JNSA　PKIDay2007

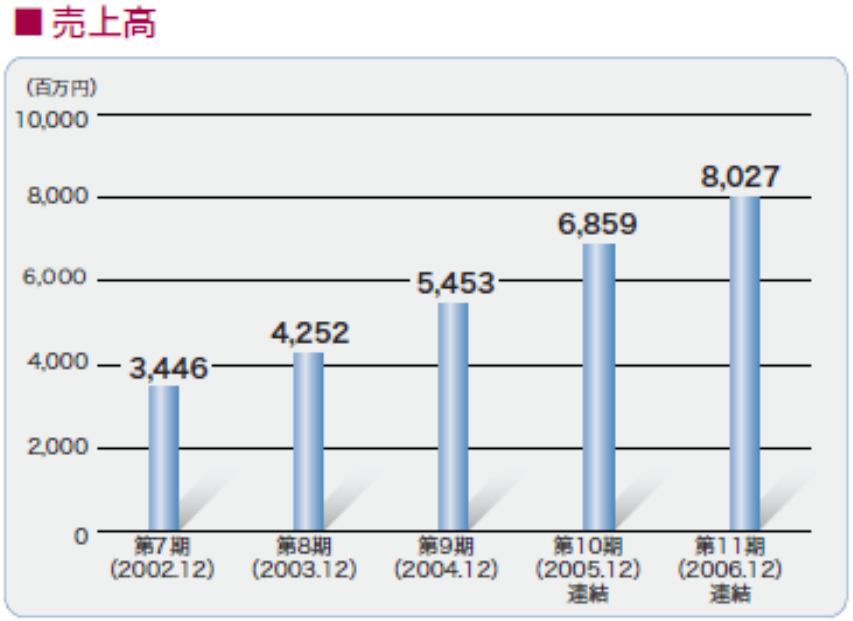
PKIから
社会システムとセキュリティを考える

技術は、セキュリティ課題を解決しているか。

NEC　共通基盤ソフトウェア研究所
小松文子

ＰＫＩ技術の浸透

- 市場動向
  - EV　SSL証明書
  - 日本ベリサイン
    の売り上げ
    →2.3倍(2002→2006)



http://www.verisign.co.jp/corporate/releases/20070410/10.pdf

- 技術動向
  - 認証連携技術
  - Windows　CardSPace
  - TCG/TPM

PKIの利用：電子署名と相手認証

- 電子署名
  - ディジタル署名を利用し情報に証拠能力を与える
  - メッセージ認証と本人認証を併せ持つ
    - 非改ざん性と、否認拒否を防ぐ
  - ビジネスプロセスとつながりが強い
- 相手認証
  - 相互の共有情報をPKIで安全に交換することで相手の確からしさを確認する。
  - これまで実現できなかった複数システム間連携をオープンに実現するために必要

PKIの困難さ　～　公開鍵証明書の相互接続性

バージョン・シリアル番号
署名アルゴリズム＊
発行元（CA名）＊
有効期限（開始と終了）＊
サブジェクト（所有者名）
サブジェクトの公開鍵　＊
AKI（認証局の鍵識別）
SKI（サブジェクトの鍵識別）
鍵用途・拡張鍵用途
私有鍵期限
ポリシ情報
ポリシマッピング
サブジェクトおよび発行者の別名
基本制約とポリシ制約
失効情報配布点（アドレス）
認証局アドレス（VAのアドレスなど）
サブジェクトディレクトリ情報

→ 信頼基盤の構築

→ **サブジェクトの識別基盤**

・所有者のIDをどのように管理していくかの基盤が必要
・所有者の権限管理

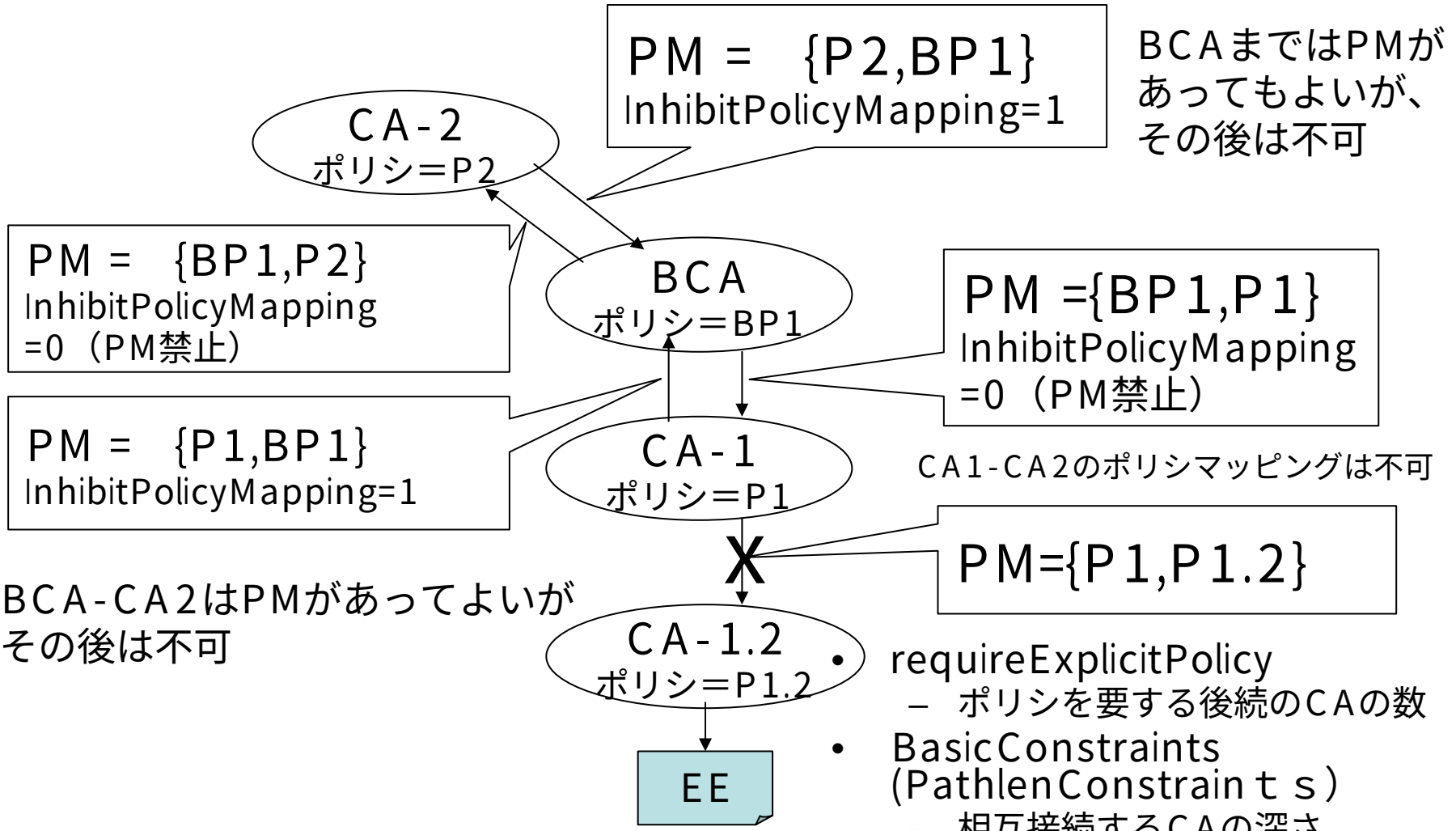
ポリシの相互接続性要件項目

・組織のポリシとその合意

ポリシの相互接続性要件項目

ＣＡ信頼パス構築における ポリシー制御の例

- Policy Mapping
  - 異なるポリシを許容することを明示
- InhibitPolicyMapping
  - ポリシマッピングが許されなくなるまでの証明書数



- requireExplicitPolicy
  - ポリシを要する後続のＣＡの数
- BasicConstraints (PathlenConstraｔｓ)
  - 相互接続するＣＡの深さ

社会システムとセキュリティを考える

技術は、セキュリティ課題を解決しているか。

- 信頼基盤の構築
  - 電子署名、認証、ICカード、お財布携帯、プリペイドマネー
  - 安心感の醸成
- 情報セキュリティと経済効果関連
  - 市場原理がはたらかない
  - プライバシ保護と情報活用
- 情報セキュリティと法制度等
  - JSOX法とアクセス制御
  - 個人情報保護法と情報活用