暗号技術評価委員会 CRYPTRECについて

暗号技術評価委員会委員長
東京大学生産技術研究所
今井秀樹
http://imailab-www.iis.u-tokyo.ac.jp/

情報セキュリティ技術が支えるネットワーク社会

ネットワーク社会

政治	経済	文化
電子投票 電子役所 電子警察 電子公証	電子商取引 電子決済 （電子マネー）	コンテンツ流通 著作権保護

法・制度・保険
運用・管理

社会制度

倫理
監視・監査
教育・啓発など

セキュリティシステム構築技術

情報セキュリティシステム技術

セキュアプロトコル技術　　PKI構築技術

アクセス制御技術　　鍵回復技術　　侵入検知技術

情報セキュリティ要素技術

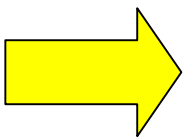
個人認証技術　　暗号技術　　電子透かし技術

PKI: (Public Key Infrastructure)

電子情報通信学会誌900号より

設立の経緯
～CRYPTREC以前の動き～

- 情報処理振興事業協会（IPA)の調査研究
  - コンサルティング委員会
- 総務省（旧郵政省）「暗号通信の普及・高度化に関する研究会」
  - 技術分科会
- 共通の結論
  - 国内で暗号技術を評価できる体制が必要



経済産業省（旧通商産業省）の電子政府情報セキュリティ技術開発事業の一環として、情報処理振興事業協会へ委託（調査事業）

プロジェクトへの要求の背景

- OECD「暗号政策に関するガイドライン」
  - 原則1　暗号手法に対する信頼

    暗号手法は，情報通信システムの利用に対する信頼感を醸成するため，信頼に足るものであるべきである。

    市場は，安心できるシステムに対する信用を樹立するのに資するべきであって，政府の規則，ライセンス，及び暗号手法の利用もまた，ユーザの信頼を促進することができる。

    （堀部政男教授監訳）

プロジェクトへの要求の背景

- OECD「暗号政策に関するガイドライン」
  - 原則2　暗号手法の選択

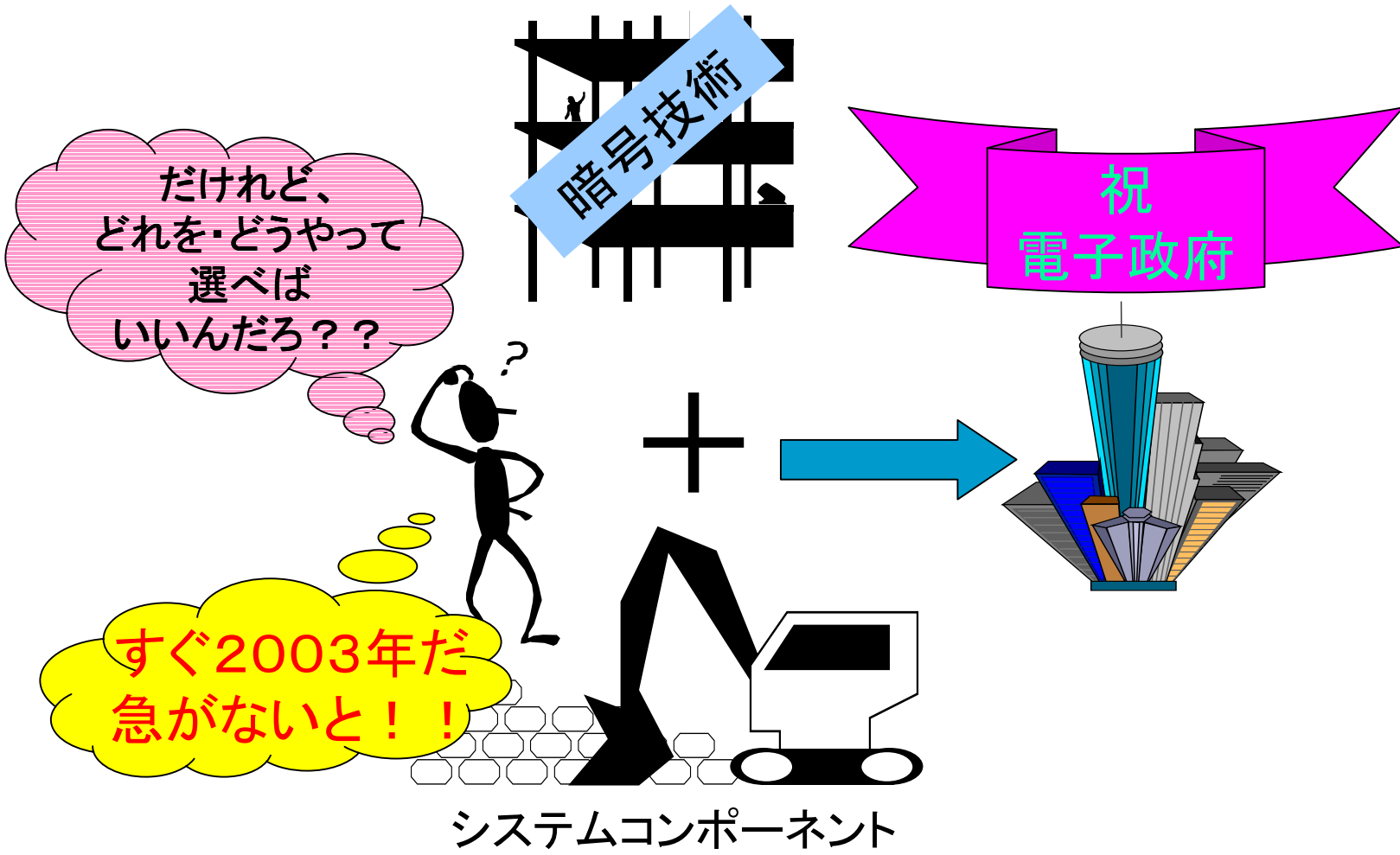
    データを所有し，管理し，アクセスし，使用し，又は蓄積する個人又は主体は，かかるデータの機密性と完全性を保護する責任を持つことがあり，またそれゆえに適切な暗号手法を使用する責任を有することがある。

    （堀部政男教授監訳）

プロジェクトへの要求

- 平成15年度（2003年度）電子政府の基盤の構築
  - 安全性・信頼性を高めること
  - 情報セキュリティ確保のため、電子政府で利用可能な暗号の安全性等についての評価が必要。
- 国際的な標準化との調和
  - ISO／IEC JTC1での標準暗号制定の動き
  - 米国次期標準暗号（AES）の選定
  - 欧州（NESSIE）で暗号標準化を開始

暗号技術評価委員会の背景



CRYPTRECの活動

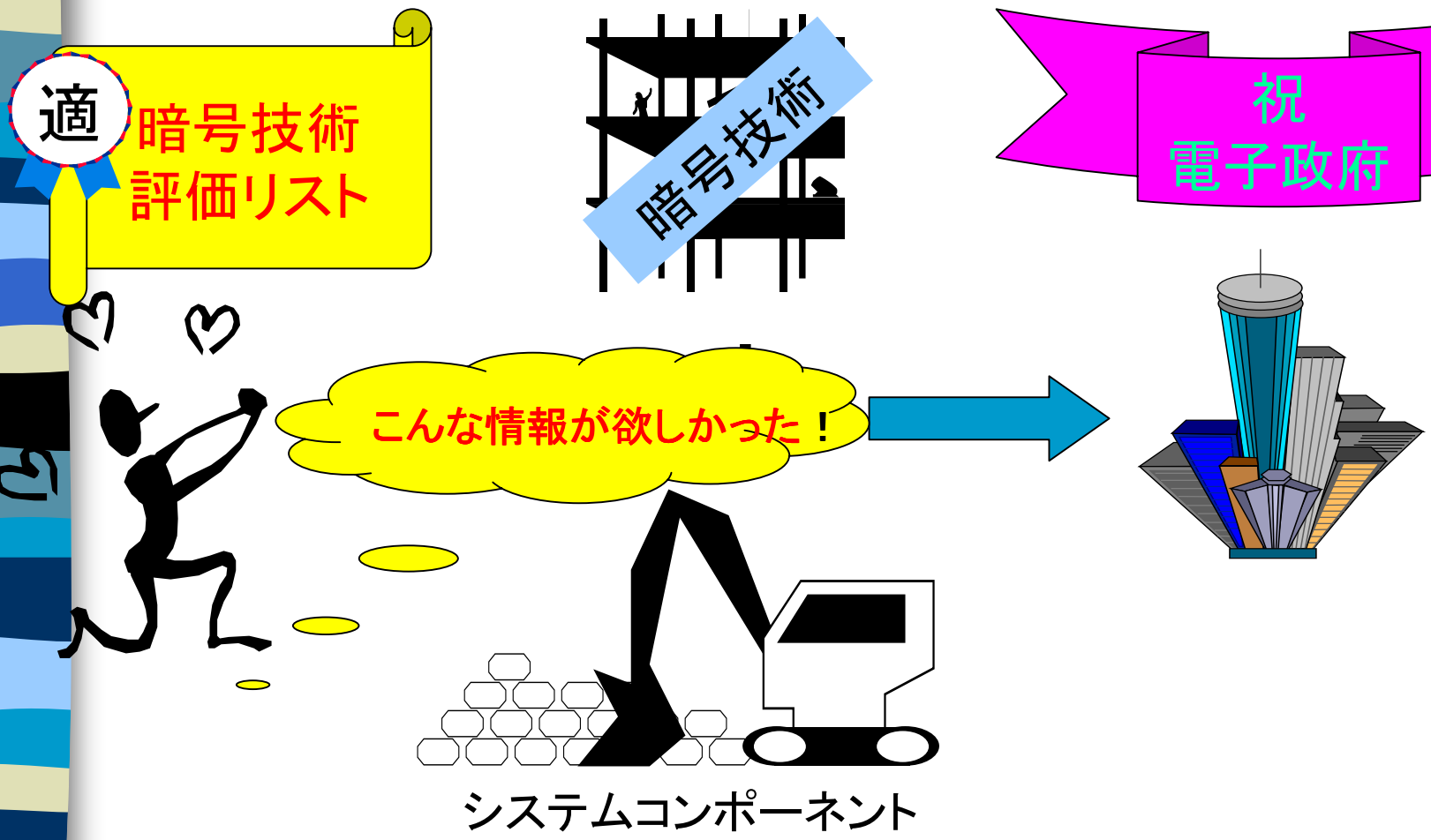
- 暗号技術評価委員会（Cryptography Research & Evaluation Committee）
  - 事務局：IPAセキュリティセンター
    http://www.ipa.go.jp/security/
- 暗号技術公募
- 電子政府に利用可能な暗号のリストアップ
  - 安全性
  - 実装性

CRYPTRECの目的

- 電子政府システムに適用可能な暗号技術を公募
- 応募のあった暗号技術を技術的・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

暗号技術評価委員会の目的

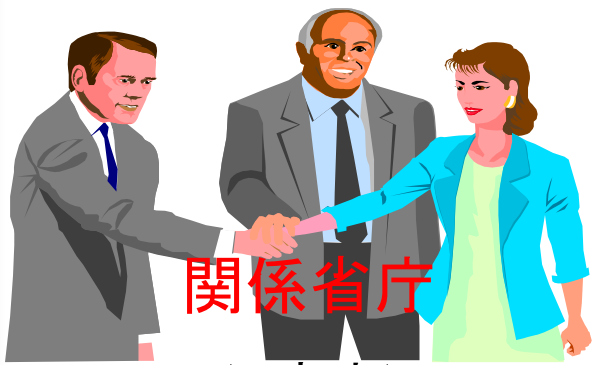


意　義

- 関係各省庁がオブザーバーで参画
  - 内閣官房
  - 警察庁
  - 防衛庁
  - 総務省
  - 法務省
  - 財務省
  - 経済産業省
- 第１線の研究者を糾合
- 安全性と実装性のバランス

暗号技術評価委員会の意義

暗号技術評価委員会



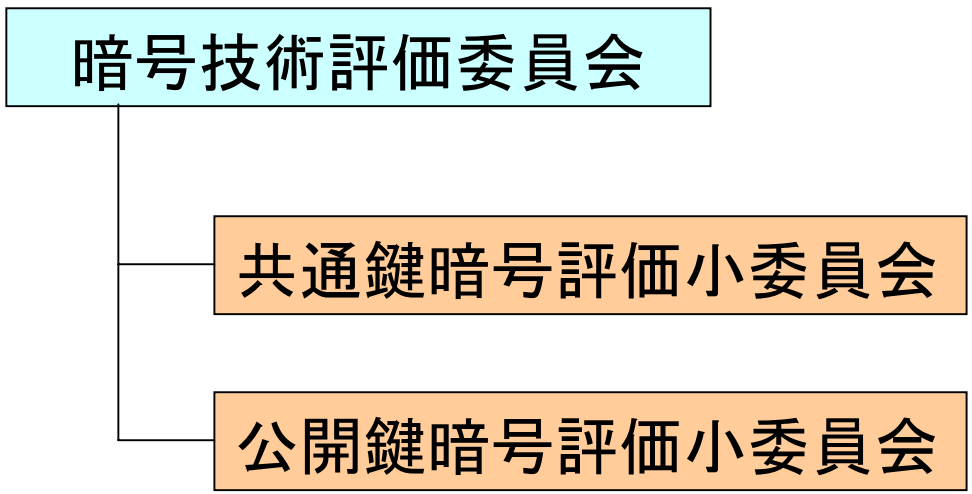
関係省庁

（7省庁）

第１線の研究者

体制

- CRYPTREC（暗号技術評価委員会）を組織し、評価を実施
  - 我が国の暗号技術開発を主導する有識者で構成



暗号技術評価委員会　委員

委員長	今井　秀樹	東京大学生産技術研究所
委員	岩下　直行	日本銀行金融研究所
委員	岡本　栄司	東邦大学理学部情報科学科
委員	岡本　龍明	日本電信電話株式会社情報流通ﾌﾟﾗｯﾄﾌｫｰﾑ研究所
所		
委員	金子　敏信	東京理科大学理工学部電気工学科
		（共通鍵暗号評価小委員会　委員長）
委員	櫻井　幸一	九州大学大学院システム情報科学研究院
委員	佐々木　良一	株式会社日立製作所システム開発研究所
顧問	辻井　重男	中央大学理工学部情報工学科
特別委員	苗村　憲司	慶應義塾大学大学院政策・メディア研究科
委員	松井　充	三菱電機株式会社情報技術総合研究所
委員	松本　勉	横浜国立大学工学部
		（公開鍵暗号評価小委員会　委員長）

共通鍵暗号小委員会　委員

委員長	金子	敏信	東京理科大学理工学部電気工学科
委員	荒木	純道	東京工業大学大学院理工学研究科
委員	香田	徹	九州大学大学院システム情報科学院
委員	川村	信一	株式会社東芝研究開発センター
委員	神田	雅透	日本電信電話株式会社情報流通ﾌﾟﾗｯﾄﾌｫｰﾑ研究所
委員	古原	和邦	東京大学生産技術研究所
委員	櫻井	幸一	九州大学大学院システム情報科学研究院
委員	下山	武司	株式会社富士通研究所ｺﾝﾋﾟｭｰﾀｼｽﾃﾑ研究所
委員	宝木	和夫	株式会社日立製作所システム開発研究所
委員	館林	誠	松下電器産業株式会社マルチメディア開発センター
委員	角尾	幸保	日本電気株式会社情報通信メディア研究本部
委員	時田	俊雄	三菱電機株式会社情報技術総合研究所
委員	森井	昌克	徳島大学工学部

公開鍵暗号評価小委員会　委員

委員長	松本	勉	横浜国立大学工学部
委員	有田	正剛	日本電気株式会社情報通信メディア研究本部
委員	小暮	淳	株式会社富士通研究所ｺﾝﾋﾟｭｰﾀｼｽﾃﾑ研究所
委員	酒井	康行	三菱電機株式会社情報技術総合研究所
委員	静谷	啓樹	東北大学情報処理教育センター
委員	新保	淳	株式会社東芝研究開発センター
委員	**高橋**	**昌史**	**株式会社日立製作所システム開発研究所**
委員	趙	晋輝	中央大学理工学部
委員	藤岡	淳	日本電信電話株式会社情報流通ﾌﾟﾗｯﾄﾌｫｰﾑ研究所
委員	松崎	なつめ	松下電器産業株式会社マルチメディア開発センター
委員	宮地	充子	北陸先端科学技術大学院大学情報科学研究科

スケジュール

- 評価・調査のスケジュール

	平成12年							平成13年			
	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月
公募	←	→									
スクリーニング評価			←	→							
詳細評価					←					→	
結果の公表											★

公募内容(要領)

- ２段階の評価
  - スクリーニング評価
  - 詳細評価
    - 技術情報の公開
    - 公開評価 (Call for Evaluation)
- 特徴(安全性、実装性等)を整理
  - 外部委託による評価
  - 学会等での評価等

公募暗号の種別

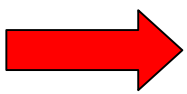
- 公開鍵暗号
  - 守秘，認証，署名，鍵共有
  - 暗号スキームと暗号プリミティブの組み合わせで募集
    - 暗号プリミティブ：因数分解問題や離散対数問題に基づく暗号の基本アルゴリズム
    - 暗号スキーム：暗号プリミティブやハッシュ関数のような補助関数を組み合わせてセキュリティ機能を達成するためのアルゴリズム
- 共通鍵暗号
  - ストリーム暗号，64ビット暗号，128ビット暗号
- ハッシュ関数
- 疑似乱数生成

公募結果（応募暗号）

- 公開鍵暗号　　24件
  - 守秘　7件、認証　1件、署名　10件、鍵共有　6件
- 共通鍵暗号　　19件
  - ストリーム暗号　6件、64ビット暗号　4件、128ビット暗号　9件
- ハッシュ関数　　0件
- 疑似乱数生成　　5件

スクリーニング評価

- 安全性重視の評価
  - 詳細評価を行うに値するかを判断
- 実装性評価
  - 情報（記述の有無、記述内容の論理的整合性/自己完結性）が整っていることの確認
  - 書面上で容易に判明するような欠点（解読手法など）の検査
  - 応募時点で提出された暗号技術仕様書、自己評価の内容の点検と正当性（内容の妥当性）の確認



詳細評価の候補の絞り込み

スクリーニング評価結果（詳細評価実施の暗号）

- 公開鍵暗号　　16件
  - 守秘　5件、認証　1件、署名　6件、鍵共有　4件
- 共通鍵暗号　　12件
  - ストリーム暗号　2件、64ビット暗号　4件、128ビット暗号　6件
- ハッシュ関数　　0件
- 疑似乱数生成　　1件

評価報告暗号技術(1)

- **公開鍵暗号(守秘)**
  - HIME-1(HITACHI)（←鍵共有）
  - HIME-2(HITACHI)
  - EPOC(NTT)（→ EPOC-1,2,3として評価）
  - PSEC(NTT)（→ PSEC-1,2,3として評価）
  - ECAES in SEC1(FUJITSU & Certicom)
  - ACE Encryption(IBM)
- **公開鍵暗号(認証)**
  - ESIGN-identification (NTT)（署名のESIGN-signatureと合併）

評価報告暗号技術(2)

- **公開鍵暗号(鍵共有)**
  - ECDHS in SEC1 (FUJITSU & Certicom)
  - ECMQVS in SEC1 (FUJITSU & Certicom)
  - HEF-ECDH(JAIST & MATSUSHITA)
- **公開鍵暗号(署名)**
  - MY-ELLTY ECMR-OEF-h(MATSUSHITA)
  - MY-ELLTY ECMR-192-h(MATSUSHITA)
  - MY-ELLTY ECMR-160-h(MATSUSHITA)

  - ESIGN-signature(NTT)
  - ECDSA in SEC1(FUJITSU & Certicom)
  - ACE Sign(IBM)

評価報告暗号技術(3)

- 共通鍵暗号（ストリーム暗号）
  - MULTI-S01(HITACHI)
  - TOYOCRYPTO-HS1(TOYOCOM）
- 共通鍵暗号（64ビット暗号）
  - CIPHERUNICORN-E(NEC)
  - MISTY1(MITSUBISHI)
  - FEAL-NX(NTT)
  - Hierocrypt-L1(TOSHIBA)

評価報告暗号技術(4)

- 共通鍵暗号（128ビット暗号）
  - CIPHERUNICORN-A(NEC)
  - Camellia(NTT & MISTUBISHI)
  - RC6(RSA Data Security)
  - SC2000(FUJITSU)
  - MARS(IBM)
  - Hierocrypt-3(TOSHIBA)
- 擬似乱数生成
  - TOYOCRYPTO-HR1(TOYOCOM）

リストに入れるべき他の重要な暗号技術

- リストにいれるべき暗号技術
  - 現在様々なシステムで使用されている
  - 電子政府システム構築上，不可欠と判断した方式
  - 公開鍵暗号
    - RSA-OAEP, RSA-PSS, DSA, DH Key Exchange （→計21件）
  - 共通鍵暗号
    - AES(Rijndael)
    - Triple-DES （→計14件）
  - ハッシュ関数
    - SHA-1, MD-5, RIPEMD-160 （→計3件）
  - 擬似乱数生成
    - RNG based on SHA1 （→計2件）（総計40件）

詳細評価対象とならなかった理由(1)

（1）公募された暗号技術のカテゴリーに該当しないもの．

- **暗号用技術としての仕様記述が十分でない又は提案された種目の暗号技術として分類できないもの**

（2）詳細評価を実施するために必要な資料・データが揃っていないもの．

- **安全性の自己評価が不十分であり，詳細評価の対象とし難いと判断したもの**

詳細評価対象とならなかった理由(2)

（3） 安全性・実装性などにおいて，明らかな問題点が指摘されているもの．

- **提案書の方法では想定外の数学的欠陥があり，安全性に疑問があるもの**
- **電子政府用暗号としては，速度性能が十分でないと判断したもの**

（4） その他

- **他カテゴリーで応募されている暗号と同一の技術であり，他カテゴリー側での評価結果が準用できると判断し，当該応募カテゴリーでの詳細評価は行わないこととしたもの**
- **書類不備又は自ら辞退したもの**

詳細評価(要領)

- 海外評価
  - 海外委託先:第一線の研究者
  - 研究者独自の視点で複数の方式を評価
- 国内評価
  - 共通の評価項目で複数の方式を評価
  - 候補暗号技術特有の評価(解読)
  - ハードウェアの実装性評価
- 公開評価
  - 学会での評価(期待)

詳細評価（ポイント）

- 安全性
  - 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）
- 実装性（ソフトウェア &ハードウェア)
  - **SW：共通プラットフォーム**
    - **処理速度、リソース使用量等**
  - **HW：共通プラットフォーム**
    - **ゲート規模、処理速度**

詳細評価の基準（1）

- 公開鍵暗号の安全性評価
  - スキームとプリミティブの組み合わせで評価
  - スキームの評価
    - **攻撃（受動的攻撃、能動的攻撃、等）**
    - **機能（守秘、認証、署名、鍵共有）への影響**
  - **プリミティブの評価**
    - **既知の攻撃法に対する計算量的耐性**

詳細評価の基準(2)

- ストリーム暗号の安全性評価
  - **周期、線形複雑度、相互情報量**
  - **統計的性質(1/0等頻度性、連、一様性)**
  - ヒューリスティックな解読攻撃
- ブロック暗号の安全性評価
  - **汎用的な攻撃法（線形攻撃法、差分攻撃法など）**
  - **代数次数、耐高階差分攻撃**
  - **アバランシュ性評価**
- 疑似乱数生成の安全性評価
  - **統計量的な性質の評価と乱数性（例えば、FIPS140-1）**

詳細評価の基準(3)

- 実装性評価
  - 第三者実装ができるか？
    - 暗号技術仕様書だけで、実装できるか？
    - 応募者しか知らない情報がないか？
- 設計基準
  - パラメータ／鍵の設定基準が明確化？

詳細委評価依頼先機関数

	海外	国内
公開鍵暗号技術	5	9
共通鍵暗号技術	3	11

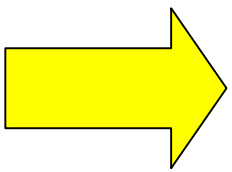
詳細評価の結果（概要）
～公開鍵暗号技術～

- 安全性
  - いずれの方式も、パラメータの設定に関しては、注意を払う必要がある。

特段の問題が指摘されていない方式	10
仕様が変更されている方式	2
応募者の主張と評価者の報告に差異があり、更なる検討と評価が必要な方式	10
長期間有効性を保つことが求められる署名方式としては推奨できない方式	1

詳細評価の結果（概要）
～公開鍵暗号技術～

- 実装性
  - いずれの方式も、概ね許容できる処理性能を有していることを確認出来た。
  - 実装のために仕様の追加があった方式も存在



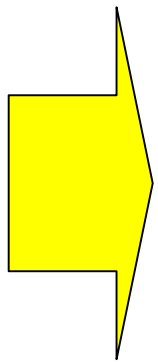
詳細な報告は小委員長から

詳細評価の結果（概要）
～共通鍵暗号技術（ブロック暗号）～

- 安全性

64ビットブロック暗号	
問題点の指摘がなかった方式	3
更なる評価と検討が必要な方式	1
長期間の使用は薦めない方式	1

128ビットブロック暗号	
問題点の指摘がなかった方式	5
更なる検討と評価が必要な方式	2



詳細な報告は小委員長から

詳細評価の結果（概要）
～共通鍵暗号技術（ブロック暗号）～

- 実装性
  - SWによる実装性
    - Triple-DESとの相対比較
    - Pentium　III上での例

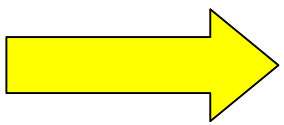
64ビットブロック暗号	
速い	3
同程度	2

128ﾋﾞｯﾄﾌﾞﾛｯｸ暗号	
速い	5
同程度	1
評価しなかった	1

  - HWによる実装性
    - 64bitブロック暗号3種、128bitブロック暗号4種を評価
    - 実装上の問題点の指摘はない

詳細評価の結果（概要）
～共通鍵暗号技術（ストリーム暗号）～

- 安全性
  - 問題点の指摘がなかった方式　1
  - 「改良が必要」との指摘のあった方式　1
- 実装性
  - SW実装で速い　1
  - HW実装向き　1



詳細な報告は小委員長から

まとめと将来への課題（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
  - 継続的な評価／改良の必要性を指摘
    - 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

まとめと将来への課題(2)

- 暗号技術評価の継続
  - 組織・体制づくりの整備が必要
  - 継続的な評価の必要がある
- 公募の継続
  - 当面2003年の電子政府が目標
  - 募集期間・評価期間とも短かすぎる
    - 埋もれた暗号の発掘や改良方式の評価が必要
- 成果の活用
  - 実装環境の整備

まとめと将来への課題（3）
～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
  - 米国次期標準暗号（AES）
  - 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

謝辞

- IPA「政府調達情報セキュリティ標準に関する調査研究」，郵政省「暗号通信の普及・高度化に関する研究会」
- 委員，小委員会委員長・委員（提案者も含まれていたが，利害を超え，公正な観点からご協力頂いた．）
- 事務局（IPAセキュリティセンター，暗号技術調査室）
- オブザーバー
- 評価委託先
- ボランティアとして評価頂いた方々
- 提案者