【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成29年6月15日(2017.6.15)

【公表番号】特表2016-541134(P2016-541134A)
【公表日】平成28年12月28日(2016.12.28)
【年通号数】公開・登録公報2016-070
【出願番号】特願2016-518121(P2016-518121)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｌ　9/14　(2006.01)
Ｇ０６Ｆ　21/60　(2013.01)
Ｇ０６Ｆ　21/62　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｄ
Ｈ０４Ｌ　9/00　６０１Ｅ
Ｈ０４Ｌ　9/00　６４１
Ｇ０６Ｆ　21/60　３２０
Ｇ０６Ｆ　21/62　３１８

【手続補正書】
【提出日】平成29年5月2日(2017.5.2)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
コンテンツのセキュリティを確保するためのメモリコントローラ内で使用できる方法であって、
メモリデバイス内の論理メモリ領域を異なるドメインに前記メモリコントローラにおいて割り当てるステップであって、前記メモリデバイスは、前記メモリコントローラの外部にある、割り当てるステップと、
ドメイン内の1つまたは複数のマスターに対するアクセス制御設定内のアクセス許可を、前記メモリコントローラにおいて定義するステップであって、前記アクセス許可は、前記ドメイン内の前記1つまたは複数のマスターに対する読出しアクセスおよび/または書込みアクセスのうちの少なくとも1つを指定する、定義するステップと、
前記異なるドメインごとに異なるドメイン固有鍵を前記メモリコントローラにおいて入手するステップであって、各ドメイン固有鍵は、少なくともマスター鍵と、ドメイン固有情報との関数であり、前記ドメイン固有情報は、前記ドメイン内の前記1つまたは複数のマスターに対する読出しアクセスおよび/または書込みアクセスのうちの少なくとも1つを指定する前記アクセス許可を含む、入手するステップと、
前記メモリデバイスとは別の独立したセキュアメモリ空間に前記ドメイン固有鍵を記憶するステップと、
ドメイン内の1つまたは複数のマスターに対するアクセス制御設定への変更が検出されると、前記セキュアメモリ空間に記憶されたドメイン固有鍵を更新するステップと、
各論理メモリ領域が割り当てられるドメインに対応するドメイン固有鍵を用いて、各論理メモリ領域に書き込まれるコンテンツを、前記メモリコントローラにおいて暗号化するステップと

を含む、方法。
【請求項２】
前記コンテンツが記憶される各論理メモリ領域が割り当てられるドメインに対応するドメイン固有鍵を用いて、各論理メモリ領域から読み出されるコンテンツを、前記メモリコントローラにおいて解読するステップとさらに含む、請求項1に記載の方法。
【請求項３】
第1のメモリ領域が割り当てられる第1のドメインに関連付けられるすべてのマスターに対して、第1の論理メモリ領域へのアクセスを制限するステップをさらに含む、請求項1に記載の方法。
【請求項４】
前記ドメイン固有鍵は生成されるか、またはあらかじめ生成された1組の鍵から選択される、請求項1に記載の方法。
【請求項５】
前記メモリコントローラまたはセキュアドプロセッサにおいて前記ドメイン固有鍵を生成するステップをさらに含む、請求項1に記載の方法。
【請求項６】
第1のメモリ領域内の第1のメモリページが第1のドメイン固有鍵に関連付けられ、第1のドメインに割り当てられ、前記第1のメモリ領域内の第2のページが第2のドメイン固有鍵に関連付けられ、第2のドメインに割り当てられる、請求項1に記載の方法。
【請求項７】
第1の論理メモリ領域を第1のドメインから第2のドメインに動的に再割当てするステップをさらに含み、前記第1のドメインおよび前記第2のドメインは異なるドメイン固有鍵に関連付けられる、請求項1に記載の方法。
【請求項８】
前記第1のドメインから前記第2のドメインへの前記第1の論理メモリ領域の前記再割当ては、前記第1の論理メモリ領域からコンテンツを消去することなく行われる、請求項7に記載の方法。
【請求項９】
前記ドメイン固有鍵は、前記メモリコントローラのリセット時に自動的に変更される、請求項1に記載の方法。
【請求項１０】
第1のドメイン固有鍵が第1の論理メモリ領域に関連付けられ、第1のドメインおよび第2のドメインに割り当てられ、前記第1のドメイン固有鍵は、少なくともマスター鍵と、前記第1のドメインからの第1のドメイン固有情報と、前記第2のドメインからの第2のドメイン固有情報との関数である、請求項1に記載の方法。
【請求項１１】
メモリコントローラであって、
メモリデバイス内の論理メモリ領域を異なるドメインに割り当てるように構成されるメモリ割当て回路であって、前記メモリデバイスは、前記メモリコントローラの外部にある、メモリ割当て回路と、
ドメイン内の1つまたは複数のマスターに対するアクセス制御設定内のアクセス許可を定義するように構成されるアクセス制御回路であって、前記アクセス許可は、前記ドメイン内の前記1つまたは複数のマスターに対する読出しアクセスおよび/または書込みアクセスのうちの少なくとも1つを指定する、アクセス制御回路と、
前記異なるドメインごとに異なるドメイン固有鍵を入手するように構成されるドメイン固有鍵発生器回路であって、各ドメイン固有鍵は、少なくともマスター鍵と、ドメイン固有情報との関数であり、前記ドメイン固有情報は、前記ドメイン内の前記1つまたは複数のマスターに対する読出しアクセスおよび/または書込みアクセスのうちの少なくとも1つを指定する前記アクセス許可を含む、ドメイン固有鍵発生器回路と、
各論理メモリ領域が割り当てられるドメインに対応するドメイン固有鍵を用いて、各論

理メモリ領域に書き込まれるコンテンツを暗号化するように構成されるコンテンツ暗号化回路と
を備え、
前記ドメイン固有鍵発生器回路は、
前記メモリデバイスとは別の独立したセキュアメモリ空間に前記ドメイン固有鍵を記憶し、かつ、
ドメイン内の1つまたは複数のマスターに対するアクセス制御設定への変更が検出されると、前記セキュアメモリ空間に記憶されたドメイン固有鍵を更新する
ようにさらに構成される、メモリコントローラ。
【請求項１２】
前記コンテンツを要求するマスターと、前記コンテンツが記憶される各論理メモリ領域が割り当てられるドメインとに対応するドメイン固有鍵を用いて各論理メモリ領域から読み出されるコンテンツを解読するように構成されるコンテンツ解読回路をさらに備える、請求項11に記載のメモリコントローラ。
【請求項１３】
前記アクセス制御回路は、第1の論理メモリ領域へのアクセスを、第1のメモリ領域が割り当てられる第1のドメインに関連付けられる第1のマスターのみに制限するようにさらに構成される、請求項11に記載のメモリコントローラ。
【請求項１４】
前記ドメイン固有鍵は動的に生成されるか、またはあらかじめ生成された1組の鍵から動的に選択される、請求項11に記載のメモリコントローラ。
【請求項１５】
前記ドメイン固有鍵発生器回路は、前記ドメイン固有鍵を前記メモリコントローラのみがアクセス可能なレジスタ内に記憶するようにさらに構成される、請求項11に記載のメモリコントローラ。
【請求項１６】
前記ドメイン固有鍵発生器回路は、前記メモリコントローラにおいて前記ドメイン固有鍵を生成するか、またはセキュアドプロセッサから前記ドメイン固有鍵を入手するように構成される、請求項11に記載のメモリコントローラ。
【請求項１７】
第1のメモリ領域内の第1のメモリページが第1のドメイン固有鍵に関連付けられ、第1のドメインに割り当てられ、前記第1のメモリ領域内の第2のページが第2のドメイン固有鍵に関連付けられ、第2のドメインに割り当てられる、請求項11に記載のメモリコントローラ。
【請求項１８】
前記メモリ割当て回路は、第1の論理メモリ領域を第1のドメインから第2のドメインに動的に再割当てするようにさらに構成され、前記第1のドメインおよび前記第2のドメインは異なるドメイン固有鍵に関連付けられる、請求項11に記載のメモリコントローラ。
【請求項１９】
前記第1のドメインから前記第2のドメインへの前記第1の論理メモリ領域の前記再割当ては、前記第1の論理メモリ領域からコンテンツを消去することなく行われる、請求項18に記載のメモリコントローラ。
【請求項２０】
前記ドメイン固有鍵は、前記メモリコントローラのリセット時に自動的に変更される、請求項11に記載のメモリコントローラ。
【請求項２１】
第1のドメイン固有鍵が第1の論理メモリ領域に関連付けられ、第1のドメインおよび第2のドメインに割り当てられ、前記第1のドメイン固有鍵は、少なくともマスター鍵と、前記第1のドメインからの第1のドメイン固有情報と、前記第2のドメインからの第2のドメイン固有情報との関数である、請求項11に記載のメモリコントローラ。

【請求項２２】
メモリコントローラであって、
メモリデバイス内の論理メモリ領域を異なるドメインに割り当てるための手段であって、前記メモリデバイスは、前記メモリコントローラの外部にある、割り当てるための手段と、
ドメイン内の1つまたは複数のマスターに対するアクセス制御設定内のアクセス許可を定義するための手段であって、前記アクセス許可は、前記ドメイン内の前記1つまたは複数のマスターに対する読出しアクセスおよび/または書込みアクセスのうちの少なくとも1つを指定する、定義するための手段と、
前記異なるドメインごとに異なるドメイン固有鍵を入手するための手段であって、各ドメイン固有鍵は、少なくともマスター鍵と、ドメイン固有情報との関数であり、前記ドメイン固有情報は、前記ドメイン内の前記1つまたは複数のマスターに対する読出しアクセスおよび/または書込みアクセスのうちの少なくとも1つを指定する前記アクセス許可を含む、入手するための手段と、
前記メモリデバイスとは別の独立したセキュアメモリ空間に前記ドメイン固有鍵を記憶するための手段と、
ドメイン内の1つまたは複数のマスターに対するアクセス制御設定への変更が検出されると、前記セキュアメモリ空間に記憶されたドメイン固有鍵を更新するための手段と、
各論理メモリ領域が割り当てられるドメインに対応するドメイン固有鍵を用いて、各論理メモリ領域に書き込まれるコンテンツを暗号化するための手段と
を備える、メモリコントローラ。
【請求項２３】
前記コンテンツが記憶される各論理メモリ領域が割り当てられるドメインに対応するドメイン固有鍵を用いて、各論理メモリ領域から読み出されるコンテンツを、前記メモリコントローラにおいて解読するための手段とさらに備える、請求項22に記載のメモリコントローラ。
【請求項２４】
命令を記憶している非一時的機械可読記憶媒体であって、メモリコントローラ内の少なくとも1つのプロセッサによって実行されるときに、前記少なくとも1つのプロセッサに、
メモリデバイス内の論理メモリ領域を異なるドメインに割り当てることであって、前記メモリデバイスは、前記メモリコントローラの外部にある、割り当てることと、
ドメイン内の1つまたは複数のマスターに対するアクセス制御設定内のアクセス許可を定義することであって、前記アクセス許可は、前記ドメイン内の前記1つまたは複数のマスターに対する読出しアクセスおよび/または書込みアクセスのうちの少なくとも1つを指定する、定義することと、
前記異なるドメインごとに異なるドメイン固有鍵を入手することであって、各ドメイン固有鍵は、少なくともマスター鍵と、ドメイン固有情報との関数であり、前記ドメイン固有情報は、前記ドメイン内の前記1つまたは複数のマスターに対する読出しアクセスおよび/または書込みアクセスのうちの少なくとも1つを指定する前記アクセス許可を含む、入手することと、
前記メモリデバイスとは別の独立したセキュアメモリ空間に前記ドメイン固有鍵を記憶することと、
ドメイン内の1つまたは複数のマスターに対するアクセス制御設定への変更が検出されると、前記セキュアメモリ空間に記憶されたドメイン固有鍵を更新することと、
各論理メモリ領域が割り当てられるドメインに対応するドメイン固有鍵を用いて、各論理メモリ領域に書き込まれるコンテンツを暗号化することと
を行わせる、命令を記憶している非一時的機械可読記憶媒体。
【請求項２５】
前記セキュアメモリ空間は、前記メモリコントローラを含む集積回路内に配置される、請求項1に記載の方法。

【請求項２６】
前記セキュアメモリ空間は、ユーザ制御アプリケーションに対してアクセス不可能である、請求項1に記載の方法。
【請求項２７】
前記セキュアメモリ空間は、前記メモリコントローラを含む集積回路内に配置される、請求項11に記載のメモリコントローラ。
【請求項２８】
前記セキュアメモリ空間は、前記メモリコントローラを含む集積回路内に配置される、請求項22に記載のメモリコントローラ。
【請求項２９】
前記セキュアメモリ空間は、前記メモリコントローラを含む集積回路内に配置される、請求項24に記載の非一時的機械可読記憶媒体。