IT最前線：電子マネー

村松 晃 (日立製作所)
a-muramatsu@itg.hitachi.co.jp

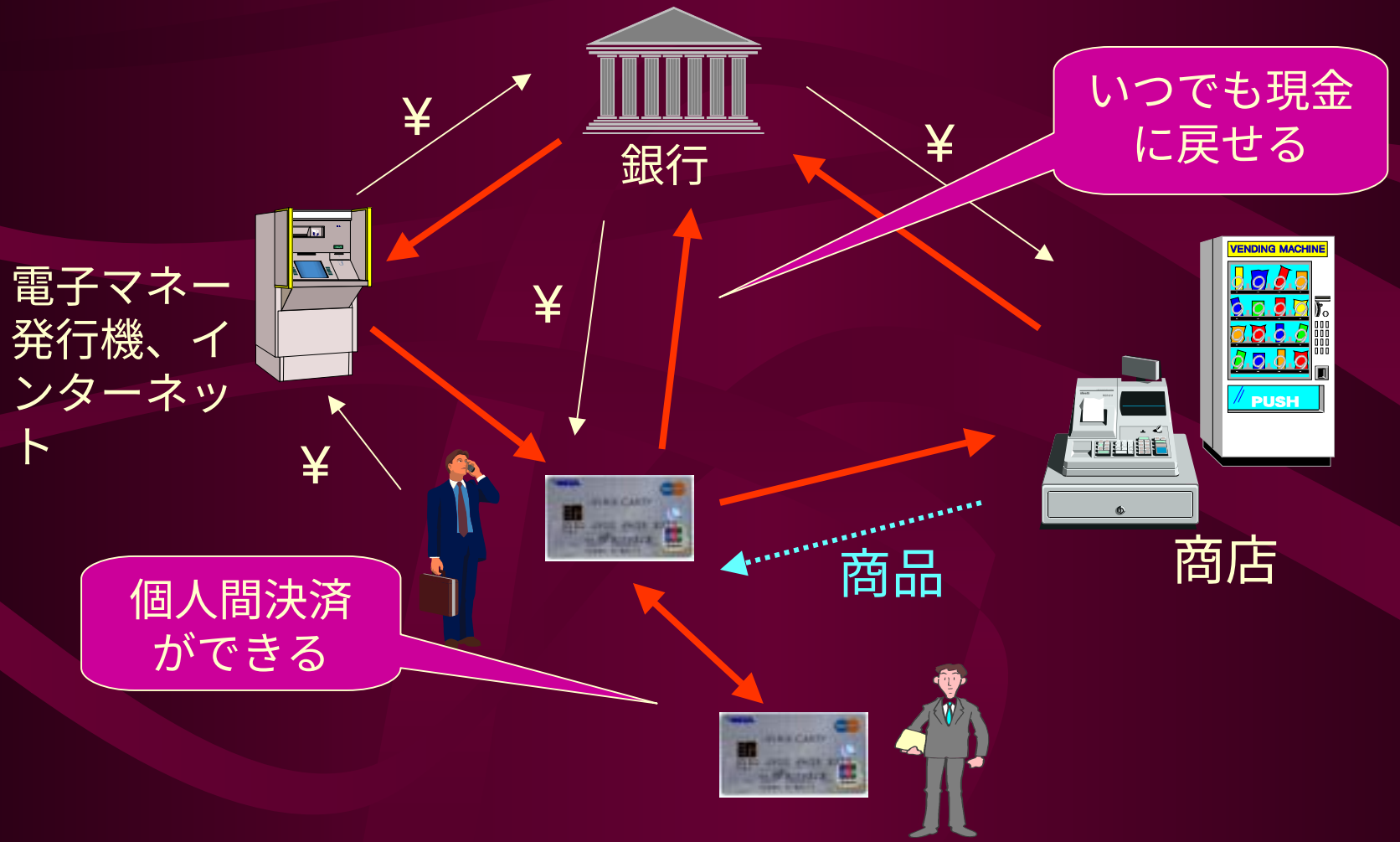
電子マネーって、古いじゃん

- 1996-7年頃話題になった
  - モンデックス
  - ビザキャッシュ
  - プロトン、ゲルトカルテ、eキャッシュ・・・
- でも今Yahooで電子マネーを引くと
  - Web Money
  - スーパーキャッシュ（NTT）
  - デジコイン
  - ビットキャッシュ
  - ビットワレット
  - NET-U

あの頃の電子マネー：正統派

- 通貨を電子化する
  - 第一の波：金属通貨　[希少性]
  - 第二の波：紙幣　[経済成長]
  - 第三の波：電子マネー
- 偽造が減る
- インターネットで使う
- 世界中で使える
- 銀行を介さず直接決済
  - 銀行不要論
  - 銀行は逆に電子マネーのライセンサーを目指す
    - ナットウェスト銀行のT. Jones

電子マネーの例：モンデックス



基本になる考え方を検証する　1

- 電子マネーは「通貨」か
  - 決済手段(交換媒体)　　[NO]
  - 価値を比較する尺度　　[NO]
  - 価値を保存する手段　　[NO]
- 常にリアルマネーと一緒でなければ機能しない（信心不足）
- 現状は通貨の電子的な表現、電子的な決済の方法と言うべき
- 将来、一部の電子マネー （モンデックスなどの現金模倣型）は通貨として機能しうる

基本になる考え方を検証する 2

- インターネットで使えるか
- 世界中で使えるか
  - 技術的には使えるし、現に使われている
  - 安心して使える状況にはない
    - eコマースの法的基盤が未整備
    - 消費者保護
    - プライバシーリスク
  - コンテツ販売に向いている（マイクロペイメント）
    - Pay per View, Pay per Play, Pay per night, ...
    - 方式はまだ確立されていない

基本になる考え方を検証する　3

- 銀行を介さず直接決済できるか
- 決済方法
  - 現金決済　[電子マネー]　[取引の証明？]
  - 預金を利用　[従来]　[取引の証明あり]
- 誰が直接決済を望むか
  - 大金の移動には不向き
  - 小口支払い向き（自販機、マイクロペイメント）

今の電子マネー（日本）

- プリペイドカード（返金できない）
  - WebMoney：インターネットショッピング
    - スクラッチカード（コンビニで販売）
  - BitCash：インターネットショッピング
    - プリペイド番号（コンビニ、インターネットで販売）
  - NET-U（NTT系）：インターネットショッピング
    - 会員登録→口座開設、入金
  - Edy：リアルショッピング（SONY）
    - 非接触ICカード

Euro
Dollar
Yen

Edyについて

- Suicaと同じ非接触カード技術
  - 高速支払い ← 共通鍵方式のため
  - 将来は一枚のカードで交通機関利用と買い物が可能に
  - ネットワークに接続された端末が不可欠

電子マネーの不安

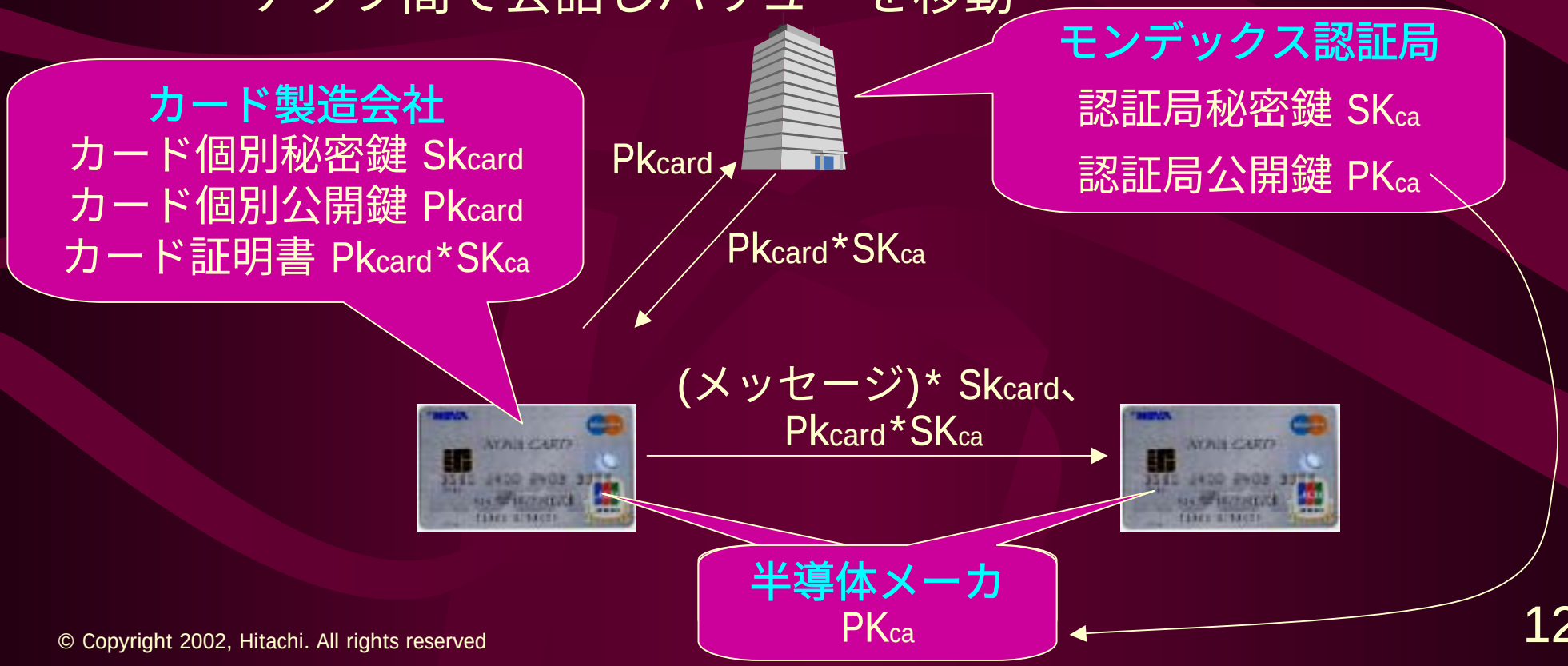
- 電子マネーはデジタル情報だから偽造しやすい？　[政府、金融機関]
- 電子マネーは匿名性がなく、誰がどこで何を買ったか知られてしまう。　[利用者]
- 電子マネーなんだから、落としても何とかなる？　[利用者]
- 電子マネーを利用するためのインフラ構築が大変。　[商店、金融機関]

電子マネーのセキュリティ

- 希少性を守ることが通貨の必須条件
- デジタル情報の暗号化で複製を防止する
- ICカードの耐タンパー性を活用し、さらにセキュリティを高める
  - 耐タンパー性：外部からのハッキングに耐え、改ざんを許さない性質
    - コーティング
    - 干渉検知 & 自動消去
    - 鍵情報等のスクランブル
    - ダミーの演算処理、等々

電子マネーの暗号処理

- モンデックスの例
  - 公開鍵を利用した最高水準のセキュリティ
  - チップ間で会話しバリューを移動



公開鍵方式でないと・・・

- 共通鍵方式では、万一一つの鍵が破られるとシステムが崩壊する
- 公開鍵方式なら、一枚のカードの個別鍵が破られても他のカードには影響しない

電子マネーの匿名性

- キミは電子マネーでポルノを買えるか
- 原理的に匿名性が実現されている電子マネー
  - eキャッシュ：使用されているブラインド署名は、技術的には興味深い
  - 会員登録しないすべてのプリペイド
- 運用で匿名性を実現している電子マネー
  - モンデックス、ビザキャッシュ等
- 非匿名の電子マネー
- 匿名性の是非については議論あり
  - プライバシー
  - マネーロンダリング

電子マネーを落とすと・・・

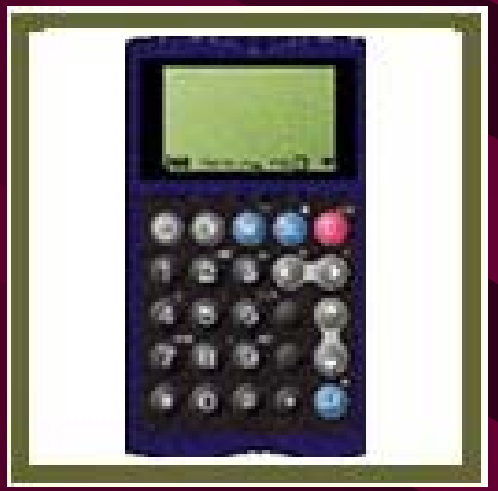
- 多くは現金と同じく「紛失」する
- 暗証番号でロックできるものは、拾っても使えないので戻ってくるケースが多い
  - モンデックス
- カードの中に本当のバリューが入っていないタイプは、届け出て口座をロックしてもらえば被害は出ない（原理的には）
  - プロトン

電子マネーのインフラ：モンデックスの例１

- 利用者端末類

残高表示機

スリーブ



電子財布

電子マネーのインフラ：モンデックスの例 2

- 商店用端末

マーチャントターミナル

電子マネーのインフラ：モンデックスの例 3

- バリューチャージ用機器

モンデックス
ATM 1

モンデックス
ATM 2

電子マネーのインフラ：モンデックスの例 4

- 銀行用システム

金庫

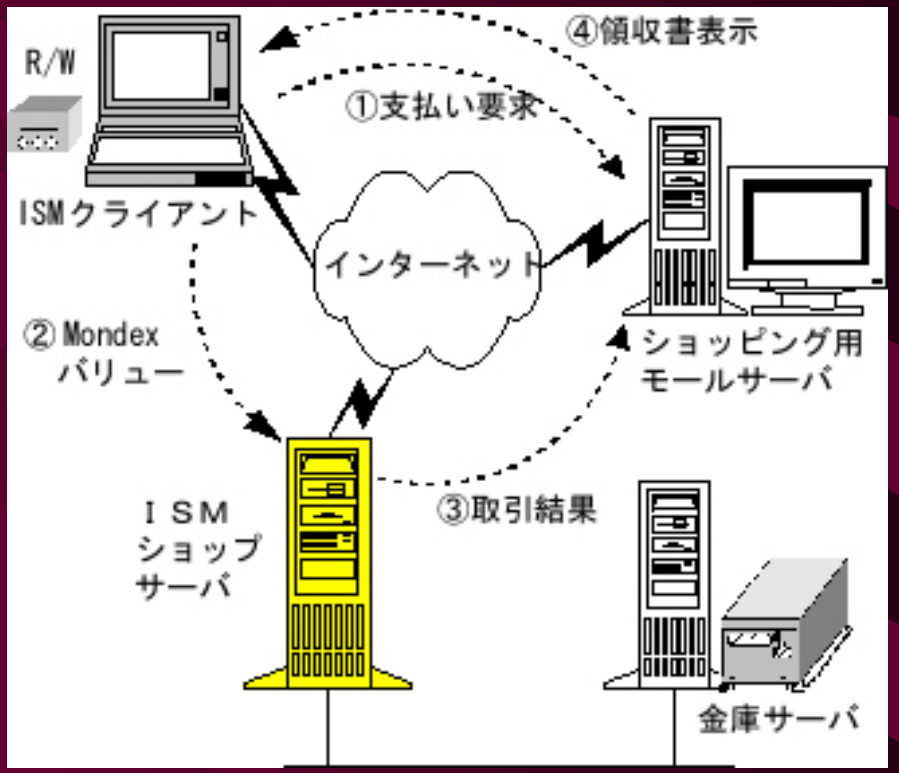
マルチカード
ボックス

通信装置

電子マネーのインフラ：モンデックスの例 5

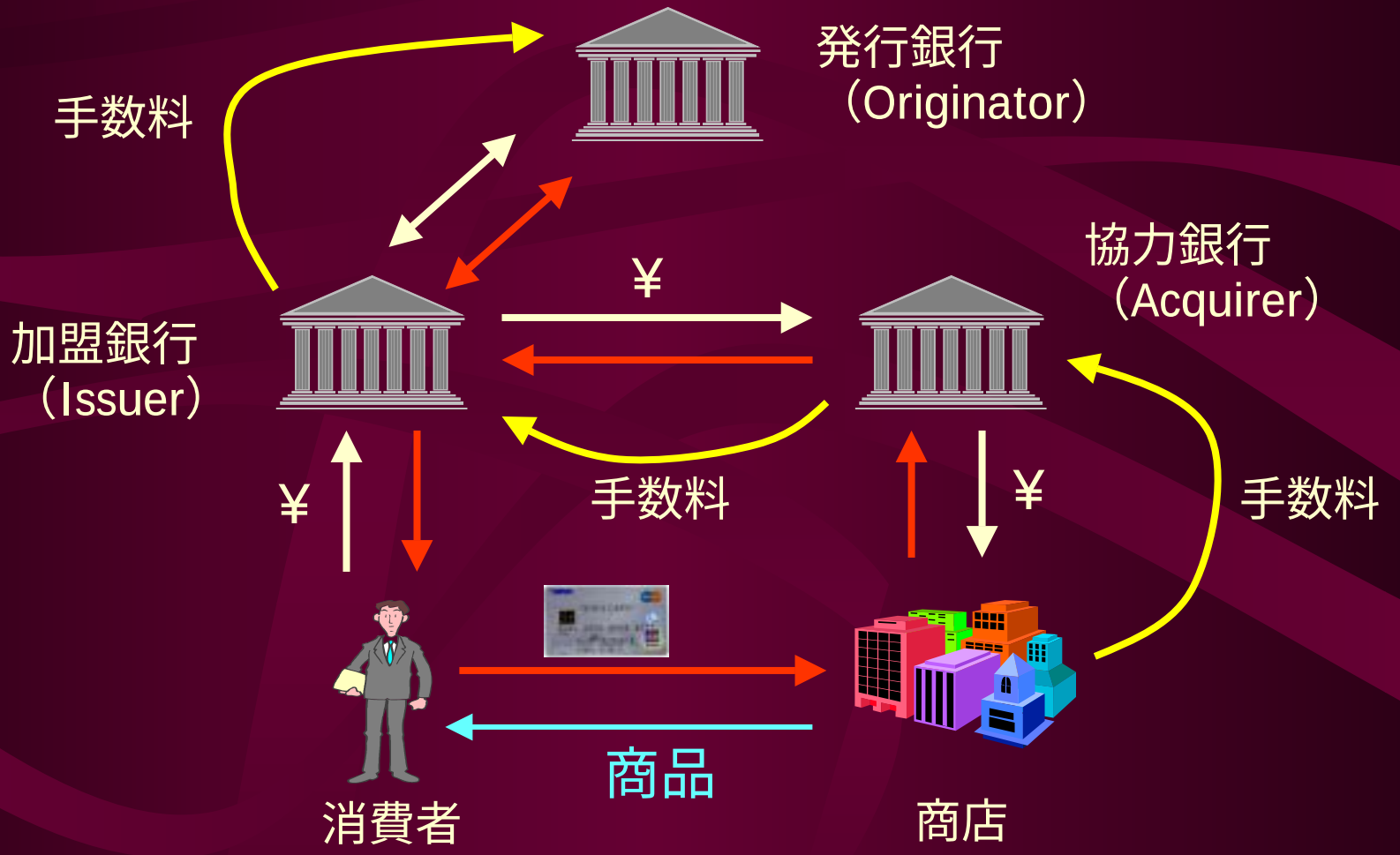
- インターネット関連

PC用リーダライタ



インターネットサーバー

電子マネーのビジネスモデル



難問

- 各参加者の動機は？
  - 銀行：取引量が多く手数料収入が大なら
  - 商店：(現金の方がいいが) お客が望めば
  - 消費者：どこでも使えて便利なら
    - 商店POSでの利用はそれほど便利ではない
    - 自販機などの無人支払い環境では便利
    - インターネット/携帯では現金は使えない
- 誰が電子マネーのインフラコストを負担するか？

モバイルコマースでの利用

- 携帯電話に電子財布を内蔵
  - バリューはいつでもどこでも無線でチャージ
  - バーチャルショッピング
  - リアルの店舗では赤外線または非接触インタフェースで支払い
  - Suicaなど交通切符も実装される？
- インフラは消費者が自分のお金で構築する！

欧州のモバイルコマース携帯電話

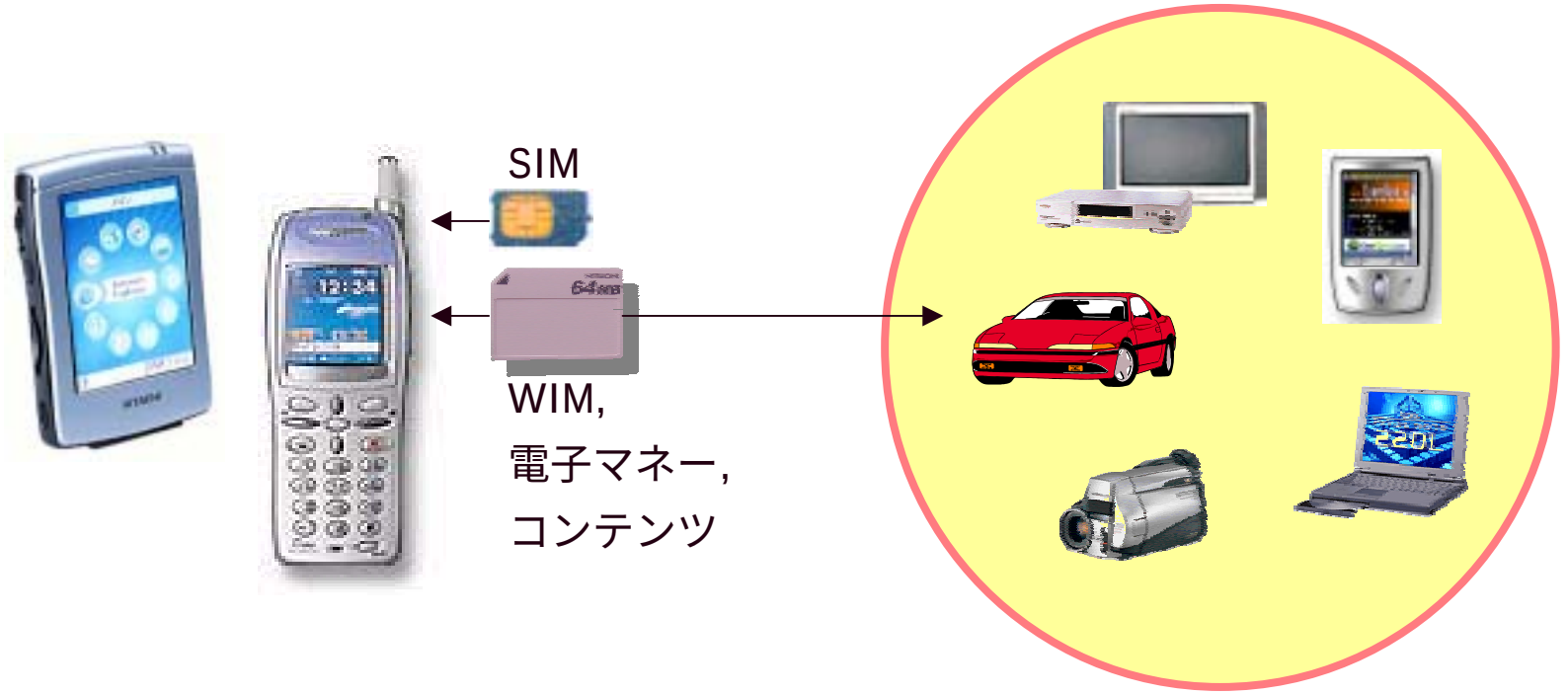
SWIM

Dual slot

Dual Chip

わたしの提案

- セキュア・メモリカードでモバイルコマースを



まとめ

- 電子マネーは技術的進歩にもかかわらず、ビジネス的には成功していない
- インフラコスト負担の論理が不透明
- 現状はプリペイドに移行
- モバイルコマースが起爆剤になるか
- 将来は通貨の電子化に移行する