

1. 各セキュリティ機能設定表

単一電源フラッシュメモリー・内蔵マイコンの各セキュリティ機能を有効にした場合の Erase コマンド、Program コマンドの関係は次のとおりです。

	CHIP Erase コマンド	Block Erase コマンド	Program コマンド	Read コマンド
Disable Cihp Erase	無効	無効	有効 ^{注1}	有効
Disable Block Erase	有効	無効	有効	有効
Disable Program	有効	無効	無効	有効
Disable Read	有効	有効	有効	無効
Disable Boot block cluster reprogramming	無効	有効 ^{注2}	有効 ^{注2}	有効

注1 Erase コマンドは無効となるため、すでにフラッシュ・メモリに書かれているデータと異なるデータを書き込むことが出来ません。

注2 ブート領域指定以外の領域に対してのみ有効となります。

2. 設定について

Disable Chip Erase をチェックすると、以降、そのデバイスに対し消去も書き込みも出来なくなります。

Disable Block Erase / Disable Program / Disable Read これらの設定は Operation Mode で Chip 選択時の消去コマンドによってクリアできます。

3. 従来と同様な設定

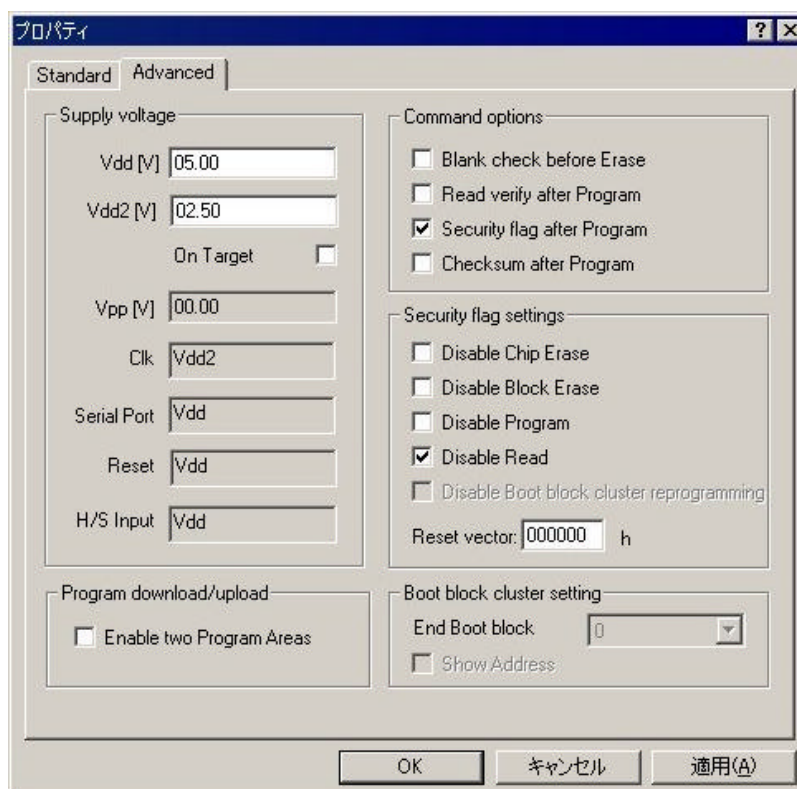
セキュリティ機能の無い、従来のデバイスは次の設定でした。(実際には Security 画面はありません。)

この設定では「再書き込み可能」「消去可能」「内部データリード禁止」となります。

Security Flag Setting では Disable Read のみチェックがされております。

Command Option では Security Flag After Program にチェックが入っております。

EPV の Program の直後に、Security を書き込む指定です。



抜粋 FL-PR4 ユーザーズ・マニュアル 62 ページより。

本文書の内容は参考とさせていただきます。詳細な情報はライターに付属の FL-PR4 ユーザーズ・マニュアルやデバイスデータシートをご覧頂くか、デバイスメーカーにお問い合わせください。