【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６部門第３区分
【発行日】平成26年1月30日(2014.1.30)

【公開番号】特開2013-251016(P2013-251016A)
【公開日】平成25年12月12日(2013.12.12)
【年通号数】公開・登録公報2013-067
【出願番号】特願2013-194105(P2013-194105)
【国際特許分類】
Ｇ０６Ｆ　21/57　　(2013.01)
Ｇ０６Ｆ　21/44　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/00　　１５７Ｂ
Ｇ０６Ｆ　21/20　　１４４Ｂ

【手続補正書】
【提出日】平成25年12月3日(2013.12.3)
【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】
セキュアなエントリ命令をデコードするデコーダと、
前記セキュアなエントリ命令がデコードされると、複数の個々の認証済みコードモジュール、認証済みコードモジュールと前記認証済みコードモジュールを実行するプロセッサとの対応関係を示すエントリを有する整合テーブル、及び、マスタヘッダを含むマスタ認証済みコードモジュールの前記整合テーブルから自身のプロセッサに対応するエントリを見つけ、前記マスタ認証済みコードモジュールから前記マスタヘッダ及び見つけた前記エントリに示される前記複数の個々の認証済みコードモジュールの１つを読み出す制御ロジックと、
を備えるプロセッサ。
【請求項２】
セキュアなモードに構成されるキャッシュをさらに備え、
前記制御ロジックは、前記マスタヘッダおよび前記個々の認証済みコードモジュールを、前記セキュアなモードに構成された前記キャッシュへと読み込む、
請求項１に記載のプロセッサ。
【請求項３】
前記制御ロジックはさらに、前記マスタヘッダおよび前記個々の認証済みコードモジュールを前記キャッシュ内で認証する、
請求項２に記載のプロセッサ。
【請求項４】
前記制御ロジックはさらに、前記マスタヘッダおよび前記個々の認証済みコードモジュールを認証した後で、マスタハッシュをトークンに送信する、
請求項３に記載のプロセッサ。
【請求項５】
第１のプロセッサにより、認証済みコードモジュールと前記認証済みコードモジュールを実行するプロセッサとの対応関係を示すエントリを有するマスタ認証済みコードモジュールの整合テーブルから、前記第１のプロセッサに対応する第１のエントリを見つける段

階と、
前記第１のプロセッサにより、マスタヘッダを、前記マスタ認証済みコードモジュールから第１のセキュアなメモリにロードする段階と、
前記第１のプロセッサにより、見つけた前記第１のエントリに示される前記第１のプロセッサの第１の個々の認証済みコードモジュールを、マスタ認証済みコードモジュールから前記第１のセキュアなメモリにロードする段階と、
を備える方法。
【請求項６】
前記第１のプロセッサにより、セキュアなエントリ命令を発行する段階をさらに備え、
前記第１のエントリを見つける段階、前記マスタヘッダをロードする段階、および前記第１の個々の認証済みコードモジュールをロードする段階は、前記セキュアなエントリ命令を発行する段階に対して行われる、
請求項５に記載の方法。
【請求項７】
前記第１のセキュアなメモリは、前記第１のプロセッサのキャッシュメモリである、
請求項５に記載の方法。
【請求項８】
前記第１のプロセッサにより、前記マスタヘッダおよび前記第１の個々の認証済みコードモジュールを前記第１のセキュアなメモリ内で認証する段階をさらに備える、
請求項５に記載の方法。
【請求項９】
前記マスタヘッダおよび前記第１の個々の認証済みコードモジュールを認証する段階の後で、前記第１のプロセッサによりマスタハッシュをトークンに送信する段階をさらに備える、
請求項８に記載の方法。
【請求項１０】
第２のプロセッサにより、前記マスタ認証済みコードモジュールの前記整合テーブルから、前記第２のプロセッサに対応する第２のエントリを見つける段階と、
前記第２のプロセッサにより、前記マスタヘッダを、前記マスタ認証済みコードモジュールから第２のセキュアなメモリにロードする段階と、
前記第２のプロセッサにより、前記第２のプロセッサの第２の個々の認証済みコードモジュールを、前記マスタ認証済みコードモジュールから前記第２のセキュアなメモリにロードする段階とを備える、
請求項５に記載の方法。
【請求項１１】
前記第２のセキュアなメモリは、前記第２のプロセッサのキャッシュメモリである、
請求項１０に記載の方法。
【請求項１２】
前記第２のプロセッサにより、前記マスタヘッダおよび前記第２の個々の認証済みコードモジュールを前記第２のセキュアなメモリ内で認証する段階をさらに備える、
請求項１０に記載の方法。
【請求項１３】
第１のプロセッサと第２のプロセッサとを備えるシステムであって、
前記第１のプロセッサは、
セキュアなエントリ命令を復号するデコーダと、
セキュアなエントリメッセージを送信するメッセージングロジックと、
前記セキュアなエントリ命令が復号されると、認証済みコードモジュールと前記認証済みコードモジュールを実行するプロセッサとの対応関係を示すエントリを有するマスタ認証済みコードモジュールの整合テーブルから、前記第１のプロセッサに対応する第１のエントリを見つけ、前記マスタ認証済みコードモジュールからマスタヘッダおよび見つけた

前記第１のエントリに示される第１の個々の認証済みコードモジュールを読み出す第１の制御ロジックとを有し、
前記第２のプロセッサは、
前記セキュアなエントリメッセージを受信するメッセージングロジックと、
前記セキュアなエントリメッセージが受信されると、前記マスタ認証済みコードモジュールの前記整合テーブルから、前記第２のプロセッサに対応する第２のエントリを見つけ、前記マスタ認証済みコードモジュールから前記マスタヘッダおよび見つけた前記第２のエントリに示される第２の個々の認証済みコードモジュールを読み出す第２の制御ロジックとを有する、
システム。
【請求項１４】
不揮発性格納装置をさらに備え、前記不揮発性格納装置は、前記整合テーブルと、前記第１の個々の認証済みコードモジュールと、前記第２の個々の認証済みコードモジュールと、マスタハッシュとを含む前記マスタ認証済みコードモジュールを格納し、前記マスタハッシュは、前記整合テーブルと、前記第１の個々の認証済みコードモジュールと、前記第２の個々の認証済みコードモジュールとに基づく、
請求項１３に記載のシステム。
【請求項１５】
前記マスタ認証済みコードモジュールが前記不揮発性格納装置からロードされるシステムメモリをさらに備える、
請求項１４に記載のシステム。
【請求項１６】
前記マスタヘッダおよび前記第１の個々の認証済みコードモジュールを前記第１のプロセッサのセキュアなメモリ内で認証した後で、前記マスタ認証済みコードモジュールのマスタハッシュをロードするトークンをさらに備える、
請求項１３に記載のシステム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００４６
【補正方法】変更
【補正の内容】
【００４６】
以上のように、複数の認証済みコードモジュールを利用してセキュアなコンピューティング環境に入るシステム、装置、および方法を記載してきた。特定の実施形態に限って説明、および図示してきたが、これら実施形態は広義の発明の例示であり限定は意図しておらず、当業者であれば様々な他の変形例を想到することが明らかであり、記載、図示してきた特定の構成および配置に本発明を限定することは意図されていないことに留意されたい。本技術分野は急速な進歩を遂げており、未来の技術進化を予測することは難しく、未来の技術進歩如何によって、本開示の原理または添付請求項の範囲を逸脱することなく、開示されている実施形態の配置、詳細等を修正可能になるであろうことは容易に予想がつく。本発明の実施形態の例を項目として示す。
［項目１］
セキュアなエントリ命令を復号するデコーダと、
セキュアなエントリ命令が復号されると、
１以上のプロセッサのための１以上の認証済みコードモジュール、及び、認証済みコードモジュールと認証済みコードモジュールを実行するプロセッサとの対応関係を示すエントリを有する整合テーブル、並びに、マスタハッシュを含むマスタヘッダ、を有するマスタ認証済みコードモジュール中における整合テーブルから、自身のプロセッサに対応するエントリを見つけ、マスタ認証済みコードモジュールからマスタヘッダおよび見つけたエントリに示される個々の認証済みコードモジュールを読み出す制御論理と、

を備え、
認証済みコードモジュールの各々は対応するハッシュと、コード及びデータとを含み、マスタハッシュは、整合テーブル、及び、複数の認証済みコードモジュールの複数の対応するハッシュに基づいて生成される、
プロセッサ。
［項目２］
セキュアなモードに構成されるキャッシュをさらに備え、
制御論理は、マスタヘッダおよび個々の認証済みコードモジュールを、セキュアなモードに構成されたキャッシュへと読み込む項目１に記載のプロセッサ。
［項目３］
制御論理はさらに、マスタヘッダおよび個々の認証済みコードモジュールをキャッシュ内で認証する項目２に記載のプロセッサ。
［項目４］
制御論理はさらに、マスタヘッダおよび個々の認証済みコードモジュールを認証した後で、マスタハッシュをトークンに送信する項目３に記載のプロセッサ。
［項目５］
第１のプロセッサにより、
１以上のプロセッサのための１以上の認証済みコードモジュール、及び、認証済みコードモジュールと認証済みコードモジュールを実行するプロセッサとの対応関係を示すエントリを有する整合テーブル、並びに、マスタハッシュを含むマスタヘッダ、を有するマスタ認証済みコードモジュール中における整合テーブルから、第１のプロセッサに対応する第１のエントリを見つける段階と、
第１のプロセッサにより、マスタヘッダを、マスタ認証済みコードモジュールから第１のセキュアなメモリにロードする段階と、
第１のプロセッサにより、見つけたエントリに示される第１のプロセッサの第１の個々の認証済みコードモジュールを、マスタコードモジュールから第１のセキュアなメモリにロードする段階と
を備え、
認証済みコードモジュールの各々は対応するハッシュと、コード及びデータとを含み、マスタハッシュは、整合テーブル、及び、複数の認証済みコードモジュールの複数の対応するハッシュに基づいて生成される、
方法。
［項目６］
第１のプロセッサにより、セキュアなエントリ命令を受信する段階をさらに備え、
第１のエントリを見つける段階、マスタヘッダをロードする段階、および第１の個々の認証済みコードモジュールをロードする段階は、セキュアなエントリ命令を発行する段階が行われると行われる項目５に記載の方法。
［項目７］
第１のセキュアなメモリは、第１のプロセッサのキャッシュメモリである項目５又は６に記載の方法。
［項目８］
第１のプロセッサにより、マスタヘッダおよび第１の個々の認証済みコードモジュールを第１のセキュアなメモリ内で認証する段階をさらに備える項目５から７のいずれか１項に記載の方法。
［項目９］
第１のプロセッサにより、マスタヘッダおよび第１の個々の認証済みコードモジュールを認証する段階の後で、マスタハッシュをトークンに送信する段階をさらに備える項目８に記載の方法。
［項目１０］
第２のプロセッサにより、マスタ認証済みコードモジュールの整合テーブルから、第２

のプロセッサに対応する第２のエントリを見つける段階と、
　第２のプロセッサにより、マスタヘッダを、マスタ認証済みコードモジュールから第２のセキュアなメモリにロードする段階と、
　第２のプロセッサにより、第２のプロセッサの第２の個々の認証済みコードモジュールを、マスタコードモジュールから第２のセキュアなメモリにロードする段階とをさらに備える項目５から９のいずれか１項に記載の方法。
［項目１１］
　第２のセキュアなメモリは、第２のプロセッサのキャッシュメモリである項目１０に記載の方法。
［項目１２］
　第２のプロセッサにより、マスタヘッダおよび第２の個々の認証済みコードモジュールを第２のセキュアなメモリ内で認証する段階をさらに備える項目１０又は１１に記載の方法。
［項目１３］
　第１のプロセッサと第２のプロセッサとを備えるシステムであって、
　第１のプロセッサは、
　セキュアなエントリ命令を復号するデコーダと、
　セキュアなエントリメッセージを送信するメッセージング論理と、
　セキュアなエントリ命令が復号されると、
　１以上のプロセッサのための１以上の認証済みコードモジュール、及び、認証済みコードモジュールと認証済みコードモジュールを実行するプロセッサとの対応関係を示すエントリを有する整合テーブル、並びに、マスタハッシュを含むマスタヘッダ、を有するマスタ認証済みコードモジュール中における整合テーブルから、第１のプロセッサに対応する第１のエントリを見つけ、マスタ認証済みコードモジュールからマスタヘッダおよび見つけた第１のエントリに示される第１の個々の認証済みコードモジュールを読み出す第１の制御論理とを有し、
　第２のプロセッサは、
　セキュアなエントリメッセージを受信するメッセージング論理と、
　セキュアなエントリメッセージが受信されると、マスタ認証済みコードモジュールの整合テーブルから、第２のプロセッサに対応する第２のエントリを見つけ、マスタ認証済みコードモジュールからマスタヘッダおよび見つけた第２のエントリに示される第２の個々の認証済みコードモジュールを読み出す第２の制御論理とを有し、
　認証済みコードモジュールの各々は対応するハッシュと、コード及びデータとを含み、マスタハッシュは、整合テーブル及び複数の認証済みコードモジュールの複数の対応するハッシュに基づいて生成される、
　システム。
［項目１４］
　マスタ認証済みコードモジュールを格納する不揮発性格納装置をさらに備える項目１３に記載のシステム。
［項目１５］
　マスタ認証済みコードモジュールが不揮発性格納装置からロードされるシステムメモリをさらに備える項目１４に記載のシステム。
［項目１６］
　マスタヘッダおよび第１の個々の認証済みコードモジュールを第１のプロセッサのセキュアなメモリ内で認証した後で、マスタ認証済みコードモジュールのマスタハッシュをロードするトークンをさらに備える項目１５に記載のシステム。