５、アドレス変換キャッシュ７８、ＭＭＵ４６、検証管理部７９、検証情報生成部８０、外部読込部８１、外部書出部８２、記憶領域管理部８３、検証記憶部８４、鍵保存ユニット６７、外部メモリ７を備える。
【０２４８】
ＭＭＵ４６は、アドレス解決部４６ａを備える。
【０２４９】
検証管理部７９は、検証情報取得部７９ａ、改ざん判定部７９ｂ、検証情報計算部７９ｃを備える。
【０２５０】
記憶領域管理部８３は、参照関係更新部（ページテーブル参照関係更新部）８３ａ、バッファ領域管理部８３ｂ、バッファ書出管理部（検証用バッファ書出管理部）８３ｃを備える。
【０２５１】
ここで、アドレス変換キャッシュ７８とＭＭＵ４６とは、アドレス変換部３に対応する。アドレス変換キャッシュ７８は、１次アドレス変換キャッシュ４９及び２次アドレス変換キャッシュ５０に対応する。
【０２５２】
外部読込部８１及び外部書出部８２は、外部入出力部２に対応する。
【０２５３】
検証情報計算部７９ｃ及び検証情報生成部８０は、検証計算部４に対応する。
【０２５４】
改ざん判定部７９ａは、検証部５に対応する。
【０２５５】
参照関係更新部８３ａは、上記図１の更新部６に対応する。
【０２５６】
バッファ領域管理部８３ｂ及びバッファ書出管理部（検証用バッファ書出管理部）８３ｃは、上記図１の置換管理部２０に対応する。
【０２５７】
検証記憶部８４は、内部メモリ８に対応する。
【０２５８】
<データ参照処理と情報処理装置６５の構成との関係>
上記の図１３の各構成要素と上記図１１，１２のフローチャートとの関係を説明する。

【０２５９】
命令実行ユニット４５は、ステップＳ００１において、データ参照要求を発行し、ステップＳ００２において、アドレス変換キャッシュ７８に、ゲストＯＳの仮想アドレスに対応する物理アドレスがキャッシュされているか否かを問い合わせる。
【０２６０】
アドレス変換キャッシュ７８に参照要求された仮想アドレスに対応する物理アドレスがキャッシュされていない場合、ＭＭＵ４６のアドレス解決部４６ａは、ステップＳ００３において、アドレス解決処理を実行する。
【０２６１】
アドレス解決処理において、ＭＭＵ４６は、ステップＳ１０１でページウォークを実行し、ステップＳ１０２において検証記憶部８４に記憶されている該当のテーブルブロックT301のテーブルエントリE301-1をチェックする。
【０２６２】
テーブルエントリが有効の場合、処理はステップＳ１０４に移動する。
【０２６３】
テーブルエントリが無効の場合、その旨を示す結果を検証管理部７９に通知し、結果を受けた検証管理部７９は、ステップＳ１０３において、このテーブルエントリによって参照されるページブロックに対して検証処理を行う。検証処理終了後、検証管理部７９は、参照関係更新部８３ａに通知を行い、参照関係更新部８３ａは、無効であったテーブルエントリを有効化する。その後、検証管理部７９は読み込みを完了として制御をＭＭＵ４６に戻す。
【０２６４】
ステップＳ１０４において、ＭＭＵ４６は、データブロックまでのアドレスが解決したかチェックし、アドレスが未解決の場合にはステップＳ１０１のページウォークに処理が戻る。
【０２６５】
アドレスが解決された場合、ステップＳ１０５において、ＭＭＵ４６は、データ参照処理を再開し、アドレス解決処理を終了する。
【０２６６】
アドレス解決が完了した段階で、検証管理部７９及び記憶領域管理部８３は、検証済みの状態で、アドレス解決に必要なページテーブルを、検証記憶部８４に動的に確保されたバッファ領域７１に記憶する。
【０２６７】
ＭＭＵ４６は、ステップＳ００４において、アドレス解決の結果であるアドレス変換情報をアドレス変換キャッシュ７８にキャッシュする。
【０２６８】
アドレス変換キャッシュ７８に参照要求された仮想アドレスに対応する物理アドレスがキャッシュされている場合、又は、アドレス解決が実行された場合、ＭＭＵ４６は、ステップＳ００５において、対応する物理アドレスを用いてデータを読み込む。
【０２６９】
アドレス変換キャッシュにアドレス変換情報が記憶されており、既にデータ参照が行われていた場合には、検証済みデータが検証記憶部８４に記憶されている。アドレス変換キャッシュ７８には、検証記憶部８４のバッファのアドレスが記憶されている。アドレス変換キャッシュ７８から変換済みの物理アドレスが検証記憶部８４に送られ、ステップＳ００５において、検証記憶部８４のデータが命令実行ユニット４５に返される。
【０２７０】
<データブロックに関する検証処理の詳細>
図１４は、本実施形態に係る検証処理を例示するフローチャートである。図１４に示す検証処理は、上記図１２のアドレス解決処理で発生する。ここでは、上記図９のデータブロックB301-1-0-511の検証処理について説明する。

【０２７１】
ステップＳ２０１において、セキュアＶＭＭ６８は、データブロックB301-1-0-511の検証処理を開始し、内部メモリ８の検証バッファ領域７２に空き領域が存在するか否かチェックする。検証バッファ領域７２に空き領域がない場合、セキュアＶＭＭ６８は、ステップＳ２０２において、置き換え処理により領域の解放を行う。
【０２７２】
続いて、セキュアＶＭＭ６８は、ステップＳ２０３において、検証されるデータブロックB301-1-0-511を、外部メモリ７のアドレスEaddr(B301-1-0-511)から、内部メモリ８の検証バッファ領域７２の空き領域へコピーする。このとき、セキュアＤＭＡコントローラ５２は、データブロックB301-1-0-511、データブロックB301-1-0-511の外部メモリ７のアドレスEaddr(B301-1-0-511)、内部メモリ８に存在する上位の検証ブロックのカウンタブロックT302-1-0のカウンタ値C301-1-0-511に基づいて、ＭＡＣ値を生成する。
【０２７３】
そして、セキュアＶＭＭ６８は、ステップＳ２０４において、生成されたＭＡＣ値に基づいて検証対象データブロックB301-1-0-511の改ざん検証を行う。改ざん検証において、外部メモリ７からＭＡＣ値を読み込む必要がある場合、セキュアＶＭＭ６８は、検証対象データブロックB301-1-0-511に対応するＭＡＣ値を外部メモリ７から読み込み、読み込まれたＭＡＣ値M301-1-0-511を内部メモリ８の一時バッファ領域７４に記憶する。内部メモリ８のＭＡＣ値M301-1-0-511が使用される場合、セキュアＶＭＭ６８は、検証対象データブロックB301-1-0-511に対応するＭＡＣ値M301-1-0-511を内部メモリ８から読み込み、読み込まれたＭＡＣ値を一時バッファ領域７４に記憶する。そして、セキュアＶＭＭ６８は、一時バッファ領域７４に記憶されたＭＡＣ値M301-1-0-511と、セキュアＤＭＡコントローラ５２で生成されたＭＡＣ値とを比較する。
【０２７４】
セキュアＶＭＭ６８は、ステップＳ２０５において、ＭＡＣ値が整合しない場合、検証失敗と判断し、ステップＳ２０６の検証失敗後処理に制御を移す。ステップＳ２０６において、セキュアＶＭＭ６８は、検証失敗後処理でエラー処理などを行い、その後に検証処理を終了させる。
【０２７５】
セキュアＶＭＭ６８は、ステップＳ２０５において、ＭＡＣ値が整合した場合、検証成功と判断する。セキュアＶＭＭ６８は、ステップＳ２０７において、無効となっていたテーブルエントリE301-1-0-511の参照先アドレスに、検証対象データブロックB301-1-0-511の内部メモリ８のアドレスIaddr(B301-1-0-511)を書き込む。このとき、データブロックB301-1-0-511の外部メモリ７のアドレスEaddr(B301-1-0-511)は、バッファブロック単位にバッファ管理情報領域７３に記憶される。その後、セキュアＶＭＭ６８は、検証処理を終了する。
【０２７６】
上記図１４の検証処理と、上記図１３の情報処理装置６５の構成とを関連付けて説明する。
【０２７７】
検証管理部７９は、ステップＳ２０１において、記憶領域管理部８３のバッファ領域管理部８３ｂに、検証記憶部８４の空き領域の有無を照会する。空き領域がない場合、検証管理部７９は、ステップＳ２０２において、記憶領域管理部８３に読み込み済みバッファ領域解放を要求し、空き領域のアドレスを取得する。
【０２７８】
ステップＳ２０３において、検証管理部７９の検証情報取得部７９ａは、検証記憶部８４に存在する上位の検証ブロックのＭＡＣブロックT303-1-0のＭＡＣ値M303-1-0-511を取得し、検証記憶部８４に存在する上位の検証ブロックのカウンタブロックT302-1-0のカウンタ値C301-1-0-511を取得する。また、検証情報取得部７９ａは、外部読込部８１を通じて、検証対象データブロックB301-1-0-511、検証対象データブロックB301-1-0-511に対応

するＭＡＣ値M301-1-0-511を、外部メモリ７から取得し、取得した検証対象データブロックB301-1-0-511及びＭＡＣ値M301-1-0-511を、検証記憶部８４の空き領域に記憶する。

【０２７９】

ステップＳ２０４において、検証情報計算部７９ｃは、検証対象データブロックB301-1-0-511及びカウンタ値C301-1-0-511と秘密鍵とに基づいて、ＭＡＣ値を計算する。改ざん判定部７９ｂは、計算されたＭＡＣ値を取得済みのＭＡＣ値M301-1-0-511と照合する。

【０２８０】

ＭＡＣ値が整合せず検証に失敗した場合、ステップＳ２０６において、検証管理部７９は、命令実行ユニット４５に検証失敗を通知し、その後の処理を中止する。

【０２８１】

ＭＡＣ値が整合して検証に成功した場合、ステップＳ２０７において、検証管理部 ７９は、参照関係更新部８３ａに読み込み成功を通知する。参照関係更新部８３ａは、無効となっていたテーブルエントリE301-1-0-511の参照先アドレスに、検証対象データブロックB301-1-0-511の内部メモリ８のアドレスIaddr(B301-1-0-511)を記憶する。さらに、参照関係更新部８３ａは、データブロックB301-1-0-511の外部メモリ７のアドレスEaddr(B301-1-0-511)を、バッファブロック単位にバッファ管理情報領域７３に記憶し、検証処理を終了する。

【０２８２】

<データブロックに関する置き換え処理の詳細>

図１５は、本実施形態に係る置き換え処理を例示するフローチャートである。図１５に示す置き換え処理は、上記図１４の検証処理で発生する。置き換え処理を発生させたデータブロックをB301-1-0-511、最も使用されていないデータブロックをB301-1-0-1として説明する。

【０２８３】

セキュアＶＭＭ６８は、置き換え処理を開始し、ステップＳ３０１において、内部メモリ８の置き換え対象を選択する。セキュアＶＭＭ６８は、ＬＲＵなどのような置き換えアルゴリズムに基づいて、データブロックB301-1-0-511の置き換え対象としてデータブロックB301-1-0-1を選択する。

【０２８４】

セキュアＶＭＭ６８は、ステップＳ３０２において、データブロックB301-1-0-1を内部メモリ８から追い出す追い出し対象として選択する。

【０２８５】

セキュアＶＭＭ６８は、ステップＳ３０３において、追い出し処理を実行する。

【０２８６】

追い出し処理終了後、ステップＳ３０４において、セキュアＶＭＭ６８は、置き換え対象データブロックB301-1-0-1が内部メモリ８に存在するかチェックし、置き換え対象データブロックB301-1-0-1は内部メモリ８に存在しないので、置き換え処理を終了する。なお、置き換え対象が内部メモリ８に存在するか否かをチェックする理由は、バッファ管理の方針に依存して、後述のように置き換え対象がテーブルブロックの場合に参照ブロックの追い出しを必要とし、複数回の追い出しが必要となる場合があるためである。上記の例では、１回の追い出し処理で追い出しは完了する。

【０２８７】

上述の置き換え処理終了後、内部メモリ８の検証バッファ領域７２には、空き領域が確保される。

【０２８８】

上記図１５の置き換え処理と、上記図１３の情報処理装置６５の構成とを関連付けて説明する。

【０２８９】

ステップＳ３０１において、検証管理部７９から要求を受けたバッファ領域管理部８３ｂは、最も使用されていないデータブロックB301-1-0-1を置き換え対象として選択する。

【０２９０】
ステップＳ３０２において、バッファ領域管理部８３ｂは、置き換え対象データブロックB301-1-0-1を追い出し対象として選択し、ステップＳ３０３において、追い出し処理を実行する。
【０２９１】
追い出し処理終了後、セキュアＶＭＭ６８は、ステップＳ３０４において、置き換え対象がまだ検証記憶部８４に存在するかチェックする。
【０２９２】
置き換え対象が検証記憶部８４に存在する場合、置き換え対象が検証記憶部８４に存在しなくなるまでステップＳ３０２以降の処理が繰り返される。セキュアＶＭＭ６８は、置き換え対象が検証記憶部８４に存在しなくなると、置き換え処理を終了する。
【０２９３】
<データブロックに関する追い出し処理の詳細>
図１６は、本実施形態に係る追い出し処理を例示するフローチャートである。図１６に示す追い出し処理は、上記図１５の置き換え処理で発生する。追い出し対象となるデータブロックをデータブロックB301-1-0-1とする。このデータブロックB301-1-0-1のカウンタ値C301-1-0-1は、内部メモリ８に記憶されている。データブロックB301-1-0-1のＭＡＣ値M301-1-0-1は、外部メモリ７に記憶されている。外部メモリ７のＭＡＣ値M301-1-0-1は、外部メモリ７に記憶されているデータブロックB301-1-0-1のＭＡＣ値である。よって、内部メモリ８で更新されたデータブロックB301-1-0-1が外部メモリ７へ書き戻される場合には、ＭＡＣ値M301-1-0-1の更新処理が必要となる。一方、内部メモリ８のデータブロックB301-1-0-1が更新されなかった場合、外部メモリ７と内部メモリ８でデータブロックB301-1-0-1の内容に差がないことから、ＭＡＣ値M301-1-0-1の更新処理は必要ない。
【０２９４】
セキュアＶＭＭ６８は、データブロックB301-1-0-1の追い出し処理を開始し、ステップＳ４０１において、追い出し対象となったデータブロックB301-1-0-1の内容に更新があるか確認する。更新がない場合はステップＳ４０５へ進む。
【０２９５】
更新がある場合は、ステップＳ４０２において、セキュアＶＭＭ６８は、追い出し対象データブロックB301-1-0-1のＭＡＣ更新処理を行う。セキュアＶＭＭ６８は、追い出し対象データブロックB301-1-0-1の上位の検証ブロックのカウンタブロックT302-1-0に含まれるカウンタ値C301-1-0-1をインクリメントし、セキュアＤＭＡコントローラ５２は、追い出し対象データブロックB301-1-0-1、変換リストを用いて変換された外部メモリ７のアドレスEaddr(B301-1-0-1)、インクリメントされたカウンタ値C301-1-0-1に基づいて、追い出し対象データブロックB301-1-0-1の新しいＭＡＣ値M301-1-0-1を生成する。
【０２９６】
その後、セキュアＶＭＭ６８は、ステップＳ４０３において、内部メモリ８の変換リストを用いてデータブロックB301-1-0-1の書き出し先となる外部メモリ７のアドレスEaddr(B301-1-0-1)を決定する。
【０２９７】
セキュアＤＭＡコントローラ５２は、ステップＳ４０４において、追い出し対象データブロックB301-1-0-1を外部メモリ７のアドレスEaddr(B301-1-0-1)に、生成されたＭＡＣ値M301-1-0-1を外部メモリ７のＭＡＣブロックT303-1-0の所定の場所に、書き出す。
【０２９８】
内部メモリ８で追い出し対象データブロックB301-1-0-1が更新されていない場合、又は、ＭＡＣ更新と追い出し対象の書き出しが実行された場合、ステップＳ４０５において、セキュアＶＭＭ６８は、追い出し対象データブロックB301-1-0-1を指すテーブルエントリE301-1-0-1の参照先アドレスを外部メモリ７のアドレスEaddr(B301-1-0-1)に書き換え、追い出し対象テーブルエントリE301-1-0-1を無効にする。そして、セキュアＶＭＭ６８は、内部メモリ８のバッファ管理情報領域７３に記憶された追い出し対象データブロックB3

01-1-0-1に関する制御情報を削除し、検証バッファ領域７２のデータブロックB301-1-0-1が記憶されていた領域を解放する。この処理によって、検証バッファ領域７２にデータブロックサイズの空き領域が生まれる。そして、セキュアＶＭＭ６８は、追い出し処理を終了する。

【０２９９】

上記図１６の追い出し処理と、上記図１３の情報処理装置６５の構成とを関連付けて説明する。

【０３００】

バッファ書出管理部８３ｃは、追い出し対象データブロックB301-1-0-1の追い出し処理を開始する。バッファ書出管理部８３ｃは、ステップＳ４０１において、追い出し対象となったデータブロックB301-1-0-1の内容に更新があるか否かを確認する。

【０３０１】

更新がない場合、バッファ書出管理部８３ｃは、ステップＳ４０５において、データを破棄して内部メモリ８のバッファ領域を解放し、参照関係更新部８３ａは、テーブルエントリの書き換え処理を行う。

【０３０２】

更新がある場合、バッファ書出管理部８３ｃは、ステップＳ４０２において、検証情報生成部８０に追い出し対象データブロックB301-1-0-1のＭＡＣ更新処理を依頼する。検証情報生成部８０は、追い出し対象データブロックB301-1-0-1の上位検証ブロックのカウンタブロックT302-1-0に含まれるカウンタ値C301-1-0-1をインクリメントし、追い出し対象データブロックB301-1-0-1、変換リストを用いて変換された外部メモリ７のアドレスEaddr(B301-1-0-1)、インクリメントされたカウンタ値C301-1-0-1に基づいて、追い出し対象データブロックB301-1-0-1の新しいＭＡＣ値M201-1-0-1を生成する。

【０３０３】

その後、バッファ書出管理部８３ｃは、ステップＳ４０３において、内部メモリ８の変換リストを用いて、追い出し対象データブロックB301-1-0-1の書き出し先となる外部メモリ７のアドレスEaddr(B301-1-0-1)を決定し、ステップＳ４０４において、外部書出部８２に、追い出し対象データブロックB301-1-0-1を外部メモリ７のアドレスEaddr(B301-1-0-1)に書き込む依頼をし、生成されたＭＡＣ値M301-1-0-1を外部メモリ７のＭＡＣブロックT303-1-0の所定のアドレスへ書き込む依頼をする。

【０３０４】

ＭＡＣ更新とデータの書き出しが実行された場合、ステップＳ４０５において、参照関係更新部８３ａは、追い出し対象データブロックB301-1-0-1を指すテーブルエントリE301-1-0-001の参照先アドレスを外部メモリ７のアドレスEaddr(B301-1-0-1)に書き換え、エントリを無効にする。そして、バッファ領域管理部８３ｂは、内部メモリ８のバッファ管理情報領域７３に記憶された追い出し対象データブロックB301-1-0-1に関する制御情報を削除し、検証バッファ領域７２の追い出し対象データブロックB301-1-0-1が記憶されていた領域を解放する。この処理によって、検証バッファ領域７２にデータブロックサイズの空き領域が確保される。そして、バッファ書出管理部８３ｃは、追い出し処理を終了する。

【０３０５】

以上が、アドレス解決、検証、置き換え、追い出しの各処理に必要な上位のテーブルブロックが全て内部メモリ８に記憶済みの場合のデータブロックに対する各処理である。

【０３０６】

（テーブルブロックの検証処理）

以下では、データブロックB301-1-0-511のアドレス解決に必要なテーブルブロックの一部が内部メモリ８に存在しない場合、換言すれば、テーブルブロックが検証される場合の処理について説明する。

【０３０７】

テーブルブロックT301，T301-1とそれらに付されるカウンタブロックT302，T302-1は内

部メモリ８の検証バッファ領域７２に記憶されるとする。検証バッファ領域７２は検証記憶部８４に含まれる。テーブルブロックT301-1-0とそれに付随するカウンタブロックT302-1-0は内部メモリ８に記憶されていないとする。

【０３０８】

<テーブルブロックに関するアドレス解決処理>

テーブルブロックに関するアドレス解決処理は、先で説明した図１２のフローチャートを流用して説明する。

【０３０９】

ＭＭＵ４６は、データブロックB301-1-0-511のアドレス解決処理を開始し、ステップＳ１０１において、ページウォークによるアドレス解決を行う。

【０３１０】

ＭＭＵ４６は、ステップＳ１０２において、テーブルブロックT301のテーブルエントリE301-1をチェックする。

【０３１１】

ＭＭＵ４６は、テーブルエントリE301-1が有効の場合に、テーブルエントリE301-1を参照する。

【０３１２】

ＭＭＵ４６は、ステップＳ１０４において、データブロックB301-1-0-511のアドレスが解決したかチェックし、未解決の場合には、ステップＳ１０１のページウォークを繰り返す。

【０３１３】

ＭＭＵ４６は、テーブルブロックT301-1のテーブルエントリE301-1-0が無効であることを検出すると制御をセキュアＶＭＭ６８に移す。セキュアＶＭＭ６８は、ステップＳ１０３において、テーブルエントリE301-1-0によって参照されるテーブルブロックT301-1-0の検証処理を行う。検証処理終了後、セキュアＶＭＭ６８は、無効であったテーブルエントリE301-1-0を有効とし、制御はセキュアＶＭＭ６８からＭＭＵ４６に戻る。

【０３１４】

ＭＭＵ４６は、ステップＳ１０４において、データブロックB301-1-0-511までのアドレスが解決したかチェックし、未解決の場合には、再度、ステップＳ１０１のページウォークを行い、同様の処理が繰り返される。

【０３１５】

データブロックB301-1-0-511までのアドレスが解決された場合、ステップＳ１０５において、ＭＭＵ４６は、データ参照処理を再開し、アドレス解決処理を終了する。

【０３１６】

上記のようなページテーブルのアドレス解決処理と、上記図１３に示す情報処理装置６５の構成とを関連付けて説明する。

【０３１７】

命令実行ユニット４５は、データ参照要求を発行する。ＭＭＵ４６は、テーブルブロックT301-1-0が未読み込みであるため、アドレス変換キャッシュ７８のキャッシュミスと判断し、ＭＭＵ４６のアドレス解決部４６ａは、アドレス解決を実行する。ＭＭＵ４６のアドレス解決部４６ａは、ステップＳ１０１において、ページウォークを実行する。

【０３１８】

ＭＭＵ４６は、ステップＳ１０２において、検証記憶部８４に記憶されたテーブルブロックT301のテーブルエントリE301-1をチェックし、有効であることからテーブルエントリE301-1を参照する。

【０３１９】

ＭＭＵ４６は、ステップＳ１０４において、データブロックB301-1-0-511のアドレスが解決されたかチェックし、未解決であるためステップＳ１０１のページウォークを繰り返す。

【０３２０】

ＭＭＵ４６は、ステップＳ１０２において、テーブルブロックT301-1のテーブルエントリE301-1-0が無効であることを検出すると、その旨を検証管理部７９に通知する。

【０３２１】

検証管理部７９は、ステップＳ１０３において、テーブルエントリE301-1-0-511によって参照されるデータブロックB301-1-0-511の検証処理を実行する。検証処理終了後、検証管理部７９は、参照関係更新部８３ａに通知を行い、参照関係更新部８３ａは、無効であったテーブルエントリE301-1-0を有効化する。検証管理部７９は、ＭＭＵ４６に読み込み完了を通知する。

【０３２２】

ＭＭＵ４６は、ステップＳ１０４において、データブロックB301-1-0-511までのアドレスが解決したかチェックし、未解決の場合には、再度、ステップＳ１０１のページウォークを行い、同様の処理が繰り返される。

【０３２３】

アドレスが解決すると、ＭＭＵ４６は、ステップＳ１０５において、データ参照処理を再開し、アドレス解決処理を終了する。

【０３２４】

アドレス解決が完了した段階では、アドレス解決に必要なページテーブルは、検証管理部７９によって検証され、記憶領域管理部８３により検証記憶部８４に動的に確保されたバッファに、検証済みの状態で記憶される。そして、ＭＭＵ４６は、アドレス解決結果をアドレス変換キャッシュ７８にキャッシュする。

【０３２５】

<テーブルブロックに関する検証処理の詳細>

ページテーブルに関する検証処理は、先で説明した図１４の検証処理を流用して説明する。ここでは、テーブルブロックT301-1-0の検証処理を説明する。

【０３２６】

セキュアＶＭＭ６８は、テーブルブロックT301-1-0の検証処理を開始し、ステップＳ２０１において、内部メモリ８の検証バッファ領域７２に空き領域が存在するか否かチェックする。

【０３２７】

空き領域がない場合、セキュアＶＭＭ６８は、ステップＳ２０２において、置き換え処理により領域の解放を行う。

【０３２８】

続いて、セキュアＶＭＭ６８は、ステップＳ２０３において、検証されるテーブルブロックT301-1-0を、外部メモリ７のアドレスEaddr(T301-1-0)から内部メモリ８の検証バッファ領域７２の空き領域へコピーする。このとき、セキュアＤＭＡコントローラ５２は、ＭＡＣツリー構造又はＭＡＣ＋カウンタ構造で定義されるＭＡＣ生成方法に基づいて、読み込まれたデータのＭＡＣ値を生成する。

【０３２９】

そして、セキュアＶＭＭ６８は、ステップＳ２０４において、生成されたＭＡＣ値を使って検証対象テーブルブロックT301-1-0の改ざん検証を行う。セキュアＶＭＭ６８は、検証対象テーブルブロックT301-1-0に対応するＭＡＣ値M301-1-0を外部メモリ７から読み込み、内部メモリ８の一時バッファ領域７４に記憶し、このＭＡＣ値M301-1-0とセキュアＤＭＡコントローラ５２で生成されたＭＡＣ値とを比較する。ＭＡＣ値M301-1-0は、外部メモリ７のＭＡＣブロックT303-1に含まれている。正しい上位カウンタ値に対応するＭＡＣ値は、秘密鍵がなければ計算できない。上位カウンタ値は、上位テーブルとともに検証されている。このため、読み込まれたＭＡＣ値M301-1-0に対する検証は実行される必要がない。

【０３３０】

セキュアＶＭＭ６８は、ステップＳ２０５において、ＭＡＣ値が不整合の場合、検証失敗と判断し、ステップＳ２０６の検証失敗後処理に制御を移す。ステップＳ２０６におい

て、セキュアＶＭＭ６８は、検証失敗後処理でエラー処理などを行い、その後に検証処理を異常終了させる。

【０３３１】

セキュアＶＭＭ６８は、ステップＳ２０５において、ＭＡＣ値が整合した場合、検証成功と判断する。セキュアＶＭＭ６８は、ステップＳ２０７において、無効となっていたテーブルエントリE201-1-0の参照先アドレスに、検証対象テーブルブロックT301-1-0の内部メモリ８のアドレスIaddr(T301-1-0)を書き込む。このとき、テーブルブロックT301-1-0の外部メモリ７のアドレスEaddr(T301-1-0)は、バッファブロック単位にバッファ管理情報領域７３に記憶される。その後、セキュアＶＭＭ６８は、検証処理を終了する。

【０３３２】

上記のようなテーブルブロックの検証処理を、上記図１２のアドレス解決処理のフローチャートと上記図１３に示す情報処理装置６５の構成とを関連付けて説明する。

【０３３３】

ＭＭＵ４６のアドレス解決部４６ａは、データブロックB301-1-0-511のアドレス解決処理を開始し、ステップＳ１０１において、ページウォークによるアドレス解決を行う。

【０３３４】

アドレス解決部４６ａは、ステップＳ１０２において、検証記憶部８４を参照し、テーブルブロックT301のテーブルエントリE301-1をチェックし、テーブルエントリE301-1が有効であるため、テーブルエントリE301-1を参照する。

【０３３５】

ＭＭＵ４６は、ステップＳ１０４において、データブロックB301-1-0-511のアドレスが解決したか否かチェックし、未解決であるため、ステップＳ１０１のページウォークを繰り返す。

【０３３６】

ＭＭＵ４６は、ステップＳ１０２において、テーブルブロックT301-1のテーブルエントリE301-1-0が無効であることを検出すると、その旨を検証管理部７９に通知する。

【０３３７】

検証情報取得部７９ａは、記憶領域管理部８３へ空き領域の確保を依頼する。記憶領域管理部８３のバッファ領域管理部８３ｂは、ステップＳ２０１において検証記憶部８４に空き領域が存在するか否か判断し、空き領域がない場合に、ステップＳ２０２の置き換え処理を実行する。

【０３３８】

検証情報取得部７９ａは、ステップＳ２０３において、検証記憶部８４に存在する上位検証ブロックのカウンタブロックT302-1のカウンタ値C301-1-0を取得する。検証情報取得部７９ａは、外部読込部８１を経由して検証対象ページブロックT301-1-0及び検証対象ページブロックT301-1-0に対応するＭＡＣ値M301-1-0を外部メモリ７から検証記憶部８４の空き領域に読み込む。

【０３３９】

ステップＳ２０４において、検証情報計算部７９ｃは、検証対象ページブロックT301-1-0、カウンタ値C301-1-0、秘密鍵に基づいて、ＭＡＣ値を計算する。

【０３４０】

改ざん判定部７９ｂは、ステップＳ２０５において、計算されたＭＡＣ値を取得済みのＭＡＣ値M301-1-0と照合する。

【０３４１】

ＭＡＣ値が整合せず検証に失敗した場合、ステップＳ２０６において、検証管理部７９は、命令実行ユニット４５に検証失敗を通知し、その後の処理を中止する。

【０３４２】

ＭＡＣ値が整合して検証に成功した場合、ステップＳ２０７において、検証管理部７９は、参照関係更新部８３ａに読み込み成功を通知する。参照関係更新部８３ａは、無効となっていたテーブルエントリE301-1-0の参照先アドレスに検証対象ページブロックT301-1

-0の検証記憶部８４のアドレスIaddr(T301-1-0)を書き込む。さらに、参照関係更新部８３ａは、テーブルエントリE301-1-0に記憶されている検証対象ページブロックT301-1-0の外部メモリ７のアドレスEaddr(T301-1-0)を、バッファブロック単位にバッファ領域管理部８３ｂに記憶し、検証処理を終了する。

【０３４３】

<テーブルブロックに関する置き換え処理の詳細>

テーブルブロックに関する置き換え処理は、先で説明した図１５の置き換え処理を流用して説明する。ここでは、置き換え処理を発生させたテーブルブロックをT301-1-0とし、最も使用されていないテーブルブロックをT301-1-511として説明する。テーブルブロックの置き換えを行う場合には、そのテーブルブロックの関連ブロックも共に内部メモリ８から外部メモリ７へ追い出される。すなわち、テーブルブロックT301-1-511が置き換え対象となる場合、テーブルブロックT301-1-511から参照可能であり内部メモリ８に存在するデータブロックB301-1-511-0～B301-1-511-511も、テーブルブロックT301-1-511と共に、置き換え対象として選択される。この場合には、セキュアＶＭＭ６８は、テーブルブロックT301-1-511の上位のテーブルブロックT301-1に含まれるテーブルエントリE301-1-511を無効にする。ただし、本実施形態において必ずしも全ての関連ブロックを置き換え対象とする必要はない。例えば、適切なバッファ管理が実行された場合には、データブロックB301-1-511-0～B301-1-511-511は、テーブルブロックT301-1-511の追い出し処理後であっても内部メモリ８に存在し続けていてもよい。関連ブロックの一部がキャッシュされているようなデータ管理方法としては、ファイルシステムのディレクトリキャッシュなどで用いられる手法を適用することができる。

【０３４４】

セキュアＶＭＭ６８は、置き換え処理を開始し、ステップＳ３０１において、内部メモリ８の置き換え対象テーブルブロックを選択する。セキュアＶＭＭ６８は、置き換えアルゴリズムに基づいて、テーブルブロックT301-1-0の置き換え対象としてテーブルブロックT301-1-511を選択する。

【０３４５】

セキュアＶＭＭ６８は、ステップＳ３０２において、置き換え対象テーブルブロックT301-1-511、関連ブロックであるデータブロックB301-1-511-0～B301-1-511-511のうち内部メモリ８に存在するデータブロックを内部メモリ８から追い出す追い出し対象として選択し、ステップＳ３０３において追い出し処理を実行する。このように、置き換え対象がテーブルブロックの場合、置き換え対象テーブルブロックとその配下にある関連ブロックとが置き換え対象として選択される。

【０３４６】

追い出し処理終了後、セキュアＶＭＭ６８は、ステップＳ３０４において、置き換え対象が内部メモリ８に存在するか否かチェックする。置き換え対象の置き換え処理が全て終了し、置き換え対象の全てが内部メモリ８に存在しなくなるまで、ステップＳ３０２以降の処理が繰り返される。セキュアＶＭＭ６８は、置き換え対象が内部メモリ８に存在しなくなると、置き換え処理を終了する。

【０３４７】

上述の置き換え処理終了後、内部メモリ８の検証バッファ領域７２には、テーブルブロックT301-1-511とカウンタブロック、及び、内部メモリ８に存在した関連ブロックに応じた空き領域が確保される。

【０３４８】

上記のようなテーブルブロックに関する置き換え処理と、上記図１３に示す情報処理装置６５の構成とを関連付けて説明する。

【０３４９】

バッファ領域管理部８３ｂは、検証管理部７９から要求を受け、ステップＳ３０１において、最も使用されていないテーブルブロックT301-1-511と、このテーブルブロックT301-1-511の配下にある関連ブロックとを置き換え対象として選択する。

【０３５０】
バッファ領域管理部８３ｂは、ステップＳ３０２において、置き換え対象のテーブルブロックT301-1-511及び関連ブロックのいずれかを、追い出し対象として選択し、ステップＳ３０３において、追い出し処理を実行する。
【０３５１】
バッファ領域管理部８３ｂは、ステップＳ３０４において、置き換え対象の全てが内部メモリ８から追い出されるまで追い出し処理を繰り返す。
【０３５２】
<テーブルブロックに関する追い出し処理の詳細>
テーブルブロックに関する追い出し処理は、先で説明した図１６のフローチャートを流用して説明する。ここでは、追い出し対象がテーブルブロックT301-1-511の場合を例として説明する。このテーブルブロックT301-1-511のカウンタ値C301-1-511は、内部メモリ８に記憶されている。テーブルブロックT301-1-511のＭＡＣ値M301-1-511は、外部メモリ７に記憶されている。外部メモリ７のＭＡＣ値M301-1-511は、外部メモリ７に記憶されているテーブルブロックT301-1-511のＭＡＣ値である。よって、内部メモリ８で更新されたテーブルブロックT301-1-511が外部メモリ７へ書き戻される場合には、ＭＡＣ値M301-1-511の更新処理が必要となる。一方、内部メモリ８のテーブルブロックT301-1-511が更新されなかった場合、外部メモリ７と内部メモリ８でテーブルブロックT301-1-511の内容に差がないことから、ＭＡＣ値M301-1-511の更新処理は必要ない。
【０３５３】
セキュアＶＭＭ６８は、テーブルブロックT301-1-511の追い出し処理を開始し、ステップＳ４０１において、追い出し対象のテーブルブロックT301-1-511の内容に更新があるか確認する。
【０３５４】
更新がない場合、セキュアＶＭＭ６８は、ステップＳ４０５の内部メモリ８の領域の解放へ進む。
【０３５５】
更新がある場合は、セキュアＶＭＭ６８は、ステップＳ４０２において、テーブルブロックT301-1-511のＭＡＣ更新処理を行う。セキュアＶＭＭ６８は、テーブルブロックT301-1-511の上位の検証ブロックのカウンタブロックT302-1に含まれるカウンタ値C301-1-511をインクリメントし、セキュアＤＭＡコントローラ５２は、テーブルブロックT301-1-511、変換リストを用いて変換された外部メモリ７のアドレスEaddr(T301-1-511)、インクリメントされたカウンタ値C301-1-511に基づいて、テーブルブロックT301-1-511の新しいＭＡＣ値M301-1-511を生成する。
【０３５６】
その後、セキュアＶＭＭ６８は、ステップＳ４０３において、内部メモリ８の変換リストを用いてテーブルブロックT301-1-511の書き出し先となる外部メモリ７のアドレスEaddr(T301-1-511)を決定する。
【０３５７】
セキュアＤＭＡコントローラ５２は、ステップＳ４０４において、テーブルブロックT301-1-511を外部メモリ７のアドレスEaddr(T301-1-511)に書き出し、生成されたＭＡＣ値M301-1-511を外部メモリ７のＭＡＣブロックT303-1の所定の場所に書き出す。
【０３５８】
テーブルブロックT301-1-511に内容の更新がない場合、又は、ＭＡＣ更新とデータの書き出しが実行された場合、セキュアＶＭＭ６８は、ステップＳ４０５において、テーブルブロックT301-1-511を指すテーブルエントリE301-1-511の参照先アドレスを外部メモリ７のアドレスEaddr(T301-1-511)に書き換え、テーブルエントリE301-1-511を無効にする。そして、セキュアＶＭＭ６８は、バッファ管理情報領域７３に記憶されているテーブルブロックT301-1-511に関する制御情報を削除し、検証バッファ領域７２においてテーブルブロックT301-1-511の記憶領域を解放する。

【０３５９】
この処理によって、検証バッファ領域７２にテーブルブロックとカウンタブロックサイズの空き領域が生まれる。最後に、セキュアＶＭＭ６８は、追い出し処理を終了する。
【０３６０】
上記のようなテーブルブロックに関する追い出し処理と、上記図１３に示す情報処理装置６５の構成とを関連付けて説明する。
【０３６１】
バッファ領域管理部８３ｂは、テーブルブロックT301-1-511の追い出し処理を開始し、ステップＳ４０１において、追い出し対象のテーブルブロックT301-1-511の内容に更新があるか判断する。更新がない場合、処理はステップＳ４０５の検証記憶部８４の領域の解放へ進む。
【０３６２】
更新がある場合、検証情報生成部８０は、ステップＳ４０２において、テーブルブロックT301-1-511のＭＡＣ更新処理を行う。検証情報生成部８０は、テーブルブロックT301-1-511の上位検証ブロックのカウンタブロックT302-1に含まれるカウンタ値C301-1-511をインクリメントする。検証情報生成部８０は、テーブルブロックT301-1-511、変換リストを用いて変換された外部メモリ７のアドレスEaddr(T301-1-511)、インクリメントされたカウンタ値C301-1-511に基づいて、テーブルブロックT301-1-511の新しいＭＡＣ値M201-1-511を生成する。
【０３６３】
その後、参照関係更新部８３ａは、ステップＳ４０３において、検証記憶部８４の変換リストを用いてテーブルブロックT301-1-511の書き出し先となる外部メモリ７のアドレスEaddr(T301-1-511)を決定する。外部書出部８２は、ステップＳ４０４において、テーブルブロックT301-1-511を外部メモリ７のアドレスEaddr(T301-1-511)に書き出し、生成されたＭＡＣ値M301-1-511を外部メモリ７のＭＡＣブロックT303-1の所定の場所に書き出す。
【０３６４】
テーブルブロックT301-1-511が更新されていない場合、又は、ＭＡＣ更新と書き出しが完了済みの場合、ステップＳ４０５において、参照関係更新部８３ａは、テーブルロックT301-1-511を指すテーブルエントリE301-1-511の参照先アドレスを外部メモリ７のアドレスEaddr(T301-1-511)に書き換え、テーブルエントリE301-1-511を無効にする。そして、バッファ領域管理部８３ｂは、バッファ管理情報領域７２に記憶されたテーブルブロックT301-1-511に関する制御情報を削除し、検証バッファ領域７２においてテーブルブロックT301-1-511が記憶されていた領域を解放する。この処理によって、検証バッファ領域７２にテーブルブロックサイズの空き領域が確保される。最後に、バッファ領域管理部８３ｂは、追い出し処理を終了する。
【０３６５】
上記のようなテーブルブロックに対する各種処理は、例えば、データブロックのアドレス解決、検証、置き換え、追い出しの各処理において、必要なテーブルブロックが内部メモリ８に記憶されていない場合に実行される。
【０３６６】
以下で、本実施形態に係る情報処理装置６５が特定のアーキテクチャを持つ場合について説明する。
【０３６７】
X[A:B]は、値XのAビット目からBビット目までの範囲を表すとする。例えば、X[63:6]は、値Xの６３ビットから６ビット目までの範囲を表す。
【０３６８】
図１７は、特定のアーキテクチャのテーブルエントリ構造を例示するデータ構造図である。
【０３６９】

テーブルエントリＴＥ１は、データブロックを参照するレベル３のテーブルエントリとする。

【０３７０】

テーブルエントリＴＥ２は、データブロックを参照するレベル１又はレベル２のテーブルエントリとする。

【０３７１】

テーブルエントリＴＥ３は、テーブルブロックを参照するテーブルエントリとする。

【０３７２】

ソフトウェア使用予備フィールド８５は、ＴＥ１[58:55]又はＴＥ２[58:55]とする。ソフトウェア使用予備フィールド８５は、テーブルエントリＴＥ１又はＴＥ２の上位ブロック属性フィールド８６内に配置されている。ソフトウェア使用予備フィールド８５は、特に使用用途が定義されていないデータフィールドである。ソフトウェア使用予備フィールド８５は、ハードウェアレベルで未定義とする。

【０３７３】

ＨＡＰフィールド８７は、ＴＥ１[7:6]又はＴＥ２[7:6]とする。ＨＡＰフィールド８７は、テーブルエントリＴＥ１又はＴＥ２の下位ブロック属性フィールド８８内に配置されている。ＨＡＰフィールド８７は、アクセス制御を行うための情報を格納する。

【０３７４】

図１８は、ＨＡＰフィールド８７の仕様を例示するテーブルである。

【０３７５】

ＨＡＰフィールド８７は、アクセス制御を行うための情報を格納する。

【０３７６】

ＨＡＰ[1:0]が00の場合、アクセス権限は無効を示す「No Access」とする。

【０３７７】

ＨＡＰ[1:0]が01の場合、アクセス権限は読み込みを示す「Read-only」であるとする。

【０３７８】

ＨＡＰ[1:0]が10の場合、アクセス権限は書き込みを示す「Write-only」であるとする。

【０３７９】

ＨＡＰ[1:0]が11の場合、アクセス権限は読み出し及び書き込みを示す「Read/Write」であるとする。

【０３８０】

テーブルエントリＴＥ１及びテーブルエントリＴＥ２は、上位ブロック属性フィールド８６内のソフトウェア使用予備フィールド８５、下位ブロック属性フィールド８８を備える。これに対して、テーブルエントリＴＥ３は、テーブルエントリＴＥ１及びテーブルエントリＴＥ２とは異なるデータフィールドを定義している。しかしながら、ＴＥ３[58:52]とＴＥ３[11:2]は未定義である。テーブルエントリＴＥ２の未定義フィールドは、テーブルエントリＴＥ１及びＴＥ２の対応するデータフィールドと同様の定義により利用可能である。以下では、ＴＥ１[58:55]、ＴＥ２[58:55]、ＴＥ３[58:55]のデータフィールドを、Ｅｎｔｒｙ[58:55]と表す。ＴＥ１[7:6]、ＴＥ２[7:6]、ＴＥ３[7:6]のデータフィールドを、Ｅｎｔｒｙ[7:6]と表す。

【０３８１】

ＭＭＵ４６は、ステージ２のアドレス変換時に、ＨＡＰ[1:0]＝No Accessであることを検出した場合、フォールトを発生し、セキュアＶＭＭモードとなる。本実施形態においては、ＭＭＵ４６がＨＡＰに基づいてフォールトを発生する仕組みを利用して検証を行う。

【０３８２】

ソフトウェア使用予備フィールド８５のＥｎｔｒｙ[58:55]は４ビットである。ソフトウェア使用予備フィールド８５のＥｎｔｒｙ[58:55]は、２ビットの予備フラグＡ、１ビットの予備フラグＶ、１ビットの予備フラグＩを含む。

【０３８３】

予備フラグＡは、本来のＨＡＰデータの保存に用いられる。
【０３８４】
予備フラグＶは、検証の有無を示すために用いられる。
【０３８５】
予備フラグＩは、未定義とする。
【０３８６】
ＨＡＰが格納されるＥｎｔｒｙ[7:6]は、検証の実施／未実施を管理する。無効であるテーブルエントリ（未検証ブロックを指すテーブルエントリ）では、ＨＡＰ＝No Accessとする。本来のＨＡＰは、予備フラグＡに保存する。有効であるテーブルエントリでは、ＨＡＰに、No Accessではない他の値が格納される。
【０３８７】
特定のアーキテクチャ環境では、アドレス解決を行う際に、ＨＡＰを利用して意図的にＭＭＵ４６にフォールトを発生させる。これにより、セキュアＶＭＭ６８に制御を移すことが可能となり、検証処理を実行することができる。検証処理終了後は、予備フラグＡに保存していた本来のＨＡＰデータをＨＡＰフィールド８７に書き込む。
【０３８８】
図１９は、特定のアーキテクチャにおいてデータ参照要求が発生した場合のアドレス解決処理を例示するフローチャートである。ソフトウェアであるセキュアＶＭＭ６８によって実現される処理は、先で述べた処理と同様である。この図１９の説明では、セキュア検証子ツリー１２２はＭＡＣ＋カウンタ構造を持つとする。データブロックB301-1-0-511に対して、データ参照要求が発生した場合を例として説明する。
【０３８９】
ＨＡＰに基づくアクセス制御は、検証実行時に、所定機能を実現する。具体的には、例えば、ＨＡＰ＝Read-onlyであるテーブルエントリに対して、Read/Writeアクセスを行った場合には、ページ保護エラーが発生する。
【０３９０】
ＭＭＵ４６は、データブロックB301-1-0-511のアドレス解決処理を開始し、ステップＳ５０１において、ページウォークによるアドレス解決を行う。
【０３９１】
ＭＭＵ４６は、ステップＳ５０２において、テーブルブロックT301のテーブルエントリE301-1をチェックする。ＭＭＵ４６は、テーブルエントリE301-1が有効（ＨＡＰ＝0ther）であることから、テーブルエントリE301-1を参照する。
【０３９２】
ＭＭＵ４６は、ステップＳ５０３において、データブロックB301-1-0-511までのアドレスが解決したかチェックする。
【０３９３】
アドレスは未解決であるため、ＭＭＵ４６は、ステップＳ５０１のページウォークを繰り返す。
【０３９４】
ＭＭＵ４６は、ステップＳ５０２において、テーブルブロックT301-1-0のテーブルエントリE301-1-0-511をチェックする。
【０３９５】
テーブルエントリE301-1-0-511が無効（ＨＡＰ＝No Access）の場合、ＭＭＵ４６は、フォールトを発生させ、制御をセキュアＶＭＭ６８に移す。
【０３９６】
セキュアＶＭＭ６８は、ステップＳ５０４において、テーブルエントリE301-1-0-511の予備フラグＡをチェックする。
【０３９７】
セキュアＶＭＭ６８は、テーブルエントリE301-1-0-511が無効である場合(予備フラグＡ＝No Access)、ステップＳ５０５において、ページ保護エラーハンドラに制御を移し、

処理を終了する。
【０３９８】
予備フラグＡがNo Accessではない場合(予備フラグＡ＝0ther)、セキュアＶＭＭ６８は、ステップＳ５０６において、テーブルエントリE301-1-0-511の予備フラグＶをチェックする。
【０３９９】
セキュアＶＭＭ６８は、参照ブロックが検証対象外の場合(予備フラグＶ＝NV)、ステップＳ５０７において、内部エラーハンドラに制御を移し、処理を終了する。
【０４００】
セキュアＶＭＭ６８は、参照ブロックが検証対象の場合(予備フラグＶ＝V)、ステップＳ５０８において、データブロックB301-1-0-511の検証処理を行う。セキュアＶＭＭ６８は、検証処理終了後、無効であったテーブルエントリE301-1-0-511を有効にする。
【０４０１】
これにより、データブロックB301-1-0-511の参照が可能となる。セキュアＶＭＭ６８は、予備フラグＡの値をＨＡＰに書き込み、制御をＭＭＵ４６に戻す。
【０４０２】
ＭＭＵ４６は、ステップＳ５０３において、データブロックB301-1-0-511までのアドレスが解決したかチェックする。
【０４０３】
データブロックB301-1-0-511までアドレスが解決した場合には、ＭＭＵ４６は、ステップＳ５０９において、データ参照処理を再開し、アドレス解決処理を終了する。
【０４０４】
以上説明したように、本実施形態においては、セキュアページテーブルツリー１２１と改ざん検証用のセキュア検証子ツリー１２２のグラフ構造を整合させ、内部メモリ８の記憶状態を安全に管理し、効率よく検証処理を実行することができ、外部メモリ７への改ざん攻撃から厳密に情報処理装置６５を保護することができる。
【０４０５】
本実施形態においては、外部メモリ７から内部メモリ８へテーブルブロックと検証ブロックとが同時に読み込まれ、同時に検証される。これにより、情報処理装置６５は、改ざん可能な外部メモリ７のページテーブルツリー９、検証子ツリー１０及びデータを、完全性を保証した状態で、効率よく、安全に、内部メモリ８に記憶し、使用することができる。
【０４０６】
本実施形態においては、更新された内部メモリ８のセキュアページテーブルツリー１２１又はデータが外部メモリ７へ書き戻される場合に、この書き戻されるページテーブル又はデータから検証子が計算され、検証子に基づいて内部メモリ８に記憶されているセキュア検証子ツリー１２２が更新される。これにより、更新後に、ページテーブル又はデータが内部メモリ８に読み込まれる場合に、読み込まれるページテーブル又はデータの改ざんを検知することができる。
【０４０７】
本実施形態においては、ページテーブルが内部メモリ８から外部メモリ７へ書き出され、その後、当該ページテーブルが外部メモリ７から内部メモリ８へ読み込まれ、当該ページテーブルのテーブルエントリによって参照されるページテーブル又はデータが未だ内部メモリ８に記憶されていない場合に、当該テーブルエントリが無効を示すように管理される。これにより、下層のページテーブル又はデータに対する参照処理及び検証処理を正しく実行することができる。
【０４０８】
［第３の実施形態］
本実施形態は、上記第２の実施形態の変形例である。本実施形態においては、ゲストＯＳの不具合、誤動作によってセキュアＶＭＭ６８の情報が破壊されることを防止するため

に、セキュアＶＭＭ６８の情報がゲストＯＳのアクセス領域から分離される。
【０４０９】
（中間物理アドレスレベルの制限）
まず、ゲストＯＳのアクセス可能なアドレス領域の制限について説明する。ゲストＯＳに対するアドレス領域の制限には２種類の制限形態がある。
【０４１０】
第１の制限形態は、ゲストＯＳのアクセス可能な中間物理アドレス領域を制限する。
【０４１１】
図２０は、本実施形態に係るセキュアページテーブルツリー１２１及びセキュア検証子ツリー１２２に関する仮想アドレス領域の第１の制限形態を例示するブロック図である。
【０４１２】
この図２０では、ステージ２ページテーブルツリーの基本構造を例示している。ステージ２ページテーブルツリーは、中間物理アドレスから物理アドレスへの変換を定義する。
【０４１３】
ステージ２ページテーブルツリー全体をT400と表記し、データ全体をB400と表記する。
【０４１４】
セキュアＶＭＭ６８は、ＭＭＵ４６のアドレス変換機能を用いてメモリにアクセスする仮想アドレスモードと、ＭＭＵ４６を利用しない実アドレスモードとの双方で、メモリにアクセス可能である。
【０４１５】
セキュアＶＭＭ６８は、実アドレスモードにおいて無条件で全てのメモリ空間にアクセス可能である。セキュアＶＭＭ６８は、実アドレスモードを、割込ベクタを設定する際及び最初にページテーブルを設定する際に用いる。
【０４１６】
セキュアＶＭＭ６８は、仮想アドレスモードにおいて、ステージ２ページテーブルツリーT400による変換対象となっている全ての領域にアクセス可能である。
【０４１７】
上記の図７に示す物理アドレス領域７０２，７０３に配置されたページテーブルは、階層構造に一致した検証子を持つ。内部メモリ８を除く全てのメモリ領域が検証子のツリーにより検証可能である。
【０４１８】
誤動作による破壊防止のために、一般的に、ゲストＯＳに対しては、ゲストＯＳ自身に割り当てられたステージ２ページテーブルへの参照ができないように、アクセス制御がなされる。本実施形態では、このようなゲストＯＳに対するアドレス領域の制限を例として説明する。
【０４１９】
中間物理アドレス空間８９は、中間物理アドレス空間全体を表す。
【０４２０】
中間物理アドレス空間８９のうちのアドレス領域８９ａは、セキュアＶＭＭ６８がアクセス可能であり、ゲストＯＳがアクセス不可である。
【０４２１】
中間物理アドレス空間８９のうちのアドレス領域８９ｂは、ゲストＯＳとセキュアＶＭＭ６８とが共通にアクセス可能な領域である。
【０４２２】
セキュアＶＭＭ６８は、アドレス領域制限レジスタ９０に、アドレス領域８９ｂをセットする。換言すれば、アドレス領域制限レジスタ９０には、ゲストＯＳがアクセス可能なアドレス領域が設定される。アドレス領域制限レジスタ９０によるアドレス領域の制限は、ゲストＯＳの実行中に適用される。
【０４２３】
ゲストＯＳは、トップレベルのページテーブルT401からアドレス解決を開始する場合に

は、潜在的にはページテーブルT401にマッピングされた全ての物理アドレス領域にアクセス可能である。

【０４２４】

しかし、上記の中間物理アドレスレベルのアドレス領域の制限を行うことにより、変換された物理アドレスレベルでアクセス可能なアドレス領域が、物理アドレス空間９１のうちのアドレス領域９１ａに制限される。したがって、ゲストＯＳから、外部メモリ７に記憶されているセキュアＶＭＭ６８のイメージがアクセスされることを禁止することができる。また、内部メモリ８のセキュアＶＭＭプログラム領域７７がゲストＯＳからアクセスされることを禁止することができる。

【０４２５】

このような中間物理アドレスレベルでのアクセス領域の制限は、ＭＭＵ４６によるアドレス変換時に、中間物理アドレス空間８９をチェックすることで実現可能である。

【０４２６】

第２の制限形態では、最上位のページテーブルを指定するレジスタ６４により、ゲストＯＳのアドレス領域が制限される。

【０４２７】

特定のアーキテクチャでは、制御レジスタ設定により、セキュアページテーブルツリー１２１のアドレスを示すレジスタ６４のポイント先を、レベル２以降のページテーブルに設定可能である。

【０４２８】

図２１は、本実施形態に係るセキュアページテーブルツリー１２１及びセキュア検証子ツリー１２２に関する仮想アドレス領域の第２の制限形態を例示するブロック図である。

【０４２９】

例えば、レジスタ６４は、レベル２のページテーブルT401-3を指すポインタを設定する。このように、最上位のページテーブルを適宜設定可能とすることにより、アクセス可能なアドレス領域を、上記図２０の場合と同じ物理アドレス領域９１ａに制限することができる。この図２１の例では、中間物理アドレス領域８９ｃが物理アドレス領域９１ａにマップされる。

【０４３０】

（セキュア検証子ツリー１２２とアクセス制御との関係）

レジスタ６４による制限を用いる場合、ゲストＯＳ実行時に使用されるレジスタ６４は、セキュアページテーブルツリー１２１の一部であるレベル２のページテーブルT401-3を指す。当然、このページテーブルT401-3を最上位とするセキュア検証子ツリーは、レベル１のページテーブルを最上位とする全セキュア検証子ツリー１２２の一部であり、この一部のみではツリー検証を行うことができない。しかし、検証の実行はレベル１のページテーブルにアクセス可能なセキュアＶＭＭ６８が行うため、ゲストＯＳデータの検証発生時でも、上位の検証子へのアクセスが可能であり、ツリー検証を行うことができる。

【０４３１】

具体的には、ゲストＯＳの実行中にページテーブルT401-3が不在だった場合、ページフォールトが発生する。フォールトが発生するとセキュアＶＭＭ６８に制御が移り、レジスタ６４はレベル１のテーブルブロックT401を参照するよう設定される。この後に、セキュアＶＭＭ６８は、フォールトが発生したレベル２のページテーブルT401-3を、上位のレベル１のＭＡＣブロックT402を用いて、上記第２の実施形態で説明した検証処理に基づいて検証を行う。

【０４３２】

図２２は、アドレスマップと物理アドレス領域との関係を例示するブロック図である。この図２２では、上記図７で示される内部メモリ８、マスクＲＯＭ６９、セキュアＶＭＭプログラム領域７０１、物理アドレス領域７０２からセキュアＯＳページテーブル領域７０４、セキュアＶＭＭ作業領域７０５及びセキュアＶＭＭ ＭＡＣ領域７０６、予備領域７１０、非セキュアＯＳ領域７５、予備領域７１１、セキュアＯＳ領域７６ごとに、上記

図７の符号、物理アドレス領域、ブート時検証の有無、検証の有無、未検証状態ブロックの符号、サイズを示している。

【０４３３】

以上説明した本実施形態においては、ゲストＯＳとセキュアＶＭＭ６８とでアクセス可能なアドレス領域を変えることができる。これにより、例えば、ゲストＯＳとセキュアＶＭＭ６８とがセキュアページテーブルツリー１２１を共有しつつ、セキュア検証子ツリー１２２を用いた検証に関連するデータを誤動作から保護することができる。

【０４３４】

より具体的に説明すると、多機能のゲストＯＳは、潜在的な脆弱性を持つ場合がある。本実施形態では、ゲストＯＳのアクセス領域を限定し、これによりゲストＯＳの脆弱性に基づく誤動作からセキュアＶＭＭ６８を保護することができる。本実施形態において、セキュアＶＭＭ６８は、自身の作業領域をゲストＯＳから保護することができ、セキュア検証子ツリー１２２に基づく改ざん検証によってセキュアページテーブルツリー１２１を保護することができる。

【０４３５】

本実施形態においては、ゲストＯＳが誤動作した場合であっても、セキュアＶＭＭ６８の作業領域を保護し、セキュアＶＭＭ６８の健全性を保証することができる。本実施形態においては、ゲストＯＳとセキュアＶＭＭ６８とがセキュアページテーブルツリー１２１を共有することで、効率的な保証を実現することができる。

【０４３６】

本実施形態においては、セキュアＶＭＭ６８がゲストＯＳのアクセス可能なアドレス領域をレジスタ９０にセットすること、又は、レジスタ６４で示されるトップのページテーブルを任意に設定することにより、ゲストＯＳによってアクセス可能なアドレス領域を制限することができる。これにより、ゲストＯＳの不具合、誤動作によるセキュアＶＭＭ６８の情報の破壊を防止することができる。

【０４３７】

［第４の実施形態］

本実施形態においては、上記第２及び第３の実施形態の変形例について説明する。上記第３の実施形態では、ゲストＯＳとセキュアＶＭＭ６８とがセキュアページテーブルツリー１２１を共有した構成で、ゲストＯＳがアクセス可能なアドレス領域を制限する例について説明した。

【０４３８】

これに対して、本実施形態では、ゲストＯＳとセキュアＶＭＭ６８が別々のセキュアページテーブルツリーを持つ場合について説明する。本実施形態では、例えば、ゲストＯＳとセキュアＶＭＭ６８とが、個別のステージ２ページテーブルを持つことにより、ゲストＯＳがアクセス可能なアドレス領域を制限する例を説明する。

【０４３９】

上記第３の実施形態において説明した上記図２０及び図２１は、セキュア検証子ツリーと一体化した状態でセキュアＶＭＭ６８によって管理されるセキュアページテーブルツリーT400を例示している。

【０４４０】

図２３は、ゲストＯＳのステージ２ページテーブルツリーを例示するデータ構造図である。

【０４４１】

ステージ２ページテーブルツリー全体をT500と表記する。

【０４４２】

この図２３のステージ２ページテーブルツリーT500は、ページテーブルT501～T501-0-511を含む。ページテーブルT501-0-0～T501-0-511は、データB401-3-0-0～B401-3-0-511を参照する。データB401-3-0-0～B401-3-0-511は、上記第３の実施形態においてゲストＯＳが参照可能なデータ領域９１ａに配置される。

【０４４３】
例えば、初期状態では、上記図２０及び図２１に示すセキュアＶＭＭ６８のレベル１のテーブルブロックT401及び検証ブロックT402だけが内部メモリ８に記憶されている。セキュアＶＭＭ６８のレジスタ６４は、テーブルブロックT401の内部メモリ８の記憶先であるIaddr(T401)に設定される。
【０４４４】
ゲストＯＳの実行に先立って、セキュアＶＭＭ６８は、ゲストＯＳのステージ２ページテーブルT501を検証し、その後内部メモリ８に記憶する。ここでページテーブルT501はゲストＯＳ自身が管理して変更することが許されたステージ１ページテーブル(物理アドレス領域９１ａ内に配置)ではなく、ゲストＯＳ自身は操作できないことを前提としたステージ２ページテーブル（セキュアＯＳページテーブル領域７０４に配置）である。
【０４４５】
ゲストＯＳのステージ２ページテーブルツリーT500には、検証子ツリーが付随していない。ステージ２ページテーブルツリーT500の検証と読み込みでは、セキュアＶＭＭ６８がステージ２ページテーブルツリーT500を構成するテーブルブロックを、セキュアＶＭＭ６８のステージ２ページテーブルツリーT400に付随するセキュア検証子ツリーに基づいて検証し、内部メモリ８に記憶する。
【０４４６】
図２４は、本実施形態に係るデータの検証、読み込み、アクセス制御を例示するフローチャートである。
【０４４７】
ゲストＯＳの実行中は、レジスタ６４にIaddr(T501)が設定されており、ＭＭＵ４６は、ステージ２ページテーブルツリーT500によるステージ２アドレス変換を実行する。ＭＭＵ４６は、ステップＳ６０１において、データ参照のフォールトが発生すると、ステップＳ６０２において、制御をＭＭＵ４６からセキュアＶＭＭ６８へ移行する。
【０４４８】
セキュアＶＭＭ６８は、ステップＳ６０３において、レジスタ６４の値を、Iaddr(T401)に変更する。このとき、セキュアＶＭＭ６８は、中間物理アドレスが０番地だったとすると、データブロックB401-3-0-0のデータを内部メモリ８に記憶する。
【０４４９】
データブロックB401-3-0-0の検証を行うための検証子は、セキュアＶＭＭ６８で管理されているステージ２ページテーブルツリーT400においてデータブロックB401-3-0-0を参照するテーブルブロックT401-3-0に付されている。そこで、ステップＳ６０４において、セキュアＶＭＭ６８は、ステージ２ページテーブルツリーT400により、データブロックB401-3-0-0を参照するテーブルエントリE401-3-0-0を含むテーブルブロックT401-3-0のアドレスを逆解決する。このようなアドレス逆解決の方法は当業者にはよく知られている。本実施形態においては、管理用のステージ２ページテーブルツリーT400は、アドレス変換を行わない。管理用のステージ２ページテーブルツリーT400を用いることで、データブロックB401-3-0-0を参照するテーブルエントリE401-3-0-0を特定することができる。
【０４５０】
セキュアＶＭＭ６８は、ステップＳ６０５において、上記第２の実施形態の同様の処理で、ステージ２ページテーブルツリーT400に付されるセキュア検証子ツリーによる検証処理を実行する。
【０４５１】
その後、セキュアＶＭＭ６８は、ステップＳ６０６において、２つのステージ２ページテーブルT400，T500について、それぞれデータブロックB401-3-0-0を参照するテーブルエントリE401-3-0-0及びE501-1-0-0の参照先を、データブロックB401-3-0-0の内部メモリ８の記憶先であるIaddr(B401-3-0-0)に変更する。
【０４５２】
次に、セキュアＶＭＭ６８は、ステップＳ６０７において、ゲストＯＳ用のレジスタ６

４にIaddr(T501)を設定し、ゲストＯＳへの実行切り替えを行い、ステップＳ６０８において、ゲストＯＳの実行を再開する。

【０４５３】

以上説明した本実施形態においては、データブロックの読み込みについて説明したが、ゲストＯＳのステージ２ページテーブルツリーT500のテーブルブロックが未読み込みの場合も同様の処理により内部メモリ８への読み込みが実行される。

【０４５４】

本実施形態においては、ゲストＯＳのステージ２ページテーブルツリーT500とセキュアＶＭＭ６８のステージ２ページテーブルツリーT400とが完全に独立している。これにより、ゲストＯＳから参照可能な中間物理アドレスのメモリ配置とアクセス制御の自由度を高くすることが可能である。さらに、セキュアＶＭＭ６８のステージ２ページテーブルツリーT400に付属するセキュア検証子ツリーによりメモリ検証を行うことができる。

【０４５５】

本実施形態においては、ゲストＯＳのメモリ配置の自由度を高くすることによって、データの内部読み込み時に２つのセキュアページテーブルツリーT400，T500に対してデータブロック参照先を変更する書き換え処理が必要となる。この負荷を軽減する方法として、ゲストＯＳとセキュアＶＭＭ６８は、ステージ２ページテーブルツリーT400，T500におけるレベル１及びレベル２を個別に持ち、レベル３のページテーブルをゲストＯＳとセキュアＶＭＭ６８で共有してもよい。この場合、ゲストＯＳのメモリマップの自由度は、レベル３のページテーブル１個単位、この場合には２メガバイト単位と粒度が大きくなるが、頻度の高いデータブロックの読み込み処理によってステージ２ページテーブルツリーT400，T500の書き換え負荷が大きくなることを防止することができる。

【０４５６】

システムアーキテクチャによっては通信入出力などの特殊バッファメモリに、特定の物理アドレス領域（仮想化されている場合は中間物理アドレス領域）を割り当てることがある。複数のＯＳでページテーブルが共有され、１つの物理アドレス領域に１つの物理アドレスイメージしか割り当てられない場合には、複数のゲストＯＳを並列動作させることが困難である。ゲストＯＳ間だけでなく、ゲストＯＳとセキュアＶＭＭ６８との間でも、同様の衝突が発生する場合がある。しかしながら、本実施形態においては、ゲストＯＳごとに、個別の２ページテーブルツリーT400，T500を持つことができ、これにより、ゲストＯＳごとに、個別の中間物理アドレス領域を割り当てることができる。

【０４５７】

［第５の実施形態］

本実施形態においては、上記第２乃至第４の実施形態の変形例について説明する。本実施形態においては、読み込みに伴う検証とともに復号を行う。また、本実施形態においては、書き出し時に暗号化を行う。例えば、単純なＭＡＣの代わりに、認証付き暗号利用モードであるＣＣＭ(Counter with CBC-MAC)モードを利用する。これにより、検証子の計算と同時に効率的に暗号化を行うことができる。暗号化及び復号は、ＭＡＣの計算及び検証に併せて実行されてもよいが、他の様々な実装により暗号化及び復号が実行されてもよい。

【０４５８】

本実施形態のように、内部メモリ８から外部メモリ７へ移動されるページテーブル又はデータを暗号化し、外部メモリ７から内部メモリ８へ移動されるページテーブル又はデータを復号することにより、完全性に加えて、機密性を保証することができる。

【０４５９】

［第６の実施形態］

本実施形態においては、上記第２乃至第５の実施形態の変形例について説明する。

【０４６０】

本実施形態では、データブロックの改ざん検証の計算に中間物理アドレスを用い、ゲストＯＳごとのセキュアページテーブルツリー及びセキュア検証子ツリーを備える場合を説

明する。

【０４６１】

本実施形態においては、ゲストＯＳごとのセキュアページテーブルツリーが、それぞれ独立にセキュア検証子ツリーと対応付けられる。本実施形態においては、上記第４の実施形態のように、ページテーブル又はデータの読み込みに基づいて、影響を受けるゲストＯＳに対するセキュアページテーブルツリーとセキュアＶＭＭ６８に対する共通のセキュアページテーブルとを更新する必要はなく、影響を受けるゲストＯＳに対するセキュアページテーブルツリーだけを更新すればよい。

【０４６２】

図２５は、本実施形態に係るゲストＯＳごとのセキュアページテーブルツリーを例示するデータ構造図である。

【０４６３】

第１のゲストＯＳのセキュアページテーブルツリーT600は、データB600を参照する。セキュアページテーブルツリーT600には、第１のゲストＯＳのセキュア検証子ツリー９２１が付されている。図２５において、第１のゲストＯＳは、実行中であり、レジスタ６４には、セキュアページテーブルツリーT600の最上位テーブルT601のアドレスが格納される。

【０４６４】

第２のゲストＯＳのセキュアページテーブルツリーT700は、データB700を参照する。ページテーブルツリーT700には、第２のゲストＯＳのセキュア検証子ツリー９２２が付されている。図２５において、第２のゲストＯＳは、待機状態とする。

【０４６５】

レジスタ６４には、第１のゲストＯＳの実行中に、第１のゲストＯＳに対応するセキュアページテーブルツリーT600のアドレスが設定される。レジスタ６４には、第２のゲストＯＳの実行中に、第２のゲストＯＳに対応するページテーブルツリーT700のアドレスが設定される。図２５では、第１のゲストＯＳが実行中であるため、レジスタ６４に、第１のゲストＯＳに対応するセキュアページテーブルツリーT600のアドレスが設定されている。本実施形態では、内部メモリ８に読み込まれた状態のページテーブルによって形成されるツリー及び検証子によって形成されるツリーは、その時点で、レジスタ６４から参照されアドレス変換に使われているか否かに関わらず、セキュアページテーブルツリー及びセキュア検証子ツリーと呼ぶ。

【０４６６】

上記第３及び第４の実施形態と比較して、本実施形態は、以下の第１乃至第３の特徴を持つ。

【０４６７】

本実施形態の第１の特徴は、ゲストＯＳのセキュアページテーブルツリーT600，T700ごとにセキュア検証子ツリー９２１，９２２を備えることである。

【０４６８】

第２の特徴は、データとページテーブルとで検証子の計算に用いられるアドレスが異なることである。データブロックB601-0-0-0～B601-0-0-511の検証子の計算に使うアドレス値としては、図３のような物理アドレスではなく中間物理アドレスを使うとする。

【０４６９】

第３の特徴は、セキュア検証子ツリー９２１，９２２のルート検証情報１３１，１３２をゲストＯＳごとに個別に保持することである。ルート検証情報１３１，１３２は、秘密鍵と最上位の検証子との組み合わせとする。

【０４７０】

図２６は、本実施形態に係る情報処理装置の構成を例示するブロック図である。

【０４７１】

情報処理装置９３のＭＭＵ４６は、レジスタ６４を備える。検証管理部７９は、ルート検証切替部（ルート検証情報切替部）７９ｄを備える。記憶領域管理部８３は、ルート検証特定部（ルート検証情報特定部）８３ｄを備える。

【０４７２】
本実施形態に係る情報処理装置９３の動作において、上記第３及び第４の実施形態と異なるのは、検証の実行及び置き換えであり、他の動作は共通である。
【０４７３】
本実施形態では、２つのゲストＯＳのそれぞれに個別のセキュア検証子ツリー９２１，９２２が用いられる場合を例として説明するが、さらに、セキュアＶＭＭ６８のプログラムイメージおよびデータについて、独自のセキュア検証子ツリーが用いられてもよい。
【０４７４】
ゲストＯＳのステージ２ページテーブルツリー及び検証子ツリーは、かなり大きなサイズとなる場合がある。ゲストＯＳのステージ２ページテーブルツリーはセキュアＶＭＭ６８が管理するデータであり、当然改ざん防止が必要となる。セキュアＶＭＭ６８で管理されるデータを独立のセキュア検証子ツリーで検証する場合の動作の説明は、ゲストＯＳのデータ検証とセキュアＶＭＭ６８のデータ検証とが並行して行われるため煩雑となる。本実施形態では、説明を単純にするため、２つのゲストＯＳが独立のセキュア検証子ツリー９２１，９２２を持つ例を説明する。しかしながら、セキュアＶＭＭ６８で管理されるデータを独立のセキュア検証子ツリーにより検証することも可能である。
【０４７５】
（検証処理の詳細）
図２７は、本実施形態に係る情報処理装置９３の検証処理を例示するフローチャートである。この検証処理は、テーブルブロックT601-0-0の検証処理を例として説明する。
【０４７６】
セキュアＶＭＭ６８は、テーブルブロックT601-0-0の検証処理を開始し、ステップＳ７０１において、内部メモリ８の検証バッファ領域７２に空き領域が存在しているかチェックする。
【０４７７】
セキュアＶＭＭ６８は、空き領域がない場合に、ステップＳ７０２の置き換え処理により領域の解放を行う。
【０４７８】
続いて、セキュアＶＭＭ６８はステップＳ７０３において、以下で行う検証処理のルート検証情報として、フォールト発生時に実行していた第１のゲストＯＳのルート検証情報１３１を選択する。
【０４７９】
セキュアＶＭＭ６８は、ステップＳ７０４において、検証対象テーブルブロックT601-0-0、この検証対象テーブルブロックT601-0-0に関連付けられている検証ブロックT602-0-0，T603-0-0を外部メモリ７のアドレスEaddr(T601-0-0)から内部メモリ８の検証バッファ領域７２の空き領域へコピーする。
【０４８０】
ステップＳ７０５において、セキュアＤＭＡコントローラ５２は、検証対象テーブルブロックT601-0-0及び検証ブロックT602-0-0，T603-0-0の検証処理を実行する。セキュアＶＭＭ６８は、読み込まれた検証対象テーブルブロックT601-0-0及び検証ブロックT602-0-0，T603-0-0を記憶するバッファ領域ごとに、対応するゲストＯＳＩＤを記憶する。
【０４８１】
その後の検証処理のステップＳ７０６～Ｓ７０８は、上記第２の実施形態の図１４のステップＳ２０５～Ｓ２０７と同様である。
【０４８２】
本実施形態に係るデータの検証処理と上記図２６に示す情報処理装置９３の構成との関係を、上記図２７を流用して説明する。この説明では、上記図２５のデータブロックB601-0-0-0に対して検証処理が実行される場合を例として説明する。
【０４８３】
検証管理部７９は、ステップＳ７０１において、記憶領域管理部８３のバッファ管理部

８３ｂに、検証記憶部８４の空きバッファ領域の有無を照会する。
【０４８４】
空き領域がない場合、検証管理部７９は、ステップＳ７０２において、記憶領域管理部８３に読み込み済みバッファ領域の解放を要求し、空き領域のアドレスを取得する。
【０４８５】
検証管理部７９の検証情報取得部７９ａは、検証記憶部８４に存在する上位検証ブロックのＭＡＣブロックT602-0-0及びカウンタブロックT603-0-0に含まれるＭＡＣ値M601-0-0-0及びカウンタ値C601-0-0-0を取得する。
【０４８６】
本実施形態は、ルート検証切替部７９ｄが、ステップＳ７０３において、鍵保存ユニット６７に記憶されている現在実行中のゲストＯＳの秘密鍵、及び、必要であればルート検証情報１３１を取得し、検証情報取得部７９ａに引き渡す特徴を持つ。
【０４８７】
検証情報取得部７９ａは、ステップＳ７０４において、外部読込部８１を通じて、検証対象データブロックB601-0-0-0を外部メモリ７から検証記憶部８４の空き領域に移動する。
【０４８８】
検証情報計算部７９ｃは、Ｓ７０５において、検証対象データブロックB601-0-0-0、上位のカウンタブロックT603-0-0に含まれているカウンタ値C601-0-0-0、秘密鍵に基づいて、ＭＡＣ値を計算する。本実施形態は、記憶領域管理部８３が、ルート検証特定部８３ｄにゲストＯＳＩＤを通知し、ルート検証特定部８３ｄがバッファ領域ごとにゲストＯＳＩＤを記憶する特徴を持つ。改ざん判定部７９ｂは、計算されたＭＡＣ値を取得済みのＭＡＣ値M601-0-0-0と照合する。
【０４８９】
ステップＳ７０６においてＭＡＣ値が整合せず検証に失敗した場合、検証管理部７９は、ステップＳ７０７において、命令実行ユニット４５に検証失敗を通知し、その後の処理を中止する。
【０４９０】
ステップＳ７０６においてＭＡＣ値が整合して検証に成功した場合、検証管理部７９は、参照関係更新部８３ａに読み込み成功を通知する。ステップＳ７０８において、参照関係更新部８３ａは、無効となっていたテーブルエントリの参照先アドレスとして、検証対象データブロックB601-0-0-0の検証記憶部８４のアドレスIaddr(B601-0-0-0)を書き込む。
【０４９１】
さらに、参照関係更新部８３ａは、データブロックB601-0-0-0の外部メモリ７のアドレスEaddr(B601-0-0-0)を、バッファブロック単位にバッファ管理情報領域７３に記憶し、検証処理を終了する。
【０４９２】
（検証子計算に用いるブロックアドレス）
本実施形態では、データブロックとテーブルブロックで検証子の計算に用いられるアドレスが異なる。
【０４９３】
データブロックB601-0-0～B601-0-511及びデータブロックB701-0-0～B701-0-511の検証子の計算に使用されるアドレスは、物理アドレスではなく中間物理アドレスでもよい。本実施形態では、それぞれのセキュア検証子ツリー９２１，９２２に個別のルート検証情報１３１，１３２が割り当てられるため、複数のゲストＯＳがデータブロックの検証子の計算に中間物理アドレスを使ったとしても検証子の衝突は起きない。他方、検証子の計算に中間物理アドレスを使うことにより、ある中間物理アドレスに対応するデータが配置される物理アドレスは、自由に変更されてもよく、実装の自由度を上げることができる。
【０４９４】

しかしながら、ステージ２セキュアページテーブルツリーT600，T700に含まれるテーブルブロックの検証子は、物理アドレスに基づいて計算される。テーブルブロックは、ゲストＯＳのコンテキストであり、テーブルブロックには中間物理アドレスが割り当てられていないためである。テーブルブロックの再配置ができなくても、テーブルブロックの参照関係を明示的に変更することで、同様の効果を得ることができる。

【０４９５】

（追い出し処理の詳細）

図２８は、本実施形態に係る情報処理装置９３の追い出し処理を例示するフローチャートである。この図２８に示す追い出し処理は、例えば、上記図１５に示す置き換え処理で発生する。

【０４９６】

追い出し対象となるテーブルブロックは、例えば上記図２５で示す第２のゲストＯＳのテーブルブロックT701-0-0とする。

【０４９７】

追い出し対象のテーブルブロックT701-0-0に代わって、内部メモリ８に記憶される読み込み対象のテーブルブロックは、第１のゲストＯＳのテーブルブロックT601-0-0とする。

【０４９８】

追い出し対象のテーブルブロックT701-0-0のカウンタ値C701-0-0は、内部メモリ８に記憶されている。テーブルブロックT701-0-0のＭＡＣ値M701-0-0は、外部メモリ７に記憶されている。外部メモリ７のＭＡＣ値M701-0-0は、外部メモリ７のテーブルブロックT701-0-0のＭＡＣ値である。よって、内部メモリ８で更新されたテーブルブロックT701-0-0を外部メモリ７へ書き戻す場合には、ＭＡＣ値M701-0-0の更新処理が必要となる。内部メモリ８のテーブルブロックT701-0-0が更新されていない場合は、外部メモリ７と内部メモリ８でテーブルブロックT701-0-0の内容に差分がないことから、ＭＡＣ値M701-0-0の更新処理は必要ない。

【０４９９】

上記第２の実施形態では、追い出し対象のテーブルブロックと、この追い出しの契機となる読み込み対象のテーブルブロックとは、同じゲストＯＳのページテーブル要素である。

【０５００】

しかしながら、本実施形態においては、追い出しの契機となる読み込み対象のページテーブルT601-0-0は、第１のゲストＯＳの実行によって発生しているのに対し、追い出し対象のページテーブルT701-0-0は第２のゲストＯＳの実行によって発生している。すなわち、本実施形態では、異なるゲストＯＳで、読み込みと追い出しとが発生している。さらに、この２つのゲストＯＳは、セキュアページテーブルツリーT600，T700、セキュア検証子ツリー９２１，９２２ばかりでなくルート検証情報１３１，１３２もそれぞれ個別に持つ。

【０５０１】

このような特徴に基づいて、本実施形態では、セキュアＶＭＭ６８は、ステップＳ８０１において、追い出し対象テーブルブロックT701-0-0の更新をチェックする。

【０５０２】

追い出し対象テーブルブロックT701-0-0が更新されている場合、ステップＳ８０２において、セキュアＶＭＭ６８は、追い出しを行うセキュアページテーブルツリーT700のルート検証情報１３２を取得し、追い出しを行うセキュアページテーブルツリーT700を認識する。すわわち、セキュアＶＭＭ６８は、これまで実行中であった第１のゲストＯＳのルート検証情報１３１ではなく、第２のゲストＯＳのルート検証情報１３２を取得する。

【０５０３】

セキュアＶＭＭ６８は、ステップＳ８０３において、第２のゲストＯＳのルート検証情報１３２を使って、追い出し対象テーブルブロックT701-0-0のＭＡＣ更新処理を実行する。

【０５０４】
セキュアＶＭＭ６８は、ステップＳ８０４において、書き出し先物理アドレスの決定を、第２のゲストＯＳのセキュアページテーブルツリーT700の逆変換又は読み込み時の物理アドレスを保持しておくなどの方法により解決する。
【０５０５】
ステップＳ８０５，Ｓ８０６は、上記第２の実施形態で説明した図１６のステップＳ４０４，Ｓ４０５と同様である。
【０５０６】
上記のようなページテーブルに関する追い出し処理及びその周辺処理と、上記図２６に示す情報処理装置９３の構成とを関連付けて説明する。
【０５０７】
ステップＳ２０１、ステップＳ２０２において、検証管理部７９は、記憶領域管理部８３に空きバッファを要求する。記憶領域管理部８３は、バッファ領域管理部８３ｂを参照し、空きバッファを探す。
【０５０８】
記憶領域管理部８３は、空きバッファがない場合に、ステップＳ３０２において、追い出し対象ページテーブルとなるバッファ領域を所定のアルゴリズムにより選択する。バッファ書出管理部８３ｃは、ステップＳ８０１において、バッファ領域管理部８３ｂによって選択された追い出し対象ページテーブルに対して、当該バッファ領域の更新有無を判断する。
【０５０９】
更新ありの場合、ステップＳ８０２において、ルート検証特定部８３ｄは、追い出しを行う場合に、追い出しバッファに対応するゲストＯＳＩＤを取得し、対応するルート検証情報１３１又は１３２を取得し、セキュアページテーブルツリーT600，T700を認証する。
【０５１０】
ルート検証特定部８３ｄは、検証情報生成部８０にルート検証情報１３１又は１３２を通知する。
【０５１１】
ステップＳ８０３において、検証情報生成部８０は、追い出し対象ページテーブルのＭＡＣ更新処理を行う。
【０５１２】
ステップＳ８０４において、バッファ領域管理部８３ｂは、書き出し先となる外部メモリ７のアドレスを決定する。
【０５１３】
ステップＳ８０５において、外部書出部８２は、追い出し対象ページテーブル及び生成された検証子を外部メモリ７に書き出す。
【０５１４】
バッファ領域からの書き出しが完了すると、ステップＳ８０６において、参照関係更新部８３ａは、ページテーブルの参照関係を更新する。
【０５１５】
（ＯＳ切替処理）
図２９は、本実施形態に係るＯＳ切り替え処理を例示するフローチャートである。
【０５１６】
セキュアＶＭＭ６８は、ステップＳ９０１において切替先のゲストＯＳを決定し、ステップＳ９０２においてルート検証情報１２１，１２２を切り替え、ステップＳ９０３においてレジスタ６４を書き換え、ステップＳ９０４において切替先のゲストＯＳの実行を開始する。
【０５１７】
以上説明した本実施形態においては、ゲストＯＳごとにセキュアページテーブルツリーT600，T700及びセキュア検証子ツリー９２１，９２２を生成し、ゲストＯＳの切り替えに

応じてセキュアページテーブルツリーT600，T700及びセキュア検証子ツリー９２１，９２２を切り替える。これにより、ゲストＯＳごとのセキュアページテーブルツリーT600，T700の更新を効率的に行うことができる。

【０５１８】

本実施形態においては、中間物理アドレスを用いてデータの検証子を計算することにより、データの改ざん検証に中間物理アドレスを用いることができる。

【０５１９】

［第７の実施形態］

上記の各実施形態においては、情報処理装置６５，９３の全体のメモリイメージ、又は、それぞれのゲストＯＳ全体のメモリイメージが、１つのルート検証情報１３，１３１，１３２に集約される。換言すれば、上記各実施形態は、情報処理装置６５，９３全体のメモリ内容、又は、それぞれのゲストＯＳのメモリ内容が１ビットでも変化した場合、その変化はルート検証情報１３，１３１，１３２の変化となって現れる性質を持つ。

【０５２０】

本実施形態は、この性質を利用して、情報処理装置６５，９３のメモリ内容が、正常な動作を含めて、ある時点から変化していないことを確認する機能を実現する。この機能は、事故あるいは犯罪行為などが発生した時点の情報処理装置６５，９３の状態を保全(Perpetuation of evidence)する、いわゆるデジタルフォレンジックに関する。

【０５２１】

図３０は、本実施形態に係る情報処理システムを例示するシステム構成図である。

【０５２２】

図３１は、本実施形態に係る情報処理システムの構成を例示するブロック図である。

【０５２３】

図３２は、本実施形態に係る情報処理システムのフォレンジック処理を例示するフローチャートである。

【０５２４】

情報処理システム９４は、情報処理装置（データ参照装置）９５と、管理サーバ９６とが、ネットワーク９７経由で通信可能に接続された構成を持つ。

【０５２５】

情報処理装置９５は、上記の情報処理装置６５，９３と同様の構成を持ち、さらに署名生成部９５１、メッセージ送信９５２を備える。

【０５２６】

ステップＳ１００１において、情報処理装置９５に備えられるセキュアＶＭＭ６８は、管理サーバ９６からの通知又は自律的な異常検出機能などに基づいて、情報の保全処理を開始する。

【０５２７】

ステップＳ１００２において、セキュアＶＭＭ６８は、保全処理対象がゲストＯＳの場合、ゲストＯＳの実行を停止し、停止状態において検証記憶部８４に記憶されたデータ、セキュアページテーブルツリー１２１、セキュア検証子ツリー１２２を外部メモリ７に順次書き出す。

【０５２８】

ステップＳ１００３において、署名生成部９５１は、外部メモリ７への書き出しが完了すると、鍵保存ユニット６７に記憶されているルート検証情報のＭＡＣ値とシステム時刻とに対して、鍵保存ユニット６７に記憶されているフォレンジック署名用の秘密鍵を用いて、フォレンジック情報（署名情報）を生成する。

【０５２９】

ステップＳ１００４において、メッセージ送信部９５２は、生成されたフォレンジック情報を、ネットワーク９７経由で所定の管理サーバ９６に送信する。ルート検証情報のうちＭＡＣ生成用の秘密鍵は、外部に開示することが不適切であるため送信しない。

【０５３０】

以上説明した本実施形態においては、情報処理装置９５を回収した機関は、正当な法的権限に基づいて管理サーバ９６で管理されているフォレンジック情報と、情報処理装置９５内部のゲストＯＳのルート検証情報とを比較する。

【０５３１】

もしフォレンジック情報が生成された時点より後に、何者かが情報処理装置９５のデータを改ざんした場合、当然に、ルート検証情報が変化するため、不正を検出することができる。

【０５３２】

フォレンジックの観点からは、メモリに対する物理攻撃だけでなく、正常な稼働による記録の上書きなども不正行為となる。本実施形態のようにフォレンジック情報を送信し、保存しておくことにより、このような不正行為を検出することができる。

【０５３３】

［第８の実施形態］

本実施形態においては、上記第１乃至第７の実施形態の変形例について説明する。

【０５３４】

本実施形態においては、外部メモリ７から内部メモリ８へコピーされるデータに対して、毎回検証を行うか、１回だけ検証を行うか、検証を行わないか、判断する。なお、本実施形態において、外部メモリ７から内部メモリ８へコピーされるテーブルに対しては、例えばデータ保護方式などのテーブルに含まれている各種の設定情報が外部の攻撃者によって変更されることを防止するために、毎回検証が行われるとする。これにより、データの検証のレベルを適切化することができ、プロセッサ６６の処理速度が低下することを防止することができる。本実施形態において、電源投入から電源断までの間でプロセッサ６６に読み込まれるデータの検証は毎回実行か、１回実行か、検証なしか判断されるが、例えば、検証の回数は、毎回又は１回に限定されるものではなく、２回以上など他の回数としてもよい。

【０５３５】

外部メモリ７から内部メモリ８へコピーされるデータが毎回検証される場合には、プロセッサ６６の稼働中にデータ保護が可能である。データ保護には、例えば、改ざんの検証、暗号化による安全性の確保などが含まれる。しかしながら、内部メモリ８のサイズより大きなデータがプロセッサ６６で実行される場合（例えば、内部メモリ８のサイズより大きなプログラムがプロセッサ６６で実行される場合）には、内部メモリ８に格納されていないデータ（例えば、プログラム）の参照が発生しやすく、キャッシュミスの発生が増え、ページングを実行するためにオーバーヘッドが大きくなる。

【０５３６】

一方で、プロセッサ６６が稼働中の不揮発メモリに対するデータ改ざん及び窃視攻撃は、プロセッサ６６が停止中の不揮発メモリに対するデータ改ざん及び窃視攻撃と比較して困難性が高いため、プロセッサ６６の用途によっては、あえてデータ改ざん及び窃視攻撃への対策をプロセッサ６６の停止中に限定し、プロセッサ６６が稼働中のデータ改ざん及び窃視攻撃による攻撃リスクを許容し、プロセッサ６６が稼働中のオーバーヘッドの削減をデータ保護より優先してもよい。

【０５３７】

以下では３種類のデータ保護方式が混在するプロセッサ６６について説明する。３種類のデータ保護方式の動作概要を以下に示す。

【０５３８】

第１のデータ保護方式は、毎回検証（ETV: Each Time Verification)である。毎回検証は、外部メモリ７から内部メモリ８へデータがコピーされる場合に、毎回、検証されたデータを内部メモリ８に格納する。例えば、内部メモリ８は、ＳＲＡＭ（Static Random Access Memory）のバッファメモリである。内部メモリ８からあふれるデータは外部メモリ７に書き出される。毎回検証では、内部メモリ８から外部メモリ７への書き出し時に、毎回、例えば、ＭＡＣ値などの検証子が更新される。内部メモリ８から外部メモリ７への書

き出し時に暗号化を行い、外部メモリ７から内部メモリ８への読み出し時に復号を行うとしてもよい。

【０５３９】

第２のデータ保護方式は、１回検証（OTV: One Time Verification）である。１回検証は、電源投入後の初回のデータ参照時のみ、外部メモリ７のデータに対して直接検証を行う。外部メモリ７のデータが暗号化されている場合には、外部メモリ７のデータが復号される。その後、外部メモリ７のデータに対する２回目以降の参照では、外部メモリ７のデータが検証及び復号されることなく、直接参照される。プロセッサ６６の電源断の前に、復号された状態のデータは、再度暗号化され、データに対する検証子が更新される。

【０５４０】

第３のデータ保護方式は、検証なし(NOV: No Verification)である。検証なしでは、プロセッサ６６は、外部メモリ７のゲストＯＳのデータを、検証処理を実行することなく直接参照する。

【０５４１】

本実施形態において、電源投入及び電源断は、ゲストＯＳの再起動なしにソフトウェアの実行状態をメモリに維持したまま電源を断するいわゆるノーマリーオフ動作を含む。

【０５４２】

複数のデータ保護方式が混在する場合には、悪影響を与える相互作用を排除する必要がある。本実施形態において、あるデータ（ページデータ）に対するデータ保護方式は、仮想マシンモニタ（セキュアＶＭＭ６８）が管理する内部情報と、ページテーブルにおけるデータ保護方式の設定情報によって決められる。複数のデータ保護方式のいずれであっても、ページテーブルの改ざんが防止されることにより、外部の攻撃者がデータ保護方式を変更することはできない。

【０５４３】

本実施形態では、複数のデータ保護方式ごとに、データが保護されるレベル、換言すればデータの安全性の高低、が異なる。しかしながら、複数のデータ保護方式のいずれであっても、データ保護方式を設定するページテーブル自体に対しては毎回検証が実行され、ページテーブルは保護され、稼働中のデータ改ざんを含む攻撃から保護される。、本実施形態の冒頭でも説明されているが、このように、ページテーブルに対して毎回検証を適用することで、ページテーブルに含まれる各種の設定情報の保護レベルを高くすることができる。したがって、本実施形態では、低い保護レベルのデータが改ざんされたとしても、その被害はより高い保護レベルのデータには及ばないことが担保できる。停止中のデータ改ざんにより、検証なしのデータ保護方式のデータが改ざんされたとしても、１回検証及び毎回検証のデータ保護方式のデータは、影響を受けない。また、ゲストＯＳがセキュアＶＭＭ６８で管理されるページテーブルを直接操作することはできない。例えば、第１のゲストＯＳが、当該第１のゲストＯＳと第２のゲストＯＳとの間に共有メモリ領域を設定する場合、第１のゲストは、ＶＭＭにサービス要求を発行し、間接的にページテーブルの設定が変更される可能性はある。しかしながら、このようなページテーブルの設定の変更を許可する条件が十分に検討されていれば、第１のゲストＯＳから第２のゲストＯＳのデータを無差別に破壊するような攻撃は排除できる。したがって、複数のデータ保護方式が混在していても、本実施形態では、悪影響を与える相互作用を排除することができる。

【０５４４】

（１回検証の動作）

外部メモリ７が不揮発性の主記憶装置の場合の１回検証の動作について説明する。

【０５４５】

１回検証は、上記第２の実施形態で説明した図２と同様の構成によって実現可能である。

【０５４６】

図３３は、本実施形態に係るページテーブルエントリのフィールド形式を例示するデータ構造図である。この図３３のページテーブルエントリは、上記図１７のページテーブル

エントリの変形例である。

【０５４７】

データブロックを参照するテーブルエントリＴＥ１，ＴＥ２は、ソフトウェア使用予備フィールド８５を含む。

【０５４８】

ソフトウェア使用予備フィールド８５及び有効／無効フラグ８５４は、データ保護形式と保護対象データの状態とを制御するための制御フィールドとして用いられる。例えば、ソフトウェア使用予備フィールド８５は、データ保護方式フィールド８５１、暗号化フィールド８５２、使用状態フィールド８５３を含む。

【０５４９】

データ保護方式フィールド（PTF:Protection Type Field）８５１に設定される情報は、毎回検証、１回検証、検証なし、予備、のいずれかを示す。

【０５５０】

暗号化フィールド８５２に設定されている情報は、暗号化による保護あり、又は、暗号化による保護なし、を示す。

【０５５１】

使用状態フィールド８５３は、１回検証のために設けられているフィールドである。使用状態フィールド８５３に設定されている情報が使用中を示す場合、データは検証済み（暗号化ありの場合復号済み）であることを示す。使用状態フィールド８５３に設定されている情報が未使用（未検証）を示す場合、データは電源投入後、データが未参照の状態であり、データは未検証であることを示す。

【０５５２】

さらに、ページテーブルエントリは、当該ページテーブルエントリが有効か無効かを示す有効／無効フラグ８５４を含む。

【０５５３】

（複数のデータ保護方式の動作）

図３４は、本実施形態に係る、データ保護方式ごとのデータのコピー状態及び検証状態を例示する状態遷移図である。この図３４では、外部メモリ７がＭＲＡＭであり、内部メモリ８がＳＲＡＭであるとする。

【０５５４】

図３５は、複数のデータ保護方式におけるページテーブルエントリの制御フィールドの状態、ページテーブルエントリが有効か否かを示す有効／無効フラグ８５４、次回参照データの状態、次回参照データの状態を示す符号、の関係を例示する図である。有効／無効フラグ８５４は、換言すれば、アドレス変換の可能／不可能を表す。

【０５５５】

例えば、使用状態フィールド８５３に１が設定されている場合には使用中を示し、０が設定されている場合には未使用を示す。

【０５５６】

例えば、有効／無効フラグ８５４が１の場合は有効を示し、０の場合は無効を示す。有効／無効フラグ８５４が有効の場合、ページテーブルエントリで参照されるデータは命令実行ユニット４５で利用可能である。有効／無効フラグ８５４が無効の場合、ページテーブルエントリで参照されるデータは命令実行ユニット４５で利用可能ではない。

【０５５７】

以下の説明で、次回参照データとは、ゲストＯＳのあるデータがコピーされた結果、同時に複数の場所（例えば、外部メモリ７と内部メモリ８の双方）に格納されている場合に、次にセキュアＶＭＭ６８又はゲストＯＳによって実際に利用されるデータを意味する。例えば、毎回検証において、内部メモリ８にデータが読み込まれていない状態では、内部メモリ８に読み込まれる前の、外部メモリ７に格納されており未検証の状態ＮＤ１のデータが次回参照データである。そして、外部メモリ７の状態ＮＤ１のデータが検証され、内部メモリ８に読み込まれた場合、内部メモリ８に格納されている検証済みの状態ＮＤ２の

データが次回参照データである。内部メモリ８における次回参照データに対しては、ゲストＯＳによる参照又は追い出しが行われる。内部メモリ８の状態ＮＤ２のデータに対して検証子（たとえば、ＭＡＣ値）が再計算され、状態ＮＤ２のデータが外部メモリ７に格納され、内部メモリ８の状態ＮＤ２のデータが消去された場合には、次は、外部メモリ７に格納されており未検証の状態ＮＤ１のデータが次回参照データになる。

【０５５８】

毎回検証において、データは状態ＮＤ１と状態ＮＤ２との間を遷移する。状態ＮＤ１と状態ＮＤ２とでは、データイメージの格納される位置、検証実行及びＭＡＣ値計算などの状態が異なる。毎回検証では、次回参照データが状態ＮＤ１（外部メモリ７の未検証）の場合に、次回参照データに必ず検証を行い、暗号化保護ありの場合には次回参照データを復号し、次回参照データを内部メモリ８に格納する。命令実行ユニット４５によるデータ参照は、状態ＮＤ２（内部メモリ８の検証済み）の次回参照データに対して行われる。状態ＮＤ２の次回参照データが外部メモリ７に書き出される場合には、次回参照データのＭＡＣ値が計算され、暗号化保護ありの場合には次回参照データが暗号化され、次回参照データが外部メモリ７に格納され、外部メモリ７に格納された次回参照データは状態ＮＤ１（外部メモリ７の未検証）となる。このように暗号化保護ありの場合、外部メモリ７から内部メモリ８への次回参照データのコピーにおいて復号が実行され、内部メモリ８から外部メモリ７への次回参照データの書き出しにおいて暗号化が実行される。再度、外部メモリ７から内部メモリ８へ次回参照データがコピーされる場合には、外部メモリ７の状態ＮＤ１の次回参照データが読み込まれ、検証され、復号され、内部メモリ８に格納され、次回参照データは状態ＮＤ２となる。データ参照は、状態ＮＤ２の次回参照データに対して行われる。

【０５５９】

１回検証において、データは状態ＮＤ３と状態ＮＤ４との間を遷移する。本実施形態に係る１回検証では、状態ＮＤ３と状態ＮＤ４のいずれの場合であっても、データイメージの格納されるアドレスは同一としてもよい。１回検証では、次回参照データが状態ＮＤ３（外部メモリ７の未検証）の場合に、内部メモリ８へのコピーを行わずに外部メモリ７上で次回参照データの検証を行う。暗号化保護ありの場合には、外部メモリ７の次回参照データが検証とともに復号される。外部メモリ７で使用中の状態ＮＤ４（外部メモリ７の検証済み）の次回参照データに対するＭＡＣ値の更新は次回電源断までに行われる。電源断時には、状態ＮＤ４の次回参照データは、状態ＮＤ３（外部メモリ７の未使用）に戻される。暗号化保護ありの場合には、外部メモリ７における状態ＮＤ４の次回参照データに対して、再暗号化が実行され、その後、再暗号化された次回参照データは、状態ＮＤ３となる。

【０５６０】

検証なしでは、外部メモリ７における状態ＮＤ５の次回参照データに対して検証が行われない。命令実行ユニット４５は、外部メモリ７に格納されており未検証の状態ＮＤ５の次回参照データを参照可能である。この検証なしでは、電源断における終了処理も行われない。

【０５６１】

なお、上記のデータ書き出し、ＭＡＣ値の計算、データの再暗号化は、上記第２の実施形態で説明したように、データが更新された場合のみ行うとしてもよい。したがって、上記第２の実施形態のように、データ書き出し、ＭＡＣ値の計算、データの再暗号化の前に、データ更新有無の判定が実行されてもよいが、以下では説明を簡素化するために、データが更新された場合の動作のみを説明する。

【０５６２】

ページテーブルについては毎回検証を行うため、上記第１及び第２の実施形態と同様である。説明を簡素化するために、本実施形態では、データに対する検証のみを説明し、ページテーブルの検証については説明を省略する。

【０５６３】

（検証処理）
以下においては、検証処理のうち上記第２の実施形態と異なる部分を説明する。
【０５６４】
読み込み対象のデータのページテーブルエントリは、電源投入後の初期状態において、以下の状態のいずれかを含む。
【０５６５】
毎回検証(ETV)：Ｄ／Ｆフラグ＝Ｆ：有効／無効フラグ＝０（状態ＮＤ１）
１回検証(OTV)：Ｄ／Ｆフラグ＝Ｆ：有効／無効フラグ＝０（状態ＮＤ３）
検証なし(NOV)：Ｄ／Ｆフラグ＝Ｆ：有効／無効フラグ＝０（状態ＮＤ５）
初期状態において制御フィールドにこの情報が設定されるための電源断処理については後述する。
【０５６６】
上述のように１回検証の場合であっても、ページテーブルはすべて毎回検証される。したがって、データ検証までの処理は上記第１及び第２の実施形態と同様である。以下では、上記第１及び第２の実施形態と異なる処理についてのみ説明する。
【０５６７】
図３６は、本実施形態に係る複数のデータ保護方式に対応する検証処理を例示するフローチャートである。
【０５６８】
この図３６は、上記図１２のアドレス解決処理のステップＳ１０３における検証処理として実行可能である。
【０５６９】
まず、ステップＳ２０Ａにおいて、セキュアＶＭＭ６８は、データを参照するページテーブルエントリで設定されているデータ保護方式を判断する。
【０５７０】
データ保護方式が毎回検証の場合には、処理はステップＳ２０１に移動する。
【０５７１】
データ保護方式が１回検証の場合には、処理はステップＳ２０Ｄに移動する。
【０５７２】
ステップＳ２０３の後、セキュアＶＭＭ６８は、ステップＳ２０Ｂにおいて、内部メモリ８のデータに対する検証を実行する。このステップＳ２０Ｂの処理は、後述の図３７で説明する。ステップＳ２０Ｂの後、処理はステップＳ２０５に移動する。
【０５７３】
ステップＳ２０７の後、セキュアＶＭＭ６８は、ステップＳ２０Ｃにおいて、データを参照するページテーブルエントリの使用状態フィールド８５３に対して、使用中を示す情報を設定する（未使用を使用中に変更する）。その後処理は、正常終了する。
【０５７４】
ステップＳ２０Ｄにおいて、セキュアＶＭＭ６８は、外部メモリ７のデータに対する検証を実行する。このステップＳ２０Ｄの処理は、後述の図３８で説明する。ステップＳ２０Ｄでは、外部メモリ７に格納されている検証対象データを読み出し、検証のためのＭＡＣ値を計算し、検証を行うが、その際読み出したデータは内部メモリ８に転送しない。
【０５７５】
ステップＳ２０Ｅにおいて、セキュアＶＭＭ６８は、検証が成功か否か判断する。
【０５７６】
検証が失敗の場合には、処理はステップＳ２０６へ移動する。
【０５７７】
検証が成功の場合には、ステップＳ２０Ｆにおいて、セキュアＶＭＭ６８は、データを参照するページテーブルエントリの使用状態フィールド８５３に対して使用中を示す情報を設定する。その後処理は、正常終了する。
【０５７８】

１回検証で検証が成功した場合には、毎回検証で検証が成功した場合と同様、当該データを参照するページテーブルエントリが有効化され、データ参照処理が再開される。

【０５７９】

図３７は、内部メモリ８のデータに対する検証の処理の一例を示すフローチャートである。この図３７は、上記図３６のステップＳ２０Ｂに相当する。

【０５８０】

ステップＳ１１０１において、セキュアＶＭＭ６８は、データを参照するページテーブルエントリの暗号化フィールド８５２で暗号化保護が設定されているか否か判断する。

【０５８１】

暗号化保護が設定されていない場合、処理はステップＳ１１０３に移動する。

【０５８２】

暗号化保護が設定されている場合、ステップＳ１１０２において、セキュアＶＭＭ６８は、外部メモリ７のデータを復号し、内部メモリ８へ読み込む。

【０５８３】

ステップＳ１１０３において、セキュアＶＭＭ６８は、内部メモリ８のデータを検証する。

【０５８４】

図３８は、外部メモリ７のデータに対する検証の処理を例示するフローチャートである。この図３８は、上記図３６のステップＳ２０Ｄに相当する。

【０５８５】

ステップＳ１２０１において、セキュアＶＭＭ６８は、データを参照するページテーブルエントリの暗号化フィールド８５２で暗号化保護が設定されているか否か判断する。

【０５８６】

暗号化保護が設定されていない場合、処理はステップＳ１２０３に移動する。

【０５８７】

暗号化保護が設定されている場合、ステップＳ１２０２において、セキュアＶＭＭ６８は、外部メモリ７のデータを復号する。

【０５８８】

ステップＳ１２０３において、セキュアＶＭＭ６８は、外部メモリ７のデータを検証する。

【０５８９】

（追い出し処理）

１回検証のデータは、単に１回しか検証が実行されないだけではなく、内部メモリ８に読み込まれない。したがって、１回検証のデータは、内部メモリ８から外部メモリ７への追い出し処理の対象にはならない。１回検証において、検証が１回実行され、使用中になったデータは、その後電源断まで、使用中の状態が維持され、ゲストＯＳによるデータ参照要求に対して、外部メモリ７のデータが直接参照される。

【０５９０】

１回検証で、データを参照する上位ページテーブルが内部メモリ８から外部メモリ７へ追い出される場合に、参照先のデータに対するＭＡＣ値の計算などの処理は行われない。また、上位ページテーブルが内部メモリ８から外部メモリ７へ追い出される場合に、当該上位ページテーブル自体のＭＡＣ値は計算され、上位ページテーブルは内部メモリ８から外部メモリ７へ書き出されるが、上位ページテーブルのページテーブルエントリの無効化は行われない。したがって、もう一度、データが参照される場合には、対応する上位ページテーブルが検証され、上位ページテーブルが外部メモリ７から内部メモリ８に再度読み込まれるだけでよい。内部メモリ８に再度読み込まれた上位ページテーブルはすでに有効状態である。すなわち、上位ページテーブルのページテーブルエントリで”使用中”が設定されているデータの参照では、上位ページテーブルのページテーブルエントリの有効化は不要である。

【０５９１】

（電源断前処理）
上記のように、上位ページテーブルのページテーブルエントリで”使用中”が設定されているデータは、その後電源断まで外部メモリ７で直接参照される。
【０５９２】
電源断前には、使用中が設定されているデータに対して、ＭＡＣ値の計算、暗号化、データを参照する上位ページテーブルのページテーブルエントリの更新、が実行される。これにより、次の電源投入時に、上記の検証処理が適切に動作する。
【０５９３】
図３９は、本実施形態に係る電源断前処理を例示するフローチャートである。
【０５９４】
ステップＳ１３０１において、セキュアＶＭＭ６８は、毎回検証が設定されている内部メモリ８のデータに対する追い出し処理を実行する。
【０５９５】
ステップＳ１３０２において、セキュアＶＭＭ６８は、１回検証が設定されている外部メモリ７のデータに対する更新処理を実行する。
【０５９６】
ステップＳ１３０３において、セキュアＶＭＭ６８は、上記図６で説明したように、内部メモリ８のページテーブルの追い出し処理を実行する。
【０５９７】
図４０は、本実施形態に係る１回検証が設定されているデータの更新処理を例示するフローチャートである。この図４０は、上記図３９のステップＳ１３０２に相当する。
【０５９８】
この図４０の処理は、使用中が設定されているデータの上位ページテーブルのページテーブルエントリに対して繰り返し実行される。
【０５９９】
ステップＳ１４０１において、セキュアＶＭＭ６８は、外部メモリ７に格納されているデータに対して、ＭＡＣ値を更新し、暗号化保護が設定されている場合には暗号化を行う。
【０６００】
ステップＳ１４０２において、セキュアＶＭＭ６８は、データを参照する上位ページテーブルのページテーブルエントリに対して、未使用及び無効を設定する。
【０６０１】
図４１は、本実施形態に係る外部メモリ７に格納されているデータに対する更新処理の一例を示すフローチャートである。この図４１は、上記図４０のステップＳ１４０１に相当する。
【０６０２】
ステップＳ１５０１において、セキュアＶＭＭ６８は、外部メモリ７に格納されているデータに対して、ＭＡＣ値を計算する。
【０６０３】
ステップＳ１５０２において、セキュアＶＭＭ６８は、データを参照するページテーブルエントリの暗号化フィールド８５２で暗号化保護が設定されているか否か判断する。
【０６０４】
暗号化保護が設定されていない場合、処理は終了する。
【０６０５】
暗号化保護が設定されている場合、ステップＳ１５０３において、セキュアＶＭＭ６８は、外部メモリ７のデータを暗号化する。
【０６０６】
上記の電源断前処理により、１回検証のデータを参照するページテーブルエントリには、未使用かつ無効が設定される。このため、次回電源投入後のデータ参照時には、外部メモリ７のデータに対する複数回のデータ参照のうち前記複数回より少ない少なくとも１回

に対して、検証が行われる。すなわち、あるデータに対する参照の初回には必ずアドレス変換の失敗が発生し、この失敗に基づいて、当該データに対して少なくとも１回の検証が実行される。

【０６０７】

上記のように、電源断前処理では、上位ページテーブルのページテーブルエントリに使用中が設定されているすべてのデータに対して、ＭＡＣ値計算と暗号化が実行され、ページテーブルエントリの設定が使用中から未使用に変更される。ＭＡＣ値計算と暗号化とページテーブルエントリの設定変更とを併せて検証更新処理と呼ぶ。なお、上記第２の実施形態で説明されたカウンタ方式では、カウンタの更新も検証更新処理に含まれる。並行して、ＭＡＣ値計算の影響を受ける上位ページテーブルについてもＭＡＣ値計算が行われ、全ての下位ページテーブルの検証更新処理が完了したページテーブルに対して逐次検証更新処理が実行される。１回検証のページテーブルに対する検証更新処理は毎回検証の場合と同様である。

【０６０８】

上記図３９のフローチャートでは、電源断前処理として、内部メモリ８に格納されており毎回検証が設定されているデータの外部メモリ７への追い出し処理、１回検証が設定されているデータの外部メモリ７での検証更新処理、内部メモリ８に格納されているページテーブルの追い出し処理を、逐次的に実行している。これらの処理は必ずしもこの順序で行う必要はなく順序を入れ替えてもよい。ただし、内部メモリ８からのページテーブルの追い出し処理は、データの追い出し処理と検証更新処理に依存するため、最後に行う必要がある。また、複数の種類のデータ保護方式が混在するページテーブルに対して、データ保護方式ごとに検証更新処理を実行する処理では、検証更新処理を実行する際に一度追い出された参照元ページテーブルの再読み込みが必要になる場合がある。このため、１つのデータ参照元ページテーブルに対して、複数の種別のデータ保護方式が混在する場合には、当該ページテーブルに含まれる全ての種別のデータ保護方式に対してまとめて検証更新処理を実行する。これにより、データ参照元ページテーブルの再読み込み回数を少なくすることができる。

【０６０９】

カウンタ方式では、上位ページテーブルのＭＡＣ値計算のために、下位データに対応するカウンタ値が必要とされる。しかしながら、上位ページテーブルのＭＡＣ値計算のために、下位データのＭＡＣ値は必要とされない。

【０６１０】

したがって、１回検証では、あるページテーブルの１回検証のページテーブルエントリが使用中になると、カウンタ値を予め１つ増分し、下位ページのページ更新を待つことなく、当該ページテーブルの検証更新処理を実行可能となる。よってカウンタ方式が用いられる場合、１回検証のデータに対する電源断時の検証更新処理と、ページテーブルの検証更新処理を独立に行うことができる。ただし、データの状態又はアドレス情報がページテーブルに格納されている場合、ページテーブルを内部メモリ８へ読み込む必要がある。この場合、使用中のデータの状態情報、制御情報、又は、アドレス情報をページテーブルとは別の一時リストなどで管理することで、電源断時のデータ更新に、再度ページテーブルを読み込むことを不要とすることができる。１回検証のデータと、毎回検証及び検証なしのデータが混在しており、使用中のデータの総数が少ない場合、上記一時リストは、ページテーブルと比較してサイズが小さくなる。このため、内部メモリ８を節約しつつ、電源断時の処理時間を短縮することができる。

【０６１１】

（構成）

図４２は、本実施形態に係るメモリ管理装置１の構成を例示するブロック図である。

【０６１２】

メモリ管理装置１の検証計算部４は、方式判断部９９を含む。

【０６１３】

メモリ管理装置１は、電源遮断前処理部９８をさらに備える。

【０６１４】

方式判断部９９は、複数のデータ保護方式のうち設定されているデータ保護方式を判断し、判断結果に応じて処理を切り替える。

【０６１５】

電源断前処理部９８は、上記図３９で説明した電源断前処理を実行する。

【０６１６】

以上説明した本実施形態においては、上記第１乃至第７の実施形態と同様の階層的検証を適用可能であり、攻撃耐性とオーバーヘッドとが異なる複数のデータ保護方式を共存させることができる。データ保護方式の割り当ては、ゲストＯＳ毎にそれぞれ異なるデータ保護方式を割り当ててもよく、１つのゲストＯＳ内のデータ毎に複数のデータ保護方式が共存してもよい。検証処理の内容自体は、それぞれのデータ毎に割り当てられたデータ保護方式に応じて正しく機能する。

【０６１７】

１回検証では、データのサイズが内部メモリ８に格納可能なサイズに制約されないため、例えば２メガバイトのデータのような大きなサイズのデータであっても対応可能である。

【０６１８】

［第９の実施形態］

上記第８の実施形態では、外部メモリ７がＭＲＡＭなどのようなワードアクセス可能な不揮発性メモリの場合を例として説明している。しかしながら、現時点ではワードアクセス可能な不揮発性メモリより、アクセスがページ単位に限られ、書き込み回数に制限のあるフラッシュメモリの方がビット単価が安くコスト優位である。そこで、本実施形態においては、上記のデータ保護方式を、例えばフラッシュメモリなどのような不揮発性メモリ（不揮発性ページメモリ）と、例えばＤＲＡＭ（Dynamic Random Access Memory）などのような揮発性メモリ（揮発性ワードアクセスメモリ）とを組み合わせた外部の主記憶装置、に適用する場合を説明する。

【０６１９】

図４３は、本実施形態に係る情報処理装置６５のハードウェア構成を例示するブロック図である。

【０６２０】

プロセッサ６６と、不揮発性メモリ４００と、揮発性メモリ４０１とは、外部バス４４を介して、データ、信号、命令を互いに送受信可能とする。

【０６２１】

上記のように、不揮発性メモリ４００としては、例えばフラッシュメモリが用いられる。揮発性メモリとしては、例えばＤＲＡＭが用いられる。しかしながら、それぞれ同様のメモリの性質を備える場合には、他の様々なメモリを適用可能である。

【０６２２】

ＤＲＡＭは揮発性ではあるが、ワードアクセスが可能であり、書き換え可能回数は事実上無制限である。ＤＲＡＭをビット単価の安いフラッシュメモリの一時バッファメモリとして使うことで低コストに主記憶装置を構成することができる。

【０６２３】

揮発性のＤＲＡＭが用いられる場合には、秘匿対象のデータが、電源断の後ある程度の時間が経過すればＤＲＡＭから消失するという利点がある。これは特に上述の１回検証における暗号化されたデータの処理との組み合わせにおいて利点となる。

【０６２４】

以下、外部メモリ７が、不揮発性メモリ４００と揮発性メモリ４０１との組み合わせを含む場合において、上記の３種類のデータ保護方式が適用される例を説明する。

【０６２５】

不揮発性メモリ４００は、停止状態においてセキュアＶＭＭ６８、セキュアＯＳ５６、

非セキュアＯＳ５７を格納する。
【０６２６】
（不揮発性メモリ４００に対するアクセス）
例えば、ページ単位でのアクセスに限定された不揮発性メモリ４００は、直接物理メモリアドレスにマッピングされず、コントローラ経由でアクセスされる。この場合、不揮発性メモリ４００では、ページ毎に物理アドレスが与えられるとは限らない。本実施形態では、不揮発性メモリ４００と揮発性メモリ４０１又は内部メモリ８との間の間のデータ転送は、ページ単位で行われる場合を説明する。ページが転送される場合に、不揮発性メモリ４００のアクセス先が適切に識別できれば、不揮発性メモリ４００が直接メモリアドレスにマッピングされていなくても動作可能である。具体的には、不揮発性メモリ４００に対するアクセスにおいて、ページテーブルが保持する変換先物理アドレスが、後述のＤ／Ｆ(ＤＲＡＭ／フラッシュ)フラグに基づいて、フラッシュメモリのデータブロック識別子に変更される。この変更の結果得られたデータブロック識別子に基づいて、不揮発性メモリ４００がアクセスされる。
【０６２７】
以下では、説明を簡略化にするため、不揮発性メモリ４００がメモリアドレスにマッピングされている場合を例として説明する。
【０６２８】
（複数のデータ保護方式の動作）
図４４は、本実施形態に係るページテーブルエントリのフィールド形式を例示するデータ構造図である。この図４４は、上記図３３のページテーブルエントリの変形例である。
【０６２９】
例えば、ソフトウェア使用予備フィールド８５は、データ保護方式フィールド８５１、暗号化フィールド８５２、使用状態フィールド８５３、Ｄ／Ｆフラグ８５５を含む。
【０６３０】
Ｄ／Ｆフラグ８５５は、次回参照データが揮発性メモリ４０１及び内部メモリ８のいずれかに格納されているか、又は、不揮発性メモリ４００に格納されているか、を示す。
【０６３１】
例えば、Ｄ／Ｆフラグ８５５にＤが設定されている場合には、次回参照データが、揮発性メモリ４０１及び内部メモリ８のいずれかに格納されていることを示す。Ｄ／Ｆフラグ８５５にＦが設定されている場合には、次回参照データが、不揮発性メモリ４００に格納されていることを示す。
【０６３２】
図４５は、本実施形態に係る、データ保護方式ごとのデータのコピー状態及び検証状態を例示する状態遷移図である。この図４５では、次回参照データは、不揮発性メモリ４００、揮発性メモリ４０１、内部メモリ８のいずれかに格納されている。
【０６３３】
図４６は、複数のデータ保護方式におけるページテーブルエントリのデータ保護方式フィールド８５１の状態、Ｄ／Ｆフラグ８５５、有効／無効フラグ８５４、次回参照データの状態、次回参照データの状態を示す符号、の関係を例示する図である。
【０６３４】
以下では、上記第２及び第８の実施形態と相違する部分について、説明する。
【０６３５】
毎回検証において、データは、状態ＮＤ６乃至状態ＮＤ８の間を遷移する。状態ＮＤ６乃至状態ＮＤ８では、データの格納位置、検証実行及びＭＡＣ値計算などの状態が異なる。毎回検証では、状態ＮＤ６の次回参照データが不揮発性メモリ４００に格納されている場合に、次回参照データに必ず検証を行い、次回参照データを内部メモリ８に格納する。暗号化保護ありの場合には、次回参照データが検証とともに復号される。命令実行ユニット４５によるデータ参照は、状態ＮＤ７（内部メモリ８の検証済み）の次回参照データに対して行われる。稼働中に、状態ＮＤ７の次回参照データが内部メモリ８から外部メモリ

７へ書き出される場合には、次回参照データのＭＡＣ値が計算され、暗号化保護ありの場合には、次回参照データが暗号化され、次回参照データが揮発性メモリ４０１に格納され、揮発性メモリ４０１に格納された次回参照データは状態ＮＤ８（揮発性メモリ４０１の未検証）となる。再度、次回参照データが参照される場合には、揮発性メモリ４０１の状態ＮＤ８の次回参照データが読み込まれ、検証され、暗号化保護ありの場合には次回参照データが復号され、内部メモリ８に格納され、内部メモリ８に格納された次回参照データは状態ＮＤ７となる。この状態ＮＤ７の次回参照データが命令実行ユニット４５によって参照される。

【０６３６】

電源断において、次回参照データが内部メモリ８に格納されている場合には、内部メモリ８の次回参照データのＭＡＣ値が計算され、暗号化保護ありの場合には次回参照データが復号され、次回参照データが不揮発性メモリ４００に格納され、不揮発性メモリ４００に格納された次回参照データは状態ＮＤ６（不揮発性メモリ４００の未検証）となる。

【０６３７】

電源断において、次回参照データが揮発性メモリ４０１に格納されている場合には、揮発性メモリ４０１の次回参照データが不揮発性メモリ４００へ転送され、次回参照データが不揮発性メモリ４００に格納され、不揮発性メモリ４００に格納された次回参照データは状態ＮＤ６（不揮発性メモリ４００の未検証）となる。内部メモリ８から揮発性メモリ４０１へのデータ書き出しにおいて、ＭＡＣ値の計算及び次回参照データの暗号化は実行済みであるため、揮発性メモリ４０１から不揮発性メモリ４００へ次回参照データが転送される場合には、ＭＡＣ値の計算及び次回参照データの暗号化は必要ない。

【０６３８】

１回検証において、データは、状態ＮＤ９と状態ＮＤ１０との間を遷移する。状態ＮＤ９と状態ＮＤ１０とでは、データの格納される位置、検証実行及びＭＡＣ値計算などの状態が異なる。１回検証では、次回参照データが状態ＮＤ９（不揮発性メモリ４００の未検証）の場合に、次回参照データに検証を行い、暗号化保護ありの場合には次回参照データを復号し、次回参照データを揮発性メモリ４０１に格納する。揮発性メモリ４０１の次回参照データは状態ＮＤ１０（揮発性メモリ４０１の検証済み）となる。命令実行ユニット４５によるデータ参照は、揮発性メモリ４０１から内部メモリ８へのコピーは行われず、状態ＮＤ１０の次回参照データに対して行われる。状態ＮＤ１０の次回参照データが揮発性メモリ４０１から不揮発性メモリ４００へ書き出される場合には、次回参照データのＭＡＣ値が計算され、暗号化保護ありの場合には次回参照データが暗号化され、次回参照データが不揮発性メモリ４００に格納され、不揮発性メモリ４００に格納された次回参照データが状態ＮＤ９（不揮発性メモリ４００の未検証）となる。揮発性メモリ４０１に格納されている次回参照データに対するＭＡＣ値計算と、揮発性メモリ４０１から不揮発性メモリ４００への書き出しは、次回の電源断までに行う。

【０６３９】

検証なしにおいて、データは、状態ＮＤ１１と状態ＮＤ１２との間を遷移する。状態ＮＤ１１と状態ＮＤ１２とでは、データの格納される位置が異なる。検証なしでは、次回参照データが状態ＮＤ１１（不揮発性メモリ４００）の場合に、次回参照データを揮発性メモリ４０１に転送する。揮発性メモリ４０１の次回参照データは状態ＮＤ１２（揮発性メモリ４０１）となる。命令実行ユニット４５によるデータ参照において揮発性メモリ４０１から内部メモリ８へのコピーは行われず、命令実行ユニット４５によるデータ参照は状態ＮＤ１２の次回参照データに対して行われる。状態ＮＤ１２の次回参照データが揮発性メモリ４０１から不揮発性メモリ４００へ転送されると、次回参照データが不揮発性メモリ４００に格納され、不揮発性メモリ４００に格納された次回参照データは状態ＮＤ１１となる。揮発性メモリ４０１に格納されている次回参照データに対する揮発性メモリ４０１から不揮発性メモリ４００への転送は、次回の電源断までに行う。

【０６４０】

本実施形態においても、上記第８の実施形態と同様に、データ書き出し、ＭＡＣ値の計

算、データの再暗号化は、データが更新された場合にのみ実行されるとしてもよい。

【０６４１】

本実施形態においても、上記第８の実施形態と同様に、ページテーブルについては毎回検証を行う。説明を簡素化するためにめ、本実施形態では、データに対する検証のみを説明し、ページテーブルの検証については説明を省略する。その他にも、上記各実施形態と同様の説明については省略する。

【０６４２】

（検証転送処理）

読み込み対象のデータのページテーブルエントリは、電源投入されると、以下の状態のいずれかを持つ。

【０６４３】

毎回検証(ETV)：Ｄ／Ｆフラグ＝Ｆ：有効／無効フラグ＝０（状態ＮＤ６）

１回検証(OTV)：Ｄ／Ｆフラグ＝Ｆ：有効／無効フラグ＝０（状態ＮＤ９）

検証なし(NOV)：Ｄ／Ｆフラグ＝Ｆ：有効／無効フラグ＝０（状態ＮＤ１１）

図４７は、本実施形態に係るアドレス解決処理の例示するフローチャートである。

【０６４４】

ステップＳ１０２の判断の結果、テーブルエントリが無効の場合、制御はＭＭＵ４６からセキュアＶＭＭ６８に移り、ステップＳ１０Ａにおいて、セキュアＶＭＭ６８は、後述の図４８で説明される検証転送処理を実行し、その後処理はステップＳ１０４に移動する。

【０６４５】

図４８は、本実施形態に係る複数のデータ保護方式に対応する検証転送処理を例示するフローチャートである。この図４８は、上記図４７のアドレス解決処理のステップＳ１０Ａの検証転送処理として呼び出される処理である。この図４８では、不揮発性メモリ４００をフラッシュ、揮発性メモリ４０１をＤＲＡＭと表記しているが、これに限定されないことは先で述べた通りである。以下で説明される他の図面についても同様である。

【０６４６】

ステップＳ１６０１において、セキュアＶＭＭ６８は、データを参照するページテーブルエントリに設定されている情報に基づいて、データ保護方式を判断する。データ保護方式が毎回検証の場合、処理はステップＳ１６１１に移動する。データ保護方式が１回検証の場合、処理はステップＳ１６２１に移動する。データ保護方式が検証なしの場合、処理は、ステップＳ１６３１に移動する。

【０６４７】

データ保護方式が毎回検証の場合、ステップＳ１６１１において、セキュアＶＭＭ６８は、Ｄ／Ｆフラグ２５５がＤＲＡＭを示すか、又は、フラッシュを示すか、判断する。

【０６４８】

Ｄ／Ｆフラグ２５５がＤＲＡＭを示す場合、ステップＳ１６１２において、セキュアＶＭＭ６８は、ＤＲＡＭのデータを内部メモリ８の空き領域にコピーする。

【０６４９】

Ｄ／Ｆフラグ２５５がフラッシュを示す場合、ステップＳ１６１２において、セキュアＶＭＭ６８は、フラッシュのデータを内部メモリ８の空き領域にコピーする。

【０６５０】

ステップＳ１６１４において、セキュアＶＭＭ６８は、検証対象データの内部メモリ８での検証及び復号処理を実行する。

【０６５１】

ステップＳ１６１５において、セキュアＶＭＭ６８は、検証が成功したか否か判断する。

【０６５２】

検証成功の場合には、ステップＳ１６１６において、セキュアＶＭＭ６８は、データのコピー先の内部メモリ８のアドレスをページテーブルエントリに設定する。

【０６５３】
ステップＳ１６１７において、セキュアＶＭＭ６８は、ページテーブルエントリのＤ／Ｆフラグ８５５にＤを設定し、有効／無効フラグ８５４に１を設定する。そして、処理は終了する。
【０６５４】
検証失敗の場合には、処理はステップＳ１６４１に移動する。
【０６５５】
ステップＳ１６４１において、セキュアＶＭＭ６８は、検証失敗後処理を実行し、処理は終了する。
【０６５６】
データ保護方式が１回検証の場合、ステップＳ１６２１において、セキュアＶＭＭ６８は、フラッシュのデータをＤＲＡＭの空き領域にコピーする。
【０６５７】
ステップＳ１６２２において、セキュアＶＭＭ６８は、検証対象データのＤＲＡＭでの検証及び復号処理を実行する。
【０６５８】
ステップＳ１６２３において、セキュアＶＭＭ６８は、検証が成功したか否か判断する。
【０６５９】
検証失敗の場合には、処理は上記のステップＳ１６４１に移動する。
【０６６０】
検証成功の場合には、ステップＳ１６２４において、セキュアＶＭＭ６８は、データのコピー先のＤＲＡＭのアドレスをページテーブルエントリに設定する。
【０６６１】
ステップＳ１６２５において、セキュアＶＭＭ６８は、ページテーブルエントリのＤ／Ｆフラグ８５５にＤを設定し、有効／無効フラグ８５４に１を設定する。そして、処理は終了する。
【０６６２】
データ保護方式が検証なしの場合、ステップＳ１６３１において、セキュアＶＭＭ６８は、フラッシュのデータをＤＲＡＭの空き領域にコピーする。
【０６６３】
ステップＳ１６３２において、セキュアＶＭＭ６８は、データのコピー先のＤＲＡＭのアドレスをページテーブルエントリに設定する。
【０６６４】
ステップＳ１６３３において、セキュアＶＭＭ６８は、ページテーブルエントリのＤ／Ｆフラグ８５５にＤを設定し、有効／無効フラグ８５４に１を設定する。そして、処理は終了する。
【０６６５】
（追い出し処理）
本実施形態における追い出し処理は、内部メモリ８から揮発性メモリ４０１又は不揮発性メモリ４００への追い出し処理と、揮発性メモリ４０１から不揮発性メモリ４００への追い出しの２種類がある。このうち、揮発性メモリ４０１から不揮発性メモリ４００への追い出し処理は、後で説明する図５１の電源断前の追い出し処理と基本的に同一であるためここでは説明を省略する。ここでは、稼働中の内部メモリ８から揮発性メモリ４０１への追い出し処理について説明する。内部メモリ８から揮発性メモリ４０１への追い出し処理は、毎回検証のデータに対して実行される。
【０６６６】
図４９は、本実施形態に係る稼働中の内部メモリ８から揮発性メモリ４０１への追い出し処理を例示するフローチャートである。
【０６６７】

ステップＳ１７０１において、セキュアＶＭＭ６８は、追い出し対象データのＭＡＣ値を計算する。

【０６６８】

ステップＳ１７０２において、セキュアＶＭＭ６８は、追い出し対象データを、ＤＲＡＭの空き領域にコピーする。

【０６６９】

ステップＳ１７０３において、セキュアＶＭＭ６８は、追い出し対象データのコピー先のＤＲＡＭのアドレスをページテーブルエントリに設定する。

【０６７０】

ステップＳ１７０４において、セキュアＶＭＭ６８は、ページテーブルエントリのＤ／Ｆフラグ８５５にＤ、有効／無効フラグ８５４に０を設定する。そして、処理は終了する。

【０６７１】

（電源断前処理）

図５０は、本実施形態に係る電源断前処理を例示するフローチャートである。

【０６７２】

ステップＳ１８０１において、セキュアＶＭＭ６８は、内部メモリ８に格納されており毎回検証が設定されているデータのフラッシュへの追い出し処理を実行する。

【０６７３】

次に、使用中が設定されているデータを参照する上位ページテーブルのページテーブルエントリに対して、ステップＳ１８０２が繰り返される。

【０６７４】

ステップＳ１８０２では、セキュアＶＭＭ６８は、ＤＲＡＭのデータのフラッシュへの追い出し処理を実行する。

【０６７５】

このように、ステップＳ１８０１を実行し、さらに、使用中が設定されているデータを参照する上位ページテーブルの全てに対してステップＳ１８０２の処理が繰り返されることで、内部メモリ８及びＤＲＡＭにおけるゲストＯＳのデータの書き出し処理は完了する。

【０６７６】

次に、ステップＳ１８０３において、セキュアＶＭＭ６８は、内部メモリ８のページテーブルをフラッシュへコピーする追い出し処理を実行する。そして、処理は終了される。

【０６７７】

図５１は、本実施形態に係る揮発性メモリ４０１から不揮発性メモリ４００への追い出し処理の一例を示すフローチャートである。

【０６７８】

ステップＳ１９０１において、セキュアＶＭＭ６８は、データを参照するページテーブルエントリに設定されている情報に基づいて、データ保護方式を判断する。

【０６７９】

データ保護方式が１回検証の場合、ステップＳ１９０２において、セキュアＶＭＭ６８は、データのＭＡＣ値計算及び暗号化処理を実行する。１回検証の場合のステップＳ１９０２のＭＡＣ値計算及び暗号化処理は、セキュアＤＭＡコントローラ５２によって、データ転送と並行して処理されてもよい。

【０６８０】

データ保護方式が毎回検証又は検証なしの場合、処理はステップＳ１９０３に移動する。毎回検証の場合には、内部メモリ８からの追い出し時にＭＡＣ値計算及び暗号化処理が実行されている。また、検証なしの場合には、データに対するＭＡＣ値計算及び暗号化処理は不要である。

【０６８１】

データ保護方式が毎回検証、１回検証、検証なしのいずれの場合であっても、ステップ

Ｓ１９０３において、セキュアＶＭＭ６８は、データをＤＲＡＭからフラッシュへ転送（コピー）する処理を実行する。

【０６８２】

ステップＳ１９０４において、セキュアＶＭＭ６８は、データのコピー先のフラッシュのアドレスをページテーブルエントリに設定する。

【０６８３】

ステップＳ１７０５において、セキュアＶＭＭ６８は、ページテーブルエントリのＤ／Ｆフラグ８５５にＦ、有効／無効フラグ８５４に０を設定する。そして、処理は終了する。

【０６８４】

以上説明した本実施形態においては、例えばＭＲＡＭなどのような高価な不揮発性のランダムアクセスメモリではなく、比較的安価な例えばフラッシュメモリなどのような不揮発性メモリ４００と、ＤＲＡＭなどのような揮発性メモリ４０１とが併用され、データに対して３種類のデータ保護方式のいずれかが実行される。これにより、プロセッサ６６のオーバーヘッドを低減させるとともに、製造コストを低減させることができる。

【０６８５】

上記の第８及び第９の実施形態において、あるＯＳでは毎回検証を適用し、他のＯＳでは１回検証又は検証なしを適用してもよい。例えば、セキュアＯＳ５６のデータに対して検証を行い、非セキュアＯＳ５７のデータに対して検証を行わないとしてもよい。

【０６８６】

上記の第８及び第９の実施形態において、あるＯＳに対するデータであっても、一部のデータに対して毎回検証を適用し、他のデータに対して１回検証又は検証なしを適用してもよい。例えば、セキュアＯＳ５６と非セキュアＯＳ５７とが相互に読み書き可能な共有データ領域を持ち、セキュアＯＳ５６が読み込み時にデータを検証し、非セキュアＯＳ５７が書き込み時に検証子を書き込まない場合を考える。この場合において、非セキュアＯＳ５７が共有データ領域に書き込んだデータをセキュアＯＳ５６が読み出すと、セキュアＯＳ５６が読み出したデータに対して検証子が計算されておらず、検証失敗となる。しかしながら、上記の第８及び第９の実施形態において、例えば、セキュアＯＳ５６の検証対象データに対して毎回検証が適用され、セキュアＯＳ５６のデータのうち非セキュアＯＳ５７と共有される検証不要なデータに対して検証なしが適用される。これにより、非セキュアＯＳ５７が共有データ領域に書き込んだデータを、セキュアＯＳ５６が読み出す場合に検証失敗となることを防止することができる。

【０６８７】

［第１０の実施形態］

本実施形態においては、上記第１乃至第９の実施形態で用いられる暗号化及び改ざん検証の具体例について説明する。本実施形態では、暗号化方式XTS-AESの詳細について説明する。また、本実施形態においては、ページテーブル又はデータに対するアドレス及びバージョン毎のリプレイ攻撃防止に用いられるTweakと呼ばれる暗号パラメータについて説明する。例えば、XTS-AESによる暗号化とハッシュ値を利用した改ざん検証とを組み合わせることにより、リプレイ攻撃が排除される。本実施形態においては、XTS-AESによる暗号化を利用した改ざん検証用ＭＡＣ値計算についても説明する。

【０６８８】

AESはIEEE P1619として標準化されており、例えばディスク装置等のランダムアクセスデータに適用される暗号化方式である。AESはTweak及びSequence Numberと呼ばれるパラメータを持つ。同じ秘密鍵による同じ平文に対する暗号化であっても、パラメータが異なっていれば、暗号文は全く異なったものとなる。パラメータの秘匿性は不要である。したがって、あるパラメータにおいて平文－暗号文のペアが攻撃者にとって既知であっても、別のパラメータに基づく暗号文のデータ機密性は守られる。

【０６８９】

図５２は、XTS-AESを例示する概念図である。

【０６９０】
XTS-AESは、１２８ビット又は２５６ビットの連鎖からなるブロック平文データ{P0,P1,…Pm}を暗号化して、同一サイズの暗号文{C0,C1,…,Cm}を得る暗号化方式である。
【０６９１】
XTS-AESは、C= XTS-AES（Key,P,i,j）で表記される。
【０６９２】
Keyは秘密鍵であり、秘匿が必要である。例えば、Keyは２５６ビットとする。
【０６９３】
Pは平文であり、ビット数は任意とする。
【０６９４】
iはTweakであり、秘匿は不要である。例えば、iは１２８ビットとする。
【０６９５】
jはSequence Numberであり、秘匿は不要である。例えば、jは１２８ビットとする。
【０６９６】
Cは暗号文であり、ビット数はPと同じである。
【０６９７】
本実施形態では、ゲストＯＳ毎に異なる秘密鍵を使用される。したがって、リプレイ攻撃の対策は、同一ＯＳ内のページ要素（ページテーブル及びデータページ）について、時間（安全でないストレージへの格納回数）と空間（メモリアドレス）とについて行われれば十分である。
【０６９８】
本実施形態では、ゲストＯＳの構成要素は、データページだけでなく、ページテーブルと、当該ページテーブルと連携する検証ツリーも含まれる。これらページテーブル及び検証ツリーに対する改ざん検証及び暗号化も、データと同一の秘密鍵に基づいて実行されることが、鍵管理のオーバーヘッドを減らす観点で望ましい。
【０６９９】
図５３は、本実施形態に係るTweakとSequence Numberの例を示す図である。
【０７００】
iはTweakに対応する。共通ページインデックスには、データページとページテーブルとで重複しない個別のTweakが割り当てられる。共通ページインデックスは２つの要素を含む。第１の要素は、ページアドレスインデックスである。ページアドレスインデックスは、データページについてはアドレス変換前の中間物理アドレス、ページテーブルについては当該ページテーブルが関わるデータページの１つのアドレス変換前の中間物理アドレスとする。アドレスが６４ビットの場合、ページ(４０９６バイト分)の下位アドレス１２ビットは不要のため、ページアドレスインデックスとして５２ビットが使われる。
【０７０１】
第２の要素は、レベルである。ページアドレスインデックスだけを用いた場合にはデータページとページテーブルでTweakが衝突する。レベルは、この衝突を防止するためのインデックスである。例えば、レベルは、データページ及びページテーブルの階層を表す3ビットのインデックスである。
【０７０２】
ページアドレスインデックスとレベルを結合した情報が、共通ページインデックスである。共通ページインデックスを用いることで、データページとページテーブルとの改ざん検証及び暗号化を同一の暗号方式で処理することができる。
【０７０３】
Tweakのうち、残りのビットはデータ格納回数を表すカウンタとして用いられる。本実施形態で、カウンタは７３ビット確保される。
【０７０４】
jはSequence Numberに対応する。Sequence Numberは、一般に、データページ又はページテーブル内の暗号ブロック（１６バイト）のシーケンス番号用カウンタとして用いられ

る。４キロバイトのデータページ又はページテーブルの場合、シーケンス番号用カウンタとして８ビットが割り当てられる。２メガバイトのデータページ又はページテーブルの場合、シーケンス番号用カウンタとして２０ビットが割り当てられる。Sequence Numberの残りのフィールドは、データページ又はページテーブルの書き換え回数のカウンタとして補助的に用いられてもよい。

【０７０５】

図５４は、ページテーブルに対する暗号化保護なしの場合のＭＡＣ値計算及び検証処理を例示する概念図である。

【０７０６】

この図５４において、改ざんの検証対象PT|CTRは、ページテーブルPTとカウンタCTRとの組み合わせとする。この組み合わせの検証対象PT|CTRに対して、SHA-256に基づくハッシュ値H(PT|CTR)が計算され、ハッシュ値H(PT|CTR)に対して上記パラメータKey，i，jを用いて暗号化が行われ、ＭＡＣ値が計算される。この検証対象PT|CTRとＭＡＣ値とが検証のペアとなる。ただし、上述のように、ＭＡＣ値は１階層上のページテーブルのカウンタと関連付けられるため、検証対象PT|CTRとＭＡＣ値とは、離れたアドレスに格納される。

【０７０７】

検証はＭＡＣ値計算の逆を行う。検証対象PT|CTRに対してSHA-256に基づいてハッシュ値H(PT|CTR)が計算される。別途ＭＡＣ値がXTS-AESに基づいて復号される。SHA-256に基づいて計算されたハッシュ値H(PT|CTR)と、XTS-AESに基づいて復号されたハッシュ値H(PT|CTR)とが照合され、一致すれば改ざんの検証は成功と判断される。

【０７０８】

図５５は、ページデータに対する暗号化保護ありの場合のＭＡＣ値計算及び検証処理を例示する概念図である。

【０７０９】

この図５５において、改ざんの検証対象PDは、ページデータのみとする。この検証対象PDに対して、SHA-256に基づくハッシュ値H(PD)が計算され、検証対象PDとハッシュ値H(PD)との組み合わせPD|H(PD)に対して上記パラメータKey，i，jを用いて暗号化が行われ、暗号文CとＭＡＣ値が計算される。暗号文CとＭＡＣ値とが検証のペアとなる。暗号文CとＭＡＣ値とは、上記と同様に、離れたアドレスに格納される。

【０７１０】

検証は暗号化及びＭＡＣ値計算の逆を行う。暗号文CとＭＡＣ値とがXTS-AESに基づいて復号され、平文ページデータである検証対象PDと、ハッシュ値H(PD)の期待値とが得られる。検証対象PDに対して、SHA-256に基づいてハッシュ値H(PD)が計算される。SHA-256に基づいて計算されたハッシュ値H(PD)とハッシュ値H(PD)の期待値とが照合され、一致すれば改ざんの検証は成功と判断される。

【０７１１】

以上説明した本実施形態においては、データの保護とページテーブルの保護に用いる秘密鍵及び暗号化におけるパラメータの大部分を共通化することができる。

【０７１２】

また、多くの暗号アクセラレータに搭載されている標準の暗号化方式XTS-AESを用いて、効率的な改ざん検証及び暗号化を行うことができる。

【０７１３】

上記各実施形態において、暗号化、復号、及び検証の各種処理は、ソフトウェアで実現されてもよく、ハードウェアで実現されてもよい。暗号化、復号、及び検証の各種処理がハードウェアで実現された場合には、暗号化、復号、及び検証の各種処理を高速化することができる。

【０７１４】

上記各実施形態において、カウンタ値及びアドレスが暗号化されることにより、カウンタ値及びアドレスの不正取得を防止することができる。

【０７１５】

上記各実施形態において、データとページテーブルとで、検証を実行すか否か、暗号化を実行するか否かを、区別してもよい。

【０７１６】

例えば、ページテーブルに対しては検証を行い、暗号化を行わず、データに対しては、暗号化のみを行うとしてもよい。

【０７１７】

例えば、ページテーブルに対しては検証を行い、暗号化を行わず、データに対しては、検証と暗号化との双方を行うとしてもよい。

【０７１８】

例えば、ページテーブルに対しては検証と暗号化の双方を行い、データに対しては、検証と暗号化とのうちの少なくとも一方を行うとしてもよい。

【０７１９】

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

【符号の説明】

【０７２０】

１…メモリ管理装置、２…外部入出力部、３…アドレス変換部、４…検証計算部、５…検証部、６…更新部、２０…置換管理部、７…外部メモリ、８…内部メモリ、９…ページテーブルツリー、１０…検証子ツリー、１０１…親テーブル、２０１～２０ｍ…子テーブル、３０１～３０ｘ…データ、ｐｅ１～ｐｅｍ…親エントリ、ｐｖ１～ｐｖｍ…親検証子、ｃｅ１～ｃｅｘ…子エントリ、ｃｖ１～ｃｖｘ…子検証子、１２１…セキュアページテーブルツリー、１２２…セキュア検証子ツリー、４５…命令実行ユニット、４６…ＭＭＵ、４６ａ…アドレス解決部、５２…セキュアＤＭＡコントローラ、５６…セキュアＯＳ、５７…非セキュアＯＳ、６７…鍵保存ユニット、６８…セキュアＶＭＭ。

【図１】

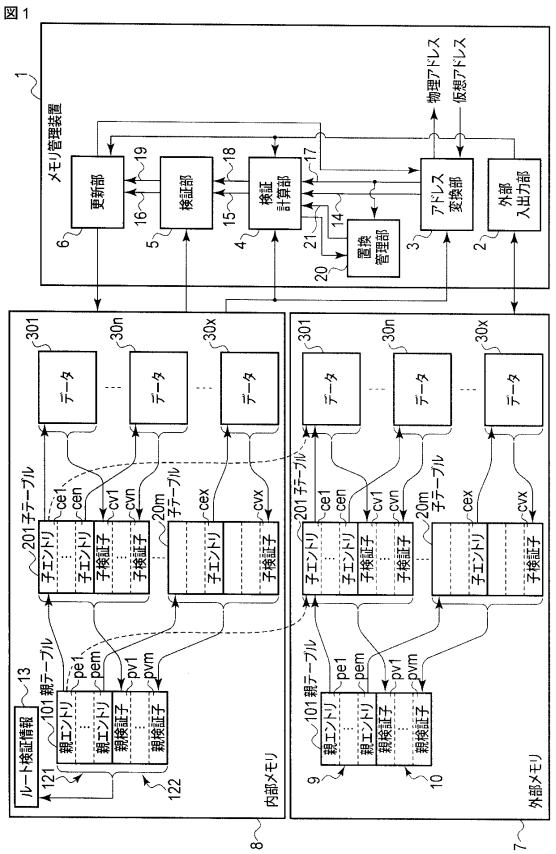


図1
メモリ管理装置
更新部
検証部
検証計算部
置換管理部
アドレス変換部
外部入出力部
物理アドレス
仮想アドレス
ルート検証情報
親エントリ
親検証子
子エントリ
子検証子
データ
内部メモリ
外部メモリ

【図２】

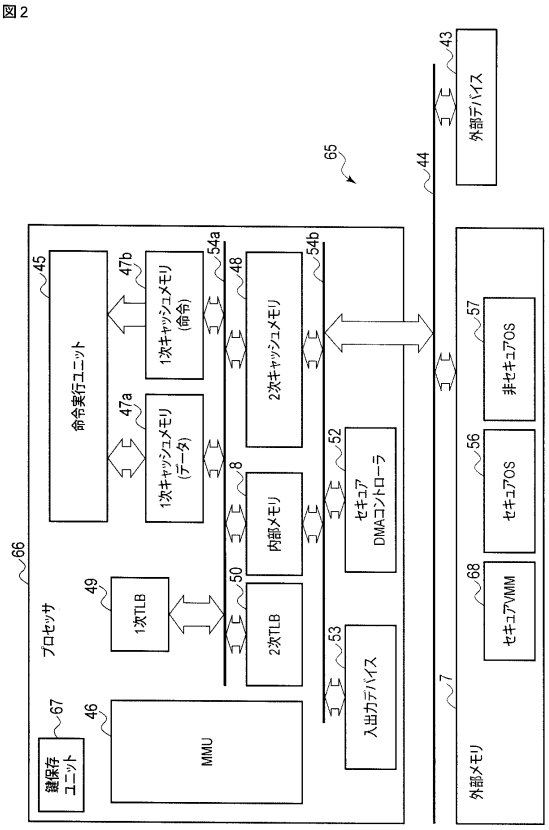


図2
プロセッサ
命令実行ユニット
1次TLB
2次TLB
MMU
内部メモリ
1次キャッシュメモリ(命令)
1次キャッシュメモリ(データ)
2次キャッシュメモリ
セキュアDMAコントローラ
入出力デバイス
鍵保存ユニット
外部メモリ
外部デバイス
非セキュアOS
セキュアOS
セキュアVMM

【図３】

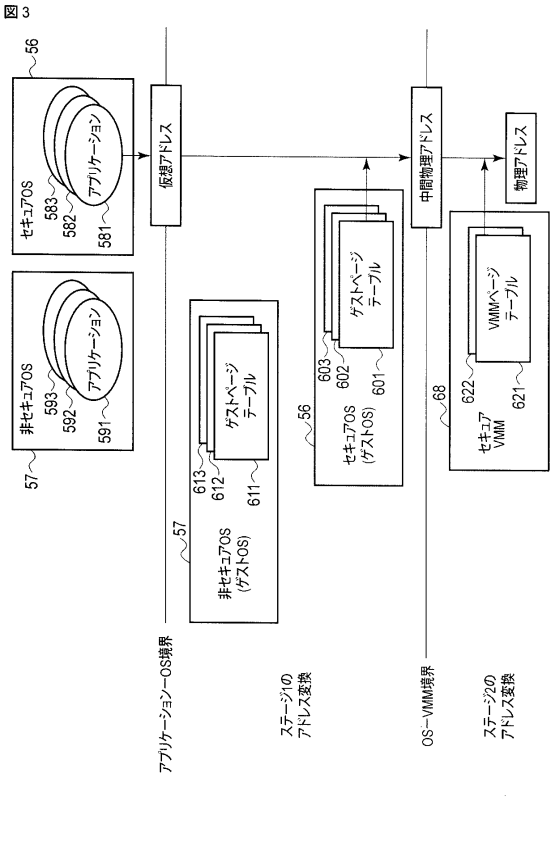


図3
セキュアOS
非セキュアOS
アプリケーション
仮想アドレス
中間物理アドレス
物理アドレス
ゲストページテーブル
VMMページテーブル
非セキュアOS(ゲストOS)
セキュアOS(ゲストOS)
セキュアVMM
アプリケーション－OS境界
OS－VMM境界
ステージ1の
アドレス変換
ステージ2の
アドレス変換

【図４】

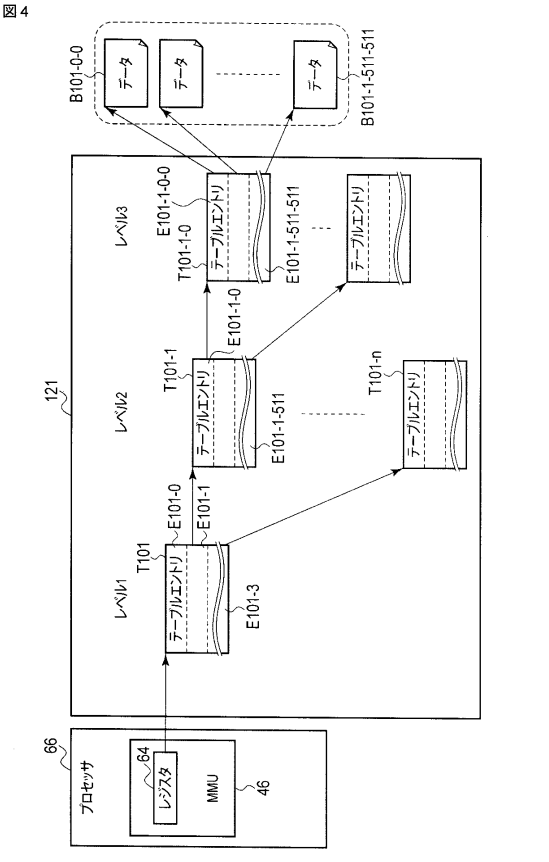
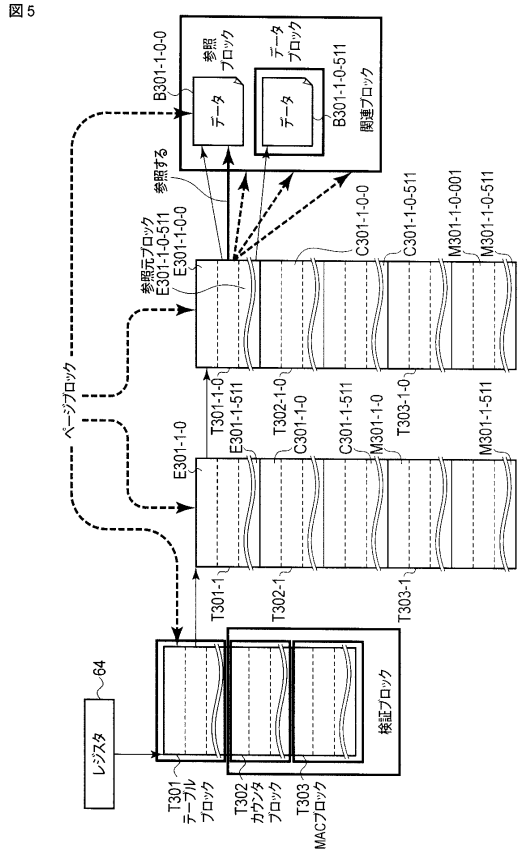


図4
データ
テーブルエントリ
レベル1
レベル2
レベル3
プロセッサ
レジスタ
MMU

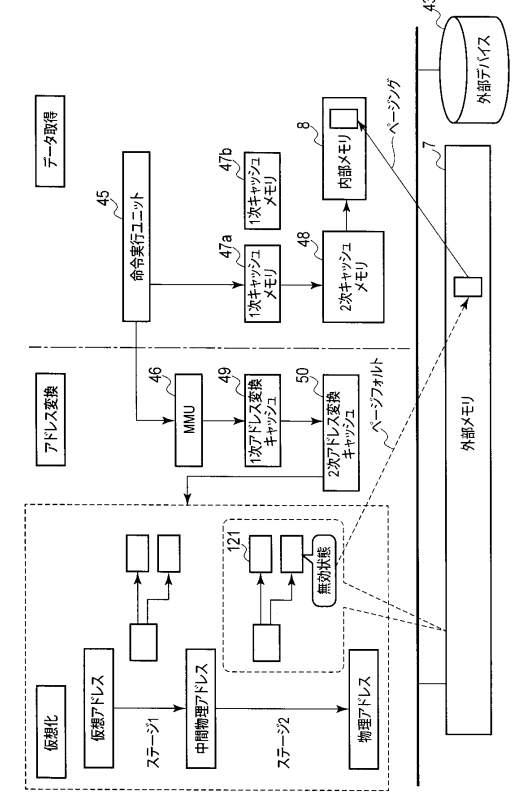
【図５】

図5



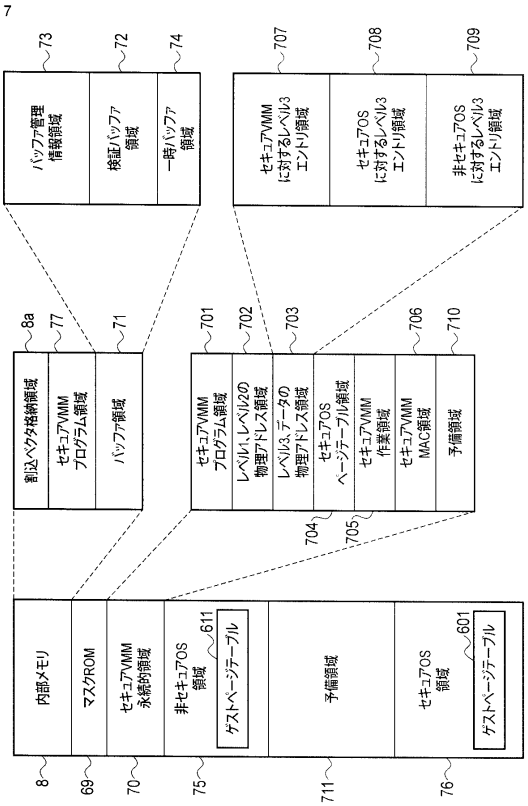
【図６】

図6



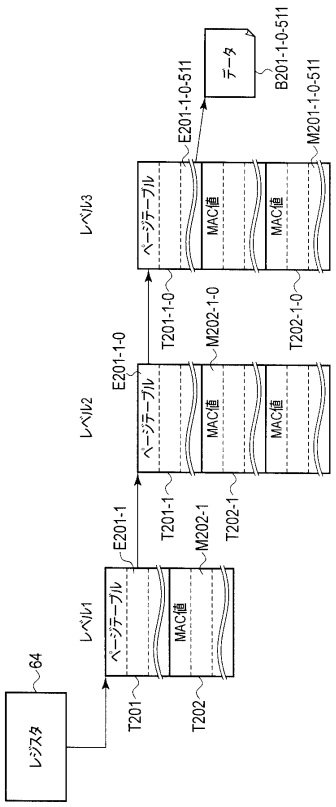
【図７】

図7



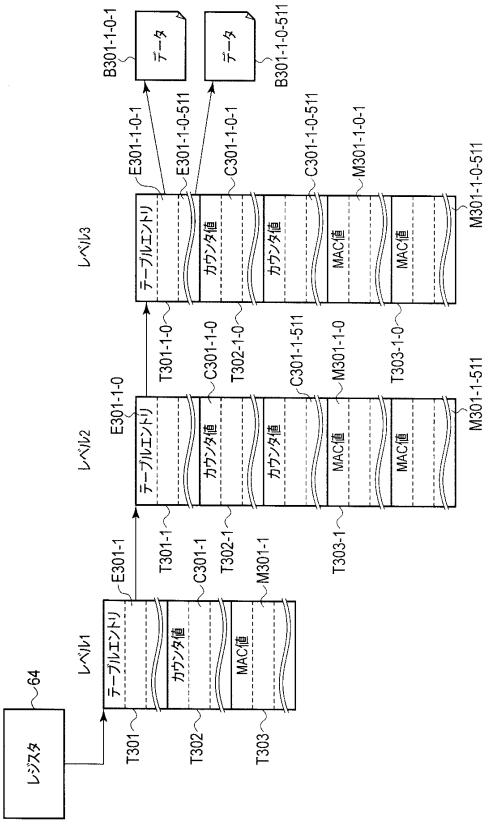
【図８】

図8



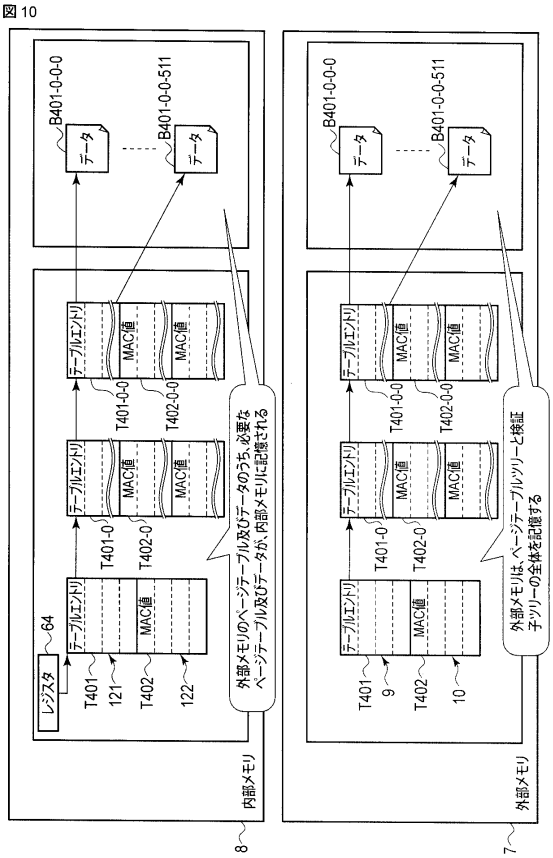
【図９】

図9



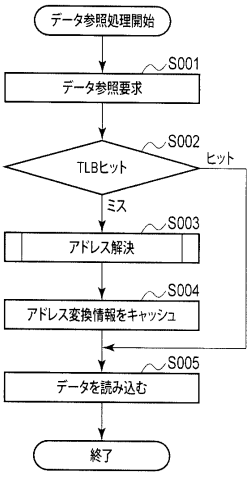
【図１０】

図10



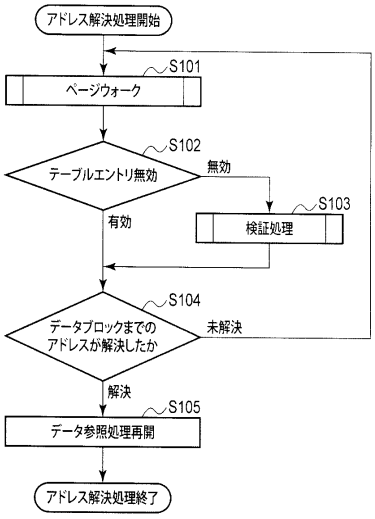
【図１１】

図11



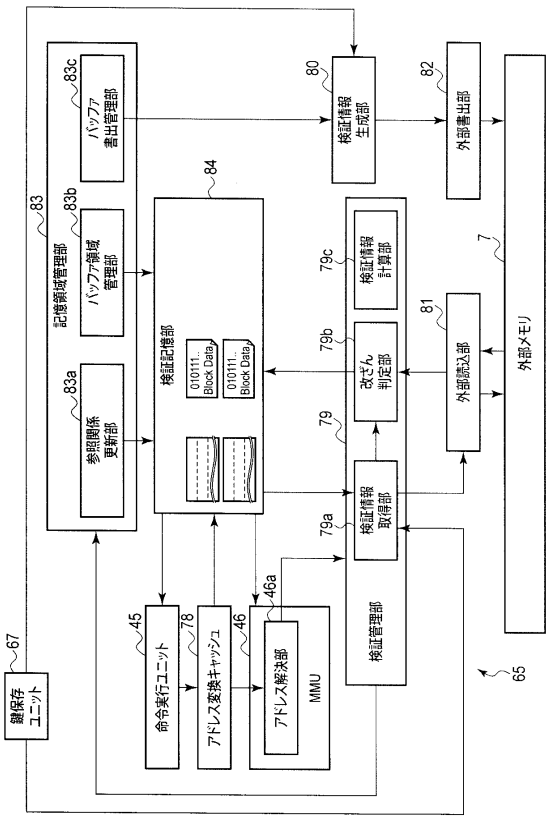
【図１２】

図12



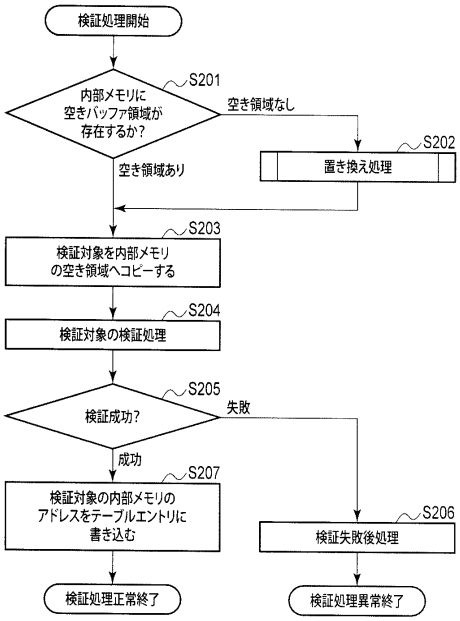
【図１３】

図13



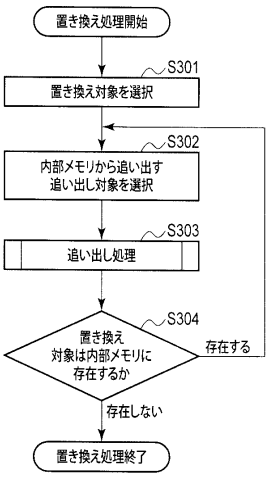
【図１４】

図14



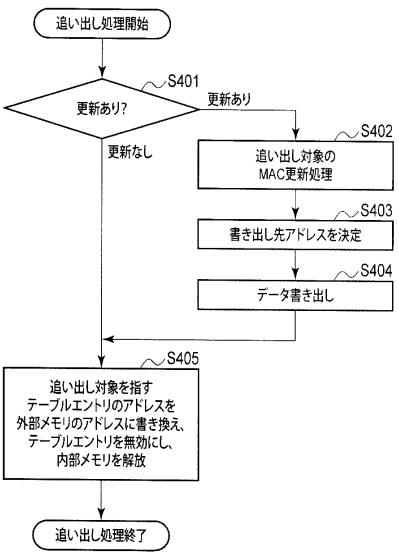
【図１５】

図15



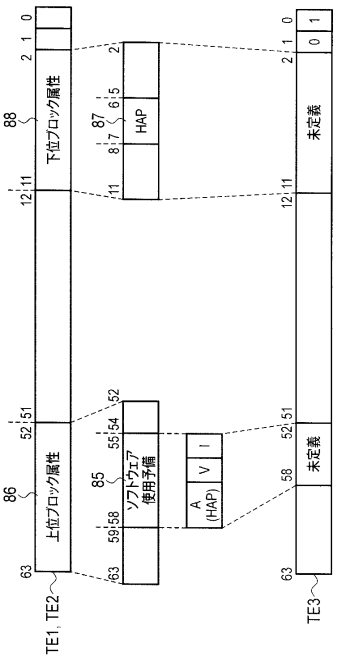
【図１６】

図16



【図１７】

図17



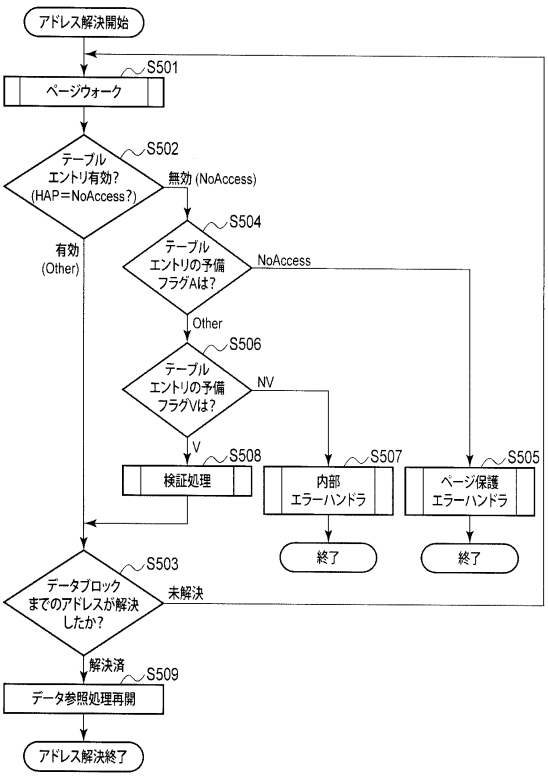
【図１８】

図18

HAP [1:0]	アクセス権限
00	NoAccess
01	Read-only
10	Write-only
11	Read／Write

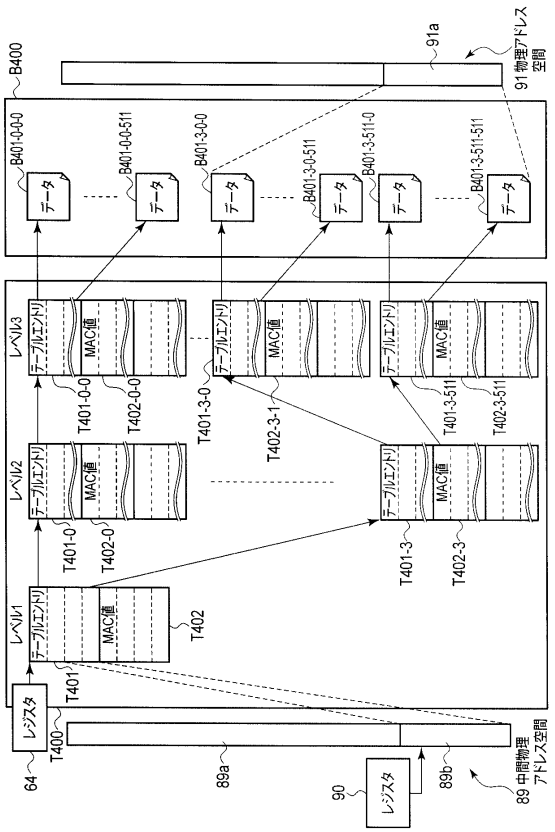
【図１９】

図19



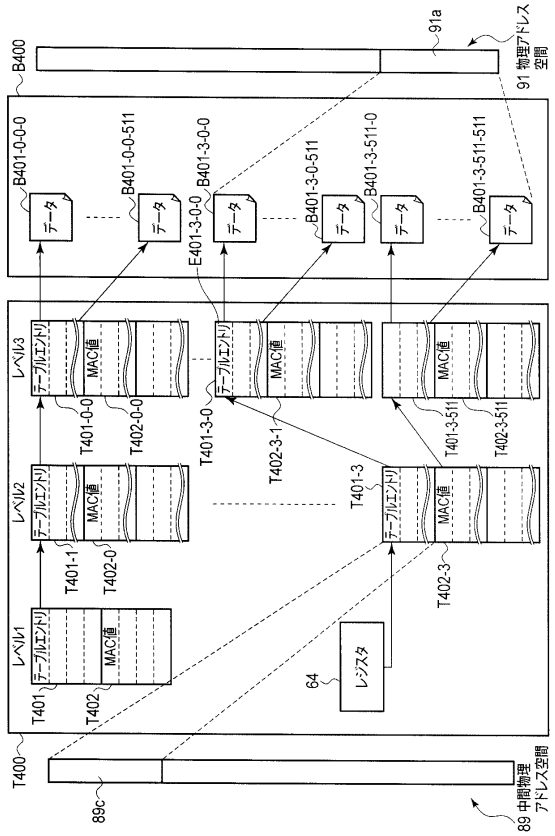
【図２０】

図20



【図２１】

図21



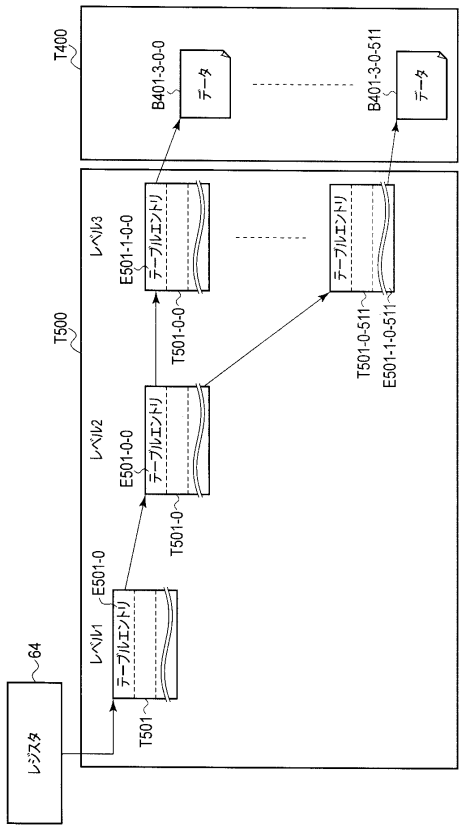
【図２２】

図22

	メモリマップ符号	物理アドレス領域	ブート時検証	ページ検証	未検証状態のブロック符号	サイズ
内部メモリ	8	0x00000000 ～ 0x000fffff	–	–	–	1MB
マスクROM	69	0x00100000 ～ 0x001fffff	–	–	–	1MB
セキュアVMM プログラム領域	701	0x00100000 ～ 0x001fffff	✓	–	–	1MB
物理アドレス領域 セキュアOS	702-704	0x02000000 ～ 0x0fffffff	–	✓	B401-0-1-0 ～ B401-0-128-511	254MB
セキュアVMM作業領域 セキュアVMMMAC領域	705-706	0x10000000 ～ 0x1fffffff	–	✓	B401-0-129-0 ～ B401-0-256-511	256MB
予備領域	710	0x20000000 ～ 0x3fffffff	–	–	B401-0-257-0 ～ B401-0-511-511	512MB
非セキュアOS領域	75	0x40000000 ～ 0x7fffffff	–	–	B401-1-0-0 ～ B401-1-511-511	1GB
予備領域	711	0x80000000 ～ 0xbfffffff	–	–	B401-2-0-0 ～ B401-2-511-511	1GB
セキュアOS領域	76	0xc0000000 ～ 0xffffffff	–	✓	B401-3-0-0 ～ B401-3-511-511	1GB

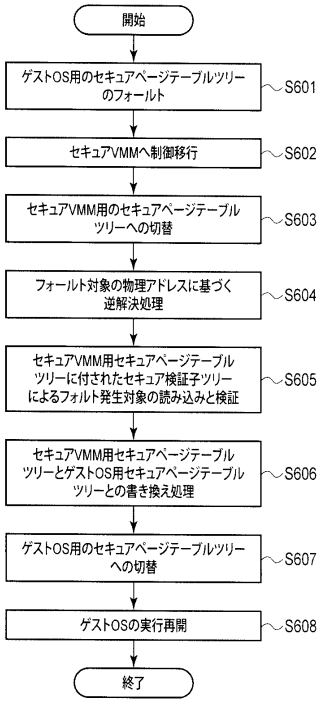
【図２３】

図23



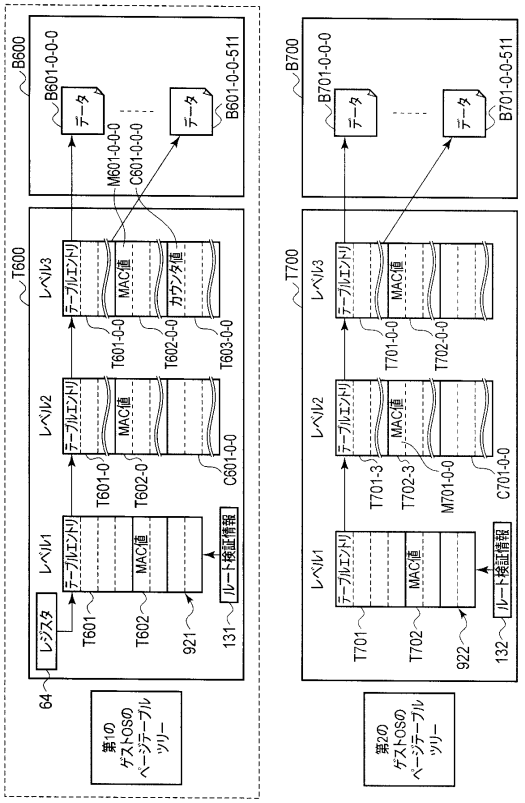
【図２４】

図24



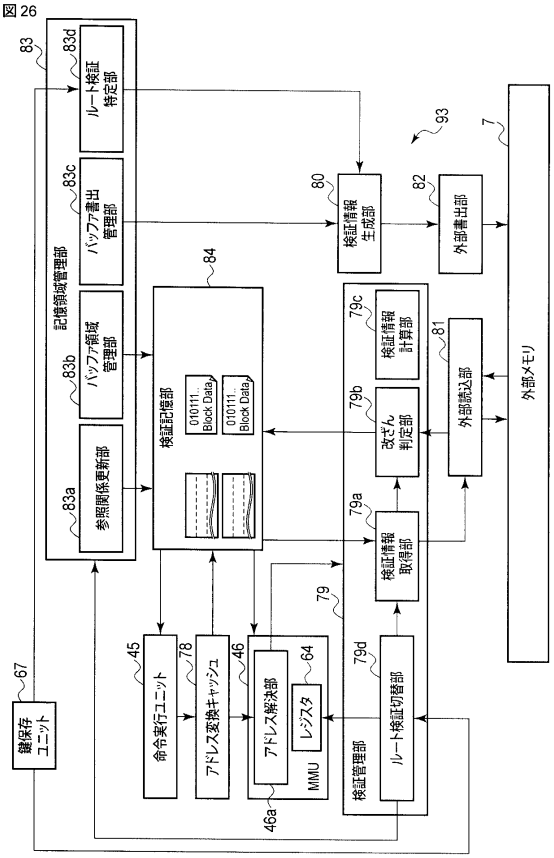
【図２５】

図25



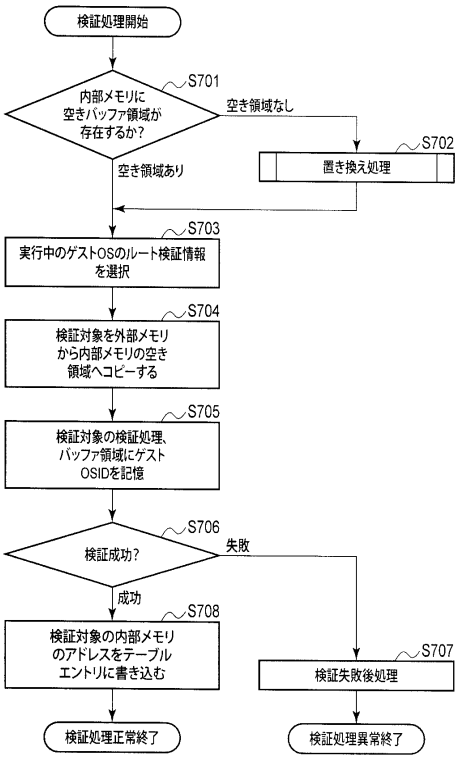
【図２６】

図26



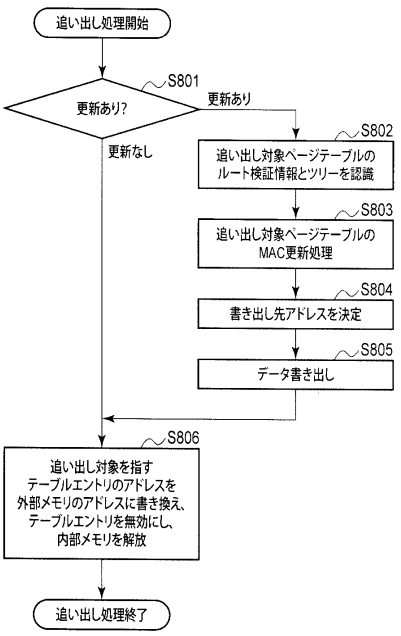
【図２７】

図27



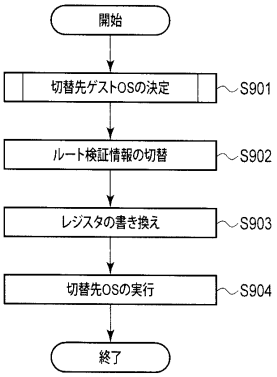
【図２８】

図28



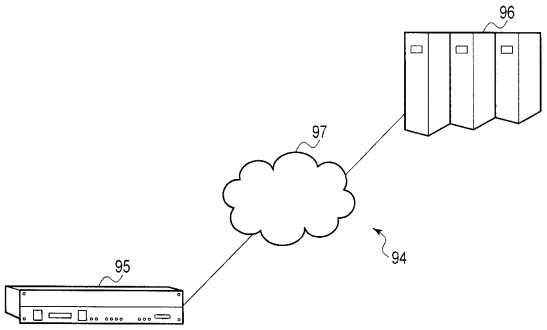
【図２９】

図29



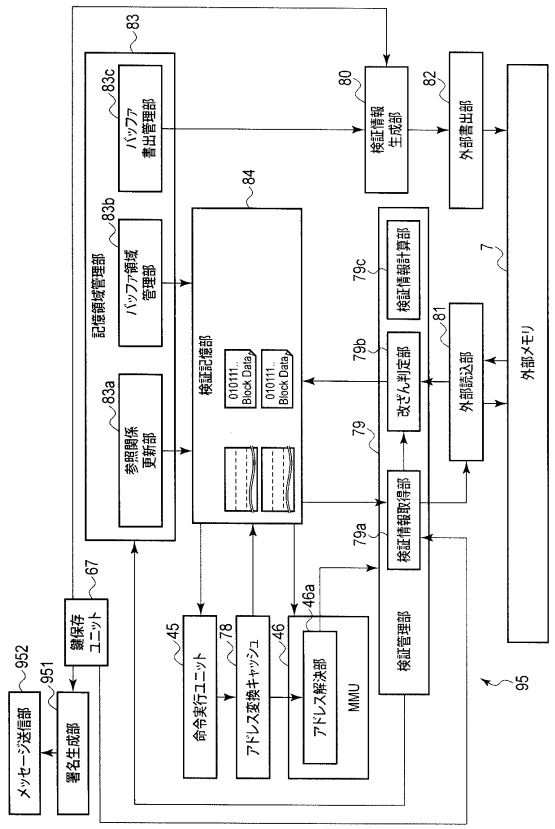
【図３０】

図30



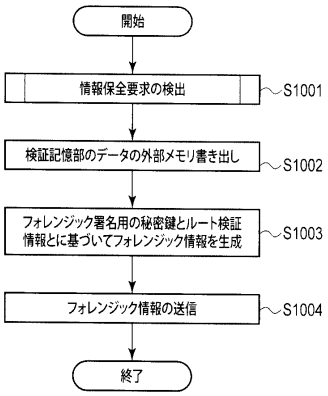
【図３１】

図31



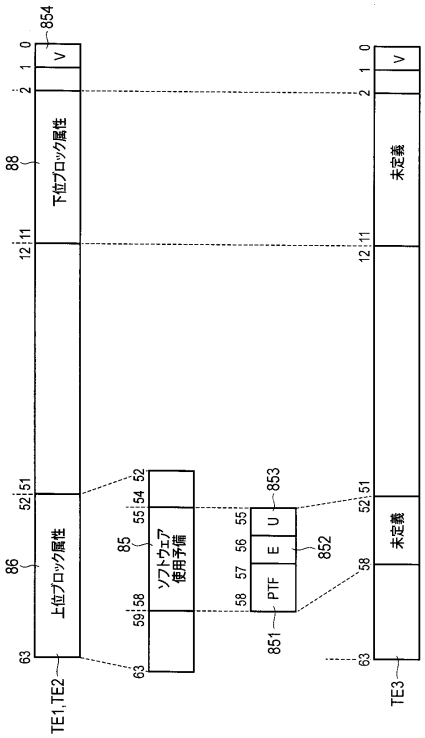
【図３２】

図32



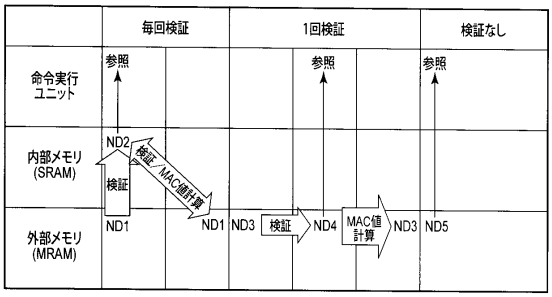
【図３３】

図33



【図３４】

図34



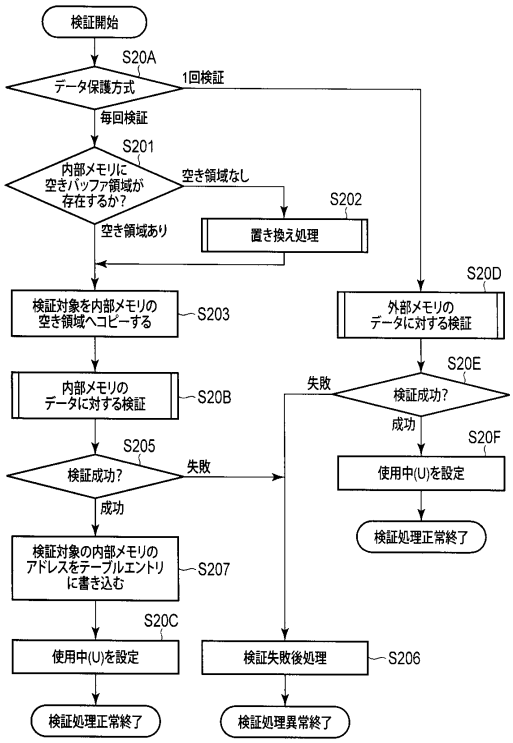
【図３５】

図35

PTF	使用状態(使用中)	有効／無効	次回参照データの状態	状態の符号
毎回検証(ETV)	0	0	外部メモリ(未検証)	ND1
	1	1	内部メモリ(検証済み)	ND2
1回検証(OTV)	0	0	外部メモリ(未検証)	ND3
	1	1	外部メモリ(検証済み)	ND4
検証なし(NOV)	1	1	外部メモリ(検証なし)	ND5

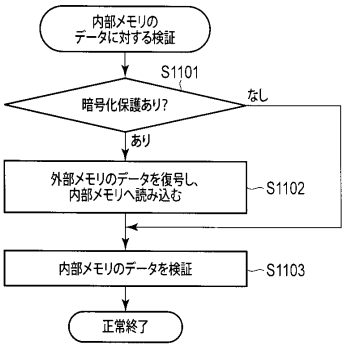
【図３６】

図36



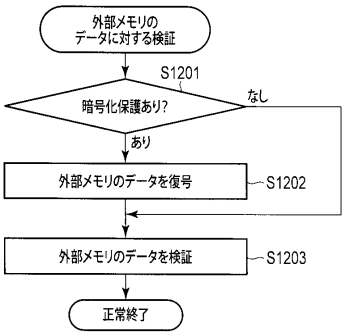
【図３７】

図37



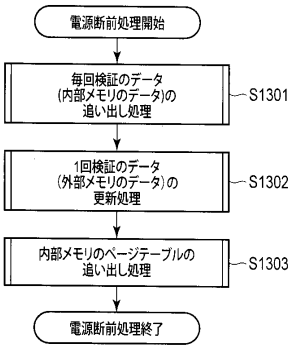
【図３８】

図38



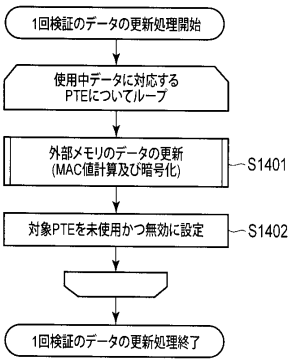
【図３９】

図39



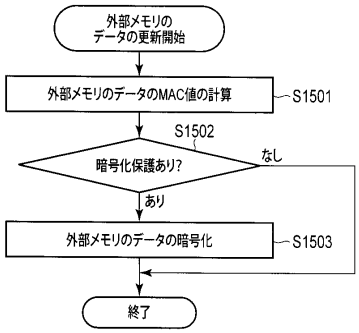
【図４０】

図40



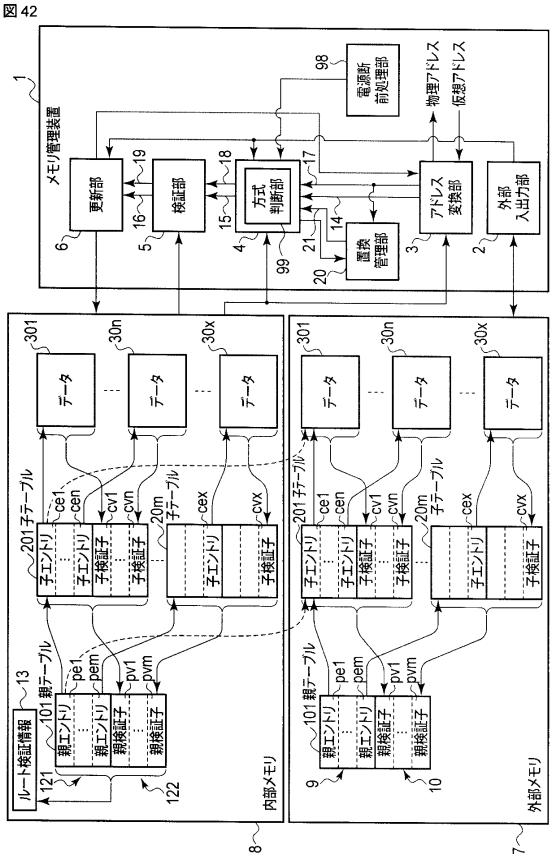
【図４１】

図41



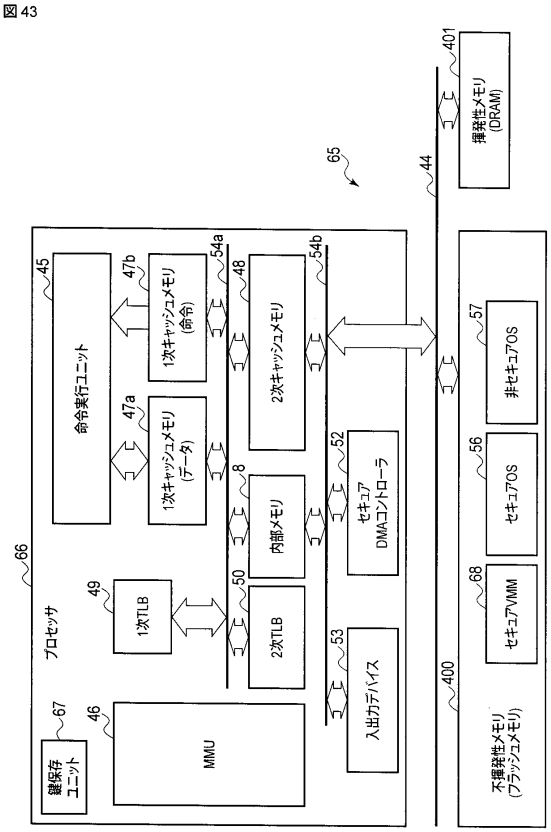
【図４２】

図42



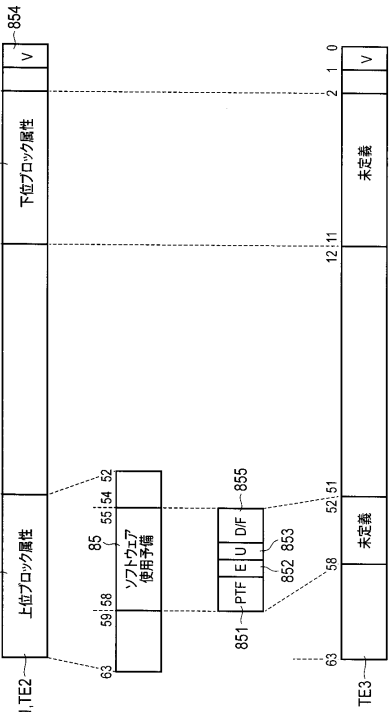
【図４３】

図43



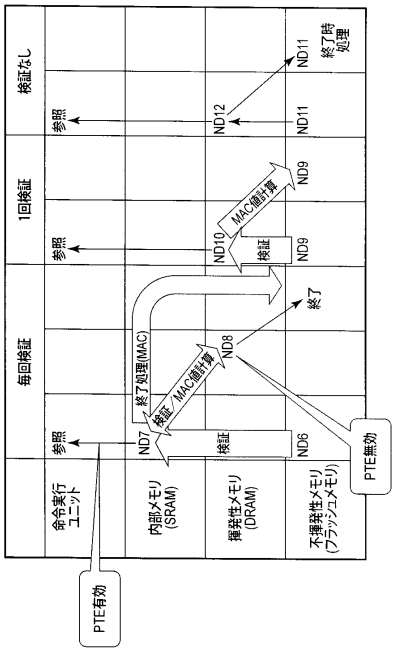
【図４４】

図44



【図４５】

図45



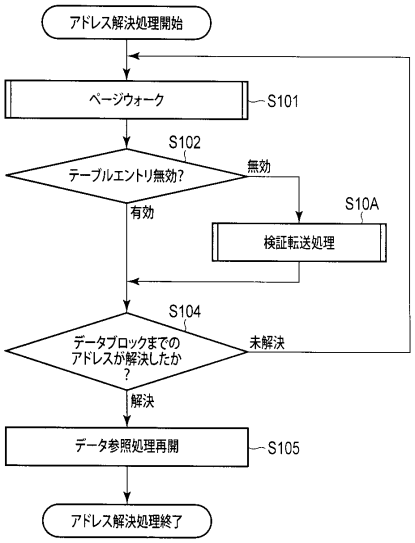
【図４６】

図46

PTF	D／F	有効／無効	次回参照データの状態	状態の符号
毎回検証(ETV)	F	0	フラッシュ(未検証)	ND6
	D	0	DRAM(未検証)	ND8
	D	1	内部メモリ(検証済み)	ND7
1回検証(OTV)	F	0	フラッシュ(未検証)	ND9
	D	1	DRAM(検証済み)	ND10
検証なし(NOV)	F	0	フラッシュ(検証なし)	ND11
	D	1	DRAM(検証なし)	ND12

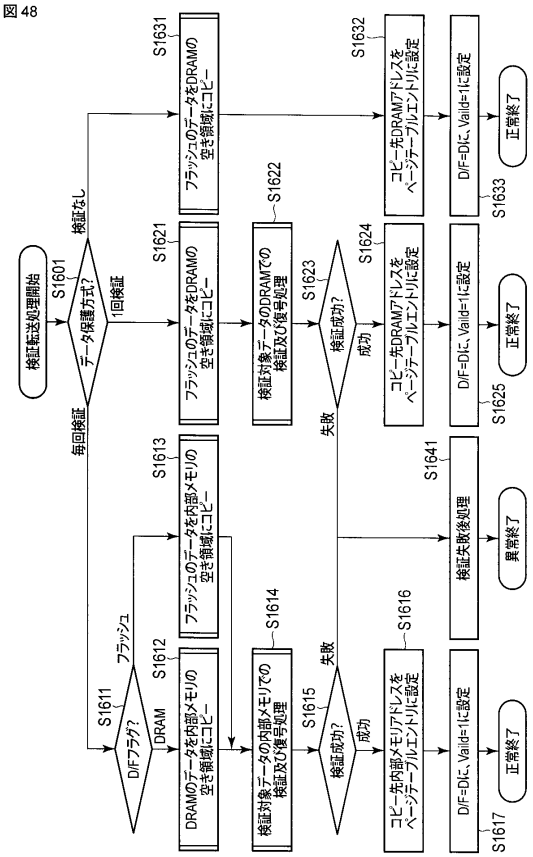
【図４７】

図47



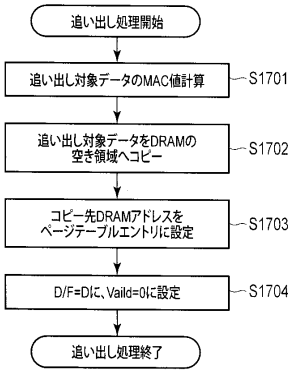
【図４８】

図48



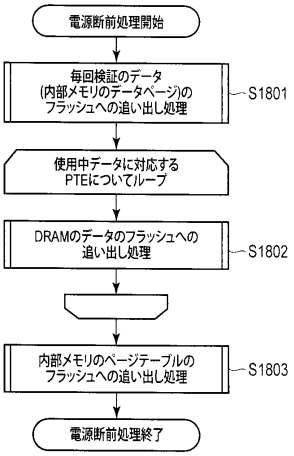
【図４９】

図49



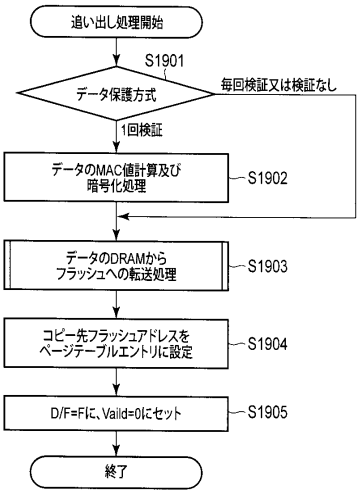
【図５０】

図50



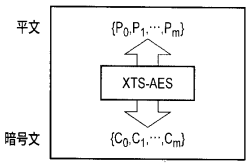
【図５１】

図51



【図５２】

図52



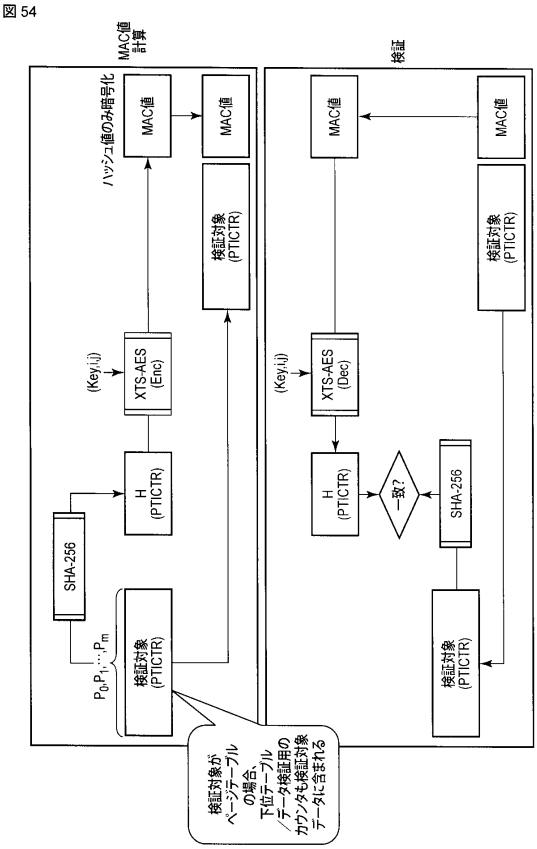
【図５３】

図53

	ビット数	フィールド	細目	ビット数
i	128	共通ページインデックス	ページアドレスインデックス	52
			レベル	3
		Count		73
j	128	(Count)		120(108)
		暗号ブロックのシーケンス番号		8(20)

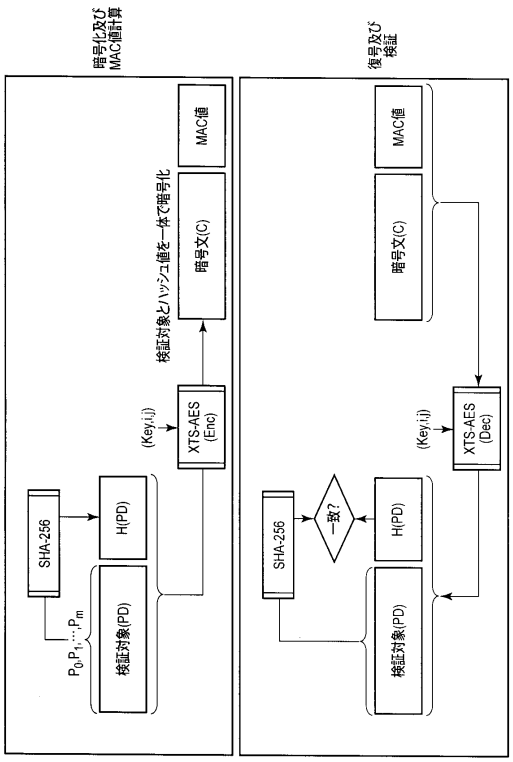
【図５４】

図54



【図５５】

図55



フロントページの続き

(72)発明者　林　良太郎
東京都港区芝浦一丁目１番１号　株式会社東芝内

審査官　金沢　史明

(56)参考文献　特開２０１２－０６８９５９（ＪＰ，Ａ）
特表２０１３－５２２７０２（ＪＰ，Ａ）
米国特許出願公開第２０１０／０１５３７３２（ＵＳ，Ａ１）
米国特許出願公開第２００８／０１４１２６６（ＵＳ，Ａ１）
Siddhartha Chhabra et al., SecureME: A Hardware-Software Approach to Full Sysem Security, Proceedings of the international conference on Supercomputing (ICS '11), 米国, ACM, ２０１１年　5月３１日, pp. 108-119

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ　２１／６４
Ｇ０６Ｆ　１２／１００９
Ｇ０６Ｆ　１２／１０３６