暗号技術検討会の活動概要

－２００１年度の活動報告と２００２年度の活動内容－

2002年4月16日

暗号技術検討会事務局

検討会報告書目次

1．はじめに
2．検討会開催の背景、構成員及び開催状況
3．暗号技術に関する現状
4．電子政府推奨暗号の策定
5．暗号技術評価結果について
6．要件調査WGにおける検討結果
7．今後の検討課題
8．暗号プロトコル評価、及び暗号モジュール評価の重要性
9．次年度以降の評価を含む活動指針

【資料】
- 要件WG活動報告
- 評価委員会報告書

検討会開催の背景

- 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社会推進戦略本部決定）においては、我が国の高度情報通信ネットワークの安全性及び信頼性を世界最先端のＩＴ国家にふさわしいものにするため、高度情報通信ネットワークにおける脅威に起因するサービス提供機能の停止が最小限となるように、政府は各種の施策を実施することとしている。

- 特に、電子署名等の電子認証の普及、電子政府の構築等に向けて、高度情報通信ネットワークの安全性及び信頼性を確保するためには、基盤技術である暗号技術について、客観的な評価や標準化が重要になっていく。

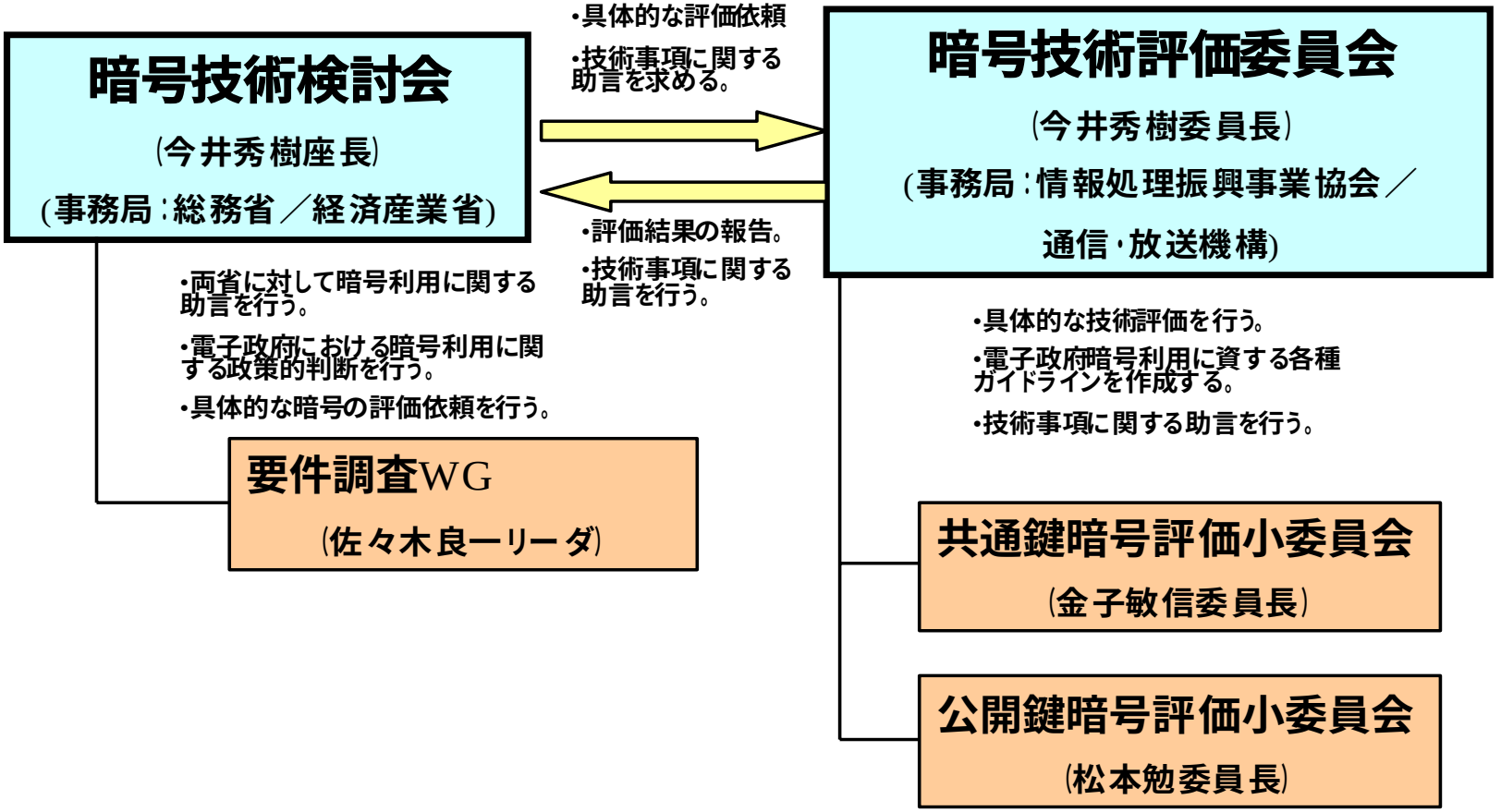
- このため、総務省及び経済産業省は、暗号技術を公募の上客観的に評価し、実装性に優れた利用可能性の高い暗号技術を各省に推薦し、高度な信頼性及び安全性に支えられた電子政府の構築に貢献することを目指すこととした。

検討体制

- 2001年度は、下記の体制で検討・評価を進めた。
  - 暗号技術検討会：総務省及び経済産業省を事務局に、政策的な検討を行う。検討会の下に要件調査ＷＧを設置し、電子政府で求められる暗号技術の要件を調査した。
  - 暗号技術評価委員会：情報処理振興事業協会及び通信・放送機構を事務局に、技術的な評価を行う。

- なお、CRYPTRECとは、従来（2000年度）は、暗号技術評価委員会（Cryptography Research & Evaluation Committee）のことを指していたが、2001年度より、総務省及び経済省の両担当局長の主催により、暗号技術検討会が開催されたこと、及びCRYPTRECという名称が既に日本における暗号技術の評価プロジェクトとして広く国内外において認知されていることから、今後は、暗号技術検討会及び暗号技術評価委員会の両者を含めた形でプロジェクト名としてCRYPTRECを使用することとする。なお、CRYPTREC は 、 Cryptography Research & Evaluation Committeesの略称とする。

CRYPTREC体制


暗号技術検討会
(今井秀樹座長)
(事務局：総務省／経済産業省)
・具体的な評価依頼
・技術事項に関する助言を求める。
・評価結果の報告。
・技術事項に関する助言を行う。
暗号技術評価委員会
(今井秀樹委員長)
(事務局：情報処理振興事業協会／通信・放送機構)
・両省に対して暗号利用に関する助言を行う。
・電子政府における暗号利用に関する政策的判断を行う。
・具体的な暗号の評価依頼を行う。
・具体的な技術評価を行う。
・電子政府暗号利用に資する各種ガイドラインを作成する。
・技術事項に関する助言を行う。
要件調査WG
(佐々木良一リーダ)
共通鍵暗号評価小委員会
(金子敏信委員長)
公開鍵暗号評価小委員会
(松本勉委員長)

検討会メンバー

座長	今井　秀樹	東京大学生産技術研究所教授
顧問	辻井　重男	中央大学理工学部情報工学科教授
WGﾘｰﾀﾞ	佐々木良一	東京電機大学工学部情報通信工学科教授
	生宗　潤	(社)情報サービス産業協会セキュリティ委員会委員
	岩下　直行	日本銀行金融研究所研究第２課調査役
	岡崎　宏	通信機械工業会常務理事
	岡本　栄司	東邦大学理学部情報科学科教授
	岡本　龍明	日本電信電話株式会社情報流通プラットフォーム研究所主席研究員（電気通信事業者協会代表兼務）
	加藤　義文	(社)テレコムサービス協会技術委員会委員長
	金子　敏信	東京理科大学理工学部電気工学科教授
	国分　明男	ニューメディア開発協会常務理事開発本部長
	櫻井　幸一	九州大学大学院システム情報科学研究科助教授
	宝木　和夫	(社)電子情報技術産業協会情報セキュリティ委員会委員
	苗村　憲司	慶應義塾大学環境情報学部教授
	松井　充	三菱電機株式会社情報技術総合研究所情報セキュリティ技術部チームリーダー
	松本　勉	横浜国立大学大学院環境情報研究院教授

オブザーバー

須永　和男	内閣官房情報セキュリティ対策推進室内閣参事官（～第５回）
吉原　順二	内閣官房情報セキュリティ対策推進室内閣参事官（第６回～）
松田　正一	警察庁情報通信局技術対策課長
中島　明彦	防衛庁運用局指揮通信課長（～第２回）
中村　範明	防衛庁運用局指揮通信課長（第３回～）
高森　國臣	総務省行政管理局管理官
太田　健治	法務省民事局総務課民事調査官
粗　　信仁	外務省大臣官房情報通信課長（～第５回）
石川　正紀	外務省大臣官房情報通信課長（第６回～）
中田　悟	財務省大臣官房審議官室長（～第３回）
中山　峰孝	財務省大臣官房審議官室長（第４回～）
木戸　達雄	経済産業省産業技術環境局標準課情報電気標準化推進室長
福地　　一	独立行政法人通信総合研究所 情報通信部門長
大蒔　和仁	独立行政法人産業技術総合研究所 情報処理研究部門長
鈴木　　薫	通信・放送機構研究企画管理部長
小林　正彦	情報処理振興事業協会セキュリティセンター所長（～第２回）
内藤　　理	情報処理振興事業協会セキュリティセンター所長（第３回～）
米倉　昭利	(財)日本品質保証機構電子署名・認証調査センター所長
小倉　久宜	(財)金融情報システムセンター監査安全部長

要件調査WGメンバー

ﾘｰﾀﾞ	佐々木良一	東京電機大学工学部情報通信工学科教授
	岩下　直行	日本銀行金融研究所研究第２課調査役
	岡本　栄司	東邦大学理学部情報科学科教授
	川村　信一	株式会社東芝研究開発センター　コンピュータ・ネットワークラボラトリー主任研究員
	洲崎　誠一	株式会社日立製作所システム開発研究所第７部Ｈ０１研究ユニット　研究員
	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メディア情報グループチームリーダ
	米倉　昭利	(財)日本品質保証機構電子署名・認証調査センター所長
	渡辺　創	独立行政法人産業技術総合研究所　情報処理部門

開催状況

第一回　2001年５月１６日（水）：「開催要綱案、実施計画案」等

第二回　６月２２日（金）：「電子政府での暗号技術の要件整理調査」等

第三回　７月２７日（金）：「2001年度暗号技術公募要領」等

第四回　１０月３日（水）：「電子政府で利用する暗号」等

第五回　2002年１月１８日（金）：「電子政府推奨暗号リストの作成」等

第六回　２月２２日（金）：「要件調査ＷＧの検討状況」

第七回　３月１１日（月）：「2001年度報告書　最終案」

電子政府推奨暗号の策定

１．e-Japan重点計画における標準化の位置づけ

2001年３月２９日にＩＴ戦略本部で決定されたe-Japan重点計画において、暗号技術の標準化の推進が決定された。

２．セキュリティ・アクションプランにおける標準化の位置づけ

2001年１０月１０日に、情報セキュリティ対策推進会議において決定された「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」において今後のプロセスが決定。

電子政府推奨暗号の意味

①想定システム：電子申請システムや、電子入札システム等、政府と国民との間で書類の申請等についてやりとりを行う必要があるシステムを想定する。（国防関係の特別なシステムや、政府間限りのやりとりを行うシステムについてはこの対象としない。）なお、地方公共団体についﾄは、普及・広報等を通じて本利用方針の活用を奨励していく。

②耐用期間：１０年間は解読されない暗号を想定する。（ただし、署名の検証においては、１０年過ぎた後でも検証を行う必要性がでる可能性があるのでこの限りではない。）

③合意範囲（拘束度合い）：「可能な限り利用する。」との表現を用い、推奨のレベルとする。最終的な調達の判断は各省の責任で行う。

④特許・知的財産権の扱い：リストのあり方によるが、複数リストの場合には特許・知的財産権の無償化を義務づけることは考えないが、１つに絞った場合にはその無償化を検討する必要がある。

作業スケジュール

１．2001年度末

検討会において、要件調査ＷＧを中心に、電子政府において用いられている、または将来用いられるであろう暗号技術に求められる要件について調査し、結果をまとめた。また、評価委員会において、技術的な観点から、電子政府推奨暗号として利用することが可能である電子政府暗号候補（技術的な観点から安全性及び実装性について評価委員会において特に問題がないと判断された暗号）を策定した。

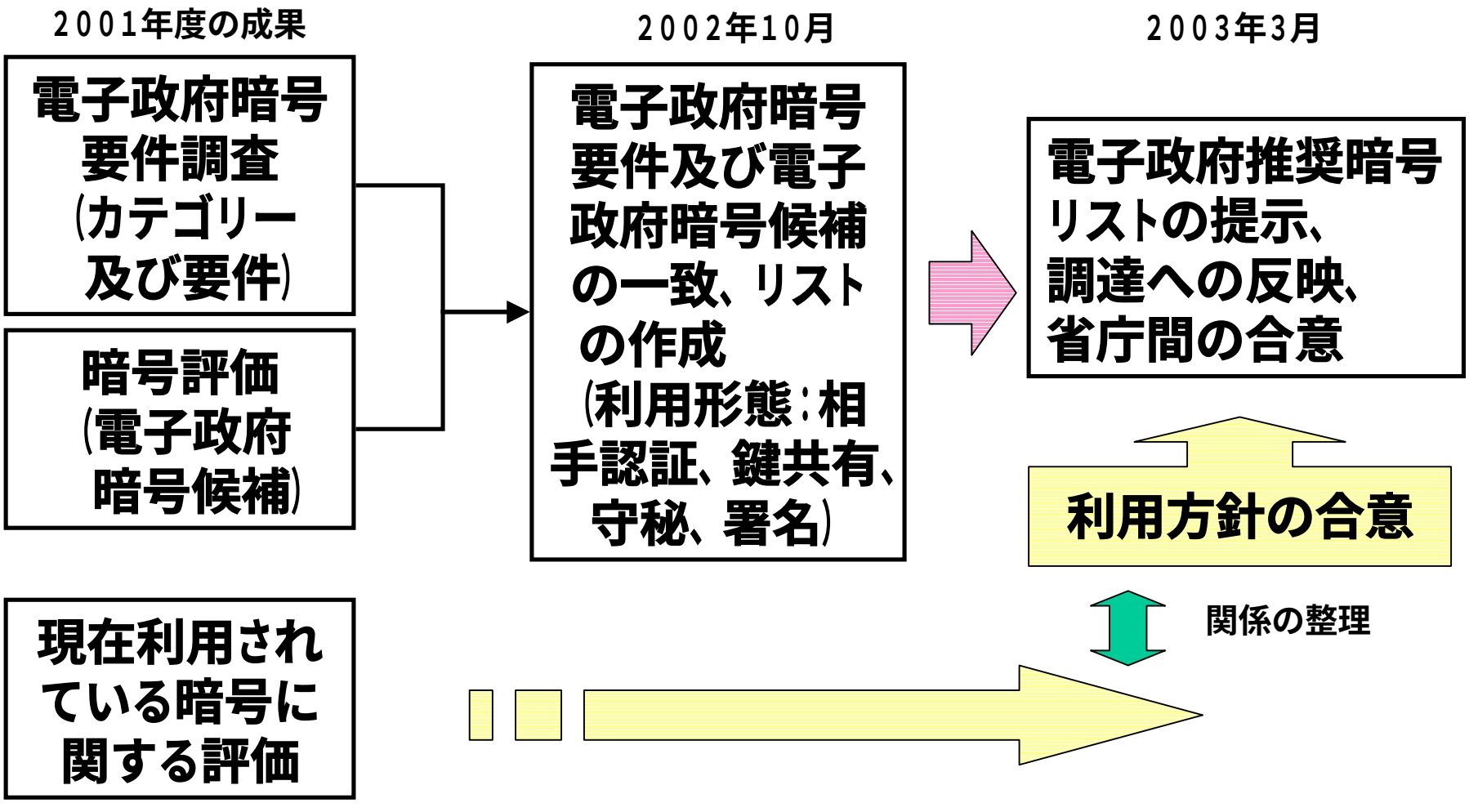
２．2002年１０月

要件調査の結果まとめられた要件に基づき、電子政府暗号候補から、電子政府推奨暗号リスト案を作成する。あわせて、調達のためのガイドブック案を作成する。

３．2002年度末

リスト案に基づき、総務省及び経済産業省において利用方針案を作成し、各省庁において、利用方針の合意を目指す。併せて調達のためのガイドブックを総務省及び経済産業省より各省庁へ提示する。

今後のスケジュール


2001年度の成果
2002年10月
2003年3月
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
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)
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

電子政府暗号候補

① 公開鍵暗号技術

【守秘】

RSA-OAEP

【署名】

DSA、ECDSA　(ANSI X9.62)、ECDSA in SEC1、RSA-PKCS#1 v1.5、RSA-PSS

【鍵共有】

DH、ECDH in SEC1

② 共通鍵暗号技術

【64ビットブロック暗号】

CIPHERUNICORN-E、Hierocrypt-L1、MISTY1、Triple DES

【128ビットブロック暗号】

Advanced Encryption Standard、Camellia、CIPHERUNICORN-A、
Hierocrypt-3、RC6 Block Cipher、SC2000

【ストリーム暗号】

MULTI-S01

③ ハッシュ関数

RIPEMD-160、SHA-1、draft SHA-256、draft SHA-384、draft SHA-512

④ 擬似乱数生成系

PRNG based on SHA-1

２００２年度詳細評価対象暗号候補

① 公開鍵暗号技術

【守秘】

ECIES in SEC1

HIME(R)

【署名】

ESIGN

【鍵共有】

PSEC-KEM

②共通鍵暗号技術

【ストリーム暗号】

MUGI

RC4

電子署名法の指針の改正に関する検討

ESIGN

指針に記載されたパラメータの一部に署名の偽造が可能なものが含まれているので、電子署名法に係る指針の改訂を検討すべきである。

RSA

RSA-PKCS#1 v1.5については、証明可能安全性は示されていないが、2001年時点で特に安全性の問題は存在しない。しかし、RSA-PSSを電子署名法に係る指針に新たに追加し、将来的にはRSA-PSSに一本化することを含めた議論をしていく必要がある。

MD5

MD5については、2000年度の評価結果として「MD５は128ビットのハッシュ値であり、．．．最近の研究では少なくとも160ビット以上必要であると考えられている。」との報告がなされており、指針から外すことを検討する必要がある。

今後の検討課題

(1) 推奨暗号数

① 単独暗号

② 複数暗号 (2～3個)

③ 複数暗号 (数は限定せず、安全性等の観点から一定の条件をクリアした暗号をリストアップする。)

(2) 相互接続性の問題

(3) 製品との関係

(4) 推奨暗号と暗号プロトコルとの関係

(5) 暗号プロトコル評価、及び暗号モジュール評価の必要性

(6) 標準化に関する考え方

リスト案の内容

① 分類
- 利用形態（電子署名、通信、データ保存等）
- 製品（ＩＣカード等）
- 暗号方式（公開鍵、共通鍵、ハッシュ等）
- 利用目的（守秘、認証、署名等）
- その他（求められる安全性のレベル等）

② 最低限の条件（要件）
- 安全性
- 実装性
- その他考慮すべき事項

③ その他、調達に必要な事項

調達のためのガイドブック案の内容

① 暗号選定
- セキュリティと暗号との関係（セキュリティポリシーとの関係）
- システムと利用目的
- 推奨暗号と製品の関係（製品リスト）
- 実際に調達する暗号方式及び推奨暗号
- 各推奨暗号の特性

② 実装
- 実装時の留意点

③ 運用
- 運用に係る鍵管理、実装、利用モード

④ その他関連情報
- 標準

2002年度活動案

①　４月～９月

リスト案の作成。（評価の継続及び精査、要件の精査）
調達のためのガイドブック案の作成。
新規提案暗号に関する公募は行わない。

②１０月～３月

各省庁合意のサポート。
調達のためのガイドブックの完成。
普及・啓蒙。
新規提案暗号に関する公募は行わない。

２００３年度以降の活動案

●電子政府推奨暗号のモニタリング。

●５年ごとの評価見直し。

●暗号の利用方法に関する各種ガイドラインの整備（作成、改訂）。

●データベースの管理。

●体制の拡充、高度化に向けた研究開発、人材育成、利用の定常化、普及の推進。

●暗号プロトコル評価、暗号モジュール評価の実施。

●米国NIST、ISO/IEC JTC1 SC27等との国際協力。

●必要に応じ国際標準との関係を整理。

●評価体制のあり方

２００３年度以降の評価体制のあり方について、米国ＮＩＳＴ等を参考にしつつ、恒常的な評価事務局の設置も含め、引き続き検討を行う必要がある。