情報社会は
リスクと如何に向き合うべきか

平松　雄一
電子商取引安全技術研究組合（ECSEC）
JSSM　常任理事

“個”の定義

これまでの“個”は各種規制前提で定義　消費者＝社会的弱者

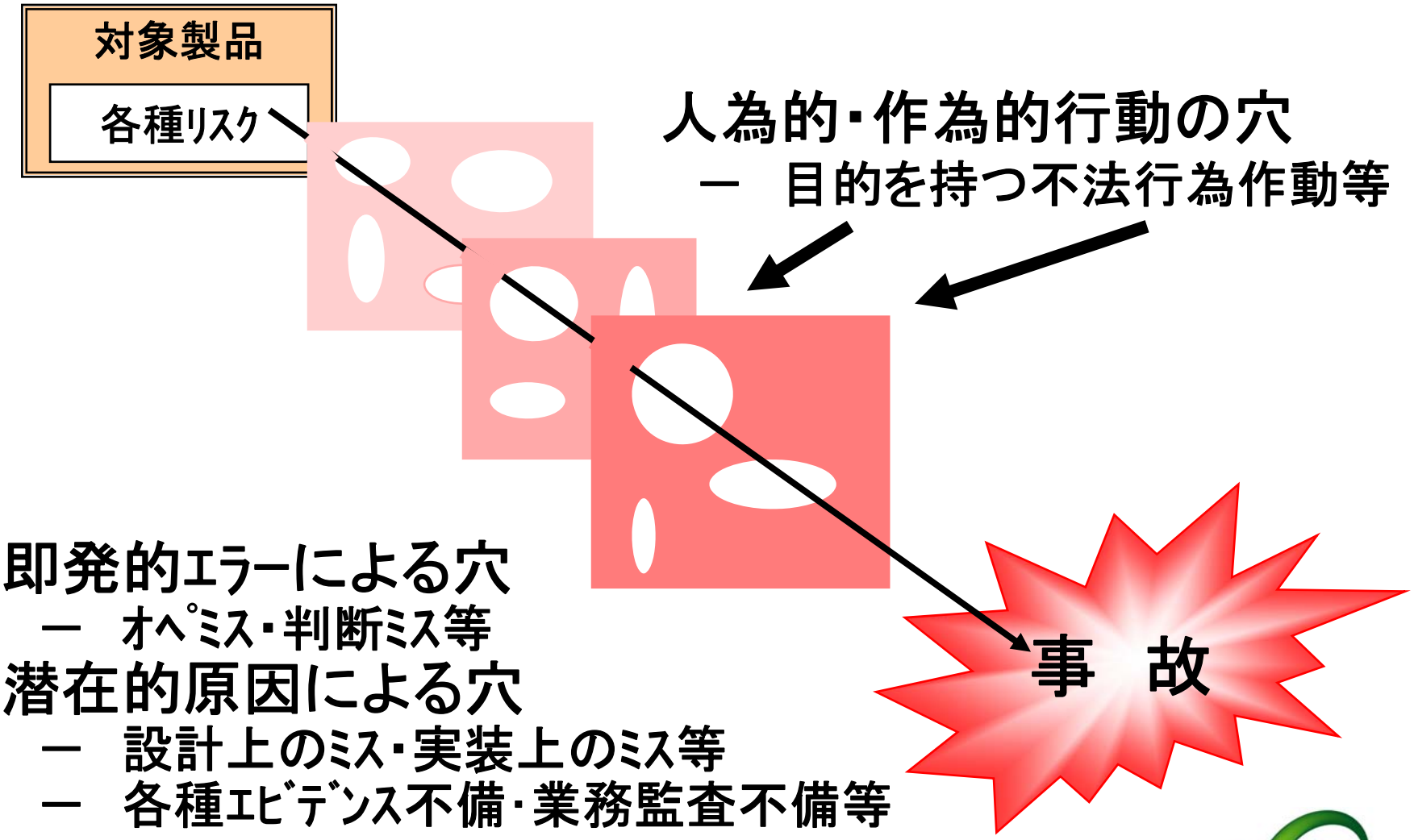
規制緩和が進む現在、新たな表現が必要
「消費」は「生産」に対峙する経済行為
“個”は「消費」のみを意味するのではなく「生活」を営む人

“個”＝　生活者／行動する者

生活の基本が「人間の自己生産であることを自覚しているもの」であり、「時間と金銭における必要と自由を設定し、常に識別し、あくまでも必要を守りながら」、大衆消費社会の「営利主義的戦略の対象としての、消費者であることを自ら最低限に止めよう」とする人々である。　・・・　経済学者　大熊信行（1893－1977）

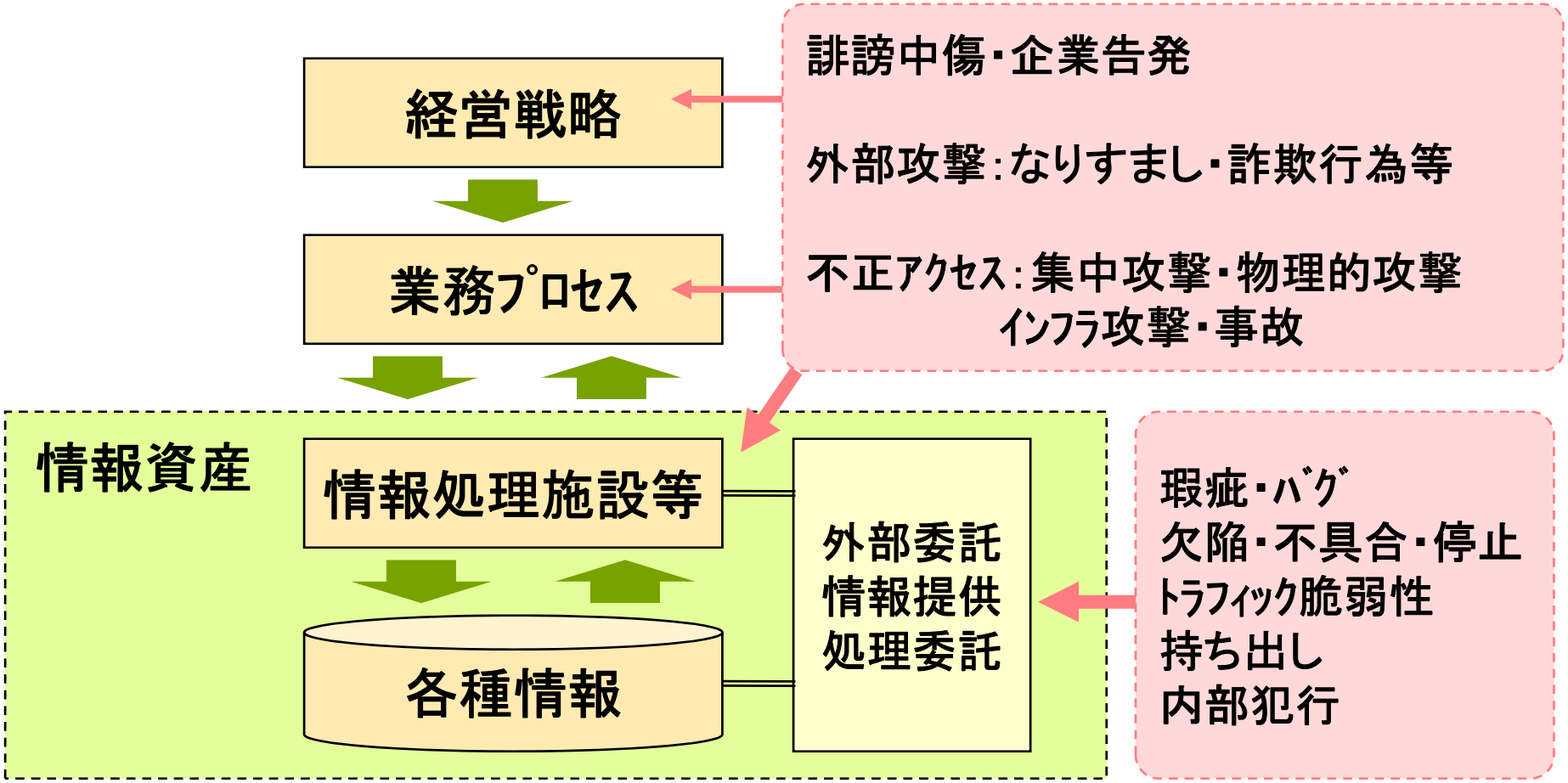
ユビキタス社会における“個”は、
“権利”“責任”“義務”の対応如何で行動範囲が決まる。

事故発生の共通点



予想される攻撃・リスク

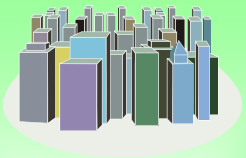
企業・組織活動



今後3年間の重点政策

政府機関・
地方公共団体

重要ｲﾝﾌﾗ



企業

個人

目標	情報ｾｷｭﾘﾃｨ対策の「ﾍﾞｽﾄﾌﾟﾗｸﾃｨｽ」へ	国民生活・社会経済活動の基盤としての安定供給の確保	市場に評価される情報ｾｷｭﾘﾃｨ対策の実施	IT社会の担い手としての意識の向上
個別設計図	政府機関統一基準	重要ｲﾝﾌﾗ行動計画	各省庁による施策	各省庁による施策

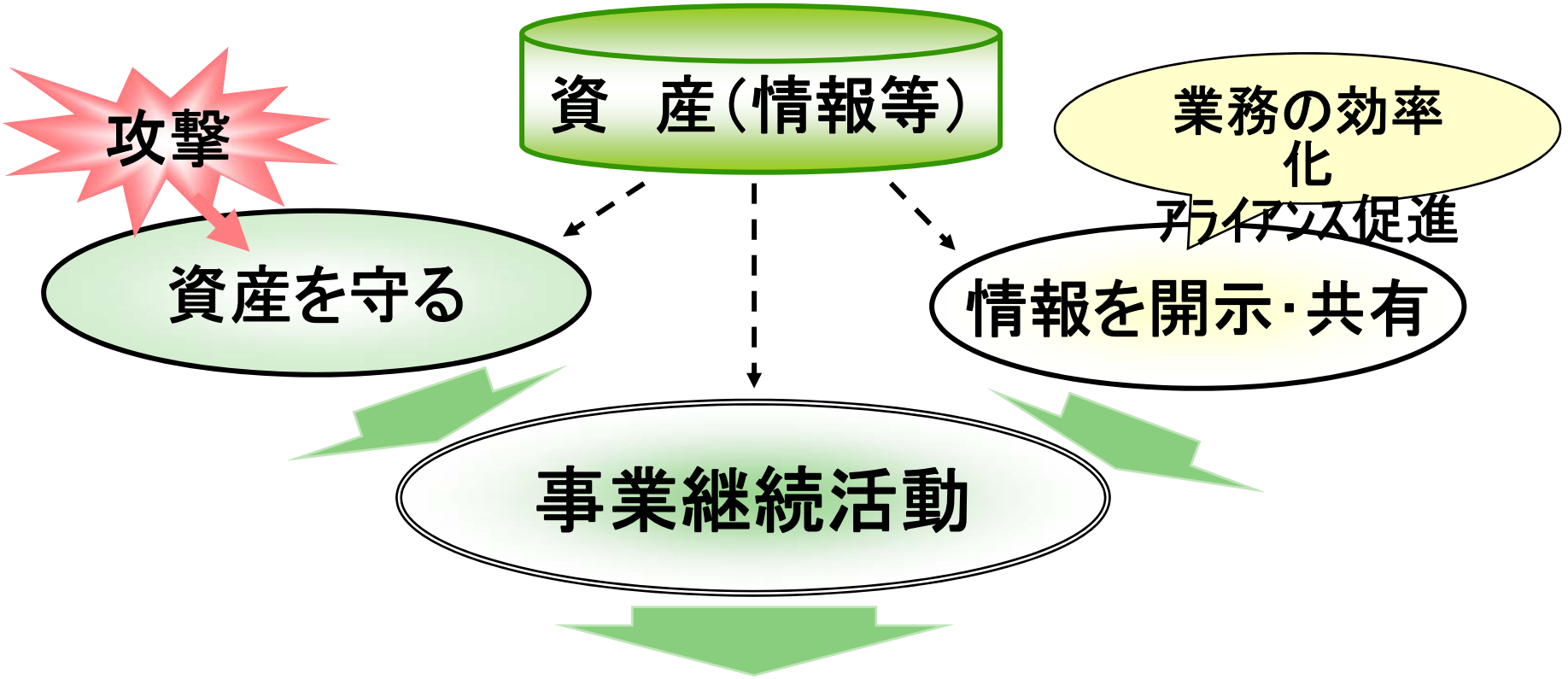
横断的基盤の形成

- 情報ｾｷｭﾘﾃｨ技術戦略の推進
- 情報ｾｷｭﾘﾃｨ人材の育成確保
- 国際連携・協調の推進
- 犯罪の取締り、権利利益の保護救済

分野別の重点政策

- 政府機関・地方公共団体
  - 政府機関統一基準に基づいた各省庁の評価
  - ｻｲﾊﾞｰ攻撃等への緊急対応能力の強化
- 重要ｲﾝﾌﾗ
  - 情報共有・分析機能の整備
  - 重要ｲﾝﾌﾗ連絡協議会の設置
  - 分野横断的な演習、相互依存性解析の実施
- 企業
  - 政府調達における入札条件の整備
  - 情報ｾｷｭﾘﾃｨ監査等第三者評価制度の活用推進
  - ｺﾝﾋﾟｭｰﾀｳｨﾙｽ等への対応体制の強化
- 個人
  - 情報ｾｷｭﾘﾃｨ教育の推進
  - 「情報ｾｷｭﾘﾃｨの日（2月2日）」の創設等広報啓発の強化
  - ﾕｰｻﾞｰﾌﾚﾝﾄﾞﾘｰなｻｰﾋﾞｽの提供等の環境整備

企業・組織運営における行動



情報資産を守り、かつ情報の戦略的活用を促進
＜組織力向上＞

“モノ造り”における情報セキュリティへの対応

サービス提供者（調達者）の考え得る範囲で、セキュリティ対策について開発者へ提示
- 脅威の調査
- パスワード管理
- 監視体制
- 暗号化
- ログ管理等

これまで

- トータルな視点から対策を立てられず
- 対策に漏れが生じる可能性
- 調達の都度対策を考え、開発者に要請
- 客観的にその対策の妥当性確認できず

セキュリティ対策に不安内在

これから　“コト”が起こる前に

調達時ISO/IEC 15408の考え方導入
- 適切なセキュリティレベル満たした製品/システムを効率的に調達可能

- ISO/IEC 15408 認証済み製品調達
- PPを提示し、セキュリティ対策項目明示
- 0から対策項目を検討する必要ない
- 第三者機関により妥当性を評価

国際標準に準拠した信頼性の高いセキュリティ水準を確保

金融機関における評価認証制度

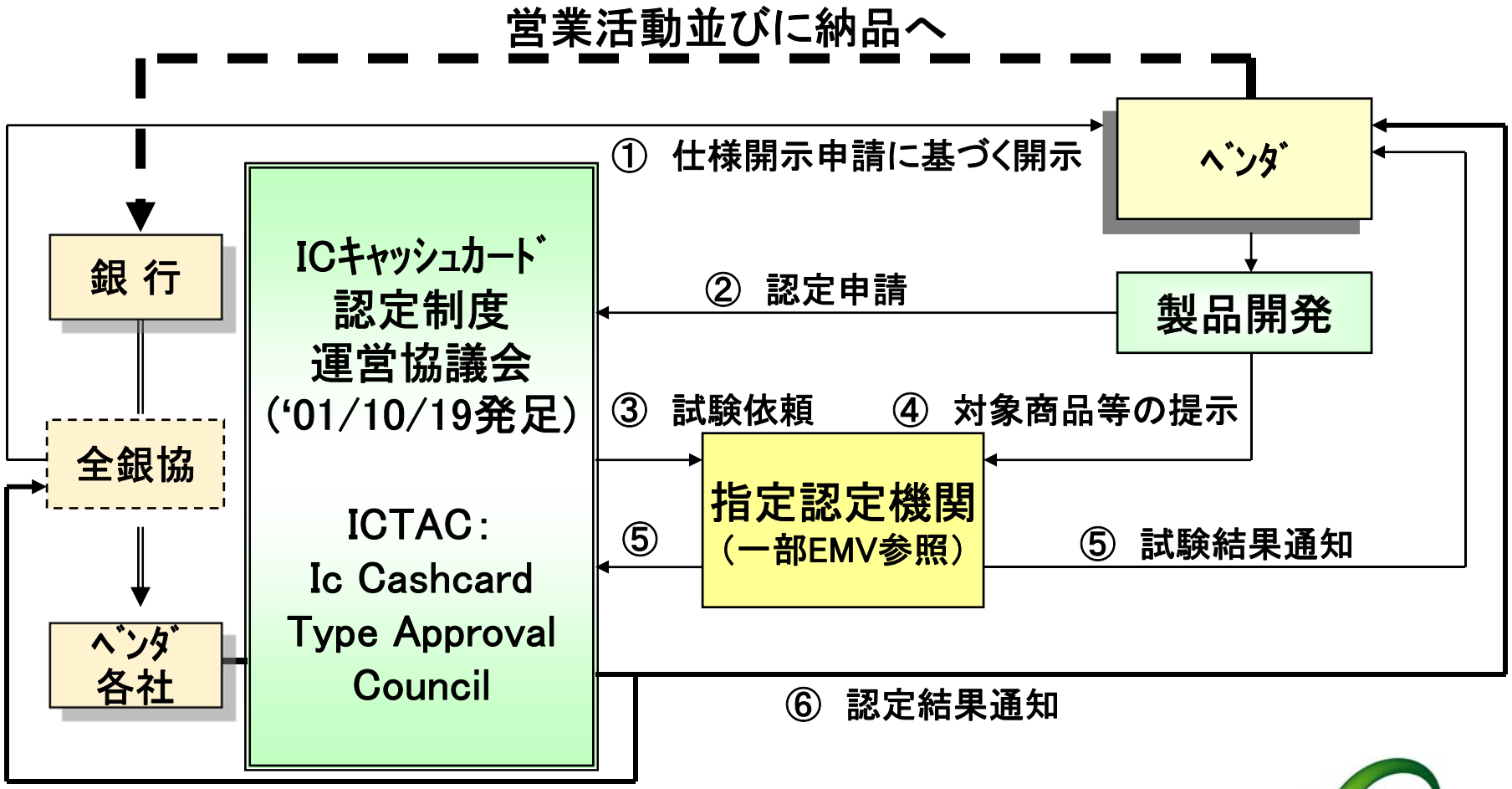
- 金融機関における相互運用性の確保
  - セキュリティ・顧客利便性に優れたICカードの普及
  - ICカード・関連機器・システムベンダー等の開発コストの低廉化
  - 標準化対象業務・・・他業界で定めていない業務
    - ① 国内キャッシュカード業務
    - ② 国内デビットカード業務（オンライン/オフライン）
- 金融機関の自由な創意による商品開発の確保
  - 標準仕様では
    - ① 業務仕様・・・業務内容・ユーザ要求
    - ② 技術仕様・・・国内ネットワーク環境下での必要技術要件

    定期見直し（5年程度毎に）実施

  を制定

ICキャッシュカード認定制度運営協議会

目的：標準仕様に基づくICカード・関連機器の相互運用性の確保



IC乗車券システムにおけるセキュリティ確保

- 利用の側面、並びに運用・製造者の側面で多くの脅威が想定される。
- 規則・組織等の整備を徹底しても、システム自体に脆弱性が存在すると安全とは云えない。
- 共通IC乗車券システムは、運用者が多岐にわたると共に、利用者は一般市民。

セキュリティ確保の必要性

IC乗車券システムに対するセキュリティ確保は社会的責務

誰 が 検証・認証

① 鉄道事業者（調達者）自ら検証 ⇒ 技術的・時間的に不可能
② 開発ﾍﾞﾝﾀﾞｰ（製造者）自ら検証 ⇒ コストとの兼合いから検査が手抜きとなるおそれ
☞ ③ 第三者（中立的立場）検証 ⇒ 信頼性の高い検証が継続的に可能

認　　定

第三者認証によりセキュリティ確保 ・・・ 安全性・信頼性・互換性等々

⇓

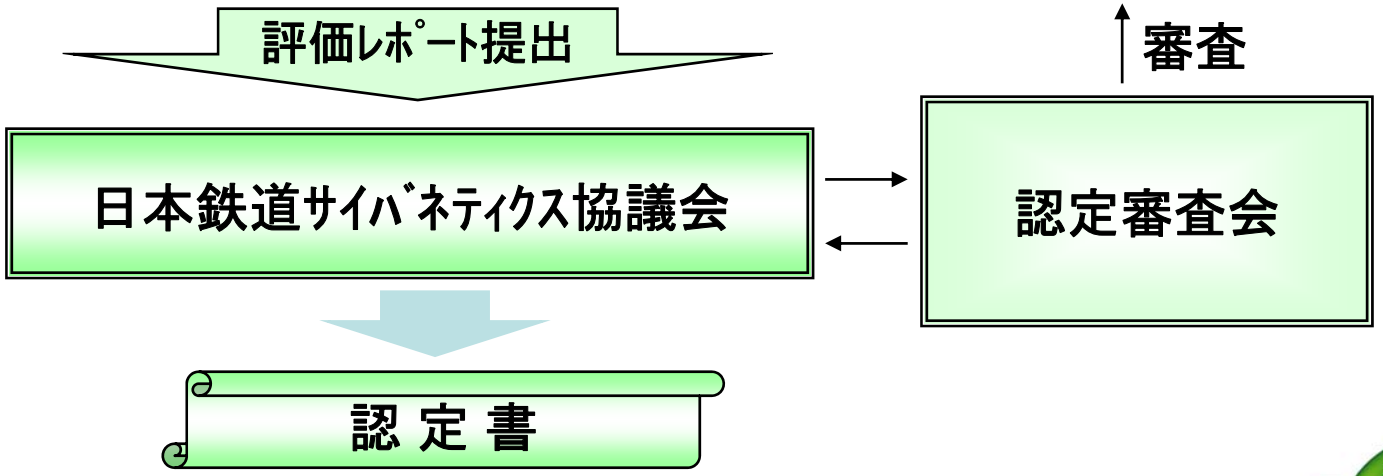
機器評価・認証機関創設

参考事例 ： 銀行業界における「ICｷｬｯｼｭｶｰﾄﾞ認定制度（ICTAC）」
EMV 等

機器評価・認定制度の創設

第三者評価機関の役割

共通IC乗車券基本仕様に準拠した基本セキュリティ要求仕様書（PP）の作成
基本セキュリティ要求仕様書に基づくシステム・機器（カード・端末等）の評価
・カード（物理的・電気的・論理的仕様）に対する評価
・端末（物理的・電気的・論理的仕様）に対する評価
・アプリケーション機能に対する評価
・相互互換性の評価(カード・端末機・レスポンスタイム等を対象)

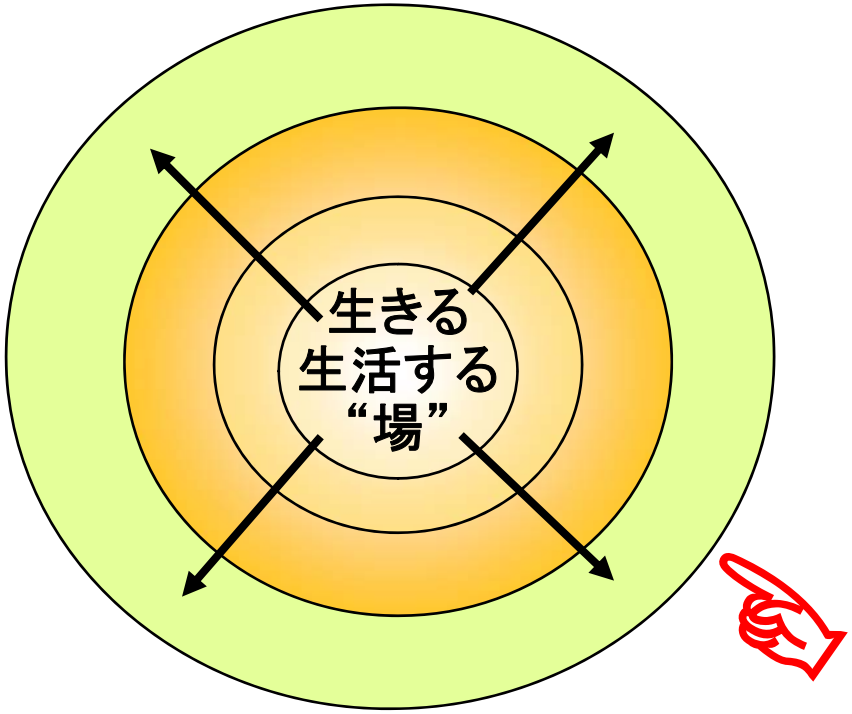


必要となる情報倫理

- 情報倫理、
  「情報の処理･加工、記憶･蓄積、及び交換･伝達に関する情報行動において、人間として行うべき、または行ってはならない原理･原則」
  セキュリティハンドブックⅢ（日本情報セキュリティマネジメント学会編）
- 人間が分担する“人的情報システム”
  情報技術が介在する“情報システム”
  ⇒ この双方で“情報倫理問題”は発生
- 情報倫理対応の階層
  - 個人レベル
  - 企業/組織レベル
  - 国家/社会レベル
  - 国際レベル

まとめ

1. 情報セキュリティ/情報倫理が最重要課題
   ― 専門職の倫理観を持った行動必須
2. 自律性
3. 行動規範の遵守
   ① 個人規範
   ② コミュニティ規範
   ③ 組織規範
   ④ 専門職規範
4. 専門性を支える柱
   ① 献身
   ② 誠実
   ③ 責任
   ④ 説明責任



安心･安全･信頼をﾍﾞｰｽに生活できる
社会構築へ積極的に行動 ！