インテル® SGX 命令とデータ構造の概要

この記事は、インテル® デベロッパー・ゾーンに公開されている「Overview of Intel Software Guard Extensions Instructions and Data Structures」の日本語参考訳です。

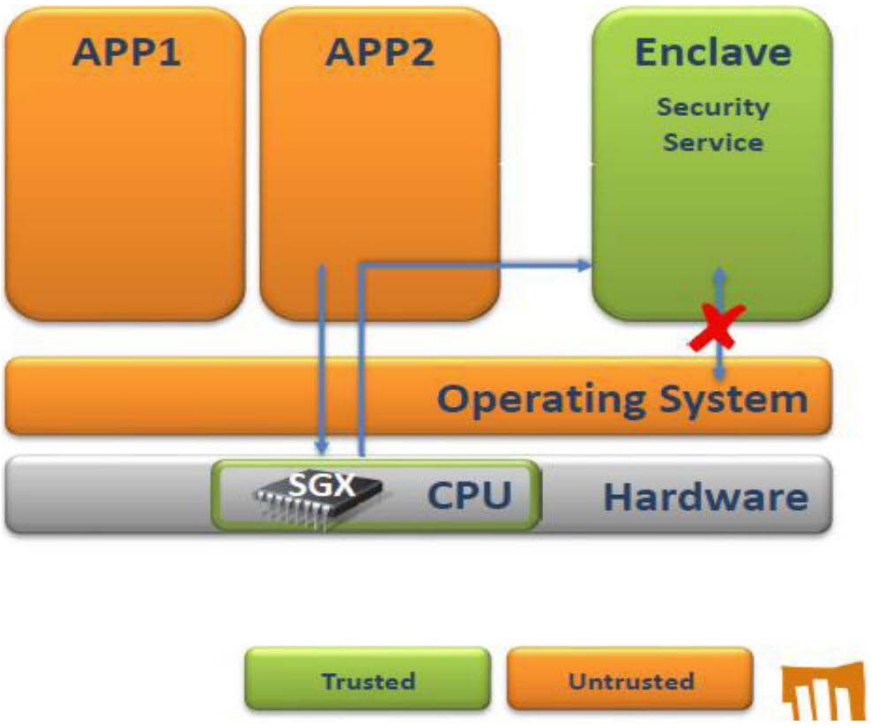
この記事では、インテル® ソフトウェア・ガード・エクステンション (インテル® SGX) 命令とデータ構造に関する情報を開発者に紹介します。インテル® SGX には 18 種類の命令があり、13 のデータ構造を利用できます。

以下のトピックがあります。

1. インテル® SGX
2. 基本 - リングの分離
3. インテル® SGX 命令とデータ構造
4. インテル® SGX メモリーアクセス制御
5. インテル® SGX 制御構造アクセス

インテル® SGX:

- **セキュリティー的に重要なコードを保護領域に分離します。**
- **CPU のみ信頼します。**
  - 透過的なメモリー暗号化
  - 18 の新しい命令
- **保護領域はシステムに影響を与えることはありません。**
  - 非特権コード (CPU リング 3) のみ
  - メモリー保護
- **マルチコアシステム向けに設計されています。**
  - 保護領域のマルチスレッド実行
  - 保護領域および信頼されていないコードの並列実行
  - 保護領域は割り込み可能
- **プログラミング・リファレンスが用意されています。**



基本 - リングの分離:

- **4 つの異なる特権レベルがあります。**
  - **0 = カーネル**
  - **1、2 = デバイスドライバー**
  - **3 = アプリケーション**
- **現在の特権レベルは CPU によりコード・セグメント・レジスター CS で管理されます。**

インテル® SGX 保護領域:

- **保護領域はコードとデータの分離されたメモリー領域です。**
- **物理メモリー (RAM) の一部は保護領域向けに予約されます。**
  - 予約された部分は**保護領域ページキャッシュ (EPC)** と呼ばれます。
  - EPC メモリーはメインメモリー (RAM) で暗号化されます。
  - 信頼されるハードウェアは CPU ダイのみで構成されます。
  - EPC は OS/VMM により管理されます。

インテル® SGX 命令とデータ構造:

- **18 の命令**
  - 13 のスーパーバイザー命令
  - 5 つのユーザー命令
- **13 のデータ構造**
  - 8 つのデータ構造は特定の保護領域に関連付けられます。
  - 3 つのデータ構造は特定のメモリーページに関連付けられます。
  - 2 つのデータ構造は全体的なリソース管理に関連付けられます。

インテル® SGX スーパーバイザー命令:

スーパーバイザー命令	**説明**
ENCLS[EADD]	ページを追加します。
ENCLS[EBLOCK]	EPC ページをブロックします。
ENCLS[ECREATE]	保護領域を作成します。
ENCLS[EDBGRD]	デバッガーでデータを読み取ります。
ENCLS[EDBGWR]	デバッガーでデータを書き込みます。
ENCLS[EEXTEND]	EPC ページ測定を拡張します。
ENCLS[EINIT]	保護領域を初期化します。
ENCLS[ELDB]	EPC ページをブロックとしてロードします。
ENCLS[ELDU]	EPC ページを非ブロックとしてロードします。
ENCLS[EPA]	バージョン配列を追加します。
ENCLS[EREMOVE]	EPC からページを削除します。
ENCLS[ETRACK]	EBLOCK チェックを有効にします。
ENCLS[EWB]	EPC ページをライトバック/無効化します。

インテル® SGX ユーザー命令:

ユーザー命令	説明
ENCLU[EENTER]	保護領域に入ります。
ENCLU[EEXIT]	保護領域を出ます。
ENCLU[EGETKEY]	暗号鍵を作成します。
ENCLU[EREPORT]	暗号レポートを作成します。
ENCLU[ERESUME]	保護領域に再度入ります。

インテル® SGX データ構造詳細:

1. **インテル® SGX 保護領域制御構造 (SECS):**
    - 1 つの保護領域を表します。
    - 例えば、ハッシュ、ID、サイズなどを含みます。
2. **スレッド制御構造 (TCS):**
    - 保護領域の各実行スレッドは、スレッド制御構造と関連付けられます。
    - 例えば、エントリーポイント、SSA へのポインターを含みます。
3. **ステート保存エリア (SSA):**
    - 保護領域で実行中に AEX が発生した場合、アーキテクチャー・ステートはスレッドの SSA に保存されます。
4. **ページ情報 (PAGEINFO):**
    - PAGEINFO は、EPC 管理命令のパラメーターとして使用されるアーキテクチャー・データ構造です。
        - リニアアドレス
        - ページの有効アドレス (仮想アドレス)
        - SECINFO
        - SECS
5. **セキュリティー情報 (SECINFO):**
    - SECINFO データ構造は、保護領域ページに関するメタデータを保持します。
        - 読み取り/書き込み/実行
        - ページタイプ (SECS、TCS、通常ページまたは VA)
6. **ページング暗号化メタデータ (PCMD):**
    - PCMD 構造は、ページアウトされたページと関連する暗号化メタデータを保持するために使用されます。PAGEINFO と組み合わせて、ページアウトされた EPC ページの確認、復号化、リロードに必要な情報をプロセッサーに提供します。
    - EWB は、(予約されたフィールドと) MAC 値を書き込みます。
    - ELDB/U は、フィールドを読み取り、MAC をチェックします。
    - 保護領域 ID、SECINFO および MAC を含みます。
7. **バージョン配列 (VA):**
    - 退避された EPC ページのバージョンを安全に格納するため、インテル® SGX はバージョン配列 (VA) と呼ばれる特別な EPC ページタイプを定義します。
        - 各 VA ページは 512 のスロットを含みます。各スロットは EPC から退避されたページの 8 バイトのバージョン番号を含みます。
    - EPC ページが退避されると、ソフトウェアは VA ページの空のスロットを選択します。このスロットは、退避されているページの固有のバージョン番号を受け取ります。
        - EPC がリロードされた場合、VA スロットはページのバージョンを保持する必要があります。ページが正常にリロードされると、VA スロットのバージョンはクリアされます。
    - VA ページは、ほかの EPC ページのように退避できます。
        - VA ページを退避する場合、ほかの VA ページのバージョンスロットを使用して、退避している VA のバージョンを受け取る必要があります。

1. **保護領域ページ・キャッシュ・マップ (EPCM):**
    - EPCM は、EPC のコンテンツを追跡するためプロセッサーにより使用されるセキュア構造です。EPCM は、EPC に現在ロードされている各ページについて 1 つのエントリーのみ保持します。EPCM はソフトウェアによりアクセスできません。EPCM フィールドのレイアウトは実装固有です。
    - 例えば、RWX、ページタイプ、リニアアドレス、ステートなどを含みます。
2. **保護領域署名構造 (SIGSTRUCT):**
    - SIGSTRUCT は、保護領域の署名者からの保護領域に関する情報を含みます。
    - SIGSTRUCT は、SHA256 として ENCLAVEHASH を含みます。
    - SIGSTRUCT は、4 つの 3072 ビット整数 (MODULUS、SIGNATURE、Q1、Q2) を含みます。
3. **EINIT トークン構造 (EINITTOKEN):**
    - EINIT トークンは、保護領域が起動を許可されていることを確認するため EINIT により使用されます。
    - 例えば、保護領域の属性、ハッシュおよび署名者を含みます。
    - 起動鍵を使用する EINITTOKEN の暗号化 MAC で認証されます。
4. **レポート (REPORT):**
    - REPORT 構造は EREPORT 命令の出力です。
        - 保護領域の属性
        - 保護領域のハッシュ
        - 保護領域の署名者
        - 保護領域とターゲット保護領域間の通信に使用されるデータのセット
        - レポート鍵を使用したレポートの CMAC
5. **レポートターゲット情報 (TARGETINFO):**
    - この構造は、EREPORT 命令の入力パラメーターです。EREPORT により返された REPORT 構造を暗号的に確認できる保護領域を識別するために使用されます。
    - ターゲット保護領域の属性およびハッシュを含みます。
6. **鍵リクエスト (KEYREQUEST):**
    - この構造は、EGETKEY 命令の入力パラメーターです。
    - 適切な鍵およびその鍵の派生に必要な追加パラメーターを選択するために使用されます。

インテル® SGX メモリーアクセス制御:

2 方向のアクセス制御

1. **保護領域から「外部」**
    - 悪意のある保護領域を分離します。
    - 保護領域は外部 (例えば、「ホスト・アプリケーション」) と通信する手段が必要です。
2. **「外部」から保護領域**
    - 保護領域メモリーは以下から保護する必要があります。
        - アプリケーション
        - 特権レベルの高いソフトウェア (OS/仮想マシンモニター (ハイパーバイザー))
        - その他の保護領域

インテル® SGX MAC 保護領域から「外部」:

保護領域から「外部」

- すべてのメモリーアクセスは、OS/VMM によるセグメンテーションとページングポリシーを満たす必要があります。
- 保護領域はそれらのポリシーを操作できません。保護領域の内部の非特権命令のみ操作できます。
- 保護領域の内部から保護領域の外部のリニアアドレスにフェッチを行うと一般保護違反 (0) が発生します。

インテル® SGX MAC「外部」から保護領域:
「外部」から保護領域

- EPC メモリーへの非保護領域アクセスはアボート・ページ・セマンティクスを引き起こします。
- 外部から保護領域にマップするリニアアドレスへの直接ジャンプは保護領域モードを有効にせず、アボート・ページ・セマンティクスおよび未定義の動作を引き起こします。
- ハードウェアは、オリジナルの直接 EA がページの割り当てに使用した変換と異なる論理-リニアアドレス変換を使用した保護領域アクセスを検出して防ぎます。変更された変換が検出されると一般保護違反 (0) が発生します。

インテル® SGX 制御構造アクセス:
インテル® SGX 制御構造は直接アクセス不可

- すべての EPC ページにはタイプ (SECS、TCS、通常ページまたは VA) があります。
- 保護領域の外部からはアクセスできません。
- 「通常ページ」のみ保護領域の内部からアクセスできます。
- SECS、TCS および VA は、ハードウェアにより初期化され操作されます。

インテル® SGX に関する情報は、こちらでご覧いただけます。

コンパイラーの最適化に関する詳細は、最適化に関する注意事項を参照してください。