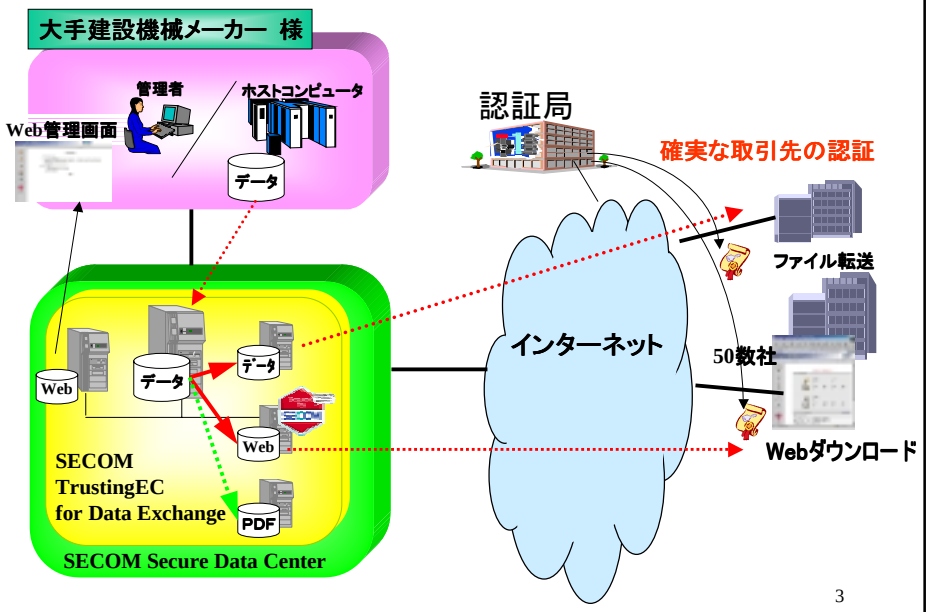
PKI導入編

セコムトラストネット株式会社
松本　泰
yas-matsumoto@secomtrust.net

なぜPKIが必要か？PKIに何が要求されるか？

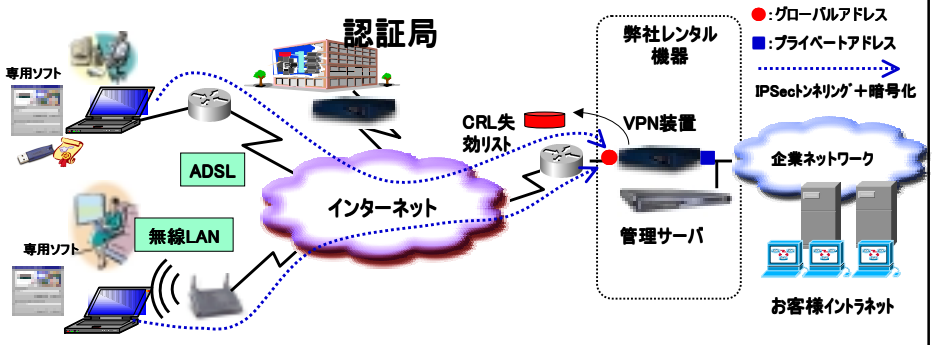
- ユビキタス時代に要求される便利で安全な認証
  - ブローバンド、ユビキタス社会における、安心、安全なインターネット環境（PKI空間）のために、様々な用途の認証、様々なレベルの認証、広いドメインでの認証を実現したい
  - 広く採用するには、標準化された技術を採用したい
- 電子政府と政府認証基盤(GPKI)など動向
  - GtoBのための認証基盤　ー＞GPKI
  - 3300の地方自治体のための認証基盤　-＞ LGPKI
  - GtoCのための認証基盤 -> 公的個人認証基盤
- Identrusのような国を超えたB2Bの認証基盤
  - サイバー世界では国境がない。
  - 世界に通用するセキュリティが必要
- 認証と署名
  - 認証と署名の使い分け

Web－EDI



3

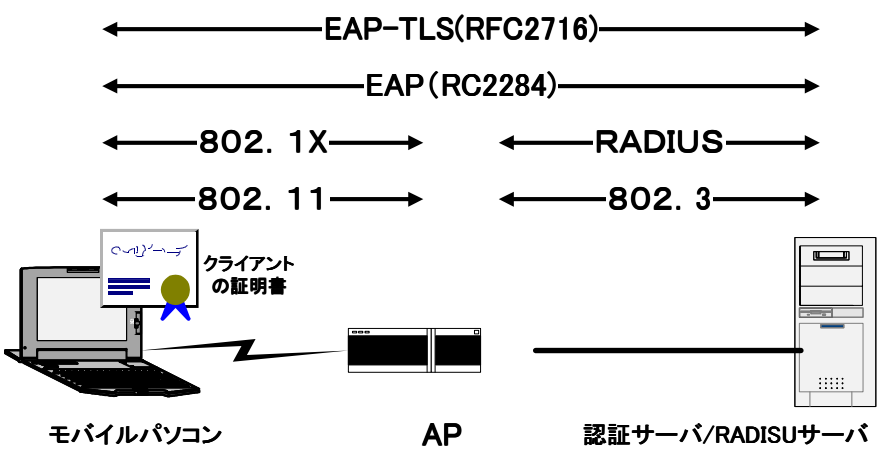
Internet-VPNサービス



Anywhere, Anytime, Anyplace モバイルオフィスを実現するためには、確実な認証が必要

4

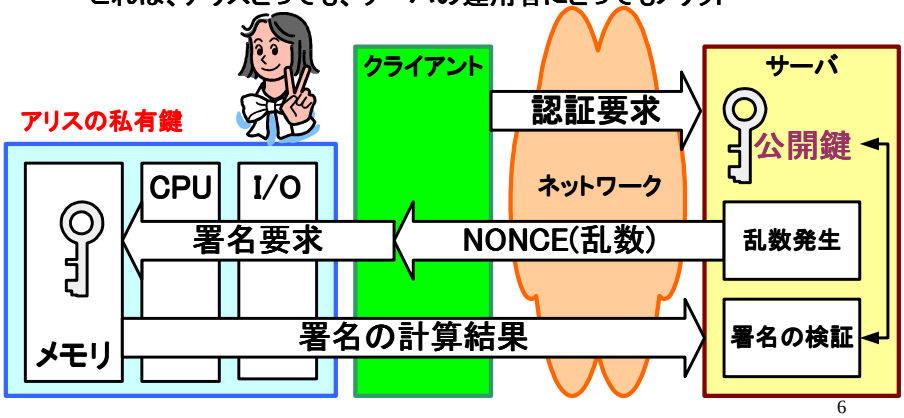
無線LANセキュリティ
IEEE 802.1x EAP-TLS



5

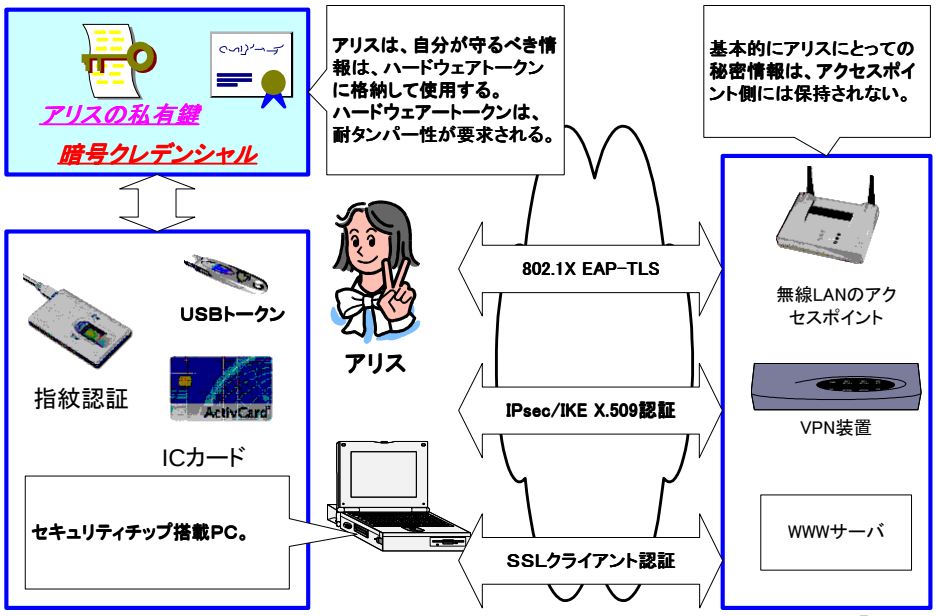
ハードウェアトークンを使用した認証の例

- アリスの秘密情報(私有鍵)はハードウェアトークンから出ない
  - もちろんネットワークにも流れない
- アリスの秘密情報は、サーバには、格納されない
  - サーバは、アリスの秘密情報(例えばパスワード)を預かる必要がない
  - これは、アリスとっても、サーバの運用者にとってもメリット



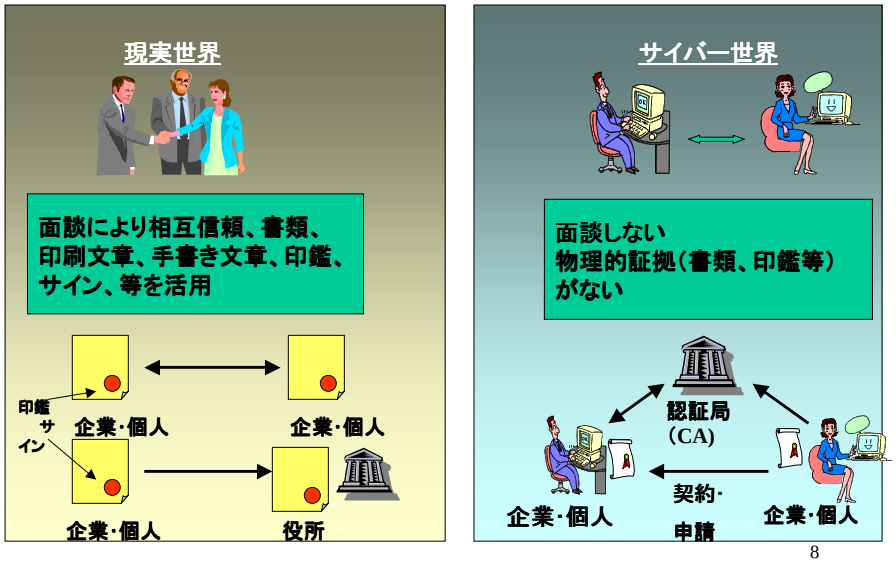
6

ユビキタス時代に要求される便利で安全な認証



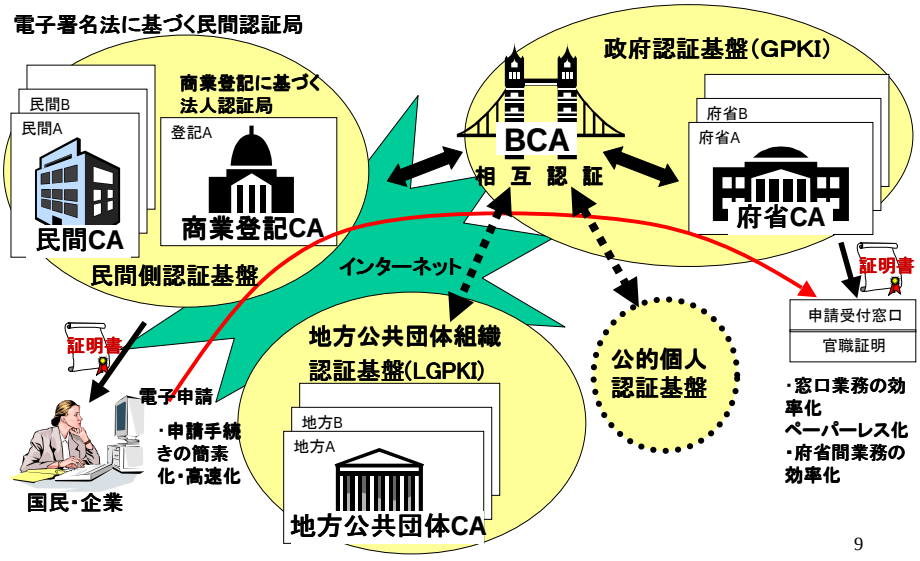
7

現実世界とサイバー世界での確認比較

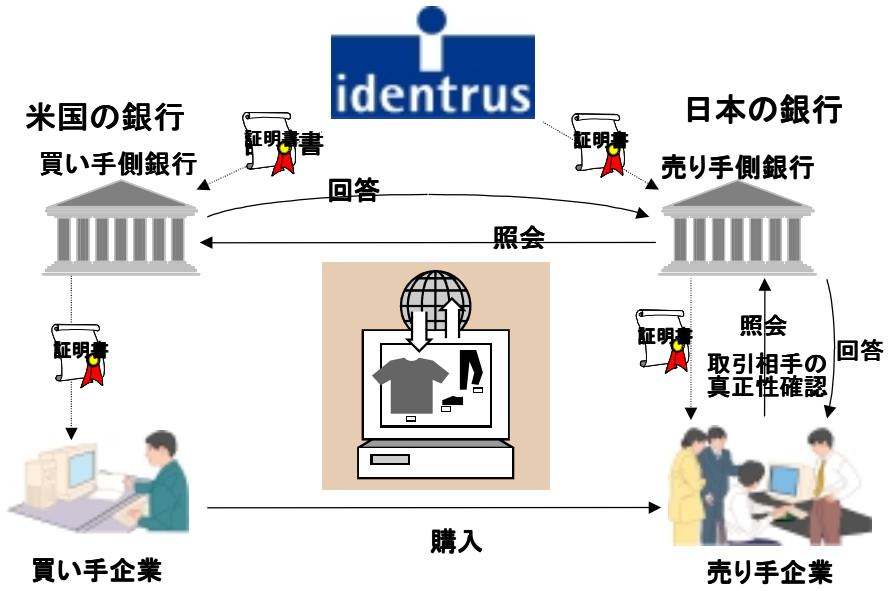


8

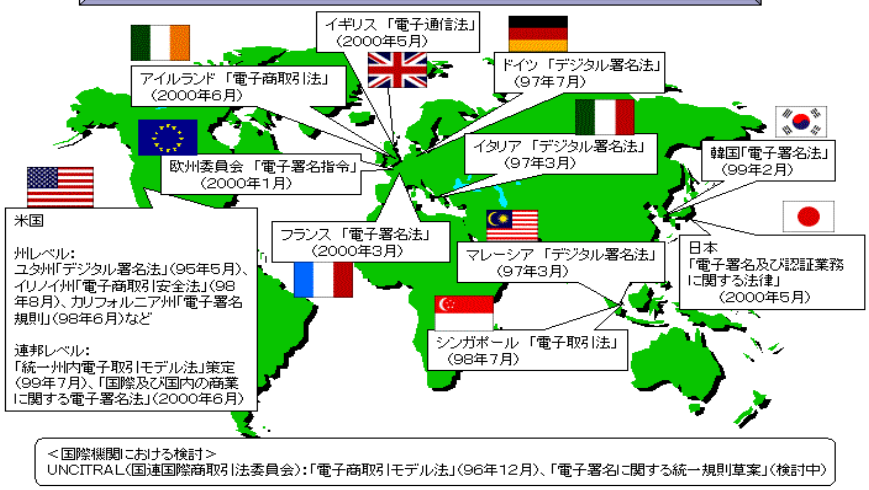
政府認証基盤(GPKI)と
地方公共団体組織認証基盤(LGPKI)



Identrusのビジネスの枠組み

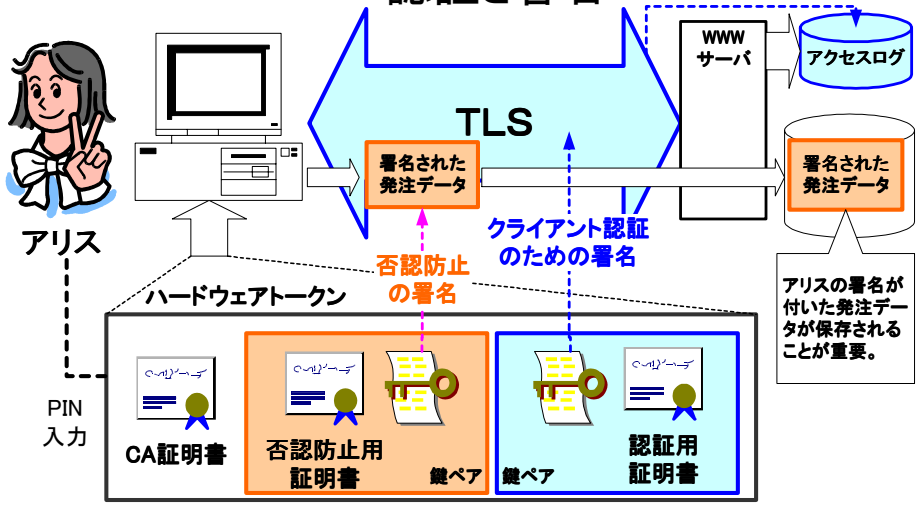


■諸外国の法制度整備の動向



出典：政府委員会資料を参考に作成

認証と署名



銀行を中心としたPKIであるIdentrusや、フィンランドの市民カードでのあるFINEIDでは、この例のように2つの証明書を発行している。

12