(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-503191
(P2017-503191A)
(43)公表日　平成29年1月26日(2017.1.26)

(51)Int.Cl.		F I			テーマコード（参考）
G09C 1/00	(2006.01)	G09C	1/00	660D	5J104
G06F 21/60	(2013.01)	G06F	21/60	320	
H04L 9/14	(2006.01)	H04L	9/00	641	

審査請求 有　予備審査請求 未請求　（全 30 頁）

(21)出願番号　特願2016-535156 (P2016-535156)
(86)(22)出願日　平成27年1月14日 (2015.1.14)
(85)翻訳文提出日　平成28年6月30日 (2016.6.30)
(86)国際出願番号　PCT/US2015/011341
(87)国際公開番号　WO2015/108931
(87)国際公開日　平成27年7月23日 (2015.7.23)
(31)優先権主張番号　61/927,914
(32)優先日　平成26年1月15日 (2014.1.15)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　14/596,113
(32)優先日　平成27年1月13日 (2015.1.13)
(33)優先権主張国　米国 (US)

(71)出願人　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５４　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　チェリトン、ダイヴィッド、アール.
アメリカ合衆国　９５０５４　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００　インテル・コーポレーション内

Fターム(参考)　5J104 AA12　AA16　NA02　NA37

最終頁に続く

(54)【発明の名称】重複排除に基づくデータセキュリティ

(57)【要約】
データセキュリティを実現することは、ストレージにデータコンテンツを書き込むよう求める要求に応じて、データコンテンツに基づいて暗号化データコンテンツを生成することと、ストレージにおける暗号化データコンテンツに対する参照を取得するよう試みることと、暗号化データコンテンツに対する参照を取得した場合、ストレージにおける暗号化データコンテンツに対する参照を参照するようにトランスレーションラインを修正することと、暗号化データコンテンツに対する参照を取得しなかった場合には、暗号化データコンテンツを新しいロケーションに格納することと、新しいロケーションに格納されている暗号化データコンテンツに対する参照を取得することと、新しいロケーションに格納されている暗号化データコンテンツに対する参照を参照するようトランスレーションラインを修正することとを含む。

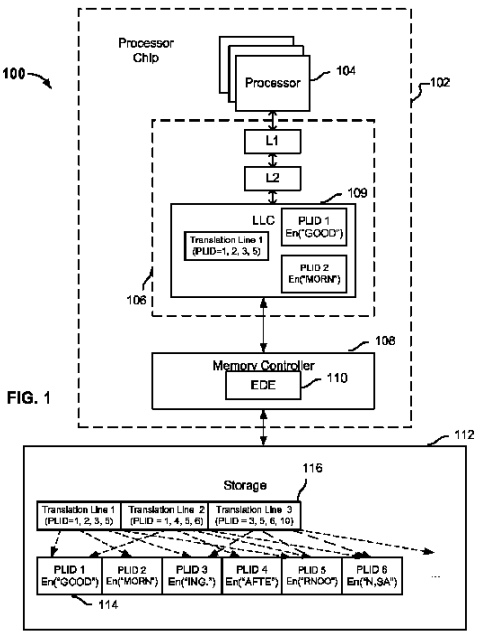


FIG. 1

【特許請求の範囲】
【請求項１】
ストレージと、
前記ストレージに結合されているメモリコントローラと
を備え、
前記メモリコントローラは、
前記ストレージにデータコンテンツを書き込むよう求める要求に応じて、前記データコンテンツに少なくとも部分的に基づいて暗号化データコンテンツを生成し、
前記ストレージにおける前記暗号化データコンテンツに対する参照を取得するよう試み、
前記暗号化データコンテンツに対する前記参照を取得した場合、前記ストレージにおける前記暗号化データコンテンツに対する前記参照を参照するようにトランスレーションラインを修正し、
前記暗号化データコンテンツに対する前記参照を取得しなかった場合には、
前記暗号化データコンテンツを新しいロケーションに格納し、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する参照を取得し、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する前記参照を参照するよう前記トランスレーションラインを修正する
セキュアシステム。
【請求項２】
前記ストレージは、メインメモリ、セカンダリストレージまたは両方を有する
請求項１に記載のシステム。
【請求項３】
前記メモリコントローラは、確定的暗号化関数を実行して前記暗号化データコンテンツを生成する
請求項１に記載のシステム。
【請求項４】
前記メモリコントローラは、アドバンスド・エンクリプション・スタンダード（ＡＥＳ）、ＥＣＢ－Ｍｉｘ－ＥＣＢ（ＥＭＥ）、ＸＥＸ－ＴＣＢ－ＣＴＳ（ＸＴＳ）およびＣＢＣ－Ｍａｓｋ－ＣＢＣ（ＣＭＣ）のうち１または複数を実施する
請求項１に記載のシステム。
【請求項５】
前記メモリコントローラに結合されているキャッシュをさらに備え、
前記キャッシュは暗号化されていないデータを格納する
請求項１に記載のシステム。
【請求項６】
前記メモリコントローラに結合されているキャッシュをさらに備え、
前記キャッシュは重複排除されたデータを格納する
請求項１に記載のシステム。
【請求項７】
前記メモリコントローラに結合されているキャッシュをさらに備え、
前記メモリコントローラはさらに、キャッシュミスの場合にセキュアパッドを生成して、前記セキュアパッドを用いて前記ストレージからフェッチされる暗号化データを復号化する
請求項１に記載のシステム。
【請求項８】
前記メモリコントローラに結合されているキャッシュをさらに備え、
前記メモリコントローラはさらに、
読み出しロケーションにあるデータコンテンツへアクセスするよう要求に応じて、前記

読み出しロケーションに対応するトランスレーションラインおよびデータラインが前記キャッシュにおいて利用可能であるか否かを判断し、
前記データラインが前記キャッシュにおいて利用可能でない場合、
前記データラインを前記ストレージからロードし、
前記データラインを復号化して、
前記復号化の結果を前記キャッシュに保存する
請求項１に記載のシステム。
【請求項９】
前記メモリコントローラに結合されているキャッシュをさらに備え、
前記データコンテンツを書き込むよう求める要求は、前記データコンテンツを格納しているキャッシュラインをエビクションするよう求める要求によって発生し、前記キャッシュラインは、最後にストレージに書き込まれた後修正されている
請求項１に記載のシステム。
【請求項１０】
前記データコンテンツを書き込むよう求める要求を生成するプロセッサをさらに備え、
前記プロセッサのアドレス空間は、複数の重複排除ドメインを含み、
各重複排除ドメインは、前記各重複排除ドメインにおけるデータコンテンツを暗号化するために用いられる対応する鍵を持つ
請求項１に記載のシステム。
【請求項１１】
前記トランスレーションラインは暗号化されている
請求項１に記載のシステム。
【請求項１２】
前記トランスレーションラインは暗号化されており、
前記データコンテンツおよび前記トランスレーションラインは複数の異なる鍵を用いて暗号化されている
請求項１に記載のシステム。
【請求項１３】
前記ストレージにおける前記暗号化データコンテンツに対する前記参照を取得するよう試みることは、コンテンツディレクトリにおいて前記暗号化データコンテンツを検索することを含む
請求項１に記載のシステム。
【請求項１４】
前記ストレージにおける前記暗号化データコンテンツに対する前記参照を取得するよう試みることは、コンテンツディレクトリにおいて前記暗号化データコンテンツを検索することを含み、
前記コンテンツディレクトリは暗号化メタデータを含む
請求項１に記載のシステム。
【請求項１５】
前記暗号化メタデータは、前記コンテンツディレクトリを共有している複数の保護ドメインの間で共有されている共通鍵を用いて暗号化される
請求項１４に記載のシステム。
【請求項１６】
書き込み処理の完了指示は、前記書き込み処理を実行するために用いられる指定所要時間を変更するよう修正される
請求項１に記載のシステム。
【請求項１７】
データラインへの読み出しアクセスの場合、前記メモリコントローラはさらにインテグリティチェックを実行し、前記インテグリティチェックは、前記データラインの前記データコンテンツが前記データラインに対応付けられているメタデータに一致するか否かを判

断することを含む
請求項１に記載のシステム。
【請求項１８】
前記データラインの前記データコンテンツが前記データラインに対応付けられている前記メタデータに一致しない場合、セキュリティ侵害の可能性が報告される
請求項１７に記載のシステム。
【請求項１９】
前記データラインに対応付けられている前記メタデータは、セキュアな鍵付きハッシュ関数を用いて生成される
請求項１７に記載のシステム。
【請求項２０】
前記ストレージは、レイテンシが異なる複数のメモリを含むハイブリッドメモリを有する
請求項１に記載のシステム。
【請求項２１】
前記ストレージは、レイテンシが異なる複数のメモリを含むハイブリッドメモリを有し、
低レイテンシメモリの暗号化の単位は、高レイテンシメモリの暗号化の単位とはサイズが異なる
請求項１に記載のシステム。
【請求項２２】
前記ストレージは、同じデータコンテンツを持つ複数のデータラインの暗号化の結果が異なるオーバーフローエリアを含む
請求項１に記載の方法。
【請求項２３】
ストレージにデータコンテンツを書き込むよう求める要求に応じて、前記データコンテンツに基づいて暗号化データコンテンツを生成する段階と、
前記ストレージにおける前記暗号化データコンテンツに対する参照を取得するよう試みる段階と、
前記暗号化データコンテンツに対する前記参照を取得した場合、前記ストレージにおける前記暗号化データコンテンツに対する前記参照を参照するようにトランスレーションラインを修正する段階と、
前記暗号化データコンテンツに対する前記参照を取得しなかった場合には、
前記暗号化データコンテンツを新しいロケーションに格納する段階と、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する参照を取得する段階と、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する前記参照を参照するよう前記トランスレーションラインを修正する段階と
を備える方法。
【請求項２４】
データセキュリティを実現するためのコンピュータプログラム製品であって、前記コンピュータプログラム製品は、有形のコンピュータ可読記憶媒体で具現化され、複数のコンピュータ命令を含み、
前記複数のコンピュータ命令は、
ストレージにデータコンテンツを書き込むよう求める要求に応じて、前記データコンテンツに基づいて暗号化データコンテンツを生成し、
前記ストレージにおける前記暗号化データコンテンツに対する参照を取得するよう試み、
前記暗号化データコンテンツに対する前記参照を取得した場合、前記ストレージにおける前記暗号化データコンテンツに対する前記参照を参照するようにトランスレーションラ

インを修正し、
前記暗号化データコンテンツに対する前記参照を取得しなかった場合には、
前記暗号化データコンテンツを新しいロケーションに格納し、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する参照を取得し、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する前記参照を参照するよう前記トランスレーションラインを修正する
ためのコンピュータ命令である
コンピュータプログラム製品。

【発明の詳細な説明】

【技術分野】

【０００１】

＜他の出願に対する相互参照＞本願は、米国仮特許出願第６１／９２７，９１４号（発明の名称：ＤＥＤＵＰＬＩＣＡＴＩＯＮ－ＢＡＳＥＤ　ＭＥＭＯＲＹ　ＥＮＣＲＹＰＴＩＯＮ、出願日：２０１４年１月１５日）に基づき優先権を主張する。当該仮出願は全て、参照により本願に組み込まれる。

【背景技術】

【０００２】

セキュアなコンピュータシステムは、コンピュータのメインメモリへのアクセスを求める侵入者による攻撃を阻止するべく、セキュアなメモリを必要とする。例えば、いわゆるコールドブート攻撃では、攻撃者は、メインメモリのダイナミックランダムアクセスメモリ（ＤＲＡＭ）からデータコンテンツを抽出することが可能であるが、この際メモリのコンテンツが失われない。このため、メモリ内に平文の極秘情報が格納されていれば、セキュリティが侵害されてしまう。デュアルポートＤＲＡＭは、システム動作中に攻撃者がＤＲＡＭにおける読み書きトラフィックを観察可能となり得ることを意味する。不揮発性ランダムアクセスメモリ（ＮＶＲＡＭ）を利用してメインメモリを実現するということは、データがメインメモリ内に保存され、コールドブート攻撃よりも必要な労力が少なくて済む攻撃に対しても脆弱であることを意味する。

【０００３】

現在、従来のストリーム暗号化は、セキュアメモリの暗号化には適さないと考えられている。これは、従来のストリーム暗号化技術は、同じデータの２つのインスタンスが同じ暗号文に暗号化されないように疑似乱数値で暗号化をシードすることを要件とするためである。この条件がなければ、同じ暗号文の発生回数を観察することで、攻撃者は頻度分析攻撃を実行することができる。このシードまたは初期化ベクトル（ＩＶ）を格納するオーバーヘッド、および、このＩＶを利用するために暗号化または復号化を設定するためのオーバーヘッドは通常、暗号化の単位として比較的大量のデータを必要とする。例えば、１６バイトのＩＶを利用することは、４キロバイトという従来のページサイズの粒度で暗号化を行えば、ＩＶについての空間オーバーヘッドが０．１パーセントに過ぎないことを意味する。しかしながら、プロセッサキャッシュとメインメモリとの間で要件とされるように、暗号化の単位が１つのキャッシュラインである場合、暗号化または復号化の処理毎に取得および設定に多大なコストがかかると思われる。例えば、従来のキャッシュラインサイズは６４バイトであるので、１６バイトのＩＶの空間オーバーヘッドは２５パーセントとなる。

【０００４】

セキュアデータのインテグリティのためにも、同様の理由から大きな単位とする必要がある。従来の方法では特に、データ単位毎に１２８ビットのメッセージ認証コード（ＭＡＣ）が必要となる。このように、ページのような大きな単位を利用すると、このＭＡＣのオーバーヘッドが消却されるが、キャッシュラインという単位では、上述したＩＶオーバーヘッドに加えて大きなオーバーヘッドが発生する。

【０００５】

コンピュータ用の標準的なセキュリティ／脅威モデルにおいて、プロセッサチップ自体はセキュアに形成されており、攻撃者はこのシリコンを修正できないよう、そして、プロセッサチップ内に存在する保護されたデータへのアクセスができないよう制限されていると仮定される。（例えば、プロセッサチップは、チップを修正しようとする試みまたはサポートされていない動作を実行しようとする試みが発見されると、コンテンツを破壊または削除するよう設計され得る。）特に、Ｌ１、Ｌ２等、最終レベルキャッシュまでのキャッシュに格納されているデータは、公開または侵害の危険性を心配することなく平文で格納することができ、プロセッサは、演算毎にデータを復号化することなくデータに対して演算を行うことができ、結果が生成されると直後に再度暗号化することができる。さらに、プロセッサチップのキャッシュに存在する他のメタデータも同様に、このチップの物理的なセキュリティおよびセキュアな設計によって、保護することができる。しかしながら、このようなデータの量は、プロセッサチップに対する物理的制約、例えば、電力およびコスト上の制限から大幅に制限され、メインメモリで利用可能な量に比べるとその一部に過ぎない。例えば、現時点において、オンチップキャッシュの状態は数十メガバイトに限定されるのが普通だが、メインメモリは容易に数十ギガバイト、または、それ以上となり、１０００倍も大きくなり得る。一方で、プロセッサチップ外に格納されるデータは、上述したように、例えば、ＤＲＡＭ自体を取り外すことによって、または、ＤＲＡＭに対して第２のポートに結合することによって、攻撃者がアクセス可能であると仮定される。

【０００６】

このため、メモリライン単位を高効率で暗号化および復号化しつつ、データの機密性およびインテグリティを強化する必要性がある。

【図面の簡単な説明】

【０００７】

本発明のさまざまな実施形態を以下の詳細な説明および添付図面において開示する。

【０００８】

【図１】重複排除した暗号化データコンテンツをサポートするシステムの実施形態を示すブロック図である。

【０００９】

【図２Ａ】複数の重複排除ドメインの実施形態を示すデータ構造図である。

【図２Ｂ】複数の重複排除ドメインの実施形態を示すデータ構造図である。

【００１０】

【図３】データをストレージに書き込むためのプロセスの実施形態を示すフローチャートである。

【００１１】

【図４】ストレージ内のロケーションからデータを読み出すためのプロセスの実施形態を示すフローチャートである。

【００１２】

【図５】データラインをキャッシュからエビクションするためのプロセスの実施形態を示すフローチャートである。

【００１３】

【図６】初期化ベクトル（ＩＶ）を含むデータ構造の例を示す図である。

【００１４】

【図７Ａ】従来の実施例における構造化メモリをサポートするために用いられるメタデータの例を示すデータ構造図である。

【００１５】

【図７Ｂ】セキュアな実施例における構造化メモリをサポートするために用いられるメタデータの例を示すデータ構造図である。

【発明を実施するための形態】

【００１６】

本発明は、数多くの方法で実施可能である。例えば、プロセス、装置、システム、組成

物、コンピュータ可読記憶媒体で具現化されるコンピュータプログラム製品、および／または、プロセッサに結合されているメモリに格納されている命令および／または当該メモリが提供する命令を実行するよう構成されているプロセッサ等のプロセッサとして実現される。本明細書において、これらの実施例または本発明を実施し得る任意のその他の形態は、「技術」と呼ぶ場合がある。概して、開示したプロセスのステップの順序は、本発明の範囲内で変更するとしてよい。特に明記されていない限り、あるタスクを実行するよう構成されていると説明されているプロセッサまたはメモリ等のコンポーネントは、所与のタイミングにおいて当該タスクを実行するよう一時的に構成される汎用コンポーネントとして、または、当該タスクを実行するよう製造されている特別なコンポーネントとして、実現されるとしてよい。本明細書で用いる場合、「プロセッサ」という用語は、コンピュータプログラム命令等のデータを処理するよう構成されている１または複数のデバイス、回路および／または処理コアを意味する。

【００１７】

本発明の原理を図示している添付図面と共に、本発明の１または複数の実施形態の詳細な説明を以下に記載する。本発明は、下記のような実施形態に関連付けて説明するが、本発明はどの実施形態にも限定されない。本発明の範囲は、請求項によってのみ限定されるものであり、本発明は数多くの代替例、変形例および均等例を含む。以下の説明では、本発明を完全に理解していただくべく、数多く具体的且つ詳細な内容を記載する。このような詳細な内容は、例示を目的として記載しているものであり、本発明は後述する具体的且つ詳細な内容のうち一部または全てを採用することなく請求項にしたがって実施され得る。説明を分かり易くするべく、本発明の関連技術分野で公知の技術的内容については、詳細な説明を省略しており、本発明が不要にあいまいにならないようにしている。

【００１８】

重複排除ストレージの暗号化および復号化を利用したコンピュータセキュリティを開示する。一部の実施形態において、データコンテンツをストレージに書き込むよう求める要求に応じて、当該データコンテンツに基づく暗号化データコンテンツを生成する。ストレージ内の暗号化データコンテンツに対する参照を取得するよう試みる。暗号化データコンテンツに対する参照を取得した場合、ストレージ内の暗号化データコンテンツに対する参照を参照するようにトランスレーションラインを修正する。暗号化データコンテンツに対する参照を取得しなかった場合、暗号化データコンテンツは新しいロケーションに格納される。新しいロケーションに格納された暗号化データコンテンツに対する参照を取得する。新しいロケーションに格納されている暗号化データコンテンツに対する参照を参照するようトランスレーションラインを修正する。

【００１９】

図１は、重複排除した暗号化データコンテンツをサポートするシステムの実施形態を示すブロック図である。本例において、システム１００では、プロセッサチップ１０２がストレージ１１２に接続されている。プロセッサチップ１０２は、階層キャッシュ１０６に接続されている１または複数のプロセッサコア１０４等、多くの回路素子を有する。本例では３レベルから成るキャッシュ階層を図示しているが、キャッシュレベルが異なる他のキャッシュ階層を利用するとしてもよい。キャッシュ内では、データおよびコードは暗号化されていない平文で格納されている。キャッシュ（具体的には、最終レベルキャッシュ（ＬＬＣ）１０９）は、メモリコントローラ１０８に接続されている。メモリコントローラ１０８は、１または複数の通信インターフェースおよび暗号化／復号化エンジン（ＥＤＥ）１１０を有する。

【００２０】

メモリコントローラはストレージ１１２に接続されている。さまざまな実施形態において、ストレージ１１２は、ダイナミックランダムアクセスメモリ（ＤＲＡＭ）、スタティックダイナミックランダムアクセスメモリ（ＳＲＡＭ）、相変化メモリ（ＰＣＭ）、ランダムアクセスメモリ（ＲＡＭ）等の１または複数のメモリデバイス（メインメモリとも呼ぶ）、不揮発性ランダムアクセスメモリ（ＮＶＲＡＭ）、光ディスクあるいは磁気ディス

ク、フラッシュドライブ等の１または複数のセカンダリストレージデバイス、または、１または複数のメモリデバイスとセカンダリストレージデバイスとの組み合わせ等を含む。例示を目的として、物理メモリを用いて実現されるストレージを含む例を詳細に以下で説明するが、当該技術は、セカンダリストレージデバイス、または、メモリとセカンダリストレージとの組み合わせを用いて実現されるストレージにも適用可能である。

【００２１】

本例において、メモリコントローラ１０８およびストレージ１１２は共に、ハイキャンプ・システムズ社（Ｈｉｃａｍｐ　Ｓｙｓｔｅｍｓ、米国カリフォルニア州メンローパーク）製の階層普遍コンテンツアドレッシング可能メモリプロセッサ（Ｈｉｅｒａｒｃｈｉｃａｌ　Ｉｍｍｕｔａｂｌｅ　Ｃｏｎｔｅｎｔ　Ａｄｄｒｅｓｓａｂｌｅ　Ｍｅｍｏｒｙ　Ｐｒｏｃｅｓｓｏｒ、ＨＩＣＡＭＰ（商標））等の構造化メモリを実現している。他の適切なデータラインベースのメモリアーキテクチャを利用することもできる。各データラインは、当該データラインが割り当て解除されて新しいコンテンツに割り当て直されるまで変更されないコンテンツを格納するよう構成されている。ＨＩＣＡＭＰ等の構造化重複排除メモリの実装および動作は、当業者に公知である。

【００２２】

図示しているように、ストレージの一部は、小さい（例えば、数バイトから数百バイトのオーダの）データライン１１４のアレイを含む。各データラインは、データライン識別子（ＰＬＩＤ）によってアドレス指定される。一部の実施形態において、各データラインは、当該ラインの寿命の限り不変のままのコンテンツを持つ。言い換えると、データラインが作成されデータがポピュレートされると、データラインのコンテンツは、メモリが割り当て解除されて別のコンテンツを格納するよう割り当て直されるまで、変更されない。一部の実施形態において、各データラインのデータコンテンツは、重複排除されている。言い換えると、各データラインは一意的なデータコンテンツを持つ。

【００２３】

本例において、各データラインは、暗号化データコンテンツの１ブロックを含む。格納されている暗号化データラインは、ある程度の間接性を持ってアクセスされ、２またはより多い別個のアドレスが実際には同じデータラインを参照し得る。また、暗号化データラインは重複排除されている。間接アクセスおよび重複排除の詳細については後述する。一部の実施形態において、厳密な重複排除は必要ではなく、複数の異なるデータラインは、所定の状況下で同じコンテンツを格納することが許容される。可能性として、重複したデータラインは、重複排除したデータラインとは別個に保持される。

【００２４】

一部の実施形態において、データラインにアクセスするためのある程度の間接性は、トランスレーションラインを用いることで得られる。図１において、ストレージ１１２の一部はトランスレーションライン１１６を格納している。トランスレーションライン（間接ラインとも呼ばれる）は、特定のコンテンツ（例えば、ページコンテンツ）を含む順番に並べられた１セットのデータラインの論理構造を形成する。一のトランスレーションラインは１セットのデータラインを参照すると記載する。これは、一の間接ラインが、複数のデータラインのアドレスまたは識別子（例えば、データラインのＰＬＩＤ）を含み得るか、または、対応する１セットのデータラインに対応付けられていることを意味する。図示した例によると、トランスレーションラインは、対応するデータラインのＰＬＩＤ値を含む複数のエントリを含む。データラインは重複排除されているので、複数のトランスレーションラインは、同じデータコンテンツについて同じデータラインを参照する。例えば、トランスレーションライン１および２はともに、ＰＬＩＤ「１」のデータラインを参照している。

【００２５】

本例およびその他の例で示すトランスレーションラインおよびデータラインのフォーマット、サイズおよび数は、例示を目的としたものに過ぎず、他の実施形態では変更し得る。例えば、一部の実施形態において、各データラインは６４バイトで、各間接ラインは２

５６バイト（共有可能なデータラインの識別子（またはアドレス）を含む４バイトエントリを６４個含む）である。以下に記載する例ではサイズを固定値として説明するが、一部の実施形態において、サイズを可変とすることが可能である（例えば、システムは、モード毎に単位サイズが異なる複数のモードをサポートするとしてよい）。一部の実施形態において、データラインおよび／またはトランスレーションラインには追加のメタデータが含まれる。一部の実施形態において、データラインはコンテンツディレクトリに配置され、ディレクトリ内でデータラインのコンテンツを検索することによってデータラインのアドレス指定が可能である。

【００２６】

一部の実施形態において、ストレージへのアクセスは、複数のセグメントとして行われる。各セグメントは、複数のデータラインから成る論理的に連続したシーケンスであり、データラインの有向非巡回グラフ（ＤＡＧ）として構造化されている。セグメントテーブルでは、各セグメントを、ＤＡＧの根を表すＰＬＩＤにマッピングする。セグメントは、セグメント識別子（ＳｅｇＩＤ）によって識別されアクセスされる。プロセッサ内の特定用途向けレジスタ（イテレータレジスタと呼ばれる）によって、セグメントに格納されているデータへのアクセス、例えば、ＤＡＧからのデータのロード、イタレーション、プリフェッチ、および、セグメントコンテンツの更新等が効率化される。

【００２７】

図示している例では、データラインのコンテンツは、Ｅｎ（ｘ）と表す暗号化データコンテンツを含む。尚、ｘは暗号化されていないデータコンテンツである。各データラインのデータコンテンツは重複排除されており一意的であるので、特定のコンテンツ（例えば、「ＧＯＯＤ」の暗号化バージョンＥｎ（"ＧＯＯＤ"））は複数のデータラインの中で１回のみ登場する。暗号化されたブロックの重複排除によって、ブロック暗号化に対する公知の攻撃、特に頻度分析攻撃は、所与のデータコンテンツについて格納されている複製が多くても１つのみであるので、失敗に終わる。このような重複排除は、暗号メディア拡張（ＥＭＥ）等のブロック暗号化方法は、徹底的に検討した結果ＥＭＥは「一意的なメッセージ」についてセキュアであると結論付けられたことに基づき、データブロックに適用し得ることを意味する。本願では、重複排除メカニズムによって、データラインはコンテンツとして一意的なメッセージを含むことが保証される。

【００２８】

一部の実施形態において、トランスレーションラインも暗号化される。データラインコンテンツおよび／またはトランスレーションラインの暗号化、復号化およびアクセスの方法の詳細については後述する。

【００２９】

メモリコントローラは、コンテンツディレクトリに基づく技術を用いてメモリの重複排除をサポートする。コンテンツディレクトリに基づく技術は、より詳細に以下で説明する。トランスレーションラインおよびデータラインは、必要に応じて、キャッシュ１０６にロードされ、キャッシュ１０６に書き戻され、または、キャッシュ１０６からエビクションさせられる。メモリコントローラ内のＥＤＥは、キャッシュ１０６から取得しストレージ１１２に格納すべきデータを暗号化し、ストレージ１１２から取り出しキャッシュ１０６に転送すべきデータを復号化する。

【００３０】

上述したメモリコントローラおよびＥＤＥ等のモジュールは、１または複数のプロセッサ上で実行されるソフトウェアコンポーネントとして、所定の機能を実行するよう設計されているプログラマブルロジックデバイスおよび／または特定用途向け集積回路等のハードウェアとして、または、両者の組み合わせとして実現され得る。一部の実施形態において、モジュールは、不揮発性記憶媒体（光ディスク、フラッシュストレージデバイス、モバイルハードディスク等）に格納可能なソフトウェア製品の形態で、例えば、コンピュータデバイス（パーソナルコンピュータ、サーバ、ネットワーク機器等）に本願の実施形態で説明する方法を実施させるための複数の命令として具現化され得る。複数のモジュール

は、一のデバイスで実現されるとしてもよいし、または、複数のデバイスにわたって分散しているとしてもよい。それぞれのモジュールの機能は、互いに統合するとしてもよいし、または、複数のサブモジュールにさらに分割するとしてもよい。

【００３１】

図２Ａおよび図２Ｂは、複数の重複排除ドメインの実施形態を示すデータ構造図である。図２Ａおよび図２Ｂに示すデータ構造の詳細については以下で説明する。

【００３２】

図３は、データをストレージに書き込むプロセスの実施形態を示すフローチャートである。プロセス３００は、システム１００等のシステムで実行することができ、具体的には、メモリコントローラ１０８によって実行され得る。

【００３３】

３０２において、所与のデータコンテンツをストレージに書き込むよう求める要求を受信する。一部の実施形態において、当該要求は、プロセッサが発行し、メモリコントローラが受信する。一部の実施形態において、当該要求はメインメモリ内の物理アドレスを特定しており、メモリコントローラは、当該要求に応じて、マッピングテーブルで検索するか、トランスレーション関数を適用するか、または、任意のその他の適切な技術を用いて、物理アドレスをトランスレーションラインエントリに対する参照にトランスレーションする。例えば、当該要求は、データコンテンツ"ｈｅｌｌｏ"を物理アドレス「１１００」に書き込むことを含むとしてよい。メモリコントローラは、トランスレーションを実行し、識別子「１１０」を持つトランスレーションラインの最初のエントリがこの物理アドレスに対応すると判断する。

【００３４】

３０４において、当該要求に応じて、書き込むべきデータコンテンツに基づき暗号化コンテンツを生成する。一部の実施形態において、暗号化関数Ｅｎ（ｘ）をデータコンテンツｘに適用して暗号化出力を生成する。本例において、暗号化コンテンツはＥｎ（"ｈｅｌｌｏ"）と表す。Ｅｎ（ｘ）は、その他の入力パラメータ、例えば、セキュリティ鍵および／または初期化ベクトル（ＩＶ）値等を追加する必要があるとしてよい。これらは必要に応じて取得される。一部の実施形態において、セキュリティ鍵は、特定のレジスタ等の公知のロケーションに格納されている。複数のドメインが用いられる実施形態では、現在のドメインについて適切な鍵が選択される。

【００３５】

さまざまな暗号化技術を実施し得る。一部の実施形態において、ＥＤＥは、暗号化データコンテンツを生成するために確定的暗号化関数を実行する。確定的ブロック暗号化方式（確率的暗号化方式とは逆）は常に、所与の入力データブロックについて同じ暗号文を生成する。複数のデータラインについて、これらは重複排除されておりそれぞれ異なる暗号化結果を格納しているので、別個の暗号鍵またはＩＶを用意する必要はない。このため、頻度分析攻撃に対する脆弱性は無い。一部の実施形態において、メモリコントローラ内のＥＤＥは、アドバンスド・エンクリプション・スタンダード（ＡＥＳ）技術を採用して１６バイトのブロックサイズでブロック暗号化を実現する。一部の実施形態において、ＥＤＥは、ＥＣＢ－Ｍｉｘ－ＥＣＢ（ＥＭＥ）技術を採用して、従来のプロセッサの６４バイトのキャッシュラインを処理するワイドブロックセキュア疑似ランダム置換（ＰＲＰ）を構築する。ＥＭＥは並列化の傾向が強いので、複数の独立したハードウェアサブモジュールは、復号を並列に実行することができる。この結果、キャッシュミスのレイテンシが最小限に抑えられる。暗号化についても同様であってよく、キャッシュラインエビクション時間が短くなる。ＥＭＥを適用することで、例で示したサイズよりも大きいキャッシュラインサイズおよび小さいキャッシュラインサイズがサポートされ得る。例示を目的としてＡＥＳおよびＥＭＥ等の技術を詳細に説明したが、他の適切な暗号化／復号化技術を利用することができる。他の実施形態では、例えば、ＸＥＸ－ＴＣＢ－ＣＴＳ（ＸＴＳ）、ＣＢＣ－Ｍａｓｋ－ＣＢＣ（ＣＭＣ）およびその他の等長暗号化／復号化技術を利用することができる。

【００３６】
３０５において、暗号化データコンテンツに対する参照を取得するよう試みる。さまざまな実施形態において、参照は、ポインタ、アドレス、ハンドル、識別子、または、特定のコンテンツにアクセスするための任意のその他の適切な指示情報であってよい。一部の実施形態において、暗号化データコンテンツに対する参照を取得しようとする試みは、暗号化データコンテンツを所与として参照を取得するための処理を実行することを含む。例えば、暗号化データコンテンツＥｎ（"ｈｅｌｌｏ"）の検索処理を実行する。一部の実施形態において、このような処理は構造化メモリ実装によってサポートされる。
【００３７】
３０６において、暗号化データコンテンツに対する参照の取得に成功したか否かを判断する。暗号化データコンテンツが既にストレージ内に存在している場合、暗号化データコンテンツに対する参照の取得に成功し得る。例えば、Ｅｎ（"ｈｅｌｌｏ"）が既にストレージ内にあり当該コンテンツを格納しているデータラインがＰＬＩＤ「１４」を持つ場合、既に存在する暗号化コンテンツＥｎ（"ｈｅｌｌｏ"）を参照するＰＬＩＤ「１４」を取得する。より詳細に後述するが、一部の実施形態において、暗号化データコンテンツは、特定コンテンツを素早く検索可能なコンテンツディレクトリ／ハッシュテーブルに格納される。
【００３８】
暗号化データコンテンツに対する参照の取得に成功した場合、３１２において、トランスレーションラインを修正して、取得した参照を参照する。一部の実施形態において、トランスレーションラインは、参照自体を格納する。一部の実施形態では、トランスレーションラインは、アドレス、ポインタ、ハンドル、または、参照に対応付けられる同様のものを格納する。本例において、トランスレーションライン１１０の最初のエントリ（要求された物理アドレス「１１００」に対応）を修正して、取得した参照であるＰＬＩＤ「１４」を参照する。
【００３９】
しかしながら、暗号化コンテンツはまだストレージには存在せず、暗号化データコンテンツに対する参照を取得しなかった場合、３１０において、暗号化コンテンツを新しいロケーションに格納し、この新しいロケーションに格納されている暗号化コンテンツに対する参照を取得する。例えば、Ｅｎ（"ｈｅｌｌｏ"）がまだストレージ内に存在しないと判断されると、ＰＬＩＤ「１９」を持つ新しいデータラインを作成してＥｎ（"ｈｅｌｌｏ"）を格納し、ＰＬＩＤ「１９」を取得する。３１４において、トランスレーションラインを修正して、新しいロケーションに格納されている暗号化コンテンツに対する参照を参照する。本例において、トランスレーションライン１１０の最初のエントリ（物理アドレス「１１００」に対応）を修正してＰＬＩＤ「１９」を参照する。
【００４０】
図４は、ストレージ内のロケーションからデータを読み出すプロセスの実施形態を示すフローチャートである。プロセス４００は、システム１００等のシステム、具体的にはメモリコントローラ１０８で実行されるとしてよい。
【００４１】
４０２において、あるロケーション（読み出しロケーションとも呼ばれる）のデータコンテンツにアクセスするよう求める要求を受信する。一部の実施形態において、当該要求はプロセッサが発行し、当該要求で特定されるロケーションはメインメモリ内の物理アドレスに対応する。
【００４２】
４０４において、物理アドレスは、マッピングテーブルにおいて検索することによって、トランスレーション関数を適用することによって等の方法で、トランスレーションラインロケーション（例えば、トランスレーションライン内のエントリのアドレス）にトランスレーションされる。例えば、物理アドレス１２００にあるデータコンテンツを求める要求は、ＰＬＩＤ「１９」を格納するトランスレーションライン１２０のエントリ２に対応

するとしてよい。

【００４３】

４０６において、当該要求に応じて、データコンテンツはキャッシュ内で利用可能か否かを判断する。具体的には、キャッシュにおけるトランスレーションラインおよびＰＬＩＤを持つ対応するデータラインの利用可能性を確認する。４つの可能性がある。

ミス／ミス（つまり、トランスレーションラインもデータラインもキャッシュ内で利用可能でない

ヒット／ミス（つまり、トランスレーションラインはキャッシュ内で利用可能であるが、データラインは利用可能でない）

ヒット／ヒット（つまり、トランスレーションラインおよびデータラインの両方がキャッシュ内で利用可能）

ミス／ヒット（つまり、トランスレーションラインはキャッシュ内で利用可能でないが、データラインはキャッシュ内で利用可能）

【００４４】

４０８において、ミス／ミスの場合を処理する。具体的には、トランスレーションラインおよびＰＬＩＤを持つデータラインは両方とも、メインメモリからロードされ、必要に応じて復号化される。例えば、トランスレーションライン１２０およびＰＬＩＤ「１９」を持つデータラインがいずれもキャッシュ内で利用可能でない場合、トランスレーションライン１２０（ＰＬＩＤエントリも含む）をストレージからキャッシュへロードして、ＰＬＩＤ「１９のデータラインも、対応する暗号化コンテンツと共に、メインメモリからロードして、復号化して、復号結果をキャッシュに保存する。一部の実施形態において、トランスレーションライン１２０内の全てのエントリのコンテンツを復号化してキャッシュにロードする。一部の実施形態では、要求されている（この場合は、ＰＬＩＤ「１９」の）特定のデータラインエントリのコンテンツのみを復号化してキャッシュにロードする。キャッシュ内のデータはこの後、要求元に対して提示する。一部の実施形態において、トランスレーションラインは重複排除されていないので、頻度分析攻撃に対する保護が必要になる。ＩＶ、ＭＡＣまたはその他のセキュアメモリ技術を用いる暗号化／復号化技術を用いてトランスレーションラインを保護するとしてよい。

【００４５】

４１０において、ヒット／ミスの場合を処理する。具体的には、トランスレーションラインは既にキャッシュ内に存在し、データラインの暗号化コンテンツはメインメモリからロードされ、復号化され、キャッシュに保存される。例えば、トランスレーションライン１２０が既にキャッシュ内に存在するがＰＬＩＤ「１９」のデータラインが存在しない場合、データラインの暗号化コンテンツはメインメモリからロードされ、復号化され、キャッシュに保存される。ミス／ミスの場合にトランスレーションラインの全てのエントリのコンテンツが復号化されてキャッシュにロードされる実施形態では、トランスレーションラインが既にキャッシュ内に存在すれば、対応するＰＬＩＤエントリも同様であるので、ヒット／ミスのシナリオは比較的稀である可能性が高いことに留意されたい。

【００４６】

４１４において、ヒット／ヒットの場合を処理する。この場合、トランスレーションラインおよびデータラインの両方がキャッシュ内に存在し、メインメモリからさらに取り出す必要はない。キャッシュ内のデータラインのデータコンテンツを要求元に提示する。キャッシュ内に格納されているものは平文に復号化されているので復号化は不要であることに留意されたい。

【００４７】

４１２において、ミス／ヒットの場合を処理する。この場合、トランスレーションラインをキャッシュにロードするが、データラインの読み出しまたはトランスレーションは、データラインが既にキャッシュ内に存在するので、必要はない。

【００４８】

４１４において、キャッシュ内のデータラインのデータコンテンツを要求元に提示する

。例えば、キャッシュ内のＰＬＩＤ「１９」の復号化データコンテンツを要求元に提示する。

【００４９】

キャッシュアクセスプロセスは以下の理由から効率的に実行される。

ｉ）トランスレーションラインおよび対応するデータラインが大抵、キャッシュ内で発見されるので、ヒット／ヒットのケースが非常に一般的になる

ｉｉ）暗号鍵は、プロセッサで実行されるプロセスで共通なので、利用の度にプロセッサコアの外部から取得する必要がない

ｉｉｉ）プロセッサアクセスはプロセッサキャッシュで十分であり、プロセッサキャッシュにデータが平文で格納されているので、メインメモリへのアクセスは大抵の場合に行われないこのため、これらの場合では、利用前のメインメモリアクセスまたは復号化は不要である。

【００５０】

一部の実施形態において、キャッシュラインミスの際にセキュアパッドの生成（そして、結果として、暗号化メモリからのフェッチ）と暗号化メモリラインのフェッチとを同時に行うように、ＥＤＥが実現される。本明細書で用いられる場合、「セキュアパッド」とは、復号化中にマスクとして機能する複数のバイナリ値のシーケンスを意味する。セキュアパッド生成技術は当業者には公知である。そして、復号化は、暗号化データラインをメインメモリから受信すると、暗号化ラインとセキュアパッドとの間の単純なＸＯＲを実行して平文データを生成することを必要とする。これによって復号化のレイテンシの影響を最小限に抑える。

【００５１】

キャッシュ空間は限られているので、一部のキャッシュラインに存在するデータは、新しいデータのためにキャッシュラインを利用できるようにするべく、時折エビクションする必要がある。エビクションすべきキャッシュライン内のデータが修正されている場合、修正後のデータをストレージに書き戻す必要がある。図５は、キャッシュからデータラインをエビクションするためのプロセスの実施形態を示すフローチャートである。プロセス５００は、システム１００等のシステムで実行することができ、具体的にはメモリコントローラ１０８によって実行し得る。

【００５２】

５０２において、データラインを格納するキャッシュラインをエビクションするよう求める要求を受信する。例えば、ＰＬＩＤ「２１」を持ち、データコンテンツ"ｈｅｌｌｏ"を有するデータラインを格納するキャッシュラインをエビクションするよう求める要求を受信する。

【００５３】

５０４において、キャッシュラインのコンテンツがストレージ（例えば、メインメモリ）に最後に書き込まれた時点以降でキャッシュラインが修正されたか否かを判断する。一部の実施形態において、データラインが修正された場合は常に設定される「ダーティ」フラグが設けられている。５０４の判断は、このフラグを確認することで行う。

【００５４】

キャッシュラインのコンテンツがストレージに最後に書き込まれた時点以降にデータラインを格納しているキャッシュラインが修正されていないと判断される場合、５０６において、データラインはキャッシュから削除することができ、キャッシュラインを空けるか、または、利用可能とマーキングする。エビクションプロセスを終了する。

【００５５】

しかし、キャッシュラインのコンテンツがストレージに最後に書き込まれた時点以降にデータラインを格納しているキャッシュラインが修正されたと判断される場合、この修正をストレージに書き込む必要がある。５０８において書き戻し処理を実行する。本例では、書き戻し処理は図３のプロセス３００と同一であり、キャッシュライン内の修正後のコンテンツをストレージに書き込む。

【００５６】
上記の例では、ストレージ内のデータラインは、暗号化されており、重複排除されている。一部の実施形態において、キャッシュ（例えば、ＬＬＣ）も、特定のデータコンテンツが既にキャッシュ内に存在するか否かを判断する同様のコンテンツディレクトリベースの検索メカニズムを実現することによって、重複排除をサポートする。これによって、キャッシュレベルで重複を排除することでキャッシュリソース（例えば、キャッシュ空間）に対する要件が軽減される。
【００５７】
上述した技術を利用することで、プロセッサは、キャッシュミスが発生した場合のメモリラインの復号化について、そして書き戻しの際の暗号化についても同様に、効率的に低いレイテンシで実現することができる一方、メモリ内のデータの暗号化について高い安全性を保証することができ、大容量のメインメモリまでスケーリングすることができる。
【００５８】
＜トランスレーションラインの暗号化＞　上述した例では、トランスレーションラインは暗号化されていない。一部の実施形態において、トランスレーションラインは暗号化されている。このため、ＬＬＣ外にあるトランスレーションラインへのアクセスは、データラインについてのステップと同様のステップを実行することによって処理される。つまり、トランスレーションラインをＬＬＣにロードする際に当該ラインを復号化する。同様に、修正されたトランスレーションラインを書き戻す場合には、トランスレーションラインを暗号化して暗号化状態を作成することが必要になる。
【００５９】
トランスレーションラインは必ずしも重複排除されていないことに留意されたい。図６は、初期化ベクトル（ＩＶ）を含むデータ構造の例を示す図である。ＩＶ値は、暗号化の際にＥＤＥが利用するランダムに選択されたパラメータを含む。同じデータコンテンツを異なるＩＶ値を利用して暗号化すると、暗号化の結果として異なるものが作成される。本例において、各トランスレーションラインはＩＶフィールドを含み、複数の非重複排除トランスレーションラインには複数の異なるＩＶ値が割り当てられる。例えば、トランスレーションライン１００および５０２は、同じコンテンツを有するが、異なるＩＶ値が割り当てられている。一部の実施形態において、ＥＤＥは確定的ブロック暗号化を実行する。図示されているように、同じデータを含むトランスレーションラインの暗号化の結果が異なるのは、暗号化エンジンによる入力の一部として異なるＩＶ値が用いられるためである。これによって、トランスレーションラインは頻度分析攻撃から保護される。さらに、トランスレーションラインはメモリ全体から見ると占める割合は小さいので、トランスレーションライン毎にＩＶ値を含めても大量の空間オーバーヘッドが発生するわけではない。
【００６０】
一部の実施形態において、ＥＤＥは、暗号化／復号化を実行するためにＩＶに加えて鍵を必要とする。この鍵はレジスタまたはその他の公知のロケーションに格納することができる。こうして空間またはアクセスのオーバーヘッドを最小限に抑える。
【００６１】
一部の実施形態において、トランスレーションラインについて利用される鍵は、データラインについて利用される鍵とは異なる。
【００６２】
一部の実施形態において、トランスレーションラインのセットは複数あり、トランスレーションラインセット毎に別個の鍵を利用する。一部の実施形態において、複数の異なる保護ドメインにおける複数の異なるトランスレーションラインについて複数の別個の鍵を利用する。例えば、マシン上の複数の異なるプロセスについて複数のトランスレーションラインセットが割り当てられており、各プロセスに対応する別個のトランスレーションラインセットについて別個の鍵を利用する。別の例として、プロセッサのアドレス空間は複数の異なるセグメントに分割することができ、一部のセグメントは複数のプロセスが共有する。このため、共有セグメントは、当該共有セグメントにアクセスし得る複数のプロセ

スが共有する鍵を用いて暗号化され、専用セグメントは、専用の共有されていない鍵を用いて暗号化される。複数のトランスレーションラインセットの割り当ては他の方法も可能である。

【００６３】

＜コンテンツディレクトリのメタデータの暗号化＞

図７Ａは、従来の実施例において構造化メモリをサポートするために用いられるメタデータの例を示すデータ構造図である。本例において、構造化メモリはコンテンツディレクトリ８００によってサポートされている。コンテンツディレクトリ８００は、データコンテンツと、エントリの署名等の対応メタデータとを格納しているメインメモリ内のハッシュテーブルである。特定のデータコンテンツが既にメモリ内に存在するか否かを判断するために、データコンテンツのハッシュ値を計算してハッシュテーブルで検索する。このため、実質的には、各データラインにハッシュインデックスが対応付けられている。例えば、暗号化を実施しない従来のシステムにおいて、アドレスＡｉに割り当てられているラインは、Ａｉからハッシュテーブルのベースアドレス（Ｂｉ）を減算し、減算結果をバケットのサイズ（Ｓ）で除算することによって、あるバケットに対応付けられていると判断され得る。メタデータはハッシュインデックスを含む。

【００６４】

本例において、メタデータは、ハッシュバケットの各エントリに対応付けられている署名を含む。当該署名は、データコンテンツの別のハッシュとして算出され、ハッシュバケット内で特定のエントリを検索する際にセカンダリインデックスとして利用される。

【００６５】

本例において、データラインエントリ毎に、当該エントリを参照するトランスレーションラインの数を示す参照カウントが設けられている。参照カウントがゼロになると、対応するデータラインはガベージコレクションの対象となり、メモリが空く。

【００６６】

図７Ｂは、セキュアな実施例における構造化メモリをサポートするために用いられるメタデータの例を示すデータ構造図である。この例において、メタデータ値は暗号化されるので、不正な修正を検出することができる。具体的には、ハッシュインデックスは、セキュアな鍵付きハッシュ（ＳｅｃＨａｓｈ）を暗号化データコンテンツ（Ｅｎ（"ｈｅｌｌｏ"））に対して用いることで算出される。暗号化データコンテンツは、ハッシュインデックスに対応するテーブル内のロケーションに格納されており、暗号化コンテンツの検索はこのハッシュインデックスを用いて実行される。対応付けられている署名ラインは同様に算出される。一部の実施形態において、ハッシュインデックスおよび署名は、一のセキュアな鍵付きハッシュ、例えば、ハッシュベースのメッセージ認証コード（ＨＭＡＣ）のうち異なる部分を切り取ることで得られる。同様に、参照カウントも暗号化され得る。データコンテンツとメタデータとが不一致の場合、不正な修正等のセキュリティ違反が発生している可能性がある。

【００６７】

他の実施形態では異なるメタデータ構造および検索処理を利用し得る。例えば、一部の実施形態において、データラインの暗号化されていないデータコンテンツについてハッシュを算出する。この後、データコンテンツを暗号化して算出されたロケーション（つまり、暗号化されていないデータコンテンツに対応するハッシュテーブル内のロケーション）に格納する。このような実施形態において、暗号化コンテンツを検索するべく、または、データラインの暗号化データコンテンツに対する参照を取得するべく、暗号化データコンテンツを復号化して、復号化の結果に基づきハッシュエントリロケーションを決定する。

【００６８】

＜データ鍵ドメイン＞　一部の実施形態において、複数の別個の保護ドメインは、データラインを暗号化するために複数の別個のデータ暗号鍵を利用する。これによって、これらのドメイン間の保護が強化される。本明細書で用いる場合、「保護ドメイン」は、データラインが選択されたプロセスにのみアクセス可能であるメモリの領域を意味する。

【００６９】
複数の別個のドメインにおけるデータラインについて複数の別個の鍵を利用する一部の実施形態において、データラインは、メインメモリ内の共通の共有コンテンツディレクトリ（例えば、共通ハッシュテーブル）に格納されている。異なるコンテンツの２つのラインについて、２つの異なる鍵で暗号化すると同じ暗号化データコンテンツが得られる可能性がある。このため、原理的には、複数の異なる保護ドメインがコンテンツディレクトリにおいて同じエントリを共有することになる可能性がある。例えば、データドメイン１について、データコンテンツ"ｈｅｌｌｏ"の暗号化が"ｘｙｚ１２３"であり、データドメイン２について、データコンテンツ"ｗｏｒｌｄ"の暗号化もまた"ｘｙｚ１２３"である。メインメモリには"ｘｙｚ１２３"のインスタンスは１つのみ格納される。

【００７０】
一部の実施形態では共通データ暗号鍵を利用する。これによって、複数の異なる保護ドメイン間であっても、復号化および再暗号化を実施することなく、データを複製し得る。複数の異なるドメインにおいて復号化および再暗号化する必要があるのは、影響を受けたトランスレーションラインのみである。これは、複数の異なるドメインでは複数の異なる鍵を用いてトランスレーションラインが保護されているためである。このため、復号化および再暗号化の必要処理量が低減される。

【００７１】
一部の実施形態において、複数の特定のドメインが、一の共有鍵を用いて暗号化され共有されている。例えば、２つの別個のプロセスは共に、共有されているセキュアな暗号化データにアクセスすることができる。これは、共通ドメインについて共通共有鍵を提供することで実現される。どちらのプロセスも同じデータを復号化することができる。一方、秘密にしているデータは、共有されない秘密鍵を用いて暗号化される。

【００７２】
一部の実施形態において、複数の暗号化コンテンツは複数の別個の鍵を用いて暗号化されるが、コンテンツディレクトリに対応付けられているメタデータは、このコンテンツディレクトリを共有している複数の保護ドメインにわたって共有されている共通鍵を用いて暗号化される。メタデータについて共通鍵を共有することで、各保護ドメインは、例えば、参照カウント、バケットに対応付けられている署名ライン等、重複したエントリに対応付けられているメタデータにアクセスして更新することができる。

【００７３】
複数の特定の保護ドメイン間で共有メタデータ鍵が拒否される場合、実施形態は、以下で説明するように、複数の別個の重複排除ドメインをサポートするとしてよい。

【００７４】
＜重複排除ドメイン＞　一部の実施形態において、プロセッサのアドレス空間は複数の重複排除ドメインに分割される。本明細書で用いられる場合、「重複排除ドメイン」は、メモリのうちデータラインが重複排除され一意的なコンテンツを持つ領域を意味する。プロセッサは、一の重複排除ドメインにおいて、所与のデータコンテンツについて既に存在する複製を検索する。

【００７５】
メモリには一の所与のデータブロックについて複数のインスタンスが存在し得る場合がある。しかし、複数の重複排除ドメインにおける所与のデータブロックの頻度は、依然としてアプリケーション全体での所与のデータブロックの頻度とは無関係であるので、頻度に基づく分析および攻撃を防ぐことができる。さらに、複数の別個の重複排除ドメインは複数の別個の鍵を利用することができるので、各ドメインの同じコンテンツは同じ値として格納されることはない。言い換えると、所与の暗号文の頻度（例えば、データラインの暗号化コンテンツ）は、任意の特定の平文の発生頻度とは無関係である。

【００７６】
一部の実施形態において、重複排除ドメイン毎に別個の秘密鍵を利用して当該重複排除ドメインで用いられているデータラインを暗号化するので、ある重複排除ドメインにおけ

るアプリケーション（または、ある重複排除ドメインにおいてメモリへのアクセスを取得することが可能な攻撃者）は、別の重複排除ドメインのデータを復号することができない。一部の実施形態において、システムは、複数の重複排除ドメインを持つように構成されており、別個の保護ドメイン毎に１つ設けられている。

【００７７】

図２Ａは、複数のドメインを持つ実施形態を示すデータ構造図である。同図に示すように、複数の異なるドメインについて、データラインの暗号化には複数の別個の秘密鍵を用いている。鍵は、それぞれ値が異なり、予め指定されたレジスタに格納され得る。一部の実施形態において、鍵はフォーマットが異なる。例えば、一のドメインについて１２８ビットの鍵を用いることができ、別のドメインについては２５６ビットの鍵を用いることができる。ドメインの構成要素は、実施例に応じて異なり、複数の異なる実施形態で異なるとしてよい。例えば、別個のユーザが別個のドメインに対応するとしてよく、別個の鍵をそれぞれ対応するドメインにおけるデータラインを暗号化／復号化するために用いるとしてよい。保護ドメインについては他の方法で割り当てを行うことも可能である（複数の別個のプロセスについて複数の別個のドメインを割り当てる等）。本例では、データラインは、それぞれのドメイン内では重複排除されているが、必ずしも複数のドメインにわたってそうではない。このため、複数の別個のドメインには重複したデータラインが存在する可能性がある。メモリコントローラがデータの暗号化または復号化を必要とする場合、現在のドメインに対応付けられている鍵にアクセスして暗号化または復号化に利用する。複数の別個の重複排除ドメインを暗号化するために複数の別個の鍵を用いることで、複数の重複排除ドメイン間の保護が改善され、複数の異なるドメインの同じデータコンテンツは異なる方法で暗号化されるので、頻度分析攻撃に対する防御を高めることが保証される。

【００７８】

図２Ｂの実施形態において、各重複排除ドメインは任意で、別個のトランスレーションライン鍵を用いてトランスレーションラインに用いられるデータを暗号化し、別個のメタデータ鍵を用いてコンテンツディレクトリに対応付けられているメタデータを暗号化する。これらの鍵は値が異なり、予め指定されたレジスタに格納されるとしてよい。

【００７９】

＜タイミング攻撃の阻止＞　一部の実施形態において、書き戻し処理のタイミングを人工的に修正して、書き込み処理を実行するために用いられる指定所要時間を変更する。これによって、コンテンツが既にメモリに格納されている場合、コンテンツはまだ存在せず新しいメモリラインを割り当てる必要がある場合、または、メモリラインをオーバーフローエリアに書き込み中である場合について、重複排除メモリへの書き込みの指定所要時間に差異は認識できなくなる。

【００８０】

方法の１つとして、これらの処理のうちの任意の処理によって必要とされる最大の時間だけ、各書き込みの完了指示を遅延させる方法がある。この方法は、大半の書き戻し処理は「ポストされ（ｐｏｓｔｅｄ）」（つまり、アプリケーション実行に対して非同期に発生し）、遅延が増加しても通常はメモリ書き戻しスループットが下がることはないので、アプリケーション性能に重大な悪影響を及ぼすことはないはずである。

【００８１】

＜メモリのインテグリティ＞　一部のセキュアシステムについては、システム実行中に暗号化データを修正できると仮定される攻撃者を阻止してデータのインテグリティを保証するようさらに要求される。

【００８２】

本願では、重複排除をサポートするべく、コンテンツディレクトリは、明示的または暗示的に、上述したようにコンテンツに基づいて（コンテンツ検索の一環として）データのロケーションを決定する場合に有用なメタデータを含む。

【００８３】

上述したように、一部の実施形態によると、メタデータによって特定のハッシュバケッ

ト内のデータラインのロケーション（つまり、ハッシュバケットインデックス）を算出することができる。

【００８４】

一部の実施形態において、メモリインテグリティチェックは、データラインへの読み出しアクセスの場合、データラインのコンテンツを確認してデータコンテンツが当該データラインに対応付けられているメタデータに一致することを確認する。ＰＬＩＤ（または、均等物として、アクセス対象のアドレス）およびデータコンテンツは、読み出しアクセスの際に既に利用可能な状態であり、さらにメモリアクセスを実行することなくインテグリティチェックを実行することが可能である。具体的には、データラインのハッシュインデックスを算出し直して、データラインのロケーションを含むハッシュバケットと比較する。署名は、データラインコンテンツに基づいて算出されバケット内のエントリを決定するが、同様に算出し直されエントリと比較して確認する。算出したハッシュインデックスがハッシュバケット内のデータラインロケーションと一致しない場合、または、算出された署名がハッシュバケットのエントリの署名と一致しない場合、メモリインテグリティの侵害が示唆される。このため、検出されることなく（言い換えると、データインテグリティを侵害することなく）攻撃者がデータを修正できるのは、データコンテンツを修正しても修正後のデータコンテンツが、対応付けられているメタデータに依然として一致することができる場合に限られる。

【００８５】

さらに、一部の実施形態において、コンテンツ検索または論理書き込みの際に、データラインエントリ内のコンテンツが書き戻すべきコンテンツに実際に一致すると確認することが既に要件となっている。このため、この場合には、既にインテグリティチェックが実施されている。

【００８６】

さらに、一部の実施形態において、コンテンツ検索の際に、メタデータに関するデータラインエントリのデータインテグリティもまた、データコンテンツに基づきメタデータを算出すること、および、結果を格納されているメタデータと比較することによって、確認する。

【００８７】

一部の実施形態において、ハッシュインデックスメタデータおよび署名メタデータは、セキュアな鍵付きハッシュ関数によって生成される。これについては先述している。このため、このような実施形態によると、暗号化データラインを修正する攻撃者は、メタデータ鍵を知らなければ、修正後の暗号化データがこのメタデータに一致するか否かを判断できない。これに代えて、攻撃者が修正後のデータラインに対する参照を偽造でき、このラインへアクセスしようと試みる場合、システムは、データコンテンツに基づいてメタデータを算出し、メタデータとデータコンテンツとが一致しないと検出することによって、インテグリティの侵害を検出するであろう。セキュリティ侵害の可能性が報告される。ハッシュテーブルにおいてセキュアなハッシュを利用するので、現在のバケットロケーションに一致する値を推測することによってラインを不正に修正しようと試みる侵入者は、正しい値を推測できない可能性が高い。このため、セキュリティ侵害が発生している旨を示すアラート（ログまたはメッセージ等）がトリガされる。

【００８８】

上述したように、データインテグリティチェックは空間を余分に犠牲にすることなく実現される。

【００８９】

＜オーバーフローの処理＞　一部の実施形態において、ストレージはオーバーフローエリアを持つ。このような実施形態において、書き戻し時には、コンテンツがマッピングされているコンテンツディレクトリハッシュバケットにおいて空いているエントリが無い場合、メモリラインはオーバーフローエリアに書き込まれる。

【００９０】

一部の実施形態において、オーバーフローエリアはラインに対して重複排除を行わない。このため、同じデータの２またはより多いインスタンスを、重複排除ドメインに対応付けられているオーバーフローエリアで格納する可能性がある。オーバーフローラインをセキュアに処理するべく、別個のＩＶ等の余分なメタデータをオーバーフローデータライン毎に格納し、当該データラインのデータコンテンツを暗号化するために用いる。複数の異なるＩＶを用いて暗号化した同じデータコンテンツは暗号化の結果が異なるので、ラインレベルの暗号化は確定的でないことが保証される。つまり、オーバーフローエリアに格納されている同じデータの２つのインスタンスを暗号化しても、同じ暗号文は得られない。

【００９１】

さらに、以下のシナリオが発生し得る場合がある。最初に、データラインの第１の書き戻し処理時にはコンテンツディレクトリに空いているエントリが無いので、データラインをオーバーフローエリアに格納する。この後、ガベージコレクションが実施され、コンテンツディレクトリ内の１または複数のエントリが空く。この後、同じデータコンテンツを持つデータラインの第２の書き戻し処理が実行され、当該データラインは通常の重複排除コンテンツディレクトリに格納される。このように同じデータの２つのインスタンスが同じ暗号文に暗号化されないのは、これら２つのインスタンスは依然として実質的に、２つのＩＶを暗号化の際に利用しているためである。コンテンツディレクトリのハッシュバケット内のデータに対応付けられているＩＶは固定値またはヌル値であり、オーバーフローエリア内のエントリのＩＶはランダム値であるがハッシュバケットに対応付けられているＩＶとは異なる。

【００９２】

一部の実施形態において、プロセッサ／メモリコントローラは、要求されたアドレスがどこにあるかを確認することによって、読み出しアクセスがコンテンツディレクトリのオーバーフローエリアへのアクセスか否か、または、コンテンツディレクトリの非オーバーフローエリアへのアクセスか否かを検出できる。そして、ＩＶを利用した復号化を適用するとしてよい。同様に、コンテンツディレクトリを実装しているメモリコントローラは、コンテンツのハッシュバケットが埋まっている場合にはその事実を認識している必要がある。このため、オーバーフローエントリに対応するＩＶを用いてデータラインを暗号化し直すことができる。

【００９３】

複数の重複排除ドメインを持つ一部の実施形態において、複数の異なる重複排除ドメインのオーバーフローエリアは、異なる鍵を利用する。このため、複数の異なるドメイン内の同じコンテンツは、暗号化の結果が互いに異なることになる。

【００９４】

実際には、オーバーフローエリアはメモリ全体から見ると占める割合は小さいので、ＩＶメタデータのために発生する余分なオーバーヘッドは、オーバーフローラインだけに限定され、空間またはアクセス時間のいずれの観点からも重要ではない。

【００９５】

重複排除メモリの利用に関する調査で証明されたように、重複排除を採用することで大半のアプリケーションに必要な電力および物理メモリの量が減る。一部の実施形態において、重複排除によってＩＶ等のセキュアメタデータの空間オーバーヘッドも小さくなる。これは、セキュアメタデータはトランスレーションラインおよびオーバーフローラインについてのみ必要となるためである。

【００９６】

＜ハイブリッドメモリ＞　一部の実施形態において、ストレージは、レイテンシが異なる複数のメモリの組み合わせを用いて実現されるハイブリッドメモリを含む。後述する実施形態において、不揮発性ランダムアクセスメモリ（ＮＶＲＡＭ）およびダイナミックランダムアクセスメモリ（ＤＲＡＭ）を含むハイブリッドメインメモリを例示を目的として説明する。他の実施形態では他の種類のメモリを利用し得る。ＮＶＲＡＭは、ＤＲＡＭに比べて、レイテンシが長く、コストは低く、消費電力は少ない。このように構成されるハ

イブリッドメインメモリシステムは、ＤＲＡＭのみで実現可能な容量をはるかに超える容量を、比較的低い設備投資コストで、比較的低消費電力で実現しつつ、アクセス頻度が高いデータをＤＲＡＭにキャッシュすることによってアクセス時間を妥当なものとする。

【００９７】

ハイブリッドメインメモリを用いる一部の実施形態において、データラインは、上述したように、高レイテンシメモリおよび低レイテンシメモリ（例えば、ＮＶＲＡＭおよびＤＲＡＭ）の両方において用いるメモリラインサイズおよび鍵を同じとしつつ、確定的に暗号化され重複排除される。このため、ＤＲＡＭとＮＶＲＡＭとの間では、データに対して暗号化／復号化の処理を行うことなく、データラインを転送可能である。例えば、ＤＭＡエンジンは、暗号鍵へのアクセスを必要とすることなく、データラインを転送することができる。ＤＲＡＭと同様に、ＮＶＲＡＭにおいて重複排除を採用することで、重複排除を採用しなければ複製に費やしていたであろう空間、および、ＩＶの格納に費やしたであろう余剰空間を節約できる。

【００９８】

一部の実施形態において、低レイテンシメモリおよび高レイテンシメモリにおけるデータラインは、キャッシュおよびメインメモリにおけるデータラインと同様の方法で管理される。例えば、ＤＲＡＭはキャッシュと同様に取り扱うことができる。そして、ＮＶＲＡＭはメインメモリと同様に取り扱うことができる。データラインは、最初にＤＲＡＭに書き込まれ、その後で適宜ＮＶＲＡＭに書き戻される。ＤＲＡＭ内のデータラインは、修正済みとフラグを立てることが可能で、重複排除は行われず、ＮＶＲＡＭに対してマッピングもされない。ＤＲＡＭ内の修正されたデータラインをエビクションする場合、プロセス５００と同様のプロセスを実行する。具体的には、修正されたデータラインのデータコンテンツはＮＶＲＡＭ内のコンテンツディレクトリで検索される。データコンテンツがＮＶＲＡＭ内のコンテンツディレクトリに存在している場合、既に存在するラインのロケーションが判明する。そうでない場合、新しいデータラインをコンテンツディレクトリの適切なバケットに割り当てる。さらに、修正されたデータラインを参照するトランスレーションラインのロケーションを特定し、修正されたデータラインに対する参照を書き換えて、ＮＶＲＡＭ内の既に存在するラインを指し示すようにする。

【００９９】

一部の実施形態において、ハイブリッドメモリシステムにおける低レイテンシメモリからのトランスレーションラインエビクションおよびデータラインエビクションは、キャッシュからのトランスレーションラインエビクションおよびデータラインエビクションと同様に処理される。トランスレーションラインをＤＲＡＭからエビクションする前に、当該トランスレーションラインが参照する修正されたデータラインはそれぞれ、ＮＶＲＡＭにおいて重複排除して、データラインコンテンツについてＮＶＲＡＭにおけるＰＬＩＤ（ＮＶＲＡＭ　ＰＬＩＤと呼ぶ）を決定する。そして、この新しいＮＶＲＡＭ　ＰＬＩＤを参照するよう当該トランスレーションラインを更新する。参照するトランスレーションラインが無いデータラインはいずれも、エビクションの際に破棄する。このような実施形態において、ＮＶＲＡＭの重複排除は出来る限り後に回す。場合によっては、エビクションされる前にラインが破棄されるので、重複排除は行わない。このようにして、重複排除オーバーヘッドを削減する。ＮＶＲＡＭおよびＤＲＡＭについて複数の異なる鍵を用いる実施形態では、ＮＶＲＡＭへのエビクションの際に、修正されたラインを最初に読み出して復号化してキャッシュに保存し、ＮＶＲＡＭ鍵で暗号化し直して、ＮＶＲＡＭに重複排除で保存する。

【０１００】

一部の実施形態において、メモリコントローラは、ＮＶＲＡＭ内に存在するトランスレーションラインへの第１のデータアクセスにおいて、要求されたラインを返した後、対応付けられているトランスレーションラインが参照している他のデータラインをプリフェッチしてＤＲＡＭに転送する。これによって、後続の参照が生じる場合にはそれらについてのレイテンシを短くする。このように最適化することによって、ＮＶＲＡＭとＤＲＡＭと

の間の転送単位を大きくする利点の一部が得られることが期待される。

【０１０１】

一部の実施形態において、低レイテンシメモリにおける暗号化の単位は、高レイテンシメモリにおける暗号化の単位とは異なる。本明細書で用いる場合、「暗号化の単位」とは、一の暗号を生成するために暗号化されるデータ量を意味する。例えば、ＤＲＡＭの１つのメモリラインが一単位として暗号化される一方、ＮＶＲＡＭでは複数のメモリラインが一緒に一単位として暗号化される（例えば、６４個のラインが一緒に暗号化される）。ＮＶＲＡＭからＤＲＡＭへとデータを転送する場合、ＮＶＲＡＭの複数のメモリラインを含む一単位を復号化して、復号化された複数のラインをＤＲＡＭに転送して個別に暗号化する。一部の実施形態において、暗号化／復号化メカニズムはプロセッサチップ上で実現される。データ転送単位（例えば、６４個のライン）をＮＶＲＡＭからプロセッサへ転送する場合、プロセッサがこのデータ転送単位を復号して複数のメモリラインをキャッシュに格納する。続いて、複数のメモリラインを個別に暗号化し直してＤＲＡＭに書き戻す。一部の実施例によると、ＮＶＲＡＭは、ＮＶＲＡＭがＤＲＡＭとは異なるデータ単位サイズを採用したとしても、重複排除および確定的暗号化を採用して管理される。一部の他の実施例では、ＤＲＡＭ部分のみが重複排除および確定的暗号化を実施して、ＮＶＲＡＭは従来の確率的暗号化を利用する。

【０１０２】

ＮＶＲＡＭがＤＲＡＭよりも大きい単位でデータの暗号化および転送を実行する実施形態において、ＮＶＲＡＭは実質的に、プロセッサに対するＩ／Ｏデバイスである。つまり、プロセッサは実際にはこのＮＶＲＡＭに対して直接読み書きを実行するわけではない。これに代えて、ＤＲＡＭおよびＮＶＲＡＭはそれぞれ、キャッシュおよびメインメモリと同様に利用される。具体的には、相対的に大きいデータブロックをＮＶＲＡＭからＤＲＡＭへ読み出し、プロセッサが利用できるようにする。書き戻しについても同様のメカニズムを実施する。実質的に、当該システムはＤＲＡＭとＮＶＲＡＭとの間でページングの一形態を実施する。

【０１０３】

重複排除に基づくメモリ暗号化を説明してきた。上述した技術は、メインメモリおよびセカンダリストレージ素子の両方に適用可能である。本明細書で用いる場合、セカンダリストレージ素子は、オペレーションシステムおよびアプリケーションソフトウェアがメモリではなく格納素子として扱う、ＮＶＲＡＭベースのドライブ等のソリッドステートドライブ、磁気ディスクまたは光ディスク等のコンポーネント等を意味する。オペレーティングシステムおよびアプリケーションソフトウェアは通常、メモリアクセスコールではなくＩ／Ｏ関数呼び出しを用いて、セカンダリストレージシステムに対して読み書きを行う。セカンダリストレージシステムの一部の実施形態において、トランスレーションラインおよびメタデータは、各データのアクセス毎のコストが概してＤＲＡＭの場合よりも大幅に高いので、キャッシュされる。例えば、データラインの参照カウントは、ＤＲＡＭに格納するとしてよく、セカンダリストレージ（例えば、ＮＶＲＡＭ）を走査して各データラインに対する参照数をカウントすることで、リブート時に算出し直すとしてよい。これによって、これらの値をセカンダリストレージで格納または更新する必要がなくなる。

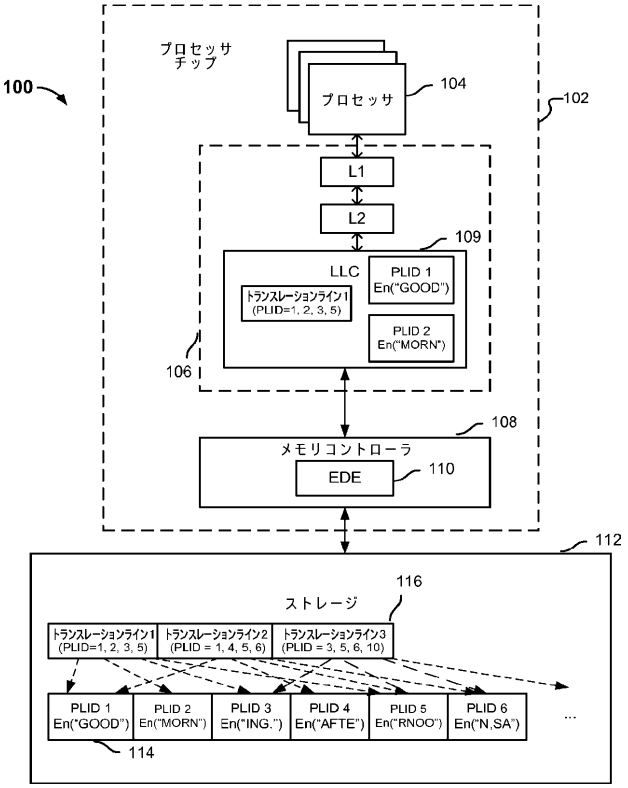
【０１０４】

重複排除ストレージの暗号化および復号化を利用したコンピュータセキュリティを開示した。上述した技術によれば、低レイテンシの暗号化および復号化を高効率で実行可能であり、高いデータセキュリティおよびスケーラビリティが保証され、大半のアプリケーションに必要なリソース（例えば、物理メモリ、電力、空間オーバーヘッド）の量が低減され、空間的に余分な犠牲を払うことなくデータセキュリティが得られる。

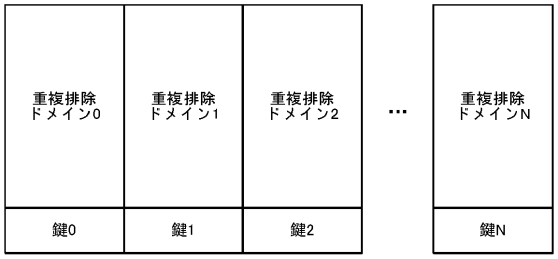
【０１０５】

上述した実施形態は理解を深めるという目的である程度詳細に説明したが、本発明は記載した詳細に限定されない。本発明の実施方法としては多くの代替例がある。開示した実施形態は一例に過ぎず、限定的ではない。

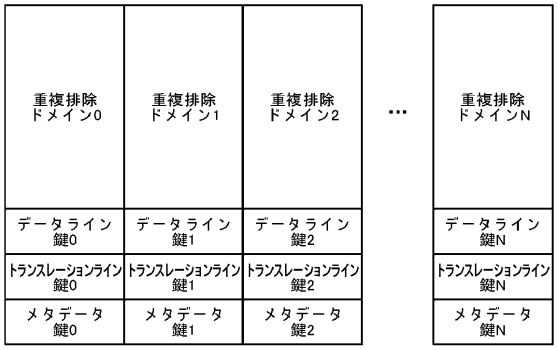
【図１】



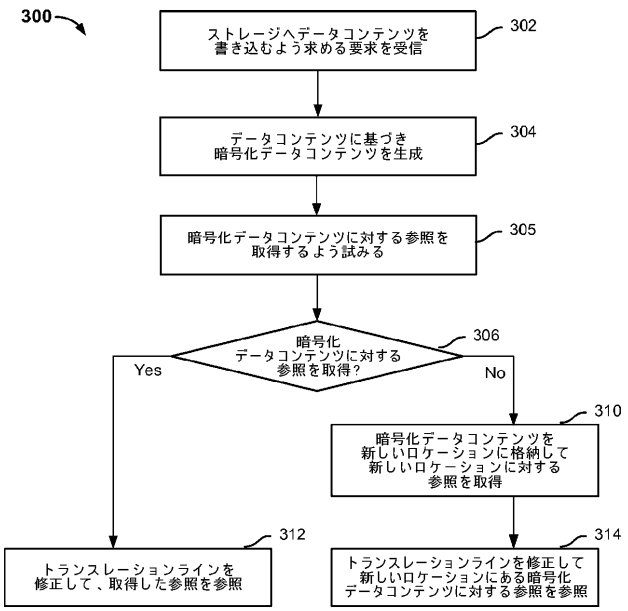
【図２Ａ】



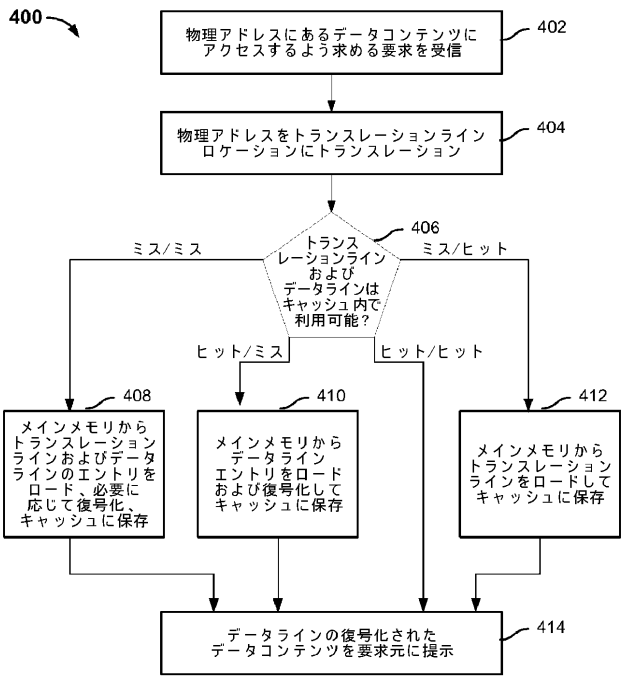
【図２Ｂ】



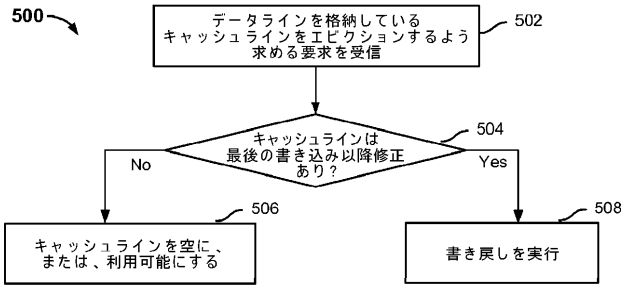
【図３】



【図４】



【図５】



【図６】

トランスレーションライン	IV	PLID	PLID	...	PLID	暗号化コンテンツ
100	259	3	40	...	99	AZ95MKP0
...	...	...	...	...	...	...
502	802	3	40	...	99	MPLLR092
503	243	98	2	...	71	REW10832
...	...	...	...	...	...	...

【図７Ａ】

インデックス	署名	参照カウント	コンテンツ
...	...	...	...
$(A_i\text{-}B_i)/S$	Hash(“hello”)	2	“hello”
$(A_{i+1}\text{-}B_i)/S$	Hash(“world”)	4	“world”
...	...	...	...

【図７Ｂ】

インデックス	署名	参照カウント	コンテンツ
...	...	...	...
$SecHash_1(En(\text{“hello”}))$	$SecHash_2(En(\text{“hello”}))$	En(2)	En(“hello”)
...	...	...	...

【手続補正書】
【提出日】平成28年6月30日(2016.6.30)
【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】
ストレージと、
前記ストレージに結合されているメモリコントローラと
を備え、
前記メモリコントローラは、
前記ストレージにデータコンテンツを書き込むよう求める要求に応じて、前記データコンテンツに少なくとも部分的に基づいて暗号化データコンテンツを生成し、
前記ストレージにおける前記暗号化データコンテンツに対する参照を取得するよう試み、
前記暗号化データコンテンツに対する前記参照を取得した場合、前記ストレージにおける前記暗号化データコンテンツに対する前記参照を参照するようにトランスレーションラインを修正し、
前記暗号化データコンテンツに対する前記参照を取得しなかった場合には、
前記暗号化データコンテンツを新しいロケーションに格納し、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する参照を取得し、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する前記参

照を参照するよう前記トランスレーションラインを修正する
セキュアシステム。
【請求項２】
前記ストレージは、メインメモリ、セカンダリストレージまたは両方を有する
請求項１に記載のセキュアシステム。
【請求項３】
前記メモリコントローラは、確定的暗号化関数を実行して前記暗号化データコンテンツを生成する
請求項１または２に記載のセキュアシステム。
【請求項４】
前記メモリコントローラは、アドバンスド・エンクリプション・スタンダード（ＡＥＳ）、ＥＣＢ－Ｍｉｘ－ＥＣＢ（ＥＭＥ）、ＸＥＸ－ＴＣＢ－ＣＴＳ（ＸＴＳ）およびＣＢＣ－Ｍａｓｋ－ＣＢＣ（ＣＭＣ）のうち１または複数を実施する
請求項１から３のいずれか一項に記載のセキュアシステム。
【請求項５】
前記メモリコントローラに結合されているキャッシュをさらに備え、
前記キャッシュは暗号化されていないデータを格納する
請求項１から４のいずれか一項に記載のセキュアシステム。
【請求項６】
前記メモリコントローラに結合されているキャッシュをさらに備え、
前記キャッシュは重複排除されたデータを格納する
請求項１から５のいずれか一項に記載のセキュアシステム。
【請求項７】
前記メモリコントローラに結合されているキャッシュをさらに備え、
前記メモリコントローラはさらに、キャッシュミスの場合にセキュアパッドを生成して、前記セキュアパッドを用いて前記ストレージからフェッチされる暗号化データを復号化する
請求項１から６のいずれか一項に記載のセキュアシステム。
【請求項８】
前記メモリコントローラに結合されているキャッシュをさらに備え、
前記メモリコントローラはさらに、
読み出しロケーションにあるデータコンテンツへアクセスするよう求める要求に応じて、前記読み出しロケーションに対応するトランスレーションラインおよびデータラインが前記キャッシュにおいて利用可能であるか否かを判断し、
前記データラインが前記キャッシュにおいて利用可能でない場合、
前記データラインを前記ストレージからロードし、
前記データラインを復号化して、
前記復号化の結果を前記キャッシュに保存する
請求項１から７のいずれか一項に記載のセキュアシステム。
【請求項９】
前記メモリコントローラに結合されているキャッシュをさらに備え、
前記データコンテンツを書き込むよう求める要求は、前記データコンテンツを格納しているキャッシュラインをエビクションするよう求める要求によって発生し、前記キャッシュラインは、最後に前記ストレージに書き込まれた後修正されている
請求項１から８のいずれか一項に記載のセキュアシステム。
【請求項１０】
前記データコンテンツを書き込むよう求める要求を生成するプロセッサをさらに備え、
前記プロセッサのアドレス空間は、複数の重複排除ドメインを含み、
各重複排除ドメインは、前記各重複排除ドメインにおけるデータコンテンツを暗号化するために用いられる対応する鍵を持つ

請求項１から９のいずれか一項に記載のセキュアシステム。
【請求項１１】
前記トランスレーションラインは暗号化されている
請求項１から１０のいずれか一項に記載のセキュアシステム。
【請求項１２】
前記トランスレーションラインは暗号化されており、
前記データコンテンツおよび前記トランスレーションラインは複数の異なる鍵を用いて暗号化されている
請求項１から１１のいずれか一項に記載のセキュアシステム。
【請求項１３】
前記ストレージにおける前記暗号化データコンテンツに対する前記参照を取得するよう試みることは、コンテンツディレクトリにおいて前記暗号化データコンテンツを検索することを含む
請求項１から１２のいずれか一項に記載のセキュアシステム。
【請求項１４】
前記ストレージにおける前記暗号化データコンテンツに対する前記参照を取得するよう試みることは、コンテンツディレクトリにおいて前記暗号化データコンテンツを検索することを含み、
前記コンテンツディレクトリは暗号化メタデータを含む
請求項１から１２のいずれか一項に記載のセキュアシステム。
【請求項１５】
前記暗号化メタデータは、前記コンテンツディレクトリを共有している複数の保護ドメインの間で共有されている共通鍵を用いて暗号化される
請求項１４に記載のセキュアシステム。
【請求項１６】
書き込み処理の完了指示は、前記書き込み処理を実行するために用いられる指定所要時間を変更するよう修正される
請求項１から１５のいずれか一項に記載のセキュアシステム。
【請求項１７】
データラインへの読み出しアクセスの場合、前記メモリコントローラはさらにインテグリティチェックを実行し、前記インテグリティチェックは、前記データラインのデータコンテンツが前記データラインに対応付けられているメタデータに一致するか否かを判断することを含む
請求項１から１６のいずれか一項に記載のセキュアシステム。
【請求項１８】
前記データラインの前記データコンテンツが前記データラインに対応付けられている前記メタデータに一致しない場合、セキュリティ侵害の可能性が報告される
請求項１７に記載のセキュアシステム。
【請求項１９】
前記データラインに対応付けられている前記メタデータは、セキュアな鍵付きハッシュ関数を用いて生成される
請求項１７または１８に記載のセキュアシステム。
【請求項２０】
前記ストレージは、レイテンシが異なる複数のメモリを含むハイブリッドメモリを有する
請求項１から１９のいずれか一項に記載のセキュアシステム。
【請求項２１】
前記ストレージは、レイテンシが異なる複数のメモリを含むハイブリッドメモリを有し、
低レイテンシメモリの暗号化の単位は、高レイテンシメモリの暗号化の単位とはサイズ

が異なる
請求項１から１９のいずれか一項に記載のセキュアシステム。
【請求項２２】
前記ストレージは、同じデータコンテンツを持つ複数のデータラインの暗号化の結果が異なるオーバーフローエリアを含む
請求項１から２１のいずれか一項に記載のセキュアシステム。
【請求項２３】
ストレージにデータコンテンツを書き込むよう求める要求に応じて、前記データコンテンツに基づいて暗号化データコンテンツを生成する段階と、
前記ストレージにおける前記暗号化データコンテンツに対する参照を取得するよう試みる段階と、
前記暗号化データコンテンツに対する前記参照を取得した場合、前記ストレージにおける前記暗号化データコンテンツに対する前記参照を参照するようにトランスレーションラインを修正する段階と、
前記暗号化データコンテンツに対する前記参照を取得しなかった場合には、
前記暗号化データコンテンツを新しいロケーションに格納する段階と、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する参照を取得する段階と、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する前記参照を参照するよう前記トランスレーションラインを修正する段階と
を備える方法。
【請求項２４】
データセキュリティを実現するためのプログラムであって、実行されることに応じてコンピュータに、
ストレージにデータコンテンツを書き込むよう求める要求に応じて、前記データコンテンツに基づいて暗号化データコンテンツを生成させ、
前記ストレージにおける前記暗号化データコンテンツに対する参照を取得するよう試みさせ、
前記暗号化データコンテンツに対する前記参照を取得した場合、前記ストレージにおける前記暗号化データコンテンツに対する前記参照を参照するようにトランスレーションラインを修正させ、
前記暗号化データコンテンツに対する前記参照を取得しなかった場合には、
前記暗号化データコンテンツを新しいロケーションに格納させ、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する参照を取得させ、
前記新しいロケーションに格納されている前記暗号化データコンテンツに対する前記参照を参照するよう前記トランスレーションラインを修正させる
プログラム。
【請求項２５】
請求項２４に記載のプログラムを格納するコンピュータ可読記憶媒体。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/011341

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/62 G06F21/78 G06F3/06 G06F17/30
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/313040 A1 (LUMB CHRISTOPHER R [US]) 9 December 2010 (2010-12-09) paragraph [0029] - paragraph [0047] paragraph [0065] - paragraph [0075] figures 1,4,10,12B,13A,13B -----	1-24
A	US 2009/268903 A1 (BOJINOV HRISTO [US] ET AL) 29 October 2009 (2009-10-29) paragraphs [0036], [0041] - paragraph [0054] paragraph [0092] - paragraph [0096] figures 9A,9B -----	1-24
	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 March 2015	08/04/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Cartrysse, Kathy

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/011341

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2012/166401 A1 (LI JIN [US] ET AL) 28 June 2012 (2012-06-28) paragraph [0024] - paragraph [0057] paragraph [0092] - paragraph [0096] figures 9A,9B figures 1,5	1-24
A	US 2011/238634 A1 (KOBARA MAKOTO [JP]) 29 September 2011 (2011-09-29) paragraph [0041] - paragraph [0088] figures 5,6	1-24
A	EP 1 299 971 B1 (MICROSOFT CORP [US]) 9 April 2003 (2003-04-09) paragraph [0029] - paragraph [0057]	1

2

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/011341

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010313040 A1	09-12-2010	US 2010313040 A1	09-12-2010
		US 2014325216 A1	30-10-2014
US 2009268903 A1	29-10-2009	US 2009268903 A1	29-10-2009
		WO 2009132144 A2	29-10-2009
US 2012166401 A1	28-06-2012	CN 102591946 A	18-07-2012
		EP 2659376 A2	06-11-2013
		US 2012166401 A1	28-06-2012
		WO 2012092212 A2	05-07-2012
US 2011238634 A1	29-09-2011	JP 4892072 B2	07-03-2012
		JP 2011203842 A	13-10-2011
		US 2011238634 A1	29-09-2011
EP 1299971 B1	09-04-2003	AT 487297 T	15-11-2010
		AU 9520801 A	20-11-2001
		EP 1299971 A2	09-04-2003
		US 6983365 B1	03-01-2006
		US 2004215962 A1	28-10-2004
		US 2004221159 A1	04-11-2004
		US 2004221160 A1	04-11-2004
		US 2005229012 A1	13-10-2005
		US 2005235146 A1	20-10-2005
		WO 0186396 A2	15-11-2001

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US