(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4737592号
(P4737592)

(45)発行日　平成23年8月3日(2011.8.3)　(24)登録日　平成23年5月13日(2011.5.13)

(51)Int.Cl.　　F I
G06F 21/22 (2006.01)　　G06F 9/06 660L
G06F 9/38 (2006.01)　　G06F 9/38 330A
　　G06F 9/38 330F

請求項の数 3　(全 13 頁)

(21)出願番号　特願2005-38760(P2005-38760)
(22)出願日　平成17年2月16日(2005.2.16)
(65)公開番号　特開2006-227777(P2006-227777A)
(43)公開日　平成18年8月31日(2006.8.31)
審査請求日　平成20年2月13日(2008.2.13)

(73)特許権者　302062931
ルネサスエレクトロニクス株式会社
神奈川県川崎市中原区下沼部１７５３番地
(74)代理人　100089071
弁理士　玉村　静世
(72)発明者　平岡　徹
東京都小平市上水本町５丁目２２番１号　株式会社日立超エル・エス・アイ・システムズ内
(72)発明者　杉野　貴美広
東京都千代田区丸の内二丁目４番１号　株式会社ルネサステクノロジ内
(72)発明者　萩原　今朝巳
東京都千代田区丸の内二丁目４番１号　株式会社ルネサステクノロジ内
最終頁に続く

(54)【発明の名称】データ処理装置

(57)【特許請求の範囲】
【請求項１】
命令コードを実行可能な中央処理装置と、
暗号化された命令コードを保持可能な命令キャッシュと、
上記中央処理装置と上記命令キャッシュとの間に配置され、上記暗号化された命令コードを、上記命令キャッシュを介して取り込み、それを復号化して上記中央処理装置に供給するための命令コード復号化論理と、を含むデータ処理装置であって、
上記命令コード復号化論理は、上記暗号化された命令コードをパイプライン処理によって順次復号化し、
上記中央処理装置は、分岐先命令アドレスに対応して、分岐先命令コードの復号化後の命令を、上記分岐命令アドレスに関連付けて保持可能な信号変換バッファを含み、上記信号変換バッファ内に分岐先アドレスに対応する分岐先命令コードが存在する場合には、それを読み出して実行することを特徴とするデータ処理装置。
【請求項２】
上記命令キャッシュを介して上記命令コード復号化論理に取り込まれる命令コードは、コプロセッサによって暗号化されたものを含む請求項１記載のデータ処理装置。
【請求項３】
マイクロコンピュータとして一つの半導体基板に形成された請求項２記載のデータ処理装置。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、データ処理技術、特に顧客プログラムの保護強化を図るための技術に関する。
【背景技術】
【０００２】
ソフトウエア及びデータの保護に関する技術として、中央処理装置に暗号化・復号部及び鍵格納部を付加して、記憶装置に格納されている暗号化された機械語命令及びデータを復号部によって復号して中央処理装置で実行させ、また中央処理装置から記憶装置にデータを格納する時は暗号化部によってデータを暗号化して格納するようにした技術が知られている（例えば特許文献１参照）。
【０００３】
また、情報処理装置においてソフトウエア等の機密保護を図る際に、暗号強度と計算機のスループットがトレードオフにならないようにし、もって機密保護と高速処理とをともに実現できるようにすることを目的とした技術として、第２の記憶手段に格納されている暗号化された命令及びデータを復号して第１の記憶手段に格納してデータ処理手段で実行及び処理し、データ処理手段から第２の記憶手段にデータを出力する時は一旦第１の記憶手段に格納した後、暗号化手段で暗号化して第２の記憶手段に格納する技術が知られている（例えば特許文献２参照）。
【０００４】
【特許文献１】特開平２－１５５０３４号公報（図１）
【特許文献２】特開平９－２５９０４４号公報（図１）
【発明の開示】
【発明が解決しようとする課題】
【０００５】
従来はメモリ上の暗号化された命令コードを一旦復号化して命令キャッシュやユーザＲＡＭ（ランダム・アクセス・メモリ）に置いてから中央処理装置によって命令が処理されていた。この方式では、命令キャッシュやユーザＲＡＭには復号化された命令コードが存在するため、デバッグツールや悪意を持ったプログラムにより顧客プログラムの機密保護が守られないことがあり得る。そこで、命令キャッシュやユーザＲＡＭとＣＰＵの間で命令コードの復号化を実施することが必要となる。それについて本願発明者が検討したところ、中央処理装置で命令が処理される直前に復号化すると、復号化に要する処理時間が大きいため、命令の処理性能が大幅に劣化してしまうことが見いだされた。
【０００６】
本発明の目的は、顧客プログラムの保護の強化を図ることにある。
【０００７】
本発明の別の目的は、命令の処理性能を劣化させることなく、顧客プログラムの保護の強化を図るための技術を提供することにある。
【０００８】
本発明の前記並びにその他の目的と新規な特徴は本明細書の記述及び添付図面から明らかになるであろう。
【課題を解決するための手段】
【０００９】
本願において開示される発明のうち代表的なものの概要を簡単に説明すれば下記の通りである。
【００１０】
すなわち、命令コードを実行可能な中央処理装置と、暗号化された命令コードを保持可能な命令キャッシュと、上記中央処理装置と上記命令キャッシュとの間に配置され、上記暗号化された命令コードを、上記命令キャッシュを介して取り込み、それを復号化して上記中央処理装置に供給するための命令コード復号化論理と、を含んでデータ処理装置を構

成する。
【００１１】
上記の手段によれば、命令キャッシュと中央処理装置との間に命令コード復号化論理が設けられているため、命令キャッシュの内容は暗号化された命令コードとされ、復号化された命令コードが命令キャッシュに格納されることがない。このことが、顧客プログラムの保護の強化を達成する。
【００１２】
このとき、命令の逐次読み出し時や分岐命令発生時の命令実行処理においてオーバヘッドが生じないようにするには、上記命令コード復号化論理において、上記暗号化された命令コードをパイプライン処理によって復号化すると良い。
【００１３】
また、分岐命令発生時の分岐先命令コードの復号化処理によるオーバヘッドを隠蔽化するには、分岐先命令アドレスに対応して、分岐先命令コードの復号化後の命令を、上記分岐命令アドレスに関連付けて保持可能な信号変換バッファを上記中央処理装置内に設けると良い。
【００１４】
そして、命令コード復号化によるオーバヘッドと分岐命令発生時の分岐先命令読み出しに関するオーバヘッドとの双方の隠蔽化を可能とするには、命令フェッチアドレスをキーとして当該命令の分岐先アドレスを出力可能な動的分岐予測機構としての分岐先アドレスバッファを上記中央処理装置内に設け、上記分岐先アドレスバッファを介して投機的に命令フェッチを実行するようにすると良い。
【００１５】
さらに、上記構成のデータ処理装置は、マイクロコンピュータとして一つの半導体基板に形成することができる。
【発明の効果】
【００１６】
本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば下記の通りである。
【００１７】
すなわち、顧客プログラムの保護の強化を図るための技術を提供することができる。
【発明を実施するための最良の形態】
【００１８】
図１０には、本発明にかかるデータ処理装置の一例であるマイクロコンピュータが示される。
【００１９】
図１０に示されるデータ処理装置は、特に制限されないが、命令キャッシュ（ＩＮＳ－ＣＡＣＨＥ）１００、命令コード復号化論理（ＩＮＳ－ＤＥＣ）３００、中央処理装置（ＣＰＵ）１６００、及びメモリ（ＭＥＭ）１５００とを含み、公知の半導体集積回路製造技術により、例えば単結晶シリコン基板などの一つの半導体基板に形成される。暗号化された命令コードは、上記命令キャッシュ１００を介して上記命令コード復号化論理３００に伝達される。上記命令コード復号化論理３００は、暗号化された命令コードを上記ＣＰＵ１６００の直前で復号化してから上記ＣＰＵ１６００に供給する。上記ＣＰＵ１６００は、上記命令コード復号化論理３００によって復号化された命令を実行する。例えば、上記暗号化された命令コードは、上記ＣＰＵ１６００や図示しないコプロセッサで暗号化し、上記ＭＥＭ１５００に格納されていてもよいし、上記ＭＥＭ１５００に予め格納されていてもよいし、上記データ処理装置の外部から暗号化された命令コードが伝達されるものであってもよい。
【００２０】
図１には、上記ＣＰＵ１６００の詳細な構成例が示される。
【００２１】

図１に示されるようにＣＰＵ１６００は、命令キュー５００、命令デコーダ（ＤＥＣ）６００、オペランドアドレス加算器（ＯＰ－ＡＤＲ－ＡＤＤ）７００、オペランドキャッシュ（ＯＰ－ＣＡＣＨＥ）８００、オペランドデータ復号化論理（ＯＰ－ＤＥＣ）９００、命令実行部（ＩＮＳ－ＰＲＡ）１０００、オペランドデータ暗号化論理（ＯＰ－ＣＯＤ）１１００、命令アドレス加算器（ＩＮＳ－ＡＤＲ－ＡＤＤ）１２００、逐次命令フェッチアドレス生成論理（ＡＤＲ－ＣＲＥ）１３００、及びセレクタ９０－１，９０－２，９０－３を含んで成る。

【００２２】

上記命令キュー５００は、上記命令コード復号化論理３００から伝達された３２バイトの命令を格納する。上記セレクタ９０－１は、上記命令コード復号化論理３００の出力と、上記命令キュー５００の出力とを選択的に命令デコーダ６００に伝達する。命令デコーダ６００は、上記セレクタ９０－１を介して伝達された命令の解読を行う。オペランドアドレス加算器７００は命令のオペランドアドレスを生成する。オペランドキャッシュ８００は、上記オペランドアドレスによって生成される。オペランドデータ復号化論理９００は、上記オペランドキャッシュ８００から出力された暗号化データを復号化する。命令実行部１０００は、上記命令デコーダ６００でデコードされた命令を実行する。この命令実行部１０００での命令実行結果はセレクタ９０－３及びオペランドデータ暗号化論理１１００に伝達される。上記命令アドレス加算器１２００は分岐命令の分岐先アドレスを計算する。上記逐次命令フェッチアドレス生成論理１３００は逐次命令読み出し時のアドレスを計算する。セレクタ９０－２は、命令をフェッチするため、上記命令アドレス加算器１２００と上記逐次命令フェッチアドレス生成論理１３００の出力とを選択的に上記命令キャッシュ１００に伝達する。フェッチすべき命令が命令キャッシュ１００内に存在する場合には、当該命令が命令コード復号化論理３００に伝達される。しかし、フェッチすべき命令が命令キャッシュ１００内に存在しない場合には、対応する命令がメモリ１５００から読出される。このとき、当該命令は命令キャッシュ１００に記憶される。

【００２３】

図１において、Ｉ１，Ｉ２，Ｉ－ＤＣ～ＷＢ、及びＯ－ＤＣなどは命令の処理におけるパイプライン処理との対応を示している。Ｉ１，Ｉ２は命令キャッシュ参照ステージを示し、Ｉ－ＤＣは命令キャッシュ１００から読み出された命令コードの復号化ステージを示し、ＩＱは命令キューに滞留しているステージを示し、ＩＤは命令の解読ステージを示し、Ｅ１はレジスタリード及び分岐先命令アドレス加算、オペランドアドレス加算ステージを示し、Ｅ２，Ｅ３は演算実行ステージ又はオペランドキャッシュ参照ステージを示し、Ｏ－ＥＣはオペランドストアデータの暗号化ステージを示し、Ｏ－ＤＣはオペランドキャッシュ８００からのロードデータの復号化ステージを示し、ＷＢは命令実行結果の書き込み（ライトバック）を示す。Ｉ－ＤＣステージ、Ｏ－ＥＣステージ、及びＯ－ＤＣステージは通常数サイクル以上必要である。

【００２４】

一つの命令の命令長は２バイトで、一度の命令フェッチで命令キャッシュからフェッチする命令コードは４命令（８バイト）と仮定する。命令コードはメモリから読み出されるとバス２００を通して命令キャッシュ１００に格納される。逐次命令処理の場合、逐次命令フェッチアドレス生成論理１３００で生成されたアドレスにより命令キャッシュ１００を参照する。命令キャッシュ１００から読み出された命令コードは命令コード復号化論理３００に転送され復号化される。命令コード復号化論理３００によって復号化された命令コードは、命令キュー５００に格納され、また、命令デコーダ６００に転送されて命令の解読が行われる。命令デコーダ６００で解読された命令がロード型命令の場合、オペランドアドレス加算器７００によりオペランドアドレスが生成され、そのアドレスに基づいてオペランドキャッシュ８００が参照される。オペランドキャッシュ８００から読み出されたオペランドは、オペランドデータ復号化論理９００で復号化され、ＣＰＵ１６００内の図示されないレジスタに格納される。命令デコーダ６００で解読された命令がストア型命令の場合、図示されないレジスタから読み出されたデータは命令実行部１０００を経由し

、オペランドデータ暗号化論理１１００で暗号化された後に、上記メモリ１５００に書き込まれる。命令デコーダ６００で解読された命令が演算型命令の場合、命令実行部１０００で演算が行われ、その演算結果は、セレクタ９０－３を介して、図示されないレジスタに書き込まれる。

【００２５】

図２には、上記構成における命令処理タイミングが示される。

【００２６】

図２において命令１から命令４までの８バイトはサイクル１からサイクル２で命令キャッシュ１００から読み出される。読み出された８バイトの命令コードはサイクル３からサイクル８の間で復号化される。復号化された命令コードは命令キュー５００に転送するとともに、先頭の命令１は命令デコーダ６００に転送される。命令１はサイクル９で命令の解読が行われる。説明の便宜上、命令１乃至命令９及び命令１０乃至命令１７は演算型命令と仮定する。以降命令１はパイプライン処理され、サイクル１３で結果の書き込みが行われる。命令２は命令キュー５００から命令デコーダ６００に転送され、サイクル１０で命令の解読が行われる。同様に命令３はサイクル１１で命令の解読が行われ、命令４はサイクル１２で命令の解読が行われる。次に命令５から命令８までの８バイトはサイクル２からサイクル３で命令キャッシュ１００から読み出される。しかし、サイクル４では、命令コード復号化論理３００が未だ命令１から命令４の復号化処理を行っているため、命令５から命令８の復号化処理の開始はサイクル９まで待たされる。命令５から命令８の復号化処理はサイクル９に開始され、サイクル１４で完了する。復号化された命令コードは命令キュー５００に転送するとともに、命令５は命令デコーダ６００に転送される。従って命令５はサイクル１５で命令の解読が行われ、サイクル１９で結果の書き込みが行われる。このように命令４の終了（サイクル１６）と命令５の終了（サイクル１９）の間に２サイクルのオーバヘッド（処理の遅れ）が生じる。同様に命令８と命令９の間にも２サイクルのオーバヘッドが生じる。分岐命令はサイクル２２で命令の解読が行われ、サイクル２３で命令アドレス加算器１２００により分岐先命令アドレスが求まる。その分岐先命令アドレスにより、サイクル２４及びサイクル２５で命令キャッシュ１００を参照する。分岐先命令の命令コード（命令１０から命令１３）の復号化処理はサイクル２６に開始され、サイクル３１で完了する。分岐先命令である命令１０はサイクル３２で命令の解読が行われ、サイクル３６で結果の書き込みが行われる。

【００２７】

上記例によれば、以下の作用効果を得ることができる。

【００２８】

命令キャッシュ１００と命令キュー５００との間に命令コード復号化論理３００が配置されたことにより、命令キャッシュ１００の内容は暗号化された命令コードとなり、復号化された命令コードが命令キャッシュ１００に格納されることが無いため、顧客プログラムの保護を強化することができる。すなわち、デバッグ機構により命令キャッシュ１００の内容を表示したり、命令キャッシュ１００の中の命令コードを他の記憶装置に転送しても、その命令コードを解読することはできないため、顧客プログラムの保護が実現できる。

【００２９】

図３には、上記ＣＰＵ１６００の別の構成例が示される。

【００３０】

図３に示されるＣＰＵ１６００が図１に示されるのと大きく相違するのは、命令コード復号化論理３００において暗号化された命令コードの復号化がパイプライン処理によって行われる点、及び分岐先命令のアドレスに対応させてその分岐先の８命令分の暗号化された命令コードに対応する復号化後の命令コードを連想して保持するための復号変換バッファ（ＤＴＢ）４００が設けられている点である。

【００３１】

図３において、Ｉ１，Ｉ２は命令キャッシュ参照ステージを示し、Ｉ－ｄｃ１乃至Ｉ－

ｄｃ６は命令キャッシュ１００から読み出された命令コードの復号化ステージを示し、ＩＱは命令キューに滞留しているステージを示し、ＩＤは命令の解読ステージを示し、Ｅ１はレジスタリード及び分岐先命令アドレス加算、オペランドアドレス加算ステージを示し、Ｅ２，Ｅ３は演算実行ステージまたはオペランドキャッシュ参照ステージを示し、Ｏ－ｅｃ１乃至Ｏ－ｅｃ６はオペランドストアデータの暗号化ステージを示し、Ｏ－ｄｃ１乃至Ｏ－ｄｃ６はオペランドキャッシュ８００からのロードデータの復号化ステージを示し、ＷＢは命令実行結果の書き込み（ライトバック）を示す。Ｉ－ｄｃ１～Ｉ－ｄｃ６ステージＯ－ｅｃ１～Ｏ－ｅｃ６ステージ及びＯ－ｄｃ１～Ｏ－ｄｃ６ステージは通常数サイクル以上必要な復号化や暗号化の処理をパイプライン処理化したステージである。

【００３２】

命令キャッシュ１００から読み出された命令コードは、セレクタ９０－４を介して、命令コード復号化論理３００に転送され復号化される。命令コード復号化論理３００から出力される復号化された命令コードは命令キュー５００に格納されるとともに、命令デコーダ６００に転送されて命令の解読が行われる。また、分岐命令の分岐先の８命令については命令コード復号化論理３００で復号化された後に、対応する分岐先命令アドレスと対にして信号変換バッファ４００に格納される。命令デコーダ６００で解読された命令がロード型命令の場合、オペランドアドレス加算器７００によりオペランドアドレスが生成され、オペランドキャッシュ８００が参照される。オペランドキャッシュ８００から読み出されたオペランドはオペランドデータ復号化論理９００で復号化されてＣＰＵ１６００内の図示されないレジスタに格納される。命令デコーダ６００で解読された命令がストア型命令の場合、図示されないレジスタから読み出されたデータは命令実行部１０００を経由してオペランドデータ暗号化論理１１００で暗号化された後に、メモリ１５００に書き込まれる。命令デコーダ６００で解読された命令が演算型命令の場合、命令実行部１０００で演算が行われ、その演算結果は、図示されないレジスタに書き込まれる。

【００３３】

図４には、上記構成における命令処理タイミングが示される。

【００３４】

命令１から命令４までの８バイトはサイクル１からサイクル２で命令キャッシュ１００から読み出される。読み出された８バイトの命令コードはサイクル３からサイクル８の間で復号化される。復号化された命令コードはセレクタ９０－４７を介して命令キュー５００に転送される。尚、復号化された先頭の命令１は命令デコーダ６００に転送される。命令１はサイクル９で命令の解読が行われる。説明の便宜上、命令１乃至命令９及び命令１０乃至命令２１は演算型命令と仮定する。以降命令１はパイプライン処理され、サイクル１３で結果の書き込みが行われる。命令２は命令キュー５００から命令デコーダ６００に転送され、サイクル１０で命令の解読が行われる。同様に命令３はサイクル１１で命令の解読が行われ、命令４はサイクル１２で命令の解読が行われる。次に命令５から命令８までの８バイトはサイクル２からサイクル３で命令キャッシュ１００から読み出される。命令５から命令８の復号化処理はサイクル４に開始され、サイクル９で完了する。復号化された命令コードは命令キュー５００に転送される。従って命令５はサイクル１３で命令の解読が行われ、サイクル１７で結果の書き込みが行われる。以降、命令９まで同様に処理される。分岐命令はサイクル１８で命令の解読が行われ、サイクル１９で命令アドレス加算器１２００により分岐先命令アドレスが求まる。その分岐先命令アドレスにより、サイクル２０及びサイクル２１で命令キャッシュ１００を参照する。分岐先命令の命令コード（命令１０から命令１３）の復号化処理はサイクル２２で開始され、サイクル２７で完了する。一方、分岐先命令アドレスと「分岐先命令アドレス＋８」のアドレスは信号変換バッファ４００にも送られ、サイクル２０で信号変換バッファ４００内に当該分岐先アドレスに対応する復号化された分岐先命令コードが存在するか否か判定される。所望の分岐先命令コードが信号変換バッファ４００に存在する場合、サイクル２１で復号化された後の分岐先命令コードが信号変換バッファ４００から読み出される。読み出された命令コードはセレクタ９０－４を介して命令キュー５００に転送される。先頭の命令１０は命令デコ

ーダ６００に転送される。また、サイクル２１で信号変換バッファ４００内に、「分岐先命令アドレス＋８」に対応する、復号化された分岐先命令コードが存在するか否か判定される。所望の命令コードが符号化変換バッファ４００に存在する場合、サイクル２２で復号化された後の分岐先命令コードが信号変換バッファ４００から読み出される。読み出された命令コードは、セレクタ９０－４を介して命令キュー５００に転送される。分岐先命令である命令１０はサイクル２２で命令の解読が行われ、サイクル２６で結果の書き込みが行われる。このように分岐命令と命令１０の間には命令アドレス加算器１２００で分岐先アドレスを計算して、信号変換バッファ４００から分岐先命令コードを読み出すまでの３サイクルのオーバヘッドが生じる。尚、信号変換バッファ４００に分岐先命令の命令コードが存在しない場合は、サイクル２７で分岐先命令コードの復号化処理が完了するので、サイクル２８で命令１０の命令の解読を行うことができる。以降、命令１１から命令１７までは同様に命令が実行される。命令１０から命令１３までの命令コードはサイクル２１に命令キャッシュ１００から読み出され、命令１４から命令１７までの命令コードはサイクル２２で命令キャッシュ１００から読み出されるため、命令１８から命令２１までの命令コードはサイクル２３で読み出される。読み出された命令コードはサイクル２４から命令コード復号化処理され、サイクル２９で復号化処理が完了する。復号化された命令コード（命令１８から命令２１）は命令キュー５００に転送されるとともに、先頭の命令１８は命令デコーダ６００に転送される。命令１８はサイクル３０で命令の解読が行われ、サイクル３４で結果の書き込みが行われる。このような処理によれば、命令１０から命令２１の命令処理についてオーバヘッドが生じることはない。

【００３５】

上記の例によれば、命令キャッシュ１００と命令キューの間に命令コードの復号化論理３００を有することにより、命令キャッシュ１００の内容は暗号化された命令コードとなり、復号化された命令コードが命令キャッシュ１００に格納されることが無いため、顧客プログラムの保護を強化することができる。また、命令コード復号化論理３００での復号化がパイプライン処理されることにより、逐次命令読み出し時のオーバヘッドを隠蔽化することができる。さらに、信号変換バッファ４００を設けることにより、分岐先アドレスに対応して分岐先の命令コードの復号化後の命令を記憶するようにしているため、分岐命令発生時の復号化処理によるオーバヘッドを隠蔽化することが可能となる。

【００３６】

図５には、上記復号変換バッファ４００の構成例が示される。

【００３７】

図５に示される復号変換バッファ４００はタグ部とデータ部とを含む。特に制限されないが、ダイレクトマッピング方式が採用され、タグ部は７０４バイト構成とされ、データ部は２Ｋバイト構成とされる。尚、復号変換バッファ４００は、２－ｗａｙや４－ｗａｙのセットアソシアティブ方式であっても良いし、フルアソシアティブ方式であっても良い。

【００３８】

図６には、図５に示される復号変換バッファ４００において参照（Ｒｅａｄ）及び書き込み（Ｗｒｉｔｅ）についての動作が示される。

【００３９】

参照時は分岐先命令アドレスの［１０：３］の８ビットにより２５６カラムの中からタグ及びデータを読み出す。読み出されたタグには、復号変換バッファに登録されている命令コードに対応する命令アドレスの［３１：１１］とその内容が有効であることを示すバリッドビット［Ｖ］が含まれる。コンパレータ（Ｃｍｐ．）では、分岐先アドレスの［３１：１１］と読み出されたタグの［３１：１１］との比較が行われる。バリッドビットが論理値“１”で、かつ分岐先アドレスの［３１：１１］と読み出されたタグの［３１：１１］が一致した場合、復号変換バッファ４００に復号後の命令コードが存在するため、復号変換バッファ４００から読み出された命令コードが命令キュー５００及び命令デコーダ６００に転送される。復号変換バッファ４００に復号後の命令コードが存在しない場合は

、命令コード復号化論理３００で復号化された命令コードが命令キュー５００及び命令デコーダ６００に転送されるとともに、復号変換バッファ４００にも転送されて復号変換バッファ４００への書き込みが行われる。このとき、復号後の命令コードに対応する命令アドレスの［１０：３］の８ビットにより２５６カラムの中の一つのカラムに書き込まれる。そしてタグには命令アドレスの［３１：１１］が書き込まれるとともに、バリッドビットに論理値“１”が書き込まれる。また、復号後の命令コードも同じカラムに書き込まれる。

【００４０】

図７には、上記ＣＰＵ１６００の別の構成例が示される。

【００４１】

図７に示されるのが、図１に示されるのと大きく相違するのは、暗号化された命令コードの復号化がパイプライン処理によって行われる点、さらには、動的分岐予測機構などによる投機的命令フェッチ方式を併用し、命令フェッチアドレスをキーとして当該命令フェッチする命令コードの中に以前に分岐成功した分岐命令が存在するときにその分岐命令の分岐先アドレスを出力可能な分岐先アドレスバッファ（ＢＴＢ）１４００を備える点である。そして上記分岐先アドレスバッファ１４００が設けられたことに対応して、セレクタ９０－２は、上記命令アドレス加算器１２００の出力と、上記分岐先アドレスバッファ１４００の出力信号と、上記逐次命令フェッチアドレス生成論理１３００の出力とを選択的に上記命令キャッシュ１００及び上記分岐先アドレスバッファ１４００に伝達可能に構成される。

【００４２】

図７において、Ｉ１，Ｉ２，Ｉ－ｄｃ１などは命令の処理におけるパイプライン処理との対応を示している。Ｉ１，Ｉ２は命令キャッシュ参照ステージを示し、Ｉ－ｄｃ１乃至Ｉ－ｄｃ６は命令キャッシュ１００から読み出された命令コードの復号化ステージを示し、ＩＱは命令キューに滞留しているステージを示し、ＩＤは命令の解読ステージを示し、Ｅ１はレジスタリード及び分岐先命令アドレス加算、オペランドアドレス加算ステージを示し、Ｅ２，Ｅ３は演算実行ステージまたはオペランドキャッシュ参照ステージを示し、Ｏ－ｅｃ１乃至Ｏ－ｅｃ６はオペランドストアデータの暗号化ステージを示し、Ｏ－ｄｃ１乃至Ｏ－ｄｃ６はオペランドキャッシュ８００からのロードデータの復号化ステージを示し、ＷＢは命令実行結果の書き込み（ライトバック）を示す。Ｉ－ｄｃ１～Ｉ－ｄｃ６ステージＯ－ｅｃ１～Ｏ－ｅｃ６ステージ及びＯ－ｄｃ１～Ｏ－ｄｃ６ステージは通常数サイクル以上必要な復号化や暗号化の処理をパイプライン処理化したステージである。

【００４３】

ここで、図３に示される構成によれば、図８に示されるように、命令の逐次読み出し時及び分岐命令発生時での命令コードの復号化処理オーバヘッドは隠蔽化されるものの、分岐命令発生時の分岐先命令読み出しに関するオーバヘッドは矢印で示されるように隠蔽化されない。これに対して図７に示される構成によれば、以下に詳述するように、命令コードの復号化によるオーバヘッドと、分岐命令発生時の分岐先命令読み出しに関するオーバヘッドとの両方を隠蔽化することができる。

【００４４】

図９には、図７に示される構成における命令処理タイミングが示される。

【００４５】

命令１と分岐命令１はサイクル１及びサイクル２で命令キャッシュ１００から読み出される。同時にサイクル１では分岐先アドレスバッファ１４００が参照され、サイクル２では分岐命令１の分岐先アドレス（すなわち命令２の命令アドレス）が分岐先アドレスバッファ１４００から出力される。サイクル３及びサイクル４では分岐先アドレスバッファ１４００から出力された分岐命令１の分岐先アドレスにより命令２及び分岐命令２を命令キャッシュ１００から読み出すとともに分岐先アドレスバッファ１４００を参照し、サイクル４では分岐命令２の分岐先アドレス（すなわち命令３の命令アドレス）が分岐先アドレスバッファ１４００から出力される。サイクル５及びサイクル６では分岐先アドレスバッ

ファ１４００から出力された分岐命令２の分岐先アドレスにより命令３及び分岐命令３が命令キャッシュ１００から読み出されて分岐先アドレスバッファ１４００が参照され、サイクル６では分岐命令３の分岐先アドレス（すなわち命令４の命令アドレス）が分岐先アドレスバッファ１４００から出力される。サイクル７及びサイクル８では分岐先アドレスバッファ１４００から出力された分岐命令３の分岐先アドレスにより命令４から命令７までが命令キャッシュ１００から読み出される。一方、命令１及び分岐命令１はサイクル３からサイクル８の間で復号化され、命令１はサイクル９に命令の解読が行われ、分岐命令１はサイクル１０で解読される。命令２及び分岐命令２はサイクル４で命令キャッシュ１００から読み出されているため、サイクル５からサイクル１０の間で復号化され、命令２はサイクル１１で命令の解読が行われ、分岐命令２はサイクル１２で命令が解読される。命令３及び分岐命令３はサイクル６で命令キャッシュ１００から読み出されているため、サイクル７からサイクル１２の間で復号化され、命令３はサイクル１３で命令の解読が行われ、分岐命令３はサイクル１４で解読される。命令４から命令７はサイクル８で命令キャッシュ１００から読み出されているため、サイクル９からサイクル１４の間で復号化され、命令４はサイクル１５で解読され、命令５はサイクル１６で解読され、命令６はサイクル１７で解読され、命令７はサイクル１８で解読される。このように分岐先アドレスバッファ１４００などの動的分岐予測機構によって投機的に命令フェッチを実行することにより、命令コードの復号化によるオーバヘッドと、分岐命令発生時の分岐先命令読み出しに関するオーバヘッドとの両方を隠蔽化することができる。

【００４６】

以上本発明者によってなされた発明を具体的に説明したが、本発明はそれに限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【００４７】

例えば、命令キャッシュ１００、命令コード復号化論理３００、及びＣＰＵ１６００をそれぞれ別個の半導体チップにより形成することができる。

【００４８】

以上の説明では主として本発明者によってなされた発明をその背景となった利用分野であるマイクロコンピュータに適用した場合について説明したが、本発明はそれに限定されるものではなく、各種データ処理装置に広く適用することができる。

【００４９】

本発明は、ＣＰＵ（中央処理装置）を含むことを条件に適用することができる。

【図面の簡単な説明】

【００５０】

【図１】本発明にかかるデータ処理装置の一例であるマイクロコンピュータにおけるＣＰＵの構成例ブロック図である。

【図２】図１に示される構成の動作タイミング図である。

【図３】上記マイクロコンピュータにおけるＣＰＵの別の構成例ブロック図である。

【図４】図３に示される構成の動作タイミング図である。

【図５】図３における主要部の構成例説明図である。

【図６】図３における主要部の別の構成例説明図である。

【図７】上記マイクロコンピュータにおけるＣＰＵの別の構成例ブロック図である。

【図８】図７に示される構成の比較対象とされる構成の動作タイミング図である。

【図９】図７に示される構成の動作タイミング図である。

【図１０】上記マイクロコンピュータの全体的な構成例ブロック図である。

【符号の説明】

【００５１】

９０－１～９０－３　セレクタ

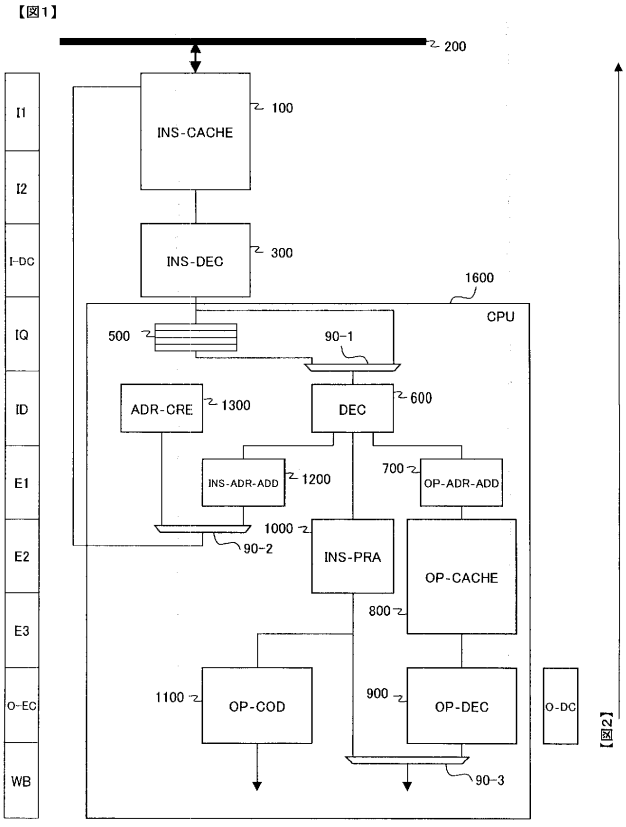
１００　命令キャッシュ

２００　バス

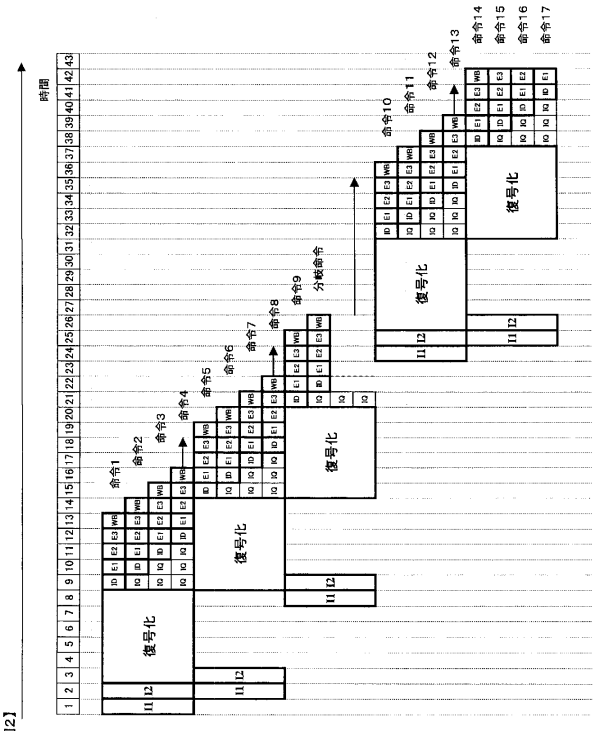
３００　命令コード復号化論理

５００　命令キュー
６００　命令デコーダ
７００　オペランドアドレス加算器
８００　オペランドキャッシュ
９００　オペランドデータ復号化論理
１０００　命令実行部
１１００　オペランドデータ暗号化論理
１２００　命令アドレス加算器
１３００　逐次命令フェッチアドレス生成論理
１４００　分岐先アドレスバッファ
１５００　メモリ
１６００　ＣＰＵ

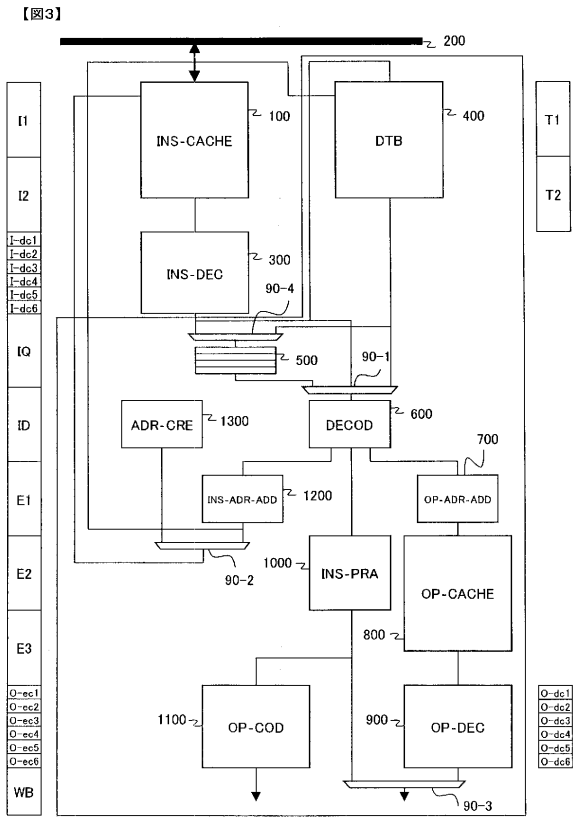
【図１】



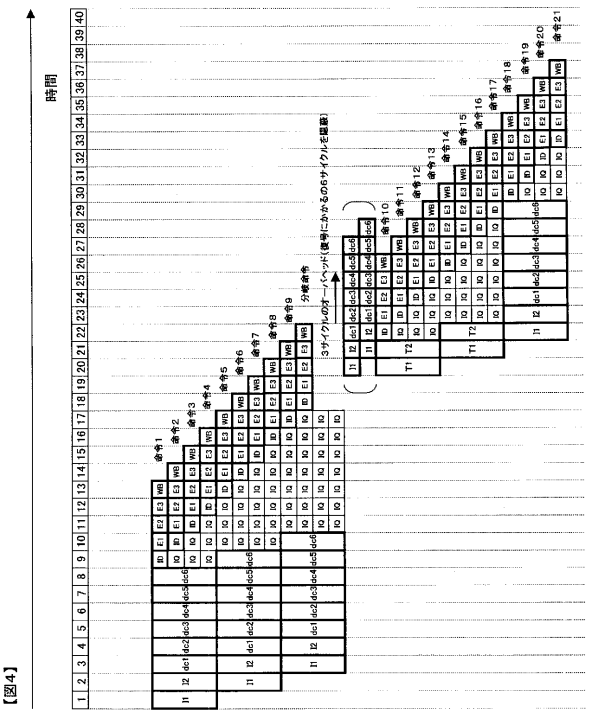
【図２】



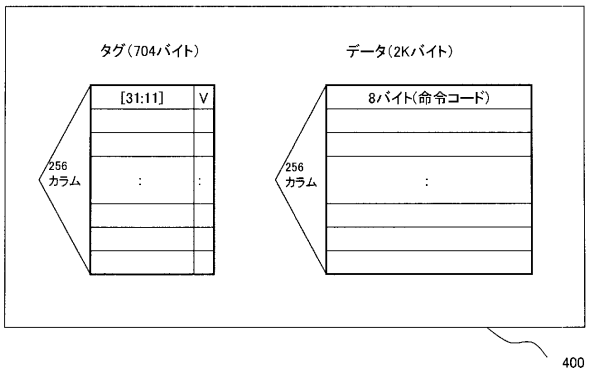
【図３】


【図3】
200
I1
I2
I-dc1
I-dc2
I-dc3
I-dc4
I-dc5
I-dc6
IQ
ID
E1
E2
E3
O-ec1
O-ec2
O-ec3
O-ec4
O-ec5
O-ec6
WB
INS-CACHE
100
DTB
400
T1
T2
INS-DEC
300
90-4
500
90-1
ADR-CRE
1300
DECOD
600
700
INS-ADR-ADD
1200
OP-ADR-ADD
90-2
1000
INS-PRA
OP-CACHE
800
1100
OP-COD
900
OP-DEC
O-dc1
O-dc2
O-dc3
O-dc4
O-dc5
O-dc6
90-3

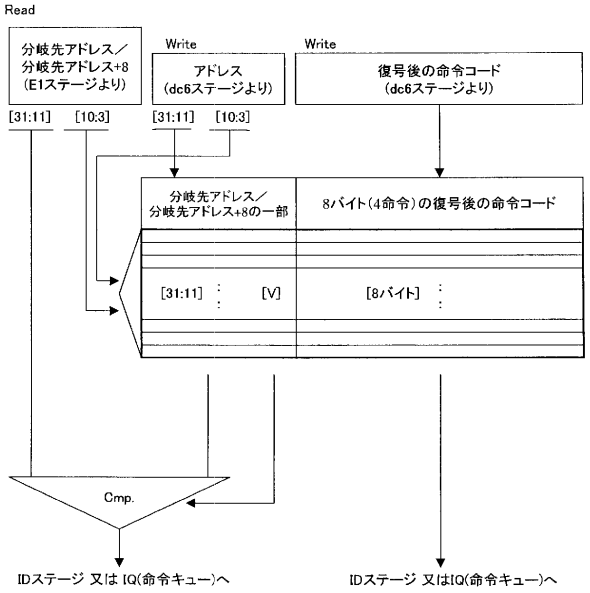
【図４】


【図4】
時間
分岐命令
3サイクルのオーバヘッド(後半にかかるのも1サイクル)を確認!

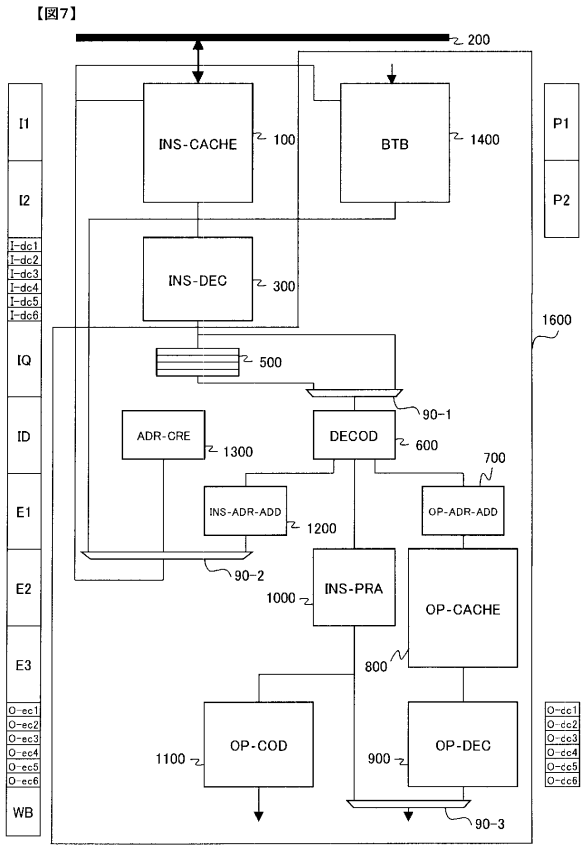
【図５】


【図5】
タグ(704バイト)
データ(2Kバイト)
[31:11]
V
256
カラム
8バイト(命令コード)
400

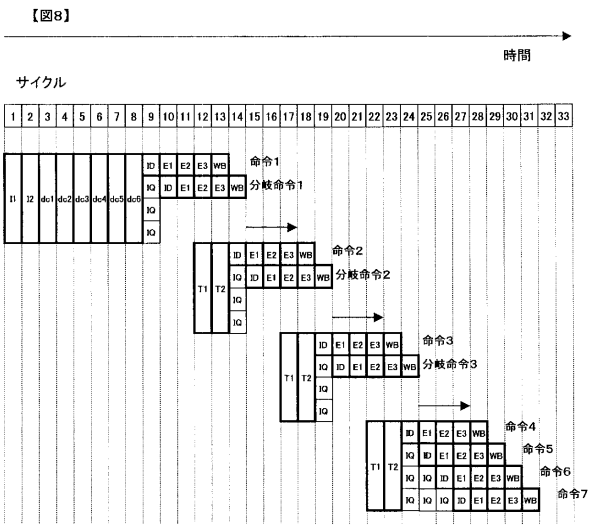
【図６】


【図6】
Read
分岐先アドレス／
分岐先アドレス+8
(E1ステージより)
Write
アドレス
(dc6ステージより)
Write
復号後の命令コード
(dc6ステージより)
[31:11]
[10:3]
[31:11]
[10:3]
分岐先アドレス／
分岐先アドレス+8の一部
8バイト(4命令)の復号後の命令コード
[31:11]
[V]
[8バイト]
Cmp.
IDステージ 又は IQ(命令キュー)へ
IDステージ 又はIQ(命令キュー)へ

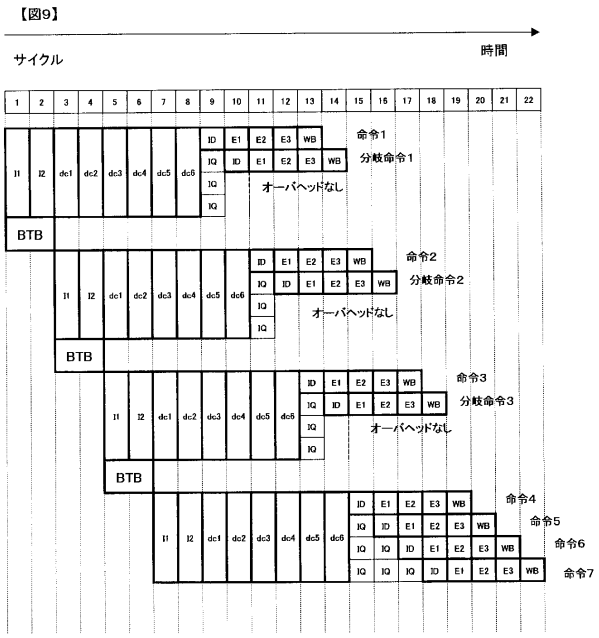
【図７】


【図7】
200
I1
I2
I-dc1
I-dc2
I-dc3
I-dc4
I-dc5
I-dc6
IQ
ID
E1
E2
E3
O-ec1
O-ec2
O-ec3
O-ec4
O-ec5
O-ec6
WB
INS-CACHE
100
BTB
1400
P1
P2
INS-DEC
300
1600
500
90-1
ADR-CRE
1300
DECOD
600
700
INS-ADR-ADD
1200
OP-ADR-ADD
90-2
1000
INS-PRA
OP-CACHE
800
O-dc1
O-dc2
O-dc3
O-dc4
O-dc5
O-dc6
1100
OP-COD
900
OP-DEC
90-3

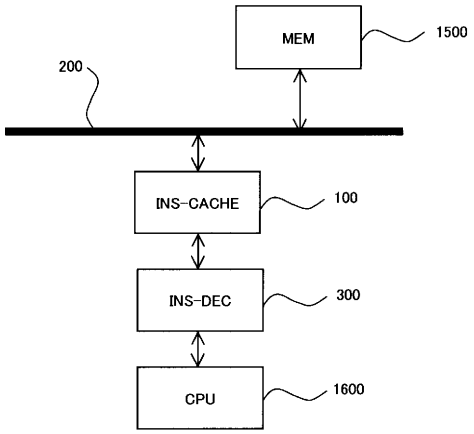
【図８】


【図8】
時間
サイクル
命令1
分岐命令1
命令2
分岐命令2
命令3
分岐命令3
命令4
命令5
命令6
命令7

【図９】


【図9】
時間
サイクル
命令1
分岐命令1
オーバヘッドなし
BTB
命令2
分岐命令2
オーバヘッドなし
BTB
命令3
分岐命令3
オーバヘッドなし
BTB
命令4
命令5
命令6
命令7

【図１０】


【図10】
MEM
1500
200
INS-CACHE
100
INS-DEC
300
CPU
1600

フロントページの続き

(72)発明者　小林　浩二
東京都小平市上水本町５丁目２２番１号　株式会社日立超エル・エス・アイ・システムズ内

審査官　後藤　彰

(56)参考文献　特開２００５－０１８４３４（ＪＰ，Ａ）
特開２００４－２４６６３７（ＪＰ，Ａ）
特開２００３－１０８４４２（ＪＰ，Ａ）
特開２００１－１４２７０４（ＪＰ，Ａ）
特開平０４－０９００２７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２２
Ｇ０６Ｆ　９／３８