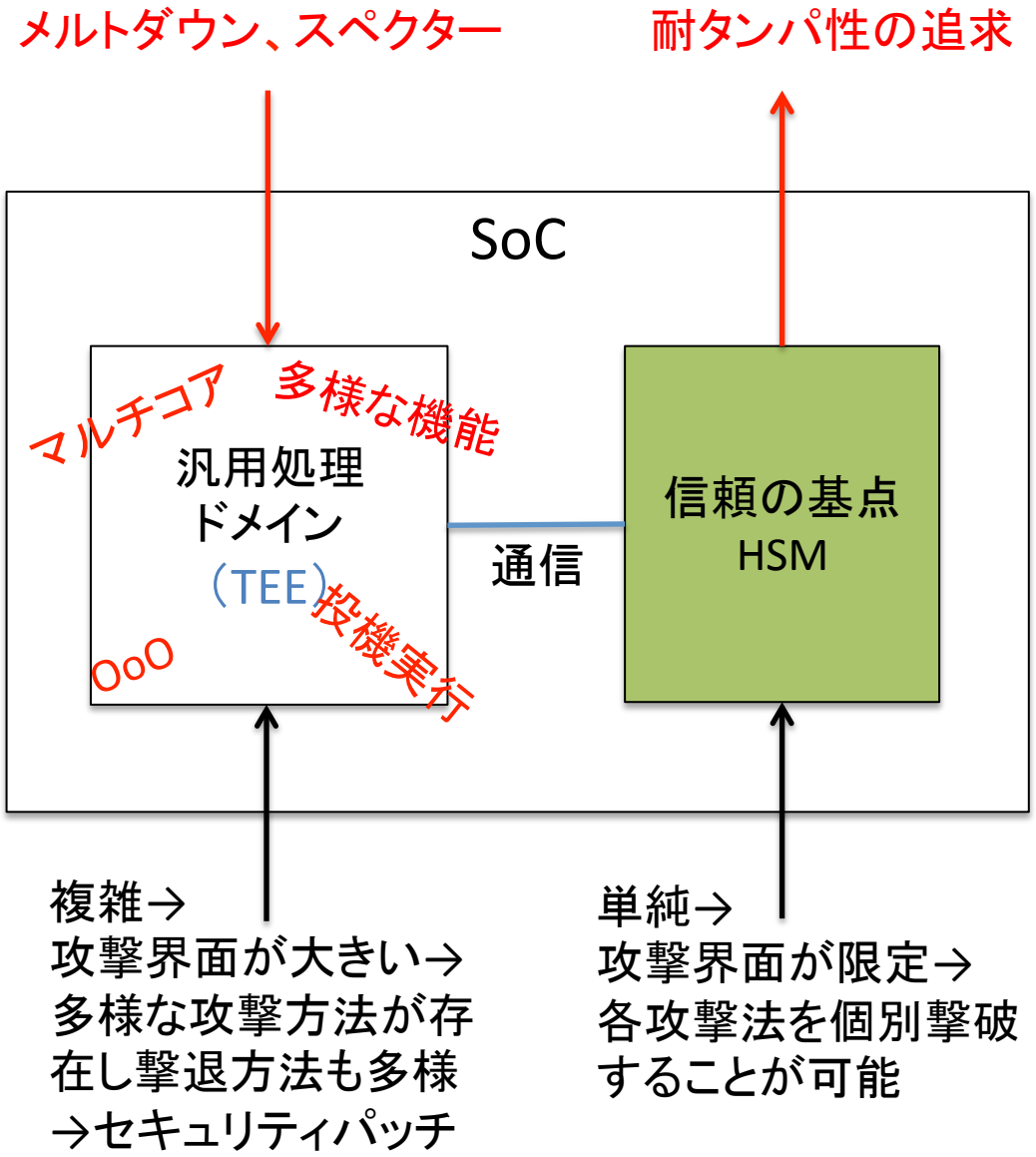
SoC用信頼の基点
ハードウエアセキュリティモジュール（HSM）



- 汎用処理ドメインを守ろうとするとシステムは複雑で、守る方法が特定できない。
- 信頼の起点を分離、単純なシステムを護る方が有効。
- スマホではルートオブトラストを基盤に保護層を数層創り、システム全体を護っている。