CodeGuard ™中間セキュリティ

本セクションには以下の主要項目を記載しています。

1.0 はじめに

CodeGuard™ 中間セキュリティは、フラッシュ プログラムメモリに格納された知的財産に不変性とアクセス制御を提供します。本機能は、1 つのデバイス上で複数の作成者によるコード作成、セキュアな書き換え不可のブート、セキュアなフィールド アップデート等の幅広いシステム セキュリティ ユースケースに合わせて構成できます。デュアルブート プログラムメモリ採用デバイスでは、これらの機能を使う事でさらなるセキュリティ機能の拡張も可能です。

デバイスのタイプによっては、フラッシュ プログラムメモリを複数 (最大 4 つ) のコード空間セグメントに分割して構成できます。これらの各セグメントには、暗黙的にセキュリティ権限レベルとシステム機能が設定されます。コードまたはデータ内容の発見や読み出しを可能にする恐れのある全てのシステム動作は、その動作の起動元セグメントまたは対象セグメントが持つセキュリティ権限に応じて制限されます。これには以下が含まれます。

- プログラミング、消去、ベリファイ動作
- コード空間の読み出しと書き込み
- セキュア セグメント外からセキュア セグメント内へのプログラムフロー変更
- セキュア セグメント内への割り込みベクタ

CodeGuard 中間セキュリティ機能はフラッシュプログラムメモリ空間にのみ適用されます。データメモリは制限を受けず、どのコードセグメントからも自由にアクセスできます。

2.0 制御レジスタ

プログラムコード セキュリティ機能は、デバイス起動時に全てデバイス コンフィグレーション ビットで制御します。これらのビットの格納場所は、デバイスファミリごとに異なります。大部分の dsPIC33 および PIC24 デバイスのコンフィグレーション ビットは、FSEC および FBSLIM フラッシュ コンフィグレーション レジスタに格納されています。デバイスファミリ固有の詳細は各デバイスのデータシートを参照してください。

ここでは、以下のコンフィグレーション ビットについて説明します。

- CSS<2:0>(コンフィグレーション セグメント セキュリティ コンフィグレーション)
- CWRP(コンフィグレーション セグメント書き込み保護)
- BSEN(ブートセグメント イネーブル)
- BSS<1:0>(ブートセグメント セキュリティ コンフィグレーション)
- BWRP(ブートセグメント書き込み保護)
- GSS<1:0>(汎用セグメント セキュリティ コンフィグレーション)
- GWRP(汎用セグメント書き込み保護)
- AIVTDIS(代替 IVT ディセーブル)
- BSLIM<12:0>(ブートセグメント制限値)

デュアルブート プログラムメモリを備えるデバイスでは、BTMOD<1:0> ビット (通常 FBOOT コンフィグレーション レジスタ内) でも、選択したブートモードに応じて CodeGuard セキュリティ機能の挙動を変更できます。

3.0 コードセグメントの構成

フラッシュ プログラムメモリは複数のセグメントに分割され、各セグメントは専用のコード保護 (CP) および書き込み保護 (WRP) 設定を持ちます。必要に応じて、ブートセグメント (BS) を定義して汎用セグメント (GS) から切り離す事もできます。複数セグメントに分割する事で、全タイプのアクセスと動作に対してセグメント間の制限が可能になり、チェーンオブ トラストを実現できます。デュアルブート モードで動作する場合、アクティブ パーティションと非アクティブ パーティションの間でもコードセグメントが制限されます。

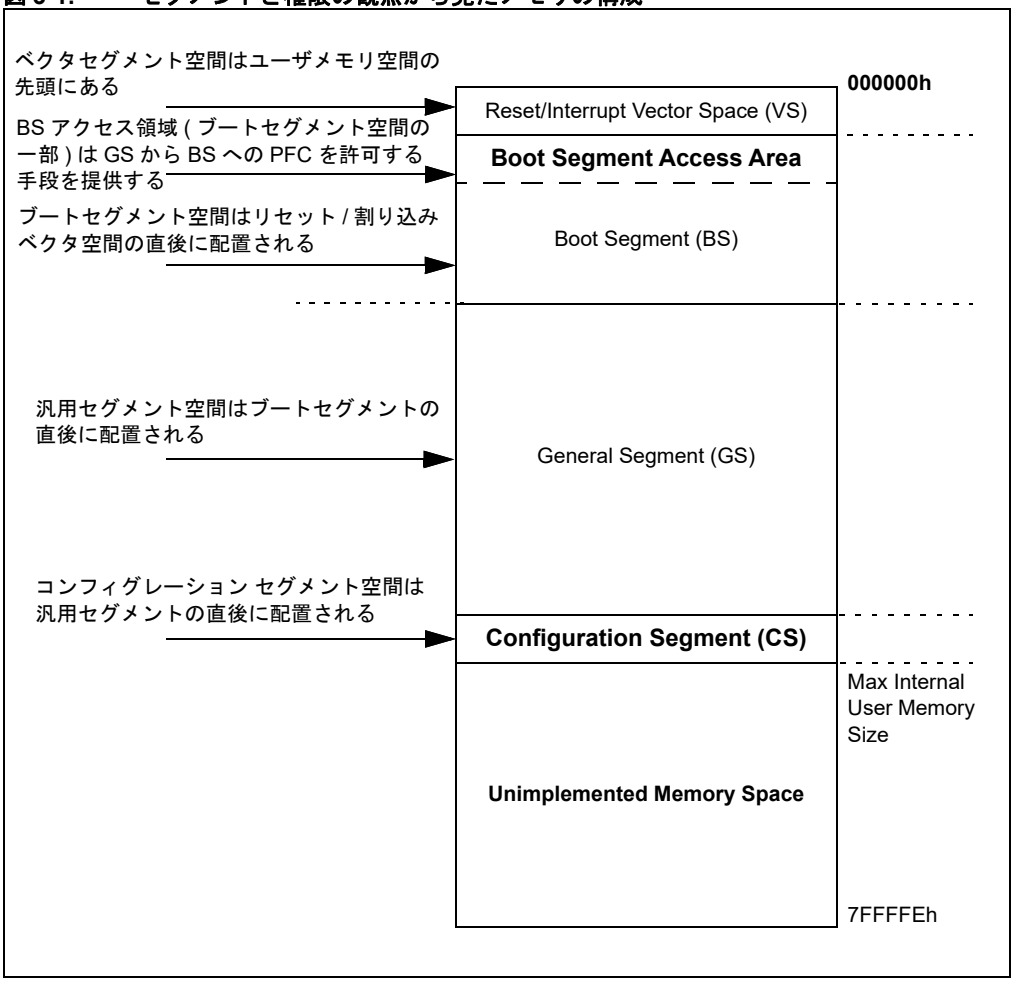
3.1 コード保護ビット

各セグメントの個別のコード保護機能は、ユーザ プログラムメモリの末尾に位置するフラッシュ コンフィグレーション ビットで設定します。これには、セキュリティ レベル (BSS、GSS、または CSS) を定義するコード保護 (CP) ビットと、特定のセグメントに対する全ての書き込み動作をブロックする書き込み保護 (WRP) ビットが含まれます。これらのコンフィグレーション ビットは、その他の全てのフラッシュ コンフィグレーション ビットと同様、既定値でセット (= 1) されており、個々のビットを書き込む事でクリア (= 0) されます。

他のフラッシュ コンフィグレーション ビットとは異なり、コード保護ビットは書き込みのみ可能です。CP ビットの消去 (「0」から「1」へ) はできません。コード保護ビットを消去するには、チップ消去、非アクティブ パーティション消去か、コンフィグレーション セグメント ページを対象としたページ消去 (既存のコード保護値で許可されている場合) のどちらかを使って全コード保護ビットを消去してコード保護を削除する必要があります。

開発段階では、コード保護を有効にするとデバッグモードへの移行が抑止される可能性があります。そのため、デバッグモードに移行する前にコード保護を無効にする必要があります。

図 3-1: セグメントと権限の観点から見たメモリの構成



3.2 ブートセグメント (BS)

ブートセグメント (BS) は、同一デバイスまたは外部インターフェイス上で実行される他のコードから保護する必要があるブートローダ コードまたはその他の知的財産のための高度にセキュアなコード空間を提供します。ブートセグメント内のブートコードは不変である事が重要です。なぜなら、ブートコードに干渉された場合、チェーンオブ トラストを変更または排除し得る攻撃にシステムをさらす可能性があるからです。そのため、ブートセグメントは他のセグメントより高いセキュリティ権限を持っており、他のセグメントへのアクセスもできます。ブートセグメント書き込み保護を有効にしない場合、ブートセグメントは自身の領域を書き換える事ができ、使い捨て鍵の保存と更新が可能になります。

3.2.1 BS の割り当て

ブートセグメントを作成するには、BSENコンフィグレーション ビットを書き込み(= 0)、BSLIMxコンフィグレーション ビット(FBSLIM<12:0>)で0より大きいページサイズを定義します。BSLIMxビットの値はブートセグメント ページ数を反転した値です。これは、ビットをクリアして現在のブートセグメントのサイズが小さくなるのを防ぐためです。ブートセグメントのサイズが小さくなると、既存のブートコードが実質的に低いセキュリティの汎用セグメント内に配置されてしまいます。

BSLIMx ビットはコード保護ビットと同様に書き込み専用で、「ライトワンス」ビットでもあります。リセット シーケンス中にフラッシュから読み込んだ値が消去されていない (全て「1」) 場合、FBSLIM はプログラミングできません。ライトワンス以降、試行しても失敗し、何も影響を与えません。

3.2.2 セキュリティ レベルの選択

ブートセグメントのセキュリティ レベルは BWRP および BSS<1:0> コンフィグレーション ビットを使って設定します。このセキュリティ レベルを使って他のセグメントからブートセグメントへのアクセスを制限します。セキュリティ レベルを 3 通りに設定可能なデバイスでは、2 つのセキュリティ レベル (標準 / 高) と「保護なし」のいずれかを選択できます。詳細は**セクション 4.1「プログラムフローに関する規則」**を参照してください。

図 3-2: ブートセグメントの割り当て

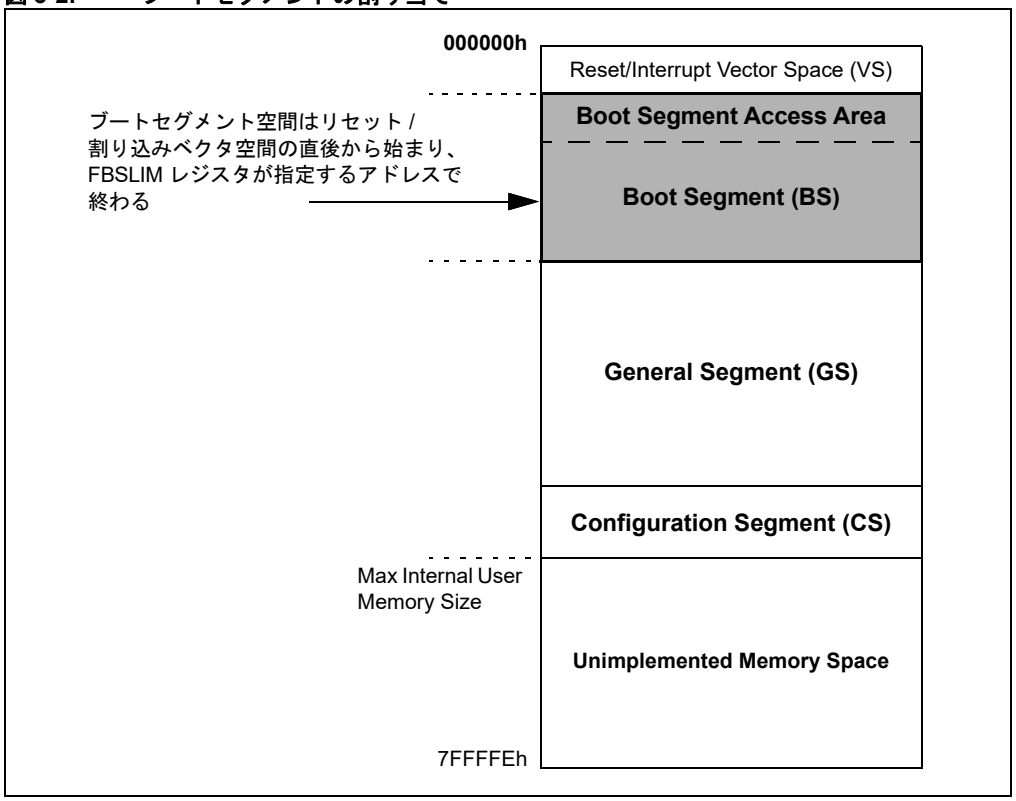


表 3-1:　　ブートセグメントの設定オプション

BSEN	BSS<1:0>	セキュリティ レベル
1	xx	ブートセグメントを定義しない
0	11	セキュリティなし (オプションの書き込み保護以外)
0	10	標準セキュリティ
0	0x	高セキュリティ

3.3　汎用セグメント (GS)

汎用セグメント (GS) のセキュリティ権限レベルはブートセグメントよりも低くなります。通常、汎用セグメントはアプリケーション コードの大部分を格納します。汎用セグメントは、ベクタセグメントまたはブートセグメント (ブートセグメント実装時) の後のページ境界から始まります。

3.3.1　GS のセキュリティ レベル

汎用セグメントのセキュリティ レベルは最大 3 通りに設定できます (何通りに設定できるかはデバイスによって異なります)。汎用セグメントの保護レベルは、コンフィグレーション ビット GSS<1:0> で指定します (表 3-2 参照)。セキュリティ レベルを 3 通りに設定可能なデバイスでは、2 つのセキュリティ レベル (標準 / 高) と「保護なし」のいずれかを選択できます。詳細は**セクション 4.1「プログラムフローに関する規則」**を参照してください。

3.3.2　GS の書き込み保護

コンフィグレーション ビット GWRP をプログラムする事により、汎用セグメントにもブートセグメントと同様の書き込み保護を設定できます。このビットが未プログラム状態 (「1」) の場合、書き込み保護は無効です。汎用セグメントの書き込み保護を有効にするには、このビットをプログラムする必要があります。

図 3-3:　　汎用セグメントの割り当て

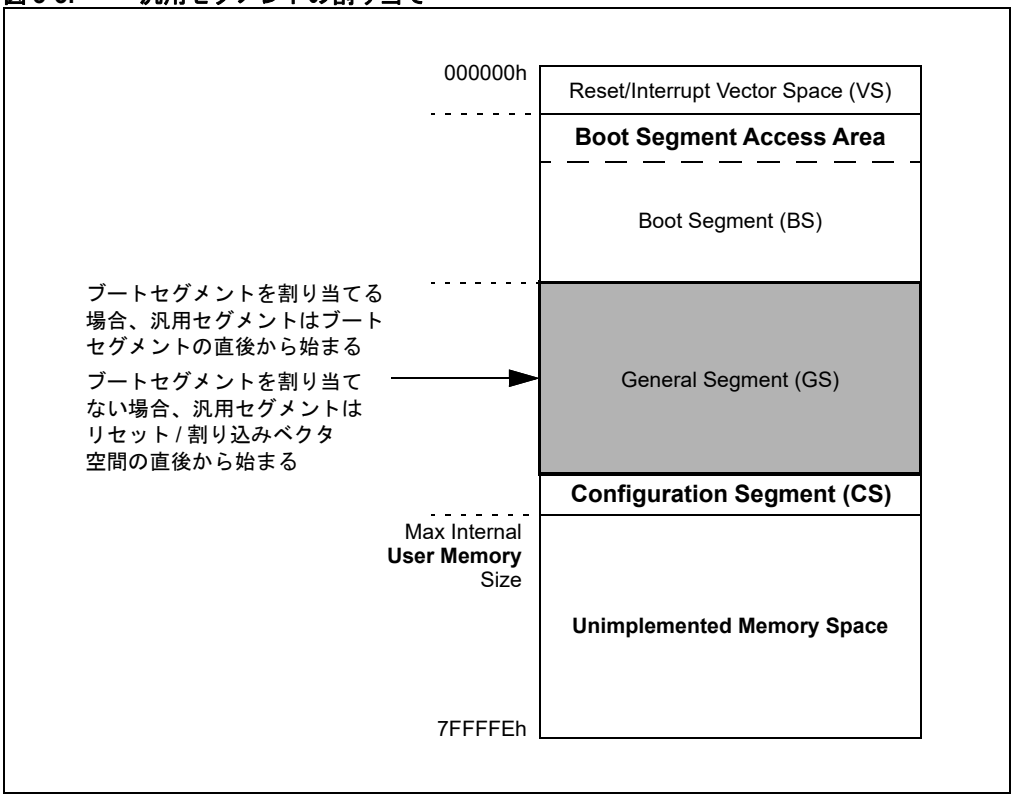


表 3-2:　汎用セグメントの設定オプション

GSS<1:0>	セキュリティ レベル
11	セキュリティなし (オプションの書き込み保護以外)
10	標準セキュリティ
0x	高セキュリティ

3.4　コンフィグレーション セグメント (CS)

コンフィグレーション セグメント (CS) は、実装されたプログラムメモリの最後のページに配置されています。コンフィグレーション セグメントは全てのコンフィグレーション データをフラッシュ プログラムメモリに保持しています。リセット シーケンス中、コンフィグレーションデータは自動的に読み出され、デバイスのコンフィグレーション レジスタに書き込まれます。コンフィグレーション セグメントは、単独ではコードを実行しません。そのため、ブートセグメントまたは汎用セグメントのような特殊な権限レベルを持ちません。しかし、汎用セグメントとブートセグメントから独立したセキュリティと書き込み保護を実装しています。

3.4.1　CS のセキュリティ レベル

セキュリティ レベルは、CSS<2:0> コンフィグレーション ビットで 4 つのレベルのうちの 1 つに設定します (表 3-3 参照)。コンフィグレーション セグメントは、デバイスのセキュリティと書き込み保護に重要なデータを収めているため、他のプログラムメモリ アクセスから独立してページ消去動作を柔軟に制御できるように拡張セキュリティ レベルを備えています。詳細は**セクション 4.1「プログラムフローに関する規則」**を参照してください。

3.4.2　CS の書き込み保護

コンフィグレーション ビット CWRP をプログラムする事により、コンフィグレーション セグメントにもブートセグメントと同様の書き込み保護を設定できます。このビットが未プログラム状態 (「1」) の場合、書き込み保護は無効です。コンフィグレーション セグメントの書き込み保護を有効にするには、このビットをプログラムする必要があります。

図 3-4:　コンフィグレーション セグメントの割り当て

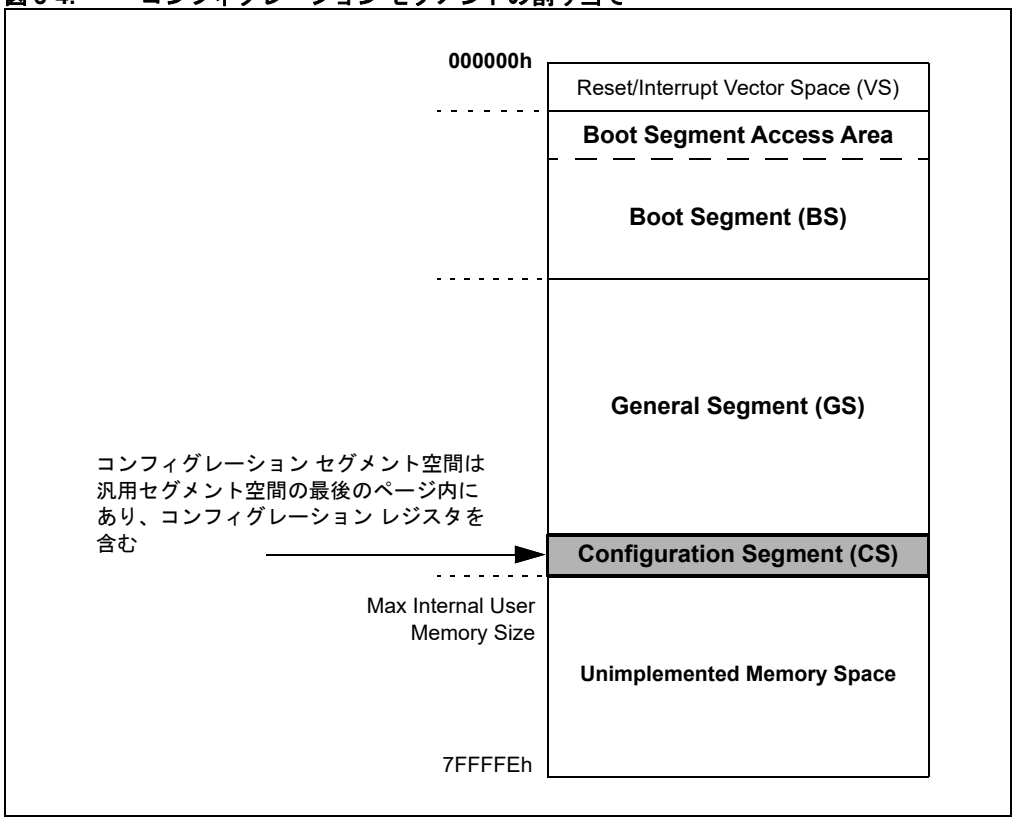


表 3-3: コンフィグレーション セグメントの設定オプション

CSS<2:0>	セキュリティ レベル
111	セキュリティなし (オプションの書き込み保護以外)
110	標準セキュリティ
10x	拡張セキュリティ
0xx	高セキュリティ

3.5 ベクタセグメント (VS)

ベクタセグメント (VS) はリセット、トラップ、割り込みサービスルーチン (ISR) ベクタを格納します。PIC24 デバイスではフラッシュメモリの先頭の 256 命令ワードであり、dsPIC33 デバイスでは先頭の 512 命令ワードです。ブートセグメントが定義されている場合、AIVT(代替割り込みベクタテーブル) を使う事もできます。コンフィグレーション セグメント同様、ベクタセグメントは単独ではコードを実行しません。そのため、その他のセグメントのような特殊な権限レベルは持ちません。

ベクタセグメントの保護は、ブートセグメントまたは汎用セグメントのセキュリティ設定の状態によって決まります。ブートセグメントが定義されている場合、ベクタセグメントのセキュリティレベルと書き込み保護レベルはブートセグメントと同じです。ブートセグメントが定義されていない場合、ベクタセグメントのセキュリティ レベルと書き込み保護レベルは汎用セグメントと同じです。

Note: 「高」セキュリティに設定した場合、VS は変更できます。そのため、フィールドアップデート中に IVT と AIVT のプログラミングが可能です。アクセス条件は**セクション 4.0「セキュリティ権限と規則」**を参照してください。

3.5.1 AIVT(代替割り込みベクタテーブル)

CodeGuard 中間セキュリティを備えたデバイスは、ブートセグメント内に 2 つ代替 IVT (AIVT) を実装できます。AIVT は、AIVTDIS コンフィグレーション ビットをプログラミングする事で有効にできます。AIVT をサポートするには、ブートセグメントのサイズは 2 ページ (1 ページは IVT と BS 用、もう 1 ページは AIVT 用) 以上に設定する必要があります。AIVT は、BSLIMx コンフィグレーション ビットで定義するブートセグメントの最後のページに格納されます。AIVT を有効にすると、ユーザは AIVTEN 制御ビット (INTCON2<8>) で IVT または AIVT からのベクタに例外を指示できます。

AIVT はブートセグメントのセキュリティ設定を受け継ぎます。ブートセグメント コード保護が「高」セキュリティに設定されている場合、実行中にブートセグメント内で発生する全ての割り込みは、ブートセグメント内の 1 つのセキュアベクタ位置 (アドレス : [BS ベースアドレス + 40h]) を指定します。この機能によりブートセグメントは、汎用セグメント内の ISR に実行を許可する前に、ブートセグメント コンテクストとリターンアドレスを保護する事で、チェーンオブトラストを確立できます。詳細は**セクション 4.2「割り込みに関する規則」**を参照してください。

Note: リセットベクタはAIVT内では複製されません。そのため、リセットは常に000000hを指定します。

3.5.2 デュアルブート モードの AIVT に関する注意事項

IVT と AIVT はどちらもアクティブ パーティションから読み出す事ができます。そのため、非アクティブ パーティションのコードを更新する際にセキュリティの問題が生じる可能性があります。この問題に対応するには、AIVTDIS 制御ビットで非アクティブ パーティションの AIVT を無効にします。こうする事で、ブートセグメントのセキュリティをコードに適用し、アクティブパーティションのコードセグメントからのアクセスをブロックできます。その後、セキュアなブートローダのコードは、AIVT がアクティブ パーティションに割り当てられる前に AIVT を有効にできます。

4.0 セキュリティ権限と規則

2 つのコード保護セグメント間の相対的な権限レベルについて理解する事が重要です。動作の中には、対象となるセグメントとの間の相対的な権限の高低によって制限が課されるものがあります。権限が低いセグメントから権限が高いセグメント内のコードにアクセスするには、呼び出しを発行する必要があります。アクセス権に関する規則について以降のセクションで説明します。表 4-1 ～ 表 4-5 に、通常動作時に適用される規則をまとめて示します。

4.1 プログラムフローに関する規則

プログラムフローとは、プログラムメモリ内のプログラム命令を実行する順番を意味します。通常、命令はプログラム カウンタ (PC) のインクリメントに従って順次実行されます。

PFC(プログラムフロー変更) は、分岐命令の結果としてプログラム カウンタがリロードされると発生し、これを使うとプログラムフローを変更できます。これらの分岐命令には呼び出し、ジャンプ、計算型ジャンプ、リターン、サブルーチンからのリターンが含まれます。同じセグメント内の分岐は無制限ですが、よりセキュリティ レベルの高いセグメントへの分岐は制限付き PFC によってのみ可能です。制限付き PFC を使うと、特殊なセグメント アクセス領域を介してよりセキュリティ レベルの高いセグメントへプログラムを分岐できます。

VFC(ベクタフロー変更) は、割り込み要求またはハードウェア例外トラップの結果としてプログラム カウンタがリロードされると発生します。これらは主に割り込みまたはトラップ ベクタです。

意図しない位置にある保護コードにプログラムがジャンプした場合、コード漏洩の検知アルゴリズムの対象になる恐れがあります。このため、権限階層に違反する PFC/VFC 動作は制限されます。同一セグメント内の PFC に制限はありません。ブートセグメントが「高」セキュリティに設定されている場合を除き、あるセグメントから別のセグメントへの PFC/VFC にも制限はありません。ブートセグメントが「高」セキュリティに設定されている場合、セグメント間の PFC/VFC には以下の制限があります。

- ブートセグメント内のコード実行の整合性を確保するため、ユーザはセキュリティ レベルを「高」に設定する事でこのセグメントへのプログラムフローを制限する必要があります。
- 分岐先をセキュア セグメント アクセス領域に限定するために、プログラムフローを制限できます。
- セキュア セグメント アクセス領域はブートセグメントの最初の 32 命令位置です。

図 4-1 に、通常のプログラムフローと制限されたプログラムフローを示します。

ブートセグメント内のコードの所有者は、セグメント アクセス領域からアプリケーション コードの特定部分以外に分岐しないようにする事で、アルゴリズムの漏洩を防止できます。

制限されたメモリ位置をターゲットとした PFC または VFC は、セキュリティ リセットを引き起こします。この場合、デバイスがリセットし、不正な動作を示す IOPUWR (RCON<14>) ステータスビットがセットされます。

このセキュリティ リセットに加えて、全てのデバイスはプログラムフロー チェック機能を内蔵しています。PFC または VFC が未実装のプログラムメモリ空間をターゲットにすると、アドレスエラー トラップが発生します。

リセット位置にある命令を除き、ベクタセグメントからのコード実行は許可されません。そのようなコード実行はアドレスエラー トラップを引き起こします。

4.1.1 非アクティブ パーティションへのフロー変更

デュアルブート モードでは、非アクティブ パーティションのアドレス空間への PFC は不正なアドレスへのフロー変更とみなされます。なぜなら、非アクティブ パーティションのアドレス空間からの実行は許されておらず、不正アドレストラップが発生するためです。

表 4-1: VS(アクティブ パーティション) アクセス規則

ブートセグメント		未定義 (GSS セキュリティ)						定義済み (BSS セキュリティ)					
セグメント セキュリティ レベル		なし		標準		高		なし		標準		高	
書き込み保護		なし	あり	なし	あり	なし	あり	なし	あり	なし	あり	なし	あり
要求動作													
VS の読み出し	BS から	不可						可					
	GS から	可						可					
VS のプログラム / ページ消去	BS から	不可						あり	(1)	あり	(1)	あり	(1)
	GS から	あり	なし	あり	なし	あり	なし	あり	不可				

Note 1: IVT からの動作はできません。AIVT からの動作はできます。

表 4-2: BS(アクティブ パーティション) アクセス規則

セグメント セキュリティ レベル		なし		標準		高	
書き込み保護		不可	可	不可	可	不可	可
要求動作 :							
BS の読み出し	BS から	可				可	
	GS から	可		不可			
BS のプログラム / ページ消去	BS から	可	不可	可	不可	可	不可
	GS から	可	不可				

表 4-3: GS(アクティブ パーティション) アクセス規則

セグメント セキュリティ レベル		なし		標準		高	
書き込み保護		不可	可	不可	可	不可	可
要求動作 :							
GS の読み出し	BS から	可				不可	
	GS から	可					
GS のプログラム / ページ消去	BS から	可 (1)	不可	可 (1)	不可		
	GS から				不可	可	不可

Note 1: GS の最後のページのページ消去は、CSS<2:0> で設定したセキュリティ レベルで定義されます。

表 4-4: CS アクセス規則

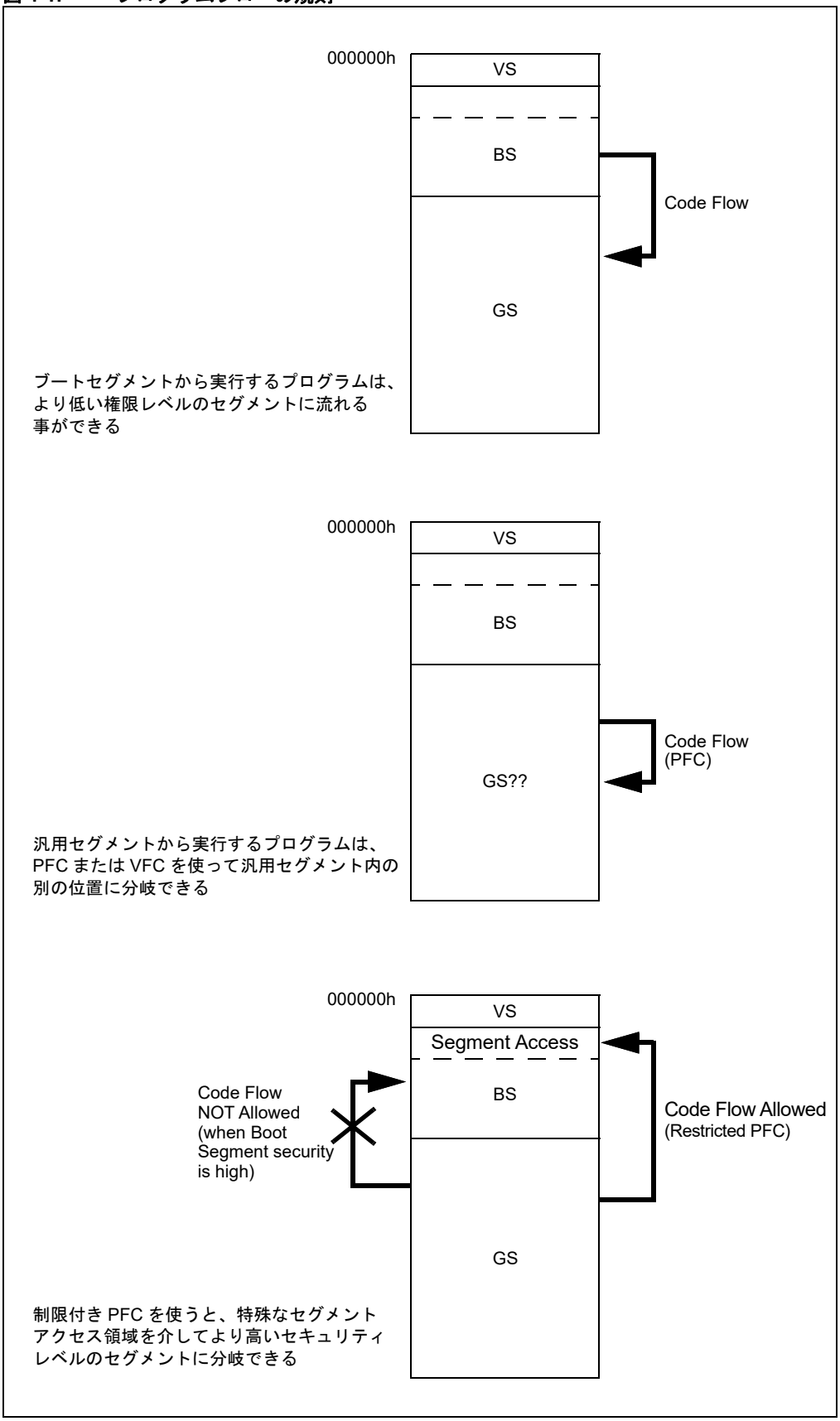
アクティブな CS の セキュリティ レベル		なし		標準		拡張		高	
書き込み保護		不可	可	不可	可	不可	可	不可	可
要求動作 :									
CS の読み出し	BS から	可							
	GS から	可							
CS のプログラム	BS から	可	不可	可	不可	可	不可	可	不可
	GS から				不可				
CS のページ消去	BS から	可	不可	可	不可	可	不可		
	GS から		不可						

表 4-5: パーティション消去規則

要求動作	セグメント	
	BS から	GS から
チップ消去 (アクティブ パーティション)[(1)]	不可	不可

Note 1: チップ消去は全てのユーザ空間を消去します。チップ消去は ICSP モードでデバイスをプログラミングする場合のみ許可されます (**セクション 4.3.4「インサーキット シリアル プログラミング ™(ICSP™) の規則」**参照)。

図 4-1:　　プログラムフローの規則



4.2 割り込みに関する規則

割り込み処理は、以下に示す理由で制限されます。

- 割り込みからのリターンは、(スタック内のリターンアドレスの悪意ある変更により) 意図したプログラムフローを破壊する一因になる
- セキュアなコードとするには、割り込みに応答する前にレジスタと RAM から機密性の高い情報を消去する必要がある

ブートセグメント コード保護が「高」に設定されている場合、実行中に発生するブートセグメント ベクタ内の全ての割り込みは、*1* つのセキュアベクタ位置 (アドレス : [BS 開始アドレス + 40h]) に格納できます。この機能によりブートセグメントは、汎用セグメント内の ISR に実行を許可する前に、ブートセグメント コンテクストとリターンアドレスを保護できます。

4.2.1 セキュアな割り込み処理シーケンス

セキュアな処理シーケンスの目的は、実行中に「高」セキュリティに設定したブートセグメントから発生する汎用セグメント例外を処理する前に、W レジスタまたはデータメモリ内に格納されているセキュア情報を全て削除する事によって、チェーンオブ トラストを繋げる事です (セキュア情報は後で復元されます)。これにより、意図したプログラムのフローが破壊される可能性 (スタック内のリターンアドレスを変更する事で可能) を回避できます。

ブートセグメント コードが「高」セキュリティで実行中に割り込みまたはトラップが発生した場合、リターンアドレスがスタックにプッシュされ、PC には通常の割り込みベクタではなくセキュアベクタ位置 [ベースアドレス + 40h] のアドレスが書き込まれます。このアドレスはブートセグメント用の特殊 ISR を指しています。

1. この特殊なブートセグメント内の ISR では以下を実行します。
   a) W レジスタまたはデータメモリ内の全てのセキュアな情報を削除する。
   b) 実際のリターンアドレスをスタックから取得し、データメモリに保存する (必要に応じて暗号化する)。
   c) 実際のリターンアドレスを、ブートセグメント開始アドレスとブートセグメント開始アドレス + 03Eh(先頭の 32 命令位置) の間に位置する新しいリターンアドレスに置き換える。
   d) INTTREG を読み出し、どの割り込みベクタにジャンプすべきかを判断する。
   e) 割り込みベクタテーブルから割り込みベクタを読み出し、間接ジャンプを実行する。
2. アプリケーションの汎用セグメント内の ISR を実行する (ユーザコードを実行し割り込みから戻る)。これによりアプリケーションは「新しいリターンアドレス」に戻る。これはリカバリルーチンとなる (またはリカバリルーチンにジャンプする)。
3. データメモリから本来のリターンアドレスを読み出す。

4.3 フラッシュ アクセスの規則

4.3.1 フラッシュ読み出しの規則

`TBLRD` と、PSV アドレス指定でプログラムメモリをアドレス指定する命令は制限できます。保護されたプログラムメモリ位置を不正に読み出すと、全て「`0`」が読み出されます。ブートセグメントがセキュリティなし (BSS<1:0> = `11`) に設定されていない限り、汎用セグメントはブートセグメントを読み出す事はできません。汎用セグメントが「高」セキュリティ (BSS<1:0> = `0x`) に設定されていない限り、ブートセグメントは汎用セグメントを読み出す事ができます。コンフィグレーション セグメントとベクタセグメントは常にブートセグメントと汎用セグメントから読み出す事ができます。これらのセグメントのセキュリティ レベルは問いません。

デュアルブート モードをサポートするデバイスでは、上記の規則はアクティブ パーティション アドレス空間と非アクティブ パーティション アドレス空間の間に適用されます。

4.3.2 RTSP(実行時自己プログラミング) の規則

RTSP(実行時自己プログラミング) は、まずフラッシュの一部を消去し、次に書き込みラッチに新規データを書き込みます。セキュリティ機能は、セグメントの規則に基づいて実際の書き込み動作を防ぎます。セグメントの書き込み保護を有効にすると、書き込みはブロックされます。

デュアルブート モードをサポートするデバイスでは、非アクティブ パーティション内のターゲット セグメントの書き込み保護は無視されます。例外は、保護デュアルブート モードです (**セクション 5.2.2「保護デュアルブート モード」**参照)。特権デュアルブート モードでは、非アクティブ パーティションを消去できます。しかし、セキュリティ機能によって、BSLIMx ビット設定は強制的に非アクティブからアクティブに変更されます。

4.3.3 セグメントの消去とコード保護のクリア

コンフィグレーション セグメントは、全てのデバイスコード保護制御ビットを格納し、汎用セグメントの直後のユーザ空間に位置しています。セグメントのコード保護を解除する唯一の手段は、上記の制限を受けるコンフィグレーション セグメントを消去する事です。コンフィグレーション セグメントはフラッシュページより大幅に小さくなる事に注意が必要です。従って汎用セグメントは、利用可能なフラッシュ空間を最大化するため、コンフィグレーション セグメントの先頭にいたる全域に配置できます。従って、コンフィグレーション セグメントのページ消去によって起こる以下の事に注意する必要があります。

- コンフィグレーション セグメントのセキュリティ レベルが汎用セグメントのセキュリティ レベルより高くなる場合がある。
- 同一ページの全ての汎用セグメントコードが消去される。

従って、ブートセグメントがコンフィグレーション セグメントを更新する場合、コンフィグレーション セグメントページ内の汎用セグメントも再書き込みする必要があります。

4.3.4 インサーキット シリアル プログラミング ™(ICSP™) の規則

デバイスをデバイス プログラマに接続した状態では、デバイスコード メモリとデータフラッシュメモリの消去、プログラミング、ベリファイのみが可能です。デバイス プログラマはチップ消去、パーティション消去、ページ消去のいずれかのコマンドを使ってデバイスを消去し、コード保護をクリアします。ICSP プログラミングは、書き込み保護されていない汎用セグメント上でのみ実行できます。デバイス内のコード保護されたセグメントをベリファイしようとすると「0」が読み出されます。ブートモードでデバイスにコードをプログラミングすると、コンフィグレーション ビットが書き込まれコード保護レベルが有効になります。これ以降にデバイスのコードを変更するには、コード自体が自己プログラミングを実行するか、消去とコード保護のクリアを再度実行する必要があります。

5.0 デュアルブートのセキュリティ

Note: 一部の dsPIC33/PIC24 デバイスはデュアルブート動作を備えていません。詳細は各デバイス データシート内の**「メモリ構成」**を参照してください。

デュアルブート モードを使うアプリケーションでは、その他のセキュリティ機能が利用できます。アクティブ パーティション内のセグメント間の権限に加えて、アクティブ パーティションで実行するコードによる非アクティブ パーティションへの動作も制限されます。コード保護をさらに拡張する 2 つの特殊なデュアルブート モードも備えています。非アクティブ パーティション内のセグメントからは、任意の形態の消去または書き込み動作を含め、いかなるコードも実行できません。

5.1 デュアルブートの概要

Note: デュアルブート動作の詳細は各デバイスのデータシート内の**「フラッシュ プログラムメモリ」**を参照してください。

デバイスがいずれかのデュアルブート モードにある場合、2 つの独立したアプリケーションを使い、それぞれ専用のパーティション内でメモリをプログラミングできます (これらのパーティションをパーティション 1、パーティション 2 と呼ぶ事もあります)。デバイスの初期化中、ブートシーケンス番号が小さい方のパーティションがアクティブ パーティションに割り当てられ実行されます。両パーティションのブートシーケンス番号が等しい場合、パーティション 1 がアクティブ パーティションに割り当てられます。アクティブ パーティションと非アクティブ パーティションは、実行時とブートシーケンス番号変更によるデバイスリセット実行のどちらかでスワップできます。

各コードのパーティション (パーティション 1 および 2) はそれぞれ独立したコード保護設定を持っています。これは、ブートセグメント サイズ、セキュリティ レベル、各パーティションの CS 内にある書き込み保護を含みます。書き込み保護は、アクティブ パーティションにあるコードに対してのみ機能し、非アクティブ パーティションに割り当てられているコードに対しては機能しません (非アクティブ パーティションでは書き込み保護されません)。そのため、非アクティブ パーティション内のセグメントがアクティブ パーティションに移動した際に書き込み保護に設定されていても、アクティブ パーティション内の書き込み保護されたセグメントは、非アクティブ パーティション内のセグメントを書き込みまたは消去できます。

Note: `BOOTSWP` 命令を使ってパーティションのスワップが開始された場合、BSLIMx ビットとコード保護値を含む全ての設定がアクティブ パーティションの新規設定に基づいて再設定される訳ではありません。コード保護設定データが異なる場合、新たにアクティブになったパーティションに再割り当てするために、デバイスリセットが必要です。あるいは、これらのデータを全く同じにプログラミングする事でソフトスワップ時にセキュリティの隙間が生じないようにします。

表 5-1: VS(非アクティブ パーティション) アクセス規則

ブートセグメントのステータス		未定義 (GSS セキュリティ)			定義済み (BSS セキュリティ)		
セグメント セキュリティ レベル		なし	標準	高	なし	標準	高
アクティブ セグメントからの要求動作							
VS の読み出し	BS	不可			可		
	GS から	可			可		
VS のプログラム / ページ消去	BS	不可			可		
	GS から	可			可	不可	

表 5-2: BS および GS(非アクティブ パーティション) アクセス規則

セグメント セキュリティ レベル		なし	標準	高
アクティブ セグメントからの要求動作				
BS の読み出し	BS	可		
	GS から	可	不可	
BS のプログラム / ページ消去	BS	可		
	GS から	可	不可	
チップ消去	BS	不可		
	GS から	不可		
非アクティブ パーティションの消去 (1)	BS	可		
	GS から	可	不可	
GS の読み出し	BS	可		不可
	GS から	可		
GS のプログラム / ページ消去	BS	可		不可
	GS から	可		

Note 1: 非アクティブパネルの消去コマンドは BS または GS 内のコードから実行できます (BS のセキュリティ レベルが「なし」の場合)。

表 5-3: CS(非アクティブ パーティション) アクセス規則

非アクティブ CS セキュリティ レベル		なし	標準	拡張	高
アクティブ セグメントからの要求動作					
CS の読み出し	BS	可			
	GS から	可			
CS のプログラム	BS	可			
	GS から	可		不可	
CS のページ消去	BS	可			不可
	GS から	可	不可		

5.2 デュアルブートのセキュリティ モード

デュアルブート モードでは、以下の BTMODE 設定に基づいて 3 つのセキュリティ モードが利用できます。

- デュアルブート モード
- 保護デュアルブート モード
- 特権デュアルブート モード

5.2.1 デュアルブート モード

デバイスがデュアルブート モードで動作している場合、適用される唯一のセキュリティ制限は、コード保護ビットで定義されるものです。非アクティブ パーティションのコードに対する書き込み保護は常に無視され、非アクティブ パーティションは常時プログラミングできます。アクティブ パーティションと同様に、非アクティブ パーティションの VS は、ブートセグメントが定義されていない場合は汎用セグメントの権限を引き継ぎ、ブートセグメントが定義されている場合はブートセグメントの権限を引き継ぎます。表 5-1 ～ 表 5-3 に、非アクティブ パーティションの指定されたコード保護設定におけるアクティブ パーティションの動作による相互作用を示します。

5.2.2 保護デュアルブート モード

保護デュアルブート モードは、その他の機能を追加する事でパーティション 1 の「工場設定」のイメージを恒久的に消去 / 書き込み保護します。保護デュアルブート モードでは、非アクティブ パーティションに割り当てられている場合、セキュリティ設定に関係なく、パーティション 1 は常に書き込み保護されます。アクティブ パーティションに割り当てられている場合、パーティション 1 のコードのセキュリティは、書き込みビットとコード保護ビットの設定で定義されます。

5.2.2.1 保護デュアルブート モードの例

以下に示す保護デュアルブート モードの例で、パーティション 1 の工場設定のコードイメージは非アクティブ パーティションに割り当てられています。パーティション 2 は、実行するアクティブなコードイメージを含みます。工場設定のコードは、工場設定以外のコードを有効にするのに必要な全てのコードと、リカバリに必要な全ての手順を含む必要があります。

この構成を実現するには以下の手順に従います。

1. デバイスを保護デュアルブート モードに設定する。
2. ブートセグメントを有効にしブートシーケンス番号が FFFh になるように、パーティション 1 を設定する。
3. 工場で設定された既定値のコードイメージを書き込む。
4. 工場設定のコードがアクティブ パーティションに割り当てられた際に自己変更する必要がない限り、パーティション 1 の全てのコードセグメントの書き込み保護を有効にする。
5. 必要なアプリケーション コードイメージを (非アクティブ) パーティション 2 に書き込む。アプリケーション コードが自己変更する必要がある場合、そのパーティションがブートセグメントを含むように設定する。
6. パーティション 2 のブートシーケンス値を FFFh 未満の値にプログラミングする事で、パーティション 2 をアクティブ パーティションに設定する。

アクティブなコードをフィールドで更新する場合、最初にアクティブ パーティションを消去しブートシーケンス番号をリセットします。こうする事で、エラー発生時に工場設定が使われます。

Note:	保護デュアルブート モードでは、パーティション 1 の書き込み保護を有効にすると、全チップ消去を除き全ての書き込みと消去からコードを完全に保護します。

5.2.3 特権デュアルブート モード

特権デュアルブート モードを使うとその他のセキュリティ保護を利用できます。このモードでは、デバイス内で複数の企業がソフトウェアを所有している場合、ブートサイズを制限する事で知的財産を保護できます。一部のデュアルブート デバイスは特権デュアルブート モードを備えていません。詳細は各デバイスのデータシートを参照してください。

特権デュアルブート モードでは、非アクティブ パーティションを消去すると、非アクティブ パーティションのブートサイズ制限はアクティブ パーティションのコンフィグレーション ワードから自動的にコピーされます。これにより、不正コードによって非アクティブ ブート サイズが変更される事を防ぎ、アクセスされる汎用セグメント空間にブートセグメント コードを効果的に配置できます。

特権デュアルブート モードで動作する場合、非アクティブ パーティションのブートセグメント内には何も書き込まない場合でも、ブートセグメントの作成者が非アクティブ パーティション空間とアクティブ パーティション空間の両方に同じサイズのブートセグメントを作成する事を推奨します。これにより、汎用セグメントの作成者によって小さいシーケンス番号で非アクティブ パーティションの汎用セグメントに不正コードが書き込まれ、不正コードを含む非アクティブ パーティションのブートセグメントが作成されるのを防ぐ事ができます。不正コードが書き込まれた時点で汎用セグメントはコンフィグレーション セグメントへの書き込みアクセス権を持ち、次のリセットで「トロイの木馬」がアクティブになる事ができます。その場合、ブートセグメントの作成者のコードの内容を読み出してダンプできます。

5.2.3.1 特権デュアルブート モードの例

以下の例では、2 つの独立した企業のアプリケーション コードが 1 つのデバイスにプログラミングされ、それらのアプリケーション コードはストールする事なくフィールドで更新可能です。この例では、企業 1 は独自のアルゴリズムとブートローダ コードの作成者であり、企業 2 は企業 1 のアルゴリズムへのアクセス権を持たないメイン アプリケーション コードの作成者です。理想的には、ブートセグメントに保存した暗号化コードを使ったフィールド アップデート機器向けには、ブートローダは暗号化された通信方式を使うべきです。

この場合、企業 1 は以下を実行します。

1. 企業 1 は、両パーティションで定義された同じサイズのブート空間を持つ特権デュアルブート モードにデバイスを設定する。ブートセグメント コード保護ビットは「高」セキュリティ、コンフィグレーション セグメントコード保護ビットは「標準」セキュリティ、汎用セグメントコード保護ビットは「低」セキュリティ (書き込みは可能だが消去は不可) に設定する。
2. ブートローダと独自のアルゴリズムをブートセグメントに書き込む。その後、ブートセグメントの書き込み保護を有効にする。これによりコンフィグレーション セグメントは、ブートセグメント以外からは書き込む事ができなくなり、汎用セグメント内の企業 2 のコードから効果的に保護される。
3. 部分的にプログラミングされたデバイスが企業 2 に出荷される。

企業 2 は、汎用セグメントにメイン アプリケーション コードを書き込み、汎用セグメントとコンフィグレーション セグメントを「高」セキュリティに設定します。これで、ブートセグメントは汎用セグメントを消去も書き込みもできなくなります。

フィールド アップデートが必要な場合、アプリケーション コードは更新要求を認識および認証し、ブートセグメント内のブートローダにジャンプします。更新コードは、アクティブ パーティションのブートセグメントから非アクティブ パーティションのブートセグメントに書き込まれます。

Note:	更新アプリケーションがブートセグメントのサイズ変更を必要とする場合、デバイスリセット時にアプリケーションを書き込む前に新しいパーティション サイズ (BSLIMx ビットで定義) とコード保護ビットを書き込む必要があります。

汎用セグメントを更新する場合、RAM データを保存した後、更新が必要である事を汎用セグメントに対してブートセグメントがフラグで知らせるようにします。汎用セグメントが自己更新できるように、汎用セグメント内のあらかじめ定義された位置へのジャンプが実行されます。

非アクティブ パーティションはアクティブにでき、その後ソフトウェア リセットが実行されます。

6.0 ISCP Write Inhibit によるフラッシュ OTP

ICSP Write Inhibit は、有効にすると、フラッシュメモリ全体が書き込み保護されるアクセス制限機能です。ICSP Write Inhibit を一度有効化すると、ICSP フラッシュ書き込みおよび消去動作は恒久的に禁止されます。この動作は無効化できません。この機能は OTP (One-Time-Programmable) デバイスと同様の挙動でフラッシュメモリの内容が改変されるのを防ぐ事を目的としています。

6.1 ICSP Write Inhibit の有効化

ICSP Write Inhibit はコンフィグレーション メモリ空間に 2 つのフラッシュワード (1 ワードあたり 16 ビットの事前定義された有効化値) を書き込む事で有効化できます。ターゲット NVM アドレスと有効化に必要な値については、各デバイスのデータ シートを参照してください。両方のアドレスに有効化値が書き込まれると、次回デバイスをリセットした時点で ICSP Write Inhibit は恒久的に有効化されます。ICSP Write Inhibit が正常に有効化された後は、これらのアドレスはいかなる手段によっても消去または変更できません。

これらのアドレスを書き込む順序は任意で、別々の ICSP/ 拡張 ICSP/RTSP セッションで書き込む事もできますが、不正な 16 ビット値の書き込み操作、または行プログラミングを使った値の書き込み操作は、既存のデータを変更する事なく中止されます。

6.2 ICSP Write Inhibit によるセキュリティの拡張

ICSP Write Inhibit はデバイスを ICSP 操作からロックし、デバイス フラッシュの内容を再プログラムまたは消去しようとする試みを制限します。

RTSP 操作 (消去と書き込みを含む) は ICSP Write Inhibit が有効化されていても制限されませんが、RTSP 操作を実行するためのコードは ICSP Write Inhibit を有効化する前にデバイスに書き込んでおく必要があります。これにより、ICSP Write Inhibit が有効でも、ブートローダ アプリケーションでフラッシュの内容を更新できます。

6.3 デバッグモード移行の無効化

リリースモードで ICSP Write Inhibit モードがオンになると、デバッグモードへの移行が恒久的に禁止されます。

デバッグモード中に ICSP Write Inhibit モードを有効化した場合、ライトビットがロックされ、フラッシュの消去と書き込みが完全に制限されるため、デバッグモードを終了できなくなります。従って、ICSP Write Inhibit は本番用にプログラムされたデバイスのみで有効化します。

7.0 書き換え不可のセキュアブート

デバイスのブートコードはリセット後に最初に実行されるコードであり、安全な「ルートオブ トラスト」環境を構築するために使用できます。ルートオブ トラスト セグメントへのあらゆるコード変更を防止するため、ルートオブ トラスト領域は書き換え不可である事が不可欠です。セキュアなルートオブ トラストは、ソフトウェアを実行する前にその真正性と完全性を検証するために使われるため、セキュリティを強化するための強固な基盤となります。さらに、セキュアなフィールド アップデート、公開鍵と証明書の不変ストレージ、セキュアブートの促進等の機能もサポートします。

CodeGuard™ 中間セキュリティは、汎用セグメント内のコードからのアクセスや消去を防ぎ、ブートセグメント内のコードがブートセグメント自体を変更できなくする事で、セキュアなブートセグメントのための書き換え不可の環境を構築します。CodeGuard はブートセグメント (セキュアブート コードまたは独自のアルゴリズムを含む可能性がある) に 3 つのセキュリティ レベルを提供します。ブートセグメントが「高」セキュリティに定義されている場合、「標準」/「低」セキュリティに比べて許可される操作が制限されます。このセキュリティ レベルでは、CodeGuard はブートセグメントへのセキュアベクタ（ブートセグメントのベースアドレス + 40h）も有効にします。これにより、「高」セキュリティのブートセグメントからの実行中に発生する汎用セグメントの例外を処理する前に、W レジスタや RAM 内のセキュアな情報を認識して保護できます。

ブートセグメントは BWRP コンフィギュレーション ビットをプログラムする事によって書き込み保護する事もできます。書き込み保護された場合、ブートセグメントを対象とするページ消去と行またはワード プログラミング動作は禁止されます。

ICSP Write Inhibit は ICSP 操作からデバイスを保護し、特に ICSP によるブートセグメント フラッシュの再プログラムや消去の試みを制限します。

これら全ての機能により、CodeGuard™ 中間セキュリティと ICSP Write Inhibit は、セキュアなルートオブ トラストコードのための書き換え不可の環境を確立させます。

7.1 デバイスのブート ローディング

コード保護が必要になる典型的なシナリオはフィールド アップグレード可能なシステムです。このセクションでは、ティア 1 メーカーが製品を OEM に出荷する際に、ブートセグメントに含まれる独自のコード /IP を保護する方法を示すシナリオについて説明します。その後、OEM は汎用セグメントでアプリケーションを開発し、ティア 1 メーカーがブートセグメントに実装した API や機能を利用できます。

このシナリオでは、ティア 1 メーカーは製造プロセス中にデバイスに自社のコードを書き込んだ後、**セクション 7.1.1「ティア 1 メーカーによる書き込み」**の説明に従ってブートセグメントに適切なコード保護値を設定する事でデバイスを保護します。このコードには、ティア 1 メーカー独自のアルゴリズムと、フィールド アップデートを受信して検証するためのセキュア ブートローダ コードが含まれる場合があります。その後、OEM はそのメイン アプリケーション コードを自社で最終製品に書き込む必要があります (**セクション 7.1.2「OEM による書き込み」**参照)。最後に、フィールド アップデートを可能にするため、アプリケーション コード（および場合によってはティア 1 メーカーのコード）は受信したパッチ アップデートを RTSP 経由で適用できます。最終的に、OEM もティア 1 メーカーも相手のコード / データを読み出しまたは変更する事はできません。この例では、シングルブート モデルを想定し、コードにブートセグメントと汎用セグメントを使用しています。

7.1.1 ティア 1 メーカーによる書き込み

ティア 1 メーカーは、ブートセグメントに独自のコードを書き込み、ブートセグメントのセキュリティ レベルを「高」に、コンフィギュレーション セグメントのセキュリティを「標準」に設定します。コンフィギュレーション セグメントは未だ汎用セグメントによって書き込み可能です（消去はできません）。従って、汎用セグメントがブートセグメントのコード保護セキュリティを下げてブートコードにアクセスする事はできません。ブートセグメントには、セキュアなフィールド アップデートをサポートするブート ファームウェアを含める事もできます。その後、製品が OEM に出荷されます。

7.1.2 OEM による書き込み

OEM は、セキュア ブートローディングによって汎用セグメントに書き込んだ後、汎用セグメントとコンフィギュレーション セグメントのセキュリティ レベルを「高」に設定します。これにより、汎用セグメントはブートセグメントから読み取れなくなり、コンフィギュレーション セグメントはブートセグメントからも汎用セグメントからも消去または書き込みできなくなります。以上で、ブートセグメントと汎用セグメントは互いにセキュアになりました。

7.1.3 フィールド アップデート

フィールドで稼働しているシステムに、技術者が再プログラミング ツールを接続します。アプリケーションはこの接続を認識し、ブートセグメントのアクセス領域に分岐します。この分岐はブートセグメント アクセス領域を経由する必要があり、この分岐を変更しようとするとデバイスリセットが発生する事に注意してください。

ブートセグメントには、ツールとの間の認証済みの通信を可能にするためのコードが含まれます。また、ブートセグメントには、ECC-P256 ベースの ECDSA 等の非対称暗号アルゴリズムによる署名検証に使われる公開鍵が含まれる事もあります。公開鍵はブートセグメント コード保護を「高」に設定した状態でブートセグメントに配置されるため、公開鍵にアクセスできるのはセキュアなブートローダ コードのみです。

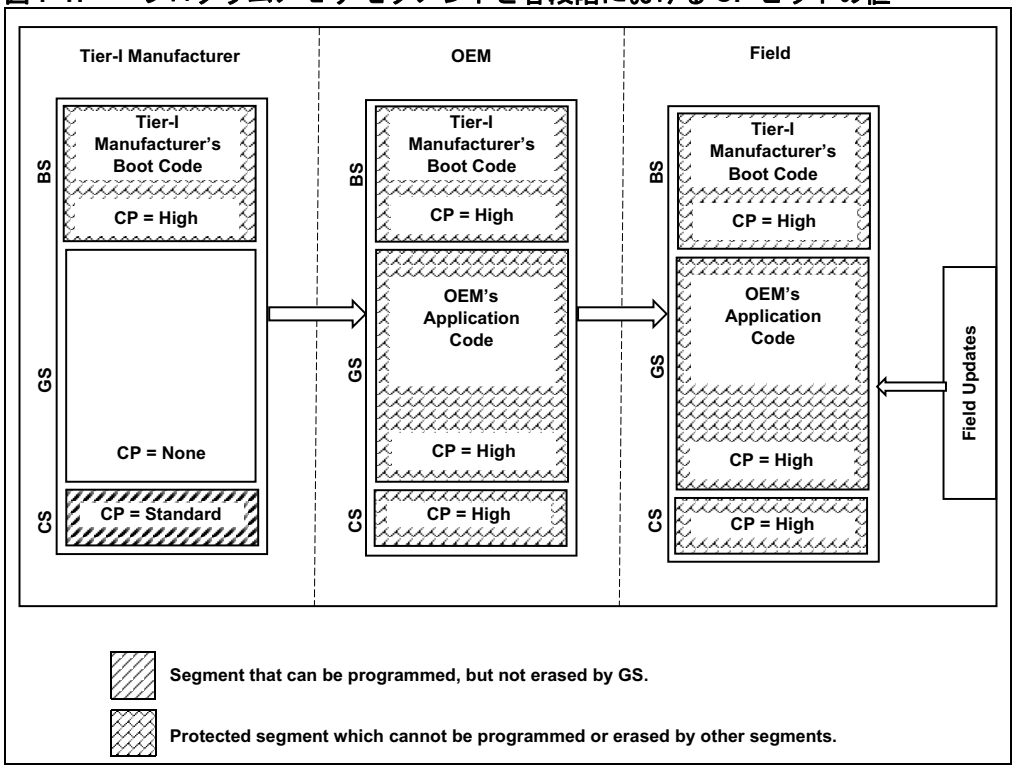
ブートローダは、ツールとの間で有効な通信が確立された事を確認した後、ツールから更新コードを受信し、それを相互に合意された RAM 領域に格納できます。

更新対象が汎用セグメントである場合、ブートセグメントは汎用セグメントコードにアップデートが必要であるというフラグを立て、事前に定義された位置で汎用セグメントコードに戻ります。汎用セグメントコードはフラグを確認し、パッチが必要な領域を再フラッシュ (ページ消去、プログラム、およびベリファイ) します。汎用セグメントのセキュリティは「高」であるため、再フラッシュは汎用セグメント内でしか実行できません。

更新対象がブートセグメントである場合、ブートセグメントがパッチを適用します。

ブートローダは、割り込みまたはトラップをブートローダ内の安全なベクタ位置へ分岐させる事ができるため、ブートローダの動作が割り込みやトラップによって中断する事はありません。アップデート後にアプリケーションがソフトウェア リセットされるかどうかはパッチによって異なります。

図 7-1: プログラムメモリ セグメントと各段階における CP ビットの値



8.0 設計のヒント

質問 1: **既定値コード保護設定のデバイスでブートローダを使えますか。**

回答 : 既定値コード保護設定のデバイスには汎用セグメントしかありません。セグメントが 1 つしか存在しないため、そこに格納されているブートローダ自体を消去せずにそのセグメントを消去し、コード保護をクリアする事はできません。

このためブートの選択肢は限られます。ただし、ブートが全く不可能という訳ではありません。この場合、ブートローダは、「セグメントよりも小さな」パーティションを消去 / 再プログラムする必要があり、汎用セグメントの書き込み保護を設定する事もできません。読み込んだコードをブートローダ自体に起因する漏洩から保護する事もできません。

質問 2: **システムがまずコードの一部を読み込み、残りを後で読み込む事はできますか。**

回答 : セグメントが書き込み保護されておらず、かつ「高」セキュリティに設定されていなければ、「インクリメンタル」読み込みは可能です。また、「高」セキュリティのセグメントであっても、ローダがそのセグメントに格納されていれば、インクリメンタル読み込みは可能です。しかし、セグメントに書き込み保護を設定した後は、セグメント消去命令を使ってセグメント全体を消去しコード保護をクリアするまで、コードは変更できません。

割り込みベクタ用のジャンプテーブルを保護対象外のセグメントに配置し、割り込みベクタを変更する事でジャンプテーブルを更新する方法もあります。この方法であれば、ブートセグメントを書き込み保護できます。

9.0 関連文書

本書に関連する参考文書を以下に記載します。一部の文書は dsPIC33 または PIC24 製品ファミリ向けではありません。ただし概念は共通しており、変更が必要な場合や制限事項が存在する場合があるものの適用は可能です。

CodeGuard ™中間セキュリティに関連する、現在提供中の文書は以下の通りです。

タイトル	文書番号
CodeGuard™ Security: Protecting Intellectual Property in Collaborative System Designs	DS70179

Note: dsPIC33/PIC24 ファミリ関連のアプリケーション ノートとサンプルコードは Microchip 社のウェブサイト (www.microchip.com) でご覧になれます。

10.0 改訂履歴

リビジョン A (2014 年 5 月)

本書は初版です。

リビジョン B (2023 年 4 月)

このリビジョンでの変更内容は以下の通りです。

- セクション :
  - **セクション 6.0「ISCP Write Inhibit によるフラッシュ OTP」**と**セクション 7.0「書き換え不可のセキュアブート」**を追加
  - **セクション 1.0「はじめに」**、**セクション 3.0「コードセグメントの構成」**、**セクション 3.1「コード保護ビット」**、**セクション 3.2「ブートセグメント (BS)」**、**セクション 3.2.1「BS の割り当て」**、**セクション 3.2.2「セキュリティ レベルの選択」**、**セクション 3.3.2「GS の書き込み保護」**、**セクション 3.5.1「AIVT(代替割り込みベクタテーブル)」**、**セクション 4.1「プログラムフローに関する規則」**、**セクション 4.2「割り込みに関する規則」**、**セクション 4.2.1「セキュアな割り込み処理シーケンス」**、**セクション 5.1「デュアルブートの概要」**を更新
- 図 :
  - 図 3-1
- 表 :
  - 表 4-2、表 4-3、表 5-2

NOTE:

Microchip 社製品のコード保護機能について以下の点にご注意ください。

- Microchip 社製品は、該当する Microchip 社データシートに記載の仕様を満たしています。
- Microchip 社では、通常の条件ならびに動作仕様書の仕様に従って使った場合、Microchip 社製品のセキュリティ レベルは、現在市場に流通している同種製品の中でも最も高度であると考えています。
- Microchip 社はその知的財産権を重視し、積極的に保護しています。Microchip 社製品のコード保護機能の侵害は固く禁じられており、デジタル ミレニアム著作権法に違反します。
- Microchip 社を含む全ての半導体メーカーで、自社のコードのセキュリティを完全に保証できる企業はありません。コード保護機能とは、Microchip 社が製品を「解読不能」として保証するものではありません。コード保護機能は常に進化しています。Microchip 社では、常に製品のコード保護機能の改善に取り組んでいます。

本書および本書に記載されている情報は、Microchip 社製品を設計、テスト、お客様のアプリケーションと統合する目的を含め、Microchip 社製品に対してのみ使う事ができます。それ以外の方法でこの情報を使う事はこれらの条項に違反します。デバイス アプリケーションの情報は、ユーザの便宜のためにのみ提供されるものであり、更新によって変更となる事があります。お客様のアプリケーションが仕様を満たす事を保証する責任は、お客様にあります。その他のサポートは Microchip 社正規代理店にお問い合わせ頂くか、https://www.microchip.com/en-us/support/design-help/client-support-services をご覧ください。

Microchip 社は本書の情報を「現状のまま」で提供しています。Microchip 社は明示的、暗黙的、書面、口頭、法定のいずれであるかを問わず、本書に記載されている情報に関して、非侵害性、商品性、特定目的への適合性の暗黙的保証、または状態、品質、性能に関する保証をはじめとするいかなる類の表明も保証も行いません。

いかなる場合も Microchip 社は、本情報またはその使用に関連する間接的、特殊的、懲罰的、偶発的または必然的損失、損害、費用、経費のいかんにかかわらず、また Microchip 社がそのような損害が生じる可能性について報告を受けていた場合あるいは損害が予測可能であった場合でも、一切の責任を負いません。法律で認められる最大限の範囲を適用しようとも、本情報またはその使用に関連する一切の申し立てに対する Microchip 社の責任限度額は、使用者が当該情報に関連して Microchip 社に直接支払った額を超えません。

Microchip 社の明示的な書面による承認なしに、生命維持装置あるいは生命安全用途にMicrochip社の製品を使う事は全て購入者のリスクとし、また購入者はこれによって発生したあらゆる損害、クレーム、訴訟、費用に関して、Microchip 社は擁護され、免責され、損害をうけない事に同意するものとします。特に明記しない場合、暗黙的あるいは明示的を問わず、Microchip社が知的財産権を保有しているライセンスは一切譲渡されません。

商標

Microchip 社の名称とロゴ、Microchip ロゴ、Adaptec、AVR、AVR ロゴ、AVR Freaks、BesTime、BitCloud、CryptoMemory、CryptoRF、dsPIC、flexPWR、HELDO、IGLOO、JukeBlox、KeeLoq、Kleer、LANCheck、LinkMD、maXStylus、maXTouch、MediaLB、megaAVR、Microsemi、Microsemi ロゴ、MOST、MOST ロゴ、MPLAB、OptoLyzer、PIC、picoPower、PICSTART、PIC32 ロゴ、PolarFire、Prochip Designer、QTouch、SAM-BA、SenGenuity、SpyNIC、SST、SST ロゴ、SuperFlash、Symmetricom、SyncServer、Tachyon、TimeSource、tinyAVR、UNI/O、Vectron、XMEGA は米国とその他の国における Microchip Technology Incorporated の登録商標です。

AgileSwitch、APT、ClockWorks、The Embedded Control Solutions Company、EtherSynch、Flashtec、Hyper Speed Control、HyperLight Load、Libero、motorBench、mTouch、Powermite 3、Precision Edge、ProASIC、ProASIC Plus、ProASIC Plus ロゴ、Quiet-Wire、SmartFusion、SyncWorld、Temux、TimeCesium、TimeHub、TimePictra、TimeProvider、TrueTime、ZL は米国における Microchip Technology Incorporated の登録商標です。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、Augmented Switching、BlueSky、BodyCom、Clockstudio、CodeGuard、CryptoAuthentication、CryptoAutomotive、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、Espresso T1S、EtherGREEN、GridTime、IdealBridge、In-Circuit Serial Programming、ICSP、INICnet、Intelligent Paralleling、IntelliMOS、Inter-Chip Connectivity、JitterBlocker、Knob-on-Display、KoD、maxCrypto、maxView、memBrain、Mindi、MiWi、MPASM、MPF、MPLAB Certified ロゴ、MPLIB、MPLINK、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、PowerSmart、PureSilicon、QMatrix、REAL ICE、Ripple Blocker、RTAX、RTG4、SAM-ICE、Serial Quad I/O、simpleMAP、SimpliPHY、SmartBuffer、SmartHLS、SMART-I.S.、storClad、SQI、SuperSwitcher、SuperSwitcher II、Switchtec、SynchroPHY、Total Endurance、Trusted Time、TSHARC、USBCheck、VariSense、VectorBlox、VeriPHY、ViewSpan、WiperLock、XpressConnect、ZENA は米国とその他の国における Microchip Technology Incorporated の商標です。

SQTP は米国における Microchip Technology Incorporated のサービスマークです。

Adaptec ロゴ、Frequency on Demand、Silicon Storage Technology、Symmcom はその他の国における Microchip Technology Incorporated の登録商標です。

GestIC は、その他の国における Microchip Technology Germany II GmbH & Co. KG (Microchip Technology Incorporated の子会社) の登録商標です。

その他の商標は各社に帰属します。

ISBN: 978-1-6683-3312-9

Microchip 社の品質管理システムについては www.microchip.com/quality をご覧ください。

各国の営業所とサービス

南北アメリカ

本社
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
技術サポート :
http://www.microchip.com/support
URL:
www.microchip.com

アトランタ
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

オースティン、TX
Tel: 512-257-3370

ボストン
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

シカゴ
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

ダラス
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

デトロイト
Novi, MI
Tel: 248-848-4000

ヒューストン、TX
Tel: 281-894-5983

インディアナポリス
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453
Tel: 317-536-2380

ロサンゼルス
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608
Tel: 951-273-7800

ローリー、NC
Tel: 919-844-7510

ニューヨーク、NY
Tel: 631-435-6000

サンノゼ、CA
Tel: 408-735-9110
Tel: 408-436-4270

カナダ - トロント
Tel: 905-695-1980
Fax: 905-695-2078

アジア / 太平洋

オーストラリア - シドニー
Tel: 61-2-9868-6733

中国 - 北京
Tel: 86-10 -8569-7000

中国 - 成都
Tel: 86-28-8665-5511

中国 - 重慶
Tel: 86-23-8980-9588

中国 - 東莞
Tel: 86-769-8702-9880

中国 - 広州
Tel: 86-20-8755-8029

中国 - 杭州
Tel: 86-571-8792-8115

中国 - 香港 SAR
Tel: 852-2943-5100

中国 - 南京
Tel: 86-25-8473-2460

中国 - 青島
Tel: 86-532-8502-7355

中国 - 上海
Tel: 86-21-3326-8000

中国 - 瀋陽
Tel: 86-24-2334-2829

中国 - 深圳
Tel: 86-755-8864-2200

中国 - 蘇州
Tel: 86-186-6233-1526

中国 - 武漢
Tel: 86-27-5980-5300

中国 - 西安
Tel: 86-29-8833-7252

中国 - 厦門
Tel: 86-592-2388138

中国 - 珠海
Tel: 86-756-3210040

アジア/太平洋

インド - バンガロール
Tel: 91-80-3090-4444

インド - ニューデリー
Tel: 91-11-4160-8631

インド - プネ
Tel: 91-20-4121-0141

日本 - 大阪
Tel: 81-6-6152-7160

日本 - 東京
Tel: 81-3-6880-3770

韓国 - 大邱
Tel: 82-53-744-4301

韓国 - ソウル
Tel: 82-2-554-7200

マレーシア - クアラルンプール
Tel: 60-3-7651-7906

マレーシア - ペナン
Tel: 60-4-227-8870

フィリピン - マニラ
Tel: 63-2-634-9065

シンガポール
Tel: 65-6334-8870

台湾 - 新竹
Tel: 886-3-577-8366

台湾 - 高雄
Tel: 886-7-213-7830

台湾 - 台北
Tel: 886-2-2508-8600

タイ - バンコク
Tel: 66-2-694-1351

ベトナム - ホーチミン
Tel: 84-28-5448-2100

欧州

オーストリア - ヴェルス
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

デンマーク - コペンハーゲン
Tel: 45-4485-5910
Fax: 45-4485-2829

フィンランド - エスポー
Tel: 358-9-4520-820

フランス - パリ
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

ドイツ - ガーヒンク
Tel: 49-8931-9700

ドイツ - ハーン
Tel: 49-2129-3766400

ドイツ - ハイルブロン
Tel: 49-7131-72400

ドイツ - カールスルーエ
Tel: 49-721-625370

ドイツ - ミュンヘン
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

ドイツ - ローゼンハイム
Tel: 49-8031-354-560

イスラエル - ラーナナ
Tel: 972-9-744-7705

イタリア - ミラノ
Tel: 39-0331-742611
Fax: 39-0331-466781

イタリア - パドヴァ
Tel: 39-049-7625286

オランダ - ドリューネン
Tel: 31-416-690399
Fax: 31-416-690340

ノルウェー - トロンハイム
Tel: 47-7288-4388

ポーランド - ワルシャワ
Tel: 48-22-3325737

ルーマニア - ブカレスト
Tel: 40-21-407-87-50

スペイン - マドリッド
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

スウェーデン - ヨーテボリ
Tel: 46-31-704-60-40

スウェーデン - ストックホルム
Tel: 46-8-5090-4654

イギリス - ウォーキンガム
Tel: 44-118-921-5800
Fax: 44-118-921-5820