



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2004 情財第 397 号

暗号の危殆化に関する調査 報告書

2005 年 3 月
独立行政法人 情報処理推進機構

目 次

1. 暗号技術を取り巻く状況.....	1
2. 暗号危殆化の定義.....	3
2.1. 暗号危殆化の定義.....	3
2.2. 暗号危殆化の要因.....	5
2.3. 暗号危殆化の進行過程.....	7
3. 暗号危殆化をめぐる国内外の状況.....	8
3.1. 研究開発の状況.....	8
3.2. 公的機関における検討の状況.....	16
4. 暗号危殆化の電子政府への影響分析.....	37
4.1. 電子政府システム.....	37
4.2. 暗号アルゴリズム危殆化の影響分析.....	41
4.3. 電子政府システムに係る文書の長期保存.....	46
4.4. まとめ.....	48
5. 暗号危殆化に係わる問題点.....	49
5.1. 電子政府に係わるプレイヤーから見た問題点.....	49
5.2. 法的な問題点.....	58
6. 暗号危殆化に備えた対策のあり方.....	63
6.1. 想定する対策の対象と体制.....	63
6.2. 暗号危殆化のレベル.....	64
6.3. 暗号危殆化のレベルに対応した対策のあり方.....	66
7. 提言.....	77
7.1. 内容.....	77
7.2. 優先度またはスケジュール.....	79

1. 暗号技術を取り巻く状況

1994年に開始された電子政府構想は、2004年3月末現在、行政手続きの電子化推進アクションプランに定められた¹約13,000件の電子化対象手続きの約96%の電子化²、マルチペイメントネットワークを利用した行政手数料の支払い(2004年1月)、公的個人認証サービスの運用開始(2004年1月)等、着実に推進されている。また、2003年の電子商取引の市場規模は、BtoB 77兆円、BtoC 4.4兆円となっている³。このように、商用、非商用にかかわらず、インターネットを介したサービスは拡大してきている。これらのサービスにおいては、SSL(Secure Socket Layer)をはじめとするPKI(Public Key Infrastructure)等、暗号技術がコア技術として使用されている。

現在の暗号技術は、計算機を用いても解読するために莫大な時間や費用がかかることを前提として、その安全性を保障している⁴。しかし、Gridコンピューティング等の計算機技術の進歩や暗号解読技術の発展により、現実的な時間で暗号が解読されるという事例が報告され始めている。たとえば、米国商務省標準局(National Bureau of Standard, NBS)が1977年に一般コンピュータ用標準暗号として選定したDES(Data Encryption Standard)は、1999年1月、RSA Security社が主催したDES Challenge IIIにおいて、約22時間で解読されている⁵。また、代表的な公開鍵暗号であり、最も普及しているRSA暗号においても、同RSA Security社のFactoring Challenge⁶において、2003年12月3日に576bitの素因数分解が報告された。これにより、現在主に利用されている1024bit鍵のRSA暗号および署名に対して、危機感を募らせている研究者も存在する。

また、暗号をソフトウェアやハードウェアで実装した暗号モジュールにおいては、実装上または運用上の脆弱性から内部の秘密鍵が漏洩し、社会的に影響が及ぶ場合がある。例えば、PKIにおける認証局(Certification Authority: CA)が有するCA鍵は耐タンパー性⁷を有するハードウェアモジュールにより保護されているが、モジュール実装上の脆弱性や運用上の問題が存在する場合、それを原因としてCA鍵が漏洩し、CAに成りすますことが可能になることがある。これにより、CAが提供する認証等のサービスの信頼性が低下し、さまざまな影響が出ることが予想される。このようなモジュール実装上の脆弱性をついた暗号の解読技術は、サイドチャネル攻撃と呼ばれ、近年学会等で盛んに検討されている。

¹ 行政手続きの電子化推進アクションプラン、<http://www.e-gov.go.jp/doc/action.html>

² 総務省、“電子政府の推進に関する調査報告書”、2004年6月9日。

³ 経済産業省、電子商取引推進協議会、(株)NTTデータ経営研究所、“平成15年度電子商取引に関する実態・市場規模調査”、2004年6月11日。

⁴ 計算量的安全性と呼ばれる。これに対して、情報量的安全性がある。

⁵ DES Challenge III, <http://www.rsasecurity.com/rsalabs/node.asp?id=2108>

⁶ The New Factoring Challenge, <http://www.rsasecurity.com/rsalabs/node.asp?id=2092>

⁷ モジュール内部をのぞき見ることが困難な性質。ハードウェアの物理的な性質を利用して実現されることが多い。

上記のように、ある一定の信頼性を持っていた暗号が計算機能力の向上やモジュール実装上の問題により、秘密に保持されるべき鍵が漏洩し得る状態は、暗号の危殆化と呼ばれる。電子政府や電子商取引が実用化された現在、これらのシステムで使用されている暗号が危殆化することにより、システム全体に影響が及ぶことが予想される。例えば、電子署名に使用していた暗号が危殆化することにより、生成された、または、生成される電子署名の信頼性が低下し、その証拠性に対する疑義が生じることが予想される。

暗号の危殆化は、技術の進歩等により長期的には必然性を有している。しかし、暗号の危殆化問題は、専門家の間においても認識され始めたばかりであり、その認識にはばらつきがあるようである。政府における暗号の危殆化に対する体制として、日本における CRYPTREC (CRYPTography Research & Evaluation Committees)⁸のように、暗号の安全性監視体制を持つ国は少ない。また、CRYPTRECにおいては、自身が策定した電子政府推奨暗号リストに対して、安全性上の問題から、ある暗号をそのリストから削除する権限を有するが、危殆化に対して積極的な行動を起こすことは現状ではできない。

以上まとめると、暗号の危殆化は必然性を有し、その影響が広範に及ぶことが予想されるが、専門家および政府における認識にばらつきがあり、技術的および制度的対策が不十分である。そこで、本調査においては、暗号の危殆化問題に対して、専門化および政府を始めとして共通認識をはかり、主に電子政府における暗号アルゴリズムの危殆化の影響範囲を把握することを目的とする。さらには、暗号アルゴリズムの危殆化に対する現状における技術的および制度的対策を明らかにしつつ、2005 年度以降の CRYPTREC の活動を含む技術的、制度的対策立案に資する提言を行うことを目的とする。

⁸ CRYPTREC, <http://www.ipa.go.jp/security/enc/CRYPTREC/index.html>

2. 暗号危殆化の定義

ここでは暗号危殆化の定義を示す。

2.1. 暗号危殆化の定義

前章で示すように、暗号の安全性が危ぶまれる事態としては、暗号アルゴリズム自体に問題が見つけれられた場合、暗号の実装に関して問題が見つけれられた場合など、原因や影響範囲の点で様々な事態が考えられる。危殆化という用語は、情報セキュリティ分野においてしばしば使われてきたが、その指し示す対象によって異なる意味で用いられている⁹。危殆化という用語が指し示す局面は、(1)暗号アルゴリズム自体に問題がある場合、(2)暗号を実装したソフトウェア/ハードウェア等に問題がある場合、(3)暗号を利用したシステムにおける運用上の問題が生じた場合の3つに大別できる。

そこで、暗号技術の専門家等の有識者の知見を踏まえ、暗号の危殆化を幅広く論じる際に含まれ得る範囲を把握するとともに今回の調査の対象範囲を明確化するために、以下のように3つの階層に分けて暗号危殆化の定義を行った。

2.1.1. 暗号アルゴリズムの危殆化

暗号アルゴリズムの危殆化を次のように定義する。

暗号アルゴリズムの危殆化とは、ある暗号アルゴリズムについて、当初想定したよりも低いコストで、そのセキュリティ上の性質を危うくすることが可能な状況を指すものとする。ここで暗号アルゴリズムおよびそのセキュリティ上の性質とは以下を指す。

共通鍵暗号	<ul style="list-style-type: none">・ 秘密鍵を持つ場合のみ暗号化および復号が可能である性質・ 平文と暗号文のペアが与えられた際に、秘密鍵の推定が困難である性質
公開鍵暗号	<ul style="list-style-type: none">・ 秘密鍵を持つ場合のみ復号が可能である性質・ 平文と暗号文のペアおよび/または公開鍵が与えられた際に、秘密鍵の推定が困難である性質
ハッシュ関数	<ul style="list-style-type: none">・ 一方向性・ 衝突困難性
疑似乱数	<ul style="list-style-type: none">・ 統計的性質（統計的一様性、無相関性、長周期性等）・ 予測不可能性（非線形性）

⁹ 一般にcompromise（英語）の訳語として危殆化が当てられている。compromiseという言葉は、システムセキュリティ分野においては侵入を受けた状態を示す際などに用いられる（RFC2828等を参照）。また、PKI技術分野においては秘密鍵が漏洩等により機密性を失った場合を指して「鍵の危殆化」と呼んでいる。

暗号アルゴリズムの危殆化に関する検討においては、要素技術としての暗号アルゴリズムに危殆化の要因が存在する問題のみを検討の対象とする。

広く使われている暗号アルゴリズムについて、従来主張されなかった知的財産権が主張されることによりその利用が困難になる事態も想定されるが、これは利用可能性に係る問題とみなし、暗号アルゴリズムの危殆化とはみなさない。

本報告書では、特にハッシュ関数を含む暗号アルゴリズムの危殆化を中心に検討を行う。

2.1.2. 暗号モジュールの危殆化

ここでは暗号アルゴリズムの実装であるソフトウェア、ハードウェア、あるいはそれらの組み合わせを暗号モジュールと定義する。暗号モジュールの危殆化を次のように定義する。

暗号モジュールの危殆化とは、ある暗号モジュールについて、当初想定したより低い現実的なコストで、権限が与えられていないデータや資源にアクセス可能な状況を指すものとする。ここでいうアクセスとは、秘密情報や暗号機能の推定・開示、変更、使用を含む。

暗号モジュールの危殆化に関する検討においては、暗号アルゴリズムを利用した製品等の暗号モジュールの実装に関する諸問題が検討の対象となる。

2.1.3. 暗号を利用するシステムの危殆化

ここでは、単数あるいは複数の暗号モジュールを含むシステムを、暗号を利用するシステムとして定義する。暗号を利用するシステムの危殆化を次のように定義する。

暗号を利用するシステムの危殆化とは、あるシステムにおける暗号が関連する機能について、当初想定したよりも低い現実的なコストで、権限が与えられていないデータやシステム資源にアクセス可能な状況を指すものとする。

暗号を利用するシステムの危殆化に関する検討においては、暗号を用いたシステムの構成・運用における諸問題が主な検討の対象となる。

2.2. 暗号危殆化の要因

暗号アルゴリズムの危殆化要因については、暗号技術分野における(1)攻撃手法の進歩以外に、より一般的な(2)計算機能力の向上(3)計算機モデルの変化が挙げられる。これらに関する整理を図 2-1に示す。

また、暗号モジュールの危殆化および暗号利用システムの危殆化については、暗号アルゴリズムの危殆化以外の要因を含め、整理した結果を図 2-2、図 2-3に示す。

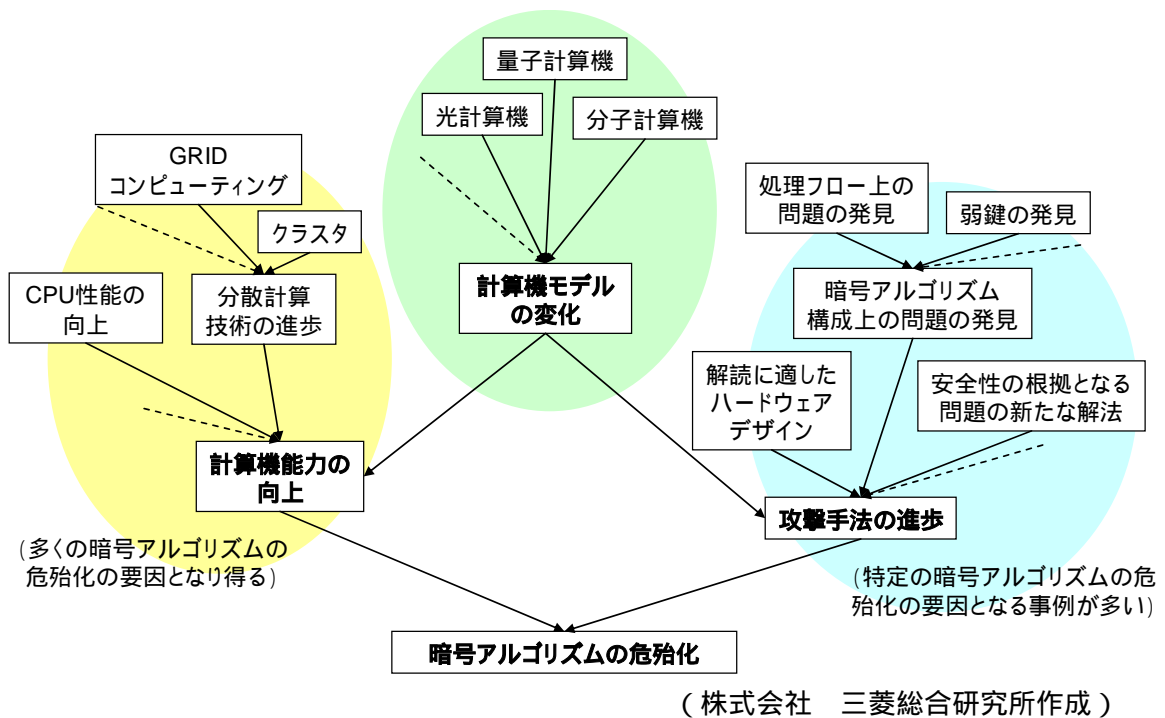
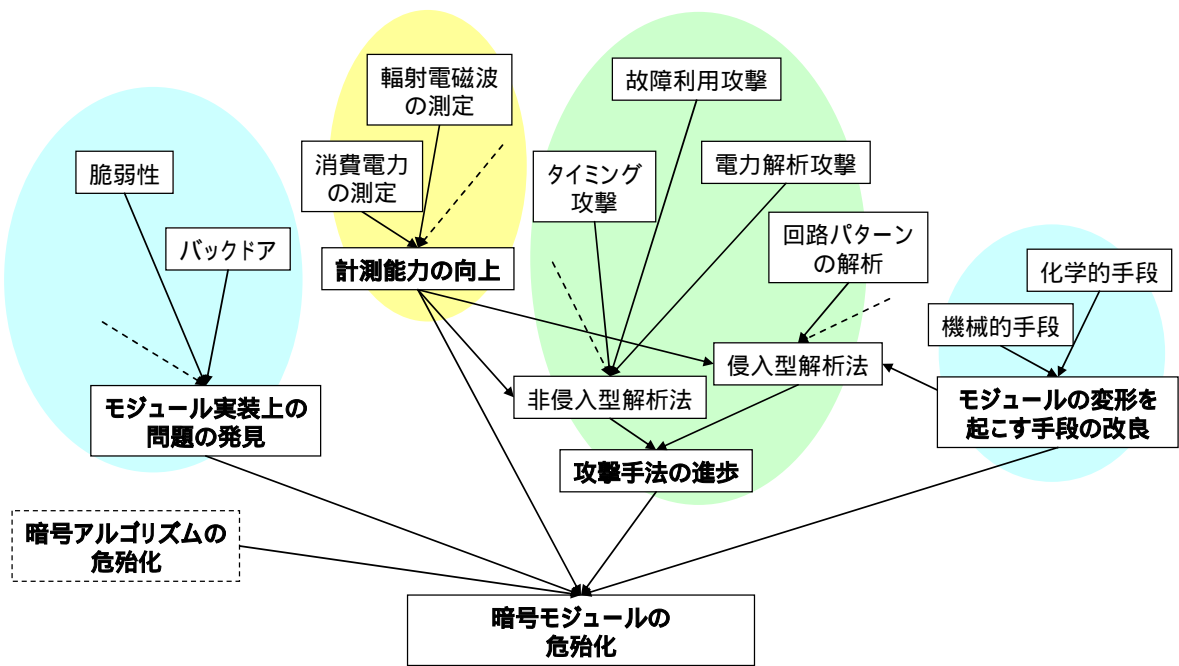
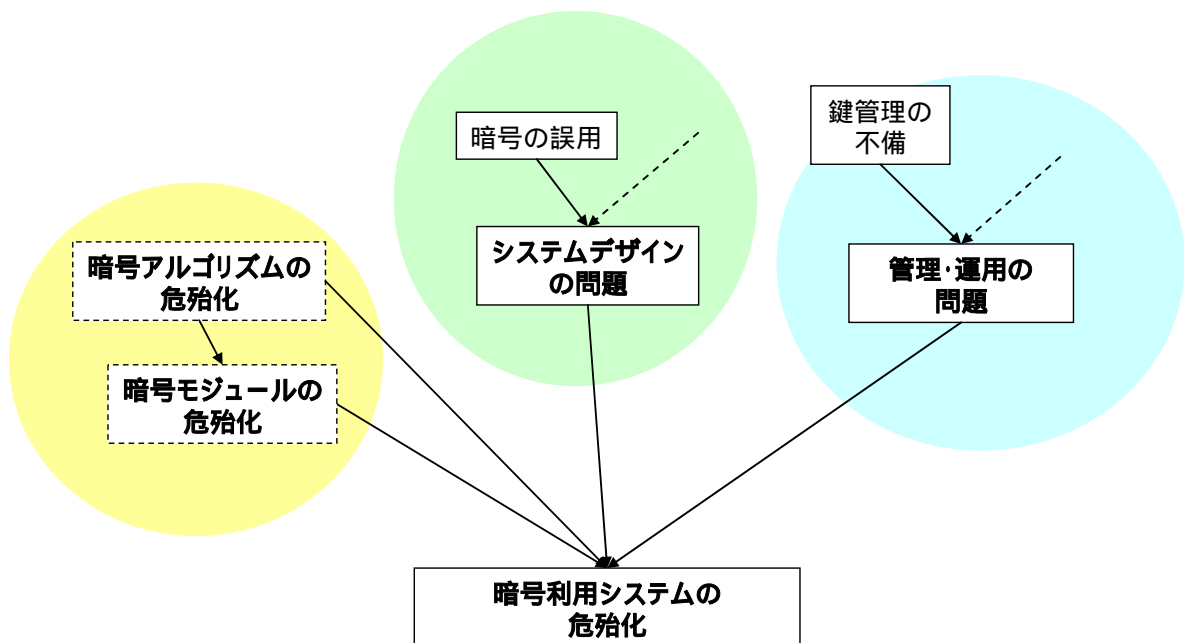


図 2-1 暗号アルゴリズムの危殆化要因



(株式会社 三菱総合研究所 作成)

図 2-2 暗号モジュールの危殆化要因



(株式会社 三菱総合研究所 作成)

図 2-3 暗号利用システムの危殆化要因

2.3. 暗号危殆化の進行過程

本報告書においては、暗号アルゴリズムの危殆化には以下の特徴があると想定し、これらを踏まえた上で暗号アルゴリズムの危殆化に対する技術的・制度的対策を検討した。

- ・ 一般に暗号アルゴリズムの危殆化は段階的に進行する。暗号アルゴリズムの安全性が明日にも脅かされるといった可能性が提示されることは稀であり、多くの場合は近い将来の危殆化を想定して、今後の暗号アルゴリズムの利用に注意を促すことが可能である。
- ・ 暗号技術に関する継続的な安全性評価と情報収集により、危殆化の進行状況が捉えられる。主に学会等で公表される情報に基づいて将来の危殆化が予告されるため、問題発生前に事態の把握は比較的行きやすい。
- ・ 危殆化の判明が進む速度の緩急により、これに応じて必要な対策の進行速度に差は生じるが、おおむね、同じ手順で対策を組むことが可能である。

3. 暗号危殆化をめぐる国内外の状況

3.1. 研究開発の状況

現代の主要な暗号の安全性は、計算機を用いても解読するためには膨大な時間や費用がかかることを前提とした、計算量的安全性に依拠している。しかし、計算機能力の向上や解読手法の進歩といった技術進歩により暗号の安全性が低下して危殆化した状態になると、デジタル署名等の証拠性に疑義が生じてくる。

そこで、暗号危殆化への技術的対策としては、計算能力向上や解読技術といったそもそもの暗号アルゴリズム危殆化の要因に左右されないような暗号アルゴリズムを設計するという**安全性確保型**と、デジタル署名等の証拠性を確保または補強するような**証拠性確保型**がある。安全性確保型対策には、計算能力向上といった危殆化要因に対する対策である**計算能力対応型**と既知の解読手法への耐性を持たせる**脆弱性補完型**がある。証拠性確保型の対策には、使用している暗号が危殆化しても偽造の判定等を可能とする**偽造判定型**と、暗号危殆化に備えて電子文書等の原本を安全に保管しておく**データ保管型**の対策がある。

以上、まとめると表 3-1 のようになる。

表 3-1 暗号危殆化の対策技術分類

	前提	応用
暗号技術	計算機能力が向上したとしても、解読には膨大な時間がかかる。	署名等に関して、長期にわたる証拠性確保が可能となる。
暗号危殆化問題	計算機能力向上、解読技術の進歩により暗号の安全性が低下する。	署名等の証拠性に疑義が生じる。
対策技術分類	安全性確保型	証拠性確保型
	計算機能力対応型	脆弱性補完型

(株式会社 三菱総合研究所 作成)

暗号危殆化の対策技術の分類の詳細と具体的技術を下表 3-2 にまとめる。

表 3-2 暗号危殆化技術分類

大分類	小分類	詳細	個別技術
安全性確保型	計算機能力対応型	計算機能力が向上しても、安全性を確保可能な暗号アルゴリズムを構成する。	Unconditional Secure 署名 量子公開鍵暗号
	脆弱性補完型	解読技術等に対応するために、既知の攻撃への耐性を持たせるような暗号アルゴリズムを構成する。	暗号設計技術
証拠性確保型	偽造判定型	電子署名等のデータに何らかの情報を織り込んでおいて、偽造等を判別可能とする方法。暗号が危殆化しても、偽造された署名であるか等判定可能であるので、ある一定の証拠性を確保できる。	タイムスタンプ (ETSI TS 101 155) Forward Secure 署名 Key Insulated 署名 Intrusion Resilient 署名 電子署名アリバイ実現機構 ハードウェア確認タグ付署名 Fail Stop 署名
	データ保管型	暗号が危殆化したときのために、電子文書データ等を安全に保管しておく技術。危殆化後に保管されているデータを証拠として利用する。	セキュア・アーカイバ 電子公証

(株式会社 三菱総合研究所 作成)

以下、個別に概略を述べる。

3.1.1.1. 計算能力対応型

現代の主要暗号の多くは計算量的安全性に依拠して設計されているため、計算機技術の進歩による計算能力向上や費用低減は、暗号危殆化の根本的な要因となる。従って、暗号の理論研究においては、計算機技術の進歩に左右されないような暗号アルゴリズムを設計するものがあり、これらは暗号危殆化の根本要因に対する対策技術となる。

(1) Unconditional Secure 署名¹⁰

Unconditional Secure 署名は、四方らによって提案された署名方式である。

この方式は、計算量理論ではなく、情報理論に基づいて設計された署名アルゴリズムであるため、量子計算機等が実現したとしても、その署名偽造の困難性などの安全性は情報

¹⁰ Junji Shikata, Goichiro Hanaoka, Yuliang Zeng and Hideki Imai, “Security Notions for Unconditionally Secure Signature Schemes”, Proc. Of EUROCRYPT 2002, LNCS 2332, pp.434—pp.449, Springer-Verlag, 2002.

理論的に保証される。

(2) 量子公開鍵暗号¹¹

量子公開鍵暗号は、岡本らによって提案された公開鍵暗号方式である。

RSA暗号などは、量子計算機が実現するとその安全性が保証されないことが報告されている¹²。そこで、この方式は量子計算機を用いても解読するために膨大な時間や費用を要するように設計された公開鍵暗号方式である。

3.1.2. 脆弱性補完型

現代暗号の安全性は、解読するために必要な計算量が膨大となることを前提とした計算量的安全性に依拠している。しかし、その構成の仕方によっては、その前提となる計算量未満で解読が可能となることがある。このような暗号アルゴリズム構成上の脆弱性は、専門家が解析を行なうことで発見され、新たな解読手法に利用される。他方、新たな暗号アルゴリズムを構成する際には、既知の解読手法に対して十分に安全であるように設計される。

このように、解読手法と暗号設計技術は相互補完的に進められ、新たな暗号アルゴリズム構成上の脆弱性を補完する。

3.1.3. 偽造判定型

偽造判定型の技術は、何らかの要因により、秘密に保持されているはずの署名生成鍵の漏洩等により、署名の偽造が可能な状況になったとしても、署名生成時期等に関する情報や署名生成モジュールに関する情報をデジタル署名データに付すことで、偽造署名と正当な署名を判別可能にする。これにより、これらの技術は、デジタル署名に対してある一定の証拠性確保を保持させることを目的とした技術である。

(1) タイムスタンプ技術

タイムスタンプ技術は、作成された文書データ等に対して、信頼できるオーソリティが履歴や時刻といった情報を文書データに付して、電子署名をつけることで、オーソリティが署名を付した時間にその文書データが存在していたことを証明する技術である。

タイムスタンプ技術には、大別して、シンプル・プロトコルとリンキング・プロトコルが存在する。

- シンプル・プロトコル

¹¹ Tatsuaki Okamoto, Keisuke Tanaka, Shigenori Uchiyama, “Quantum Public Key Cryptosystems,” Proc of CRYPTPTO 2000, LNCS 1880, pp.147—pp.165, Springer-Verlag, 2000.

¹² Peter W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM Journal on Computing, Vol.26, No.5, pp.1484—pp.1509, Oct. 1997.

タイムスタンプ技術におけるシンプル・プロトコルは、存在を証明したい文書のハッシュ値に対して、タイムスタンプ・オーソリティが原子時計等から入手した時刻情報を付加し、デジタル署名を付すことで、その文書がある時刻に存在したことを証明する（図 3-1）。

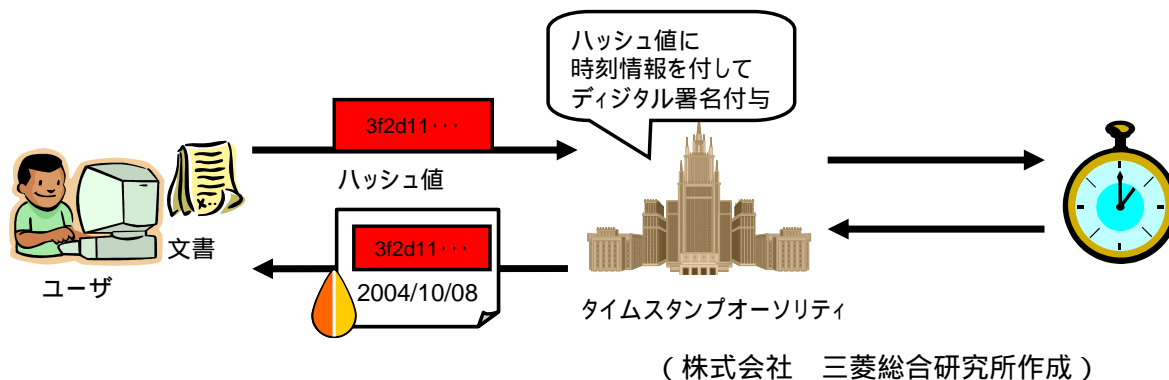


図 3-1 シンプル・プロトコル

- リンキング・プロトコル

リンキング・プロトコルは、存在を証明したい文書のハッシュ値に対して、タイムスタンプ・オーソリティがこれまでのリンク情報(これまでの文書のハッシュ値とそれらの順序関係が暗号的に証明可能な情報)を用いて、新たなリンク情報を生成し、保管することで、その文書がある文書と別の文書の間が存在したことを保証するものである（図 3-2）。

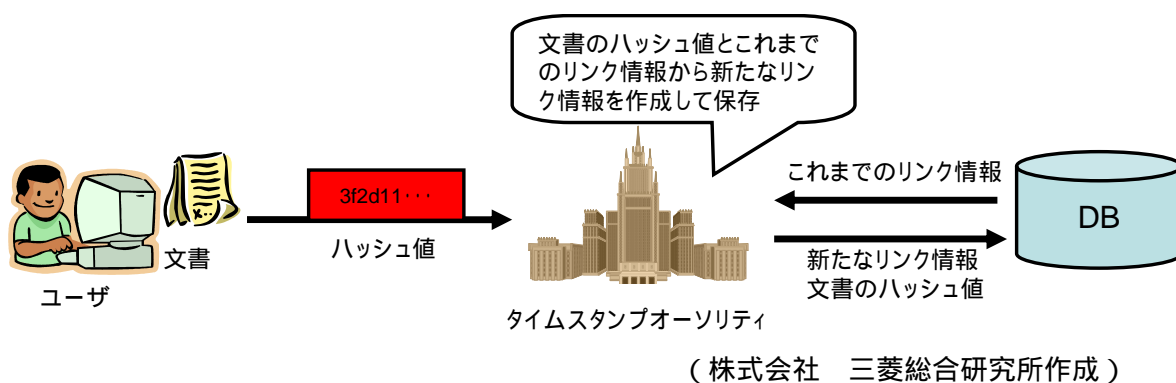
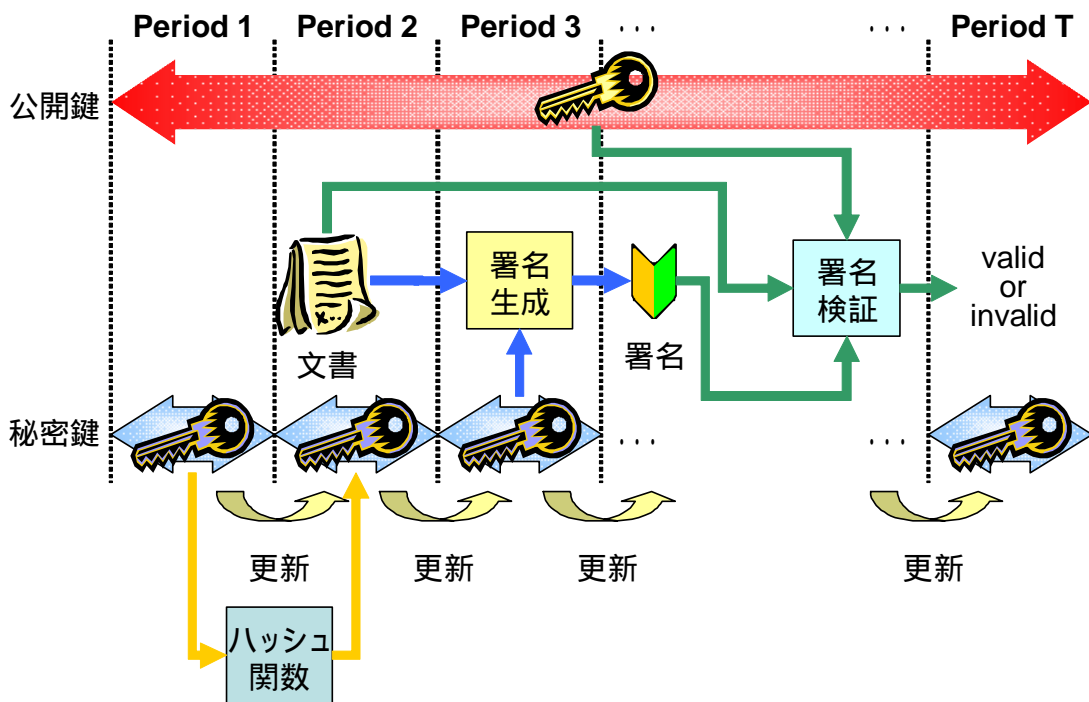


図 3-2 リンキング・プロトコル

(2) Forward Secure 署名¹³

電子署名においては、署名生成鍵は秘密に管理されていることが前提となっている。しかし、暗号の危殆化により、署名生成鍵が漏洩する可能性や署名が偽造される可能性が高まると、ある署名生成鍵で生成した全ての電子署名について、偽造の可能性が発生する。

Forward Secure 署名は、期間ごとに署名生成鍵を更新することで、ある期間に署名生成鍵が漏洩したとしても、それ以前の期間に生成した電子署名に影響が及ばないようにする署名方式である。なお、公開される署名検証鍵は期間に依らず一定である。()



(株式会社 三菱総合研究所作成)

図 3-3 Forward Secure 署名

(3) Key-Insulated 署名¹⁴

Key-Insulated 署名は、Forward Secure 署名と同様に、期間ごとに署名生成鍵を更新することにより、署名生成鍵の漏洩により偽造署名作成可能な期間を狭める。Forward

¹³ Mihir Bellare and Sara K. Miner, "A Forward-Secure Digital Signature Scheme," Proceedings Of CRYPTO'99, LNCS 1666, Springer-Verlag, July 1999.

¹⁴ Yevgeniy Dodis, Janathan Katz, Shouhuai Xi, Moti Yung, "Key-Insulated Public Key Cryptosystem," Proc. Of Eurocrypt 2002, LNCS 2332, Springer-Verlag, pp.65—pp.82, 2002.

Secure 署名と異なるのは、古い署名生成鍵だけでなく、新しい署名生成鍵に関してもこの性質を実現したところである。

Key-Insulated 署名では、署名生成鍵がベース鍵とユーザ鍵からなっている。そして、あらかじめ決められた期間ごとに、ベース鍵とその期間の一つ前の期間のユーザ鍵から新たなユーザ鍵を生成する。これにより、ベース鍵が安全に保管されているのであれば、ある期間のユーザ鍵が漏洩したとしても、それ以降のユーザ鍵を生成することは困難となり、新たな署名生成鍵を用いて偽造署名を作成することはできなくなる。

(4) Intrusion Resilient 署名¹⁵

Intrusion Resilient 署名は、Key-Insulated 署名のアイデアにおけるユーザ鍵だけでなくベース鍵も更新することで、ベース鍵の保管に関するコストを低減する。

(5) 電子署名アリバイ実現機構¹⁶

電子署名アリバイ実現機構は、各署名生成者自身でも偽造困難な形で自身の署名生成履歴を安全に保管し、その署名生成履歴を使用して電子署名を生成することで、署名の偽造の有無を裁判所等の調停者に証明可能とする仕組みである。

本機構では、偽造された可能性のある電子署名付メッセージに関するデータが、署名生成履歴に含まれているか否かで、正当な電子署名付メッセージと偽造されたものとを区別できるようにする。つまり、たとえ同じ署名生成鍵を使っても生成された電子署名であっても、正当な署名生成者が有する署名生成履歴に含まれないものは偽造されたものだと判断できるようになっている。

本機構では、署名生成履歴への改ざん等が行われていないことを担保することが重要である。そのため、本機構では署名生成履歴をICカードなどの耐タンパー性を有するモジュール内に格納することとしている。さらに、ICカードなどの記憶容量の制限等も考慮し、署名生成履歴への改ざんを著しく困難にする方法として、ヒステリシス署名と履歴交差がある⁴。

- ヒステリシス署名

RSA 署名や DSA 署名のような従来の電子署名方式を構成要素の一部として利用する電子署名方式の一形態である。署名対象となるメッセージに電子署名を施す際に、それ以前の署名生成履歴などといったヒステリシス情報と署名対象のメッセージから、デジタル署名を生成する方式である。これにより、ヒステリシス情報が現

¹⁵ Gene Itkis and Leonid Reyzin, “SiBIR: Signer-Base Intrusion-Resilient Signatures,” Proc. Of CRYPTO 2002, pp.499—pp.514, LNCS 2442, Springer-Verlag, 2002.

¹⁶ 洲崎誠一、松本勉、“電子署名アリバイ実現機構 ヒステリシス署名と履歴交差、”情

在のデジタル署名データに反映され、正当なヒステリシス情報が反映されているデジタル署名データかどうかで、偽造の有無が検知可能となる。

- 履歴交差

ヒステリシス署名の署名能力を向上させるための方法である。二人以上のヒステリシス情報（の一部）を交換して、ヒステリシス署名を生成する。これにより、ある署名生成者の署名生成履歴が別の署名生成者の署名生成履歴に反映されることになる。

(6)ハードウェア確認タグ付署名¹⁷

ハードウェア確認タグ付署名は、当該署名を生成したモジュールを高い確率で判定可能とすることにより、署名生成鍵が漏洩したとしても、当該モジュールから生成された署名であるか否かを判定することができる。本方式では、当該署名を生成したモジュールを特定するために、耐クロン・モジュールを仮定する。耐クロン・モジュールとは、入出力の集合のサイズが非常に大きな関数であり、その入出力関係を再現する別のモジュールを構成することが困難なモジュールのことである。この耐クロン・モジュールの仮定により、モジュールが個別化される。

(7)Fail-stop署名¹⁸

Fail-stop 署名は、計算機能力の向上により、偽造署名を生成することが十分可能な状況になったとしても、高い確率で偽造署名を判定できる署名アルゴリズムである。これは、文書データとそれに対応する署名データの組から導出される署名生成鍵の候補が複数存在するに署名アルゴリズムを構成しておくことで、数多くの署名生成鍵の候補からあつて一つを利用して署名を偽造しても、本来の署名生成鍵と一致する確率が低いことにより実現される。

報処理学会論文誌、Vol.43 No.8、August 2002.

¹⁷ 松本 勉、田中 直樹、“計算の実行ハードウェアを確認する方法、” コンピュータセキュリティシンポジウム 2000 論文集、pp.199—pp.294、情報処理学会、2000 年。

¹⁸ Torben Pryds Pedersen, Birgit Pfitzmann, “Fail-stop Signatures,” SIAM Journal on Computing, Vol.2, pp.291—pp.330, 1997.

3.1.4. データ保管型

データ保管型の対策は、そもそもの文書データの原本を安全に保管しておき、問題発生時にその原本の文書データを利用するための対策である。基本的には、どのように安全に文書データを保管するが問題であり、それを実現する専用のシステムを構成することが対策の中心となる。

(1) セキュア・アーカイバ

セキュア・アーカイバは、デジタル署名等による文書データの改ざん検出、文書データのアクセス・コントロールや履歴管理等を行うための専用のハードウェアである。ハードウェア自体も耐タンパー性を有するように構成されており、文書データへの物理的なアクセスにも対応している¹⁹。これらのセキュア・アーカイバの機能のより、文書データの原本性が保たれる。

(2) 電子公証²⁰

電子公証制度は、信頼できるオーソリティが署名付文書データに署名を施すとともに、履歴を管理する制度である。オーソリティの署名と保管されている履歴から、その文書データの存在を証明し、事後に偽造判定や証拠に利用するものである。

¹⁹ “国内初、専用ハードウェアにて電子データの原本性を確保した電子保存装置「セキュアアーカイバ」新発売”、富士通株式会社、プレスリリース、2002年5月28日。

<http://pr.fujitsu.com/jp/news/2002/05/28-1.html>

²⁰ 法務省民事局、“公証制度に基礎をおく電子公証制度について”、

<http://www.moj.go.jp/MINJI/MINJI24/minji24.html>

3.2. 公的機関における検討の状況

ここでは、暗号技術の安全性に関する公的機関等の係り方について、米国および欧州における検討状況について述べる。米国については、個別の暗号方式の危殆化に関する対応の流れに着目し、米連邦政府の標準暗号に関する動向を述べる。欧州については、暗号方式全般に関する技術評価および利用推奨方策に注目し、EU における技術開発政策の動向を述べる。

3.2.1. 米国 NIST における検討の状況

米連邦政府調達に関する暗号技術の標準については、米国標準技術局 (National Institute of Standards and Technology, NIST) がメンテナンスを担当している。NIST には法令により連邦政府システムに関する情報セキュリティについて、強い権限が与えられている。また、各省庁のセンシティブな情報 (unclassified sensitive information) の保護には、原則として、NIST が示す連邦情報処理規格 (Federal Information Processing Standard, FIPS) が適用される。

暗号危殆化の対応について、NIST の取り組みを参考とする際には、NIST は法的裏付けをもつ米連邦政府標準を示す機関であることに注意が必要である。NIST には強い執行権限が与えられており、その決定の及ぼす影響力は大きい。つまり、日本や EU において政府系主導で進められる暗号技術評価プロジェクトのアウトプットと、米連邦により進められる FIPS とは基本的性格が大きく異なると言える。

FIPS に示された標準暗号については、事前に安全性のマージンを考慮した上で策定され、一定期間ごとに見直しが行われる。新たな攻撃技術の公表やアルゴリズムの弱点が発見された時点でも NIST が見直しを行う旨が表明されている。

以下に FIPS に示された標準暗号である DES、AES および SHA-1 について述べる。

(1) DES

FIPS46 Data Encryption Standard (DES) は米国連邦政府におけるセンシティブ情報を保護するための標準暗号として、1977 年 1 月に発行された。

DES 標準には当初より 5 年ごとの見直しが規定されている。1993 年の 3 回目の見直し以後は、パブリックコメントで学界、産業界、政府機関等に意見を求め、その時点の安全性、リスク、改定に伴う影響について NIST 内部で検討が行われた。

DES は、その安全性の低下が現実的な脅威となった 1990 年代より、標準取り下げを睨んだアナウンスや標準改定が慎重かつ段階的に進められ、ほぼ終局に近づきつつある。

DES の取り下げに至るプロセスは、暗号危殆化の対応の具体的事例であり、わが国における危殆化対応の検討に際して参考とすべき点は多い。

下表に標準暗号としての DES の経緯を解読技術等の変遷と併せて示す。

表 3-3 DES に関する主な経緯

		背景	政府 (NIST) における対応
1977 年	1 月		FIPS46 発行。DES が政府調達基準に示された標準暗号となる。
1983 年			FIPS46 を再承認。
1987 年	3 月		FIPS46 の 2 度目の見直しに関してパブリックコメントを募集。
1988 年	1 月		FIPS46-1 発行。字句の誤りを正す以外に本質的な改定は無かった。
1990 年		差分攻撃に関する研究論文が発表される ²¹ 。(DESのS-BOXは差分攻撃を考慮して設計されていたがこのことは後年DESが事実上解読可能となるまで伏せられていた)	
1992 年			FIPS46-1 の見直しに関してパブリックコメントを募集。
1993 年		線形攻撃法に関する研究論文が発表される ²² 。	
	12 月		FIPS46-2 発行。政府標準暗号としての DES の承認期間を FIPS46-2 の期限となる 1998 年までと決定した。(実際には承認期間は延長され 2004 年に廃止の方針が示された)
1994 年		線形解読法によるDESの解読に成功 ²³	
	2 月		FIPS185 (EES) 発行 ²⁴ 。NSAが開発したSkipjackアルゴリズムが用いられた。
1996 年			Skipjackの仕様を公開 ²⁵ (米政府はEESの導入を事実上断念)

²¹ Biham, Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, Vol. 4 No. 1, pp. 3-72, 1991. (The extended abstract appeared at CRYPTO'90)

²² Matsui, "Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology EUROCRYPT'93, LNCS 765, Springer-Verlag, 1993.

²³ Matsui, "The first experimental cryptanalysis of the Data Encryption Standard," Advances in Cryptology CRYPTO'94, LNCS 839, Springer-Verlag, 1994.

²⁴ NIST, "Escrowed Encryption Standard (EES)," FIPS PUB 185, <http://csrc.nist.gov/publications/fips/fips185/fips185.txt>

²⁵ NIST, "SKIPJACK and KEA Algorithms," <http://csrc.nist.gov/CryptoToolkit/skipjack/skipjack.pdf>

		背景	政府 (NIST) における対応
1997 年	1 月	DES Challenge I 開催 (~7 月) 。米 RSA 社が主催した。このコンテストは全数探索法で鍵を探し解読を行うもの。distributed.net プロジェクトがインターネットに接続された約 1 万台の PC を利用した分散コンピューティングにより、140 日間で解読に成功。	AES プロジェクトを開始 ²⁶ 。NIST は DES に代わる次世代の標準暗号アルゴリズムを選定する計画を宣言した。AES への移行期間中は Triple-DES の使用を促すとした。
	9 月		AES 候補の受付開始 (1998 年 6 月に締め切り)
1998 年	1 月	DES Challenge II-1 開催 (~2 月) 。distributed.net プロジェクト ²⁷ が約 4 万台相当の PC により、39 日間で解読に成功。	
	7 月	DES Challenge II-2 開催。Electronic Frontier Foundation が解読専用ハードウェア DES Cracker ^{28,29} を用いて、56 時間で解読に成功。	
1999 年	1 月	DES Challenge III 開催 ³⁰ 。distributed.net と EFF が協力し、22 時間 15 分で解読に成功。	
	8 月		AES 最終候補発表
	10 月		FIPS46-3 を発行 ³¹ 。以後は原則として、新規に調達するシステムにはトリプル DES あるいは AES を使い、シングル DES は政府の旧来のシステムにおいてのみ利用するものとした。
2000 年	10 月		Rijndael を AES Winner として選定
2001 年	11 月		FIPS197 として AES を発行 ³² 。

²⁶ NIST, "Advanced Encryption Standard (AES) Development Effort,"

<http://csrc.nist.gov/CryptoToolkit/aes/index2.html>

²⁷ distributed.net, "Project DES," <http://www.distributed.net/des/>

²⁸ Electronic Frontier Foundation, "EFF: DES Cracker Project,"

http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/

²⁹ Electronic Frontier Foundation, "Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design," <http://cryptome.org/cracking-des.htm>

<http://www.genpaku.org/crackdes/cracking-desj.html> (in Japanese)

³⁰ RSA Security, "DES Challenge III," <http://www.rsasecurity.com/rsalabs/node.asp?id=2108>

³¹ NIST, "Data Encryption Standard (DES); specifies the use of Triple DES," FIPS PUB 46-3,

<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>

³² NIST, "Advanced Encryption Standard (AES)," FIPS PUB 197,

<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

		背景	政府（NIST）における対応
2004年	5月		SP800-67を発行 ³³ 。暗号化標準としてトリプルDESおよびAESを定めた。承認期限を2030年、AESへの段階的移行を行うものとした。シングルDESに関する廃止の方向性を言及した。
2004年	7月		NISTはシングルDESを暗号化標準として不適当とし、FIPS46-3を廃止して政府での利用を止める方針を示しコメントを募集した ³⁴ 。方針によれば、SP800-67に示すように政府におけるトリプルDESの利用は引き続き認めるものの、AESへの移行を推奨している。
2004年	10月		NISTはFIPS140-1およびFIPS140-2に関するパブリックコメントを募集開始した。この中でFIPS46-2取り下げ後2年間の移行期間の後はDES実装モジュールを非公認とする姿勢を示した。

（株式会社 三菱総合研究所 作成）

標準暗号としてのDESに関して、特に見直しと取り下げに係る経緯の詳細を以下に示す。

(a)DESの発行から1度目のレビューまで（1977年～1983年）

1977年1月にFIPS46 Data Encryption Standard (DES)は米国連邦政府の標準規格としてNISTの前身である米国標準局(National Bureau of Standards, NBS)により発行された。

1982年、米国安全保障局(National Security Agency, NSA)は政府DES機器認定プログラム(Government Endorsed DES Equipment Program)を設立した。これはDESが当初より意図していたハードウェア実装についてDES準拠ハードウェア製品の評価および認定をNSAに一本化するものであった。このプログラムにおいて認定されたDES製品の購入者には暗号鍵がNSAから交付された。

1983年、DESは特に変更されることなくNBSにより再承認された。

³³ NIST, "SP 800-67 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," <http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf>

³⁴ http://www.nist.gov/public_affairs/techbeat/tb2004_0730.htm

(b)2 度目のレビュー (1984 年 ~ 1988 年)

1984 年、大統領令 NSDD-145 に基づきコンピュータセキュリティに関する管理が NBS から NSA に移され、NSA は暗号に関する問題について NBS に対する拒否権を持つこととなった。

1986 年、NSA は次のレビュー(1988 年)に DES を承認すべきでないとの勧告を行い、NSA がこれまで行ってきた DES 準拠製品の評価認定も取りやめる旨を表明した(ただし既に認定済みの製品については販売を許可し、認定リストへの掲載、暗号鍵の交付については継続するとの意向を示した)。

NSA は DES に代わる暗号として商用 COMSEC 認定プログラム (Commercial COMSEC Endorsement Program, CCEP) を提案した。これは NSA が設計した非公開のアルゴリズムを実装する耐タンパー化 VLSI チップにより暗号機能を提供するシステムであった。

1987 年、NBS は NSA の発表を受けて 3 月 6 日の官報で FIPS46 の 2 度目の見直しにあたって、検討すべき方策案を 3 つ挙げてパブリックコメント募集を行った。

以下に 1987 年の意見募集の一部を示す。

概要 (一部):

連邦情報処理標準 (FIPS) 46 データ暗号化規格 (1977 年公表) は、電子ハードウェアデバイスに実装され、計算機データの暗号的な保護のために使われるアルゴリズムを提供するものである。同標準は、その妥当性を評価するため、5 年以内で見直されると規定していた。

最初の見直しは 1983 年に行われ、同標準は連邦政府における利用が再承認された (1983 年 9 月 13 日付 48FR41062)。

本通知は、コンピュータデータを守るための標準の継続的な妥当性評価のための 2 回目のレビュー実施を発表するためのものである。

産業界および一般からのコメントは FIPS46-1 に関する次の選択肢に関して要請される。これらの選択肢についてコスト (影響) および利点がコメントに含められることが望ましい。

- ・同標準の更なる 5 年間の再承認。この場合、米国標準局は同標準を実装するデバイスの妥当性を検証し続けうる。FIPS 46 が非機密扱いのコンピュータデータを認可されていない改ざんや露呈から保護するための認定された手法であり続けうる。

- ・同標準の撤回。この場合、米国標準局は以後同標準をサポートしない。各組織は既存の同標準を実装するデバイスを利用し続け得る。また、非政府組織は、望むならば新たな実装を行うことができる。政府組織は国家安全保証局 (NSA) による商用 COMSEC 認定プログラム (CCEP) に基づく新たなセキュリティデバイスの利用を始めることとなる。

- ・同標準の適用範囲の見直し。本標準の適用範囲に関する記述は、電子資金決済を保護するための同標準の使用といった、特定用途の指定に変更されうる。このレビューにお

いては、同アルゴリズムの技術的な変更は考慮の対象ではない。

連邦政府機関、米国銀行業者協会 等より 33 件の回答が寄せられたが、うち 31 組織が DES の再承認を支持した。当時、再承認が支持された主な理由を以下にまとめる。

- ・ DES は非常に広範な製品およびアプリケーションにおいて利用されており、廃止や変更がなされた場合に相当の混乱が予想される。
- ・ DES の代替として容認されうるアルゴリズムが存在しない。
- ・ 既存の DES 準拠製品の将来が危ぶまれる。
- ・ 全く新たな暗号技術が採用された場合、現在のアプリケーションに複雑な機能を追加する必要が生じる可能性がある。
- ・ 製品利用者はベンダによるサポートの続行を望んでいる。
- ・ 廃止あるいは変更を行った場合、安全性に関する疑念が製品利用者には生じかねない。

新たな暗号アルゴリズムとして NSA の技術を用いることについては、以下のような理由から反対意見があった。

- ・ ベンダは今後新たな暗号技術を手に入できなくなる恐れがある。
- ・ NSA が暗号文を解読可能な立場となる。
- ・ DES 準拠製品よりも厳しい輸出規制が課せられる。

NSA は金融業界との徹底的な討論の末、金融データの標準暗号としての DES の利用を無期限に承認する旨を公表し、DES に替わる新暗号方式への移行が可能となるまでは DES 機器に関する財務省認定を支持することを示す覚書を財務省との間に交わした。

1988 年、DES は FIPS46-1 として 92 年までの期限付きで再承認された。NSA は政府 DES 機器認定計画の撤廃を決め、以後の DES 製品の認定は米財務省が行うこととなった。

(c)3 度目のレビュー（1989 年～1993 年）

1992 年、NIST は官報で FIPS46-1 の再承認についての意見募集を行った。ここでも NIST は 3 つの方向性（再承認、規格取り下げ、適用範囲 / 条文の変更）について、それぞれのコスト（インパクト）とメリットに関する意見の提示を公に求めた。

以下に 92 年の意見募集の一部を示す。

概要（一部）：

連邦情報処理標準（FIPS）46 データ暗号化規格（1977 年公表）は、電子ハードウェアデバイスに実装され、計算機データの暗号的な保護のために使われるアルゴリズムを提供するものである。同標準はその妥当性を評価するため 5 年以内で見直されると規定していた。

最初の見直しは 1983 年に行われ、同標準は連邦政府における利用が再承認された（1983 年 9 月 13 日付 48FR41062）。2 回目の見直しは 1987 年に行われ、同標準は連邦政府における利用が再承認された。（52FR7006）

本通知はコンピュータデータを守るための標準の継続的な妥当性評価のレビュー実施を発表するためのものである。

産業界および一般からのコメントは FIPS46-1 に関する次の選択肢に関して要請される。これらの選択肢についてコスト（影響）および利点がコメントに含まれることが望ましい。

- ・同標準の更なる 5 年間の再承認。この場合、NIST は同標準を実装するデバイスの妥当性を検証し続けうる。FIPS46-1 が非機密扱いのコンピュータデータを保護する唯一の認定された手法であり続けうる。

- ・同標準の撤回。この場合、NIST は以後同標準をサポートしない。各組織は既存の同標準を実装するデバイスを利用し続け得る。他の複数の標準が DES の代替として NIST により公表されうる。

- ・同標準の適用範囲および / または実装の記述の見直し。このような修正は、同標準を変更し、ハードウェアと同様にソフトウェアで DES の実装の使用を許すこと、特定のアプリケーションで DES の反復的な使用を許すこと、あるいは、NIST により認められ登録される代替アルゴリズムの使用を許すことが含まれうる。

1993 年、NIST は FIPS 46-2 を発行した。集められたコメントに基づいて、5 年間の承認期間の再延長と、今後代替アルゴリズムを検討する旨が盛り込まれた。

以下に FIPS46-2 の 15 節「制限」および 19 節「特記事項」より DES の期限に関する部分の抜粋（和訳）を示す。

15. 制限（一部）

NIST は、通信のセキュリティに関し責任を有する行政機関の技術的支援を受け、本標準で指定されるアルゴリズムが関連づけられたデバイスの標準的ライフサイクルを越える期間にわたって高レベルの保護を提供するものと判断した。潜在的な新たな脅威に対し本アルゴリズムにより提供される保護については、その妥当性を評価するために 5 年以内に見直しが行われる（特記事項の節を参照のこと）。加えて、本標準および本標準の利用により提供されるセキュリティを低下させる潜在的脅威については、NIST および問題を認識している他の複数の連邦機関により継続的なレビューが行われる。その時点で利用可能な新技術については本標準に対する影響を判断するために評価される。さらに、技術のブレイクスルーあるいはアルゴリズムの数学的な弱点について認識した場合には、NIST は本標準を再評価し、必要な修正を行う。

次の見直し（1998 年）においては、本標準で指定されたアルゴリズムは開発されて 20 年以上となる。NIST はより高レベルのセキュリティを提供する複数の代案を考慮する。これらの代案の 1 つが 1998 年の見直し時に代替標準として提案されうる。

（中略）

19. 特記事項

本標準の制限の節に示すように、本標準のレビューは 1977 年の採用以後 5 年ごとに行われている。本標準はそれらのレビューごとに再承認されている。

この標準の本文に関する今回の改訂は、本アルゴリズムへのソフトウェア実装を許す変更、また、他の FIPS により承認された暗号アルゴリズムの使用を妨げないことを含む。

(d) 4 度目のレビュー (1994 年 ~ 1999 年)

1990 年代前半に有効な暗号解読手法が発表され、1994 年には DES の解読に実際に成功した事例が公表された。この時期に、DES の安全性については実世界における脅威が現実的なものとなったと言える。

1997 年に AES プロジェクトが開始され、NIST は DES に代わる次世代の標準暗号アルゴリズムを選定する計画を宣言した³⁵。NIST は、AES への移行期間中は Triple-DES の使用を促すとした。

1999 年に FIPS 46-3 が発行された³⁶。この改訂において、以後は原則として連邦政府が新規に調達するシステムにはトリプル DES あるいは AES を用いることが明記され、シングル DES は政府の旧来のシステムにおいてのみ利用するものとされた。

(e) 5 度目のレビュー以後 (2000 年 ~ 2004 年)

FIPS 46-3 の発行以後は、連邦政府においては、シングル DES は旧来のシステムにおいてのみ利用され、新たなシステムにはトリプル DES あるいは AES を用いることとなった。

2001 年に FIPS 197 として AES が発行された³⁷。

2004 年 5 月に SP 800-67 が発行された³⁸。この中で標準暗号としてトリプル DES および AES を定めた。この標準では期限を 2030 年と設定して AES への段階的移行を行うことを示している。また、シングル DES に関する廃止の方向性について明確に言及している。

2004 年 7 月に NIST は DES (シングル DES) を政府標準暗号から取り下げを提案した。また、取り下げに関するパブリックコメントを受け付けた³⁹。この募集は同年 9 月に締め切られた。2005 年 2 月現在のところコメントへの返答は公開されておらず、NIST からの次のアクションは示されていない。

2004 年 10 月に NIST は FIPS 140-1 および FIPS 140-2 に示される暗号モジュール評価プログラム (Cryptographic Module Validation Program, CMVP) に関して、パブリックコ

³⁵ NIST, Advanced Encryption Standard (AES) Development Effort,"

<http://csrc.nist.gov/CryptoToolkit/aes/index2.html>

³⁶ NIST, "Data Encryption Standard (DES); specifies the use of Triple DES," FIPS PUB 46-3,

<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>

³⁷ NIST, "Advanced Encryption Standard (AES)," FIPS PUB 197,

<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

³⁸ NIST, "SP 800-67 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," <http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf>

³⁹ http://www.nist.gov/public_affairs/techbeat/tb2004_0730.htm

メントを開始した⁴⁰。ここでNISTは政府において現在利用されるDES 実装の暗号モジュールを、代替の暗号モジュールに移行するための計画を示し、意見を求めた。

以下に同文書に示された DES 実装製品の扱いに関する案の概要を示す。

- 1 . 連邦政府機関は、FIPS140-1 または FIPS140-2 において評価認定済みの暗号モジュールについては、2 年間の間は NIST の認定のもとで利用し続けることができる。この期間を AES あるいは Triple DES への移行期間とする。
 - (ア) FIPS140-1 または FIPS140-2 の DES を実装する暗号モジュールに与えられる認定は、移行期間内に限定されたものに変更される。
 - (イ) 移行期間内は DES を実装する暗号モジュールに対して移行期間内限りの期限付き適合認定書を発行する。
- 2 . この2年間の移行期間を過ぎた後
 - (ア) DES を FIPS140-2 の添付書類から削除する。
 - (イ) FIPS140-1 または FIPS140-2 において、DES を非公認レベルに引き下げる。FIPS140-1 または FIPS140-2 の評価を受けた DES のみを実装する暗号モジュールに関しては、FIPS140-1 または FIPS140-2 の要件に適合せず連邦機関において使用しないことが記載されている場合のみ、認定済みモジュールのリストへの記載を認める。
 - (ウ) この移行処置は、DES MAC のようなシングル DES を含む他の機能についても該当する。

仮にこの案に示されたように FIPS46-3 の取り下げプロセスが進められた場合、FIPS46-3 の廃止が公表された時点より 2 年間は代替暗号への移行期間となる。移行期間の後には連邦政府において DES が実装された製品は標準に準拠していないものとなる。

(f) 現在

2005 年 2 月時点では、標準暗号としての DES の取り下げの具体的日程に関しては公表されていないが、検討が依然続けられている模様である。シングル DES は、米連邦政府のシステムには適切ではないものと見なされており、新規システムに採用もできないが、依然として政府標準暗号ではある。

もし NIST が FIPS46-3 を取り下げた場合でも、取り下げ以後の一定の移行期間は、公認暗号としての位置づけを残す可能性がある。NIST は、この移行期間中に代替暗号を用いたシステムへの改修・更新が進むことを期待している。しかし、移行期間後でも更新されないシステム等で DES を実装したモジュールが一部残る可能性がある。

FIPS46-3 はトリプル DES (TDEA) に関する標準でもある。FIPS46-3 が取り下げら

⁴⁰ Department of Commerce, National Institute of Standards and Technologies, “Announcing Development of Federal Information Processing Standards(FIPS) 140-3, a revision of FIPS140-2, Security Requirement for Cryptographic Modules”, <http://csrc.nist.gov/cryptval/notices.htm>

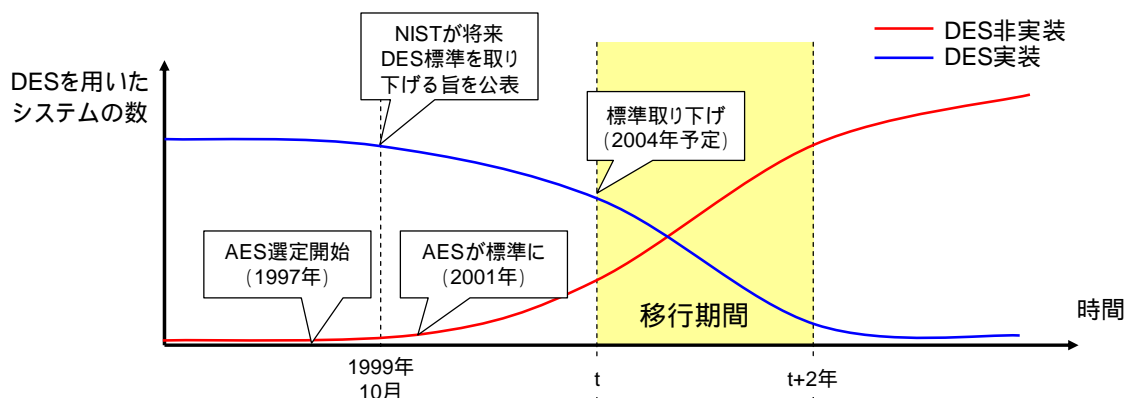
れた場合でも、トリプル DES は SP800-67 に示されているため今後の連邦政府における使用が認められる。ただし、NIST は、トリプル DES に比べ処理が高速で高い強度をもつ AES の使用を推奨している。

DES は、政府標準暗号としてのお墨付きを持つフリーな暗号として多数の民間規格においても採用されている。連邦政府がこれを標準から取り下げた場合には、影響範囲は極めて広く大きい。取り下げに関しては、NIST には政府のみならず民間における影響も考慮が求められている。

(g) 分析

図 3-4 に NIST における DES の段階的な標準取り下げと AES への移行に関するプロセスを示す。

米連邦政府におけるDESの廃棄プロセス



連邦政府 における 利用	通常の利用	旧来のシステムで 利用	旧来のシステムで 利用	システム更新により 順次利用終了
	新規調達	通常の新規調達	新規調達停止	
	モジュール 認定	認定	条件付認定	非公認 アルゴリズム扱い

(グラフはNISTの示す計画より推察される意図をイメージ化したもの)

(株式会社 三菱総合研究所作成)

図 3-4 NIST の進める DES 廃棄プロセス

NIST が行った次のようなアクションや施策は、わが国における危殆化対応においても参考となる所が大きい。

- ・ **幅広い意見収集。** 以下のような複数の視点に基づく意見が得られる。
 - 暗号の強度に関する専門家の意見
 - 暗号が実装されるシステムの関係者、運用者、利用者、開発者（ベンダ）の意見
 - 政府が認める暗号（お墨付きの暗号）であることに基づいて民間規格等に活用している業界等の意見 等

NIST は毎回の見直しを行う際にこれらの意見を積極的に収集している。収集された情報は危殆化の対応に関する意思決定、決定を行った場合の影響範囲の把握想定、対策スケジュールの策定等に活用していると推測される。

- ・ **定期的な標準暗号見直しの設定。** DES に関しては適用システムのライフサイクルに合わせ 5 年間の有効期限を設けて見直しの可能性を明示している。これは、将来の危殆化を前提に標準暗号を参照・利用するよう促す効果がある。十分な時間をかけた代替暗号アルゴリズムへの段階的な移行を推進する際には、計画の策定と実施が容易になる。
- ・ **代替暗号への移行のマージン設定。** AES については 5 年をかけて選定を行い、DES を標準暗号から取り下げる以前の移行方策として Triple-DES および AES の新規システムへの適用を促している。このマージンについては、AES の周知、旧来のシステムにおける DES 適用箇所の洗い出し、開発側における AES 実装環境の成熟、DES から AES への置換作業 等に要する時間やコストが考慮されているものと想定される。さらに、DES 取り下げ後も一定のシステム移行期間を設けるなどの配慮を行っている。

また、DES に関する危殆化の進行度について NIST より提示される情報は殆ど無いが、これまでの経緯からは、専門家による暗号強度に関する技術的な評価が対応推進の方針のベースとなり、これに標準暗号としての利用状況や様々な影響が考慮されて、対応策が作られていることが伺える。

(2) AES

前項でも述べたように、AES は DES に代わる暗号として、1997 年より選定プロジェクトが開始され、2001 年に FIPS 197 として政府標準暗号となった。

AES については選考時に 128 / 192 / 256 ビットの異なる 3 つの鍵長に対応することが要件とされた。これは計算機能力の向上により 128 ビットの鍵の安全性がいずれ脅かされる事態を想定して十分な安全性マージンを取るためであった。現在のところ、NIST は AES を 2030 年まで標準暗号とし続ける見通しを示している。

ここでは、代替暗号に関する制度面のポリシーについて注目することとし、危殆化に備え複数の代替暗号アルゴリズムを準備、実装する方針の検討等の参考となる情報として、複数候補選定の検討について述べる。AES 選定の際の技術的要件については、既存の文書で深く取り上げられているためここでは触れない。

AES 選定の過程においては、選定方針に関する議論の中で、最終的に選定する候補数について議論が行われた⁴¹。これは、暗号アルゴリズムの危殆化に備えた代替アルゴリズムに関する考察において参考とするべき点を含む。以下に詳細を説明する。

AES の最終候補として選定するアルゴリズムの個数については、募集段階では、1 つのアルゴリズムを最終候補とするが、それらと比較して著しい特長をもつ候補があれば、複数のアルゴリズムを選ぶこともあり得る、とアナウンスされていた。

候補数については、5 つの finalist を選出したラウンド 1 の時点では大きな議論とはならなかったものの、最終候補を選定するラウンド 2 においては単一選定、複数選定のいずれをとるかについて多数の意見が出された。これらは次のような複数の観点に基づくものであった。

まず、複数選定の支持意見の論拠を以下にあげる。

- ・ 知的財産権に関するリスク：選定したアルゴリズムやその実装については、後に他者から知的財産権について主張が成される可能性がある。複数選定しておけば、そのうちの 1 つについて知的財産権上の主張が成され、使用が困難な状況になっても他の選定アルゴリズムで対処できる。
- ・ 柔軟性：AES は広い範囲で使われる。すなわち、様々な環境の上で様々な要求仕様の下に実装され、使用されることを前提としている。単一のアルゴリズムでこれを

⁴¹ The Third Advanced Encryption Standard (AES) Candidate Conference
Don Johnson, “AES and Future Resiliency: More Thoughts And Questions”
<http://csrc.nist.gov/encryption/aes/round2/conf3/papers/02-djohnson.pdf>
<http://csrc.nist.gov/encryption/aes/round2/conf3/presentations/johnson.pdf>
Ian Harvey, “The Effects of Multiple Algorithms in the Advanced Encryption Standard”
<http://csrc.nist.gov/encryption/aes/round2/conf3/papers/06-iharvey.pdf>
<http://csrc.nist.gov/encryption/aes/round2/conf3/presentations/harvey.pdf>

満たすことは困難であるので、複数を選定しておくべきである。

- ・ 安全性：複数のアルゴリズムを選定しておけば、そのうちの 1 つのアルゴリズムについて安全性に問題が生じて、他の選定アルゴリズムで対処できる。

これに対し、単一選定の支持意見の論拠を以下にあげる。

- ・ 知的財産権に関するリスク：複数のアルゴリズムを選定して、それらが実装されることは、逆に知的財産権上の問題が発生するリスクが増す。
- ・ 柔軟性：特殊な条件下で実装され使用される暗号としては、既に FIPS において幾つかの暗号が制定されている。今回単一選定される AES は高い柔軟性を持っており、AES と既に FIPS で制定されている暗号で、十分に広い範囲をカバーできる。
- ・ 安全性：今回の選定においては安全性が十分に考慮されている。複数選定することは、選定されたアルゴリズムの安全性について NIST に対する信任に疑問を抱かせる結果になりかねない。
- ・ 実装コスト：複数のアルゴリズムを選定すると、それらの間で相互運用性を確保するための実装コストが増大してしまう。また、単一のアルゴリズムを選定した方がハードウェア実装の性能向上を促し易い。

最終的な NIST の公式見解は、以下を考慮した総合的な判断を踏まえ単一選定であった。

- ・ 柔軟性：トリプル DES や他に民間において開発された暗号アルゴリズムの発展が今後予想されるため、単一選定で問題はない。
- ・ 安全性：単一選定されたアルゴリズムにおいて、鍵長の拡大が可能ならば、安全性の観点からも単一選定で問題はない。
- ・ 実装コストおよび知的財産権上のリスク：複数選定にした場合にベンダにかかる負担およびリスクが高い。

単一のアルゴリズムを選定した背景については次のようなことも言える。

- ・ 第 3 回 AES Conference において NIST は出席者に単一選定が良いか複数選定がよいかのアンケートを取った。単一選定が良いとする者が大多数（145 人中 110 人）であったため、NIST による決定に影響を与えた可能性がある。
- ・ 候補に Rijndael という優れたアルゴリズムが含まれていたため、結果として Rijndael のみを選定すれば大きな問題は起きないと予想された。つまり、単一選定か複数選定かを決めてから Rijndael を選出したのではなく、Rijndael があったから 1 つのみの候補選定となった側面がある。
- ・ 十分な選考過程を経た最終候補については、実際に適用可能でかつ決定的な解読手法が唐突に発表されることは稀であり、解読法のアイデアや部分的な弱点が発表され始めてから実用レベルでの解読が実現するまでには年単位のタイムラグが存在し、

単一選定したアルゴリズムについて安全性の問題が発生しても対処は可能との意見があった。

また、単一選定のアルゴリズムの他にバックアップアルゴリズムを選ぶべきという意見もあったが、これは実質的に複数のアルゴリズムを選出することとなり、複数選定の欠点を伴うため採用されなかった。

(3)SHA-1

2004年にはハッシュ関数に関する新たな攻撃手法が相次いで公表され、NISTはこれに応じる形で2010年までにSHA-1を取り下げる見通しを含むコメントを示した。SHA-1の段階的な取り下げプロセスは、2005年現在も進行中であるが、急速に進行する危殆化の事例とみなすことができる。

2005年2月にSHA-1の衝突発見に関する研究成果についての速報がWebニュース等を通じて報じられた。RSA Conferenceに参加した専門家の中で概要が出回ったことに端を発するものであった。現時点では攻撃の詳細は不明ではあるが存在が伝えられている状況で、詳細公表後の専門家による確認が待たれている。

暗号技術分野において定評がある研究者チームによる研究成果であることを受けて、NISTは詳細情報の公表以前に短いコメントを発表した。この中でNISTは、調査結果が未確認であることを前置きしつつ、流布している研究概要から判断可能な限りでは、実際のシステムへの現実的な攻撃は依然として困難である見込みを示し、攻撃について全詳細が公開された際には追加の情報の発表を行う予定を示した。

これに先立つ2004年8月に開かれた国際学会CRYPTO 2004においては、MD5、SHA-0に衝突が発見された旨の報告が行われた。上の研究との関連は不明である。

既にNISTは、2004年8月にSHA-0に対する攻撃手法が公表されたことを受け、計算力の進歩を背景要因として、より大きなビット数に対応するハッシュ関数（SHA-224、SHA-256、SHA-384、SHA-512）の使用を推進し、SHA-1およびそれと同程度の強度を持つアルゴリズムを2010年までに廃止するとの計画を示した。また、新規開発については、上に示したハッシュ関数を使うことを推奨すると共に、特に政府機関においては、作業の優先順位付けの際にシステムの機密性確保を考慮に入れ、より大きなハッシュ関数に整然と移行するよう時宜に適った根拠に基づく計画を策定することを勧めている。

NISTによるSHAに関する移行の経緯について表3-4に示す。

表 3-4 SHA に関する主な経緯

		背景	政府 (NIST) における対応
1993 年	5 月		FIPS 180 Secure Hash Standard 発行 ⁴² (SHA-0)
1995 年	4 月		FIPS 180-1 発行 ⁴³ (SHA-1)。SHA-0 の欠陥を修正した別のアルゴリズム
1998 年		CRYPTO98 においてSHA-0 に関して衝突をより低い計算量で発見可能な攻撃が発表される ⁴⁴	
2001 年			FIPS180-2 ドラフト公開。SHA-256, SHA-384, SHA-512 が発表される。
2002 年	8 月		FIPS180-2 発行 ⁴⁵ (SHA-1, SHA-256, SHA-384, SHA-512)
2004 年	2 月		FIPS180-2 にSHA-224 を追記 ⁴⁶ (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)。SHA-224 は 2-Key Triple-DESの鍵長との互換性を考慮したアルゴリズム。
2004 年	8 月	CRYPTO2004 においてSHA-0 の衝突発見が発表される ⁴⁷	NISTは今後 10 年でSHA-1 を段階的に廃し、SHA-224/256/384/512 に移行する計画を示した ⁴⁸
2005 年	2 月	SHA-1 の衝突を発見可能な攻撃の概要が提示される ⁴⁹	NISTは左の攻撃に関する詳細情報を入手後に再度アナウンスを行う旨を示すと共に、8 月に示した対応プロセス案を再提示した ⁵⁰

(株式会社 三菱総合研究所 作成)

⁴² National Institute of Standards and Technology, NIST FIPS PUB 180, "Secure Hash Standard," U.S. Department of Commerce, May 1993

⁴³ National Institute of Standards and Technology, NIST FIPS PUB 180-1, "Secure Hash Standard," U.S. Department of Commerce, April 1995

⁴⁴ Florent Chabaud, Antoine Joux, "Differential Collisions in SHA-0," Advances in Cryptology - CRYPTO'98, August 1998.

⁴⁵ National Institute of Standards and Technology, NIST FIPS PUB 180-2, "Secure Hash Standard," U.S. Department of Commerce, August 2002

⁴⁶ National Institute of Standards and Technology, NIST FIPS PUB 180-2, "Secure Hash Standard," U.S. Department of Commerce, February 2004

<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf>

⁴⁷ 発表はランブセッションで行われた。基となった論文はWeb公開されている。

<http://eprint.iacr.org/2004/199>

⁴⁸ NIST Brief Comments on Recent Cryptanalytic Attacks on Secure Hashing Functions and the Continued Security Provided by SHA-1

<http://csrc.nist.gov/NIST%20Brief%20Comments%20on%20Hash%20Standards%208-25-2004.pdf>

⁴⁹ Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu, "Collision Search Attacks on SHA1", February 13, 2005 <http://theory.csail.mit.edu/~yiqun/shanote.pdf>

⁵⁰ NIST Brief Comments on Recent Cryptanalytic Attacks on SHA-1

<http://csrc.nist.gov/news-highlights/NIST-Brief-Comments-on-SHA1-attack.pdf>

3.2.2. 欧州における検討の状況

EU においては情報技術に関する研究開発政策がフレームワークプロジェクト(以下 FP と示す)を中心に進められている。以下に FP の暗号危殆化に関連するプロジェクトにおける検討の状況を示す。

(1)NESSIE⁵¹

NESSIE (New European Schemes for Signature, Integrity, and Encryption) は FP5 の IT 分野のプログラムである IST の一環として 2000 年 1 月より開始された 3 ヶ年計画のプロジェクトである。NESSIE プロジェクトは、さまざまな暗号技術に関するプリミティブを評価して、産学のコンセンサスの下に欧州における暗号プリミティブの推奨リストの作成を主目的として進められた。この目的の実現のため、暗号方式の公募の実施、透明性の高いオープンなプロセスでの評価が行われ、その結果として、多様なプラットフォーム向けに高い強度を持つ暗号方式のポートフォリオが策定された。

NESSIE プロジェクトの開始時に示された要件を表 3-5 に示す。

表 3-5 NESSIE公募時の各暗号プリミティブに関する要件⁵²

	Type of Primitives	Security Requirements for Each Primitive
1	Block Ciphers	a) High. Key length of at least 256 bits. Block length at least 128 bits b) Normal. Key length of at least 128 bits. Block length at least 128 bits. c) Normal-Legacy. Key length of at least 128 bits. Block length 64 bits
2	Synchronous stream ciphers	a) High. Key length of at least 256 bits. Internal memory of at least 256 bits. b) Normal. Key length of at least 128 bits. Internal memory of at least 128 bits.
3	Self-synchronizing stream ciphers	a) High. Key length of at least 256 bits. Internal memory of at least 256 bits. b) Normal. Key length of at least 128 bits. Internal memory of at least 128 bits.
4	Message Authentication Codes (MACs)	The primitive should support all output lengths (in multiples of 32 bits) up to the key length (inclusive). a) High. Key length of at least 256 bits. b) Normal. Key length of at least 128 bits.
5	Collision-resistant hash functions	a) High. Output length of at least 512 bits. b) Normal. Output length of at least 256 bits.

⁵¹ NESSIE <https://www.cosic.esat.kuleuven.be/nessie/index.html>

⁵² NESSIE, “The NESSIE Call for Cryptographic Primitives,” March 8, 2000, <https://www.cosic.esat.kuleuven.be/nessie/call/>

6	One-way hash functions	These hash functions shall be preimage resistant and second preimage resistant. a) High. Output length of at least 256 bits. b) Normal. Output length of at least 128 bits.
7	Families of pseudo-random functions	Fixed block length of at least 128 bits. a) High. Key length of at least 256 bits. b) Normal. Key length of at least 128 bits.
8	Asymmetric encryption schemes	The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions.
9	Asymmetric digital signature schemes	The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions.
10	Asymmetric identification schemes	The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions. The probability of impersonation should be smaller than 2^{-32} .

(The NESSIE Call for Cryptographic Primitives を基に作成)

NESSIE の選定基準は、長期間にわたる安全性、市場の要求、効率性（性能）と柔軟性である。より具体的には以下のようにアナウンスされている。

- ・ 安全性：もっとも重要な基準とされる。これは暗号プリミティブの安全性は信頼性とコンセンサスを得るために必須と考えられるためである。この評価プロセスはプロジェクト外部における進歩（たとえば新たな攻撃手法や評価手法等）に影響される。
- ・ 市場の要求：2 番目に重要な評価項目。プリミティブの必要性、可用性、世界的な利用の可能性である。
- ・ 特定の環境でのプリミティブの性能：3 番目に重要な評価項目。ソフトウェア環境については、8 ビットプロセッサから 64 ビットプロセッサまで多岐にわたる。ハードウェアについては FPGA と ASIC が考慮される。
- ・ 柔軟性：4 番目の評価項目。広範囲で利用できるプリミティブが明らかに望ましい

同プロジェクトの最終結果として公表されたポートフォリオを表 3-6に示す。

表 3-6 NESSIEが推奨する暗号プリミティブのポートフォリオ⁵³

Type of Primitives	NESSIE portfolio
64-bit Block Ciphers	MISTY1
128-bit Block Ciphers	AES, Camellia
256-bit Block Ciphers	SHACAL-2
Stream Ciphers and Pseudorandom Number Generators	(該当なし)
Collision-Resistant Hash Functions	Whirlpool, SHA-256, SHA-384,

⁵³ NESSIE, “NESSIE Portfolio of recommended cryptographic primitives,” February 27, 2003
<https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf>

	SHA-512
Message Authentication Codes	UMAC, TTMAC, EMAC, HMAC
Asymmetric encryption schemes	PSEC-KEM, RSA-KEM, ACE-KEM
Digital signature schemes	RSA-PSS, ECDSA, SFLASH
Asymmetric Identification Schemes	GPS

(NESSIE Portfolio of recommended cryptographic primitives を基に作成)

(2) ECRYPT⁵⁴

ECRYPT (European Network of Excellence for Cryptology) は、現在進行中の欧州研究開発政策の FP6 (2002 ~ 2006 年) の IST の一環として 2004 年 2 月より開始されている。プロジェクトは、情報セキュリティ分野、特に暗号と電子透かし (watermarking) に関する欧州の産学の研究者間のコラボレーション強化を目的としている。

ECRYPT は暗号アルゴリズムおよび鍵長について検討を行った結果を公開している。以下にそれらの概要を示す。

(a) ECRYPT Position Paper: Recent Collision Attacks on Hash Functions⁵⁵

2005 年 2 月に公表された。2004 年 8 月の Crypto 2004 における報告について公表時点における意味と影響についての見解と、ECRYPT の勧告を示している。以下に勧告の概要を示す。

- ・ 一般に、 2^{80} 回以下の処理で実現可能な攻撃への耐性が十分に考慮されない限りは、160 ビット未満の出力のハッシュ関数の利用は勧められない。
- ・ MD5 あるいは SHA-1 を用いる HMAC については即時対応する必要はないが、HMAC-MD5 については、HMAC-SHA-1 あるいはコリジョンについて問題がないハッシュ関数を用いた HMAC への置き換えが賢明である。
- ・ 中程度あるいは高度なセキュリティを要するアプリケーションにおける署名には MD5 の使用を続けることを勧めない。SHA-1 の新規の利用については注意が必要。既存の SHA-1 ベースの署名に危険は今のところはない。
- ・ 3 年から 5 年の期間で利用するアプリケーションにおける RIPEMD-160 の即時置き換えの必要はない。
- ・ 長期的視点では、可能であれば、FIPS180-2 に示されるハッシュ関数や Whirlpool のような代替方式の利用を検討することを推奨する。

⁵⁴ ECRYPT Main <http://www.ecrypt.eu.org/index.html>

⁵⁵ ECRYPT, "ECRYPT Position Paper: Recent Collision Attacks on Hash Functions," February 17, 2005. http://www.ecrypt.eu.org/documents/STVL-ERICS-2-HASH_STMT-1.1.pdf

(b) ECRYPT Yearly Report on Algorithms and Key Lengths (2004)⁵⁶

2005年3月に公表された報告書で、暗号アルゴリズムおよび目的に応じた鍵長等のパラメータ設定について勧告が示されている。この報告書は、記述時点の公知の技術に基づく検討結果を比較的平易に記述しており、今後毎年更新版が公表される予定である。

報告書は、総論、(I)鍵長に関する勧告、(II)対称鍵暗号プリミティブに関する検討、(III)非対称暗号プリミティブに関する検討から構成されており、暗号危殆化の一般論に関しては総論および(I)に多数の参考となる記述が含まれる。

同報告書で推奨する対称鍵暗号方式に関する最小鍵長を表3-7に示す。表3-7における攻撃者の想定については1996年に発表された論文⁵⁷に基づいている。また、この表に示す最小鍵長は、攻撃者が2,3ヶ月間で行う攻撃に耐えうる程度を想定している。

表 3-7 鍵長の最小値に関する勧告 (ECRYPT 2004 年報告)

攻撃者	攻撃者の 予算 [\$]	攻撃者が使用するハ ードウェア	最小鍵 長 [bits]
ハッカー	0	PC	51
	< 400	PC(s)/FPGA	56
	0	“ Malware ”	59
小規模組織	10K	PC(s)/FPGA	62
中規模組織	30K	FPGA/ASIC	66
大規模組織	10M	FPGA/ASIC	72
諜報機関	300M	ASIC	81

(ECRYPT Yearly Report on Algorithms and Keysizes (2004)より引用)

公開鍵暗号方式の鍵長については、ECRYPT の検討結果として対称鍵暗号の鍵長との対応付けが提示されている。表 3-8にこれを示す。

表 3-8 鍵長の対応付け (ECRYPT2004 年報告)

非対称鍵の鍵長 [bits]	RSA [bits]	DLOG		EC [bits]
		field size [bits]	subfield [bits]	
56	512	512	112	112
64	768	768	128	128
80	1024	1024	160	160
112	2048	2048	224	224

⁵⁶ ECRYPT, “ECRYPT Yearly Report on Algorithms and Keysizes (2004),” March 1, 2005
<http://www.ecrypt.eu.org/documents/D.SPA.10-1.0.pdf>

⁵⁷ M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson and M. Wiener.
“Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security,” Report of ad hoc panel of cryptographers and computer scientists. January 1996.
<http://www.crypto.com/papers/keylength.pdf>

128	3072	3072	256	256
160	5120	5120	320	320
192	8192	8192	384	384
256	14720	14720	512	512

(ECRYPT Yearly Report on Algorithms and Keysizes (2004)より引用)

また、セキュリティレベルとして対称鍵の鍵長と提供可能な防護との対応付けを提示している。これを表 3-9に示す。

表 3-9 セキュリティレベルと対称鍵の鍵長との対応

セキュリティレベル	非対称鍵の鍵長 [bits]	防護可能な攻撃	コメント
1	32	実時間でハッカーにより行われる攻撃への防護	認証のタグにのみ使用可能
2	64	非常に短い時間で小規模組織により行われる攻撃への防護	新規システムにおける機密性確保には使わべきではない
3	72	短時間で中規模組織により行われる攻撃、あるいは、中期間で小規模組織により行われる攻撃への防護	
4	80	非常に短い時間で諜報機関により行われる攻撃、あるいは、長期間で小規模組織により行われる攻撃への防護	一般的用途に関する最小の防護。5年未満程度
5	112	中期の防護	約 20 年間程度
6	128	長期の防護	約 30 年間程度
7	256	“ 予測可能な未来 ”	量子計算機に対する適度な防護

(ECRYPT Yearly Report on Algorithms and Keysizes (2004)より引用)

(3) その他

欧州における暗号危殆化に係るその他の動向について述べる。

欧州電気通信標準化機構(ETSI : European Telecommunications Standards Institute) においては、ETSI TS (technical specification) 101 733 に署名検証に必要なデータが損失した状況への対策として署名トークンの技術仕様が規定されている⁵⁸。この中でハッシュ関数および暗号アルゴリズムの危殆化に関し想定が必要な旨が言及されている。

ドイツ政府においては、電子署名法に 1997 年制定時より、電子署名済みのデータが署

⁵⁸ European Telecommunications Standards Institute (ETSI), "ETSI TS 101 733: Electronic Signatures and Infrastructure (ESI); Electronic Signature Formats, v1.5.1 ", 2003.

名時に用いた暗号アルゴリズムの危殆化により真正性を保ち続けられなくなる点に配慮し、アルゴリズムが危殆化する前に新たなアルゴリズムとパラメータを用いて署名を作り直すことが定められている⁵⁹。

3.2.3. 国内の公的機関における検討の状況

CRYPTREC においては、安全性マージンについて、推奨する暗号方式を検討する過程で議論がなされており、電子政府推奨暗号リストの策定にあたって反映されている。

危殆化に関する情報収集としては、暗号技術監視委員会において、電子政府推奨暗号の監視、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする調査・検討が行われている。継続的な監視業務を行う要員数名が情報通信研究機構及びIPAに配置されており、国内外の学会・会議、文献、Web等を含む幅広い関連情報源に基づく情報収集と分析を行っている。

<http://portal.etsi.org/esi/el-sign.asp>

⁵⁹ タイムビジネス推進協議会, “タイムビジネスに関するドイツ動向調査報告書,” http://www.scat.or.jp/time/PDF/doitsu_houkokosyo.pdf

4. 暗号危殆化の電子政府への影響分析

政府では、e-Japan戦略⁶⁰に基づき、電子政府の構築を進めている。e-Japan戦略の中では、1)行政内部の電子化、2)官民接点のオンライン化、3)行政情報のインターネット公開および利用促進、4)調達方式の見直しを行うことが述べられている。1)および2)については、電子申請・届出システムとして、3)は電子政府の総合窓口⁶¹として、4)は電子入札・改札システムとして、構築・運用されている。また、e-Japan2002 プログラム⁶²により、行政の電子化の着実な推進のために、電子申請・届出に必要とされる公的個人認証サービスに係るシステムの構築を各地方公共団体ごとに進めることが定められ、2004年1月29日よりサービスが開始されている。

これらのサービスは、電子署名およびSSLを用いた暗号通信を用いている。従って、これらシステムが使用している暗号が危殆化した際には、影響を受けることになる。

4.1. 電子政府システム

電子政府システムは、大別して政府認証基盤（GPKI）、電子申請・届出システム、電子入札・開札システム、歳入金納付システム、内部管理・業務システムより構成される。

4.1.1. 政府認証基盤（GPKI）

政府認証基盤（GPKI：Government Public Key Infrastructure）は、各府省庁が運営する府省認証局と各府省認証局をつなぐブリッジ認証局により構成される。また、ブリッジ認証局は、特定認証業務に係る民間認証局や商業登記認証局、地方公共団体が運営する認証局（LGPKI）および公的個人認証サービスに係る認証局と相互接続されている。

(1) ブリッジ認証局

総務省が運営を管轄する。各府省が運営する府省認証局や特定認証業務に係る認証局、商業登記認証局、LGPKI および公的個人認証サービスに係る認証局と相互接続し、認証局間の相互認証機能を実現する。

ブリッジ認証局は、2048bitのRSA鍵を用いて、各認証局に対して認証局証明書を発行する。

(2) 府省認証局

府省認証局は、各府省庁により構築、運営されている。主に官職に対して、官職証明書

⁶⁰ 高度情報通信ネットワーク社会推進戦略本部、“e-Japan戦略”、2001年1月22日。

⁶¹ <http://www.e-gov.go.jp/>

⁶² IT戦略本部、“e-Japan2002プログラム”、2001年6月26日。

を発行する。また、電子申請・届出サービスや電子入札・開札システムなど国民側とインターネットを介して通信を行う場合に、安全な通信を行うための証明書（サーバ証明書）や Java アプレット等の正当性を示すためのコード証明書を発行する府省認証局も存在する。

(3) 特定認証業務に係る民間認証局

特定認証業務の認定を受けた民間が運営する認証局であり、電子申請・届出サービス等を利用する国民等に対して証明書を発行する。

特定認証業務に係る民間認証局は、19 事業者（2004 年 12 月 6 日現在）存在する。

(4) 商業登記認証局

法務省が運営し、電子申請・届出システム等を利用する国民等に対して証明書を発行する。

(5) LGPKI

地方公共団体において、許認可等を行う官職に対して証明書を発行する認証局のネットワークであり、総合行政ネットワークの一部として構築された。

(6) 公的個人認証サービスに係る認証局

公的個人認証サービスとは、地方公共団体が国民等に対して電子証明書を発行するサービスであり、2004 年 1 月 29 日からサービスを開始した。公的個人認証サービスは、「電子署名に係る地方公共団体の認証業務に係る法律（公的個人認証法）」により法的に位置づけられている。公的個人認証サービスは、住民基本台帳ネットワークを電子証明書の発行窓口として、地方公共団体が認証局を運営する。

4.1.2. 電子申請・届出システム

(1) 概要

電子申請・届出サービスは、インターネットを介して行政手続きを行うことができる行政サービスである。これまで行政手続きを行う際には、窓口へ直接出向くか郵送の必要があったが、電子申請・届出サービスにより、その必要がなくなるという利点がある。

2004 年 3 月末オンライン化対象手続き 13,834 件中、96%がオンライン化済である⁶³。

(2) システム概要

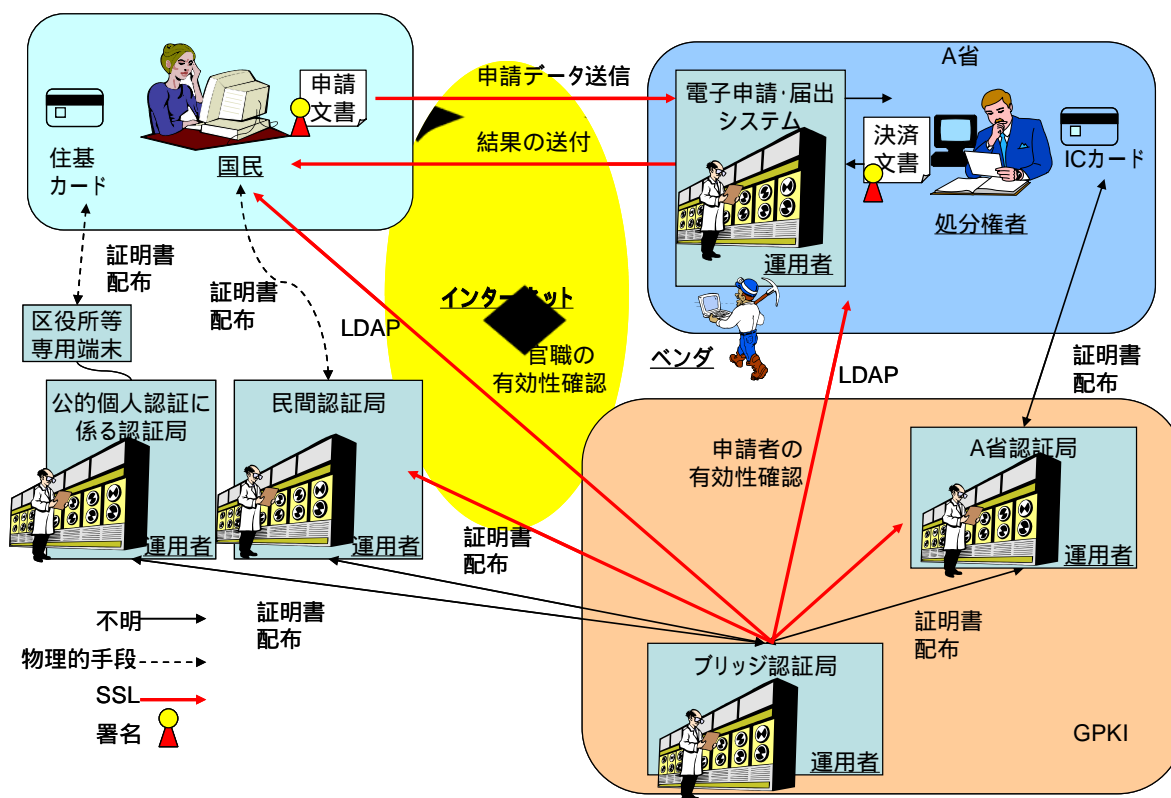
電子申請・届出サービスを実現するのが電子申請・届出システムである。電子申請・届出システムには、税関への輸入関係手続きや特許の出願手続き等の申請件数の多い手続き、

⁶³ 総務省 “電子政府の進捗に関する調査報告書”、2004 年。

特定業種に係る手続き等を処理する個別の専用システムと、それ以外の手続きに係る汎用の電子申請・届出システムがある。専用システムでは、申請から認可にいたる全てのプロセスが手続きごとに構築されている。他方、汎用の電子申請・届出システムでは、申請等の受付および許認可等の申請者への通知に係る部分は汎用受付等システムの仕様⁶⁴に基づき、府省庁ごとに構築されている。また、汎用の電子申請・届出等システムでは、個別手続きごとに業務システムが構築されており、受け付けた申請を処理する。

申請等を行う国民等は、特定認証業務に係る認証局または公的個人認証サービスに係る認証局から、電子証明書の発行を受けて電子申請・届出システムを利用する。

申請データの送信、許認可公文書の取得等、国民等と行政との通信はSSLを用いて行われる。また、申請データに付する証明書や公文書に付される官職の署名等の検証はGPKIを介して行われる(図4-1)。



(株式会社 三菱総合研究所作成)

図 4-1 電子申請・届出システム

⁶⁴行政情報化推進各省庁連絡会議幹事会了承 “申請・届出等手続のオンライン化に関わる汎用受付等システムの基本的な仕様” 2001年8月6日。

4.1.3. 電子入札・開札システム

(1) 概要

府省庁や地方自治体が行う公共工事や物品調達などの入札から落札にいたる全ての過程を、インターネットを介して行う。これにより、受発注手続きの透明性向上、業務効率の向上等の効果がある。

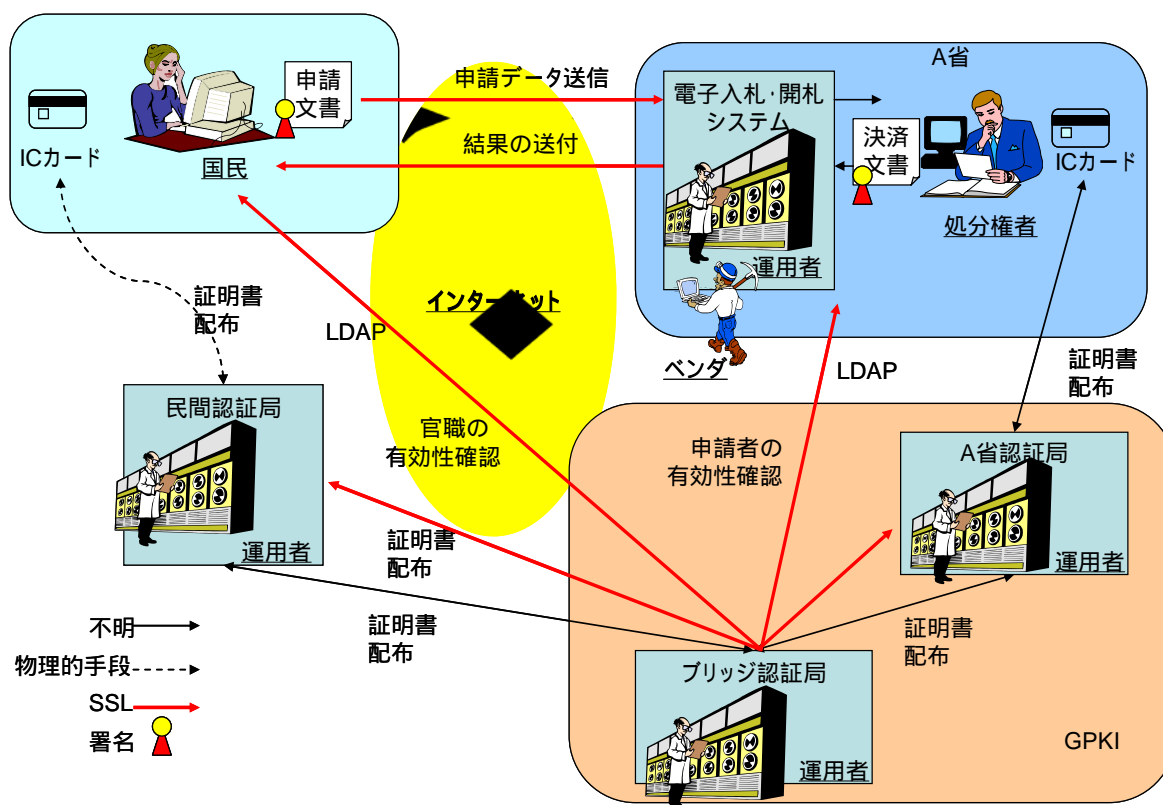
公共工事分野では、国土交通省は、2001年10月から直轄事業において、電子入札・開札を導入した。また、2003年度より、地方整備局等が発注する建設工事及び建設コンサルタント業務等の全てを対象に電子入札を開始しており、その他の府省においても2003年度中に導入済みである。非公共工事分野においては、総務省が2002年10月から電子入札・開札を実施、その他の府省においても2003年度中に導入済みである⁶⁵。

(2) システム概要

発注者と受注者は、GPKI等から配布される証明書と秘密鍵をICカードに格納する。

発注者は、発注に関する情報を電子入札・開札システムに登録する。入札者は、電子入札・開札システムで検索を行い、希望の入札案件を見つける。そして、必要書類等をそろえ、電子入札・開札システムに入力する。この際の処理は、インターネットを介して行われるため、電子入札・開札システムではICカードを用いてSSL通信を用いて行われる(図4-2)。

⁶⁵ “e-Japan重点計画-2003等に掲げられた施策の推進状況の調査報告(2004年春)”, 高度情報通信ネットワーク社会推進戦略本部(IT戦略本部) 第26回会合 資料11、2004年6月15日。



(株式会社 三菱総合研究所 作成)

図 4-2 電子入札・開札システム

4.1.4. 歳入金納付システム

歳入金納付システムは、2004年1月より財務省によって運営されているシステムである。本システムは、申請手続き等の手数料をATMやインターネットバンキングを使用して納付するためのシステムである。

4.1.5. 内部管理・業務システム

内部管理・業務システムは、人事管理、給与管理等、行政内部の管理業務に係るシステムである。現在、個別府省庁ごとにシステム構築が進められている。

4.2. 暗号アルゴリズム危殆化の影響分析

4.2.1. 電子政府における暗号の使用状況

電子政府における暗号の使用状況を表4-1に示す。

主に、インターネット上でのSSL通信と認証局から発行される証明書、および、申請手続きで生成される申請データおよび許認可等公文書データへの署名(データ署名)に暗号

が使用されている。

表 4-1 電子政府における暗号の使用状況

分類	暗号名称		GPKI	電子申請・届出システム、電子入札・開札システム				電子政府推奨暗号リストへの記載
			CA 鍵	官職等鍵	証明書	データ署名	SSL 通信	
公開鍵暗号	RSA Encryption (注1)	2048 bit 鍵						
		1024 bit 鍵						
	Diffie-Hellman							
共通鍵暗号	DES							
	3-key Triple DES							(注2)
	RC2							
	RC4							(注3)
ハッシュ関数	MD5							
	SHA-1							

(注1) 認証局証明書は 2048 ビット、それ以外の証明書は 1024 ビットの鍵で生成される。

(注2) FIPS46-3 で規定されていること、および、デファクトスタンダードの地位を保っていることを理由に電子政府推奨暗号リストに記載されている。

(注3) 128bit 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。

(株式会社 三菱総合研究所作成)

4.2.2. 暗号アルゴリズムの各危殆化要因と影響の仕方

暗号アルゴリズムは、様々な要因で危殆化する(2.2節参照)。各種要因には、それぞれ影響の仕方に特徴がある。

量子計算機や分子計算機は、現在の PC 等とは異なる計算機モデルで計算が行われる。従って、新たな計算機モデルが考案されると、現代の主要暗号の全てについて安全性について再検証を行う必要がある。そのため、影響範囲は全ての暗号に及ぶ。しかし、新たに考案された計算機モデルが現実に実装されるかどうかは暗号の危殆化においては問題である。なぜなら、強力な計算機モデルでも実装されなければ現実に危殆化するに至らないからである。従って、新たな計算機モデルが現実に構成されると突発的に影響が露見する。しかし、実際に計算機が構成されるまでに、計算機モデル上では各種暗号アルゴリズムごとに安全性の検証が行えるため、危殆化の程度はある程度理論的に推測可能である。

現代の主要暗号は、PC 等の計算機を用いても解読するために膨大な時間やコストがかかることをその安全性の根拠にしている。しかし、LSI の集積度向上による CPU パワーの増大や GRID コンピューティング等の分散計算技術といった計算機技術が進歩し、計算

機能力が向上するとその安全性も相対的に低下することになる。従って、計算機能力が向上すると全ての暗号方式が危殆化することになる。また、量子計算機等の開発を除く計算機技術は、急激に進歩するとは考えにくいいため、計算機能力向上による暗号危殆化は徐々に進行すると考えられる。また、同様にその影響の大きさがある程度推測可能である。

暗号の解読手法は、個別暗号ごとに構成される。従って、その影響範囲は、開発された解読手法が対象とする暗号アルゴリズムにのみ影響する。しかし、その解読手法が構成されるまで、影響の大きさは推測できず、また、その出現を予測できないため突発的に影響が発生することになる。

以上まとめると、表 4-2 のようになる。

表 4-2 暗号アルゴリズム危殆化要因と影響の仕方

危殆化要因	詳細	暗号アルゴリズムへの影響		
		範囲	大きさ	特徴
計算機モデルの変化	量子・分子計算機 等	暗号全般	推察可能	計算機が構成されると突発的に露見
計算機能力の向上	CPU 性能向上 Grid コンピューティング 等	暗号全般	推察可能	徐々に進行
攻撃手法の進歩	弱鍵発見 処理フロー上の問題発見 ベースとなる問題の解法発見 解読に適したハードウェア デザイン 等	個別暗号	予測不能	突発的に発生

(株式会社 三菱総合研究所 作成)

4.2.3. 暗号アルゴリズムの危殆化状況

電子政府システムで使用されている暗号のうち、RSA Encryption、DES、RC4、MD5、SHA-1 に関して、暗号アルゴリズムの危殆化状況を示す。

(1) RSA Encryption (素因数分解問題)

RSA Inc., New Factoring Challengeにおいて、2003年12月3日にドイツのScientific Computing InstituteのJ. Frankにより、576bitの素因数分解に成功したことが報告された

⁶⁶。

⁶⁶ <http://www.rsasecurity.com/rsalabs/node.asp?id=2096>

(2)DES

RSA社主催のDES Challenge IIIにおいて、1999年1月18日、Electronic Frontier FoundationのDeep Crackとdistributed.net（暗号解読専門のインターネット・グリッドコンピューティング）の共同により、22時間15分で解読。攻撃方法は鍵の全数探索により行なわれた⁶⁷。

(3)RC4

CRPTRECは、これまでのところ、128bit鍵 RC4 に関しては現実的な解読法は存在しないとされているが、40bit鍵のRC4 に関しては安全性が低いことを認めている⁶⁸。

(4)MD5

2004年8月のCRYPTO 2004 Rump Sessionにおいて、MD5のコリジョンに関する報告がなされた⁶⁹。IACRのePrint Archiveによる同報告論文によると、IBM P690 を用いて、15秒から5分程度の探索でコリジョンが発見できるとされている⁷⁰。

(5)SHA-1

2005年2月、世界的に著名な研究者であるBruce SchneierのWEBページ上で、全数探索よりも少ないコストでSHA-1 のコリジョンを発見する方法が存在することが公表された⁷¹。しかし、本攻撃手法を考案した研究者らは、まだ具体的な方法を公表してはいない⁷²。

4.2.4. 影響分析

(1) 影響範囲

表 4-1 電子政府における暗号の使用状況から、RSA Encryption または SHA-1 がアルゴリズム上危殆化した場合、電子政府システムに対して広範に影響が及ぶ。その影響の仕方としては、申請データおよび許認可等への電子署名の信頼性低下、SSL におけるサーバ認証等の信頼性低下が挙げられる。他方、そのほかの暗号アルゴリズムが危殆化した場合には、SSL 通信に影響がおよび通信の守秘性が担保できなくなる。

(2) 暗号アルゴリズムの危殆化要因と電子政府システムへの影響

計算機モデルの変化により、RSA Encryption および SHA-1 が危殆化した場合には、そ

⁶⁷ <http://www.rsasecurity.com/rsalabs/node.asp?id=2108>

⁶⁸ CRYPTREC Report 2002,

http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030401_report01.html

⁶⁹ <http://www.iacr.org/conferences/crypto2004/rump.html>

⁷⁰ <http://eprint.iacr.org/2004/199>

⁷¹ <http://www.schneier.com/blog/archives/2005/02/index.html>

⁷² <http://theory.csail.mit.edu/~yiqun/shanote.pdf>

の影響が突発的に現れるため、電子政府システムに大きな影響を与えられられる。しかし、暗号アルゴリズムの危殆化の程度は理論的に推測可能であるため、対策を準備しておくことはできる。それ以外の暗号の場合には、SSL で使用するリストからはずすなどの処置で影響を軽微にできる。

計算機能力の向上は、全ての暗号に対して影響するが、徐々に進行するため、電子政府システムへの影響も徐々に進行すると考えられる。従って、十分な対策を検討しておくことで、電子政府への影響を軽微にできる。

攻撃手法の進歩は、個別暗号アルゴリズムごとに影響し、突発性があり、また危殆化の程度が予測できない。そのため、RSA Encryption および SHA-1 に対して、攻撃手法が進歩した場合には、電子政府システムへの影響が大きくなる可能性がある。他方、それ以外の暗号アルゴリズムの場合には、SSL で使用するリストからはずすなどの処置を講じることで、電子政府システムへの影響を軽微にできる。

(3)SSL への影響に関して

SSL は電子申請・届出システムを始めとする電子政府システムにおいて利用されている。SSL で使用できる暗号のうち、512bit 鍵 RSA Encryption、共通鍵暗号 DES およびハッシュ関数 MD5 においては、暗号専門家の間では既に危殆化したと認定されている。また、MD5 においては、現実的にコリジョンを発見することが可能である。従って、これら 3 つの暗号の使用に際しては、実際の使用状況を考慮した実質的プロセスの検討が必要である。

また、SSL の仕様において、ハッシュ関数は SHA-1 および MD5 の選択になっている。従って、MD5 が既に危殆化していることを考慮すると、SHA-1 が危殆化した際には、SSL 自体に問題が生じることになる。このため、実質的利用状況をみつつ、対処スケジュールおよび実質的プロセスの検討が必要である。

(4)申請・届出手続きにおける暗号危殆化の影響規模

RSA Encryption または SHA-1 が危殆化した場合の影響規模を、電子申請・届出システムを例として、分析する。前提として、全ての申請に対する許認可等結果に関する公文書データには官職のデジタル署名が付されているものとする。

RSA Encryption または SHA-1 が危殆化すると、官職等証明書や公文書データに付されるデジタル署名に対する信頼性が低下する。その結果、電子申請・届出システムを介して行われた申請や結果の通知に関して疑義が生じる。従って、RSA Encryption または SHA-1 が危殆化した場合、前提から、電子申請・届出システムを利用した全ての申請・届出に影響がでることになる。

表 4-3に電子申請・届出システムの利用率を示す⁷³。表 4-3より、電子申請・届出シス

⁷³ 総務省、“電子政府の推進に関する調査”、2004年6月9日

テムを利用した申請・届出件数は、全体の80%程度であることがわかる。従って、RSA EncryptionまたはSHA-1が危殆化した場合、申請・届出件数の80%程度に影響が出ることが予想される。

表 4-3 オンライン申請による申請・届出等手続の利用状況

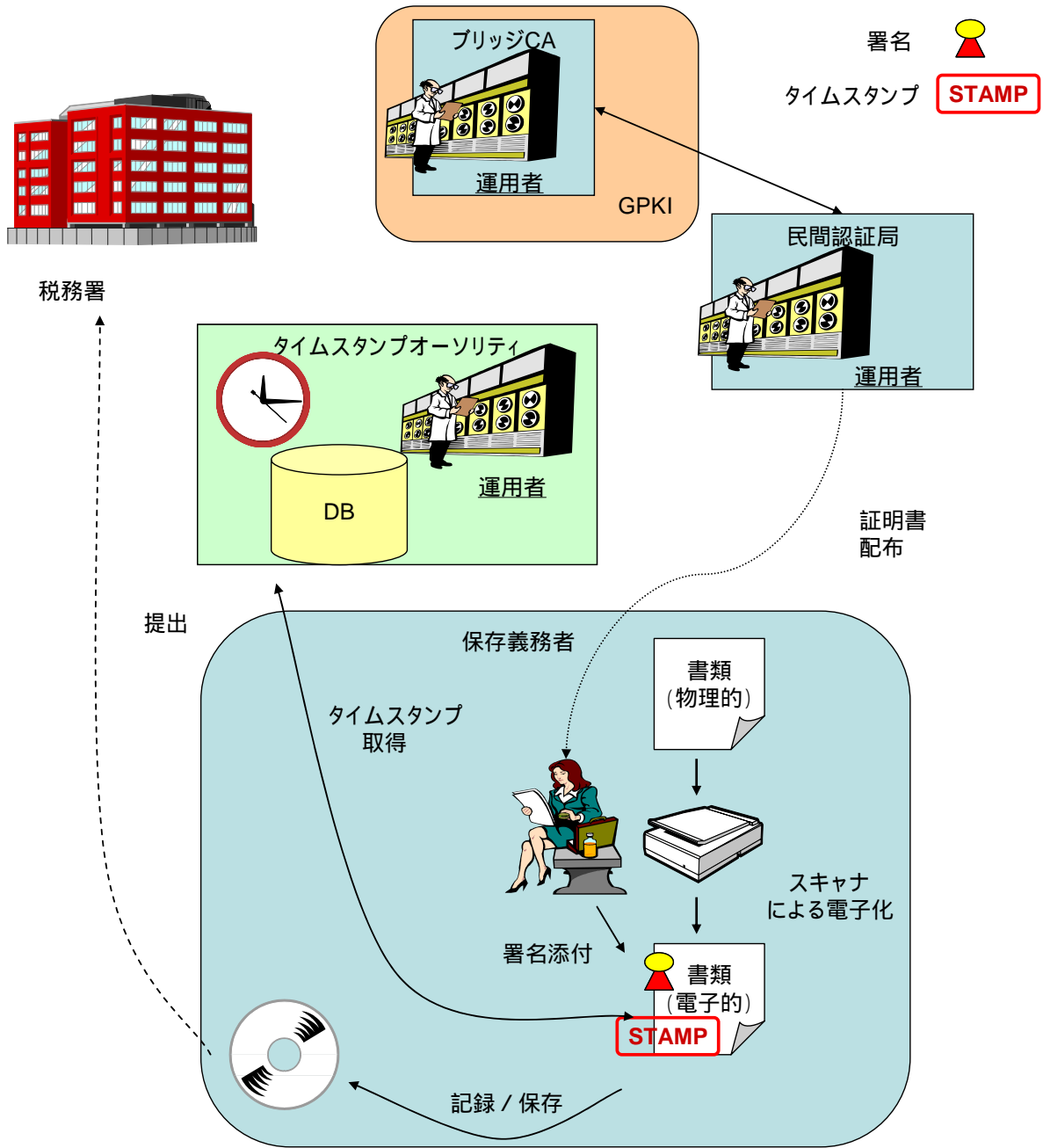
	2002年度(平成14年度)	2003年度(平成15年度)
全体	86.4 % (737 手続 : 5,009 万件中 4,326 万件)	81.0 % (4,113 手続 : 8,210 万件中 6,654 万件)
専用システム (特定業種)	86.9 % (159 手続 : 4,976 万件中 4,326 万件)	81.9 % (464 手続 : 8,124 万件中 6,653 万件)
汎用システム	1.3 % (578 手続 : 33 万件中 4,300 件)	0.7 % (3,649 手続 : 86 万件中 6,400 件)

(総務省、“電子政府の推進に関する調査”を参考に作成)

4.3. 電子政府システムに係る文書の長期保存

2005年1月31日付け財務省令第1号「電子計算機を使用して作成する国税関係帳簿書類の保存方法の特例に関する法律施行規則の一部を改正する省令」により、国税関係書類のうち棚卸表、貸借対照表等の電子的保存が認められた。本省令によると、保存対象となる国税関係書類をスキャナで電子化した後、特定認証業務の認定を受けた認証局から公開鍵証明書の発行を受けた保存義務者が国税関係書類データに対して署名を付し、その後タイムスタンプ・オーソリティによりタイムスタンプを付すことが示されている(図 4-3)。

国税関係書類は税法上7年、商法上10年の保存義務があるため、電子化された国税関係データに関しても同等の保存義務が生じると考えられる。したがって、署名やタイムスタンプに使用する暗号アルゴリズムが危殆化した場合、法律上の保存義務年限を担保できなくなる可能性がある。



(株式会社 三菱総合研究所作成)

図 4-3 国税関係書類の電子化保存プロセス

4.4.まとめ

電子政府システムにおいては、RSA Encryption または SHA-1 が危殆化した場合に、大きな影響が発生すると考えられる。また、ハッシュ関数においては、MD5 が既に危殆化している状態であると専門家の間では認識されており、数分程度の探索でコリジョンが発見できるとの報告がなされている。

電子申請・届出システムや電子入札・開札システム等に用いられる SSL においては、ハッシュ関数においては SHA-1 または MD5 の選択となっている。しかし、MD5 は現実的にコリジョンが発見可能な状況であるため、SHA-1 が危殆化した場合には、SSL 通信を使用するシステム全般に影響が及ぶ。

国税関連関係書類の電子化に伴い、今後一層の文書の電子化が促進されると考えられる。そこで重要となるのは、長期保存文書の証拠性確保である。現状では、電子署名やタイムスタンプにより、証拠性を確保する。しかし、電子署名やタイムスタンプ等でも RSA 等公開鍵方式やハッシュ関数を用いる。したがって、これら暗号アルゴリズムが危殆化した場合には、長期保存文書の証拠性が担保できなくなる。

上記より、電子政府システムにおいて MD5 を使用する場合には、利用実態を考慮した実質的プロセスの検討が必要である。また、SHA-1 を始めとする暗号においても、実質的利用状況をみつつ、対処スケジュールおよび実質的プロセスの検討が必要である。この際、暗号のアプリケーション、例えば署名による証拠性確保や、通信内容の秘匿等を考慮することが望ましい。

5. 暗号危殆化に係わる問題点

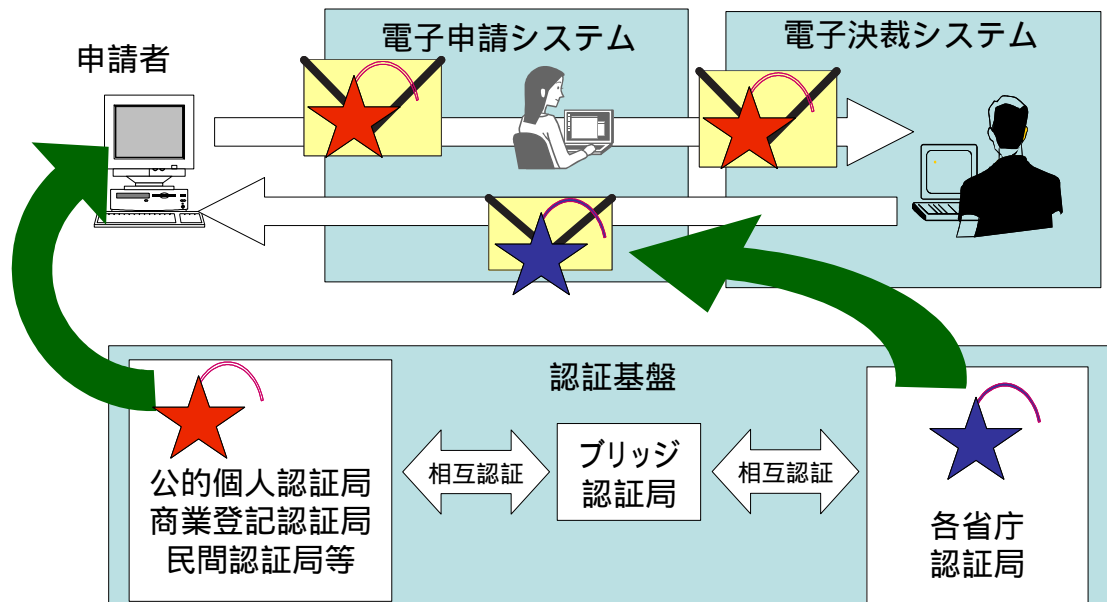
5.1. 電子政府に係わるプレイヤーから見た問題点

5.1.1. 電子申請システムに係わる問題点

(1) プレイヤの定義

電子政府システムのうち、最も典型的なシステムである電子申請システムに関して、プレイヤーを定義する。

電子申請システムのイメージは、図 5-1の通りである。



(株式会社 三菱総合研究所 作成)

図 5-1 電子申請システムのイメージ

プレイヤーは、以下のように定義できる。

- ・ 申請者
- ・ 決裁担当者 (審査担当者)
- ・ 電子申請システム開発運用担当者
- ・ 公的個人認証局、商業登記認証局または民間認証局

(2)想定するシナリオ

暗号アルゴリズムの危殆化に関して、以下の暗号アルゴリズムの危殆化を想定する。

- ・ 官職証明書発行の際の、署名に用いる暗号アルゴリズム
- ・ 電子申請に係わる暗号化通信の際の、サーバ証明書発行時の署名に用いる暗号アルゴリズム
- ・ 公的個人認証局、商業登記認証局または民間認証局が、企業や個人の証明書発行時の署名に用いる暗号アルゴリズム
- ・ 申請者が、公的個人認証局、商業登記認証局、または民間認証局から法人や個人の証明書発行時に暗号通信を行う際の、サーバ証明書発行時の署名に用いる暗号アルゴリズム

想定するシナリオにおいて、これらの暗号アルゴリズムは同一であるものとする。なお、申請者は、通常の汎用ブラウザおよび一連の手続き向けのアドオンソフトウェアを用いるものとする。

さらに、電子申請システムおよび公的個人認証局の運用担当者は、以下の措置をとることを想定する。

- 1) 暗号アルゴリズムの危殆化が宣言されたら、新しい暗号アルゴリズムに移行する計画を策定する
- 2) ソフトウェア開発等の関連システムの再構築を行う
- 3) 申請者や決裁担当者等へのソフトウェア等の配布も含めた移行を行う
- 4) 移行の際に、失効した証明書を CRL に記載する

(3)申請者に係わる問題点

公的個人認証を用いる場合の申請者に係わる問題点を処理フロー毎に挙げる。

- 1) 公的個人認証局等から申請者の証明書を取得する

この場面においては、申請者に以下の負担を強いる問題がある。

- ・ 住民基本台帳カードに格納されている秘密鍵を変更する必要がある、市町村の窓口に出向かなければならない
- ・ 証明書とクライアントソフトを変更するために、市町村の窓口に出向かなければならない
- ・ この際に、証明書再発行コストの負担に関しては明確になっていない

- 2) 申請者が証明書の検証を行う

この場面においては、以下の問題がある。

- ・ 申請者における証明書の検証は、IC カードに蓄積されているクライアントソフトウ

ェアにより行うものであり、クライアントソフトウェアが更新されていない限り、
証明書に問題があることはわからない

3) 申請者の証明書を添えて、電子申請を行う

4) 大臣名電子公文書を受領する

これらの場面においては、以下の負担を強いる問題がある。

- ・ 暗号通信のため、ブラウザの設定変更または別のブラウザのインストールが必要となる
- ・ 各種電子申請手続きのための専用ソフトウェアが必要な場合、専用ソフトウェアの設定変更または再インストールが必要となる

5) 大臣名電子公文書を利用する

この場面においては、以下の問題点が存在する。

- ・ 電子公文書取得時には表示された有効期限内に利用したにも係わらず、その途中で暗号アルゴリズムが危殆化しており、官職証明書が失効していた場合、利用者は再度電子申請を行う必要がある
- ・ 上記の場合、システムのバグ等により危殆化した暗号アルゴリズムにより生成された電子公文書が利用可能となった場合の措置に関しては検討が必要である

(4) 決裁担当者に係る問題点

決裁担当者に関しては、以下の問題点が存在する。

- 1) 電子決裁システムのためのソフトウェアの設定またはインストールが必要となる
- 2) システム構成によっては、危殆化した暗号アルゴリズムに対応する官職証明書を誤って添付する可能性がある
- 3) システム構成によっては、危殆化した暗号アルゴリズムに対応する申請者の証明書を処理することがあり、その場合の措置は検討が必要である

(5) 電子申請システム（または電子決裁システム）運用担当者に係る問題点

電子申請システム運用担当者に関しては、以下の問題点が存在する。

1) 暗号アルゴリズム危殆化の判断

暗号アルゴリズムが危殆化したと判断することは、各省庁の電子申請システム運用担当者では困難である。

2) 暗号アルゴリズム危殆化時の措置

暗号アルゴリズム危殆化時の措置に関して、以下が想定されるが、予めマニュアル等が整備されていないと対応は困難である。

- ・ 危殆化した暗号アルゴリズムから新しい暗号アルゴリズムへの切り替えスケジュール

ル等の決定

- ・ 暗号アルゴリズム切り替えに伴うシステム再構築作業の実施
- ・ 旧システムから新システムへの移行作業
- ・ 移行後のフォロー

3) 切り替えスケジュール

切り替えスケジュール作成に際しては、以下の留意点がある。

- ・ 危殆化の緊急性と新しい暗号アルゴリズムによるシステム再構築作業の期間のバランス
- ・ コスト
- ・ 他のシステムの移行時期

4) 暗号アルゴリズム切り替えに伴うシステム再構築作業の実施

システム再構築作業に際しては、以下の点に留意する必要がある。

- ・ ハードウェアや OS 等の既存環境との移植性確保
- ・ 危殆化した暗号アルゴリズムにより署名された、申請者の証明書や官職証明書に対する処理が考えられていること

5) 移行作業

移行作業に関しては、以下の点に留意する必要がある。

- ・ 申請者、決裁担当者を含むシステムの利用者への移行スケジュールの徹底
- ・ 関係するソフトウェアの配布方法および配布時期
- ・ テスト期間の設定
- ・ テスト期間におけるソフトウェアバグ等のトラブルへの対処

6) 移行後のフォロー

移行後のフォローに際しては、以下の点の留意が必要である。

- ・ ソフトウェアバグへの対処
- ・ 危殆化した暗号アルゴリズムによって署名がなされた証明書の失効化
- ・ 申請者へのフォロー

(6) 公的個人認証局、商業登記認証局または民間認証局に係る問題点

公的個人認証局、商業登記認証局または民間認証局運用担当者に関しては、以下の問題点が存在する。

1) 暗号アルゴリズム危殆化の判断

暗号アルゴリズムが危殆化したと判断することは、各自治体の公的個人認証局および商業登記認証局またはシステム運用担当者では困難である。特定認証業務を遂行している民間認証局運用担当者の場合、公的な暗号監視機関との連携が前提となることが考えられるが、特定認証業務以外の認証業務の方が先行して代替暗号とする可能性がある。

2) 暗号アルゴリズム危殆化時の措置

暗号アルゴリズム危殆化時の措置に関して、以下が想定されるが、予めマニュアル等が整備されていないと対応は困難である。

- ・ 危殆化した暗号アルゴリズムから新しい暗号アルゴリズムへの切り替えスケジュール等の決定
- ・ 暗号アルゴリズム切り替えに伴うシステム再構築作業の実施
- ・ 旧システムから新システムへの移行作業
- ・ 移行後のフォロー

3) 切り替えスケジュール

切り替えスケジュール作成に際しては、以下の留意点がある。

- ・ 危殆化の緊急性と新しい暗号アルゴリズムによるシステム再構築作業の期間のバランス
- ・ コスト
- ・ 他のシステムの移行時期

4) 暗号アルゴリズム切り替えに伴うシステム再構築作業の実施

システム再構築作業に際しては、以下の点に留意する必要がある。

- ・ ハードウェアや OS 等の既存環境との移植性確保
- ・ 危殆化した暗号アルゴリズムにより署名された、個人や企業の証明書に対する処理が考えられていること

5) 移行作業

移行作業に関しては、以下の点に留意する必要がある。

- ・ 申請者、決裁担当者を含むシステムの利用者への移行スケジュールの徹底
- ・ 関係するソフトウェアの配布方法および配布時期
- ・ テスト期間の設定
- ・ テスト期間におけるソフトウェアバグ等のトラブルへの対処
- ・ CRL への掲載

6) 移行後のフォロー

移行後のフォローに際しては、以下の点の留意が必要である。

- ・ ソフトウェアバグへの対処
- ・ 危殆化した暗号アルゴリズムによって署名がなされた証明書の失効化
- ・ 申請者へのフォロー

(7)まとめ

電子政府システムにおけるプレイヤーから見た問題点を、表 5-1に総括する。

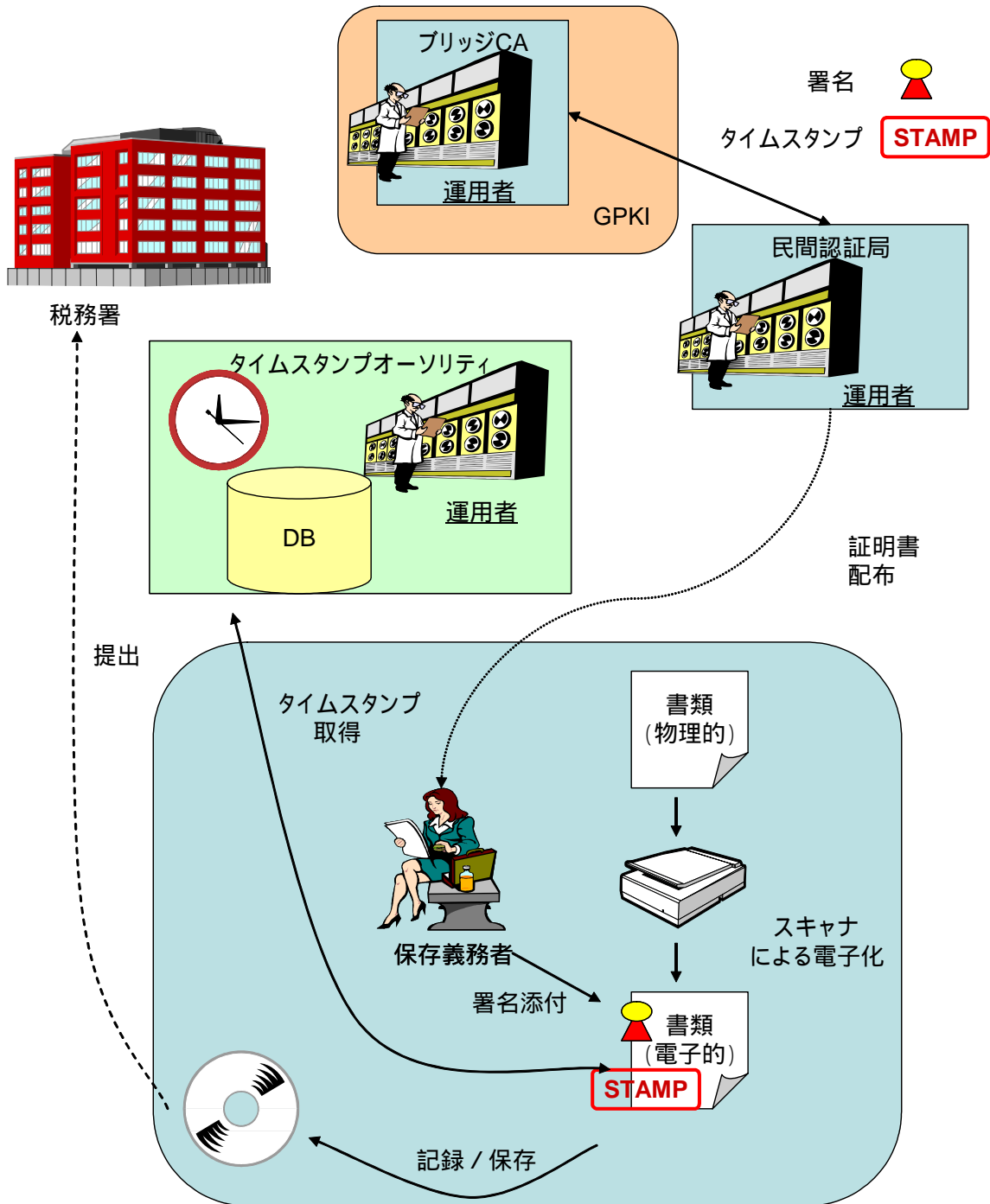
表 5-1 電子政府システムにおけるプレイヤーから見た問題点の総括

プレイヤー	問題点概要
申請者	<ul style="list-style-type: none">・ 秘密鍵および証明書の書き換えのために、認証局まで出向く手間が発生する可能性がある・ 証明書の検証に関して、クライアントソフトウェア等を更新しなければならないという問題がある・ 関連するソフトウェアの再設定または再インストールが必要となる・ 証明書再発行のコスト負担に関して不明確である
決裁担当者	<ul style="list-style-type: none">・ 関連するソフトウェアの再設定または再インストール等が必要である・ 危殆化した暗号アルゴリズムによる申請者の証明書に対応することが必要である
システム運用担当者	<ul style="list-style-type: none">・ 暗号アルゴリズム切り替えの判断が困難である・ 暗号アルゴリズム切り替えのスケジュール設定が困難である・ 申請者、決裁担当者、他関連システム運用担当者に対して、切り替えスケジュールを周知徹底することが必要である
認証局	システム運用担当者と同様であるが、他には以下の問題がある <ul style="list-style-type: none">・ 各自治体のコスト負担の問題がある・ 申請者への証明書およびクライアントソフトウェアの配布に係わる徹底の問題がある

(株式会社 三菱総合研究所 作成)

5.1.2. 電子文書の長期保存に係わる問題点

(1) プレイヤの定義



(株式会社 三菱総合研究所 作成)

図 5-2 電子文書の長期保存文書の典型例 (電子申告システム)

図 5-2は、税金の電子申告システムのイメージ図である。長期保存文書は、納税者側で管理する必要がある。この場合の、保存文書とは、電子帳簿保存法に規定された、税務関係書類であり、帳簿等である。こうした書類は、商法上 10 年の保存義務が課されている。以下にプレイヤを定義する。

- ・ 納税者
- ・ 税務署
- ・ タイムスタンプ・オーソリティ
- ・ 民間認証局

(2)シナリオ

シナリオは、長期文書に焦点を絞り、以下の通りとする。

- 1) 納税者が、民間認証局から個人証明書と秘密鍵を取得する
- 2) 納税者が、帳簿を作成し、民間認証局から取得した秘密鍵により署名を施し、さらにタイムスタンプにより時刻確定を行う。
- 3) 3 年後、納税者が取得した個人証明書を施した民間認証局の暗号アルゴリズムおよびタイムスタンプ・オーソリティの暗号アルゴリズムが危殆化した

(3)納税者（保存義務者）に係る問題点

納税者に関しては、以下の問題点が存在する。

- ・ 帳簿は、10 年間保存義務があるが、3 年経過した時点で暗号アルゴリズムの危殆化により鍵も危殆化しており、帳簿の真正性が担保されない
- ・ 3 年経過以後に、帳簿にさらに署名を行おうとすると、再度民間認証局から証明書を獲得する必要がある

(4)税務署に係る問題点

税務署に関しては、以下の問題点が存在する。

- ・ 納税者から申告書類を受け取った際、電子帳簿等の添付書類に署名が施されており、それがすでに危殆化した暗号アルゴリズムで署名されていた場合、文書の真正性を推定する方法がない（当該文書のある程度の真正性は担保されると推定される）

(5) タイムスタンプ・オーソリティに係る問題点

タイムスタンプ・オーソリティに関しては、以下の問題点が存在する。

- ・ 暗号危殆化以後、暗号危殆化以前に時刻刻印した電子文書について時刻に関する担保ができない。

(6) 民間認証局に係る問題点

民間認証局に関しては、以下の問題点が存在する。

- ・ 民間認証局は、暗号が危殆化した時点で、当該暗号アルゴリズムによる公開鍵ペアに対する証明書はCRLに掲載することになり、民間認証局から見た場合、当該電子帳簿類は真正性を保証できないが、ある程度の推定効を有することが推察される

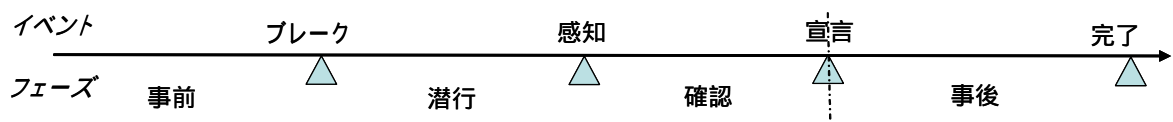
5.2. 法的な問題点

5.2.1. 概要

ここでは、暗号の危殆化に際して訴訟になった場合、相当の被害を被ったことを主張する側が、そうした被害に関して暗号の危殆化の結果であることを証明する義務があることを前提として、暗号危殆化に関する法的問題点の概要を示す。

(1) 暗号通信および認証に係わる問題

暗号通信および認証に係わる行為が問題となる場合、なりすましがなされたと主張する日時を暗号危殆化の宣言の前後で分けて考えることが可能である。



(2) 公開鍵証明書に係わる問題

公開鍵証明書に関しては、以下のように分けて考えることができる。

- ・ 「宣言」以前に作成された証明書が、「宣言」～「完了」の間に利用された場合
- ・ 「宣言」以後に作成された証明書が、「完了」の前に利用された場合

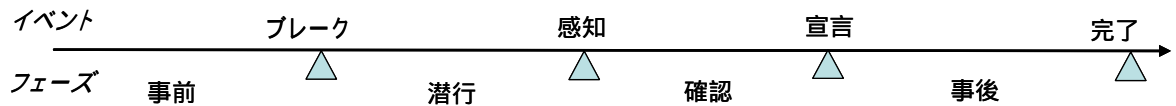
(3) 署名付文書に係わる問題

署名付文書に関しては、以下のように分けて考えることができる。

- ・ 「宣言」以前に作成された署名付文書が「完了」以前に参照された場合（参照時点で有効期限内または外）
- ・ 「宣言」以前に作成された署名付文書が「完了」以後に参照された場合（参照時点で有効期限内または外）
- ・ 「宣言」以後に作成された署名付文書が「完了」以前に参照された場合（参照時点で有効期限内または外）
- ・ 「宣言」以後に作成された署名付文書が「完了」以後に参照された場合（参照時点で有効期限内または外）

5.2.2. 暗号通信および認証に係わる問題

暗号通信および認証に関しては、電子政府の運用責任者の責任に焦点を当てることが適切である。



上記図において、暗号通信および認証がどの時点でなされるかが問題となる。

(1) 想定される問題

以下の問題が典型的であると想定される。

- ・ 認証機能に関して、正規の利用者が、暗号の危殆化によりなりすまされたとして、電子政府システムの利用を認めず、電子政府システムの運用責任者を訴える。

(2) 論点

上記の想定される問題に関して、以下の論点が存在する。

- ・ なりすましがなされたことを正規の利用者が証明する必要がある
- ・ 電子政府システムの運用責任者は、宣言後速やかに適切な対策を施した場合、責任を追及される可能性は少ない

上記をまとめると、原告が訴える場合、以下のように考えることができる。

- 1) 危殆化宣言より以前の行為の場合、電子政府システムの運用責任者には処置の施しようがないため、責任は発生しない
- 2) 危殆化宣言より以後の行為の場合、電子政府システムの運用責任者が、適切な対策を施しているのであれば、責任は発生しない

5.2.3. 公開鍵証明書に係わる問題について

公開鍵証明書は、認証機関が発行するものであり、認証機関に係わる責任を検討することが重要である。

(1) 想定される問題

発生する問題は以下のように想定できる。

- ・「宣言」以前に作成された公開鍵証明書が「宣言」以後に検証されたが、CRL に掲載がなく検証の結果、有効となった。

- ・「宣言」以後に作成された公開鍵証明書が「完了」以前に検証されたが、CRL に掲載がなく検証の結果、有効となった。

(2) 論点

上記の問題における論点は以下の通りである。

- ・認証機関は、「宣言」後、当該暗号に係わる公開鍵証明書は全て CRL に掲載することが望ましいが、一方で「事後」の対策は完了しておらず、認証機関が CRL 掲載の有無に関して責任を問われる可能性に関しては不明である

本件に関しては、電子政府システムの可用性と安全性のトレードオフとなることが想定され、認証機関の責任に関しては不明である。

5.2.4. 署名付文書に係わる問題

署名付文書に係わる問題においては、電子署名の推定効に関する検討を行うことが重要である。なお、署名付文書には、長期保存文書が含まれる。

(1) 想定される問題

以下の問題が想定される。

- ・ 署名付文書に関して、その有効期限内に危殆化宣言がなされ、署名付文書の真正性が問題とされた
- ・ 危殆化宣言以後に作成された署名付文書に関して、その有効期限内にもかかわらず、署名付文書の真正性が問題とされた

(2) 論点

上記の問題に関しては、以下のような論点が存在する。

- ・ 危殆化宣言がなされる以前に作成された署名付文書に関して、危殆化宣言がなされる以前の推定効に関しては、CRL に当該公開鍵証明書に掲載がなければ、問題となることはないと推察される
- ・ 危殆化宣言がなされる以前に作成された署名付文書に関して、危殆化宣言がなされた後の推定効に関しては、CRL に当該公開鍵証明書に掲載がなければ、かなりの効力を有すると推察される
- ・ 危殆化宣言がなされる以前に作成された署名付文書に関して、危殆化宣言および事後の対策が完了した後、CRL に当該公開鍵証明書が掲載されれば、効力は非常に少なくなると推察される
- ・ 危殆化宣言後、認証機関が CRL に関連する公開鍵証明書を掲載しない場合、責任を問われる可能性に関しては不明である

上記を総括すると、以下ようになる。

危殆化宣言がなされる以前に作成された署名付文書に関して、危殆化宣言がなされた後も、文書の真正性に係わる推定効全てが消失することはなく、ある程度の推定効は保持される。

5.2.5. その他

(1) 暗号危殆化に係わる政府の責任

暗号危殆化に係わる政府の責任は、暗号危殆化の宣言および電子政府システムの運用に関して発生することが想定される。

(a) 暗号危殆化宣言に係わる政府の責任

政府機関が、適切な時期に暗号危殆化の宣言を行うことが求められる。適切な時期とは、対策の進捗と法的リスク（署名の偽造、なりすまし等が行われる危険）の増大のバランスに依存する。つまり、全く対策が進んでいない時期に宣言を行うと、法的リスクが極端に大きくなるため、ある程度対策が進んだ時期に宣言を行うことが肝要である。逆に、対策に時間を掛けすぎると、対策中の法的リスクが増大する。

(b) 電子政府システムの運用者としての責任

電子政府システムの運用者として、通常的判断力を有しているのであれば、当然に気づき（主観的予見可能性）対応できるであろう処置（回避可能性）があるにもかかわらず、これに対応しない場合（回避義務違反）、管理義務違反が問われることになる。そのため、暗号危殆化の宣言が出されている際に、適切な処置を施さなければならない。

さらに、当該電子政府システムの利用暗号アルゴリズムが、電子政府推奨暗号リストに掲載されておらず早期に危殆化した場合、当該電子政府システムの運用責任者には、他の電子政府システム運用責任者とは別の行政上の責任が問われる可能性がある。

6. 暗号危殆化に備えた対策のあり方

6.1. 想定する対策の対象と体制

暗号危殆化の事前対策および危殆化進行に伴う対策として、電子政府および電子署名法に関係する対策を想定する。具体的に対策を推進する組織としては「暗号監視機関」、「省庁横断的対策推進機関」、「電子政府システム毎の対応チーム」を想定する。

(1) 暗号監視機関

暗号技術の専門家から構成される機関であり、暗号アルゴリズムの危殆化状況を監視するとともに、各レベルにおける技術的事項の集約を行う。ここでは CRYPTREC を想定している。

(2) 省庁横断的対策推進機関

暗号監視機関からの連絡・提言を受けて、政府全体の対応に係わる意思決定を行う政府機関である。ここでは 2005 年 4 月に内閣官房に設置が予定されている国家情報セキュリティセンター等を想定している。

(3) 対応チーム

各電子政府システムに設けられたチームであり、省庁横断的対策推進機関からの指示・支援に基づいて電子政府システムの具体的対策の実行にあたる。省庁担当者、ベンダ、専門家から構成されることを想定している。

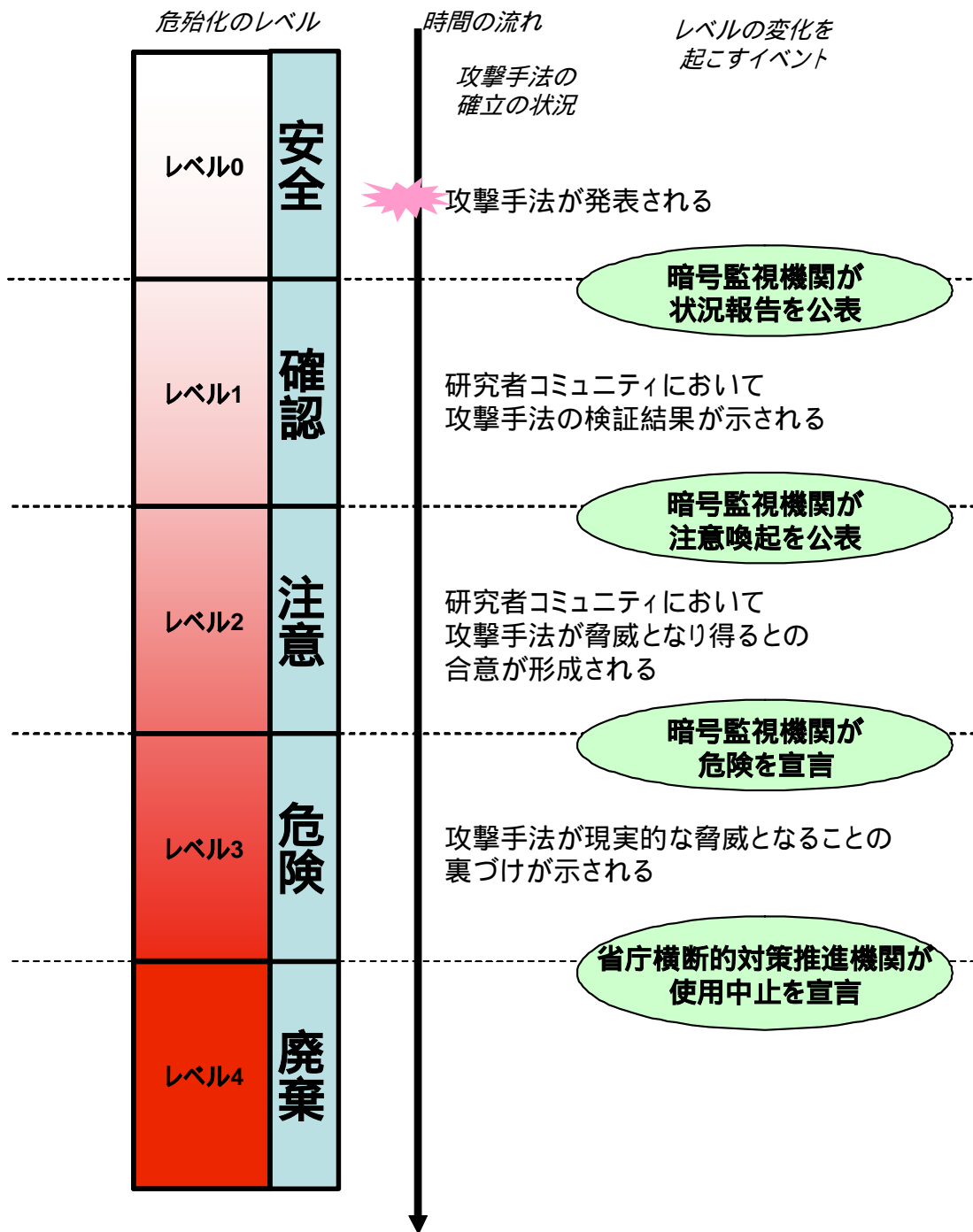
6.2. 暗号危殆化のレベル

2.3 節で述べたように、暗号の危殆化は急激に進行するものではなく、徐々に進行することが一般的である。暗号の危殆化に対する対策は、この特徴を踏まえて進めることが重要である。そこで、暗号アルゴリズムの危殆化の進行に合わせて対策を推進するタイミングを設定するために必要な概念として、暗号危殆化のレベルを表 6-1 のように定義する。また、暗号危殆化のレベルの時間的遷移を図 6-1 に示す。

本定義において、脅威となる攻撃手法とは、現時点の最速の計算機を用いて 5 年後程度で解読が可能となるような攻撃手法を想定する（表 6-1 レベル 2）。ここでの暗号アルゴリズムの危殆化のレベルは、暗号アルゴリズム毎に設定される。また、危殆化レベルは、以前の危殆化レベルを定めた攻撃手法とは異なる攻撃手法によって更に高いレベルに変化し得る。

表 6-1 暗号危殆化のレベル

		レベルの要件
レベル 0	安全	<ul style="list-style-type: none"> 攻撃手法が報告されていない
レベル 1	確認	<ul style="list-style-type: none"> ある攻撃手法が報告されている 暗号監視機関より、上の攻撃手法に関する事実確認と継続的調査が必要との判断が示されている (暗号監視機関により状況報告として公表されている)
レベル 2	注意	<ul style="list-style-type: none"> ある攻撃手法について信頼のおける情報源から検証結果が提示されている 暗号監視機関より、上の検証結果に基づき主に理論的観点からその攻撃手法が近い将来に脅威となり得るとの判断が示されている (暗号監視機関より注意喚起として公表されている)
レベル 3	危険	<ul style="list-style-type: none"> ある攻撃手法について複数の信頼のおける情報源から検証結果が提示されている。 暗号監視機関より、近い将来に上の攻撃手法が実際に運用されるシステムに対して適用された場合に脅威となるとの判断が示されている (暗号監視機関より危険宣言として示されている)
レベル 4	廃棄	<ul style="list-style-type: none"> 省庁横断的対策推進機関において、暗号監視機関の危険宣言を受けた検討を行い、使用を中止すべきと判断している (省庁横断的対策推進機関より使用中止宣言されている) 電子政府における影響分析および移行計画の策定が完了している



(株式会社 三菱総合研究所 作成)

図 6-1 暗号アルゴリズムの危殆化レベルの時間的遷移

6.3. 暗号危殆化のレベルに対応した対策のあり方

暗号危殆化のレベルに対応した、対策のあり方について述べる。概要を図 6-2に示す。

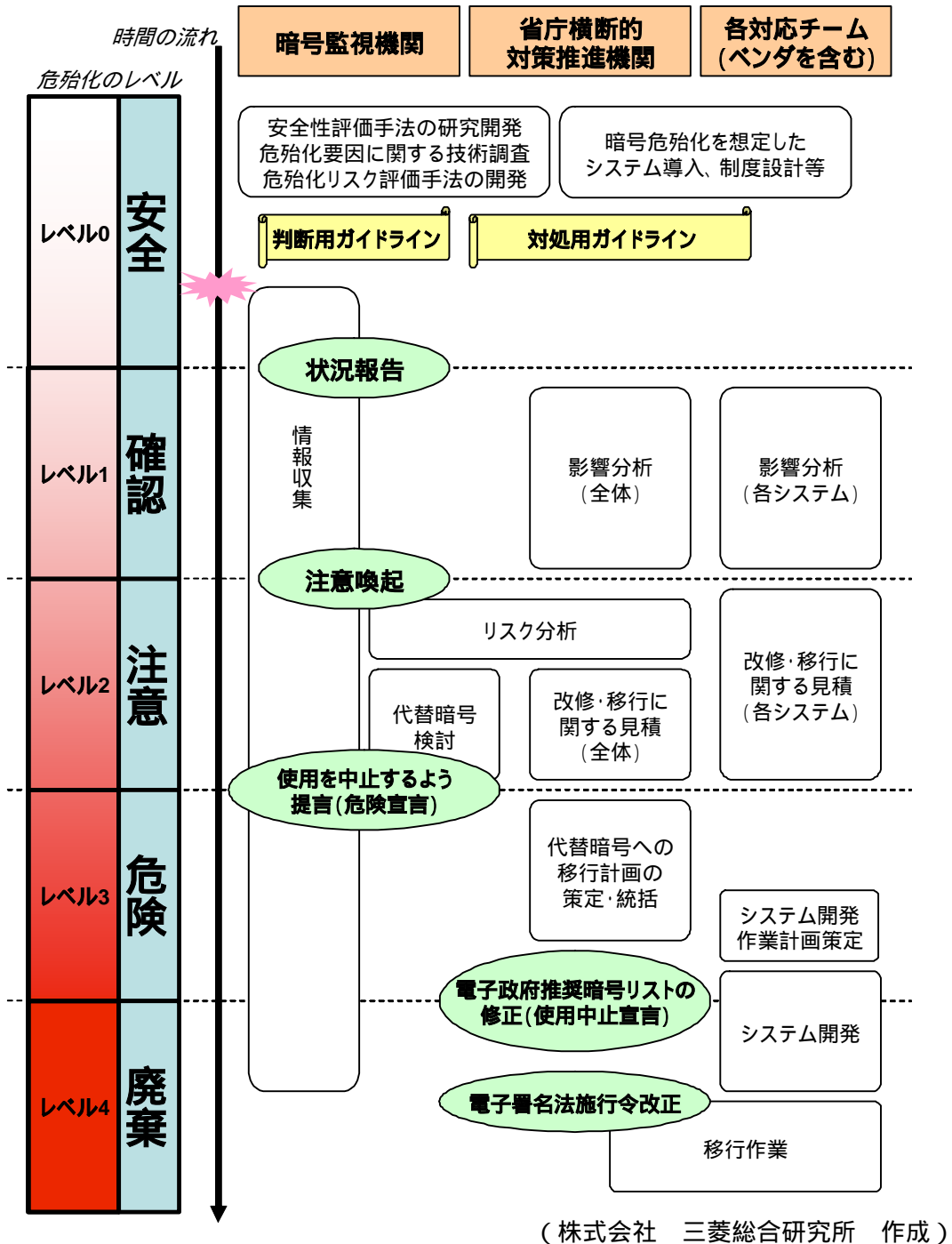


図 6-2 暗号アルゴリズムの危殆化への対策概要

以下に各レベルにおける対策の方向性を述べる。

6.3.1. レベル 0

(1) 暗号監視機関

レベル 0 において暗号監視機関の行う対策の詳細を以下に述べる。

(a) 事前対策

レベル 0 において、暗号監視機関は将来の危殆化の進行に備えた事前対策を推進する。これらには個別のシステムに依存しない以下の対策が含まれる。また、これらの対策は異なる暗号アルゴリズムについて共通化が可能な部分を多く含む。

- ・ 危殆化対策にあたっての暗号監視機関における判断用ガイドラインの策定

(b) 情報収集

レベル 0 において、暗号監視機関は、電子政府システムにおいて利用される暗号に関して、危殆化に係わる情報収集を行う。

以下の関連学会等を含む情報源について、暗号アルゴリズムの危殆化に関する情報を中心に関連動向を観察し分析を行う。

- ・ CRYPTO
- ・ EUROCRYPT
- ・ ASIACRYPT
- ・ SEC
- ・ FSE
- ・ SCIS
- ・ CSEC 等 関連学会
- ・ 研究者による Web ページ
 - <http://www.schneier.com/>
 - <http://www.cl.cam.ac.uk/users/rja14/>
 - <http://theory.lcs.mit.edu/~rivest/>
- ・ 暗号技術関連メーリングリスト

(c) 状況報告

上記の情報収集において、電子政府システムに利用されている暗号の攻撃手法に係わる報告を検知し分析を行った結果、その攻撃手法について今後も特に注目する必要があると判断される場合には、その旨を省庁横断的対策推進機関に伝達するとともに、一般に対して状況報告として公表する。この報告には以下が含まれる。

- ・ 当該暗号アルゴリズムの用途を含む概要

- ・ 当該攻撃手法が電子政府等の実システムに短期的に与える影響の有無
- ・ 当該暗号アルゴリズムに関するこれまでの調査状況
- ・ 現段階において推奨される対応
- ・ 継続的な調査を続ける旨の表明
- ・ 省庁横断的対策推進機関に伝達した旨の表明

(2) 省庁横断的対策推進機関

(a) 事前対策

レベル0を目安に、省庁横断的対策推進機関は、将来の危殆化の進行に備えた事前対策を行う。

- ・ 後述するレベル3、レベル4における対策推進のための対処用ガイドラインの整備

(b) 連絡

省庁横断的対策推進機関は、暗号監視機関から状況報告を受けた場合、各省庁に対して、特定の暗号アルゴリズムの攻撃手法が発見された旨の連絡を行うと共に、関係省庁を通じて、各電子政府システムに関する対応チームの結成を促す。

(3) 電子政府システム毎の対応チーム

レベル0において、対応チームは結成されていない。省庁横断的対策推進期間の連絡を各省庁が受けたことを機会として、電子政府システム毎に対応チームが結成される。

6.3.2. レベル 1

(1) 暗号監視機関

(a) 情報収集

レベル 1 において、暗号監視機関は、注意喚起の対象となった暗号アルゴリズムについて、レベル 0 に示した情報収集に加えて、特に手法を検証する報告や手法を補強する情報の収集に努める。必要であれば専門家へのヒアリングを行う。

(b) 攻撃手法の検証・分析

レベル 1 において、暗号監視機関は、収集した情報を基に、攻撃手法が確立しうるかをディスカッション等で集中的に検証する。また、この段階において攻撃の成立に要するコストについて、レベル 0 において事前に収集した情報を基に概算を試みる。

(c) 注意喚起

暗号監視機関は、情報収集に基づく検討により、攻撃手法が有効な攻撃手法として確立したとの見解の一致を得た場合には、省庁横断的対策推進機関に対して当該暗号アルゴリズムについてはその安全性に懸念がある旨を連絡し、将来の使用の中止を視野に入れた影響分析およびリスク分析を開始するよう提案する。また、一般に対しても調査および検討の結果を公表する。この内容には以下が含まれる。

- ・ 当該暗号アルゴリズムの用途を含む概要
- ・ 当該攻撃手法が電子政府等の実システムに与える短期的影響の有無
- ・ 当該暗号アルゴリズムに関するこれまでの調査状況
- ・ 現段階において推奨される対応
- ・ 省庁横断的対策推進機関に連絡を行った旨の表明

(2) 省庁横断的対策推進機関

(a) 影響分析

レベル 1 を目安に、省庁横断的対策推進機関は、暗号アルゴリズム危殆化による、電子政府システム全体における影響を把握するため、影響分析を開始する。電子政府に含まれるシステムに関して以下を分析の対象とする。

- 1) 電子政府システムへの影響
- 2) 電子政府システムに関連する外部システムに係わる影響

- 3) 利用者（申請者、省庁内決裁担当者等）への影響
- 4) 社会的影響

上記のうち、1)～3)に関しては、電子政府システム毎の対応チームと連携し、各対応チームより提供される中間報告を総合して、電子政府における危殆化の影響の全体像の導出に努める。4)については電子政府を起点とした危殆化の脅威および対策の進行が社会に及ぼす影響について分析を行う。

(b)連絡

省庁横断的対策推進機関は、暗号監視機関から注意喚起を受けた場合に、各省庁および電子政府システム毎の対応チームに対して、その旨を連絡する。

(3)電子政府システム毎の対応チーム

レベル1を目安に、各省庁において電子政府システム毎に対応チームが結成される。このチームにはベンダが含まれる。各電子政府システムの対応チームは、以下の対策を行う。

(a)影響範囲の特定

レベル1を目安に、電子政府システム毎の対応チームは、当該電子政府システムにおいて、省庁横断的対策推進組織より連絡を受けた暗号アルゴリズムの利用箇所を調査し、モジュールレベルまで特定する。

調査結果は、省庁横断的対策推進機関にフィードバックする。

(b)影響の分析

レベル1を目安に、電子政府システム毎の対応チームは、以下の観点から各電子政府システムに関する影響分析を行い、省庁横断的対策推進組織に結果をフィードバックする。

- ・ 当該電子政府システムにおいて影響を受ける機能
- ・ 当該電子政府システムの利用者への影響（利用頻度、利用者数）

6.3.3. レベル 2

(1) 暗号監視機関

(a) 情報収集

レベル 2 において、暗号監視機関は、当該暗号アルゴリズムに係わる情報収集を引き続き行う。特に複数の信頼のおける情報源から攻撃手法についての検証結果と、攻撃手法が実システムに適用可能となる可能性についての判断材料を集める。

(b) 代替暗号アルゴリズムに係わる検討

レベル 2 を目安に、暗号監視機関は、省庁横断的対策推進機関と連携し、暗号アルゴリズムの切り替えに係わる検討を行う。以下の項目については暗号監視機関が中心となって検討を進める。

- ・ 代替暗号アルゴリズム
- ・ 各電子政府システムに共通する対処方法
- ・ ブラウザ等の基本ソフトウェアに関する留意事項

(c) 危険宣言

暗号監視機関は、当該暗号アルゴリズムに関する継続的な情報収集と検討に基づき、近い将来に攻撃手法が実際に運用されるシステムに対して適用された場合に脅威となるとの判断を下す。

この時点で、当該暗号アルゴリズムの使用が危険であることを省庁横断的対策推進機関に連絡するとともに、使用を中止して代替暗号への移行等の対策を加速するよう提案を行う。また、一般に向けて公表する。

(2) 省庁横断的対策推進機関

(a) 各種の見積

レベル 2 を目安に、省庁横断的対策推進機関は、電子政府システム毎の対応チームと連携の上、電子政府システム全体に関して以下の見積を行う。

- ・ ソフトウェア改修規模（時間およびコスト）
- ・ ハードウェア・ネットワークを含めたシステム移行規模（時間およびコスト）

(b) リスク分析

レベル 2 を目安に、省庁横断的対策推進機関は、暗号監視機関と連携しリスク分析を行

う。電子政府システム毎の対応チームより得た情報を基に、以下のリスクを分析する。

- ・ 危殆化暗号の利用を続けた場合のリスクの評価
- ・ 代替暗号への移行に伴うリスクの評価

この分析結果は代替暗号への切り替え時期の検討に用いる

(c) 移行計画の策定

レベル2を目安に、省庁横断的対策推進機関は、暗号監視機関と連携し、暗号アルゴリズムの切り替えに係わる検討を行う。以下の項目については省庁横断的対策推進機関が中心となって検討を進める。

- ・ 電子政府システム全体に関する計画（システム開発、移行作業）
- ・ 各電子政府システムにおける切り替えコスト
- ・ 各電子政府システムの対応チーム向け、切り替え作業マニュアル

(3) 電子政府システム毎の対応チーム

(a) 改修・移行に関する見積

レベル2を目安に、電子政府システム毎の対応チームは、各電子政府システムに関して以下の見積を行う。

- ・ ソフトウェア改修規模（時間、コスト、人員規模）
- ・ ハードウェア・ネットワークを含めたシステム移行規模（時間、コスト、人員規模）
- ・ 改修・移行に伴う影響の推定

6.3.4. レベル 3

(1) 暗号監視機関

(a) 情報収集

レベル 3 においては代替暗号アルゴリズムに関する情報収集を中心とする。

(b) 使用中止宣言に係わる検討への支援

レベル 3 において暗号監視機関は、省庁横断的対策推進機関に協力して、使用中止宣言に係わる検討に加わる。

(2) 省庁横断的対策推進機関

(a) 代替作業の統括

レベル 3 において、省庁横断的対策推進機関は、省庁および電子政府システム毎の対応チームと連携の上、代替作業を統括する。この段階における代替作業は、ソフトウェアおよび暗号モジュールの改修を想定する。具体的には、以下を実施する。

- ・ 共通的事項の共有化（ブラウザ、ライブラリ等に関する修正にかかわる情報等）
- ・ 全体スケジュールの管理

(b) 移行計画の策定

レベル 3 を目安に、省庁横断的対策推進機関は、電子政府システム毎の対応チームと連携の上で移行計画を策定する。移行計画には、以下が含まれる。

- 1) ソフトウェアまたは暗号モジュールの改修
 - ・ 電子政府システム全般において共通する改修箇所の対処法
 - ・ 一般的な改修方法
 - ・ 電子政府システム全体の改修規模
 - ・ スケジュール
- 2) システム全体
 - ・ リプレースすべきハードウェアやネットワーク
 - ・ 全体テスト計画
 - ・ 電子政府システム全体での結合テスト
 - ・ 利用者を含む総合テスト（移行期間）

- ・スケジュール

3) その他

- ・移行時の推進体制
- ・移行期間における問題のフィードバック方法の検討

(c) 使用中止宣言に係わる検討

レベル3において省庁横断的対策推進機関は、暗号監視機関の協力を受け、使用中止宣言に係わる検討を行う。基本的には電子政府システム全体において、ソフトウェアおよび暗号モジュールの改修に目処が立った時点で使用中止宣言を行う。

(d) 使用中止宣言

上述したように、電子政府システム全体で、ソフトウェアまたは暗号モジュールの改修に目処が立った時点で、当該暗号アルゴリズムの電子政府における使用中止を推奨する旨を一般に公表する。当該暗号アルゴリズムを電子政府推奨暗号リストから削除する。

(3) 電子政府システム毎の対応チーム

(a) ソフトウェアまたは暗号モジュールの基本設計

改修すべきソフトウェアまたは暗号モジュールの基本設計を行う。

(b) 作業計画の策定

電子政府システム毎の対応チームは、システム開発に関する作業計画を策定する。計画には、以下が含まれる。

1) ソフトウェアまたは暗号モジュール改修

- ・ 電子政府システムを共通して改修すべき箇所
- ・ 一般的な改修方法
- ・ 電子政府システム全体の改修規模
- ・ スケジュール

2) システム全体

- ・ リプレースすべきハードウェアやネットワーク
- ・ 単独テスト計画
- ・ 他のシステムとの連携を含む結合テスト計画（テスト項目、実施体制、スケジュール）

- ・ 利用者を含む総合テスト計画（テスト項目、実施体制、スケジュール）
- ・ 移行時の推進体制
- ・ スケジュール

(c)ソフトウェアまたは暗号モジュール改修

レベル3において、電子政府システム毎の対応チームは、ソフトウェアまたは暗号モジュールの改修を行う。詳細設計、開発作業、単独テストを実施する。

6.3.5. レベル 4

(1) 暗号監視機関

(a) 移行作業に伴う技術的情報の収集と検討

レベル 4 における暗号監視機関は、移行に伴う技術的問題が発生した場合に、情報の集約および検討を行う。

(2) 省庁横断的対策推進機関

(a) 移行作業の統括

省庁横断的対策推進機関は、移行作業の統括を行う。特に、省庁間をまたがる結合テストおよび利用者を含む総合テストに関しては、スケジュール等の細部の調整を行う。さらには、技術的共通事項の集約も行う。

(b) 電子署名及び認証業務に関する法律施行規則の改定作業

必要に応じて、省庁横断的対策推進機関は、法務省、総務省、経済産業省と連携の上、電子署名及び認証業務に関する法律施行規則の改定作業を実施する。

(3) 電子政府システム毎の対応チーム

(a) 移行作業の実施

電子政府システム毎の対応チームは、移行作業を実施する。

(b) CRL への掲載

各省庁認証局においては、失効する証明書の CRL への掲載を行う。

7. 提言

7.1. 内容

電子政府システムの円滑な運用、および民間における電子商取引の安全な運用に鑑み、関係機関においては、以下の事項の早急な対応が望まれる。

(1) 暗号の危殆化に対する対応の認識

暗号の危殆化に対する制度的・技術的対応が必要である。具体的には、以下の方向での対応が望ましい。

- ・ 危殆化の進行に合わせた対応

暗号の危殆化については、攻撃手法の確立状況による危殆化の進行度をはかり、それに合わせた対処を考慮すべきである。具体的には、安全時、確認を要する事態、今後の使用に際して注意を要する事態、使用に際して明らかな危険が伴う事態、電子政府等において速やかな廃棄を進める事態のそれぞれに分けて、制度的・技術的対応策を検討すべきである。

- ・ 暗号アルゴリズム、暗号モジュール、暗号利用システムのそれぞれにおける対応

暗号の危殆化は、暗号アルゴリズム、暗号モジュール、暗号利用システムそれぞれに分けて考えることが可能である。

(2) 暗号アルゴリズムの危殆化に備えた体制整備

暗号アルゴリズムの危殆化に備えた体制整備に関しては、以下の機関を設置することが望まれる。

- ・ 暗号アルゴリズムの危殆化を監視する機関（暗号監視機関）

暗号アルゴリズムの危殆化状況を監視し、分析に基づいて状況を公表し、電子政府等に暗号アルゴリズムの使用に関する提言を行う機関が必要である。

- ・ 暗号アルゴリズムの危殆化宣言を受け対応する省庁横断的対策推進機関

上記の暗号アルゴリズムの危殆化を監視する機関による提言を受けて、電子政府システム全体における対策を検討する省庁横断的な機関が必要である。

- ・ 暗号アルゴリズムの危殆化の事後対応を行う各システムの対応チーム

電子申請等の個別の電子政府システムに関しては、それらに係わる省庁担当者、ベンダ、インテグレータ、有識者等から成るチームによる対応が必要である。

(3) 各種ガイドラインの整備

以下のガイドラインを整備することが望ましい。

(a) 暗号監視機関向けガイドライン

内容は、以下を想定している。

1. 暗号危殆化の定義
2. 暗号危殆化を判断する機関
3. 暗号危殆化を検知する方法
4. 暗号危殆化の判断基準
5. 暗号危殆化の宣言の時期と方法

(b) 省庁横断的機関向けガイドライン

内容は、以下を想定している。

1. 暗号危殆化の定義
2. 暗号危殆化に備えた措置
内容例
 - ・複数の暗号の併用
 - ・切替機能の実装
3. 暗号危殆化発生時の措置
 - 3.1. 緊急措置
内容例
 - ・CRL への追加
 - ・利用者への告知 等
 - 3.2. 通常措置
内容例
 - ・暗号の切替
 - ・利用者への告知 等

7.2. 優先度またはスケジュール

上記 7.1 の提言に関しては、以下のスケジュールで実行することが望まれる。

- 1) 産業界、学会、世間一般に対する暗号アルゴリズム危殆化への対処必要性アピール
- 2) 暗号アルゴリズムの危殆化に備えた体制整備
- 3) 各種のガイドラインの整備

2005 年度以降のこれらに係わるスケジュール案を、表 7-1 に提案する。

表 7-1 提言に係わる事項のスケジュール案

	2005 年度		2006 年度		2007 年度 以降
	上期	下期	上期	下期	
必要性アピ ール				→	
	ワークショップ等開催				
体制整備		→			
	全体の枠組みの検討				
	暗号監視機関発足				
		→ 各組織等の詳細検討			
		省庁横断的対策推進組織の発足			
		各省庁と連携し順次活動開始			
各種ガイド ライン整備		→			
	暗号監視機関向け ガイドライン整備				
				→	
			省庁横断的対策推進組織向け ガイドライン整備		