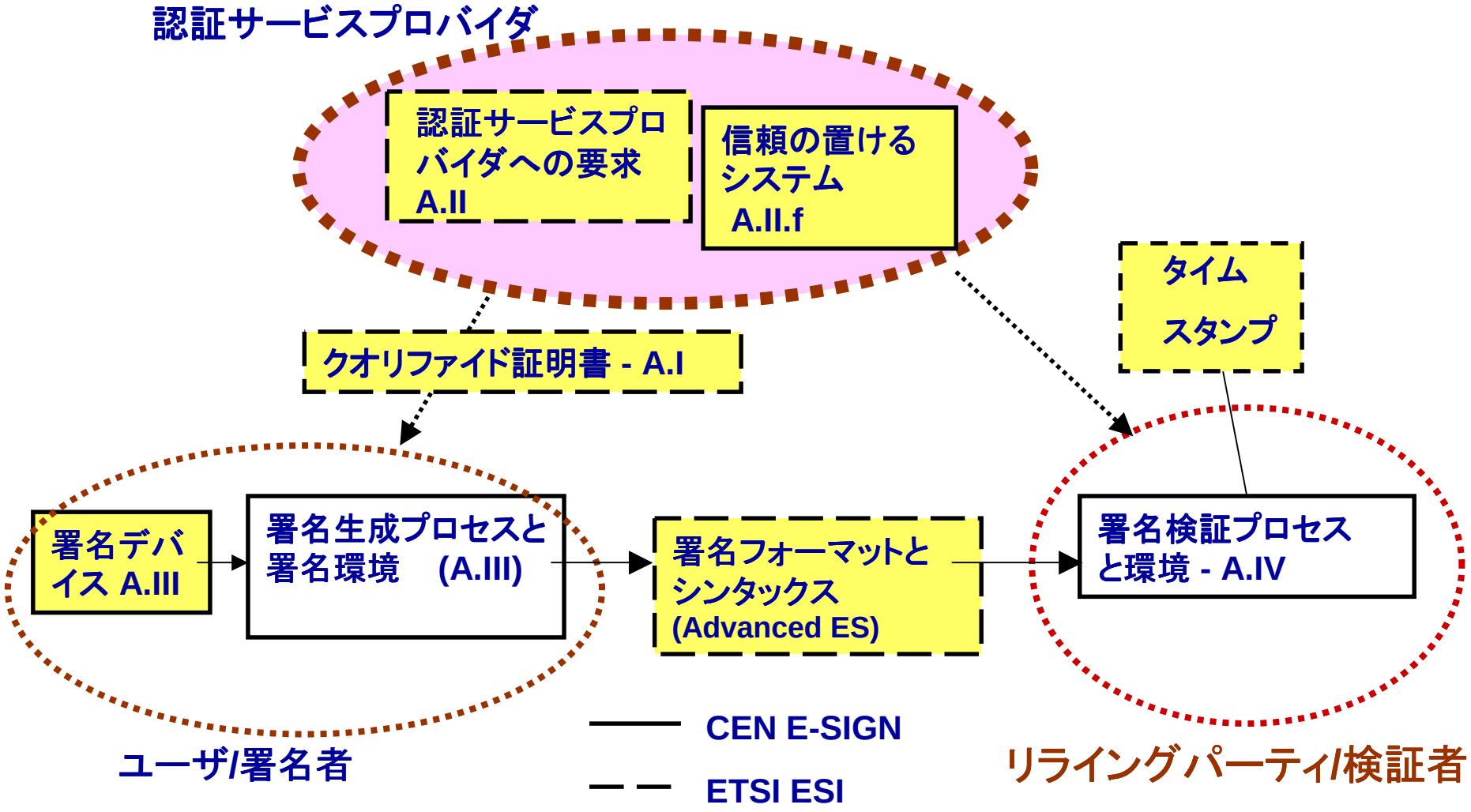
セコムIS研究所
Intelligent Systems Laboratory

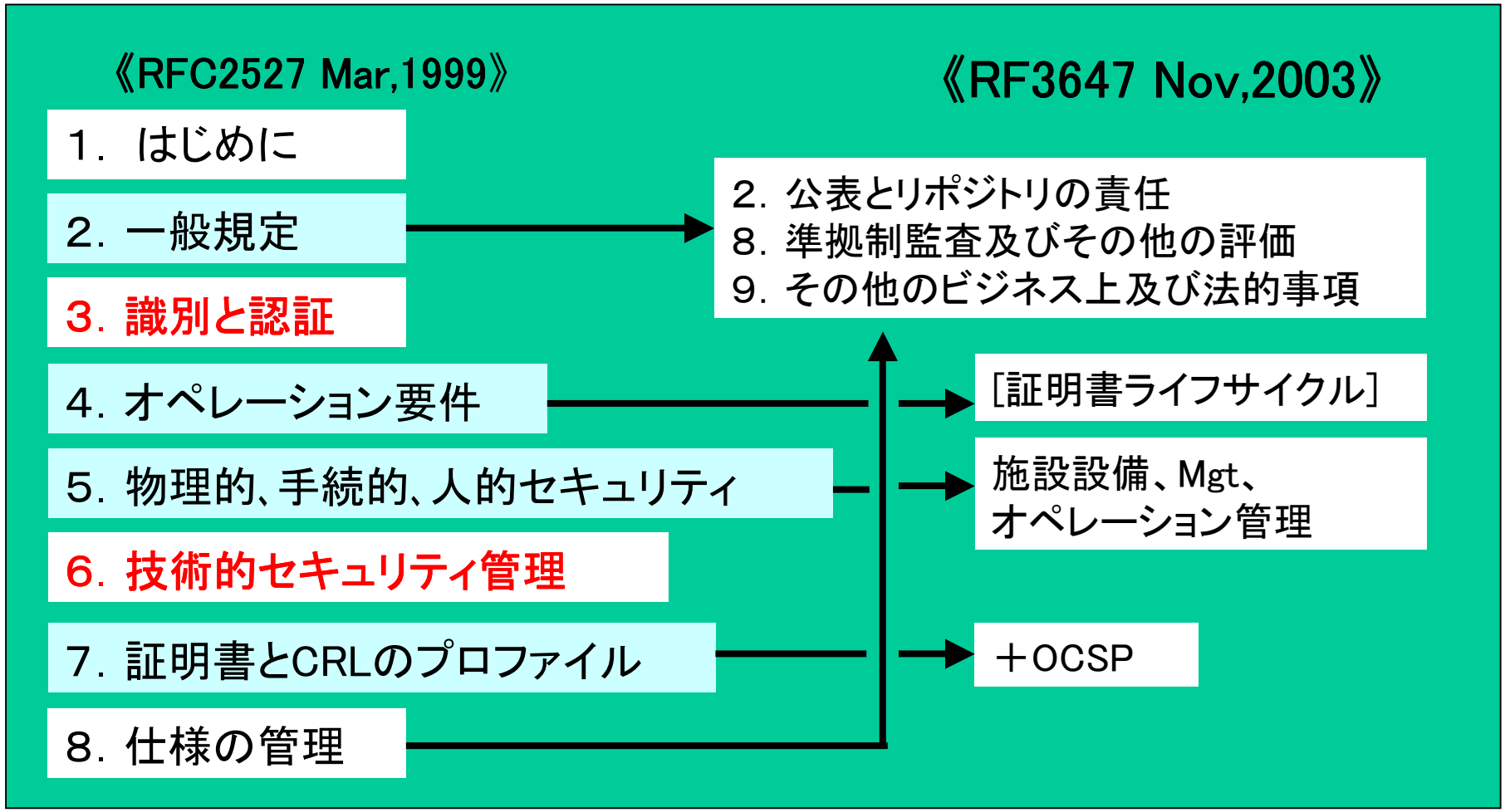
認証局の信頼

認証局の信頼
EESSIの認証フレームワーク

セコム IS 研究所
Intelligent Systems Laboratory



認証局の信頼
CP／CPSの記述構成
RFC2527（RF3647）
Certificate and Certification Practices Framework



認証局の信頼

RFC2527：CP/CPS記載内容と検討ポイント

－3．識別と認証－

■ネーミングルール

規約、解釈、ペンネームの可否．．．
［ユニークであることの確保］

■識別、認証（個人、組織）

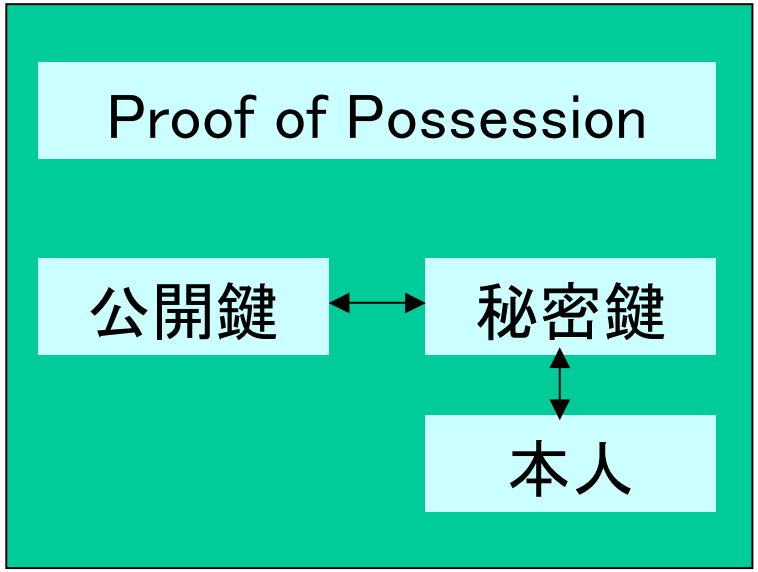
本人又は組織の真偽の確認

例：各種の公的証明書

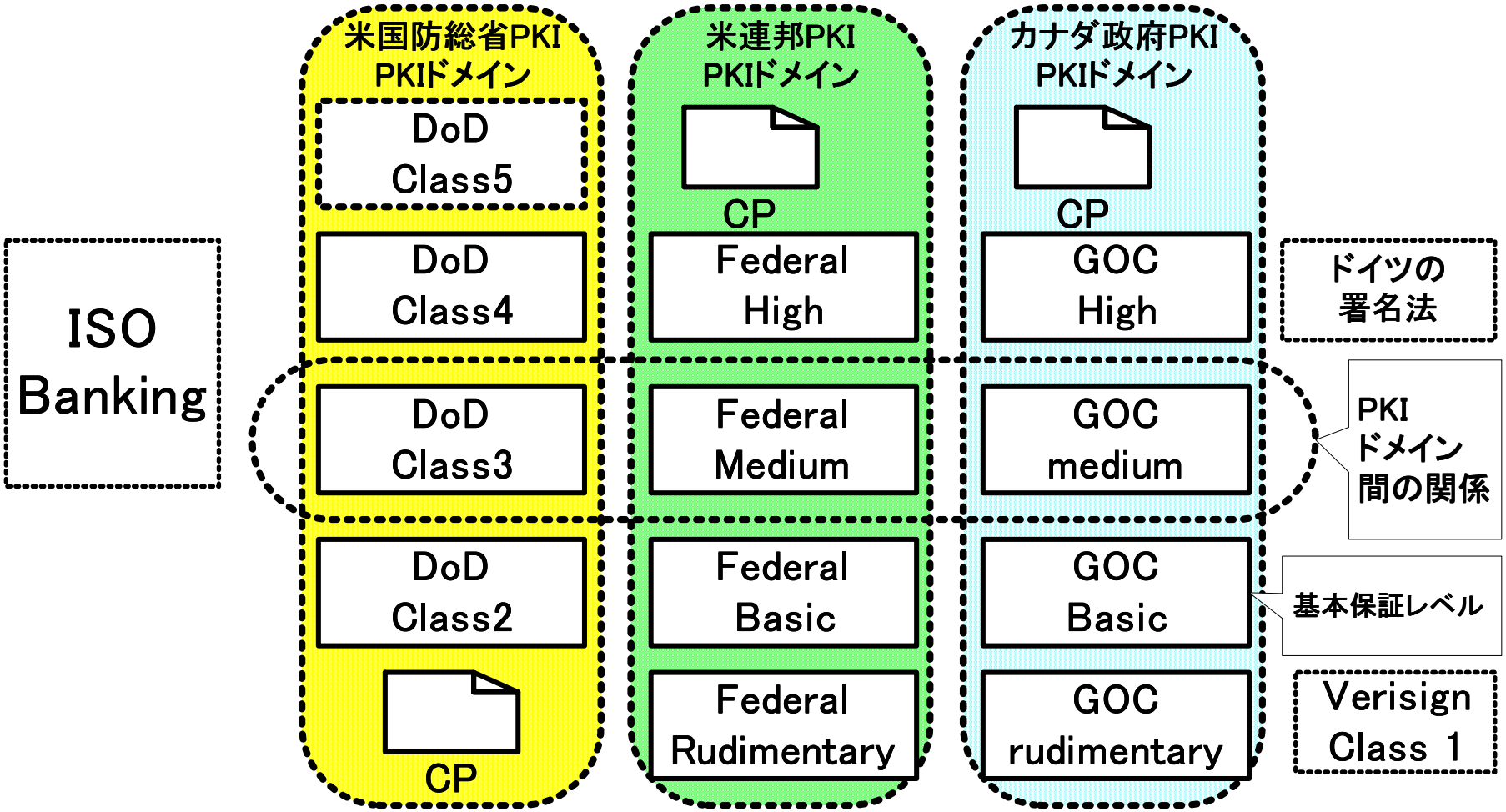
■初期登録／更新／失効後

要求方法・手続

認証方法・手続



認証局の信頼
証明書ポリシと保証レベル



US Federal PKI のCPの例

3. IDENTIFICATION AND AUTHENTICATION

3.1.9 Authentication of individual identity

Assurance Level	Identification Requirements
Rudimentary	身元確認のために要求はない。申込者は、電子メール・アドレスを送ることによって、証明書を受け取るかもしれない
Basic	Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or comparison with trusted information in a data base of user-supplied information (obtained and/or checked electronically, through other trusted means (such as the U.S. mail), or in-person); or by attestation of a supervisor, or administrative or information security officer, or a person certified by a state or Federal Entity as being authorized to confirm identities.
Medium	Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)
High	申請者がR A に出向き、提出情報を法令に則って確認する。また、政府発行の写真付IDカード、または、ふたつの非政府発行のIDカード(ひとつは写真が必要、運転免許書など)で確認する。

認証局の信頼

RFC2527：CP/CPS記載内容と検討ポイント

－6．技術的セキュリティ管理－

■鍵ペア生成、鍵管理

RFC2527：CA、RA、リポジトリ、EEについて記載

認証事業者側の鍵管理は最重要

暗号モジュール、鍵長、Dual Control、鍵ライフサイクル管理．．．

CPとCPSを分けるなら．．．

EEの鍵管理→CP

■いわゆるコンピュータ／ネットワークセキュリティ

認証業務システムの情報セキュリティ（C,I,A）

セキュリティ"管理"が実装されていること

認証局の信頼
HSM　Hardware Security Modules
セキュアなハードウェア鍵管理装置

セコムIS研究所
Intelligent Systems Laboratory

- HSM　Hardware Security Modules
  - セキュアなハードウェア鍵管理装置
  - 鍵を守るための色々な仕組みを持つ
- FIPS 140-2
  - 米国標準技術院(NIST)によって1994年に策定された暗号モジュールの安全性に関する米国政府調達基準
  - FIPS 140-1と、見直された FIPS 140-2
  - 用途による複数のレベル　　Level 1　から　Level 4
  - FIPS 140-2 Level 2
    - 比較的簡易な認証局、サーバ、エンドユーザの鍵などの使用されている
  - FIPS 140-2 Level 3
    - 多くの商用の認証局で多く使用されている
- 電子署名法特定認証業務
  - FIPS 140 Level 3相当を要求

US Federal PKI のCPの例

6.2 PRIVATE KEY PROTECTION

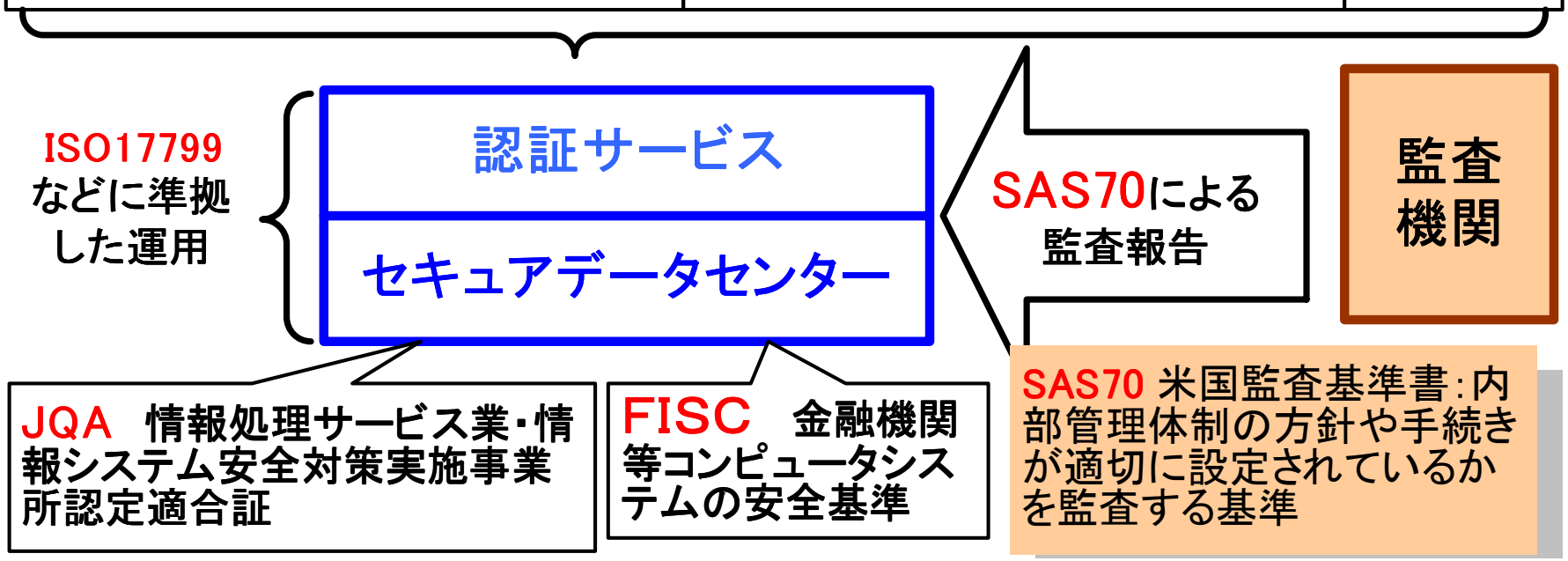
6.2.1 Standards for cryptographic module

Assurance Level	Certification Authority	Subscriber	Registration Authority
Rudimentary	FIPS 140-2 Level 1 (HW or SW)	N/A	FIPS 140-2 Level 1 (HW or SW)
Basic	FIPS 140-2 Level 2 (HW or SW)	FIPS 140-2 Level 1 (HW or SW)	FIPS 140-2 Level 1 (HW or SW)
Medium	FIPS 140-2 Level 2 (HW)	FIPS 140-2 Level 1 (HW or SW)	FIPS 140-2 Level 2 (HW)
High	FIPS 140-2 Level 3 (HW)	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (HW)

認証局の信頼
認証サービスの運用基準と監査

セコムIS研究所
Intelligent Systems Laboratory

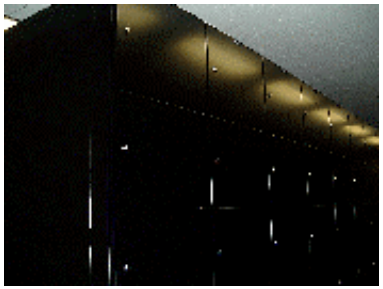
認証サービス名	運用基準など	状況
Identrus Express Partner	Identrus CCAG (Identrusの運用監査基準)	認定
セコムパスポート For GID	電子署名法特定認証業務	認定
セコムパスポート For Member	セコムトラスネットの運用基準	―



認証局の信頼
セコムのセキュアデータセンター

セコムIS研究所
Intelligent Systems Laboratory

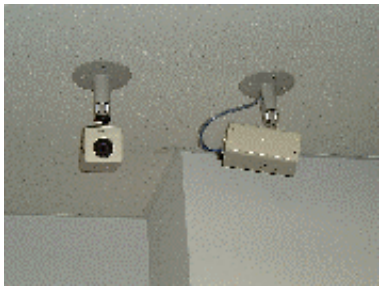

最高レベル室

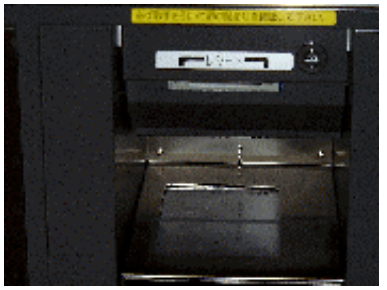

特殊鍵付ラック


JQA認定証

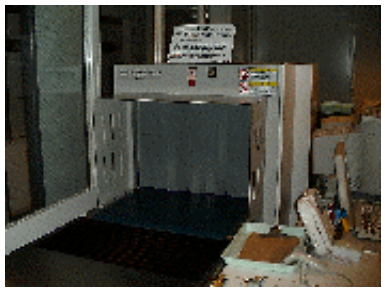

虹彩デュアルコントロール

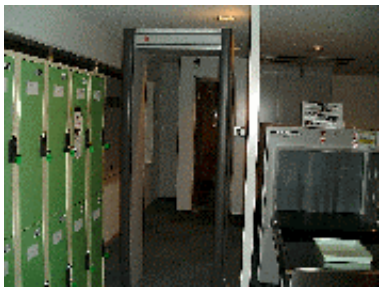

タグ検知ゲート


死角の無いカメラ設置


貴重品保管BOX


セサモID（指紋認証）


X線検査機


金属探知機


サークルゲート


常駐警備員

セコムIS研究所
Intelligent Systems Laboratory

Q&A

参考(1)

セコム IS 研究所
Intelligent Systems Laboratory

- JNSA Network Security Forum 2002でのセミナ　Challenge PKI 2001の資料
  - http://www.jnsa.org/nsf2002/r_12_b1.html
  - http://www.jnsa.org/nsf2002/pdf/B1.pdf
- NSF 2003 SpringでのJNSAのセミナーChallenge PKI 2002 とマルチドメインPKI
  - 「PKIアプリケーションの相互運用を促進するChallenge PKI 2002」
  - http://www.jnsa.org/nsf2003spring/pdf/b4.pdf
- Internet Week 2002 チュートリアルプレゼンテーション
  - PKI～技術概要と利用の実際～
  - 富士ゼロックスの稲田氏と松本が講師を務めたIWのPKIチュートリアル
  - http://www.nic.ad.jp/ja/materials/iw/2002/proceeding/
  - http://www.nic.ad.jp/ja/materials/iw/2002/proceeding/T9-1.pdf
  - http://www.nic.ad.jp/ja/materials/iw/2002/proceeding/T9-2.pdf
  - http://www.nic.ad.jp/ja/materials/iw/2002/proceeding/T9-3.pd

参考(2)

セコム IS 研究所
Intelligent Systems Laboratory

- PKI 関連相互運用性に関する調査報告(CPKI2001)
  - PKI の相互運用性に関する現状
  - http://www.ipa.go.jp/security/fy13/report/pki_interop/pki_interop.html
  - http://www.ipa.go.jp/security/fy13/report/pki_interop/pki_interop.pdf
- 電子政府情報セキュリティ相互運用支援技術の開発 (CPKI2002)
  - http://www.ipa.go.jp/security/fy14/development/pki/interop.html
  - GPKI アプリケーション実装ガイド
  - PKI 相互運用テストスィート
  - GPKI アプリケーション サンプル実装
- IPA「本人認証の現状に関する調査報告書」
  - http://www.ipa.go.jp/security/fy14/reports/authentication/index.html
  - PKI、ICカード、バイオメトリクスを中心に、電子政府における本人認証技術の提言を行っている。

セコムIS研究所
Intelligent Systems Laboratory

End