第４回　CRYPTREC の在り方に関する検討グループ　議事概要

１．日時　平成２７年８月３日（月）　１７：００～１９：００

２．場所　経済産業省本館９階西８共用会議室

３．出席者（敬称略）

構成員：松本勉(座長)、上原哲太郎、太田和夫、近澤武、手塚悟、松本泰、盛合志帆

オブザーバ：NISC（森安隆、大川伸也）

事務局：総務省（大森一顕、中西悦子、筒井邦弘、丸橋弘人、今野孝紀）

経済産業省（上村昌博、上坪健治、中野辰実、中村博美）

４．配布資料

（資料番号）	（資　料　名）
資料１－１	第２回議事概要（案）
資料１－２	第２回議事録（案）　※関係者限り
資料２	CRYPTREC の在り方に関する検討グループまとめ案 ※関係者限り
参考資料１	CRYPTREC に関する現状について（第２回事務局配布資料）

５．議事概要

１　開会

事務局から開会の宣言があり、参考資料１に関して、前回会合での構成員意見を追記した旨説明があった。

２　議事

（１）前々回の議事確認と今回の議論の進め方について

前々議事概要については、文書の体裁についてコメントがあり、事務局が修正し、後日再度構成員にメールにて展開することとなった。

（２）CRYPTREC の在り方に関する検討グループまとめ案

資料２に基づき、以下のポイントについてこれまでの議論の振り返りと事務局提案がなされた。

①システムにおける暗号技術のセキュリティ確保の全体俯瞰図

②CRYPTREC の活動の目的の見直し

③CRYPTREC の対象となる活動領域の見直し

④CRYPTREC の活動及び成果物の主な適用範囲の見直し

⑤CRYPTREC の成果物

⑥タスク整理と体制の見直し

（３）全体を通しての意見交換

議事（２）の説明を踏まえて行われた意見交換の内容は以下のとおり。

①システムにおける暗号技術のセキュリティ確保の全体俯瞰図について

松本座長：事務局資料の全体俯瞰図について、カバーすべきところは位置づけられていると思うが、何か意見はあるか。

松本（泰）構成員：CRYPTREC が使用している「危殆化」と、認証事業者が使用している「危殆化」にはずれがある気がする。認証事業者がいう「危殆化」とは「鍵の危殆化」を意味しており、取り返しのつかないことを意味する。例えば B-CAS カードは「危殆化」した典型的な例としてあげられる。また、オランダの認証事業者である DigiNotar 社の例では、認証局がクラッキングされて不正な証明書が発行され、その結果 DigiNotar 社は倒産しサービスも停止した。これは、暗号鍵の危殆化に近い。CRYPTREC で議論している「危殆化」が「暗号アルゴリズムの危殆化」だけを意味しているのかが気になる。

盛合構成員：「危殆化」が生じた場合、システム全体までに重大な影響を与える可能性があるため、暗号アルゴリズムとシステム全体の両方の意味が含まれていると考えた方がよいのではないか。

手塚構成員：以前暗号が「危殆化」した際（SHA-1）、各事業者が 2048 ビットに変更するために相当時間を要した。

松本座長：確かに、「危殆化」の解釈を俯瞰図に反映させたほうが、この図の説明能力が増すと思う。鍵が漏れたことに対する対応と、暗号が弱くなって交換することでは意味が違う。またシステム開発時のセキュリティの危殆化も色々な種類が考えられる。

②CRYPTREC の活動の目的の見直しについて

松本座長：CRYPTREC の目的の見直しに関する課題及び事務局案の提起があった。内容として CRYPTREC 暗号に暗号アルゴリズムだけでなくて、暗号プロトコルをもう少し含めること、関係機関との連携及び政策提言が追記されているが、意見があるか。

手塚構成員：CRYPTREC の活動がシステム全体のセキュリティに関連していくという図となっているが、どこまでフォローするのか。暗号プロトコルまで活動範囲を広げることには構成員の皆さんが合意していると思うが、その先は NISC の政府統一基準なのか、CRYPTREC と NISC がどのように切れ目無く連続的に活動範囲を埋め合うのか、他の中間組織の関与が必要なのか、先を見据えた全体のフレームワークの議論が必要。

松本座長：CC や EDSA などが、手塚構成員の言う中間組織に当たるのか。NISC の担当業務は非常に幅広く、その中で暗号が関係する部分は CRYPTREC が担当している。現行

の CRYPTREC の活動の延長で政府統一基準すべての面倒をみるかどうかは曖昧になっている。

手塚構成員：そこが難しい。

松本座長：検討グループの議論で課題がある、ということは明らかになったが、今は課題の洗い出し段階であり、まだギャップが残るままでも良いと思う。

上原構成員：CRYPTREC の活動の出口はあくまでも政府統一基準だと思う。意識しなくとも、政府統一基準は一般向けシステム用の基準にいろいろな意味で引用されているため、電子政府と一般向けシステムの違いは余り意識する必要はなく、NISC との関係では、CRYPTREC の成果物を政府統一基準等にもっと入れ込んでもらえるかが大事。

松本座長：参照すべきものがないと NIST のドキュメントがまとまっているものとして便利で使い勝手が良いので、使われてしまうため、日本では CRYPTREC が暗号に関してドキュメントを作成・改定して貢献すべき。JCMVP の認証制度は、名指しで入れ込まれているわけではなく、日本ではそのような形で参照されている。CRYPTREC の守備範囲は暗号だが、電子政府に限定する必要はなく、政府統一基準は行政機関向けのものである。

事務局（経済産業省）：CRYPTREC 暗号リストは総務省・経産省の連名であり、政府統一基準に反映するように両省で調整した。NISC への提案、関係者との意見交換を踏まえ、より使い勝手の良いものとすることが事務局の役目であると理解している。

松本座長：暗号技術検討会の目的に、政策提言機能を入れ込むことに意見はあるか。

近澤構成員：昨年、活用委で普及促進や人材育成について提言をまとめたが、現行の体制でその提言を実行できるのか疑問を持っている。

松本座長：現行の体制だと難しいかもしれないが、少なくとも政策をつくる立場の人に本当に重要なことを、暗号技術の専門家が分かりやすく伝えていかなければいけない。CRYPTREC の活動のミッションに「政策提言」という言葉を入れ込むことが適切かわからないが、必要なことを検討して政策として提案していくことは大事。

上原構成員：政策提言を受け取る側がいないと、政策にならない。

松本座長：課題があり、それを検討して政策として実現する体制が必要であると考えているが、それは誰が担当すべきかが問題。

盛合構成員：前回のプレゼンでは活用委員会が担うべきと申し上げた。技術のみでなく、政府統一基準への記載、制度化が必要なのかなどを議論するのが活用委員会ではないか。

松本座長：活用委員会で対応すべきかも含め、CRYPTREC の活動として位置づけるべきだと考えるのであれば、政策提言という言葉よりも適した言葉はないか。

事務局（経済産業省）：政府では提言をそのまま受けとめられない部分もあるため、ブリッジできるよう対応していくことが大事。具体的な活動に向けて道筋をつけられるよう、受け止められる可能性があるか否かを含めて議論いただきたい。「政策提言」と

いうより「暗号技術の活用に向けた方策の提言」でよいのでは。

松本座長：提言すべき対象は「情報セキュリティ対策」が良いのではないか。

上原構成員：政府の情報セキュリティに関する対策に関わってくるのであれば、NISC に提言を受け取ってもらえるとありがたい。

手塚構成員：CRYPTREC からみた提言の宛先は総務省、経済産業省になるのか。

松本座長：そのとおり。

上原構成員：提言の範囲をもう少し広げて民間も含めた出口もあるのではないか。

松本座長：それでは、必ずしも政策という言葉を使わないことで検討を続けることとしたい。

③CRYPTREC の対象となる活動領域の見直しについて

松本座長：CRYPTREC の活動領域は必要なものを取り込んでいくこと、プロトコルについては CELLOS 側からどう協力してもらえるのか、実装や製品評価分野などの連携を議論したい。

太田構成員：政府システムからのインプットが有用とのことであるが、ここで言うインプットとは何を指しているのか。

事務局（総務省）：政府システムで使われているプロトコルの利用状況など、政府側からの情報提供がないと議論できないという発言を受けて記載したもの。

太田構成員：政府システムで利用されているプロトコルに対して、具体的に何かシステムを導入させたいという意向なのか。

事務局（総務省）：そこまでは意図していないが、政府で利用するシステム情報を提示することが CRYPTREC での検討に有用であると考えている。

松本座長：次に、事務局資料の「活動の網羅性」（プロトコル、システム運用、鍵管理、エンティティ認証等に CRYPTREC としてどう対応するのか）について意見はあるか。

太田構成員：非常に良い案ではあるが、実作業に落とすのは困難であると考えている。また、資料に「国産暗号（軽量暗号等）の普及促進」とあるが、CRYPTREC 関係者は軽量暗号を進めていることにどこまでアグリーしているのかは分かりかねる。とはいえ IoT 社会において軽量暗号は必要だと思うので、今後 10 年の CRYPTREC の成果となればよい。まずは提言に落とし込み、それを受け取ってくれる人がいればいいと思う。

松本構成員：太田構成員の議論は政府調達でなく、IoT の議論。IoT における軽量暗号の位置づけが俯瞰できると、提言先もわかるということか。

太田構成員：まずはインプット先をみつけ、産業界にもメリットがあるようなシナリオとしたい。

松本座長：政府統一基準の観点から、IoT 社会において、どのようなタイプの事柄に対して基準があるといいという議論が必要である。例えば暗号アルゴリズムが仮にいい加減でも鍵管理さえしっかりしていれば大丈夫だとか、また逆の事例もあるなど鍵管

理に係る基準は非常に重要であるのに日本では作っていない。NIST 基準が現時点で鍵管理の運用に影響を与えているが、CRYPTREC でも議論は可能ではないか。

軽量暗号については、CRYPTREC は、２年間かけて詳細なレポートも作成しており、これ程まとまったものは他にはないのではないか。

盛合構成員:軽量暗号の優位性などをまとめられたのは一つの成果だと思っている。NIST のワークショップでも軽量暗号をシステマティックに扱っていることに対する評価があった。さらに今後、軽量暗号をどう使ったら良いかのガイドラインを作成する方針である旨伝えたところ、参照したいなどのコメントがあった。

松本座長：公平な立場で軽量暗号を評価した一覧を作成することは、利用者の暗号選択に役立つが、それが一方で開発側にとっては一覧に入れ込むインセンティブにつながるということだと思うが、そこまでコンセンサスが得られているか。

盛合構成員：まだコンセンサスが得られてないが、公平に評価したガイドライン作成からはじめたい。

太田構成員：CRYPTREC の活動に対して、民間企業の研究者や技術者に協力してもらうために、政府統一基準への引用という出口に加え、もっと資金確保といったビジネスにつながるシナリオを書けるようになればよいのではないか。

松本座長：つまりそのようなシナリオがないと CRYPTREC の活動に対して、民間の研究者等がどれだけ協力してくれるのか分からず、研究員も個人的な支援であり、所属機関の業務の一部で対応できないのではないかという懸念があるということですね。

松本（泰）構成員：その意見に全く同意であり、暗号の重要性が増していることは間違いなく、暗号技術の重要性を一般の人、一般の技術者に理解してもらうためにも俯瞰図の作成は重要であるが、単なる技術マップではなく、社会にとってどう影響があるか、どのように産業競争力に貢献するかという観点から、一般の人や技術者に分かりやすいものにする必要がある。何分、暗号技術はその説明が困難であり、四苦八苦しているところ。

松本座長：IoT イコール軽量暗号ではなく、IoT だからこそ実現が難しい高度な暗号を使う必要があるかもしれず、暗号の重要性はさらに増していると考えられる。そのため、産業活性化のために、暗号に携わる人材を確保していかなくてはならない。

上原構成員：暗号技術はひとつの標準化技術であり、標準化戦略は政府にて議論されているが、企業にとっては標準化すればするほど、特許料が少なくなるので、大きな標準化戦略を作り、その中で軽量暗号を位置づけるといった取組みがなければ、ビジネスとしての軽量暗号の標準化は困難と思われる。

松本座長：国際標準の重要性もあるが、国内需要を喚起し、まずは国内標準とすることが妥当なところか。その実装システムには専門家が必要となるので、そこにビジネスチャンスがあるのかもしれない。

近澤構成員：CELLOS との連携について、評価委員会と活用委員会のどちらになると考え

られるのか。

事務局（総務省）：CELLOS ではプロトコルの仕様を評価する活動と、実装の問題を踏まえて脆弱性を指摘する活動があると認識している。前者は評価委員会、後者は戦略 WG で議論が必要だが、その結果として活用委員会で検討を行うこともあり得ると考えている。

手塚構成員：CELLOS は立ち上げ当初は仕様レベルの確認をしっかりしていこうとしていたが、現在では一般への貢献を考慮し、運用段階のセキュリティの実運用を迅速に行うのがポイントであると考えている。暗号の場合、実運用がどういった状況か確認が難しいが、プロトコルでは実運用での脆弱性対応が多く、知見を活かすことができると認識している。

松本座長：CRYPTREC は実運用に関しては、現状機動力のあるアクティビティはできていない。

手塚構成員：ニーズがあり対応するべきことは理解するものの、具体的にどのように行動するのかよく見えない。

松本座長：現状の暗号技術の監視活動は、仕様段階については、研究者が論文で脆弱性を発表し、当該情報を収集する。開発段階では実装攻撃に対する情報収集を行っていると思う。運用段階での監視活動としては、危殆化対応規程を策定するなど対応はした。しかし、実運用面でサービスとして常時頼りになる活動は現状実施できていない。

手塚構成員：プロトコルでは時々問題が発生しているが、万一暗号について実運用レベルで脆弱性が発生した場合、システムには大きなリスクが生じる。

事務局（経済産業省）：参考の事例としてはこの間の MISTY に関するまとめがある。

事務局（総務省）：アルゴリズムレベルでも、緊急に脆弱性対応が必要な場合には、実運用でどうすべきか CRYPTREC でも言及すべきだと思うが、今まで該当する事例がないためやっていないという認識である。

盛合構成員：CELLOS の速報も、必ず評価委員会が担当するのではなく、内容に応じて評価委員会、活用委員会と担当が違ってもいいのかもしれない。

近澤構成員：とはいえ、評価委員会と活用委員会の境界の案件の対応時にどちらが担当するかを決定するのにロスが生じる。プロトコル対応はどこか１つの委員会や WG でみることが理想だと思う。

松本座長：オペレーションセンターのような対応が必要かもしれない。

盛合構成員：それは NICT、IPA の共同事務局が行っていた。

松本座長：CELLOS のように速報対応するのであれば、評価委員会や活用委員会の事務局との兼任といったものではなく、専任の人を配置した体制が必要ではないか。

手塚構成員：監視、というよりも常時アンテナを張っておくことが必要となる。

松本座長：つまり、アンテナを出していて何かあったらすぐ有益な情報としてまとめて発表するために専任の人がいないと回らないということですね。

近澤構成員：網羅的なプロトコルのガイドラインをつくるには、システム開発と実運用両方の要素を一つとして捉えての対応が必要だと思う。プロトコルについて担当する委員会は一つの方が、成果が出しやすいと思う。

松本座長：プロトコルにも、様々なレベルものがあり、かなり対応も異なると思うが、関係者がアウトプットを出すに当たり、効率的な体制づくりを選択すべきという理由は理解できる。

手塚構成員：組織を運営していくには、定期的な対応と、突発的事象への対応があるので、後者のような組織構造が必要になってくる。

松本座長:仕事の種類が異なるのであれば､体制もそれに適したものとする必要がある。

手塚構成員：CRYPTREC にて運用面での活動も行うとした場合に、どのような構造にするかよく検討が必要。

松本座長：機動力をどうやって確保するかがポイントとなる。問題がいつ発生するか分からないため、暗号監視活動は今回の MISTY の件も含め、手間がかかる。

盛合構成員：NICT では人的ネットワークを活用して監視はしている。

松本座長：NISC の政府統一基準に活用させるべく、運用段階の体制を強化するならば、どうすれば良いか。例えば、CELLOS にどうやって協力してもらえるのかを今後の論点としたい。

⑤CRYPTREC の成果物について

松本座長：「政府調達に向け統一基準から参照可能な成果物体系の議論を引き続き継続」という記載があるが、目にみえる形にすることや適切な情報発信の在り方については、先程の議論と関係するため、今後の案件として整理したい。

⑥タスク整理と体制の見直しについて

太田構成員：「システム全体における暗号技術のセキュリティ確保」とは、システム全体におけるセキュリティ確保で暗号技術に関連した部分という意味か。

事務局（総務省）：俯瞰図全体のことを指しており、暗号技術に限るという前提で、このシステム全体において、いろいろな段階のものがあるという意味で使っている。

松本座長：35、36 ページが非常に重要。検討グループを４回開催し、様々な議論できたことは非常に有意義である。今後、戦略 WG を設置するのか，継続して議論するのかについて意見はあるか。

上原構成員：これまで開催した４回の検討グループにおいて、とても実のある議論ができたのは、この人数規模だからだと思う。暗号技術検討会は参加者が多すぎるため、承認ができても議論はできない。検討グループほどの人数規模の委員会等に実質的な全体戦略を決める機能を移し、具体的な案を打ち込むのであれば、名前を変えて改めて戦略 WG としてスタートした方がよい。また、暗号技術検討会に戦略 WG がどういう

位置づけか報告する必要がある。

近澤構成員：「戦略ＷＧ」において私や盛合構成員は、構成員と事務局のどちらの立場で参加することになるのか。

松本座長：盛合構成員と近澤構成員には、NICT や IPA の代表ということではなく、これまでの検討グループと同様に構成員として加わってほしい。

事務局（総務省）：戦略 WG は、検討グループの人数規模に２～３名追加し２年～３年で委員会構成を見直すことを想定している。検討グループの議論を引き続き行うこととなった場合は、もう少し短い期間で議論して、ある程度一定の結論が出たら解消するというイメージ。戦略 WG の場合は、今年度もしくは来年度を目処に機能をきちんと定義した組織を確立して何年か運用し、うまく運用できなければ組織の見直しを行うこともイメージしている。

事務局（経済産業省）：戦略 WG を立ち上げることには賛成であるが、立ち上げる際は、メンバー追加の必要性と提案の経緯を検討会構成員に対して丁寧に説明する必要がある。

松本座長：今後、検討グループの議論をまとめて、検討会での意見を踏まえて進めていくという理解で良いか。

事務局（経済産業省）：そのとおり。

松本座長：うまく回っていくような筋道がつけられ、戦略 WG 立ち上げとなった場合は、今年度から開始できるのか。

事務局（総務省）：今年度の第１回検討会でご承認いただき、今年度後半発足という案。拙速過ぎるならば、中間報告という形で報告し、引き続き検討する形を想定している。

松本座長：検討会構成員の皆さんの賛同を得ること、その説明は丁寧にやっていく必要がある。一方で、ある程度スピードをもった対応が必要であり、今いるメンバーに協力を仰ぎつつ、戦略 WG につなげていきたい。

上原構成員：これからの CRYPTREC の活動の出口として、電子政府推奨暗号として多く参照してもらえるような成果を想定しているのであれば、NISC のコミットは不可欠。どのように NISC にコミットしてもらえるかどうかを考えながら体制を進めたらよい。NISC が戦略を立てる上で、CRYPTREC に求めるものを上から落とせるようなチャネルを築くことが重要。

松本座長：NISC には CRYPTREC への要望を適切に言える形であれば良い。

上原構成員：NISC からは、政府統一基準にて求めるものが具体的に何なのか、ガイドラインであればこの分野を作成すれば助かるといった希望が入るとよい。NISC とのリンクの機能は別途議論してもらえれば良い。

松本座長：第１回検討会にて戦略 WG 立ち上げについて提案することとしたい。仮に提案がリジェクトされた場合、第５回検討グループを開催すれば良い。

盛合構成員：事務局体制については審議がなされていないが、どういった取扱いか。

松本座長：事務局体制については、これから議論する位置づけとしたい。

３　閉会

事務局から、第１回暗号技術検討会は９月下旬～１０月上旬に開催予定である旨の連絡があった。検討会の資料については、８月末～９月上旬までに事務局にて作成したものを構成員がメールにて審議することとなった。

以上