1

ｾｷｭﾘﾃｨの日「第2回JSSMｾｷｭﾘﾃｨ公開討論会」

基調講演 2
リスク低減の社会的枠組み

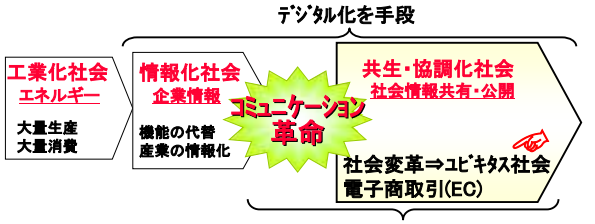
1. 社会構造の変化と現在起きていること
2. ﾘｽｸと安心確保への行動
3. “ﾓﾉ造り”の変化と社会的枠組み

平松 雄一
電子商取引安全技術研究組合(ECSEC)
JSSM 常任理事

2

1. 社会構造の変化と現在起きていること

ﾃﾞｼﾞﾀﾙ社会からﾕﾋﾞｷﾀｽ社会へ

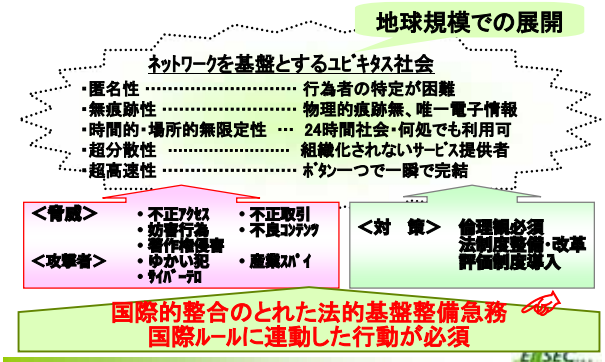


ITﾃｸﾉﾛｼﾞｰをｿﾘｭｰｼｮﾝとして安心・安全・信頼の確保

社会構造の連続性維持
ﾎﾞｰﾀﾞﾚｽ化・ｱﾅﾛｸﾞ/ﾃﾞｼﾞﾀﾙ・対面/非対面

3

ﾕﾋﾞｷﾀｽ社会の特徴

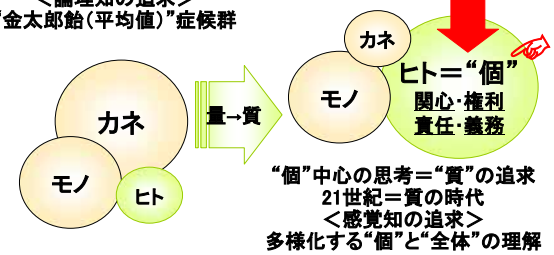


4

「量の世界」から「質の世界」へ

“カネ”中心の思考＝“量”の追求
20世紀＝量の時代
＜論理知の追求＞
“金太郎飴(平均値)”症候群

個々のﾓﾁﾍﾞｰｼｮﾝにより2極化

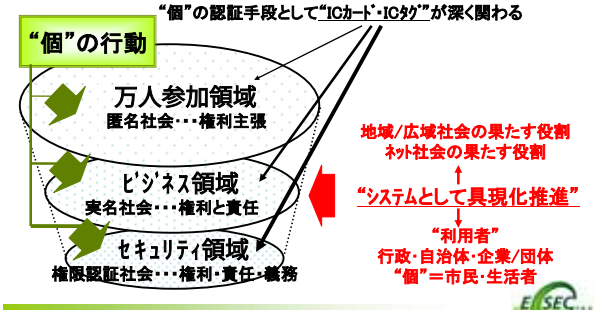


“個”中心の思考＝“質”の追求
21世紀＝質の時代
＜感覚知の追求＞
多様化する“個”と“全体”の理解

5

ﾕﾋﾞｷﾀｽ社会における“個”の階層化

ﾈｯﾄﾜｰｸを基盤とするﾕﾋﾞｷﾀｽ社会：非対面と対面の同居



6

情報犯罪の全体像とその影響

- ﾎｰﾑﾍﾟｰｼﾞ改竄
- 不正ｱｸｾｽ
- 頻発するｳｨﾙｽとその多様化
- なりすまし/詐欺
  - 振り込め詐欺/ﾌｨｯｼﾝｸﾞ・ﾌｧｰﾐﾝｸﾞ詐欺
  - 媒体改竄 ・・・ ｶｰﾄﾞ・ﾌｧｲﾙ等
- 情報漏洩 ・・・ 内部犯罪/外部攻撃
  - 企業情報 ・・・ 機密情報・営業情報
  - 個人情報
  - 情報の持ち出し
- 関連者間での情報紛失
- ｼｽﾃﾑ破壊
- ﾎｰﾑﾍﾟｰｼﾞを“場”とする告発・中傷
- ｻｲﾊﾞｰ犯罪 ・・・ ﾓﾊﾞｲﾙ機器の脅威
- ﾄﾗﾌｨｯｸ脆弱性への攻撃
- 設計/実装上のﾐｽ
- ｵﾍﾟﾐｽ・判断ﾐｽ 等々

企業・組織が失うもの/問われるもの
・信頼
・ﾌﾞﾗﾝﾄﾞ
・経営管理能力
・緊急対応姿勢
・対応ｺｽﾄ
・情報資産 等々

2. リスクと安全確保への行動

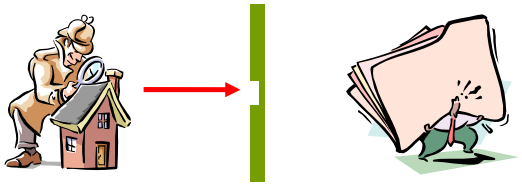
脅威と脆弱性あるところにリスクあり

7

脅威
弱点を狙うもの

脆弱性
それ自身が持っている弱点

リスク
所有者に対する不利益



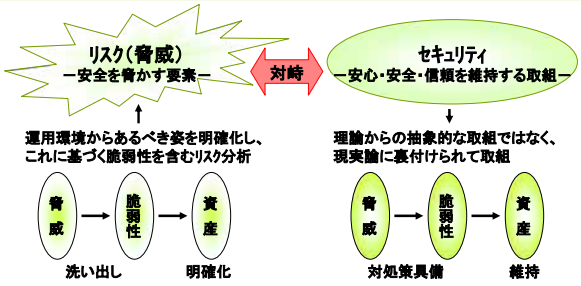
情報資産に何らかの損失を与える可能性がある事象

想定していない方法や、異なる目的での利用を可能とする、情報資産が持つ特性

情報資産に損失を与え得る、予想不可能な事象が起こる可能性

リスクとセキュリティの関係

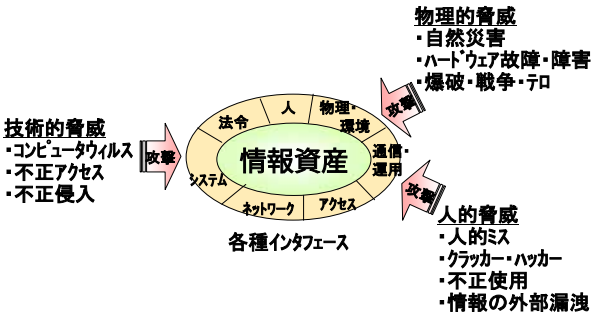
8



セキュリティは、まずリスク認識の啓発による“認識の原則”、そして行動主体の責任明確化による“責任の原則”、これが2002.7.25.改訂のOECDセキュリティガイドライン
ここから“セキュリティ文化（Culture of Security）の熟成が開始されている

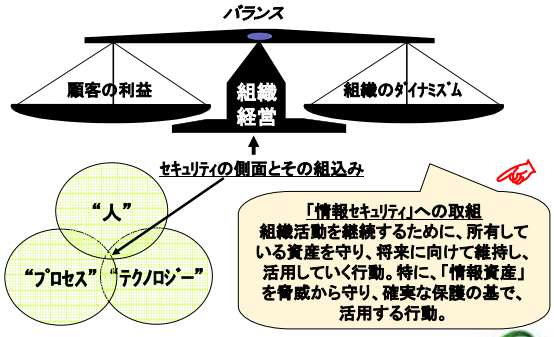
守る対象（情報資産）と各種脅威

9



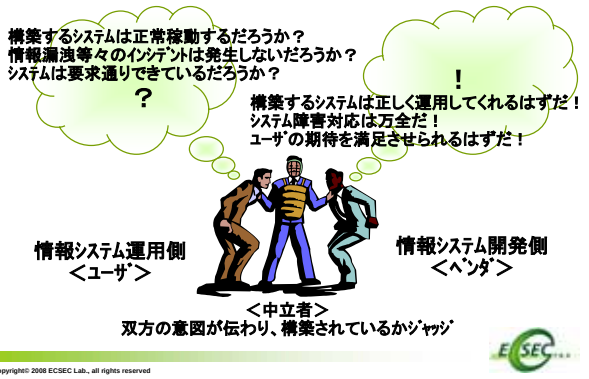
正しいセキュリティ導入が鍵

10



情報セキュリティ確保における課題

11



欧州における情報化への取組み姿勢

12

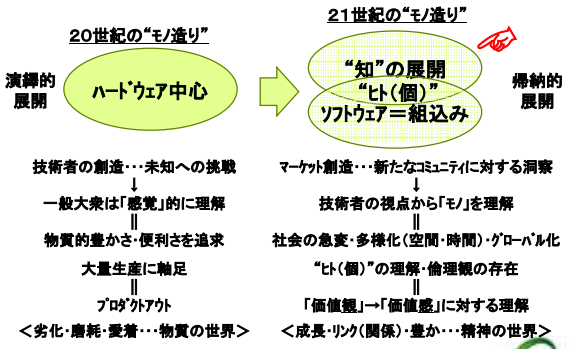
－日常生活に根ざした展開－

- 新たな情報通信手段の導入において、日常生活パターンを変えることなく、自然体での受け入れを前提
- 受入までに時間が必要であり、目標期限に振り回されず、着実な導入姿勢を堅持
- 常に、対象とする顧客に対し、安全・信頼等を維持するため、セキュリティ面へ配慮。セキュリティに対応する姿勢は、
  ① 事業者自身が、セキュリティ対策を計画・推進 ・・・ フランス・ドイツ等
  ② セキュリティ機能はベンダーに依存、具備された製品を調達 ・・・ 英国
- 特に、日常生活に密着した重要手段に対しては、利用者の立場を分析・理解し、新たなサービス展開に向け着実な展開

3. “モノ造り”の変化と社会的枠組み

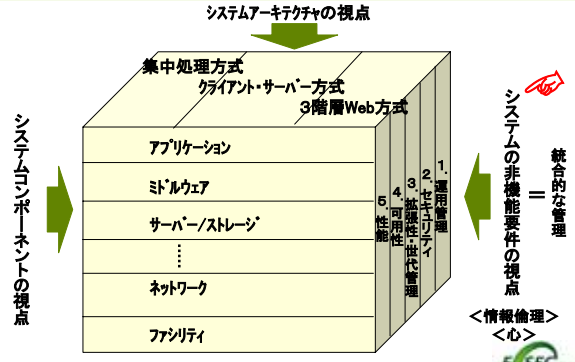
“モノ造り”の変化

13



“モノ造り”時に必要な視点

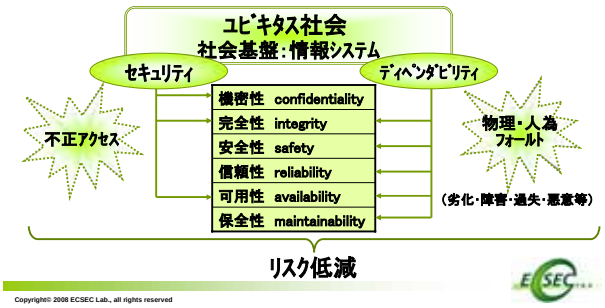
14



利用者視点との融合

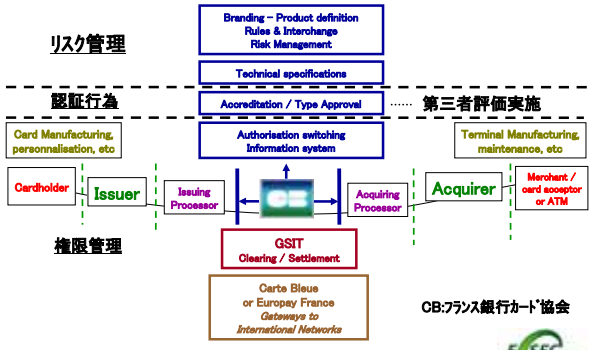
15

- ニューディペンダビリティ
  情報システムのセキュリティとディペンダビリティを、社会システムにおける利用者視点で融合



仏・CBシステムのスキーム

16



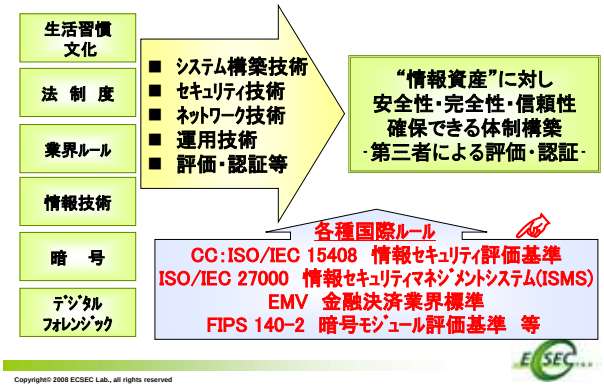
業界ルールとその下での競争

17

- 業界ルール
  1. 銀行相互間取引定義、技術標準化、機器型式認定(カード、端末、プロトコル)
  2. VISA/マスターカードとGSIT(国内精算センタ)との互換性保持
  3. セキュリティとリスク管理は第三者機関チェック
     - SICB：VISA/マスターカード対応銀行とCB発行銀行との情報処理
     - e-rsb:国内認証とネットワーク
  4. 銀行間の決済ルール…手数料等
  5. 契約書類のひな形
     - 銀行とカードホルダー間
     - 銀行と加盟店間
     - 欧州規定のモニタリング
  6. 加盟店と消費者連合との協調維持
- 国内は総てデビット取引、海外ではVISA/マスターと連携したクレジット取引…クレジットが搭載されていないCBが基本
- 加盟銀行は、以下の事項を尊重し、個々独立に行動
  マーケティングポリシー　顧客関係　カード発行　加盟店関係
  手数料　取引処理

リスク低減への行動

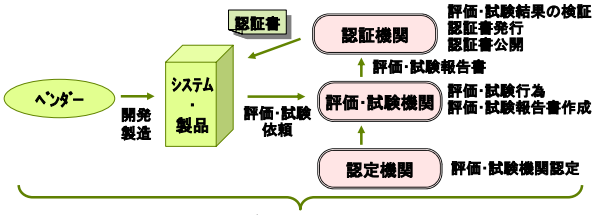
18



第三者による評価・認証制度

19

- 特定の環境で利用されるシステム・製品が、想定される脅威に対して適切な対策が講じられていることを、中立な立場で評価し、その結果を認証する。



国際ルールに基づき実施 ・・・ 信頼性維持

企業・組織はリスク低減に的確な認識

20

- セキュリティに対する認識
  - 守るセキュリティ ・・・ クローズド領域からオープン領域へ
  - 生かすためのセキュリティ ・・・ セキュリティのないところに価値が生まれない
  - 保証するセキュリティ ・・・ 社会的メカニズムの要求
  - 投資するセキュリティ ・・・ “コト(事・混乱)”が起きる前の対策
- 対処療法的対策からの脱却
  - 自律的継続的取組み
  - 事業継続における重要要素
  - 企業価値の向上
- “法”に対する積極的理解
  - 情報倫理観を持った対応
- “法”と“技術的手段”のバランス ・・・ ダイナミック コラボレーション
- 情報セキュリティ ガバナンスの確立
- 形式的“マーク取り”からの脱却
- 認証基盤の整備・確立

企業・組織が取組むべき姿勢

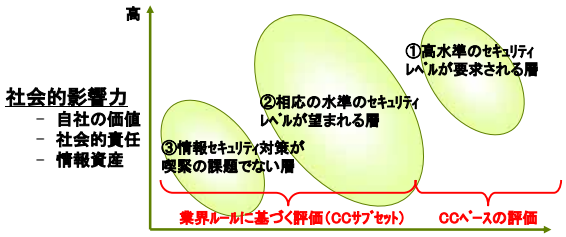
21

- 高度にネットワーク化されたユビキタス社会では、企業・組織の事故によるトラブルが社会・経済全体に影響を及ぼす可能性が大。従って、企業・組織の情報セキュリティ確保は、自身の被害の局限化や法令遵守に留まらず、社会を構成する一員として企業・組織の責務。
- 確立した情報セキュリティガバナンスの基、「あるべき姿」に向かって、自律的・継続的に改善・向上することで、事業継続。
  - 事故前提に事業継続計画:BCP (Business Continuity Plan) 策定
- 行動としては、
  1. 技術的手段の適用推進
  2. 組織体制の確立推進
  3. 早期警戒(情報共有・緊急対応)
  4. 普及啓発・人材育成

  } 第三者評価/認証・監査

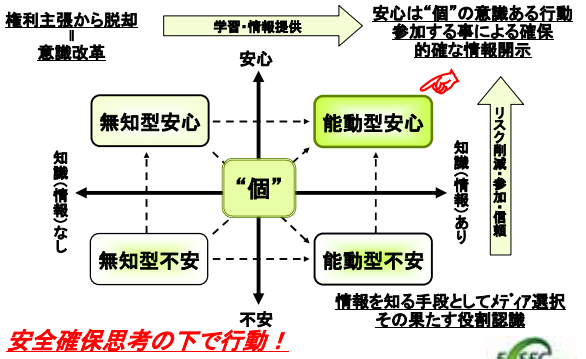
第三者評価に対する試案

22



“個”の安心確保への行動

23



安全確保思考の下で行動！

まとめ

24

- 重要性を増す “コト” が起こる前の対応
- リスク低減へ各業界として“個”を理解した対処
- “個”の前向きな行動と企業・組織の「マーク取り」から脱却
- その上で、連帯感ある社会的枠組み構築
  - 最終利用者“個”へ “安心・安全の提供と信頼” 確保
  - サービス運営者の “サービス提供におけるセキュリティ責任” 確保
  - システム開発者の “システム開発におけるセキュリティ正当性” 確保
  - 評価・試験者は “対象に対し第三者として正当な評価”
  - 認証者は “関連者の評価・試験行動の認証”

⇒ **ユビキタス社会に生きる利用者を明確にし、関心・権利のみではなく責任・義務を持った行動の維持・確保できる社会的枠組み構築**