【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17年2月17日(2005.2.17)

【公表番号】特表2004-523015(P2004-523015A)
【公表日】平成16年7月29日(2004.7.29)
【年通号数】公開・登録公報2004-029
【出願番号】特願2002-508208(P2002-508208)
【国際特許分類第７版】
　ＧＯ６Ｆ　12/14
　ＧＯ６Ｆ　 1/00
【ＦＩ】
　ＧＯ６Ｆ　12/14　　３１０Ｈ
　ＧＯ６Ｆ　12/14　　３２０Ｂ
　ＧＯ６Ｆ　 9/06　　６６０Ｌ

【手続補正書】
【提出日】平成15年2月3日(2003.2.3)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
実行ユニットと、
前記実行ユニットに結合され、安全なメモリ区分への任意のアクセスを監視する安全な区分実施ロジックであって、区分エントリ・ポイントへの、または前記安全な区分内の別の位置から前記安全な区分内の位置への命令以外の命令の実行がトラップされる安全な区分実施ロジックと、
前記実行ユニットに結合された暗号ロジックと
を備えるプロセッサ。
【請求項２】
複数の安全な区分レジスタをさらに備える請求項１に記載のプロセッサ。
【請求項３】
安全な区分レジスタが区分エントリ・ポイント・レジスタを含む請求項２に記載のプロセッサ。
【請求項４】
暗号ロジックに結合されたアドレス変換バッファをさらに備え、安全な区分実施ロジックが実行ユニットとアドレス変換バッファとの間に結合された請求項３に記載のプロセッサ。
【請求項５】
第１のメモリと、
前記第１のメモリに結合され、仮想メモリ位置の区分を確立し、その区分へのアクセスを監視する安全な区分実施ロジックを含むプロセッサであって、区分エントリ・ポイントへの、または前記区分内の別の位置から前記区分内の位置への命令以外の命令の実行がトラップされるプロセッサと
を備えるコンピュータ・システム。
【請求項６】
プロセッサがさらに暗号ロジックを含む請求項５に記載のコンピュータ・システム。

【請求項７】
不揮発性メモリをさらに備え、安全な区分ロジックがさらに、不揮発性メモリ中に安全なメモリ位置区分を確立する請求項６に記載のコンピュータ・システム。
【請求項８】
不揮発性メモリが検証実施命令を記憶し、プロセッサがさらに、検証実施命令の信憑性を検証するためのブートストラップ・セキュリティ・ロジックを含む請求項６に記載のコンピュータ・システム。
【請求項９】
プロセッサがさらに、区分エントリ・ポイントを第１のメモリに記憶するための区分エントリ・ポイント・レジスタを含む請求項６に記載のコンピュータ・システム。
【請求項１０】
命令を実行する前に前記命令を調べることと、
前記命令が仮想メモリ中の位置区分内の位置への未許可アクセスであるときは、前記命令を実行しないと決定することと、
前記命令が区分エントリ・ポイントへの、または前記区分内の別の位置から仮想メモリ中の前記位置区分内の位置への命令であるときは、前記命令の実行を許可することとを含む命令処理方法。
【請求項１１】
命令を実行しないとする前記決定がさらに、トラップ・ハンドラにトラップすることを含む請求項１０に記載の方法。
【請求項１２】
命令が区分内の位置にあるデータに作用するものであり、命令が区分内に記憶されていないときは、命令は未許可アクセスである請求項１０に記載の方法。
【請求項１３】
命令が区分外の位置からの分岐であり、分岐が区分内の位置への分岐であり、分岐が区分エントリ・ポイントへの分岐でないときは、命令は未許可アクセスである請求項１０に記載の方法。
【請求項１４】
命令が区分エントリ・ポイントに記憶されておらず、前に実行された命令が区分の開始の直前の命令であったときもまた、命令は未許可アクセスである請求項１３に記載の方法。
【請求項１５】
命令が区分内のある位置から区分内の別の位置に分岐するときは、命令を実行すること、および
命令が区分外の位置から区分エントリ・ポイントに分岐するときは、命令を実行することをさらに含む請求項１４に記載の方法。
【請求項１６】
メモリ中の安全な区分へのアクセスを監視するステップであって、前記安全な区分の区分エントリ・ポイントへの、または前記安全な区分内の別の位置から前記安全な区分内の位置へのアクセス以外のアクセスがトラップされるアクセスを監視することと、
前記アクセスが許可された場合は、暗号化された命令を前記安全な区分からプロセッサに読み込むことと、
前記読み込んだ命令を暗号化解除することと、
前記暗号化解除した命令を実行することを含む命令処理方法。
【請求項１７】
暗号化解除した命令を実行することが、
命令が安全な区分からデータを読み取る命令であるかどうかを決定すること、および
命令が安全な区分からデータを読み取る命令である場合は、安全な区分からデータを読み取って、読み取ったデータを暗号化解除することを含む請求項１６に記載の方法。
【請求項１８】
暗号化解除した命令を実行することが、

命令が安全な区分中の位置にデータを書き込む命令であるかどうかを決定すること、および
命令が安全な区分中にデータを書き込む命令である場合は、データを暗号化して、安全な区分中の位置にデータを書き込むことを含む請求項１６に記載の方法。
【請求項１９】
命令が安全な区分からデータを読み取る命令であるかどうかの前記決定が、データの仮想アドレスを安全な区分の境界と比較することを含む請求項１７に記載の方法。
【請求項２０】
前記区分エントリ・ポイントが、前記安全なメモリ区分にアクセスする前記命令の信憑性を検証する検証ルーチンを備える請求項１に記載のプロセッサ。
【請求項２１】
前記安全な区分実施ロジックが、適切な読み取り／書き込み許可なしに前記安全なメモリ区分中のデータに操作することを試みるいかなる命令をもさらにトラップする請求項１に記載のプロセッサ。
【請求項２２】
前記安全な区分実施ロジックによってトラップされた命令を管理するトラップ・ハンドラをさらに備える請求項２１に記載のプロセッサ。
【請求項２３】
前記暗号ロジックが、前記安全なメモリ区分に記憶されるべき情報を暗号化し、前記安全なメモリ区分から読み出される情報を暗号化解除する請求項１に記載のプロセッサ。
【請求項２４】
前記暗号ロジックが、プロセッサ・キー・ストレージに記憶されているプロセッサ・キーを使用する請求項２３に記載のプロセッサ。
【請求項２５】
前記区分エントリ・ポイントが、前記区分にアクセスする前記命令の信憑性を検証する検証ルーチンの開始を備える請求項５に記載のコンピュータ・システム。
【請求項２６】
前記安全な区分実施ロジックが、適切な読み取り／書き込み許可なしに前記区分中のデータ上で動作することを試みるいかなる命令をもさらにトラップする請求項５に記載のコンピュータ・システム。
【請求項２７】
前記暗号ロジックが、前記区分に記憶されるべき情報を暗号化し、前記区分から読み出される情報を暗号化解除する請求項６に記載のコンピュータ・システム。
【請求項２８】
前記区分に記憶されるべき情報を暗号化するステップをさらに含む請求項１０に記載の方法。
【請求項２９】
前記区分から読み出される情報を暗号化解除するステップをさらに含む請求項１０に記載の方法。