電子政府推奨暗号リストについて

2003年5月22日

総務省情報通信政策局
通信規格課標準化推進官
藤本 昌彦

電子政府の実現

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推進戦略本部決定）

5．行政の情報化及び公共分野における情報通信技術の活用の推進

＜目標＞

① 行政の情報化については、行政情報の電子的提供、申請・届出等手続の電子化、文書の電子化、ペーパーレス化及び情報ネットワークを通じた情報共有・活用に向けた業務改革を重点的に推進し、**2003年度までに、電子情報を紙情報と同等に扱う行政を実現する。**

（2）施策の意義

国の行政機関においては、行政の情報化により、事務・事業及び組織の改革を推進するとともに、**セキュリティの確保に留意しつつ、**「紙」による情報の管理からネットワークを駆使した電子化された情報の管理へ移行し、**高度に情報化された行政、すなわち以下のような「電子政府」を実現する。**

（主な項目）
- 行政情報の電子的提供
- 申請・届出等手続の電子化
- 歳入・歳出の電子化
- 調達手続の電子化
- ペーパレス化（電子化）

e-Japan重点計画における暗号技術評価の位置付け

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推進戦略本部決定）

6．高度情報通信ネットワークの安全性及び信頼性の確保

（3）具体的施策

①情報セキュリティに係る制度・基盤の整備

ウ）暗号技術の標準化の推進（総務省及び経済産業省）

客観的にその安全性が評価され、実装性に優れた暗号技術を採用するため、2002年度までに、ISO、ITU等における暗号技術の国際標準化の状況を踏まえ、専門家による検討会の開催等を通じて電子政府利用等に資する暗号技術の評価及び標準化を行う。

セキュリティ・アクションプランにおける暗号技術評価の位置付け

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
（2001年10月10日 情報セキュリティ対策推進会議決定）

2．具体的な方策

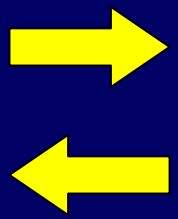
（2）暗号の標準化の推進

- 「電子政府」におけるセキュリティ確保のためには、政府調達における一定水準のセキュリティ確保のための情報機器等に関する基準（具体的にはISO/IEC15408）を可能な限り利用することと同様、暗号についても、一定水準以上の安全性及び信頼性を有するものの利用が不可欠であり、これを推進することが必要である。
- このため、総務省及び経済産業省は、両省で実施している研究会の成果等も踏まえ、2002年度中に「電子政府」における調達のための推奨すべき暗号のリストを作成し、これを踏まえ、各省庁における暗号の利用方針について合意を目指す。

CRYPTREC (Cryptography Research and Evaluation Committees)

・暗号アルゴリズム等に関する技術的評価の依頼
・その他、技術的事項に関する助言を求める

暗号技術検討会
(座長: 今井秀樹 東京大学教授)
事務局: 総務省、経済産業省



暗号技術評価委員会
(委員長: 今井秀樹 東京大学教授)
事務局: 通信・放送機構、
情報処理振興事業協会

・総務省及び経済産業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。

・暗号アルゴリズム等に関する評価結果の報告
・その他、技術的事項に関する助言を行う

・具体的な技術的評価を行う
・電子政府における暗号利用に資する各種ガイドラインを作成する
・技術的事項に関する助言を行う

暗号調達ガイドブック作成WG
(リーダ: 佐々木良一 東京電機大学教授)

共通鍵暗号評価小委員会
(委員長: 金子敏信 東京理科大学教授)

公開鍵暗号評価小委員会
(委員長: 松本 勉 横浜国立大学教授)

暗号技術検討会構成員

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	中央大学理工学部教授
	岩下 直行	日本銀行金融研究所調査第2課企画役
	岡崎 宏	情報通信ネットワーク産業協会常務理事
	岡本 栄司	筑波大学電子・情報工学系教授
	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管研究員
	小田 雅一	社団法人情報サービス産業協会セキュリティ委員会委員
	小柳津 育郎	NTTエレクトロニクス株式会社セキュリティシステム事業部技術部長
	加藤 義文	社団法人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	財団法人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教授
	佐々木 良一	東京電機大学工学部情報メディア学科教授
	宝木 和夫	社団法人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員教授

（2003年3月末現在、敬称略）

暗号技術検討会の開催状況（2001年度）

第1回　2001年5月16日

（主な議題）座長の選出
開催要綱及び2001年度活動計画の検討　ほか

第2回　2001年6月22日

（主な議題）「電子政府における暗号技術の要件調査」の実施　ほか

第3回　2001年7月27日

（主な議題）要件調査WGの検討状況　ほか

第4回　2001年10月3日

（主な議題）要件調査WGの検討状況
2001年度暗号技術公募状況　ほか

第5回　2002年1月18日

（主な議題）要件調査WGの検討状況
電子政府推奨暗号リストの作成に向けて　ほか

第6回　2002年2月22日

（主な議題）要件調査WGの検討状況
電子政府推奨暗号リストの作成に向けて　ほか

第7回　2002年3月11日

（主な議題）電子政府暗号候補及び2002年度詳細評価対象暗号の決定
要件調査WGの検討結果報告　ほか

暗号技術検討会の開催状況（2002年度）

第1回　2002年5月16日

（主な議題）暗号技術検討会の2002年度活動計画
暗号調達ガイドブック作成ワーキンググループの設置　ほか

第2回　2002年7月16日

（主な議題）暗号調達のためのガイドブック案の検討状況
電子政府推奨暗号リスト素案の検討状況
暗号モジュール評価の現状把握　ほか

第3回　2002年9月30日

（主な議題）電子政府推奨暗号リスト案
暗号調達のためのガイドブック案

第4回　2002年11月27日

（主な議題）電子政府推奨暗号リスト案及びパブリックコメント
暗号調達のためのガイドブック案
暗号プロトコルの現状把握（1）　ほか

第5回　2003年2月12日

（主な議題）電子政府推奨暗号リストの決定及びパブリックコメントに対する回答
暗号調達のためのガイドブック案
暗号プロトコルの現状把握（2）　ほか

第6回　2003年3月24日

（主な議題）暗号調達のためのガイドブックの確定
今後のCRYPTREC活動

電子政府システムで利用する暗号に求められる要件

2001年度、暗号技術検討会の下に「要件調査WG（リーダ：佐々木良一東京電機大学教授）」を設置し、「電子政府で用いられる、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求条件の調査及び検討」を実施

要件調査WGがまとめた、「電子政府で利用される暗号」が満たすべきと考えられる要件は以下のとおり。

（一般的要件）

- 暗号強度が十分高く、10年間、電子政府システムで安心して使えること
- 一般に使われる商用ソフトに予め入っているか、入る可能性の高いものが最低限一つは選ばれること

（その他、満たしていることが好ましい要件）

- 処理速度が速いこと
- ICカードへの実装性が優れていること
- 何らかの暗号標準又はプロトコル標準になっていること

暗号技術評価の概要

- 具体的な技術的評価は暗号技術評価委員会で実施

- 電子政府において利用が可能であると想定される暗号技術を以下の4つの分類に分け、評価対象暗号の募集及び選定を行い、各暗号技術を評価

  - 公開鍵暗号技術
  - 共通鍵暗号技術
  - ハッシュ関数
  - 擬似乱数生成系

- 電子署名法で使用される暗号や、その他評価が必要と判断された暗号についても評価を実施

電子署名法で使用される暗号技術の評価及び指針の改定

電子署名法で使用される暗号（電子署名の方式）の安全性評価を平成13年度に実施。
以下の方式について、電子署名法の指針の改定を提言。

技術分類	名称	評価結果の概要
公開鍵暗号	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。指針の改定を検討すべきである。
	RSA	RSA-PSSを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。
ハッシュ関数	MD5	MD5のハッシュ値は128ビットだが、最近の研究では、少なくとも160ビット以上が必要と考えられるため、指針から外すことを検討する必要がある。

本提言を踏まえて、平成14年11月に、総務省、経済産業省及び法務省は、電子署名法の指針を以下のとおり改定。

- 「ESIGN」を指針から削除
- 「RSA-PSS」を指針に追加
- 「MD5」の規定を指針から外す

電子政府推奨暗号リストの公表

- 暗号技術評価委員会から報告された暗号技術評価結果、及び、要件調査WGの調査結果に基づき、2002年11月に「電子政府推奨暗号リスト案」を作成

- 同リスト案は、2002年11月から同年12月までパブリックコメントを実施

- パブリックコメントで寄せられた意見等を、暗号技術検討会において検討し、2003年2月20日に総務省及び経済産業省から「電子政府推奨暗号リスト」として公表

報道資料（パブリックコメントの結果）

報道資料

平成１５年２月２０日
総　　務　　省
経　済　産　業　省

「電子政府」における調達のための推奨すべき暗号のリスト案に対する意見募集の結果

総務省及び経済産業省は、「電子政府」における調達のための推奨すべき暗号（以下「電子政府推奨暗号」という）のリスト案（以下「電子政府推奨暗号リスト案」という）について、平成１４年１１月２８日から同年１２月２５日までの期間、両省のホームページに掲載するなどして、国民の皆様から広く意見を受け付けたところ、２件の御意見を頂きました。お寄せいただいた御意見及び当該意見に対する総務省及び経済産業省の考え方は別紙１のとおりです。
お寄せいただいた御意見等を検討した結果、電子政府推奨暗号リストは原案どおりといたします（別紙２）。
なお、「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」（平成１３年１０月１０日情報セキュリティ対策推進会議）に基づき、本リストを踏まえ、本年度中に各省庁における電子政府推奨暗号の利用方針について合意を目指す予定です。

１．概要

総務省及び経済産業省は、「電子政府」におけるセキュリティ確保のために、暗号について一定水準以上の安全性及び信頼性を有するものの利用が不可欠であることから、総務省及び経済産業省が開催する「暗号技術検討会（座長：今井秀樹東京大学教授）」、並びに、通信・放送機構（ＴＡＯ）及び情報処理振興事業協会（ＩＰＡ）が開催する「暗号技術評価委員会（委員長：今井秀樹東京大学教授）」の両研究会による暗号評価プロジェクト「CRYPTREC（Cryptography Research and Evaluation Committees）」（別添参照）により暗号を公募の上客観的に評価し、１０年間は安心して利用できるという観点から選定した電子政府推奨暗号リスト案について、平成１４年１１月２８日から同年１２月２５日まで意見募集を行ったところ、２件の御意見を頂きました。

お寄せいただいた御意見に対する総務省及び経済産業省の考え方は別紙１のとおりです。

２．今後の予定

「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」に基づき、本リストを踏まえ、本年度中に各省庁における電子政府推奨暗号の利用方針について合意を目指す予定です。

連絡先：総務省情報通信政策局通信規格課
（担当：佐藤専門職、福岡）
電話　：（代表）０３－５２５３－５１１１
内線５７６２
（直通）０３－５２５３－５７６２
ＦＡＸ：０３－５２５３－５７６４

別紙１

「電子政府」における調達のための推奨すべき暗号のリスト案に対する御意見及びそれに対する考え方

提出元	御意見	総務省及び経済産業省の考え方
個人	特許権の使用料を求める暗号化アルゴリズムは電子政府推奨暗号リストから除外するべきと考える。 （理由） 特許料の徴収によりコストが増大することと特許権の行使により個人のソフトウェア作者が実装出来ない場合が起こりえるから。	御指摘の点に関し、CRYPTRECでは、電子政府推奨暗号アルゴリズムについて応募元に知的財産権に関する調査を実施しており、応募元が所有する知的財産権の電子政府における使用に関し、同暗号アルゴリズムの通常実施権（又は著作権の利用）が非差別的かつ妥当な条件（無償を含む）で許諾される旨の回答を受けています。 また、同リスト案には、技術分類別に複数個の暗号アルゴリズムが選定されていることから、電子政府システムの調達者は、各暗号アルゴリズムの知的財産権の実状も把握した上で適切な暗号アルゴリズムを選定できると考えます。
企業	今後の暗号リスト案の見直し時期・更新の手続きを明確にすべき。 （理由） 本リストは、電子政府のセキュリティ確保という重要かつ恒久的な分野に用いるための暗号リストであり、暗号技術の進歩に対する「維持管理」が重要な課題となる。その観点から、少なくとも、国際的標準化／評価機関などでの暗号方式の認定を参考にすべきであり、継続的にこれらの動向を監視し、わが国の電子政府構築に関係する暗号方式が認定された場合には、速やかに暗号リストの見直しを行うべきである。	電子政府推奨暗号の監視及び電子政府推奨暗号リストの改訂の在り方については、現在CRYPTRECにおいて検討しているところです。なお、電子政府推奨暗号リストの改訂については、今後の電子政府推奨暗号の電子政府システムにおける利用状況等も考慮する必要があることから、電子政府が本格的に稼働する来年度以降、CRYPTRECにおいて更に検討を継続していくこととしています。

報道資料（パブリックコメントの結果）

別紙2

電子政府推奨暗号リスト

平成１５年２月２０日
総　　務　　省
経　済　産　業　省

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5(注 1)
	鍵共有	DH
		ECDH
		PSEC-KEM(注 2)
共通鍵暗号	64 ビットブロック暗号(注 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(注 4)
	128 ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注 5)
その他	ハッシュ関数	RIPEMD-160(注 6)
		SHA-1(注 6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系(注 7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

注釈：

（注 1）　SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。

（注 2）　KEM（**Key Encapsulation Mechanism**）-DEM(Data **Encapsulation Mechanism**)構成における利用を前提とする。

（注 3）　新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

（注 4）　3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。

1）　FIPS46-3 として規定されていること

2）　デファクトスタンダードとしての位置を保っていること

（注 5）　128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。

（注6）　新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。

（注7）　擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

暗号技術評価件数等の内訳

	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	合計
	守秘	署名	鍵共有	認証	64ビットブロック暗号	128ビットブロック暗号	ストリーム暗号				
応募総数	9	10	8	1	4	9	9	0	9	2	61
評価総数	10	15	9	1	6	11	10	6	15	2	85
最終結果	**2**	**4**	**3**	**0**	**4**	**5**	**3**	**5**	**3***	**0**	**29**

＊　例示

電子政府推奨暗号リスト（1/3）

公開鍵暗号　9方式

公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5（注1）
	鍵共有	DH
		ECDH
		PSEC-KEM（注2）

（注1） SSL3.0/TLS1.0で使用実績があることから当面の使用を認める。

（注2） KEM（Key Encapsulation Mechanism）－ DEM（Data Encapsulation Mechanism）構成における利用を前提とする。

電子政府推奨暗号リスト（2/3）

共通鍵暗号　12方式

共通鍵暗号（注3）	64ビットブロック暗号	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES（注4）
	128ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4（注5）

（注3） 新たな電子政府システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128ビットブロック暗号を選択することが望ましい。

（注4） 3-key Triple DESは、以下の条件を考慮し、当面の使用を認める。
1) FIPS46-3として規定されていること
2) デファクトスタンダードとしての位置を保っていること

（注5） 128-bit RC4は、SSL3.0/TLS1.0以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。

電子政府推奨暗号リスト(3/3)

その他　　8方式

その他	ハッシュ関数	RIPEMD-160(注6)
		SHA-1(注6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系 (注7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+change notice 1) revised Appendix 3.1

(注6) 新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号の仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。

(注7) 擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

電子政府推奨暗号の仕様に関する情報提供

TAOホームページ
（http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec20030425_spec01.html）
IPAホームページ
（http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030425_spec01.html）

において、電子政府推奨暗号の仕様に関する情報（仕様書又は仕様参照先URL）を提供

暗号の利用方針に関する省庁間合意

2003年2月28日に、行政情報システム関係課長連絡会議において「各府省の情報システム調達における暗号の利用方針」が了承された。

（「各府省の情報システム調達における暗号の利用方針」から抜粋）

電子政府における情報セキュリティ確保のために、各府省の情報システムにおいて暗号を利用する場合には、一定水準以上の安全性及び信頼性を有する暗号の利用が不可欠であり、また、その安全性・信頼性は客観的な評価を得たものであることが必要である。

（中略）

これを踏まえ、**各府省は、情報システムの構築にあたり暗号を利用する場合には、**調達仕様書において上記暗号リストに掲載された暗号を利用することを入札要件とする等の方法により、必要とされる安全性・信頼性などに応じ、**可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとする。**

なお、**総務省及び経済産業省は、「電子政府推奨暗号リスト」に掲載された暗号の安全性及び信頼性について、今後の情報通信技術の進展を踏まえ必要に応じ評価を行う**とともに、「電子政府推奨暗号リスト」の内容の変更を行う場合には、本会議に報告することとする。

報道資料（暗号の利用方針に関する省庁間合意）

報道資料

平成１５年３月３日
総　　務　　省

各府省の情報システム調達における暗号の利用方針

平成１５年２月２８日、各府省の情報システム関係課長を構成員とする「行政情報システム関係課長連絡会議」（事務局：総務省行政管理局）において、「各府省の情報システム調達における暗号の利用方針」が了承されましたので、公表します。

本利用方針は、「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」（平成１３年１０月１０日、情報セキュリティ対策推進会議）に基づき策定された「電子政府推奨暗号リスト」（平成１５年２月２０日、総務省・経済産業省）を踏まえ、各府省が情報システムの構築に当たり暗号を利用する場合の基本的な方針、「電子政府推奨暗号リスト」の内容の変更があった場合の対応について定めたものです。

別紙：「各府省の情報システム調達における暗号の利用方針」
（平成１５年２月２８日、行政情報システム関係課長連絡会議了承）

（連絡先）
＜暗号の利用方針＞
総務省行政管理局行政情報システム企画課
担当：宮崎課長補佐、中原係長
（TEL）　03-5253-5341（直通）
（FAX）　03-5253-5346
＜電子政府推奨暗号リスト＞
総務省情報通信政策局通信規格課
担当：佐藤専門職、福岡
（TEL）　03-5253-5111（内線 5762）
03-5253-5762（直通）
（FAX）　03-5253-5764

各府省の情報システム調達における暗号の利用方針

平成１５年２月２８日
行政情報システム関係課長連絡会議了承

電子政府における情報セキュリティ確保のために、各府省の情報システムにおいて暗号を利用する場合には、一定水準以上の安全性及び信頼性を有する暗号の利用が不可欠であり、また、その安全性・信頼性は客観的な評価を得たものであることが必要である。

かかる観点から、「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」（平成１３年１０月１０日、情報セキュリティ対策推進会議）に基づき、総務省及び経済産業省において、電子政府における調達のための推奨すべき暗号のリスト（「電子政府推奨暗号リスト」：別添参照）を策定したところである。

これを踏まえ、各府省は、情報システムの構築に当たり暗号を利用する場合には、調達仕様書において上記暗号リストに掲載された暗号を利用することを入札要件とする等の方法により、必要とされる安全性・信頼性などに応じ、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとする。

なお、総務省及び経済産業省は、「電子政府推奨暗号リスト」に掲載された暗号の安全性及び信頼性について、今後の情報通信技術の進展を踏まえ必要に応じ評価を行うとともに、「電子政府推奨暗号リスト」の内容の変更を行う場合には本会議に報告することとする。

電子政府構築計画（仮称）

- 本年6月末を目途に、各府省情報化統括責任者（CIO）連絡会議において「電子政府構築計画（仮称）」が決定される予定。
- 2003年度～2005年度の3か年計画
- 同連絡会議において、3月31日に、電子政府構築の原則、各府省計画の検討にあたっての基本的考え方等を明記した「電子政府構築計画の策定に向けて」を決定。

電子政府構築計画（仮称）イメージ

（計画期間：2003年度（平成15年度）～2005年度（平成17年度））

1月 ～ 3月

電子政府構築計画の策定に向けて

（3月31日 CIO連絡会議決定）

第1 基本的考え方

電子政府構築の原則、目標、計画の構成等

第2 施策の基本方針

Ⅰ 国民の利便性・サービスの向上
- 1 オンライン利用の促進
- 2 ワンストップサービスの拡大
- 3 利用者視点に立ったシステムの整備、サービスの改善

Ⅱ IT化に対応した業務改革
- 1 内部管理等の業務・システムの効率化・合理化
- 2 個別業務の業務・システムの効率化・合理化

Ⅲ 共通的な環境整備

4月 ～ 6月

電子政府構築計画

（6月末目途 CIO連絡会議決定）

第1 基本的考え方

第2 施策の基本方針

Ⅰ 国民の利便性・サービスの向上
- 1 オンラインの利用の促進
- 2 ワンストップサービスの拡大
- 3 利用者視点に立ったシステムの整備、サービスの改善

Ⅱ IT化に対応した業務改革
- 1 内部管理等の業務・システムの効率化、合理化
- 2 個別業務の業務・システムの効率化、合理化

Ⅲ 共通的な環境整備

第3 各府省別計画
- 1 内閣府計画
- 2 総務省計画
- ⋮

電子政府構築計画（仮称）における暗号の利用方針の取扱い

「電子政府構築計画（仮称）の策定に向けて（2003年3月31日 各府省情報化統括責任者（CIO）連絡会議決定）」では、電子政府構築にあたっての共通的な環境整備の一つとして「情報セキュリティ対策等の充実・強化」が掲げられており、その中で、「暗号の利用方針」に基づく暗号の利用の推進が述べられている。

（「電子政府構築計画（仮称）の策定に向けて」から抜粋）

第２　施策の基本方針

Ⅲ　共通的な基盤整備

３　情報セキュリティ対策等の充実・強化

（１）情報システムの安全性・信頼性の確保

③　各府省の情報システムの構築にあたり暗号を利用する場合には、「各府省の情報システム調達における暗号の利用方針」（2003年（平成15年）2月28日行政情報システム関係課長連絡会議了承）に基づき、客観的な評価を得た、一定水準以上の安全性・信頼性を有する暗号の利用を推進する。