National Institute of
Advanced Industrial Science
and Technology
AIST

Research Center for
Information Security

# 暗号LSIの安全性評価に関する国際標準化の動向

(独)産業技術総合研究所
情報セキュリティ研究センター
ハードウェアセキュリティ研究チーム
佐藤　証

National Institute of Advanced Industrial Science and Technology
AIST

# ICカードのセキュリティ要件

1. ICカードが所有者以外に不正使用されないこと
2. ICカードが偽造されたり内部情報の改ざん・不正読出しがされないこと
3. ICカードとリーダおよびサーバーとの通信を第三者に傍受，改ざんされないこと

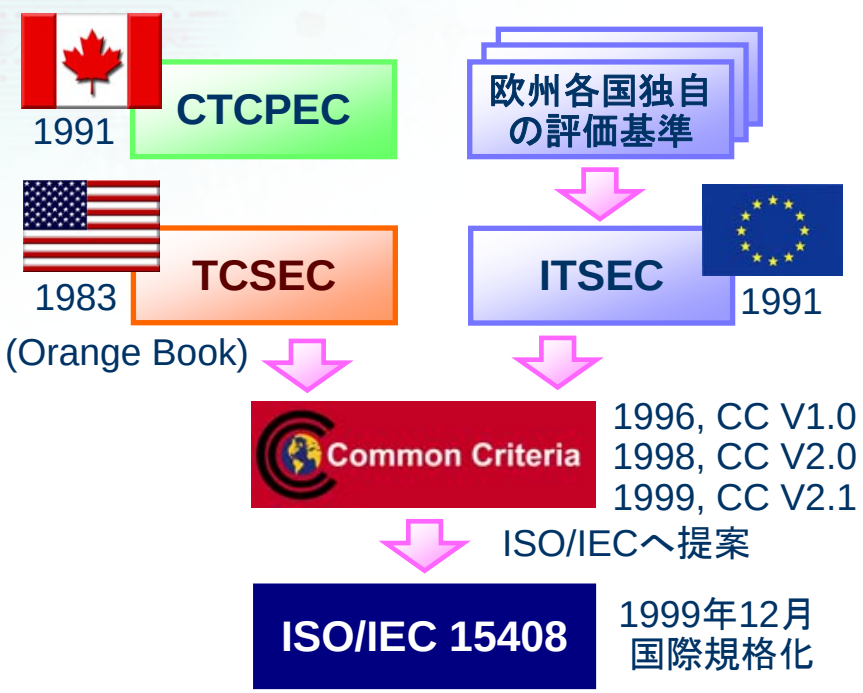
1. パスワードやPINコード，バイオメトリックスによる対策
2. ハードウェアによる物理的な対策
3. 暗号技術による理論的な対策

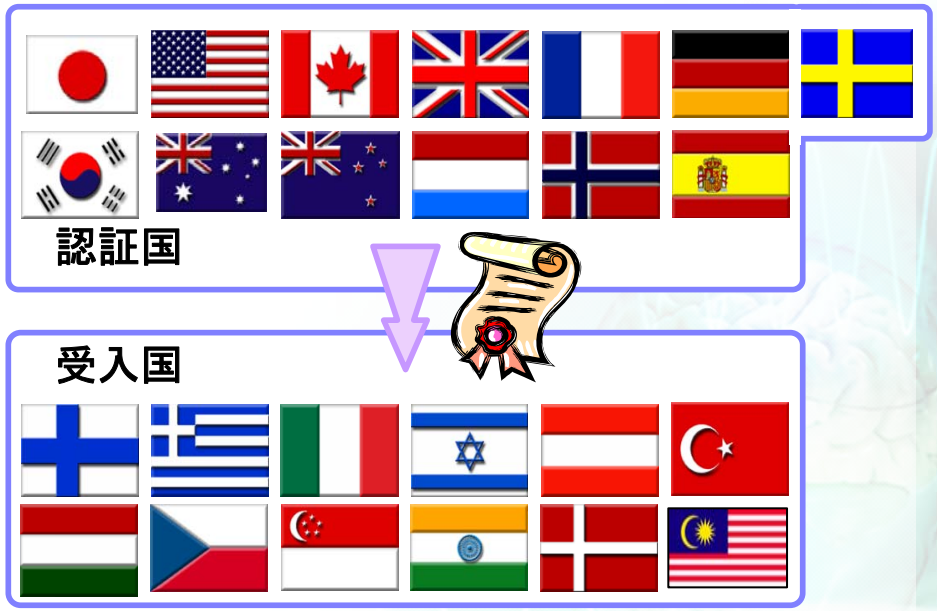
3. データ盗聴，改ざん防止
2. ICカードの偽造改ざん防止
1. 所有者以外の利用禁止

National Institute of Advanced Industrial Science and Technology
AIST

# ISO/IEC 15408 (Common Criteria)

- ISO/IEC 15408 はIT製品のセキュリティ要件と評価手法を定めた国際標準
- 1980~90年代に欧米諸国はIT製品の軍用・政府調達に独自のセキュリティ評価を実施
- 米国，カナダ，英国，フランス，ドイツはこれらセキュリティ評価基準の統一を目的に1996 年にCC V1.0 を策定，1999年12月にCC V2.1がISO/IEC 15408:1999として標準化された
- CCは評価の現状を迅速に反映するためISOよりも短いサイクルで規格を改定している
- CCRA (Common Criteria Recognition Arrangement)に加入する認証国（13ヶ国）で評価・認証されたIT製品は，他の認証国・受入国（12ヶ国）でも認証の効力を持つ




TCSEC : Trusted Computer System Evaluation Criteria
CTCPEC : Canadian Trusted Computer Product Evaluation
ITSEC : Information Technology Security Evaluation Criteria

National Institute of Advanced Industrial Science and Technology
AIST

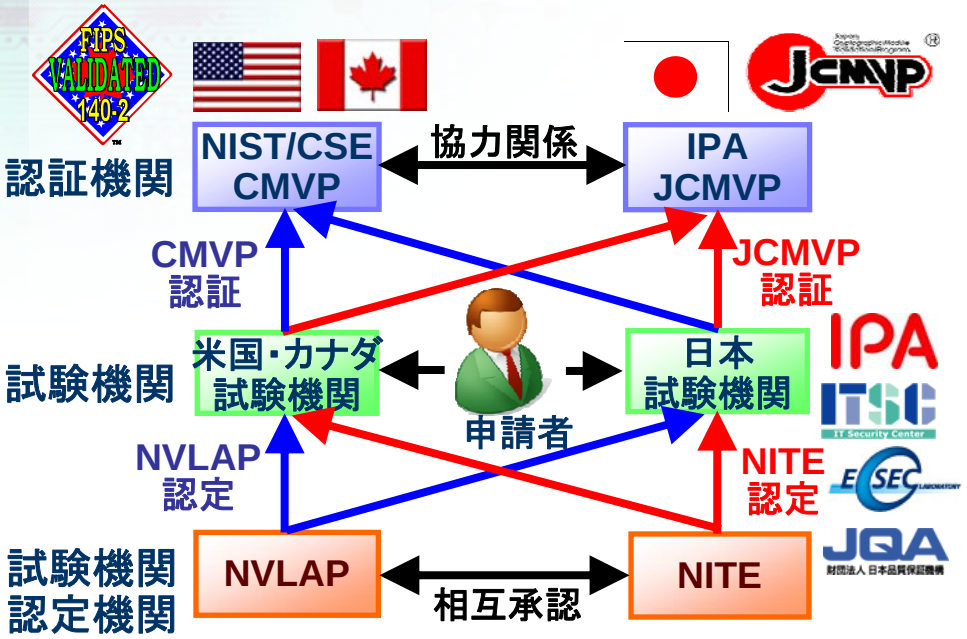
# ISO/IEC 15408 (Common Criteria)

- 保証レベルEAL( Evaluation Assurance Level)1~7はセキュリティ強度ではなく，STに記述された機能の信頼度を表し，高レベルほど確認範囲(証拠資料)が広く詳細度が深くなる
- CCRAによる相互認証はEAL1~4までで，より高いEAL は一部の国内限定で認証される
- 評価結果を比較可能とするための共通評価手法CEM (Common Evaluation Methodology)が開発され，現在EAL5までが規定されている
- ICカードはEAL4以上の取得が主流で，欧州を中心とするICチップメーカー，ユーザ，評価機関，認証機関で構成される作業部会であるJIL (Joint Interpretation Library) Hardware Attacks Subgroup (JHAS)が策定したICカードの物理セキュリティも補助文書が利用される
- 日本もIPAおよびECSECが中心となり業界団体をまとめて2009年にJHASに加盟

National Institute of Advanced Industrial Science and Technology
AIST

# ISO/IEC 19790 (FIPS 140-2 )

- 暗号モジュールのセキュリティ要件を11のカテゴリ毎に定め，“強度”に応じた評価を行う
- 11のカテゴリ毎のレベル1~4の中で最も低いものがその製品のOverall Levelとなる
- 国内ではISO/IEC 19790（JIS X 19790）に基づき，IPAが暗号モジュール試験及び認証制度JCMVP®(Japan Cryptographic Module Validation Program)を運用している
- JCMVPではCRYPTRECによる電子政府推奨暗号リストの暗号アルゴリズムが評価対象
- 申請者はNITEとNVLAP認定を受けたCMVP/JCMVP試験機関で試験を行うことで，将来CMVPとJCMVP双方の認証を受けることが可能に
- サイドチャネル攻撃を取り入れISO/IEC19790とFIPS140-3への改訂作業が同時進行している
- 攻撃のコストを重視した評価を採用の見込み




| FIPS 140-2 | |
|---|---|
| 1 | 暗号モジュール仕様 |
| 2 | 暗号モジュールのポートインタフェース |
| 3 | 役割，サービス，及び認証 |
| 4 | 有限状態モデル |
| 5 | 物理セキュリティ |
| 6 | 動作環境 |
| 7 | 暗号鍵管理 |
| 8 | 電磁妨害／電磁両立性(EMI/EMC) |
| 9 | 自己テスト |
| 10 | 設計保証 |
| 11 | その他の攻撃の対処 |

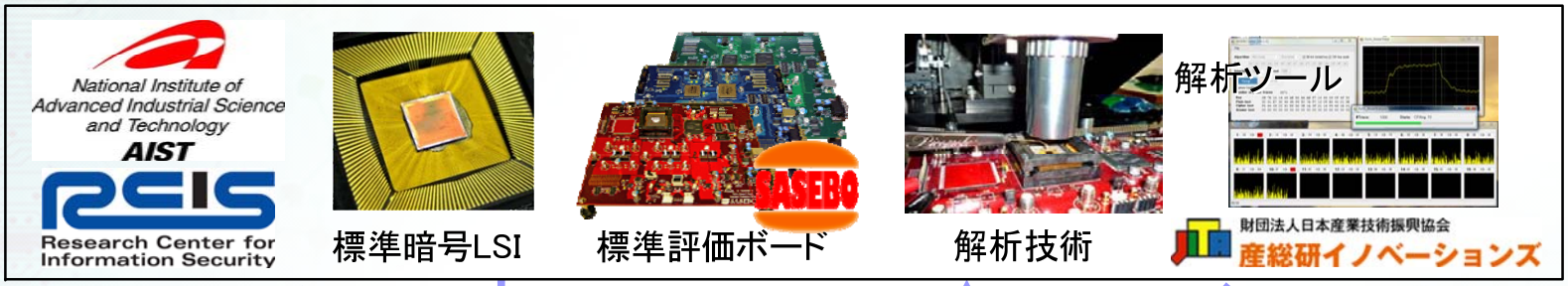
| FIPS 140-3 | |
|---|---|
| 1 | 暗号モジュール仕様 |
| 2 | 暗号モジュールのインタフェース |
| 3 | 役割，サービス，及び認証 |
| 4 | ソフトウェア・ファームウェアセキュリティ |
| 5 | 動作環境 |
| 6 | 物理セキュリティ |
| 7 | 物理セキュリティ(非破壊) |
| 8 | Security Sensitive Parameter 管理 |
| 9 | 自己テスト |
| 10 | ライフサイクル保証 |
| 11 | その他の攻撃への対処 |

CSE: Communications Security Establishment
NVLAP: National Voluntary Laboratory Accreditation Program
NITE: (独)製品評価技術基盤機構

National Institute of Advanced Industrial Science and Technology
AIST

# SASEBOプロジェクト

- 標準評価プラットフォームSASEBO(Side-channel Attack Standard Evaluation Board)を開発し国内外の70以上の研究機関が利用
- ICカード等の安全性評価ガイドライン策定に向けて国内外の研究機関と協力
- 開発したハードウェア・ソフトウェアを事業化し産業へ貢献




最先端技術 ↔ 標準実験環境提供 ↔ 技術サポート ↔ 技術移転

## 共同研究

- 東北大学
- 横浜国立大学
- 電気通信大学
- 中央大学
- 神戸大学

論文発表

## 学術貢献

国際会議運営

国内外の研究機関

新規解析技術

## 標準規格策定・運用

FIPS 140-3
ISO/IEC 19790
ISO/IEC 24759

電子政府暗号評価

海外供給
国内供給

## 事業化

ICカード解析ツール

ハードウェア開発

National Institute of Advanced Industrial Science and Technology
AIST

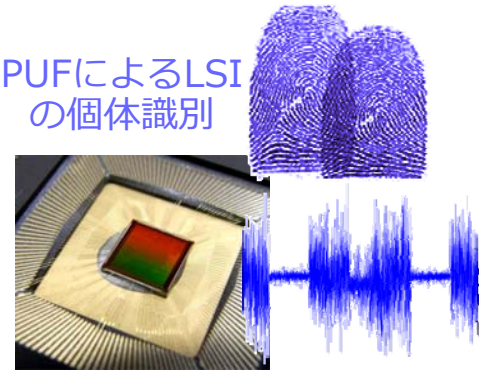
# LSIの偽造防止技術

- 半導体製品の模造品被害が深刻化し，偽物を見分ける技術の開発が急がれている
- SEMI（Semiconductor Equipment and Materials International）は，流通過程での模造品の混入防止のトレーサビリティ技術を仕様「T20」にまとめ，ISO化(TC246/247)を進めている
  - –第三者認証機関が発行した固有IDをメーカーが製品に付与し，製品データベースを管理
  - –IDの付与と管理は大量のID発行時にも数円/個の費用がかかることが課題の一つ
  - –2次元バーコード，ホログラムやRFID等の利用が見込まれるが，これも偽造が不可能ではない
  - –チップにIDをレーザー刻印したりナノインクでドットを印刷する技術等が開発されているが，特殊なマーキングや検査の装置が必要
- 人の指紋のように，LSI個々の特性のばらつきを利用して個体識別を行う技術PUF（Physically Unclonable Function ）の研究が進み，回路パターンやデジタルデータがコピーされても真贋判定が可能なためLSIの偽造対策等に有望視されている

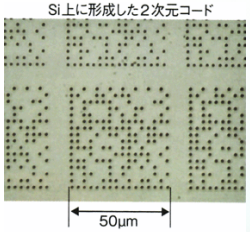
模造LSIの検出


日経エレクトロニクス
2010-04-19

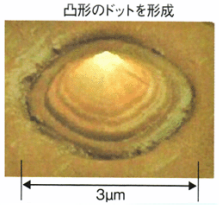
PUFによるLSIの個体識別



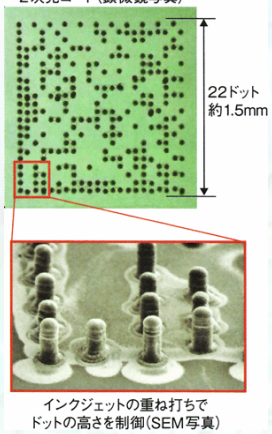
Si上に形成した2次元コード




凸形のドットを形成




2次元コード（顕微鏡写真）




インクジェットの重ね打ちで
ドットの高さを制御（SEM写真）

日経エレクトロニクス
2010-04-19

TC246: Project committee: Anti-counterfeiting tools
TC247: Fraud countermeasures and controls