電子政府における
暗号技術評価の位置付け

2002年4月16日

総務省情報通信政策局
通信規格課長　喜安　拓

電子政府の実現

高度情報通信ネットワーク社会形成基本法に基づく e-Japan重点計画
（2001年3月29日 高度情報通信ネットワーク推進戦略本部決定）

5．行政の情報化及び公共分野における情報通信技術の活用の推進

＜目標＞

① 行政の情報化については、行政情報の電子的提供、申請・届出等手続の電子化、文書の電子化、ペーパーレス化及び情報ネットワークを通じた情報共有・活用に向けた業務改革を重点的に推進し、**2003年度までに、電子情報を紙情報と同等に扱う行政を実現する。**

（2）施策の意義

国の行政機関においては、行政の情報化により、事務・事業及び組織の改革を推進するとともに、**セキュリティの確保に留意しつつ、**「紙」による情報の管理からネットワークを駆使した電子化された情報の管理へ移行し、**高度に情報化された行政、すなわち以下のような「電子政府」を実現**する。

- 行政情報の電子的提供
- 申請・届出等手続の電子化
- 歳入・歳出の電子化
- 調達手続の電子化
- ペーパレス化（電子化）

e-Japan重点計画における暗号技術評価の位置付け

高度情報通信ネットワーク社会形成基本法に基づく e-Japan重点計画
（２００１年3月２９日 高度情報通信ネットワーク推進戦略本部決定）

６．高度情報通信ネットワークの安全性及び信頼性の確保

（3）具体的施策

①情報セキュリティに係る制度･基盤の整備

ウ）暗号技術の標準化の推進（総務省及び経済産業省）

客観的にその安全性が評価され、実装性に優れた暗号技術を採用するため、2002年度までに、ISO、ITU等における暗号技術の国際標準化の状況を踏まえ、専門家による検討会の開催等を通じて電子政府利用等に資する暗号技術の評価及び標準化を行う。

セキュリティ・アクションプランにおける暗号技術評価の位置付け

電子政府の情報セキュリティ確保のためのアクションプラン
（２００１年１０月１０日 情報セキュリティ対策推進会議決定）

２．具体的な方策

（２）暗号の標準化の推進

- **「電子政府」におけるセキュリティ確保のためには、政府調達における一定水準のセキュリティ確保のための情報機器等に関する基準（具体的にはISO/IEC15408）を可能な限り利用することと同様、暗号についても、一定水準以上の安全性及び信頼性を有するものの利用が不可欠であり、これを推進することが必要である。**
- **このため、総務省及び経済産業省は、両省で実施している研究会の成果等も踏まえ、2002年度中に「電子政府」における調達のための推奨すべき暗号のリストを作成し、これを踏まえ、各省庁における暗号の利用方針について合意を目指す。**

政府における暗号評価への取り組み

- 総務省（旧郵政省）「暗号技術の普及・高度化に関する研究会」(2000.7)
- 情報処理振興事業協会（IPA）
  「政府調達情報セキュリティ標準（基準）に関する調査研究」(2000.10)

  ➡「暗号技術の評価」の必要性を提言

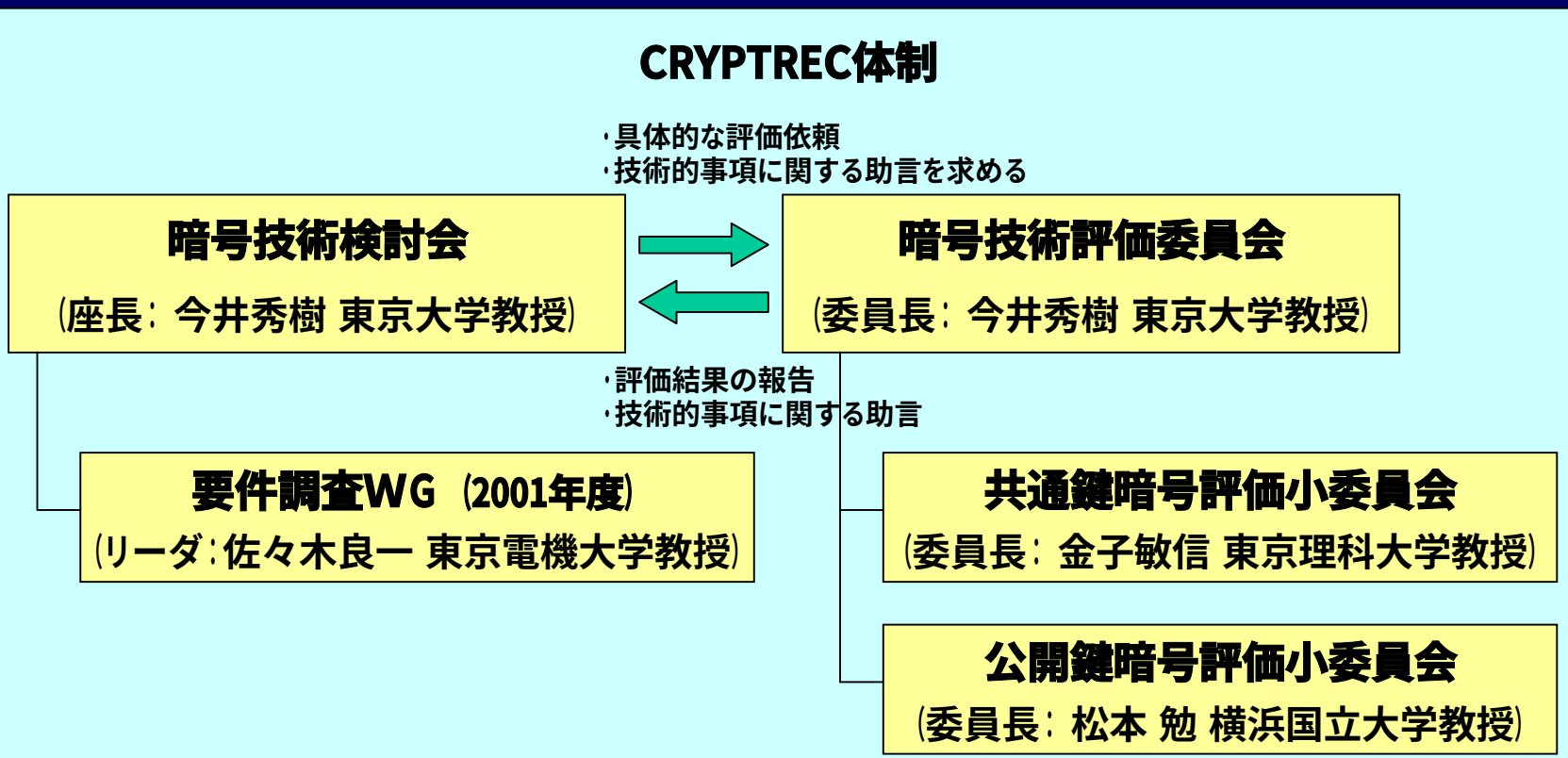
- 「暗号技術評価委員会」の設立（2000.5）
  - 経済産業省（旧通商産業省）からIPAへの委託事業
  - 経済産業省、総務省（旧郵政省及び旧総務庁）、防衛庁、内閣官房、警察庁、法務省、財務省がオブザーバ参加

- 「暗号技術検討会」の開催 (2001.5)
  - 総務省及び経済産業省が共同で開催
  - 内閣官房、警察庁、防衛庁、法務省、外務省、財務省等がオブザーバ参加

CRYPTREC (CRYPTography Research and Evaluation Committees)

- **暗号技術検討会 (事務局：総務省及び経済産業省)**
  - 暗号技術の評価を実施。
- **暗号技術評価委員会 (事務局：ＴＡＯ及びＩＰＡ)** (TAO：通信・放送機構)
  - 暗号技術の公募、具体的な技術的評価を実施。

CRYPTREC体制

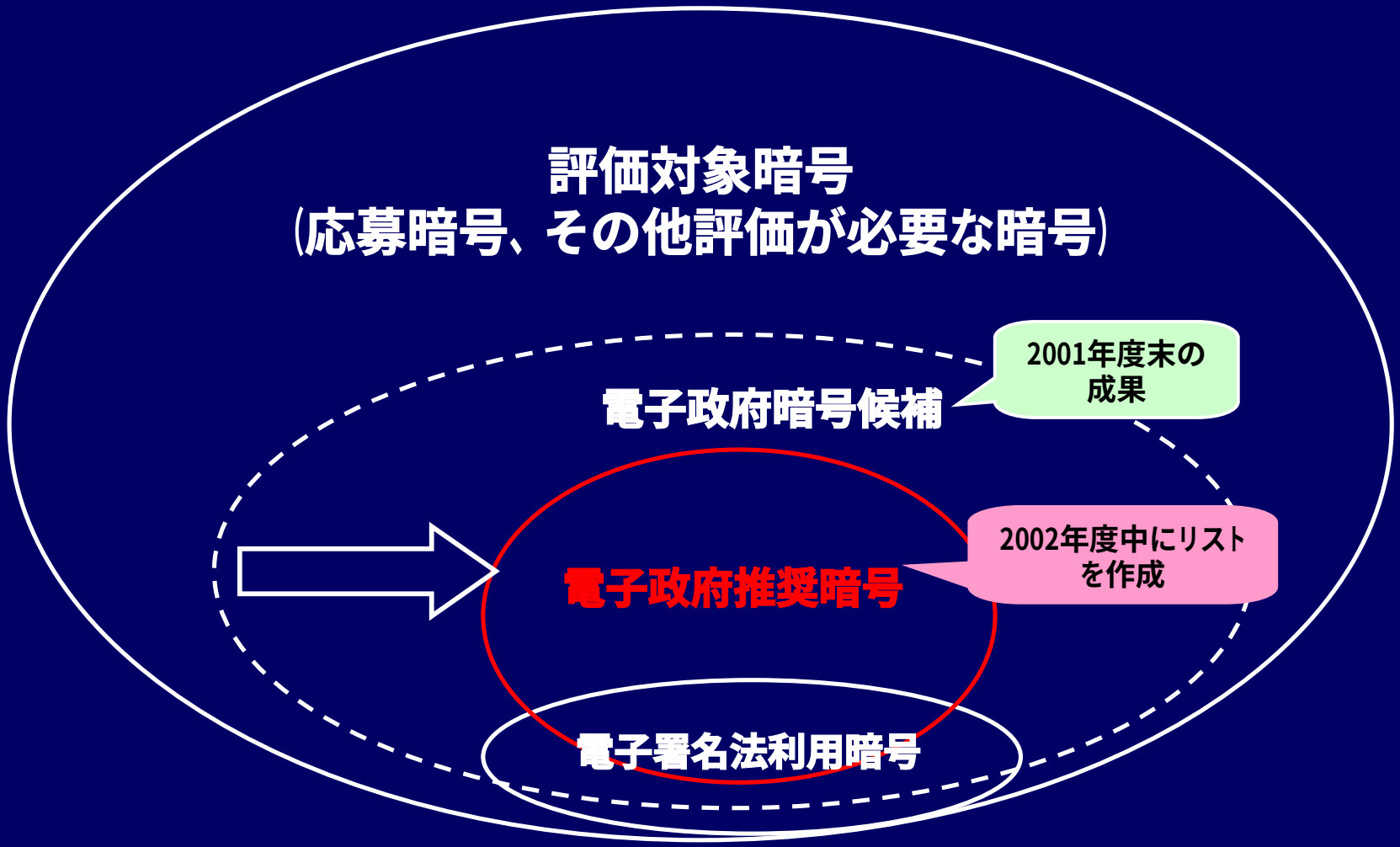


暗号技術検討会の2001年度活動内容

- **電子政府推奨暗号リストの作成のための検討**
  - 暗号技術の評価を実施し、電子政府暗号候補を提示
  - 暗号に対する技術的要件に関する調査を実施
  - SSLプロトコル自体及びSSLで利用されている暗号の評価を実施 *
- **電子署名法に基づいて利用される暗号に関する助言**
  - 電子署名法に係る指針にある署名方式に関する安全性評価を実施 *
- **暗号技術に関する国際標準化への対応**
  - ISO/IEC SC27国内委員会からの評価依頼に基づき、評価を実施 *

* 具体的な技術的評価は暗号技術評価委員会に依頼

電子政府推奨暗号


評価対象暗号
（応募暗号、その他評価が必要な暗号）
電子政府暗号候補
2001年度末の
成果
電子政府推奨暗号
2002年度中にリスト
を作成
電子署名法利用暗号

今後のスケジュール

2001年度の成果

電子政府暗号要件調査（カテゴリー及び要件）

暗号評価（電子政府暗号候補）

現在利用されている暗号に関する評価

2002年10月

電子政府暗号要件及び電子政府暗号候補の一致、リストの作成（利用形態：相手認証、鍵共有、守秘、署名）

2003年3月

電子政府推奨暗号リストの提示、調達への反映、省庁間の合意

利用方針の合意

関係の整理