第３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７月３日（金）　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（奥山剛、大川伸也）

事務局：総務省（赤阪晋介、筒井邦弘、中村一成）

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	第２回議事概要（案）
資料２	「CRYPTREC で取り組む新しい暗号技術」（盛合構成員）
資料３	「これからの CRYPTREC について」（手塚構成員）
資料４	第１回及び第２回の論点整理

５．議事概要

１　開会

事務局から開会の宣言があった。

２　議事

（１）前回議事確認と本日の議論の進め方について

前回議事概要について、正式版は後日メールにて展開する旨、事務局より説明があった。

（２）CRYPTREC で取り組む新しい暗号技術

資料２に基づき、盛合構成員より説明が行われた。質疑応答は以下のとおり。

上原構成員：経済産業省のガイドラインにおいて、個人情報が「高度暗号化」されていれば漏えい時の通知義務が緩和されることになっている。「高度暗号化」に関する具体的な議論を行うことで、CRYPTREC として貢献できるのではないか。

松本座長：個人情報に関する議論に関しては、制度的な体系と技術的な体系が整理されておらず、各技術項目について具体的に何を示すのか明確化されていないということではないか。

手塚構成員：盛合構成員の考えとして、CRYPTREC の活動やテーマを拡張した方が良いと

いうことか。

盛合構成員：暗号プリミティブだけでなく、上位の暗号プロトコルについても対象とした方が良い。また、電子政府向けの暗号技術に限定せず、今後社会で活用が見込まれる暗号技術にも焦点を当てるべき。軽量暗号とプライバシー保護技術は最初のステップとして良い。今後１０年間を見据えて適切な時期に活動を開始するイメージ。

近澤構成員：軽量暗号のリストを作成する場合、既存のリストとの関係はどうするか。

盛合構成員：電子政府向けと IoT 向けでは基準が異なってくると予想されるので、別リストの方が良い。両者で重複する暗号技術もあると思うので、両者の関係性については別途議論が必要。

（３）これからの CRYPTREC について

資料３に基づき、近澤構成員より説明が行われた。質疑応答は以下のとおり。

太田構成員：「第３者判断」とは具体的にどのような意味か。

近澤構成員：従来の「技術中立性」の観点に加えて、ユーザ側の種々の制約を勘案した上で判断することを「第３者判断」と定義した。

太田構成員：暗号技術活用委員会の検討項目のうち「その他、暗号技術評価委員会で扱わない項目」として、具体的にイメージしているものはあるか。

近澤構成員：リスト改定時の評価基準に係る議論など。

事務局（総務省）：説明の中で、ガイドライン作成等の活動を IPA に任せるべきということと CRYPTREC のクレジットを付けることとの関係性はどのようになっているのか。現在の運用ガイドライン作成時のプロセスとどのように異なっているのか。

近澤構成員：具体的な作業プロセスはまだ十分に検討できていない。基本的に、どのようなガイドラインを作るべきかを決定するのは CRYPTREC であり、作業の部分を IPA で行うイメージ。

手塚構成員：実施する組織単位で考えるのではなく、まず機能面に着目して議論を進めた方がよい。暗号技術に係る取組として必要と思われる機能を俯瞰図に表し、次にそれぞれの機能を担う組織はどこか、といった順番で議論した方がよい。

（４）第１回、第２回の発言ポイントまとめ

資料４に基づき、事務局より説明が行われた。

（５）全体を通しての意見交換

議事（２）～（４）までの議論を踏まえて行われた意見交換の内容は以下のとおり。

松本座長：機能面に着目して俯瞰的に考えることに賛成である。論点として、CRYPTREC が扱う技術をプロトコルやシステムのレイヤーにまで広げるかという点、成果物の適用範囲を電子政府から広く一般社会へ広げるかという点の２点がある。

手塚構成員：第２回会合の資料２に示されていた俯瞰図が分かりやすい。この図にある「設計フェーズ」「実装フェーズ」について別々に議論した方がよい。現在の CRYPTREC の取組は「設計フェーズ」の「暗号の安全」に関するものだが、拡張の方向性として「実装フェーズ」の方向と上位レイヤーに向かう方向とがある。さらに、そもそも暗号技術全体についてどの組織がどのように取り組むべきか決定する、上位の機能を設定することも考えられる。議論にあたって「設計フェーズ」と「実装フェーズ」をしっかり分けて考えることが重要。

松本座長：これまでの議論で、暗号アルゴリズムを中心に行ってきた従来の活動を拡張する方向として、軽量暗号等の新しい暗号アルゴリズムや、取組が不十分であるプロトコルや製品・システムレベルでの取組が挙げられた。ただし、プロトコルや製品・システムレベルの領域には様々なものが含まれており、整理が必要。

手塚構成員：「設計の安全」はセキュリティ・バイ・デザインといえる部分であり、「実装の安全」は製品やシステムが設計通りに作られているか評価するフェーズ。

松本座長：安全性確保に係る取組として、学会での情報収集等による安全性評価・監視活動といったアルゴリズム・プロトコルレベルのものと、実装の確認や脆弱性対策といった製品レベルのものがある。

近澤構成員：公的機関が行う普及促進の活動はアルゴリズムレベルで行うもの。プロトコルや製品といったレイヤーに係る取組はガイドライン作りとなるのではないか。

手塚構成員：CRYPTREC 暗号リストの作成も、普及促進の観点を含んだ活動だと思う。

松本座長：CRYPTREC 暗号リストでは、安全な暗号技術の選択肢が単純に示されているだけであり、使用方法にまで言及していない。「設計の安全」自体もいくつかの段階に分けられるのではないか。

松本座長：CRYPTREC の現在の活動内容は、暗号アルゴリズムに関する安全性評価・監視活動と、国産暗号の普及促進に係る取組である。また、政府調達に関して、暗号アルゴリズムだけでなく、プロトコル等の上位レイヤーについても安全性確保が必要だが、現在はどのような仕組みになっているのか。

手塚構成員：政府統一基準においては明確な形では行われていない。

上原構成員：CRYPTREC 暗号リストの掲載はあるが、JCMVP について記載されていないし、CC についても強制されていない。

奥山オブザーバ：認証を取得した製品が存在しない分野があるため、強制することができない。

松本座長：なるべく多くの分野で安全性が担保された製品を調達できるようにすることが必要。CRYPTREC として貢献できる部分はあるか。

盛合構成員：政府統一基準等の文書において、CRYPTREC 暗号リスト以外の CRYPTREC の成果物が参照されるようになると良い。

松本（泰）構成員：「高度暗号化」について、議論にあたっては暗号技術以外の技術も含

めた中立性が求められる一方で、暗号技術を前提とした強制力のある要件を決めないと実質的に産業競争力があるソリューションが出てこないという問題がある。

手塚構成員：「高度暗号化」について定義しても、製品がなければ基準の意味がない。基準が作られた後にすぐ製品が作られるよう工夫する必要がある。

上原構成員：「高度暗号化」することで当事者への連絡や、場合によっては情報の存在自体を公表せずとも良いこととされているが、インセンティブとして小さく、具体的なルールも定められていない。

松本（泰）構成員：暗号技術による個人情報保護に関して、適切な鍵管理が最も重要である。また、個人情報を暗号化した際に利用した暗号化鍵を廃棄した場合に個人情報を消去したものとして取り扱えるか、検討する必要がある。暗号化鍵の管理が適切に行われており、その暗号化鍵を破棄したことが証明できれば個人情報を消去したものとして取り扱えるのではないか。

松本座長：個人情報保護のために暗号技術をいかに使用できるか、という論点であるが、CRYPTREC が様々な助言を行えるようになるべき。課題の分析が必要であるが、現在は暗号技術と制度に係る論点はどこで議論されているのか。

手塚構成員：適切に鍵管理を行うためには、暗号専門家とシステムエンジニアの両者の知見を合わせる必要がある。CRYPTREC でそのような場を提供できないか。NIST の SP 文書に鍵管理に関するものがあるが、これらの文書は両者の協力なくしては作成できない。

松本座長：部品としての暗号の安全性確保は大前提として、技術の社会への適用を進めることが肝要。制度設計として技術要件をあえて厳しく設定することも考えられ、米国等で上手く機能しているが、日本では誰が議論するのか。

盛合構成員：システムエンジニアの視点は暗号技術活用委員会で担うことができるのではないか。システム運用に知悉した委員が含まれており、さらに追加することも可能。制度面の課題や必要とされる文書等について議論できるのではないか。

松本座長：現在日本で基準がない部分について、米国の SP 文書を参照しているが、海外の文書に依存することは好ましくない。アルゴリズムより上位のレイヤーについて「設計の安全」「実装の安全」両面から日本として取り組むことが必要。一方で、軽量暗号については、ある程度体系的に整理できると考えているか。

盛合構成員：整理できると考えている。

手塚構成員：別の論点であるが、CRYPTREC の文書を体系化すると良いのではないか。検討経緯や改定プロセスが外部から確認出来た方がよい。

松本座長：暗号アルゴリズムからプロトコル、製品といった上位レイヤーにまで活動範囲を広げるべき。全てを CRYPTREC がカバーできるか分からないが、本検討グループを通じて俯瞰図を共有し、現状を整理できるとよい。また、成果物の適用範囲として電子政府から IoT に広げた方が良いという論点もあった。

盛合構成員：軽量暗号は数多く提案されており、これらの特徴や比較方法についてガイドラインを作成したい。また、軽量暗号のリストがあるとユーザにとって利便性が高い。

松本（泰）構成員：電子政府推奨暗号リスト以外の暗号を使用することによるシステム利用者からの不安を緩和できるという効果があり、リストは有用。

松本座長：CRYPTREC 暗号リストへの信頼性との並びを考えると、軽量暗号のリストの取扱は十分に検討する必要がある。盛合構成員が発表で言及された個人情報保護や匿名化のための技術には暗号技術以外の技術も含まれる。

盛合構成員：そのとおり。ただ、まだどのような技術を使うかそもそもリストアップもされていない段階である。

松本座長：CRYPTREC としてどこまで活動範囲を広げるか、あえて限定する必要はない。セキュリティ技術について評価・意見する主体も他に存在しないため、受け手を考えずとりあえず情報発信していくことが必要。

松本（泰）構成員：エストニアでは SHAREMIND という暗号技術、秘密通信を使い複数機関にあるデータを直接結合せずに統計情報を得る取組がある。有用な仕組みではあるが、同様の取組を現行法制下の日本で行うことは困難である。プライバシー保護等に有効な暗号技術は、法制度との整合なしには発展しない側面がある。

上原構成員：プライバシーの議論で安全性の白黒を明確にすることは困難。技術論だけでなく運用面からも議論し、決断して線を引くことが必要。そのための決定権限があると良い。

盛合構成員：個人情報保護技術や匿名化技術に関する基準作りは、政府主導の取組だけでなく、草の根的な活動も始まりつつある。CRYPTREC でも同様の議論を行うことが可能。

松本座長：CRYPTREC の活動に関するその他の大きな論点として、脆弱性対応等に CRYPTREC がどのように関与していくかという点がある。

手塚構成員：脆弱性にも、実装方法の問題で生じた脆弱性とプロトコルの理論そのものに欠陥があり生じた脆弱性の２種類がある。後者は標準化に際して十分に安全性が評価されていないことが原因であり、CELLOS で取り組んでいきたいと考えている部分である。

松本座長：現在 CRYPTREC では理論面での安全性評価・監視活動に注力しているので、対象とする技術範囲をアルゴリズムからプロトコルまで拡張するのであれば、プロトコルについても監視活動の対象になる。また、プロトコルとして適切に実装できるのかどうか確認することも必要であるが、JCMVP の対象範囲外であり、どのように安全性を確保していくかが課題である。最後に、日々発見される脆弱性に対する監視活動をどのように行っていくかという点がある。CELLOS の活動が参考になると思う。

松本座長：暗号プロトコルまで活動範囲に含めるのであれば、プロトコルの専門家に

CRYPTREC に参画してもらうことが必要。もしくは、外部の団体に依頼することも考えられる。また、活動全般に関して、CRYPTREC から IPA や NICT に作業を依頼し、CRYPTREC の会議体で確認するというスキームも考えられる。

手塚構成員：CRYPTREC の権限や責任に関する制度上の位置づけが不明確であるという点も課題。現在、機能面に着目して議論を進めているが、権限の与え方まで含めて議論することが肝要。

松本座長：権限の与え方等の制度設計に必要な材料について議論し、政策決定者へ提供する立場である。NISC、総務省及び経済産業省に判断してもらえるよう、情報共有をしていくことが大切。

手塚構成員：問題意識として、CRYPTREC と他団体との連携がどのような関係性であるのか不明確であるという点である。どのような機能が必要であるか決定したあと、機能実施群の権限を決める必要があるので、その点を意識しつつ議論を進めるべき。

３　閉会

事務局から、第４回の日程について連絡があった。

以上