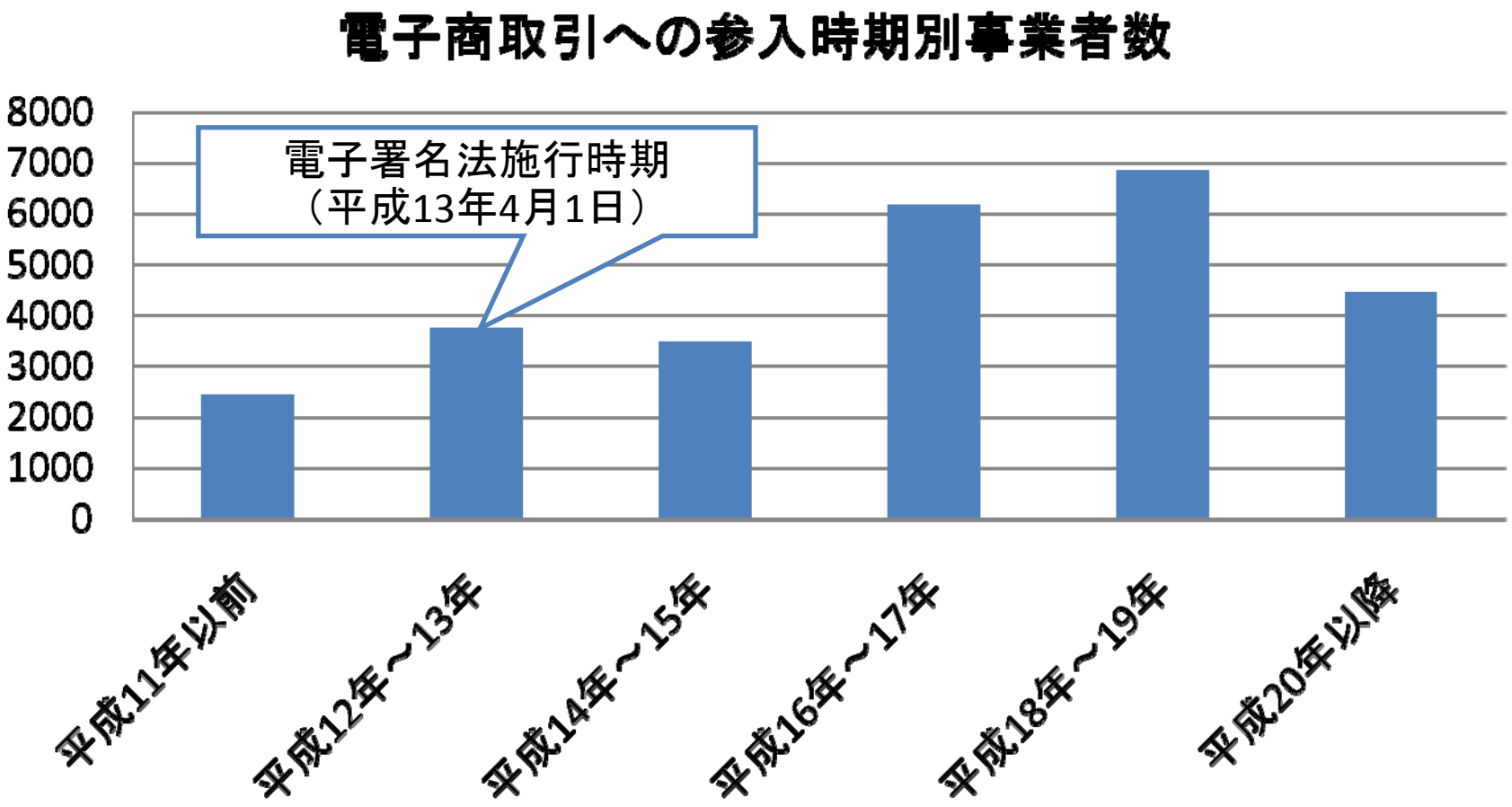
電子署名法の課題

株式会社　イマーディオ
満塩　尚史
2010年6月29日

平成２１年消費者向け電子商取引実態調査結果
経済産業省　平成22年6月11日

- 年間売上高
  - 1社当たりの売り上げが3千万円未満の事業者数では、全体の約8割
  - 1社当たり１０億円以上の事業者の年間売り上げが全体売り上げ2兆3482億円の中で8割弱。
- 取扱品目
  - カテゴリ別にみると、物品が1兆5139億円（構成比48.1％）、以下、サービスが1兆4341億円（同45.5％）、デジタルコンテンツが2008億円（同6.4％）。
  - 取扱品目別（２２品目）にみると、旅行が8945億円（構成比28.4％）で最も多く、以下、衣料品・アクセサリー、家電品・PC及びPC関連製品の順。
- 消費者からみた取引形態
  - 消費者が購入時に使用した端末形態の実態をみると、パソコンによる購入が１兆7964億円で８割強。
  - 消費者の購入時の決済方法の実態を見ると、クレジットカードによる購入が1兆2976億円（構成比44.3％）、以下、代金引換、銀行振込・郵便為替の順。
- 電子モールへの出店の実態
  - 電子モールに出店して販売のみ行っている事業者は4割、自社ホームページのみによる販売を行っている事業者が3割強。

平成21年消費者向け電子商取引実態調査結果
経済産業省　平成22年6月11日



電子署名法の課題

- 電子商取引における寄与しているか？
  - 電子署名の利用の確保
    ⇒電子商取引の問題解決、促進となっているか？

- 取引等の成立の推定に電子署名が必要か？
  - 推定考の議論が必要と考えていた。
  - 一方、経産省の統計調査を読み解くと、
    - 電子モールを活用
      ⇒認証システムの活用とログ分析と十分？
    - クレジットカードによる購入
      ⇒電子データのやり取りだけではなく、実態上は、支払能力がされていれば、十分？

- 実際の電子商取引で、送信「否認」もしくは、電子データを作成した事実の「否認」が論点となった事故・事例等があるか？
  - 不正アクセス禁止法を侵さずに、送信または作成「否認」を行なう状況が作りづらい。

電子署名（PKI）の貢献

- SSLサーバ証明書の普及
  - 個人情報入力における情報漏洩対策としては必須と理解されつつある。
  - 正常な設定がされていれば、ブラウザーが警告しない限りは、気にかけなくてよい。
- 付加価値の高い領域における認証技術としての普及
  - オンラインバンク等でのPCの特定に活用
  - ただし、電子署名ではなく、あくまでも認証技術として活用
- 「否認」防止技術としての存在
  - 現時点でも、「否認」されることを防御する方法としては、PKI以外には、考えにくい。

電子署名法における認証局の認定

- PKIの構造上、上位認証局が問題を起こしてはいけない
  - cf. PGPでは、「友達の輪」が重要。しかし、オープンな空間においては、「友達の輪」を構築するのが困難。

- そのため、認証局は問題を起こっていないか、起こさないか認定する必要性がある。
  - 認定するための審査項目
    - 本人確認手段、ポリシー整備、物理的セキュリティ、論理的セキュリティ、組織的セキュリティ、サービスの継続性
      - cf. マイクロソフトIEにルート証明書を登録するためには、WebTrust for CAの認定が必要。
    - ⇒電子署名法の認証局にも認定制度を取りこむ。

認証局の認定の比較

項目	WebTrust for CAの認定	電子署名法の認定
基本的考え方	自己で定めたポリシーに基づき実施されていることと実施されていることの情報公開	電子署名法にもとづき特定認証業務を満たしていること確認でき、認定認証局として認定可能な条件
証明書発行対象	認証局、人、企業、サーバ等ポリシーに基づき設定	自然人（基本4情報） （その他の属性情報の認証を禁止しているものではない）
本人確認方法	ポリシーで定義。下位の認証局やSSLサーバ証明書用の企業の本人確認。	電子署名法の認定基準で定義。自然人として、基本4情報（氏名（漢字）、性別、生年月日、住所）で区別する。具体的な本人確認方法（戸籍、住民票等）は、電子署名法で定義。
ポリシー整備 物理的セキュリティ 論理的セキュリティ 組織的セキュリティ	ポリシーで定義。ただし、業界標準的なレベル感はあった。	電子署名法の認定基準で定義。ただし、WebTrust　for CAを準拠。
サービスの継続性	ポリシーで定義。ただし、業界標準的なレベル感はあった。	特に定義していない。

意見

- 「否認」防止の手段としては、現在でも、電子署名は、有効な技術である。
  - 将来的には、必要な技術である。
    - インターネットだけで取引が完結する可能性のあるデジタルコンテンツの取引が増大した場合。
    - 電子商取引や電子契約書が重要な取引（土地の売買）等にも活用するシーンが増大した場合。
- インターネット空間で、社会のリソースであるエンティティをどう区別するということを整理する必要があった（ある）のではないか？
  - エンティティ：自然人、企業、住所情報、外字情報
  - 特定方法：国民としてのID、企業コード、GIS情報、外字データベース
- 電子署名だけが、取引の成立を推定する技術ではないのではないか？
  - 現状の物品等の購入を中心とする電子商取引で、必要か？
- 公開鍵暗号方式の解説が必要だったのだろうか？
  - 公開鍵暗号方式の「仕組み」を、一般の人にも理解させようとしてきたのではないか？
  - SSLサーバ証明書の「仕組み」は、理解していなくても「効果」である盗聴防止は、理解していると思われる。
  - 電子署名の「効果」を説明するのを否定するものではない。