CRYPTREC活動報告

―2000～2002年―

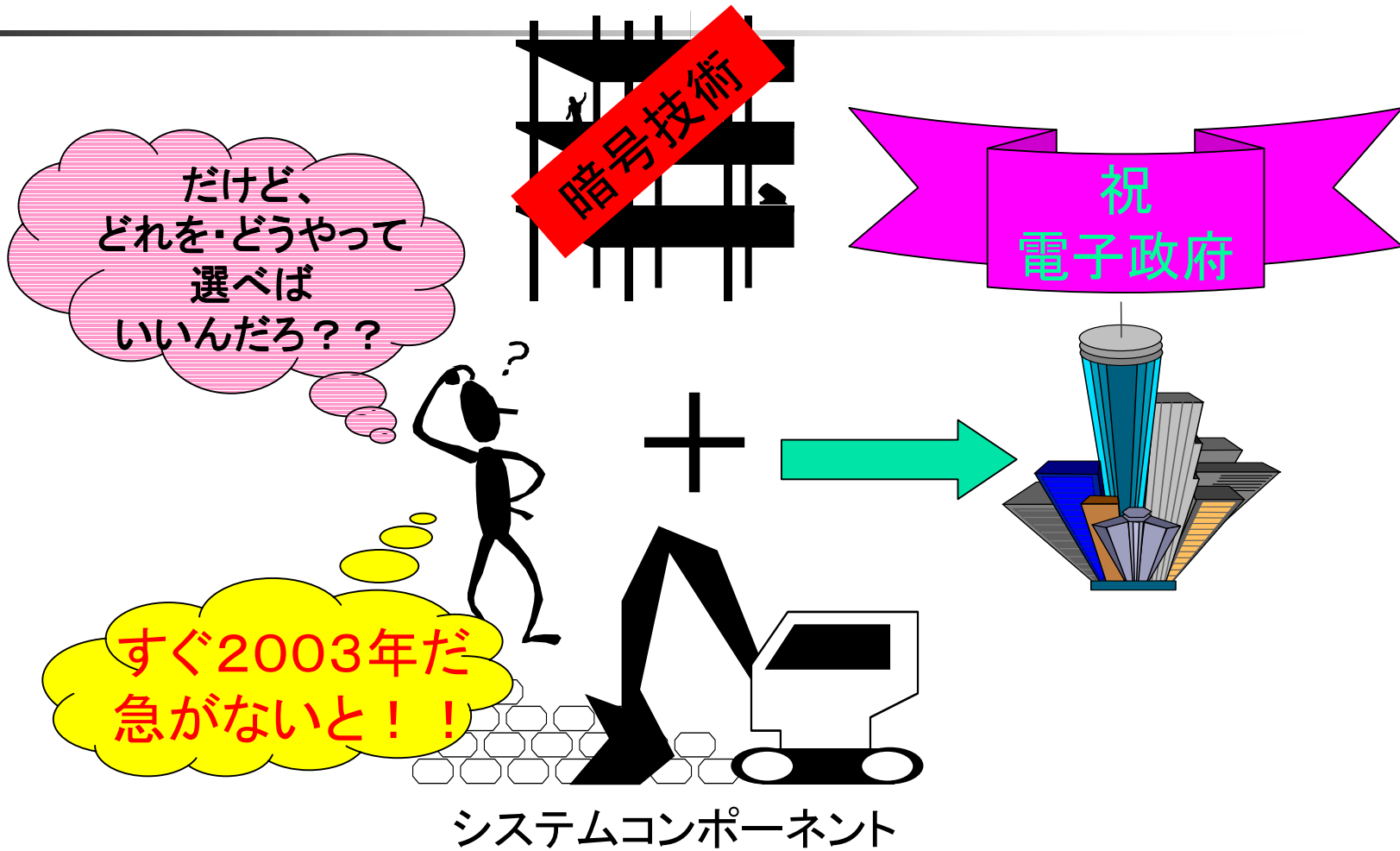
2003年5月22日

暗号技術検討会座長
暗号技術評価委員会委員長
今井秀樹(東京大学)

はじめに

- CRYPTRCの背景
  - 2003年度に電子政府の構築
  - セキュリティ基盤の確立が急務
  - 一般には，暗号技術の評価は極めて困難
- 活動目標
  - 暗号アルゴリズムを公募し選定
  - 専門的観点から安全性や実装性を評価し、電子政府で利用可能な暗号をリストアップ
  - 国内暗号技術評価体制確立に向けた活動

CRYPTRECの背景



CRYPTREC体制

暗号技術検討会

(事務局：総務省，経済産業省)

- 電子政府の暗号に関する政策検討
- 暗号に関する政府への助言
- 暗号技術の要件抽出
- 暗号技術の普及促進

暗号技術要件調査WG（2001年度）

暗号調達ガイドブック作成WG （2002年度）

暗号技術評価委員会

(事務局：情報処理振興事業協会，通信・放送機構)

- 暗号技術の評価
- 検討会に対する技術的助言
- 暗号技術評価手法の検討

共通鍵暗号評価小委員会

公開鍵暗号評価小委員会

電子政府に利用可能な暗号技術とは

- 電子政府システムを対象
  - 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
- 適用期間10年程度
- 国際標準との整合性
  - ISO/IEC,NESSIE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
- 使いやすい暗号
  - 暗号調達のためのガイドブックなど

暗号技術評価委員会の目的

- 電子政府に推奨できる暗号技術の提示
  - 電子政府システムに適用可能な暗号技術を公募
  - 暗号技術を技術的・専門的見地から評価
  - 安全性、実装性等の特徴を分析・整理したリストを作成
- 暗号技術標準化への貢献
- 暗号技術に対する信頼感醸成
  - 活動の公平性・透明性（評価活動内容はWEBにて公開など）

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
	岩下　直行	日本銀行金融研究所
	岡崎　宏	情報通信ネットワーク産業協会
	岡本　栄司	筑波大学
	岡本　龍明	日本電信電話株式会社
	小田　雅一	社団法人情報サービス産業協会
	小柳津　育郎	NTTエレクトロニクス株式会社
	加藤　義文	社団法人テレコムサービス協会
	金子　敏信	東京理科大学
	国分　明男	財団法人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	社団法人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	筑波大学
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

公開鍵暗号技術評価小委員会

委員長	松本 勉	横浜国立大学 大学院
委員	有田 正剛	日本電気株式会社
委員	太田 和夫	電気通信大学
委員	小暮 淳	株式会社富士通研究所
委員	酒井 康行	三菱電機株式会社
委員	静谷 啓樹	東北大学
委員	新保 淳	株式会社東芝
委員	洲崎 誠一	株式会社日立製作所
委員	松崎 なつめ	松下電器産業株式会社
委員	渡辺 創	独立行政法人産業技術総合研究所

共通鍵暗号技術評価小委員会

委員長	金子 敏信	東京理科大学
委員	荒木 純道	東京工業大学 大学院
委員	青木和麿呂	日本電信電話株式会社
委員	川村 信一	株式会社東芝
委員	香田 徹	九州大学 大学院
委員	古原 和邦	東京大学
委員	櫻井 幸一	九州大学 大学院
委員	下山 武司	株式会社富士通研究所
委員	宝木 和夫	株式会社日立製作所
委員	館林 誠	松下電器産業株式会社
委員	角尾 幸保	日本電気株式会社
委員	時田 俊雄	三菱電機株式会社
委員	森井 昌克	徳島大学

オブザーバー

関係各省庁のオブザーバー参加による横断的な体制づくり

- 内閣官房
- 警察庁
- 防衛庁
- 総務省
- 法務省
- 外務省
- 財務省
- 経済産業省

暗号技術評価委員会

暗号技術評価委員会

関係省庁

第１線の研究者

2000年度の暗号技術評価活動

- 2000年5月　　暗号技術評価委員会の設置
- 2000年6-7月　　2000年度暗号技術の公募
- 2000年8-10月　　2000年度スクリーニング評価
- 2000年10月　　暗号技術シンポジウム
- 2000年10月-01年3月　2000年度詳細評価
- 2001年3月　　「CRYPTREC Report 2000」作成
- 2001年4月　　暗号技術評価報告会(2000年度)
- 2001年11月　　JIS-TR(CRYPTREC Report 2000)

2001年度の暗号技術評価活動

- 2001年5月　　暗号技術検討会の設置
- 2001年6月　　要件調査WGの設置
- 2001年8-9月　　2001年度暗号技術の公募
- 2001年10月　　応募暗号説明会
- 2001年8月-02年3月　2001年度詳細評価・スクリーニング評価
- 2002年1月　　暗号技術評価ワークショップ
- 2002年3月　　「CRYPTREC Report 2001」作成
- 2002年4月　　暗号技術評価報告会(2001年度)
- 2003年3月　　JIS-TR(CRYPTREC Report 2001)

2002年度の暗号技術評価活動

- 2002年5月　　暗号調達ガイドブック作成WG設置
- 2002年4－11月　　詳細評価
- 2002年10月－03年1月　　電子政府推奨暗号リスト作成
- 2002年10月－03年2月　　2003年度以降の活動・体制の検討
- 2003年3月　　「CRYPTREC Report 2002」作成
- 2003年5月　　暗号技術評価報告会(2002年度)

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
- 評価が必要な暗号技術と判断した暗号技術
  - 暗号技術検討会からの評価依頼などにより暗号技術評価委員会が判断

評価対象暗号分類

- 公開鍵暗号
  - 守秘，認証，署名，鍵共有
- 共通鍵暗号
  - ストリーム暗号
  - 64ビットブロック暗号，128ビットブロック暗号
- ハッシュ関数
- 擬似乱数生成系

暗号技術評価

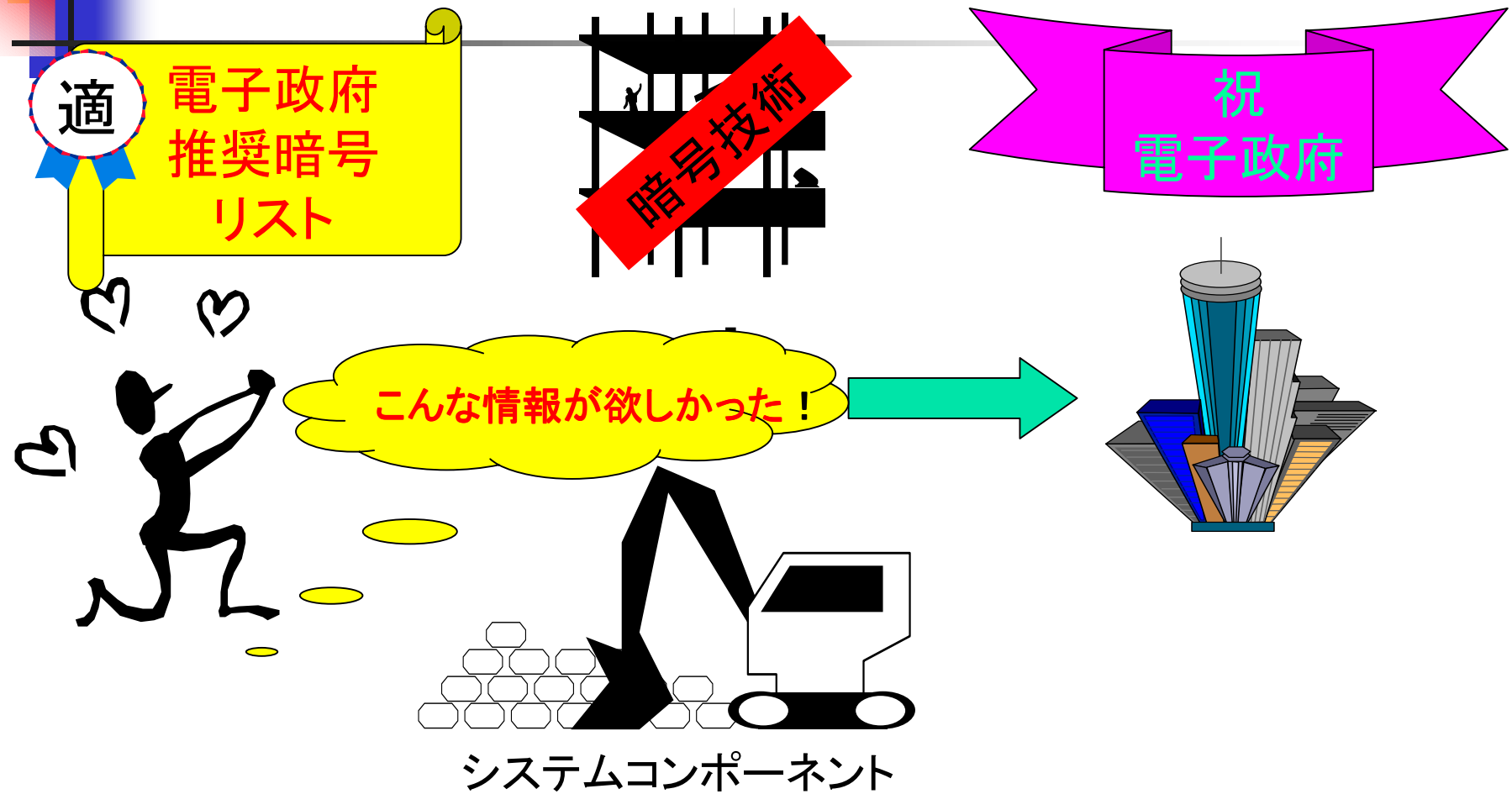
- 国内外の専門家による外部評価
- 技術情報の公開(ワークショップやCall for comments)
- ２段階(スクリーニング評価と詳細評価)評価
- スクリーニング評価(詳細評価対象暗号技術の絞込み)
  - 安全性に明らかな問題がないかの第一次評価
  - 第三者実装上問題がないかの第一次評価
- 詳細評価
  - 既知の攻撃法での統一的な評価
  - 各候補暗号個別の強度評価(攻撃)
  - パラメータ／鍵の設定基準に問題がないか
  - ソフトウェア実装評価

評価結果の概要

	公開鍵暗号				共通鍵暗号			ハッシュ関数	擬似乱数生成系	その他
	守秘	署名	鍵共有	認証	64bitブロック暗号	128bitブロック暗号	ストリーム暗号			
応募総数	9	10	8	1	4	9	9	0	9	2
評価総数	10	15	9	1	6	11	10	6	15	2
最終結果	2	4	3	0	4	5	3	5	3＊	0

＊は例示

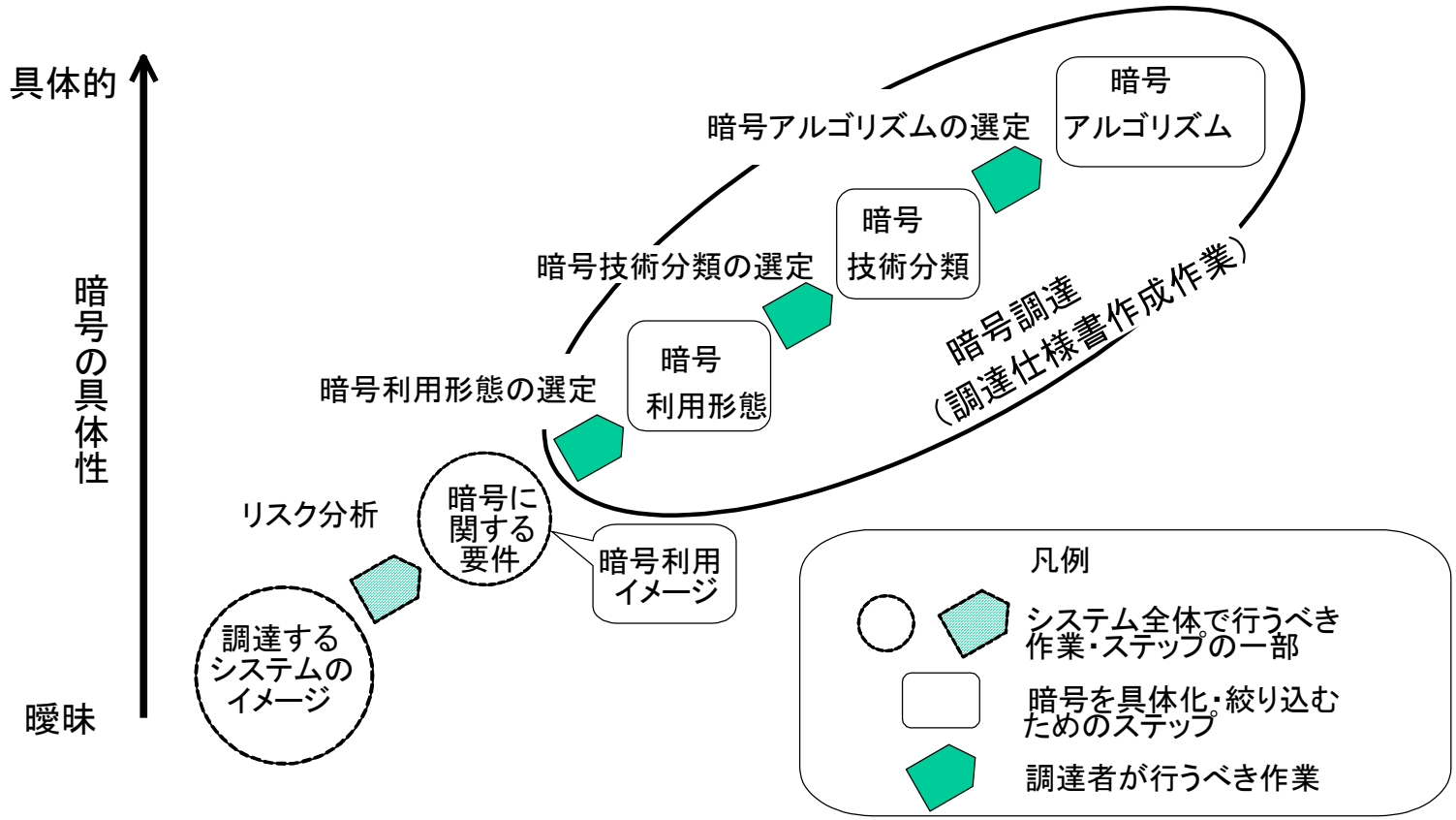
CRYPTRECの成果



暗号調達ガイドブック

- 目的
  - 暗号の利用目的の抽出から暗号アルゴリズムの選定までの手引き
  - 電子政府推奨暗号及び電子政府推奨暗号リストの解説
  - 調達仕様書作成にあたり、暗号に関連して留意すべき点を示す

選定までのステップ


具体的
暗号の具体性
曖昧
調達するシステムのイメージ
リスク分析
暗号に関する要件
暗号利用イメージ
暗号利用形態の選定
暗号利用形態
暗号技術分類の選定
暗号技術分類
暗号アルゴリズムの選定
暗号アルゴリズム
暗号調達（調達仕様書作成作業）
凡例
システム全体で行うべき作業・ステップの一部
暗号を具体化・絞り込むためのステップ
調達者が行うべき作業

まとめ（1）

- CRYPTRECの意義
  - 暗号技術の中立的評価
  - ユーザ（政府）自身による評価
  - 日本の暗号技術の進展に貢献
- 評価の結果
  - 当初の目的（暗号のリストアップ）は果たせた
  - 継続的な情報収集／評価の必要性を指摘
    - 詳細評価結果の検証の時間が必要
    - 現在の技術での評価→技術進歩による変化

まとめ（2）
～海外プロジェクトとの連携～

- 国際プロジェクト
  - ISO／IEC JTC1での暗号標準化
  - 欧州（NESSIE）
- 評価基準のレベル合わせ
  - 意見交換
  - 評価結果の共有

NESSIE プロジェクト（参考１）

- 欧州委員会が行なった欧州暗号標準化計画

New European Schemes for Signatures, Integrity, and Encryption

2000年1月	NESSIEプロジェクト開始
2000年3月	公募要項公開
2000年9月	公募締め切り
2000年11月13,14日	第1回 NESSIE会議(ベルギー)
2001年9月12,13日	第2回 NESSIE会議（イギリス）
2001年10月	第1次選考
2002年10月	第3回 NESSIE会議
2003年2月	第4回 NESSIE会議 最終選考

http://cryptonessie.org/

NESSIE プロジェクト(参考2)

- NESSIEの最終目標は産学の「コンセンサス」
  ISO 等の標準化活動へのはたらきかけ
- IPR (Intellectual Property Rights) Jungle
  NESSIE は応募アルゴリズムの IPR に対する強制力をもたない
- 選考結果は大きな影響力をもつ
  幅広い対象、超一流の主催者グループ，Industrial board との協調
- 日本製・日本生まれの暗号の活躍
  公開鍵暗号：(守秘)PSEC-KEM(1／3)，(署名)SFLASH(1／3)

  共通鍵暗号：(64ビットブロック暗号)MISTY1(1／1)
  (128ビットブロック暗号)Camellia(1／2)

CRYPTREC vs NESSIE

- 共通点
  - それぞれの立場からの主体的・自主的な評価
  - 専門家による評価
  - リスト作成
  - 安全性だけでなく実装性も考慮
- 違い
  - 監視体制の有無
  - 用途
    - CRYPTRECは電子政府用途が主目的
    - NESSIEは産学のコンセンサスづくり

まとめ（3）

- 期間的な問題
  - 2003年までに評価完了が至上命題
  - 事前検討を含め4年間
    - 評価できなかった技術も存在
  - 組織の立ち上げと評価が同時並行
- 公募（評価）対象
  - 選択と集中が必要
  - ユーザーのニーズ（電子政府での用途）が曖昧

将来への課題(1)

- 暗号技術評価の継続
  - 組織・体制づくりの整備
    - 今後開発される技術の評価
  - 継続的な評価が重要
  - 実装された暗号製品の評価
- 成果の活用
  - 実装環境の整備

今後のCRYPTREC体制図

暗号技術検討会　（事務局：総務省、経済省）

（事務局：ＴＡＯ、ＩＰＡ）

暗号技術監視委員会

（１）電子政府推奨暗号の監視
（２）暗号アルゴリズム等を主な対象とする調査・検討
（３）電子政府推奨暗号リストの改訂に関する調査・検討

暗号技術調査WG

暗号モジュール委員会

（１）暗号モジュール評価基準及び試験基準の作成
（２）暗号実装関連技術を主な対象とする調査・検討

将来への課題(2)

- **暗号技術監視委員会**
  - **電子政府推奨暗号の監視**
  - **暗号アルゴリズムを主な対象とする調査・検討**
  - **電子政府推奨暗号リストの改訂に関する調査・検討**
  - 恒久的セキュリティ研究機関への布石

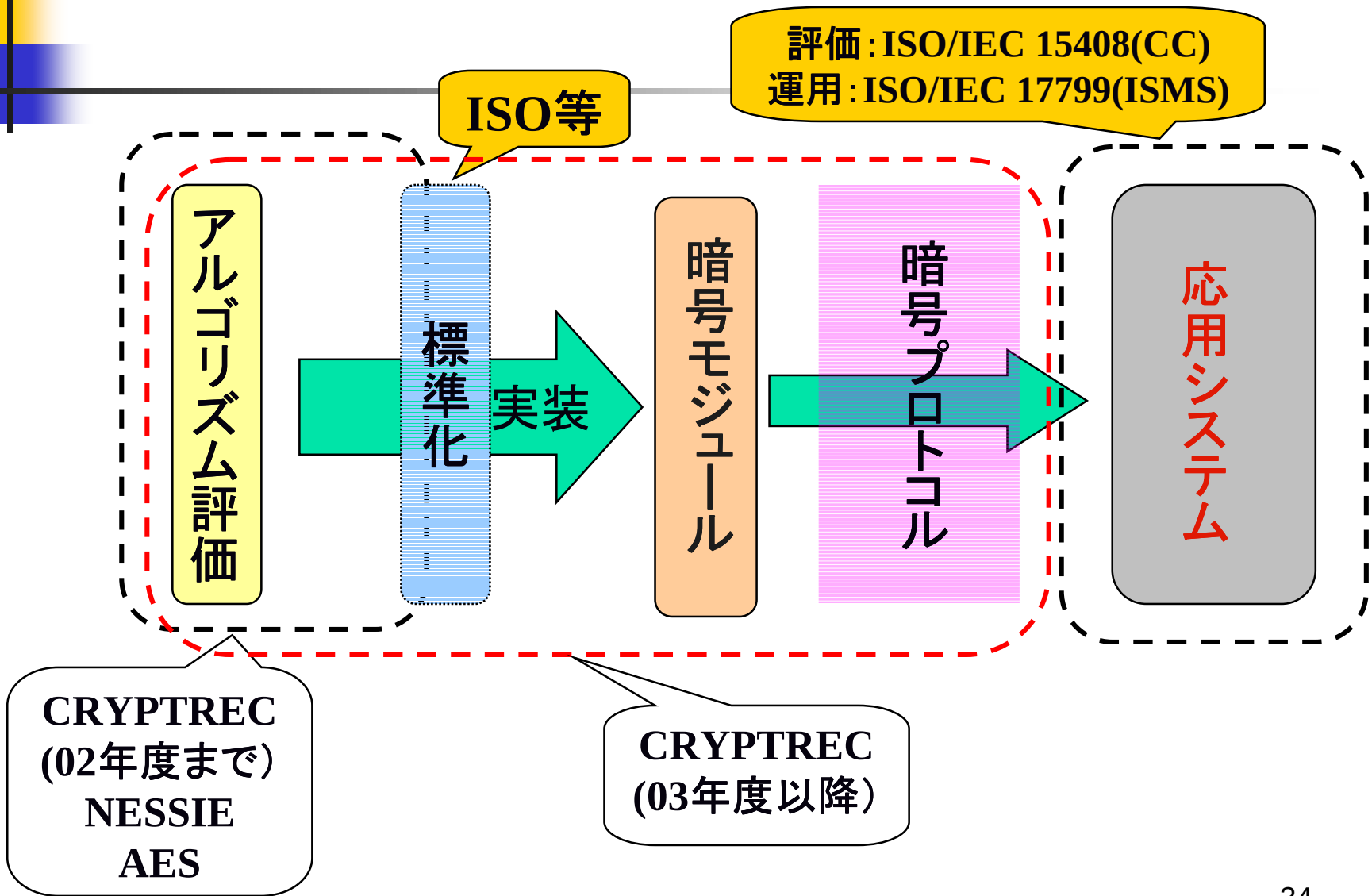
将来への課題(3)

- **暗号モジュール委員会**
  - **暗号モジュール評価基準の作成**
  - **暗号モジュール試験基準の作成**
  - **暗号実装関連技術等**
    - **耐タンパー技術、サイドチャネル攻撃等**
  - **政府調達基準等も視野に入れ** る
  - 評価・認証制度の構築

将来への課題(4)

- 暗号プロトコルの調査研究
  - 暗号プロトコルの安全性評価手法の調査研究
- 推奨リストの活用
  - 電子政府から一般の情報セキュリティシステムへ
  - 推奨暗号の利用は安全な情報セキュリティシステムの試金石

暗号技術評価の位置づけ



CRYPTRECホームページ

詳細な情報や問合せについて

- 情報処理振興事業協会

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

- 通信・放送機構

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

謝辞

- 暗号技術検討会
- 暗号技術評価委員会
- **暗号調達ガイドブック作成**WG
- **共通鍵暗号評価小委員会**
- **公開鍵暗号評価小委員会**

の委員諸氏の献身的努力に感謝します。

- **オブザーバー，事務局（総務省/経済産業省**/TAO/IPA)

お疲れ様でした．今後も宜しくお願いします．