SafeNet | THE DATA PROTECTION COMPANY

HSMってなに？

日本セーフネット株式会社

チーフエバンジェリスト

亀田　治伸

ハードウェア暗号モジュール（HSM）とは

決まった定義は存在しないが、以下の特性（もしくはその一部）を備えるものを指す

暗号処理および鍵管理デバイスが備えるべき特性を定義した、国際規格などの認定を取得しているデバイス

FIPS
CommonCriteria
JCMVP等

ICチップ搭載型ICカード（Visa、Master、JCBのクレジットカードなど）やUSB型トークンも含むが、狭義の意味では基幹システムの暗号化に使用する汎用型アプライアンス、もしくはPCI型ボードを指すケースが多い

意外と忘れている事実

暗号解読の必要なもの
暗号の解読方法＋暗号鍵

1. RSA暗号、楕円曲線暗号、3DES暗号、AES暗号等
   主要暗号はすべて、**アルゴリズムが公開**されており
   暗号の解読方法があらかじめ分かっている事実

2. ソフトウェアによる暗号化処理では、**サーバのメモリ上に暗号鍵が展開**されてしまう事実

暗号システムの安全性≒鍵の安全性
鍵の隠匿化≒不可能領域での暗号処理

FIPS140-2認定

米国連邦政府の省庁等各機関が利用する、ハードウェア及びソフトウェア両方を含む “暗号モジュール” に関する要件を規定している。

【レベル1】
一番低いレベルであり、非常に限定した要件を課する; 大まかに、すべてのコンポーネントが製品品質であり、**甚だしくセキュリティの欠如がない**こと。
（ソフトウェア製品の取得可能認定上限： iOS6や弊社仮想アプライアンス等）
【レベル2】
レベル1に次の要件を加える; **物理的な改竄の痕跡を残す**こと、及びオペレータの役割ベースでの認証を行うこと。
【レベル3】
レベル2に次の要件を加える; **物理的な改竄への耐性**(モジュール中に含まれる取扱注意情報への**攻撃者のアクセスを困難にする**)を持つこと、オペレータのIDベースでの認証を行うこと、及び重要なセキュリティパラメータがモジュールに出入力するインタフェースと、その他のインタフェースとを物理的又は論理的に分離すること。
(wikipediaより)

HSMが担保できるもの

暗号鍵、解読鍵の対攻撃性
HSMが物理的に盗難されない限り、外部からの攻撃では鍵が漏洩しない

高速暗号処理
専用チップによる暗号・解読処理

鍵の集約中央管理
アプリケーションと分離させることで、別権限での鍵管理を実現

HSMの技術的特性　ワンチップ形成

ワンチップ形成

暗号処理は複雑な計算を複数組み合わせて繰り返し処理を多用する。
その組み合わされる複数の処理は全て1つのチップで処理を行うよう努める。

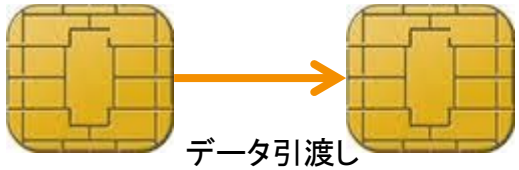
例：ある数字に“2をかけ、2をたす”暗号処理

元の数字	暗号された数字
1	4
2	6
3	8
4	10
5	12

ワンチップ処理

元の数字	盗まれたデータ	暗号化された数字
1	2	4
2	4	6
3	6	8
4	8	10
5	10	12

ツーチップ処理



HSMの技術的特性　一体型形成

一体型形成

セーフネットの社員でも、基本分解できないハメ殺し構造

どうしても分解したい！

上蓋をこじあける

HSMの技術的特性　一体型形成

一体型形成

セーフネットの社員でも、基本分解できないハメ殺し構造

どうしても分解したい！

上蓋をこじあける

中身のデータの全消去
タンパーイベント

HSMの技術的特性　真性乱数生成

真性乱数生成

暗号処理には高度な乱数システムが必ず必要。
一般的には暗号化鍵は巨大な数字であり、予測されないように作成された無作為なデータである必要がある

「物理的」な乱数の定義
生成された値が、1個前に生成された値との連続性を持たないこと

コンピュータは1と0で動作するが、1が“電気あり”、0が“電気なし”ではありません。“電気なし”だとコンピュータは止まります。メモリ上のデータもすべて消えてしまいます。
正確には、電圧が“高い”、“低い”であり、ようは一連の電気の流れが高い電圧と低い電圧を行ったり来たりしているだけで、全てつながっています。

HSMはこれらを特殊な方法で実装しており「真正乱数」といわれています。
この機能は暗号処理以外には、宝くじの番号抽選等でも使用されています。

日本では、マイナンバー制度のおけるリンクコードシステムが大量の乱数を使用する予定であり、需要を見込まれています。

HSMの技術的特性　改竄防止ソリューション

HSMからは鍵が漏洩しない

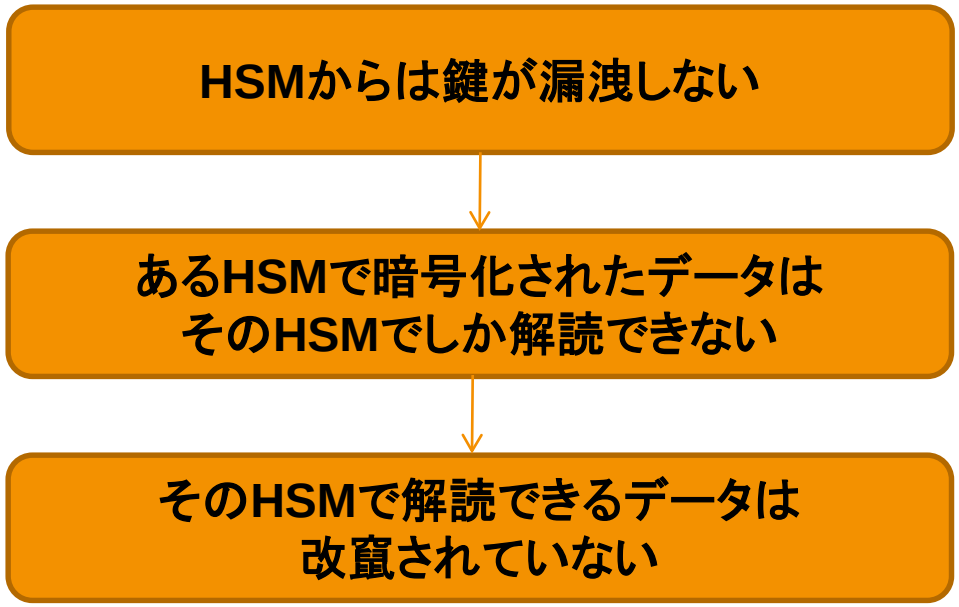
HSMの技術的特性　改竄防止ソリューション

HSMからは鍵が漏洩しない

↓

あるHSMで暗号化されたデータは
そのHSMでしか解読できない

HSMの技術的特性　改竄防止ソリューション



主な使用用途：

パスポート、運転免許証、ハイエンドネットワーク機器、ハイエンドプリンタ用トナー、BlueRay、ゲーム機、iPhone、intel IPTチップ

ご参考資料

基幹システムに“クラウド化の時代”は来るのか？
http://www.keyman.or.jp/kc/30006428/

基幹システムのクラウド化と“仮想化サーバ暗号”の特徴と懸念点
http://www.keyman.or.jp/kc/30006452/

クラウド利用における複数拠点の課題と「KMIP」という潮流
http://www.keyman.or.jp/kc/30006464/

HSMの仮想化技術とセキュリティ暗号「FIPS140-2」
http://www.keyman.or.jp/kc/30006474/

ハードウェア暗号モジュールの秘密と特性…結局、なんなの？
http://www.keyman.or.jp/kc/30006498/

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

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）:

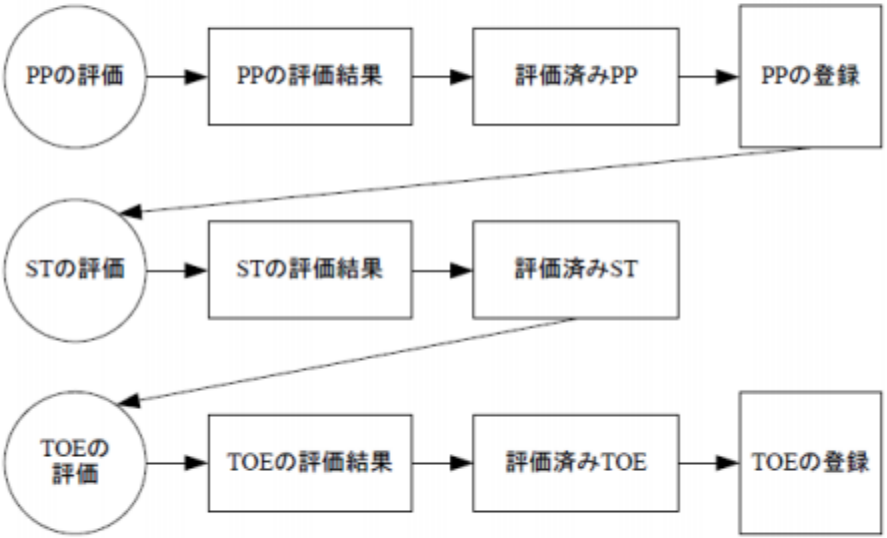
情報セキュリティ面での設計方針を厳密に記述した要件定義書を「セキュリティターゲット（ST）」と呼ぶ。
STは個々の製品ごとに開発者が作成し、同じ分野の製品であっても、相異なる製品であれば、STもまたそれぞれに作成されなければならない

- 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以上を審査可能な期間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？）