SafeNet | THE DATA PROTECTION COMPANY

# ハードウェア暗号関連商品調達要件（ICカード、USBトークン、HSM）におけるCCとFIPS140-2Level3

2014年9月29日
日本セーフネット株式会社
CDP事業部 サービスプロバイダ営業部 部長
JIPDEC客員研究員
亀田治伸

# CCの簡単な用語解説

- EAL（EvaluatonAssuaranceLevel）:

製品の開発過程全般をカバーする保証要件のパッケージであり、7段階の厳格さに対応する。EAL1 は最も基本的（したがって実施するのも評価を受けるのも安あがり）であり、EAL7 は最も厳しい（最も高価）。通常、ST や PP の著者は保証要件を一つ一つ選ぶことはせず、EAL を一つ選び、必要であればより高レベルの保証要件をいくつか**追加**する。**より高い EAL が必ずしも「より良いセキュリティ」を含意するとは限らず、主張している TOE セキュリティ保証がより広範に検証されたことを意味するに過ぎない。**
**日本ではEAL4+までしか流通していない（詳細は後述）**

- TOE（Target of Evaluation）:

**TOE 内の暗号系の実装に関する詳細は、CC の適用領域外である。**代わりに米政府標準 FIPS 140 などが暗号モジュールの仕様を規定し、使用する暗号アルゴリズムの仕様については様々な標準がある。

# 簡単な用語解説

- ST（SecurityTarget）:

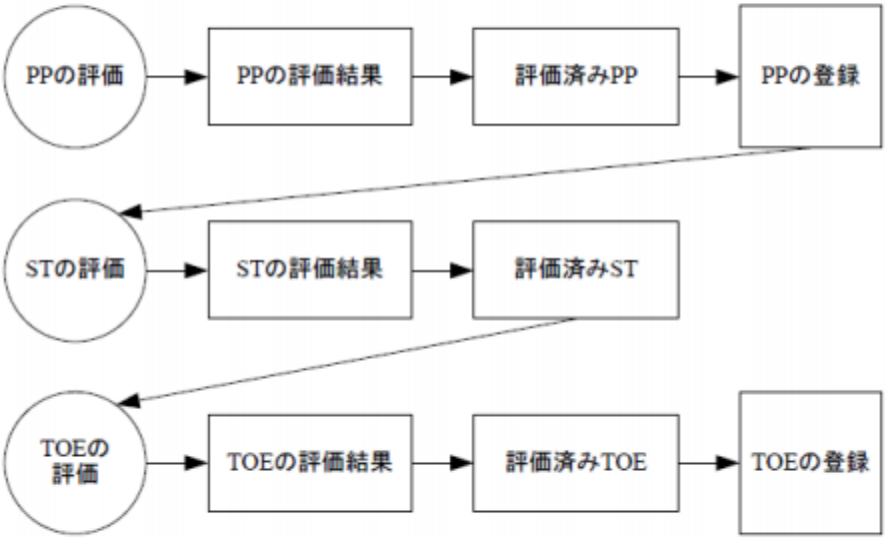
情報セキュリティ面での設計方針を厳密に記述した要件定義書を「セキュリティターゲット（ST）」と呼ぶ。
STは個々の製品ごとに開発者が作成し、同じ分野の製品であっても、相異なる製品であれば、STもまたそれぞれに作成されなければならない

- PP（ProtectionProfile）:

セキュリティ要件（要求仕様）を特定する文書。通常、利用者（または利用者の団体）が、自分の要求仕様を文書化したもの。実質的に、セキュリティデバイスの分類を規定している（例えば、デジタル署名用のスマートカード）。
ある製品分野に共通のセキュリティ脅威とその対策として機能の共通項を括り出し、STの雛形として作成されるのが、表題に掲げた「プロテクションプロファイル（PP）」と呼ばれる。

ICカードの耐タンパ性を定義したもの：PP
Safenet eTokenが定義すべきもの：ST

# Common Criteria（CC）パート1
## PP、ST及びTOEの評価







http://www.cistec.or.jp/service/iinkaidayori/houkokusho2010/data_kamotsu/kamotsu5-1.pdf

# 簡単な用語解説

- CCRA

コモンクライテリア承認アレンジメント (**CCRA**, Common Criteria Recognition Arrangement) は条約に準ずる国際協定である。[4] CCRA の各加盟国は、他の加盟国でなされた CC 規格評価を相互に承認することになっている。**EAL4までが承認対象となり、より高い EAL については、非常に込み入っているので、国境を越えて承認する義務はなく、一部の国において国内限定で評価・認証が行われている。**

**EAL5以上を審査可能な機関は日本に存在していない。（2014年9月現在）**

# ポイント

結局EALの概念のみが流通している。
（しかも間違った形で・・・）

- PP、ST、TOEに対する周知が薄い
- EALはセキュリティレベルと理解されている。
  - 実際は「セキュリティ機能.の評価方法のレベル」

- EALに対するCCRAのわかりやすい解説がWebに存在しない

多階層かつ多重のマトリックス構造となっており、一般ユーザーが把握するには複雑で難解

# 現場で起きている変なこと

- 調達仕様書にて「EAL4以上もしくはFIPS140-2Level3」認定取得、と記載される。
  - PP/ST/TOEに対する基準がない
- EAL4+取得済商品とFIPS140-2Level3取得済商品とのセキュリティ強度比較が行われる
- EAL4+より、EAL5+取得済商品が安全と認識される。

# 結論として

- CCは一般人が理解するには複雑で難解。

- 「暗号商品調達」に限定するのであれば、FIPS140-2Level3の方が、わかりやすく適しているのではないか？（現時点では）
  - もしくはPPの周知徹底を強化する？

- 一方で、CC、PP、ST、TOE、CCRAを可能な限り周知させるための、Webサイトのコンテンツ拡充を図る必要がある。
  - （誰かまずはWikipediaを書き換えませんか？）