CRYPTREC活動報告

ー２００１年度報告ー

2002年4月16日

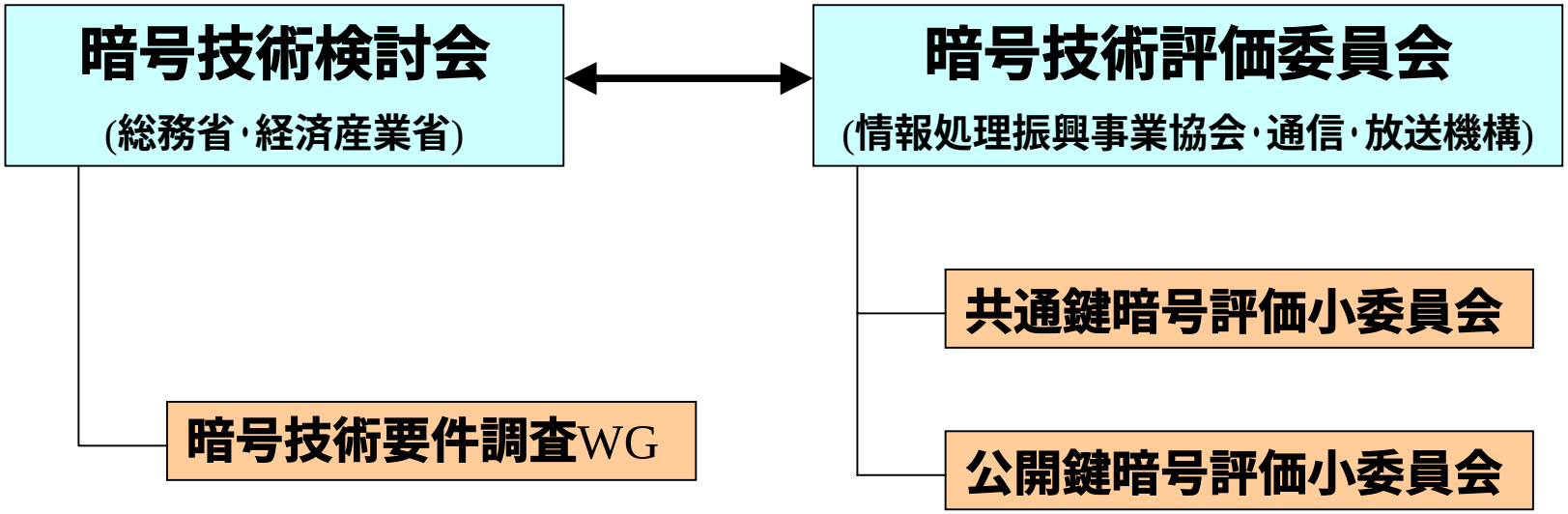
暗号技術検討会座長
暗号技術評価委員会委員長
今井秀樹(東京大学)

CRYPTREC活動の主旨

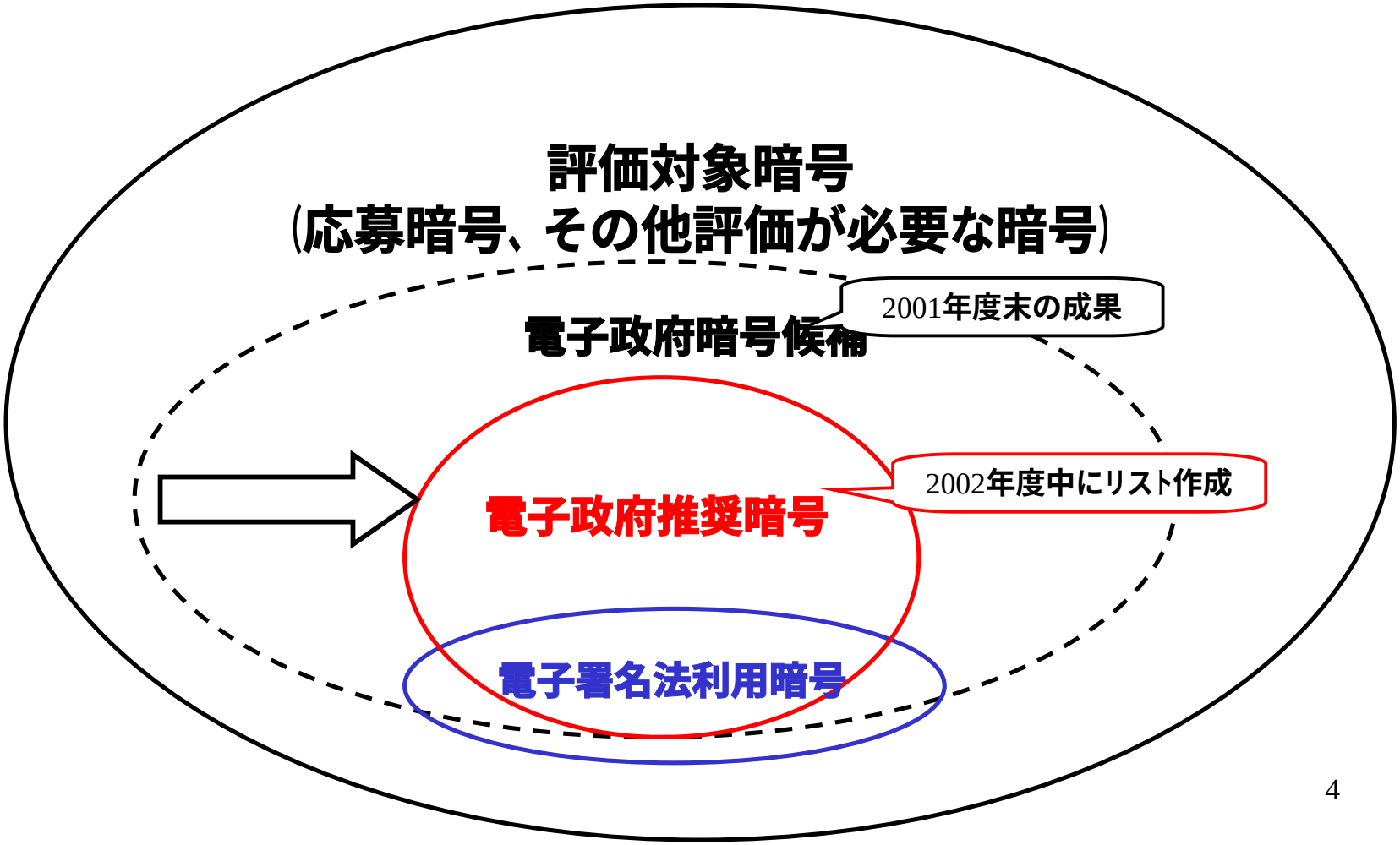
- 国内暗号技術評価体制確立に向けた活動
- 電子政府に利用可能かの観点で暗号技術評価を実施
- 標準化活動支援

活動の公平性･透明性
(評価活動内容はWEBにて公開)

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

暗号技術評価活動


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年度中にリスト作成
電子署名法利用暗号

原理的に安全な暗号の例

- 守秘
  - バーナム暗号 (ワンタイムパッド暗号) : ただし, 非展性 (Non-Malleability)は満たさない.
  - Ding-Rabin暗号 : メモリ制約が必要
  - SHZI暗号 (四方・花岡・鄭・今井) ＊
- 鍵共有
  - 量子暗号 : 認証は必要
  - 情報量的に安全なKPS (松本・今井) ＊
- 署名
  - HSZI署名 (花岡・四方・鄭・今井) ＊

＊大きなメモリと信頼できるイニシャライザー (TI)が必要

GOALS OF NESSIE

- put forward a portfolio of strong cryptographic primitives that have been obtained based on an OPEN call and an OPEN evaluation process
- deliver input to AES
- develop evaluation methodology and software toolbox
- consensus building and dissemination
- strengthen European research and industry

- recommend algorithms
- collaborate with industry and standardization bodies on evaluation

- NOT for government use
- NESSIE is NOT a standardization body

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)

暗号技術検討会
(政策的検討が中心)

暗号技術検討会　座長　今井秀樹

2001年5月に設置　7回開催

－電子政府推奨暗号に関する検討

－今後の暗号評価のあり方を検討

暗号技術検討会2001年度報告書

要件調査WG　リーダ　佐々木良一

2001年6月に設置　12回開催

－電子政府暗号技術の要件を調査検討

要件調査ワーキンググループ報告書

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

暗号技術要件調査
ワーキンググループ

ﾘｰﾀﾞｰ	佐々木良一	東京電機大学
	岩下　直行	日本銀行金融研究所
	岡本　栄司	筑波大学
	川村　信一	株式会社東芝
	洲崎　誠一	株式会社日立製作所
	館林　誠	松下電器産業株式会社
	米倉　昭利	(財)日本品質保証機構
	渡辺　創	独立行政法人産業技術総合研究所

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
- 独立行政法人通信総合研究所
- 独立行政法人産業技術総合研究所
- 情報処理振興事業協会
- (財)日本品質保証機構
- (財)金融情報システムセンター

CRYPTREC：暗号技術検討会
～活動内容～

1　電子政府推奨暗号リストの策定

電子申請システム等の電子政府システムで利用される暗号アルゴリズムに関する推奨暗号リストを作成し、安全性及び信頼性の高いシステム構築に貢献。そのために昨年度に引き続き、継続評価及び新規評価を行うとともに、電子政府に求められる暗号要件に関する調査をWG（ﾘｰﾀﾞ：佐々木電機大教授）において実施。

2　電子署名法に基づいて利用される暗号に関する助言

①　電子署名法第2条第3項の電子署名基準（暗号に関するもの）への反映、及び見直し。

②　電子署名法第３３条に基づく暗号技術の評価に関する調査研究。

3　暗号技術に関する国際標準化への対応

ISO、ITU等の場における暗号の国際標準化に関する活動について支援を行う。

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**

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**

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

2000年5月に設置　2001年度11回開催

公開鍵暗号評価小委員会　委員長 松本勉

2000年5月に設置　2001年度17回開催

共通鍵暗号評価小委員会　委員長 金子敏信

2000年5月に設置　2001年度16回開催

－暗号技術分類毎の評価方法検討

－応募暗号技術・その評価が必要な暗号技術の評価実施

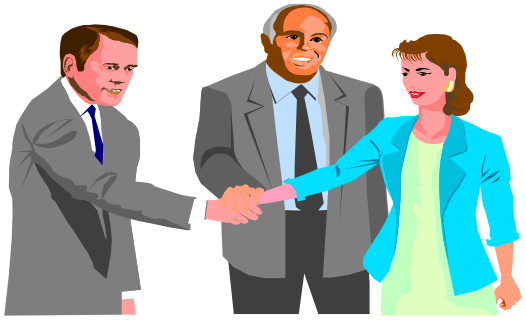
暗号技術評価報告書 (2001年度版)

暗号技術活用ガイドライン(ドラフト版)

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

暗号技術検討会ー暗号技術評価委員会



関係省庁

暗号ユーザ

第1線の研究者

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

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

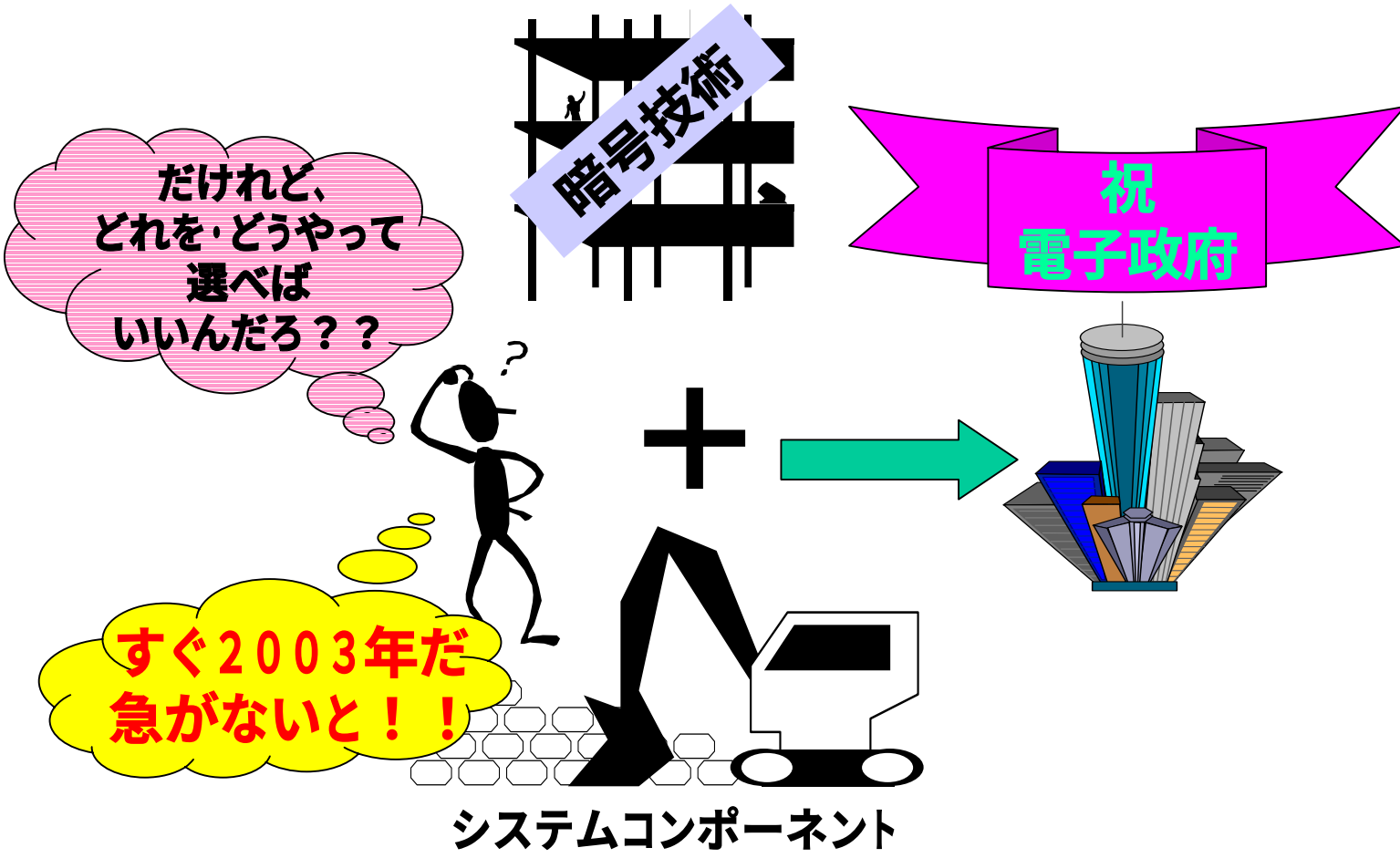
共通鍵暗号技術評価小委員会

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	川村 信一	株式会社東芝
委員	神田 雅透	日本電信電話株式会社
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

- 警察庁
- 防衛庁
- 総務省
- 経済産業省
- 独立行政法人通信総合研究所

暗号技術評価委員会の背景

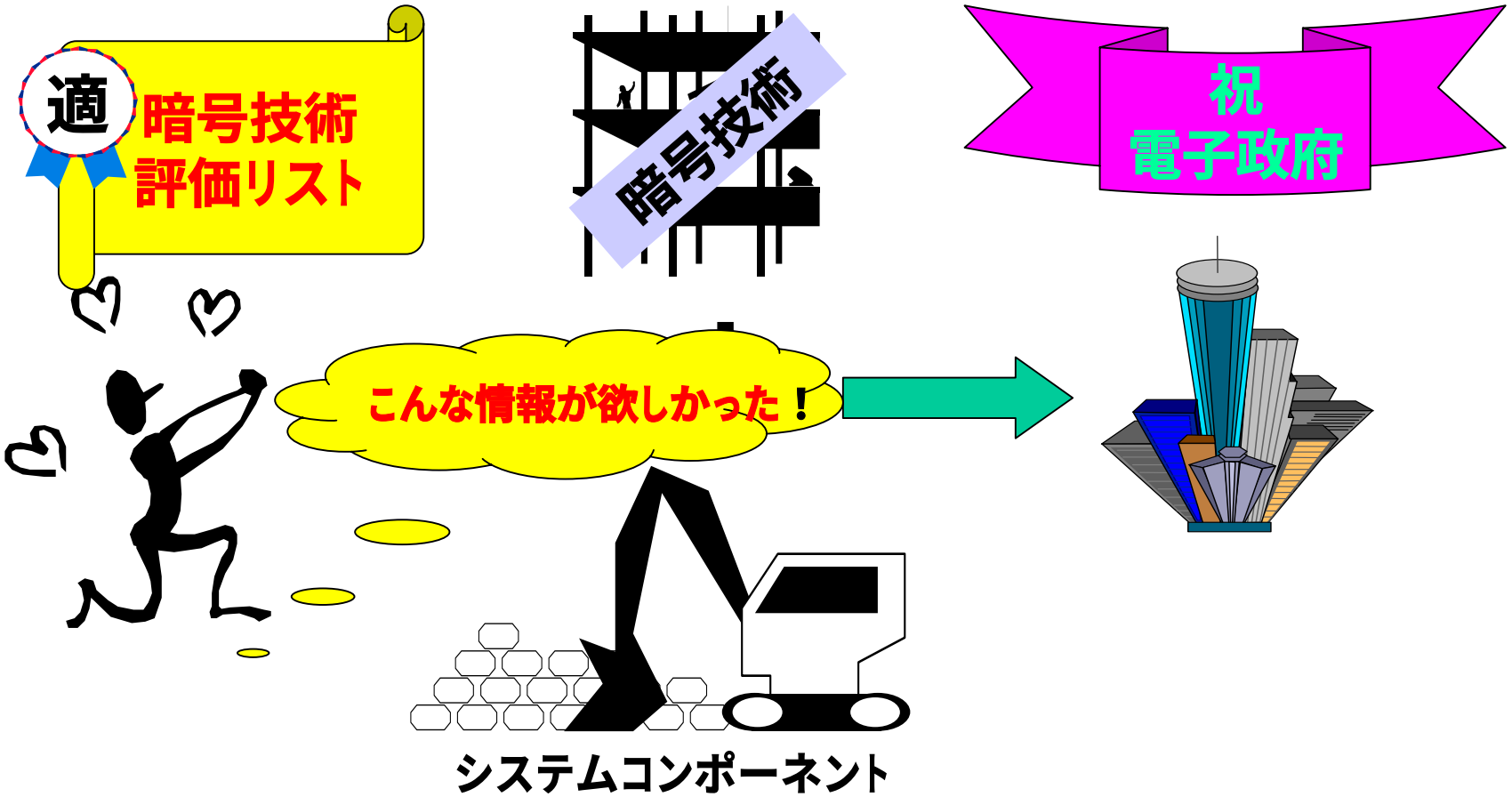


暗号技術評価委員会の目的

- 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

暗号技術評価委員会の目的



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

公開鍵暗号技術
(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

共通鍵暗号技術

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

2001年度評価対象暗号技術

公開鍵暗号技術　　１７件（１４件）[33(29)]

（守秘：５件[10(10)]、認証：０件[0(0)]、署名：７件[15(12)]、
鍵共有：５件[8(7)]）

共通鍵暗号技術　　１７件（１２件）[28(22)]

（ストリーム暗号：５件[10(9)]、６４ビット暗号：５件[6(4)]、
１２８ビット暗号：７件[12(9)]）

ハッシュ関数　　３件（　０件）[4(0)]

疑似乱数生成系　　５件（　４件）[10(9)]

その他　　２件（　２件）[2(2)]

（　）内は応募暗号，[　]内は2000，2001年度計

暗号技術評価

国内外の専門家よる外部委託評価
技術情報の公開(ワークショップやCall for comment)
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

2002年度評価予定の暗号
(詳細評価実施の暗号)

監視状態の暗号	公開鍵暗号技術	守秘	1(10)
		署名	5(15)
		鍵共有	2(8)
	共通鍵暗号技術	64bitブロック暗号	4(6)
		128bitブロック暗号	7(12)
		ストリーム暗号	1(10)
	ハッシュ関数		3(4)
	擬似乱数生成系		1(10)
計			24(77)
詳細評価対象候補	公開鍵暗号技術	守秘	2
		署名	1
		鍵共有	1
	共通鍵暗号技術 (ストリーム暗号)		2
計			6

() 内は評価対象暗号数

監視状態の暗号技術(1)

詳細評価の結果安全性など技術的観点から、特に問題がないと判断された暗号技術

- 公開鍵暗号技術(守秘)
  - RSA-OAEP
- 公開鍵暗号技術(署名)
  - DSA
  - ECDSA in SEC1
  - ECDSA(ANSI X9.62)
  - RSA-PKCS#1v1.5
  - RSA-PSS
- 公開鍵暗号技術(鍵共有)
  - DH
  - ECDH in SEC1

監視状態の暗号技術(2)

- 共通鍵暗号技術 (64bitブロック暗号)
  - CIPHERUNICORN-E
  - Hierocrypt-L1
  - MISTY1
  - Triple-DES
- 共通鍵暗号技術 (128bitブロック暗号)
  - AES (FIPS 197)
  - Camellia
  - CIPHERUNICORN-A
  - Hierocrypt-3
  - RC6 Block Cipher
  - SC2000
  - SEED

監視状態の暗号技術(3)

- 共通鍵暗号技術（ストリーム暗号）
  - MULTI-S01
- ハッシュ関数
  - RIPEMD-160
  - SHA-1
  - Draft SHA-256/-384/-512
- 擬似乱数生成系
  - PRNG based on SHA-1

詳細評価対象暗号技術候補

- 公開鍵暗号技術 (守秘)
  - ECIES in SEC1
  - HIME(R)
- 公開鍵暗号技術 (署名)
  - ESIGN
- 公開鍵暗号技術 (鍵共有)
  - PSEC-KEM
- 共通鍵暗号技術 (ストリーム暗号)
  - MUGI
  - RC4

SSL/TLSプロトコル調査結果

■SSL3.0を利用するにあたっては、既知のセキュリティホールを十分認識した上での設定（SSL2.0の利用を不可とする、等）を行うべき。

■市販のSSLソフトを利用する場合、セキュリティホールにパッチの当てられた最新版を用いるべき。

■Internet Explorer及びNetscape Navigatorでは公開鍵証明無効化リスト（CRL）を不正に消去した上で不正な証明書を用いて認証を欺くという攻撃がありうる。よって、証明書を格納するファイルは厳密なアクセス管理を行うべき。

■匿名認証モードの利用は推奨しない。（情報の盗聴、改ざんを受ける可能性）

■version rollback攻撃を防ぐため、特に理由がない限りSSL/TLSの最新版のみを使用するよう設定運用すべき。

■SSL3.0では、利用する暗号方式について変更出来ない。一方、TLS1.0は新しい暗号方式を追加することが可能であるため、既存の暗号技術に問題があった場合でも対応可能。

■TLSは機能追加を目的として拡張作業が行われているが、これらの拡張に伴って新たなセキュリティホールが発生する可能性もあるため、今後とも、TLSの動向に注目し、その安全性について継続的な調査、検討が必要。

SSL/TLSで利用される暗号技術評価

■鍵長40bitのDES及びRC2は、鍵総当りにより現実的な時間で解読可能

→ 安全性が必要なシステムにおいては、用いられるべきでない。

■鍵長56bitのDESは、もはや現実的に解読可能な領域に達しつつある

→ 高い安全性が必要なシステムにおいては、用いられるべきでない。

■鍵長168bitのTDESは、当面の間の使用には特に問題ない。しかし、TDESに替わる更に安全な暗号がSSLに採用されれば、それに置き替える方が望ましい。

■鍵長128bitのRC2は、鍵総当りよりも効率の良い解読方法が存在

→ 新規に構築するシステムにおいては、採用することを勧めない。

■64bitブロック暗号であるRC2, DES, TDESは、2^{32}ブロック以上を同じセッション鍵で暗号化すると、平文1bitの情報が漏れる恐れ

→ セッション鍵の更新に注意すべき

■鍵長512bitのRSAは、現実的に素因数分解可能であり、安全でない。
2001年度時点では、1024bit以上の鍵長を用いれば安全であると考えられる。

※ RC4は現在評価中であり、2002年度中に評価報告予定

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
    - 今後開発される技術の評価
  - 継続的な評価の必要がある
    - 2002年度の検討課題
- 成果の活用
  - 実装環境の整備
  - 実装された暗号製品の評価体制の検討

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
  - 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

CRYPTREC Report 2001

第1 章 暗号技術評価の概要
第2 章 公開鍵暗号技術の評価
第3 章 共通鍵暗号技術の評価
第4 章 ハッシュ関数の評価
第5 章 擬似乱数生成系の評価
第6 章 SSL プロトコルに関する暗号技術
第7 章 2002 年度評価予定暗号の問い合わせ先一覧
第8 章 評価暗号一覧
応募暗号技術仕様(CD-ROM)

暗号技術活用ガイドライン

CRYPTREC Report 2001を読む際に
必要と思われる暗号技術関連情報を整理

2001年度ドラフト版作成

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

E-mail:cryptrec-call@ipa.go.jp