暗号を核とする情報セキュリティ評価の在り方について

2002年4月16日

暗号技術検討会顧問

暗号技術評価委員会顧問

辻井重男 (中央大学)

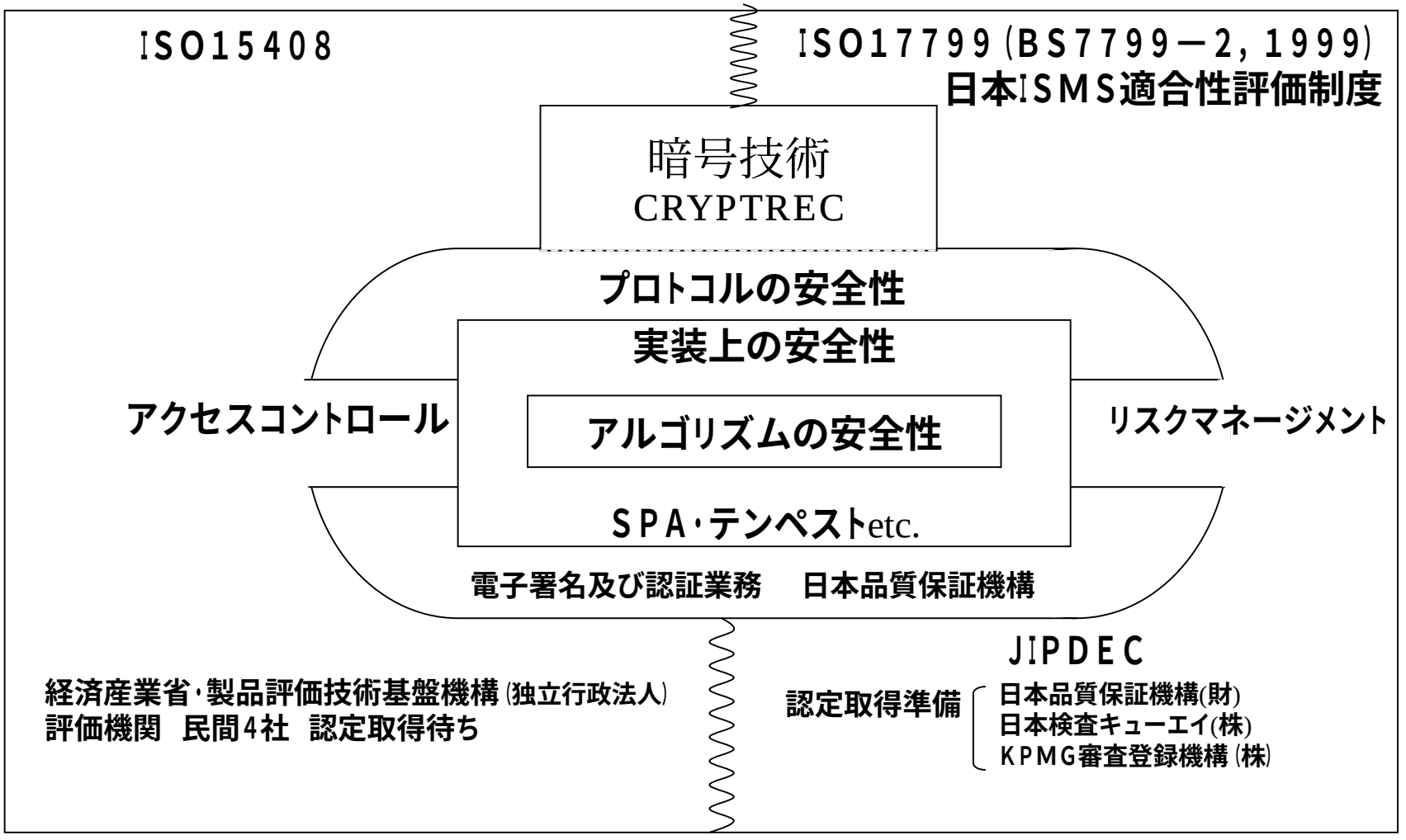
(1) 暗号については委員会組織としてのCRYPTRECが
電子政府で利用しうる暗号方式をリストアップ

(2) 情報製品に対するISO15408関連については、
独立法人製品評価技術基盤機構が評価機関を認定

(3) 運用に入った情報システム･ネットワークに対する
管理･運用基準としてのISO17799（我が国ではISMS適合性評価制度）
については、日本情報処理開発協会が評価機関を認定

(4) 電子署名及び認証業務に関する法律に対応して、
日本品質保証機構（電子署名・認証調査センター）が認証機関を認定

図1　情報セキュリティ評価基準と暗号技術



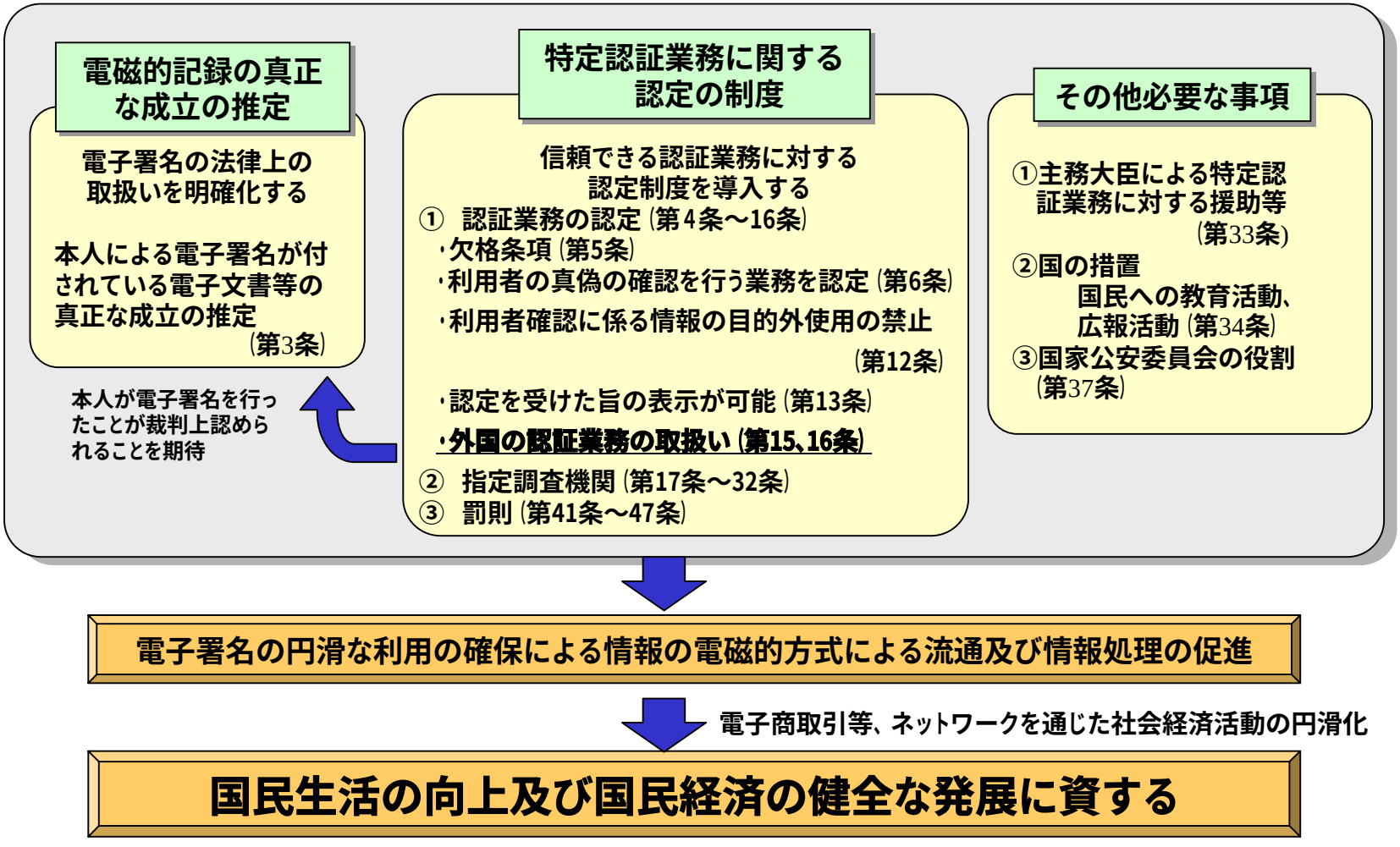
暗号理解の4段階

- 第1段階　暗号＝諜報

  軍事･外交, エシュロン

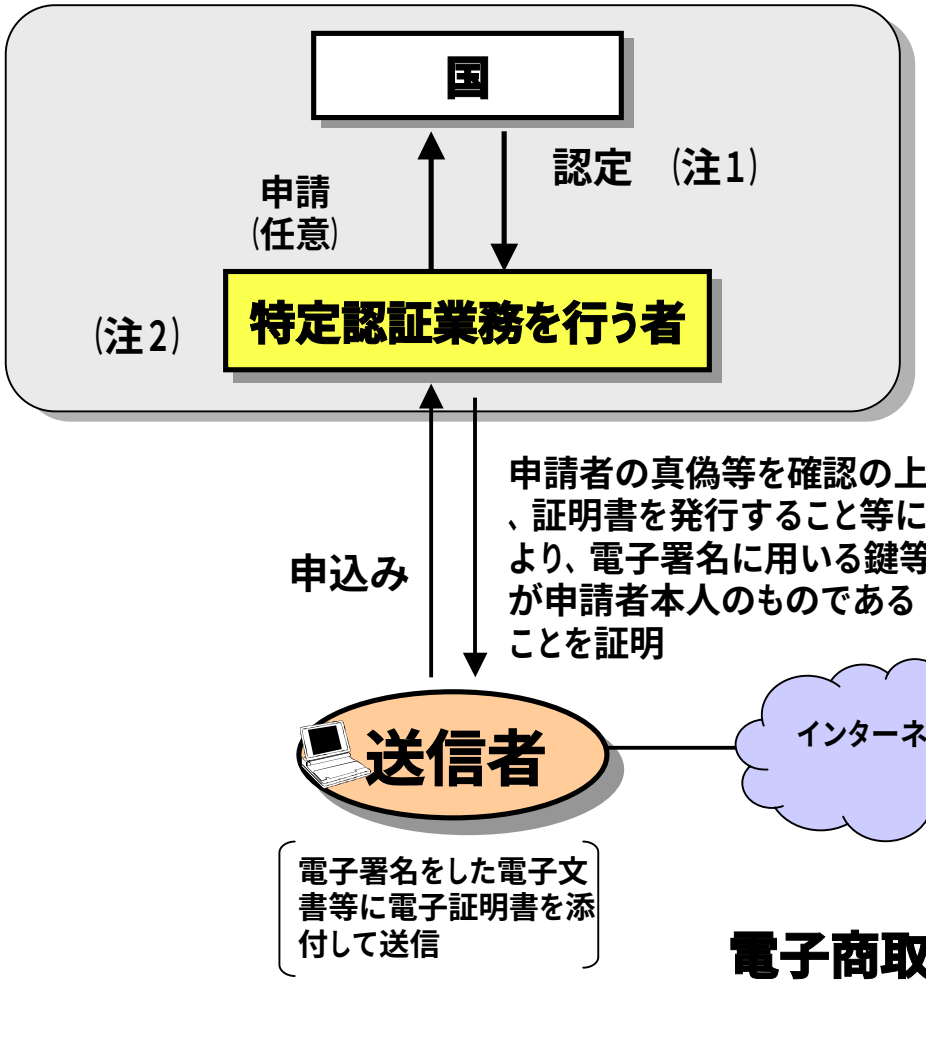
  文春新書“エシュロンと情報戦争”p.66
- 第2段階　IT社会にも必要らしい
- 第3段階　証真防偽シテ真偽峻別
- 第4段階　証明可能安全性

図2　電子署名及び認証業務に関する法律の構成



2002年3月15日電子署名法の認定基準等に関する検討会資料

図3　特定認証業務に関する認定制度



(注1)
業務の実地の調査については指定調査機関(国が指定、公益法人に限られない)に行わせることが可能。

(注2)
外国の認証事業者も認定を受けることが可能。その際、外国の承認調査機関による実地の調査を受けることができる。また**外国で認定を受けている場合に実地の調査を省略することも可能。**

2002年3月15日電子署名法の認定基準等に関する検討会資料

図４　電子署名及び認証業務に関する法律に基づく認定認証業務一覧

平成１４年３月１日現在

	第１号	第2号	第3号	第4号	第5号
認定に係る特定認証業務の名称	AccreditedSign パブリックサービス	電子入札用電子認証サービス	AccreditedSign パブリックサービス２	株式会社日本電子公証機構認証サービスiPROVE	日本行政書士会連合会認証サービス
業務を行う者の名称	日本認証サービス株式会社	株式会社帝国データバンク	日本認証サービス株式会社	株式会社日本電子公証機構	日本行政書士会連合会
業務を行う者の住所	東京都港区芝一丁目10番11号	東京都港区南青山二丁目５番２０号	東京都港区芝一丁目10番11号	東京都渋谷区代々木３丁目２５番３号	東京都目黒区青葉台三丁目１番６号
認定の年月日	平成13年7月13日	平成13年9月6日	平成13年10月19日	平成13年12月14日	平成14年3月1日
認定がその効力を失う時期	平成14年7月12日	平成14年9月5日	平成14年10月18日	平成14年12月13日	平成15年2月28日

日本認証サービス株式会社の提供するAccreditedSignパブリックサービス２については、平成１４年２月１３日付けで業務の実施方法の変更認定を行い、同年２月２２日付けで、民間認証局として初めてＧＰＫＩのブリッジ認証局との相互認証が認められたところ。

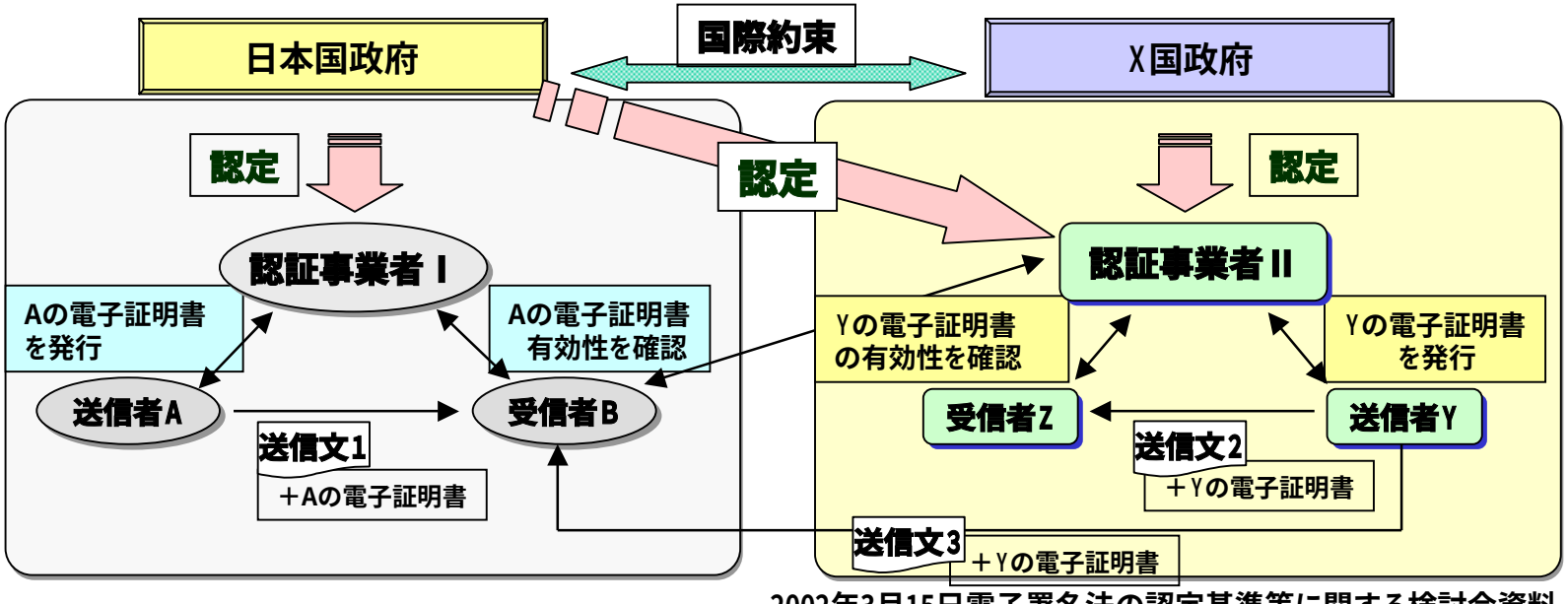
2002年3月15日電子署名法の認定基準等に関する検討会資料

図5　認定制度に係る国際相互承認について

■ **外国の認証事業者から認定の申請があった場合、下記の3つの要件を満たせば当該認証事業者は、日本の省令で定める事項を記載した書類を提出することで、実地の調査が免除される。**（電子署名法第15条第3項）

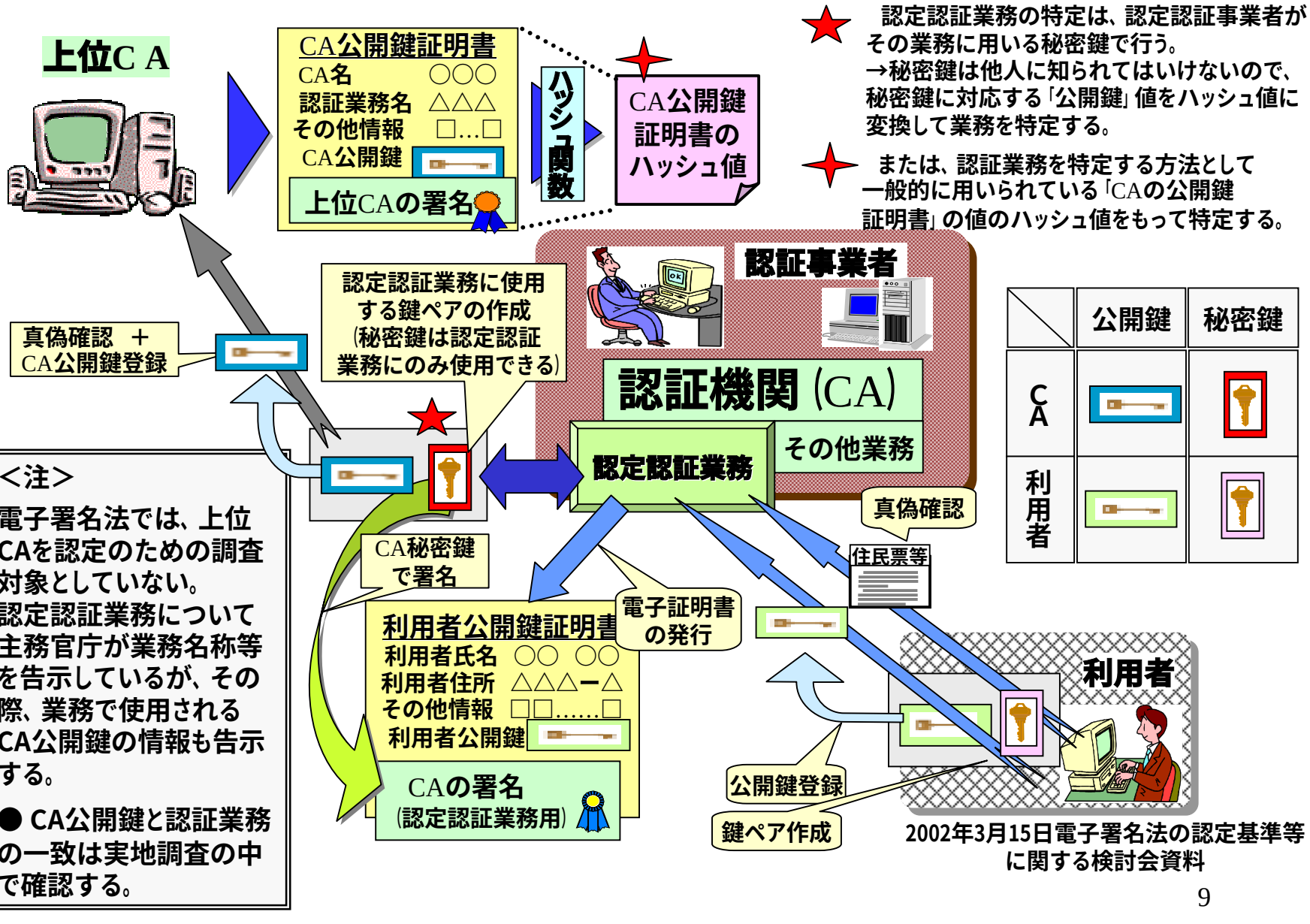
- 当該外国において、日本の認定制度に類する認定等を受けていること
- 我が国と当該外国の間で、認証事業者の相互認証等に関する国際約束等が存在していること
- 主務大臣が、その国際約束を誠実に履行するために必要があると認めたこと

※ 本年1月、日・シンガポール新時代経済連携協定（JSEPA）の中で法第15条第3項の適用を予定している国際約束が締結されている。



2002年3月15日電子署名法の認定基準等に関する検討会資料

図6　発行者署名検証符号（CA公開鍵）情報の告示について



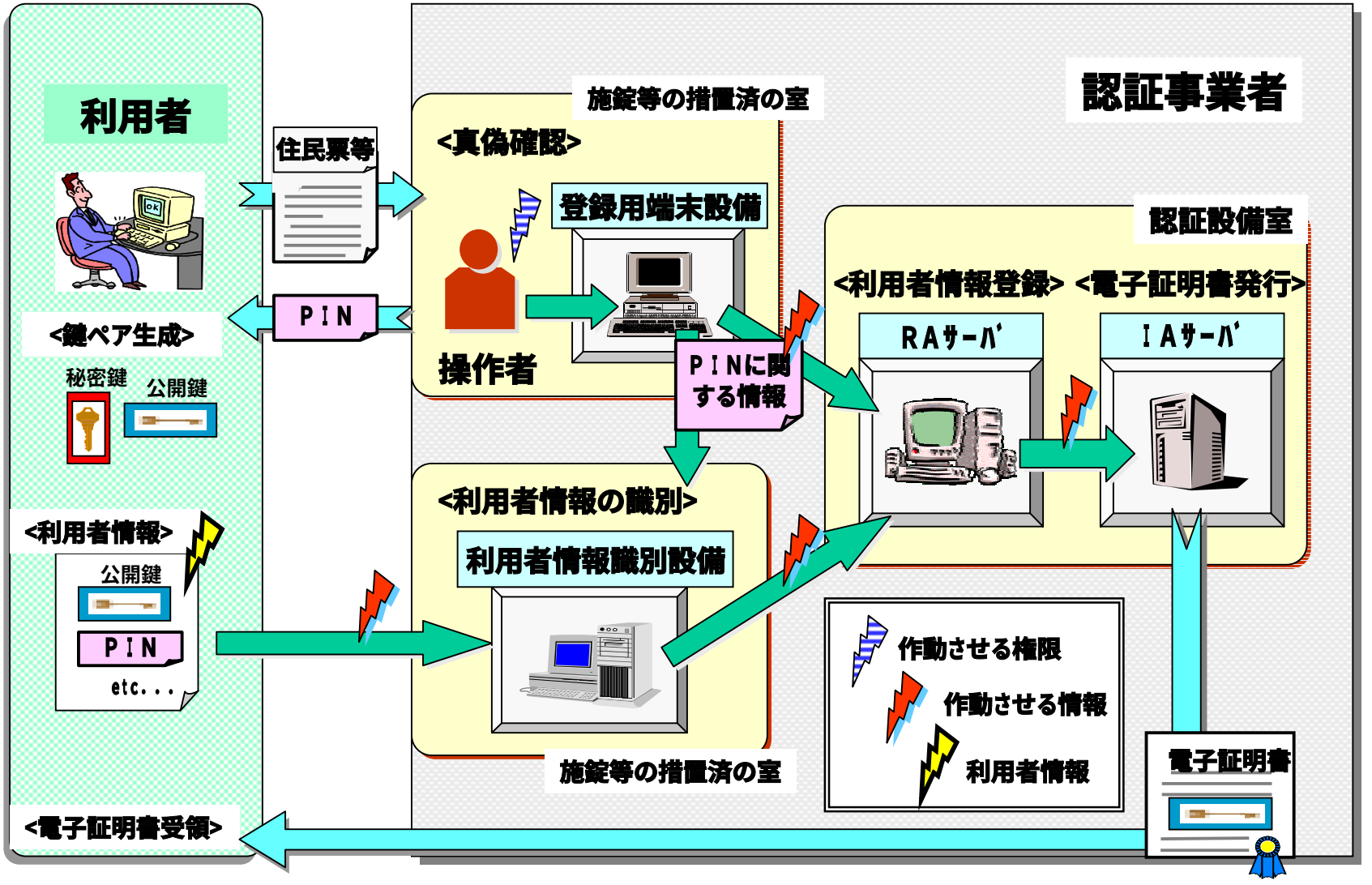
＜注＞

電子署名法では、上位CAを認定のための調査対象としていない。
認定認証業務について主務官庁が業務名称等を告示しているが、その際、業務で使用されるCA公開鍵の情報も告示する。

● CA公開鍵と認証業務の一致は実地調査の中で確認する。

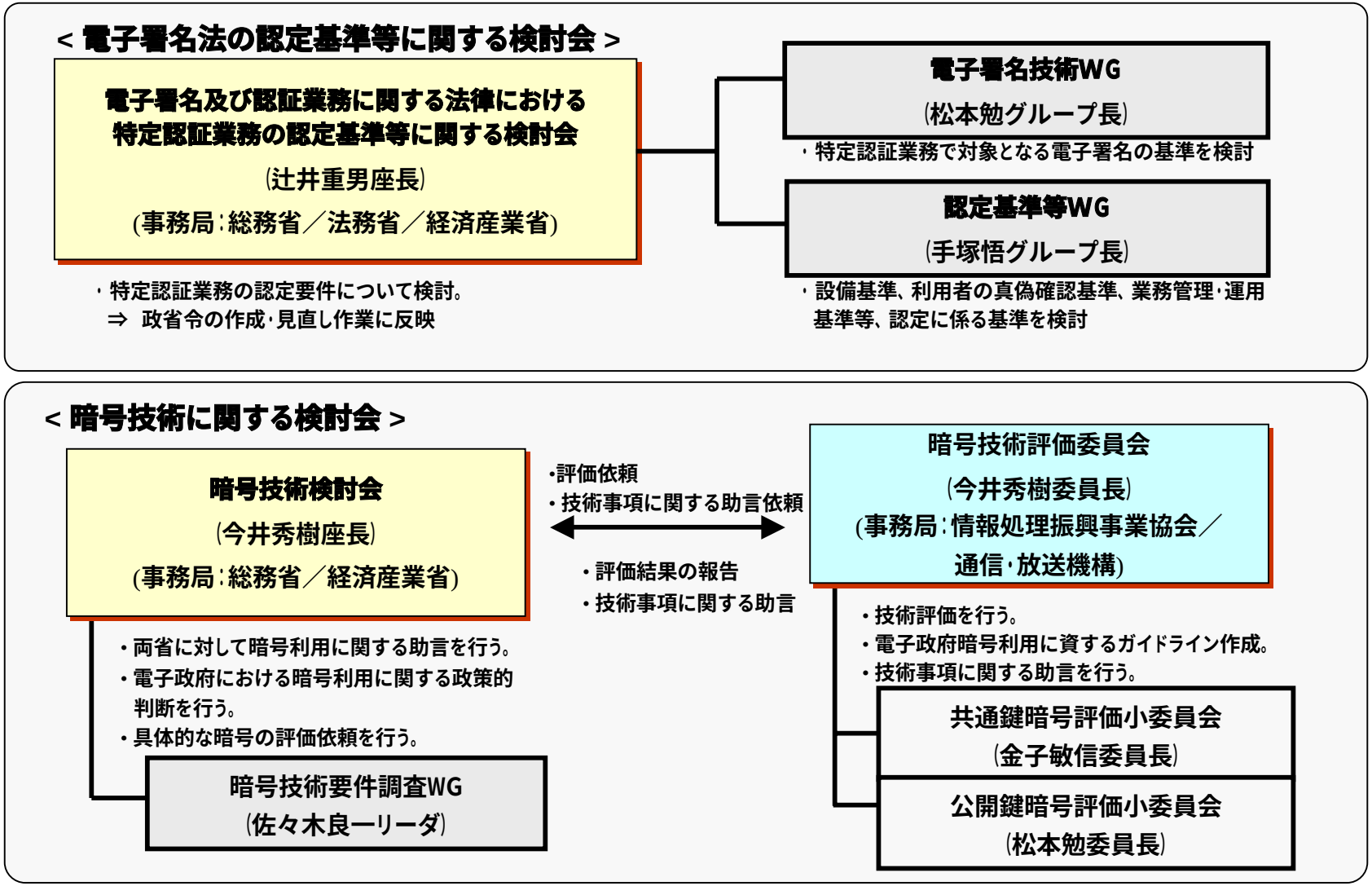
2002年3月15日電子署名法の認定基準等に関する検討会資料

図7　操作者及び利用者情報等による設備の動作について



2002年3月15日電子署名法の認定基準等に関する検討会資料

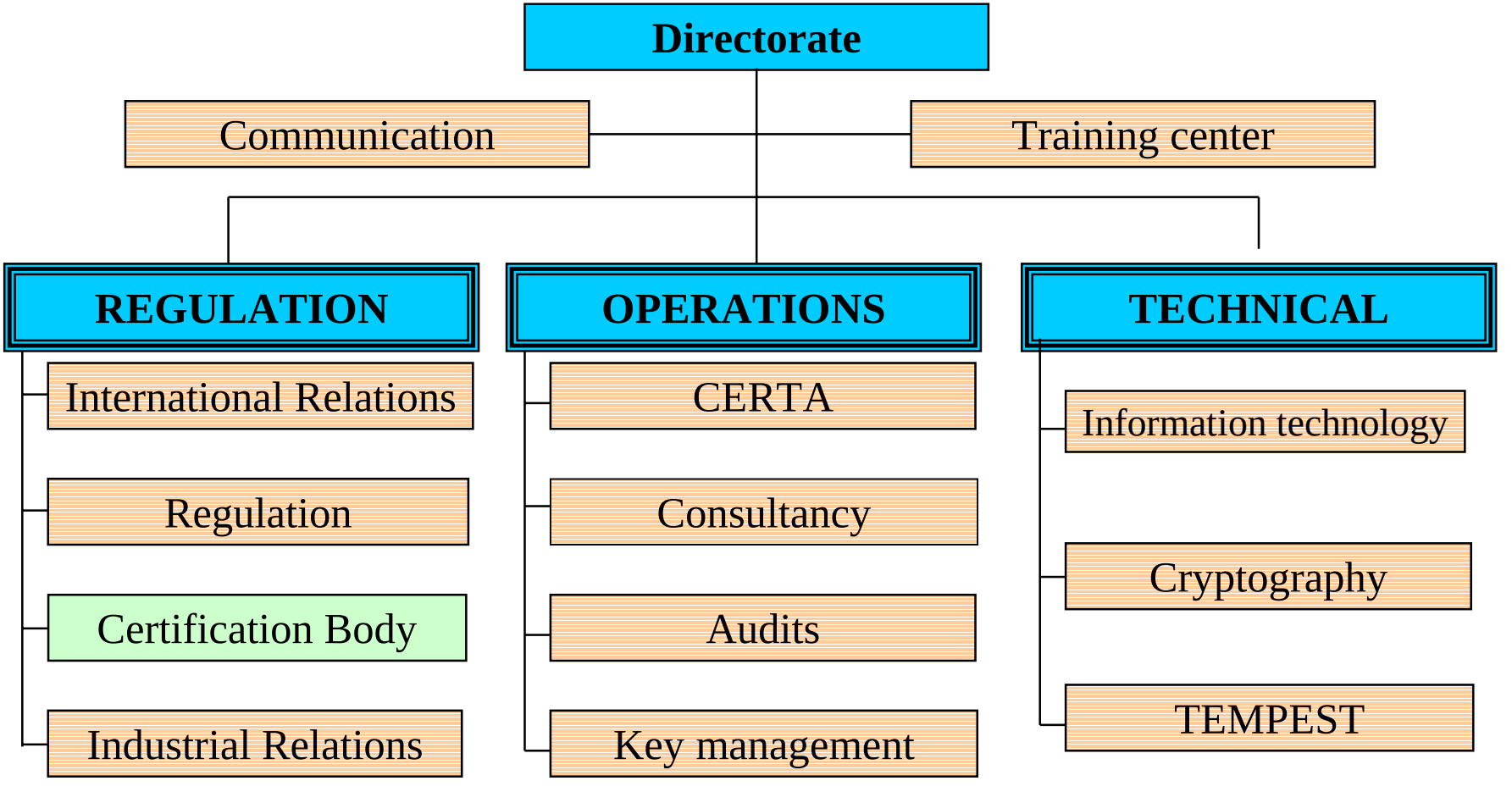
図8 「電子署名法の認定基準等に関する検討会」と「暗号技術に関する検討会」の体制



2002年3月15日電子署名法の認定基準等に関する検討会資料

図9　フランスの安全性評価･認証･認定･監査等の体制

DCSSI organization



① OECD暗号政策ガイドラインに謳われているように、
暗号・セキュリティ技術に対する信頼感の醸成
② 公的機関が利用する標準方式の選定上の必要性
③ 万一、暗号が解読されるような事態における責任問題等に関連して、
その時点での最高の技術的知見の動員による継続的安全性評価の必要性
④ グローバル化に対応して、国際間で必要となる相互承認に際しての必要性

いずれにしても、このような機関がないことには、
国家としてのインテグリィティに欠け、
我が国は諸外国から先進国としての鼎(かなえ)の軽重を問われかねない。
明治の先覚者は、通信主権の重要性をいち早く覚っていた。
現代はいわば情報セキュリティ主権の時代である。