THALES（タレス）紹介資料

東京エレクトロン デバイス株式会社
CNカンパニー

HSM – Hardware Security Module

THALES

■ 暗号鍵の生成・保管専用の耐タンパ性のハードウェア

- **耐タンパ性** ： 容易に外部から解析を試みるような非正規な手段による機密データの読み取りを防ぐ能力

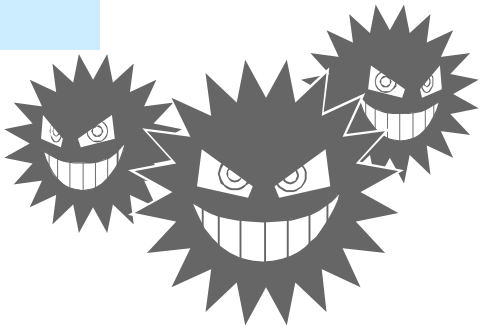
HSMは、ハードウェア的に機密データを保護し、外部から読み取ろうとすると機密データを破壊する仕組みが一般的

■ セキュリティは、NISTのFIPS 140-2の認定レベルで規定

- **FIPS 140-2** ： 米国標準技術院(NIST) 策定の、暗号モジュールの安全性に関する米国政府調達基準

■ Common Criteria EAL4+の認定

- **Common Criteria** ： 情報システムのセキュリティの要求仕様を示し、開発し、評価するというプロセスが厳密な方式で行なわれたという保証する国際的なセキュリティ評価基準



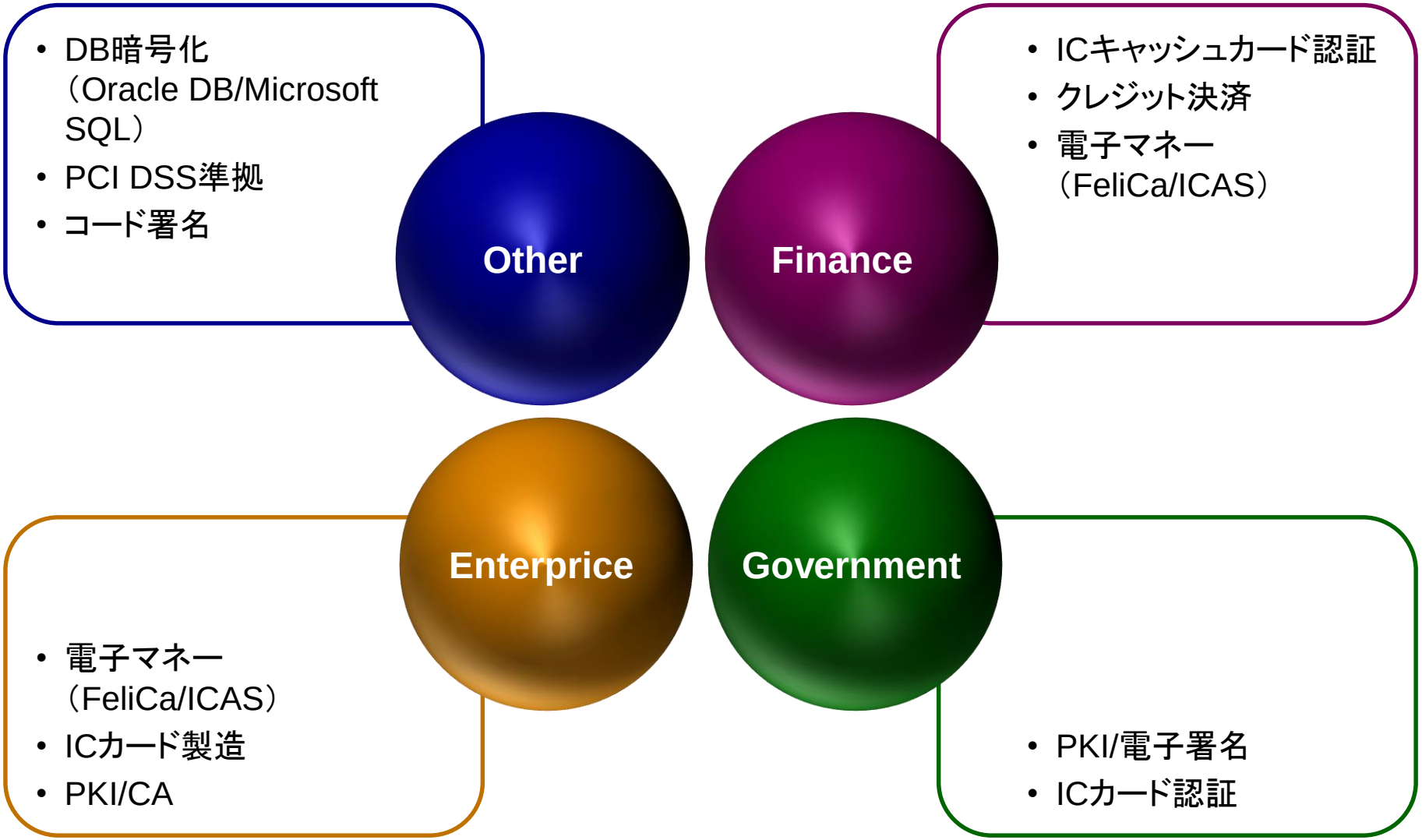
THALES社 HSM製品nShieldの特徴

- 暗号鍵を安全に保護するHSM
  - FIPS 140-2 Level 2 / Level 3認定　(Level 2か3かは機種に依存)
  - Common Criteria (ISO/IEC 15408) EAL4+認証も取得

    コンピュータセキュリティ製品の要求仕様を示し、開発し、評価するというプロセスが厳密な方式で行なわれたという保証を提供するもの
- 暗号鍵管理を提供するセキュアなハードウェア
  - 耐タンパ性（内部データの物理的な読み取り防止）
  - RSA高速演算機能（アクセラレーション）
  - ECC高速演算機能（アクセラレーション）
  - ハードウェア乱数生成器を使用した乱数・暗号鍵の生成
  - スマートカードを用いたアクセス制御
- 多くの暗号アルゴリズムをサポート
- アプリケーション自体も隠蔽可能 (CodeSafe機能)
- 異なるサーバOS間での鍵管理の共有可能

日本におけるnShield HSMの実績

THALES



東京エレクトロン デバイス株式会社

THALES社 nShield HSM製品概要

THALES

■ nShield Solo+

– カード型HSM

■ nShield Connect+

– ネットワーク型HSM

■ nShield Edge

– USB型HSM

■ 開発ツールキット（SDK）

– CipherTools開発者ツールキット
– CodeSafe開発者ツールキット
– payShieldオプション

東京エレクトロン デバイス株式会社

HSM使用例

Webシステム

- Webサーバーの秘密鍵の保護
- SSLアクセラレーション

認証局

- 認証局の署名鍵の保護
- 署名処理のアクセラレーション

カード発行システム

- マスター鍵の保護

データベース暗号化

- マスター鍵の保護
- データ暗号化鍵の高速暗号化

HSM使用例（CodeSafe/SEE）

- **CodeSafe Secure Engine**
  - アプリケーションコードをHSM内部で実行
  - パスワード処理、SSL処理、独自暗号アルゴリズムなどを保護

お問い合わせ

THALES

- お問合せは: 東京エレクトロン デバイス株式会社
  CN第一営業本部
  パートナー第一営業部
  fj-sales@teldevice.co.jp
  03-5908-1962