7-3　CRYPTREC 活動と電子政府推奨暗号リスト改定

黒川貴司　金森祥子　野島　良　大久保美也子　盛合志帆

本稿では 2011 年度から 2015 年度までの間にセキュリティ基盤研究室が主に担当した CRYPTREC 活動について紹介する。本稿では、2002 年度に「電子政府推奨暗号リスト」として策定し、2012 年度に改定した「CRYPTREC 暗号リスト」に焦点を合わせるが、リスト改定後の現在の CRYPTREC 活動概要についても触れる。

1　まえがき

CRYPTREC とはCryptography Research and Evaluation Committees の略であり、暗号技術の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。第 2 期中期計画時に開始された電子政府推奨暗号リストの改定作業*1 は、第 2 期中期計画と第 3 期中長期計画にまたがって行われた。また、電子政府推奨暗号リストの改定前後で、CRYPTREC の体制に変更があり、活動内容にも変更があった。本稿では、はじめに、**2** において CRYPTREC の体制について述べ、次に、**3** において電子政府推奨暗号リストの改定について述べ、**4** において、第 3 期中期計画における活動内容について述べ、最後に、今後の課題について述べる。

2　CRYPTREC の体制

2.1　2009 年度から 2012 年度までの体制

電子政府推奨暗号リストの改定に向けて、2009 年度から図 1 のとおり組織改編を行った。以下では、セキュリティ基盤研究室が主に担当した暗号方式委員会に係る活動内容について記す。

暗号方式委員会

電子政府推奨暗号リストに記載されている暗号技術の安全性に関する監視、電子政府推奨暗号リストの改定に向けた暗号技術の安全性評価及び将来、電子政府での利用が見込まれる暗号技術の調査・検討を行う。

暗号実装委員会*2

電子政府推奨暗号に準拠した暗号モジュールに対するセキュリティ要件・試験要件の策定及び電子政府推奨暗号リストの改定に向けた実装性評価に関する調査・検討を行う。

暗号運用委員会*2

新しい電子政府推奨暗号リスト（以下、CRYPTREC 暗号リスト*3 という。）を策定するにあたり設置された委員会で、電子政府システム等で利用される CRYPTREC 暗号リストの適切な運用について、システム設計者・運用者の観点から調査・検討を行う。

2.2　2013 年度から 2015 年度までの体制

電子政府推奨暗号リスト改定後の 2013 年度から図 2 のとおり組織改編を行った。以下では、セキュリティ基盤研究室が主に担当した暗号技術評価委員会に係る活動内容について記す。

暗号技術評価委員会

2009 年度から 2012 年度まで設置された暗号方式委員会における活動内容と、暗号実装委員会の一部の活動内容を引き継ぎ、2013 年度に設置された委員会で

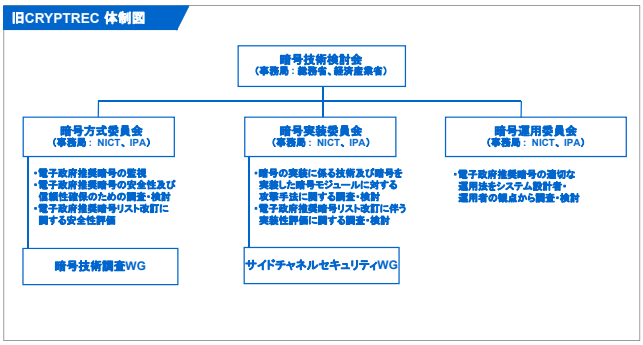


図 1　旧 CRYPTREC 体制図（2009 年度から 2012 年度まで）

＊1　第 2 期中期計画（2006 年度から 2010 年度まで）においてセキュリティ基盤研究室が主に担当した CRYPTREC 活動内容については［1][4]-[9]において詳しく説明をした。
＊2　独立行政法人情報処理推進機構が主担当であった。
＊3　2012 年度の改定前までは仮称としていたが、2012 年度の改定時に、正式に「CRYPTREC 暗号リスト」と称することになった。

は、具体的には、下記の(1)～(3)に関する調査・検討を行う。

(1) 暗号技術の安全性及び実装に係る監視及び評価
(2) 新世代暗号に係る調査(軽量暗号、耐量子計算機暗号等)
(3) 暗号技術の安全な利用方法に関する調査(技術ガイドラインの整備、学術的な安全性の調査・公表等)

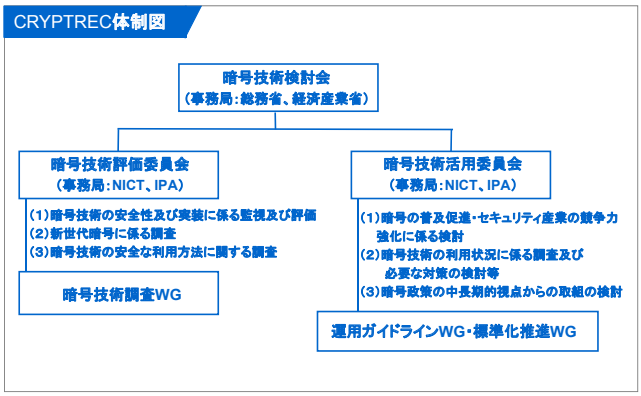


図2　CRYPTREC体制図(2013年度から2015年度まで)

暗号技術活用委員会

2009年度から2012年度まで設置された暗号運用委員会における活動内容と、暗号実装委員会の一部の活動内容を引き継ぎ、2013年度に設置された委員会では、具体的には、下記の(1)～(3)に関する調査・検討を行う(2013年度及び2014年度)。

(1) 暗号の普及促進・セキュリティ産業の競争力強化に係る検討
(2) 暗号技術の利用状況に係る調査及び必要な対策の検討等
(3) 暗号政策の中長期的視点からの取組の検討

また、2015年度からは、情報システム全体のセキュリティ確保に寄与することを目的として、運用マネジメントの作成やメンテナンスのための調査・検討を行うための取り組みをはじめた。

2.3　委員会の開催状況

2011年度から2015年度までの委員会など各会合の開催日は表1(1)(2)のとおりである。

表1　第3期中長期計画における委員会開催日一覧(1)

	平成23年度		平成24年度	
暗号方式委員会	第1回	平成23年8月5日	第1回	平成24年6月8日
	第2回	平成24年2月24日	第2回	平成24年7月24日
	第3回(合同)	平成24年3月9日	第3回	平成24年10月9日
			第4回	平成25年3月5日
			第5回(合同)	平成25年3月26日
暗号技術調査WG(リストガイド)	第1回	平成23年11月14日	第1回	平成24年8月29日
	第2回	平成24年1月24日	第2回	平成24年12月20日
	第3回(合同)	平成24年3月9日	第3回	平成25年2月25日
			第4回(合同)	平成25年3月26日
暗号技術調査WG(計算機能力評価)	第1回	平成23年10月6日	第1回	平成24年12月21日
	第2回	平成23年12月21日	第2回	平成25年2月22日
	第3回(合同)	平成24年3月9日	第3回(合同)	平成25年3月26日
暗号実装委員会	第1回	平成23年9月12日	第1回	平成24年7月5日
	第2回	平成23年12月19日	第2回	平成24年9月4日
	第3回	平成24年2月13日	第3回	平成24年10月9日
	第4回(合同)	平成24年3月9日	第4回	平成25年3月14日
			第5回(合同)	平成25年3月26日
サイドチャネルセキュリティWG	第1回	平成23年12月19日	第1回	平成24年7月5日
	第2回	平成24年2月13日	第2回	平成25年3月14日
	第3回(合同)	平成24年3月9日	第3回(合同)	平成25年3月26日
暗号運用委員会	第1回	平成23年9月21日	第1回	平成24年6月8日
	第2回	平成23年11月18日	第2回	平成24年7月25日
	第3回	平成24年1月27日	第3回	平成24年10月4日
	第4回	平成24年2月24日	第4回	平成25年3月1日
	第5回(合同)	平成24年3月9日	第5回(合同)	平成25年3月26日
			*利用調査報告会	平成24年9月24日
			*合同委員会(委員長会議)	平成24年11月15日

3 電子政府推奨暗号リストの改定（第 3 期中長期計画分）

CRYPTREC では、第 2 期中期計画の期間内において、主に、

（1）電子政府推奨暗号リスト改訂*4 のための骨子案
（2）電子政府推奨暗号リスト改訂のための暗号技術公募（2009 年度）
（3）第 1 次評価

を実施していた。以下では、第 3 期中長期計画における活動内容について記す。

3.1　第 2 次評価

第 2 次評価とは、第 1 次評価を通過した応募暗号技術に対して継続して行った評価全般及び旧電子政府推奨暗号リストに記載された 128 ビットブロック暗号等に対する再評価のことをいう*5。

応募暗号技術に対して実施した評価は、ソフトウェア実装性能及びハードウェア実装性能であった。ソフトウェア実装性能では、評価項目として、処理速度を中心に初期化時間や使用するメモリ量を測定した。また、ハードウェア実装性能では、評価項目として、クリティカルパス遅延やスループット、実装サイズなどを測定するとともに、サイドチャネル攻撃への対策可能性を検証するため、対策版と未対策版の各々に対する攻撃の有効性と対策コストの評価を行った。なお、これらソフトウェア実装性能及びハードウェア実装性能に関する評価を担当した委員会は暗号実装委員会であり、詳細については、CRYPTREC Report 2011（暗号実装委員会報告）[2] 及び CRYPTREC Report 2012（暗号実装委員会報告）[3] を参照していただきたい。

3.1.1　旧電子政府推奨暗号リストに記載された暗号技術の再評価

2011 年度には、旧電子政府推奨暗号リストに記載された 128 ビットブロック暗号に対して、鍵拡大関数の安全性評価を実施し、関連鍵攻撃に対する安全性評価を目的として鍵拡大関数の差分特性確率の上界を評価した。また、192 /256 ビット鍵の場合の安全性評価を実施し、192 /256 ビット鍵の場合の計算量的安全性を関連鍵攻撃まで想定して概算で見積もるため、差分／線形特性確率の上界を評価した。評価結果において、現実的な脅威になり得る問題は見つからなかった。

また、2012 年度には、128 ビットブロック暗号（応募暗号技術である CLEFIA 及び旧電子政府推奨暗号である AES、CIPHERUNICORN-A、Camellia、Hierocrypt-3、SC2000）を評価対象とし、関連鍵攻撃

*4　CRYPTREC 暗号リスト策定を契機に「改訂」ではなく「改定」を用いるようになった。
*5　狭義の意味では、前者の評価のみを指す。

表 1　第 3 期中長期計画における委員会開催日一覧 (2)

	平成25年度		平成26年度		平成27年度	
暗号技術評価委員会	第 1 回	平成25年 7 月29日	第 1 回	平成26年 8 月 4 日	第 1 回	平成27年11月18日
	第 2 回	平成25年12月13日	第 2 回	平成26年12月25日	第 2 回	平成28年 3 月 8 日
	第 3 回	平成26年 3 月 6 日	第 3 回	平成27年 3 月 2 日		
			第 4 回（合同）	平成27年 3 月20日		
暗号技術調査WG（暗号解析評価）	第 1 回	平成25年 9 月 3 日	第 1 回	平成26年 9 月 2 日	第 1 回	平成28年 1 月22日
	第 2 回	平成26年 2 月20日	第 2 回	平成26年 2 月17日	第 2 回	平成28年 3 月 3 日
			第 3 回（合同）	平成27年 3 月20日		
暗号技術調査WG（軽量暗号）	第 1 回	平成25年 9 月17日	第 1 回	平成26年 8 月29日	第 1 回	平成27年10月20日
	第 2 回	平成25年12月26日	第 2 回	平成26年11月12日	第 2 回	平成27年12月24日
	第 3 回	平成26年 2 月20日	第 3 回	平成27年 2 月 2 日	第 3 回	平成28年 2 月 9 日
			第 4 回（合同）	平成27年 3 月20日		
暗号技術活用委員会	第 1 回	平成25年 9 月11日	第 1 回	平成26年10月30日	第 1 回	平成28年 3 月 2 日
	第 2 回	平成25年12月13日	第 2 回	平成27年 1 月26日		
	第 3 回	平成26年 3 月19日	第 3 回	平成27年 3 月10日		
			第 4 回（合同）	平成27年 3 月20日		
運用ガイドラインWG	第 1 回	平成25年10月10日	第 1 回	平成26年10月17日		
	第 2 回	平成25年12月 4 日	第 2 回	平成26年12月16日		
	第 3 回	平成26年 3 月12日	第 3 回	平成27年 2 月25日		
			第 4 回（合同）	平成27年 3 月20日		
標準化推進WG	第 1 回	平成26年 2 月10日	第 1 回	平成26年10月15日		
	第 2 回	平成26年 2 月10日	第 2 回	平成26年12月11日		
			第 3 回	平成27年 2 月23日		
			第 4 回（合同）	平成27年 3 月20日		

及び中間一致攻撃（Biclique 攻撃を含む）に関して評価を行った。評価結果において、現実的な脅威になり得る問題は見つからなかった。

また、ストリーム暗号 128 ビット鍵 RC4 を、SSL3.0 /TLS1.0 以上で利用する際の安全性評価を実施し、Broadcast セッティング（同じ平文を多数の異なる鍵で暗号化して送信するような場合）では、全てのバイトの平文を導出する攻撃が報告され、現実的な脅威になり得ることが判明した。詳細については、CRYPTREC Report 2011（暗号方式委員会報告）[4] 及び CRYPTREC Report 2012（暗号方式委員会報告）[5] を参照していただきたい。

3.2　選定ルールのフレームワーク

2012 年度の暗号方式委員会では、2011 年度の暗号技術検討会において承認された「電子政府推奨暗号選定のための選考基準案」[6] に基づき、暗号技術の評価を行う必要があった。暗号方式委員会における検討内容については、下記の小節において説明をするが、その前に、暗号を選定するためのフレームワークについてのみ概説しておく。なお、詳細について、暗号運用委員会での審議内容は、CRYPTREC Report 2011（暗号運用委員会活動報告）[7] 及び CRYPTREC Report 2012（暗号運用委員会活動報告）[8] を、また、暗号技術検討会での審議内容は、暗号技術検討会 2012 年度報告書 [9] を参照いただきたい。

2011 年度暗号運用委員会の活動報告 [7] をもとに、2011 年度の暗号技術検討会にて次期電子政府推奨暗号選定のため選考基準案についての審議を行った結果、次期電子政府推奨暗号を以下の考え方（表 2）により選定することが了承された。

この選考基準に基づき、以下の方法により選定することになった（図 3）。

- (i) により選定される可能性がある暗号技術は、評価 A において「現在の利用実績が十分である」と判断されたものである（選定ルート①を通るもの）。
- (ii) により選定される可能性がある暗号技術は、評価 B により「現在の利用実績は十分とは言えないが、今後の利用促進の可能性が高い」と判断されたものである（選定ルート②③を通るもの）。

3.2.1　基本的方針

承認された選定ルールのフレームワークにおいて、暗号方式委員会が検討する必要があったのは次の 3 項目である（図 3 内の青矢印）。

1）「安全性評価」
　評価対象の暗号技術が電子政府での利用において安全性上問題がないかを評価し、推奨候補暗号リストに入れるか、リスト対象外とするかを判定する。

2）「評価 B」
　「評価 A」で利用実績が十分でないと判定された暗号技術について、今後の利用促進の可能性が高いかどうかを判定するための 1 項目として、「安全性」に関して「市場が認める程度の技術的アドバンテージがあるか」を判定する。

表 2　選考基準

<table>
<tr><td>選考基準の考え方</td><td colspan="2">国際標準化・製品化促進の手段として電子政府推奨暗号リストを活用</td></tr>
<tr><td></td><td colspan="2">「安全性」、「現状の調達容易性（利用実績）」、「将来的な調達容易性（利用実績）」の見通しを踏まえつつ、電子政府推奨暗号リストの掲載個数を限定したうえで、提案暗号の普及展開をどのように進めるべきかといった「非技術的なその他要件」を最大限加味</td></tr>
<tr><td></td><td colspan="2">米国政府標準暗号以外の暗号は国際標準化や規格化、製品化からも排除される流れが強まっている点を考慮。提案暗号に対する国としてのバックアップの明確化</td></tr>
<tr><td>選考基準</td><td colspan="2">(i)すでに現状の調達容易性（利用実績）が十分に高く、かつ将来的な安全性にも十分な余裕度があって、今後も安定して利用できる見込みがある暗号技術を選定する。</td></tr>
<tr><td></td><td rowspan="3">(ii)現状の調達容易性（利用実績）は十分に高いとは言えないものの、以下の3条件すべてを満たす暗号技術を選定する。</td><td>(i)で選定される暗号技術のなかで最も高い安全性を有するものと同等かそれ以上の安全性を有すると評価される。</td></tr>
<tr><td>今後の普及展開支援によって、国際標準化・製品化促進が図られると期待できる根拠がある。</td></tr>
<tr><td>今後の普及展開支援によって、将来的な調達容易性（利用実績）が十分に高くなると期待できる根拠がある。</td></tr>
</table>

引用：暗号技術検討会 2011 年度報告書 [6]

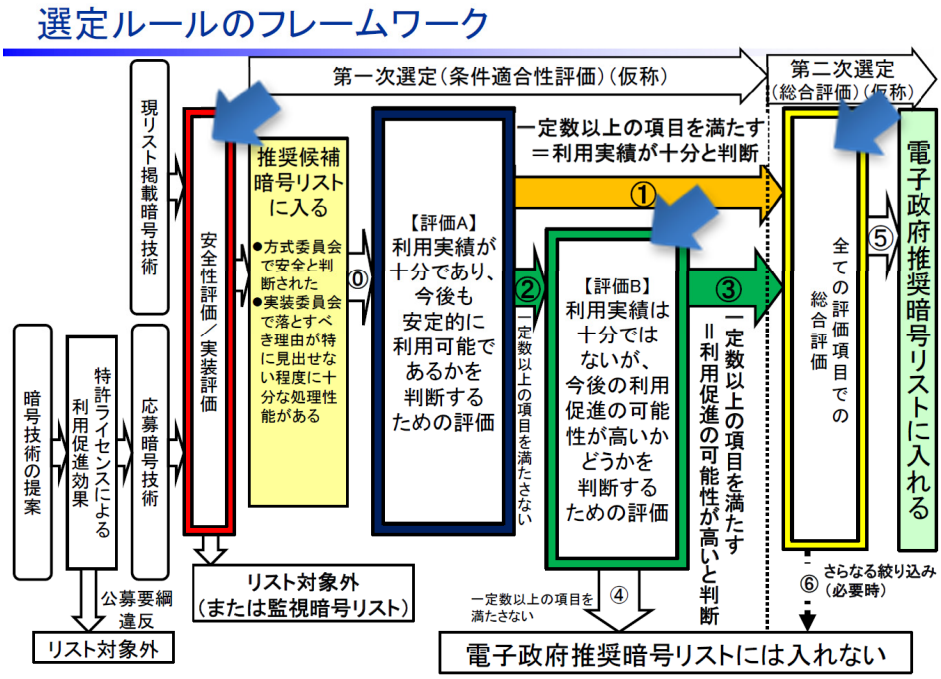


図３　選定ルールのフレームワーク
図の中の丸数字⓪～⑥は選定の順番を意味する。

表３　安全性に係る判定方針

①リスト（2002 年度版）に記載されている暗号技術に対する選定方針	（ア）監視結果等から判断して、リスト（2002 年度版）策定時における安全性評価結果が現在も妥当と判断されること。ただし、新たな攻撃方法等が提案されている場合、それらに対しても安全性に関して問題がないと判断されること。
	（イ）注釈が付いている場合、その内容が現在も妥当かどうかを検討した上で、安全性に問題がないと判断されること。
	（ウ）（ア）及び（イ）を満たさない場合、原則として運用監視暗号リストに含める。
②2009 年度応募暗号技術に対する選定方針	（ア）安全性評価結果（今年度に評価を実施する場合はそれも含む）に関して問題がないこと。
	（イ）（ア）を満たさない場合、次期リストの選考外とする。
③事務局選出暗号技術に対する選定方針	（ア）安全性評価結果（今年度に評価を実施する場合はそれも含む）に関して問題がないこと。
	（イ）（ア）を満たさない場合は、原則として次期リストの選考外とする。

3）「総合評価」

本評価は、更なる絞り込みを行うために設けられたものである。評価項目の「技術的側面」の２項目「安全性についての仕様上のアドバンテージ」と「論文数の多寡によるアドバンテージ」の採点を行う。今回は、暗号技術検討会にて不要と判断されたため実施されなかった。

3.2.2 「安全性評価」判定方法

検討の対象となっている暗号技術には、①リスト（2002 年度版）に記載されている暗号技術、② 2009 年度応募暗号技術（128 ビットブロック暗号／ストリーム暗号／メッセージ認証コードの３つの暗号カテゴリを含む）、③事務局選出暗号技術（メッセージ認証コード／暗号利用モード／エンティティ認証の３つの暗号カテゴリを含む）、の３つがある。暗号方式委員会では安全性に係る判定方針を表３の①～③のとおり決定した。

3.2.3 「評価 B」「総合評価」に関する評価項目・配点

（1）「評価 B」に関する評価項目について

「評価 B」において、今後の利用促進の可能性が高いかどうかを判定するための１項目として「市場が認める程度の技術的アドバンテージがあるか」（以下、技術的アピールポイント）が設けられた*6。暗号方式委員会では、「安全性」に関する技術的アピールポイントとして、表４

*6　技術的アピールポイントは、安全性と実装性能の２つの観点があり、それぞれ暗号方式委員会と暗号実装委員会が評価し、少なくとも一方で「アドバンテージがある」と判断すれば、技術的アピールポイントがあると判定する。

表４　「技術的アピールポイント」に係る評価方針及び評価項目

「技術的アピールポイント」に係る評価方針	● 同じ暗号カテゴリにおける他の暗号アルゴリズムと比べて、安全性に関して事務局が指定する範囲のいずれかの評価項目において、技術的に優れている点が存在するかどうかの判定を行う。なお、応募者への問い合わせ内容において、事務局が指定する範囲外の評価項目が存在する場合は、暗号方式委員会にて承認があれば認めるものとする。
	● 応募暗号技術の場合は、応募者にその旨を問い合わせる。それ以外の場合は、事務局が調査する。
	● その内容の妥当性を暗号方式委員会が認めた場合、「技術的アピールポイント」があるものと判定する。
「技術的アピールポイント」に係る評価項目	● 証明可能安全性の有無や安全性評価の容易性
	● 安全性証明における仮定の妥当性
	● 安全性証明の帰着効率
	● 鍵の全数探索等よりも効率のよい攻撃の有無
	● 安全性マージン（現時点での最長攻撃可能段数）
	● 安全性に関連する利用上の制限の有無
	● 提案論文が採録された国際会議・論文誌

のとおり評価方針及び評価項目を設定した。

(2)「総合評価」に関する評価項目について

「総合評価」の評価項目「安全性についての仕様上のアドバンテージ」に関する評価方針は表５のとおり了承された。また、「総合評価」の評価項目「論文の多寡によるアドバンテージ」に関する評価方針は表６のとおり了承された。なお、被引用数をポイントへ換算する方法としては、提案時から 2012 年８月末時点までの被引用数の値そのものを、配点（20 点）を上限としてポイントとすることとなった。

(3)「総合評価」に関する配点について

「安全性についての仕様上のアドバンテージ」と「論文の多寡によるアドバンテージ」の配点について、「論文の多寡によるアドバンテージ」は「安全性についての仕様上のアドバンテージ」における各評価項目と同等の扱いとし、「安全性についての仕様上のアドバンテージ」における評価項目の総数がＮ個の場合、当該比率をＮ対１と決定した。了承された配点に基づき、「総合評価」の評価項目「安全性についての仕様上のアドバンテージ」「論文の多寡によるアドバンテージ」の配点は表７のとおりとなった。

3.3　「安全性評価」判定結果と CRYPTREC 暗号リスト

承認された選定ルールのフレームワークでは、評価Ａ、評価Ｂ及び総合評価に掛ける前に、リスト（2002 年度）、新規応募暗号及び事務局選出暗号を、推奨候補暗号または運用監視暗号に分類する必要がある。暗号方式委員会では、表８のとおり推奨候補暗号か否かについての判定を行った。

その後、暗号方式委員会、暗号実装委員会及び暗号運用委員会の３つの委員会による評価結果をもとに作成された「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）（案）」が暗号技術検討会にて承認され、パブリックコメントを募集することが決定された。そして、確定したリストは、2013 年３月１日（金）に総務省及び経済産業省から公表された（表９）。

4　暗号技術評価委員会の活動内容

2013 年度からは、名称を「暗号方式委員会」から「暗号技術評価委員会」と変更し、暗号技術の安全性評価を中心とした技術的な検討、すなわち、

(a) 新世代暗号に係る調査（軽量暗号、セキュリティパラメータ、ペアリング、耐量子計算機暗号等）
(b) 暗号技術の安全性に係る監視及び評価
(c) 暗号技術の安全な利用方法に関する調査（技術ガイドラインの整備、学術的な安全性の調査・公表等）

を実施することになった。下記の小節において主な活動内容を簡単に説明する。

4.1　仕様書の参照先の変更

DSA（NIST FIPS 186-2（+Change Notice）から NIST FIPS 186-4 へ）に関しては、有限体及びハッシュ関数のサイズの拡張は、パラメータ修正等の簡易な修正であると判断し、仕様書の参照先の変更について了承された。

表５　「安全性についての仕様上のアドバンテージ」に関する評価方針

「安全性についての仕様上のアドバンテージ」に関する評価方針	・各暗号カテゴリの評価項目数は同じにする。		
	・各評価項目のポイントの比率は同じとする。		
	・各暗号カテゴリの評価項目は右記のとおりにする（評価項目数は 5）。	(a) 公開鍵暗号	(1) 証明可能安全性の有無
			(2) 安全性証明における仮定の妥当性
			(3) 帰着効率の良し悪し
			(4) 利用上の制限の有無
			(5) 査読付きの国際会議・論文誌で提案論文が採録されたか否か
		(b) 共通鍵暗号（64 ビット及び 128 ビットブロック暗号、ストリーム暗号）	(1) 証明可能安全性の有無または安全性評価の容易性
			(2) 全数探索よりも効率の良い攻撃の有無
			(3) 安全性マージン（最長攻撃可能段数／仕様段数）
			(4) 利用上の制限の有無
			(5) 査読付きの国際会議・論文誌で提案論文が採録されたか否か
		(c) ハッシュ関数	(1) ハッシュ長（256 ビット以上か否か）
			(2) 衝突発見困難性に関する安全性マージン（最長攻撃可能段数／仕様段数）
			(3) 第二原像計算困難性に関する安全性マージン（最長攻撃可能段数／仕様段数）
			(4) 原像計算困難性に関する安全性マージン（最長攻撃可能段数／仕様段数）
			(5) 利用上の制限の有無
		(d) メッセージ認証コード	(1) 証明可能安全性の有無
			(2) 安全性証明における仮定の妥当性
			(3) 帰着効率の良し悪し
			(4) 利用上の制限の有無
			(5) 査読付きの国際会議・論文誌で提案論文が採録されたか否か
		(e) 暗号利用モード	(1) 証明可能安全性の有無
			(2) 安全性証明における仮定の妥当性
			(3) 帰着効率の良し悪し
			(4) 利用上の制限の有無
			(5) 査読付きの国際会議・論文誌で提案論文が採録されたか否か
		(f) エンティティ認証	(1) 証明可能安全性の有無
			(2) 安全性証明における仮定の妥当性
			(3) 帰着効率の良し悪し
			(4) 利用上の制限の有無
			(5) 査読付きの国際会議・論文誌で提案論文が採録されたか否か

表６　「論文数の多寡によるアドバンテージ」に関する評価方針

「論文数の多寡によるアドバンテージ」に関する評価方針	暗号技術が提案された文献の被引用数の多い・少ないを判定する。
	調査対象となる暗号技術に対する安全性評価に関する論文のみを対象とする。安全性評価に関する論文に限定するため、被引用数が多い暗号技術に対しては、サンプリングより被引用数を推定する。
	引用論文の調査範囲は、論文誌または Springer LNCS、IEEE、ACM で論文が出版されている査読付き国際会議とし、調査先は、検索サイト（例：GoogleScholar, http://scholar.google.co.jp/）または既存の学術データベースを利用する。
	引用元である暗号技術が提案された文献に関して複数の候補がある場合には、主要な 3 つの文献に基づいて調査する。また、重複は可能な限り除外する。
	暗号カテゴリ間のポイントのばらつきに起因する調整は行わない。

表 7　「総合評価」に関する配点

「総合評価」に関する配点	安全性についての仕様上のアドバンテージ（各暗号カテゴリ 5 項目）	100
	論文の多寡によるアドバンテージ	20

表 8　「安全性評価」判定結果*7

安全性評価の判定結果	技術分類	名称
推奨候補暗号と判定した暗号技術	署名	DSA, ECDSA, RSA-PSS, RSASSA-PKCS1 -v1 _5
	守秘	RSA-OAEP
	鍵共有	DH, ECDH, PSEC-KEM（注釈付き）
	64 ビットブロック暗号（注釈付き）	CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, 3 -key Triple DES（注釈付き）
	128 ビットブロック暗号	AES, Camellia, CIPHERUNICORN-A, CLEFIA, Hierocrypt-3, SC2000
	ストリーム暗号	Enocoro-128 v2, KCipher-2, MUGI, MULTI-S01（注釈付き）
	ハッシュ関数	SHA-256, SHA-384, SHA-512
	暗号利用モード	CBC, CFB, CTR, OFB, CCM, GCM（注釈付き）
	メッセージ認証コード	CMAC, HMAC, PC-MAC-AES
	エンティティ認証	ISO/IEC 9798 -2, ISO/IEC 9798 -3, ISO/IEC 9798 -4
運用監視暗号と判定した暗号技術	守秘	RSAES-PKCS1 -v1 _5
	ストリーム暗号	128 -bit RC4（注釈付き）
	ハッシュ関数	RIPEMD-160, SHA-1
	メッセージ認証コード	CBC-MAC（注釈付き）

表 9　CRYPTREC 暗号リスト（平成 25 年 3 月 1 日 総務省 経済産業省）
(1) 電子政府推奨暗号リスト　(2) 候補暗号リスト　(3) 運用監視暗号リスト

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するものリスト。

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS（注1）
		RSASSA-PKCS1-v1_5（注1）
	守秘	RSA-OAEP（注1）
	鍵共有	DH
		ECDH
共通鍵暗号	64 ビットブロック暗号（注2）	3-key Triple DES（注3）
	128 ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM（注4）
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

（注1）　「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25 年 3 月 1 日現在）

（注2）　より長いブロック長の暗号が利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3）　3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。
1）NIST SP 800-67 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4）　初期化ベクトル長は 96 ビットを推奨する。

[1] 総務省政策統括官（情報通信担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。
[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM（注6）
共通鍵暗号	64 ビットブロック暗号（注6）	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128 ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01（注7）
ハッシュ関数		該当なし
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		PC-MAC-AES
エンティティ認証		ISO/IEC 9798-4

（注5）　KEM（Key Encapsulating Mechanism）－ DEM（Data Encapsulating Mechanism）構成における利用を前提とする。

（注6）　より長いブロック長の暗号が利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7）　平文サイズは 64 ビットの倍数に限る。

[3] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5（注8）（注9）
	鍵共有	該当なし
共通鍵暗号	64 ビットブロック暗号	該当なし
	128 ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4（注10）
ハッシュ関数		RIPEMD-160
		SHA-1（注8）
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		CBC-MAC（注11）
エンティティ認証		該当なし

（注8）　「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25 年 3 月 1 日現在）

（注9）　SSL 3.0 / TLS 1.0, 1.1, 1.2 で利用実績があることから当面の利用を認める。

（注10）　128-bit RC4 は、SSL（TLS 1.0 以上）に限定して利用すること。

（注11）　安全性の観点から、メッセージ長を固定して利用すべきである。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

*7　後日、RSA と SHA-1 については、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成 20 年 4 月 情報セキュリティ政策会議決定、平成 24 年 10 月情報セキュリティ対策推進会議改訂）に関する注釈が付いた。

4.2　暗号技術活用委員会からの質問に対する回答の検討について

暗号技術活用委員会から、Perfect forward secrecy と forward secrecy に関する技術的見解を求められたため、回答を行った。

4.3　技術ガイドラインの発行

4.3.1　CRYPTREC 暗号技術ガイドライン（SSL/TLS における近年の攻撃）

2013 年度は、SSL/TLS における近年の攻撃に関して、その攻撃手法の概要、システムに対する影響を分析するとともに、暗号スイートにおける安全性の観点での影響について、SSL/TLS に対する近年の攻撃に関するガイドラインを作成した。

4.3.2　CRYPTREC 暗号技術ガイドライン（SHA-1）

電子政府のシステム調達者及び電子政府システムを構築する開発者に向けて、CRYPTREC 暗号リストの運用監視暗号リストに記載されているハッシュ関数 SHA-1 を利用する際に必要となる情報、すなわち、SHA-1 に関する非推奨及び許容事項や参考情報について記載した。

4.4　128-bit key RC4 の注釈の変更について

128-bit key RC4 は、運用監視暗号リストに掲載され、「128-bit RC4 は、SSL（TLS1.0 以上）に限定して利用すること」という注釈が付与されている。近年、報告されている脆弱性を考慮し、「互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること」という変更案が決定された。

4.5　注意喚起レポートについて

CRYPTREC 暗号リストの安全性及び実装に係る技術の監視活動を通じて、国際会議等で発表された攻撃等の概要や想定される影響範囲、対処方法について早期に公開することが望ましいと判断された場合、注意喚起レポートを発行する。暗号技術評価委員会が発行した注意喚起レポートは下記のとおりである。

「擬似乱数生成アルゴリズム Dual_EC_DRBG について」（2013 年 11 月 6 日）[10]

「64 ビットブロック暗号 MISTY1 の安全性について」（2015 年 7 月 16 日）[11]

「64 ビットブロック暗号 MISTY1 の安全性について（続報）」（2015 年 8 月 12 日）[12]

「SHA-1 の安全性について」（2015 年 12 月 18 日）[13]

4.6　ハッシュ関数 SHA-2、SHA-3 の取扱いについて

今後において電子政府システム等での利用が見込まれると判断される暗号技術の追加を検討した。暗号技術評価委員会での審議結果、ハッシュ長が 256 ビット以上のアルゴリズムのみとすることとなった。具体的な対象アルゴリズムは以下のとおり。

SHA-2: SHA-512 /256
SHA-3: SHA3 -256, SHA3 -384, SHA3 -512, SHAKE256

4.7　暗号技術調査ワーキンググループ（暗号解析評価）

公開鍵暗号の安全性は、素因数分解の困難性や離散対数問題の困難性など様々な数学的問題に依存している。このワーキンググループでは、素因数分解問題の困難性及び離散対数問題の困難性の他にも、量子計算機が実現しても安全性が保たれると期待されている「耐量子計算機暗号」を支える数学的問題の困難性に関する調査を行っている。詳しくは、CRYPTREC Report 2013（暗号技術評価委員会活動報告）[14]、CRYPTREC Report 2014（暗号技術評価委員会活動報告）[15] 及び CRYPTREC Report 2015（暗号技術評価委員会活動報告）[16] を参照いただきたい。

4.8　暗号技術調査ワーキンググループ（軽量暗号）

軽量暗号技術が求められるサービスにおいて、電子政府のみならず利用者が最適な暗号方式を選択でき、容易に調達できることを目指し、これまでに提案されている軽量暗号の調査（安全性、実装性能及びアプリケーションの調査など）を行っている。また、軽量暗号を選択・利用する際の技術的判断に資すること、今後の利用促進を図ることを目的とした「暗号技術ガイドライン（軽量暗号）」を発行する予定である。詳しくは、CRYPTREC Report 2013（暗号技術評価委員会活動報告）[14]、CRYPTREC Report 2014（暗号技術評価委員会活動報告）[15] 及び CRYPTREC Report 2015（暗号技術評価委員会活動報告）[16] を参照いただきたい。

5　今後の課題

「電子政府推奨暗号改訂のための骨子案」立案時においては、リストガイドは暗号のリストの中に位置していた（[1] の図 9 を参照のこと）。リストガイドのような、暗号技術の適切な利用方法に関する情報提供をシステム運用者・利用者に対して行う取り組みは、そ

の重要性から現在の CRYPTREC 活動内容においても、暗号技術評価委員会及び暗号技術活用委員会において、技術ガイドライン及び運用ガイドラインとして、それぞれ受け継がれている。しかしながら、現在の CRYPTREC 暗号リストを見る限り、それらのガイドラインとリストとの直接的な結びつきは見られない。これらの取り組みを骨子案に沿うような形に仕上げるために、どのようにして暗号のリストと「一体化」させるのかが今後の課題であると思われる。

6　むすび

本稿では、2011 年度から 2015 年度までの間にセキュリティ基盤研究室が主に担当した CRYPTREC 活動について紹介した。また、電子政府推奨暗号リスト改定する際に実施した評価内容についても紹介した。

謝辞

この場を借りて、今まで CRYPTREC 活動に参加し、暗号アルゴリズムの安全性評価や実装性評価の検討にご協力していただいたすべての方々に感謝する。特に、2014 年度までの長い間、暗号技術評価委員会等の委員長を引き受けてくださり、CRYPTREC 活動を支えていただいた今井秀樹先生に感謝する。

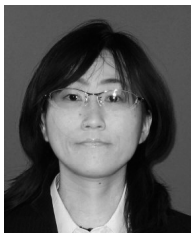
【参考文献】

1　黒川貴司，金森祥子，“4-9 CRYPTREC 活動，”情報通信研究機構季報（ネットワークセキュリティ特集），vol.57 nos. 3/4 2011.
2　CRYPTREC Report 2011（暗号実装委員会報告）
3　CRYPTREC Report 2012（暗号実装委員会報告）
4　CRYPTREC Report 2011（暗号方式委員会報告）
5　CRYPTREC Report 2012（暗号方式委員会報告）
6　暗号技術検討会 2011 年度報告書
7　CRYPTREC Report 2011（暗号運用委員会報告）
8　CRYPTREC Report 2012（暗号運用委員会報告）
9　暗号技術検討会 2012 年度報告書
10　「擬似乱数生成アルゴリズム Dual_EC_DRBG について」（2013 年 11 月 6 日）http://www.cryptrec.go.jp/topics/cryptrec_20131106_dual_ec_drbg.html
11　「64 ビットブロック暗号 MISTY1 の安全性について」（2015 年 7 月 16 日）http://www.cryptrec.go.jp/topics/cryptrec_20150716_misty1_cryptanalysis.html
12　「64 ビットブロック暗号 MISTY1 の安全性について（続報）」（2015 年 8 月 12 日）http://www.cryptrec.go.jp/topics/cryptrec_20150812_misty1_cryptanalysis.html
13　「SHA-1 の安全性について」（2015 年 12 月 18 日）http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html
14　CRYPTREC Report 2013（暗号技術評価委員会報告）
15　CRYPTREC Report 2014（暗号技術評価委員会報告）
16　CRYPTREC Report 2015（暗号技術評価委員会報告）

黒川貴司　（くろかわ　たかし）
サイバーセキュリティ研究所
セキュリティ基盤研究室
技術員
暗号技術の安全性評価

金森祥子　（かなもり　さちこ）
サイバーセキュリティ研究所
セキュリティ基盤研究室
技術員
プライバシー

野島　良　（のじま　りょう）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（工学）
暗号理論、暗号プロトコル、情報セキュリティ、プライバシー、セキュリティ



大久保美也子　（おおくぼ　みやこ）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（工学）
暗号理論、暗号プロトコル

盛合志帆　（もりあい　しほ）
サイバーセキュリティ研究所
セキュリティ基盤研究室
室長
博士（工学）
暗号技術、セキュリティ評価、プライバシ保護技術