セキュリティ製品認証制度の
エコシステム構築の重要性

独立行政法人情報処理推進機構（IPA）
セキュリティセンター　セキュリティ技術評価部

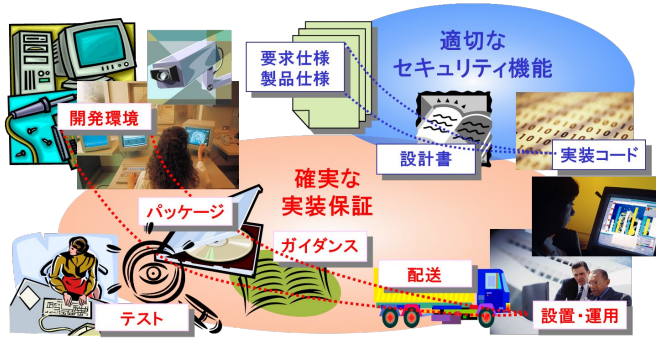
神田　雅透

JISEC認証制度 & JCMVP認証制度

ITセキュリティ評価及び認証制度（JISEC）

国際標準ISO/IEC 15408（Common Criteria）に基づき、IT製品・システムのセキュリティ機能の適切性・正確性を客観的に評価・認証する日本の制度

- セキュリティ機能がライフサイクル全般に渡って**適切に設計**され、**正しく実装**されていることを仕様書などを対象に客観的に検査
  - セキュリティ機能要件（特定した脅威・リスクに対抗するセキュリティ機能を適切に選択）
  - セキュリティ保証要件（セキュリティ機能の正確性をライフサイクル全体として保証）
- 保証要件の**評価検証の深さに依存**して評価保証レベルをEAL1～EAL7まで設定
- CC認証承認アレンジメント（CCRA）**加盟31ヶ国間で相互承認**を実施



暗号モジュール試験及び認証制度（JCMVP）

国際標準ISO/IEC 19790に基づき、暗号モジュールのセキュリティ機能等の確実性・安全性を客観的に試験・認証する日本の制度

- 暗号化機能、ハッシュ機能、署名機能等の**承認されたセキュリティ機能（暗号アルゴリズム）**が**正しく実装**されていることを客観的に検査
- セキュリティ機能、暗号鍵やパスワード等の重要情報を**適切に保護**していることを試験項目に従って客観的に検査
  - **試験する攻撃耐性に依存**して保護レベルをLev1～Lev4まで設定
- 相互承認スキームは**ない**

ITセキュリティ評価及び認証制度の設立背景
～ CC認証とJISEC認証との違い ～

※ COTS : Commercial Off-The-Shelf

- 欧米政府のCOTS（市販既成製品）調達におけるセキュリティ確保を目的
  - 1990年代前半：【調達主導型】
    主に軍事上の観点から、欧米では政府調達のセキュリティ要件を規定・提示
    → 開発者・製品ベンダがそれに従ったCOTS製品を開発、機能評価を依頼
    → 認証されたCOTS製品を政府が調達
    - 米：TCSEC（1983～通称：Orange Book）、英独仏蘭：ITSEC （1991～）、加：CTCPEC（1991～）
  - 1990年代後半：【国際標準化】
    国際的な製品流通と調達効率化のため、セキュリティ要件を統合した共通基準を作成
    - Common Criteria（1996）→ ISO/IEC 15408（1999） → JIS X 5070（2000）
  - CC認証書の相互承認協定：【相互承認】
    - 米加英独仏で相互承認MRAスタート（1998）→参加国増加に伴い、CCRAに改組（2000）
- 日本では調達に先立ち、国際標準準拠の制度として設立（2001年4月）
  - 他国調達か、開発者が自ら安全性の表明を目的として認証取得【ベンダ主導型】
    - ISO/IEC 15408, CC準拠。CCRA加盟（2003年）

暗号モジュール試験及び認証制度の設立背景 ～ CMVP認証とJCMVP認証との違い ～

■ 米国政府での安全な暗号装置調達のための認証プログラム

- FS-1027 (1982) → FIPS 140 (1988)
  - 通信機器用DES暗号装置での最小セキュリティ要件を規定した認証プログラム。一般調達局（GSA）開発
  - 1988年にNISTに移管し、FIPS 140を附番
- FIPS 140-1 (1994)
  - センシティブデータ保護に利用する全米国政府システムでの暗号モジュールが満たすべきセキュリティ要件を規定。11カテゴリのセキュリティ要件に再編し、4段階のセキュリティレベルを設定
  - FIPS 140-1認証プログラム開始18ヶ月後から認証済モジュールの調達義務化を予告
  - カナダ通信安全保障局（CSE）が参加し、暗号モジュール認証プログラム（CMVP）と命名
- FIPS 140-2 (2001)
  - FIPS 140-1以降の標準規格や技術などへの対応を考慮した改訂
  - ISO/IECに提案 → ISO/IEC 19790:2006発行 → ISO/IEC 19790:2006に準拠しないことを決定
- FIPS 140-3 (2019)／SP800-140x
  - ISO/IEC 19790:2012改訂 → ISO/IEC 19790:2012に準拠する改訂を実施

■ 日本では調達に先立ち、国際標準準拠の制度として設立（2007年4月）

- ISO/IEC 19790:2006発行に貢献

セキュリティ認証制度のエコシステム構築のために

- **「誰」**が**「何の目的」**で認証制度を必要としているのか
  - **開発者**が必要としている**目的**は何か
  - **購入者／調達者**が必要としている**目的**は何か
  - **スキームオーナーの目的（思い）は関係がない**
- 開発者は「どこまで」コスト（金額・時間・稼働）がかけられるのか
  - コストをかけて得られる**開発者メリット**は何か
- 購入者／調達者は「どこまで」コスト（金額）を負担する気があるか
  - コストに見合うだけの**購入者メリット**が得られるか
- 「どのような」スキームオーナーが必要か
  - どこまでの**認証（検証）レベル・認証（検証）能力**が必要なのか
  - **公平性・中立性・客観性**がどこまで必要か
  - **相互認証**が必要なのか

認証「目的」とベンダが「負担できるコスト」の関係

Why do customers certify?

強制要件対応

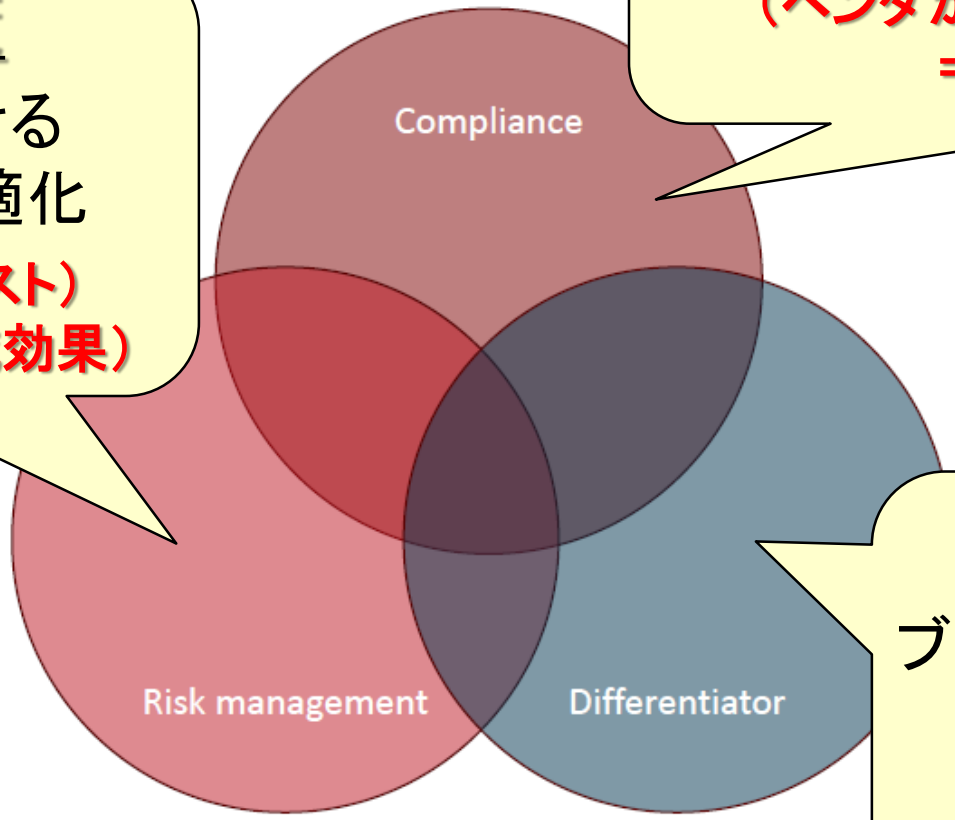
守らなければそもそも市場に参入できない

（ベンダがかけられるコスト）
＝（要件を満たすために必要なコスト）

リスク管理策

リスク対策にかける
費用対効果の最適化

（ベンダがかけられるコスト）
＜（リスク軽減効果）



差異化・差別化

ブランドアピール／ブランド力向上による収益増化

（ベンダがかけられるコスト）
＜（ブランド価値=収益増）

7