２０１２年度　第３回暗号技術検討会　議事概要

１．日時　平成２５年２月２２日（金）　１５：００～１６：１５

２．場所　経済産業省本館２階　２東３共用会議室

３．出席者（敬称略）

構成員：今井 秀樹（座長）、辻井 重男（顧問）、太田　和夫、岡本 栄司、金子 敏信、国分 明男、佐々木　良一、武市 博明、近澤 武、中山 靖司、本間 尚文、時田 俊雄（松井 充 構成員代理）、松尾 真一郎、松本 勉、松本 泰、渡辺　創

オブザーバ：三角 育生、羽室 英太郎、大平　利幸（栗原 利男代理）、中山 紀雄（濱島 秀夫代理）、楢木野 由善（中村 耕一郎代理）、浜田 和之（代田 雅彦代理）、谷口　晋一（木村 和仙代理）、平 和昌、寶木 和夫、笹岡 賢二郎

暗号方式委員会事務局：盛合 志帆（独立行政法人情報通信研究機構（ＮＩＣＴ））

暗号実装委員会事務局：大熊 建司（独立行政法人情報処理推進機構（ＩＰＡ））

暗号運用委員会事務局：神田 雅透（独立行政法人情報処理推進機構（ＩＰＡ））

暗号技術検討会事務局：

総務省　阪本 泰男、山碕 良志、上原 哲太郎、飯田 恭弘、吉田 丈夫、橋本 直樹

経済産業省　中山　亨、上村 昌博、中谷 順一、守山 速飛

４．配布資料

（資料番号）	（資料名）
資料１	「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）に対する意見並びにこれに対する総務省及び経済産業省の考え方（案）
資料２	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）
資料３	今後の検討課題に関する方針（案）
資料４	2013 年度 暗号技術検討会及び関連委員会の体制（案）
参考資料１	2012 年度 第２回 暗号技術検討会議事概要
参考資料２	次期電子政府推奨暗号リスト策定スキーム
参考資料３	電子政府推奨暗号リスト（現行リスト）
参考資料４	2012 年度　暗号技術検討会　構成員・オブザーバ名簿
参考資料５	「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）に対する意見募集（平成 24 年 12 月 12 日報道発表）
参考資料６	2012 年度　CRYPTREC シンポジウム開催のご案内

５．議事概要

１　開会

暗号技術検討会事務局から開会の宣言があり、総務省の阪本政策統括官から開会の挨拶。

参考資料４について、岡本 龍明構成員、松井 充構成員（時田 俊雄氏が代理出席）、持麾 裕之構成員は欠席。

２　議事

（１）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）について【承認事項】

資料１及び資料２に基づき、意見募集で寄せられた意見に対する考え方、意見募集の結果を踏まえたCRYPTREC暗号リスト（案）を暗号技術検討会事務局から説明。質疑等なし。原案どおり承認。

（２）今後の検討課題に関する方針（案）ついて【討議事項】

資料３に基づき、今後の検討課題に関する方針案を暗号技術検討会事務局から説明。以下質疑等を踏まえた修正については座長に一任され、暗号技術検討会事務局にて修正案を作成、座長の確認後、各構成員にメールにて送付されることとなった。

○CRYPTRECに求められる活動

辻井顧問：資料中にも触れられているが、プライバシー保護等と個人情報活用の両立にあたって、暗号技術を活用することが求められている。主催しているフォーラムでも暗号の重要性を発信しているが、例えば医療の現場等、なかなか社会に理解されない印象がある。管理（Management）、倫理（Ethics）、法制度（Law system）及び技術（Technology）を合わせて「MELT」とすれば、これら四者の密接な結合と連携による「MELT-UP」が今まさに求められている。暗号化されていればプライバシー情報とすべきではないとの意見がある、とは第２回検討会においても議論があったが、暗号の活用を考えれば技術論だけでなく、法律家との連携が求められている。暗号の活用方法の一つとして電子署名があるが、社会保障・税番号制度における公的個人認証のように電子行政全体の在り方を考えていくことがどこかの場で必要ではないか。

松本（泰）構成員：同様に、CRYPTRECとして視野を広げるべきとの観点から２点申し上げたい。１点目は例えば「２．暗号技術に関する検討」においても「暗号応用」としてプロトコルだけに着目されているが、もっと広く、例えばプライバシー保護等のニーズから求められている暗号の応用にCRYPTRECが視野を広げるべきではないかということ。２

点目は、評価された暗号アルゴリズムが簡単には破れることのない、信頼できる技術に成熟してきた現状を踏まえ、国産暗号アルゴリズムの普及だけにとどまらず、広義の暗号技術の普及のために必要な活動にCRYPTRECが取り組むべきなのではないか、ということ。例えば米国のHIPPAでは暗号化していなかった場合の情報流出に対するペナルティが定められており、これが暗号技術製品開発の強いインセンティブになっている。また、ネット選挙活動の実施のためには、例えばS/MIME技術を活用した電子メールへの電子署名が有用であり、このような応用分野にも目を向ける必要があるのではないか。

佐々木構成員：松本（泰）構成員の御発言と一部重複するが、暗号アルゴリズムそのものは信頼できても、プロトコルまで視野を広げると現実的な攻撃の脅威が知られている。現在の検討会は主に暗号アルゴリズムの専門家で構成されていると思うが、求められる課題によって体制も変えていく必要があるだろう。

辻井顧問：欧州のENISAでも、インシデントが起きた際にどれだけ準備していたかで措置が変わってくるとも聞いている。セキュリティ政策の全ての課題をCRYPTRECで担うべきとは思わないが、社会のニーズに着目してキメの細かい議論が暗号利用の現場、法律家とも求められているように感じる。

今井座長：セキュリティ政策全体を考えたときには、やるべきことは多い。それぞれの役割の中で、CRYPTRECとしては何をするのか、具体論を描いていく必要があるのではないか。

暗号技術検討会事務局：CRYPTREC以外の関係者と対話し、他の組織や会議体と連携することも模索したい。体制を含んで本格的に検討を開始するとなれば、来年度、再来年度にかけて腰を据えて取り組んでいくことも考えたい。また、CRYPTRECシンポジウム2013でも、本日頂いた御意見を踏まえた今後の取組の発信を考えたい。また、暗号アルゴリズムに議論が閉じていることが暗号技術の普及が進まない一因との意見も聞かれる。資料との関係で言えば、１－ウの「普及展開の促進策」については暗号アルゴリズムに着目した普及であるが、３－アの「暗号技術の利用促進」については、暗号アルゴリズムだけでなく、その応用分野に取り組んでいく方針として捉えており、本日頂いた御意見に留意して今後のCRYPTRECの活動を進めていきたい。

○小改定の実施時期

松本（勉）構成員：資料中、次回小改定の時期について「３年（又は２年）」とあるが、３年か２年かはいつ決めるのか。仮に２年だとすれば、作業スケジュールの関係から早めに決定する必要があるのではないか。

暗号技術検討会事務局：利用実績調査をどの頻度で実施するかも考慮し

なければならない。構成員の方々から２年とする御意見があるかは、伺いたい。また、２００９年度の公募時点で３リストの関係を図示した際に、推奨候補暗号リストから削除するにあたって「３年経っても製品化されないもの」の記載があるため、３年目の利用実績調査を先に示した。

松本（勉）構成員：コスト的な視点から、２年とすることは難しい面がある、と受け取って良いか。

暗号技術検討会事務局：予算の確保だけの面で言えば、２年ごとの利用実績調査を実施することは不可能でない。１０年間の中で、どのように定期的に利用実績を確認していくべきか、という視点に立ち、２０１３年度第１回検討会において各委員会の活動計画を承認するまでに、明確化することとしたい。

松本（勉）構成員：暗号運用委員会では今回のリスト案作成のための利用実績調査で、ノウハウが蓄積された側面もある。次に調査が必要となった場合には、今回より効率的な方法で実施することができるだろう。

〇軽量暗号の検討の進め方

今井座長：軽量暗号の取扱いに係る検討の進め方についてはいかがか。

暗号方式委員会事務局：軽量暗号が利用されている用途、求められているニーズについて検証するため、ＷＧを設置して検討していきたいと考えている。

今井座長：最初の小改定が２年後だとすると、間に合うか。

暗号方式委員会事務局：もう少し長いスパンでの検討を想定していた。

今井座長：軽量暗号については、いわゆる国産暗号としての強みもあり、暗号技術の普及、産業競争力の強化の観点から CRYPTREC としても是非取り組むべき課題だと認識している。標準化の進捗に照らしても、早めの検討が求められているのではないか。

〇人材育成

松本（勉）構成員：「暗号人材育成に向けた取組」については、プライバシー保護と個人情報活用の両立のニーズだけが具体的に言及されているが、より多様な人材が求められているのではないか。例えば、１０年後の CRYPTREC 事務局が務まる人材、暗号をベースに産業界で活躍する人材、暗号研究を担う人材、暗号の標準化を推進する人材もある。

暗号技術検討会事務局：具体的に記載する修正案を考えたい。

今井座長：本日の議論をもとに、資料の修正案を暗号技術検討会事務局にて作成頂きたい。また、今後の修正については座長に一任願いたい。

（異議無し）

暗号技術検討会事務局：資料の修正版については、座長に御確認頂いた後、構成員の皆様にメールで配付することとし、また、来年度の各委員会の活動計画に反映させていくこととしたい。

（３） 2013 年度 暗号技術検討会及び関連委員会の体制（案）について【承認事項】

資料４に基づき、2013 年度の暗号技術検討会及び関連委員会の体制（案）について暗号技術検討会事務局から説明。質疑等なし。原案どおり承認。

（４） その他

暗号方式委員会事務局から、CRYPTREC シンポジウム 2013 の開催について、プログラム及びパネルディスカッションの概要が説明された。

３ 閉会

経済産業省の中山商務情報政策局審議官から閉会の挨拶。

暗号技術検討会事務局から、次回暗号技術検討会の時期、場所等の詳細については、別途連絡する旨が説明された。

以上