MITSUBISHI 三菱電機 Changes for the Better

ケーススタディ

三菱電機おける暗号技術開発

MITSUBISHI 三菱電機 Changes for the Better

三菱電機での暗号技術研究の歴史

1985年～1990年 情報電子研究所 メディア部 情セG

- 黎明期（技術蓄積、文献研究中心、技術的には試行錯誤）

1990年～1995年 情報システム研究所 メディア部 情セG

- 基礎技術研究段階（ゼロ知識証明，線形解読法，DESの解読実験，等）

1995年 情報技術総合研究所 情報セキュリティ技術開発センター

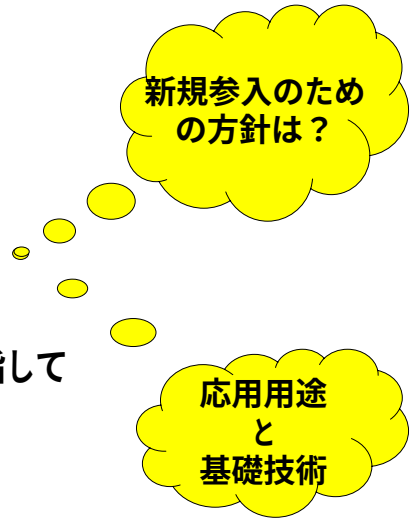
- 基礎技術から製品展開（アプリケーションの模索）へ
  - （MISTY，PowerMISTY，Japan-Netシステム，暗号LSI, DVD-ROM著作権方式等）

1996年～ 情報技術総合研究所 情報セキュリティ技術部

- 実用化段階
  - 基礎技術開発：楕円暗号，暗号強度評価，KASUMI, Camellia, 量子暗号
  - 製品対応開発：ETCSAM, SMTK（認証ﾗｲﾌﾞﾗﾘ），CryptoSign，TRUSTWEB, CERTMANAGER(企業向け認証ｻｰﾊﾞ)侵入検知システム,電子カルテ,PDF署名,TurboMISTY他

基礎技術の蓄積と研究方針の確立

- 研究開発の発端
  - 興味本位，他者追従
  - アンダーグラウンド
  - 試行錯誤
- 研究方針の確立期
  - 独自コンセプトを目指して
  - “強い暗号”とは？



Case Study （I）

- 研究/開発方針の設定
  - 課題：情報セキュリティ分野への新規参入を図る
  - 求める成果のポイント
    - ターゲットとする市場設定
    - ターゲットとする製品
    - 製品に要求される技術の分析
    - 開発の力点＝差別化技術/訴求点
  - 各ポイント達成のアプローチは？
    - 具体的に提案せよ！

MITSUBISHI 三菱電機 Changes for the Better

暗号技術と評価技術

- 新規(独自)暗号技術“売り”は何か
  - 安全性
    - どうして「安全」なのか？
  - 強度評価＝解読の手間
- “線形解読法”の発見
  - DESが解けた!

MITSUBISHI 三菱電機 Changes for the Better

新規技術(MISTY)の普及に向けて

- 「強い暗号」の開発
  - MISTYの公表
  - 「証明可能安全性」を持つ暗号
- 事業化への壁
  - 「アルゴリズム」≠「金」
  - 手軽に使える環境整備
    - 暗号LSI、暗号ライブラリー
  - 自社開発か、共同開発か

普及方策は？

MITSUBISHI 三菱電機 Changes for the Better

Case Study (II)

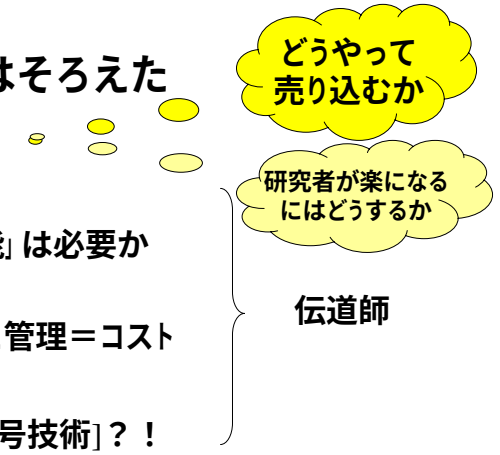
- 事業化に向けて
  - 前提条件:
    - 他社/世界で競争力を持った独自暗号技術
  - 課題:独自暗号技術の事業化を検討せよ
    - ターゲットとする市場設定
    - ターゲットとする製品
    - 普及策
  - どうすれば独自暗号技術を使ってもらえるか?
    - 具体的に提案せよ! (最低限の目標:開発研究費の回収)
      - 特に、独創的なビジネスモデル・製品 (コンセプト)

        →特許を書いてみよう!

MITSUBISHI 三菱電機 Changes for the Better

情報セキュリティシステムの構築

- 利用環境 (部品)はそろえた
- 応用用途の模索
  - 客先訪問
    - 「セキュリティ機能」は必要か
    - 「守る」対象は?
    - システムの運用と管理=コスト
  - 複数からの選択
    - 選ぶ基準は、「暗号技術」?!



Case Study (III)

- 応用用途の開拓
  - 強制的に使わせる！
    - EC
    - ETC
    - 電子政府
  - 自然に(知らないうちに)使わせる！
    - Windows/Internet/i-mode
  - 課題：キラーアプリを考案せよ
    - 特許を書いてみよう！

参考資料の入手先等

- 情報処理振興事業協会(IPA)
  - 市場動向調査

    http://www.ipa.go.jp/security/fy12/report/sec_biz.pdf
  - 製品情報

    http://www.ipa.go.jp/security/enc/product.htm
- 講師への連絡先
  - 山岸

    atsuhiro@iss.isl.melco.co.jp

    Subject名に[IT最前線]と明記してね！