CRYPTRECの活動概要

2002年1月28日

暗号技術検討会座長/暗号技術評価委員会委員長

東京大学教授　今井秀樹

CRYPTREC活動の主旨

- 国内暗号技術評価体制確立に向けた活動
- 電子政府に利用可能かの観点で
  暗号技術評価を実施
- 標準化活動支援

活動の公平性・透明性
(評価活動内容はWEBにて公開)

電子政府に利用可能な暗号技術とは

暗号技術利用方針の適用期間　　１０年程度

電子政府システムの対象

　　国民との行政サービスに関連するシステムを対象

　　地方公共団体についても考慮

国際標準

　　ISO/IEC,NESSIE,AESなどとの協力

インターオペラビリティと安全性

　　暗号用途分類と推奨暗号数

その他検討事項

　　システム調達のためのガイドブックなど

評価対象暗号技術

- 2000年度公募への応募暗号技術
- 2001年度公募への応募暗号技術
- 検討会及び委員会にて判断した
  評価が必要な暗号技術

評価対象暗号分類

公開鍵暗号
(暗号スキームと暗号プリミティブの組み合わせ)

守秘，認証，署名，鍵共有

共通鍵暗号

ストリーム暗号

６４ビット暗号，１２８ビット暗号

ハッシュ関数

擬似乱数生成系

暗号技術評価ステップ

スクリーニング評価

詳細評価を実施するための評価

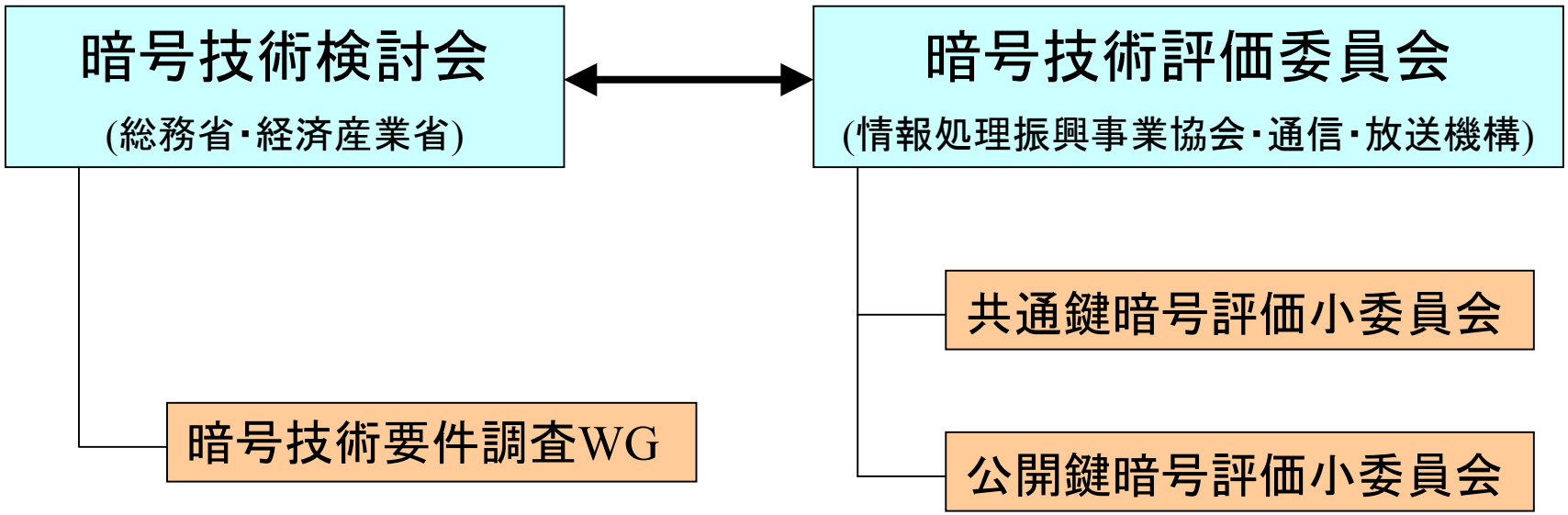
- 安全性に明らかな問題がないかの第一次評価
- 第三者実装上問題がないかの第一次評価

詳細評価

電子政府で利用可能かどうかの観点で評価

- 既知の攻撃法での統一的な評価
- 各候補暗号個別の強度評価（攻撃）
- パラメータ／鍵の設定基準に問題がないか
- ソフトウェア実装評価

CRYPTREC体制


暗号技術検討会
(総務省・経済産業省)
暗号技術評価委員会
(情報処理振興事業協会・通信・放送機構)
暗号技術要件調査WG
共通鍵暗号評価小委員会
公開鍵暗号評価小委員会

暗号技術検討会
（政策的検討が中心）

座長　今井秀樹

要件調査ＷＧリーダ　佐々木良一

－電子政府推奨暗号に関する利用方針案の作成
－暗号技術の要件を整理
－今後の暗号評価のあり方を検討

事務局　総務省・経済産業省

暗号技術検討会構成員

座長	今井　秀樹	東京大学
顧問	辻井　重男	中央大学
	生宗　潤	情報サービス産業協会
	岩下　直行	日本銀行金融研究所
	岡崎　宏	通信機械工業会
	岡本　栄司	東邦大学
	岡本　龍明	日本電信電話株式会社
	加藤　義文	(社)テレコムサービス協会
	金子　敏信	東京理科大学
	国分　明男	ニューメディア開発協会
	櫻井　幸一	九州大学
	佐々木良一	東京電機大学
	宝木　和夫	(社)電子情報技術産業協会
	苗村　憲司	慶応義塾大学
	松井　充	三菱電機株式会社
	松本　勉	横浜国立大学大学院

暗号技術評価委員会
（技術評価が中心）

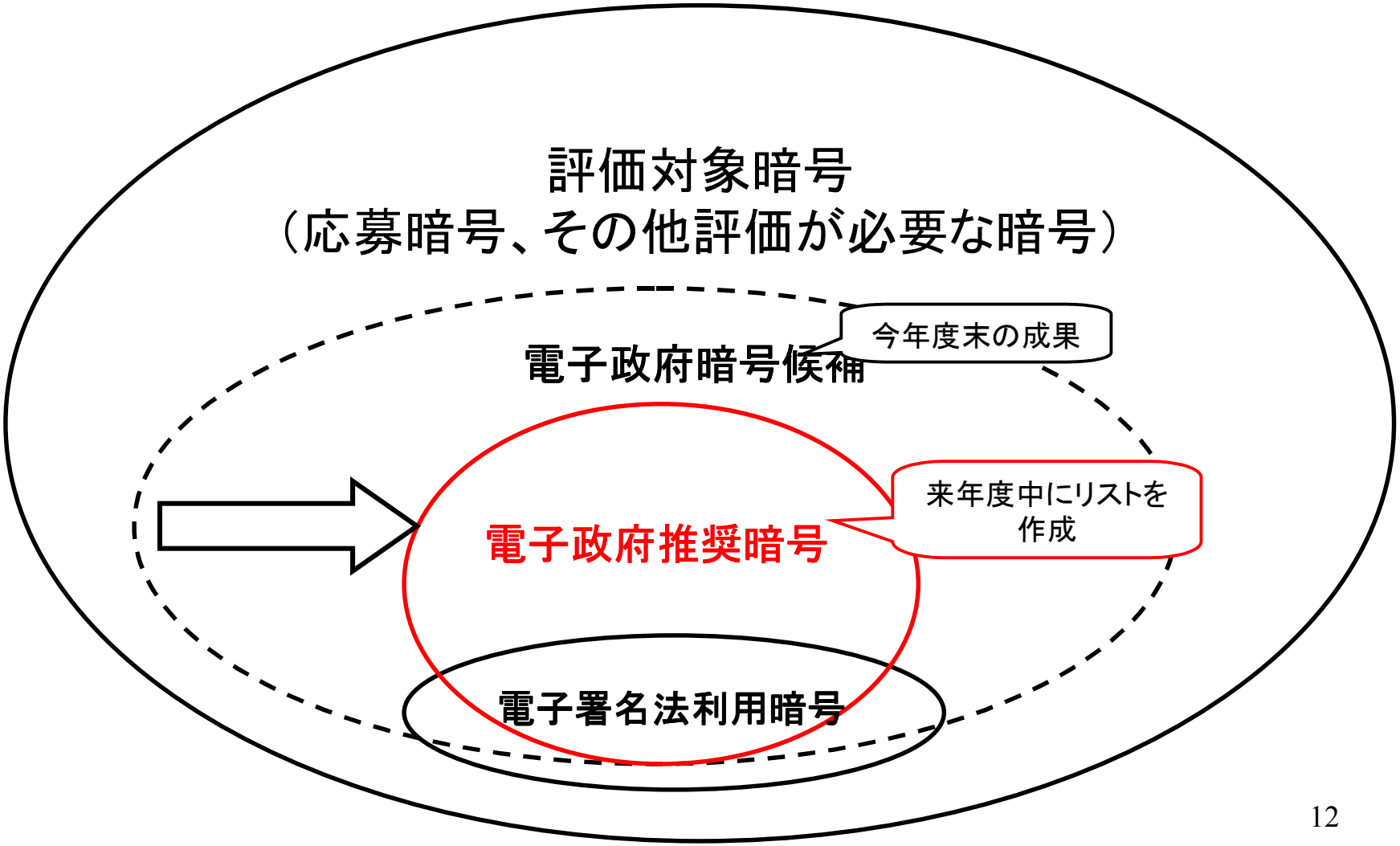
暗号技術評価委員会委員長　今井秀樹
公開鍵暗号評価小委員会委員長　松本勉
共通鍵暗号評価小委員会委員長　金子敏信
　－暗号技術分類毎の評価方法検討
　－応募暗号技術の評価

事務局　情報処理振興事業協会・通信・放送機構

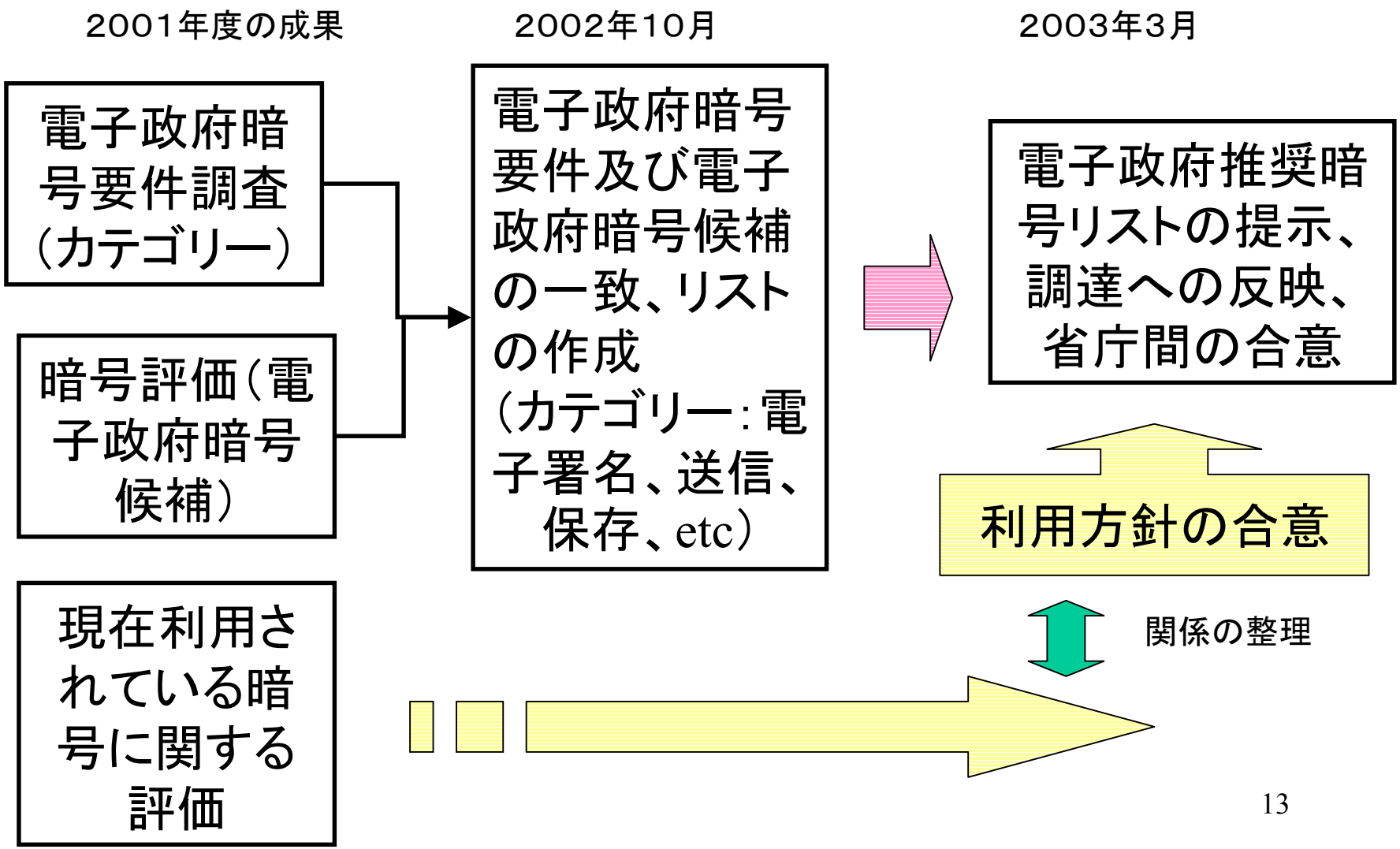
暗号技術評価委員会委員

委員長	今井	秀樹	東京大学
顧問	辻井	重男	中央大学
委員	岡本	栄司	東邦大学
委員	岡本	龍明	日本電信電話株式会社
委員	金子	敏信	東京理科大学
委員	松井	充	三菱電機株式会社
委員	松本	勉	横浜国立大学大学院

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）
今年度末の成果
電子政府暗号候補
来年度中にリストを
作成
電子政府推奨暗号
電子署名法利用暗号

電子政府推奨暗号検討スケジュール



2003年電子政府に向けて

2000年度

暗号技術評価委員会の設置

- 電子政府暗号技術の公募
- 電子政府暗号技術の評価(スクリーニング評価と詳細評価)

2001年度

暗号技術検討会の設置

- 暗号評価のあり方検討
- 電子政府の暗号技術要件の整理

暗号技術評価委員会

- 電子政府暗号技術の2次公募
- 電子政府暗号技術の評価(スクリーニング評価と継続評価)

2003年電子政府に向けて

2002年度活動予定

電子政府推奨暗号の選定

　　要件調査分類と暗号技術評価分類の整理

電子政府システム調達のためのガイドブック

暗号技術検討会

　　暗号技術要件確定

暗号技術評価委員会

　　電子政府暗号技術の評価　(詳細評価と継続評価)

　　2002年度は新規公募の予定無し

今年度報告書の発表予定

2002年4月16日　CRYPTREC 2001報告会

暗号技術検討会報告書

暗号評価委員会報告書

CRYPTREC Report 2001

(2001年度評価報告書+暗号技術仕様)

暗号技術活用ガイドライン

今後の課題

電子政府システム調達に必要な情報

JIS-TR化

暗号技術調達ガイドブック

暗号実装プロトコルやモジュール評価

中立・公的機関による恒久的な評価

国際連携

AES,ISO/IEC,NESSIEなどとの協力

コメント募集中

評価対象暗号技術に関するコメントを受付中

送付先メールアドレス

cryptrec-comment@ipa.go.jp

詳細はCRYPTRECホームページ:

IPA:http://www.ipa.go.jp/security/enc/CRYPTREC/index.html

TAO:http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html